Cisco Secure Access Identity Synchronization met Active Directory en Microsoft EntraID

Inhoud

uitgeven

Gebruikers ondervonden problemen bij het aanbieden van gebruikers en groepen uit twee identiteitsbronnen met dezelfde domeinnaam in Cisco Secure Access. Het specifieke scenario betrof het synchroniseren van identiteiten van zowel on-premises Active Directory als Microsoft EntraID (voorheen Azure AD) waar beide bronnen dezelfde domeinnaam gebruikten (bijv. domain.com).

De voornaamste punten van zorg waren:

- Begrijpen hoe identiteitseigendom en groepslidmaatschapstoewijzing zich gedragen wanneer dezelfde gebruikers en groepen in beide identiteitsbronnen bestaan
- Zorgen voor consistente handhaving van het beleid voor veilige toegang voor hybride gebruikers die toegang hebben tot zowel on-premises als cloudbronnen
- Behoud van interne IP-zichtbaarheid voor gebruikers in deze hybride identiteitsconfiguratie
- Bepalen of gelijktijdige synchronisatie van beide bronnen problemen zou veroorzaken in een productieomgeving

Concurrent synchronisatie van dezelfde gebruikers en groepen vanuit de Cisco AD Connector en de Cisco User Management for Secure Access-app wordt niet ondersteund en leidt tot inconsistente handhaving van toegangsregels.

milieu

- Cisco Secure Access met AD Connector en EntraID-integratie
- On-premises Active Directory met overeenkomende domeinnaam EntraID-domein

- Microsoft EntraID (Azure AD) met dezelfde domeinnaam als on-premises AD
- SAML SSO-configuratie voor identiteitsfederatie
- Secure Web Gateway (SWG)-module voor beleidshandhaving
- Hybride omgeving die toegang vereist tot zowel on-premises als cloudbronnen

resolutie

Het volgende gedrag werd bevestigd voor gelijktijdige synchronisatie van zowel Active Directory- als EntraID-bronnen:

groepssynchronisatiegedrag

Bij het synchroniseren van groepen met dezelfde naam uit beide bronnen:

- Twee afzonderlijke groepsobjecten worden gemaakt in Cisco Secure Access - één van elke bron
- Groepen kunnen worden onderscheiden aan de hand van hun bronvoorvoegsel in toegangsbeleid
- On-premises AD-groepen worden weergegeven als: AD-Domain/GroupName
- EntraID-groepen worden weergegeven als: GroupName

Lab verificatie toonde succesvolle synchronisatie met de boodschap "Succes. <<<< Synced" voor groepen uit meerdere EntraID-domeinen.

gebruikerssynchronisatiegedrag

Bij synchronisatie van gebruikers met dezelfde gebruikersnaam uit beide bronnen:

- De gebruikersidentiteit wordt overschreven tijdens synchronisatie

- Slechts één unieke gebruikersnaam blijft zichtbaar in Secure Access
- De uiteindelijke synchronisatiebron bepaalt de attributen en groepslidmaatschappen van de gebruiker
- EntraID-synchronisatie heeft meestal voorrang op on-premises AD wanneer beide zijn geconfigureerd

Configuratie toegangsbeleid

Beide groepstypen kunnen worden gebruikt in toegangsbeleid:

- Raadpleeg on-premises AD-groepen via het volledige pad: AD-Domain/GroupName
- Verwijs naar EntraID-groepen met de eenvoudige naam: GroupName
- Beleid kan onderscheid maken tussen gebruikers op basis van hun groepslidmaatschapsbron

Het volgen van Set up werkt goed voor veel klanten.

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

Oorzaak

Tijdens onze tests hebben we bevestigd dat wanneer een gebruiker wordt gesynchroniseerd vanaf de On-Premises AD Connector, deze die identiteit effectief "claimt" in het Umbrella-dashboard. Als dezelfde gebruiker al bestaat via de Azure AD-synchronisatie, overschrijft de On-Premises-synchronisatie de bestaande EntraID-gebruikersgegevens.

Dit gedrag is een gedocumenteerde beperking. Volgens de officiële technische documentatie van Cisco: https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

Gelijktijdige synchronisatie van dezelfde gebruikers- en groepsidentiteiten vanuit de Umbrella AD Connector en de Cisco Umbrella Azure AD-app wordt niet ondersteund en leidt tot inconsistente

beleidshandhaving.

Conclusie: De gewenste configuratie (VA-zichtbaarheid voor gebruikers die in zowel Azure als On-Prem bestaan) wordt bevestigd als een niet-ondersteunde configuratie.Het pad voorwaarts vereist het gebruik van Roaming Clients om consistente identiteitsafdwinging te garanderen.

Verwante inhoud

- Levering van identiteiten van Azure AD - Cisco Umbrella Documentation
- 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.