

# ACTIVE DIRECTORY RIGHT MANAGEMENT SERVICES (AD RMS)

## I. Giới thiệu:

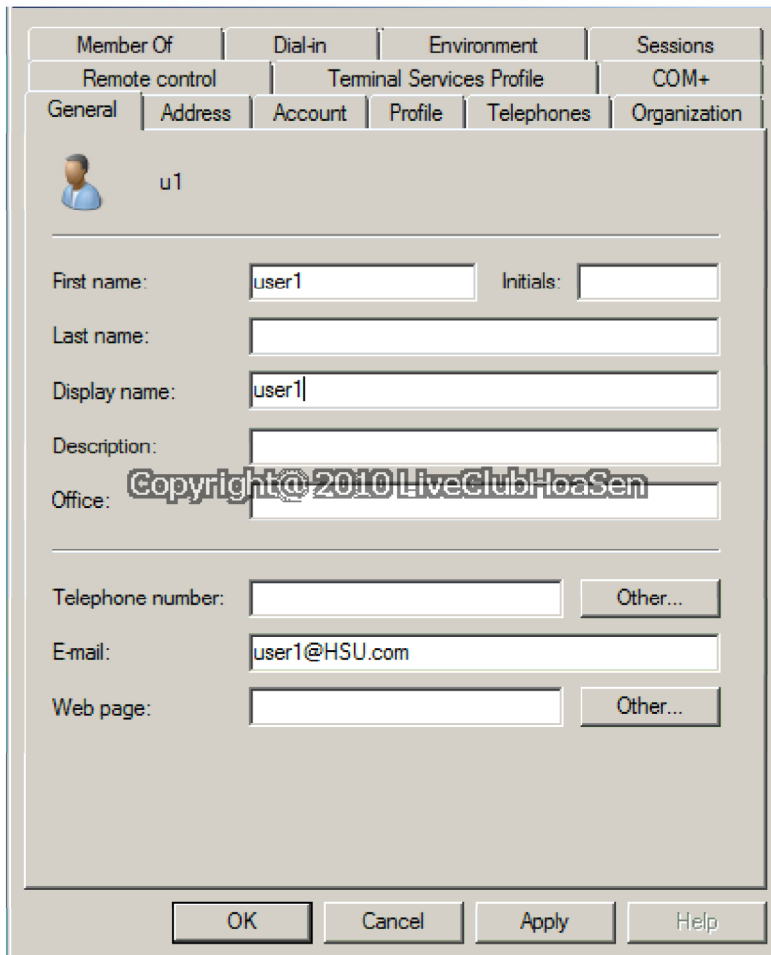
- Dịch vụ **Active Directory Right Management Services (AD RMS)** trên **Windows Server 2008** có chức năng phân quyền cho user trên tài nguyên cụ thể (document, e-mail....)
- Các loại dữ liệu hỗ trợ **AD RMS** gồm: **MS Word, MS Excel, MS Power Point, MS Outlook** từ phiên bản **Microsoft Office 2003** trở lên.

Hôm nay chúng ta sẽ thực hiện các bước cài đặt và cấu hình dịch vụ **AD RMS** trên Một máy **Windows Server 2008** đã nâng cấp **Domain Controller (DC)**. Với các user được tạo sẵn **User1, User2, RMS\_VT071A** và **Administrator**.

Sau khi hoàn thành bài lab chúng ta sẽ kiểm tra bằng việc phân quyền trên file **test.docx** với đường dẫn **C:\Test.docx** cho các **user1, user2** và kiểm tra quyền trên từng user.

## II. Chuẩn bị:

- Login vào máy DC với quyền Admin Domain (HSU\Administrator).
- Nhấn Start, chọn Administrative Tools, mở Active Directory Users And Computers, Chọn Domain HSU.com, Trong mục User chuột phải User1, chọn Properties, điền thông tin E-mail là [user1@HSU.com](mailto:user1@HSU.com).



The screenshot shows the 'Properties' dialog box for a user named 'u1' in the Active Directory Users and Computers console. The 'General' tab is selected, showing the user's profile picture and name. The 'First name' field contains 'user1', and the 'Initials' field is empty. The 'Last name' field is empty. The 'Display name' field contains 'user1'. The 'Description' field is empty. The 'Office' field is empty. The 'Telephone number' field is empty, with an 'Other...' button next to it. The 'E-mail' field contains 'user1@HSU.com'. The 'Web page' field is empty, with an 'Other...' button next to it. The dialog box has 'OK', 'Cancel', 'Apply', and 'Help' buttons at the bottom.

Member Of	Dial-in	Environment	Sessions
Remote control	Terminal Services Profile	COM+	
General	Address	Account	Profile
Telephones	Organization		

u1

First name: user1 Initials:

Last name:

Display name: user1

Description:

Office:

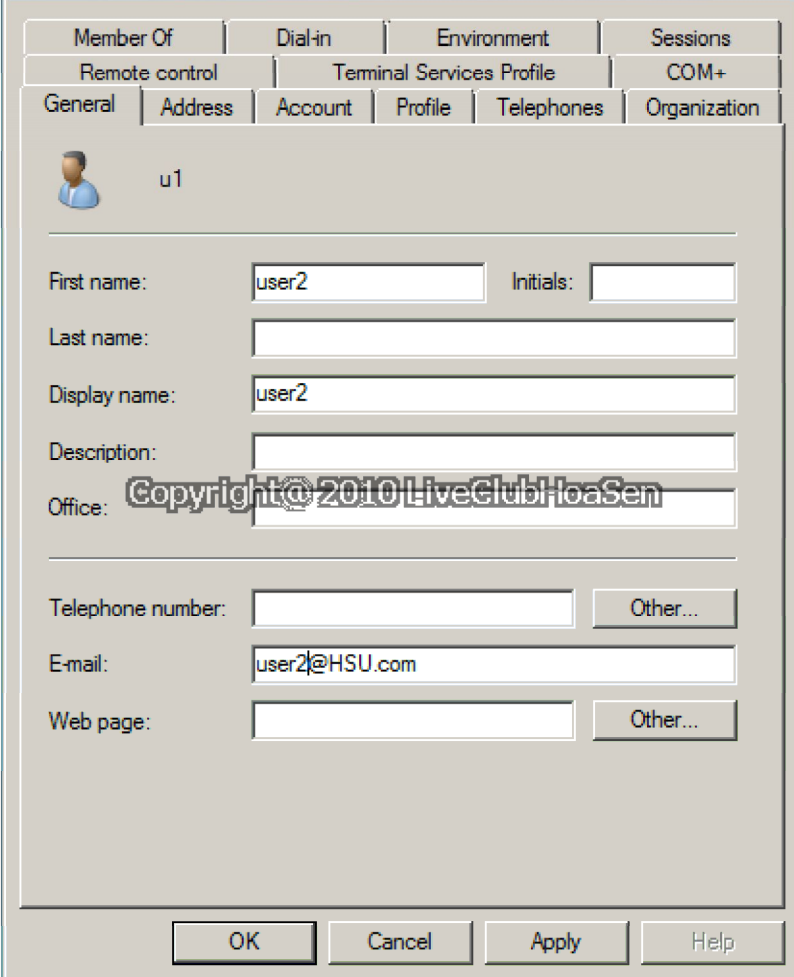
Telephone number: Other...

E-mail: user1@HSU.com

Web page: Other...

OK Cancel Apply Help


- Trong cửa sổ **Properties** của User2, điền thông tin E-mail là [user2@HSU.com](mailto:user2@HSU.com).



Member Of   Dial-in   Environment   Sessions

Remote control   Terminal Services Profile   COM+

General   Address   Account   Profile   Telephones   Organization

 u1

First name:  Initials:

Last name:

Display name:

Description:

Office:

Telephone number:  Other...

E-mail:

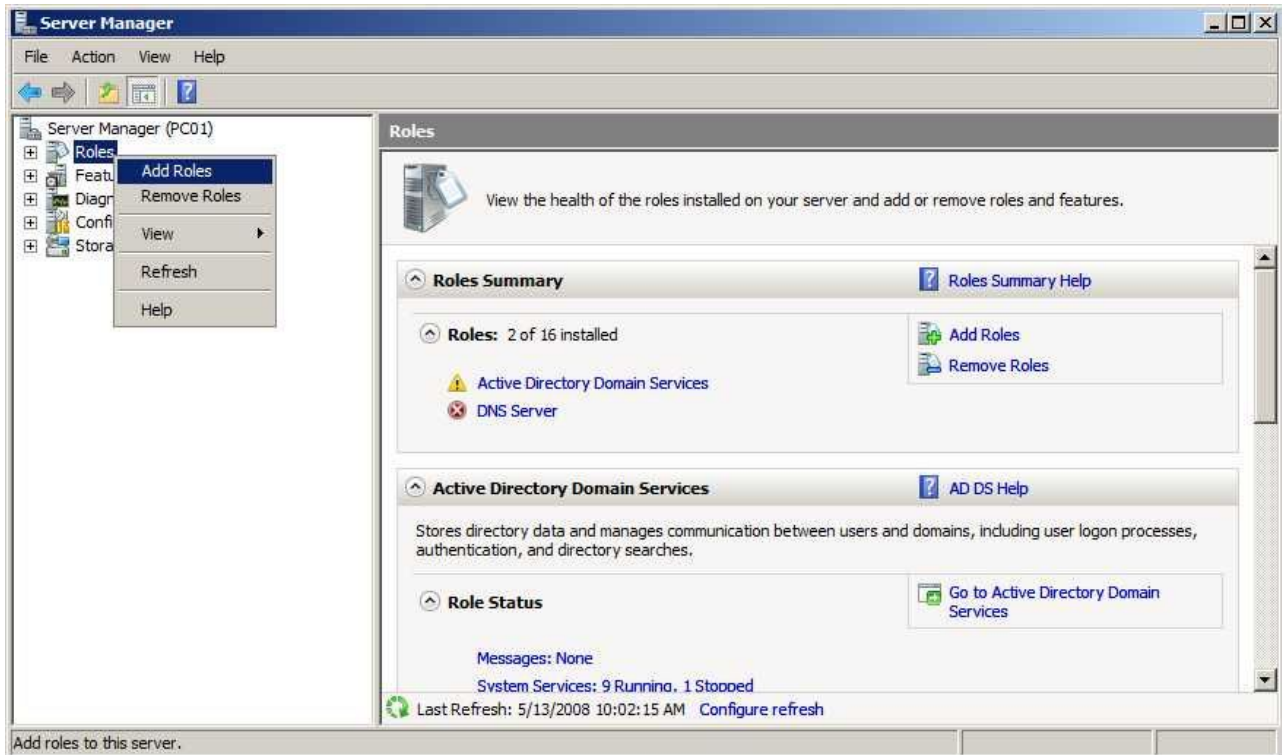
Web page:  Other...

OK   Cancel   Apply   Help

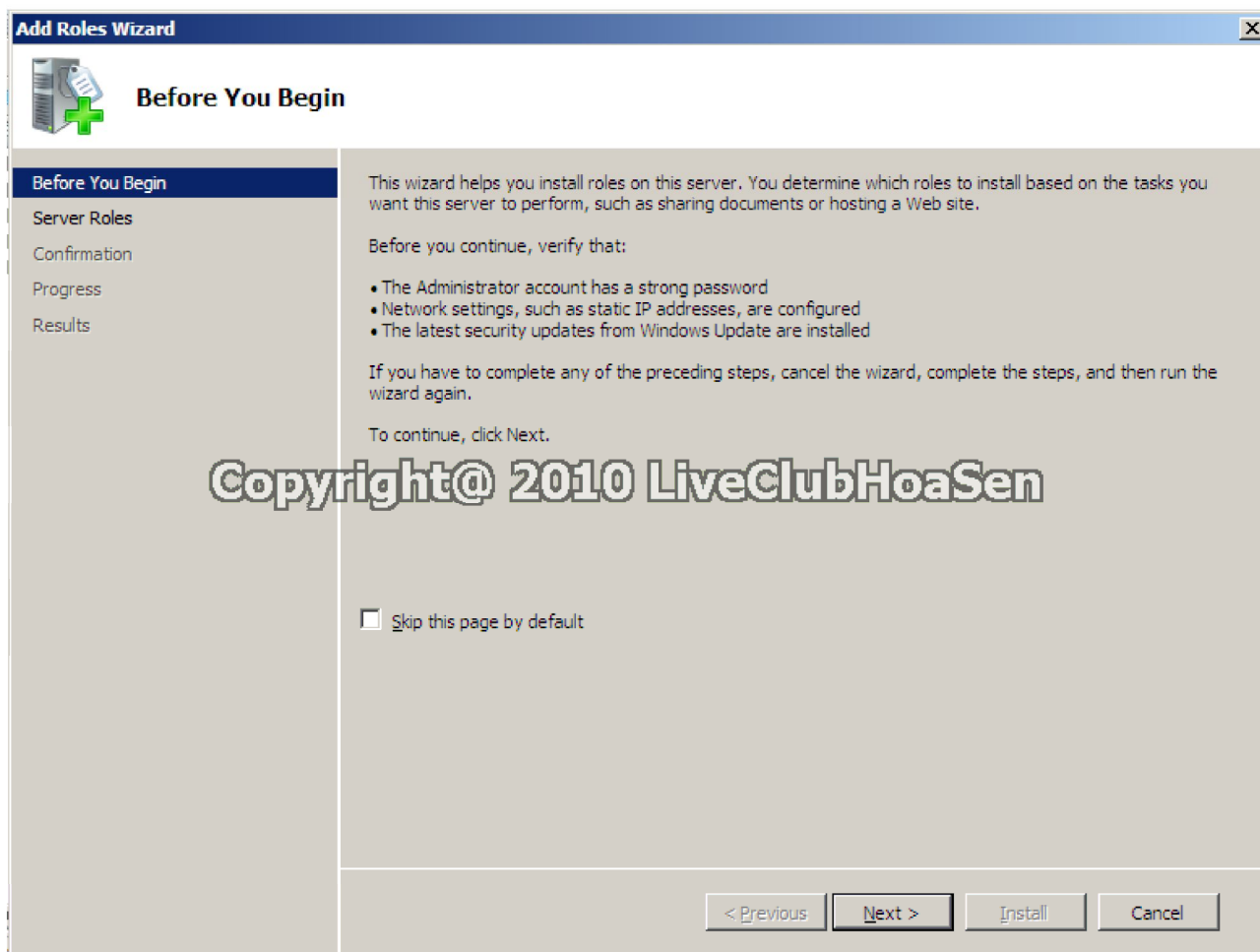
### III. Thực hiện:

