3

Lab

Triển khai Active Directory trên Windows Server

Setting up Active Directory in Windows Server

Thực hành môn Quản trị mạng và hệ thống

GVTH: Nguyễn Thanh Hòa

Tháng 9/2017

Lưu hành nội bộ

A. TỔNG QUAN

1. Mục tiêu

- Xây dựng mô hình Workgroup
- Xây dựng mô hình Domain với Active Directory
- So sánh sự khác nhau giữa 2 mô hình Workgroup và Domain
- Triển khai ADC và RODC trông mô hình sử dụng Active Directory
- So sánh ADC và RODC trong mô hình sử dụng Active Directory

2. Thời gian thực hành

- Thực hành tại lớp: **5** tiết
- Hoàn thành báo cáo kết quả thực hành: tối đa **7** ngày.

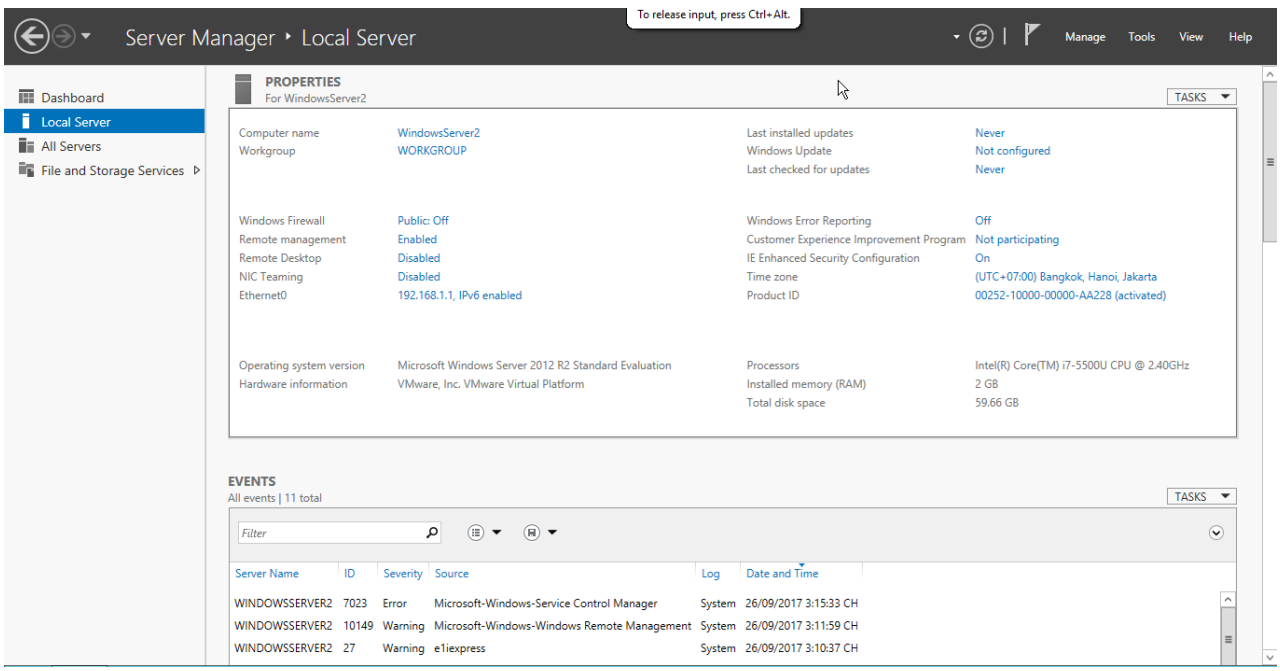
3. Môi trường & công cụ

Sinh viên cần chuẩn bị trước máy tính với môi trường thực hành gồm:

Tối thiểu 2 máy sử dụng Windows Server 2012 *(Domain Controller)*

Tối thiểu 1 máy sử dụng Windows 7/8/10/Server 2012 *(Client - có thể tham gia domain)*

***Ghi chú**: Các máy trên có thể sử dụng dưới dạng máy ảo trên phần mềm VMWare, sinh viên cũng có thể sử dụng Windows Server bản mới hơn để thực hành.*



Hình 1. Server Manager trên Windows Server 2012

B. THỰC HÀNH

1. Xây dựng mô hình Workgroup

> Ⓡ Trước khi bắt đầu thực hành, sinh viên hãy trả lời câu hỏi sau:
>
> *Mô hình Workgroup hoạt động như thế nào?*

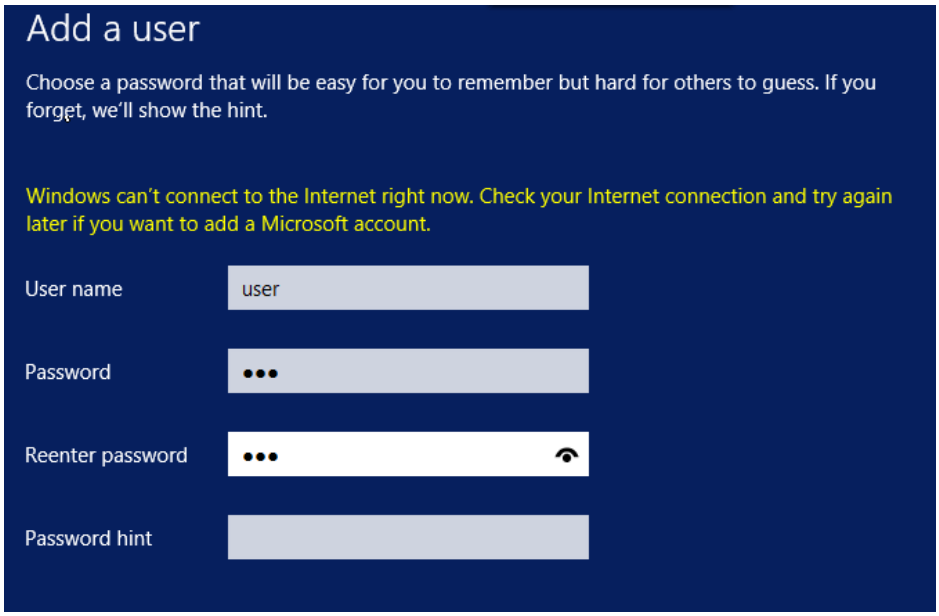
Xây dựng mô hình Workgroup như sau:

Hình 2. Mô hình Workgroup

Mô hình này chỉ cần 2 máy tính Windows trong cùng 1 lớp mạng như bảng sau:

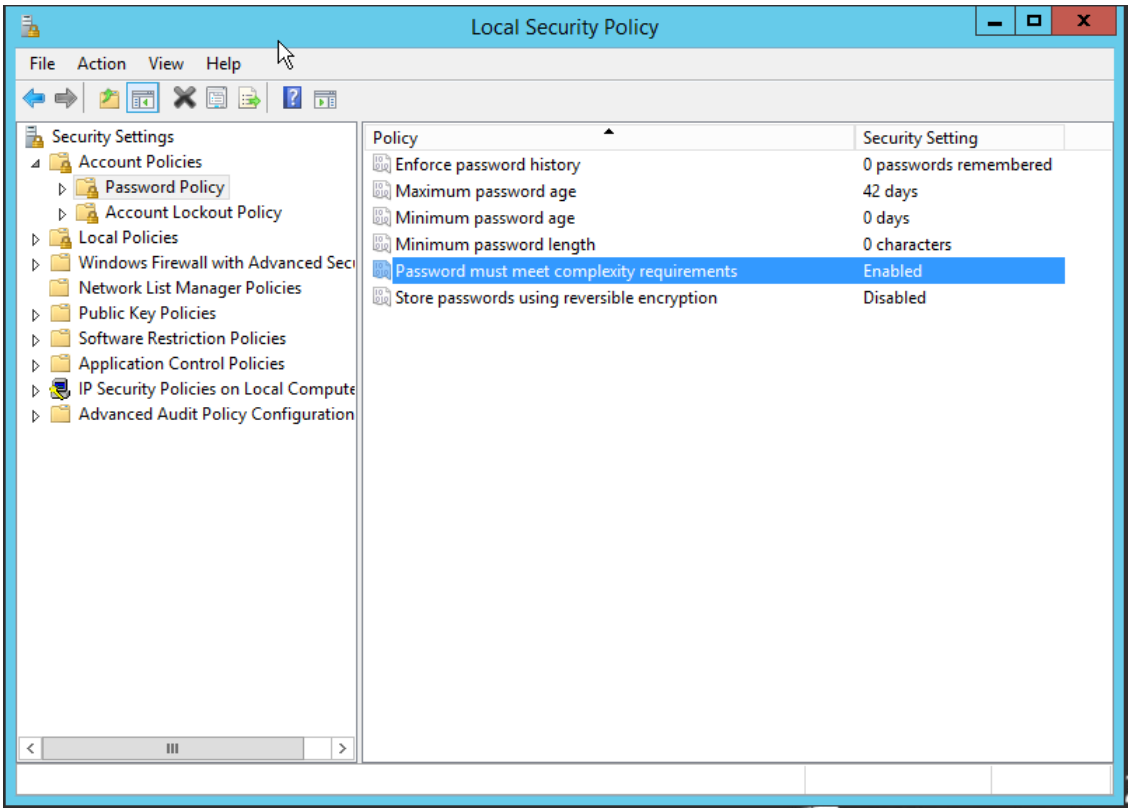
	IP Address	Subnet Mask
Client	192.168.1.2	255.255.255.0
File Server	192.168.1.1	255.255.255.0

- **Bước 1:** Trên máy chủ Windows Server 2012 đóng vai trò là File Server, tạo:
  - Thư mục **Data** để chia sẻ dữ liệu
  - Tạo tài khoản **user** có mật khẩu là **123** và không cho phép user thay đổi thông tin của mình, chỉ có **Administrator** mới được quyền thay đổi



Hình 3. Tạo user mới trong Windows Server

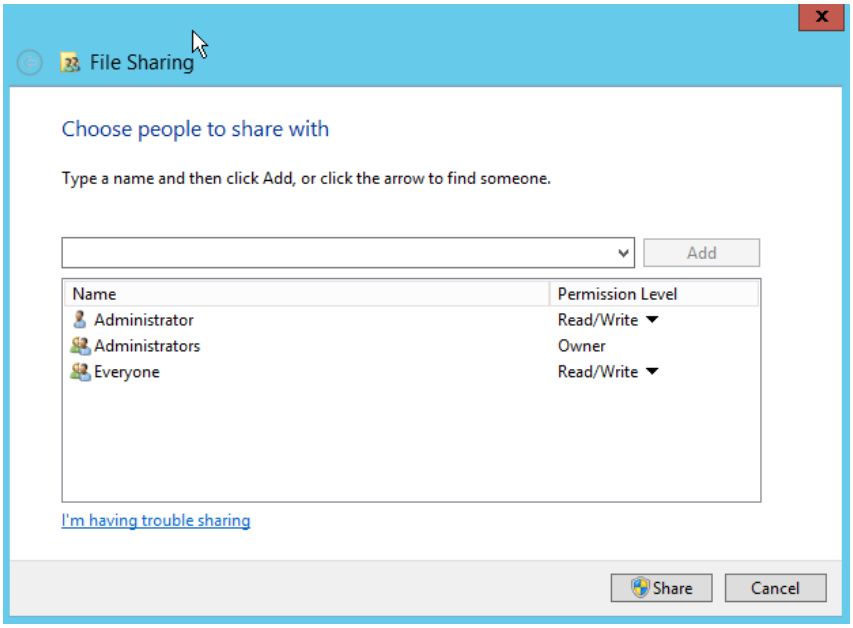
Gợi ý: Nếu muốn tạo tài khoản với password mình mong muốn thì phải bỏ chính sách password phức tạp:



Hình 4. Chỉnh sửa chính sách tại Administrative Tools → Local Security Policy

Tại mục *Password must meet complexity requirements*, thay đổi thành Disabled

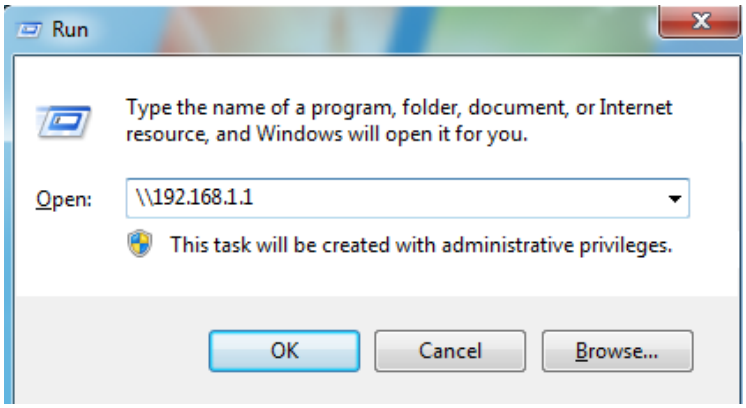
- **Bước 2:** Phân quyền chia sẻ trên thư mục **Data** để mọi người đều có quyền Read/Write.



Hình 5. Thay đổi quyền Read/Write cho Everyone

- **Bước 3:** Từ máy Client, kết nối vào máy chủ với tài khoản user đã tạo ở bước 2.

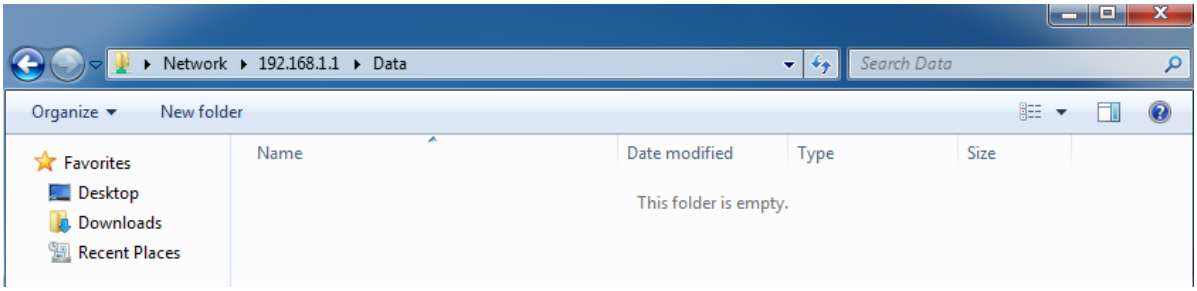
  Lưu ý: nên tạm thời tắt Firewall trước khi kết nối.



*Hình 6. Tại máy client vào Run gõ \\<**địa chỉ IP của server**>*

Hình 7. Nhập Username và Password của user đã tạo trên server

- **Bước 4:** Kiểm tra có thể kết nối và truy cập, thay đổi các tập tin trong thư mục Data trên máy chủ hay không



*Hình 8. Truy cập thành công thư mục **Data** trên máy chủ*

® Mở rộng:

- Tìm hiểu và thực hiện gỡ tài khoản đã lưu khi đã đăng nhập vào máy chủ.

