Acceso de la configuración HTTPS para la herramienta de diagnóstico del pórtico del marco UCCE con el certificado firmado del Certificate Authority (CA)

Contenido

Introducción

Este documento describe el proceso de configuración en cómo instalar el certificado firmado de CA para la herramienta de diagnóstico unificada del pórtico del marco de la empresa del Centro de contacto (UCCE).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Active Directory
- Servidor del Domain Name System (DNS)
- Infraestructura de CA desplegada y que trabaja para todos los servidores y cliente
- Pórtico de diagnóstico del marco

Acceder la herramienta de diagnóstico del pórtico del marco tecleando la dirección IP en el navegador sin la recepción de la advertencia del certificado está fuera de alcance de este artículo.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

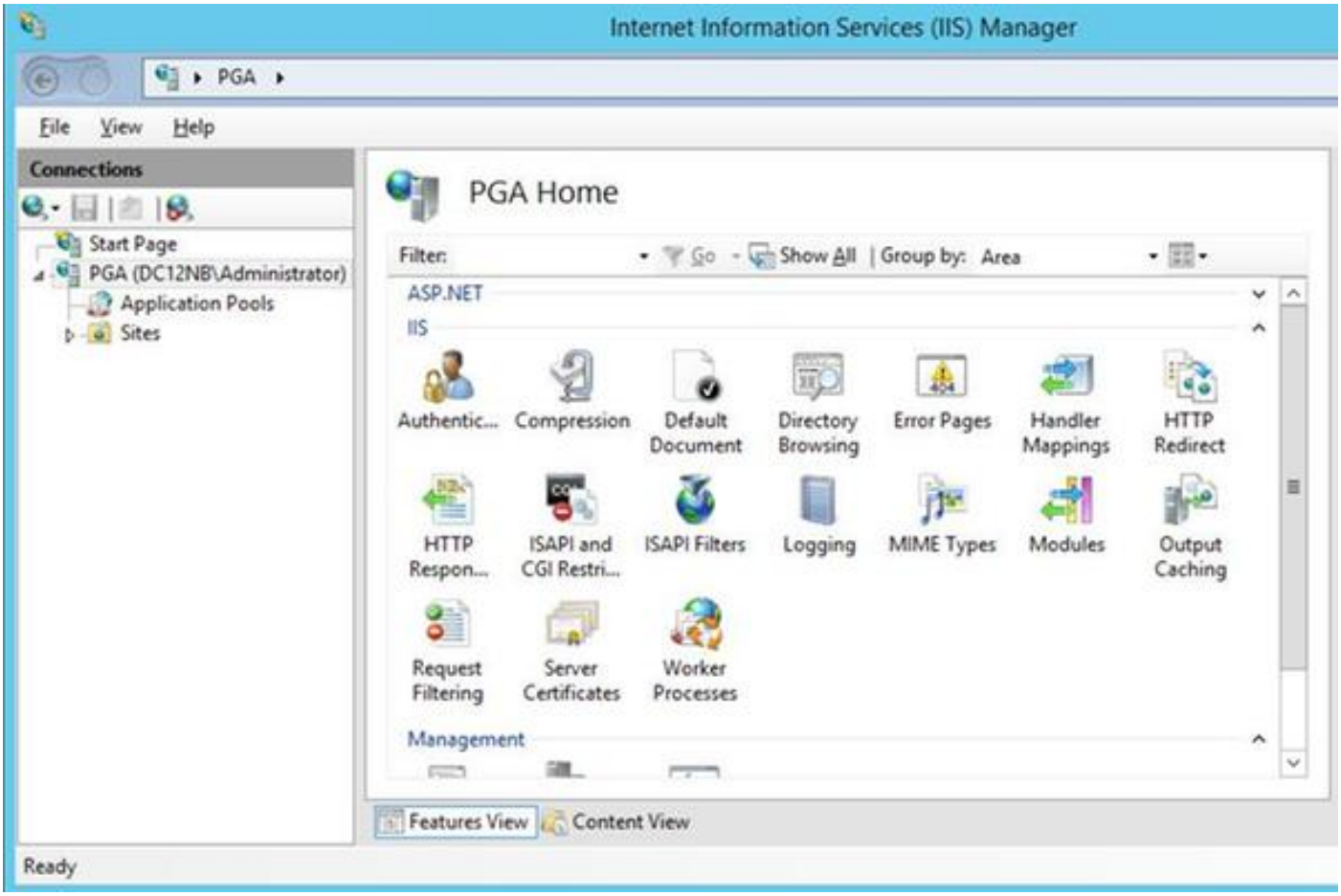
- Cisco UCCE 11.0.1
- R2 del Microsoft Windows server 2012
- Certificate Authority del r2 del Microsoft Windows server 2012
- Microsoft Windows 7 SP1 OS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

