Cisco DCM - ondersteuning voor externe verificatie

Inhoud

Inleiding

Dit document beschrijft de Cisco Digital Content Manager (DCM)-softwareRemote-verificatie met behulp van RADIUS.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Cisco DCM-softwareversie 16 en hoger.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Cisco DCM-software v16.10 en hoger.
- RADIUS-server die wordt uitgevoerd met freeRadius open-source software.

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.

Achtergrondinformatie

In V16.10 van de DCM is een nieuwe functie geïntroduceerd die het mogelijk maakt om

gebruikersaccounts die op een RADIUS-server zijn ingesteld, te gebruiken om toegang te krijgen tot de DCM GUI. Dit document beschrijft de instellingen die op de DCM en de RADIUS-server vereist zijn om van deze functie gebruik te maken.

GUI-rekeningen op DCM

In versies 16.0 en lager waren de gebruikersrekeningen die vereist zijn om toegang tot de GUI te krijgen, lokaal bij de DCM, d.w.z. gemaakt, gewijzigd, gebruikt en verwijderd op de DCM.

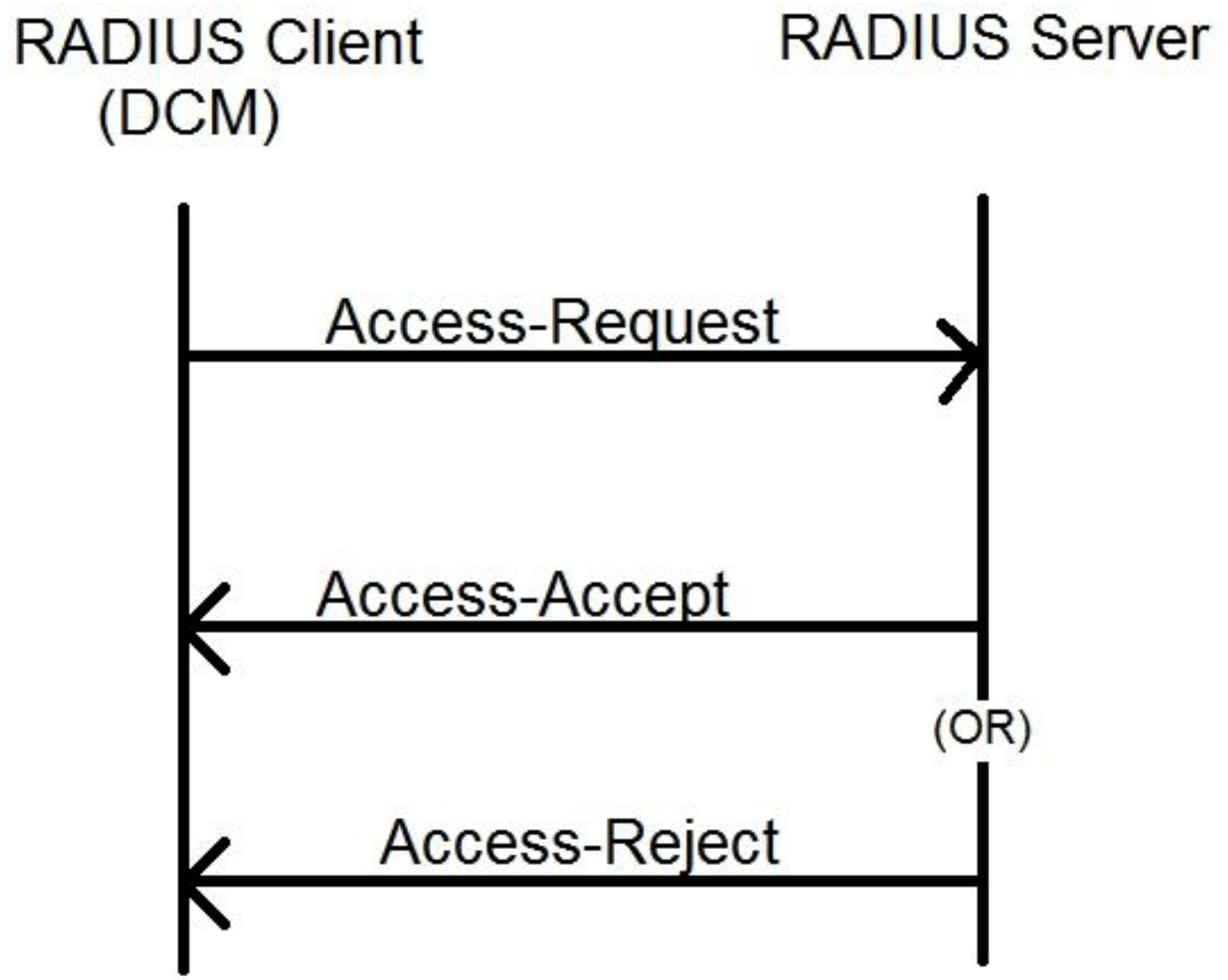
Een GUI-gebruikersaccount kan tot een van deze groepen behoren:

