Lesson 21: Installing and Configuring Active Directory Rights Management Services

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Microsoft Official Academic Course

WILEY

Overview

- Objective 6.4 – Install and configure Active Directory Rights Management Services (AD RMS).
  - Install a licensing or certificate AD RMS server
  - Manage AD RMS Service Connection Point (SCP)
  - Manage AD RMS client deployment
  - Manage Trusted User Domains
  - Manage Trusted Publishing Domains
  - Manage Federated Identity Support
  - Manage RMS templates
  - Configure exclusion policies

Understanding Active Directory Rights Management

Lesson 21: Installing and Configuring Active Directory Rights Management Services

Active Directory Rights Management Services (AD RMS)

- ***Active Directory Rights Management Services (AD RMS)*** is technology used to provide an extra level of security to documents, such as email and Microsoft Office documents, by using encryption to limit access to a document or web page and what can be done with that document or web page.
- For example, you can limit whether a document or web page can be printed, copied, edited, forwarded, or deleted.
- RMS helps contain confidential information so that it stays within the organization and helps limit who can access the data.

Active Directory Rights Management Services (AD RMS)

- AD RMS is an information protection technology used to minimize unauthorized transmission of data or data leakage, specifically with Microsoft products and operating systems including Microsoft Exchange, Microsoft SharePoint, and the Microsoft Office suite.
- To control who can access a file or email, AD RMS encrypts the file or email.
- To read the file, the user will need the encryption key to decrypt the file, which is stored in the AD RMS server.
- As a user opens or accesses the file, he or she will automatically retrieve the key from the AD RMS server and open the file.
- Since the Microsoft products are AD RMS aware, they also help limit what you can do with a document as specified with the rights assigned using rights management.

Active Directory Rights Management Services (AD RMS)

- If someone copies the file to a USB storage device and takes it offsite, or emails it to someone else, the person who opens the file needs to access the AD RMS to retrieve the keys.
- If the person cannot access the rights management server (for whatever reason), or is not authorized to access the file, he or she will not get the key and will not be able to open and read the file's content.

AD RMS Components

- ***AD RMS server***
  - A Windows server that is a member of an Active Directory Domain Services (AD DS) domain.
  - When you install AD RMS servers, the location of the server is published to AD DS to a location known as the service connection point.
  - Because RMS can be an important component when securing documents, AD RMS might deploy AD RMS with high availability using clustering.

AD RMS Components

- ***AD RMS client***
  - With Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 operating systems, the client is included.
  - With Windows XP, Windows Server 2003, and Windows Server 2003 R2, the client can be downloaded and installed.
  - Computers that are members of the domain query AD DS for the service connection point to determine the location of AD RMS services.

AD RMS Components

- ***AD RMS-enabled applications***
  - An application that allows users to create and consume AD RMS-protected content.
  - Examples of AD RMS-enabled applications include Microsoft Word, Microsoft Excel, and Microsoft Outlook.

AD RMS Components

- ***AD RMS root certification cluster***
  - The first AD RMS server that you deploy in a forest.
  - It manages all licensing and certification traffic for the domain in which it is installed.
  - The configuration information is installed in a Microsoft SQL database.
  - AD RMS root certification clusters are typically found in large branch offices to distribute licenses used in content consumption and publishing.

AD RMS Components

- ***Licensing-only cluster***
  - An optional component that is not part of the root cluster.
  - It relies on the root cluster for certification and other services.
  - It only provides both publishing licenses and use licenses to users.
  - It is typically used when supporting unique rights management requirements of a department or of external business partners.

AD RMS Certificates and Licenses

- ***Server licensor certificate (SLC)***
  - A certificate containing the public key that encrypts the content key in a publishing license.
  - It allows the AD RMS server to extract the content key and issue end use licenses (EULs) against the publishing key.
  - It is generated when you create the AD RMS cluster.
  - It allows the AD RMS cluster to issue SLCs to other servers in the cluster, rights account certificates to clients, Client licensor certificates, publishing licensing, use licenses, and to deploy rights policy template.
  - It has a validity of 250 years. Since it is one of the core components, it is important to back up the SLCs on a regular basis.

