Active Directory Rights Management Services

Integration Guide

gemalto
security to be free

Document Part Number: 007-011230-001, Rev. J

Release Date: August 2016

Contents

Preface

This guide provides instructions for setting up a small test lab with Microsoft AD RMS running with SafeNet Luna HSM for securing the rights management keys.

Scope

This document describes how to install and configure Microsoft AD RMS with SafeNet Luna HSM. Refer to the SafeNet Luna HSM documentation for general SafeNet Luna HSM setup procedures.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: Command-line commands and options (Type **dir /p**.) Button names (Click **Save As**.) Check box and radio button names (Select the **Print Duplex** check box.) Window titles (On the **Protect Document** window, click **Yes**.) Field names (**User Name:** Enter the name of the user.) Menu names (On the **File** menu, click **Save**.) (Click **Menu** > **Go To** > **Folders**.) User input (In the **Date** box, type **April 1**.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

If you encounter a problem while installing, registering or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

Overview

This document outlines the steps to configure and integrate Active Directory Rights Management Services with SafeNet Luna HSM.

Active Directory Rights Management Services (AD RMS) is an information protection technology that works with AD RMS-enabled applications to help safeguard digital information from unauthorized use. Content owners can define who can open, modify, print, forward, or take other actions with the information. A single HSM (SafeNet Luna HSM) is deployed to provide a security framework to the data in use, data at rest, and the data in transit.

Microsoft Office 2007/2010 Enterprise Edition uses Microsoft Active Directory Rights Management Services to implement document security utilizing Luna Cryptographic Service Provider (CSP) to store the AD RMS cluster keys on SafeNet Luna HSM.

SafeNet Luna HSM secures the AD RMS Cluster Key generated and used by the AD RMS. You can integrate the AD RMS with the Luna SA by using the MSCAPI interface. The benefits of using SafeNet Luna HSM with the AD RMS are:

- Secure storage of the AD RMS Cluster Key
- FIPS 140-2 level 3 validated hardware
- Full life cycle management of the keys
- Failover support
- Load balancing

Scope

3rd Party Application Details

- Microsoft Active Directory Rights Management Services

Supported Platforms

Active Directory Rights Management Services Integration with SafeNet Luna HSM has been tested with the following:

Platforms Tested	Luna Client Software Version	SafeNet Luna HSM Appliance Software Version	Appliance Firmware Version
Widows Server 2012 R2 Standard	6.2.1	6.2.1	6.10.9
Widows Server 2012 R2 Standard	6.2.0	6.2.0	6.10.9
Widows Server 2012 Standard	5.3.0 5.2.1	Luna SA v5.3.0 Luna SA v5.2.1	6.20.0 6.10.1
Windows Server 2008 R2	5.1 5.0 4.4.3	Luna SA v5.1.0 Luna SA v5.0.0 Luna SA v4.4.3	6.2.1 6.0.8 4.8.1

Prerequisites

SafeNet Network HSM Setup

Refer to the SafeNet Network HSM documentation for installation steps and details regarding configuring and setting up the box on Windows systems. Before you get started, ensure the following:

1. SafeNet Network HSM appliance and a secure admin password
2. SafeNet Network HSM, and a hostname, suitable for your network
3. SafeNet Network HSM network parameters are set to work with your network
4. Initialize SafeNet Network HSM.
5. Create and exchange certificates between SafeNet Network HSM and Client system.
6. Create a partition on SafeNet Network HSM. Remember the partition password that will be later used by Microsoft ADRMS.
7. Register the client with the partition. Run the "vtl verify" command on the client system to display a registered partition. The general form of command for Windows is

   ```
   C:\Program Files\SafeNet\LunaClient>vtl verify.
   ```

8. Enabled Partition "Activation" and "Auto Activation" (Partition policy settings 22 and 23 (applies to Luna SA with Trusted Path Authentication [which is FIPS 140-2 level 3] only).

2

Integrating Microsoft AD RMS with SafeNet Luna HSM (Windows Server 2008 R2)

This chapter outlines the steps to install and integrate Active Directory Rights Management Services with SafeNet Luna HSM.

Before You Begin

It is recommended that you should familiarize yourself with Microsoft Active Directory Rights Management Services and the setup process for the AD RMS. Refer to the appropriate help files provided by Microsoft for more information and pre-installation requirements.

Set up

Requirements to setup the ADRMS is given below.

1. The setup comprises the following systems in a private network as per the table below:

Operating System	Applications and Services	Description	Computer Name
Windows Server 2008 R2 Enterprise	Active Directory, Domain Name System (DNS)	Domain Controller	ADRMS-DC
Windows Server® 2008 R2 Enterprise	AD RMS, Internet Information Services (IIS) 7.0, and Message Queuing	AD RMS Server	ADRMS-SRV
Windows Vista®	Microsoft Office Word 2007 Enterprise Edition or Microsoft Office Word 2010 Enterprise Edition	AD RMS Client	ADRMS-CLNT

2. Configure the domain controller on ADRMS-DC.
3. Configure the AD RMS root cluster computer on ADRMS-SRV.
4. Configure the AD RMS client computer on ADRMS-CLNT.

Configure user accounts and groups

Create following user accounts and groups in the LUNARMS domain.

First, add the user accounts shown in the following table to Active Directory or AD DS. Use the procedure following the table to create the user accounts.

Account Name	User Logon Name	E-mail Address	Group
ADRMSADMIN	ADRMSADMIN	-	Enterprise Admins
ADRMSSRVC	ADRMSSRVC	-	
Nicole Holliday	NHOLLIDA	nhollida@lunarms.com	Employees, Finance
Limor Henig	LHENIG	lhenig@lunarms.com	Employees, Marketing
Stuart Railson	SRAILSON	srailson@lunarms.com	Employees, Engineering

Once the user accounts have been created, Active Directory Universal groups should be created and these users added to them. The following table lists the Universal groups that should be added to Active Directory. Use the procedure following the table to create the Universal groups.

Group Name	E-mail address
Finance	finance@lunarms.com
Marketing	marketing@lunarms.com
Engineering	engineering@lunarms.com
Employees	employees@lunarms.com

Finally, create a shared folder on ADRMS-SRV so that other users can find documents saved to the network. To create a shared network folder that can be modified by CP&L employees.

1. Click **Start**, click **My Computer**, and then double-click **Local Disk (C :)**.
2. Click **File**, point to **New**, and then click **Folder**.
3. Type **Public** for the new folder, and then press **ENTER**.
4. Right-click **Public** and then click **Sharing and Security**.
5. On the **Sharing** tab click the **Share this folder** option, and ensure that **Public** is in the **Share name** box.
6. Click **Permissions**.
7. In the **Group or user name** box click **Everyone**.
8. Select the **Full Control** check box in the **Allow** column of the Permissions for **Everyone** box.
9. Click **OK**.
10. Click the **Security** tab, and then click Users **(ADRMS-SRV\Users)** in the **Group or user name** box.

11. In the **Permissions for Users** box select the **Full Control** check box in the **Allow** column.
12. Click **OK**.

Configure AD RMS client computer (ADRMS-CLNT)

To configure ADRMS-CLNT, install Windows Vista operating system, configure TCP/IP properties, and then join ADRMS-CLNT to the domain **lunarms.com**. AD RMS-enabled application also needs to be installed. In this example, Microsoft Office Word 2007/2010 Enterprise Edition is installed on ADRMS-CLNT.

To install Microsoft Office Word 2007/2010 Enterprise

1. Log on to **ADRMS-CLNT** with the **LUNARMS\Administrator** account or another user account in the local Administrators group.
2. Double-click **setup.exe** from the Microsoft Office 2007/2010 Enterprise product disc.
3. Click **Customize** as the installation type, set the installation type to **Not Available** for all applications except Microsoft Office Word 2007 Enterprise, and then click **Install Now**. This might take several minutes to complete.

Install Luna Cryptographic Service Provider (CSP) on ADRMS-SRV

For Luna Client 4.4.1 & 5.1:

- Run the command, *register.exe* to register Luna CSP. The general form of command is

  ```
  C:\Program Files\LunaSA\CSP>Register.exe
  ```

  Follow the instruction to register the Luna SA partition and provide the partition password when it prompts for password.
- To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is

  ```
  C:\Program Files\LunaSA\CSP>Register.exe /l
  ```

For Luna Client v5.0:

- Run the command, *registerCSP64.exe* to register Luna CSP. The general form of command is

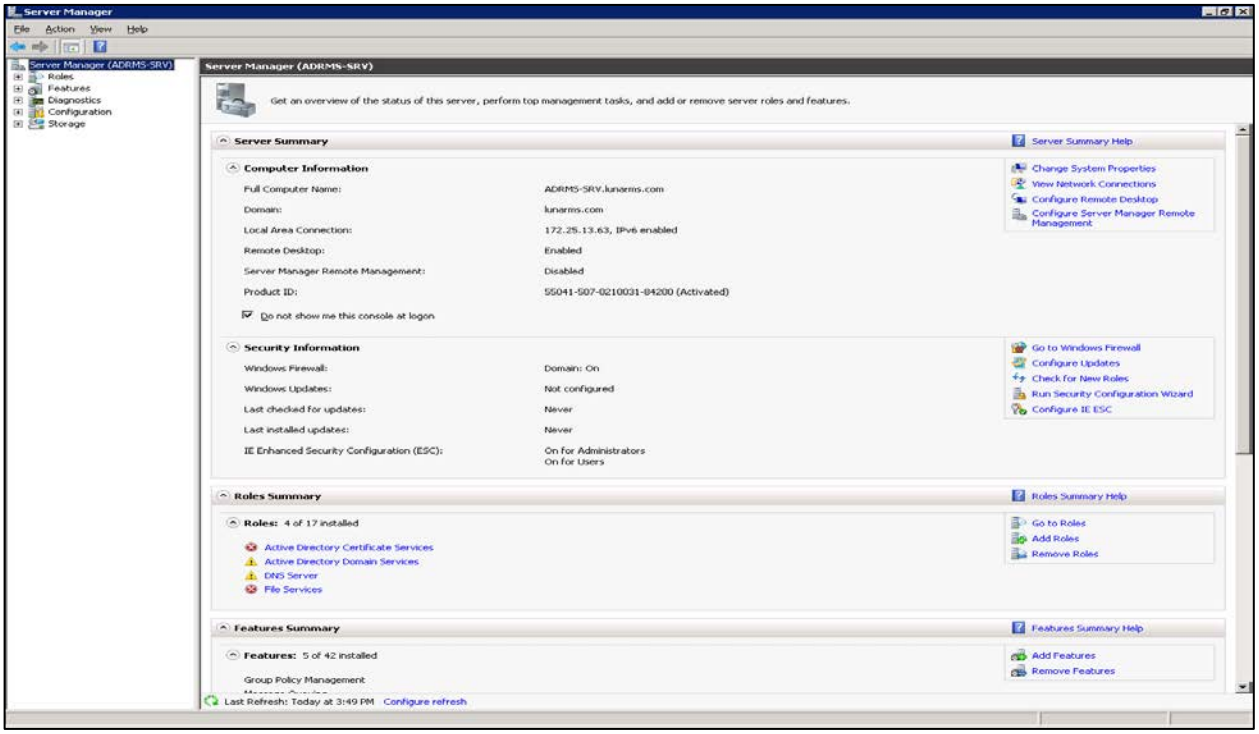
  ```
  C:\Program Files\LunaSA\CSP>RegisterCSP64.exe
  ```
- To list the Luna Cryptographic Services for Microsoft Windows. The general form of command is

  ```
  C:\Program Files\LunaSA\CSP>RegisterCSP64.exe /l
  ```

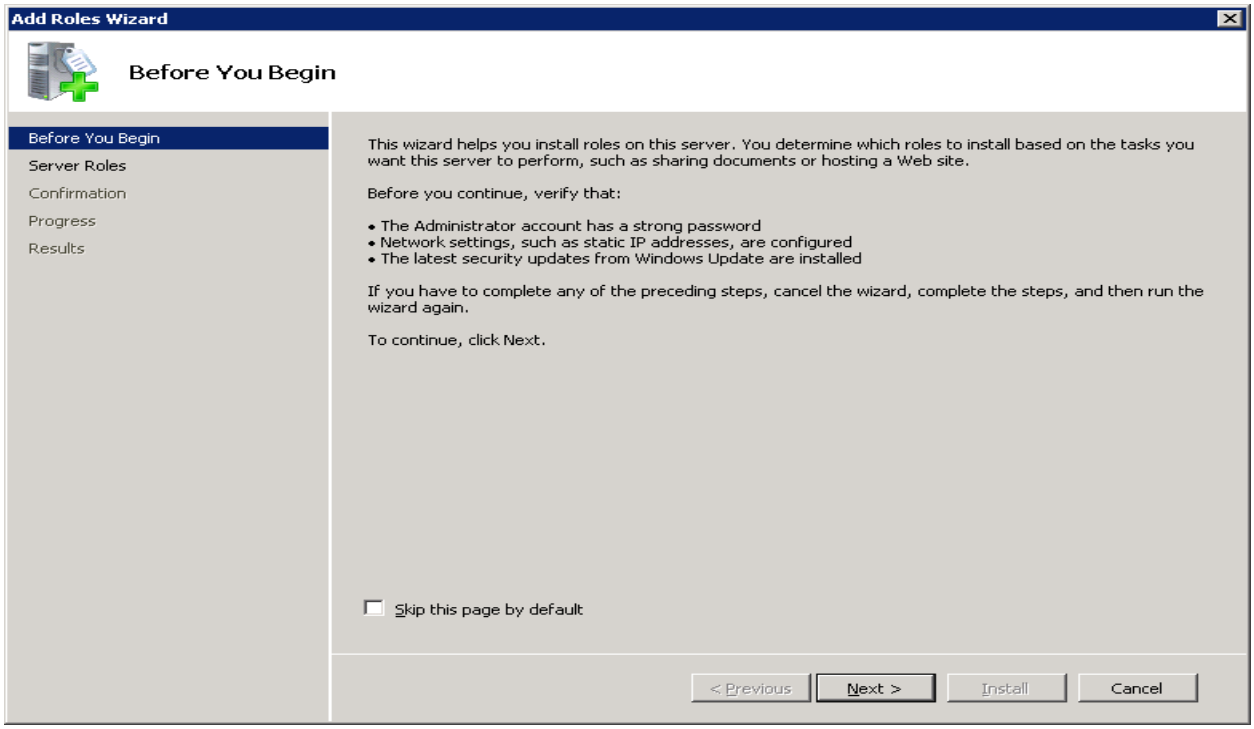
Install AD RMS with Luna Cryptographic Service Provider (CSP) on Windows Server 2008 R2

To install the Microsoft Active Directory Rights Management Services:

1. Login to ADRMS-SRV as lunarms\adrmsadmin.
2. Click **Start**, point to **Administrative tools**, and then click **Server Manager**. The Server Manager snap-in displays.
3. Select **Roles** in the console tree.

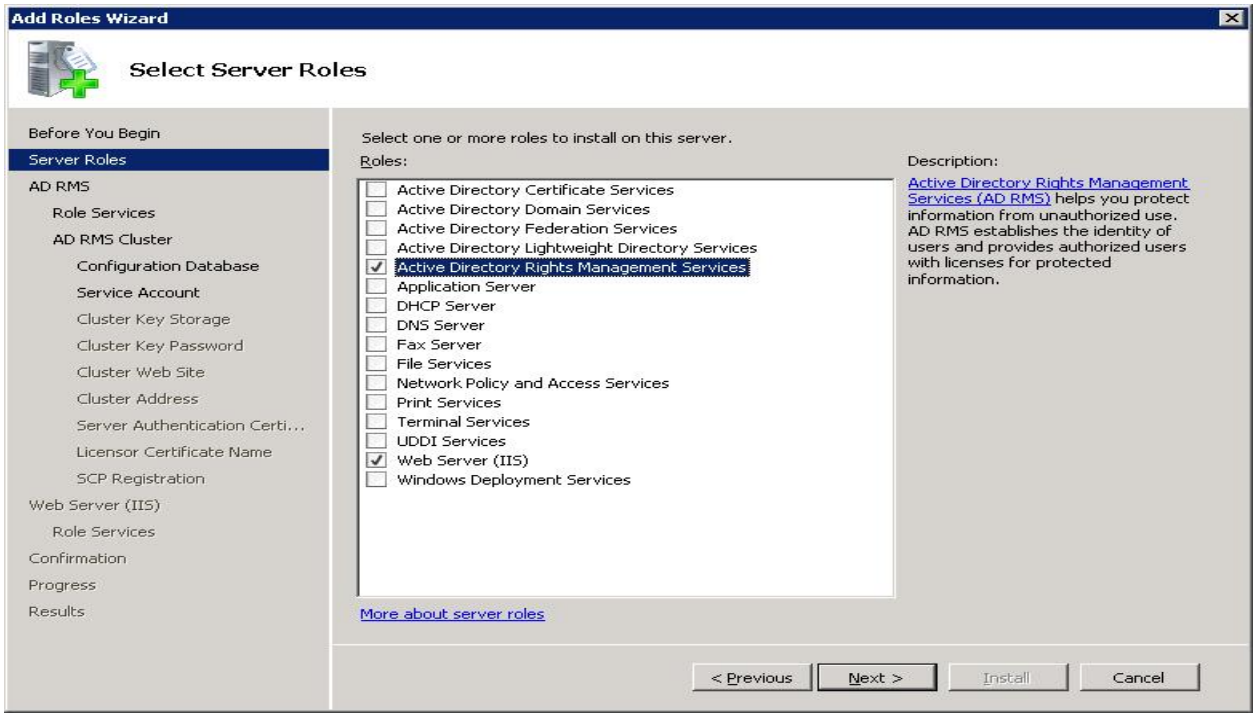


4. Right-click **Roles** and then click, **Add roles**. The **Add Roles** wizard displays.



5. Click **Next**.

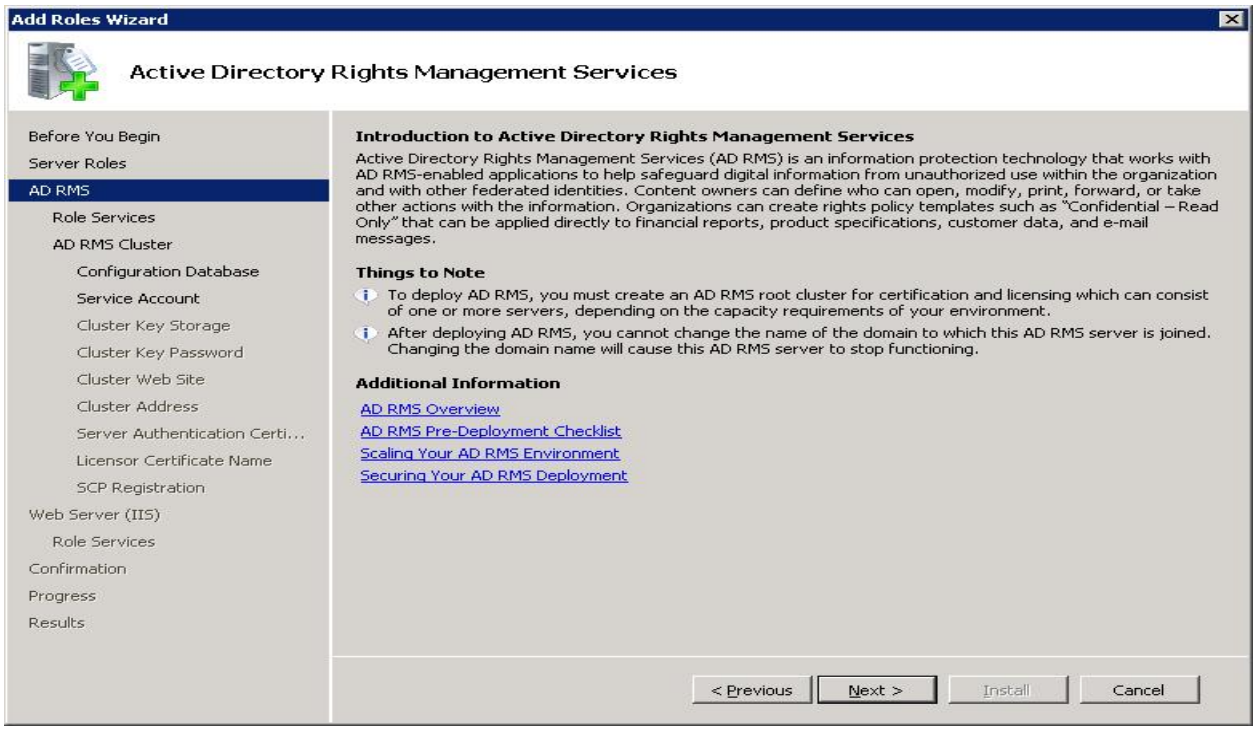
6. Select the **Active Directory Rights Management Services** check box from **Server Roles** to install on this server. You receive a warning stating **Add roles services and features required for Active Directory Rights Management Services**.