#### A. Cài đặt RMS

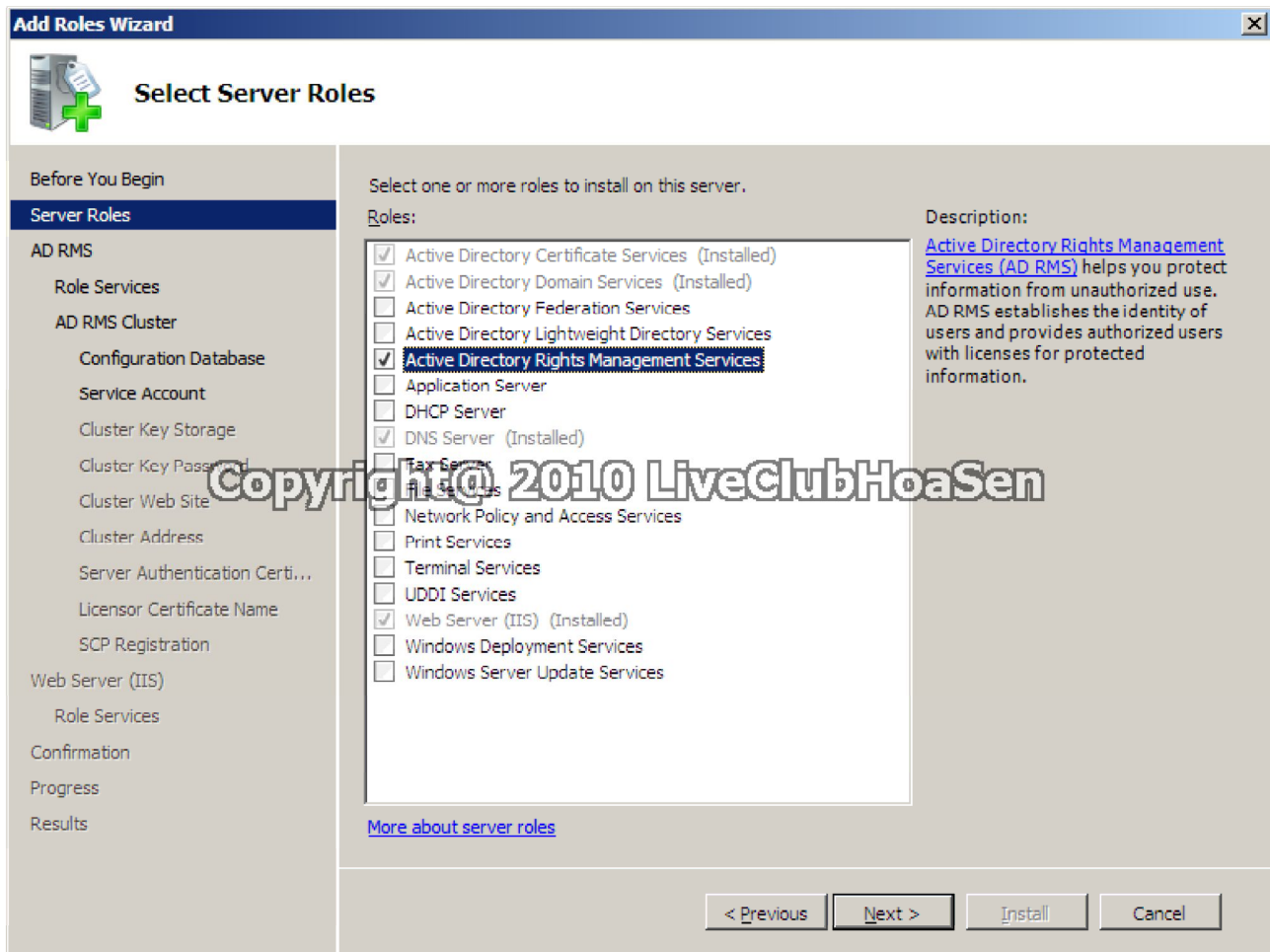
- Login vào máy DC với quyền Admin Domain (HSU\Administrator).
- Nhấn **Start**, chọn **Administrative Tools**, mở **Server Manager** chuột phải **Roles** chọn **Add Roles**.



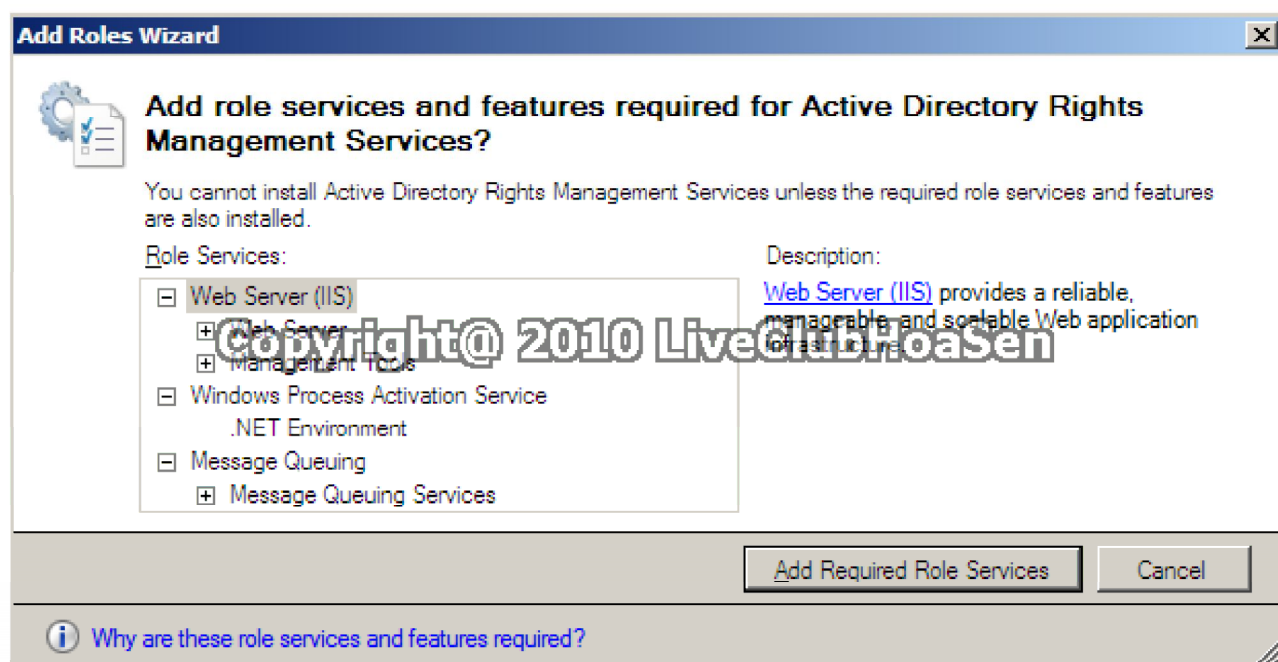
- Trong mục **Before You Begin**, nhấn **Next**.



- Trong mục **Select Server Roles**, đánh dấu chọn **Active Directory Rights Management Services**, nhấn **Next**.




- Trong hộp thoại **Add Roles Wizard**, nhấn **Add Required Features**.



- Trong mục **Active Directory Rights Management Services**, nhấn **Next**.

**Add Roles Wizard** [X]

 **Specify Service Account**

**Before You Begin**  
**Server Roles**  
**AD RMS**  
    **Role Services**  
        **AD RMS Cluster**  
            **Configuration Database**  
            **Service Account** (selected)  
            Cluster Key Storage  
            Cluster Key Password  
            Cluster Web Site  
            Cluster Address  
            Server Authentication Certificate  
            Licensor Certificate Name  
            SCP Registration  
Web Server (IIS)  
    Role Services  
Confirmation  
Progress  
Results

A domain user account is required to provide a network identity for AD RMS so that it can communicate with other services on this computer and the network. The domain account should be a standard domain user account with no additional permissions.

Specify the account under which the AD RMS cluster will run. The AD RMS service account will be a member of the AD RMS service group and will have the permissions defined for that group.

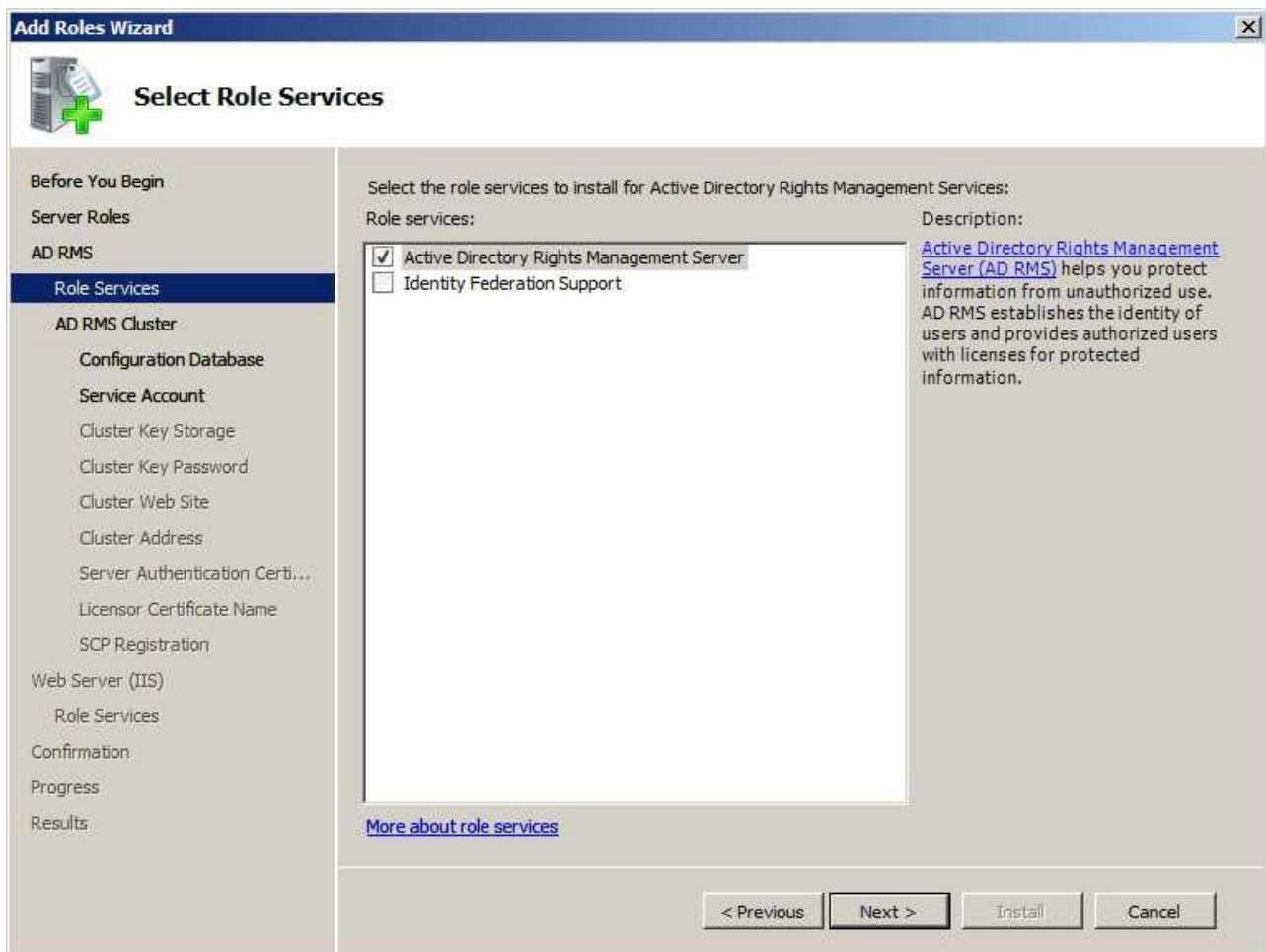
Domain User Account:

**Copyright@ 2010 LiveClubHoaSen**

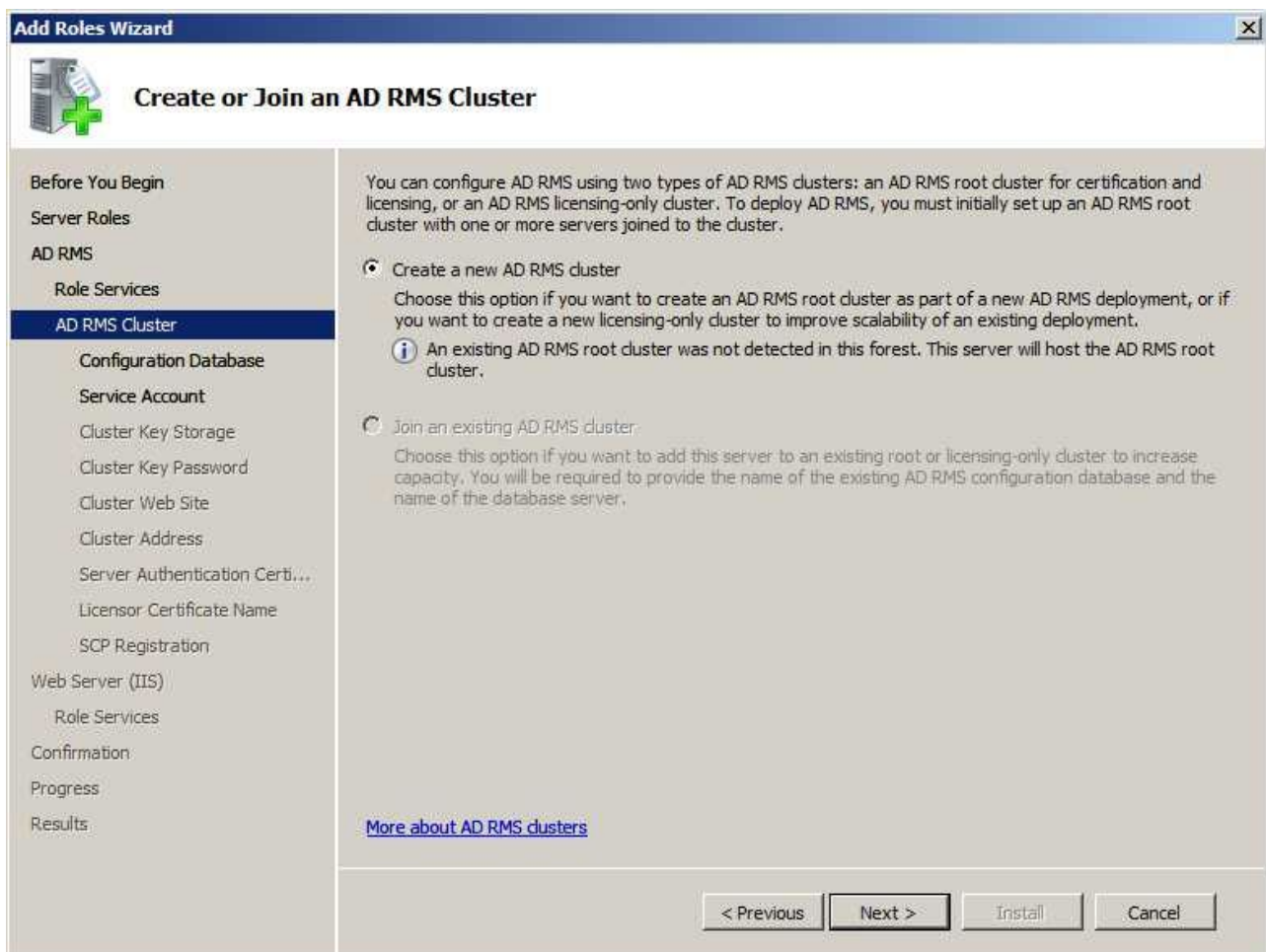
< Previous    Next >    Install    Cancel



- Trong mục **Select Role Services**, đánh dấu chọn **Active Directory Rights Management Server**, nhấn **Next**.



- Trong mục **Create or Join an AD RMS Cluster**, nhấn **Next**.



- Trong mục **Select Configuration Database**, nhấn **Next**.

The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard'. The main window has a left-hand navigation pane and a right-hand content area. The navigation pane lists the following steps: 'Before You Begin', 'Server Roles', 'AD RMS', 'Role Services', 'AD RMS Cluster', 'Configuration Database' (highlighted with a blue background), 'Service Account', 'Cluster Key Storage', 'Cluster Key Password', 'Cluster Web Site', 'Cluster Address', 'Server Authentication Certi...', 'Licensor Certificate Name', 'SCP Registration', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main content area is titled 'Select Configuration Database' and contains the following text: 'AD RMS clusters use a database to store configuration and policy information. The database can be hosted either by Windows Internal Database or another database server.' Below this text are two radio button options. The first option, 'Use Windows Internal Database on this server', is selected. Below it is a paragraph: 'Using Windows Internal Database will limit this AD RMS cluster to a single-server cluster. If you intend to join more servers to this AD RMS cluster, do not use this option.' The second option is 'Use a different database server'. Below this option are two input fields: 'Server:' with a text box and a 'Select...' button, and 'Database Instance:' with a dropdown menu. Below these fields is a 'Validate' button. At the bottom of the content area is a blue hyperlink: 'More about AD RMS databases'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

**Add Roles Wizard**

**Select Configuration Database**

AD RMS clusters use a database to store configuration and policy information. The database can be hosted either by Windows Internal Database or another database server.

☒ Use Windows Internal Database on this server

Using Windows Internal Database will limit this AD RMS cluster to a single-server cluster. If you intend to join more servers to this AD RMS cluster, do not use this option.

☐ Use a different database server

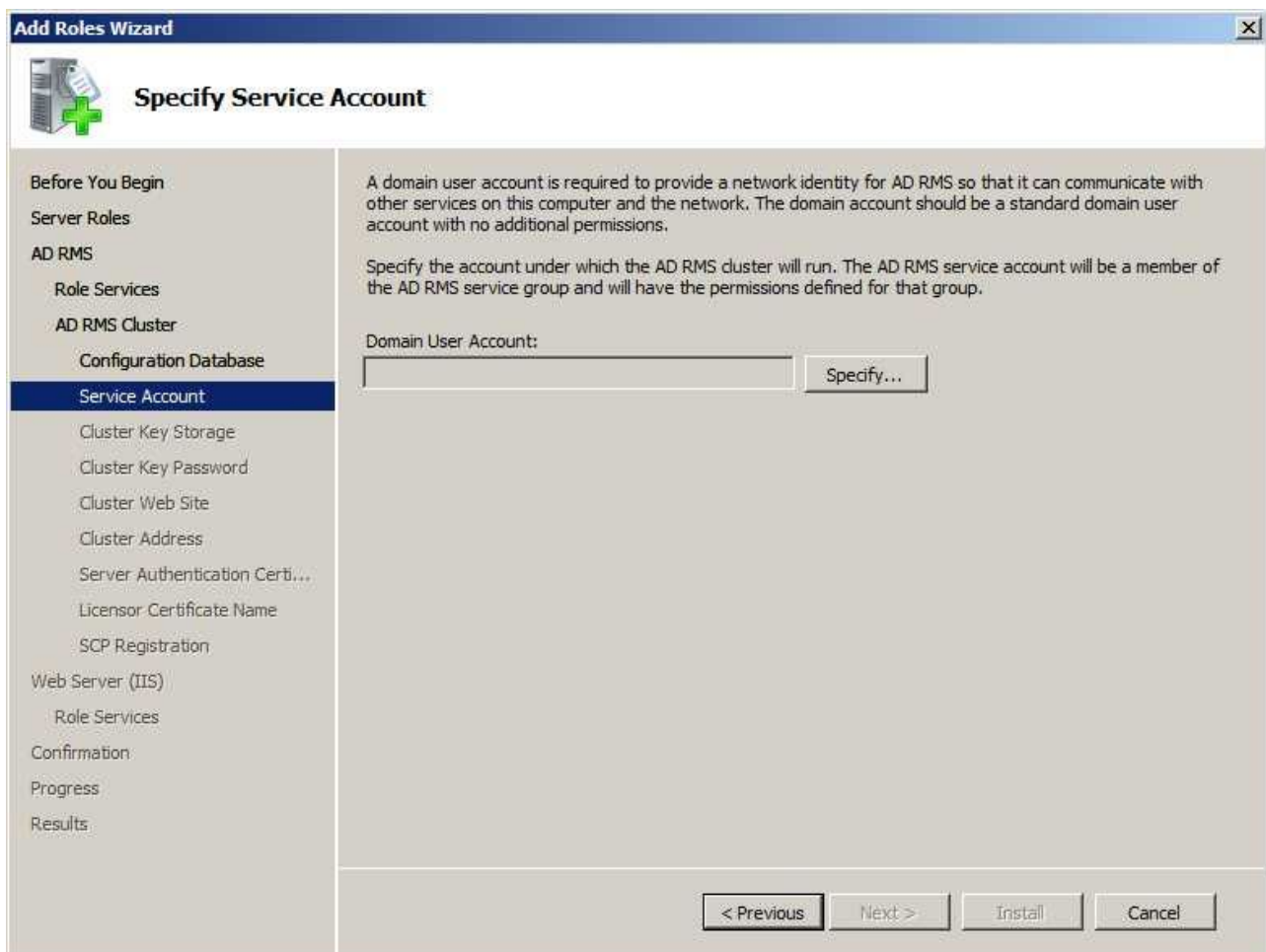
Server:  

Database Instance:

[More about AD RMS databases](#)

