Windows: Install Certificate Authority

Type of Systems: Windows AD Domain Controller

Windows Certificate Authority (AD CD) is a component of Active Directory that creates a PKI infrastructure to generate certificates for TLS, HTTPS, or IPSEC. You can use group policy to automatically deploy public certs to domain computers, or generate certs manually for other purposes.

Install

You must have a domain admin account for these steps.

1. > Add-WindowsFeature Adcs-Cert-Authority -IncludeManagementTools
2. You probably want to create a new cert authority.
    a. >Install-AdcsCertificationAuthority -CAType EnterpriseRootCA
    b. You can also choose Standalone for CAType for a CA that is not attached to AD.

GUI INSTALL

- From the Windows Server 2012 R2 Server Manager, click Add Roles and Features.
- Select Active Directory Certificate Services.
- Click the Add Features in the popup window to allow installation of the Certification Authority Management Tools
- Select the options you want to install. I recommend the following services:
    - – Certification Authority (this is your main CA)
    - – Certification Enrollment Policy Web Service
    - – Certificate Enrollment Web Service (web portal to request certificates)
    - – Certification Web Enrollment
- Once installed, Select AD CS in your Server Manager. Notice the button warning that no configuration is done yet. Click on More.
- This will bring you to the All Servers Task Details and Notifications. Click on Configure Active Directory Certificates Services in the Action column. This will launch the AD CS configuration wizard.

Use the following parameters when going through the different steps in the wizard:

```
PowerShell
```

```
Role Services to configure          Certificate Authority + Certificate Authority
Web Enrollment


Type of CA                          Enterprise CA (if Active Directory
integrated; otherwise choose StandAlone CA


Type of CA                          Root CA (if 1<sup>st</sup> one) or
Subordinate CA (additional CA in existing authority)


Type of Private Key                 in most cases, <b>create a new private
key</b> will be the best option


Cryptographic options               RSA#Microsoft Software Key Storage Provider


2048 as Key Length


SHA1 as hash algorithm


(or any other combination for your situation)

```

- Enter a descriptive name for your Certificate CA in the Common Name field. In my example, I named it 2012R2 domain CA. Click Next.
- Update the validity period to 5 years (or whatever fits your need).
- Accept the default database locations or modify according to your own requirements.
- This completes the configuration of the first two CA components. Let's continue with the other two. In the Select Role Services to configure, choose Certificate Enrollment Web Service and Certificate Enrollment Web Policy Service.

Use the following parameters when going through the configuration wizard:

PowerShell

```
Specify CA                          Select CA Name (using Select…)


Type of Authentication              Windows Integrated


Service Account                     use the built-in application pool
identity

```

```
7
8  Authentication type for CEP          Windows Integrated
9
   Specify Authentication Certificate   <select an existing SSL certificate from the
   list)
```

This completes the configuration of all required Certificate Authority services.

Management

Unfortunately, the Powershell module for ADCS (ADCSAdministration) kind of sucks. You can see the available commands it has with:
> Get-Command -Module AdcsAdministration

Verify Certificate Authority Functionality

To verify that the CA server is operational, we can check both from within our browser as well as by checking the Certificate Authority management console.

Using the Browser: Certificate Authority Web Services

From any server in the domain, you can connect to http:<CA-Server>/certsrv. This will launch the Certificate Authority Web Enrollment portal.

We will use this portal later on to complete a certificate request…

Using the Certificate Authority Management Tool

- From the CA server, start the Certificate Authority Management tool. If all is well, this will show your CA server with a green icon, meaning the different CA services are up and running.

Complete an Internal Certificate Request

In this last step, we will walk through the process on how to request an internal SSL certificate from an IIS web server in the domain, against our internal deployed CA.

- From within IIS, select your server. Click on Server Certificates in the middle pane.

- On the right, click on Create Certificate Request.
- Enter the different fields in the request template. Most important field here is the common name, which should be set to the same name as the URL you want to use (eg. Workfolders.pdtit.be in my situation)
- Complete the wizard with the default settings and save your request file as text file on your system.

In previous Windows Server versions it was sufficient to logon to your CA Web Enrollment portal again and copy/paste the details of the certificate request file. Alas, it won't work in Windows Server 2012 R2. If you perform the same steps, you are faced with the following error message.

I could have explained the different steps on how to solve this matter, but there is already a great Microsoft Technet Wiki article that explains the different configuration steps that need to be taken in order to publish your CertSRV certificate Enrollment portal using HTTPS.

Once you have done all these steps, it should be possible to complete the certificate request steps from within the portal.

- Logon to your CA server using your browser (http://<CAserver>/certsrv).
- Select Request a Certificate.
- Select Advanced Certificate Request.
- Select Create and Submit a Request to This CA.
- In the Certificate Template select Web Server.
- Copy/paste the contents from your certificate request file (the "garbage text," including the first and last line "— beginning of new request file —" and "— end of new request file —").
- Save your certificate output as a CER-file.
- Copy this CER-file over to your web server.
- From within IIS, select Complete Certificate Request.
-