**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

Logo, company name

Description automatically generated**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

**PHAN VĂN SƠN**

**MSV : 1571020226**

**TRIỂN KHAI HỆ THỐNG QUẢN TRỊ NGƯỜI DÙNG VÀ KIỂM SOÁT TRUY CẬP MẠNG DOANH NGHIỆP VỚI ACTIVE DIRECTORY CHO CÔNG TY CPTM XUẤT NHẬP KHẨU HPC**

**BÁO CÁO ĐỒ ÁN TỐT NGHIỆP**

**NGÀNH : CÔNG NGHỆ THÔNG TIN**

**HÀ NỘI, NĂM 2025**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

Logo, company name

Description automatically generated**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

**PHAN VĂN SƠN**

**MSV:1571020226, KHÓA 15**

**TRIỂN KHAI HỆ THỐNG QUẢN TRỊ NGƯỜI DÙNG VÀ KIỂM SOÁT TRUY CẬP MẠNG DOANH NGHIỆP VỚI ACTIVE DIRECTORY CHO CÔNG TY CPTM XUẤT NHẬP KHẨU HPC**

**BÁO CÁO ĐỒ ÁN TỐT NGHIỆP**

**NGÀNH : CÔNG NGHỆ THÔNG TIN**

**GIẢNG VIÊN HƯỚNG DẪN: Th.S LÊ VĂN PHONG**

**HÀ NỘI, NĂM 2025**

LỜI CAM ĐOAN

Em Phan Văn Sơn, dưới đây xin ký tên xác nhận rằng toàn bộ nội dung báo cáo và mã nguồn trong xây dựng đồ án tốt nghiệp đề tài: “Triển khai hệ thống quản trị người dùng và kiểm soát truy cập mạng doanh nghiệp với Active Directory cho Công ty CPTM Xuất nhập khẩu HPC” là kết quả nghiên cứu và làm việc độc lập của em.

Em cũng xin cam kết rằng không có sự sao chép hay lạm dụng tài nguyên từ nguồn nào khác mà không được chỉ rõ. Mọi tài liệu tham khảo của bên thứ ba đều được em trích dẫn đầy đủ.

Trong quá trình xây dựng bài toán, em đã tự tin với sự hiểu biết và kỹ năng của mình. Khi thử sức với những điều mới trong học tập thì mọi quyết định và lựa chọn thiết kế đều dựa trên kiến thức và kinh nghiệm của em trong lĩnh vực này.

Hy vọng rằng chương trình này sẽ mang lại giá trị và tiện ích cho người sử dụng và là một bước tiến quan trọng trong sự phát triển cá nhân và chuyên môn của em.

Ngày tháng năm 2025

LỜI CẢM ƠN

Trước tiên, em xin gửi lời cảm ơn sâu sắc đến thầy Lê Văn Phong đã tận tình hướng dẫn, chỉ bảo em trong suốt quá trình thực hiện đồ án tốt nghiệp. Thầy không chỉ giúp em định hướng đúng đắn mà còn hỗ trợ, góp ý để em hoàn thành tốt bài làm của mình.

Em cũng xin chân thành cảm ơn quý thầy cô trong khoa Công nghệ thông tin, Trường Đại học Đại Nam đã giảng dạy, truyền đạt kiến thức, tạo điều kiện thuận lợi giúp em có nền tảng vững chắc để thực hiện đồ án này. Đồng thời, em cảm ơn nhà trường đã hỗ trợ về cơ sở vật chất, tài liệu và môi trường học tập tốt nhất.

Bên cạnh đó, em xin gửi lời cảm ơn đến Công ty CPTM Xuất nhập khẩu HPC, nơi đã tạo điều kiện để em có cơ hội tiếp cận thực tế, áp dụng kiến thức vào triển khai hệ thống, từ đó rút ra những bài học kinh nghiệm quý báu.

Cuối cùng, em xin gửi lời cảm ơn chân thành đến gia đình và bạn bè, những người luôn đồng hành, động viên và hỗ trợ em trong suốt quá trình học tập cũng như thực hiện đồ án này.

Em xin chân thành cảm ơn!

DANH MỤC KÝ HIỆU VÀ TỪ NGỮ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **Ký hiệu chữ viết tắt** | **Chữ viết tắt đầy đủ** |
| 1 | AD | Active Directory |
| 2 | AD DS | Active Directory Domain Services |
| 3 | OU | Organizational Unit |
| 4 | GPO | Group Policy Object |
| 5 | DNS | Domain Name System |
| 6 | DC | Domain Controller |
| 7 | PDC | Primary Domain Controller |
| 8 | FSMO | Flexible Single Master Operations |
| 9 | GC | Global Catalog |
| 10 | GCS | Global Catalog Server |
| 11 | SSO | Single Sign-On |
| 12 | IP | Internet Protocol |
| 13 | VM | Virtual Machine |
| 14 | MFA | Multi-Factor Authentication |
| 15 | SID | Security Identifier |
| 16 | RDN | Relative Distinguished Name |
| 17 | DN | Distinguished Name |
| 18 | TPM | Trusted Platform Module |
| 19 | UPS | Uninterruptible Power Supply |
| 20 | ERP | Enterprise Resource Planning |
| 21 | WAN | Wide Area Network |
| 22 | LAN | Local Area Network |
| 23 | ADC | Additional Domain Controller |

# **DANH MỤC HÌNH ẢNH**

[Hình 1.1: Active Directory 7](#_Toc199690913)

[Hình 1.2 : Directory Service 9](#_Toc199690914)

[Hình 1.3: Global Catalog Server 10](#_Toc199690915)

[Hình 1.4: Cơ chế Single Sign-on 12](#_Toc199690916)

[Hình 2.1: Cấu trúc Tổ chức trong Active Directory 19](#_Toc199690917)

[Hình 3.1: Cấu hình ổ cứng 27](#_Toc199690918)

[Hình 3.2: Cấu hình Ram 28](#_Toc199690919)

[Hình 3.3: Thiết lập tài khoản quản trị viên 28](#_Toc199690920)

[Hình 3.4: Cấu hình DNS 29](#_Toc199690921)

[Hình 3.5: Tạo tên miền 30](#_Toc199690922)

[Hình 3.6: Cấu hình Domain Controller 31](#_Toc199690923)

[Hình 3.7: Tạo các OU 32](#_Toc199690924)

[Hình 3.8: Kiểm tra zone 33](#_Toc199690925)

[Hình 3.9: Cấu hình New Host 33](#_Toc199690926)

[Hình 3.10:Cấu hình Website 35](#_Toc199690927)

[Hình 3.11:Kết quả hoạt động Web Server 35](#_Toc199690928)

[Hình 3.12:Mở Group Policy Management 37](#_Toc199690929)

[Hình 3.13:Password and Account Security Policy 37](#_Toc199690930)

[Hình 3.14:Cấu hình chính sách mật khẩu 39](#_Toc199690931)

[Hình 3.15:Cấu hình chính sách khóa tài khoản 39](#_Toc199690932)

[Hình 3.16:USB and software Restriction Policy 40](#_Toc199690933)

[Hình 3.17:Thiết lập All Removable Storage classes 41](#_Toc199690934)

[Hình 3.18: Hoàn tất thiết lập All Removable Storage classes 41](#_Toc199690935)

[Hình 3.19: Phân quyền truy cập Web Server IIS 43](#_Toc199690936)

[Hình 3.20:Tạo người dùng mới 46](#_Toc199690937)

[Hình 3.21:Tạo và nối máy trạm 47](#_Toc199690938)

[Hình 3.22:Kiểm tra xác minh 47](#_Toc199690939)

[Hình 3.23:Cấp quyền thích hợp 48](#_Toc199690940)

[Hình 3.24:Client truy cập thư mục chia sẻ 49](#_Toc199690941)

[Hình 3.25:Kiểm tra chính sách mật khẩu 50](#_Toc199690942)

[Hình 3.26:Kiểm tra cấm sử dụng USB 50](#_Toc199690943)

[Hình 3.27:Kiểm tra truy cập trang web sau khi phân quyền 51](#_Toc199690944)

[Hình 3.28:Kiểm tra theo dõi hoạt động 52](#_Toc199690945)

DANH MỤC BẢNG BIỂU

[Bảng 1.1: Danh mục các thiết bị 13](#_Toc199680361)

[Bảng 2.1: Bảng Mô hình các miền con 17](#_Toc199680362)

[Bảng 2.2: Bảng thiết kế sơ đồ tổ chức 23](#_Toc199680363)

[Bảng 2.4: Bảng thu hoạch IP chi tiết 25](#_Toc199680364)

**MỤC LỤC**

[LỜI CAM ĐOAN i](#_Toc200487463)

[LỜI CẢM ƠN ii](#_Toc200487464)

[DANH MỤC KÝ HIỆU VÀ TỪ NGỮ VIẾT TẮT iii](#_Toc200487465)

[DANH MỤC HÌNH ẢNH iv](#_Toc200487466)

[DANH MỤC BẢNG BIỂU vi](#_Toc200487467)

[LỜI MỞ ĐẦU 1](#_Toc200487468)

[1. Giới thiệu đề tài 1](#_Toc200487469)

[2. Lý do chọn đề tài 1](#_Toc200487470)

[3. Mục đích nghiên cứu 2](#_Toc200487471)

[4. Phương pháp nghiên cứu 3](#_Toc200487472)

[5. Phạm vi nghiên cứu 3](#_Toc200487473)

[6. Kết cấu của đồ án 3](#_Toc200487474)

[CHƯƠNG 1: CƠ SỞ LÝ THUYẾT 5](#_Toc200487475)

[1.1 Giới thiệu về Active Directory (AD) 5](#_Toc200487476)

[1.2 Chức năng của Active Directory 5](#_Toc200487477)

[1.3 Cấu trúc Active Directory 7](#_Toc200487478)

[1.3.1 Cấu trúc logic 7](#_Toc200487479)

[1.3.2 Cấu trúc vật lý 8](#_Toc200487480)

[1.4. Cơ chế hoạt động Active Directory 8](#_Toc200487481)

[1.4.1 Directory Service 8](#_Toc200487482)

[1.4.2 Active Directory Schema 9](#_Toc200487483)

[1.4.3 Global Catalog 10](#_Toc200487484)

[1.4.4 Global Catalog Server 10](#_Toc200487485)

[1.4.5 Distinguished và Relative Distinguished Name 11](#_Toc200487486)

[1.4.6 Cơ chế Single Sign-on 11](#_Toc200487487)

[1.2 Giới thiệu về Công ty CPTM Xuất nhập khẩu HPC 12](#_Toc200487488)

[1.2.1 Khảo sát yêu cầu thực trạng 12](#_Toc200487489)

[1.2.2 Danh mục các thiết bị 13](#_Toc200487490)

[CHƯƠNG 2: PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG QUẢN TRỊ 17](#_Toc200487491)

[NGƯỜI DÙNG VỚI ACTIVE DIRECTORY 17](#_Toc200487492)

[2.1 Thiết kế mô hình hệ thống Active Directory 17](#_Toc200487493)

[2.1.1 Mô hình Tổng quan Active Directory 17](#_Toc200487494)

[2.2.2 Cấu trúc Tổ chức trong Active Directory 18](#_Toc200487495)

[2.2.3 Phân cấp Domain Controller (DC) 20](#_Toc200487496)

[2.2 Lập kế hoạch triển khai tài khoản người dùng, nhóm và máy tính 22](#_Toc200487497)

[2.2.1 Lập bảng thiết kế sơ đồ tổ chức 22](#_Toc200487498)

[2.2.2 Bảng thu hoạch IP 24](#_Toc200487499)

[CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG ACTIVE DIRECTORY 27](#_Toc200487500)

[3.1 Triển khai Forest và Domain 27](#_Toc200487501)

[3.1.1 Cài đặt Windows Server trên môi trường ảo hóa VMware 27](#_Toc200487502)

[3.1.2 Cấu hình địa chỉ IP tĩnh cho máy chủ 28](#_Toc200487503)

[3.1.3 Cài đặt dịch vụ Active Directory Domain Services (AD DS) 29](#_Toc200487504)

[3.1.4 Thăng cấp máy chủ thành Domain Controller 30](#_Toc200487505)

[3.2 Cấu hình Organizational Unit (OU) 31](#_Toc200487506)

[3.2.1 Mở công cụ Active Directory Users and Computers 31](#_Toc200487507)

[3.2.2 Tạo OU chính và các OU con 31](#_Toc200487508)

[3.3 Tích hợp Domain Name System (DNS) vào Active Directory 32](#_Toc200487509)

[3.3.1 Kiểm tra Forward Lookup Zones 32](#_Toc200487510)

[3.3.2 Thêm bản ghi Host (A Record) 33](#_Toc200487511)

[3.4 Cấu hình IIS Web Server (HTTP và HTTPS) trên Windows Server 2016 34](#_Toc200487512)

[3.4.1 Cài đặt dịch vụ IIS 34](#_Toc200487513)

[3.4.2 Tạo Website với giao thức HTTP 34](#_Toc200487514)

[3.4.3 Kiểm tra hoạt động Web Server 35](#_Toc200487515)

[3.5 Chính sách bảo mật 36](#_Toc200487516)

[3.5.1 Mở Group Policy Management 36](#_Toc200487517)

[3.5.2 Cấu hình chính sách mật khẩu 38](#_Toc200487518)

[3.5.3 Cập nhật chính sách 39](#_Toc200487519)

[3.5.4 Cấm sử dụng USB 39](#_Toc200487520)

[3.5.5 Cấu hình xác thực và phân quyền truy cập Web Server IIS 42](#_Toc200487521)

[3.5.6 Theo dõi hoạt động hệ thống (Audit Logs) 43](#_Toc200487522)

[3.5.7 Rủi ro khi không triển khai chính sách chặt chẽ 45](#_Toc200487523)

[3.6 Kết quả sau khi tạo thành công chính sách bảo mật mật khẩu và nối máy client vào domain hpc.com.vn 46](#_Toc200487524)

[3.6.1 Tạo người dùng mới trên Domain Controller 46](#_Toc200487525)

[3.6.2 Tạo và nối máy trạm (client) vào domain hpc.com.vn 47](#_Toc200487526)

[3.6.3 Chia sẻ file giữa máy chủ với client 48](#_Toc200487527)

[3.6.4 Kiểm tra chính sách mật khẩu 50](#_Toc200487528)

[3.6.5 Kiểm tra cấm sử dụng USB 51](#_Toc200487529)

[3.6.6 Kiểm tra truy cập trang web sau khi phân quyền 51](#_Toc200487530)

[3.6.7 Kiểm tra theo dõi hoạt động – Xem nhật ký trong Event Viewer 52](#_Toc200487531)

[KẾT LUẬN 54](#_Toc200487532)

[DANH MỤC TÀI LIỆU THAM KHẢO 56](#_Toc200487533)

LỜI MỞ ĐẦU

1. Giới thiệu đề tài

Trong bối cảnh chuyển đổi số mạnh mẽ, việc quản lý người dùng và kiểm soát truy cập mạng đóng vai trò quan trọng trong việc bảo vệ an toàn thông tin và nâng cao hiệu suất hoạt động doanh nghiệp. Khi quy mô doanh nghiệp ngày càng mở rộng, hệ thống mạng trở nên phức tạp hơn, kéo theo những thách thức về quản trị, bảo mật và phân quyền truy cập. Nếu không có một giải pháp quản lý tập trung, doanh nghiệp có thể đối mặt với nguy cơ rò rỉ dữ liệu, truy cập trái phép hoặc gián đoạn hệ thống, ảnh hưởng trực tiếp đến hoạt động kinh doanh.

Công ty CPTM Xuất nhập khẩu HPC, với tốc độ phát triển nhanh, cũng không nằm ngoài những thách thức trên. Việc triển khai một hệ thống quản trị người dùng hiệu quả không chỉ giúp tối ưu hóa công tác quản lý nhân sự mà còn đảm bảo quyền truy cập được kiểm soát chặt chẽ, giảm thiểu rủi ro bảo mật và nâng cao tính linh hoạt trong vận hành.

Hệ thống Active Directory mang lại giải pháp quản lý tập trung, cho phép doanh nghiệp thiết lập các chính sách bảo mật mạnh mẽ, quản lý quyền truy cập một cách hiệu quả, đồng thời hỗ trợ tự động hóa nhiều quy trình quản trị CNTT. Ngoài ra, việc áp dụng Active Directory còn giúp doanh nghiệp tuân thủ các tiêu chuẩn an toàn thông tin, nâng cao khả năng bảo vệ dữ liệu quan trọng và tạo nền tảng vững chắc cho việc mở rộng hệ thống trong tương lai.

2. Lý do chọn đề tài

Đề tài "Triển khai hệ thống quản trị người dùng và kiểm soát truy cập mạng doanh nghiệp với Active Directory cho Công ty CPTM Xuất nhập khẩu HPC" được lựa chọn với các lý do trọng tâm sau:

Thứ nhất, trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, yêu cầu về bảo mật và quản lý hệ thống thông tin của các doanh nghiệp ngày càng tăng cao. Các doanh nghiệp đang có xu hướng tìm kiếm các giải pháp quản lý hệ thống hiệu quả, có khả năng đảm bảo an toàn thông tin và tối ưu hóa quy trình làm việc. Đồng thời, các doanh nghiệp cũng cần những giải pháp phù hợp để cá nhân hóa quyền truy cập, phù hợp với từng vai trò và nhiệm vụ của nhân viên. Vậy nên, việc triển khai một hệ thống quản trị người dùng chuyên nghiệp sẽ giúp cho Công ty CPTM Xuất nhập khẩu HPC mở rộng khả năng kiểm soát truy cập, không còn bị giới hạn bởi các phương pháp quản lý thủ công. Điều này không chỉ gia tăng mức độ bảo mật thông tin mà còn nâng cao hiệu quả làm việc của nhân viên.

Thứ hai, hệ thống Active Directory sẽ giúp tăng hiệu quả quản lý. Thay vì quản lý thủ công, việc sử dụng hệ thống tự động sẽ giúp công ty quản lý tài khoản người dùng, quyền truy cập, chính sách bảo mật và các báo cáo thống kê hoạt động một cách chính xác và hiệu quả hơn. Điều này giúp giảm thiểu sai sót và tiết kiệm thời gian, đồng thời cung cấp dữ liệu kịp thời và chính xác để hỗ trợ ra quyết định.

Thứ ba, sự thuận lợi của công nghệ. Active Directory là một công nghệ mạnh mẽ và phổ biến trong quản lý hệ thống thông tin hiện nay. Sử dụng công nghệ này đảm bảo hệ thống có hiệu suất cao, bảo mật tốt và dễ dàng mở rộng trong tương lai. Active Directory cung cấp khả năng xây dựng các chính sách bảo mật mạnh mẽ, quản lý quyền truy cập một cách hiệu quả, đồng thời hỗ trợ tự động hóa nhiều quy trình quản trị CNTT. Việc sử dụng công nghệ và hệ thống để quản lý người dùng mang lại nhiều lợi ích, bao gồm kiểm soát truy cập dễ dàng, quản lý tài khoản hiệu quả, và tạo ra một môi trường làm việc an toàn và hiệu quả cho nhân viên.

Cuối cùng, một hệ thống quản lý người dùng tốt là yếu tố quyết định thành công của việc bảo mật và quản lý thông tin trong doanh nghiệp. Active Directory với khả năng tạo ra các chính sách bảo mật linh hoạt và quản lý quyền truy cập chi tiết sẽ giúp bảo vệ thông tin quan trọng của công ty. Một hệ thống quản lý người dùng thân thiện không chỉ nâng cao hiệu quả làm việc của nhân viên mà còn đảm bảo an toàn thông tin cho toàn bộ hệ thống.

Với những lý do trên, việc lựa chọn đề tài này có thể mang lại nhiều cơ hội và lợi ích kinh doanh đáng kể cho các nhà nghiên cứu và doanh nghiệp quan tâm đến lĩnh vực quản lý hệ thống thông tin và bảo mật.

3. Mục đích nghiên cứu

- Triển khai và cấu hình hệ thống Active Directory cho doanh nghiệp HPC.

- Tạo ra một cơ chế quản lý người dùng và kiểm soát truy cập mạng hiệu quả, linh hoạt.

