ĐẠI HỌC THÁI NGUYÊN

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

GIÁO TRÌNH QUẢN TRỊ HỆ THỐNG WINDOWS SERVER

TS. Đỗ Đình Cường (Chủ biên), TS. Nguyễn Đức Bình, ThS. Trần Quang Huy, ThS. Dương Thúy Hường

LỜI NÓI ĐẦU

MỤC LỤC

DANH MỤC HÌNH ẢNH

CHƯƠNG 1 TỔNG QUAN VỀ QUẢN TRỊ MẠNG

1.1 Giới thiệu về nghề quản trị mạng

Sự phát triển vượt bậc của công nghệ thông tin đã tạo ra một cuộc cách mạng về cách chúng ta làm việc, giao tiếp và tương tác với thế giới xung quanh. Từ khi mạng Internet ra đời cho đến những khám phá mới trong lĩnh vực trí tuệ nhân tạo và điện toán đám mây, mọi khía cạnh của cuộc sống và kinh doanh đều dựa vào các hệ thống thông tin và mạng máy tính.

Ngày nay, hầu hết mọi tổ chức, từ doanh nghiệp lớn đến các tổ chức phi lợi nhuận và cả cá nhân, đều phụ thuộc vào hệ thống máy chủ và mạng máy tính để hoạt động hiệu quả. Mạng máy tính kết nối con người với thế giới, cho phép trao đổi thông tin một cách nhanh chóng và tiện lợi. Từ gửi email đến thực hiện các giao dịch tài chính trực tuyến, mạng máy tính đóng vai trò quan trọng trong mọi khía cạnh của cuộc sống.

Tuy nhiên, sự phát triển đáng kinh ngạc này cũng đồng nghĩa với việc tạo ra những thách thức và nguy cơ mới. Với sự phổ biến của Internet, mạng máy tính trở nên phức tạp hơn, và nguy cơ về bảo mật và an ninh dữ liệu ngày càng tăng cao. Hệ thống máy chủ cần phải được duy trì và quản lý để đảm bảo tính hoạt động liên tục và hiệu suất cao. Điều đó đã dẫn đến sự ra đời của một vị trí việc làm được gọi là chuyên viên quản trị mạng.

Quản trị mạng và quản trị hệ thống máy chủ không chỉ là một công việc, mà còn là một nghệ thuật đòi hỏi sự tinh tế, sự nhạy bén và sự kiên trì. Có hai khía cạnh chính mà một hoặc nhiều chuyên viên trong một công ty phải đảm nhiệm đó là quản trị mạng (network administrator) và quản trị hệ thống (system administrator).

Network administrator (quản trị mạng) là người đảm nhận trách nhiệm xây dựng, duy trì và quản lý mạng lưới thông tin của một tổ chức. Họ là những người phải đối mặt với việc triển khai các giải pháp mạng, đảm bảo mạng luôn hoạt động ổn định, bảo mật và có khả năng mở rộng khi cần thiết. Network administrator cũng phải giải quyết các vấn đề kỹ thuật liên quan đến kết nối, băng thông và giao tiếp giữa các thiết bị trong mạng.

System administrator (quản trị hệ thống máy chủ) là người quản lý, bảo trì và cấu hình hệ thống máy chủ và dịch vụ liên quan trong một tổ chức. Họ đảm bảo rằng các máy chủ hoạt động ổn định, đáp ứng nhu cầu của người dùng và duy trì tính bảo mật của hệ thống. System administrator phải xử lý vấn đề về hiệu suất, tối ưu hóa tài nguyên và thực hiện các biện pháp đảm bảo an ninh mạng, sao lưu dữ liệu để đảm bảo rằng hệ thống luôn sẵn sàng hoạt động và có khả năng phục hồi sau sự cố.

Thông thường, tùy vào quy mô của đơn vị, chuyên viên quản trị mạng của các công ty, doanh nghiệp sẽ phải thực hiện một trong hai hoặc cả hai khía cạnh quản trị mạng và quản trị hệ thống, điều này đòi hỏi chuyên viên phải có nền tảng kiến thức vững vàng về mạng và máy chủ, đồng thời cần có khả năng tích lũy kiến thức, kinh nghiệm trong quá trình làm việc thực tế lâu dài. Chuyên viên quản trị mạng càng có nhiều kinh nghiệm thì càng dễ dàng hơn trong việc triển khai, quản lý và vận hành một hệ thống mạng quy mô lớn. Từ đó giúp tăng cường khả năng hoạt động của đơn vị, giảm thiểu rủi ro có thể dẫn đến mất mát tài liệu, dữ liệu của khách hàng.

1.2 Máy chủ là gì và máy chủ làm nhiệm vụ gì?

Server hay còn gọi là máy chủ là một hệ thống (bao gồm: hệ điều hành, phần mềm và phần cứng máy tính phù hợp) đáp ứng yêu cầu trên một mạng máy tính để cung cấp, hoặc hỗ trợ cung cấp một dịch vụ mạng. Các server có thể chạy trên một máy tính chuyên dụng, mà cũng thường được gọi là "máy chủ", máy tính này thường được cấu tạo bởi các thành phần phần cứng chuyên dụng và thường được lắp đặt triển khai tại các phòng đặt máy chuyên dụng hoặc các trung tâm dữ liệu.

Hình 1-1 Máy chủ HP

Các máy chủ thường hoạt động trong một mô hình client-server, server (máy chủ) là các chương trình máy tính đang chạy để phục vụ yêu cầu của các chương trình khác, các client (khách hàng). Do đó, các máy chủ thực hiện một số nhiệm vụ thay mặt cho khách hàng. Các khách hàng thường kết nối với máy chủ thông qua mạng nhưng có thể chạy trên cùng một máy tính. Trong hệ thống hạ tầng của mạng Internet Protocol (IP), một máy chủ là một chương trình hoạt động như một socket listener (giao thức nghe).

Các máy chủ thường cung cấp các dịch vụ thiết yếu qua mạng, hoặc là để người dùng cá nhân trong một tổ chức lớn hoặc cho người dùng nào thông qua Internet. Các máy chủ máy tính điển hình là máy chủ cơ sở dữ liệu (database server), máy chủ tập tin (file server), máy chủ mail (mail server), máy chủ in (print server), máy chủ web (web server), máy chủ game (game server), máy chủ ứng dụng (application server), hoặc một số loại khác của máy chủ.

Nhiều hệ thống sử dụng mô hình client/server này, bao gồm các mạng nội bộ LAN, hoặc các dịch vụ khác trên Internet như www, e-mail,.v.v do vậy máy chủ đóng

vai trò quan trọng trong việc duy trì hoạt động của hệ thống thông tin hiện đại và cung cấp các dịch vụ quan trọng cho người dùng và tổ chức.

1.3 Phân loại máy chủ

Chúng ta có thể phân loại máy chủ theo hai cách, theo mục đích sử dụng và theo cấu tạo vật lý.

Máy chủ có thể phân thành các loại chính sau, dựa theo cấu tạo vật lý.

- Máy chủ dạng tháp (Tower Server): đây là loại máy chủ có hình dạng tương tự một thùng máy tính cá nhân (PC) thông thường. Chúng thường được đặt đứng độc lập, tương tự như một máy tính để bàn. Hình 1-2 Máy chủ dạng tháp Tower Server cho chúng ta thấy hình dạng của một máy chủ dạng tháp.

Hình 1-2 Máy chủ dạng tháp Tower Server

- Máy chủ dạng phiến (Blade Server): thường được biết đến với tên gọi khác là máy chủ mật độ cao. Đây là một thiết bị bao gồm nhiều mô đun nhỏ được lắp chung trong một cấu trúc dạng hộp giúp tối ưu hóa diện tích và hiệu năng của hệ thống. Máy chủ dạng phiến được mô tả trong hình dưới đây.

Hình 1-3 Máy chủ dạng phiến - Blade Server

- Máy chủ đặt trong rack (Rack-mount Server): là loại máy chủ thông dụng nhất hiện nay, nó được thiết kế để được gắn lên các tủ rack chuyên dụng được đặt trong các trung tâm dữ liệu hoặc phòng máy chủ. Rack-mount Server có kích thước cố định để có

thể phù hợp với các tủ rack và được tính theo đơn vị U. Rack-mount Server 1U có kích thước chiều rộng – chiều cao và chiều sâu lần lượt là 19" x 1.75" x 17.7". Hình dưới cho chúng ta thấy hình dạng của một máy chủ đặt trong rack với kích thước 1U. Ngoài ra còn có các kích thước khác như 2U, 4U, 5U, 6U có tỉ lệ tương đương. Các thành phần phần cứng trong Rack-mount Server thường được triển khai dưới dạng mô đun và có tính năng hot-plug giúp người quản trị dễ dàng trong việc kiểm tra, bảo trì bảo dưỡng và xử lý sự cố khi cần.

