

TRIỂN KHAI CERTIFICATION AUTHORITY (CA)

I. Giới thiệu :

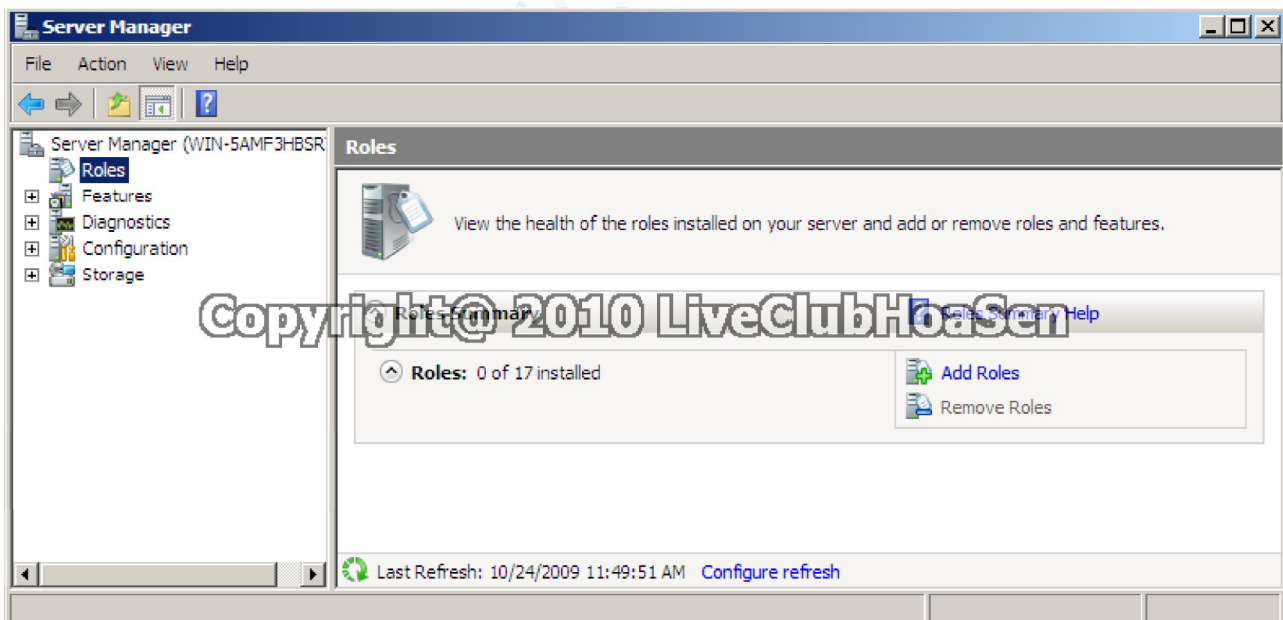
- Ngày nay chúng ta đã quá quen thuộc với việc sử dụng **certificate** trong mã hóa hay chứng thực **CERTIFICATION AUTHORITY (CA)** đúng như tên gọi nó là 1 dịch vụ cấp phát và quản lí các certificate cho người dùng hay cho máy.
- Đặc biệt là trong mạng nội bộ nhu cầu sử dụng **certificate** để chứng thực cho các máy server, user,... hay mã hóa những tài liệu quan trọng của mỗi user, email,... rất lớn.

Hôm nay chúng ta sẽ cùng nhau thực hiện các bước cài đặt **CA** trên Một máy **Windows Server 2008** đã nâng cấp **Domain Controller (DC)** cài đặt HĐH **windows server 2008**.

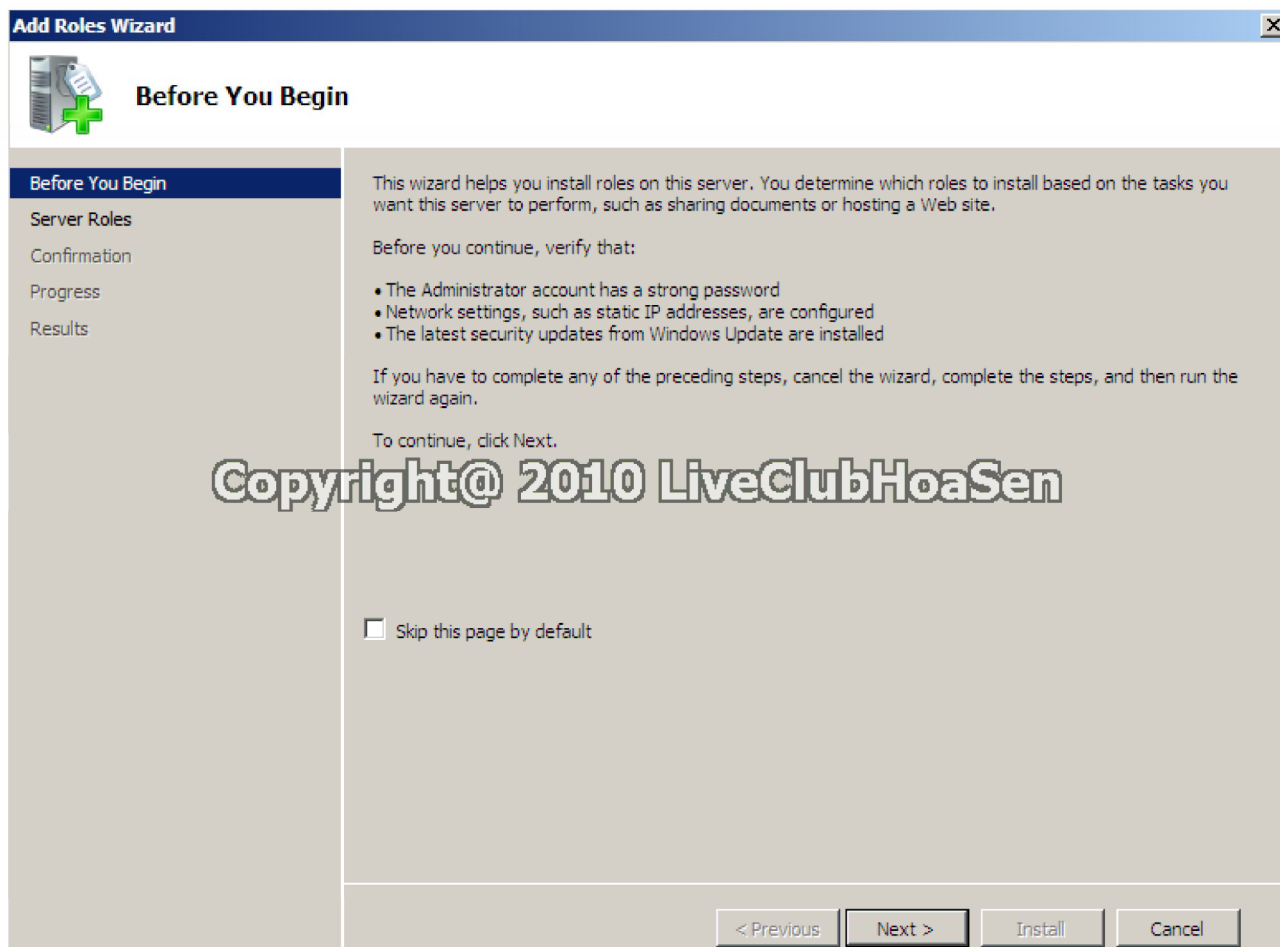
II. Thực hiện :

A. Cài đặt CA:

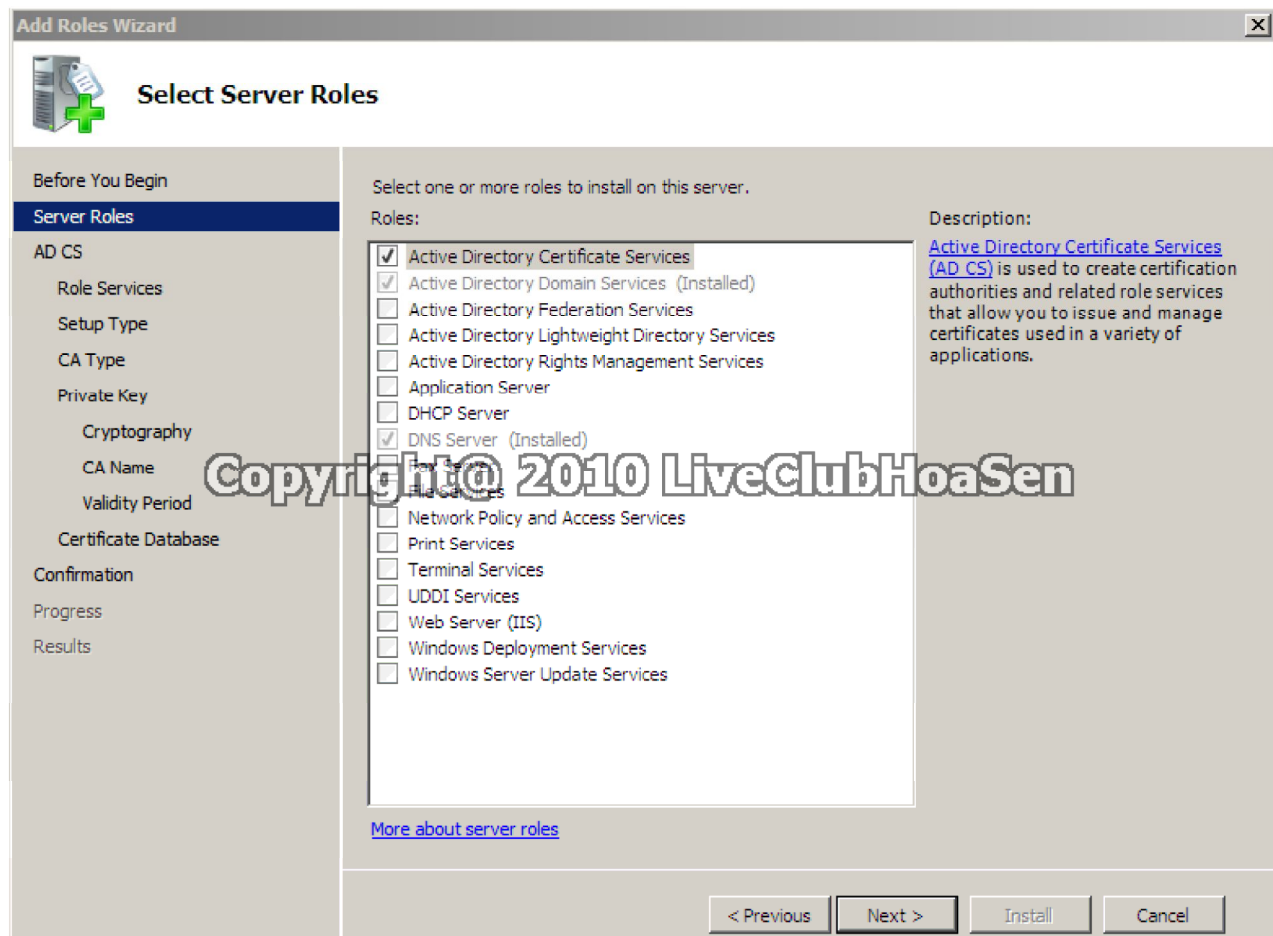
- Login vào máy DC với quyền Admin Domain (HSU\Administrator). Nhấn Start, trong Administrative Tools.
- Mở Server Manager chuột phải Roles chọn Add Roles.



