外部認証のSAML Azureグループ照合エラーのトラブルシューティング

内容

はじめに

このドキュメントでは、外部認証のAzure Active Directory SAMLグループ要求エラーのトラブルシューティング方法について説明します。

前提条件

外部認証は、Cisco Secure Email Gateway、Cisco Secure Email、およびWeb Managerアプライアンスで実行されます。

要件

次の項目に関する知識が推奨されます。

- SAML 2.0 SSOは、少なくとも1つのテストアカウントですでに構成され、機能しています。

- アプライアンスでグループマッピングが有効になっており、グループ要求Microsoft Schemas - Identity Claims Groupを使用するように設定されています。
- エントリIDにアクセスして、アプリケーションのグループ要求の構成を変更します。

使用するコンポーネント

- 製品：Cisco Secure Email Gateway(ESA)およびCisco Secure Email and Web Manager(SMA)(SAML 2.0シングルサインオン(SSO)用に設定されている場合)
- IDプロバイダー(IdP): Microsoft Entra ID (Azure AD)。
- 許可方式：SAMLグループ要求に基づくアプライアンスのロール/権限の割り当て（グループマッピング）。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

症状

- SSOは、ユーザが明示的にマッピングされている場合（たとえば、ユーザIDによって）は成功しますが、認可がグループマッピングに依存している場合は失敗します。
- SSOログには、グループ属性またはグループマッピングの不一致エラーが表示されます。

原因

ユーザが150を超えるグループのメンバである場合、Microsoft Entra IDはSAMLアサーションで予期されるグループ要求(Microsoft Schemas - Identity Claims Group)を生成しません。その代わりに、アプライアンスが役割のマッピングに使用できないMicrosoftスキーマ – 要求グループを生成します。

トラブルシューティング

適用対象：アプライアンスがSAMLグループ要求を認証（グループマッピング）に使用する、Microsoft Entra ID(Azure AD)で構成されたSAML 2.0 SSO。

SSOログの確認

Cisco Secure Eメールアプライアンスで、GUIログからシングルサインオン(SSO)認証試行ログを収集します。たとえば、次のコマンドを実行します。

```
grep -i sso gui_logs
```

問題がアイデンティティプロバイダー(IdP)アサーションのグループマッピングに関連している場合は、SSOログに次のエラーメッセージが表示される可能性があります。

```
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応答のキャプチャ

問題の原因が多数のグループメンバーシップにあるかどうかを確認するには、SAML認証が失敗した際にハイパーテキスト転送プロトコル(HTTP)アーカイブ(HAR)ファイルを収集します。ブラウザ開発者ツールまたは承認されたブラウザ拡張機能を使用する。パブリックオンラインデコーダまたはサードパーティのアップロードツールを使用してSAML応答を検査しないでください。

手順：

1. ブラウザの開発者ツールを開き、ネットワークキャプチャを開始します。
2. Cisco Secure Email GatewayまたはCisco Secure Email and Web Manager Webインターフェイスに移動します。
3. SAMLシングルサインオン(SSO)フローを開始し、認証失敗を再現します。
4. キャプチャしたセッションをHARファイルとしてエクスポートします。

注：実際の手順はブラウザによって異なります。サポートされているブラウザ方式を使用して、SAML応答をワークステーションのローカルに保持します。

HARファイルの分析

HARファイルを使用して、Microsoft Entra IDがSAMLアサーションで返すグループ属性を確認します。

1. ブラウザ開発者ツールでHAR ファイルを開きます。
2. 図1に示すように、SAML 応答要求を見つけます。
3. SAMLResponseフィールドの値をコピーします。図1では、value=の後の引用符で囲まれたエンコードされた値を識別します。
4. 承認済みのオフライン方式を使用して、Base64エンコードSAMLResponse値をデコードします。たとえば、ローカルコマンドラインユーティリティを使用します。

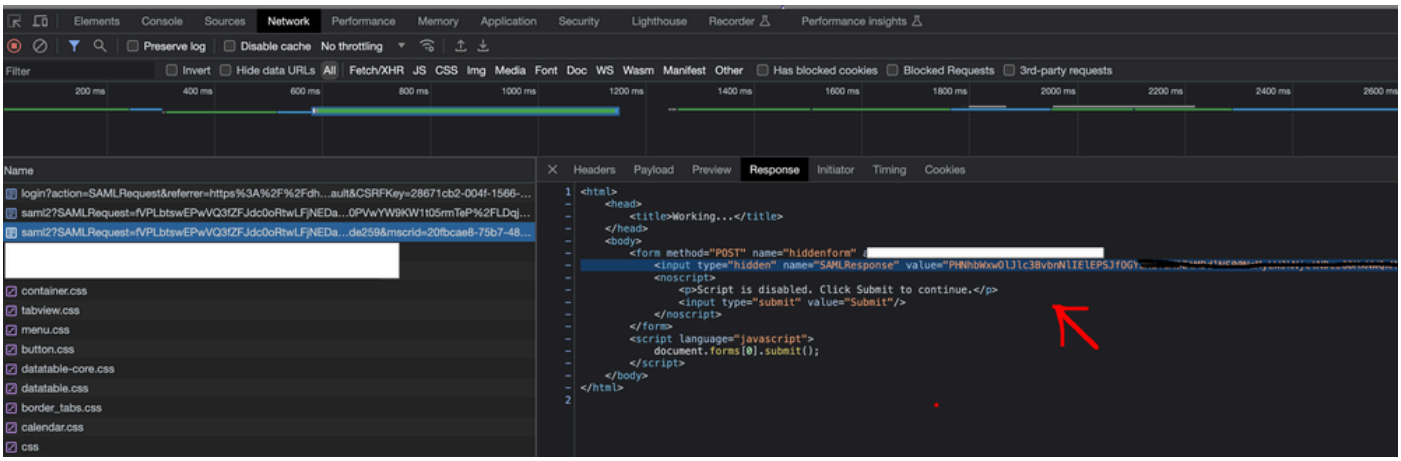
```
# macOS/Linux
printf '%s' "