AD RMS Certificates and Licenses

- ***AD RMS machine certificate***
  - Used to identify a trusted computer or device.
  - It is also used to encrypt the rights account certificate private key and decrypts the rights account certificates.
- ***Rights account certificate (RAC)***
  - A RAC is issued the first time a user attempts to access AD RMS-protected content, which is used to identify a specific user.
  - RACs can be issued only to users in AD DS whose user accounts have email addresses that are associated with them.
  - The default validity time for a RAC is 365 days.

AD RMS Certificates and Licenses

- ***Temporary rights account certificate***
  - Issued to users who are accessing AD RMS-protected content from a computer that is not a member of the same or trusted forest as the AD RMS cluster.
  - A temporary RAC has a validity time of 15 minutes.
- ***Active Directory Federation Services (AD FS) RACs***
  - Issued to federated users.
  - They have a validity of seven days.
- ***Windows Live ID RAC***
  - Used with Microsoft account, formerly called Windows Live Accounts. Windows Live ID RACs used on private computers have a validity of six months.
  - Windows Live ID RACs on public computers are valid until the user logs off.

AD RMS Certificates and Licenses

- ***Client licensor certificate***
  - Allows a user to publish AD RMS-protected content when the client computer is not connected to the same network as the AD RMS cluster.
  - The client licensor certificate public key encrypts the symmetric content key and includes it in the publishing license that it issues.
  - The client licensor certificate private key signs any publishing licenses that are issued when the client is not connected to the AD RMS cluster.
  - Because client licensor certificates are tied to a specific user's RAC, when another user without a RAC attempts to publish AD RMS-protected content from the same client, that user will not be able to until the client connects to the AD RMS cluster so that the user can get a RAC.

AD RMS Certificates and Licenses

- ***Publishing license (PL)***
  - Determines the rights that apply to AD RMS-protected content.
  - It contains the content key, which is encrypted using the public key of the licensing service.
  - It also contains the URL and the digital signature of the AD RMS server.
- ***End use license (EUL)***
  - Required to consume AD RMS-protected content.
  - The AD RMS server issues one EUL per user per document.
  - EULs are cached by default.

Protecting a Document with AD RMS

- How to protect and access a document using AD RMS:
  1. When an author configures rights protection for information the first time, he or she receives a client licensor certificate from the AD RMS server.
  2. When the author defines a collection of usage rights and usage of the file, the application encrypts the file with a symmetric key.
  3. This symmetric key is encrypted to the public key of the AD RMS server used by the author.

Protecting a Document with AD RMS

4. When a recipient opens the file using an AD RMS application or browser, if the recipient does not have an account certificate on the current host, one will be issued to the user.
5. When the user has the account certificate, the application or browser transmits a request to the author's AD RMS server for a use license.
6. The AD RMS server determines whether the recipient is authorized. If the recipient is authorized, the AD RMS server issues a use license.
7. The AD RMS server decrypts the symmetric key that was encrypted in step 3, using its private key.
8. The AD RMS server re-encrypts the symmetric key using the recipient's public key and adds the encrypted session key to the use license.