- Beheerders (volledige controle)
- Gebruikers (lezen)
- gasten (alleen lezen)
- Automation triggers (externe triggers)
- DTF-beheerders (DTF-sleutelconfiguratie)

Remote-verificatie

Het idee van externe authenticatie is om een gecentraliseerde verzameling gebruikersrekeningen te hebben die kan worden gebruikt om toegang te krijgen tot een apparaat, toepassing, dienst enz.

De stappen in het beeld leggen uit wat er gebeurt als u externe authenticatie gebruikt:



Stap 1. Gebruiker geeft de inlognaam en het wachtwoord in (gebruikersaccount ingesteld op een RADIUS-server) op de inlogpagina op de DCM GUI.

Stap 2. De DCM stuurt een toegangsaanvraag-bericht met de referenties naar de RADIUS-server.

Stap 3. De RADIUS-server controleert of het verzoek van een van de geconfigureerde klanten is ingediend en of de gebruikersaccount op de DB/File ervan bestaat en bevestigt of het wachtwoord juist is of niet, waarna een van de volgende berichten naar de DCM wordt teruggestuurd

- Toegang-accepteren - Dit betekent dat de aanmeldingsgegevens geldig zijn. De geconfigureerde RADIUS-kenmerken worden teruggegeven.
- Toegang-afwijzing - Dit betekent dat de aanmeldingsgegevens ongeldig zijn en dat de RADIUS-server mogelijk is geconfigureerd om bepaalde RADIUS-kenmerken te verzenden om de fout in te lichten.
- Access-Challenge - Dit betekent dat de RADIUS-server extra informatie nodig heeft voor het valideren van de authenticiteit van de gebruiker. Niet verwerkt in de DCM.

Indien een RADIUS-server een toegangsverwerp verstuurt, controleert de DCM of de gebruikersaccount plaatselijk is bij de DCM zelf en wordt de verificatieprocedure gevolgd.

De gebruiker wordt opnieuw geauthentiseerd met een interval van 15 minuten (intern) om te bevestigen dat de gebruikersnaam/het wachtwoord nog steeds geldig is en de gebruiker tot een van de GUI-accountgroepen behoort. Als de verificatie mislukt, wordt de huidige gebruikerssessie ongeldig geacht en worden alle rechten voor de gebruiker ingetrokken.

RADIUS-server configureren

Om de gebruikersaccounts te kunnen gebruiken die op een RADIUS-server aanwezig zijn om de GUI te bereiken, moeten deze stappen worden gevolgd:

DCM moet worden ingesteld als een client voor de RADIUS-server.

1. Voeg de IP van de DCM als client voor de RADIUS-server toe.
2. Voeg het gedeelde geheim toe aan de clientconfiguratie (dit gedeelde geheim moet hetzelfde zijn als dat ingesteld is op de DCM, zie sectie De DCM configureren).
3. Voor elke DCM wordt een ander gedeeld geheim aanbevolen.
4. De lengte van het gedeelde geheim moet minimaal 22 tekens lang zijn.
5. Het gedeelde geheim moet zo willekeurig mogelijk zijn.

   Voorbeeld van een goed gedeeld geheim : ‘89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345’

Voor een gebruikersaccount moet het bericht Toegang-Accept van de RADIUS-server een RADIUS-kenmerk hebben dat de GUI-accountgroep identificeert waartoe de gebruiker behoort. De attributennaam kan worden geselecteerd en moet in het instellingsbestand op de DCM worden ingesteld.

