Waarom kan ik geen AD-groepen voor vertrouwde domeinen vinden terwijl ik een Directory-zoekopdracht uitvoert in toegangsbeleid?

Inhoud

Vraag:

Waarom kan ik geen AD-groepen voor vertrouwde domeinen vinden terwijl ik een Directory-zoekopdracht uitvoert in toegangsbeleid?

Milieu: Cisco Web Security Appliance (WSA), NTSL-verificatie, Trusted Domains

Symptomen:

- Gebruiker probeert een "Active Directory Group" op te zoeken om als Policy Member Definition te gebruiken in een van zijn Access Policies en de groep wordt niet weergegeven in de Directory Search.
- De groep behoort tot een betrouwbaar AD-domein en niet tot het domein waartoe de WSA is toegetreden.

Dit gedrag is van opzet. Tijdens het configureren van groepen in toegangsbeleid, zullen de groepen van vertrouwde domeinen niet verschijnen in de Directory Search.

Op alle versies van AsyncOS heeft WSA de mogelijkheid om gebruikers van een ander domein te authenticeren en hun respectievelijke AD-groepen te matchen als het andere domein een bidirectioneel vertrouwen heeft met het domein dat door WSA is verbonden.

In een dergelijk scenario kunnen we de groepen van een betrouwbaar domein in toegangsbeleid toevoegen met behulp van de volgende stappen:

1. Bladeren naar GUI —> Web Security Manager —> Toegangsbeleid —> <Beleidsnaam> —> Geselecteerde groepen en gebruikers —> Groepen
2. Typ handmatig de volledige groepsnaam, samen met de domeinnaam, in het veld 'Directory Search'
3. Klik op de knop "Toevoegen"
4. Klik op Gereed en voer vervolgens de wijzigingen in

Merk op dat de WSA niet zal overeenkomen met de handmatig ingestelde groepen als het andere

domein geen 2-weg vertrouwensrelatie heeft met het domein dat door WSA is verbonden

Opmerking: Op AsyncOS versies 7.7 en hoger, WSA ondersteunt meerdere NTLM-domeinen en voor scenario's waar er geen vertrouwensrelatie is tussen de 2 domeinen, kunnen we een nieuw NTLM-domein voor het tweede domein creëren. Met meerdere NTLM-domeinen kan WSA opzoekgroepen van verschillende domeinen binnen het toegangsbeleid.

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.