


Upgrading AD RMS to Windows Server 2016

Article • 09/24/2021 • 24 minutes to read

Introduction

Active Directory Rights Management Services (AD RMS) is a Microsoft service that protects sensitive documents and emails. Unlike traditional protection methods, such as firewalls and ACLs, AD RMS encryption and protection are persistent no matter where a file goes or how it is transported.

This document provides guidance for migrating from Windows Server 2012 R2 with SQL Server 2012 to Windows Server 2016 and SQL Server 2016. The same process can be used to migrate from older but supported versions of AD RMS. Please note that Active Directory Rights Management Services is no longer in active development, and for the latest capabilities customers should consider migrating to [Azure Information Protection](#) , which offers a much more comprehensive set of features with more complete device and application support.

For information on migrating to Azure Information Protection from AD RMS without having to re-protect your content see [the Azure Information Protection migration documentation](#).

About the environment used in this guide

AD FS is an optional component of an AD RMS installation. In this guide, the use of AD FS is assumed. If AD FS hasn't been used in your environment for supporting AD RMS users, you can skip all steps that refer to AD FS.

In this guide, SQL Server is upgraded to SQL Server 2016 by performing a parallel install and moving the databases over via a backup. Alternatively, if you can upgrade your AD RMS and AD FS database servers to SQL Server 2016 in-place, you can move to the next section in this document after having done that without having to follow the steps in this section.

Installation

Configuring SQL Server 2016

The following section details implementation tasks related directly to the SQL Server 2016 configuration. This guide focuses on using the Server Manager and the SQL Server Management Studio to complete these tasks.

These steps must be completed on a SQL Server 2016 installation. Install SQL Server 2016 on suitable hardware as per your organization's standard practices and policies.

Preparing the SQL Server

The following section details how to prepare the SQL Server so that it can be upgraded to SQL Server 2016 before upgrading other services in the AD RMS platform to use Windows Server 2016.

Adding CNAME for SQL Server 2016 to DNS

The CNAME is used to help ensure that the Windows Server 2016 setup will be getting the appropriate data since it will be pointed at the new SQL Server 2016. **Note: If already using a CNAME for the AD FS and AD RMS service, you can move on to the next steps.**

To add a CNAME for SQL Server 2016 to DNS

1. Log on to the Windows Server 2012 R2 Domain Controller with Domain admin credentials.
2. Open Server Manager.
3. Click **Tools** and select **DNS** to open the DNS Manager.
4. From the left navigation pane, expand the DC and open up **Forward Lookup Zones**.
5. Open the appropriate domain resources then right click in the right view pane and select **New Alias (CNAME)** to begin creating the CNAME.
6. For the alias name enter in a logical name to differentiate it from other that may be present (Ex. SQLADRMS or SQLADFS)
7. After entering the name, provide the FQDN for the target host which will be the new SQL Server 2016 server. (ex. SQL2016.contoso.com)
8. Once all the information has been entered, click **OK**.

Backup the AD RMS and AD FS Databases

The AD RMS and AD FS databases hold critical information necessary to AD RMS, such as the public key of the Server Licenser Certificate, rights policy templates, AD FS configuration data, and logging information. Without these databases, clients cannot issue licenses to consume protected content, among other issues.

Of the databases, the AD RMS configuration database is considered the most important, as it stores the SLC, rights policy templates, users' keys, and configuration information. Therefore, though you should take care to back up all of the AD RMS and AD FS databases, you should plan to back up the configuration database regularly.

The logging database stores information about user requests to the AD RMS cluster for certificates and use licenses. Your backup strategy of this database should be based on company policy for retaining this type of information.

The directory services database is not critical to AD RMS functionality and, if the latest data is lost, the database will repopulate with information as the AD RMS server receives requests for certificates and use licenses. You do not need to backup this database regularly, but you do need to have at least a copy of the database as it was originally configured after deploying AD RMS.

To backup an AD RMS and/or AD FS database with Microsoft SQL Server

1. Log on to the Windows Server 2012 R2 AD RMS database server with SQL 2012.
2. Click **Start**, click **All Programs**, click **Microsoft SQL Server**, and click **SQL Server Management Studio**.
3. In the **Connect to Server** window, confirm the server hosting the AD RMS databases is in the **Server Name** box and click **Connect**.
4. Expand **Databases**. Right click the appropriate database (**DRMS** and **Adfs**), point to **Tasks**, and select **Backup**.
5. Repeat step 4 for the remaining databases.
6. Ensure that the backup of the databases can be accessed by other machines on the network or using a storage device as they will be needed for later steps during the migration.

