如何排除TC/CE终端升级后TMS上的“无HTTPS响应”错误

目录

简介

本文档介绍如何对网真管理套件(TMS)上的“无HTTPS响应”消息进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科TMS
- Windows 服务器

使用的组件

本文档中的信息基于以下软件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

当终端迁移到TC 7.3.6和协作终端(CE)8.1.0软件或更高版本时，会发生此问题。

问题

终端升级到TC7.3.6或8.1.0或更高版本后，终端与TMS之间的通信方法设置为传输层安全(TLS)，通过在“系统”>“导航器”下选择终端，TMS上会弹出错误消息“无HTTPS响应”。

这种情况发生。

- 根据版本说明，TC 7.3.6和CE 8.1.0及更高版本不再支持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

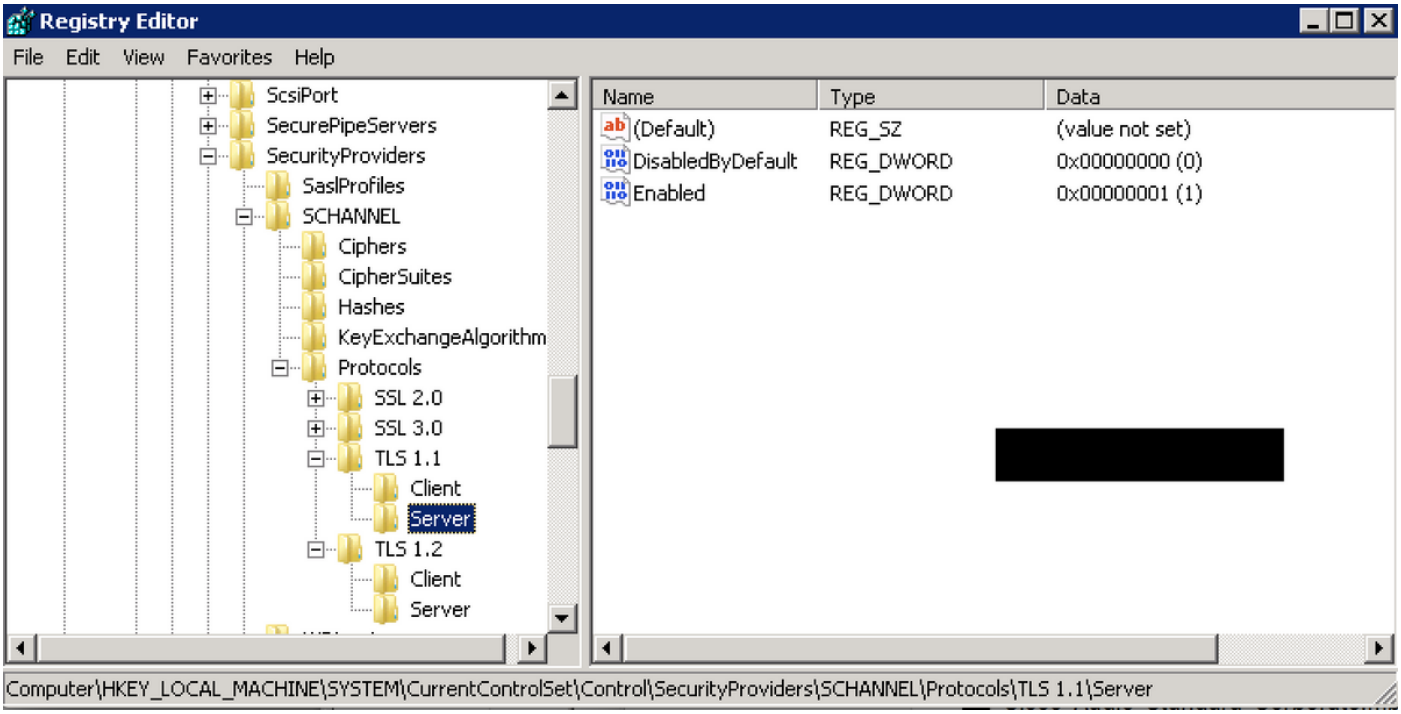
- Microsoft Windows服务器默认禁用TLS版本1.1和1.2。
- 默认情况下，TMS工具在其传输层安全选项中使用中型通信安全。
- 当TLS版本1.0被禁用且TLS版本1.1和1.2均被启用时，在TCP三次握手与终端成功后，TMS不会发送安全套接字层(SSL)客户端问候。但是，仍能使用TLS版本1.2加密数据。
- 使用工具或在Windows注册表中启用TLS版本1.2是不够的，因为TMS仍将仅在其客户端Hello消息中发送或通告1.0。

