

MỤC LỤC

| | |
|---|-----------|
| CHƯƠNG 1. TỔNG QUAN | 1 |
| 1.1 Định nghĩa về Domain Controller | 1 |
| 1.1.1 Định nghĩa | 1 |
| 1.1.2 Chức năng chính | 1 |
| 1.2 Hệ điều hành Linux | 2 |
| 1.2.1 Định nghĩa | 2 |
| 1.2.2 Đặc điểm của Linux | 3 |
| 1.2.3 Lợi ích của Linux trong triển khai Domain Controller | 3 |
| CHƯƠNG 2. VAI TRÒ VÀ HOẠT ĐỘNG DOMAIN CONTROLLER | 5 |
| 2.1 Phân Loại Domain Controller | 5 |
| 2.1.1 Primary Domain Controller | 5 |
| 2.1.2 Backup Domain Controller (BDC) | 5 |
| 2.1.3 Additional Domain Controller (ADC) | 6 |
| 2.2 Nguyên lý hoạt động của Domain Controller trong một mạng | 7 |
| 2.3 Vai trò của Domain Controller trong một mạng | 8 |
| 2.4 Lợi ích và ứng dụng sự dụng Domain Controller | 9 |
| 2.5 Tầm quan trọng của việc triển khai Domain Controller trong tổ chức doanh nghiệp | 10 |
| CHƯƠNG 3. TRIỂN KHAI | 11 |
| 3.1 Điều kiện chuẩn bị | 11 |
| 3.2 Thiết lập máy chủ | 11 |
| 3.2 Vô hiệu hóa dịch vụ phân giải DNS | 12 |
| 3.3 Cài đặt Samba | 13 |
| 3.4 Cấu hình Samba Active Directory | 15 |
| 3.5 Thiết lập đồng bộ hóa thời gian | 16 |
| 3.6 Xác minh Samba Active Directory | 17 |
| 3.7 Tạo người dùng Samba Active Directory mới | 19 |
| 3.8 Tham gia và đăng nhập vào miền Samba Active Directory | 19 |
| CHƯƠNG 4: QUẢN LÝ DOMAIN CONTROLLER | 23 |
| 4.1 Cài đặt công cụ quản trị máy chủ từ xa (RSAT) | 23 |
| 4.2 quản lý người dùng trong miền | 25 |
| 4.2.1 Mô tả tình huống, vấn đề thách thức | 25 |
| 4.2.2 Thư mục trang chủ người dùng | 26 |
| 4.3 Tạo shared folders | 38 |
| 4.4 Chuyển hướng thư mục (Folder Redirection) | 42 |
| 4.5 Policy mật khẩu mạnh | 49 |
| 4.6 Tạo Home folders | 51 |
| KẾT LUẬN | 54 |
| TÀI LIỆU THAM KHẢO | 55 |

CHƯƠNG 1. TỔNG QUAN

1.1 Định nghĩa về Domain Controller

1.1.1 Định nghĩa

Domain Controller (DC) là một hệ thống máy chủ được thiết lập nhằm mục đích quản lý, kiểm tra domain. Trong đó, 1 domain controller là 1 hệ thống chịu trách nhiệm quản lý các vấn đề an ninh trên mạng. Domain Controller hoạt động giống như một người gác cổng với vai trò xác thực cũng như ủy quyền user.

1.1.2 Chức năng chính

Global Catalog Servers:

Global Catalog Server (GCS) có vai trò quan trọng trong hệ thống quản lý domain và là điểm tập trung của toàn bộ forest. Khi một Domain Controller được cấu hình làm Global Catalog Server, nó trở thành một nguồn thông tin tổng hợp, lưu trữ thông tin về tất cả các domain có trong forest.

Vai trò quan trọng của Global Catalog Server nằm ở khả năng chia sẻ thông tin từ nhiều domain, tăng tốc độ và hiệu quả trong quá trình truy xuất dữ liệu. Điều này giúp người dùng dễ dàng truy cập vào các tài nguyên mà họ cần một cách thuận tiện, đồng thời giảm áp lực đối với các Domain Controller khác trong hệ thống.

Ngoài ra, Global Catalog Server cũng cho phép các Domain Controller khác trong hệ thống lưu trữ dữ liệu cho một thư mục hoặc một domain cụ thể trong forest. Điều này tạo ra sự linh hoạt trong việc quản lý tài nguyên, giúp tối ưu hóa hiệu suất hệ thống.

Một điểm đặc biệt của GCS là khả năng lưu trữ các đối tượng không thuộc domain hiện tại. Những đối tượng này được lưu trữ trong một phần của bản sao lưu Domain, giúp đồng bộ hóa và chia sẻ thông tin linh hoạt giữa các domain trong forest.

Quá trình triển khai Global Catalog Server không chỉ là việc tạo ra một nguồn thông tin đa domain, mà còn là một bước quan trọng trong việc xây dựng một hệ thống mạng linh hoạt và hiệu suất cao. Sự tích hợp thông tin tại Global Catalog Server giúp tối ưu hóa quản lý, giảm độ trễ và đảm bảo rằng mọi người dùng có thể truy cập vào tài nguyên của họ một cách mượt mà và hiệu quả.

Operations Masters

Operation Master, hay còn được biết đến với tên gọi Flexible Single Master Operations (FSMO), giúp đảm bảo tính thống nhất và ngăn chặn xung đột giữa các entry trong cơ sở dữ liệu của một hệ thống mạng.

Operation Master có năm vai trò chính, mỗi vai trò đều đóng góp vào sự linh hoạt và ổn định của hệ thống:

- Trước hết là vai trò quản lý các thay đổi trong sơ đồ tổng thể, đảm bảo tính nhất quán và hiệu suất của hệ thống.
- Vai trò thứ hai là cơ sở hạ tầng, chịu trách nhiệm duy trì thông tin về cơ sở hạ tầng của domain, bao gồm các site và subnet.
- Primary Domain Controller (PDC) đóng vai trò thứ ba, đảm bảo rằng mọi thay đổi liên quan đến người dùng và mật khẩu được thực hiện một cách đồng bộ và hiệu quả.
- Vai trò thứ tư, tên miền Master, quản lý quá trình thay đổi tên miền và đảm bảo chúng được thực hiện một cách an toàn và đồng bộ.
- Cuối cùng, vai trò RID (Relative ID) chịu trách nhiệm tạo ra các số ID tương đối cho các đối tượng mới trong domain, giúp ngăn chặn xung đột giữa các đối tượng.

Operation Master không chỉ là một cột mốc trong việc quản lý hệ thống mạng mà còn đóng vai trò trong việc bảo vệ tính toàn vẹn của dữ liệu. Với khả năng đồng bộ và kiểm soát thông tin, nó giúp đảm bảo rằng mọi thay đổi đều được thực hiện một cách an toàn và chính xác, ngăn chặn sự xung đột và mất mát dữ liệu không mong muốn.

1.2 Hệ điều hành Linux

1.2.1 Định nghĩa

Linux là hệ điều hành mã nguồn mở và hoàn toàn miễn phí, được phát triển từ Unix vào năm 1991 và viết dựa trên ngôn ngữ C. Hiện nay, Linux hỗ trợ trên nhiều thiết bị khác nhau, bao gồm máy tính xách tay, máy tính để bàn PC hoặc các thiết bị nhúng, máy chủ (Server).

1.2.2 Đặc điểm của Linux

Linux là một hệ điều hành miễn phí và mã nguồn mở: mã nguồn mở cung cấp quyền tự do chạy chương trình, tự do phân phối lại các bản sao, tự do thay đổi mã để phù hợp với nhu cầu và tự do phân phối các bản sao đã được sửa đổi. Hơn nữa, không phải trả tiền cho nó.

Tính ổn định: Linux có tính ổn định cao, ít bị lỗi khi sử dụng so với các HĐH khác. Linux có thể chạy nhiều năm, không cần reboot.

Bảo mật cao: Linux cung cấp một số tùy chọn bảo mật để giúp người dùng an toàn khỏi vi-rút, phần mềm độc hại, hạn chế làm chậm và treo máy. Mỗi người dùng chỉ làm việc trên một không gian dành riêng. Nó không hoàn toàn an toàn, nhưng nó ít nguy hiểm hơn các hệ điều hành khác

Đa người dùng, đa chương trình và đa xử lý: Linux tương thích với nhiều hệ điều hành: Linux có khả năng tương thích rộng rãi với nhiều hệ điều hành khác nhau, bao gồm Windows, macOS, và các distro Linux khác nhau như Ubuntu, Fedora, và Debian. Linux hỗ trợ nhiều giao thức mạng, bắt nguồn và phát triển từ dòng BSD. Thêm vào đó, Linux còn hỗ trợ nhiều hệ thống tập tin, hỗ trợ việc tính toán thời gian thực

1.2.3 Lợi ích của Linux trong triển khai Domain Controller

Miễn phí và mã nguồn mở: Linux là một phần mềm mã nguồn mở, điều này có nghĩa là không có chi phí phát sinh cho việc sử dụng, cũng như không có chi phí cho việc mua bản quyền hay trả tiền cho các tính năng bổ sung. Điều này giúp giảm bớt gánh nặng tài chính cho tổ chức.

Linh hoạt: Linux hỗ trợ nhiều nền tảng phần cứng và môi trường hệ thống khác nhau. Điều này cho phép triển khai Domain Controller trên các loại máy chủ khác nhau, từ máy chủ vật lý đến máy chủ ảo hoặc điện toán đám mây.

Tính bảo mật cao: Linux nổi tiếng với tính bảo mật cao, điều này làm cho nó trở thành một lựa chọn an toàn cho việc lưu trữ và quản lý dữ liệu nhạy cảm trên Domain Controller. Cộng đồng mã nguồn mở liên tục kiểm tra và vá lỗi, giúp tăng cường tính bảo mật của hệ thống.

Hiệu suất và ổn định: Linux thường có hiệu suất cao và ổn định, giúp Domain Controller hoạt động một cách mượt mà và đáng tin cậy. Hệ điều hành này thường ít tài nguyên hơn so với các hệ điều hành thương mại, đồng thời cũng giảm thiểu các vấn đề về trì hoãn và gián đoạn.

Hỗ trợ cộng đồng lớn: Linux có một cộng đồng người dùng và nhà phát triển rộng lớn, đảm bảo rằng bạn có thể tìm thấy hỗ trợ và giải pháp cho các vấn đề một cách nhanh chóng và hiệu quả. Bạn có thể tìm thấy thông tin hữu ích, tài liệu và cộng đồng trực tuyến sẵn lòng giúp đỡ qua các diễn đàn và trang web chuyên ngành.

CHƯƠNG 2. VAI TRÒ VÀ HOẠT ĐỘNG DOMAIN CONTROLLER

2.1 Phân Loại Domain Controller

2.1.1 Primary Domain Controller

Trong hệ thống quản lý domain, Primary Domain Controller (PDC) đóng vai trò quan trọng, đảm bảo sự an toàn và bảo mật của mọi tài nguyên và dữ liệu trong domain đó. Loại PDC này không chỉ là một phần của hệ thống quản lý mạng, mà còn là trái tim của mọi hoạt động liên quan đến domain.

PDC là nơi tổ chức thông tin một cách cẩn thận và có tổ chức. Mỗi tài nguyên, hình ảnh, và dữ liệu quan trọng đều được đặt trong cơ sở dữ liệu tại các thư mục chính, đặc biệt là trên các máy chủ Windows Server. Điều này giúp đảm bảo thông tin quan trọng không chỉ được lưu trữ một cách an toàn mà còn dễ dàng truy cập và quản lý.

Trong môi trường doanh nghiệp, PDC trở thành một trụ cột không thể thiếu, là nguồn đáng tin cậy cho việc duy trì tính toàn vẹn của dữ liệu và thông tin quan trọng. Khả năng tự động đồng bộ và sao lưu giữa các PDC giúp đảm bảo rằng mọi thay đổi được thực hiện một cách đồng nhất trong toàn bộ hệ thống mạng.

Mặc dù có sự xuất hiện của các hệ thống quản lý cloud và giải pháp thay thế, nhưng PDC vẫn giữ vững vai trò của mình trong việc duy trì sự ổn định và hiệu suất cao cho các hệ thống mạng truyền thống. Sự chuyên nghiệp và tính linh hoạt của PDC làm cho nó trở thành một lựa chọn lý tưởng cho những tổ chức và doanh nghiệp đòi hỏi mức độ an ninh và quản lý cao nhất cho dữ liệu của mình.

2.1.2 Backup Domain Controller (BDC)

Backup Domain Controller (BDC) là một phần quan trọng trong hệ thống quản lý domain, đặc biệt khi Primary Domain Controller (PDC) gặp sự cố hay bị lỗi. Trong tình huống này, BCD đóng vai trò như một giải pháp linh hoạt, đảm bảo rằng hoạt động của domain vẫn diễn ra mượt mà và an toàn.

Khi PDC gặp sự cố không thể khắc phục, BCD nhanh chóng đảm nhận vai trò của PDC, tiếp tục quản lý khối lượng công việc và đồng thời tự động sao chép cơ sở dữ liệu trong mỗi chu kỳ hoạt động của nó. Điều này giúp đảm bảo rằng dữ liệu quan trọng, tài nguyên và thông tin trong domain được bảo toàn một cách toàn diện.

Quá trình sao chép cơ sở dữ liệu của BCD không chỉ mang lại sự an toàn mà còn giúp giảm thiểu rủi ro mất mát thông tin bên trong các thư mục chính. Điều này làm cho hệ thống trở nên linh hoạt hơn và có khả năng khôi phục nhanh chóng sau khi gặp sự cố. Khả năng tự động chuyển giao giữa PDC và BCD tạo ra một môi trường mạng ổn định và đáng tin cậy.

Trong bối cảnh ngày nay, tính liên tục của hoạt động kinh doanh đòi hỏi sự đảm bảo và khả năng khôi phục nhanh chóng, BCD trở thành một yếu tố không thể thiếu trong kiến trúc mạng của nhiều tổ chức. Khả năng của BCD trong việc duy trì sự ổn định của domain và giảm thiểu tác động tiêu cực khi PDC gặp sự cố đã làm cho nó trở thành một công cụ quan trọng đối với các nhà quản trị hệ thống và IT.

2.1.3 Additional Domain Controller (ADC).

Additional Domain Controller trong bối cảnh giải pháp quản lý website của doanh nghiệp. Additional Domain Controller, hay ADC, là một phần mềm hoặc thiết bị được triển khai bổ sung vào mạng hệ thống để cung cấp tính khả dụng và độ tin cậy cao hơn cho dịch vụ website.

ADC thường được sử dụng để tăng cường khả năng chịu tải (load balancing) và cung cấp khả năng dự phòng (failover) cho các dịch vụ trên website, như cơ sở dữ liệu, ứng dụng web, và các dịch vụ mạng khác. Bằng cách triển khai ADC, doanh nghiệp có thể tăng cường hiệu suất của hệ thống, đồng thời đảm bảo rằng website của họ hoạt động ổn định và không bị gián đoạn.

2.2 Nguyên lý hoạt động của Domain Controller trong một mạng

Domain Controller có thể được xem như một người gác cổng đáng tin cậy, hoạt động như bản đồ hướng dẫn cho mọi yêu cầu của người dùng trong hệ thống mạng. Đóng vai trò quản lý thông tin và quyền truy cập, nó giữ chìa khóa cho việc xác thực danh tính và ủy quyền đăng nhập.

Quá trình hoạt động của Domain Controller bắt đầu khi người dùng đưa ra yêu cầu truy cập vào một tài nguyên nào đó trên website. Thay vì trực tiếp truy cập vào tài nguyên đó, yêu cầu của người dùng sẽ được đưa đến Domain Controller. Đây là nơi quyết định xem người dùng có quyền truy cập hay không, dựa trên thông tin xác thực được cung cấp.

Quá trình xác thực thường sử dụng thông tin đăng nhập của người dùng, bao gồm tên người dùng và mật khẩu. Domain Controller kiểm tra thông tin này trong cơ sở dữ liệu người dùng của mình để đảm bảo tính chính xác và an toàn. Nếu thông tin xác thực chính xác, Domain Controller sẽ tiếp tục ủy quyền cho người dùng, mở cánh cổng để họ truy cập vào tài nguyên mà họ yêu cầu.

Quan trọng nhất, Domain Controller không chỉ giữ vai trò trong việc xác thực người dùng, mà còn đảm nhận trách nhiệm về việc quản lý quyền truy cập. Nó xác định được những tài nguyên nào mà người dùng cụ thể có thể truy cập và những hành động mà họ được phép thực hiện. Điều này tạo ra một môi trường an toàn và có tổ chức, nơi mà quản lý tài nguyên và bảo mật dữ liệu trở nên hiệu quả.

Sau khi xác thực và ủy quyền hoàn tất, người dùng có thể tự tin sử dụng tài nguyên trên website mà không lo lắng về việc bị truy cứu lỗi xác thực. Domain Controller không chỉ đơn thuần là một cổng truy cập, mà là một người quản lý thông tin và quyền truy cập, làm cho trải nghiệm của người dùng trở nên thuận tiện và an toàn hơn.

2.3 Vai trò của Domain Controller trong một mạng

Quản lý Chứng thực: Domain Controller kiểm soát việc xác thực người dùng khi họ cố gắng truy cập vào các tài nguyên trên mạng. Khi người dùng đăng nhập vào hệ thống, thông tin đăng nhập của họ được gửi đến Domain Controller để xác thực.

Quản lý Tài nguyên: Domain Controller là nơi chứa thông tin về các tài nguyên như máy tính, người dùng, nhóm người dùng, ứng dụng, và các đối tượng khác trong domain. Nó quản lý quyền truy cập và phân quyền cho các tài nguyên này.

Đồng bộ hóa dữ liệu: Domain Controller đảm bảo dữ liệu trên mạng domain được đồng bộ hóa và cập nhật. Điều này bao gồm việc đồng bộ hóa thông tin người dùng, nhóm và các thiết bị trong mạng.

Quản lý Chính sách: Domain Controller cho phép quản trị viên thiết lập và triển khai các chính sách an ninh, cấu hình và hạn chế truy cập trên toàn bộ mạng domain.

Quản lý Đăng ký: Domain Controller giữ một bản ghi của tất cả các đối tượng trong domain, bao gồm người dùng, máy tính, nhóm và ứng dụng. Nó giữ quản lý cơ sở dữ liệu đăng ký và xử lý các yêu cầu truy cập từ các máy tính và người dùng trên mạng.

Dịch vụ Cấp phát IP: Trong một môi trường Active Directory, Domain Controller thường cũng hoạt động như một máy chủ DHCP để cấp phát địa chỉ IP cho các thiết bị trong mạng.

Điều khiển Cập nhật: Domain Controller thường cũng chịu trách nhiệm cho việc triển khai cập nhật và vá lỗi trên các máy tính và thiết bị trong mạng domain.

2.4 Lợi ích và ứng dụng sự dụng Domain Controller

Quản lý tập trung: Domain Controller cho phép quản trị viên quản lý và kiểm soát tất cả các người dùng, máy tính, nhóm và tài nguyên khác trong mạng domain từ một vị trí tập trung. Điều này giúp tăng tính linh hoạt và hiệu quả trong quản lý hệ thống.

Tính bảo mật cao: Domain Controller hỗ trợ xác thực và kiểm soát truy cập dựa trên quyền. Quản trị viên có thể thiết lập chính sách an ninh như mật khẩu phức tạp, quyền truy cập tài nguyên và giám sát hoạt động mạng để đảm bảo tính bảo mật cao cho hệ thống.

Đồng bộ hóa dữ liệu: Domain Controller đảm bảo rằng thông tin về người dùng, nhóm và tài nguyên là nhất quán trên toàn bộ mạng. Điều này giúp người dùng truy cập vào các tài nguyên một cách dễ dàng và hiệu quả hơn.

Quản lý chính sách: Domain Controller cho phép quản trị viên triển khai và quản lý các chính sách an ninh và cấu hình trên mạng domain. Điều này bao gồm quản lý mật khẩu, cấu hình tường lửa, cập nhật phần mềm và nhiều hơn nữa.

Quản lý phân quyền: Domain Controller cho phép quản trị viên quản lý và phân quyền truy cập cho người dùng và nhóm người dùng trong mạng domain. Điều này giúp đảm bảo rằng chỉ những người có quyền truy cập cụ thể mới có thể truy cập vào các tài nguyên.

Giảm chi phí vận hành: Bằng cách tập trung quản lý và kiểm soát, sử dụng Domain Controller có thể giúp giảm chi phí vận hành hệ thống. Việc tự động hóa các nhiệm vụ quản lý cũng có thể giảm thiểu thời gian và công sức của nhân viên IT.

