配置UCCE诊断框架门廊工具的HTTPS访问有Certificate Authority (CA)签名证书的

目录

简介

本文描述关于怎样的配置过程安装Unified Contact Center企业(UCCE)诊断框架门廊工具的CA签名证书。

先决条件

要求

Cisco 建议您了解以下主题：

- Active Directory
- 域名系统 (DNS) 服务器
- 部署和工作为所有服务器和客户端的CA基础设施
- 诊断框架门廊

访问诊断框架门廊工具通过键入在浏览器的IP地址没有接收证书警告是出于范围此条款。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科UCCE 11.0.1
- MS Windows服务器2012个R2

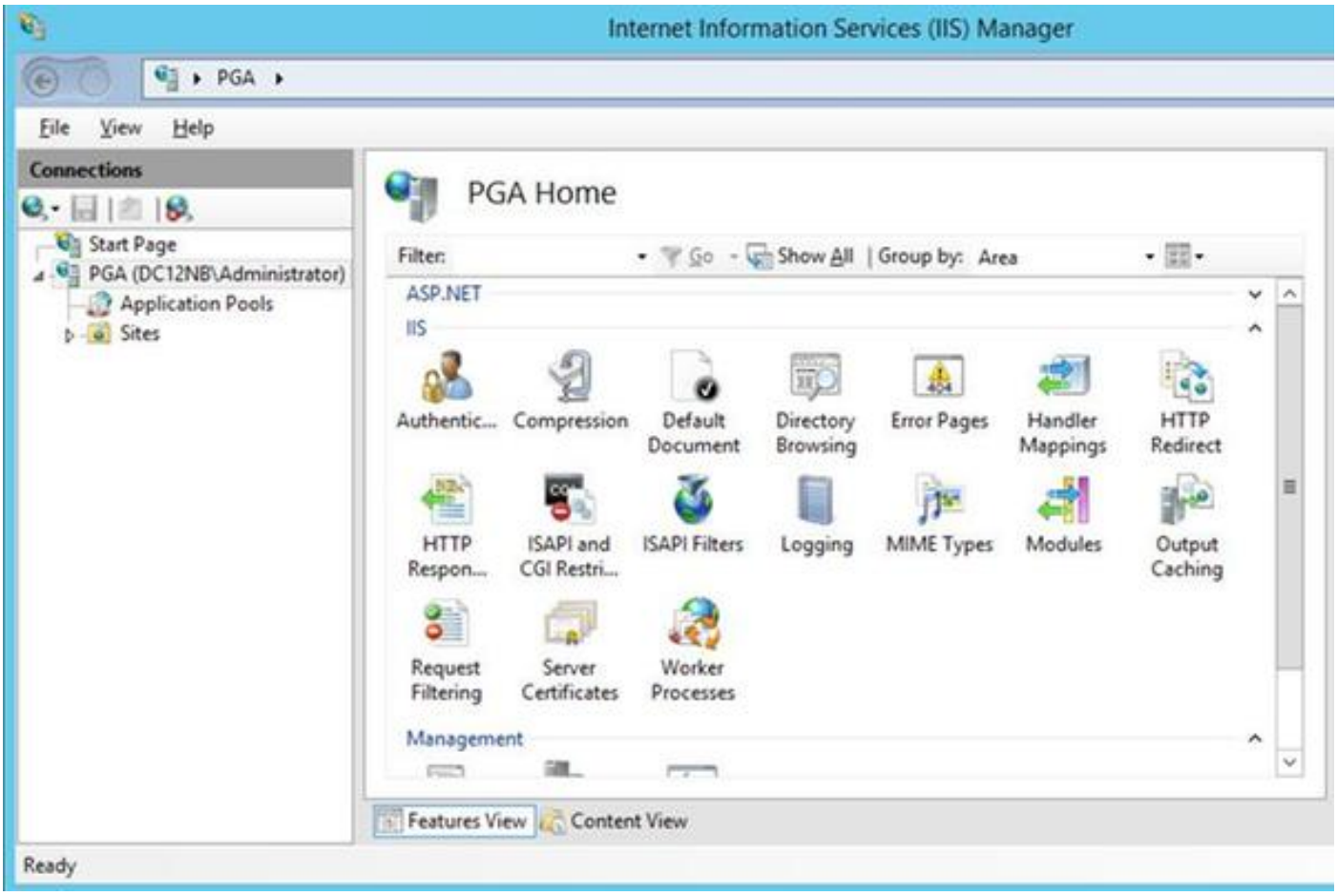
- MS Windows服务器2012个R2认证机关
- Microsoft Windows 7 SP1 OS