Hình 1-4 Máy chủ rack

Trên đây là ba loại máy chủ vật lý thông dụng nhất, ngoài ra tùy vào điều kiện sử dụng, các nhà sản xuất cũng đưa ra thị trường các dòng máy chủ chuyên dụng khác. Có thể kể đến như máy chủ công nghiệp, máy chủ lưu trữ, máy chủ mô đun,.v.v. Mỗi loại máy chủ khác nhau sẽ có các đặc điểm khác nhau về cấu tạo vật lý cũng như năng lực vận hành khác nhau tùy thuộc vào điều kiện sử dụng. Kĩ sư quản trị mạng cần lên kế hoạch, nghiên cứu kĩ lưỡng từng đặc tính, hiệu năng, giá thành, các tính năng chuyên biệt của từng loại máy chủ để có thể lựa chọn loại máy chủ phù hợp với doanh nghiệp của mình.

1.4 Sự khác biệt giữa máy chủ và máy tính cá nhân

Về cơ bản máy chủ và máy tính cá nhân đều là một hệ thống máy tính bao gồm đầy đủ các thành phần như: bộ vi xử lý, bo mạch chủ, RAM, ổ đĩa lưu trữ, bộ nguồn. Tuy nhiên do mục đích sử dụng khác nhau nên máy chủ (server) và máy tính cá nhân (PC) sẽ có một số khác biệt như sau.

- Khác biệt về mục đích sử dụng:
  - Máy chủ: Thường được sử dụng để cung cấp dịch vụ và tài nguyên cho nhiều người dùng hoặc thiết bị khác nhau từ xa. Ví dụ như dịch vụ lưu trữ dữ liệu, cung cấp dịch vụ trang web, thư điện tử, hoặc các dịch vụ ảo hóa.
  - Máy tính cá nhân: Thường được sử dụng bởi một người dùng trực tiếp để thực hiện các công việc hàng ngày như: soạn thảo văn bản, truy cập các trang web, kiểm tra thư điện tử, hoặc các tác vụ giải trí như xem video, chơi trò chơi,.v.v.

- Khác biệt về hiệu suất: Từ những đặc điểm về mục đích sử dụng ta có thể đưa ra được những yêu cầu khác nhau về hiệu suất giữa máy chủ và máy tính cá nhân như sau.
  - Máy chủ: Cần có khả năng xử lý và phục vụ đồng thời nhiều yêu cầu từ nhiều người dùng khác nhau. Cần có khả năng hoạt động liên tục mà không bị gián đoạn trong một khoảng thời gian dài.
  - Máy tính cá nhân: Chỉ được thiết kế để đáp ứng nhu cầu của một người dùng đơn lẻ nên không yêu cầu hiệu suất cao.
- Khác biệt về phần cứng và tài nguyên:
  - Máy chủ: Được cung cấp bổ sung các thành phần phần cứng làm tăng khả năng sẵn sàng của hệ thống như: 02 CPU, 02 PSU, có nhiều khe cắm mở rộng để hỗ trợ nâng cấp thêm RAM và ổ đĩa lưu trữ. Ngoài ra phần cứng máy chủ thường được thiết kế theo dạng module để có thể dễ dàng thay thế khi có sự cố. Đa số các thành phần phần cứng đều được thiết kế để hỗ trợ khả năng hot-plug cho phép thay thế linh kiện ngay cả khi máy chủ vẫn đang hoạt động.
  - Máy tính cá nhân: Thường chỉ bao gồm các thành phần phần cứng cơ bản đủ để đáp ứng tốt các nhu cầu cá nhân.
- Khác biệt về hệ điều hành, phần mềm và khả năng bảo mật:
  - Máy chủ: Hệ điều hành dành cho máy chủ thường được thiết kế riêng để tối ưu hóa hiệu suất, tăng cường khả năng xử lý đồng thời nhiều yêu cầu, cắt giảm các giao diện đồ họa để tăng hiệu năng. Đồng thời có khả năng quản lý tài nguyên và phân quyền hiệu quả. Máy chủ cần có mức độ bảo mật cao hơn để đảm bảo an toàn dữ liệu cho các đơn vị sử dụng.
  - Máy tính cá nhân: Hệ điều hành dành cho máy tính cá nhân thường tập trung vào trải nghiệm của người dùng với các giao diện đồ họa đẹp mắt. Máy tính cá nhân cũng yêu cầu độ bảo mật thấp hơn và chỉ tập trung vào bảo vệ dữ liệu cá nhân của người dùng.

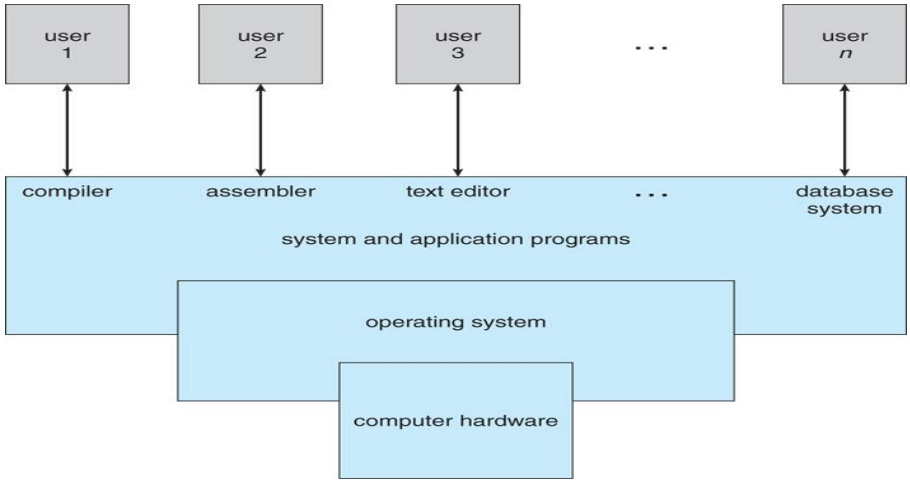
1.5 Hệ điều hành dành cho máy chủ

A. Định nghĩa chung về hệ điều hành: Hệ điều hành là một chương trình máy tính hoặc một phần mềm có chức năng quản lý các thiết bị phần cứng và tài nguyên trên máy tính. Nó cung cấp một nền tảng trung gian giữa các chương trình ứng dụng, người sử dụng và các thiết bị phần cứng.

Một khía cạnh tuyệt vời của hệ điều hành là khả năng thiết kế đa dạng để hoàn thành được rất nhiều các nhiệm vụ khác nhau. Cụ thể đối với các hệ thống Server – Các hệ thống máy tính được sử dụng để lưu trữ, xử lý dữ liệu lớn – thì hệ điều hành được

thiết kế để tối ưu hóa hiệu suất sử dụng phần cứng. Còn đối với các máy tính cá nhân PC thì các hệ điều hành lại được thiết kế tập trung vào trải nghiệm của người sử dụng với các phần mềm soạn thảo văn bản, hoặc các phần mềm giải trí. Nhìn chung một số hệ điều hành được thiết kế để ưu tiên cho tính thuận tiện, một số khác lại ưu tiên hiệu suất xử lý hoặc kết hợp cả hai đặc tính trên.

Với tính chất phức tạp của một hệ điều hành, nó thường được thiết kế theo từng thành phần. Trong đó mỗi thành phần được quy định đầy đủ chức năng, nhiệm vụ, dữ liệu input và output của thành phần đó đối với hệ thống. Hình dưới mô tả vai trò của hệ điều hành trong một hệ thống máy tính.



Hình 1-5 Vai trò của hệ điều hành

Trong đó, các thiết bị phần cứng bao gồm: bộ xử lý trung tâm CPU, bộ nhớ RAM, và các thiết bị nhập/xuất. Những thành phần này là các tài nguyên cơ bản mà một hệ thống máy tính cung cấp. Các chương trình ứng dụng như trình soạn thảo văn bản, bảng tính hay trình duyệt web thể hiện cách thức mà máy tính sử dụng tài nguyên để giải quyết các yêu cầu đến từ người dùng. Hệ điều hành có vai trò điều khiển các thiết bị phần cứng, điều phối tài nguyên cho các chương trình ứng dụng khác nhau phục vụ các yêu cầu khác nhau đến từ những người sử dụng.

Chúng ta cũng có thể xem một hệ thống máy tính là một tập hợp của phần cứng, phần mềm và dữ liệu. Trong đó hệ điều hành là một phần mềm trung gian thực hiện việc cung cấp các tài nguyên phân cứng một cách hợp lý. Hệ điều hành chỉ đơn giản là một môi trường để các chương trình ứng dụng khác thực hiện công việc của mình một cách hiệu quả, độc lập và an toàn về mặt phần cứng.

