Dépannage d'une erreur « Aucune réponse HTTPS » sur TMS après la mise à niveau des terminaux TC/CE

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Problème](#)
[Solution](#)
[Activer TLS 1.1 et 1.2 sur TMS Windows Server pour TMS 15.x et versions ultérieures](#)
[Modification de la sécurité dans l'outil TMS](#)
[Considérations relatives à la mise à niveau des paramètres de sécurité](#)
[Vérification](#)
[Pour les versions TMS inférieures à 15](#)

Introduction

Ce document décrit comment dépanner le message « no HTTPS response » sur Telepresence Management Suite (TMS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco TMS
- Serveur Windows

Components Used

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- TC 7.3.6 et versions ultérieures
- CE 8.1.0 et versions ultérieures
- TMS 15.2.1
- Windows Server 2012 R2
- SQL Server 2008 R2 et 2012

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

live, make sure that you understand the potential impact of any command.

Informations générales

Ce problème se produit lorsque les terminaux sont migrés vers le logiciel TC 7.3.6 et Collaboration Endpoint (CE) 8.1.0 ou version ultérieure.

Problème

Après une mise à niveau du point de terminaison vers TC7.3.6 ou supérieur ou 8.1.0 ou supérieur et la méthode de communication entre le point de terminaison et le TMS est configurée en tant que TLS (Transport Layer Security), le message d'erreur « no HTTPS response » apparaît sur le TMS en sélectionnant le point de terminaison, sous **System > Navigator**.

Cela se produit à la suite de ces situations.

- TC 7.3.6 et CE 8.1.0 et versions ultérieures ne prennent plus en charge TLS 1.0 selon les notes de version.
  http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf

- Par défaut, TLS versions 1.1 et 1.2 est désactivé sur le serveur Microsoft Windows.
- Les outils TMS utilisent par défaut la sécurité des communications moyennes dans ses options de sécurité de la couche transport.
- Lorsque TLS version 1.0 est désactivée et que TLS version 1.1 et 1.2 sont activés, TMS n'envoie pas d'Hello client SSL (Secure Socket Layer) après la réussite de la connexion TCP en 3 étapes avec le point de terminaison. Cependant, il est toujours possible de chiffrer les données à l'aide de TLS version 1.2.
- L'activation de TLS version 1.2 à l'aide d'un outil ou dans le Registre Windows n'est pas suffisante, car TMS n'enverra ou annoncera toujours que 1.0 dans ses messages Hello Client.

Solution

Le serveur Windows sur lequel TMS est installé doit avoir TLS version 1.1 et 1.2 activé, ce qui peut être réalisé avec la procédure suivante.

Activer TLS 1.1 et 1.2 sur TMS Windows Server pour TMS 15.x et versions ultérieures

Étape 1. Ouvrez une connexion Bureau à distance à Windows Server sur lequel TMS est installé.

Étape 2. Ouvrez l'éditeur du Registre Windows (**Start**->**Run**->**Regedit**).

