TLS 通信用の TMS ツールを使用した TMS 証明 書の設定例

内容

<u>概要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>設定</u>
<u>確認</u>
<u>トラブルシュート</u>

概要

このドキュメントでは、TelePresence Management Suite(TMS)ツールを使用して、発信接続を 開始するときにTMSアプリケーションによって使用される証明書を設定する方法について説明し ます。TMSサーバがドメインの一部である場合、TMSツールに証明書作成オプションが表示され ない可能性があります。

前提条件

要件

Cisco では次の前提を満たす推奨しています。

- •TMSがインストールされ、HTTPおよびHTTPSからアクセス可能
- •インターネットインフォメーションサービス(IIS)サーバを再起動するためのアクセス
- ユーザーの管理者権限
- インストールする必要があるTransport Layer Security(TLS)証明書へのアクセス

使用するコンポーネント

このドキュメントの情報は、TMSバージョン14.3.2、14.2.2、および14.5に基づくものです。

このドキュメントのすべてのスクリーンショットは、TMSバージョン14.5インターフェイスのものです。他のバージョンの証明書も、同じ手順で生成できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

設定

TMSサーバから完全なTLS通信を行い、TMSでTLS証明書を使用する場合は、TMSツールで設定 する必要があります。

alialia cisco	TMS Tools						
Configuration	Security Settings	Utilities	Diagnostic Tools				
Encryption Key TLS Client Certificates Advanced Security Settings			The list shows certificates available in the local computer's personal trust store. Select one or more certificates for Cisco TMS to use when initiating outbound connections and click Save. The private keys of all selected certificates must be readable by the accounts which run the Cisco TMS web application and processes.				
			SUBJECT	ISSUER	EXPIRES		
			Restart IIS and all TMS set	vices for the changes to tak	e effect. Certificate(s) selected.	VIEW CERTIFICATE	

システムの個人証明書ストアから証明書が表示されます。この画面には、サーバの個人信頼スト アで現在使用可能な証明書が一覧表示されます。この証明書は、前述のように選択して使用でき ます。

次に示す証明書の管理者ガイドには、2つの要件が記載されています。

- ここに証明書がリストされていない場合は、Cisco TMSツールを実行するために使用するア カウントに、証明書の秘密キーへの読み取りアクセス権があることを確認します。
- •TMSサービスがログオンしているすべてのアカウントが、証明書の秘密キーに読み取りアク セスできることを確認します。

個人信頼ストアに証明書をインストールするには、Microsoft管理コンソール(MMC)を開き、証明 書のスナップインを追加する必要があります。

1. Microsoft Windowsサーバで実行するMMCを開きます。

2. MMCで証明書スナップインを追加します。

·	Console1 - [Console Root]	_ 0 X
🖀 File Action View Favorites Window	Help	- <i>0</i> ×
🗢 🔶 📷 🔂 🖬 📷		
🔁 Console Root	Name	Action
	There are no items to show in this view.	Console Root
		More Actions +
	Add or Remove Snap-ins	
	You can select snap-ins for this console from those evaluate on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.	
	Available shap-inc: Selected shap-inc:	
	Snap-in Vendor A Contole Root Edit Extensions	
	ActiveX Centrel Microsoft Cor Remove	
	Cartification Microsoft Cor	
	Konsonent Services Microsoft Cor Move Up	
	Device Manager Microsoft Cor Hove Down	
	Monostration Microsoft and Add >	
	Contract Provider Microsoft Cor	
	Group Policy Object Hisrosoft Cor	
	Internet Informatio Microsoft Cor If Security Monitor Microsoft Cor	
	IP Security Policy M Microsoft Cor	
	Littlichk to Web Address Microsoft Cor Y	
	Description: The Cartificates scenario allows way to because the contents of the cartificate stores for wayself, a service, or a computer	
	The coloradia and there is a contract in contract of the collected to be an a state of the collected of the company.	
	OK Caros	
	I	J
L		

3. 証明書がコンピュータアカウントに追加されていることを確認してください。

a	Console1 - [Console Root]		_ 0 X
Tile Action View Fevorites Window	Help		- 0 ×
🗢 🔿 💼 📴 💼			
Console Root	Name	Actions	
	There are no items to show in this view.	Console Root	•
		More Actions	,
	Add or Domon Case inc		
	Ceruncates shap-in distances of shapins. For		
	This snap-in will always manage cartificates for:		
	O Ny user account Edit Extensions		
	Computer account Remove		
	Move Lin		
	Nove forum		
	The sound		
	Advanced		
	< Back. Next > Cancel A computer.		
	OK Canod		
L			

4. [Personal] > [Certificates]で証明書をインポートし、[Manage Private Keys]をクリックしま す。



- 5. TMSツールにアクセスできるすべてのユーザにアクセス権を追加し、読み取りアクセス権を 付与します。
- 6. TMSツールを開き、[TLS Client Certificates]に移動します。

altalia cisco	TMS Tools					
Configuration	Security Settings	Utilities	Diagnostic Tools			
Encryption Key TLS Client Certificates Advanced Security Settings		S S S	The list shows certificates tore. elect one or more certificates for ave. he private keys of all selected cer- leb application and processes. SUBJECT CN=tms14.tplab1.local, O CN=tmsxe14-4-cl-2.tplab1	a vailable in the local Cisco TMS to use when initia tificates must be readable by ISSUER CN=tplab1-DCTMS1-CA, CN=tmsxe14-4-cl-2.tplab1	I computer's per ating outbound conne y the accounts which EXPIRES 4/22/2016 4/17/2114	rsonal trust ctions and click run the Cisco TMS
		R	estart IIS and all TMS services fo	r the changes to take effect.		VIEW CERTIFICATE

7. [Save]をクリックし、IISを再起動します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。