Comment dépanner l'erreur de « aucune réponse HTTPS » sur TMS après mise à jour de points finaux TC/CE

Contenu

Introduction

Ce document décrit comment dépanner le message de « aucune réponse HTTPS » sur la suite de gestion TelePresence (TMS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco TMS
- Windows Server

Composants utilisés

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

- Comité technique 7.3.6 et en haut
- CE 8.1.0 et en haut
- TMS 15.2.1
- Windows Server 2012 R2
- Serveur SQL 2008 R2 et 2012

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Cette question se produit quand les points finaux sont migrés vers le comité technique 7.3.6 et le logiciel 8.1.0 de point final de Collaboration (CE) ou en haut.

Problème

Après qu'une mise à jour de point final à TC7.3.6 ou en haut ou 8.1.0 ou en haut et le moyen de communication entre le point final et le TMS soit installée comme Transport Layer Security (TLS), le message d'erreur « aucune réponse HTTPS » s'affiche sur TMS en sélectionnant le point final, sous le **système** > le **navigateur**.

Ceci se produit en raison du ce des situations.

- Le comité technique 7.3.6 et le CE 8.1.0 et au-dessus de plus prennent en charge le TLS 1.0 selon les notes de mise à jour.
  http://www.cisco.com/c/dam/en/us/td/docs/telepresence/endpoint/software/tc7/release_notes/tc-software-release-notes-tc7.pdf

- Le serveur de Microsoft Windows fait désactiver des versions 1.1 et 1.2 de TLS par défaut.
- TMS usine la sécurité des communications moyenne d'utilisations dans ses options de Transport Layer Security par défaut.
- Quand la version 1.0 de TLS est désactivée et les deux TLS des versions 1.1 et 1.2 sont activées, TMS n'envoie pas le client de Protocole SSL (Secure Socket Layer) bonjour après que la prise de contact à trois voies de TCP réussisse avec le point final. Néanmoins encore capable chiffrer des données utilisant la version 1.2 de TLS.
- L'activation de la version 1.2 de TLS utilisant un outil ou dans le registre de Windows n'est pas assez, car la volonté TMS néanmoins seulement envoient ou annoncent 1.0 dans ses messages Hello de client.

Solution

Les Windows Server où le TMS est installé, doivent avoir des versions 1.1 et 1.2 de TLS activées, ceci peuvent être réalisés avec la prochaine procédure.

Activez le TLS 1.1 et 1.2 sur des Windows Server TMS pour TMS 15.x et plus élevé

Étape 1. Ouvrez Remote Desktop Connection aux Windows Server où TMS est installé.

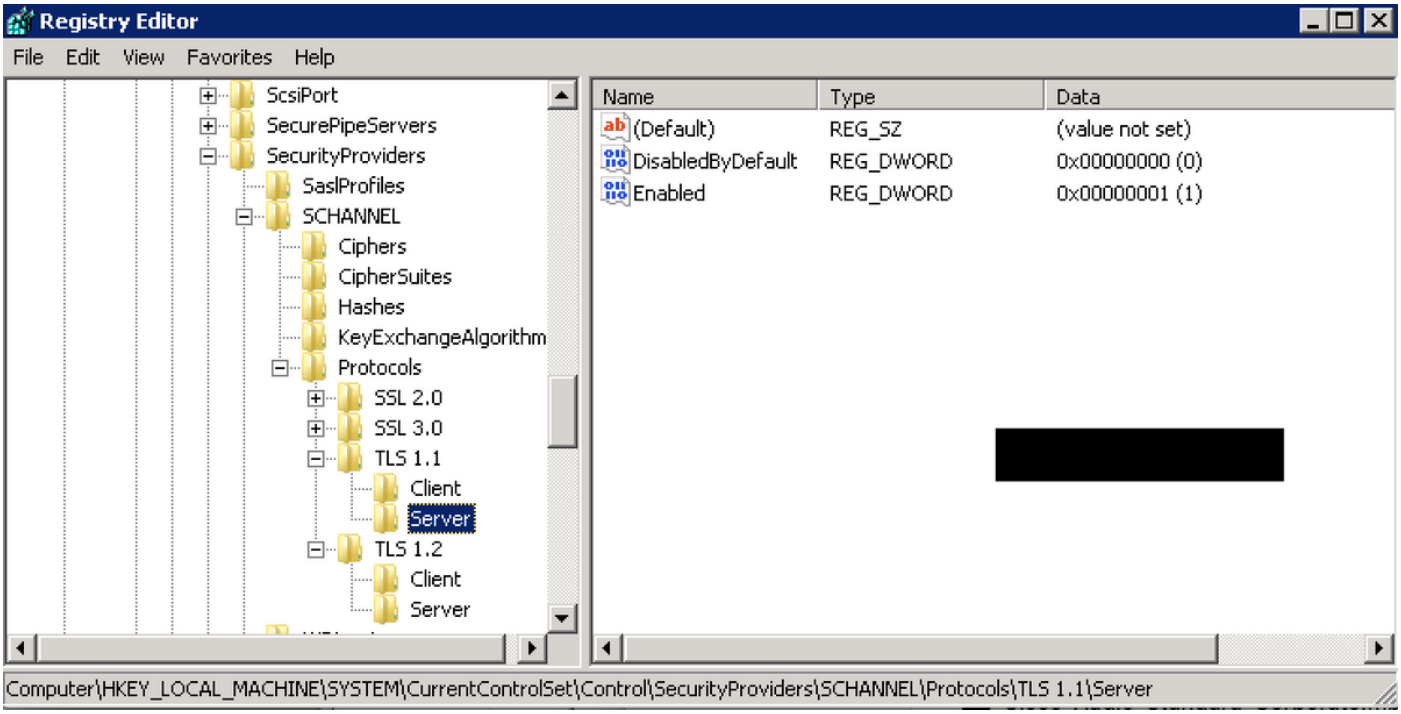
Étape 2. Éditeur de registre de Windows ouvert (**Start->Run->Regedit**).