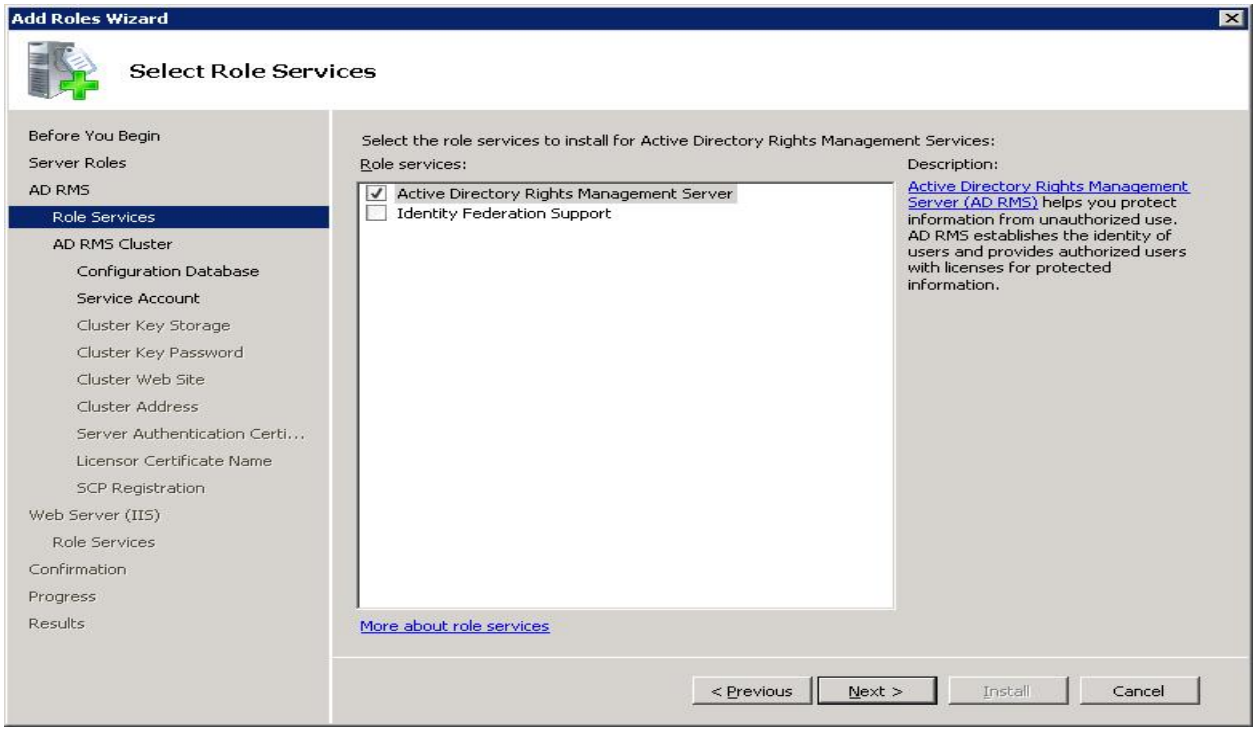
7. Click **Add Required Role Services**.

8. Click **Next** to continue.

9. Click **Next** on the Active Directory Rights Management Services window.

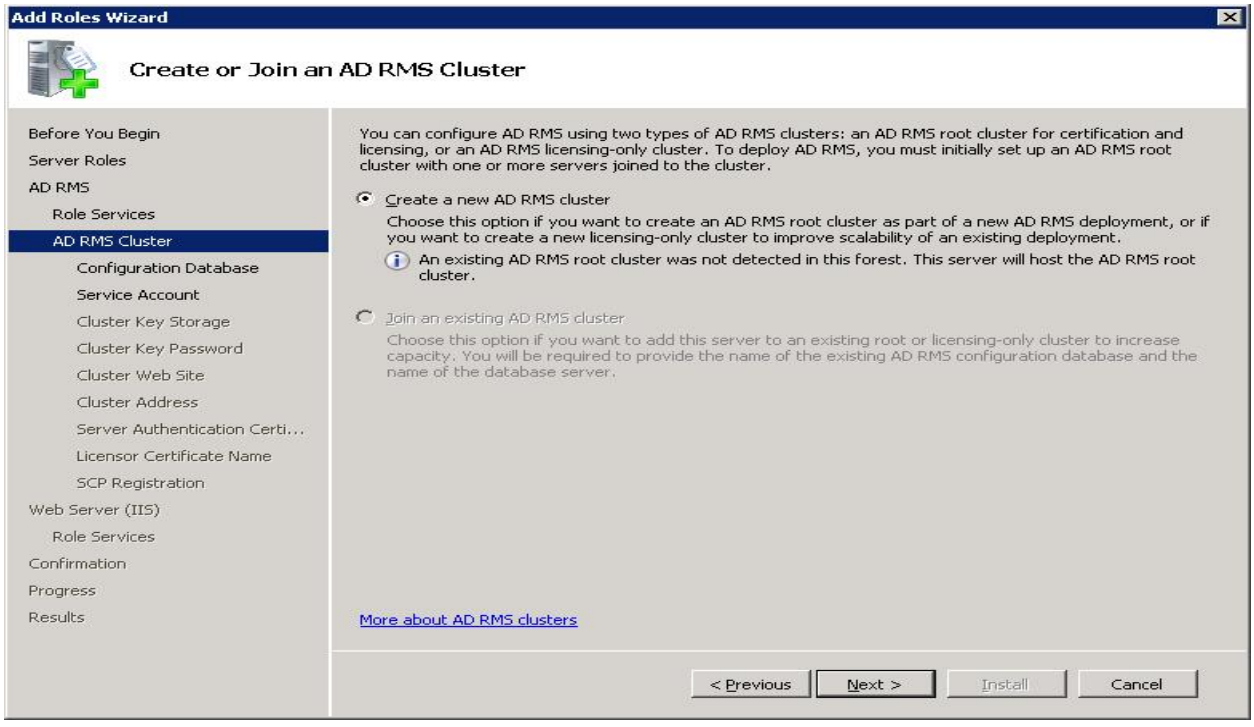


10. Select the **Active Directory Rights Management Server** check box from the **Role Services**.



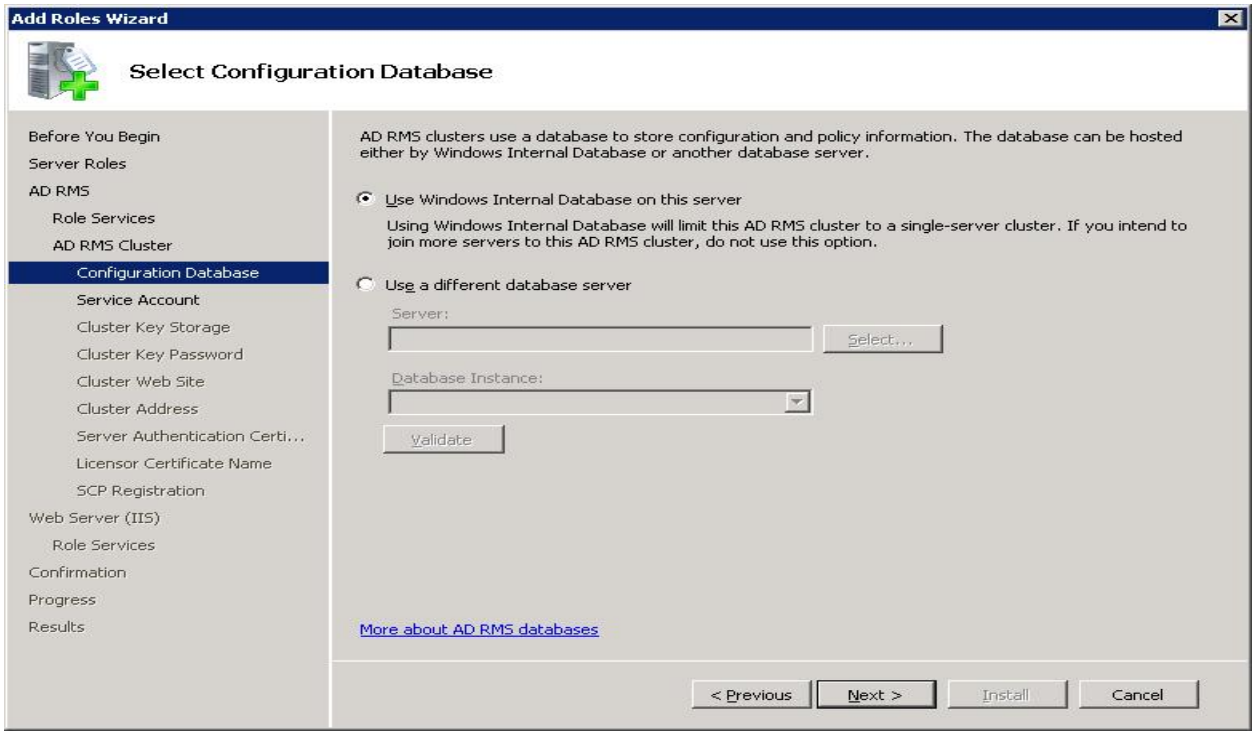
11. Click **Next** to continue.

12. Select the **Create a new AD RMS cluster** radio button.

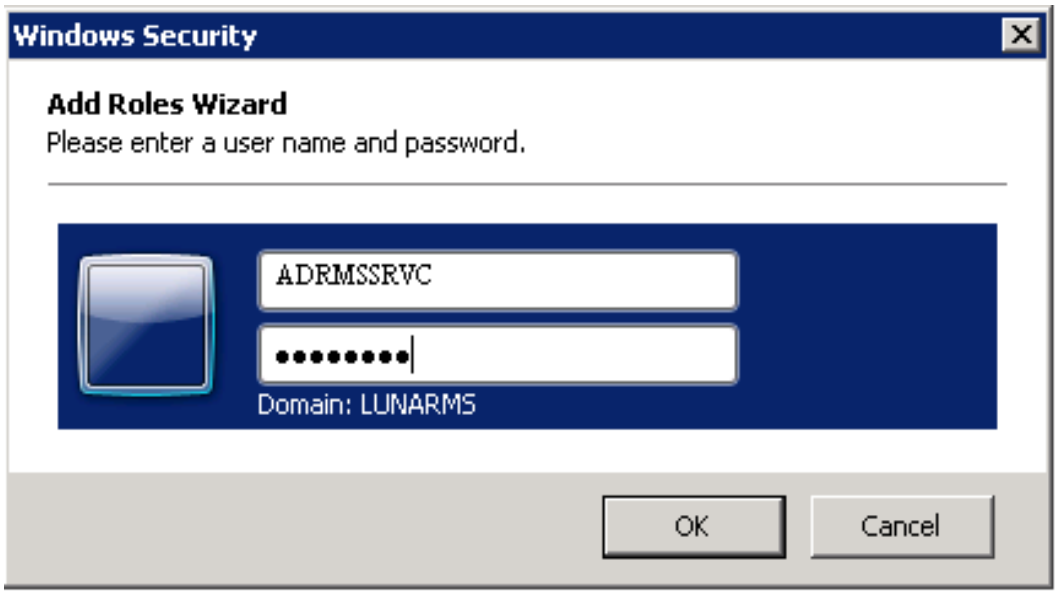


13. Click **Next** to continue.

14. Select the **Use Windows Internal Database on this Server** radio button.

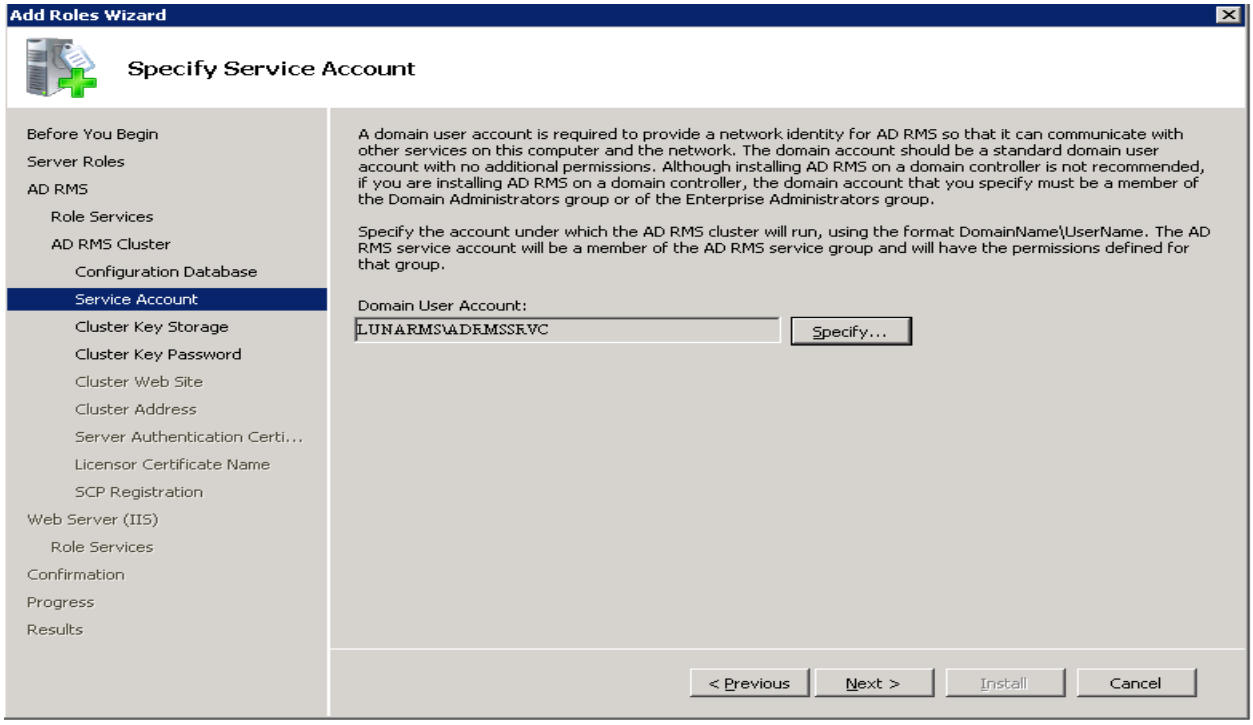


15. Click **Next** to continue.
16. Specify the **Domain User Account**.

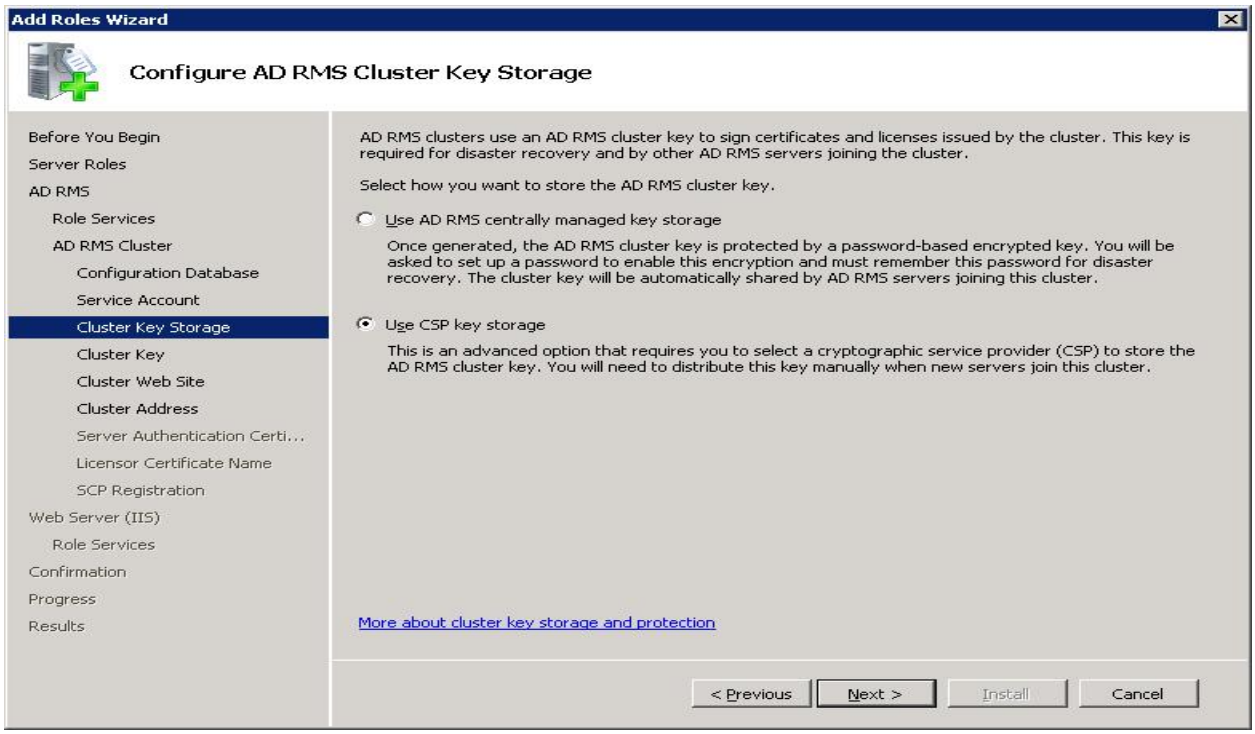


17. Click **OK** to continue.

18. Click **Next** to continue.

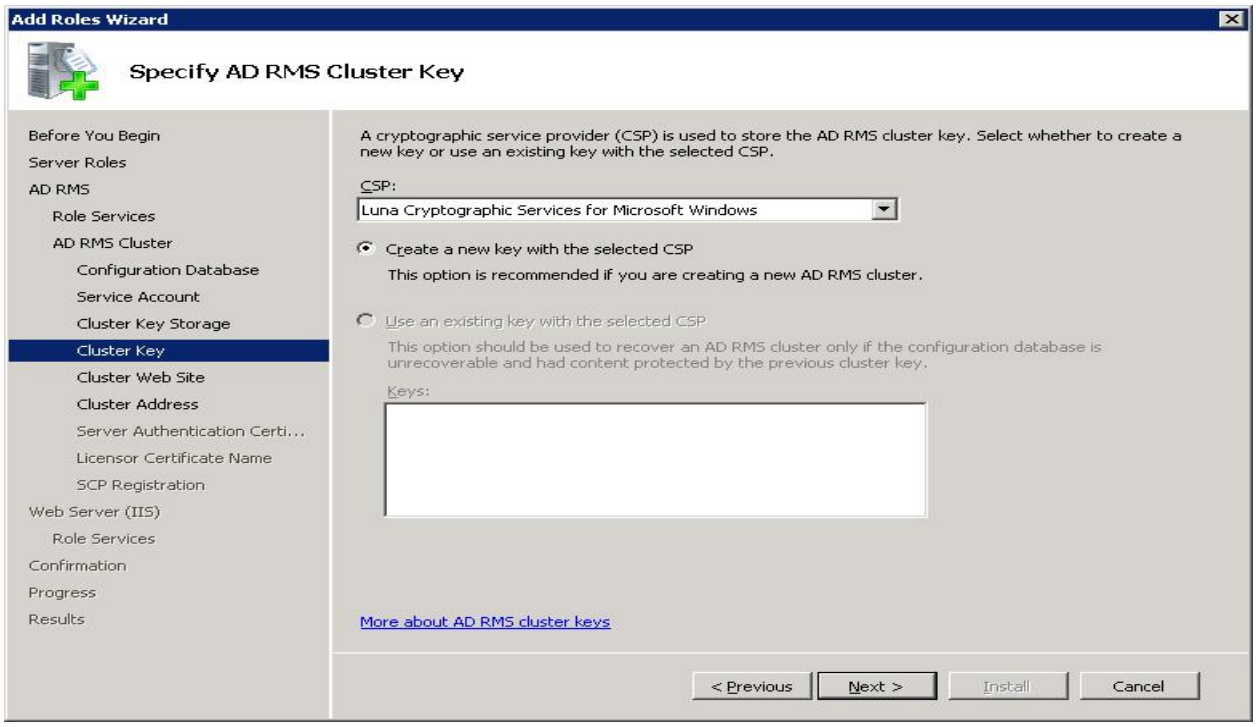


19. Select the **Use CSP key storage** radio button for AD RMS cluster key storage.



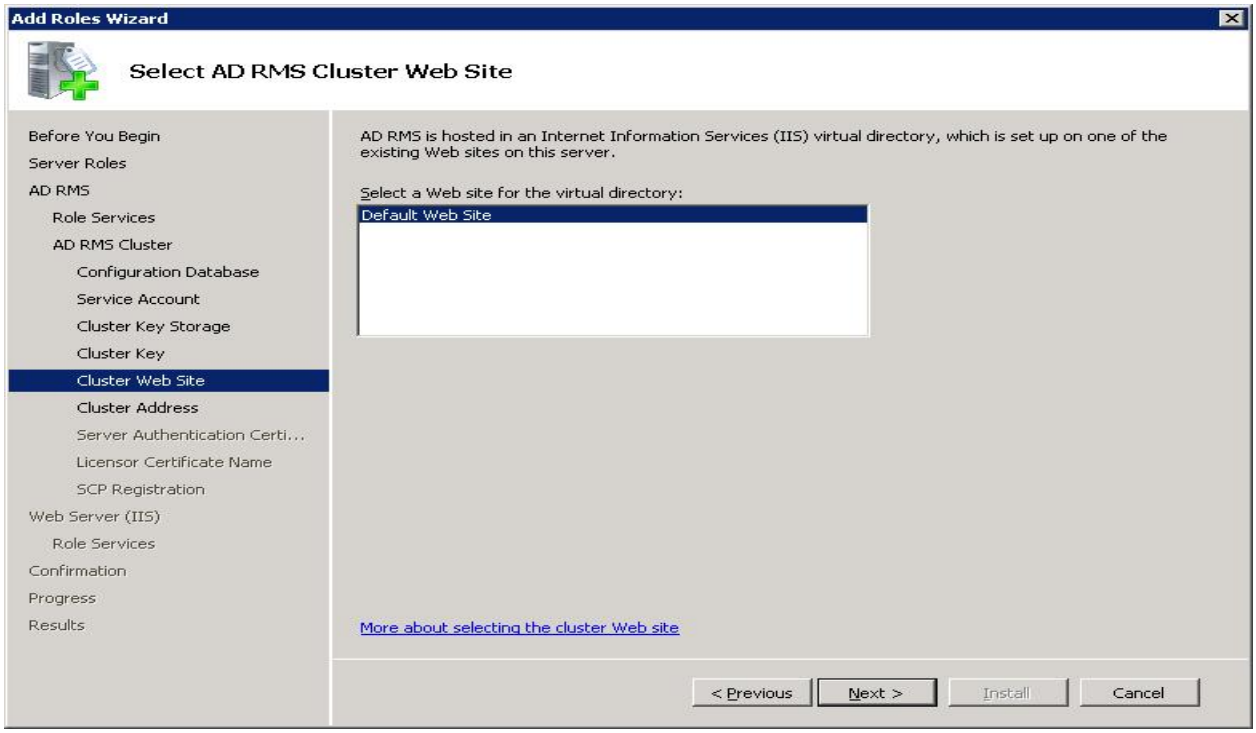
20. Click **Next** to continue.

