Expiration du certificat du connecteur de ressources d'accès sécurisé et avertissements de mise à niveau OS

Table des matières

Problème

Ressource

Les connecteurs déployés sur VMware ESXi présentent les erreurs suivantes :

1. Ce connecteur est connecté, mais sa configuration ne peut pas être synchronisée. Exécutez des diagnostics et vérifiez les paramètres du pare-feu pour résoudre les problèmes de connectivité

2. État de la configuration

Impossible de récupérer les configurations DNS ou l'état de configuration. Vérifiez les paramètres de votre pare-feu.

3. Version du connecteur

Inconnu

v 2.0.85

(v 2.0.93)

Les données peuvent ne pas être à jour.

Ajouté

Jan 20, 2026 7:15 UTC

Version du système d'exploitation

Inconnu

2509300328

(2601240447)

- Les données peuvent ne pas être à jour.

Environnement

- Connecteurs de ressources Cisco Secure Access version 2.0.85
- Plate-forme de virtualisation VMware ESXi
- Connecteurs de ressources déployés par paires haute disponibilité
- Pare-feu CSG avec confirmation qu'aucun pare-feu n'est supprimé
- Connectivité réseau confirmée sans modification du routage ou de la NAT
- Plusieurs paires de connecteurs de ressources dans le même environnement avec des politiques de pare-feu, de routage, de NAT et de sécurité identiques
- Modèle de problème récurrent toutes les 5 semaines environ

Motif

Les deux RC affichent cette erreur : failed to setup controller connection error="SetupControllerConnection::Failed to create controller connection - err=failed to create connection: network Error : context delay beyond"

Aucun problème de connectivité à partir de RC n'a été détecté. Le DNS est correct. Les ports sont autorisés, mais la commande PING ONLY vers ces URL a échoué :

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 (146.12.59.20) 56(84) octets de données.

2026-02-12 14:10:26.899047500

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

2026-02-12 14:10:26.899048500 5 paquets transmis, 0 reçu, 100% de perte de paquets, durée 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 sepki-prd.pureca.cryptosvcs.cisco.com (3.225.142.190) 56(84) octets de données.

2026-02-12 14:10:35.926674500

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

2026-02-12 14:10:35.926709500 5 paquets transmis, 0 reçu, 100% de perte de paquets, temps 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 Tête de réseau CA SSE -> RÉUSSITE

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

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

Les messages précédents sont des faux positifs.

Le certificat en question a été renouvelé en raison d'échecs OCSP lorsque le RC tente de vérifier OCSP pour l'API SSE. Dans les journaux, vous pouvez voir que le statut renvoyé est HTTP 403 :

026-02-12T14:23:26Z ERR n'a pas pu vérifier l'erreur de révocation de certificat="error validating cert revocation status err=exit status

Ces lignes de débogage peuvent être utiles :

Erreur lors de l'interrogation du répondeur 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 routines:OSSL_HTTP_REQ_CTX_nbio:unknown content type:../crypto/http/http_client.c:676:required=application/ocsp-response, real=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\n" func=VerifyCertificateStatus

2026-02-12T14:23:26Z INF configuration de la connexion du contrôleur

Si vous avez des blocs sur le pare-feu, autoriser le trafic vers http://ssepki.cryptosvcs.cisco.com:80\n peut éliminer davantage d'erreurs de certification.

Mises à jour OS

L'absence de mises à niveau du système d'exploitation est liée à des limitations techniques et à d'autres facteurs qui ont incité l'équipe ENG à décider de ne pas tenter de mettre à niveau le système d'exploitation sur des RC basés sur VM.

Il est recommandé d'éviter de redéployer régulièrement des RC basés sur des machines virtuelles en effectuant des déploiements basés sur des conteneurs, ce qui permet à votre équipe de gérer les mises à niveau et la maintenance du système d'exploitation hôte du conteneur de manière indépendante.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.