AN NINH MÁY TÍNH

Lab05 – Web Security

Sinh viên:

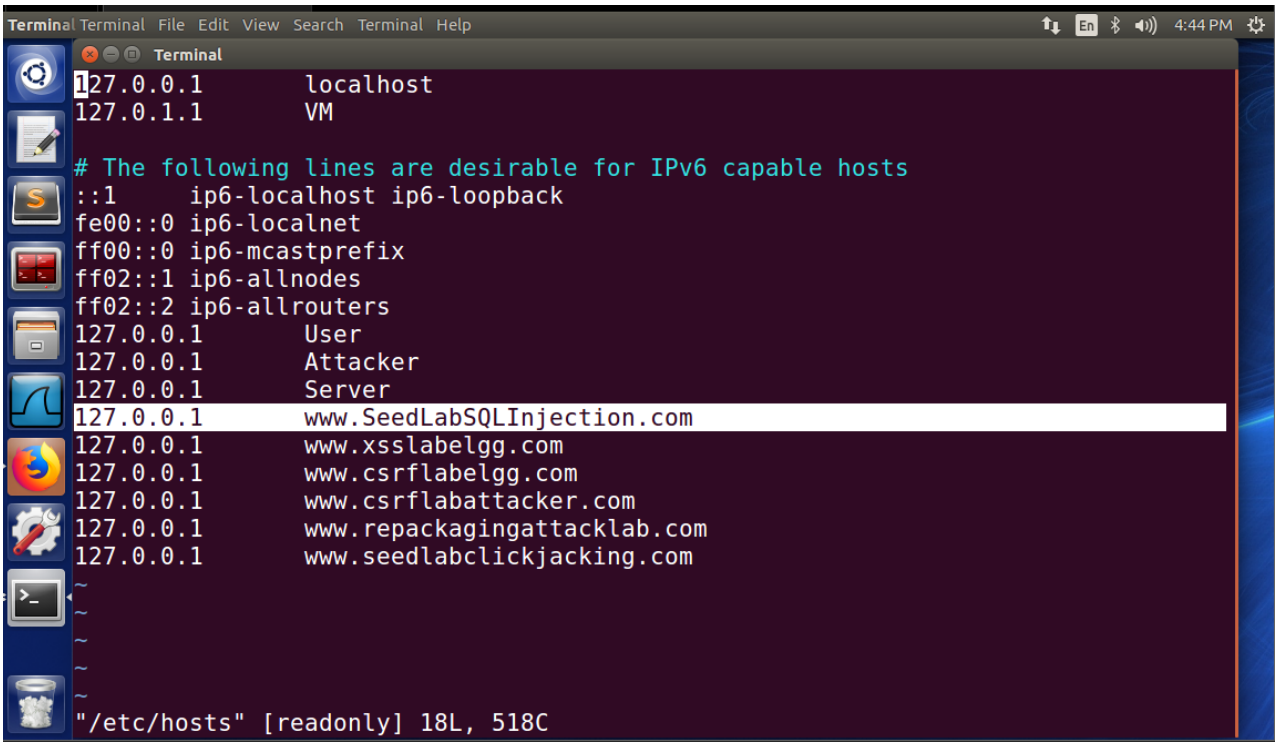
Đỗ Trọng Nghĩa - 18120477

Khoa Công nghệ Thông tin
Đại học Khoa học Tự nhiên TP HCM

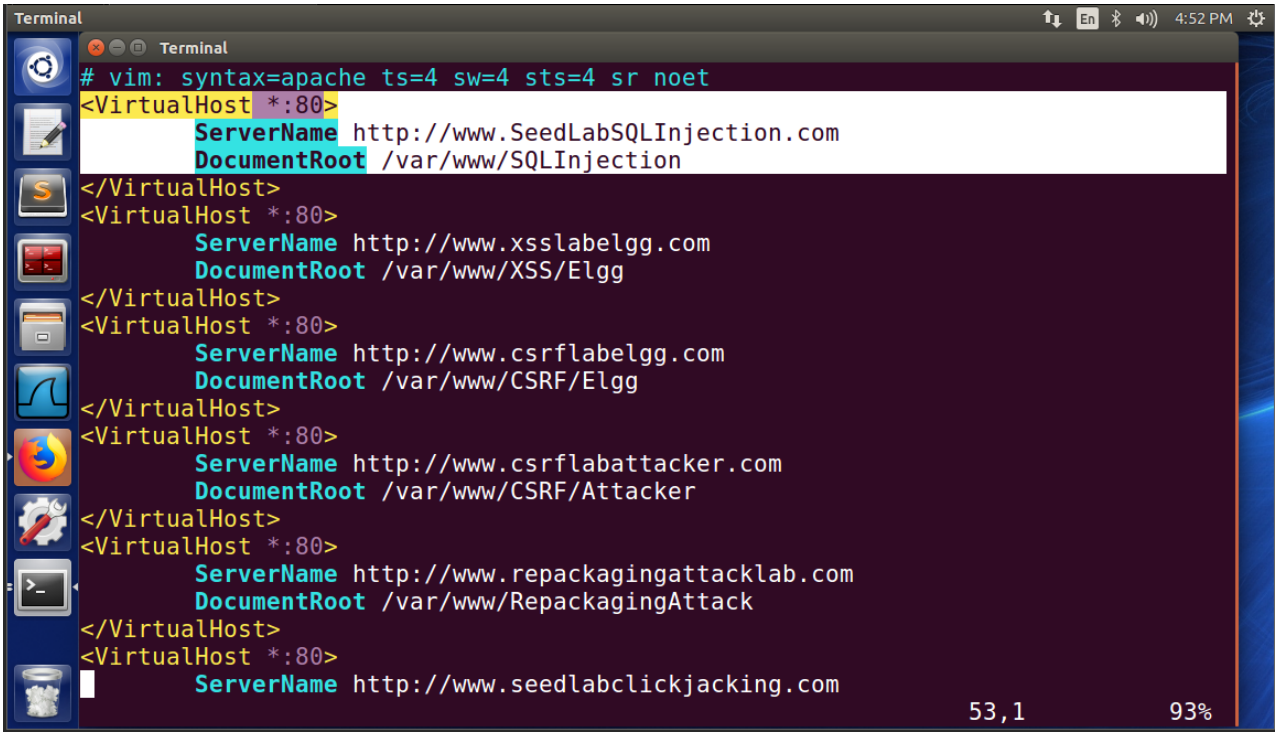
I. SQL Injection

I.1. Tổng quan môi trường

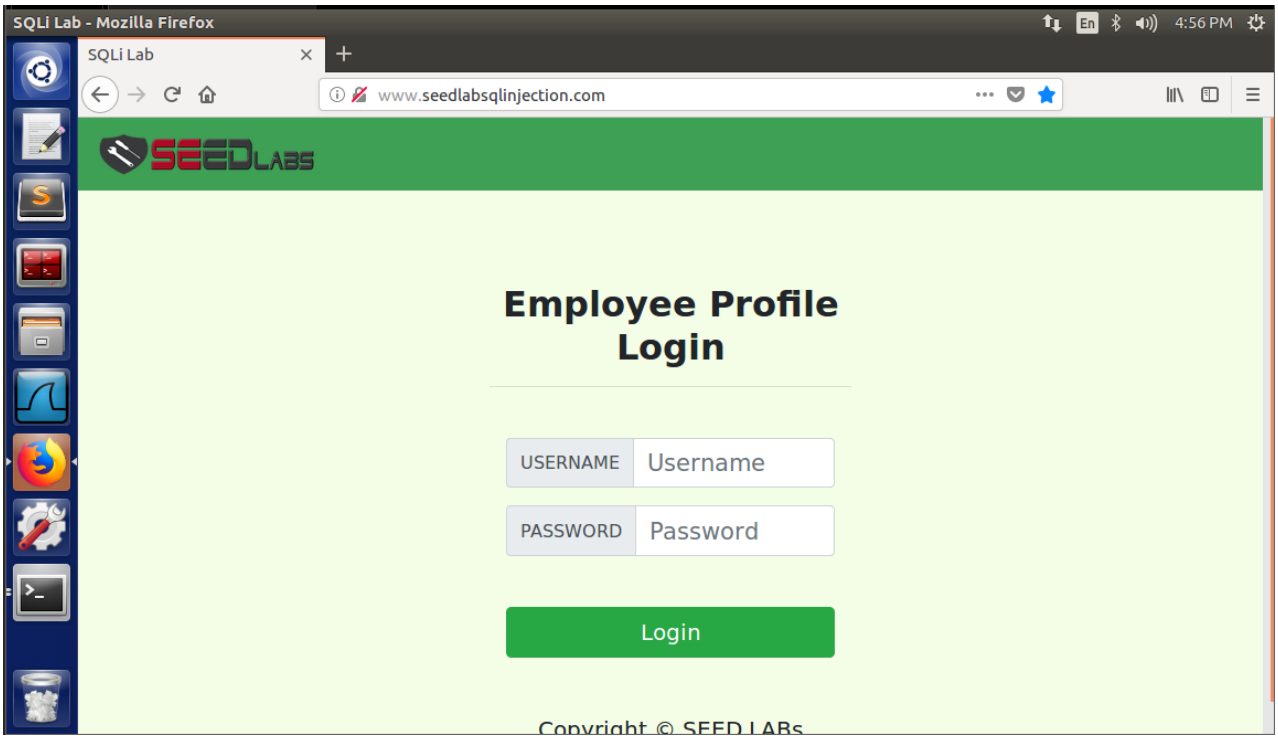
- Sử dụng Pre-built Ubuntu 16.04 VM (được tải từ SEEDLabs)
- Xem thông tin IP máy chủ và tên miền: **#vi /etc/hosts**
- Có thể thấy các địa chỉ trang web đã được cấu hình lại thay cho **localhost**. Trong bài này ta dùng www.SeedLabSQLInjection.com



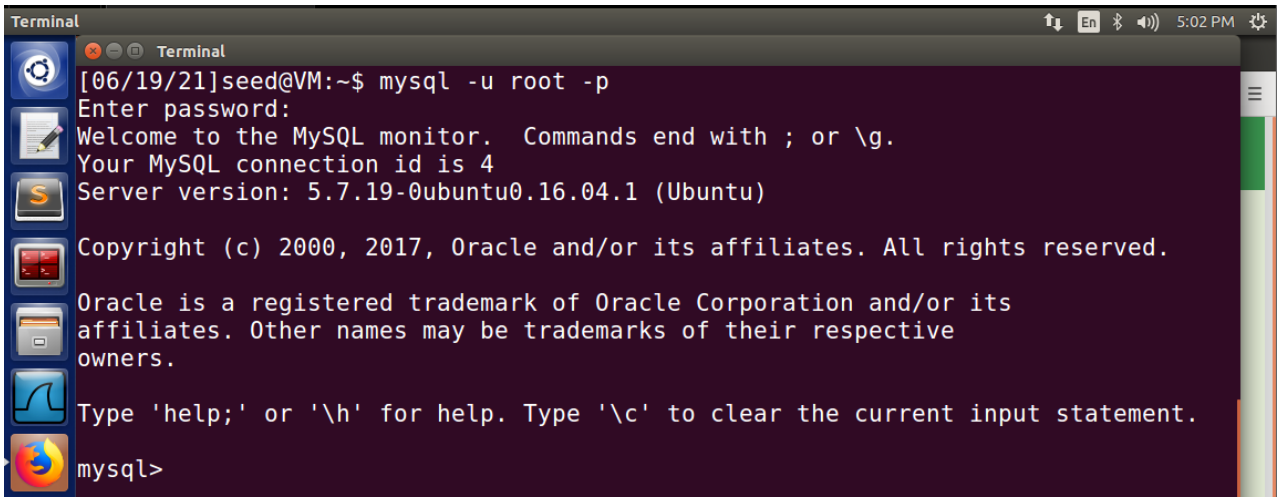
- Xem thông tin của một số địa chỉ duyệt web và physical path: **#vi /etc/apache2/sites-available/000-default.conf**



- Trang web để khai thác lỗ hổng Databse: www.SeedLabSQLInjection.com

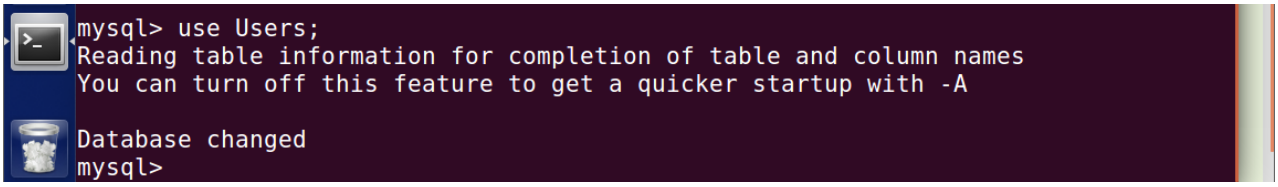


- Xem Database: **mysql -u root -p** với password là **seedubuntu**



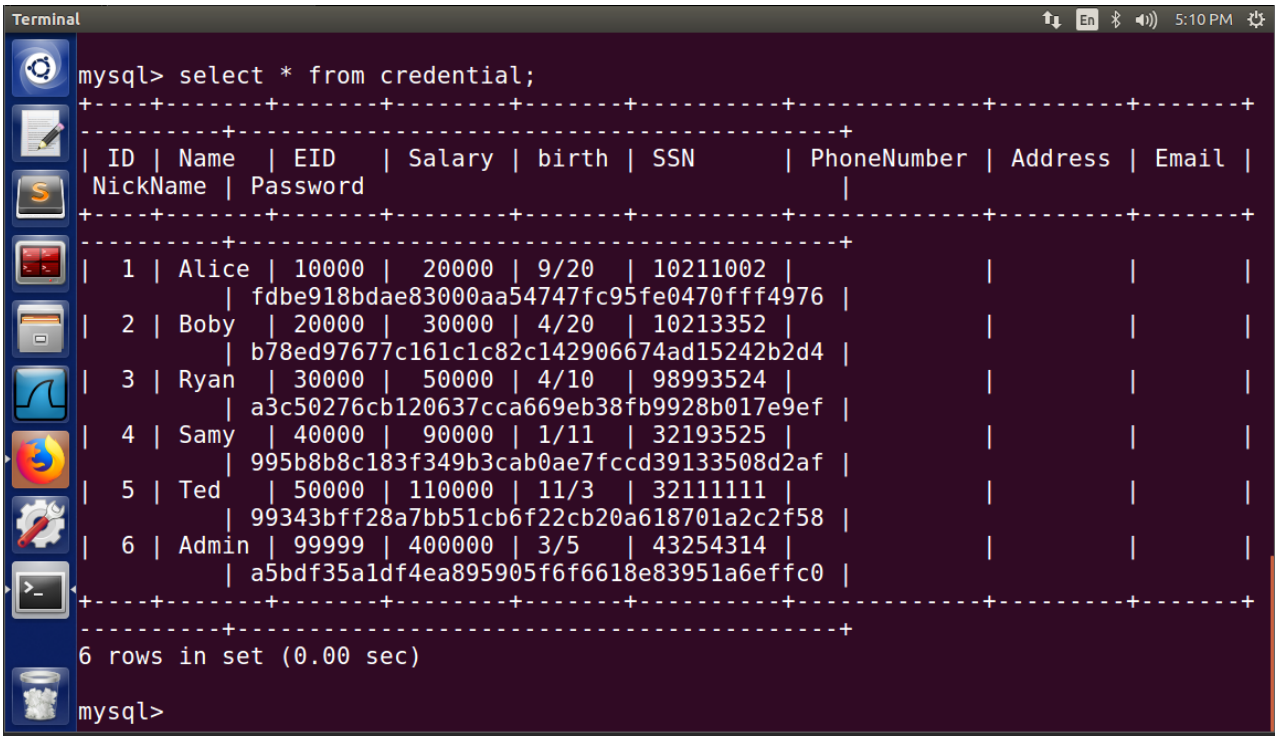
- **show databases;**

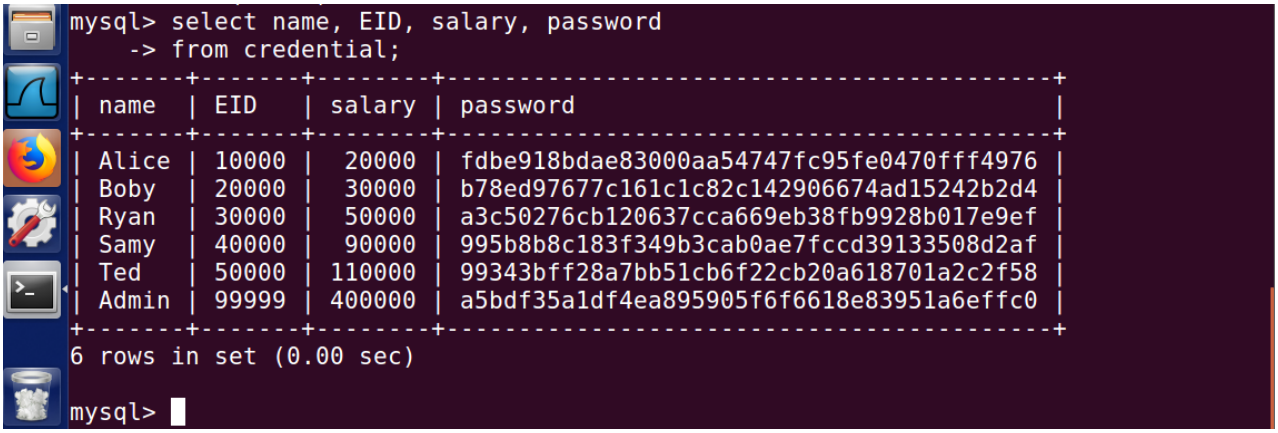
- Dùng Database **Users**: **use Users;**



- Xem các thông tin trong bảng

- Xem thông tin các nhân viên

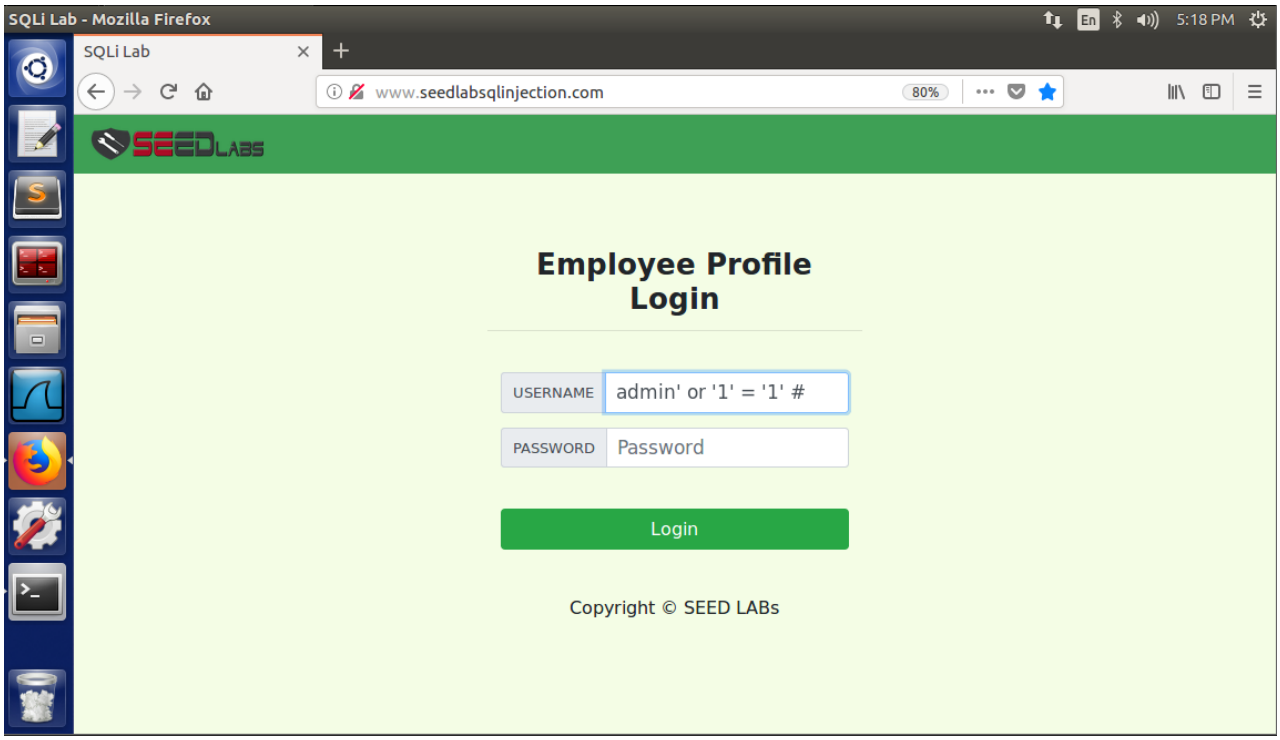




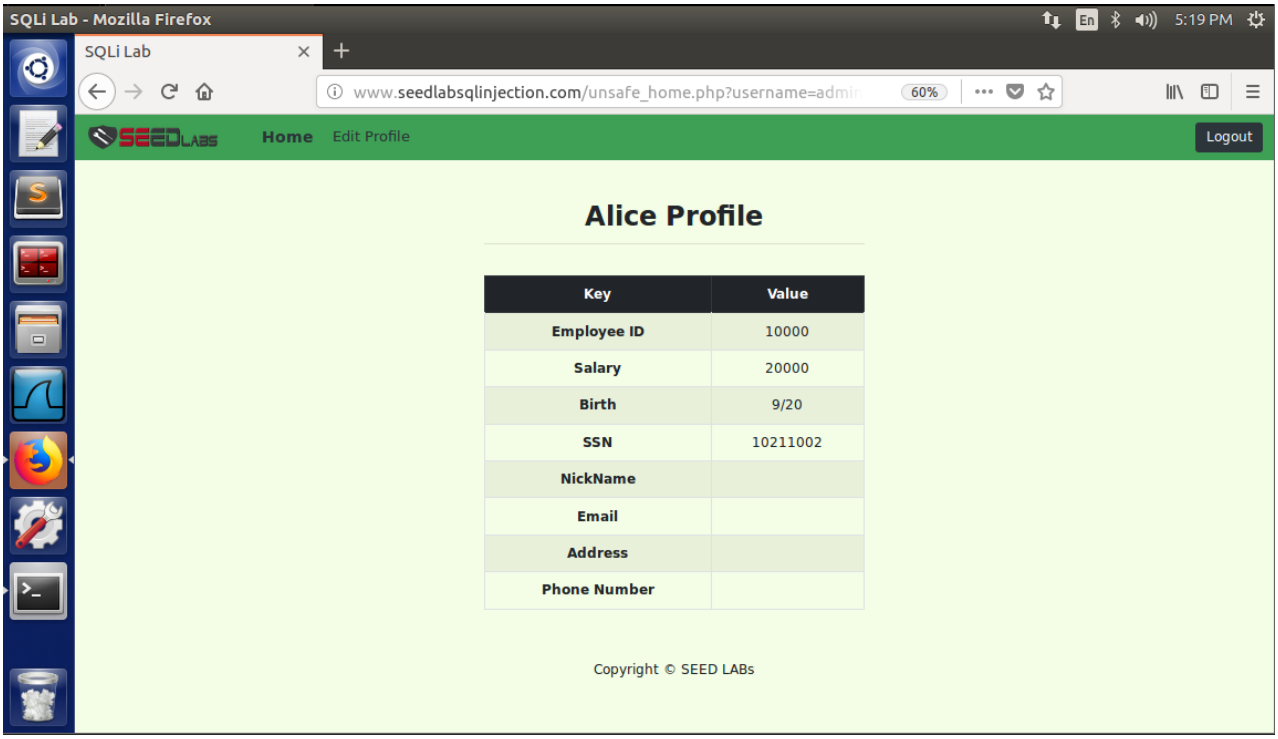
I.2. Khai thác lỗ hổng

I.2.1. Điều chỉnh mức lương Alice

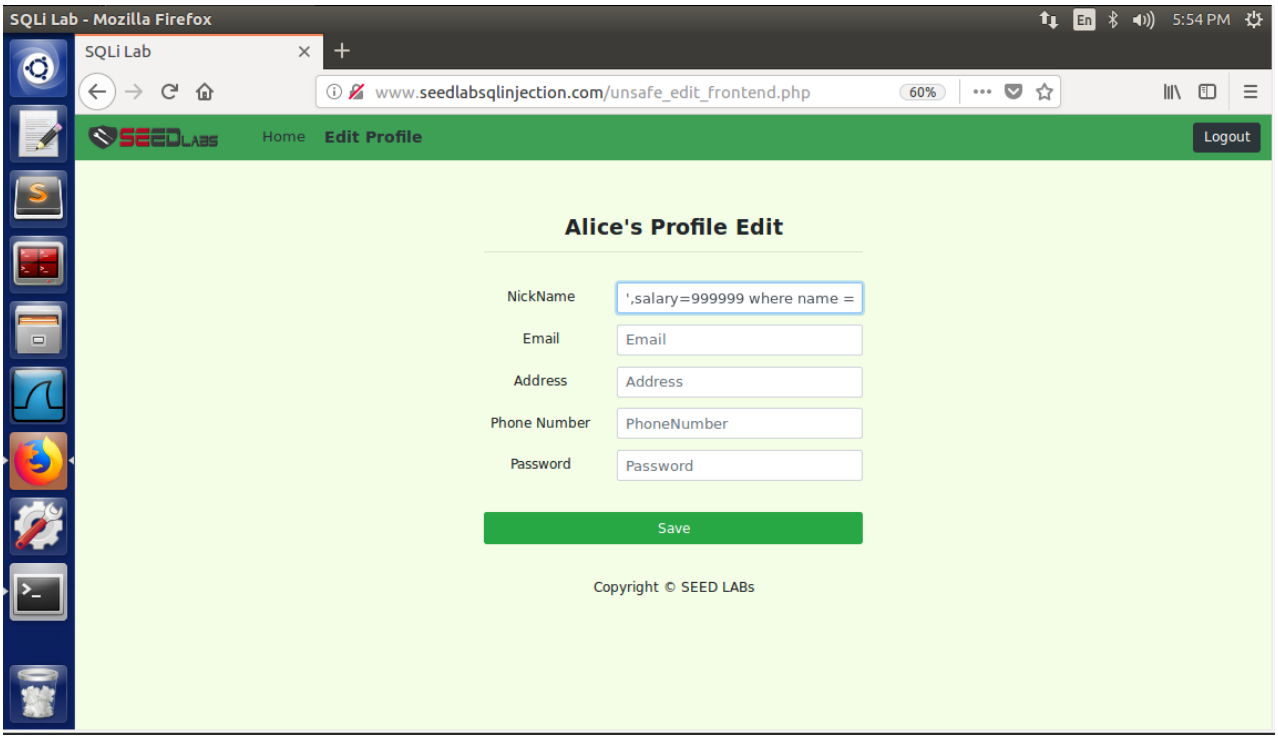
- Bypass đăng nhập vào tài khoản Alice



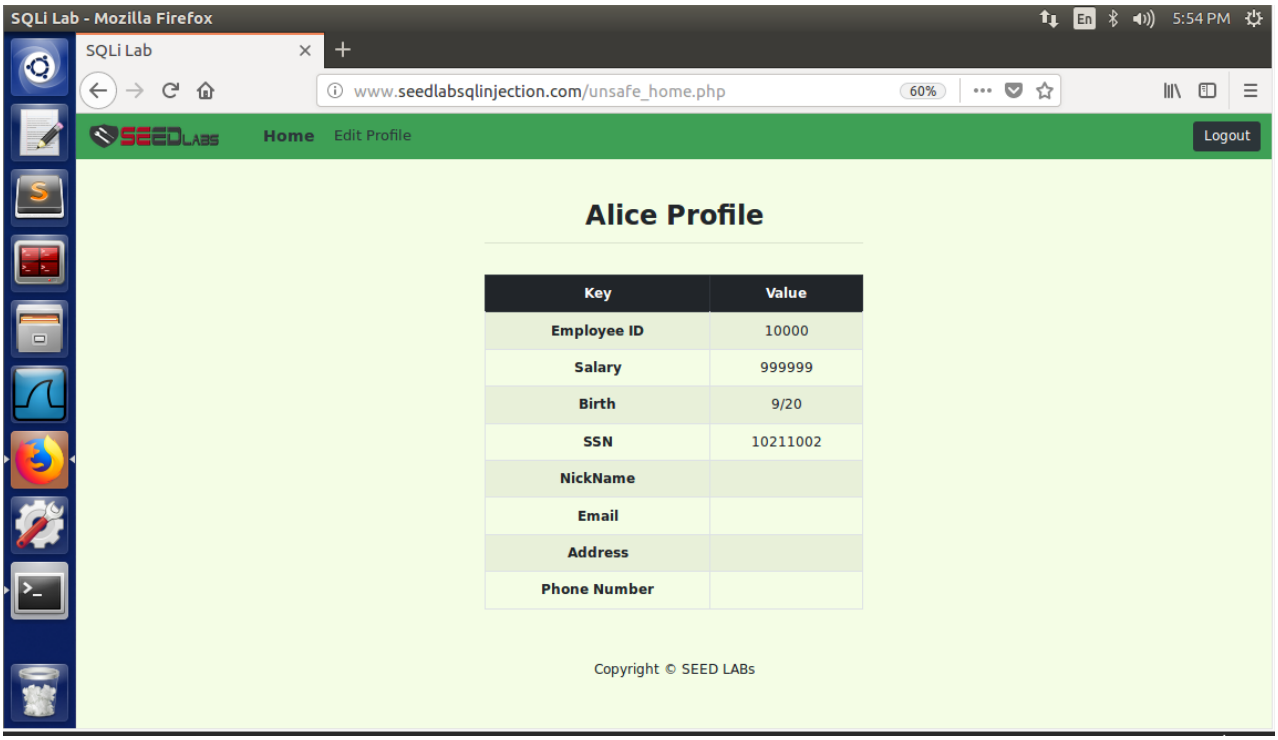
- Đăng nhập thành công



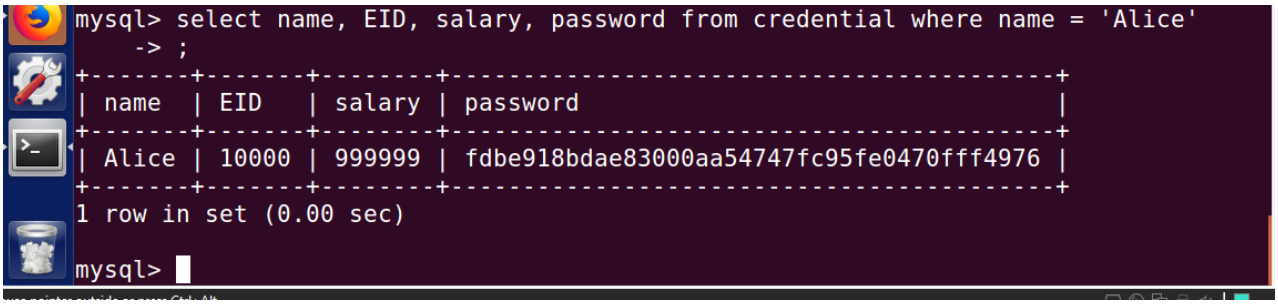
- Chọn **Edit Profile** và để câu truy vấn: ',salary=999999 where name = 'Alice' ; # vào ô **NickName** (sửa lương Alice thành 999999) và lưu lại



- Sửa thành công



- Kiểm tra ở Database

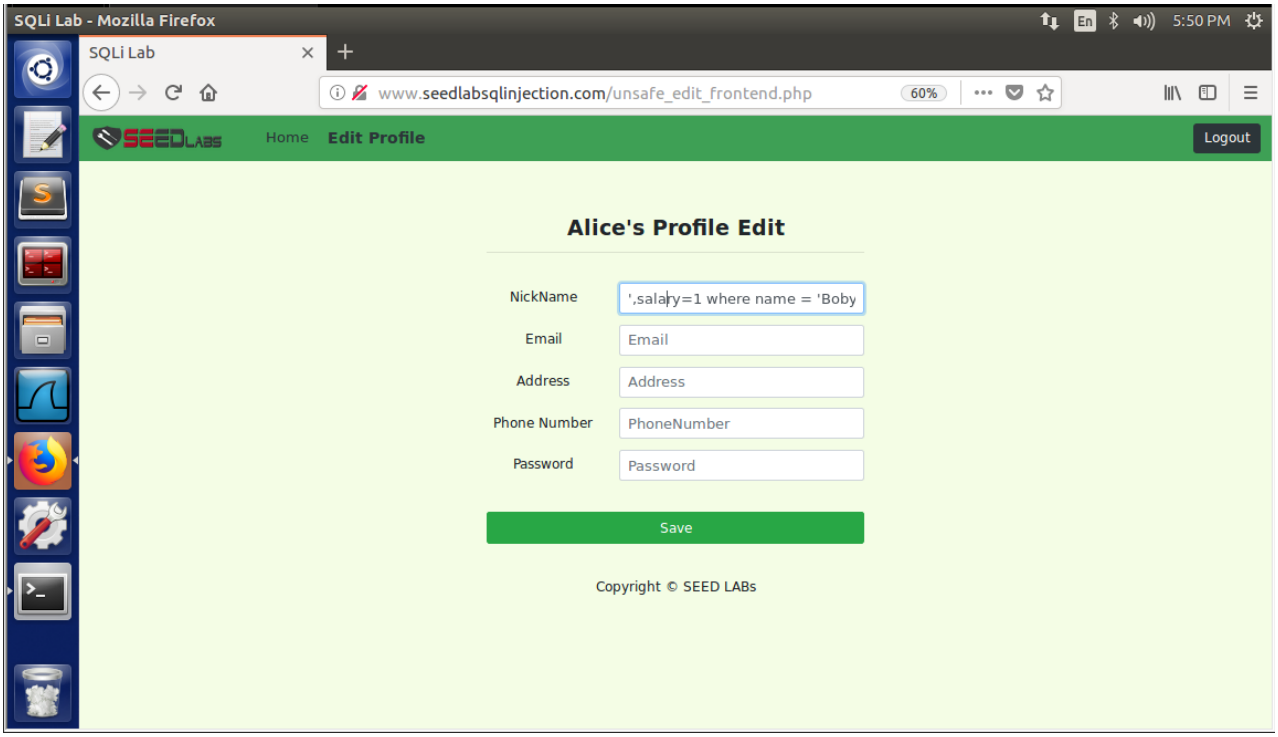


I.2.2. Sửa lương của nhân viên Boby

- Chọn sửa lương của Boby thành 1. Kiểm tra trước ở Database

```
mysql> select name, EID, salary, password from credential where name = 'Boby';
+------+-------+--------+------------------------------------------+
| name | EID   | salary | password                                 |
+------+-------+--------+------------------------------------------+
| Boby | 20000 |  30000 | b78ed97677c161c1c82c142906674ad15242b2d4 |
+------+-------+--------+------------------------------------------+
1 row in set (0.00 sec)
```

- Sử dụng lại trang **Edit Profile** của Alice đã bypass đăng nhập được và để câu truy vấn : ',salary=1 where name = 'Boby' ; # (sửa lương của Boby thành 1) và lưu lại

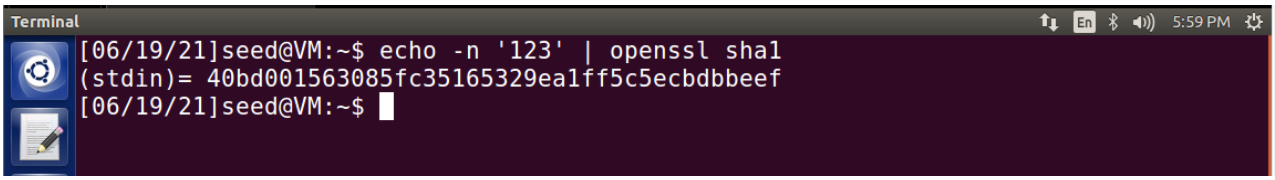


- Kiểm tra ở Database thấy lương của Boby đã được sửa

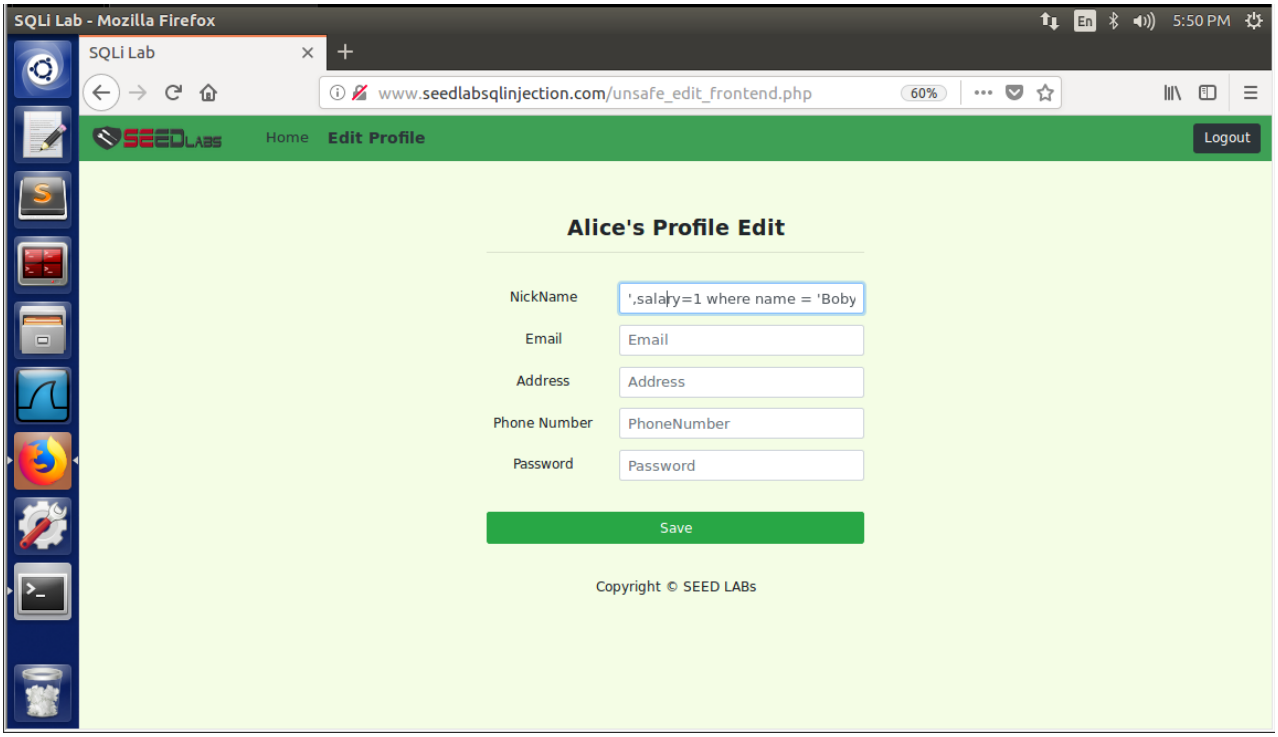
```
mysql> select name, EID, salary, password from credential where name = 'Boby';
+------+-------+--------+------------------------------------------+
| name | EID   | salary | password                                 |
+------+-------+--------+------------------------------------------+
| Boby | 20000 |      1 | b78ed97677c161c1c82c142906674ad15242b2d4 |
+------+-------+--------+------------------------------------------+
1 row in set (0.00 sec)

mysql>
```

I.2.3. Thay đổi mật khẩu của Boby

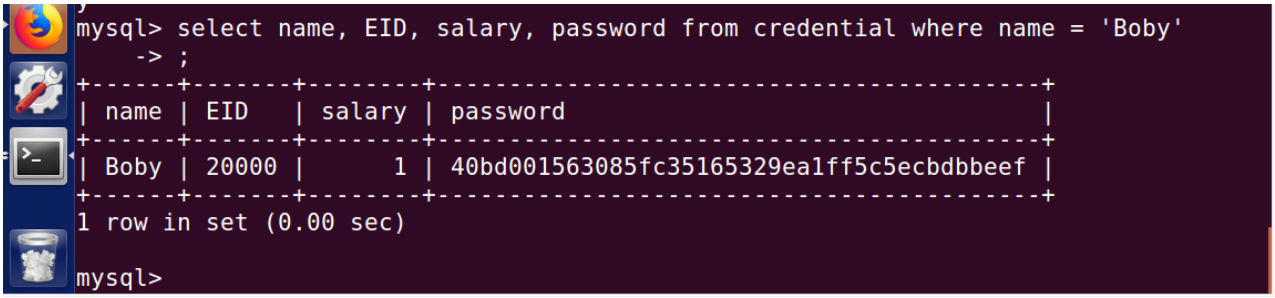
- Tạo hàm băm SHA1 từ chuỗi ‘123’



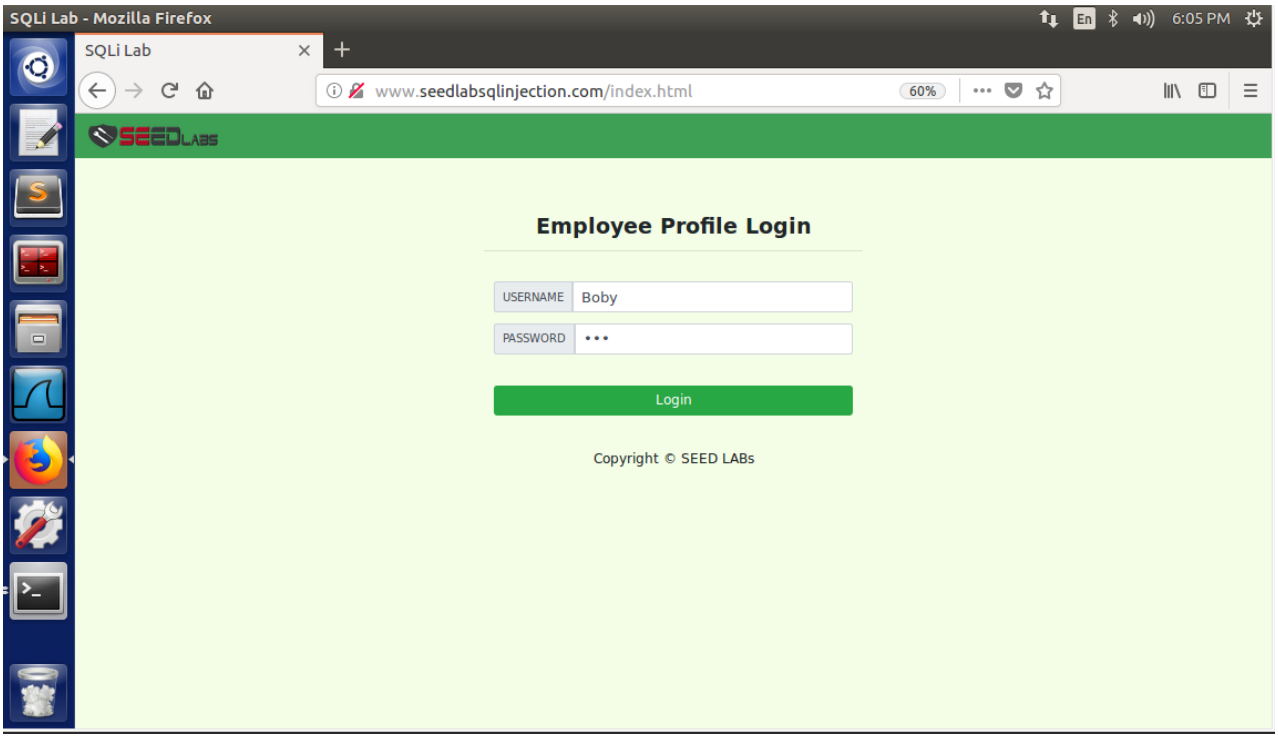
- Kiểm tra mật khẩu dưới dạng SHA1 của Boby (khác so với lúc ta băm ‘123’
- Sử dụng lại trang **Edit Profile** của Alice đã bypass đăng nhập được và để câu truy vấn : ',password='40bd001563085fc35165329ea1ff5c5ecbdbbeef' where name = 'Boby'; # (sửa lương của Boby thành ‘123’) và lưu lại



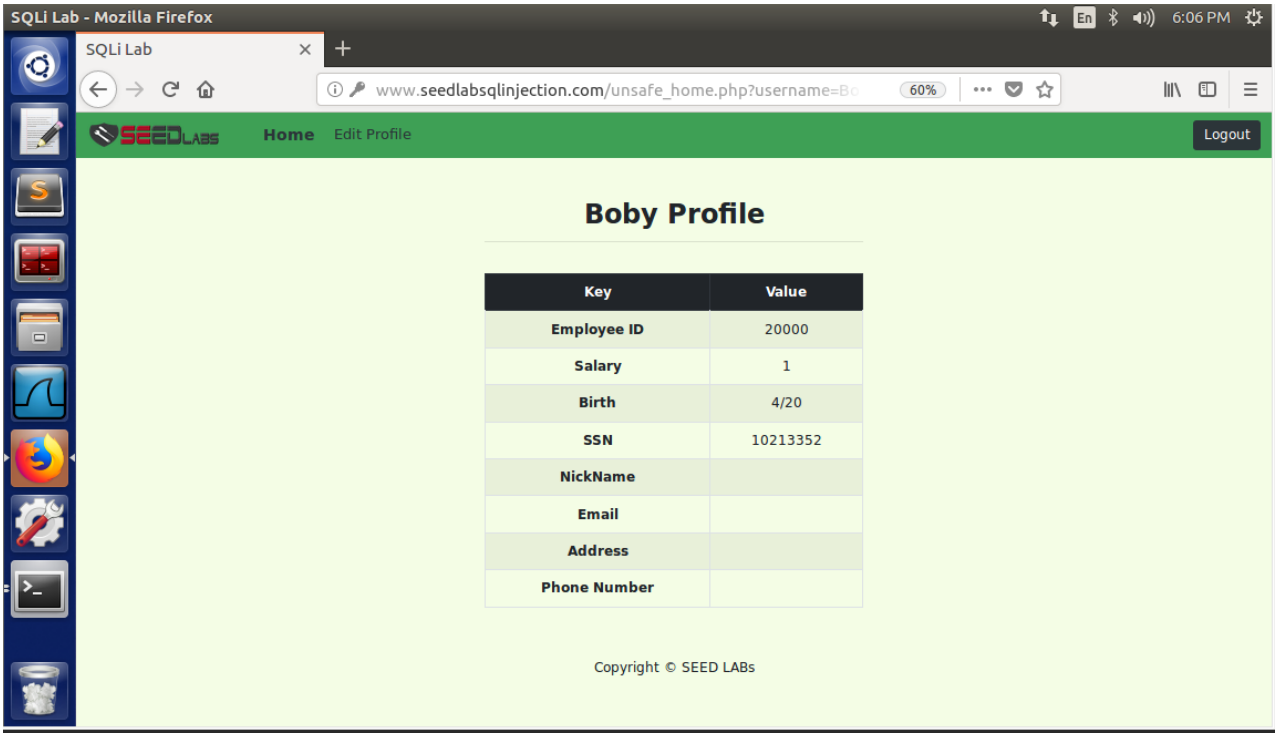
- Kiểm tra dưới Database thì thấy mật khẩu đã đổi theo chuỗi băm mà ta mong muốn



- Tiến hành đăng nhập tài khoản của Boby với mật khẩu là ‘123’

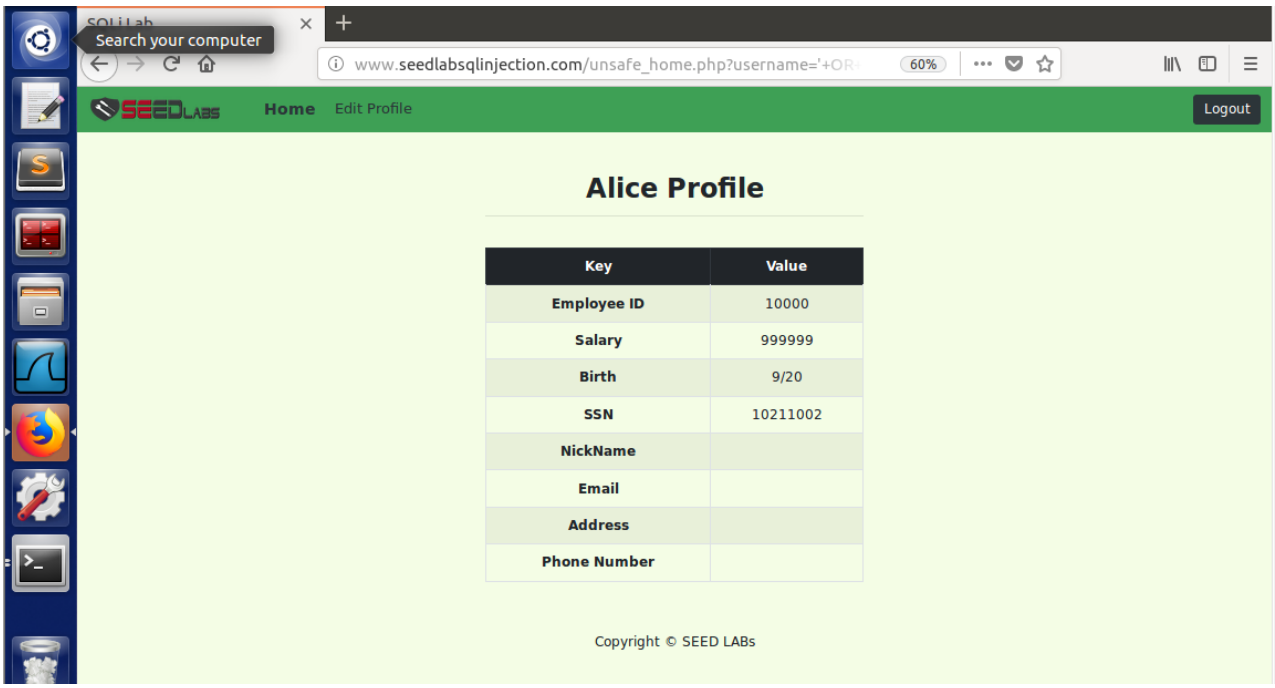


- Đăng nhập thành công

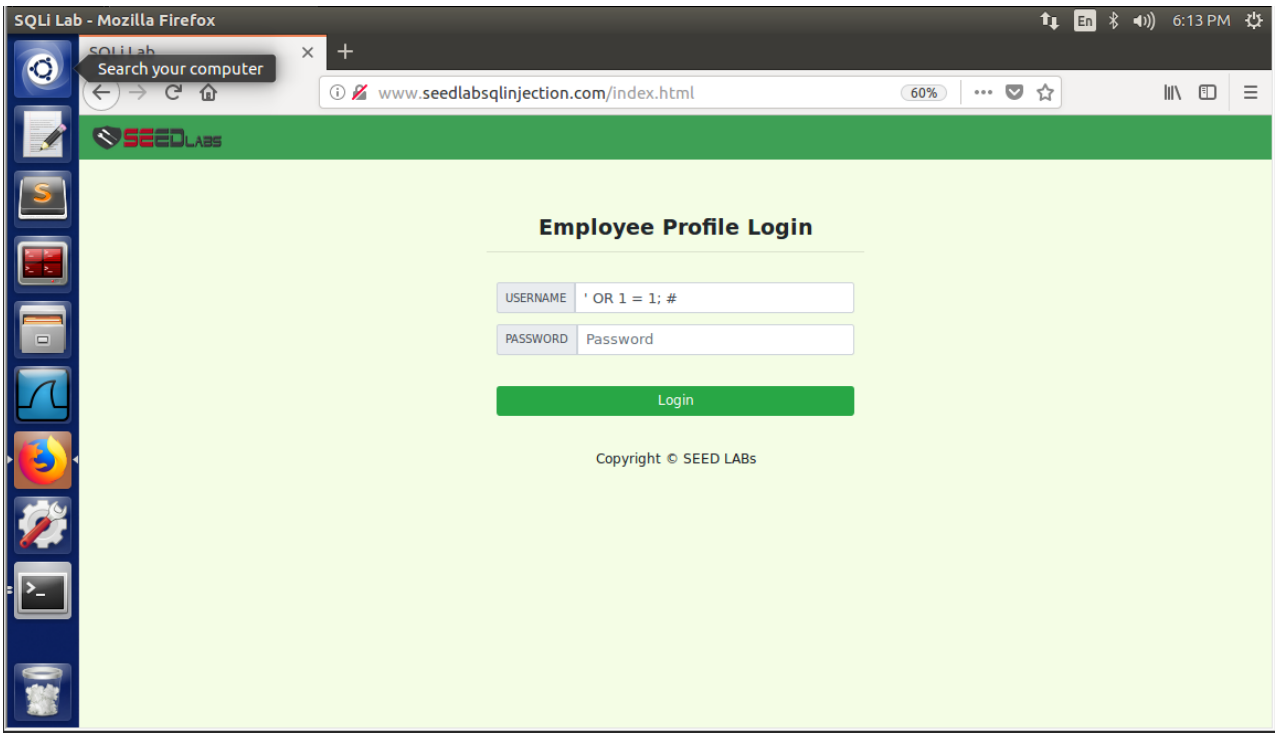


I.2.4. Lấy dữ liệu nhân viên đầu tiên (Alice)

