**Lab 8. Applied Cryptography**

* Lab 5.1. Telnet & SSH
* Lab 5.2. HTTPS
  + Tạo CA server cấp Certificate cho máy chủ web server
  + Cấu hình Web server để truy cập Website qua giao thức HTTPS

**Lab 1. Telnet & SSH**



**Telnet:**

* **Configure IP addresses**
* **Configure telnet (Router)**

R(config)#line vty 0 4

R(config-line)#password 123456

R(config-line)#login

* **Enable password:**

R(config)#enable password 111111

(Hoặc R(config)#enable secret 222222)

**Ssh:**

* **Configure IP addresses**
* **Configure hostname & domain-name**

R(config)#hostname R1

R(config)#ip domain-name hcmute.edu.vn

* **Set console and enable password**

R(config)#line console 0

R(config-line)#password 123456

R(config-line)#login

R(config)#enable password 654321

* **Tạo khóa (RSA)**

R(config)#crypto key generate rsa

* **Setup line vty**

R(config)#line vty 0 4

R(config-line)#transport input ssh

R(config-line)#login local

* **Tạo account cho đăng nhập SSH**

R(config)#username admin password 111111

* Kiểm tra cấu hình

C:\> ssh –l <username> <IP>

(show ip ssh)

* Lab .2. HTTPS
  + Tạo CA server cấp Certificate cho máy chủ web server
  + Cấu hình Web server để truy cập Website qua giao thức HTTPS

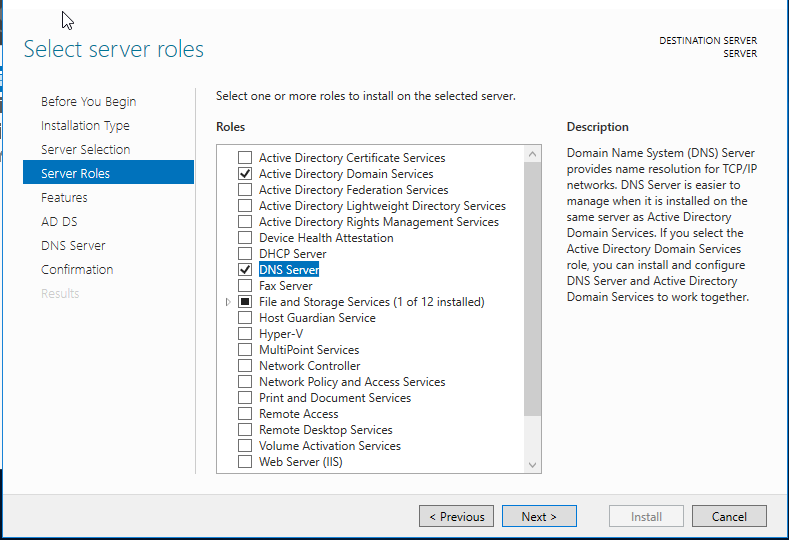
**Bước 1. Tạo CA server**

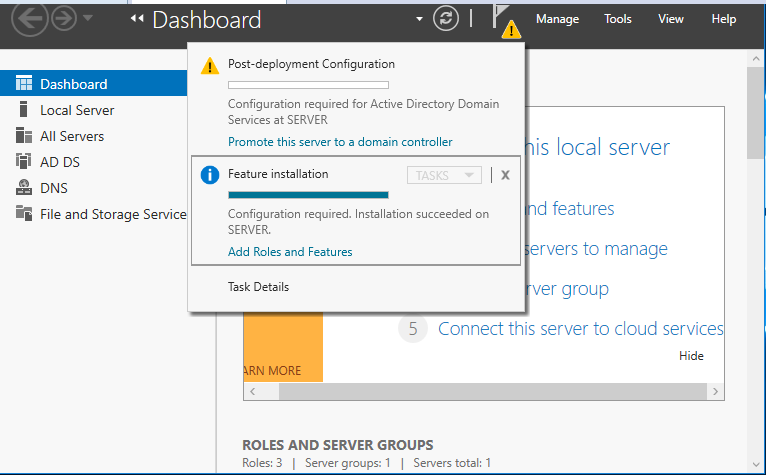
**Cài máy chủ làm Domain Controller (XYZ.COM) để cấp CA**

**Thông tin máy làm CA server:**

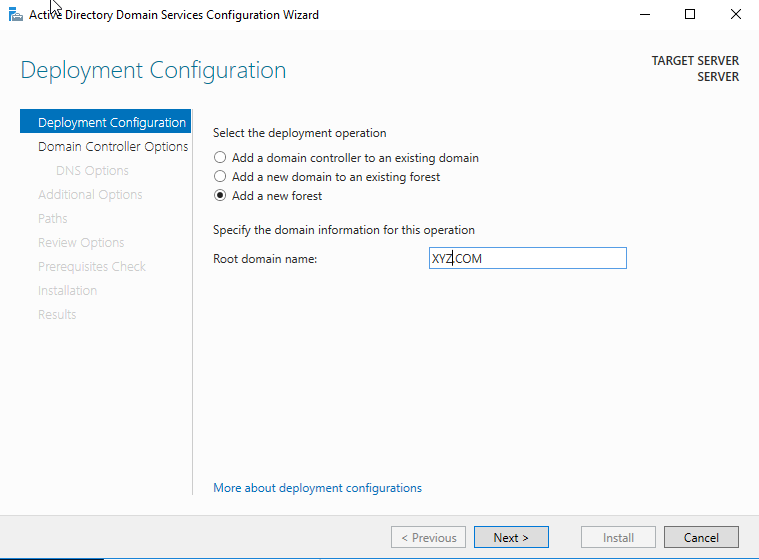
1. **Nâng cấp lên DC**

* IP address: 192.168.12.254
* Subnet mask: 255.255.255.0
* DNS server: 192.168.12.254

