Problemen oplossen " Toegang geweigerd" Waarschuwing in Umbrella AD-connector

Inhoud

Inleiding

In dit document wordt beschreven hoe problemen kunnen worden opgelost wanneer de Cisco Umbrella Active Directory (AD)-connector zich in de status Waarschuwing of Fout bevindt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

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.

Probleem

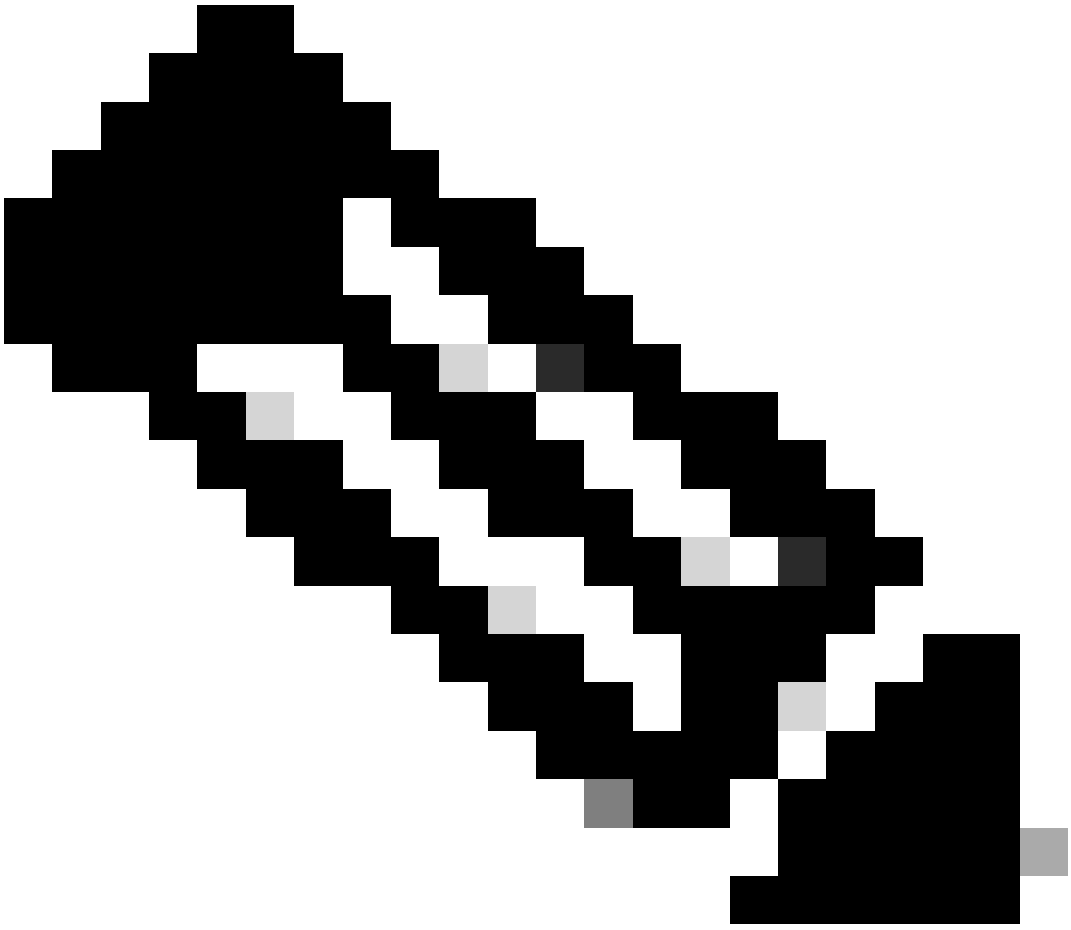
U merkt dat een AD-connector een waarschuwing of foutstatus weergeeft en het bericht dat wordt weergegeven wanneer u over de waarschuwing zweeft, bevat 'Toegang geweigerd' naar een van de geregistreerde AD-servers.