21. Choose **Luna Cryptographic Services for Microsoft Windows** from the **CSP** drop-down menu to store the AD RMS cluster key and select the **Create a new key with the selected CSP** radio button.



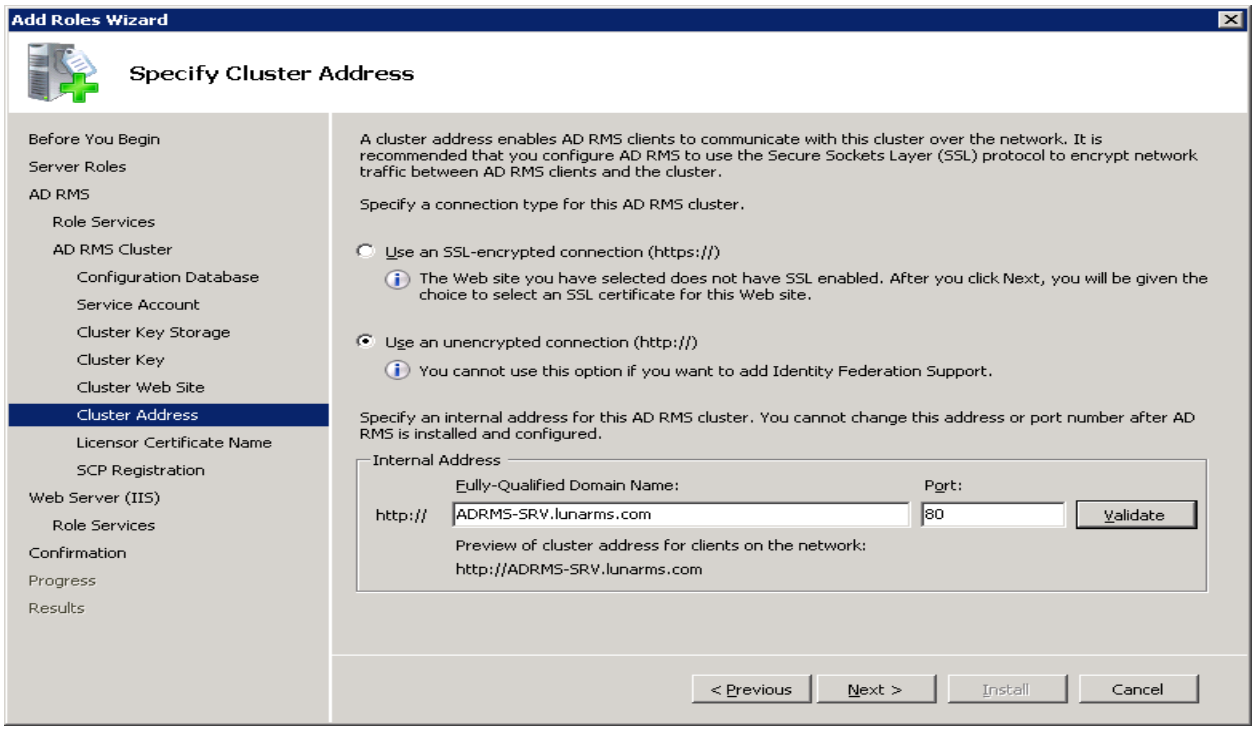
22. Click **Next** to continue.

23. Select **Default Web Site** for the virtual directory.



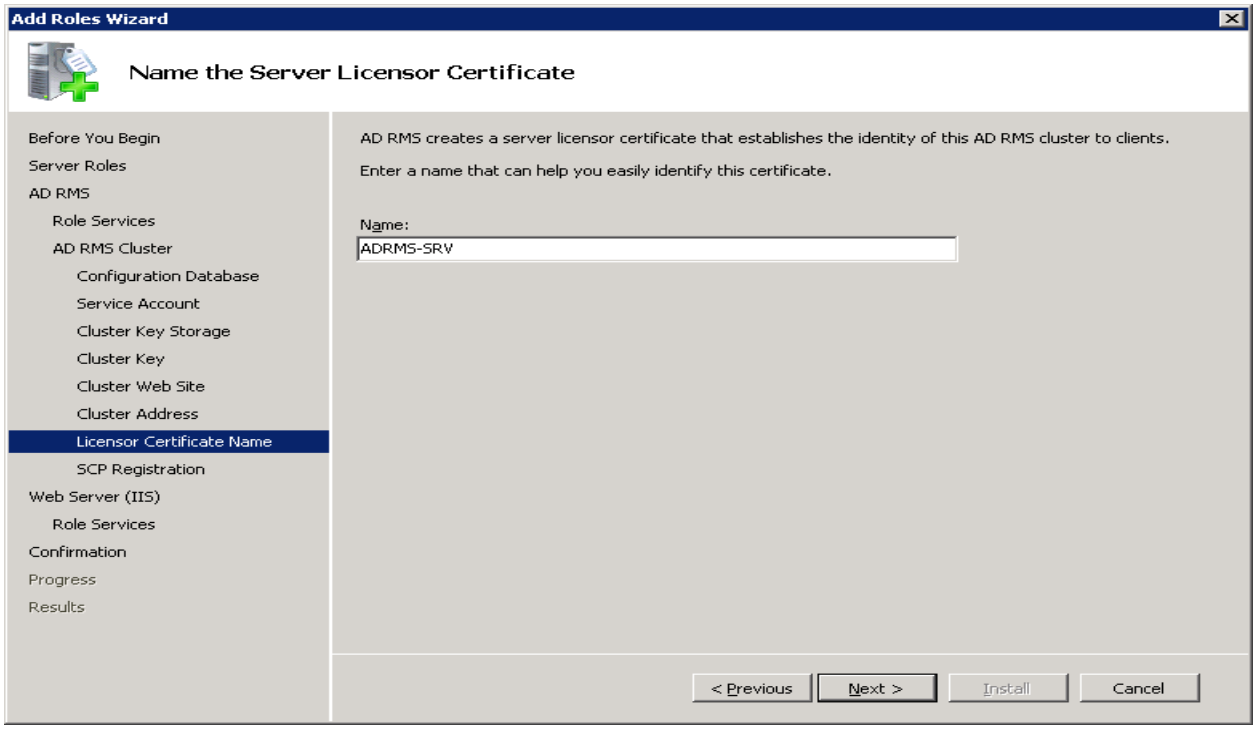
24. Click **Next** to continue.

25. Select **Use an unencrypted connection (http://)** for the connection type for the AD RMS cluster. Give the FQDN then click **Validate**.



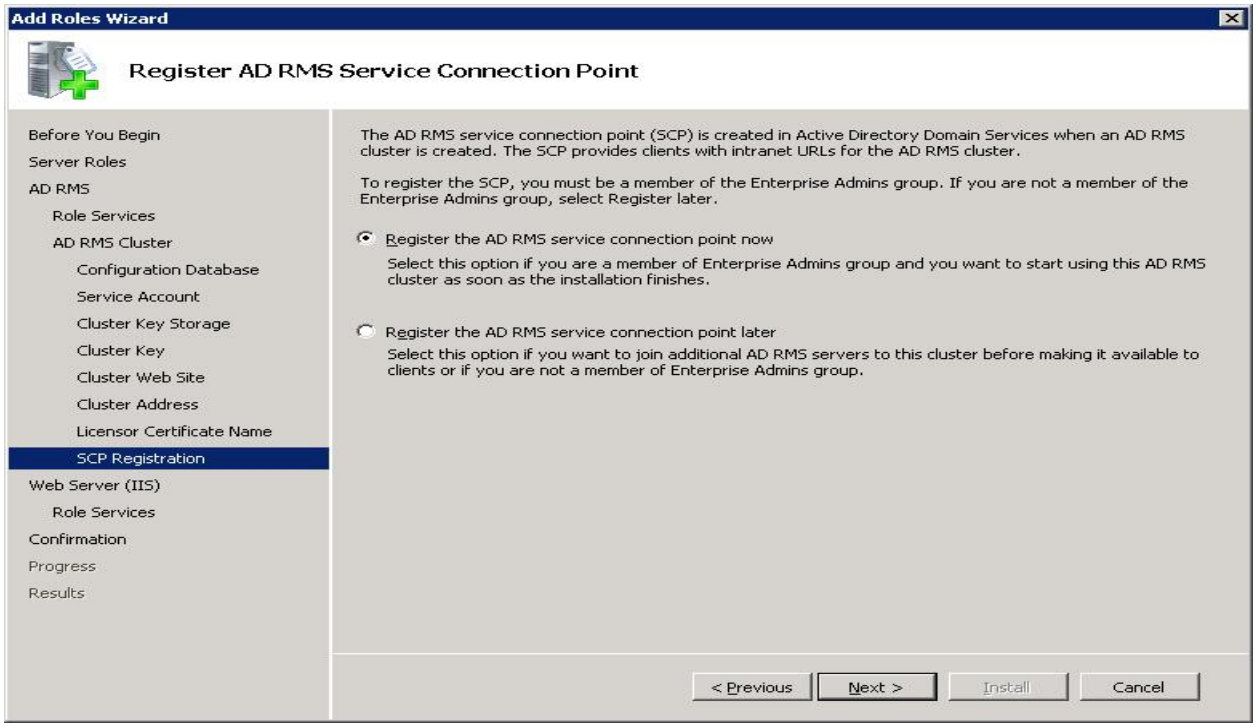
26. Click **Next** to continue.

27. Enter a name for the server licensor certificate.

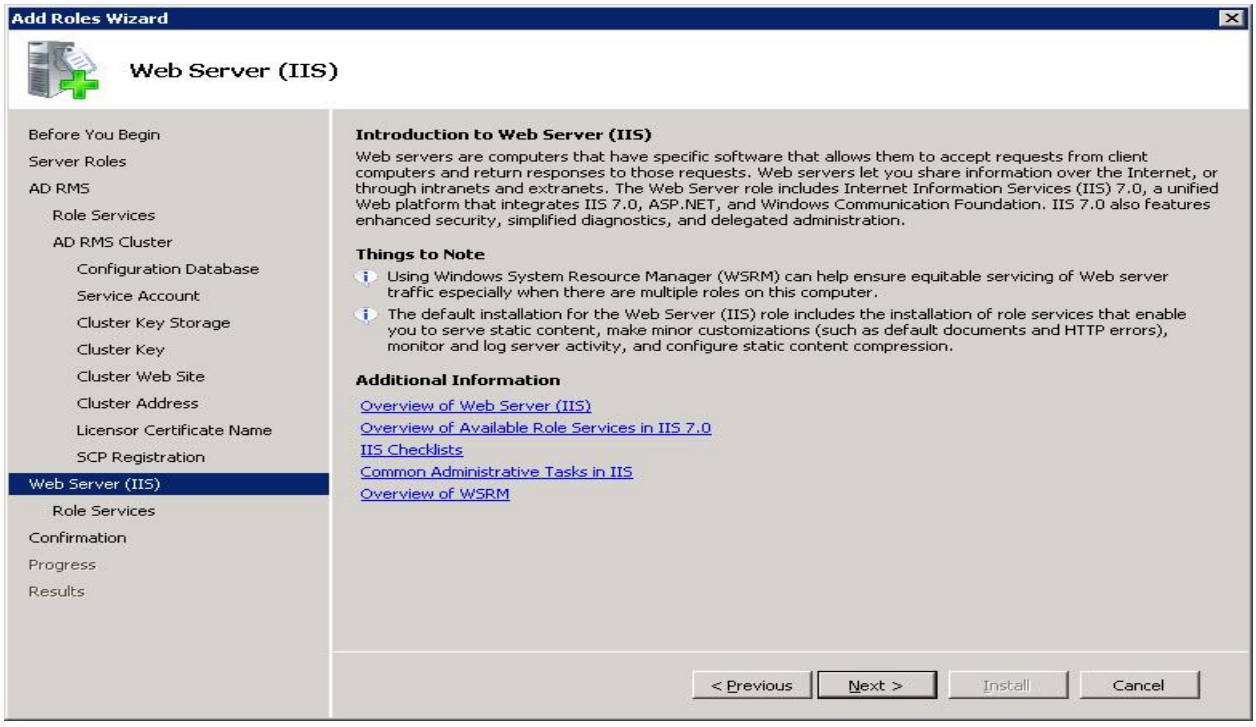


28. Click **Next** to continue.

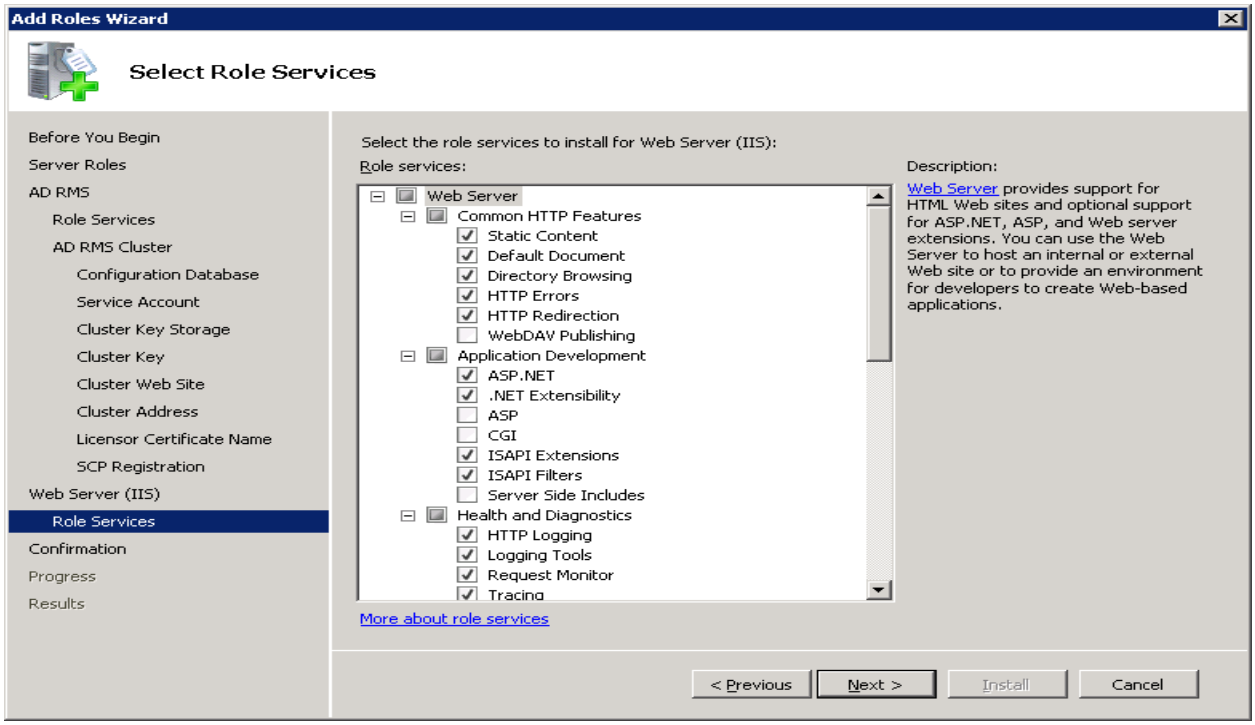
29. Ensure that the **Register the AD RMS service connection point now** radio button is selected, and then click **Next** to register the AD RMS service connection point (SCP) in Active Directory during installation.



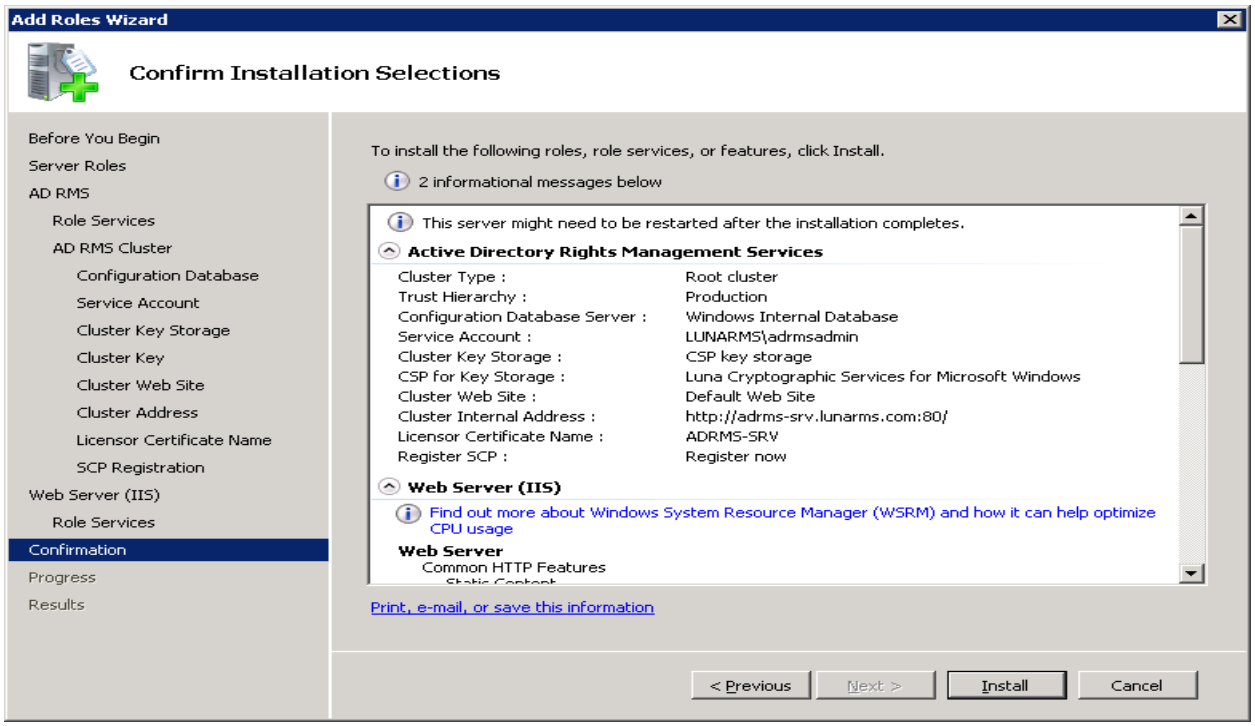
30. Click **Next** on the Web Server (IIS) page.



