Dépannage de l'échec de correspondance de groupe Azure SAML pour l'authentification externe

Table des matières

Introduction

Ce document décrit comment dépanner les échecs de revendication de groupe SAML Azure Active Directory pour l'authentification externe.

Conditions préalables

L'authentification externe s'effectue sur les appliances Cisco Secure Email Gateway, Cisco Secure Email et Web Manager.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- L'authentification unique SAML 2.0 est déjà configurée et fonctionne pour au moins un

compte de test.

- Le mappage de groupe est activé sur l'appliance et configuré pour utiliser la revendication de groupe : Schémas Microsoft - Groupe de revendications d'identité.
- Accès à Entra ID pour modifier la configuration des revendications de groupe de l'application.

Composants utilisés

- Produits : Cisco Secure Email Gateway (ESA) et Cisco Secure Email and Web Manager (SMA), lorsqu'ils sont configurés pour l'authentification unique SAML 2.0.
- Fournisseur d'identités (IdP) : Microsoft Entra ID (Azure AD).
- Méthode d'autorisation : Attribution de rôle/privilège d'appliance basée sur des revendications de groupe SAML (mappage de groupe).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Symptômes

- L'authentification unique réussit lorsqu'un utilisateur est explicitement mappé (par exemple, par ID utilisateur), mais échoue lorsque l'autorisation repose sur le mappage de groupe.
- Les journaux SSO affichent les erreurs de non-concordance d'attribut de groupe ou de mappage de groupe.

Motif

Lorsqu'un utilisateur est membre de plus de 150 groupes, Microsoft Entra ID n'émet pas la revendication de groupe attendue (Schémas Microsoft - Groupe de revendications d'identité) dans l'assertion SAML. À la place, il émet Schémas Microsoft - Groupe de revendications, que la solution matérielle-logicielle ne peut pas utiliser pour le mappage de rôles.

Dépannage

S'applique à : SSO SAML 2.0 configuré avec Microsoft Entra ID (Azure AD) où l'appliance utilise des revendications de groupe SAML pour l'autorisation (mappage de groupe).

Vérification des journaux SSO

Sur l'appliance de messagerie sécurisée Cisco, collectez les journaux des tentatives d'authentification SSO (Single Sign-On) à partir des journaux de l'interface utilisateur graphique. Par exemple, exécutez la commande :

```
grep -i sso gui_logs
```

Si le problème est lié au mappage de groupe dans l'assertion du fournisseur d'identité (IdP), les journaux SSO peuvent afficher les messages d'erreur suivants :

```
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
```

Capturer la réponse SAML

Pour confirmer si le problème est causé par un nombre élevé d'appartenances au groupe, collectez un fichier d'archivage HTTP (Hypertext Transfer Protocol) (HAR) lors d'une tentative d'authentification SAML ayant échoué. Utilisez les outils de développement de navigateur ou une extension de navigateur approuvée. N'utilisez pas de décodeurs publics en ligne ou d'outils de téléchargement tiers pour vérifier la réponse SAML.

Procédure:

1. Ouvrez les outils de développement du navigateur et lancez une capture réseau.
2. Accédez à l'interface Web Cisco Secure Email Gateway ou Cisco Secure Email and Web Manager.

3. Lancez le flux SSO (Single Sign-On) SAML et reproduisez l'échec de l'autorisation.

4. Exportez la session capturée en tant que fichier HAR.

Remarque : Les étapes exactes varient selon le navigateur. Utilisez une méthode de navigateur prise en charge qui conserve la réponse SAML en local sur la station de travail.

Analyser le fichier HAR

Utilisez le fichier HAR pour vérifier quel attribut de groupe Microsoft Entra ID renvoie dans l'assertion SAML.

1. Ouvrez le fichier HAR dans les outils de développement du navigateur.

2. Recherchez la demande de réponse SAML, comme illustré dans l'image 1.

3. Copiez la valeur du champ SAMLResponse. Dans l'image 1, identifiez la valeur codée entre les guillemets après value=.

4. Décodez la valeur SAMLResponse codée en Base64 à l'aide d'une méthode hors ligne approuvée. Par exemple, utilisez un utilitaire de ligne de commande local :

