TACACS+ verificatie op CIMC met ISE-server configureren

Inhoud

Inleiding

Dit document beschrijft de configuratie van Terminal Access Control System Plus (TACACS+)-verificatie op Cisco Integrated Management Controller (CIMC).

TACACS+ wordt gewoonlijk gebruikt om netwerkapparaten met een centrale server te authentiseren. Sinds release versie 4.1(3b) ondersteunt Cisco IMC TACACS+-verificatie. De ondersteuning van TACACS+ op CIMC verlicht de inspanning om meerdere gebruikersrekeningen te beheren die toegang tot het apparaat hebben. Deze optie is van hulp om de geloofsbrieven van de gebruiker periodiek te veranderen en gebruikersrekeningen ver te beheren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Integrated Management Controller (CIMC)
- Terminaltoegangscontrollerkaart voor toegangscontrolesysteem Plus (TACACS+)

Gebruikte componenten

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

- UCS C220-M4S SWITCH
- CIMC-versie: 4.1(3b)

- Cisco Identity Services Engine (ISE) versie 3.0.0.458

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Configuratie van TACACS+ serverzijde voor associatie met prioriteit

Het voorkeursniveau van de gebruiker wordt berekend op basis van de waarde **cisco-av-**paar die voor die gebruiker is ingesteld. Er moet een **cisco-av-paar** worden gemaakt op de TACACS+ server voor gebruikers die geen standaard TACACS+ eigenschappen kunnen gebruiken. De drie synbelastingen zoals hieronder wordt weergegeven, worden ondersteund voor de eigenschap **cisco-av**.

Voor **admin** privilege:

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

Voor **gebruikersrechten**:

```
cisco-av-pair=shell:roles="user"
```

Voor **alleen-lezen** privilege:

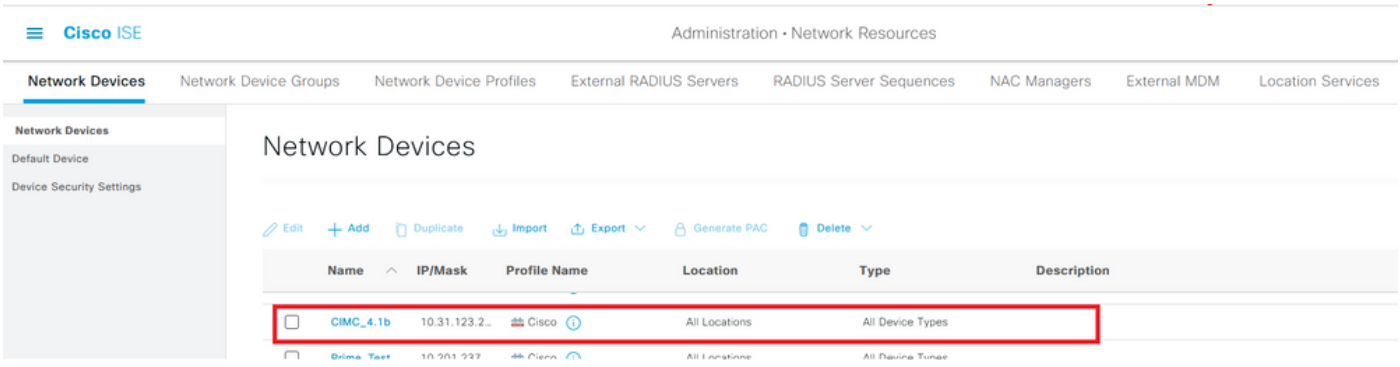
```
cisco-av-pair=shell:roles="read-only"
```

Om andere apparaten te ondersteunen, als andere rollen moeten worden toegevoegd dan kunnen ze met een komma als scheidingsteken worden toegevoegd. UCSM ondersteunt bijvoorbeeld **AAA**, zodat **shell:rollen="admin,aaa"** kan worden geconfigureerd en CIMC accepteert dit formaat.

