외부 인증에 대한 SAML Azure 그룹 일치 실패 문제 해결

목차

소개

이 문서에서는 외부 인증에 대한 Azure Active Directory SAML 그룹 클레임 오류를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

외부 인증은 Cisco Secure Email Gateway, Cisco Secure Email 및 Web Manager 어플라이언스에서 수행됩니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SAML 2.0 SSO가 이미 구성되어 있으며 하나 이상의 테스트 계정에 대해 작동합니다.
- 그룹 매핑은 어플라이언스에서 활성화되며 다음과 같은 그룹 클레임을 사용하도록 구성됩니

다. Microsoft 스키마 - ID 클레임 그룹입니다.

- Entra ID에 액세스하여 애플리케이션의 그룹 클레임 컨피그레이션을 수정합니다.

사용되는 구성 요소

- 제품: Cisco ESA(Secure Email Gateway) 및 Cisco SMA(Secure Email and Web Manager)(SAML 2.0 SSO(Single Sign-On)에 대해 구성된 경우).
- IDp(ID 공급자): Microsoft Enterprise ID(Azure AD)입니다.
- 권한 부여 방법: SAML 그룹 클레임에 기반한 어플라이언스 역할/권한 할당(그룹 매핑).

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

증상

- SSO는 사용자가 명시적으로 매핑될 때(예: 사용자 ID로) 성공하지만 권한 부여가 그룹 매핑을 사용하는 경우에는 실패합니다.
- SSO 로그에는 그룹 특성 또는 그룹 매핑 불일치 오류가 표시됩니다.

원인

사용자가 150개가 넘는 그룹의 구성원인 경우 Microsoft Entra ID는 SAML assertion에서 예상 그룹 클레임(Microsoft Schemas - Identity Claims Group)을 내보내지 않습니다. 대신 어플라이언스에서 역할 매핑에 사용할 수 없는 Microsoft 스키마 - 클레임 그룹을 방출합니다.

문제 해결

적용 대상: 어플라이언스가 권한 부여(그룹 매핑)를 위해 SAML 그룹 클레임을 사용하는 Microsoft Azure AD(Enterprise ID)로 구성된 SAML 2.0 SSO.

SSO 로그 확인

Cisco Secure Email Appliance에서 SSO(Single Sign-On) 인증 시도 로그를 gui 로그에서 수집합니다. 예를 들어 다음 명령을 실행합니다.

```
grep -i sso gui_logs
```

문제가 IdP(Identity Provider) 어설션의 그룹 매핑과 관련된 경우 SSO 로그에 다음 오류 메시지가 표시될 수 있습니다.

```
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 응답 캡처

많은 수의 그룹 멤버십으로 인해 문제가 발생하는지 확인하려면 실패한 SAML 인증 시도 중에 HTTP(Hypertext Transfer Protocol) HAR(Archive) 파일을 수집합니다. 브라우저 개발자 도구 또는 승인된 브라우저 확장을 사용합니다. SAML 응답을 검사하기 위해 공용 온라인 디코더 또는 서드파티 업로드 툴을 사용하지 마십시오.

절차:

1. 브라우저 개발자 도구를 열고 네트워크 캡처를 시작합니다.
2. Cisco Secure Email Gateway 또는 Cisco Secure Email and Web Manager 웹 인터페이스로 이동합니다.
3. SAML SSO(Single Sign-On) 플로우를 시작하고 권한 부여 실패를 재현합니다.
4. 캡처된 세션을 HAR 파일로 내보냅니다.

참고: 정확한 단계는 브라우저마다 다릅니다. SAML 응답을 워크스테이션의 로컬로 유지하는 지원되는 브라우저 방법을 사용합니다.

HAR 파일 분석

HAR 파일을 사용하여 Microsoft Entra ID가 SAML assertion에서 반환하는 그룹 특성을 확인합니다
.

1. 브라우저 개발자 도구에서 HAR 파일을 엽니다.
2. 이미지 1과 같이 SAML 응답 요청을 찾습니다.
3. SAMLResponse 필드의 값을 복사합니다. 이미지 1에서 value=뒤에 있는 따옴표 사이에 인코딩된 값을 식별합니다.
4. 승인된 오프라인 방법을 사용하여 Base64 인코딩 SAMLResponse 값을 디코딩합니다. 예를 들어 로컬 명령줄 유틸리티를 사용합니다.

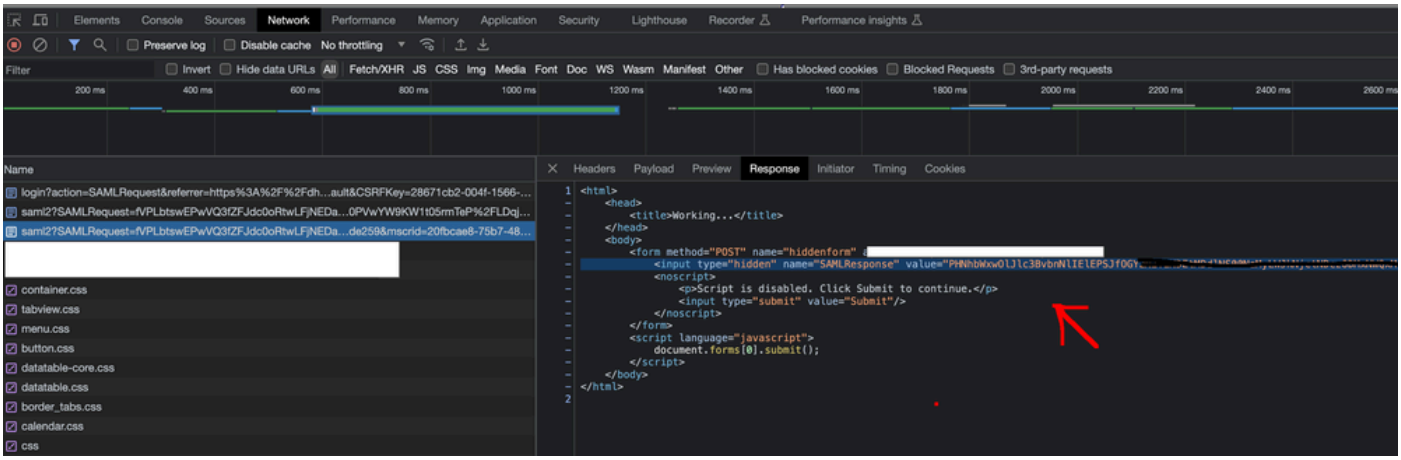
```
# macOS/Linux
printf '%s' "

