

ISE 3.5 Externe EntraID-groepen vragen naar prestatieproblemen en de oplossing van Microsoft Graph API-machtigingen

Inhoud

uitgifte

Cisco ISE 3.5-patch2 met EntraID REST ID Store-configuratie ondervindt aanzienlijke verificatievertragingen tijdens EAP-TLS-verificatie bij het opvragen van EntraID.ExternalGroups. De fase Queried PIP - EntraID.ExternalGroups duurt meer dan 30 seconden om te voltooien, waardoor EAP-clients een time-out krijgen en de verificatie opnieuw opstarten, waardoor een succesvolle sessie niet kan worden voltooid.

Wanneer u bovendien probeert Groepsattributen op te slaan in de configuratie van de EntraID REST ID Store, verschijnt de volgende foutmelding:

```
java.rmi.RemoteException: null; nested exception is: java.lang.NullPointerException
```

De verificatielogboeken tonen asynchrone PIP-fouten en opschorting van de beleidsengine tijdens het opzoekproces van externe groepen. Het probleem manifesteert zich als mislukte verificatieworkflows waarbij clients EAP-sessies niet kunnen voltooien vanwege de verlengde querytijden.

milieu

- Cisco Identity Services Engine (ISE) versie 3.5.0.527 met Patch 2
- Integratie van Microsoft EntraID (Azure Active Directory) via REST ID Store
- EAP-TLS-verificatie geconfigureerd

- REST-bron geconfigureerd voor EntraID met ophalen van groepskenmerken
- Probleem waargenomen op ISE 3.4 patch4/patch5 en ISE 3.5 patch2/patch3

resolutie

De oplossing houdt in dat de juiste Microsoft Graph API-machtigingen worden toegekend aan de Azure-toepassing die wordt gebruikt door de ISE EntraID REST ID Store-integratie.

Stap 1: Vereiste Microsoft Graph API-machtigingen verlenen

Navigeer naar het Azure-portaal en zoek de toepassingsregistratie die wordt gebruikt voor ISE-integratie. Geef deze API-toestemming voor het type toepassing:

`Directory.Read.All`

Zorg ervoor dat de beheerder toestemming geeft voor deze toestemming.

Stap 2: ISE-services opnieuw starten

Na het verlenen van de `Directory.Read.All`-toestemming, voert u een herstart van de services uit op alle ISE-knooppunten om ervoor te zorgen dat de nieuwe machtigingen van kracht worden.

Stap 3: Resolutie controleren

Test het verificatieproces om te bevestigen dat de fase `Queried PIP - EntraID.ExternalGroups` binnen aanvaardbare termijnen wordt voltooid en dat Groepsattributen zonder fouten kunnen worden opgeslagen.

De resolutielogboeken moeten succesvol worden voltooid zonder de `AsynchronousPIPErrors`:

2026-05-26 14:21:47,981 DEBUG [I/O dispatcher 1][[]] cisco.ise.ropc.utilities.HttpClientWrapper -:::-

Oorzaak

Het probleem wordt veroorzaakt door Cisco bug ID CSCwu13703, die ISE 3.5 patch 3 en aanverwante versies beïnvloedt. De bug is gerelateerd aan onvoldoende Microsoft Graph API-rechten voor de EntraID-integratie. Zonder de juiste Directory.Read.All-toestemming kan ISE niet efficiënt externe groepen van EntraID bevragen, wat resulteert in time-outvoorwaarden en opschorting van de beleidsengine via AsynchronousPIPEError-uitzonderingen.

Het verificatieproces mislukt omdat elke mislukte evaluatie ervoor zorgt dat de beleidsengine AsynchronousPIPEError gooit en de verificatieworkflow opschort, wat leidt tot de verlengde querytijden en uiteindelijke clienttime-out.

Gerelateerde inhoud

- [Cisco bug ID CSCwu13703](#)
- [Cisco ISE met Microsoft Active Directory Entra ID en Intune Configuration Guide](#)

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.