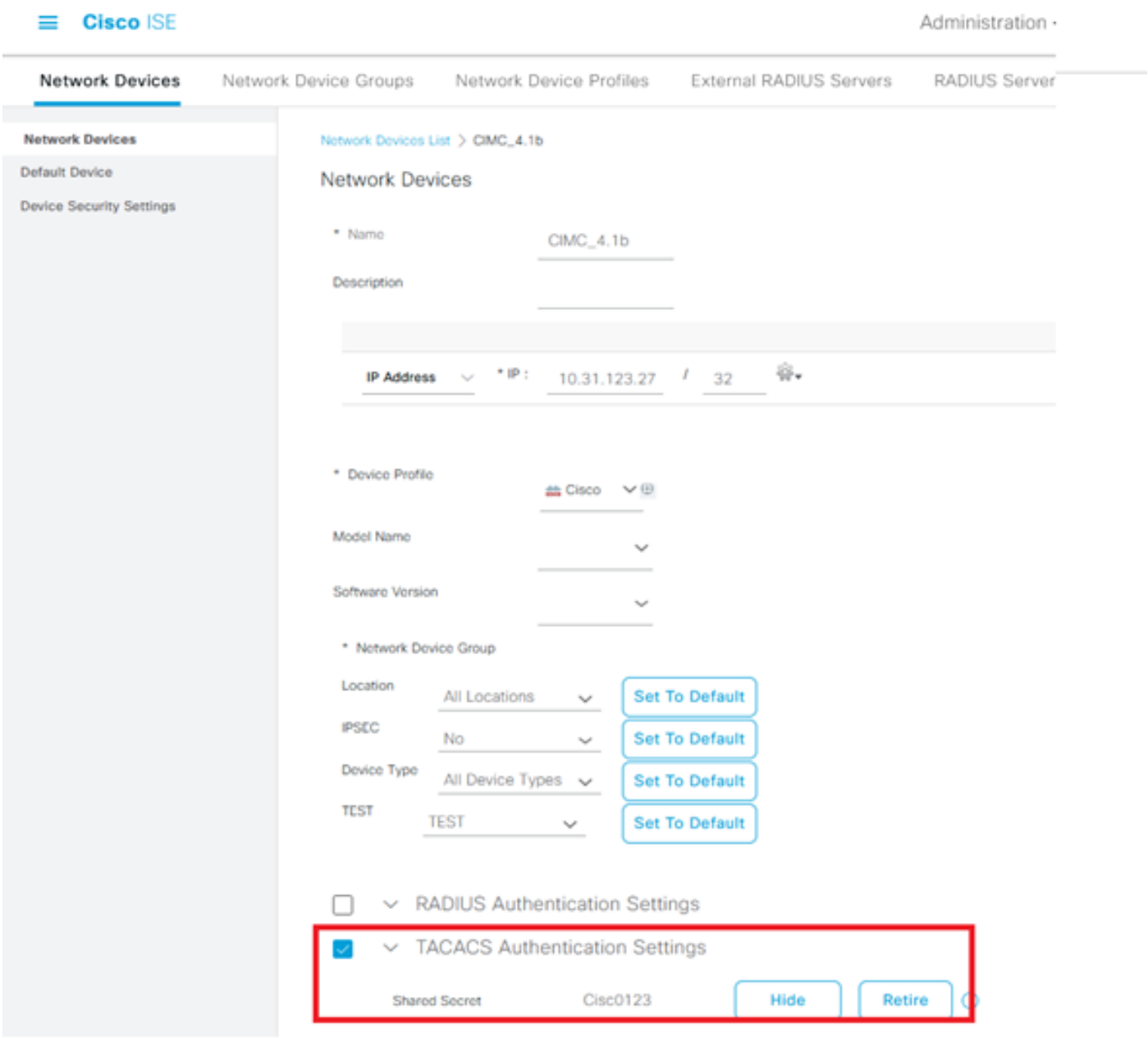
> **Opmerking:** Als **cisco-av-paar** niet op de TACACS+ server is ingesteld, heeft een gebruiker met die server een **alleen-lezen** privilege.

