Active Directory Rights Management

Server 2012R2

- **In a nutshell, AD RMS is an information protection technology that is designed to minimize the possibility of data leakage.**

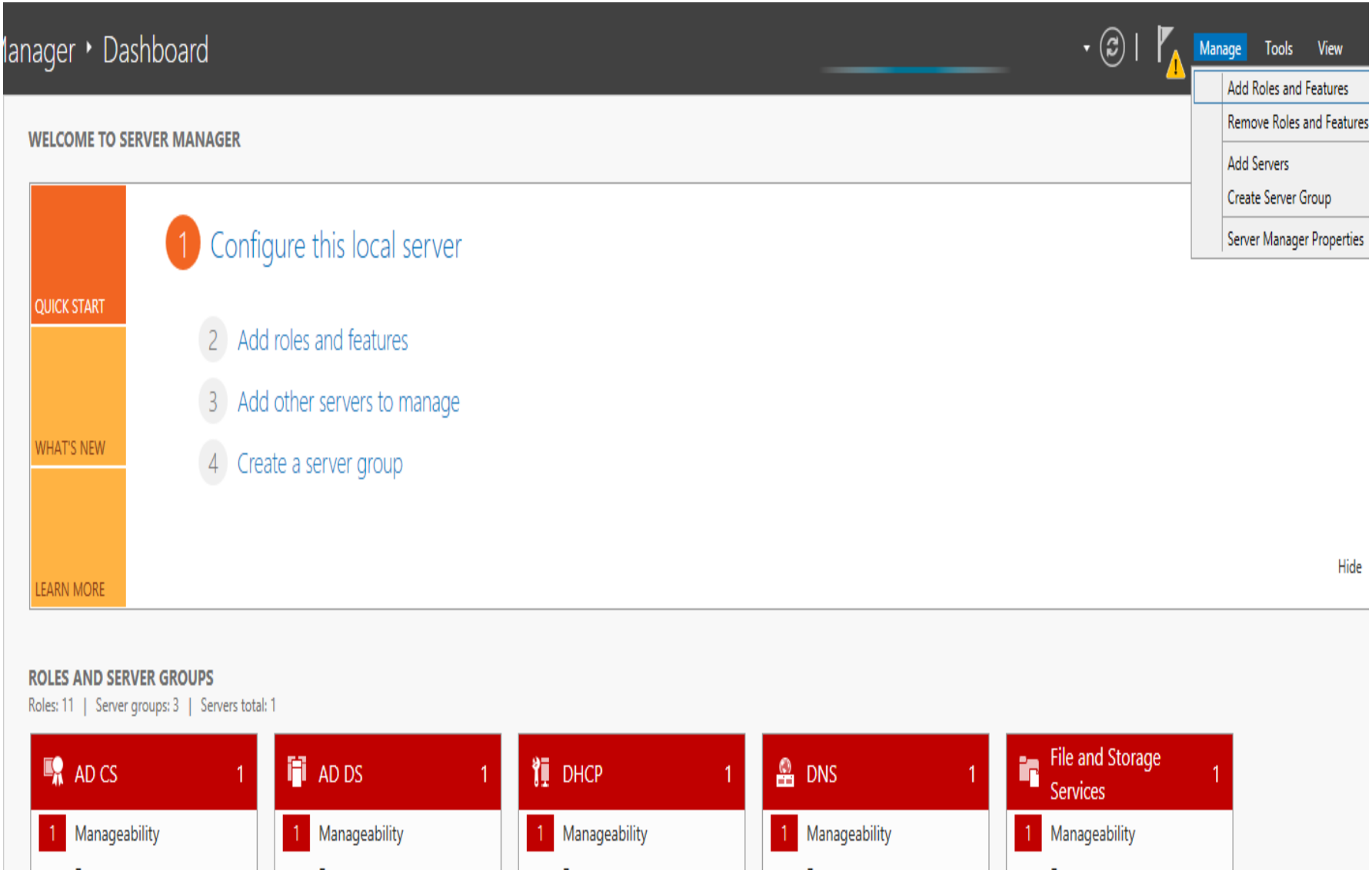
- Data leakage is the unauthorized transmission of information – either to people within the organization or people outside the organization – who should not be able to access that information.

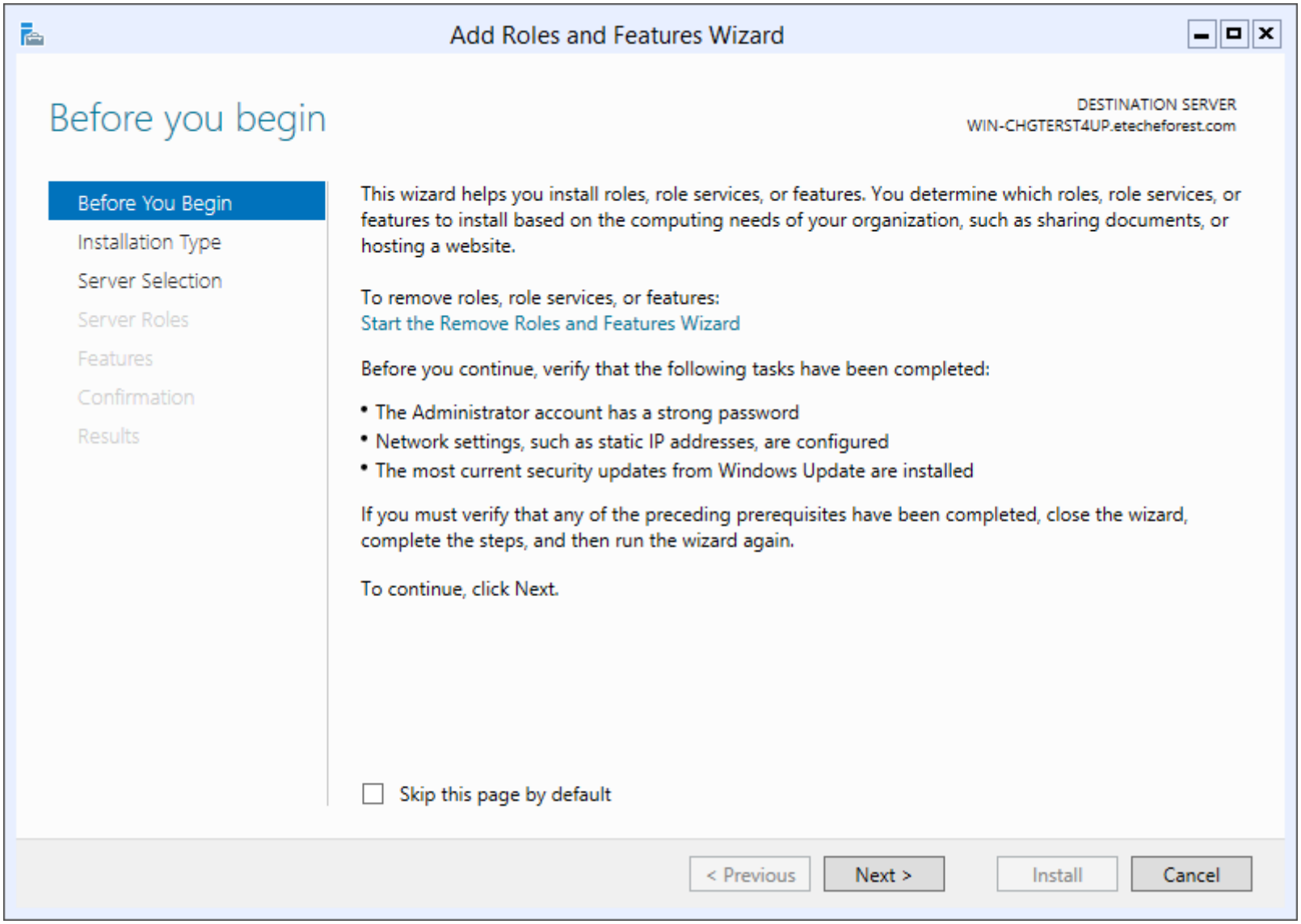
- AD RMS integrates with existing Microsoft products and OS's including Windows Server, Exchange Server, SharePoint Server, and the Microsoft Office Suite.

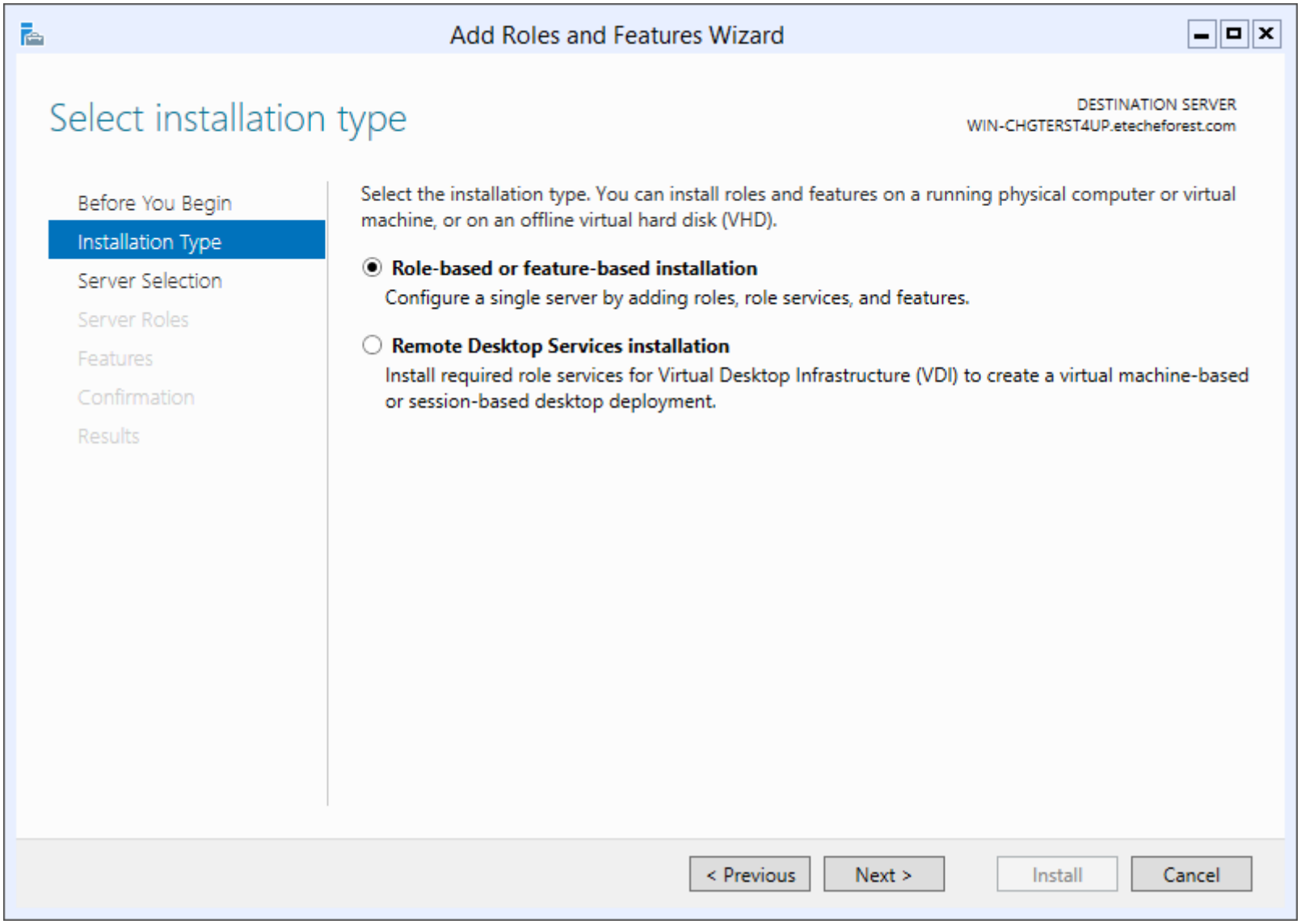
- AD RMS can protect data in transit and at rest. For example, AD RMS can protect documents that are sent as email messages by ensuring that a message cannot be opened even if it is accidentally addressed to the wrong recipient.

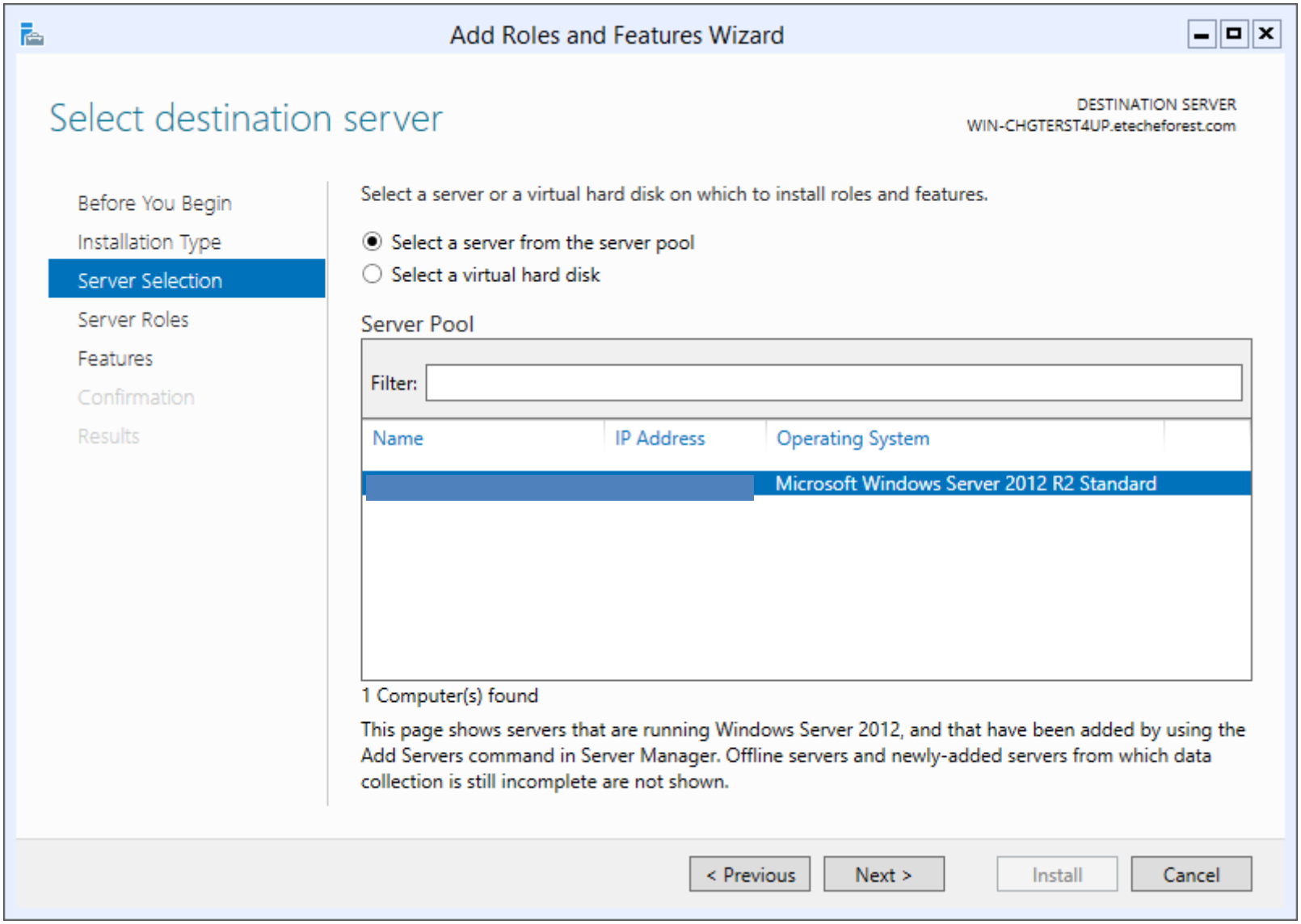
Lets start by **creating ADRMS service account on Domain Server** (Service account – Microsoft recommends using a standard domain user account with additional permissions. You can use a managed service account as the AD RMS service account).