Dit is het formaat van de string die verzonden moet worden als waarde voor een eigenschap van de RADIUS-server:

OU=<group_name_string>group_name_string kan één van deze zijn:

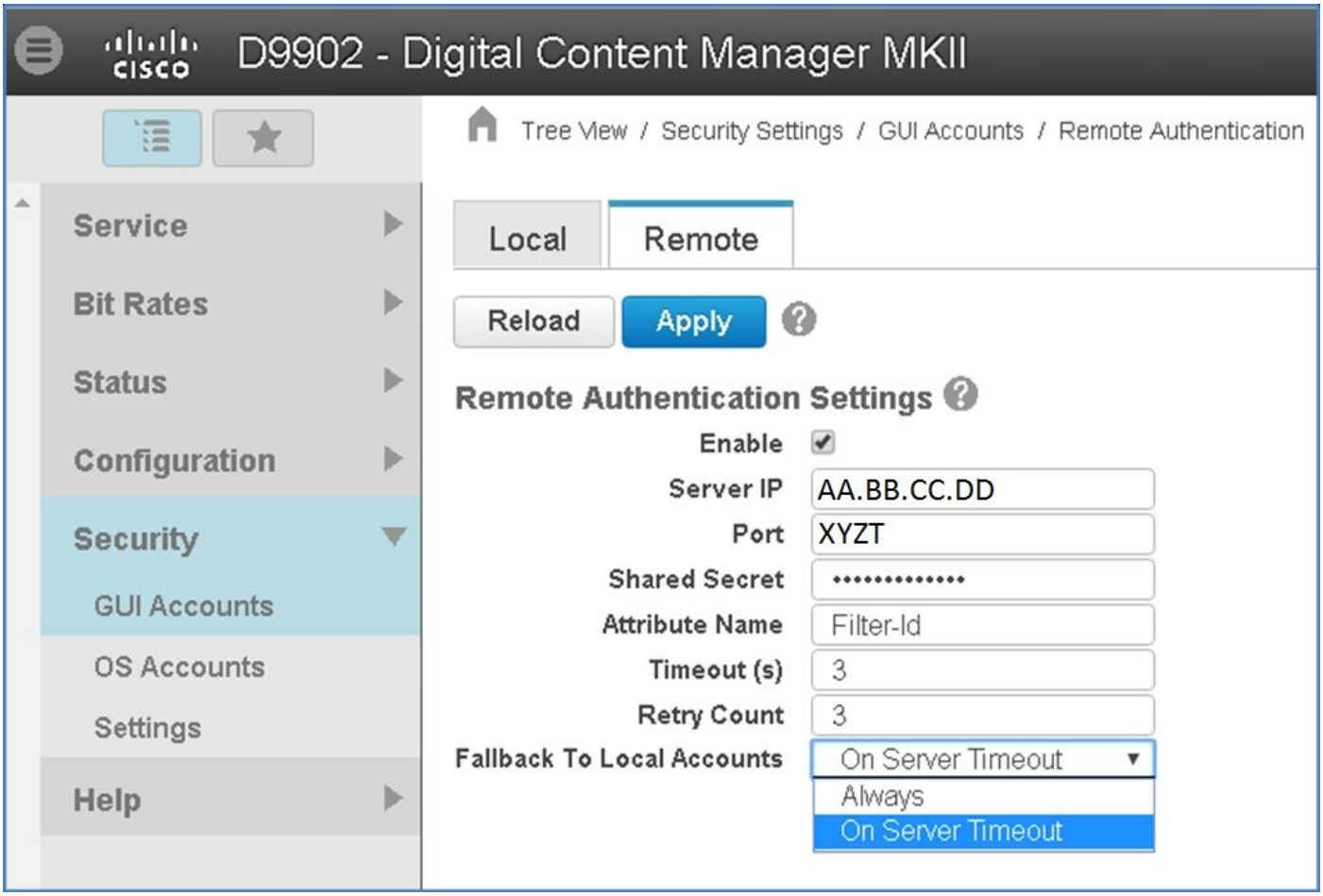
Groep	Naam van groep
Beheerders (volledige controle)	beheerders
Gebruikers (lezen)	gebruikers
gasten (alleen lezen)	gasten
Automation triggers (extern) triggers)	automatisering
DTF-beheerders (DTF-sleutel) configuratie)	dtfadmins

Cisco DCM configureren

Om de functie voor externe verificatie op de DCM in te schakelen/aan te passen, is een Administrator-account vereist.
Deze stappen geven aan hoe u afstandsverificatie kunt configureren:

Stap 1. Meld u aan bij de DCM met behulp van een Administrator-account.