2. Triển khai Active Directory và xây dựng mô hình Domain

> ® Trước khi bắt đầu thực hành, sinh viên hãy tìm hiểu và trả lời câu hỏi sau:
> - *Active Directory là gì?*

Cho mô hình gồm 3 máy tính như sau:

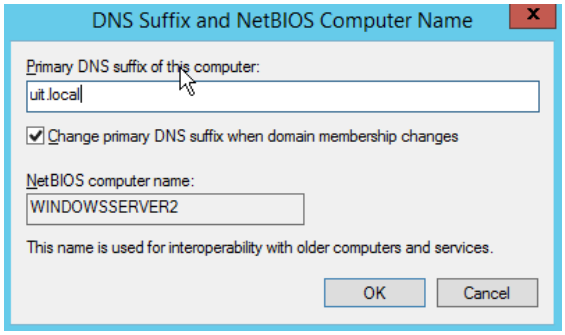
Hình 9. Mô hình Domain cần triển khai

Chuẩn bị 2 máy ảo sử dụng **Windows Server 2012** và 1 máy ảo sử dụng **Windows 7/8/10** *(hoặc có thể dung cả 3 máy ảo sử dụng Windows Server 2012).* Thiết lập IP cho các máy theo bảng dưới đây và tiến hành xây dựng mô hình Domain.

	IP Address	Subnet Mask	DNS
Client	192.168.1.3	255.255.255.0	192.168.1.2
File Server	192.168.1.1	255.255.255.0	192.168.1.2
Active Directory	192.168.1.2	255.255.255.0	192.168.1.2

Hình 10. Bảng thông tin IP

- **Bước 1:** Đặt Primary DNS Suffix thành **nhomX.local** *(với X là số thứ tự nhóm).* Trong hướng dẫn này đặt là **uit.local**



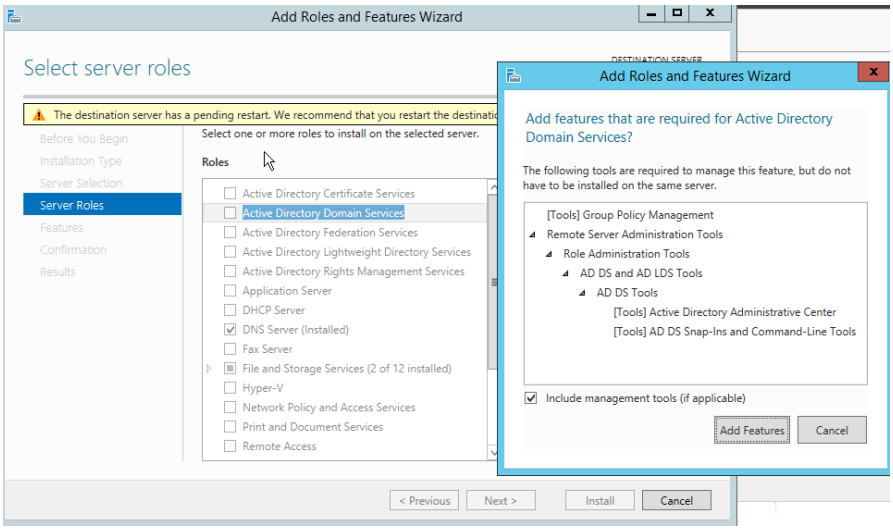
Hình 11. Thay đổi DNS Suffix trong System Properties

Sau khi thực hiện các bước trên, tiến hành restart lại máy chủ để áp dụng các cài đặt.

- **Bước 2:** Cài đặt dịch vụ Active Directory Domain Service
  - Vào Server Manager →Manage → Add Roles and Features

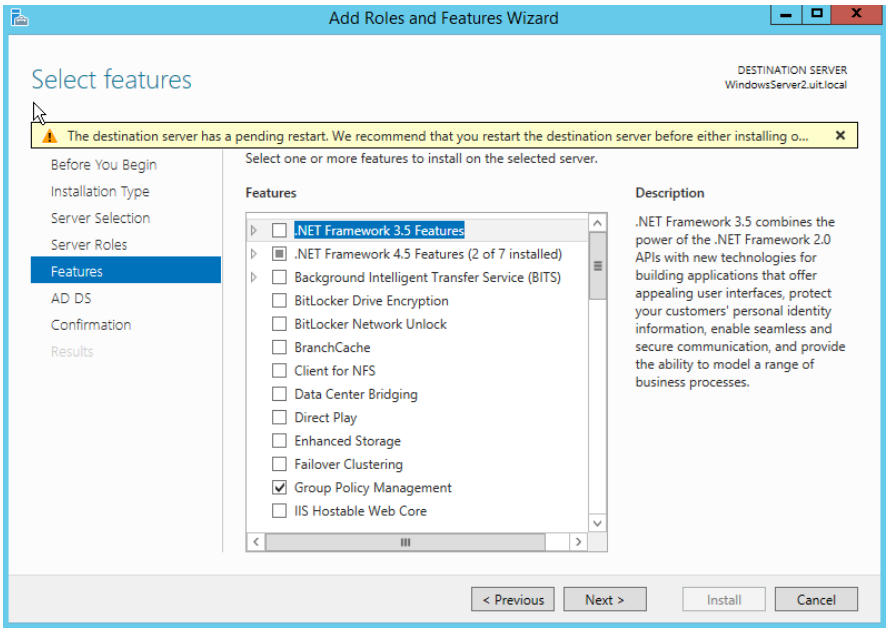
Hình 12. Chọn Add Roles and Features

  - Chọn Next tại các bước Before You Begin, Installation Type, Server Selection
  - Chọn **Active Directory Domain Services** tại bước Server Roles



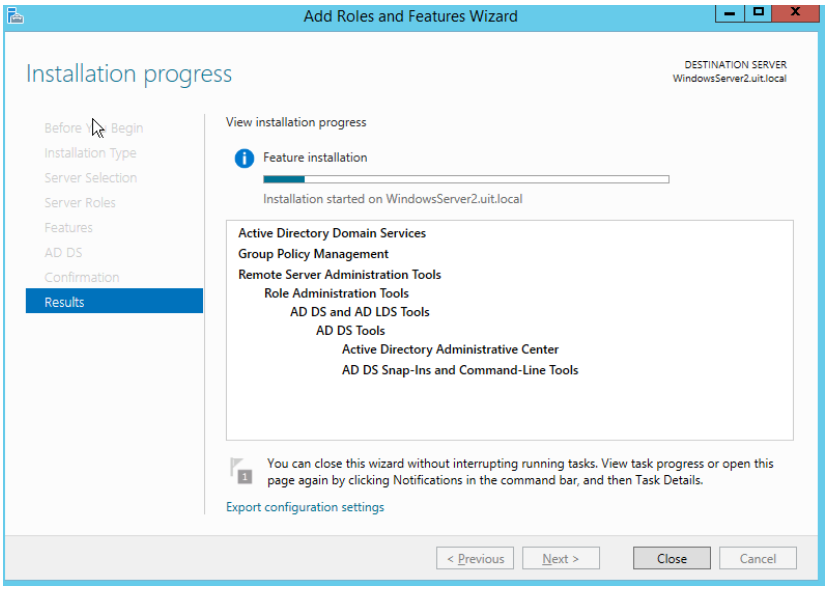
Hình 13. Chọn Active Directory Domain Services

  - Chọn **Group Policy Management** tại bước Features và Next ở bước AD DS.



Hình 14. Chọn Group Policy Management

- Xác nhận và chọn **Install** ở bước Confirmation
- Chờ quá trình cài đặt hoàn thành và chọn Close để kết thúc.

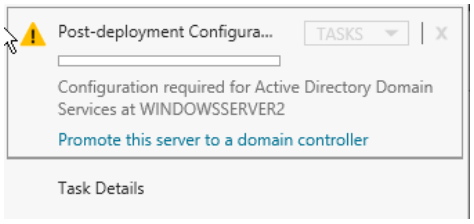


Hình 15. Chờ quá trình cài đặt hoàn tất

Sau khi cài đặt hoàn tất dịch vụ ActiveDirectory Domain Service, tiến hành nâng cấp lên Domain Controller.

