Begrijp parapluversleuteling voor AD Sync

Inhoud

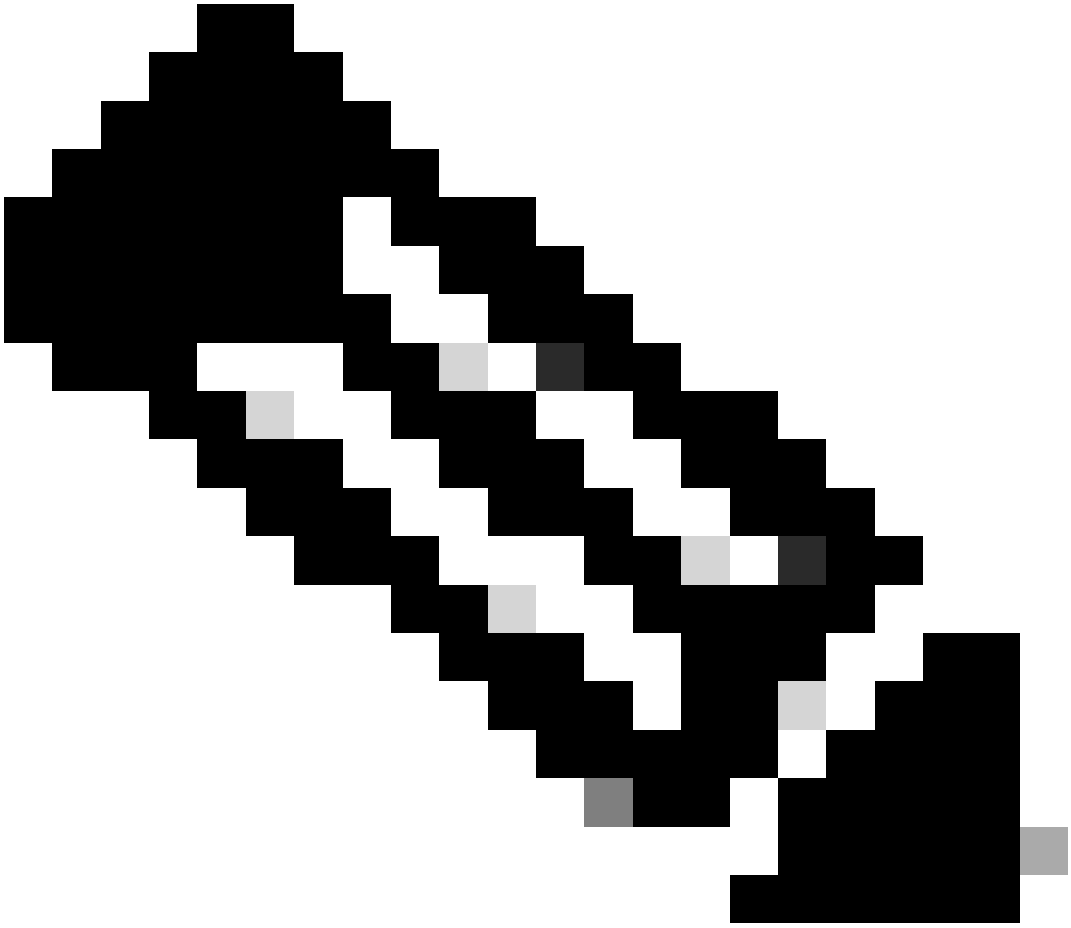
Inleiding

Dit document beschrijft Umbrella-codering voor AD-synchronisatie, zoals de manier waarop deze gegevensoverdracht wordt gecodeerd.

Achtergrondinformatie

De Umbrella AD Connector-software haalt details van gebruikers-, computer- en groepsinformatie op van uw AD Domain Controller met behulp van LDAP. Van elk object worden alleen de benodigde attributen opgeslagen, waaronder sAMAaccountName, dn, userPrincipalName, memberOf, objectGUID, primaryGroupId (voor gebruikers en computers), en primaryGroupToken (voor groepen).

Deze gegevens worden vervolgens geüpload naar Umbrella voor gebruik in Beleidsconfiguratie en Rapportage. Deze gegevens zijn ook vereist voor filtering per gebruiker of per computer.



Opmerking: objectGUID wordt in gehashte vorm verzonden.

Om erachter te komen wat er precies wordt gesynchroniseerd, kunt u kijken naar de .ldif-bestanden in:

```
C:\Program Files\OpenDNS\OpenDNS Connector\ADSync\*.ldif
```

In dit artikel wordt beschreven hoe deze gegevensoverdracht wordt gecodeerd.

