

TACACS+-verificatiedomein configureren in UCS Manager met ISE Server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratie](#)

[TACACS+-configuratie op ISE](#)

[Opzetten van TACACS+ op ISE](#)

[Configureer de attributen en regels op ISE](#)

[TACACS+-configuratie op UCSM](#)

[Rollen voor gebruikers maken](#)

[Een TACACS+-provider maken](#)

[Een TACACS+-providergroep maken](#)

[Een verificatiedomein maken](#)

[Problemen oplossen](#)

[Gemeenschappelijke TACACS+-kwesties inzake UCSM](#)

[UCSM-beoordeling](#)

[Gemeenschappelijke TACACS+-kwesties inzake ISE](#)

[ISE-beoordeling](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt de configuratie beschreven van de verificatie Terminal Access Controller Access-Control System Plus (TACACS+) op Unified Compute System Manager (UCSM). TACACS+ is een netwerkprotocol dat wordt gebruikt voor authenticatie-, autorisatie- en verantwoordingsdiensten (AAA), het biedt een gecentraliseerde methode om Network Access Devices (NAD) te beheren waar u regels kunt beheren en maken via een server, in dit gebruiksscenario gebruiken we Identity Services Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco UCS Manager (UCSM)
- Terminal Access Controller Access Control System Plus (TACACS+)
- Identity Services Engine (ISE)

Gebruikte componenten

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

- UCSM 4.2 (3d)
- Cisco Identity Services Engine (ISE) versie 3.2

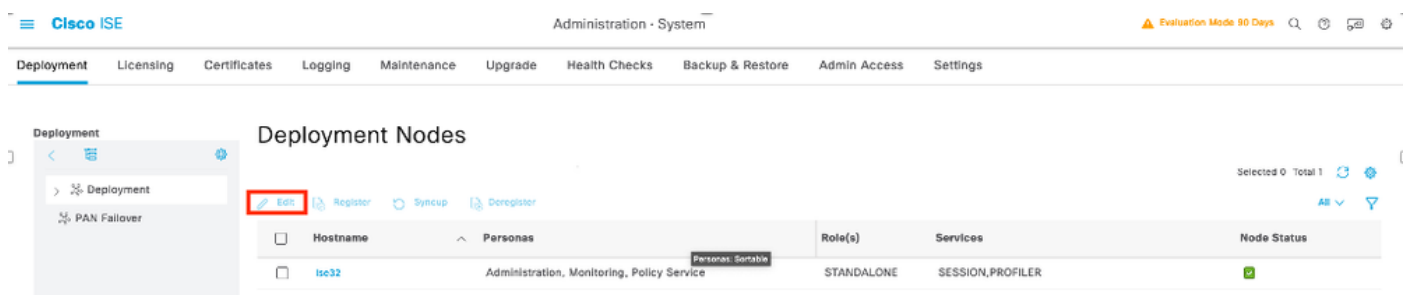
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratie

TACACS+-configuratie op ISE

Opzetten van TACACS+ op ISE

Stap 1. De eerste taak is om te controleren of de ISE de juiste mogelijkheden heeft om TACACS+-verificaties te verwerken, zodat u moet controleren of u in de gewenste Policy Service Node (PSN) de functie voor Device Admin Service hebt, bladert u door het menu Beheer > Systeem > Implementatie, selecteert u de node waar de ISE TACACS+ uitvoert en selecteert u de knop bewerken.



Stap 2. Scroll naar beneden totdat u de bijbehorende functie ziet met de naam Apparaatbeheerservice (merk op dat u voor deze functie eerst Policy Server-persona op de node moet hebben ingeschakeld en bovendien licenties voor TACACS+ beschikbaar moet hebben in uw implementatie), selecteer dat selectievakje en sla de configuratie op:

Cisco ISE Administration · System Evaluation Mode 90 Days

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Other Monitoring Node

☐ Dedicated MNT

☒ Policy Service

☒ Enable Session Services

Include Node in Node Group
None

☒ Enable Profiling Service

☐ Enable Threat Centric NAC Service

☐ Enable SXP Service

☐ Enable Device Admin Service

☐ Enable Passive Identity Service

☐ pxGrid

[Reset](#) [Save](#)

Stap 3. Configureer het Network Access Device (NAD) dat de ISE als TACACS+ gebruikt als server, navigeer naar het menu Beheer > Netwerkbronnen > Netwerkapparaten en selecteer vervolgens de knop +Toevoegen.

Cisco ISE Administration · Network Resources

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM

Network Devices

Default Device

Device Security Settings

Network Devices

[Edit](#) [+ Add](#) [Duplicate](#) [Import](#) [Export](#) [Generate PAC](#) [Delete](#)

☐	Name	IP/Mask	Profile Name	Location	Type	Description
No data available						

Stap 4. Configureer in deze sectie:

- Een naam voor de UCSM om de TACACS+-client te zijn.
- De IP-adressen die de UCSM gebruikt om verzoeken naar ISE te sturen.
- TACACS+ Shared Secret, dit is het wachtwoord dat moet worden gebruikt om de pakketten tussen de UCSM en ISE te coderen

Network Devices

Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM pxGrid Direct Connectors Location Services

Network Devices List > USCM

Network Devices

Name USCM

Description

IP Address * IP: 10.31.123.9 / 32

IP Address * IP: 10.31.123.8 / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type All Device Types Set To Default

☐ RADIUS Authentication Settings

☒ TACACS Authentication Settings

Shared Secret Show Retire

☐ Enable Single Connect Mode

☒ Legacy Cisco Device



Opmerking: voeg voor een clusterconfiguratie de IP-adressen van de beheerpoort toe voor beide verbindingen. Deze configuratie zorgt ervoor dat externe gebruikers kunnen blijven inloggen als de eerste verbindingsoververbinding mislukt en het systeem niet overschakelt naar de tweede verbindingsoververbinding. Alle aanmeldingsverzoeken zijn afkomstig van deze IP-adressen, niet van het virtuele IP-adres dat wordt gebruikt door Cisco UCS Manager.