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

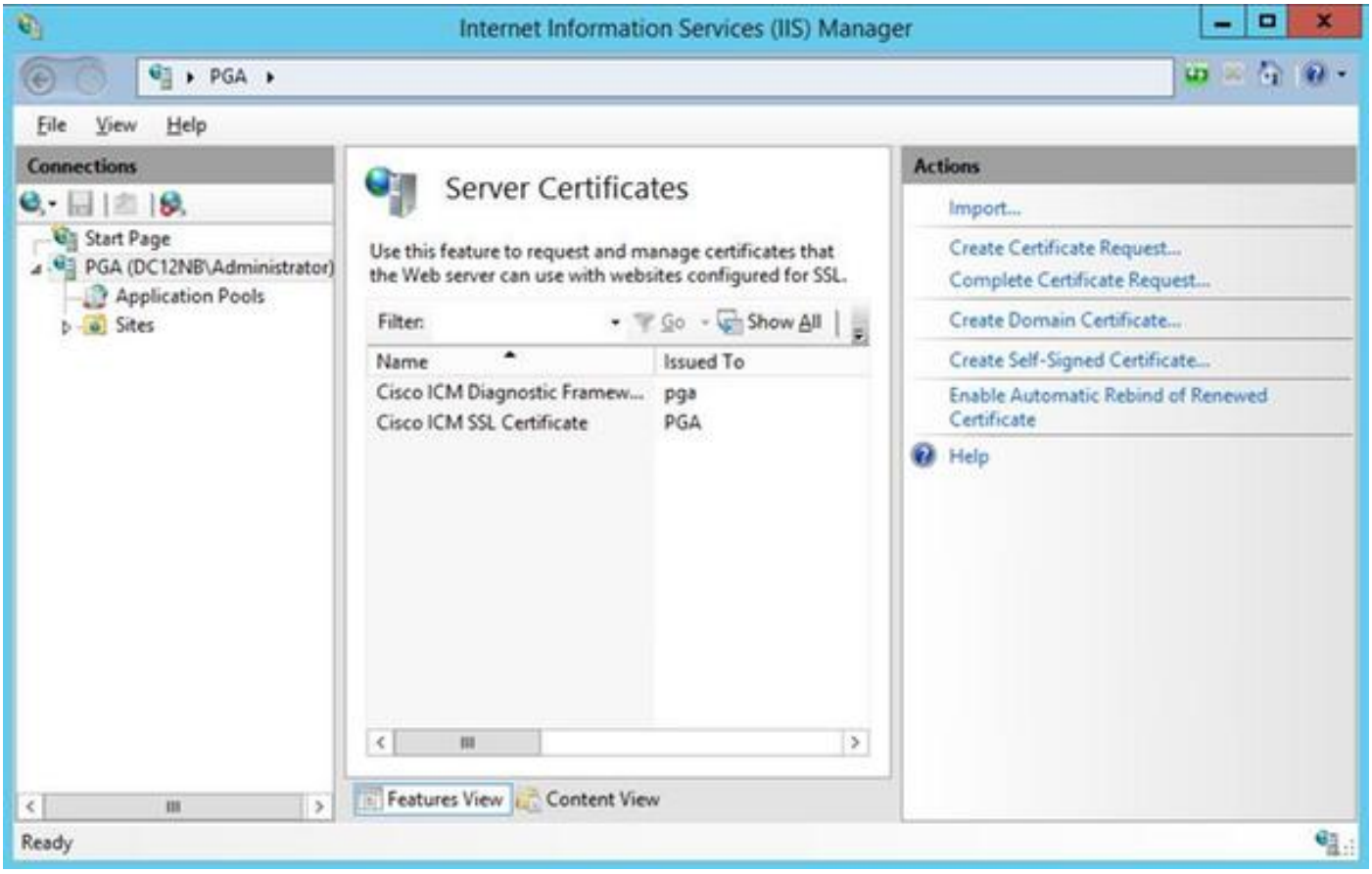
配置

