UCSM-verificatie configureren met RADIUS (FreeRADIUS)

Inhoud

Inleiding

Dit document beschrijft het configureren van UCSM-verificatie met behulp van RADIUS.

Voorwaarden

Vereisten

- FreeRADIUS is operationeel.
- UCS Manager, Fabric Interconnects en FreeRADIUS-server communiceren met elkaar.

Het doelpubliek is UCS-beheerders met een basiskennis van UCS-functies.

Cisco raadt u aan bekend te zijn met deze onderwerpen:

- Linux-versie van configuratiebestand
- UCS Manager
- FreeRADIUS
- Ubuntu of een andere Linux-versie

Gebruikte componenten

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

- UCS Manager (UCS M) 4.3(3a) of hoger.
- Fabric Interconnect 6464
- Ubuntu 22.04.4 LTS
- FreeRADIUS versie 3.0.26

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

FreeRADIUS-configuratie voor UCSM-verificatie

Voor deze stappen is basistoegangsrecht nodig voor de freeRADIUS-server.

Stap 1. Configureer het UCSM-domein als een client.

Navigeer naar het bestand clients.conf in de map /etc/freeradius/3.0 en bewerk het bestand met een teksteditor van uw voorkeur. Dit voorbeeld 'vim' editor is gebruikt en client 'UCS-POD' is gemaakt.

<#root>

```
root@ubuntu:/etc/freeradius/3.0#

vim clients.conf
*Inside clients.conf file*

client UCS-POD {
ipaddr = 10.0.0.100/29
secret = PODsecret
}
```

Het veld iPad kan alleen de IP van de primaire fabric interconnect bevatten. In dit voorbeeld werd IP 10.0.0.100/29 IP gebruikt om de VIP + mgmt0 IP van beide FI's te omvatten.

Het geheime veld bevat het wachtwoord dat wordt gebruikt in de CSM RADIUS-configuratie (Stap 2.)

Stap 2. Configureer de lijst met gebruikers die toestemming hebben om hun gegevens te verifiëren op UCSM.

In dezelfde map - /etc/freeradius/3.0 - open het gebruikers bestand en maak een gebruiker. Bij dit voorbeeld, gebruiker 'alerosa' met wachtwoord 'wachtwoord' werd gedefinieerd om in te loggen als beheerder van het UCSM-domein.

<#root>

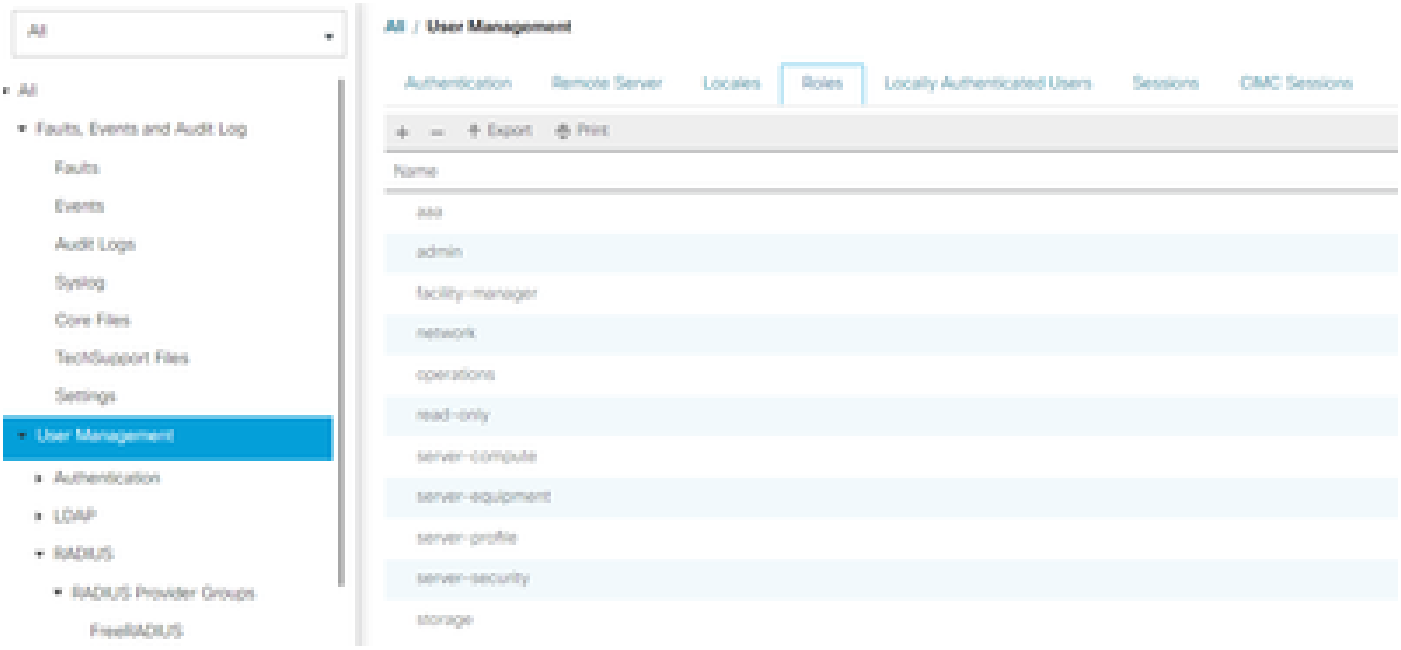
```
root@ubuntu:/etc/freeradius/3.0#

vim users
*Inside users file*
```

```
alerosa Cleartext-Password := "password"
Reply-Message := "Hello, %{User-Name}",
cisco-avpair = "shell:roles=admin"
```

