Cómo resolver problemas el error de “ninguna respuesta HTTPS” en TMS después de la actualización de los puntos finales TC/CE

Contenido

Introducción

Este documento describe cómo resolver problemas el mensaje de “ninguna respuesta HTTPS” en el conjunto de administración del TelePresence (TMS).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco TMS
- Servidor Windows

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- TC 7.3.6 y arriba
- CE 8.1.0 y arriba
- TMS 15.2.1
- R2 del Servidor Windows 2012
- R2 2008 y 2012 del SQL Server

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Este problema ocurre cuando los puntos finales se emigran a TC 7.3.6 y al software 8.1.0 del punto final de la Colaboración (CE) o arriba.

Problema

Después de que una actualización del punto final a TC7.3.6 o arriba o 8.1.0 o arriba y el método de comunicación entre el punto final y el TMS se configure como Transport Layer Security (TLS), el mensaje de error “que ninguna respuesta HTTPS” surge en TMS seleccionando el punto final, bajo el **sistema** > el **navegador**.

Esto sucede como resultado de este las situaciones.

- El TC 7.3.6 y el CE 8.1.0 y sobre no más soportan el TLS1.0 según los Release Note. http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf

- El Microsoft Windows server tiene TLS versión 1.1 y 1.2 inhabilitados por abandono.
- TMS equipa la Seguridad de comunicación media de las aplicaciones en sus opciones de Transport Layer Security por abandono.
- Cuando se inhabilita el TLS versión 1.0 y se habilita el TLS versión 1.1 y 1.2, TMS no envía los saludos del cliente del Secure Socket Layer (SSL) después de que el apretón de manos de tres vías TCP tenga éxito con el punto final. Al menos aún capaz de cifrar los datos usando el TLS versión 1.2.
- Habilitar el TLS versión 1.2 usando una herramienta o en el registro de Windows no es bastante, pues la voluntad TMS sin embargo envía o hace publicidad solamente de 1.0 en sus mensajes de los saludos del cliente.

Solución

El Servidor Windows donde el TMS está instalado, necesita tener TLS versión 1.1 y 1.2 habilitados, esto puede ser alcanzado con el procedimiento siguiente.

Habilite TLS 1.1 y 1.2 en el Servidor Windows TMS para TMS 15.x y más arriba

Paso 1. Abra una conexión del Escritorio Remoto al Servidor Windows donde TMS está instalado.

Paso 2. Editor de registro de las ventanas abiertas (**Start->Run->Regedit**).

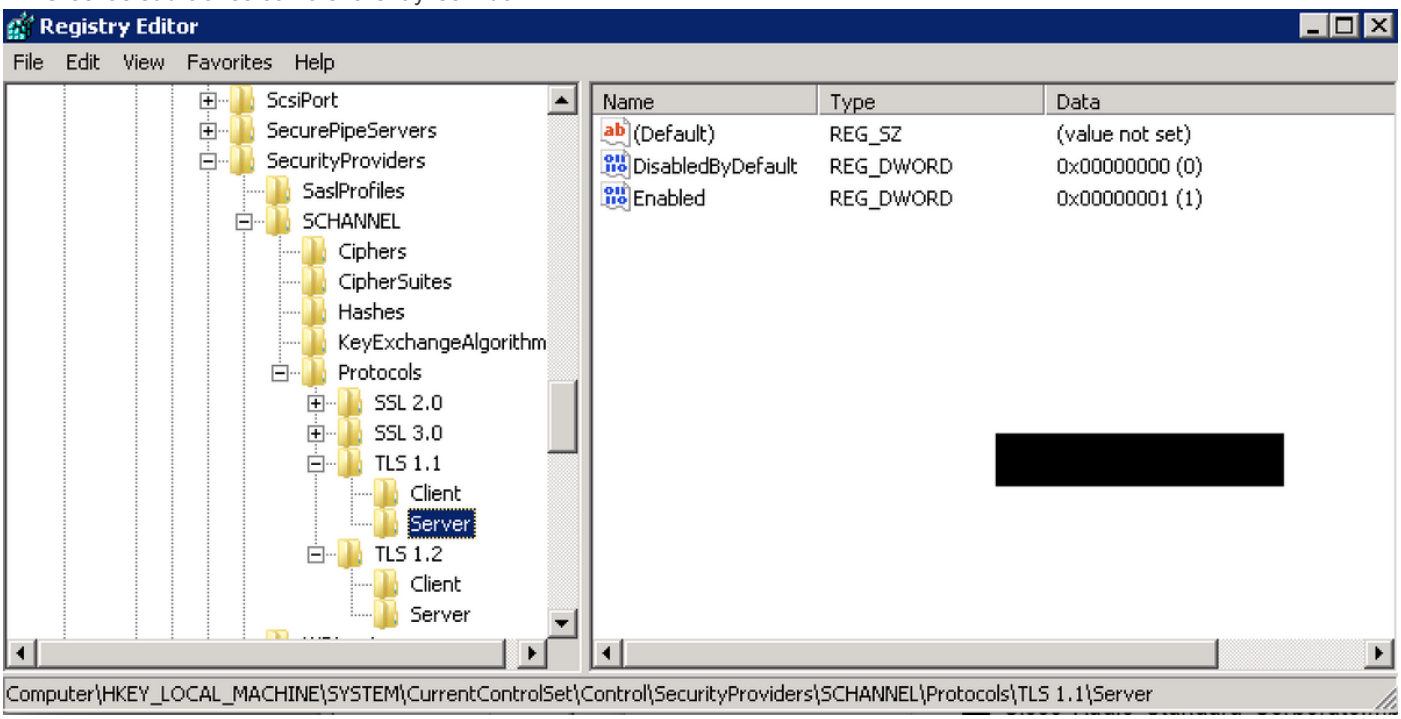
Paso 3. Respaldo de la toma del registro.

