

TC/CE エンドポイントのアップグレード後の TMS での「No HTTPS response」エラーをトラブルシューティングする方法

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[問題](#)

[解決方法](#)

[TMS 15.x 以上の TMS Windows サーバで TLS 1.1 と 1.2 を有効にする](#)

[TMS ツールのセキュリティ設定を変更する](#)

[セキュリティ設定のアップグレードにあたっての留意点](#)

[確認](#)

[TMS 15 より前のバージョンの場合](#)

概要

このドキュメントでは、TelePresence Management Suite (TMS) で「no HTTPS response」メッセージが表示された場合のトラブルシューティングについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco TMS
- Windows Server

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- TC 7.3.6 以上
- CE 8.1.0 以上
- TMS 15.2.1
- Windows Server 2012 R2
- SQL サーバ 2008 R2 および 2012

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています

。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

この問題は、エンドポイントのソフトウェアを TC 7.3.6 以上、コラボレーション エンドポイント (CE) 8.1.0 以上に移行すると発生します。

問題

エンドポイントを TC 7.3.6 以上または CE 8.1.0 以上にアップグレードし、エンドポイントと TMS 間の通信方式を Transport Layer Security (TLS) に設定していると、TMS 上で [System] > [Navigator] でエンドポイントを選択した際に「no HTTPS response」というエラーメッセージが表示される。

この問題は次の理由で発生します。

- リリースノートに記載のとおり、TC 7.3.6 以上または CE 8.1.0 以上のバージョンでは TLS 1.0 をサポートしていません。
http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/c-software-release-notes-tc7.pdf
- Microsoft Windows Server では TLS バージョン 1.1 および 1.2 はデフォルトで無効に設定されています。
- TMS ツールの [Transport Layer Security Option] はデフォルトで [Medium Communication Security] に設定されています。
- TLS バージョン 1.0 が無効で、TLS バージョン 1.1 と 1.2 が両方とも有効になっていると、TMS はエンドポイントとの TCP 3 ウェイ ハンドシェイク成功後にセキュア ソケット レイヤ (SSL) Client hello を送信しません。ただし、TLS バージョン 1.2 を使ってデータを暗号化することは可能です。
- いずれかのツールまたは Windows レジストリから TLS バージョン 1.2 を有効にするだけでは、TMS が送信または Client hello メッセージでアダプタイズするのは 1.0 のみのままなので、十分な解決策ではありません。

解決方法

TMS がインストールされている Windows サーバで、TLS バージョン 1.1 と 1.2 を有効にする必要があります。有効にする手順は次のとおりです。

TMS 15.x 以上の TMS Windows サーバで TLS 1.1 と 1.2 を有効にする

1TMS [Remote Desktop Connection to Windows Server]

2Windows [Start] > [Run] > [Regedit]

3

-

-

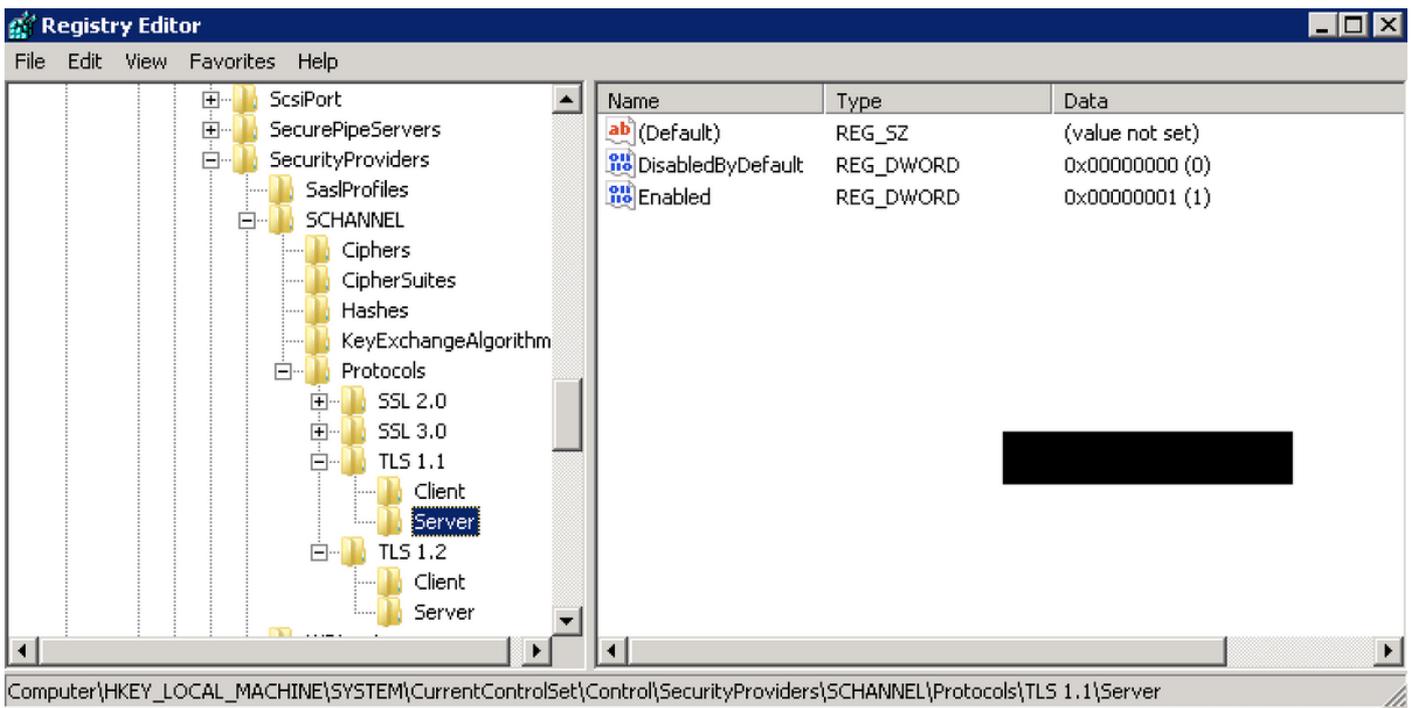
{File} [Export]