Het kenmerk Cisco-paar is verplicht en moet dezelfde syntaxis volgen.

De beheerdersrol kan worden gewijzigd voor elke rol die in UCSM is geconfigureerd in Beheerder > Gebruikersbeheer > Rollen. In deze specifieke setup bestaan deze rollen



Als een gebruiker meerdere rollen moet hebben, kan er een komma worden gebruikt tussen de rollen en de syntaxis moet er ongeveer zo uitzien als cisco-avpair = "shell:rollen=aaa, facility-manager, read-only". Als een rol die niet in UCSM is gemaakt in de gebruiker wordt gedefinieerd, mislukt de verificatie in UCSM.

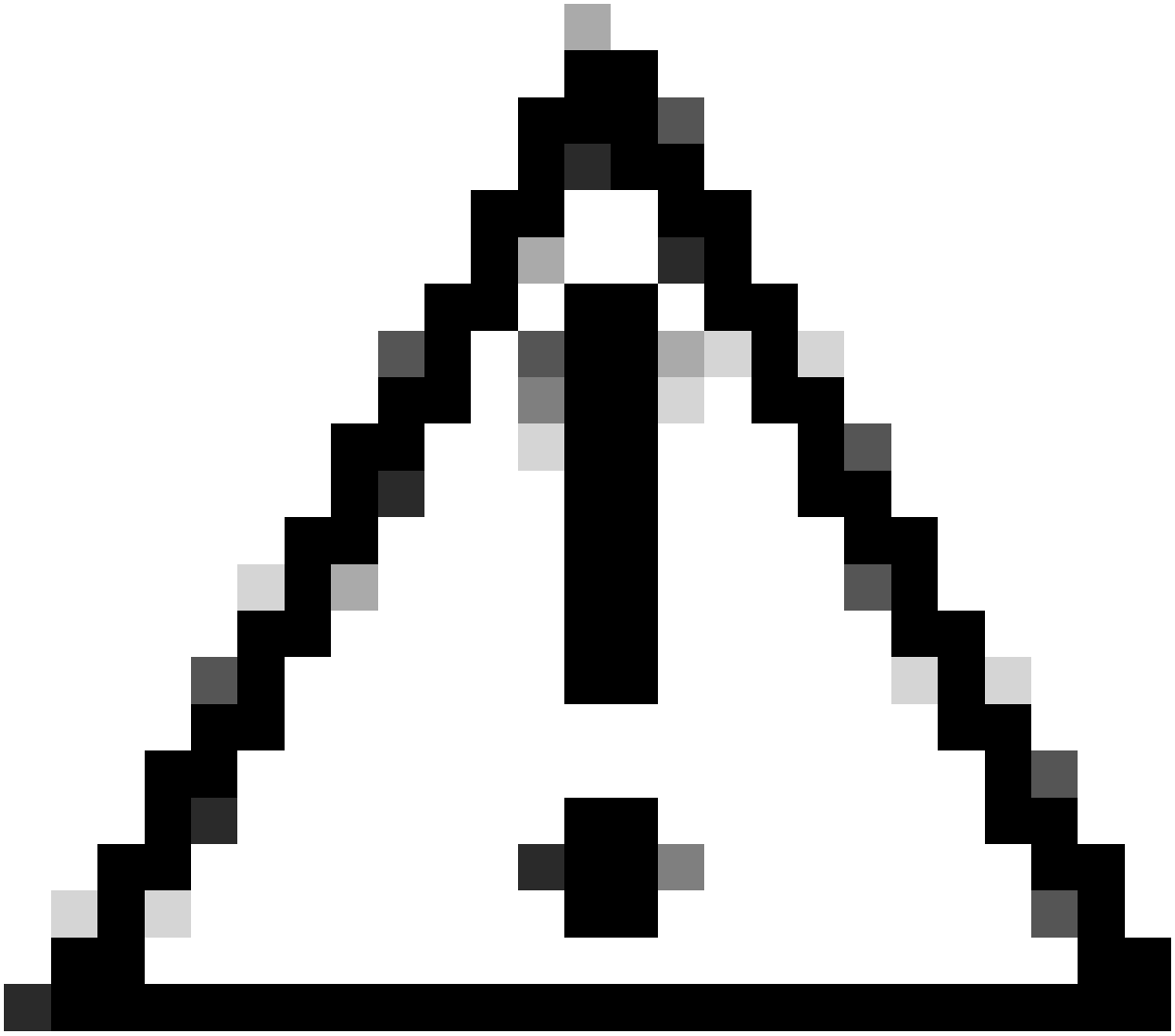
Stap 3. Schakel FreeRADIUS daemon in/uit.

