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

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

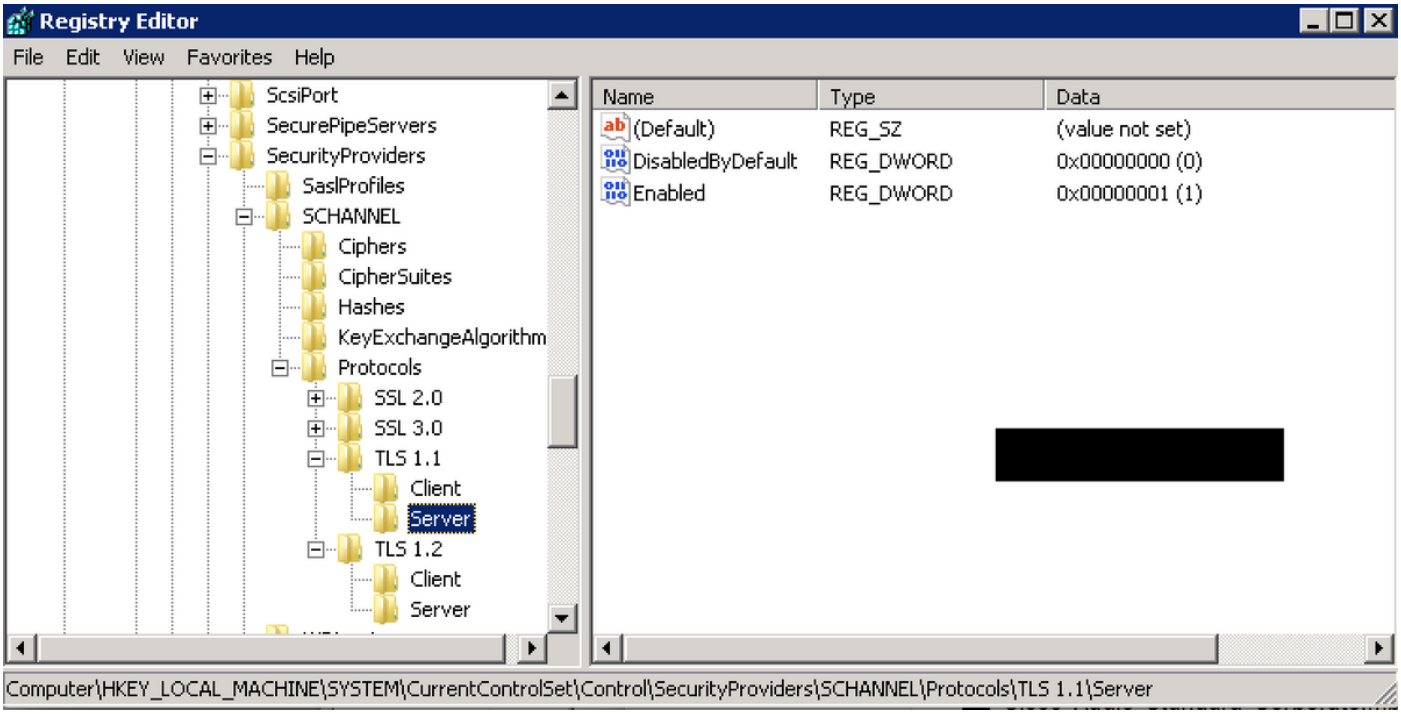
- Microsoft Windows伺服器預設禁用TLS版本1.1和1.2。
- 預設情況下，TMS工具在其傳輸層安全選項中使用介質通訊安全。
- 當TLS版本1.0被禁用，同時啟用TLS版本1.1和1.2時，TMS不會在與終端的TCP三次握手成功後傳送安全套接字層(SSL)客戶端hello。但是仍然可以使用TLS 1.2版加密資料。
- 使用工具或在Windows登錄檔中啟用TLS版本1.2是不夠的，因為TMS仍然只在其客戶端hello消息中傳送或通告1.0。