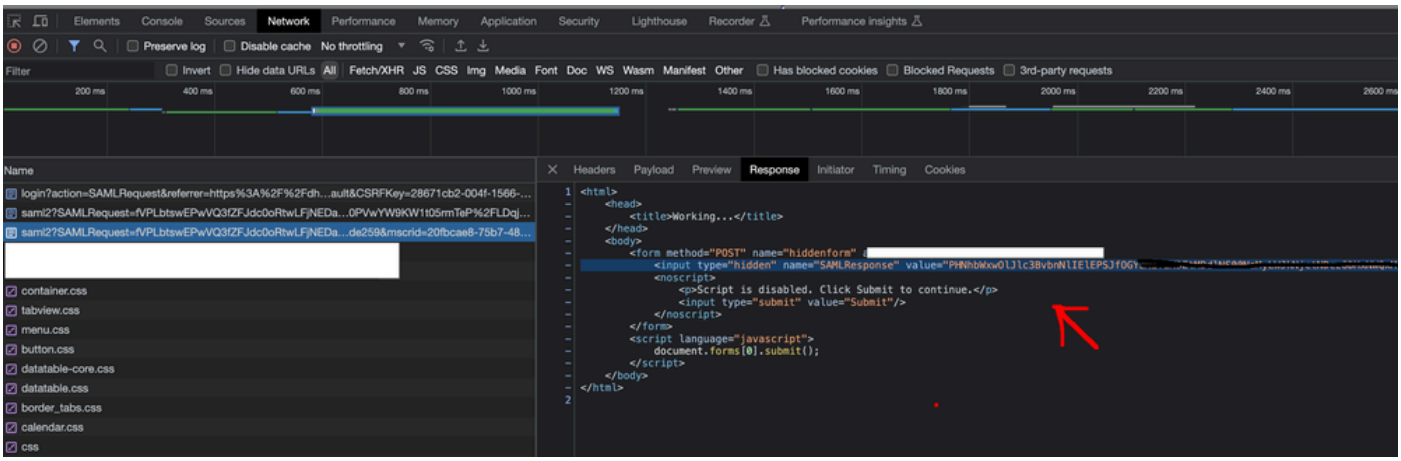
```
# macOS/Linux
printf '%s' "

       " | base64 --decode > saml_response.xml

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

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

5. Vérifiez le code XML décodé et vérifiez si Microsoft Entra ID renvoie l'attribut groups attendu ou l'attribut de liaison de remplacement.



Identifier le comportement de revendication de groupe Azure

Dans un scénario de travail, la réponse SAML décodée contient l'attribut groupes attendus : Schémas Microsoft - Groupes de revendications d'identité . Lorsque ce problème se produit, Microsoft Entra ID renvoie Microsoft Schemas - Claims Groups au lieu de l'attribut groups attendu.

Ce comportement se produit parce que Microsoft Entra ID limite le nombre de groupes émis dans la revendication de groupes SAML. Si l'assertion SAML contient plus de 150 appartenances de groupe, Azure AD renvoie l'attribut groups.link au lieu de l'attribut groups. L'appliance de messagerie sécurisée Cisco ne peut pas utiliser groups.link pour le mappage des rôles, donc l'autorisation échoue.

Résolution

Modifiez l'application Microsoft Entra ID de sorte que l'assertion SAML renvoie une revendication de groupe utilisable pour l'appliance. L'objectif est d'empêcher Azure AD de renvoyer des schémas Microsoft - Revendications Groups au lieu de l'attribut groups attendu.

1. Dans Azure AD, ouvrez l'application d'entreprise utilisée pour l'authentification Cisco Secure Email Gateway ou Cisco Secure Email and Web Manager SAML.
2. Accédez à la configuration des attributs de jeton SAML ou des revendications de groupe.
3. Modifiez le paramètre Revendications de groupe sur Groupes affectés à l'application, si ce

paramètre répond aux exigences de déploiement.

4. Assurez-vous que le compte d'administrateur affecté est affecté uniquement aux groupes requis pour l'autorisation de l'appliance.
5. Enregistrez la configuration Azure AD et démarrez une nouvelle tentative de connexion SAML.
6. Sur l'appliance, exécutez la commande grep -i sso gui.current à partir de /data/pub/gui_logs et vérifiez que les erreurs d'autorisation précédentes ne se produisent plus.
7. Validez la réponse SAML décodée et confirmez qu'Azure AD renvoie des schémas Microsoft - Groupes de revendications d'identité au lieu de schémas Microsoft - Groupes de revendications.

Remarque : Si la configuration requise des revendications de groupe Azure AD n'est pas disponible ou ne répond pas aux exigences de déploiement, contactez l'administrateur Microsoft Entra ID ou l'équipe de support technique Microsoft.

Informations connexes

- Microsoft Learn : Configurer les revendications de groupe pour les applications
- MuleSoft : Limitation d'attribut de groupe Azure AD SAML

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.