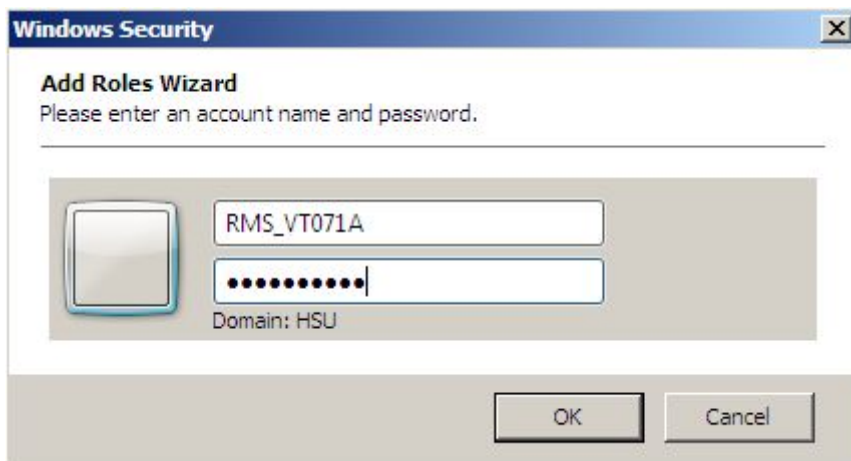
< Previous   Next >   Install   Cancel

- Trong mục **Specify Service Account**, nhấn **Specify...**



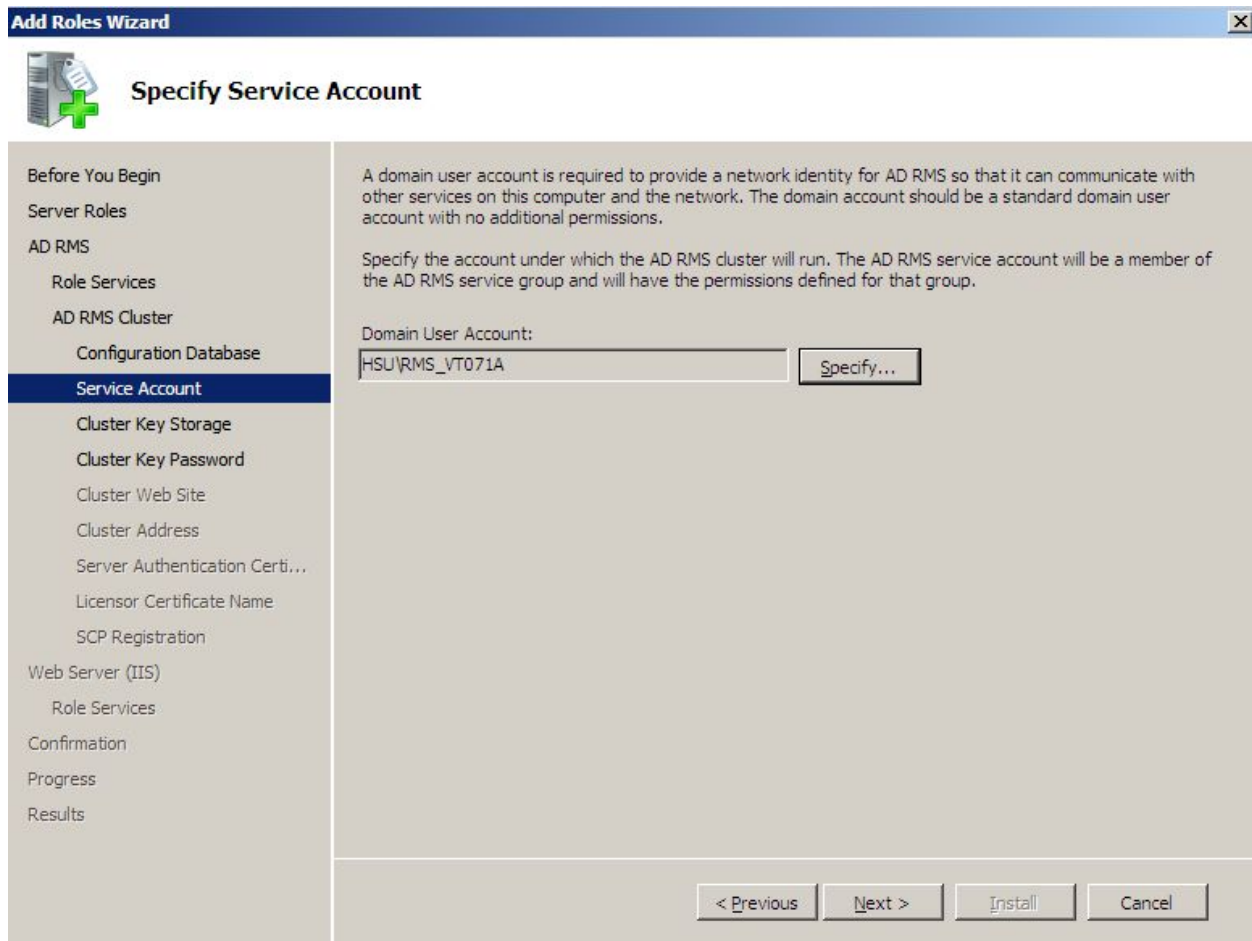
The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard'. The main title is 'Specify Service Account'. On the left is a tree view with the following items: 'Before You Begin', 'Server Roles', 'AD RMS', 'Role Services', 'AD RMS Cluster', 'Configuration Database', 'Service Account' (highlighted), 'Cluster Key Storage', 'Cluster Key Password', 'Cluster Web Site', 'Cluster Address', 'Server Authentication Certi...', 'Licensor Certificate Name', 'SCP Registration', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main pane contains the following text: 'A domain user account is required to provide a network identity for AD RMS so that it can communicate with other services on this computer and the network. The domain account should be a standard domain user account with no additional permissions.' and 'Specify the account under which the AD RMS cluster will run. The AD RMS service account will be a member of the AD RMS service group and will have the permissions defined for that group.' Below this text is a text box labeled 'Domain User Account:' and a 'Specify...' button. At the bottom right are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

- Trong mục **Add Roles Wizard**, nhập user là **RMS\_VT071A** password **P@ss123456**, nhấn **OK**.



**Chú ý:** Ở bước này ko thể dùng account đang **login** để nhập vào mà phải sử dụng user khác vì vậy cần add user **RMS\_VT071A** vào group **admin** để ko bị chặn bởi chưa chính policy **Allow logon locally**.

- Trong mục **Specify Service Account**, nhấn **Next**.



The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard'. The main window has a left-hand navigation pane and a right-hand content area. The navigation pane lists the following steps: 'Before You Begin', 'Server Roles', 'AD RMS', 'Role Services', 'AD RMS Cluster', 'Configuration Database', 'Service Account' (highlighted with a blue background), 'Cluster Key Storage', 'Cluster Key Password', 'Cluster Web Site', 'Cluster Address', 'Server Authentication Certi...', 'Licensor Certificate Name', 'SCP Registration', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The 'Specify Service Account' step is active, and the content area displays the following text: 'A domain user account is required to provide a network identity for AD RMS so that it can communicate with other services on this computer and the network. The domain account should be a standard domain user account with no additional permissions.' Below this, it says: 'Specify the account under which the AD RMS cluster will run. The AD RMS service account will be a member of the AD RMS service group and will have the permissions defined for that group.' A text box labeled 'Domain User Account:' contains the text 'HSU\RMS\_VT071A'. To the right of the text box is a button labeled 'Specify...'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

**Add Roles Wizard**

**Specify Service Account**

Before You Begin  
Server Roles  
AD RMS  
Role Services  
AD RMS Cluster  
Configuration Database  
**Service Account**  
Cluster Key Storage  
Cluster Key Password  
Cluster Web Site  
Cluster Address  
Server Authentication Certi...  
Licensor Certificate Name  
SCP Registration  
Web Server (IIS)  
Role Services  
Confirmation  
Progress  
Results

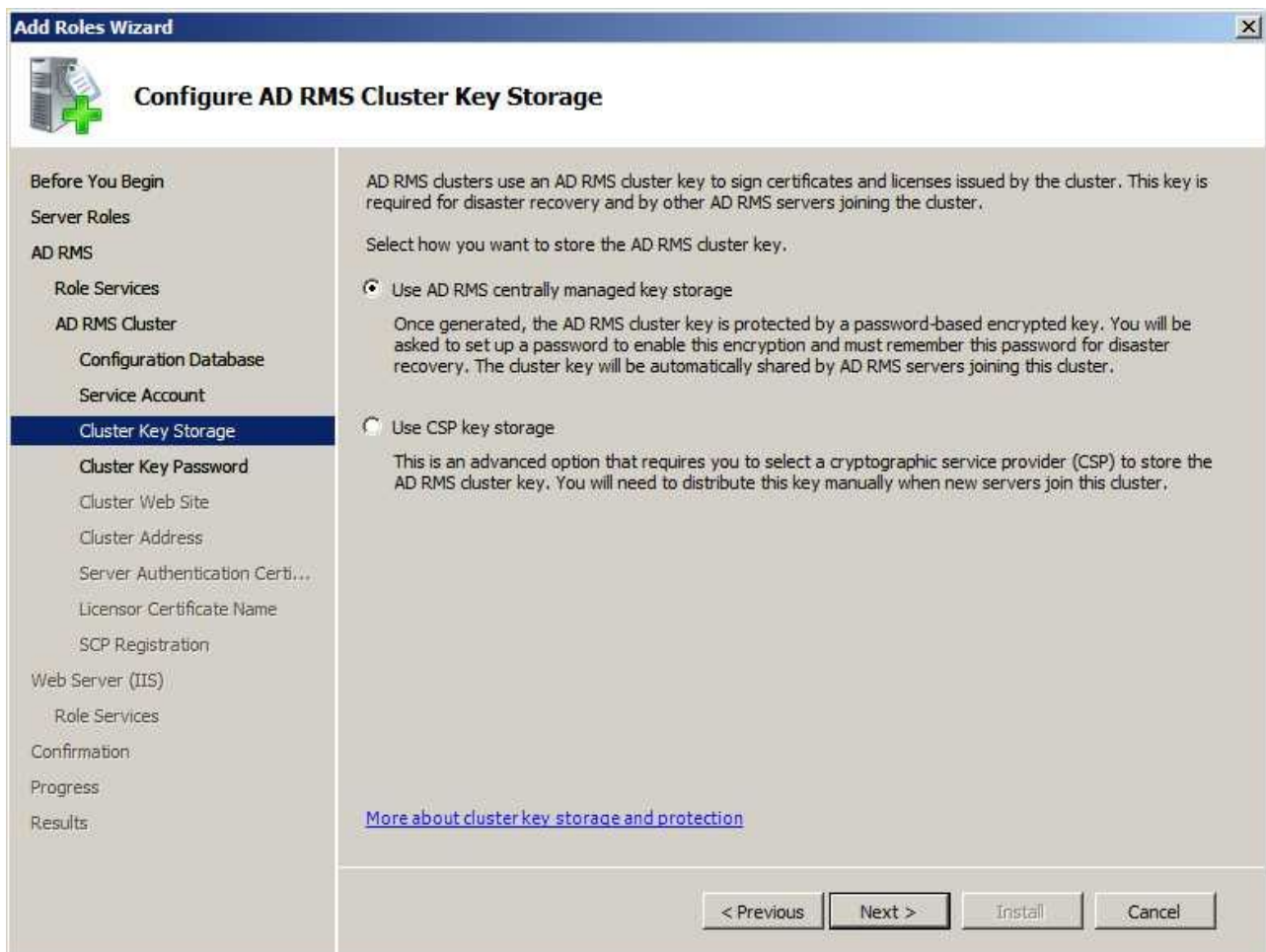
A domain user account is required to provide a network identity for AD RMS so that it can communicate with other services on this computer and the network. The domain account should be a standard domain user account with no additional permissions.

Specify the account under which the AD RMS cluster will run. The AD RMS service account will be a member of the AD RMS service group and will have the permissions defined for that group.

Domain User Account:  
HSU\RMS\_VT071A Specify...

< Previous Next > Install Cancel

- Trong mục **Configure AD RMS Cluster Key Storage**, chọn **Use AD RMS centrally managed key storage**, nhấn **Next**.



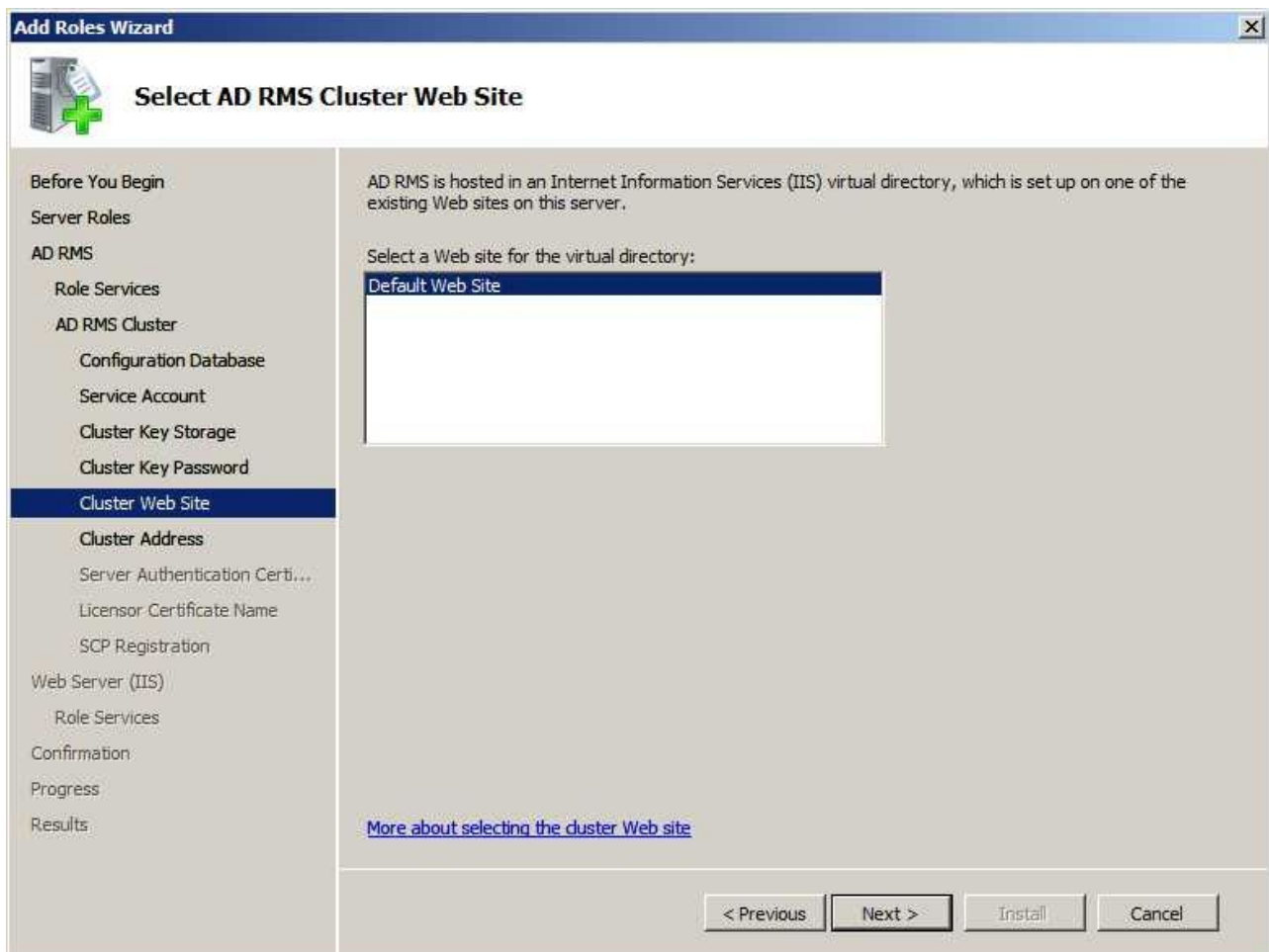


- Trong mục **Specify AD RMS Cluster Key Password**, nhập **P@ss123** vào ô **Password** và **Confirm Password**, nhấn **Next**.

