

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG
KHOA CÔNG NGHỆ THÔNG TIN



QUẢN TRỊ HỆ THỐNG MẠNG

Người thực hiện:
Nguyễn Dư Thành Long - 52100976
Đinh Phương Mỹ - 52100703
Đặng Minh Phong - 52100987

Nhóm: 20

Giảng viên hướng dẫn:
Lê Viết Thanh

THÀNH PHỐ HỒ CHÍ MINH – 2023

LỜI CẢM ƠN

Nhóm 20 xin được gửi lời cảm ơn đến thầy Lê Viết Thanh đã tận tình giảng dạy và giúp đỡ nhóm trong việc hoàn thành bài tập, cũng như hiểu vấn đề của môn học đề ra.

Với những kiến thức nhóm 20 tích lũy được qua những ngày học tập, đây là kết quả của quá trình học tập của nhóm. Tuy vẫn còn nhiều mặt còn hạn chế, nhưng nhóm 20 sẽ cố gắng để đạt được kết quả tốt nhất có thể.

ĐỒ ÁN CUỐI KỲ ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Nhóm 20 xin cam đoan đây là bài báo cáo sản phẩm đồ án cuối kỳ chỉ của riêng nhóm. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa được công bố dưới bất kỳ hình thức nào. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đề tài còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc rõ ràng và cụ thể.

Nếu phát hiện có bất kỳ sự gian lận nào nhóm 20 xin hoàn toàn chịu trách nhiệm về nội dung của bài đồ án cuối kỳ Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền trong quá trình thực hiện của em.

TP. Hồ Chí Minh, ngày 30 tháng 11 năm 2023

Sinh viên thực hiện,

Nguyễn Dư Thành Long

Dinh Phương Mỹ

Đặng Minh Phong

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ

Phần đánh giá của giảng viên chấm bài:

.....
.....
.....
.....
.....

TP. Hồ Chí Minh, ngày.... tháng.... năm 2023
Giảng viên chấm bài,

Phần đánh giá của giảng viên hướng dẫn:

TP. Hồ Chí Minh, ngày.... tháng.... năm 2023
Giảng viên hướng dẫn,

Mục lục

1 Lý thuyết	5
1 Các khái niệm	5
2 Tính năng	6
3 Cách thức hoạt động	6
4 Tầm quan trọng	8
2 Thực hành	10
1 Nội dung	10
2 Thực hành trên GUI	12
2.1 Cài đặt Active Directory Domain	12
2.2 Cài Active Directory Certificate Services	27
2.3 Kiểm tra	50
3 Thực hành trên PowerShell	51
3.1 Cài đặt Active Directory Domain Controller	51
3.2 Cài Active Directory Certificate Services role	58
3.3 Kiểm tra	66
3 Kết luận	70

Chương 1

Lý thuyết

1 Các khái niệm

- Certificate Services (Dịch vụ chứng chỉ): Là một dịch vụ trong hệ thống Public Key Infrastructure (PKI) được sử dụng để quản lý và cấp phát chứng chỉ số (digital certificates). Chứng chỉ số đóng vai trò quan trọng trong việc xác thực và bảo mật thông tin trong các môi trường mạng, tạo điều kiện cho việc sử dụng khóa công cộng và khóa riêng tư.
- Public Key Infrastructure (PKI): Là một hệ thống bao gồm phần cứng, phần mềm, con người, chính sách và thủ tục, tất cả nhằm mục đích tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi các chứng chỉ số (digital certificates). Được sử dụng để đảm bảo tính bảo mật, xác thực và toàn vẹn của thông tin trong quá trình truyền thông.
- Digital Certificates (Chứng chỉ số): Là một thành phần quan trọng của PKI, chứng chỉ số là một loại tài liệu số được ký bởi một Certificate Authority (CA) để xác nhận danh tính của một đối tượng (người dùng, máy tính, hay thiết bị) và kèm theo khóa public của họ. Mục đích chính của digital certificates là thực hiện các nhiệm vụ bảo mật như xác thực, mã hóa và giữ tính toàn vẹn của dữ liệu trong một môi trường mạng.

- Certificate Authority (CA - Tổ chức chứng chỉ): Là một tổ chức tin cậy có trách nhiệm quản lý quá trình cấp phát chứng chỉ số. CA ký chứng chỉ số bằng cách sử dụng khóa riêng tư của mình, cung cấp chứng minh về tính hợp lệ và tin cậy của chứng chỉ.

2 Tính năng

- Cấp phát chứng chỉ
 - Cho phép cấp phát chứng chỉ số cho người dùng, máy client, và máy chủ.
 - Hỗ trợ việc xác định và chứng thực danh tính của các thực thể trong mạng.
- Thu hồi chứng chỉ
 - Hỗ trợ quá trình thu hồi chứng chỉ khi chúng không còn hợp lệ.
 - Đảm bảo tính an toàn và tin cậy bằng cách ngăn chặn sử dụng chứng chỉ đã bị thu hồi.
- Sử dụng các Certificate Authorities (CAs)
 - Sử dụng Certificate Authorities để xác thực tính hợp lệ của người dùng và máy tính.
 - Cung cấp chứng chỉ số để chứng minh tính xác thực đó.

3 Cách thức hoạt động

- Yêu cầu chứng chỉ (Certificate Request)
 - Người dùng, máy tính hoặc dịch vụ muốn có một chứng chỉ số để xác nhận danh tính.
 - Một yêu cầu chứng chỉ được tạo, chứa thông tin về thực thể yêu cầu chứng chỉ và thuật toán mã hóa sẽ được sử dụng.

- Gửi yêu cầu đến Certificate Authority (CA): yêu cầu chứng chỉ được gửi đến CA, nơi quyết định liệu yêu cầu này có hợp lệ không.
- Xác nhận và xác định quyền (Validation and Authorization)
 - CA kiểm tra xem yêu cầu có đáp ứng các tiêu chí an toàn và chính xác không.
 - Nếu yêu cầu được chấp nhận, CA xác định quyền hạn cụ thể cho chứng chỉ (ví dụ: thời gian hiệu lực, mục đích sử dụng).
- Tạo chứng chỉ (Certificate Issuance): CA tạo một chứng chỉ mới với thông tin được xác nhận và quyền hạn được xác định.
- Phân phối chứng chỉ (Certificate Distribution)
 - Chứng chỉ mới được gửi trở lại cho thực thể yêu cầu (người dùng, máy tính hoặc dịch vụ).
 - Phương tiện phân phối có thể bao gồm truyền qua mạng, lưu trữ tại nơi nào đó trên mạng, hoặc thậm chí trên một thiết bị vật lý như thẻ thông minh.
- Kiểm tra chuỗi chứng chỉ (Certificate Chain Validation): Thực thể sử dụng chứng chỉ phải kiểm tra chuỗi chứng chỉ để đảm bảo rằng chứng chỉ được ký bởi một CA tin cậy và không bị thu hồi.
- Quản lý chuỗi chứng chỉ (CRL Management): CA duy trì một danh sách chứng chỉ bị thu hồi (CRL), và thực thể sử dụng chứng chỉ kiểm tra xem chứng chỉ có hiệu lực hay không dựa trên CRL.
- Tự động hóa và theo dõi (Automation and Logging)
 - Các quy trình này thường được tự động hóa để giảm công việc quản trị.
 - Sự kiện và hoạt động liên quan đến chứng chỉ thường được ghi lại để giúp theo dõi và phân tích.

4 Tâm quan trọng

- Bảo mật thông tin và tài nguyên: AD CS cung cấp cơ sở hạ tầng chứng chỉ để xác nhận danh tính và bảo vệ thông tin quan trọng trong môi trường doanh nghiệp. Việc sử dụng chứng chỉ giúp ngăn chặn các tấn công giả mạo và đảm bảo an toàn cho dữ liệu quan trọng.
- Quản lý truy cập và quyền hạn: Chứng chỉ được sử dụng để xác định quyền hạn và truy cập đối với người dùng, máy tính và dịch vụ trong hệ thống. Điều này giúp quản trị viên kiểm soát chính xác ai có quyền truy cập vào tài nguyên nào.
- Tuân thủ chuẩn mạng và an toàn: AD CS hỗ trợ các tiêu chuẩn chứng chỉ như X.509, giúp đảm bảo rằng hệ thống tuân thủ các chuẩn mạng và an toàn quốc tế.
- Tự động hóa và giảm công việc quản trị: Quy trình tự động hóa cấp và phân phối chứng chỉ giúp giảm công việc quản trị. Autoenrollment cho phép tự động cấp chứng chỉ cho người dùng và máy tính mà không cần sự can thiệp thủ công nhiều.
- Quản lý chuỗi chứng chỉ và thu hồi chứng chỉ: AD CS giữ cho danh sách chứng chỉ bị thu hồi (CRL) được cập nhật để ngăn chặn việc sử dụng chứng chỉ đã bị thu hồi. Điều này đóng vai trò quan trọng trong việc duy trì tính toàn vẹn và an toàn của hệ thống.
- Hỗ trợ mô hình chứng chỉ tùy chỉnh: AD CS cho phép quản trị viên tạo và quản lý các mô hình chứng chỉ tùy chỉnh, giúp đáp ứng đối với các yêu cầu cụ thể của doanh nghiệp.
- Hỗ trợ cho Elliptic Curve Cryptography (ECC): ECC là một thuật toán mã hóa mạnh mẽ với kích thước chìa khóa nhỏ hơn so với

RSA. AD CS hỗ trợ ECC, cung cấp tính linh hoạt và bảo mật cao hơn.

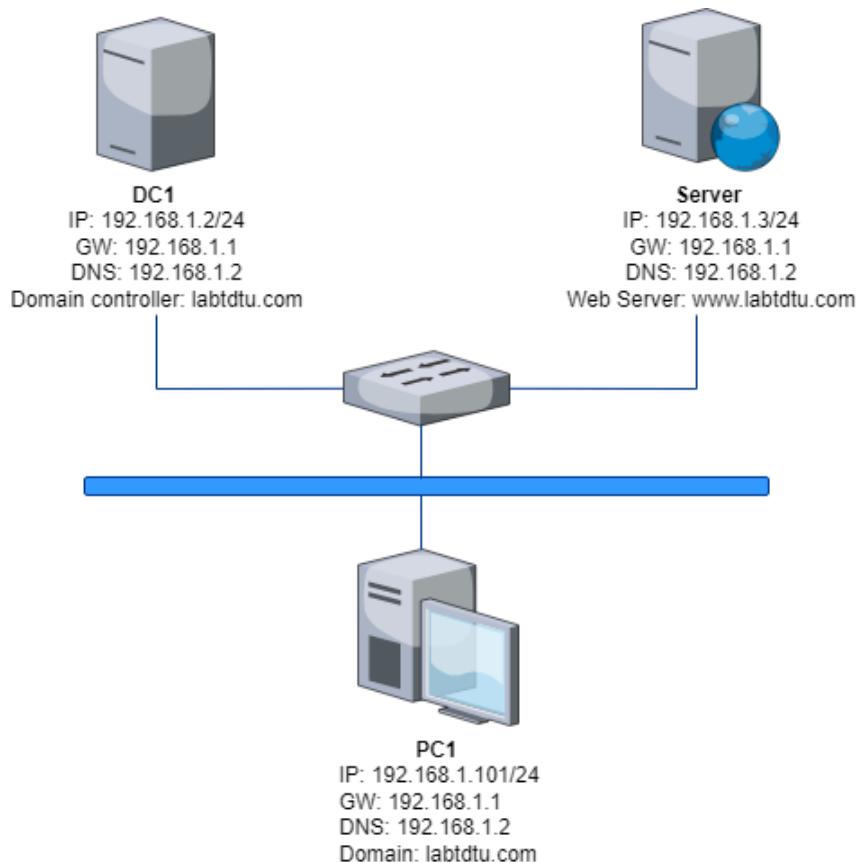
- Quản lý tích hợp với Active Directory: AD CS tích hợp chặc chẽ với Active Directory, giúp quản trị viên quản lý chứng chỉ và quyền hạn một cách hiệu quả trong môi trường Active Directory.

Chương 2

Thực hành

1 Nội dung

- **Yêu cầu:** Sử dụng Active Directory Certificate Services (ADCS) để bảo mật WebServer.
- **Mô hình mạng**



Hình 2.1: Mô hình mạng

- Chuẩn bị

- 2 máy Windows Server 2022 đặt tên lần lượt là DC1 và Server
- 1 máy Windows 8.1 Enterprise đặt tên là PC1.

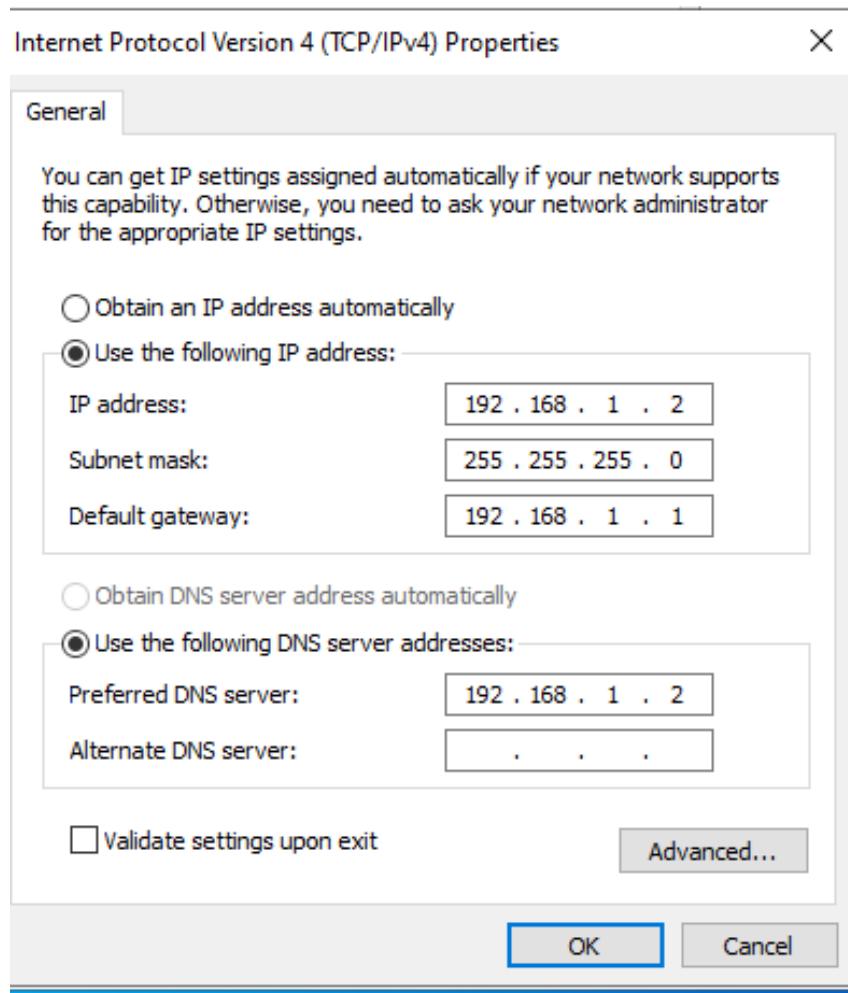
- Các bước thực hiện

- Trên máy DC1, cài đặt Active Directory Domain Controller. Sau đó join máy Server vào domain và PC1 vào domain
- Trên máy Server, cài đặt Active Directory Certificate Services và cấu hình Web Server.
- Đúng trên máy PC1 truy cập vào web site: www.labtdtu.com
- **Chú ý:** Khi thực hiện trên GUI thì các tên máy không đổi nhưng khi thực hiện trên PowerShell các tên sẽ có một chút thay đổi để không bị lẫn lộn, các tên được thay đổi như sau:
 - * DC1 đổi thành FIT-DC
 - * Server đổi thành FIT-WEB
 - * PC1 đổi thành FIT-WIN08-01

2 Thực hành trên GUI

2.1 Cài đặt Active Directory Domain

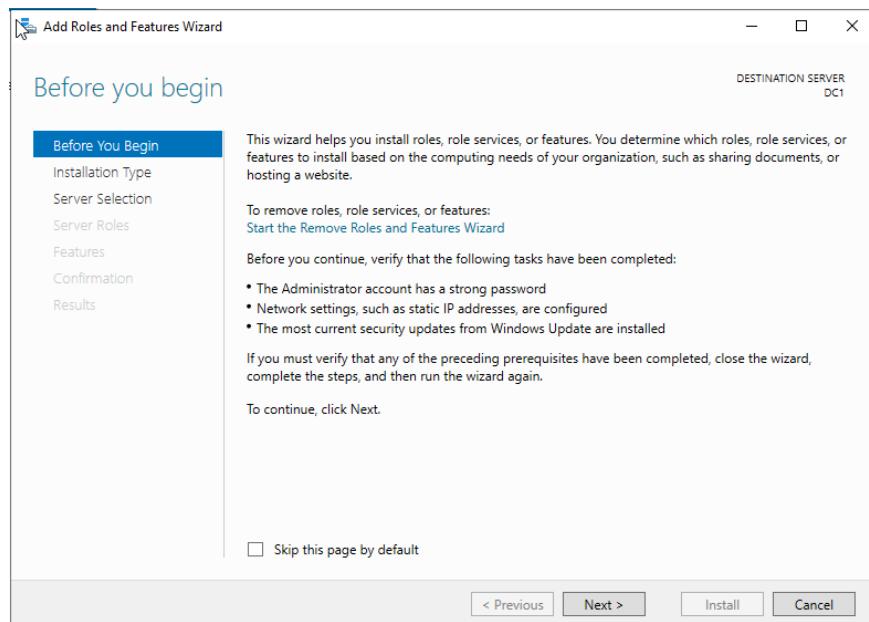
- Trên máy DC1, cài đặt địa chỉ IP tĩnh cho server trước khi thực hiện cài đặt



Hình 2.2: Thiết lập ip cho Domain Controller

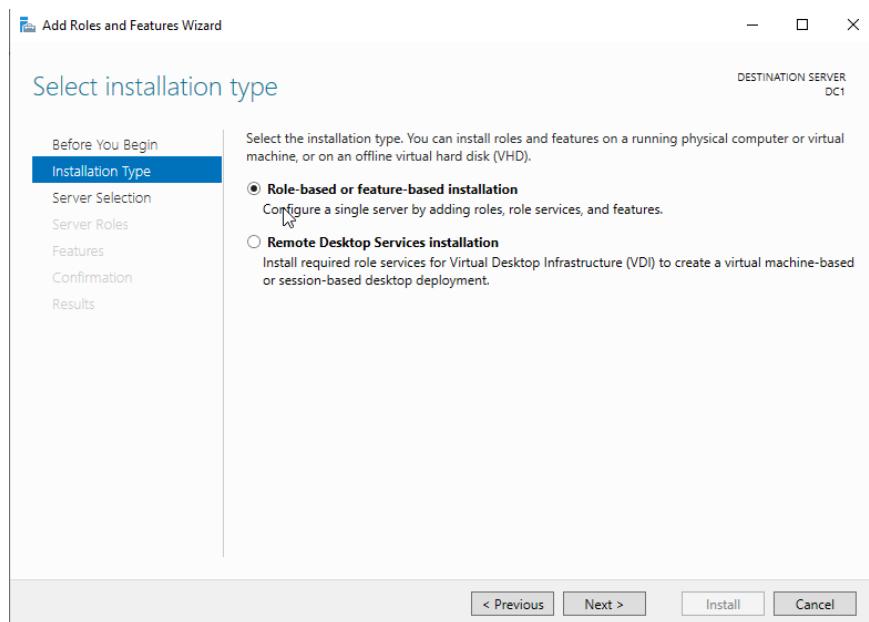
- Chọn menu Start > Administrative Tools > Server Manager. Chọn Roles > Add Roles and Features

- Xuất hiện cửa sổ Before You Begin, chọn Next.



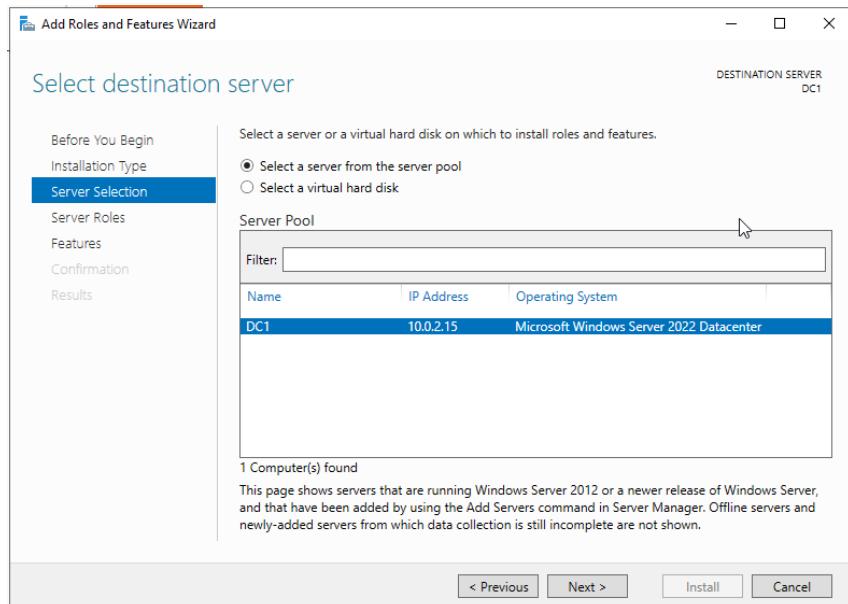
Hình 2.3: Cửa sổ Before You Begin

- Xuất hiện cửa sổ Select Installation Type, chọn Role-based or feature-based installation > Next



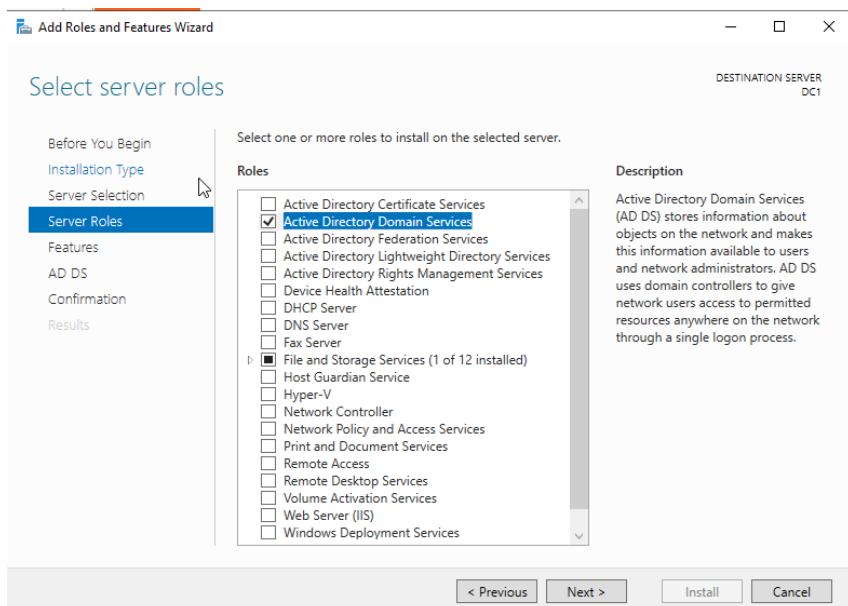
Hình 2.4: Thiết lập ip cho Domain Controller

- Xuất hiện cửa sổ Select Destination Server, chọn Select a server from the server pool > Next



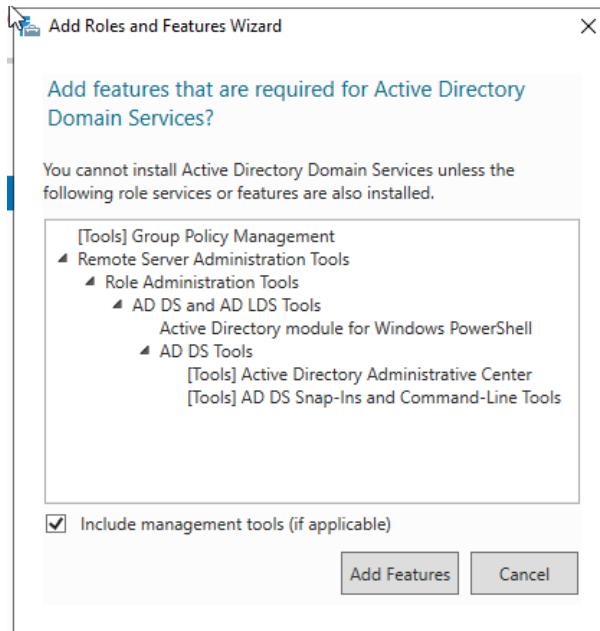
Hình 2.5: Cửa sổ Select Destination Server

- Xuất hiện cửa sổ Select Server Roles, chọn mục Active Directory Domain Services > Next



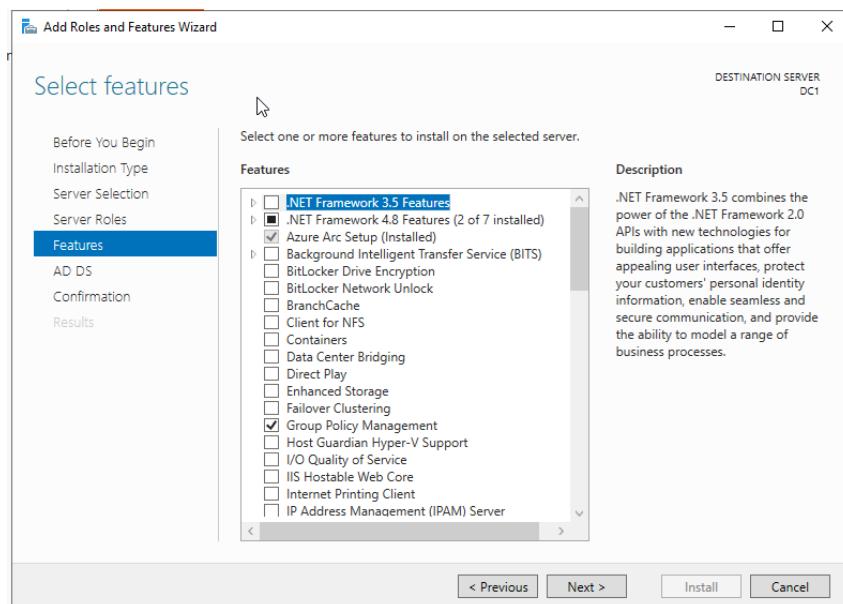
Hình 2.6: Cửa sổ Select Server Roles

- Các tính năng bổ sung được yêu cầu để thêm AD DS. Nhấp vào nút Add Features.



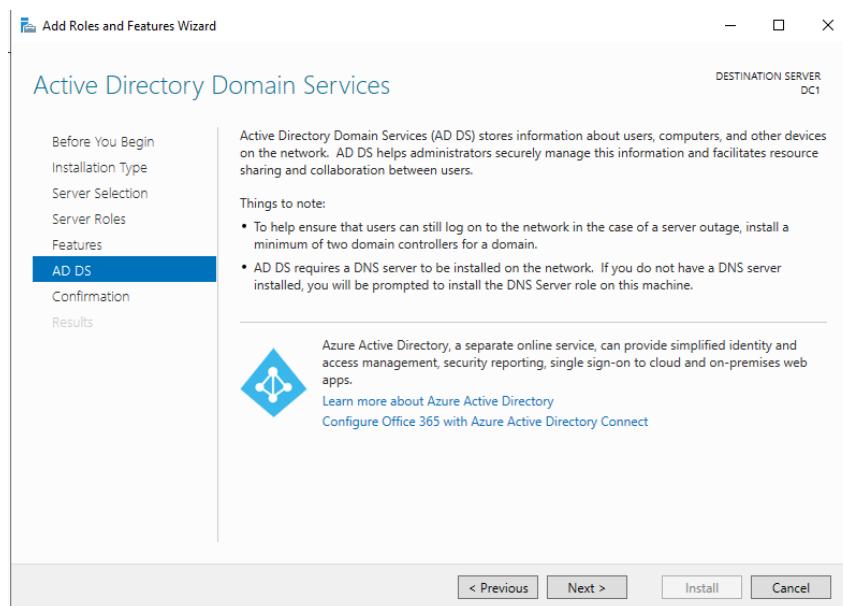
Hình 2.7: Các tính năng bổ sung

- Xuất hiện cửa sổ Select Features, chọn Next.



