Microsoft Azure AD에 대한 SAML 구성이 그룹을 매핑하지 않습니다.

적용 가능성

Splunk 클라우드

설명

SAML 인증은 Splunk 설명서에 따라 구성됩니다.
Microsoft Azure AD 또는 AD FS를 ID 공급자로 사용하는 SSO 구성
그러나 사용 권한이 제대로 매핑되지 않았습니다.

조사

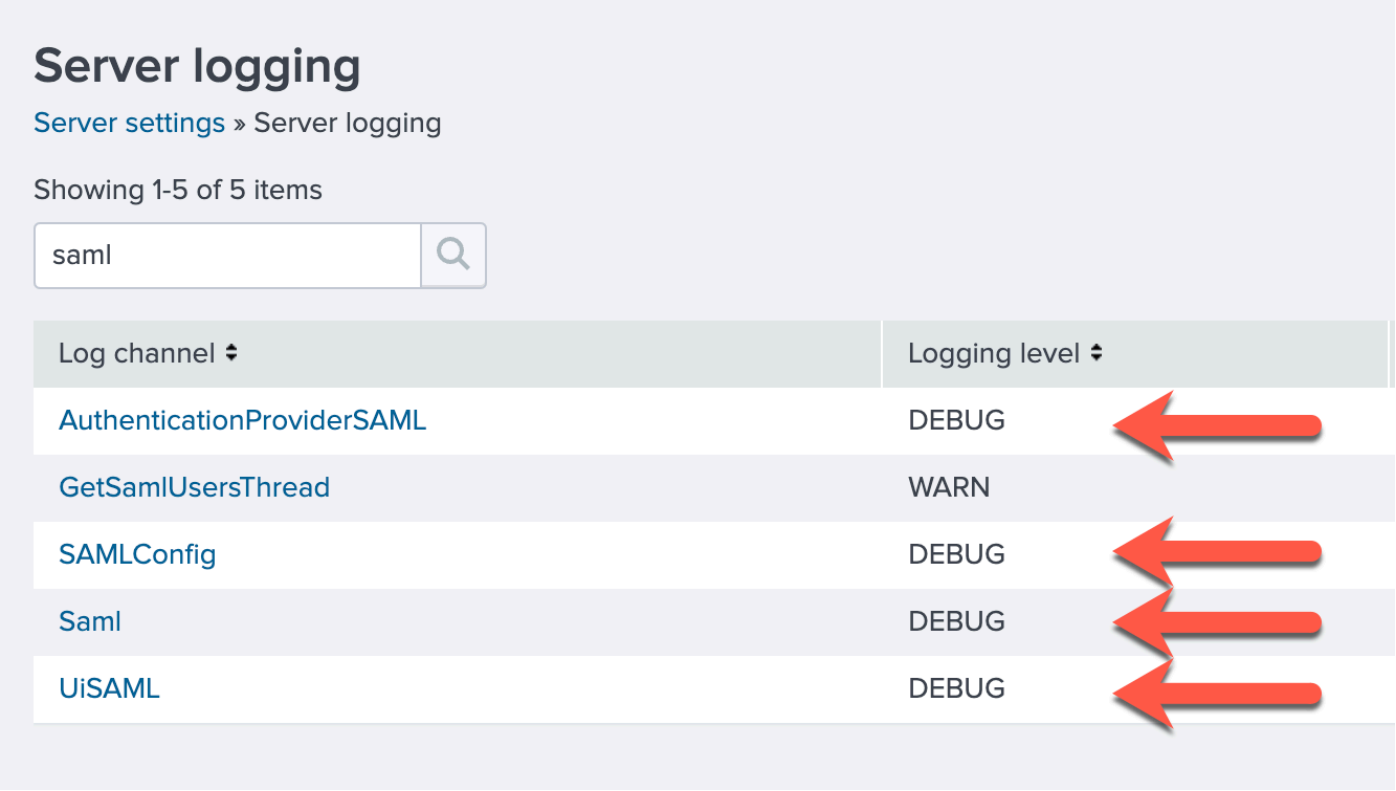
사용자가 Splunk 웹 UI에서 로그인을 시도할 때 다음 오류가 발생합니다.

```
'no valid role found in local mapping'
```

Splunk Cloud의 매핑 그룹이 일치하지 않습니다. 그룹 이름이 Azure AD 그룹의 ObjectId와 일치하지 않습니다. Splunk 매핑 그룹은 Splunk에서 매핑할 그룹의 Azure AD ObjectId를 사용하여 호출해야 합니다. 예를 들어, 다음 항목이 필요합니다.

매핑할 그룹의 Azure AD ObjectId: 99fvd7-fvddfv999-99999njhhb
Splunk 매핑 그룹 이름: 99fvd7-fvddfv99-99999njhhb

사용자가 로그인할 때 가지고 있는 그룹을 검증하려면 Splunk GUI에서 SAML에 대한 디버깅을 켭니다.



그런 다음 사용자가 다시 로그인하고 다음 SPL을 실행하여 반환되는 그룹을 확인합니다.

```
index=_internal sourcetype=splunkd samlp
```

여기에서 splunk의 saml 매핑이 IdP에서 반환되는 매핑과 일치하는지 확인할 수 있습니다.

해결

이 시나리오에서는 기존 매핑 그룹을 삭제하고 다시 만들어야 하므로 구성이 업데이트되고 IdP Azure AD 그룹에서 반환되는 항목과 일치해야 합니다. 매핑된 Azure AD 그룹의 사용자가 Splunk Cloud에 로그인하면 사용자가 인증 섹션의 Settings(설정) > Access Control(액세스 제어) > Users with SAML authentication type(SAML 인증 유형의 사용자)에 표시됩니다.

관련 링크

Microsoft Azure AD 또는 AD FS를 ID 공급자로 사용하는 SSO 구성

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.