Étape 3. Sauvegarde de prise de registre.

Si vous êtes incité pour un mot de passe administrateur ou une confirmation, tapez le mot de passe ou fournissez la confirmation.
Localisez et cliquez sur la clé ou la sous-clé que vous voulez sauvegarder.
Cliquez sur le menu File, et puis cliquez sur l'exportation.
Dans la sauvegarde dans la case, sélectionnez l'emplacement à où vous voulez sauvegarder la copie de sauvegarde, et puis introduisez un nom pour le fichier de sauvegarde dans la case de nom du fichier.
Cliquez sur **Save**.

Étape 4. TLS 1.1 d'enable et TLS 1.2.

Ouvrez le registre
Naviguez vers **HKEY_LOCAL_MACHINE** --> **SYSTÈME** --> **CurrentControlSet** --> **contrôle** --> **SecurityProviders**--> **SCHANNEL** --> **protocoles**
Ajoutez le support du TLS 1.1 et du TLS 1.2
Créez le TLS 1.1 et le TLS 1.2 répertoire
Créez les sous-titre-clés comme client et 'serveur



Créez **DWORDs** pour des les deux client et serveur pour chaque clé de TLS créée.

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

Étape 5. Les Windows Server de la reprise TMS pour assurer le TLS les prennent effet.

Remarque: Visitez ce lien pour des informations spécifiques sur des versions aplicable 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 nécessaires par TLS après que vous fassiez que vous devez redémarrer le serveur. Vous pouvez le télécharger de ce lien https://www.nartac.com/Products/IISCrypto/Download

Modification de la sécurité sur l'outil TMS

Quand les bonnes versions sont activées, changez les paramètres de sécurité sur des outils TMS avec cette procédure.

Étape 1. Ouvrez les outils TMS

Étape 2. Naviguez vers des **paramètres de sécurité** > des **configurations de sécurité avancée**

Étape 3. Sous des **options de Transport Layer Security**, placez la sécurité des communications à la Support-**haute**

Étape 4. **Sauvegarde de** clic

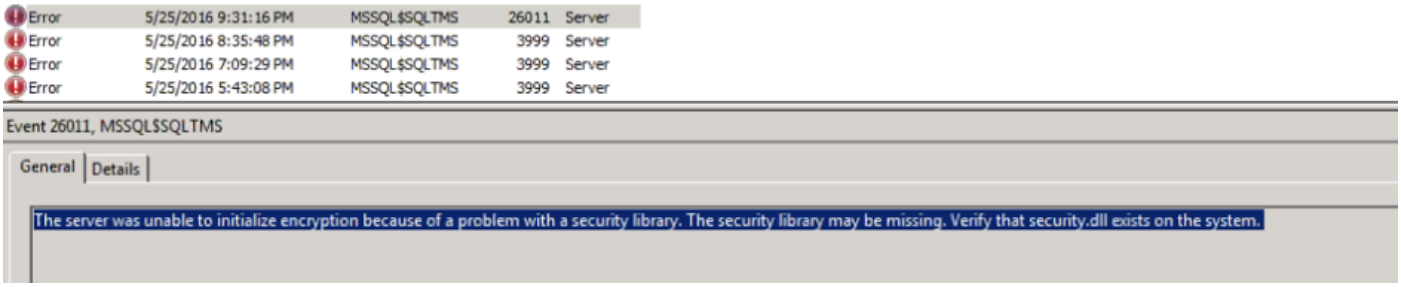
Étape 5. Alors redémarrez l'Internet Information Services (IIS) sur le serveur et **TMSDatabaseScannerService** et commencez **TMSPLCMDirectoryService** (s'il a arrêté)

