Vereiste machtigingen voor de OpenDNS_Connector-gebruiker begrijpen

Inhoud

Inleiding

Overzicht

Vereiste machtigingen

Directory-wijzigingen repliceren

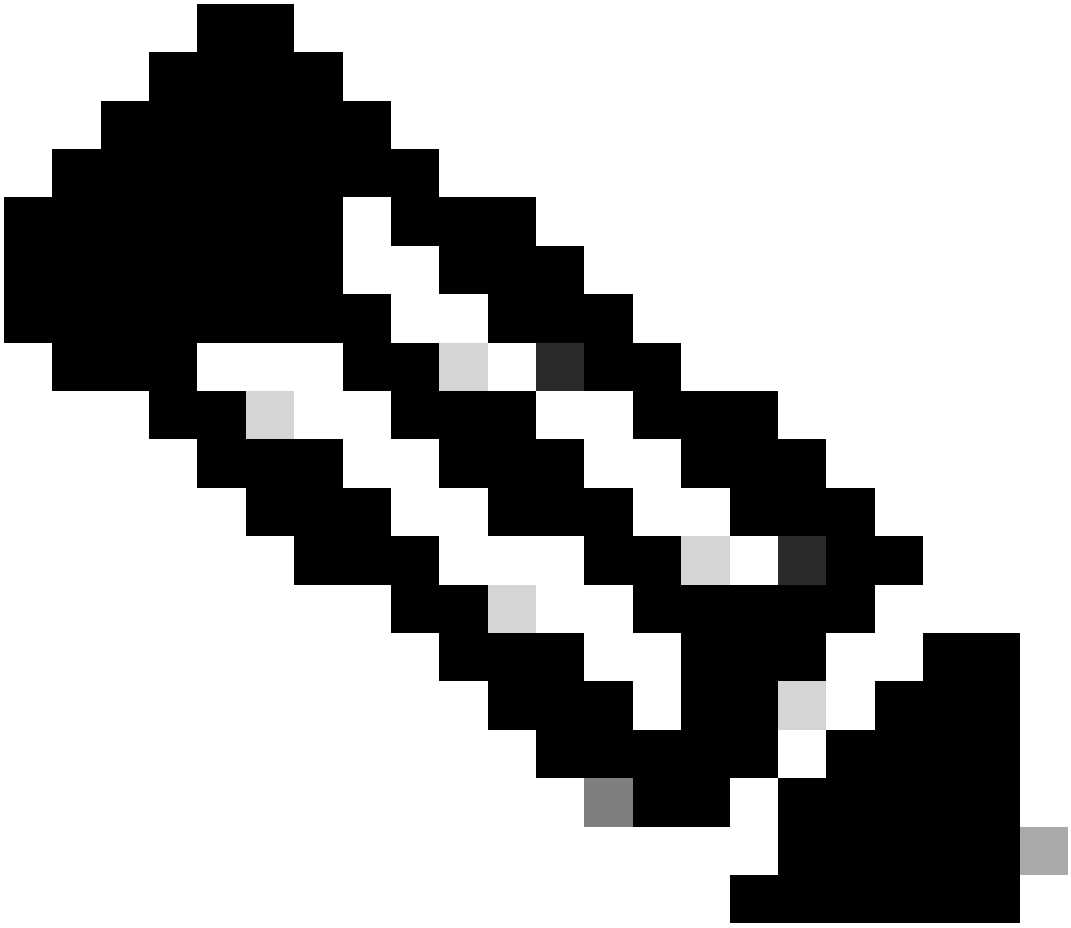
Gebeurtenislogboeklezers

Extern beheer

controlebeleid

Inleiding

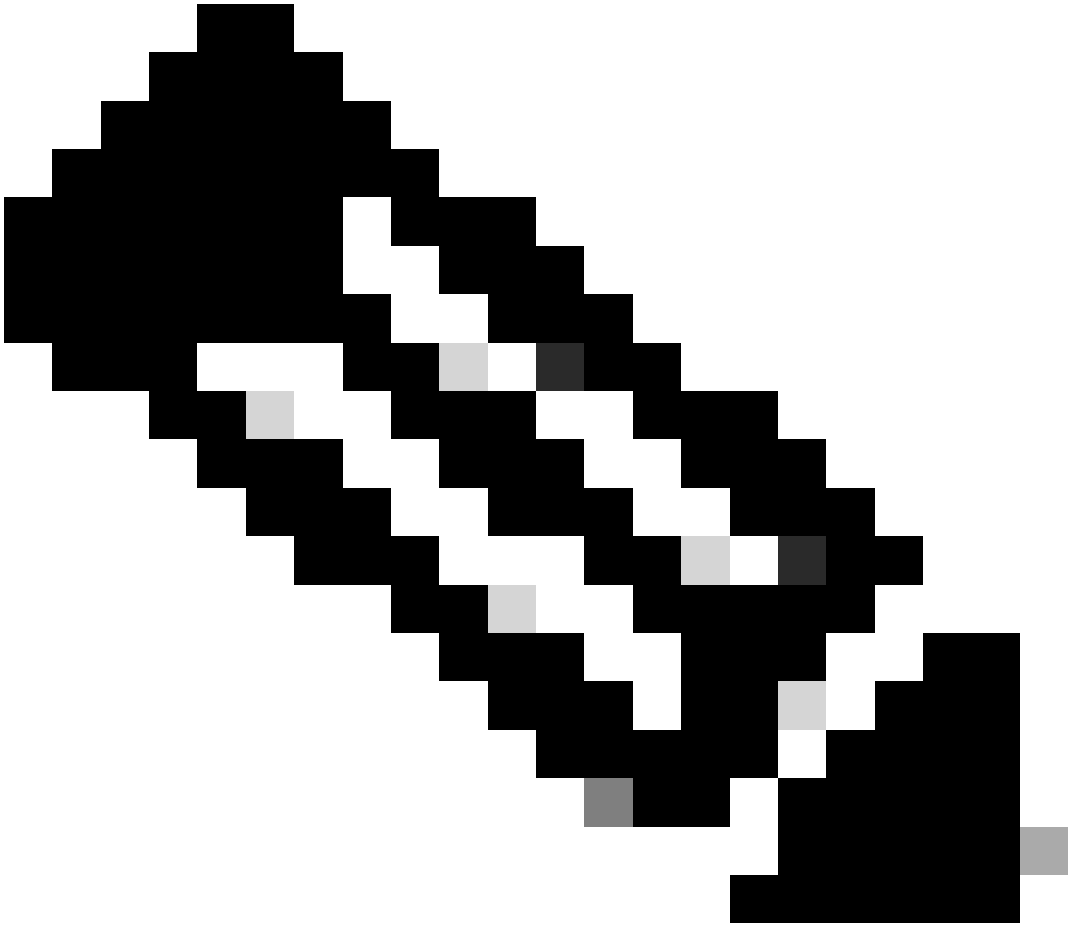
In dit document worden de vereiste machtigingen voor gebruikers van OpenDNS_Connector beschreven.



Opmerking: In overeenstemming met re-branding inspanningen, de veronderstelde AD gebruikersnaam "OpenDNS_Connector" is onlangs bijgewerkt tot nu "Cisco_Connector" plaats.

Overzicht

Het Windows Connector-script stelt normaal gesproken de vereiste machtigingen in voor de Cisco_Connector-gebruiker. In strikte AD-omgevingen is het echter mogelijk dat sommige beheerders geen VB-scripts op hun domeincontrollers mogen uitvoeren en daarom de acties van het Windows-configuratiescript handmatig moeten repliceren. In dit artikel wordt beschreven welke machtigingen moeten worden ingesteld op de DC.



Opmerking: Voor het doel van dit artikel wordt Cisco_Connector verondersteld de sAMAaccountName van uw Connector-account in AD te zijn. Als u in plaats daarvan een aangepaste naam gebruikt, gebruikt u dezelfde instructies met de sAMAaccountName van uw connectoraccount in plaats van Cisco_Connector.

Als de Cisco_Connector-gebruiker onvoldoende machtigingen heeft om te werken, toont een AD-connector een waarschuwing of foutstatus in het dashboard en wordt het bericht weergegeven wanneer u over de waarschuwing beweegt, Toegang geweigerd aan een van de geregistreerde domeincontrollers.