生成证书签字的请求

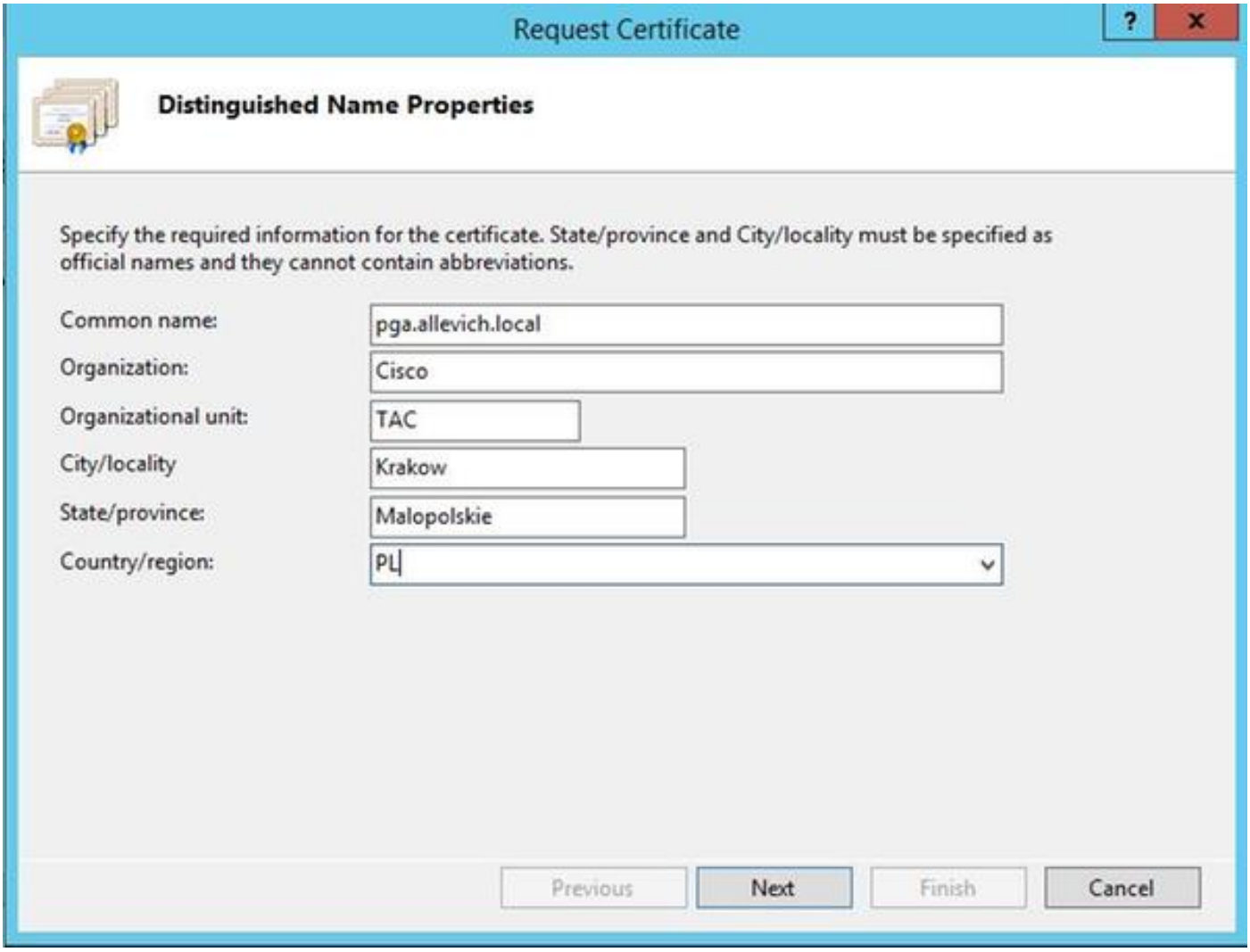
打开互联网信息服务(IIS)管理器，选择您的站点、外围网关A (PGA)在示例和**服务器证书**。