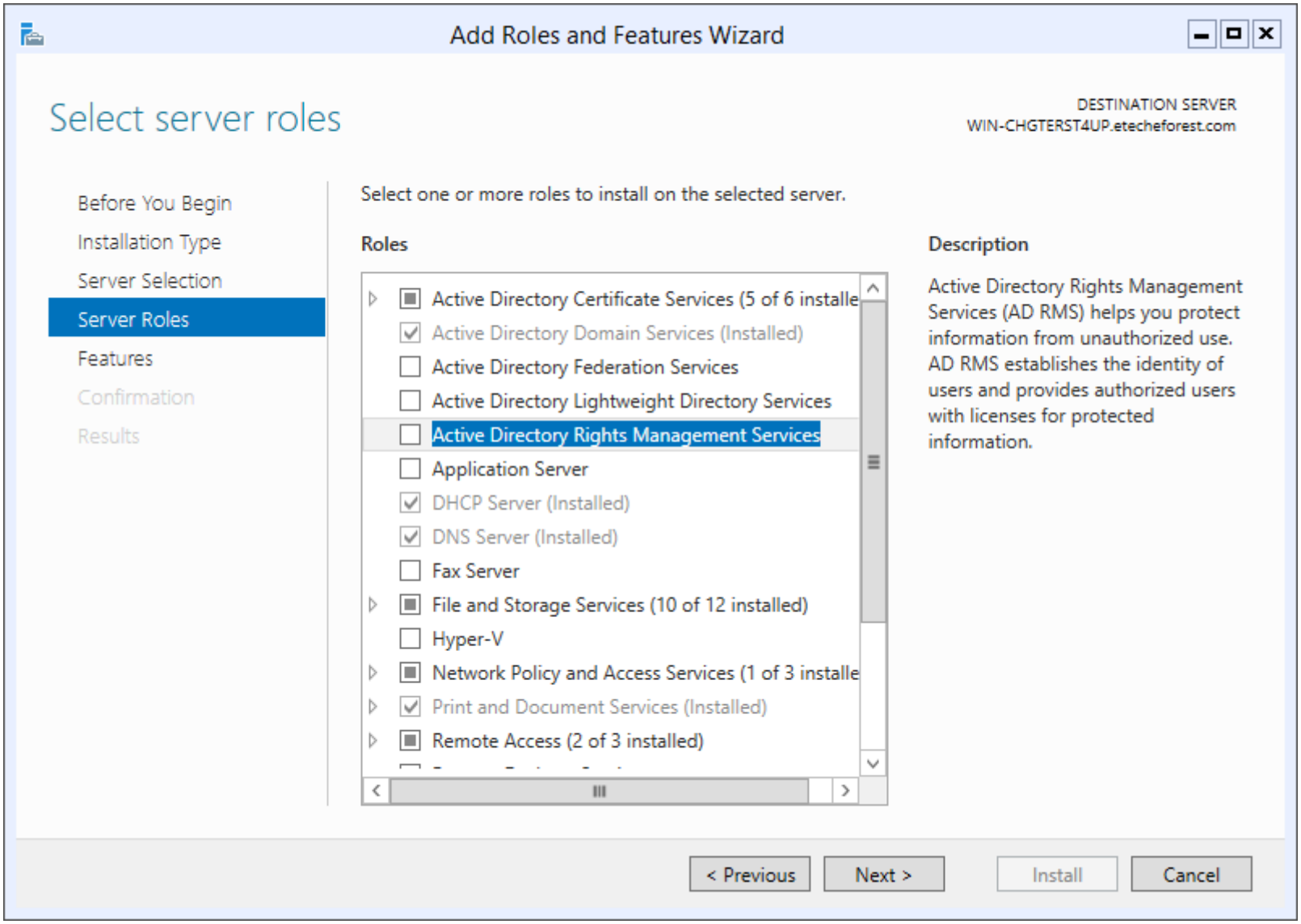
Access Active Directory Users and computers and create a standard user account

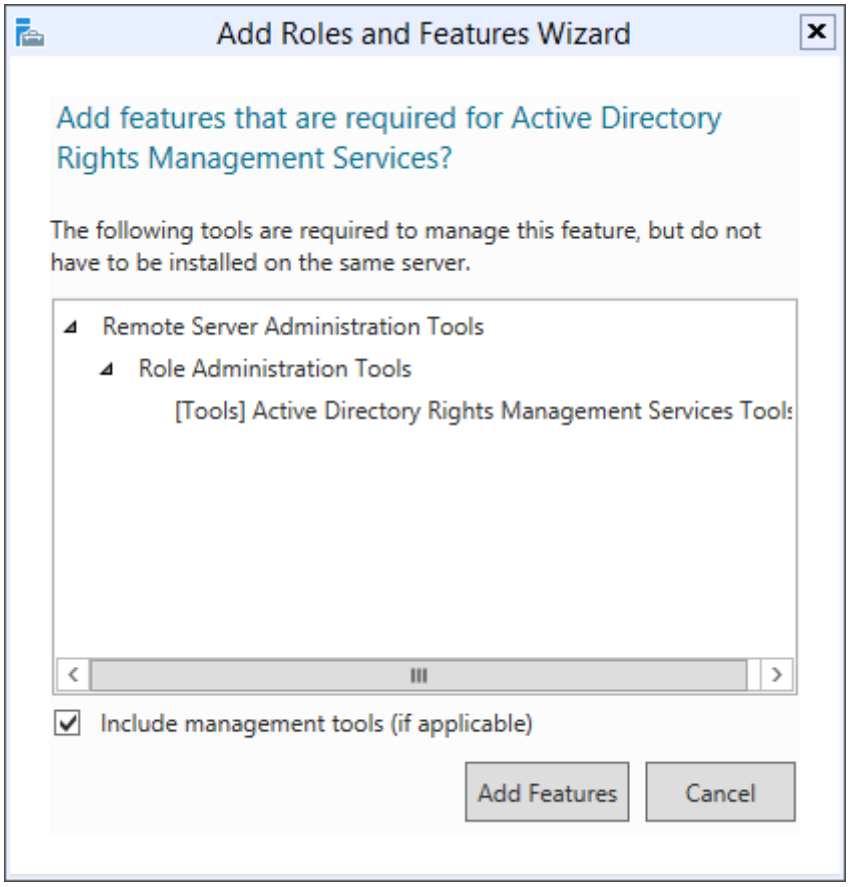

anager ‣ Dashboard
Manage
Tools
View
Add Roles and Features
Remove Roles and Features
Add Servers
Create Server Group
Server Manager Properties
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
Hide
ROLES AND SERVER GROUPS
Roles: 11 | Server groups: 3 | Servers total: 1
AD CS 1
AD DS 1
DHCP 1
DNS 1
File and Storage Services 1
1 Manageability
1 Manageability
1 Manageability
1 Manageability
1 Manageability

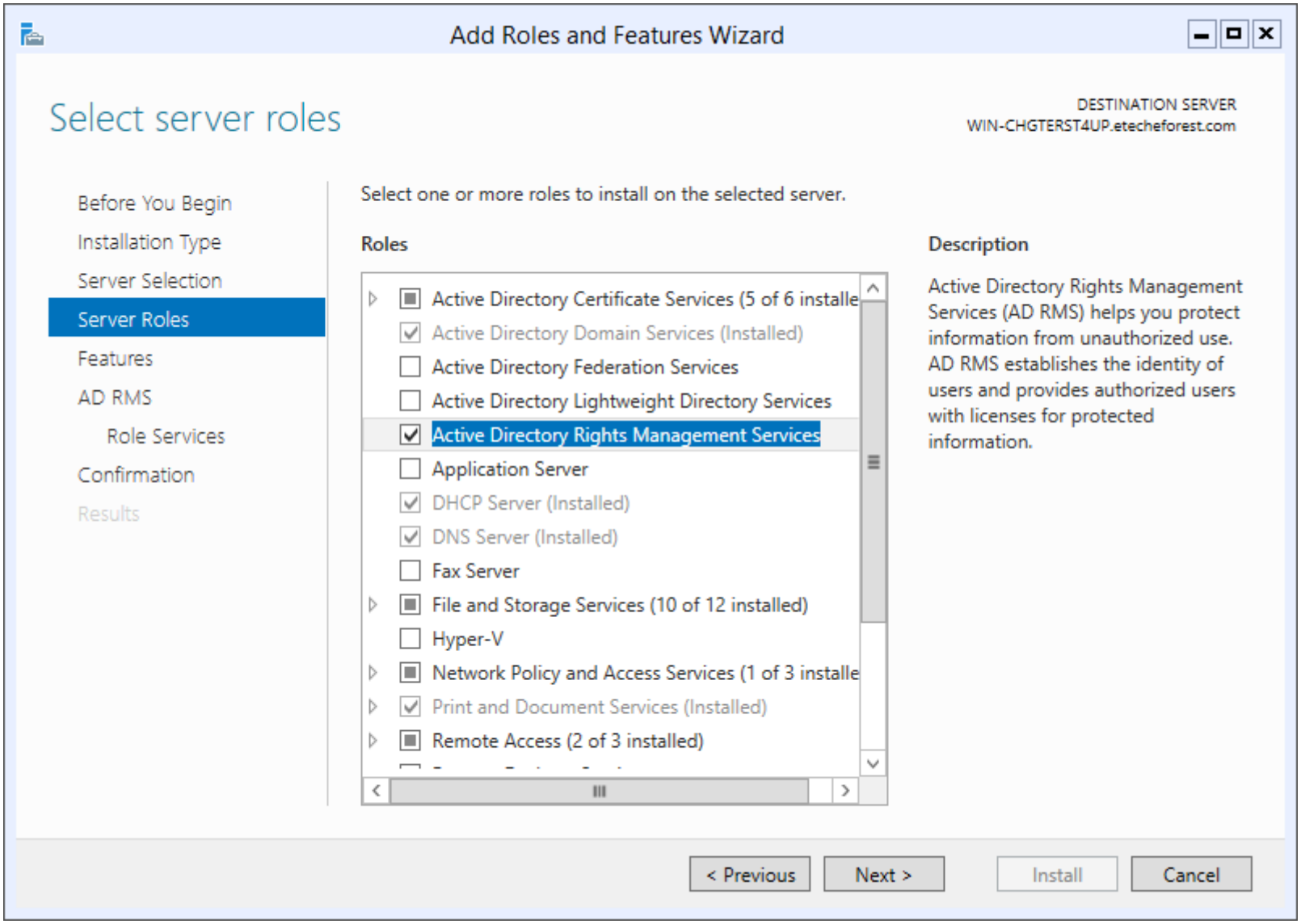

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel

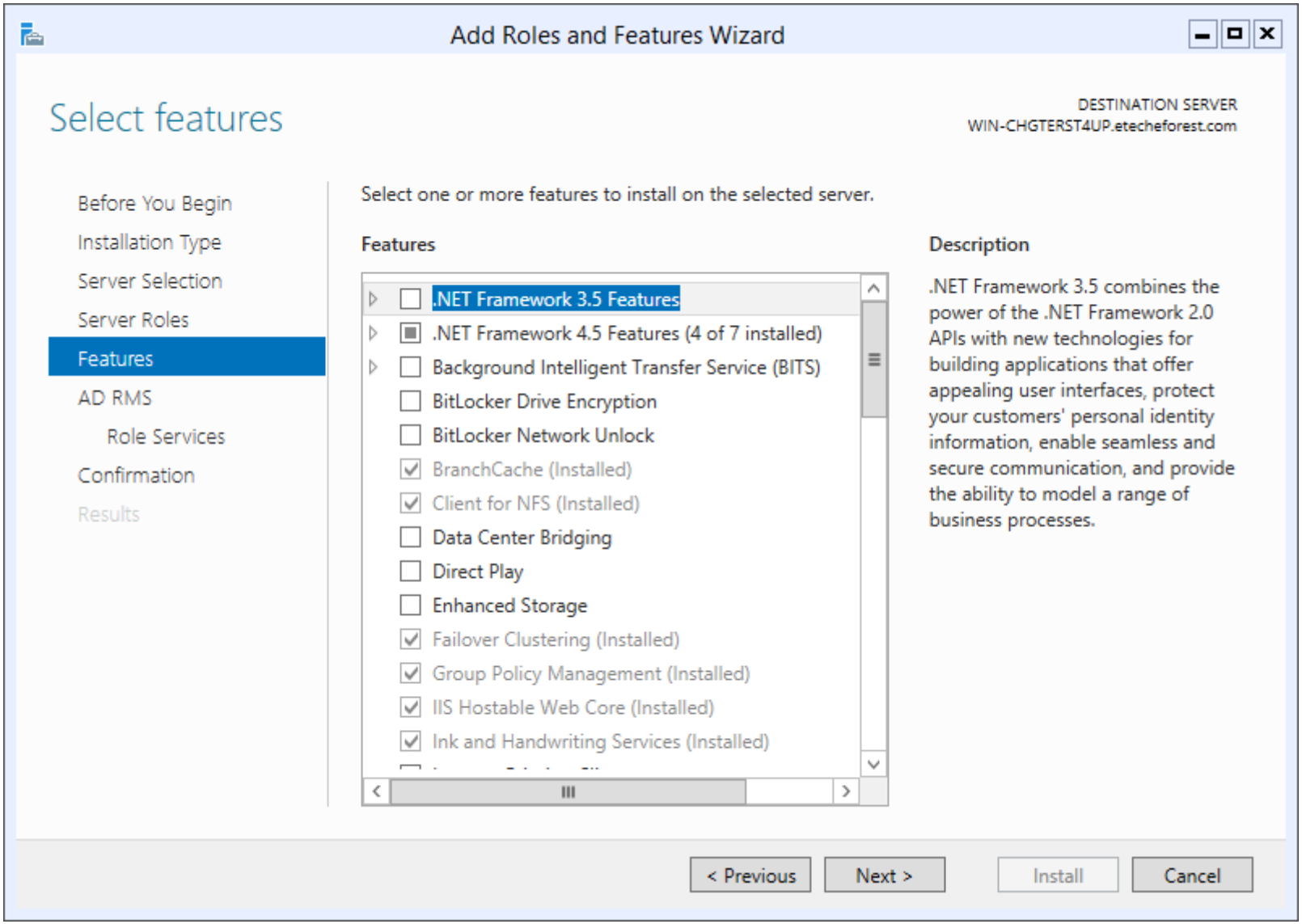

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel

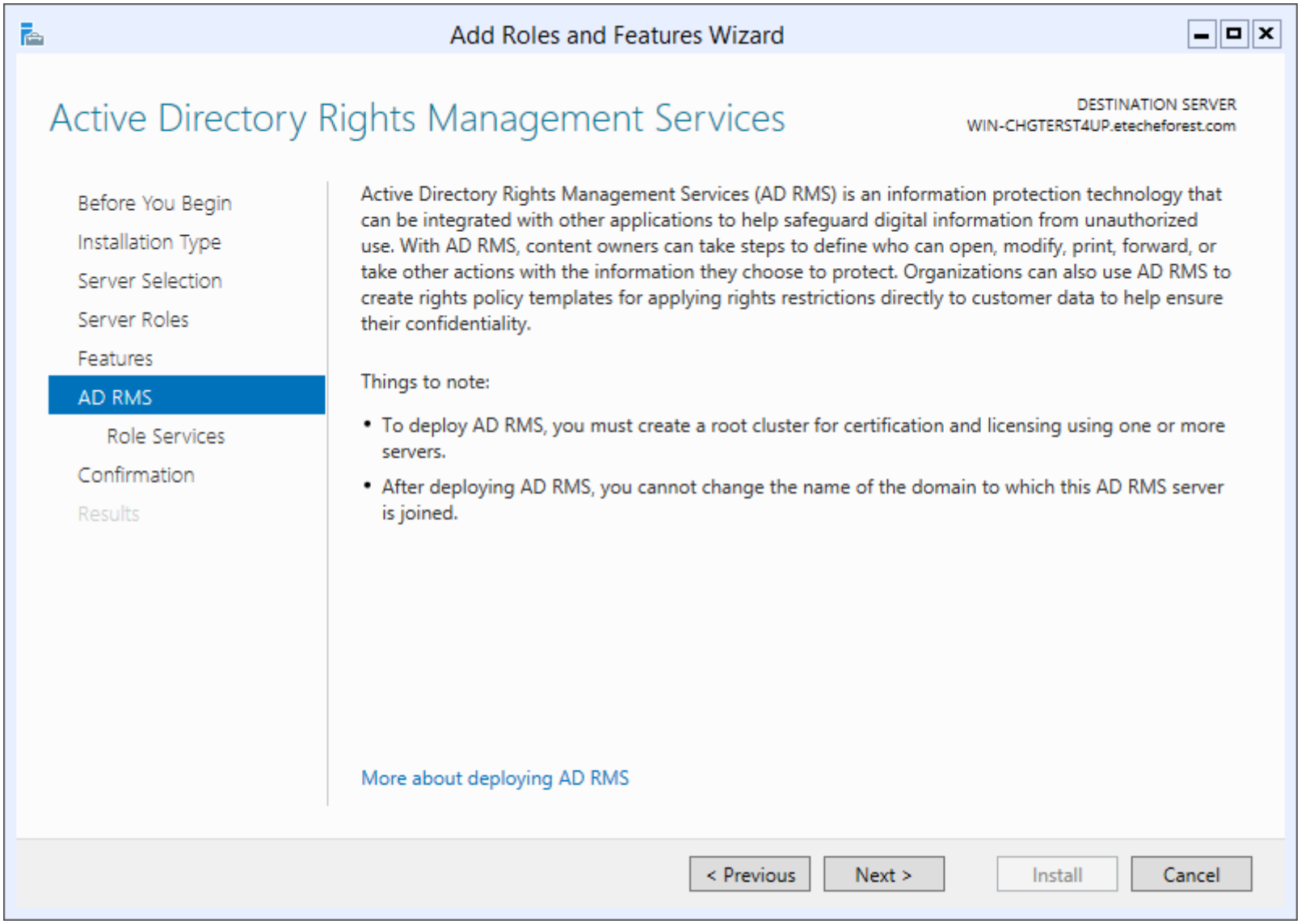

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
Microsoft Windows Server 2012 R2 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

