Ablaufdatum des Zertifikats für den Connector der sicheren Zugriffsressource und Betriebssystem-Upgrade-Warnungen

Inhalt

Problem

Ressource

Connectors, die auf VMware ESXi bereitgestellt wurden, zeigen folgende Fehler an:

1. Dieser Connector ist angeschlossen, seine Konfiguration kann jedoch nicht synchronisiert werden. Führen Sie eine Diagnose aus, und überprüfen Sie die Firewall-Einstellungen, um Verbindungsprobleme zu beheben.

2. Konfigurationsstatus

DNS-Konfigurationen oder Konfigurationsstatus können nicht abgerufen werden. Überprüfen Sie Ihre Firewall-Einstellungen.

3. Steckerausführung

Unbekannt

Version 2.0.85

(Version 2.0.93)

Die Daten können veraltet sein.

Hinzugefügt

20.01.2026 07:15 UTC

Betriebssystemversion

Unbekannt

2509300328

(2601240447)

- Die Daten können veraltet sein.

Umwelt

- Cisco Secure Access Resource Connectors Version 2.0.85
- Virtualisierungsplattform VMware ESXi
- Ressourcen-Connectors in HA-Paaren bereitgestellt
- CSG-Firewall ohne Firewall-Drops
- Netzwerkverbindung ohne Routing- oder NAT-Änderungen bestätigt
- Mehrere Ressourcen-Connector-Paare in derselben Umgebung mit identischen Firewall-, Routing-, NAT- und Sicherheitsrichtlinien
- Wiederkehrendes Fehlermuster etwa alle 5 Wochen

Ursache

Beide RCs zeigen diesen Fehler an: Fehler beim Einrichten der Controller-Verbindung. Fehler="SetupControllerConnection::Fehler beim Erstellen der Controller-Verbindung - Fehler=Fehler beim Erstellen der Verbindung: Netzwerk-Fehler : Kontextzeitraum überschritten"

Es wurden keine Verbindungsprobleme von RC erkannt. Der DNS ist in Ordnung. Ports sind zulässig, aber PING ONLY an diese URLs ist fehlgeschlagen:

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) Bytes an Daten.

2026-02-12 14:10:26.899047500

2026-02-12 14:10:26.899048500 — api.sse.cisco.com Ping-Statistik —

2026-02-12 14:10:26.899048500 5 Pakete übertragen, 0 empfangen, 100% Paketverlust, Zeit 4082ms

12.02.2026, 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) Bytes an Daten.

2026-02-12 14:10:35.926674500

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

2026-02-12 14:10:35.926709500 5 Pakete übertragen, 0 empfangen, 100% Paketverlust, Zeit 4078ms

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

2026-02-12 14:15:54.892823500 Selbst -> [0;32mERFOLG

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-Zertifikat-API ->[0;32mSUCCESS

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

2026-02-12 14:15:54.89314500 SSE ACME PureCA OCSP -> [0;31mFAILED

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

Bei den vorhergehenden Meldungen handelt es sich um Fehlalarme.

Das fragliche Zertifikat wurde aufgrund von OCSP-Fehlern erneuert, wenn der RC versucht, OCSP auf die SSE-API zu überprüfen. In den Protokollen wird der Status HTTP 403 zurückgegeben:

026-02-12T14:23:26Z ERR konnte nicht auf Zertifikatsperrung überprüfen error="error validating certsperrung status err=exit status

Die folgenden Debug-Zeilen können hilfreich sein:

Fehler beim Abfragen der OCSP-Antwort\n807BB6508C770000:error:1E800069:HTTP-Routinen:parse_http_line1:received error:../crypto/http/http_client.c:440:code=403, reason=Verboten\n807BB6508C770000:error:1E800076:HTTP-Routinen:OSSL_HTTP_REQ_CTX_nbio:unerwarteter Inhaltstyp:../crypto/http/http_client.c:676:erwartet=application/ocsp-response, actual=text/html; charset=\"utf-8\"\n807BB77000058C800067:1C Routinen:OSSL_HTTP_REQ_CTX_exchange:error received:../crypto/http/http_client.c:874:server=http://ssepki.cryptosvcs.cisco.com:80\n" func=VerifyCertificateStatus

2026-02-12T14:23:26Z INF Controller-Verbindung einrichten

Wenn Sie Blöcke in der Firewall haben, können weitere Zertifikatfehler durch das Zulassen von Datenverkehr an http://ssepki.cryptosvcs.cisco.com:80\n verhindert werden.

Betriebssystem-Updates

Das Fehlen von Betriebssystem-Upgrades hängt mit technischen Einschränkungen und anderen Faktoren zusammen, die dazu beigetragen haben, dass das ENG-Team entschieden hat, keine Betriebssystem-Upgrades auf VM-basierten RCs zu versuchen.

Die Empfehlung, VM-basierte RCs nicht regelmäßig neu bereitstellen zu müssen, besteht darin, container-basierte Bereitstellungen durchzuführen, die es Ihrem Team ermöglichen, die Upgrades und die Wartung des Container-Host-Betriebssystems unabhängig zu verwalten.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.