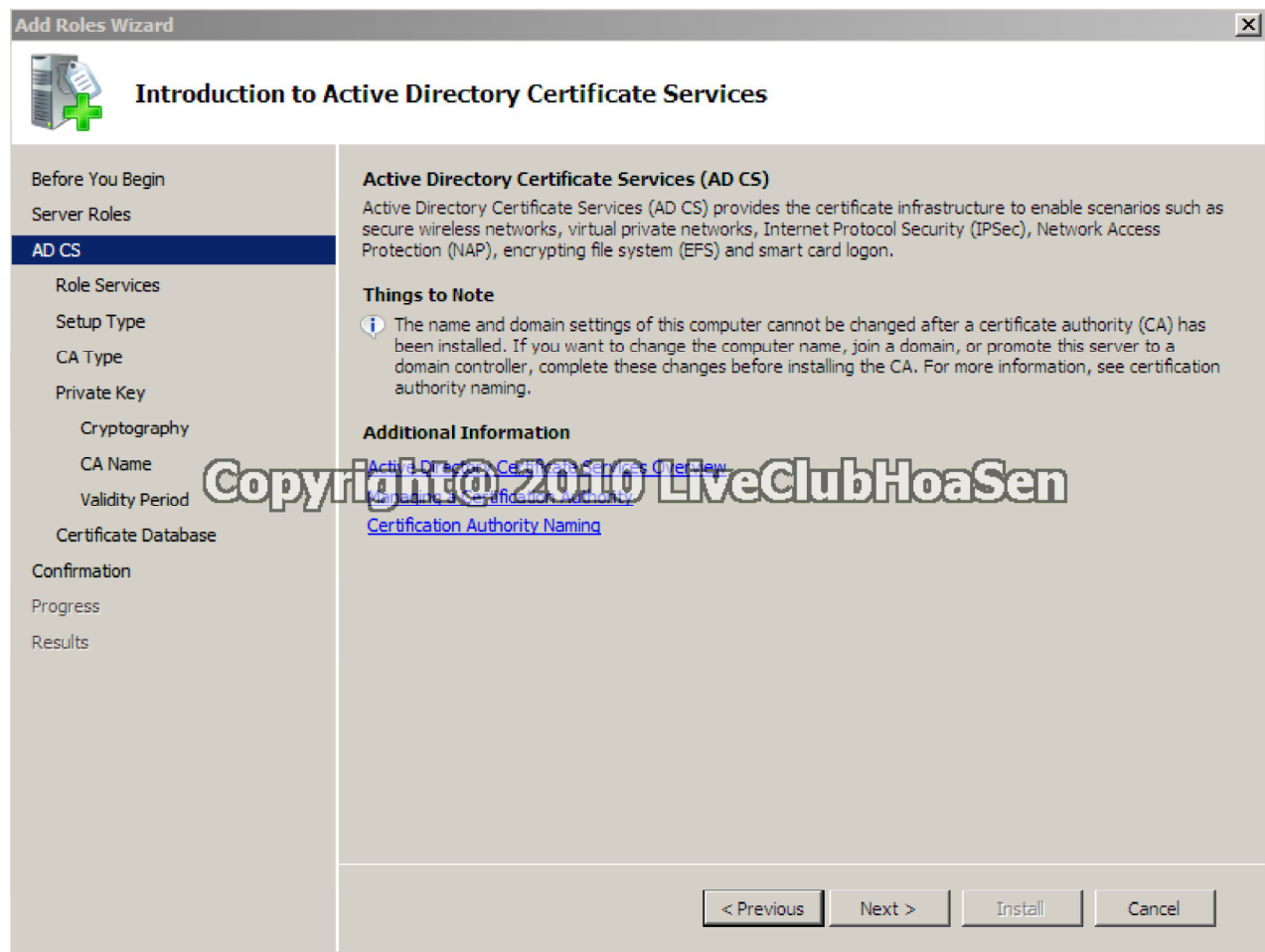
- Trong mục **Before You Begin**, chọn **Next**.



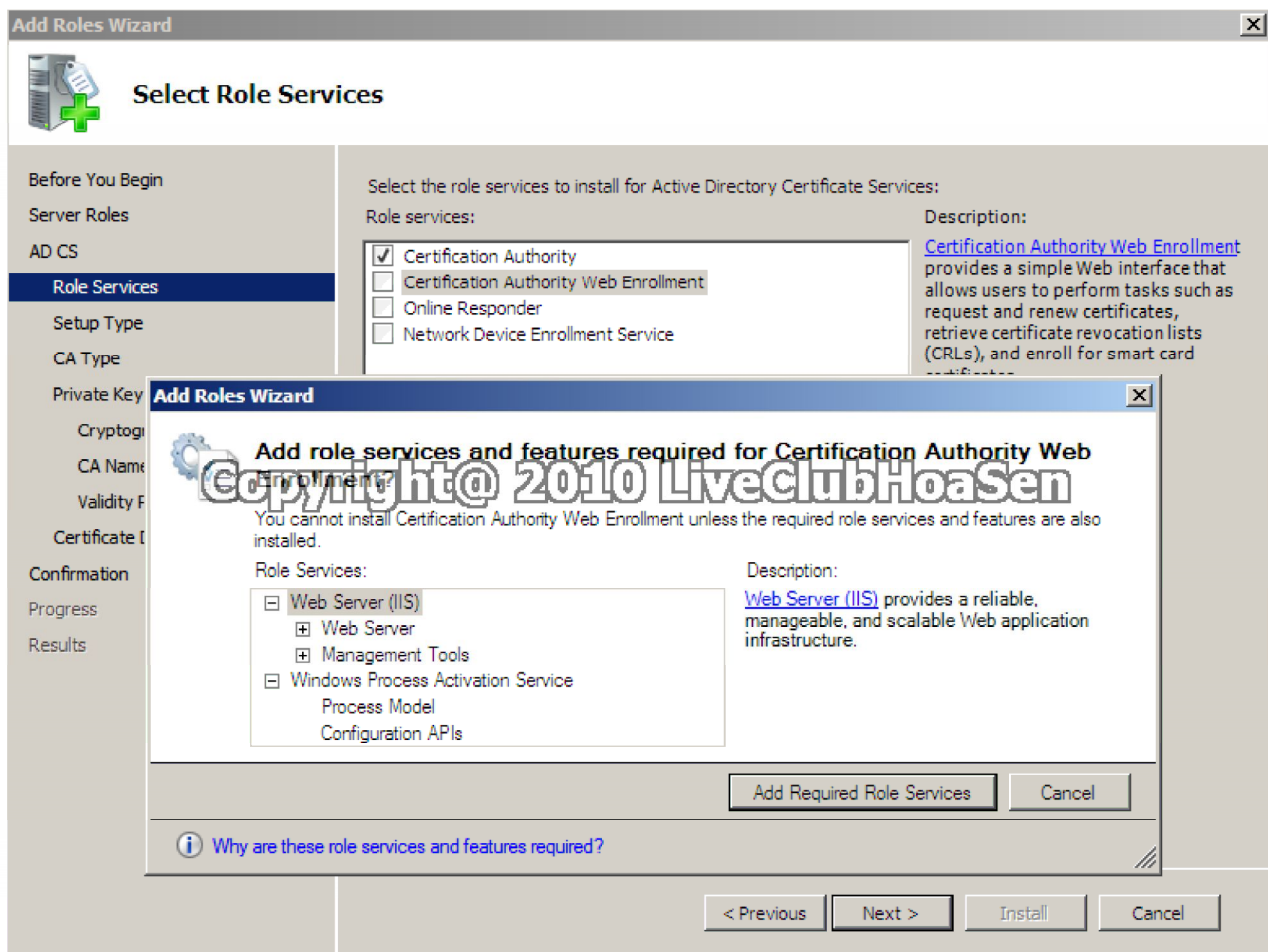
- Trong mục **Select Server Roles**, đánh dấu chọn **Active Directory Certificate Services**, chọn **Next**.