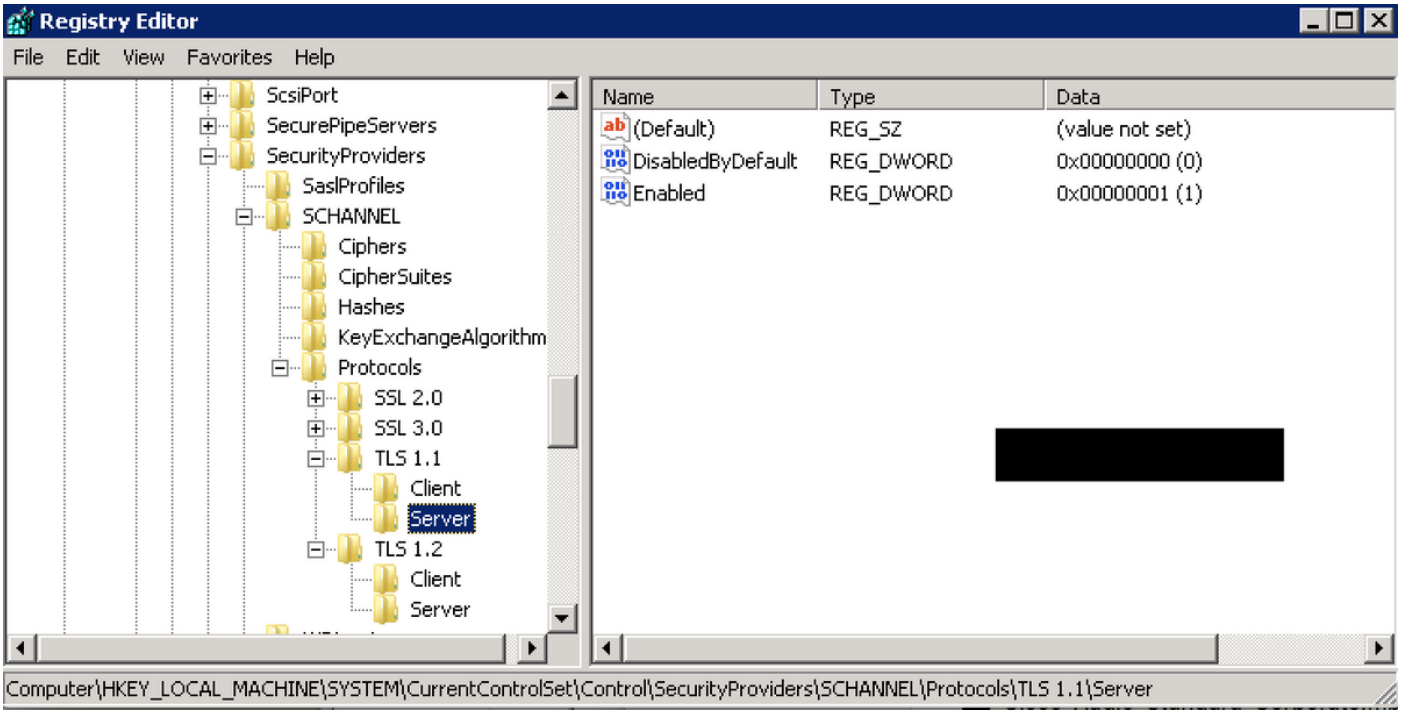
Étape 3. Sauvegarder le Registre.

Si vous êtes invité à saisir un mot de passe administrateur ou une confirmation, saisissez-le ou fournissez une confirmation.
Recherchez et cliquez sur la clé ou la sous-clé à sauvegarder.
Cliquez sur le menu Fichier, puis sur Exporter.
Dans la zone Enregistrer dans, sélectionnez l'emplacement où vous voulez enregistrer la copie de sauvegarde, puis tapez un nom pour le fichier de sauvegarde dans la zone Nom du fichier.
Click Save.

Étape 4. Activez TLS 1.1 et TLS 1.2.

Ouvrir le registre

Accédez à **HKEY_LOCAL_MACHINE** —> **SYSTEM** —> **CurrentControlSet** —> **Control** —> **SecurityProviders**—> **SCHANNEL** —> **Protocoles**
Ajout de la prise en charge TLS 1.1 et TLS 1.2
Créer des dossiers TLS 1.1 et TLS 1.2
Créer des sous-clés en tant que client et serveur



Créez **des DWORD** pour le client et le serveur pour chaque clé TLS créée.

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

Étape 5. Redémarrez le serveur Windows TMS pour vous assurer que TLS prend effet.

Note: Visitez ce lien pour obtenir des informations spécifiques sur les versions applicables https://technet.microsoft.com/en-us/library/dn786418%28v=ws.11%29.aspx#BKMK_SchannelTR_TLS12

Conseil : l'outil NARTAC peut être utilisé pour désactiver les versions TLS nécessaires après que vous avez fait cela que vous devez redémarrer le serveur. Vous pouvez le télécharger à partir de ce lien https://www.nartac.com/Products/IISCrypto/Download

Modification de la sécurité dans l'outil TMS

Lorsque les versions correctes sont activées, modifiez les paramètres de sécurité sur les outils TMS à l'aide de cette procédure.

Étape 1. Outils TMS ouverts

Étape 2. Accédez à **Paramètres de sécurité > Paramètres de sécurité avancés**

Étape 3. Sous **Options de sécurité de la couche transport**, définissez la sécurité des communications sur **Moyen-Élevé**

