SAML 인증 및 Bencode 사전 오류와 함께 Cisco Secure Client VPN 연결 실패

목차

문제

Google IdP에서 SAML 인증을 사용할 때 Cisco Secure Client를 사용하는 VPN 연결을 설정하지 못했습니다. IdP 측에서 SAML 인증이 성공하더라도 클라이언트는 인증 후 처리 중에 실패하고 연결이 끊긴 상태로 전환되어 VPN 터널을 생성할 수 없습니다.

환경

- Cisco Secure Client 버전 5.1.13.177
- Google IdP로 구성된 SAML 인증
- 보안 액세스 - 보안 클라이언트 원격 액세스(VPN, 보안 상태, 개인 리소스)
- Google IdP 인증 로그에 성공적인 SAML 인증 표시

해결

Cisco Secure Client를 다시 설치하여 문제가 해결되었습니다. 다음과 같은 트러블슈팅 접근 방식이 문서화되었습니다.

초기 진단 단계

1단계: 영향을 받는 엔드포인트에서 DART 로그 수집 -

https://www.cisco.com/c/en/us/support/docs/security/secure-client/221919-collect-dart-bundle-for-secure-client.html

Extract Dart Bundle(DART 번들 추출) > Cisco Secure client(Cisco 보안 클라이언트) > Anyconnect VPN > Logs(로그) > Under VPN Folder(VPN 폴더) > AnyConnectVPN.txt(AnyConnectVPN.txt에서) - 내부 설정을 읽는 동안 다음 오류가 표시되고 다음 오류가 계속 표시됩니다.

- Bencode 사전 내부화에 실패했습니다.
- Bencode 사전을 만들지 못했습니다.
- PHONEHOMEVPN_ERROR_UNEXPECTED
- GLOBAL_ERROR_INVOLVED

2단계: IdP 측에서 SAML 인증 상태 확인

Google IdP 로그에 성공적인 SAML 인증이 표시되어 클라이언트 측 사후 인증 처리로 문제를 격리하는지 확인합니다.

해결 구현

1단계: Cisco Secure Client 재설치

기존 Cisco Secure Client 설치를 제거하고 클라이언트 소프트웨어를 완전히 다시 설치합니다.

2단계: VPN 연결 복원 확인

다시 설치한 후 SAML 인증을 사용하여 VPN 연결을 테스트하여 연결이 성공적으로 설정되고 터널이 올바르게 생성되었는지 확인합니다.

Cisco Secure Client의 재설치로 VPN 기능이 복원되어 SAML 인증 및 터널 설정이 성공했습니다.

원인

근본 원인은 Cisco Secure Client 설치 내의 손상된 내부 컨피그레이션 데이터와 관련이 있으며, 특

히 인증 후 처리 중에 Bencode 사전 데이터를 처리하는 CPhoneHomeVpn/PhoneHomeAgent 구성 요소의 기능에 영향을 줍니다. 반복되는 "Bencode dictionary internalize failed" 및 "Bencode dictionary를 만들지 못했습니다." 오류는 클라이언트가 SAML 인증에 성공한 후 VPN 터널을 설정하는 데 필요한 내부 구성 데이터를 제대로 구문 분석하거나 처리할 수 없음을 나타냅니다.

이 문제는 클라이언트 재설치를 통해 해결되었으며, 서버 측 컨피그레이션 또는 IdP 통합 문제가 아닌 손상된 클라이언트 측 데이터와 관련된 문제임을 시사합니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.