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
    -



TLS**DWORD**

```
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

NARTACTLShttps://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」**

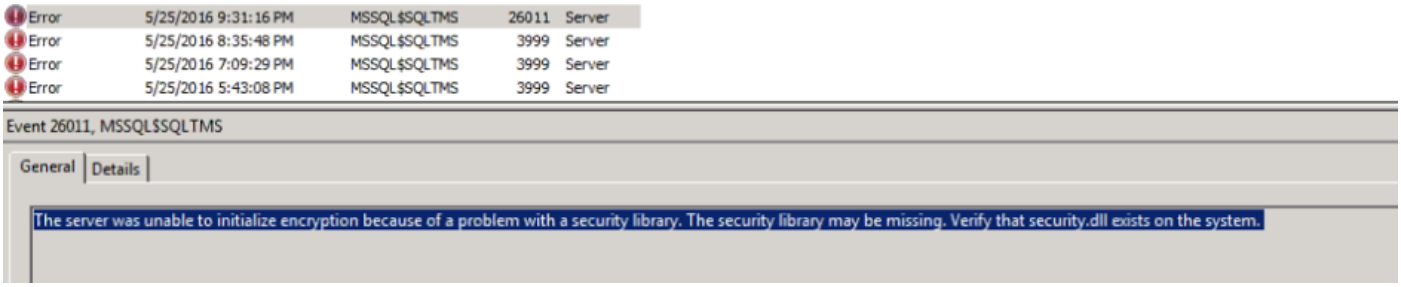
步驟5.然後重新啟動伺服器上的Internet資訊服務(IIS)和**TMSDatabaseScannerService**，並啟動**TMSPLCMDirectoryService**（如果已停止）

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：



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」。

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
```

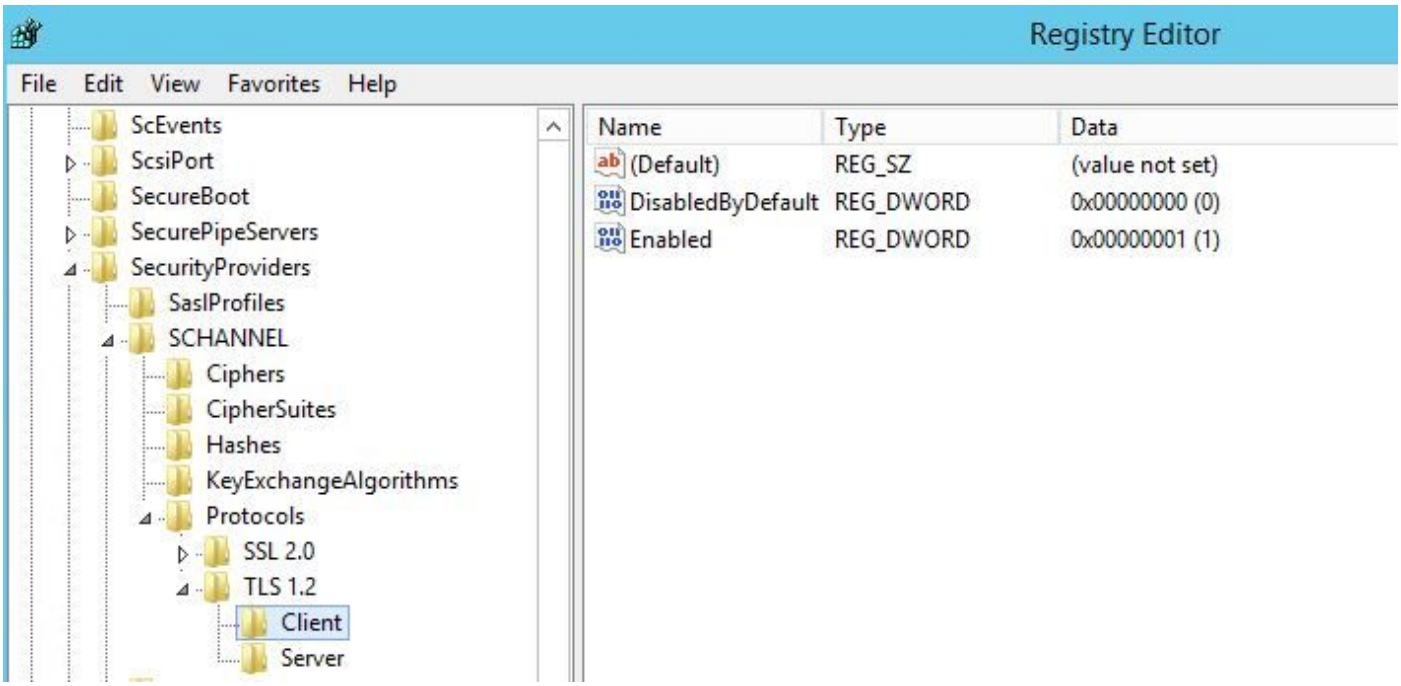
TLS 1.2版已通告：

```
▷ 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
◢ Secure Sockets Layer
  ◢ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 292
    ▷ Handshake Protocol: Client Hello
```