       " | base64 --decode > saml_response.xml

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

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

5. デコードされたXMLを確認し、Microsoft Entra IDが予期されるグループ属性または代替リンク属性を返すかどうかを確認します。



Azureグループ要求の動作の識別

作業シナリオでは、デコードされたSAML応答に必要なグループ属性(Microsoft Schemas - Identity Claims Groups)が含まれています。この問題が発生すると、Microsoft Entra IDは、予期されるグループ属性の代わりにMicrosoft Schemas - Claims Groupsを返します。

この動作が発生するのは、SAMLグループ要求で生成されるグループの数がMicrosoft Entra IDによって制限されるためです。SAMLアサーションに150を超えるグループメンバーシップが含まれている場合、Azure ADはgroups属性の代わりにgroups.link属性を返します。Cisco Secure Eメールアプライアンスでは、役割マッピングにgroups.linkを使用できないため、認証が失敗します。

解決策

SAMLアサーションがアプライアンスの使用可能なグループ要求を返すように、Microsoft Entra IDアプリケーションを変更します。この目的は、Azure ADが予期されるグループ属性の代わりにMicrosoftスキーマ – 要求グループを返さないようにすることです。

1. Azure ADで、Cisco Secure Email GatewayまたはCisco Secure Email and Web ManagerのSAML認証に使用されるエンタープライズアプリケーションを開きます。
2. SAML トークン属性またはグループ要求構成に移動します。
3. グループ要求の設定が展開要件を満たしている場合は、その設定をアプリケーションに割り当てられたグループに変更します。

4. 影響を受ける管理者アカウントが、アプライアンス認証に必要なグループのみに割り当てられていることを確認します。
5. Azure AD 設定を保存し、新しいSAML ログインを試行します。
6. アプライアンスで、/data/pub/gui_logsからgrep -i sso gui.current コマンドを実行し、以前の認証エラーが発生しなくなったことを確認します。
7. デコードされた SAML 応答を検証し、Azure ADがMicrosoftスキーマ – 要求グループではなくMicrosoftスキーマ – Identity要求グループを返すことを確認します。

注：必要なAzure ADグループ要求の構成が使用できないか、展開要件を満たしていない場合は、Microsoft Entra ID管理者またはMicrosoftサポートチームにお問い合わせください。

関連情報

- Microsoftラーニング：アプリケーションのグループ要求の構成
- MuleSoft: Azure AD SAMLグループ属性の制限

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。