- Nhập ' OR 1 = 1; # trong màn hình đăng nhập

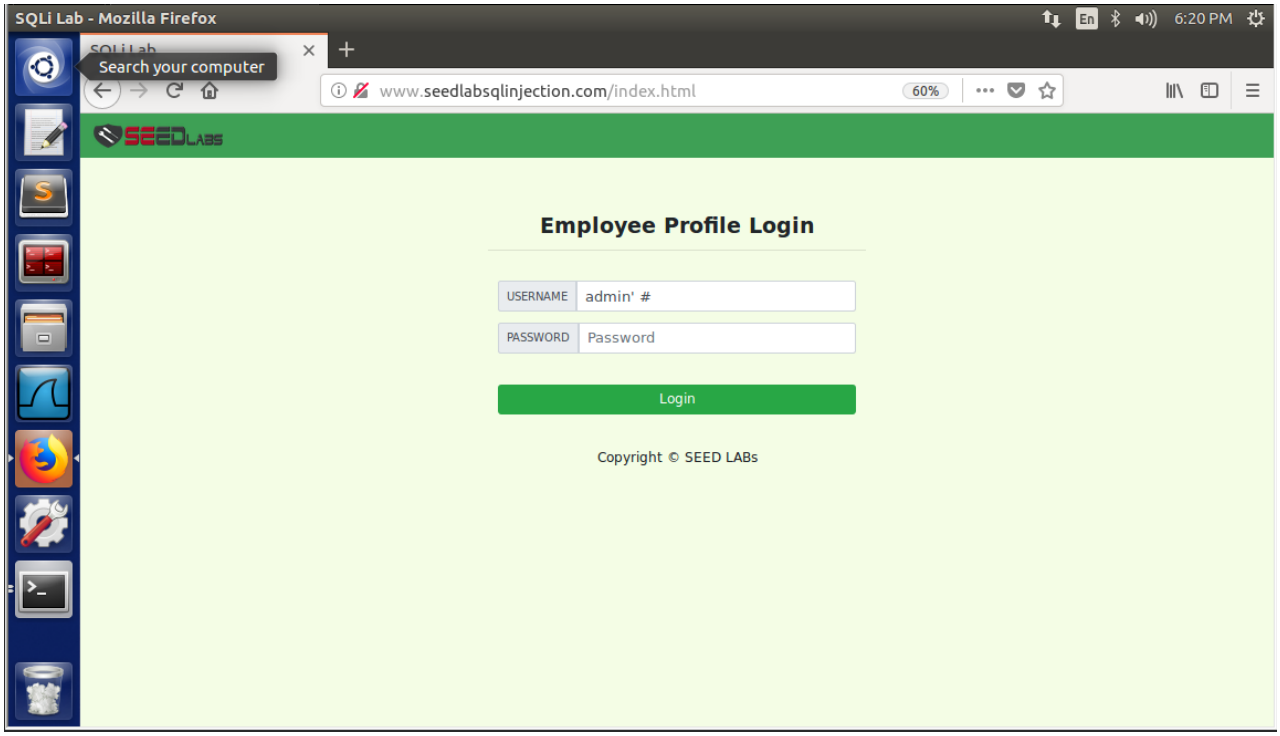


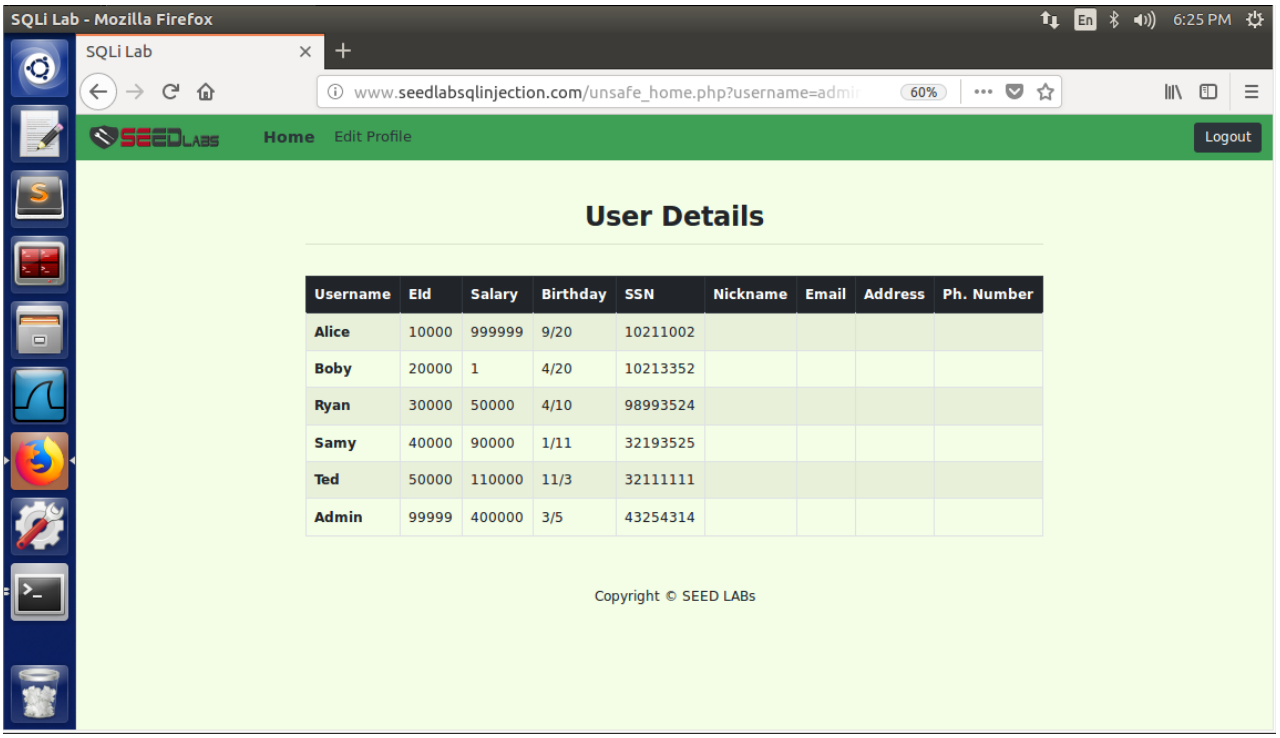
- Câu lệnh này thực chất là thấy được tất cả các nhân viên nhưng do được thiết kế chỉ xem được một người và Alice là người đầu tiên



I.2.5. Xem tất cả thông tin các người dùng

- Nhập admin' # khi đăng nhập (đây là câu lệnh xem thông tin của admin, trường hợp này cho ra tất cả các thông tin các tài khoản)





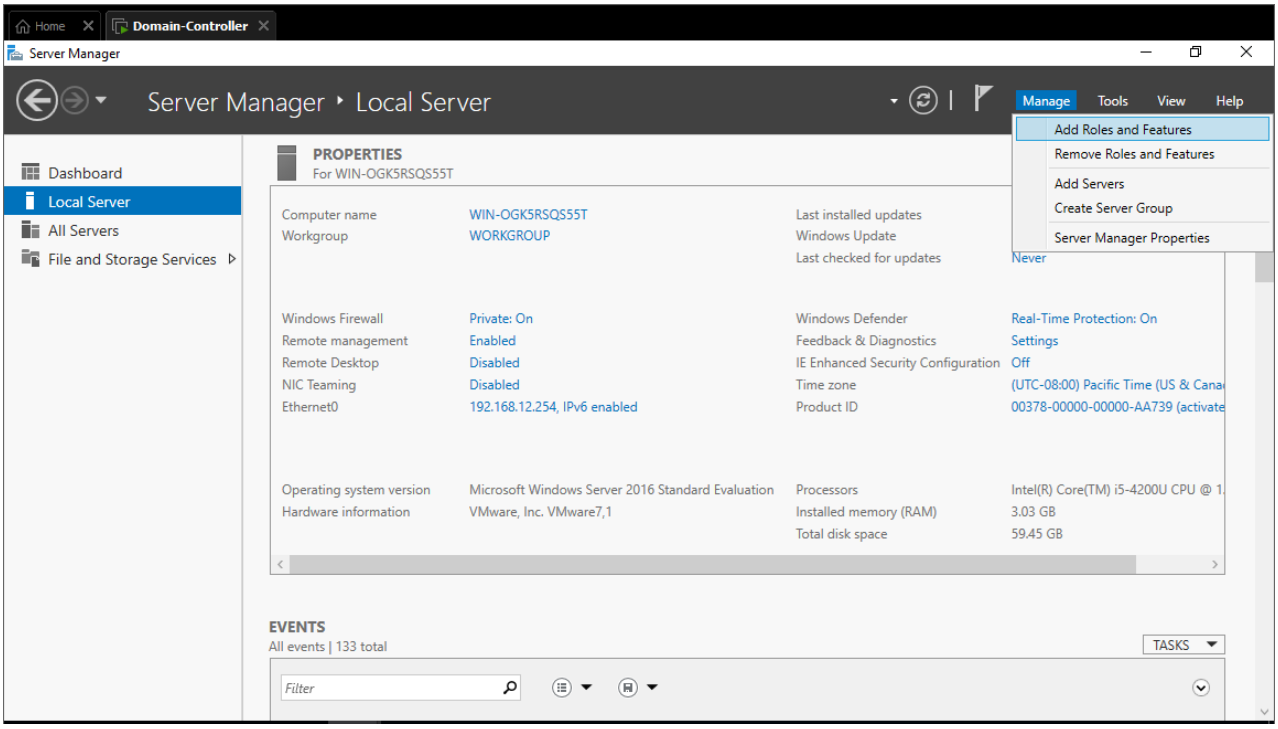
II. HTTPS

Máy Domain – Controller cấp Certificate cho máy chủ Web – Server nên cũng đóng vai trò như một CA Server

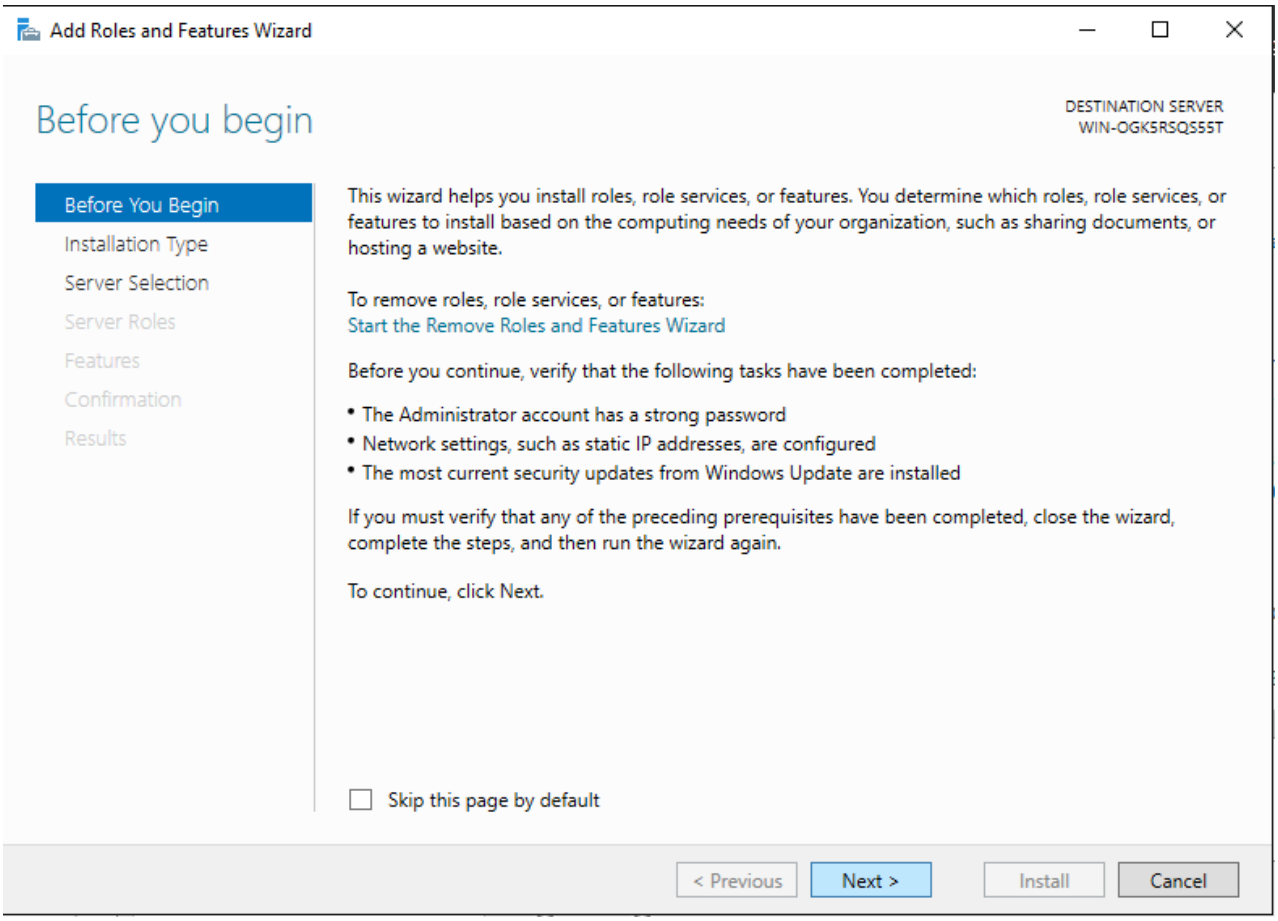
II.1. Cài đặt các dịch vụ

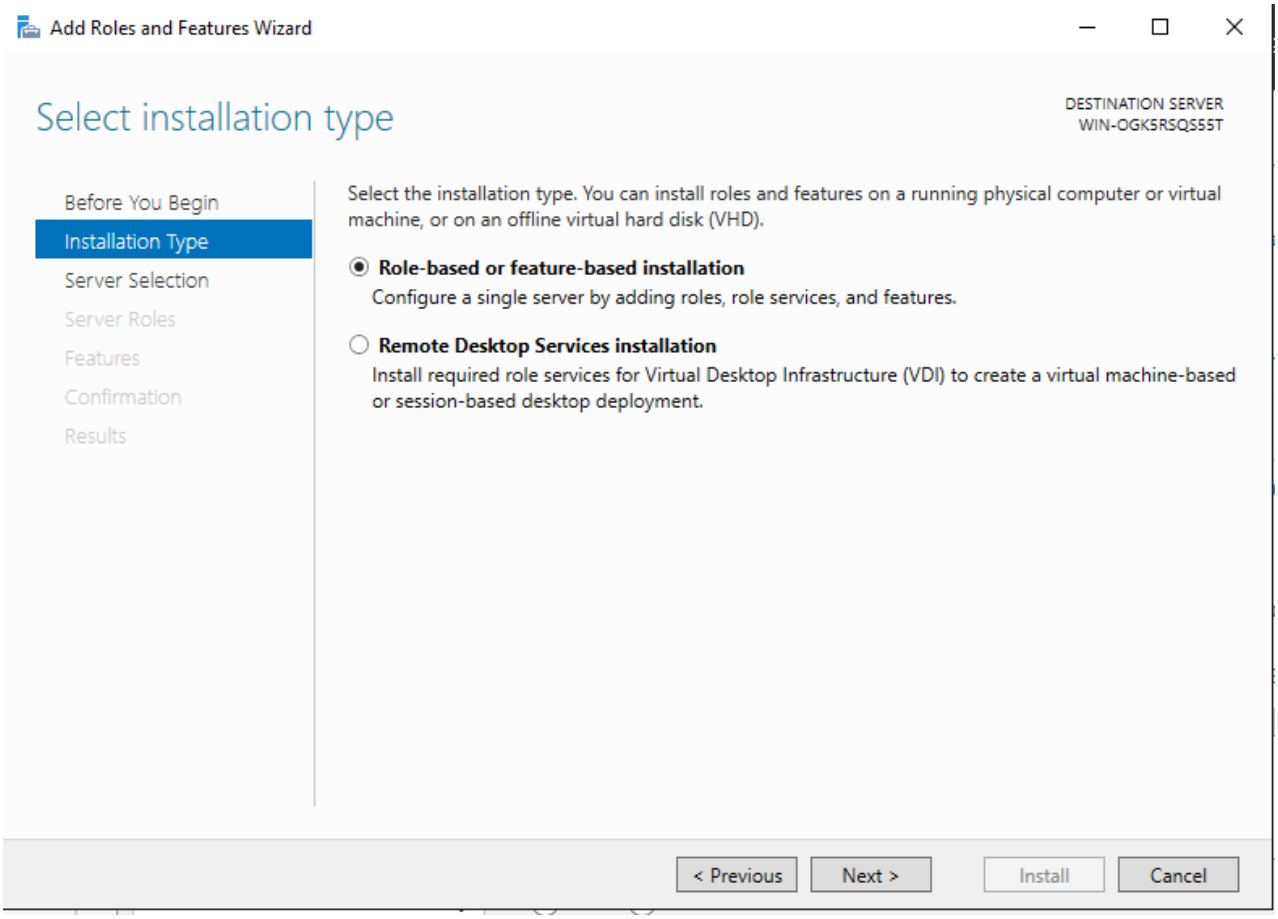
II.1.1. Domain – Controller (CA Server)

- Thực hiện cài đặt **DNS**, **Active Directory Domain Services**.
- Chọn **Add Roles and Features.**

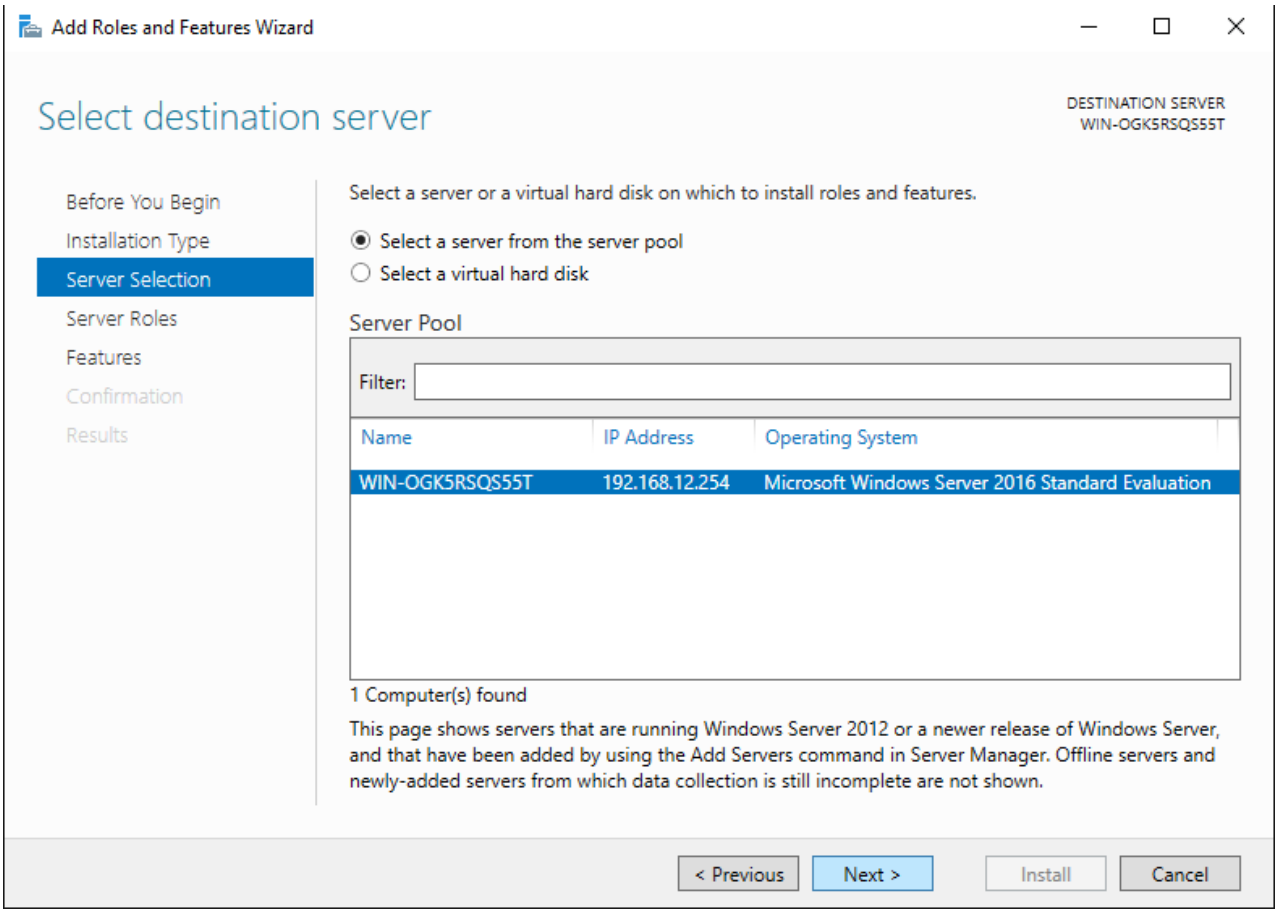


- Các phần tiếp theo, ta chọn next

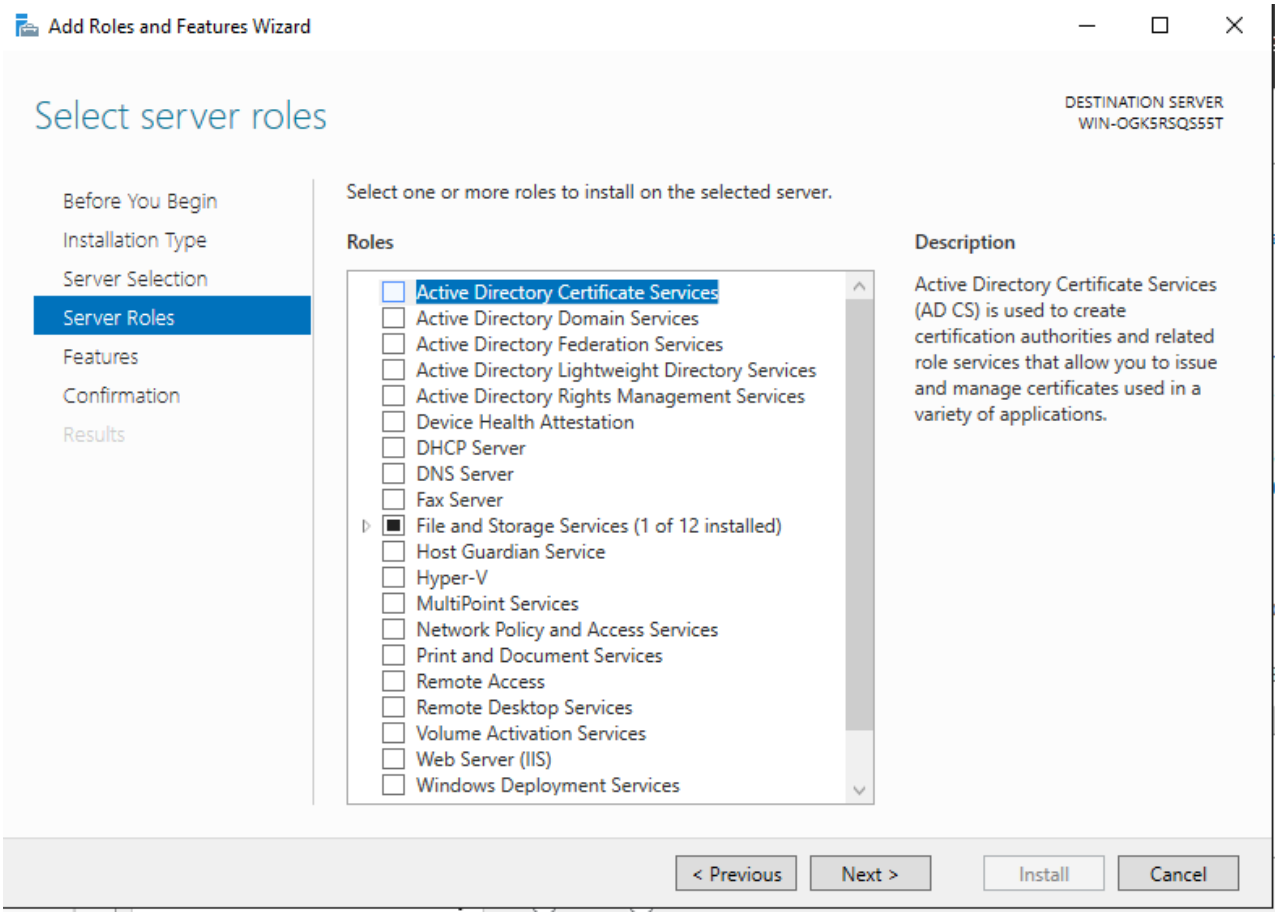


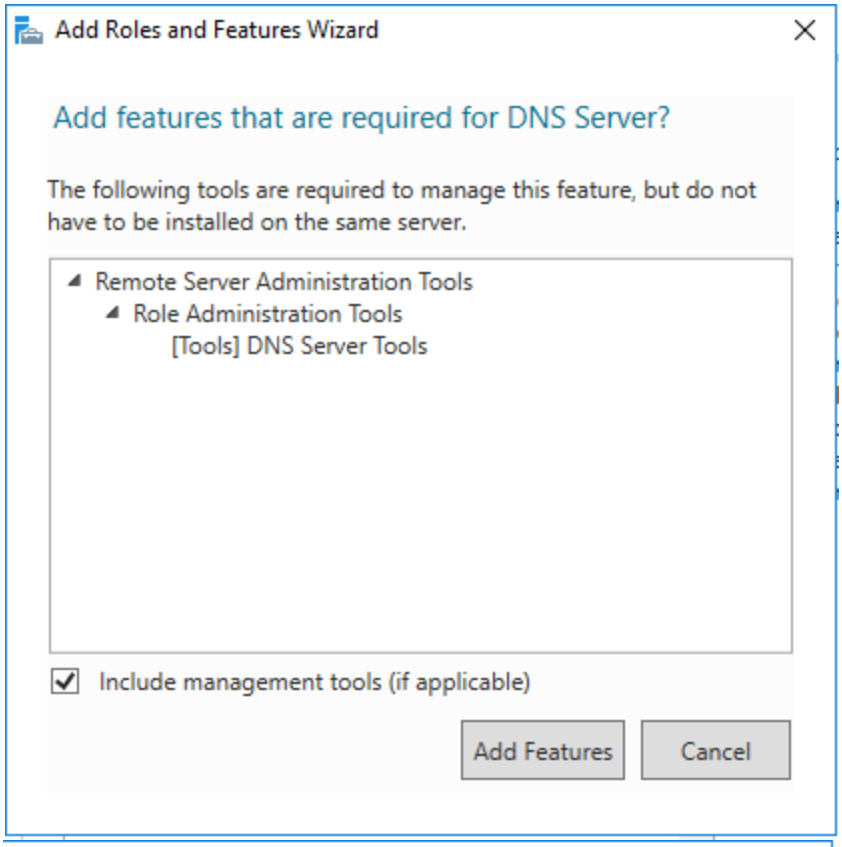

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WIN-OGK5RSQS55T
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, 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

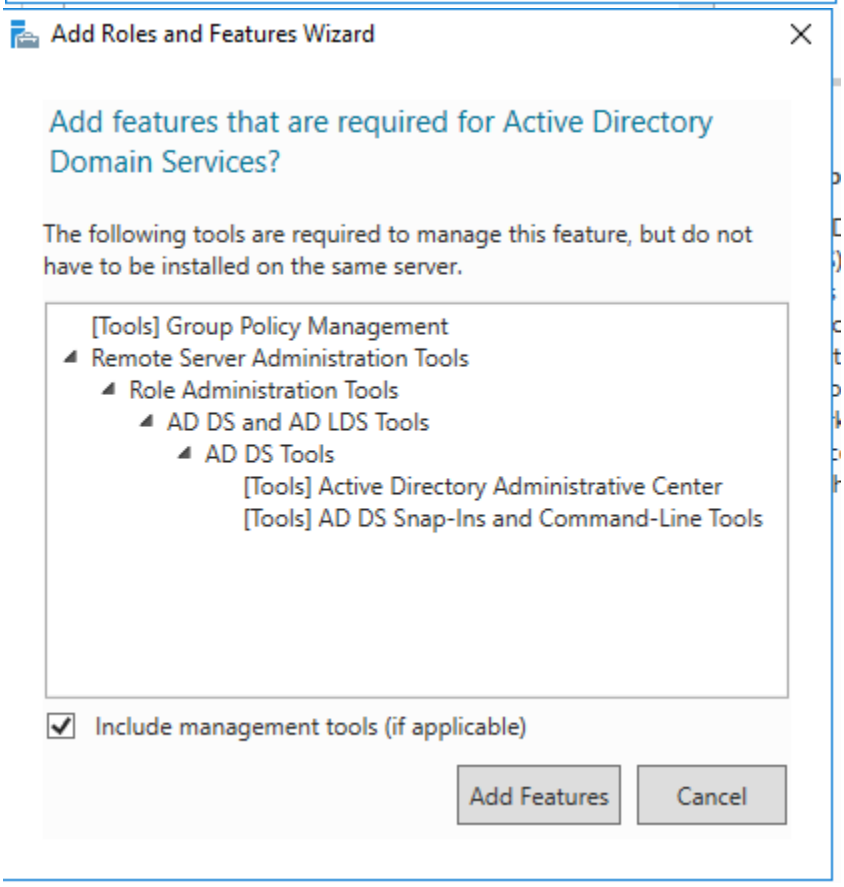
- Destination Server

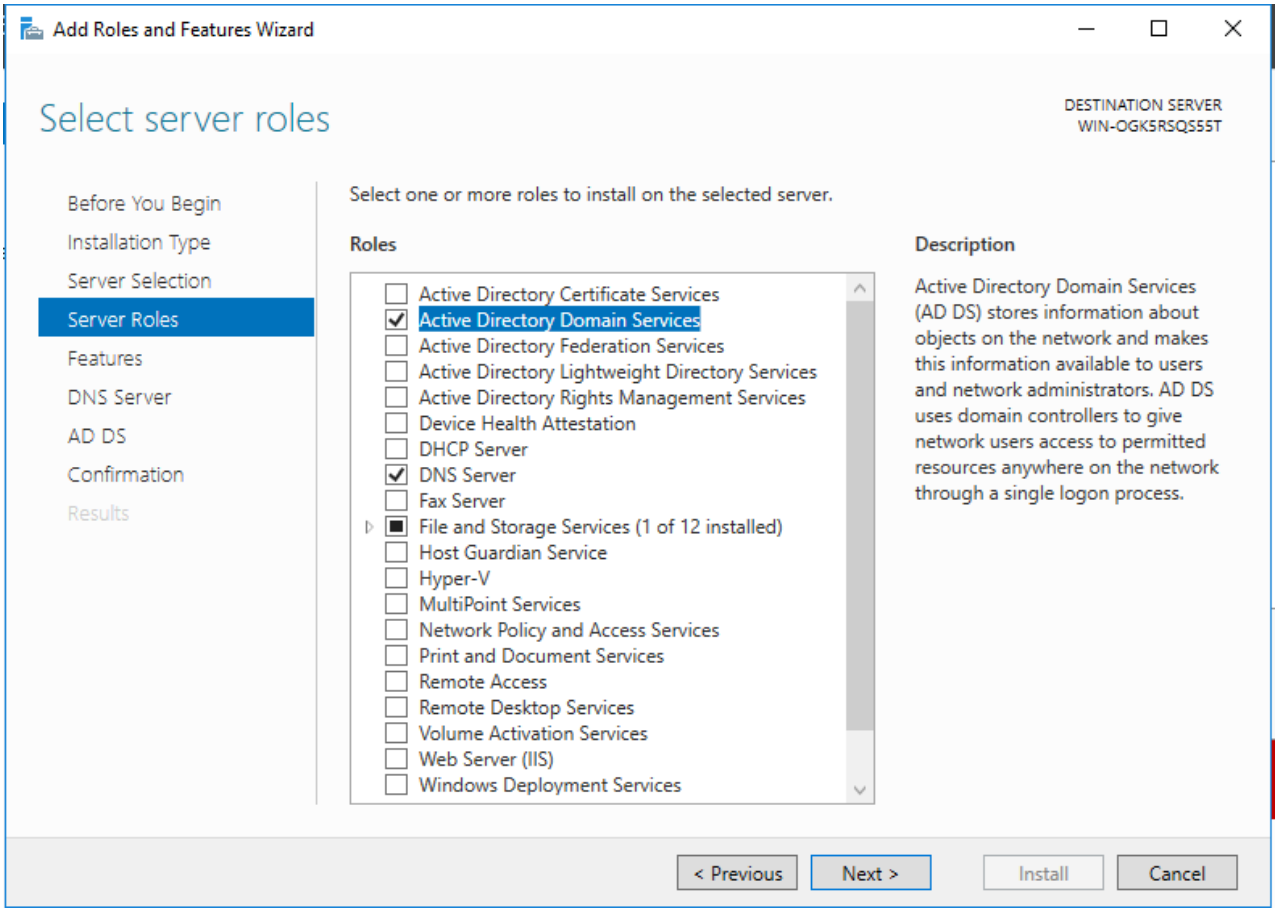


- Phần **Server Roles,** thêm các **Roles**: **DNS**, **Active Directory Domain Services**, và các **Features** đi kèm.

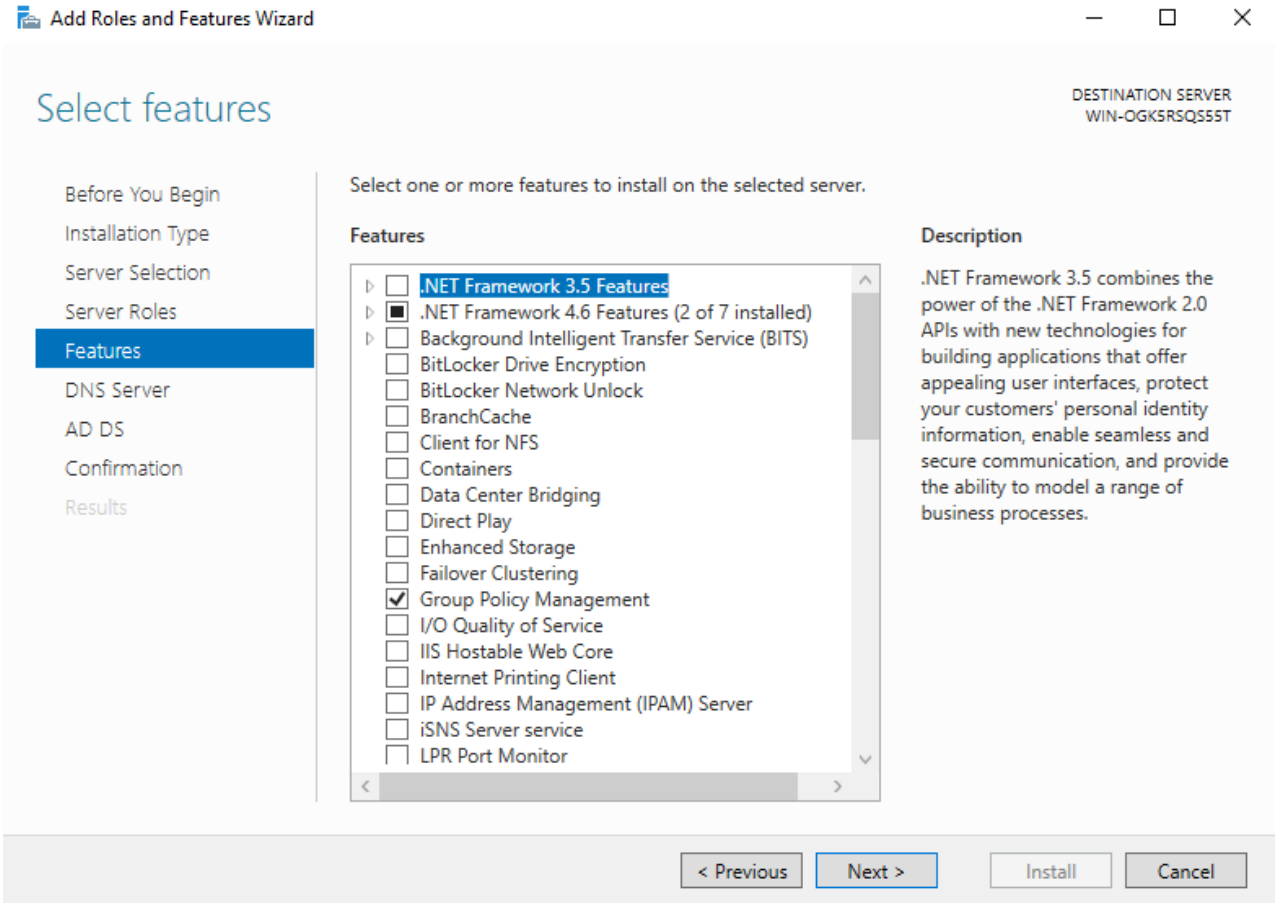


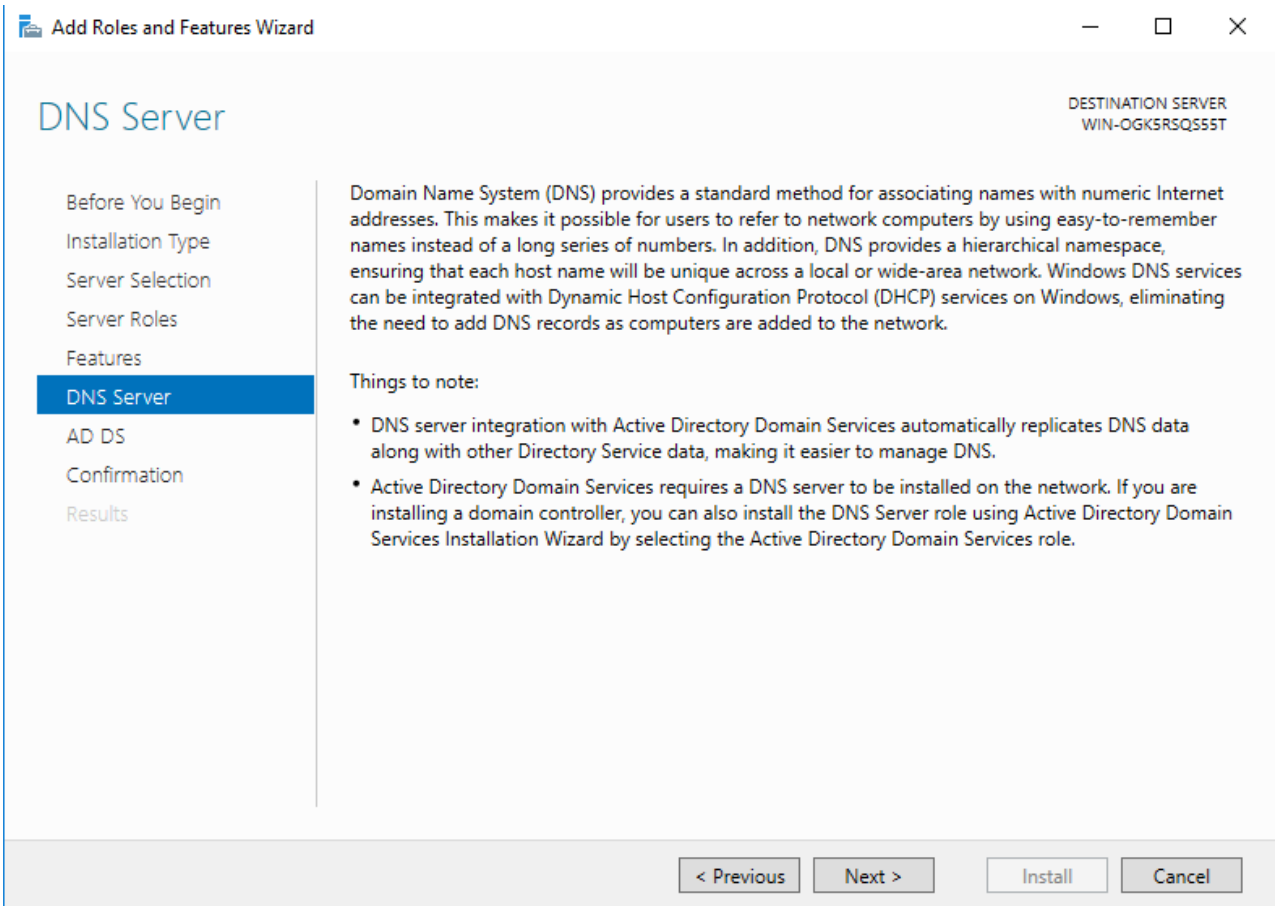

Add Roles and Features Wizard
Add features that are required for DNS Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DNS Server Tools
Include management tools (if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

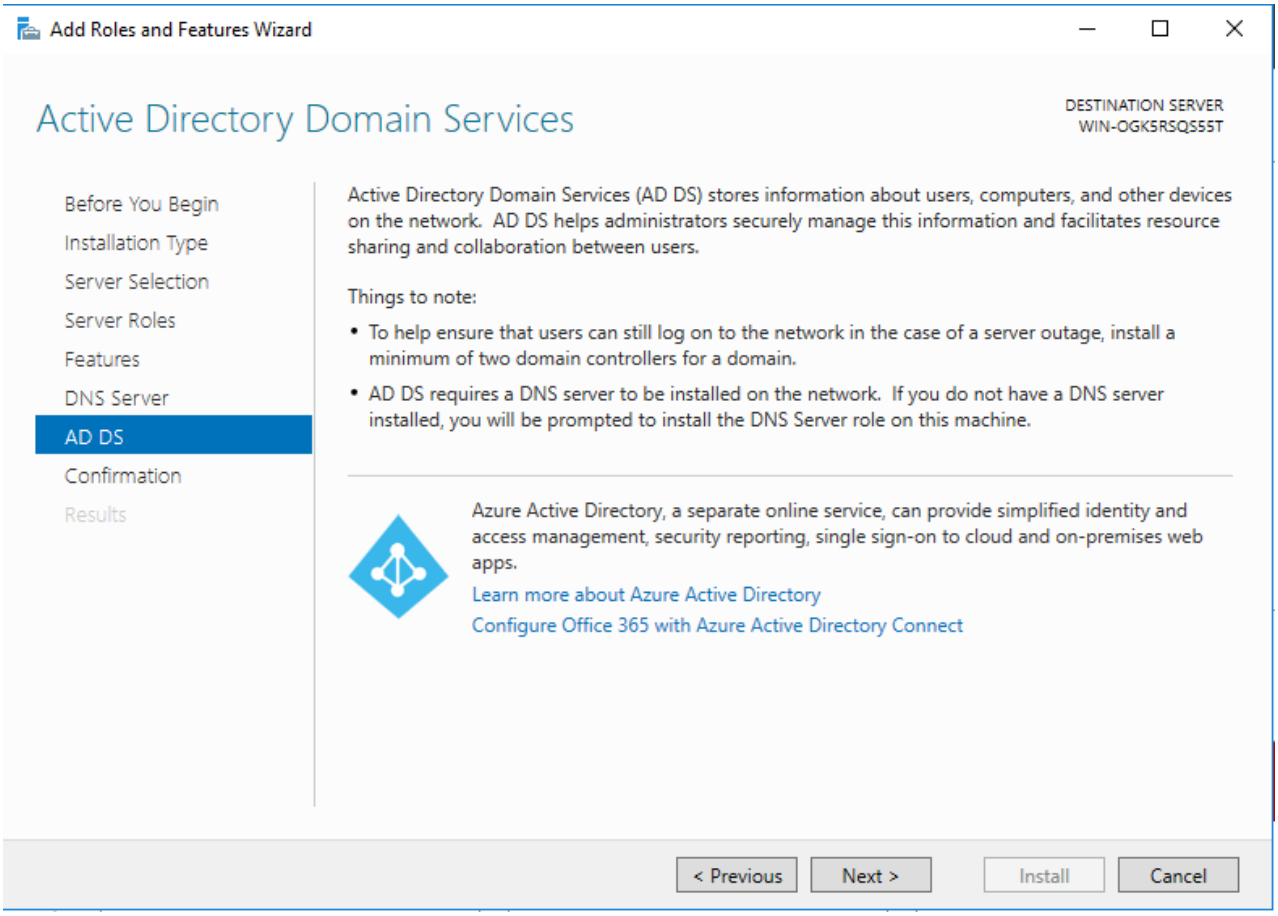

Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
The following tools are required to manage this feature, but do not have to be installed on the same server.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel


Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-OGK5RSQS55T
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DNS Server
AD DS
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
< Previous
Next >
Install
Cancel

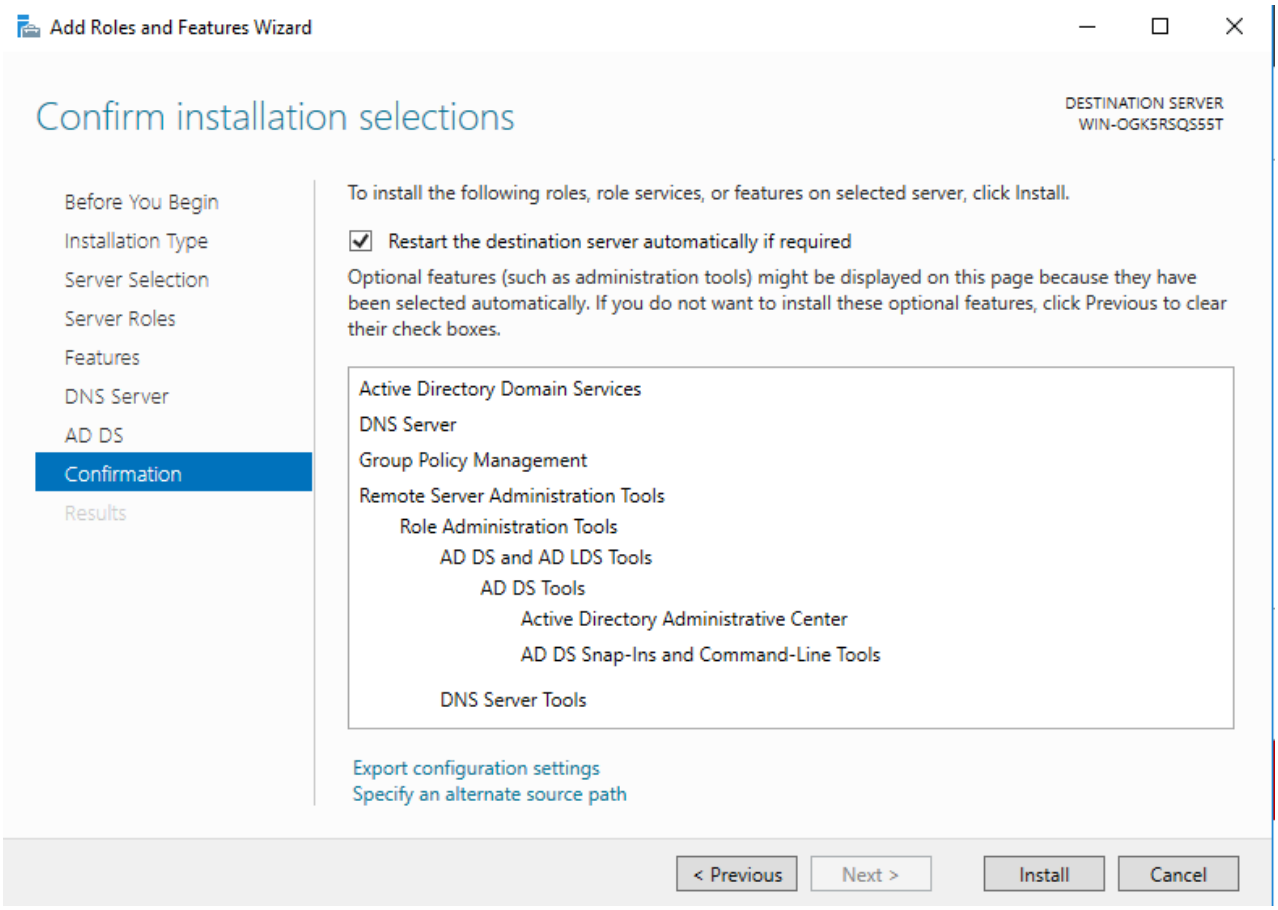
- Các phần tiếp theo ta chọn next



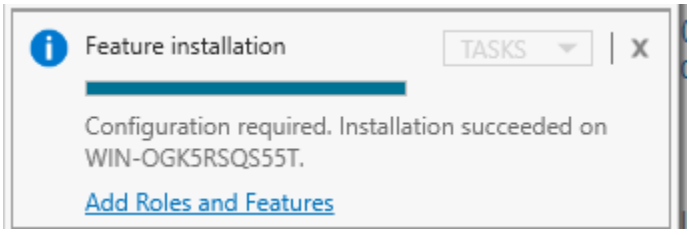

Add Roles and Features Wizard
DNS Server
DESTINATION SERVER
WIN-OGK5RSQS55T
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DNS Server
AD DS
Confirmation
Results
Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This makes it possible for users to refer to network computers by using easy-to-remember names instead of a long series of numbers. In addition, DNS provides a hierarchical namespace, ensuring that each host name will be unique across a local or wide-area network. Windows DNS services can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminating the need to add DNS records as computers are added to the network.
Things to note:
DNS server integration with Active Directory Domain Services automatically replicates DNS data along with other Directory Service data, making it easier to manage DNS.
Active Directory Domain Services requires a DNS server to be installed on the network. If you are installing a domain controller, you can also install the DNS Server role using Active Directory Domain Services Installation Wizard by selecting the Active Directory Domain Services role.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
WIN-OGK5RSQS55T
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DNS Server
AD DS
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.
Things to note:
To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect
< Previous
Next >
Install
Cancel