ISE-configuratievereisten

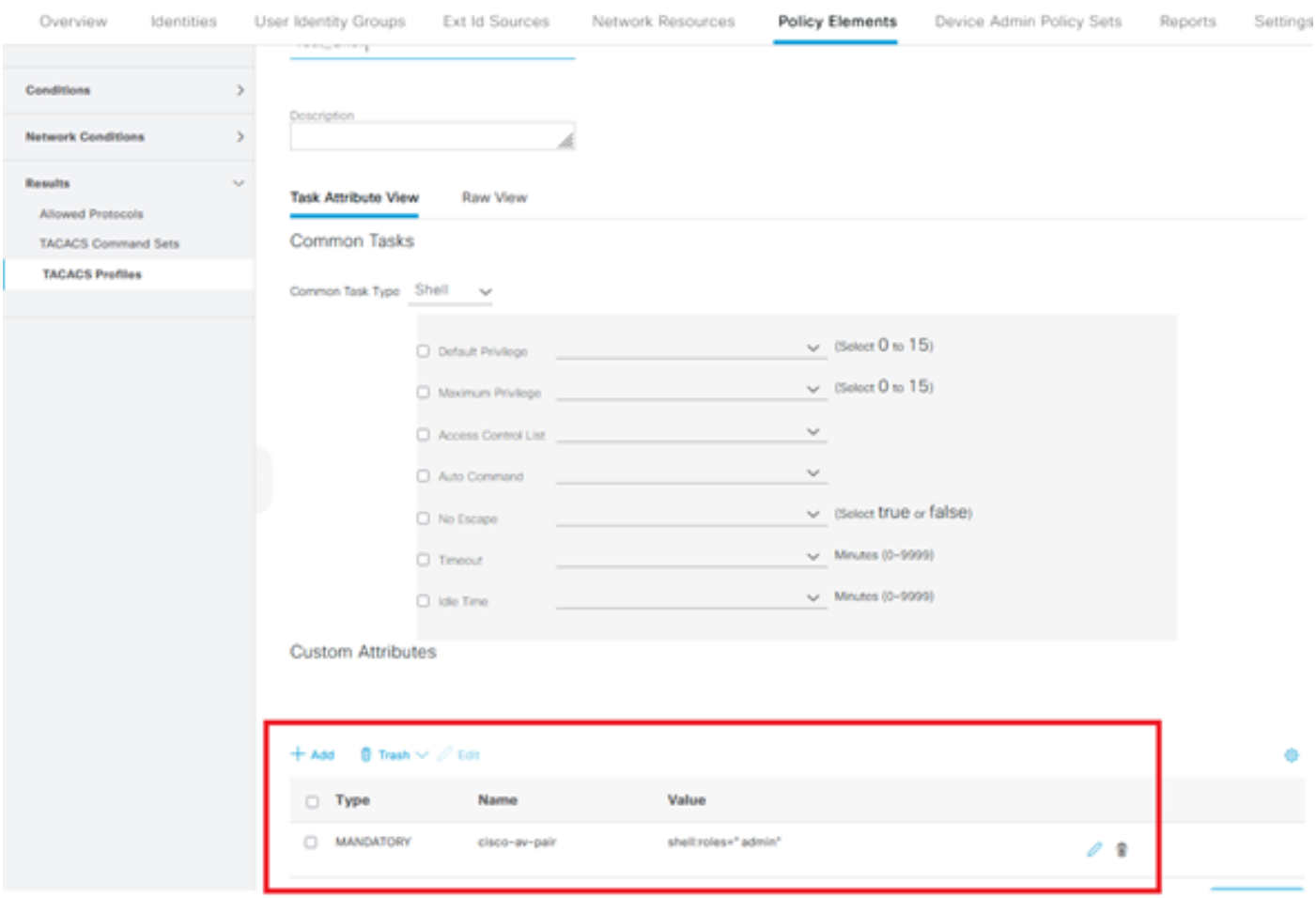
Het beheer IP van de server moet zijn toegestaan op het ISE-netwerkapparaat.



Gedeeld geheime wachtwoord dat op CIMC moet worden ingevoerd.



Shell Profile met **cisco-av-paar**, met admin-rechten.

