安全訪問資源聯結器證書到期和作業系統升級警告

目錄

問題

資源

在VMware ESXi上部署的聯結器顯示以下錯誤：

1.此聯結器已連線，但無法同步其配置。運行診斷並檢查防火牆設定以解決連線問題

2.配置狀態

無法檢索DNS配置或配置狀態。請檢查您的防火牆設定。

3.聯結器版本

未知

v2.0.85

(v2.0.93)

資料可能已過時。

已新增

世界協調時2026年1月20日7點15分

OS版本

未知

2509300328

(2601240447)

- 資料可能已過時。

環境

- 思科安全存取資源聯結器版本2.0.85
- VMware ESXi虛擬化平台

- 以HA對部署的資源聯結器
- CSG防火牆，確認無防火牆丟棄
- 網路連線已確認，無路由或NAT更改
- 同一環境中的多個資源聯結器對具有相同的防火牆、路由、NAT和安全策略
- 大約每5週重複發生一次的問題模式

原因

兩個RC都顯示以下錯誤：無法設定控制器連線error="SetupControllerConnection:：無法建立控制器連線 — err=無法建立連線：網路錯誤：超出上下文期限"

未檢測到來自RC的連線問題。DNS正常。允許使用埠，但僅對以下URL執行PING操作失敗：

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

2026-02-12 14:26:39.736870500 SSE ACME PureCA OCSP -> [0;31m失敗

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)位元組資料。

2026-02-12 14:10:26.899047500

2026-02-12 14:10:26.899048500 — api.sse.cisco.com ping統計資訊 —

2026-02-12 14:10:26.899048500 5個資料包已傳輸，0個已接收，100%資料包丟失，時間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)個位元組的資料。

2026-02-12 14:10:35.926674500

2026-02-12 14:10:35.926709500 — ssepki-prd.pureca.cryptosvcs.cisco.com ping統計資訊 —

2026-02-12 14:10:35.926709500 5 packets transmitted， 0 received, 100% packet loss， time 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網關 — > 0;32mSUCCESS

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

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

2026-02-12 14:15:54.893071500 SSE AC頭端 — >成功

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

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

上述消息為誤報。

當RC嘗試檢查OCSP的SSE API時，由於OCSP故障而續訂了相關證書。在日誌中，您可以看到返回的狀態是HTTP 403:

026-02-12T14:23:26Z ERR無法檢查證書吊銷錯誤="error validating cert revocation status err=exit status

以下調試行可能很有用：

查詢OCSP響應程式時出錯\n807BB6508C770000:error:1E800069:HTTP常式：parse_http_line1:received error:../crypto/http/http_client.c:440:code=403, reason=Forbidden\n807BB6508C770000:error:1E800076:HTTP常式：OSSL_HTTP_REQ_CTX_nbio：意外內容type:../crypto/http/http_client.c:676:expected=application/ocsp-response，actual=text/html;charset=\"utf-8\"\n807BB6508C770000:error:1E800067:HTTP常式：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設定控制器連線

如果防火牆上有阻止，允許流量到達http://ssepki.cryptosvcs.cisco.com:80\n可以消除更多證書錯誤。

作業系統更新

作業系統升級不足與技術限制和其他因素有關，這些因素促使ENG團隊決定不在基於VM的RC上嘗試作業系統升級。

避免定期重新部署基於VM的RC的建議是執行基於容器的部署，從而使您的團隊能夠獨立管理容器主機作業系統的升級和維護。

相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。