Dễ dàng mở rộng: Domain Controller cho phép mở rộng mạng domain một cách dễ dàng bằng cách thêm mới các máy chủ Domain Controller phụ (additional domain controller) vào hạ tầng mạng hiện có.

2.5 Tầm quan trọng của việc triển khai Domain Controller trong tổ chức doanh nghiệp

Quản lý tập trung: Domain Controller cho phép quản trị viên quản lý tất cả các tài nguyên và người dùng trong mạng domain từ một vị trí tập trung. Điều này giúp đơn giản hóa quá trình quản lý và bảo trì hệ thống.

Bảo mật cao: Domain Controller cung cấp cơ chế xác thực và quản lý quyền truy cập để đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào các tài nguyên và thông tin nhạy cảm.

Phân quyền và kiểm soát truy cập: Domain Controller cho phép quản trị viên thiết lập và quản lý các chính sách phân quyền dựa trên nhóm người dùng, máy tính, hoặc các yếu tố khác trong mạng. Điều này giúp kiểm soát chặt chẽ việc truy cập đến các tài nguyên và dữ liệu.

Tăng tính nhất quán và đồng nhất: Domain Controller giúp đồng bộ hóa dữ liệu và cài đặt trên các máy tính và thiết bị trong mạng domain. Điều này giúp đảm bảo tính nhất quán và đồng nhất trong môi trường hệ thống.

Dễ dàng mở rộng và mở rộng: Domain Controller cho phép mở rộng hệ thống mạng một cách dễ dàng bằng cách thêm mới các máy tính, người dùng và tài nguyên vào mạng domain mà không cần thay đổi quá nhiều cấu hình.

Quản lý chính sách và cập nhật: Domain Controller cho phép quản trị viên triển khai và quản lý các chính sách an ninh, cập nhật, và cấu hình trên toàn bộ mạng domain một cách hiệu quả.

Tích hợp ứng dụng: Domain Controller hỗ trợ tích hợp với nhiều ứng dụng và dịch vụ khác nhau, bao gồm dịch vụ email, ứng dụng di động, và các giải pháp bảo mật.

CHƯƠNG 3. TRIỂN KHAI

3.1 Điều kiện chuẩn bị

Trong hướng dẫn này sẽ sử dụng:

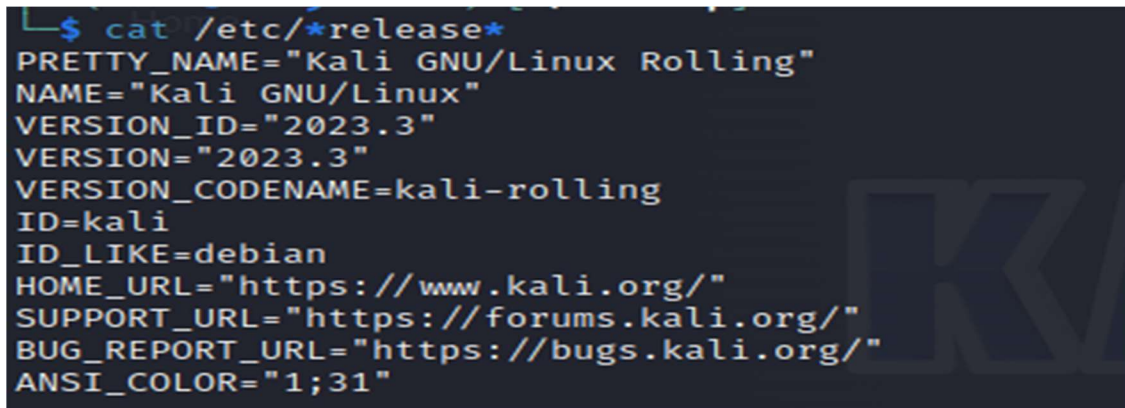
Một máy chủ:

Hostname: dc1

IP Address: 192.168.78.134

Domain: onn.com

FQDN: dc1.onn.com



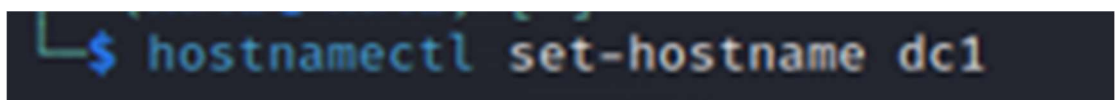
```
$ cat /etc/*release*
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION_ID="2023.3"
VERSION="2023.3"
VERSION_CODENAME=kali-rolling
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
```

Tài khoản người dùng quyền sudo.

Một máy tính Windows 10 trên cùng một mạng với máy chủ.

3.2 Thiết lập máy chủ

Mở terminal máy server, thay đổi tên máy chủ thành dc1. Sau đó reboot.



```
$ hostnamectl set-hostname dc1
```

Nhập chỉ định địa chỉ IP, FQDN và tên máy chủ của máy chủ.

Mở tệp máy chủ trong trình soạn thảo văn bản. Xóa bất kỳ mục nhập nào ánh xạ tên máy chủ hoặc FQDN của bạn đến bất kỳ IP nào ngoài IP tĩnh. Sau đó thêm một mục nhập ánh xạ FQDN và địa chỉ ip tĩnh của máy chủ lưu trữ.

```
sudo vi /etc/hosts
```

```
127.0.0.1    localhost
127.0.1.1    anhnha.localhost
#setup FQDN dc1.onn.com
192.168.78.134 dc1.onn.com dc1
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

```
$ hostname -f
dc1.onn.com
```

Xác minh FQDN của máy chủ Samba.

```
hostname -A
```

```
ping -c4 dc1.onn.com
```

3.2 Vô hiệu hóa dịch vụ phân giải DNS

Dừng và vô hiệu hóa dịch vụ phân tích cú pháp systemd.

```
sudo systemctl disable --now systemd-resolved
```

Xóa liên kết tượng trưng

```
$ sudo unlink /etc/resolv.conf
```

Thêm trình phân giải DNS dự phòng (trình phân giải DNS công cộng của Cloudflare)

```
sudo nano /etc/resolv.conf
```

```
Samba server IP address
nameserver 192.168.78.134

# fallback resolver
nameserver 1.1.1.1

# main domain for Samba
search onn.com
```

Lệnh sau để làm cho tệp tệp bất biến. Bước này đảm bảo rằng trình phân giải không vô tình thay đổi vì bất kỳ lý do gì.

```
$ sudo chattr +i /etc/resolv.conf
```

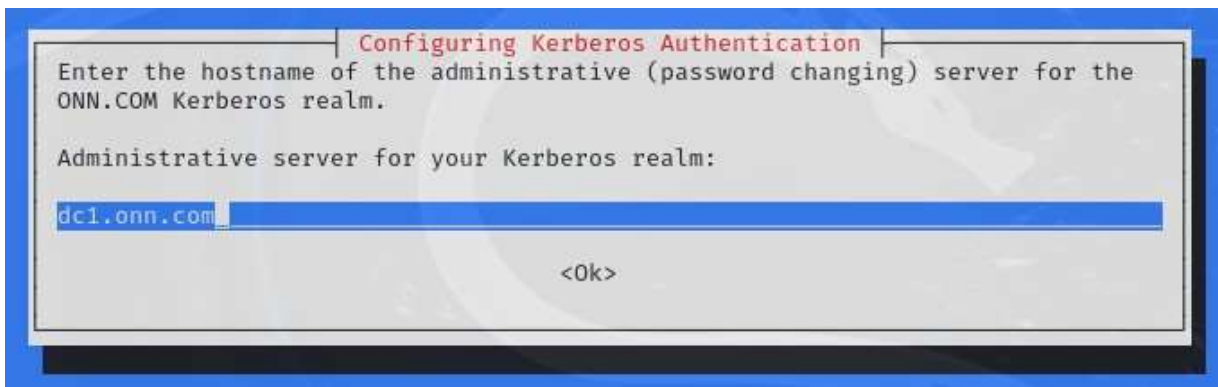
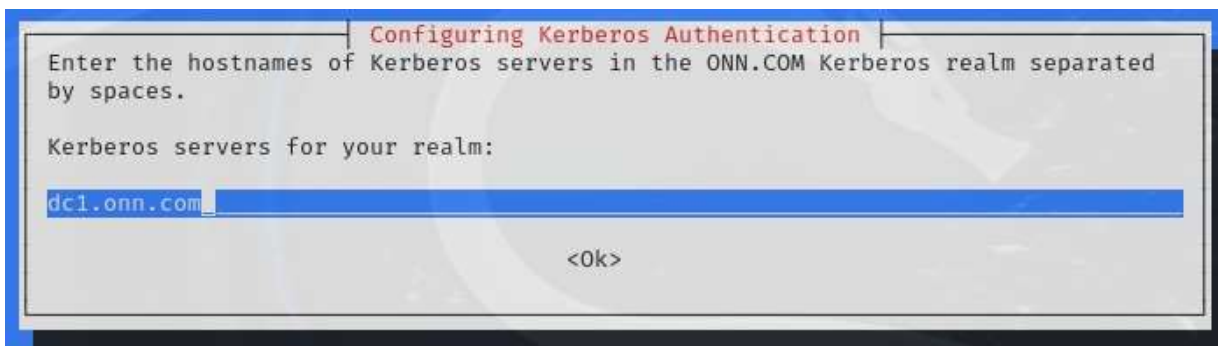
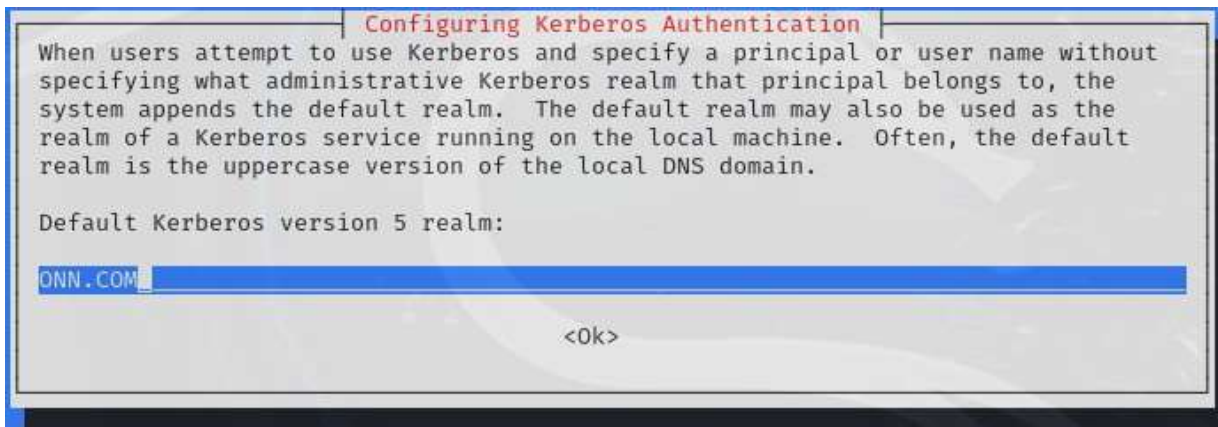
3.3 Cài đặt Samba

```
$ sudo apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
386 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

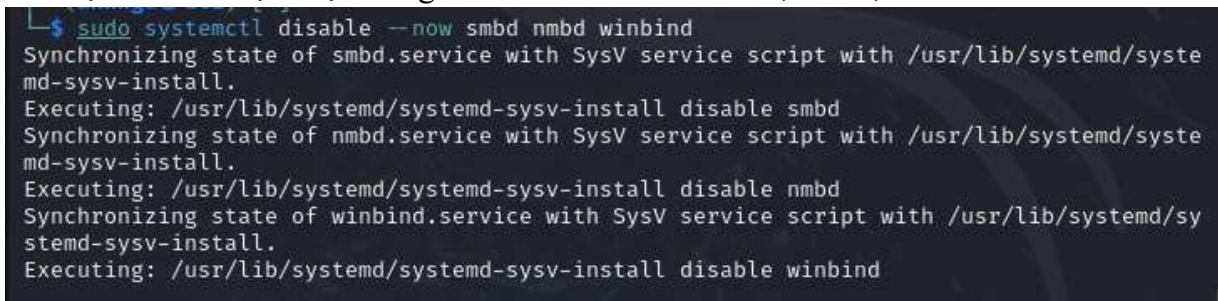
Cài đặt các gói cần thiết.

```
$ sudo apt install -y acl attr samba samba-dsdb-modules samba-vfs-modules smbclient wi
nbind libpam-winbind libnss-winbind libpam-krb5 krb5-config krb5-user dnsutils chrony ne
t-tools
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
acl is already the newest version (2.3.2-1).
acl set to manually installed.
attr is already the newest version (1:2.5.2-1).
attr set to manually installed.
net-tools is already the newest version (2.10-0.1).
net-tools set to manually installed.
The following additional packages will be installed:
bind9-dnsutils bind9-host bind9-libs libgssrpc4 libkadm5clnt-mit12 libkadm5srv-mit12
libldb5-10 libldb2 libsmbclient libwbclient0 python3-ldb python3-samba
samba-ad-provision samba-common samba-common-bin samba-libs winexe
Suggested packages:
```

Cấu hình xác thực Kerberos, nhập miền DNS bằng chữ hoa



Vô hiệu hóa các dịch vụ không cần thiết như là winbind, smb, nmbd.



Kích hoạt và kích hoạt dịch vụ samba-ad-dc. Dịch vụ này là những gì Samba cần để hoạt động như một máy chủ Linux điều khiển miền Active Directory.

```
sudo systemctl unmask samba-ad-dc
```

```
$ sudo systemctl enable samba-ad-dc
Synchronizing state of samba-ad-dc.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable samba-ad-dc
Created symlink /etc/systemd/system/samba.service → /usr/lib/systemd/system/samba-ad-dc.service.
Created symlink /etc/systemd/system/multi-user.target.wants/samba-ad-dc.service → /usr/lib/systemd/system/samba-ad-dc.service.
```

3.4 Cấu hình Samba Active Directory

Sao lưu các tệp smb.conf, krb5.conf.

```
$ sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.orig
```

Cung cấp Samba Active Directory.

```
sudo samba-tool domain provision
```

Quảng bá Samba lên máy chủ Linux bộ điều khiển miền Active Directory.

–use-rfc2307 => cho phép DC quản lý tài khoản người dùng dựa trên UNIX một cách thích hợp.

```
$ sudo samba-tool domain provision
Realm [ONN.COM]:
Domain [ONN]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [192.168.78.134]: 1.1.1.1
Administrator password:
Retype password:
INFO 2024-03-11 12:32:15,991 pid:20747 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2128: Looking up IPv4 addresses
INFO 2024-03-11 12:32:15,991 pid:20747 /usr/lib/python3/dist-packages/samba/provision/__init__.py #2128: Looking up IPv4 addresses
```



```
INFO 2024-03-11 12:32:22,060 pid:20747 /usr/lib/python3/dist-packages/samba/provision/
init__.py #498: Server Role: active directory domain controller
INFO 2024-03-11 12:32:22,060 pid:20747 /usr/lib/python3/dist-packages/samba/provision/
init__.py #499: Hostname: dc1
INFO 2024-03-11 12:32:22,060 pid:20747 /usr/lib/python3/dist-packages/samba/provision/
init__.py #500: NetBIOS Domain: ONN
INFO 2024-03-11 12:32:22,060 pid:20747 /usr/lib/python3/dist-packages/samba/provision/
init__.py #501: DNS Domain: onn.com
INFO 2024-03-11 12:32:22,060 pid:20747 /usr/lib/python3/dist-packages/samba/provision/
init__.py #502: DOMAIN SID: S-1-5-21-2185711356-665357012-1791803168
```

Sao chép tệp cấu hình Samba AD Kerberos vào /etc/kerb.conf.

```
$ sudo mv /etc/krb5.conf /etc/krb5.conf.orig
$ sudo cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Bật trạng thái dịch vụ **sudo systemctl start samba-ad-dc**

```
$ sudo systemctl status samba-ad-dc
● samba-ad-dc.service - Samba AD Daemon
   Loaded: loaded (/usr/lib/systemd/system/samba-ad-dc.service; enabled; preset: disabled)
   Active: active (running) since Mon 2024-03-11 12:34:20 EDT; 13s ago
     Docs: man:samba(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 22198 ExecCondition=/usr/share/samba/is-configured samba (code=exited, status=0)
 Main PID: 22200 (samba)
    Status: "samba: ready to serve connections ..."
      Tasks: 58 (limit: 4568)
    Memory: 192.5M (peak: 267.1M)
       CPU: 3.616s
    CGroup: /system.slice/samba-ad-dc.service
```

3.5 Thiết lập đồng bộ hóa thời gian.

Thay đổi quyền và quyền sở hữu mặc định của thư mục. Người dùng/nhóm phải có quyền đọc thư mục

```
$ sudo chown root:chrony /var/lib/samba/ntp_signd/
$ sudo chmod 750 /var/lib/samba/ntp_signd/
```

Cấu hình này cho phép máy chủ NTP chrony và trở vị trí ổ cắm NTP đến.

/var/lib/samba/ntp_signd/ntp_signed_chronyntp_signed

```
# bind the chrony service to IP address of the Samba AD
bindcmdaddress 192.168.78.134

# allow clients on the network to connect to the Chrony NTP server
allow 192.168.78.0/24

# specify the ntpsigndsocket directory for the Samba AD
ntpsigndsocket /var/lib/samba/ntp_signd
```

Khởi động lại và xác minh dịch vụ trên máy chủ Samba AD.

```
$ sudo systemctl enable --now chrony
Synchronizing state of chrony.service with SysV service script with /usr/lib/systemd/s
ystemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable chrony
Created symlink /etc/systemd/system/chronyd.service → /usr/lib/systemd/system/chrony.s
ervice.
Created symlink /etc/systemd/system/multi-user.target.wants/chrony.service → /usr/lib/
systemd/system/chrony.service.
```

```
$ sudo systemctl status chronyd
● chrony.service - chrony, an NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chrony.service; enabled; preset: disable>
   Active: active (running) since Mon 2024-03-11 12:40:56 EDT; 1min 50s ago
     Docs: man:chronyd(8)
           man:chronyc(1)
           man:chrony.conf(5)
  Main PID: 25797 (chronyd)
    Tasks: 2 (limit: 4568)
   Memory: 1.4M (peak: 1.9M)
      CPU: 32ms
   CGroup: /system.slice/chrony.service
           └─25797 /usr/sbin/chronyd -F 1
             25798 /usr/sbin/chronyd -F 1

Mar 11 12:40:56 dc1 systemd[1]: Starting chrony.service - chrony, an NTP client/serve>
Mar 11 12:40:56 dc1 chronyd[25797]: chronyd version 4.5 starting (+CMDMON +NTP +REFCL>
Mar 11 12:40:56 dc1 chronyd[25797]: Loaded 0 symmetric keys
Mar 11 12:40:56 dc1 chronyd[25797]: Frequency -5.806 +/- 1000000.000 ppm read from /v>
Mar 11 12:40:56 dc1 chronyd[25797]: Using right/UTC timezone to obtain leap second da>
Mar 11 12:40:56 dc1 chronyd[25797]: MS-SNTP authentication enabled
Mar 11 12:40:56 dc1 chronyd[25797]: Loaded seccomp filter (level 1)
```

3.6 Xác minh Samba Active Directory.

Kiểm tra domain.

```
$ host -t A dc1.onn.com
dc1.onn.com has address 192.168.78.134
```

```
$ host -t A onn.com
onn.com has address 192.168.78.134
```

Xác minh rằng và bản ghi dịch vụ đều trỏ đến FQDN của máy chủ Samba Active Directory.

```
$ host -t SRV _kerberos._udp.onn.com
_kerberos._udp.onn.com has SRV record 0 100 88 dc1.onn.com.
```

```
$ host -t SRV _ldap._tcp.onn.com
_ldap._tcp.onn.com has SRV record 0 100 389 dc1.onn.com.
```

Xác minh các tài nguyên mặc định có sẵn trên Samba Active Directory.

```
$ smbclient -L onn.com -N
Anonymous login successful

      Sharename      Type      Comment
      _____      _____
      sysvol          Disk
      netlogon         Disk
      IPC$             IPC       IPC Service (Samba 4.19.5-Debian)
SMB1 disabled -- no workgroup available
```

Xác thực với máy chủ Kerberos bằng cách sử dụng người dùng và xác minh vé Kerberos được lưu trong bộ nhớ cache trên hệ thống của bạn.