The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard'. The main title is 'Specify AD RMS Cluster Key Password'. On the left is a tree view with the following items: 'Before You Begin', 'Server Roles', 'AD RMS', 'Role Services', 'AD RMS Cluster', 'Configuration Database', 'Service Account', 'Cluster Key Storage', 'Cluster Key Password' (selected), 'Cluster Web Site', 'Cluster Address', 'Server Authentication Certi...', 'Licensor Certificate Name', 'SCP Registration', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main area contains the following text: 'The AD RMS cluster key password is used to encrypt the cluster key that is stored in the configuration database. For other AD RMS servers to join this cluster, you must be able to supply this password.' Below this are two password input fields: 'Password:' and 'Confirm Password:', both containing masked characters. An information icon (i) is followed by the text: 'It is highly recommended that you carefully preserve this password. This password is required for other AD RMS servers to join this AD RMS cluster. This password is also needed to restore the AD RMS cluster from a backup.' At the bottom right are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.



- Trong mục **Select AD RMS Cluster Web Site**, chọn **Default Web Site**, nhấn **Next**.



- Trong mục **Specify Cluster Address**, chọn **Use an SSL-encrypted connection (https://)**, nhấn **Next**.

**Add Roles Wizard**

**Specify Cluster Address**

Before You Begin

Server Roles

AD RMS

Role Services

AD RMS Cluster

Configuration Database

Service Account

Cluster Key Storage

Cluster Key Password

Cluster Web Site

**Cluster Address**

Server Authentication Certi...

Licensor Certificate Name

SCP Registration

Web Server (IIS)

Role Services

Confirmation

Progress

Results

A cluster address enables AD RMS clients to communicate with this cluster over the network. It is recommended that you configure AD RMS to use the Secure Sockets Layer (SSL) protocol to encrypt network traffic between AD RMS clients and the cluster.

Specify a connection type for this AD RMS cluster.

☒ Use an SSL-encrypted connection (https://)

The Web site you have selected does not have SSL enabled. After you click Next, you will be given the choice to select an SSL certificate for this Web site.

☐ Use an unencrypted connection (http://)

You cannot use this option if you want to add Identity Federation Support.

Specify an internal address for this AD RMS cluster. You cannot change this address or port number after AD RMS is installed and configured.

Internal Address

Fully-Qualified Domain Name:  Port:

https://

Preview of cluster address for clients on the network:

< Previous Next > Install Cancel

- Trong mục **Choose a Server Authentication Certificate for SSL Encryption**, chọn **Create a self-signed certificate for SSL encryption**, nhấn **Next**.

The screenshot shows the 'Add Roles Wizard' window with the title 'Choose a Server Authentication Certificate for SSL Encryption'. The left sidebar contains a tree view with the following items: 'Before You Begin', 'Server Roles', 'AD RMS', 'Role Services', 'AD RMS Cluster', 'Configuration Database', 'Service Account', 'Cluster Key Storage', 'Cluster Key Password', 'Cluster Web Site', 'Cluster Address', 'Server Authentication Certi...', 'Licensor Certificate Name', 'SCP Registration', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The 'Server Authentication Certi...' item is selected and highlighted in blue.

The main content area contains the following text:

When communicating with clients, AD RMS uses the Secure Sockets Layer (SSL) protocol to encrypt network traffic. Choose a server authentication certificate suitable for SSL encryption to add to the AD RMS site in Internet Information Services (IIS).

There are three radio button options:

- ☐ Choose an existing certificate for SSL encryption (recommended)  
This option is recommended for most production scenarios. You should use a certificate issued by an external certification authority (CA) or you can use a certificate issued by your own internal CA if the CA is trusted by clients connecting to this server. The subject name of the certificate must match the host name of this server.
- ☒ Create a self-signed certificate for SSL encryption  
This option is recommended for small-scale deployments or test scenarios only. After installing AD RMS, you must manually install the certificate on clients that communicate with this server.
- ☐ Choose a certificate for SSL encryption later  
This option is recommended if you plan to request a certificate from a CA and import it later.  
 For AD RMS to function, you must configure this server with a valid certificate.

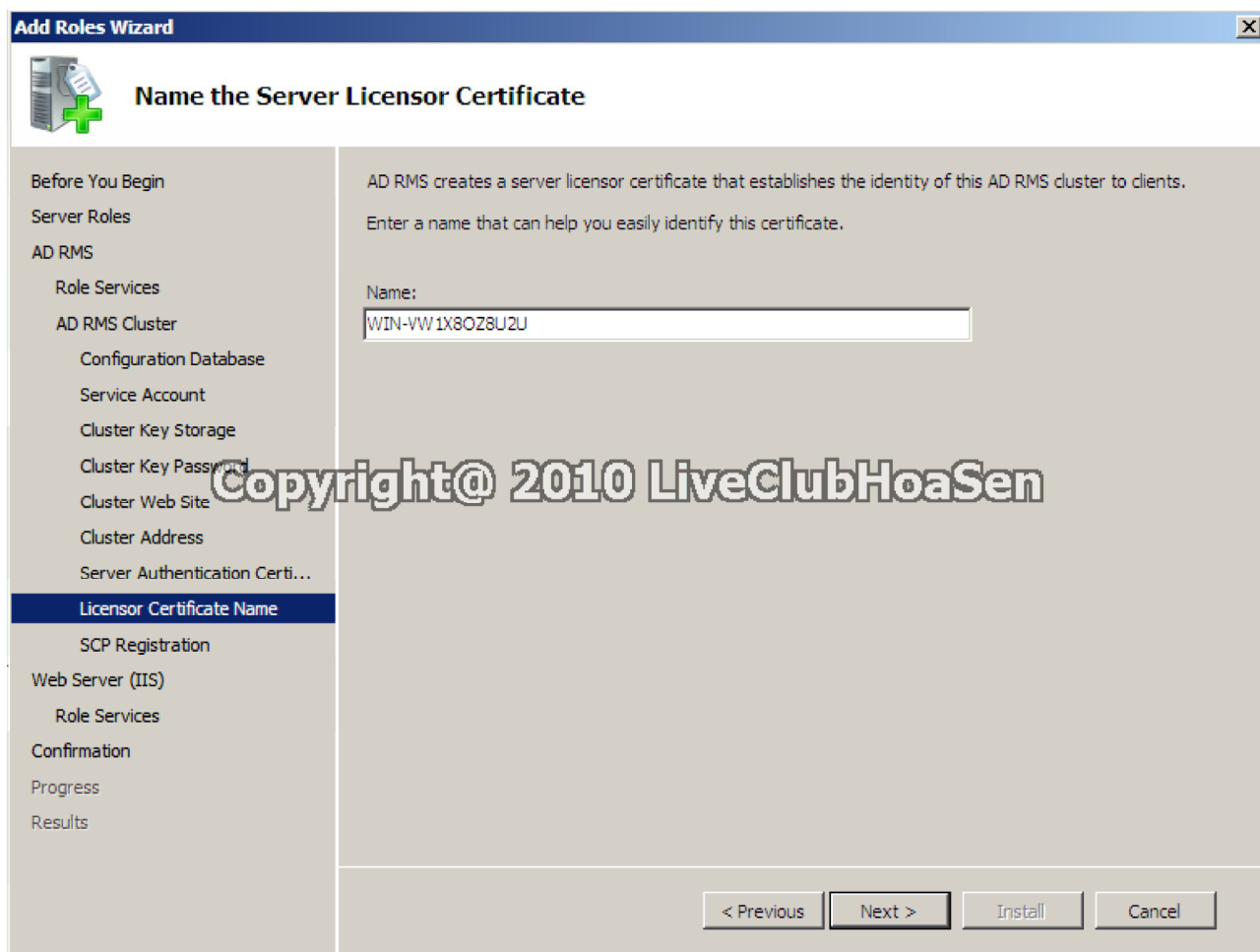
Below the options is a table with the following data:

Issued To	Issued By	Expiration Date	Intended Purpose
WIN-VW1X8OZ8U2U...	HSU-WI...	10/24/2010	Client Authentication,...
HSU-WIN-VW1X8OZ...	HSU-WI...	10/24/2014	<Any EKU>, CRL Sign...

To the right of the table are three buttons: 'Properties', 'Import', and 'Refresh'.

At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

- Trong mục **Name the Server Licensor Certificate**, nhập tên máy Server vào ô **Name**, nhấn **Next**.



**Add Roles Wizard**

**Name the Server Licensor Certificate**

Before You Begin  
Server Roles  
AD RMS  
Role Services  
AD RMS Cluster  
Configuration Database  
Service Account  
Cluster Key Storage  
Cluster Key Password  
Cluster Web Site  
Cluster Address  
Server Authentication Certificate  
**Licensor Certificate Name**  
SCP Registration  
Web Server (IIS)  
Role Services  
Confirmation  
Progress  
Results

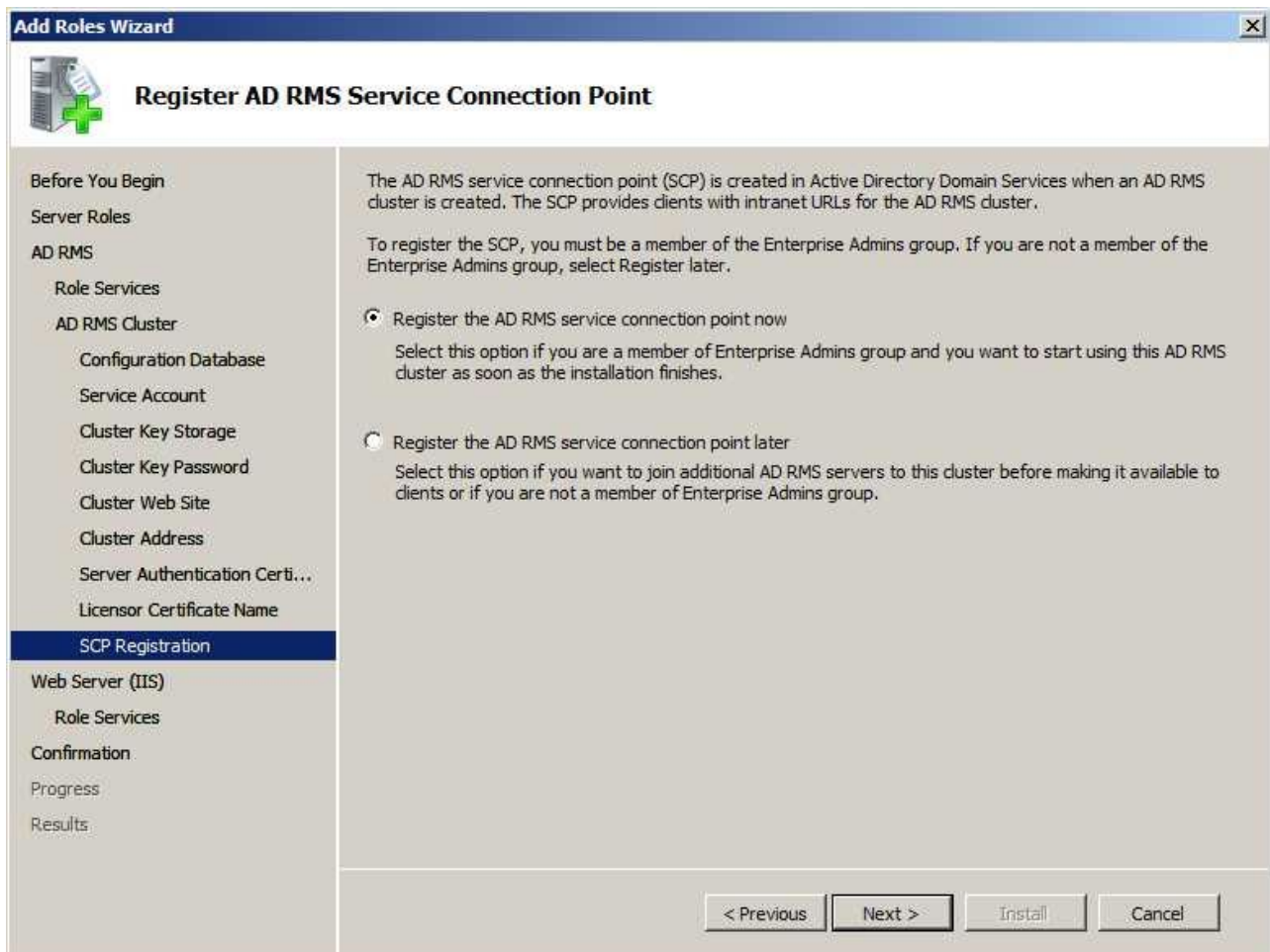
AD RMS creates a server licensor certificate that establishes the identity of this AD RMS cluster to clients.  
Enter a name that can help you easily identify this certificate.