B. Hệ điều hành dành cho máy chủ trong mô hình Client – Server cho phép tập trung các chức năng và ứng dụng trong một hoặc nhiều máy chủ chuyên dụng. Các máy chủ trở thành trung tâm của hệ thống, cung cấp tài nguyên và các chính sách về an ninh. Các máy trạm – client – có quyền truy cập vào các nguồn tài nguyên sẵn có trên máy

chủ. Các hệ điều hành dành cho máy chủ cung cấp các cơ chế để tích hợp tất cả các thành phần của mạng và cho phép nhiều người dùng có thể đồng thời truy cập và sử dụng các nguồn tài nguyên mà không phụ thuộc vào vị trí địa lý. Unix/Linux và các phiên bản Server của hệ điều hành Windows là những đại diện của các hệ điều hành dành cho máy chủ.

Windows Server

Hệ điều hành Windows Server được Microsoft phát triển từ những năm 1993 với phiên bản đầu tiên có tên gọi Windows NT 3.1 Advanced Server. Năm 1994 phiên bản Windows NT Server và Windows NT Workstation version 3.5 được phát hành, tiếp theo đó ra đời các bản version 3.51.

Hệ điều hành Windows NT được phát triển song song hai phiên bản là Windows NT Workstation và Windows NT Server. Trong đó phiên bản Workstation được thiết kế để phục vụ mô hình mạng ngang hàng còn phiên bản Server dành cho các mô hình mạng Client/Server với các hệ thống quản lý tập trung, in ấn và chia sẻ tài nguyên.

Cho đến nay hệ điều hành Windows Server đã phát hành được 7 phiên bản. Bao gồm: Windows NT Server, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2. Đặc biệt từ Windows Server 2003 trở đi, với mỗi phiên bản Windows ra đời. Microsoft đưa ra các phiên bản cụ thể để hỗ trợ các thiết bị phần cứng và vai trò sử dụng khác nhau như: Web Edition, Standard Edition, Datacenter Edition, Enterprise Edition, Server core Edition,.v.v.

Một số tính năng chính của Windows Server:

- Windows Server cung cấp các dịch vụ như: Dịch vụ Active Directory, dịch vụ web IIS, các dịch vụ cơ sở hạ tầng như Microsoft DHCP Server, Domain Name System (DNS) Server, và Windows Internet Name Service (WINS) Server, cung cấp các dịch vụ cơ bản cho mạng nội bộ và các máy khách trên Internet. Cung cấp khả năng định tuyến TCP/IP, khả năng hỗ trợ từ xa Routing and Remote Access Services, chuyển đổi địa chỉ NAT, các dịch vụ file và in ấn qua mạng, các dịch vụ bảo mật..v.v.
- Đối với các phiên bản hỗ trợ hoạt động của doanh nghiệp Windows Server cung cấp các tính năng như: Windows System Resource Manager – WSRM, Windows Deployments Services, Fail-over Clustering, Server Migration,.v.v. Nền tảng windows server cung cấp cho mạng doanh nghiệp khả năng hoạt động ổn định cùng các giải pháp sao lưu và khôi phục dữ liệu tối ưu. Cùng với đó là khả năng tích hợp đa dịch vụ, các công cụ theo dõi và chuẩn đoán tình trạng mạng, xác định và giải quyết các vấn đề một cách hiệu quả. Đem lại sự vận hành tối ưu nhất cho mạng doanh nghiệp.

- Ảo hóa: Từ phiên bản Server 2008 trở đi. Windows cung cấp thêm khả năng ảo hóa máy chủ với công nghệ Hyper-V. Cho phép giảm chi phí, tăng khả năng sử dụng phần cứng, tối ưu hóa cơ sở hạ tầng và khả năng phục vụ của máy chủ. Công nghệ ảo hóa của windows cho phép ảo hóa nhiều loại hệ điều hành – windows, linux trên cùng một hệ thống máy chủ. Với các bước cấu hình cài đặt đơn giản và linh động. Hyper-V đem lại lợi ích tối ưu cho các hệ thống mạng.
- Bảo mật: Windows Server được tối ưu hóa về bảo mật với những tính năng như: Network Access Protection, Right Management Services, các công nghệ truy cập từ xa như VPN, Direct Access. Theo dõi và đưa ra các quy định đối với người sử dụng bằng Group Policy và Event Viewer. Thực thi các chính sách kiểm soát và ngăn chặn bằng Windows Firewall giúp giảm thiểu tối đa những mối nguy hại đối với Server.

Linux Server

Linux là tên gọi của một hệ điều hành máy tính tương tự như Unix, là một hệ điều hành cung cấp độ tin cậy và an ninh cao trong các ứng dụng chuyên nghiệp. Nhiều máy chủ trên khắp thế giới mà chúng lưu trữ các dữ liệu cho các website phổ biến (như YouTube và Google) sử dụng biến thể của Unix, Linux cũng là tên hạt nhân của hệ điều hành.

Phiên bản Linux đầu tiên do Linus Torvalds viết vào năm 1991, lúc ông còn là một sinh viên của Đại học Helsinki tại Phần Lan. Ông làm việc một cách hăng say trong vòng 3 năm liên tục và cho ra đời phiên bản Linux 1.0 vào năm 1994. Bộ phận chủ yếu này được phát triển và tung ra trên thị trường dưới bản quyền GNU (General Public License). Do đó mà bất cứ ai cũng có thể tải và xem mã nguồn của Linux.

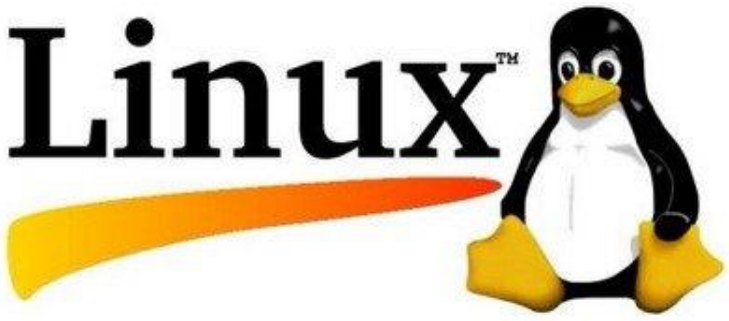
Thuật ngữ "Linux" được sử dụng để chỉ nhân Linux, nhưng tên này được sử dụng một cách rộng rãi để miêu tả tổng thể một hệ điều hành giống Unix (còn được biết đến dưới tên GNU/Linux) được tạo ra bởi việc đóng gói nhân Linux cùng với các thư viện và công cụ GNU, cũng như là các bản phân phối Linux. Thực tế thì đó là tập hợp một số lượng lớn các phần mềm như máy chủ web, các ngôn ngữ lập trình, các hệ quản trị cơ sở dữ liệu, các môi trường làm việc desktop như GNOME và KDE, và các ứng dụng thích hợp cho công việc văn phòng như OpenOffice.

Ban đầu, Linux được phát triển và sử dụng bởi những người say mê. Tuy nhiên, hiện nay Linux đã có được sự hỗ trợ bởi các công ty lớn như IBM và Hewlett-Packard, đồng thời nó cũng bắt kịp được các phiên bản Unix độc quyền và thậm chí là một thách thức đối với sự thống trị của Microsoft Windows trong một số lĩnh vực. Sở dĩ Linux đạt được những thành công một cách nhanh chóng là nhờ vào các đặc tính nổi bật so với các hệ thống khác: chi phí phần cứng thấp, tốc độ cao (khi so sánh với các phiên bản

Unix độc quyền) và khả năng bảo mật tốt, độ tin cậy cao (khi so sánh với Windows) cũng như là các đặc điểm về giá thành rẻ, không bị phụ thuộc vào nhà cung cấp. Một đặc tính nổi trội của nó là được phát triển bởi một mô hình phát triển phần mềm nguồn mở hiệu quả.

Tuy nhiên, hiện tại số lượng phần cứng được hỗ trợ bởi Linux vẫn còn rất khiêm tốn so với Windows vì các trình điều khiển thiết bị tương thích với Windows nhiều hơn là Linux. Nhưng trong tương lai số lượng phần cứng được hỗ trợ cho Linux sẽ tăng lên.

Linux hiện nay có nhiều bản phân phối khác nhau, một phần bởi tính chất nguồn mở của nó. Sau đây là một số bản phân phối chủ yếu: Debian GNU/Linux, Red Hat, Fedora Core, SuSE, Ubuntu, Mandrake/Mandriva, Gentoo, Slackware, Hacao.