Controleer of de Cisco_Connector-gebruiker lid is van de AD-groepen:

- Enterprise Read-only Domain Controllers
- Lezers voor gebeurtenissenlogboeken (alleen als de implementatie virtuele apparaten bevat)

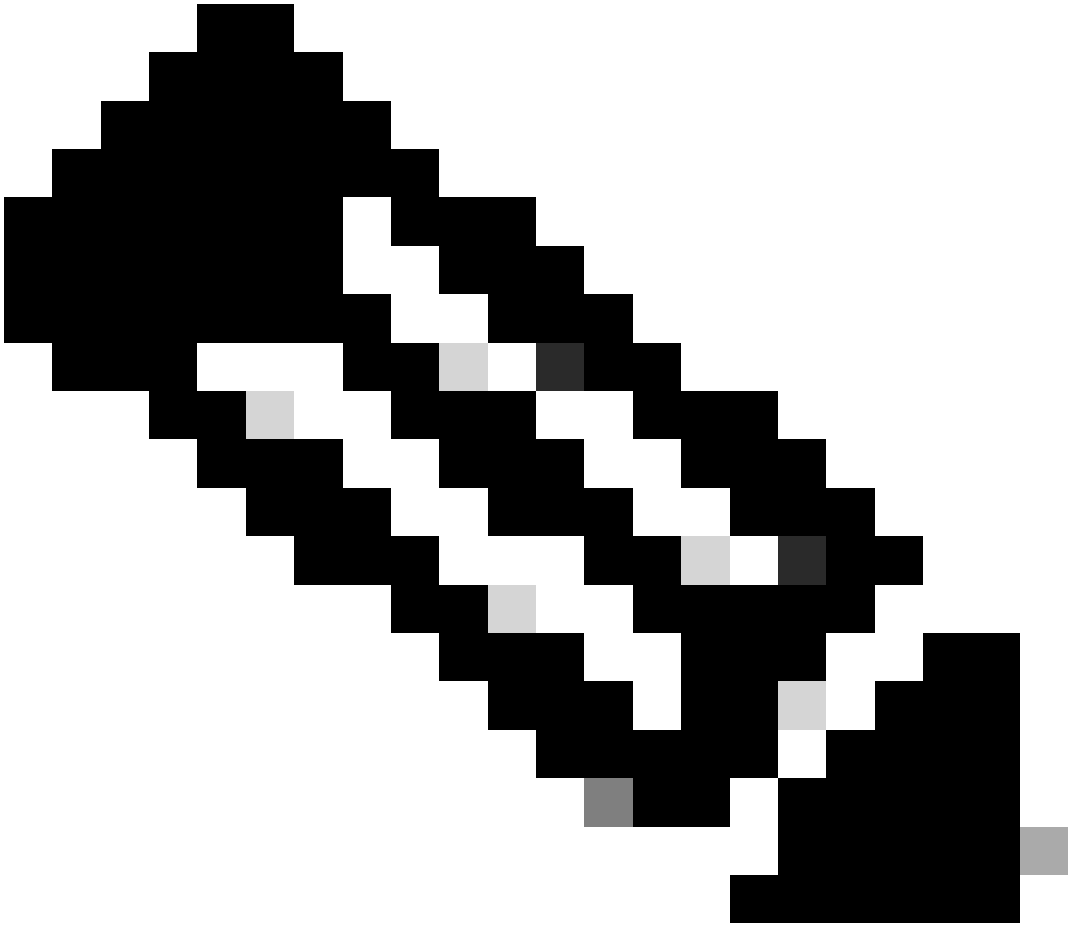
Bovendien moet de Cisco_Connector-gebruiker behoren tot de groepen "Domeingebruikers" en "Gebruikers". U kunt het groepslidmaatschap van de Cisco_Connector-gebruiker verifiëren met de

opdracht:

dsquery-gebruiker -samid Cisco_Connector | dsget-gebruiker -member -expand

De Umbrella AD Connector voert twee primaire taken uit waarvoor deze machtigingen nodig zijn. Ten eerste haalt het LDAP-informatie uit Active Directory om u in staat te stellen beleid te maken op basis van AD-groepen en om AD-gebruikersnamen en -groepsnamen weer te kunnen geven in het overkoepelende dashboard. De machtiging `Directory-wijzigingen repliceren` staat dit toe.