选择**创建证书请求**在操作面板中。



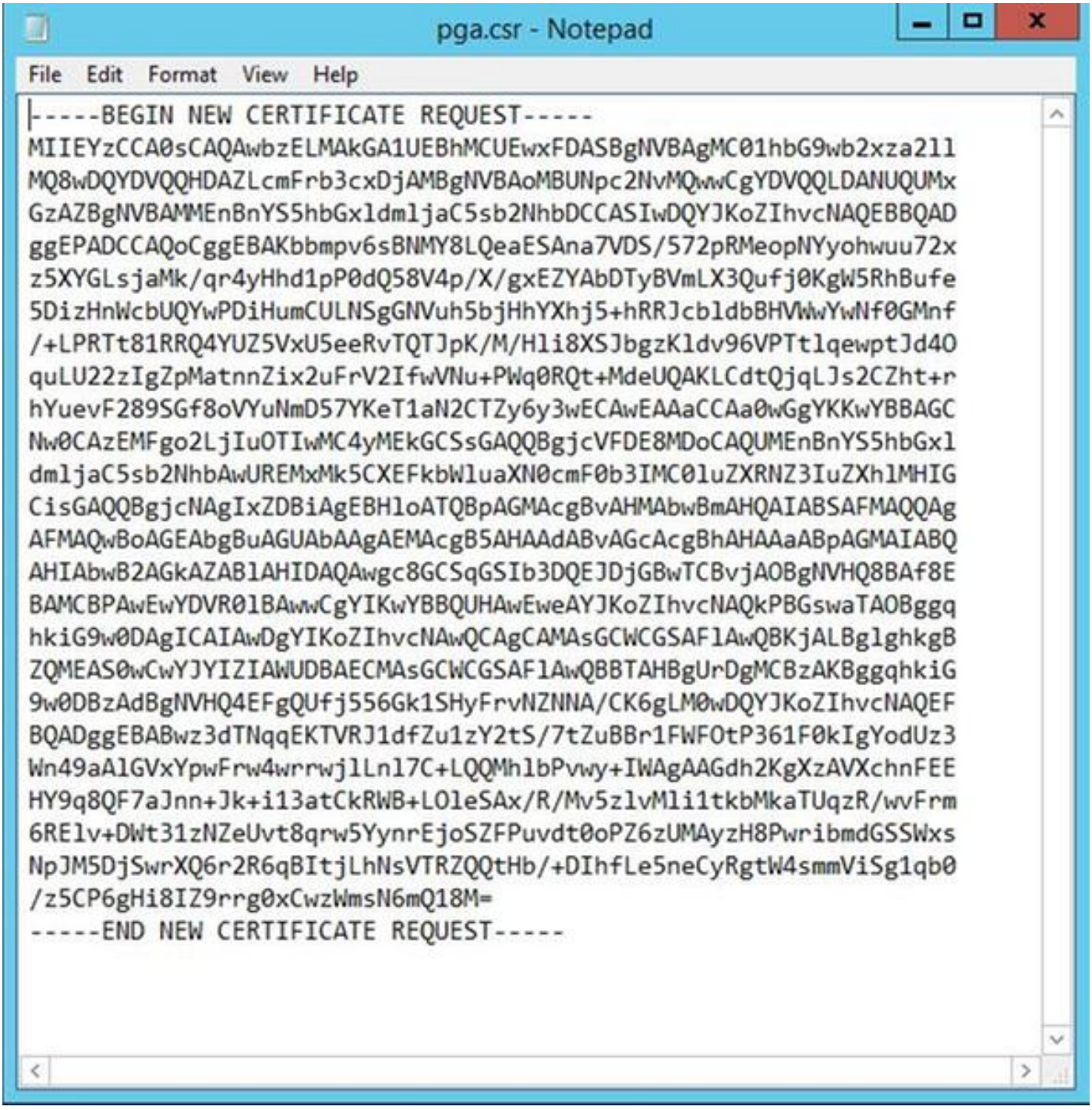
输入**共同名称(CN)**，**组织**(o)，**组织单位(OU)**，**现场**(l)，**状态**(ST)，**国家**(c)字段。公用名称必须是相同的象您的完全合格的域名(FQDN)主机名+域名。