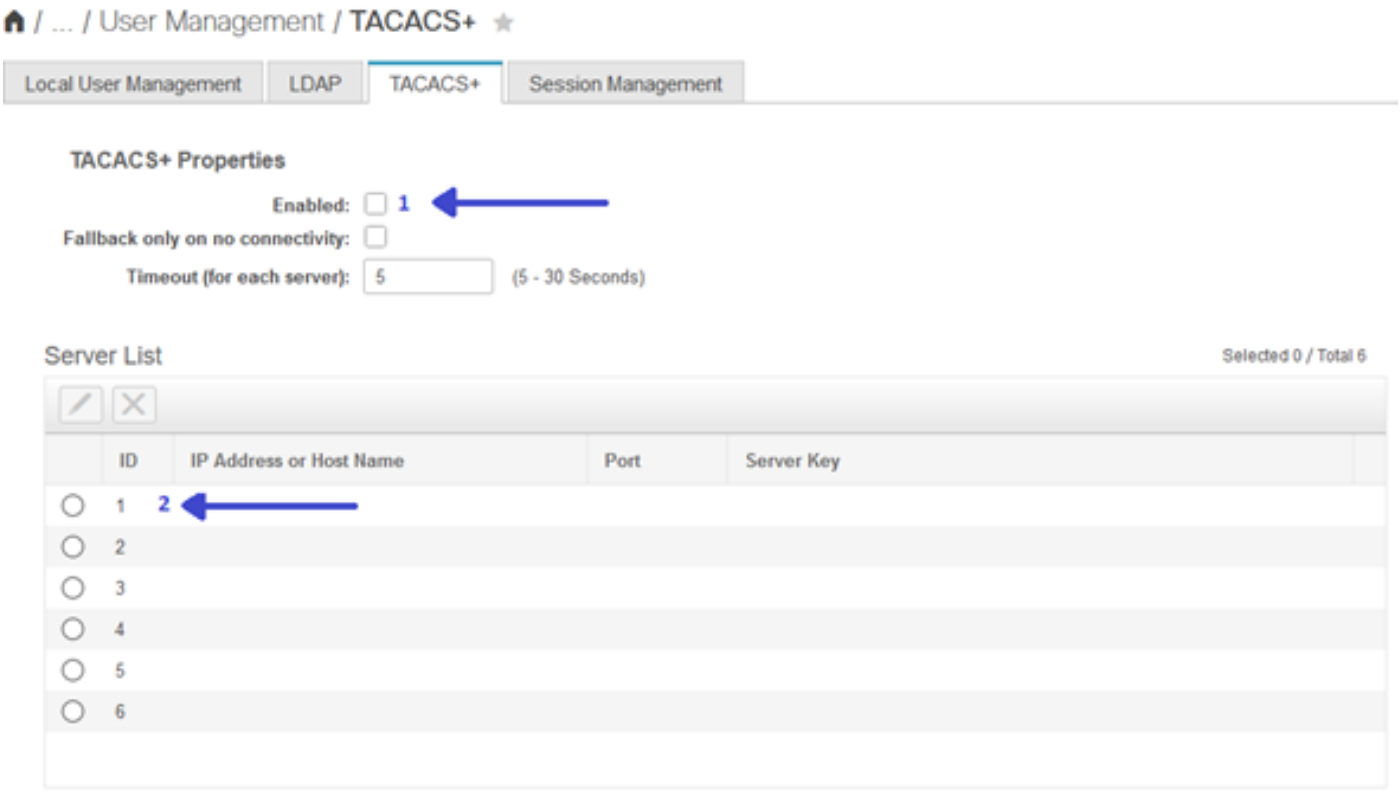


TACACS+ configuratie op CIMC

Stap 1. Navigeer naar **Admin > Gebruikersbeheer > TACACS+**

Stap 2. Selecteer het selectieteken om **TACACS+** in te schakelen

Stap 3. Een nieuwe server kan bij een van de 6 rijen in de tabel worden toegevoegd. Klik op de rij of selecteer de rij en klik op de knop **bewerken** boven in de tabel, zoals in deze afbeelding weergegeven.

