Solucionar Problemas de Falha de Correspondência de Grupo do SAML Azure para Autenticação Externa

Contents

Introdução

Este documento descreve como solucionar problemas de falhas de declaração de grupo SAML do Ative Diretory do Azure para autenticação externa.

Pré-requisitos

A autenticação externa está no Cisco Secure Email Gateway, no Cisco Secure Email e nos dispositivos Web Manager.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O SSO do SAML 2.0 já está configurado e funcional para pelo menos uma conta de teste.

- O mapeamento de grupo está habilitado no aplicativo e configurado para usar a declaração de grupos: Esquemas da Microsoft - Grupo de Declarações de Identidade.
- Acesso ao Entra ID para modificar a configuração de declarações de grupo do aplicativo.

Componentes Utilizados

- Produtos: Cisco Secure Email Gateway (ESA) e Cisco Secure Email and Web Manager (SMA), quando configurado para SAML 2.0 Single Sign-On (SSO).
- Provedor de identidade (IdP): ID do Microsoft Entra (Azure AD).
- Método de autorização: Atribuição de função/privilégio de aplicativo com base em declarações de grupo SAML (mapeamento de grupo).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Sintomas

- O SSO é bem-sucedido quando um usuário é mapeado explicitamente (por exemplo, por ID de usuário), mas falha quando a autorização depende do mapeamento do grupo.
- Os logs SSO mostram erros de incompatibilidade de atributo de grupo ou de mapeamento de grupo.

Causa

Quando um usuário é membro de mais de 150 grupos, o Microsoft Entra ID não emite a declaração de grupos esperada (Microsoft Schemas - Identity Claims Group) na asserção SAML. Em vez disso, ele emite Microsoft Schemas - Claims Group, que o equipamento não pode usar para mapeamento de função.

Troubleshooting

Aplicável a: SAML 2.0 SSO configurado com Microsoft Entra ID (Azure AD) onde o aplicativo usa declarações de grupo SAML para autorização (mapeamento de grupo).

Verificar registros SSO

No Cisco Secure Email Appliance, colete logs de tentativas de autenticação do SSO (Single Sign-On, sign-on único) dos logs da interface de usuário. Por exemplo, execute o comando:

```
grep -i sso gui_logs
```

Se o problema estiver relacionado ao mapeamento de grupo na asserção do Provedor de Identidade (IdP), os logs de SSO poderão mostrar estas mensagens de erro:

```
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
```

Capturar Resposta SAML

Para confirmar se o problema é causado por um alto número de associações de grupo, colete um arquivo HAR (Archive) do Protocolo de Transferência de Hipertexto (HTTP) durante uma tentativa de autenticação SAML que falhou. Use ferramentas de desenvolvimento de navegador ou uma extensão de navegador aprovada. Não use decodificadores públicos online ou ferramentas de carregamento de terceiros para inspecionar a resposta SAML.

Procedimento:

1. Abra as ferramentas do desenvolvedor do navegador e inicie uma captura da rede.
2. Navegue até a interface da Web do Cisco Secure Email Gateway ou do Cisco Secure Email and Web Manager.
3. Inicie o fluxo do SSO (Single Sign-On SAML) e reproduza a falha de autorização.
4. Exporte a sessão capturada como um arquivo HAR.

Note: As etapas exatas variam de acordo com o navegador. Use um método de navegador suportado que mantenha a resposta SAML local para a estação de trabalho.

Analisar arquivo HAR

Use o arquivo HAR para verificar qual atributo de grupo o Microsoft Entra ID retorna na asserção SAML.

1. Abra o arquivo HAR nas ferramentas do desenvolvedor do navegador.
2. Localize a solicitação de resposta SAML, como mostrado na Imagem 1.
3. Copie o valor do campo SAMLResponse. Na Imagem 1, identifique o valor encoded entre as aspas depois de value=.
4. Decodifique o valor SAMLResponse codificado na Base64 usando um método off-line aprovado. Por exemplo, use um utilitário de linha de comando local:

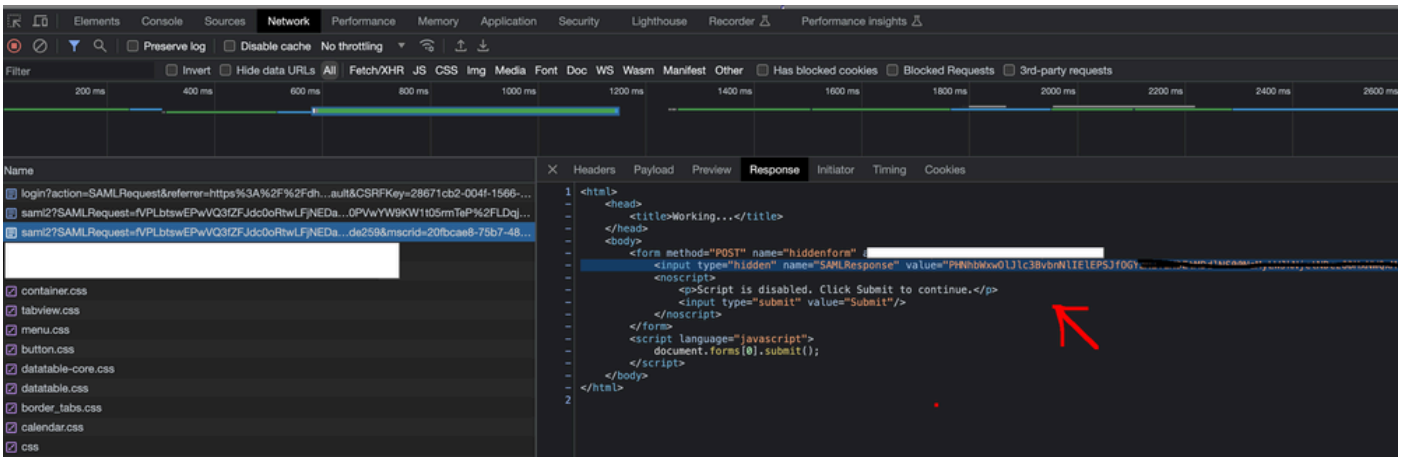
```
# macOS/Linux
printf '%s' "

       " | base64 --decode > saml_response.xml

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

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

5. Revise o XML decodificado e verifique se o Microsoft Entra ID retorna o atributo de grupos esperado ou o atributo de link alternativo.



Identificar o Comportamento da Declaração de Grupo do Azure

Em um cenário de trabalho, a resposta SAML decodificada contém o atributo de grupos esperado: Esquemas da Microsoft - Grupos de Declarações de Identidade . Quando esse problema ocorre, o Microsoft Entra ID retorna Microsoft Schemas - Claims Groups em vez do atributo de grupos esperado.

Este comportamento ocorre porque o Microsoft Entra ID limita o número de grupos emitidos na declaração de grupos SAML. Se a asserção SAML contiver mais de 150 associações de grupo, o Azure AD retornará o atributo groups.link em vez do atributo groups. O Cisco Secure Email Appliance não pode usar groups.link para mapeamento de função, portanto, a autorização falha.

Resolução

Modifique o aplicativo Microsoft Entra ID para que a asserção SAML retorne uma declaração de grupos utilizáveis para o aplicativo. O objetivo é impedir que o Azure AD retorne Esquemas da Microsoft - Grupos de Declarações em vez do atributo de grupos esperado.

1. No Azure AD, abra o aplicativo empresarial usado para o Cisco Secure Email Gateway ou a autenticação do Cisco Secure Email and Web Manager SAML.
2. Navegue até a configuração SAML token attributes ou group claims.
3. Altere a configuração group claims para Groups assigned to the application, se essa

configuração atender aos requisitos de implantação.

4. Verifique se a conta de administrador afetada está atribuída somente aos grupos necessários para autorização do equipamento.
5. Salve a configuração do Azure AD e inicie um novo SAML log na tentativa.
6. No equipamento, execute o comando grep -i sso gui.current em /data/pub/gui_logs e confirme se os erros de autorização anteriores não ocorrem mais.
7. Valide a resposta decodificada SAML e confirme se o Azure AD retorna Esquemas da Microsoft - Grupos de Declarações de Identidade em vez de Esquemas da Microsoft - Grupos de Declarações.

Note: Se a configuração necessária das declarações de grupo do Azure AD não estiver disponível ou não atender aos requisitos de implantação, contate o administrador do Microsoft Entra ID ou a equipe de suporte da Microsoft.

Informações Relacionadas

- Aprendizado da Microsoft: Configurar Reivindicações de Grupo para Aplicativos
- MuleSoft Limitação de Atributos do Grupo SAML do Azure AD

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.