Como pesquisar defeitos de “o erro nenhuma resposta HTTPS” em TMS após a elevação dos valores-limite TC/CE

Índice

Introdução

Este documento descreve como pesquisar defeitos de “a mensagem nenhuma resposta HTTPS” na suite de gerenciamento do TelePresence (TMS).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco TMS
- Windows Server

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- TC 7.3.6 e acima
- CE 8.1.0 e acima
- TMS 15.2.1
- Windows Server 2012 R2
- Servidor SQL 2008 R2 e 2012

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Esta edição ocorre quando os valores-limite estão migrados a TC 7.3.6 e a software 8.1.0 do valor-limite da Colaboração (CE) ou acima.

Problema

Depois que uma elevação do valor-limite a TC7.3.6 ou acima ou 8.1.0 ou acima e o método de comunicação entre o valor-limite e o TMS é o Transport Layer Security estabelecido (TLS), o Mensagem de Erro “que nenhuma resposta HTTPS” estala acima em TMS selecionando o valor-limite, sob o **sistema** > o **navegador**.

Isto acontece em consequência do este situações.

- O TC 7.3.6 e o CE 8.1.0 e acima de já não apoiam o TLS1.0 conforme os Release Note. http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf

- O Microsoft Windows server tem a versão TLS 1.1 e 1.2 desabilitados à revelia.
- TMS utiliza ferramentas a Segurança de comunicação média dos usos em suas opções do Transport Layer Security à revelia.
- Quando a versão TLS 1.0 é desabilitada e a versão TLS 1.1 e 1.2 está permitida, TMS não envia hellos do cliente do Secure Socket Layer (SSL) depois que o aperto de mão da 3-maneira TCP sucede com o valor-limite. De qualquer modo ainda capaz de cifrar dados usando a versão TLS 1.2.
- Permitir a versão TLS 1.2 usando uma ferramenta ou no registro de Windows não é bastante, porque a vontade TMS ainda assim somente envia ou anuncia 1.0 em suas mensagens dos hellos do cliente.

Solução

O Windows Server onde o TMS é instalado, precisa de ter a versão TLS 1.1 e 1.2 permitidos, isto pode ser conseguido com o procedimento seguinte.

Permita TLS 1.1 e 1.2 em TMS Windows Server para TMS 15.x e mais altamente

Etapa 1. Abra uma conexão do Desktop remoto a Windows Server onde TMS é instalado.

Etapa 2. Editor de registro das janelas aberta (**Start->Run->Regedit**).

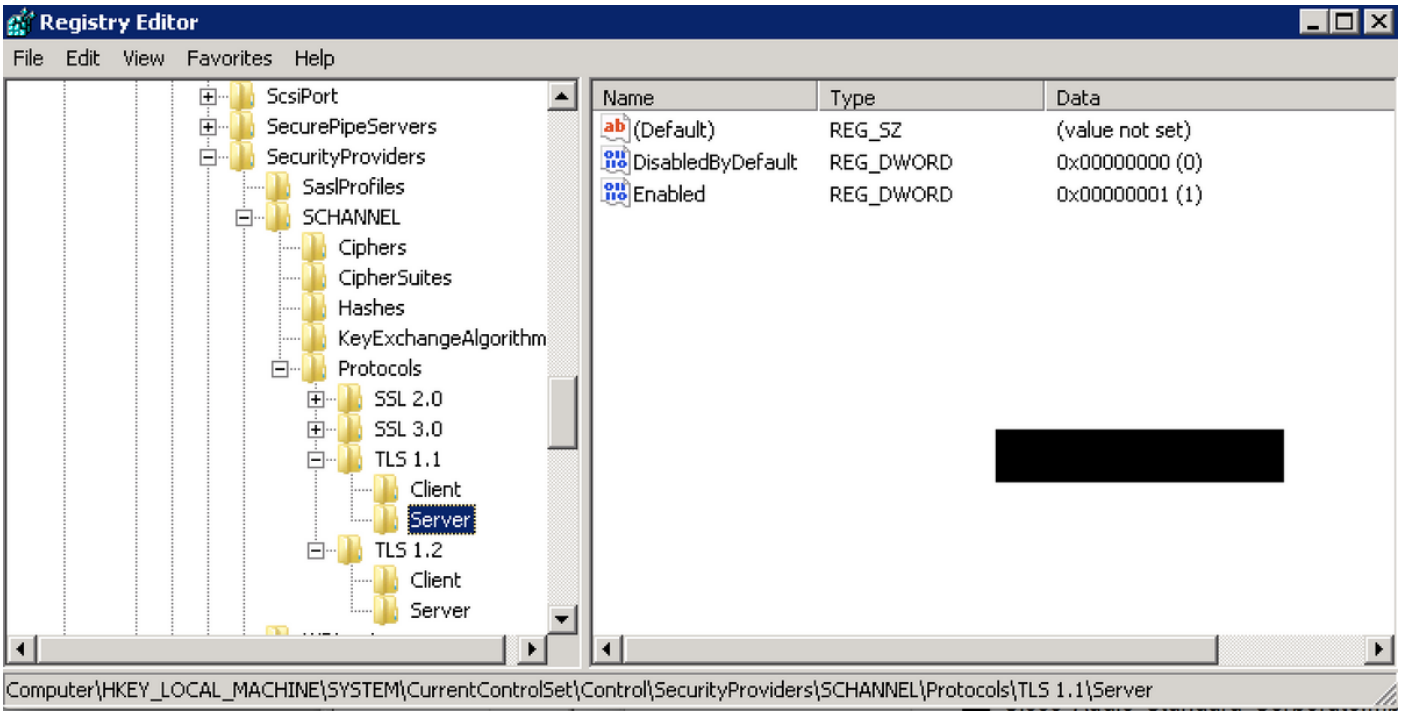
Etapa 3. Backup da tomada do registro.

