Windows DC-configuratiescript begrijpen

Inhoud

Inleiding

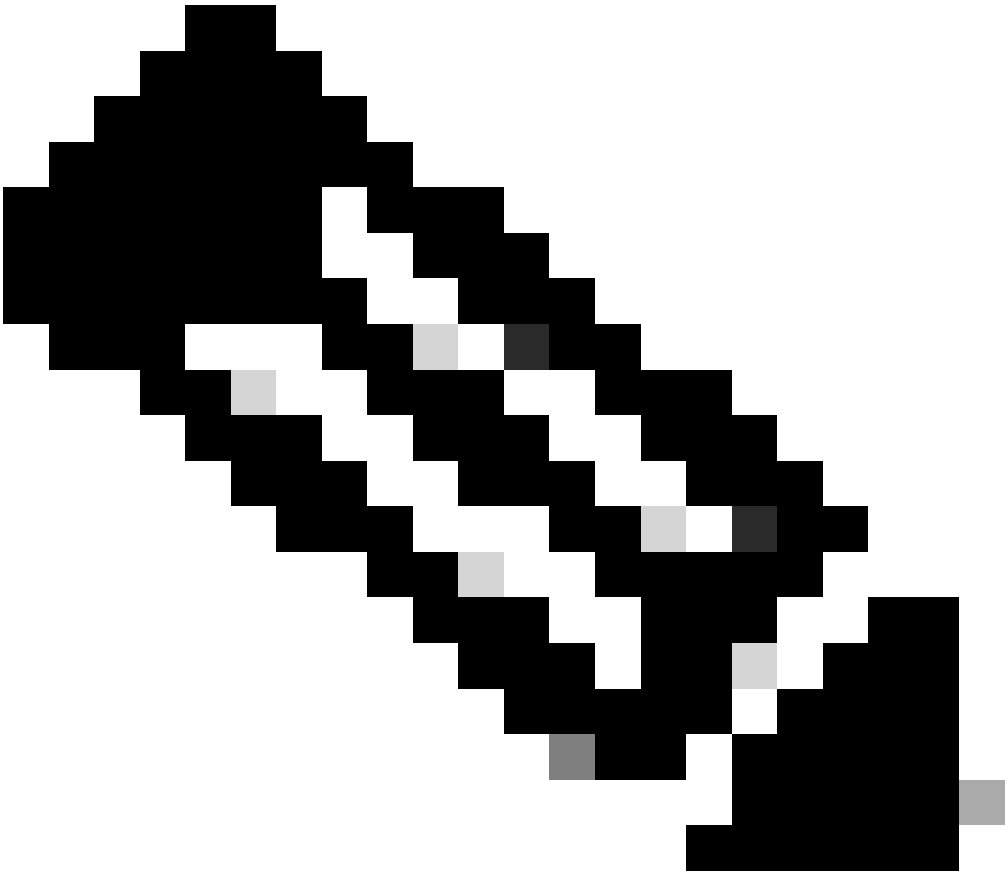
In dit document worden de wijzigingen beschreven die in uw Windows-omgeving zijn aangebracht door ons configuratiescript voor domeincontrollers.

- Voor de basisvereisten zie de Insights documentatie: https://docs.umbrella.com/deployment-umbrella/docs/2-prerequisites
- Zie dit artikel voor gedetailleerde informatie over het handmatig instellen van deze machtigingen: Vereiste rechten voor de OpenDNS_Connector-gebruiker.

Overzicht van DC-configuratiescript

Elke domeincontroller vereist een eenmalige registratie bij de Umbrella API/Dashboard. Ons DC-configuratiescript initieert dit samen met deze functies:

1. Controleer of de benodigde machtigingen en firewallregels zijn geconfigureerd
2. (Optioneel) Deze machtigingen automatisch configureren
3. (Optioneel) Registreer de Domeincontroller met de Umbrella API/Dashboard, alleen als deze controles zijn geslaagd.