Configureer de attributen en regels op ISE

Stap 1. Maak een TACACS+ profiel, ga naar het menu Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles, en selecteer Add

Cisco ISE

Work Centers - Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles

Conditions >

Network Conditions >

Results

Allowed Protocols

TACACS Command Sets

TACACS Profiles

Add Duplicate Trash Edit

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile

Stap 2. In deze sectie configureert u het profiel met een naam en in de sectie Aangepaste kenmerken selecteert u Toevoegen, vervolgens maakt u een kenmerk van kenmerk VERPLICHT,

noemt u het cisco-av-pair en selecteert u in de waarde een van de rollen die beschikbaar zijn binnen de UCSM en voert u in dat als een shell-rol, in dit voorbeeld gebruikt u de rol admin en de geselecteerde invoer moet shell:roles="admin" zijn zoals hier wordt weergegeven,

Cisco ISE Work Centers · Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

Conditions > Name
UCSM PROFILE ADMIN

Network Conditions >

Results v Description

Allowed Protocols

TACACS Command Sets

TACACS Profiles

Task Attribute View Raw View

Common Tasks

Common Task Type **Shell** v

☐ Default Privilege (Select 0 to 15)

☐ Maximum Privilege (Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape (Select true or false)

☐ Timeout Minutes (0-9999)

☐ Idle Time Minutes (0-9999)

Custom Attributes

Add Trash v Edit

Type	Name	Value
☐ MANDATORY	cisco-av-pair	shell:roles="admin"

Cancel Save

Als u in hetzelfde menu de onbewerkte weergave voor het TACACS-profiel selecteert, kunt u de corresponderende configuratie van het kenmerk dat via ISE moet worden verzonden, controleren.

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Admin Policy Sets Reports Settings

Conditions > TACACS Profiles > UCSM PROFILE ADMIN
TACACS Profile

Name
UCSM PROFILE ADMIN

Description

Task Attribute View **Raw View**

Profile Attributes

cisco-av-pair=shell:roles=" admin"

Cancel Save



Opmerking: De naam cisco-av-pair is de tekenreeks die de attribuut-ID voor de TACACS+-provider biedt.

Stap 3. Selecteer op het vinkje en sla uw configuratie op.

Stap 4. Maak een Device Admin Policy Set die voor uw UCSM kan worden gebruikt, navigeer in het menu Work Centers > Device Administration > Device Admin Policy Sets, selecteer vervolgens vanuit een bestaande beleidsset het tandwielpictogram om vervolgens nieuwe rij invoegen te selecteren

Cisco ISE Work Centers · Device Administration Evaluation Mode 89 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	Default	Tacacs Default policy set		Default Device Admin			

Insert new row above

Reset Save

Stap 5. Noem deze nieuwe beleidsset, voeg voorwaarden toe afhankelijk van de kenmerken van de TACACS+-verificaties die op de UCSM-server worden uitgevoerd en selecteer als Toegestane protocollen > Standaardapparaatbeheer, sla uw configuratie op.

Cisco ISE Work Centers · Device Administration Evaluation Mode 89 Days

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

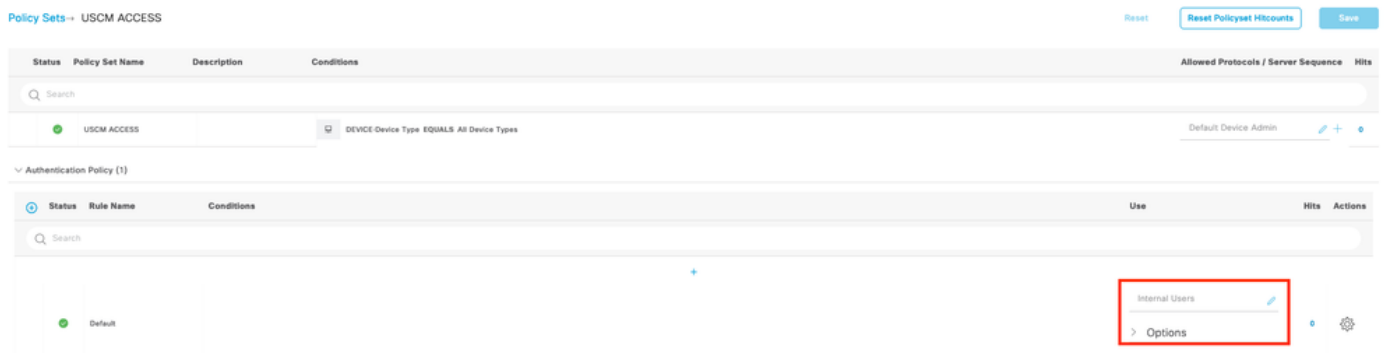
Policy Sets

Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	USCM ACCESS		DEVICE Device Type EQUALS All Device Types	Default Device Admin			
●	Default	Tacacs Default policy set		Default Device Admin			

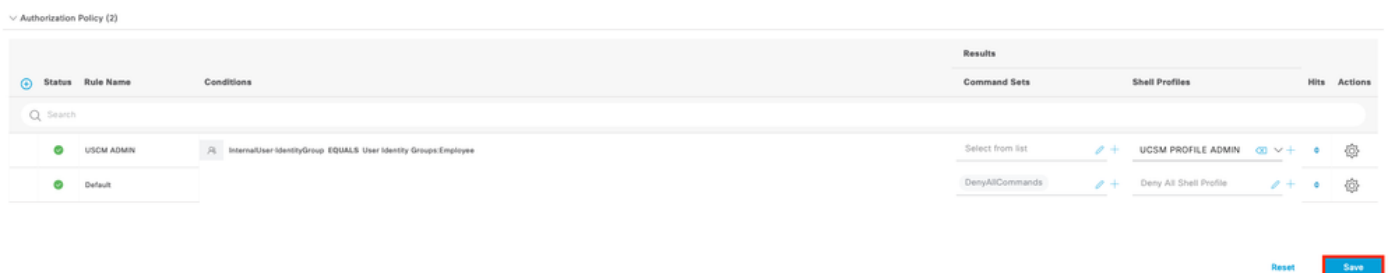
Reset Save

Stap 6. Selecteer in de optie > weergave en selecteer in de sectie Authenticatiebeleid de externe identiteitsbron van waaruit de ISE de gebruikersnaam en referenties opvraagt die in de UCSM worden ingevoerd, in dit voorbeeld komen de referenties overeen met interne gebruikers die zijn opgeslagen in ISE.