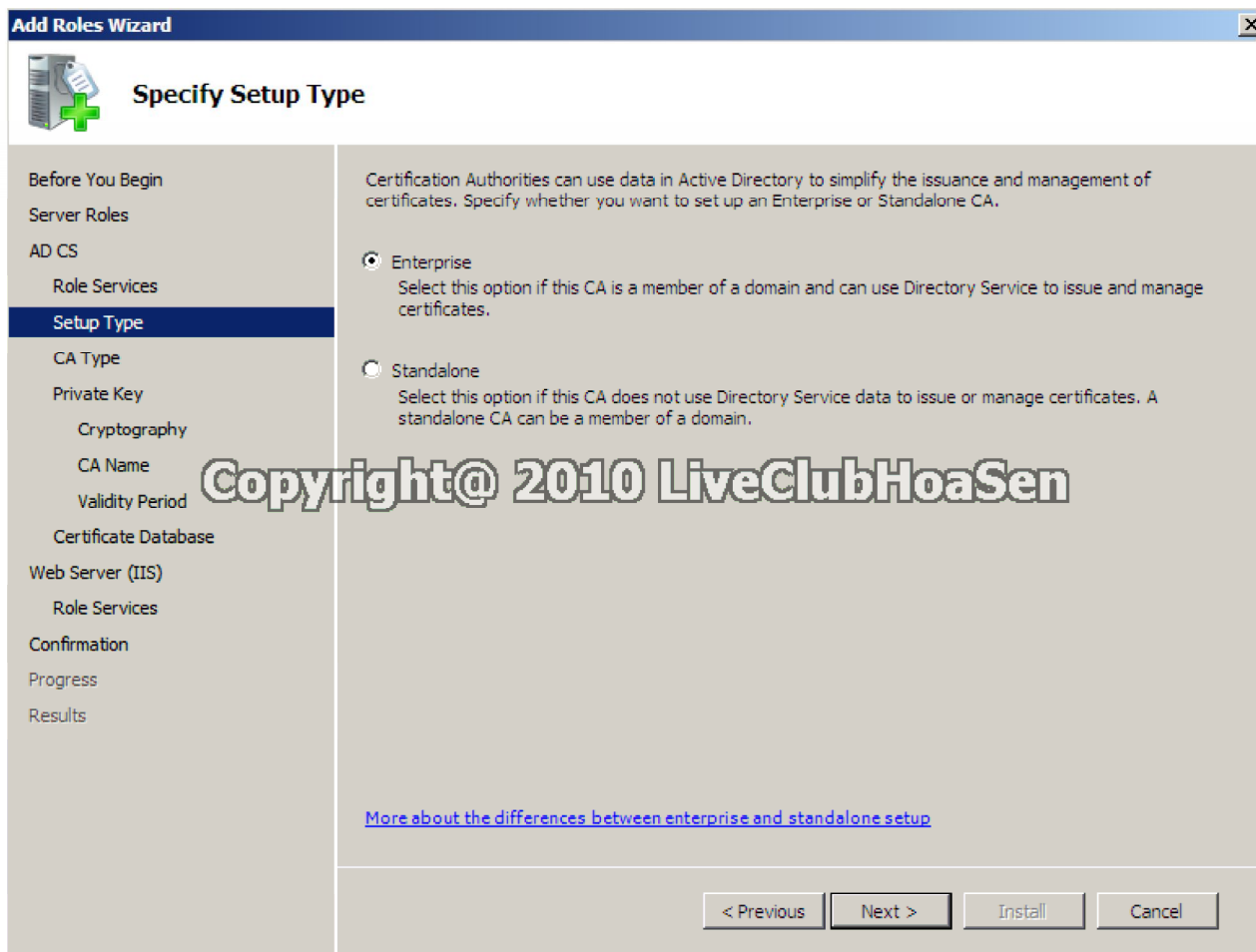
- Trong mục **Introduction to Active Directory Certificate Services**, chọn **Next**.



- Trong mục **Select Role Services**, đánh dấu chọn ô **Certification Authority Web Enrollment**, mục **Add role services required for Certification Authority Web Enrollment**, chọn **Add Required Role Services**.

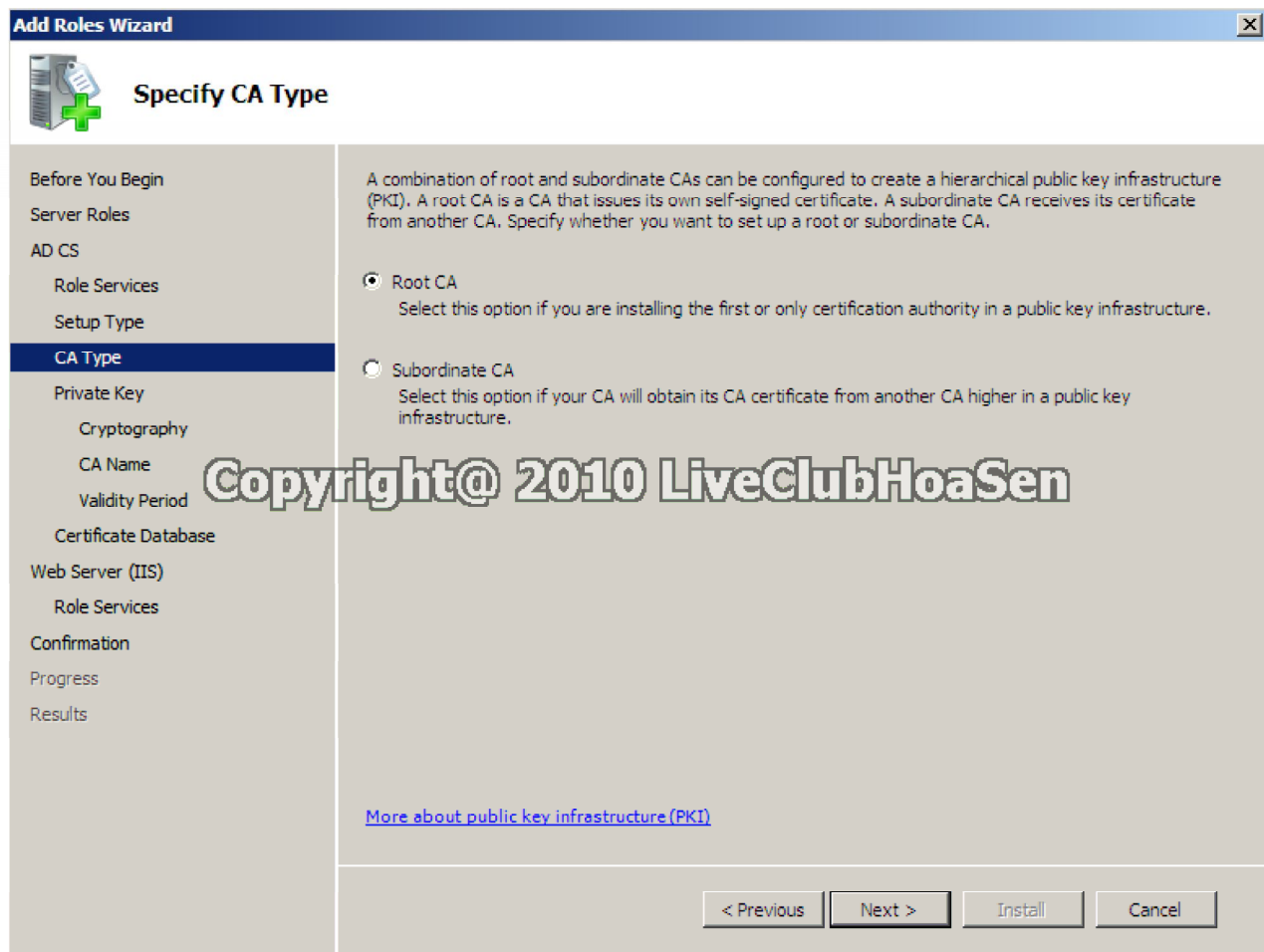


- Hộp thoại **Specify Setup Type**, chọn **Enterprise**, chọn **Next**.



Chú ý : Nếu máy cài CA ko phải là DC hay user login ko phải là Domain admin thì chỉ chọn được chế độ standalone.

- Trong mục **Specify CA Type**, chọn **Root CA**, chọn **Next**.



Add Roles Wizard

Specify CA Type

Before You Begin
Server Roles
AD CS
 Role Services
 Setup Type
CA Type
 Private Key
 Cryptography
 CA Name
 Validity Period
 Certificate Database
Web Server (IIS)
 Role Services
Confirmation
Progress
Results