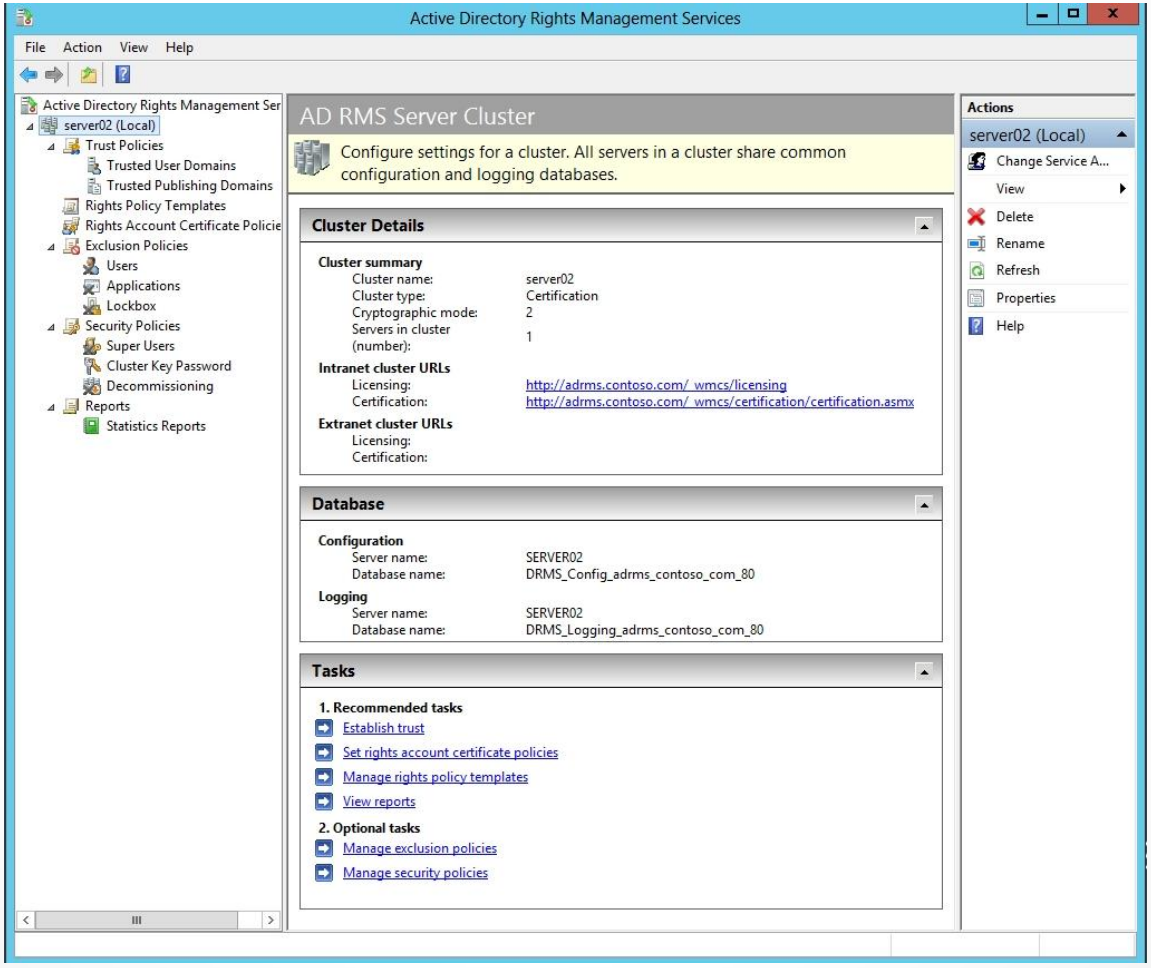
AD RMS Cluster

- An AD RMS deployment consists of one or more servers known as a cluster.
- Additional servers can be added for scalability, if you use a dedicated SQL server.
- When you deploy AD RMS in a single forest, you would have a single AD RMS cluster.
- If you have multiple forests, each forest will have its own AD RMS root cluster.
- Only one root cluster can exist in an AD DS forest.

Active Directory Rights Management Services Console

- The primary tool used to manage AD RMS is the Active Directory Rights Management Services console.
- When you open the console, you can see the cluster name, the intranet and extranet cluster URLs, and the location of the databases.