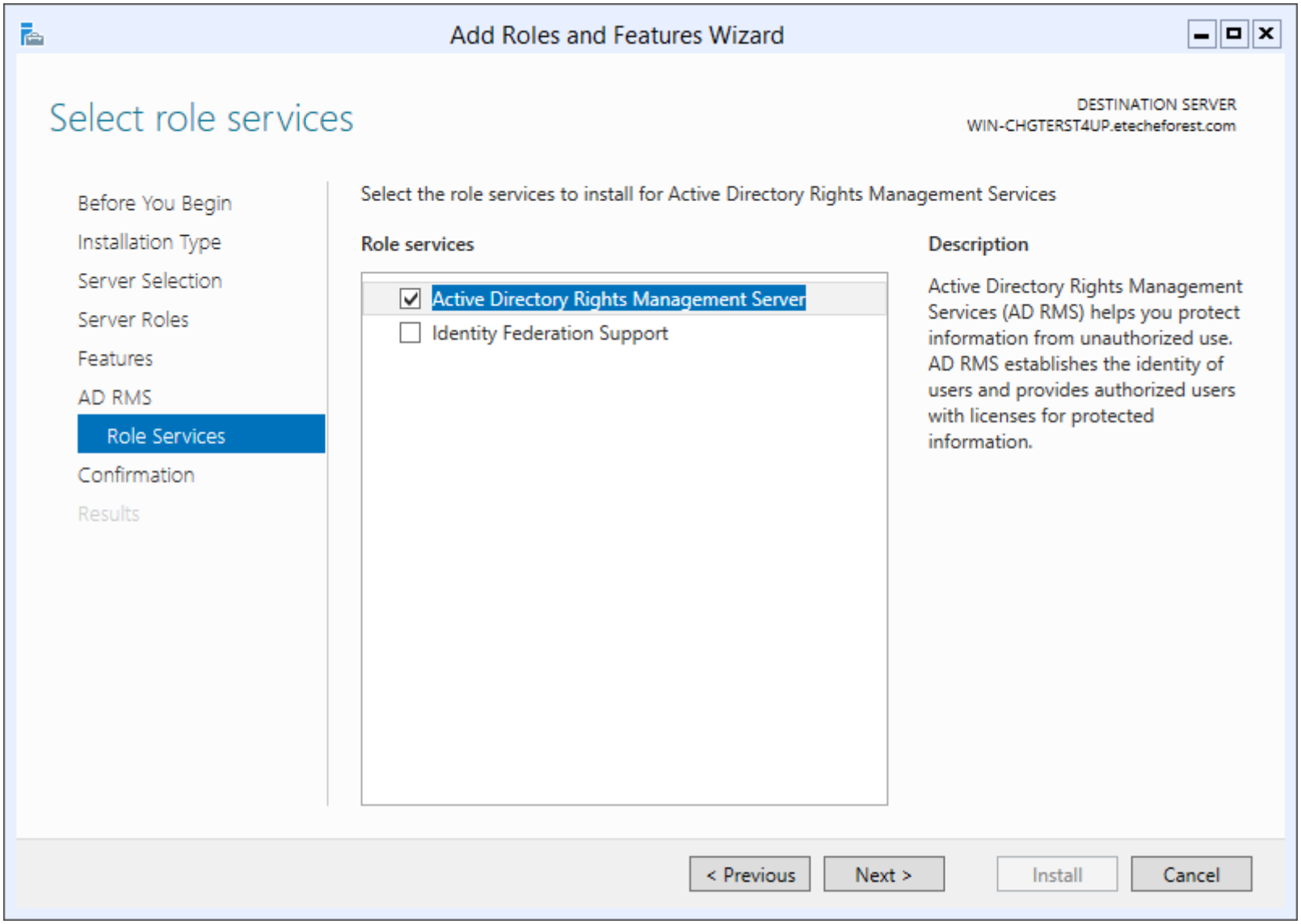

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services (5 of 6 installe
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server (Installed)
DNS Server (Installed)
Fax Server
File and Storage Services (10 of 12 installed)
Hyper-V
Network Policy and Access Services (1 of 3 installe
Print and Document Services (Installed)
Remote Access (2 of 3 installed)
Description
Active Directory Rights Management Services (AD RMS) helps you protect information from unauthorized use. AD RMS establishes the identity of users and provides authorized users with licenses for protected information.
< Previous
Next >
Install
Cancel

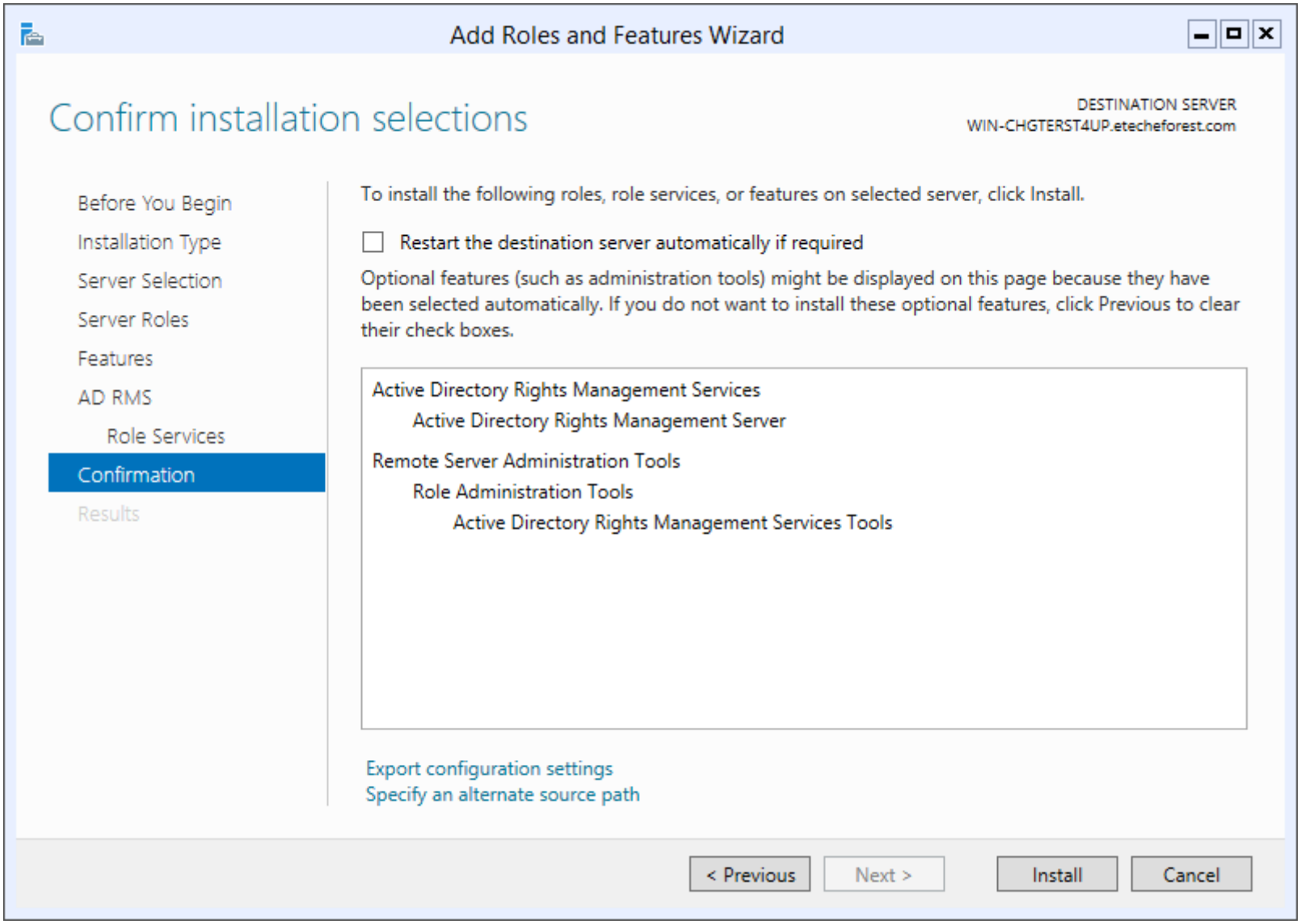

Add Roles and Features Wizard
Add features that are required for Active Directory Rights Management Services?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] Active Directory Rights Management Services Tools
Include management tools (if applicable)
Add Features
Cancel

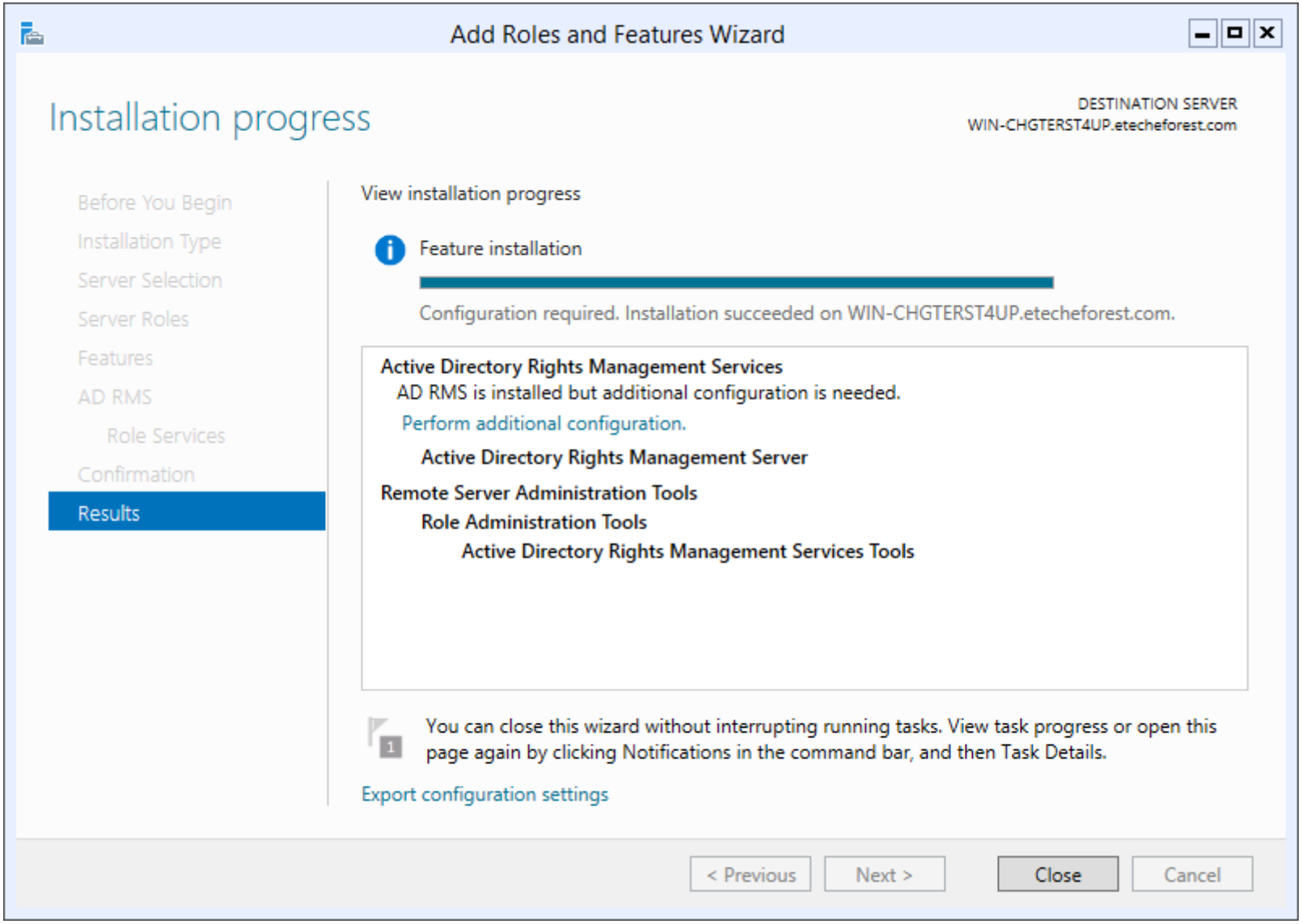

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD RMS
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services (5 of 6 installe
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server (Installed)
DNS Server (Installed)
Fax Server
File and Storage Services (10 of 12 installed)
Hyper-V
Network Policy and Access Services (1 of 3 installe
Print and Document Services (Installed)
Remote Access (2 of 3 installed)
Description
Active Directory Rights Management Services (AD RMS) helps you protect information from unauthorized use. AD RMS establishes the identity of users and provides authorized users with licenses for protected information.
< Previous
Next >
Install
Cancel

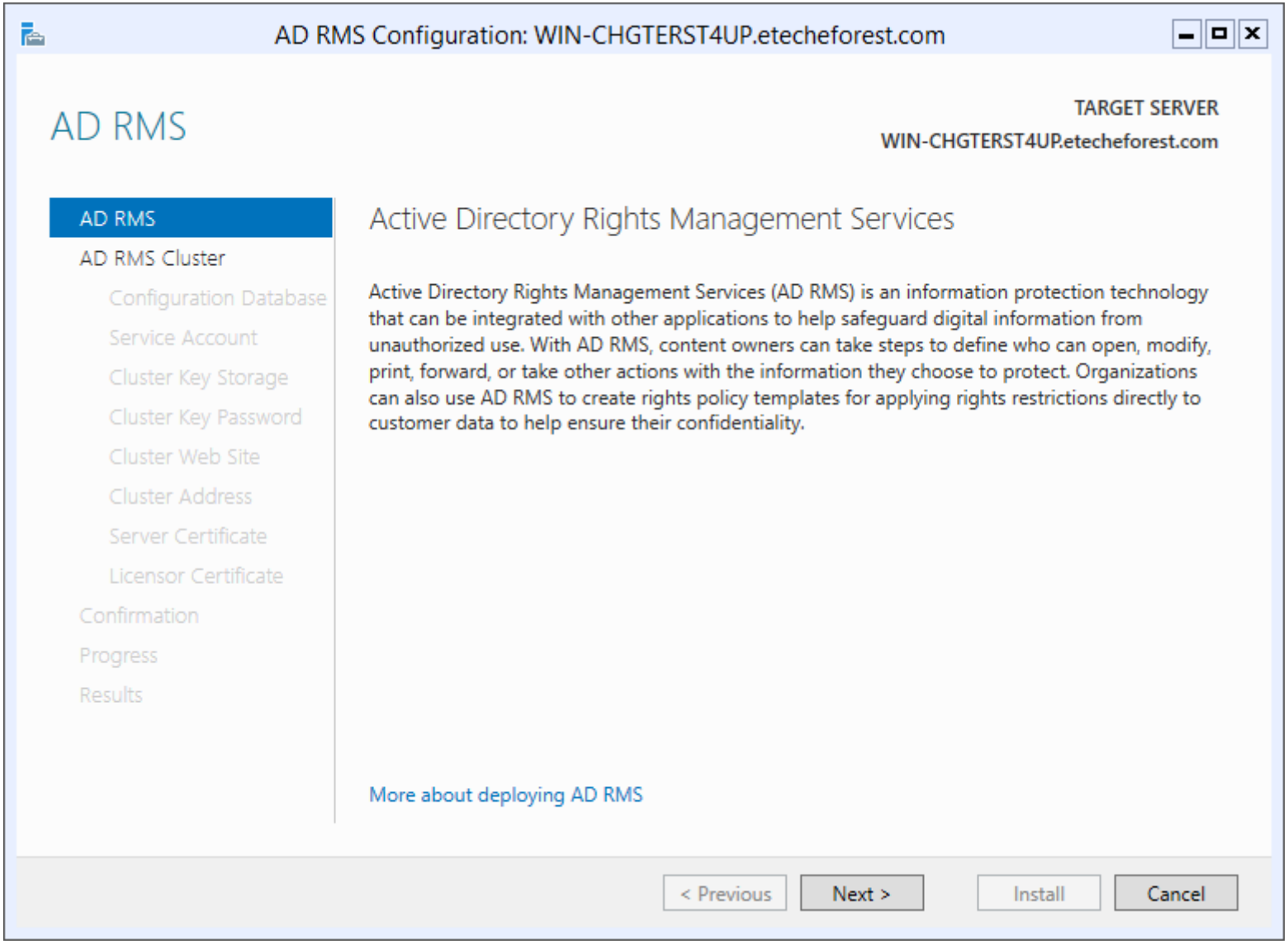

Add Roles and Features Wizard
Select features
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD RMS
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.5 Features (4 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache (Installed)
Client for NFS (Installed)
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering (Installed)
Group Policy Management (Installed)
IIS Hostable Web Core (Installed)
Ink and Handwriting Services (Installed)
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

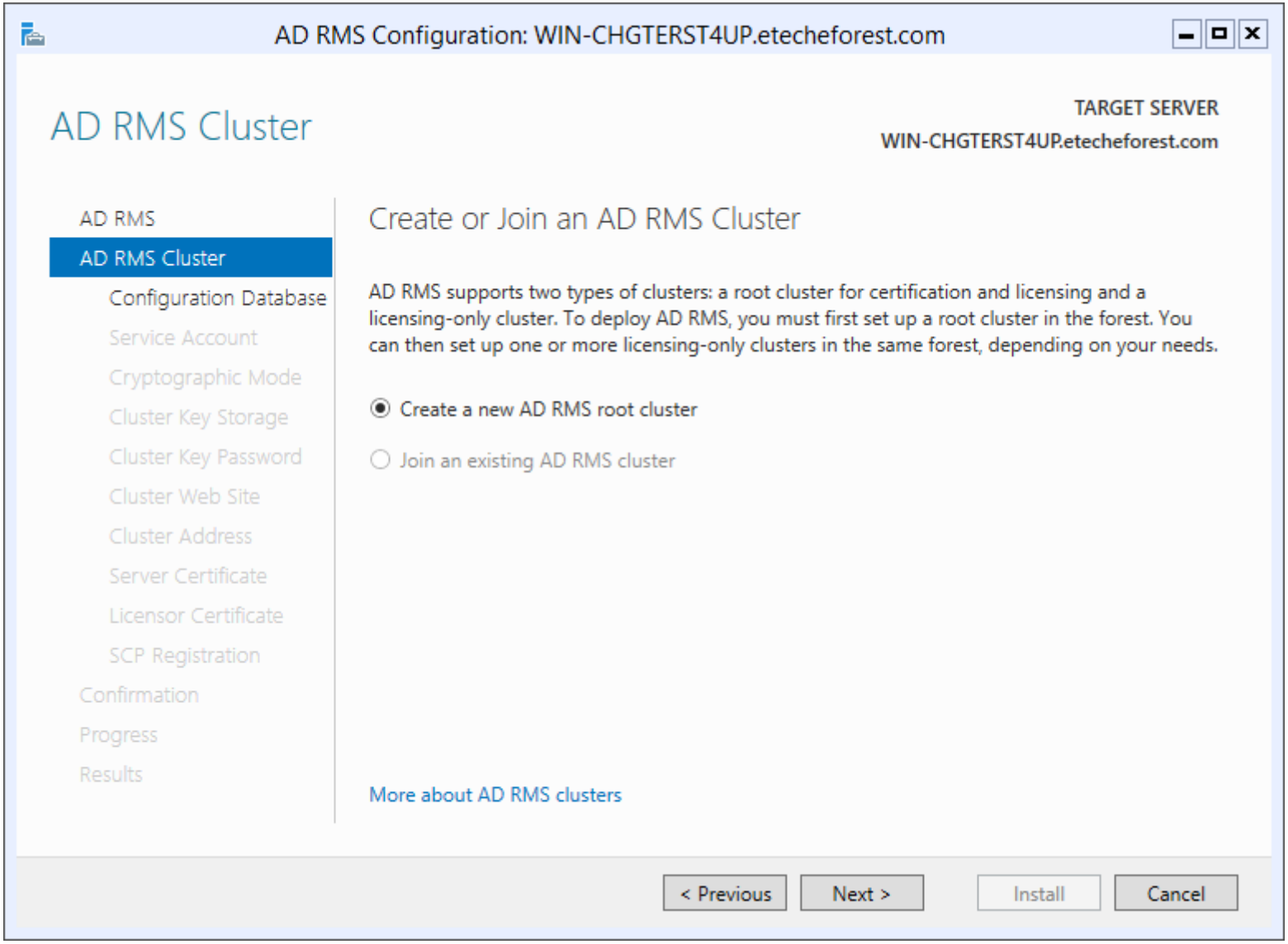

Add Roles and Features Wizard
Active Directory Rights Management Services
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD RMS
Role Services
Confirmation
Results
Active Directory Rights Management Services (AD RMS) is an information protection technology that can be integrated with other applications to help safeguard digital information from unauthorized use. With AD RMS, content owners can take steps to define who can open, modify, print, forward, or take other actions with the information they choose to protect. Organizations can also use AD RMS to create rights policy templates for applying rights restrictions directly to customer data to help ensure their confidentiality.
Things to note:
• To deploy AD RMS, you must create a root cluster for certification and licensing using one or more servers.
• After deploying AD RMS, you cannot change the name of the domain to which this AD RMS server is joined.
More about deploying AD RMS
< Previous
Next >
Install
Cancel