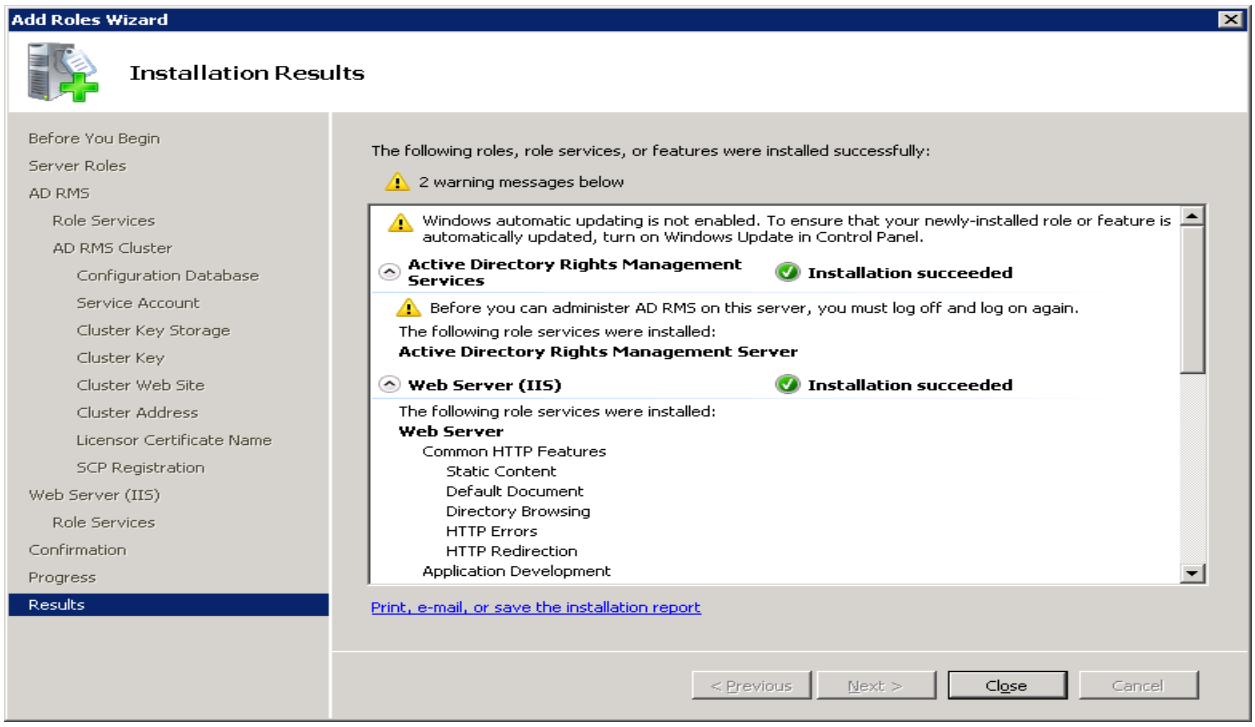
31. Click **Next** on the Select Role Services page.



32. Click **Install** on the Confirm Installation Selections page.

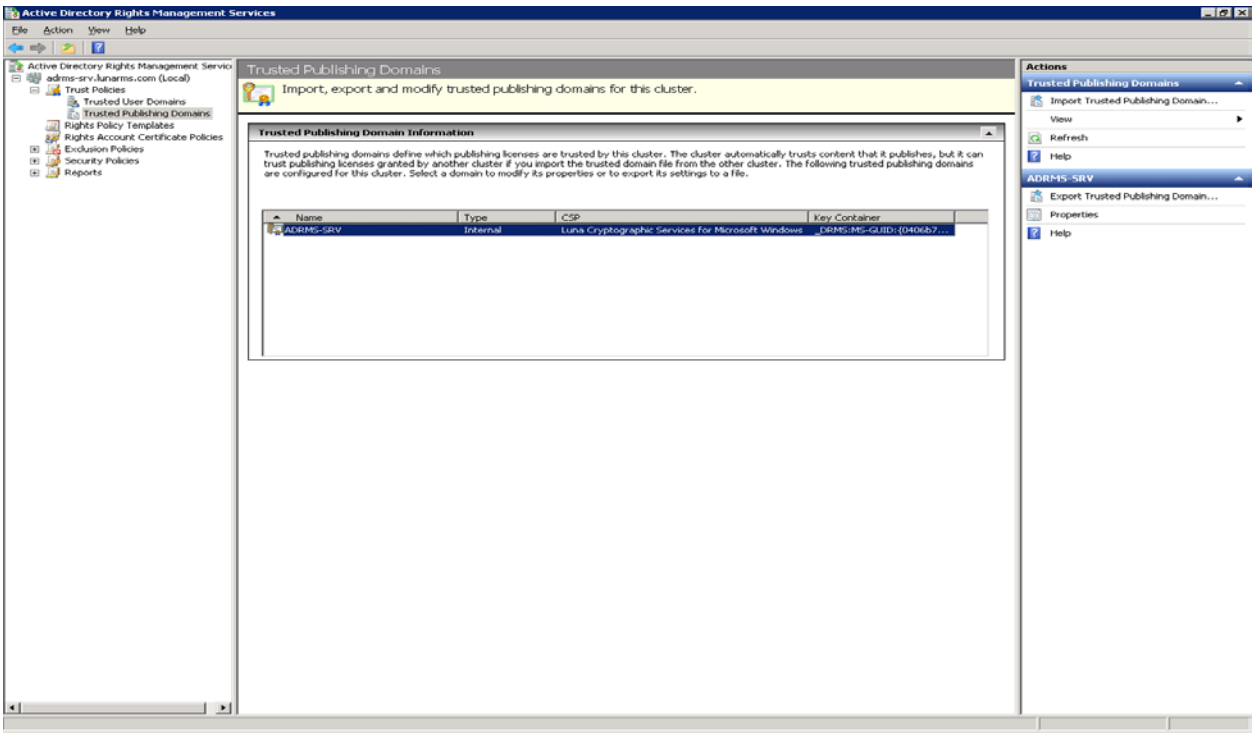


33. Click **Close** to exit the **Add Roles Wizard** after viewing the installation results. AD RMS root cluster keys will be generated and stored on SafeNet Luna HSM.

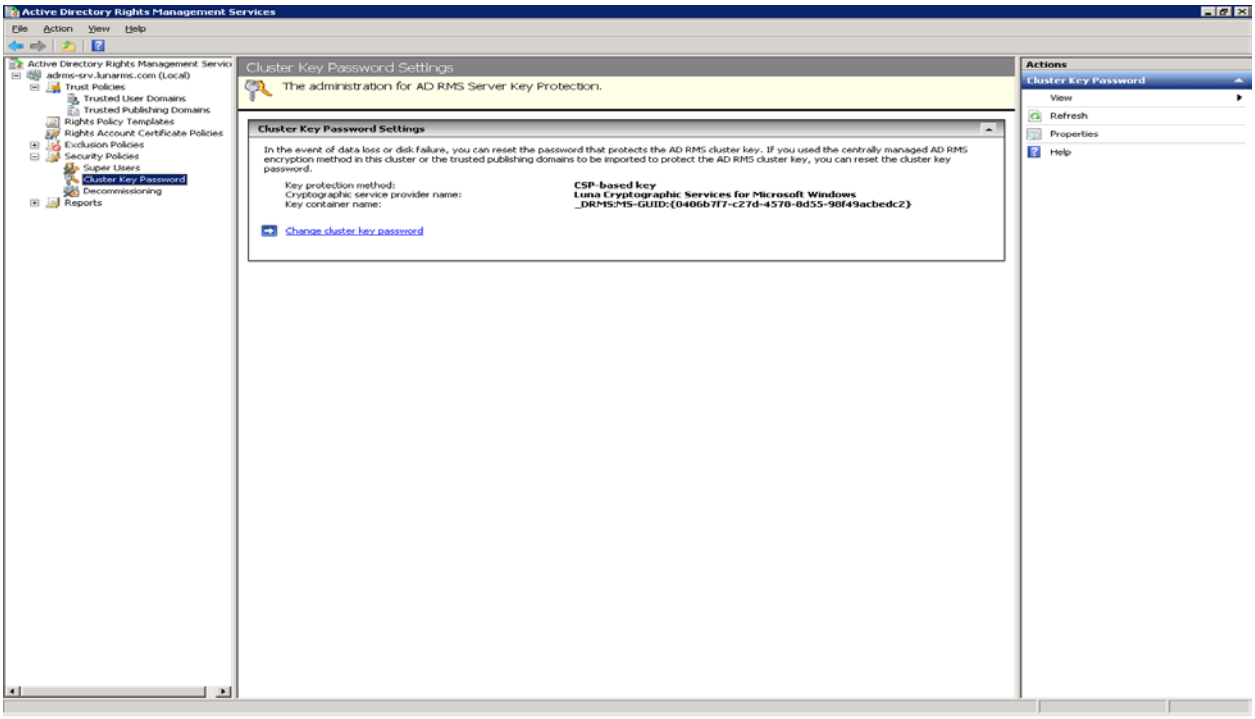


34. After restarting the system, login as **lunarms\adrmsadmin** and open the Active Directory Rights Management Services console. You will see Luna Cryptographic Services for Microsoft Windows under:

- **Trust Policies** -> **Trusted Publishing Domains**



- **Security Policies –> Cluster Key Password**



3

Integrating Microsoft AD RMS with SafeNet Luna HSM (Windows Server 2012/R2)

This chapter outlines the steps to install and integrate Active Directory Rights Management Services with SafeNet Luna HSM.

Before You Begin

It is recommended that you should familiarize yourself with Microsoft Active Directory Rights Management Services and the setup process for the AD RMS. Refer to the appropriate help files provided by Microsoft for more information and pre-installation requirements.

Setup

1. The setup consists of the following systems in a private network as per the table below:

Operating System	Applications and Services	Description	Computer Name
Windows Server 2012 Standard	Active Directory, Domain Name System (DNS).	Domain Controller	ADRMS-DC
Windows Server 2012 Standard	AD RMS, Internet Information Services (IIS), and Message Queuing	AD RMS Server	ADRMS-SRV
Windows Server 2012 Standard	Microsoft Office Word 2007 Enterprise Edition	AD RMS Client	ADRMS-CLNT

2. Configure the domain controller on **ADRMS-DC.**
3. Configure the AD RMS root cluster computer on **ADRMS-SRV.**
4. Configure the AD RMS client computer on **ADRMS-CLNT.**

Configure user accounts and groups

In this section, you create the user accounts and groups in the HSMSERVER domain.

First, add the user accounts shown in the following table to Active Directory or AD DS. Use the procedure following the table to create the user accounts.

Account Name	User Logon Name	E-mail address	Group
ADRMSADMIN	ADRMSADMIN		Enterprise Admins
ADRMSSRVC	ADRMSSRVC		
Nicole Holliday	NHOLLIDA	nhollida@hsmserver.com	Employees, Finance
Limor Henig	LHENIG	lhenig@hsmserver.com	Employees, Marketing
Stuart Railson	SRAILSON	srailson@hsmserver.com	Employees, Engineering

Once the user accounts have been created, Active Directory Universal groups should be created and these users added to them. The following table lists the Universal groups that should be added to Active Directory. Use the procedure following the table to create the Universal groups.

Group Name	E-mail address
Finance	finance@hsmserver.com
Marketing	marketing@hsmserver.com
Engineering	engineering@hsmserver.com
Employees	employees@hsmserver.com

Finally, create a shared folder on ADRMS-SRV so that other users can find documents saved to the network. To create a shared network folder that can be modified by CP&L employees

1. Click **Start**, click **Computer**, and then double-click **Local Disk (C :).**
2. Click **Home**, and then click **New Folder**.
3. Type **Public** for the new folder, and then press **ENTER**.
4. Click **Share** and then click **Specific people…**.
5. On the **File Sharing** window, type **Everyone** and click **Add**.
6. In the **Permission Level,** click **Everyone** and select **Read\Write**.
7. Click **Share** and verify that Public folder is displayed.
8. Click **Done**.

Configure AD RMS client computer (ADRMS-CLNT)

To configure ADRMS-CLNT, install Windows Server 2012/R2, configure TCP/IP properties, and then join ADRMS-CLNT to the HSMSERVER domain. AD RMS-enabled application also needs to be installed. In this example, Microsoft Office Word 2007/2010 Enterprise Edition is installed on ADRMS-CLNT.

To install Microsoft Office Word 2007/2010 Enterprise

1. Log on to **ADRMS-CLNT** with the **HSMSERVER\Administrator** account or another user account in the local Administrators group.
2. Double-click **setup.exe** from the Microsoft Office 2007/2010 Enterprise product disc.
3. Click **Customize** as the installation type, set the installation type to **Not Available** for all applications except Microsoft Office Word 2007 Enterprise, and then click **Install Now**. This might take several minutes to complete.

Install Luna Cryptographic Service Provider (CSP) on Windows Server 2012/R2

- Open the command prompt, run the *register.exe* to register Luna CSP. The general form of command is

  ```
  C:\Program Files\SafeNet\LunaClient\CSP>register.exe
  ```

  Follow the instruction to register the Luna SA partition and provide the partition password when it prompts for password.

- Run the command to list the CSP libraries. The general form of command is

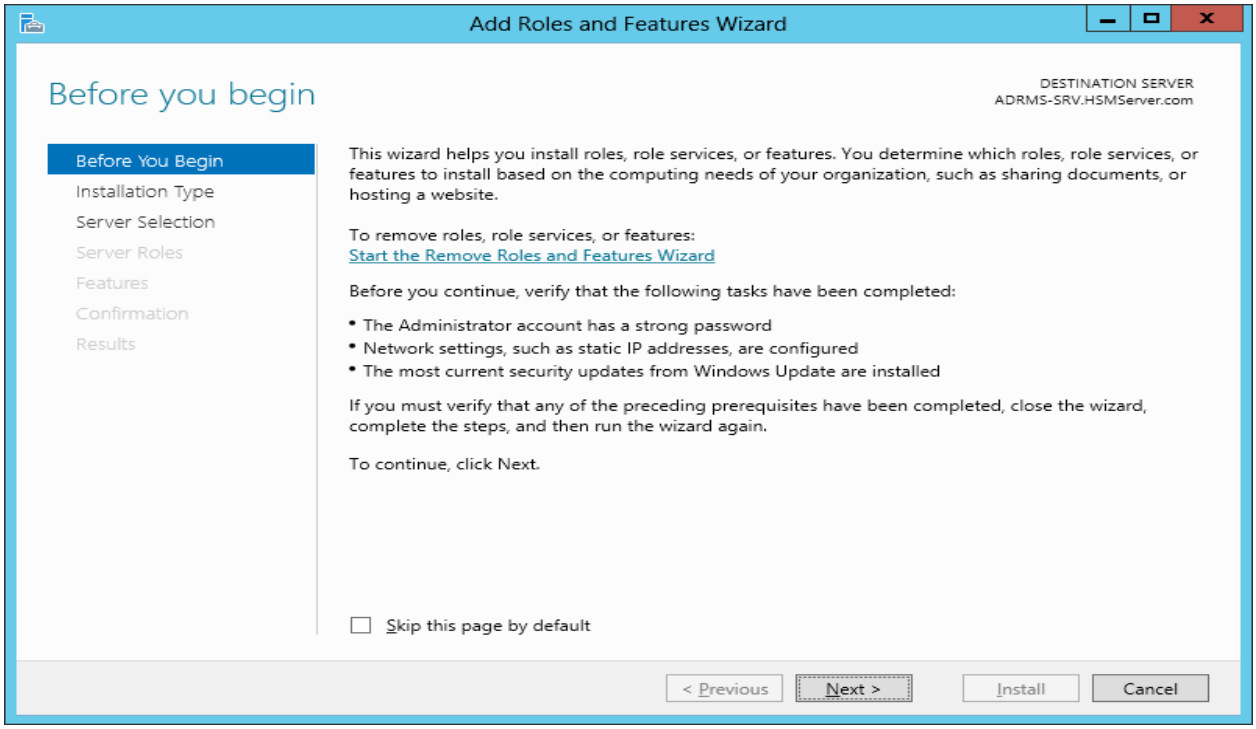
  ```
  C:\Program Files\SafeNet\LunaClient\CSP>register.exe /library
  ```

Install AD RMS with Luna Cryptographic Service Provider (CSP) on Windows Server 2012

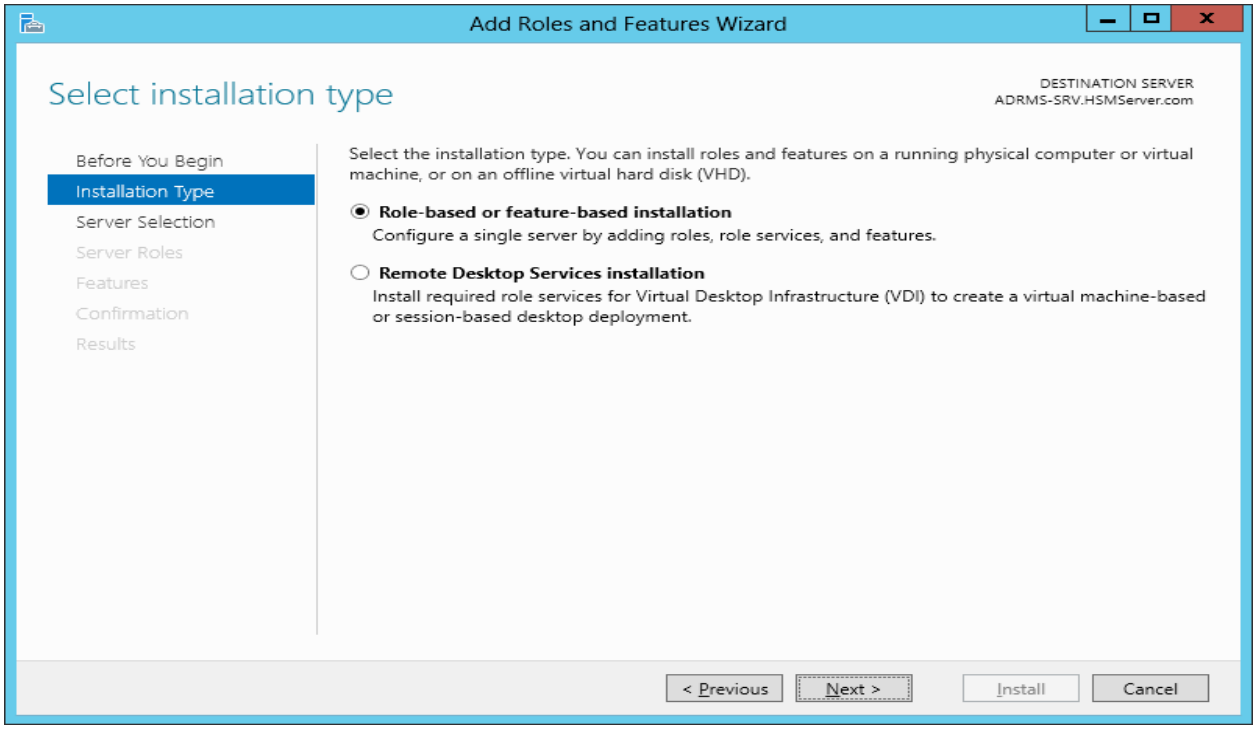
To install the Microsoft Active Directory Rights Management Services:

1. Login to ADRMS-SRV as hsmserver\adrmsadmin.
2. Click **Start**, point to **Administrative Tools**, and then click **Server Manager**. The Server Manager snap-in displays.
3. Click **Add Roles and Features** in the Server Manager Dashboard.

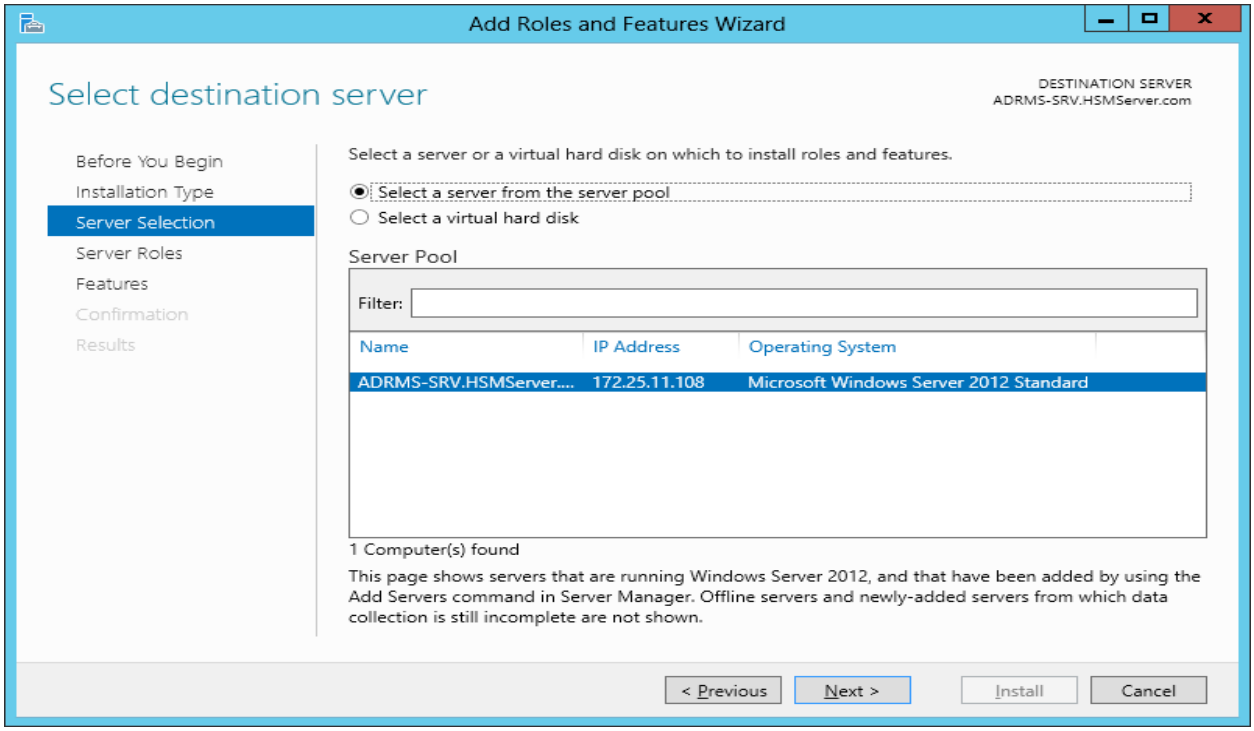
4. Click **Next** on the **Before You Begin** page.