Now you can store the database copies in a secure location. Remember to back up your databases frequently.

Adding Domain Admin, SQL, AD RMS, and/or AD FS Service Account to SQL Server 2016

The following steps will showcase how to add the various Service Accounts to SQL Server 2016 to assist with migrating the data from the Windows Server 2012 R2 environment. This will give the proper permissions when trying to access the content and handle the data.

To add the Domain Admin, SQL, AD RMS, and/or AD FS Service Account to SQL Server

1. Log on to the server with SQL Server 2016 as the Local Admin account.
2. Click **Start**, click **All Programs**, click **Microsoft SQL Server**, and click **SQL Server Management Studio**.
3. In the **Connect to Server** window, confirm the server hosting the AD RMS databases is in the **Server Name** box then for Authentication click the drop-down menu and select **SQL Server Authentication**.
4. In the **Login** field enter the name of the Local Admin account (Ex. localadmin) and then provide the appropriate password and click **Connect**.
5. Expand **Security** and then right-click **Logins** and select **New Login** from the context menu that appears.
6. Once the window appears enter in the Domain Admin account in the **Login name** field (Ex. Contoso\ContosoAdmin)
7. From the left navigation pane, choose **Server Roles**.
8. Then mark the checkbox for **sysadmin** under the server roles and click **OK**.
9. Restart **SQL Server Management**.
10. In the **Connect to Server** window, confirm the server hosting the AD RMS databases is in the **Server Name** box then for Authentication click the drop-down menu and select **Windows Authentication** and click **Connect**.

Restoring the AD RMS and AD FS Databases to SQL Server 2016

The following steps will showcase how to restore the data from the previous SQL Server instance to the new 2016 instance. This will allow the new SQL to utilize the relevant configuration data from the previous AD RMS and AD FS databases.

To restore the data from the previous SQL Server to the new SQL Server

1. Log on to the server with SQL Server 2016 with the appropriate account.

2. From the left navigation pane, right-click **Databases** and select **Restore Database** to begin the restoration process.
3. Under **Source** choose **Device** and then browse for the location where the database files were stored in the earlier steps.
4. Once the files have been selected, click **OK**.
5. Ensure that all the database files have been added and complete the process by clicking **OK**.

Configuring Windows Server 2016 Active Directory Federation Services (AD FS)

AD FS has been deployed to provide single sign-on (SSO) access to AD RMS as an application. It has also been configured with the AD RMS Mobile Device Extension (MDE), which enables Mac and mobile device support for end users.

The following sections provide guidance on operational tasks you may need to perform on your AD FS deployment.

Adding a 2016 AD FS Server to the Farm

You can deploy additional AD FS servers to support the AD RMS deployment. You may choose to perform this action in the event of increased traffic to the AD RMS servers, or additional applications, or if you need to retire one of the servers currently being used for AD FS.

To add the 2016 AD FS server to the farm

1. From the Azure AD Connect server, double click the **Azure AD Connect** icon to launch the Azure AD Connect wizard.
2. In the Welcome page, click **Configure**.
3. In the Additional Tasks page, click **Deploy an additional Federation Server** and then click **Next**.
4. In the Connect to Azure AD page, enter the user name and password of an account with Global Administrative permissions and then click **Next**.
5. In the Domain Administrator credentials page, enter the user name and password of an account with Domain Admin permissions and click **Next**.

6. Click **Browse** and select the certificate file used when configuring the AD FS farm using the Azure AD Connect.
7. Click **Enter Password** to open the Certificate Password dialog box.
8. Enter the password of the certificate in the Password field and then click **OK**.
9. Click **Next**.
10. In the AD FS Servers page, enter the name or the IP address of the new AD FS server and click **Add**.
11. In the Ready to Configure page, click **Install**.
12. In the Installation Complete page, click **Exit**.

Raising the AD FS Farm Behavior Level

When deploying an AD FS server that exceeds the current environment level such as, having an AD FS on Windows Server 2012 R2 and then adding an AD FS Windows Server 2016, the Farm Behavior Level will need to be increased. This is needed to ensure that the environment is using the most up to date information and functions.