解决方案

安装TMS的Windows服务器需要启用TLS版本1.1和1.2，这可以通过下一步骤实现。

在TMS Windows Server上为TMS 15.x及更高版本启用TLS 1.1和1.2

1.TMSWindows Server
2.Windows(->->)
3.
    -
    -
    “”“”
    -
    “”“”
    Click Save.
4.TLS 1.1TLS 1.2
    -
    HKEY_LOCAL_MACHINE —> **SYSTEM** —> **CurrentControlSet** —> **Control** —> **SE**—> SCHANNEL —>
    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

NARTACTLShttps://www.nartac.com/Products/IISCrypto/Download

TMS工具上的安全更改

启用正确的版本后，使用此过程更改TMS工具上的安全设置。

步骤1.打开TMS工具

步骤2.导航至“安全设**置”>“高**级安**全设置”**

步骤3.在“传**输层安全选项”**下，将“通信安全”设**置为“中高”**

步骤4.单击“保**存”**

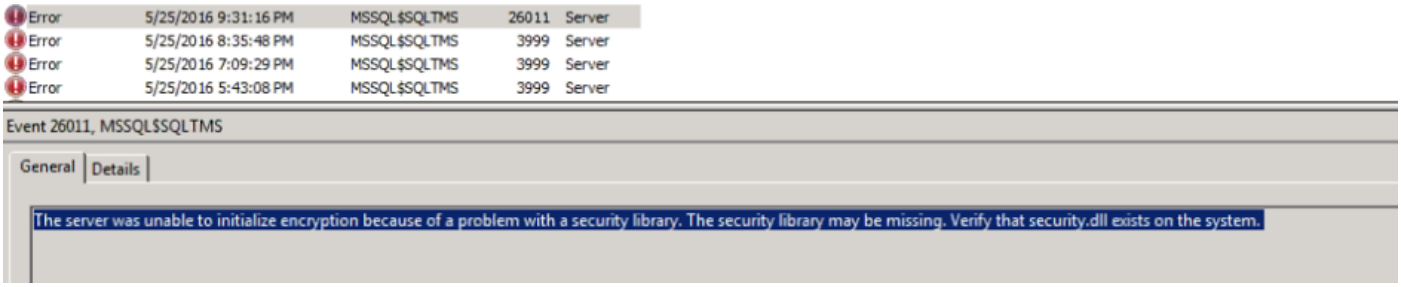
步骤5.然后重新启动服务器上的Internet信息服务(IIS)和**TMSDatabaseScannerService**，并启动**TMSPLCMDirectoryService**（如果已停止）

> **警告：**：当TLS选项从Medium更改为Medium-High时，Telnet和简单网络管理协议(SNMP)将被禁用。这将导致TMSSNMPservice停止，并在TMS Web界面上引发警报。

升级安全设置的注意事项

当SQL 2008 R2正在使用并安装在TMS windows服务器上时，我们需要确保同时启用TLS1.0和SSL3.0，否则SQL服务将停止且不会启动。

必须在事件日志中看到以下错误：



在使用SQL 2012时，如果安装在TMS windows服务器(https://support.microsoft.com/en-us/kb/3052404)上，则需要更新它以处理TLS更改。