Automatisch starten inschakelen voor FreeRADIUS bij opstarten van het systeem.

```
systemctl enable freeradius
```

Start de FreeRADIUS daemon:

```
systemctl restart freeradius
```



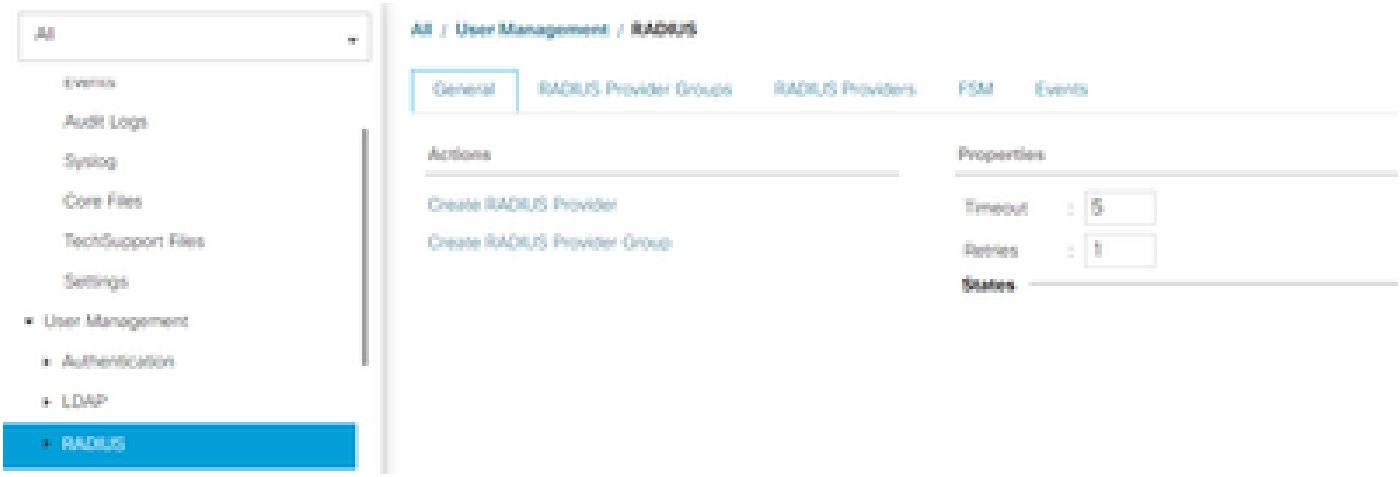
Voorzichtig: Wanneer wijzigingen worden aangebracht in de 'clients.conf' of 'gebruikers' bestanden, moet de FreeRADIUS daemon opnieuw opgestart worden, anders worden de wijzigingen niet toegepast

Configuratie UCS M-RADIUS-verificatie

De configuratie van UCS Manager volgt de instructies uit dit document - https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configura

Stap 1. Geconfigureerde standaardeigenschappen voor RADIUS-providers.

Navigeer naar Beheer > Gebruikersbeheer > RADIUS en gebruik de standaardwaarden.



Stap 2. Maak een RADIUS-provider.