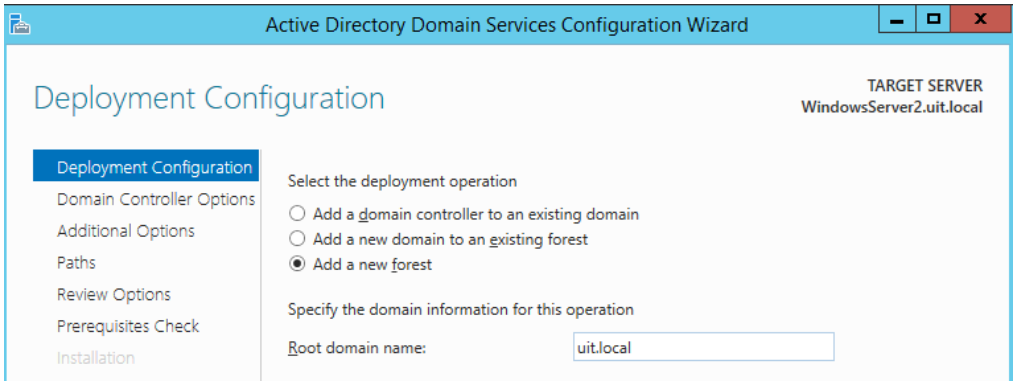
- **Bước 3:** Nâng cấp máy chủ Active Directory lên Domain Controller

- Vào **Server Manager** sẽ thấy biểu tượng cảnh báo, nhấn vào và chọn **Promote this server to a domain controller**

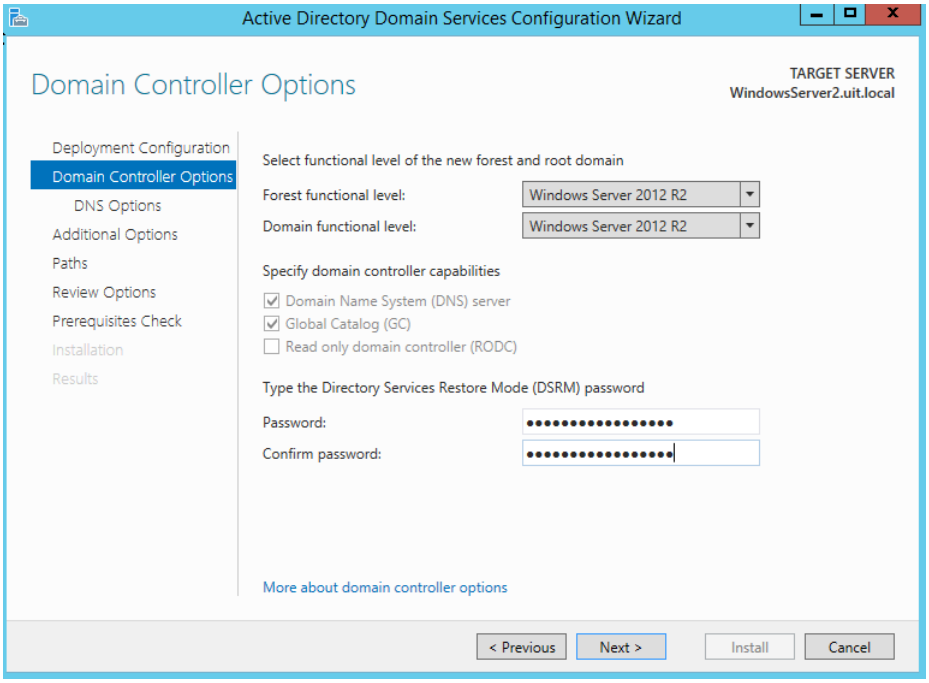


Hình 16. Chọn Promote this server to a domain controller

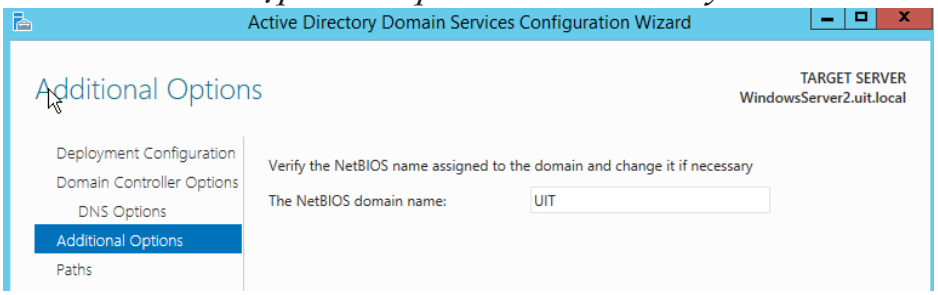
- Thực hiện quá trình nâng cấp như sau:



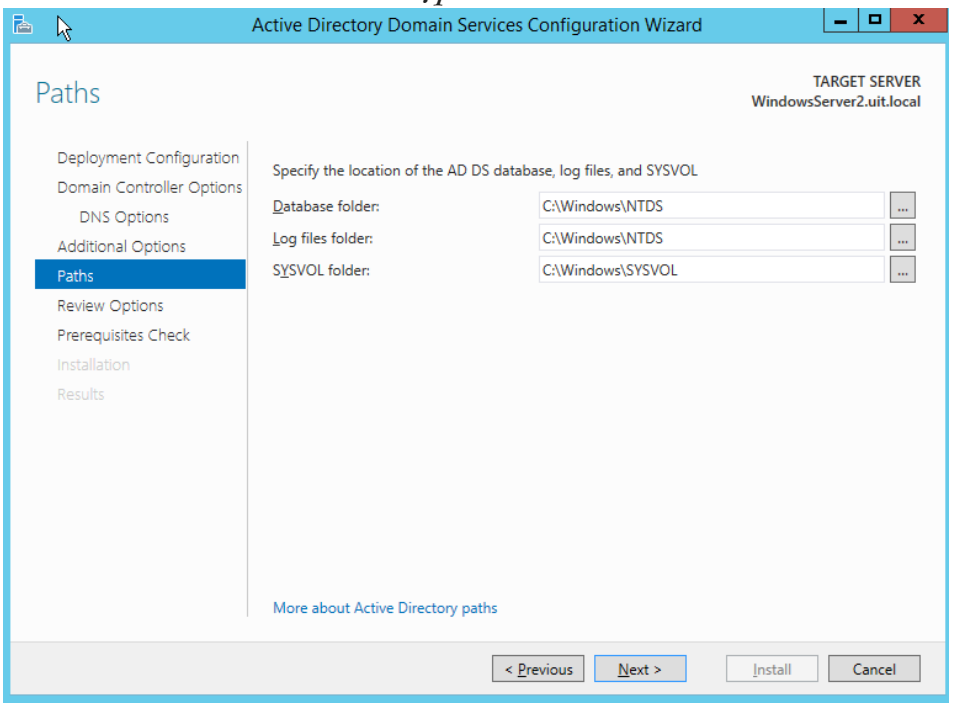
Hình 17. Chọn Add newforest và Root domain là tên domain



