SHA1 해싱 비호환성이 있는 엔드포인트 DLP 인증서 기반 자동 등록 실패

목차

문제

엔드포인트 DLP 등록은 반복되는 초기화 오류와 함께 인증서 기반 자동 등록 중에 실패합니다. 등록 프로세스에서 클라이언트 ID 인증서를 사용하여 인증할 수 없으므로 재시도가 계속됩니다.

다음 오류 메시지가 등록 로그에 표시됩니다.

```
[2026-02-05 13:24:58.154989] [info] [AutoEnrollMonitor.cpp:633] Auto-enrollment attempt #5 with enrollm
[2026-02-05 13:24:58.154989] [info] [SSEZtnaEnroller.cpp:185] Processing start event
[2026-02-05 13:24:58.155992] [info] [SSEZtnaEnroller.cpp:205] Starting Enrollment
[2026-02-05 13:24:58.398260] [error] [SSEZtnaEnroller.cpp:335] spIdentities count: 1
[2026-02-05 13:24:58.399259] [error] [SSEZtnaEnroller.cpp:355] None of the 1 user store client certific
[2026-02-05 13:24:58.407289] [info] [SSEZtnaEnroller.cpp:2237] Notifying enrollment completion with res
[2026-02-05 13:24:58.407289] [info] [SSEZtnaEnroller.cpp:2241]
Enrollment Stats
================
Authentication type           : certificate
Bootstrap                     : failure (0.251 sec)
----------------
Overall result                : failure (0.251 sec)
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:214] Notified of enrollment state change to
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:214] Notified of enrollment state change to
[2026-02-05 13:24:58.408287] [info] [AutoEnrollMonitor.cpp:615] Will retry the enrollment with enrollme
```

추가 TLS 레벨 인증 실패는 다음과 같은 오류 메시지와 함께 문서화됩니다. "수신된 TLS 알림: 치명적인/잘못된 인증서."

환경

- 기술: 솔루션 지원(SSPT - 계약 필요)
- 하위 기술: 보안 액세스 - 통합 정책(인터넷 정책, 개인 정책, DLP 정책, RBI, 보안 프로파일)

- 소프트웨어 버전: 모두
- 인증 방법: 인증서 기반 자동 등록
- 인증서 저장소: 사용자 저장소 클라이언트 인증서
- 인증서 해싱 알고리즘: SHA1(더 이상 사용되지 않음)

해결

이 확인에서는 지원되는 해싱 알고리즘으로 ID 인증서를 다시 생성하고 올바른 인증서 설치 및 컨피그레이션을 보장합니다.

1단계: 지원되는 해싱 알고리즘으로 ID 인증서 재생성

더 이상 사용되지 않는 SHA1 알고리즘 대신 SHA256 또는 SHA-3 해싱을 사용하여 ID 인증서를 생성하고 재발급합니다. 인증서는 다음 사양으로 생성해야 합니다.

- 해싱 알고리즘: SHA256 또는 SHA-3(SHA1은 지원되지 않음)
- 형식: PKCS#12(PFX) 형식
- 필수 필드: 등록을 위해 지정된 RFC822 이름이 있는 SAN 필드

2단계: 올바른 인증서 저장소에 업데이트된 인증서 설치

새로 생성된 인증서를 적절한 인증서 저장소 위치에 설치합니다.

- 인증서 저장소 위치: User/Machine Personal > Certificates store(인증서 저장소)
- 인증서 형식: PKCS#12(PFX)

3단계: 엔드포인트를 재부팅하여 인증 다시 트리거

업데이트된 인증서를 설치한 후 엔드포인트 시스템을 재부팅하여 인증 프로세스를 다시 트리거하고 등록 메커니즘이 새 인증서를 탐지하도록 합니다.

4단계: 비기업 네트워크에서 인증 테스트

에지 방화벽에 의한 SSL 검사 또는 암호 해독 간섭을 배제하려면 비기업 네트워크 환경에서 인증 프로세스를 테스트합니다. 이렇게 하면 등록 프로세스에 방해가 될 수 있는 잠재적인 네트워크 수준 인증서 검사 문제를 격리하는 데 도움이 됩니다.

5단계: 엔드포인트 DLP 등록 재시도

인증서 교체 및 시스템 리부팅을 완료한 후 엔드포인트 DLP 등록 프로세스를 다시 시도합니다. 등록 로그를 모니터링하여 인증 성공 및 등록 완료를 확인합니다.

원인

등록 실패는 클라이언트 ID 인증서에서 SHA1 해싱 알고리즘을 사용했기 때문에 발생합니다. SHA1은 더 이상 등록 정책 요구 사항에서 지원되지 않는 더 이상 사용되지 않는 암호화 해싱 알고리즘입니다. 등록 시스템은 특히 최신 보안 표준 및 정책 준수를 충족하기 위해 SHA256 또는 SHA-3과 같은 현대적이고 안전한 알고리즘으로 인증서를 해시하도록 요구합니다.

등록 프로세스가 등록 선택 정책에 대해 클라이언트 인증서를 검증할 때 더 이상 사용되지 않는 SHA1 해싱 알고리즘을 사용하는 인증서를 거부하므로, "None of the 1 user store client certificate(s) match the enrollment choice policy(s) match the enrollment choice policy)" 오류 메시지 및 후속 초기화 실패가 발생합니다.

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.