

如何在TC/CE終端升級後排除TMS上的「無HTTPS響應」錯誤

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[問題](#)

[解決方案](#)

[在TMS Windows Server上為TMS 15.x及更高版本啟用TLS 1.1和1.2](#)

[TMS工具的安全更改](#)

[升級安全設定的注意事項](#)

[驗證](#)

[對於低於15的TMS版本](#)

簡介

本文描述如何對Telepresence Management Suite(TMS)上的「no HTTPS response」(無HTTPS響應)消息進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco TMS
- Windows伺服器

採用元件

本檔案中的資訊是根據以下軟體版本：

- TC 7.3.6及更高版本
- CE 8.1.0及更高版本
- TMS 15.2.1
- Windows Server 2012 R2
- SQL Server 2008 R2和2012

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設)的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

當終端遷移到TC 7.3.6和Collaboration Endpoint(CE)8.1.0軟體或更高版本時，會出現此問題。

問題

當終端升級到TC7.3.6或更高版本或8.1.0或更高版本並且終端與TMS之間的通訊方法設定為傳輸層安全(TLS)後，通過在System > Navigator下選擇Endpoint，在TMS上彈出錯誤消息「no HTTPS response」。

這種情況導致了這種情況。

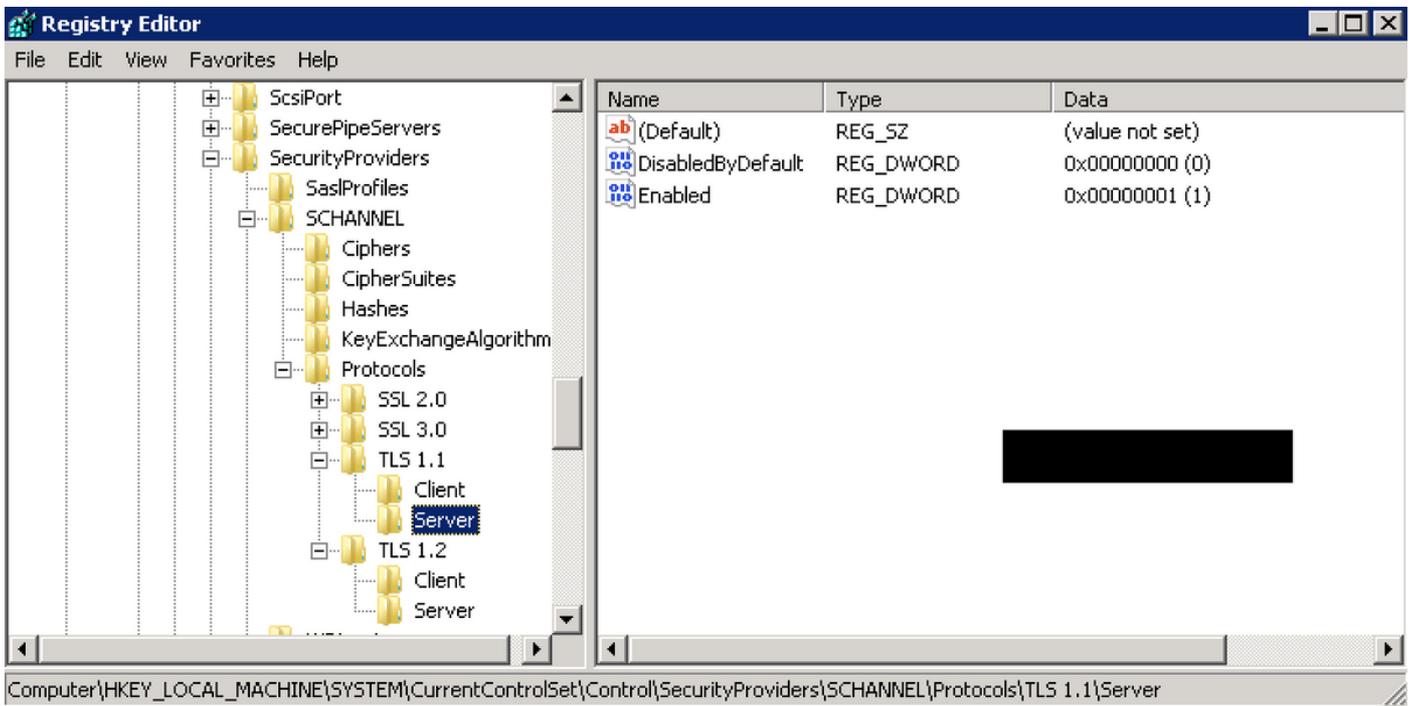
- 根據發行說明，TC 7.3.6和CE 8.1.0及更高版本不再支援TLS 1.0。
http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf
- Microsoft Windows伺服器預設禁用TLS版本1.1和1.2。
- 預設情況下，TMS工具在其傳輸層安全選項中使用介質通訊安全。
- 當TLS版本1.0被禁用，同時啟用TLS版本1.1和1.2時，TMS不會在與終端的TCP三次握手成功後傳送安全套接字層(SSL)客戶端hello。但是仍然可以使用TLS 1.2版加密資料。
- 使用工具或在Windows登錄檔中啟用TLS版本1.2是不夠的，因為TMS仍然只在其客戶端hello消息中傳送或通告1.0。

