Configurez HTTPS Access pour l'outil diagnostique de portique de cadre UCCE avec le certificat signé d'Autorité de certification (CA)

Contenu

Introduction

Ce document décrit le processus de configuration sur la façon dont installer le certificat signé CA pour l'outil diagnostique de portique de cadre d'Unified Contact Center Enterprise (UCCE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Active Directory
- Serveur de Système de noms de domaine (DNS)
- Infrastructure CA déployée et fonctionnante pour tous les serveurs et client
- Portique diagnostique de cadre

Accéder à l'outil diagnostique de portique de cadre en tapant l'adresse IP dans le navigateur sans recevoir l'avertissement de certificat est hors de portée de cet article.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

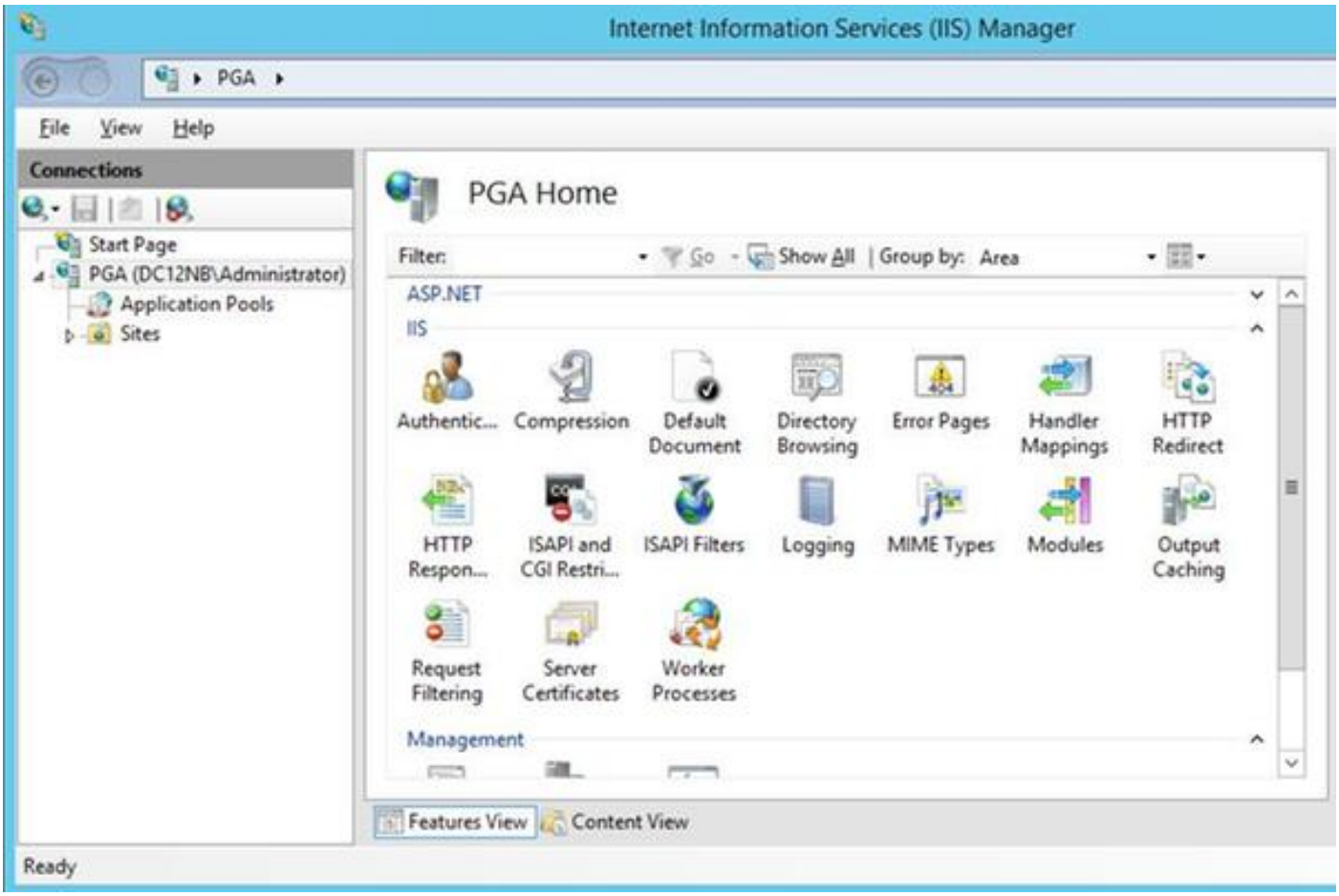
- Cisco UCCE 11.0.1
- Microsoft Windows Server 2012 R2
- Autorité de certification R2 de la Microsoft Windows Server 2012
- SYSTÈME D'EXPLOITATION SP1 de Microsoft Windows 7