- Đảm bảo tính an toàn, bảo mật thông tin trong hệ thống mạng của doanh nghiệp.

- Đưa ra kế hoạch và giải pháp cụ thể để áp dụng công nghệ này trong thực tế.

4. Phương pháp nghiên cứu

**- Phương pháp khảo sát thực tiễn:** Thu thập thông tin về hiện trạng mạng và yêu cầu quản lý của công ty HPC.

**- Phương pháp phân tích tài liệu:** Nghiên cứu các tài liệu, sách hướng dẫn và các tiêu chuẩn triển khai Active Directory.

**- Phương pháp thực nghiệm:** Triển khai thử nghiệm trên môi trường giả lập trước khi áp dụng vào thực tế.

**- Phương pháp đánh giá:** Kiểm tra, đánh giá hiệu quả hệ thống thông qua các tiêu chí về bảo mật, quản lý và hiệu suất.

5. Phạm vi nghiên cứu

- Tập trung vào triển khai hệ thống Active Directory tại Công ty CPTM Xuất nhập khẩu HPC.

- Nghiên cứu các thành phần chính như Forest, Domain, OU, User Account, Group Policy và Site.

- Đánh giá hiệu quả quản trị người dùng và kiểm soát truy cập sau khi triển khai.

6. Kết cấu của đồ án

Đồ án này gồm có năm phần:

- Mở đầu, giới thiệu tổng quan về đề tài, trình bày lý do chọn đề tài, phương pháp nghiên cứu và phạm vi nghiên cứu.

- Chương 1: Yêu cầu bài toán, đi sâu phân tích cụ thể các yêu cầu đặt ra của hệ thống, bao gồm các yêu cầu về chức năng và phi chức năng, đồng thời giới thiệu về các công nghệ sử dụng trong đồ án.

- Chương 2: Phân tích và thiết kế hệ thống, trình bày chi tiết quá trình khảo sát hiện trạng hệ thống mạng của doanh nghiệp HPC, thiết kế mô hình hệ thống Active Directory và lập kế hoạch triển khai tài khoản người dùng, nhóm và máy tính.

- Chương 3: Xây dựng, triển khai và tích hợp, tập trung vào quá trình triển khai hệ thống Active Directory, bao gồm việc cấu hình Forest, Domain, Organization Unit (OU), Group Policy Object (GPO), tích hợp Domain Name System (DNS) và quản lý Site.

- Kết luận tóm tắt và đánh giá kết quả đạt được, phân tích ưu điểm, nhược điểm của hệ thống, đồng thời đề xuất hướng phát triển trong tương lai.

CHƯƠNG 1: CƠ SỞ LÝ THUYẾT

1.1 Giới thiệu về Active Directory (AD)

Active Directory (AD) có thể được xem như một bước tiến quan trọng trong việc quản lý tài nguyên mạng so với hệ thống LAN Manager trên Windows NT 4.0. Về bản chất, Active Directory hoạt động như một cơ sở dữ liệu lưu trữ thông tin về các tài nguyên mạng (hay còn gọi là đối tượng) cùng với các thuộc tính liên quan. Tuy nhiên, ý tưởng về dịch vụ thư mục (Directory Service) không phải là mới mẻ, vì trước đó Novell đã triển khai công nghệ này trong nhiều năm.

Mặc dù Windows NT 4.0 là một hệ điều hành mạng khá ổn định, nhưng khi áp dụng trong các hệ thống lớn, nó bộc lộ nhiều hạn chế. Đối với các mạng quy mô nhỏ, công cụ Network Neighborhood tỏ ra khá hữu ích, giúp người dùng duyệt và tìm kiếm tài nguyên một cách thuận tiện. Tuy nhiên, khi số lượng máy tính và tài nguyên tăng lên, việc tìm kiếm và quản lý hệ thống trở nên phức tạp hơn, đặc biệt khi người dùng không nhớ chính xác tên của máy chủ hoặc máy in cần truy cập.

Một điểm yếu khác của Windows NT 4.0 là việc quản trị viên phải phân chia hệ thống thành nhiều domain riêng lẻ và thiết lập quan hệ ủy quyền giữa chúng để đảm bảo quản lý hiệu quả. Quá trình này không chỉ tốn thời gian mà còn dễ phát sinh lỗi nếu không được cấu hình chính xác. Active Directory đã giải quyết được những hạn chế này bằng cách cung cấp một nền tảng quản lý tập trung và linh hoạt hơn, giúp doanh nghiệp vận hành hệ thống mạng một cách hiệu quả.

Với Active Directory, mỗi domain có thể lưu trữ hàng chục triệu đối tượng, đủ khả năng phục vụ một lượng lớn người dùng mà không gặp phải các vấn đề về hiệu suất. Điều này giúp AD trở thành một công cụ mạnh mẽ cho các tổ chức có quy mô lớn, nơi yêu cầu quản lý tập trung nhưng vẫn đảm bảo khả năng mở rộng và bảo mật.

1.2 Chức năng của Active Directory

Active Directory đóng vai trò như một hệ thống quản lý tập trung, giúp doanh nghiệp dễ dàng kiểm soát tài nguyên mạng và bảo mật dữ liệu. Các chức năng chính bao gồm:

Quản lý danh sách tập trung các tài khoản người dùng và máy tính

+ AD lưu trữ thông tin về tài khoản người dùng, bao gồm tên đăng nhập, mật khẩu và quyền hạn tương ứng.

+ Ngoài ra, hệ thống cũng duy trì danh sách các thiết bị trong mạng, giúp việc quản lý trở nên thuận tiện hơn.

Cung cấp máy chủ xác thực và quản lý đăng nhập

+ AD sử dụng Domain Controller (DC) để xác thực danh tính người dùng khi họ đăng nhập vào mạng.

+ Máy chủ này chịu trách nhiệm kiểm tra thông tin đăng nhập, cấp quyền truy cập và đảm bảo tính bảo mật của hệ thống.

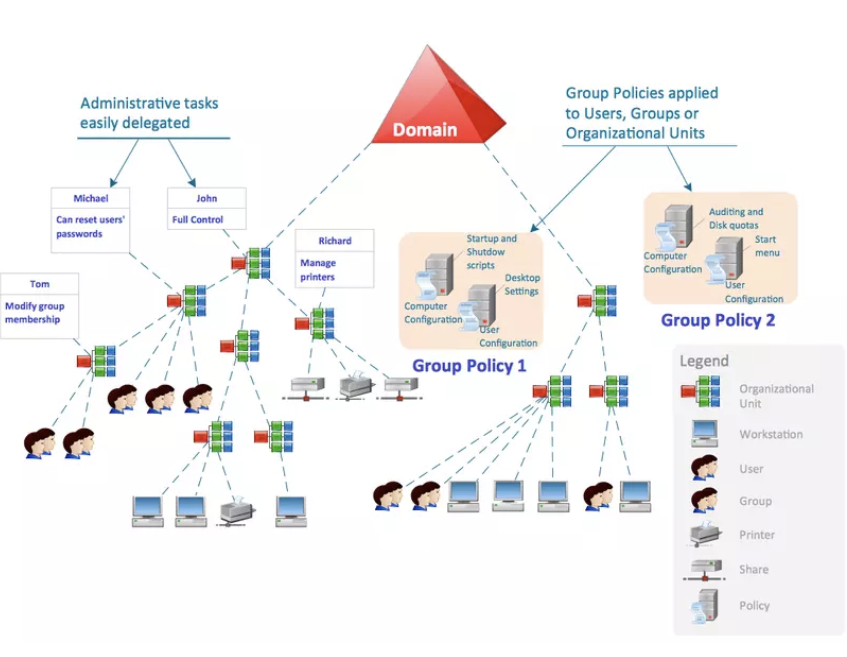
Hỗ trợ tìm kiếm và định vị tài nguyên nhanh chóng

+ AD duy trì một hệ thống chỉ mục và danh mục toàn cầu (Global Catalog) giúp các máy tính trong mạng dễ dàng tìm kiếm tài nguyên trên các thiết bị khác trong cùng hệ thống.

+ Điều này giúp tăng tốc độ truy vấn và tối ưu hóa hiệu suất hoạt động của mạng.

Phân quyền linh hoạt theo từng nhóm người dùng: AD cho phép tạo tài khoản với các quyền hạn khác nhau tùy theo vai trò của từng người dùng. Điều này đảm bảo mỗi người chỉ có thể thực hiện các thao tác phù hợp với nhiệm vụ của họ.

Hỗ trợ phân chia miền thành các vùng nhỏ để quản lý hiệu quả : AD cho phép chia nhỏ hệ thống thành các miền con (Subdomain) hoặc các đơn vị tổ chức (Organizational Unit - OU). Việc này giúp phân quyền quản lý cho từng bộ phận cụ thể trong tổ chức, giảm tải cho quản trị viên chính và tăng tính linh hoạt trong quản trị hệ thống



Hình 1.1: Active Directory

( Nguồn: Microsoft Learn )

1.3 Cấu trúc Active Directory

Active Directory được tổ chức theo mô hình phân cấp (hierarchical structure), bao gồm các thành phần logic và vật lý nhằm mục tiêu quản lý tập trung tài nguyên mạng, tài khoản người dùng và chính sách bảo mật trong hệ thống Windows Server. Cấu trúc của Active Directory được chia thành hai nhóm chính:

1.3.1 Cấu trúc logic

Đây là phần cốt lõi trong việc tổ chức và phân quyền người dùng, tài nguyên, bao gồm các thành phần sau:

Forest (Rừng): Là mức cao nhất trong AD, bao gồm một hoặc nhiều domain. Forest chia sẻ một sơ đồ (schema) và danh mục toàn cầu (Global Catalog). Một Forest đại diện cho ranh giới tin cậy và bảo mật.

Domain (Miền): Là đơn vị quản lý chính của Active Directory. Domain chứa người dùng, nhóm, máy tính, và các đối tượng bảo mật khác. Mỗi domain có chính sách bảo mật riêng và mối quan hệ tin cậy (trust) với domain khác.

Organizational Unit (OU): Là đơn vị tổ chức trong domain, dùng để nhóm các đối tượng như người dùng, nhóm, hoặc máy tính. OU giúp dễ dàng phân quyền và áp dụng Group Policy. OU có thể lồng nhau để tạo thành cấu trúc phân cấp.

Tree (Cây): Là một hoặc nhiều domain được liên kết với nhau theo thứ bậc và chia sẻ một không gian tên liên tục (contiguous namespace). Các domain trong cùng một tree có mối quan hệ tin cậy hai chiều mặc định.

1.3.2 Cấu trúc vật lý

Cấu trúc vật lý thể hiện cách Active Directory triển khai và quản lý dữ liệu trong hệ thống mạng thực tế:

Domain Controller (DC): Là máy chủ cài đặt Active Directory Domain Services (AD DS), chịu trách nhiệm xác thực người dùng, lưu trữ và cung cấp dịch vụ thư mục. Mỗi domain nên có ít nhất hai Domain Controller để đảm bảo tính sẵn sàng.

Site (Trang): Là đại diện cho một hoặc nhiều subnet mạng vật lý có kết nối tốt với nhau (thường là tốc độ cao). Việc tạo site giúp tối ưu hóa lưu lượng truy cập mạng và quá trình replication (đồng bộ dữ liệu) giữa các Domain Controller.

Replication (Sao chép dữ liệu): Là cơ chế đồng bộ dữ liệu giữa các Domain Controller trong cùng domain hoặc khác domain. Có hai loại replication chính:

Intra-site replication (trong cùng site): Diễn ra thường xuyên và nhanh chóng.

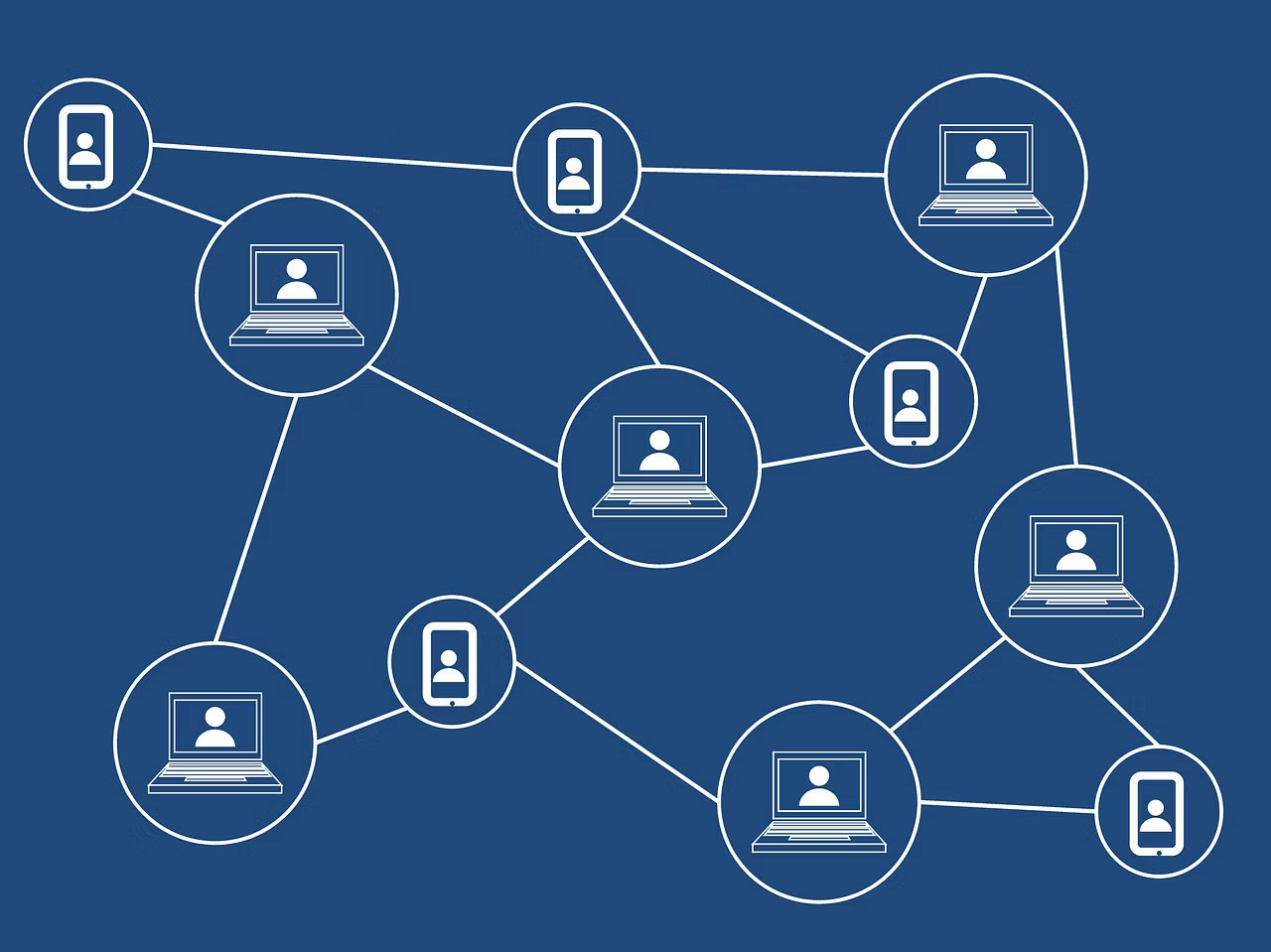
Inter-site replication (giữa các site): Diễn ra theo lịch, được tối ưu hóa để tiết kiệm băng thông.

1.4. Cơ chế hoạt động Active Directory

1.4.1 Directory Service

Directory Service là một hệ thống lưu trữ thông tin về người dùng, nhóm, thiết bị và các tài nguyên khác trong mạng. Tất cả dữ liệu này được lưu trong một tập tin cơ sở dữ liệu gọi là NTDS.DIT.

Dịch vụ danh bạ không chỉ là một nơi lưu trữ thông tin mà còn là nền tảng giúp Active Directory vận hành một cách hiệu quả. Nhờ có Directory Service, các hệ thống có thể dễ dàng quản lý thông tin, thực hiện truy vấn dữ liệu nhanh chóng và hỗ trợ xác thực người dùng trong toàn bộ hệ thống mạng.



Hình 1.2 : Directory Service

( Nguồn: Microsoft Learn )

* + 1. Active Directory Schema
* Schema là một tập hợp các định nghĩa về loại đối tượng và thuộc tính của các đối tượng trong Active Directory. Nó giúp xác định các thông tin cần thiết để mô tả từng loại đối tượng khác nhau:
* Mỗi đối tượng trong AD (người dùng, máy tính, máy in, nhóm,…) đều có một tập

hợp thuộc tính nhất định.

* Schema có thể được mở rộng và tùy chỉnh theo nhu cầu của tổ chức .

1.4.3 Global Catalog

Global Catalog là một thành phần quan trọng trong Active Directory giúp tăng tốc độ truy vấn dữ liệu và xác thực người dùng trên toàn hệ thống.

Chức năng của Global Catalog:

* Lưu trữ thông tin về tất cả các đối tượng trong domain và một phần thông tin của

các domain khác trong cùng một forest.

* Cho phép tìm kiếm nhanh chóng đối tượng trong Active Directory mà không cần

kết nối đến từng domain riêng lẻ.

* Hỗ trợ quá trình xác thực người dùng khi họ đăng nhập vào hệ thống.

1.4.4 Global Catalog Server

Global Catalog Server (GCS) là một máy chủ đặc biệt trong hệ thống Active Directory có nhiệm vụ lưu trữ một bản sao của Global Catalog.

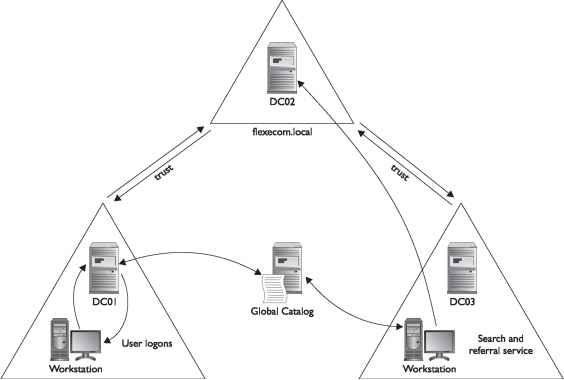
Tầm quan trọng của Global Catalog Server:

* Giúp định vị đối tượng trong AD một cách nhanh chóng.
* Hỗ trợ quá trình đăng nhập của người dùng bằng cách cung cấp thông tin về nhóm

mà người dùng thuộc về.

* Nếu Global Catalog Server không hoạt động, người dùng chỉ có thể đăng nhập vào

máy tính cục bộ trừ khi họ là thành viên của nhóm Domain Administrator.



Hình 1.3: Global Catalog Server

( Nguồn: Microsoft Learn )

1.4.5 Distinguished và Relative Distinguished Name

* Distinguished Name (DN):

Mỗi object trong Active Directory sẽ có một tên duy nhất. Đây là tên được xem như là DN. Nó chứa đầy đủ các thông tin về đối tượng bao gồm tên của domain nơi lưu trữ đối tượng và đường dẫn đầy đủ mà thông qua đó đối tượng có thể được chỉ ra.

* Relative Distinguished Name (RDN):

RDN của một đối tượng là một thuộc tính của chính đối tượng đó, hỗ trợ truy vấn bằng thuộc tính. Vì thế mỗi đối tượng đó có thể được xác định ngay cả khi không biết về DN của nó. Một thuộc tính quan trọng được sử dụng để truy vấn trong Active Directory là RDN.

