Avvisi di scadenza del certificato del connettore di risorse per l'accesso sicuro e di aggiornamento del sistema operativo

Sommario

Problema

Risorsa

I connettori implementati su VMware ESXi mostrano i seguenti errori:

1. Il connettore è connesso, ma non è possibile sincronizzarne la configurazione. Eseguire gli strumenti di diagnostica e controllare le impostazioni del firewall per risolvere i problemi di connettività

2. Stato della configurazione

Impossibile recuperare le configurazioni DNS o lo stato della configurazione. Controllare le impostazioni del firewall.

3. Versione connettore

Sconosciuto

v2.0.85

(v2.0.93)

I dati possono essere obsoleti.

Aggiunto

20 gen 2026 7:15 UTC

Versione del sistema operativo

Sconosciuto

2509300328

(2601240447)

- I dati possono essere obsoleti.

Ambiente

- Cisco Secure Access Resource Connector versione 2.0.85
- Piattaforma di virtualizzazione VMware ESXi
- Connettori di risorse distribuiti in coppie HA
- Firewall CSG con nessuna perdita confermata del firewall
- Connettività di rete confermata senza routing o modifiche NAT
- Più coppie di connettori di risorse nello stesso ambiente con identici criteri di firewall, routing, NAT e sicurezza
- Modello di problema ricorrente che si verifica approssimativamente ogni 5 settimane

Causa

Errore visualizzato da entrambe le RFC: impossibile configurare la connessione del controller errore="SetupControllerConnection::Failed to create controller connection - err=failed to create connection: network Error : context limit exceeded" (errore di rete: scadenza contesto superata)

Non sono stati rilevati problemi di connettività da RC. Il DNS funziona correttamente. Le porte sono consentite, ma il PING SOLO per questi URL non è riuscito:

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 14:10:26.89046500 PING api.sse.cisco.com (146.112.59.20) 56(84) byte di dati.

2026-02-12 14:10:26,899047500

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

2026-02-12 14:10:26,899048500 5 pacchetti trasmessi, 0 ricevuti, 100% perdita di pacchetti, tempo 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) byte di dati.

2026-02-12 14:10:35,926674500

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

2026-02-12 14:10:35,926709500 5 pacchetti trasmessi, 0 ricevuti, 100% perdita di pacchetti, tempo 4078 ms

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 Headend AC -> SUCCESSO

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

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

I messaggi precedenti sono falsi positivi.

Il certificato in questione è stato rinnovato a causa di errori OCSP durante il tentativo da parte di RC di controllare OCSP per l'API SSE. Nei registri è possibile verificare che lo stato restituito è HTTP 403:

026-02-12T14:23:26Z ERR non è stato in grado di verificare la presenza di un errore di revoca del certificato="errore di convalida dello stato di revoca del certificato err=stato di uscita

Le righe di debug seguenti possono essere utili:

Errore durante la query sul risponditore OCSP\n807BB6508C770000:error:1E800069:HTTP routines:parse_http_line1:received error:../crypto/http/http_client.c:440:code=403, reason=Forbidden\n807BB6508C770000:error:1E800076:HTTP routine:OSSL_HTTP_REQ_CTX_nbio:tipo di contenuto imprevisto:../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 receive:../crypto/http/http_client.c:874:server=http://ssepki.cryptosvcs.cisco.com:80\Certificaten"

2026-02-12T14:23:26Z INF impostazione connessione controller

Se nel firewall sono presenti blocchi, consentendo al traffico di http://ssepki.cryptosvcs.cisco.com:80\n è possibile eliminare un numero maggiore di errori relativi ai certificati.

Aggiornamenti del sistema operativo

La mancanza di aggiornamenti del sistema operativo è dovuta a limitazioni tecniche e ad altri fattori che hanno contribuito a far sì che il team ENG decidesse di non tentare gli aggiornamenti

del sistema operativo su RC basati su VM.

Per evitare di dover ridistribuire RFC basati su VM su base regolare, si consiglia di eseguire distribuzioni basate su container che consentano al team di gestire gli aggiornamenti e la manutenzione del sistema operativo host del contenitore in modo indipendente.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).