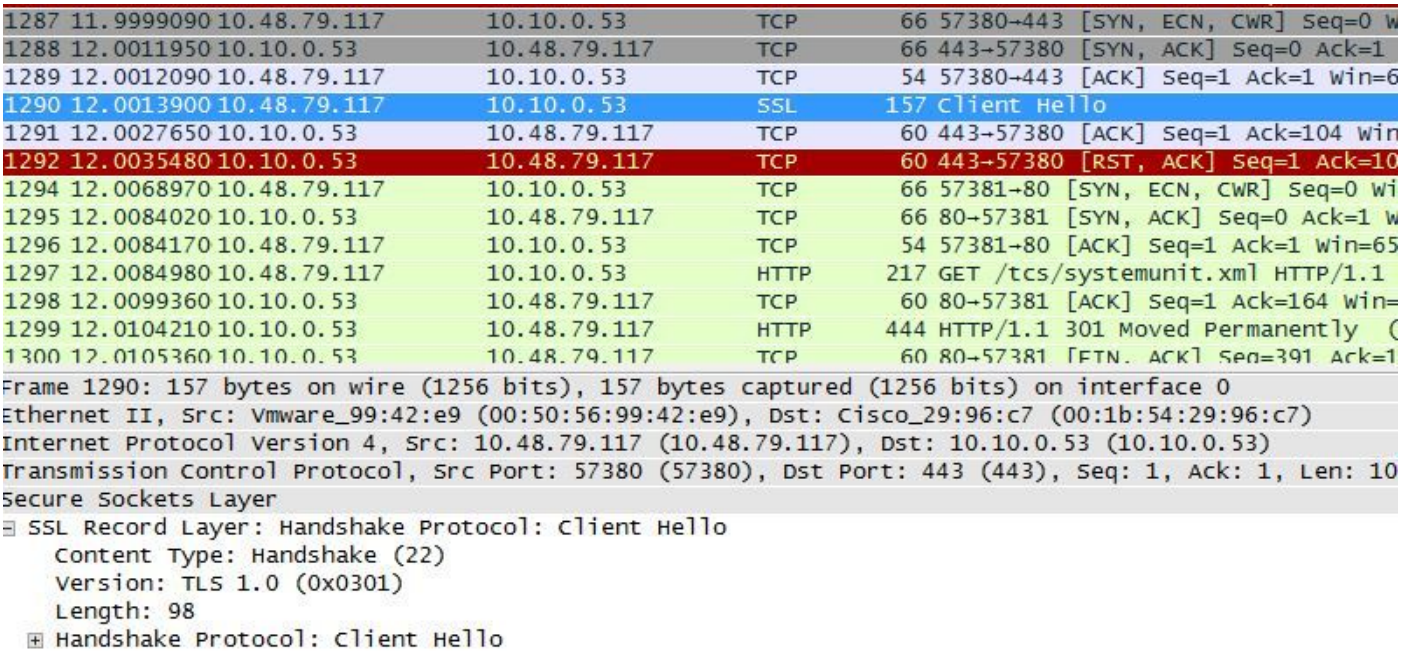
如果保留在**medium**，則TMS在協商階段僅傳送版本1.0的SSL Client hello，該階段指定它作為客戶端支援的最高TLS協定版本，在本例中為TMS。