```
$ kinit administrator@ONN.COM
Password for administrator@ONN.COM:
Warning: Your password will expire in 41 days on Mon Apr 22 12:32:20 2024
```

```

$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: administrator@ONN.COM

Valid starting     Expires            Service principal
03/11/24 13:41:07  03/11/24 23:41:07  krbtgt/ONN.COM@ONN.COM
        renew until 03/12/24 13:41:02

```

3.7 Tạo người dùng Samba Active Directory mới

```

$ sudo samba-tool user create thuy thuythanh777@
User 'thuy' added successfully

```

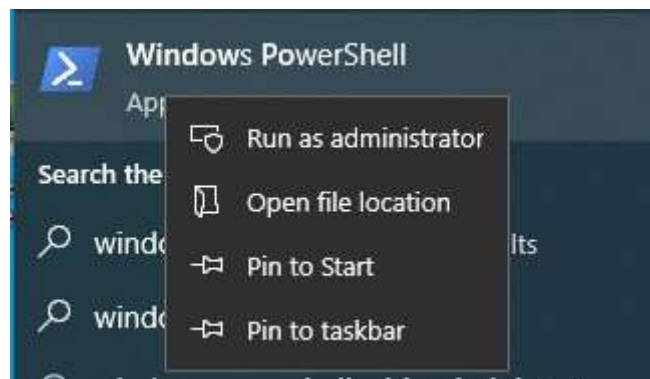
```

$ sudo samba-tool user list
Guest
Administrator
krbtgt
thuy

```

3.8 Tham gia và đăng nhập vào miền Samba Active Directory

Click run as administrator.



Liệt kê các bộ điều hợp ethernet có sẵn trên PC Windows.

```

PS C:\> Get-NetAdapter

Name      InterfaceDescription          ifIndex Status      MacAddress           LinkSpeed
----      -
Ethernet0 Intel(R) 82574L Gigabit Network Conn... 9 Up         00-0C-29-2B-FE-46    1 Gbps

```


Thay đổi máy chủ DNS của bộ điều hợp thành địa chỉ IP của Samba Active Directory với dự phòng bổ sung Cloudflare DNS. Thực hiện bước này đảm bảo rằng máy trạm của bạn sử dụng máy chủ Samba AD để phân giải tên. 1.1.1.1

```
PS C:\> Set-DNSClientServerAddress "Ethernet0" -ServerAddresses ("192.168.78.134","1.1.1.1")
PS C:\> Get-DNSClientServerAddress
```

| InterfaceAlias | Interface Index | Address Family | ServerAddresses |
|-----------------------------|-----------------|----------------|--|
| Ethernet0 | 9 | IPv4 | {192.168.78.134, 1.1.1.1} |
| Ethernet0 | 9 | IPv6 | {} |
| Loopback Pseudo-Interface 1 | 1 | IPv4 | {} |
| Loopback Pseudo-Interface 1 | 1 | IPv6 | {fec0:0:0:ffff::1, fec0:0:0:ffff::2, fec0:0:0:ffff::3} |

Ping máy chủ, tên miền, kết quả ping thành công. Kết quả trở đến địa chỉ IP của máy chủ Samba AD.

```
PS C:\> ping dcl.onn.com

Pinging dcl.onn.com [192.168.78.134] with 32 bytes of data:
Reply from 192.168.78.134: bytes=32 time<1ms TTL=64
Reply from 192.168.78.134: bytes=32 time<1ms TTL=64
Reply from 192.168.78.134: bytes=32 time<1ms TTL=64
Reply from 192.168.78.134: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.78.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
PS C:\> ping onn.com

Pinging onn.com [192.168.78.134] with 32 bytes of data:
Reply from 192.168.78.134: bytes=32 time<1ms TTL=64
Reply from 192.168.78.134: bytes=32 time<1ms TTL=64
Reply from 192.168.78.134: bytes=32 time<1ms TTL=64
Reply from 192.168.78.134: bytes=32 time<1ms TTL=64

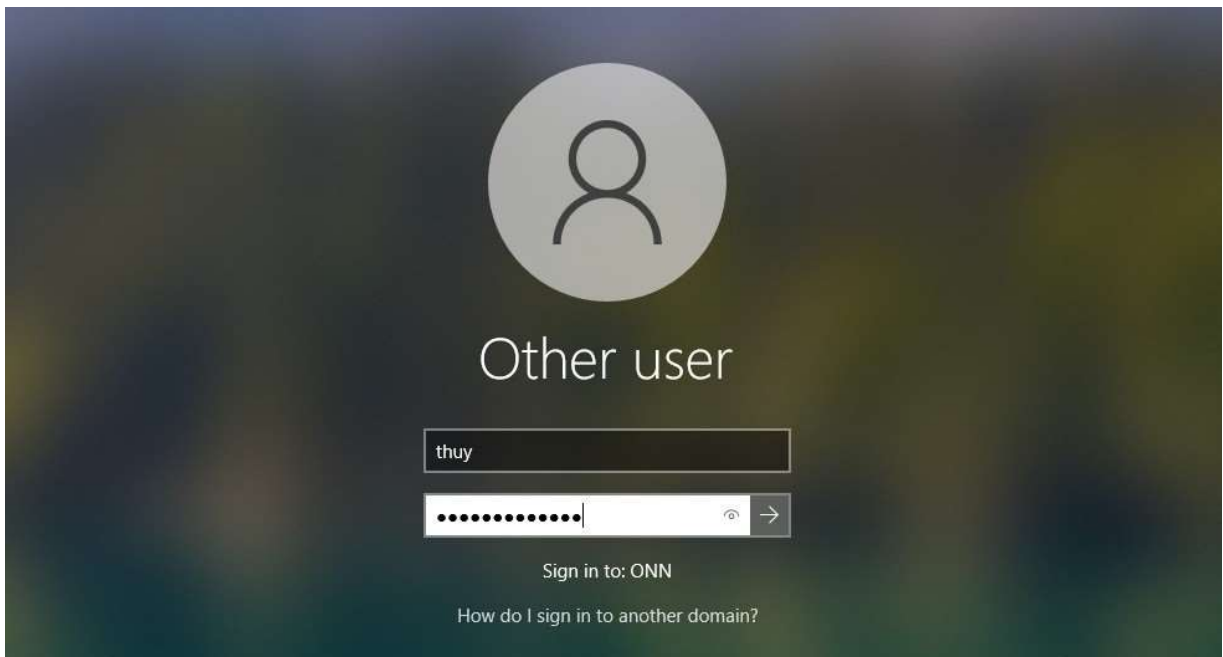
Ping statistics for 192.168.78.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\>
```

Thêm Windows 10 vào Active Directory.

Add-Computer -DomainName "onn.com" -Restart



Sau khi khởi động lại, nhấp vào màn hình đăng nhập. Nhập tên người dùng và mật khẩu Active Directory của người dùng Samba AD mà bạn đã tạo trước đó (), và nhấn Enter để đăng nhập. `thuy@onn.com`



Đăng nhập thành công, hãy mở cửa sổ PowerShell và chạy trên hoặc cả hai lệnh bên dưới để xác minh tên người dùng hiện đang đăng nhập.

```
C:\Users\thuy>whoami
onn\thuy

C:\Users\thuy>query user
 USERNAME      SESSIONNAME  ID  STATE   IDLE TIME  LOGON TIME
  -----
  admin         console      1   Disc    1  3/12/2024 12:57 AM
  >thuy         console      2   Active  1  3/12/2024 1:01 AM