Hình 1-6 Biểu tượng Linux

Các hệ điều hàng mạng sử dụng nhân linux nói chung có các ưu điểm như sau:

- Chi phí triển khai thấp do là phần mềm nguồn mở. Một số bản phân phối còn miễn phí hoàn toàn.
- Bảo mật tốt: nhờ hệ thống phân cấp người dùng tối ưu. Linux được mệnh danh là hệ điều hành không có virus.
- Hiệu suất cao và tiết kiệm được tài nguyên.
- Cung cấp đầy đủ các dịch vụ máy chủ như Web, DHCP, DNS,..v.v. Các server Linux đặc biệt thích hợp cho triển khai dịch vụ Web với giá thành rẻ và hiệu suất cao.
- Dễ dàng tích hợp thêm các module phần mềm được phát triển trong cộng đồng phát triển phần mềm nguồn mở.
- Được hỗ trợ từ cộng đồng người sử dụng là các chuyên gia.

Với đặc thù là một hệ điều hành mã nguồn mở nên đã có rất nhiều các phiên bản khác nhau của UNIX/Linux được tạo ra nhằm phục vụ mục đích của mỗi cá nhân, cơ quan doanh nghiệp hoặc các thiết bị chuyên dụng. Các phiên bản đó được gọi là các bản phân phối – distro. Trong đó các distro thông dụng nhất được sử dụng cho các hệ điều hành mạng có thể kể đến là: Debian,CentOS, Redhat Enterprise Linux và Ubuntu Server Edition.

CHƯƠNG 2 WINDOWS SERVER VÀ MÔ HÌNH ACTIVE DIRECTORY

2.1 Giới thiệu chung về Windows và Active Directory

2.1.1 Giới thiệu chung về Windows.

Microsoft Windows (hoặc đơn giản là Windows) là tên của một họ hệ điều hành dựa trên giao diện người dùng đồ hoạ được phát triển và được phân phối bởi Microsoft. Nó bao gồm một vài các dòng hệ điều hành, mỗi trong số đó phục vụ một phần nhất định của ngành công nghiệp máy tính. Hệ điều hành Windows lần đầu tiên được giới thiệu vào năm 1985 với tên gọi Microsoft Windows 1.0 là một bước đột phá ngoạn mục từ hệ điều hành MS-DOS trước đó, người sử dụng lần đầu tiên có thể sử dụng chuột để truy nhập vào các cửa sổ thay vì phải nhập các câu lệnh rườm rà như trước.

Sau nhiều năm phát triển Microsoft đã đưa ra nhiều phiên bản khác nhau phục vụ nhiều mục đích khác nhau của hệ điều hành Windows. Trong đó, có thể kể đến các phiên bản hệ điều hành phục vụ cho máy tính cá nhân chiếm thị phần rất lớn trên thị trường như Windows 95, Windows 98, Windows XP, Windows 7, Windows 8, Windows 10. Các phiên bản Windows dành cho máy tính cá nhân của Microsoft được biết đến với giao diện người dùng (GUI) thân thiện, hỗ trợ đa nhiệm, hỗ trợ nhiều loại ứng dụng phần mềm khác nhau, tương thích với nhiều hệ thống phần cứng khác nhau, có khả năng kết nối mạng và cung cấp các tính năng bảo mật hiệu quả. Đặc biệt Microsoft còn cung cấp thêm bộ phần mềm văn phòng Office với các công cụ như Word, Excel, PowerPoint giúp giải quyết các công việc văn phòng một cách hiệu quả. Chính vì vậy, hệ điều hành Windows phiên bản dành cho máy tính cá nhân được sử dụng rất nhiều tại các công ty, doanh nghiệp và cơ quan nhà nước.

Một nhánh khác của Windows là phiên bản hệ điều hành dành cho máy chủ hay còn gọi là NOS – Network Operating System. Hệ điều hành mạng, hay NOS là thuật ngữ dùng để mô tả hệ điều hành của một hệ thống mà các máy tính được nối mạng và cùng chia sẻ các loại tài nguyên khác nhau như tài khoản người dùng, nhóm. Các loại tài nguyên đó được cùng lưu trữ trong một cơ sở dữ liệu được đặt trên máy chủ, quản trị bởi chuyên viên quản trị mạng và được sử dụng bởi người dùng cuối.

Microsoft lần đầu tích hợp môi trường NOS vào đầu những năm 1990 với phiên bản Windows NT 3.0, mà trong đó kết hợp một số giao thức quản trị mạng cục bộ. Hệ điều hành NT được phát triển một cách chậm chạp, đến năm 1997, thuật ngữ Active Directory mới lần đầu được giới thiệu.

Cho đến nay thì Windows Server đã ra mắt những phiên bản như sau:

Windows NT 3.1

Năm 1993, Microsoft phát hành Windows NT 3.1, là phiên bản đầu tiên của hệ thống. Windows NT 3.1 là hệ thống 32-bit, sở hữu một phiên bản dành cho máy chủ và một phiên bản dành cho thiết bị đầu cuối.

Phiên bản máy chủ được nâng cấp thành dòng Windows Server. Do việc tách ra phiên bản máy chủ chuyên dụng của hệ điều hành là từ phiên bản NT tiêu chuẩn nên không có Windows NT Server phiên bản 1.

Windows NT 3.5

Năm 1994, Microsoft cho ra mắt Windows 3.5. Phiên bản hệ điều hành này cho phép kết nối với các hệ thống Unix và Novell Netware.

Lúc bấy giờ, Windows Server là một tên tuổi mới trên thị trường và hầu hết các mạng đều chạy trên máy chủ Unix hoặc Novell.Inc. Vì vậy, để được các doanh nghiệp sử dụng mạng chấp nhận, Windows Server phải tương thích với hai hệ thống này.

Windows NT 3.51

Năm 1995, Microsoft tạo ra Windows NT 3.51 để quản lý các máy tính chạy Windows 95. Hệ thống máy chủ có được khả năng quản lý giấy phép phần mềm cho máy khách, cài đặt, cập nhật Windows 95 và yếu tố của hệ điều hành qua mạng.

Windows NT 4.0

Năm 1996, Microsoft phát hành Windows NT 4.0, mang nét đặc trưng trong giao diện của Windows 95 và bao gồm Internet Information (IIS) 2.0 miễn phí.

IIS (máy chủ thông tin Internet) là hệ thống máy chủ web của Microsoft, cạnh tranh trực tiếp với Apache HTTP Server. Năm 2018, IIS vượt qua Apache và trở thành một trong các phiên bản windows server được cài đặt rộng rãi nhất.

Năm 1997, Microsoft tạo ra Windows NT Server Enterprise với những cải tiến như: tích hợp các dịch vụ mã hóa public key, quản lý hệ điều hành cho các máy chủ, Transaction Server và Message Queue Server.

Năm 1998, Microsoft có sự cải tiến cuối cùng cho Windows NT Server và cho ra mắt phiên bản Windows NT 4.0 Terminal Server. Phiên bản này tạo ra một cầu nối từ các ứng dụng DOS 16-bit để chúng có thể giao tiếp với môi trường Desktop 32-bit.

Windows Server 2000

Năm 2000, Microsoft không còn sử dụng thương hiệu "NT" và phát hành Windows Server 2000. Kể từ đây, tên phiên bản của Windows Server được đặt kèm theo năm phát hành.

Các tính năng của phiên bản này bao gồm: hỗ trợ cho XML, tạo Active Server Pages (ASP) và Active Directory để xác thực người dùng. Trong thời gian này, Microsoft cũng đã phát hành Advanced Server và Datacenter Server.

Windows Server 2003

Windows Server 2003 là một trong các phiên bản Windows Server được cải tiến hơn dựa trên Windows Server 2000 nhằm mục đích giảm các sự kiện yêu cầu khởi động lại hệ thống. Microsoft tập trung phát triển các tính năng bảo mật cho hệ điều hành và đây là lần đầu tiên môi trường .NET được tích hợp vào hệ điều hành Windows Server. Windows Server 2003 cho phép được điều chỉnh theo các tác vụ cụ thể. Bên cạnh phiên bản Standard, Advanced và Datacenter, Microsoft còn cung cấp phiên bản Windows Server 2003 Web.

Một thời gian sau đó, Microsoft đã tạo ra một bản cập nhật chuyển đổi hệ thống với chương trình 64-bit.

Windows Server 2003 R2

Năm 2005, Microsoft cho ra mắt Windows Server 2003 R2. Người dùng đã mua Windows Server 2003 được phép truy cập miễn phí phiên bản mới này.

Những cải tiến cho hệ thống Windows Server 2003 R2 tập trung vào vấn đề bảo mật. Active Directory với tính năng xác thực người dùng vẫn được duy trì cho đến ngày nay.

Ngoài ra, Microsoft còn phát triển tính năng Active Directory Federation Services cho hệ thống xác thực này và được tích hợp vào R2, cho phép các dịch vụ bên ngoài được bao gồm trong các quyền Single Sign On.

Tiếp theo là một nâng cấp khác của Active Directory - chế độ Active Directory Application, cho phép người dùng tiếp cận được với các ứng dụng đã được xác minh thông qua AD.