對於低於15的TMS版本

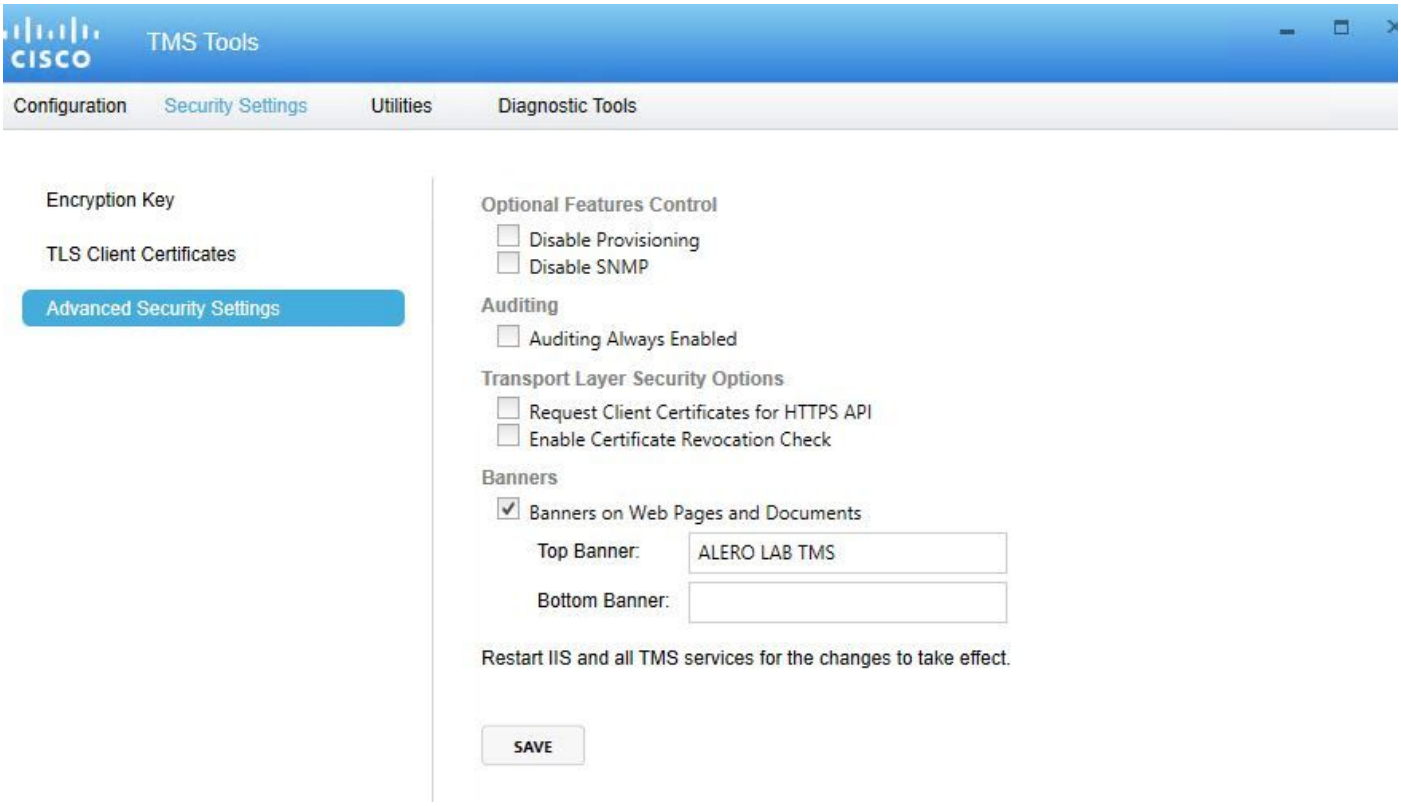
步驟1.即使TLS 1.2版已新增到登錄檔中



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



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



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。