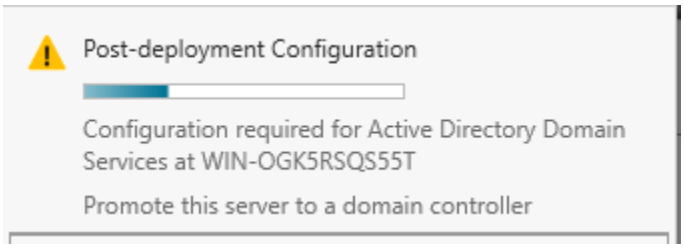
- Thực hiện cài đặt



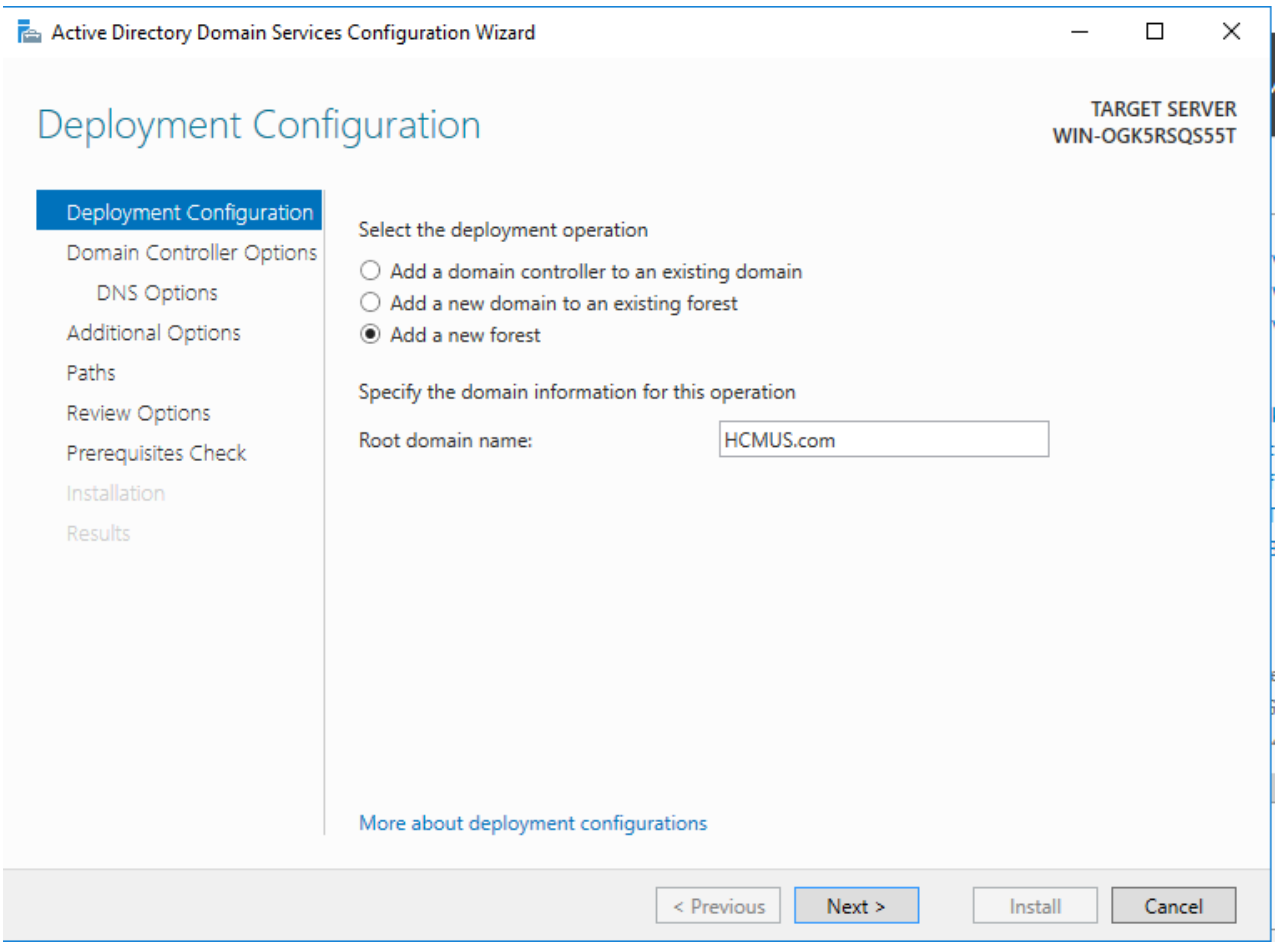
- Cài đặt thành công



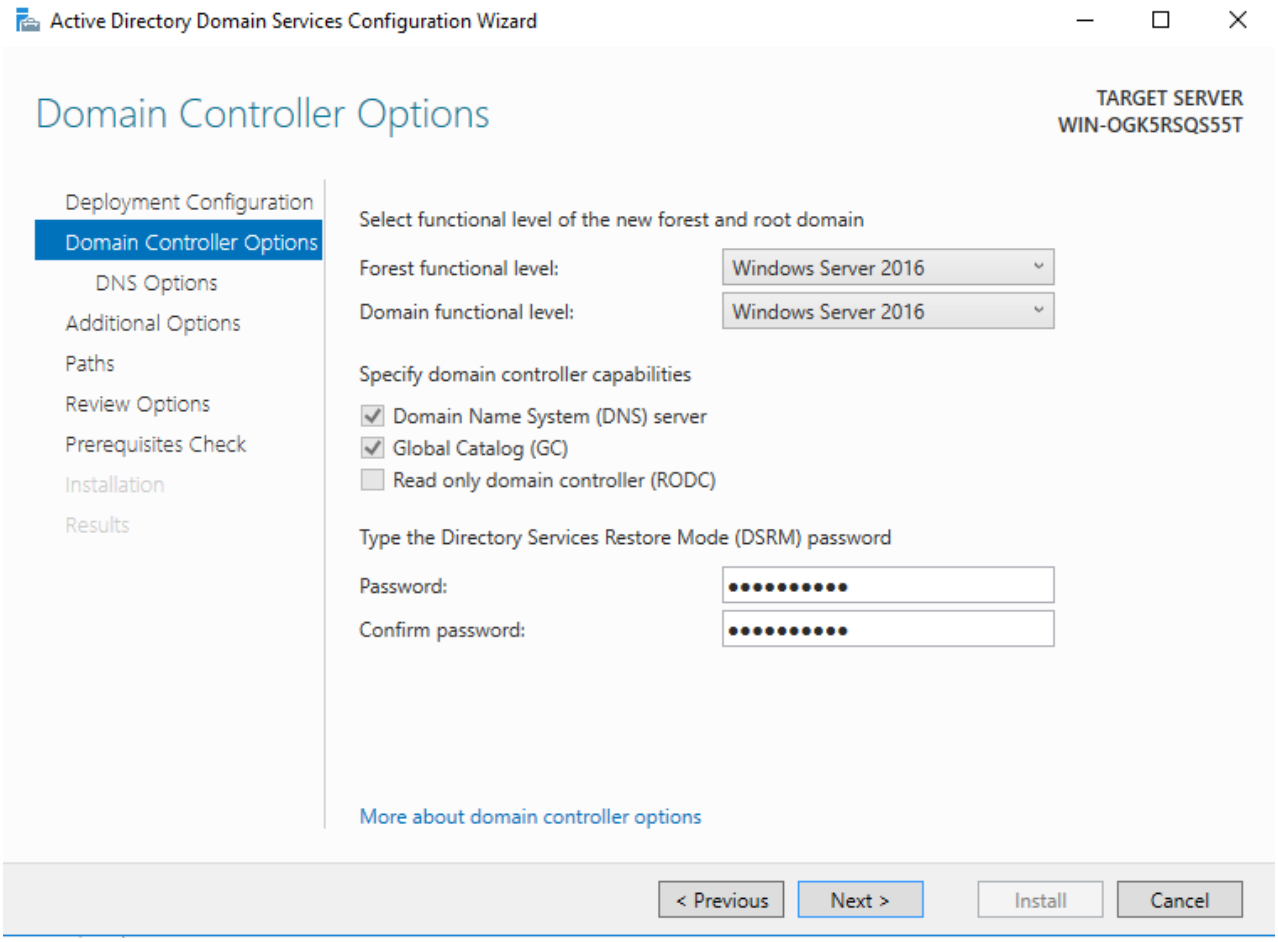
- Sau đó ta nâng cấp Server làm **Domain – Controller**



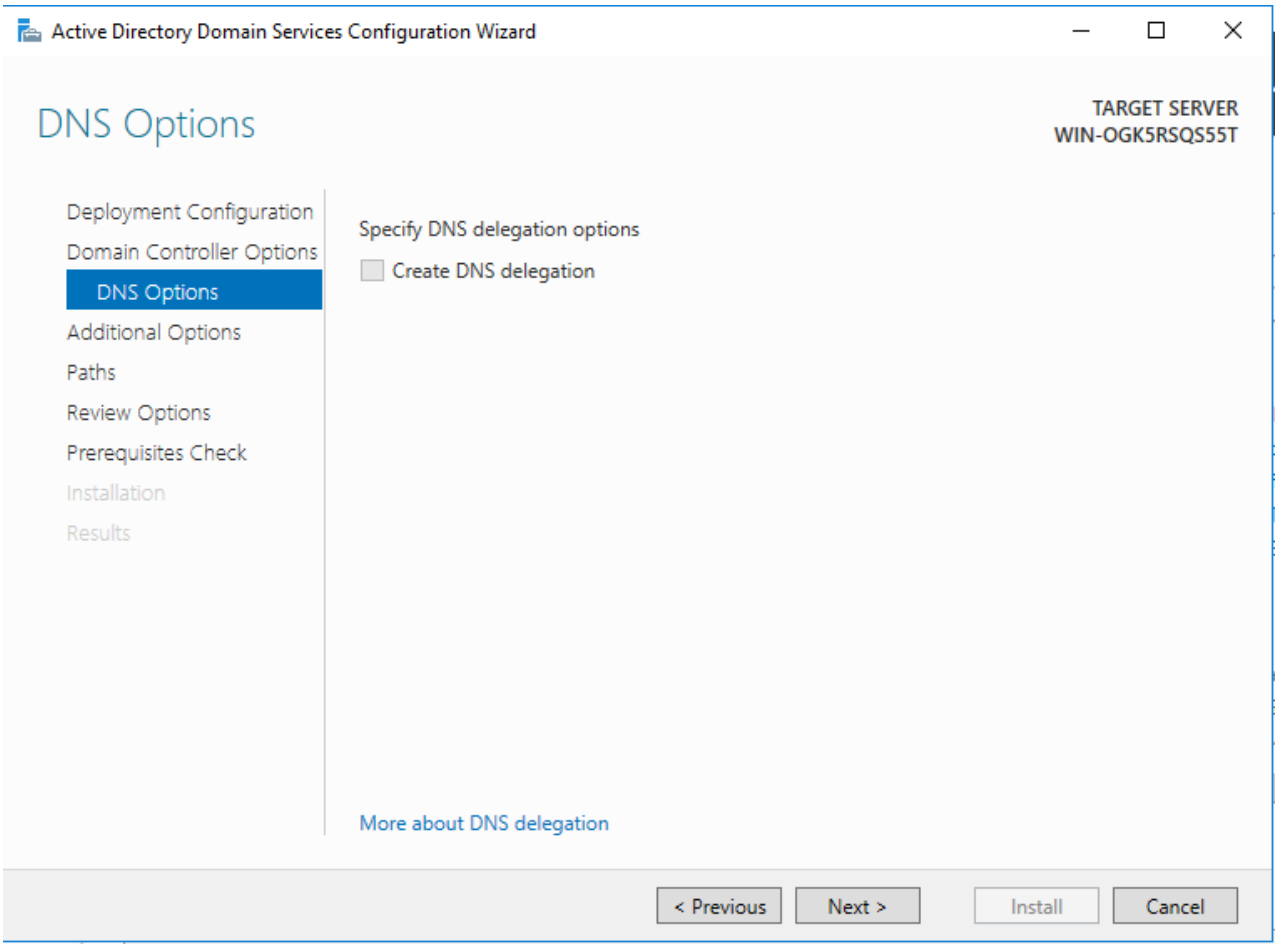
- Ở mục **Deployment Configuration** vừa hiện, ta thêm mới một **forest** với tên là **root domain** là **HCMUS.com**

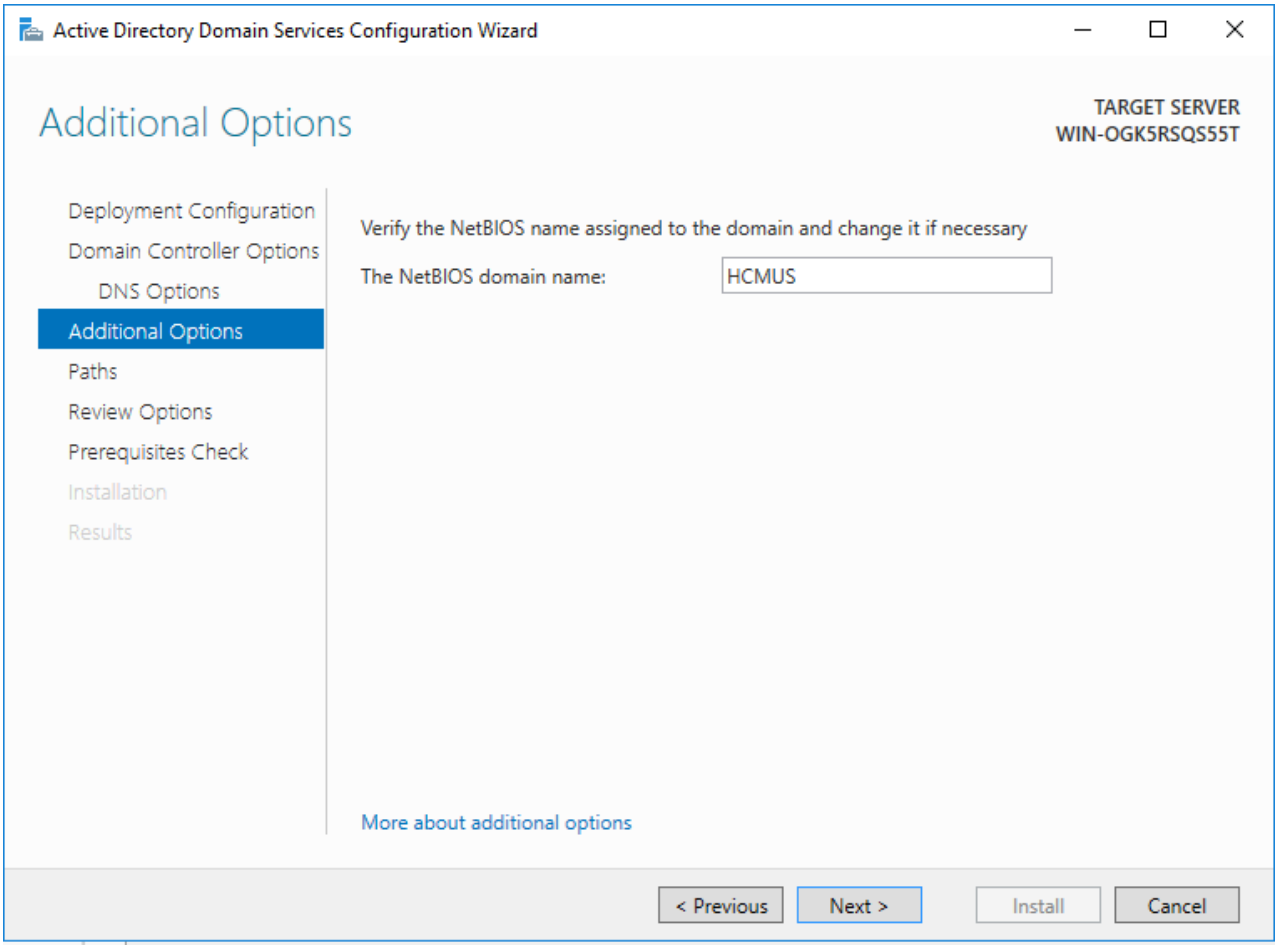


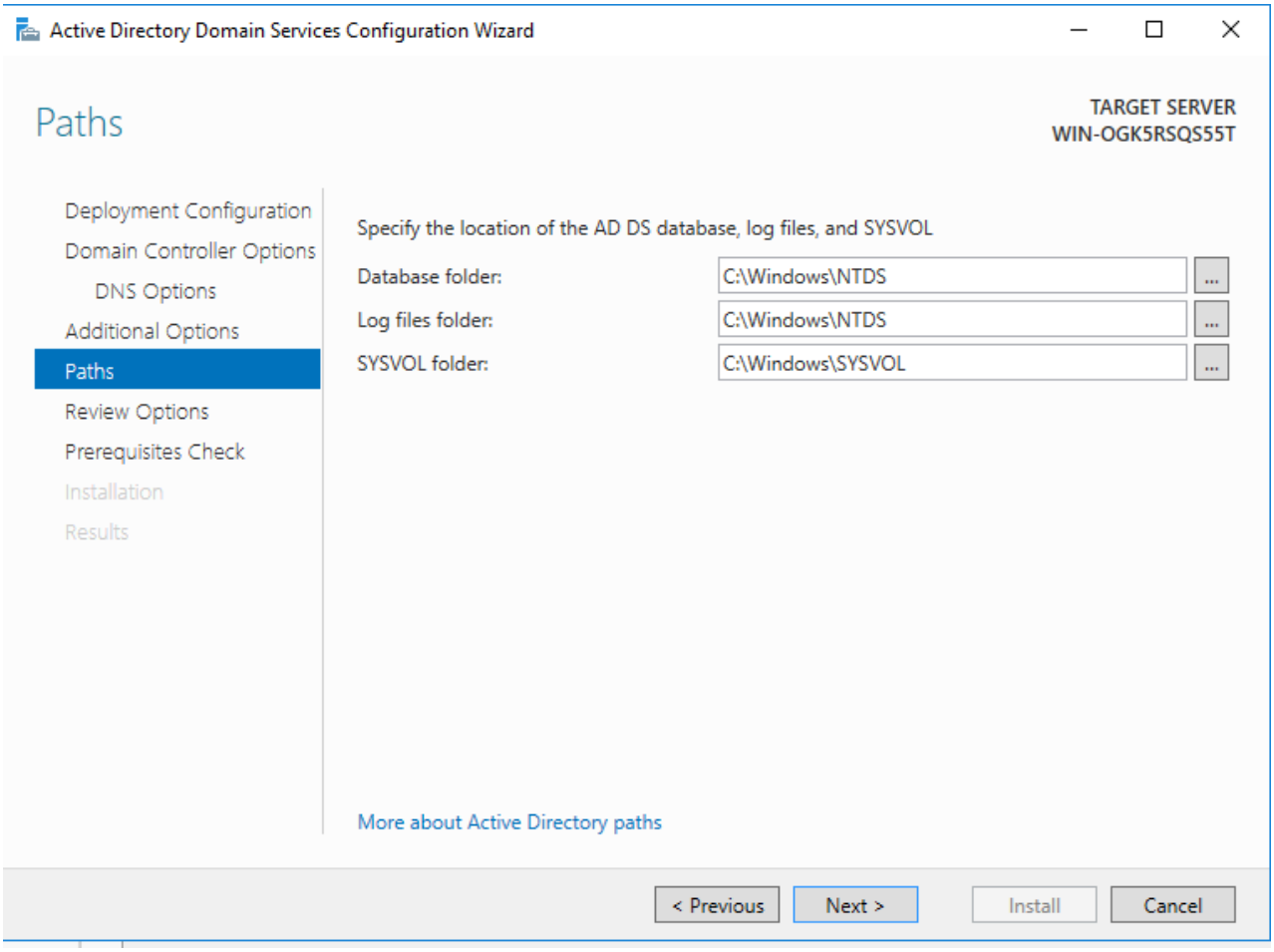
- Nhập password cho **Directory Services Restore Mode** (**DSMR**)

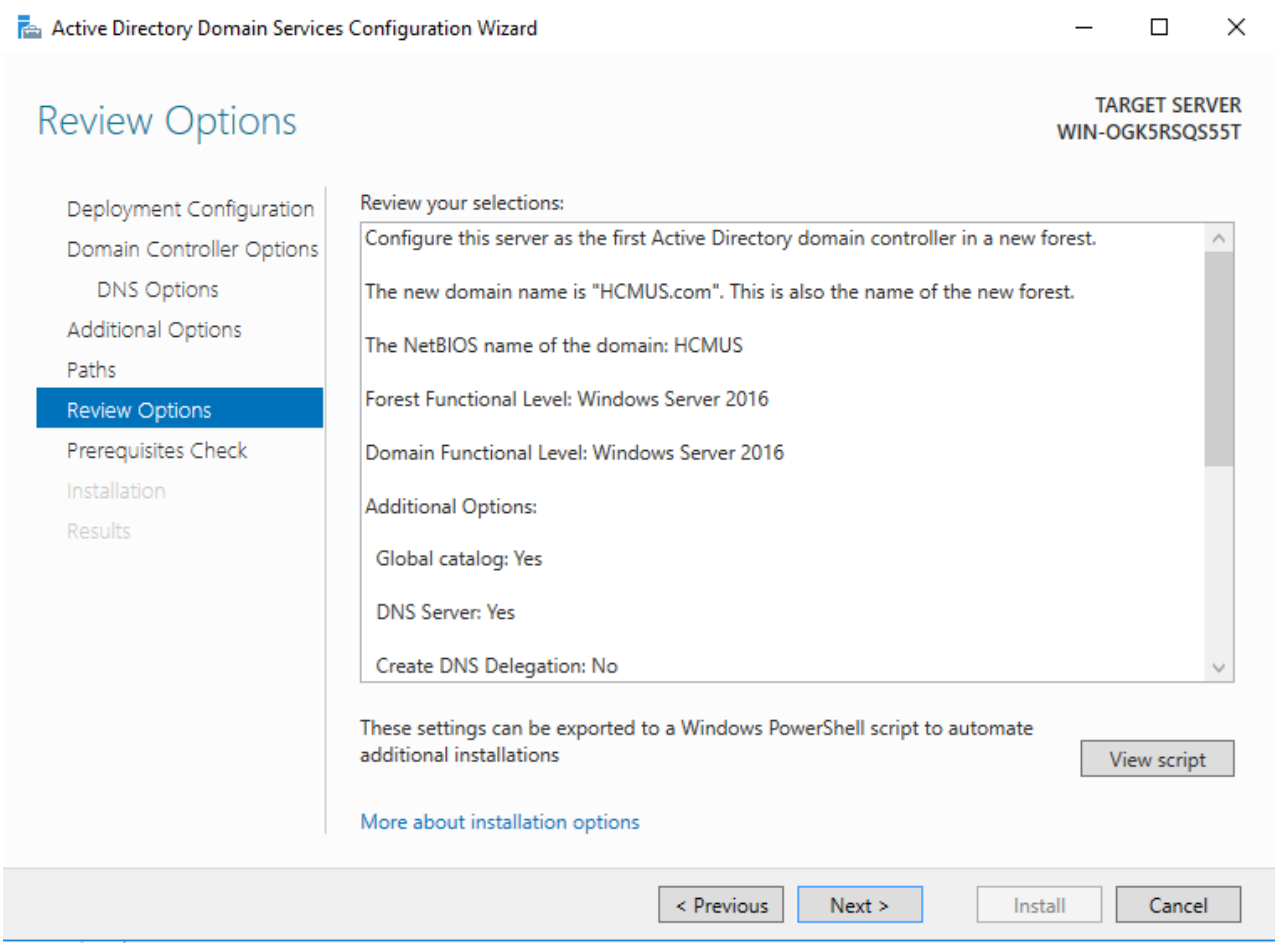


- Các bước tiếp theo, ta chọn next

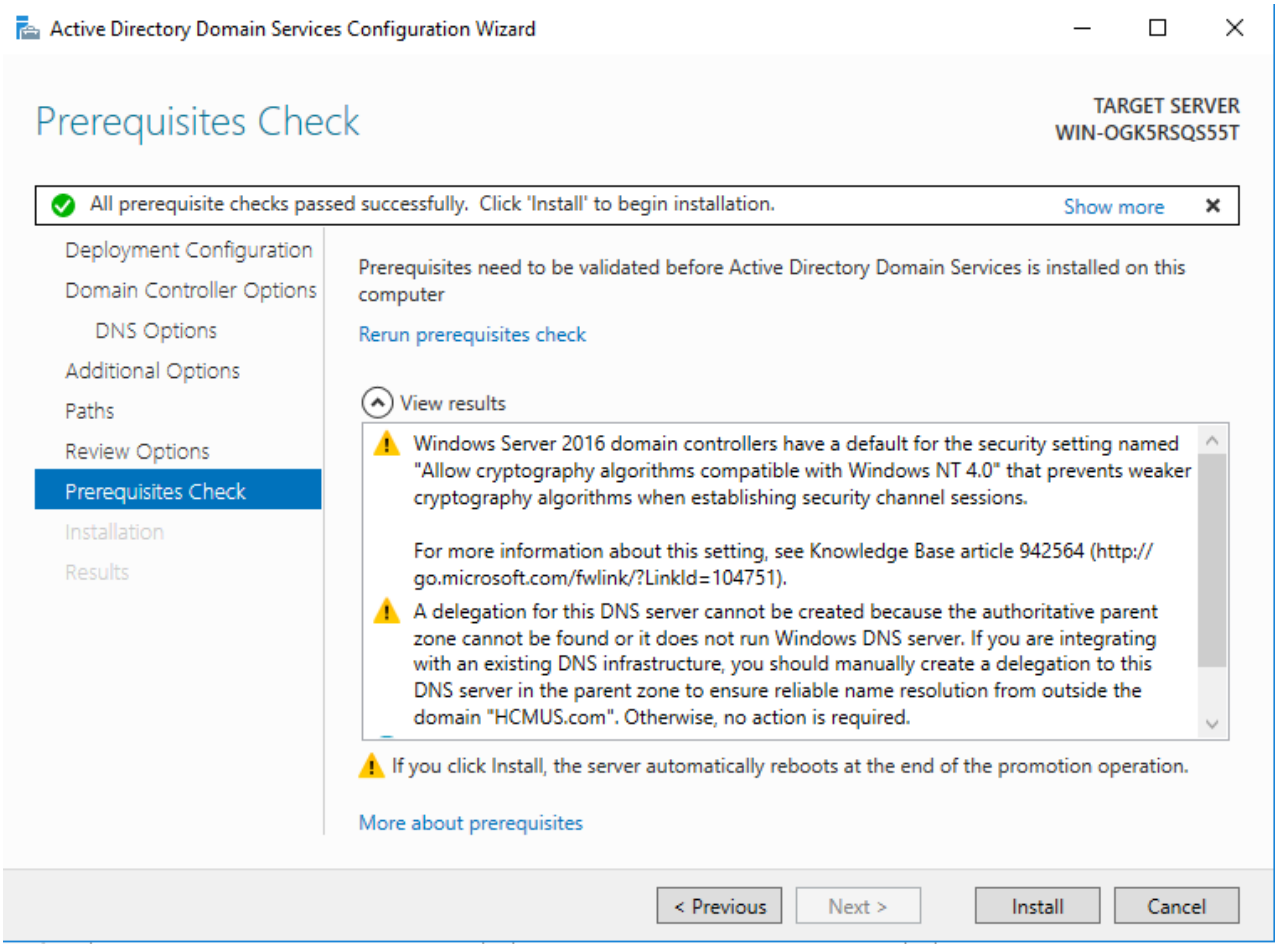



Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
WIN-OGK5RSQS55T
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
HCMUS
More about additional options
< Previous
Next >
Install
Cancel

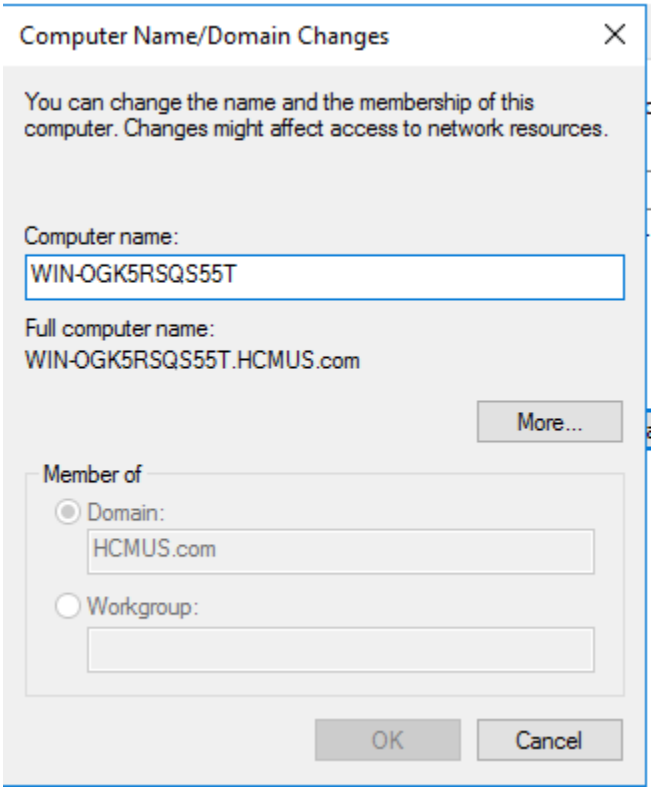

Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
WIN-OGK5RSQS55T
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Review Options
TARGET SERVER
WIN-OGK5RSQS55T
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Review your selections:
Configure this server as the first Active Directory domain controller in a new forest.
The new domain name is "HCMUS.com". This is also the name of the new forest.
The NetBIOS name of the domain: HCMUS
Forest Functional Level: Windows Server 2016
Domain Functional Level: Windows Server 2016
Additional Options:
Global catalog: Yes
DNS Server: Yes
Create DNS Delegation: No
These settings can be exported to a Windows PowerShell script to automate additional installations
View script
More about installation options
< Previous
Next >
Install
Cancel

- Tiến hành cài đặt

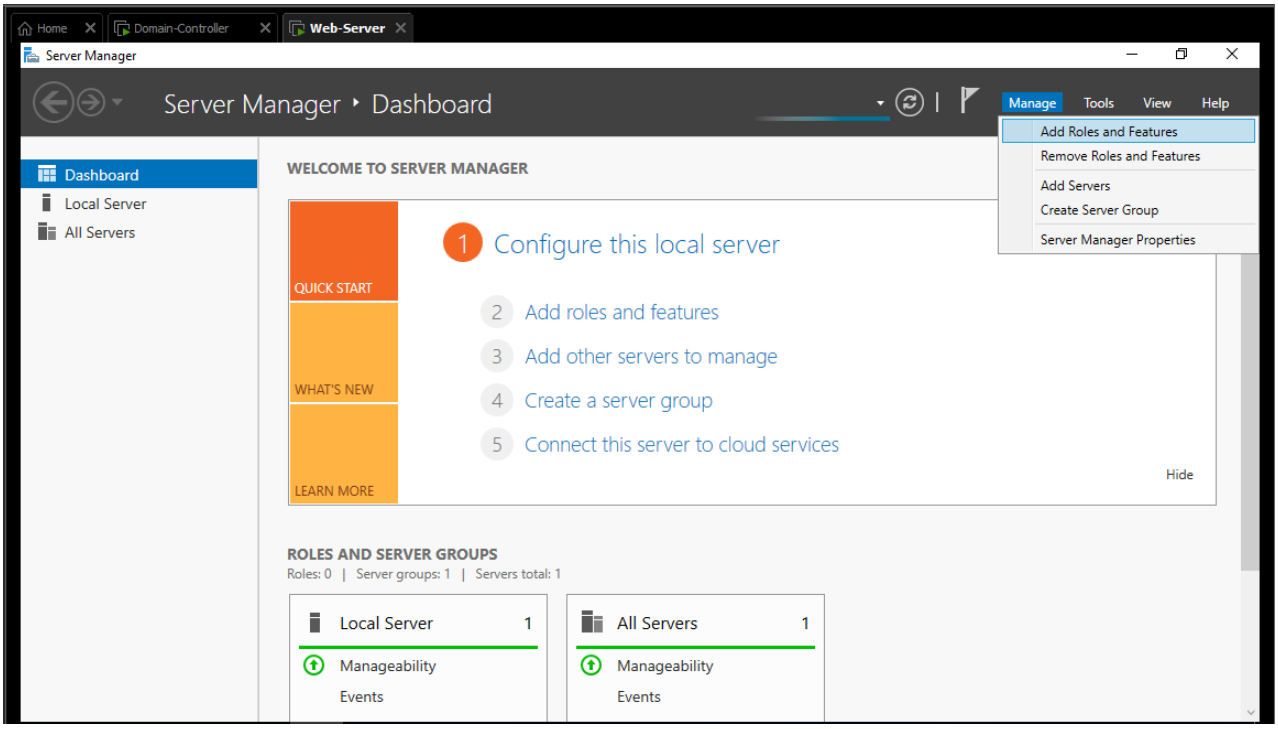


- Cài đặt thành công

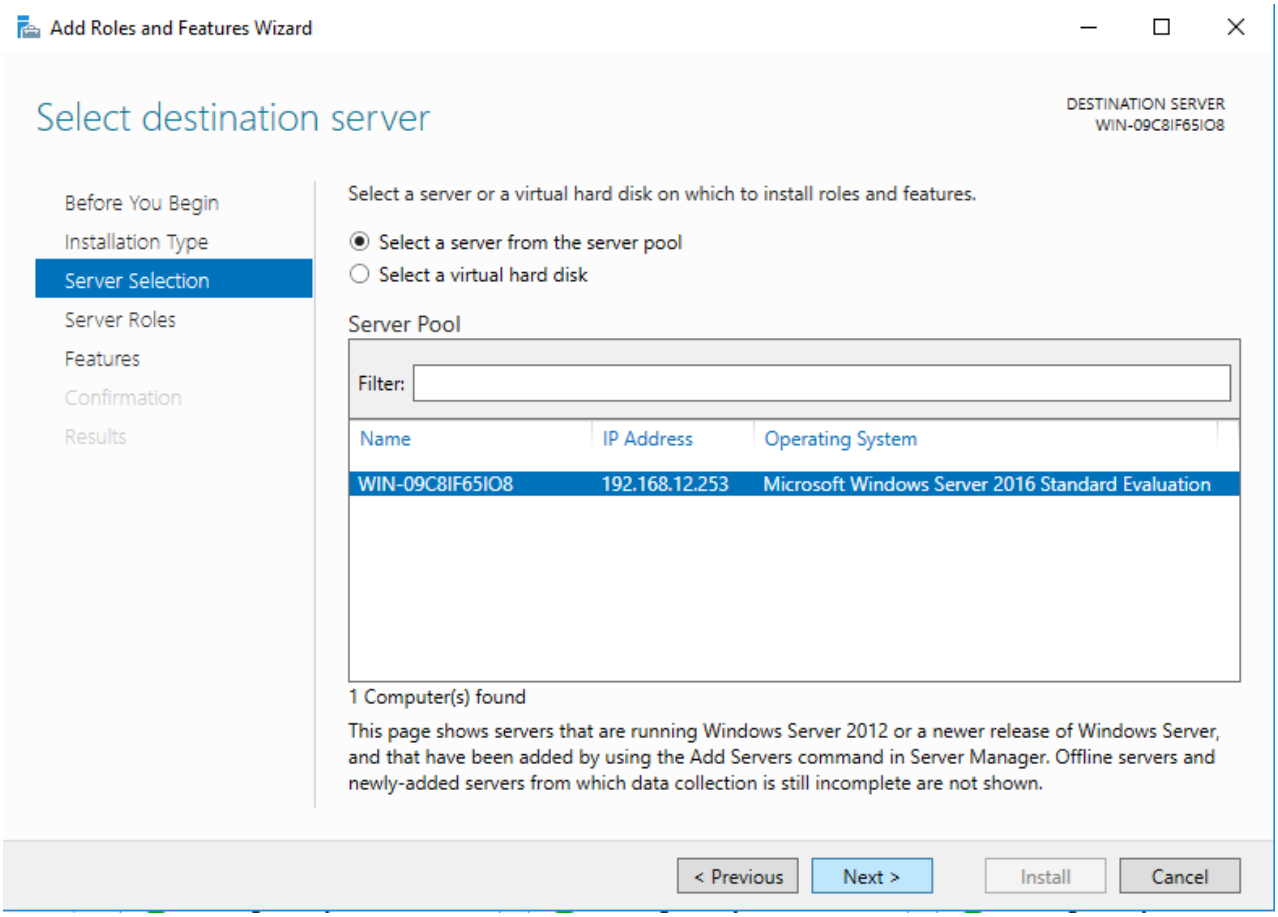


II.1.2. Web – Server

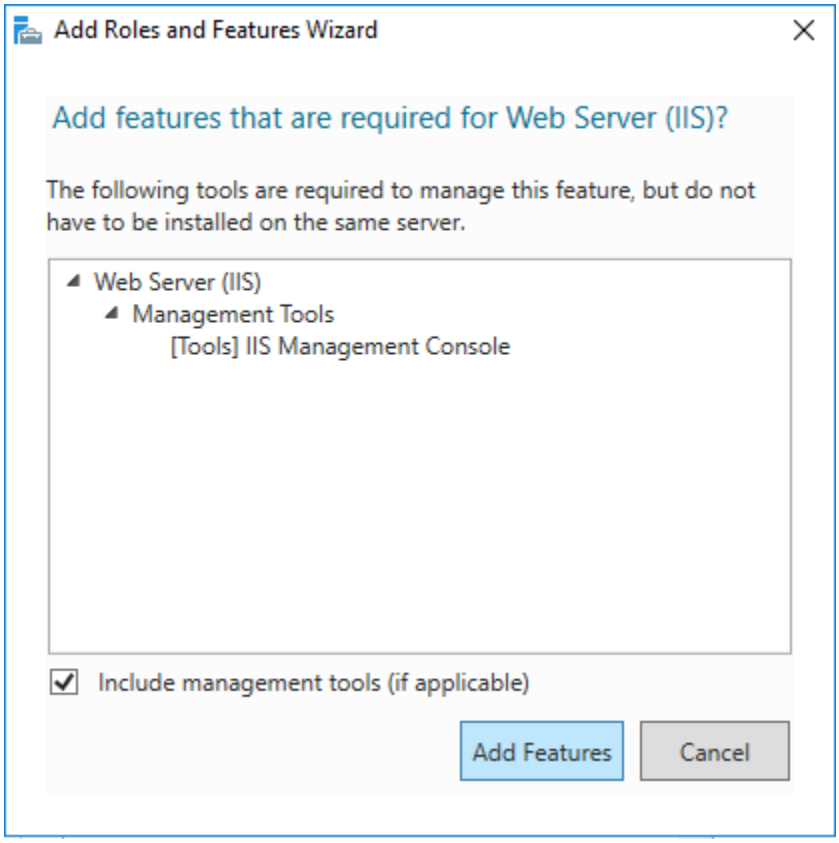
- Thực hiện cài đặt **Web Server (IIS)**
- Chọn **Add Roles and Features**

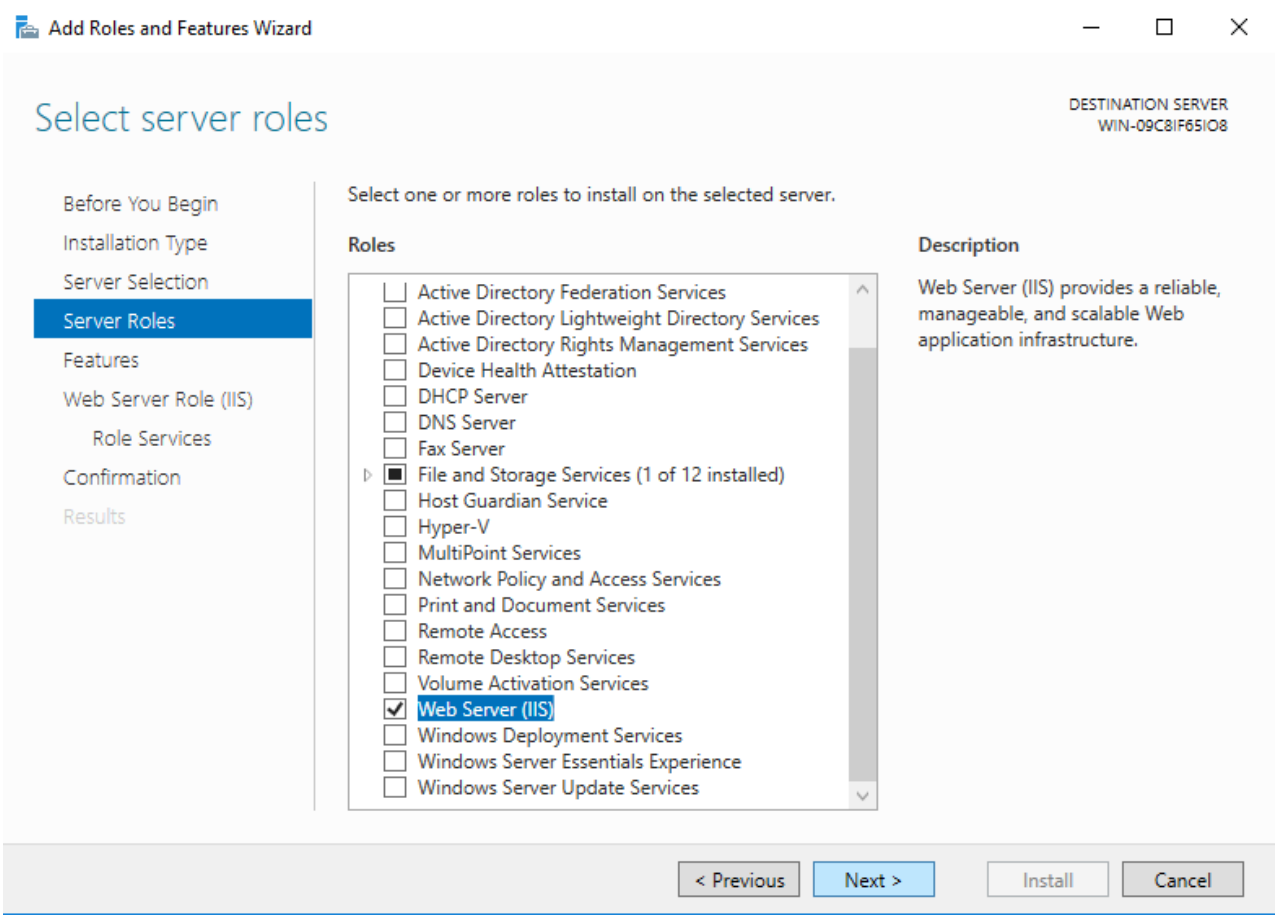


- Các bước tiếp theo ta chọn next, sử dụng thiết lập mặc định (giống máy Domain – Controller).
- Destitnation Server

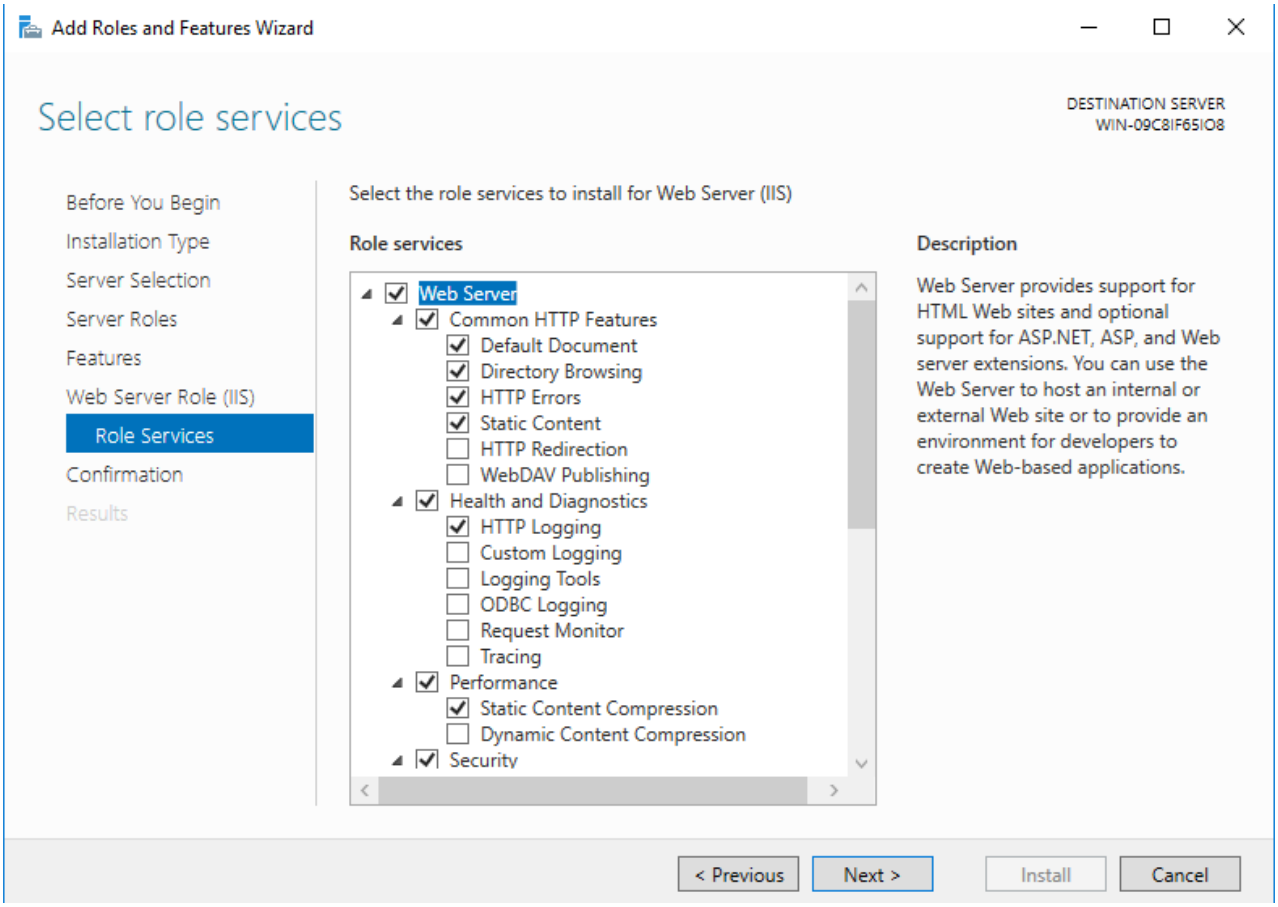


- Phần **Server Roles,** thêm **Roles: Web Server IIS** và các **Features** đi kèm

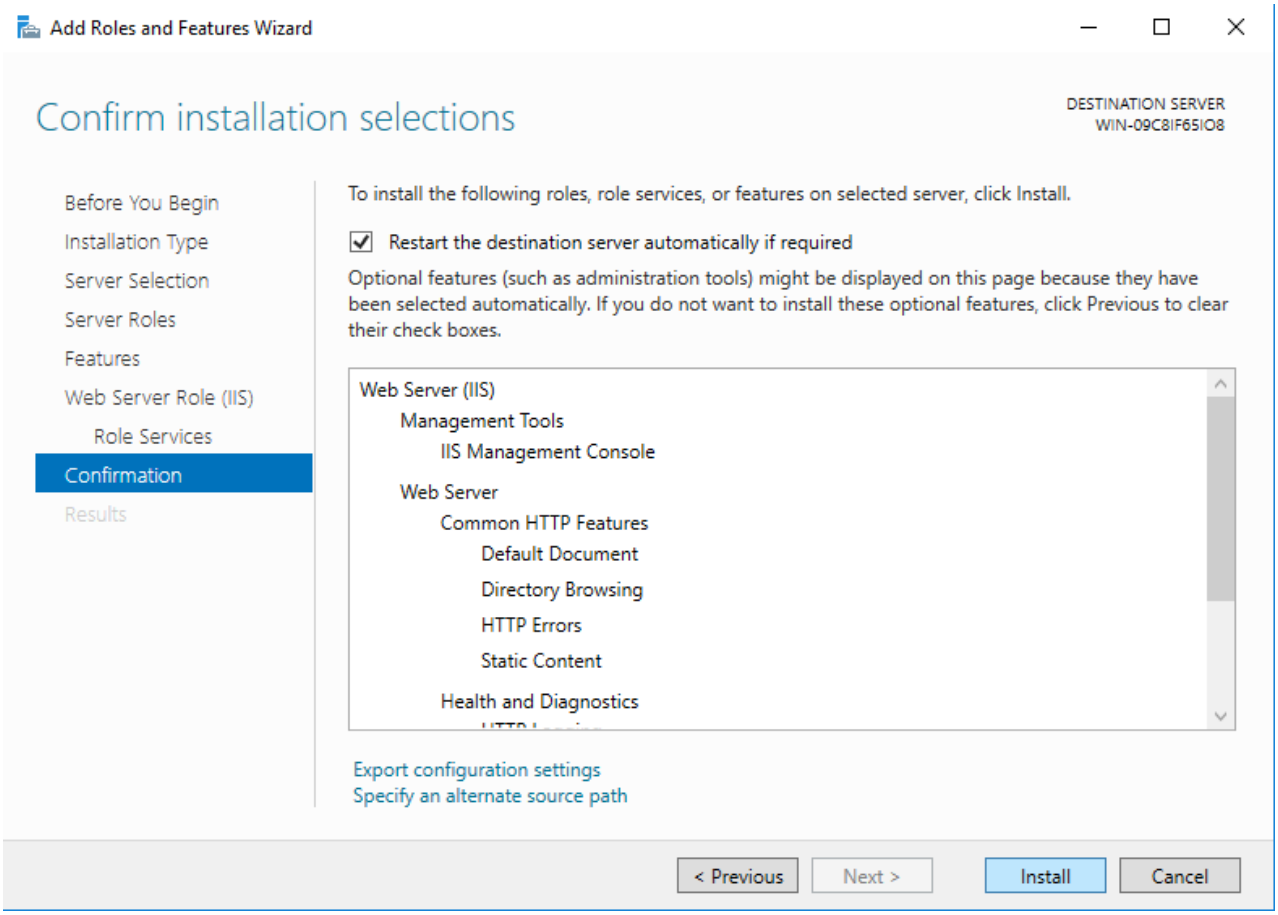



Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-09C8IF65IO8
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Essentials Experience
Windows Server Update Services
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
< Previous
Next >
Install
Cancel

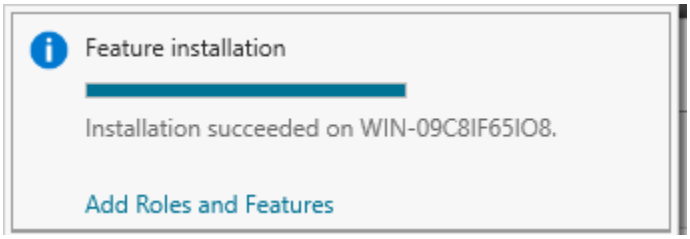
- Sau đó ta chọn next cho các phần tiếp theo (giống máy Domain – Controller)
- Phần **Role Services** của **Web Server Role (IIS)** ta để mặc định



- Tiến hành cài đặt



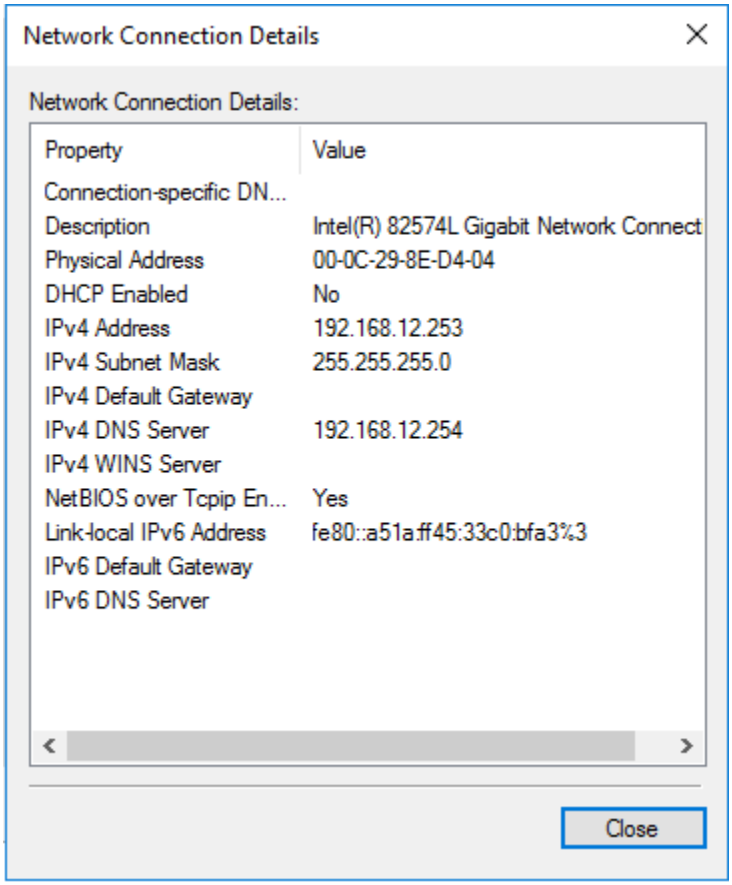
- Cài đặt thành công



II.2. Cấu hình địa chỉ IP cho các máy

- Các máy Domain – Controller (CA Server), Web – Server, Client (máy thật) cùng thuộc chung một đường mạng là: 192.168.12.0/24 (trong thực tế thì không cần thiết)
- Máy Client (máy thật) sử dụng card mạng **Vmnet1** để kết nối với các máy còn lại, có địa chỉ IP là: 192.168.12.100/24. Hai máy ảo Server còn lại sử dụng chế độ **Host-only**
- Máy Domain – Controller (CA Server): 192.168.12.254/24
- Máy Web – Server: 192.168.12.253/24

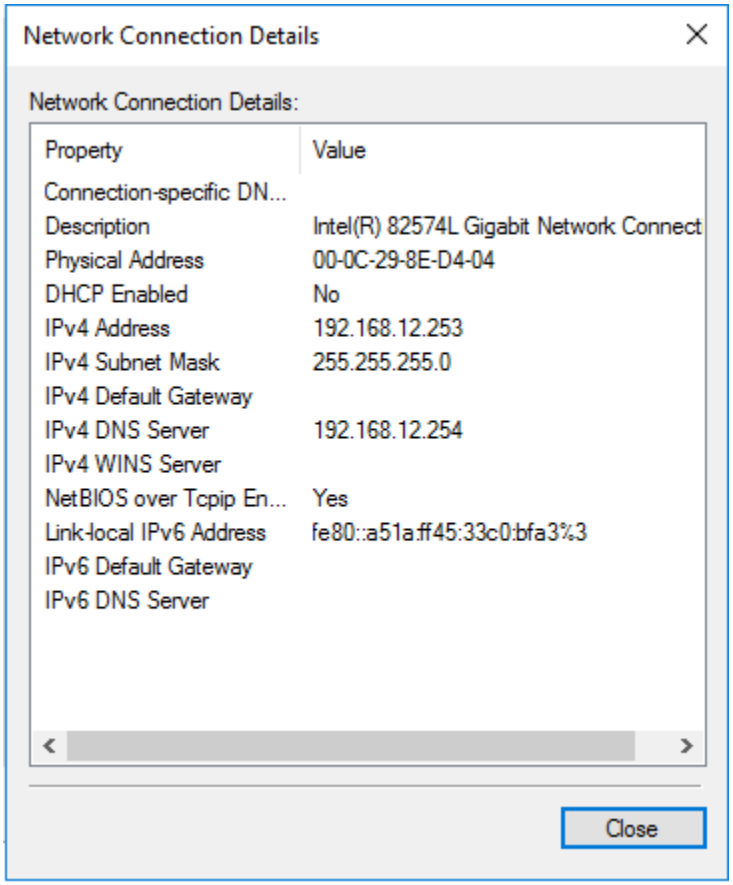
II.2.1. Domain – Controller (CA Server)