Si le indican para una contraseña del administrador o una confirmación, teclee la contraseña o proporcione la confirmación.
Localice y haga clic la clave o el subkey que usted quiere sostener.
Haga clic el menú de archivos, y después haga clic la exportación.
En la salvaguardia en el cuadro, seleccione la ubicación al donde usted quiere salvar la copia de backup, y después teclee un nombre para el archivo de backup en el cuadro del nombre del archivo.
Haga clic en Save (Guardar).

Paso 4. Permiso TLS 1.1 y TLS 1.2.

Abra el registro
Navegue al **HKEY_LOCAL_MACHINE** --> **SISTEMA** --> **CurrentControlSet** --> **control** --> **SecurityProviders**-->

SCHANNEL --> **protocolos**
Agregue el soporte de TLS 1.1 y de TLS 1.2
Cree TLS 1.1 y TLS 1.2 carpetas
Cree las sub-claves como el client y 'servidor



Cree los **DWORD** para ambos cliente y servidor para cada clave de TLS creada.

```
DisabledByDefault [Value = 0]
Enabled [Value = 1]
```

Paso 5. El Servidor Windows del reinicio TMS para asegurar TLS toma el efecto.

> Nota: Visite este link para información específica sobre las versiones aplicable https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

> Consejo: La herramienta NARTAC se puede utilizar para inhabilitar las versiones necesarias TLS después de que usted haga que usted necesita recomenzar el servidor. Usted puede descargarla de este link https://www.nartac.com/Products/IISCrypto/Download

Cambio en la seguridad en la herramienta TMS

Cuando se habilitan las versiones correctas, cambie los ajustes de seguridad en las herramientas TMS con este procedimiento.

Paso 1. Abra las herramientas TMS

Paso 2. Navegue a los **ajustes de seguridad** > a las **configuraciones de la Seguridad avanzada**

Paso 3. Bajo **opciones de Transport Layer Security**, fije la Seguridad de comunicación a Media-**alto**

Paso 4. **Salvaguardia del** tecleo

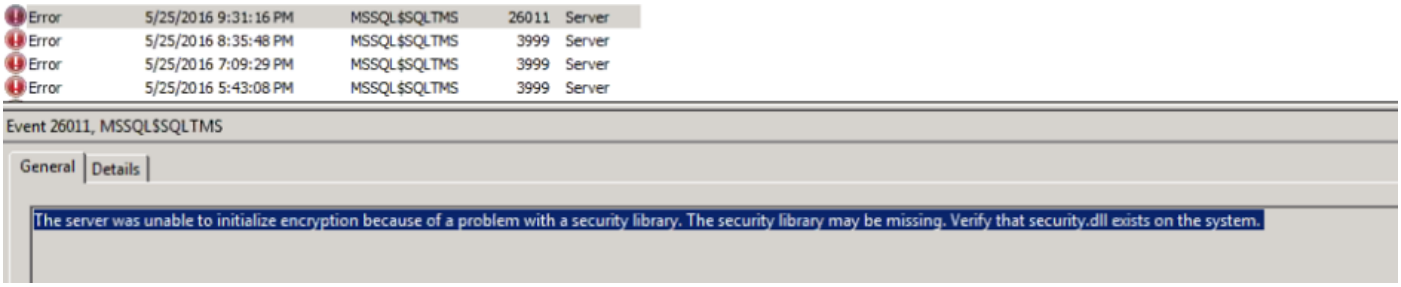
Paso 5. Después recomience los Servicios de Internet Information Server (IIS) en el servidor y **TMSDatabaseScannerService** y comience **TMSPLCMDirectoryService** (si ha parado)