{Save in} [File name]

{Save}

4TLS 1.1 TLS 1.2

HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control → curityProviders → SCHANNEL →
-TLS TLS 1.1 TLS 1.2
-TLS 1.1 TLS 1.2



-TLS [DWORD]

DisabledByDefault [Value = 0]

Enabled [Value = 1]

5TLS TMS Windows

https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchanelTR_TLS12

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

TMS ツールのセキュリティ設定を変更する

正しい TLS バージョンを有効にしたら、次の手順に従って TMS ツールのセキュリティ設定を変更します。

ステップ 1 : TMS ツールを開きます。

ステップ 2 : [Security Settings] > [Advanced Security Settings] を開きます。

ステップ 3 : [Transport Layer Security Options] で、[Communication Security] を [Medium-High] に設定します

ステップ 4 : [Save] をクリックします。

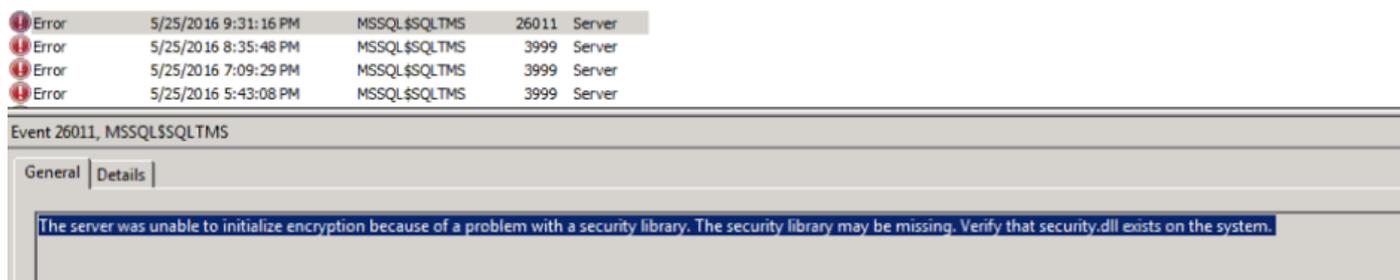
ステップ 5 : 次に、サーバー上のインターネットインフォメーションサービス(IIS)と TMSDatabaseScannerService の両方を再起動し、TMSPLCMDirectoryService を起動します (停止している場合)

警告 : TLS オプションを [Medium-High] から [Medium] に変更すると、Telnet と Simple Network Management Protocol (SNMP) が無効になります。そうすると、TMSSNMPservice が停止し、TMS の Web インターフェイスにアラートが表示されます。

セキュリティ設定のアップグレードにあたっての留意点

SQL 2008 R2 を使用する場合、TMS Windows サーバにインストールしたら必ず TLS 1.0 と SSL 3.0 も有効にする必要があります。無効になっていると SQL サービスが停止し、起動しなくなります。

イベントログにこちらのエラーが表示されます。



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

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.

SQL 2012 を使用する場合、TMS Windows サーバにインストールすると、TLS の変更に対応するためアップデートする必要があります (<https://support.microsoft.com/en-us/kb/3052404>) 。

SNMP または Telnet を使って管理されているエンドポイントでは、「Security violation:Telnet communication is not allowed」と表示されます。



MI-AHOC-HDX-Test2

Polycom HDX 9002 Status: Security violation: Telnet communication is not allowed Address: 10.20.85.121 Connectivity: Reachable on LAN Software version: Release - 3.1.10-51067

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

確認

TLS オプションを [Medium] から [Medium-High] に変更すると、TMS は TCP 3 ウェイ ハンドシェイク成功後の Client hello で TLS バージョン 1.2 をアドバタイズします。

