Dave Mulford's Blog:Active Directory Enterprise Certification Authority Setup

Posted by Dave Mulford Jan 18, 2018
This post is part 2 in a series on setting up Red Hat's mod_auth_mellon with Microsoft's Active Directory Federation Services. It is assumed that you've completed Part 1 - Active Directory Domain Services Setup.

Install the Active Directory Certificate Services feature

Go into **Server Manager** and click **Add Roles and Features**. Accept all default options by clicking **Next** until you arrive at the **Select Server Roles** screen.

Check the **Active Directory Certificate Services** feature, and click the **Add Features** button when the prompt appears. Click **Next** until you see the **Confirmation** screen.

Click the **Install** button. Installation can take a few minutes to complete.

Configure Active Directory Certificate Services

Go into **Server Manager** and find a flag with a warning icon next to it, near the top of the screen. Click the flag to open a menu, then click **Configure Active Directory Certificate Services** in the Post-Deployment Configuration item to open the **AD CS Configuration** window.

On the **Credentials** screen, choose a domain administrator if one isn't already populated in the Credentials text box, then click **Next**.

On the **Role Services** screen, select the **Certification Authority** checkbox, then click **Next**.

On the **Setup Type** screen, choose the **Enterprise CA** option. If this is disabled, your machine is not joined to a domain and you'll need to complete Part 1 - Active Directory Domain Services Setup before proceeding.

On the **CA Type** screen, choose **Root CA**, then click **Next**.

In the **Private Key** screen, choose the **Create a new private key** option.

Click **Next** on the following screens to accept the default options: Cryptography, CA Name, Validity Period, and Certificate Database.

On the **Progress** screen, click **Configure**. This can take a few minutes to complete. Click **Close**.

Configure an ADFS Certificate Template

Go into **Server Manager**, then navigate to the **Tools** -> **Certification Authority** menu to open the Certification Authority window.

Expand the domain in the left pane and right-click **Certificate Templates**, then choose **Manage** to open the **Certificate Templates Console**.

In the center pane, scroll down to the botton, then right-click **Web Server** and choose **Duplicate Template**.

In the Properties of New Template window, set the following options:

General Tab

- Change the name to "ADFS SSL Certificate"

Subject Name Tab (this sets the Common Name in the certificate to the FQDN of the Windows server)

- Choose the **Build from this Active Directory Information** option
- Under **Subject name format** drop-down, select **Common Name**
- Check **DNS Name**
- Uncheck **User principal name (UPN)**

Security Tab

Click the **Add** button to open the **Select Users and Computers Window**.

- Click the **Object Types** button, check the **Computers** option, then click **OK** to close this window.
- On the **Select Users and Computers Window**, enter the hostname of the ADFS server, then click **OK** to close the window.
- Back on the Security Tab, check **Enroll** under the **Allow** column in the Permissions section.
- Click **OK** to close this window.

On the **Certification Authority window**, right-click **Certificate Templates** and choose **New** -> **Certificate Template to Issue**.

Choose the **ADFS SSL Certificate**, then click **OK**.

The ADFS SSL Certificate Template is now added to the list of Certificate Templates and can be used to generate new certificates when setting up ADFS in part 3 of this series.
27 Views Tags: active-directory, mod_auth_mellon, windows-server

There are no comments on this post