Étape 4. Cliquez sur **Save (enregistrer)**

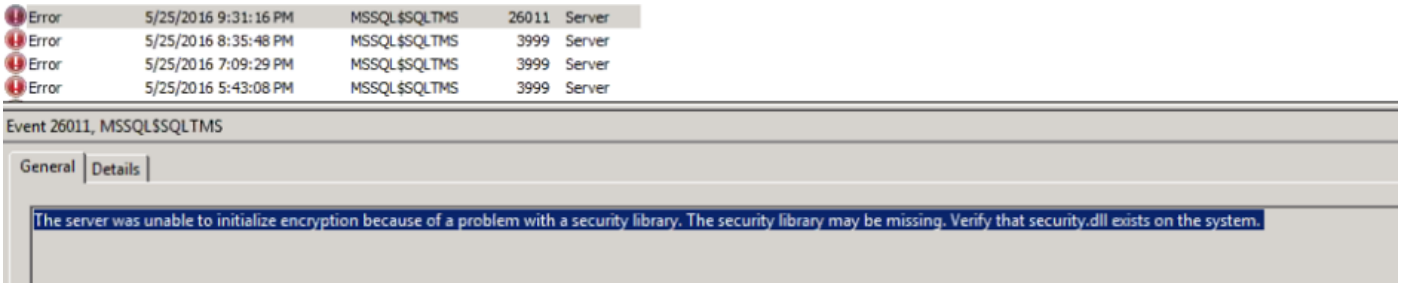
Étape 5. Redémarrez ensuite les services IIS (Internet Information Services) sur le serveur et **TMSDatabaseScannerService** et démarrez **TMSPLCMDirectoryService** (s'il est arrêté)

> **Avertissement :** : lorsque l'option TLS est remplacée par Medium-High (Moyen-Élevé) à partir de Medium, Telnet et SNMP (Simple Network Management Protocol) sont désactivés. Cela entraînera l'arrêt du service TMSSNMP et une alerte sera déclenchée sur l'interface Web de TMS.

Considérations relatives à la mise à niveau des paramètres de sécurité

Lorsque **SQL 2008 R2** est en cours d'utilisation et installé sur le serveur Windows TMS, nous devons nous assurer que TLS1.0 et SSL3.0 doivent également être activés, sinon le service SQL s'arrêtera et il ne démarrera pas.

Vous devez voir ces erreurs dans le journal des événements :

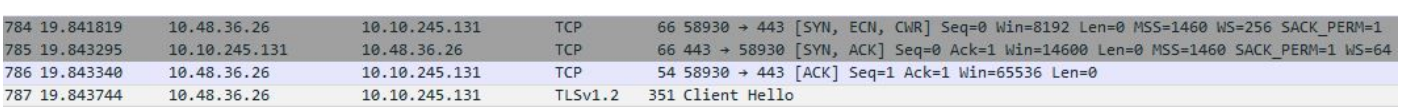


Lorsque **SQL 2012** est en cours d'utilisation, il doit être mis à jour pour s'attaquer au changement TLS s'il est installé sur le serveur Windows TMS (https://support.microsoft.com/en-us/kb/3052404)

Terminaux gérés à l'aide de SNMP ou Telnet show « Violation de sécurité : La communication Telnet n'est pas autorisée. »

Vérification

Lorsque vous changez l'option TLS de **Moyen** à **Moyen-Élevé,** cela garantit que TLS version 1.2 est annoncé dans le **client Hello** après la fin de la connexion TCP en trois étapes de TMS :



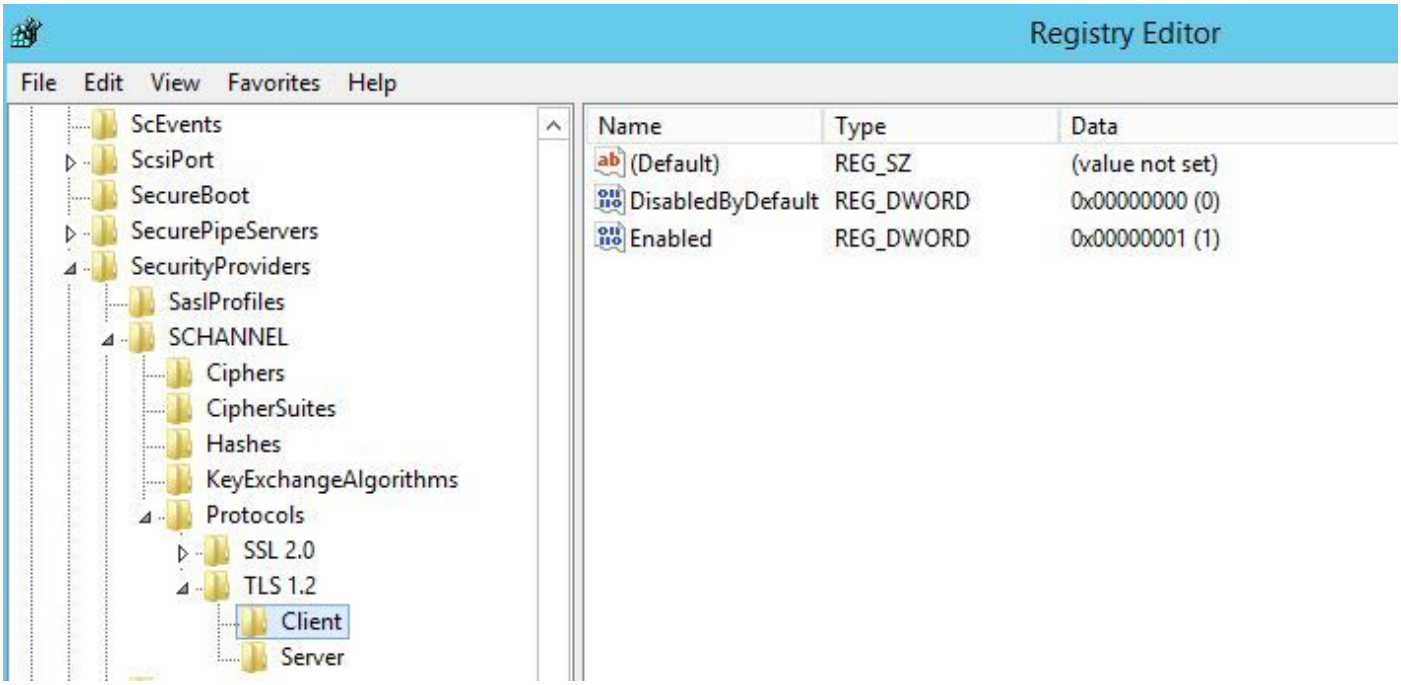
TLS version 1.2 annoncé :

```
▷ 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
```