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

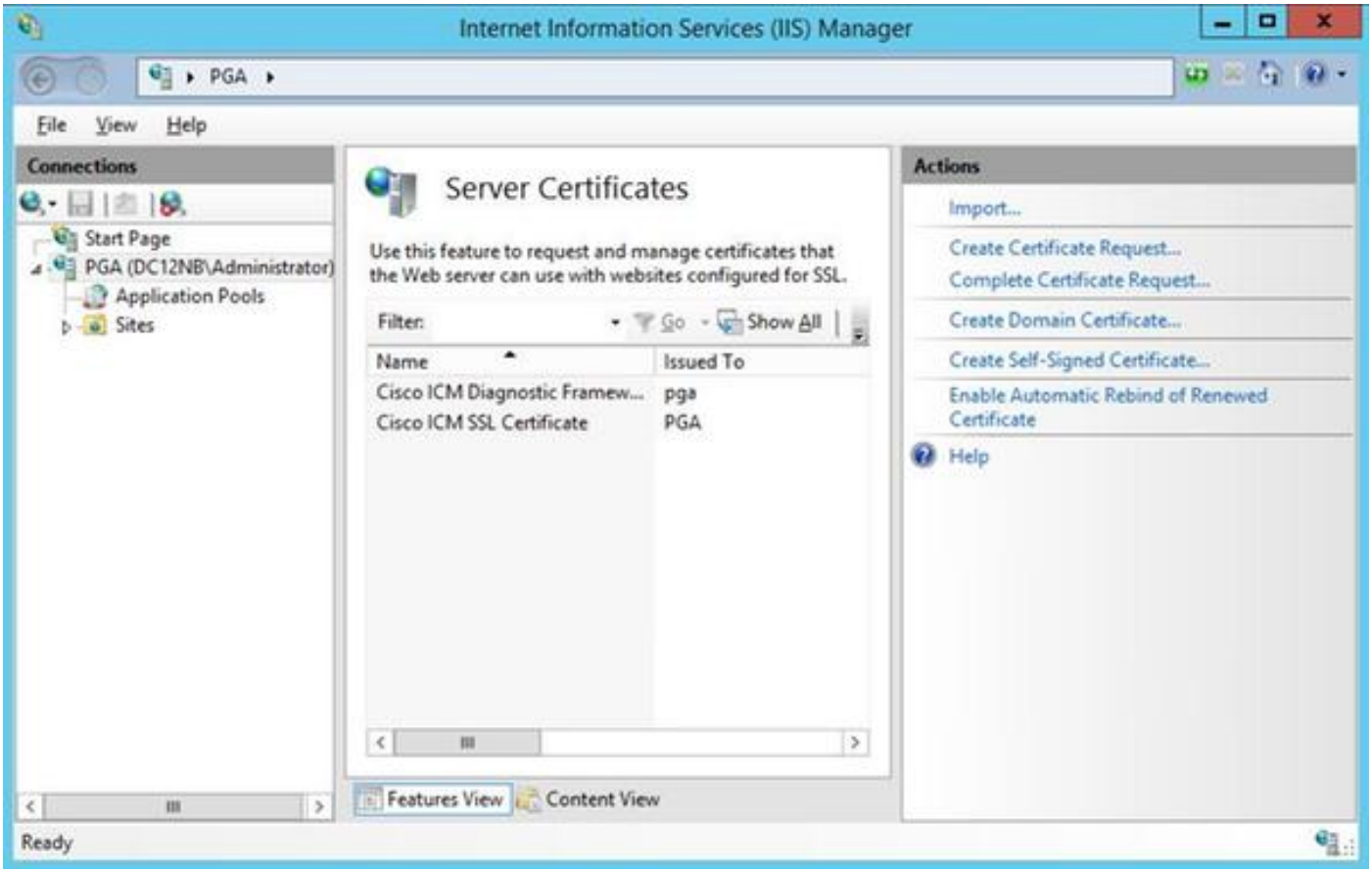
Configurez

Générez la demande signée par certificat

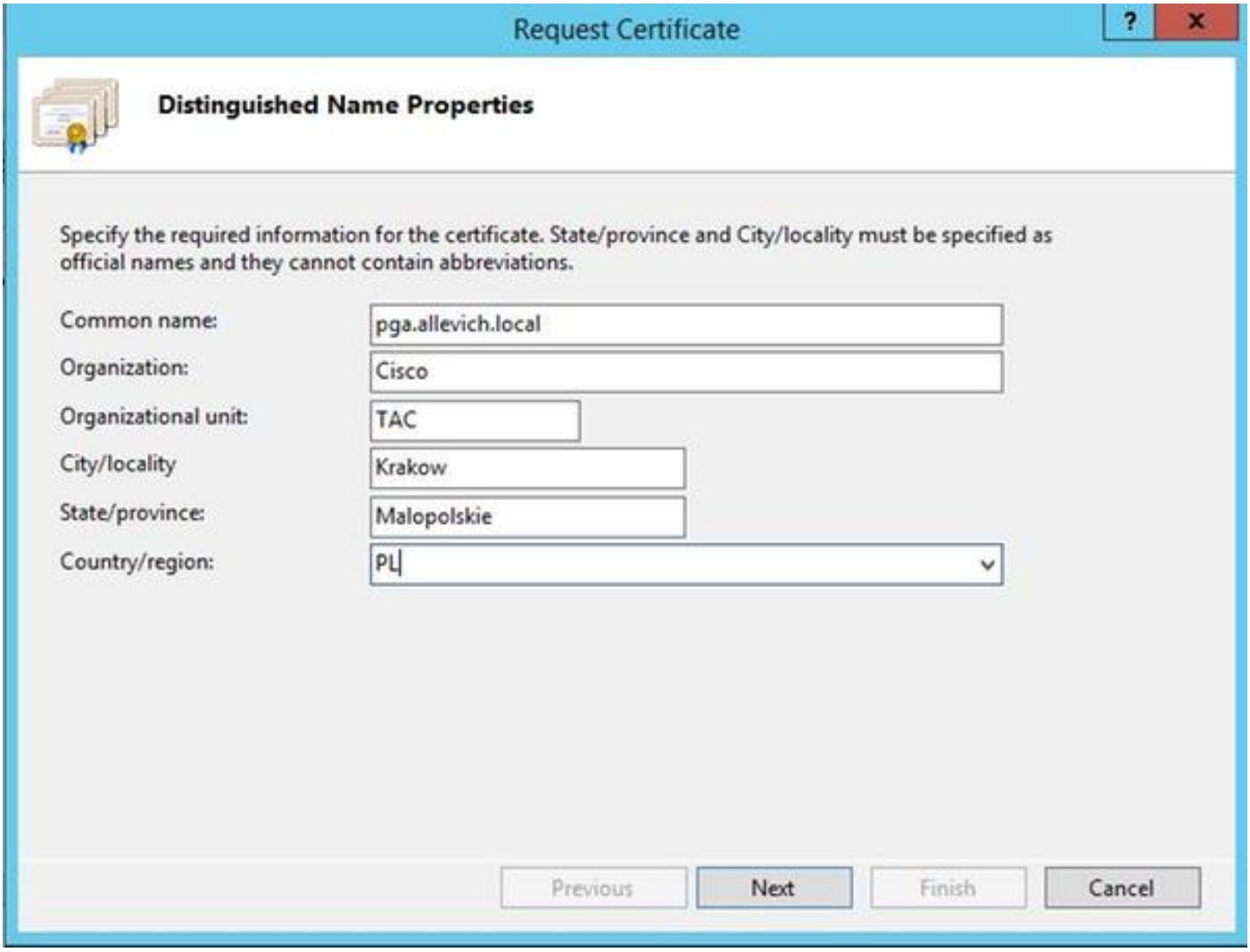
Le gestionnaire ouvert de l'Internet Information Services (IIS), sélectionnent votre site, passerelle d'accès aux périphériques A (PGA) dans l'exemple, et **Certificats de serveur**.



Choisi **créez la demande de certificat** dans le panneau d'actions.