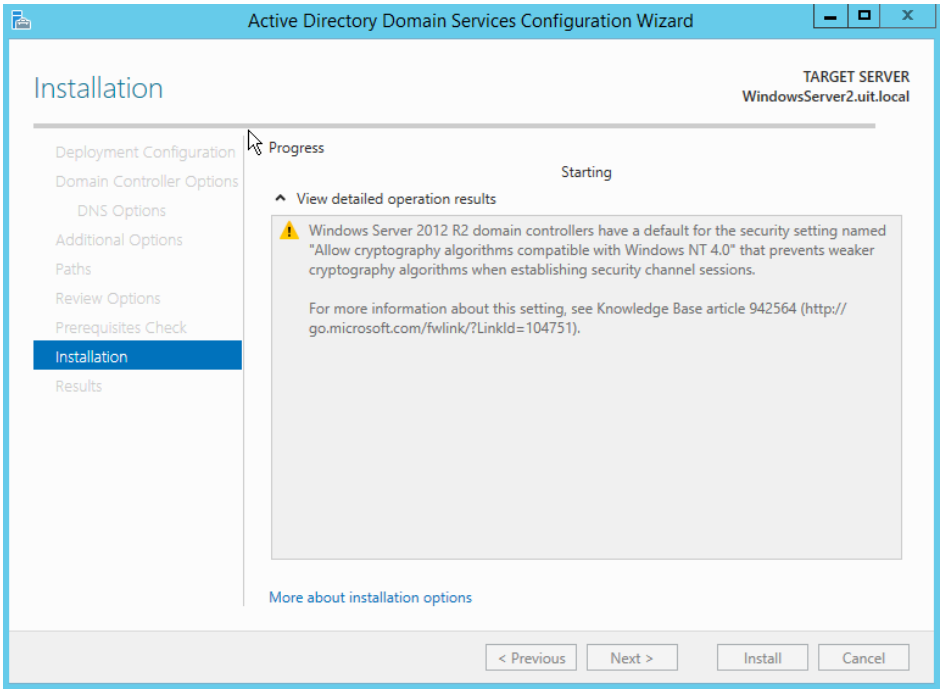
Hình 18. Thiết lập DSRM password và các tùy chỉnh như trên



Hình 19. Thiết lập NetBIOS domain name



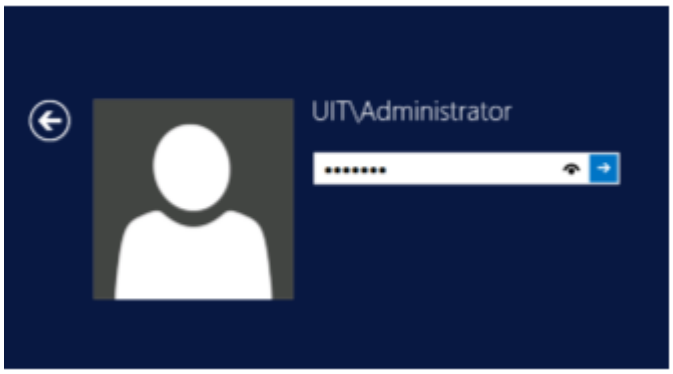
Hình 20. Giữ nguyên các tùy chỉnh mặc định



Hình 21. Chọn Install và chờ quá trình nâng cấp hoàn tất

Sau khi hoàn tất quá trình này, máy chủ sẽ khởi động lại và hoàn tất quá trình nâng cấp Domain Controller cho máy chủ Active Directory

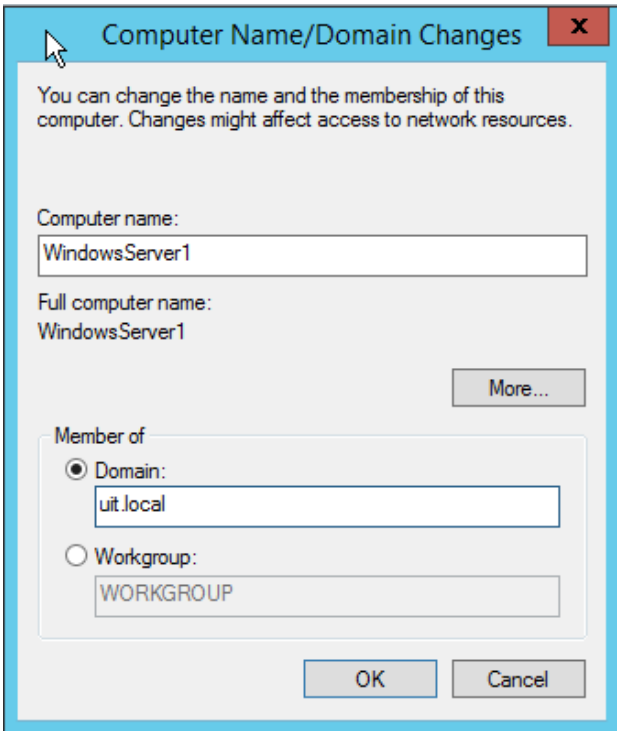
- **Bước 4:** Đăng nhập vào máy chủ Active Directory với tài khoản **Administrator**



Hình 22. Đăng nhập vào máy chủ Active Directory

- **Bước 5:** Tham gia máy chủ File (*File Server*) và Client vào Domain:

- Để tham gia một máy tính vào domain, chúng ta cần chú ý DNS của máy tính đó phải trỏ về DNS Server quản lý Domain. Trong trường hợp này, DNS được cài lên chính máy **Active Directory** nên DNS client của máy Client và File Server trỏ về 192.168.1.2.
- Tiếp tục vào *System Properties* → *Computer Name* → *Change*, tại trường Member of, chọn *Domain* và nhập tên domain.



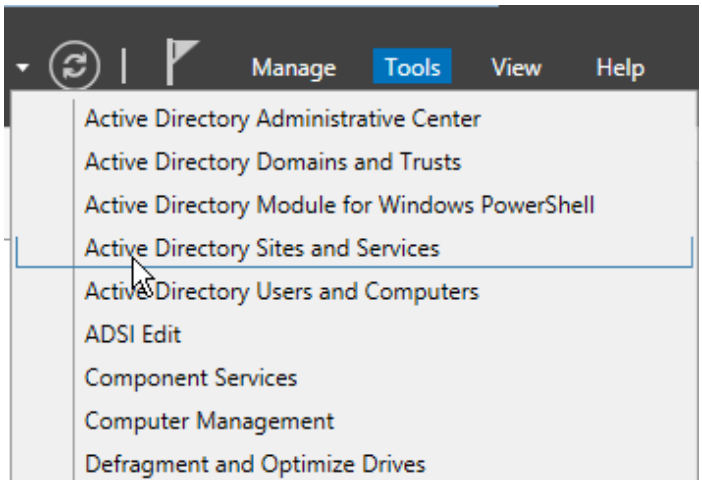
Hình 23. Nhập domain sẽ join vào

Sau khi quá trình này hoàn tất, tiến hành khởi động lại File Server.

Quá trình tham gia máy client vào domain thực hiện tương tự như quá trình tham gia máy chủ File vào domain.

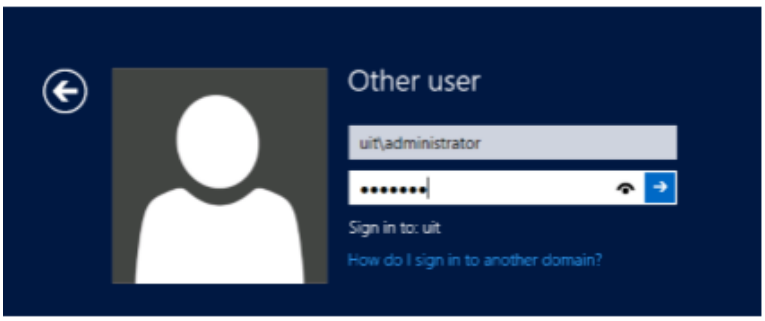
- **Bước 6:** Phân quyền và chia sẻ file từ File Server

- Tạo thư mục Data trên File Server.
- Sử dụng công cụ Active Directory User and Computer để tạo tài khoản u1/123 trên Active Directory. *Lưu ý chỉnh sửa Policy trước khi tạo tài khoản để tạo được password đơn giản*

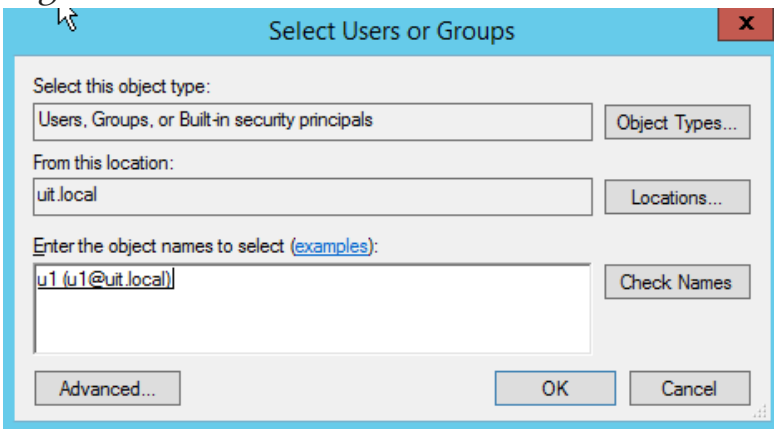


Hình 24. Active Directory User and Computer trong Active Directory

- **Bước 7:** Phân quyền thư mục Data cho User u1/123 (tài khoản này được lưu trữ trên Active Directory) quyền Read/Write.