A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

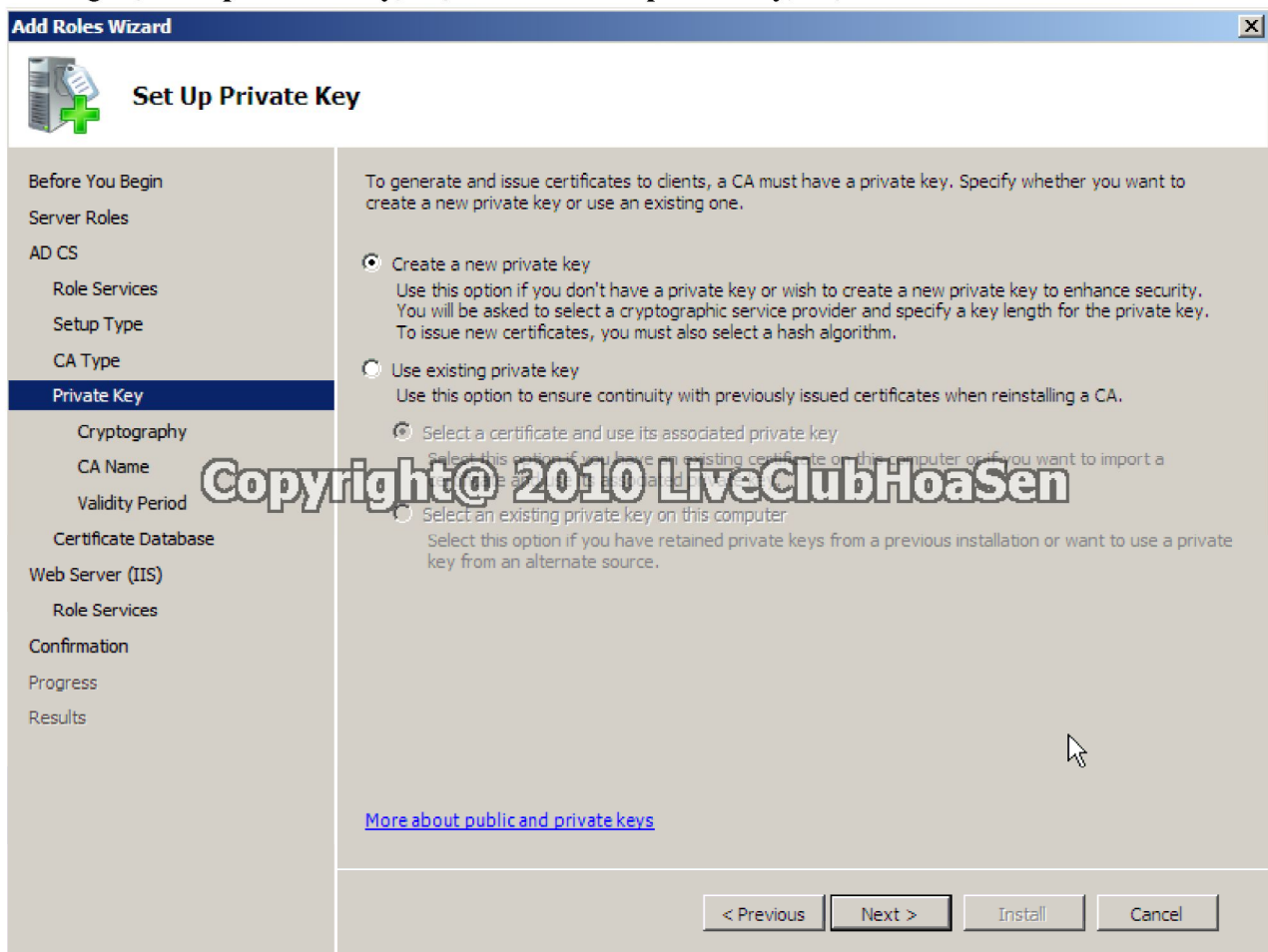
☒ **Root CA**
Select this option if you are installing the first or only certification authority in a public key infrastructure.

☐ **Subordinate CA**
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

[More about public key infrastructure \(PKI\)](#)

< Previous Next > Install Cancel

- Trong mục **Setup Private Key**, chọn **Create a new private key**, chọn **Next**.



- Trong mục **Configure Cryptography for CA**, chọn **Next**.

The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard'. The main window is titled 'Configure Cryptography for CA'. On the left is a navigation pane with the following items: 'Before You Begin', 'Server Roles', 'AD CS', 'Role Services', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography' (highlighted), 'CA Name', 'Validity Period', 'Certificate Database', 'Web Server (IIS)', 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main content area contains the following text: 'To create a new private key, you must first select a [cryptographic service provider](#), [hash algorithm](#), and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.'

Below the text are two dropdown menus: 'Select a cryptographic service provider (CSP):' with 'RSA#Microsoft Software Key Storage Provider' selected, and 'Key character length:' with '2048' selected. Below these is another dropdown menu: 'Select the hash algorithm for signing certificates issued by this CA:' with 'sha1' selected. A checkbox labeled 'Use strong private key protection features provided by the CSP (this may require administrator interaction every time the private key is accessed by the CA)' is unchecked. At the bottom of the main content area is a link: '[More about cryptographic options for a CA](#)'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Copyright@ 2010 LiveClubHoaSen

- Trong mục **Configure CA Name**, chọn **Next**.

Add Roles Wizard

Configure CA Name

Before You Begin
Server Roles
AD CS
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Web Server (IIS)
Role Services
Confirmation
Progress
Results

Type in a common name to identify this CA. This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:
HSU-WIN-5AMF3HBSRT5-CA

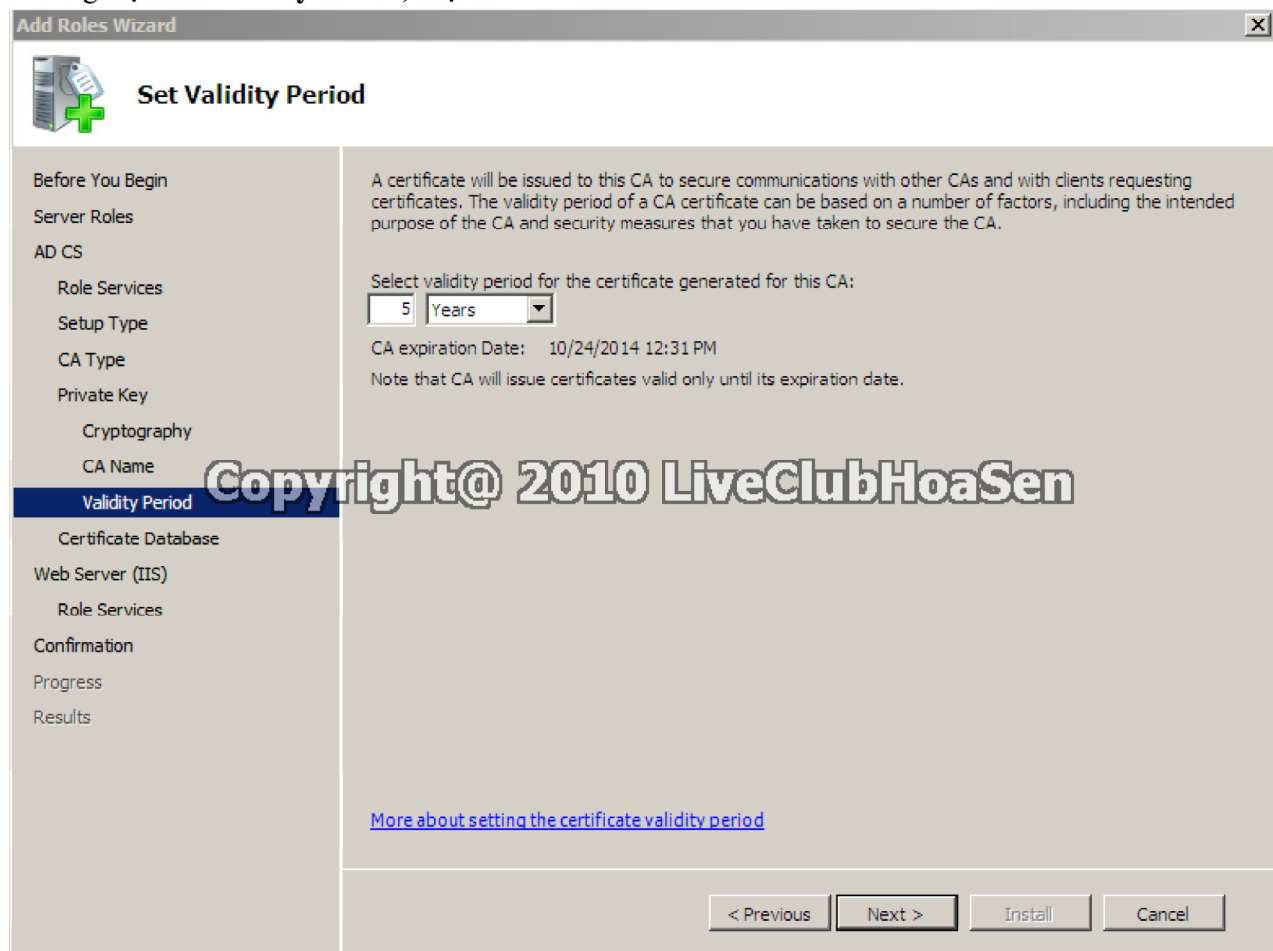
Distinguished name suffix:
DC=HSU,DC=com

Preview of distinguished names:
CN=HSU-WIN-5AMF3HBSRT5-CA,DC=HSU,DC=com

[More about configuring a CA name](#)

< Previous Next > Install Cancel

- Trong mục **Set Validity Period**, chọn **Next**.



Add Roles Wizard

Set Validity Period

Before You Begin

Server Roles

AD CS

Role Services

Setup Type

CA Type

Private Key

Cryptography

CA Name

Validity Period

Certificate Database

Web Server (IIS)

Role Services

Confirmation

Progress

Results

A certificate will be issued to this CA to secure communications with other CAs and with clients requesting certificates. The validity period of a CA certificate can be based on a number of factors, including the intended purpose of the CA and security measures that you have taken to secure the CA.

Select validity period for the certificate generated for this CA:

5 Years

CA expiration Date: 10/24/2014 12:31 PM

Note that CA will issue certificates valid only until its expiration date.

[More about setting the certificate validity period](#)

< Previous Next > Install Cancel

- Trong mục **Configure Certificate Database**, chọn **Next**.

Add Roles Wizard

Configure Certificate Database

The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

Certificate database location:
C:\Windows\system32\CertLog Browse...