To raise the AD FS Farm Behavior Level

1. Navigate to the Windows Server 2016 AD FS.
2. Open an admin PowerShell session.
3. Enter the following command: **\$cred = Get-Credential**
4. A window will appear asking for credentials, enter in the domain admin credentials.
5. Then enter this command: **Invoke-AdfsFarmBehaviorLevelRaise -Credential \$cred**
6. A prompt will appear asking, **Do you want to continue with this operation?** Then enter **a** to accept the prompt.
7. After the command has completed, the Farm Behavior Level will be setup and ready.

Enabling Mobile Device Extension Logging

The Mobile Device Extension can log requests it receives from end user devices. Logging is disabled by default and we recommend only enabling logging in a troubleshooting scenario. All requests, from mobile devices and desktop machines, to bootstrap or

acquire an end use license are logged in the AD RMS logging database or Azure storage account. MDE logging will create two additional tables to the SQL Server used by AD RMS: the client debug log table and the client performance log table.

To enable Mobile Device Extension logging

1. From an AD RMS server, open Windows PowerShell as an administrator.
2. Type the following command and press **Enter**: **Import-Module AdRmsAdmin**
3. Type the following command and press **Enter**: **New-PSDrive -Name AdrmsCluster -PsProvider AdRmsAdmin -Root https://localhost**
4. Type the following command and press **Enter**: **Set-ItemProperty -Path AdrmsCluster:\ -Name IsLoggingEnabled -Value \$true**

If you are using MDE logging for troubleshooting, we recommend disabling it after addressing the issue.

To disable Mobile Device Extension logging

1. From an AD RMS server, open Windows PowerShell as an administrator.
2. Type the following command and press **Enter**: **Import-Module AdRmsAdmin**
3. Type the following command and press **Enter**: **New-PSDrive -Name AdrmsCluster -PsProvider AdRmsAdmin -Root https://localhost**
4. Type the following command and press **Enter**: **Set-ItemProperty -Path AdrmsCluster:\ -Name IsLoggingEnabled -Value \$false**

Upgrading AD RMS to Windows Server 2016

The following sections provide guidance on how to add a Windows Server 2016-based AD RMS Server into the current Windows Server 2012 R2 cluster. The server will be added into the cluster and the information will be replicated to it so that the previous AD RMS server can be deprecated to free up resources.

After you add one Windows Server 2016-based AD RMS server has been added to your AD RMS cluster, all nodes based on older versions of Windows will become inactive. After this is done you can deprovision those servers (e.g. shut down, repurpose or reinstall with Windows Server 2016 to join the AD RMS cluster).

You can deploy additional AD RMS servers to the cluster to support the load on your AD RMS deployment. You may also choose to perform this action in the event of increased

traffic to the AD RMS servers.

This guide doesn't cover the steps required to alter the load balancing mechanisms you might be using in your environment to exclude the servers you are deprecating and to include the ones you are adding to the cluster.

Adding a 2016 AD RMS Server

If your AD RMS cluster is using a Hardware Security Module instead of a Centrally Managed key for its Server Licenser Certificate, you will need to install the software and other HSM artifacts (e.g. key and configuration files) on the server before installing AD RMS. You will also need to connect the HSM to the server, either physically or through the relevant network configurations. Follow your HSM guidance for these steps.

To add a 2016 AD RMS Server

1. Install the AD RMS Role on the desired Windows Server 2016 deployment.
2. After installation completes, select the link to **Perform additional configuration**.
3. Select **Join an existing AD RMS cluster** and click **Next**.
4. On the **Select Configuration Database** page, enter the CNAME specified in the DNS for the 2016 SQL server (FQDN).
5. Click **List** on the second line and select the **DefaultInstance** from the drop-down.
6. Under **Configuration Database Name**, select the drop-down menu and choose the DRMS configuration that appears. Then click **Next**.
7. On the **Database Information** page, enter the cluster key password in the field provided. After that, click **Next**.
8. In the next page of the wizard, specify the AD RMS service account and provide the password for it and click **Next** once it has been verified.
9. Once the **Cluster Web Site** page appears, simply ensure that the appropriate web site has been selected and click **Next**.
10. On the **Choose a Server Authentication Certificate** page, select the imported SSL certificate and click **Next**.
11. Click **Install** to begin the installation.
12. After configuration completes, you will need to log off and back on to administer AD RMS.

