Configurar o acesso HTTPS para a ferramenta diagnóstica do pórtico da estrutura UCCE com certificado assinado do Certificate Authority (CA)

Índice

Introdução

Este original descreve o processo de configuração em como instalar o certificado assinado de CA para a ferramenta diagnóstica unificada do pórtico da estrutura da empresa do centro de contato (UCCE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Diretório ativo
- Server do Domain Name System (DNS)
- Infraestrutura de CA distribuída e que trabalha para todos os server e cliente
- Pórtico diagnóstico da estrutura

A ferramenta diagnóstica de acesso do pórtico da estrutura datilografando o endereço IP de Um ou Mais Servidores Cisco ICM NT no navegador sem receber o aviso do certificado é fora do espaço deste artigo.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

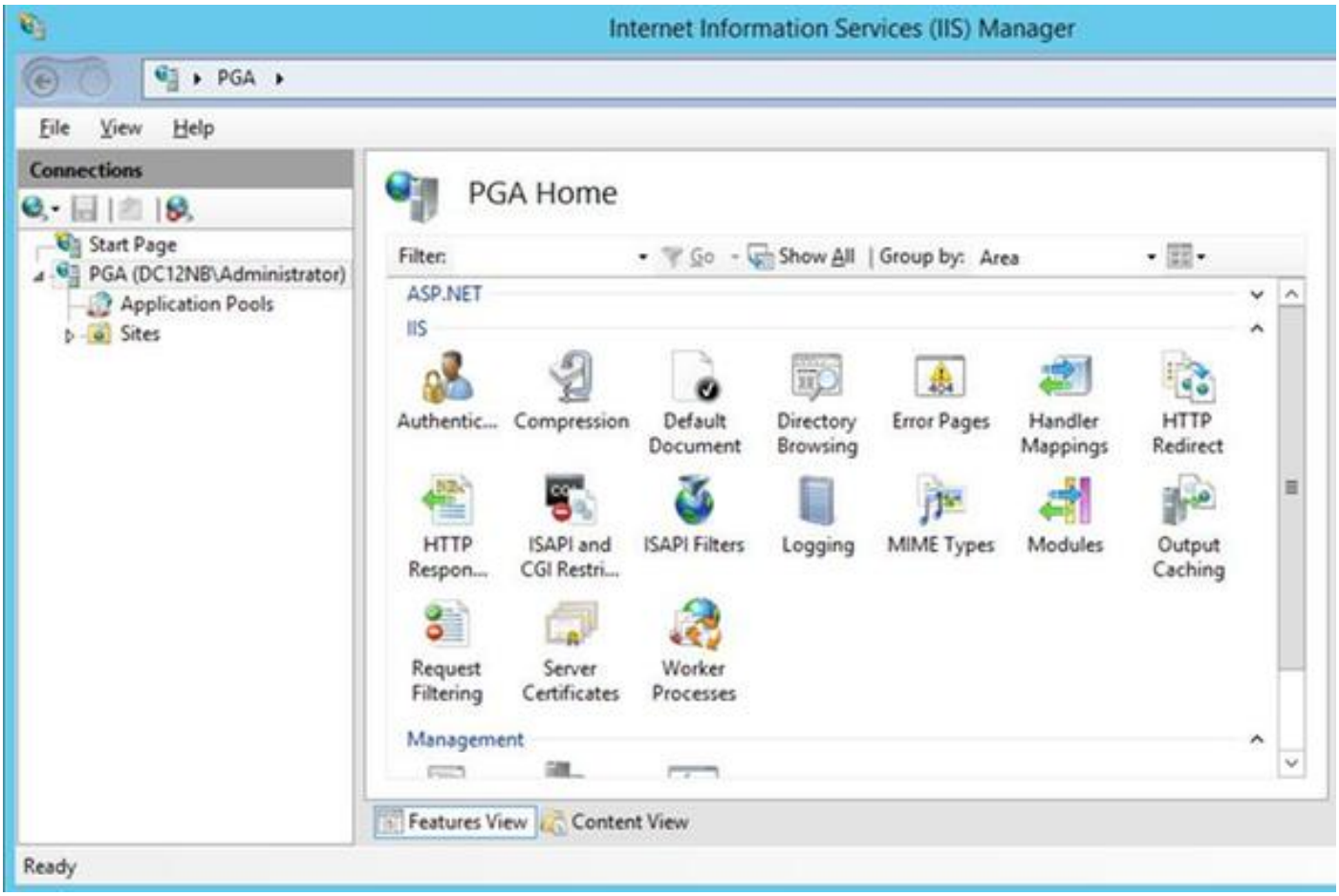
- Cisco UCCE 11.0.1
- Microsoft Windows server 2012 R2
- Certificate Authority R2 do Microsoft Windows server 2012
- OS de Microsoft Windows 7 SP1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

