Problemen met SAML Azure Group Matching Failure voor externe verificatie oplossen

Inhoud

Inleiding

In dit document wordt beschreven hoe u problemen met Azure Active Directory SAML-groepsclaims voor externe verificatie kunt oplossen.

Voorwaarden

Externe verificatie vindt plaats op Cisco Secure Email Gateway-, Cisco Secure Email- en Web Manager-apparaten.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SAML 2.0 SSO is al geconfigureerd en functioneel voor ten minste één testaccount.
- Groepstoewijzing is ingeschakeld op het toestel en geconfigureerd voor gebruik van de

groepsclaim: Microsoft Schema's - Identity Claims Group.

- Toegang tot Entra ID om de configuratie van de groepsclaims van de toepassing te wijzigen.

Gebruikte componenten

- Producten: Cisco Secure Email Gateway (ESA) en Cisco Secure Email and Web Manager (SMA), wanneer geconfigureerd voor SAML 2.0 Single Sign-On (SSO).
- Identiteitsprovider (IDp): Microsoft Entra ID (Azure AD).
- Autorisatiemethode: Toestelrol/toewijzing van bevoegdheden op basis van SAML-groepsclaims (groepstoewijzing).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Symptomen

- SSO slaagt wanneer een gebruiker expliciet is toegewezen (bijvoorbeeld door gebruikers-ID), maar mislukt wanneer autorisatie afhankelijk is van groepstoewijzing.
- In de SSO-logs worden fouten in groepsattributen of groepstoewijzingen weergegeven.

Oorzaak

Wanneer een gebruiker lid is van meer dan 150 groepen, geeft Microsoft Entra ID niet de verwachte groepsclaim (Microsoft Schemas - Identity Claims Group) in de SAML-bewering. In plaats daarvan zendt het Microsoft Schemas - Claims Group uit, die het toestel niet kan gebruiken voor roltoewijzing.

Probleemoplossing

Van toepassing op: SAML 2.0 SSO geconfigureerd met Microsoft Entra ID (Azure AD) waarbij het

toestel SAML-groepsclaims gebruikt voor autorisatie (groepstoewijzing).

SSO-logs verifiëren

Verzamel op het Cisco Secure Email-toestel logboeken voor Single Sign-On (SSO)-verificatiepogingen uit de GUI-logboeken. Voer bijvoorbeeld de opdracht uit:

```
grep -i sso gui_logs
```

Als het probleem verband houdt met groepstoewijzing in de IdP-bewering (Identity Provider), kunnen de SSO-logs de volgende foutmeldingen weergeven:

```
grep -i sso gui_logs
"An error occurred during SSO authentication. Details: Please check the configured Group Attributes, it
"An error occurred during SSO authentication. Details: User: XXXXX Authorization failed on appliance, w
"An error occurred during SSO authentication. Details: Please check the configured Group Mapping values
```

SAML-respons vastleggen

Om te bevestigen of het probleem wordt veroorzaakt door een groot aantal groepslidmaatschappen, verzamelt u een HAR-bestand (Hypertext Transfer Protocol) tijdens een mislukte SAML-verificatiepoging. Gebruik tools voor browserontwikkelaars of een goedgekeurde browserextensie. Gebruik geen openbare online decoders of uploadtools van derden om de SAML-respons te inspecteren.

Procedure:

1. Open de browser developer tools en start een netwerk vastleggen.
2. Navigeer naar de webinterface Cisco Secure Email Gateway of Cisco Secure Email and Web Manager.
3. Start de SAML Single Sign-On (SSO) -stroom en reproduceer de mislukte autorisatie.
4. Exporteer de opgenomen sessie als een HAR-bestand.

Opmerking: de exacte stappen verschillen per browser. Gebruik een ondersteunde browsermethode die de SAML-respons lokaal op het werkstation houdt.

HAR-bestand analyseren

Gebruik het HAR-bestand om te controleren welk groepskenmerk Microsoft Entra ID teruggeeft in de SAML-bewering.

1. Open het HAR-bestand in de browser developer tools.
2. Zoek het SAML-reactieverzoek op, zoals weergegeven in afbeelding 1.
3. Kopieer de waarde van het veld SAMLRresponse. Identificeer in afbeelding 1 de gecodeerde waarde tussen de aanhalingstekens na waarde=.
4. Decodeer de Base64-gecodeerde SAMLResponse-waarde met behulp van een goedgekeurde offline methode. Gebruik bijvoorbeeld een lokaal opdrachtregelhulpprogramma:

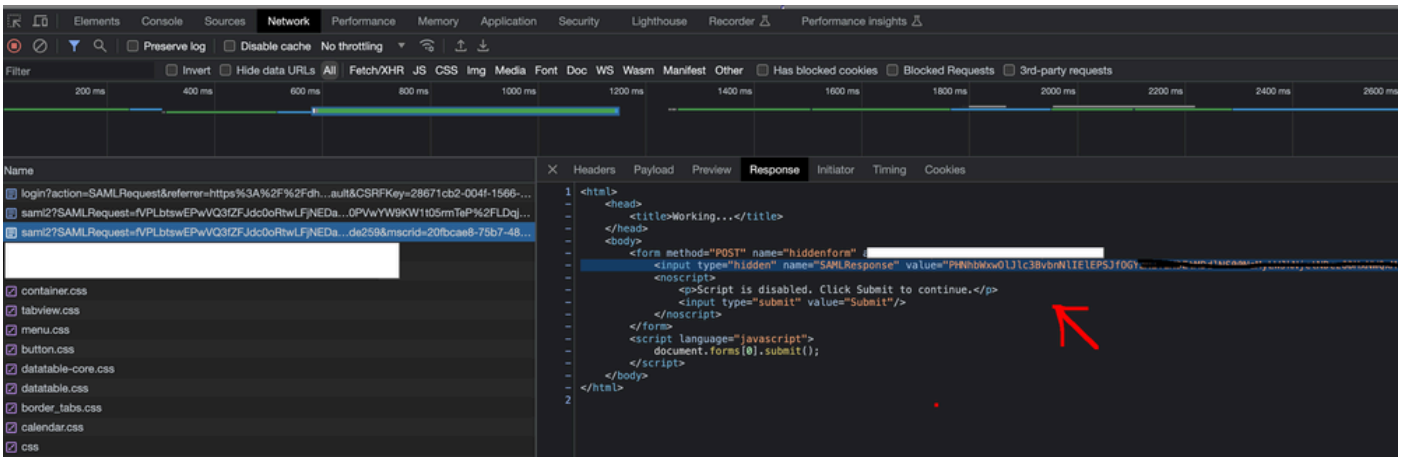
```
# macOS/Linux
printf '%s' "

       " | base64 --decode > saml_response.xml

# Windows PowerShell
[System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('

        ')) | Out-File -Encoding utf8 saml_response.xml
```

5. Controleer de gedecodeerde XML en controleer of Microsoft Entra ID het kenmerk expected groups of het kenmerk alternate link retourneert.



Beschrijf het claimgedrag van Azure Group

In een werkscenario bevat het gedecodeerde SAML-antwoord het attribuut expected groups: Microsoft Schemas - Identity Claims Groups. Wanneer dit probleem zich voordoet, retourneert Microsoft Entra ID Microsoft Schema's - Claimgroepen in plaats van het kenmerk verwachte groepen.

Dit gedrag treedt op omdat Microsoft Entra ID het aantal groepen beperkt dat wordt uitgezonden in de claim SAML-groepen. Als de SAML-bewering meer dan 150 groepslidmaatschappen bevat, retourneert Azure AD het attribuut groups.link in plaats van het attribuut groups. Het Cisco Secure Email-toestel kan groups.link niet gebruiken voor roltoewijzing, dus autorisatie mislukt.

resolutie

Wijzig de Microsoft Entra ID-toepassing zodat de SAML-bevestiging een claim voor bruikbare groepen voor het toestel retourneert. Het doel is om te voorkomen dat Azure AD Microsoft Schemas - Claims Groups retourneert in plaats van het attribuut verwachte groepen.

1. Open in Azure AD de zakelijke toepassing die wordt gebruikt voor Cisco Secure Email Gateway of Cisco Secure Email and Web Manager SAML-verificatie.
2. Navigeer naar de SAML token attributen of groep claims configuratie.
3. Wijzig de instelling voor groepsclaims in Groepen die aan de toepassing zijn toegewezen,

als die instelling voldoet aan de implementatievereisten.

4. Zorg ervoor dat de betreffende beheerdersaccount alleen is toegewezen aan de groepen die vereist zijn voor toestelautorisatie.
5. Sla de Azure AD-configuratie op en start een nieuwe SAML-aanmeldingspoging.
6. Voer op het toestel de opdracht grep -i sso gui.current from /data/pub/gui_logs uit en bevestig dat de eerdere autorisatiefouten niet langer voorkomen.
7. De gedecodeerde SAML-respons valideren en bevestigen dat Azure AD Microsoft Schemas - Identity Claims Groups retourneert in plaats van Microsoft Schemas - Claims Groups.

Opmerking: Als de vereiste configuratie voor de Azure AD-groep niet beschikbaar is of niet voldoet aan de implementatievereisten, neemt u contact op met de beheerder van Microsoft Entra ID of het ondersteuningsteam van Microsoft.

Gerelateerde informatie

- Microsoft Learn: Groepsclaims voor toepassingen configureren
- MuleSoft: Azure AD SAML Group Attribuutbeperking

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.