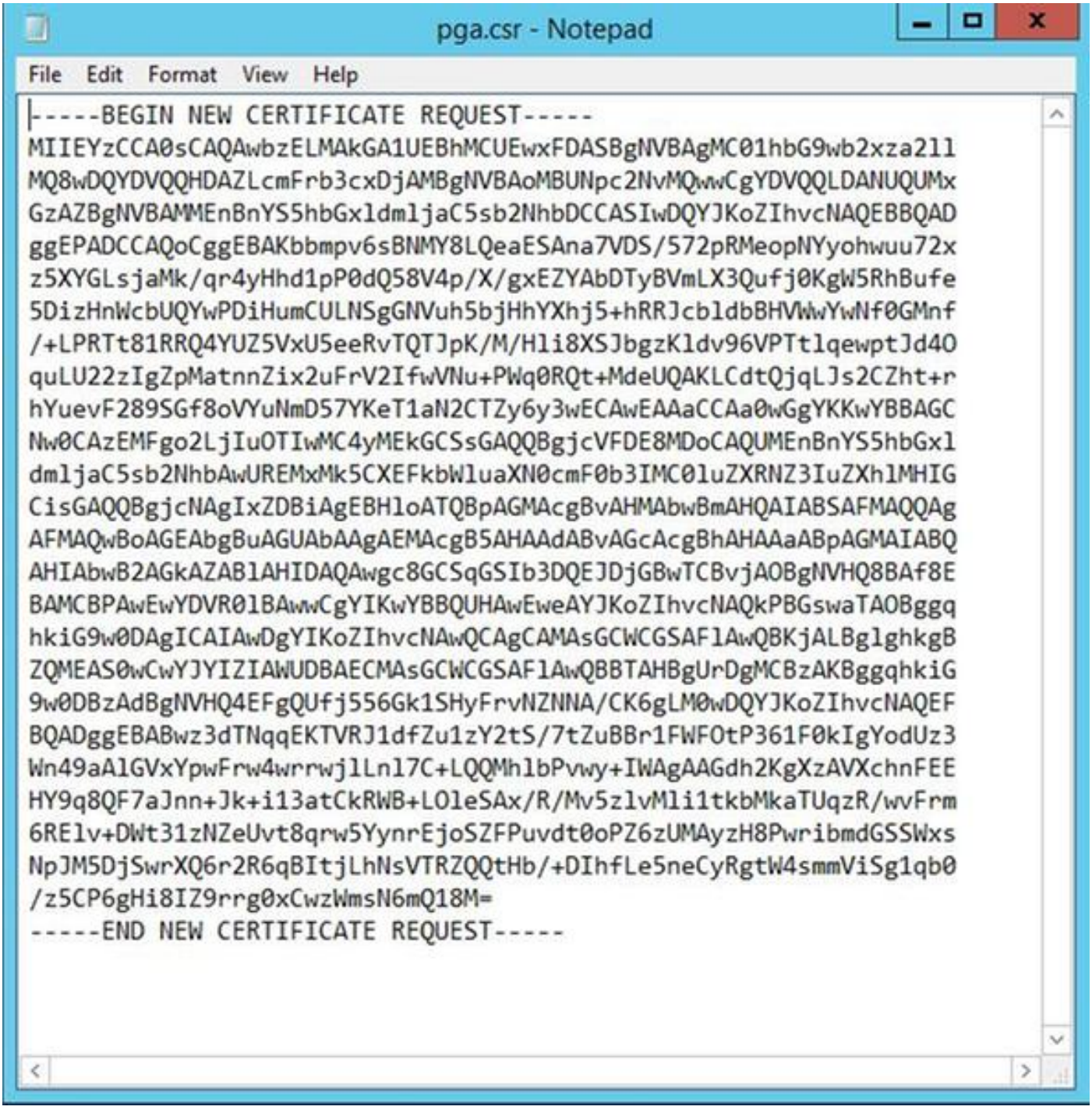
Écrivez le **nom commun** (NC), l'**organisation** (o), l'**unité d'organisation** (OU), la **localité** (l), l'**état** (St), des champs du **pays** (c). Le nom commun doit être identique que votre adresse Internet + nom de domaine du nom de domaine complet (FQDN).



Laissez les valeurs par défaut pour le fournisseur de services cryptographique et spécifiez la longueur de bit : 2048.