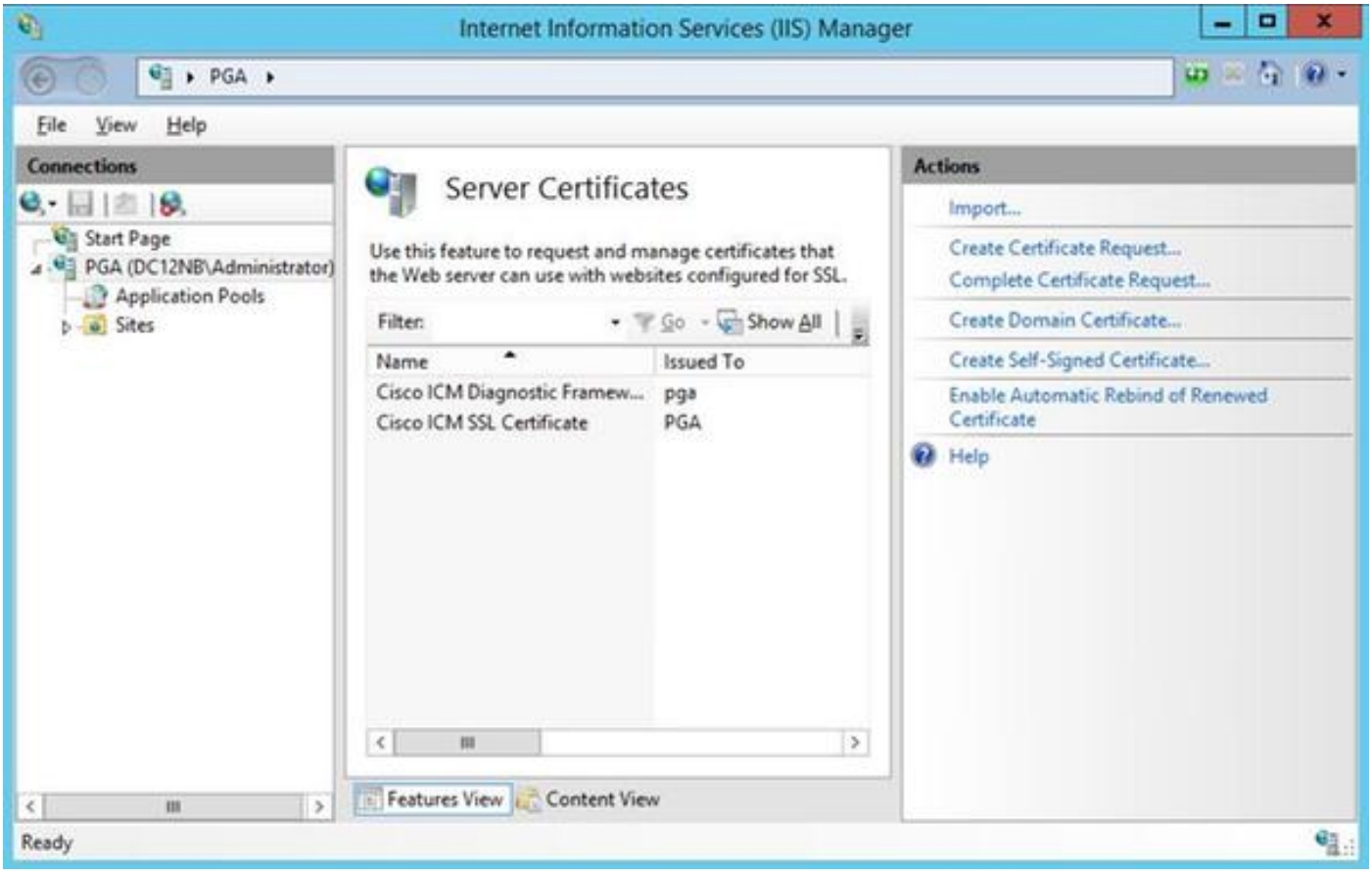
Configurar

Gerencia o pedido assinado certificado

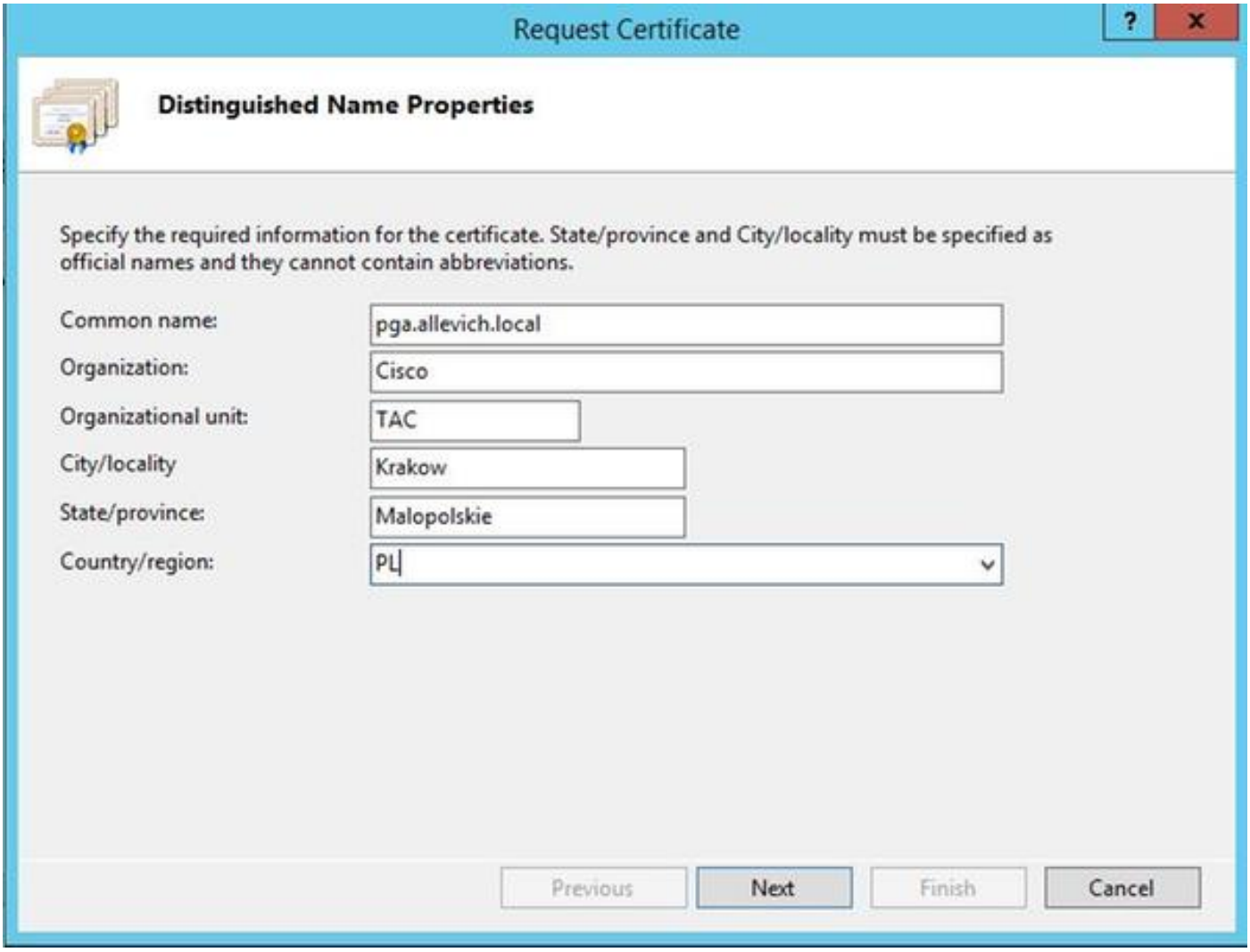
Abra o gerente do Internet Information Services (IIS), selecione seu local, Peripheral Gateway A (PGA) no exemplo, e em **certificados de servidor**.