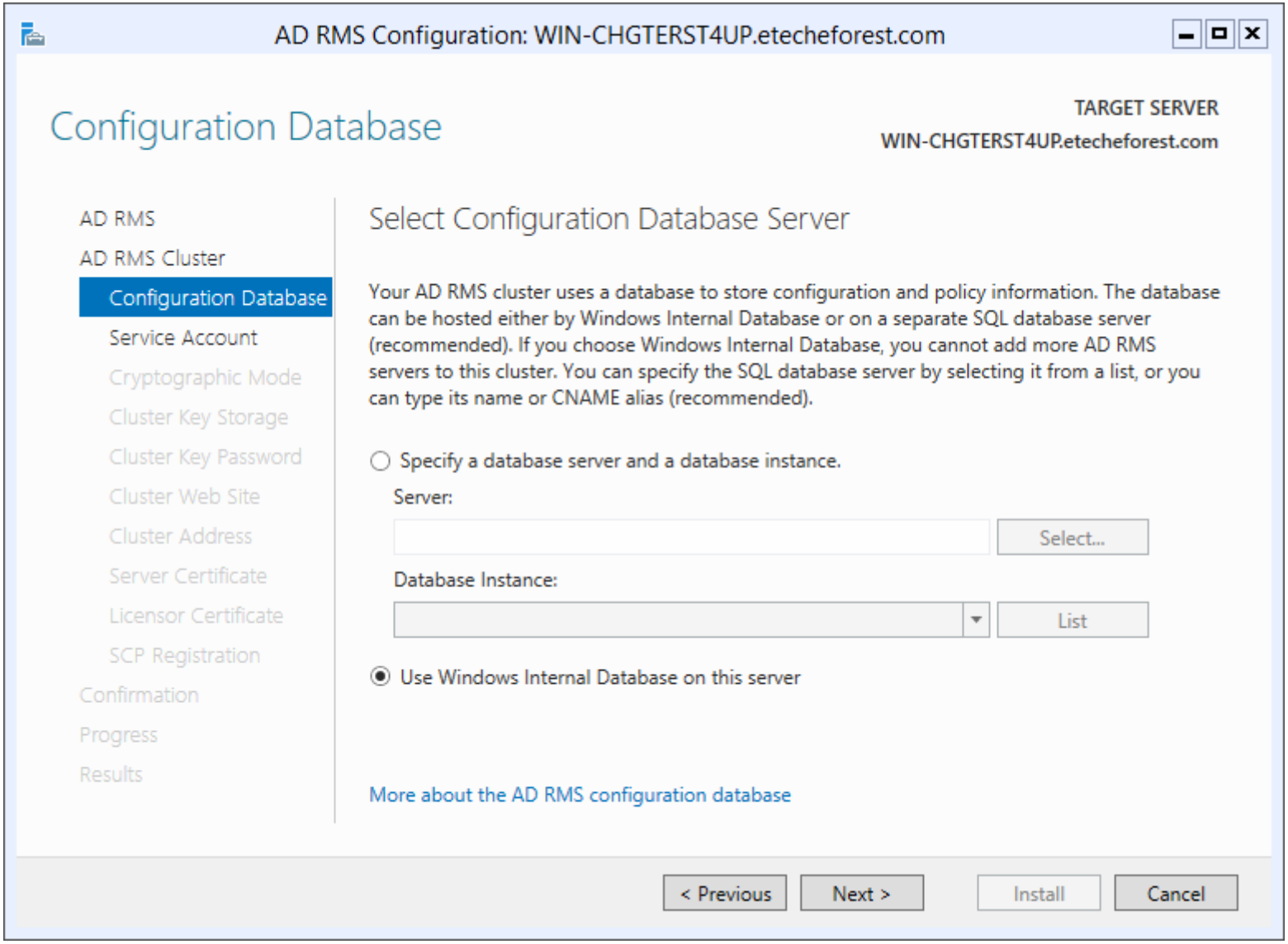

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD RMS
Role Services
Confirmation
Results
Select the role services to install for Active Directory Rights Management Services
Role services
Active Directory Rights Management Server
Identity Federation Support
Description
Active Directory Rights Management Services (AD RMS) helps you protect information from unauthorized use. AD RMS establishes the identity of users and provides authorized users with licenses for protected information.
< Previous
Next >
Install
Cancel

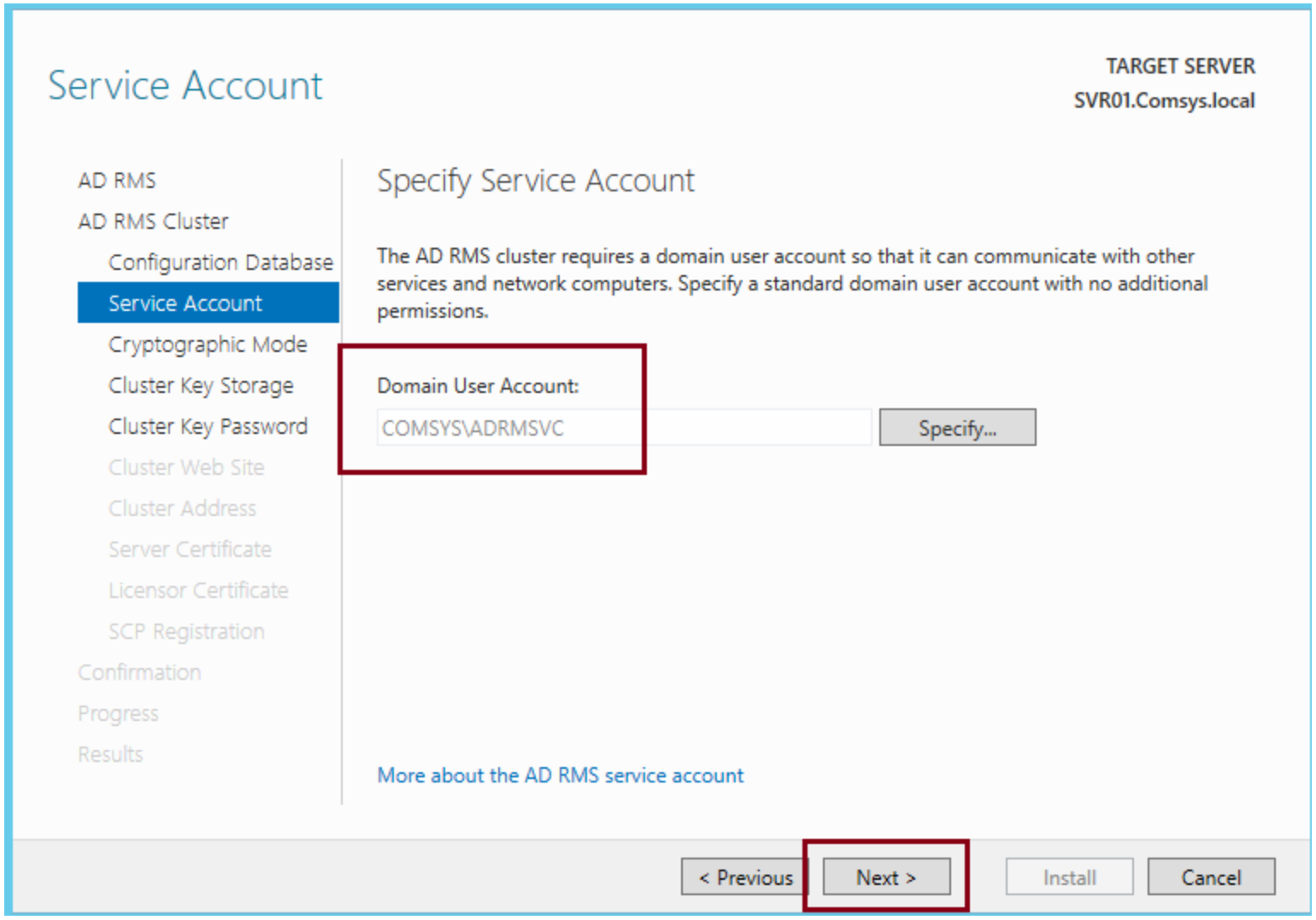

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD RMS
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Rights Management Services
Active Directory Rights Management Server
Remote Server Administration Tools
Role Administration Tools
Active Directory Rights Management Services Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

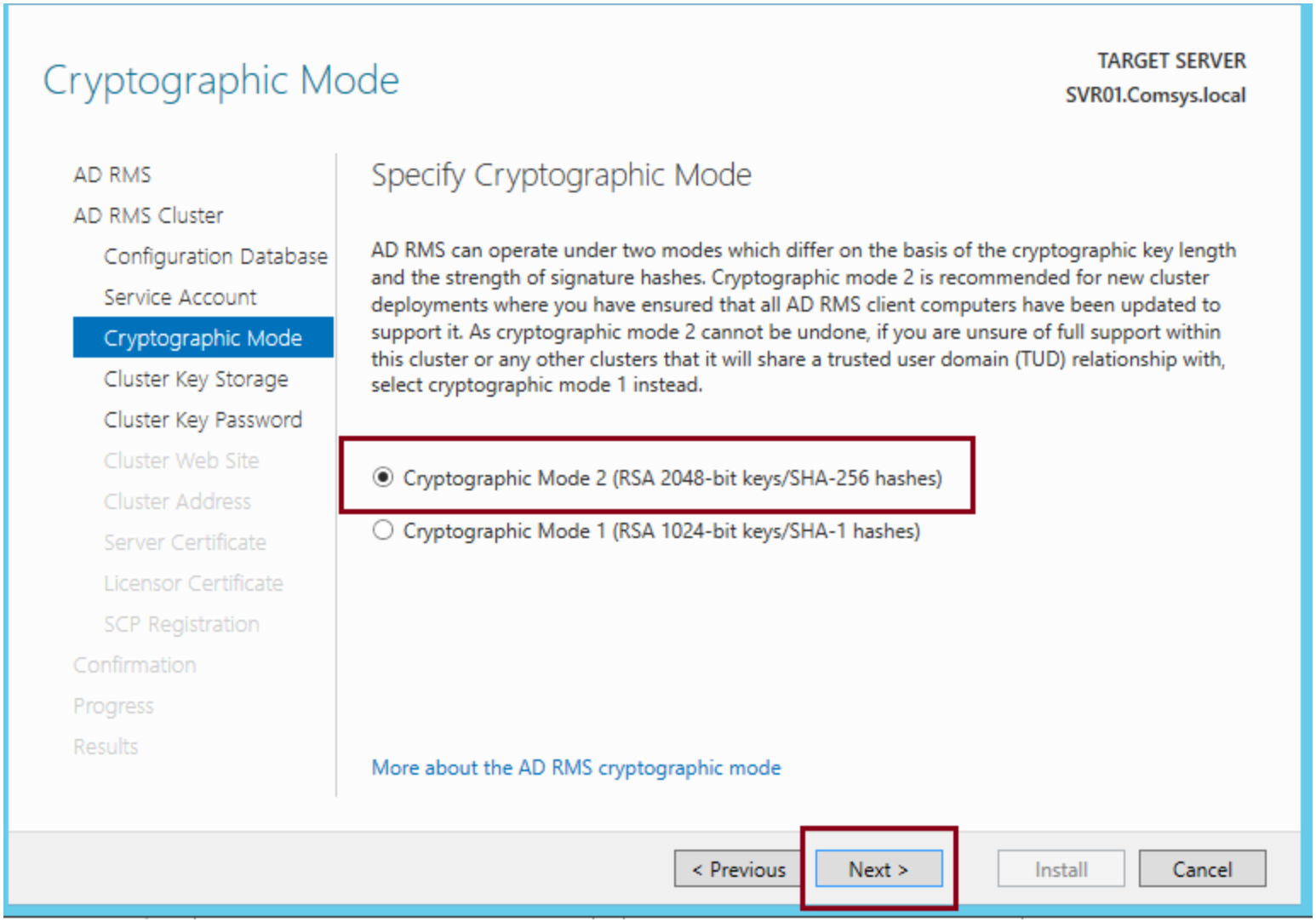

Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
WIN-CHGTERST4UP.etecheforest.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD RMS
Role Services
Confirmation
Results
View installation progress
Feature installation
Configuration required. Installation succeeded on WIN-CHGTERST4UP.etecheforest.com.
Active Directory Rights Management Services
AD RMS is installed but additional configuration is needed.
Perform additional configuration.
Active Directory Rights Management Server
Remote Server Administration Tools
Role Administration Tools
Active Directory Rights Management Services Tools
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel

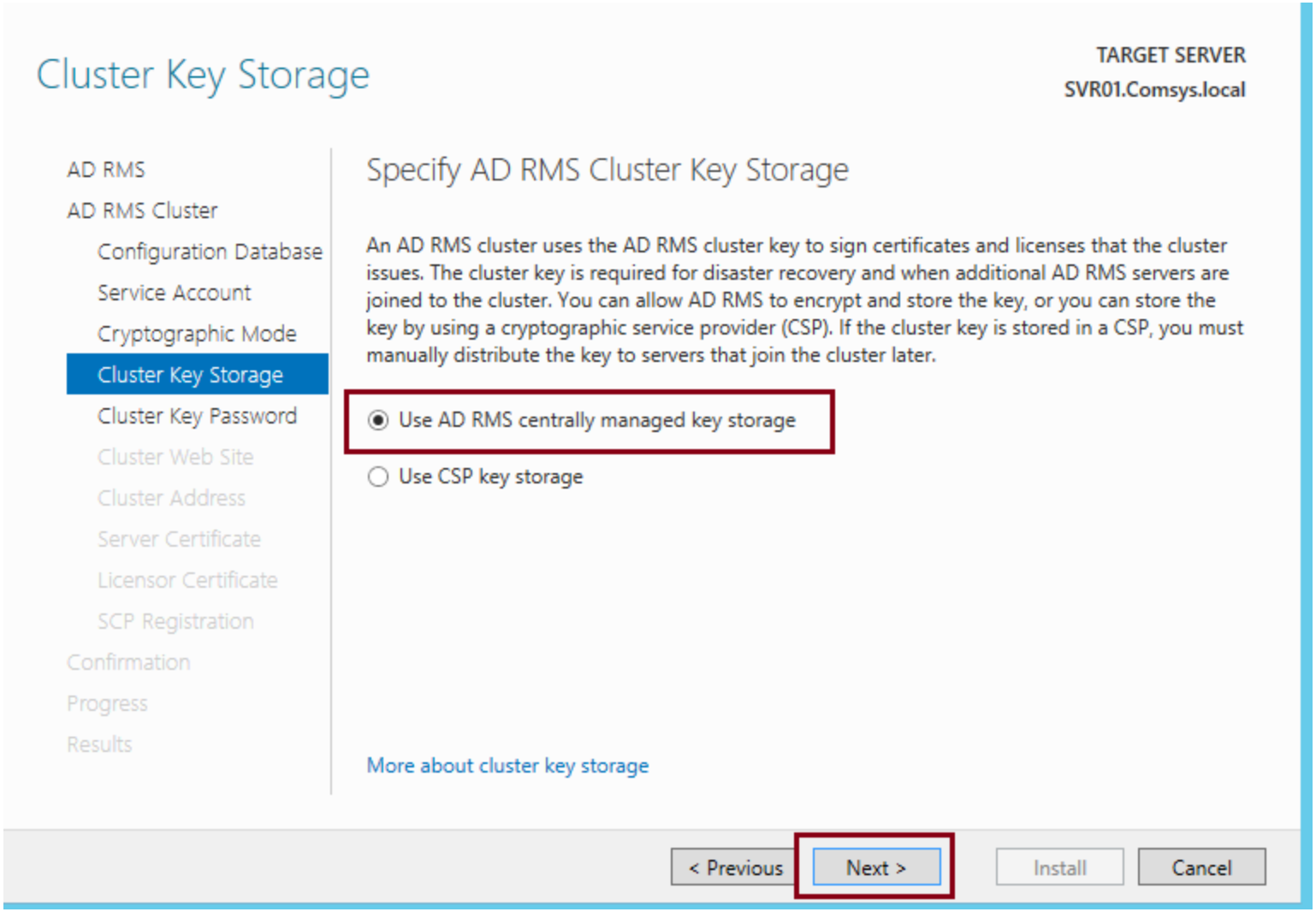

AD RMS Configuration: WIN-CHGTERST4UP.etecheforest.com
AD RMS
TARGET SERVER
WIN-CHGTERST4UP.etecheforest.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
Confirmation
Progress
Results
Active Directory Rights Management Services
Active Directory Rights Management Services (AD RMS) is an information protection technology that can be integrated with other applications to help safeguard digital information from unauthorized use. With AD RMS, content owners can take steps to define who can open, modify, print, forward, or take other actions with the information they choose to protect. Organizations can also use AD RMS to create rights policy templates for applying rights restrictions directly to customer data to help ensure their confidentiality.
More about deploying AD RMS
< Previous
Next >
Install
Cancel