- Kiểm tra kết nối bằng cách ping đến 2 máy còn lại

```
C:\Users\Administrator>ping 192.168.12.253

Pinging 192.168.12.253 with 32 bytes of data:
Reply from 192.168.12.253: bytes=32 time<1ms TTL=128
Reply from 192.168.12.253: bytes=32 time<1ms TTL=128
Reply from 192.168.12.253: bytes=32 time<1ms TTL=128
Reply from 192.168.12.253: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.12.100

Pinging 192.168.12.100 with 32 bytes of data:
Reply from 192.168.12.100: bytes=32 time<1ms TTL=128
Reply from 192.168.12.100: bytes=32 time<1ms TTL=128
Reply from 192.168.12.100: bytes=32 time<1ms TTL=128
Reply from 192.168.12.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

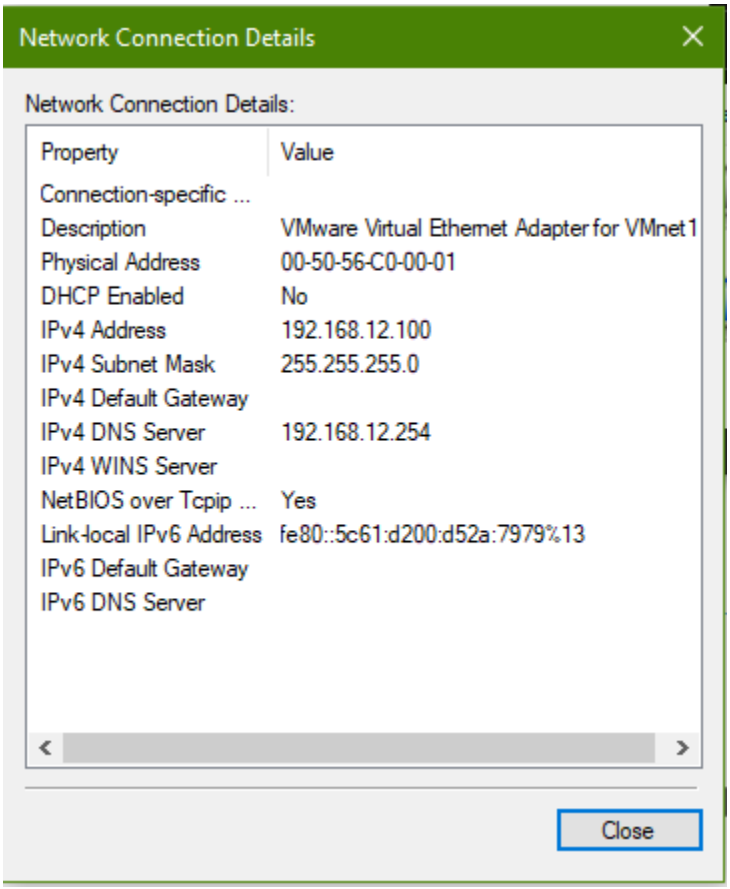
II.2.2. Web – Server



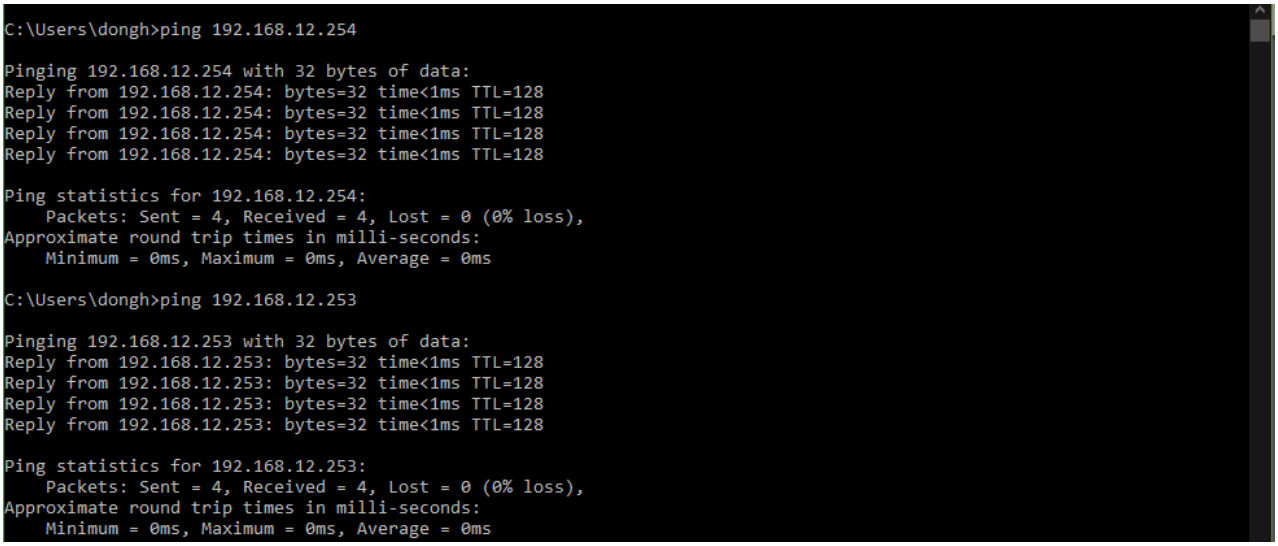
- Kiểm tra kết nối bằng cách ping đến 2 máy còn lại

```
C:\Users\Administrator>ping 192.168.12.254

Pinging 192.168.12.254 with 32 bytes of data:
Reply from 192.168.12.254: bytes=32 time<1ms TTL=128
Reply from 192.168.12.254: bytes=32 time<1ms TTL=128
Reply from 192.168.12.254: bytes=32 time<1ms TTL=128
Reply from 192.168.12.254: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping 192.168.12.100

Pinging 192.168.12.100 with 32 bytes of data:
Reply from 192.168.12.100: bytes=32 time<1ms TTL=128
Reply from 192.168.12.100: bytes=32 time<1ms TTL=128
Reply from 192.168.12.100: bytes=32 time<1ms TTL=128
Reply from 192.168.12.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.12.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

II.2.3. Client (máy thật)



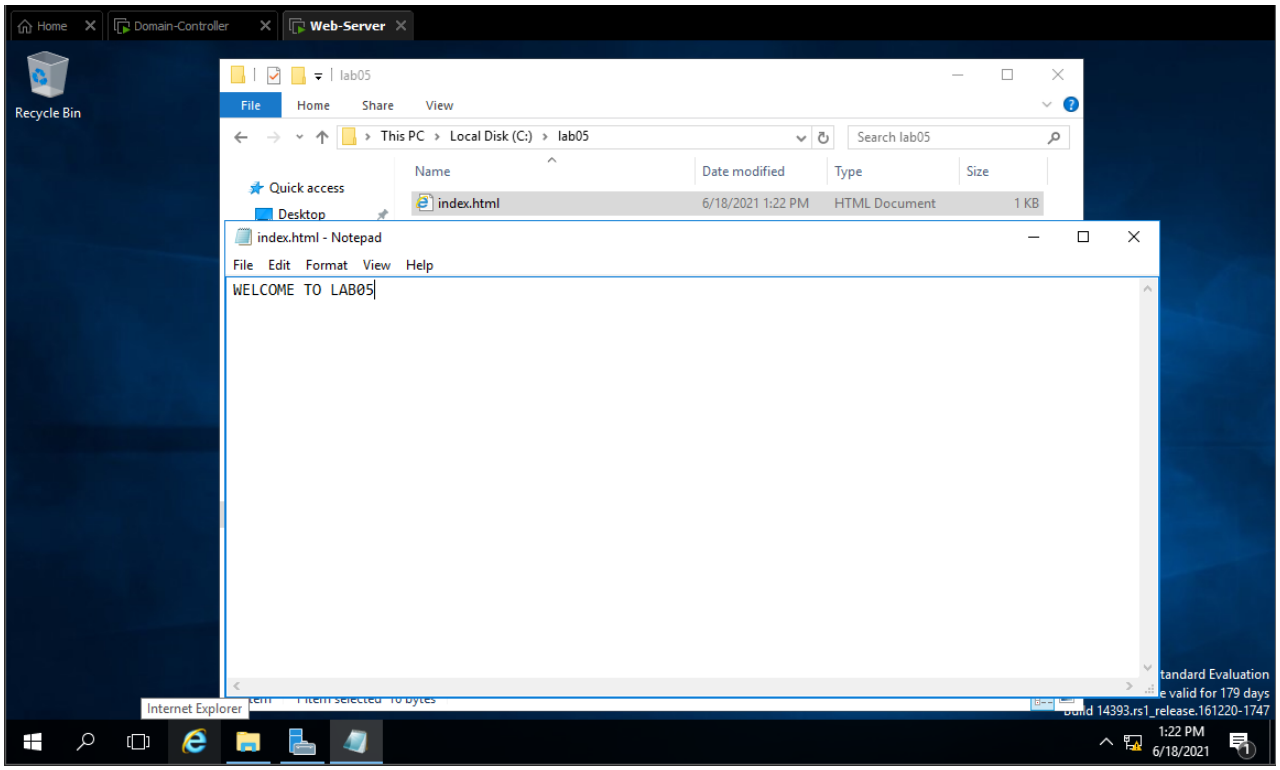
- Kiểm tra bằng cách ping đến 2 máy còn lại



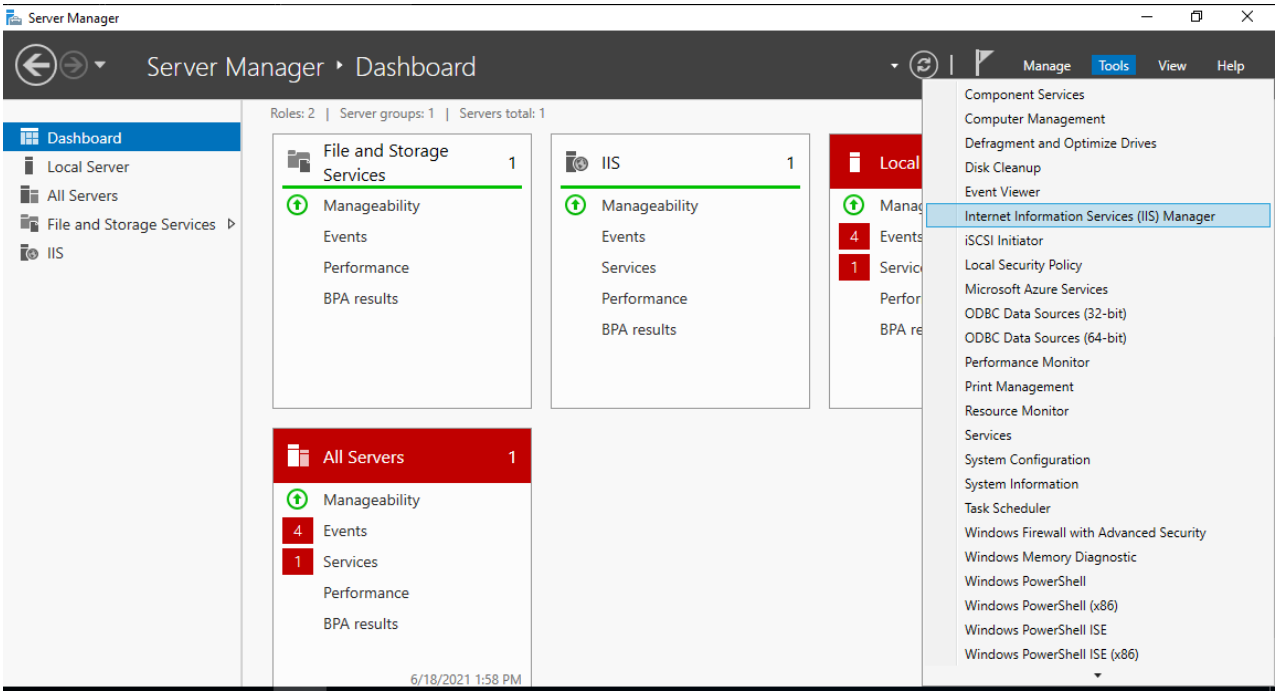
II.3. Tạo Website, cho phép máy Client truy cập thông qua Domain – Controller (CA Server)

II.3.1. Web – Server

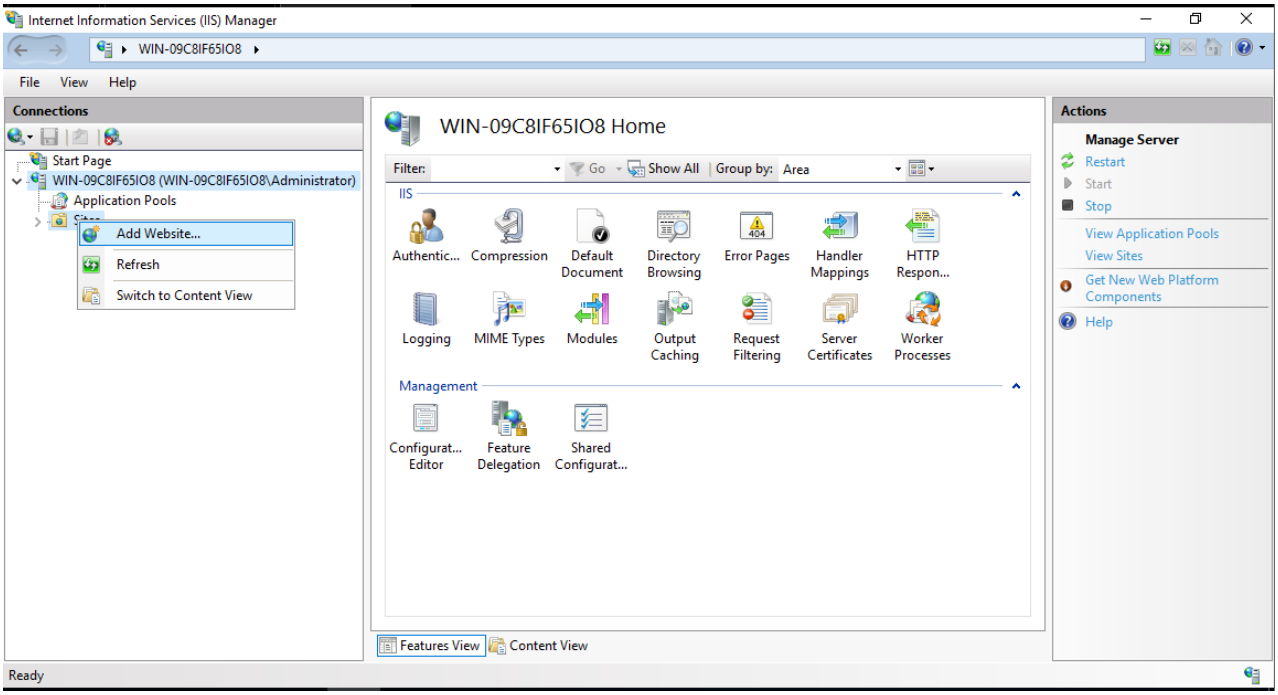
- Vào ổ **C:** sau đó tạo thư mục chứa web: **lab05** sau đó tạo một file **index.html** với nội dung như sau (khi truy cập vào được website thì sẽ hiện lên).



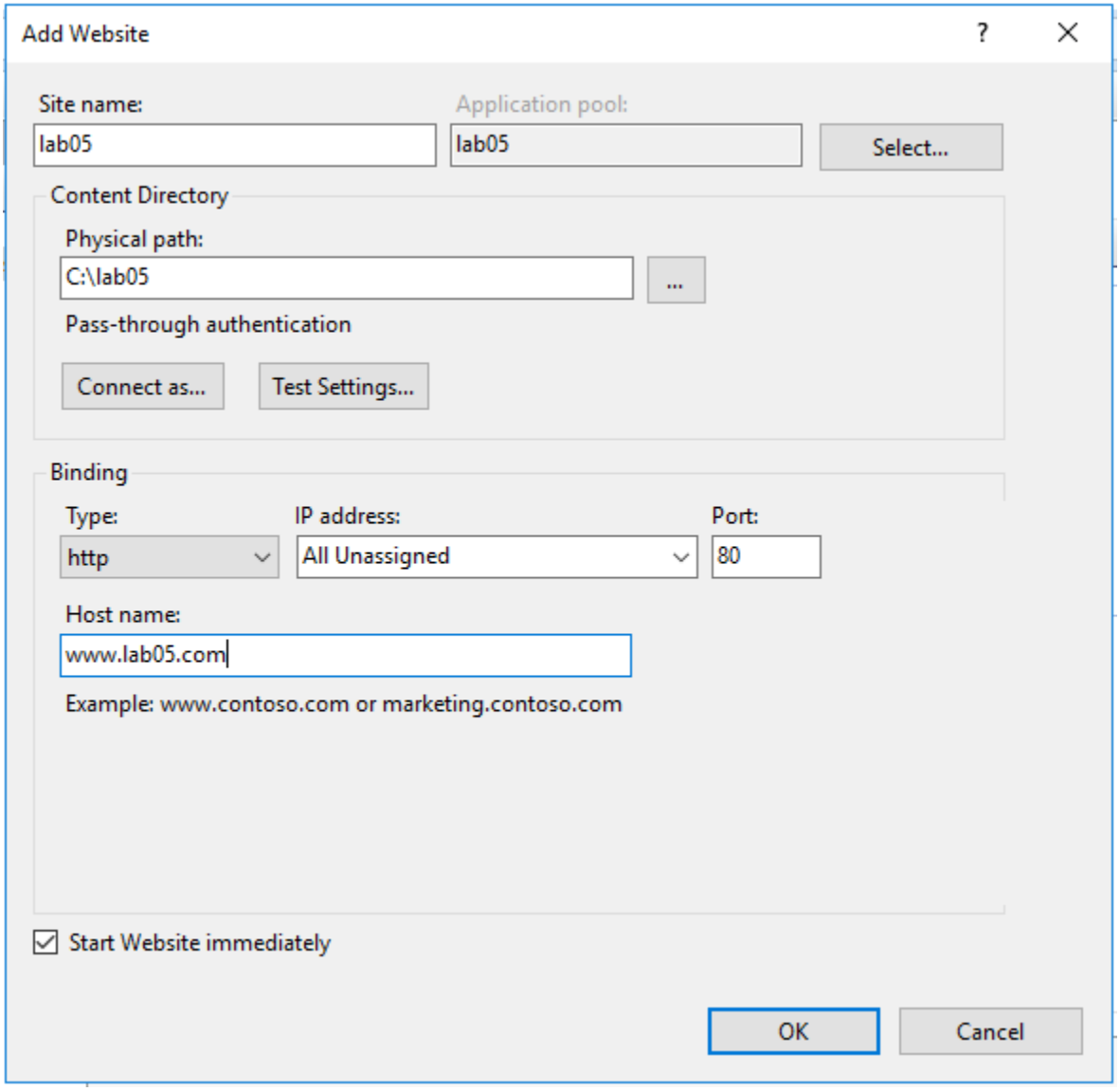
- Để public file này ra, ta vào **Server Manager => Tools => Internet Information Services (IIS) Manager**



- Ta thêm một Website mới

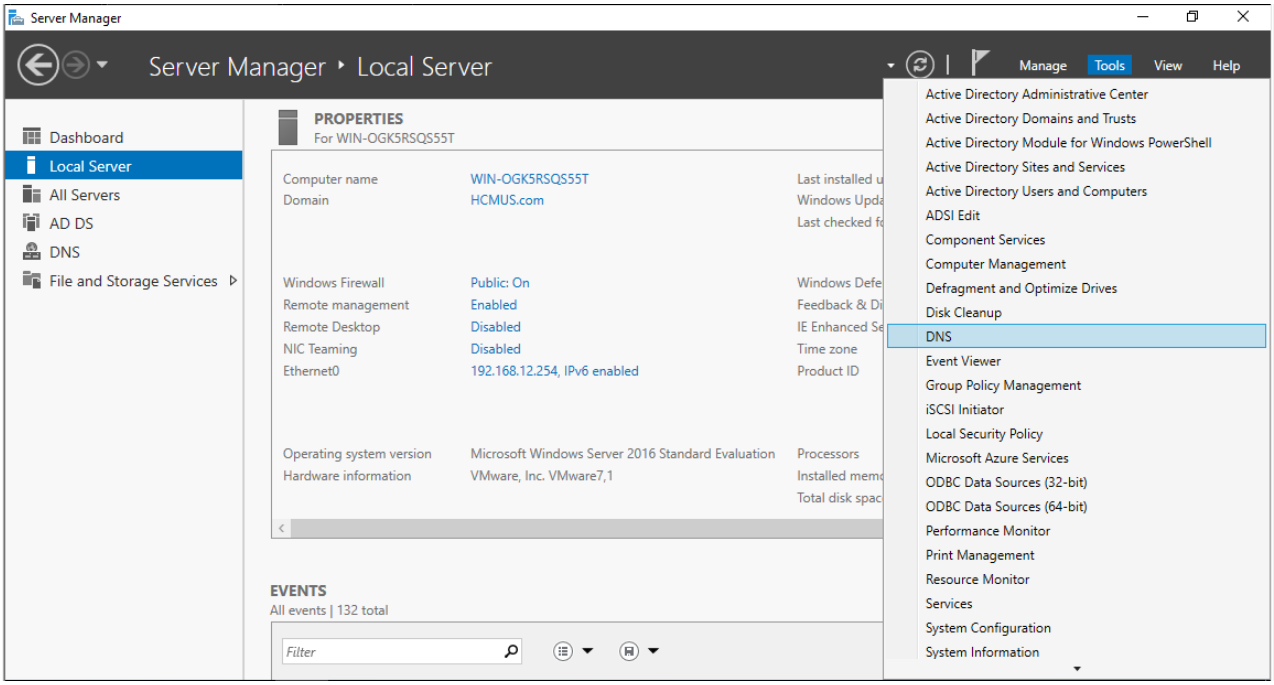


- Ta điền thông tin của Website.
- Tên: **lab05**
- Physical path: **C:\lab05** (vừa tạo ở bước đầu)
- Port: 80
- Type: **http** (để kiểm chứng độ tin cậy sau khi sau khi CA Server cấp Certificate cho Website này)
- Host name: www.lab05.com

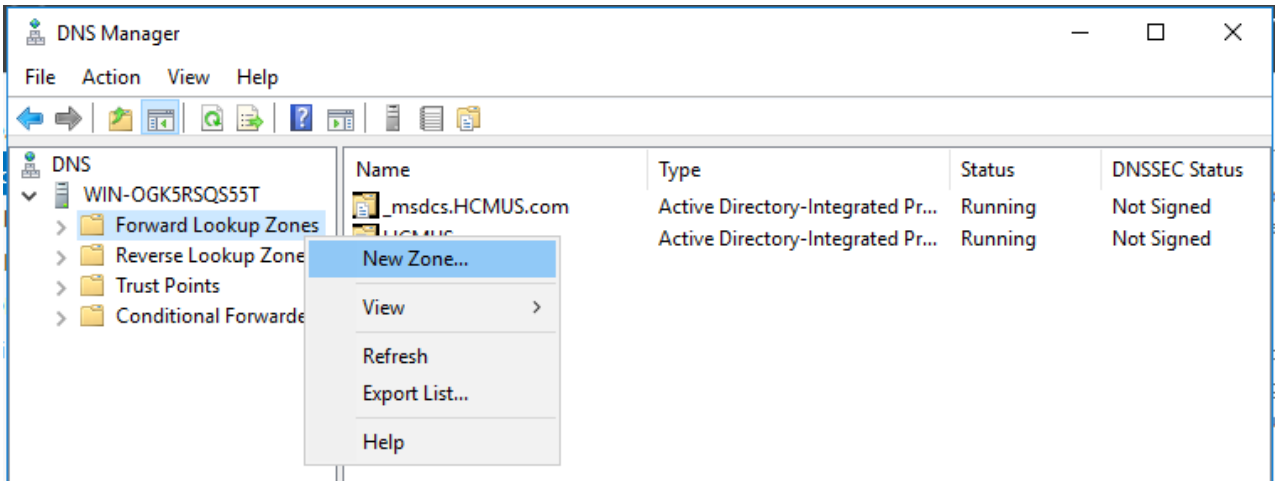


II.3.2. Domain – Controller (CA Server)

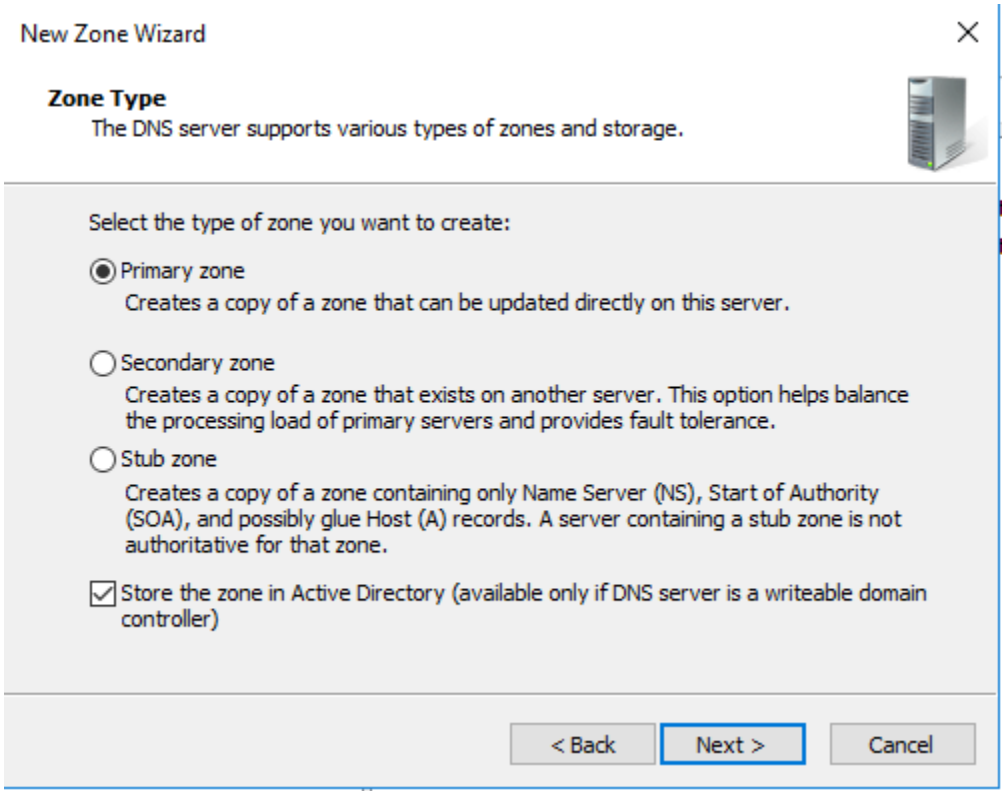
- Ta thực hiện phân giải tên miền của Website vừa tạo trên máy Web – Server
- Vào **Server Manager => Tools => DNS**

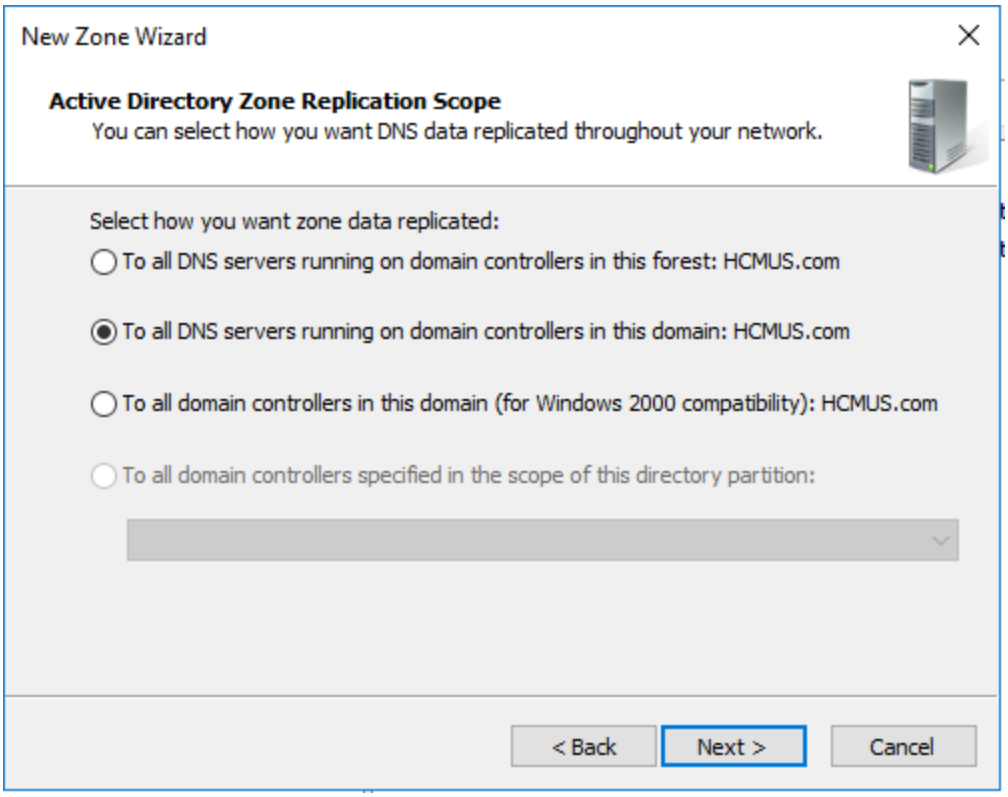


- *Trước tiên, ta tạo phân giải thuận (phân giải tên ra địa chỉ IP)*
- Trong **DNS Manager** chọn **Forward Lookup Zones => New Zone…**

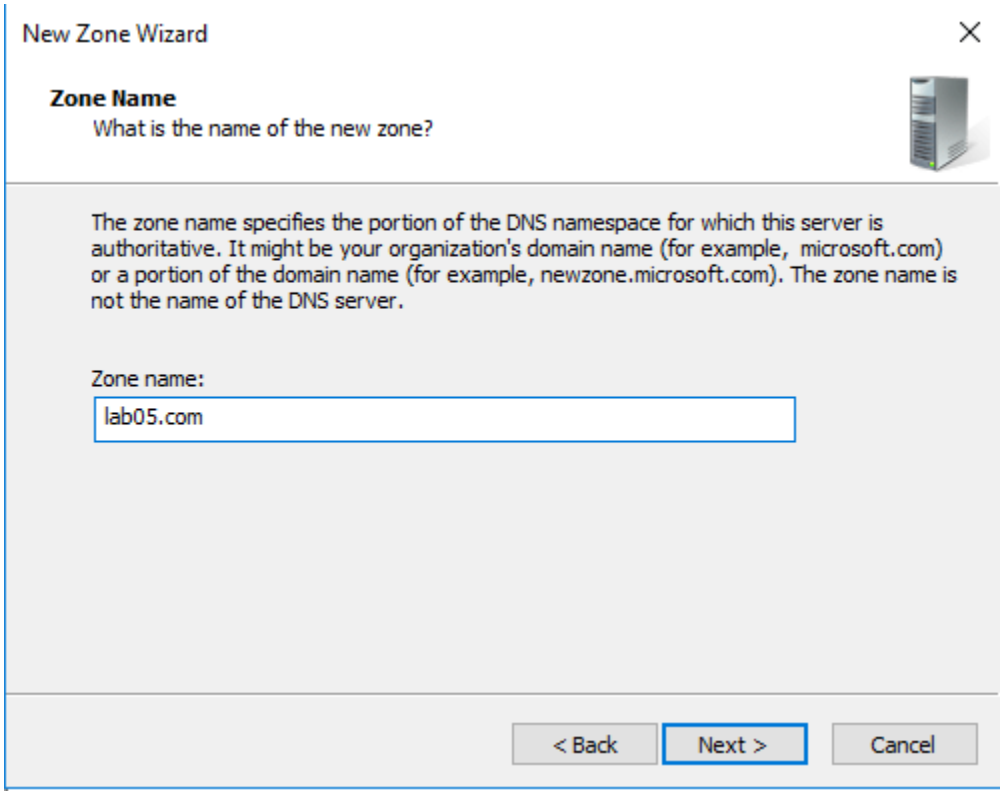


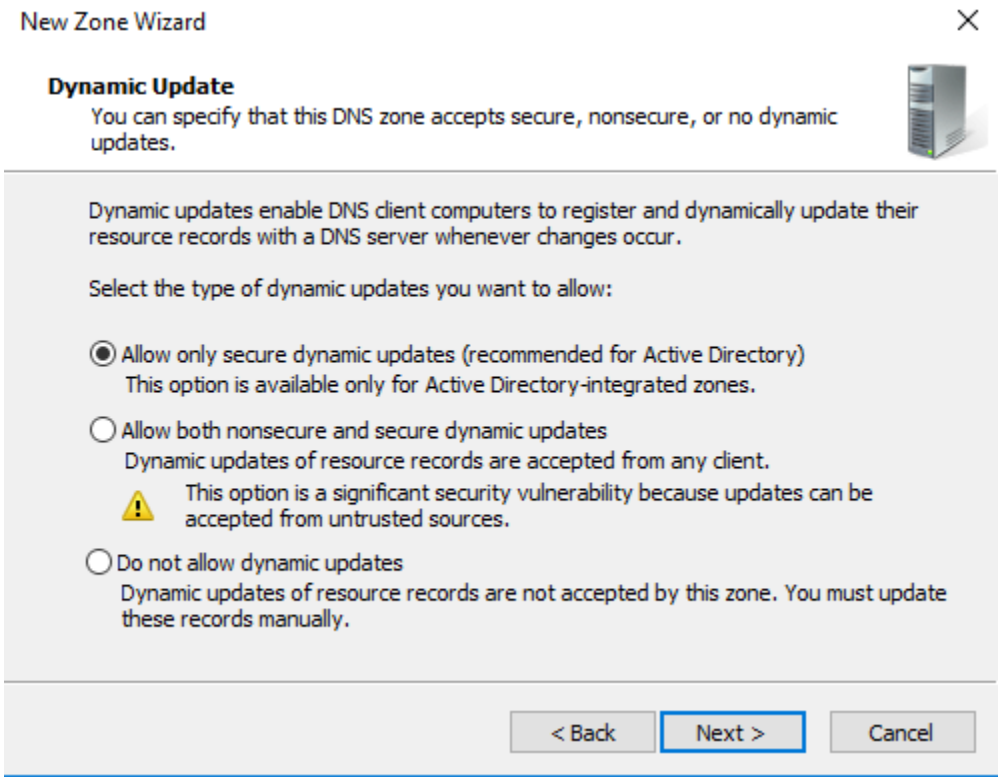
- Các bước tiếp theo, ta chọn next



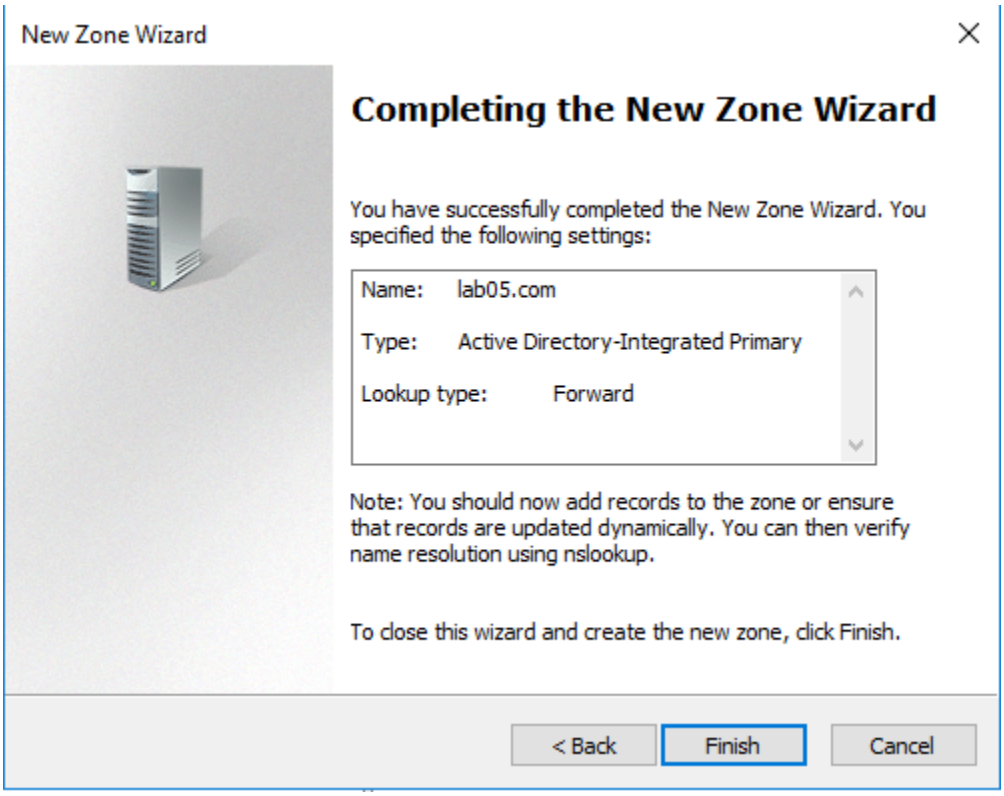


- Mục **Zone Name** ta điền: **lab05.com** (ứng với Website www.lab05.com, mục đích để tạo Alias truy cập có **www** hay không cũng được). Các bước tiếp theo ta chọn next, sử dụng thiết lập mặc định

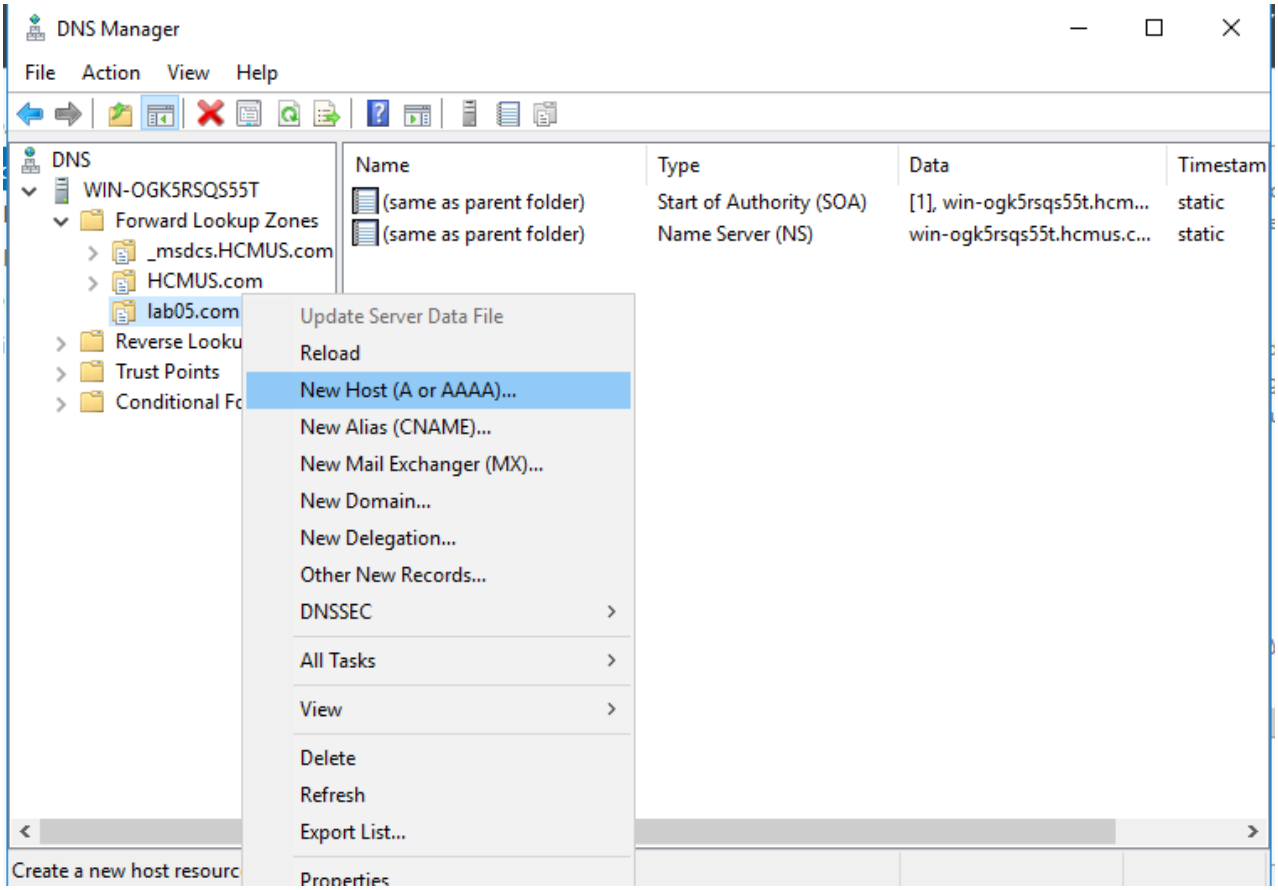

New Zone Wizard
Zone Name
What is the name of the new zone?
The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.
Zone name:
lab05.com
< Back
Next >
Cancel


New Zone Wizard
Dynamic Update
You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.
Select the type of dynamic updates you want to allow:
Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.
Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
This option is a significant security vulnerability because updates can be accepted from untrusted sources.
Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< Back
Next >
Cancel

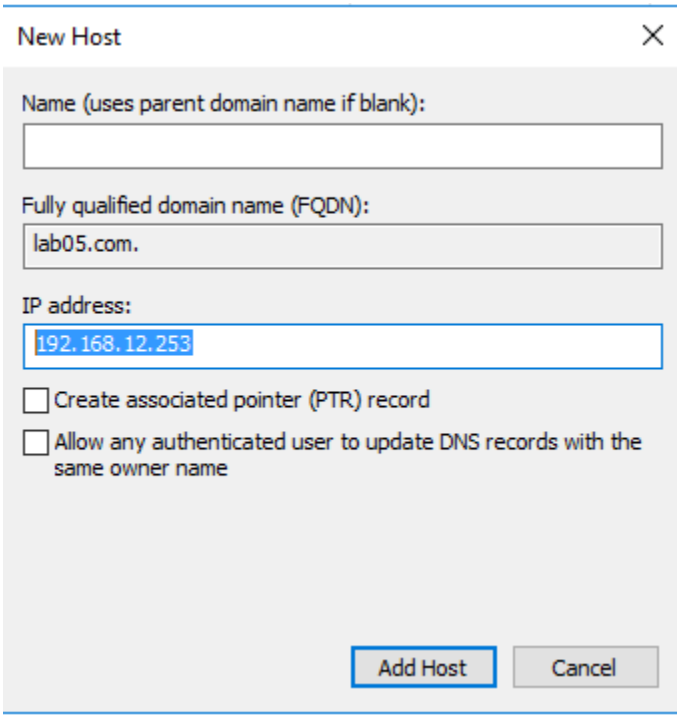
- Thêm một **Zone** mới thành công



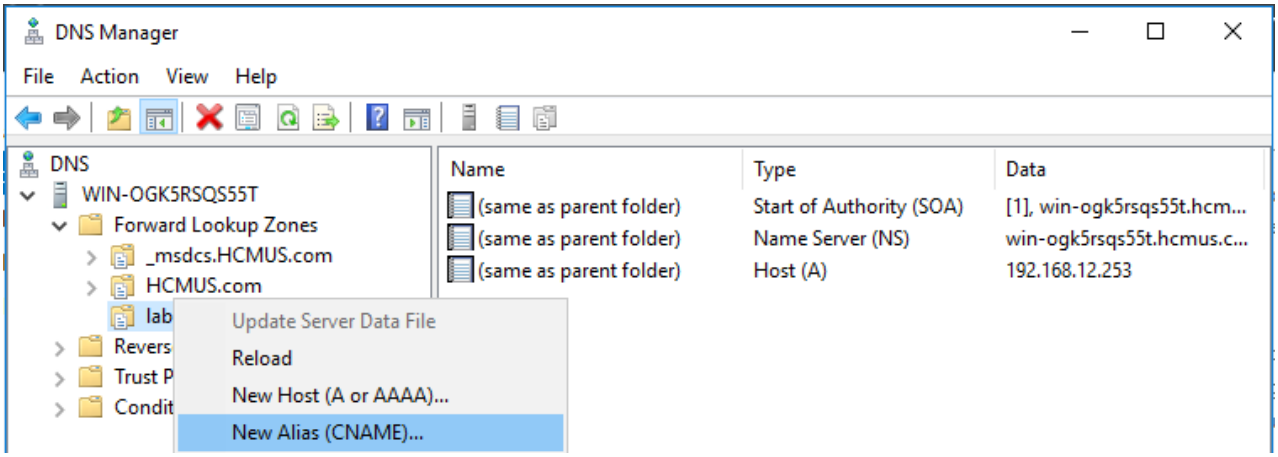
- Ở mục **Zone** vừa tạo (**lab05.com)**, ta chọn **New Host** (tạo một bản record mới, mục đích là để phân giải tên host ra IP tương ứng)



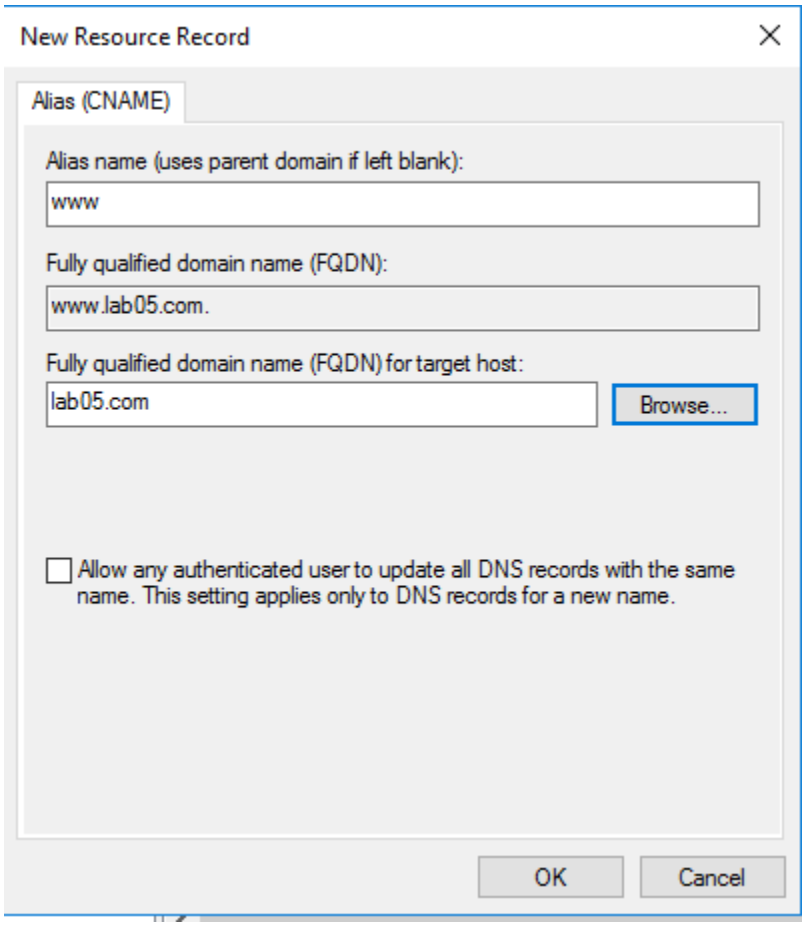
- Ta điền địa chỉ của Web – Server



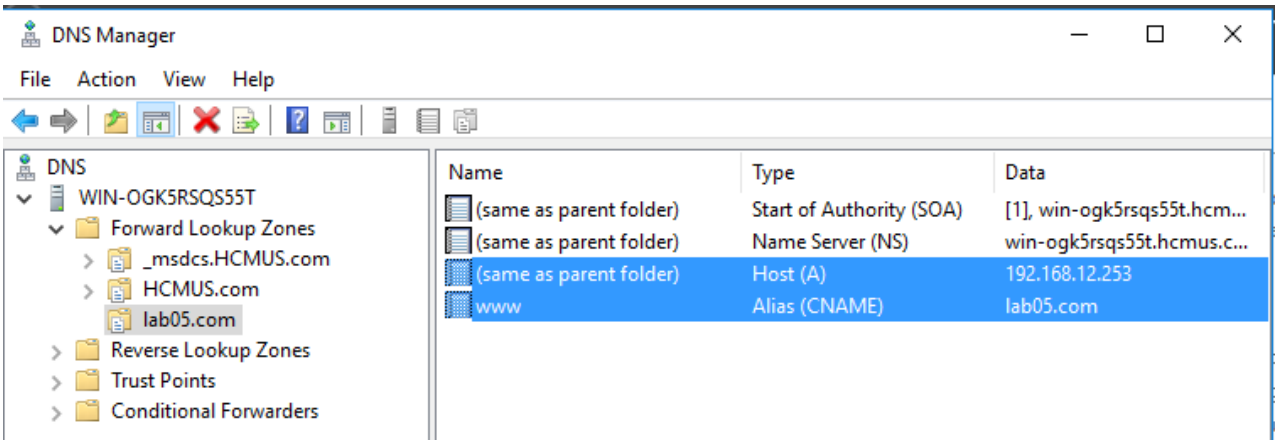
- Ta thêm môt alias để người dùng có thể truy cập mà không cần dùng **www**
- Cũng ở mục **lab05**, ta chọn **New Alias (CName)**



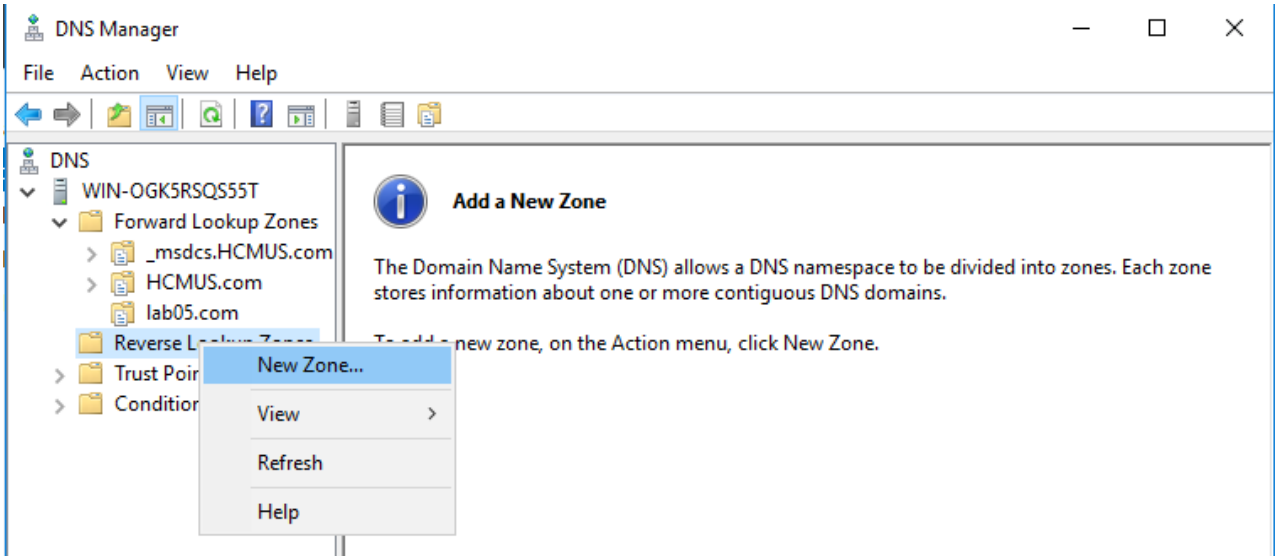
- Mục **Alias** ta điền **www** và **Fully qualified domain name (FQDN) for target host** nhập **lab05.com** tương ứng



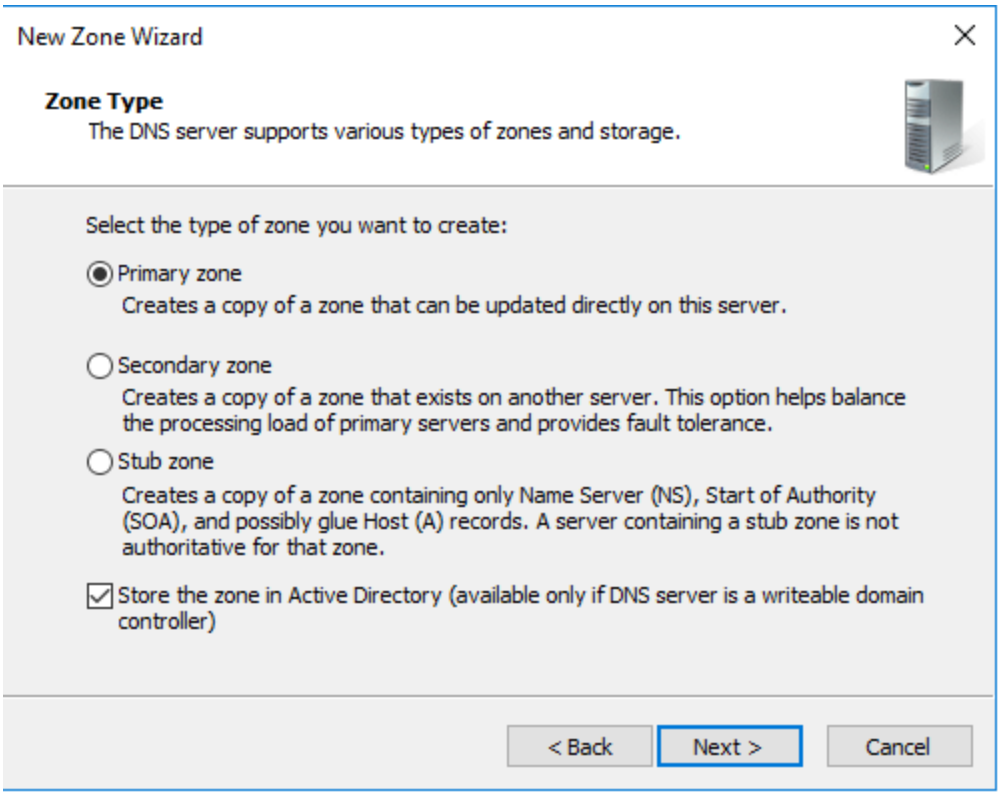
- Thêm host và alias tương ứng thành công