Gói R2 cho phép thiết lập các chính sách bảo mật cho nhóm hệ thống thông qua Security Configuration Wizard, nén dữ liệu tốt hơn để truyền file và quy trình nhân bản cho các mạng WAN multisite.

Windows Server 2008

Windows Server 2008 là một trong các phiên bản Windows Server được cập nhật các tiện ích mới là Event Viewer và Server Manager.

Đây là những công cụ quản trị hệ thống có nhiều ưu điểm vượt trội, cho phép các admin kiểm soát tốt hơn hoạt động của máy chủ.

Các phiên bản Windows Server 2008 gồm có 6 phiên bản chính:

Windows Server 2008 Standard

Windows Server 2008 Enterprise

Windows Server 2008 Data center

Windows Web Server 2008

Windows HPC (High-performance computing) Server 2008

Windows Server 2008 for Itanium-based Systems.

Ngoài ra, Windows Server 2008 còn có 3 phiên bản Standard, Enterprise, Data center không hỗ trợ Hyper-V.

Windows Server 2008 R2

Windows Server 2008 R2 khác với Windows Server 2008 về kỹ thuật và giúp đưa hệ thống thực thi chương trình lên môi trường 64-bit.

Phiên bản Windows Server có một số thay đổi khác trong Active Directory, cải thiện việc thực hiện group policy và một vài service mới xuất hiện như: Remote Desktop Services (RDS), BranchCache, DirectAccess để cải thiện quyền truy cập vào máy chủ cho người dùng từ xa.

Windows Server 2012

Năm 2012, Microsoft đã thêm công nghệ "đám mây" vào Windows Server để cho phép hệ điều hành này tương tác tốt hơn với các dịch vụ off-site. Windows Server 2012 được Microsoft quảng bá với vai trò là một "Cloud OS" (hệ điều hành đám mây).

Windows Server trong phiên bản này tập trung vào việc làm Hyper-V, tích hợp với tính năng onsite. Hệ thống lưu trữ cũng được cập nhật trong phiên bản này.

Switch ảo Hyper-V và Hyper-V Replica cũng được tích hợp trong phiên bản này. Windows Server 2012 có 4 phiên bản gồm: Essentials, Foundation, Standard và Datacenter.

Windows Server 2012 R2

Windows Server 2012 R2 là một trong các phiên bản Windows Server 2012 được ra mắt vào năm 2013.

Ở phiên bản này, PowerShell được mở rộng hơn nữa, các chức năng máy chủ onsite tốt hơn, cung cấp khả năng tích hợp các dịch vụ đám mây, các web service, hệ thống lưu trữ và ảo hóa.

Các tính năng lưu trữ được cải tiến trong bản nâng cấp này bao gồm: nhân bản các file phân tán và cải thiện quyền truy cập cho chia sẻ file, điều khiển các thiết bị di động bằng phần mềm từ máy chủ cũng được cải thiện.

Microsoft đã cho ra mắt hệ thống Desired State Configuration dựa trên PowerShell với mục đích là tăng cường quản lý cấu hình mạng.

Windows Server 2016

Windows Server 2016 thuộc loại Nano Server, bao gồm Server Core và có ít giao diện hơn. Các hệ thống VM cũng được tích hợp vào hệ thống mã hóa Hyper-V và khả năng tương tác mới hơn với Docker.

Công cụ này cho phép các quản trị viên hệ thống cung cấp phần mềm thuộc sở hữu của công ty cho các thiết bị do người dùng sở hữu. Tính năng Network Controller

trong Windows Server 2016 giúp các admin quản lý cả thiết bị mạng vật lý và ảo từ một bảng điều khiển. Windows Server 2016 không có phiên bản R2. Các phiên bản Windows Server 2016 gồm:

Windows Server 2016 Datacenter

Windows Server 2016 Standard

Windows Server 2016 Essentials

Windows Server 2016 MultiPoint Premium Server

Windows Storage Server 2016

Microsoft Hyper-V Server 2016.

Giao diện cài đặt Windows Server 2016

Giao diện cài đặt Windows Server 2016

Windows Server 2019

Windows Server 2019 được phát hành vào tháng 10 năm 2018, là phiên bản mới nhất của hệ điều hành máy chủ của Microsoft.

Hệ điều hành có các tính năng mới như: kết nối môi trường tại chỗ với Azure, bổ sung các lớp bảo mật nhằm giúp người dùng hiện đại hóa các ứng dụng cũng như cơ sở hạ tầng của máy tính.

Các phiên bản Windows Server 2019 gồm: Essentials, Standard và Datacenter.

2.1.2 Lịch sử phát triển của Active Directory

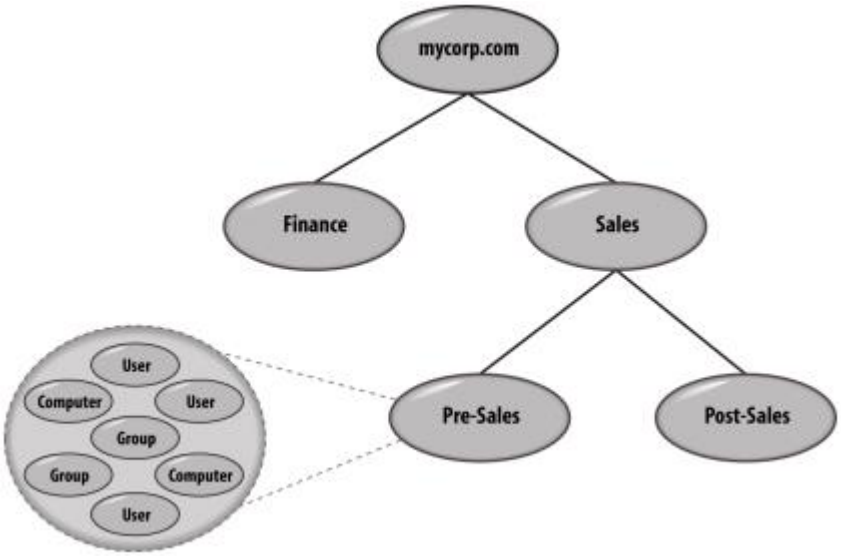
Thuật ngữ Directory Service được định nghĩa là các kho lưu trữ thông tin của các hệ thống mạng, ứng dụng và dữ liệu của một hệ điều hành mạng giúp phục vụ hoạt động của nhiều người dùng. Trong thực tế có rất nhiều kiểu dịch vụ thư mục khác nhau, có thể kể đến như hệ thống email, hệ thống DNS,.v.v. Mặc dù các hệ thống này đều có các đặc điểm của một dịch vụ thư mục nhưng chỉ có X.500 và giao thức LDAP (Lightweigh Directory Access Protocol) là xác định đầy đủ các tiêu chuẩn về việc một dịch vụ thư mục cần được triển khai và truy cập như thế nào.

Năm 1988, Liên minh viễn thông quốc tế (ITU) và tổ chức quốc tế về tiêu chuẩn hóa (ISO) đã hợp tác để phát triển một loạt các tiêu chuẩn xung quanh dịch vụ thư mục, sau này được gọi là giao thức X.500. Mặc dù X.500 được chứng minh là một mô hình tốt để cấu trúc một thư mục và cung cấp nhiều chức năng xung quanh các hoạt động nâng cao và bảo mật, nhưng X.500 tỏ ra quá phức tạp khiến cho nó không thể được triển khai ở quy mô lớn. Do đó, một nhóm các nhà nghiên cứu đến từ Đại học Michigan đã bắt đầu nghiên cứu một giao thức truy cập X.500 đơn giản hơn được gọi là LDAP. Phiên bản đầu tiên của LDAP được phát hành vào năm 1993 được mô tả trong RFC 1487, tuy nhiên phiên bản này không thành công do còn thiếu nhiều tính năng. Phải đến năm 1995

khi LDAPv2 ra mắt và được mô tả trong RFC 1977 thì LDAP mới bắt đầu trở nên phổ biến. Đến năm 1977 LDAP v3 được mô tả trong RFC 2251 đã cung cấp một số tính năng mới và làm cho LDAP đủ khả năng để mở rộng cũng như phù hợp với các nhà cung cấp. Kể từ đó thì các công ty như Netscape, Sun, Novell, IBM, OpenLDAP Foundation và Microsoft đã phát triển và vận hành các máy chủ thư mục của riêng họ dựa trên LDAP.

2.2 Mô hình AD DS

Dữ liệu lưu trữ trong Active Directory được biểu diễn với người dùng dưới dạng cấu trúc phân cấp hình cây tương tự như cách thức lưu trữ trong các hệ thống tập tin. Trong các cấp có các Object – đối tượng đại diện cho một thực thể tham gia trong hệ thống mạng. Một Object có thể là một người dùng, một thiết bị hay một nhóm. Có 02 loại Object chính là: Containers và Non Containers. Các Object thuộc loại Non Container còn được gọi là nút lá. Một hoặc nhiều Container phân nhánh từ nút gốc, mỗi Container có thể chứa các nút lá hoặc các Container khác. Một nút lá có thể chứa nhiều Object hoặc cũng có thể không chứa Object nào. Hình dưới mô tả cấu trúc của AD DS.