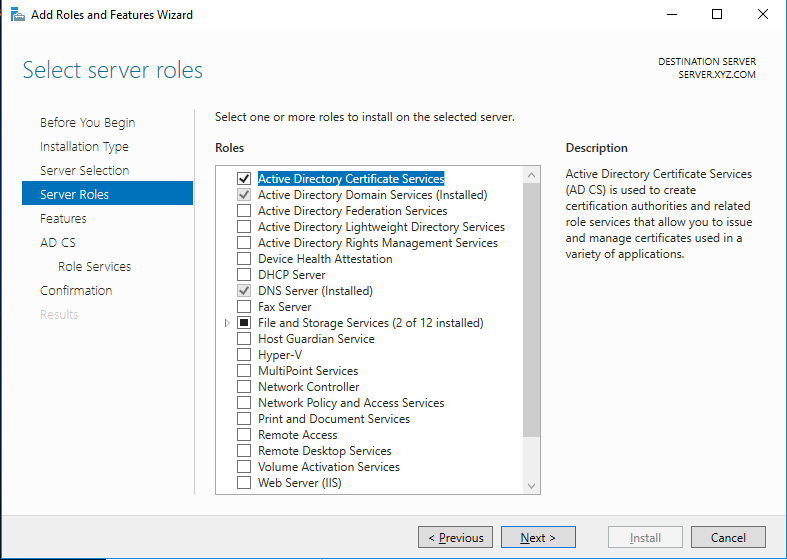


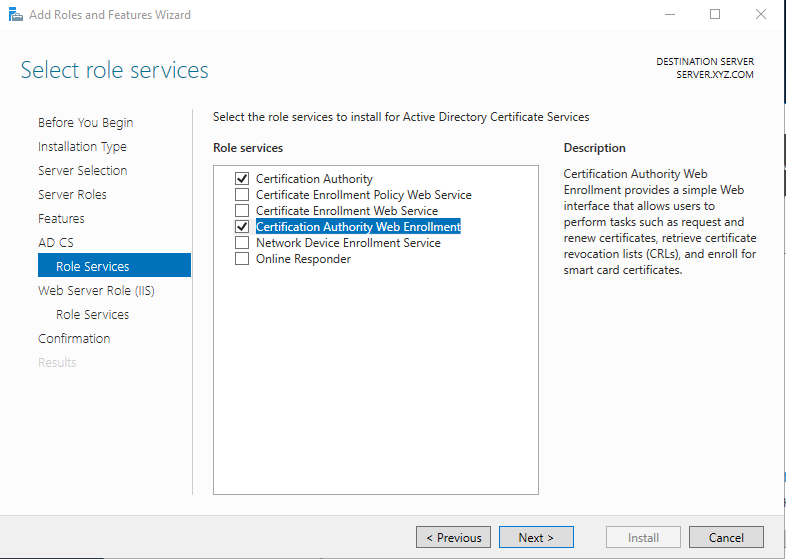


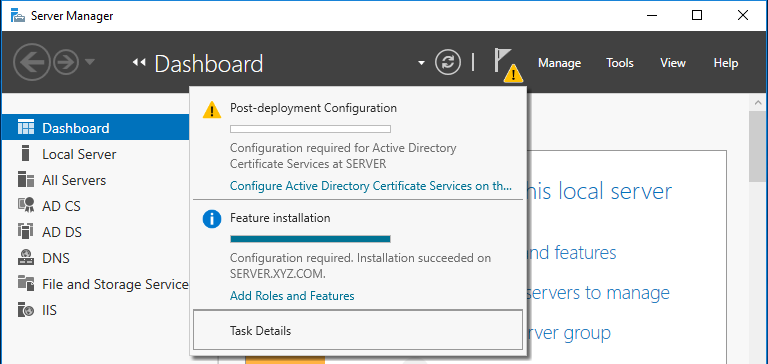
**Chọn Promote this server to a domain controller**

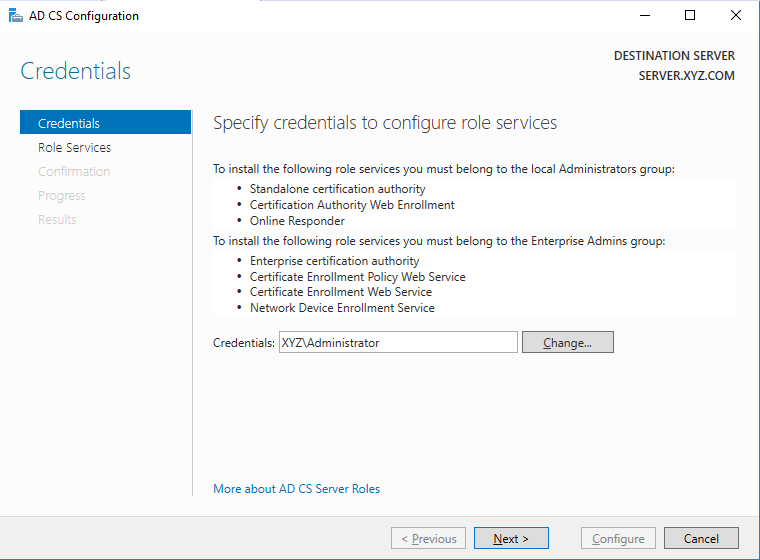


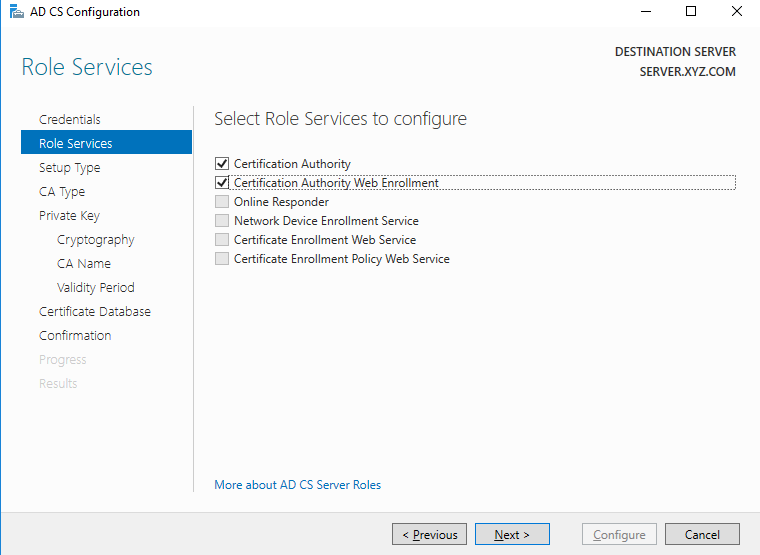
1. **Cài Active Directory Certificate Services**