☐ Use existing certificate database from previous installation at this location

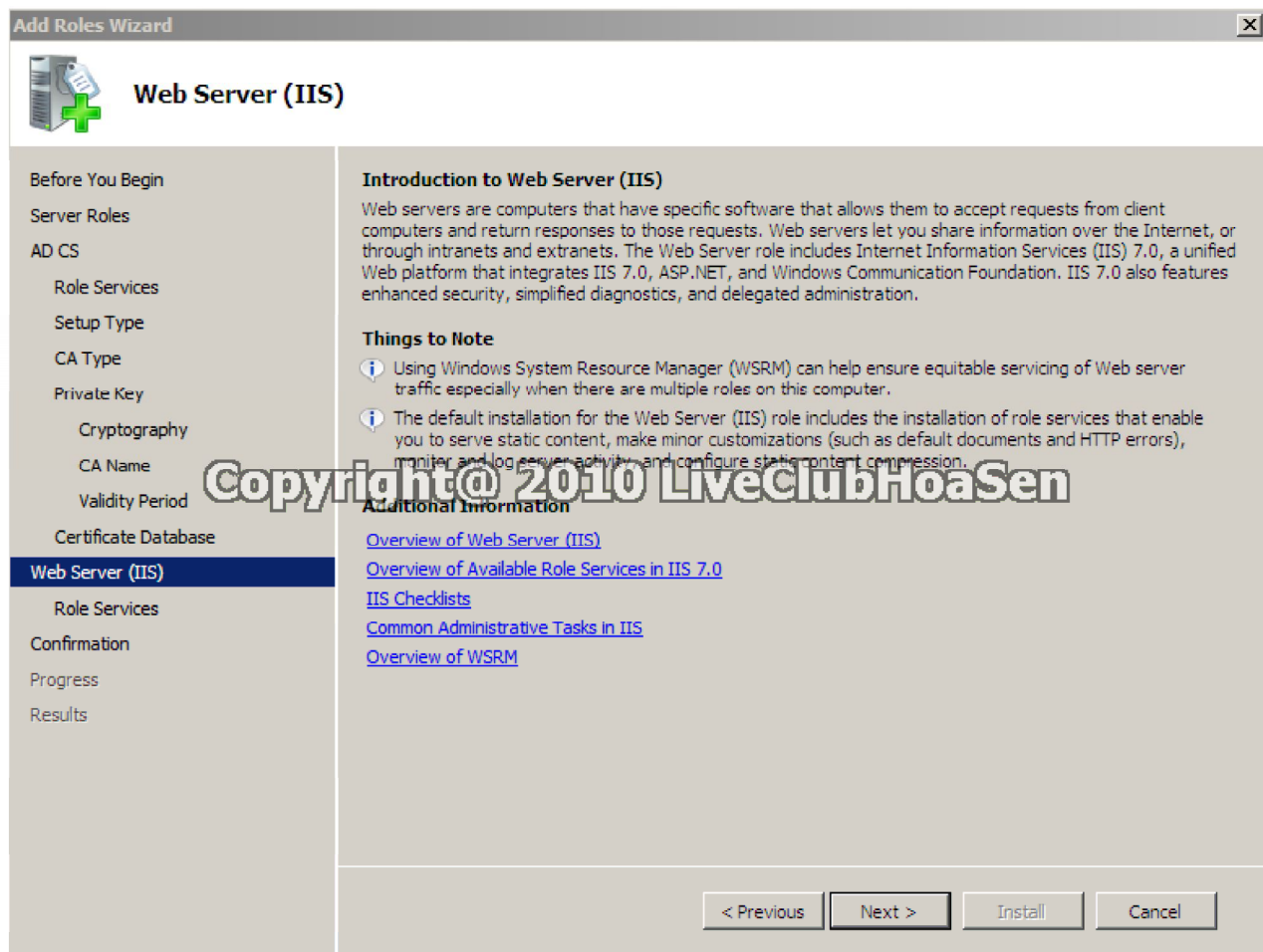
Certificate database log location:
C:\Windows\system32\CertLog Browse...

Navigation:

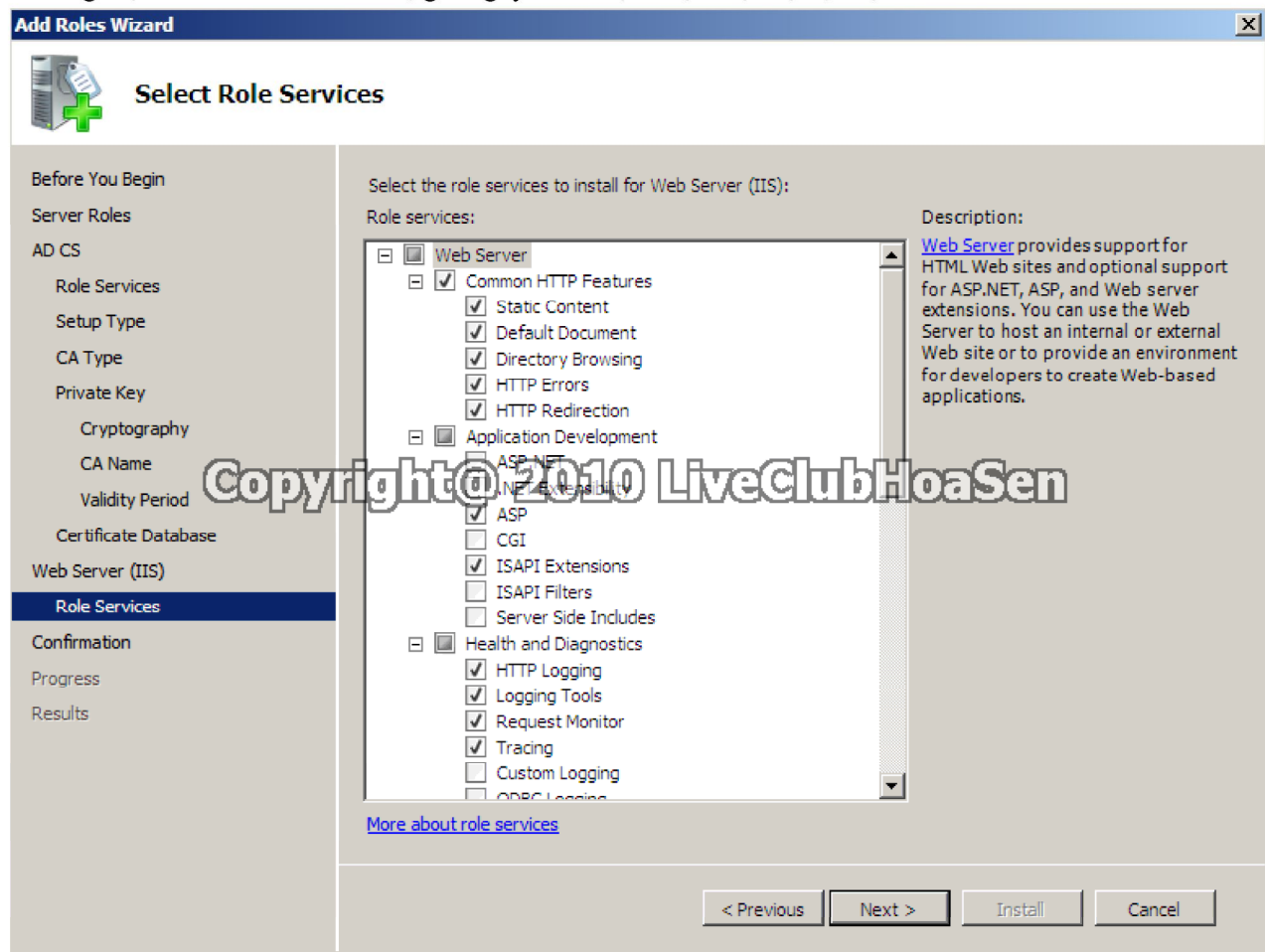
- Before You Begin
- Server Roles
- AD CS
 - Role Services
 - Setup Type
 - CA Type
 - Private Key
 - Cryptography
 - CA Name
 - Validity Period
 - Certificate Database**
 - Web Server (IIS)
 - Role Services
- Confirmation
- Progress
- Results

Buttons: < Previous, Next >, Install, Cancel

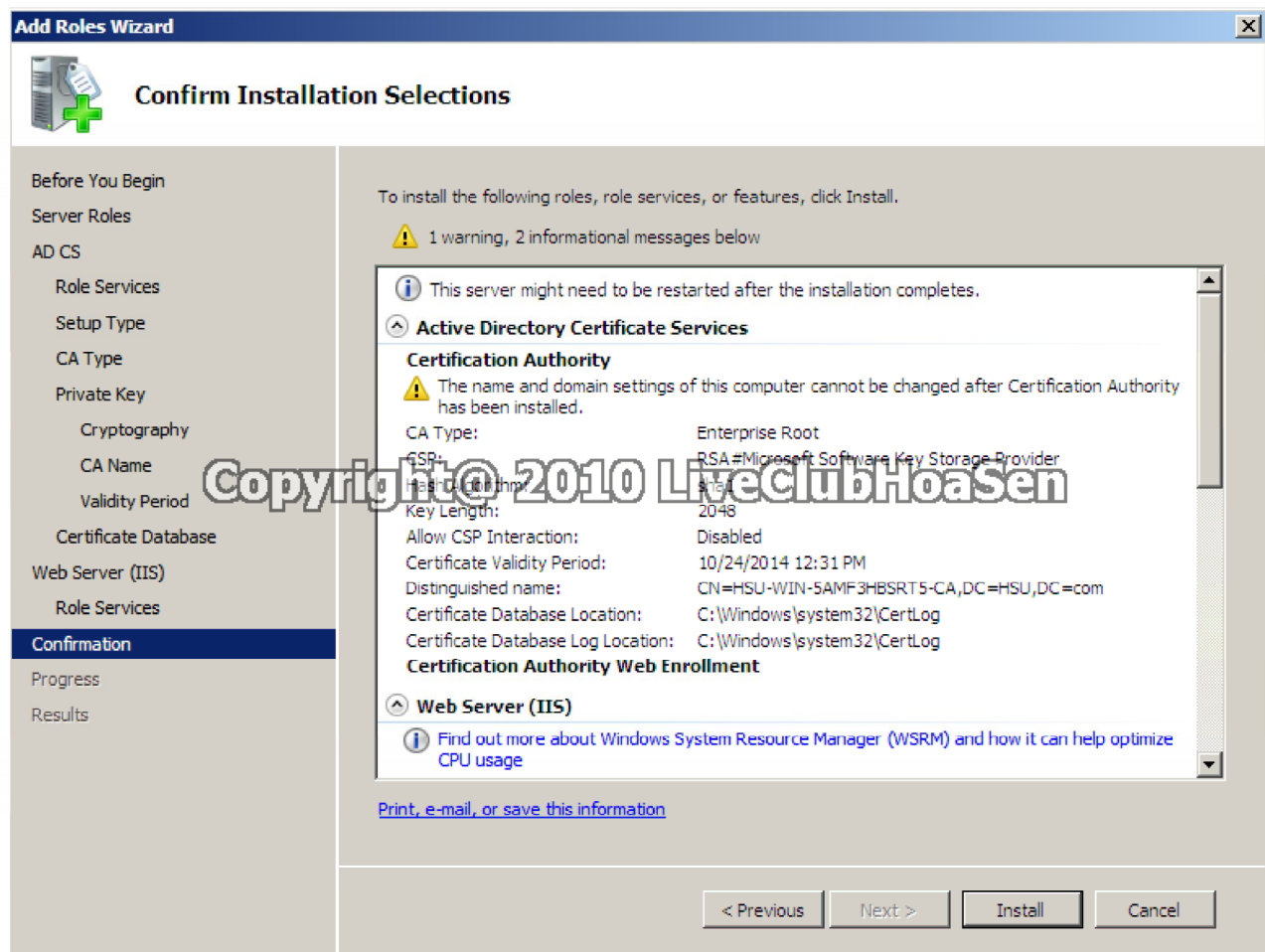
- Trong mục **Web Server (IIS)**, chọn **Next**.