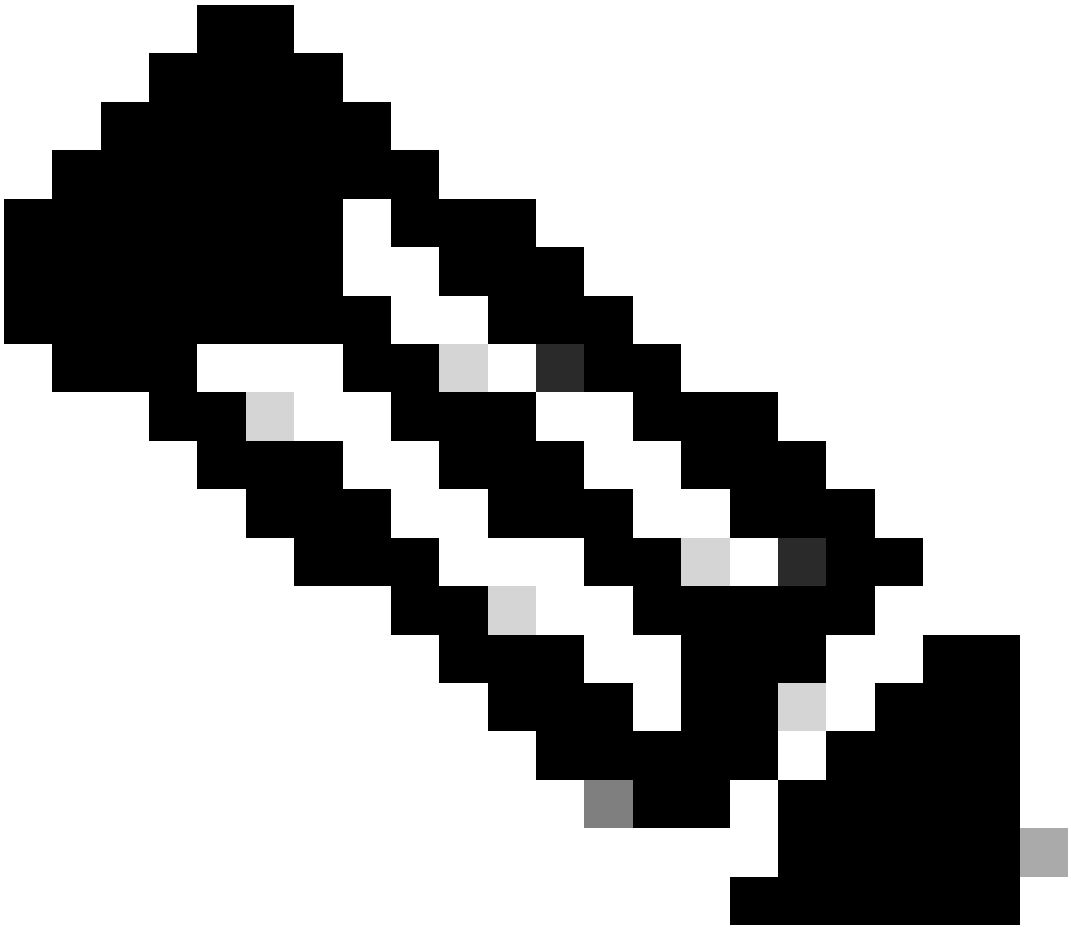
Encryptie voor AD Data Upload

De Umbrella AD Connector uploadt de AD-informatie naar Umbrella met behulp van een beveiligde HTTPS-verbinding. De upload tussen de Connector **<>** Umbrella cloud wordt altijd gecodeerd.

Encryptie voor het ophalen van AD-gegevens

Vanaf v1.1.22 probeert de Connector nu gebruikersgegevens op te halen met codering tussen Domain Controller <> Connector. Er worden twee methoden geprobeerd:

- LDAPS. Gegevens worden via een beveiligde tunnel verzonden.
- LDAP met Kerberos-verificatie. Biedt codering op pakketniveau.



> Opmerking: LDAPS wordt niet gebruikt wanneer de Connector-software wordt uitgevoerd op dezelfde server als de Domain Controller die wordt gebruikt voor ADsync.

Als deze poging om welke reden dan ook mislukt, keert het terug naar dit mechanisme:

- LDAP met NTLM-verificatie. Dit zorgt voor veilige verificatie, maar de gegevensoverdracht tussen de DC > Connector gebeurt zonder codering.

Om ervoor te zorgen dat encryptie mogelijk is, raden we aan om:

- Schakel LDAPS in op uw domeincontroller(s). Dit valt buiten het bereik van Umbrella-ondersteuning, maar kan worden ingeschakeld met de documentatie van Microsoft.
- Zorg ervoor dat de hostnaam van uw domeincontroller(s) correct is geconfigureerd in 'Implementaties > Sites en AD'. De juiste hostnaam is vereist voor beide coderingsmethoden. Als de hostnaam om welke reden dan ook onjuist is, raden we aan de domeincontroller opnieuw te registreren met behulp van ons configuratiescript of contact op te nemen met Umbrella Support.

Bevestigen dat encryptie plaatsvindt. U kunt het logbestand hier bekijken:

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\OpenDNSAuditClient.log
```

Tijdens AD-synchronisatie ziet u logboekvermeldingen zoals:

LDAPS-verbinding geslaagd:
SSL gebruiken voor <SERVER>-communicatie om het DN op te halen.

Verificatie van Kerberos geslaagd:
Kerberos gebruiken voor <SERVER>-communicatie om het DN op te halen.

NTLM-failbackmechanisme in gebruik:
Kerberos is mislukt voor DC Host <SERVER>. De hostnaam kan ongeldig zijn. Terug naar de NTLM-query.

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.