

Come risolvere il problema "Nessuna risposta HTTPS" su TMS dopo l'aggiornamento degli endpoint TC/CE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Soluzione](#)

[Abilitare TLS 1.1 e 1.2 su TMS Windows Server per TMS 15.x e versioni successive](#)

[Modifica della sicurezza nello strumento TMS](#)

[Considerazioni per l'aggiornamento delle impostazioni di protezione](#)

[Verifica](#)

[Per le versioni TMS inferiori a 15](#)

Introduzione

Questo documento descrive come risolvere i problemi relativi al messaggio "nessuna risposta HTTPS" su Telepresence Management Suite (TMS).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco TMS
- Windows Server

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- TC 7.3.6 e superiori
- CE 8.1.0 e superiore
- TMS 15.2.1
- Windows Server 2012 R2
- SQL Server 2008 R2 e 2012

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo problema si verifica quando si esegue la migrazione degli endpoint a TC 7.3.6 e al software Collaboration Endpoint (CE) 8.1.0 o versioni successive.

Problema

Dopo l'aggiornamento di un endpoint a TC7.3.6 o versione successiva o 8.1.0 o versione successiva e l'impostazione del metodo di comunicazione tra l'endpoint e il TMS come Transport Layer Security (TLS), viene visualizzato il messaggio di errore "no HTTPS response" (Nessuna risposta HTTPS) sul TMS selezionando Endpoint in **System > Navigator**.

Questo accade a causa di questa situazione.

- TC 7.3.6 e CE 8.1.0 e versioni successive non supportano più TLS 1.0 come indicato nelle note di rilascio.
http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf
- Per impostazione predefinita, sul server Microsoft Windows TLS versione 1.1 e 1.2 è disattivato.
- Per impostazione predefinita, gli strumenti TMS utilizzano la protezione di comunicazione media nelle opzioni di protezione del livello di trasporto.
- Quando TLS versione 1.0 è disabilitato e TLS versione 1.1 e 1.2 sono abilitate, TMS non invia un messaggio di benvenuto al client SSL (Secure Socket Layer) dopo che l'handshake TCP a 3 vie ha avuto esito positivo con l'endpoint. Tuttavia, è ancora possibile crittografare i dati utilizzando TLS versione 1.2.
- L'attivazione di TLS versione 1.2 mediante uno strumento o nel Registro di sistema di Windows non è sufficiente, in quanto TMS invierà o annuncerà solo la versione 1.0 nei messaggi di benvenuto del client.

Soluzione

Per il server Windows in cui è installato il TMS, è necessario che TLS versione 1.1 e 1.2 sia abilitato. A tale scopo, eseguire la procedura seguente.

Abilitare TLS 1.1 e 1.2 su TMS Windows Server per TMS 15.x e versioni successive

Passaggio 1. Aprire Connessione desktop remoto a Windows Server in cui è installato TMS.

Passaggio 2. Aprire l'editor del Registro di sistema di Windows (**Start->Run->Regedit**).

Passaggio 3. Eseguire il backup del Registro di sistema.

Se viene richiesta una password di amministratore o una conferma, digitare la password o confermarla.

Individuare e fare clic sulla chiave o sottochiave di cui si desidera eseguire il backup.

Scegliere **Esporta** dal menu **File**.

Nella casella **Salva in** selezionare il percorso in cui si desidera salvare la copia di backup e quindi digitare un nome per il file di backup nella casella **Nome file**.

Fare clic su **Salva**.

Passaggio 4. Abilitare TLS 1.1 e TLS 1.2.