Stap 7. Scroll omlaag tot de sectie Autorisatiebeleid tot het standaardbeleid, selecteer het tandwielpictogram en plaats vervolgens één regel.

Stap 8. Geef de nieuwe autorisatieregel een naam, voeg voorwaarden toe met betrekking tot de gebruiker die al zijn geverifieerd als groepslidmaatschap en voeg in de sectie Shell-profielen het TACACS-profiel toe dat u eerder hebt geconfigureerd, sla de configuratie op.



TACACS+-configuratie op UCSM

Meld u aan Cisco UCS Manager bij de GUI met een gebruiker met beheerdersbevoegdheden.

Rollen voor gebruikers maken

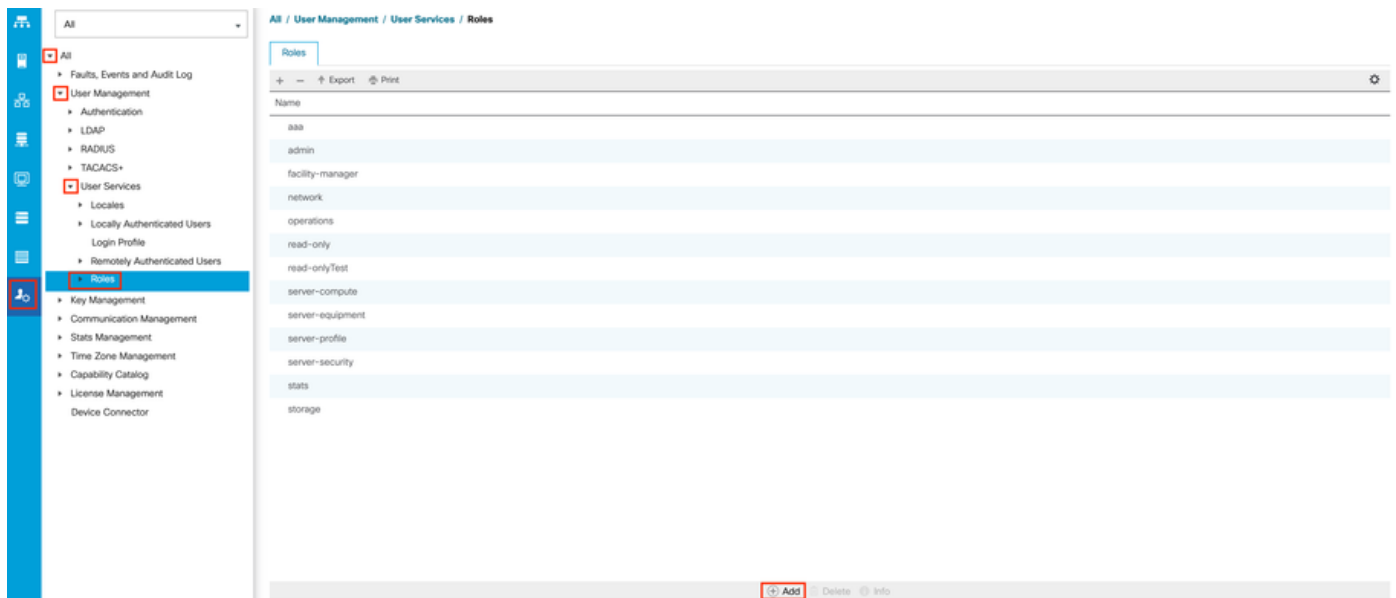
Stap 1. Selecteer in het navigatiedeelvenster het tabblad Beheer.

Stap 2. Vouw op het tabblad Beheer > Alles > Gebruikersbeheer > Gebruikersservices > Rollen uit.

Stap 3. Selecteer in het deelvenster General het tabblad.

Stap 4. Selecteer Toevoegen voor aangepaste rollen. Dit voorbeeld gebruikt standaard rollen.

Stap 5. Controleer of de naam van de rol overeenkomt met de naam die eerder is geconfigureerd in het TACACS-profiel.