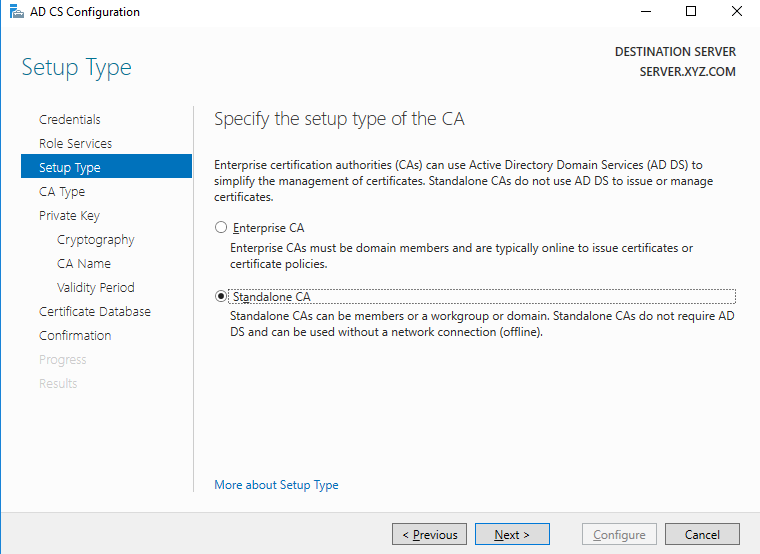


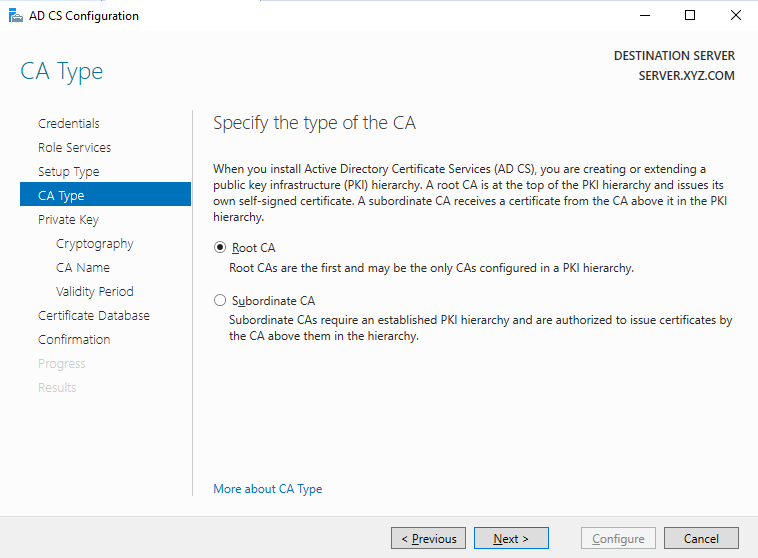


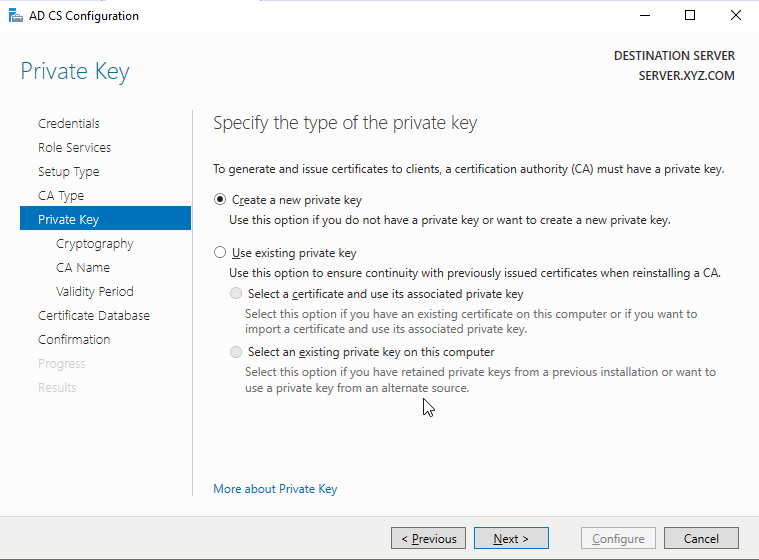


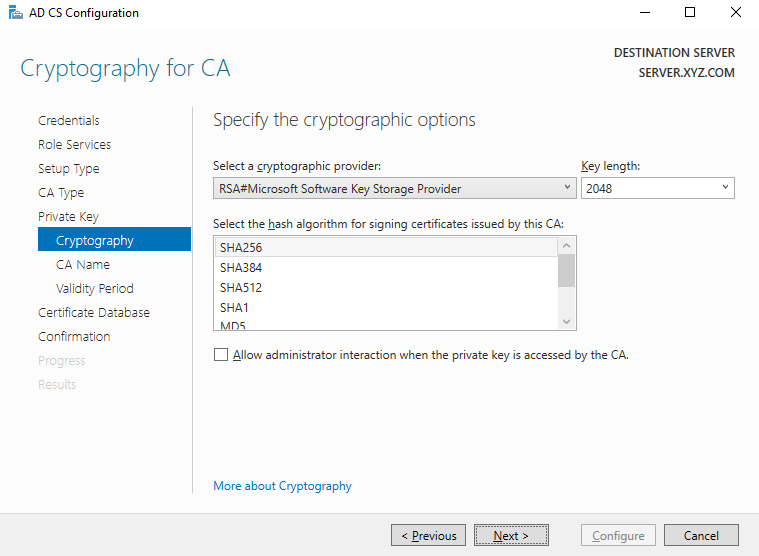


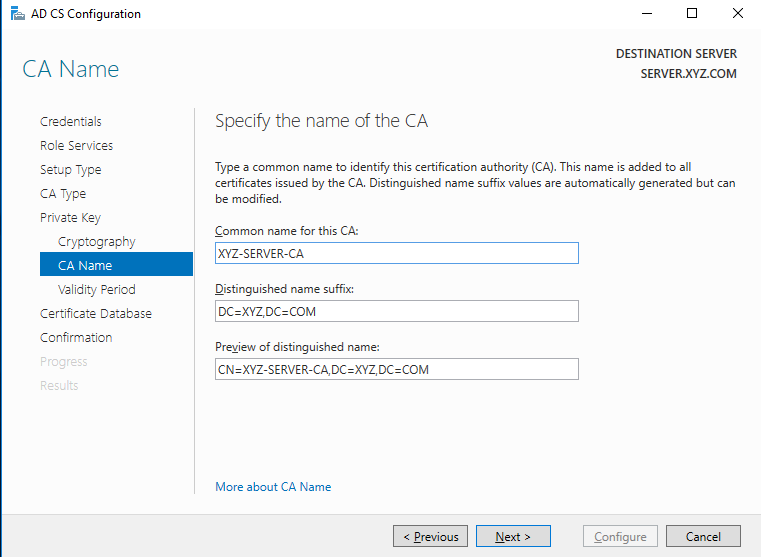


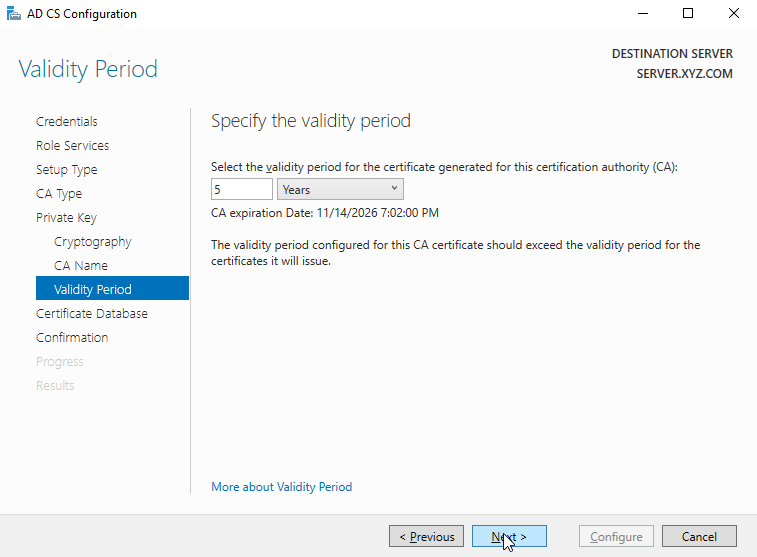


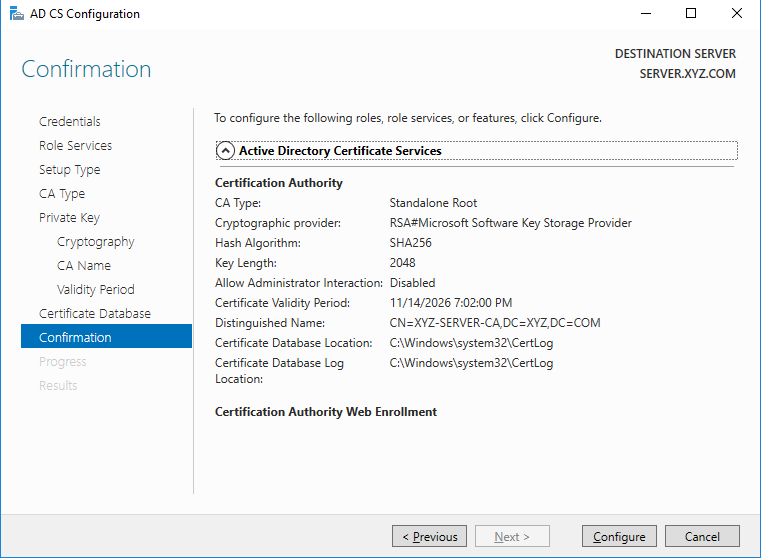


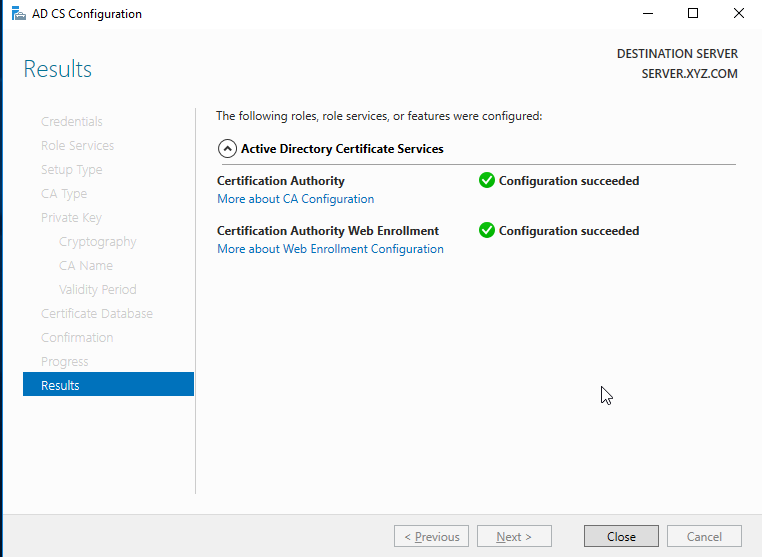




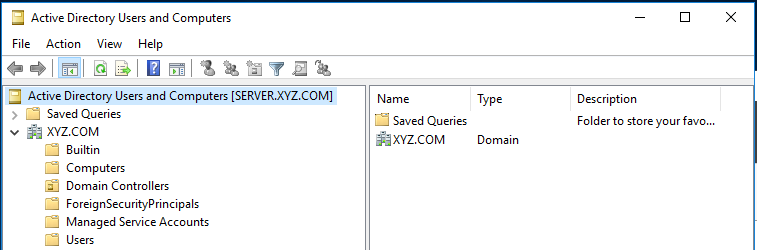