Hình 2-1 Cấu trúc của AD DS

Cùng xem xét đến quan hệ cha con của các Container trong hình.. Gốc của cây có 02 Container con là Finance và Sales. Cả hai đều là Container có thể chứa các Object. Sales có 02 Container con của riêng nó là Pre-Sales và Post-Sales. Chỉ có Pre-Sales có chứa các Object con, các Object này có thể là User, Computer và Group. Mỗi Object con này sẽ gọi Pre-Sales là cha và phải thực thi các chính sách được áp dụng từ cha xuống. Sơ đồ mà chúng ta vừa phân tích trong Active Directory được gọi là Domain.

UID

Với hàng triệu Object có trong cơ sở dữ liệu của Active Directory, mỗi Object cần được lưu trữ và định danh một cách riêng biệt. Để giải quyết vấn đề đó hệ thống của Microsoft đã tạo ra GUID – mã định danh cho từng Object riêng biệt. GUID được biểu diễn bởi 128 bit nhị phân theo cấu trúc của UUID của công ty DEC. UUID/GUID không được đảm bảo là duy nhất, tuy nhiên nó được đảm bảo sự không trùng lặp trong một khoảng thời gian dài. GUID của một Object vẫn tồn tại với Object đó cho đến khi nó bị xóa, kể cả trong trường hợp Object đó bị đổi tên hay di chuyển trong cây thông tin thư mục DIT của Active Directory. GUID của một Object cũng sẽ được giữ nguyên nếu chúng ta di chuyển Object này giữa các miền trong cùng một vùng đa miền. Tuy nhiên, GUID không dễ nhớ và cũng không dựa trên cấu trúc phân cấp của AD cho nên người ta đã sử dụng một cách khác để tham chiếu các Object, nó được gọi là tên riêng biệt – distinguished name (DN).

Tên riêng biệt hay distinguished name (DN) là một tiêu chuẩn trong kiến trúc LDAP được sử dụng để tham chiếu duy nhất đến một Object. Một DN trong Active Directory thường có dạng:

dc=mycorp,dc=com

Trong ví dụ trên ta có thể thấy domain gốc là mycorp.com, các thành phần được phân tách nhau bởi dấu phẩy và phân biệt bởi các tiền tố "dc" ở đầu.

Bên cạnh DN, chúng ta còn một thuật ngữ nữa đó là RDN – Relative distinguished name. RDN được dùng để tham chiếu đến một Object được chứa trong các container của một cấu trúc AD. Ví dụ về một RDN của tài khoản Administrator nằm trong container User của domain mycorp.com như sau:

cn=Administrator,cn=Users,dc=mycorp,dc=com

RDN phải luôn là duy nhất trong container mà chúng tồn tại. Trong một cấu trúc AD có thể có hai Object trùng tên với nhau tuy nhiên chúng phải được chứa trong các container khác nhau. Không thể có hai đối tượng có dùng cn là Administrator ở trong container User.

Ngoài tiền tố "dc" và "cn" ở trên, Bảng … liệt kê các tiền tố thường xuyên được sử dụng trong DN. Các tiền tố này được công bố trong RFC 2253 "Light-weight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names".

Domain và Domain Tree

Cấu trúc logic của Active Directory được xây dựng xung quanh khái niệm domain. Thuật ngữ này đã được giới thiệu trong Windows NT 3.1 và 4.0. Microsoft đã liên tục cải tiến và cập nhật cấu trúc của Active Directory, cho đến nay một domain trong Active Directory bao gồm các thành phần hay chức năng sau:

- Một cấu trúc phân cấp để lưu trữ các Object và container dựa trên giao thức X.500

- Sử dụng dịch vụ DNS làm mã định danh duy nhất.

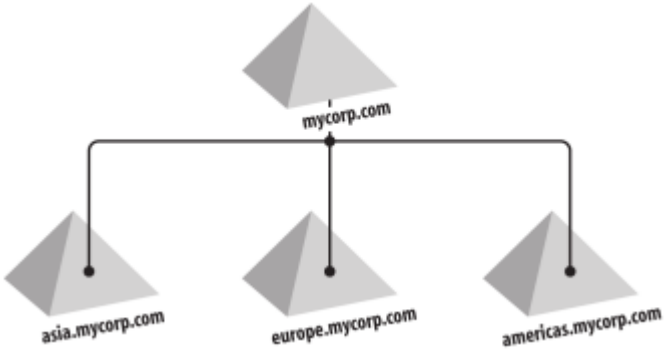
- Cung cấp dịch vụ bảo mật xác thực và cấp phép truy cập tài nguyên thông qua tài khoản trong miền.

- Các chính sách giúp quy định hoặc giới hạn các chức năng theo từng người dùng hoặc máy tính trong miền.

Một trong những thành phần không thể thiếu trong kiến trúc Active Directory là máy chủ điều khiển miền hay Domain Controller. Máy chủ này sẽ có nhiệm vụ lưu trữ cơ sở dữ liệu của Active Directory bao gồm các Object, Container và các dịch vụ liên quan. Mỗi một máy chủ DC chỉ được phép lưu trữ cơ sở dữ liệu của một domain. Khi chúng ta tiến hành nâng cấp một máy chủ lên thành máy chủ DC nếu trong hệ thống chưa tồn tại bất kì một máy chủ DC hoặc một miền nào thì mặc định miền được tạo ra sẽ là gốc của một cây domain và máy chủ DC đó sẽ chỉ được phép lưu trữ cơ sở dữ liệu của domain đã được tạo.

Trong thực tế triển khai, chúng ta có thể thấy cấu trúc cây của domain rất phù hợp cho các công ty, doanh nghiệp có nhiều chi nhánh và các bộ phận khác nhau. Lúc này mỗi đơn vị nhỏ hơn sẽ là một nhánh của cây, nó sẽ chịu quản lý theo phân cấp từ gốc cho đến các nhánh và đến từng Object riêng biệt.

Xét ví dụ với công ty MyCorp có domain mycorp.com như trong hình dưới đây.



Hình 2-2 Domain mycorp.com

Ta có thể thấy, khi miền mycorp.com được khai báo, nó sẽ mặc định là gốc của một cấu trúc gọi là cây domain, hay domain tree. Nếu Mycorp có các chi nhánh, nó sẽ được thêm vào cây domain này với vai trò là các nhánh của cây, và sẽ được đặt tên theo cấu trúc tương tự. Ví dụ như europe.mycorp.com, asia.mycorp.com, americas.mycorp.com. Cấu trúc này giúp hệ thống dễ dàng quản lý người dùng và tài nguyên, các miền trong cùng một cấu trúc cây sẽ có các quy tắc ngầm định trong việc tin tưởng lẫn nhau. Cụ thể hơn là, người quản trị của miền asia.mycorp.com có thể cho

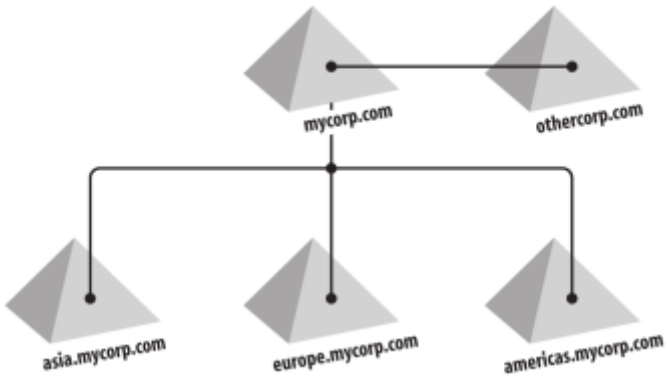
phép bất kì người dùng nào ở các miền khác truy cập vào tài nguyên của miền asia mà không bắt buộc người dùng đó phải gia nhập miền. Tuy nhiên, cần chú ý rằng các quan hệ tin cậy trong các miền không ảnh hưởng đến an ninh của hệ thống. Quyền truy cập thực tế vẫn phải được cấp bởi đội ngũ quản trị. Chính vì vậy, đội ngũ quản trị cần xem xét kĩ trước khi thực hiện cấp quyền truy cập cho người dùng trong miền.

Forest

Sau khi nắm rõ được cấu trúc của một domain tree, chúng ta cùng tìm hiểu về thành phần tiếp theo trong cấu trúc của Active Directory có tên gọi là forest. Nếu domain tree là một tập hợp của các domain thì forest là tập hợp của một hoặc vài domain tree. Toàn bộ các domain tree trong forest chia sẻ nhau các cấu trúc và cấu hình chung thông qua cơ chế chia sẻ lẫn nhau. Khi một domain được tạo ra thì mặc định cũng sẽ có một forest được tạo ra. Nếu có một domain nào khác được tham gia vào domain tree đã có hoặc có một domain tree mới được thêm vào thì vẫn chỉ tồn tại một forest trong hệ thống.

