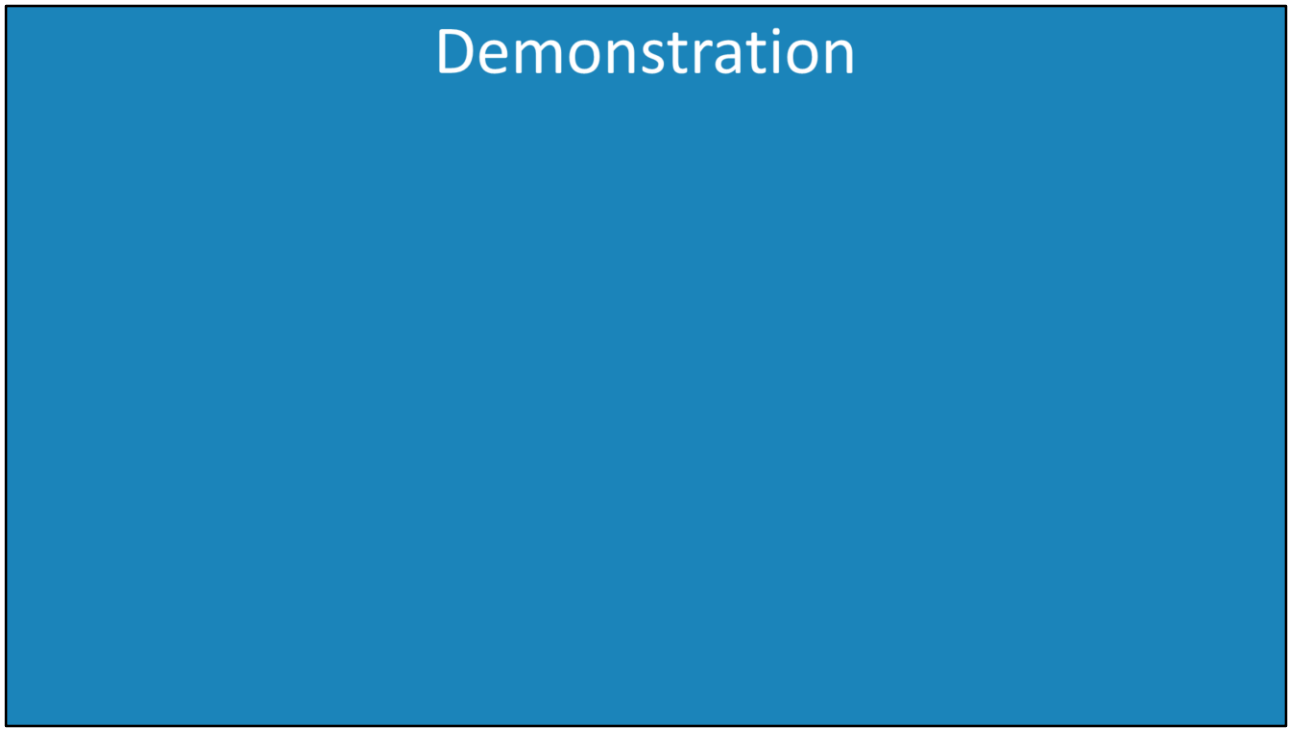
ITFreeTraining

Setting up Highcost Training ADFS 2008 R2

For the free video please see
http://itfreetraining.com/federation#/highcost

This video will look at how to set up Active Directory Federation Services in the HighCost Training domain. In this example certificate services will also be installed on the server. This means the same server will issue certificates to AD FS. Normally in a production environment you would not install certificate services on the same server as AD FS, but in this case it is done to make the install simple.



Demonstration installing Active Directory Certificate Services

00:42 Open Server Manager by selecting the icon in the quick launch bar.

00:47 From Server Manager, select roles from the left hand side and then select “Add Roles” from the right hand side to start the add roles wizard.

00:58 Skip past the welcome screen and then select the role “Active Directory Certificate Services”. AD FS will not be installed at this time because version 1.0 ships with Windows. Version 2.0 is available as a free download and will be installed later in the video. Once the option is ticked, press next to move on to the next screen.

01:24 The next screen will be the welcome screen for certificate services. Once past the welcome screen, on the next screen the components for the certificate role will be displayed. Since the role is only required to issue certificates, the only component that is required to be select is the component “Certification Authority” and then press next.