Oplossing

Controleer of de OpenDNS_Connector-gebruiker lid is van deze AD-groepen:

- Gebeurtenislogboeklezers
- Gedistribueerde COM-gebruikers
- Enterprise Read-only Domain Controllers

De oplossing is ervoor te zorgen dat DCOM, WMI en Manage Audit and Security Log correct zijn ingesteld op de betreffende AD-server.



> Opmerking: Meerdere domeinen of meerdere bossen worden standaard niet ondersteund. Raadpleeg de Multi-AD Domain Support in Umbrella aankondiging. U kunt ook contact opnemen met Umbrella Support over uw configuratie om hulp te krijgen als u tegen deze problemen aanloopt.

WMI-machtigingen controleren:

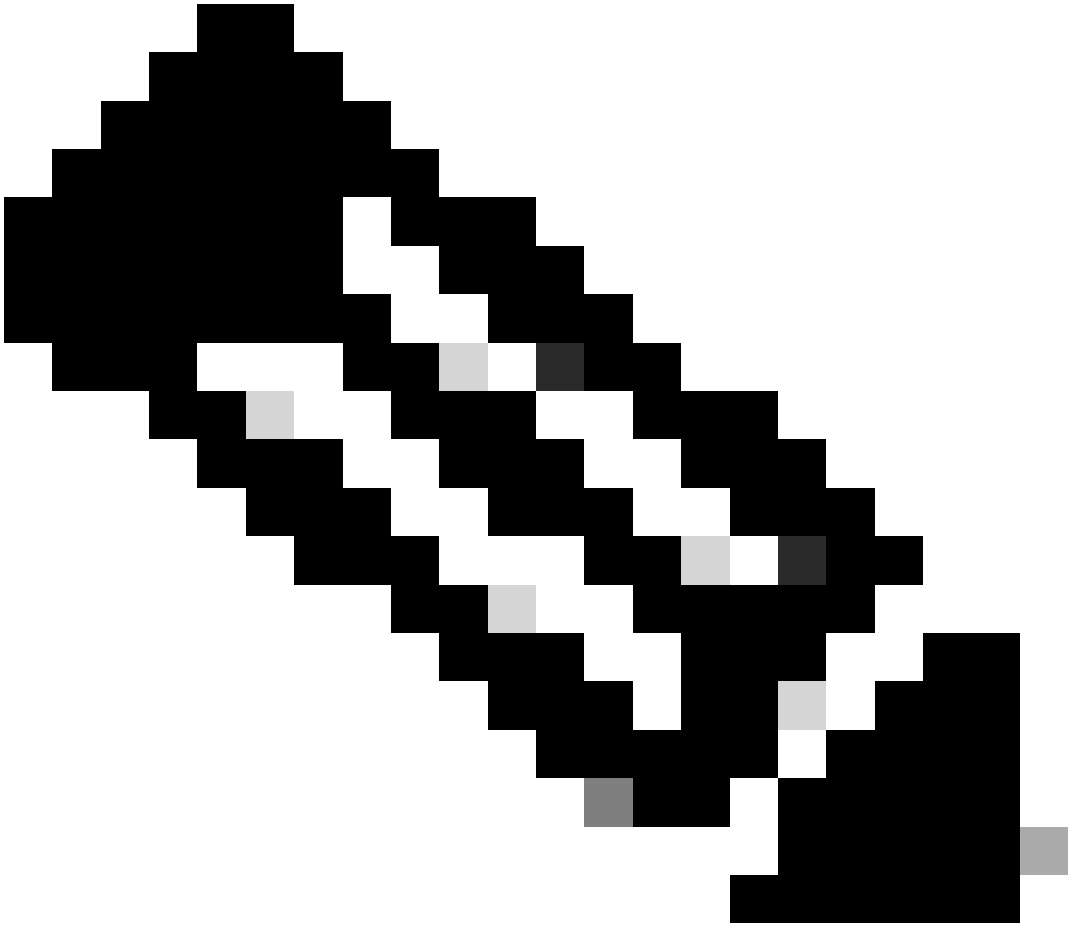
1. Selecteer Start > Uitvoeren > wmimgmt.msc om toegang te krijgen tot de Windows

