Radiusverificatie configureren en oplossen op UCSM

Inhoud

Inleiding

In dit document worden de stappen beschreven voor het configureren en oplossen van problemen met Radius in UCS Manager met behulp van een Windows Server 2022 DataCenter.

Voorwaarden

- UCS Manager - 4.2(3o) of hoger
- Windows Server 2022 DataCenter

Configuratie op Windows Server

Active Directory Domain Services installeren

Raadpleeg Microsoft-document - AD DS installeren met Serverbeheer op Windows Server 2022.

De Active Directory-gebruiker aanmaken (aanmeldingsaccount)

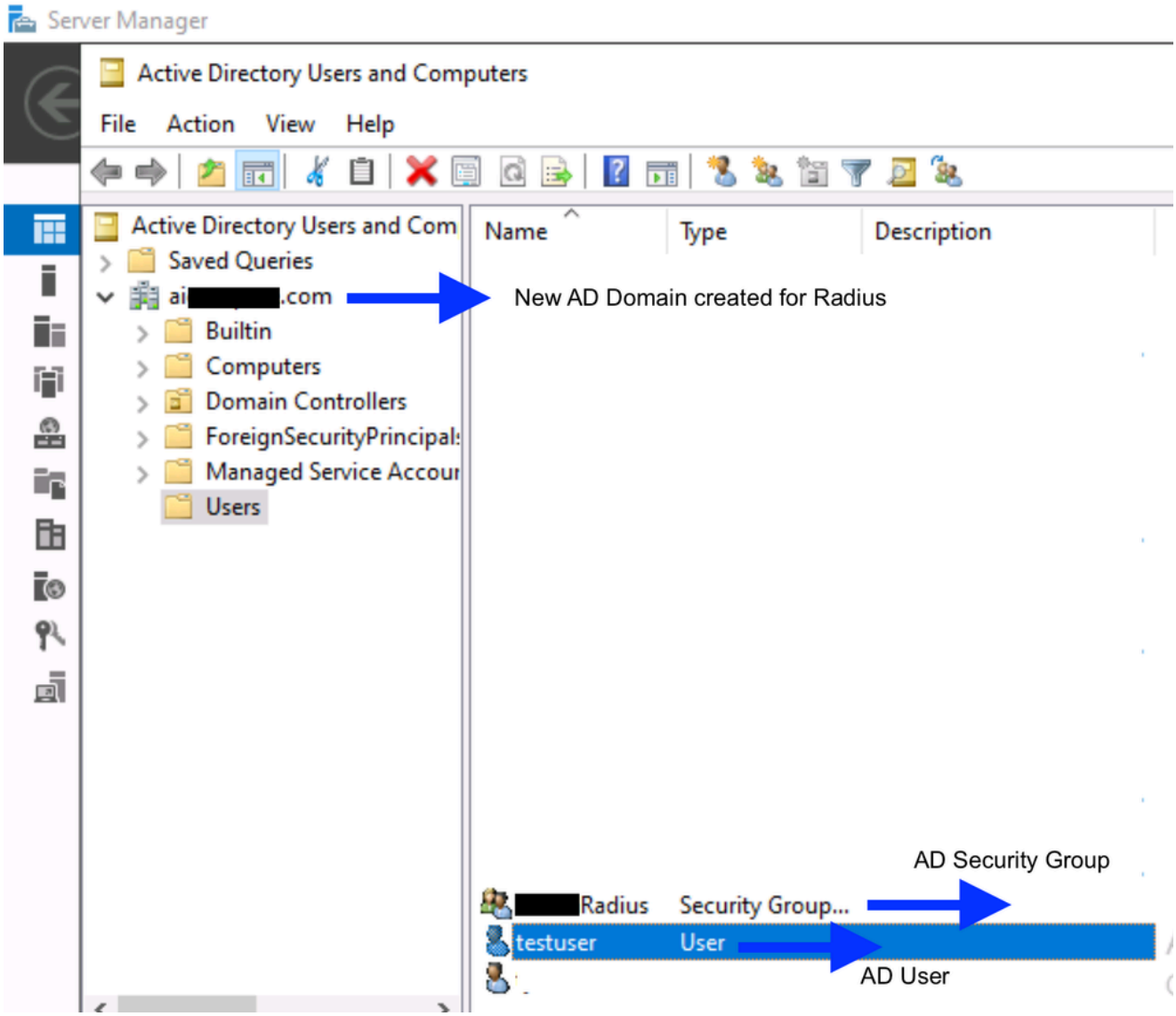
1. Open Serverbeheer > Extra > Active Directory-gebruikers en -computers.