Hình 25. Logon vào File Server với tài khoản Administrator trên domain.



Hình 26. Chọn Properties thư mục Data, chọn Share→ Find People và chọn user u1.

- **Bước 8:** Tại máy Client, logon với tài khoản uit\u1 (tài khoản này lưu trên máy chủ Active Directory).

Hình 27. Logon vào Client với tài khoản user: u1 trên domain

- **Bước 9:** Sau khi logon, truy cập vào File Server để lấy dữ liệu và kiểm tra các thao tác đọc, ghi dữ liệu tại thư mục này (giống với bài 1).

> ® **Câu hỏi:**
> - Đánh giá về việc cấp phát tài khoản và truy cập tài nguyên chia sẻ trong mạng theo mô hình Domain với Active Directory?
> - Tìm hiểu và so sánh sự khác nhau giữa mô hình Workgroup và mô hình Domain.

3. Xây dựng mô hình ADC cho dịch vụ Active Directory

> ® Trước khi thực hành, sinh viên hãy tìm hiểu và trả lời câu hỏi: Mô hình ADC hoạt động như thế nào?

Cho mô hình mạng cần triển khai như sau:

Hình 28. Mô hình ADC (HA) [1] cho dịch vụ Active Directory

Yêu cầu: Chuẩn bị 2 máy ảo sử dụng Windows Server 2012 và 1 máy ảo sử dụng Windows 7/8/10 *(hoặc có thể dùng cả 3 máy ảo sử dụng Windows Server 2012).* Thiết lập IP cho các máy theo bảng dưới đây và tiến hành xây dựng mô hình HA

	IP Address	Subnet Mask	Default Gateway	DNS
Client	192.168.1.3	255.255.255.0		192.168.1.2
Primary Active Directory	192.168.1.1	255.255.255.0		192.168.1.1 192.168.1.2
Additional Active Directory	192.168.1.2	255.255.255.0		192.168.1.2 192.168.1.1

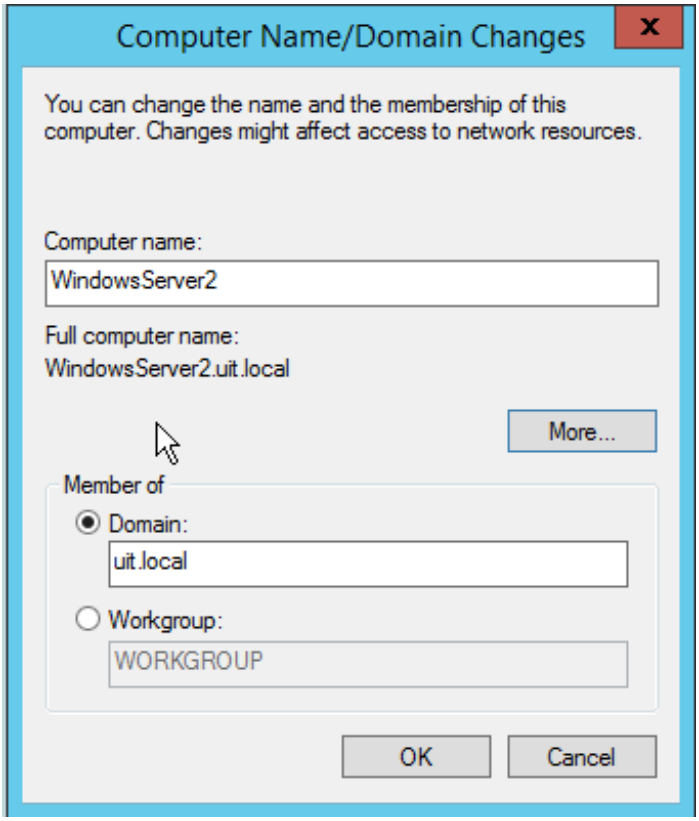
Đặt IP theo thông tin bảng thông tin IP và chỉnh DNS Suffix như ở bài 2

- **Bước 1:** Nâng cấp máy chủ Windows Server1 lên **Primary controller**

  Xem lại quá trình nâng cấp máy chủ 1 lên Domain Controller ở bài 2

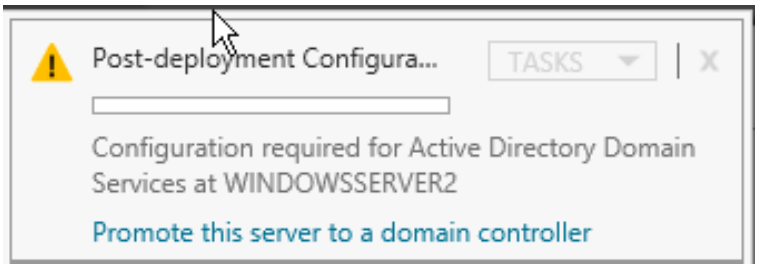
- **Bước 2:** Tham gia máy chủ 2 vào Domain và nâng cấp máy chủ Windows Server2 lên **Additional Domain Controller**