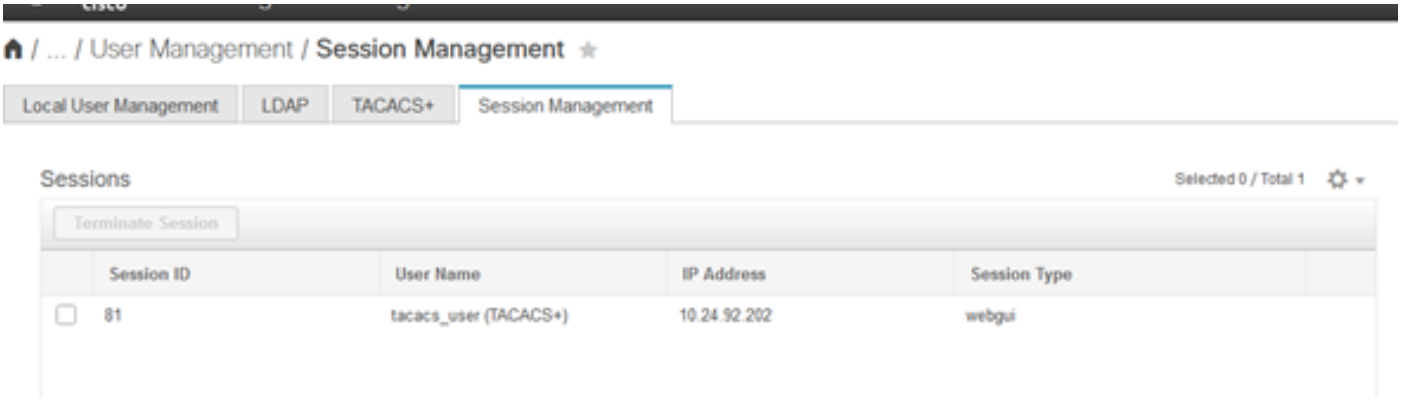


Opmerking: In het geval dat een gebruiker TACACS+ back op geen aansluitingsoptie heeft ingeschakeld, dwingt CIMC af dat de eerste authenticatie-voorrang altijd moet worden ingesteld op TACACS+ anders zou de back-upconfiguratie irrelevant kunnen worden.

Stap 4. Vul het IP-adres of de hostnaam, poort en Server-toets/gedeeld geheim in en **bewaar** de configuratie.

Cisco IMC ondersteunt maximaal zes TACACS+ externe servers. Zodra een gebruiker is geauthentiseerd, wordt de gebruikersnaam toegevoegd met (TACACS+).

Dit wordt ook weergegeven in het sessiebeheer



Verifiëren

- Er kunnen maximaal 6 TACACS+ servers worden ingesteld op de CIMC.
- De geheime sleutel die bij de server hoort kan maximaal 64 tekens lang zijn.
- De timeout kan worden ingesteld tussen 5 en 30 seconden (die evalueert tot maximaal 180 seconden om in lijn te zijn met LDAP).
- Als een TACACS+ server de servicenaam moet gebruiken om het **cisco-av-paar** te maken, moeten de gebruikers **Log in** als de servicenaam gebruiken.
- Geen ondersteuning voor roodbaars om de configuraties te wijzigen.

Controleer configuratie via CLI in CIMC

- Controleer of TACACS+ is ingeschakeld.

```
C220-WZP22460WCD# scope tacacs+
C220-WZP22460WCD /tacacs+ # show detail
TACACS+ Settings:
Enabled: yes
Fallback only on no connectivity: no
Timeout(for each server): 5
```

- Controleer de configuratiegegevens per server.