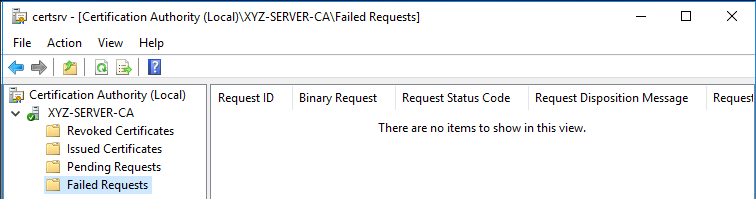






**Kết quả:**





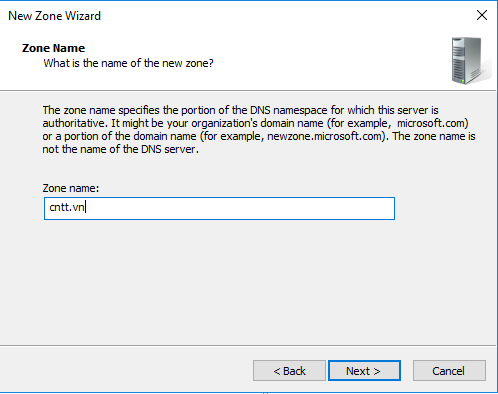
**Bước 2.** Máy Server: [www.cntt.vn](http://www.cntt.vn)

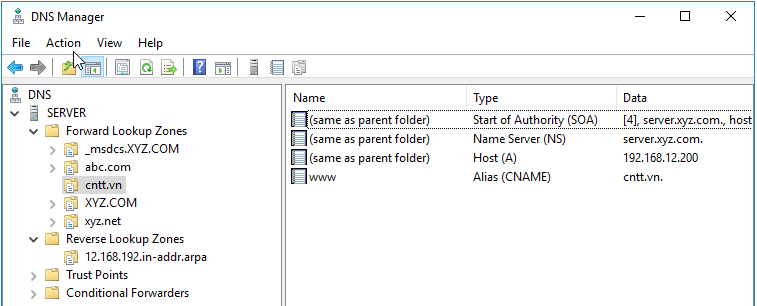
Cấu hình máy **Web Server (192.168.12.200)**

DNS server: **192.168.12.254** (Máy CA server)

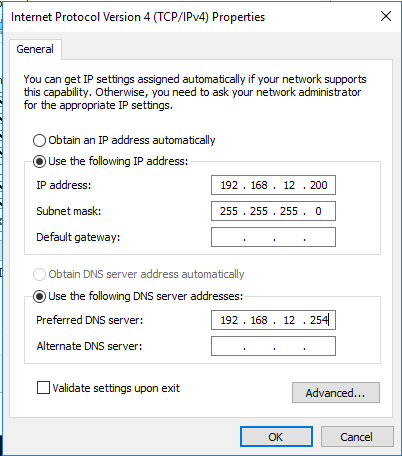
Tên miền: [www.cnttt.vn](http://www.cnttt.vn)