Ten tweede verzamelt het inloggebeurtenissen van domeincontrollers en geeft deze door aan de virtuele apparaten. Hierdoor kunnen de virtuele apparaten hun IP-to-user-mappings maken en zo gebruikers identificeren. Alle machtigingen zijn hierop van toepassing, met uitzondering van de machtiging `Wijzigingen in replicaatdirectory`. Deze machtigingen zijn alleen vereist als de implementatie virtuele apparaten bevat in dezelfde overkoepelende site als de domeincontrollers.



Opmerking: naast het instellen van de vereiste machtigingen voor de Cisco_Connector-gebruiker, registreert het Domain Controller Configuration-script ook een domeincontroller door API-oproepen naar Umbrella uit te voeren. Als u de machtigingen handmatig wijzigt

---

in plaats van het configuratiescript te gebruiken, moet deze registratie ook handmatig worden uitgevoerd. Raadpleeg de overkoepelende documentatie over het handmatig toevoegen van domeincontrollers op het Umbrella-dashboard.

Vereiste machtigingen

- Directory-wijzigingen repliceren
- Gebeurtenislogboeklezers
- Extern beheer
- controlebeleid

Directory-wijzigingen repliceren

Met deze machtiging kan de Cisco_Connector-gebruiker LDAP opvragen. Dit is de vereiste toestemming die doorgaans wordt gegeven met de groep "Enterprise Read-Only Domain Controllers". Dit biedt het Umbrella Dashboard de informatie die nodig is om de namen van AD-objecten weer te geven en om groepslidmaatschappen te bepalen. De connector vraagt om deze attributen:

`cn`: de algemene naam.

`dn` — De voorname naam.

`dNSHostName`—De apparaatnaam zoals deze is geregistreerd in DNS.

`e-mail`: e-mailadressen die aan de gebruiker zijn gekoppeld.

`memberOf`: de groepen waarin de gebruiker is opgenomen.

`objectGUID`: de groepsidentificatie van het object. Deze eigenschap wordt als hash naar Secure Access gestuurd.

`primaryGroupId`: de primaire groep-ID die beschikbaar is voor gebruikers en groepen.

`primaryGroupToken`—Het token voor de primaire groep dat alleen beschikbaar is voor groepen. Wachtwoorden of wachtwoordhashes worden niet opgehaald. Secure Access gebruikt de

`primaryGroupToken`-gegevens in het toegangsbeleid en de configuratie en rapportage. Deze gegevens zijn ook vereist voor elke gebruiker of per-computer filtering.

`sAMAaccountName`—De gebruikersnaam die u gebruikt om u aan te melden bij de Cisco AD Connector.

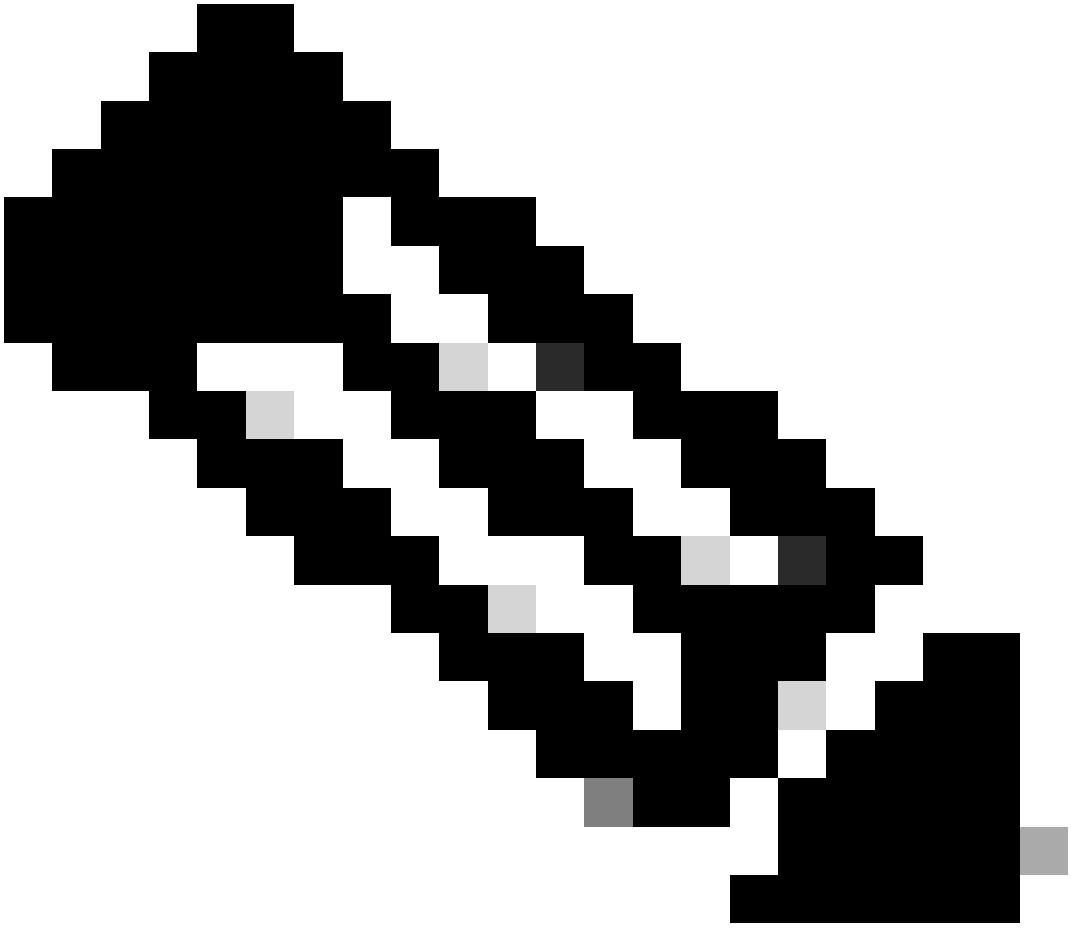
`userPrincipalName`: de hoofdnaam van de gebruiker.