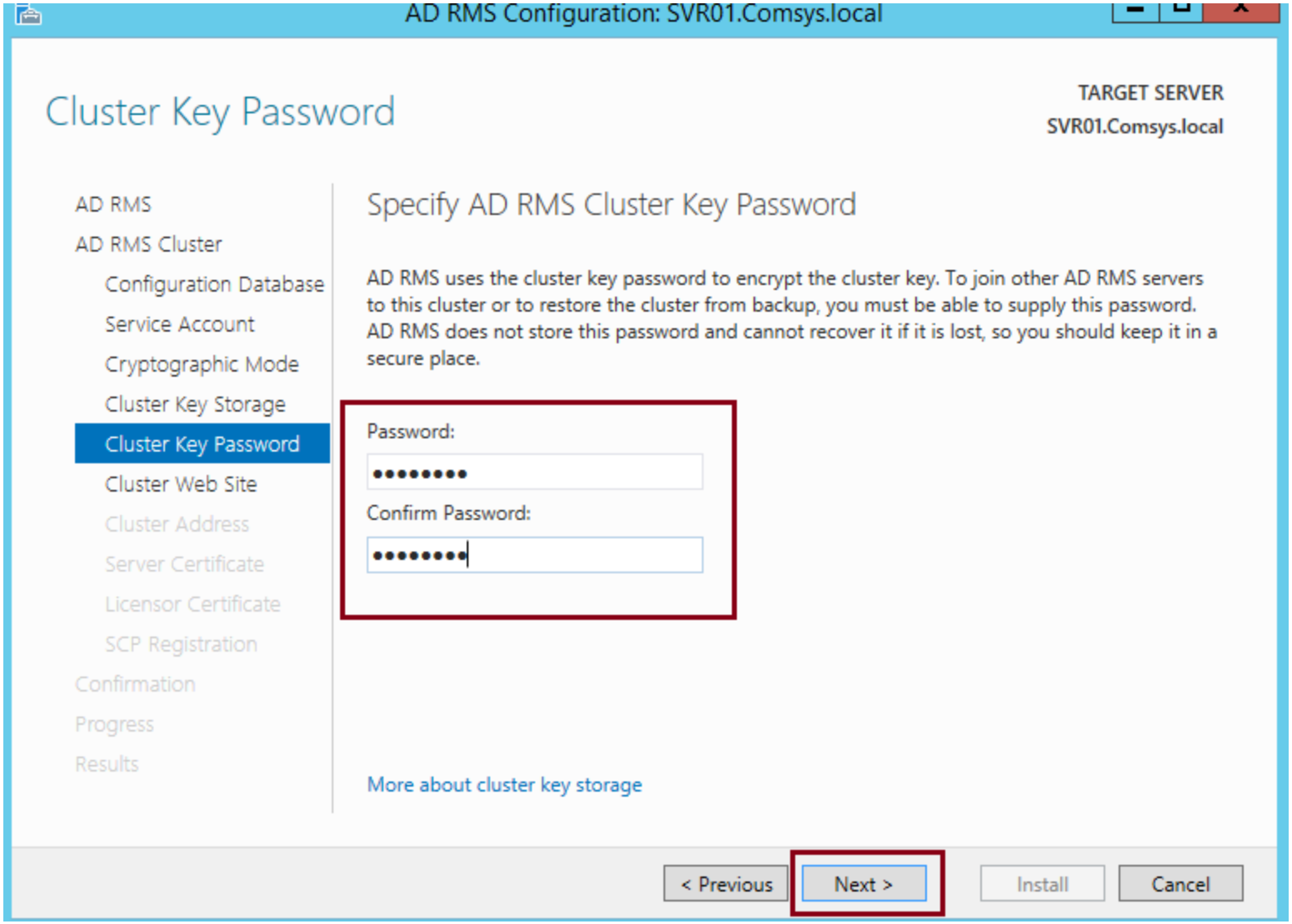

AD RMS Configuration: WIN-CHGTERST4UP.etecheforest.com
AD RMS Cluster
TARGET SERVER
WIN-CHGTERST4UP.etecheforest.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Create or Join an AD RMS Cluster
AD RMS supports two types of clusters: a root cluster for certification and licensing and a licensing-only cluster. To deploy AD RMS, you must first set up a root cluster in the forest. You can then set up one or more licensing-only clusters in the same forest, depending on your needs.
Create a new AD RMS root cluster
Join an existing AD RMS cluster
More about AD RMS clusters
< Previous
Next >
Install
Cancel

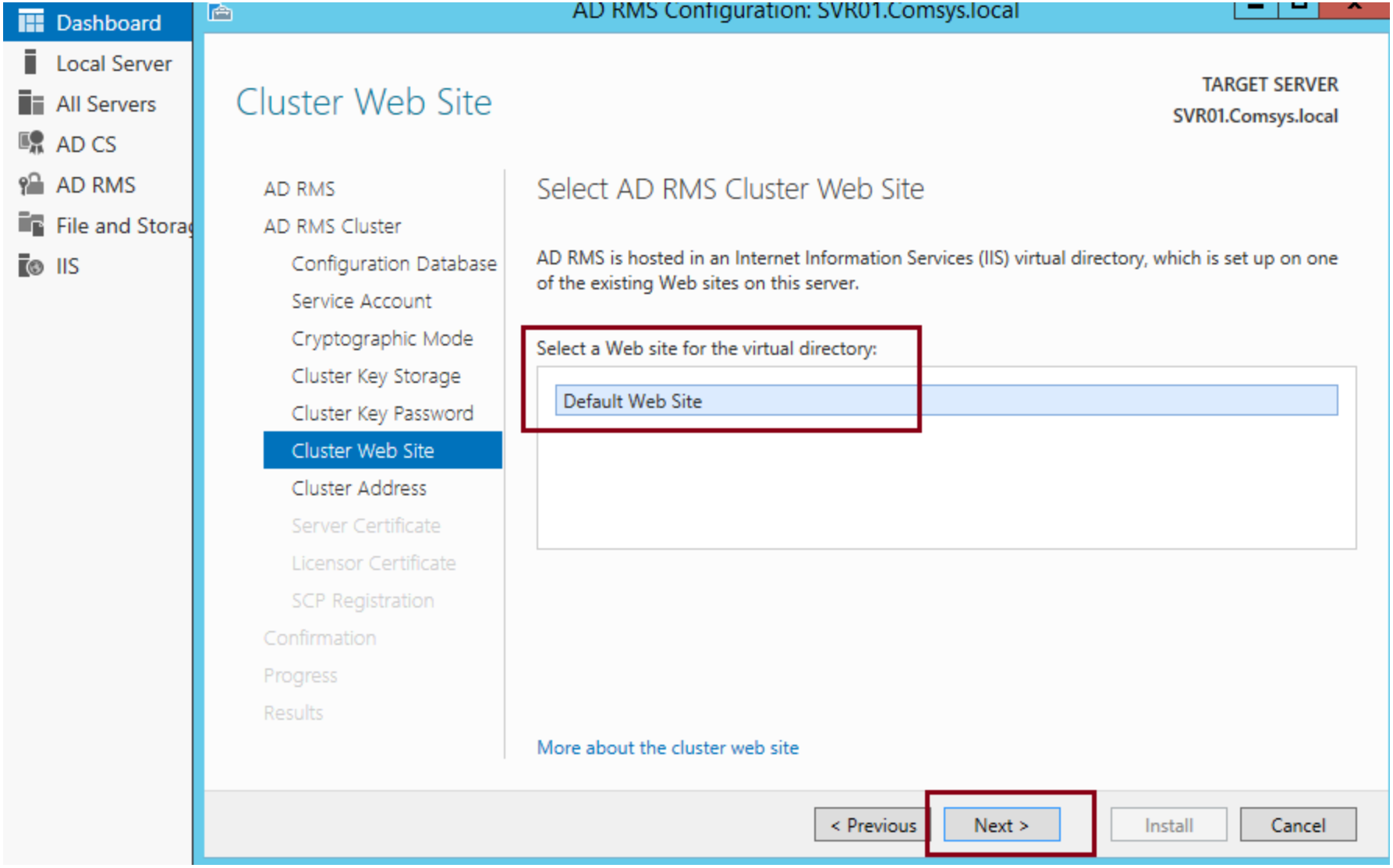

AD RMS Configuration: WIN-CHGTERST4UP.etecheforest.com
Configuration Database
TARGET SERVER
WIN-CHGTERST4UP.etecheforest.com
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Select Configuration Database Server
Your AD RMS cluster uses a database to store configuration and policy information. The database can be hosted either by Windows Internal Database or on a separate SQL database server (recommended). If you choose Windows Internal Database, you cannot add more AD RMS servers to this cluster. You can specify the SQL database server by selecting it from a list, or you can type its name or CNAME alias (recommended).
Specify a database server and a database instance.
Server:
Select...
Database Instance:
List
Use Windows Internal Database on this server
More about the AD RMS configuration database
< Previous
Next >
Install
Cancel

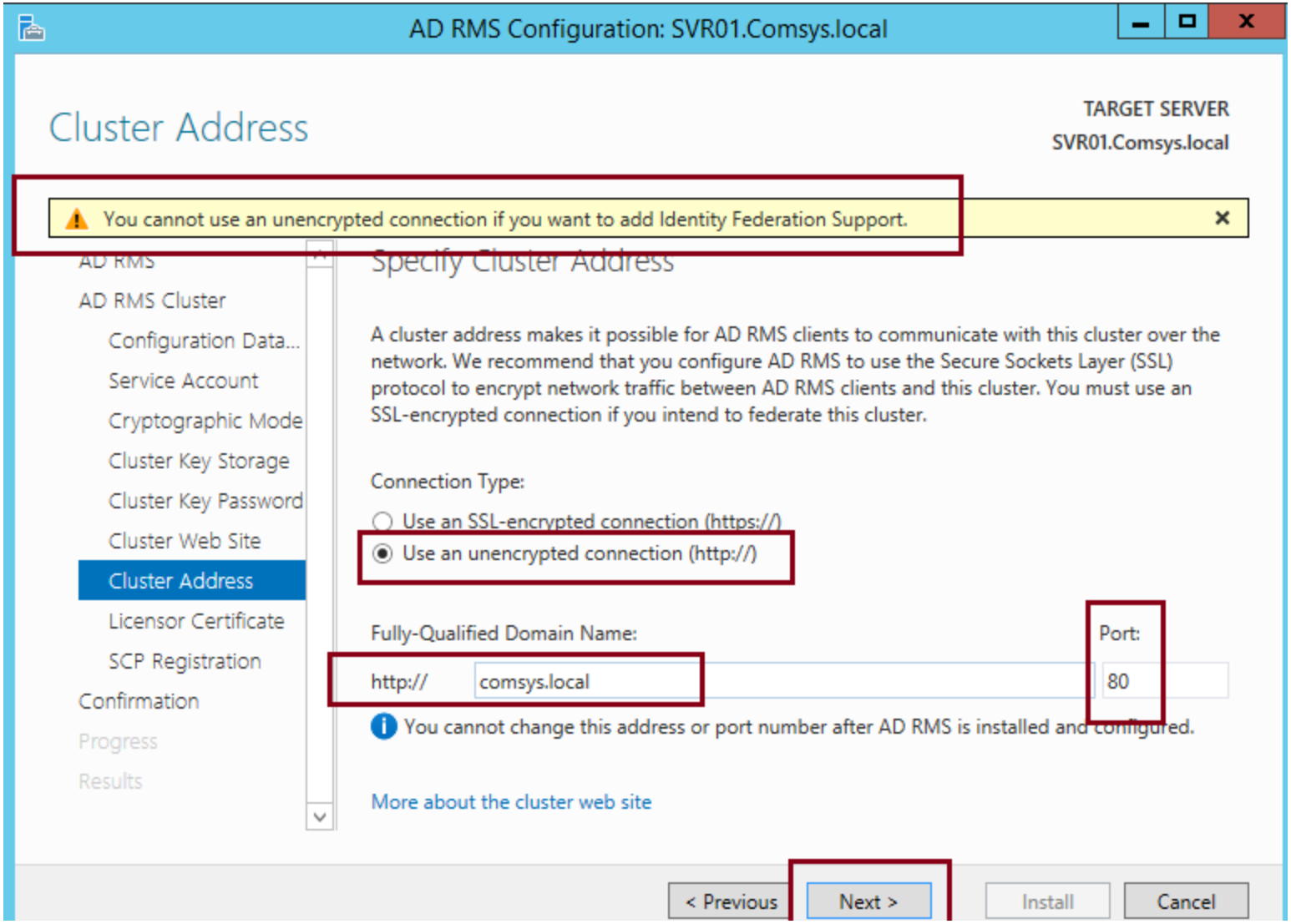

Service Account
TARGET SERVER
SVR01.Comsys.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Service Account
The AD RMS cluster requires a domain user account so that it can communicate with other services and network computers. Specify a standard domain user account with no additional permissions.
Domain User Account:
COMSYS\ADRMSVC
Specify...
More about the AD RMS service account
< Previous
Next >
Install
Cancel

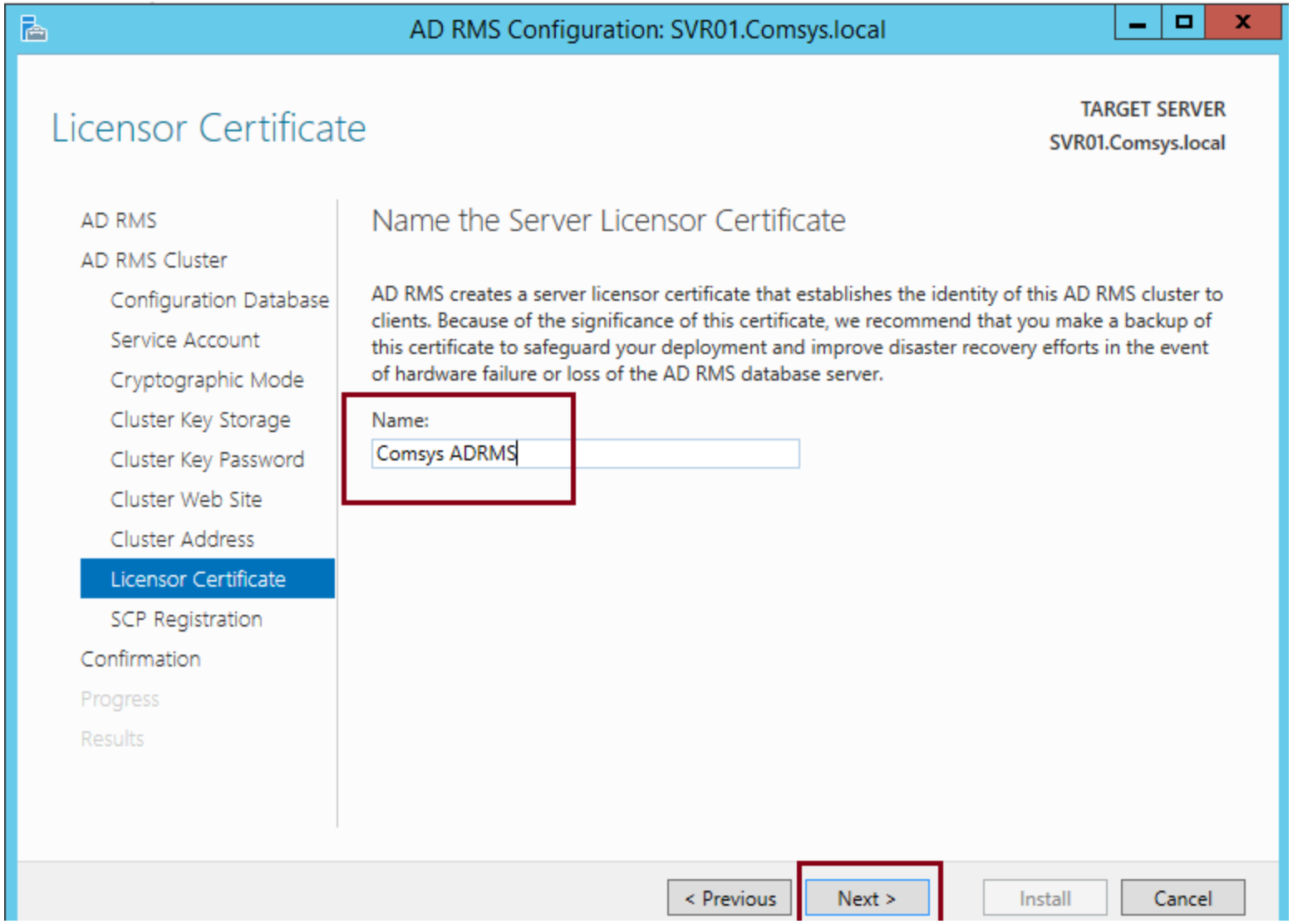

Cryptographic Mode
TARGET SERVER
SVR01.Comsys.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Cryptographic Mode
AD RMS can operate under two modes which differ on the basis of the cryptographic key length and the strength of signature hashes. Cryptographic mode 2 is recommended for new cluster deployments where you have ensured that all AD RMS client computers have been updated to support it. As cryptographic mode 2 cannot be undone, if you are unsure of full support within this cluster or any other clusters that it will share a trusted user domain (TUD) relationship with, select cryptographic mode 1 instead.
Cryptographic Mode 2 (RSA 2048-bit keys/SHA-256 hashes)
Cryptographic Mode 1 (RSA 1024-bit keys/SHA-1 hashes)
More about the AD RMS cryptographic mode
< Previous
Next >
Install
Cancel