Cấu hình DNS cho

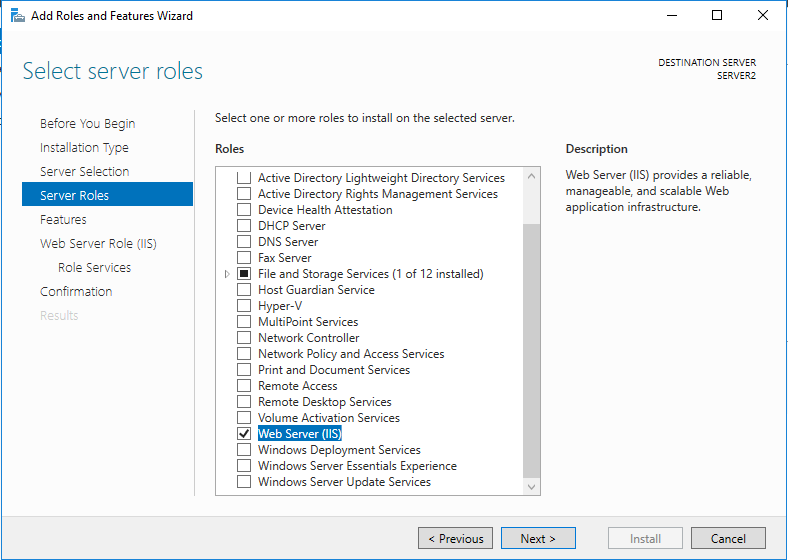


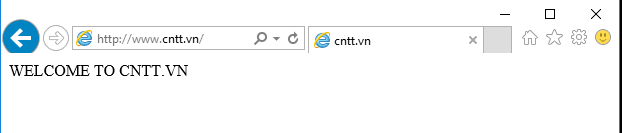


**Máy Web server**

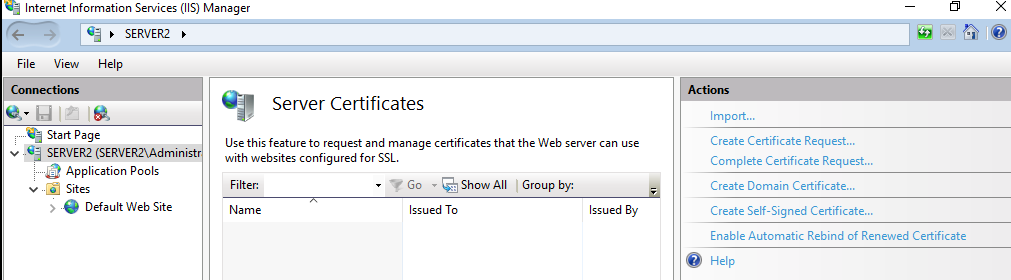


Cài dịch vụ Web server

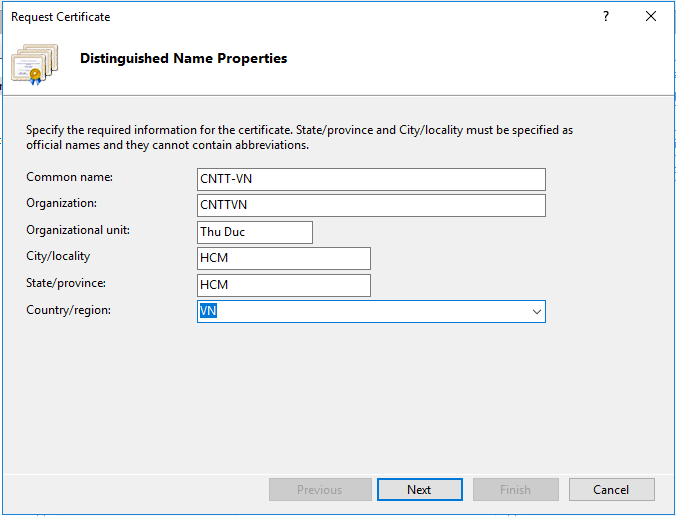


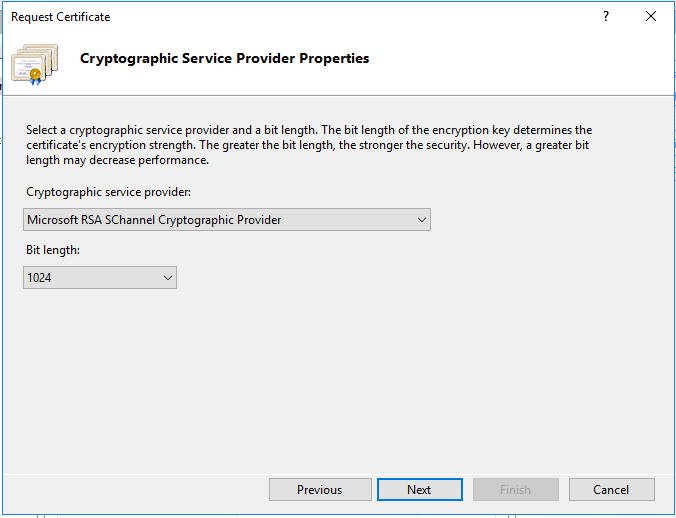


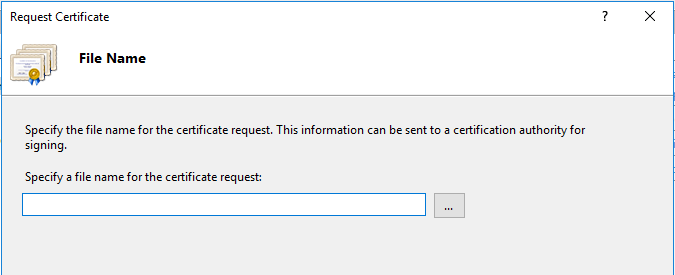
Cấu hình SSL



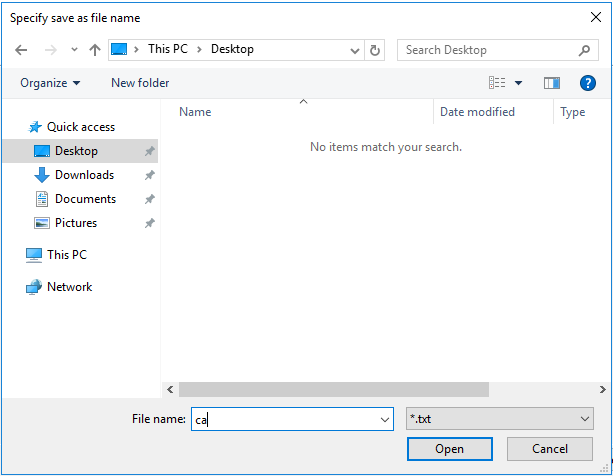
Click Create Certificate Request

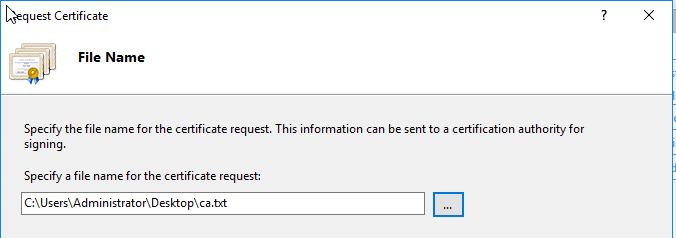




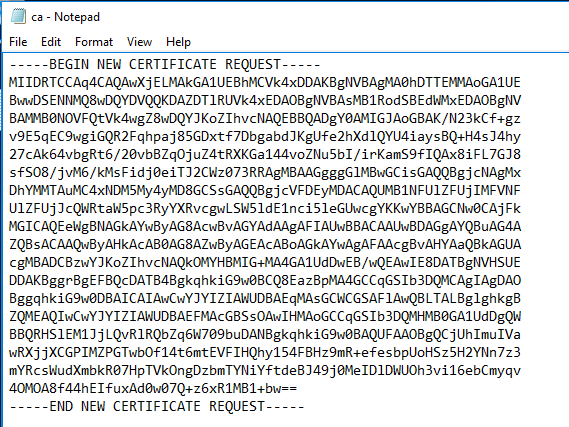


Click vào dấu …

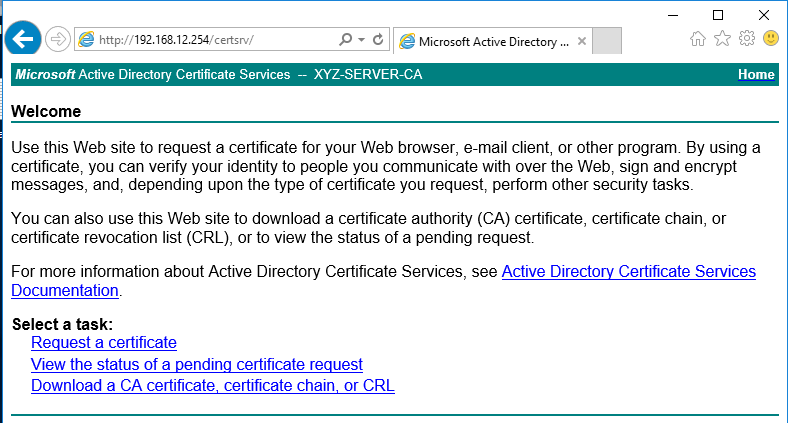




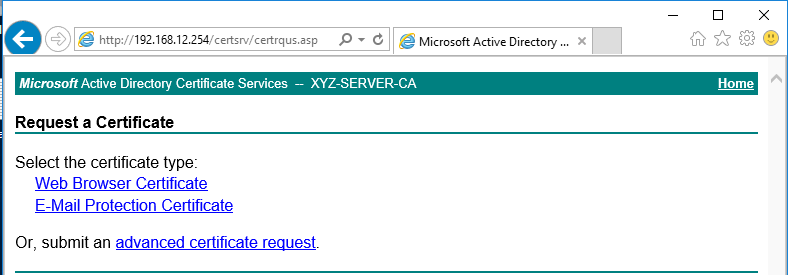
File ca.txt



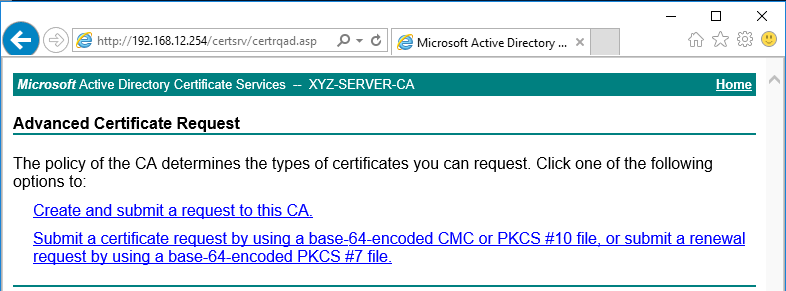
Truy cầp vào CA server: <http://192.168.12.254/certsrv>



