Cisco Security Cloud 제품에서 SAML 로그 수집

목차

소개

이 문서에서는 TAC 팀에서 로그인 문제를 트러블슈팅하고 조사하는 데 사용하는 Cisco Security Cloud Product에서 SAML 로그를 수집하는 단계를 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

문제/장애:

Cisco TAC에서는 SAML 로그를 사용하여 Cisco Security Cloud Product 로그인 문제와 관련된 문제를 해결합니다.
SAML 로그의 정보를 사용하여 TAC는 Cisco Security Cloud Product 백엔드 서버에 대한 추적을 분석하고 효율적으로 문제를 해결할 수 있습니다.

해결책:

SAML 로그 수집은 해당 로그를 가져오는 데 사용되는 브라우저에 따라 달라집니다.

크롬

1. 확장 추가 섹션에서 SAML 트레이서를 다운로드하고, 홈 > 확장 > SAML-트레이서로 이동하여, Add to Chrome > Add extension을 선택합니다
2. 확장자가 추가되면 브라우저의 오른쪽 위 모서리에 있는 세 개의 점 > More Tools > Developer

Tool로 이동합니다
3. [개발자 도구] 섹션의 맨 위에서 ">>" 옵션을 선택하고 SAML을 선택합니다
4. 문제 재현
5. SAML만 표시 확인란을 클릭합니다
6. 출력을 저장하고 TAC와 공유합니다.

파이어폭스

1. 이전 단계와 마찬가지로 SAML-tracer 도구를 Firefox에 추가하고, 권한 팝업이 표시되면 Add(추가)를 클릭한 다음 Okay(확인)를 클릭하고 비공개 창에서 확장을 사용하려면 확인란을 선택합니다
2. 브라우저의 오른쪽 상단 모서리에서 SAML-tracer 아이콘을 선택하고
3. 선택하면 다른 창이 나타나며, 이 때 로그인 문제를 재현할 수 있습니다. 시나리오를 복제한 후 출력을 복사하거나 가져와 파일을 Support Case Manage에 업로드하고 추가 조사를 위해 TAC 팀에 정보를 공유합니다

관련 정보

- 기술 지원 및 문서 – Cisco Systems

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.