1.4.6 Cơ chế Single Sign-on

Single Sign-On (SSO) là một cơ chế giúp người dùng chỉ cần đăng nhập một lần

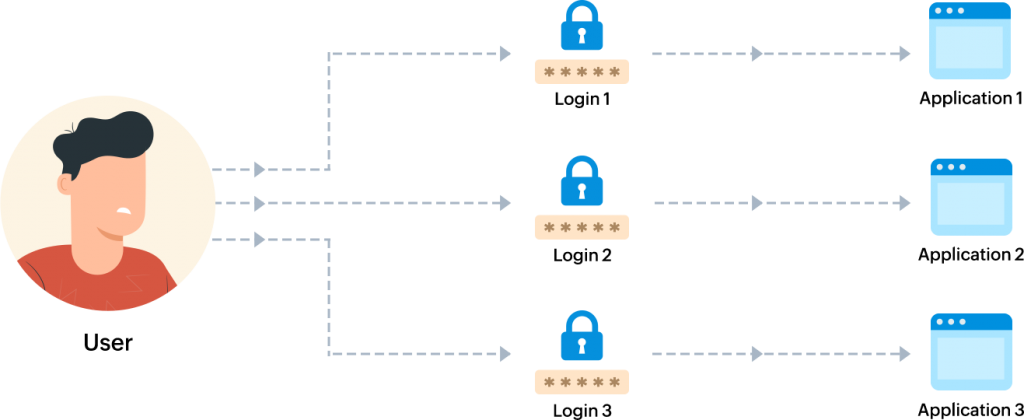
để truy cập vào nhiều dịch vụ khác nhau trong hệ thống.

Lợi ích của SSO:

+ Giảm số lần nhập mật khẩu, tăng tính tiện lợi.

+ Giúp quản trị viên dễ dàng kiểm soát quyền truy cập hơn.

Cơ chế hoạt động của SSO được triển khai thông qua một máy chủ xác thực trung tâm (Identity Provider - IdP). Khi người dùng đăng nhập thành công vào một dịch vụ thuộc hệ thống SSO, máy chủ này sẽ tạo một phiên xác thực và cấp mã thông báo (token) hoặc cookie bảo mật. Khi người dùng tiếp tục truy cập các dịch vụ khác trong cùng hệ thống, các dịch vụ đó sẽ gửi yêu cầu xác thực về IdP. Nếu phiên xác thực còn hiệu lực, người dùng sẽ được cấp quyền truy cập ngay lập tức mà không cần nhập lại thông tin đăng nhập. Quá trình này diễn ra hoàn toàn tự động và minh bạch, đảm bảo trải nghiệm liền mạch và liên tục cho người dùng.



Hình 1.4: Cơ chế Single Sign-on

( Nguồn: Microsoft Learn – [Active Directory Domain Services overview](https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview) )

1.2 Giới thiệu về Công ty CPTM Xuất nhập khẩu HPC

1.2.1 Khảo sát yêu cầu thực trạng

HPC có hệ thống tổ chức và quản lý chặt chẽ, với cơ sở hạ tầng CNTT được triển khai trên toàn bộ hệ thống công ty, bao gồm:

* Hội sở chính đặt tại TP. Hà Nội, là nơi điều hành toàn bộ hoạt động của công ty với 120 nhân viên, chia thành các bộ phận:
* Phòng Giám đốc
* Phòng Kinh doanh
* Phòng Kế toán
* Phòng Nhân sự
* Phòng CNTT
* Phòng Tuyển dụng
* Phòng Xử lý hồ sơ

Tất cả nhân viên tại hội sở đều sử dụng máy tính, được kết nối vào hệ thống mạng nội bộ để phục vụ công tác quản lý, điều hành và kinh doanh.

* Các nhà máy sản xuất: HPC có 2 nhà máy sản xuất, gồm:
* Nhà máy tại Hà Nội (HPC Factory 1)
* Nhà máy tại Đà Nẵng (HPC Factory 2)
* Mỗi nhà máy có hai bộ phận chính:
* Phòng Kỹ thuật: 20 nhân viên
* Phòng Điều hành sản xuất: 40 nhân viên
* Các nhà máy sử dụng hệ thống CNTT để quản lý quy trình sản xuất, giám sát chất lượng và vận hành hệ thống ERP.
* Các chi nhánh kinh doanh: HPC có 2 chi nhánh đảm nhiệm tiếp thị và phân phối sản phẩm:
* Chi nhánh tại TP. Hồ Chí Minh – Tên miền: hcm.hpc.com.vn
* Chi nhánh tại Đà Nẵng – Tên miền: danang.hpc.com.vn

Tổng số nhân viên tại các chi nhánh là 90 người (TP. Hồ Chí Minh 50 NV; Đà Nẵng 40 NV).

Công ty con: HPC có công ty con chuyên kinh doanh thiết bị công nghiệp, cung cấp sản phẩm cho các doanh nghiệp, nhà máy và dự án lớn. Công ty này có tên HPC Industrial, với tên miền hpcindustrial.com.vn và đặt trụ sở tại TP. Hồ Chí Minh.

HPC Industrial hoạt động độc lập về quản lý, kinh doanh và hệ thống mạng. Tuy nhiên, hệ thống của HPC Industrial vẫn kết nối với hệ thống của HPC để truyền tải dữ liệu và hỗ trợ các hoạt động kinh doanh liên kết.

1.2.2 Danh mục các thiết bị

Bảng 1.1: Danh mục các thiết bị

| **STT** | **Tên Thiết Bị** | **Đặc Tính Kỹ Thuật** | **Số Lượng** | **Thành Tiền** |
| --- | --- | --- | --- | --- |
| 1 | Máy chủ Dell PowerEdge R750 | - 2 x Intel Xeon Gold 6338 (2.0GHz, 32-core, 48MB cache)  - RAM: 64GB DDR4 ECC RDIMM  - RAID Controller PERC H755 (RAID 0,1,5,10)  - 8 x 2.5" SSD 960GB NVMe  - Dual Power 1400W, Redundant | 10 | 2.500.000.000 |
| 2 | Phần mềm Windows Server 2022 Datacenter | Hỗ trợ hệ thống ảo hóa Hyper-V, bảo mật TPM 2.0, hỗ trợ Windows Admin Center | 10 | 320.000.000 |
| 3 | Router Cisco ISR 4461 | - 8 x 10Gbps WAN/LAN  - 1 x 1Gbps Console  - VPN IPSec 500 Mbps  - Tường lửa tích hợ | 10 | 900.000.000 |
| 4 | Máy tính Dell OptiPlex 7010 Plus | - CPU Intel Core i7-13700 (16 Cores, 24 Threads)  - RAM 16GB DDR5  - SSD NVMe 1TB  - GPU Intel UHD Graphics 770  - Màn hình Dell 24" FHD IPS | 450 | 4.200.000.000 |
| 5 | |  | | --- | |  |  |  | | --- | | Bộ lưu điện APC Smart-UPS SRT 2200VA | | - Công suất: 2200VA / 1980W  - Pin Lithium-ion, tuổi thọ 8-10 năm  - Hỗ trợ kết nối SNMP | 450 | 600.000.000 |
| 6 | Máy in HP LaserJet Enterprise MFP M635h | - In tốc độ 55ppm  - Hỗ trợ in mạng, scan 2 mặt, Wi-Fi Direct  - Hộp mực LaserJet HP 147X (25.000 trang) | 120 | 1.500.000.000 |
| 7 | Switch Cisco Catalyst 9500-48Y4C | - 48 ports 10G SFP+  - 4 x 100G uplink  - Hỗ trợ SDN & VXLAN | 10 | 1.200.000.000 |
| 8 | Switch Cisco Catalyst 9300-24P | - 24 cổng 1GbE PoE+  - 4 x 10GbE uplinks  - Tích hợp Cisco DNA | 6 | 300.000.000 |
| 9 | Firewall Cisco Firepower 2140 | - 3 Gbps firewall throughput  - 10GbE interface  - Tích hợp IPS, VPN & Threat Intelligence | 6 | 350.000.000 |
| 10 | Phần mềm diệt virus Kaspersky Endpoint Security Cloud Plus | Hỗ trợ 500 users, bảo vệ đa nền tảng, AI chống mã độc tống tiền | 1 | 200.000.000 |
| 11 | Phần mềm sao lưu Acronis Cyber Protect Advanced | Hỗ trợ backup dữ liệu đám mây, phục hồi hệ thống nhanh chóng | 1 | 50.000.000 |
|  | **Tổng cộng** |  |  | **11.120.000.000** |

CHƯƠNG 2: PHÂN TÍCH VÀ THIẾT KẾ HỆ THỐNG QUẢN TRỊ

NGƯỜI DÙNG VỚI ACTIVE DIRECTORY

2.1 Thiết kế mô hình hệ thống Active Directory

2.1.1 Mô hình Tổng quan Active Directory

Hệ thống Active Directory (AD) của HPC được thiết kế để đảm bảo quản lý tập trung, bảo mật và hiệu quả cho toàn bộ hệ thống CNTT. Mô hình AD sẽ triển khai theo mô hình cây miền (Tree Domain) với các thành phần sau:

* Miền gốc (Root Domain): hpc.com.vn

**Chức năng chính:**

+ Quản lý toàn bộ tài khoản người dùng, thiết bị và tài nguyên CNTT của

công ty.

+ Điều phối việc xác thực và phân quyền trong toàn hệ thống.

+ Kiểm soát chính sách bảo mật và quyền truy cập trên các miền con.

+ Cung cấp hạ tầng mạng và dịch vụ quản trị tập trung cho toàn bộ công ty.

* Các miền con (Child Domains): Các miền con được tạo ra để quản lý các đơn vị kinh doanh khác nhau trong công ty.

Bảng 2.1: Bảng Mô hình các miền con

| **Miền con** | **Tên miền** | **Chức năng quản lý** |
| --- | --- | --- |
| **Hội sở chính & Nhà máy** | hanoi.hpc.com.vn | Quản lý tài khoản người dùng và hệ thống CNTT tại hội sở chính, nhà máy sản xuất Hà Nội. |
| **Chi nhánh TP. Hồ Chí Minh** | hcm.hpc.com.vn | Quản lý hệ thống CNTT cho chi nhánh kinh doanh và phân phối tại miền Nam. |
| **Chi nhánh Đà Nẵng** | danang.hpc.com.vn | Quản lý hệ thống CNTT và nhân sự tại chi nhánh miền Trung. |
| **Công ty con HPC Industrial** | hpcindustrial.com.vn | Hoạt động độc lập nhưng vẫn có kết nối dữ liệu với hệ thống chính để chia sẻ tài nguyên. |

* Mô hình Tree Domain mang lại nhiều lợi ích quan trọng như:

Quản lý tập trung nhưng linh hoạt: Miền gốc đóng vai trò kiểm soát chính sách, bảo mật và xác thực người dùng, trong khi mỗi miền con có thể có cấu trúc quản lý riêng, phù hợp với từng khu vực và đơn vị kinh doanh.

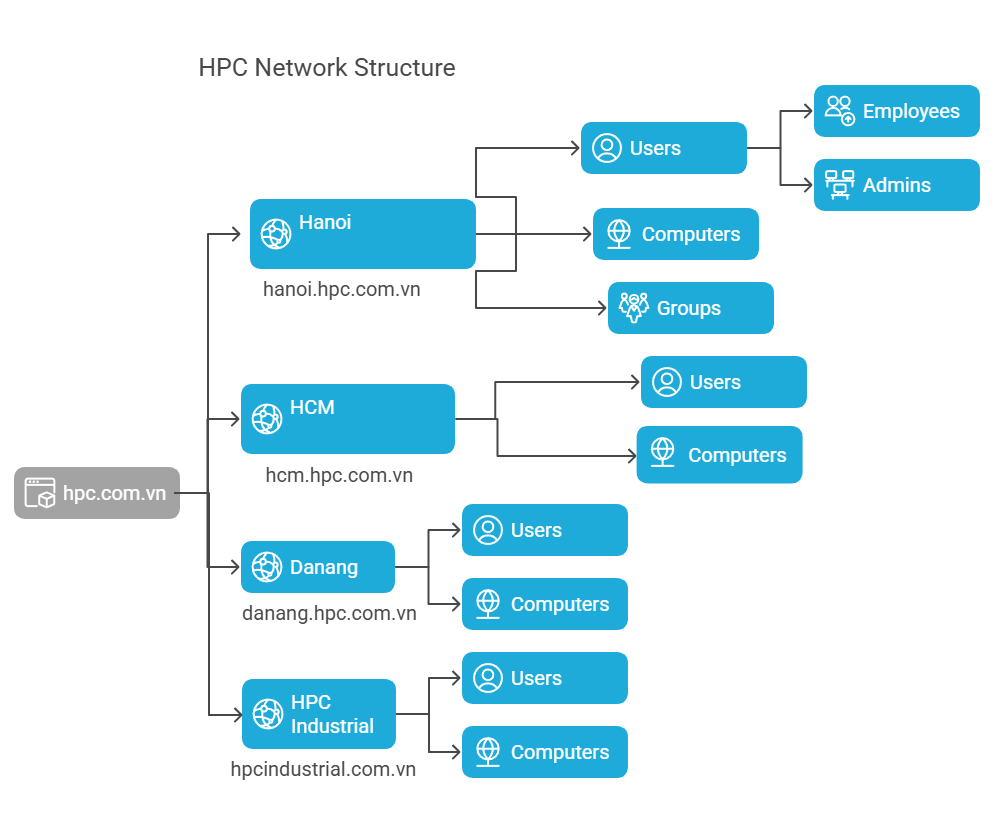
Bảo mật và kiểm soát truy cập chặt chẽ: Mỗi miền con có thể thiết lập chính sách bảo mật riêng biệt, hạn chế rủi ro xâm nhập từ bên ngoài, đồng thời phân quyền rõ ràng, giúp bảo vệ dữ liệu quan trọng.

Khả năng mở rộng dễ dàng: Khi công ty mở rộng thêm nhà máy hoặc chi nhánh mới, chỉ cần thêm miền con mới mà không ảnh hưởng đến hệ thống hiện có.

Tối ưu hóa hiệu suất hệ thống: Mỗi miền con có Domain Controller (DC) riêng, giúp giảm tải cho máy chủ trung tâm, tăng tốc độ xử lý dữ liệu và hạn chế tình trạng tắc nghẽn mạng khi có nhiều yêu cầu truy cập đồng thời.

2.2.2 Cấu trúc Tổ chức trong Active Directory

Hệ thống AD được chia theo các Organizational Units (OU) để phản ánh cơ cấu tổ chức thực tế của HPC. Việc tổ chức theo OU giúp quản lý chính sách, quyền hạn và tài nguyên một cách hiệu quả.



Hình 2.1: Cấu trúc Tổ chức trong Active Directory

- Chi tiết các OU trong Active Directory của HPC

1. Users (Người dùng)

* Mô tả: OU này chứa tất cả tài khoản người dùng theo từng đơn vị trực thuộc HPC.
* Chia nhóm cụ thể (ở chi nhánh Hanoi):

+ Admins: Tài khoản của quản trị viên CNTT và nhân sự có quyền quản lý hệ thống.

+ Employees: Tài khoản của nhân viên thông thường, giới hạn quyền truy cập theo vai trò.

* Chính sách áp dụng:

+ Các nhóm người dùng được kiểm soát bởi Group Policy Objects (GPO) để hạn chế truy cập không hợp lệ.

+ Chính sách bảo mật, bao gồm yêu cầu đổi mật khẩu định kỳ và sử dụng xác thực đa yếu tố (MFA).

2. Computers (Thiết bị đầu cuối)

* Mô tả: OU này chứa danh sách các thiết bị máy tính thuộc hệ thống của HPC, bao gồm máy trạm của nhân viên và máy chủ.
* Chính sách áp dụng:

+ Chính sách triển khai phần mềm từ xa.

+ Quản lý bản vá bảo mật tự động.

+ Theo dõi và ghi nhật ký hoạt động của thiết bị.

3. Groups (Nhóm quyền hạn - Chỉ có ở Hanoi)

* Mô tả: Phân nhóm người dùng theo các vai trò khác nhau trong tổ chức.
* Loại nhóm:

+ Security Groups (Nhóm bảo mật): Kiểm soát quyền truy cập vào các tài nguyên

+ Distribution Groups (Nhóm phân phối): Sử dụng để gửi email đến một nhóm người dùng trong nội bộ.

* Chính sách áp dụng:

+ Mỗi nhóm được cấp quyền truy cập theo nguyên tắc Least Privilege (ít quyền nhất có thể).

+ Người quản trị có thể dễ dàng thêm/xóa thành viên trong nhóm mà không ảnh hưởng đến quyền của các tài khoản khác.

2.2.3 Phân cấp Domain Controller (DC)

Hệ thống Active Directory (AD) của HPC được thiết kế với mô hình phân cấp Domain Controller (DC) nhằm đảm bảo tính sẵn sàng cao (High Availability) và khả năng phục hồi dữ liệu nhanh chóng. Việc triển khai nhiều DC giúp phân tải hệ thống, giảm thiểu rủi ro mất dữ liệu và đảm bảo hoạt động liên tục của hệ thống mạng.

Hệ thống Domain Controller của HPC được tổ chức thành 3 cấp chính:

DC chính (Primary Domain Controller - PDC): Đặt tại Hội sở Hà Nội (hanoi.hpc.com.vn), đóng vai trò trung tâm trong quản lý Active Directory.

Additional Domain Controllers (ADCs): Đặt tại các chi nhánh TP. Hồ Chí Minh (hcm.hpc.com.vn) và Đà Nẵng (danang.hpc.com.vn) để hỗ trợ phân tải và giảm thiểu downtime khi có sự cố.

HPC Industrial (hpcindustrial.com.vn): Hệ thống AD độc lập nhưng vẫn có kết nối bảo mật với hệ thống của HPC để đảm bảo tính nhất quán về dữ liệu.

* Chức năng của từng Domain Controller

DC chính tại Hội sở Hà Nội (hanoi.hpc.com.vn - PDC):

+ Là Primary Domain Controller (PDC), chịu trách nhiệm quản lý toàn bộ hệ thống AD của HPC.

+ Chứa Global Catalog Server, giúp xác thực nhanh chóng và truy vấn dữ liệu trong hệ thống AD.

Nắm giữ tất cả FSMO (Flexible Single Master Operations) Roles bao gồm:

+ Schema Master: Quản lý lược đồ của Active Directory.

+ Domain Naming Master: Kiểm soát việc tạo/xóa domain trong forest.

+ RID Master: Quản lý bộ định danh RID để cấp quyền cho các đối tượng bảo mật (SID).

+ PDC Emulator: Xử lý về xác thực mật khẩu và thời gian hệ thống.

+ Infrastructure Master: Cập nhật thông tin nhóm và người dùng giữa các domain.

Additional Domain Controllers (ADCs) tại TP. Hồ Chí Minh và Đà Nẵng:

+ Không nắm giữ FSMO Roles, nhưng hỗ trợ phân tải và đảm bảo tính sẵn sàng của hệ thống AD.

+ Có cơ chế Replication với PDC để đồng bộ dữ liệu tài khoản, nhóm, và chính sách trên toàn hệ thống.

+ Cho phép xác thực đăng nhập cục bộ tại các chi nhánh, giúp giảm tải cho DC chính ở Hà Nội

+ HPC Industrial (hpcindustrial.com.vn)

* Hệ thống AD hoàn toàn độc lập nhưng vẫn cần kết nối dữ liệu với HPC.
* Sử dụng Secure Trust Relationship để kiểm soát quyền truy cập tài nguyên một cách an toàn.
* Cơ chế Replication giữa các Domain Controller

Hệ thống AD của HPC sử dụng cơ chế Replication để đồng bộ dữ liệu trên toàn bộ các máy chủ DC, đảm bảo mọi thay đổi về tài khoản, nhóm và chính sách đều được cập nhật tức thời :

* Replication giữa PDC và ADCs: PDC tại Hà Nội thực hiện Replication với ADCs tại TP. Hồ Chí Minh và Đà Nẵng.
* Replication giữa ADCs: ADCs có thể trao đổi dữ liệu với nhau, giúp giảm tải cho PDC.
* Chính sách Replication:

+ Scheduled Replication: Đồng bộ vào thời gian cố định để giảm tải hệ thống.

+ Event-Based Replication: Đồng bộ ngay khi có thay đổi quan trọng (ví dụ: tạo tài khoản mới).

+ Replication Over WAN Optimization: Tối ưu băng thông khi đồng bộ dữ liệu giữa các chi nhánh.

* Lợi ích của mô hình phân cấp Domain Controller tại HPC

+ Độ tin cậy cao: Hệ thống phân tán giúp đảm bảo hoạt động liên tục ngay cả khi một DC gặp sự cố.

