Fehlerbehebung bei SAML Azure-Gruppenzuordnungsfehler für die externe Authentifizierung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Fehler bei Azure Active Directory-SAML-Gruppenansprüchen für die externe Authentifizierung beheben.

Voraussetzungen

Die externe Authentifizierung erfolgt über Cisco Secure Email Gateway, Cisco Secure Email und Web Manager.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- SAML 2.0 SSO ist bereits für mindestens ein Testkonto konfiguriert und funktionsfähig.

- Die Gruppenzuordnung ist auf der Appliance aktiviert und für die Verwendung des Gruppenanspruchs konfiguriert: Microsoft Schemas - Identity Claims Group.
- Zugriff auf die Entra-ID zum Ändern der Gruppenanspruchskonfiguration der Anwendung.

Verwendete Komponenten

- Produkte: Cisco Secure Email Gateway (ESA) und Cisco Secure Email und Web Manager (SMA) bei Konfiguration für SAML 2.0 Single Sign-On (SSO).
- Identitätsanbieter (IdP): Microsoft Entra ID (Azure AD).
- Autorisierungsmethode: Zuweisung von Appliance-Rollen und -Berechtigungen auf Basis von SAML-Gruppenansprüchen (Gruppenzuordnung).

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Symptome

- SSO ist erfolgreich, wenn ein Benutzer explizit zugeordnet wird (z. B. nach Benutzer-ID), schlägt jedoch fehl, wenn die Autorisierung von der Gruppenzuordnung abhängt.
- In SSO-Protokollen werden Fehler bei Gruppenattributen oder Gruppenzuordnungen angezeigt.

Ursache

Wenn ein Benutzer Mitglied von mehr als 150 Gruppen ist, gibt Microsoft Entra ID den erwarteten Gruppenanspruch (Microsoft Schemas - Identity Claims Group) in der SAML-Assertion nicht aus. Stattdessen werden Microsoft Schemas - Claims Group ausgegeben, die die Appliance nicht für die Rollenzuordnung verwenden kann.

Fehlerbehebung

Gilt für: SAML 2.0 SSO wird mit Microsoft Entra ID (Azure AD) konfiguriert, wobei die Appliance SAML-Gruppenansprüche für die Autorisierung (Gruppenzuordnung) verwendet.

Überprüfen von SSO-Protokollen

Erfassen Sie auf der Cisco Secure Email Appliance die Single Sign-On (SSO)-Authentifizierungsversuchsprotokolle aus den GUI-Protokollen. Führen Sie beispielsweise den folgenden Befehl aus:

```
grep -i sso gui_logs
```

Wenn das Problem mit der Gruppenzuordnung in der Identity Provider (IdP)-Assertion zusammenhängt, können die SSO-Protokolle folgende Fehlermeldungen anzeigen:

```
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-Antwort erfassen

Um zu überprüfen, ob das Problem durch eine hohe Anzahl von Gruppenmitgliedschaften verursacht wird, sammeln Sie eine Hypertext Transfer Protocol (HTTP) Archive (HAR)-Datei während eines fehlgeschlagenen SAML-Authentifizierungsversuchs. Verwenden Sie Browser-Entwicklungstools oder eine genehmigte Browsererweiterung. Verwenden Sie keine öffentlichen Online-Decoder oder Upload-Tools von Drittanbietern, um die SAML-Antwort zu überprüfen.

Vorgehensweise:

1. Öffnen Sie die Browser-Entwicklungstools, und starten Sie eine Netzwerkerfassung.
2. Navigieren Sie zur Webschnittstelle von Cisco Secure Email Gateway oder Cisco Secure Email und Web Manager.
3. Initiieren Sie den SAML Single Sign-On (SSO)-Fluss, und stellen Sie den Fehler bei der Autorisierung wieder her.
4. Exportiert die erfasste Sitzung als HAR-Datei.

Anmerkung: Die genauen Schritte variieren je nach Browser. Verwenden Sie eine unterstützte Browsermethode, die die SAML-Antwort lokal auf der Workstation hält.

HAR-Datei analysieren

Verwenden Sie die HAR-Datei, um zu überprüfen, welches Gruppenattribut Microsoft Entra ID in der SAML Assertion zurückgibt.

1. Öffnen Sie die HAR-Datei in den Browser-Entwicklungstools.
2. Suchen Sie die SAML-Antwortanforderung, wie in Abbildung 1 dargestellt.
3. Kopieren Sie den Wert des Felds SAMLResponse. Geben Sie in Bild 1 den kodierten Wert zwischen den Anführungszeichen nach Wert= an
4. Decodieren Sie den Base64-codierten SAMLResponse-Wert mithilfe einer genehmigten Offline-Methode. Verwenden Sie beispielsweise ein lokales Befehlszeilendienstprogramm:

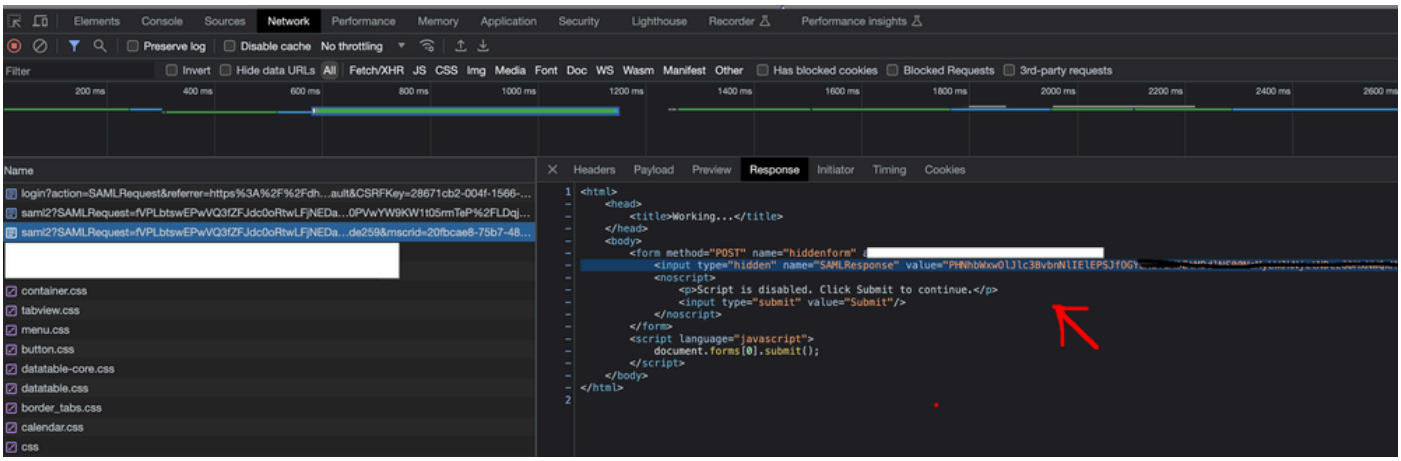
```
# macOS/Linux
printf '%s' "