Opmerking: Een lijst met domeincontrollers kan ook handmatig worden geregistreerd door Umbrella-ondersteuning. Dit is meestal handig in scenario's waarbij de API / internettoegang niet mogelijk is voor de domeincontroller. De beschreven machtigingswijzigingen MOETEN echter nog steeds worden geconfigureerd, dus we raden nog steeds sterk aan om het configuratiescript uit te voeren.

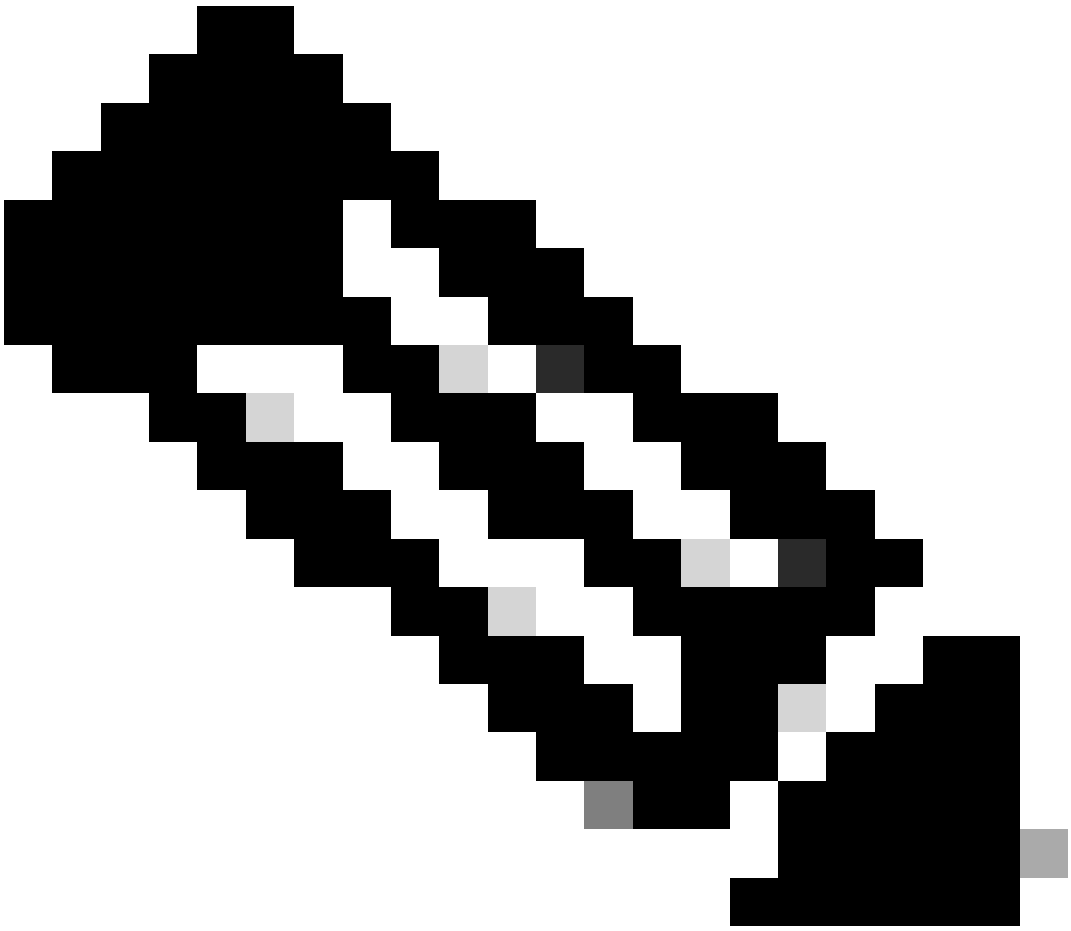
Wanneer het script in eerste instantie wordt uitgevoerd, worden er geen wijzigingen aangebracht in de omgeving. Het script controleert of alle benodigde machtigingen aanwezig zijn. Als er een probleem is, wordt u gevraagd `(Y/N)` maar voor het aanbrengen van wijzigingen.

