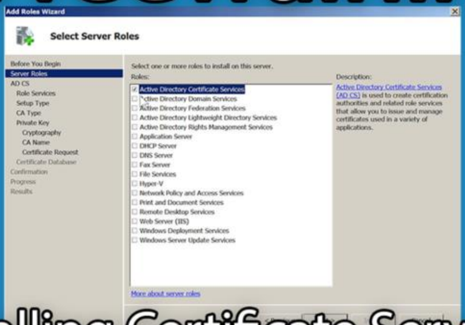
ITFreeTraining



Select one or more roles to install on this server.

Roles:

- ☑ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- □ File Services
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Desktop Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

Installing Certificate Services
Windows Server 2008

For the free video please see
http://itfreetraining.com/federation#/enterprise-ca

This video will perform a basic Active Directory Certificate Service (ADCS) install to provide a certificate for use with Active Directory Federation Services (ADFS). The video looks at how to create a template for use with ADCS. If you have an existing certificate service on your network, you can use the procedure in this video to add a template to your existing certificate server.

Demonstration

Demonstration installing the CA
To start the install, open Server Manager from the quick launch bar.
From Server Manager, select Roles from the left-hand side and then from the right-hand side select the option “Add Roles” to install the add roles wizard.
Once past the welcome screen select the role “Active Directory Certificate Services” and press next to start the Certificate Services part of the install.
The next screen is the information screen for the Certificates role. Press next to skip it.
The next screen displays all the different components that can be installed as part of the certificate role. In this case the only component that is required is “Certification Authority”. Tick this option and then press to move on to the next screen of the wizard.
On the next screen select the option of Enterprise CA. This is one of the two options to install. The Enterprise option requires the server to be a member of the domain. In later videos the standalone option is looked at to provide certificates for ADFS.
The next screen you need to decide is if the install is to be Root CA or Subordinate CA. In this case Root CA is selected because there are no other CA’s on the network. For better security a certificate hierarchy could be setup, but this video uses a simple install aimed at providing a working certificate for use with ADFS.
For the rest of the wizard all the defaults were accepted. In a production environment you may want to consider changing some of these options, for example changing the key size used for the certificate that is created for the Root CA.

Demonstration configuring the CA

To configure the certificate authority, select “Certification Authority” under “Administrative Tools” under the start menu.

Once open, expand down to Certificate Templates, right click it and select the option “Manage”. This will bring up a list of all the certificate templates that are currently configured on this server.

There is no default template for ADFS so the best option is to find a template that is simpler to the one required and then make changes to it. In this case, select the template “Web Server”, right click it and select the option “Duplicate Template”.

When duplicating the template you will be asked which version of Windows you want to use the certificate with. In this case the option “Windows Server 2008 Enterprise” was selected.

When creating templates you need to work out which is the lowest operating system that the template will be used with. In this case, no ADFS server lower than Windows Server 2008 R2 will be used so it is safe to use the option “Windows Server 2008 Enterprise”.

Once the template has been duplicated, the properties for the certificate template will automatically be opened.

On the general tab, change the “Template display name” to something meaningful. This does not affect the operation of the template but does make it easier for other administrators to understand what the template is for.

Select the tab “Subject Name” and then select the option “Build from this Active Directory information”.

From the “Subject name format” pull down, select the option “Common name”.

There are 4 tick boxes at the bottom of the screen. The only tick box that needs to be ticked is “DNS name”.

These options essentially say, take the DNS Name from Active Directory and store it in the certificate using the format common name”.

The certificate needs to be configured so the ADFS server has permission to use it. To do this, select the security tab and then press add. Press the button “Object Types” and make sure the option “Computers” is ticked.

Next enter in the computer or computers that will use this certificate template. In this case the computer name entered was “ITADFS2008R2”.

Once the permission for the computer has been added, the default permission for read will be ticked, you will also need to tick the option for “Enroll” and then press o.k. to exit.

The template has been added and configured. Next it needs to be enabled in order to allow it to start issuing certificates. To do this, in Certificate Authority Management, right click “Certificate Template” and select the option “Certificate Template to Issue” under “New”.

This will bring up the “Enable Certificate Template” Window. Find the certificate template that was just created and configured, in this case “ADFS SSL Certificate 2008 R2”, select it and press o.k. This will allow the certificate server to start issuing new certificates using that template.