> **Avertissement** : **: :** Quand l'option de TLS est changée à la Support-haute du support, le telnet et le Protocole SNMP (Simple Network Management Protocol) seront désactivés. Ceci entraînera à TMSSNMPservice pour arrêter et une alerte sera augmentée sur l'interface web TMS.

Considérations afin d'améliorer des paramètres de sécurité

Quand **SQL 2008 R2** est en service et installé sur des fenêtres serveur TMS, nous devons nous assurer que TLS1.0 et SSL3.0 devraient également être activés ou bien arrêt et lui de service SQL ne commencera pas.

Vous devez voir ce des erreurs sur le journal d'événements :

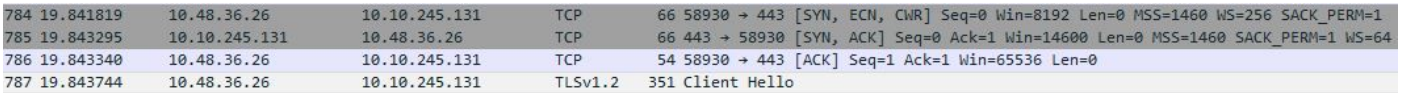


Quand **SQL 2012** est en service il exige d'être mis à jour pour aborder la modification de TLS si installé sur le serveur de fenêtres TMS (https://support.microsoft.com/en-us/kb/3052404)

Points finaux gérés utilisant violation de sécurité d'exposition SNMP ou de telnet la « : On ne permet pas la transmission de telnet ».

Vérifiez

Quand vous changez l'option de TLS du **support à la Support-haute,** ceci s'assure que la version 1.2 de TLS est annoncée dans le **client bonjour** après que la prise de contact à trois voies de TCP réussisse de TMS :



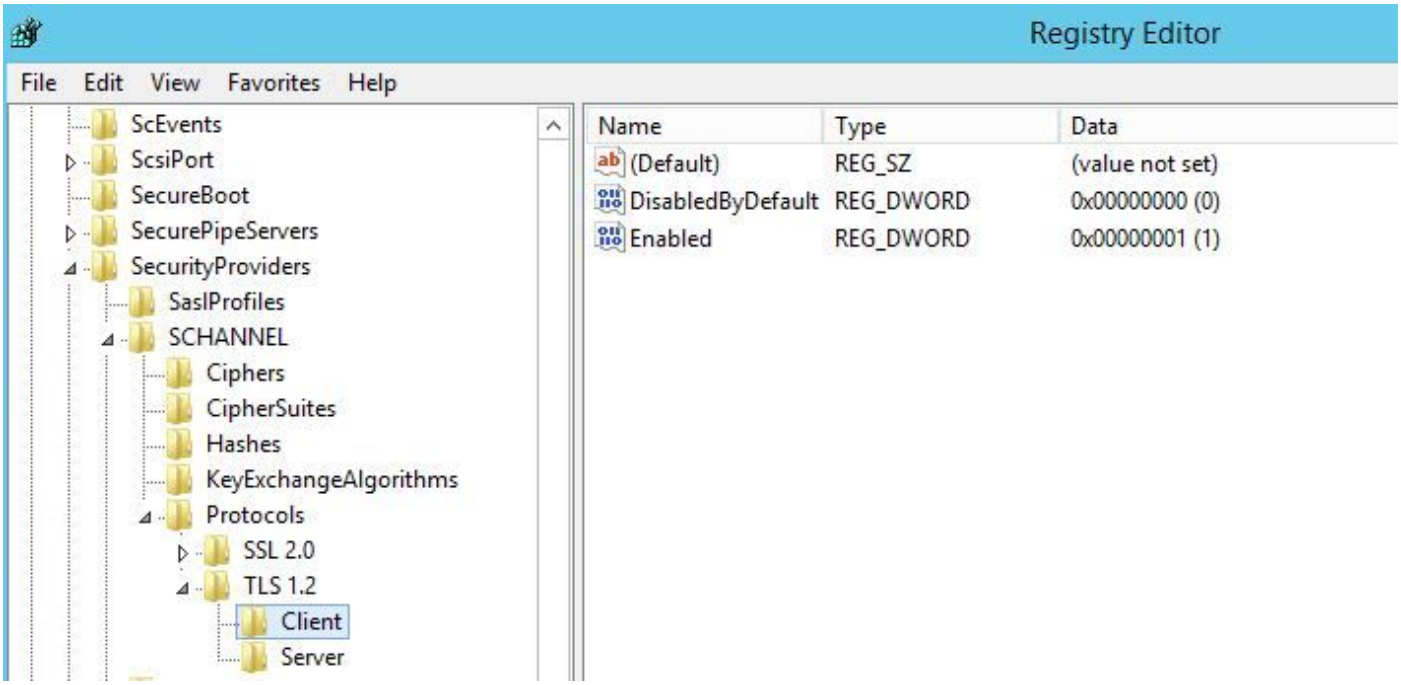
Version 1.2 de TLS annoncée :

```
▷ 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
```