Selecteer in Beheer > Gebruikersbeheer RADIUS en klik op RADIUS-provider maken.

Hostname/FQDN (of IP-adres) is het IP of FQDN van de server/virtuele machine.

Key is de sleutel/geheim gedefinieerd in de RADIUS-server in het bestand 'clients.conf' (Stap 1. van de FreeRADIUS-configuratie).

Stap 3. Maak een RADIUS-provider-groep.

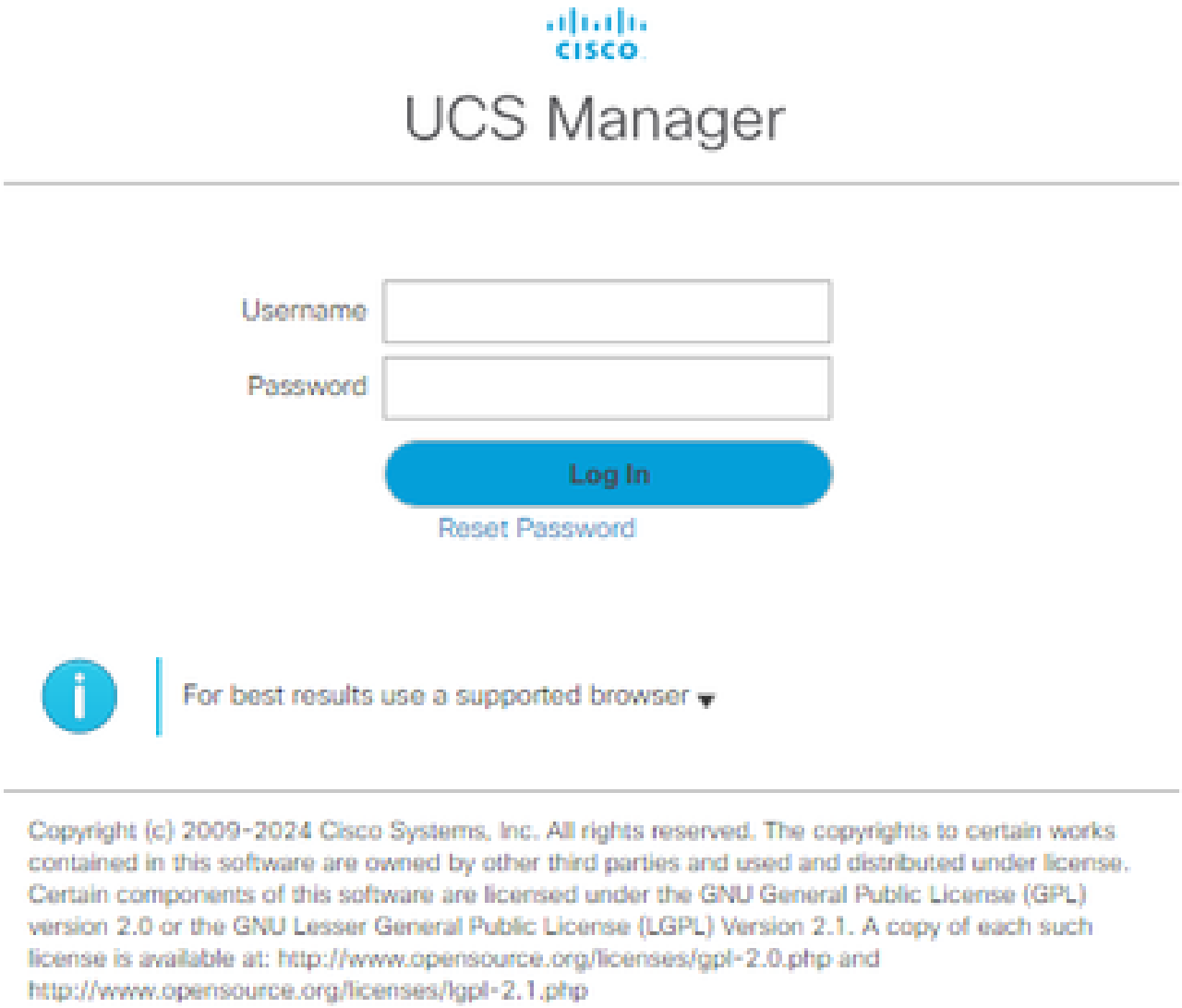
Selecteer in Beheer > Gebruikersbeheer RADIUS en klik op RADIUS-provider-groep maken.