解決方案

安裝TMS的Windows伺服器需要啟用TLS版本1.1和1.2，這可以通過下一個過程實現。

在TMS Windows Server上為TMS 15.x及更高版本啟用TLS 1.1和1.2

- 1.TMSWindows
- 2.Windows(-> —>Regedit)
3.
 -
 -
 - FileExport
 - Save inFile name
 - Save
- 4.TLS 1.1TLS 1.2
 -
 - HKEY_LOCAL_MACHINE —> SYSTEM —> CurrentControlSet —> Control —> SecurityProviders—> SCHANNEL —> (US)
 - TLS 1.1TLS 1.2
 - TLS 1.1TLS 1.2
 -



TLSDWORD

DisabledByDefault [Value = 0]

Enabled [Value = 1]

5.TMS WindowsTLS

https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

NARTACTLS<https://www.nartac.com/Products/IISCrypto/Download>

TMS工具的安全更改

啟用正確版本後，請使用此過程更改TMS工具上的安全設定。

步驟1.開啟TMS工具

步驟2.導覽至Security Settings > Advanced Security Settings

步驟3.在傳輸層安全選項下，將通訊安全性設定為中高

步驟4.按一下「Save」

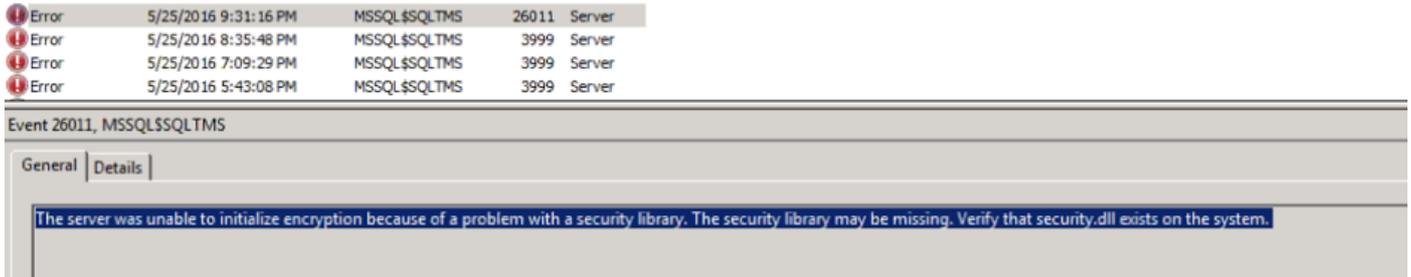
步驟5.然後重新啟動伺服器上的Internet資訊服務(IIS)和TMSDatabaseScannerService，並啟動TMSPLCMDirectoryService (如果已停止)

警告：當TLS選項從「中」更改為「中 — 高」時，將禁用telnet和簡單網路管理協定(SNMP)。這將導致TMSSNMP服務停止，並在TMS Web介面上發出警報。

升級安全設定的注意事項

當SQL 2008 R2正在使用中並安裝在TMS Windows伺服器上時，我們需要確保同時啟用TLS1.0和SSL3.0，否則SQL服務停止並且不會啟動。

您必須在事件日誌中看到以下錯誤：



Icon	Time	Source	ID	Category
Error	5/25/2016 9:31:16 PM	MSSQL\$SQLTMS	26011	Server
Error	5/25/2016 8:35:48 PM	MSSQL\$SQLTMS	3999	Server
Error	5/25/2016 7:09:29 PM	MSSQL\$SQLTMS	3999	Server
Error	5/25/2016 5:43:08 PM	MSSQL\$SQLTMS	3999	Server

Event 26011, MSSQL\$SQLTMS

General | Details

The server was unable to initialize encryption because of a problem with a security library. The security library may be missing. Verify that security.dll exists on the system.