Forest được tạo ra ngay sau khi domain đầu tiên được tạo được gọi là **forest root domain**. Forest root domain là một thành phần rất quan trọng trong cấu trúc Active Directory bởi các đặc tính riêng biệt của nó. Trong Active Directory, chúng ta không thể xóa một forest root domain, nếu các quản trị viên cố gắng thực hiện việc đó thì toàn bộ hệ thống có thể bị xóa và không thể khôi phục lại được.

Chúng ta cùng xem xét lại ví dụ với công ty MyCorp, trong trường hợp công ty có một công ty con tên là Othercorp. Công ty này có tên miền là othercorp.com. Lúc này, chúng ta có thể tạo một domain tree cho othercorp.com và cho domain tree này tham gia vào forest của mycorp.com đã tồn tại. Như vậy, forest mycorp.com sẽ tồn tại cùng lúc 02 domain và mycorp.com là forest root domain. Khi đó, quản trị viên hệ thống có thể cấu hình mức độ tin cậy giữa 02 domain để cung cấp tài nguyên chung cho cả forest. Quan hệ tin cậy này có thể từ một hoặc cả hai phía. Ví dụ về cấu trúc của forest mycorp.com được thể hiện trong hình …



Hình 2-3 Cấu trúc của forest

OU

Khi chúng ta nhìn vào cấu trúc phân cấp của Active Directory, chúng ta có thể thấy nó được tạo thành từ các Object riêng lẻ và các Object có thể hoạt động như các container để chứa các đối tượng khác. OU hay Organizational Unit là một đơn vị tổ chức dùng để chứa các Object hoặc một cấu trúc phân cấp các Object và container.

Mặc dù về mặt định nghĩa OU khá giống với container tuy nhiên nó có sự khác biệt về khả năng quản trị. OU cho phép hệ thống thực thi các chính sách nhóm – Group policy lên nó. Điều này giúp cho quản trị viên có thể dễ dàng phân cấp và gán quyền quản lý các nhóm nhỏ hơn cho một người quản trị phù hợp.

Global Catalog

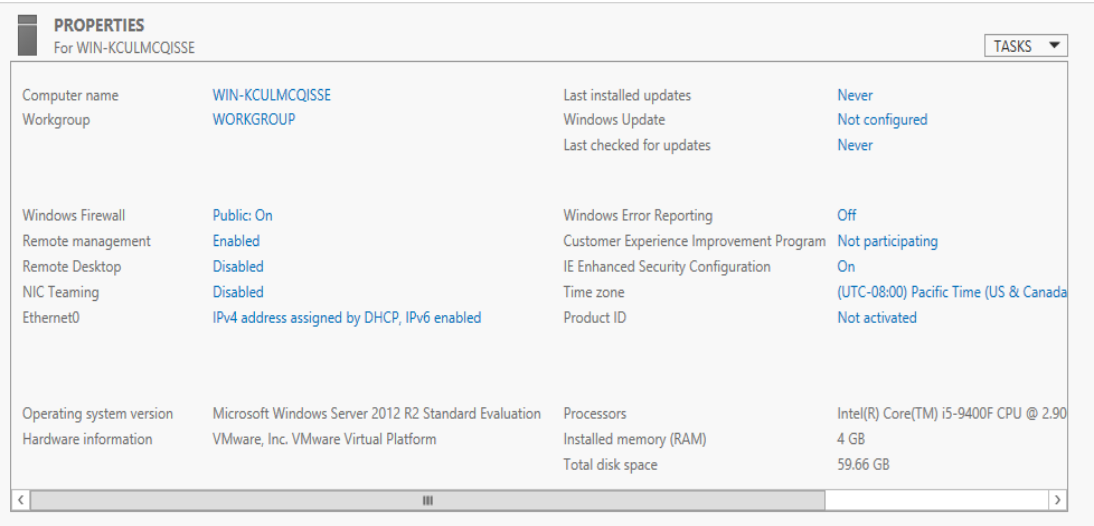
Thành phần cuối cùng và cũng là quan trọng nhất trong Active Directory có tên gọi là Global Catalog. Nó được sử dụng để thực hiện tìm kiếm trên toàn forest. Global Catalog là một danh mục bao gồm tất cả các Object và các thuộc tính cho mỗi Object. GC có thể được truy cập thông qua LDAP ở port 3268 hoặc LDAP/SSL ở port 3269. GC là một cơ sở dữ liệu dạng read-only và không thể cập nhật trực tiếp.

2.3 Triển khai AD DS

2.3.1 Post-Installation Config

Đối với bất kì hệ thống máy chủ Windows Server nào, sau khi thực hiện cài đặt hệ điều hành lên máy chủ, quản trị viên phải thực hiện một số bước cấu hình cơ bản được gọi là Post-Installation Config. Các cấu hình cơ bản này giúp đảm bảo các yếu tố về an toàn, an ninh hệ thống, đồng bộ hóa về thời gian, cấu hình mạng cũng như thay đổi tên máy chủ giúp việc quản trị trở nên dễ dàng hơn.

Để thực hiện, quản trị viên sử dụng công cụ Server Manager => lựa chọn Local Server, và thực hiện các tác vụ có trong ảnh..



Hình 2-4 Post Install Config

Các tác vụ này bao gồm

- Thực hiện đặt tên cho máy chủ
- Thực hiện bật Firewall
- Thực hiện cấu hình Remote Desktop
- Thực hiện cấu hình địa chỉ IP và NIC Teaming.
- Thực hiện cấu hình update các bản vá hệ điều hành.
- Thực hiện cấu hình đồng bộ hóa thời gian.

2.3.2 Quản trị Windows Server cơ bản

Để có thể triển khai được các dịch vụ cũng như quản trị các dịch vụ trên máy chủ Windows Server. Quản trị viên cần nắm được định nghĩa và phân biệt được vai trò của hai thành phần rất quan trọng trong Windows Server đó là Role và Features. Đây là hai khái niệm liên quan đến cách chúng ta cài đặt và quản lý các chức năng và tính năng trên hệ thống máy chủ. Cụ thể như sau:

Role: là một tập hợp các dịch vụ có các tính năng và chức năng cụ thể mà máy chủ có thể đảm nhiệm. Để một máy chủ có thể được cấu hình là máy chủ Web, máy chủ DNS hoặc máy chủ cơ sở dữ liệu. Thì người quản trị cần triển khai các Role tương ứng trong máy chủ đó.

Ví dụ: Nếu muốn cài đặt máy chủ làm nhiệm vụ Web Server, thì quản trị cần cài đặt Role có tên là IIS (Internet Information Service) đây là Role có chứa các thành phần thực hiện nhiệm vụ làm máy chủ Web.

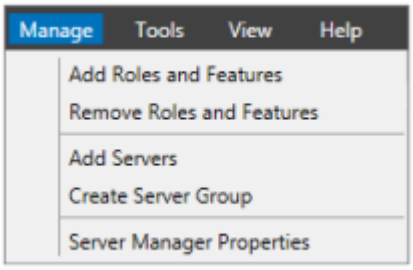
Features: Là một tính năng, một phần mềm cụ thể hoặc một thành phần của một phần mềm hoặc hệ điều hành mà chúng ta có thể cài đặt thêm hoặc gỡ bỏ nó. Tính năng này sẽ hỗ trợ hoặc thực hiện một số vai trò mà các Role cần có.

Ví dụ: Để một Webs Server có thể hỗ trợ ứng dụng ASP.NET. Chúng ta cần cài đặt Features có tên "ASP.NET" để có đầy đủ các trình biên dịch và thư viện hỗ trợ.

Để cấu hình và quản lý Role cũng như Features, quản trị viên cần thực hiện trong công cụ Server Manager.