- Tham gia máy chủ 2 vào Domain

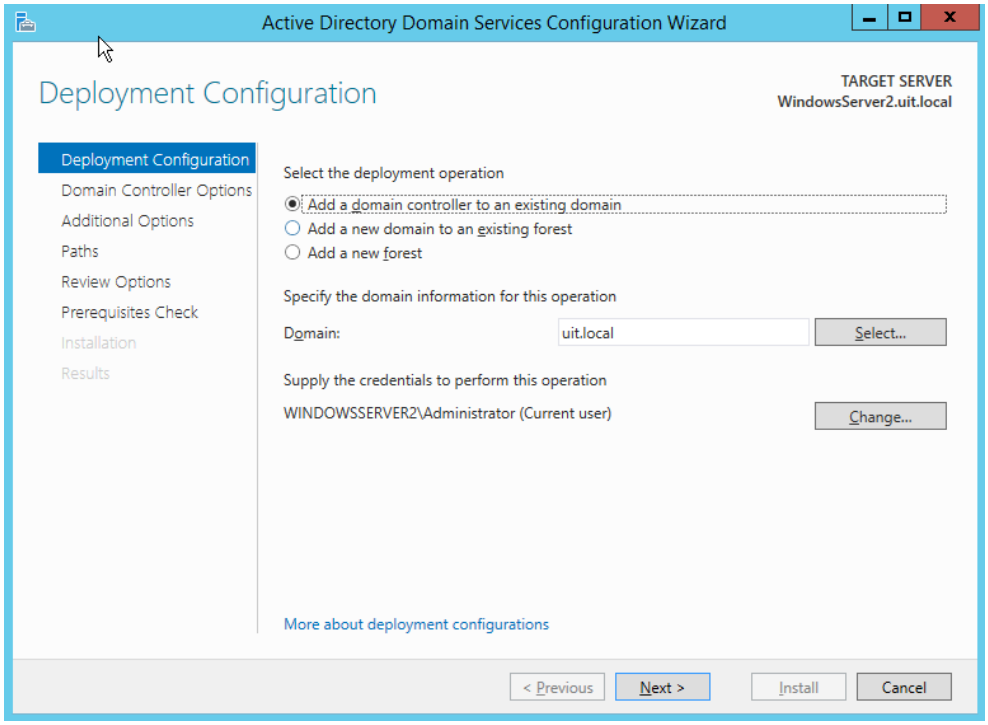


Hình 29. Nhập domain sẽ join vào

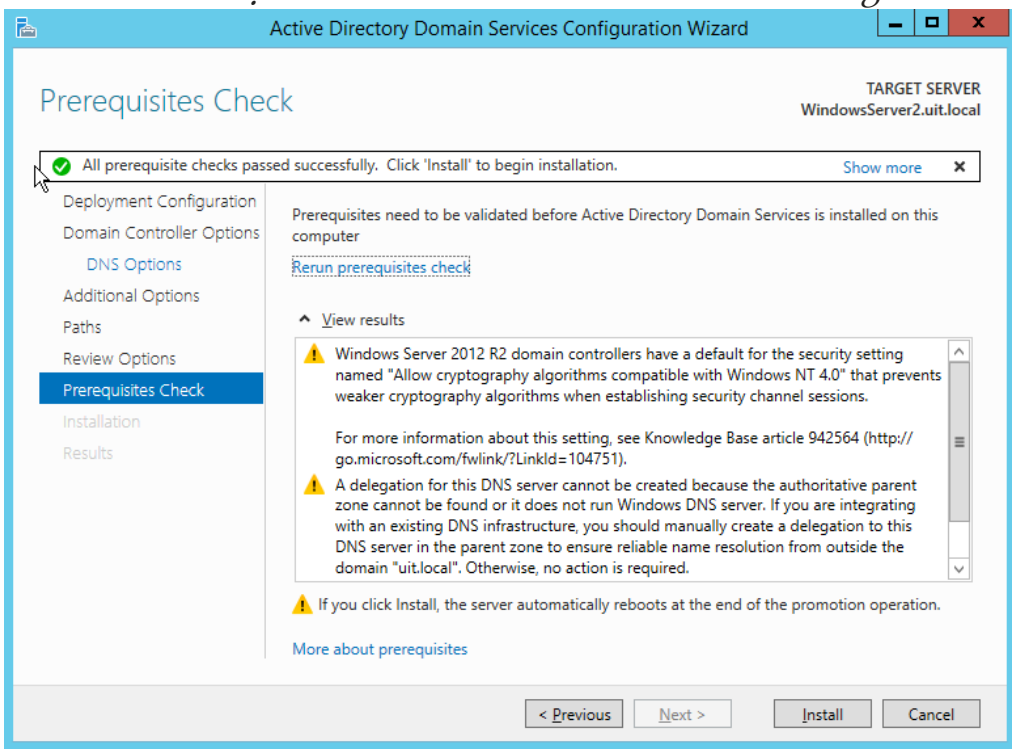
- Cài đặt dịch vụ Active Directory Domain Service như ở phần 2.
- Nâng cấp lên Additional Domain Controller



Hình 30. Chọn Promote this server to a domain controller



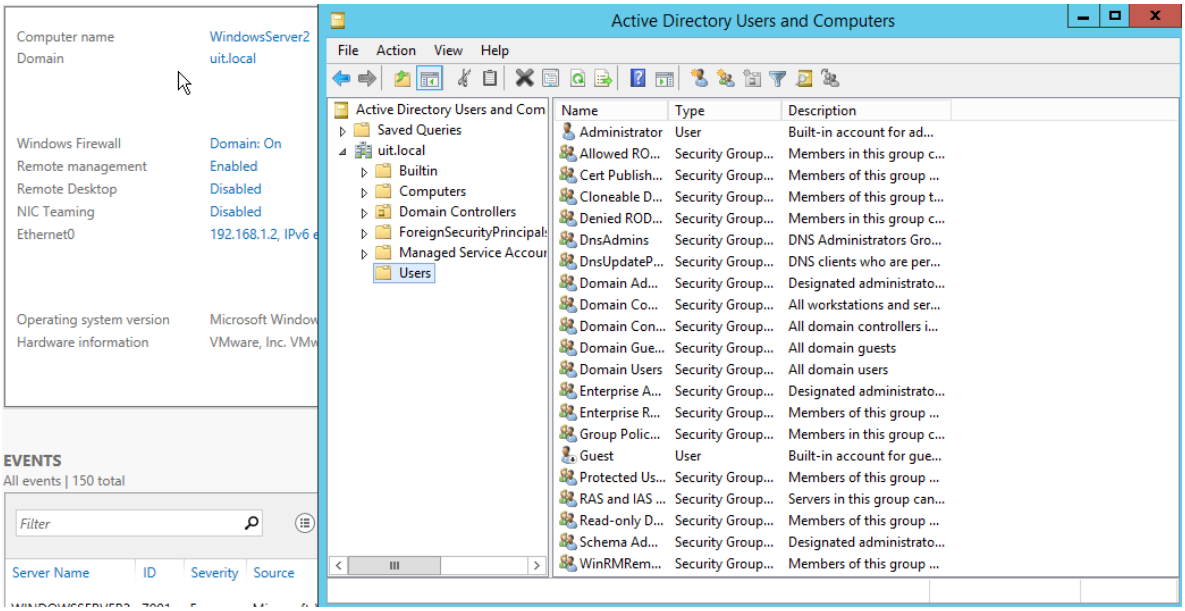
Hình 31. Chọn Add a domain controller to an existing domain



Hình 32. Tiến hành Install Domain Controller

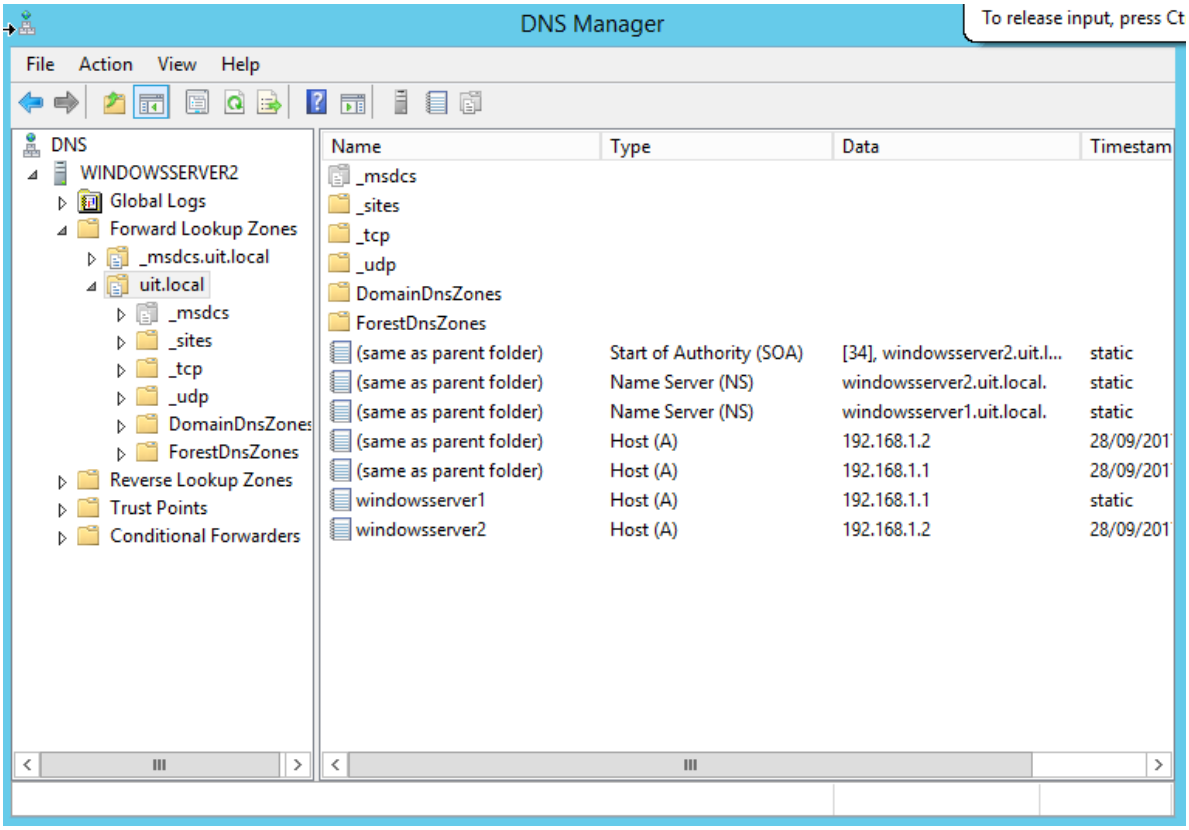
- **Bước 3:** Kiểm tra việc đồng bộ dữ liệu của 2 Domain controller

