Dave Mulford's Blog:Active Directory Federation Services Setup

Posted by Dave Mulford Jan 18, 2018
This is part 3 in a series about 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 and Part 2 - Active Directory Enterprise Certification Authority Setup.

Install the Active Directory Federation Services feature

Go into **Server Manager** and click **Add Roles and Features**. Click **Next** until you arrive at the **Server Roles** screen.

Check the **Active Directory Federation Services** checkbox. Click **Next** until you reach the **Confirmation** screen, then click **Install**.

The install can take a minute or so. Once complete, click **Close**.

Obtain a certificate from the Enterprise CA

Right-click the **Start Menu**, select **Run**, then enter "mmc" and click **OK** to open the Microsoft Management Console window.

In MMC, select **File** -> **Add/Remove Snap-In**.

Select **Certificates** from the list of available snap-ins and click the **Add** button. You will be prompted for a scope of certificates. Choose the **Computer account** option and click **Next**, then **Finish**.

Expand the **Certificates** feature and select the **Personal** folder. Choose the **View** menu, then click **Options**. In the Options windows, choose the **Certificate purpose** option under the **Organize view mode by** setting, then click **OK**.

In MMC, right-click **Server Authentication**, then choose **All Taks** -> **Request New Certificate** to launch the Certificate Enrollment window.

In the Certificate Enrollment window, click **Next** twice. Check the box next to the **ADFS SSL Certificate template**, then click **Enroll**. Once enrollment is complete, click **Finish**.

You can now close MMC and tell it no when it asks to save the snap-in configuration.

Create a KDS Root Key to allow Windows to generate service accounts and passwords

Open a **Powershell** command window and issue the following command:

```
Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
```

Close the Powershell window. If you have more than one domain controller, it will take up to 10 hours to replicate the root key. Since this tutorial has a single domain controller, this doesn't matter.

Configure the Active Directory Federation Services feature

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 Federation Services** in the Post-Deployment Configuration item to open the **AD FS Configuration** window.

On the **Welcome** screen, select the **Create the first federation server in a federation server farm** radio button, then click **Next**.

On the **Connect to AD DS** screen, The MYDOMAIN\Administrator user should be automatically populated. Click **Next**.

On the **Specify Server Properties** screen, choose the following options, then click **Next**.

- Choose the **SSL certificate** that was created earlier via enrollment
- The **Federation Service Name** field will be automatically populated when a certificate is chosen
- Enter a **friendly display name**

On the **Specify Service Account** screen, choose the following options, then click **Next**.

- Choose the **Create a Group Managed Service Account** option
- Enter a name for the account. For example, ADFSManagedAccount.

On the **Specify Database** screen, Choose the **Create a database on this server using Windows Internal Database**, then click **Next**.

On the **Review Options** screen, click **Next**.

On the **Prerequisite Checks screen**, ignore the warning about the root key's Managed Service Account, and click **Configure**. Click the **Close** button once configuration is complete.
37 Views Tags: active-directory, mod_auth_mellon, windows-server

There are no comments on this post