Active Directory Rights Management Services Console



AD RMS Administration Groups

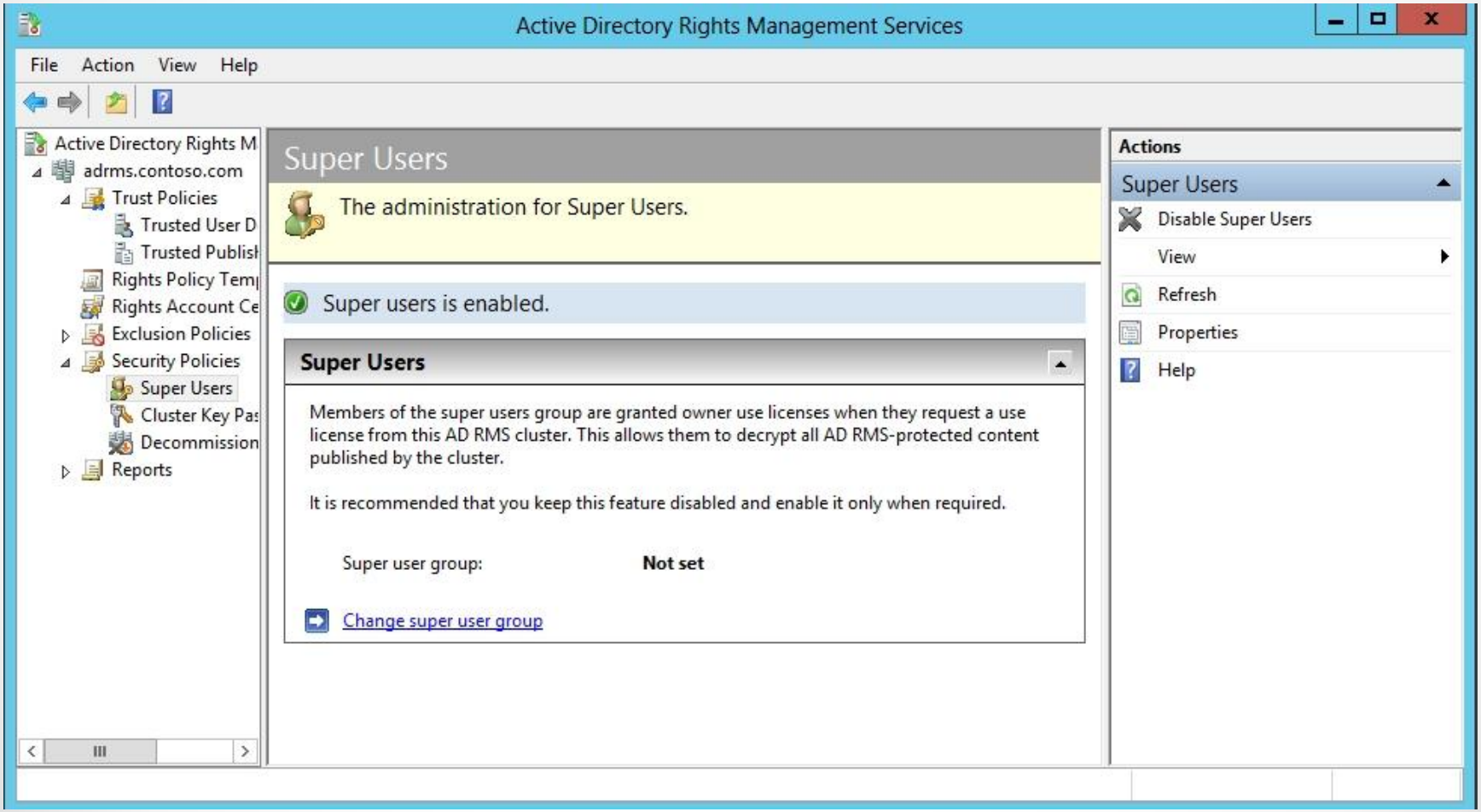
- When AD RMS is deployed, the following administration groups are created:
  - **AD RMS Enterprise Administrators**: Have access to all features in the AD RMS console. During installation of AD RMS, the installing user account is automatically added to this group.
  - **AD RMS Template Administrators**: Can only access rights policy template administration features in the AD RMS console.
  - **AD RMS Auditors**: Access the reports feature in the AD RMS console.
  - **AD RMS Service Group**: Act as the AD RMS service account. During the installation of AD RMS, the user account designated as the service account is automatically added to this group.

Super Users Group

Another important group, which is separated from the administration groups, is the super users group:

- The group is disabled and undefined by default.
- Members are granted owner use licenses when they request a user license from the AD RMS cluster.
- It allows the members to decrypt all AD RMS-protected content published by the cluster.
- When defining the super users group, you must use a Universal Security group.