Zodra het registratiescript is voltooid, is er geen software nodig om op de domeincontroller zelf te draaien. De OpenDNS Connector-service moet echter op ten minste één computer zijn geïnstalleerd (bijv. Domeincontroller of Ledenserver).

Fase 1 - Tests

Het script verzamelt in eerste instantie deze informatie:

- Controleert de versie van het besturingssysteem en het functieniveau van het forest
- Controleert of het script wordt uitgevoerd als beheerder.
- Hiermee worden het IP-adres, de hostnaam en de domeinnaam van de server opgehaald
- Controleer of Windows Firewall is ingeschakeld en of de ingebouwde regel 'Extern beheer' is toegestaan
- Controleert op de vereiste domeingebruikersaccount 'OpenDNS_Connector'



Opmerking: Als de OpenDNS_Connector-gebruiker niet bestaat, worden de resultaten afgedrukt en afgebroken. Deze domeingebruiker moet handmatig worden gemaakt voordat het script wordt uitgevoerd. Als de OpenDNS_Connector-account bestaat, gaat het script verder met deze controles.

- Controleert of de OpenDNS_Connector-gebruiker rechten heeft voor 'Extern inschakelen' en 'Leesbeveiliging' in de root\cimv2 WMI-naamruimte.
- Controleert of de OpenDNS_Connector-account de Active Directory 'Replicating Directory

Changes' machtiging heeft, die normaal wordt verleend door lidmaatschap van de Enterprise Read-Only Domain Controllers-groep.
- Controleert of de OpenDNS_Connector-account lid is van de groep 'Event Log Readers'
- Controleert of de OpenDNS_Connector-account lid is van de groep 'Distributed COM Users'
- Controleert de resulterende set van beleid (RSOP) om te zien of 'Audit Logon Events' is ingeschakeld via groepsbeleid
- Controleert de resulterende set van beleid (RSOP) om te zien of de OpenDNS_Connector-account het recht heeft om het 'audit- en beveiligingslogboek beheren' toe te kennen

Fase 1b - Testresultaten

De resultaten die door het configuratiescript worden afgedrukt, verschillen afhankelijk van de versie van het besturingssysteem.

Op server 2003 en nieuwer ziet u de volgende resultaten:

```
AD User Exists:                true/false
WMI Permissions Set:           true/false
DCOM Permissions Set:          true/false
RDC Permissions Set:           true/false
Audit Policy Set:              true/false
Manage Event Log Policy Set:   true/false
Distributed COM MemberOf:      true/false
```

Op Server 2008 en nieuwer (alleen wanneer het functionele niveau van het forest 2008+ is) wordt deze informatie ook weergegeven. (Deze groep bestaat niet in eerdere versies):

```
Event Log Readers MemberOf:     true/false
```