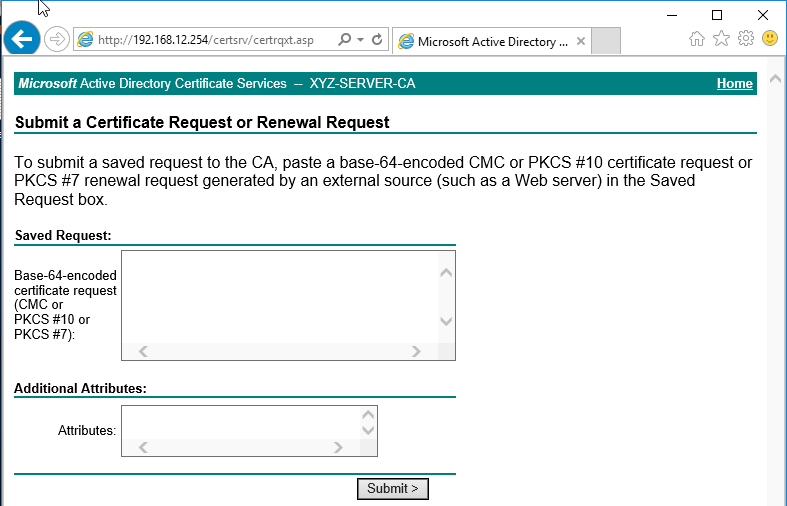
Chọn Request a certificate



Chọn advanced certificate request

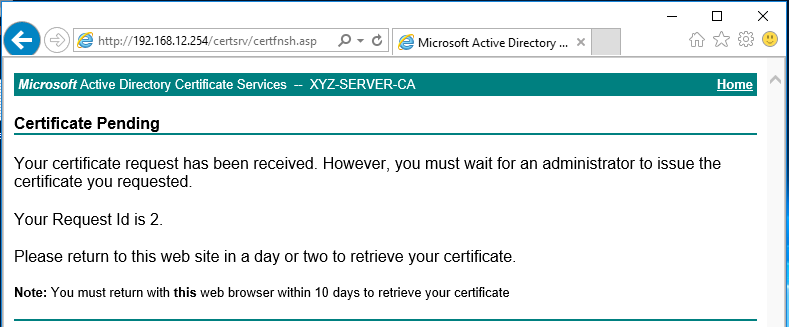


Chọn Submit a certificate by using …

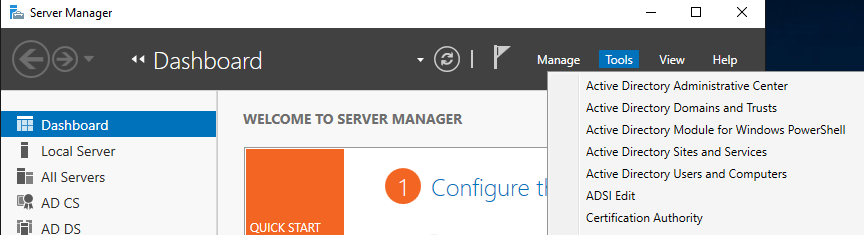


Mở và copy nội dung trong file ca.txt bỏ vào mục Base-64….

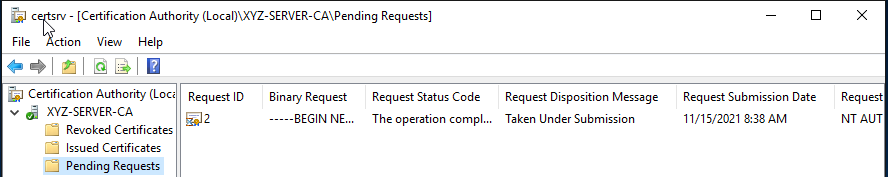
Click Submit



Step . Trên máy CA Server

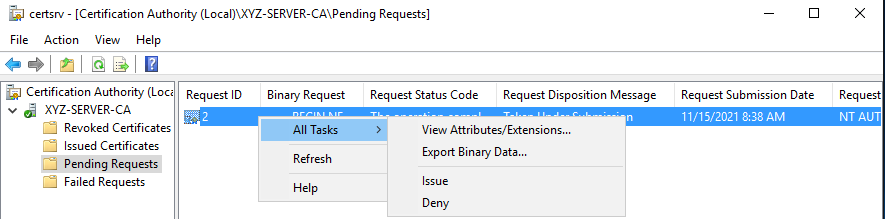


Mục Certification Authority

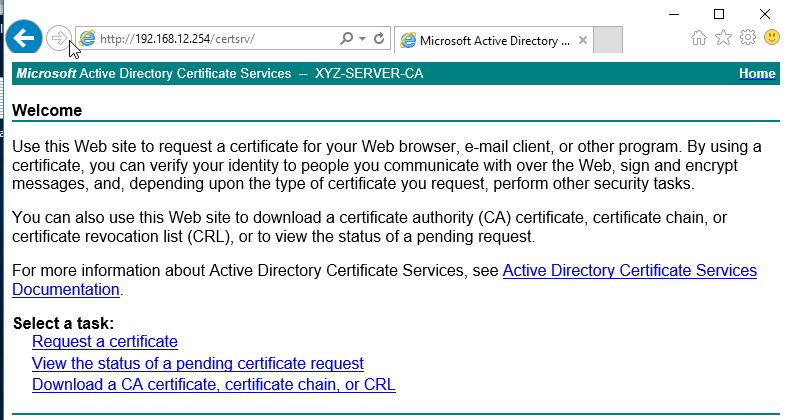


Mục Pending Requests

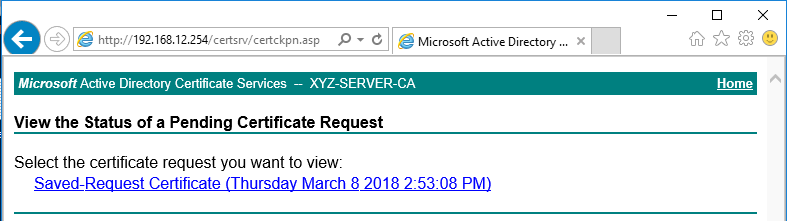
Right click 🡪 All tasks/Issue



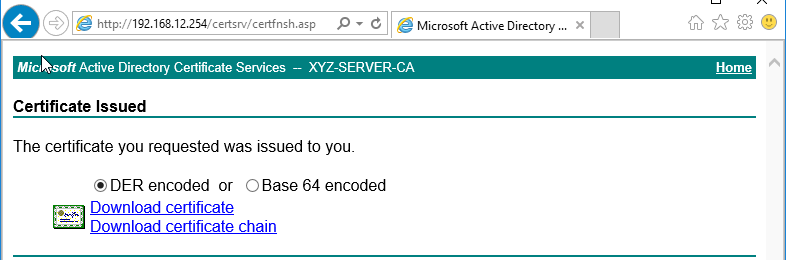
Step. Về lại máy Web server 🡪 download chứng chỉ về máy