2. Klik met de rechtermuisknop op het gemaakte domein > Nieuw > Gebruiker.

3. Voer de aanmeldnaam in (Voorbeeld - testgebruiker), stel een wachtwoord in, schakel het selectievakje Gebruiker moet wachtwoord wijzigen bij volgende aanmelding, en controleer of het wachtwoord nooit verloopt (voor een service/beheerdersaccount) > Voltooien (afhankelijk van uw lokale beveiligingsvereisten/beleid).

Een AD-beveiligingsgroep voor UCS-beheerders maken

- Klik in dezelfde console met de rechtermuisknop op uw domein > Nieuw > Groep (voorbeeld - testRadius, Beveiliging). Voeg de AD-gebruiker (testgebruiker) toe aan deze groep.
- Deze groepsnaam is wat je later moet toewijzen aan een UCS-rol.

- 

Installeer de NPS (RADIUS-rol) en registreer NPS in Active Directory

1. Navigeer naar Serverbeheer > Beheren > Rollen en functies toevoegen.

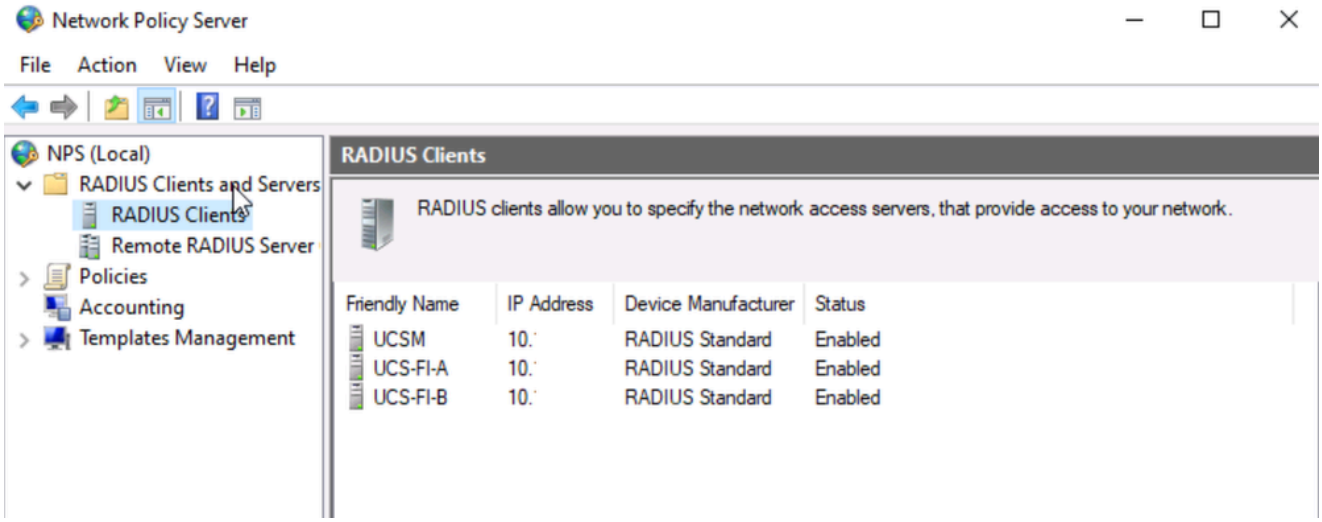
2. Selecteer Netwerkbeleid en toegangsservices > Voltooi de wizard om Netwerkbeleidsserver (NPS) te installeren.

3. Open Tools > Network Policy Server. Klik met de rechtermuisknop op NPS (Lokaal) > Registreer de server in Active Directory > OK. Hiermee kan NPS het lidmaatschap van een AD-gebruiker/groep lezen.