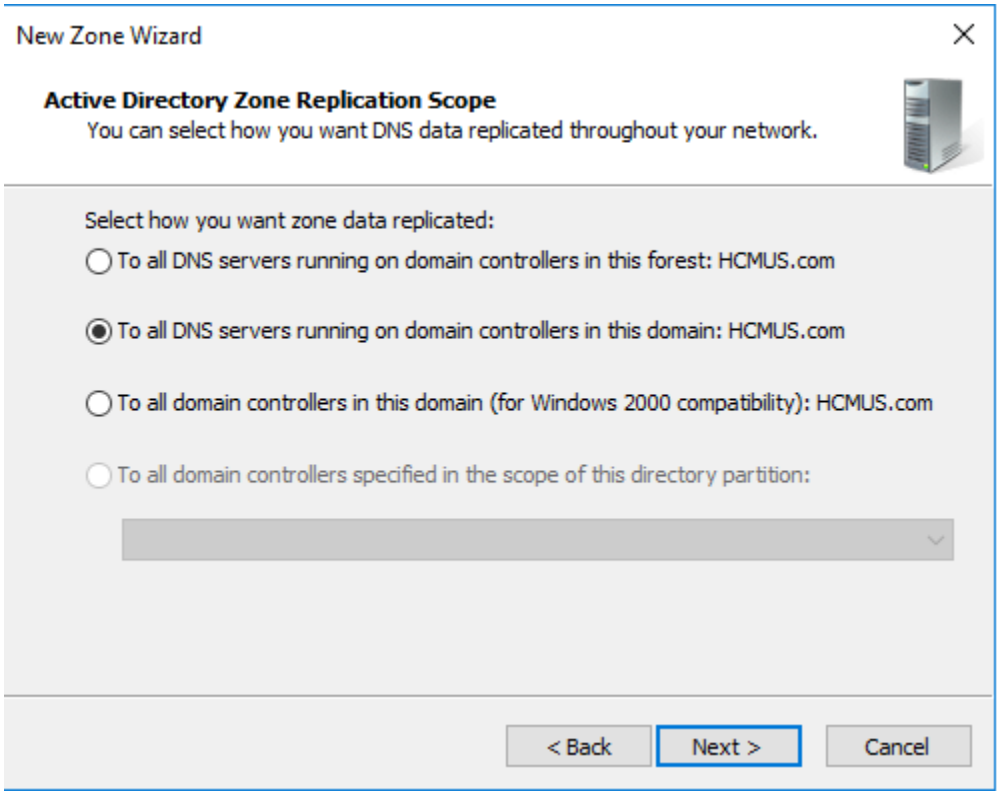


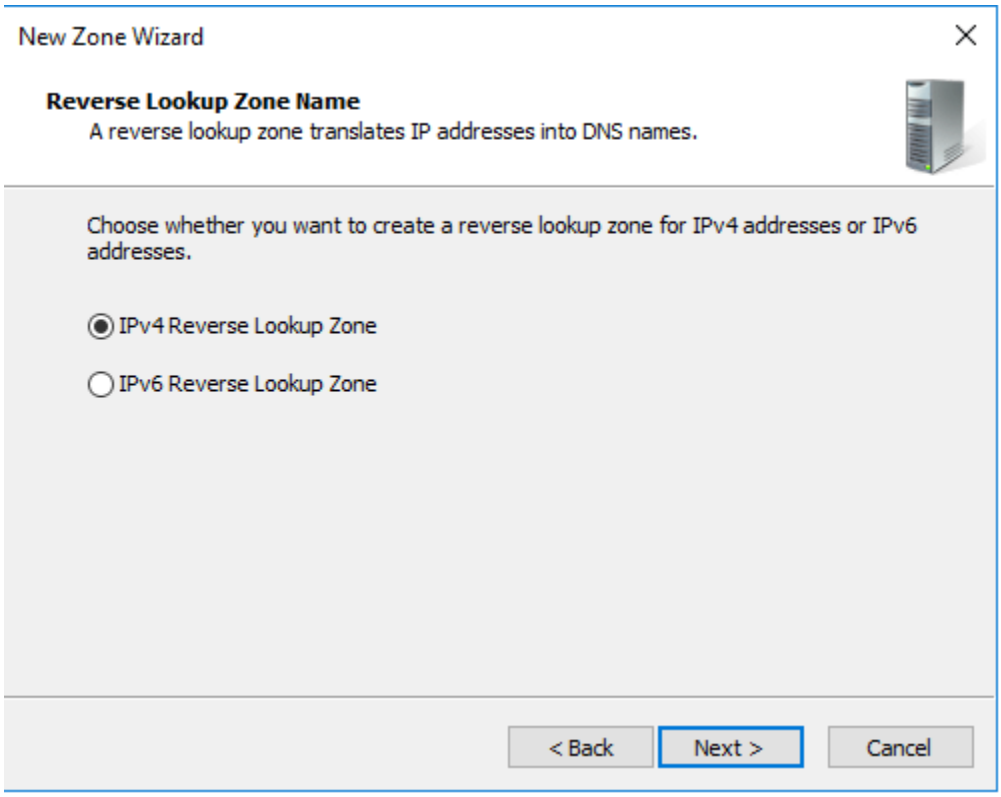
- *Sau đó, ta tạo phân giải nghịch (phân giải địa chỉ IP ra tên)*
- Chọn **Reverse Lookup Zones => New Zone…**



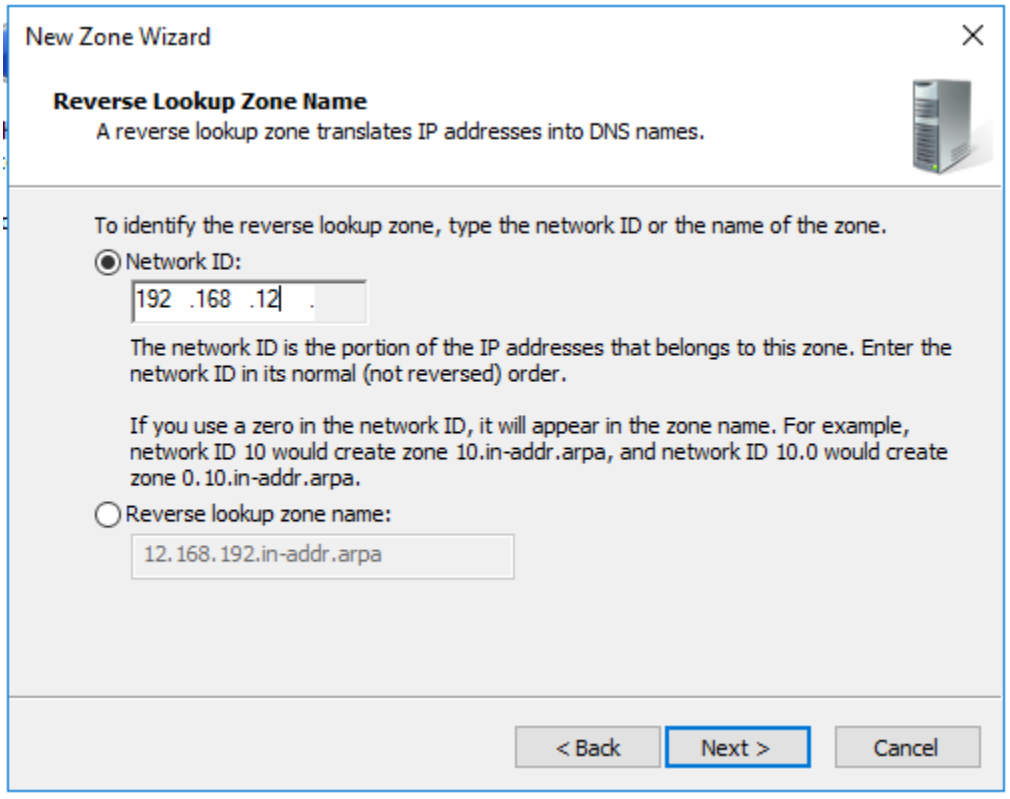
- Các bước tiếp theo, ta chọn next


New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.
Store the zone in Active Directory (available only if DNS server is a writeable domain controller)
< Back
Next >
Cancel

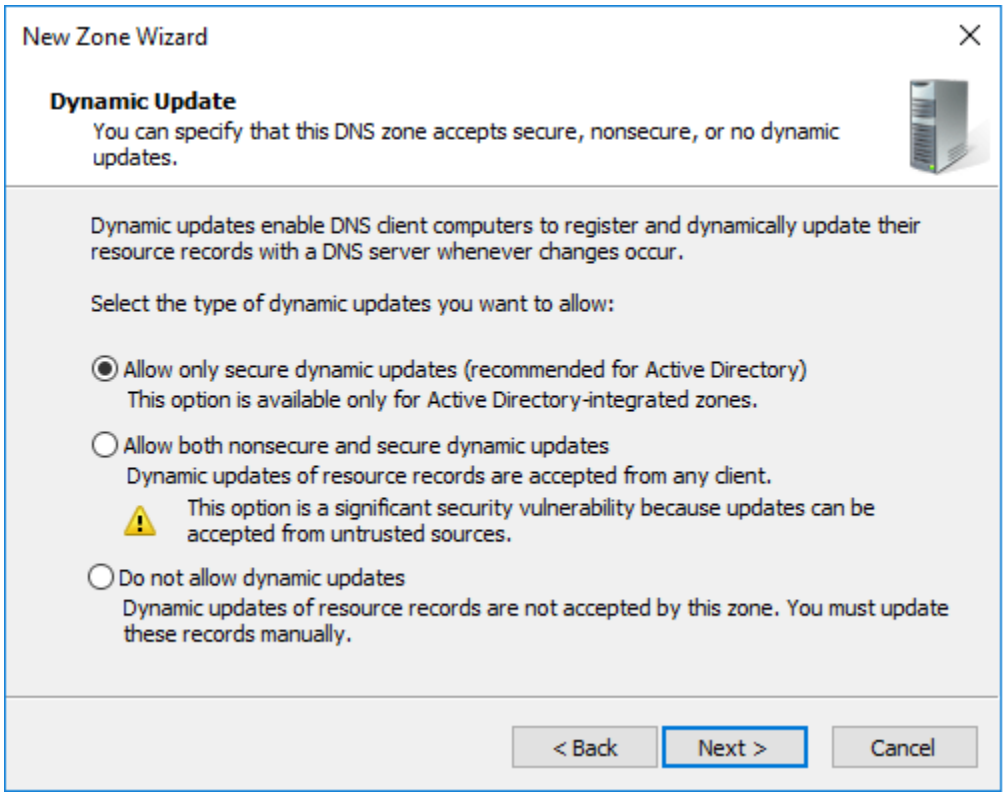

New Zone Wizard
Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.
Select how you want zone data replicated:
To all DNS servers running on domain controllers in this forest: HCMUS.com
To all DNS servers running on domain controllers in this domain: HCMUS.com
To all domain controllers in this domain (for Windows 2000 compatibility): HCMUS.com
To all domain controllers specified in the scope of this directory partition:
< Back
Next >
Cancel



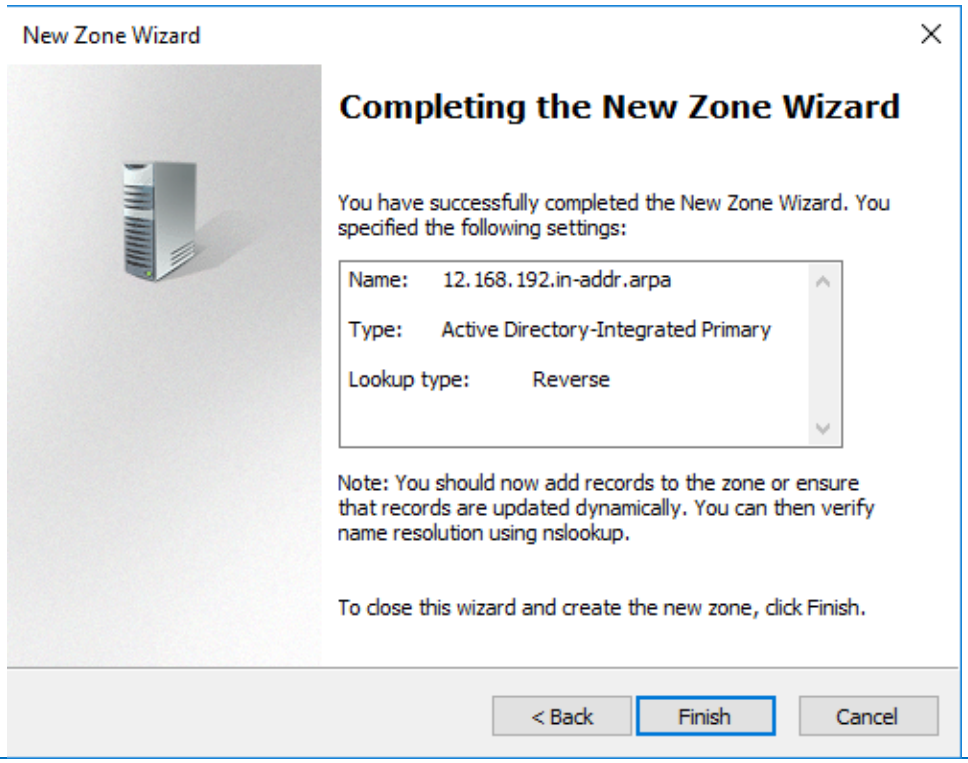
- Ta thêm địa chỉ đường mạng mà các máy cùng thuộc



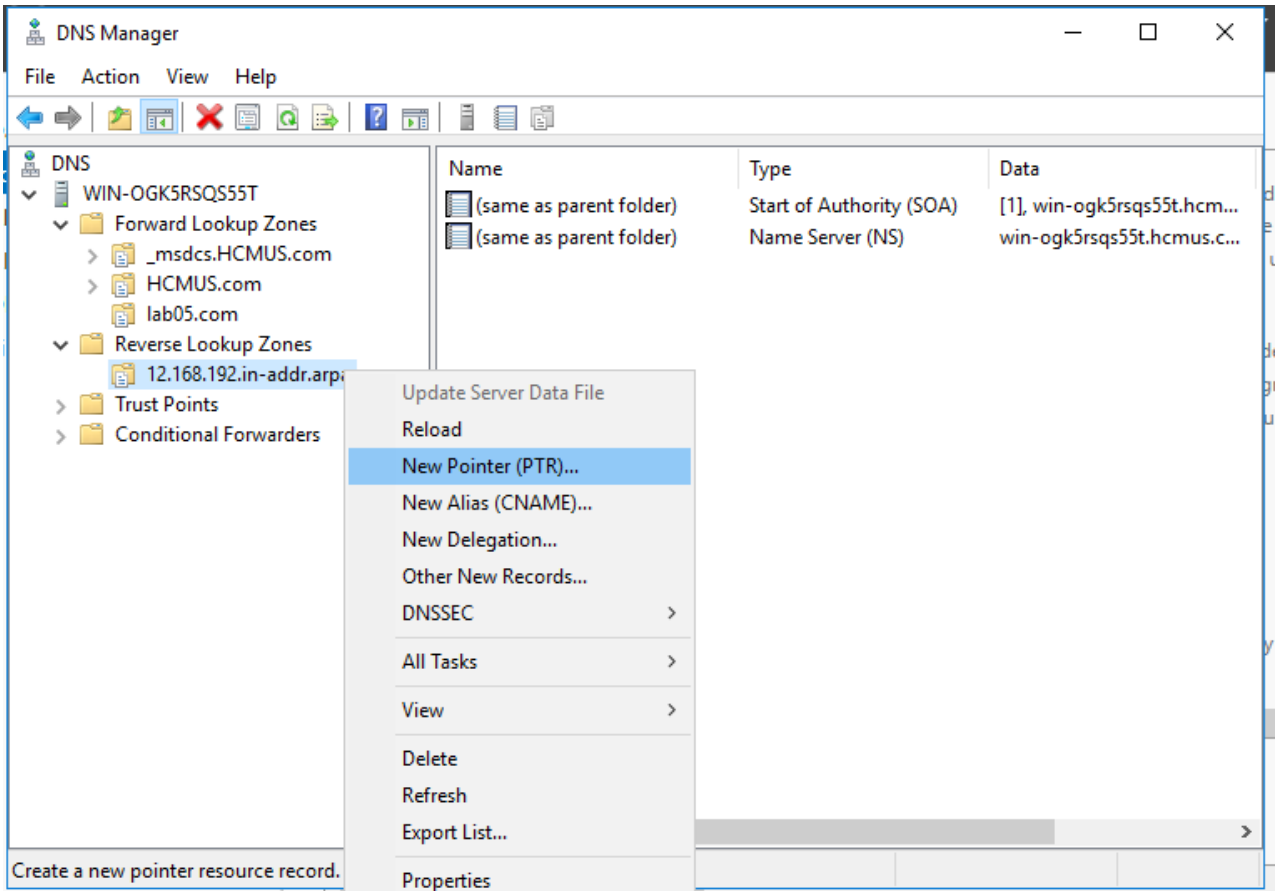
- Các bước tiếp theo, ta chọn next



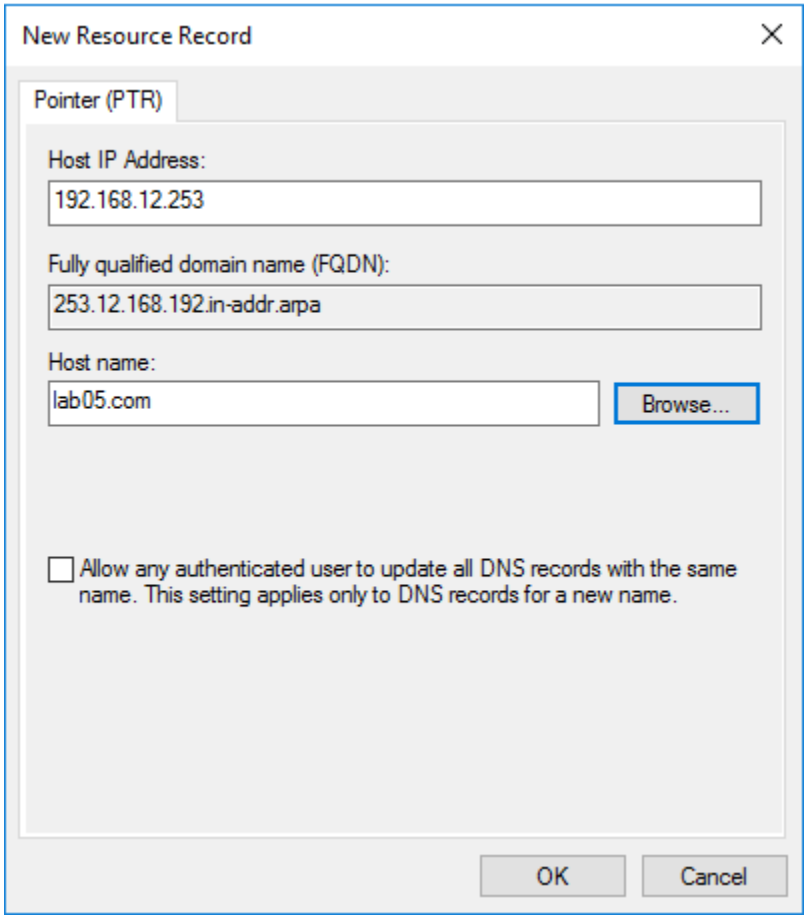
- Thêm một **Zone** mới thành công



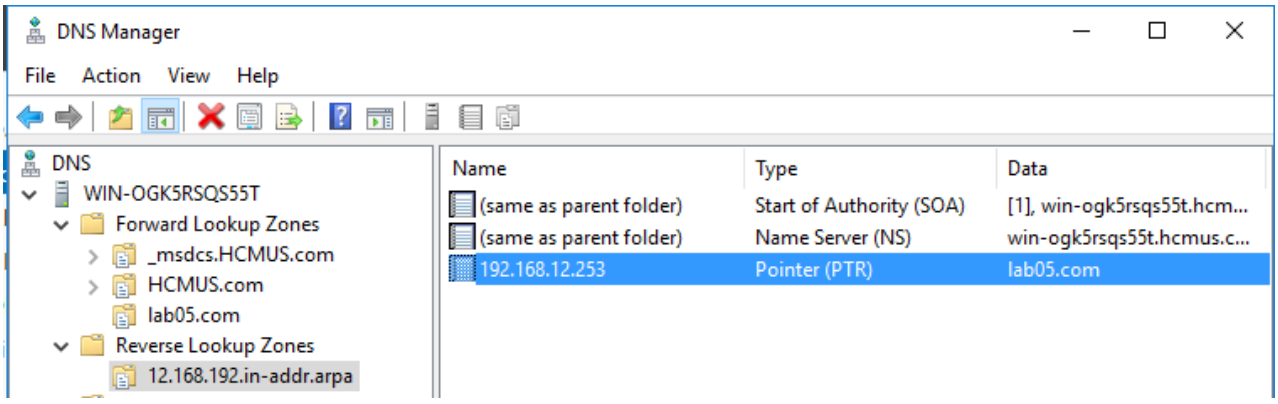
- Ở mục **Zone** vừa tạo (**12.168.192.in-addr.arpa**). Ta chọn **New Pointer (PTR)…** để tạo địa chỉ IP trỏ đến tên host (**lab05.com**) đã tạo ở **Forward Lookup Zones**



- Ta điền địa chỉ IP ứng với Web – Server (chứa Website) và tên miền cần trỏ đến: **lab05.com**

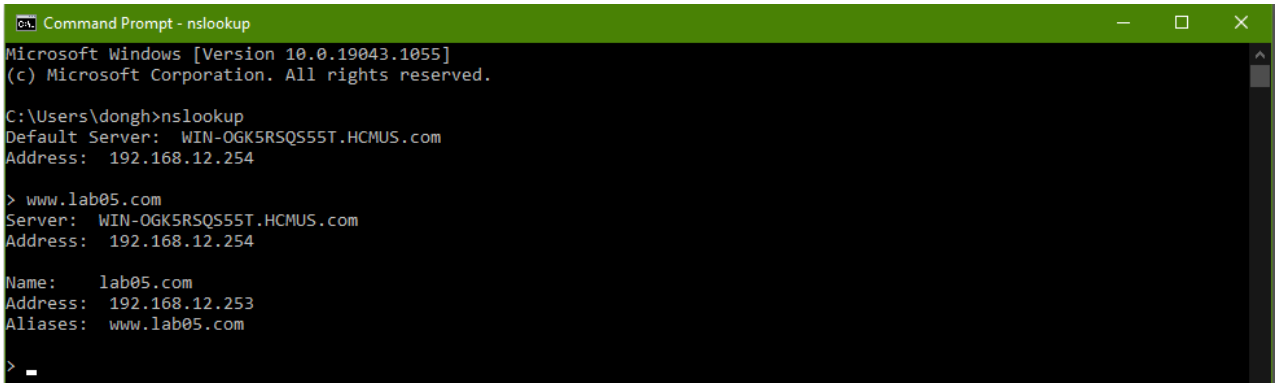


- Thêm pointer mới thành công

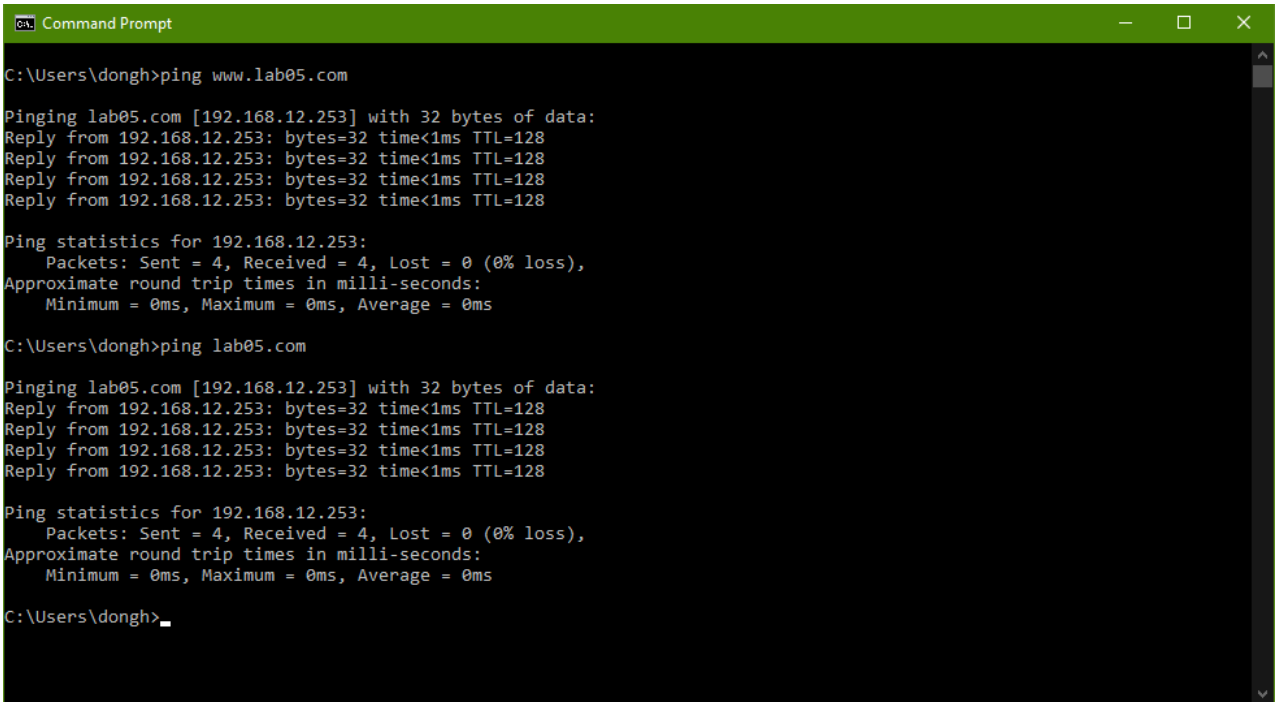


Kiểm tra:

- Từ máy Client (máy thật) ta sử dụng lệnh **nslookup** cho thấy kết quả cài đặt thành công

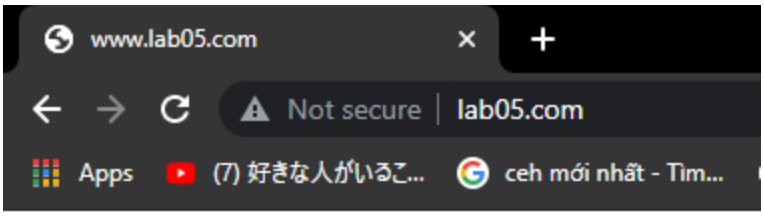


- Ping tên host và alias của nó thành công



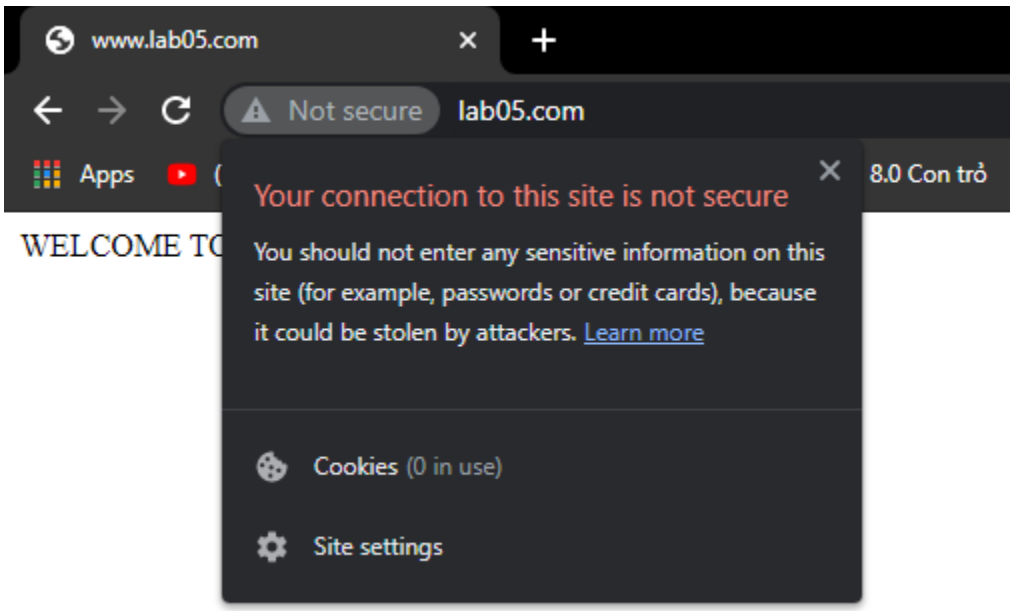
II.3.3. Duyệt web không an toàn

- Để kiểm tra việc cài đặt Website và Domain – Controller ta vào trình duyệt và thực hiện truy đến các tên miền www.lab05.com hoặc lab05.com của Web – Server.
- Cả 2 đều vào được Website



WELCOME TO LAB05

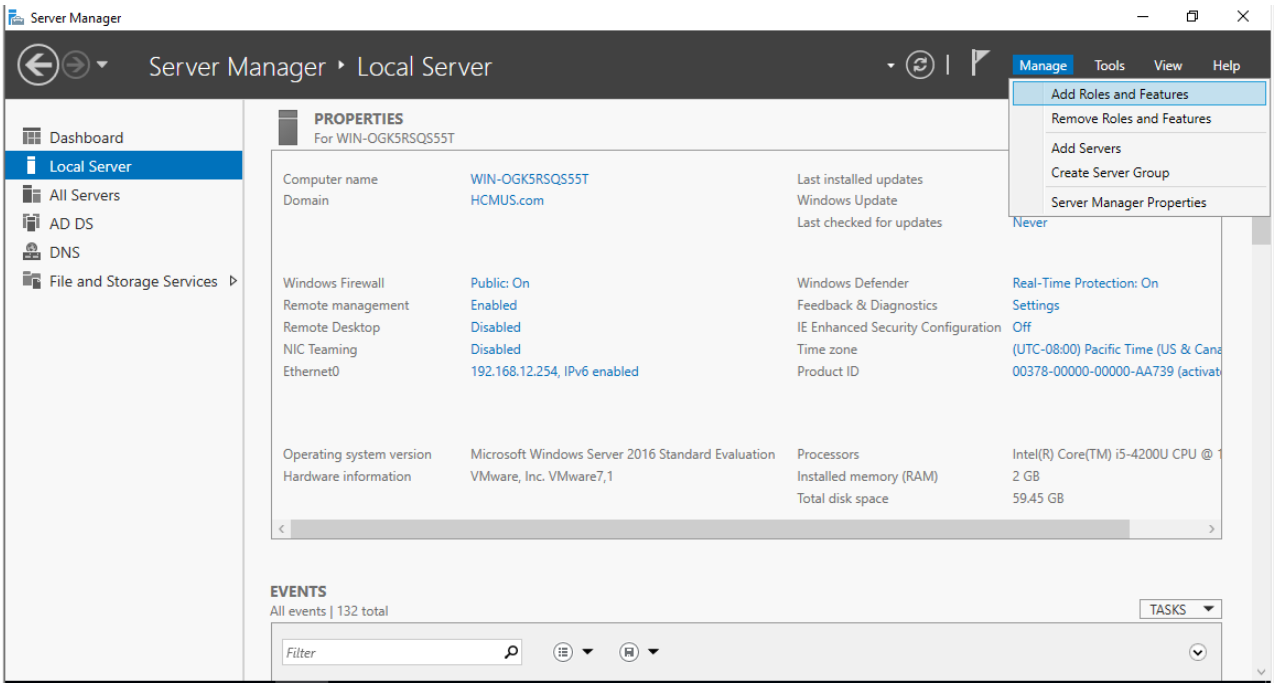
- Nhưng đều báo có vấn đề về bảo mật, do Website đang sử dụng giao thức **http**



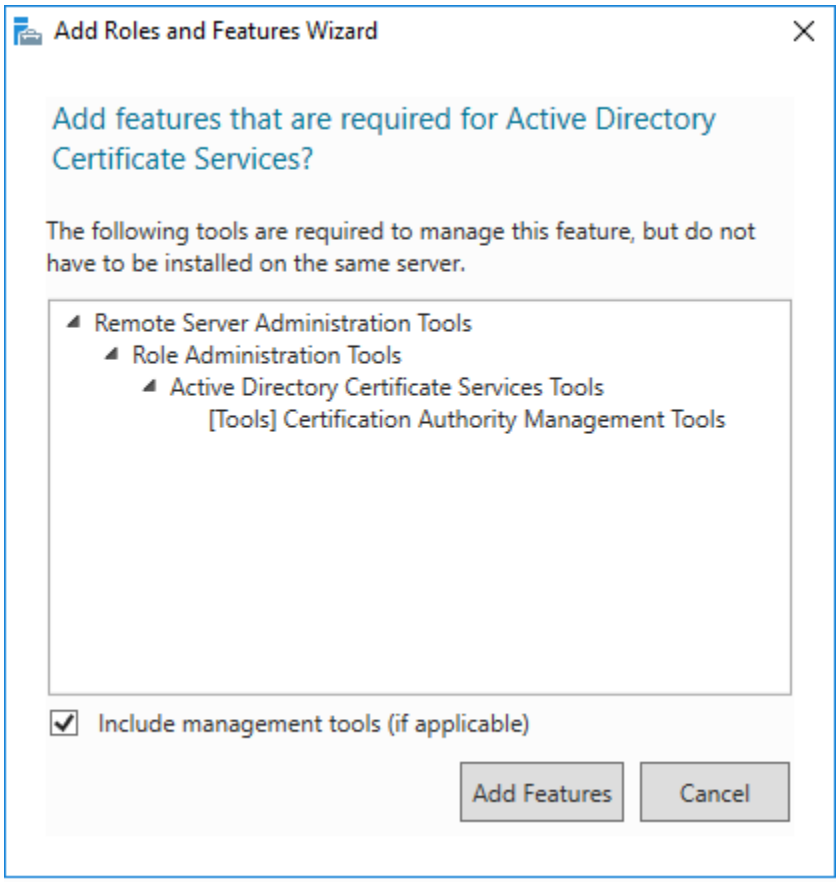
II.4. Tạo CA server cấp Certificate cho máy chủ web server

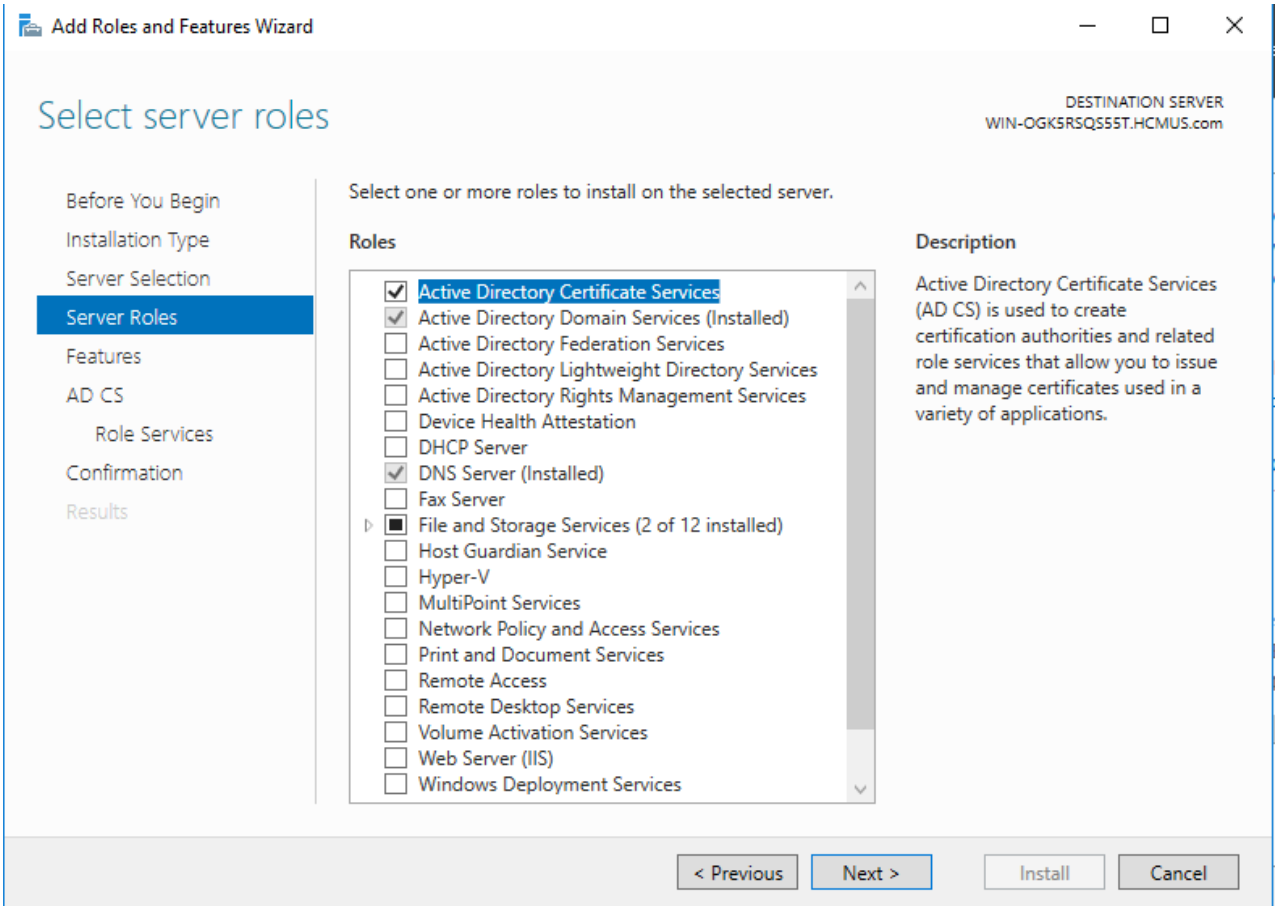
II.4.1. Cài đặt thêm dịch vụ Active Directory Certificate Services trên máy Domain – Controller

- Để Domain – Controller thành CA Server, ta cài thêm dịch vụ **Active Directory Certificate Services**
- Vào **Server Manager => Manage => Add Roles and Features**

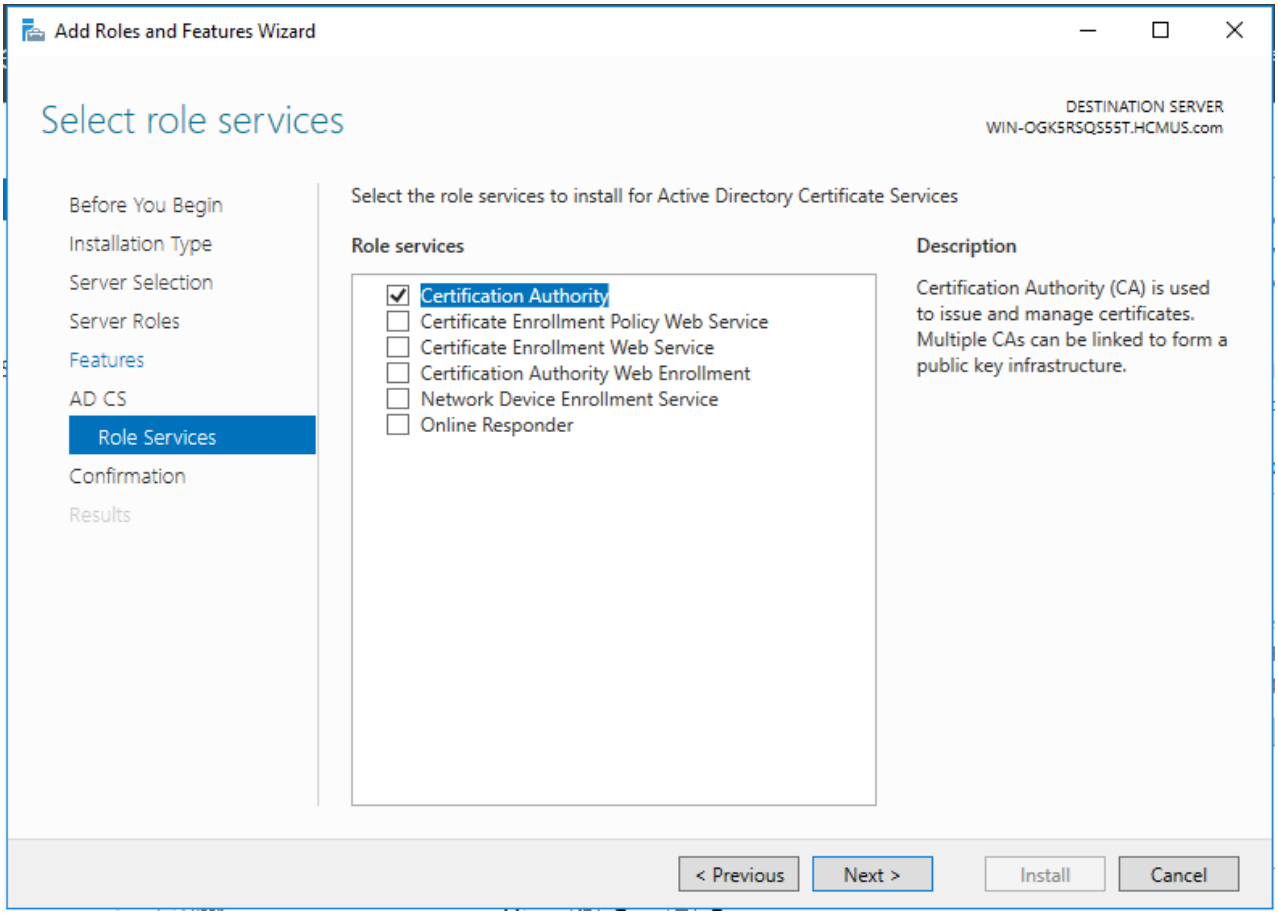


- Các bước thực hiện giống phần cài đặt các dịch vụ. Riêng phần **Server Roles**, ta thêm dịch vụ **Active Directory Certificate Services** và thêm các **Features tương ứng**. Các bước tiếp theo ta chọn next, sử dụng các thiết lập mặc định

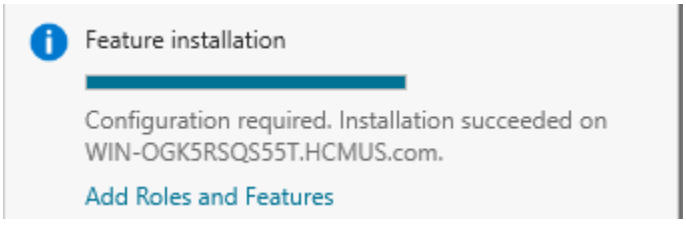



Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WIN-OGK5RSQ55ST.HCMUS.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (2 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
< Previous
Next >
Install
Cancel

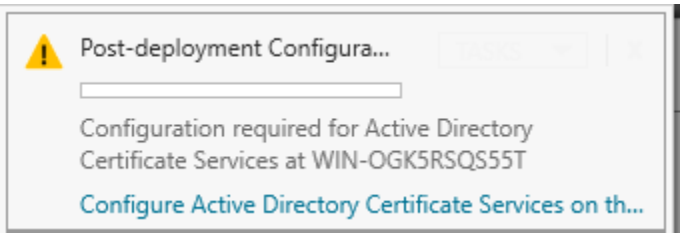
- Ở phần **AD CS => Role Services** ta chọn **Certificate Authority**



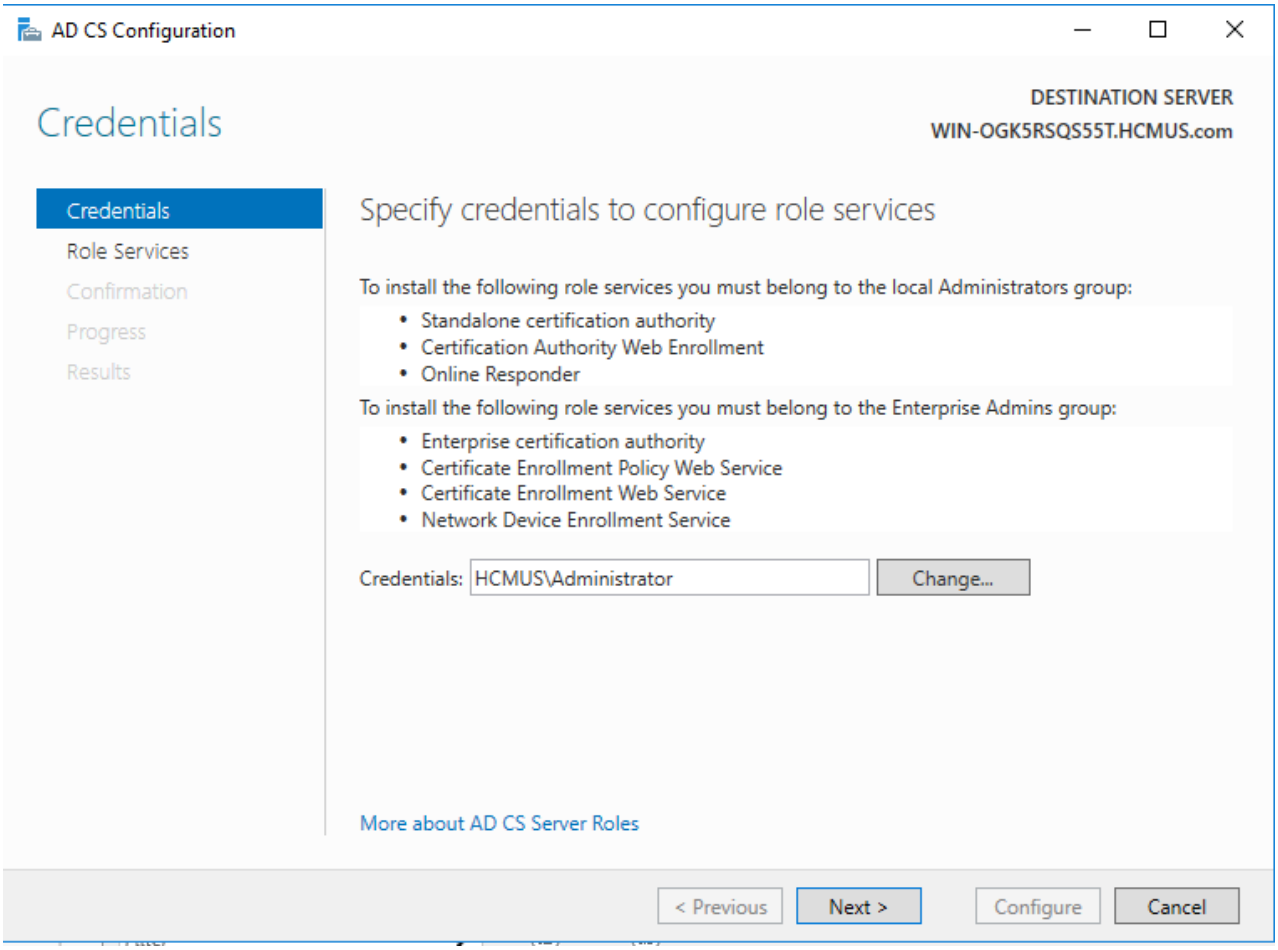
- Sau đó tiến hành cài đặt như ở phần cài đặt các dịch vụ
- Cài đặt thành công



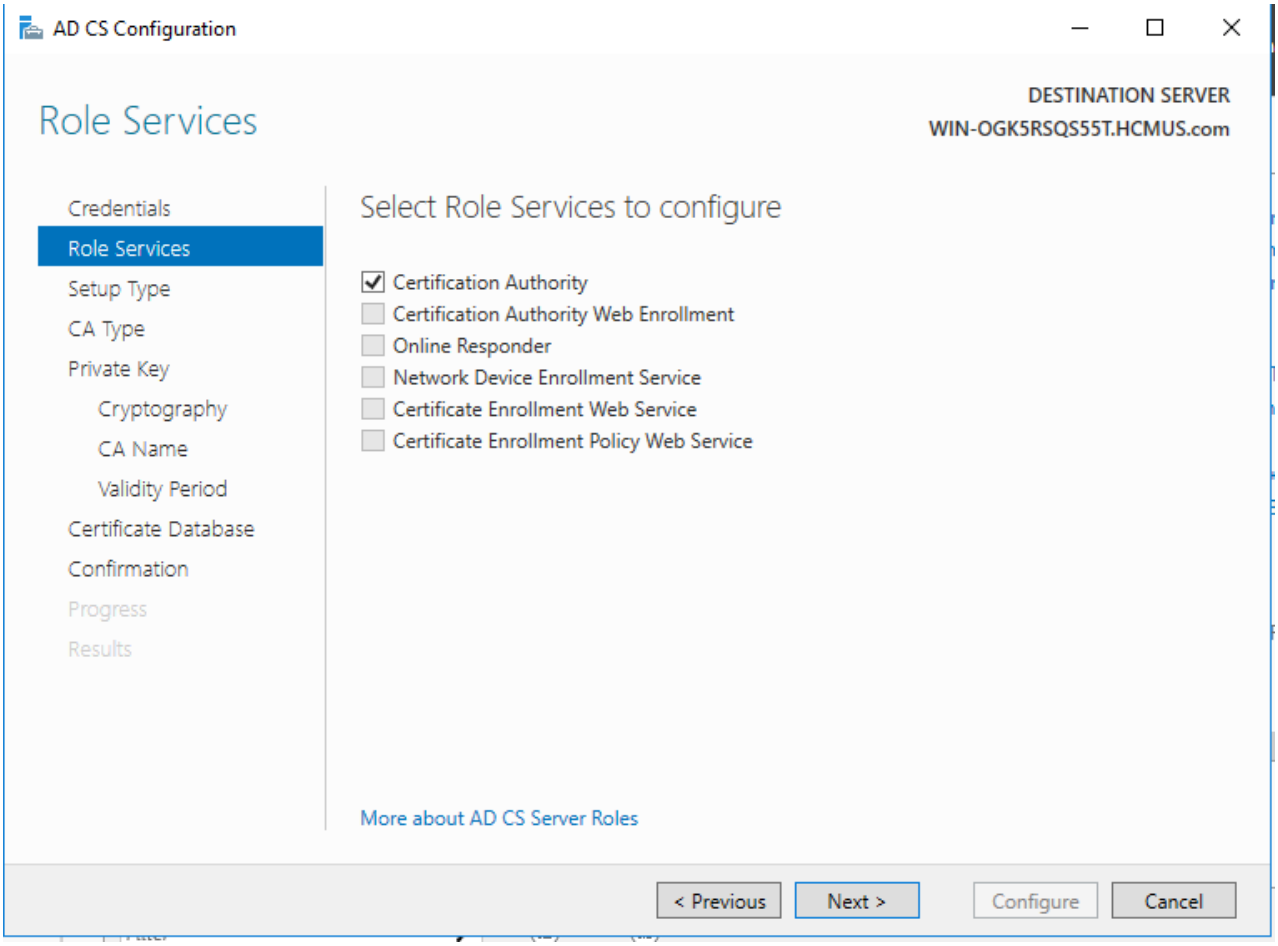
- Sau đó tiến hành thiếp lập CA trên máy Domain – Controller thành CA Server



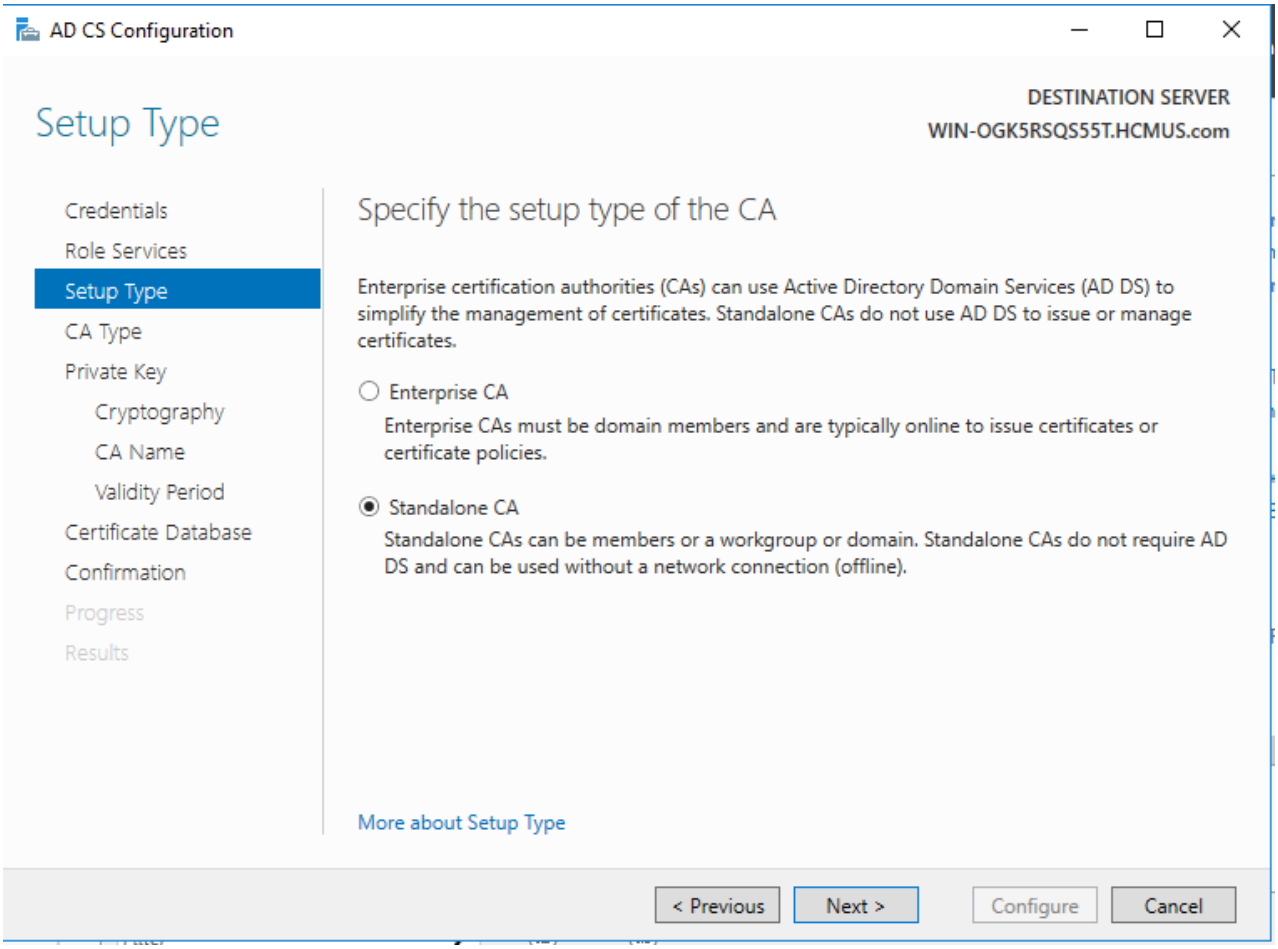
- Ở tab **Credentials** vừa hiện, ta chọn next