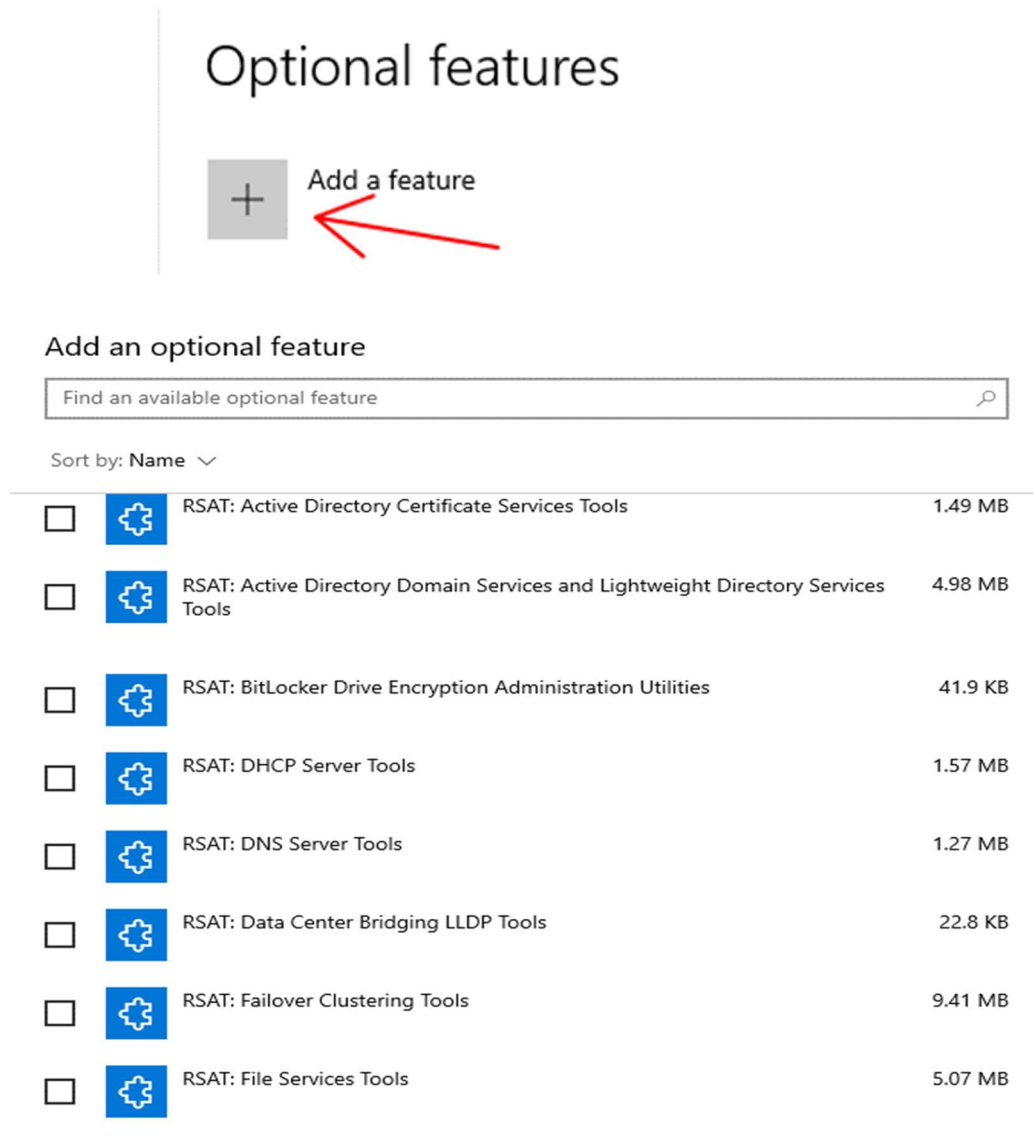
C:\Users\thuy>
```

CHƯƠNG 4: QUẢN LÝ DOMAIN CONTROLLER

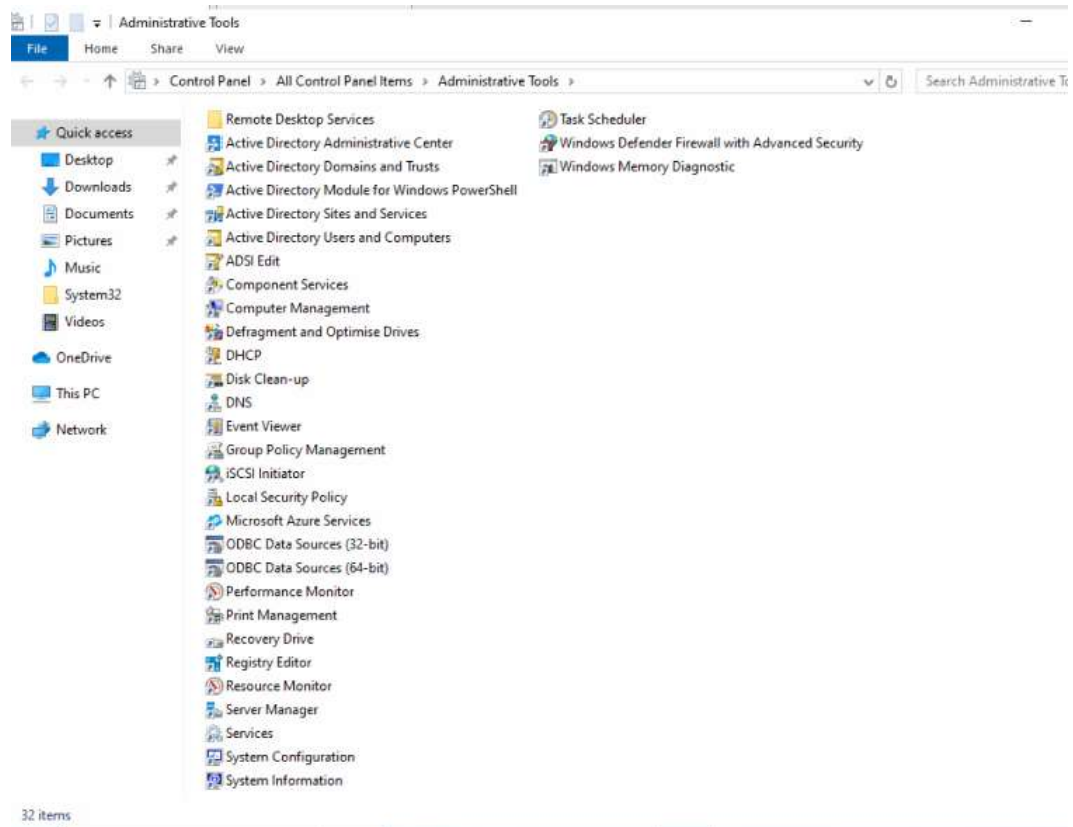
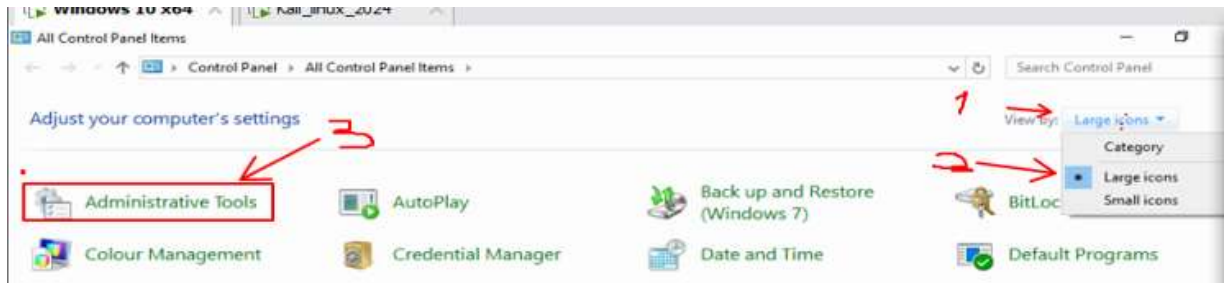
4.1 Cài đặt công cụ quản trị máy chủ từ xa (RSAT)

Nhập vào trường tìm kiếm: **Optional features**

Thêm features, cài đặt những tính năng cần thiết.

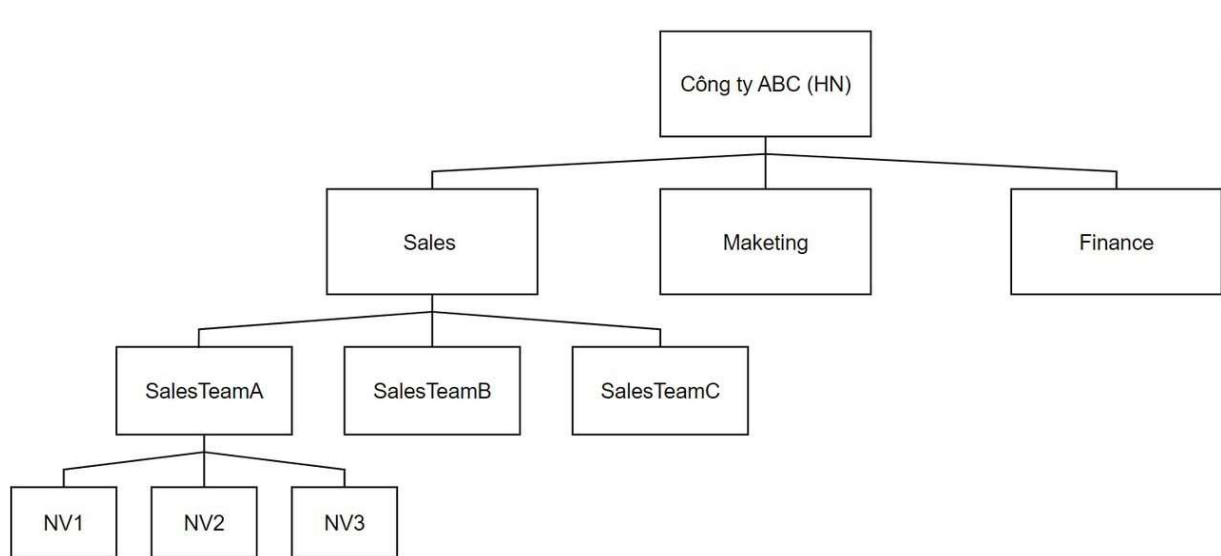


Có thể tìm thấy các tools đã cài đặt ở đây.



4.2 quản lý người dùng trong miền.

4.2.1 Mô tả tình huống, vấn đề thách thức.



Mô hình công ty ABC

Ví dụ: mô hình quản lý của 1 công ty : Một công ty ABC có chi nhánh ở Hà Nội và được chia làm các phòng ban : Sales, Marketing, Finance, Mỗi phòng ban sẽ được chia làm các Group quản lý nhân viên khác nhau. Ví dụ trong sơ đồ trên phòng ban Sales sẽ có các group sales khác nhau như là SalesTeamA, Sales Team B, SalesTeamC. Trong mỗi group sẽ có các nhân viên phục vụ cho các đối tượng phân cấp của công ty.

Một số thách thức đưa ra:

| Vấn đề: | Ví dụ: | CIA |
|------------------------|--|--|
| Quản lý quyền truy cập | Nhân viên từ phòng Marketing cần truy cập vào tài liệu quảng cáo, nhưng không nên có quyền truy cập vào tài liệu kế toán nhạy cảm. | Bảo mật (Confidentiality) - đảm bảo rằng thông tin nhạy cảm chỉ được truy cập bởi những người được ủy quyền. |

| | | |
|----------------------|--|---|
| Sự thay đổi liên tục | Khi một nhân viên từ phòng Sales chuyển sang phòng Marketing, quyền truy cập của họ cần được điều chỉnh tương ứng. | Sẵn sàng (Availability) - đảm bảo rằng hệ thống có khả năng phản ứng linh hoạt với các thay đổi và người dùng có thể truy cập vào tài nguyên khi cần thiết. |
| Hiệu suất và mở rộng | Khi công ty mở rộng và mở thêm chi nhánh mới, hệ thống domain controller cần có khả năng mở rộng linh hoạt. | Sẵn sàng (Availability) - đảm bảo rằng hệ thống có thể mở rộng để đáp ứng nhu cầu của môi trường doanh nghiệp. |
| Bảo trì và hỗ trợ | Cần có kế hoạch bảo trì định kỳ để đảm bảo tính sẵn sàng và an toàn của hệ thống. | Sẵn sàng (Availability) - đảm bảo rằng hệ thống có thể được bảo trì một cách hiệu quả mà không ảnh hưởng đến khả năng truy cập của người dùng. |

Giải pháp:

Để giải quyết vấn đề thông tin trên mạng máy tính giải pháp đưa ra cho Công ty ABC là triển khai một hệ thống quản lý Domain Controller. Domain Controller sẽ đóng vai trò như một trung tâm quản lý người dùng, máy tính và tài nguyên mạng, giúp tổ chức và quản lý dữ liệu một cách hiệu quả. Bằng cách này, công ty có thể tạo và quản lý các tài khoản người dùng, thiết lập các chính sách bảo mật, và theo dõi hoạt động trên mạng để đảm bảo tính an toàn và bảo mật của hệ thống. Qua việc triển khai Domain Controller, Công ty ABC hy vọng sẽ tăng cường khả năng quản lý và bảo vệ thông tin quan trọng của mình một cách hiệu quả.

4.2.2 Thư mục trang chủ người dùng.

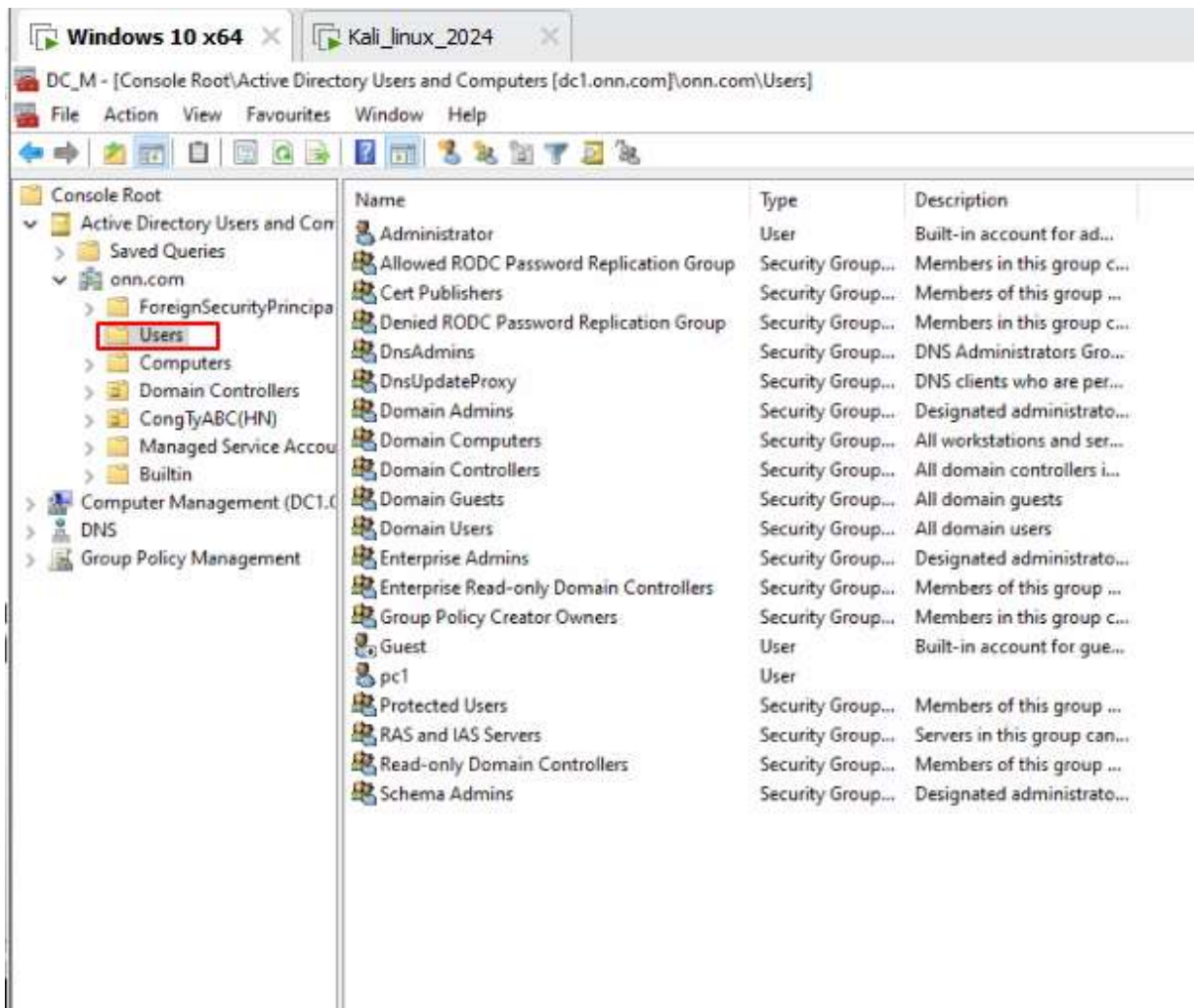
Định nghĩa cơ bản:

OU (Organizational Unit - Đơn vị Tổ chức): Là cách tổ chức và quản lý người dùng và máy tính trong một hệ thống. Giúp tổ chức các đối tượng để dễ dàng quản lý và áp dụng chính sách.

Nhóm (Group): Là một tập hợp người dùng hoặc đối tượng khác. Dùng để quản lý quyền truy cập và chia sẻ tài nguyên.

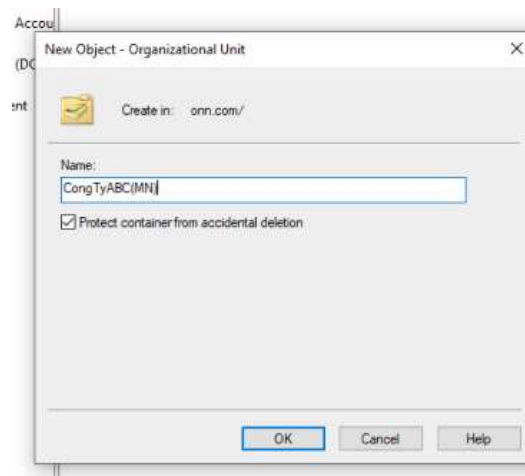
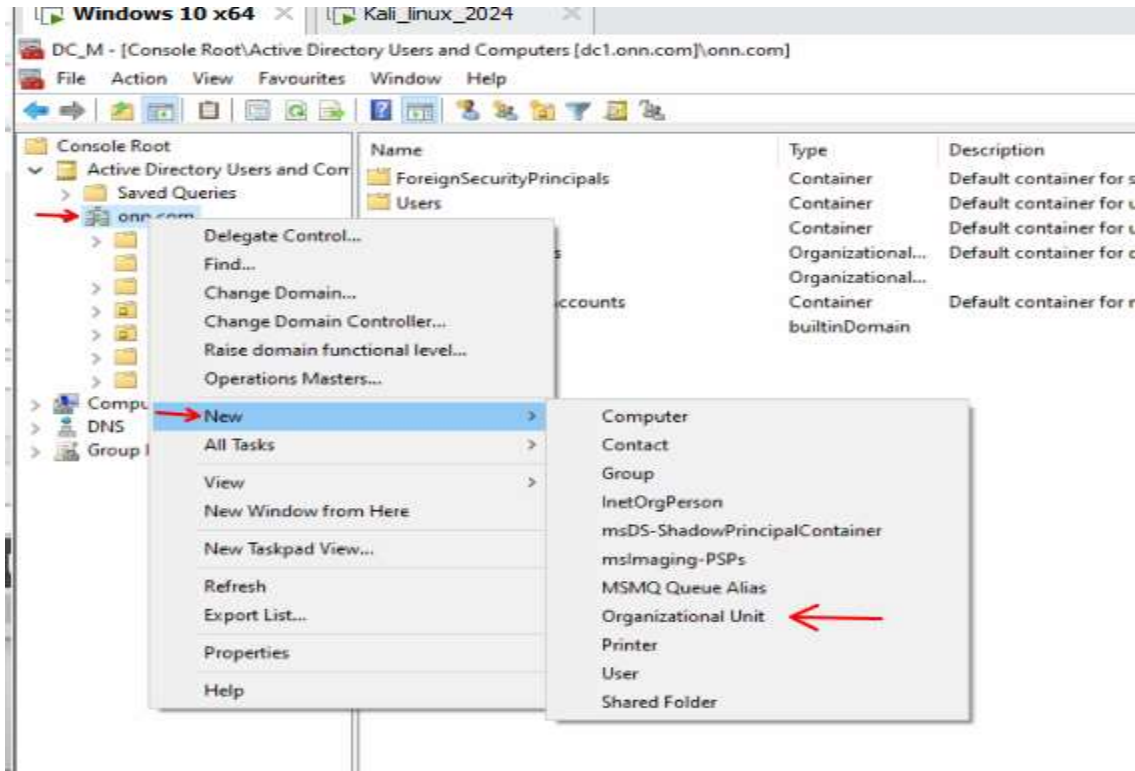
Người dùng (User): Cá nhân sử dụng hệ thống máy tính. Mỗi người dùng có một tài khoản riêng để truy cập vào hệ thống và được tổ chức vào các nhóm để quản lý quyền truy cập.

Xem tất cả nhóm người dùng, người dùng trong domain:



Tạo OU:

Nhập vào tên miền > lick chuột phải > chọn new > chọn Ogranization Unit > Đặt tên cho OU > ok để tiếp tục.

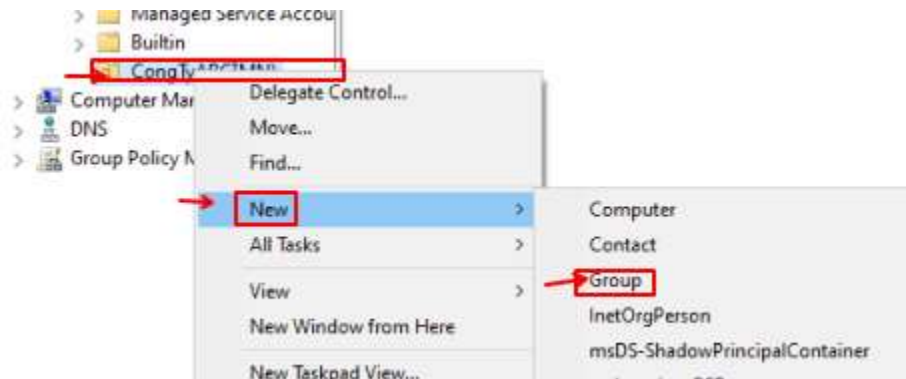


OU có tên là CongTyABC(MN) đã được tạo thành công.



Tạo group :

Nhấp vào phân cấp nơi sẽ tạo group > chuột phải > new > Group



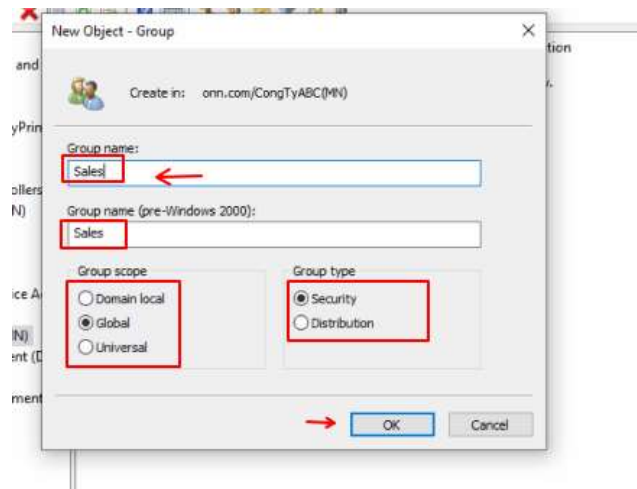
Đặt tên group > chọn scope và type.

Group scope:

- Domain local : sử dụng gán quyền truy cập vào tài nguyên trong cùng một miền hoặc trong các miền khác.
- Global: sử dụng để quản lý quyền truy cập cho người dùng và tài nguyên trong một miền cụ thể.
- Universal: sử dụng để quản lý quyền truy cập cho người dùng và tài nguyên trong các miền khác nhau.

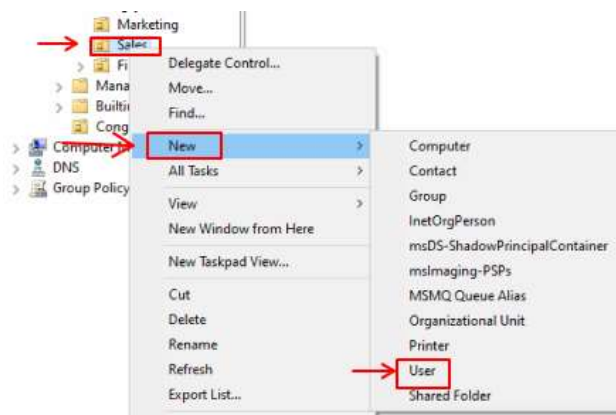
Group Type:

- Security Group: sử dụng để quản lý quyền truy cập vào tài nguyên trong hệ thống. Khi bạn thêm người dùng vào một nhóm bảo mật, họ sẽ được gán các quyền truy cập tương tự như nhóm đó.
- Distribution Group: sử dụng để gửi thư điện tử đến một nhóm người dùng. Thông điệp được gửi đến địa chỉ email của nhóm và được chuyển đến tất cả các thành viên của nhóm để đảm bảo rằng thông tin được chia sẻ với toàn bộ nhóm. Mà không cần quan tâm đến việc quản lý truy cập tài nguyên.



Tạo user:

Chuột phải vào phân cấp > new > user.



Tạo thông tin user và mật khẩu:

New Object - User

Create in: onn.com/CongTyABC(HN)/Sales

First name: nv1 Initials:

Last name:

Full name: nv1

User logon name: nv1 @onn.com

User logon name (pre-Windows 2000): ONN\ nv1

< Back Next > Cancel

New Object - User

Create in: onn.com/CongTyABC(HN)/Sales

Password:

Confirm password:

☐ User must change password at next logon

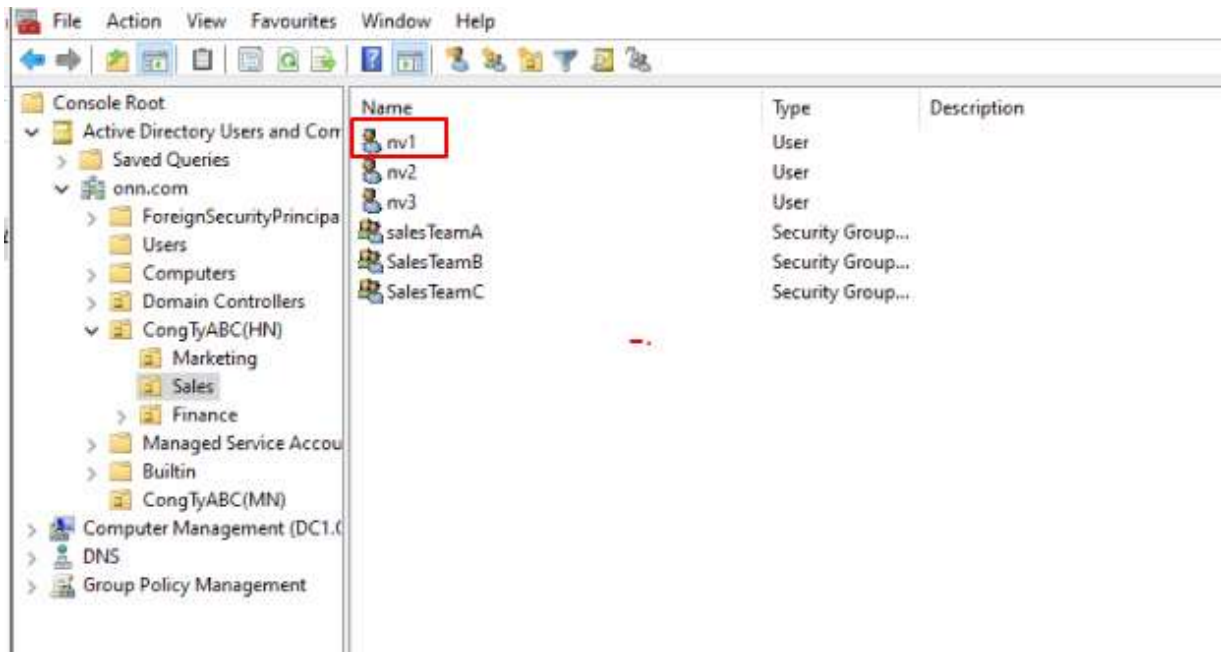
☒ User cannot change password

☐ Password never expires

☐ Account is disabled

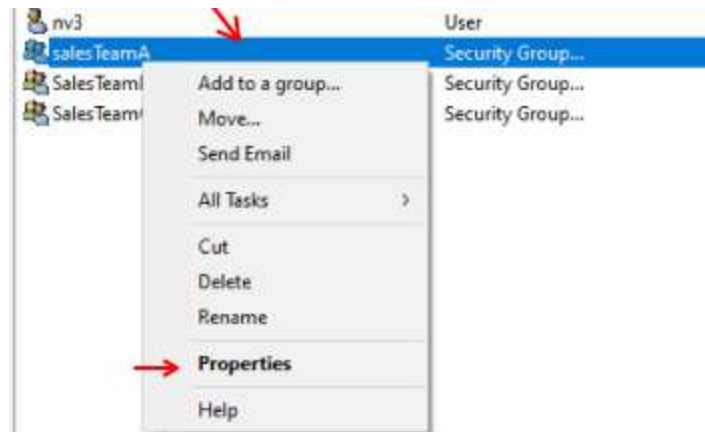
< Back Next > Cancel

Tài khoản đã được tạo thành công:

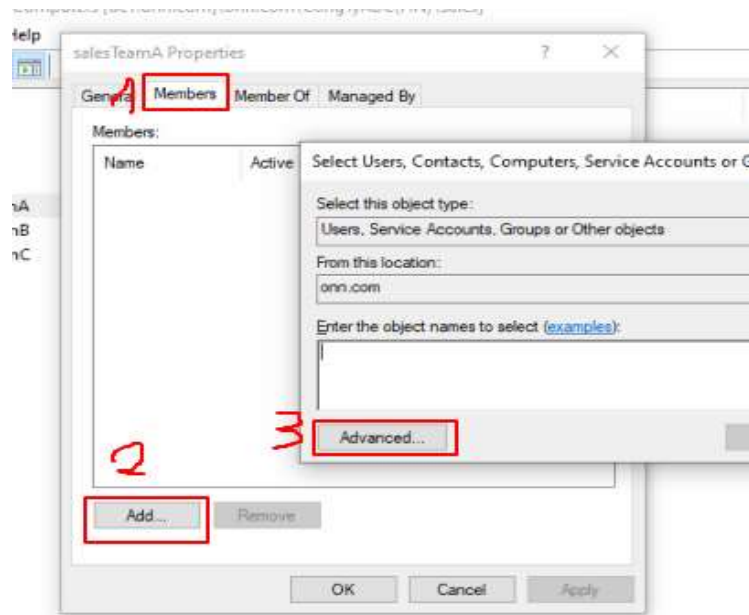


Đưa user vào group:

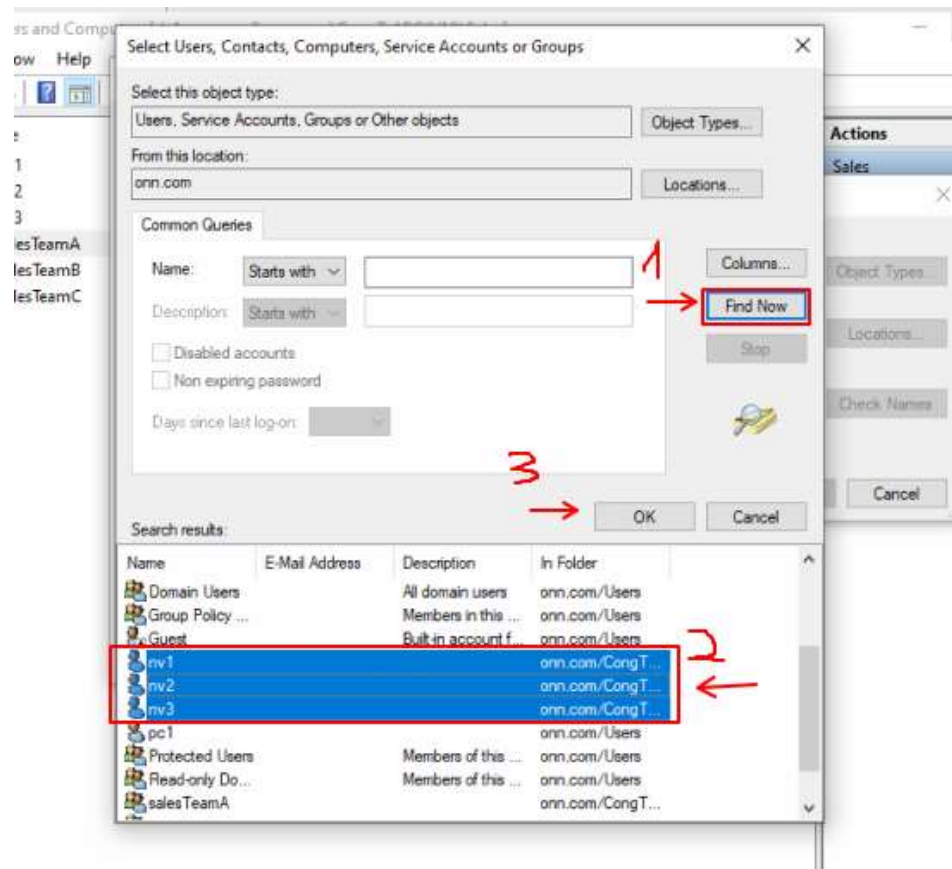
chọn group > chuột phải > thuộc tính > chọn Members > add > advanced



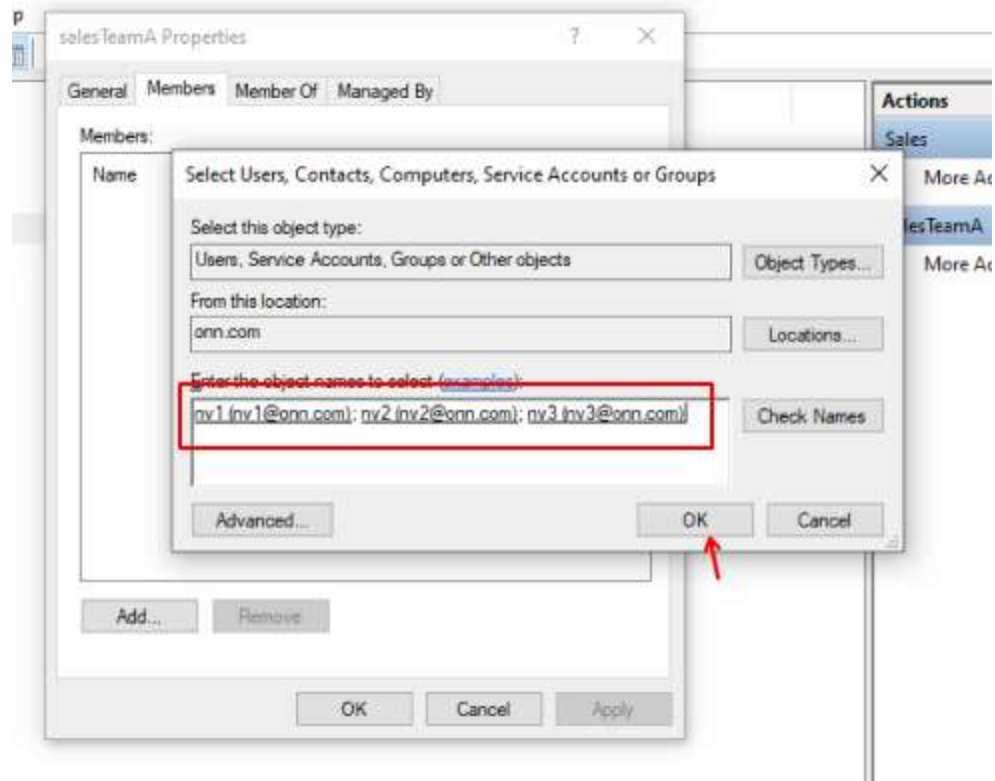
DEPLOYING-DOMAIN-CONTROLLER-ON-LINUX-SERVER



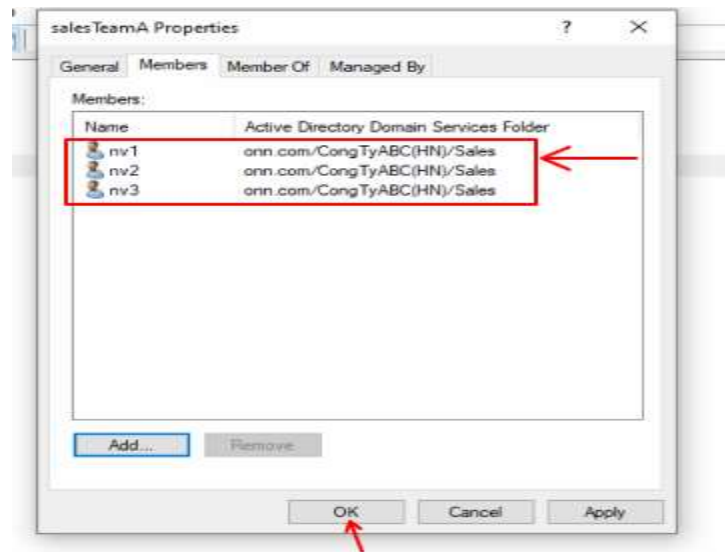
chọn find now để tìm kiếm các user > chọn các user sẽ thêm vào group > ok



kiểm tra các user cần thiết đã đúng > nhấn ok tiếp tục

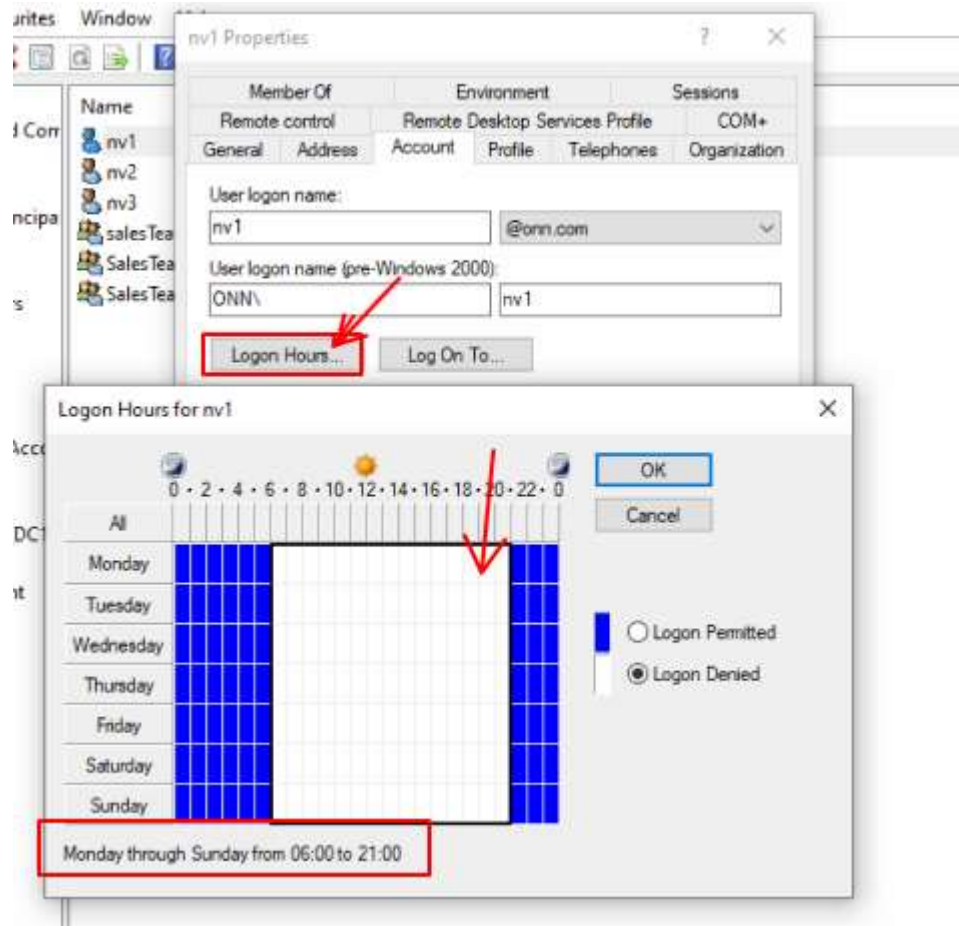


Các user được thêm vào group thành công.

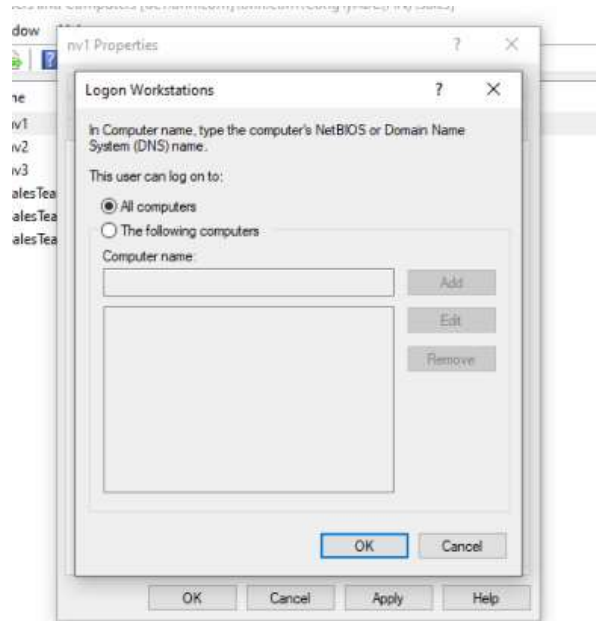


Một số thiết lập khác:

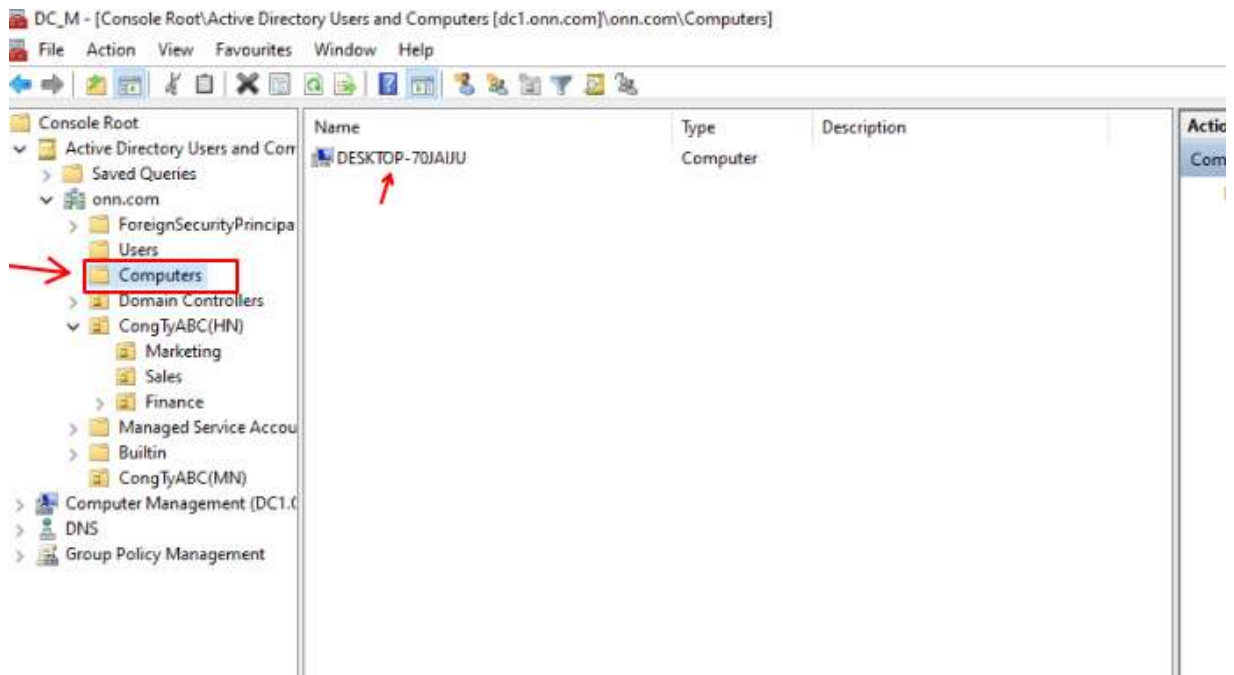
Thiết lập thời gian logon hours của người sử dụng : Hạn chế thời gian user có thể đăng nhập vào hệ thống.



Xác định máy tính mà người dùng này được phép đăng nhập trong domain.(Logon Workstations)



Xác định các máy tính đã tham gia vào miền thông qua thư mục “Computers”.

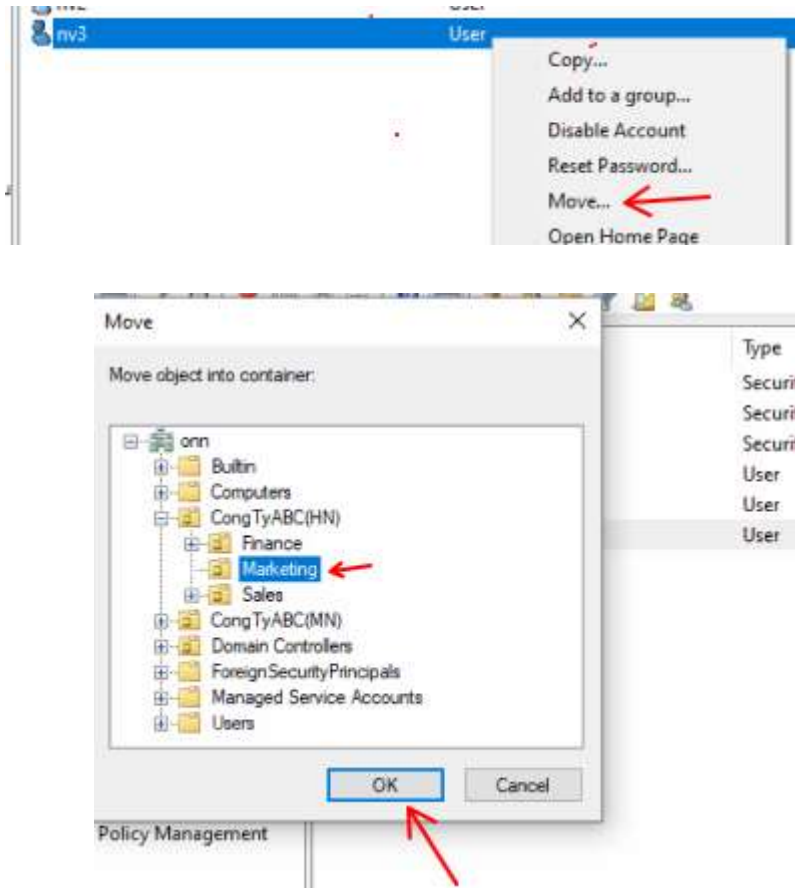


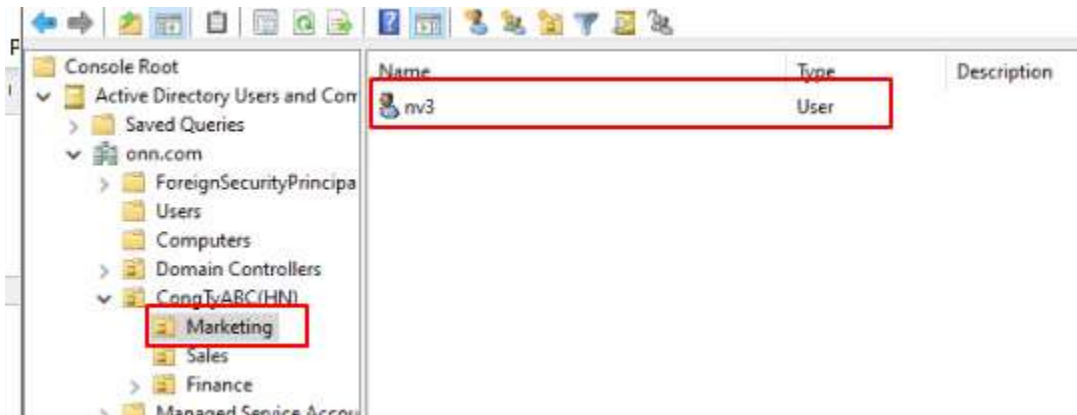
Chuyển đối tượng sang một vị trí khác trong cây thư mục thông qua “move”.

- Lưu ý : đảm bảo di chuyển đối tượng phù hợp phân cấp.

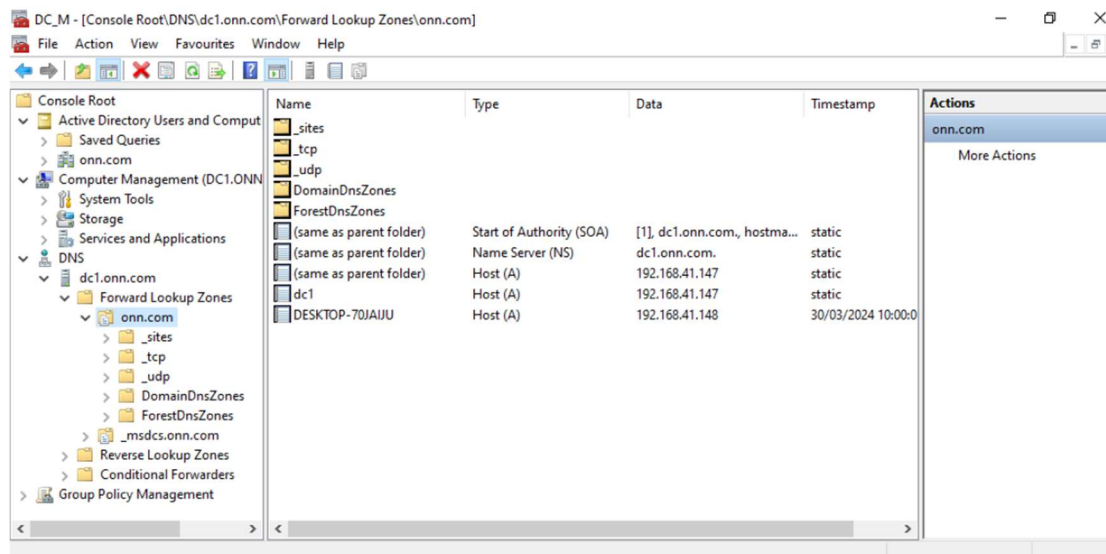
Giả sử tôi chuyển công tác một nhân viên đến 1 bộ phận khác.

- Chuột phải vào nv3 > move > chọn bộ phận nv di chuyển tới. Cụ thể trong minh họa dưới đây tôi chuyển nv3 từ group SalesTeamA sang OU Marketing.





Quản lý khu vực DNS của domain.



4.3 Tạo shared folders

Tại máy domain server tạo folders có tên là **apps**

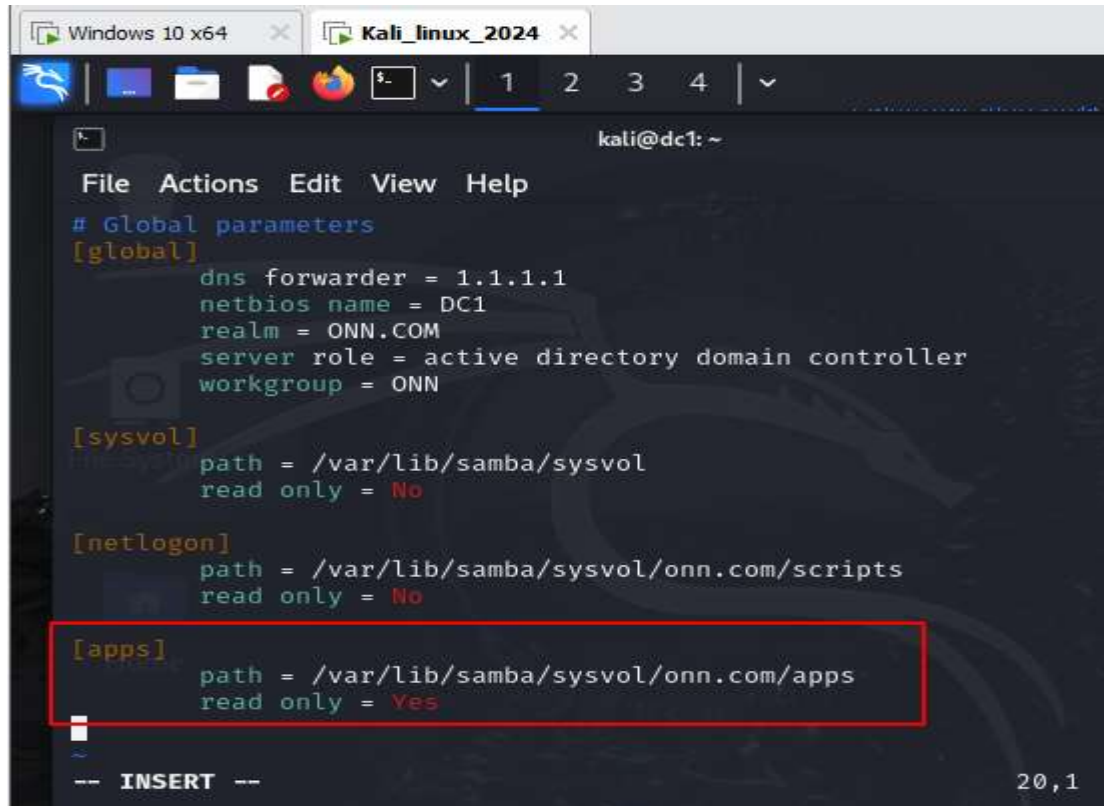
```
(kali@dc1)-[~]
$ sudo mkdir -p /var/lib/samba/sysvol/onnn.com/apps
```

Mở tệp cấu hình **smb.conf**