De UCS-verbindingen als RADIUS-clients toevoegen

- NPS vertrouwt verzoeken van UCSM. Vouw RADIUS-clients en -servers > RADIUS-clients

in NPS uit. Klik met de rechtermuisknop op Nieuw.

- Verstrekken:
  - Vriendelijke naam: Voorbeeld - UCSM
  - Adres (IP): het beheer van IP FI-A
  - Gedeeld geheim: maak een sterk geheim en schrijf het op - je moet deze exacte gedeelde geheime string later in UCSM invoeren.
- Herhaal dit voor Fabric Interconnect B en als u wilt verifiëren aan de hand van de VIP-cluster, voegt u dat IP-adres ook toe.
- 

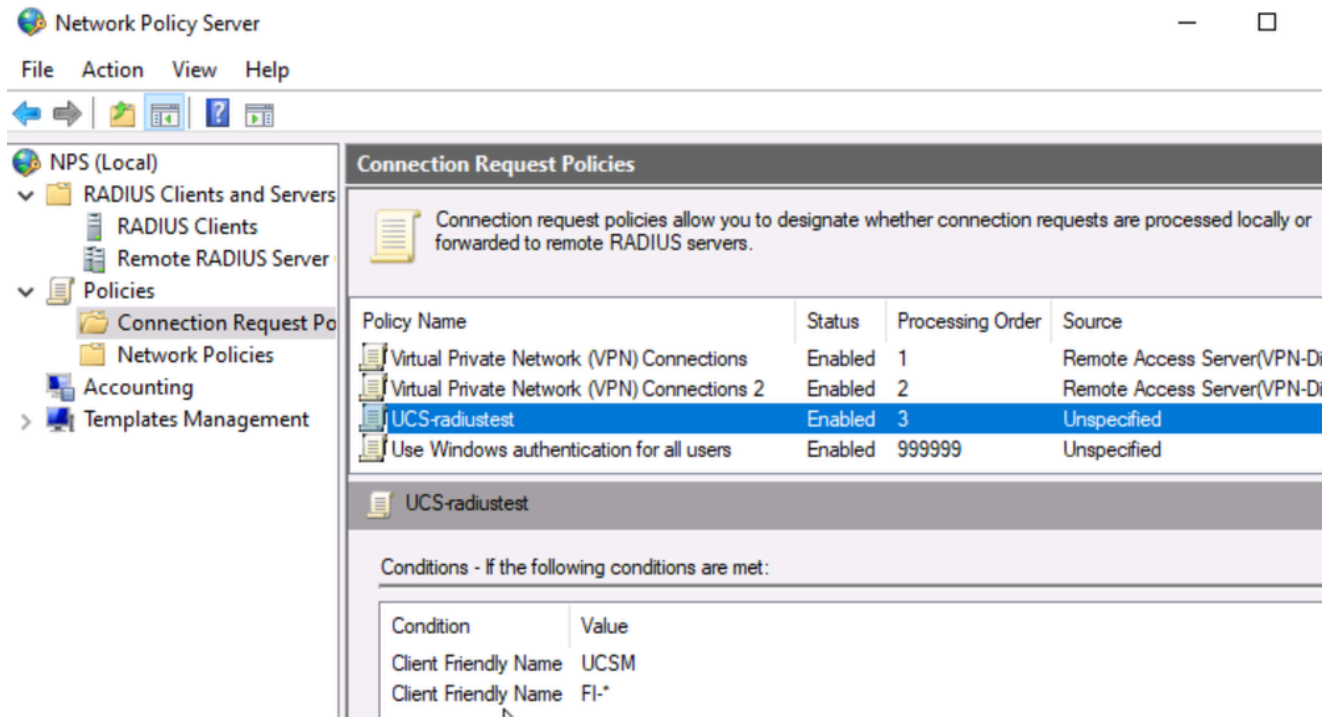
Radius-clients

Een beleid voor het aanvragen van een verbinding en een netwerkbeleid maken (autorisatie en roltoewijzing)