Geef het een naam, in dit geval werd 'FreeRADIUS' gebruikt. Voeg vervolgens de RADIUS-provider die in Stap 2 is gemaakt, toe aan de lijst met meegeleveranciers.

Stap 4. Maak een nieuw verificatiedomein (optioneel).

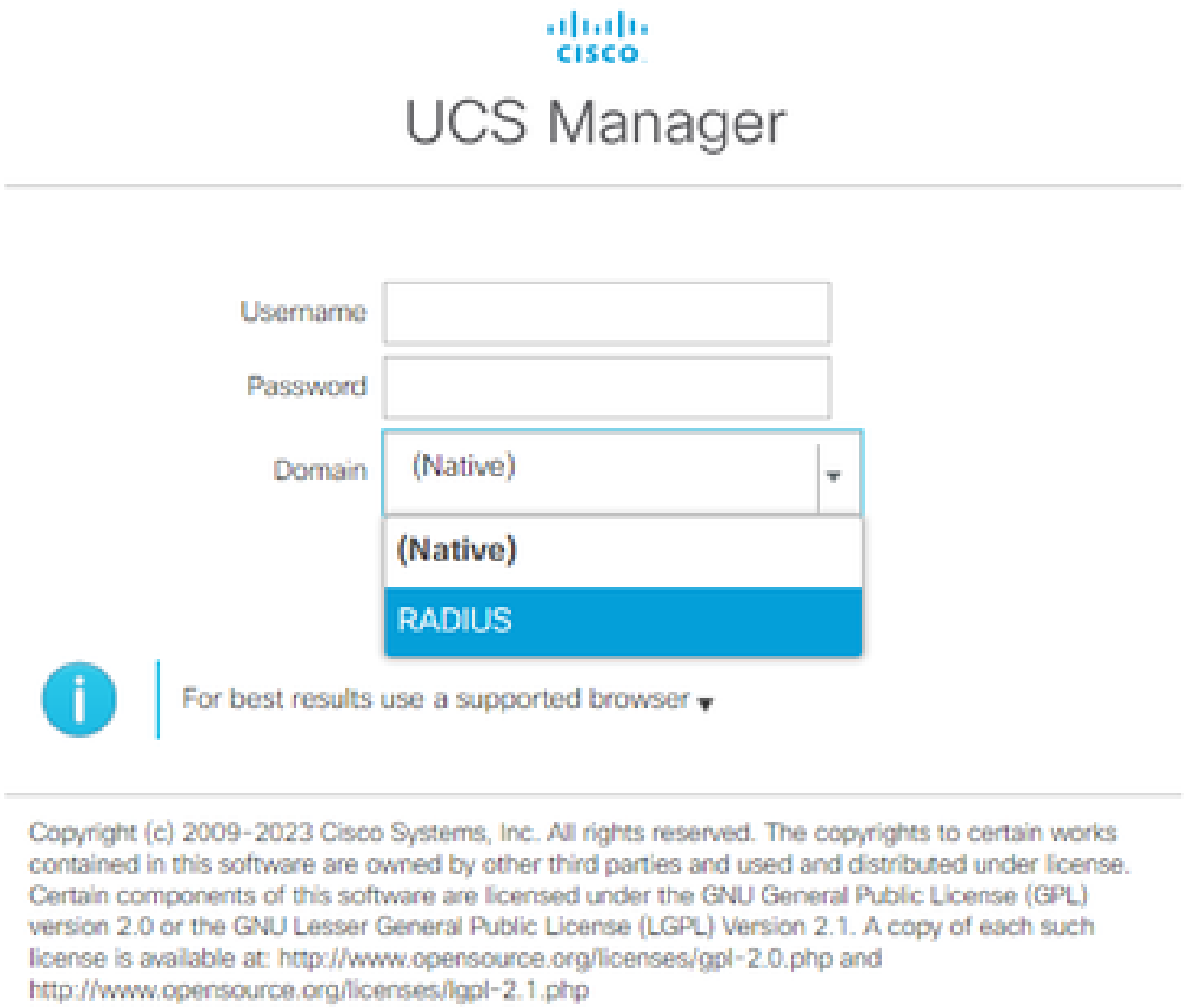
De volgende stap is niet verplicht. Het is echter uitgevoerd om een apart verificatiedomein te hebben dat verschilt van het domein dat gebruik maakt van lokale gebruikers, wat zichtbaar is in het initiële inlogscherm van UCS Manager.