+ Giảm tải cho hệ thống: Phân phối quá trình xử lý xác thực và quản lý tài khoản giúp tối ưu tài nguyên.

+ Tốc độ xác thực nhanh: Người dùng tại mỗi chi nhánh có thể xác thực cục bộ thay vì phải kết nối về PDC.

+ Bảo mật tốt hơn: Kiểm soát dữ liệu và quyền truy cập chặt chẽ thông qua các chính sách AD.

+ Khả năng mở rộng linh hoạt: Có thể dễ dàng thêm DC mới nếu HPC mở rộng thêm chi nhánh.

2.2 Lập kế hoạch triển khai tài khoản người dùng, nhóm và máy tính

2.2.1 Lập bảng thiết kế sơ đồ tổ chức

Bảng 2.2: Bảng thiết kế sơ đồ tổ chức

| **Cấp tổ chức** | **Đơn vị** | **Số lượng** | **Vai trò chính** |
| --- | --- | --- | --- |
| Hội sở chính | Hanoi  (hanoi.hpc.com.vn) | 120 | Điều hành, quản lý, kinh doanh. |
| Phòng Giám đốc |  | 5 | Quản lý cấp cao, chiến lược phát triển. |
| Phòng Kinh doanh |  | 30 | Bán hàng, tiếp thị, phát triển khách hàng. |
| Phòng Kế toán |  | 15 | Quản lý tài chính, kiểm toán, báo cáo thuế. |
| Phòng Nhân sự |  | 10 | Tuyển dụng, đào tạo, chế độ phúc lợi. |
| Phòng CNTT |  | 15 | Quản trị hệ thống, bảo mật, hỗ trợ kỹ thuật. |
| Phòng Tuyển dụng |  | 20 | Tuyển dụng nhân sự, đánh giá ứng viên. |
| Phòng Xử lý hồ sơ |  | 25 | Quản lý giấy tờ, xử lý hồ sơ khách hàng. |
| Nhà máy sản xuất | HPC Factory 1  (Hà Nội) | 60 | Sản xuất, kỹ thuật. |
| Phòng Kỹ thuật |  | 20 | Thiết kế, bảo trì, nghiên cứu công nghệ. |
| Phòng Điều hành SX |  | 40 | Vận hành dây chuyền sản xuất. |
| Nhà máy sản xuất | HPC Factory 2  (Đà Nẵng) | 60 | Sản xuất, kỹ thuật. |
| Phòng Kỹ thuật |  | 20 | Thiết kế, bảo trì, nghiên cứu công nghệ. |
| Phòng Điều hành SX |  | 40 | Vận hành dây chuyền sản xuất. |
| Chi nhánh kinh doanh | HPC HCM  (hcm.hpc.com.vn) | 50 | Tiếp thị, phân phối sản phẩm khu vực phía Nam. |
| Chi nhánh kinh doanh | HPC Đà Nẵng  (danang.hpc.com.vn) | 40 | Tiếp thị, phân phối sản phẩm khu vực miền Trung. |
| Công ty con | HPC Industrial (hpcindustrial.com.vn) | 40 | Kinh doanh thiết bị công nghiệp. |
| **Tổng Cộng** | | **370** |  |

2.2.2 Bảng thu hoạch IP

* Xác định số lượng IP cần thiết Mỗi địa điểm cần có số lượng địa chỉ IP cho:
* Người dùng (Users): Địa chỉ IP cấp cho các thiết bị đầu cuối.
* Thiết bị mạng (Router, DC, Servers, Printers, IoT devices, etc.).
* Dự phòng cho tương lai: Tối thiểu 20-30% số lượng IP để mở rộng.
* Dựa trên dữ liệu thu thập, ta tính số lượng địa chỉ IP cần thiết như sau:

**Bảng 2.3: Bảng thu hoạch IP**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Địa điểm** | **Users** | **IP tối thiểu** | **IP mở rộng (30%)** | **Tổng IP cần thiết** |
| Hội sở chính HN | 120 | 140 | 42 | 182 |
| Nhà máy 1 (HN) | 60 | 70 | 21 | 91 |
| Nhà máy 2 (ĐN) | 60 | 70 | 21 | 91 |
| Chi nhánh HCM | 50 | 60 | 18 | 78 |
| Chi nhánh ĐN | 40 | 50 | 15 | 65 |
| Công ty HPC Industrial | 40 | 50 | 15 | 65 |

+ Hội sở chính có nhu cầu cao nhất, nên cần mạng /24 (256 IP) để đảm bảo dư địa mở rộng.

+ Các nhà máy và chi nhánh lớn chọn /25 (128 IP), giúp đáp ứng nhu cầu hiện tại và mở rộng.

+ Một số chi nhánh nhỏ chọn /26 (64 IP), tuy nhiên có thể cần nâng cấp lên /25 khi mở rộng.

* Bảng IP chi tiết :

Bảng 2.4: Bảng thu hoạch IP chi tiết

| **Địa điểm** | **Users** | **Mạng nội bộ** | **Subnet Mask** | **Router (In/Out)** | **DC IP** | **Dải IP User** |
| --- | --- | --- | --- | --- | --- | --- |
| Hội sở chính HN | 120 | 192.168.1.0/24 | 255.255.255.0  (256) | 192.168.1.1 / 172.16.1.2 | 192.168.1.10 | 192.168.1.20-200 |
| Nhà máy 1 (HN) | 60 | 192.168.2.0/25 | 255.255.255.128  (128) | 192.168.2.1 / 172.16.1.3 | 192.168.2.10 | 192.168.2.20-100 |
| Nhà máy 2 (ĐN) | 60 | 192.168.3.0/25 | 255.255.255.128  (128) | 192.168.3.1 / 172.16.1.4 | 192.168.3.10 | 192.168.3.20-100 |
| Chi nhánh HCM | 50 | 192.168.4.0/25 | 255.255.255.128  (128) | 192.168.4.1 / 172.16.1.5 | 192.168.4.10 | 192.168.4.20-90 |
| Chi nhánh ĐN | 40 | 192.168.5.0/25 | 255.255.255.128 (128) | 192.168.5.1 / 172.16.1.6 | 192.168.5.10 | 192.168.5.20-80 |
| Công ty HPC Industrial | 40 | 192.168.6.0/25 | 255.255.255.128 (128) | 192.168.6.1 / 172.16.1.7 | 192.168.6.10 | 192.168.6.20-80 |

CHƯƠNG 3: TRIỂN KHAI HỆ THỐNG ACTIVE DIRECTORY

3.1 Triển khai Forest và Domain

3.1.1 Cài đặt Windows Server trên môi trường ảo hóa VMware

Để triển khai hệ thống Active Directory, trước tiên cần cài đặt hệ điều hành Windows Server trên nền tảng ảo hóa. Trong đề tài này, phần mềm VMware Workstation được sử dụng nhằm tạo lập một môi trường mô phỏng thuận tiện và dễ quản lý.

Các bước thực hiện:

Bước 1: Mở phần mềm VMware Workstation, chọn “Create a New Virtual Machine”.

Bước 2: Lựa chọn “Installer disc image file (ISO)” và chỉ định đến tệp ISO của Windows Server (ví dụ: Windows Server 2016 hoặc 2019).

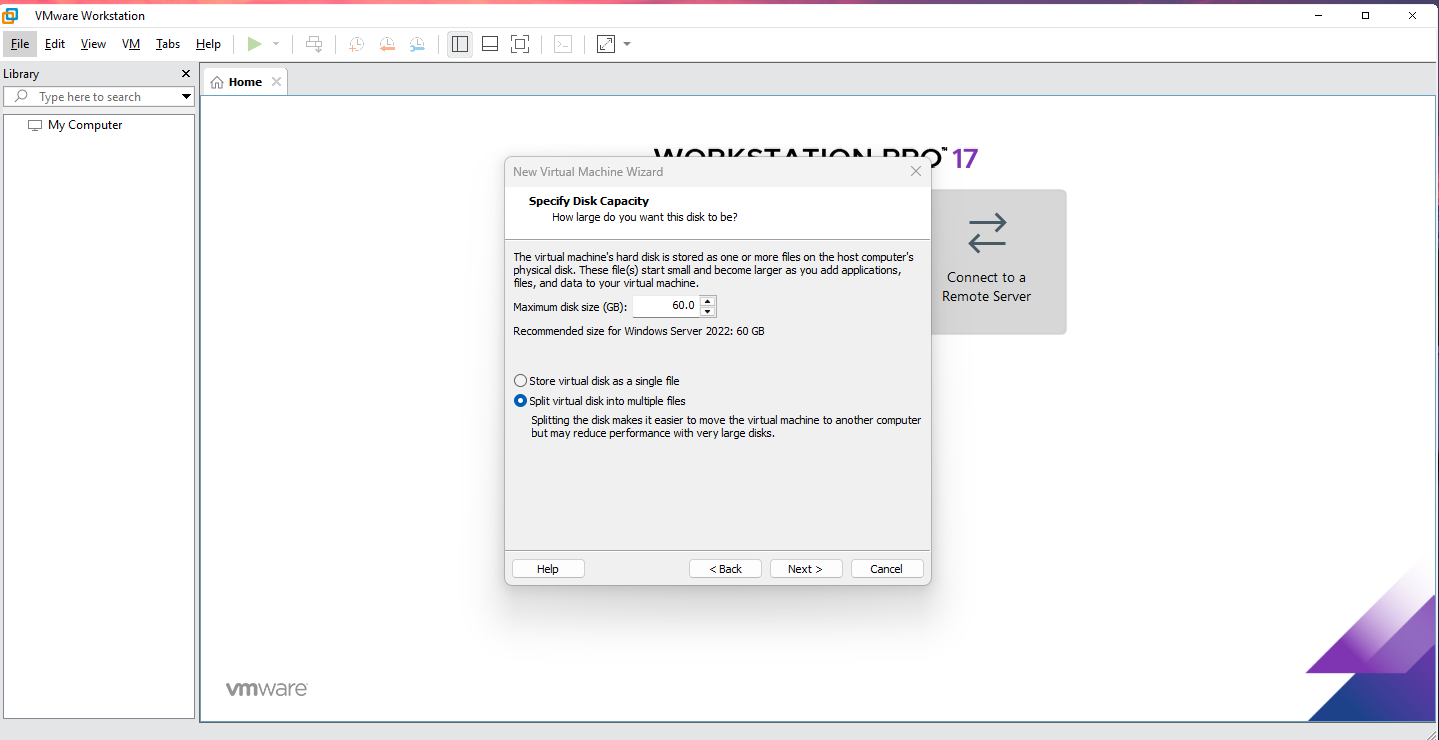
Bước 3: Đặt tên và thư mục lưu trữ máy ảo.

Bước 4: Cấu hình phần cứng cơ bản:

CPU: Tối thiểu 2 nhân (cores).

RAM: Tối thiểu 4GB.

Ổ cứng: 60GB trở lên (ưu tiên định dạng SCSI hoặc SATA).

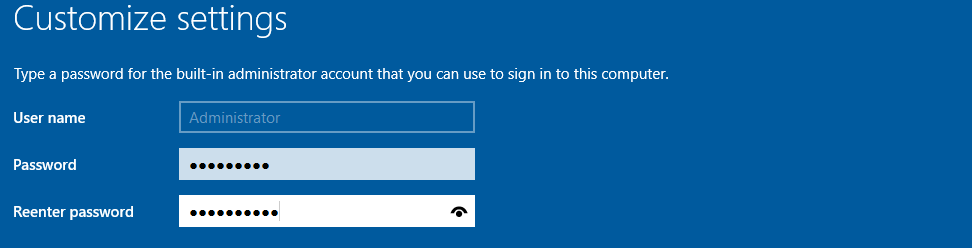


Hình 3.1: Cấu hình ổ cứng



Hình 3.2: Cấu hình Ram

Sau khi thiết lập, tiến hành cài đặt hệ điều hành Windows Server như cài đặt hệ điều hành thông thường và thiết lập mật khẩu cho tài khoản quản trị viên (Administrator).



Hình 3.3: Thiết lập tài khoản quản trị viên

3.1.2 Cấu hình địa chỉ IP tĩnh cho máy chủ

Sau khi hoàn tất cài đặt hệ điều hành, cần thiết lập địa chỉ IP tĩnh để đảm bảo tính ổn định khi kết nối mạng:

Mở cửa sổ Network Connections.

Cấu hình như sau:

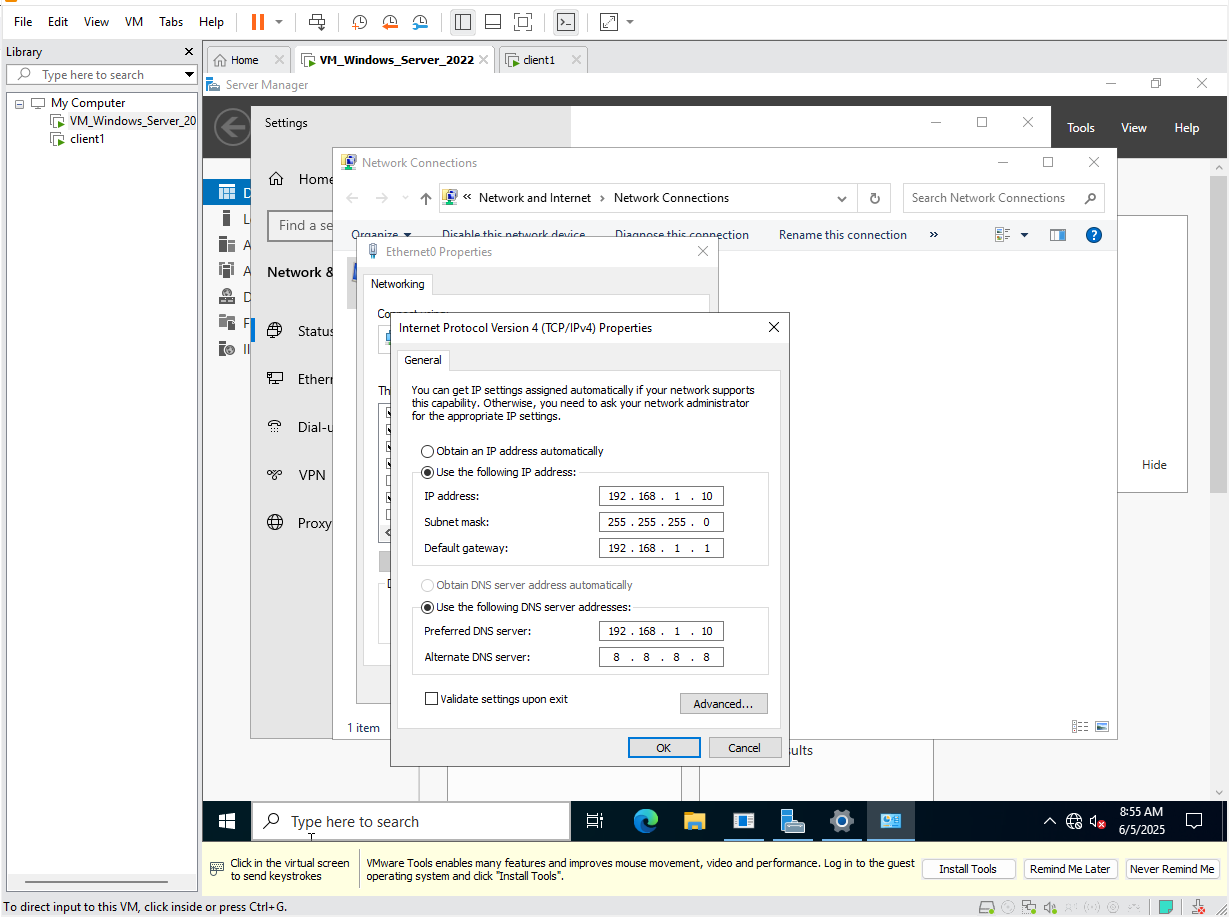
IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

Preferred DNS: 192.168.1.10

Alternate DNS: 8.8.8.8



Hình 3.4: Cấu hình DNS

Việc thiết lập IP tĩnh là điều kiện tiên quyết để triển khai dịch vụ Active Directory Domain Services một cách hiệu quả.

3.1.3 Cài đặt dịch vụ Active Directory Domain Services (AD DS)

Mở Server Manager → chọn Add Roles and Features.

Chọn kiểu cài đặt: Role-based or feature-based installation.

Ở mục Server Roles, tick chọn Active Directory Domain Services.

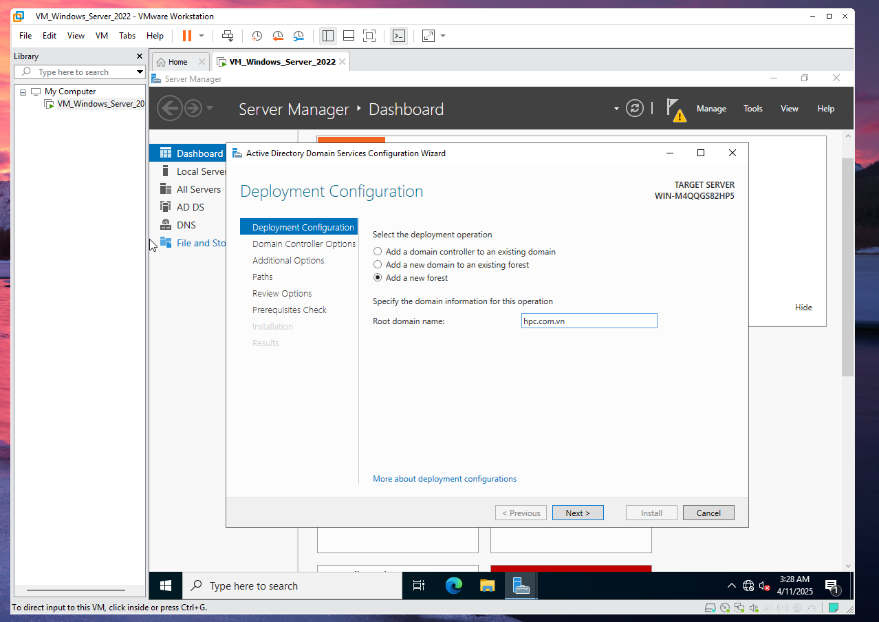
Giữ nguyên các tùy chọn mặc định ở phần Features, sau đó nhấn Install để cài đặt.

3.1.4 Thăng cấp máy chủ thành Domain Controller

Sau khi cài đặt xong AD DS, cần cấu hình để máy chủ trở thành Domain Controller:

Nhấp vào cảnh báo "Promote this server to a domain controller" trong Server Manager.

Chọn Add a new forest, nhập tên miền gốc, ví dụ: hpc.com.vn.