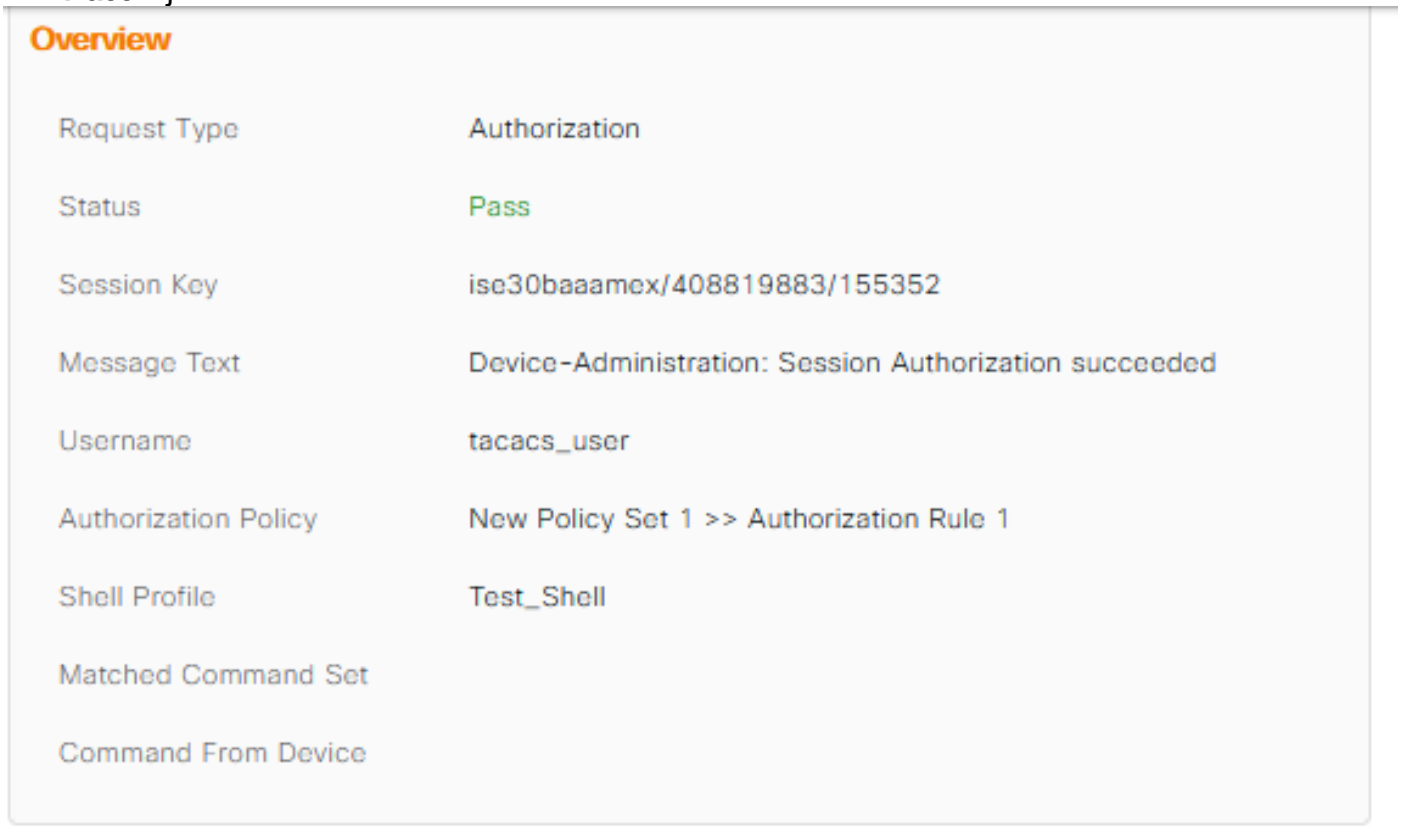
```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: ******
Server Port: 49
```