13. Once logged back on, open **Server Manager** select **Tools** and then **Active Directory Rights Management**. The management window should appear and indicate that the cluster has the additional server in the cluster.
14. If the AD RMS Mobile Device Extension was installed in the original AD RMS cluster, you need to also install the MDE in the updated cluster nodes. Follow the instructions in the MDE documentation to add MDE to your AD RMS cluster. At this point, you can repurpose all the preexisting nodes or upgrade them to Windows Server 2016 and re-join them to the AD RMS cluster using the same process outlined above.

Configuring Windows Server 2016 Web Application Proxy (WAP)

The following sections provide guidance on operational tasks you may need to perform on your Web Application Proxy deployment. This is an optional step, not required if you are publishing AD RMS to the Internet through other mechanisms.

Adding a Windows Server 2016 WAP Server

You can deploy additional Web Application Proxy servers to support the AD RMS deployment. You may choose to perform this action in the event of increased traffic to the AD RMS servers or if you need to retire one of the servers currently being used for the Web Application Proxy.

To add a 2016 Web Application Proxy server

1. From the server you wish to setup as a Web Application Proxy, navigate to the Server Manager console and click **Add roles and features**.
2. In the **Add Roles and Features Wizard**, click **Next** until you get to the Server Role selection screen.
3. On the Select Server Roles screen, select **Remote Access**, and then click **Next** until you are back at the Select Server Roles screen.
4. On the Select Server Roles screen, select **Web Application Proxy**, click **Add Features**, and then click **Next**.
5. On the Confirm Installation Selections screen, click **Install**.
6. Once the installation has completed, click **Close**.

7. Now it is time to configure the server. To do this, open the Remote Access Management console on the Web Application Proxy server. Open the **Start** menu, type **RAMgmtUI.exe**, and then select the application.
8. In the navigation pane, click **Web Application Proxy**.
9. In the Remote Access Management console click **Run the Web Application Proxy Configuration Wizard**. Once in the wizard, click **Next**.
10. On the Federation Server screen enter the fully qualified domain name of the AD FS server (Ex. adfs.contoso.com) and then enter credentials for an administrator on the AD FS server.
11. On the AD FS Proxy Certificate screen, in the list of certificates currently installed on the Web Application Proxy server, select a certificate to be used by Web Application Proxy for AD FS proxy, and then click **Next**.
12. On the Confirmation screen, review the settings then click **Configure**.
13. Once the configuration is complete, click **Close**.

DNS Configuration for 2016 WAP Server

Once the Windows Server 2016 Web Application Proxy server has been put in place, some DNS changes will need to be made. This will require using a DNS service, such as GoDaddy, to point the AD FS and AD RMS services at the 2016 WAP server.

To point the DNS at the WAP server

1. Navigate to your provider's website (ex. GoDaddy).
2. Go into Domain Management and then DNS Management.
3. Locate the AD FS and AD RMS service and replace the **Points to** portion with the Public IP Address of the 2016 WAP server and **Save**.
4. The changes may take time to propagate, but once they do this setup will be complete.

Enabling Debugging Logs

Detailed logging information is available on the Web Application Proxy servers. You can configure advanced debugging logging using the Event Viewer. Additional settings can

also be selected for the size of the logs to help ensure that the analytics are useful to the viewer.

Enabling Debugging Logs for the Web Application Proxy

1. Open the **Event Viewer** console on the Web Application Proxy.
2. Expand the **Microsoft** node.
3. Expand the **Windows** node.
4. Open the **Web Application Proxy** logs.
5. You will then be able to open the **Admin** logs.
6. Open the **Action** menu, located in the top left, and select **Properties**.
7. Under the **General** tab, choose the option to **Enable Logging**.
8. Finally, you are able to customize maximum log size and what happens when the maximum event log size is reached.

Configuring High Availability for Windows Server 2016 Services

The following sections provide guidance on operational tasks you may need to setup your Windows Server 2016 environment in High Availability.

Adding a 2016 AD RMS Server for High Availability

You can deploy additional AD RMS servers to setup High Availability. You may choose to perform this action in the event of increased traffic to the AD RMS servers.

To add a 2016 AD RMS server for High Availability

1. Install the AD RMS Role on the desired Windows Server 2016 deployment.
2. After installation completes, select the link to **Perform additional configuration**.
3. Select **Join an existing AD RMS cluster** and click **Next**.
4. On the **Select Configuration Database** page, enter the CNAME specified in the DNS for the 2016 SQL server (FQDN).
5. Click **List** on the second line and select the **DefaultInstance** from the drop-down.