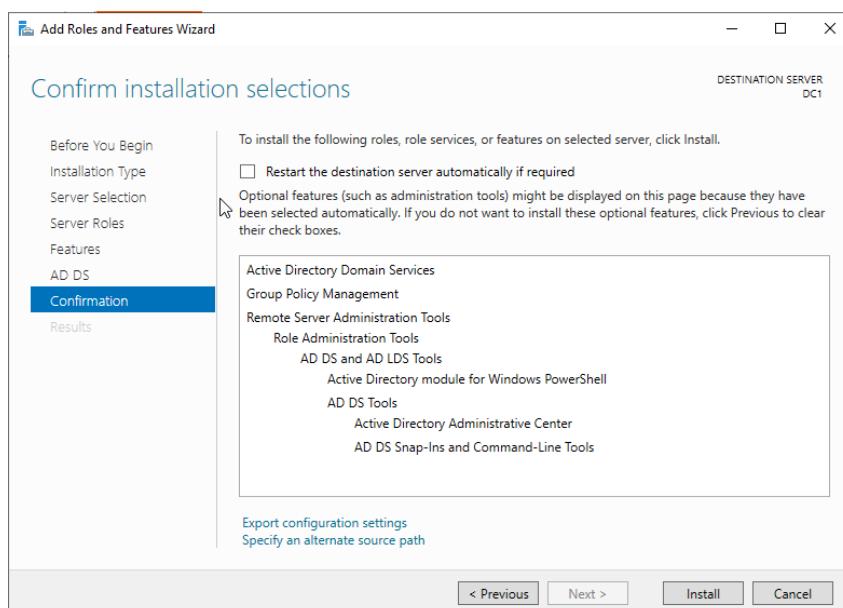
Hình 2.8: Cửa sổ Select Features

- Xuất hiện cửa sổ Active Directory Domain, chọn Next.



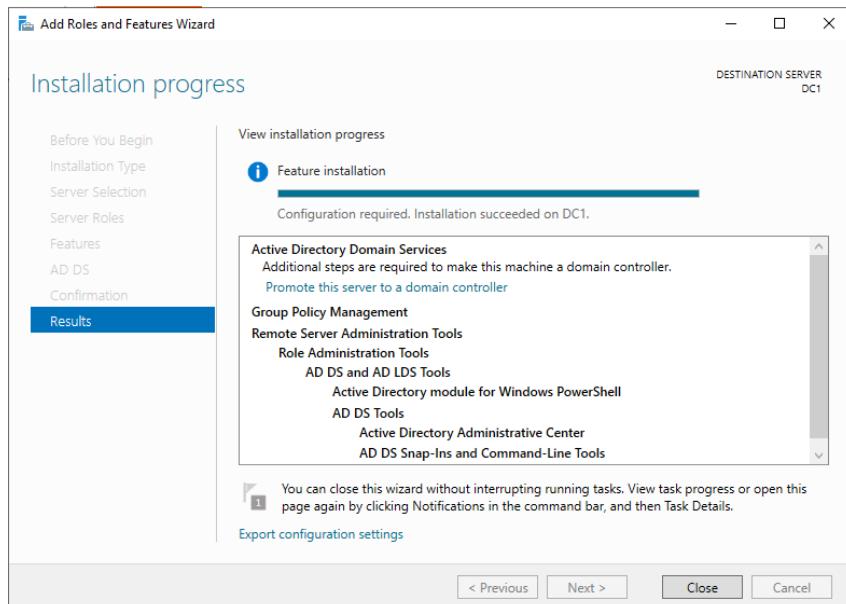
Hình 2.9: Cửa sổ Active Directory Domain

- Xuất hiện cửa sổ Confirm Installation Selections, chọn Server Selection > Next.



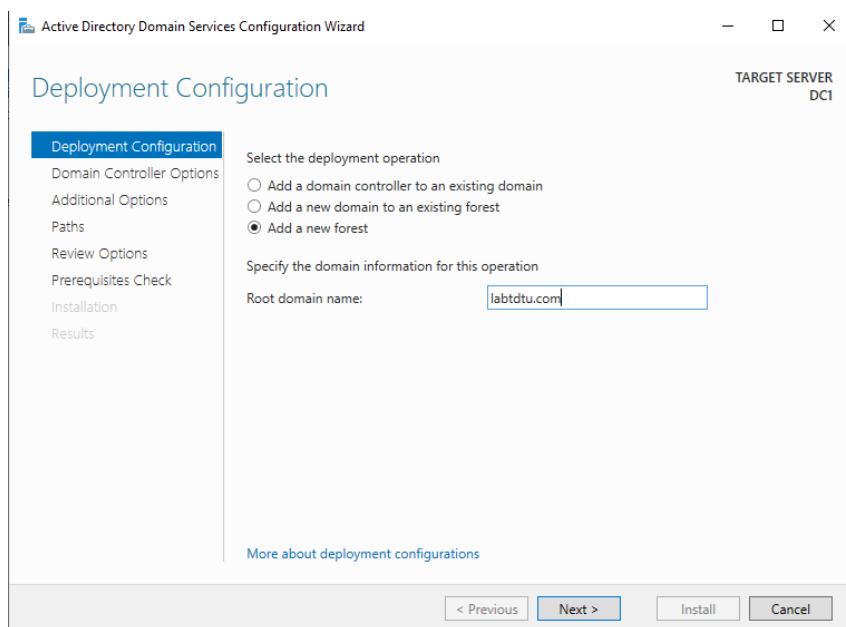
Hình 2.10: Cửa sổ Confirm Installation Selections

- Sau khi cài đặt thành công, chọn Promote this server to a domain controller.



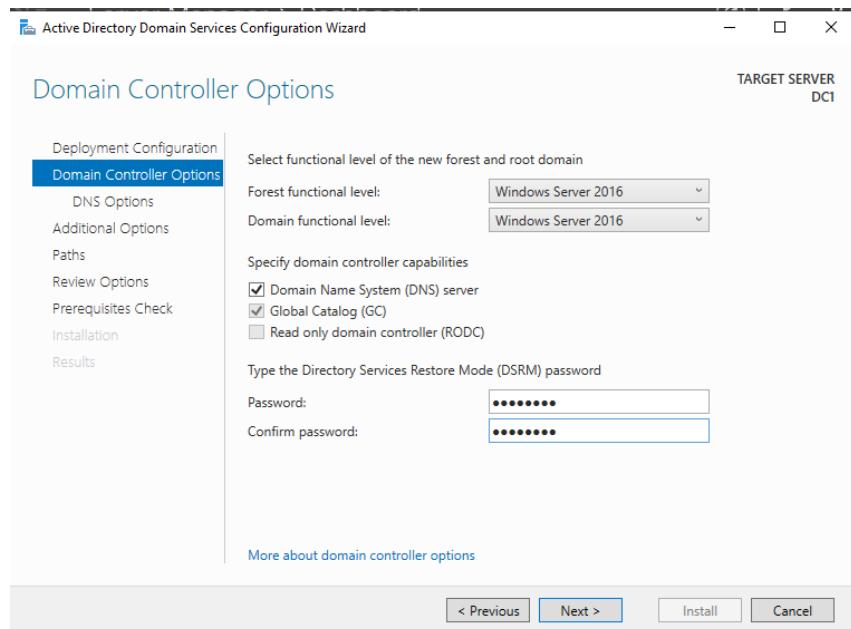
Hình 2.11: Cửa sổ cài đặt thành công

- Xuất hiện cửa sổ Deployment Configuration, chọn Add a new forest > Nhập root domain name “**labtdtu.com**” > Next.



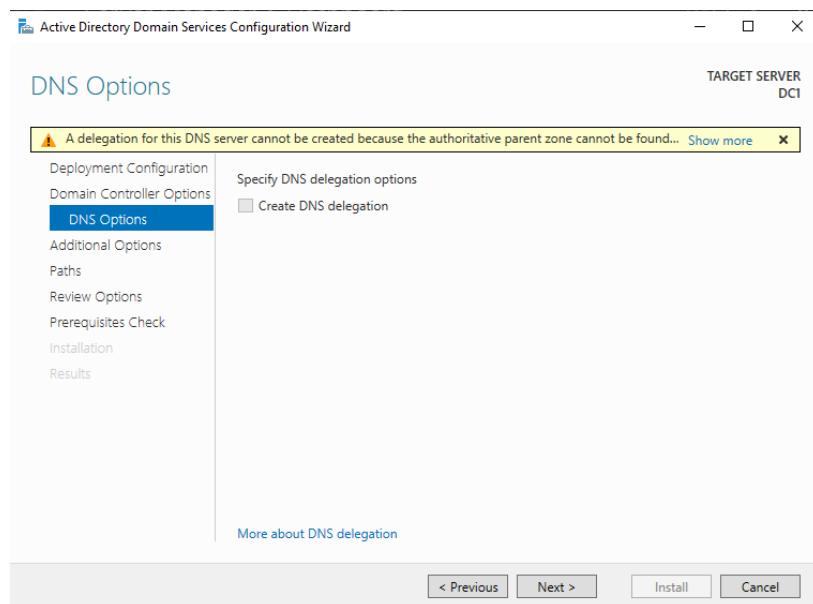
Hình 2.12: Cửa sổ Deployment Configuration

- Xuất hiện cửa sổ Domain Controller Options, nhập password là **P@ssw0rd** > Next.



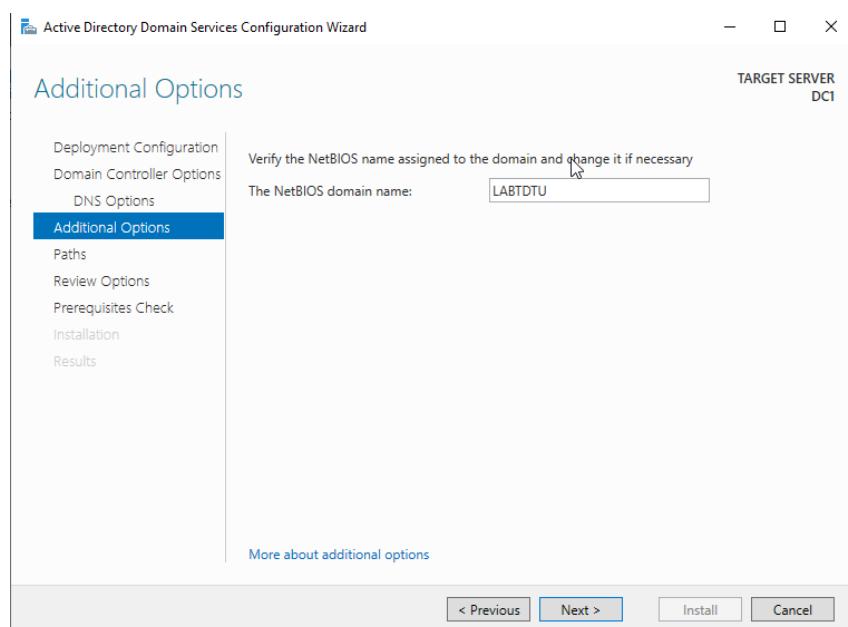
Hình 2.13: Cửa sổ Domain Controller Options

- Xuất hiện cửa sổ DNS Options, chọn Next.



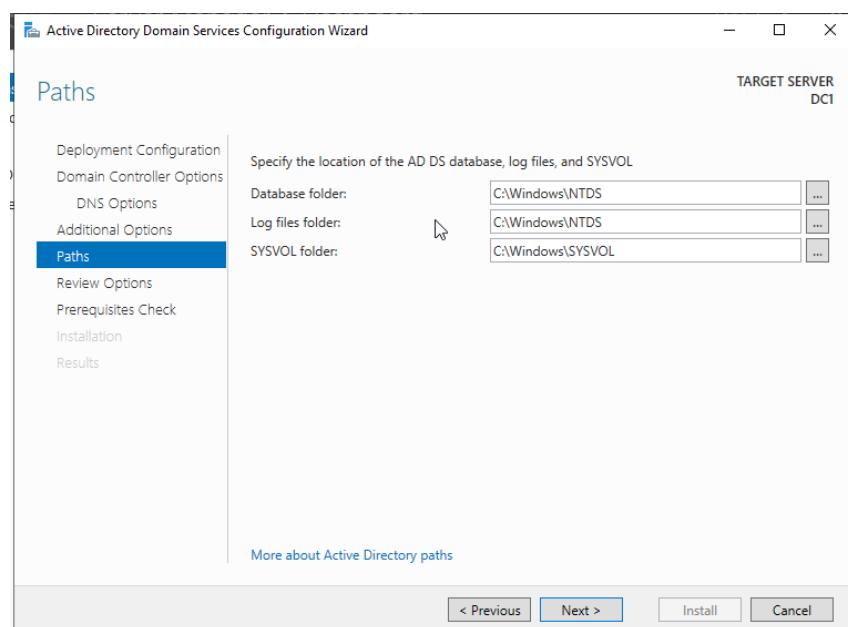
Hình 2.14: Cửa sổ DNS Options

- Xuất hiện cửa sổ Additional Options > Next



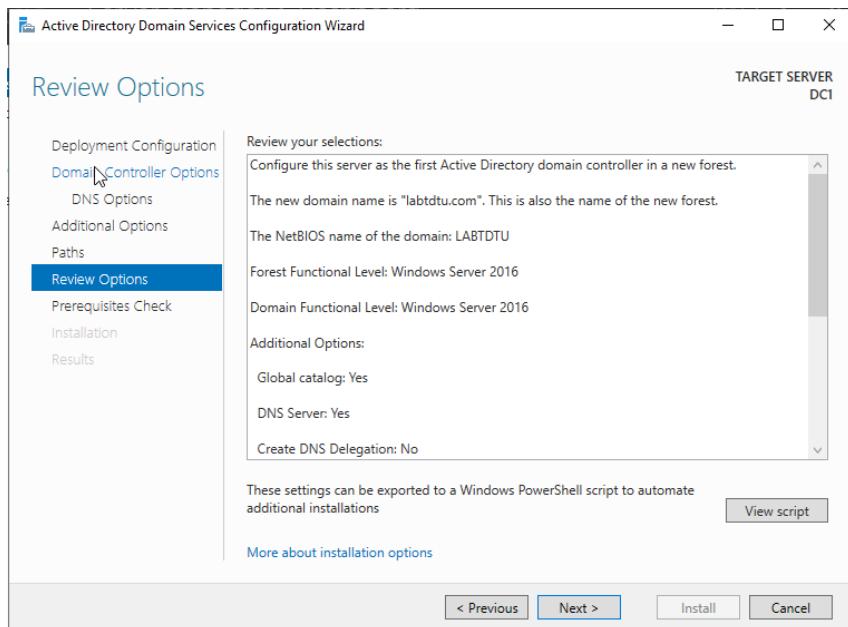
Hình 2.15: Cửa sổ Additional Options

- Xuất hiện cửa sổ Paths > Next.



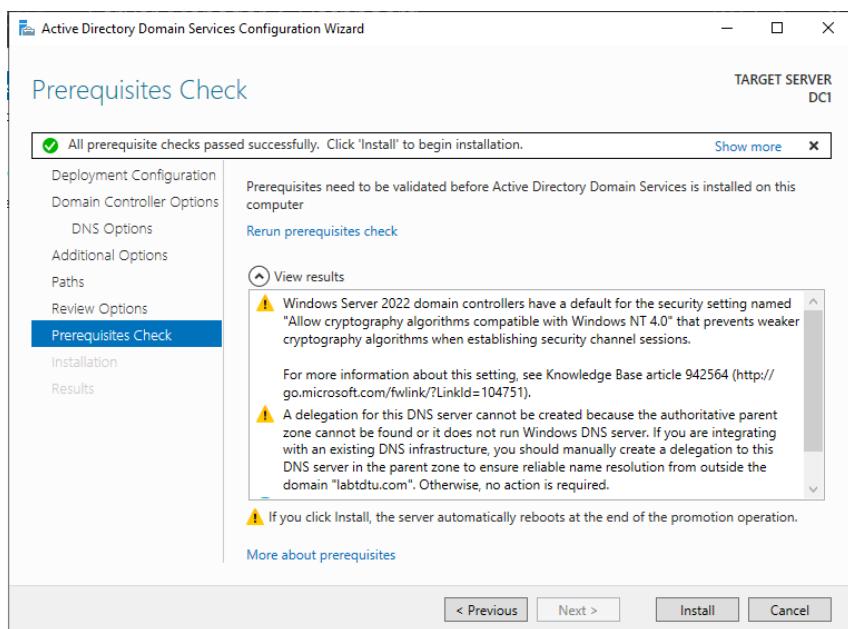
Hình 2.16: Cửa sổ Paths

- Xuất hiện cửa sổ Review Options, sau đó kiểm tra thông tin > Next.



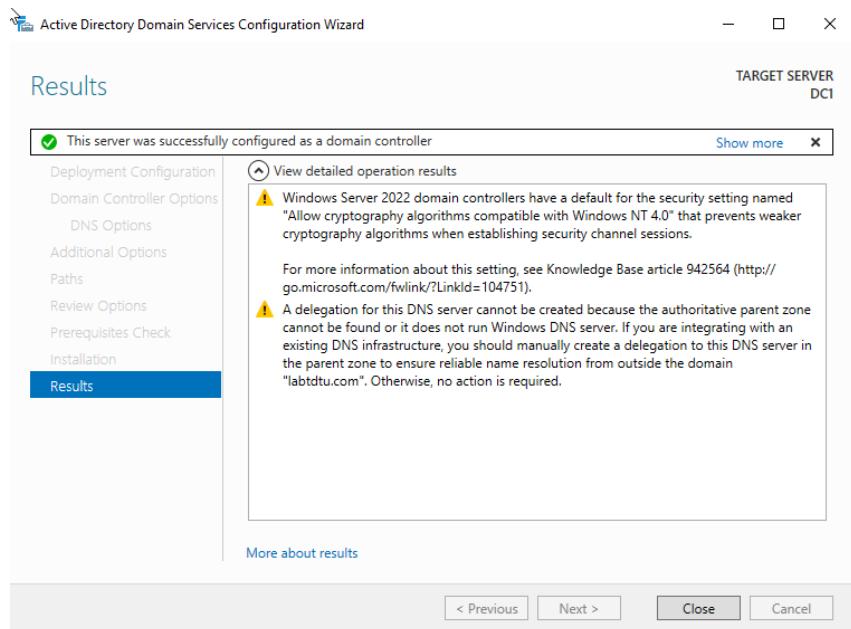
Hình 2.17: Cửa sổ Review Options

- Xuất hiện cửa sổ Prerequisites Check, chọn Install.



Hình 2.18: Cửa sổ Prerequisites Check

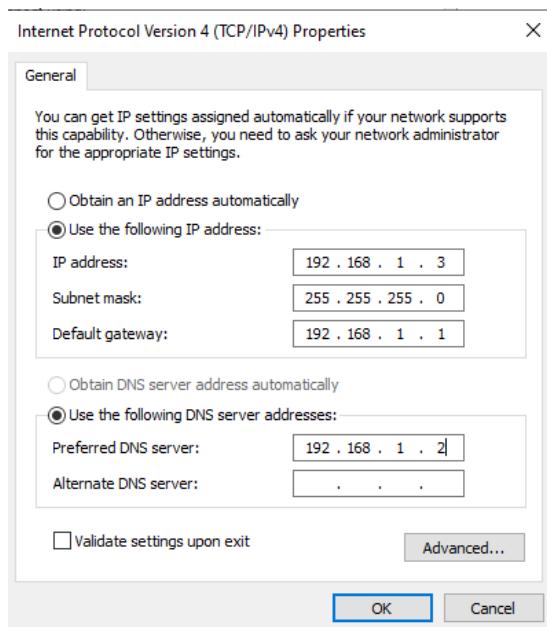
- Xuất hiện cửa sổ Result là đã cài đặt domain controller thành công.



Hình 2.19: Cửa sổ Result

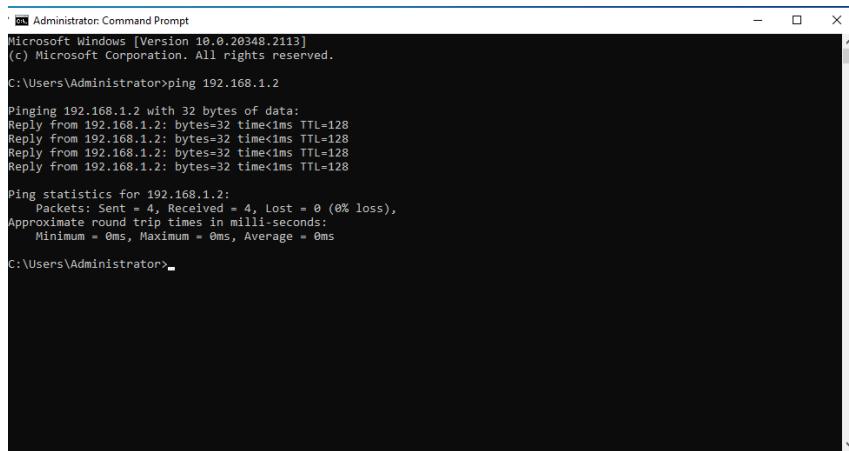
Join Server vào domain

- Thiết lập ip cho server như hình sau.



Hình 2.20: Thiết lập ip cho server

- Từ server ping thành công đến máy domain controller



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.2113]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