Van deze objectClasses:

```
(&(objectCategory=person)(objectClass=user))
(objectClass=organizationalunit)
(objectClass=computer)
(objectClass=group)
```

De ingebouwde "Enterprise Read-only Domain Controllers"-groep moet deze toestemming geven, en dus moet de Cisco_Connector-gebruiker lid zijn van deze groep. U kunt de machtigingen van de groep verifiëren of de machtigingen specifiek voor de Cisco_Connector-gebruiker opgeven (als de groep deze machtigingen niet levert):

- Open de Active Directory-module Gebruikers en computers
- Klik in het menu Weergave op Geavanceerde functies.
- Klik met de rechtermuisknop op het domeinobject, zoals "company.com", en klik vervolgens op Eigenschappen.
- Selecteer op het tabblad Beveiliging de optie "Enterprise Read-only Domain Controllers" of de gebruiker "Cisco_Connector".
    - Indien nodig kunt u de gebruiker "Cisco_Connector" toevoegen door op "Toevoegen" te klikken.
    - Selecteer in het dialoogvenster Gebruikers, Computers of Groepen selecteren de gewenste gebruikersaccount en klik vervolgens op Toevoegen.
    - Klik op OK om terug te keren naar het dialoogvenster Eigenschappen.
- Klik om de selectievakjes Replicating Directory Changes and Read uit de lijst te selecteren.
- Klik op Toepassen en klik vervolgens op OK.
- Sluit de module.



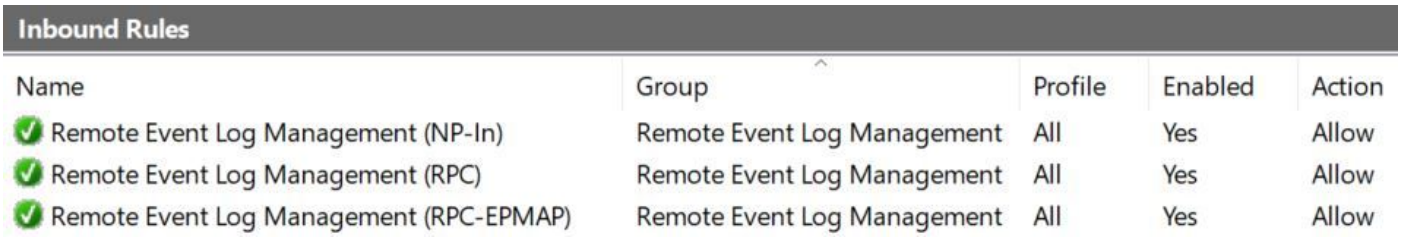
Opmerking: in een bovenliggende/onderliggende domeinscenario bestaat de "Enterprise Read-only Domain Controller" alleen in het bovenliggende domein. In dit geval moeten de machtigingen handmatig worden toegevoegd voor de Cisco_Connector, zoals wordt weergegeven.