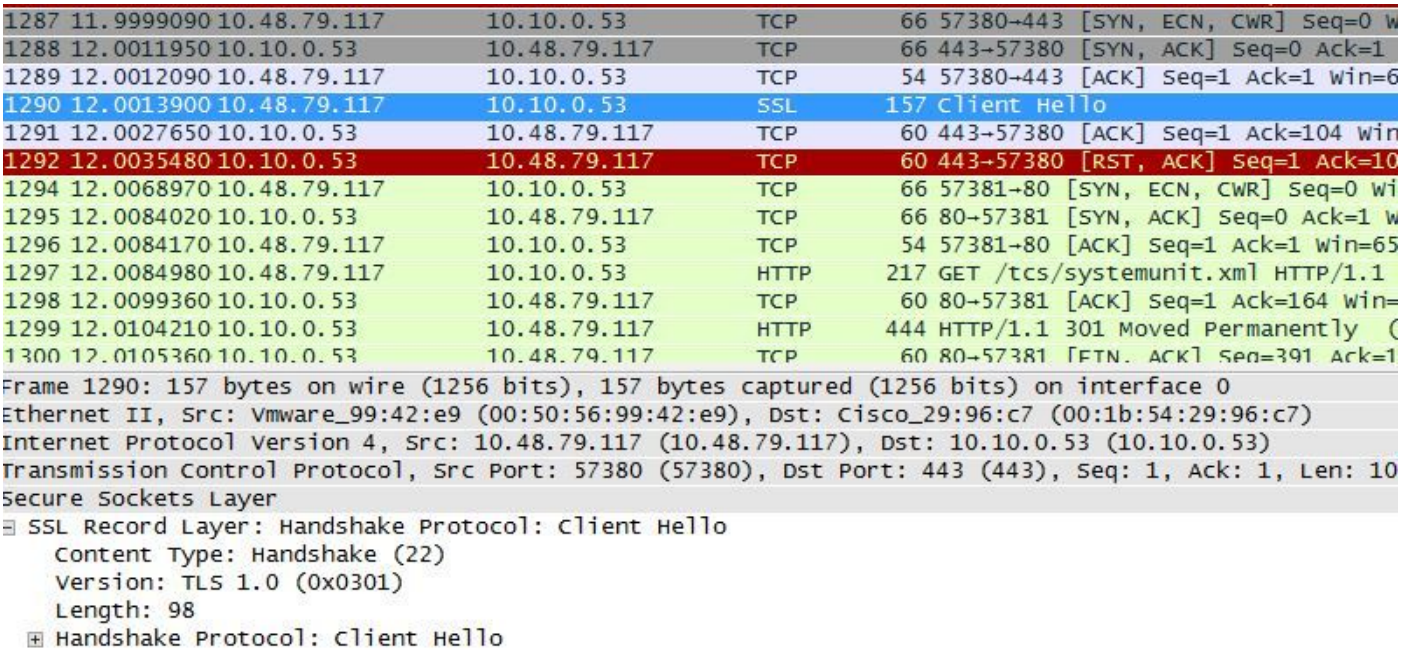
S'il est laissé à **moyen** TMS enverra seulement la version 1.0 dans le hello du client SSL pendant la phase de négociation qui spécifie la version de protocole TLS la plus élevée qu'il prend en charge en tant que client, ce que TMS est, dans ce cas.

