Risoluzione dei problemi di corrispondenza del gruppo di Azure SAML per l'autenticazione esterna

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi agli errori di attestazione basata su gruppo SAML di Azure Active Directory per l'autenticazione esterna.

Prerequisiti

L'autenticazione esterna viene effettuata sui dispositivi Cisco Secure Email Gateway, Cisco Secure Email e Web Manager.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- L'SSO SAML 2.0 è già configurato e funzionante per almeno un account di test.

- Il mapping dei gruppi è abilitato sull'accessorio e configurato per l'utilizzo dell'attestazione basata su gruppi: Schemi Microsoft - Gruppo di attestazioni d'identità.
- Accedere a Entra ID per modificare la configurazione delle attestazioni basate su gruppo dell'applicazione.

Componenti usati

- Prodotti: Cisco Secure Email Gateway (ESA) e Cisco Secure Email e Web Manager (SMA), quando configurati per SAML 2.0 Single Sign-On (SSO).
- Provider di identità (IdP): ID Entra Microsoft (Azure AD).
- Metodo di autorizzazione: Assegnazione di ruoli/privilegi dell'accessorio in base alle attestazioni di gruppo SAML (mapping di gruppi).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Sintomi

- L'SSO ha esito positivo quando un utente viene mappato in modo esplicito (ad esempio in base all'ID utente), ma ha esito negativo quando l'autorizzazione si basa sul mapping di gruppo.
- Nei log SSO vengono visualizzati errori di mancata corrispondenza del mapping degli attributi o dei gruppi del gruppo.

Causa

Se un utente è membro di più di 150 gruppi, nell'asserzione SAML Microsoft Entra ID non genera l'attestazione basata su gruppi prevista (Microsoft Schemas - Identity Claims Group). Al contrario, genera Microsoft Schemas - Claims Group, che l'accessorio non può utilizzare per il mapping dei ruoli.

Risoluzione dei problemi

Si applica a: SSO SAML 2.0 configurato con Microsoft Entra ID (Azure AD) in cui l'accessorio utilizza le attestazioni di gruppo SAML per l'autorizzazione (mapping di gruppo).

Verifica log SSO

Sul dispositivo Cisco Secure Email, raccogliere i log dei tentativi di autenticazione Single Sign-On (SSO) dai log della GUI. Ad esempio, eseguire il comando:

```
grep -i sso gui_logs
```

Se il problema è relativo al mapping dei gruppi nell'asserzione del provider di identità (IdP), nei log SSO possono essere visualizzati i messaggi di errore seguenti:

```
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
```

Acquisisci risposta SAML

Per verificare se il problema è causato da un numero elevato di appartenenze ai gruppi, raccogliere un file HAR (Hypertext Transfer Protocol) Archive durante un tentativo di autenticazione SAML non riuscito. Utilizzare gli strumenti di sviluppo del browser o un'estensione del browser approvata. Non utilizzare decoder online pubblici o strumenti di caricamento di terze parti per ispezionare la risposta SAML.

Procedura:

1. Aprire gli strumenti di sviluppo browser e avviare un'acquisizione rete.
2. Passare all'interfaccia Web Cisco Secure Email Gateway o Cisco Secure Email e Web Manager.
3. Avviare il flusso SAML Single Sign-On (SSO) e riprodurre l'errore di autorizzazione.

4. Esporta la sessione acquisita come file HAR.

Nota: I passaggi esatti variano a seconda del browser. Utilizzare un metodo browser supportato che mantenga la risposta SAML locale nella workstation.

Analizza file HAR

Utilizzare il file HAR per verificare quale attributo di gruppo Microsoft Entra ID restituisce nell'asserzione SAML.

1. Aprire il file HAR negli strumenti di sviluppo del browser.
2. Individuare la richiesta di risposta SAML, come mostrato nell'Immagine 1.
3. Copiare il valore del campo SAMLResponse. Nell'immagine 1, identificare il valore codificato tra le virgolette dopo value=.
4. Decodificare il valore SAMLResponse con codifica Base64 utilizzando un metodo non in linea approvato. Ad esempio, utilizzare un'utilità della riga di comando locale:

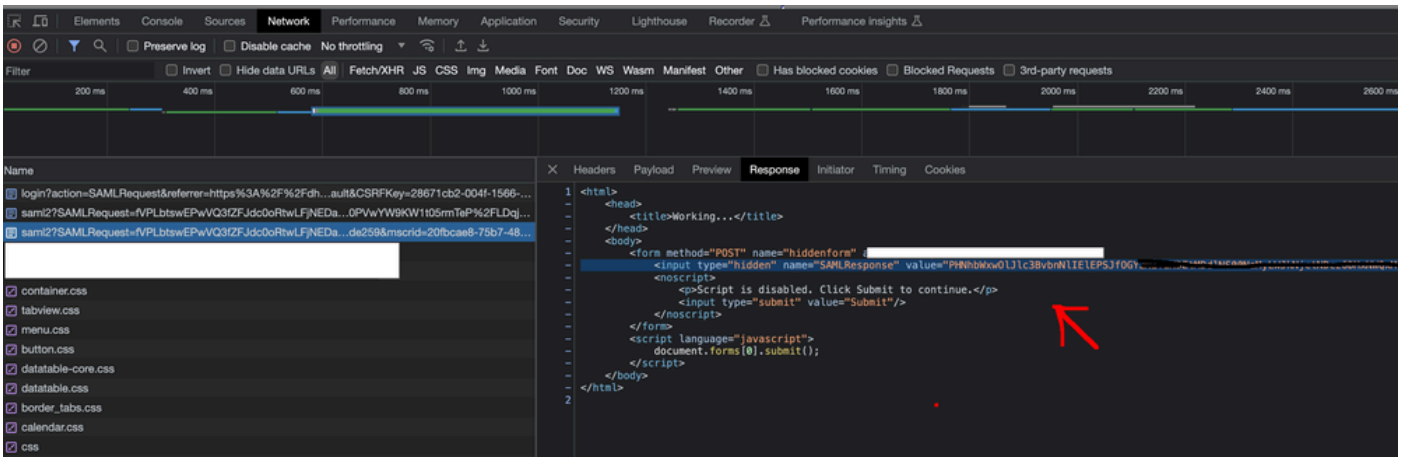
```
# macOS/Linux
printf '%s' "

       " | base64 --decode > saml_response.xml

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

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

5. Esaminare il file XML decodificato e verificare se Microsoft Entra ID restituisce l'attributo gruppi previsto o l'attributo collegamento alternativo.



Identifica comportamento di attestazione basata su gruppo di Azure

In uno scenario di lavoro, la risposta SAML decodificata contiene l'attributo groups previsto: Schemi Microsoft - Gruppi di attestazioni d'identità. Quando si verifica questo problema, Microsoft Entra ID restituisce Microsoft Schemas - Claims Groups anziché l'attributo groups previsto.

Questo comportamento si verifica perché Microsoft Entra ID limita il numero di gruppi emessi nell'attestazione dei gruppi SAML. Se l'asserzione SAML contiene più di 150 appartenenze a gruppi, Azure AD restituisce l'attributo groups.link anziché l'attributo groups. L'appliance Cisco Secure Email non può utilizzare groups.link per il mapping dei ruoli, pertanto l'autorizzazione non riesce.

Risoluzione

Modificare l'applicazione Microsoft Entra ID in modo che l'asserzione SAML restituisca un'attestazione basata su gruppi utilizzabili per l'accessorio. L'obiettivo è impedire ad Azure AD di restituire Schemi Microsoft - Gruppi attestazioni anziché l'attributo gruppi previsto.

1. In Azure AD aprire l'applicazione enterprise utilizzata per l'autenticazione SAML di Cisco Secure Email Gateway o Cisco Secure Email e Web Manager.
2. Passare alla configurazione SAML token attributes o group claim.
3. Modificare l'impostazione delle attestazioni di gruppo su Gruppi assegnati all'applicazione,

se tale impostazione soddisfa i requisiti di distribuzione.

4. Assicurarsi che l'account amministratore interessato sia assegnato solo ai gruppi richiesti per l'autorizzazione dell'accessorio.
5. Salvare la configurazione di Azure AD e avviare un nuovo log SAML nel tentativo.
6. Sull'accessorio, eseguire il comando grep -i sso gui.current da /data/pub/gui_logs e verificare che gli errori di autorizzazione precedenti non si verifichino più.
7. Convalidare la risposta SAML decodificata e verificare che Azure AD restituisca Microsoft Schemas - Identity Claims Groups anziché Microsoft Schemas - Claims Groups.

Nota: Se la configurazione richiesta delle attestazioni di gruppo di Azure AD non è disponibile o non soddisfa i requisiti di distribuzione, contattare l'amministratore di Microsoft Entra ID o il team del supporto tecnico Microsoft.

Informazioni correlate

- Informazioni su Microsoft: Configura attestazioni basate su gruppo per applicazioni
- MuleSoft Limitazione degli attributi del gruppo SAML di Azure AD

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).