Gebeurtenislogboeklezers

Deze wijziging is alleen vereist als de implementatie virtuele apparaten bevat op dezelfde overkoepelende site als de domeincontroller. Lidmaatschap in deze groep stelt de Cisco_Connector-gebruiker in staat om de aanmeldingsgebeurtenissen uit de gebeurtenislogboeken te lezen.

Zorg er op het Domain Controller-systeem in de Windows Advanced Firewall-instellingen voor dat de inkomende regels voor Remote Event Log Management (NP-In, RPC en RPC-EPMAP) zijn toegestaan. De Umbrella AD Connector registreert mogelijk een fout met de melding "De RPC-server is niet beschikbaar" en kan mogelijk aanmeldingsgebeurtenissen niet lezen als deze regels

niet zijn toegestaan.



360090909832

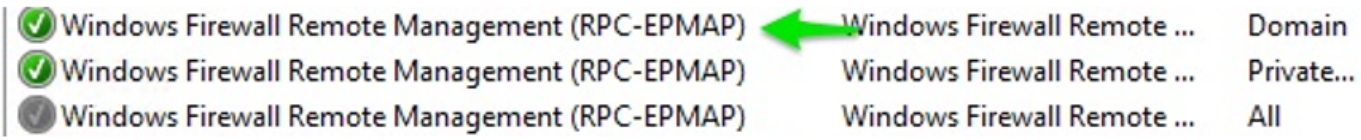
U kunt deze regels ook inschakelen via deze opdracht: netsh advfirewall set rule group="Remote Event Log Management" new enable=yes

Extern beheer

Extern beheer is nodig om de connector in staat te stellen aanmeldingsgebeurtenissen op de domeincontroller te lezen. Deze toestemming is alleen vereist als de implementatie virtuele apparaten bevat op dezelfde overkoepelende site als de domeincontroller.

Voer de volgende opdrachten uit via een opdrachtprompt:

```
netsh advfirewall firewall set rule group="remote administration" new enable=yes
netsh advfirewall set currentprofile settings remotemanagement enable
```



4413613529492

controlebeleid

Deze wijziging is alleen vereist als de implementatie virtuele apparaten bevat op dezelfde overkoepelende site als de domeincontroller. Het auditbeleid definieert welke gebeurtenissen worden vastgelegd in het gebeurtenissenlogboek van de domeincontroller. De Connector vereist dat succesvolle aanmeldingsgebeurtenissen worden geregistreerd, zodat gebruikers kunnen worden toegewezen aan hun IP-adressen.

In normale Windows Server 2008+-omgevingen moet de oude instelling "Aanmeldingsgebeurtenissen voor controle" worden geconfigureerd. Concreet moet het beleid "Aanmeldingsgegevens controleren" worden ingesteld op "Succes". Dit kan worden geverifieerd door deze opdracht uit te voeren op een opdrachtprompt:

```
GPRESULT /z
```