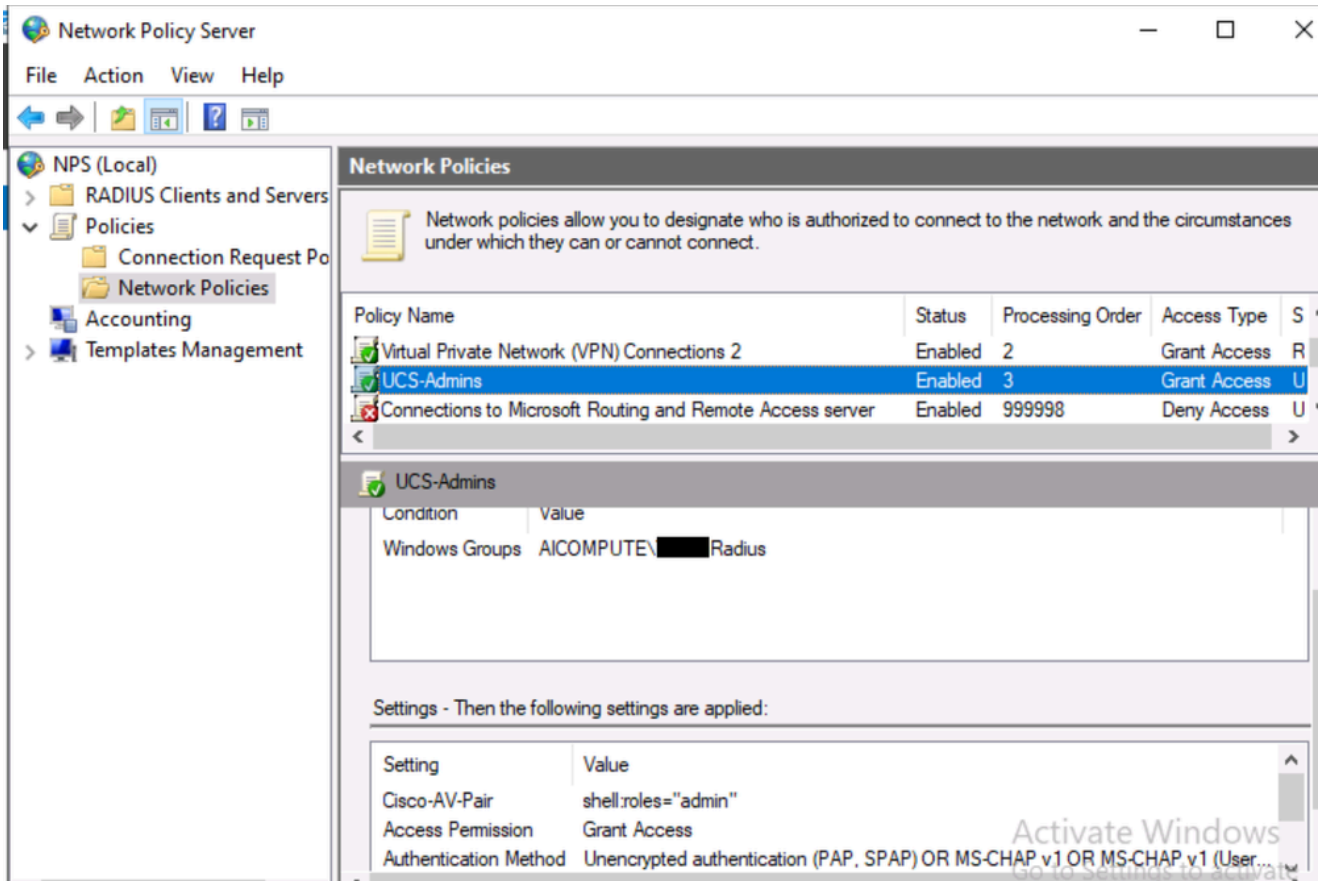
- Beleid > Verbindingsaanvraagbeleid > Nieuw > Geef het een naam (Voorbeeld - UCS-radiustest), voeg de voorwaarde voor 'klantvriendelijke naam' toe waarmee het lokaal kan worden geverifieerd. Bijvoorbeeld: FI-* of UCSM,
- Beleidsregels > Netwerkbeleid > Nieuw > Beleidsnaam
  - Voorwaarden: Windows-groepen toevoegen. Selecteer de groep TestRadius die u in stap 3 hebt gemaakt.
  - Toegangsmachtiging: Toegang verlenen
  - Verificatiemethoden: schakel ongecodeerde verificatie (PAP/SPAP) in en/of de methoden die UCS gebruikt. (UCS RADIUS gebruikt gewoonlijk PAP.)
- Instellingen configureren > Eigenschappen voor leverancier (dit is het belangrijkste onderdeel dat de AD-gebruiker toewijst aan een UCS-rol): Een kenmerk voor leverancier toevoegen > Cisco AV-Pair
  - Stel de waarde in op de tekenreeks UCS role/locale, Voorbeeld - shell:roles="admin"