使用SQL 2012時，如果安裝在TMS Windows伺服器上，則需要更新以處理TLS更改 (<https://support.microsoft.com/en-us/kb/3052404>)

使用SNMP或Telnet管理的端點顯示「Security violation:不允許Telnet通訊」。



MI-AHOC-HDX-Test2

Polycom HDX 9002 Status: Security violation: Telnet communication is not allowed Address: 10.20.65.121 Connectivity: Reachable on LAN Software version: Release - 3.1.10-51067

Edit Settings | Ticket Filters | Ticket Log

Tickets

Warning! Connection status is 'Security violation: Telnet communication is not allowed'. The settings and diagnostic messages may be unreliable.

Open:

#1160969 - TMS Connection Error (5/25/2016 9:29:19 PM)

There is a connection problem between TMS and the system.

Add custom ticket | Open system in System Navigator

驗證

當您將TLS選項從Medium更改為Medium-High時，這可確保TLS版本1.2在TMS發出TCP三次握手命令之後在Client Hello中通告：

784	19.841819	10.48.36.26	10.10.245.131	TCP	66 58930 → 443 [SYN, ECN, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
785	19.843295	10.10.245.131	10.48.36.26	TCP	66 443 → 58930 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=64
786	19.843340	10.48.36.26	10.10.245.131	TCP	54 58930 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
787	19.843744	10.48.36.26	10.10.245.131	TLSv1.2	351 Client Hello