Click View the status of a pending certificate request

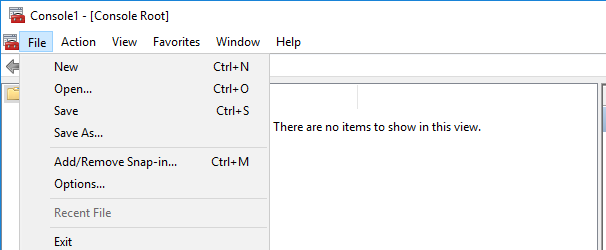


Click Save

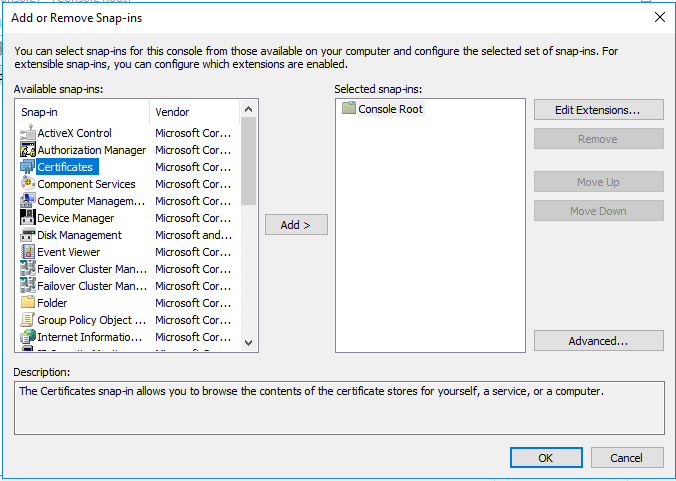


Download cả 2 về máy

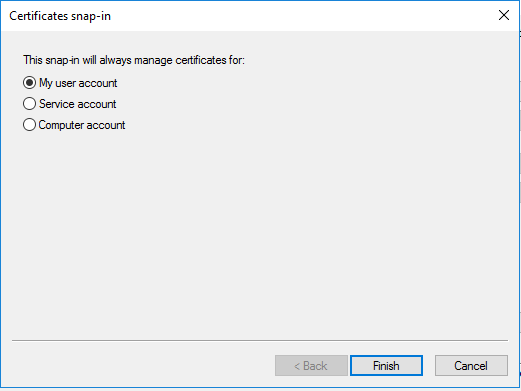
Vào Run 🡪 mmc



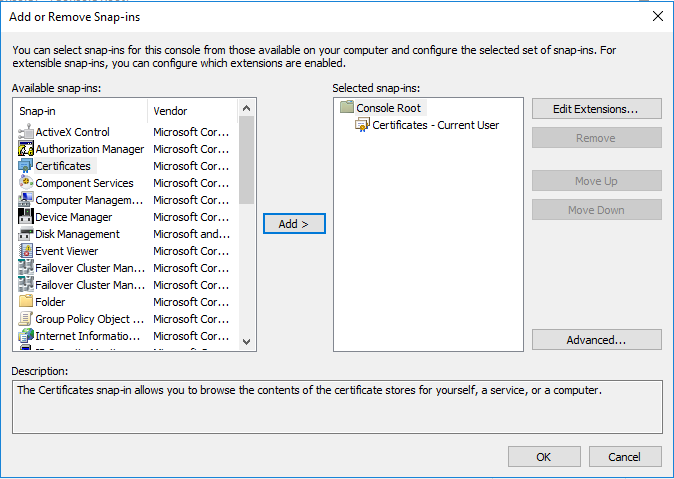
File 🡪 Add/Remove Snap-in…



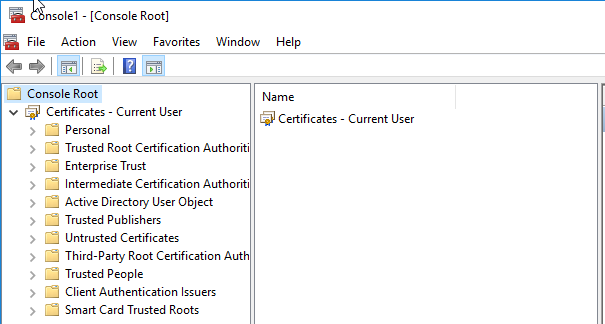
Chọn Certificate 🡪 Add



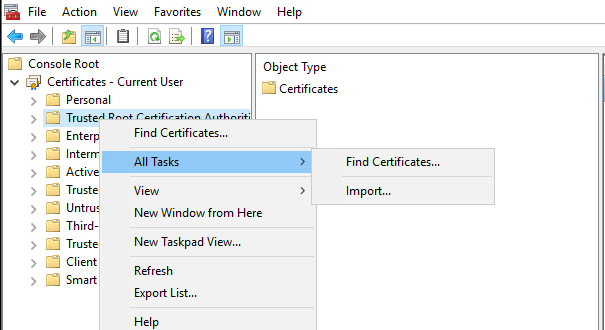
Chọn My user account



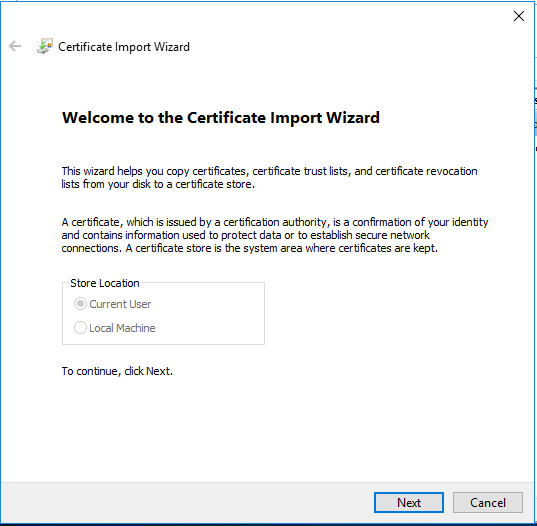
* OK

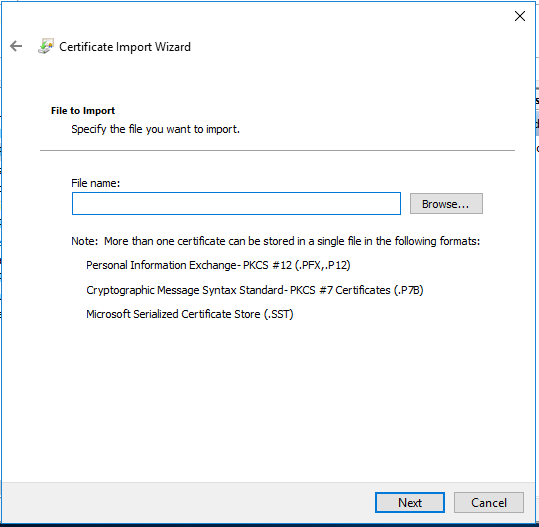


Chọn Trust Root Certificate Authority….

