Gerencia certificados auto-assinados do SHA-256 para serviços de Web de Cisco UCCE

Índice

Introdução

Este documento descreve um processo de gerar certificados auto-assinados usando o algoritmo da assinatura do certificado do SHA-256 para serviços de Web do Cisco Unified Contact Center Enterprise (UCCE) como a instalação da Web ou a administração CCE.

Problema

Cisco UCCE tem diversos serviços de Web hospedados pelo server do Internet Information Services de Microsoft (IIS). Microsoft IIS no desenvolvimento UCCE à revelia está usando certificados auto-assinados com algoritmo da assinatura do certificado SHA-1.

O algoritmo SHA-1 é considerado inseguro pela maioria dos navegadores, consequentemente em algum momento as ferramentas críticas como a administração CCE usada por supervisores para a nova formação do agente podem tornar-se não disponíveis.

Solução

A solução a esse problema é gerar Certificados do SHA-256 para que o servidor IIS use-se.

> **aviso:** Recomenda-se usar certificados assinados do Certificate Authority. Assim gerar os certificados auto-assinados descritos aqui deve ser considerada como uma solução temporária para restaurar rapidamente o serviço.

> Nota: Caso que o aplicativo do editor de script dos internet de ICM é usado para o Gerenciamento remoto do script há uma necessidade de usar a utilidade da criptografia SSL para gerar o certificado para ele.

Solução para WebSetup e administração CCE

1. Ligue a ferramenta de Windows PowerShell no server UCCE.

2. Em PowerShell datilografe o comando

```
New-SelfSignedCertificate -DnsName "pgb.allevich.local" -CertStoreLocation
"cert:\LocalMachine\My"
```

Onde o parâmetro após **DnsName** especificará o Common Name (CN) do certificado. Substitua o parâmetro após DnsName ao correto para o server. O certificado será gerado com uma validez de um ano.

> Nota: O Common Name no certificado tem que combinar o nome de domínio totalmente qualificado (FQDN) do server.

3. Abra a ferramenta do Microsoft Management Console (MMC). **Arquivo** seleto - o **>** Add**/remove Pressão-em…** - **>** os **Certificados** seletos, escolhem a **conta do computador** e **adicionar-la ao pressão-**INS selecionado. Pressione está bem, a seguir navegue ao **fundamento de console** - **> Certificados (computador local)** - **> pessoal** - **> Certificados**.

Assegure-se de que o certificado recém-criado este presente aqui. O certificado não terá o nome amigável configurado, assim que pode-se reconhecer com base em seus CN e data de expiração.

O nome amigável pode ser atribuído ao certificado selecionando as **propriedades do** certificado e enchendo a caixa de texto **amigável do nome** com o nome apropriado.

4. Comece o gerente do Internet Information Services (IIS). A website padrão seleta IIS e no painel correto escolhe **emperramentos**. **HTTPS** seleto - **> edite** e do certificado gerado SHA-256 auto-assinado seleto da lista do certificado SSL.

5. Reinicie o serviço do “Serviço de Publicação na Web”.

Solução para o pórtico diagnóstico da estrutura

1. Repita as etapas 1-3.

Um certificado auto-assinado novo será gerado. Para a ferramenta do pórtico há uma outra maneira de ligar o certificado.

2. Remova o certificado atual que liga para a ferramenta do pórtico.

```
cd c:\icm\serviceability\diagnostics\bin

DiagFwCertMgr /task:UnbindCert
```

3. Ligue o certificado auto-assinado gerado para o pórtico.

Abra o certificado auto-assinado gerado para a ferramenta do pórtico e selecione a aba dos **detalhes**. Copie o valor de Thumbprint ao editor de texto.

> Nota: Em alguns editores de texto o thumbprint prepended automaticamente com um ponto de interrogação. Remova-o.

Remova todos os caracteres de espaço do thumbprint e use-os no comando seguinte.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:<thumbprint-value>
```

4. Assegure-se de que o emperramento do certificado esteja bem sucedido usando este comando.

```
DiagFwCertMgr /task:ValidateCertBinding
```

A mensagem similar deve ser indicada na saída.
“O emperramento do certificado é VÁLIDO”

5. Reinicie o serviço diagnóstico da estrutura.

```
sc stop "diagfwsvc"
sc start "diagfwsvc"
```

Verificação

Cancele o cache de navegador e a história. Alcance o página da web do serviço da administração CCE e você deve obter um aviso do certificado auto-assinado.

Veja os detalhes certificados e assegure-se de que o certificado tenha o algoritmo da assinatura do certificado do SHA-256.

Artigos relacionados

Gerencia o certificado assinado de CA para a ferramenta diagnóstica do pórtico UCCE

Gerencia o certificado assinado de CA para a instalação da Web UCCE

Gerencia o certificado assinado de CA para o server baseado VOS usando o CLI

Gerencia o certificado assinado de CA para o server CVP OAMP