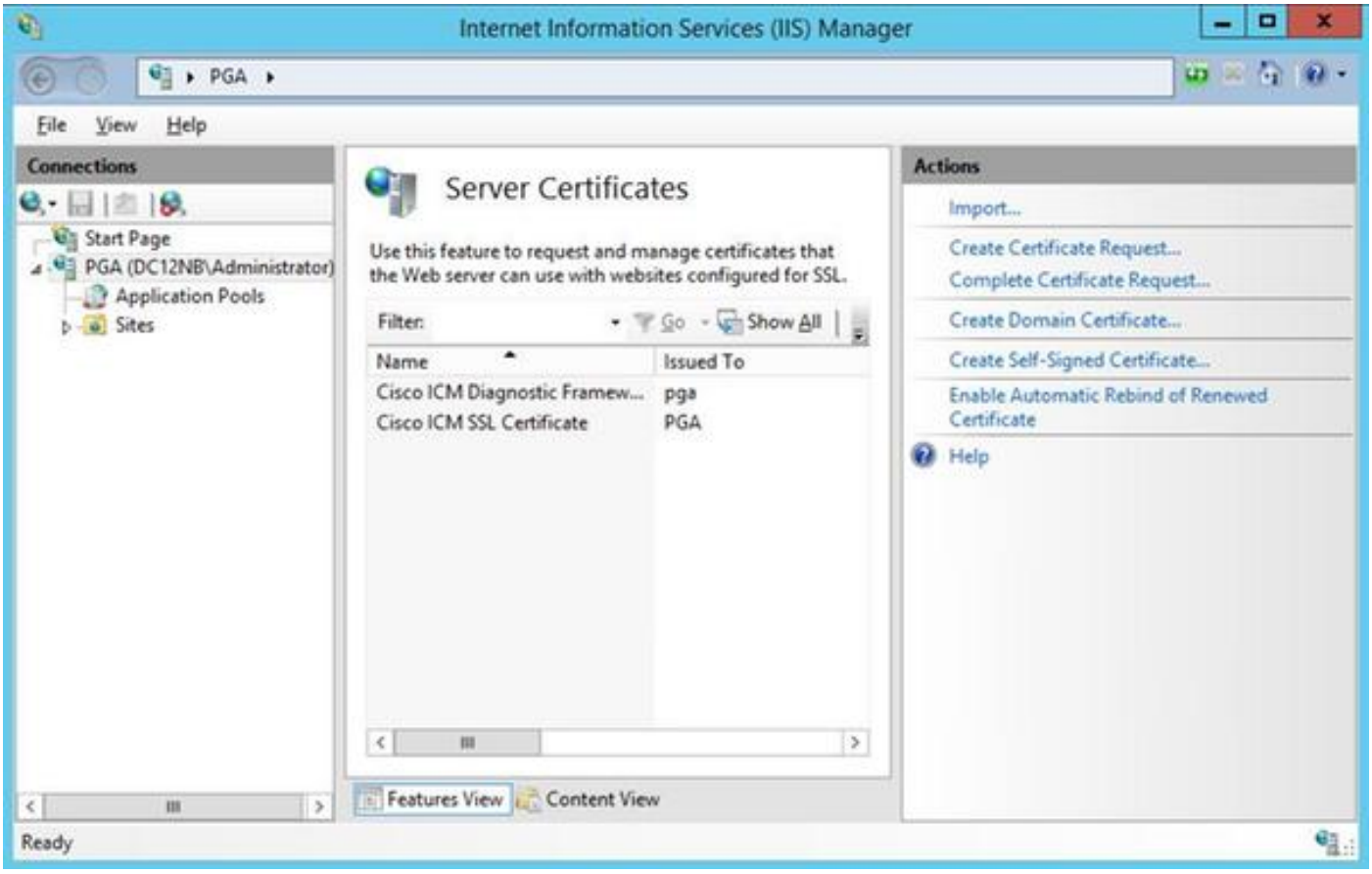
Configurar

Genere la petición firmada certificado

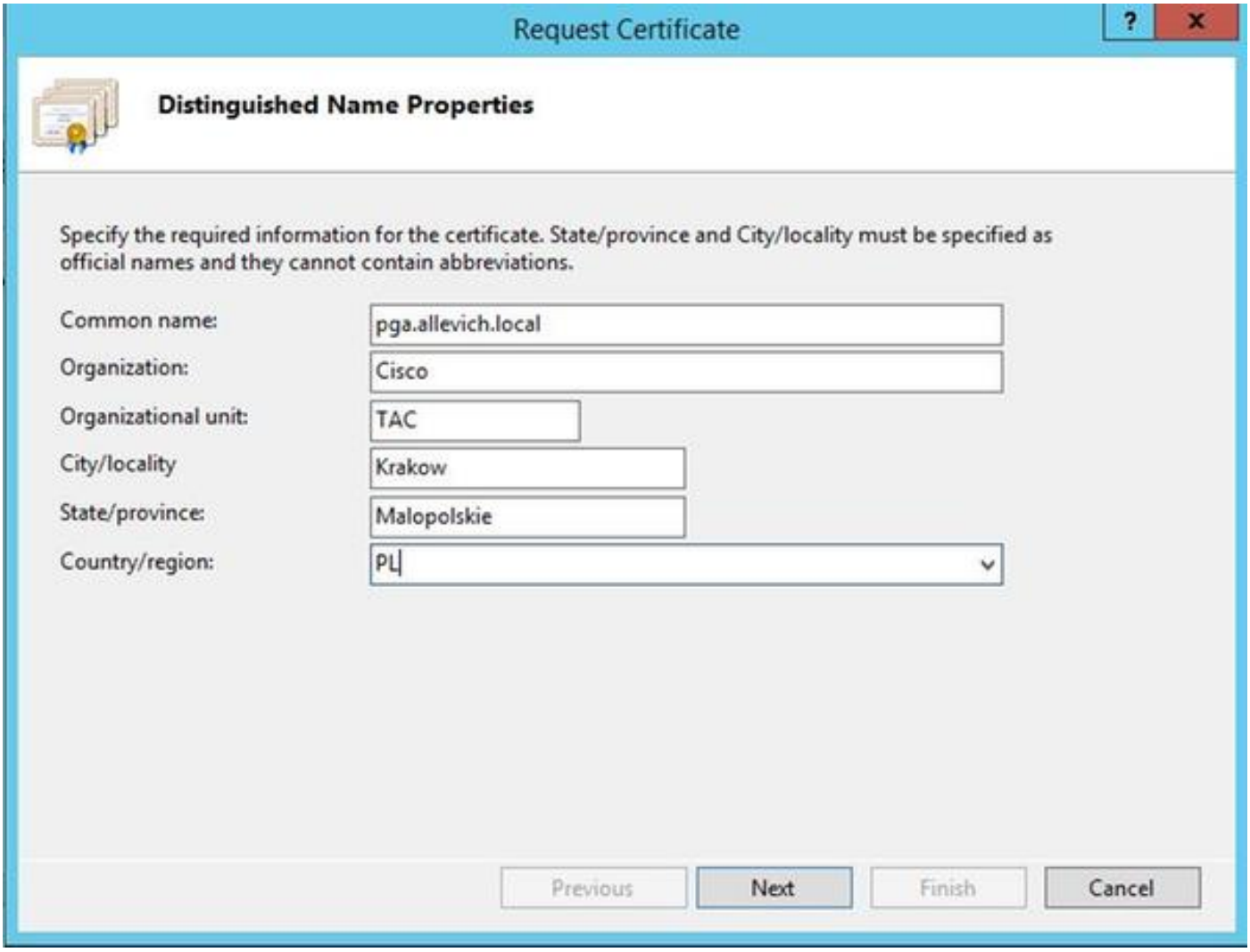
Abra al administrador de los Servicios de Internet Information Server (IIS), seleccione su sitio, Peripheral Gateway A (PGA) en el ejemplo, y los **certificados de servidor**.