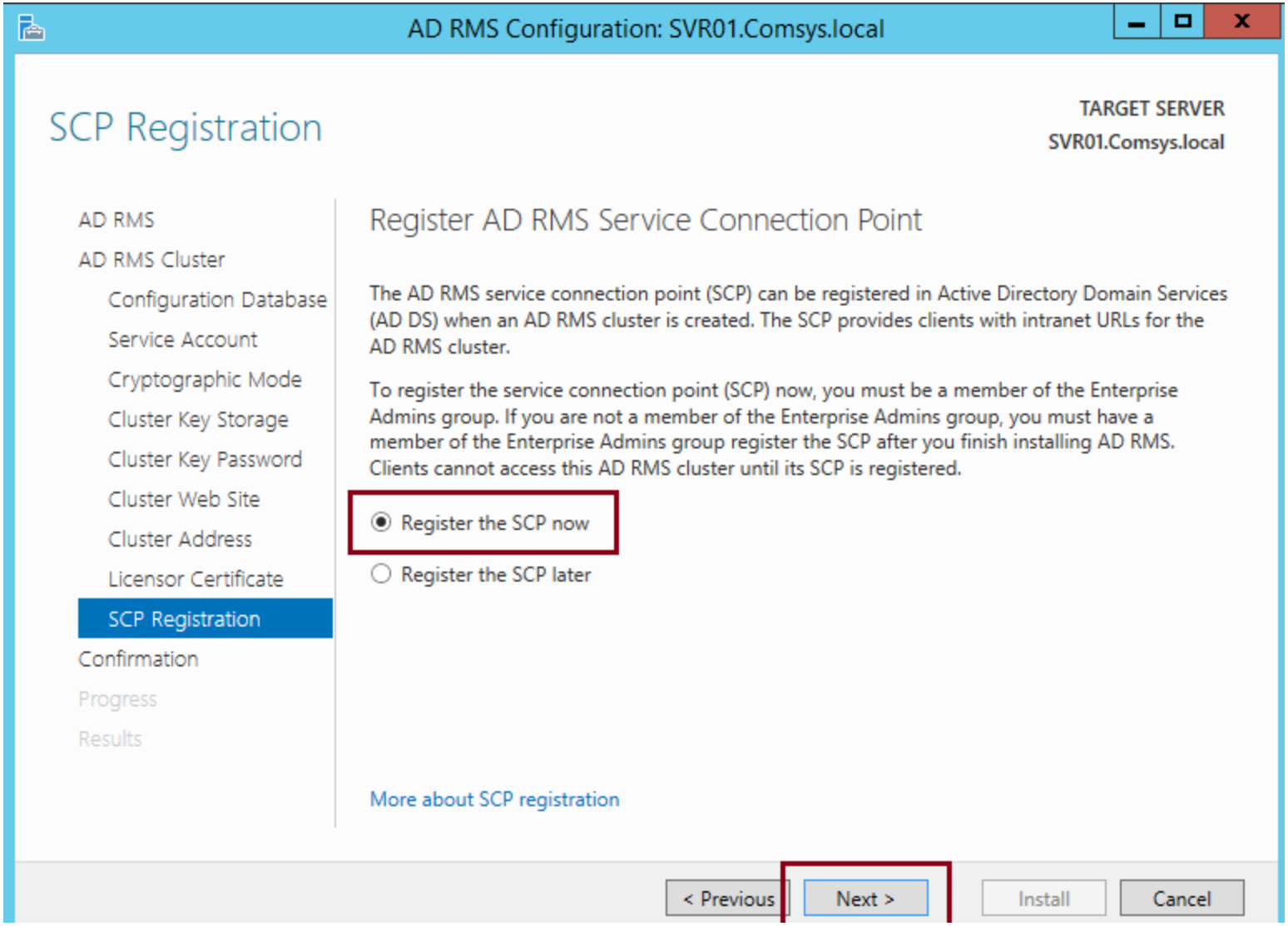

Cluster Key Storage
TARGET SERVER
SVR01.Comsys.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify AD RMS Cluster Key Storage
An AD RMS cluster uses the AD RMS cluster key to sign certificates and licenses that the cluster issues. The cluster key is required for disaster recovery and when additional AD RMS servers are joined to the cluster. You can allow AD RMS to encrypt and store the key, or you can store the key by using a cryptographic service provider (CSP). If the cluster key is stored in a CSP, you must manually distribute the key to servers that join the cluster later.
Use AD RMS centrally managed key storage
Use CSP key storage
More about cluster key storage
< Previous
Next >
Install
Cancel

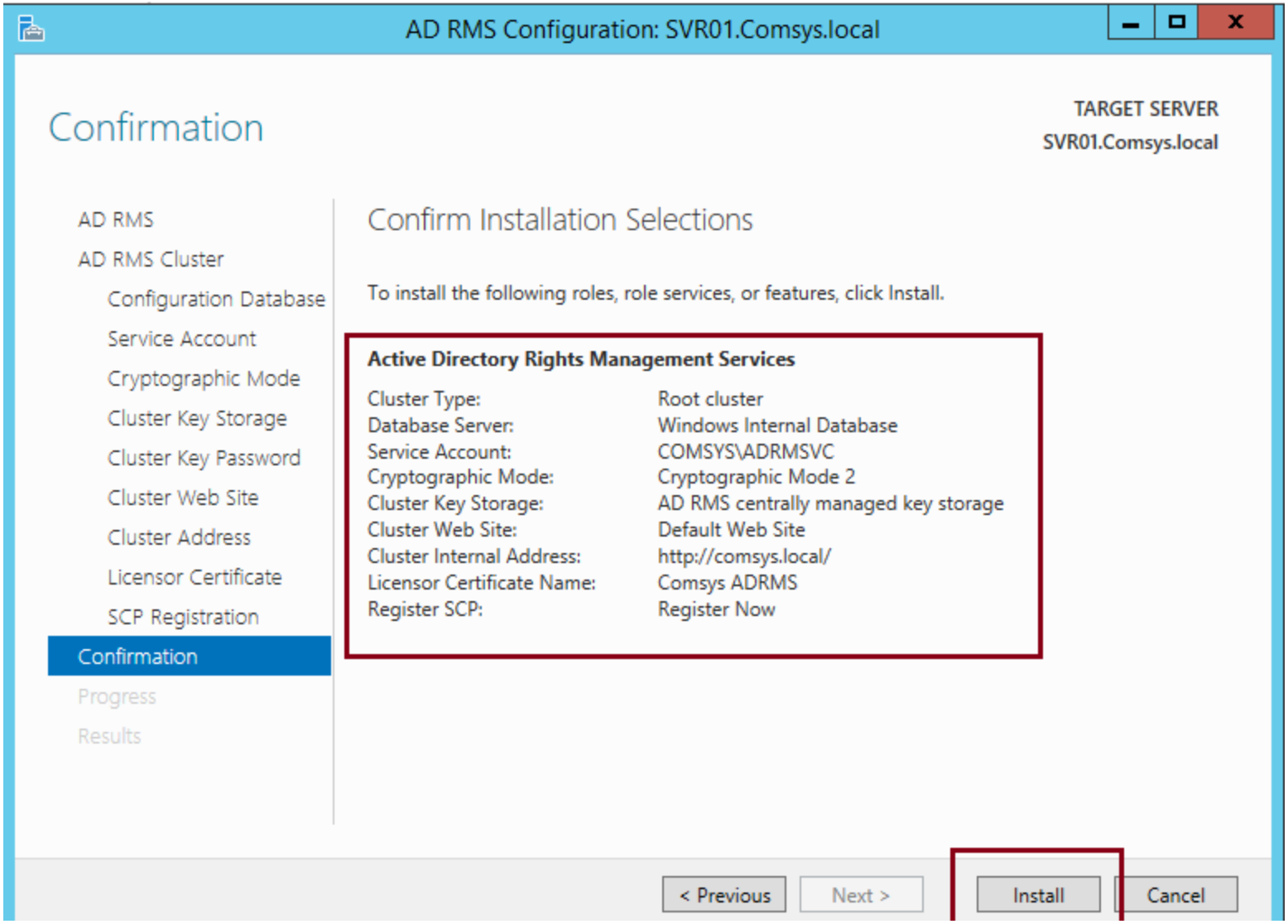

AD RMS Configuration: SVR01.Comsys.local
Cluster Key Password
TARGET SERVER
SVR01.Comsys.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify AD RMS Cluster Key Password
AD RMS uses the cluster key password to encrypt the cluster key. To join other AD RMS servers to this cluster or to restore the cluster from backup, you must be able to supply this password. AD RMS does not store this password and cannot recover it if it is lost, so you should keep it in a secure place.
Password:
Confirm Password:
More about cluster key storage
< Previous
Next >
Install
Cancel

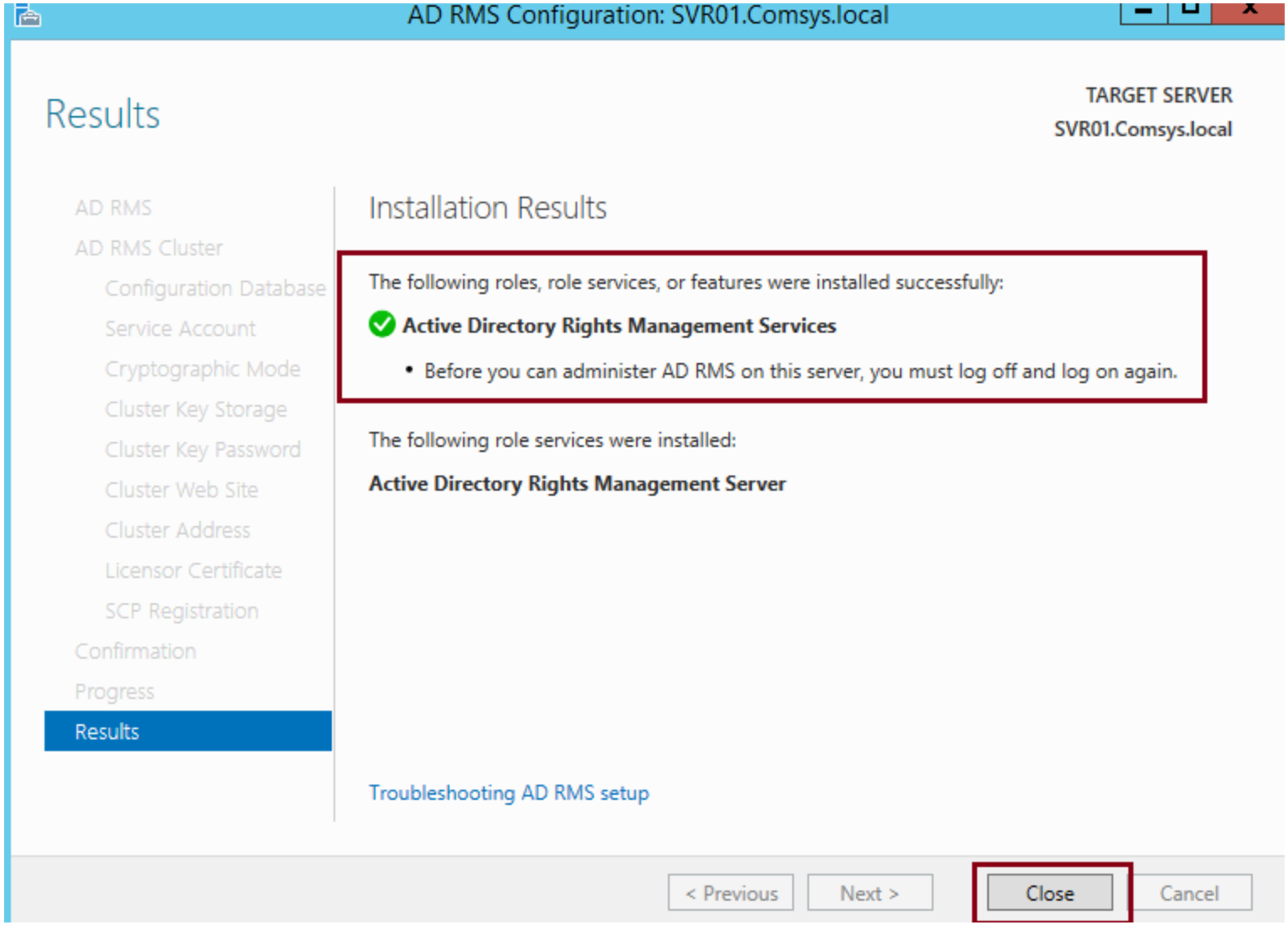

Dashboard
Local Server
All Servers
AD CS
AD RMS
File and Storag
IIS
AD RMS Configuration: SVR01.Comsys.local
Cluster Web Site
TARGET SERVER
SVR01.Comsys.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Select AD RMS Cluster Web Site
AD RMS is hosted in an Internet Information Services (IIS) virtual directory, which is set up on one of the existing Web sites on this server.
Select a Web site for the virtual directory:
Default Web Site
More about the cluster web site
< Previous
Next >
Install
Cancel

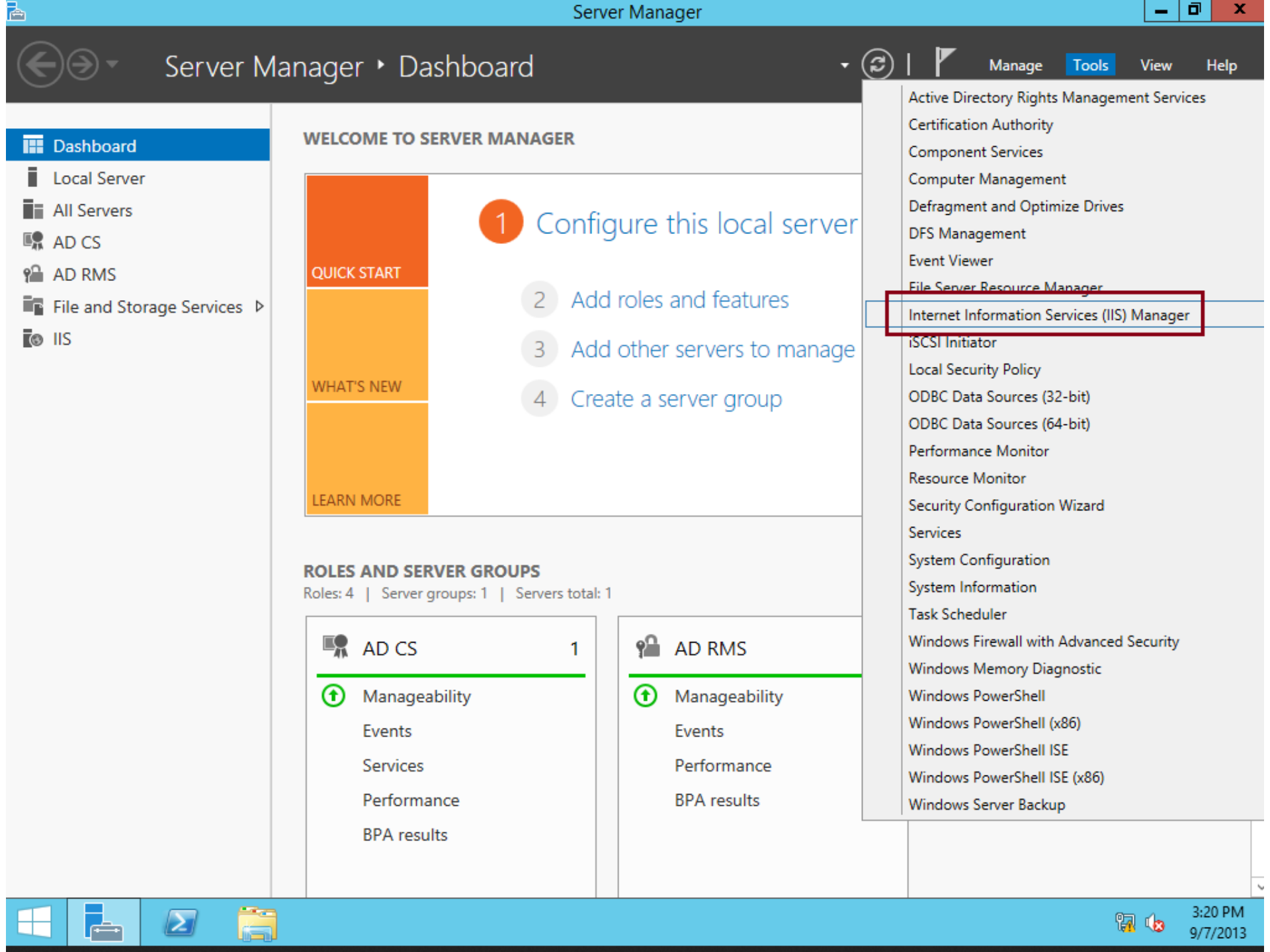

AD RMS Configuration: SVR01.Comsys.local
Cluster Address
TARGET SERVER
SVR01.Comsys.local
You cannot use an unencrypted connection if you want to add Identity Federation Support.
AD RMS
AD RMS Cluster
Configuration Data...
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Cluster Address
A cluster address makes it possible for AD RMS clients to communicate with this cluster over the network. We recommend that you configure AD RMS to use the Secure Sockets Layer (SSL) protocol to encrypt network traffic between AD RMS clients and this cluster. You must use an SSL-encrypted connection if you intend to federate this cluster.
Connection Type:
Use an SSL-encrypted connection (https://)
Use an unencrypted connection (http://)
Fully-Qualified Domain Name:
Port:
http://
comsys.local
80
You cannot change this address or port number after AD RMS is installed and configured.
More about the cluster web site
< Previous
Next >
Install
Cancel


AD RMS Configuration: SVR01.Comsys.local
Licensor Certificate
TARGET SERVER
SVR01.Comsys.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Name the Server Licensor Certificate
AD RMS creates a server licensor certificate that establishes the identity of this AD RMS cluster to clients. Because of the significance of this certificate, we recommend that you make a backup of this certificate to safeguard your deployment and improve disaster recovery efforts in the event of hardware failure or loss of the AD RMS database server.
Name:
Comsys ADRMS
< Previous
Next >
Install
Cancel