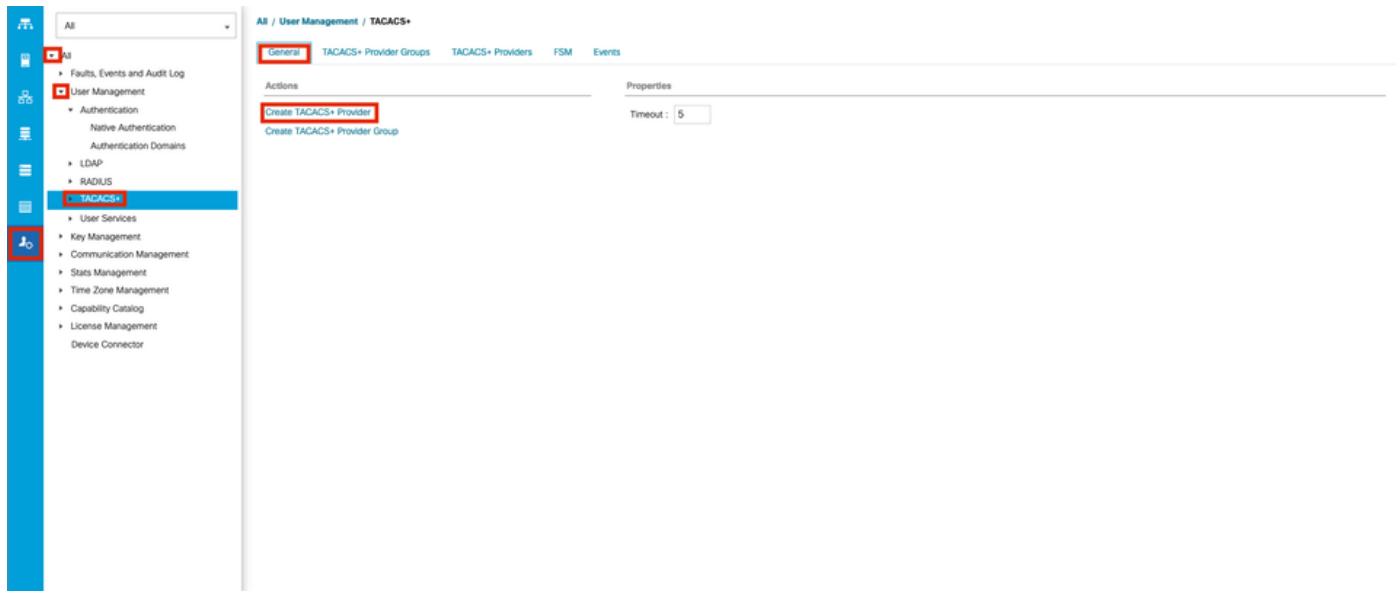
Een TACACS+-provider maken

Stap 1. Selecteer in het navigatiedeelvenster het tabblad Beheer.

Stap 2. Vouw op het tabblad Beheer Alles > Gebruikersbeheer > TACACS+ uit.

Stap 3. Selecteer het tabblad inWorkhetGeneral deelvenster.

Stap 4. Selecteer inActionshet gebiedCreate TACACS+ Provider.



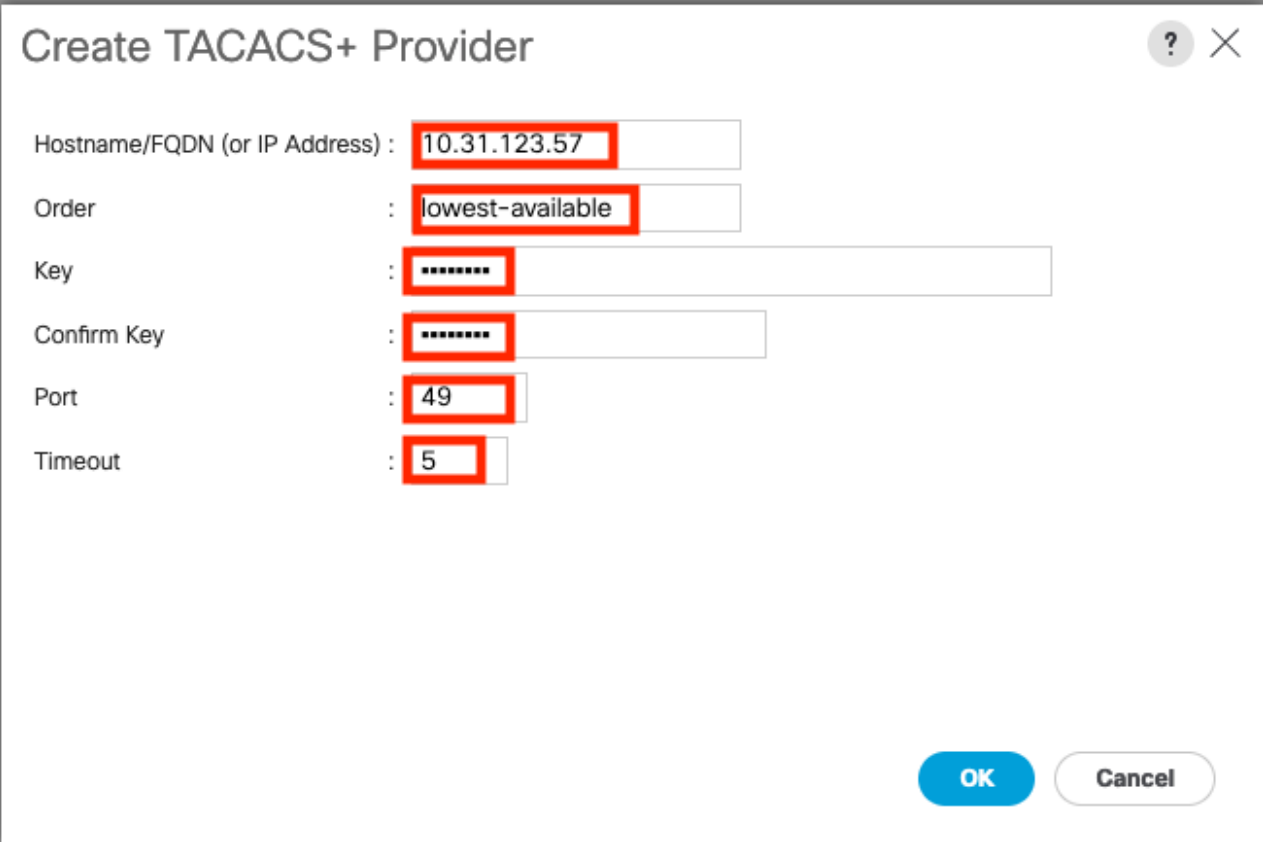
Stap 5. Voer inCreate TACACS+ Providerde wizard de juiste informatie in.

- Typ in het veld Hostname het IP-adres of de hostnaam van TACACS+ Server.
- In het veld Bestelling, de volgorde waarin Cisco UCS deze provider gebruikt om gebruikers te verifiëren.

Voer een geheel getal in tussen 1 en 16 of voer laagst beschikbare of 0 (nul) in als u wilt dat

Cisco UCS de volgende beschikbare volgorde toewijst op basis van de andere providers die in deze Cisco UCS-instantie zijn gedefinieerd.