(Als u dit kenmerk overslaat, meldt de gebruiker zich aan als alleen-lezen).

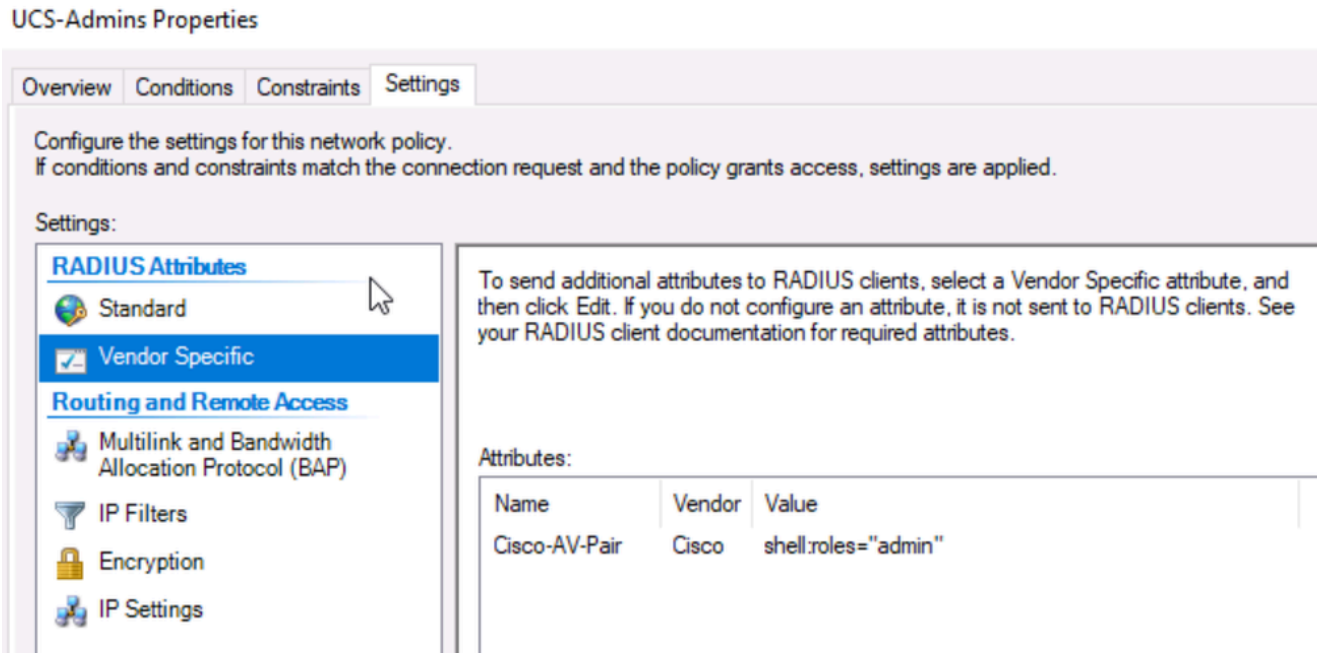
Verbindingsaanvraagbeleid

- 

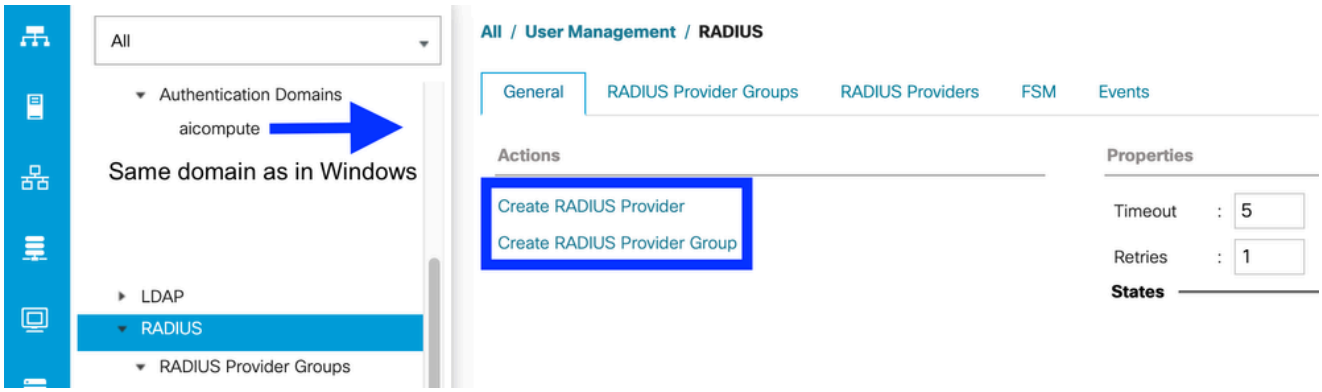
netwerkbeleid

- 

Specifiek kenmerk van leverancier

- 

Configuratie op UCSM

- 

Een radiusprovider maken en toevoegen aan een leveranciersgroep

1. Meld u aan bij de UCS Manager GUI en navigeer naar Beheer > Gebruikersbeheer > RADIUS.

2. Klik op RADIUS-provider maken (de optie +/ Aanmaken) en vul in:

- Hostnaam/FQDN of IP: uw Windows NPS-server.
- Sleutel: het exacte gedeelde geheim dat u hebt ingesteld in NPS Stap 5.
- Autorisatiepoort: 1812 (moet overeenkomen met NPS)