留下密码服务提供商的默认设置并且指定比特长度：2048.

在哪里选择路径存储。例如在有pga.csr名称的桌面。

打开在记事本的新建立的请求。



复制证书到有CTRL+C的缓冲区。

签署在的证书认证机关

> **注意**：如果使用外部认证机关(类似GoDaddy)您需要与他们联系以后安排CSR文件生成。

签字对您的CA服务器证书登记页。
https:// <CA-server-address>/certsrv

Select请求**证书**，**先进的证书请求**和粘贴证书签名请求(CSR)内容到缓冲区。然后请选择**认证模板作为Web服务器**。

下载Base64编码的证书。

打开证书并且复制容量对最新使用情况的thumbprint字段。取消从thumbprint的空间。

安装证书

复制证书

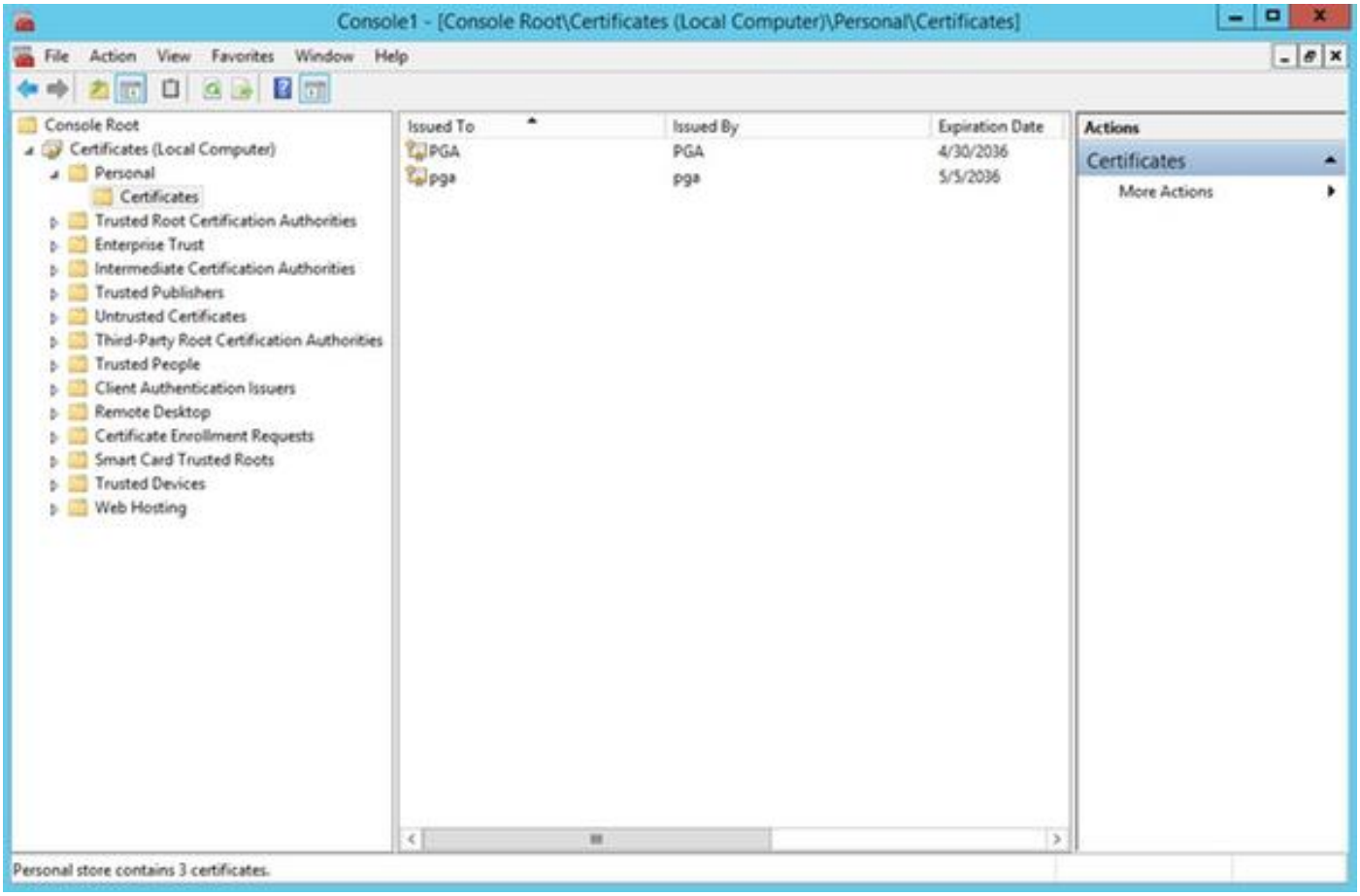
最近复制生成的证书文件到门廊工具查找的UCCE VM。

导入证书到本地计算机计算机专卖店

在同一个UCCE服务器启动微软管理控制台(MMC)控制台上通过选择开始菜单、类型**运行**和**mmc**。

单击 **添加/删除管理单元**，并且在对话框单击请 **添加**。
然后请选择**证书**菜单并且添加。
在证书卡扣式对话框中，请点击**计算机帐户>本地计算机>芬通社**。

导航到个人证书文件夹。



在操作窗格中请选择**更多操作>所有任务>导入**。

单击**其次**，**浏览**并且选择以前生成，并且在Next菜单请保证的证书证书存储设置对个人。在最后屏幕请验证选择的**证书存储**和**证书文件**并且点击**芬通社**。

绑定IIS证书

打开CMD应用程序。

导航到诊断门廊主页文件夹。

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

删除为门廊工具绑定的当前证书。

```