- In het veld Sleutel staat de SSL-coderingssleutel voor de database.
- In het veld Sleutel bevestigen wordt de SSL-coderingssleutel herhaald voor bevestigingsdoeleinden.
- In het veld Port, De poort waardoor Cisco UCS communiceren met de TACACS+ database (Port 49 standaard poort).
- In het veld Time-out: De tijdsduur in seconden die het systeem besteedt aan het zoeken naar contact met de TACACS+-database voordat de time-out optreedt.



Create TACACS+ Provider

Hostname/FQDN (or IP Address) : 10.31.123.57

Order : lowest-available

Key : *****

Confirm Key : *****

Port : 49

Timeout : 5

OK Cancel

Stap 6. Selecteer OK.



Opmerking: Als u een hostnaam gebruikt in plaats van een IP-adres, moet u een DNS-server configureren in Cisco UCS Manager.

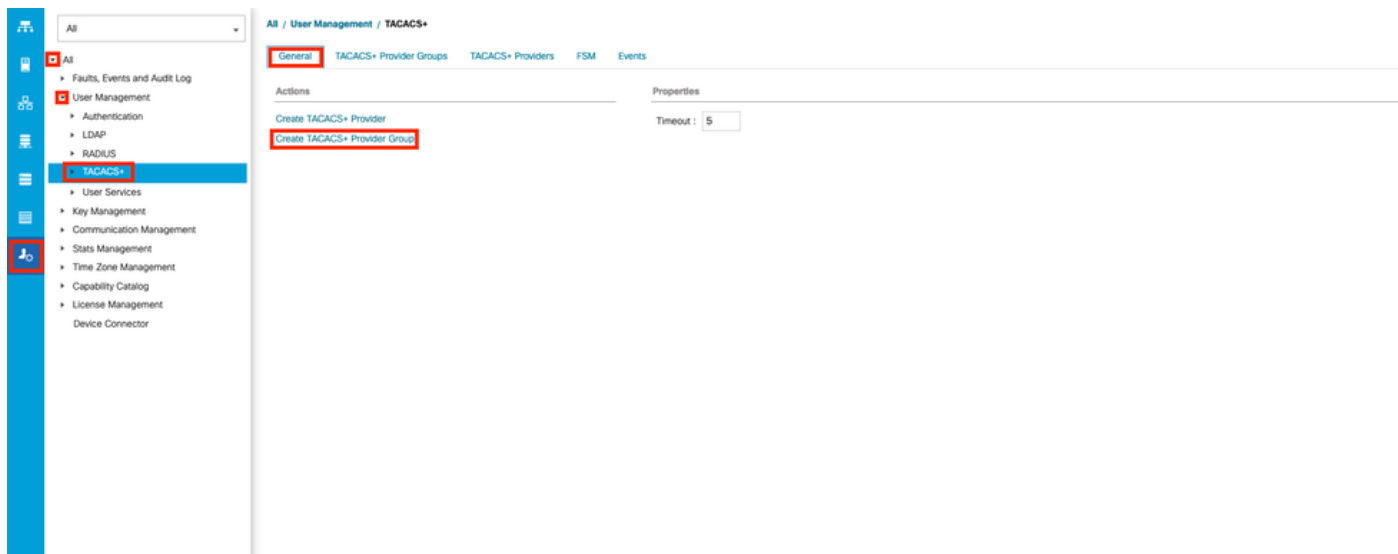
Een TACACS+-providergroep maken

Stap 1. Selecteer in **Navigation** het deelvenster het **Admin** tabblad.

Stap 2. Op **Admin** de tab, breid **All > User Management > TACACS+** uit.

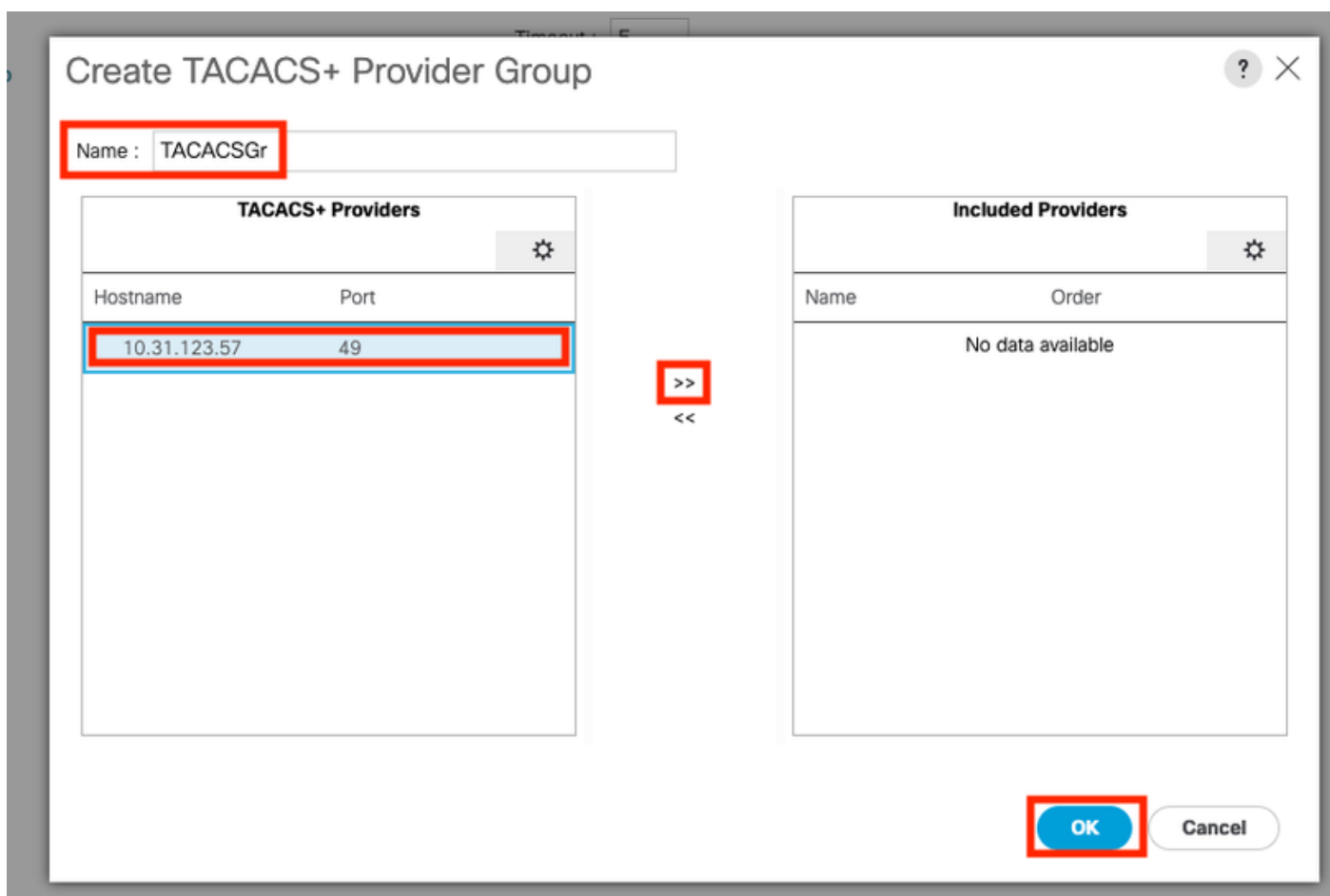
Stap 3. Selecteer in **work** het deelvenster het **General** tabblad.