```
(kali@dc1)-[~]
$ sudo vi /etc/samba/smb.conf
```


Nhập thông tin như hình và lưu file cấu hình.

readonly: nó chỉ cho phép người dùng đọc tệp hoặc thư mục được chia sẻ mà không cho phép họ thay đổi, xóa hoặc tạo mới các tệp hoặc thư mục.



```

File Actions Edit View Help
# Global parameters
[global]
    dns forwarder = 1.1.1.1
    netbios name = DC1
    realm = ONN.COM
    server role = active directory domain controller
    workgroup = ONN

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

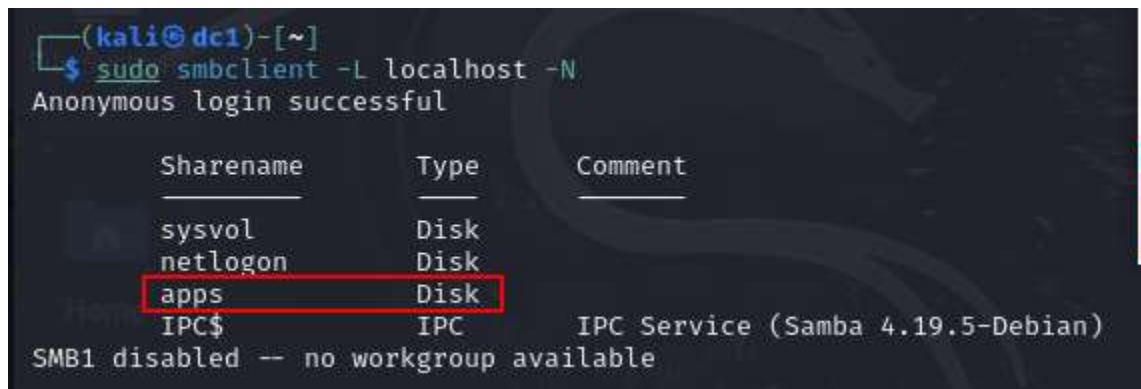
[netlogon]
    path = /var/lib/samba/sysvol/onn.com/scripts
    read only = No

[apps]
    path = /var/lib/samba/sysvol/onn.com/apps
    read only = Yes

-- INSERT --
20,1

```

Liệt kê các tài nguyên chia sẻ trên máy chủ Samba cục bộ (không yêu cầu mật khẩu xác thực)



```

(kali@dc1)-[~]
$ sudo smbclient -L localhost -N
Anonymous login successful

  Sharename      Type      Comment
  -----
  sysvol         Disk
  netlogon       Disk
  apps           Disk
  IPC$           IPC       IPC Service (Samba 4.19.5-Debian)
SMB1 disabled -- no workgroup available

```


Xem quyền và chỉnh sửa quyền cho folder apps.

755: Cho phép chủ sở hữu, nhóm sở hữu đọc, ghi, thực thi, Cho phép các người dùng khác có quyền đọc và thực thi, nhưng không được phép sửa đổi (ghi) các tệp hoặc thư mục.

```
(kali@dc1)-[~]
$ sudo ls -l /var/lib/samba/sysvol/onn.com
total 24
drwxrwx---+ 2 root root          4096 Mar 30 06:19 apps
drwxrwx---+ 4 root BUILTIN\administrators 4096 Mar 28 11:33 Policies
drwxrwx---+ 2 root BUILTIN\administrators 4096 Mar 28 11:33 scripts

(kali@dc1)-[~]
$ sudo chmod 775 /var/lib/samba/sysvol/onn.com/apps

(kali@dc1)-[~]
$ sudo ls -l /var/lib/samba/sysvol/onn.com
total 24
drwxrwxr-x+ 2 root root          4096 Mar 30 06:19 apps
drwxrwx---+ 4 root BUILTIN\administrators 4096 Mar 28 11:33 Policies
drwxrwx---+ 2 root BUILTIN\administrators 4096 Mar 28 11:33 scripts