Stap 2. Navigeer naar **Security > GUI Account** en selecteer **het** tabblad **Remote**, zoals in de afbeelding:



Stap 3. Configureer de parameters die vereist zijn voor RADIUS-communicatie:

- Inschakelen - Deze instelling bepaalt of de ondersteuning voor externe verificatie al dan niet moet worden ingeschakeld. Als deze optie is ingeschakeld, is de rest van de parameter velden ingeschakeld.

- IP-adres van de server van de RADIUS.

- Port - Port - waarop de RADIUS-server naar verificatiepakketten luistert (over het algemeen 1812 maar kan worden geconfigureerd voor andere waarden).

- Beveiliging - Dit is het gedeelde geheim dat wordt gebruikt om het wachtwoord te versleutelen voordat u het RADIUS-pakket naar de server stuurt. Dit geheim zou hetzelfde moeten zijn als dat gevormd op de RADIUS server waar het gebruikt wordt om het wachtwoord te decrypteren.

- Naam van kenmerk - de naam van de eigenschap waarin de vergunningsgegevens van de RADIUS-server worden ontvangen.

- Time-out (in seconden) - Deze instelling wordt gebruikt voor communicatie tussen de RADIUS-server en DCM. Dit is de tijd dat de DCM op een antwoord van de RADIUS-server op een bepaald verzoek moet wachten alvorens het verzoek te beëindigen.

- Count opnieuw proberen - Het aantal keer dat het RADIUS-verzoek wordt ingediend moet worden verstuurd voor het geval dat vorige verzoeken zijn getimed.

- Back to Local Account - Deze instelling is beschikbaar vanaf DCM versie 19.0. Met DCM kan u inloggen op een GUI (lokale) account dat met de GUI aangemaakt wordt. Optie biedt **Time-out bij server** de mogelijkheid om back-ups te maken van de lokale rekeningen wanneer de Radius-server niet kan worden bereikt, en niet wanneer verificatie mislukt. Optie, **altijd** staat toe om altijd terug te vallen, zelfs wanneer de authenticatie faalde.

Stap 4. Als de wijzigingen worden toegepast, wordt de waarschuwing in de afbeelding weergegeven. Klik op **OK** en de gebruikersinterface wordt opnieuw gestart.

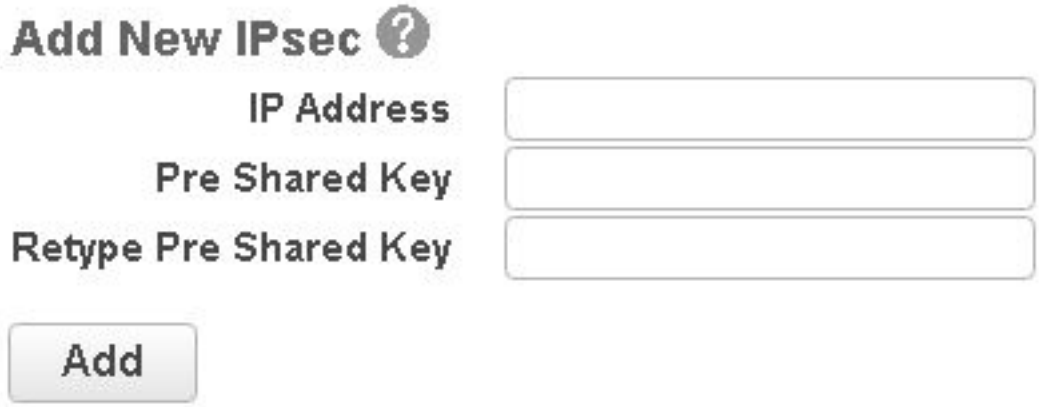
Stap 5. Nu is de DCM klaar voor externe verificatie.