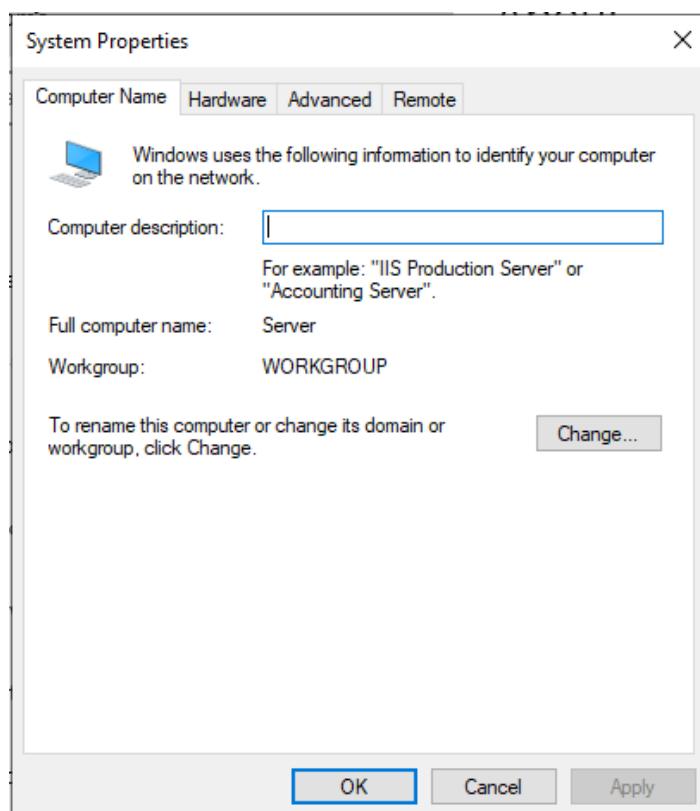
Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>

```

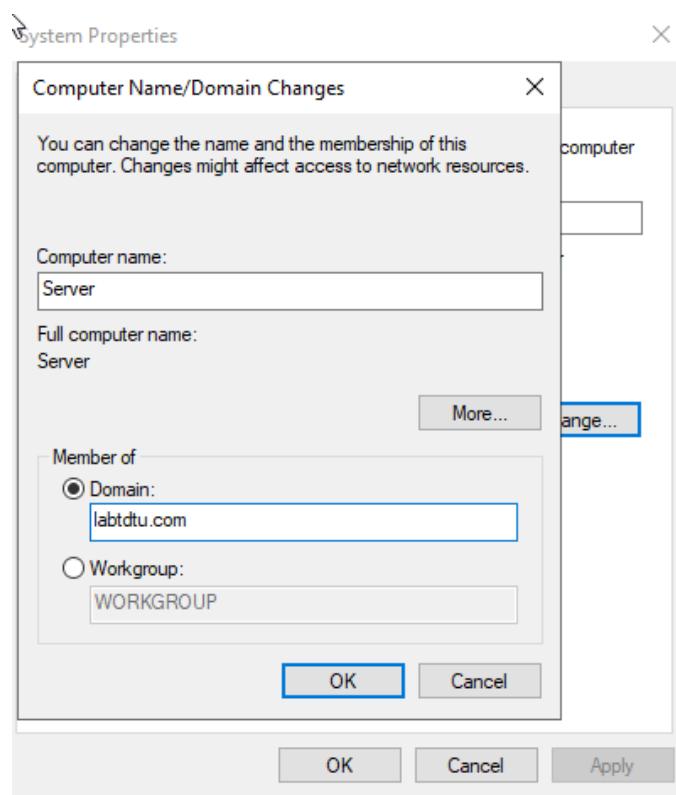
Hình 2.21: Ping thành công

- Để join vào domain **labtdtu.com**, vào System Properties > Computer Name > Change



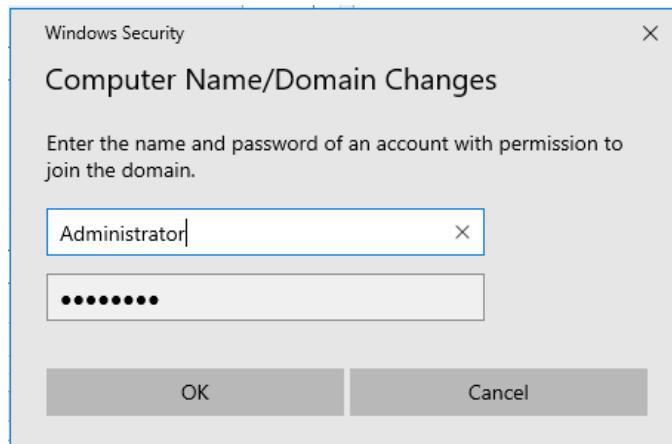
Hình 2.22: Join Server vào domain

- Member of domain > labtdtu.com



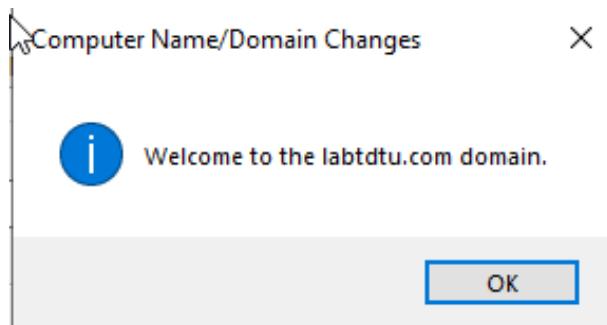
Hình 2.23: Nhập domain

- Nhập username và password



Hình 2.24: Xác thực

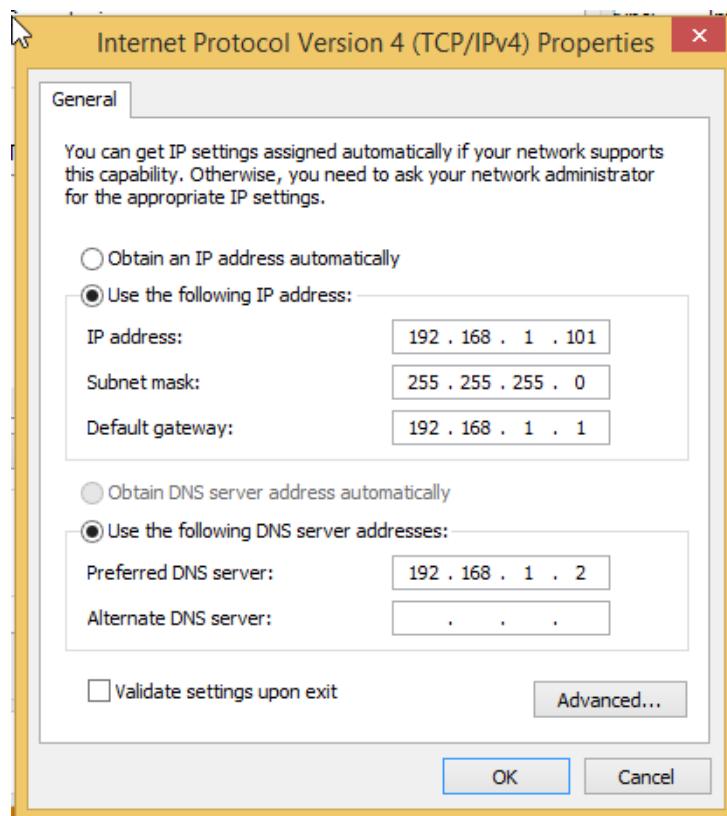
- Join domain thành công



Hình 2.25: Join domain thành công

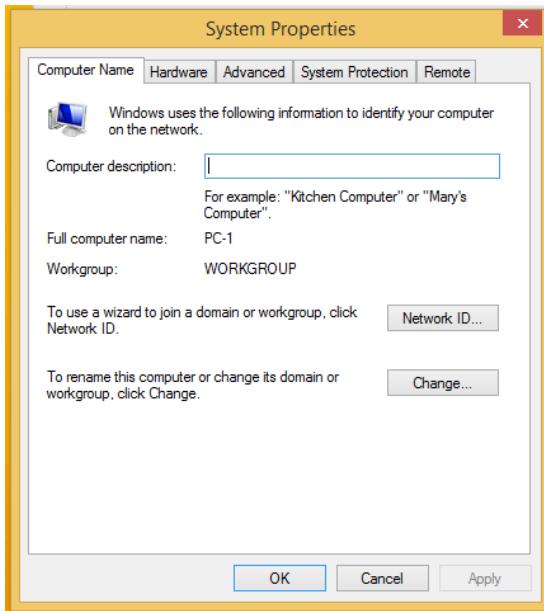
Join PC1 vào domain

- Thiết lập ip cho máy PC1



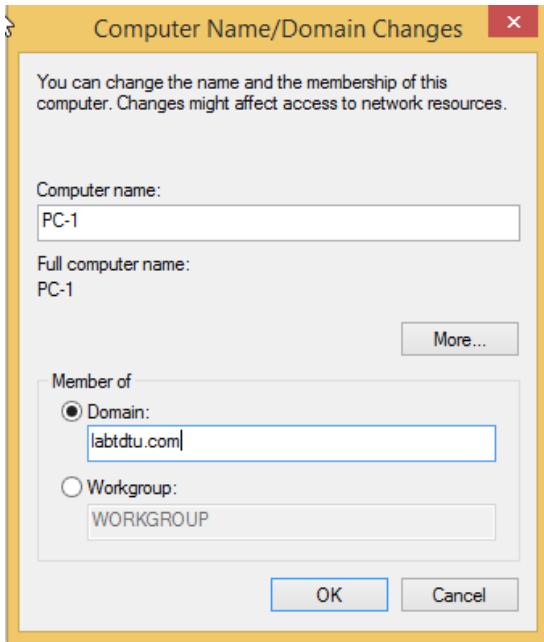
Hình 2.26: Thiết lập ip cho PC1

- Để join vào domain **labtdtu.com**, vào System Properties > Computer Name > Change



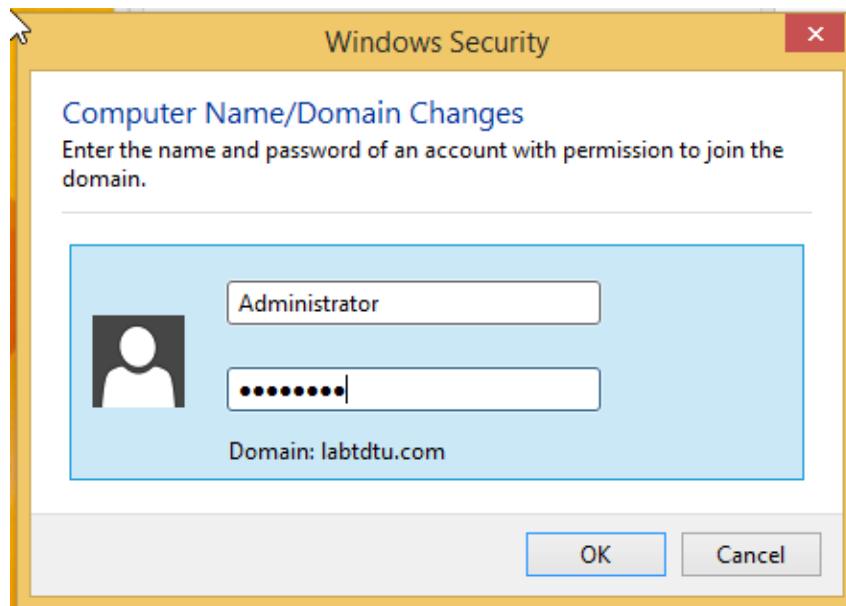
Hình 2.27: Join PC1 vào domain

- Member of domain > labtdtu.com



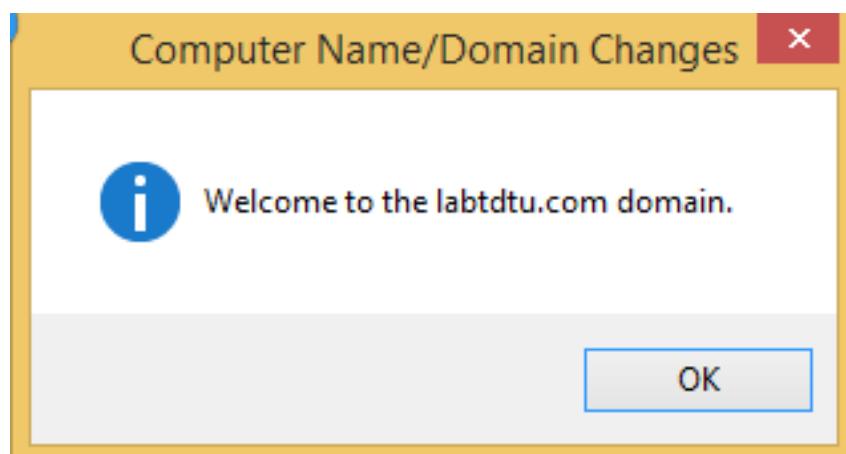
Hình 2.28: Nhập domain

- Nhập username và password



Hình 2.29: Xác thực

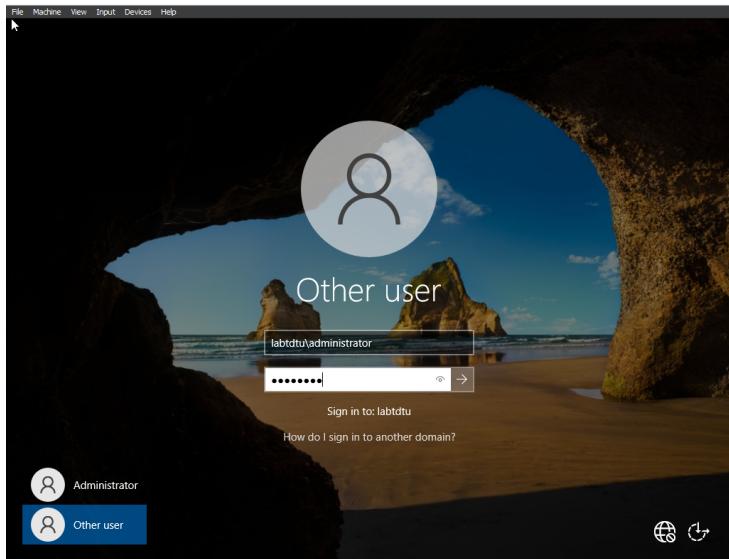
- Join domain thành công.



Hình 2.30: Join domain thành công

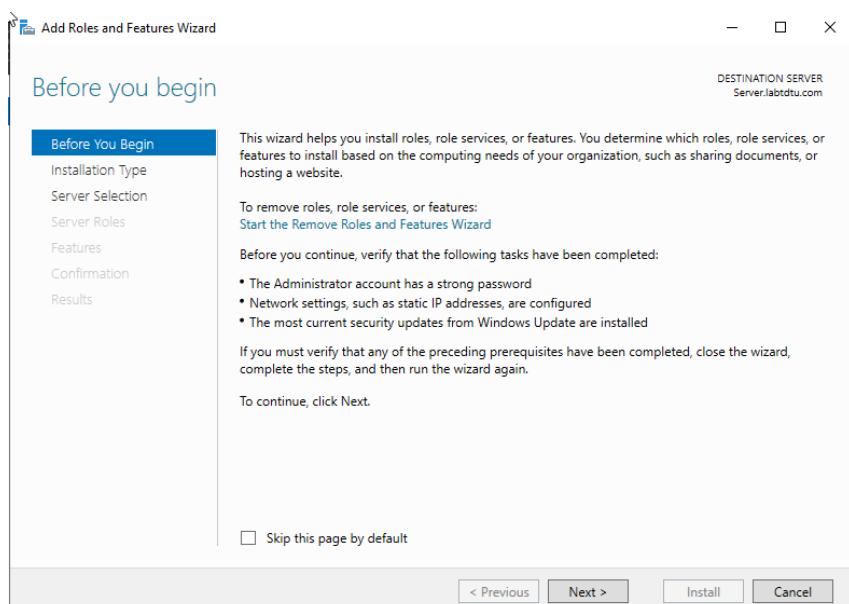
2.2 Cài Active Directory Certificate Services

- Trên server, đăng nhập bằng tài khoản **labtdtu\administrator**



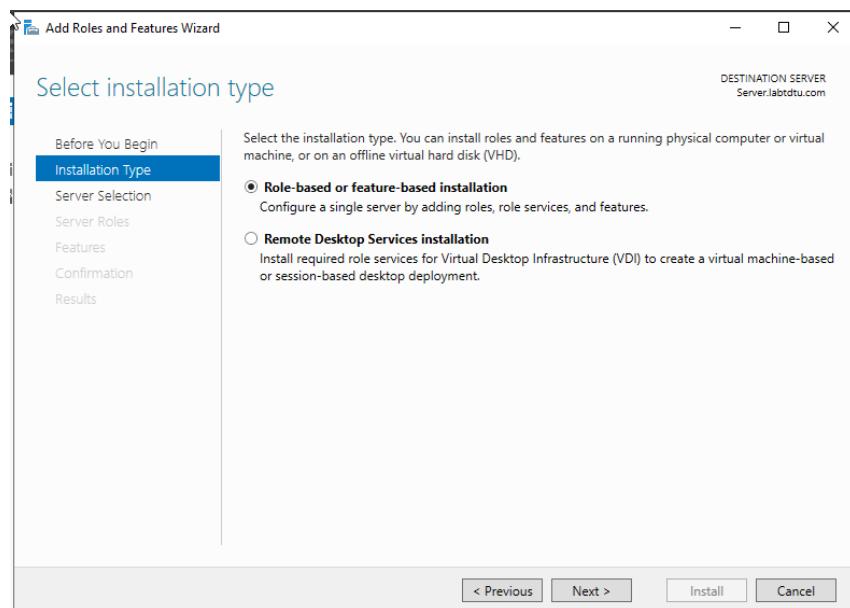
Hình 2.31: Đăng nhập bằng tài khoản Administrator

- Chọn menu Start > Administrative Tools > Server Manager. Chọn Roles > Add Roles.
- Xuất hiện cửa sổ Before You Begin, chọn Next.



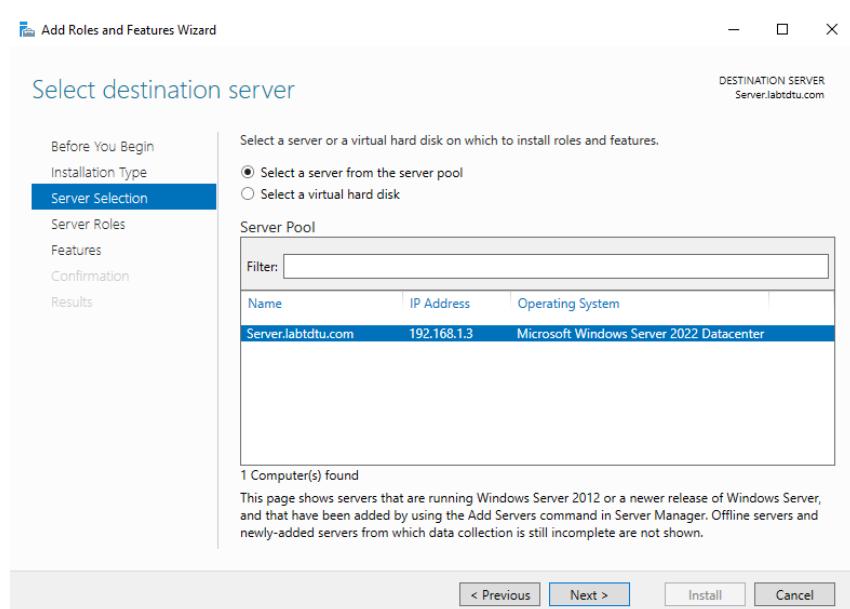
Hình 2.32: Cửa sổ Before You Begin

- Xuất hiện cửa sổ Select Installation Type, chọn Next.



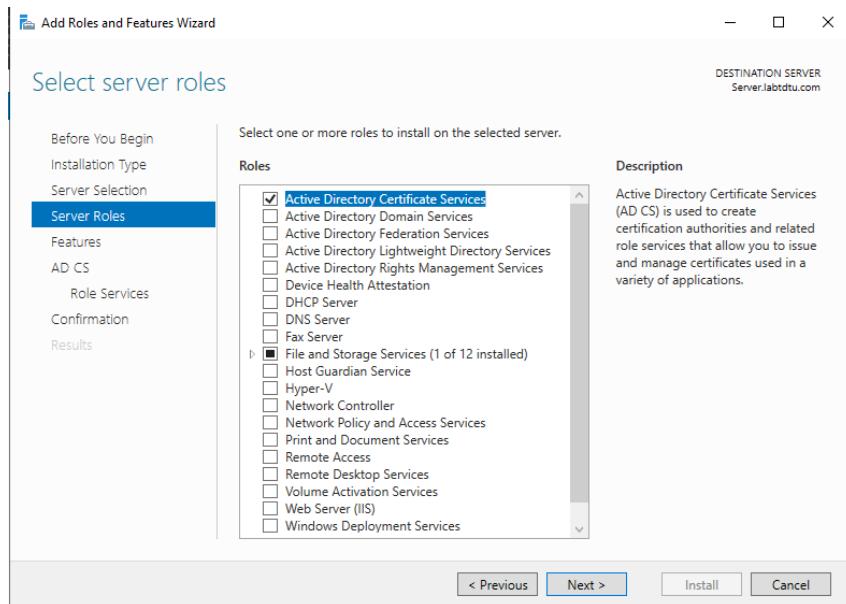
Hình 2.33: Cửa sổ Select Installation Type

- Xuất hiện cửa sổ Select Destination Server, chọn Next.



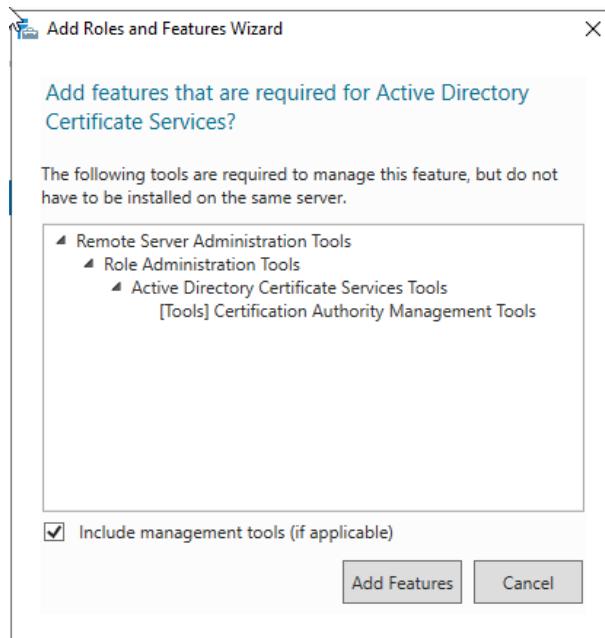
Hình 2.34: Cửa sổ Select Destination Server

- Xuất hiện cửa sổ Select Server Roles, đánh dấu chọn Active Directory Certificate Service, chọn Next.



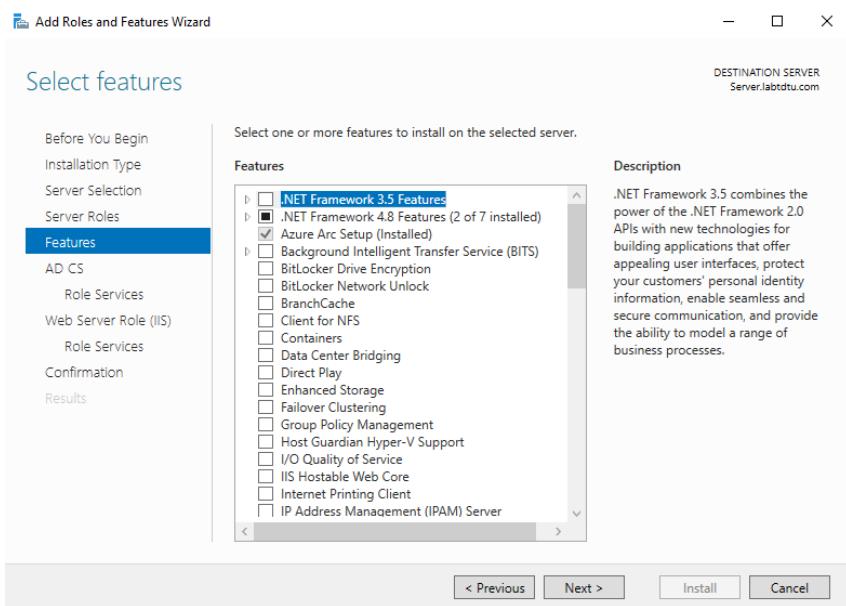
Hình 2.35: Cửa sổ Select Server Roles

- Các tính năng bổ sung được yêu cầu để thêm AD CS. Nhấp vào nút Add Features.



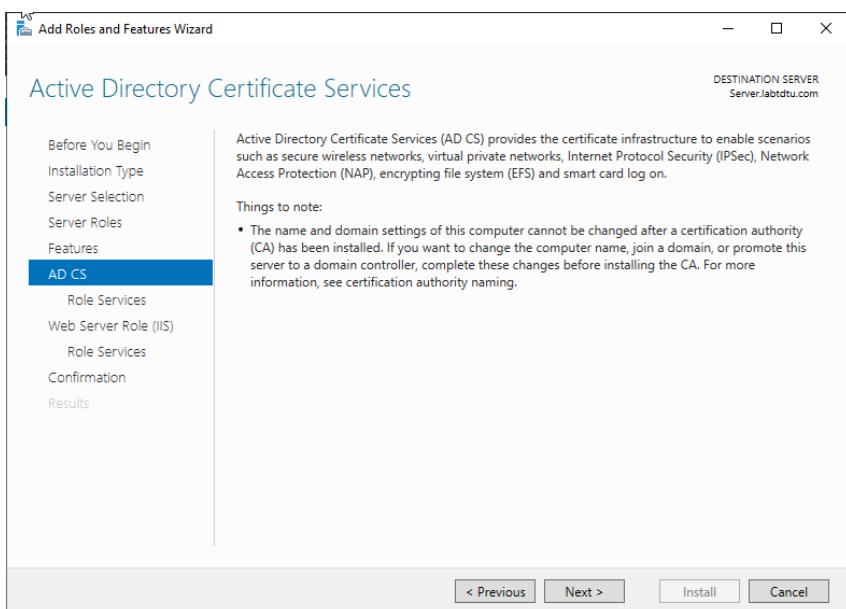
Hình 2.36: Cửa sổ các tính năng bổ sung

- Xuất hiện cửa sổ Select Features, chọn Next



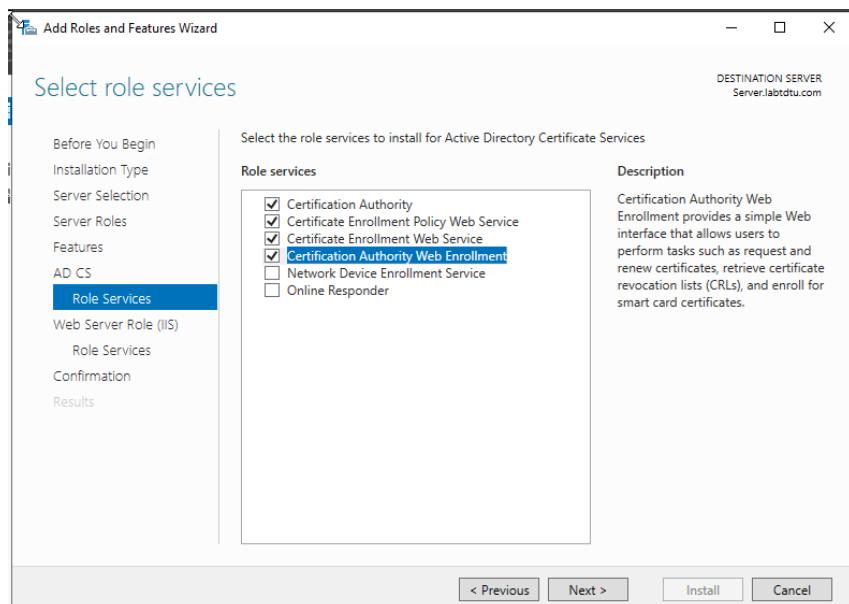
Hình 2.37: Cửa sổ Select Features

- Xuất hiện cửa sổ Active Directory Certificate Services, chọn Next.



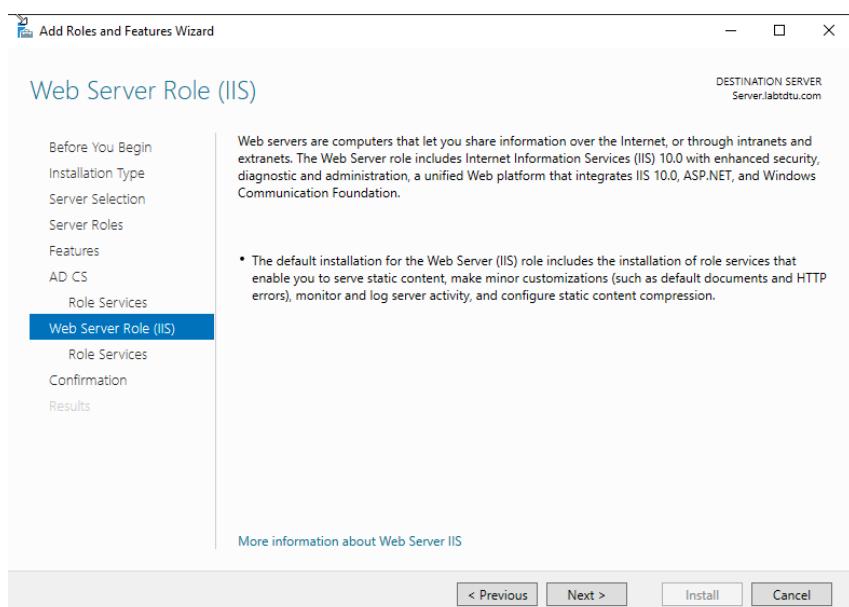
Hình 2.38: Cửa sổ Active Directory Certificate Services

- Trong cửa sổ Select Role Services, đánh dấu chọn Certificate Authority, Certificate Enrollment Policy Web Service, Certificate Enrollment Web Service, Certification Authority Web Enrollment > Next.



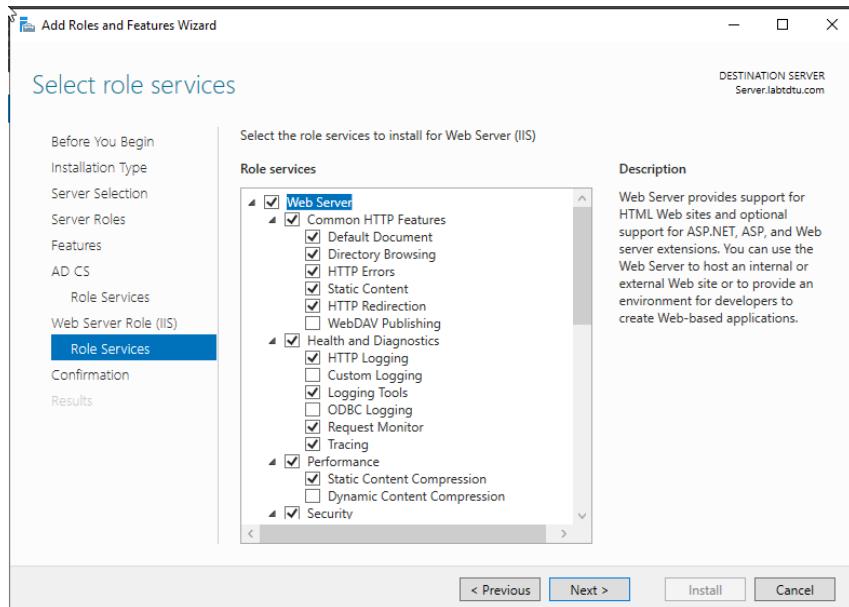
Hình 2.39: Cửa sổ Select Role Services

- Xuất hiện cửa sổ Web Server (IIS), chọn Next.



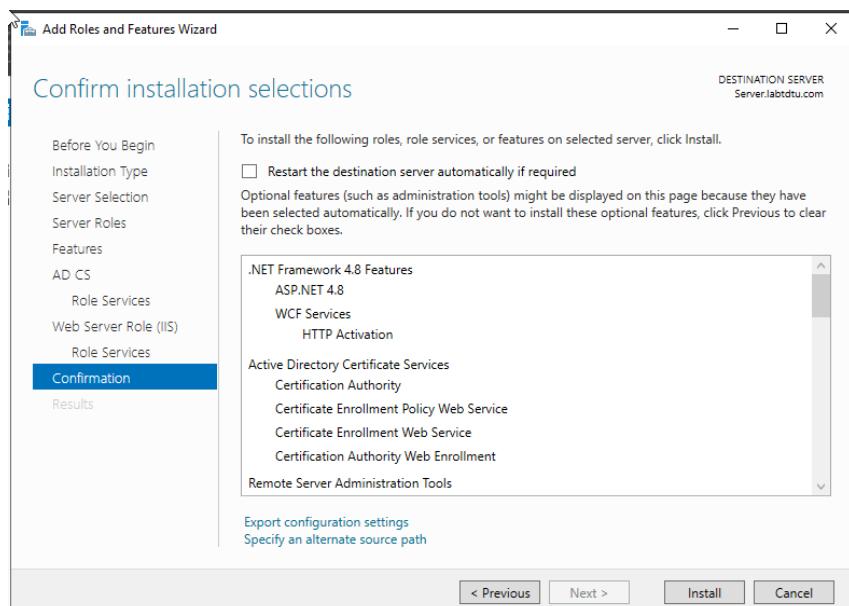
Hình 2.40: Cửa sổ Web Server (IIS)

- Trong cửa sổ Select Role Services, giữ cấu hình mặc định, chọn Next.



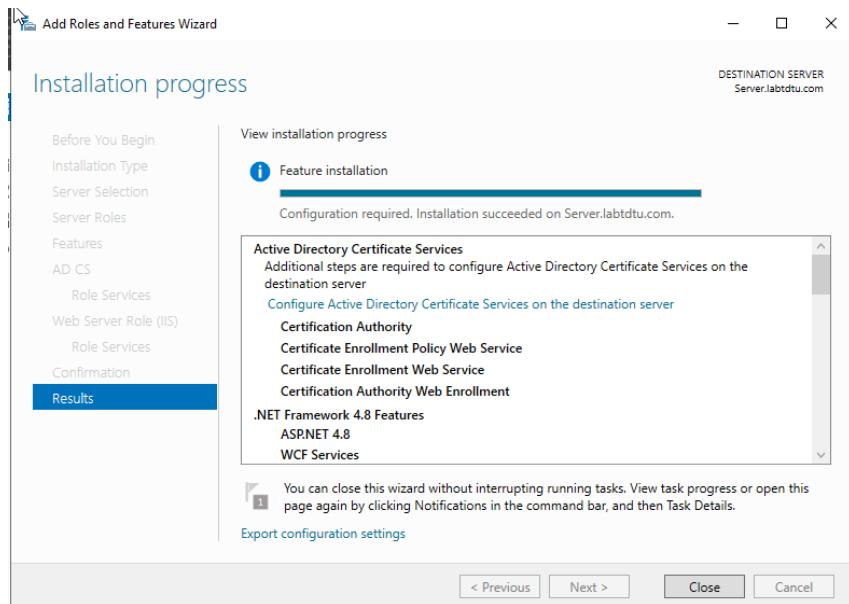
Hình 2.41: Cửa sổ Select Role Services

- Xuất hiện cửa sổ Confirm Installation Selections, chọn Install.



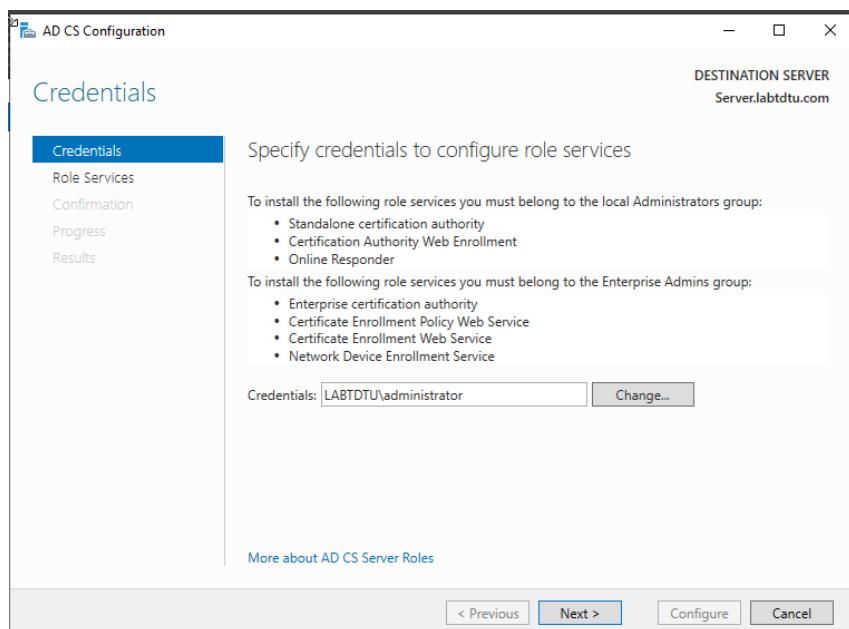
Hình 2.42: Cửa sổ Confirm Installation Selections

- Sau khi cài đặt thành công, chọn Configure Active Directory Certificate on the destination server.



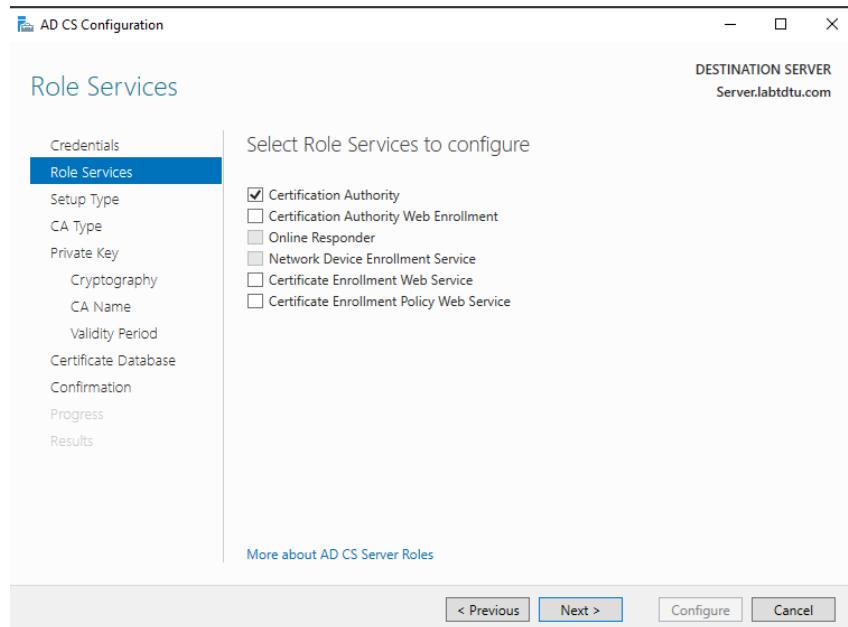
Hình 2.43: Cửa sổ cài đặt thành công

- Xuất hiện cửa sổ Credentials, chọn Next.



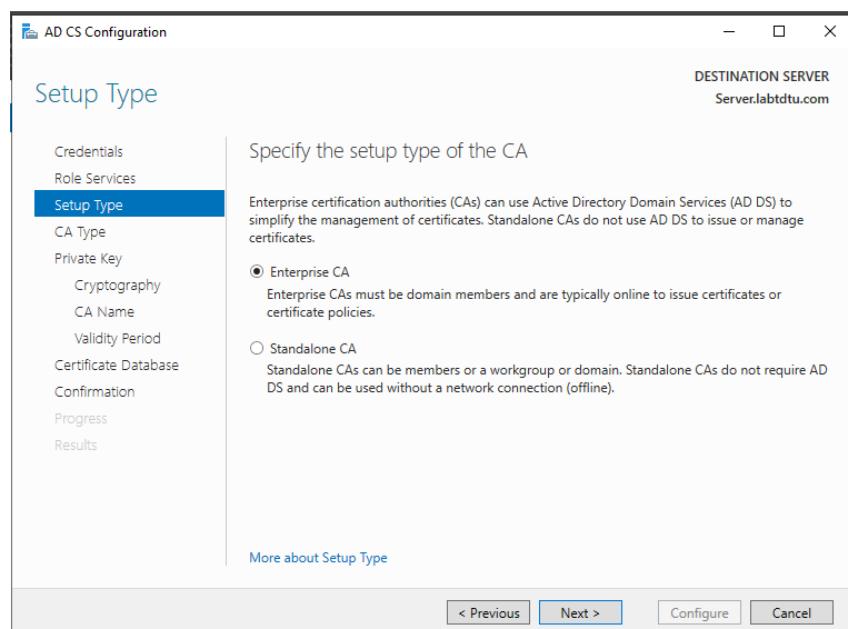
Hình 2.44: Cửa sổ Credentials

- Xuất hiện cửa sổ Role Services, chọn Certification Authority > Next.



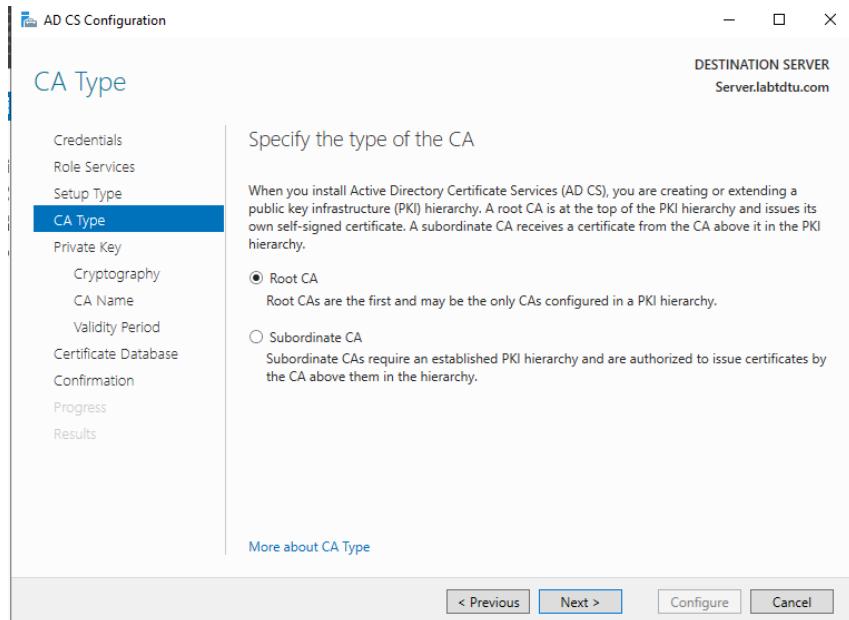
Hình 2.45: Cửa sổ Role Services

