Gebruikers, groepen en computers configureren van Active Directory naar Sync met OpenDNS Connector Service

Inhoud

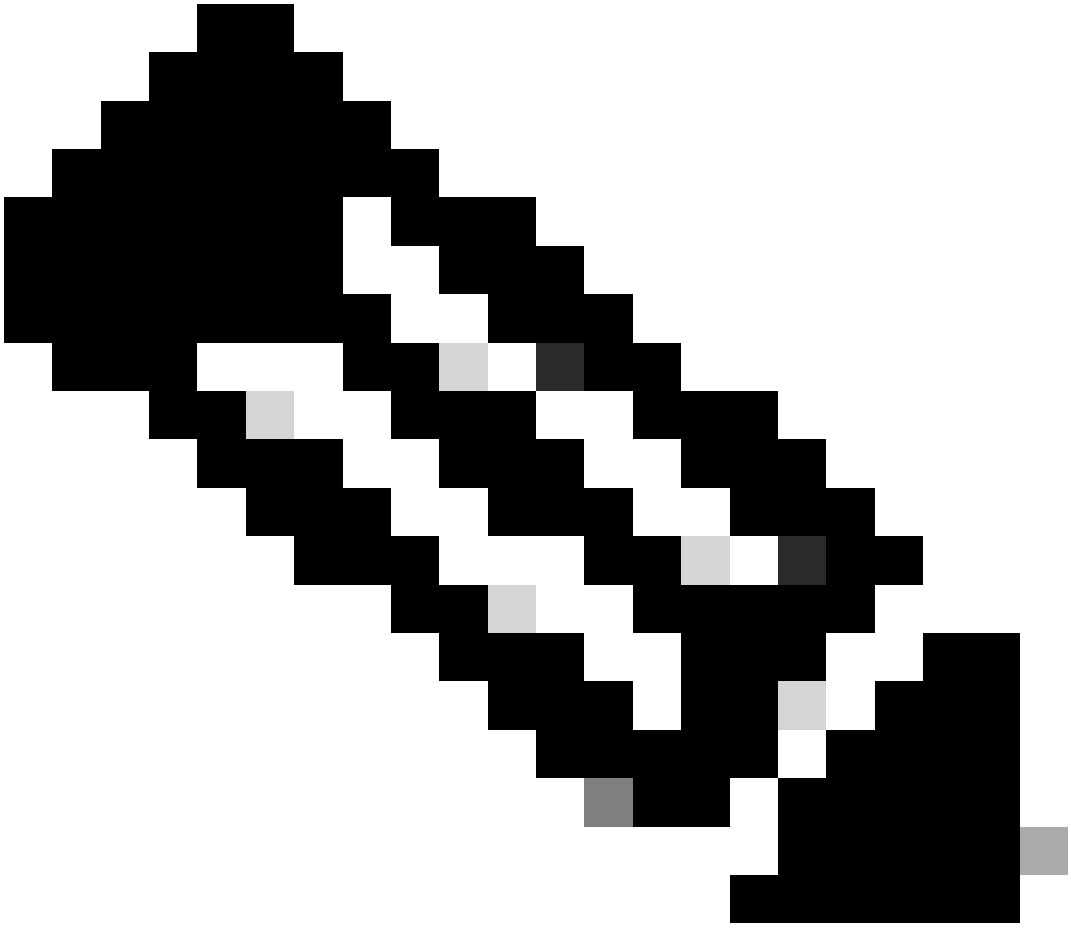
Inleiding

In dit document wordt beschreven hoe gebruikers, groepen en computers vanuit Active Directory kunnen worden gesynchroniseerd met de OpenDNS Connector-service.

Overzicht

Als onderdeel van de werking synchroniseert de OpenDNS Connector-service een lijst met gebruikers, groepen en computers uit Active Directory met behulp van het LDAP-protocol. In dit artikel wordt beschreven hoe u kunt controleren of de OpenDNS_Connector-account de juiste machtigingen heeft om die objecten te lezen.

Aan elk object (gebruikers/groepen/computers) in Active Directory zijn ACL-beveiligingsmachtigingen gekoppeld en elk object moet de gebruikersaccount van OpenDNS_Connector toestaan de kenmerken ervan te lezen.



Opmerking: In dit artikel wordt ervan uitgegaan dat de normale voorwaarden voor de 'OpenDNS_Connector'-account al zijn gecontroleerd. Als AD-gebruikers/groepen ontbreken in het Dashboard, raadpleeg dan eerst dit artikel: AD-gebruikers/groepen ontbreken in het Umbrella Dashboard.