Configuratie IPSec op DCM:

1. Log in op de DCM met behulp van een GUI-account dat tot de beveiligingsgroep van beheerders behoort.

2. Navigeer naar **Configuration > System**. De pagina Systeeminstellingen verschijnt.

3. Raadpleeg het gebied **Nieuwe IPsec toevoegen**, zoals in de afbeelding weergegeven.



4. Voer in het veld IP-adres het IP-adres van de nieuwe IPsec-peer (RADIUS-server) in.

5. Voer in de **Vooraf gedeelde** toets en retype *Vooraf gedeelde sleutel* in de *Vooraf gedeelde sleutel* voor het nieuwe IPsec-peer.

6. Klik op **Toevoegen**. De nieuwe peer IPsec wordt toegevoegd aan de tabel met IPsec-instellingen.

> **Opmerking:** Voor de configuratie van IPSec op de machine waarop de RADIUS-server draait, wordt verwezen naar de documentatie/publicatie die bij het product wordt geleverd.

Veiligheidsoverwegingen

- Het gedeelde geheim wordt opgeslagen in het heldere bestand van de DCM.
- Het gecodeerde wachtwoord wordt opgeslagen in het geheugen van de DCM voor gebruik bij herverificatie gedurende de sessie.
- Gezien de twee bovenstaande punten, is het raadzaam om te beperken wie toegang tot de DCM heeft voor het oplossen van problemen.
- Het is sterk aanbevolen IPSec te gebruiken om het communicatiekanaal tussen DCM en RADIUS te beveiligen
  server.

Beperkingen en beperkingen

- De ondersteuning van externe authenticatie is alleen beschikbaar voor de GUI-rekeningen, niet voor de OS-rekeningen.
- Een herauthenticatie wordt uitgevoerd met een interval van 15 minuten. Voorbeeld: Als de groep van een gebruiker is gewijzigd, is de slechtst denkbare tijd die voor de verandering die moet plaatsvinden 15 minuten.
- Als externe authenticatie is ingeschakeld, controleert de DCM eerst met de RADIUS-server als de gebruikersaccount al dan niet geldig is en controleert u vervolgens de lokale database.

Als er lokale rekeningen worden gebruikt die niet op de RADIUS-server bestaan, zou er een authenticatiefout bericht op de RADIUS-server zijn.

FreeRadius instellen

Deze paragraaf laat als voorbeeld zien hoe u freeRadius kunt instellen om deze voor de DCM te gebruiken als externe verificatieserver. Dit is uitsluitend ter informatie bedoeld;

Cisco biedt of ondersteunt geen FreeRadius. Er wordt aangenomen dat de configuratiebestanden voor freeRadius zijn gevonden onder **/etc/freeRadius/** (check distributie).

Wijzig deze bestanden nadat u het pakket freeRadius hebt geïnstalleerd.

- **/etc/freeradius/clients.conf** wijzigen
  Stap 1. Voeg een vermelding toe voor de IP van de DCM aan de lijst met klanten.
  Stap 2. Voeg de gedeelde sleutel toe in de clientconfiguratie en laat de andere parameters standaard staan.

  Aanbevolen wordt om voor elke DCM een uniek gedeeld geheim te hebben.
  De lengte van het gedeelde geheim moet minimaal 22 tekens lang zijn. Het gedeelde geheim moet zo willekeurig mogelijk zijn.

  Voorbeeld van een goed gedeeld geheim :
  ‘89w%$w*78619ew8r4$7$6@q!9we#%^rnEWR@#QEws13&4^%sf54gsf4@!fg3sdf#@sdf$d3g44fg3%2s2345’

- Wijzig **/etc/freeradius/radiusd.conf** om de poort te wijzigen waarop de Straalserver moet luisteren (meestal 1812)

- Wijzig de **enz/freeradius/gebruikers** om nieuwe gebruikers toe te voegen.