Selecto **cree el pedido de certificado** en el panel de las acciones.



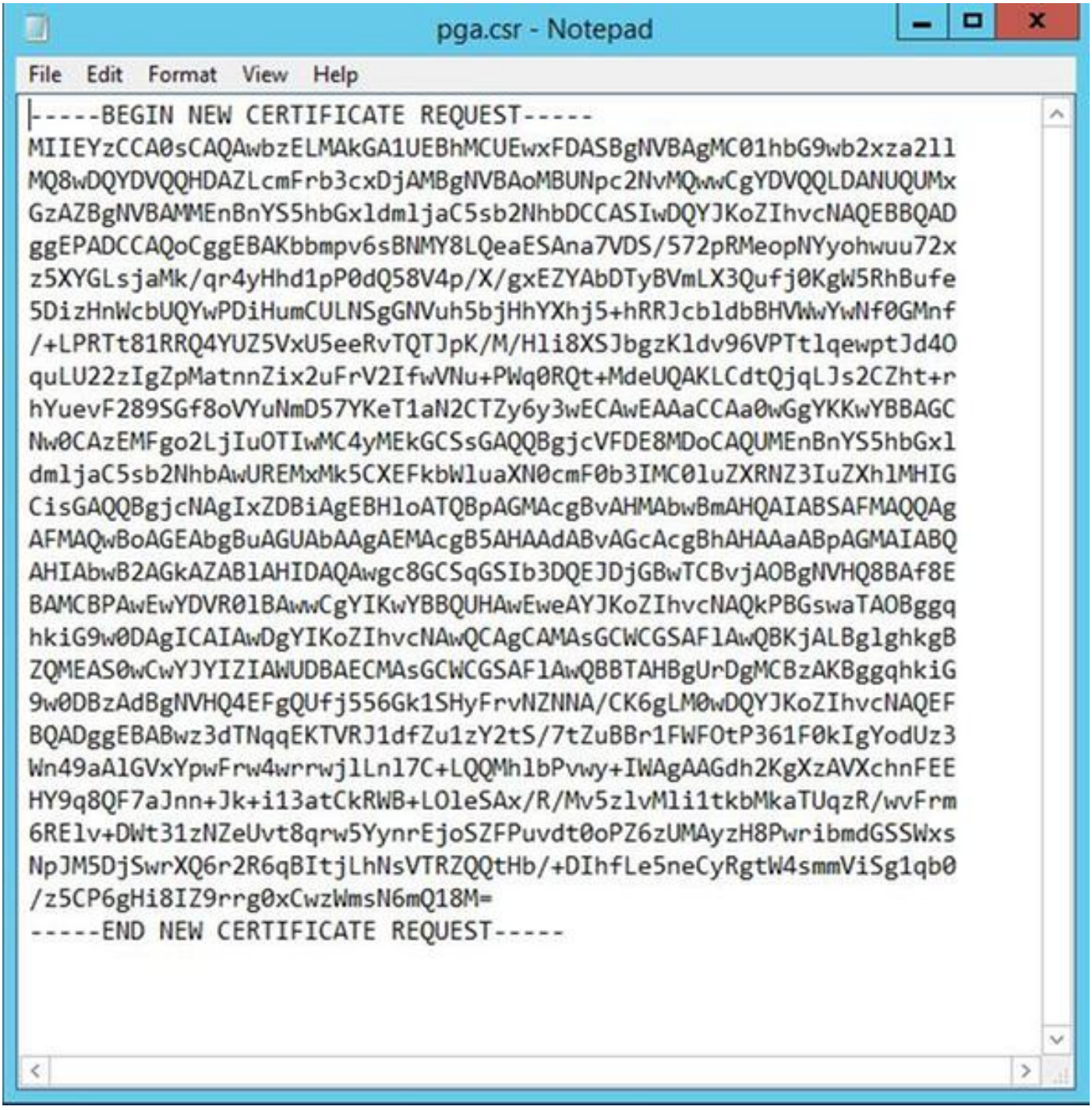
Ingrese el **Common Name (CN)**, la **organización** (o), **organization unit (OU)**, el **lugar** (l), el **estado** (ST), los campos del **país** (c). El Common Name debe ser lo mismo que su nombre de host + Domain Name del nombre de dominio completo (FQDN).