Stap 4. In **Actions** het gebied **Create TACACS+ Provider** selecteert u **Groep**.



Stap 5. Voer in het dialoogvenster TACACS+-providergroep maken de gevraagde informatie in.

- Voer in het veld **Naam** een unieke naam voor de groep in.
- In de tabel **TACACS+ Providers** kiest u de providers die u wilt opnemen in de groep.
- Selecteer de knop **>>** om de providers toe te voegen aan de tabel **Inclusieve providers**.



Stap 6. Selecteer OK.

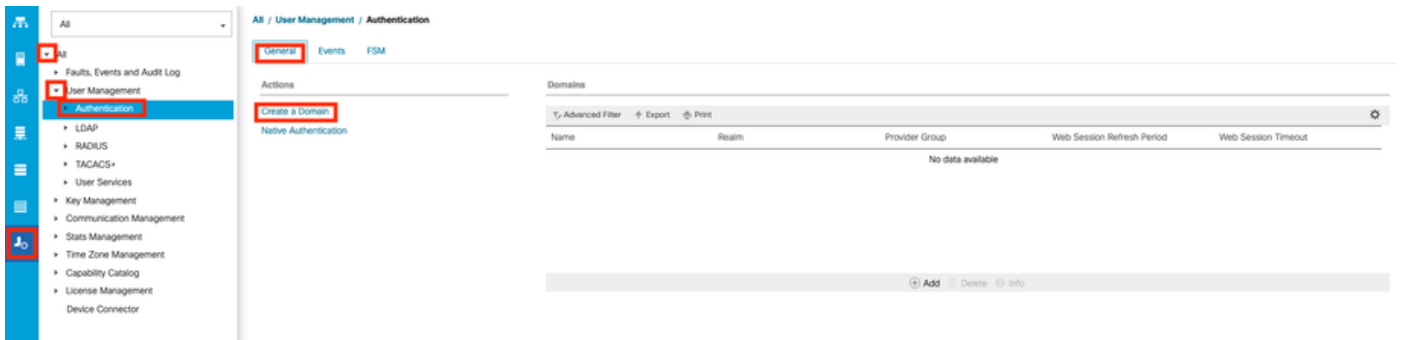
Een verificatiedomein maken

Stap 1. Selecteer in het **Navigation** deelvenster het **Admin** tabblad.

Stap 2. Vouw op het **Admin** tabblad uit **All > User Management > Authentication**

Stap 3. Selecteer in **work** het deelvenster het **General** tabblad.

Stap 4. In **Actions** het gebied selecteert u **Create a Domain**.



Stap 5. Voer in het dialoogvenster Domein maken de gevraagde informatie in.

- Voer in het veld **Naam** een unieke naam voor het domein in.
- In het **Realm**, selecteer de **Tacacs** optie.
- Selecteer in de vervolgkeuzelijst **Provider Group** de eerder gemaakte **TACACS+** providergroep en selecteer **OK**

The screenshot shows a 'Create a Domain' dialog box. It contains the following fields and options:

- Name**: A text input field containing 'TACACS'.
- Web Session Refresh Period (sec)**: A text input field containing '600'.
- Web Session Timeout (sec)**: A text input field containing '7200'.
- Realm**: A radio button group with three options: 'Local', 'Radius', and 'Tacacs'. The 'Tacacs' option is selected.
- Provider Group**: A dropdown menu showing 'TACACSGr'.
- Two Factor Authentication**: An unchecked checkbox.

At the bottom right, there are two buttons: 'OK' and 'Cancel'. The 'OK' button is highlighted with a red box.

Problemen oplossen

Gemeenschappelijke TACACS+-kwesties inzake UCSM

- Verkeerde sleutel of ongeldige tekens.
- Onjuiste poort.
- Geen communicatie met onze provider vanwege een firewall of proxy-regel.
- FSM is niet 100%.

Verifieer de UCSM TACACS+ configuratie:

U moet ervoor zorgen dat de UCSM de configuratie heeft geïmplementeerd en de status van de Finite State Machine (FSM) wordt weergegeven als 100% voltooid.