- Xuất hiện cửa sổ Setup Type, chọn Enterprise CA > Next.



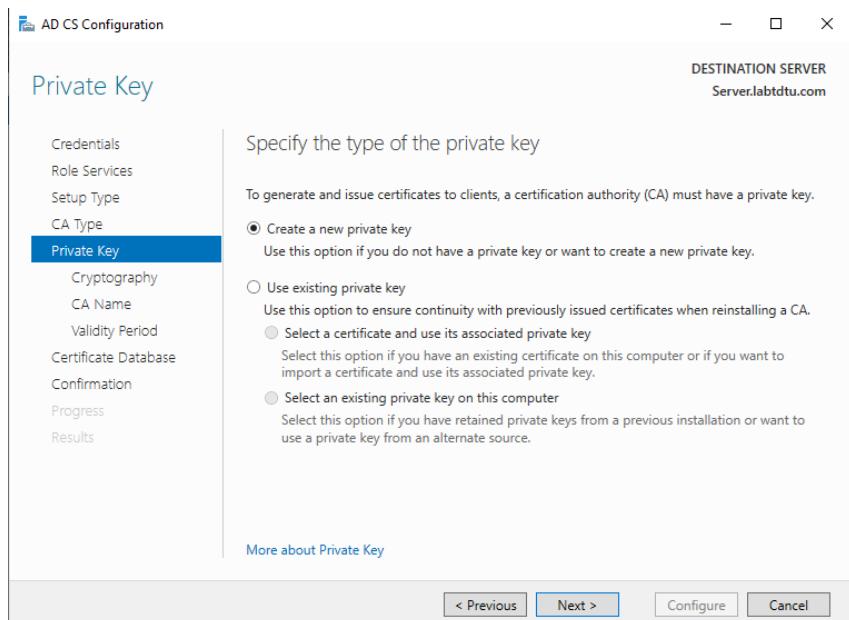
Hình 2.46: Cửa sổ Setup Type

- Xuất hiện cửa sổ CA Type, do đây là CA đầu tiên nên ta chọn Root CA > Next.



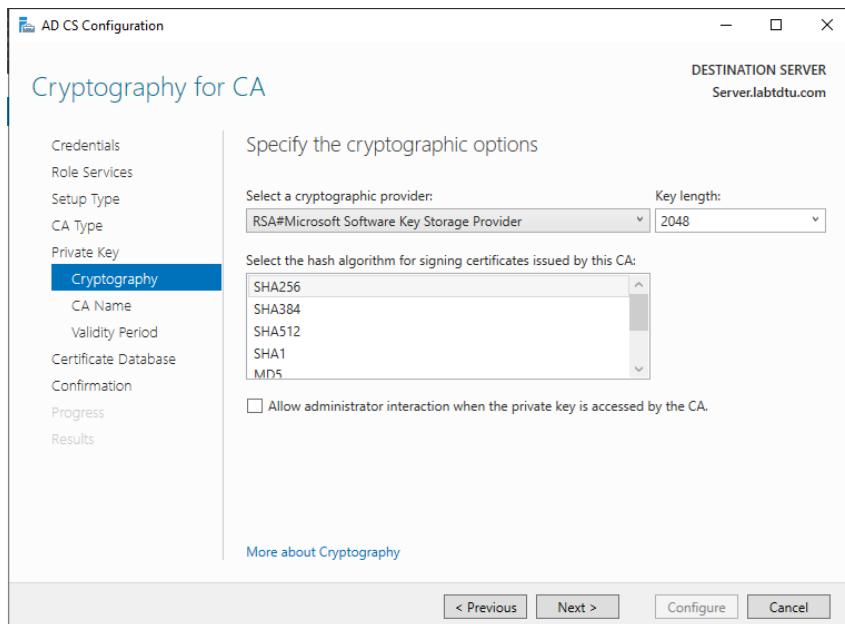
Hình 2.47: Cửa sổ CA Type

- Xuất hiện cửa sổ Private Key, chọn Create a new private key > Next.



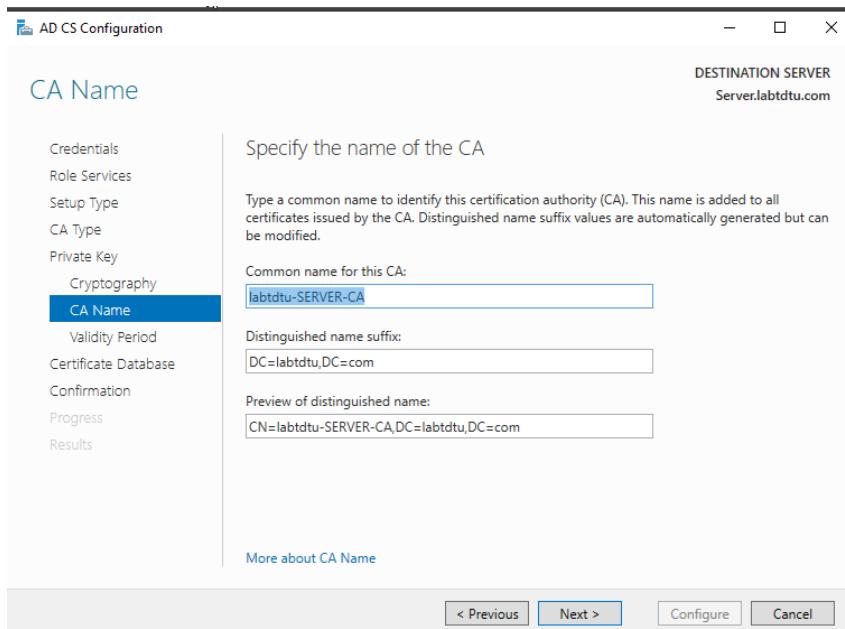
Hình 2.48: Cửa sổ Private Key

- Trong cửa sổ Cryptography For CA, chọn Next.



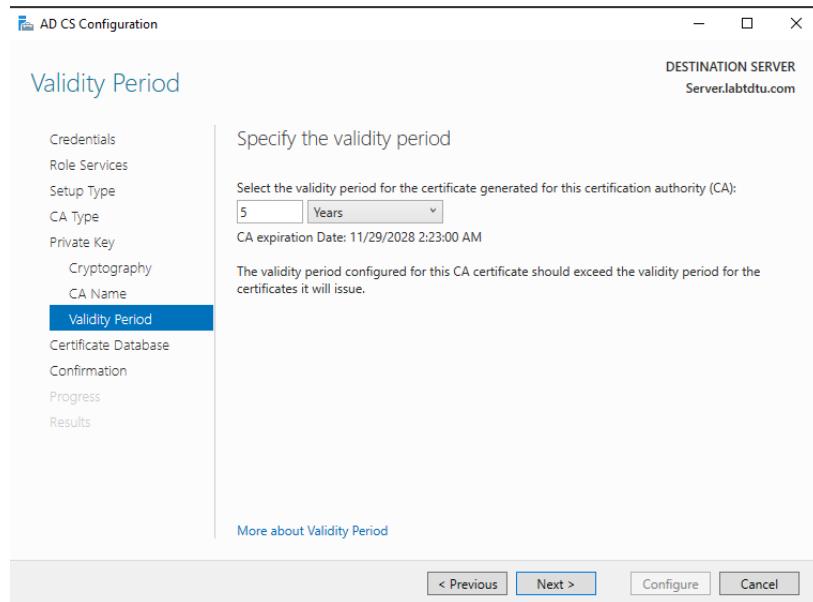
Hình 2.49: Cửa sổ Cryptography For CA

- Trong cửa sổ CA Name, đặt tên cho CA, ở đây để tên mặc định là labtdtu-SERVER-CA > Next.



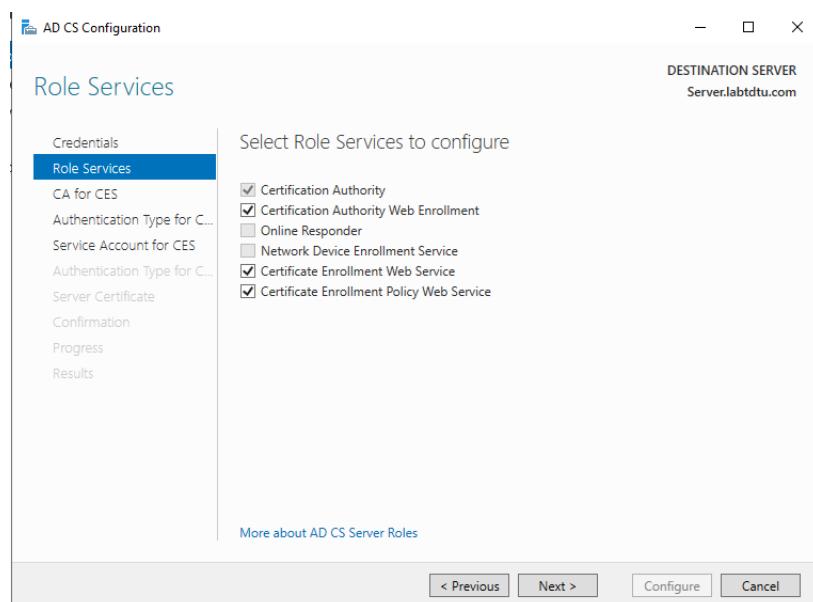
Hình 2.50: Cửa sổ CA Name

- Trong cửa sổ Validity Period, chọn Next.



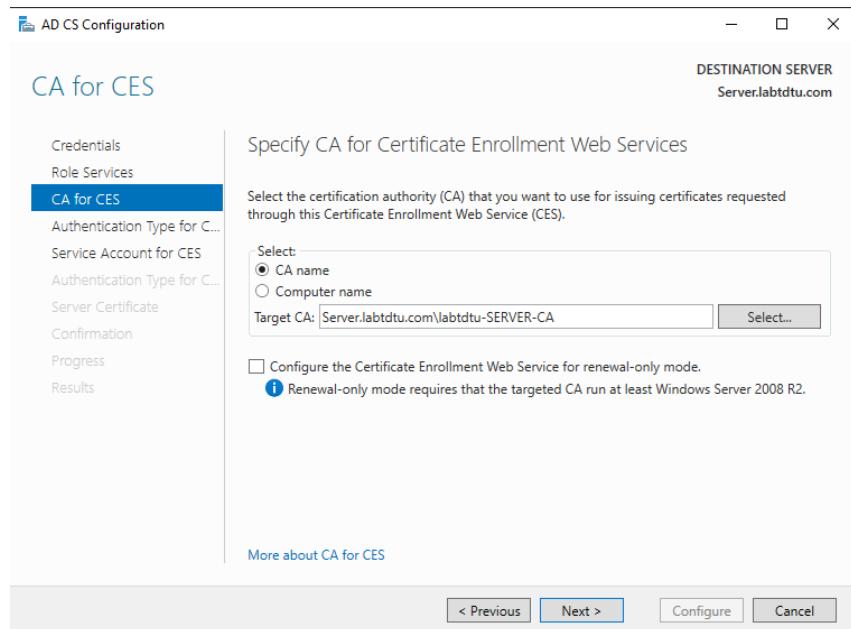
Hình 2.51: Cửa sổ Validity Period

- Tiếp tục cài đặt 3 role còn lại gồm:
 - Certificate Authority Web Enrollment
 - Certificate Enrollment Web Service
 - Certificate Enrollment Policy Web Service



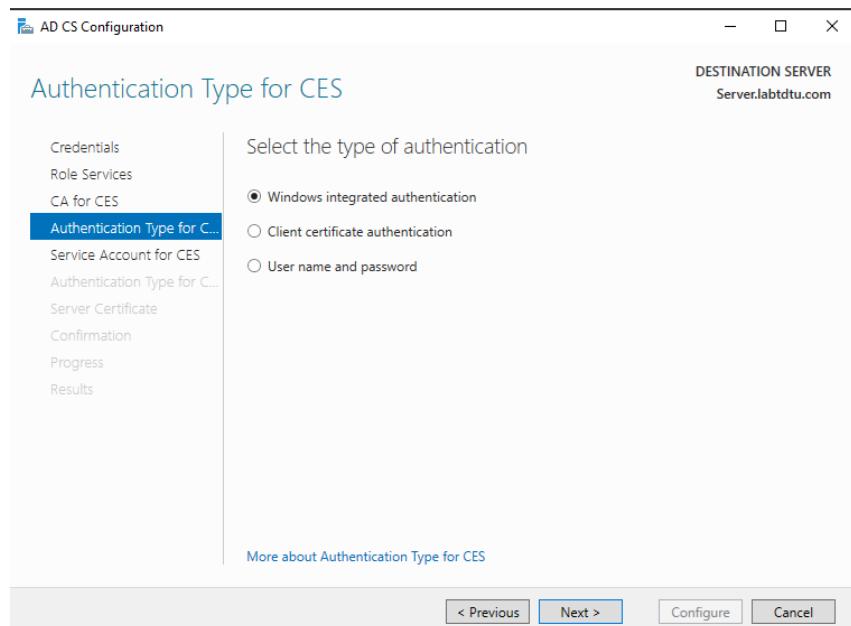
Hình 2.52: Cửa sổ các role còn lại cần cài đặt

- Sau khi cài xong 3 role như trên, xuất hiện cửa sổ CA For CES, chọn Next.



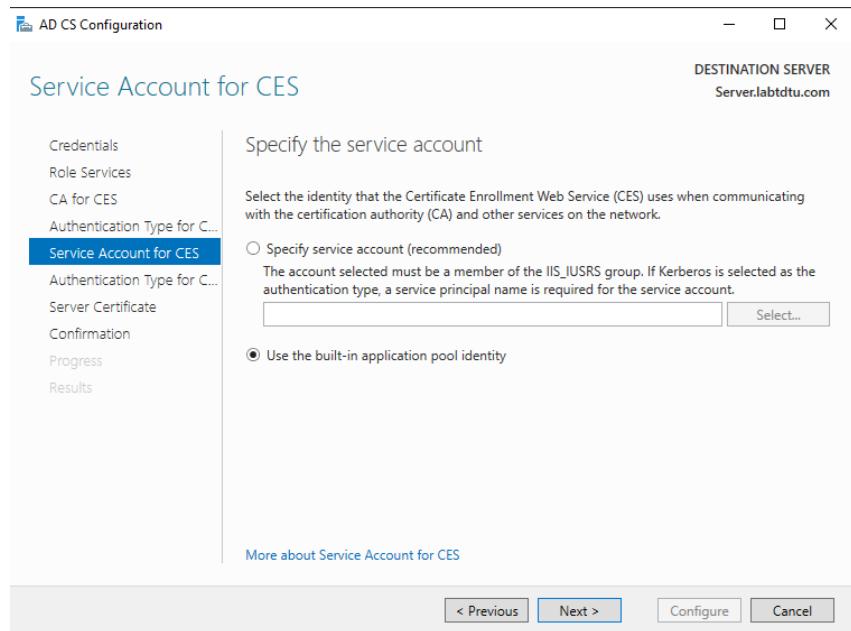
Hình 2.53: Cửa sổ CA For CES

- Xuất hiện cửa sổ Authentication Type For CES, chọn Next.



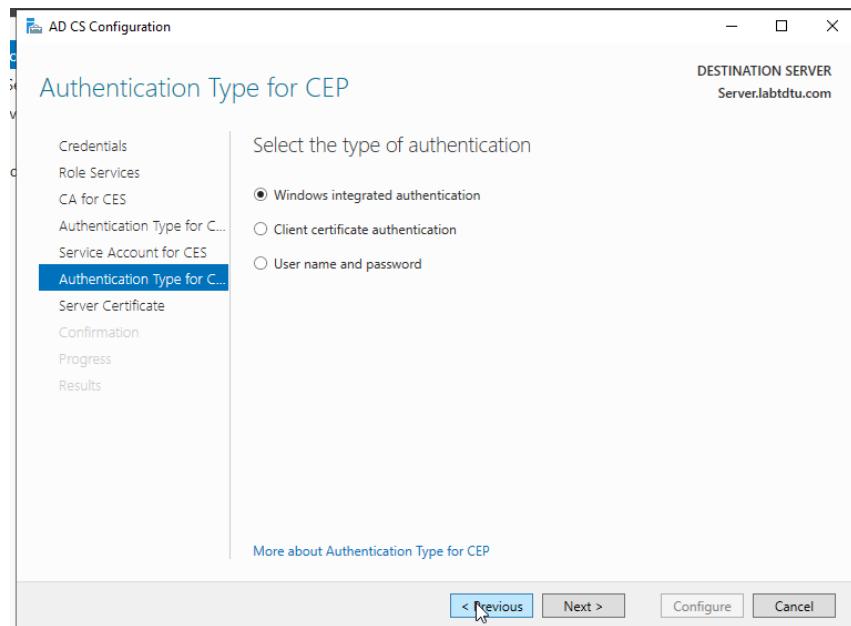
Hình 2.54: Cửa sổ Authentication Type For CES

- Xuất hiện cửa sổ Service Account For CES, chọn Use the built-in application pool identity > Next.



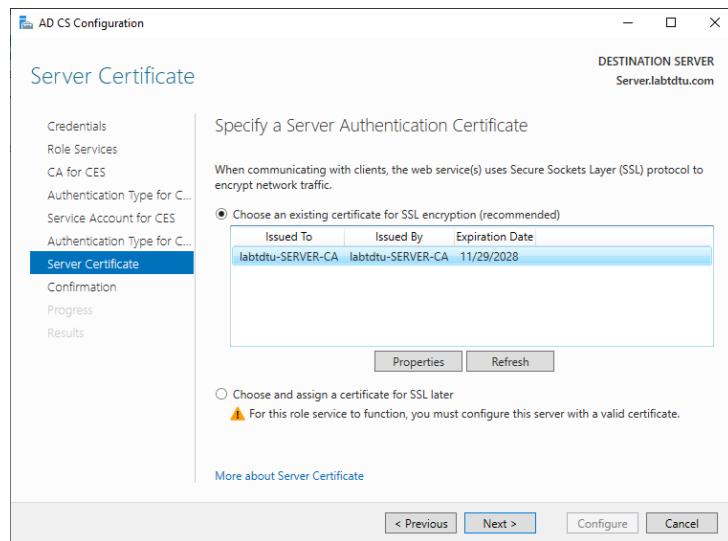
Hình 2.55: Cửa sổ Service Account For CES

- Xuất hiện cửa sổ Authentication Type For CEP, chọn Next.



Hình 2.56: Cửa sổ Authentication Type For CEP

- Xuất hiện cửa sổ Server Certificate, chọn chứng chỉ > Next.

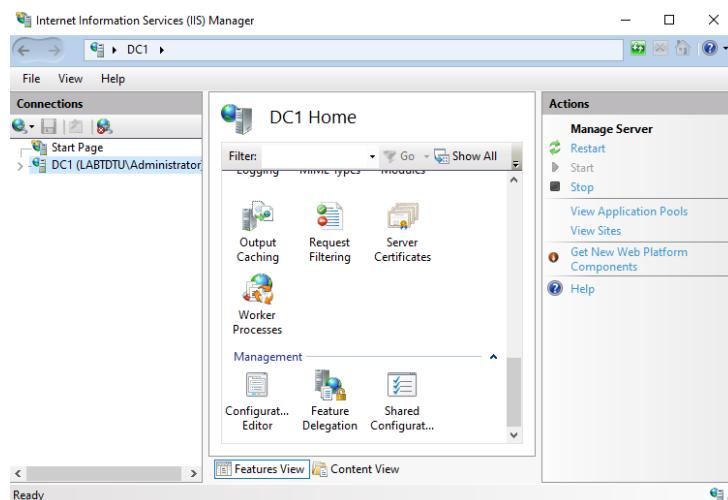


Hình 2.57: Cửa sổ Server Certificate

- Cài đặt tương tự như trên cho máy DC (Domain Controller)

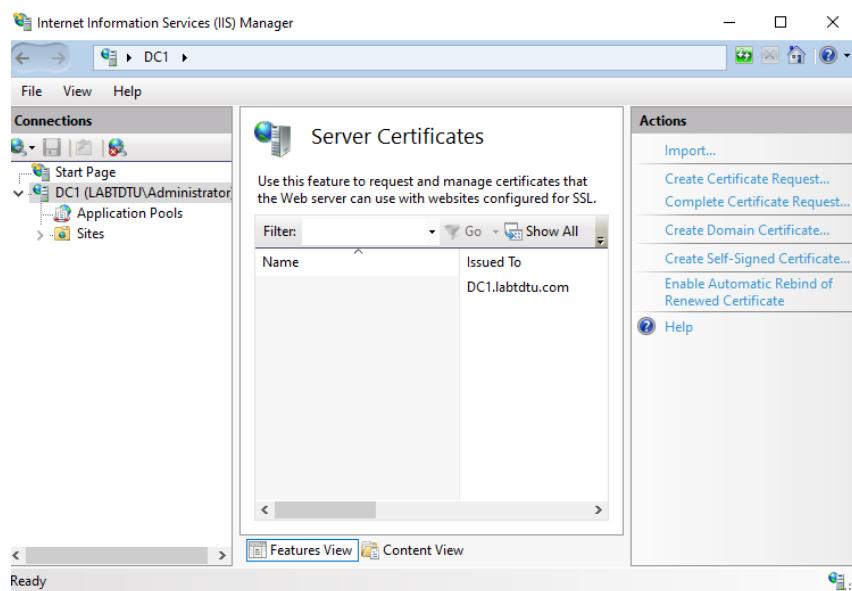
Xin SSL Certificate cho Web Server

- Trên máy DC1, mở Internet Information Services (IIS) Manager từ Administrative Tools. Chọn DC1, trong cửa sổ giữa chọn Server Certificates.



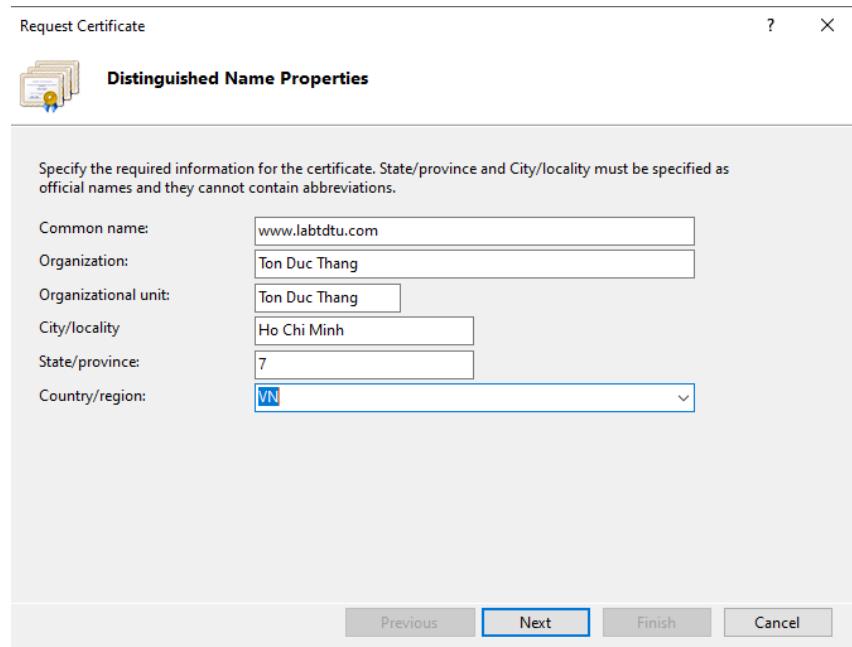
Hình 2.58: Xuất hiện cửa sổ DC1 Home

- Trong phần Action, chọn Create Certificate Request...



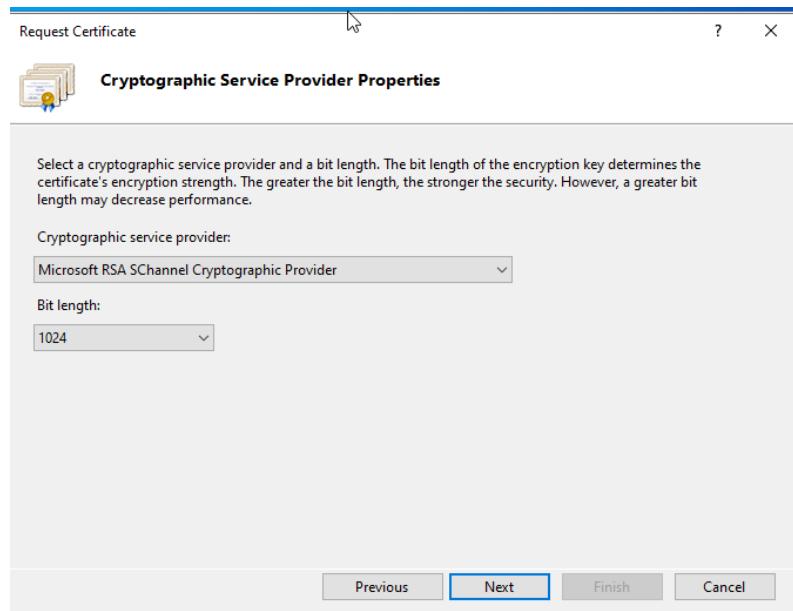
Hình 2.59: Xuất hiện Server Certificates

- Trong cửa sổ Distinguished Name Properties, nhập thông tin như sau và chọn Next.



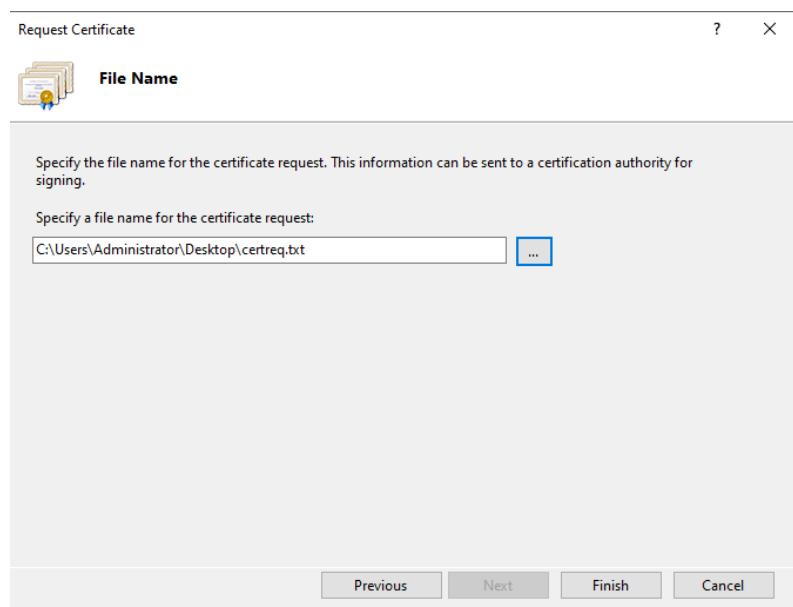
Hình 2.60: Cửa sổ Distinguished Name Properties

- Trong cửa sổ Cryptographic Service Provider Properties, giữ cấu hình mặc định, chọn Next.



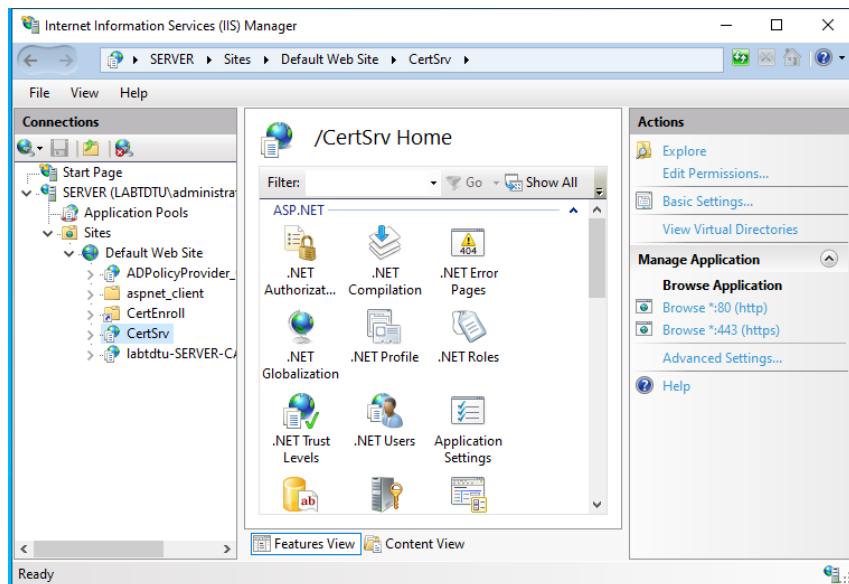
Hình 2.61: Cửa sổ Cryptographic Service Provider Properties

- Trong cửa sổ File Name nhập đường dẫn **C:\Users\Administrator\Desktop\certreq.txt** vào ô Specify a file name for the certificate request, chọn Finish.



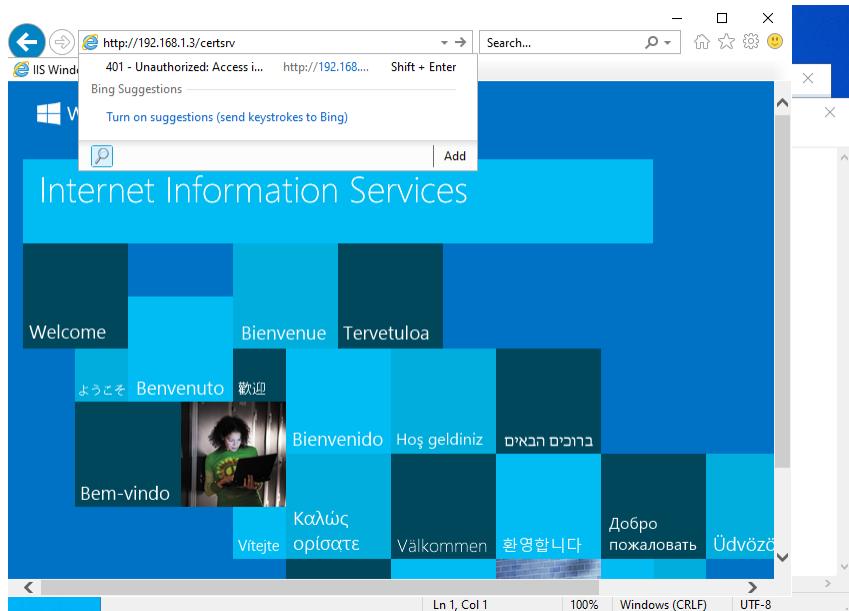
Hình 2.62: Cửa sổ File Name

- Trên máy Server, mở Internet Information Services (IIS) Manager từ Administrative Tools. Chọn SERVER > Sites > Default Web Site > CertSrv



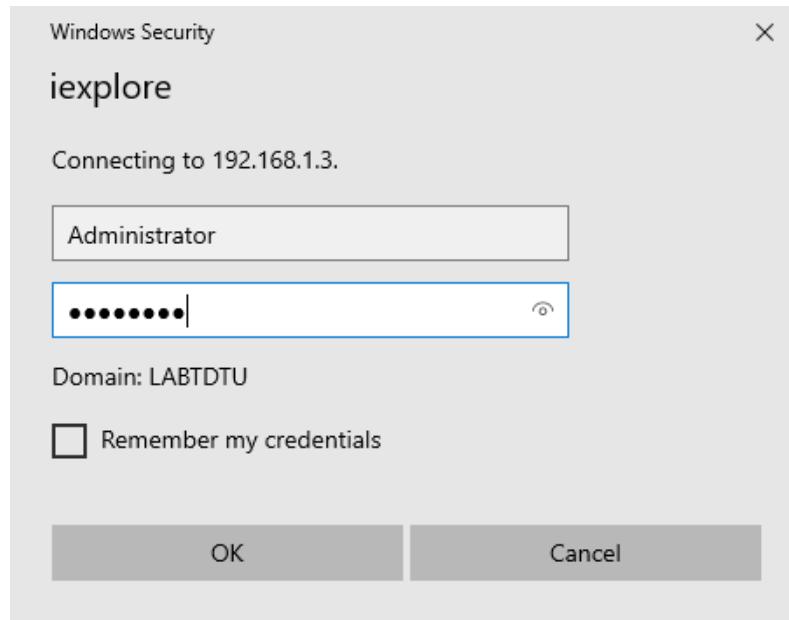
Hình 2.63: Xuất hiện cửa sổ \CertSrc Home

- Trên máy DC1, mở trình duyệt Internet Explorer và truy cập địa chỉ <http://192.168.1.3/certsrv>



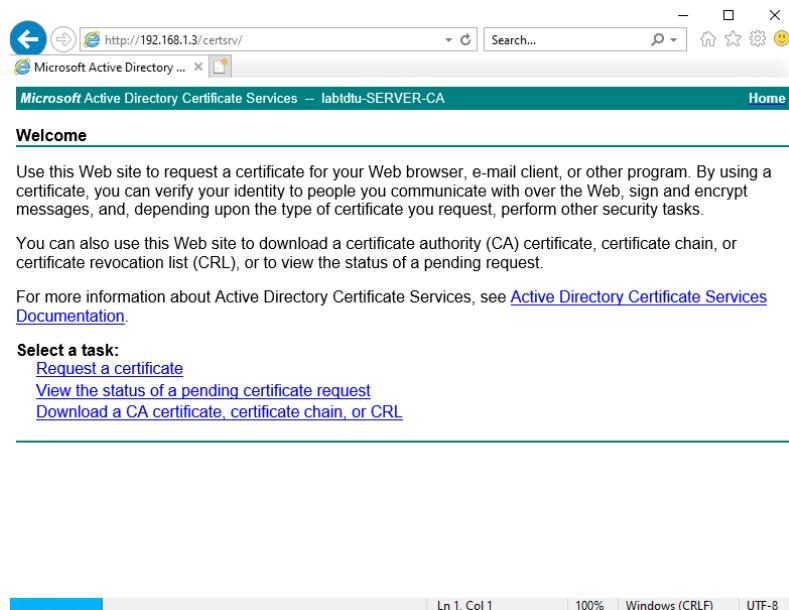
Hình 2.64: Cửa sổ trình duyệt truy cập website

- Nhập username và password



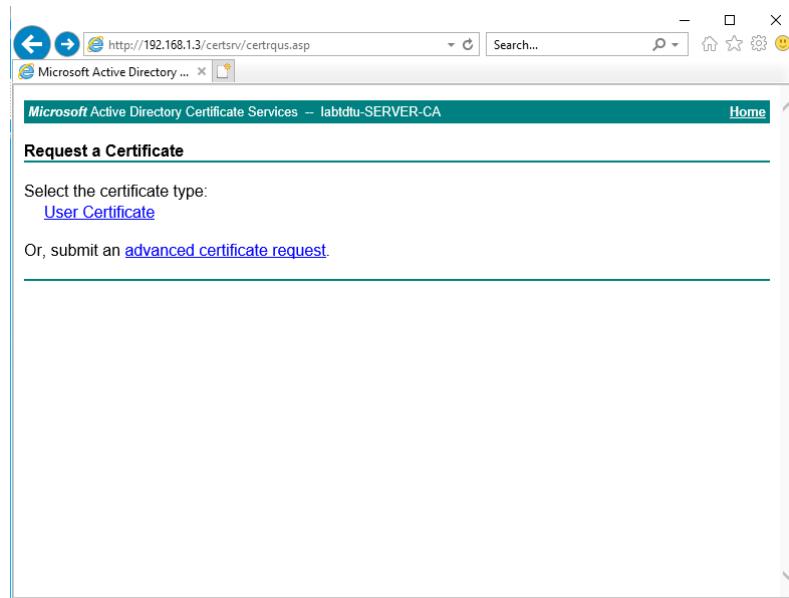
Hình 2.65: Cửa sổ xác thực

- Trong cửa sổ Welcome, chọn Request a certificate



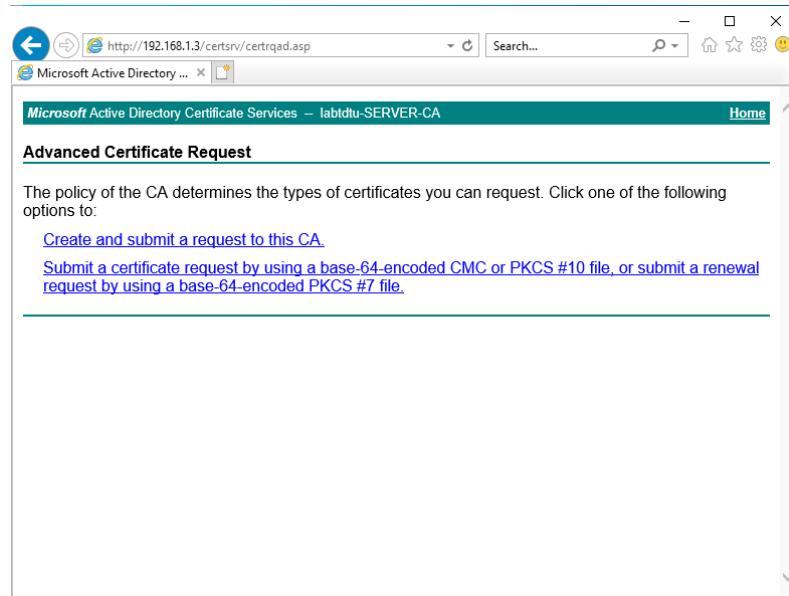
Hình 2.66: Cửa sổ Welcome

- Trong cửa sổ Request Certificate, chọn advanced certificate request.



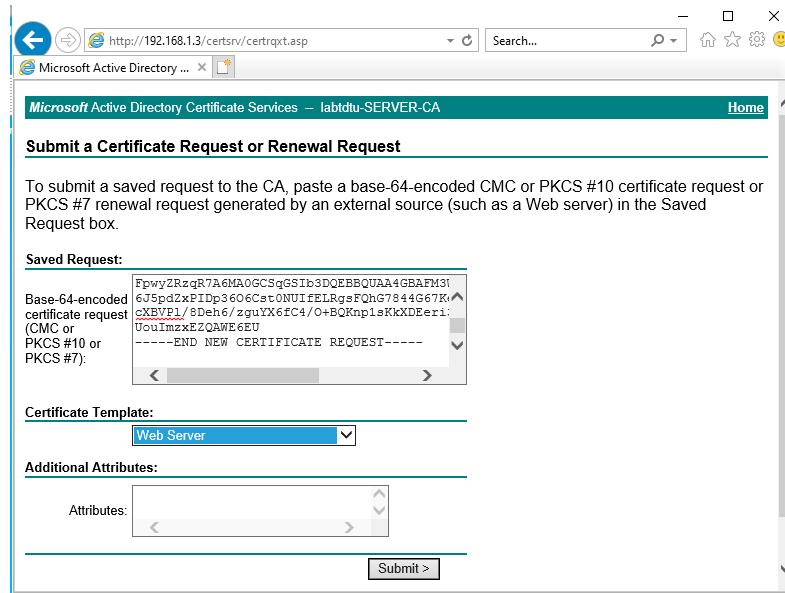
Hình 2.67: Cửa sổ Request Certificate