Deje las configuraciones predeterminadas para el proveedor de servicio criptográfico y especifique la longitud de bit: 2048.

Seleccione la trayectoria donde salvar. Por ejemplo en el escritorio con el nombre pga.csr.

Abra la petición creada recientemente en la libreta.



Copie el certificado en el buffer con el CTRL+C.

Firme el certificado en el Certificate Authority

> Nota: Si usted está utilizando el Certificate Authority externo (como GoDaddy) usted necesita entrarlos en contacto después que hacen el archivo CSR generar.

Ingrese a su CA el certificado de servidor alistan la página.
https:// <CA-server-address>/certsrv

Seleccione el **certificado de la petición**, **pedido de certificado avanzado** y pegue el contenido del pedido de firma de certificado (CSR) al buffer. Entonces seleccione el **Certificate Template plantilla de certificado como servidor Web**.

Descargue el certificado codificado base 64.

Abra el certificado y copie el contenido del campo del thumbprint para el uso posterior. Quite los espacios del thumbprint.

Instale el certificado

Copie el certificado

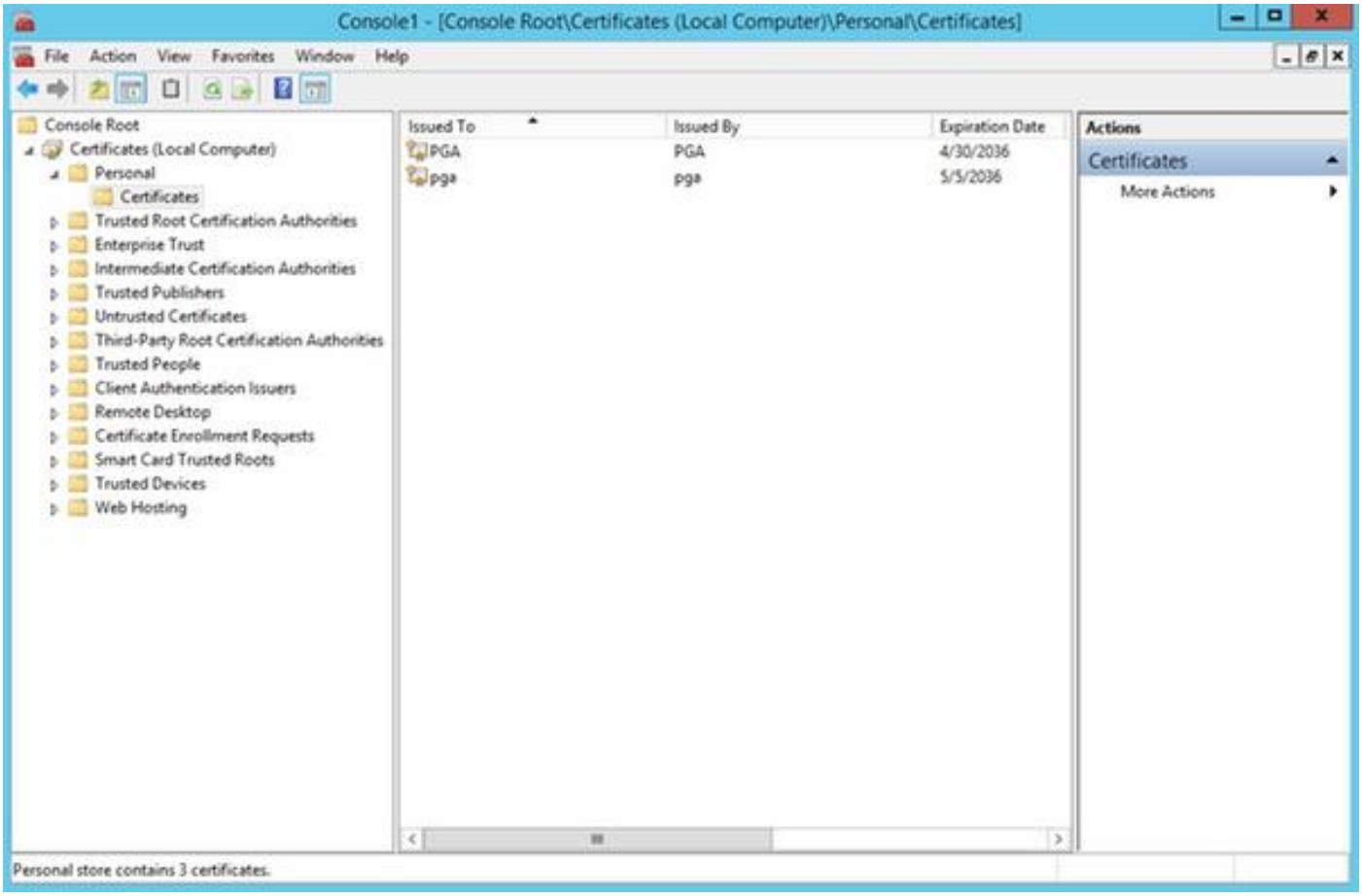
Copie el archivo de certificado nuevamente generado en UCCE VM donde se localiza la herramienta del pórtico.