Advertencia: : Cuando la opción de TLS se cambia a Media-alto del media, el telnet y el Simple Network Management Protocol (SNMP) serán inhabilitados. Esto hará a TMSSNMPservice parar y una alerta será aumentada en la interfaz Web TMS.

Consideraciones para actualizar los ajustes de seguridad

Cuando el **r2 SQL 2008** es funcionando y instalado en el Servidor Windows TMS, necesitamos asegurarnos que el TLS1.0 y SSL3.0 también sean habilitados o bien parada y él del servicio SQL no comenzará.

Usted debe ver este los errores en el registro de acontecimientos:

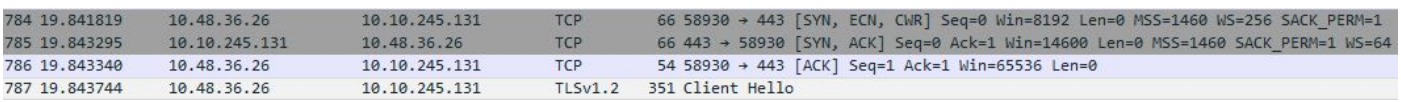


Cuando el **SQL 2012** es funcionando requiere para ser puesto al día para abordar el cambio de TLS si está instalado en el Servidor Windows TMS (https://support.microsoft.com/en-us/kb/3052404)

Puntos finales manejados usando violación de seguridad de la demostración SNMP o de Telnet la ": Las comunicaciones Telnet no se permiten".

Verificación

Cuando usted cambia la opción de TLS del **media a Media-alto,** éste se asegura de que el TLS versión 1.2 esté hecho publicidad en los **saludos del cliente** después de que el apretón de manos de tres vías TCP tenga éxito de TMS:



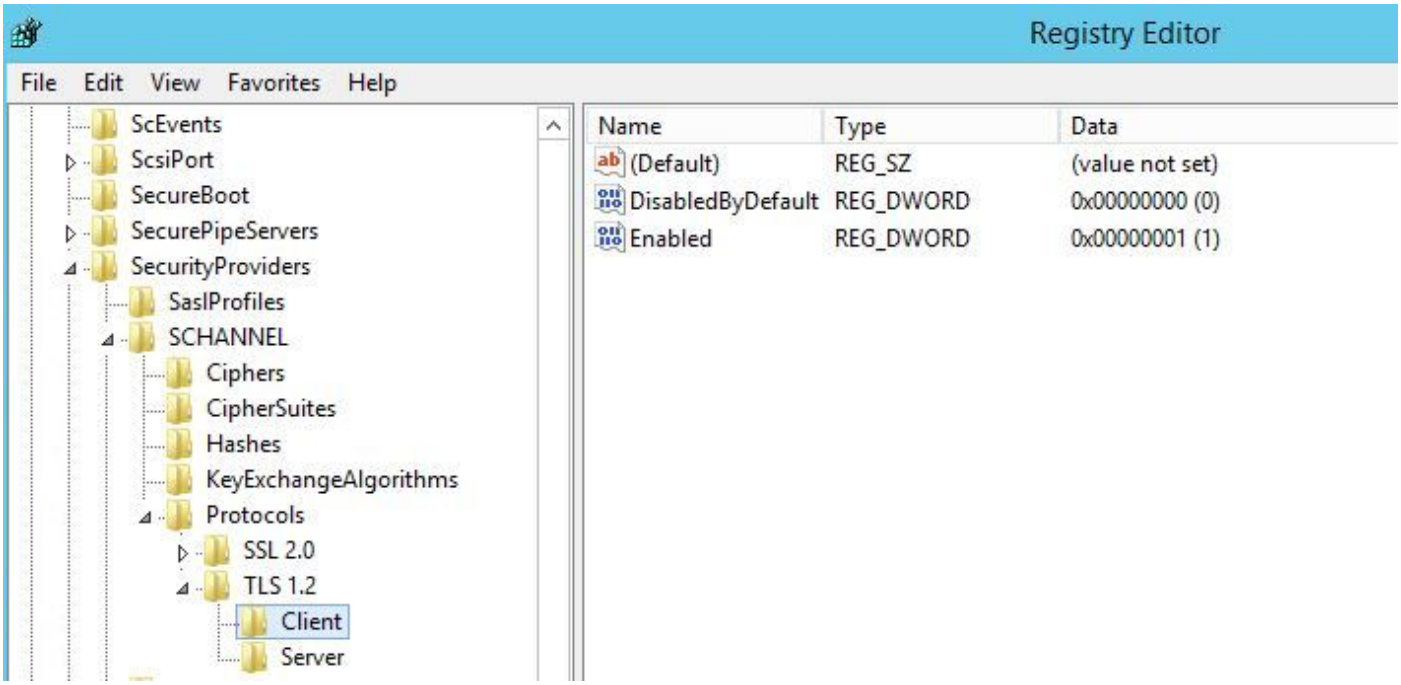
TLS versión 1.2 de divulgación:

```
▷ 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
```