- Trên máy **Additional Domain Controller**, mở công cụ **Active User and Computer** và thấy dữ liệu được đồng bộ từ Primary Domain Controller qua.



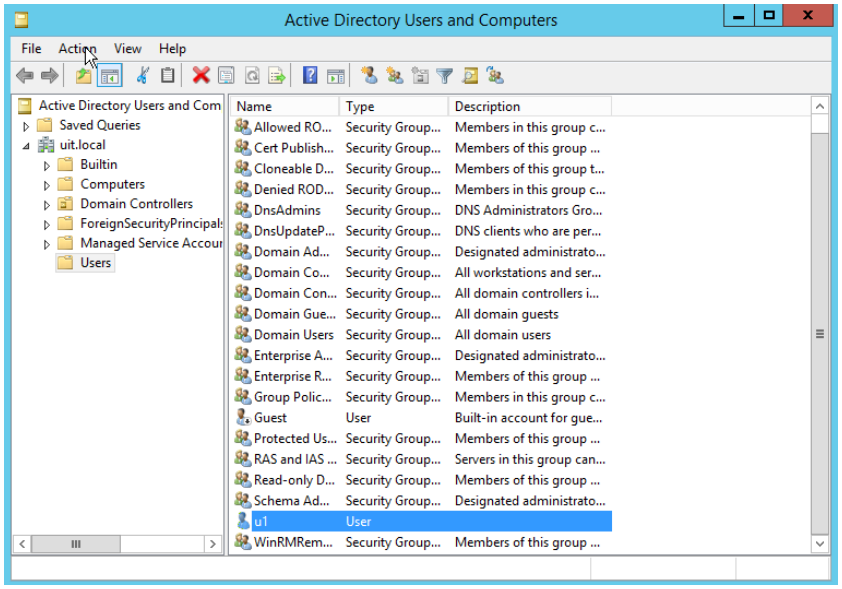
Hình 33. Vào Tools → Active Directory Users and Computers

- Trên máy **Additional Domain Controller**, chúng tả mở công cụ **DNS Manager** và thấy dữ liệu được đồng bộ từ **Primary Domain Controller** qua.



Hình 34. Vào Tools → DNS

- Tạo 1 user trên **Primary Domain Controller** và kiểm tra thấy tự đồng bộ qua **Additional Domain Controller.**



Hình 35. User u1 được đồng bộ tự động qua Addition Domain Controller

- Tạo 1 user trên **Additional Domain Controller** và kiểm tra thấy tự đồng bộ qua Primary Domain Controller

• **Bước 4:** Tham gia Client vào Domain *(Cách làm tương tự ở bài 2)*

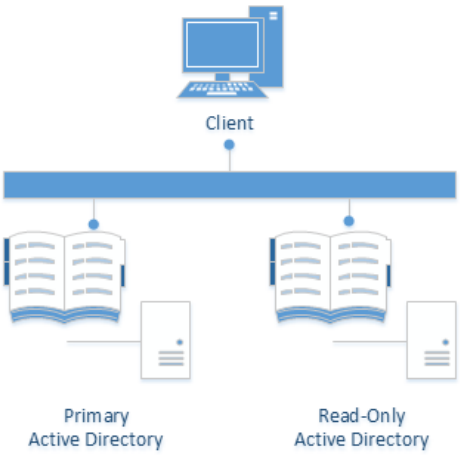
• **Bước 5:** Kiểm tra

- Login u1 vào được tại máy Client
- Tắt máy Primary Domain Controller sau đó login với user u1.
- Thực hiện chỉnh sửa thông tin u1 trên máy Aditional Domain Controller.

Kiểm tra kết quả và rút ra nhận xét.

C. MỞ RỘNG

1. Tìm hiểu và xây dựng mô hình **RODC** cho dịch vụ Active Directory như sau:



Hình 36. Mô hình RODC

Thông tin về địa chỉ IP các máy tính

	IP Address	Subnet Mask	Default Gateway	DNS
Client	192.168.1.3	255.255.255.0		192.168.1.2
Primary Active Directory	192.168.1.1	255.255.255.0		192.168.1.1 192.168.1.2
Additional Active Directory	192.168.1.2	255.255.255.0		192.168.1.2 192.168.1.1

® Sau khi thực hành phần mở rộng, hãy so sánh sự khác nhau giữa mô hình ADC và mô hình RODC.

2. Triển khai bài thực hành trên nền tảng **Windows Server 2016**.

D. YÊU CẦU & ĐÁNH GIÁ

1. Yêu cầu

- Sinh viên tìm hiểu và thực hành theo hướng dẫn. Có thể thực hiện theo nhóm (2 sinh viên/nhóm) hoặc thực hiện cá nhân. Đăng ký nhóm cố định từ buổi 1.
- Sinh viên báo cáo kết quả thực hiện và nộp bài:

Báo cáo chi tiết:

Báo cáo cụ thể quá trình thực hành (có ảnh minh họa các bước) và giải thích các vấn đề kèm theo. Trình bày trong file Word (.docx) hoặc PDF theo mẫu có sẵn tại website môn học.

Lưu ý chung: Giữ nguyên trạng thái thành công của bài thực hành để đánh giá kết quả trực tiếp tại lớp.

Đặt tên file báo cáo theo định dạng như mẫu:

[Mã lớp]-LabX_MSSV1-Tên SV1_MSSV2 –Tên SV2

Ví dụ*: [NT101.I11.1]-Lab1_14520000-Viet_14520999-Nam.*

- Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
- Nộp báo cáo trên theo thời gian đã thống nhất tại website môn học.

2. Đánh giá:

- Sinh viên hiểu và tự thực hiện được bài thực hành, đóng góp tích cực tại lớp.
- Báo cáo trình bày chi tiết, giải thích các bước thực hiện và chứng minh được do nhóm sinh viên thực hiện.

- Hoàn tất nội dung cơ bản và có thực hiện nội dung mở rộng (với lớp ANTN).

Kết quả thực hành cũng được đánh giá bằng kiểm tra kết quả trực tiếp tại lớp vào cuối buổi thực hành hoặc vào buổi thực hành thứ 2.

Lưu ý: Bài sao chép, nộp trễ, "*gánh team*", … sẽ được xử lý tùy mức độ.

E. TÀI LIỆU THAM KHẢO

[1] *Step-By-Step: Setting up Active Directory in Windows Server 2016* [Online]. Available: https://blogs.technet.microsoft.com/canitpro/2017/02/22/step-by-step-setting-up-active-directory-in-windows-server-2016/

[2] Tài liệu thực hành *Quản trị hệ thống mạng*, ThS. Nguyễn Duy, UIT, năm 2013.

HẾT

Chúc các bạn hoàn thành tốt!