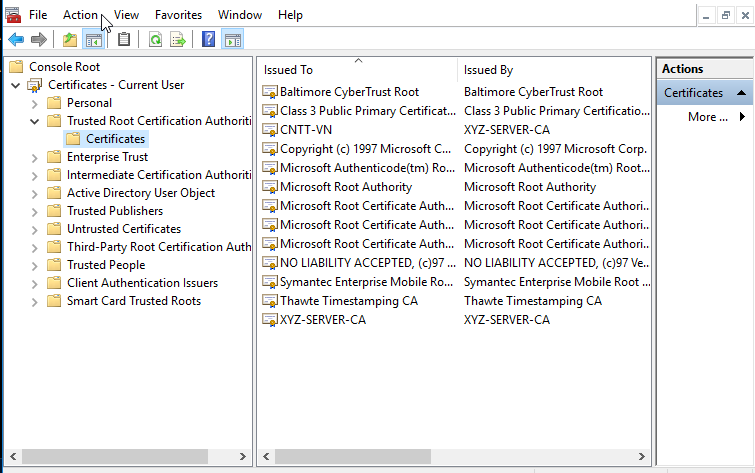


Import

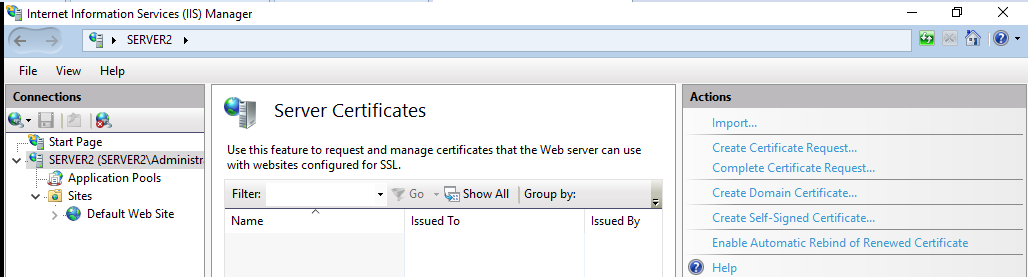




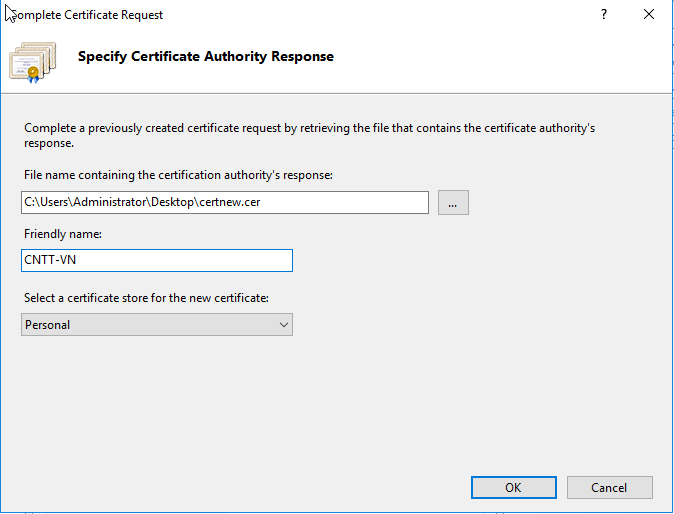
Chọn Browser… lần lượt import 2 file đã tải về lúc trước.



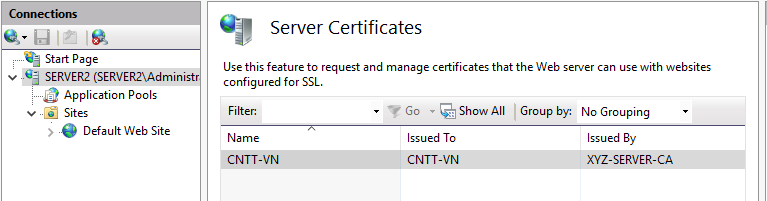
Mở lại cửa sổ IIS



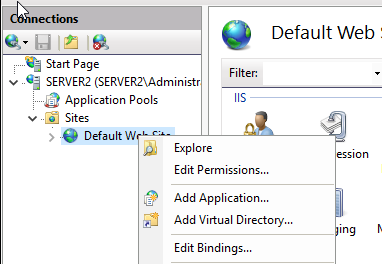
clickComplete Certificate Request



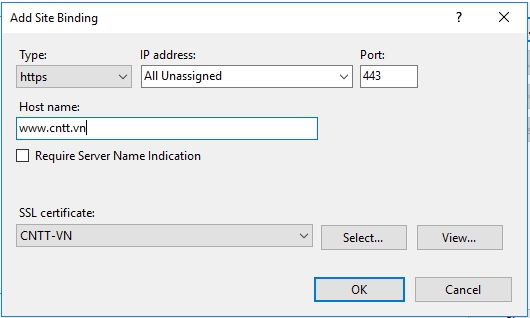
Browser tới file .cer và điền Friendly name:

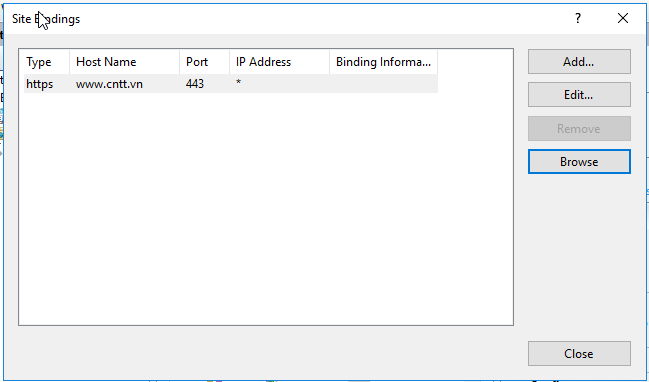


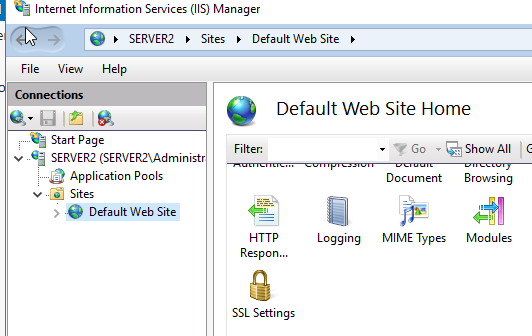
Cấu hình Web server sử dụng SSL



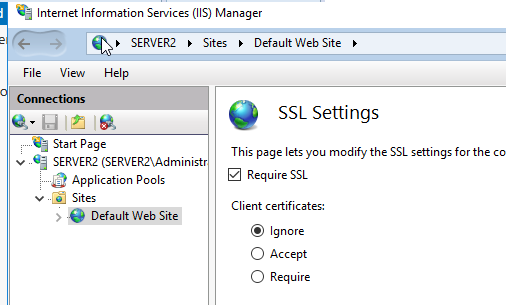
Chọn Edit bindings…







Chọn SSL Settings



Check vào mục Require SSL

Test https