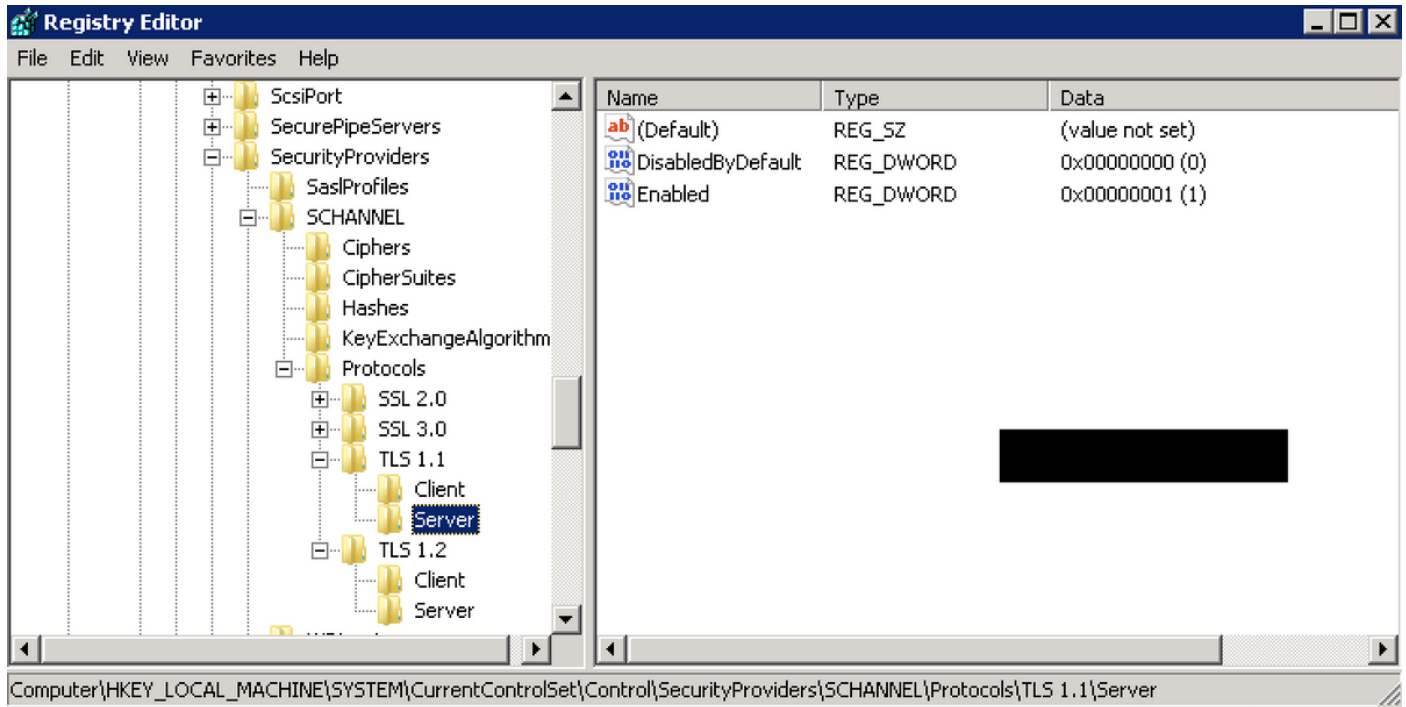
Apri Registro di sistema

Passare a **HKEY_LOCAL_MACHINE** → **SYSTEM** → **CurrentControlSet** → **Control** → **VedereProvider di protezione** → **SCHANNEL** → **Protocolli**

Aggiunta del supporto per TLS 1.1 e TLS 1.2

Creazione di cartelle TLS 1.1 e TLS 1.2

Crea sottochiavi come client e server



Creare **DWORD** per client e server per ogni chiave TLS creata.

DisabledByDefault [Value = 0]

Enabled [Value = 1]

Passaggio 5. Riavviare il server Windows TMS per rendere effettivo TLS.

Nota: Visitare questo collegamento per informazioni specifiche sulle versioni applicabili https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

Suggerimento: è possibile utilizzare lo strumento NARTAC per disabilitare le versioni TLS necessarie dopo aver riavviato il server. È possibile scaricarlo da questo collegamento <https://www.nartac.com/Products/IISCrypto/Download>

Modifica della sicurezza nello strumento TMS

Se sono attivate le versioni corrette, modificare le impostazioni di protezione in Strumenti TMS con questa procedura.