Standaardmachtigingen

Standaard kunnen alle geverifieerde gebruikers de eigenschappen van gebruikers/groepen/computers lezen, zodat de OpenDNS_Connector-gebruiker geen extra machtigingen nodig heeft om de LDAP-synchronisatie uit te voeren.

De standaardmachtigingen worden gewoonlijk als volgt ingesteld:

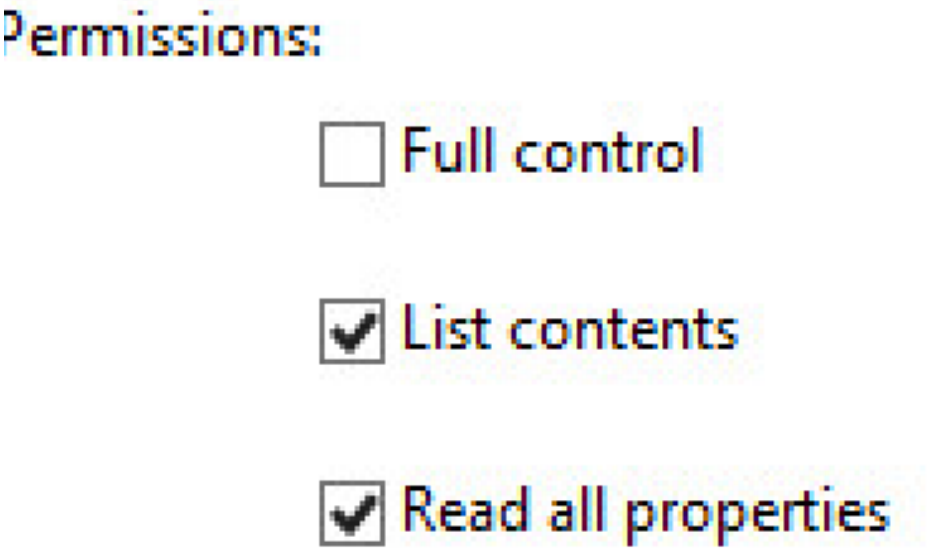
1) De groep 'Pre-Windows 2000 Compatible Access' krijgt leesrechten (lees alle eigenschappen) op het domein voor 'Descendant User Objects', 'Descendant Group Objects' en 'Descendant Computer Objects'.

U kunt dit als volgt controleren:

- Open Active Directory-gebruikers en -computers
- Klik op 'Bekijken' en selecteer de optie 'Geavanceerde functies'.
- Klik met de rechtermuisknop op het object Domain en selecteer 'Properties' en vervolgens 'Security > Advanced'
- Selecteer de 'Pre Windows 2000 Compatible Access' vermelding met 'Special' rechten:

115011616667

- Klik op 'Bewerken' om deze machtigingen in detail te bekijken.
- Selecteer 'Descendant User objects' in het gedeelte Toepassen op
- Kijk voor deze permissies:

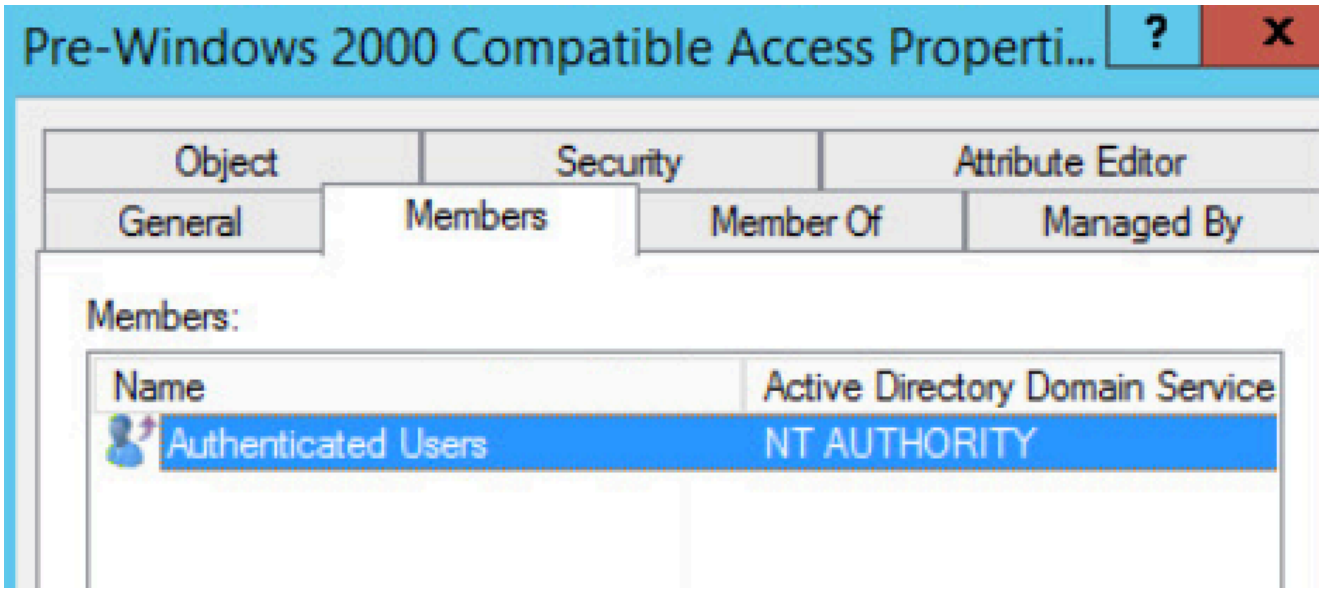


115011616687

- Herhaal deze stappen voor 'Descendant Group-objecten' en 'Descendant Computer-objecten'

2) De groep 'Alle geverifieerde gebruikers' is lid van de groep 'Pre-Windows 2000 Compatible Access' die deze instellingen aan alle gebruikers biedt.

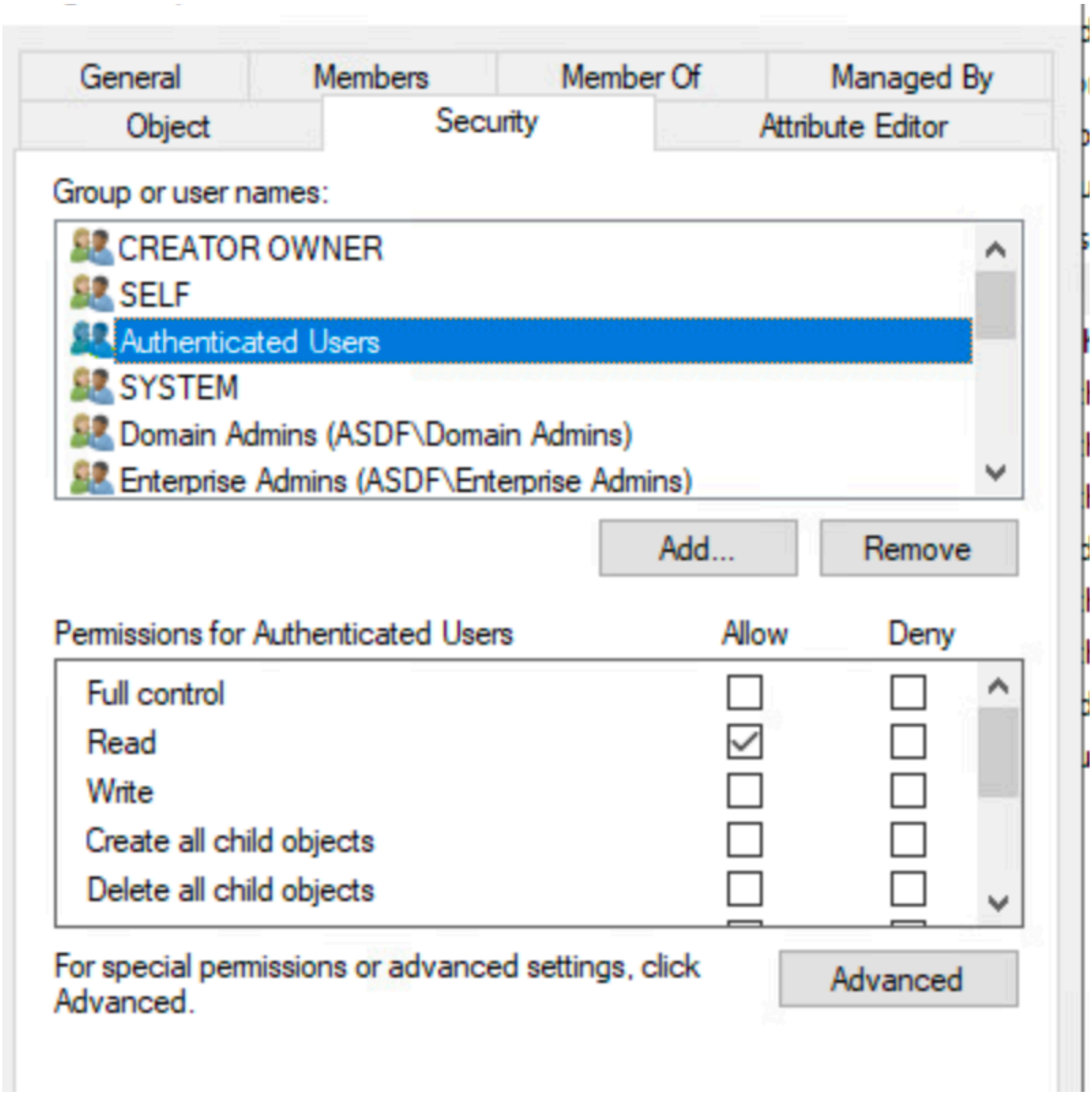
- Klik met de rechtermuisknop op de groep Pre-Windows 2000 Compatible Access, die zich normaal gesproken in de AD-container van Building bevindt.
- Selecteer 'Eigenschappen' en ga naar het tabblad 'Leden'.
- Controleer of 'Geverifieerde gebruikers' wordt vermeld.



