

Splunk에서 이전 SAML 사용자를 제거하는 방법

적용 가능성

Splunk Cloud Splunk 엔터프라이즈 액세스 제어

설명

이 문서에서는 SAML 사용자 은퇴를 위한 모범 사례 기술에 대해 중점적으로 설명합니다.

조사

SAML은 단방향 페더레이션 표준으로 작동합니다. 이는 Splunk가 로그인 중에 IdP(Identity Provider)로부터 정보를 수신한다는 것을 의미합니다. 따라서 사용자가 IdP에서 삭제되면 Splunk는 업데이트를 수신하지 않습니다. 해당 사용자는 다시 로그인하지 않기 때문입니다.

사전 요구 사항:

1. KO(사용자 지식 객체) 관리

- 지식 객체 소유자가 부서나 회사를 떠나고 해당 Splunk 계정이 비활성화되면 소유한 지식 객체는 시스템에 남습니다. 이들은 고아 지식 객체입니다. 올바른 소유자가 없는 지식 개체는 문제를 일으킬 수 있습니다. 예를 들어, 분리된 조회 정의를 참조하는 검색은 작동하지 않을 수 있습니다.

2. 폐기할 SAML 사용자에게 속하는 모든 KO를 다시 할당하려면 아래 문서 링크에 설명된 단계를 수행하십시오.

[새 소유자에게 하나 이상의 공유 지식 객체 재할당](#)

해결

제거할 사용자가 연결된 KO를 다시 할당해야 합니다(위의 사전 요구 사항 참조).

옵션 1:

REST API를 통해 .conf 파일을 수정하여 SAML 사용자를 제거합니다.

CURL\REST API Example:

```
curl -k -u admin:{password} --request DELETE https://{hostname}:8089/services/admin/SAML
```

옵션 2:

Support(지원) > Splunk Cloud(Splunk 클라우드) > Cloud Change Request(클라우드 변경 요청) 티켓에서 제거할 사용자 목록을 [첨부합니다](#).

Splunk Support의 기능:

1. 제공된 사용자의 경우 \$SPLUNK_HOME/etc/users/<directories> 및 \$SPLUNK_HOME/etc/system/local/authentication.conf에서 백업을 가져옵니다.
2. 사용자 홈 디렉토리가 제거됩니다.
3. authentication.conf 파일의 [userToRoleMap_SAML] 문자 아래에서 사용 중지된 사용자에게 해당하는 줄이 삭제됩니다.
4. 디버그/새로 고침을 수행한 다음 웹 UI 화면 하단의 설정 > 액세스 제어 > 인증 방법 > SAML 설정 다시 로드에서 SAML 구성을 다시 로드하거나 인스턴스를 다시 시작하여 변경 사항을 적용합니다.

참고: 검색 헤드에 로그인한 적이 없는 SAML 사용자의 경우 위의 해결 방법에 따라 삭제할 필요가 없습니다. 다음 설정 > 사용자 > 필터 사용자 이름 > 편집 > 삭제를 통해 간단히 제거할 수 있습니다.

관련 링크

Splunk 설명서
[고아 검색 해결](#)

Splunk Answers
[이전 saml 사용자를 제거하려면 어떻게 합니까?](#)

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.