Genere los certificados autofirmados del SHA-256 para los servicios web de Cisco UCCE

Contenido

Introducción

Este documento describe un proceso de generar los certificados autofirmados usando el algoritmo de la firma del certificado del SHA-256 para los servicios web del Cisco Unified Contact Center Enterprise (UCCE) como la configuración de la red o la administración CCE.

Problema

Cisco UCCE tiene varios servicios web recibidos por el servidor de los Servicios de Internet Information Server de Microsoft (IIS). Microsoft IIS en el despliegue UCCE por abandono está utilizando los certificados autofirmados con el algoritmo de la firma del certificado SHA-1.

El algoritmo SHA-1 es considerado unsecure por la mayor parte de los navegadores, por lo tanto en algún momento las herramientas críticas como la administración CCE usada por los supervisores para la readaptación del agente pueden llegar a ser inasequibles.

Solución

La solución a ese problema es generar los Certificados del SHA-256 para que el servidor IIS utilice.

> Advertencia: Se recomienda para utilizar los certificados firmados del Certificate Authority. Tan la generación de los certificados autofirmados descritos aquí se debe considerar como solución provisoria para restablecer el servicio rápidamente.

Solución para WebSetup y la administración CCE

1. Encienda la herramienta de Windows PowerShell en el servidor UCCE.

2. En PowerShell teclee el comando

```
New-SelfSignedCertificate -DnsName "pgb.allevich.local" -CertStoreLocation
```

```
"cert:\LocalMachine\My"
```

Donde el parámetro después de **DnsName** especificará el Common Name (CN) del certificado. Substituya el parámetro después de DnsName el correcto para el servidor. El certificado será generado con una validez de un año.

> Nota: El Common Name en el certificado tiene que hacer juego el nombre de dominio completo (FQDN) del servidor.

3. Abra la herramienta del Microsoft Management Console (MMC). **Archivo** selecto - > Add/**quite Broche-en…** - > los **Certificados** selectos, eligen la **cuenta de la Computadora** y **la agregan al broche-**INS seleccionado. Presione OK, después navegue a la **Raíz de la consola** - > **certifica (computadora local)** - > **personal** - > los **Certificados**.

Asegúrese de que el certificado creado recientemente esté presente aquí. El certificado no tendrá nombre descriptivo configurado, así que puede ser reconocido sobre la base de su CN y fecha de vencimiento.

El nombre descriptivo se puede asignar al certificado seleccionando las **propiedades del** certificado y llenando el textbox del **nombre descriptivo del** nombre apropiado.

4. Comience al administrador de los Servicios de Internet Information Server (IIS). El Sitio Web predeterminado selecto IIS y en el panel derecho elige los **atascamientos**. **HTTPS** selecto - > **edite** y del certificado generado SHA-256 uno mismo-firmado selecto de la lista del certificado SSL.

5. Recomience el servicio del “servicio editorial de Internet”.

> Nota: No hay necesidad de desatar o de atar el certificado en la herramienta de la utilidad de la encripción de SSL.

Solución para el pórtico de diagnóstico del marco

1. Relance los pasos 1-3.

Un nuevo certificado autofirmado será generado. Para la herramienta del pórtico hay otra manera de atar el certificado.

2. Quite el certificado actual que ata para la herramienta del pórtico.

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

DiagFwCertMgr /task:UnbindCert
```

3. Ate el certificado autofirmado generado para el pórtico.

Abra el certificado autofirmado generado para la herramienta del pórtico y seleccione la copia de cuadro de los **detalles el** valor de Thumbprint al editor de textos.

> Nota: En algunos editores de textos el thumbprint prepended automáticamente con un signo de interrogación. Quítelo.

Quite todos los caracteres de espacio del thumbprint y utilícelos en el siguiente comando.

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

4. Asegúrese de que el atascamiento del certificado fuera acertado usando este comando.

```
DiagFwCertMgr /task:ValidateCertBinding
```

El mensaje similar se debe visualizar en la salida.

“El atascamiento del certificado es VÁLIDO”

5. Recomience el servicio de diagnóstico del marco.

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

Verificación

Borre el caché del buscador y el historial. Acceda la página web del servicio de la administración CCE y usted debe conseguir una advertencia del certificado autofirmado.

Vea a los detalles del certificado y asegúrese de que el certificado tiene algoritmo de la firma del certificado del SHA-256.

Artículos relacionados

Genere el certificado firmado de CA para la herramienta de diagnóstico del pórtico UCCE

Genere el certificado firmado de CA para la configuración de la red UCCE

Genere el certificado firmado de CA para el servidor basado VOS usando el CLI

Genere el certificado firmado de CA para el servidor del CVP OAMP