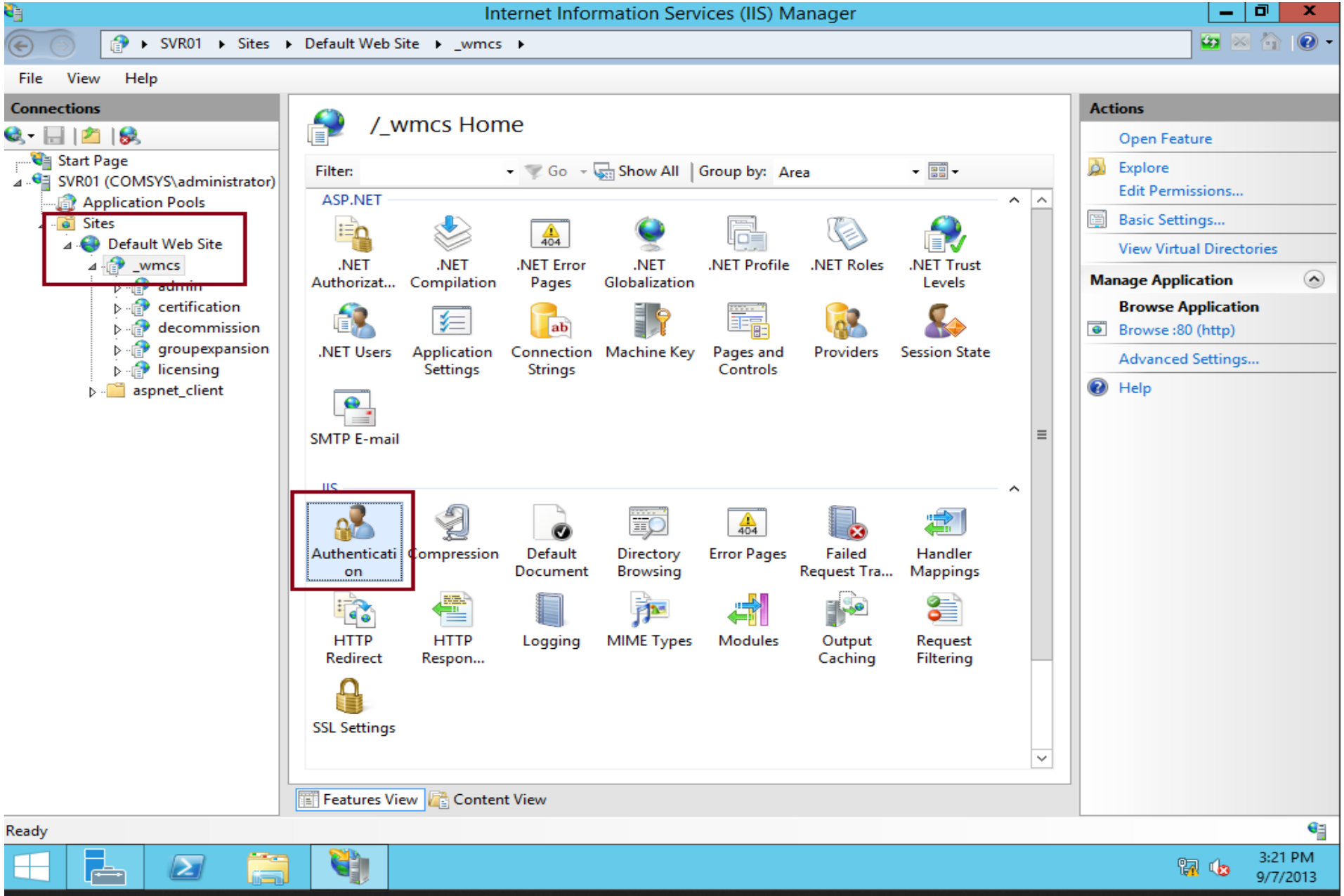

AD RMS Configuration: SVR01.Comsys.local
SCP Registration
TARGET SERVER
SVR01.Comsys.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Register AD RMS Service Connection Point
The AD RMS service connection point (SCP) can be registered in Active Directory Domain Services (AD DS) when an AD RMS cluster is created. The SCP provides clients with intranet URLs for the AD RMS cluster.
To register the service connection point (SCP) now, you must be a member of the Enterprise Admins group. If you are not a member of the Enterprise Admins group, you must have a member of the Enterprise Admins group register the SCP after you finish installing AD RMS. Clients cannot access this AD RMS cluster until its SCP is registered.
Register the SCP now
Register the SCP later
More about SCP registration
< Previous
Next >
Install
Cancel


AD RMS Configuration: SVR01.Comsys.local
Confirmation
TARGET SERVER
SVR01.Comsys.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Confirm Installation Selections
To install the following roles, role services, or features, click Install.
Active Directory Rights Management Services
Cluster Type: Root cluster
Database Server: Windows Internal Database
Service Account: COMSYS\ADRMSVC
Cryptographic Mode: Cryptographic Mode 2
Cluster Key Storage: AD RMS centrally managed key storage
Cluster Web Site: Default Web Site
Cluster Internal Address: http://comsys.local/
Licensor Certificate Name: Comsys ADRMS
Register SCP: Register Now
< Previous
Next >
Install
Cancel

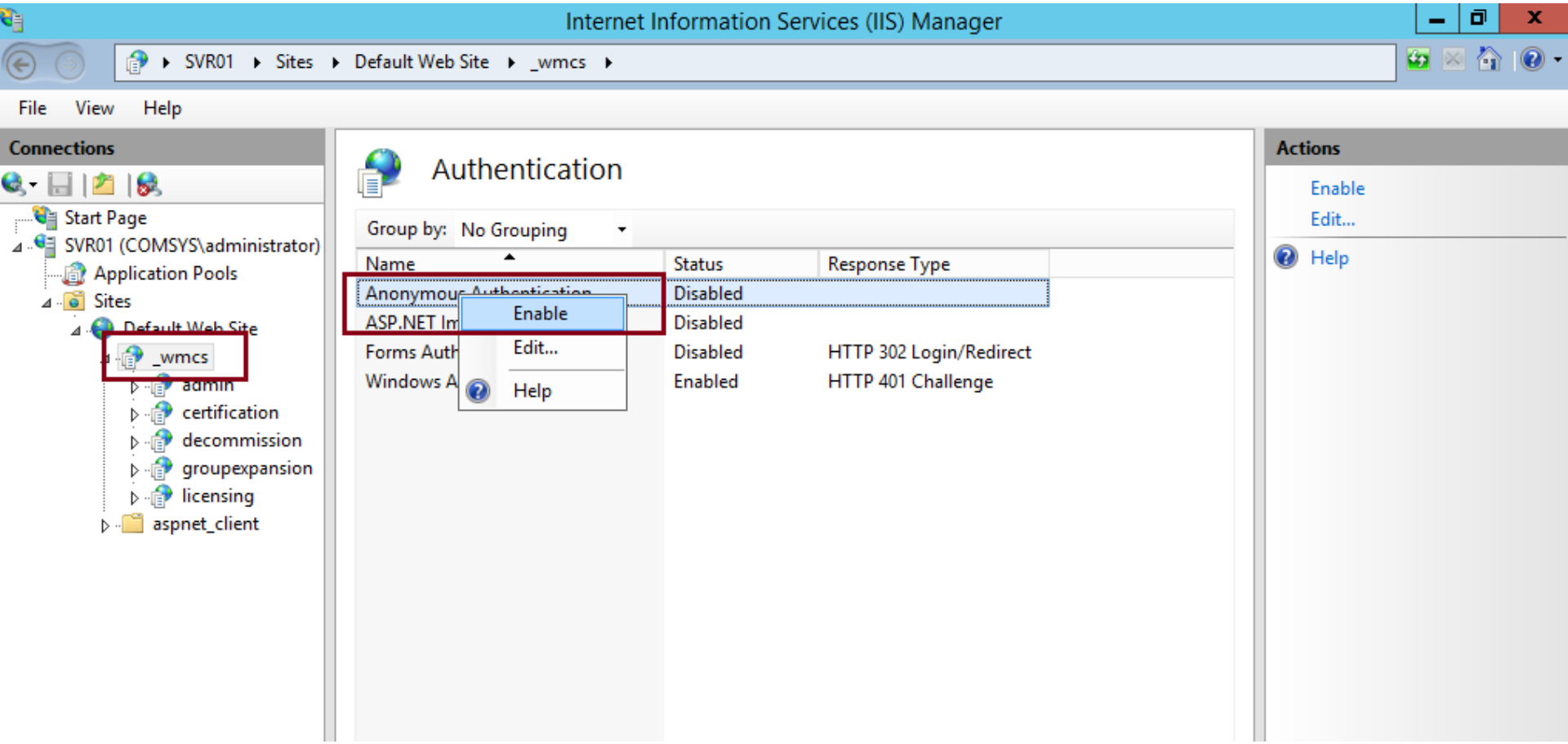

AD RMS Configuration: SVR01.Comsys.local
Results
TARGET SERVER
SVR01.Comsys.local
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Installation Results
The following roles, role services, or features were installed successfully:
Active Directory Rights Management Services
Before you can administer AD RMS on this server, you must log off and log on again.
The following role services were installed:
Active Directory Rights Management Server
Troubleshooting AD RMS setup
< Previous
Next >
Close
Cancel


Server Manager
Server Manager ▸ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD CS
AD RMS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
ROLES AND SERVER GROUPS
Roles: 4 | Server groups: 1 | Servers total: 1
AD CS 1
Manageability
Events
Services
Performance
BPA results
AD RMS
Manageability
Events
Performance
BPA results
Active Directory Rights Management Services
Certification Authority
Component Services
Computer Management
Defragment and Optimize Drives
DFS Management
Event Viewer
File Server Resource Manager
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Resource Monitor
Security Configuration Wizard
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup
3:20 PM
9/7/2013

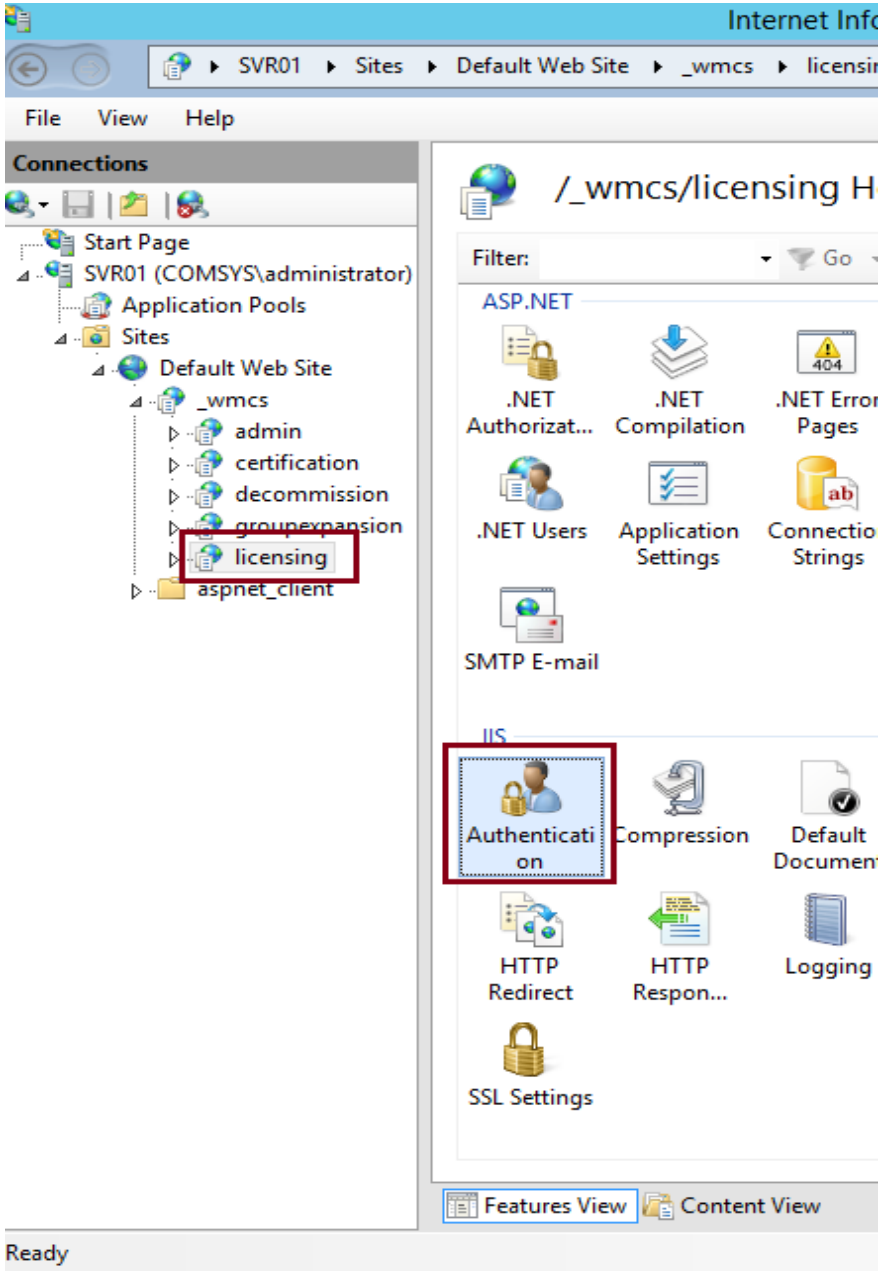
– In Internet Information Services (IIS) Manager, **expand Sites\Default Web Site and click _wmcs, then under /_wmcs Home, double-click Authentication…**



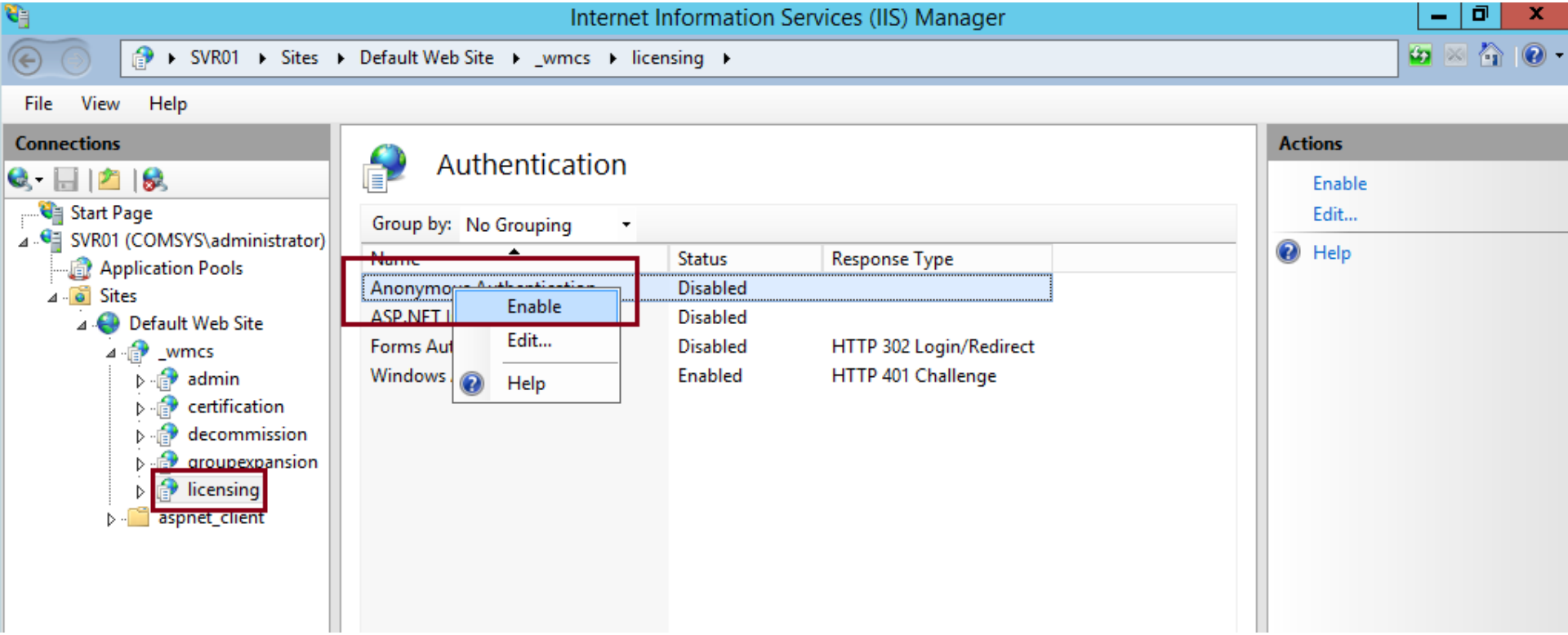
Then right-click Anonymous Authentication and click **Enable**



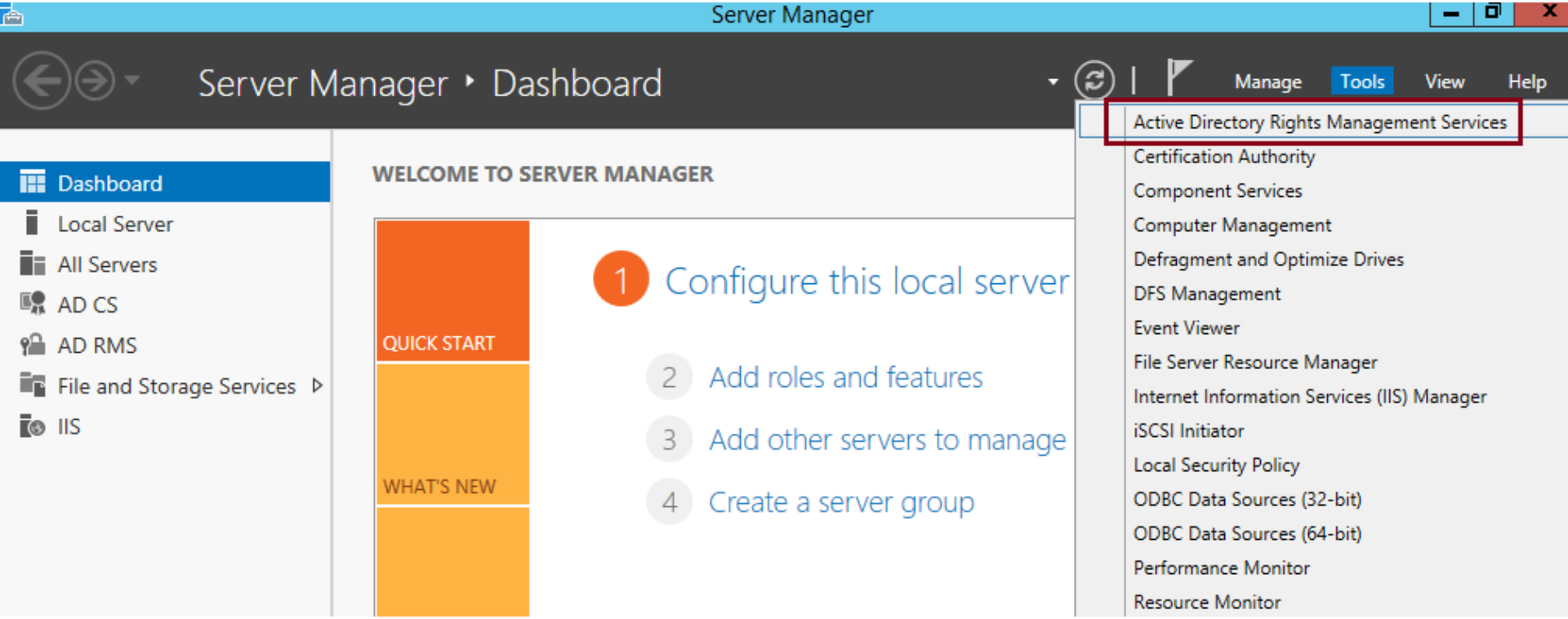
In the Connections pane, **expand _wmcs and click licensing and double-click Authentication…**