Se você é alertado para uma senha de administrador ou uma confirmação, datilografe a senha ou forneça a confirmação.
Encontre e clique a chave ou a subchave que você quer suportar.
Clique o menu de arquivo, e clique então a exportação.
Na salvaguarda na caixa, selecione o lugar a onde você quer salvar a cópia de segurança, e datilografe então um nome para o arquivo de backup na caixa do nome de arquivo.
Clique em Salvar.

Etapa 4. Permita TLS 1.1 e TLS 1.2.

Abra o registro
Navegue ao **HKEY_LOCAL_MACHINE** --> **SISTEMA** --> **CurrentControlSet** --> **controle** --> **SecurityProviders**-->

SCHANNEL --> **protocolos**
Adicionar o apoio TLS 1.1 e TLS 1.2
Crie dobradores TLS 1.1 e TLS 1.2
Crie secundário-chaves como o client e 'o server



Crie **DWORD** para ambos cliente e servidor para cada chave TLS criada.

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

Etapa 5. O Windows Server do reinício TMS para assegurar o TLS toma o efeito.

Nota: Visite este link ra obter informações específicas sobre das versões aplicable https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

Dica: A ferramenta NARTAC pode ser usada para desabilitar as versões necessárias TLS depois que você faz que você precisa de reiniciar o server. Você pode transferi-la deste link https://www.nartac.com/Products/IISCrypto/Download

Alteração de segurança na ferramenta TMS

Quando as versões corretas são permitidas, mude as configurações de segurança em ferramentas TMS com este procedimento.

Etapa 1. Abra ferramentas TMS

Etapa 2. Navegue às **configurações de segurança** > aos **ajustes da segurança avançada**

Etapa 3. Sob **opções do Transport Layer Security**, ajuste a Segurança de comunicação a Media-**alto**

Etapa 4. **Salvaguarda do** clique

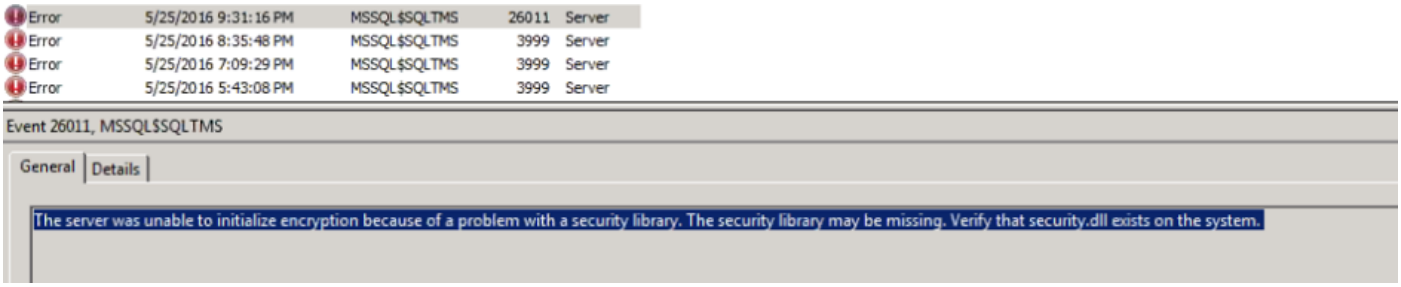
Etapa 5. Então reinicie o Internet Information Services (IIS) no server e **TMSDatabaseScannerService** e comece **TMSPLCMDirectoryService** (se parou)