01:41 The next screen will ask if the certificate authority will be Enterprise or Standalone. In this case the Standalone option will be selected. This option could be installed on any server and does not require the server to be part of the domain. Once the Standalone option has been selected press next to continue.

01:52 On the next screen there is the choice of Root CA and Subordinate CA. Root CA’s are able to issue certificates without requiring other CA’s. In this case this option is chosen so the CA can issue a certificate directly to AD FS. In a production environment for better security you would place the root CA on a standalone server and have a subordinate CA issue certificates. For the best level of security you would

have the root CA only available when required.
02:33 For the private key screen, cryptography, CA Name, Validity period and certificate database screen, I will accept all the defaults. On a production environment you will want to go through these options and work out the best settings for your network.
02:40 Once you have verified that the settings are correct for the install, press install to start the install and then the wizard can be closed.

Demonstration requesting a certificate
The certificate snap-in needs to load in MMC and then a certificate request file created which will be imported by the stand alone CA on the server to generate the certificate.
02:55 Press the start button and then enter in the run box mmc.
03:10 From the file menu select the option “Add/remove Snap-in”.
03:19 From the list of snap-ins select “Certificates” and then press the add button.
03:20 The certificate is used by the server, so when prompted, select the option for “Computer Account” and press next.
03:30 The next screen asks which computer you want to manage certificates on. In this case the default option of the local computer will be used. Press the finish button to complete adding the snap-in followed by o.k. to return to MMC.
03:48 In certificates, expand down to personal container, right click the container and then under “All Tasks” select the option “Advanced Operations” followed by “Create Custom Request”.
04:10 The Certificate Enrollment wizard will create a request file that can be used to issue a certificate from the certificate authority. On the welcome screen press next.
04:16 On the Certificate Enrollment screen, select the option “Process without enrollment Policy” and press next. Since the CA is a standalone CA and not an Enterprise CA, the option “Active Directory Enrollment Policy” cannot be used.
04:28 For the template select the option “(No template) Legacy Key”. This option is required because Active Directory Federation Services requires access to the private key. Leave the option select “PKCS #10” and press next.
04:54 Additional information needs to be configured in the certificate request. If these options are not configured AD FS will not be able to use the certificate. To access these options press the downward arrow next to details and then press the properties button.
05:03 Enter in a friendly name and description for the certificate. This does not affect how AD FS will use the certificate, however it does make it easier for other administrators to work out what the certificate is being used for. In this case, the friendly name is configured to “HighCostTraining AD FS” and description as “High Cost Training Active Directory Federation Services”.
05:20 Select the subject tab. Two fields need to be added so AD FS can identify the certificate. Under subject name select common name. For the value, enter in the fully

qualified domain name of the server. In this case “HIADFS2008R2.HighCost.Local. Once entered, press the add button.
05:46 To configure the alternative name, select DNS from the type menu. For the value enter in the fully qualified domain name of the server. In this case “HIADFS2008R2.HighCost.Local. Once entered, press the add button.
06:06 Select the extensions tab.
06:09 Expand the section “Extended Key Usage (application policies)”. In the available options select “Server Authentication” and press add and then select “Client Authentication” and press add. This allows the certificate to be used for these two tasks which are required by AD FS.
06:26 Select the private key tab.
06:30 Expand the section key options. For the key size select 2048. Microsoft recommends at least 2048. Larger key sizes can be used, but this may lead to incompatibility problems with older hardware and operating systems.
06:50 AD FS requires access to the private key, so tick the tick box “Make private key exportable” otherwise it will not be able to get access to it.
07:01 Press o.k. and then press next to move on to the next screen of the wizard.
07:08 Press the browse button and enter in a file and path to save the request file to. In this case the request will be saved to the desktop since the CA is on this server. If the CA was on a different server, the request file would be most likely saved to removable media or e-mailed. Once entered, leave the file format on “Base 64” and press finish.
07:35 To issue the certificate using the request file, open the start menu and under “Administrative Tools” select “Certification Authority”.
07:44 From Certification Authority, right click the server name and under “All Tasks” select the option “Submit new request”.
07:56 Browse the location of the request file and press open. In this case the request file is on the desktop.
08:07 To issue the certificate, open the container “Pending Requests”. The request should be in the container. Right click the request and select “Issue” under “All Tasks”.
08:21 The certificate needs to be exported and imported into the local certificate store to be used by AD FS. To do this, select the container “Issued Certificates”. Find the certificate and double click it to open it.
08:42 To export the certificate, select the details tab and then press the button “Copy to File” to launch the certificate export wizard.
08:54 In the certificate export wizard, press next to go past the welcome screen. On the next screen select the format to export the certificate in. The default format “DER encoded binary X.509 (.CER)” will work fine so press next to continue.
09:06 Enter in a filename for the exported certificate and press next. In this case the certificate will be exported to the desktop.
09:17 Press finish to complete the export of the certificate and then close all the Windows except MMC.