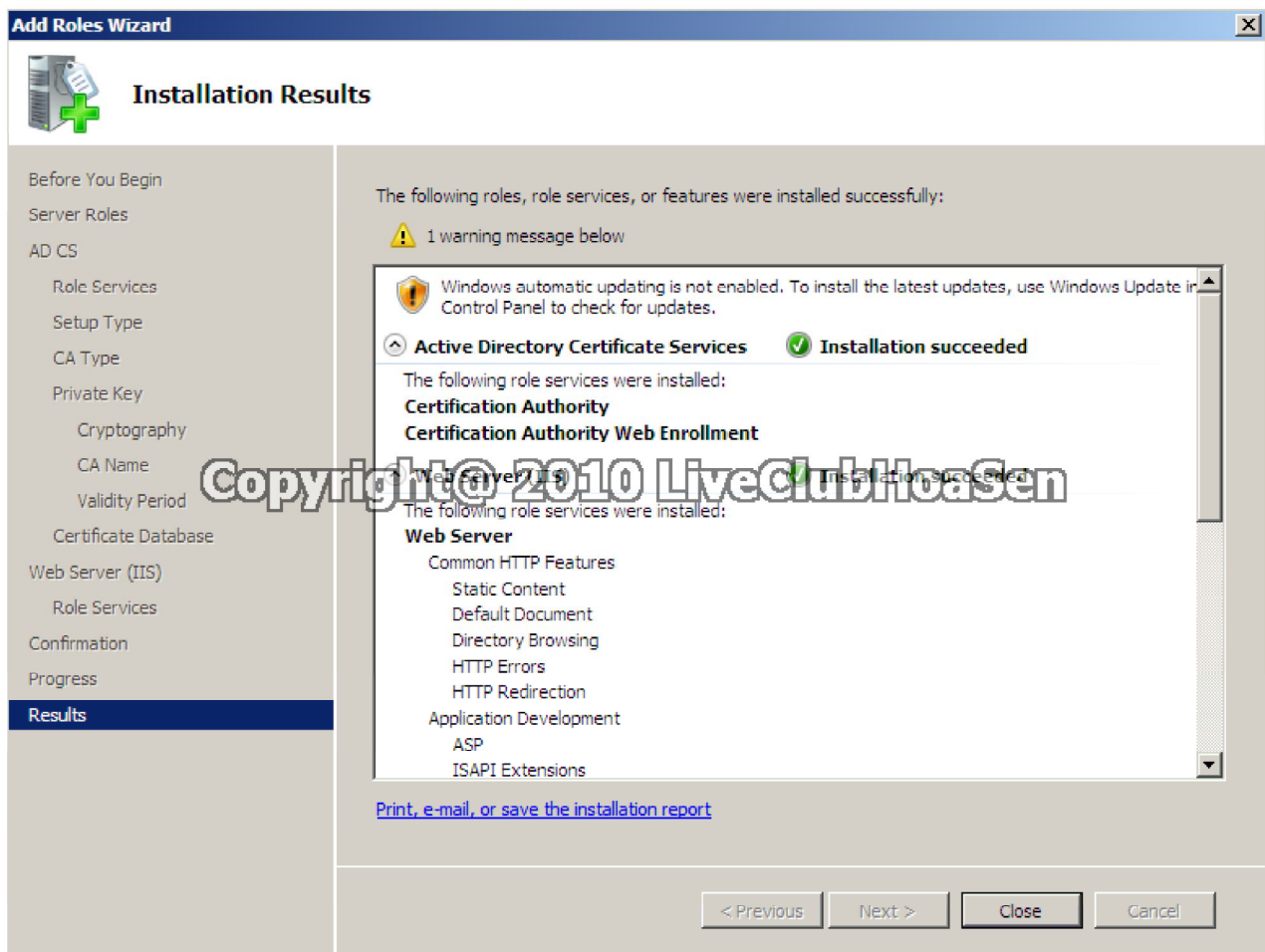
- Trong mục **Select Role Services**, giữ nguyên các lựa chọn mặc định, chọn **Next**.



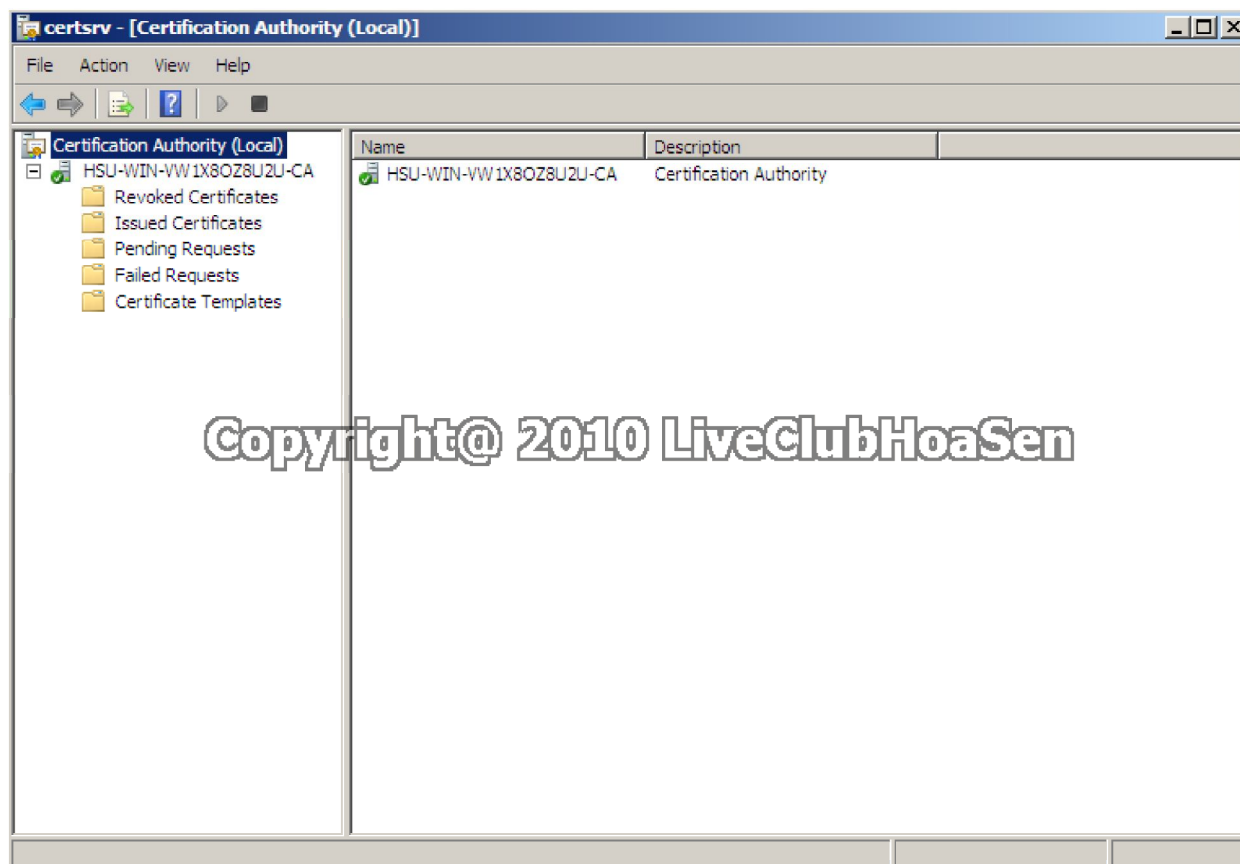
- Trong mục **Confirm Installation Selections**, chọn **Install**.



- Trong mục **Installation Results**, chọn **Close**.