Hình 3.5: Tạo tên miền

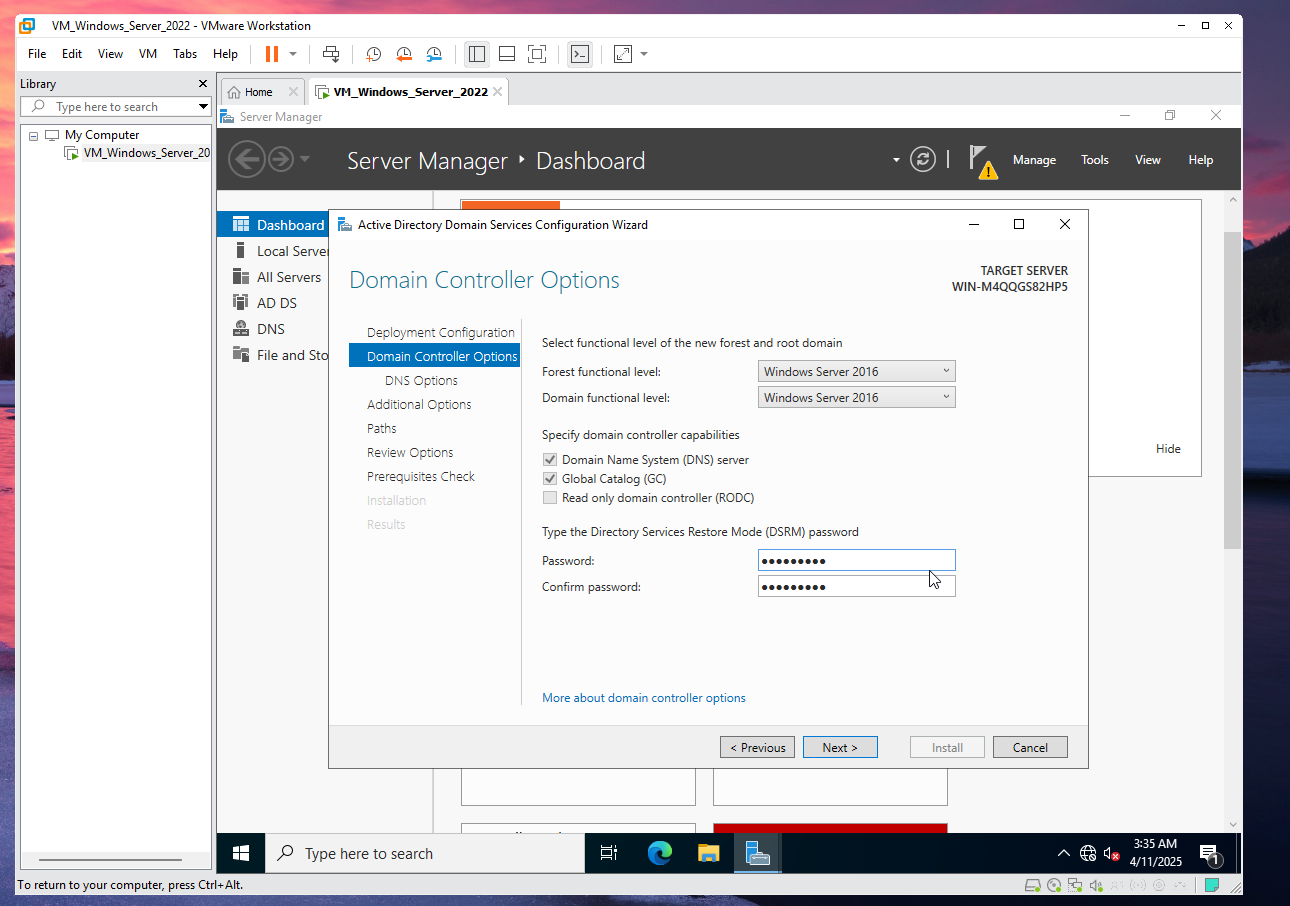
Chọn cấp độ chức năng: Windows Server 2016 (cả Forest và Domain).

Tick chọn:

DNS Server

Global Catalog (GC)

Thiết lập mật khẩu khôi phục DSRM.



Hình 3.6: Cấu hình Domain Controller

Hệ thống sẽ kiểm tra các điều kiện và tiến hành cài đặt. Sau khi hoàn tất, máy chủ sẽ tự khởi động lại và trở thành một Domain Controller chính thức trong hệ thống.

3.2 Cấu hình Organizational Unit (OU)

Organizational Unit (OU) là đơn vị tổ chức trong Active Directory, cho phép phân nhóm người dùng, máy tính hoặc nhóm khác nhau nhằm dễ dàng quản lý và áp dụng chính sách.

3.2.1 Mở công cụ Active Directory Users and Computers

Vào Start → gõ “Active Directory Users and Computers” → mở giao diện quản lý ADUC.

3.2.2 Tạo OU chính và các OU con

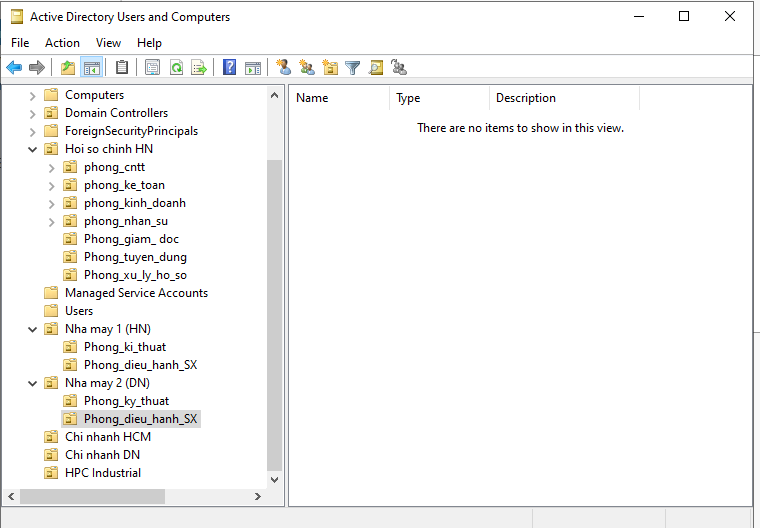
Tại giao diện cây thư mục, nhấp chuột phải vào tên miền hpc.com.vn.

Chọn New → Organizational Unit → đặt tên là Hội sở chính.

Đảm bảo tùy chọn “Protect container from accidental deletion” được bật.

Tiếp theo, tạo các OU con như:

* Phòng Kinh doanh
* Phòng Kế toán
* Phòng Nhân sự
* Phòng CNTT



Hình 3.7: Tạo các OU

Việc phân chia OU hợp lý giúp tổ chức dễ dàng triển khai các chính sách bảo mật, kiểm soát truy cập và tự động hóa quản lý.

3.3 Tích hợp Domain Name System (DNS) vào Active Directory

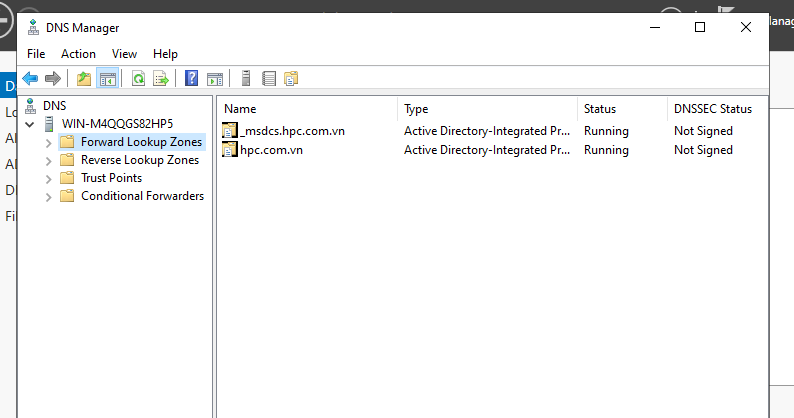
DNS đóng vai trò quan trọng trong hệ thống Active Directory, giúp phân giải tên miền thành địa chỉ IP và đảm bảo các thành phần trong mạng hoạt động ổn định.

3.3.1 Kiểm tra Forward Lookup Zones

Mở DNS Manager trong Server Manager → Tools → DNS.

Mở rộng tên máy chủ DNS → Forward Lookup Zones.

Xác minh zone trùng khớp với domain đã cấu hình (ví dụ: hpc.com.vn).



Hình 3.8: Kiểm tra zone

3.3.2 Thêm bản ghi Host (A Record)

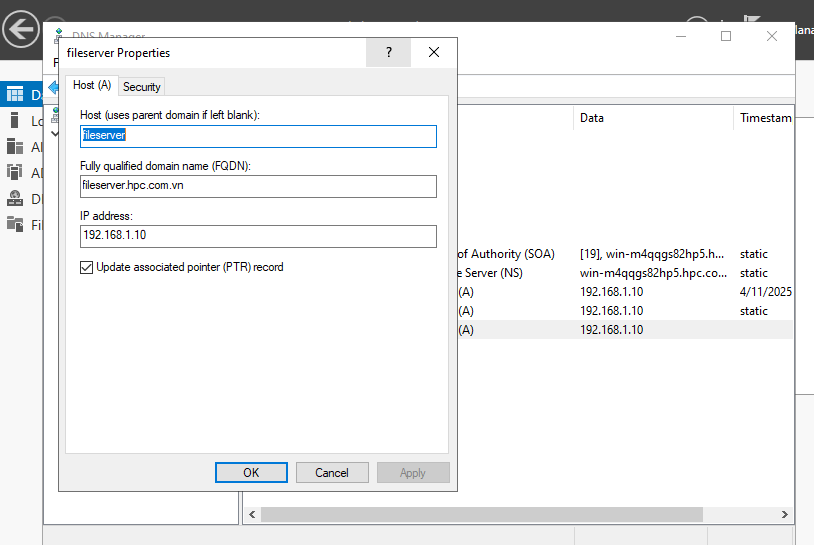
Nhấp chuột phải vào tên miền hpc.com.vn → chọn New Host (A or AAAA).

Nhập:

Name: tên máy chủ (ví dụ: fileserver)

IP Address: 192.168.1.10

Tick chọn “Create associated pointer (PTR) record” nếu cần.



Hình 3.9: Cấu hình New Host

Mỗi bản ghi A tương ứng với một thiết bị hoặc dịch vụ trong mạng nội bộ, giúp người dùng truy cập thuận tiện thông qua tên miền thân thiện.

Việc tích hợp DNS vào AD không chỉ hỗ trợ truy cập dễ dàng mà còn là thành phần thiết yếu để hệ thống Active Directory hoạt động đúng cách.

3.4 Cấu hình IIS Web Server (HTTP và HTTPS) trên Windows Server 2016

Trong mục này, hệ thống web server được triển khai trên nền tảng Windows Server 2016 sử dụng IIS (Internet Information Services) để phục vụ truy cập qua HTTP và HTTPS. Dưới đây là các bước cấu hình chi tiết:

3.4.1 Cài đặt dịch vụ IIS

Trên máy chủ Windows Server 2016, thực hiện cài đặt IIS như sau:

* Mở Server Manager → chọn Add roles and features.
* Chọn kiểu cài đặt Role-based or feature-based installation.
* Chọn server đích.
* Trong danh sách Server Roles, đánh dấu chọn Web Server (IIS).
* Tiếp tục theo wizard và nhấn Install để hoàn tất cài đặt.

3.4.2 Tạo Website với giao thức HTTP

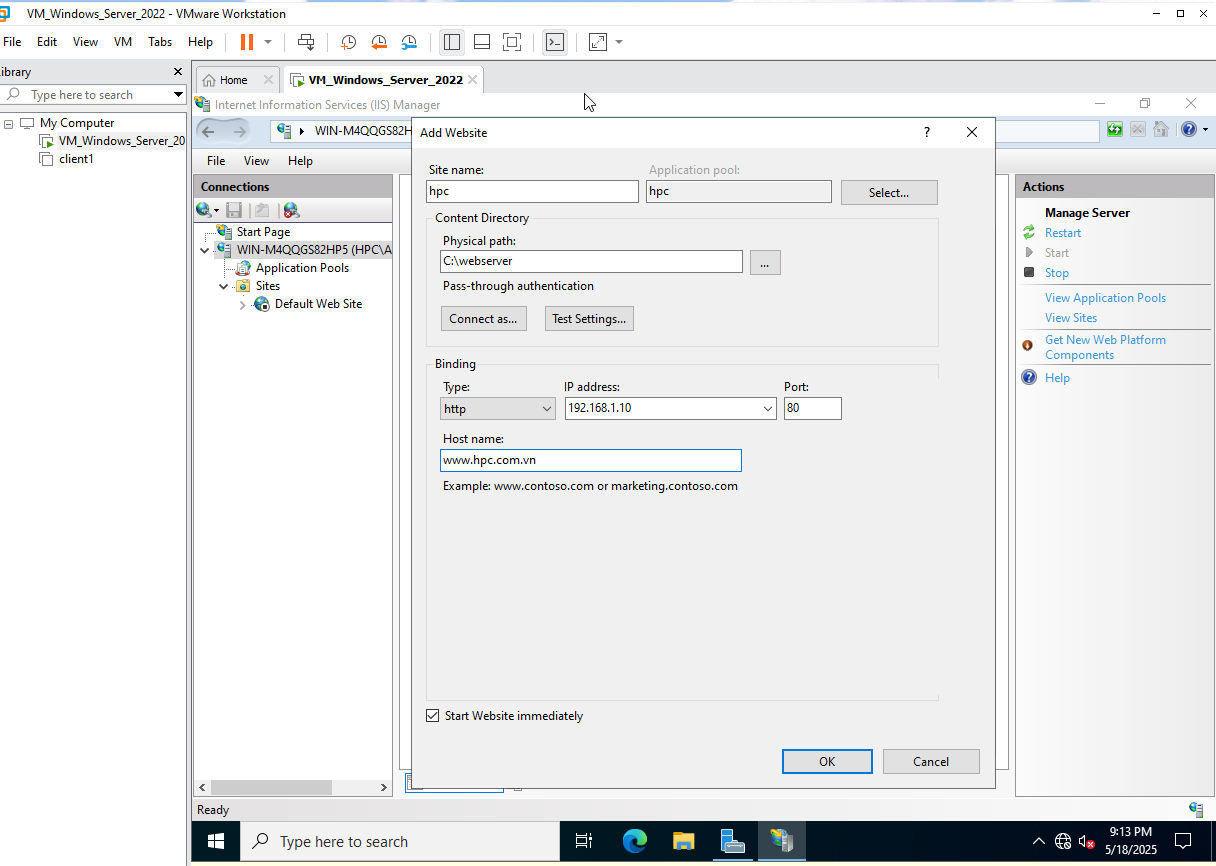
Sau khi IIS được cài đặt, tiến hành khởi tạo website trên cổng HTTP:

Mở Internet Information Services (IIS) Manager.

Chuột phải vào mục Sites → chọn Add Website.

Điền các thông tin cấu hình như sau:

* Site name: hpc
* Physical path: C:\webserver
* Binding:
* Type: http
* IP address: 192.168.1.10
* Port: 80
* Host name: www.hpc.com.vn



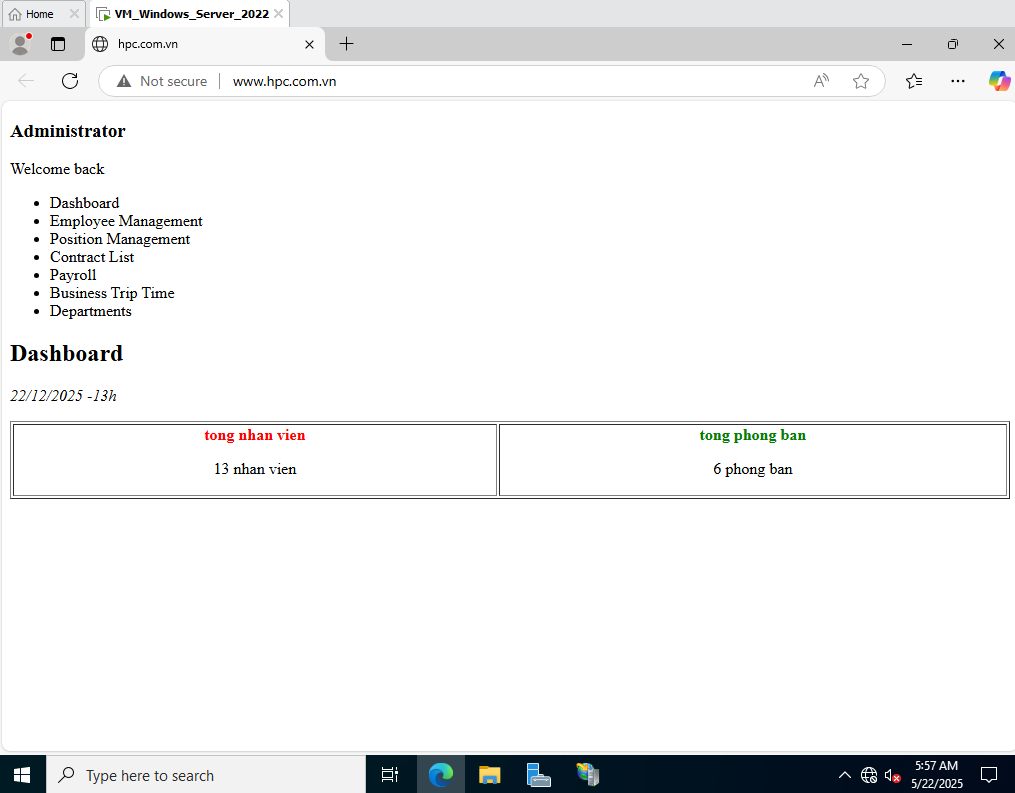
Hình 3.10:Cấu hình Website

3.4.3 Kiểm tra hoạt động Web Server

Sau khi cấu hình, người dùng có thể kiểm tra truy cập từ máy trạm trong mạng LAN:

Truy cập HTTP: http://www.hpc.com.vn hoặc http://192.168.1.10

Truy cập HTTPS: https://www.hpc.com.vn



Hình 3.11:Kết quả hoạt động Web Server

3.5 Chính sách bảo mật

Việc thiết lập các chính sách bảo mật tài khoản là bước quan trọng nhằm bảo vệ hệ thống Active Directory trước các nguy cơ truy cập trái phép. Các chính sách này bao gồm yêu cầu mật khẩu mạnh, thời hạn mật khẩu và khóa tài khoản sau nhiều lần đăng nhập sai, giúp giảm thiểu rủi ro mất an toàn thông tin.

* Mục tiêu:
  + Đảm bảo người dùng sử dụng mật khẩu mạnh và thay đổi định kỳ.
  + Hạn chế hành vi dò đoán mật khẩu bằng cách khóa tài khoản khi đăng nhập sai nhiều lần.
  + Tăng cường an ninh cho hệ thống máy chủ và toàn bộ mạng nội bộ.

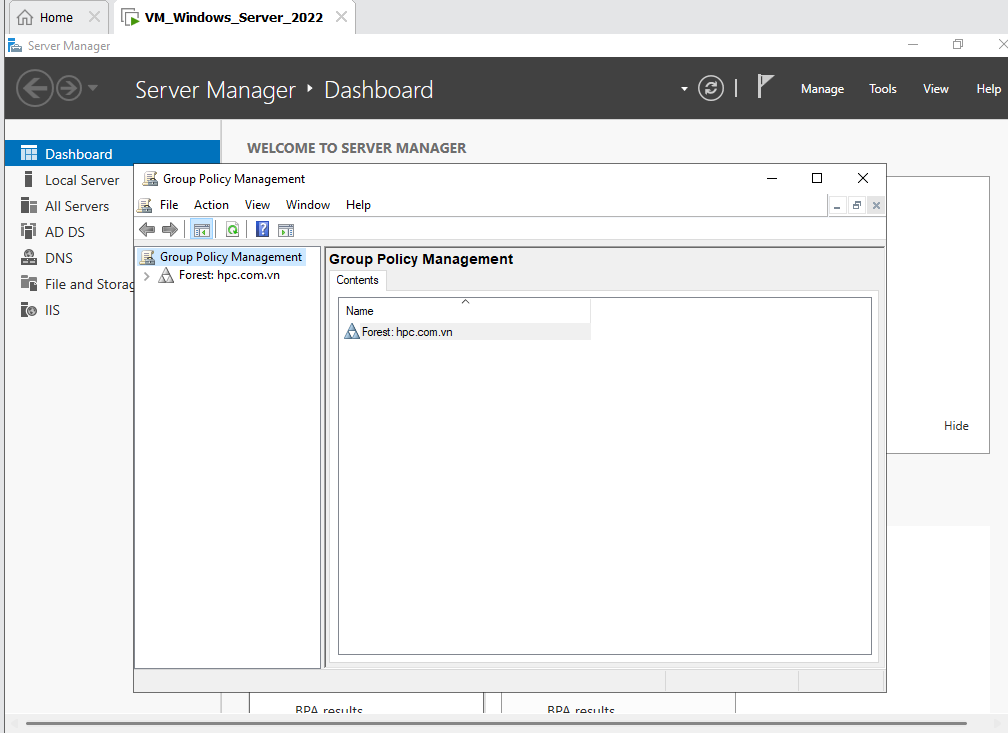
3.5.1 Mở Group Policy Management

Bước 1: Vào Start → Gõ Group Policy Management → Mở công cụ.