Super Users Group

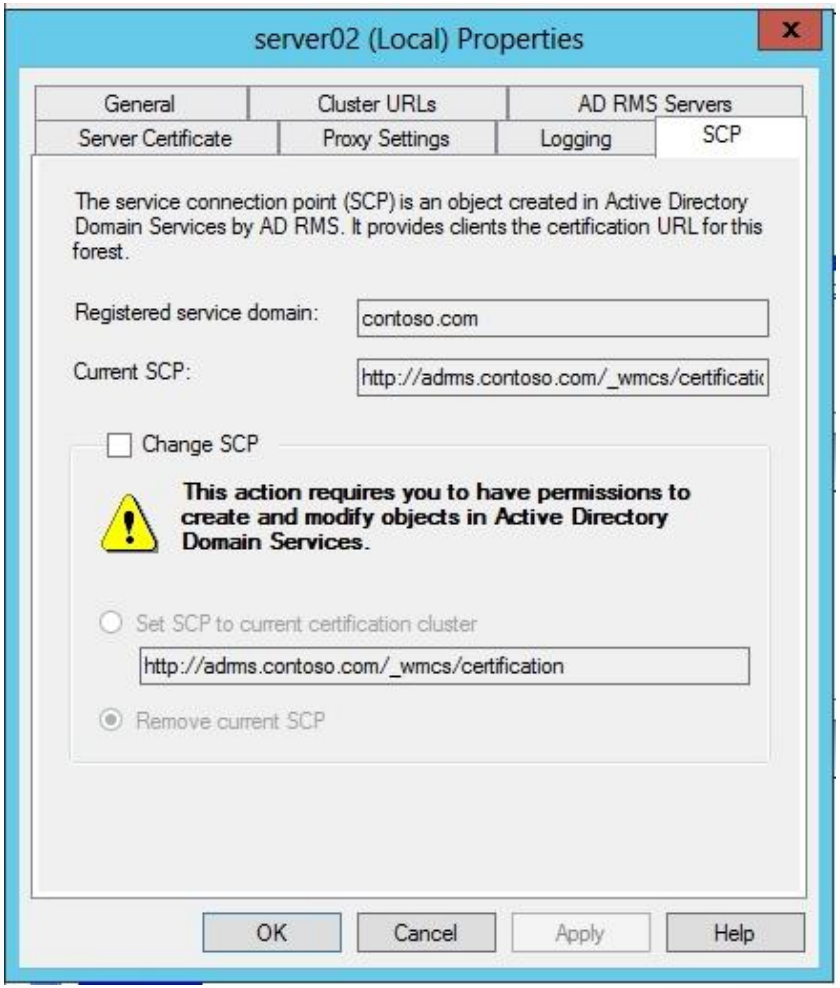


AD RMS Service Connection Point

- The Active Directory Rights Management Services (AD RMS) ***service connection point (SCP)*** is an object in Active Directory that holds the web address of the AD RMS certification cluster.
- It was defined during the installation of AD RMS. AD RMS-enabled applications use the SCP to find the AD RMS service.
- Only one SCP for AD RMS can exist in your Active Directory forest.
- The SCP can be viewed using ADSI Edit or LDP.
- To view the SCP, connect to the configuration container in ADSI Edit and navigate the following nodes:

  CN=Configuration [server name], CN=Services, CN=RightsManagementServices, CN=SCP

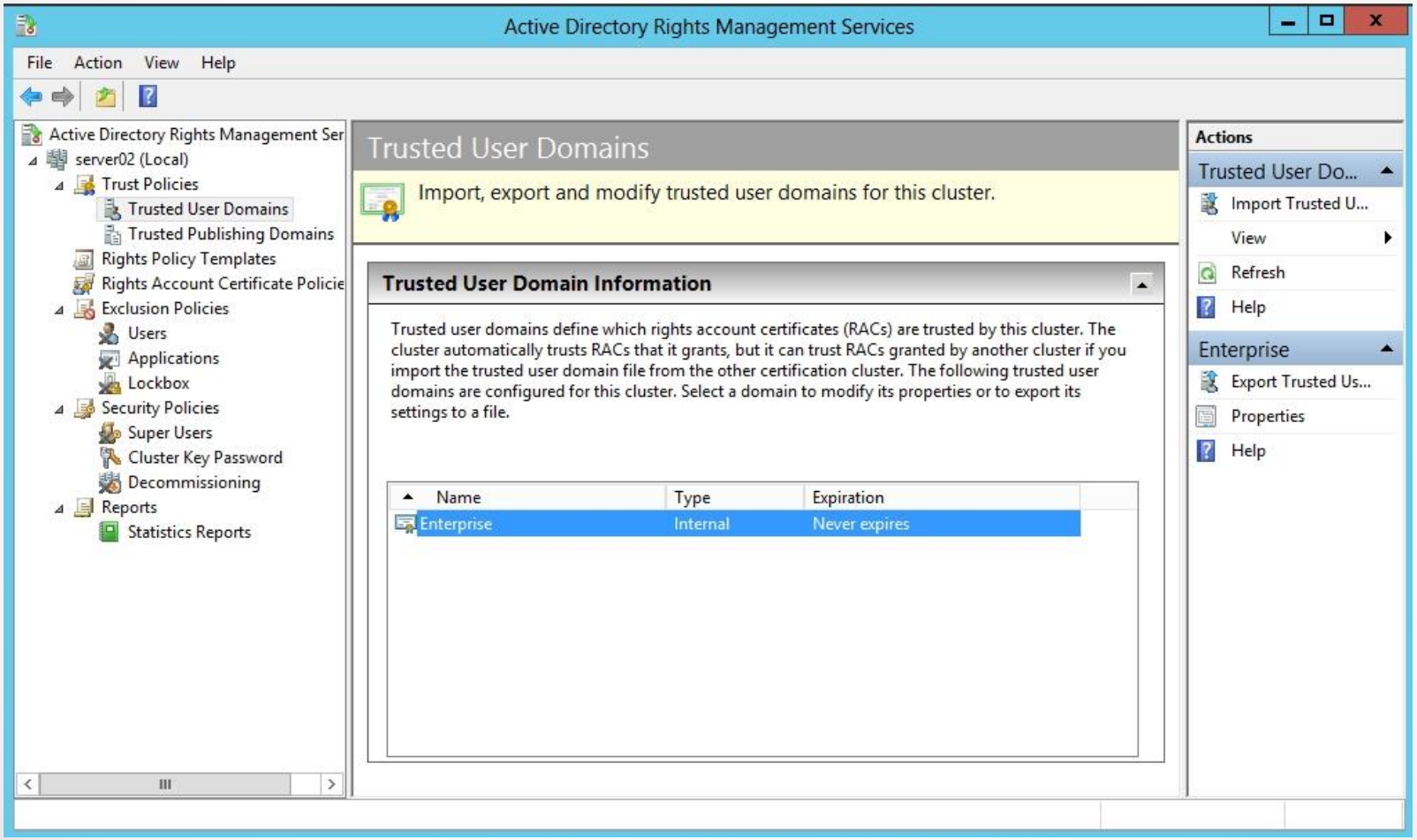
AD RMS Service Connection Point



Managing Trusted User Domains

- By default, Active Directory Rights Management Services does not service requests from users whose rights account certificate (RAC) was issued by a different AD RMS server.
- However, you can add user domains to the list of ***trusted user domains (TUDs)***, which is a trust between AD RMS infrastructures that allows one environment to accept identities from another environment as valid subjects.

Managing Trusted User Domains



Trusted Publishing Domains

- By default, servers in an AD RMS cluster can issue use licenses only against the publishing licenses issued by servers in the cluster.
- If your organization has another AD RMS root cluster located in another forest or in another separate organization, you can set up a trust relationship between AD RMS clusters so that it can grant use licenses to the other forest or organization.
- Trust relationships are created by configuring a ***trusted publishing domain (TPD)***.

Federated Identity Support

- ***Federated Identity Support*** allows users accounts to use credentials established by a federated trust relationship using Active Directory Federation Services (AD FS) instead of setting up trusted publishing domains or trusted user domains.
- When used with AD FS, users obtain rights account certificates from an AD RMS cluster.

Supporting Mobile Devices

- AD RMS can provide rights account certificates and use licenses to AD RMS-enabled applications to devices running Windows mobile operating systems such as Windows Mobile 6 and above.
- In a default AD RMS installation, mobile devices cannot obtain certificates and licenses for their users.
- However, you can enable mobile devices by configuring the DACLs of the MobileDeviceCertification.asmx file.