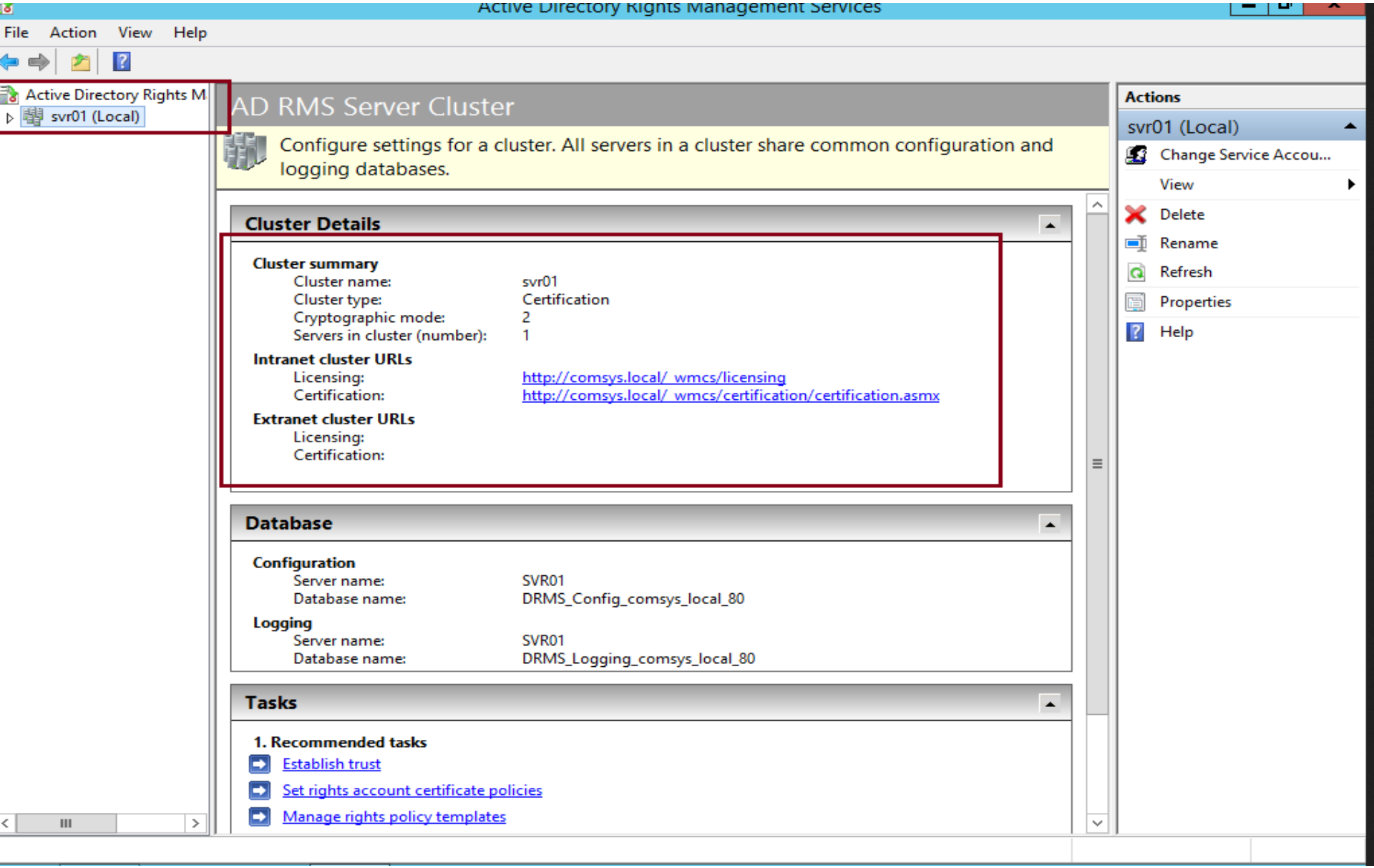
Right-click Anonymous Authentication and click **Enable, then close IIS Manager…**



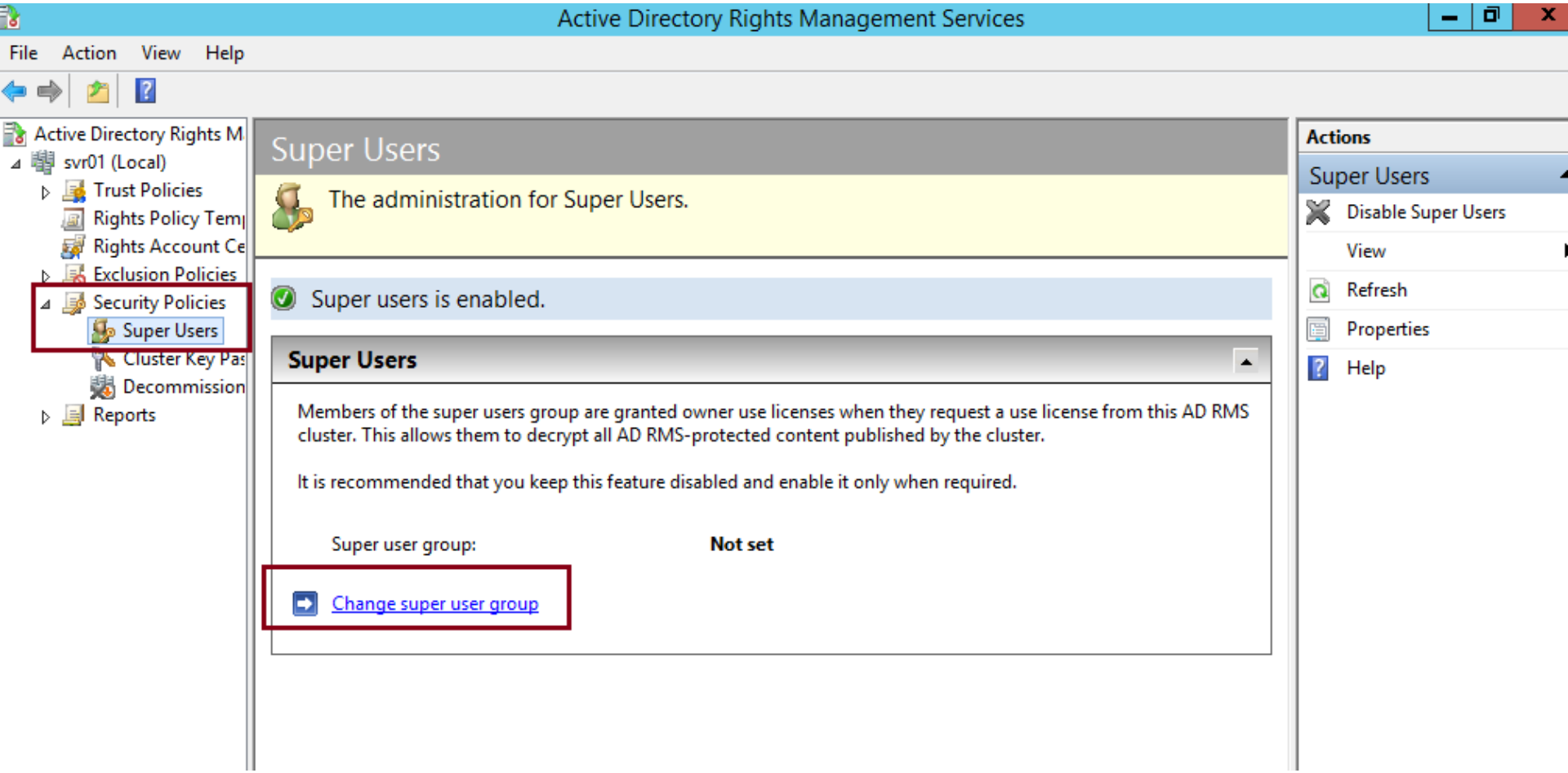
configure AD RMS super users group for SVR01

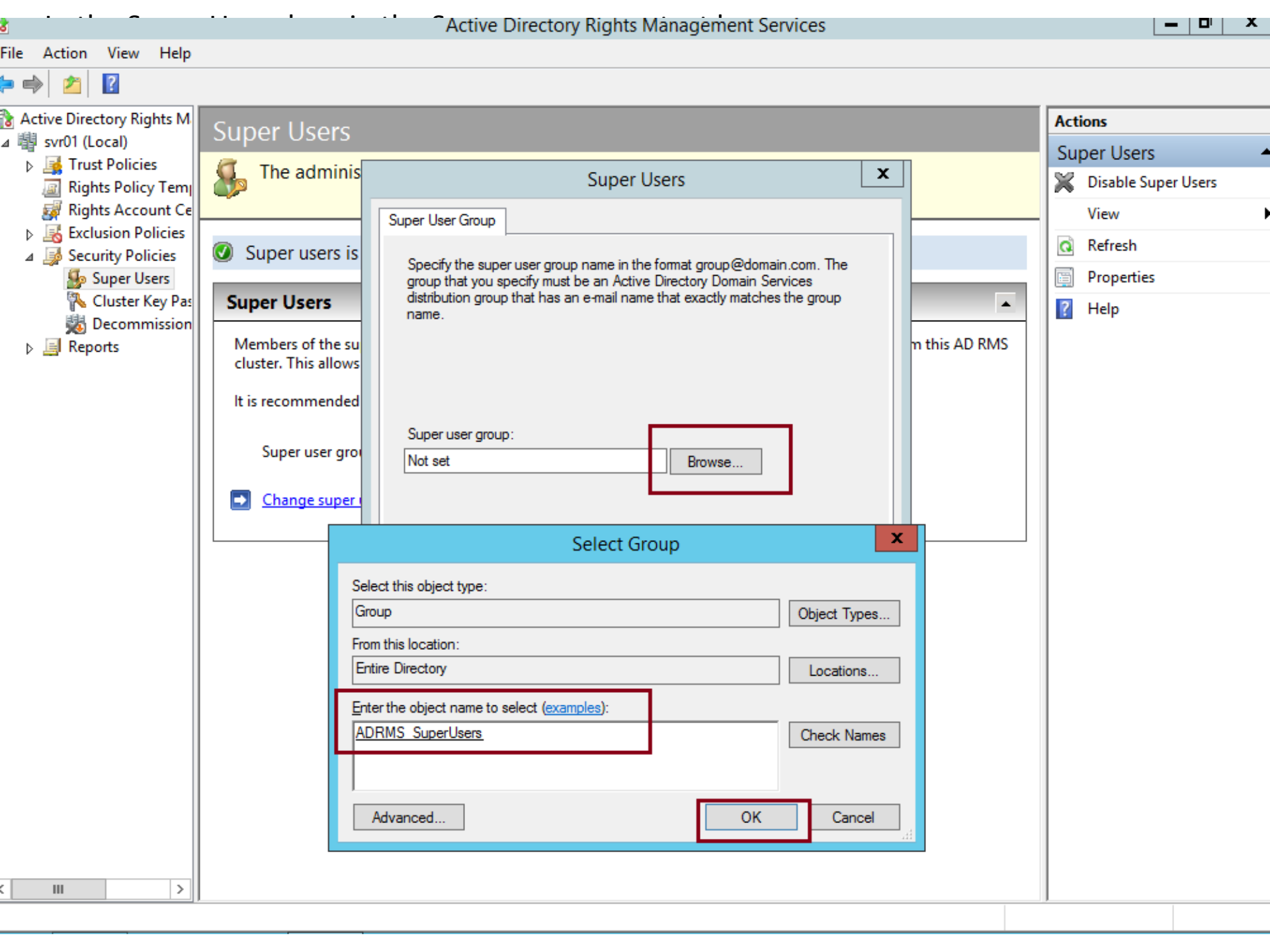


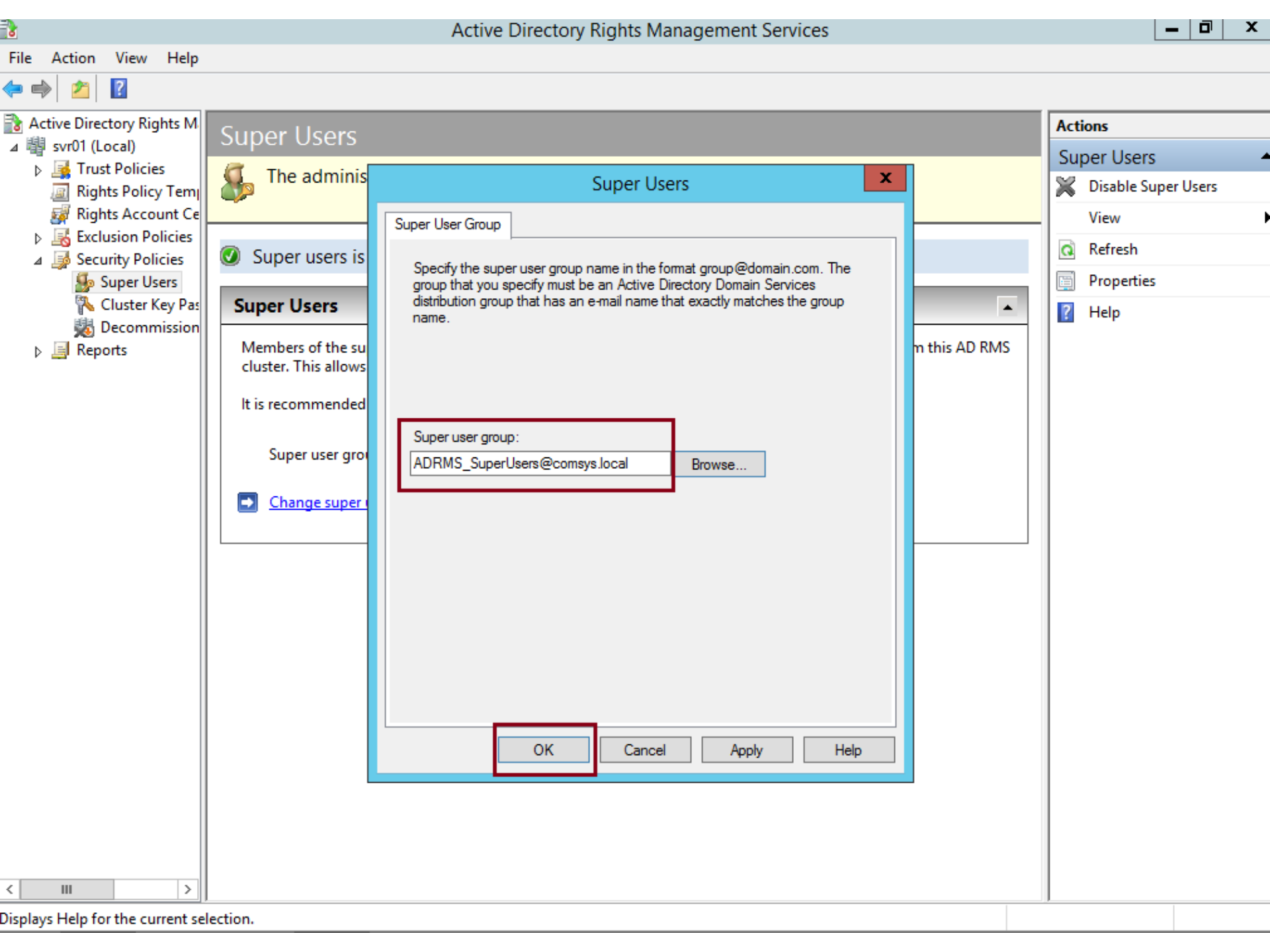
In the **Active Directory Rights Management Services console, expand the SVR01 node, and then click Security Policies…**



In the Security Policies area, under **Super Users, click Change super user group…**




Active Directory Rights Management Services
File Action View Help
Active Directory Rights M
svr01 (Local)
Trust Policies
Rights Policy Temp
Rights Account Ce
Exclusion Policies
Security Policies
Super Users
Cluster Key Pas
Decommission
Reports
Super Users
The adminis
Super users is
Super Users
Members of the su
cluster. This allows
It is recommended
Super user grou
Change super
m this AD RMS
Super Users
Super User Group
Specify the super user group name in the format group@domain.com. The group that you specify must be an Active Directory Domain Services distribution group that has an e-mail name that exactly matches the group name.
Super user group:
Not set
Browse...
Select Group
Select this object type:
Group
Object Types...
From this location:
Entire Directory
Locations...
Enter the object name to select (examples):
ADRMS_SuperUsers
Check Names
Advanced...
OK
Cancel
Actions
Super Users
Disable Super Users
View
Refresh
Properties
Help


Active Directory Rights Management Services
File Action View Help
Active Directory Rights M
svr01 (Local)
Trust Policies
Rights Policy Temp
Rights Account Ce
Exclusion Policies
Security Policies
Super Users
Cluster Key Pas
Decommission
Reports
Super Users
The adminis
Super users is
Super Users
Members of the su
cluster. This allows
It is recommended
Super user grou
Change super
m this AD RMS
Super Users
Super User Group
Specify the super user group name in the format group@domain.com. The group that you specify must be an Active Directory Domain Services distribution group that has an e-mail name that exactly matches the group name.
Super user group:
ADRMS_SuperUsers@comsys.local
Browse...
OK
Cancel
Apply
Help
Actions
Super Users
Disable Super Users
View
Refresh
Properties
Help
Displays Help for the current selection.