Sélectionnez le chemin où enregistrer. Par exemple sur l'appareil de bureau avec le nom pga.csr.

Ouvrez la demande de création récente dans le Notepad.



Copiez le certificat dans la mémoire tampon avec CTRL+C.

Signez le certificat sur l'autorité de certification

> Remarque: Si vous utilisez l'autorité de certification externe (comme GoDaddy) vous devez entrer en contact avec eux faisant ensuite générer le fichier CSR.

Connectez-vous à votre certificat de serveur CA s'inscrivent la page.
https:// <CA-server-address>/certsrv

Le certificat choisi de **demande**, la **demande avancée de certificat** et collent le contenu de la demande de signature de certificat (CSR) à la mémoire tampon. Sélectionnez alors le **modèle de certificat comme serveur Web**.

Certificat encodé de la base 64 de téléchargement.

Ouvrez le certificat et copiez le contenu du champ de thumbprint pour l'utilisation postérieure. Enlevez les espaces du thumbprint.

Installez le certificat

Copiez le certificat

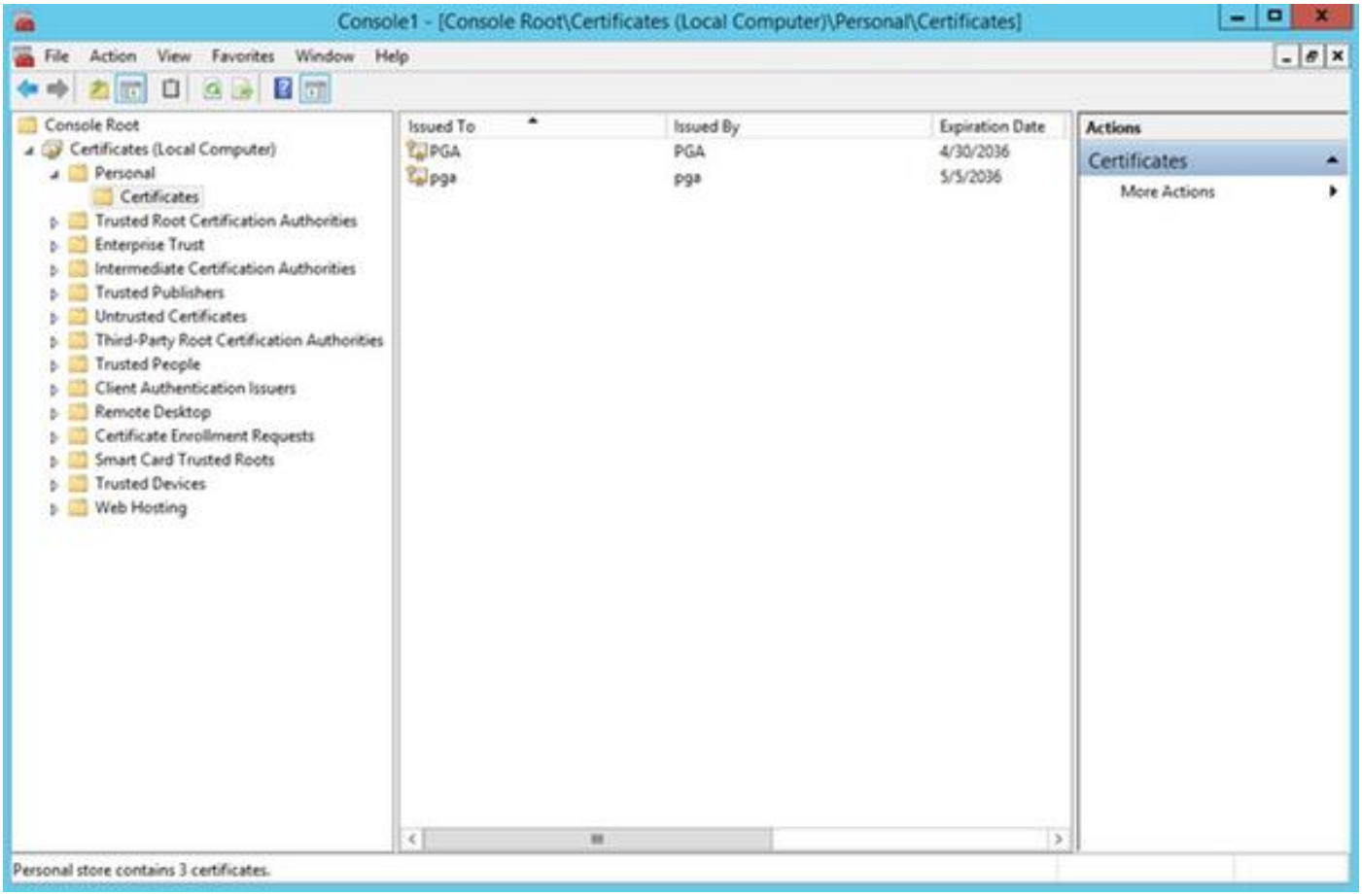
Copiez le fichier du certificat nouvellement généré dans la VM UCCE où l'outil de portique se trouve.