Controleer de configuratie vanaf de opdrachtregel van de UCSM

<#root>

UCS-A#

scope security

UCS-A /security #

scope tacacs

UCS-A /security/tacacs #

show configuration

```
UCS-AS-MXC-P25-02-A# scope security
UCS-AS-MXC-P25-02-A /security # scope tacacs
UCS-AS-MXC-P25-02-A /security/tacacs # show configuration
scope tacacs
  enter auth-server-group TACACSGr
    enter server-ref 10.31.123.57
      set order 1
    exit
  exit
enter server 10.31.123.57
  set order 1
  set port 49
  set timeout 5
!   set key
  exit
  set timeout 5
exit
```

<#root>

UCS-A /security/tacacs #

show fsm status

```
[UCS-AS-MXC-P25-02-A /security/tacacs # show fsm status
```

```
    FSM 1:
```

```
        Status: Nop
```

```
        Previous Status: Update Ep Success
```

```
        Timestamp: 2023-06-24T20:54:05.021
```

```
        Try: 0
```

```
        Progress (%): 100
```

```
        Current Task:
```

Controleer de Tacacs-configuratie vanuit het NXOS:

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

show tacacs-server

UCS-A(nx-os)#

show tacacs-server groups

```

[UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server
timeout value:5
deadtime value:0
source interface:any available
Global Test Username:test
Global Test Password:*****
total number of servers:1

following TACACS+ servers are configured:
  10.31.123.57:
    available on port:49
    TACACS+ shared secret:*****
    timeout:5
[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
  group tacacs:
    server 10.31.123.57 on port 49
    deadtime is 0
    vrf is management
  group TACACSGr:
    server 10.31.123.57 on port 49
    deadtime is 0
    vrf is management

```

Om de verificatie van NX-OS te testen, gebruikt u test aaade opdracht (alleen beschikbaar vanaf NXOS).

De configuratie van onze server valideren:

```
<#root>
```

```
UCS-A(nx-os)#
```

```
test aaa server tacacs+
```

```
<TACACS+-server-IP-address or FQDN> <username> <password>
```

```

UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/lgpl-2.1.txt.
UCS-AS-MXC-P25-02-A(nx-os)# test aaa server tacacs+ 10.31.123.57 operator Cisc0123

```

UCSM-beoordeling

Verificatie van bereikbaarheid

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

ping

<TACACS+-server-IP-address or FQDN>

```

UCS-AS-MXC-P25-02-A# connect local-mgmt
pCisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-AS-MXC-P25-02-A(local-mgmt)# ping 10.31.123.57
PING 10.31.123.57 (10.31.123.57) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.57: icmp_seq=1 ttl=64 time=0.347 ms
64 bytes from 10.31.123.57: icmp_seq=2 ttl=64 time=0.309 ms

```

Havenverificatie

<#root>

UCS-A#

connect local-mgmt

UCS-A(local-mgmt)#

telnet

<TACACS+-server-IP-address or FQDN> <Port>

```
UCS-AS-MXC-P25-02-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

UCS-AS-MXC-P25-02-A(local-mgmt)# telnet 10.31.123.57 49
Trying 10.31.123.57...
Connected to 10.31.123.57.
Escape character is '^['.
```

De meest effectieve methode om fouten te zien is om het NXOS-debug in te schakelen, met deze uitvoer kunt u de groepen, de verbinding en de foutmelding zien die miscommunicatie veroorzaakt.

- Open een SSH-sessie naar UCSM en log in met elke geprivilegieerde gebruiker met beheerdersrechten (bij voorkeur een lokale gebruiker), wijzig de NX-OS CLI-context en start de terminalmonitor.

<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

terminal monitor

- Schakel foutopsporingsvlaggen in en controleer de SSH-sessieuitvoer naar het logbestand.

<#root>

UCS-A(nx-os)#

debug aaa all

```
UCS-A(nx-os)#
```

```
debug aaa aaa-request
```

```
UCS-A(nx-os)#
```

```
debug tacacs+ aaa-request
```

```
UCS-A(nx-os)#
```

```
debug tacacs+ aaa-request-lowlevel
```

```
UCS-A(nx-os)#
```

```
debug tacacs+ all
```

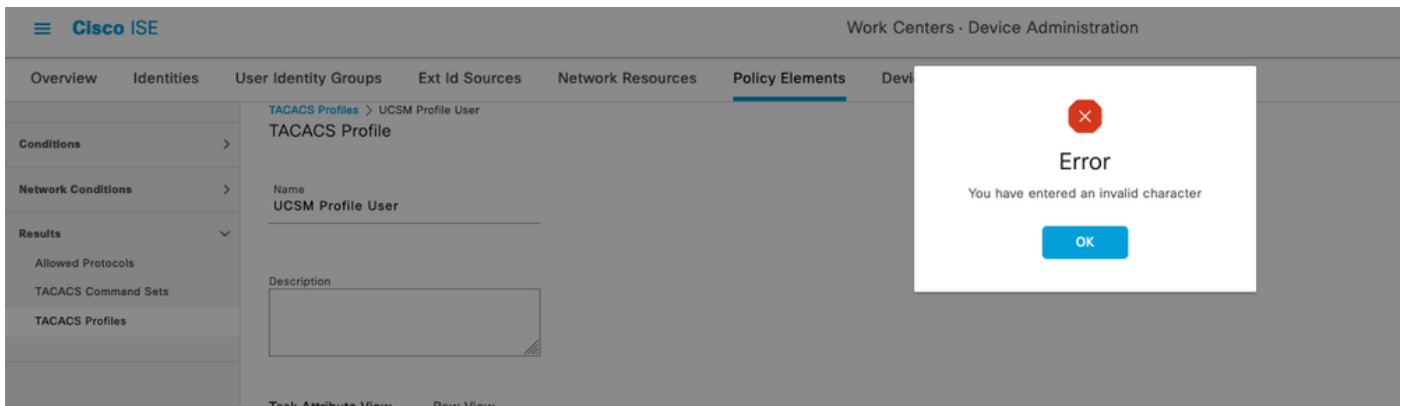
```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-A(nx-os)# terminal monitor
UCS-AS-MXC-P25-02-A(nx-os)# debug tacacs+ all
2023 Jun 26 04:42:22.104286 tacacs: event_loop(): calling process_rd_fd_set
2023 Jun 26 04:42:22.104311 tacacs: process_rd_fd_set: calling callback for fd 6
2023 Jun 26 04:42:22.104341 tacacs: fsrv didnt consume 182 opcode
2023 Jun 26 04:42:22.104994 tacacs: mts_message_handler: sdwrap_process_msg
2023 Jun 26 04:42:22.105011 tacacs: process_rd_fd_set: callback returned for fd 6
UCS-AS-MXC-P25-02-A(nx-os)# debug aaa all
```