Pour les versions TMS inférieures à 15

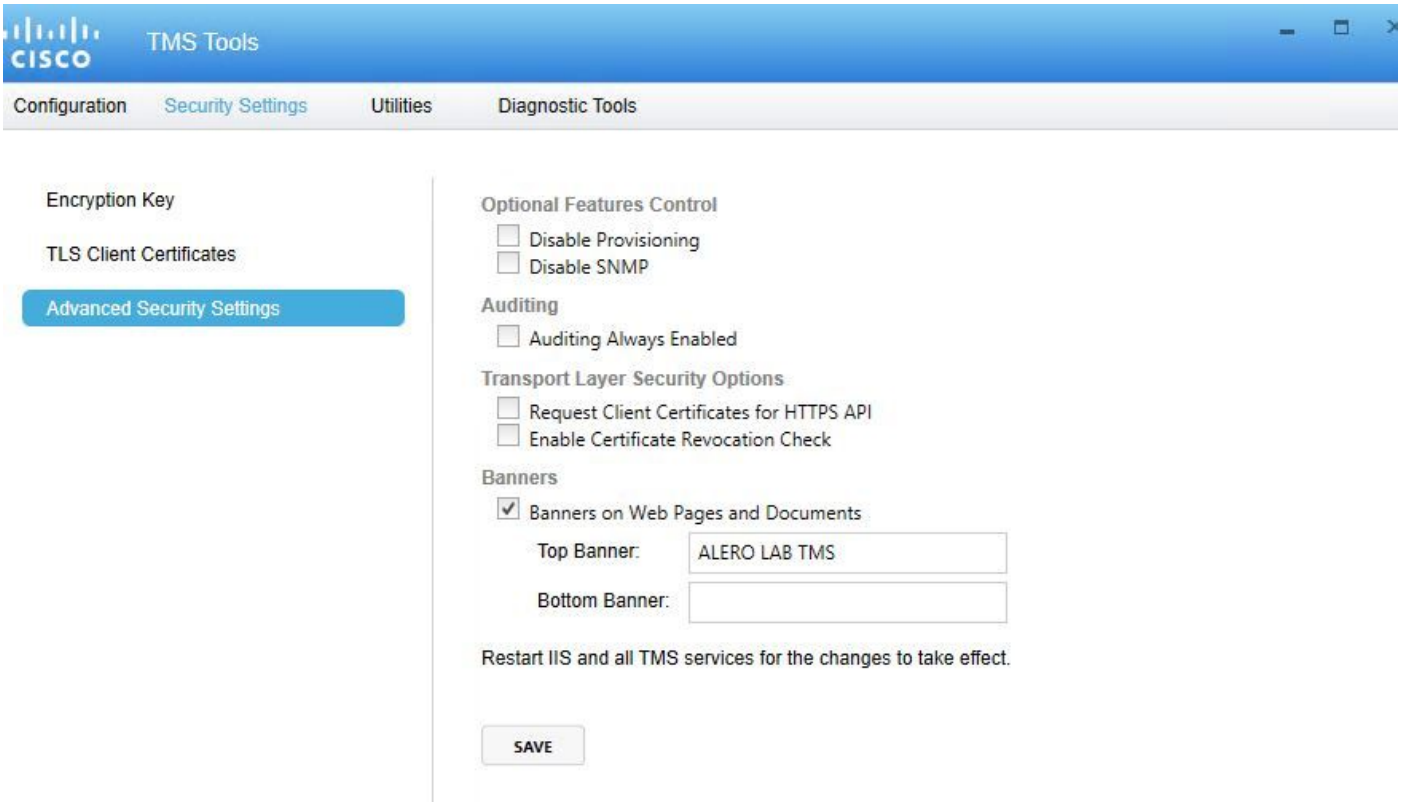
Étape 1. Même si la version 1.2 de TLS est ajoutée dans le Registre



Étape 2. Le serveur TMS n'envoie toujours pas la version prise en charge par le point de terminaison dans son Hello client SSL



Étape 3. Le problème réside alors dans le fait que nous ne pouvons pas modifier les options TLS dans les outils TMS, car cette option n'est pas disponible



Étape 4. Ensuite, la solution de contournement pour ce problème est de mettre à niveau TMS vers 15.x ou de rétrograder vos terminaux TC/CE vers 7.3.3, ce problème est suivi dans le défaut logiciel CSCuz71542 créé pour la version 14.6.X.