        " | base64 --decode > saml_response.xml

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

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

5. 디코딩된 XML을 검토하고 Microsoft Entra ID가 예상 그룹 특성을 반환하는지 또는 대체 링크 특성을 반환하는지 확인합니다.



Azure 그룹 클레임 동작 식별

작업 시나리오에서 디코딩된 SAML 응답은 예상 그룹 특성을 포함합니다. Microsoft 스키마 - ID 클레임 그룹 . 이 문제가 발생하면 Microsoft Entra ID는 Microsoft Schemas - Claims Groups를 예상 그룹 특성 대신 반환합니다.

이 동작은 Microsoft Entra ID가 SAML 그룹 클레임에 있는 그룹 수를 제한하기 때문에 발생합니다. SAML 어설션에 150개가 넘는 그룹 멤버십이 포함되어 있으면 Azure AD는 그룹 특성 대신 groups.link 특성을 반환합니다. Cisco Secure Email Appliance는 역할 매핑에 groups.link를 사용할 수 없으므로 권한 부여가 실패합니다.

해결

SAML assertion이 어플라이언스에 대해 사용 가능한 그룹 클레임을 반환하도록 Microsoft Entra ID 애플리케이션을 수정합니다. Azure AD가 예상 그룹 특성 대신 Microsoft 스키마 - 클레임 그룹을 반환하지 않도록 하기 위한 것입니다.

1. Azure AD에서 Cisco Secure Email Gateway 또는 Cisco Secure Email and Web Manager SAML 인증에 사용되는 엔터프라이즈 응용 프로그램을 엽니다.
2. SAML 토큰 특성 또는 그룹 클레임 컨피그레이션으로 이동합니다.
3. 그룹 클레임 설정이 배포 요구 사항을 충족하는 경우 애플리케이션에 할당된 그룹으로 변경합니다.
4. 영향을 받는 관리자 계정이 어플라이언스 권한 부여를 위해 필요한 그룹에만 할당되었는지 확인합니다.
5. Azure AD 구성을 저장하고 새 SAML 로그를 시작합니다.
6. 어플라이언스에서 grep -i sso gui.current from /data/pub/gui_logs 명령을 실행하고 이전 권한 부여 오류가 더 이상 발생하지 않는지 확인합니다.
7. 디코딩된 SAML 응답의 유효성을 검사하고 Azure AD가 Microsoft Schemas - Microsoft Schemas - Claims Groups 대신 ID Claims Groups를 반환하는지 확인합니다.

참고: 필요한 Azure AD 그룹 클레임 구성을 사용할 수 없거나 배포 요구 사항을 충족하지 않는 경우 Microsoft Enterprise ID 관리자 또는 Microsoft 지원 팀에 문의하세요.

관련 정보

- Microsoft Learn: 애플리케이션에 대한 그룹 클레임 구성
- MuleSoft: Azure AD SAML 그룹 특성 제한

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.