Fase 2 - Automatische configuratiewijzigingen

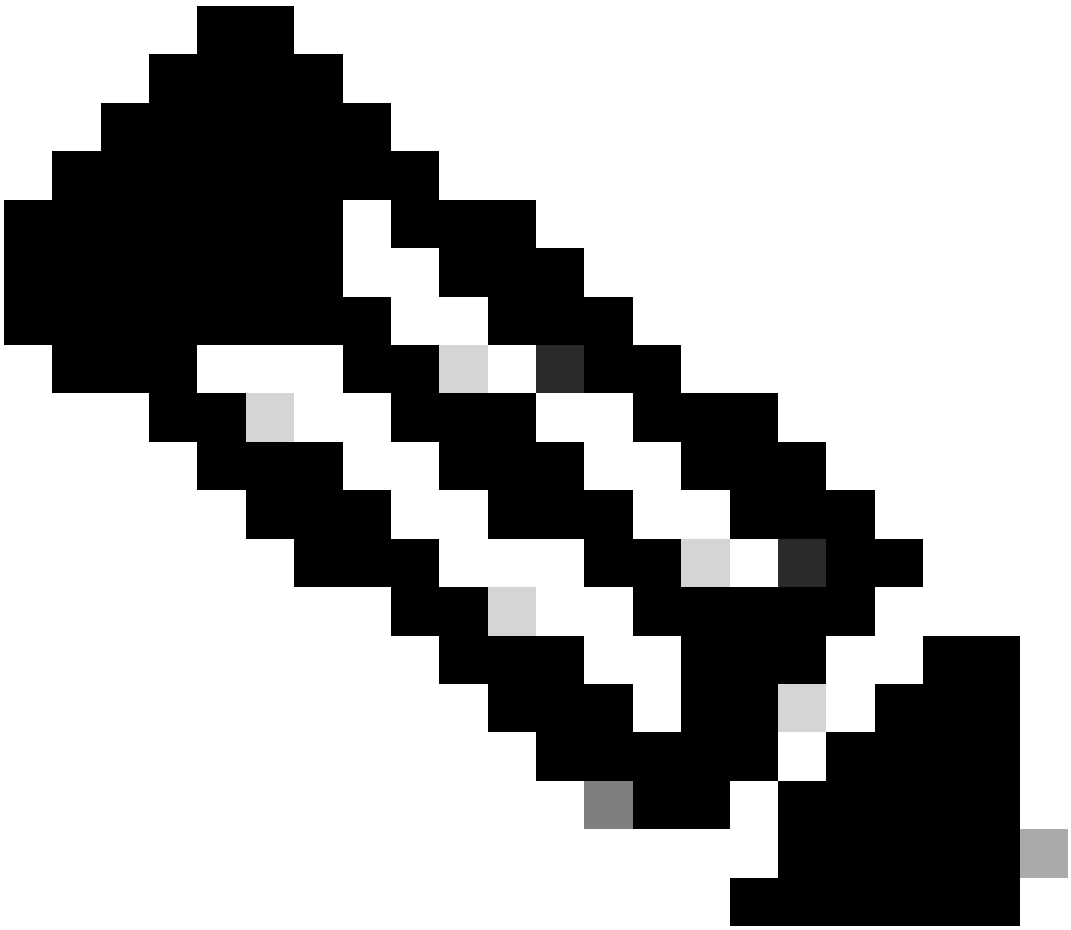
Als deze controles mislukken, wordt u gevraagd `"Wilt u dat we deze domeincontroller (y of n) automatisch configureren?"` voordat u wijzigingen aanbrengt.

Deze wijzigingen worden aangebracht:

- Schakelt indien nodig de ingebouwde Windows Firewall-regel 'Extern beheer' in
- De 'OpenDNS_Connector'-account 'Remote Enable' en 'Read Security'-machtigingen in de root\cimv2 WMI-naamruimte worden expliciet toegekend.
- Verleent expliciet de 'OpenDNS_Connector'-account 'Replicating Directory Changes' rechten
- Voegt de account 'OpenDNS_Connector' toe aan de groep 'Distributed COM users'

In 2008+ wordt deze wijziging ook doorgevoerd:

- Voegt de 'OpenDNS_Connector'-account toe aan de groep 'Gebeurtenisloglezers'



> Opmerking: Als de automatische configuratie wordt geweigerd of als deze wijzigingen mislukken, wordt het script niet geregistreerd.