6. Under **Configuration Database Name**, select the drop-down menu and choose the DRMS configuration that appears. Then click **Next**.
7. On the **Database Information** page, enter the cluster key password in the field provided. After that, click **Next**.
8. In the next page of the wizard, specify the AD RMS service account and provide the password for it and click **Next** once it has been verified.
9. Once the **Cluster Web Site** page appears, simply ensure that the appropriate web site has been selected and click **Next**.
10. On the **Choose a Server Authentication Certificate** page, select the imported SSL certificate and click **Next**.
11. Click **Install** to begin the installation.
12. After configuration completes, you will need to log off and back on to administer AD RMS.
13. Once logged back on, open **Server Manager** select **Tools** and then **Active Directory Rights Management**. The management window should appear and indicate that the cluster has the additional server in the cluster.
14. After confirming the server setup, configure your Load Balancing service to balance the load between the different AD RMS servers in the cluster.

Adding a Windows Server 2016 AD FS Server for High Availability

You can deploy additional AD FS servers to setup High Availability. You may choose to perform this action in the event of increased traffic to the AD FS servers. **Note: after raising the farm behavior level, a new database entry will be entered into the SQL Server 2016(Adfs Configv3) and the old configuration database must be deleted before continuing with these steps.**

To add the Windows Server 2016 AD FS server for High Availability

1. Install the AD RMS Role on the desired Windows Server 2016 deployment.
2. After installation completes, select the link to **Configure the federation service on this server**.
3. In the welcome section of the wizard, choose the option to **Add a federation server to a federation server farm** and then click **Next**.

4. Specify the proper admin account and click **Next**.
5. On the **Specify Farm** page, pick the **Specify database location for an existing farm using SQL Server** then enter the CNAME for the SQL service for the Database Host Name and click **Next**.
6. Under the **Specify Service Account** area of the wizard, enter the credentials for the AD FS service account and then click **Next**.
7. In **Review Options**, click **Next**.
8. Click **Configure** when the button becomes available.
9. After the configuration, restart the machine.
10. After confirming the server setup, Load Balance the AD FS servers as required.

Adding a Windows Server 2016 WAP Server for High Availability

You can deploy additional WAP servers to setup High Availability. You may choose to perform this action in the event of increased traffic to the AD RMS servers.

To add a Windows Server 2016 Web Application Proxy server for High Availability

1. From the server you wish to setup as a Web Application Proxy, navigate to the Server Manager console and click **Add roles and features**.
2. In the **Add Roles and Features Wizard**, click **Next** until you get to the Server Role selection screen.
3. On the Select Server Roles screen, select **Remote Access**, and then click **Next** until you are back at the Select Server Roles screen.
4. On the Select Server Roles screen, select **Web Application Proxy**, click **Add Features**, and then click **Next**.
5. On the Confirm Installation Selections screen, click **Install**.
6. Once the installation has completed, click **Close**.
7. Now it is time to configure the server. To do this, open the Remote Access Management console on the Web Application Proxy server. Open the **Start** menu, type **RAMgmtUI.exe**, and then select the application.
8. In the navigation pane, click **Web Application Proxy**.

9. In the Remote Access Management console click **Run the Web Application Proxy Configuration Wizard**. Once in the wizard, click **Next**.
10. On the Federation Server screen enter the fully qualified domain name of the AD FS server (Ex. adfs.contoso.com) and then enter credentials for an administrator on the AD FS server.
11. On the AD FS Proxy Certificate screen, in the list of certificates currently installed on the Web Application Proxy server, select a certificate to be used by Web Application Proxy for AD FS proxy, and then click **Next**.
12. On the Confirmation screen, review the settings then click **Configure**.
13. Once the configuration is complete, click **Close**.
14. After confirming the server setup, Load Balance the WAP servers in the DMZ.

Adding a SQL Server 2016 node for Always On High Availability

You can deploy additional SQL servers to setup Always On High Availability. You may choose to perform this action in the event of increased traffic to the AD RMS servers.

Note: ensure that both SQL Servers have the Inbound port 5022 open.