Zonder een afzonderlijk verificatiedomein ziet het inlogscherm van UCS Manager er als volgt uit:



UCS Manager-inlogscherm zonder afzonderlijk verificatiedomein

Met een apart verificatiedomein voegt het inlogscherm van UCS Manager een lijst toe van de gemaakte verificatiedomeinen.



UCS Manager-inlogscherm met een afzonderlijk verificatiedomein

Dit is handig als u de RADIUS-verificatie wilt scheiden van andere verificatietypen die ook in het UCS-domein worden gebruikt.

Ga naar Beheer > Gebruikersbeheer > Verificatie > Een domein maken.

Kies de naam van het nieuwe verificatiedomein en kies de radioknop RADIUS. Selecteer in de Provider Group de Provider Group die in Stap 3. van deze sectie is gemaakt.

Verifiëren

FreeRADIUS heeft een aantal debugging- en probleemoplossingstools, zoals de tools die hieronder worden beschreven:

1. De opdracht journalctl -u freeradius geeft waardevolle informatie over de freeRADIUS daemon, zoals fouten in de configuratie en tijdstempels van fouten of initialisaties. In het onderstaande voorbeeld kunnen we zien dat het user file onjuist is gewijzigd. (mods-config/files/authorised is gebruikers file symlink):

```
Sep 14 12:18:50 ubuntu freeradius[340627]: /etc/freeradius/3.0/mods-config/files/authorize[90]: Entry d
Sep 14 12:18:50 ubuntu freeradius[340627]: Failed reading /etc/freeradius/3.0/mods-config/files/authori
```

2. De map /var/log/freeradius bevat een aantal logbestanden die een lijst bevatten van alle logbestanden die zijn vastgelegd voor de RADIUS-server. In dit voorbeeld:

```
Tue Sep 24 05:48:58 2024 : Error: Ignoring request to auth address * port 1812 bound to server default
```

3. De opdracht systemctl status freeradius geeft informatie over de FreeRADIUS-service:

```
root@ubuntu:/# systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
Loaded: loaded (/lib/systemd/system/freeradius.service; enabled; vendor preset: enabled)
Active: active (running) since Mon 2024-09-16 11:43:38 UTC; 1 week 4 days ago
Docs: man:radiusd(8)
man:radiusd.conf(5)
http://wiki.freeradius.org/
http://networkradius.com/doc/
Main PID: 357166 (freeradius)
Status: "Processing requests"
Tasks: 6 (limit: 11786)
Memory: 79.1M (limit: 2.0G)
CPU: 7.966s
CGroup: /system.slice/freeradius.service
└─357166 /usr/sbin/freeradius -f

Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Auth-Type PAP for attr Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Auth-Type CHAP for attr Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Auth-Type MS-CHAP for attr Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Autz-Type New-TLS-Connection for attr Autz-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Post-Auth-Type REJECT for attr Post-Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Post-Auth-Type Challenge for attr Post-Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: Compiling Post-Auth-Type Client-Lost for attr Post-Auth-Type
Sep 16 11:43:38 ubuntu freeradius[357163]: radiusd: #### Skipping IP addresses and Ports ####
Sep 16 11:43:38 ubuntu freeradius[357163]: Configuration appears to be OK
Sep 16 11:43:38 ubuntu systemd[1]: Started FreeRADIUS multi-protocol policy server.
```

Raadpleeg voor verdere FreeRADIUS-probleemoplossing/controles dit document - https://documentation.suse.com/smart/deploy-upgrade/pdf/freeradius-setup-server_en.pdf.

Voor UCSM kunnen succesvolle en niet-succesvolle aanmeldingen met RADIUS-gebruikers worden gevolgd in de primaire FI met behulp van de volgende opdrachten:

- nxos aansluiten
- logbestand logboekregistratie tonen

Een succesvolle aanmelding moet er als volgt uitzien:

```
2024 Sep 16 09:56:19 UCS-POD %UCSM-6-AUDIT: [session][internal][creation][internal][2677332][sys/user-e
_8291_A, name:ucs-RADIUS\alerosa, policyOwner:local][] Web A: remote user ucs-RADIUS\alerosa logged in
```

Een onsuccesvolle login ziet er ongeveer als volgt uit:

```
2024 Sep 16 09:51:49 UCS-POD %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from X.X.X.X - svc_s
```

Waar X.X.X.X de IP is van de machine die wordt gebruikt om SSH naar Fabric Interconnect te schakelen.

Gerelateerde informatie

- Verificatie configureren in UCSM
- Setup FreeRADIUS-server
- FreeRADIUS wiki

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.