Problemen met de synchronisatie van de AD-connector voor beveiligde toegang oplossen

Inhoud

uitgifte

De AD Connector die op een domeincontroller is geïnstalleerd, synchroniseert niet goed met Cisco Secure Access. De connector ondervindt meerdere synchronisatiefouten, waaronder:

- Fouten in de Delta-synchronisatie met "Access is denied"-fouten (COMEexception 0x80070005).
- DC-gebeurtenislogboekfouten lezen met "Unauthorized AccessException: Poging om een ongeoorloofde bewerking uit te voeren".
- Problemen met cloudregistratie die "Ongeldig URI-formaat" weergeven bij het downloaden van het manifest.
- HTTP 404 "object_not_found"-fouten voor specifieke AssetID tijdens synchronisatiepogingen.

De connector lijkt connectiviteit te hebben met de Cisco Secure Access-cloudservice, maar faalt aan zowel de Active Directory-machtigingen als de cloudregistratieconfiguratie.

milieu

- Cisco Secure Access met AD-connector
- AD Connector versie 1.15.2
- AD Connector geïnstalleerd op domeincontroller
- Aangepaste serviceaccount (svcCiscoUmbrella) in plaats van standaard Cisco_Connector-account
- Instelling van test-/pilootomgeving

resolutie

De oplossing omvatte het aanpakken van zowel Active Directory-machtigingsproblemen als cloudregistratieproblemen door middel van een volledig herinstallatieproces:

Stap 1: Bestaande AD-connectorvermeldingen verifiëren en reinigen

Controleer in het Dashboard voor beveiligde toegang de invoer voor AD Connector voor de host en verwijder eventuele verouderde of dubbele vermeldingen voor dezelfde server indien aanwezig.

Stap 2: Zorg voor volledige verwijdering

Verwijder de bestaande AD Connector-service volledig om er zeker van te zijn dat er geen resterende configuratie overblijft die registratieproblemen kan veroorzaken.

Stap 3: Voer domeincontrollerscripts uit

Voordat u de connector opnieuw installeert, voert u de juiste domeincontrollerconfiguratiescripts uit om ervoor te zorgen dat de juiste machtigingen zijn ingesteld. Het script moet worden uitgevoerd op elke toepasselijke domeincontroller, hoewel de connector zelf buiten de domeincontroller kan verblijven op een andere domeingekoppelde computer.

Stap 4: Serviceaccountmachtigingen configureren

Geef de vereiste Active Directory-machtigingen aan de serviceaccount:

- AD-synchronisatiebevoegdheden (domein/hoofdbereik, indien van toepassing):
    - lezen

    - Wijzigingen in directory's repliceren
    - Directory repliceren Alles wijzigen (indien vereist in de omgeving)
    - Wijzigingen in directorys in gefilterde set repliceren (indien vereist in de omgeving)
- Toegang tot het eventlogboek op de domeincontroller:
    - Voeg de serviceaccount toe aan de groep Lezers van het eventlogboek.
    - Zorg voor gelijkwaardige, op beleid gebaseerde toestemming om het beveiligingslogboek te lezen.

Stap 5: AD Connector opnieuw installeren

Installeer de AD Connector-service opnieuw om een nieuw manifest en geldige AssetID te genereren, zodat u de juiste cloudregistratie kunt garanderen.

Stap 6: Opnieuw opstarten en valideren

Na installatie en rechtenconfiguratie:

1. Start de AD Connector-service opnieuw op.
2. Bewaak de aansluitlogs om te bevestigen dat de toegang is geweigerd en dat fouten door onbevoegden zijn gestopt.
3. Controleer of de synchronisatievermeldingen in de logboeken zijn weergegeven (bijvoorbeeld "ADSync LDIF RESPONSE: 200 Success").

Oorzaak

De synchronisatieproblemen werden veroorzaakt door twee primaire factoren:

1. Onvoldoende Active Directory-machtigingen: De aangepaste serviceaccount (svcCiscoUmbrella) beschikte niet over de vereiste AD-machtigingen voor deltasynchronisatie en DC-gebeurtenislogtoegang, wat resulteerde in "Access is denied" en

"Unauthorized AccessException"-fouten.
2. Problemen met cloudregistratie: de connectorinstantie is verkeerd geregistreerd of wijst naar een ongeldige/oude AssetID, waardoor fouten in het "Ongeldige URI-formaat" ontstaan bij het downloaden van het manifest en fouten in het "object_not_found" van HTTP 404 tijdens synchronisatiepogingen.

Deze problemen werden verergerd door onvolledige installatieprocedures waarbij de configuratiescripts van de domeincontroller niet goed werden uitgevoerd voordat de connector werd geïnstalleerd.

Gerelateerde inhoud

- Configuratie van Cisco Secure Access AD Connector
- Vereisten voor machtigingen AD-connector
- Installatiehandleiding AD-connector
- Problemen met AD-connector oplossen
- Configuratie serviceaccount AD Connector
- Cisco Technical Support en downloads

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.