Seleto **crie o pedido do certificado no** painel das ações.



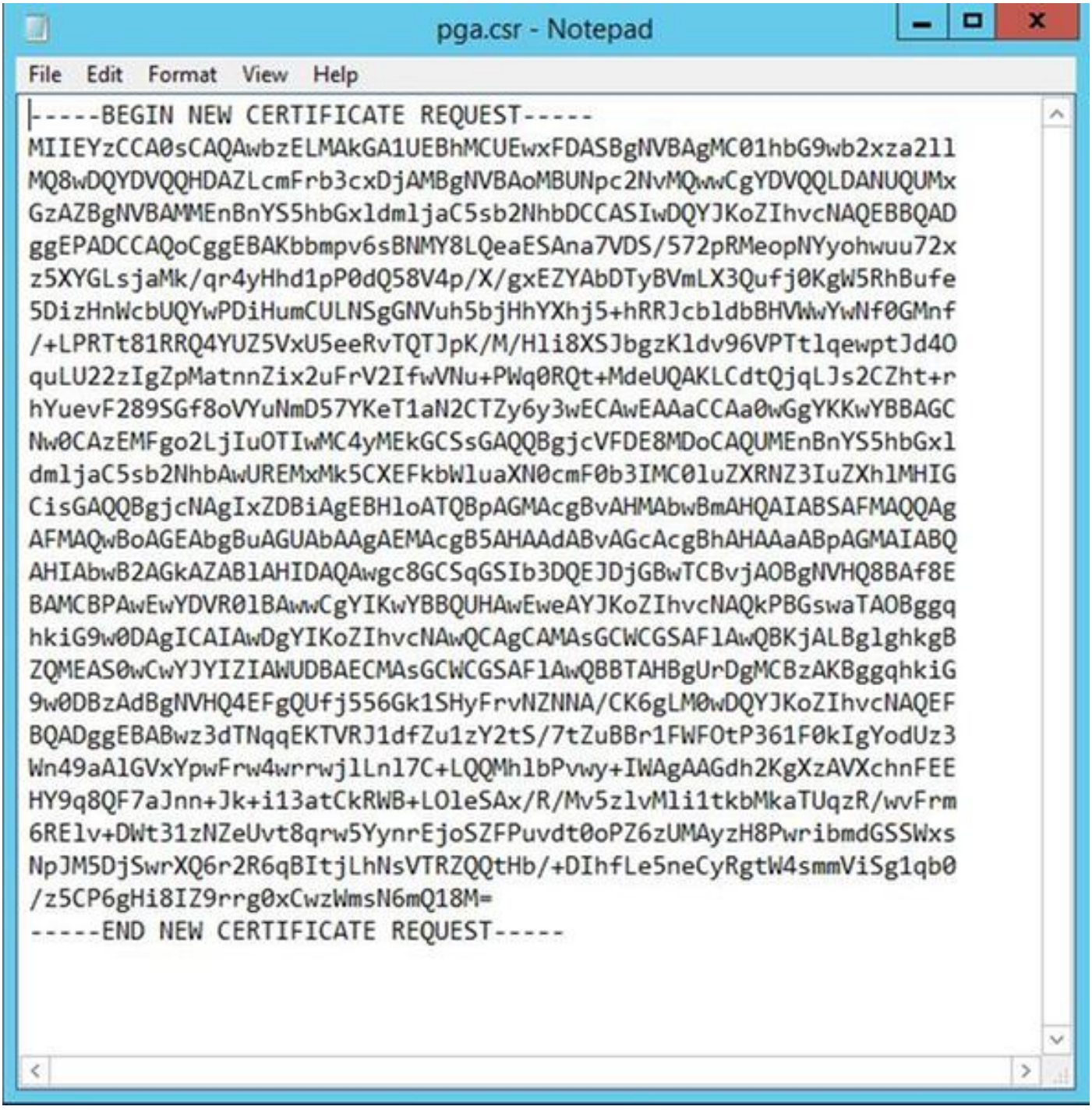
Incorpore o **Common Name (CN)**, a **organização** (O), **organization unit (OU)**, **localidade** (L), o **estado** (ST), o **país** (c) coloca. O Common Name deve ser o mesmo que seus hostname + Domain Name do nome de domínio totalmente qualificado (FQDN).