aviso: : Quando a opção TLS é mudada a Media-alto do media, o telnet e o Simple Network Management Protocol (SNMP) estarão desabilitados. Isto causará a TMSSNMPservice parar e um alerta será levantado na interface da WEB TMS.

Considerações a fim promover configurações de segurança

Quando o **SQL 2008 R2** está no uso e é instalado no Windows Server TMS, nós precisamos de assegurar-se de que o TLS1.0 e SSL3.0 devam igualmente ser permitidos ou então parada e ele do serviço SQL não comece.

Você deve ver este erros no log de eventos:

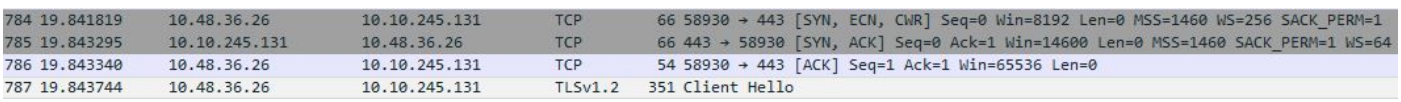


Quando o **SQL 2012** está no uso exige para ser atualizado para abordar a mudança TLS se instalado no Windows Server TMS (https://support.microsoft.com/en-us/kb/3052404)

Valores-limite controlados usando violação de segurança da mostra SNMP ou de telnet a “: Uma comunicação de Telnet não é permitida”.

Verificar

Quando você muda a opção TLS do **media a Media-alto,** este assegura-se de que a versão TLS 1.2 esteja anunciada nos **hellos do cliente** depois que o aperto de mão da 3-maneira TCP sucede de TMS:



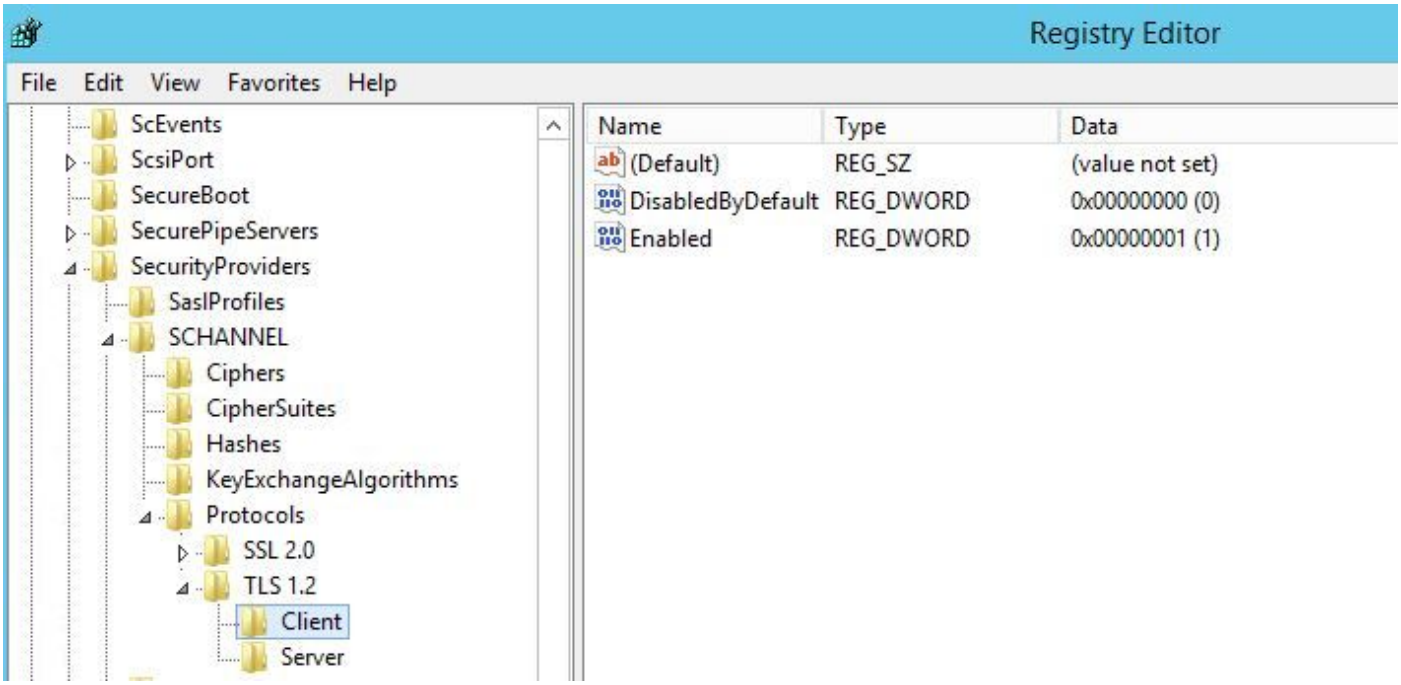
Versão TLS 1.2 anunciada:

```
▷ 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
```