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 バージョン 1.2 のアドバタイズ :

```

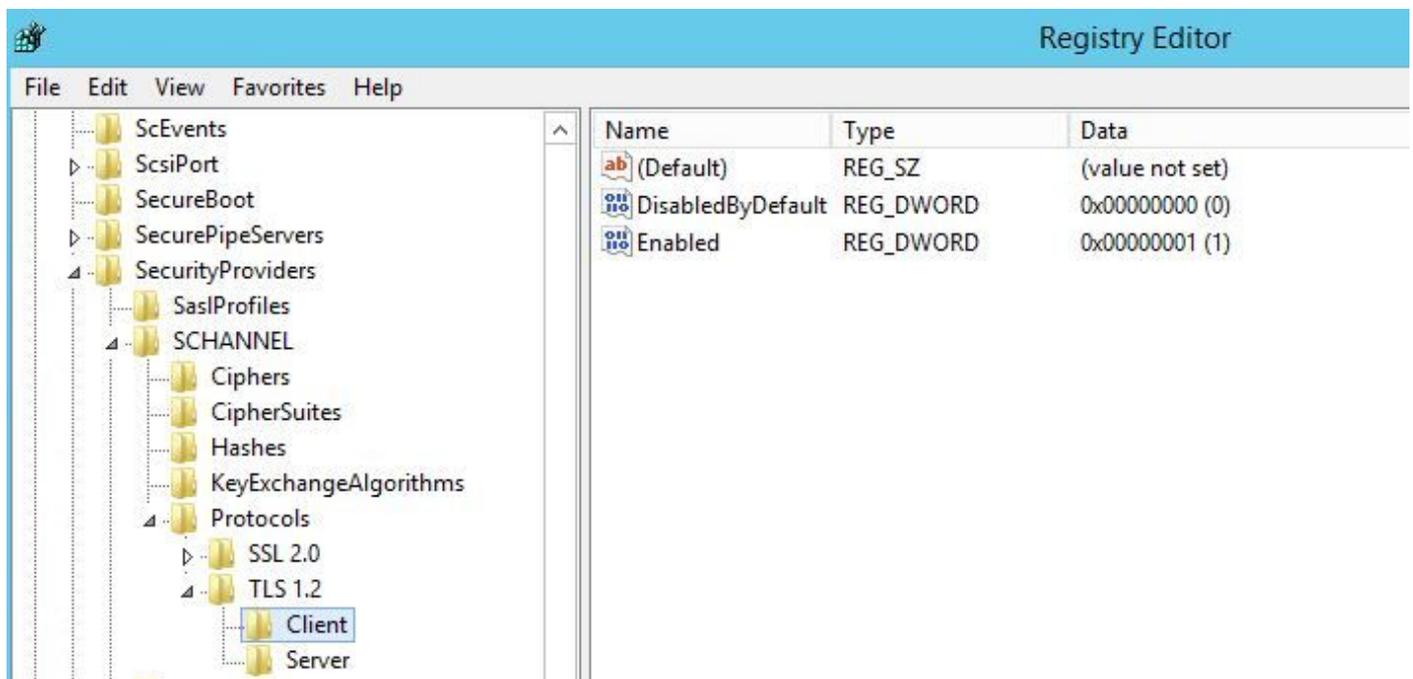
▷ Frame 787: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0
▷ Ethernet II, Src: Vmware_99:59:f1 (00:50:56:99:59:f1), Dst: CiscoInc_29:96:c3 (00:1b:54:29:96:c3)
▷ Internet Protocol Version 4, Src: 10.48.36.26, Dst: 10.10.245.131
▷ Transmission Control Protocol, Src Port: 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

```

ネゴシエーション フェーズではクライアント（この場合 TMS）がサポートしている TLS プロトコルバージョンのうち最もバージョンの高いものを指定します。しかし、TLS オプションを [Medium] のままにした場合、TMS はネゴシエーション フェーズ中の SSL Client hello で TLS バージョン 1.0 しか送信しません。

TMS 15 より前のバージョンの場合

ステップ 1：レジストリには TLS バージョン 1.2 が追加されています。



ステップ2:TMSサーバは、SSLクライアントhelloでエンドポイントがサポートするバージョンを送信しません

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 [FTN. 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

ステップ3 : 問題は、このオプションが使用できないため、TMSツールでTLSオプションを変更できないという事実にあります

The screenshot shows the Cisco TMS Tools interface. The 'Security Settings' tab is active. On the left sidebar, 'Advanced Security Settings' is selected. The main content area shows various security options, including 'Optional Features Control', 'Auditing', 'Transport Layer Security Options', and 'Banners'. The 'Banners' section has a checked checkbox for 'Banners on Web Pages and Documents', with a text input field for 'Top Banner' containing 'ALERO LAB TMS'. A 'SAVE' button is visible at the bottom.

ステップ4 : この問題の回避策として、TMSを15.xにアップグレードするか、TC/CEエンドポイントを7.3.3にダウングレードします。この問題は、バージョン14.6.X用に作成されたソフトウェア不具合CSCuz715422で2追跡2されます。