Passaggio 1. Aprire gli strumenti TMS

Passaggio 2. Passare a **Impostazioni protezione** > **Impostazioni di protezione avanzate**

Passaggio 3. In **Opzioni di protezione livello trasporto**, impostare la protezione comunicazione su **Medio-alta**

Passaggio 4. Fare clic su **Salva**

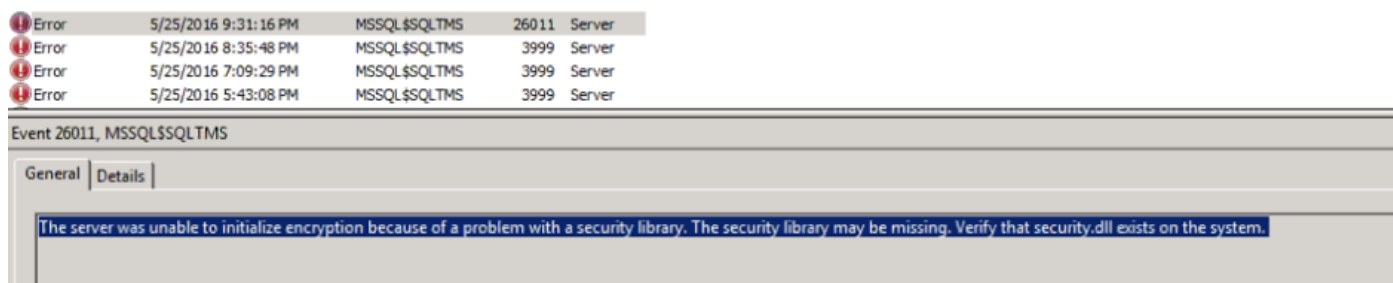
Passaggio 5. Riavviare quindi Internet Information Services (IIS) nel server e **TMSDatabaseScannerService** e avviare **TMSPLCMDirectoryService** (se è arrestato)

Avviso : quando l'opzione TLS viene modificata in Medio-alta da Media, telnet e SNMP (Simple Network Management Protocol) verranno disabilitati. Il servizio TMSSNMP verrà arrestato e verrà generato un avviso sull'interfaccia Web TMS.

Considerazioni per l'aggiornamento delle impostazioni di protezione

Quando **SQL 2008 R2** è in uso e installato nel server Windows TMS, è necessario verificare che anche TLS1.0 e SSL3.0 siano abilitati, altrimenti il servizio SQL verrà arrestato e non verrà avviato.

È necessario visualizzare questi errori nel registro eventi:



Icona	Evento	Data e Ora	Fonte	ID	Descrizione
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.

Quando **SQL 2012** è in uso, è necessario aggiornarlo per gestire le modifiche TLS se installato nel server Windows TMS (<https://support.microsoft.com/en-us/kb/3052404>)

Gli endpoint gestiti tramite SNMP o Telnet mostrano "Violazione della sicurezza: La comunicazione Telnet non è consentita".



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

Verifica

Quando si modifica l'opzione TLS da **Medio** a **Medio-Alto**, ciò assicura che TLS versione 1.2 venga pubblicizzato in **Client Hello** al termine dell'handshake TCP a 3 vie da TMS:

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 versione 1.2 pubblicizzato:

```

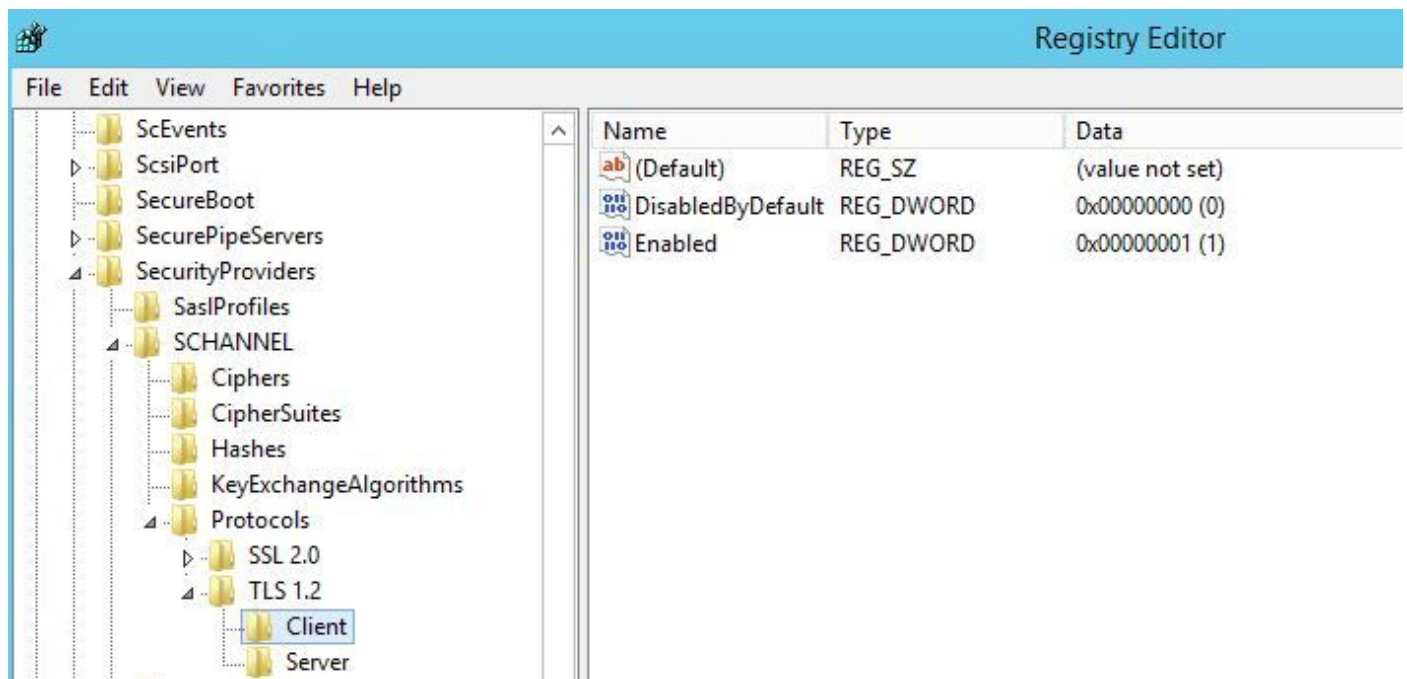
> Frame 787: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0
> Ethernet II, Src: Vmware_99:59:f1 (00:50:56:99:59:f1), Dst: CiscoInc_29:96:c3 (00:1b:54:29:96:c3)
> Internet Protocol Version 4, Src: 10.48.36.26, Dst: 10.10.245.131
> Transmission Control Protocol, Src Port: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

```

Se viene lasciato in posizione **media**, TMS invierà solo la versione 1.0 nel saluto del client SSL durante la fase di negoziazione che specifica la versione del protocollo TLS più alta supportata come client, in questo caso TMS.

Per le versioni TMS inferiori a 15

Passaggio 1. Anche se nel Registro di sistema è stata aggiunta la versione 1.2 di TLS



Passaggio 2. Il server TMS non invia ancora la versione supportata dall'endpoint nel saluto del client SSL

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

Passaggio 3. Il problema risiede nel fatto che non è possibile modificare le opzioni TLS negli strumenti TMS poiché questa opzione non è disponibile

The screenshot shows the Cisco TMS Tools interface. The 'Security Settings' tab is active, and the 'Advanced Security Settings' button is highlighted. The 'Optional Features Control' section includes 'Disable Provisioning' and 'Disable SNMP', both of which are unchecked. The 'Auditing' section has 'Auditing Always Enabled' unchecked. Under 'Transport Layer Security Options', 'Request Client Certificates for HTTPS API' and 'Enable Certificate Revocation Check' are unchecked. In the 'Banners' section, 'Banners on Web Pages and Documents' is checked, and the 'Top Banner' field contains the text 'ALERO LAB TMS'. The 'Bottom Banner' field is empty. A 'SAVE' button is located at the bottom of the configuration area.

Passaggio 4. Per risolvere il problema, aggiornare TMS alla versione 15.x o effettuare il downgrade degli endpoint TC/CE alla versione 7.3.3. Il problema viene rilevato nel software difettoso [CSCuz71542](#) creato per la versione 14.6.X.