Exemplo de Configuração de Certificados TMS com Ferramentas TMS para Comunicação TLS

Contents

Introduction Prerequisites Requirements Componente usado Configurar Verificar Troubleshoot

Introduction

Este documento descreve como usar a ferramenta TelePresence Management Suite (TMS) para configurar o certificado usado pelo aplicativo TMS ao iniciar conexões de saída. Se o servidor TMS fizer parte de um domínio, a opção de criação de certificado pode não estar visível na ferramenta TMS.

Prerequisites

Requirements

A Cisco recomenda que você:

- TMS instalado e acessível por HTTP e HTTPS
- Acesso para reiniciar o servidor do Internet Information Services (IIS)
- Direitos de administrador para o usuário
- Acesso ao certificado TLS (Transport Layer Security) que deve ser instalado

Componente usado

As informações neste documento são baseadas nas versões 14.3.2, 14.2.2 e 14.5 do TMS.

Todas as capturas de tela neste documento são da interface TMS versão 14.5. Os certificados para outras versões também podem ser gerados com o mesmo procedimento.

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.

Configurar

Quando você quiser ter uma comunicação TLS completa do servidor TMS e quiser que o TMS use um certificado TLS, configure-o com as ferramentas do TMS.



Você deve ver o certificado aqui do repositório de certificados pessoais no sistema. Esta tela lista os certificados disponíveis no momento no repositório de confiança pessoal do servidor que podem ser selecionados para serem usados conforme descrito anteriormente.

Há dois requisitos mencionados no guia do administrador para que o certificado seja listado aqui:

- Se não houver certificados listados aqui, verifique se a conta usada para executar as Ferramentas do Cisco TMS tem acesso de leitura às chaves privadas dos certificados.
- Certifique-se de que todas as contas em que os serviços do TMS estão conectados tenham acesso de leitura às chaves privadas dos certificados.

Para instalar um certificado em um repositório de confiança pessoal, você precisa abrir o Microsoft Management Console (MMC) e adicionar Snap-in para certificado:

- 1. Abra o MMC com execução no servidor Microsoft Windows.
- 2. Adicione o Snap-in de certificado no MMC:

·	Console1 - [Console Root]		_ 0 X
🖀 File Action View Favorites Window	Help		_ # ×
🗢 🔶 📅 🕞 📓 🖬			
🗀 Console Root	Name	Actions	
	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 similable on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are embled.		
	Available snap-ins: Selected snap-ins:		
	Snap-in Vendor A Console Root Edit Extensions		
	ActiveX Control Microsoft Cor Remove		
	Contificates Microsoft Cor		
	Component Services Microsoft Cor Microsoft Cor Microsoft Cor		
	Device Manager Microsoft Cor Hove Down		
	A00 >		
	Color Moraeft Cor		
	Group Policy Object Microsoft Cor		
	B P Seavity Monitor Microsoft Cor		
	S IP Security Policy M Microsoft Cor Advanced		
	Entre Diversion Address Provision Con		
	The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.		
	OK Carol		
	J		_
Les			

3. Certifique-se de adicionar o certificado na conta Computador:

a		Console1 - [Console Root]			- 0 X
File Action View Favorites Window	Help				- 0 ×
(* •) 🖬 🖬 🖬					
Console Root	Name			Actions	
		There are no items to show in this vie	EW.	Console Root	•
				More Actions	,
		Add or Domorn Coon inc	X		
	I	Certificates snap-in	af shap ins. For		
	This snap-in will alway	a manage certificates for			
	O My user account		Felt Federations		
	O Service account		Concerne and a concerne a		
	Computer account	1	Renove		
			Move Up		
			Move Down		
			_		
			Advanced		
		and the second			
		< Back Nod >	Cancel a computer.		
			OK Cancel		

4. Importe o certificado em **Pessoal > Certificados** e clique em **Gerenciar Chaves Privadas**:



- 5. Adicione acesso a todos os usuários através dos quais a ferramenta TMS pode ser acessada e forneça acesso de leitura.
- 6. Abra as Ferramentas TMS e navegue até Certificados de Cliente TLS:

altalta cisco	TMS Tools					
Configuration	Security Settings	Utilities	Diagnostic Tools			
Encryption TLS Client Advanced	Key Certificates Security Settings		The list shows certificates store. Select one or more certificates for save. The private keys of all selected cer web application and processes. SUBJECT CN=tms14.tplab1.local, O CN=tmsxe14-4-cl-2.tplab1	a vailable in the loca Cisco TMS to use when initia tificates must be readable b ISSUER CN=tplab1-DCTMS1-CA, CN=tmsxe14-4-cl-2.tplab1	il computer's per ating outbound conner y the accounts which in EXPIRES 4/22/2016 4/17/2114	sonal trust ctions and click run the Cisco TMS
			SAVE	-		

7. Clique em Salvar e reinicie o IIS.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.