- Zorg ervoor dat u de RADIUS-eigenschap toevoegt waarin de vergunningsinformatie in deze indeling naar de DCM wordt verzonden:
  <Naam van kenmerk> = **'OU=<group_name>'**

  Naam van kenmerk: Dit is de naam van de standaard RADIUS-eigenschap waarop de autorisatiegegevens naar de DCM-groep_name worden verzonden.
  beheerders - Een gebruiker die tot deze groep behoort heeft beheerrechten, d.w.z. volledige controle.
  gebruikers - Een gebruiker die tot deze groep behoort heeft rechten om te lezen.
  gasten - Een gebruiker die tot deze groep behoort zal slechts voorrecht hebben gelezen.
  automatisering - Gebruikt voor automatisering (externe triggers).
  dtfadmins - DTF-beheerder (DTF-sleutelconfiguratie)

  Voorbeeld:
  Wachtwoord voor hoofdklaring:= "testen"

Filter-ID = "OU=beheerders"

- (Re)start de Straalserver om de wijzigingen van kracht te laten worden.
- Zorg ervoor dat de firewallconfiguratie van de Straalserver externe toegang tot de gekozen server biedt
  port.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Voor het fouilleren zijn enkele extra logbestanden in het veiligheidslogboek geïntroduceerd. Om dit logbestand te bekijken navigeer naar **Help > Traces-pagina** in DCM GUI.

In dit gedeelte wordt beschreven naar wat er in de documenten moet worden gezocht, wat de problemen zouden kunnen zijn en mogelijke oplossingen.

Log lijn	Remote-inlogpoging mislukt: Het verzoek aan de RADIUS-server is verzonden.
Uitgeven	DCM kan niet communiceren met de RADIUS-server.
Mogelijke oplossing	• Controleer dat het IP-adres van de RADIUS-server dat in de configuratie van de externe verificatie in de DCM is meegeleverd, juist is. • Zorg ervoor dat de RADIUS-server toegankelijk is via de DCM. • Zorg ervoor dat de DCM is ingesteld als een geldige client op de RADIUS-server (RADIUS-server laat toegangsaanvragen van onbekende clients in stilte vallen). • Zorg ervoor dat het gedeelde geheim dat op de DCM is ingesteld, hetzelfde is als het gedeelde geheim dat op de RADIUS-server voor de DCM is ingesteld (Als de server geen gedeeld geheim voor de client heeft, wordt het verzoek stilletjes ingetrokken).
Log lijn	Remote-inlogpoging is mislukt: [10054] Een bestaande verbinding werd met kracht gesloten door de afstandsbediening.
Uitgeven	De DCM heeft een RADIUS-verzoek naar de gespecificeerde server-IP verzonden. De RADIUS-servertoepassing luistert echter niet op de poort die in de instellingen voor externe verificatie is gespecificeerd.
Mogelijke oplossing	• Zorg ervoor dat de RADIUS-server actief is. • Controleer of het poortnummer dat in de RADIUS-configuratie op de server is opgegeven, gelijk is aan het nummer dat op de DCM is ingesteld.
Log lijn	Remote-inlogpoging mislukt: Ongeldige attributennaam opgegeven of reactie van RADIUS-server ontbreekt aan vergunningsgegevens.
Uitgeven	Er is een probleem met de reactie die van de RADIUS-server is ontvangen.
Mogelijke oplossing	• Zorg ervoor dat de RADIUS-server de eigenschap (ingesteld op de DCM) verstuurt in de respons ‘Access-Accept’. • Zorg ervoor dat de parameter **Naam** van **kenmerk** die is ingesteld in de instellingen voor

	externe verificatie van DCM de exacte naam is zoals opgegeven in de gebruikersconfiguratie op de RADIUS-server.
Log lijn	Ongeldige autorisatie gegevens ontvangen van RADIUS Server.
Uitgeven	Verificatie is geslaagd maar de reactie die van de RADIUS-server is ontvangen, bevat ongeldi autorisatiegegevens, d.w.z. de naam van de beveiligingsgroep.
Mogelijke oplossing	• Zorg ervoor dat de groepsnaam die voor die gebruiker op de RADIUS-server is ingesteld, van de beveiligingsgroepnamen is die in de sectie RADIUS-server configureren is. • Zorg ervoor dat het formaat van de string die op de RADIUS-server is ingesteld, overeenk met het formaat dat in de sectie RADIUS-server configureren is gespecificeerd.