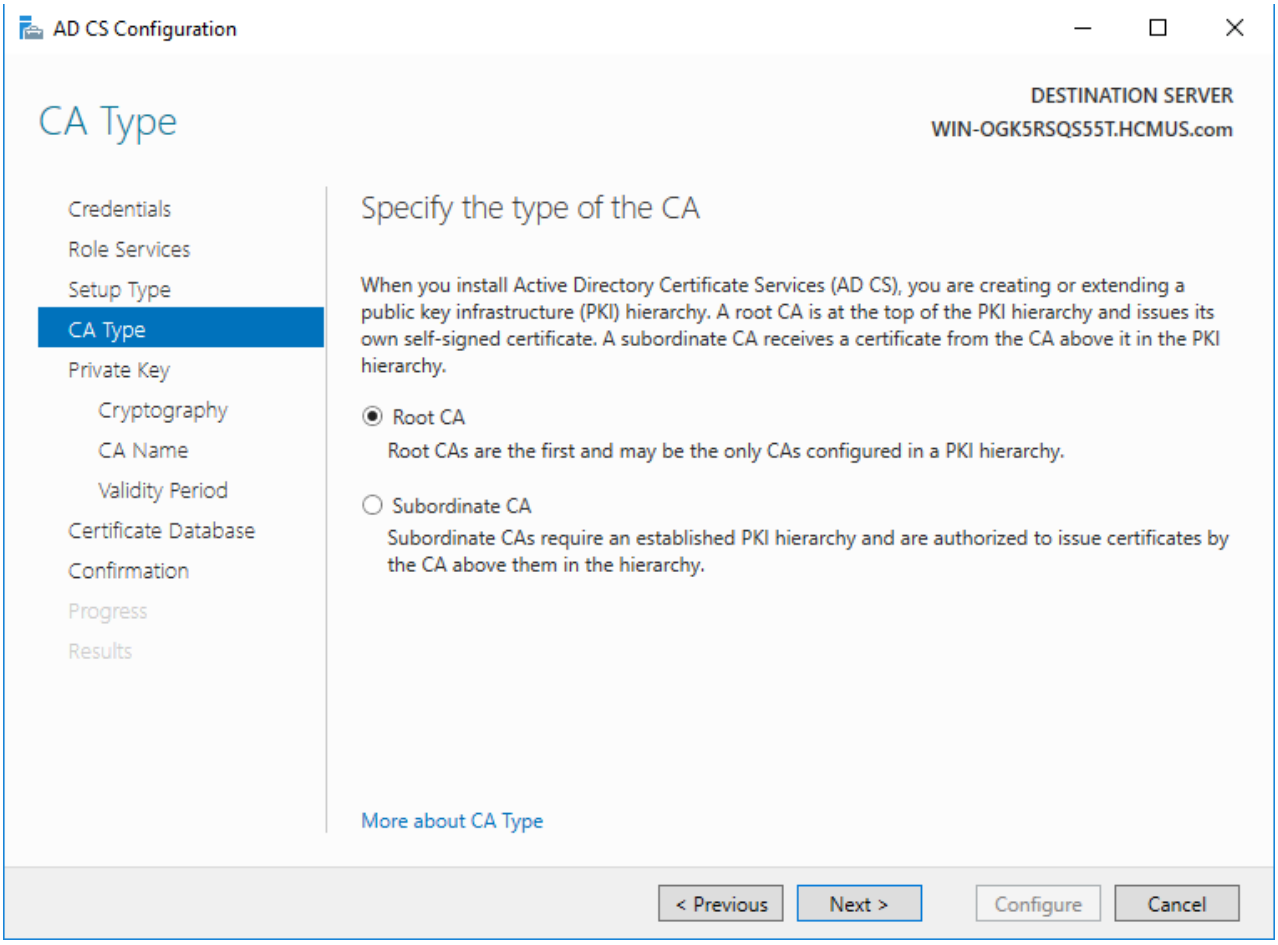
- Phần **Role Services**, ta chọn **Certification Authority**



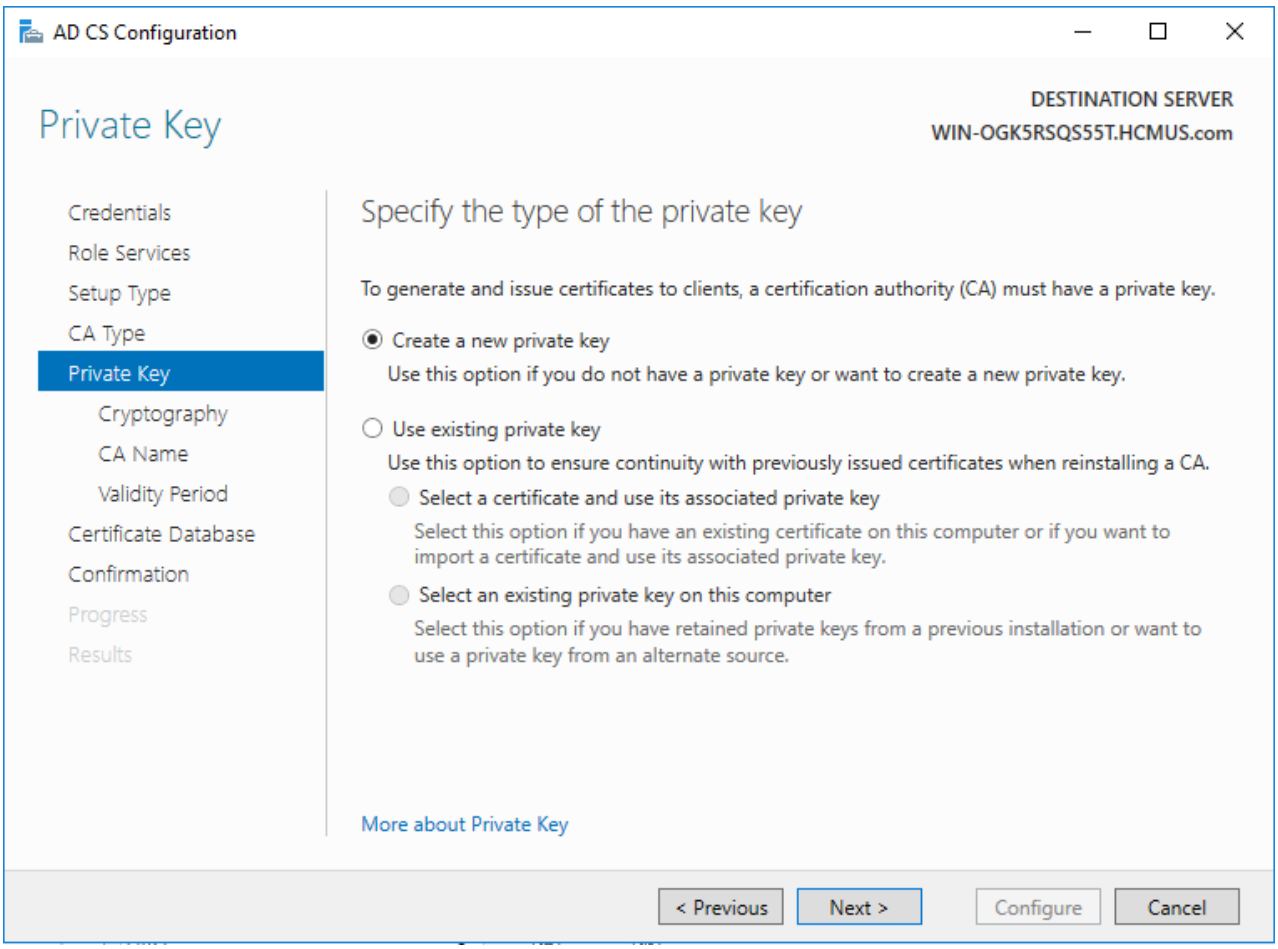
- Ở phần **Sepcify the setup type of the CA**, ta chọn **Standalone CA**



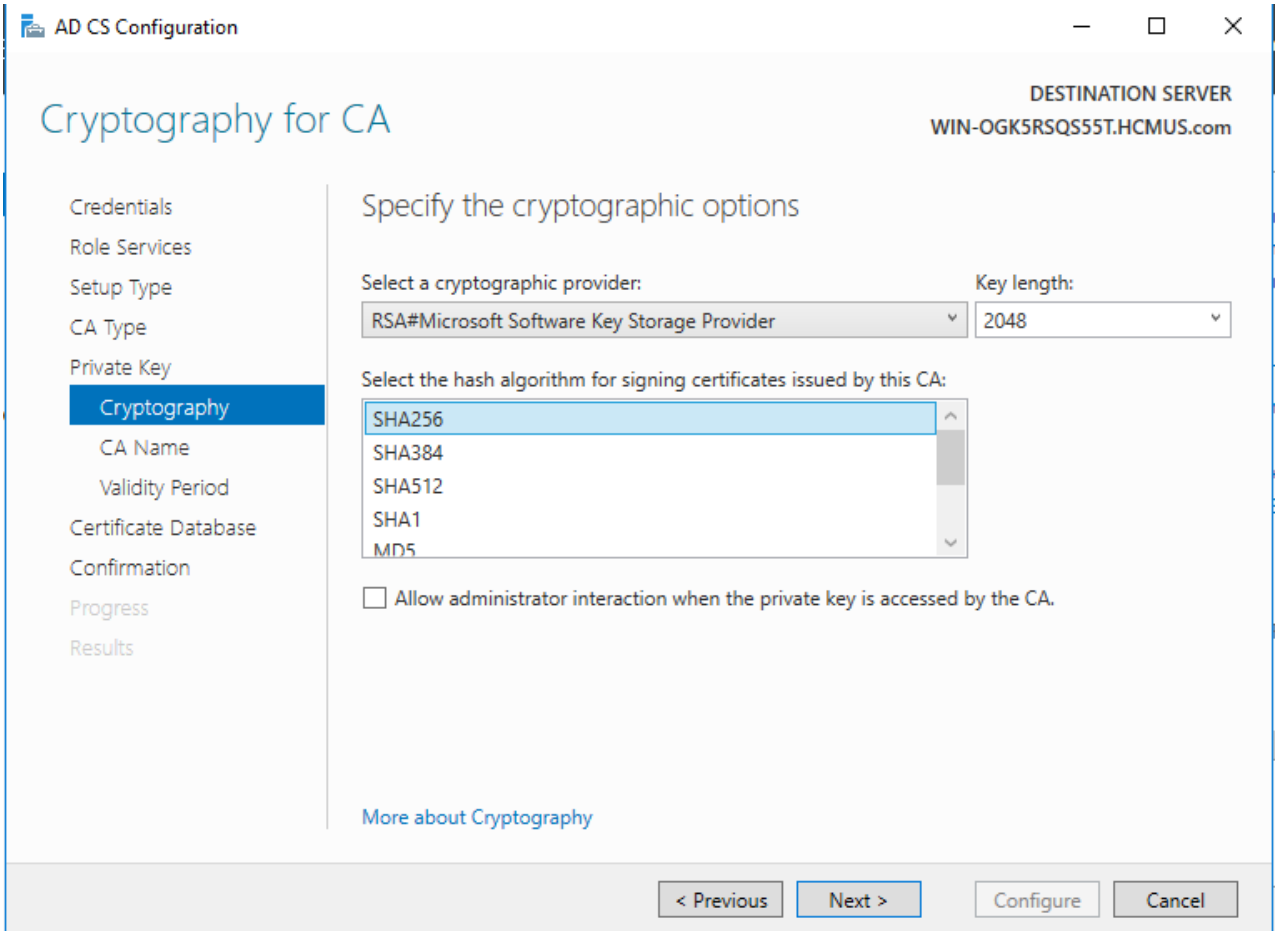
- Các phần tiếp theo, ta chọn next



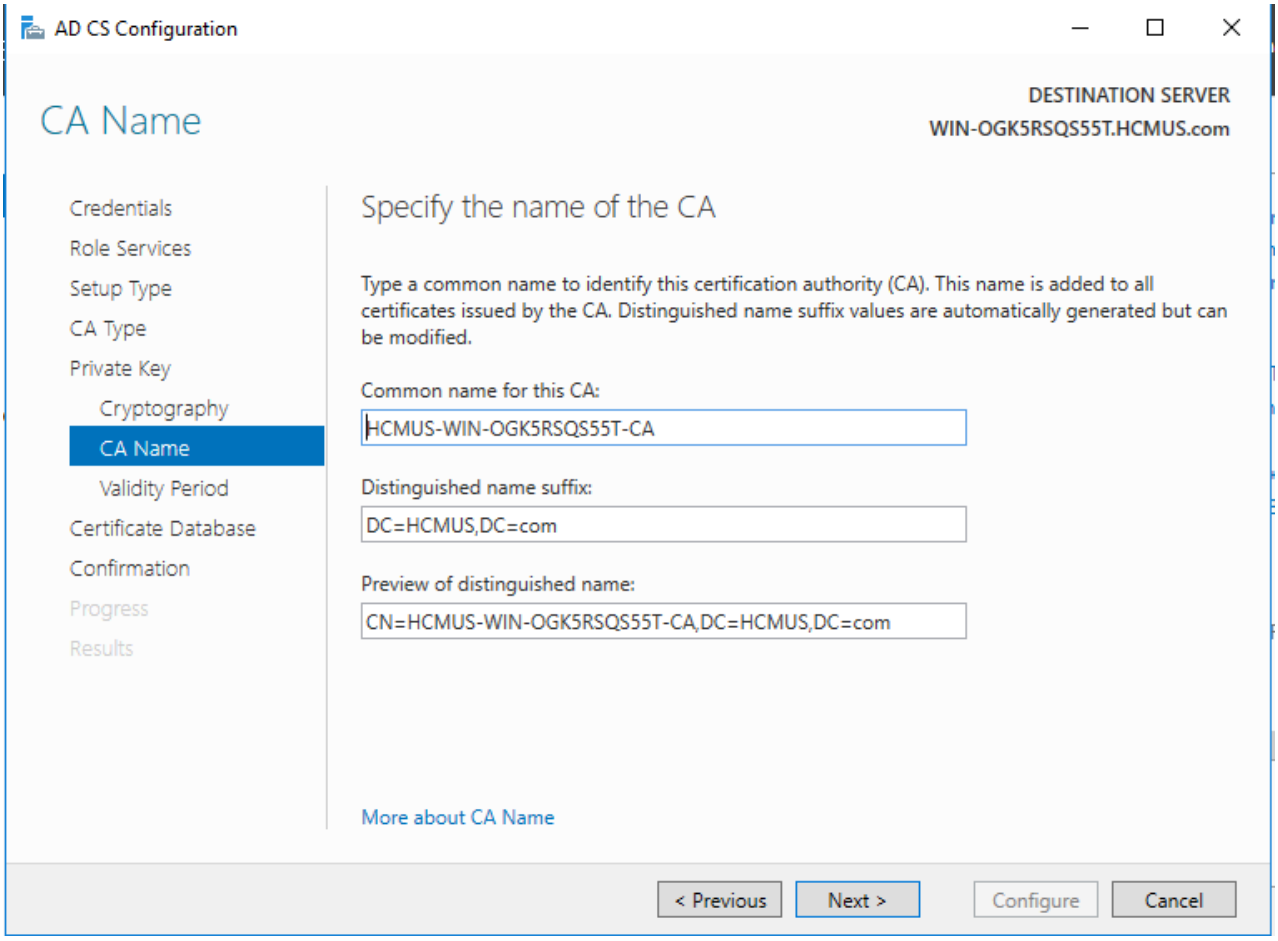
- Vì chưa có key nên ta chọn **Create a new private key**

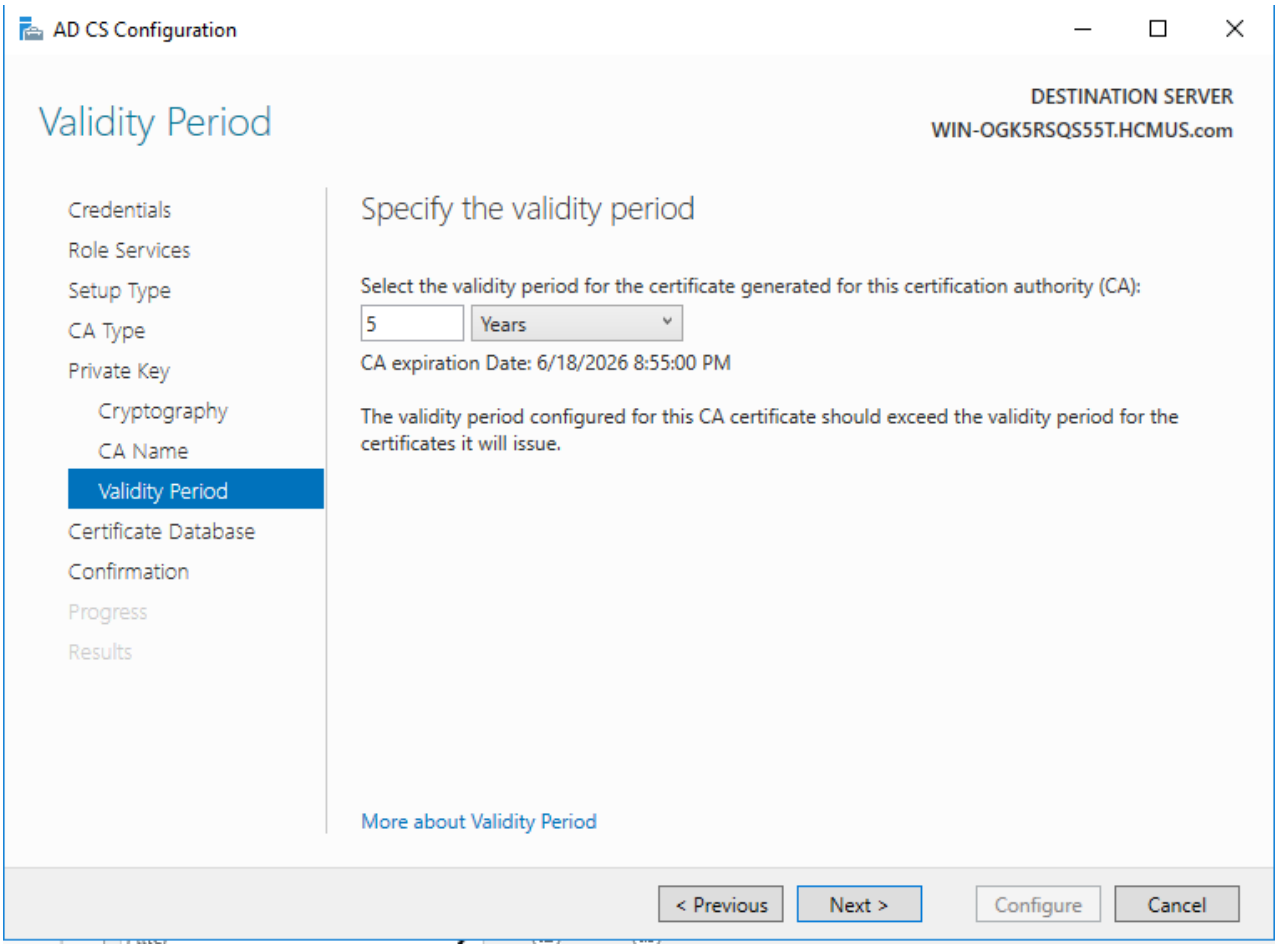


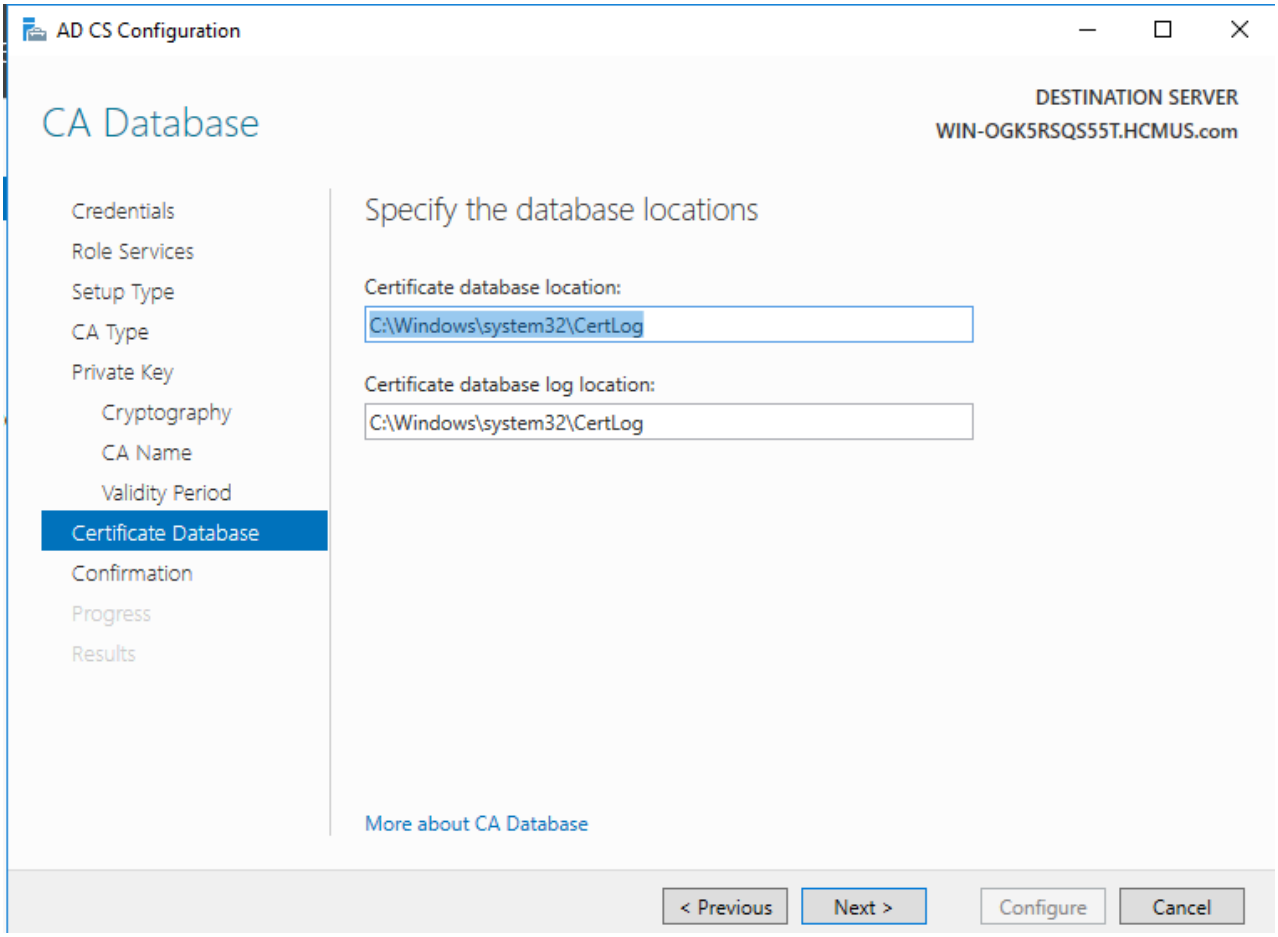
- Chọn nhà cung cấp dịch vụ mã hóa là **RSA#Microsoft Software Key Storage Proivder** – sử dụng thuật toán RSA có độ dài khóa là 2048 bit. Hàm băm được chọn để ký là **SHA256**.



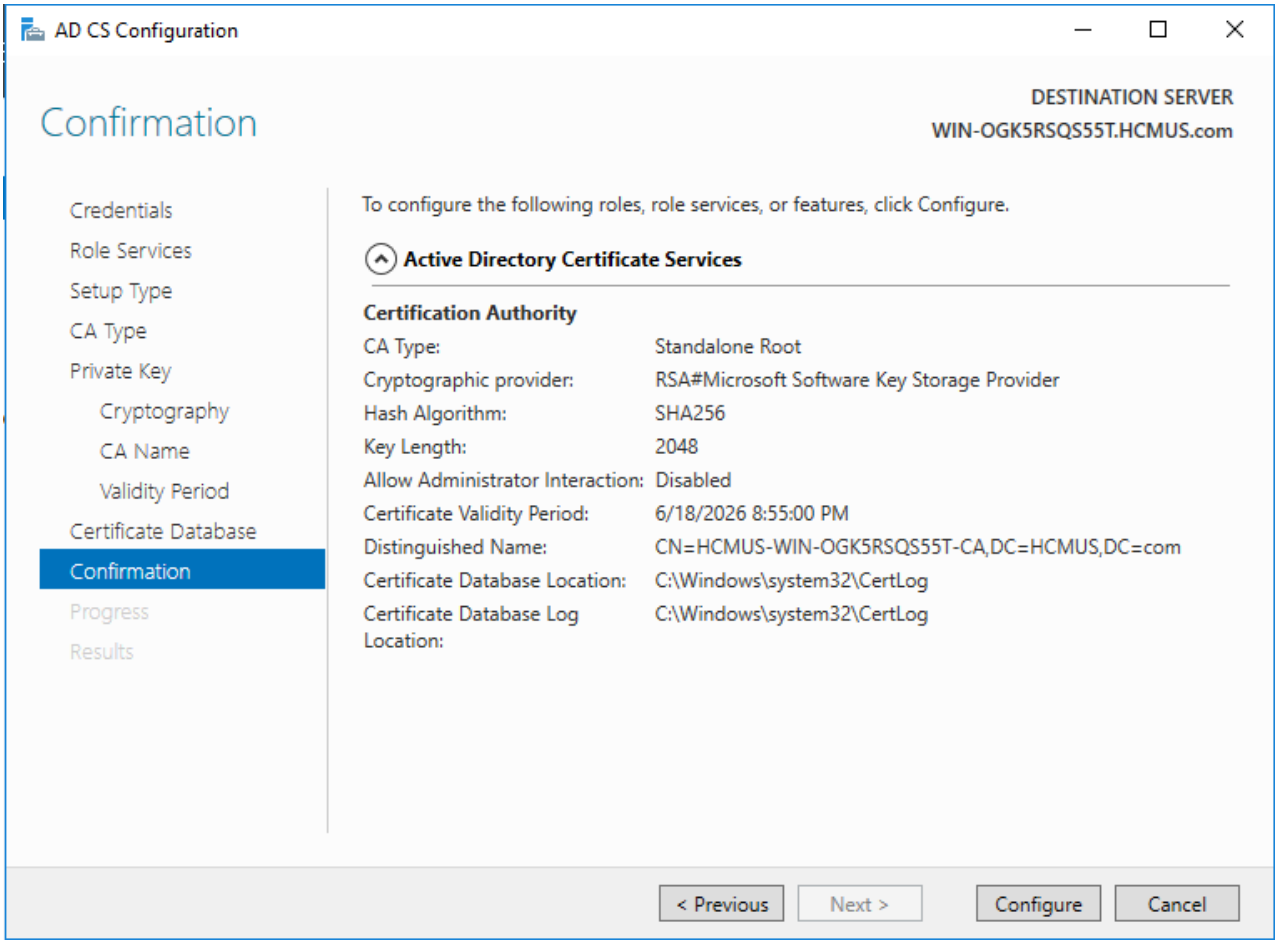
- Các bước tiếp theo ta chọn next, sử dụng thiết lập mặc định



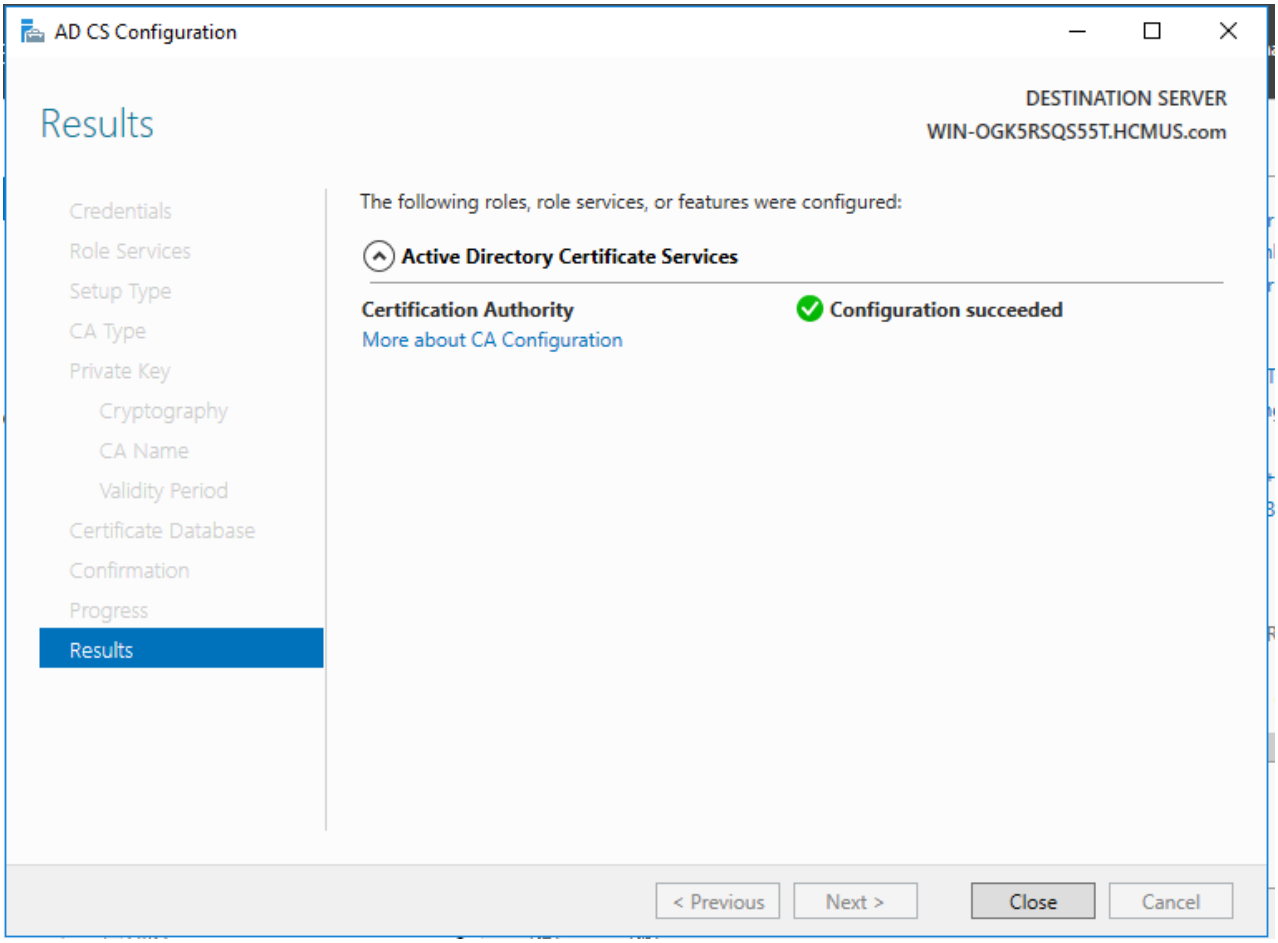

AD CS Configuration
Validity Period
DESTINATION SERVER
WIN-OGK5RSQS55T.HCMUS.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the validity period
Select the validity period for the certificate generated for this certification authority (CA):
5
Years
CA expiration Date: 6/18/2026 8:55:00 PM
The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.
More about Validity Period
< Previous
Next >
Configure
Cancel


AD CS Configuration
CA Database
DESTINATION SERVER
WIN-OGK5RSQS55T.HCMUS.com
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
Specify the database locations
Certificate database location:
C:\Windows\system32\CertLog
Certificate database log location:
C:\Windows\system32\CertLog
More about CA Database
< Previous
Next >
Configure
Cancel

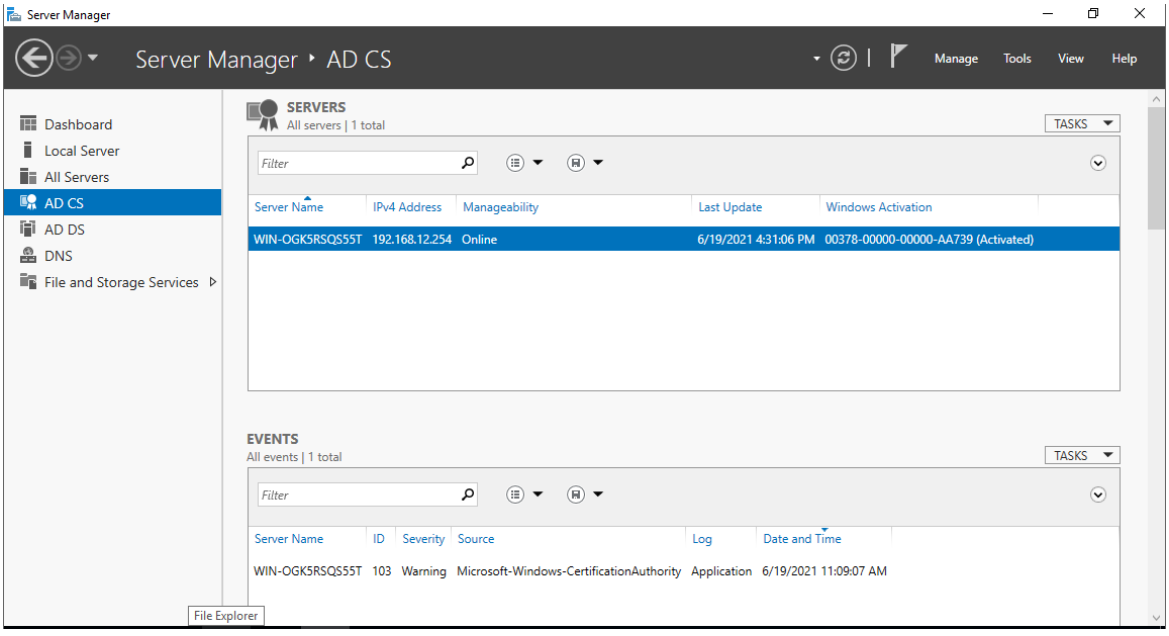
- Chọn **Configure** để thiết lập



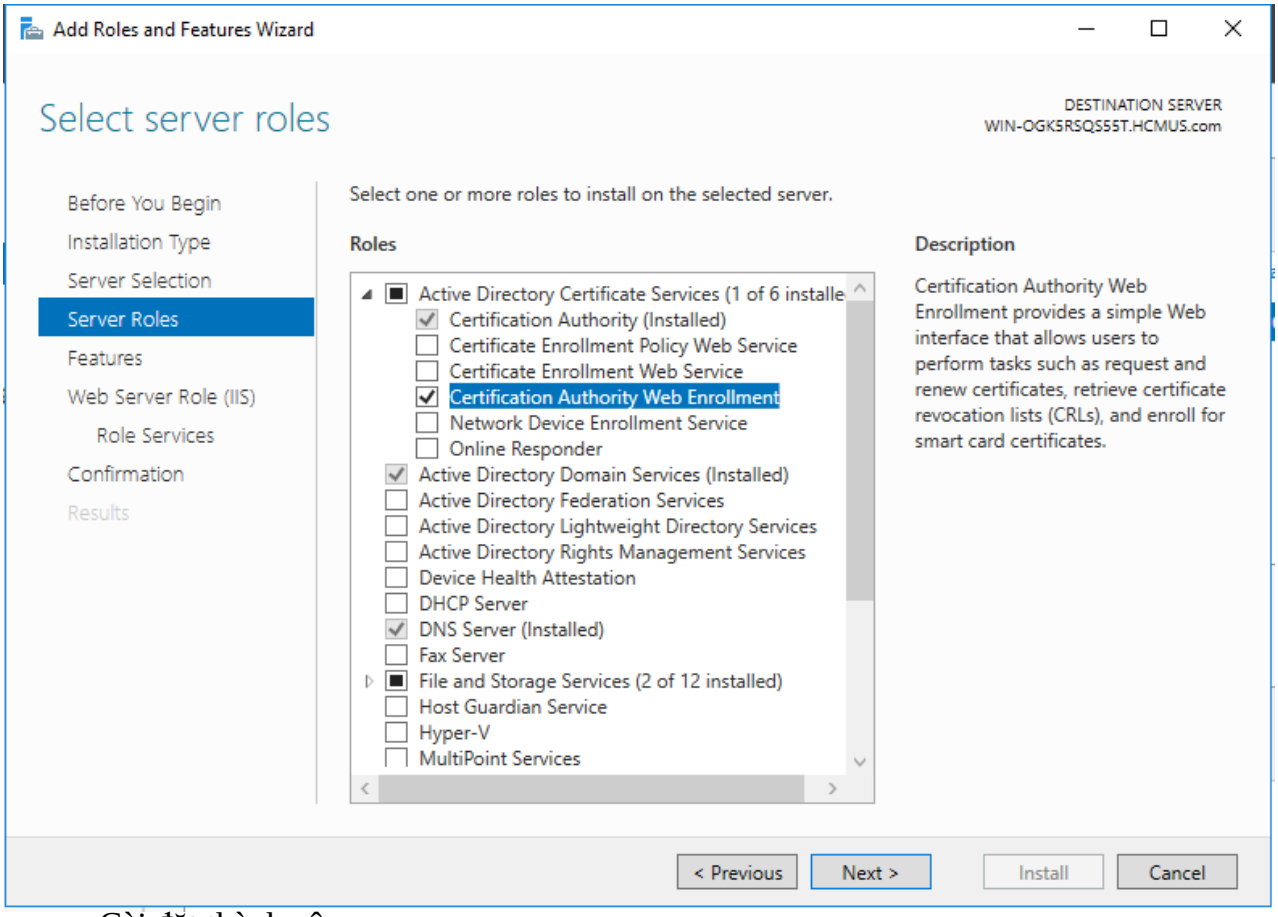
- Thiết lập thành công



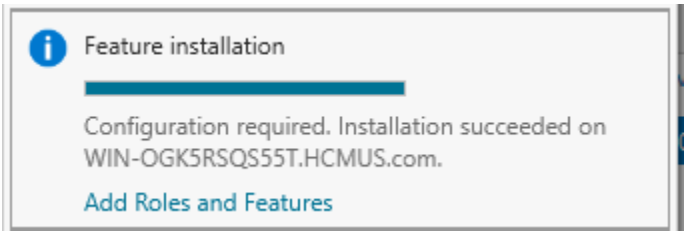
- Sau đó bật dịch vụ này lên trong **Server Manager**



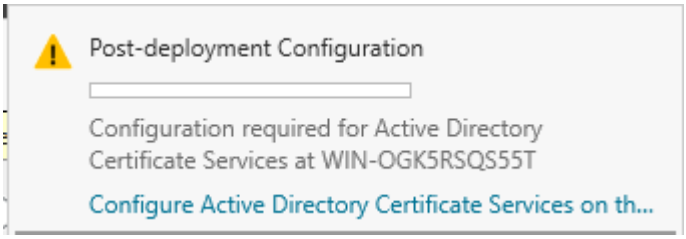
- Cài đặt như trên là xong, để có giao diện web dễ thực hiện việc cấp CA hơn, ta thêm **Certification Authority Web Enrollment**.
- Vào **Server Manager => Manage => Add Roles And Features**, thêm như hình dưới. Sau đó tến hành các cài đặt mặc định cho cả **Web Server Role (IIS)**



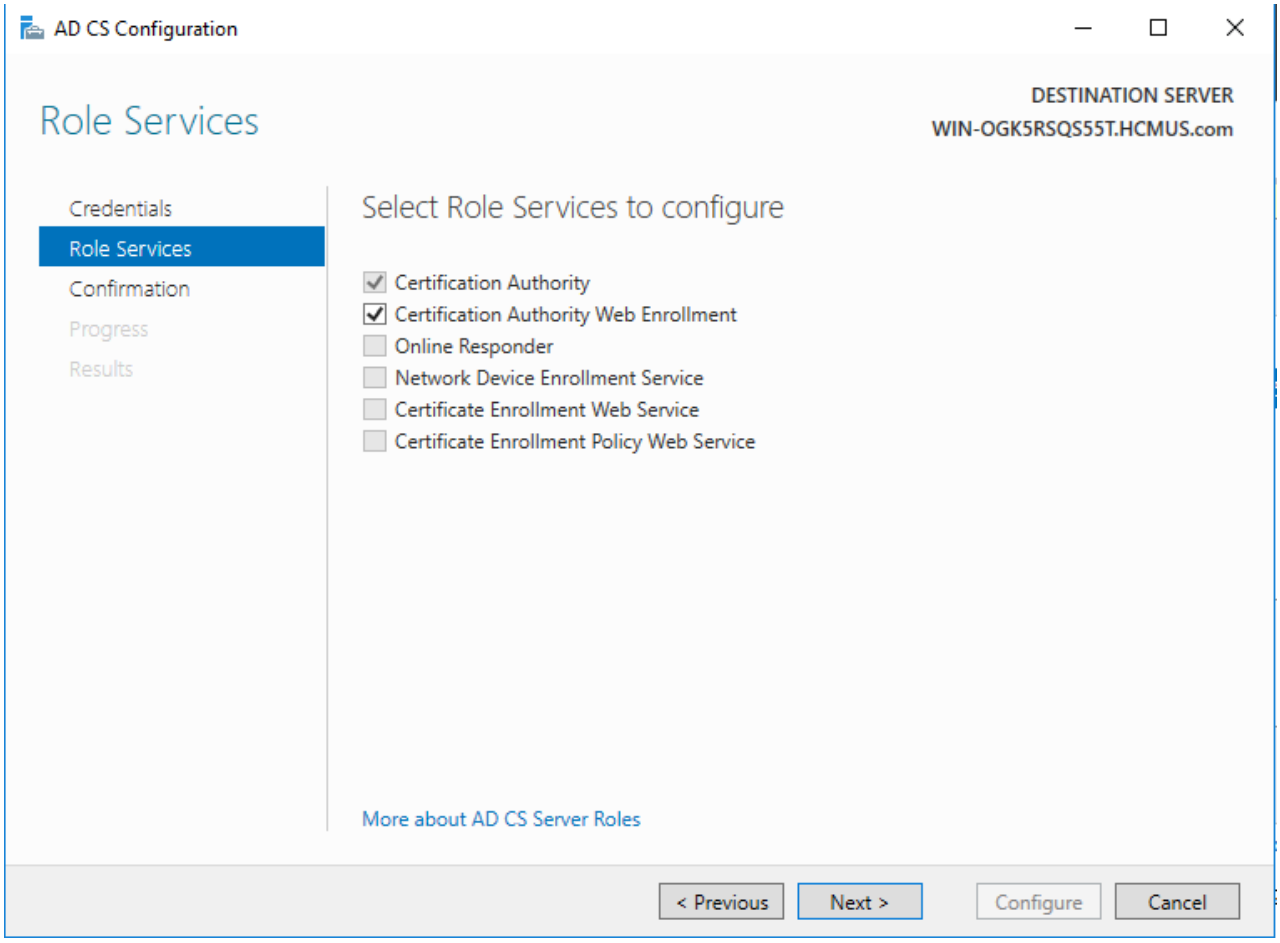
- Cài đặt thành công



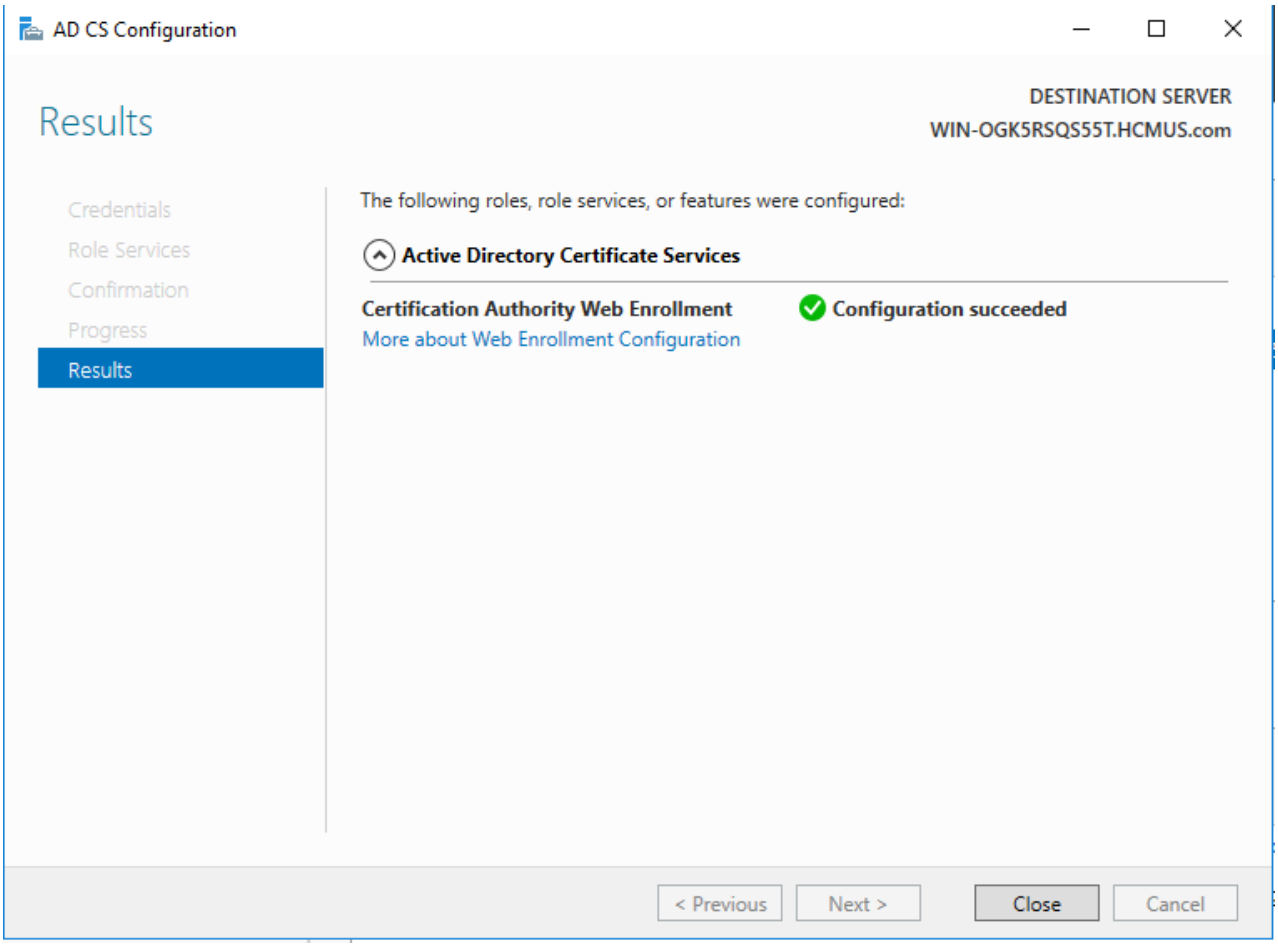
- Tiến hành thiết lập thêm



- Phần **Role Services** thêm **Certification Authority Web Enrollment**, sau đó tiến hành các cài đặt mặc định



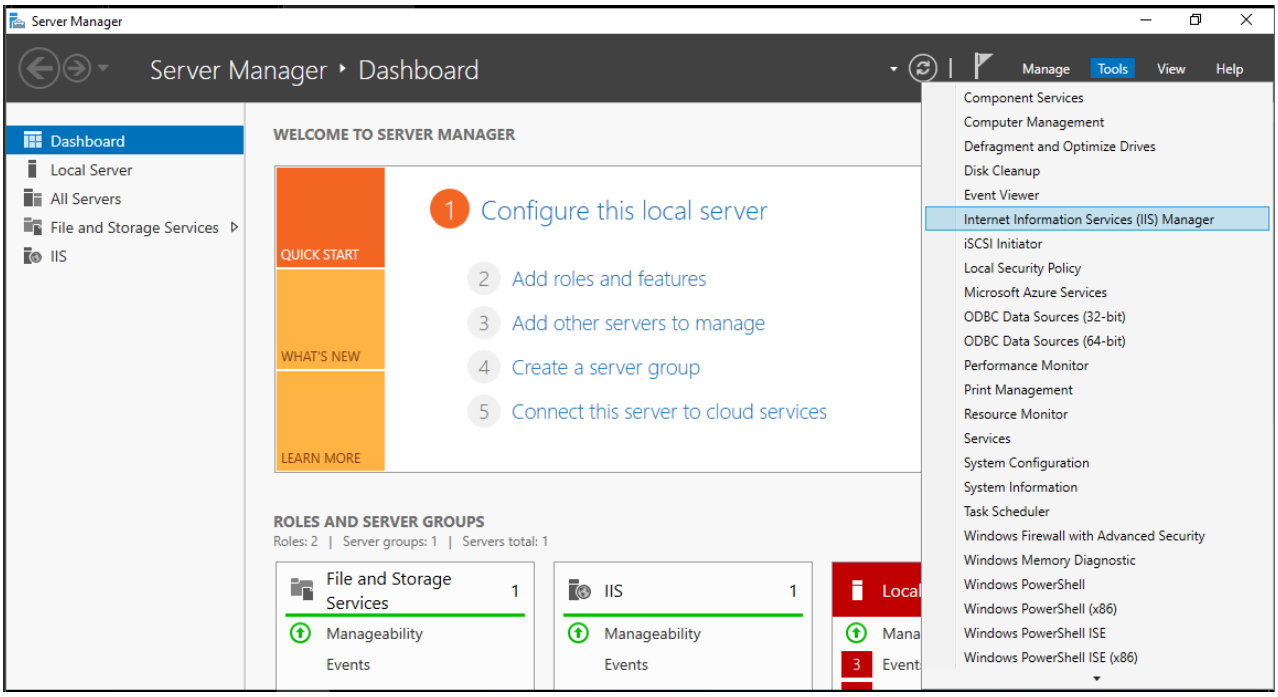
- Thiết lập thêm giao diện web thành công



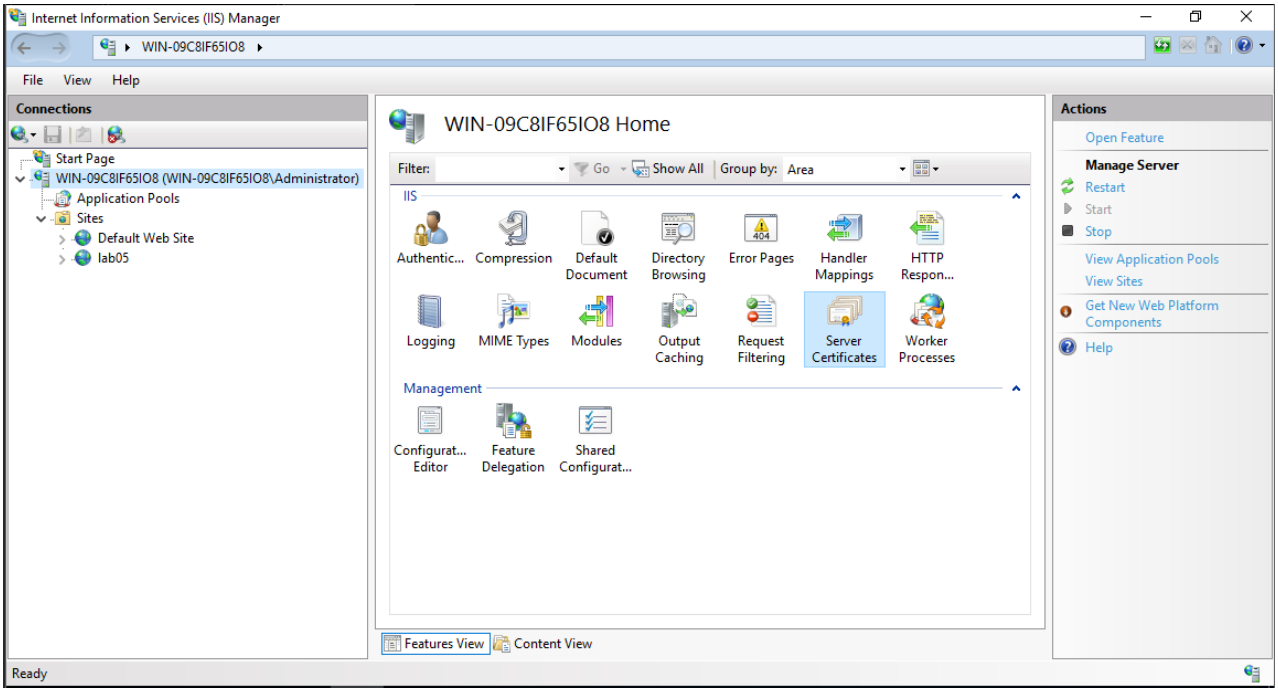
II.5. Cấu hình Web – Server để truy cập Website qua giao thức HTTPS

