Waarschuwingen voor verlopen van Secure Access Resource Connector-certificaat en upgrade van besturingssysteem

Inhoud

uitgeven

Bron

Connectors die op VMware ESXi zijn geïmplementeerd, vertonen de volgende fouten:

1. Deze connector is aangesloten, maar de configuratie ervan kan niet worden gesynchroniseerd. Diagnose uitvoeren en firewallinstellingen controleren om verbindingsproblemen op te lossen

2. Configuratiestatus

Kan geen DNS-configuraties of configuratiestatus ophalen. Controleer de instellingen van uw firewall.

3. Connectorversie

onbekend

v2.0.85

(v2.0.93)

De gegevens kunnen verouderd zijn.

toegevoegd

Jan 20, 2026 7:15 AM UTC

OS-versie

onbekend

2509300328

(2601240447)

- De gegevens kunnen verouderd zijn.

milieu

- Cisco Secure Access Resource Connectors versie 2.0.85
- VMware ESXi-virtualisatieplatform
- Bronconnectors geïmplementeerd in HA-paren
- CSG-firewall met bevestigde geen firewall daalt
- Netwerkconnectiviteit bevestigd zonder routering of NAT-wijzigingen
- Meerdere Resource Connector-koppelingen in dezelfde omgeving met hetzelfde firewall-, routing-, NAT- en beveiligingsbeleid
- Terugkerend uitgiftepatroon dat ongeveer elke 5 weken optreedt

Oorzaak

Beide RC's vertonen deze fout: controllerverbinding error="SetupControllerConnection::Controlerverbinding is niet gemaakt - err=verbinding is niet gemaakt: netwerk Error: context deadline overschreden"

Er worden geen problemen met de connectiviteit van RC gedetecteerd. De DNS is prima. Poorten zijn toegestaan, maar alleen ping naar deze URL's is mislukt:

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 aan gegevens.

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 pakketten verzonden, 0 ontvangen, 100% pakketverlies, tijd 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 aan gegevens.

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 pakketten verzonden, 0 ontvangen, 100% pakketverlies, tijd 4078ms

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

2026-02-12 14:15:54.892823500 ZELF -> [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 Certificaat API ->[0;32mSUCCESS

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

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

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

De voorgaande berichten zijn vals positief.

Het certificaat in kwestie is verlengd vanwege OCSP-fouten wanneer de RC OCSP probeert te controleren op de SSE API. In de logs kunt u zien dat de teruggegeven status HTTP 403 is:

026-02-12T14:23:26Z ERR kon niet controleren op fout bij certificaatintrekking="fout bij valideren van cert-intrekkingsstatus err=afsluitstatus

Deze foutopsporingsregels kunnen nuttig zijn:

Fout bij het opvragen van OCSP-responders\n807BB6508C770000:error:1E800069:HTTP routines:parse_http_line1:received error:../crypto/http/http_client.c:440:code=403, reason=Forbidden\n807BB6508C770000:error:1E800076:HTTP routines:OSSL_HTTP_REQ_CTX_nbio:unexpected content type: ../crypto/http/http_client.c:676:expected=application/ocsp-response, actual=text/html; charset=\"utf-8\"\n807BB6508C770000:error:1E800067:HTTP routines:OSSL_HTTP_REQ_CTX_exchange:error receiving:../crypto/http/http_client.c:874:server=http://ssepki.cryptosvcs.cisco.com:80\n" func=VerifyCertificateStatus

2026-02-12T14:23:26Z INF instellen controller verbinding

Als u blokken op de firewall hebt, kunt u met verkeer naar http://ssepki.cryptosvcs.cisco.com:80\n meer Cert-fouten elimineren.

Updates van het besturingssysteem

Het gebrek aan OS-upgrades houdt verband met technische beperkingen en andere factoren die ertoe hebben bijgedragen dat het ENG-team heeft besloten geen OS-upgrades te proberen op VM-gebaseerde RC's.

De aanbeveling om te voorkomen dat op VM gebaseerde RC's regelmatig opnieuw moeten worden geïmplementeerd, is om op containers gebaseerde implementaties uit te voeren waarmee uw team de upgrades en het onderhoud van het besturingssysteem van de containerhost onafhankelijk kan beheren.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.