- Time-out / Retries: standaardwaarden laten beginnen.

3. Maak onder Beheer >Gebruikersbeheer > RADIUS een Providergroep (Voorbeeld - RADIUS-Grp) en voeg de provider van eerder toe.

Een verificatiedomein maken

Dit is het stuk dat het allemaal met elkaar verbindt.

1. Navigeer naar Beheer > Gebruikersbeheer > Verificatie > Verificatiedomeinen.

2. Klik op Een domein maken (voorbeeld - RADIUS - domeinnaam aanbevolen om hetzelfde te zijn als het domein dat in NPS is gemaakt).

3. Set Realm = RADIUS.

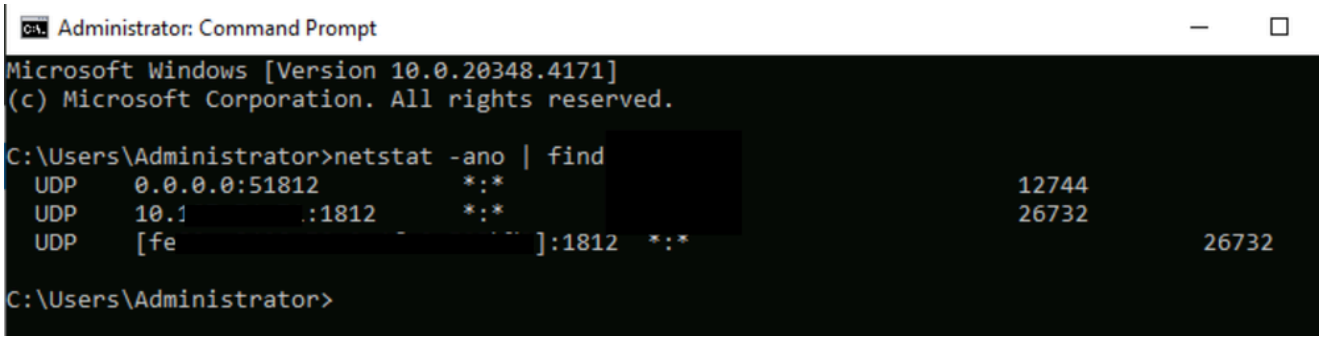
4. Wijs de door u gemaakte Providergroep toe (RADIUS-Grp) en sla deze op.