II.5.1. Máy Web – Server xin Certificate từ CA Server (Domain – Controller)

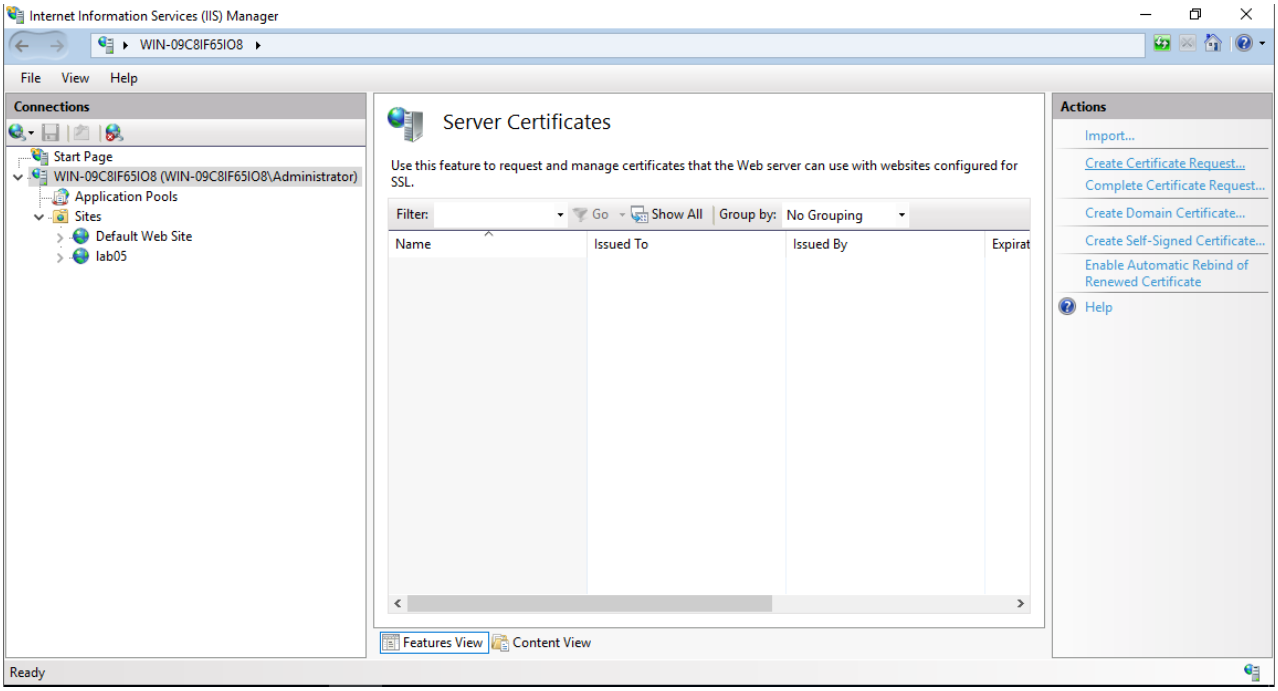
- Vào **Server – Manager => Tools => Internet Information Services (IIS) Manager**



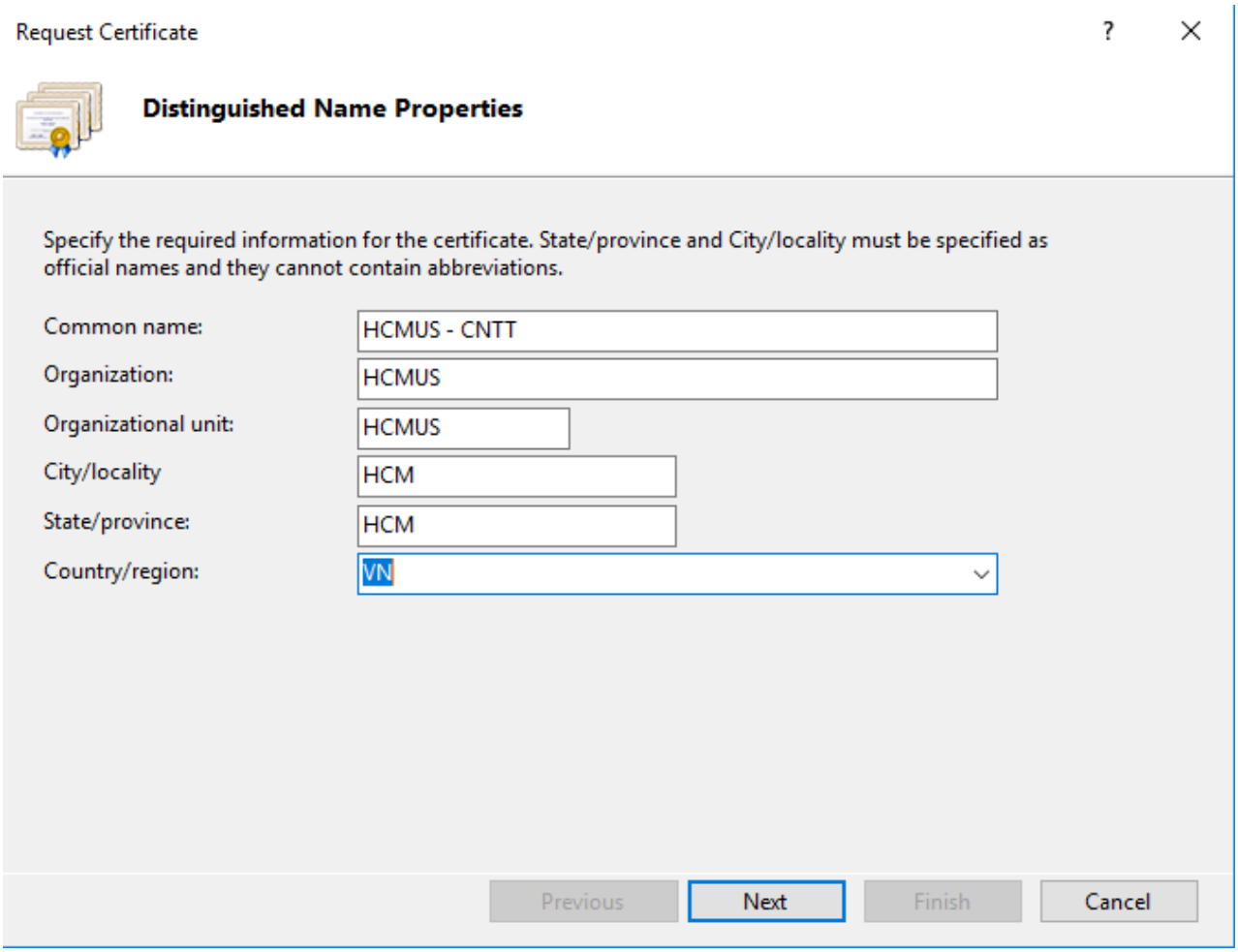
- Click vào tên máy, ở mục **IIS** chọn và mở **Server Certificates**



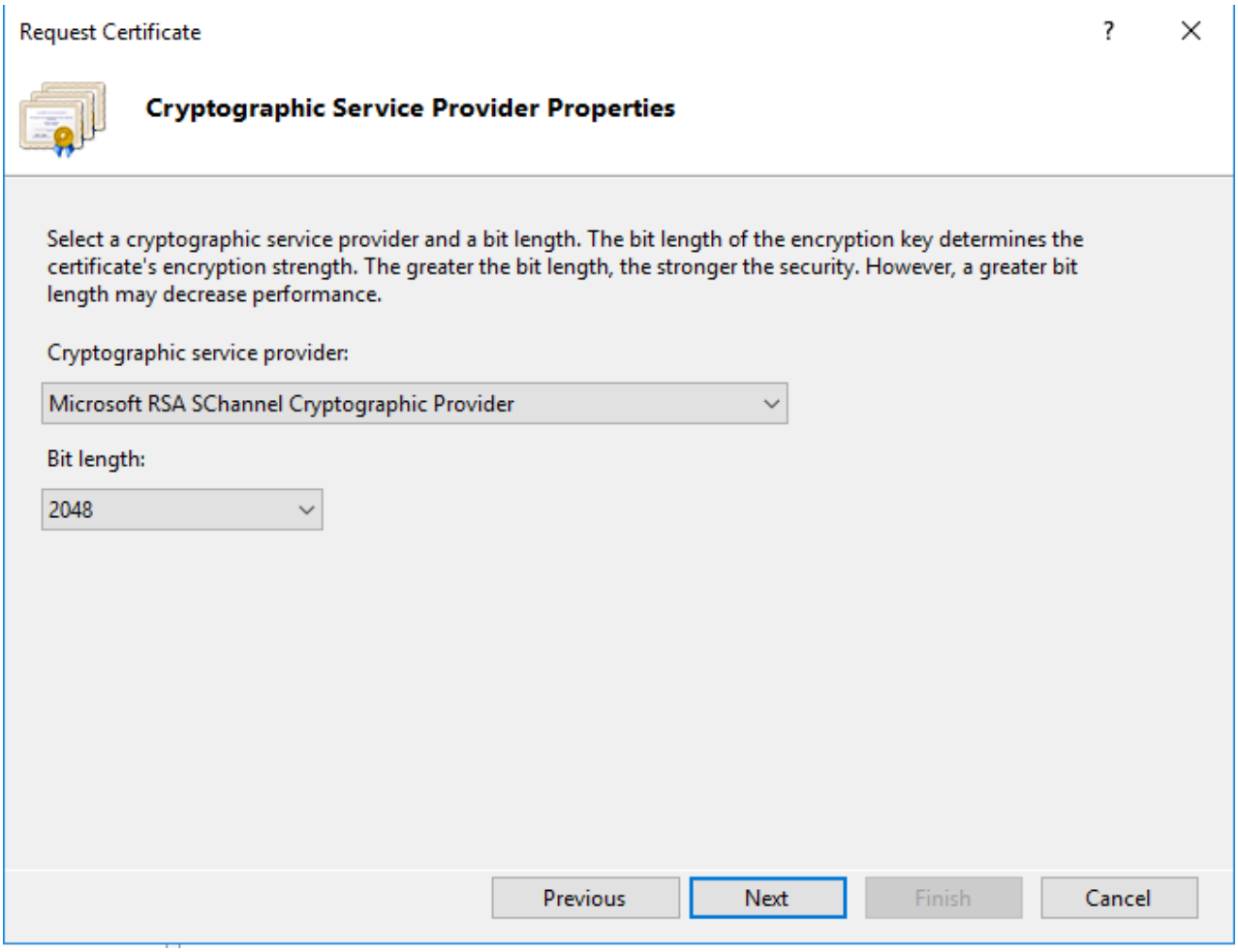
- Ở mục **Actions** bên phải, ta chọn **Create Certificate Request** để tạo một request



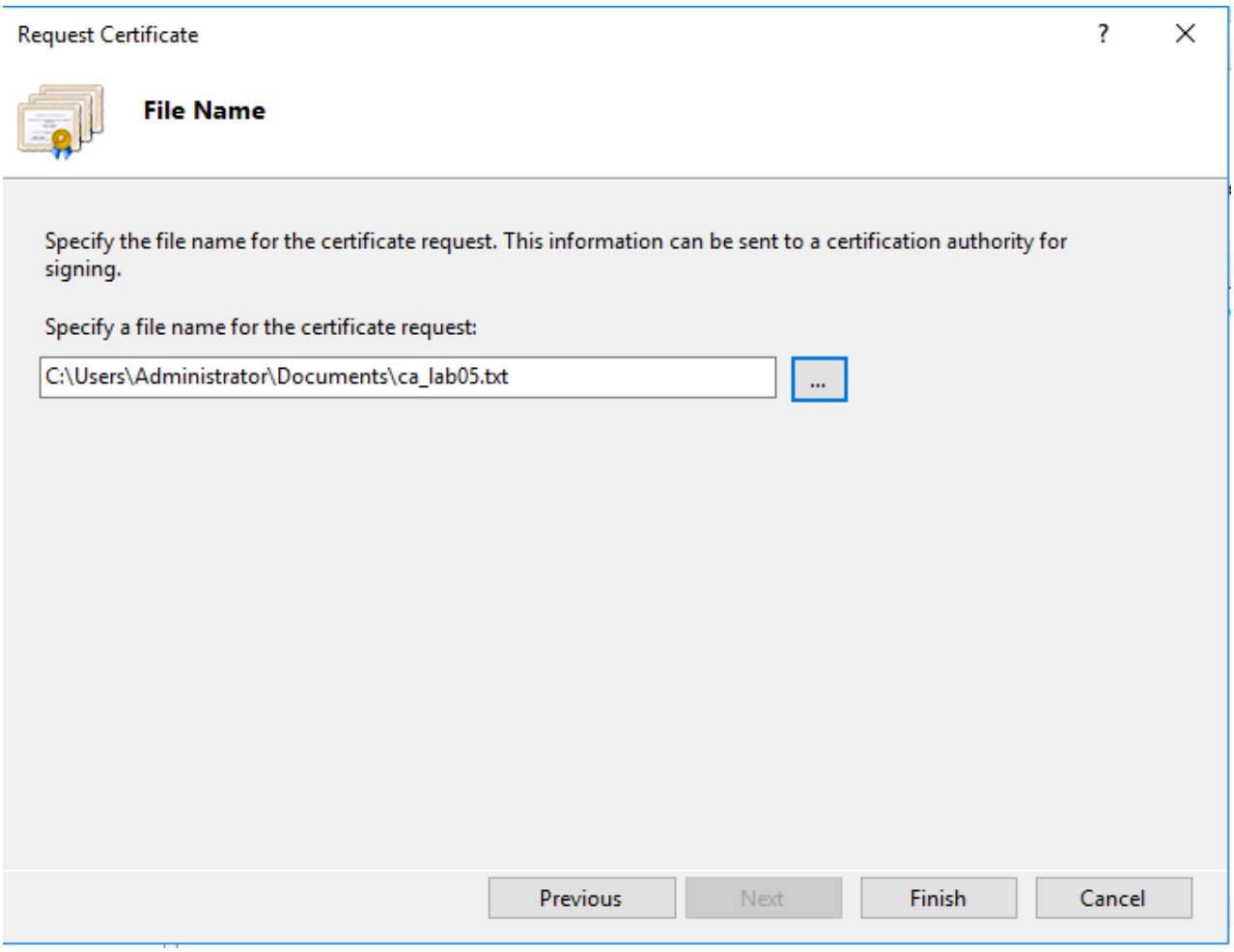
- Ta điền các thông tin của **Certificate Request** như sau



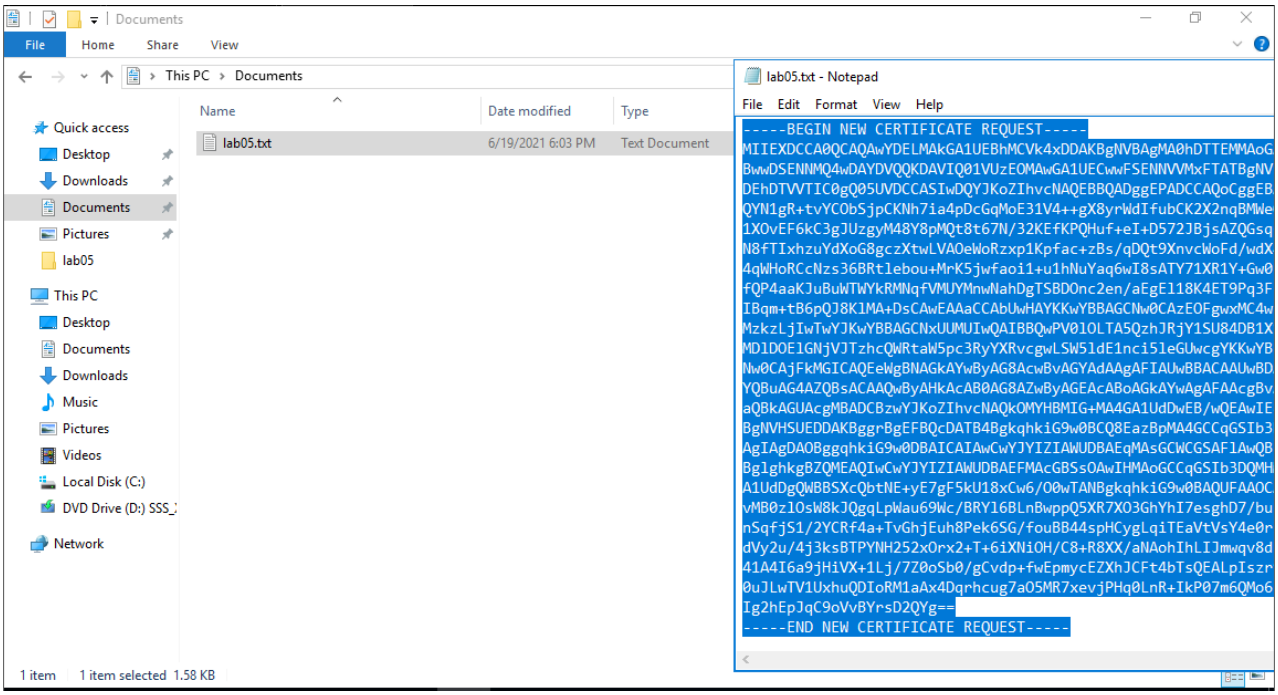
- Phần cung cấp dịch vụ mã hóa, ta chọn như sau



- Đặt tên file của **Certificate Request**: **ca_lab05** và đường dẫn mặc định (**C:\Users\Administrator\Document\ca_lab05.txt**), sao đó chọn **Finish** để tạo

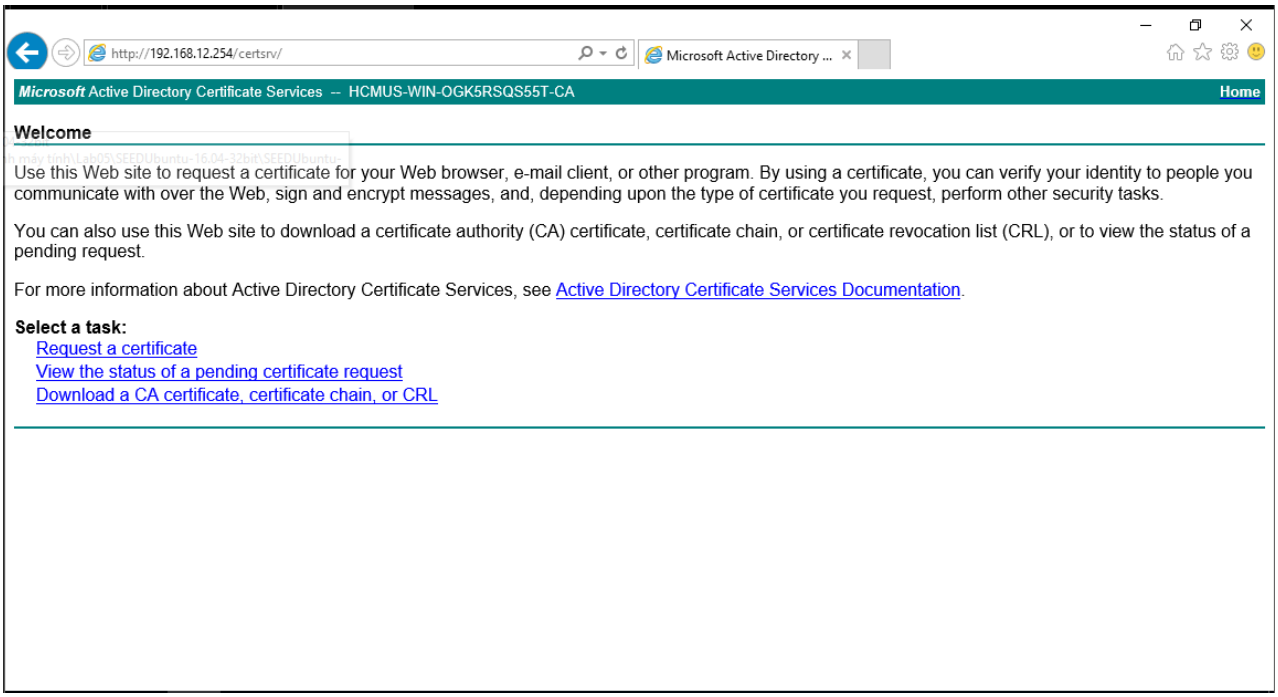


- Vào file **Certificate Request** vừa tạo, chọn copy nội dung của file

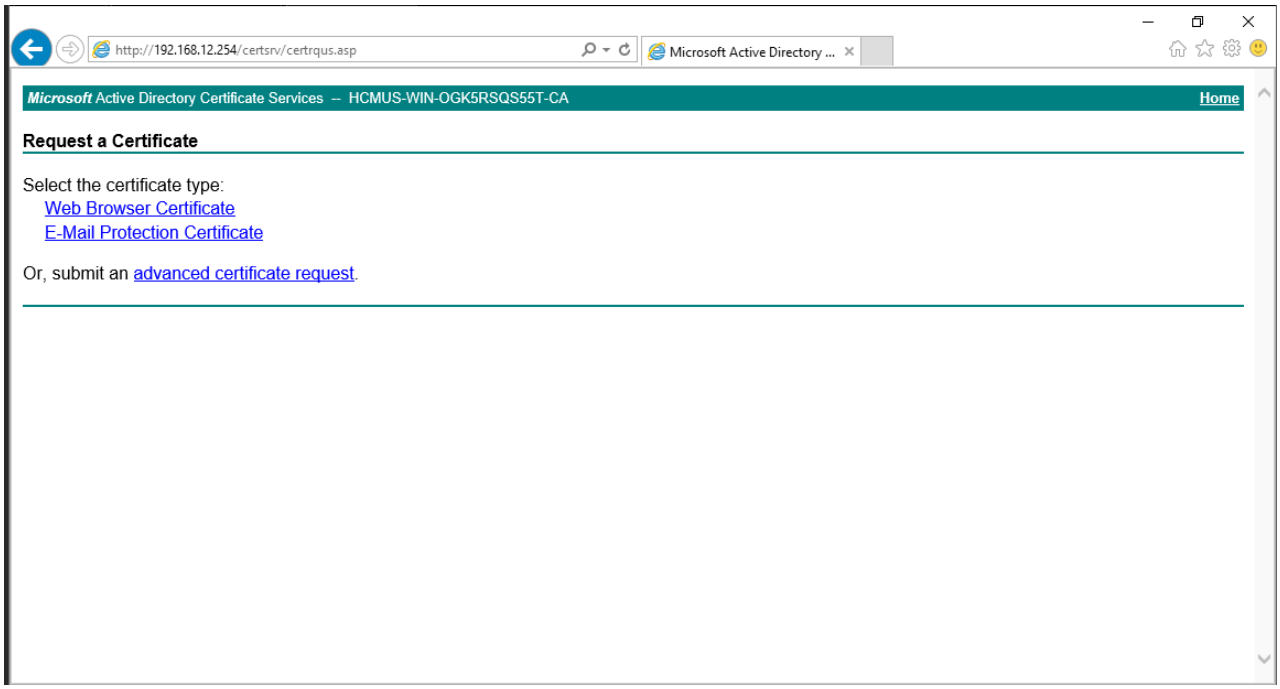


- Mở Web Browser của máy lên và truy cập địa chỉ CA Server (Domain – Contrller): 192.168.12.254/certsrv

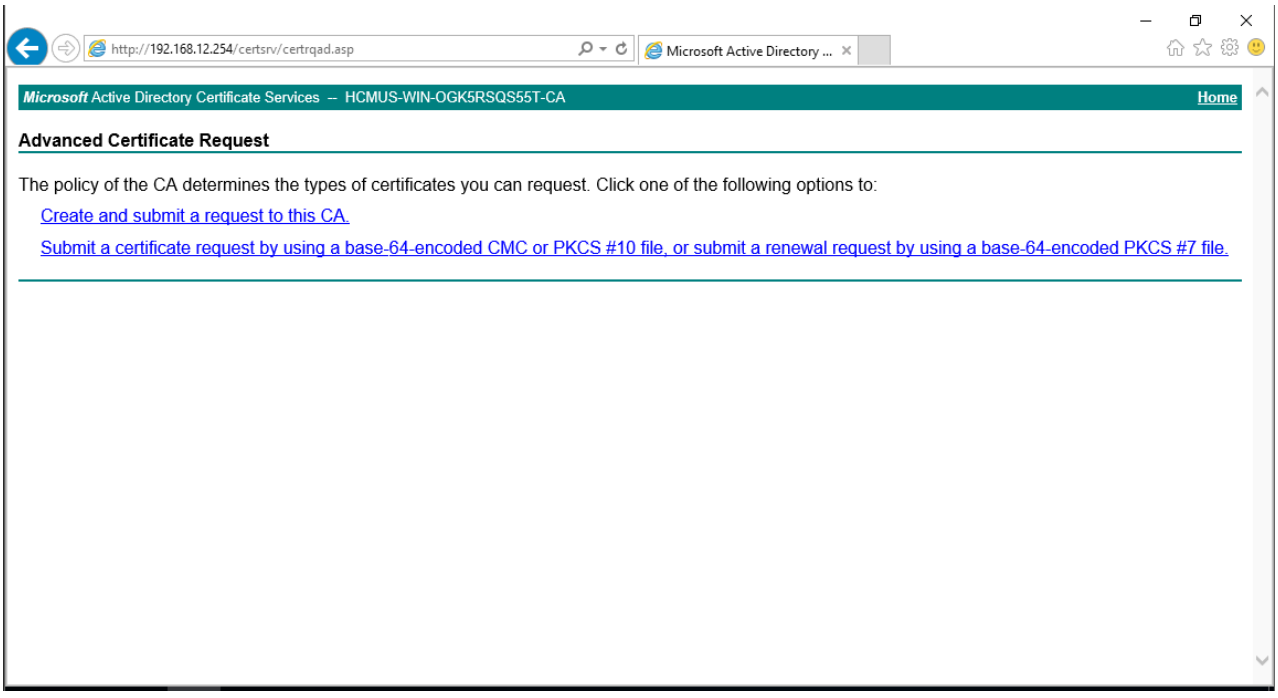
- Chọn Request a certificate



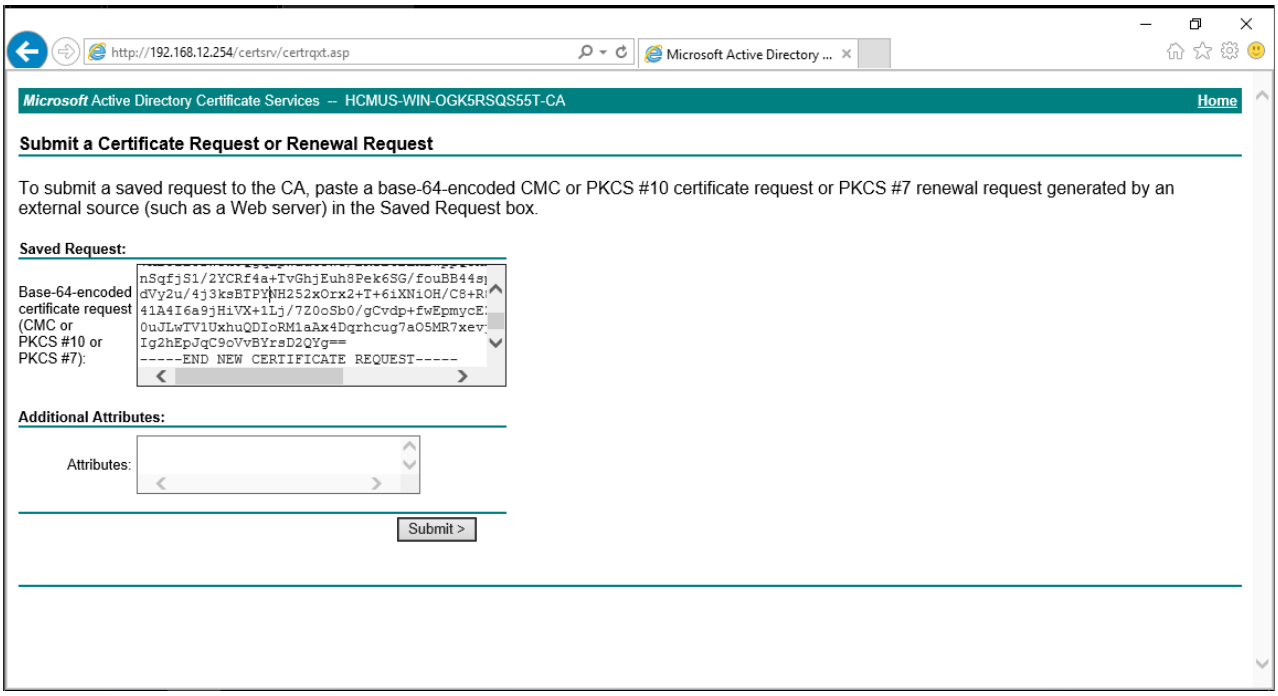
- Tiếp tục chọn advanced certificate request



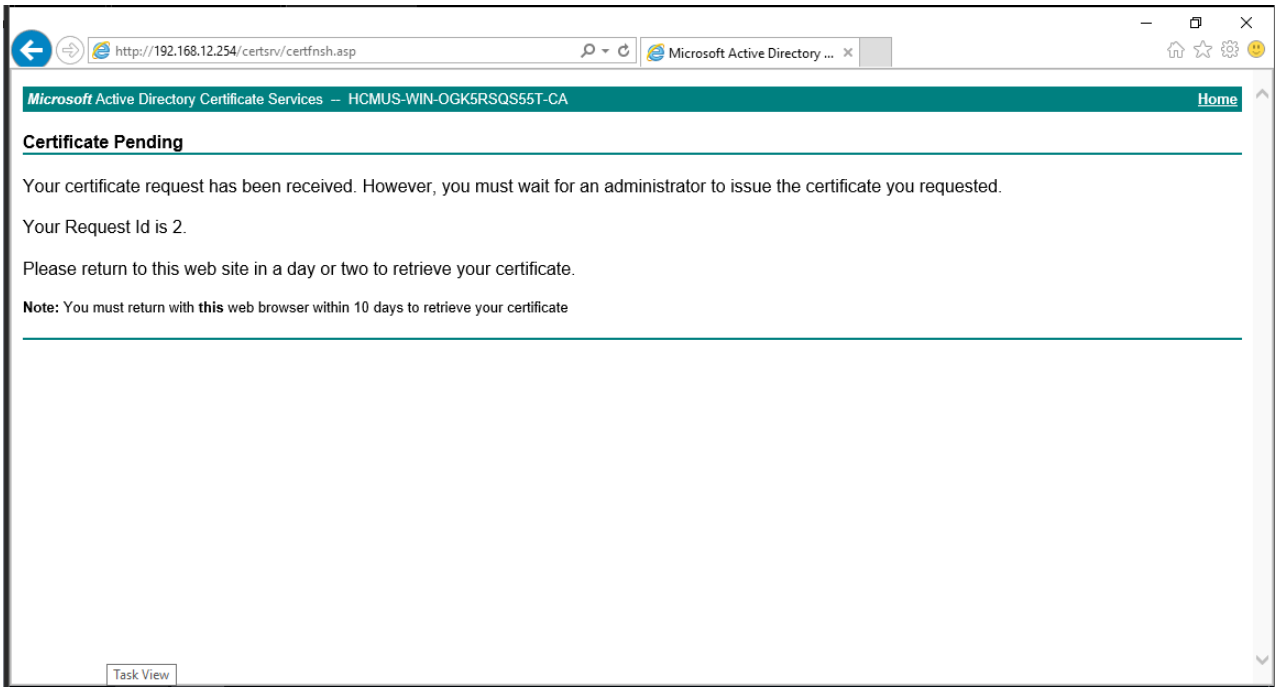
- Chọn Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.



- Sau đó điền nội dung của của file **Certificate Request** và chọn **Submit>**

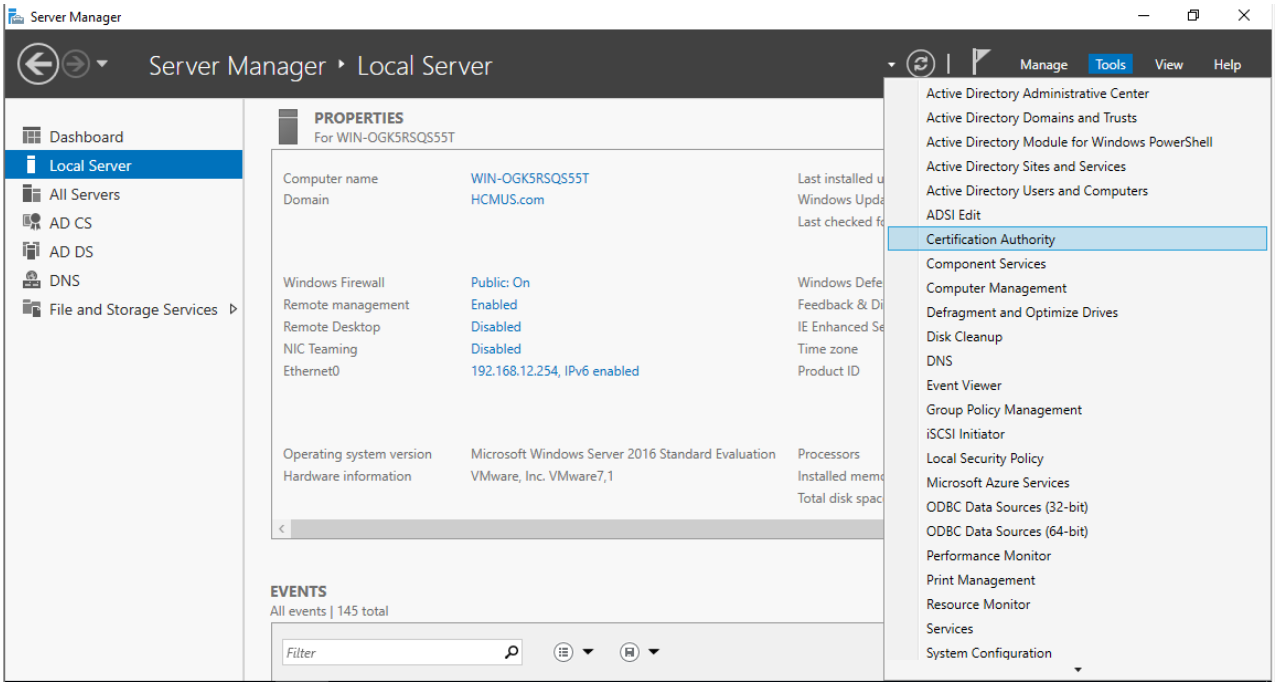


- **Submit** thành công, ta chuyển qua CA Server (Domain – Controller) để thực hiện cấp Certificate

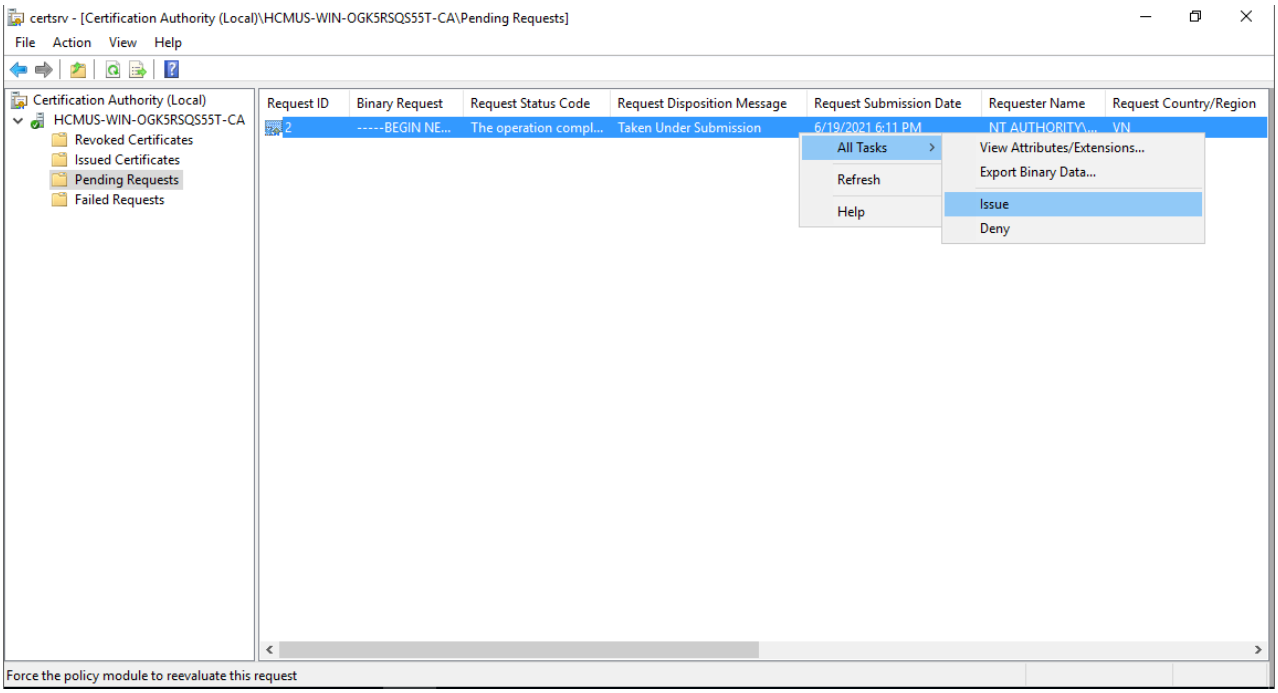


II.5.2. CA Server (Domain – Controller) cấp Ceritficate

- Vào **Server Manager** => **Tools** => **Certification Authority**

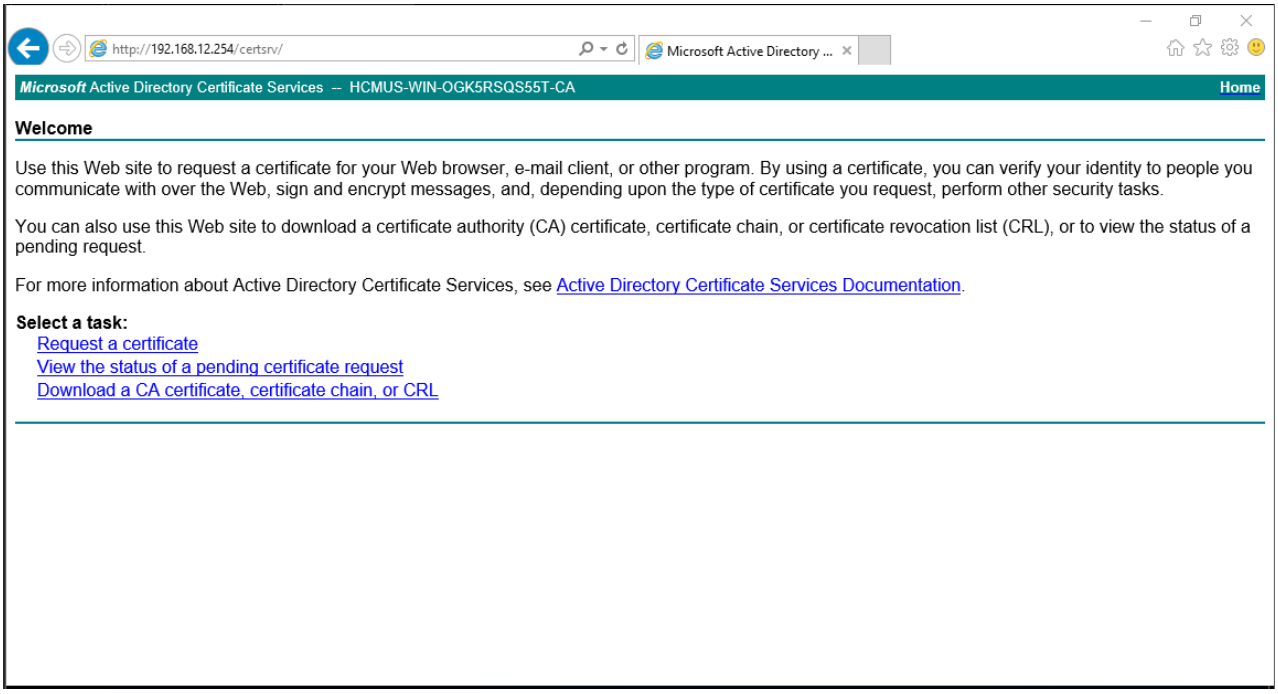


- Ở phần tên CA Server => **Pending Requests**, chọn vào request cần cấp Certificate => **All Tasks** => **Issue** để cấp Certificate

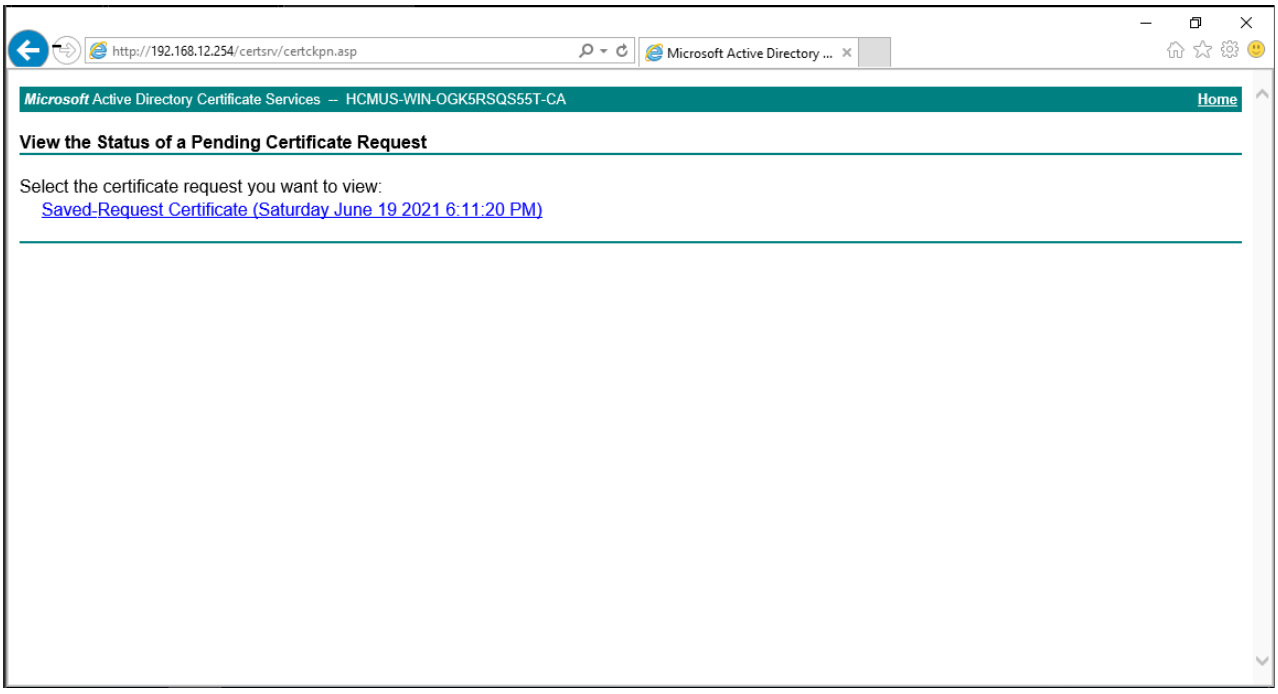


II.5.3. Máy Web – Server nhận Certificate từ CA Server (Domain – Controller)

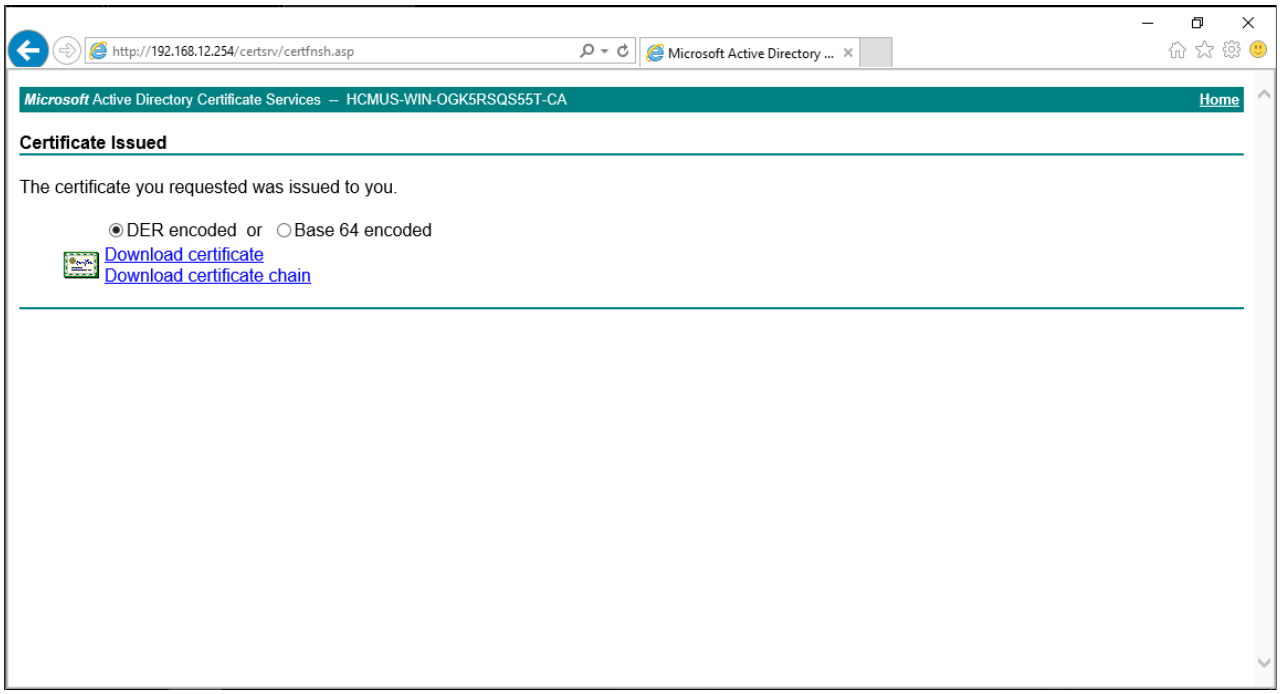
- Truy cập lại địa chỉ CA Server (Domain – Contrller): 192.168.12.254/certsrv
- Chọn View the status of pending certificate request



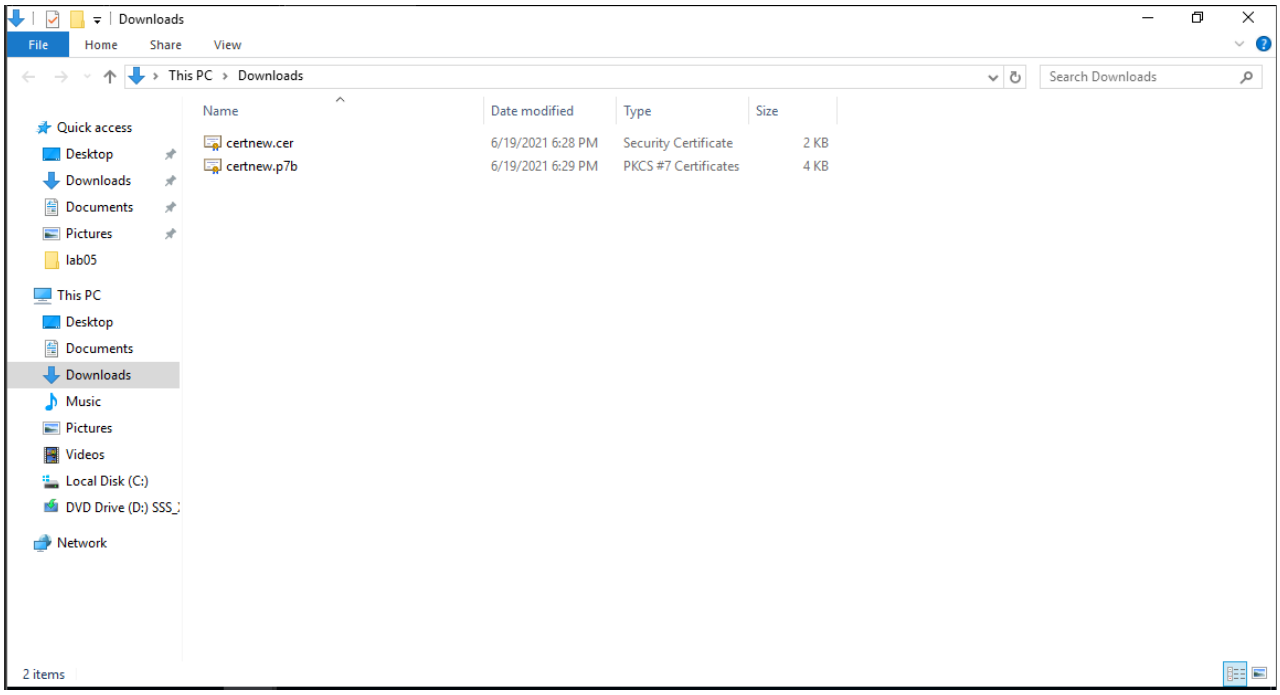
Sau đó chọn Saved-Request Certificate (Saturday June 19 2021 6:11:20 PM)



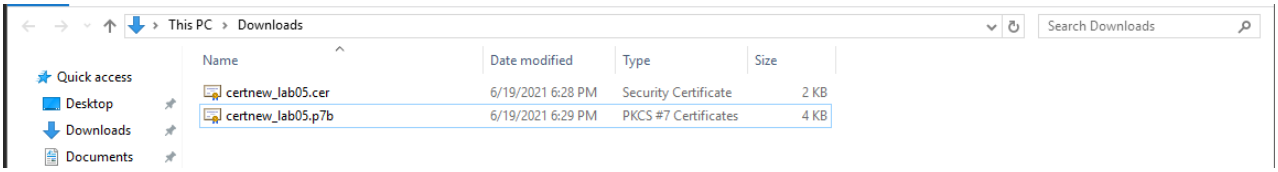
- Download cả 2 file Certificate



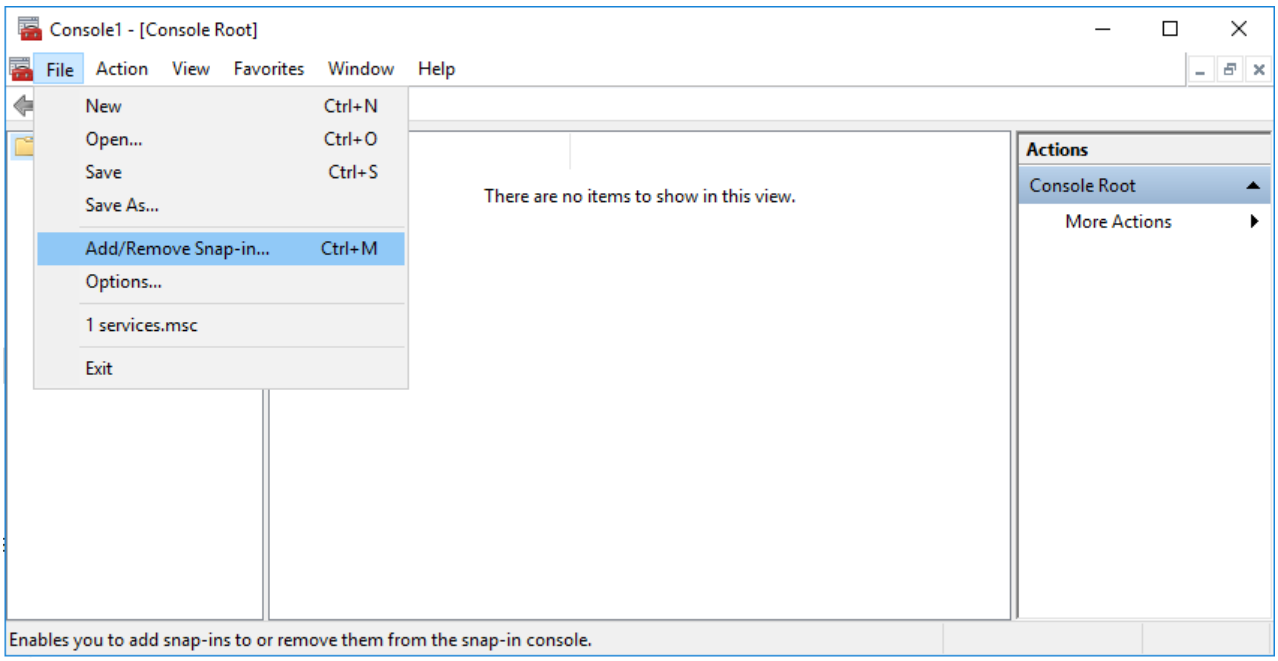
- Ta được 2 file như sau



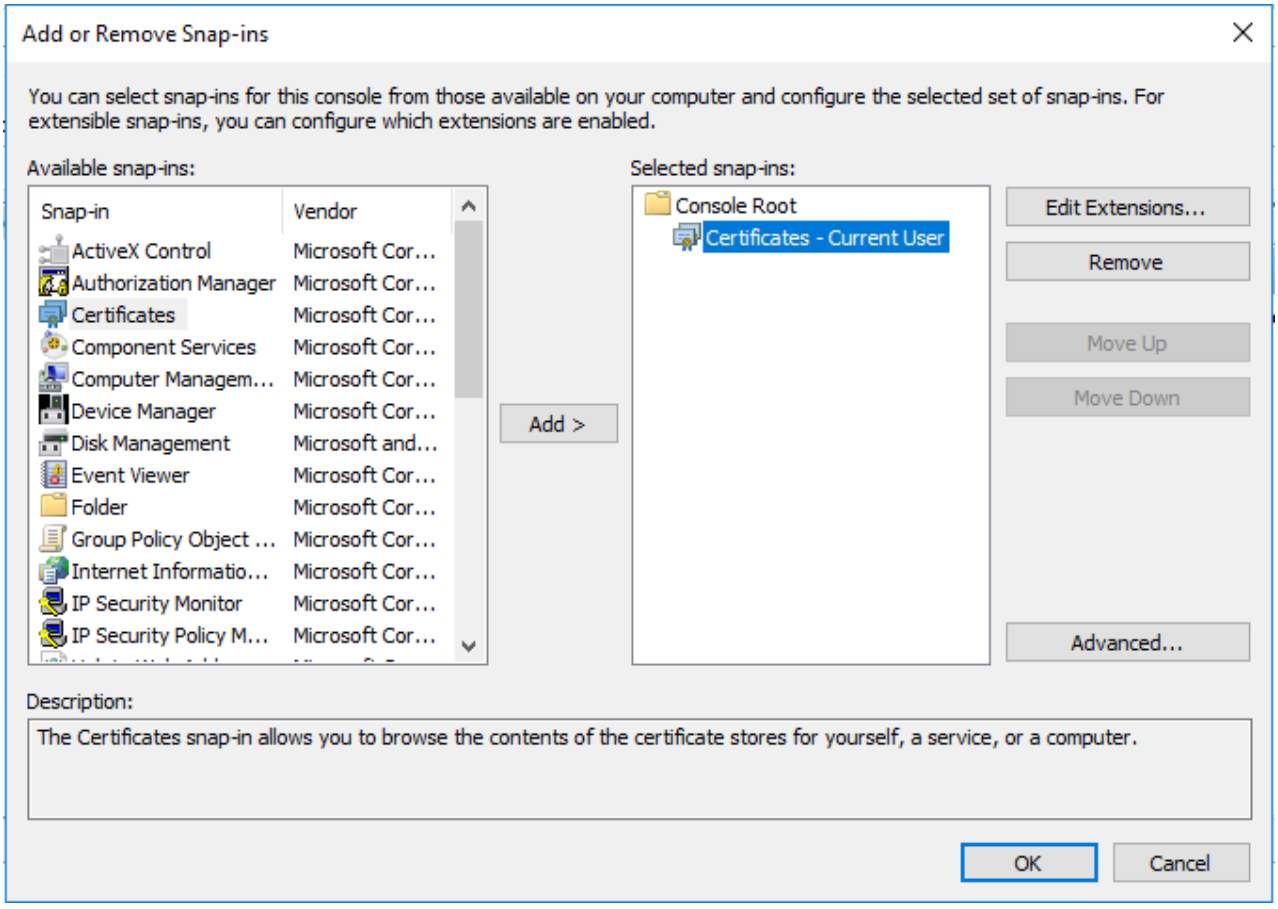
- Thực hiện đổi tên lại như sau (để dễ quản lí)