- Trong cửa sổ 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.



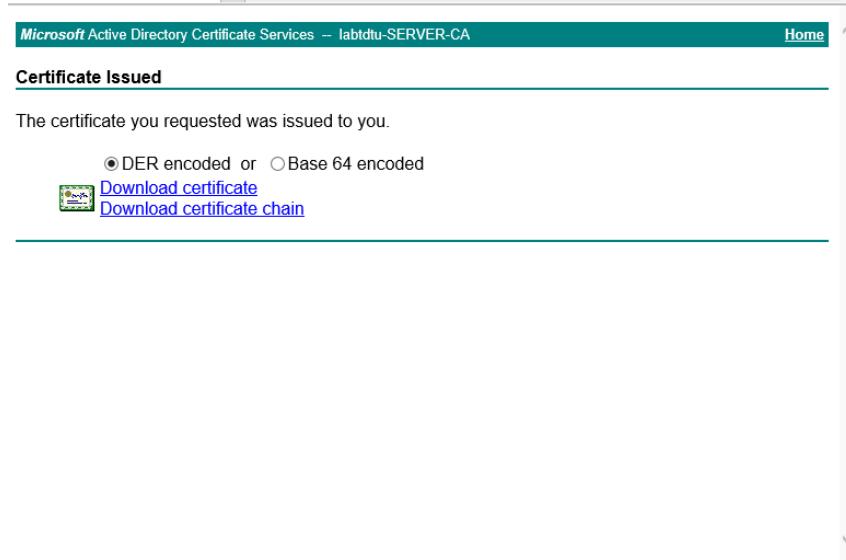
Hình 2.68: Cửa sổ Advanced Certificate Request

- Trong cửa sổ Submit a Certificate Request or Renewal Request, dán nội dung của file certreq.txt vào ô Saved Request, chọn Submit.



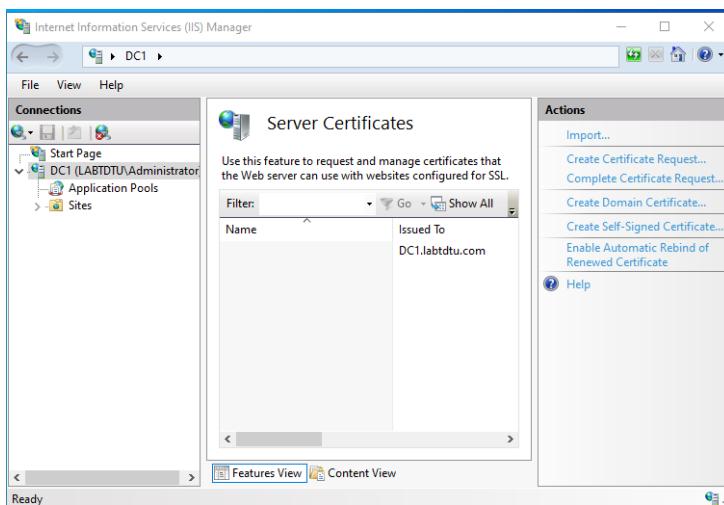
Hình 2.69: Cửa sổ Submit a Certificate Request or Renewal Request

- Sau khi Submit thành công thì xuất hiện cửa sổ Certificate Issued, chọn Download certificate.



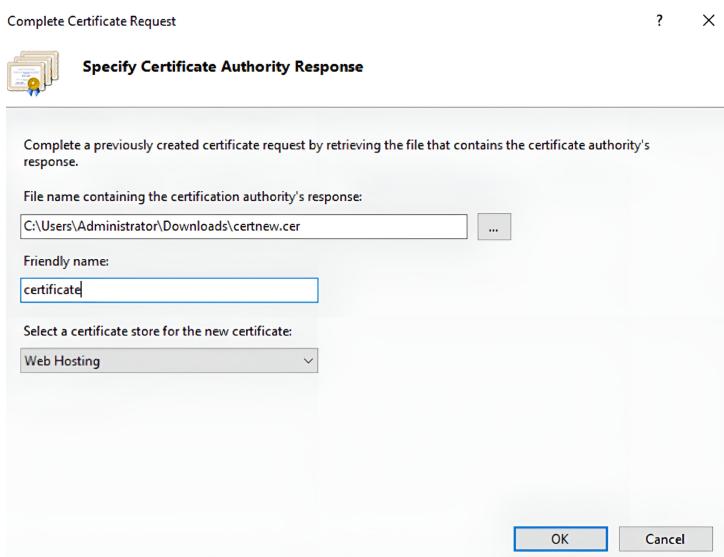
Hình 2.70: Cửa sổ Certificate Issued

- Trên máy DC1, quay trở lại Internet Information Services (IIS) Manager từ Administrative Tool. Chọn DC1, trong cửa sổ giữa chọn Server Certificate. Trong phần Action chọn Complete Certificate Request...



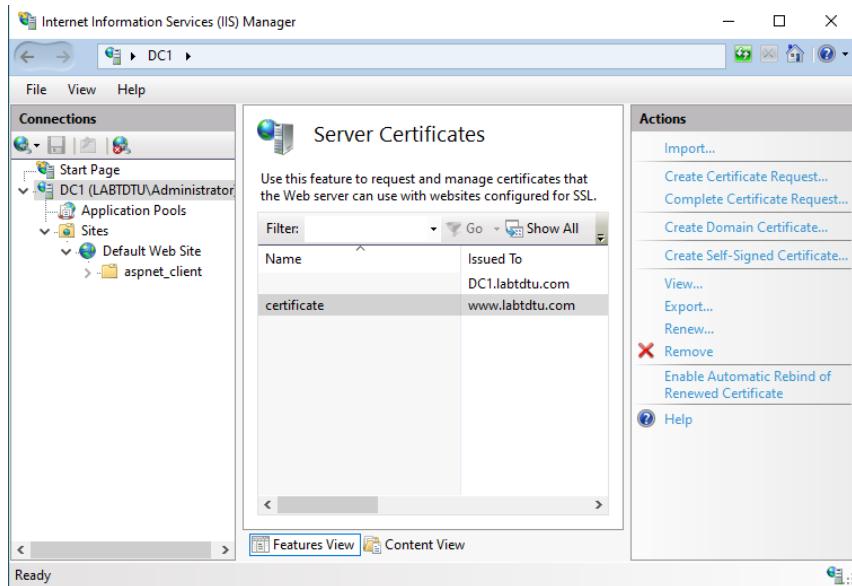
Hình 2.71: Cửa sổ Internet Information Services (IIS) Manager

- Trong cửa sổ Specify Certificate Authority Response, chỉ đường dẫn đến **C:\Users\Administrator\Desktop\certnew.cer**. Nhập tên chứng thực webserver là certificate vào ô Friendly name > chọn Web Hosting ở mục Select a certificate store for the new certificate > OK.



Hình 2.72: Cửa sổ Specify Certificate Authority Response

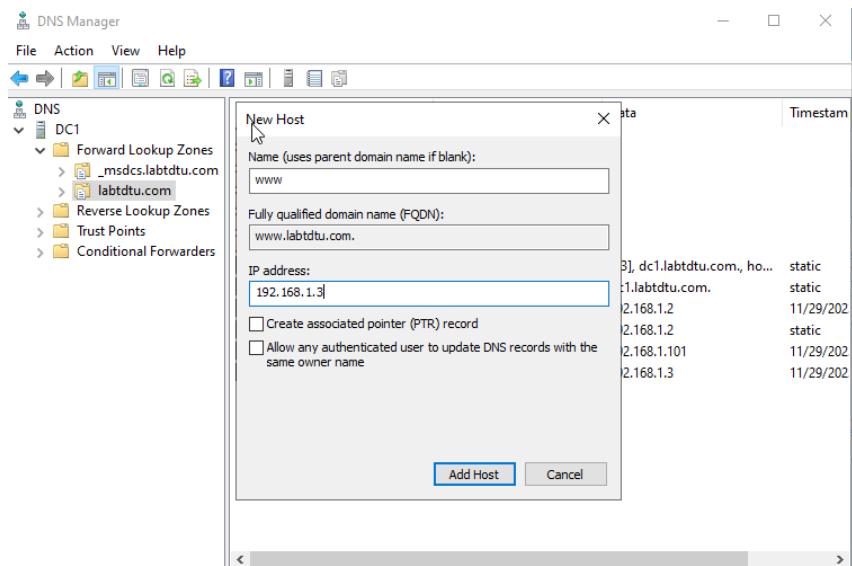
- Kiểm tra trong phần Server Certificate đã có chứng thực webserver tên là certificate hay chưa. Ở đây certificate đã thành công.



Hình 2.73: Cửa sổ Server Certificate

Thiết lập tên miền DNS và HTTPS Site

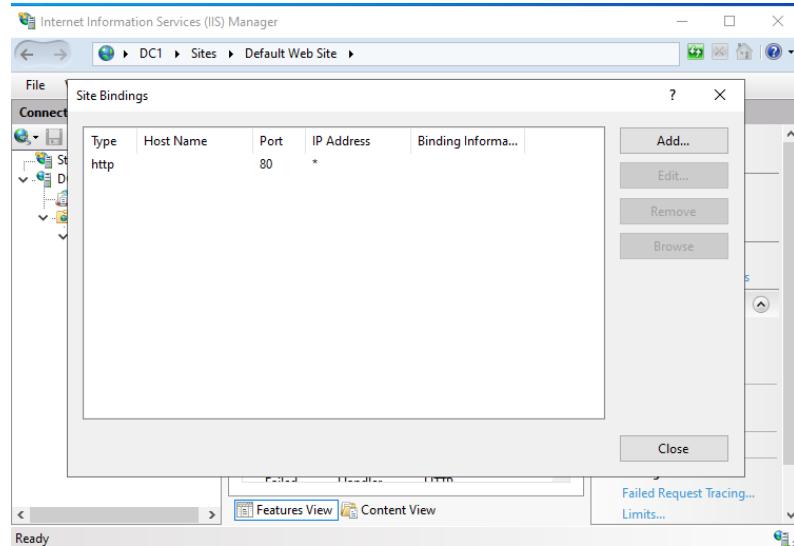
- Thiết lập tên miền DNS:** DNS Manager > DC1 > Forward Lookup Zones > labtdtu.com > Chuột Chuột phải chọn new host > Diền ip address là ip web server



Hình 2.74: Cửa sổ thiết lập tên miền DNS

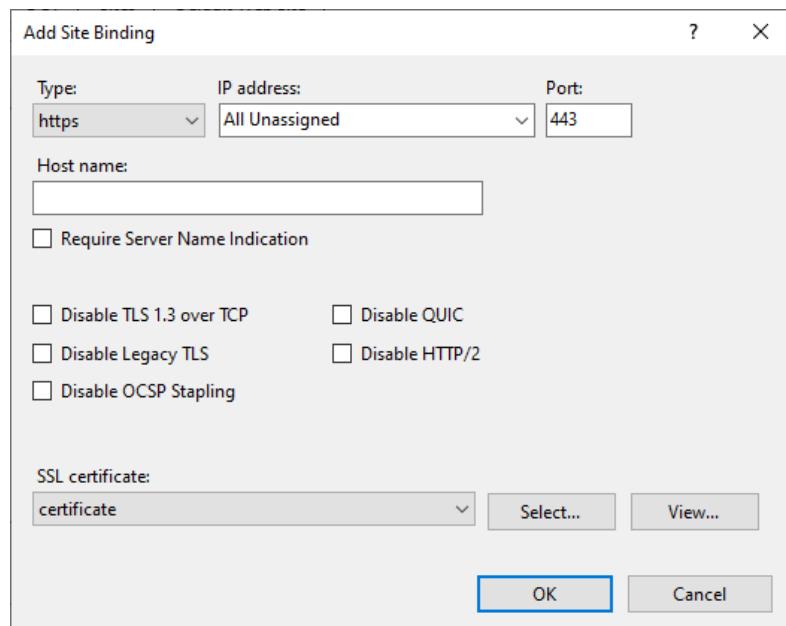
• Thiết lập HTTPS Site

- Internet Information Services Manager > DC1-Sites > Default Website > Bindings > Add



Hình 2.75: Cửa sổ thiết lập HTTPS Site

- Type->https->SSL certificate->Chọn certificate đã lưu lúc nãy->OK

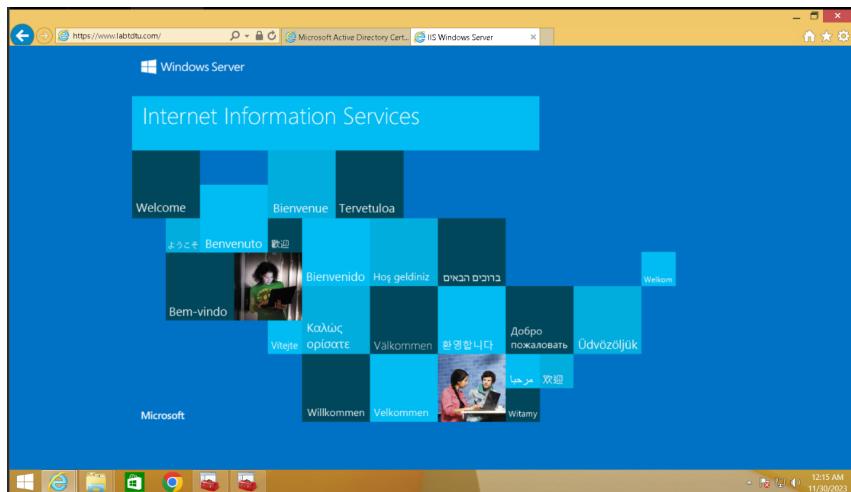


Hình 2.76: Cửa sổ

2.3 Kiểm tra

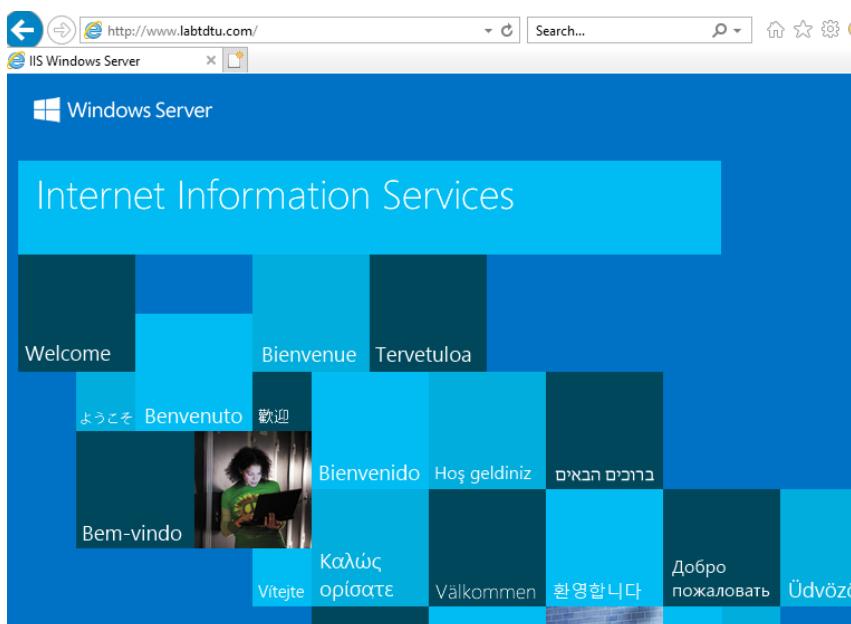
Trên máy PC1, mở trình duyệt Internet Explorer và truy cập:

- Địa chỉ website: <https://www.labtdtu.com>



Hình 2.77: Khi truy cập địa chỉ website: <https://www.labtdtu.com>

- Địa chỉ website: <http://www.labtdtu.com>



Hình 2.78: Khi truy cập địa chỉ website: <http://www.labtdtu.com>

3 Thực hành trên PowerShell

3.1 Cài đặt Active Directory Domain Controller

- Trên máy FIT-DC, cấu hình địa chỉ IP

The screenshot shows a Windows PowerShell ISE window with the following details:

- Script Editor:** The left pane displays a script named "script-1.ps1" containing PowerShell commands to configure network interfaces. The commands include setting adapter properties, creating a new NetIPInterface, and setting DNS client server addresses.
- Output Window:** The bottom-left pane shows the execution results of the script, listing various properties of the configured network interface, such as IP address, subnet mask, gateway, and store type.
- Commands History:** The right pane is a "Commands" history window titled "Commands X". It lists a large number of PowerShell cmdlets, likely from the "Add-Appx" module, such as Add-AppClientConnectionGroup, Add-AppClientPackage, and Add-AppPublishingServer.
- Search Bar:** A search bar at the bottom of the window allows users to search through the command history.

Hình 2.79: Cấu hình địa chỉ IP

- Kiểm tra cấu hình địa chỉ IP

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.20348.2113]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::540b:6181:f14e:2d0%6
  IPv4 Address . . . . . : 192.168.1.2
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1

C:\Users\Administrator>
```