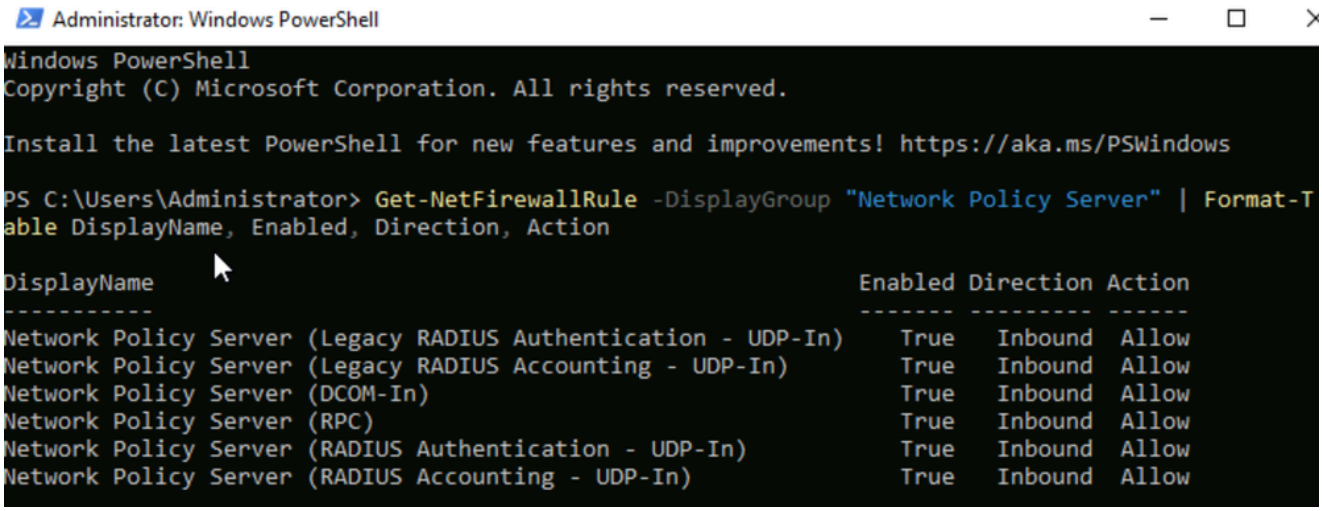
Verifiëren

Vanaf Windows Server - Firewall / poorten bevestigen

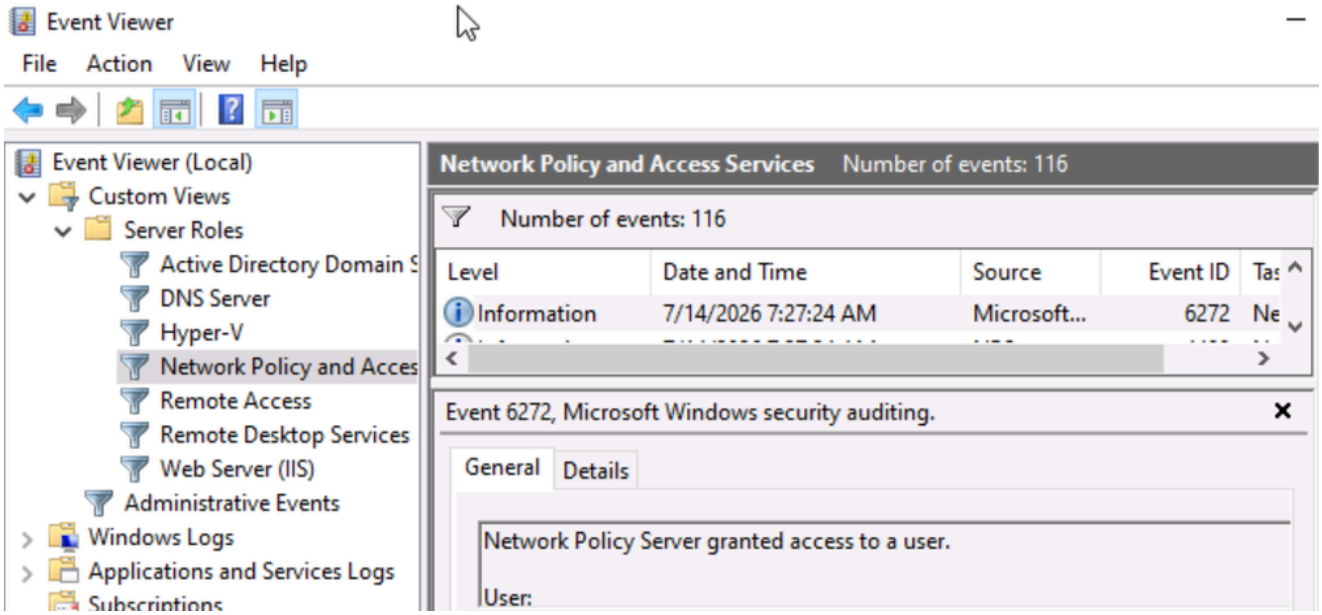
RADIUS-verificatie maakt gebruik van UDP-poort 1812 (en accounting 1813). Zorg ervoor dat de Windows-firewall en een eventuele netwerkfirewall deze toestaan van de IP's van FI-beheer.