Dit beleid wordt gedefinieerd als een groepsbeleidsobject. Als u het wilt wijzigen, bewerkt u het juiste groepsbeleid voor uw DC (meestal het "Standaardbeleid voor domeincontroller") en stelt u dit beleid in om "Succesgebeurtenissen" op te nemen:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit lo
```

Zorg ervoor dat u het groepsbeleid op de DC bijwerkt nadat u deze wijziging hebt aangebracht.

Windows Server 2008 introduceerde echter ook de Configuratie geavanceerd controlebeleid. Hoewel de bestaande Windows-controlebeleidslijnen nog steeds kunnen worden gebruikt, worden deze genegeerd als een van de geavanceerde controlebeleidslijnen is gedefinieerd. Raadpleeg de documentatie van Microsoft om te begrijpen hoe de twee controlebeleidslijnen op elkaar inwerken.

Voor de toepassing van de Connector, als er Advanced Audit Policies zijn gedefinieerd (inclusief die welke niet specifiek gerelateerd zijn aan aanmelding), dan MOETEN de Advanced Audit Policies worden gebruikt.

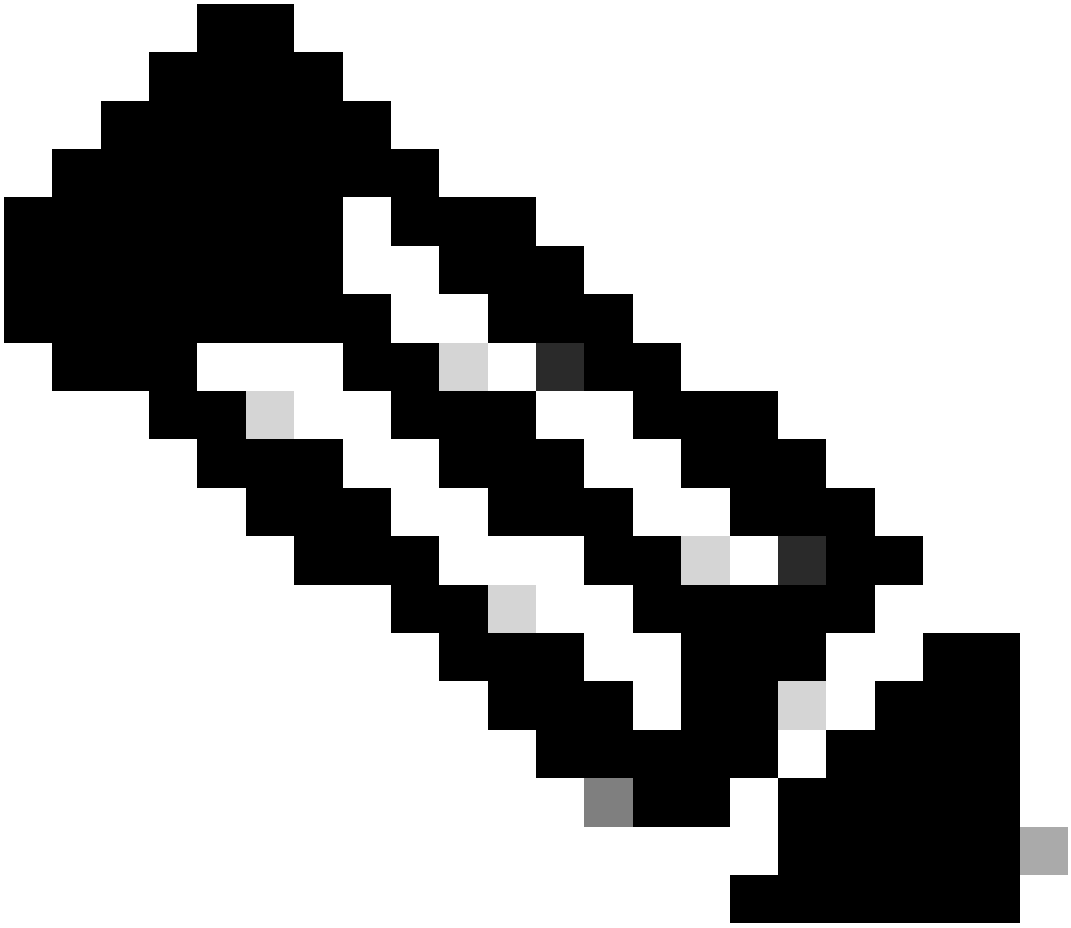
Het geavanceerde controlebeleid moet worden ingesteld voor alle DC's die gebruikmaken van groepsbeleid. Bewerk het juiste groepsbeleid voor uw DC (meestal het "Standaardbeleid voor domeincontroller") en ga naar dit gedeelte:

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\
```

Stel in dat gedeelte het beleid zodanig in dat het zowel 'Succes'- als 'Falen'-gebeurtenissen bevat:

```
Audit Logon
Audit Logoff
Audit Other Logon/Logoff Events
```

Zorg ervoor dat u het groepsbeleid op de DC bijwerkt nadat u deze wijziging hebt aangebracht.



> Opmerking: Als u de AD-connector implementeert met virtuele apparaten, moeten de wijzigingen in de firewallregel en de instellingen van het auditbeleid worden uitgevoerd op alle domeincontrollers in het domein waarmee de connector communiceert.

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

Wanneer u deze informatie aan Support verstrekt, neemt u de uitvoer van deze twee opdrachten op:

```
auditpol.exe /get /category:* > DCNAME_auditpol.txt
GPRESULT /H DC_NAME.htm
```

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.