Secure Accessリソースコネクタの証明書の有効期限とOSアップグレードの警告

内容

お問い合わせ内容

Resource

VMware ESXiに導入されたコネクタに次のエラーが表示されます。

1. このコネクタは接続されていますが、構成を同期できません。 診断を実行し、ファイアウォールの設定を確認して接続の問題をトラブルシューティングする

2. 設定状況

DNS構成または構成の状態を取得できません。 ファイアウォールの設定を確認します。

3. コネクタバージョン

Unknown

v2.0.85

(v2.0.93)

データは古くなる可能性があります。

Added（追加）

2026年1月20日午前7:15 UTC

OSバージョン

Unknown

2509300328

（2601240447）

- データは古くなる可能性があります。

環境

- Cisco Secure Access Resource Connectorバージョン2.0.85

- VMware ESXi仮想化プラットフォーム
- HAペアで導入されるリソースコネクタ
- ファイアウォールのドロップが確認されていないCSGファイアウォール
- ルーティングやNATの変更なしでネットワーク接続が確認される
- 同一のファイアウォール、ルーティング、NAT、およびセキュリティポリシーを持つ同一環境内の複数のリソースコネクタペア
- 約5週間ごとに繰り返し発生する問題パターン

原因

両方のRCで次のエラーが表示されています。「failed to setup controller connection error="SetupControllerConnection::Failed to create controller connection - err=failed to create connection: network Error : context deadline exceeded"

RCからの接続に関する問題は検出されませんでした。 DNSは正常です。 ポートは許可されますが、次のURLへのPING ONLYが失敗しました。

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)バイトのデータ。

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パケット送信、0受信、100 %パケット損失、時間4082ミリ秒

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)バイトのデータ。

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パケット送信、0受信、100 %パケット損失、時間4078ミリ秒

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証明書API ->[0;32mSUCCESS

2026-02-12 14:15:54.893071500上海ACヘッドエンド – >成功

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

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

上記のメッセージは誤検出です。

RCがSSE APIのOCSPを確認しようとしたときに、OCSPの障害により問題の証明書が更新されました。 ログで、返されたステータスがHTTP 403であることを確認できます。

026-02-12T14:23:26Z ERR could not check for certificate revocation error="error validating cert revocation status err=exit status

次のデバッグ行が役立ちます。

OCSPレスポンダの問い合わせエラー\n807BB6508C770000:error:1E800069:HTTPルーチン：parse_http_line1:received error:../crypto/http/http_client.c:440:code=403, reason=Forbidden\n807BB6508C770000:error:1E800076:HTTPルーチン：OSSL_HTTP_REQ_CTX_nbio：予期しないコンテンツタイプ：../crypto/http/http_client.c:676:expected=application/ocsp-response, actual=text/html; charset=\"utf-8\"\n807BB6508C770000:error:1E800067:HTTPルーチン：OSSL_HTTP_REQ_CTX_exchange：エラー受信：../crypto/http/http_client.c:874:server=http://ssepki.cryptosvcs.cisco.com:80\n" func=VerifyCertificateStatus

2026-02-12T14:23:26Z INFコントローラ接続の設定

ファイアウォールでブロックがある場合、http://ssepki.cryptosvcs.cisco.com:80\nへのトラフィックを許可することで、より多くの証明書エラーを排除できます。

OSのアップデート

OSアップグレードの欠如は、技術上の制約やその他の要因が原因で、VMベースのRCでOSアップグレードを行わないことをENGチームが決定したことによるものです。

VMベースのRCを定期的に再導入する必要がないようにするための推奨事項は、コンテナベースの導入を行うことです。これにより、チームはコンテナホストOSのアップグレードと維持管理を個別に管理できます。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。