Problemen oplossen

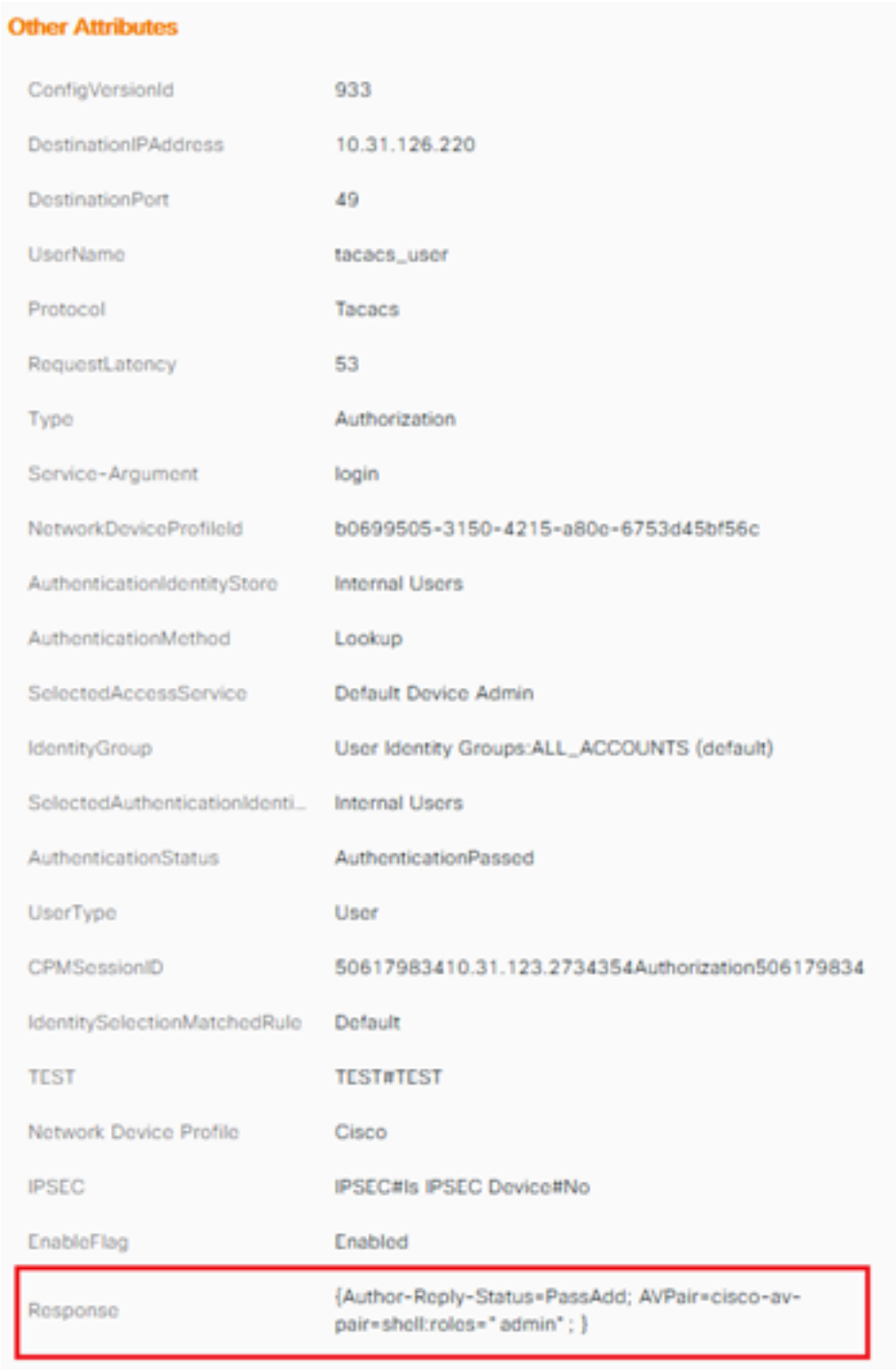
- Zorg ervoor dat IP TACACS+ server bereikbaar is vanuit CIMC en dat de poort correct is geconfigureerd.
- Zorg ervoor dat het **cisco-av-paar** correct is ingesteld op de TACACS+ server.
- Controleer of de TACACS+ server bereikbaar is (IP en poort).
- Zorg ervoor dat de geheime sleutel of de referenties overeenkomen met die welke op de TACACS+ server zijn ingesteld.
- Als u kunt inloggen met TACACS+ maar alleen lees-**only** permissies hebt, controleer of cisco-av-paar de correcte syntaxis op de TACACS+ server heeft.

ISE-probleemoplossing

- Controleer de Tacacs Live-logbestanden voor een van de authenticatiepogingen. Status moet **Pass** zijn.



- Controleer of de respons de juiste eigenschap **cisco-av-paar** heeft ingesteld.



Other Attributes

ConfigVersionId	933
DestinationIPAddress	10.31.126.220
DestinationPort	49
UserName	tacacs_user
Protocol	Tacacs
RequestLatency	53
Type	Authorization
Service-Argument	login
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
IdentityGroup	User Identity Groups:ALL_ACCOUNTS (default)
SelectedAuthenticationIdenti...	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	50617983410.31.123.2734354Authorization506179834
IdentitySelectionMatchedRule	Default
TEST	TEST#TEST
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=cisco-av-pair=shell:roles=" admin" ; }

Gerelateerde informatie

- TACACS+ verificatie van Cisco UCS-C
- Technische ondersteuning en documentatie – Cisco Systems
- ISE 2.0 configureren: IOS TACACS+ verificatie en commando-autorisatie op basis van AD-groepslidmaatschap