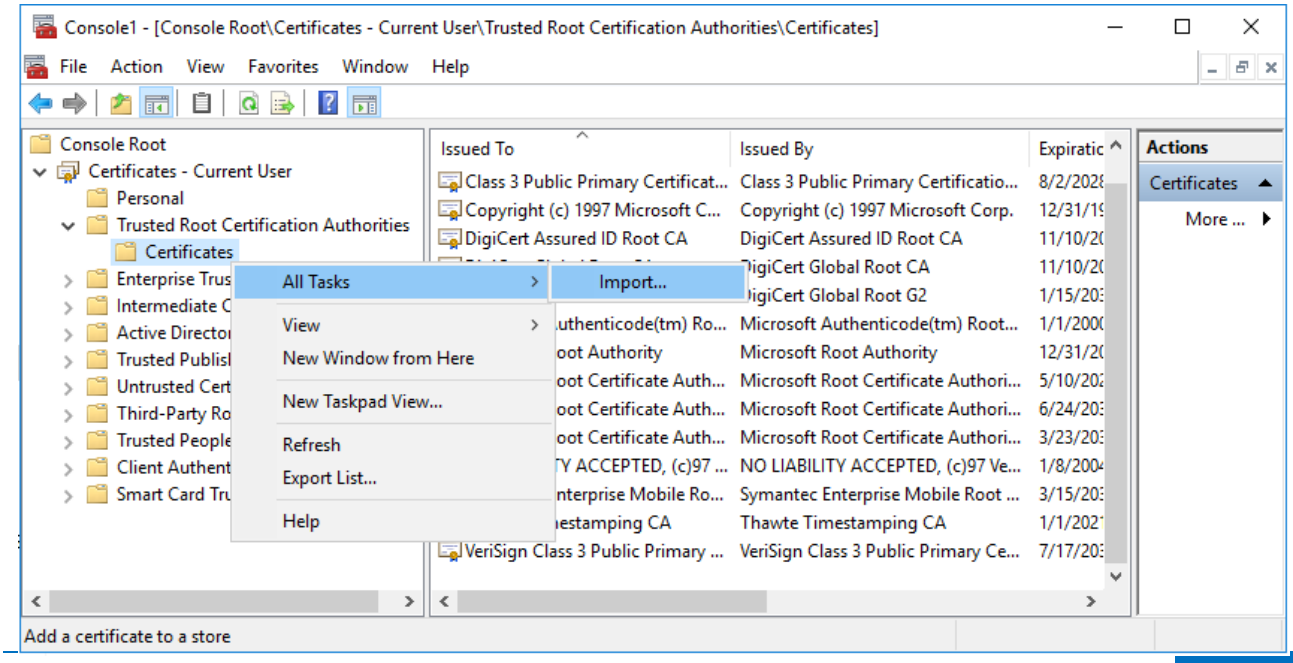
- Sau đó vào **mmc => File => Add/Remove Snap – in…**

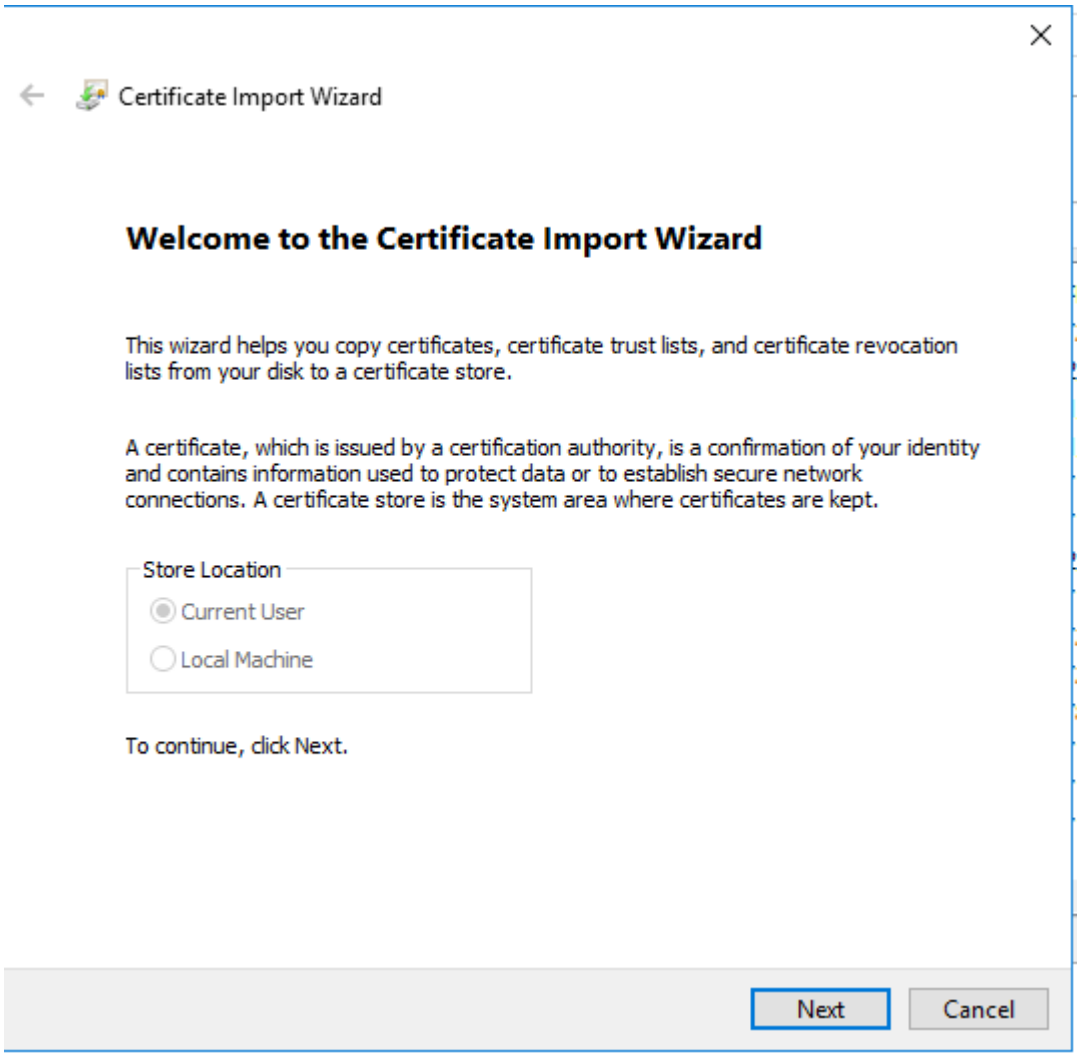


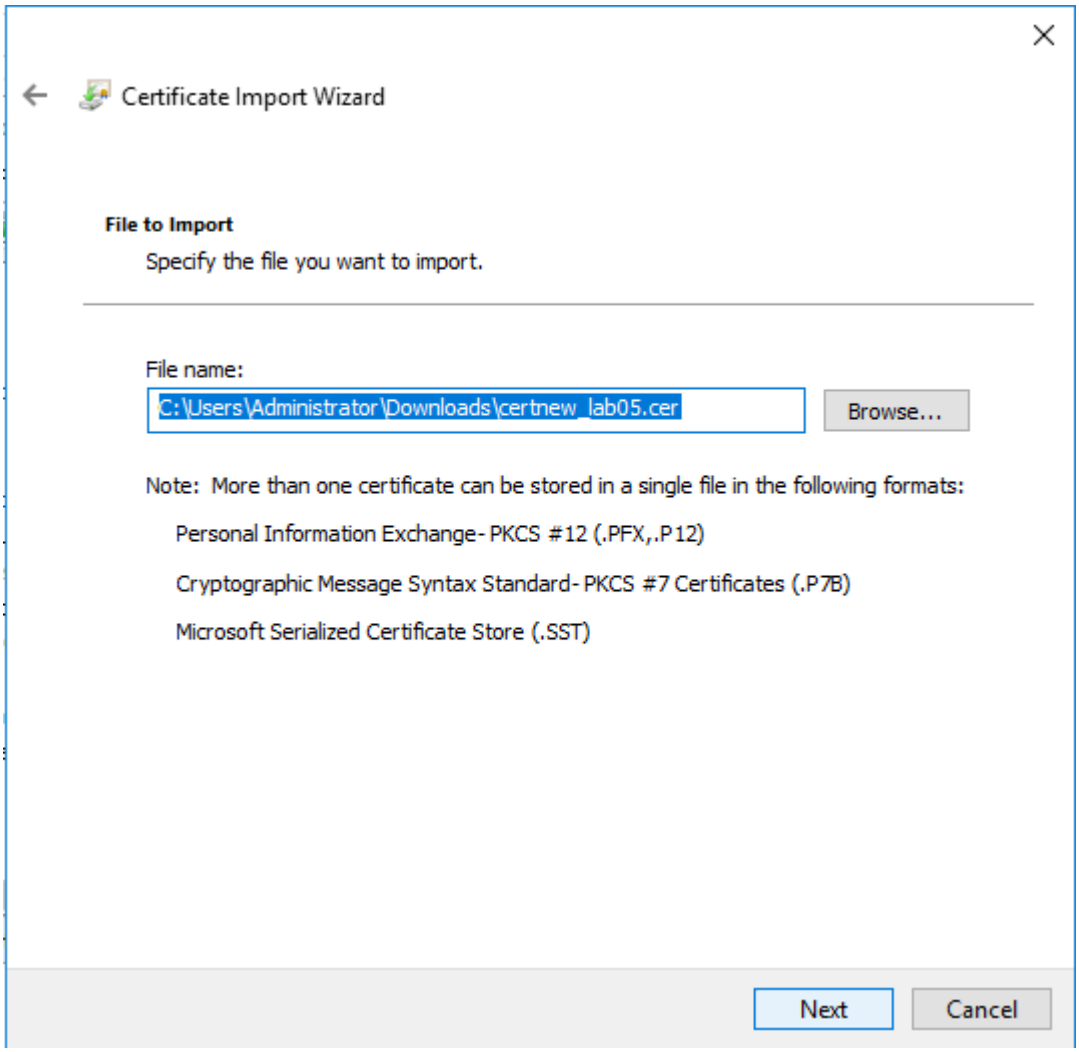
- Thêm **Certificates**

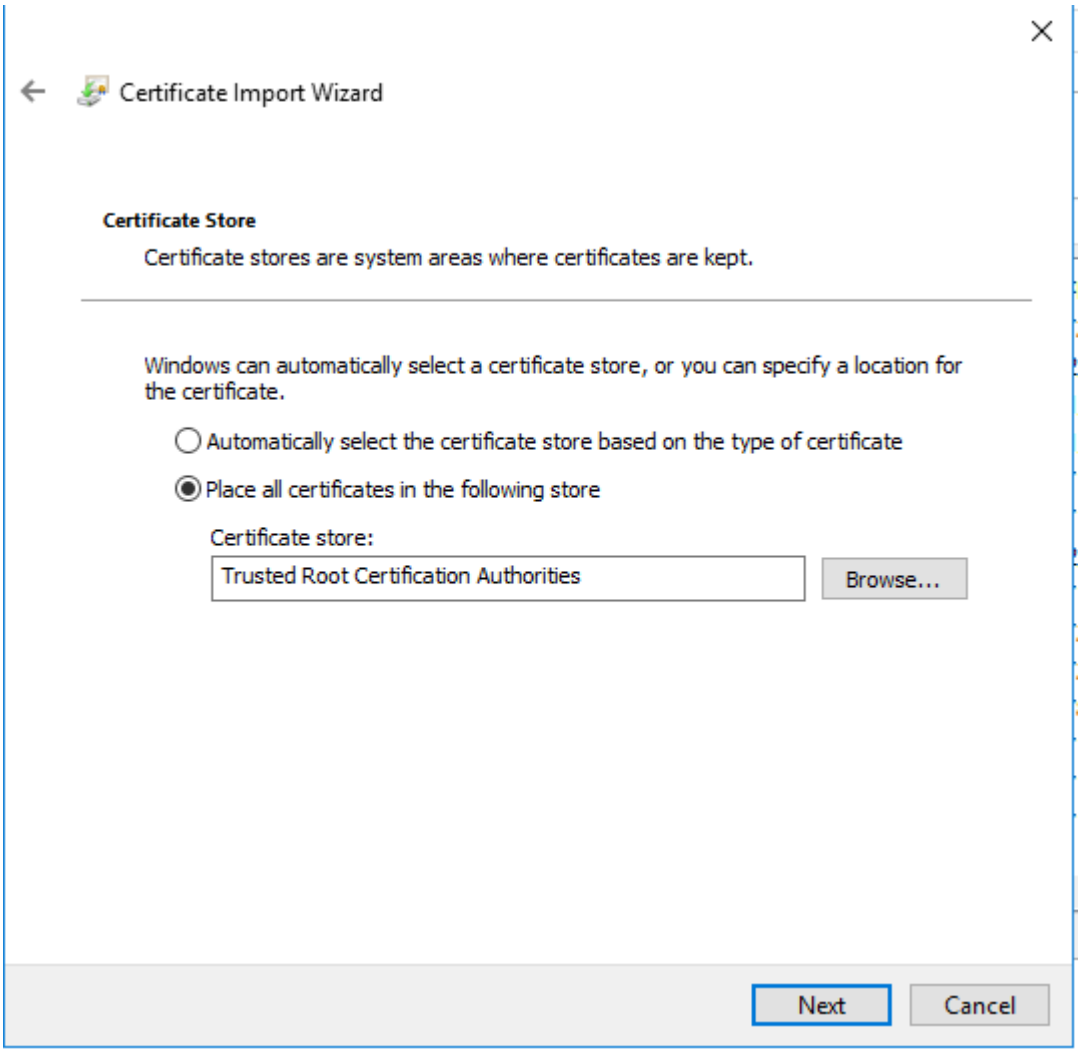


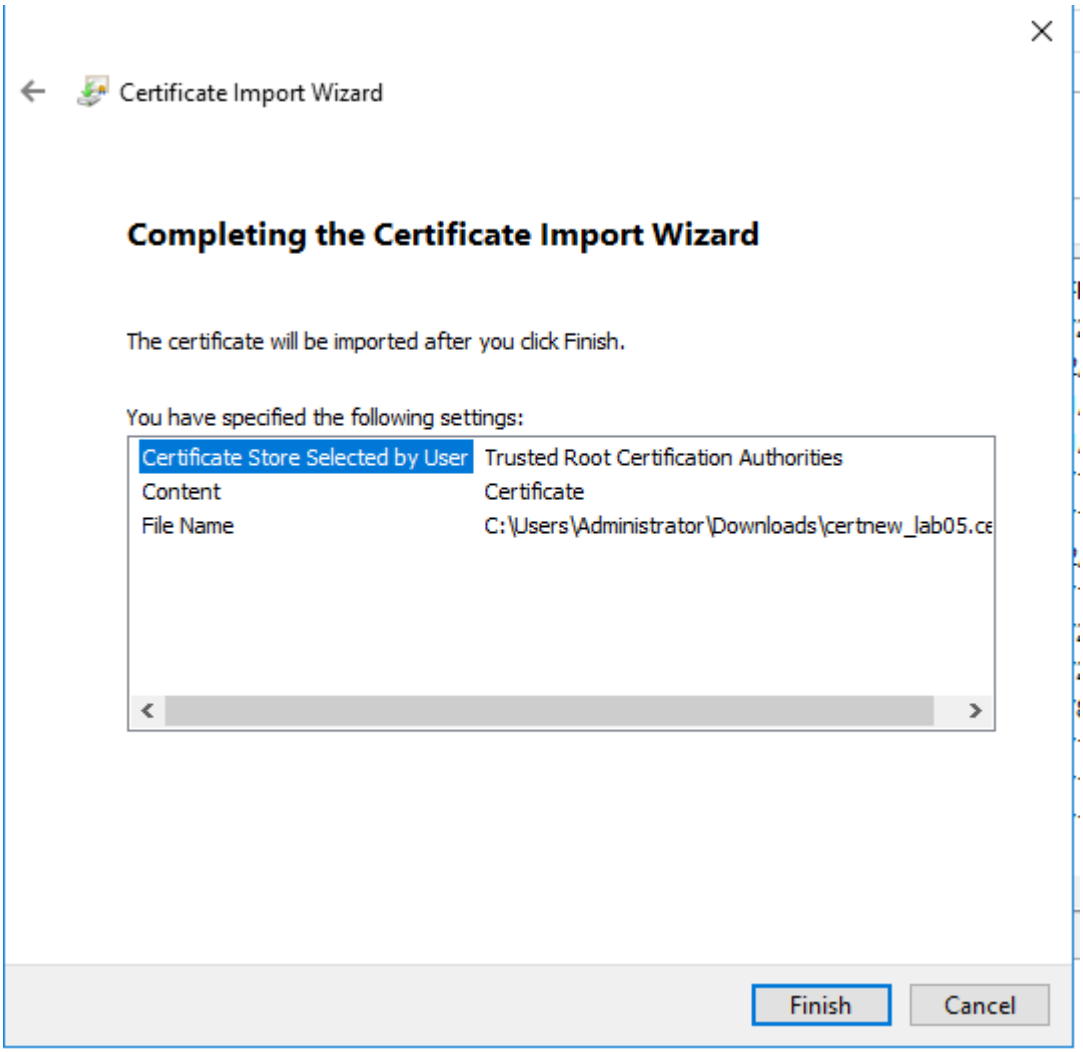
- Sau đó vào mục **Certificate – Current User => Trusted Certification Authorities => All Tasks => Import** 2 file Certificate vừa tải về



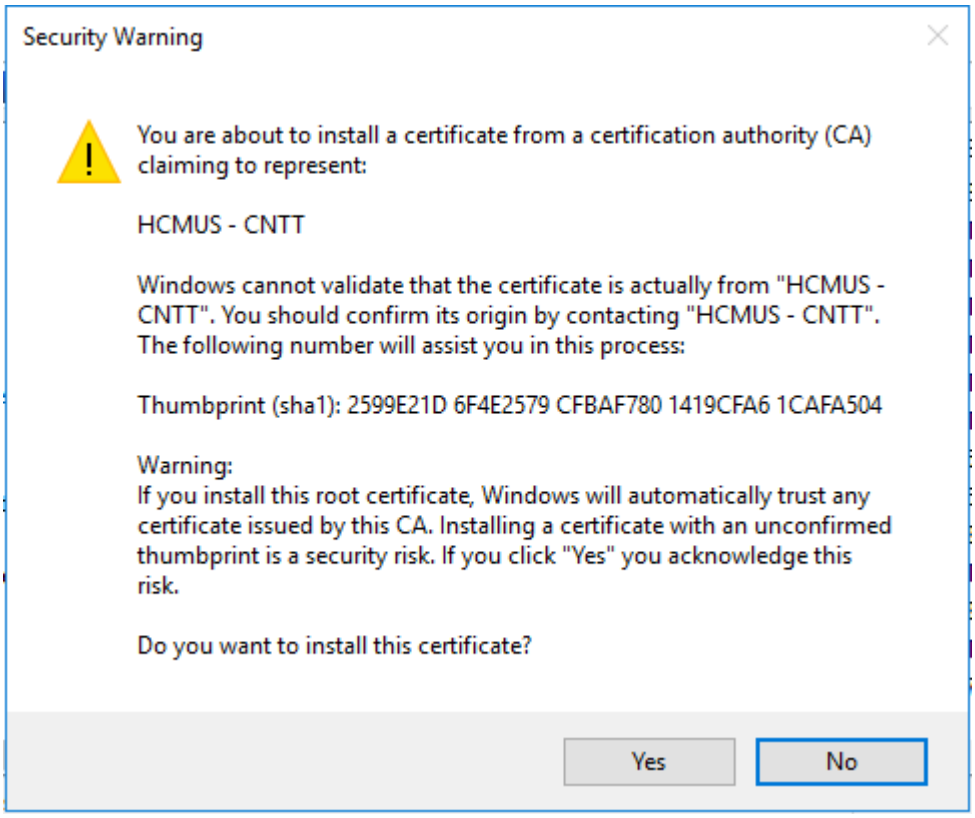

Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
C:\Users\Administrator\Downloads\certnew_lab05.cer
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Next
Cancel

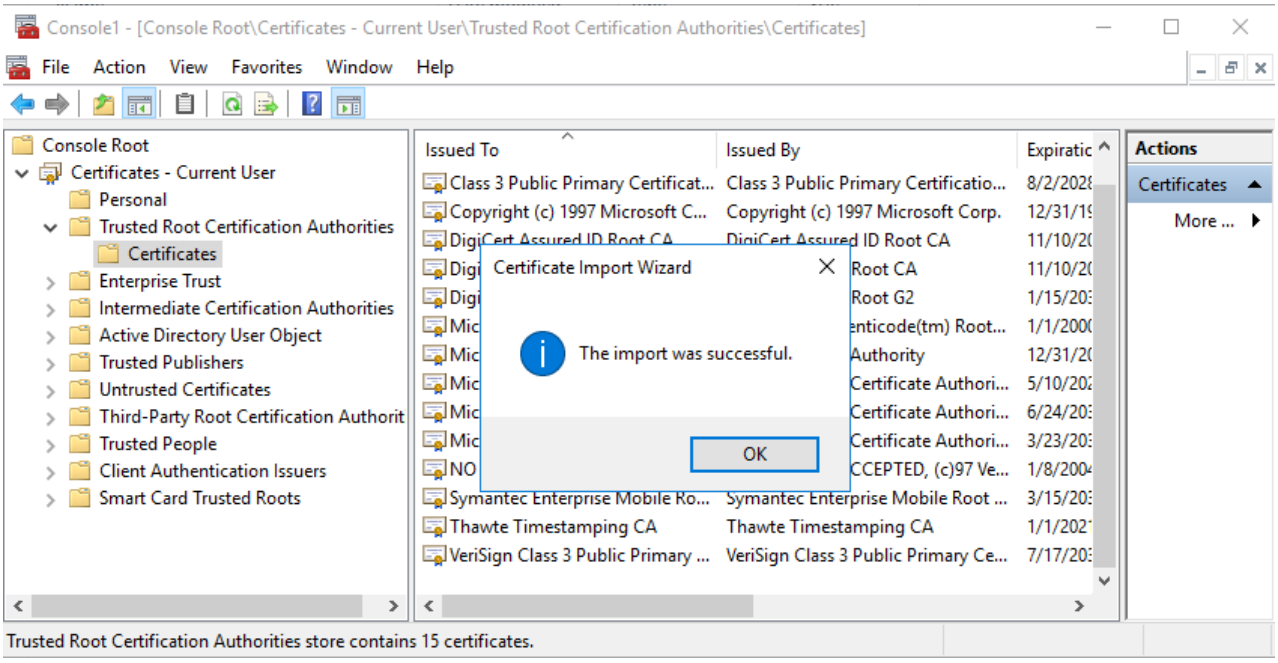

Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Next
Cancel


Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected by User
Trusted Root Certification Authorities
Content
Certificate
File Name
C:\Users\Administrator\Downloads\certnew_lab05.ce
Finish
Cancel

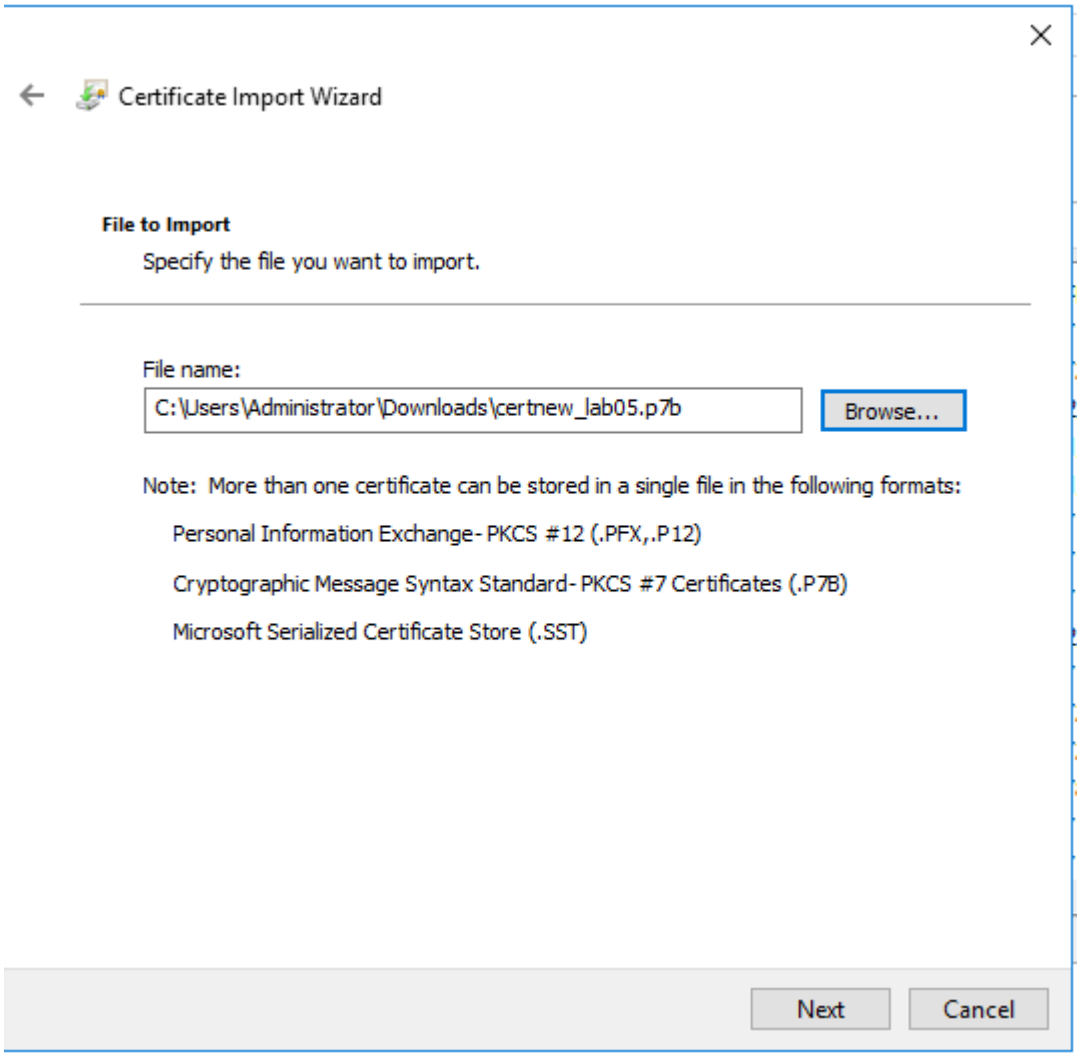
- Ta chọn **Yes**



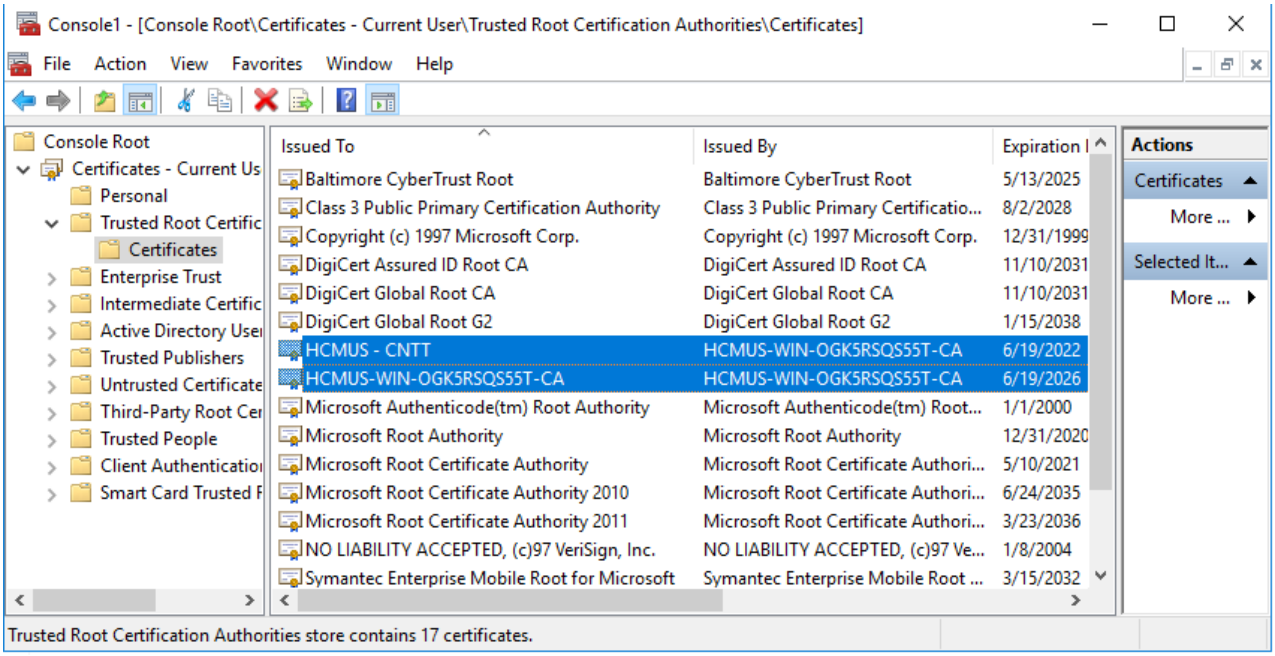
- Thêm thành công



- Tương tự ta thêm file còn lại vào

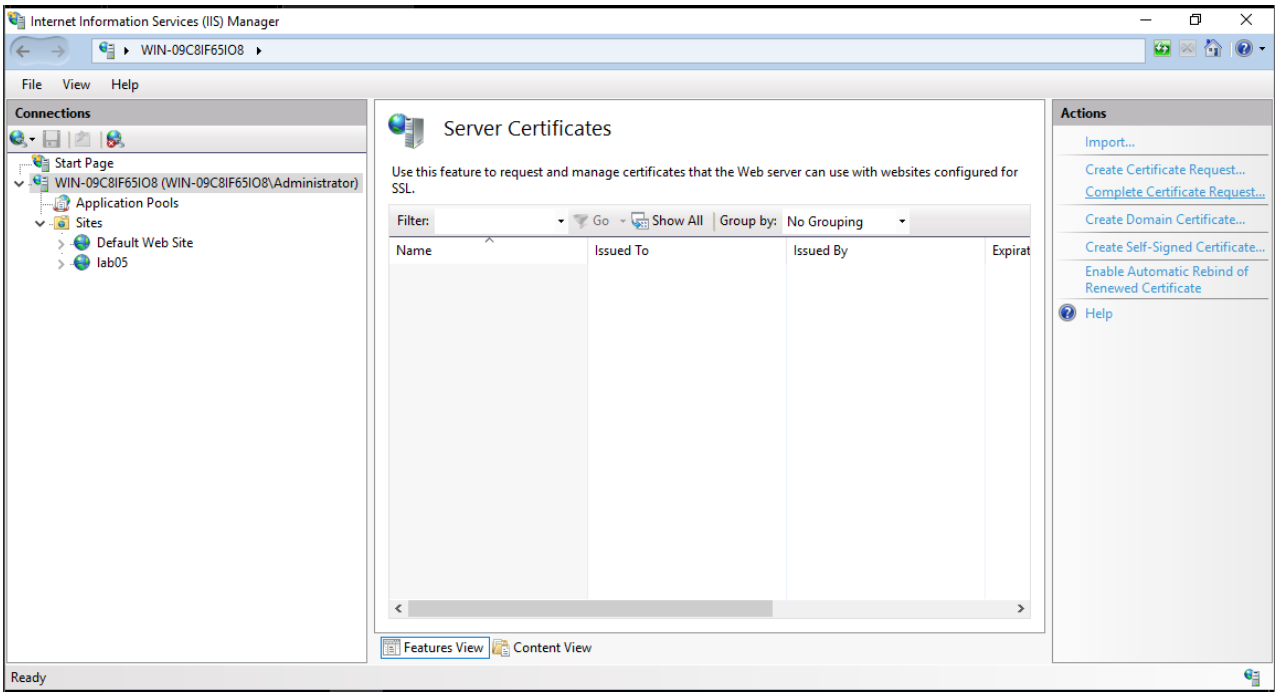


- Thêm các file thành công

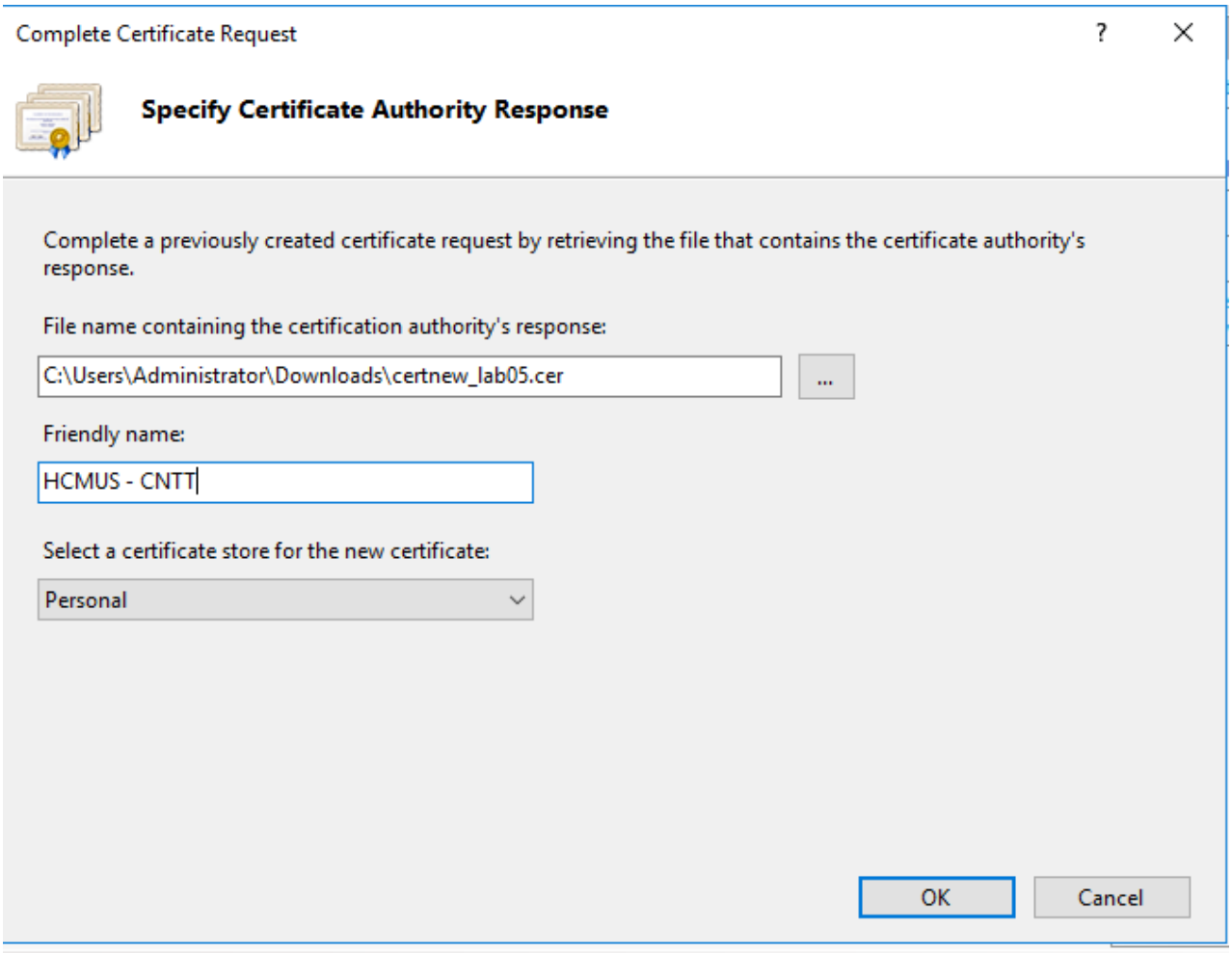


II.5.4. Web – Server thiết lập giao thức HTTPS

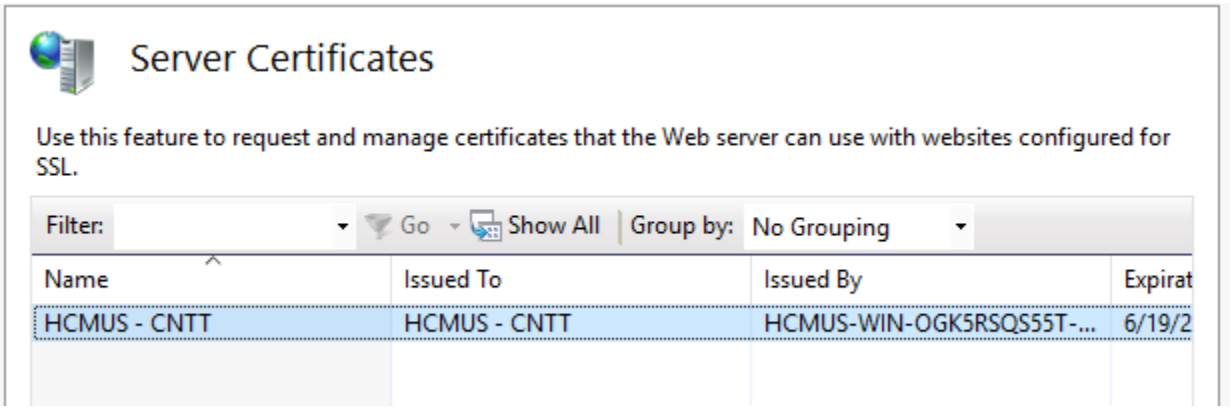
- Vào lại phần **Server Certificate** của Web – Server. Trong phần **Actions,** chọn **Complete Certificate Request**. Để hoàn thành việc cấp Certificate chon Web – Server



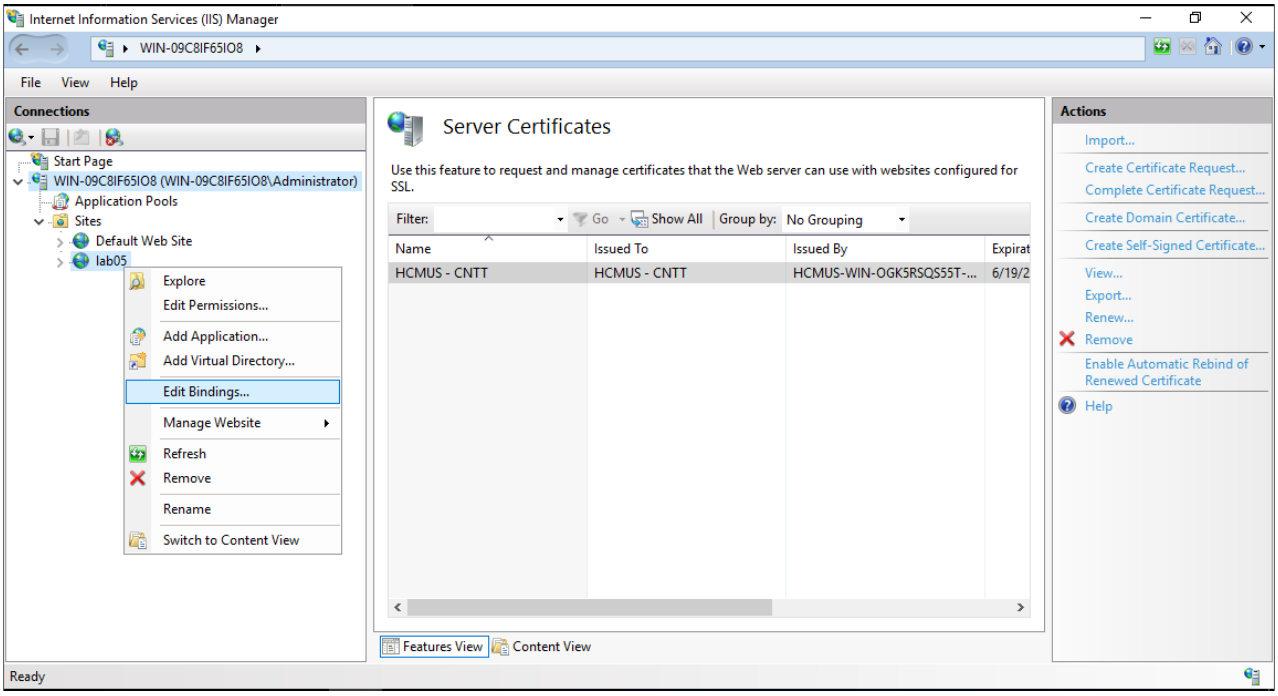
- Thêm file Certificate đã tải và **Friendly Name** tương ứng



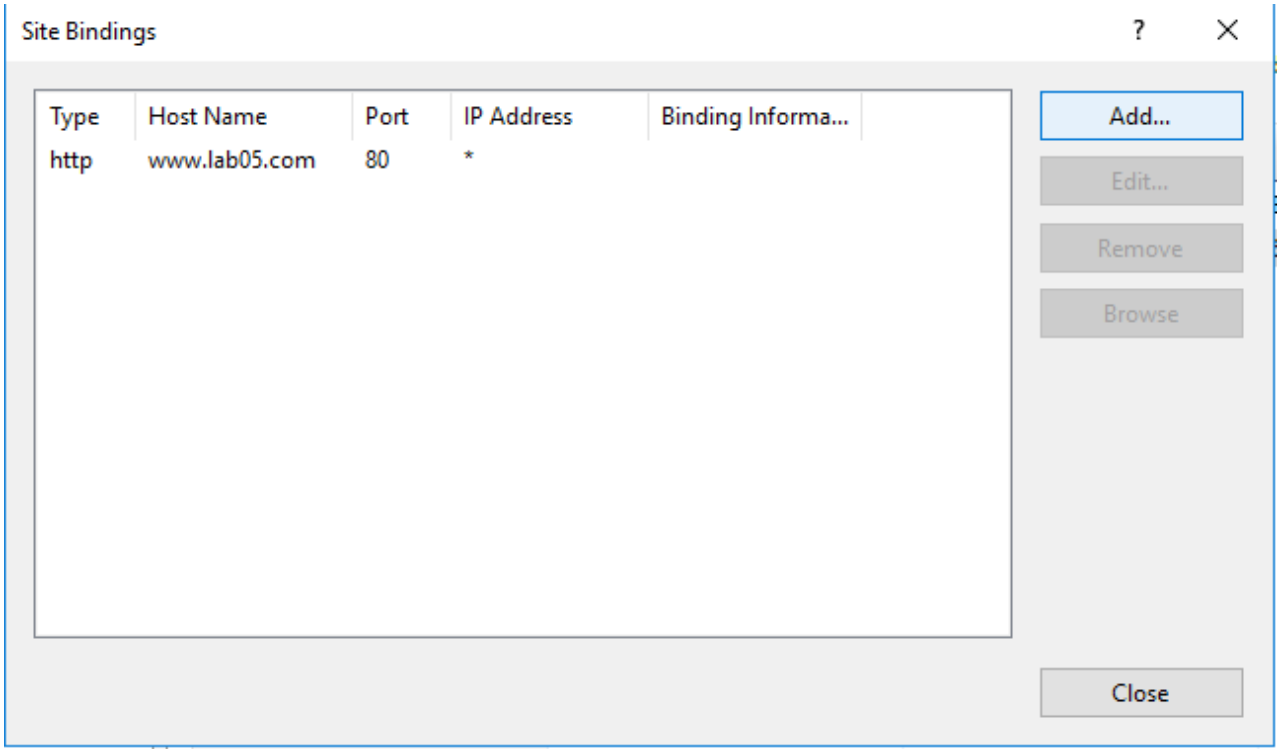
- Thêm thành công



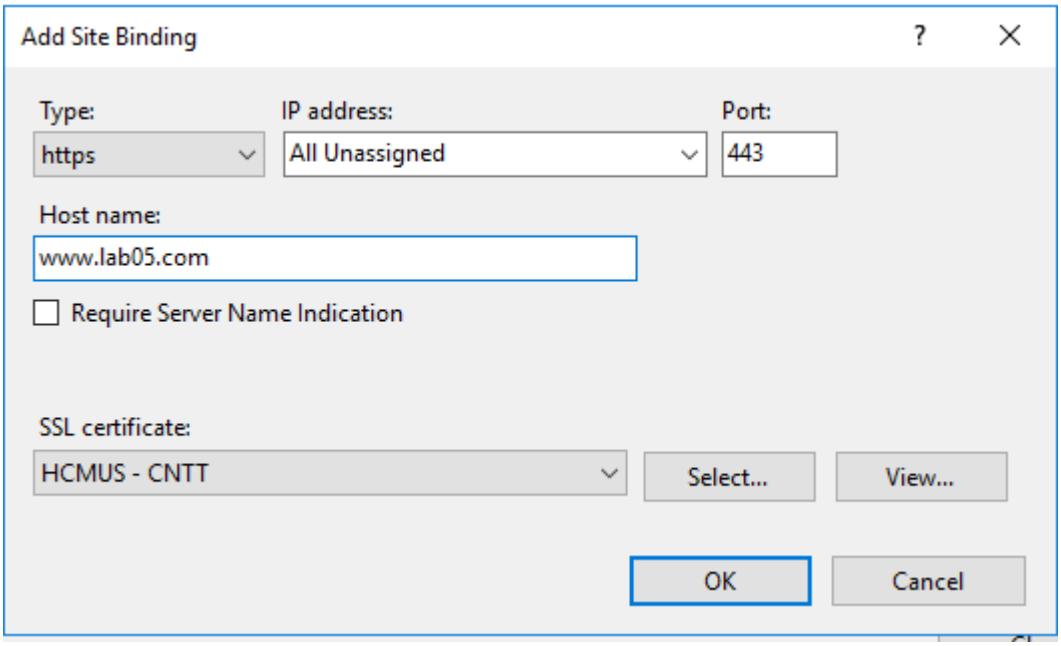
- Cần cấp giao thức cho web www.lab05.com nên ta chọn **lab05 => Edit Bindings…**



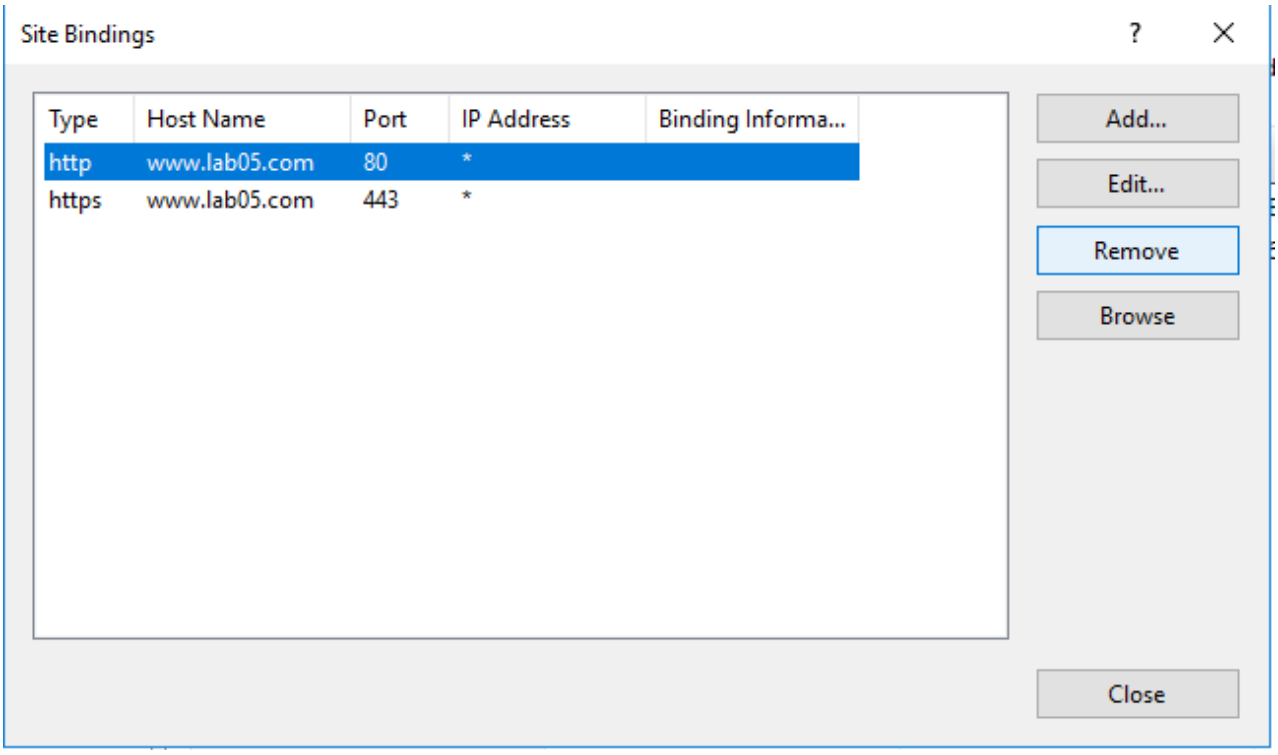
- Chọn **Add**



- Thêm Site Binding với Host name: www.lab05.com
- Type: **https**
- SSL certificate: **HCMUS – CNTT** (vừa được thêm vào)
- Port: **443**



- Ta **Remove** site cũ với giao thức là **http**



II.5.5. Duyệt web an toàn

- Vào trình duyệt trên máy Client (máy thật) và truy cập vào tên miền www.lab05.com hoặc lab05.com đều sử dụng được phương thức **https**
- Tuy truy cập được bằng phương thức **https** nhưng vẫn có cảnh cáo không an toàn là do Certificate cho **https** là do tự mình tạo, không phải là các Certificate phổ biến và thông dụng của các công ty bảo mật lớn cung cấp. Vì vậy, nên máy Client sẽ thiếu Certificate này trong máy và sẽ không hiểu mục đích của Certificate này là gì và đương nhiên sẽ có cảnh báo về bảo mật. Để khắc phục thì máy Client cần phải cài thêm Certificate do mình tạo ra