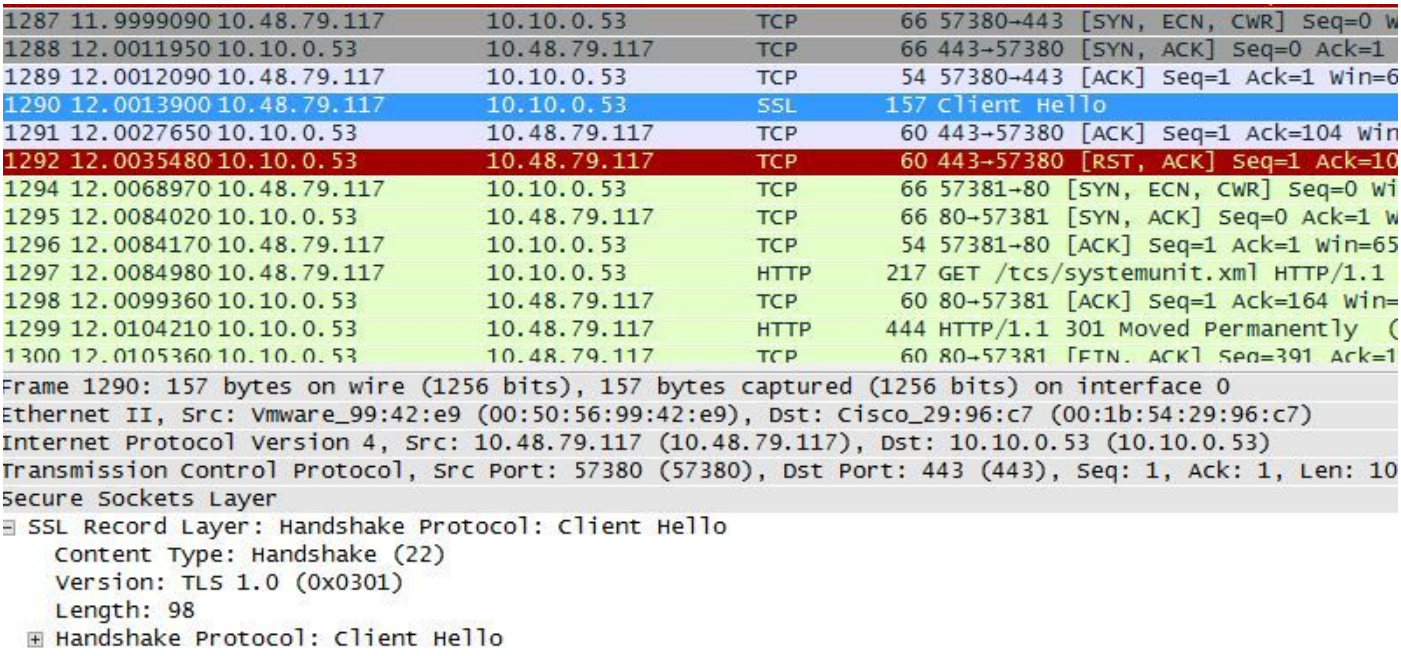
Se saiu no **media** TMS enviará somente a versão 1.0 nos hellos de cliente SSL durante a fase de negociação que especifica a versão que a mais alta do protocolo TLS apoia como um cliente, que TMS seja, neste caso.

