Solucionar problemas de error de coincidencia de grupo de SAML Azure para autenticación externa

Contenido

Introducción

Este documento describe cómo resolver problemas de fallas de reclamación de grupo SAML de Azure Active Directory para la autenticación externa.

Prerequisites

La autenticación externa se realiza en los dispositivos Cisco Secure Email Gateway, Cisco Secure Email y Web Manager.

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- El SSO de SAML 2.0 ya está configurado y funciona para al menos una cuenta de prueba.

- La asignación de grupos está habilitada en el dispositivo y configurada para utilizar la notificación de grupos: Esquemas de Microsoft: grupo de notificaciones de identidad.
- Acceso a la ID de entrada para modificar la configuración de notificaciones de grupo de la aplicación.

Componentes Utilizados

- SOPORTE DE PRODUCTO: Cisco Secure Email Gateway (ESA) y Cisco Secure Email and Web Manager (SMA), cuando se configuran para el inicio de sesión único (SSO) de SAML 2.0.
- Proveedor de identidad (IdP): ID de Microsoft Entry (Azure AD).
- Método de autorización: Asignación de privilegio/función de dispositivo basada en notificaciones de grupo SAML (asignación de grupo).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Síntomas

- SSO se ejecuta correctamente cuando un usuario está asignado explícitamente (por ejemplo, por ID de usuario), pero falla cuando la autorización se basa en la asignación de grupo.
- Los registros de SSO muestran errores de discordancia de asignación de grupo o atributo de grupo.

Causa

Cuando un usuario es miembro de más de 150 grupos, Microsoft Entra ID no emite la notificación de grupos esperada (Microsoft Schemas - Identity Claims Group) en la afirmación SAML. En su lugar, emite Microsoft Schemas - Claims Group, que el dispositivo no puede utilizar para la asignación de funciones.

Resolución de problemas

Se aplica a: SSO de SAML 2.0 configurado con ID de Microsoft Entry (Azure AD), donde el dispositivo utiliza notificaciones de grupo SAML para la autorización (asignación de grupo).

Verificar registros de SSO

En el dispositivo Cisco Secure Email, recopile los registros de intentos de autenticación de inicio de sesión único (SSO) de los registros de la GUI. Por ejemplo, ejecute el comando:

```
grep -i sso gui_logs
```

Si el problema está relacionado con la asignación de grupo en la afirmación del proveedor de identidad (IdP), los registros de SSO pueden mostrar estos mensajes de error:

```
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 respuesta SAML

Para confirmar si el problema se debe a un número elevado de pertenencias a grupos, recopile un archivo de almacenamiento (HAR) del protocolo de transferencia de hipertexto (HTTP) durante un intento fallido de autenticación SAML. Utilice herramientas de desarrollador de navegadores o una extensión de navegador aprobada. No utilice descodificadores en línea públicos ni herramientas de carga de terceros para examinar la respuesta SAML.

Procedimiento:

1. Abra browser developer tools e inicie una captura de red.
2. Vaya a la interfaz web de Cisco Secure Email Gateway o Cisco Secure Email and Web Manager.
3. Inicie el flujo de inicio de sesión único (SSO) de SAML y reproduzca el error de autorización.

4. Exportar la sesión capturada como un archivo HAR.

Nota: Los pasos exactos varían según el navegador. Utilice un método de explorador compatible que mantenga la respuesta SAML local en la estación de trabajo.

Analizar archivo HAR

Utilice el archivo HAR para comprobar qué atributo de grupo devuelve Microsoft Entra ID en la afirmación SAML.

1. Abra el archivo HAR en las herramientas de desarrollador del navegador.
2. Localice la solicitud de respuesta SAML, como se muestra en la Imagen 1.
3. Copie el valor del campo SAMLResponse. En la Imagen 1, identifique el valor codificado entre las comillas después de value=.
4. Decodificar el valor SAMLResponse codificado con Base64 mediante un método sin conexión aprobado. Por ejemplo, utilice una utilidad de línea de comandos local:

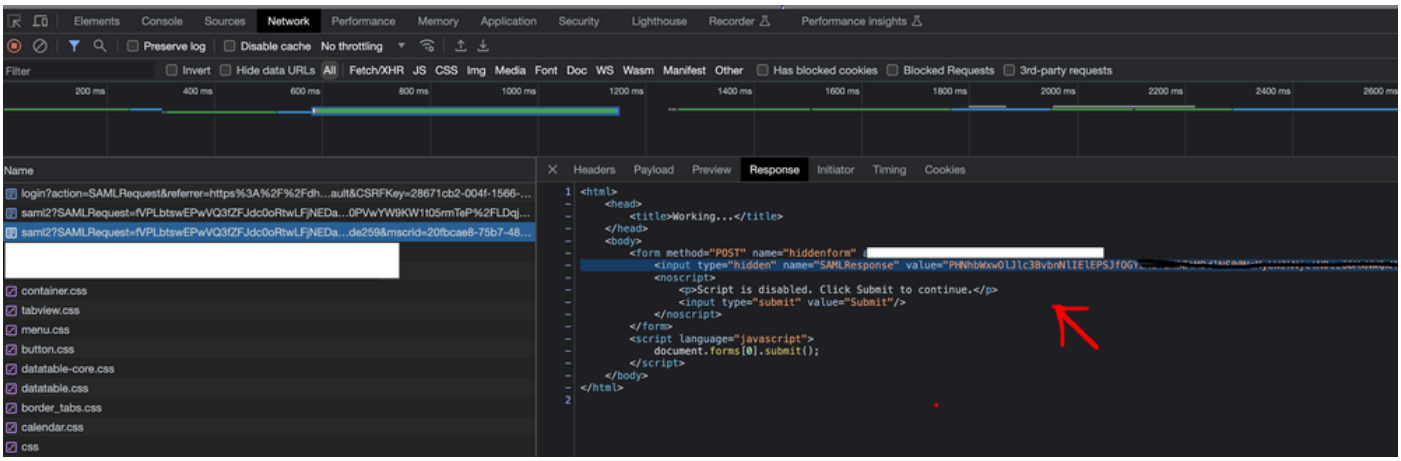
```
# macOS/Linux
printf '%s' "