Hình 2.80: Kiểm tra địa chỉ IP

● Cài đặt Active Directory Domain Controller

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-1.ps1 X Commands X
1 # CAU HINH DIA CHI IP_CHE FIT-DC
2 $Adapter = "Ethernet"
3 $IpAddress = "192.168.1.2"
4 $Subnetmask = "255.255.255.0"
5 $Defaultgateway = "192.168.1.1"
6
7 New-NetIPAddress -InterfaceAlias $Adapter -IPAddress $IpAddress -PrefixLength 24 -DefaultGateway $Defaultgateway
8
9 Set-DnsClientServerAddress -InterfaceAlias $Adapter -ServerAddresses $IpAddress
10
11 # CAU HINH DOMAIN CONTROLLER
12 # Cai dat AD DS
13 Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
14

AddressFamily : IPv4
Type : Unicast
PrefixLength : 24
PrefixOrigin : Manual
SuffixOrigin : Manual
AddressState : Invalid
ValidLifetime : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipSource : False
PolicyStore : PersistentStore

PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
Success Restart Needed Exit Code      Feature Result
----- ----- ----- ----- {Active Directory Domain Services, Group P...}

True    No        Success
Completed
PS C:\Users\Administrator> | Run Insert Copy
Ln 51 Col 28 | 1:12 PM 11/27/2023

```

Hình 2.81: Cài đặt AD DS

● Tạo 1 forest labtdtu.com mới.

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-1.ps1 X Commands X
1 # CAU HINH DOMAIN CONTROLLER
2 # Cai dat AD DS
3 Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools
4
5 # Tao forest moi
6 Install-ADForest -DomainName "labtdtu.com" -InstallDns -Force:$true
7
8 # Nang cap ten DC
9 Install-ADDomainController `
10   -NoGlobalCatalog:$false `
11   -CreateDnsDelegation:$false `
12   -Credential:(Get-Credential) `
13   -CTFReplicationOnly:$false `
14   -DatabasePath "C:\Windows\NTDS" `
15   -DomainName "labtdtu.com"
16
17
18 You're about to be signed out
The computer is being restarted because Active Directory Domain Services was installed or removed.
Close
19
20 WARNING: Windows Server 2022 domain controller is incompatible with windows NT 4.0 that prevent
21 for more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).
22
23 WARNING: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not
24 run Windows DNS services. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to
this DNS server in the parent zone to ensure reliable name resolution from outside the domain "labtdtu.com". Otherwise, no action
is required.

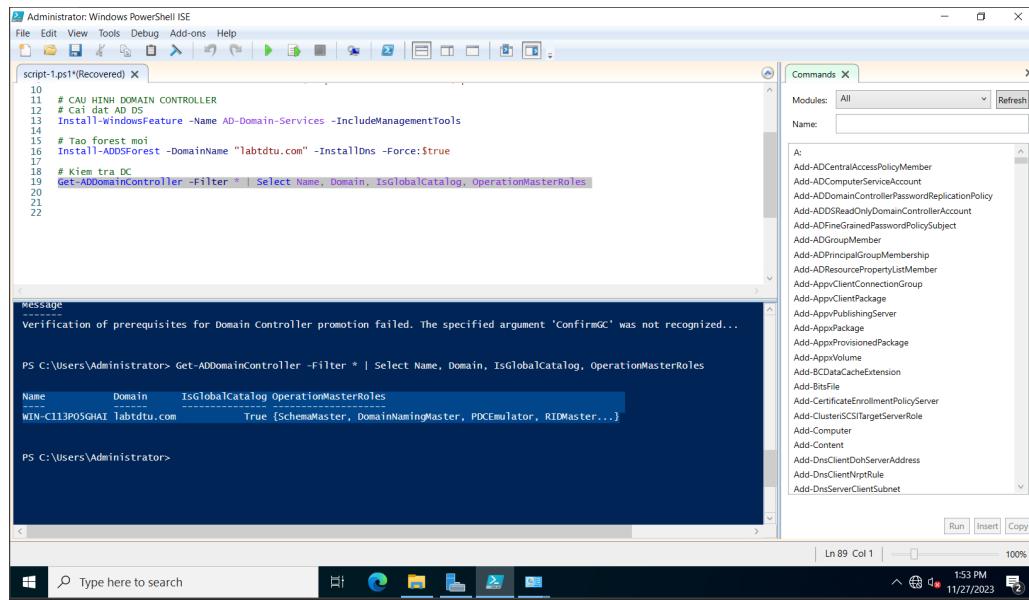
Message          Context          RebootRequired Status
Operation completed successfully DCPromo.General.3           False Success

PS C:\Windows\system32>
Completed
PS C:\Windows\system32> | Run Insert Copy
Ln 124 Col 25 | 1:42 PM 11/27/2023

```

Hình 2.82: Tạo forest labtdtu.com

- Kiểm tra xem máy FIT-DC đã trở thành một Domain Controller hay chưa.



```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-1.ps1*(Recovered) x Commands x
Modules: All Refresh
Name: A:
Add-ADCentralAccessPolicyMember
Add-ADComputerServiceAccount
Add-ADDomainControllerPasswordReplicationPolicy
Add-ADReadOnlyDomainControllerAccount
Add-ADFineGrainedPasswordPolicySubject
Add-ADGroupMember
Add-ADPrincipalGroupMembership
Add-ADResourcePropertyListMember
Add-AppClientConnectionGroup
Add-AppClientPackage
Add-AppPublishingServer
Add-AppPackage
Add-AppProvisionedPackage
Add-AppVolume
Add-BCDataCacheExtension
Add-BitsFile
Add-CertificateEnrollmentPolicyServer
Add-ClusterSCSITargetServerRole
Add-Computer
Add-Content
Add-DnsClientDohServerAddress
Add-DnsClientNrrRule
Add-DnsServerClientSubnet

PS C:\Users\Administrator> Get-ADDomainController -Filter * | Select Name, Domain, IsGlobalCatalog, OperationMasterRoles
Name Domain IsGlobalCatalog OperationMasterRoles
WIN-C113POSGHAI labtdtu.com True {SchemaMaster, DomainNamingMaster, PDCEmulator, RIDMaster...}

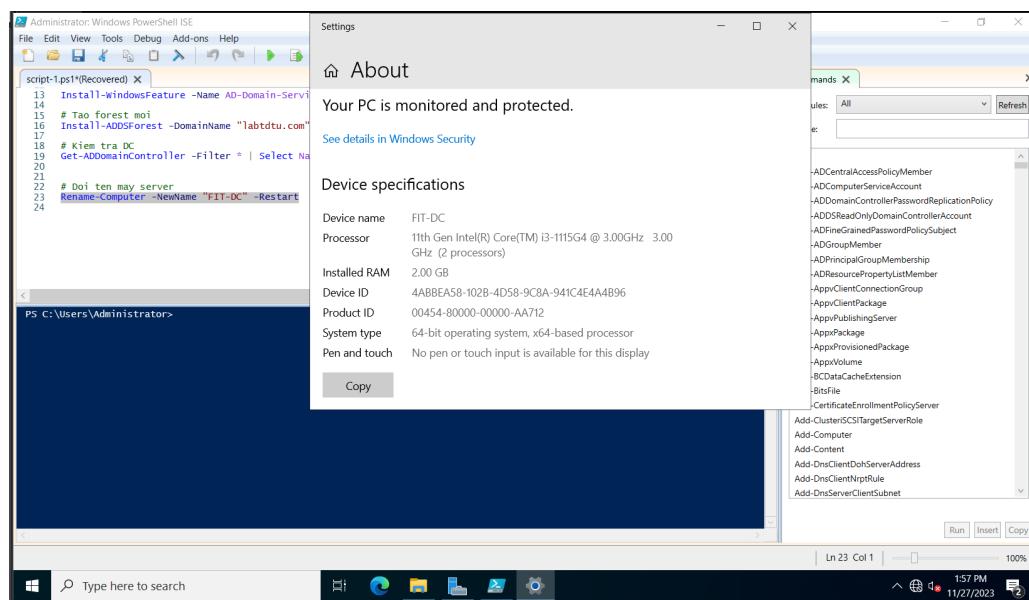
PS C:\Users\Administrator>

```

The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell ISE". It displays the output of the command "Get-ADDomainController -Filter * | Select Name, Domain, IsGlobalCatalog, OperationMasterRoles". The output shows that the server "WIN-C113POSGHAI" (which is "labtdtu.com") is a domain controller, specifically holding the Schema Master, Domain Naming Master, PDC Emulator, and RID Master roles. The PowerShell interface includes a "Commands" pane on the right containing a list of available cmdlets.

Hình 2.83: Kiểm tra đã nâng cấp lên DC

- Đổi tên server thành FIT-DC.



The screenshot shows two windows side-by-side. On the left is a Windows PowerShell window with the command "Rename-Computer -NewName "FIT-DC" -Restart". On the right is a "Device Settings" window for the device "FIT-DC", which shows the new name has been applied. The "About" section indicates the PC is monitored and protected. The "Device specifications" section lists the device name as FIT-DC, processor as 11th Gen Intel(R) Core(TM) i3-1115G4 @ 3.00GHz, 3.00 GHz (2 processors), 2.00 GB RAM, and other details. The PowerShell window shows the command was run successfully.

Hình 2.84: Đổi tên cho máy server

- Sau khi reset, DNS lúc này thành 127.0.0.1

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : FIT-DC
Primary Dns Suffix . . . . . : labtdtu.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : labtdtu.com

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-EB-D9-4F
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::540b:6181:f14e:2d%15(PREFERRED)
IPv4 Address . . . . . : 192.168.1.2(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-F6-B9-5E-00-0C-29-EB-D9-4F
DNS Servers . . . . . : ::1
127.0.0.1
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>
```

Hình 2.85: Kiểm tra lại địa chỉ IP

- Cấu hình lại DNS.

```
PS C:\Users\Administrator> # Doi ten may server
Rename-Computer -NewName "FIT-DC" -Restart
# Cau hinh lai DNS
Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -ServerAddresses "192.168.1.2"

PS C:\Users\Administrator> # cau hinh lai DNS
Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -ServerAddresses "192.168.1.2"
PS C:\Users\Administrator>
```

```
C:\Administrator: C:\Windows\system32\cmd.exe
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : FIT-DC
Primary Dns Suffix . . . . . : labtdtu.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : labtdtu.com

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-EB-D9-4F
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::540b:6181:f14e:2d%15(PREFERRED)
IPv4 Address . . . . . : 192.168.1.2(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-F6-B9-5E-00-0C-29-EB-D9-4F
DNS Servers . . . . . : ::1
192.168.1.2
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>
```

Hình 2.86: Cấu hình lại DNS

Join FIT-WEB vào domain

- Trên máy Fit-DC, thêm bản ghi cho **www.labtdtu.com** với địa chỉ **192.168.1.3**

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-1.ps1* 
22 # Doi ten may server
23 Rename-Computer -NewName "FIT-DC" -Restart
25 # Cau hinh lai DNS
26 Set-DnsClientServerAddress -InterfaceAlias "Ethernet0" -ServerAddresses "192.168.1.2"
27
28 #Cau hinh ban ghi cho www.labtdtu.com
29 $webServerIP = "192.168.1.3"
30 $recordName = "www"
31 $zoneName = "labtdtu.com"
32 $dnsServer = "FIT-DC"
33
34 Add-DnsServerResourceRecordA -Name $recordName -ZoneName $zoneName -IPv4Address $webServerIP -ComputerName $dnsServer
35 Get-DnsServerResourceRecord -ZoneName $zoneName -Name $recordName -RRType A -ComputerName $dnsServer
37

PS C:\Users\Administrator> # Cau hinh ban ghi cho www.labtdtu.com
$webServerIP = "192.168.1.3"
$recordName = "www"
$zoneName = "labtdtu.com"
$dnsServer = "FIT-DC"

Add-DnsServerResourceRecordA -Name $recordName -ZoneName $zoneName -IPv4Address $webServerIP -ComputerName $dnsServer
Get-DnsServerResourceRecord -ZoneName $zoneName -Name $recordName -RRType A -ComputerName $dnsServer
HostNmae RecordType Type Timestamp TimeToLive RecordData
----- ----- --- -----
www A ----- 0 01:00:00 192.168.1.3

PS C:\Users\Administrator>

```

Hình 2.87: Thêm và kiểm tra bản ghi cho website

- Trên máy FIT-WEB, cấu hình địa chỉ IP.

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-2.ps1* 
1 # CAU HINH DIA CHI IP CHO FIT-WEB
2 $adapter = "Ethernet0"
3 $ipaddress = "192.168.1.3"
4 $subnetmask = "255.255.255.0"
5 $defaultgateway = "192.168.1.1"
6 $dnsaddress = "192.168.1.2"
7
8 New-NetIPAddress -InterfaceAlias $adapter -IPAddress $ipaddress -PrefixLength 24 -DefaultGateway $defaultgateway
9 Set-DnsClientServerAddress -InterfaceAlias $adapter -ServerAddresses $dnsaddress
10
11
12 # Doi ten may server

AddressFamily : IPv4
Type : Unicast
PrefixLength : 24
PrefixOrigin : Manual
SuffixOrigin : Manual
AddressState : Tentative
ValidLifetime : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipPnSource : False
PolicyStore : ActiveStore
IPv4Address : 192.168.1.3
InterfaceIndex : 6
InterfaceAlias : Ethernet0
AddressFamily : IPv4
Type : Unicast
PrefixLength : 24
PrefixOrigin : Manual
SuffixOrigin : Manual
AddressState : Invalid
ValidLifetime : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipPnSource : True
PolicyStore : PersistentStore

PS C:\Users\Administrator>

```

Hình 2.88: Cài đặt địa chỉ IP

- Kiểm tra cấu hình IP.

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.20348.2113]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-58NTS7QKSSJ
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet0:

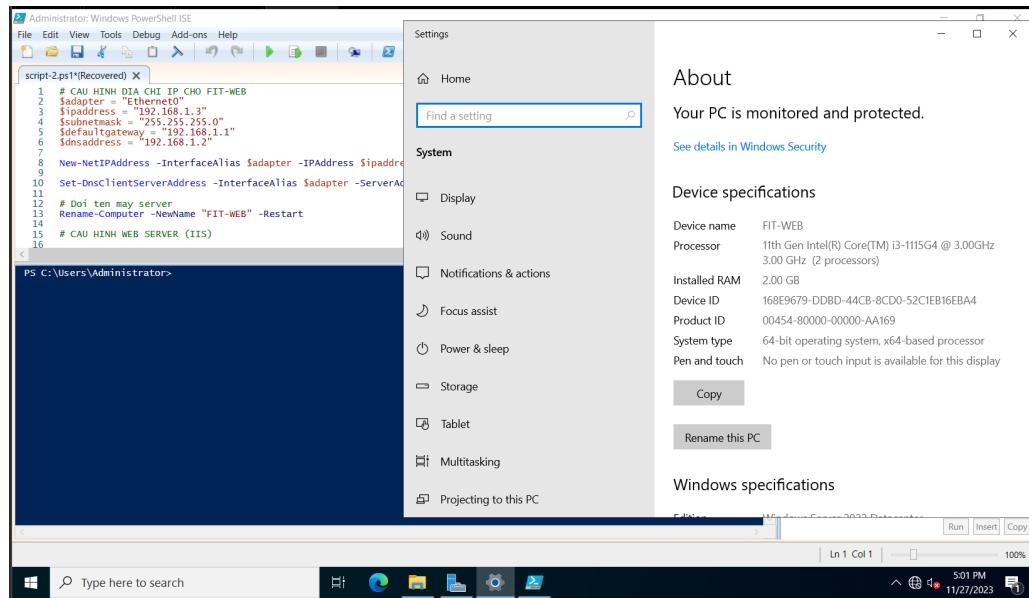
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address . . . . . : 00-0C-29-17-93-EA
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::f25e:92c6:c96e:b5e0%6(PREFERRED)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2C-F6-EF-F5-00-0C-29-17-93-EA
DNS Servers . . . . . : 192.168.1.2
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>

```

Hình 2.89: Kiểm tra địa chỉ IP

- Đổi tên sang FIT-WEB



Hình 2.90: Đổi tên thành FIT-WEB

- Join FIT-WEB vào domain labtdtu.com

```

# CAU HINH DIA CHI CHO FIT-WEB
$InterfaceAlias = "Ethernet"
$IpAddress = "192.168.1.3"
$Subnetmask = "255.255.255.0"
$DefaultGateway = "192.168.1.1"
$DnsAddress = "192.168.1.2"

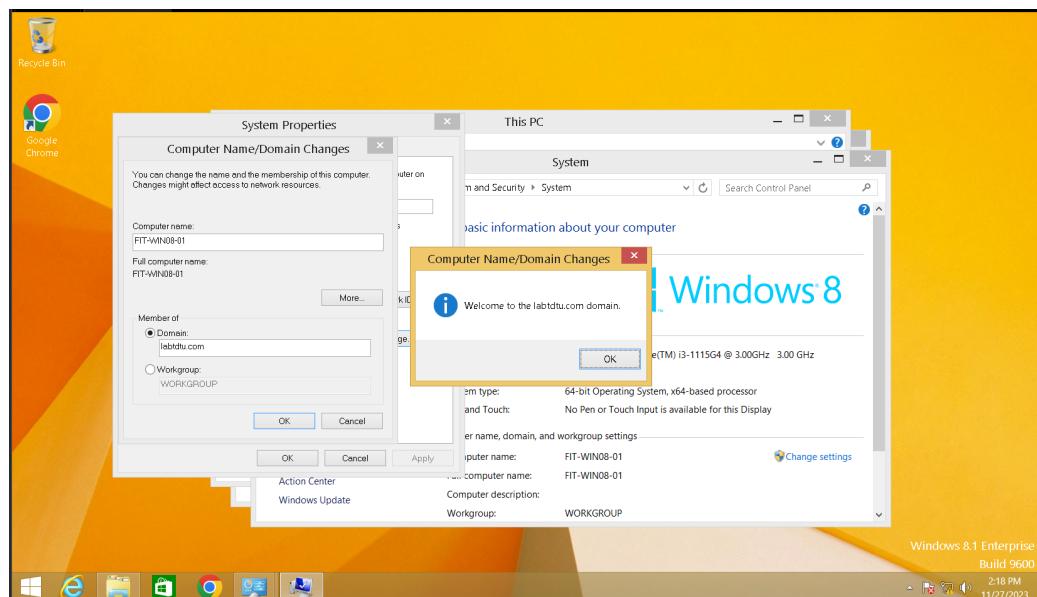
New-NetIPAddress -InterfaceAlias $InterfaceAlias -IPAddress $IpAddress -PrefixLength 24
Set-DnsClientServerAddress -InterfaceAlias $InterfaceAlias -ServerAddresses $DnsAddress
# Doi ten may server
Rename-Computer -NewName "FIT-WEB" -Restart
# Join vao domain labtdtu.com
Add-Computer -DomainName "labtdtu.com" -Credential (Get-Credential) -Restart
# CAU HINH WEB SERVER (IIS)
#<#>Add-WebAppPool -Name "Default Web Site"

```

Hình 2.91: Join vào domain

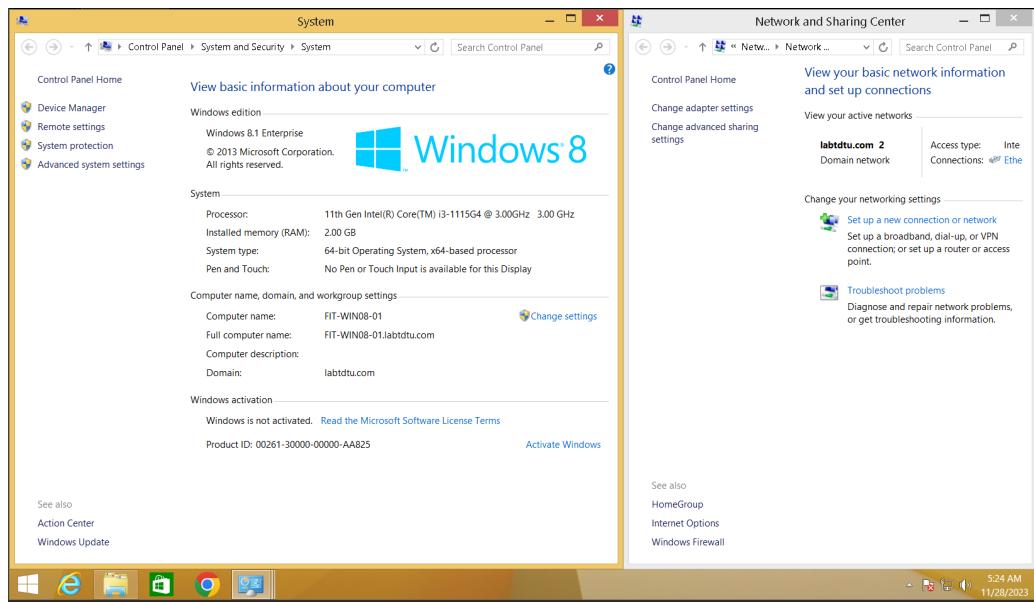
Join máy FIT-WIN08-01 vào domain

- Cấu hình địa chỉ IP cho **FIT-WIN08-01** có địa chỉ ip là 192.168.1.101
- Join máy FIT-WIN08-01 vào domain labtdtu.com



Hình 2.92: Máy client (192.168.1.101) test join vào domain

- Kiểm tra join vào domain thành công hay chưa.