Rights Policy Templates

- ***Rights policy templates***, also known as RMS templates, are used to enforce the rights that a user or group has on rights-protected content.
- They allow you to standardize the implementation of AD RMS policies across the organization.
- One template may be used on documents to grant view-only rights that block the ability to edit, save, or print.
- If used with Microsoft Exchange Server, you can configure the template to block the ability to forward or reply to a message.

Rights Policy Templates

- AD RMS templates support the following rights:
  - **Full Control**: Gives a user full control over an AD RMS-protected document including the ability to give other people access to the document.
  - **View**: Gives a user the ability to view an AD RMS-protected document.
  - **Edit**: Allows a user to modify an AD RMS-protected document.
  - **Save**: Allows a user to use the Save function with an AD RMS-protected document.
  - **Export (Save as)**: Allows a user to use the Save As function with an AD RMS-protected document.
  - **Print**: Allows an AD RMS-protected document to be printed.

Rights Policy Templates

- **Forward**: Used with Exchange Server, allows the recipient of an AD RMS-protected message to forward that message.
- **Reply**: Used with Exchange Server, allows the recipient of an AD RMS-protected message to reply to that message.
- **Reply All**: Used with Exchange Server, allows the recipient of an AD RMS-protected message to use the Reply All function to reply to that message.
- **Extract**: Allows the user to copy data from the file. If this right is not granted, the user cannot copy data from the file.
- **Allow Macros**: Allow the user to utilize macros.
- **View Rights**: Allow the user to view assigned rights.
- **Edit Rights**: Allow the user to modify the assigned rights.

AD RMS Rights

- Unlike NTFS permissions, AD RMS rights can only be granted and cannot be explicitly denied.
- If a user has not been assigned rights to the document or email, users will automatically be denied access to the document or email.

AD RMS Template Properties

- AD RMS templates can also be used to configure documents with these properties:
  - Content expiration
  - Use license expiration
  - Enable users to view protected content using a browser add-on
  - Require a new use license each time content is consumed
  - Revocation policies

Exclusion Policies

- ***Exclusion policies***
  - Allow you to specify user accounts, client software, and applications that are to be automatically denied access to AD RMS.
  - Allow you to specify a minimum version of the AD RMS client software.
- User Exclusion is disabled by default.

Lesson Summary

- Active Directory Rights Management Services (AD RMS) is technology used to provide an extra level of security to documents such as email, Microsoft Office documents, and web pages by using encryption to limit access to a document or web page and what can be done with that document or web page.
- After the AD RMS server is installed and configured, and the clients are configured to use the AD RMS server, when accessing secure documents, the decryption of a document occurs transparently.
- The primary tool used to manage AD RMS is the Active Directory Rights Management Services console (as shown in Figure 21-9). When you open the console, you can see the cluster name, the intranet and extranet cluster URLs, and the location of the databases.

Lesson Summary

- Members of the super users group are granted owner use licenses when they request a user license from the AD RMS cluster. It allows the members to decrypt all AD RMS-protected content published by the cluster.
- The Active Directory Rights Management Services (AD RMS) service connection point (SCP) is an object in Active Directory that holds the web address of the AD RMS certification cluster. It was defined during the installation of AD RMS. AD RMS-enabled applications use the SCP to find the AD RMS service.
- For clients to use AD RMS, the clients must run the AD RMS client.
- Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012 include the AD RMS client.

Lesson Summary

- By default, Active Directory Rights Management Services does not service requests from users whose rights account certificate (RAC) was issued by a different AD RMS server.
- You can add user domains to the list of trusted user domains (TUDs), which allows AD RMS to process the requests.
- If your organization has another AD RMS root cluster located in another forest or in another separate organization, you can set up a trust relationship between AD RMS clusters so that it can grant use licenses to the other forest or organization. Trust relationships are created by configuring a trusted publishing domain (TPD).

Lesson Summary

- Rights policy templates, also known as RMS templates, are used to enforce the rights that a user or group has on rights-protected content. They allow you to standardize the implementation of AD RMS policies across the organization.
- Exclusion policies allow you to specify accounts, client software, and applications to be denied access to AD RMS. It also allows you to specify a minimum version of the AD RMS client software.