(kali@dc1)-[~]
$
```

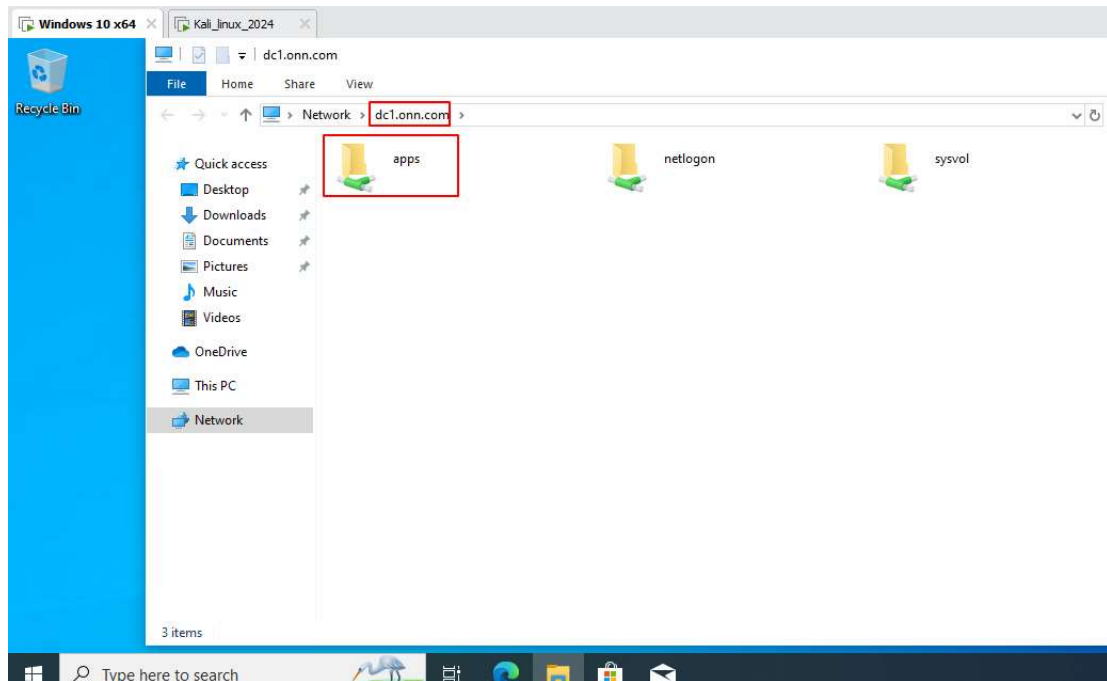
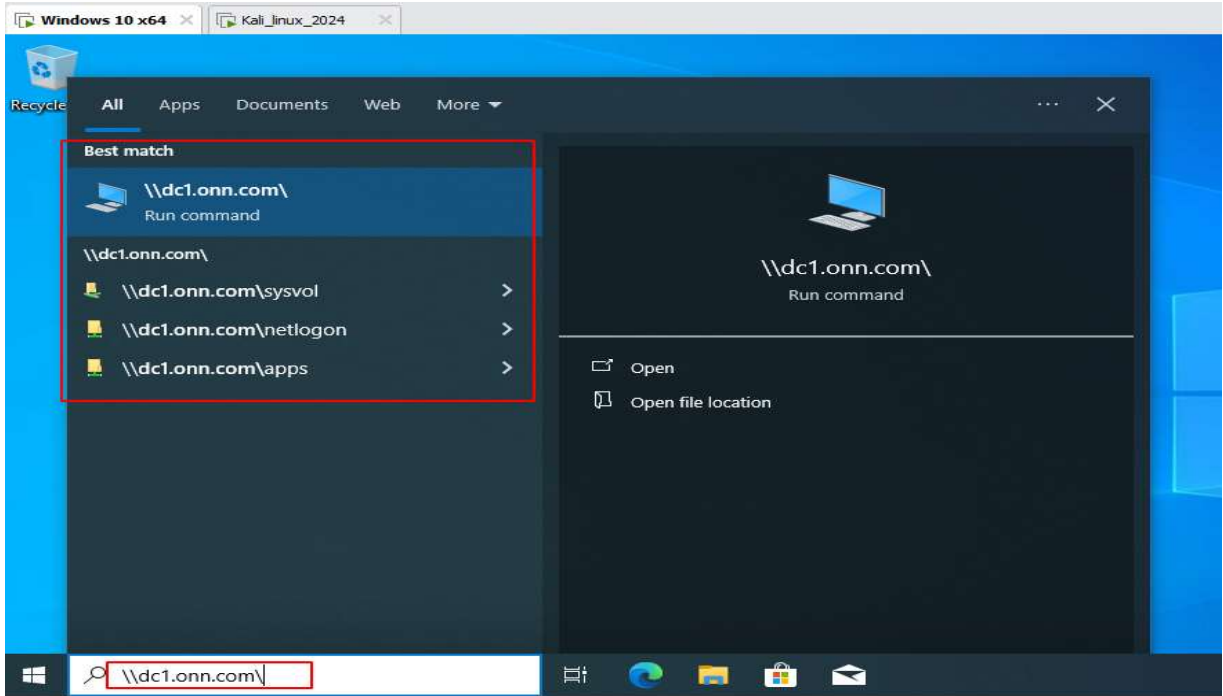
Kiểm tra trong Shared Folders đã được tạo.

| Console Root | | | | |
|-----------------------------------|--|--|--|--|
| Active Directory Users and Comput | | | | |
| Saved Queries | | | | |
| onn.com | | | | |
| Computer Management (DC1.ONN) | | | | |
| System Tools | | | | |
| Task Scheduler | | | | |
| Event Viewer | | | | |
| Shared Folders | | | | |
| Shares | | | | |
| Sessions | | | | |
| Open Files | | | | |
| Performance | | | | |
| Device Manager | | | | |
| Storage | | | | |
| Services and Applications | | | | |

| Share Name | Folder Path | Type | # Client Cor |
|------------|----------------------|---------|--------------|
| apps | C:\var\lib\samba\... | Windows | 0 |
| IPC\$ | C:\tmp | Windows | 1 |
| netlogon | C:\var\lib\samba\... | Windows | 0 |
| sysvol | C:\var\lib\samba\... | Windows | 0 |

Truy cập Shares Folders từ máy client:

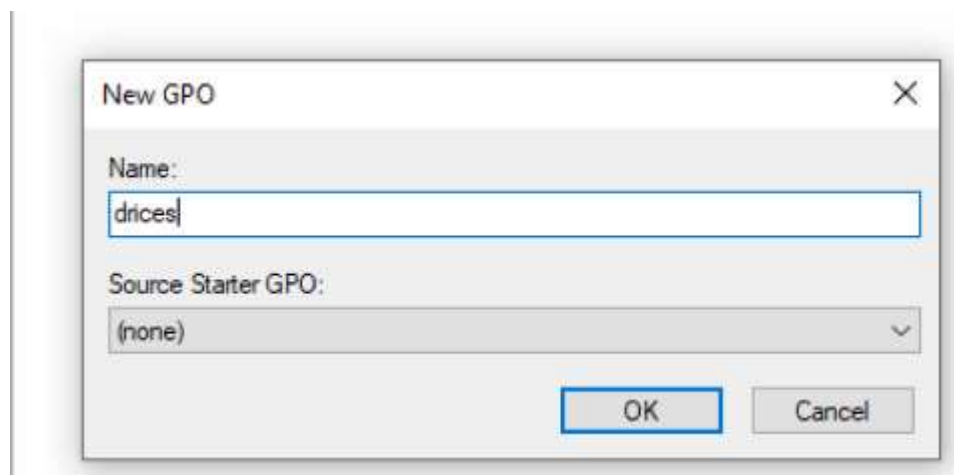
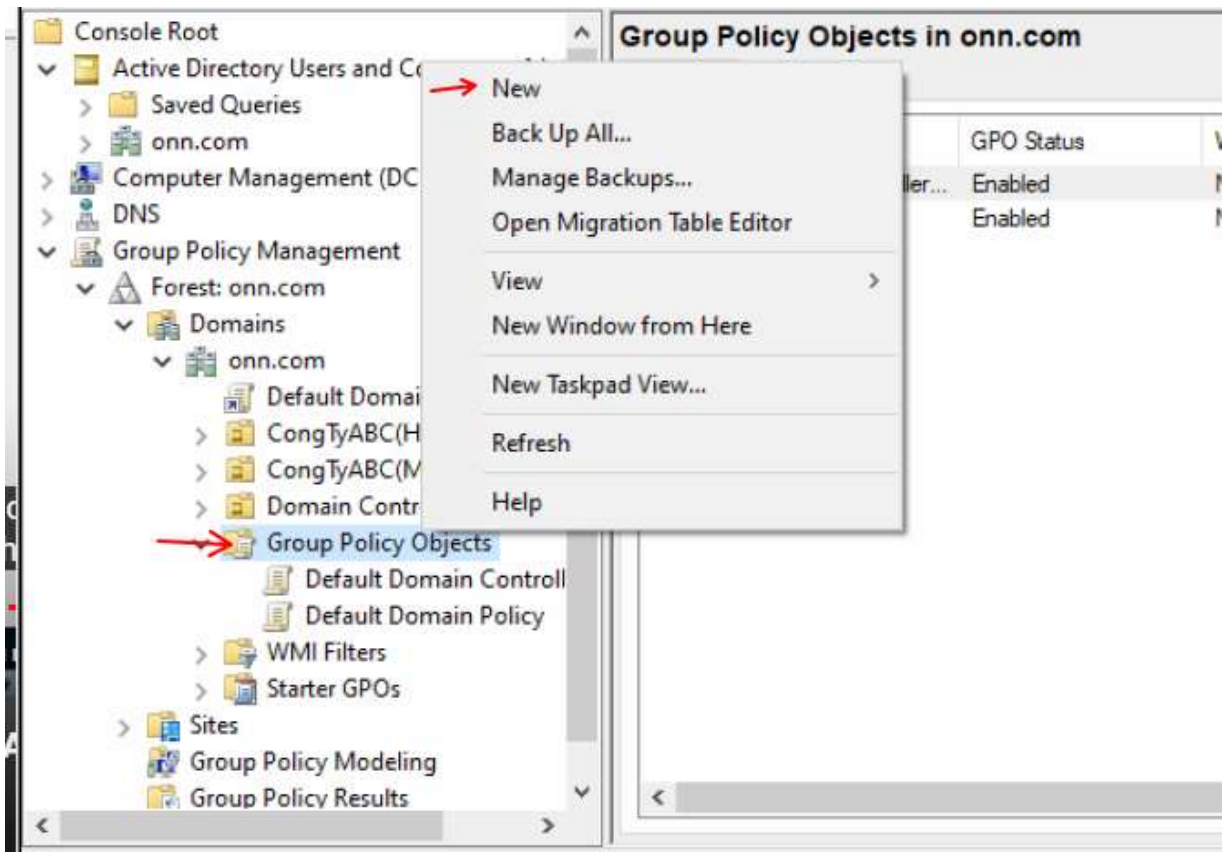
Tại thanh tìm kiếm : [\\tenmaychu\folders](https://tenmaychu.com/folders)



4.4 Chuyển hướng thư mục (Folder Redirection)

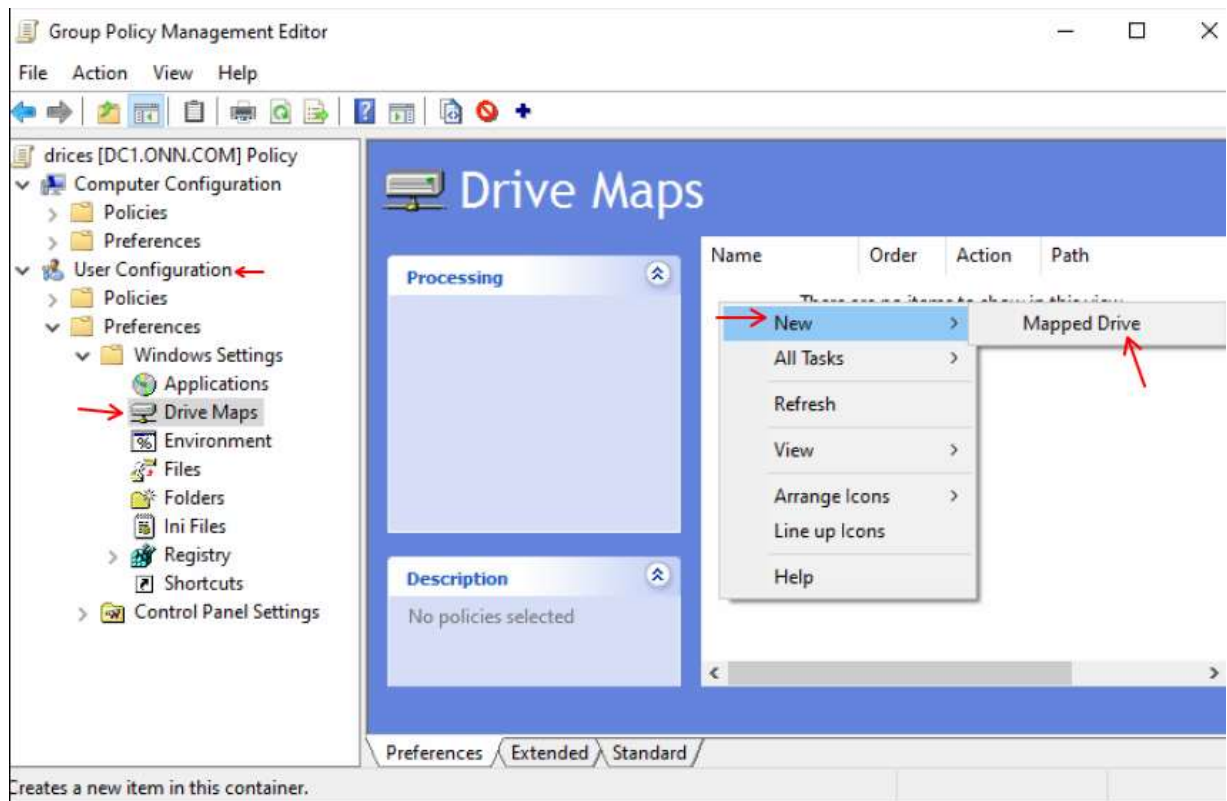
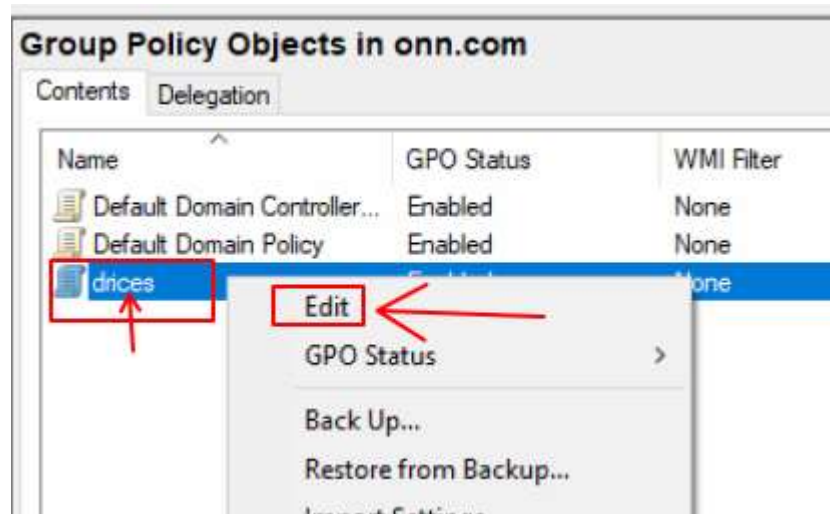
Tạo một policy ánh xạ ổ đĩa mạng.

Tạo Group pollicy > chuột phải > new > đặt tên cho policy.

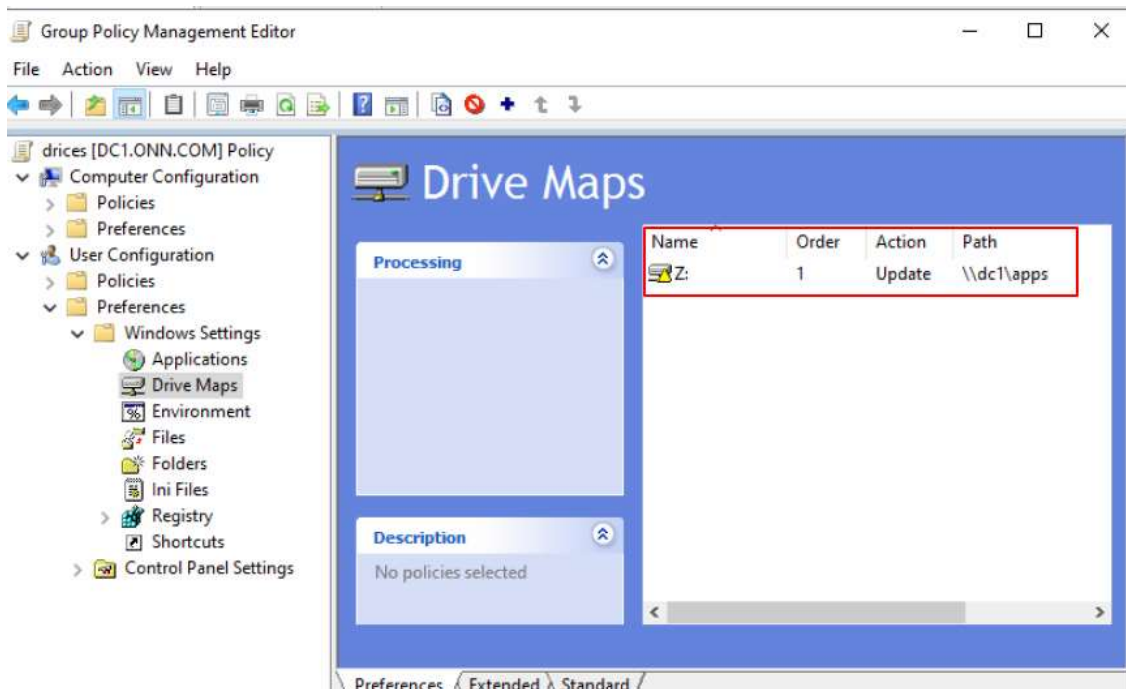
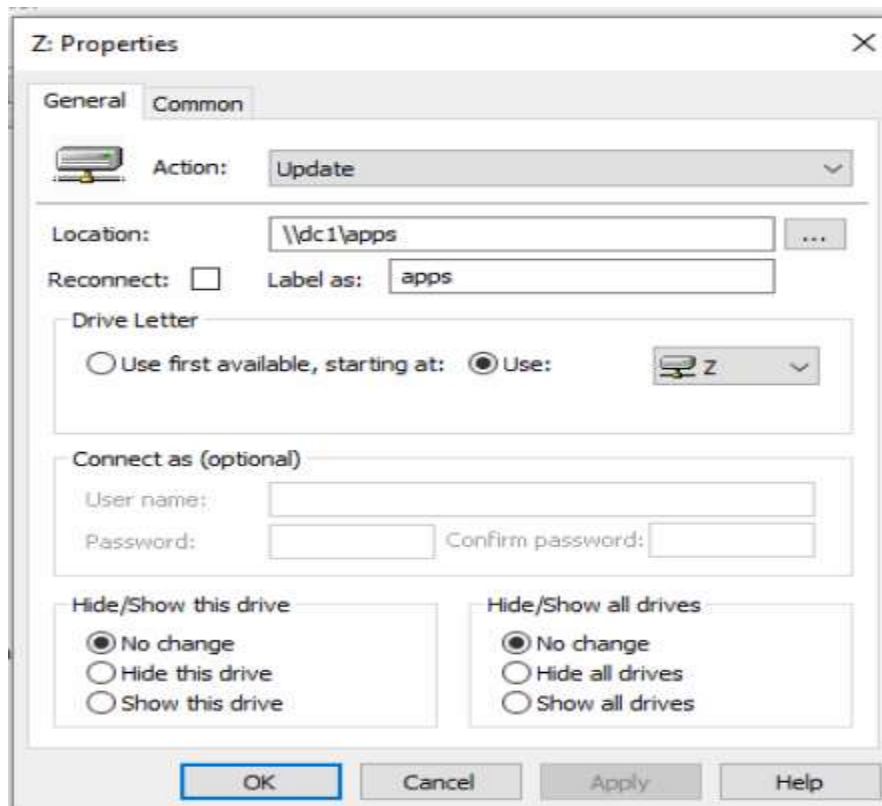


Sau khi tạo policy thành công > Edit để thiết lập policy

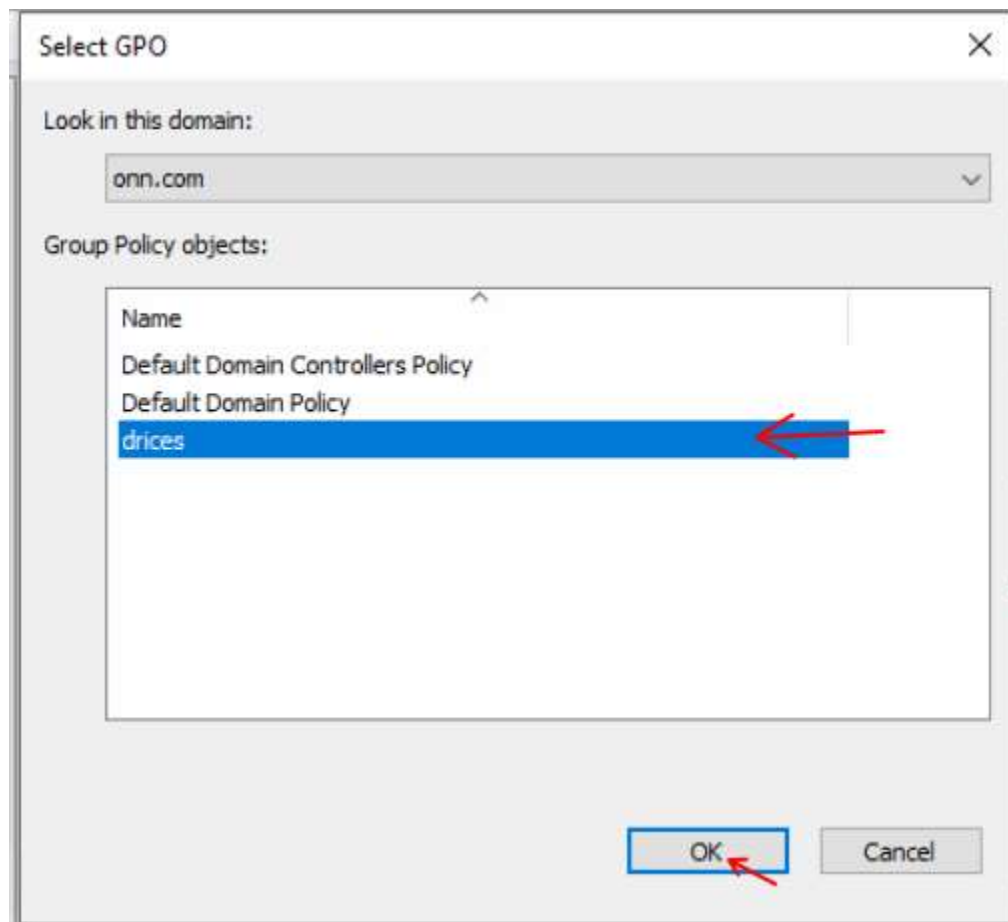
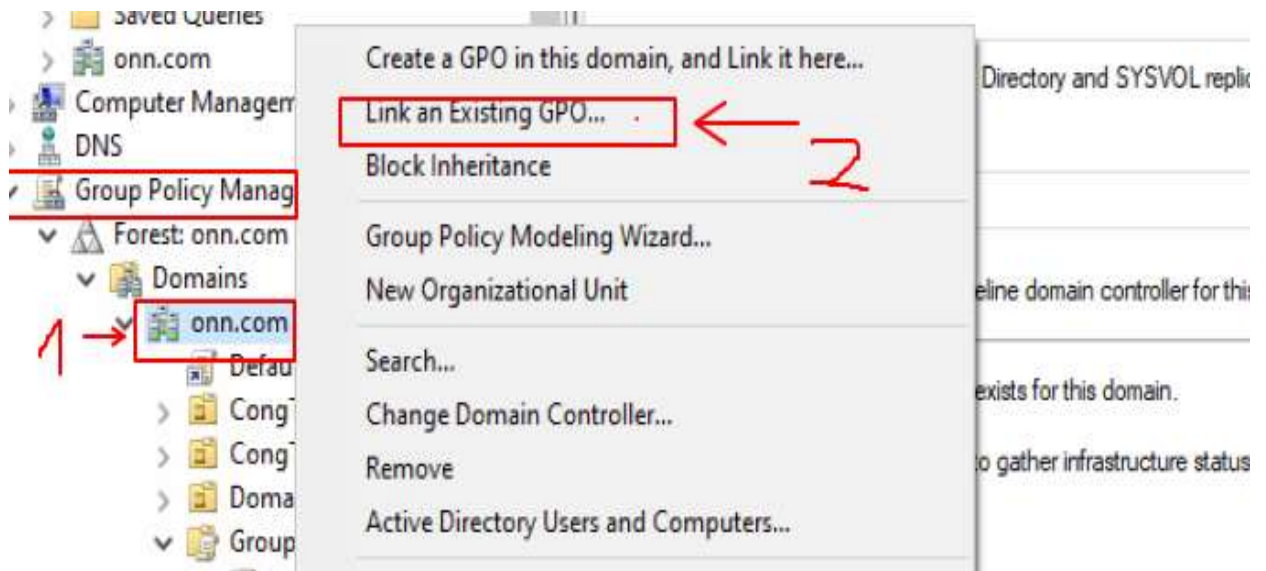
Tạo ổ đĩa Mapped drive



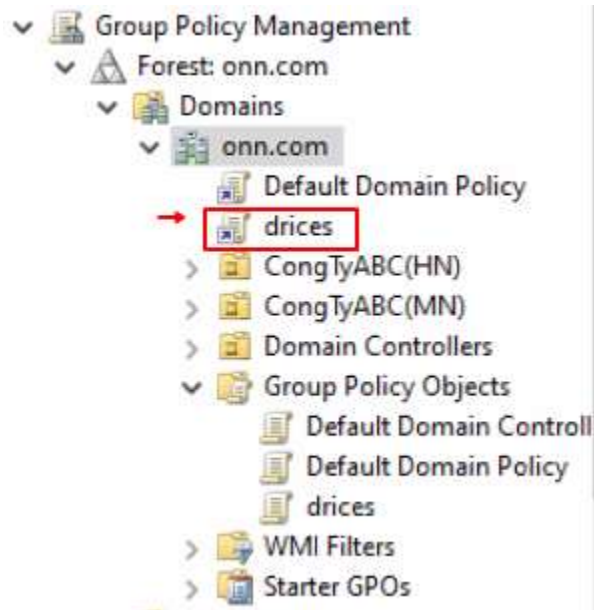
location : đường dẫn ánh xạ ổ đĩa server



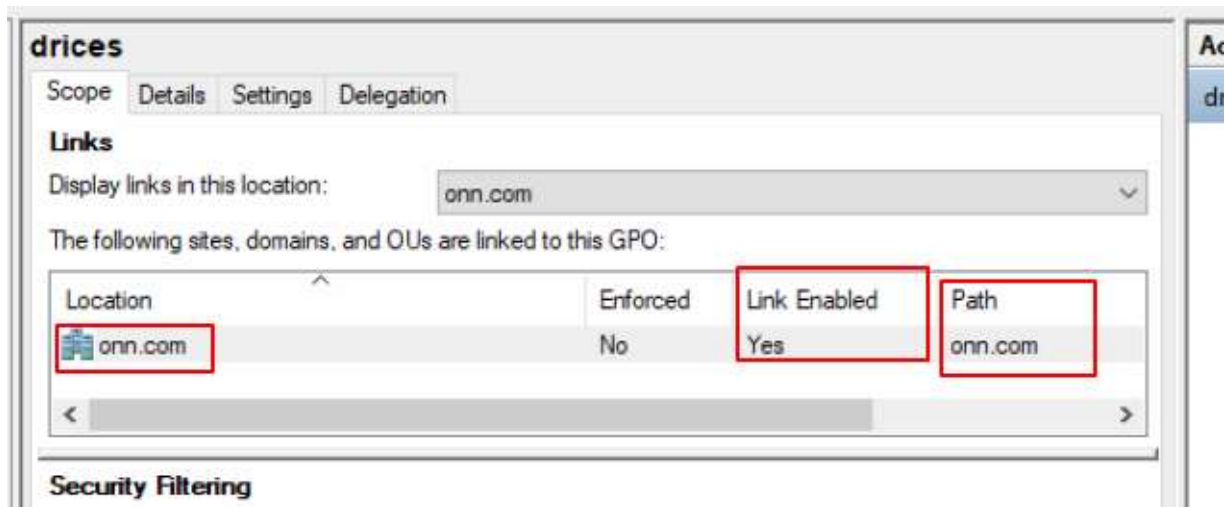
Tại domain > đúp chuột phải > Link an để thêm policy vào domain.



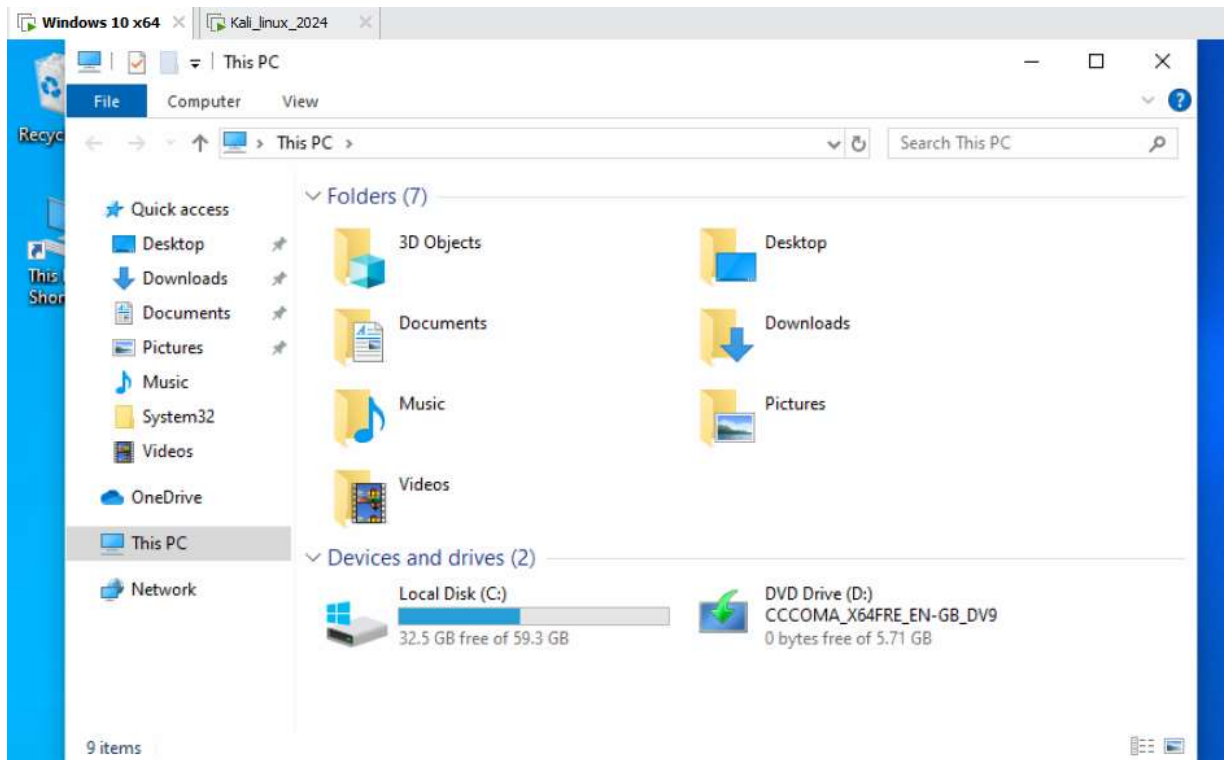
Policy đã được thêm vào



Kiểm tra trạng thái Policy trong domain.



Tại pc trong domain=> nhận thấy chưa thấy ổ đĩa được chia sẻ trong miền sau khi GPO.

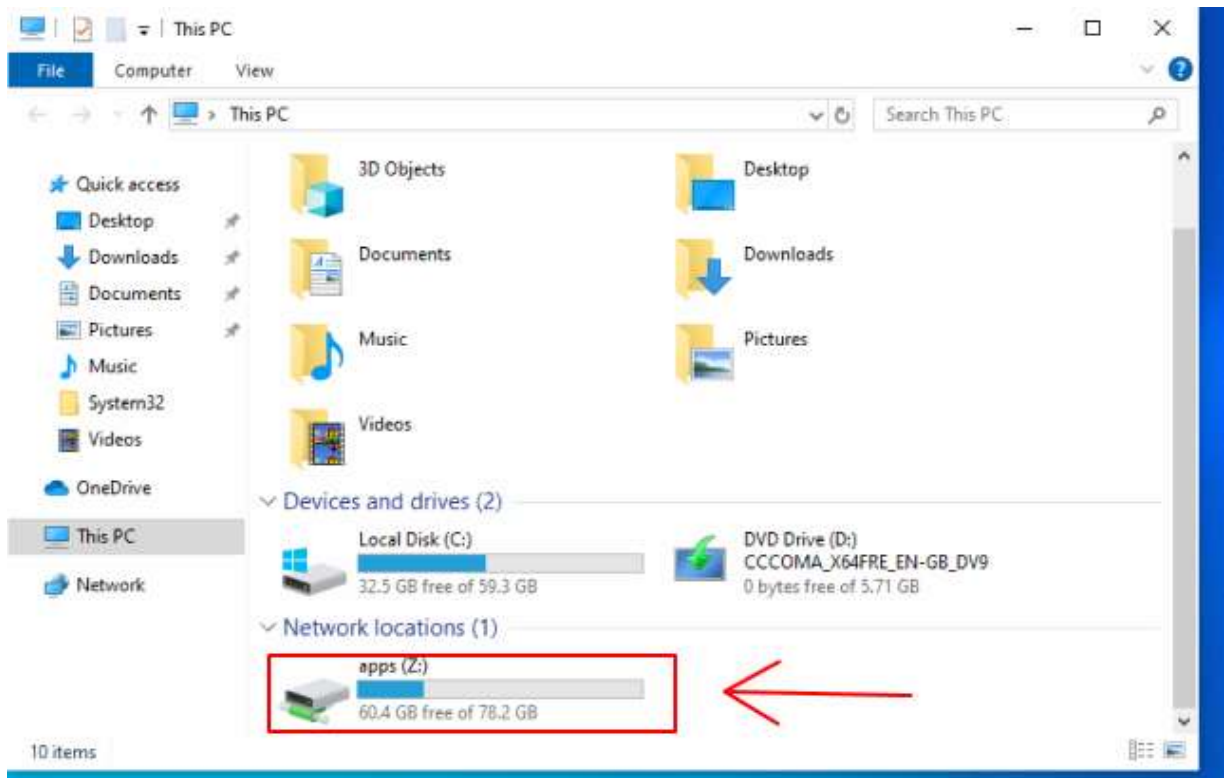


Nhập lệnh sau để cập nhật tất cả policy. Khi bạn chạy lệnh này, máy tính sẽ tải xuống và áp dụng lại tất cả các chính sách nhóm từ máy chủ Active Directory của mình.

```
C:\Users\Administrator>gpupdate /force
Updating policy...
```

Ổ đĩa ánh xạ đã xuất hiện.

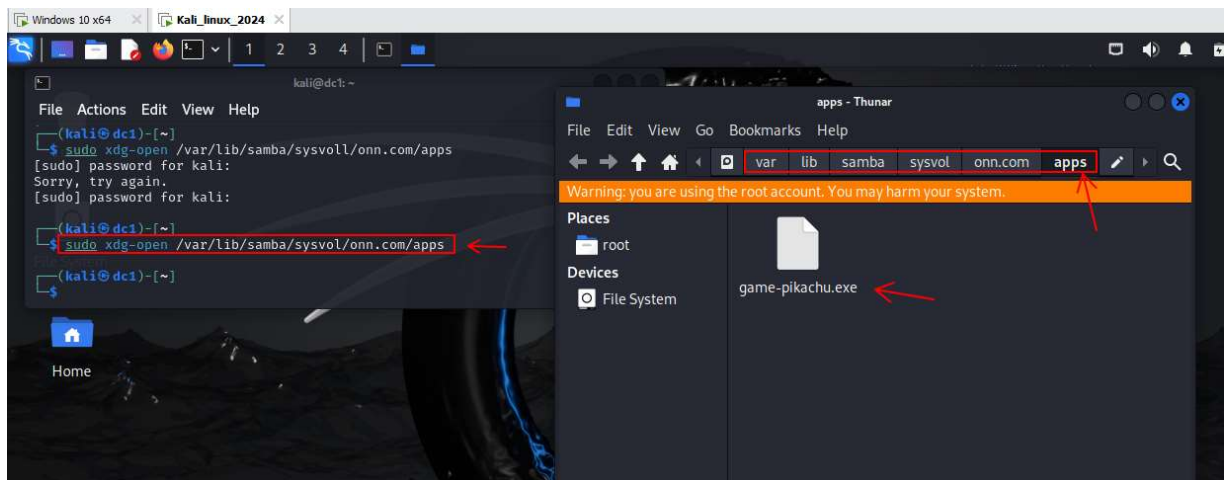
Khi được cấu hình, drive maps sẽ tự động ánh xạ các ổ đĩa mạng hoặc tài nguyên chia sẻ trên máy chủ file server vào các ổ đĩa cục bộ trên máy tính của người dùng. Điều này giúp người dùng truy cập vào các tệp và thư mục trên mạng một cách thuận tiện như thể chúng đang lưu trữ trên ổ đĩa cục bộ của họ.



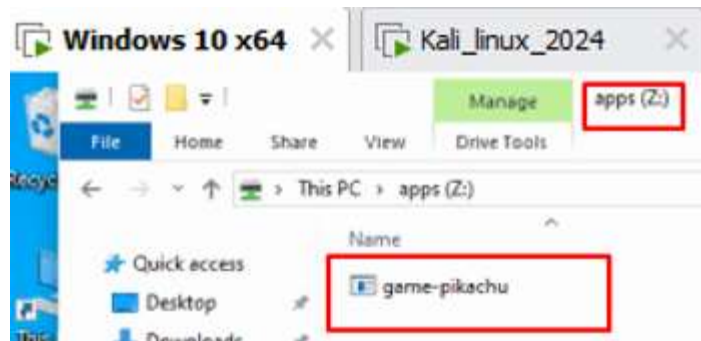
Ở phải máy chủ tôi đưa tệp file game pickachu vào thư mục apps

Dùng lệnh sau để mở trình gui thư mục thông qua terminal, sau đó đưa file vào.