Deixe configurações padrão para o provedor de serviços criptograficamente e especifique o comprimento de bit: 2048.

Selecione o trajeto onde armazenar. Por exemplo no desktop com nome pga.csr.

Abra o pedido recém-criado no bloco de notas.



Copie o certificado no buffer com CTRL+C.

Assine o certificado no Certificate Authority

> **Note**: Se você está usando o Certificate Authority externo (como GoDaddy) você precisa de contactá-los em seguida que têm o arquivo CSR gerado.

Assine dentro a seu certificado de servidor de CA registram a página.
https:// <CA-server-address>/certsrv

Selecione o **certificado do pedido**, **pedido do certificado avançado** e cole o índice da solicitação de assinatura de certificado (CSR) ao buffer. Selecione então o **molde de certificado como o servidor de Web**.

Transfira o certificado codificado Base64.

Abra o certificado e copie o índice do campo do thumbprint para um uso mais atrasado. Remova os espaços do thumbprint.

Instale o certificado

Copie o certificado

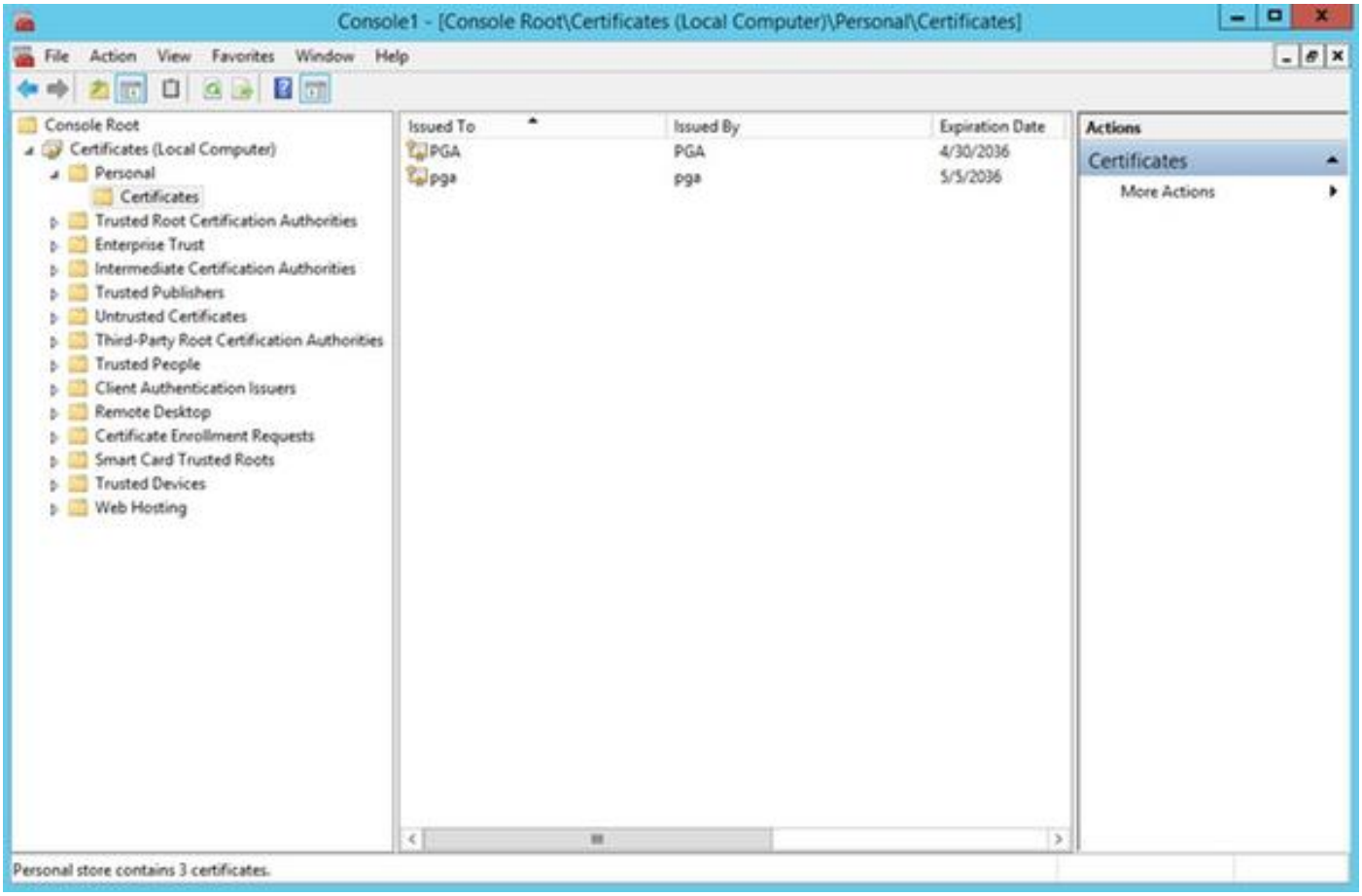
Copie o arquivo certificado recentemente gerado em UCCE VM onde a ferramenta do pórtico é encontrada.