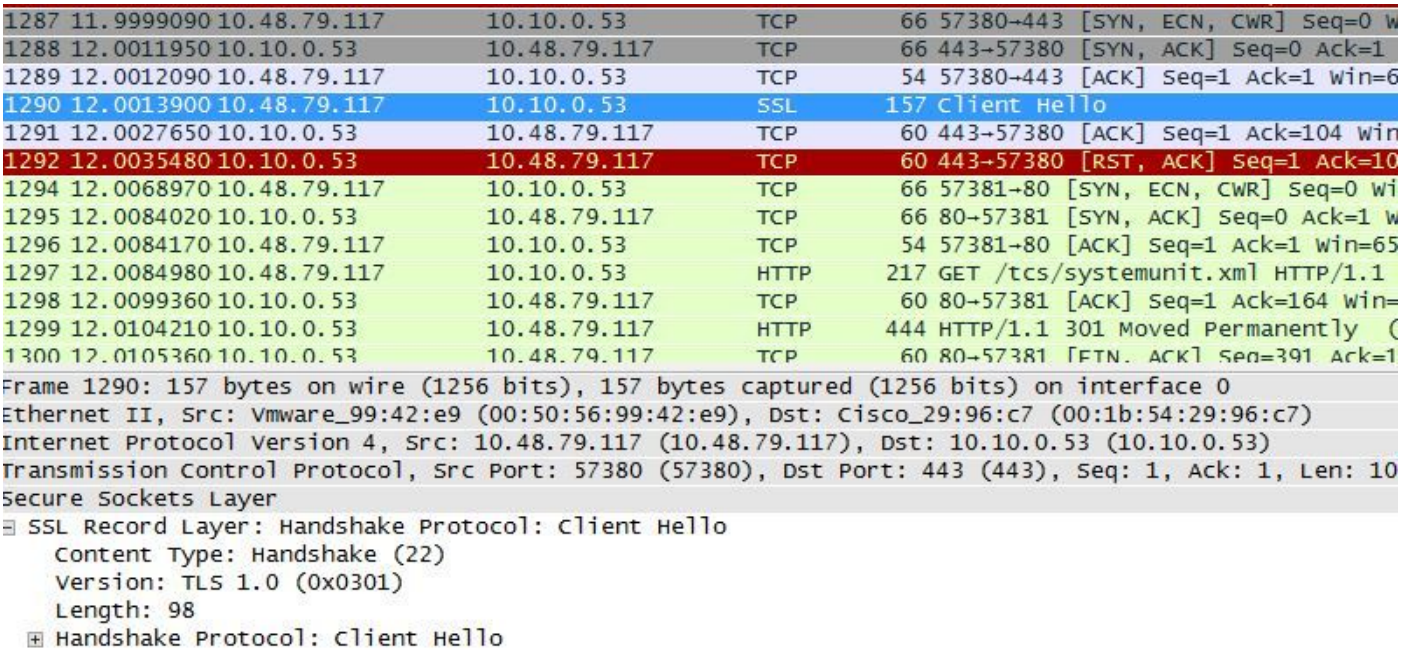
Si se ha ido en el **media** TMS envía solamente la versión 1.0 en los saludos al cliente SSL durante la fase de negociación que especifica la versión más alta del protocolo TLS que soporta como cliente, que TMS es, en este caso.