Management Infrastructure Control-console.
2. Klik met de rechtermuisknop op WMI-besturingselement > Eigenschappen > tabblad Beveiliging.
3. Selecteer Hoofdmap > CIMV2-naamruimte en selecteer de knop Beveiliging.
4. Voeg de OpenDNS_Connector-gebruiker toe en sta deze rechten toe:

- Account inschakelen
- Extern inschakelen
- leesbeveiliging

DCOM-machtigingen controleren:

1. Voer vanaf een opdrachtregel dcomcnfg uit.
2. Navigeer naar Console Root > Component Services > Computers.
3. Klik met de rechtermuisknop op Deze computer en selecteer Eigenschappen.
4. Selecteer het tabblad COM-beveiliging van My Computer Properties (Eigenschappen van deze computer).
5. Selecteer Limieten bewerken in de sectie Starten en activeren van machtigingen.
6. Voeg de OpenDNS_Connector-gebruiker toe en sta machtigingen voor starten op afstand en activering op afstand toe.
7. Selecteer OK om de eigenschappen van Deze computer te bevestigen en te sluiten.



Opmerking: in de meeste gevallen, als DCOM-wijzigingen worden aangebracht, is een reboot van die DC vereist om de wijzigingen van kracht te laten worden.

Controleren van "Audit- en beveiligingslogs beheren" op Windows 2003-servers:

1. Open op een domeincontroller een opdrachtprompt en typ deze opdracht (als u Windows 2003 uitvoert, vervangt u /r door /v):

```
gpresult /scope computer /r
```

2. Zoek naar de regel Toegepaste groepsbeleidsobjecten. Hieronder vindt u een lijst met beleidsregels die op die domeincontroller worden toegepast. Noteer er een die kan worden toegepast op alle domeincontrollers.
(zoals "Default Domain Controllers Policy"). Als er geen bestaat, moet u er een maken en toepassen.

Om het juiste beleid te bewerken:

3. Open het paneel Groepsbeleidsbeheer (via Start-/beheertools). Selecteer het gewenste beleid. Iets in de map "Domeincontrollers" is een waarschijnlijke kandidaat.

4. Klik met de rechtermuisknop op dat beleid en selecteer Bewerken om de Groepsbeleidsbeheereditor te openen.

5. Blader naar de map Computerconfiguratie\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment en selecteer Audit- en beveiligingslogboek beheren om de eigenschappen ervan te bekijken.

6. Selecteer Deze beleidsinstellingen definiëren > Gebruiker of groep toevoegen. Blader en selecteer de OpenDNS_Connector-gebruiker.

7. Voer de opdracht "gpupdate /force" uit op de domeincontroller om ervoor te zorgen dat het beleid wordt toegepast.

Oorzaak

Deze fout geeft meestal aan dat de OpenDNS_Connector-gebruiker onvoldoende rechten heeft om te werken.

Het Windows Connector-script stelt normaal gesproken de vereiste machtigingen in voor de OpenDNS_Connector-gebruiker. In strikte AD-omgevingen mogen sommige beheerders echter geen VB-scripts uitvoeren op hun domeincontrollers en moeten ze dus handmatig de acties van het Windows-configuratiescript repliceren.

Aanvullende informatie

Ga voor meer informatie over het oplossen van dit probleem naar Complete Topics for Access Denied Resolution (Complete onderwerpen voor toegang tot oplossingen voor geweigerde toegang).

Als u na het bevestigen/wijzigen van de bovengenoemde instellingen nog steeds "Toegang geweigerd"-berichten in het Dashboard ziet, stuur dan de ondersteuningslogboeken zoals beschreven in dit artikel: Ondersteuning bieden met AD Connector-logboeken.

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.