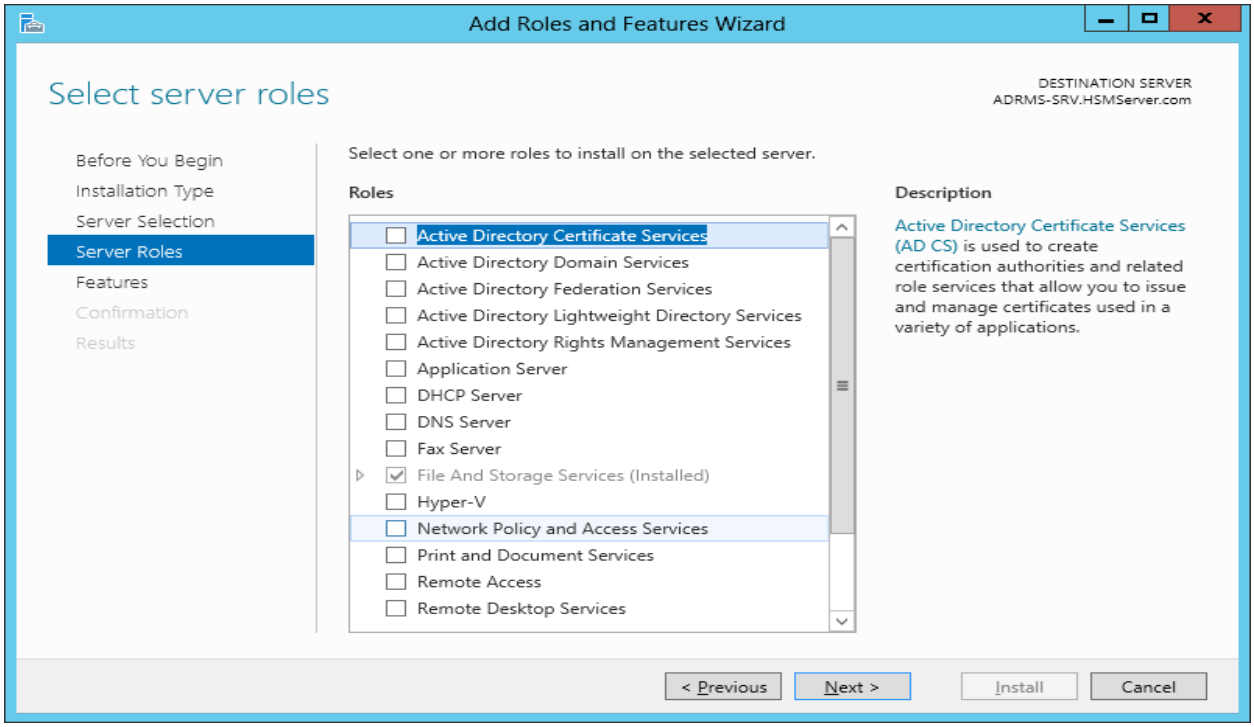
5. Select **Role-based or feature-based installation** and then click **Next** on the Installation Type page.



6. Select the server from the server pool list and click **Next** on the Server Selection page.

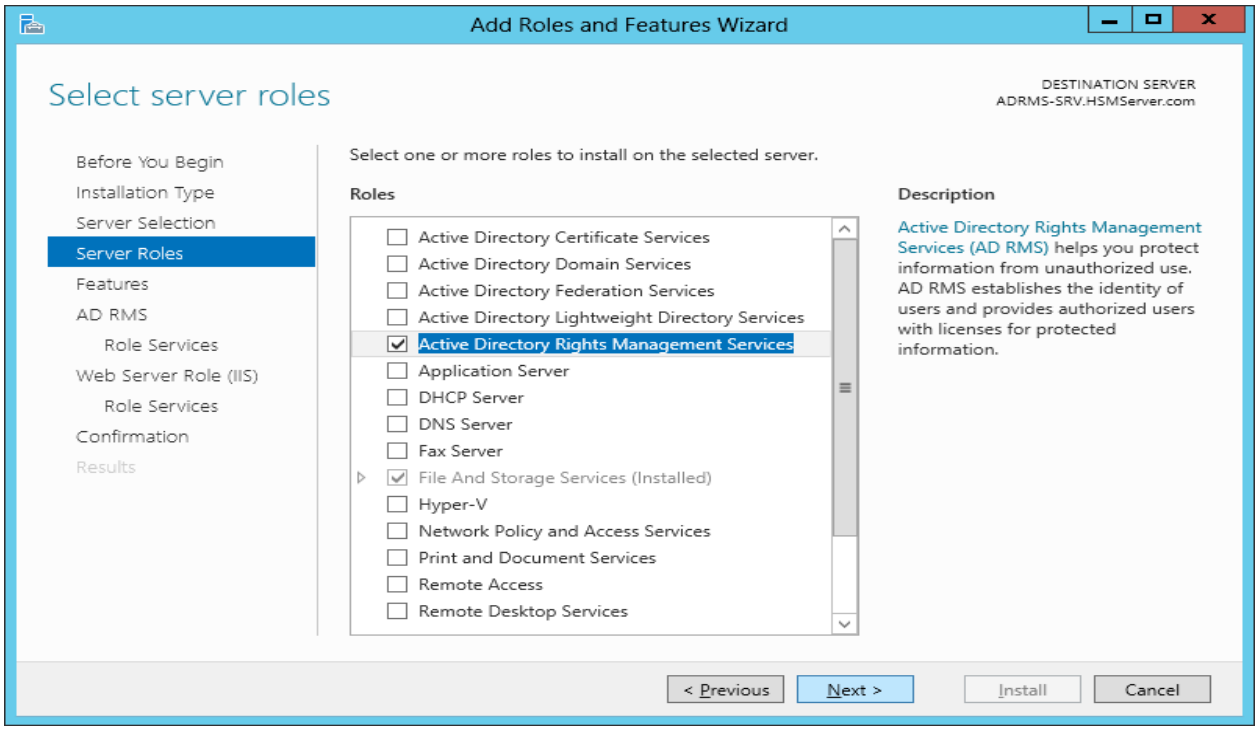


7. Select the **Active Directory Rights Management Services** check box from **Roles** to install on this server.

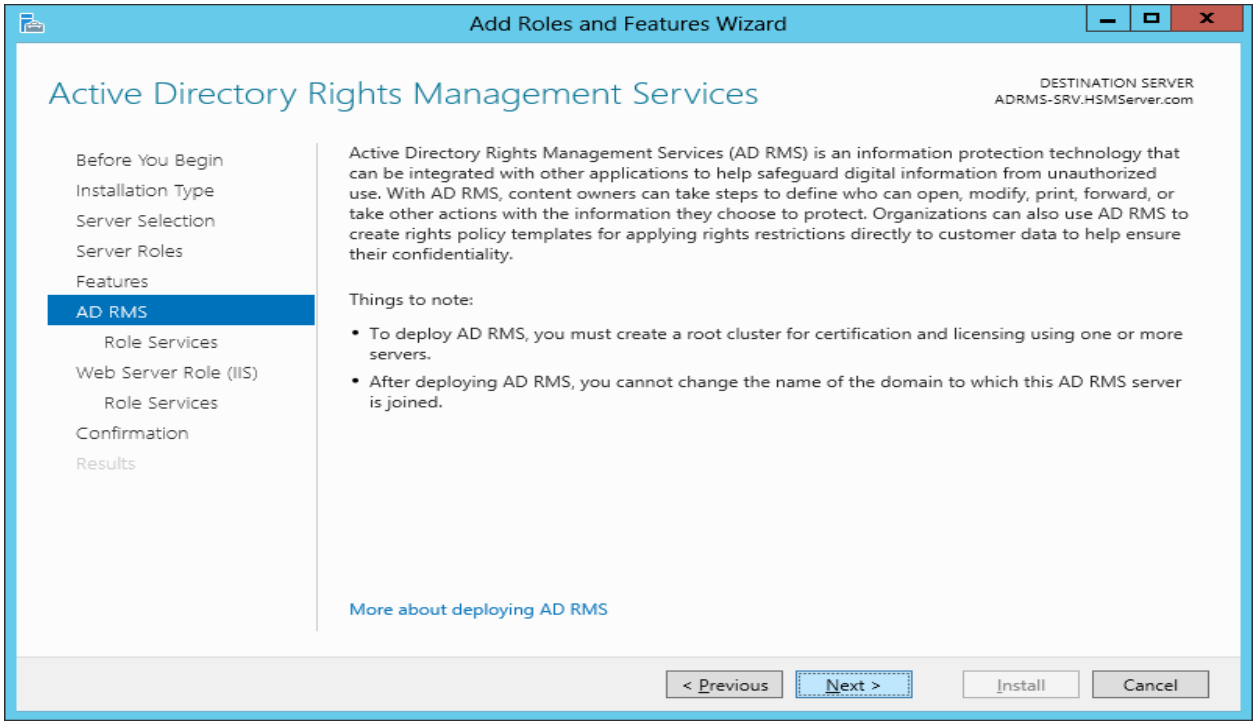


8. You receive a warning stating **Add features that are required for Active Directory Rights Management Services.** Click **Add Features**.

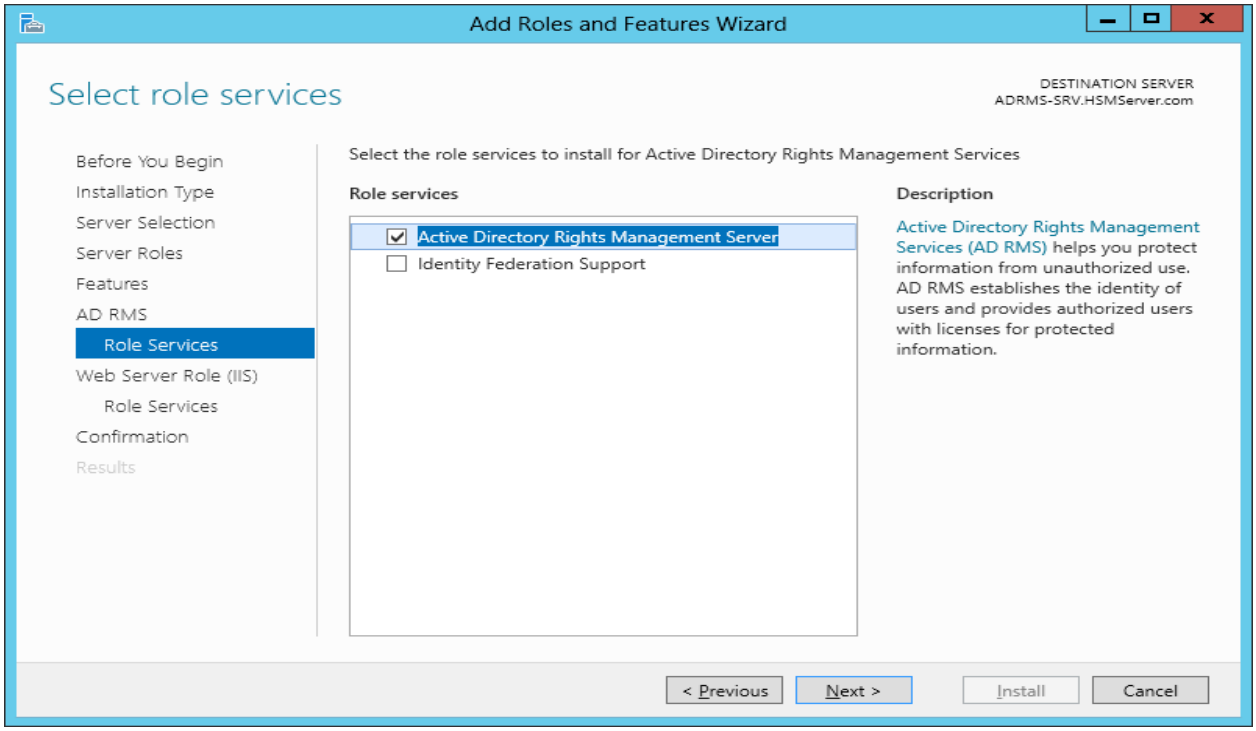
9. Click **Next** to continue on the Server Roles page.



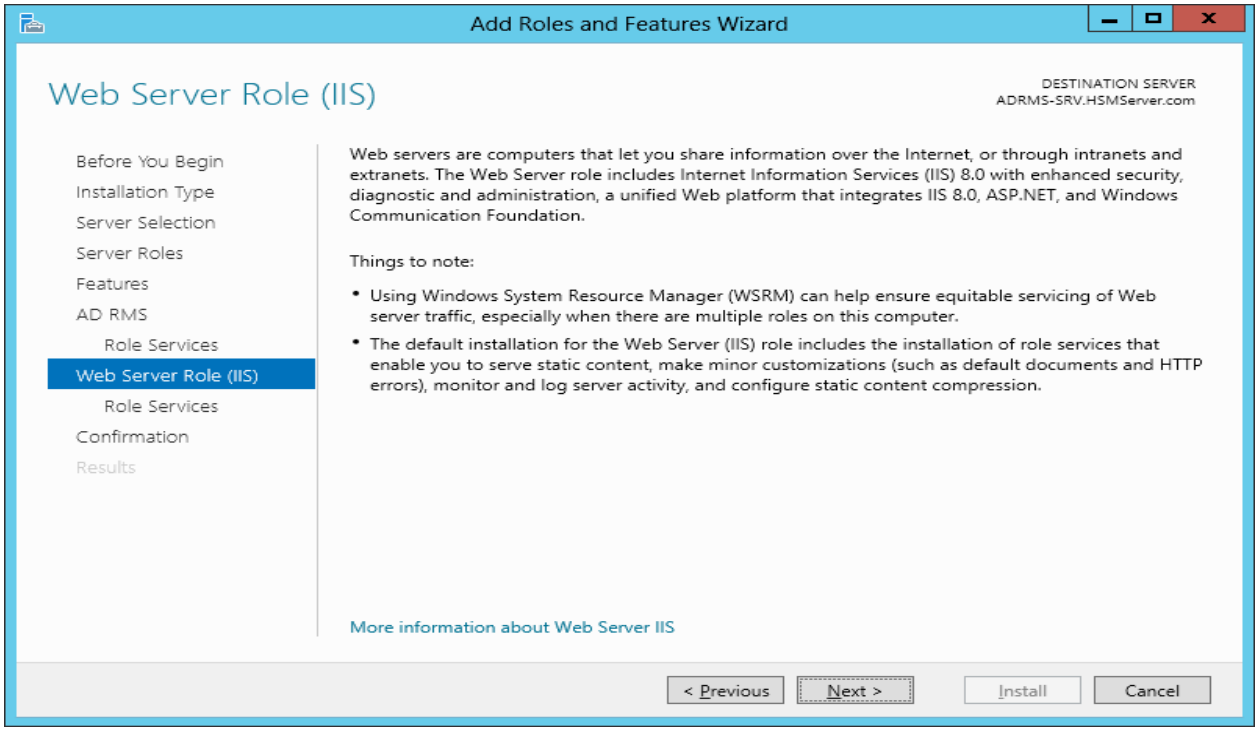
10. Click **Next** on the Active Directory Rights Management Services window.



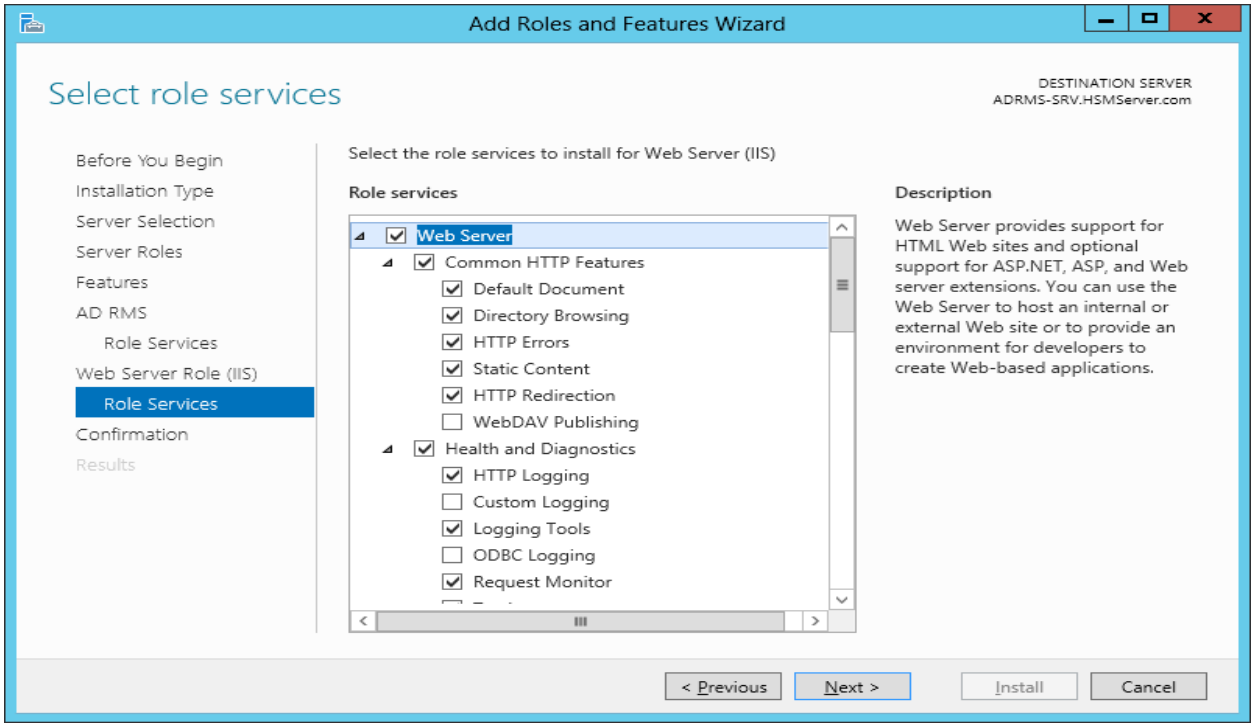
11. Select the **Active Directory Rights Management Server** check box from the **Role Services** and click **Next** to continue.



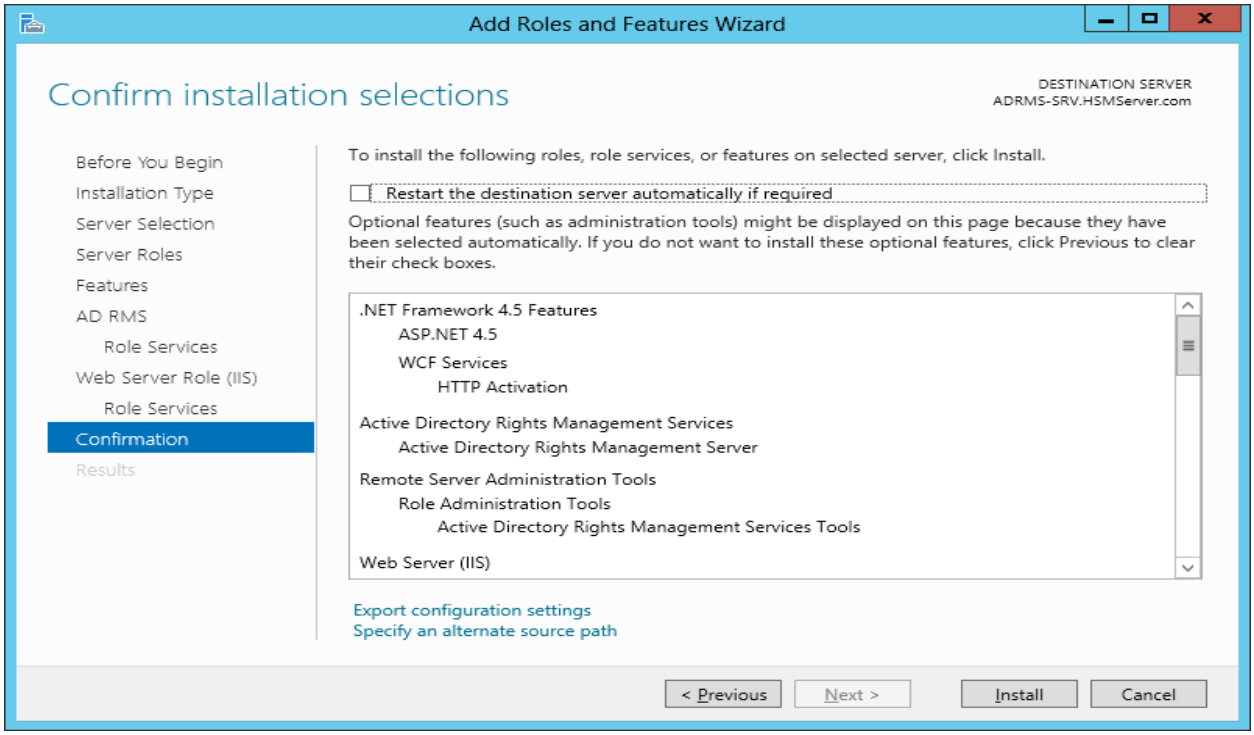
12. Click **Next** to continue on the Web Server Roll (IIS) page.