To add a SQL server 2016 server for Always On High Availability

1. From the server you wish to setup as an additional SQL Server 2016 server, navigate to the Server Manager console and click **Add roles and features**.
2. Click **Next** till the **Select Features** dialog box.
3. Select the **Failover Clustering** checkbox. **Note: follow this step for the original SQL server 2016 server as well so that both SQL Servers have the Failover Clustering feature.**
4. Click **Install** to install the Failover Clustering feature.
5. Now, open **Server Manager** and select **Tools** then **Failover Cluster Manager**.
6. From the left menu pane, right-click **Failover Cluster Manager** and select **Create Cluster**
7. This will open the **Create Cluster Wizard**.
8. Browse for the SQL server 2016 servers which will be used for Always On High Availability and enter them in then click **Next**.

9. You will receive a validation warning. Select **Yes** to Validate the Cluster nodes and then click **Next**.
10. Under the **Testing Options** page, select the option **Run all tests** and click **Next**.
11. **Note: The Cluster Validation Wizard is expected to return several Warning messages, especially if you will not be using shared storage. Other than that, if you find any error messages you need to fix them prior to creating the Windows Server Failover Cluster.**
12. In the **Access Point for Administering the Cluster** dialog box, enter the cluster name and virtual IP address for the Windows Server Failover Cluster, then click **Next**.
13. Verify that the configuration is successful in **Summary** and click **Finish**.
14. Back in the **Failover Cluster Manager**, right-click on your cluster and select **More Actions** then choose **Configure Cluster Quorum Settings**
15. Click **Next** and then pick the option for **Select the quorum witness** and hit **Next** again.
16. In the **Select Quorum Witness** page, select the **Configure a file share witness** option. Then click **Next**.
17. Select **Browse** and locate the path of the file share that you want to use in the File Share Path dialogue box. Click **Next**.
18. On the Confirmation page, click **Next**.
19. On the Summary page, click **Finish**.
20. Now, open the **Start** menu and search for **SQL Server Configuration Manager**.
21. Right-click the SQL Server name and pick **Properties**.
22. In the Properties dialog box, select the **AlwaysOn High Availability** tab. Check the **Enable AlwaysOn Availability Groups** check box. Click **OK**. **Note: do this on both SQL server 2016 servers.**
23. Then restart the SQL Server service.
24. Now, open the **Start** menu and search for **SQL Server Management Studio** and from the left navigation pane, right-click **Availability Groups** and click **New Availability Group Wizard** then click **Next**.

25. In the **Specify Availability Group Name** page pick a group name (Ex.SQLAvailabilityGroup2016). Then click **Next**.
26. Under the **Select Databases** section, specify the databases. Then click Next. **Note: some database may need to be backed up again or put into Full Recovery mode.**
27. Once on the **Specify Replicas** page, click the **Add Replica** button and pick your other 2016 SQL Server.
28. After adding the other server, click the check boxes and set the secondary server to be a readable secondary.
29. Navigate to the **Endpoints** tab and click the **Refresh** option. While also here, scroll across and ensure that the same service account is on the primary and secondary node.
30. Now, choose the **Backup Preferences** tab and select the **Prefer Secondary** option.
31. Move on to the **Listener** tab.
32. Specify a name (Ex. SQLListener) and ensure that the port is **1433** and then click **Next**.
33. In the **Select Initial Data Synchronization** page of the wizard, choose the **Full** option and specify network location accessible by all the SQL servers and then click **Next**.
34. Finally, click **Finish** and the process will complete.

Decommission Windows Server 2012 R2 nodes

The following sections provide guidance on operational tasks you may need to remove your Windows Server 2012 R2 servers after successfully upgrading the AD RMS cluster to Windows Server 2016.

Removing a Windows Server 2012 R2 AD RMS Server

You can remove unnecessary AD RMS servers after an upgrade. You may choose to perform this action when it becomes needed to decommission AD RMS servers.

To remove a Windows Server 2012 R2 AD RMS server

1. On the Windows Server 2012 R2 AD RMS server in Server Manager, select **Manage** from the top right menus and then choose **Remove Roles and Features**.

2. The **Remove Roles and Features Wizard** will open up and on the **Before you Begin** screen, click **Next**.
3. On the **Server Selection** Screen, click **Next**.
4. On the **Server Roles** screen, remove the check next to **Active Directory Rights Management Services** and click **Next**.
5. On the **Features** Screen, click **Next**.
6. On the **Confirmation** Screen, click **Remove**.
7. Once this completes, restart the server.
8. You can now shut down this server and reallocate the resources as needed.