使用SNMP或Telnet管理的终端显示“安全违规：不允许Telnet通信”。

验证

当您将TLS选项从Medium更改为Medium-High时，这可确保在TCP三次握手从TMS发出后，TLS版本1.2在客户端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
```

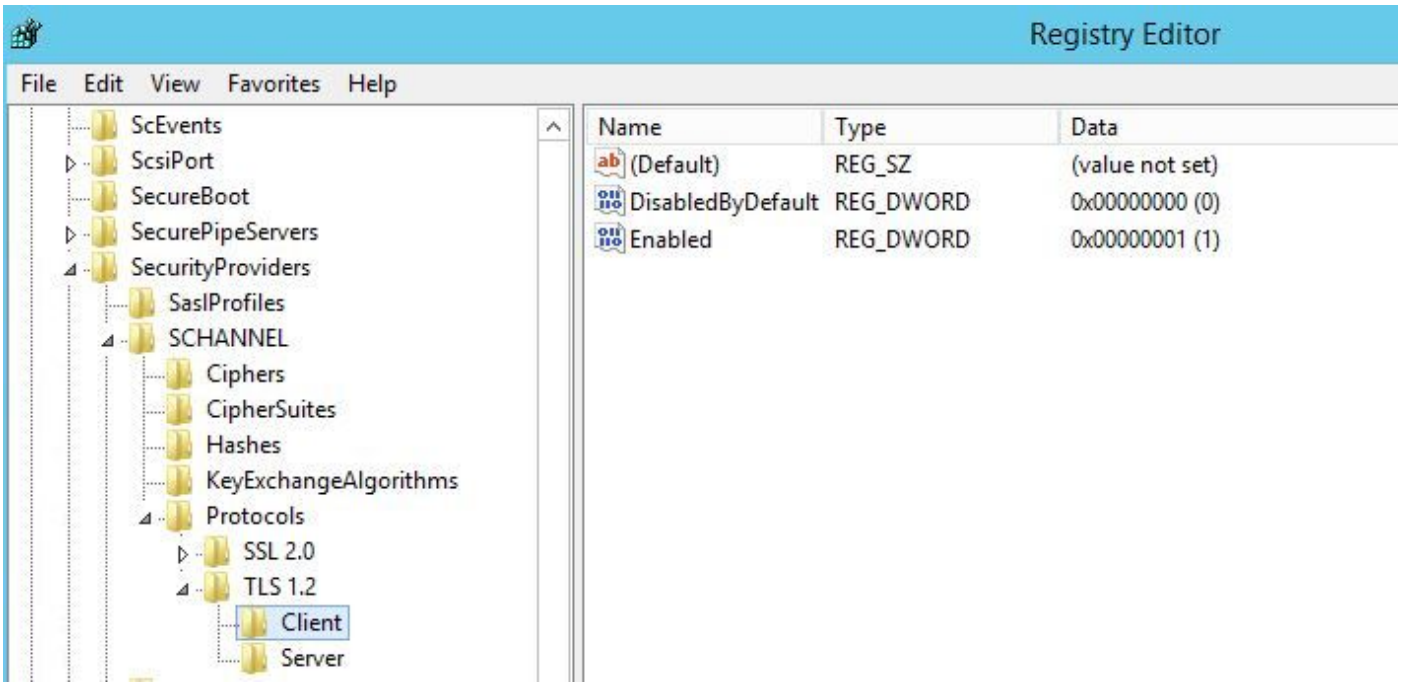
通告的TLS版本1.2:

```
▷ 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
```

如果它保留在中，则TMS在协商阶段仅发送SSL客户端hello中的版本1.0，协商阶段指定它作为客户端支持的最高TLS协议版本（在本例中为TMS）。

对于低于15的TMS版本

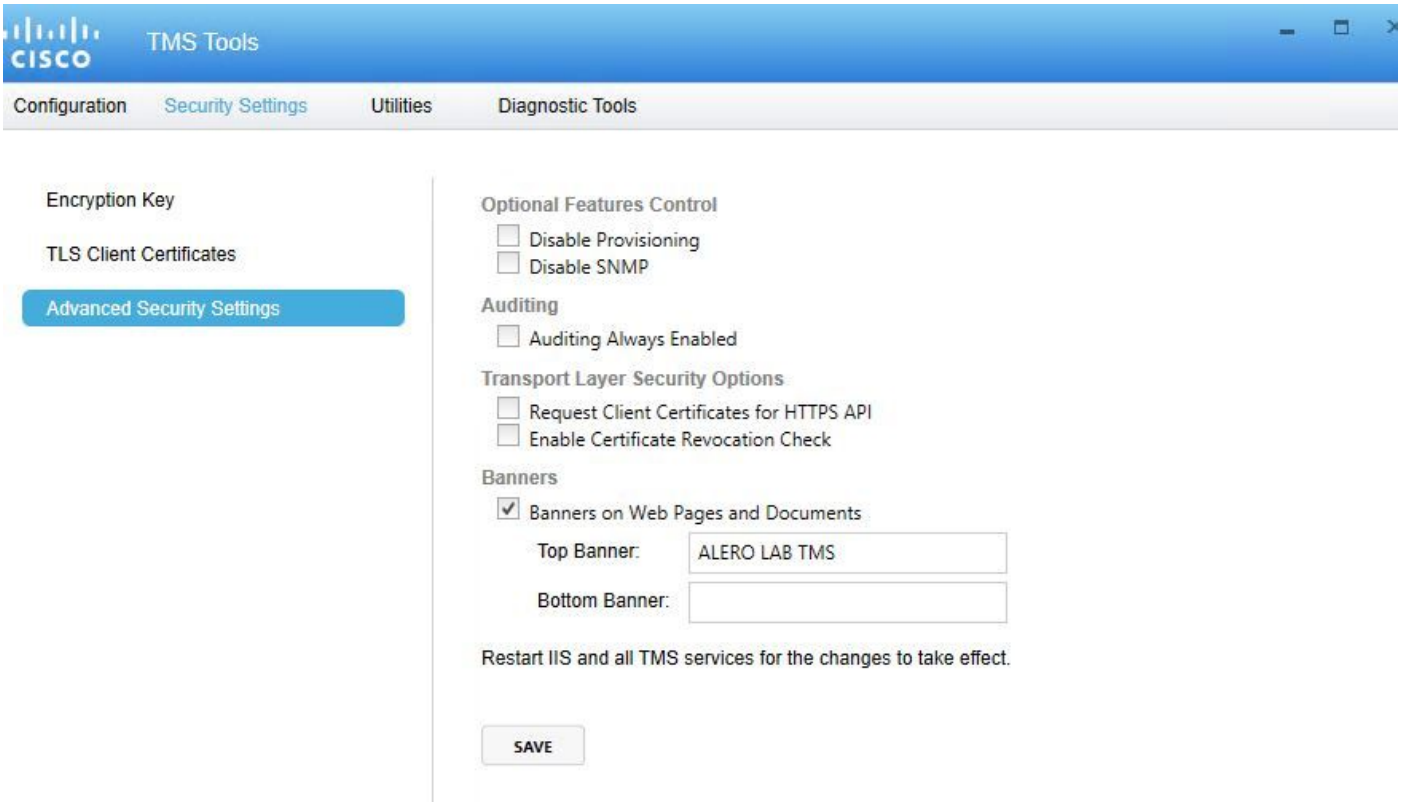
步骤1.即使TLS版本1.2已添加到注册表中



步骤2. TMS服务器仍不在其SSL客户端Hello中发送终端支持的版本

```
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
```

步骤3.然后，问题出在我们无法更改TMS工具中的TLS选项，因为此选项不可用



步骤4.然后，此问题的解决方法是将TMS升级到15.x或将TC/CE终端降级到7.3.3，此问题在为版本14.6.X创建的软件缺陷CSCuz71542中进行跟踪。