Para las versiones TMS baje que 15

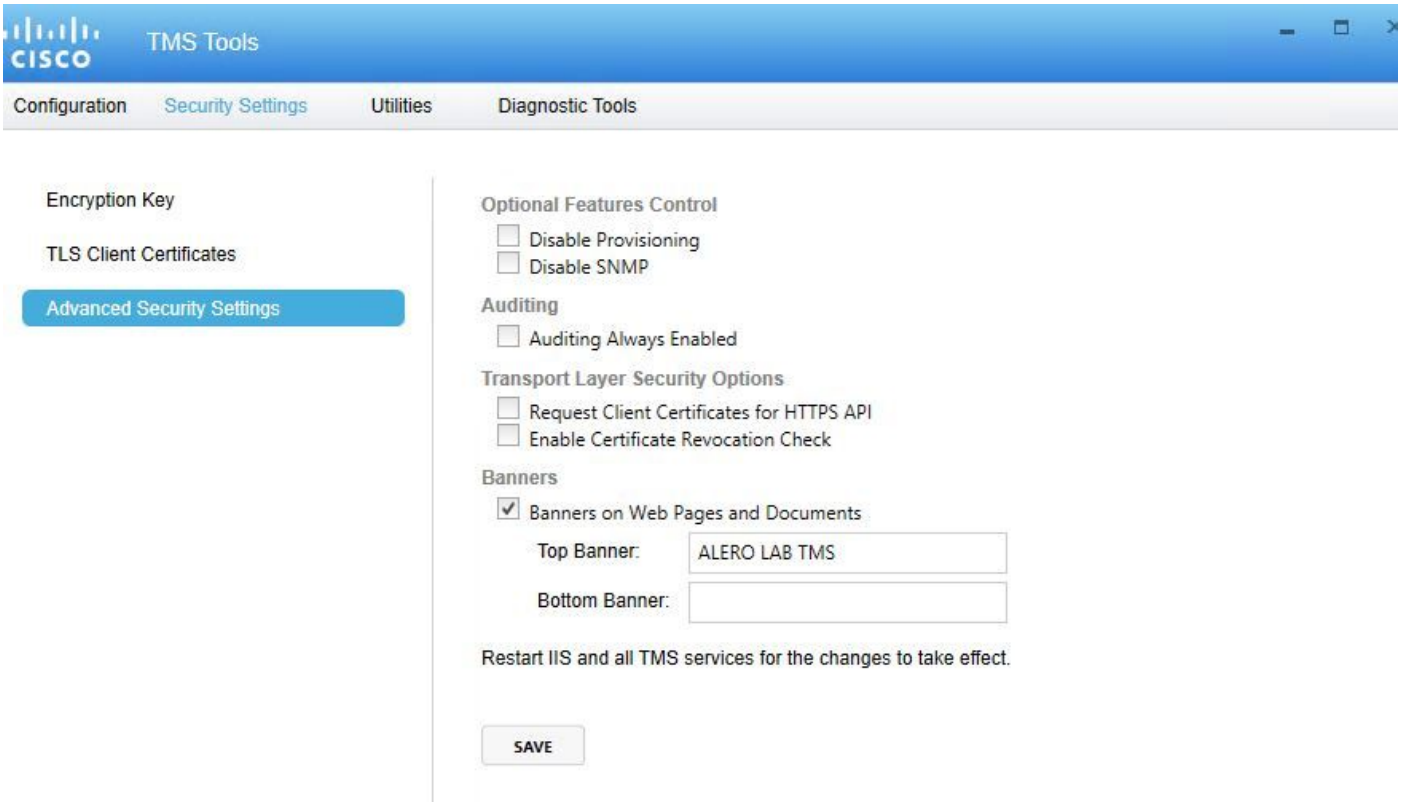
Paso 1. Aunque el TLS versión 1.2 se agrega en el registro



Paso 2. El servidor TMS todavía no envía la versión soportada por el punto final en sus saludos al cliente SSL



Paso 3. El problema entonces miente en el hecho de que no podemos cambiar las opciones de TLS en las herramientas TMS pues esta opción no está disponible



Paso 4. Después la solución alternativa para este problema es la actualización TMS a 15.x o retrocede sus puntos finales TC/CE a 7.3.3, este problema se sigue en el defecto del software CSCuz71542 creado para la versión 14.6.X.