Name:  
WIN-VW1X8OZ8U2U

< Previous   Next >   Install   Cancel

Copyright@ 2010 LiveClubHoaSen

- Trong mục **Register AD RMS Service Connection Point**, chọn **Register the AD RMS service connection point now**, nhấn **Next**.



The screenshot shows the 'Add Roles Wizard' window with the title 'Register AD RMS Service Connection Point'. The left sidebar lists the steps: 'Before You Begin', 'Server Roles', 'AD RMS', 'Role Services', 'AD RMS Cluster', 'Configuration Database', 'Service Account', 'Cluster Key Storage', 'Cluster Key Password', 'Cluster Web Site', 'Cluster Address', 'Server Authentication Certi...', 'Licensor Certificate Name', 'SCP Registration' (highlighted), 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main pane contains the following text:

The AD RMS service connection point (SCP) is created in Active Directory Domain Services when an AD RMS cluster is created. The SCP provides clients with intranet URLs for the AD RMS cluster.

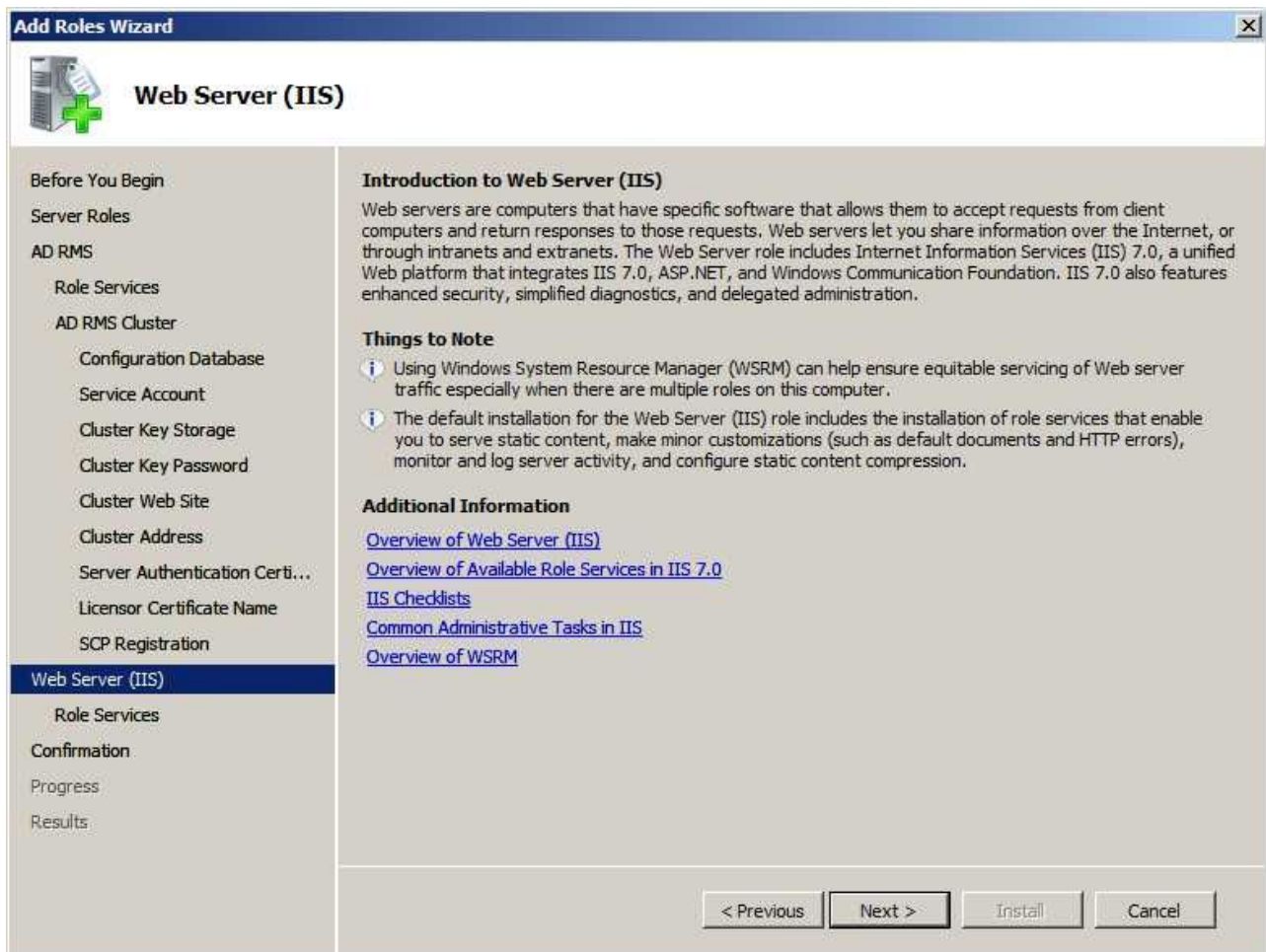
To register the SCP, you must be a member of the Enterprise Admins group. If you are not a member of the Enterprise Admins group, select Register later.

☒ Register the AD RMS service connection point now  
Select this option if you are a member of Enterprise Admins group and you want to start using this AD RMS cluster as soon as the installation finishes.

☐ Register the AD RMS service connection point later  
Select this option if you want to join additional AD RMS servers to this cluster before making it available to clients or if you are not a member of Enterprise Admins group.

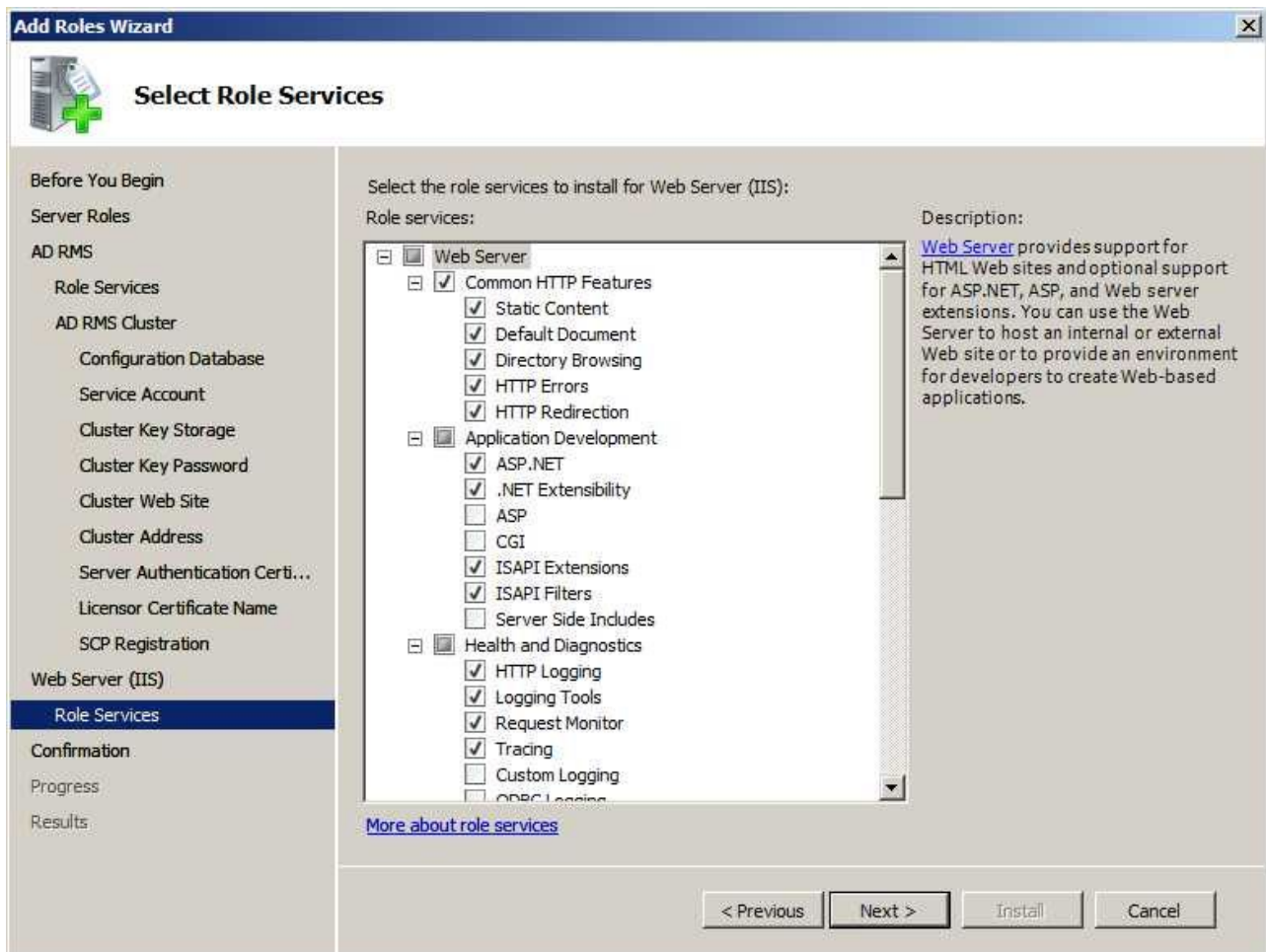
At the bottom right, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

- Trong mục **Web Server (IIS)**, nhấn **Next**.

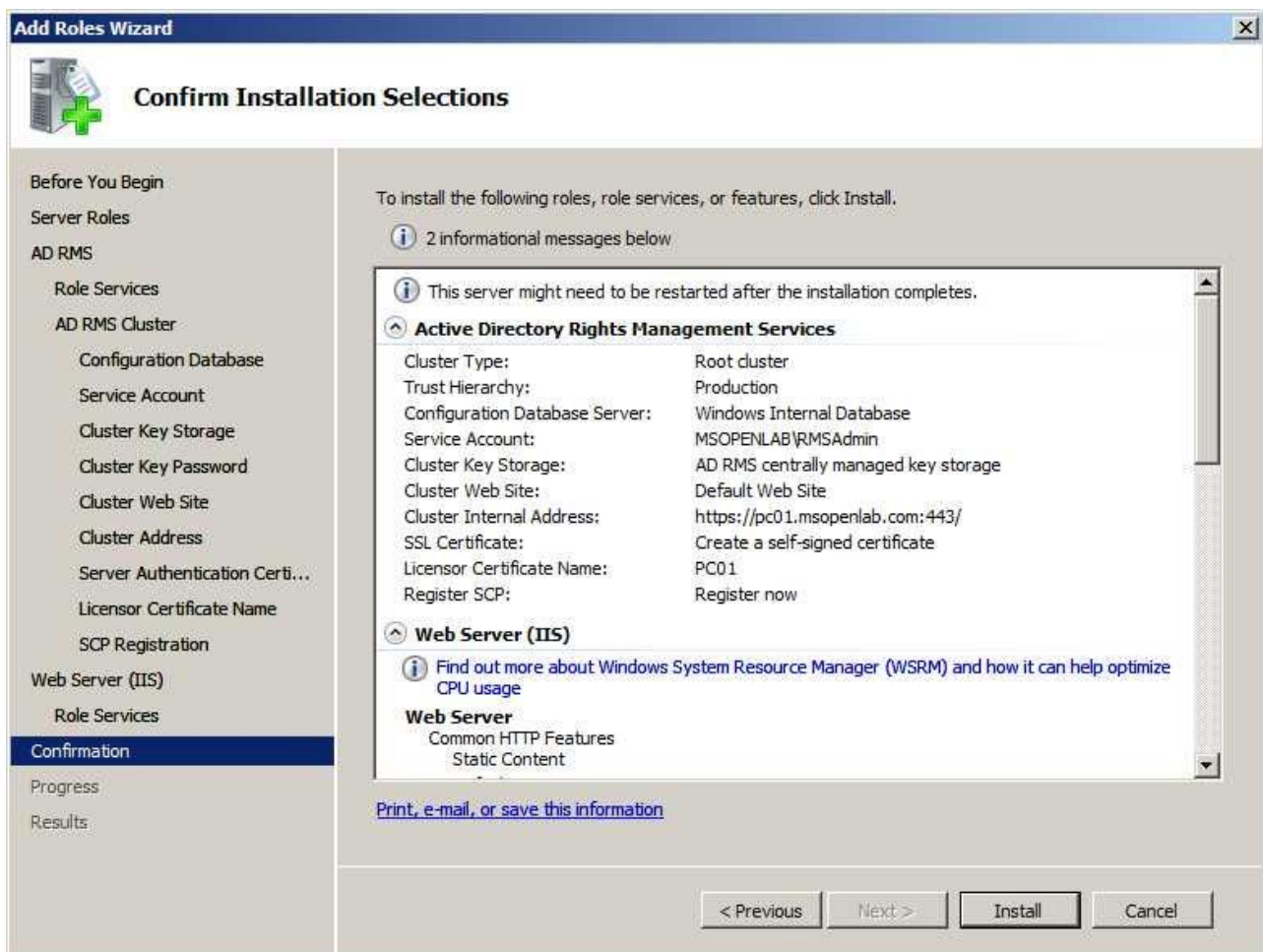




- Trong mục **Select Role Services**, nhấn **Next**.