- Open nu een nieuwe GUI- of CLI-sessie en probeer in te loggen als externe gebruiker (TACACS+).
- Zodra u een foutmelding voor het inloggen hebt ontvangen, schakelt u de foutopsporingen uit die de sessie sluiten of met deze opdracht.

```
UCS-A(nx-os)# undebug all
```

Gemeenschappelijke TACAC-kwesties inzake ISE

- Binnen ISE wordt dit gedrag weergegeven wanneer u probeert het tacacs-profiel te configureren in de attributen die nodig zijn voor UCSM om de bijbehorende rollen voor admin of een andere rol toe te wijzen, selecteert u op de knop Opslaan en dit gedrag wordt weergegeven:



Deze fout is te wijten aan de volgende bug

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917>, zorg ervoor dat u hebt waar dit defect is aangepakt.

ISE-beoordeling

Stap 1. Controleer of de TACACS+-service actief is. Dit kan worden ingecheckt:

- GUI: Controleer of de node wordt vermeld bij de service DEVICE ADMIN in Beheer > Systeem > Implementatie.
- CLI: Voer de opdracht `show ports` uit | neem 49 op om te bevestigen dat er verbindingen in de TCP-poort zijn die behoren tot TACACS+

```
<#root>
```

```
ise32/admin#
```

```
show ports | include 49
```

```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

Stap 2. Bevestig of er livelogs zijn met betrekking tot TACACS+-verificatiepogingen: dit kan worden gecontroleerd in het menu Bewerkingen > TACACS > Live-logs,

Afhankelijk van de reden van de storing kunt u uw configuratie aanpassen of de oorzaak van de storing aanpakken.

Operations - TACACS

Live Logs

Export To

Refresh Never Show Latest 20 records Within Last 3 hours

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device	Network Device	Device Type	Location	Device P...	Failure Reason	Remote Address
			Identity		Authentication Policy	Authorization Policy	Ise Node	Network Device N	Network Device	Device Type	Location	Device Port	Failure Reason	Remote Address
Jun 25, 2023 12:30:16.8...			INVALID	Authentic...	Default >> Default		ise32	USCM	10.31.123.8	Device TypeRAI...	LocationRAI Loc...		22056 Subject not found in the ap...	10.99.183.4
Jun 25, 2023 12:20:38.7...				Authentic...			ise32		10.31.123.9				13017 Received TACACS+ packet f...	
Jun 25, 2023 12:20:02.2...				Authentic...			ise32		10.31.123.9				13017 Received TACACS+ packet f...	

Stap 3. Als u geen livelog ziet, gaat u verder met het vastleggen van pakketten en navigeert u naar het menu **Bewerkingen > Problemen oplossen > Diagnostische hulpprogramma's > Algemene hulpprogramma's > TCP-dump**, selecteer bij toevoegen

Operations - Troubleshoot

Diagnostic Tools Download Logs Debug Wizard

TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

Rows/Page 0 0 0 Total Rows

Add Edit Trash Start Stop Download

Host Name	Network Interface	Filter	File Name	Repository	File S...	Number of ...	Time Limit	Promiscuous M...	Status
No data found.									

Selecteer de node Policy Service van waaruit de UCSM de verificatie verzendt en ga vervolgens in filters door met het invoeren van ip-host X.X.X.X die overeenkomt met het IP-adres van de UCSM van waaruit de verificatie wordt verzonden, noem de opname en scroll naar beneden om op te slaan, voer de vastlegging uit en log in vanaf de UCSM.

Cisco ISE

Operations - Troubleshoot

Evaluation Mode 89 Days

Diagnostic Tools

Download Logs

Debug Wizard

General Tools

TCP Dump

Session Trace Tests

TrustSec Tools

TCP Dump > New

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name*
ise32

Network Interface*
GigabitEthernet 0 [Up, Running]

Filter
ip host 10.31.123.7

E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name
taccap

Repository

File Size
10 Mb

Limit to
1 File(s)

Time Limit
5 Minute(s)

☐ Promiscuous Mode

Cancel Save Save and Run

Stap 4. Schakel de component runtime-AAA in voor foutopsporing binnen de PSN van waaruit de verificatie wordt uitgevoerd in Operations > Troubleshoot > Debug Wizard > Debug log configuratie, selecteer PSN node, selecteer vervolgens volgende in bewerken knop.

Cisco ISE

Operations - Troubleshoot

Diagnostic Tools

Download Logs

Debug Wizard

Debug Profile Configuration

Debug Log Configuration

Node List

Edit Reset to Default

Node Name	Replication Role
ise32	STANDALONE

Zoek naar de component runtime-AAA en verander het niveau om te debuggen om vervolgens het probleem opnieuw te reproduceren en ga verder met het analyseren van de logs.

Diagnostic Tools

Download Logs

Debug Wizard

Debug Profile Configuration

Debug Log Configuration

Node List > ise32.example.com

Debug Level Configuration

 Edit  Reset to Default

Component Name	Log Level	Description	Log file Name
runtime-AAA	×		
☐ runtime-AAA	DEBUG	AAA runtime messages (prrt)	prrt-server.log



Opmerking: Raadpleeg voor meer informatie de video in het YouTube-kanaal van Cisco Hoe u debugs inschakelt op ISE 3.x-versies

<https://www.youtube.com/watch?v=E3USz8B76c8>.

Gerelateerde informatie

[Beheerdershandleiding Cisco UCS Manager](#)

[Cisco UCS CIMC Configuratiegids TACACS+](#)

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.