Fase 2b - Waarschuwingen voor automatische configuratie

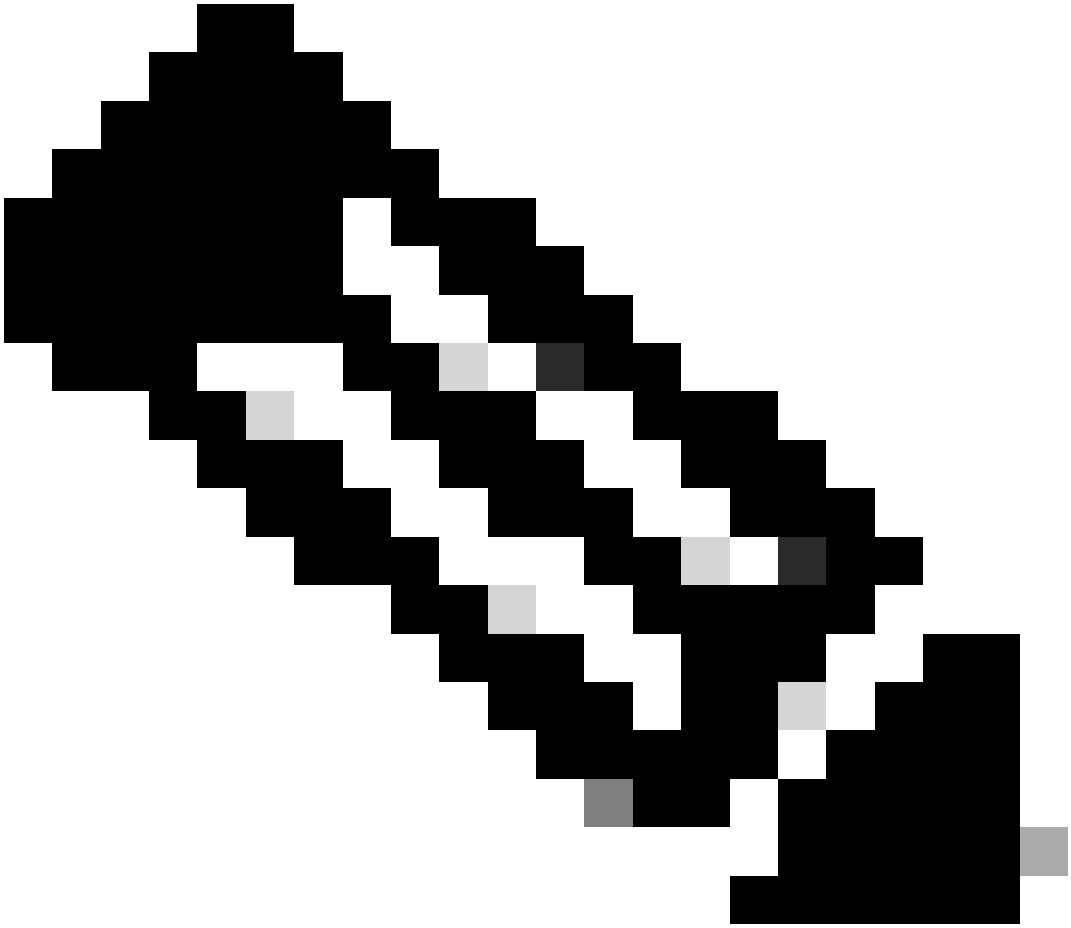
Het script produceert waarschuwingen als de instellingen voor Groepsbeleid niet correct zijn geconfigureerd. Het script kan deze problemen niet verhelpen.

Alle besturingssystemen:

- Het script WAARSCHUWT als de instelling 'Aanmeldingsgebeurtenissen controleren' niet correct is geconfigureerd in Groepsbeleid, maar Groepsbeleid niet wijzigt.

In 2003 (en 2003 op functioneel niveau):

- Het script WAARSCHUWT als het recht 'Beheren auditing en beveiligingslog' niet correct is geconfigureerd in Groepsbeleid, maar het Groepsbeleid niet wijzigt.



Opmerking: corrigeer deze problemen handmatig en voer het configuratiescript opnieuw uit. Het script gaat niet verder met de registratie totdat deze zijn gecorrigeerd.

Fase 3 - Registratie

Het script vraagt voordat u de domeincontroller registreert bij Umbrella "`Wilt u deze domeincontroller (y of n) registreren?`". Deze informatie wordt naar Umbrella verzonden:

- Domeincontroller Hostname / Label
- domeinnaam
- IP-adres
- Uw unieke organisatie-ID en token (opgenomen in uw script) om de DC uniek te identificeren met uw overkoepelende organisatie.

De registratie gebeurt veilig via https://api.opendns.com

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.