       " | base64 --decode > saml_response.xml

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

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

5. Revise el código XML descodificado y compruebe si Microsoft Entry ID devuelve el atributo de grupos esperados o el atributo de vínculo alternativo.



Identificar comportamiento de reclamación de grupo de Azure

En un escenario de trabajo, la respuesta SAML descodificada contiene el atributo de grupos esperados: Esquemas de Microsoft: grupos de notificaciones de identidad . Cuando se produce este problema, Microsoft Entry ID devuelve Microsoft Schemas - Claims Groups en lugar del atributo de grupos esperado.

Este comportamiento se produce porque Microsoft Entra ID limita el número de grupos emitidos en la reclamación de grupos SAML. Si la afirmación SAML contiene más de 150 pertenencias a grupos, Azure AD devuelve el atributo groups.link en lugar del atributo groups. El dispositivo Cisco Secure Email no puede utilizar groups.link para la asignación de roles, por lo que la autorización falla.

Resolución

Modifique la aplicación Microsoft Entra ID para que la afirmación SAML devuelva una notificación de grupos utilizables para el dispositivo. El objetivo es evitar que Azure AD devuelva Microsoft Schemas - Claims Groups en lugar del atributo de grupos esperado.

1. En Azure AD, abra la aplicación empresarial que se utiliza para la autenticación de Cisco Secure Email Gateway o Cisco Secure Email and Web Manager SAML.
2. Navegue hasta la configuración de atributos del token SAML o de reclamaciones de grupo.

3. Cambie la configuración de notificaciones de grupo a Grupos asignados a la aplicación, si esa configuración cumple los requisitos de implementación.
4. Asegúrese de que la cuenta de administrador afectada esté asignada únicamente a los grupos requeridos para la autorización del dispositivo.
5. Guarde la configuración de Azure AD e inicie un nuevo intento de inicio de sesión SAML.
6. En el dispositivo, ejecute el comando grep -i so gui.current desde /data/pub/gui_logs y confirme que ya no se producen los errores de autorización anteriores.
7. Valide la respuesta decodificada de SAML y confirme que Azure AD devuelve Microsoft Schemas - Identity Claims Groups en lugar de Microsoft Schemas - Claims Groups.

Nota: Si la configuración de notificaciones de grupo de Azure AD necesaria no está disponible o no cumple los requisitos de implementación, póngase en contacto con el administrador de Microsoft Entry ID o el equipo de soporte técnico de Microsoft.

Información Relacionada

- Microsoft Learn: Configurar notificaciones de grupo para aplicaciones
- MuleSoft: Limitación de atributos de grupo de SAML de Azure AD

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).