       " | base64 --decode > saml_response.xml

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

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

5. Überprüfen Sie den decodierten XML-Code, und stellen Sie sicher, dass Microsoft Entra ID das erwartete Gruppenattribut oder das alternative Linkattribut zurückgibt.



Azure-Gruppenanspruchverhalten identifizieren

In einem Arbeitsszenario enthält die decodierte SAML-Antwort das erwartete Gruppenattribut: Microsoft Schemas - Identity Claims Groups . Wenn dieses Problem auftritt, gibt Microsoft Entra ID Microsoft Schemas - Claims Groups anstelle des erwarteten Gruppenattributs zurück.

Dieses Verhalten tritt auf, weil Microsoft Entra ID die Anzahl der im SAML-Gruppenanspruch emittierten Gruppen begrenzt. Wenn die SAML-Assertion mehr als 150 Gruppenmitgliedschaften enthält, gibt Azure AD das Attribut groups.link anstelle des Attributs groups zurück. Die Cisco Secure Email Appliance kann groups.link nicht für die Rollenzuordnung verwenden. Die Autorisierung schlägt daher fehl.

Auflösung

Ändern Sie die Microsoft Entra ID-Anwendung so, dass die SAML-Assertion einen verwendbaren Gruppenanspruch für die Appliance zurückgibt. Dadurch soll verhindert werden, dass Azure AD Microsoft Schemas - Claims Groups anstelle des erwarteten Gruppenattributs zurückgibt.

1. Öffnen Sie in Azure AD die Enterprise-Anwendung für die Cisco Secure Email Gateway- oder Cisco Secure Email- und Web Manager SAML-Authentifizierung.
2. Navigieren Sie zu den SAML-Tokenattributen oder zur Konfiguration von Gruppenansprüchen.

3. Ändern Sie die Gruppenanspruchseinstellung in Gruppen, die der Anwendung zugewiesen sind, wenn diese Einstellung den Bereitstellungsanforderungen entspricht.
4. Stellen Sie sicher, dass das betroffene Administratorkonto nur den für die Appliance-Autorisierung erforderlichen Gruppen zugewiesen ist.
5. Speichern Sie die Azure AD-Konfiguration, und starten Sie einen neuen SAML-Anmeldeversuch.
6. Führen Sie auf der Appliance den Befehl grep -i sso gui.current aus /data/pub/gui_logs aus, und bestätigen Sie, dass die vorherigen Autorisierungsfehler nicht mehr auftreten.
7. Validieren Sie die decodierte SAML-Antwort, und bestätigen Sie, dass Azure AD Microsoft Schemas - Identity Claims Groups anstelle von Microsoft Schemas - Claims Groups zurückgibt.

Anmerkung: Wenn die erforderliche Azure AD-Gruppenanspruchskonfiguration nicht verfügbar ist oder die Bereitstellungsanforderungen nicht erfüllt, wenden Sie sich an den Microsoft Entra ID-Administrator oder das Microsoft Support-Team.

Zugehörige Informationen

- Microsoft - Informationen: Gruppenansprüche für Anwendungen konfigurieren
- MuleSoft: Azure AD SAML-Gruppenattribut-Beschränkung

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.