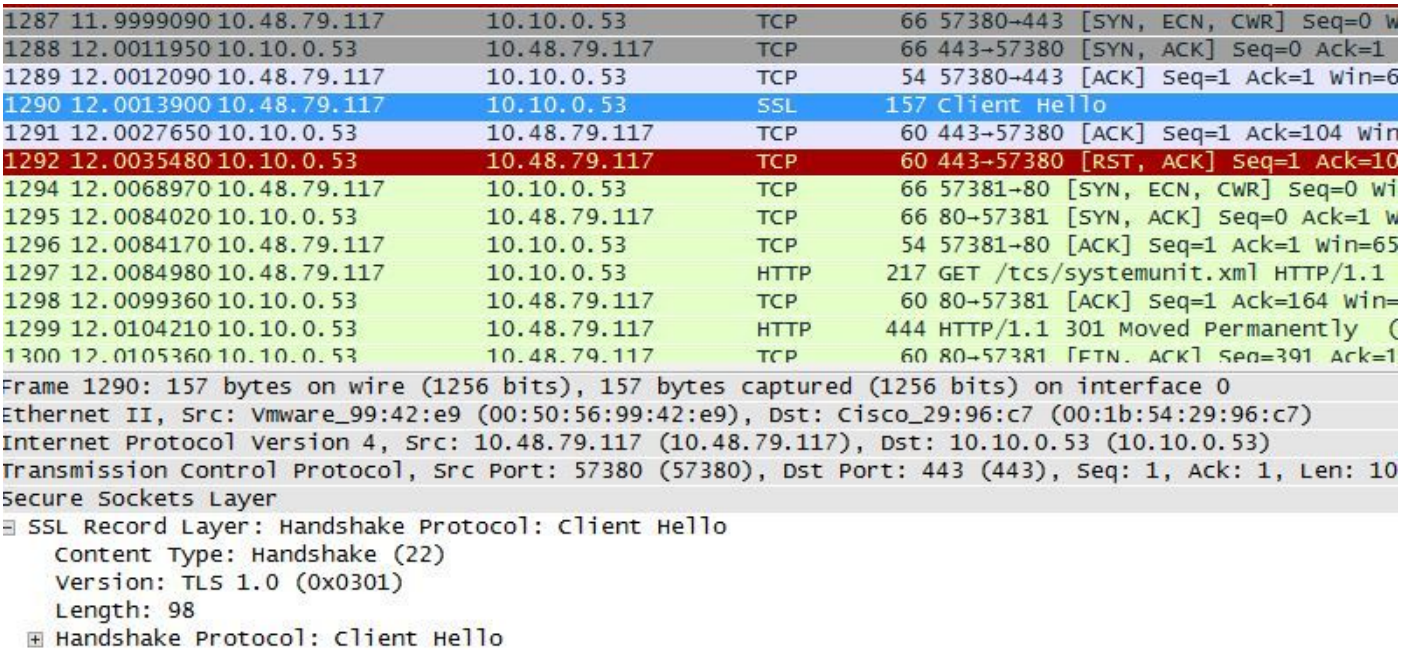
S'il est parti au **support** TMS seulement le send version 1.0 dans le client SSL bonjour pendant la phase de négociation qui spécifie la version de protocole de TLS la plus élevée qu'il le prend en charge en tant que client, qui TMS est, dans ce cas.

