Avisos de Expiração do Certificado do Conector de Recursos de Acesso Seguro e Atualização do SO

Contents

Problema

Recurso

Os conectores implantados no VMware ESXi mostram estes erros:

1. Este conector está conectado, mas sua configuração não pode ser sincronizada. Execute diagnósticos e verifique as configurações do firewall para solucionar problemas de conectividade

2. Status da configuração

Não é possível recuperar as configurações DNS ou o status da configuração. Verifique as configurações de firewall.

3. Versão do conector

Desconhecido

v2.0.85

(v2.0.93)

Os dados podem estar desatualizados.

Adicionado

20 de janeiro de 2026 07:15 UTC

Versão do SO

Desconhecido

2509300328

(2601240447)

- Os dados podem estar desatualizados.

Ambiente

- Cisco Secure Access Resource Connectors versão 2.0.85
- Plataforma de virtualização VMware ESXi
- Conectores de recursos implantados em pares HA
- Firewall CSG sem quedas de firewall confirmadas
- Conectividade de rede confirmada sem alterações de roteamento ou NAT
- Vários pares de conectores de recursos no mesmo ambiente com políticas idênticas de firewall, roteamento, NAT e segurança
- Padrão de problemas recorrentes ocorrendo aproximadamente a cada 5 semanas

Causa

Ambos os RCs estão mostrando este erro: falha ao configurar conexão do controlador error="SetupControllerConnection::Falha ao criar conexão do controlador - err=falha ao criar conexão: rede Erro: prazo final do contexto excedido"

Não foram detectados problemas de conectividade com RC. O DNS está funcionando bem. As portas são permitidas, mas o PING SOMENTE para estas URLs falhou:

2026-02-12 14:26:39.736869500 API SSE -> [0;31mFALHA

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 API SSE: 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 dados.

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 pacotes transmitidos, 0 recebidos, 100% de perda de pacotes, 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) bytes de dados.

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 pacotes transmitidos, 0 recebidos, 100% de perda de pacotes, tempo 4078ms

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

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

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

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

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

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

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

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

As mensagens anteriores são falsos positivos.

O certificado em questão foi renovado devido a falhas OCSP quando o RC estava tentando verificar o OCSP para a API SSE. Nos logs, você pode ver que o status retornado é HTTP 403:

026-02-12T14:23:26Z O ERR não pôde verificar a revogação do certificado error="erro ao validar o status de revogação do certificado err=status de saída

Estas linhas de depuração podem ser úteis:

Erro ao consultar o respondente OCSP\n807BB6508C770000:erro:1E800069:HTTP rotinas:parse_http_line1:erro recebido:../crypto/http/http_client.c:440:code=403, motivo=Proibido\n807BB6508C770000:erro:1E800076:HTTP rotinas:OSSL_HTTP_REQ_CTX_nbio:tipo de conteúdo inesperado:../crypto/http/http_client.c:676:expected=application/ocsp-response, atual=text/html; charset=\"utf-8\"\n807BB6508C770000:error:1E800067:HTTP rotinas:OSSL_HTTP_REQ_CTX_exchange:erro ao receber:../crypto/http/http_client.c:874:server=http://ssepki.cryptosvcs.cisco.com:80\n" func=VerifyCertificateStatus

2026-02-12T14:23:26Z INF configurando a conexão do controlador

Se você tiver blocos no firewall, permitir o tráfego para http://ssepki.cryptosvcs.cisco.com:80\n poderá eliminar mais erros de certificado.

Atualizações do SO

A falta de atualizações do SO está relacionada a limitações técnicas e outros fatores que contribuíram para a equipe da ENG decidir não tentar atualizações do SO em RCs baseados em VMs.

A recomendação para evitar ter que reimplantar RCs baseados em VM regularmente é fazer implantações baseadas em contêiner, o que permite que sua equipe gerencie as atualizações e a manutenção do SO do host contêiner de forma independente.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.