보안 액세스 리소스 커넥터 인증서 만료 및 OS 업그레이드 경고

목차

문제

리소스

VMware ESXi에 구축된 커넥터에 다음 오류가 표시됩니다.

1. 이 커넥터가 연결되었지만 구성을 동기화할 수 없습니다. 연결 문제를 해결하려면 진단을 실행하고 방화벽 설정을 확인하십시오

2. 컨피그레이션 상태

DNS 구성 또는 구성 상태를 검색할 수 없습니다. 방화벽 설정을 확인하십시오.

3. 커넥터 버전

알 수 없음

v2.0.85

(v2.0.93)

데이터가 오래된 것일 수 있습니다.

추가됨

2026년 1월 20일 오전 7:15 UTC

OS 버전

알 수 없음

2509300328

(2601240447)

- 데이터가 오래된 것일 수 있습니다.

환경

- Cisco Secure Access Resource Connectors 버전 2.0.85

- VMware ESXi 가상화 플랫폼
- HA 쌍으로 구축된 리소스 커넥터
- 방화벽 삭제 없음을 확인한 CSG 방화벽
- 라우팅 또는 NAT 변경 없이 네트워크 연결이 확인됨
- 동일한 방화벽, 라우팅, NAT 및 보안 정책을 사용하는 동일한 환경의 여러 리소스 커넥터 쌍
- 약 5주마다 반복되는 문제 패턴 발생

원인

두 RC에 모두 다음 오류가 표시됩니다. 컨트롤러 연결 설정 실패 오류 ="SetupControllerConnection::컨트롤러 연결 생성 실패 - 오류=연결 생성 실패: 네트워크 오류: 컨텍스트 마감일 초과"

RC의 연결에 문제가 없습니다. DNS는 정상입니다. 포트는 허용되지만 다음 URL에 대해서만 PING을 수행하지 못했습니다.

2026-02-12 14:26:39.736869500 SSE API -> [0;31mFAILED

2026-02-12 14:26:39.736870500 SSE ACME PureCA OCSP -> [0;31mFAILED

2026-02-12 14:26:39.736924500 ==========

2026-02-12 14:10:21.892855500

2026-02-12 14:10:21.892856500 ###ping SSE API: ping -w 5 -c 3 api.sse.cisco.com

2026-02-12 14:10:26.899046500 PING api.sse.cisco.com (146.112.59.20) 56(84) 바이트의 데이터
.

2026-02-12 14:10:26.899047500

2026-02-12 14:10:26.899048500 — api.sse.cisco.com ping 통계 —

2026-02-12 14:10:26.899048500 전송된 패킷 5개, 수신된 패킷 0개, 패킷 손실 100%, 시간 4082ms

2026-02-12 14:10:30.922958500 ###ping SSE ACME PureCA OCSP: ping -w 5 -c 3 ssepki-prd.pureca.cryptosvcs.cisco.com

2026-02-12 14:10:35.926673500 PING ssepki-prd.pureca.cryptosvcs.cisco.com (3.225.142.190) 56(84) 바이트의 데이터.

2026-02-12 14:10:35.926674500

2026-02-12 14:10:35.926709500 — ssepki-prd.pureca.cryptosvcs.cisco.com ping statistics —

2026-02-12 14:10:35.926709500 전송된 패킷 5개, 수신된 패킷 0개, 패킷 손실 100%, 시간 4078ms

2026-02-12 14:15:54.892666500 ========== Ping ==========

2026-02-12 14:15:54.892823500 셀프 -> [0;32m성공

2026-02-12 14:15:54.892879500 gateway -> 0;32mSUCCESS

2026-02-12 14:15:54.892964500 SSE API -> 0;31mFAILED

2026-02-12 14:15:54.893022500 SSE 인증서 API ->[0;32m성공

2026-02-12 14:15:54.893071500 SSE AC Headend -> 성공

2026-02-12 14:15:54.893144500 SSE ACME PureCA OCSP -> [0;31mFAILED

2026-02-12 14:15:54.893168500 ==========

위의 메시지는 오탐입니다.

RC가 SSE API에 대한 OCSP 확인을 시도할 때 OCSP 실패로 인해 해당 인증서가 갱신되었습니다. 로그에서 반환된 상태가 HTTP 403임을 확인할 수 있습니다.

026-02-12T14:23:26Z ERR에서 인증서 해지 오류를 확인할 수 없습니다. 오류="인증서 해지 상태를 확인하는 동안 오류가 발생했습니다. 오류=종료 상태

다음과 같은 디버그 행이 도움이 될 수 있습니다.

OCSP responder 쿼리 오류\n807BB6508C770000:error:1E800069:HTTP 루틴 :parse_http_line1:received error:../crypto/http/http_client.c:440:code=403, reason=Forbidden\n807BB6508C770000:error:1E800076:HTTP 루틴 :OSSL_HTTP_REQ_CTX_nbio:예기치 않은 콘텐츠 유형 :../crypto/http/http_client.c:676:expected=application/ocsp-response, actual=text/html; charset=\"utf-8\"\n807BB65008C770000:1error e800067:HTTP 루틴 :OSSL_HTTP_REQ_CTX_exchange:오류 수신 :../crypto/http/http_client.c:874:server=http://ssepki.cryptosvcs.cisco.com:80\n" func=VerifyCertificateStatus

2026-02-12T14:23:26Z INF 컨트롤러 연결 설정

방화벽에 차단이 있는 경우 http://ssepki.cryptosvcs.cisco.com:80에 대한 트래픽을 허용하면 더 많은 인증서 오류를 제거할 수 있습니다.

OS 업데이트

OS 업그레이드가 부족한 것은 기술적 한계와 ENG 팀이 VM 기반 RC에서 OS 업그레이드를 시도하지 않기로 결정한 다른 요인과 관련이 있습니다.

정기적으로 VM 기반 RC를 재구축하지 않는 것이 좋습니다. 컨테이너 기반 구축을 수행하면 팀이 컨테이너 호스트 OS의 업그레이드 및 유지 관리를 독립적으로 관리할 수 있습니다.

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.