```
sudo xdg-open /var/lib/samba/sysvol/onn.com/apps
```



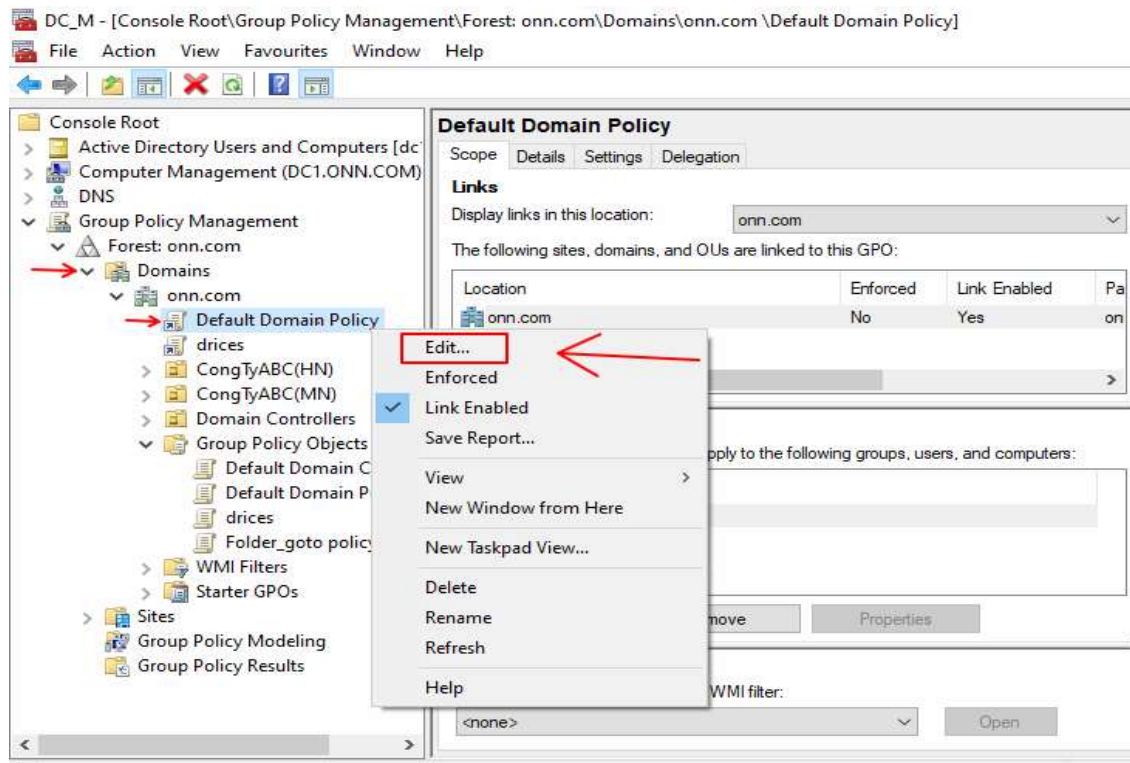
Ở pc > nhận thấy ánh xạ ổ đĩa thành công.



4.5 Policy mật khẩu mạnh.

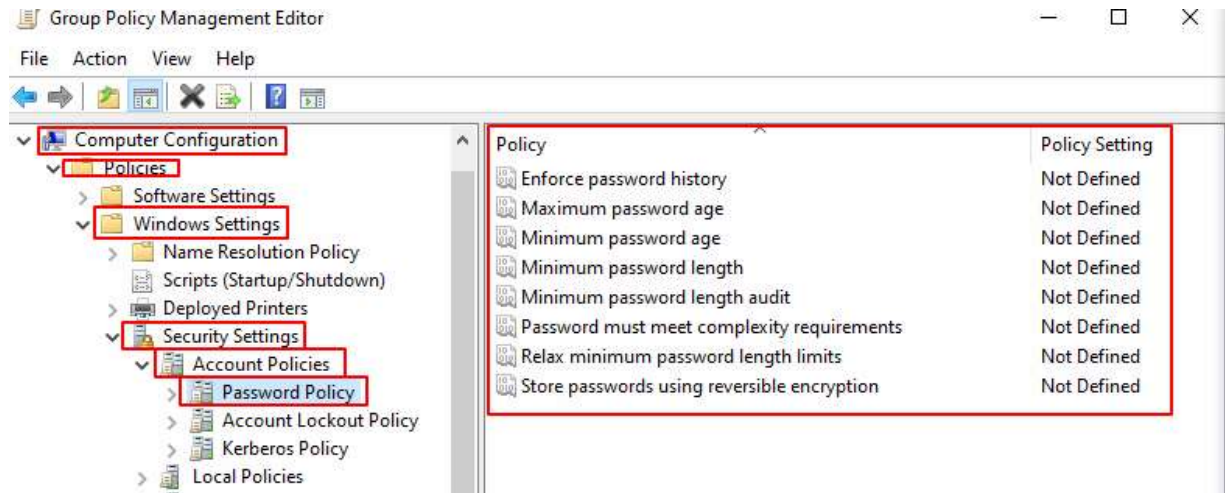
Để tăng tính bảo mật hệ thống một số yêu cầu về mật khẩu có thể đưa ra.

Thiết lập mật khẩu trong policy mặc định.



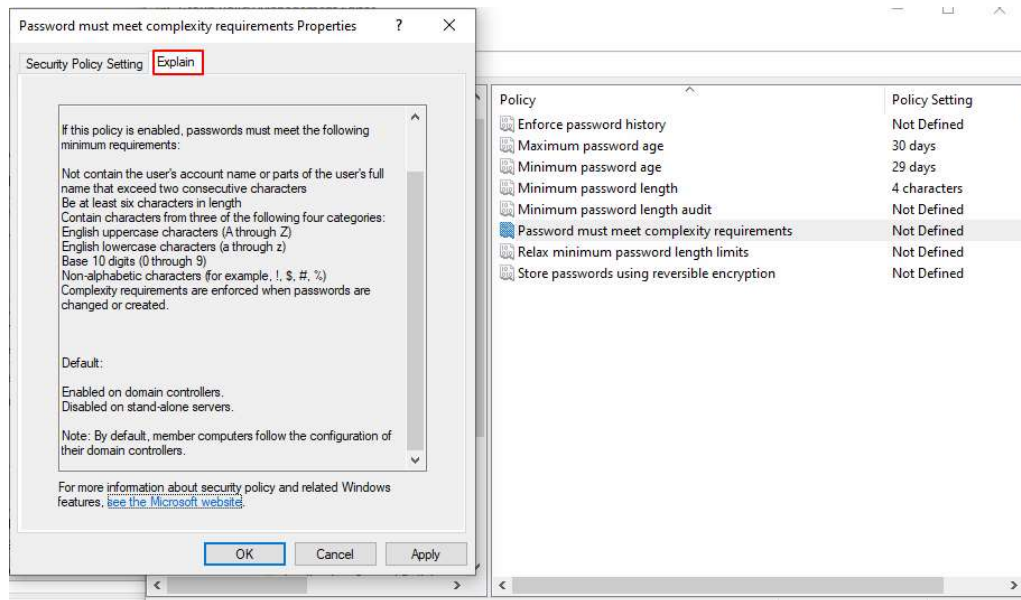
Chọn Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy.

Trong Password Policy có thể thiết lập policy cho các account.



Các tính năng có thể thiết lập như là : tuổi tối đa mật khẩu, tuổi mật khẩu tối thiểu, độ dài mật khẩu, yêu cầu về mật khẩu,... Ở đây tôi thiết lập khoảng thời gian mật khẩu tối đa là 30 ngày và mật khẩu tối thiểu 4 ký tự.

Mục Explain giải thích khi một chính sách được chọn.

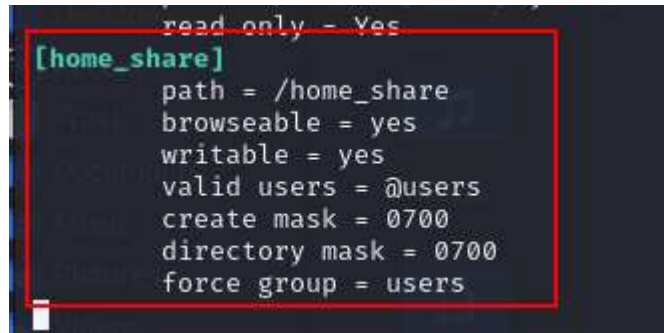


4.6 Tạo Home folders

tạo thư mục `home_share`

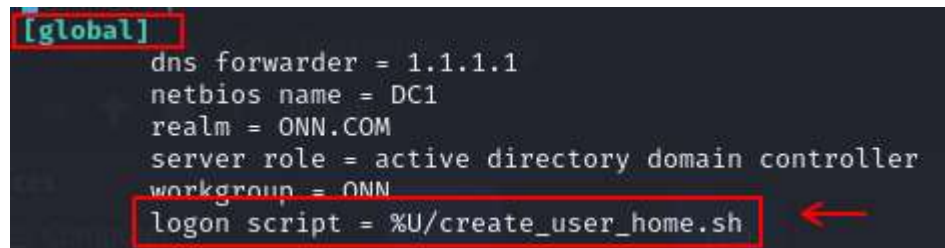
```
sudo mkdir /home_share
```

Chỉnh sửa cấu hình smb.conf : `sudo nano /etc/samba/smb.conf`



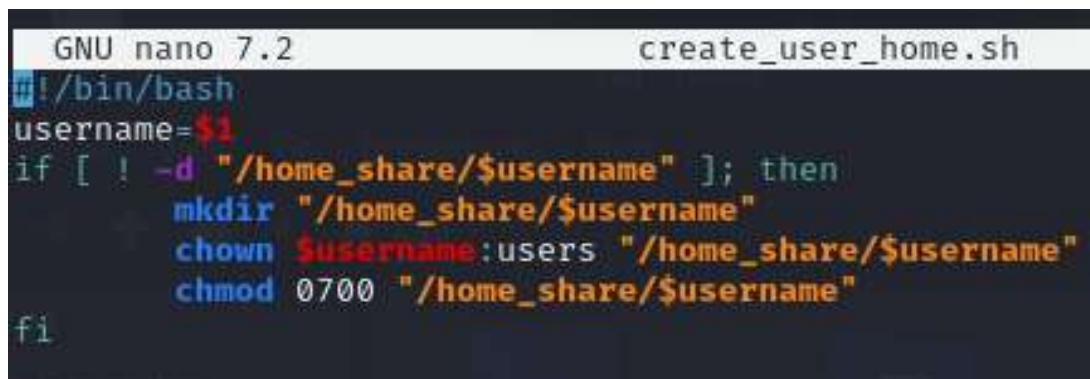
```
read only = Yes
[home_share]
path = /home_share
browseable = yes
writable = yes
valid users = @users
create mask = 0700
directory mask = 0700
force group = users
```

Thêm lệnh script sau vào [global] để tạo folder của user trên home_share.



```
[global]
dns forwarder = 1.1.1.1
netbios name = DC1
realm = ONN.COM
server role = active directory domain controller
workgroup = ONN
logon script = %U/create_user_home.sh
```

Tạo file script như sau:



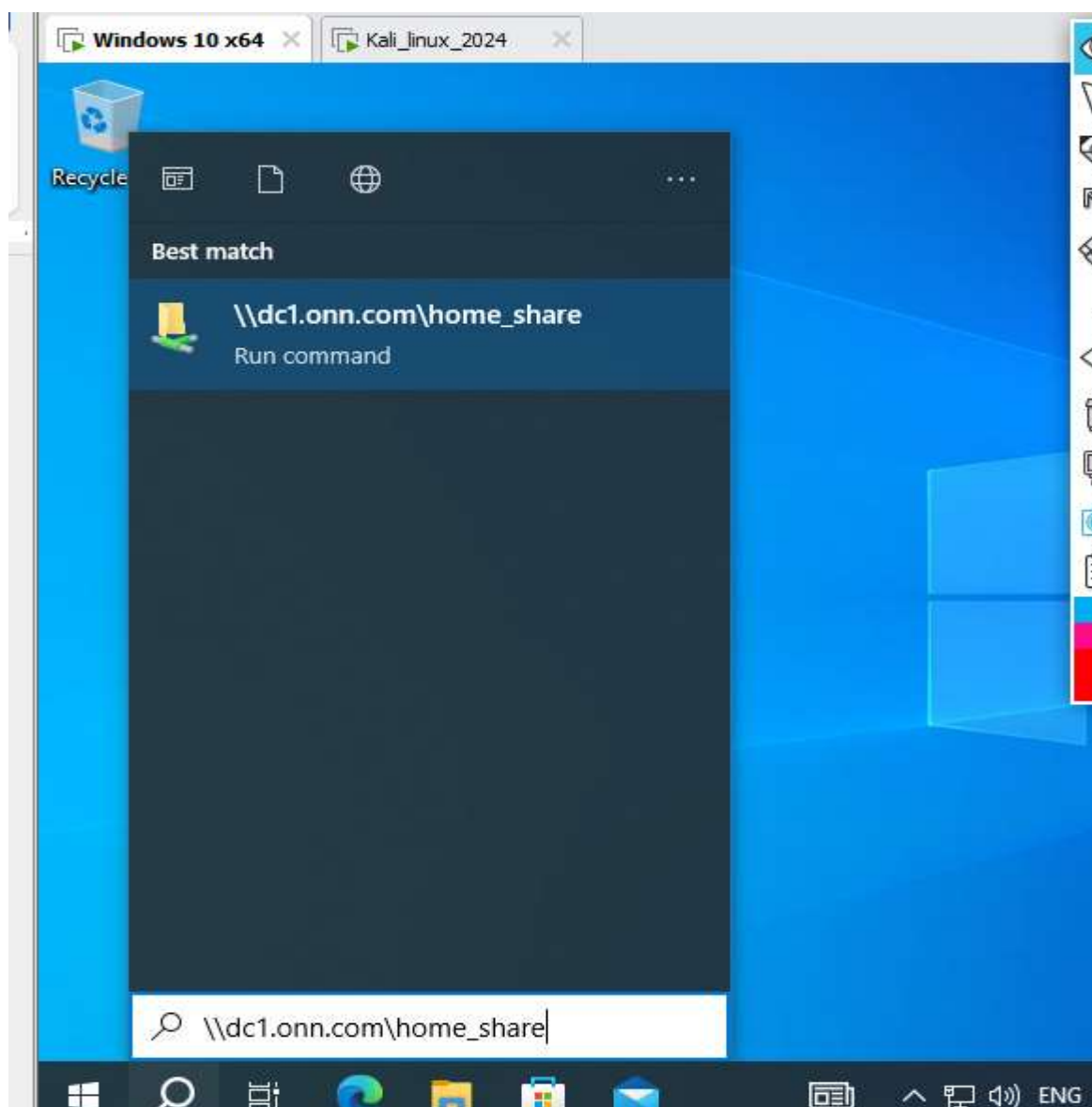
```
GNU nano 7.2 create_user_home.sh
#!/bin/bash
username=$1
if [ ! -d "/home_share/$username" ]; then
    mkdir "/home_share/$username"
    chown $username:users "/home_share/$username"
    chmod 0700 "/home_share/$username"
fi
```

Chạy lệnh `chmod +x` để cấp quyền thực thi.

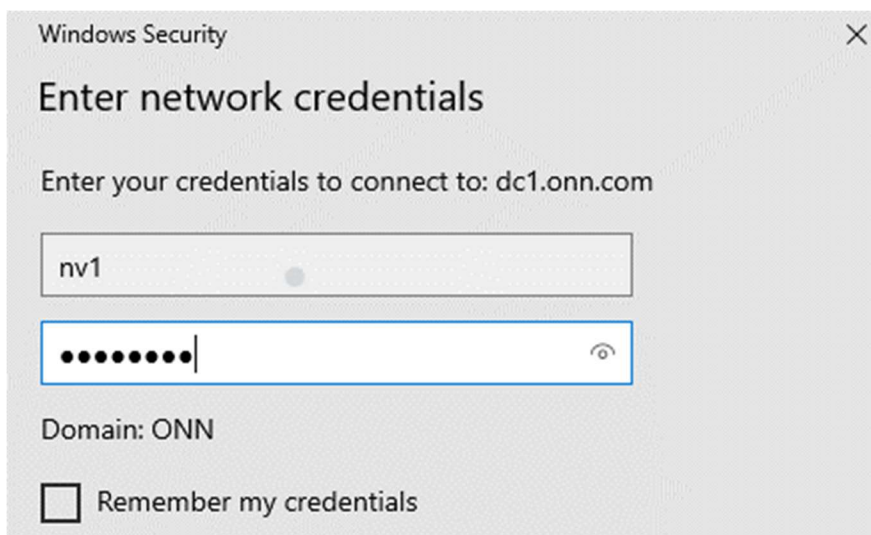
Khởi động lại dịch vụ lưu các thay đổi.

```
(kali@dc1)-[~]  
$ sudo systemctl restart smbd
```

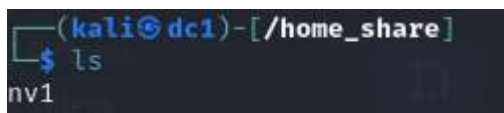
Đăng nhập vào máy client :



Điền credentials để kết nối.



Tại server kiểm tra thư mục đã được tạo tại Home_share.



KẾT LUẬN

Tóm tắt các kết quả đạt được từ việc triển khai Domain Controller trên Linux Server cho thấy sự tiềm năng và tính hiệu quả của giải pháp này. Bằng cách sử dụng Linux Server làm Domain Controller, tổ chức hoặc doanh nghiệp có thể tận dụng các tính năng mạnh mẽ của hệ điều hành mã nguồn mở này như tính linh hoạt, độ ổn định và tính bảo mật cao. Việc triển khai Domain Controller trên Linux Server cũng mở ra cơ hội cho việc sử dụng các ứng dụng và công nghệ mới như LDAP, Samba, và Kerberos, giúp tăng cường tính linh hoạt và khả năng tương thích trong môi trường mạng.

Đánh giá ưu điểm và nhược điểm khi triển khai trên Linux Server cho thấy sự cân nhắc cần thiết giữa các lợi ích và khó khăn. Ưu điểm của việc sử dụng Linux Server bao gồm chi phí thấp, tính linh hoạt cao, và khả năng tùy chỉnh linh hoạt. Tuy nhiên, cần phải nhận ra rằng triển khai Domain Controller trên Linux Server có thể đòi hỏi kiến thức kỹ thuật sâu về hệ thống và mạng, cũng như đòi hỏi thời gian và tài nguyên để triển khai và duy trì hệ thống.

Đề xuất hướng phát triển và nghiên cứu trong tương lai có thể bao gồm việc tối ưu hóa các quy trình triển khai và quản lý hệ thống, phát triển các công cụ và giao diện người dùng đơn giản hóa, cũng như nghiên cứu và áp dụng các công nghệ mới để cải thiện tính bảo mật và khả năng mở rộng của hệ thống. Ngoài ra, việc nghiên cứu và phát triển các giải pháp tích hợp sẽ giúp tối ưu hóa hiệu suất và sự linh hoạt của hệ thống Domain Controller trên Linux Server, giúp đẩy mạnh sự phát triển và ứng dụng của giải pháp này trong các tổ chức và doanh nghiệp.

TÀI LIỆU THAM KHẢO

- Arvid Larson. (2022, February 08). *adamtheautomator.com*. Retrieved from How to Perform a Samba Active Directory Install on Linux: <https://adamtheautomator.com/samba-active-directory/>
- Dang Trung. (n.d.). *www.scribd.com*. Retrieved from Đặc Điểm Của Hệ Điều Hành Linux: <https://www.scribd.com/doc/76921807>
- Linh, N. (2023, 12 03). *vinahost.vn*. Retrieved from Cách hoạt động & chức năng của Domain Controller: <https://vinahost.vn/domain-controller-la-gi/>
- tenten. (2022, 03 01). *tenten.vn*. Retrieved from Tổng Quan cơ bản về domain Controller: <https://tenten.vn/tin-tuc/domain-controller-la-gi>