Para versões TMS abaixe do que 15

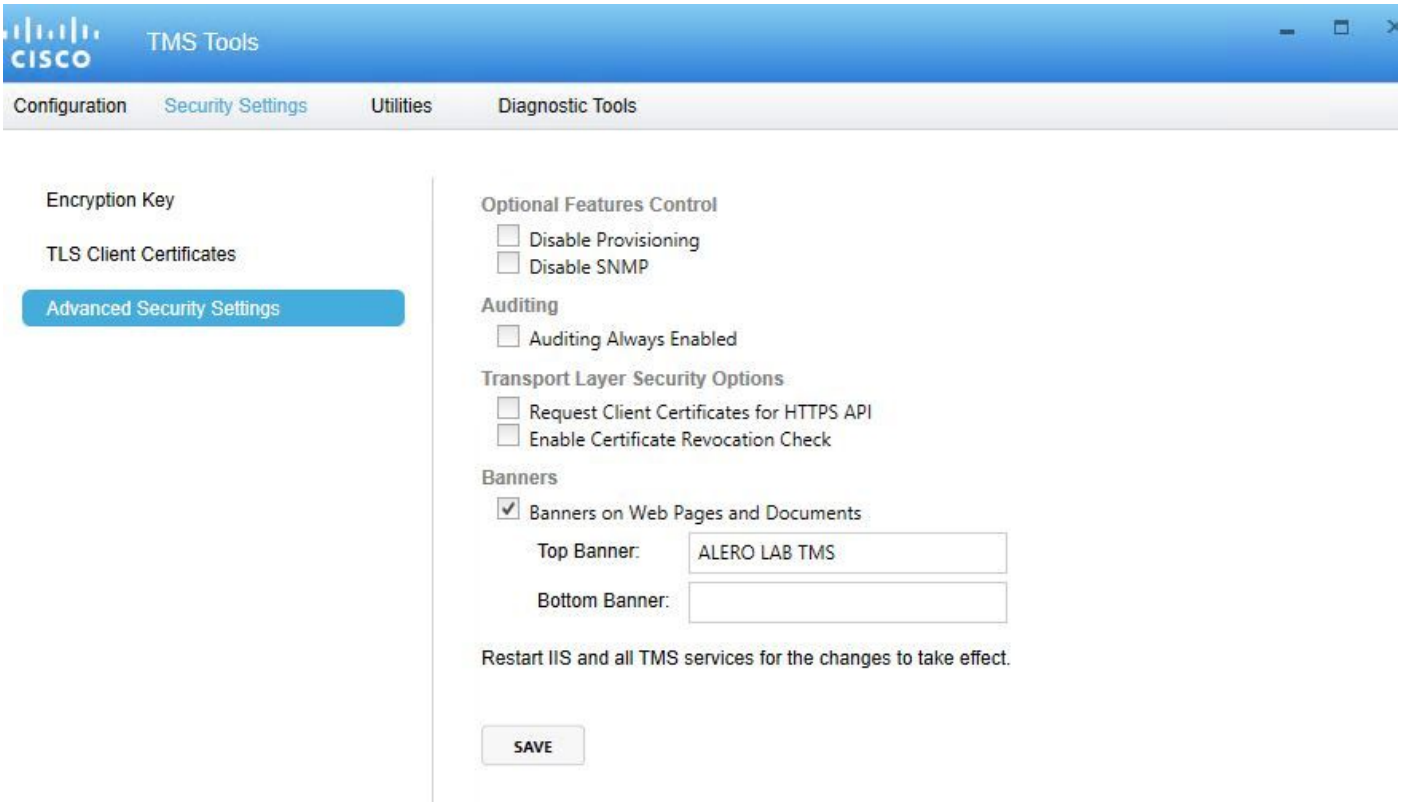
Etapa 1. Mesmo que a versão TLS 1.2 seja adicionada no registro



Etapa 2. O server TMS ainda não envia a versão apoiada pelo valor-limite em seus hellos de cliente SSL



Etapa 3. O problema encontra-se então no fato de que nós não podemos mudar as opções TLS em ferramentas TMS porque esta opção não está disponível



Etapa 4. Então a ação alternativa para esta edição é a elevação TMS a 15.x ou degrada seus valores-limite TC/CE a 7.3.3, esta edição é seguida no defeito do software CSCuz71542 criado para a versão 14.6.X.