Importe el certificado en el almacenaje informático de computadora local

En la misma consola del Microsoft Management Console del lanzamiento del servidor UCCE (MMC) seleccionando el menú Inicio, el **funcionamiento del** tipo y el **mmc**.

El tecleo **agrega/quita broche-en** y en el haga click en Add del cuadro de diálogo
Después seleccione el menú de los **Certificados** y agregue.
En los Certificados broche-en el cuadro de diálogo, haga clic la **cuenta > la computadora local > el final de la Computadora**.

Navegue a la carpeta de los certificados personales.



En el panel de acciones seleccione **más acciones > todas las tareas > importación**.

Haga clic **después**, **hojee** y seleccione el certificado que fue generado previamente y en el menú siguiente asegúrese de que el almacén de certificados fuera fijado a personal. En la pantalla más reciente verifique el **almacén de certificados** y **archivo de certificado** seleccionados y clic en Finalizar.

Ate el certificado IIS

Abra la aplicación del CMD.

Navegue a la carpeta de diagnóstico del hogar del pórtico.

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

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

```
DiagFwCertMgr /task:UnbindCert
```

Ate el certificado firmado de CA.

> Consejo: Utilice algún editor de textos (notepad++) para quitar los espacios en el hash.

Utilice el hash guardado antes con los espacios quitados.

```
DiagFwCertMgr /task:BindCertFromStore /certhash:bc6bbe23b8b3a26d8446c252400f9264c5c30a29
```

En caso de que el certificado esté limitado con éxito usted debe ver que el similares alinean en la

salida.
“El atascamiento del certificado es VÁLIDO”
Asegúrese de que el atascamiento del certificado fuera acertado usando este comando.

```
DiagFwCertMgr /task:ValidateCertBinding
```

El mensaje similar se debe visualizar otra vez en la salida.
“El atascamiento del certificado es VÁLIDO”

> Nota: DiagFwCertMgr por abandono utilizará el puerto 7890.

Recomience el servicio de diagnóstico del marco.

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

> Consejo: Mantenga la lista y especialmente el nombre del servicio del pórtico se puede marcar vía el comando del tasklist en la herramienta del CMD.

```
tasklist /v
```

Verificación

Abra la página de diagnóstico del marco usando el FQDN y no debe indicar un mensaje de advertencia del certificado.

Se retira el plan

En caso de que usted perdiera el acceso a la herramienta del pórtico usted puede regenerar el certificado autofirmado y agregar una excepción.
Puede ser hecha usando este comando.

```
DiagFwCertMgr /task:CreateAndBindCert
```

Troubleshooting

No utilice la dirección IP cuando login a la herramienta de diagnóstico del pórtico del marco. Usted todavía recibe una advertencia del certificado, porque el FQDN tiene que hacer juego con el valor especificado en el campo del certificado CN.

Verifique que todos los servidores estén sincronizados con la fuente NTP.

```
w32tm /monitor
```

Si usted intenta utilizar el nombre alternativo sujeto (SAN) o el Digital Signature Algorithm elíptico de la curva (EC DSA) o certificado de 4096 longitudes de clave - primer aislante que no es específico a una de estas características.

Artículos relacionados

UCCE \ PCCE - Procedimiento para obtener y para cargar el - del uno mismo del Servidor Windows firmado o los servidores del certificado del Certificate Authority (CA) 2008

Certificado firmado de CA de la configuración vía el CLI en el sistema operativo de la Voz de Cisco (VOS)