Pour TMS les versions diminuent que 15

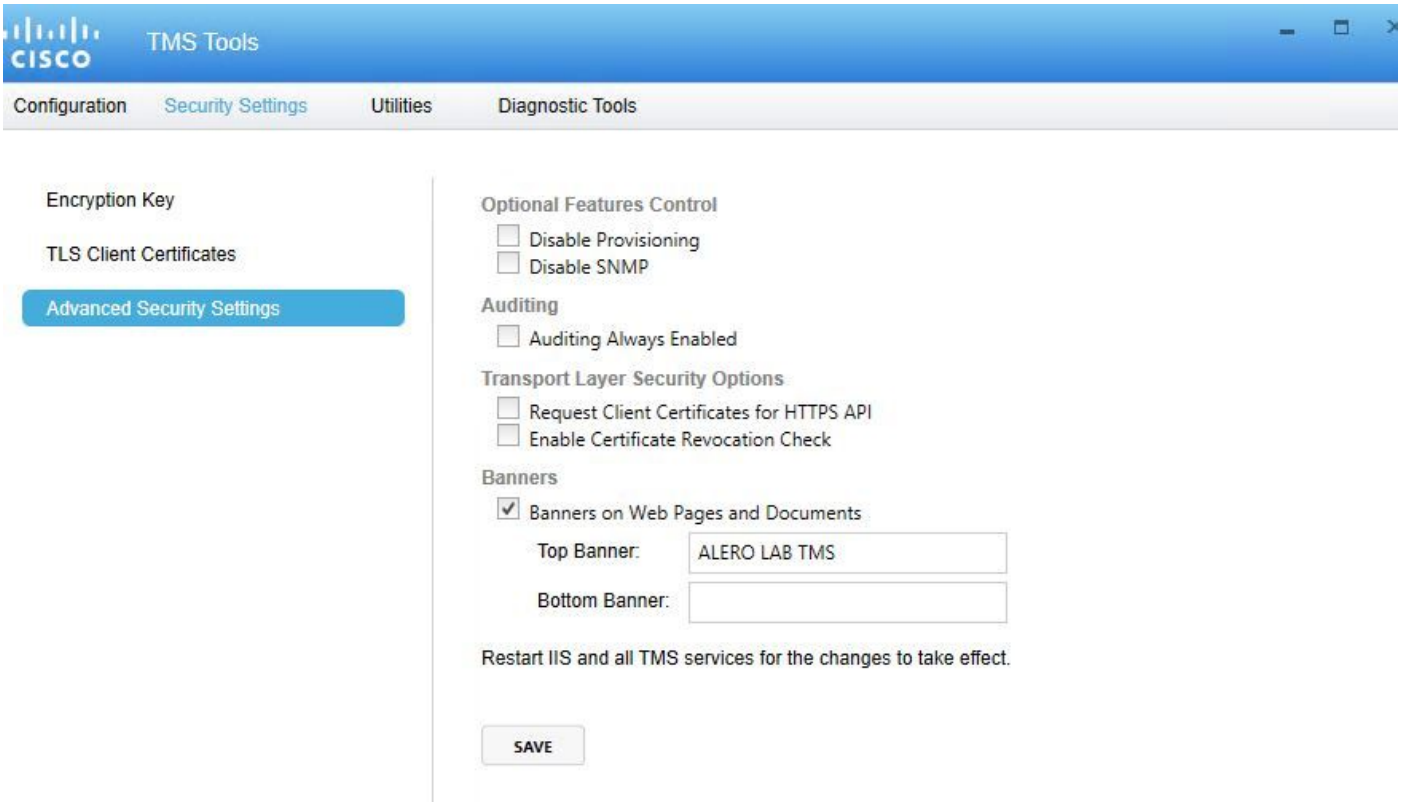
Étape 1. Quoique la version 1.2 de TLS soit ajoutée dans le registre



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



Étape 3. Le problème se situe alors dans le fait que nous ne pouvons pas changer les options de TLS dans des outils TMS car cette option n'est pas disponible



Étape 4. Alors le workaround pour cette question est la mise à jour TMS à 15.x ou déclassifie vos points finaux TC/CE à 7.3.3, cette question est dépisté dans l'erreur de logiciel CSCuz71542 créée pour la version 14.6.X.