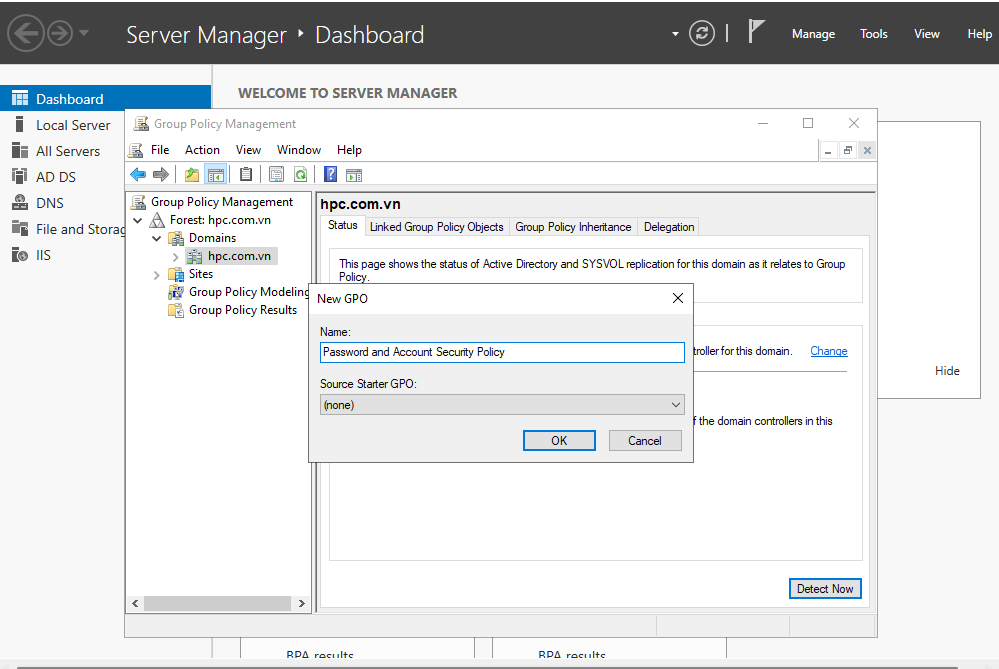
Bước 2: Trong cửa sổ Group Policy Management, mở cây điều hướng:  
Forest → Domains → yourdomain.local

Bước 3: Nhấp chuột phải vào tên miền → Chọn Create a GPO in this domain, and Link it here…

Đặt tên GPO là: Password and Account Security Policy → Nhấn OK.



Hình 3.12:Mở Group Policy Management



Hình 3.13:Password and Account Security Policy

3.5.2 Cấu hình chính sách mật khẩu

Bước 1: Nhấp chuột phải vào GPO vừa tạo → Chọn Edit.

Bước 2: Truy cập theo đường dẫn:

Computer Configuration →

Windows Settings →

Security Settings →

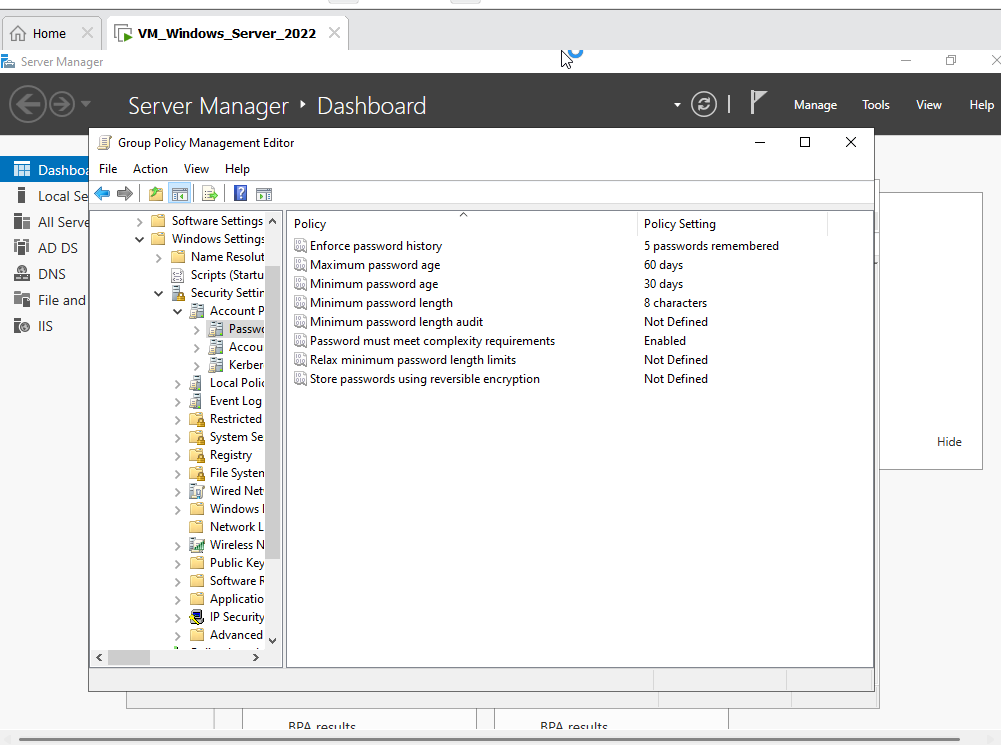
Account Policies →

Password Policy

Bước 3: Cấu hình các chính sách mật khẩu theo bảng sau:

| **Chính sách** | **Mô tả** | **Giá trị khuyến nghị** |
| --- | --- | --- |
| Enforce password history | Ghi nhớ các mật khẩu đã dùng trước đó | 5–10 lần |
| Maximum password age | Mật khẩu hết hạn sau số ngày | 60–90 ngày |
| Minimum password age | Khoảng thời gian tối thiểu trước khi đổi mật khẩu mới | 1 ngày |
| Minimum password length | Độ dài tối thiểu của mật khẩu | 8–12 ký tự |
| Password must meet complexity requirements | Yêu cầu mật khẩu phải gồm ký tự đặc biệt, chữ hoa, chữ thường, số | Enabled |

* Sau mỗi thay đổi, nhấn OK để lưu lại.

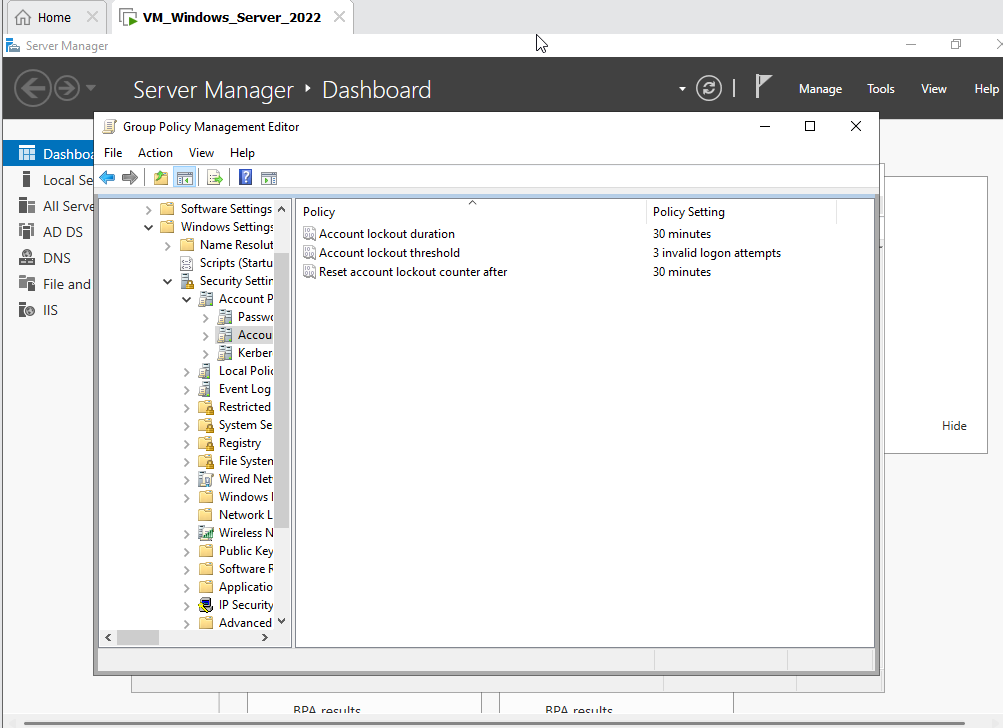


Hình 3.14:Cấu hình chính sách mật khẩu

3.5.3 Cập nhật chính sách

Trên máy client hoặc máy ảo đã join domain, thực hiện cập nhật chính sách bằng lệnh:

* + - Hoặc khởi động lại máy để đảm bảo chính sách được áp dụng.

****

Hình 3.15:Cấu hình chính sách khóa tài khoản

3.5.4 Cấm sử dụng USB

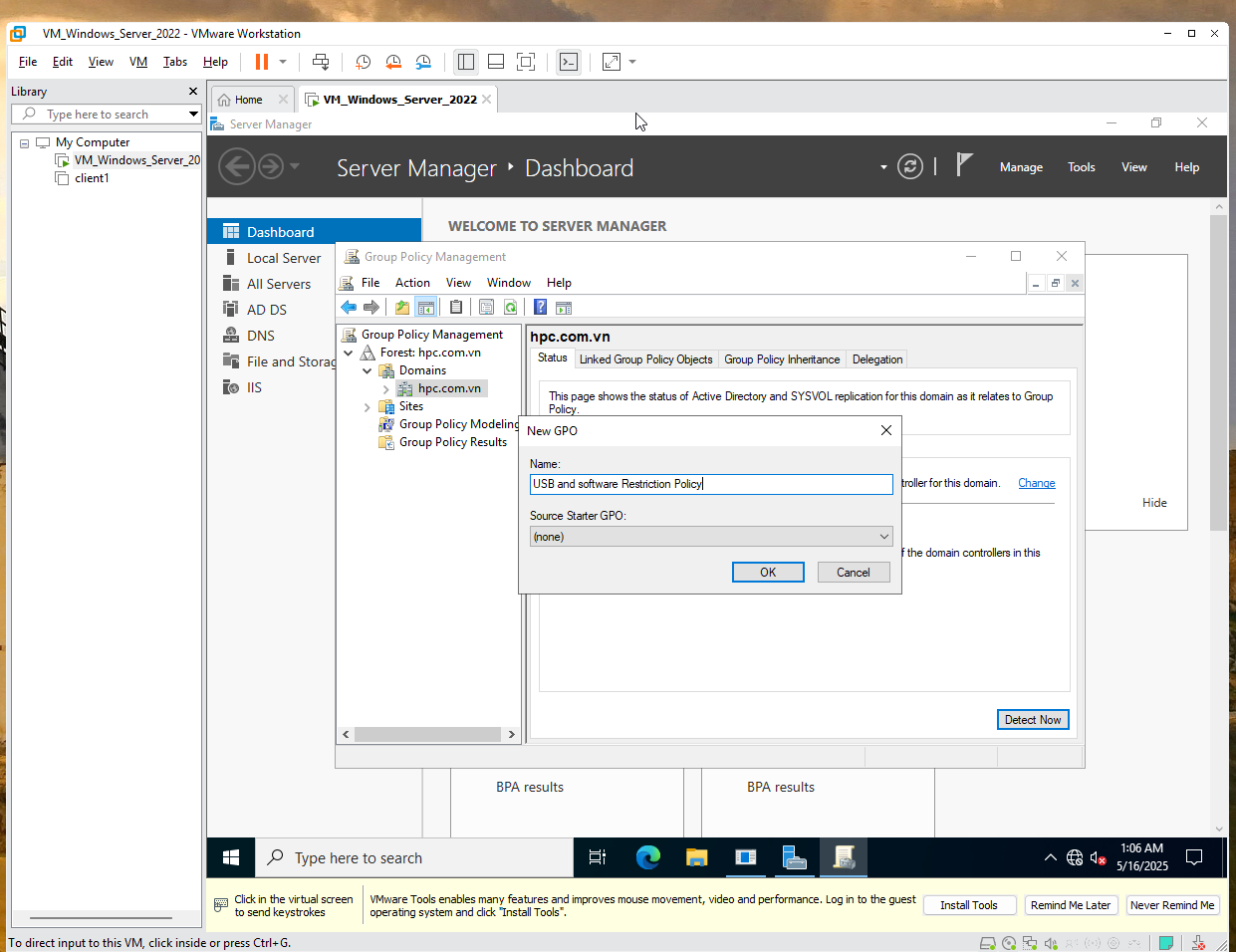
Để đảm bảo an toàn dữ liệu và ngăn chặn việc sao chép, truy xuất trái phép thông qua thiết bị USB, chính sách GPO được áp dụng để vô hiệu hóa toàn bộ quyền truy cập vào thiết bị lưu trữ ngoài.

Các bước thực hiện:

🔹 Bước 1: Trên máy chủ domain controller, mở Group Policy Management từ menu Start.

🔹 Bước 2: Trong cây quản lý chính, điều hướng đến: Forest: hpc.com.vn → Domains → hpc.com.vn

🔹 Bước 3: Chuột phải vào domain hpc.com.vn, chọn Create a GPO in this domain, and Link it here... Đặt tên GPO: USB and software Restriction Policy.

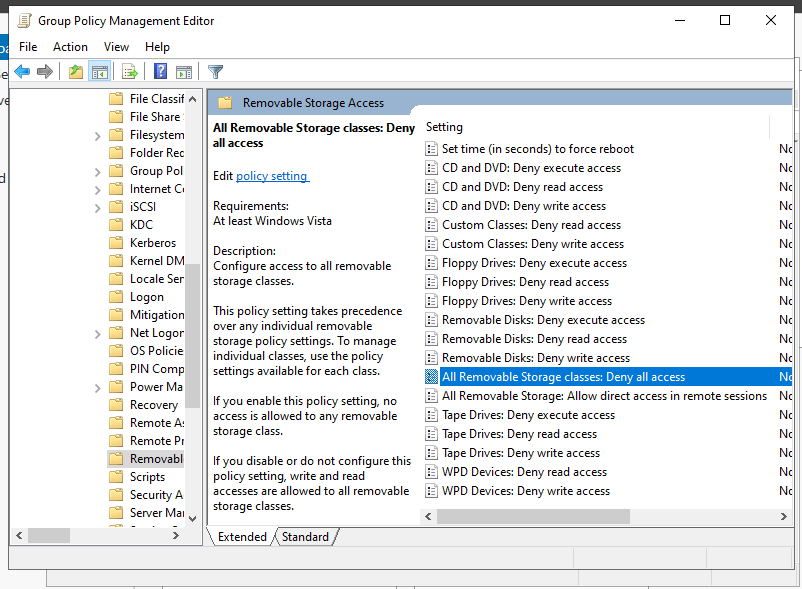


Hình 3.16:USB and software Restriction Policy

🔹 Bước 4: Chuột phải vào GPO vừa tạo → chọn Edit.

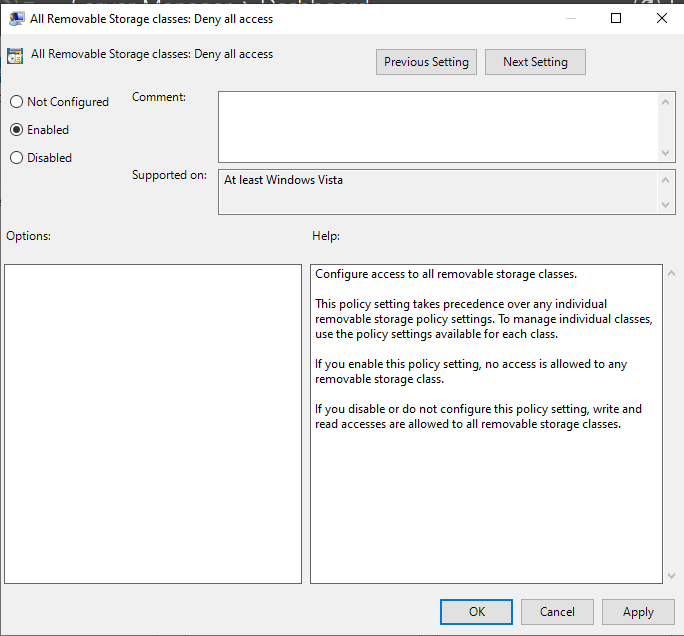
🔹 Bước 5: Trong cửa sổ Group Policy Management Editor, điều hướng:  
Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access

🔹 Bước 6: Tại đây, chọn All Removable Storage classes: Deny all access, sau đó nhấn đúp chuột để mở cấu hình.



Hình 3.17:Thiết lập All Removable Storage classes

🔹 Bước 7: Trong cửa sổ cấu hình, chọn Enabled → Nhấn OK để áp dụng.



Hình 3.18: Hoàn tất thiết lập All Removable Storage classes

3.5.5 Cấu hình xác thực và phân quyền truy cập Web Server IIS

Sau khi hoàn tất triển khai dịch vụ IIS và cấu hình website nội bộ với tên miền http://mycompany.hpc.com.vn, cần tiến hành thiết lập cơ chế xác thực và phân quyền truy cập để đảm bảo an toàn, bảo mật hệ thống. Các bước thực hiện cụ thể như sau:

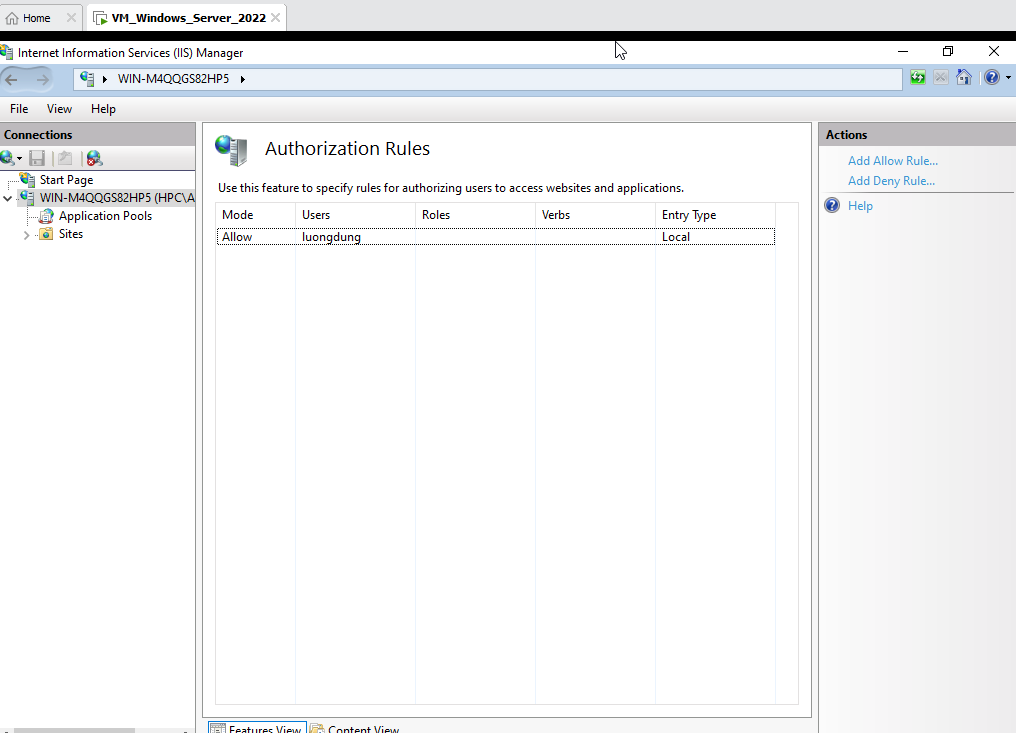
Mở công cụ IIS Manager:

* Trên Windows Server 2016, mở Internet Information Services (IIS) Manager.
* Điều hướng đến website đã tạo: Sites → mycompany.hpc.com.vn.
* Cấu hình cơ chế xác thực người dùng (Authentication):
* Chọn mục Authentication trong giao diện quản lý tính năng.

Tắt chế độ Anonymous Authentication nhằm ngăn chặn người dùng không xác định truy cập trái phép vào website.

Bật chế độ Windows Authentication để cho phép xác thực thông qua tài khoản nội bộ hoặc domain. Điều này giúp đảm bảo chỉ những người dùng có tài khoản Windows hợp lệ mới được phép truy cập.