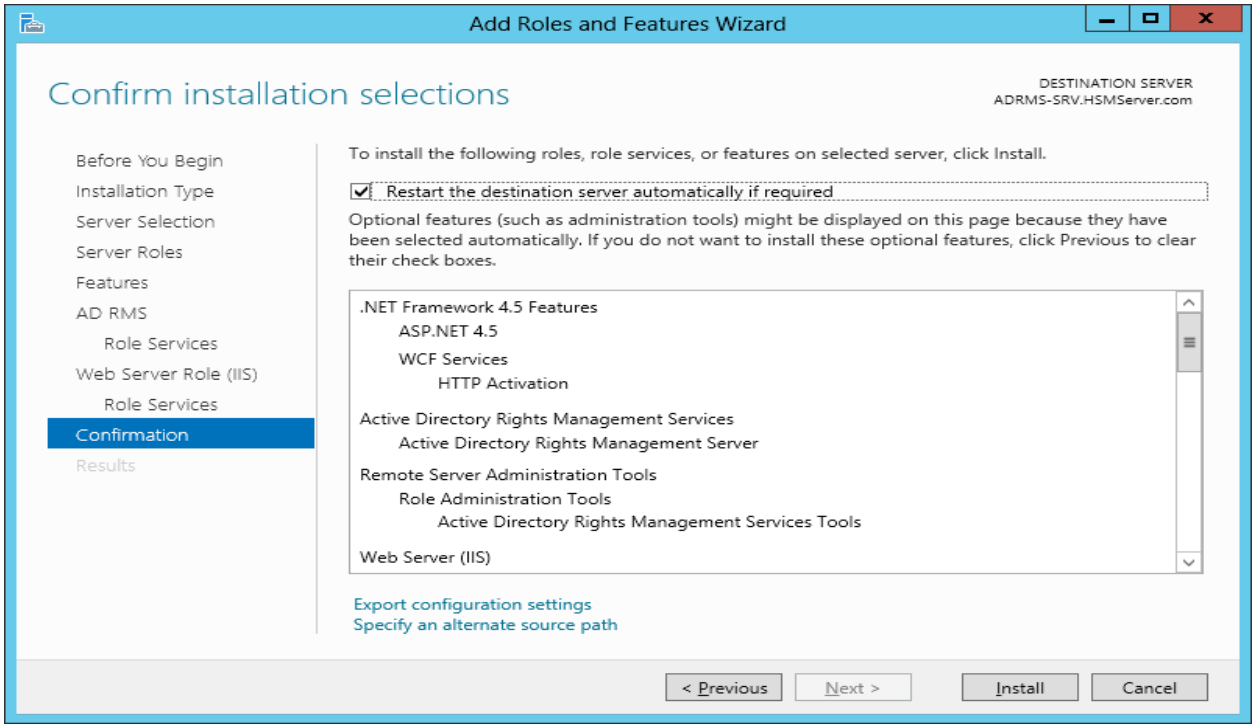
13. Use default selection and Click **Next** to continue on the Role Services page.



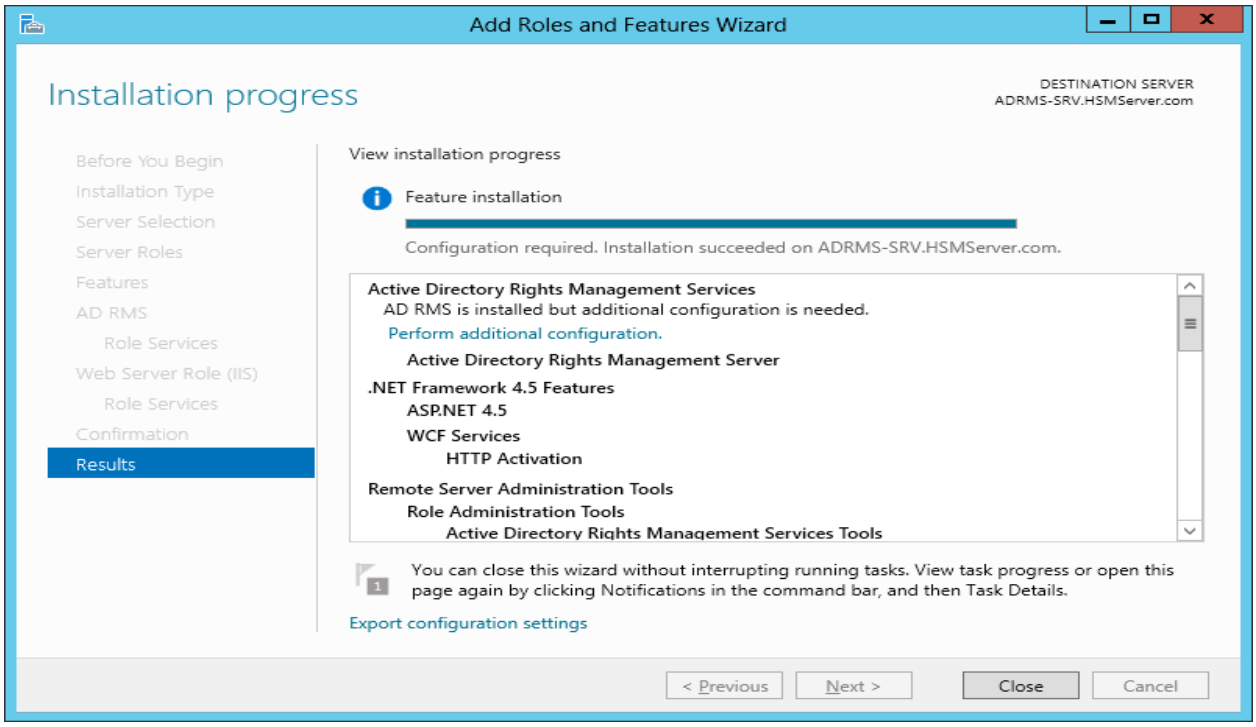
14. Select the **Restart the destination server automatically if required** check box.



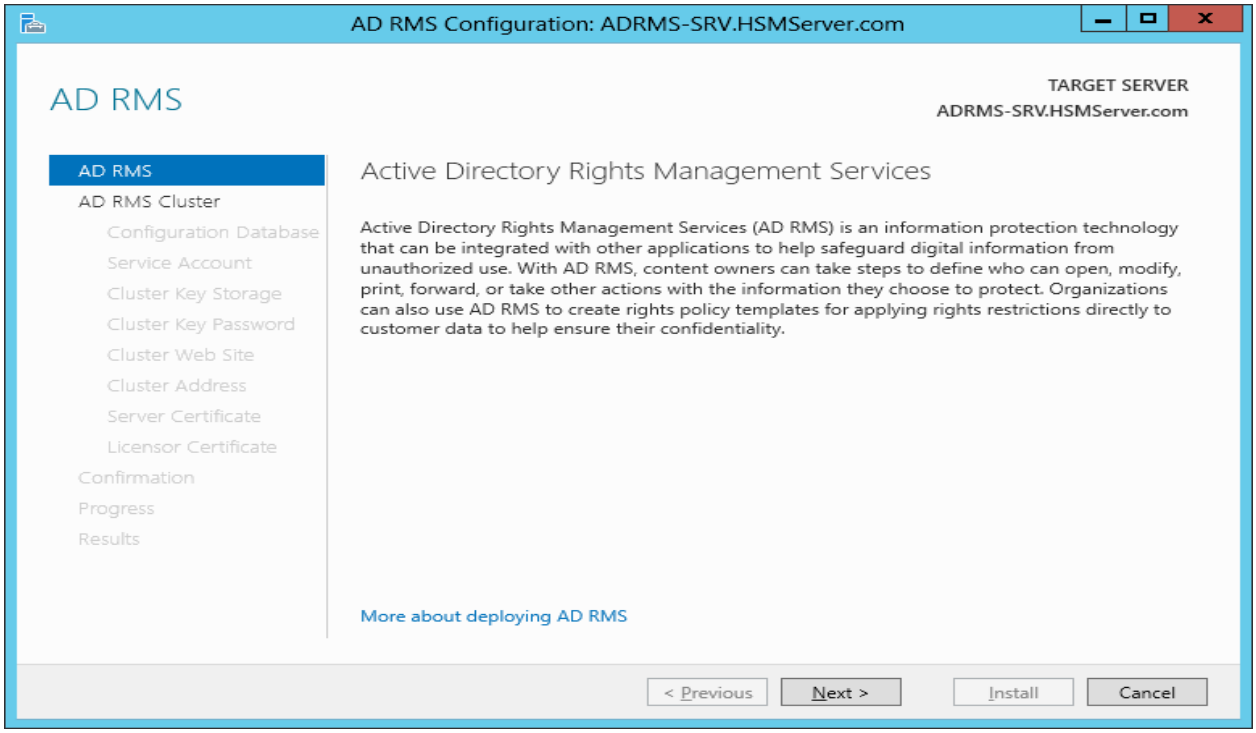
15. A warning message about restarting the server displays, click **Yes**.
16. Click **Install** on the Confirmation page.



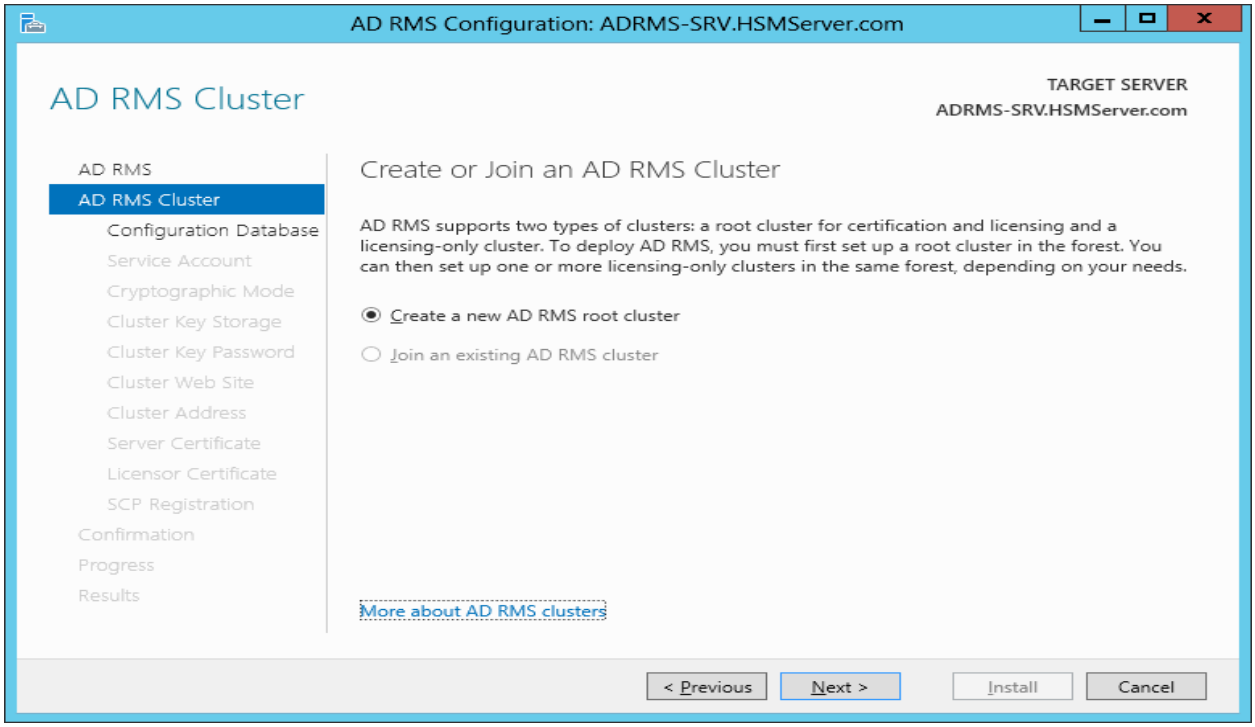
17. When installation is completed, either **Close** the wizard or click **Perform additional configuration**. You can open the configuration wizard later by clicking the Notification Flag.



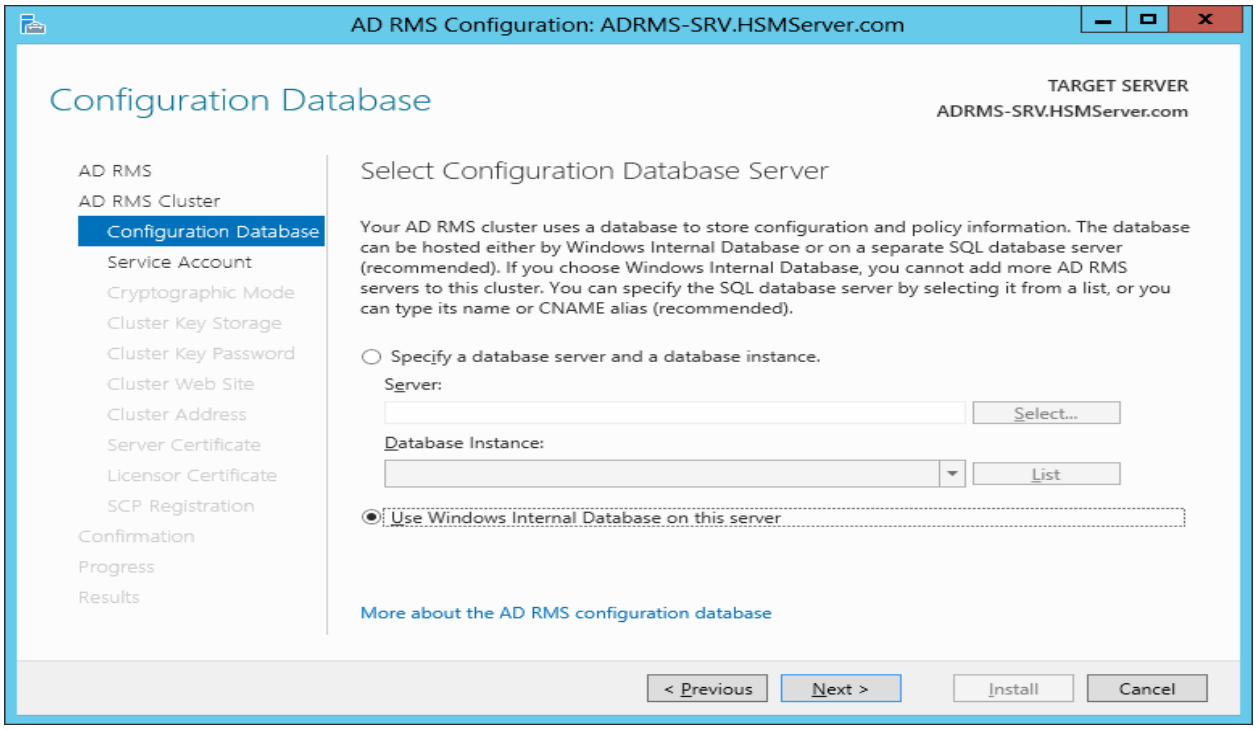
18. The AD RMS Configuration wizard displays, click **Next** to continue.



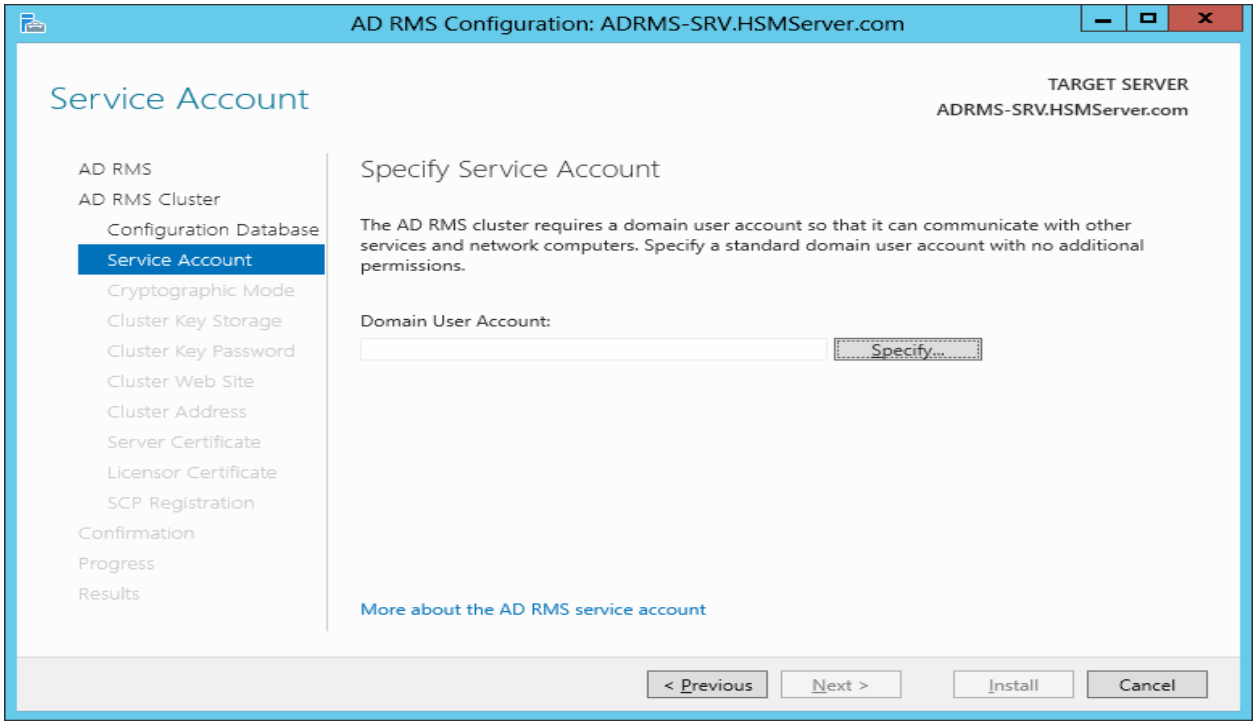
19. Select the **Create a new AD RMS root cluster** radio button and click **Next** on the AD RMS Cluster page.



20. Select the **Use Windows Internal Database** radio button on this server and click **Next** to continue.

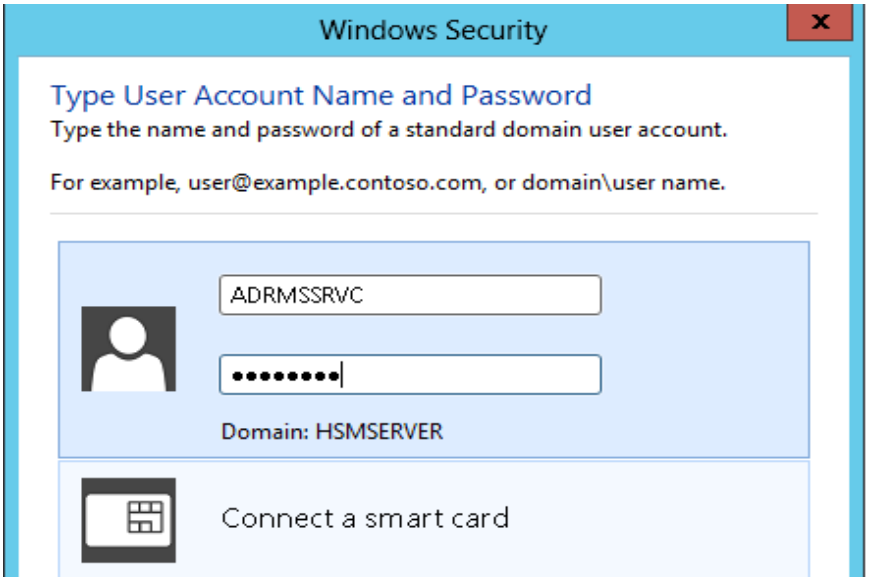


21. Click **Specify…** to specify service account.

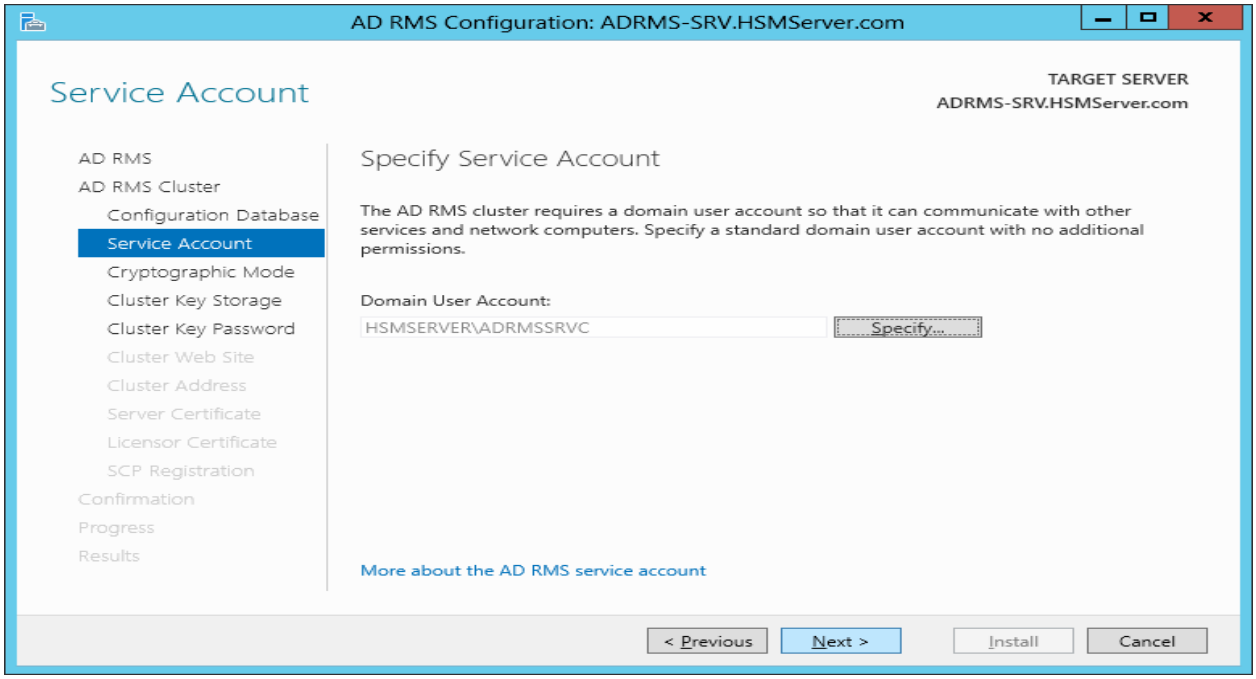


22. A window displays to add service account user, type the ADRMSSRVC and password and click **OK**

NOTE: ADRMSSRVC is the user that you have created in Active Directory, see Configure User Account and Group section above.