115011616707

In sommige AD-omgevingen kan dit machtigingsmodel echter zijn gewijzigd en zijn geverifieerde gebruikers verwijderd. Dit kan zich manifesteren als sommige gebruikers ontbreken in het Umbrella Dashboard, of als groepslidmaatschappen onjuist zijn. Als dit het geval is, voegt u de OpenDNS_Connector-gebruiker toe aan deze groep, start u de connectorservice opnieuw op en worden de ontbrekende items weergegeven in Paraplu.

In sommige zeldzame gevallen wordt het probleem nog steeds niet aangepakt. Als u dit het geval vindt, controleert u het tabblad Groepen beveiliging in Active Directory en zorgt u ervoor dat u hier geverifieerde gebruikers ziet met een inchecktoegang. Als dit niet is ingeschakeld, schakelt u het uit en start u de connectorservice opnieuw om te zien of de groepsleden worden weergegeven. Bovendien, als ze vinden dat deze beveiligingsinstelling ontbreekt in alle groepen, moeten ze de wijzigingen toepassen op alle groepen wereldwijd in bulk.



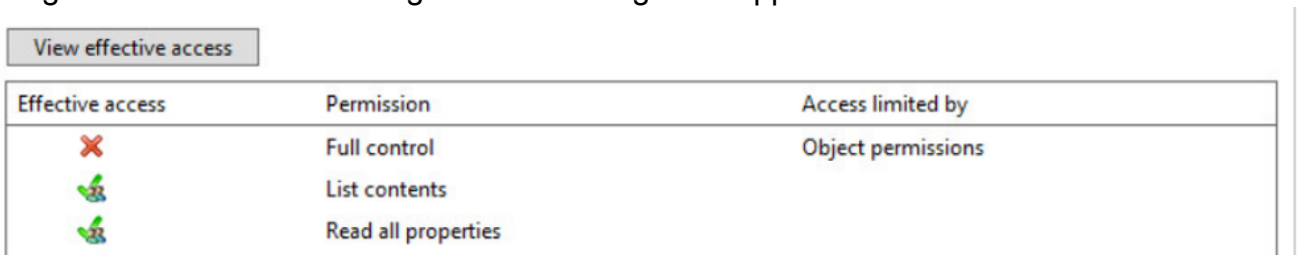
28728163336852

Effectieve toegang bekijken

U kunt de tool Windows 'Effectieve toegang' gebruiken om te zien of de OpenDNS_Connector-gebruiker een bepaald object kan lezen dat ontbreekt (of dat een onjuist groepslidmaatschap heeft).

- Open Active Directory-gebruikers en -computers
- Klik op 'Bekijken' en selecteer de optie 'Geavanceerde functies'.
- Zoek het gebruikersobject en klik met de rechtermuisknop om 'Eigenschappen' te selecteren

- Ga naar 'Beveiliging > Geavanceerd > Effectieve toegang' (dit kan zeggen 'Effectieve machtigingen')
- Klik op 'Selecteer een gebruiker' en selecteer vervolgens de gebruikersaccount 'OpenDNS_Connector'.
- Klik op 'OK' en vervolgens op 'Effectieve toegang bekijken'
- Zorg ervoor dat de connectorgebruiker alle eigenschappen kan lezen:

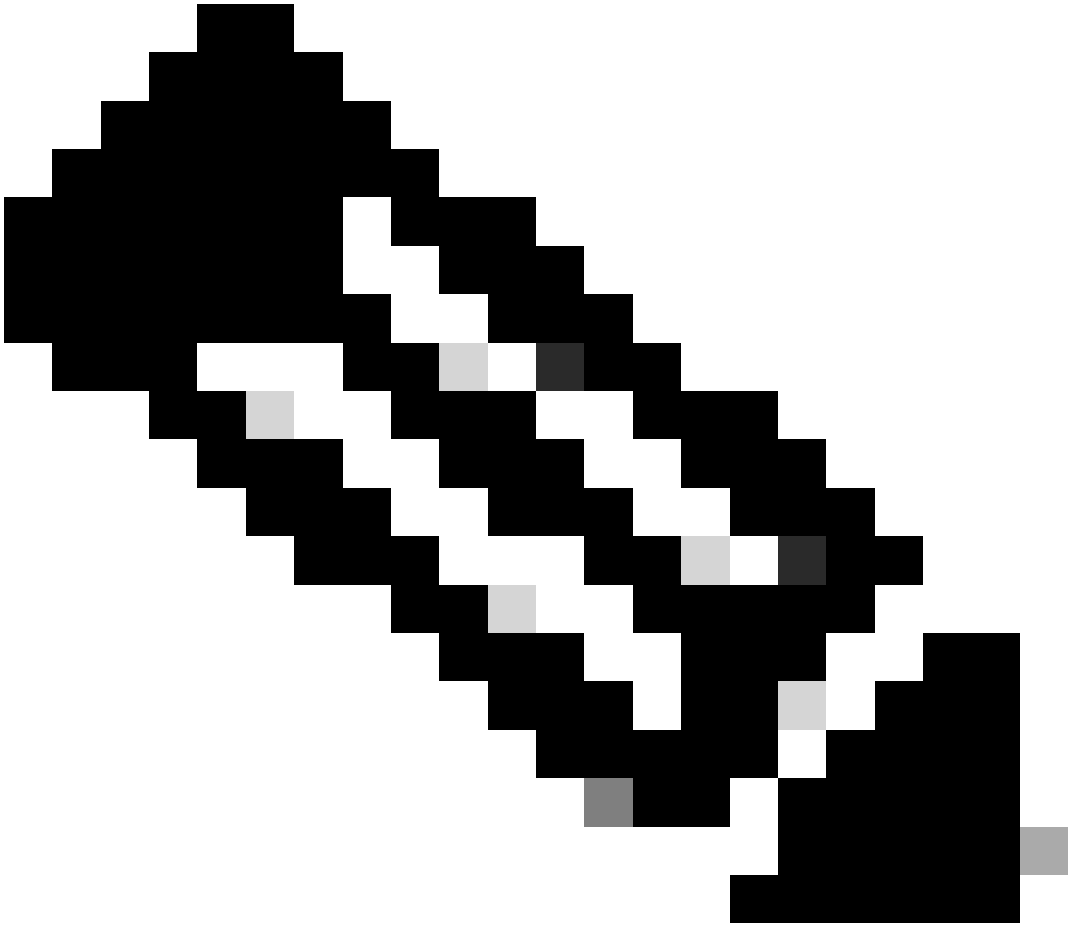


115011616727

OpenDNS_Connector LDAP-machtigingen instellen

De 'Delegate Control' wizard in AD is een snelle manier om de benodigde rechten toe te wijzen aan de 'OpenDNS_Connector' gebruiker:

1) Ga naar Systeembeheer en open de Active Directory Users and Computers snap-in.
2) Klik met de rechtermuisknop op het domein dat de OpenDNS_Connector bevat en selecteer "Beheer delegeren..." en klik vervolgens op Volgende.
3) Voeg de OpenDNS_Connector-gebruiker toe en klik op Volgende.
4) Selecteer "Alle gebruikersinformatie lezen" en klik op Volgende. [Zie afbeelding 3.]
7) Klik op Voltooien. [Zie afbeelding 6.]



Opmerking: deze stappen kunnen mislukken als overerving op sommige objecten is uitgeschakeld. Voor die objecten moet u de machtigingen handmatig instellen.

userPerms-script

Het bijgevoegde powershell-script is een andere methode om de rechten van een specifiek object (bijv. gebruiker) in AD te krijgen. Voeg de uitvoer van dit script toe wanneer u contact opneemt met Umbrella Technical support.

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.