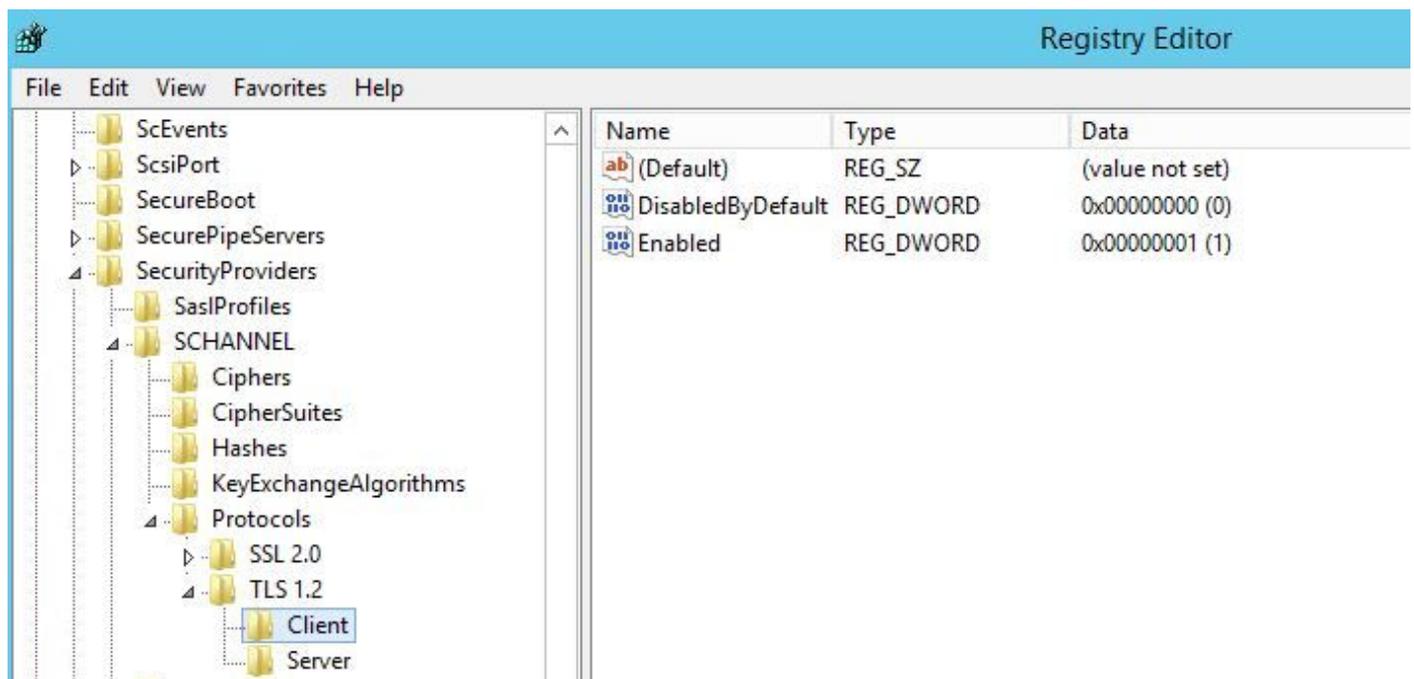
TLS 1.2版已通告：

- Frame 787: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0
- Ethernet II, Src: Vmware_99:59:f1 (00:50:56:99:59:f1), Dst: CiscoInc_29:96:c3 (00:1b:54:29:96:c3)
- Internet Protocol Version 4, Src: 10.48.36.26, Dst: 10.10.245.131
- Transmission Control Protocol, Src Port: 58930 (58930), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 297
- 4 Secure Sockets Layer
 - 4 TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 292
 - Handshake Protocol: Client Hello

如果保留在medium，則TMS在協商階段僅傳送版本1.0的SSL Client hello，該階段指定它作為客戶端支援的最高TLS協定版本，在本例中為TMS。

對於低於15的TMS版本

步驟1.即使TLS 1.2版已新增到登錄檔中



步驟2. TMS伺服器仍不傳送終端在其SSL客戶端hello中支援的版本

1287	11.9999090	10.48.79.117	10.10.0.53	TCP	66 57380-443 [SYN, ECN, cWR] Seq=0 w
1288	12.0011950	10.10.0.53	10.48.79.117	TCP	66 443-57380 [SYN, ACK] Seq=0 Ack=1
1289	12.0012090	10.48.79.117	10.10.0.53	TCP	54 57380-443 [ACK] Seq=1 Ack=1 win=6
1290	12.0013900	10.48.79.117	10.10.0.53	SSL	157 Client Hello
1291	12.0027650	10.10.0.53	10.48.79.117	TCP	60 443-57380 [ACK] Seq=1 Ack=104 win
1292	12.0035480	10.10.0.53	10.48.79.117	TCP	60 443-57380 [RST, ACK] Seq=1 Ack=10
1294	12.0068970	10.48.79.117	10.10.0.53	TCP	66 57381-80 [SYN, ECN, cWR] Seq=0 wi
1295	12.0084020	10.10.0.53	10.48.79.117	TCP	66 80-57381 [SYN, ACK] Seq=0 Ack=1 w
1296	12.0084170	10.48.79.117	10.10.0.53	TCP	54 57381-80 [ACK] Seq=1 Ack=1 win=65
1297	12.0084980	10.48.79.117	10.10.0.53	HTTP	217 GET /tcs/systemunit.xml HTTP/1.1
1298	12.0099360	10.10.0.53	10.48.79.117	TCP	60 80-57381 [ACK] Seq=1 Ack=164 win=
1299	12.0104210	10.10.0.53	10.48.79.117	HTTP	444 HTTP/1.1 301 Moved Permanently (
1300	12.0105360	10.10.0.53	10.48.79.117	TCP	60 80-57381 [FIN, ACK] Seq=391 Ack=1

Frame 1290: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
Ethernet II, Src: Vmware_99:42:e9 (00:50:56:99:42:e9), Dst: Cisco_29:96:c7 (00:1b:54:29:96:c7)
Internet Protocol Version 4, Src: 10.48.79.117 (10.48.79.117), Dst: 10.10.0.53 (10.10.0.53)
Transmission Control Protocol, Src Port: 57380 (57380), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 10
Secure Sockets Layer
SSL Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 98
Handshake Protocol: Client Hello

步驟3.問題出在無法更改TMS工具中的TLS選項，因為此選項不可用



Encryption Key

TLS Client Certificates

Advanced Security Settings

Optional Features Control

- Disable Provisioning
- Disable SNMP

Auditing

- Auditing Always Enabled

Transport Layer Security Options

- Request Client Certificates for HTTPS API
- Enable Certificate Revocation Check

Banners

- Banners on Web Pages and Documents

Top Banner:

Bottom Banner:

Restart IIS and all TMS services for the changes to take effect.

SAVE

步驟4. 然後此問題的解決方法是將TMS升級到15.x，或將TC/CE端點降級到7.3.3, [CSCuz71542](#) 軟體缺陷 (為14.6.X版建立) 中會跟蹤此問題。