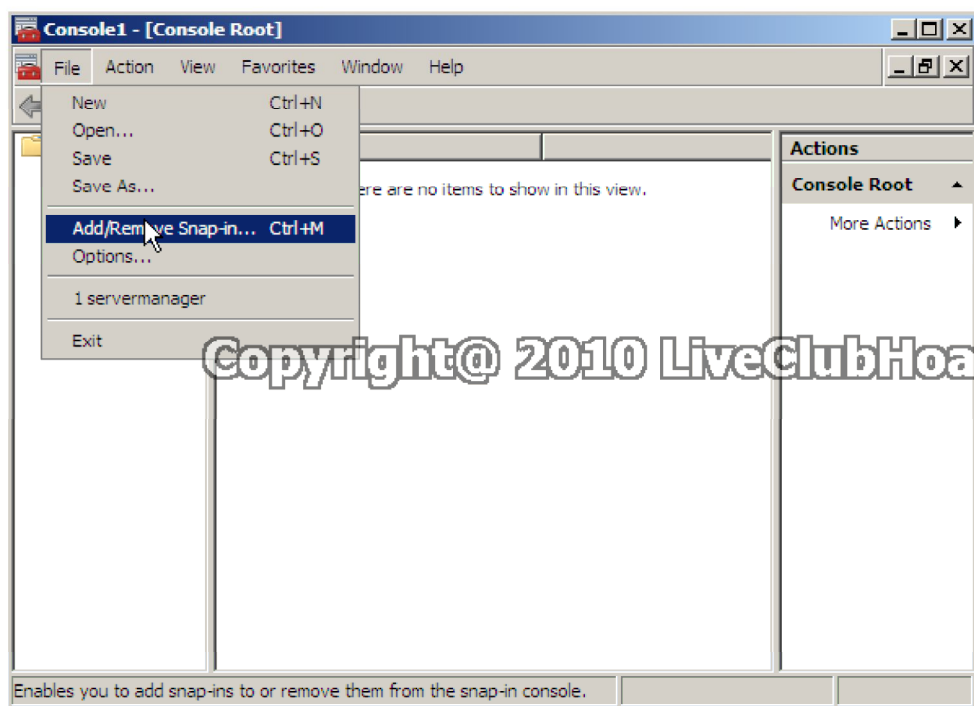


- Nhấn **Start**, trong **Administrative Tools**, chọn **Certification Authority**, để xem CA đã được cài đặt xong.

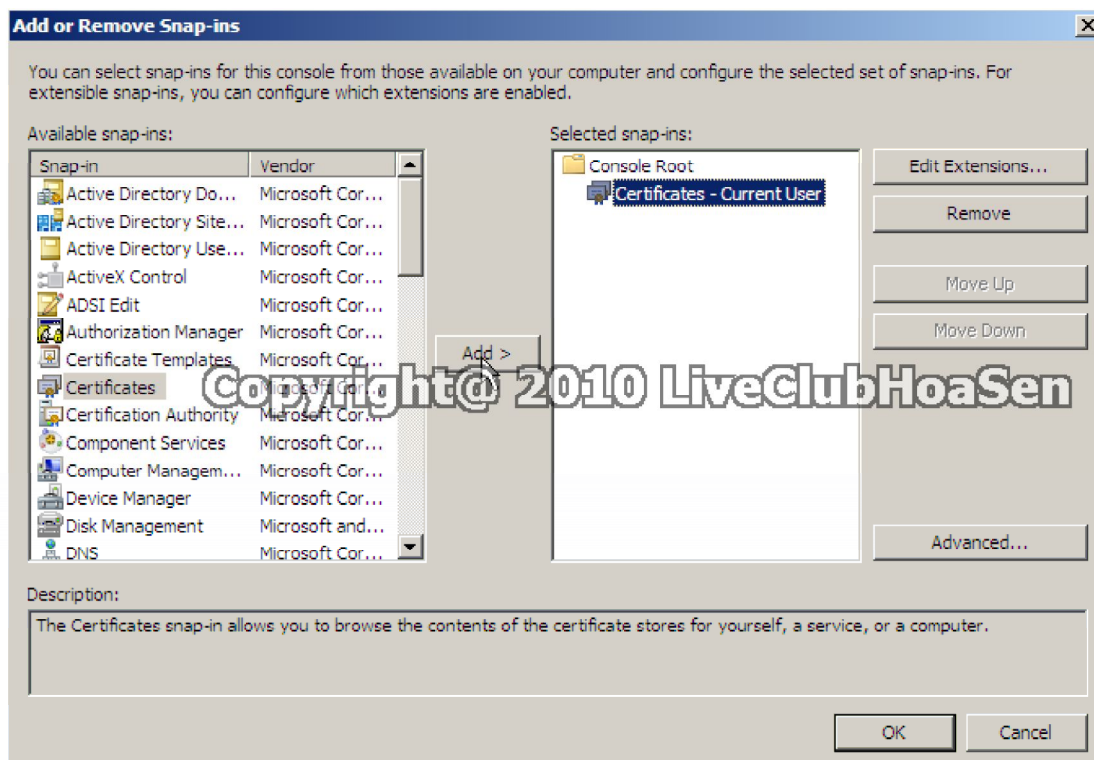


B. Xin Certificate cho User

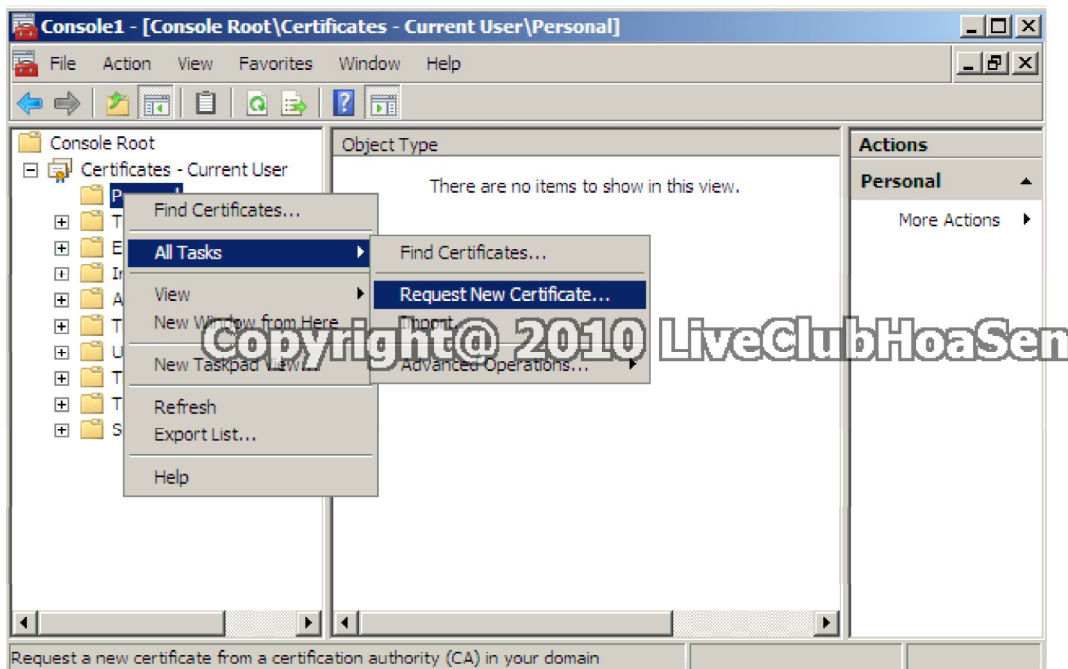
- Login vào user **u1** (**liveclub.local\u1**), vào **Start\Run**, gõ **mmc**, chọn **OK**. Trong cửa sổ **Console1**, mở **File**, chọn **Add/Remove Snap-in**.



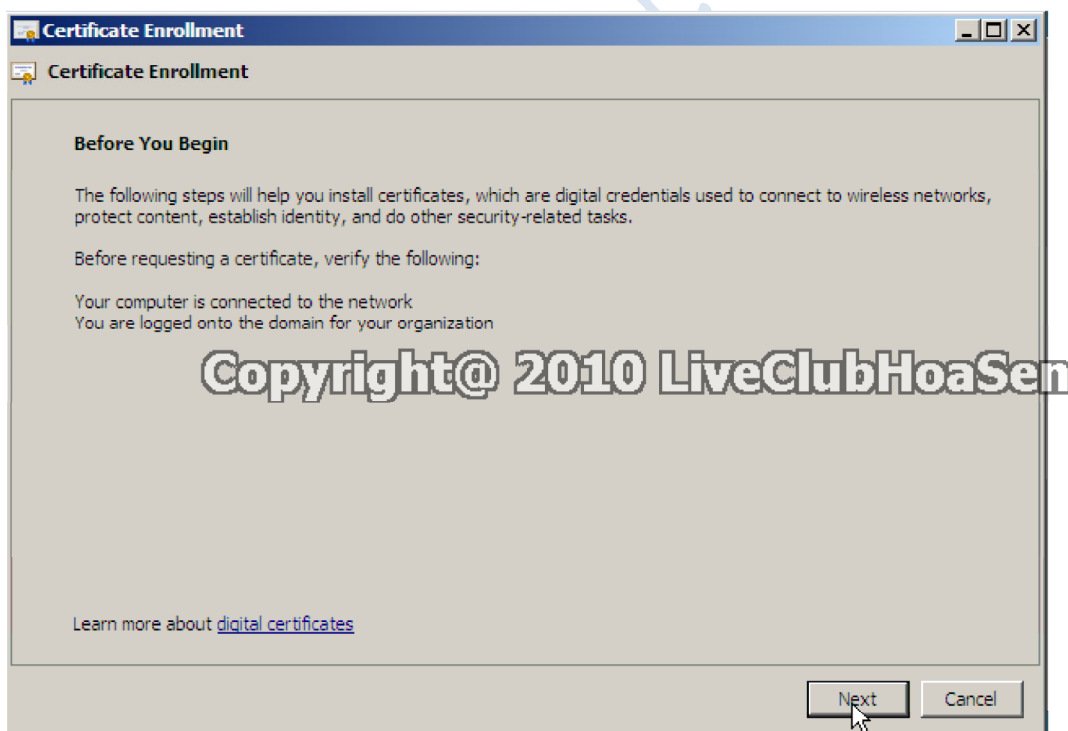
- Trong cửa sổ **Add or Remove Snap-in**, chọn **Certificates**, chọn **Add**, chọn **OK**.