Hình 2.93: Kết quả join vào domain

3.2 Cài Active Directory Certificate Services role Cấu hình web server (IIS)

- Cài đặt cấu hình Web Server bằng lệnh

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Administrator: PS C:\Users\Administrator> # cài đặt IIS
Administrator: PS C:\Users\Administrator> $subnetmask = "255.255.255.0"
Administrator: PS C:\Users\Administrator> $defaultgateway = "192.168.1.1"
Administrator: PS C:\Users\Administrator> $dnsaddress = "192.168.1.2"
Administrator: PS C:\Users\Administrator> New-NetIPAddress -InterfaceAlias $adapter -IPAddress $ipaddress -PrefixLength 24 -DefaultGateway $defaultgateway
Administrator: PS C:\Users\Administrator> Set-DnsClientServerAddress -InterfaceAlias $adapter -ServerAddresses $dnsaddress
Administrator: PS C:\Users\Administrator> # Đổi tên máy server
Administrator: PS C:\Users\Administrator> Rename-Computer -NewName "FIT-WEB" -Restart
Administrator: PS C:\Users\Administrator> # Join vào domain labtdtu.com
Administrator: PS C:\Users\Administrator> Add-Computer -DomainName "labtdtu.com" -Credential (Get-Credential) -Restart
Administrator: PS C:\Users\Administrator> # Cấu hình Web Server
Administrator: PS C:\Users\Administrator> Install-WindowsFeature -Name Web-Server -IncludeManagementTools
Administrator: PS C:\Users\Administrator>

```

Directory: C:\

Mode	LastWriteTime	Length	Name
d----	11/28/2023 10:11 PM		WEBSITE

```

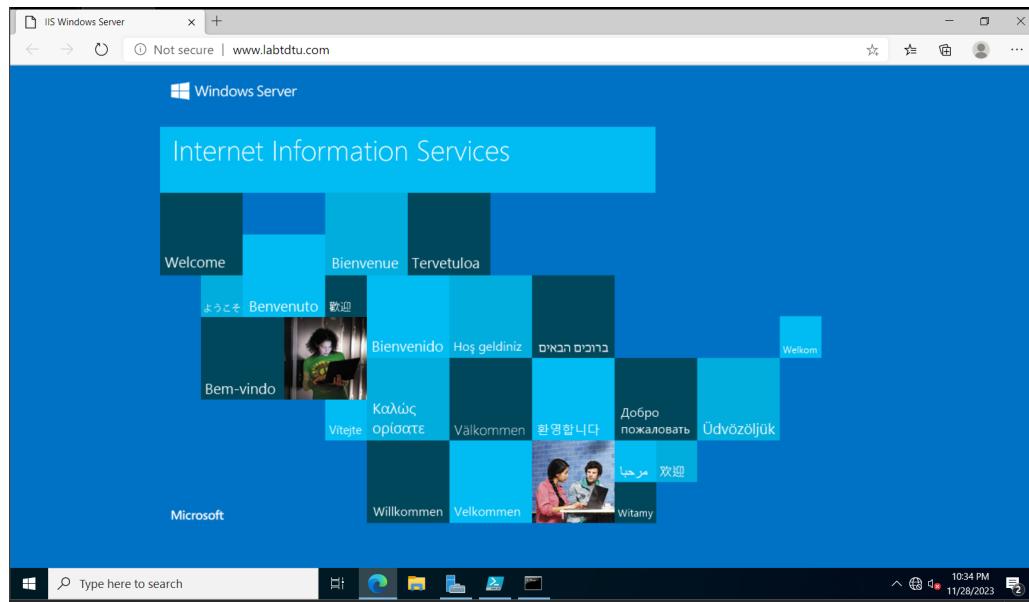
PS C:\Users\Administrator> # cài hinh web Server
Install-WindowsFeature -Name Web-Server -IncludeManagementTools
Success Restart Needed Exit Code Feature Result
----- ----- ----- -----
True No Success {Common HTTP Features, Default Document, ...

```

PS C:\Users\Administrator>

Hình 2.94: cài đặt IIS

- Truy cập thử website <http://www.labtdtu.com>



Hình 2.95: Truy cập website với http

Cấu hình Active Directory Certificate Services

- Cài đặt Active Directory Certificate Services

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-1.ps1* X Commands X
28 # Cau hinh ban ghi cho www.labtdtu.com
29 $webServerIP = "192.168.1.3"
30 $recordName = "www"
31 $zoneName = "labtdtu.com"
32 $dnsServer = "FIT-DC"
33
34 Add-DnsServerResourceRecordA -Name $recordName -ZoneName $zoneName -IPv4Address $webServerIP -ComputerName $dnsServer
35
36 Get-DnsServerResourceRecord -ZoneName "labtdtu.com" -Name "www" -RRType A -ComputerName "FIT-DC"
37 # -> CHUYEN QUA FIT-WEB
38
39 # CAI DAT AD CS
40 Install-WindowsFeature -Name ADCS-Cert-Authority -IncludeManagementTools
41 Install-WindowsFeature -Name ADCS-Web-Enrollment
42
43
Add-DnsServerResourceRecordA -Name $recordName -ZoneName $zoneName -IPv4Address $webServerIP -ComputerName $dnsServer
Get-DnsServerResourceRecord -ZoneName "labtdtu.com" -Name "www" -RRType A -ComputerName "FIT-DC"
HostName RecordType Type Timestamp TimeToLive RecordData
-----
www A 1 0 01:00:00 192.168.1.3
PS C:\Users\Administrator> # CAI DAT AD CS
Install-WindowsFeature -Name ADCS-Cert-Authority -IncludeManagementTools
Install-WindowsFeature -Name ADCS-Web-Enrollment
Success Restart Needed Exit Code Feature Result
True No Success {Active Directory Certificate Services, Ce...
True No Success {Certification Authority Web Enrollment, A...

```

Hình 2.96: Cài đặt AD CS

- Cấu hình Active Directory Certificate Services

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-1.ps1* 
40 # CAI DAT AD CS
41 Install-WindowsFeature -Name ADCS-Cert-Authority -IncludeManagementTools
42 Install-WindowsFeature -Name ADCS-Web-Enrollment
43
44 # Cấu hình AD CS
45 Install-AdcsCertificationAuthority
46 -Credential (Get-Credential)
47 -CACommonName "LABTDTU-CA"
48 -CADistinguishedNameSuffix "DC=labtdu,DC=com"
49 -CryptographicProviderName "RSAMicrosoft Software Key Storage Provider"
50 -KeyLength 2048
51 -HashAlgorithmName SHA1
52 -ValidityPeriod Years
53 -ValidityPeriodUnits 3
54 -DatabaseDirectory "C:\windows\system32\certlog"
55 -LogDirectory "C:\windows\system32\certlog"
56 -Force
57
58
59 #>>> Get-Credential at command pipeline position 1
Supply values for the following parameters:
ErrorId ErrorString
0

PS C:\Users\Administrator>
Completed
Type here to search Run Insert Copy
Ln 106 Col 28 1047 PM 11/28/2023

```

Hình 2.97: Cấu hình AD CS cài đặt CA

- Cài đặt CA Web Enrollment

```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-1.ps1* 
49 -CADistinguishedNameSuffix "DC=labtdu,DC=com"
50 -CryptographicProviderName "RSAMicrosoft Software Key Storage Provider"
51 -KeyLength 2048
52 -HashAlgorithmName SHA1
53 -ValidityPeriod Years
54 -ValidityPeriodUnits 3
55 -DatabaseDirectory "C:\windows\system32\certlog"
56 -LogDirectory "C:\windows\system32\certlog"
57 -Force
58
59 Install-AdcswebEnrollment -whatIf
60 # ->>> CHUYEN QUA FIT-WEBSITE
61

PS C:\Users\Administrator> Add-WindowsFeature ADCS-Web-Enrollment
Success Restart Needed Exit Code Feature Result
----- ----- ----- -----
True No NoChangeNeeded []

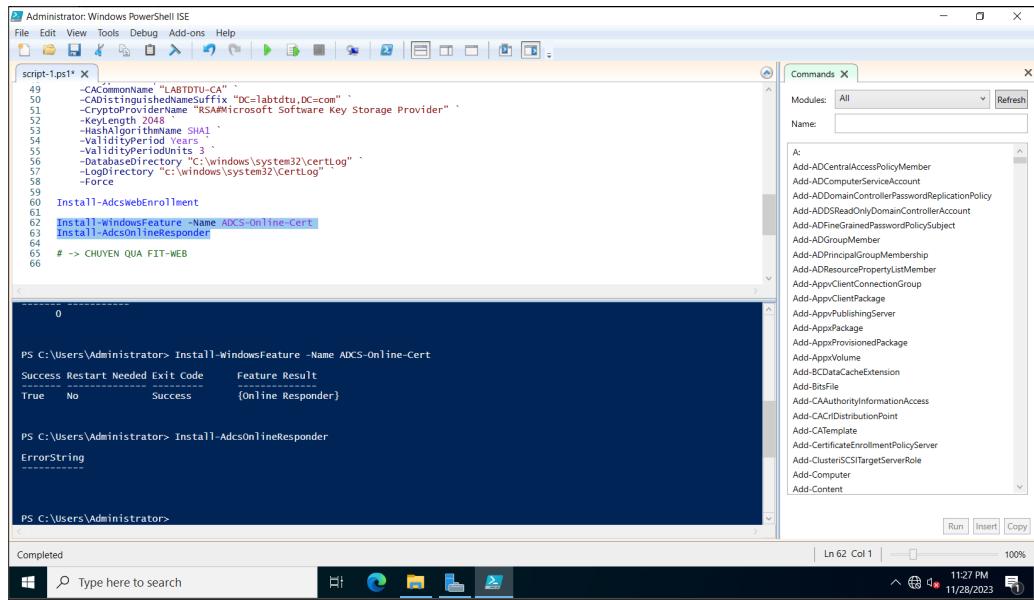
PS C:\Users\Administrator> Install-AdcswebEnrollment -whatIf
What If: Perform the operation "Install-AdcswebEnrollment" on target "FIT-DC".
The Certification Authority Web Enrollment role will be installed with the following properties:
    CAConfig: FIT-DC.labtdu.com\LABTDTU-CA
PS C:\Users\Administrator>

Completed
Type here to search Run Insert Copy
Ln 14 Col 28 11:15 PM 11/28/2023

```

Hình 2.98: Cài đặt CA Web Enrollment

● Cài đặt Online responder



```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-lps1* x Commands x
script-lps1* x Modules: All Refresh
50 -CACertificateName "LABTDTU-CA"
51 -CADistinguishedNameSuffix "DC=labtdtu,DC=com"
52 -CryptoProviderName "RSAMicrosoft Software Key Storage Provider"
53 -KeyAlgorithm "RSA"
54 -HashAlgorithmName "SHA1"
55 -ValidityPeriod_Years 1
56 -ValidityPeriodUnits 3
57 -DataDirectory "C:\windows\system32\certLog"
58 -LogDirectory "C:\windows\system32\certLog"
59 -Force
60 Install-AdcswebEnrollment
61 Install-WindowsFeature -Name ADCS-Online-Cert
62 Install-AdcsOnlineResponder
63
64
65 # -> CHUYEN QUA FIT-WEB
66

PS C:\Users\Administrator> Install-WindowsFeature -Name ADCS-Online-Cert
Success Restart Needed Exit Code Feature Result
True No Success {Online Responder}

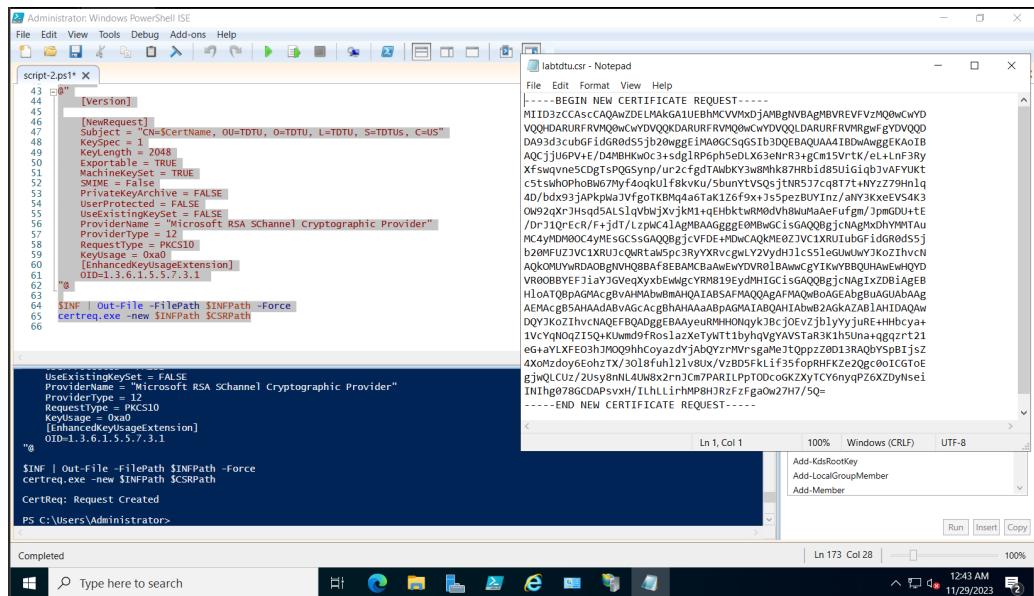
PS C:\Users\Administrator> Install-AdcsOnlineResponder
ErrorString

PS C:\Users\Administrator>
Completed
Ln 62 Col 1 11:27 PM 11/28/2023
Run Insert Copy
Type here to search

```

Hình 2.99: Cài đặt Online responder

● Tạo Certificate Request



```

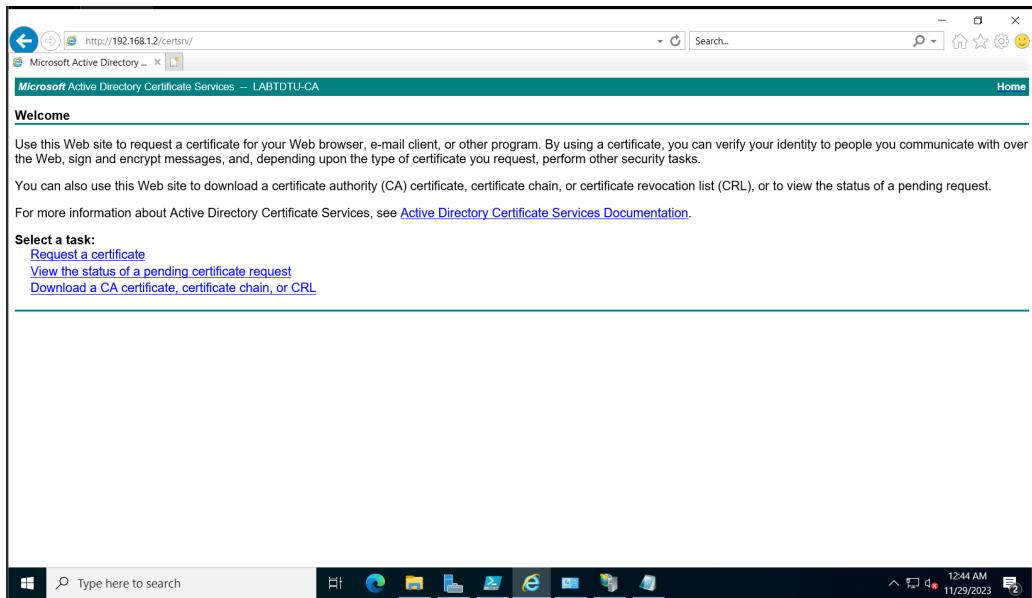
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-zps1* x labtdtu.csr - Notepad
script-zps1* x Commands x
script-zps1* x Modules: All Refresh
43 [Version]
44
45 [NewRequest]
46 Subject = "CN=$CertName, OU=TDTU, O=TDTU, L=TDTU, S=TDTUS, C=US"
47 KeySpec = 1
48 KeyLength = 2048
49 MachineKeySet = $true
50 Exportable = $true
51 SMIME = $false
52 PrivateKeyUsage = $false
53 UserKeySet = $false
54 UseExistingKeySet = $false
55 ProviderName = "Microsoft RSA Schannel Cryptographic Provider"
56 ProviderType = 12
57 RequestType = "PKCS10"
58 RequestPath = "$INPath"
59 KeyUsage = 0x40
60 [EnhancedKeyUsageExtension]
61 OID=1.3.6.1.5.5.7.3.1
62 "
63
64 $INF | Out-File -FilePath $INPath -Force
certreq.exe -new $INPath $CSRPath
65

