Advertencias sobre vencimiento de certificado y actualización de SO del conector de recursos de acceso seguro

Contenido

Problema

Recurso

Los conectores implementados en VMware ESXi muestran estos errores:

1. Este conector está conectado, pero su configuración no se puede sincronizar. Ejecute el diagnóstico y compruebe la configuración del firewall para solucionar problemas de conectividad

2. Estado de la configuración

No se pueden recuperar las configuraciones DNS o el estado de la configuración. Compruebe la configuración del firewall.

3. Versión del conector

Desconocido

v2.0.85

(v2.0.93)

Los datos pueden estar obsoletos.

Agregado

20 de enero de 2026 07:15 UTC

Versión de SO

Desconocido

2509300328

(2601240447)

- Los datos pueden estar obsoletos.

Entorno

- Cisco Secure Access Resource Connectors versión 2.0.85
- Plataforma de virtualización VMware ESXi
- Conectores de recursos implementados en pares HA
- Firewall CSG sin caídas confirmadas del firewall
- Conectividad de red confirmada sin routing ni cambios de NAT
- Varios pares de conectores de recursos en el mismo entorno con firewall, routing, NAT y políticas de seguridad idénticos
- Patrón de problemas recurrentes que ocurren aproximadamente cada 5 semanas

Causa

Ambos RC muestran este error: error al configurar la conexión del controlador error="SetupControllerConnection::Failed to create controller connection - err=failed to create connection: network Error: context deadline exceeded"

No se detectaron problemas con la conectividad de RC. El DNS está bien. Los puertos están permitidos pero el PING SOLO a estas URLs falló:

2026-02-12 14:26:39.736869500 API SSE -> [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 de datos.

2026-02-12 14:10:26.899047500

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

2026-02-12 14:10:26.899048500 5 paquetes transmitidos, 0 recibidos, 100% pérdida de paquetes, tiempo 4082 ms

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 sepki-prd.pureca.cryptosvcs.cisco.com (3.225.142.190) 56(84) bytes de datos.

2026-02-12 14:10:35.926674500

2026-02-12 14:10:35.926709500 — sepki-prd.pureca.cryptosvcs.cisco.com estadísticas de ping —

2026-02-12 14:10:35.926709500 5 paquetes transmitidos, 0 recibidos, 100% pérdida de paquetes, tiempo 4078ms

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

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

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

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

2026-02-12 14:15:54.893022500 API de certificado SSE ->[0;32mSUCCESS

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

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

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

Los mensajes anteriores son falsos positivos.

El certificado en cuestión se renovó debido a errores de OCSP cuando el RC está intentando comprobar OCSP para la API SSE. En los registros, puede ver que el estado devuelto es HTTP 403:

02-02-12T14:23:26Z ERR no pudo comprobar el error de revocación del certificado="error al validar el estado de revocación del certificado err=estado de salida

Estas líneas de depuración pueden ser útiles:

Error al consultar al respondedor OCSP\n807BB6508C770000:error:1E800069:rutinas HTTP:parse_http_line1:received error:../crypto/http/http_client.c:440:code=403, reason=Forbidden\n807BB6508C770000:error:1E800076:rutinas HTTP:OSSL_HTTP_REQ_CTX_nbio:contenido inesperado type:../crypto/http/http_client.c:676:waiting=application/ocsp-response, actual=text/html; charset=\"utf-8\"\n807BB6508C770000:error:1E800067:rutinas HTTP: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 configurar la conexión del controlador

Si tiene bloques en el firewall, permitir el tráfico a http://ssepki.cryptosvcs.cisco.com:80\n puede eliminar más errores de certificado.

Actualizaciones de SO

La falta de actualizaciones del sistema operativo está relacionada con limitaciones técnicas y otros factores que han contribuido a que el equipo de ENG decida no intentar realizar actualizaciones del sistema operativo en RC basadas en VM.

La recomendación para evitar tener que volver a implementar los RC basados en VM de forma regular es realizar implementaciones basadas en contenedores que permitan a su equipo gestionar las actualizaciones y el mantenimiento del sistema operativo del host del contenedor de forma independiente.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).