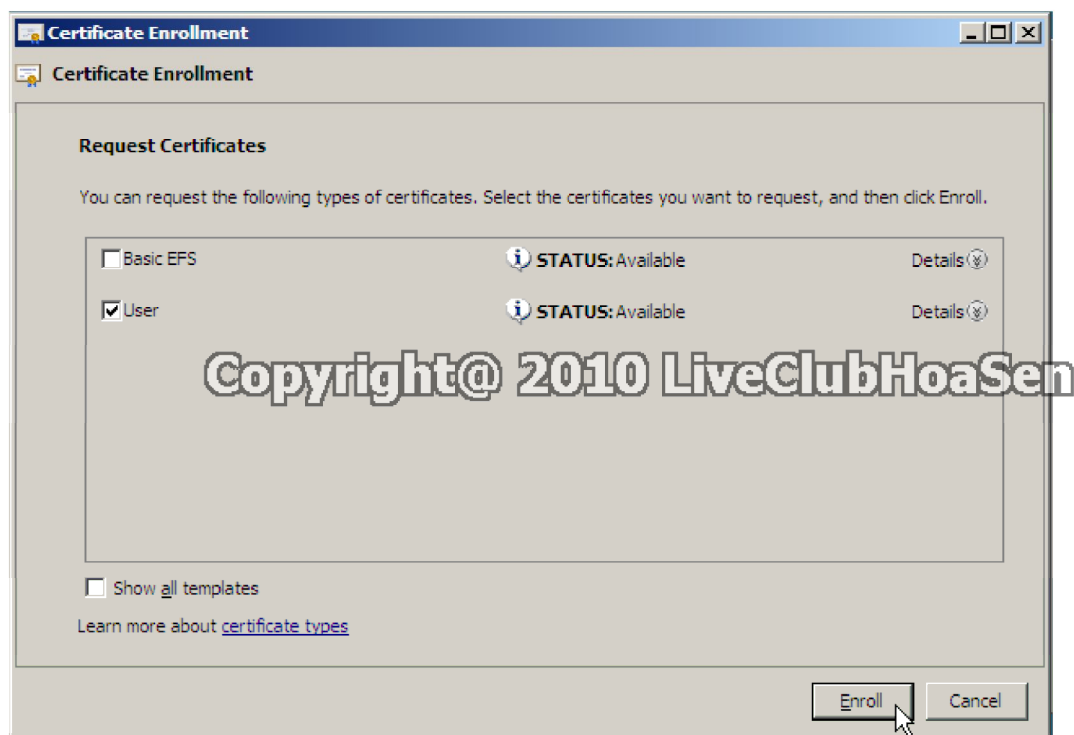
- Trong cửa sổ **Console1**, chuột phải **Personal**, chọn **All tasks**, chọn **Request New Certificate**.



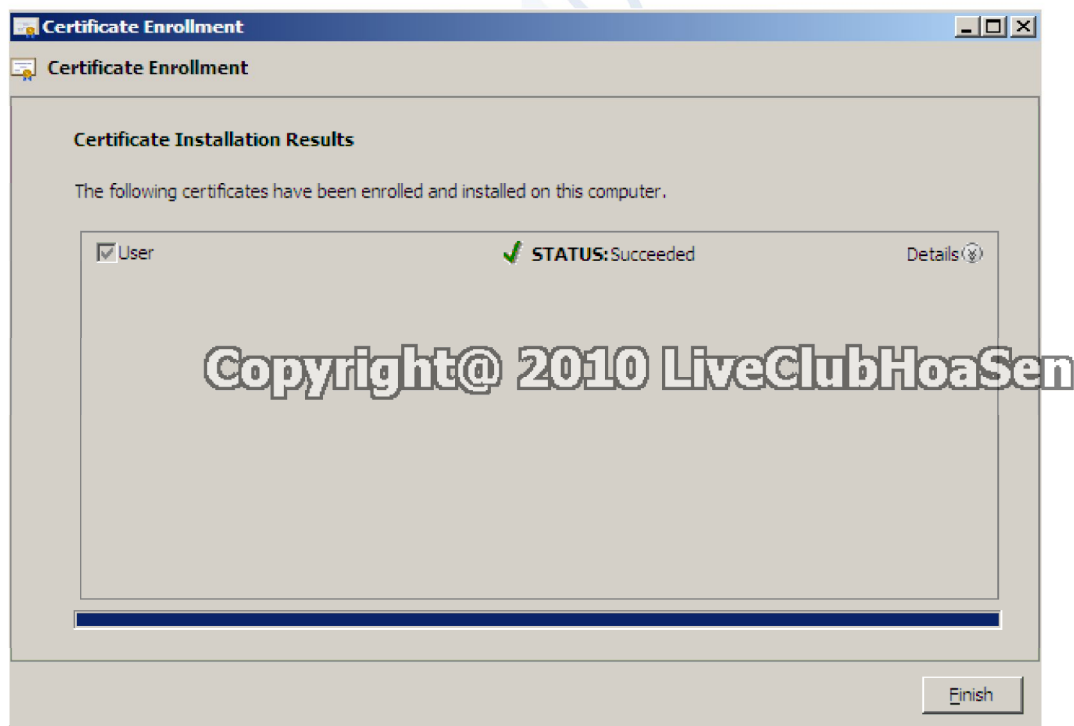
- Trong mục **Before You Begin**, chọn **Next**.



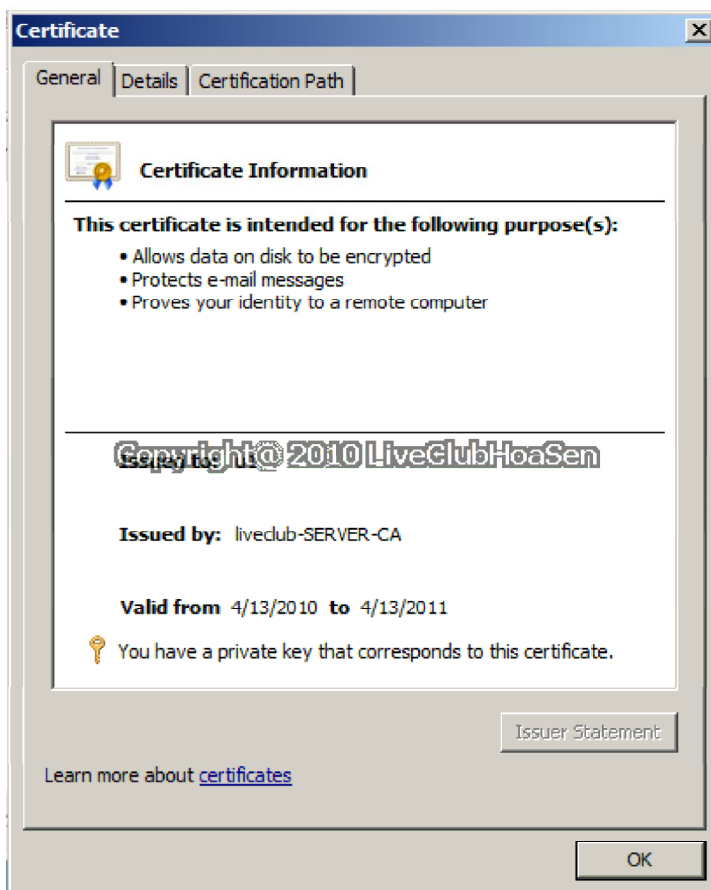
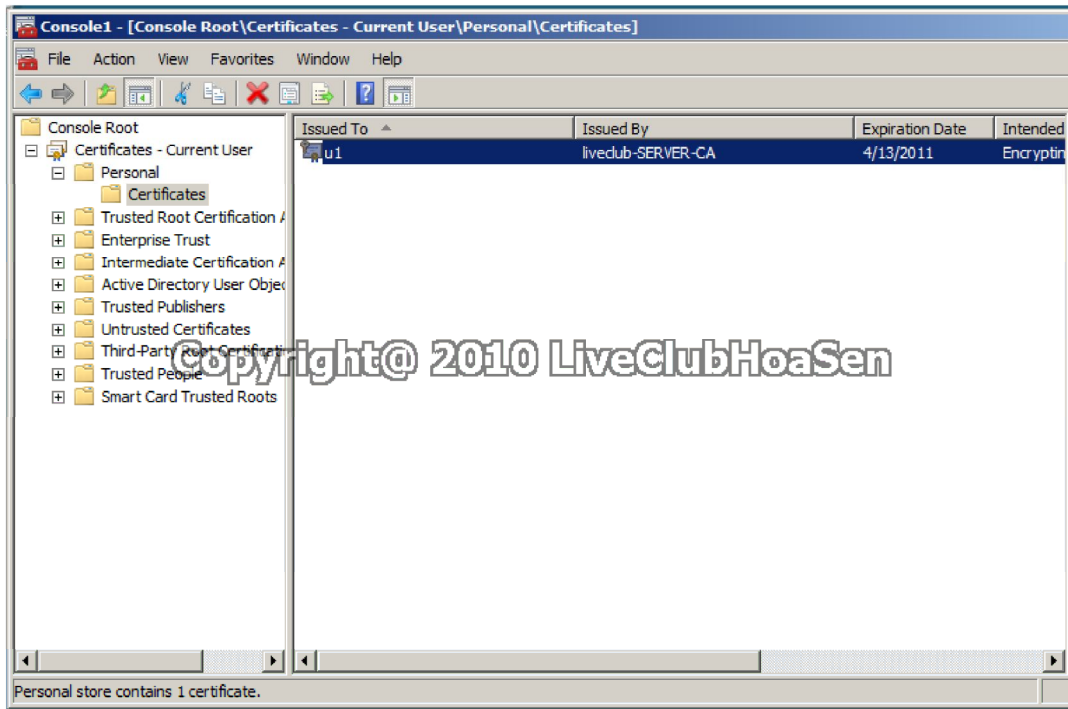
- Trong mục **Request Certificates**, đánh dấu chọn **User**, chọn **Enroll**.



- Trong mục **Certificate Installation Results**, chọn **Finish**.



- Trong cửa sổ **Console1**, mở **Personal**, chọn **certificate** tên **u1**



- Kiểm tra xin certificate cho u1 thành công.