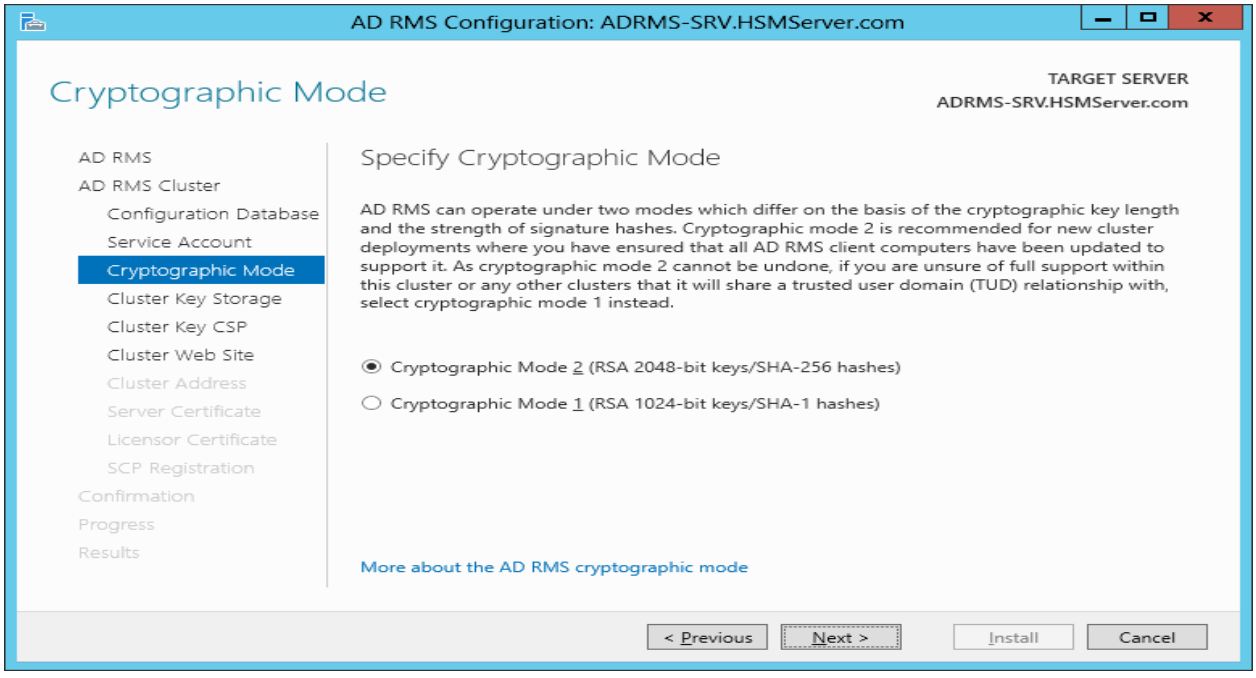


23. Click **Next** to continue on the Service Account page.

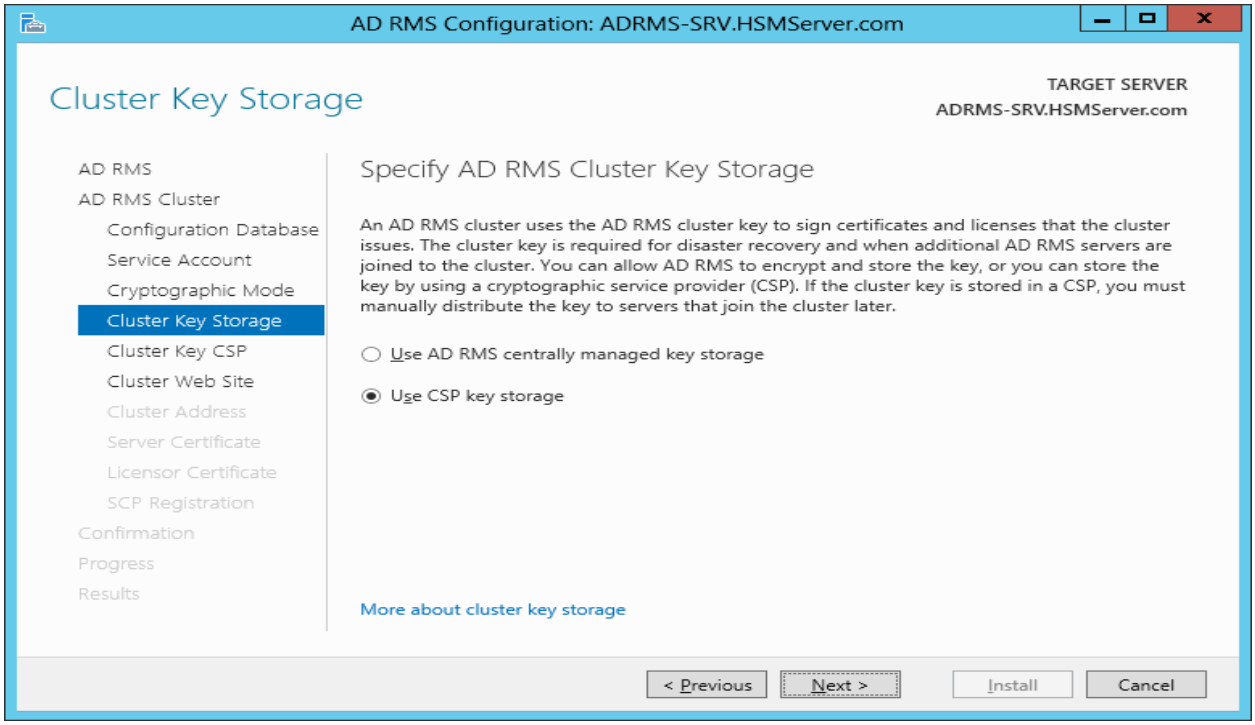


24. Select Cryptographic Mode to generate the keys and click **Next** to continue.

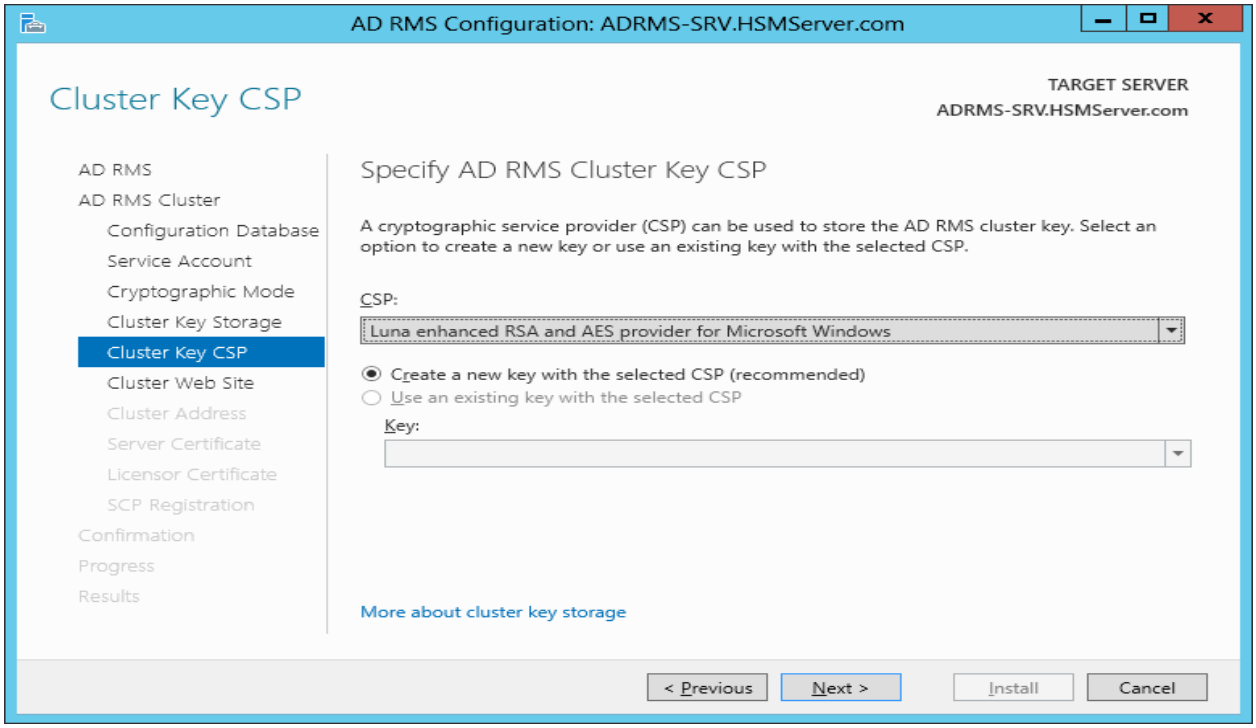
NOTE: You can select any mode on the Specify Cryptographic Mode page. Based on the selected mode, the supported Luna CSP displays.



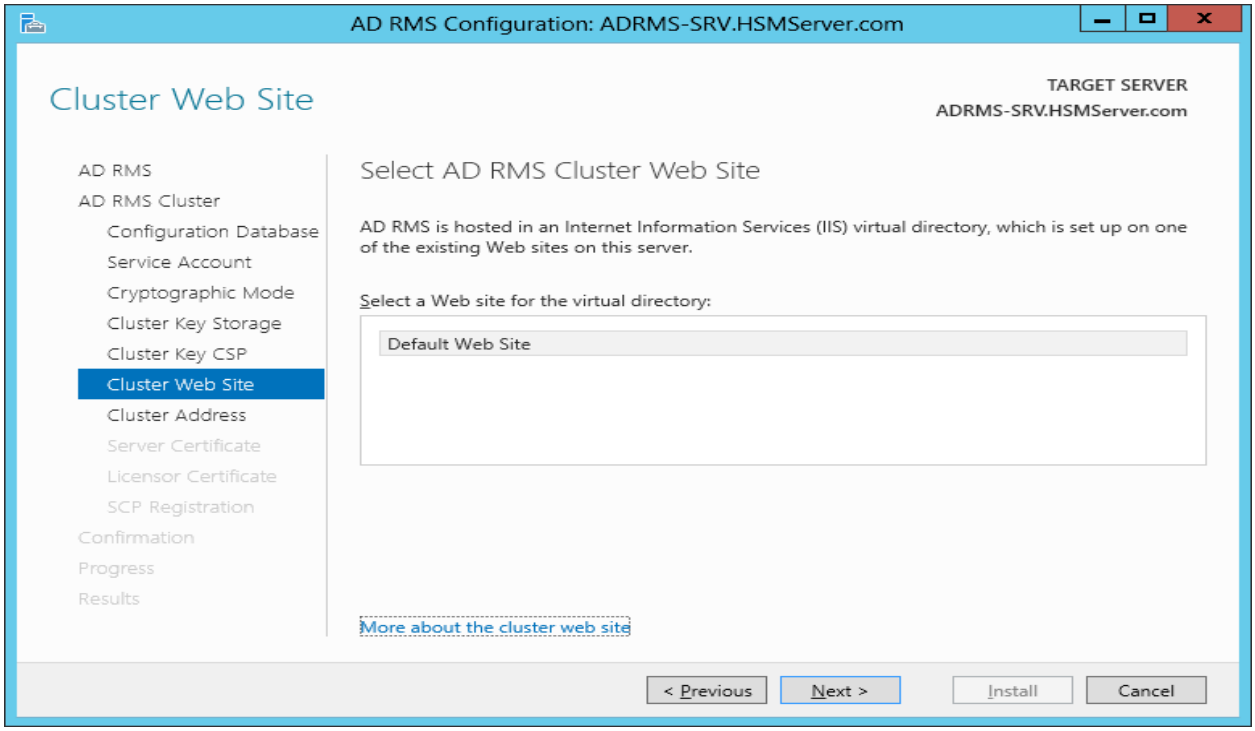
25. Select the **Use CSP key storage** radio button and click **Next** to continue.



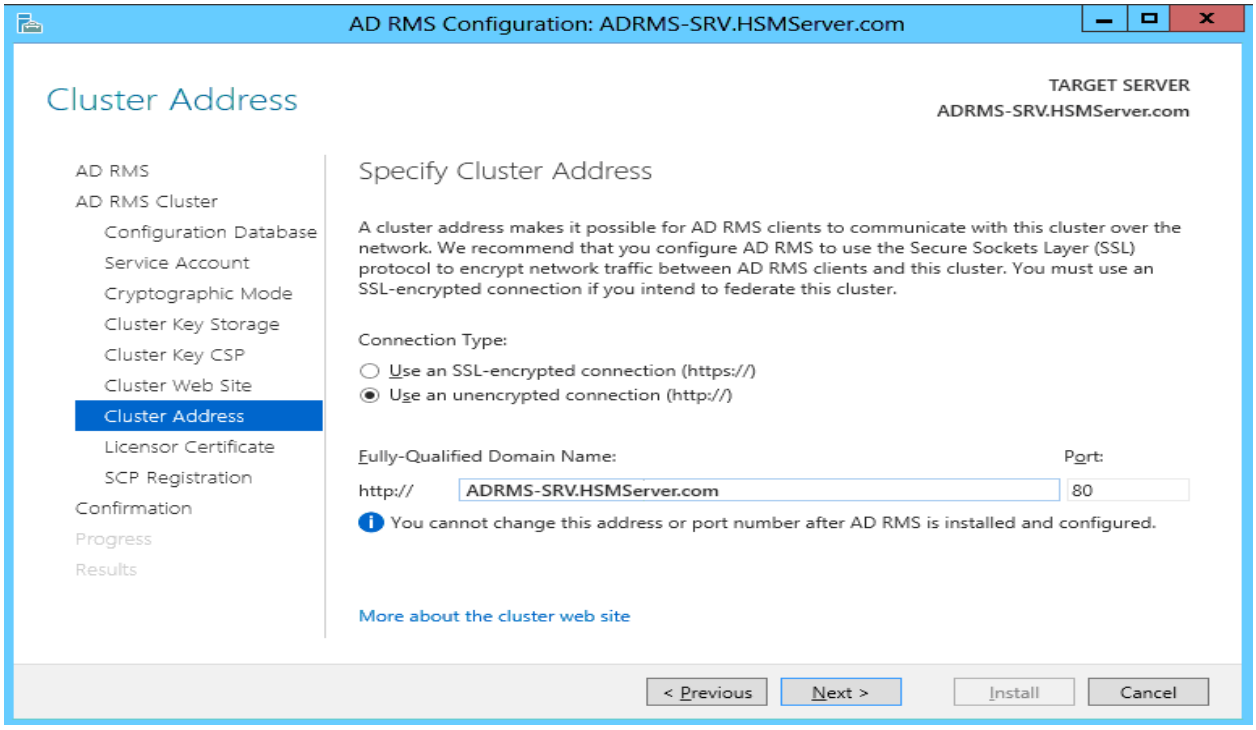
26. Choose **Luna enhanced RSA and AES provider for Microsoft Windows** from the **CSP** drop-down menu and select the **Create a new key with the selected CSP** radio button and then click **Next** to continue.



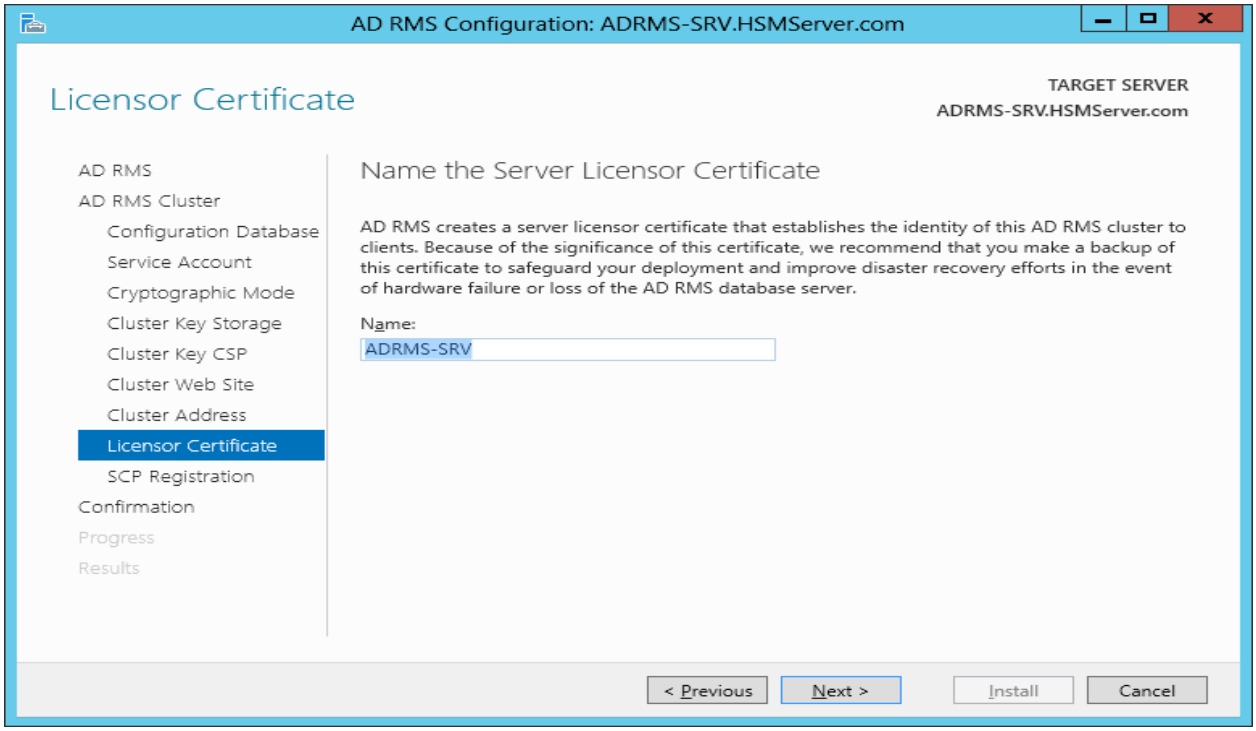
27. Click **Next** to continue on the Cluster Web Site page. Ensure that the Default Web Site is listed.