1. Bevestig dat de NPS / Radius-service luistert via de netstat -ano | findstr 1812-opdracht.

- (U krijgt een lijn te zien met UDP en *:1812 (of de server IP:1812). Dit bevestigt dat de NPS/RADIUS-service actief luistert.
- Als er niets wordt weergegeven, kan NPS niet worden uitgevoerd — controleer Services > Network Policy Server (IAS) is gestart.)
- 

- Voer op Windows Powershell de opdracht : uit
  - Get-NetFirewallRule -DisplayGroup "Network Policy Server" | Format-Table DisplayName, ingeschakeld, richting, actie.
- 

- In Windows Event Viewer:
  - Aangepaste weergaven > Serverrollen > Netwerkbeleid en toegangsservices > Pakketten worden bereikt.



Inloggen testen vanuit UCSM

1. Log uit en log in door de vervolgkeuzelijst Domein te kiezen volgens het gemaakte Radius-domein.

2. Configureer het gebruikerswachtwoord. (Zie Windows-configuratie stap 2).

- Als de login werkt en u landt met beheerdersrechten, is de Cisco AV-Pair-toewijzing (Windows-configuratie Stap 6) correct.

Stralingsverificatie oplossen

Van Windows Server

1. Voer deze opdrachten uit in Powershell voor pakketvastlegging:

- Optimon-filter Toevoegen -P 1812
- Optie start --capture --PKT-size 0 -f C:\radius_capture.etl

2. Inloggen vanuit UCSM starten en vastleggen stoppen met behulp van opdrachten:

- potmonstop
- OptieMON ETL2PCAP C:\radius_capture.etl -o C:\radius_capture.pcap

3. Open radius_capture.pcap in Wireshark: RADIUS > Waardeparen kenmerken > bevestig dat Message-Authenticator (of attribuut 80) aanwezig is. Dit betekent dat NPS het antwoord ondertekent.

Van UCSM CLI

Bij het uitvoeren van een optie op Windows, gelijktijdig vanuit UCSM CLI,

1. Uitvoeren:

- NXOS aansluiten
- terminalmonitor
- Foutopsporingsstraal Alle

2. probeer een UCSM-login na het starten van de foutopsporing.

Een succesvolle login lijkt op 2026 Jul 3 09:54:02.917044 radius: Geverifieerd bericht Authenticator in reactie van: 10.xxx.xx.xx.

- Als pakketten worden verzonden en ontvangen, maar inloggen mislukt met berichtenauthenticator is waarschijnlijk onjuist. in de debug-uitvoer - dit betekent dat de poort en bereikbaarheid prima zijn.
  - Probeer het gedeelde geheim in de Windows NPS-server en de UCSM-sleutel opnieuw te configureren (deze moeten exact overeenkomen).
  - Als het probleem zich blijft voordoen tijdens het aanmelden na het opnieuw configureren, kunnen we een bekende Cisco-bug-ID CSCwm80801 raken: Gebruiker kan zich niet aanmelden bij UCSM met behulp van Radius nadat Microsoft-patch KB5040434 een upgrade naar een genoemde vaste release vereist.

Gerelateerde informatie

- Cisco UCS Manager Management Guide 4.2 - Externe verificatie

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.