Secure Access Resource Connector Certificate Expiration and OS Upgrade Warnings

Contents

Issue

Resource

Connectors deployed on VMware ESXi shows these errors:

1. This connector is connected, but its configuration cannot be synchronized. Run diagnostics and check firewall sett

2. Configuration status

Cannot retrieve DNS configurations or configuration status. Check your firewall settings.

3. Connector version

Unknown

v2.0.85

(v2.0.93)

The data can be out-of-date.

Added

Jan 20, 2026 7:15 AM UTC

OS Version

Unknown

2509300328

(2601240447)

- The data can be out-of-date.

Environment

- Cisco Secure Access Resource Connectors version 2.0.85
- VMware ESXi virtualization platform
- Resource Connectors deployed in HA pairs
- CSG firewall with confirmed no firewall drops
- Network connectivity confirmed with no routing or NAT changes
- Multiple Resource Connector pairs in the same environment with identical firewall, routing, NAT, and securit

- Recurring issue pattern occurring approximately every 5 weeks

Cause

Both RCs are showing this error: failed to setup controller connection error="SetupControllerConnection::Failed to c
err=failed to create connection: network Error : context deadline exceeded”

No issues with connectivity from RC are detected. The DNS is fine. Ports are allowed but PING ONLY to these UR

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 of data.

2026-02-12 14:10:26.899047500

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

2026-02-12 14:10:26.899048500 5 packets transmitted, **0 received**, 100% packet loss, time 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) bytes of data.

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 5 packets transmitted, **0 received**, 100% packet loss, time 4078ms

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

2026-02-12 14:15:54.892823500 self -> [0;32mSUCCESS

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 Certificate API ->[0;32mSUCCESS

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

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

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

The preceding messages are false positives.

The certificate in question renewed due to OCSP failures when the RC is attempting to check OCSP for the SSE API

026-02-
12T14:23:26Z ERR could not check for certificate revocation error="error validating cert revocation status err=exit s

These debug lines can be helpful:

Error querying OCSP responder\n807BB6508C770000:error:1E800069:HTTP routines:parse_http_line1:received er
response, actual=text/html; charset=\"utf-
8\"\n807BB6508C770000:error:1E800067:HTTP routines:OSSL_HTTP_REQ_CTX_exchange:error receiving:../cry

2026-02-12T14:23:26Z INF setting up controller connection

If you have blocks on the firewall, allowing traffic to http://ssepki.cryptosvcs.cisco.com:80\n can eliminate more Cer

OS Updates

The lack of OS upgrades is related to technical limitations and other factors that have contributed to the ENG team d

The recommendation to avoid having to redeployment VM based RCs on a regular basis is to do container-
based deployments which allows your team to manage the upgrades and upkeep of the container host OS independen

Related Content

- Cisco Technical Support & Downloads