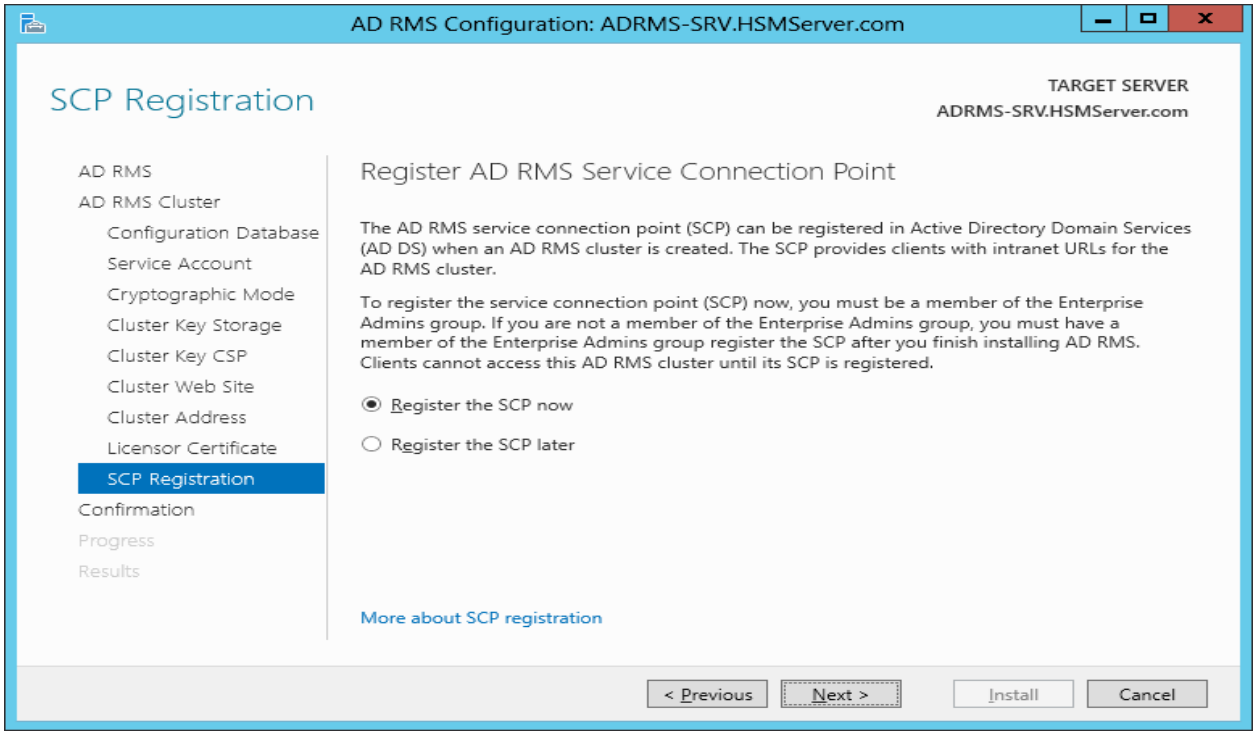
28. Select **Use an unencrypted connection (http://)** and type the fully qualified domain name then click **Next** to continue.



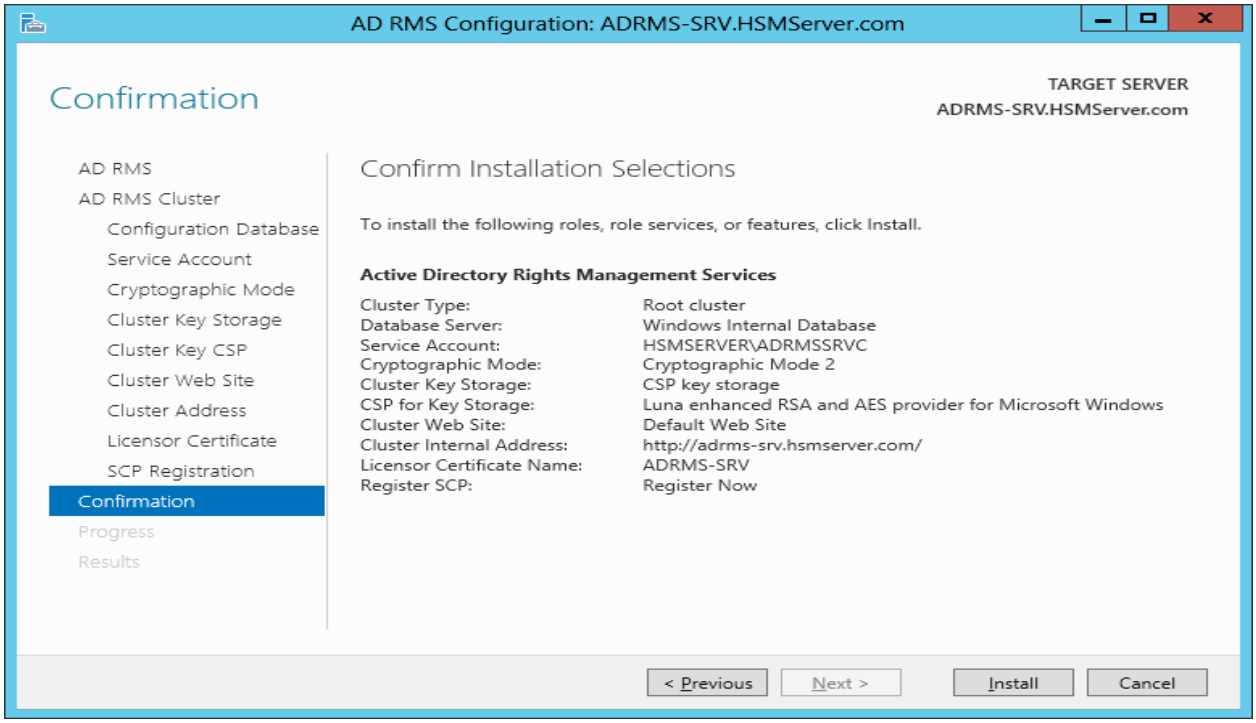
29. Ensure that the server name ADRMS-SRV is listed and click **Next** to continue.



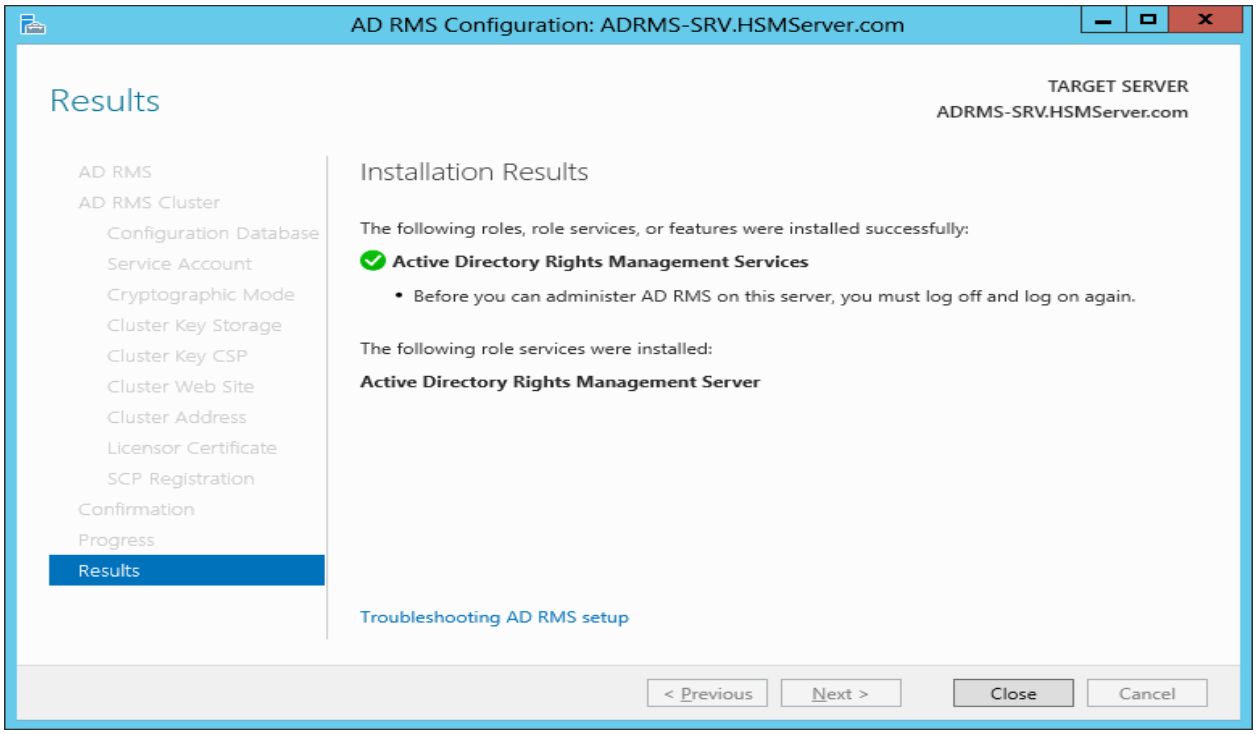
30. Select Register the SCP now and click **Next** on the SCP Registration page.



31. Click **Install** on the Confirmation page.



32. Click **Close** after successful installation of the AD RMS Services.

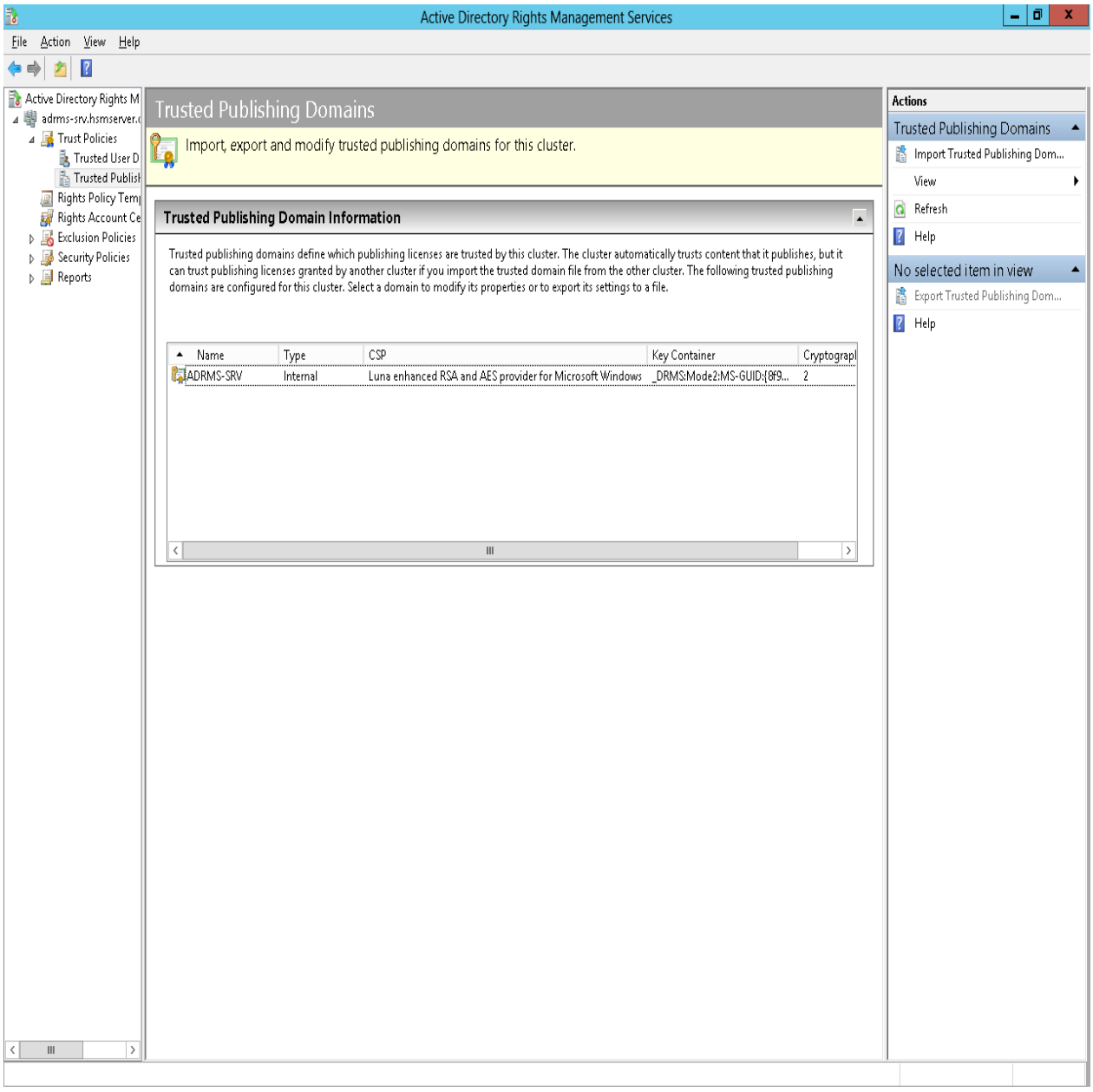


33. After restarting the system, log on as **hsmserver/adrmsadmin** and open the Active Directory Rights Management Services console by clicking **Server Manager** -> **Tools** -> **Active Directory Rights Management Services**.

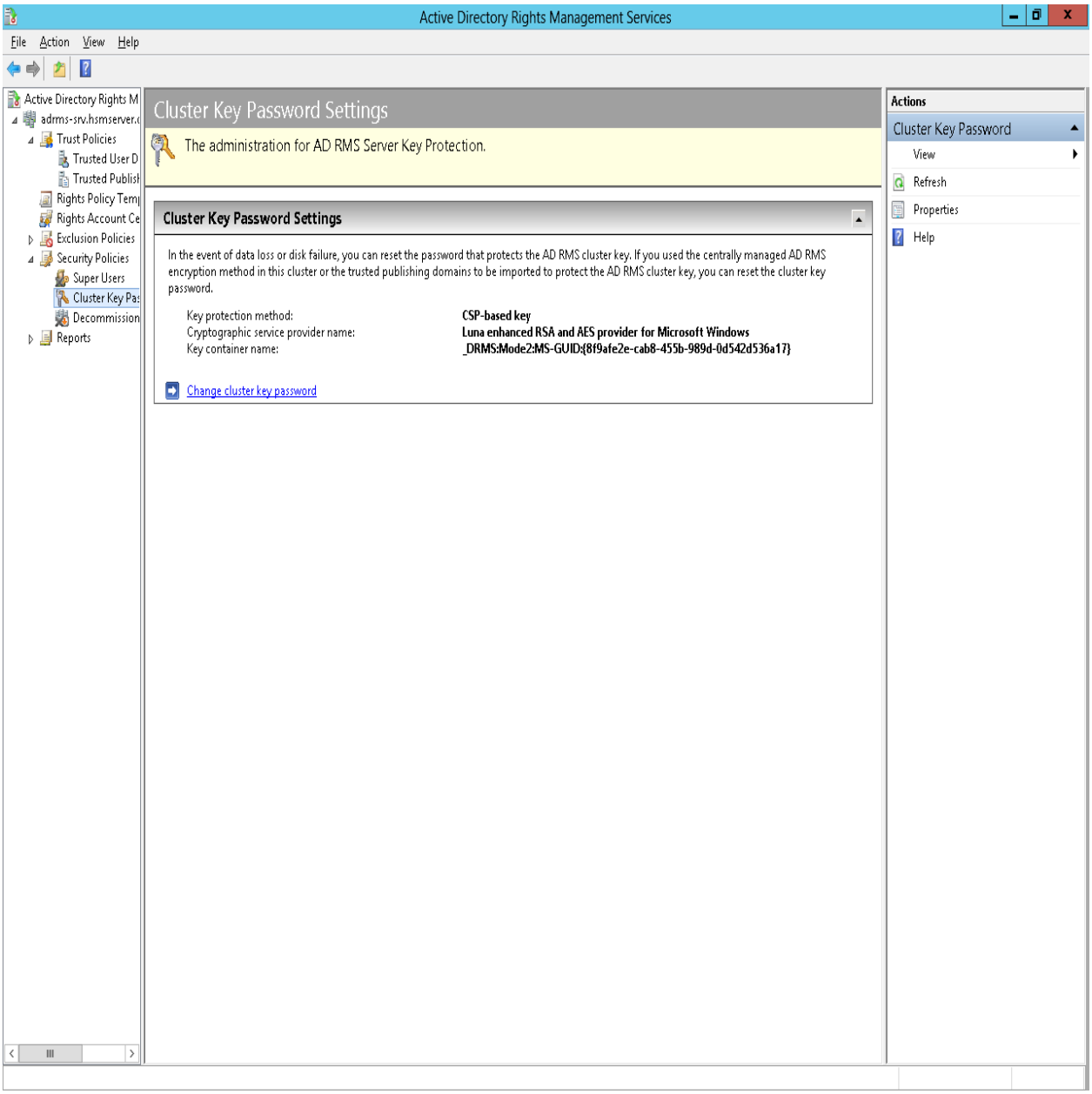
34. Expand the Active Directory Rights Management Services tree and you will see the **Luna enhanced RSA and AES provider for Microsoft Windows** under:

- **Trust Policies** -> **Trusted Publishing Domains**

NOTE: Luna CSP that you have selected at configuring the AD RMS displays here.



- **Security Policies –> Cluster Key Password**



4

Verifying AD RMS Functionality using AD RMS CLIENT

To verify the functionality of the AD RMS deployment, log on ADRMS-CLNT as Nicole Holliday and then restrict permissions on a Microsoft Word document so that members of the CP&L Engineering group are able to read the document but unable to change, print, or copy. Log out form ADRMS-CLNT and then log on as Stuart Railson, verifying that the proper permission to read the document has been granted, and nothing else. Then, log on as Limor Henig. Since Limor is not a member of the Engineering group, he should not be able to consume the rights-protected file.

Before you can consume rights-protected content, must add the AD RMS cluster URL to the Local Intranet security zone.

Add the AD RMS cluster URL to the Local Intranet security zone for all users who will be consuming rights-protected content.

1. To add AD RMS cluster to Local Intranet security zone
    - Log on to **ADRMS-CLNT** as Nicole Holliday.
    - Click **Start**, and then click **Internet Explorer**.
    - Click **Tools**, and then click Internet Options.
    - Click the **Security** tab, click **Local intranet**, and then click **Sites**.
    - In the **Add this website to the zone**, type **http://<fully qualified domain name of the server>**, for example http://ADRMS-SRV.hsmserver.com and then click Add.
    - Click **Close** and then **OK**.
    - Repeat steps 1–6 for Stuart Railson and Limor Henig.

Next, log on a Nicole Holliday and create a Microsoft Word 2007/2010 document and save it to the \\ADRMS-SRV\Public folder.

2. To restrict permissions on a Microsoft Word document
    - Log on to **ADRMS-CLNT** as Nicole Holliday.
    - Right click on the screen and select **New -> Microsoft Office Word Document**.
    - Type **CP&L engineering employees can read this document, but they cannot change, print, or copy it** on the blank document page after opening it.
    - Click the **Microsoft Office Button**, click **Prepare**, click **Restrict Permission**, and then click **Restricted Access**.
    - Click the **Restrict permission to this document** check box.

- In the **Read** box, type email of the group for which you want to grant the permission, for example **engineering@hsmserver.com** and then click **OK** to close the Permission dialog box.
- Click the **Microsoft Office Button**, click **Save As**, and then save the file as \\ADRMS-SRV\Public\ADRMS-TST.docx.
- Log off as Nicole Holliday.

Next, log on as Stuart Railson and open the document, ADRMS-TST.docx

3. To view a rights-protected document
   - Log on to ADRMS-CLNT as Stuart Railson.
   - Click **Start**, and then click **Computer**.
   - Click in the **Address bar**, type **\\ADRMS-SRV\Public\ADRMS-TST.docx**, and then press **Enter**.
   - The following message displays: "**Permission to this document is currently restricted. Microsoft Office must connect to http://adrms-srv.hsmserver.com/_wmcs/licensing to verify your credentials and download your permission**."

     Click **OK**.
   - The following message displays: "**Verifying your credentials for opening content with restricted permissions…**"
   - When the document opens, click the **Microsoft Office** Button. Notice that the Print option is not available.
   - Close Microsoft Word.
   - Log off as Stuart Railson.

Finally, log on as Limor Henig and verify that he is not able to consume the rights-protected file.

4. To attempt to view a rights-protected document.
   - Log on to ADRMS-CLNT as Limor Henig.
   - Click **Start**, and then click **Computer**.
   - Click in the **Address bar**, type **\\ADRMS-SRV\Public\ADRMS-TST.docx**, and then press **Enter**.
   - The following message displays: "**Permission to this document is currently restricted. Microsoft Office must connect to http://adrms-srv.hsmserver.com/_wmcs/licensing to verify your credentials and download your permission.**"
   - Click **OK**.
   - The following message displays: **"You do not have credentials that allow you to open this document. You can request updated permission from nhollida@hsmserver.com. Do you want to request updated permission?"**
   - Click **No**, and then close Microsoft Word.

This demonstrates the AD RMS functionality, using the simple scenario of applying restricted permissions to a Microsoft Word 2007/2010 document. This deployment can be to explore to some of the additional capabilities of AD RMS through additional configuration and testing.

Trusted Publishing Domains (TPD)

By default, an AD RMS Licensing Server can issue use licenses for only content where it originally issued the publishing license. In some situations, this may not be acceptable.

In order to specify a cluster that is allowed to issue use licenses for content protected by a different cluster, the first cluster must be defined as a trusted publishing domain. If content was published by another certification cluster either in your organization, for example, a subsidiary organization in another forest, or in a separate organization, your AD RMS cluster can grant use licenses to users for this content by configuring a Trusted Publishing Domain on your AD RMS cluster.

By adding a Trusted Publishing Domain, you set up a trust relationship between your AD RMS cluster and the other certification cluster by importing the Trusted Publishing Certificate of the other cluster.

SafeNet Luna HSM supports TPD with multiple forests. To enable Trust model TPD needs to be exported in the cluster where you protected the content and imported in the one where you are trying to consume it.

SafeNet Luna HSM is tested with two-way TPD between the two forests.

5
Troubleshooting Tips

Problem:

Error message **"Password could not be contacted"** when trying to register Service Account while installing AD RMS on the **Domain Controller**.

Solution:

1. Ensure that the user must have the member of Domain Administrator groups or Enterprise Administrator group whose credentials you are supplying.
2. User Account user should be other than that user which is installing AD RMS.