* Thiết lập phân quyền truy cập (Authorization Rules):
  + Quay lại giao diện quản lý website, chọn mục Authorization Rules.
  + Xóa các rule mặc định, đặc biệt là “Allow All Users”
  + Thêm rule cho phép truy cập (Allow Rule):
  + Chọn “Add Allow Rule”.
  + Chỉ định nhóm người dùng hoặc tài khoản cụ thể
  + Rule này cho phép chỉ nhóm được chỉ định mới có quyền truy cập.



Hình 3.19: Phân quyền truy cập Web Server IIS

3.5.6 Theo dõi hoạt động hệ thống (Audit Logs)

Việc theo dõi hoạt động hệ thống nhằm mục đích ghi nhận các hành vi quan trọng như: đăng nhập, truy cập tệp tin, thay đổi chính sách, thao tác với tài khoản người dùng,… Các hoạt động này được ghi lại trong nhật ký bảo mật (Security Logs) thông qua việc cấu hình Audit Policy. Các bước thực hiện như sau:

Bước 1: Mở công cụ Group Policy Management

Trên máy chủ Windows Server (đã cài Active Directory), nhấn Start → tìm và mở Group Policy Management (gpmc.msc).

Điều hướng đến domain hoặc OU chứa các máy cần giám sát.

Bước 2: Tạo và chỉnh sửa một GPO mới

Chuột phải vào domain hoặc OU cần áp dụng chính sách → chọn Create a GPO in this domain, and Link it here....

Đặt tên (ví dụ: AuditPolicy-GPO) → nhấn OK.

Chuột phải vào GPO vừa tạo → chọn Edit.

Bước 3: Bật các chính sách giám sát (Audit Policy)

Tại cửa sổ Group Policy Management Editor:

Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Audit Policy

Kích hoạt các chính sách sau:

|  |  |
| --- | --- |
| Tên chính sách | Thiết lập khuyến nghị |
| Audit account logon events | Success, Failure |
| Audit logon events | Success, Failure |
| Audit account management | Success, Failure |
| Audit object access | Success, Failure |
| Audit policy change | Success, Failure |
| Audit privilege use | Success |

Nhấn Apply sau mỗi thay đổi.

Bước 4: Cập nhật Group Policy trên máy cần theo dõi

Khởi động lại máy nếu cần để chính sách được áp dụng đầy đủ.

Bước 5: Xem và lọc nhật ký hoạt động hệ thống

Trên máy chủ hoặc máy được theo dõi, mở Event Viewer:

Nhấn Start → gõ eventvwr.msc → Enter.

Trong Event Viewer:

Điều hướng đến:

Windows Logs → Security

Tại đây, các sự kiện được ghi lại với mã (Event ID) cụ thể:

|  |  |  |
| --- | --- | --- |
| Hoạt động giám sát | Event ID | Mô tả |
| Đăng nhập thành công | 4624 | User đăng nhập hợp lệ |
| Đăng nhập thất bại | 4625 | Nhập sai mật khẩu, lỗi đăng nhập |
| Truy cập file hoặc thư mục | 4663 | Truy cập đến đối tượng giám sát |
| Tạo tài khoản người dùng | 4720 | Tài khoản mới được tạo |
| Xóa tài khoản | 4726 | Tài khoản bị xóa |
| Thay đổi chính sách bảo mật | 4739 | Thay đổi thiết lập GPO/policy |
| Đăng nhập qua dịch vụ mạng | 4776 | Đăng nhập qua dịch vụ Kerberos |

Bước 6: (Tùy chọn) Theo dõi truy cập thư mục cụ thể

Nếu muốn giám sát truy cập vào một thư mục nhất định:

Chuột phải vào thư mục → Properties.

Tab Security → Advanced → Tab Auditing → Add.

Chọn user/group cần theo dõi (ví dụ: Everyone).

Chọn quyền cần giám sát như: Read, Write, Delete, ...

Apply và xác nhận.

Sau đó kiểm tra Event Viewer với Event ID 4663 để xem các hành động liên quan.

3.5.7 Rủi ro khi không triển khai chính sách chặt chẽ

Việc không triển khai hoặc triển khai không đầy đủ các chính sách bảo mật trong hệ thống Active Directory có thể dẫn đến nhiều rủi ro nghiêm trọng, ảnh hưởng trực tiếp đến an toàn thông tin và hoạt động ổn định của doanh nghiệp. Một số rủi ro tiềm ẩn bao gồm:  
Nếu không áp dụng các chính sách kiểm soát truy cập như GPO, phân quyền truy cập thư mục, hoặc không sử dụng xác thực đa yếu tố (MFA), các tài khoản người dùng có thể bị truy cập trái phép. Điều này dẫn đến nguy cơ cao về mất dữ liệu, rò rỉ thông tin nhạy cảm như hồ sơ nhân sự, tài liệu kế toán, và thông tin nội bộ quan trọng.

Khi không khóa cổng USB hoặc không giới hạn quyền cài đặt phần mềm, nhân viên có thể vô tình hoặc cố ý sử dụng thiết bị ngoài để đánh cắp dữ liệu hoặc đưa mã độc vào hệ thống. Đồng thời, việc thiếu các chính sách firewall, antivirus hoặc thiếu cập nhật bản vá bảo mật có thể tạo điều kiện cho tin tặc tấn công từ bên ngoài.

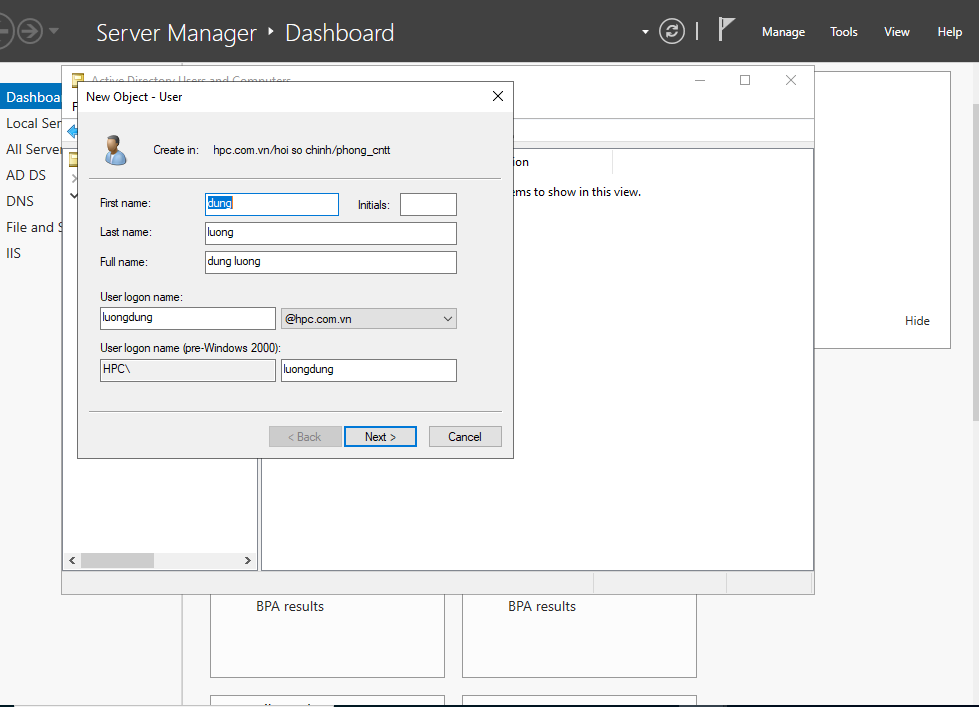
Nếu không cấu hình chính sách ghi nhận nhật ký hoạt động (Audit Policy), quản trị viên sẽ không có đủ thông tin để điều tra khi xảy ra sự cố như mất dữ liệu, truy cập bất thường, hoặc hành vi nghi ngờ. Việc này khiến thời gian phản ứng và khắc phục kéo dài, gây gián đoạn vận hành.

Nhiều doanh nghiệp hiện nay phải tuân thủ các tiêu chuẩn bảo mật như ISO 27001, GDPR, NIST,... Nếu không thiết lập chính sách bảo mật đầy đủ, doanh nghiệp có thể bị xử phạt. Việc không kiểm soát triệt để tài nguyên và truy cập khiến hệ thống dễ bị quá tải, dẫn đến hiệu suất giảm, lỗi phần mềm, hoặc tệ hơn là phải khôi phục toàn bộ hệ thống sau sự cố – gây lãng phí thời gian và nguồn lực.

3.6 Kết quả sau khi tạo thành công chính sách bảo mật mật khẩu và nối máy client vào domain hpc.com.vn

3.6.1 Tạo người dùng mới trên Domain Controller

* Trong giao diện Active Directory Users and Computers, người dùng mới có tên:
* Họ và tên: Dũng Lương
* Tên đăng nhập (User logon name): luongdung@hpc.com.vn
* Ảnh minh họa thể hiện bước khởi tạo người dùng và gán tên đăng nhập theo đúng domain được cấu hình (hpc.com.vn).



Hình 3.20:Tạo người dùng mới

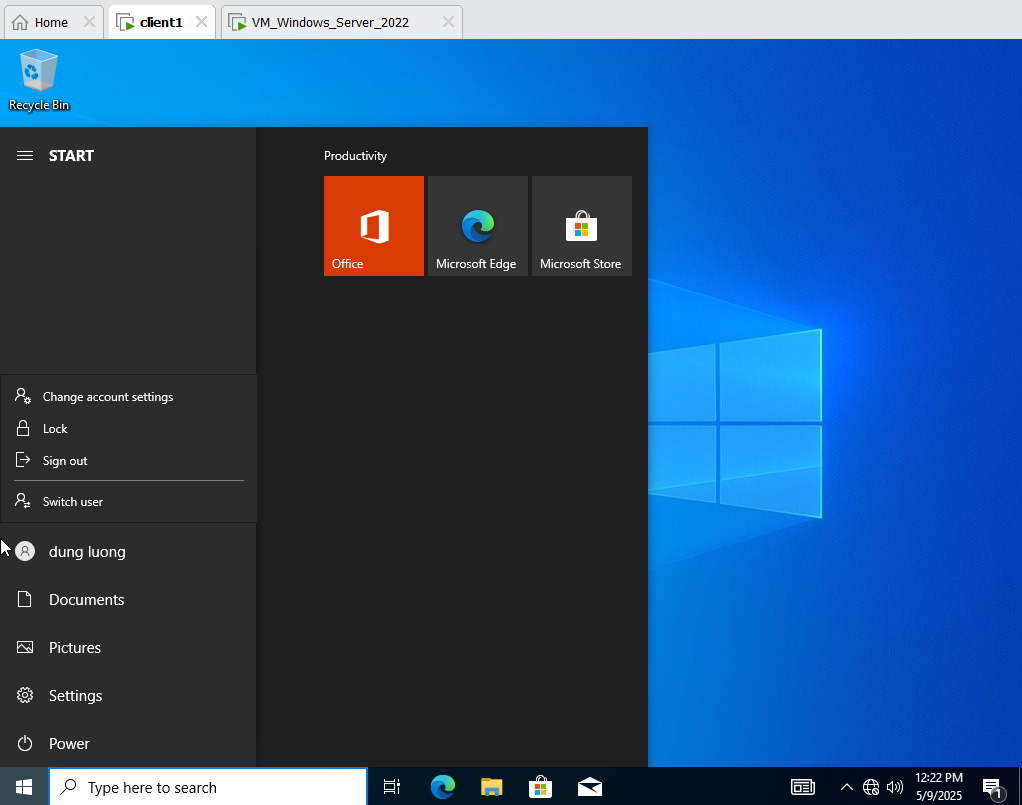
3.6.2 Tạo và nối máy trạm (client) vào domain hpc.com.vn

Một máy client đã được cài đặt hệ điều hành Windows và thực hiện nối domain thành công:

Tên domain: hpc.com.vn

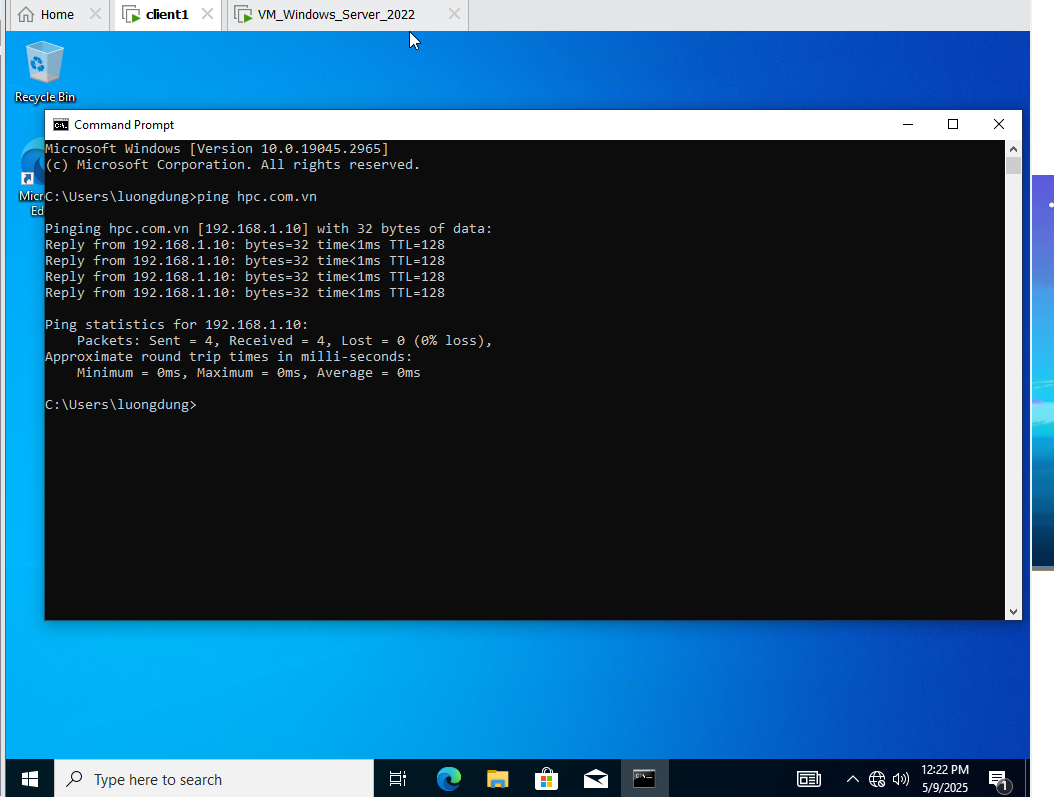
Tình trạng kết nối: Thành công, máy client đã nhận Group Policy từ domain controller.

Sau khi restart máy, người dùng luongdung có thể đăng nhập vào domain bằng tài khoản vừa tạo.



Hình 3.21:Tạo và nối máy trạm

* Đăng nhập bằng tài khoản luongdung@hpc.com.vn trên máy client thành công.
* Group Policy được đồng bộ hóa thành công từ DC xuống máy client.



Hình 3.22:Kiểm tra xác minh

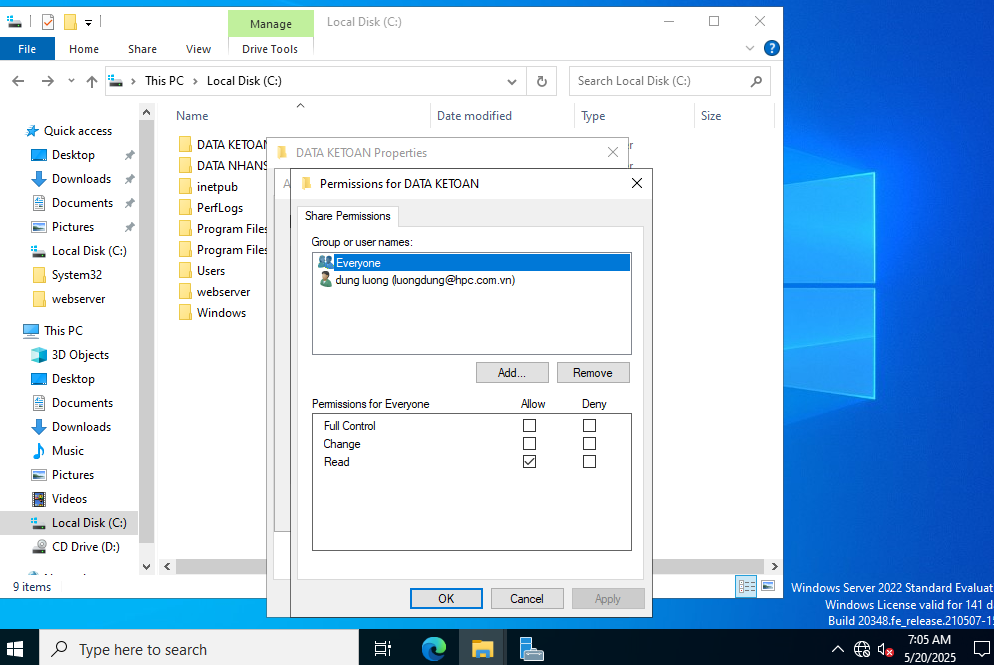
3.6.3 Chia sẻ file giữa máy chủ với client

Thiết lập chia sẻ thư mục trên máy chủ Windows Server 2022 và truy cập từ máy client trong cùng hệ thống mạng (domain hoặc LAN).

* Các bước thực hiện :
* Tạo và cấu hình thư mục chia sẻ trên máy chủ:
* Trên máy chủ Windows Server 2022, tạo các thư mục chia sẻ tại ổ đĩa hệ thống (ví dụ: DATA KETOAN, DATA NHANSU).
* Cấu hình chia sẻ bằng cách chuột phải vào thư mục → Properties → tab Sharing → chọn Advanced Sharing → đánh dấu Share this folder.
* Phân quyền truy cập :

Trong tab Permissions, thêm các nhóm người dùng được phép truy cập (ví dụ: Everyone hoặc tài khoản cụ thể như [dung.luong@hpc.com.vn](mailto:dung.luong@hpc.com.vn)).

* Cấp quyền thích hợp, ví dụ:
* Read cho quyền chỉ đọc.
* Change cho phép sửa/xóa file.
* Full Control cho toàn quyền quản lý thư mục.



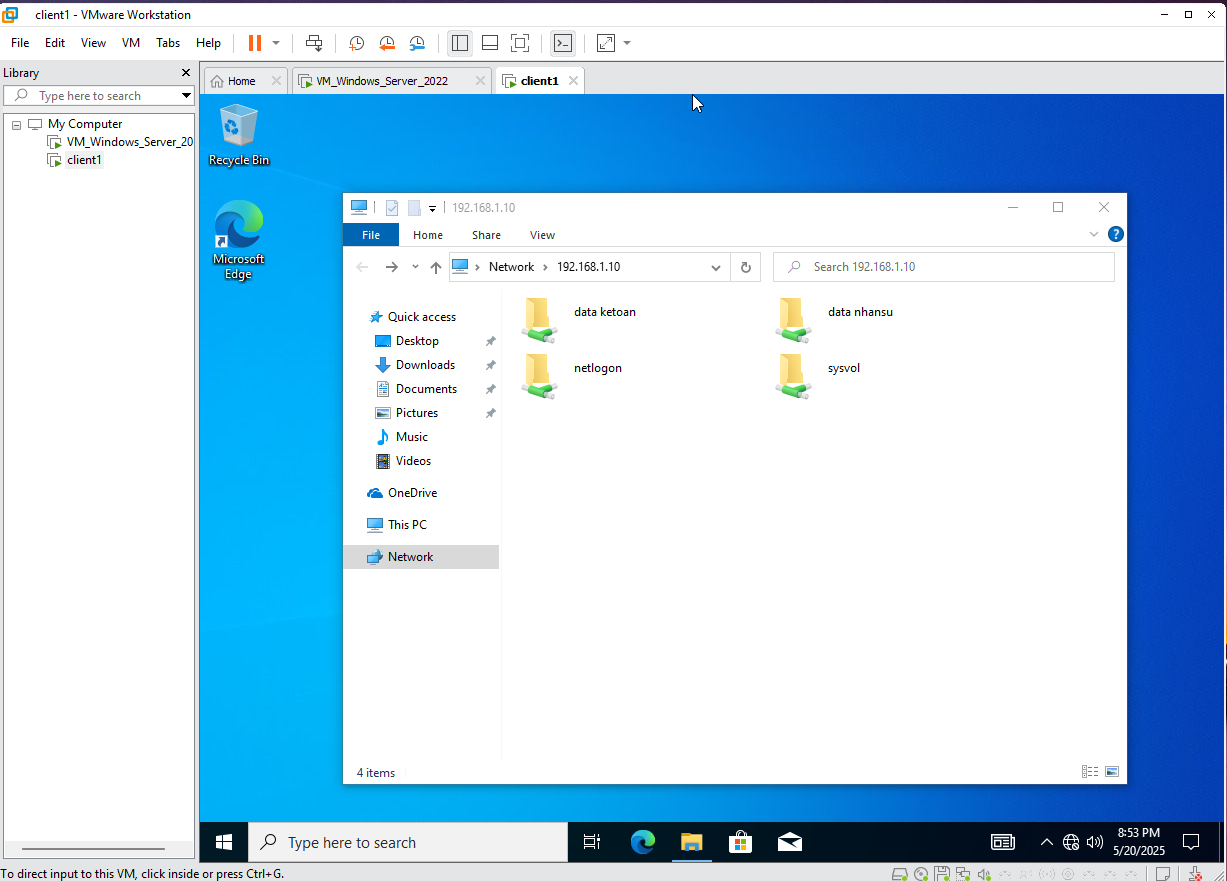
Hình 3.23:Cấp quyền thích hợp

* Client truy cập thư mục chia sẻ:

Trên máy client client1, sử dụng địa chỉ IP của máy chủ để truy cập:  
Mở File Explorer → gõ đường dẫn \\192.168.1.10 → nhấn Enter.