DiagFwCertMgr /task:UnbindCert
```

绑定CA签名证书。

提示：请使用某文本编辑(notepad++)取消在哈希的空间。

以删除的空间使用以前保存的哈希。

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

万一证书顺利地一定您在输出中应该看到相似的线路。
“证书捆绑有效”
保证证书捆绑使用此命令是成功的。

```
DiagFwCertMgr /task:ValidateCertBinding
```

再次在输出中应该显示相似的消息。
“证书捆绑有效”

注意：默认情况下DiagFwCertMgr将使用端口7890。

重新启动诊断框架服务。

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

提示：服务列表和特别是门廊服务名称可以通过tasklist in命令CMD工具被检查。

```
tasklist /v
```

验证

开放诊断框架页使用FQDN和它不应该提示证书警告消息。

取消规划

万一丢失对门廊工具的访问您能重新生成自签名证书和添加例外。
使用此命令，它可以执行。

DiagFwCertMgr /task:CreateAndBindCert

故障排除

请勿使用IP地址，当登录到诊断框架门廓工具。因为FQDN必须配比与在Certificate CN字段，指定的值您仍然收到证书警告。

验证所有服务器与Ntp source同步。

w32tm /monitor

如果设法使用附属的替代方案名称(SAN)或椭圆曲线数字签名算法(EC DSA)或4096个密钥长度证书-首先隔离不是特定到这些功能之一。

相关条款

UCCE \ PCCE -步骤获得并上载Windows服务器赛弗-签字的或在2008个服务器的Certificate Authority (CA)证书
通过在思科语音操作系统(VOS)的CLI配置CA签名证书