- Trong mục **Confirm Installation Selections**, nhấn **Install**.



**Lưu ý:** Sau khi cài đặt thành công phải **restart** máy.

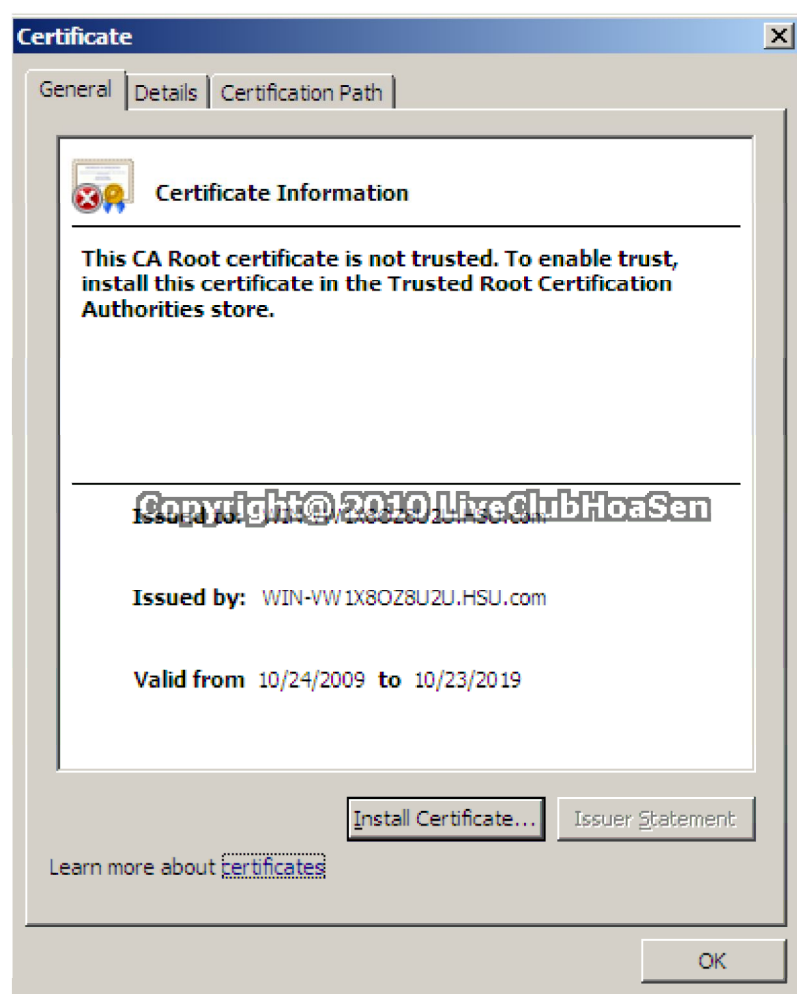


**B. Cấu hình RMS**

- Nhấn **Start**, mở **Administrative Tools**, mở **Active Directory Rights Management Services**.
- Trong khi khởi động dịch vụ chờ hộp thoại **Security Alert** xuất hiện, nhấn **View Certificate**.



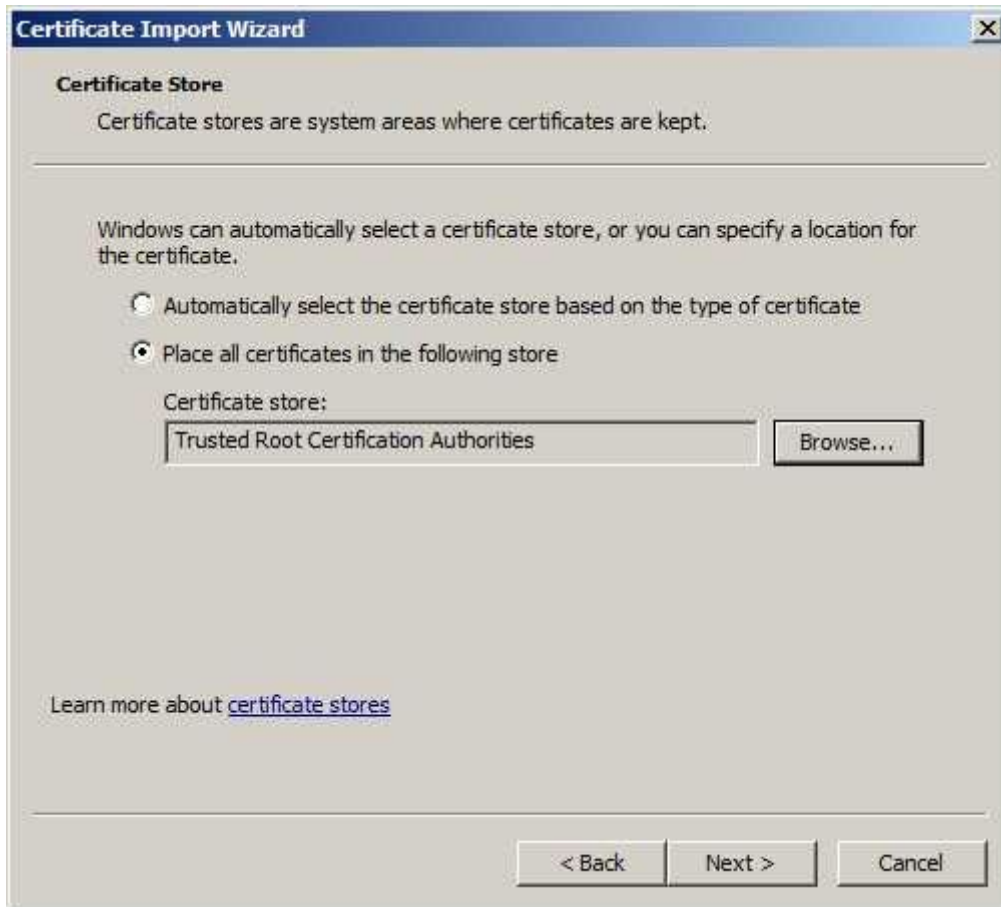
- Trong Hộp thoại **Certificate**, nhấn **Install Certificate**.



- Trong Cửa sổ **Welcome to the Certificate Import Wizard**, nhấn **Next**.



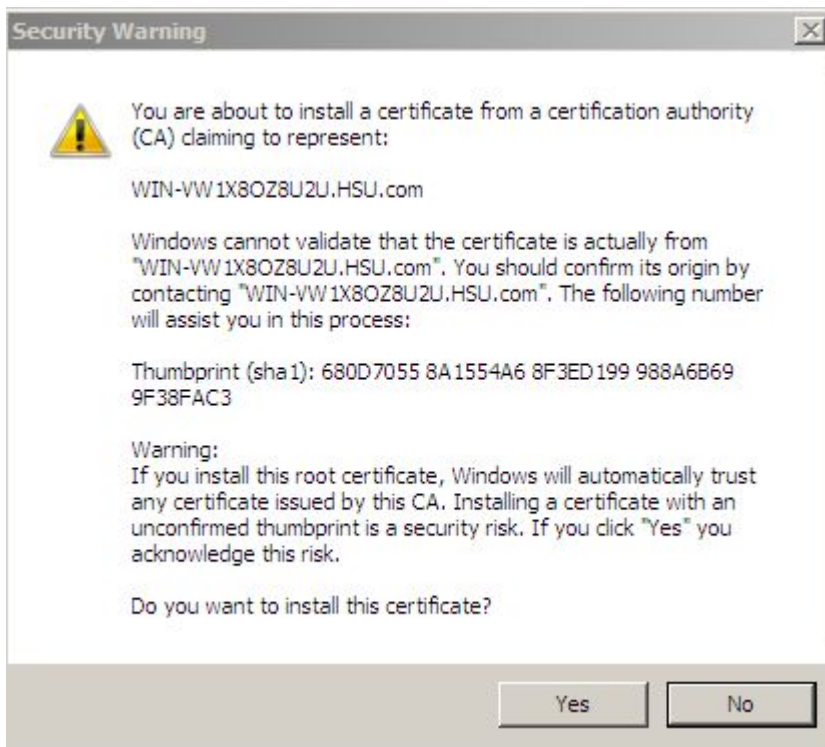
- Trong mục **Certificate Store**, chọn **Place all certificate in the following store**, trong ô **Certificate store**, chọn đường dẫn đến **Trusted Root Certification Authorities**, nhấn **Next**.



- Trong mục **Completing the Certificate Import Wizard**, nhấn **Finish**.



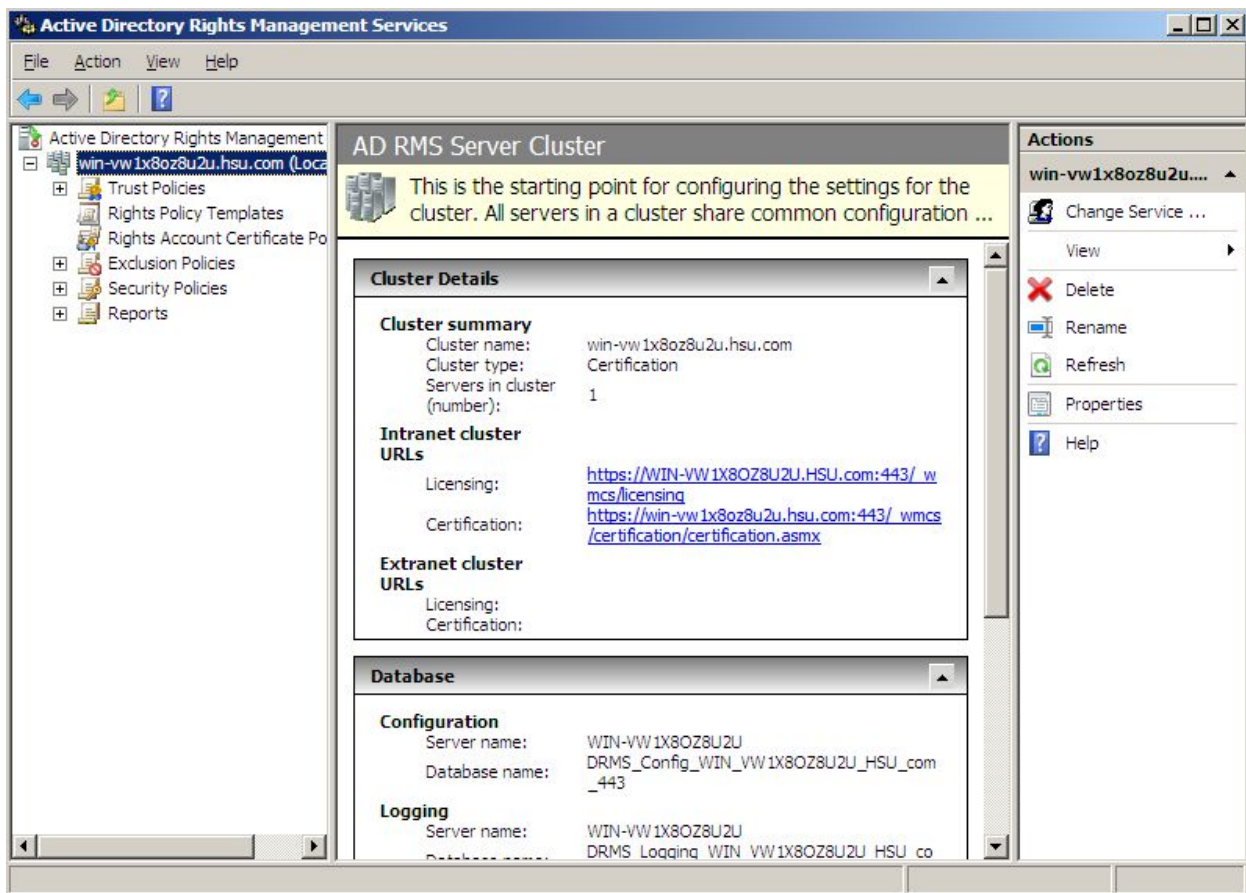
- Trong hộp thoại **Security Warning**, nhấn **Yes**.