Importez le certificat dans la boutique informatique d'ordinateur local

Sur la même console de Microsoft Management Console de lancement de serveur UCCE (MMC) en sélectionnant le menu de démarrage, le **passage de** type et le **MMC**.

Cliquez sur Add **/retirez SNAP-dans** et dans la boîte de dialogue cliquez sur Add.
Alors sélectionnez le menu de **Certificats** et ajoutez.
Dans les Certificats SNAP-dans la boîte de dialogue, **compte > ordinateur local > finition d'ordinateur de** clic.

Naviguez vers le répertoire personnel de Certificats.



Dans le volet d'actions sélectionnez **plus d'actions > toutes les tâches > importation**.

Cliquez sur Next, **parcourez** et sélectionnez le certificat qui a été généré précédemment et dans le prochain menu assurez-vous que la mémoire de certificat a été placée à personnel. Sur le dernier écran vérifiez la **mémoire** et le **fichier du certificat de certificat** sélectionnés et cliquez sur Finish.

Certificat du grippage IIS

Ouvrez l'application CMD.

Naviguez vers le répertoire home diagnostique de portique.

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

Retirez le certificat valable liant pour l'outil de portique.

```
DiagFwCertMgr /task:UnbindCert
```

Certificat signé du grippage CA.

> **Conseil** : Employez un certain éditeur de texte (notepad++) pour enlever les espaces dans les informations parasites.

Utilisez les informations parasites enregistrées avant les espaces étant coupés.

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

Au cas où le certificat serait lié avec succès vous devriez voir que les semblables rayent dans la

sortie.
« L'attache de certificat est VALIDE »
Assurez-vous que l'attache de certificat était réussie utilisant cette commande.

```
DiagFwCertMgr /task:ValidateCertBinding
```

De nouveau le message semblable devrait être affiché dans la sortie.
« L'attache de certificat est VALIDE »

> Remarque: DiagFwCertMgr par défaut utilisera le port 7890.

Redémarrez le service diagnostique de cadre.

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

> Conseil : Entretenez la liste et particulièrement le nom de service de portique peut être vérifié par l'intermédiaire de la commande de tasklist dans l'outil CMD.

```
tasklist /v
```

Vérifiez

La page diagnostique ouverte de cadre utilisant le FQDN et elle ne devrait pas inciter un message d'avertissement de certificat.

Soutiennent le plan

Au cas où vous perdiez l'accès à l'outil de portique vous pouvez régénérer le certificat auto-signé et ajouter une exception.
Il peut être fait utilisant cette commande.

```
DiagFwCertMgr /task:CreateAndBindCert
```

Dépannez

N'utilisez pas l'adresse IP quand procédure de connexion à l'outil diagnostique de portique de cadre. Vous recevez toujours un avertissement de certificat, parce que le FQDN doit s'assortir avec la valeur spécifique dans le domaine NC de certificat.

Vérifiez que tous les serveurs sont synchronisés avec le ntp source.

```
w32tm /monitor
```

Si vous essayez d'utiliser le nom alternatif soumis (SAN) ou l'algorithme elliptique de signature numérique de curve (l'EC DSA) ou certificat de longueur 4096 principale - premier isolat qu'il n'est pas spécifique à une de ces caractéristiques.

Articles relatifs

UCCE \ PCCE - Procédure pour obtenir et télécharger le - d'individu de Windows Server signé ou les serveurs de certificat d'Autorité de certification (CA) le 2008

Configurez le certificat signé CA par l'intermédiaire du CLI dans le système d'exploitation de Voix de Cisco (VOS)