Importe o certificado na loja de computador local

No mesmo console do Microsoft Management Console do lançamento do server UCCE (MMC) selecionando o menu de início, o tipo **corrida** e o **mmc**.

O clique **adiciona/remove pressão-em** e no clique da caixa de diálogo **adicionar**.
Então selecione o menu dos **Certificados** e adicionar-lo.
Nos Certificados pressão-na caixa de diálogo, clique a **conta > o computador local > o revestimento do computador**.

Navegue ao dobrador dos certificados pessoais.



Na placa das ações selecione **mais ações > todas as tarefas > importação**.

Clique **em seguida**, **consulte** e selecione o certificado que foi gerado previamente e no menu seguinte se assegure de que a loja do certificado esteja ajustada a pessoal. Na última tela verifique a **loja** e o **arquivo certificado do certificado** selecionados e clique o **revestimento**.

Ligue o certificado IIS

Abra o aplicativo do CMD.

Navegue ao dobrador diagnóstico da HOME do pórtico.

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

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

```
DiagFwCertMgr /task:UnbindCert
```

Ligue o certificado assinado de CA.

> Dica: Use algum editor de texto (notepad++) para remover os espaços na mistura.

Use a mistura salvar antes com os espaços removidos.

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

Caso que o certificado é limitado com sucesso você deve ver que o similares alinham na saída.
“O emperramento do certificado é VÁLIDO”
Assegure-se de que o emperramento do certificado esteja bem sucedido usando este comando.

```
DiagFwCertMgr /task:ValidateCertBinding
```

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

> **Note**: DiagFwCertMgr à revelia usará a porta 7890.

Reinicie o serviço diagnóstico da estrutura.

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

> Dica: Preste serviços de manutenção à lista e especialmente o nome do serviço do pórtico pode ser verificado através do comando do tasklist na ferramenta do CMD.

```
tasklist /v
```

Verificar

Abra a página diagnóstica da estrutura usando o FQDN e não deve alertar um mensagem de advertência do certificado.

A parte traseira para fora planeia

Caso que você perdeu o acesso à ferramenta do pórtico você pode regenerar o certificado auto-assinado e adicionar uma exceção.
Pode ser feita usando este comando.

```
DiagFwCertMgr /task:CreateAndBindCert
```

Troubleshooting

Não use o endereço IP de Um ou Mais Servidores Cisco ICM NT quando início de uma sessão à ferramenta diagnóstica do pórtico da estrutura. Você ainda recebe um aviso do certificado, porque o FQDN tem que combinar com o valor especificado no campo do CN do certificado.

Verifique que todos os server estão sincronizados com a fonte NTP.

```
w32tm /monitor
```

Se você tenta usar o nome alternativo sujeito (SAN) ou o Digital Signature Algorithm elíptico da curva (EC DSA) ou certificado de 4096 comprimentos chaves - primeiro isolado que não é específico a uma destas características.

Artigos relacionados

UCCE \ PCCE - Procedimento para obter e transferir arquivos pela rede o - do auto de Windows Server assinado ou os server do certificado do Certificate Authority (CA) 2008

Configurar o certificado assinado de CA através do CLI no sistema operacional da Voz de Cisco (VOS)