- Hộp thoại **Certificate Import Wizard**, nhấn **OK**.




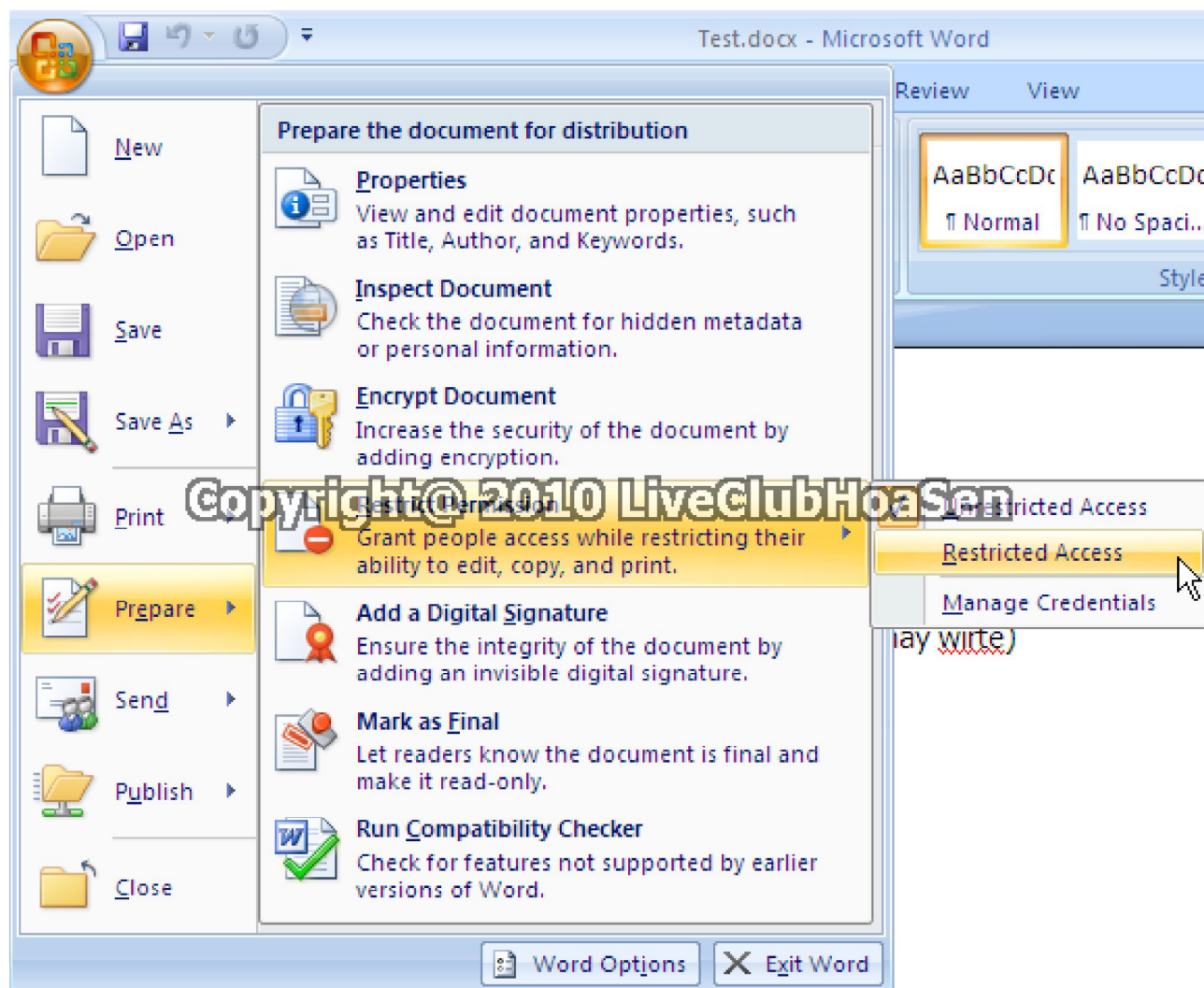
- Trong cửa sổ **Active Directory Rights Management Services**, mở **RMS server** kiểm tra cấu hình RMS đã hoàn tất.



### 3. Phân quyền trên tài nguyên

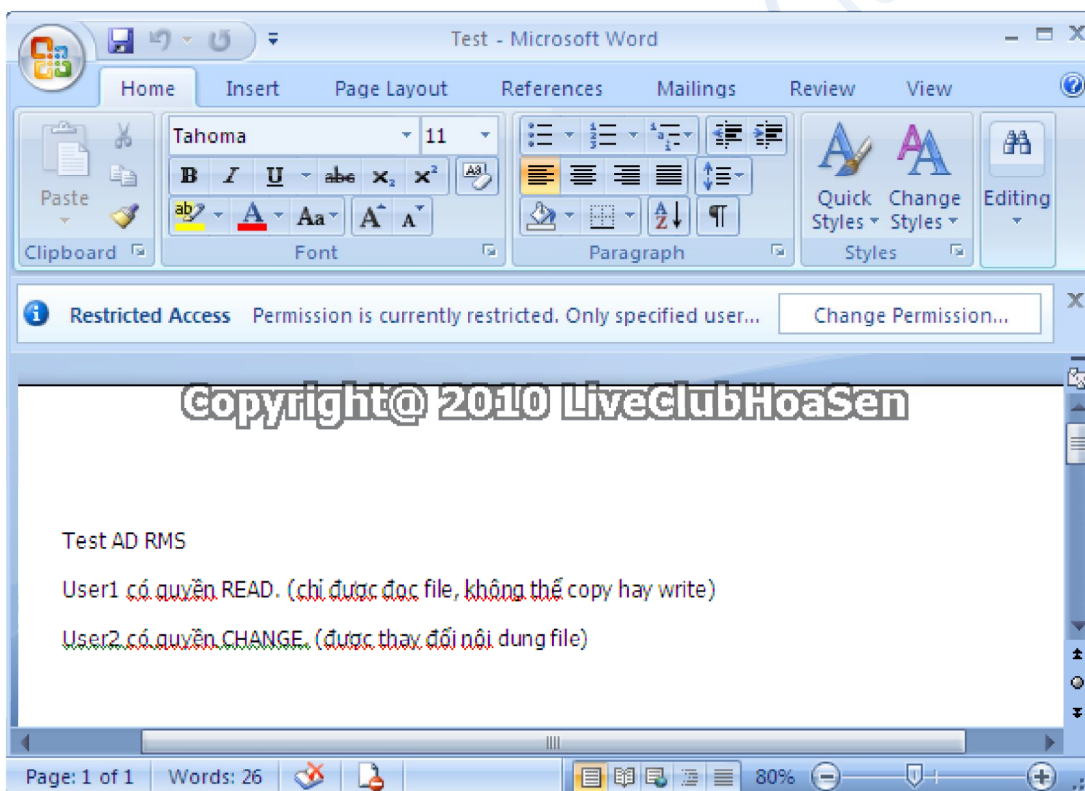
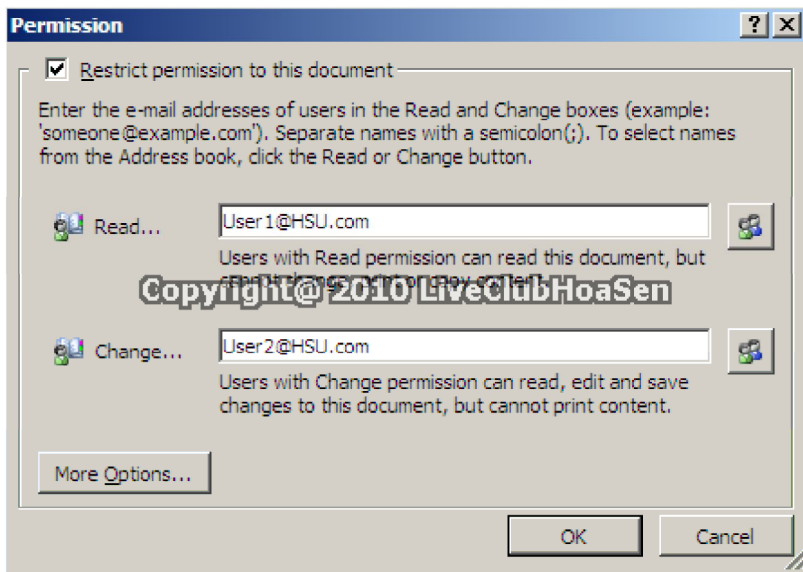


- Mở file **test.docx**, click vào biểu tượng .
- Trong **Prepare**, chọn **Restrict Permission**, chọn **Restricted Access**



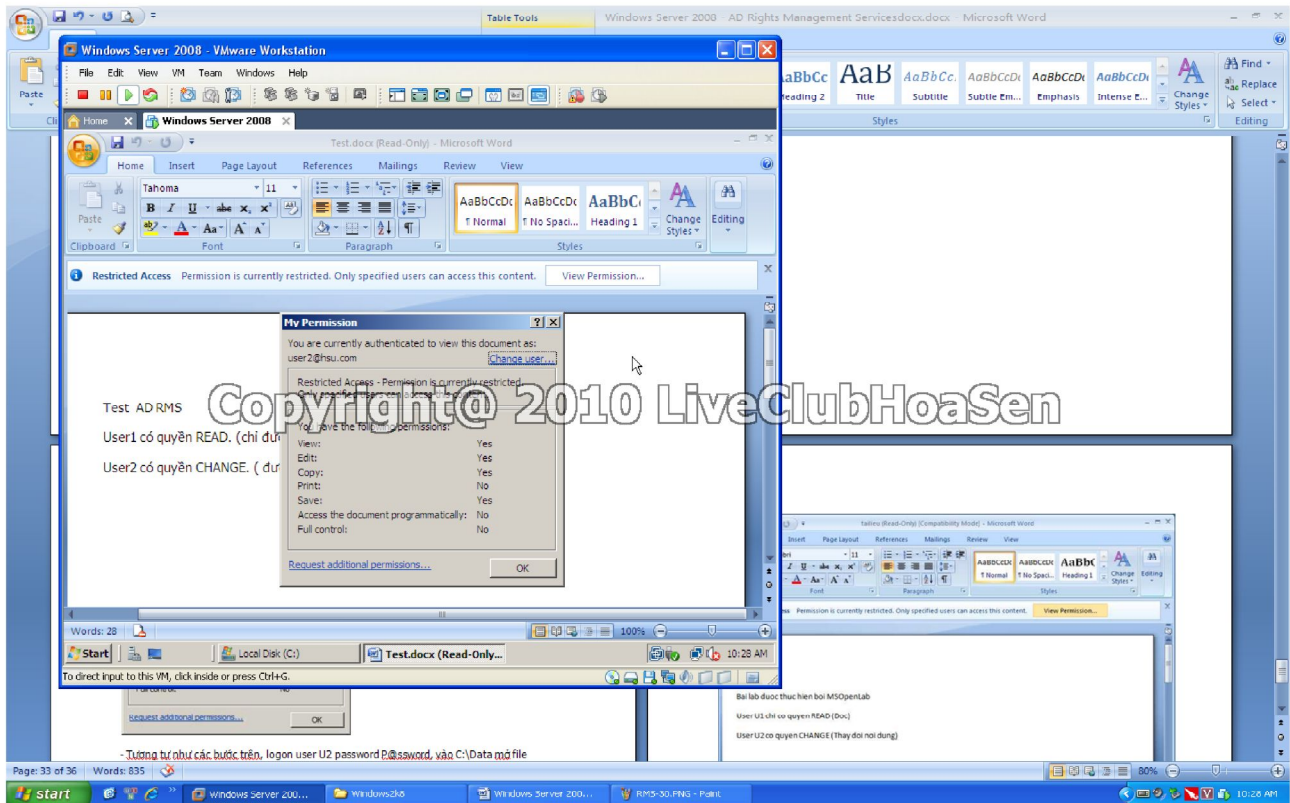


- Trong hộp thoại **Permission**, add **User1** vào ô **Read**, **User2** vào ô **Change**, nhấn **OK**.



#### 4. Kiểm tra quyền

- **Log in** User1, mở file **test.docx** trong C:\ nhập User1 và password P@ssw123, **Nhấn OK**
- Cửa sổ **Microsoft Word**, tại thanh **Restricted Access** nhấn **View Permission...**



- Làm tương tự cho **User2**.

- Cửa sổ **Microsoft Word**, tại thanh **Restricted Access** chọn **View Permission...**