09:29 The next step is to import the exported certificate to the local certificate store so that it can be used by Active Directory Federation Services. To do this, expand down to the personal container, right click it and under “All Tasks” select the option “Import” to launch the import wizard.
09:46 Once past the welcome screen of the Certificate Import Wizard, press browse and browse to the location of the exported certificate and then press next.
10:03 The next screen will ask where to store the certificate. Since I right clicked on the personal certificate container this certificate store will automatically be selected. If it is not, press the browse button and select the personal certificate store and then press next and the press finish to complete the wizard.
10:25 Close all the open Windows.

Demonstration Installing and configuring AD FS
The version of AD FS shipped with Windows Server 2008 R2 is version 1.0. There is a newer version 2.0 that is a free download from Microsoft that will be installed and configured instead.
10:32 Open Internet Explorer from the start menu.
10:36 open http://www.google.com and perform a search for “ADFS 2.0 RTW”. RTW means released to web. Select the first result. If you cannot find it go to http://www.microsoft.com/en-au/download/details.aspx?id=10909
11:00 Select the language that you want to download and then press the continue button.
11:08 The next screen will ask if you want to register with Microsoft to receive updates. This is up to you, in this case the default option no will be selected and next pressed.
11:19 At the next screen, you need to select which version of AD FS to download. In this case the 64 bit version for Windows Server 2008 R2 was selected, however there is also options for the 32 and 64 bit version for Windows Server 2008. Once you have made the selection press next to start the download and save it to the desktop.
11:44 Run the setup saved to the desktop to launch the setup wizard.
11:50 Press next to go past the welcome screen and then tick the tick box “I accept the terms in the license Agreement” and press next.
11:59 On the Server Role screen choose either Federation Server or Federation Server Proxy. In this case Federation Server is chosen. The Federation server proxy is reverse proxy like service that is used by clients to access a federation server when it is behind a firewall. When you have made your selection press next.
12:20 The next screen will tell you what prerequisite software is required to be install for AD FS. If the software has not already been installed, setup will automatically install it for you. Press next to continue. The install will then start, which will take a few minutes to complete.
12:50 On the final screen of the wizard there is a tickbox “Start the AD FS 2.0 Management Snap-in when this wizard closes”. In this case the option was left ticked

so when finish is press the Management tool will be automatically opened.
13:13 Additional post-configuration of AD FS is required. To perform this step, select the option in the middle of the screen “AD FS 2.0 Federation Server Configuration Wizard”.
13:28 On the first screen of the wizard, you can create a new federation service or add this server to an existing federation service or farm. In this case there is no existing Federation Services on the network so the first option “Create a new Federation Service” will be selected. Once selected press next to continue.
13:56 At the next screen, the administrator can choose to create a new farm or create a stand-alone install. There is no change to the functionality of the AD FS system regardless which option you choose. If you choose the stand-alone option you will not be able to add servers later on. For this reason, if you are not sure, you should choose the option “New federation server farm”. Once selected press next to continue.
14:29 On the next screen the certificate needs to be selected to use with Active Directory Federation Services. Since this server contains a CA the certificate for the CA will also appear. Make sure that if you have the CA installed on the same server that you choose the correct certificate and then press next to move on.
14:47 The next screen requires a service account. In this case I will browse to the service account that was created earlier and enter in its password. The service account can be a regular user account that has been added to the local administrators group. You could also use a domain administrator’s user account, but this is not considered to be best practice. Once the user account has been entered and the password entered, press next.
15:14 The next screen will show a summary of all the options that have been selected in the wizard. If you are happy with the options press next.
15:20 At the next screen the configuration of AD FS will occur. The results of the configuration will be shown. In this case, setup has indicated a warning stating that it could not configure the SPN on the service account. The SPN was created when the user account was created. Setup will not configure the SPN if it has already been configured. If the SPN is incorrect, you can change it by opening the properties of the user account.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
“Active Directory Federation Services 2.0 RTW” http://www.microsoft.com/en-au/download/details.aspx?id=10909