66
67 UseExistingKeySet = $false
68 ProviderName = "Microsoft RSA Schannel Cryptographic Provider"
69 ProviderType = 12
70 RequestType = "PKCS10"
71 KeyUsage = 0x40
72 [EnhancedKeyUsageExtension]
73 OID=1.3.6.1.5.5.7.3.1
74 "
75
76 $INF | Out-File -FilePath $INPath -Force
certreq.exe -new $INPath $CSRPath
77 CertReq: Request created
78 PS C:\Users\Administrator>
Completed
Ln 173 Col 28 12:43 AM 11/29/2023
Run Insert Copy
Type here to search

```

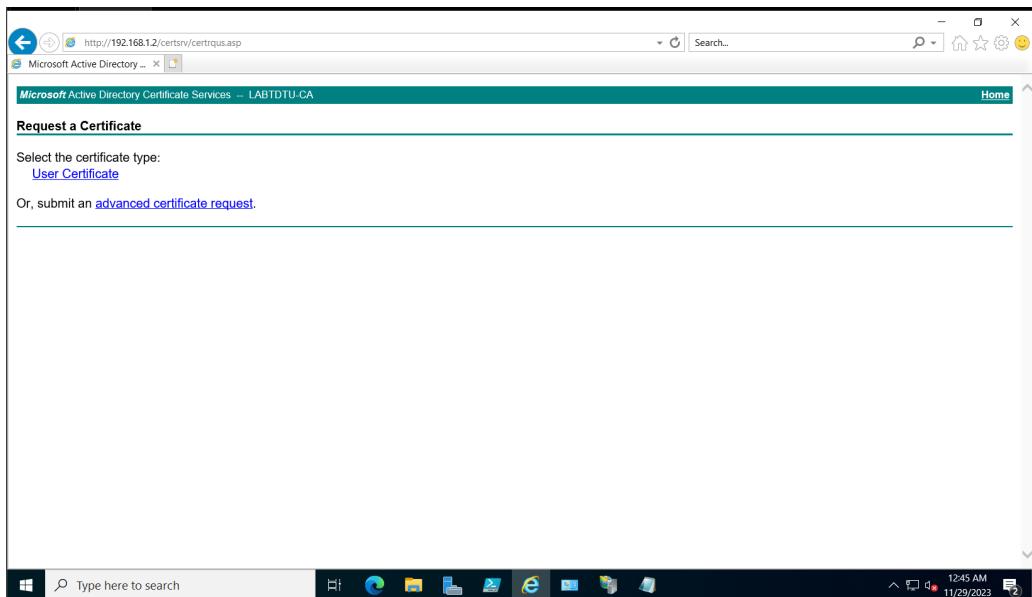
Hình 2.100: Tạo Certificate Request

- Truy cập trang <http://192.168.1.2/certsrv> > Chọn Request a Certificate



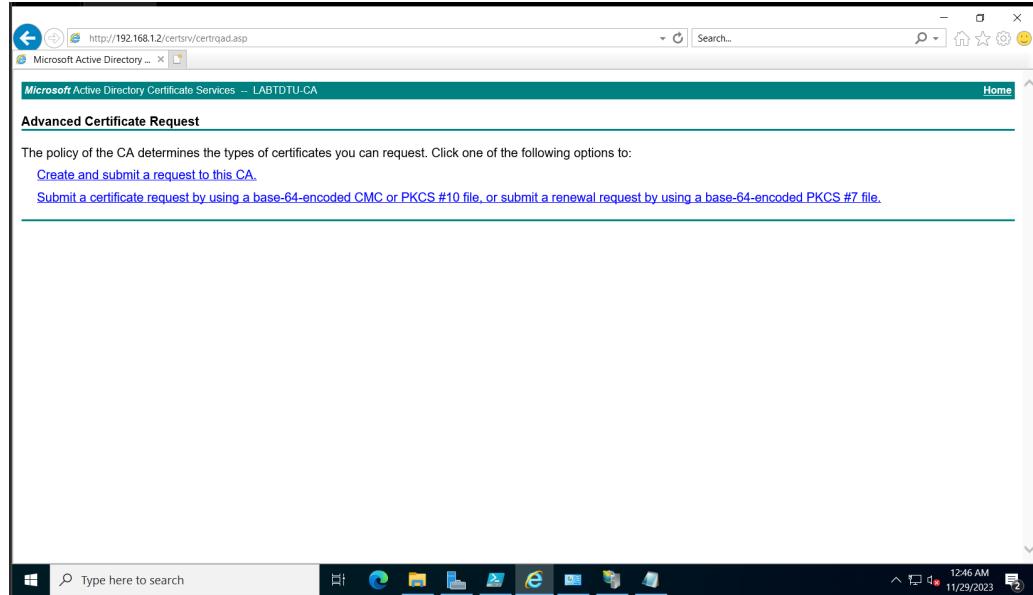
Hình 2.101: Truy cập certsrv chọn Request a Certificate

- Chọn **Submit**



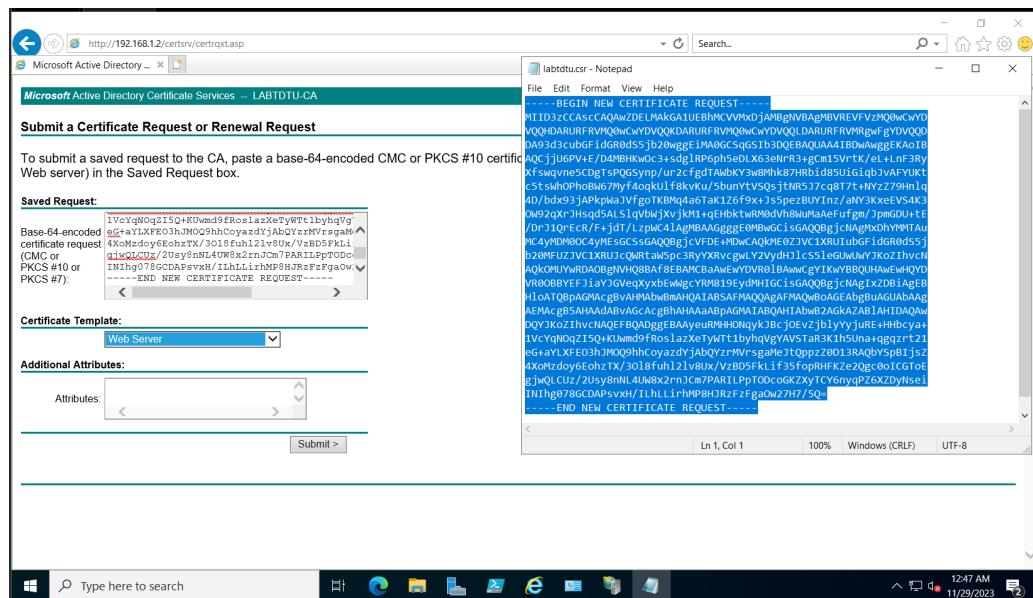
Hình 2.102: Submit

- Chọn Submit a certificate request by using base-64-encoded..



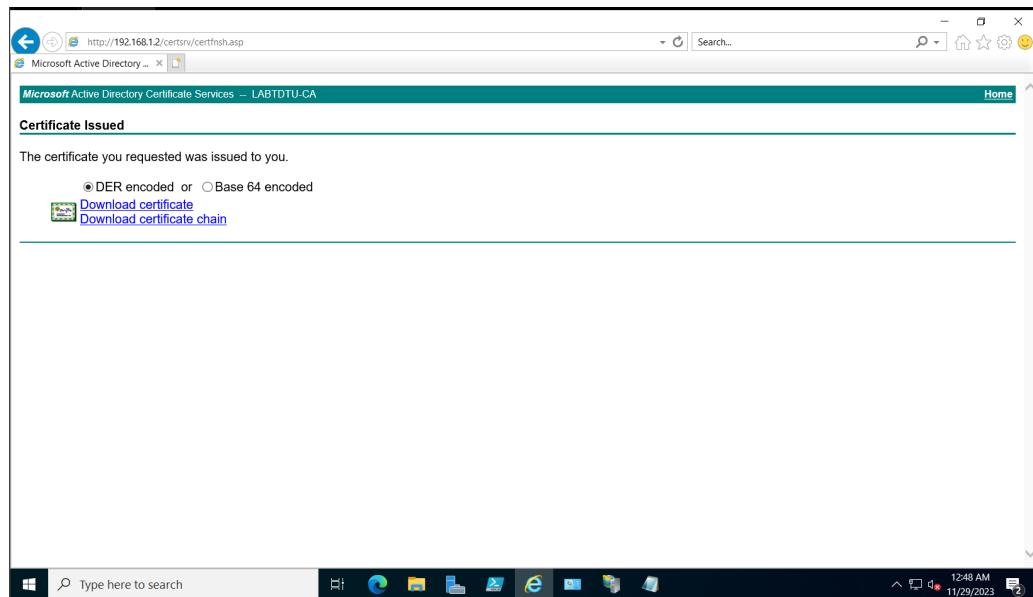
Hình 2.103: Submit a certificate request by using base-64-encoded...

- Copy nội dung CSR và paste vào và chọn template webserver.



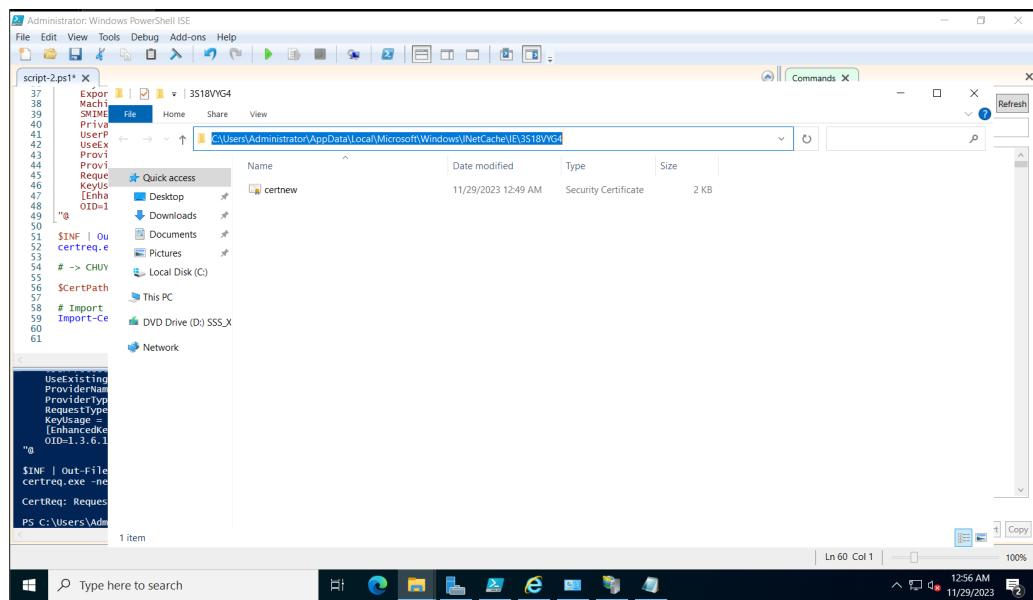
Hình 2.104: Copy nội dung CSR và paste vào và chọn template webserver

- Submit thành công, chọn **Download certificate** tải chứng chỉ về máy.



Hình 2.105: Download Certificate

- Lấy đường dẫn tới file certnew vừa được tải.



Hình 2.106: Lấy đường dẫn tới file certnew vừa được tải

- Hoàn thành chứng chỉ

The screenshot shows a Windows PowerShell ISE window with the following content:

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-2.ps1* X Commands X
Exportable = TRUE
MachineKeySet = TRUE
Protected = FALSE
PrivatekeyArchive = FALSE
UserProtected = FALSE
UseExcludedKeysSet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0x40
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1
# @
$INF | Out-File -FilePath $INFPath -Force
certreq.exe -new $INFPath $CSRPath
# -> CHUYEN QUA IE DE TIEN HANH TAI FILE CER
$CertPath = "C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\3518VYGI\certnew.cer"
Import-Certificate -FilePath $CertPath -CertStoreLocation "Cert:\LocalMachine\My"
Import-Certificate -FilePath $CertPath -CertStoreLocation "Cert:\LocalMachine\My"

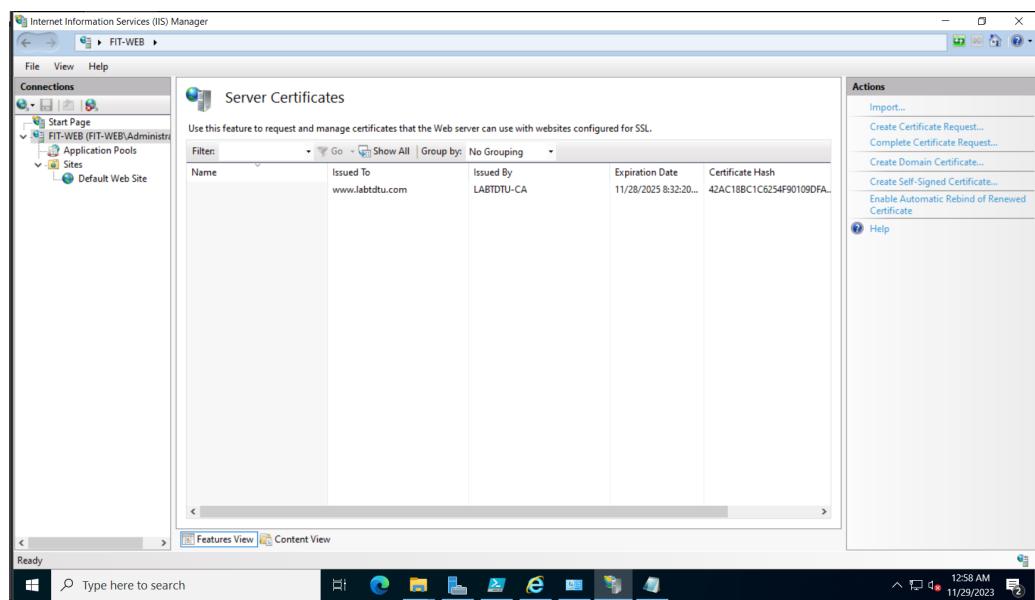
PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My
Thumbprint Subject
42AC18BC1C6254F901090FACDD4FB960BD29037 CN=www.labtdtu.com, OU=TDTU, O=TDTU, L=TDTU, S=TDTU, C=US

PS C:\Users\Administrator> |
```

The right side of the window displays a 'Commands' pane with a list of available cmdlets, such as Add-AppClientConnectionGroup, Add-AppClientPackage, and Add-AppVolume.

Hình 2.107: Complete chứng chỉ

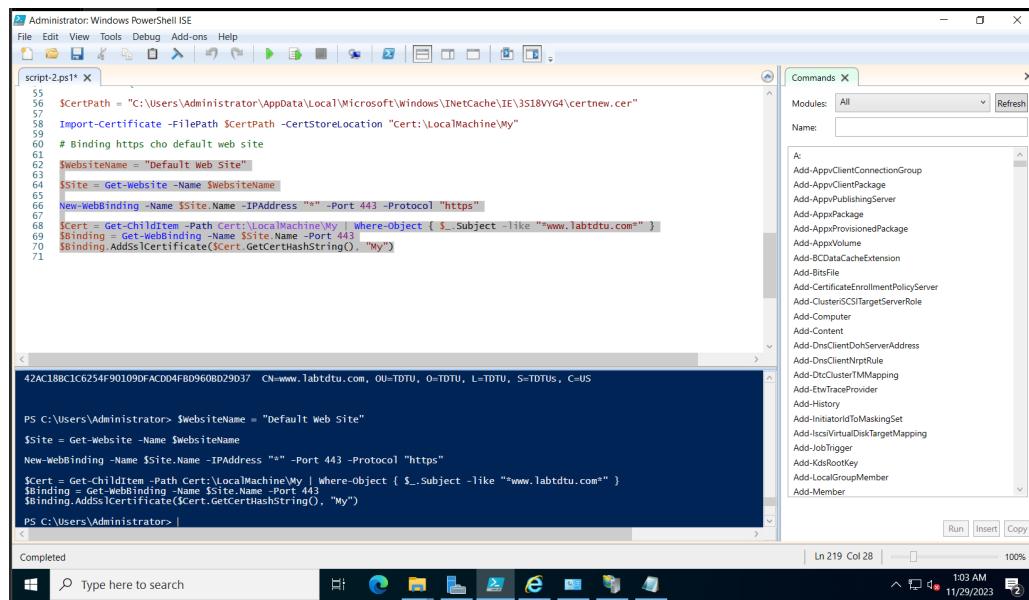
- Kiểm tra chứng chỉ đã được tạo



Hình 2.108: Chứng chỉ đã được tạo

TạoHttps cho Website

Binding https trên port 443 cho website



```

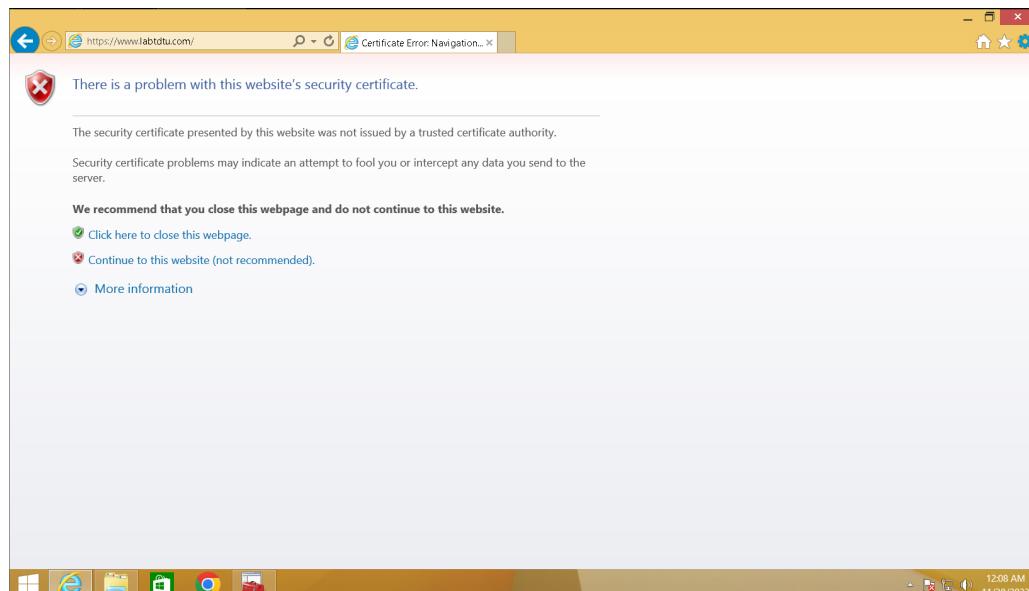
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
script-2.ps1* Commands x
55 $certPath = "C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\3S18VY4\certnew.cer"
56 Import-Certificate -FilePath $certPath -CertStoreLocation "Cert:\LocalMachine\My"
57 # Binding https cho default web site
58 $websiteName = "Default Web Site"
59 $site = Get-Website -Name $websiteName
60 New-WebBinding -Name $site.Name -IPAddress "*" -Port 443 -Protocol "https"
61 $cert = Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object { $_.Subject -like "www.labtdtu.com" }
62 $binding = Get-WebBinding -Name $site.Name -Port 443
63 $binding.AddsCertificate($cert.GetCertHashString(), "My")
71
PS C:\Users\Administrator> $websiteName = "Default Web Site"
$site = Get-Website -Name $websiteName
New-WebBinding -Name $site.Name -IPAddress "*" -Port 443 -Protocol "https"
$cert = Get-ChildItem -Path Cert:\LocalMachine\My | Where-Object { $_.Subject -like "www.labtdtu.com" }
$binding = Get-WebBinding -Name $site.Name -Port 443
$binding.AddsCertificate($cert.GetCertHashString(), "My")
PS C:\Users\Administrator>
Completed

```

Hình 2.109: Chứng chỉ đã được tạo

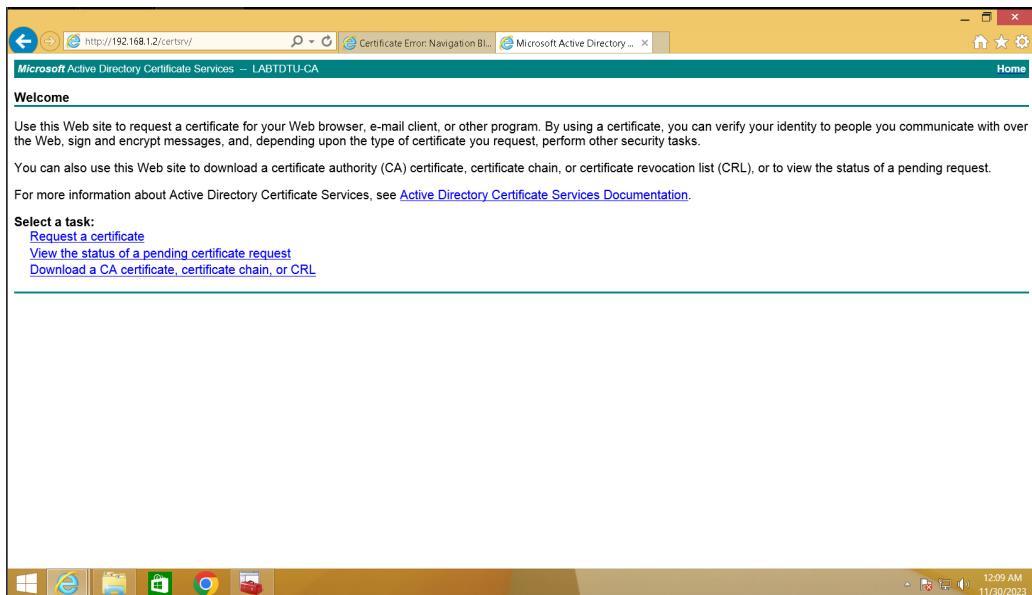
3.3 Kiểm tra

- Truy cập website labtdtu.com trên máy FIT-WIN08-01 (Chưa có chứng chỉ)



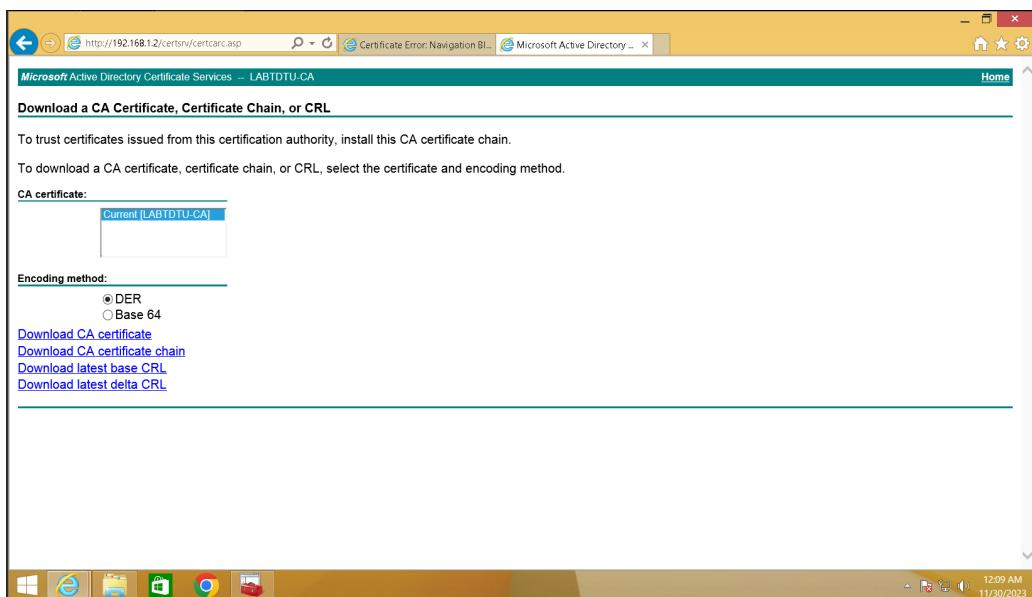
Hình 2.110: Truy cập website trên máy PC client

- Truy cập <http://192.168.1.2/certsrv> để tải chứng chỉ CA về máy



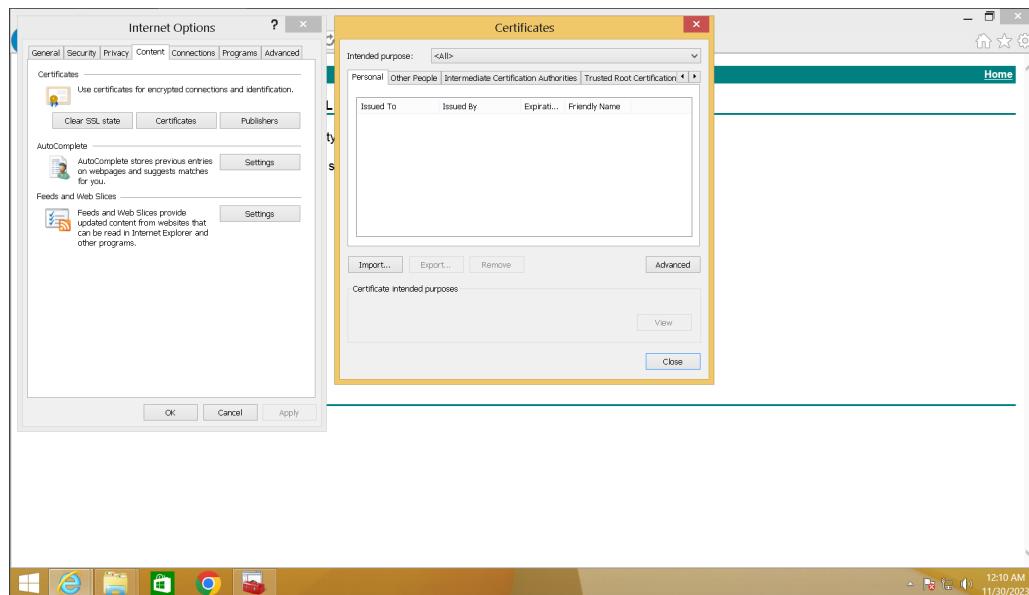
Hình 2.111: Truy cập để tải CA

- Tải chứng chỉ



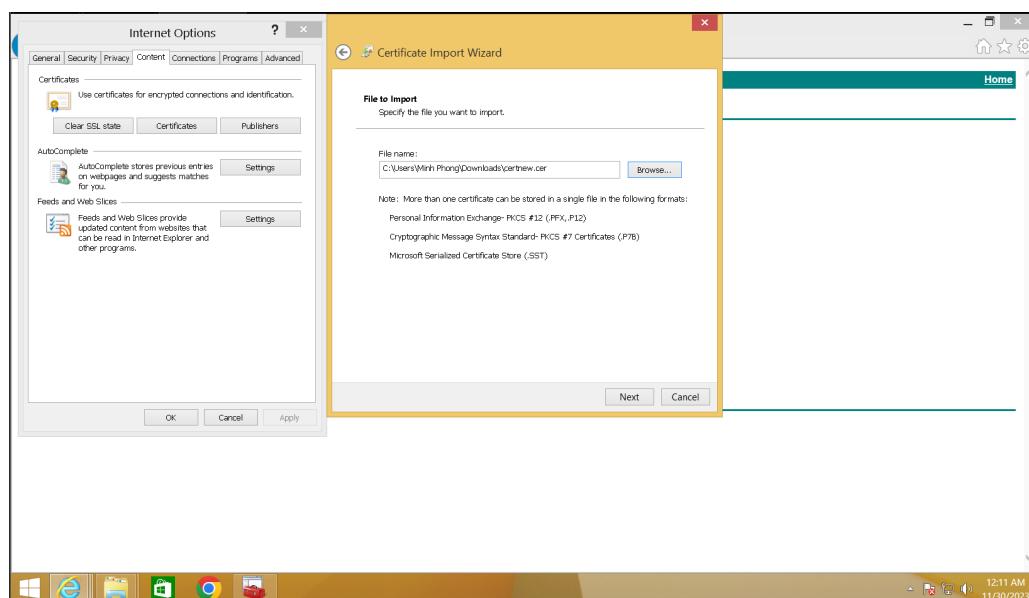
Hình 2.112: Download CA

- Trên IE -> Bánh răng -> Internet Options -> Content -> Certificate



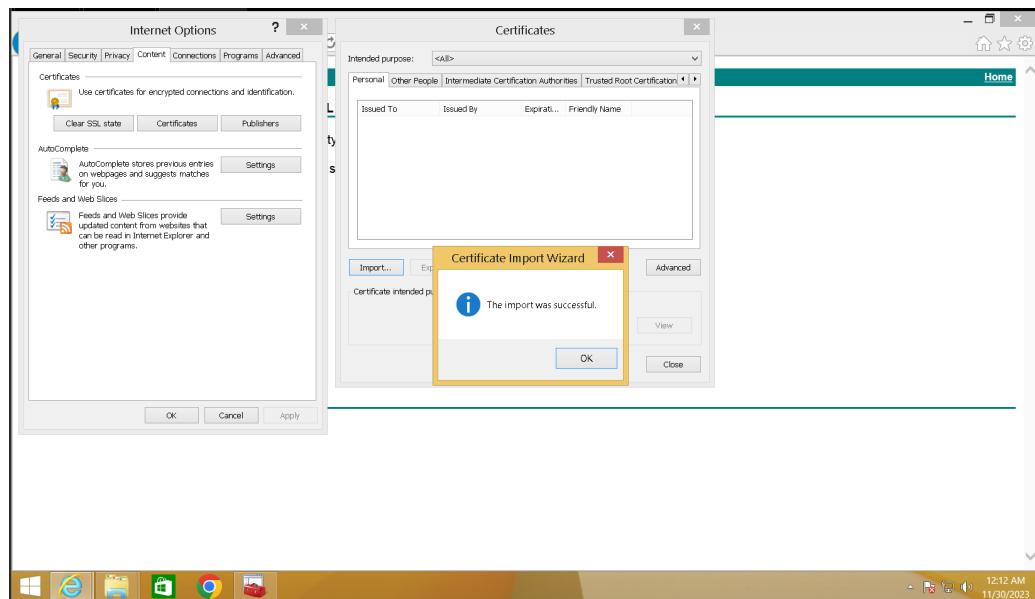
Hình 2.113: Bánh răng - Internet Options - Tab Content - Certificate

- Import file vừa tải vào Trusted Root Certification Authorities



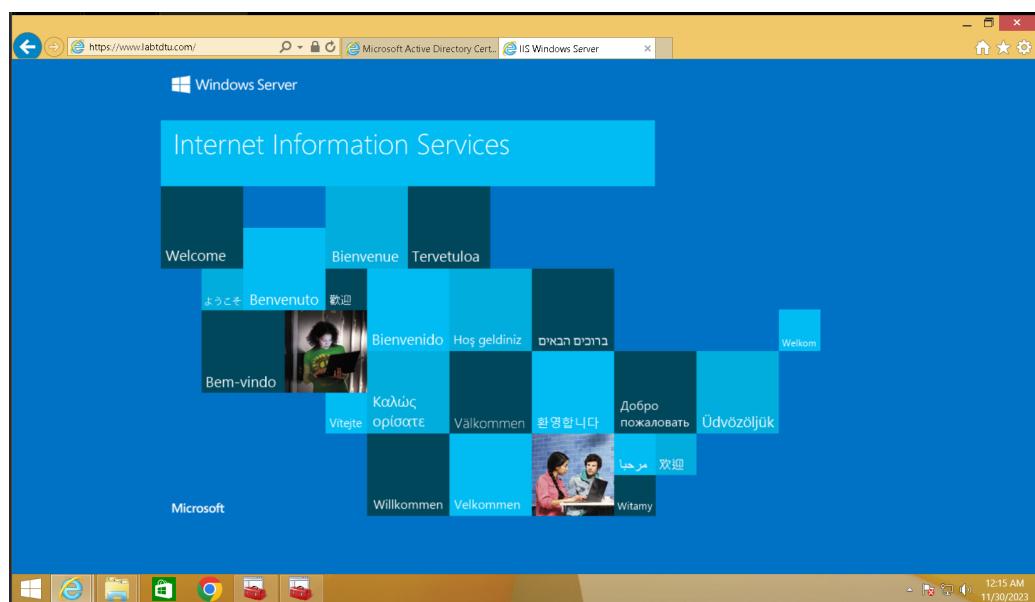
Hình 2.114: Import file vừa tải vào Trusted Root Certification Authorities

- Import hoàn tất



Hình 2.115: Đã import

- Truy cập lại <https://www.labtdtu.com>



Hình 2.116: Truy cập lại website

Chương 3

Kết luận

Sau khi kết thúc bài đồ án cuối kỳ, nhóm 20 đã nắm được những nội dung như sau:

- Hiểu về hoạt động của Active Directory Certificate Services (AD CS)
 - Biết cách AD CS tạo và quản lý chứng chỉ số.
 - Hiểu về quy trình cấp phát chứng chỉ và quy trình xác thực.
 - Nắm rõ về các thành phần chính của AD CS như Certification Authority (CA), Registration Authority (RA), và Database.
- Vận dụng AD CS để bảo mật website
 - Biết cách sử dụng AD CS để tạo và quản lý chứng chỉ số SSL/TLS.
 - Hiểu về ưu điểm của việc sử dụng chứng chỉ SSL/TLS trong bảo mật website, bao gồm cả mức độ bảo mật cao và sự tin cậy từ phía người sử dụng.
 - Có khả năng triển khai chứng chỉ trong môi trường web server.
- Thực hành trên giao diện đồ họa (GUI)
 - Biết cách sử dụng giao diện quản lý của AD CS để thực hiện các tác vụ như cấp chứng chỉ.

- Có khả năng thực hiện các thao tác quản lý chứng chỉ thông qua giao diện người dùng.
- Thực hành bằng PowerShell
 - Hiểu cách sử dụng PowerShell để tự động hóa các tác vụ liên quan đến AD CS.
 - Có khả năng tạo, quản lý, và thực hiện các tác vụ khác liên quan đến chứng chỉ bằng PowerShell.

Bên cạnh đó, nhóm 20 chưa nắm vững được các kiến thức về tư duy an toàn như là hiểu về các best practices khi triển khai AD CS để đảm bảo tính ổn định và an toàn hay là nắm vững về quản lý khóa và chứng chỉ, cũng như quản lý chuỗi chứng chỉ.

Tài liệu tham khảo

- [1] Brian Desmond, *Active Directory 5th edition*, 2003
- [2] Mike F. Robbins, *PowerShell 101*, 2020
- [3] Microsoft, *Implement and manage Active Directory Certificate Services*