Các thư mục chia sẻ như DATA KETOAN, DATA NHANSU, NETLOGON, SYSVOL sẽ hiển thị.

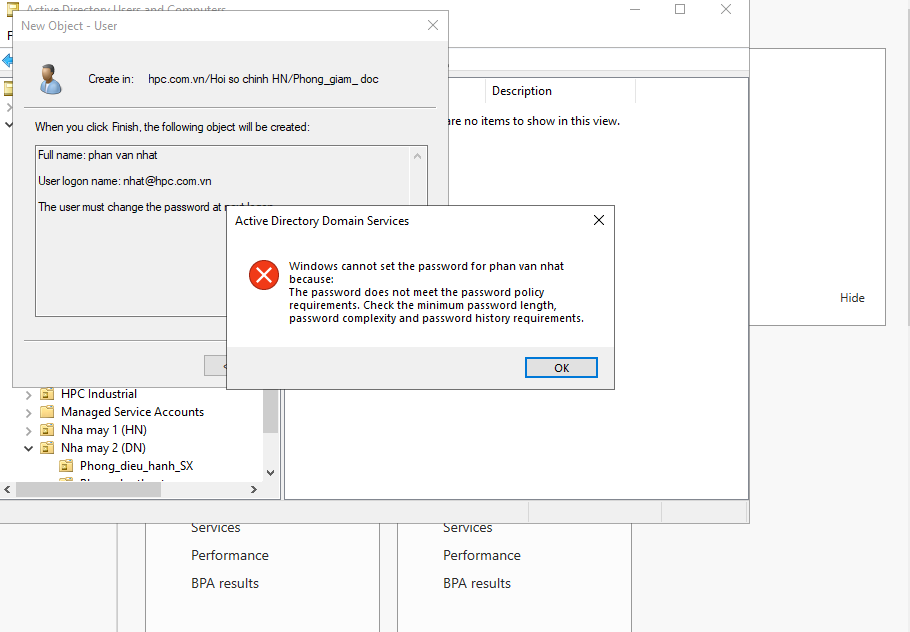
Người dùng có thể truy cập, xem hoặc chỉnh sửa dữ liệu tùy theo quyền được cấp.



Hình 3.24:Client truy cập thư mục chia sẻ

3.6.4 Kiểm tra chính sách mật khẩu

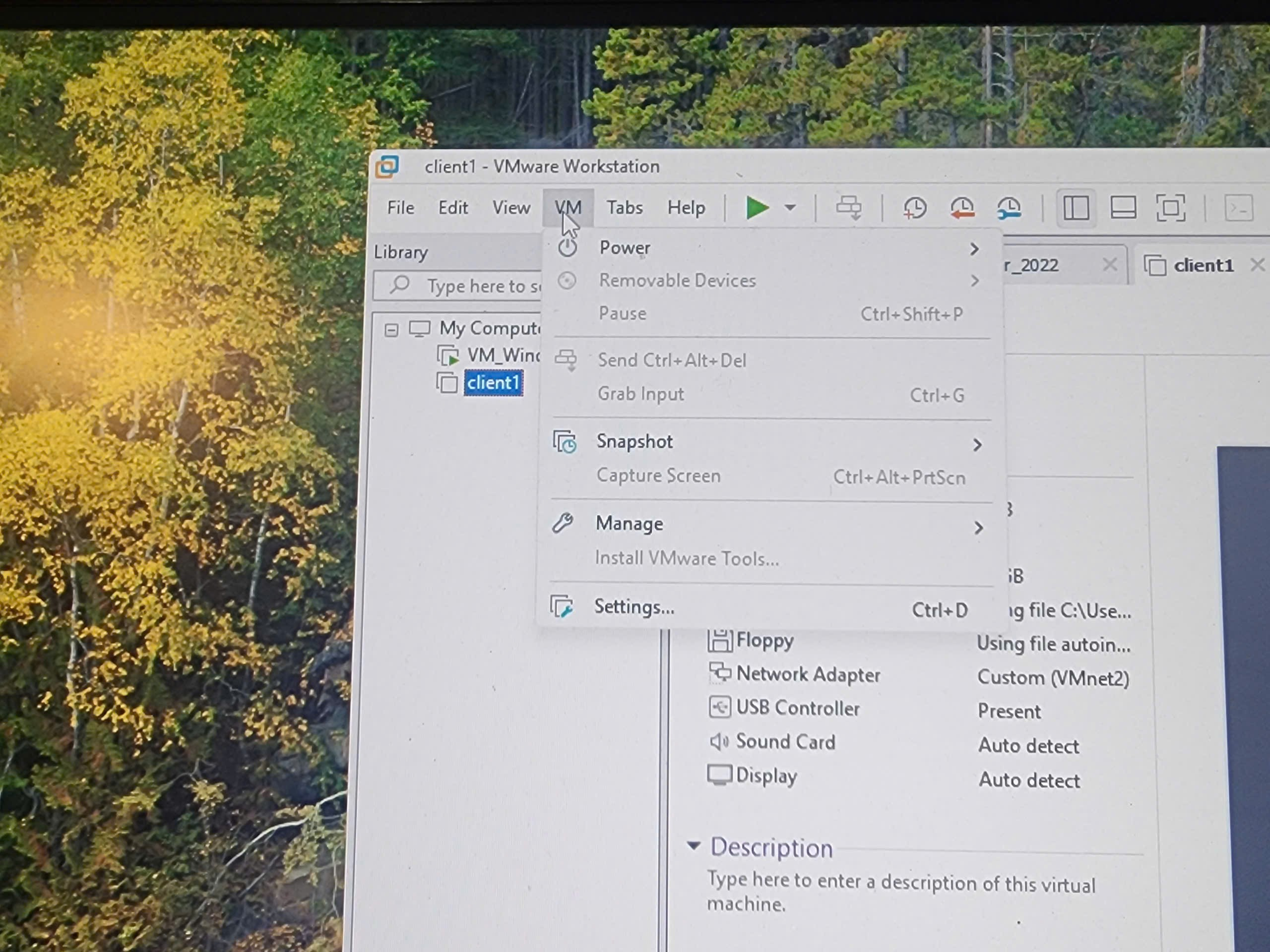
* Khi thiết lập mật khẩu không đúng với chính sách (ví dụ: thiếu ký tự đặc biệt hoặc độ dài ngắn), hệ thống từ chối và yêu cầu người dùng tuân thủ chính sách bảo mật đã được thiết lập.



Hình 3.25:Kiểm tra chính sách mật khẩu

3.6.5 Kiểm tra cấm sử dụng USB

Kết quả: Từ thời điểm chính sách có hiệu lực, tất cả người dùng và thiết bị trong domain sẽ không thể truy cập hoặc sử dụng thiết bị USB hay các thiết bị lưu trữ ngoài khác.



Hình 3.26:Kiểm tra cấm sử dụng USB

3.6.6 Kiểm tra truy cập trang web sau khi phân quyền

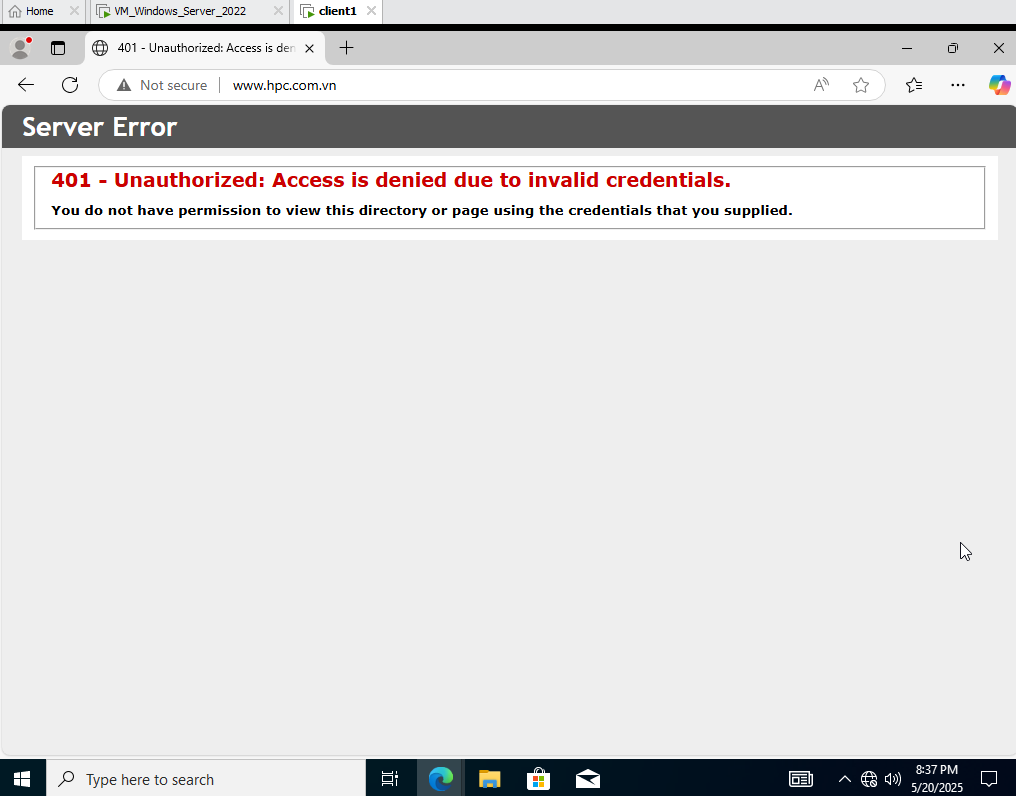
- Sau khi cấu hình xác thực và phân quyền truy cập cho website nội bộ http://mycompany.hpc.com.vn, tiến hành kiểm tra để đảm bảo thiết lập hoạt động đúng:

Truy cập trang web từ máy client đã join domain:

Nếu tài khoản thuộc nhóm được cấp quyền → truy cập thành công.

Nếu tài khoản không thuộc nhóm được cấp quyền → hiển thị thông báo Access Denied hoặc không thể truy cập.

* Thử truy cập bằng trình duyệt:
* Tắt đăng nhập tự động → khi truy cập, trình duyệt yêu cầu nhập tài khoản.
* Nhập tài khoản hợp lệ sẽ truy cập được trang web.
* Nhập tài khoản sai hoặc không có quyền → bị từ chối truy cập.



Hình 3.27:Kiểm tra truy cập trang web sau khi phân quyền

3.6.7 Kiểm tra theo dõi hoạt động – Xem nhật ký trong Event Viewer

Sau khi áp dụng các chính sách giám sát hoạt động (Audit Policy) thông qua Group Policy Object (GPO), toàn bộ các sự kiện liên quan đến bảo mật, đăng nhập, truy cập tệp, và thay đổi hệ thống sẽ được ghi lại trong hệ thống nhật ký sự kiện của Windows.

Để kiểm tra các hoạt động này, người quản trị có thể sử dụng công cụ Event Viewer có sẵn trong hệ điều hành. Cụ thể, để truy cập nhật ký bảo mật, người dùng mở ứng dụng Event Viewer, sau đó lần lượt chọn vào các mục: Windows Logs, tiếp theo là Security. Tại đây, toàn bộ sự kiện bảo mật được hệ thống ghi nhận sẽ hiển thị theo thời gian thực.

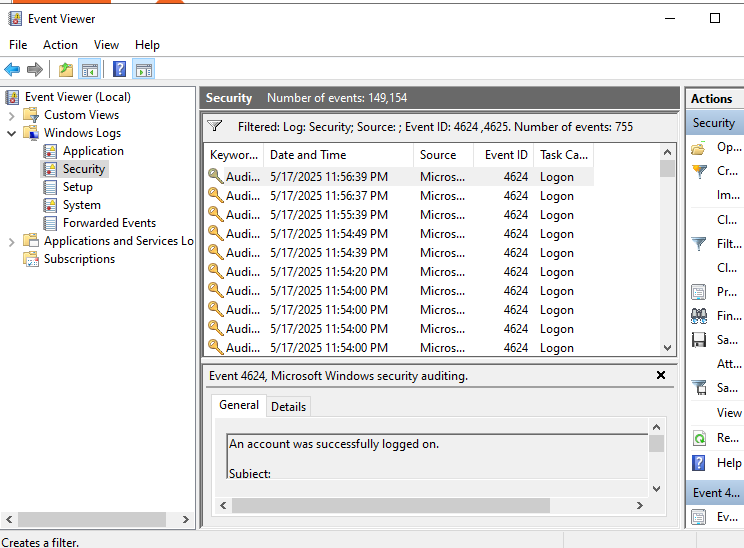
Các sự kiện quan trọng thường cần được theo dõi bao gồm:

* 4624: Đăng nhập thành công
* 4625: Đăng nhập thất bại (ví dụ như sai mật khẩu)
* 4663: Truy cập đến tệp hoặc thư mục đã bật chế độ audit
* 4720: Tạo tài khoản người dùng mới
* 4726: Xóa tài khoản người dùng
* 4739: Thay đổi chính sách bảo mật hệ thống
* 4672: Cấp quyền đặc biệt cho tài khoản (quản trị, backup, v.v.)
* 4776: Xác thực qua dịch vụ mạng (NTLM hoặc Kerberos)

Khi nhấp đúp vào từng sự kiện cụ thể, người dùng có thể xem chi tiết như: thời gian xảy ra sự kiện, tài khoản người dùng thực hiện, nguồn gốc truy cập (tên máy, địa chỉ IP), loại hành động thực hiện và trạng thái thành công hay thất bại.

Để dễ dàng theo dõi hơn, Event Viewer cũng cho phép lọc sự kiện theo mã định danh (Event ID). Người quản trị có thể thực hiện điều này bằng cách nhấn chuột phải vào mục Security, chọn Filter Current Log, sau đó nhập các mã sự kiện cần lọc như 4624, 4625, 4663,... để nhanh chóng thu hẹp phạm vi theo dõi.

Việc kiểm tra nhật ký trong Event Viewer là một bước quan trọng trong quy trình giám sát hệ thống, giúp phát hiện kịp thời các hành vi bất thường, tăng cường khả năng bảo mật và hỗ trợ điều tra sự cố nếu xảy ra.



Hình 3.28:Kiểm tra theo dõi hoạt động

KẾT LUẬN

Sau quá trình nghiên cứu và triển khai, đề tài "Triển khai hệ thống Active Directory" đã giúp người thực hiện hiểu rõ hơn về cách thiết lập và quản lý hệ thống máy chủ tập trung trong môi trường doanh nghiệp hiện đại. Việc sử dụng phần mềm VMware Workstation để mô phỏng hệ thống tạo điều kiện thuận lợi trong việc thực hành và kiểm thử các bước cấu hình, từ cài đặt hệ điều hành Windows Server, thiết lập địa chỉ IP tĩnh, đến việc cài đặt và cấu hình các dịch vụ thiết yếu như Active Directory Domain Services (AD DS), DNS, OU, Group Policy và các thành phần khác của hệ thống.

Hệ thống Active Directory mang lại nhiều ưu điểm rõ rệt. Trước hết, nó cho phép quản lý người dùng, máy tính và tài nguyên mạng một cách tập trung, giúp giảm thiểu công sức và thời gian cho quản trị viên. Khả năng áp dụng các chính sách bảo mật thông qua Group Policy giúp kiểm soát truy cập hiệu quả, tăng cường tính bảo mật của toàn bộ hệ thống. Bên cạnh đó, cấu trúc phân cấp rõ ràng với Forest, Domain, OU và Site giúp tổ chức linh hoạt, dễ dàng mở rộng khi cần thiết. Việc tích hợp DNS vào Active Directory cũng đóng vai trò quan trọng trong việc đảm bảo hoạt động ổn định của mạng nội bộ, giúp phân giải tên miền một cách nhanh chóng và chính xác.

Tuy nhiên, bên cạnh những lợi ích nổi bật, hệ thống cũng tồn tại một số hạn chế nhất định. Việc triển khai Active Directory yêu cầu chi phí bản quyền phần mềm như Windows Server và các công cụ quản trị liên quan, điều này có thể trở thành rào cản đối với các doanh nghiệp vừa và nhỏ. Ngoài ra, việc quản trị hệ thống cũng đòi hỏi người thực hiện phải có kiến thức chuyên sâu về mạng, bảo mật và hạ tầng CNTT. Nếu quá trình triển khai ban đầu không được thiết kế hợp lý, việc mở rộng hoặc tái cấu trúc hệ thống sau này sẽ gặp nhiều khó khăn và tốn kém nguồn lực.

Trong tương lai, hệ thống Active Directory có thể được phát triển theo hướng tích hợp với các dịch vụ điện toán đám mây như Azure Active Directory, nhằm tạo ra mô hình quản trị danh tính hiệu quả hơn trong môi trường hybrid. Đồng thời, việc kết hợp các giải pháp bảo mật hiện đại như xác thực đa yếu tố (Multi-Factor Authentication – MFA) sẽ nâng cao hơn nữa khả năng bảo vệ hệ thống trước các mối đe dọa từ bên ngoài. Ngoài ra, đối với các doanh nghiệp có nhiều chi nhánh, việc triển khai cấu trúc phân tán với nhiều Site kết hợp cơ chế sao chép dữ liệu tối ưu sẽ đảm bảo hiệu suất và tính ổn định cho toàn bộ tổ chức. Cuối cùng, việc ứng dụng các công cụ giám sát và phân tích nhật ký hệ thống như SIEM sẽ hỗ trợ quản trị viên theo dõi, phát hiện và xử lý kịp thời các sự cố bảo mật có thể xảy ra.

Tổng kết lại, Active Directory là một nền tảng quan trọng và không thể thiếu trong công tác quản trị hệ thống thông tin của tổ chức hiện đại. Việc nắm vững kiến thức triển khai và vận hành hệ thống không chỉ giúp đảm bảo an toàn thông tin mà còn góp phần nâng cao hiệu quả làm việc, quản lý và bảo mật trong kỷ nguyên số hóa ngày nay.

DANH MỤC TÀI LIỆU THAM KHẢO

**Danh mục các website tham khảo:**

[1]. Microsoft. (n.d.). *Active Directory Domain Services overview*. Microsoft Learn. Retrieved May 31, 2025. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/>

[2] Microsoft. (2023). Install Active Directory Domain Services (AD DS) on Windows Server. Microsoft Learn. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100->

**Danh mục sách tham khảo:**

[3] Minasi, M., Greene, D., & Rice, A. (2017). *Mastering Windows Server 2016*. John Wiley & Sons.

[4] Cisco Networking Academy. (2021). *Giáo trình Mạng máy tính – CCNA Routing and Switching*. Cisco Press.

[5] Bonaventure, O. (n.d.). *Computer networking: Principles, protocols and practice*. https://inl.info.ucl.ac.be/CNP3.