2.3.3 Cài đặt dịch vụ Active Directory và nâng cấp máy chủ lên Domain Controller

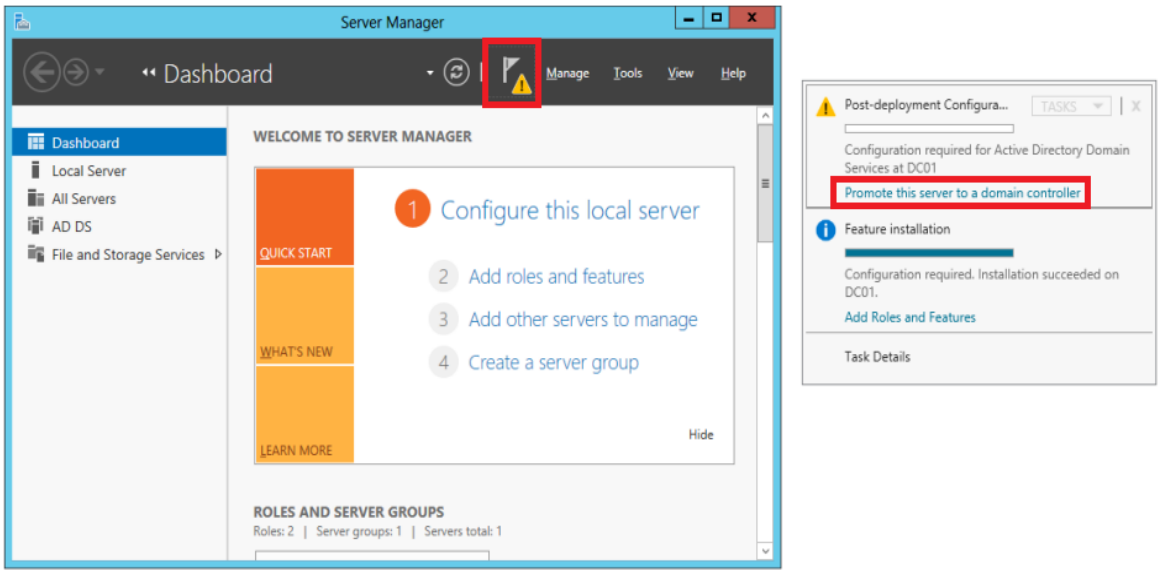
Để thực hiện cài đặt dịch vụ Active Directory lên Windows Server, bước 1 chúng ta cần khởi động công cụ Server Manager, lựa chọn Add Roles and Features như hình ..



Hình 2-5 Giao diện cài đặt Roles và Features

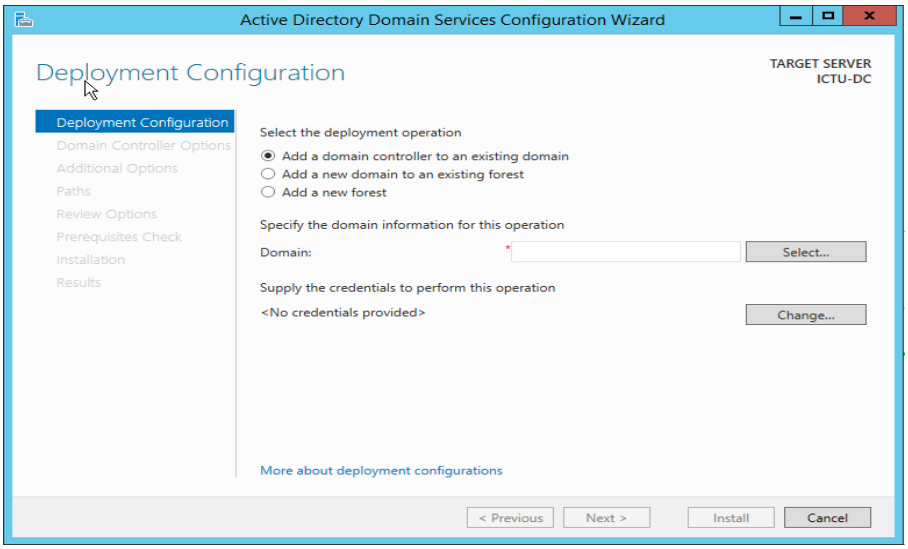
Lúc này sẽ có cửa sổ hiện lên. Chúng ta cần tích chọn vào Role: Active Directory Domain Services (AD-DS) ở bước tiếp theo, tùy theo yêu cầu của mỗi hệ thống chúng ta sẽ lựa chọn những Features cho phù hợp.

Sau khi thực hiện xong việc cài đặt Roles AD-DS ta cần thực hiện việc nâng cấp máy chủ đã có role AD-DS lên thành máy chủ Domain Controller. Việc này được thực hiện bằng cách mở lối tắt có biểu tượng lá cờ trong Server Manager như hình …



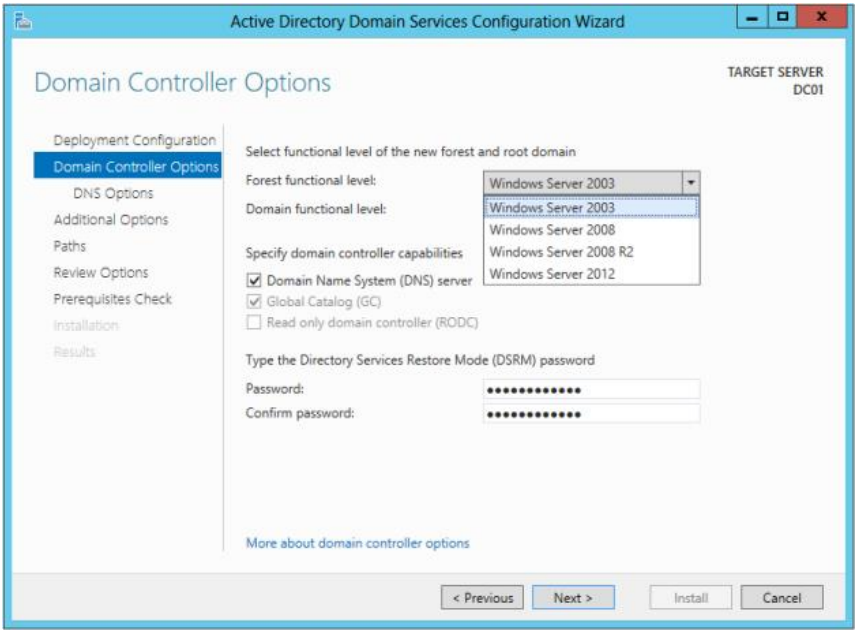
Hình 2-6 Khởi tạo một domain mới

Ở bước tiếp theo, chúng ta sẽ tiến hành khởi tạo 1 domain và forest mới hoặc gia nhập vào domain đã có.



Hình 2-7 Cấu hình tạo mới domain

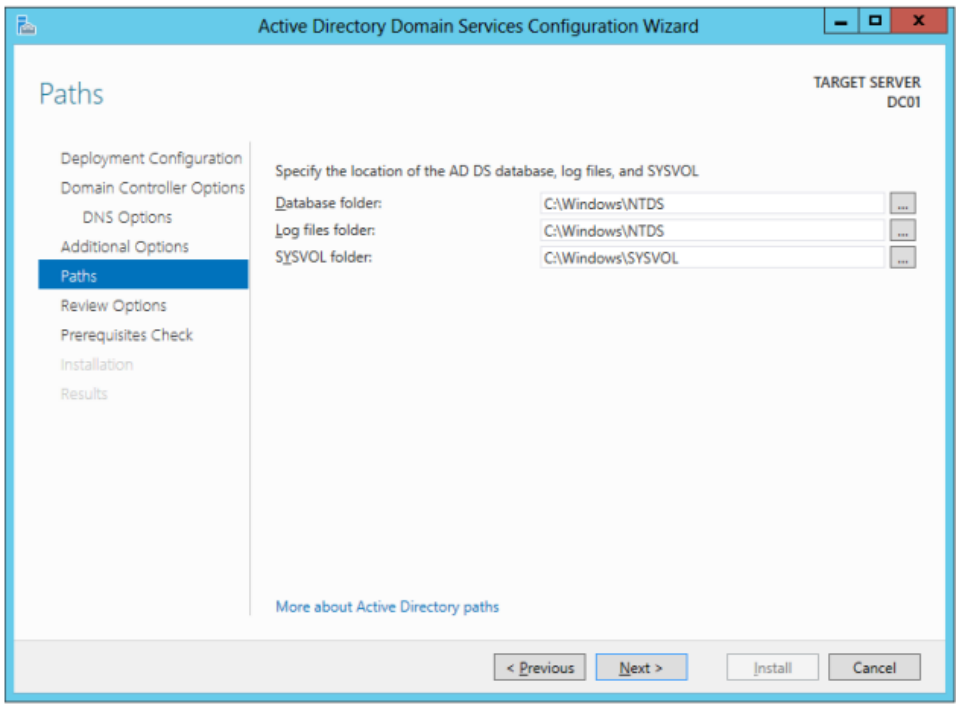
Sau đó, chúng ta cần cấu hình 2 tùy chọn liên quan đến các chức năng có trong hệ thống với tên gọi Forest Functional Level và Domain Functional Level. Forest Functional Level xác định các chức năng của các máy chủ và hệ điều hành trong forest đó. Domain Functional Level thì phụ thuộc vào hệ điều hành của máy chủ Domain Controller. Forest Functional Level thì phụ thuộc vào các domain functional level của các domain trong forest. Với mỗi phiên bản hệ điều hành Windows Server khác nhau sẽ cung cấp thêm các tính năng khác nhau, do đó có một số rằng buộc đối với việc cài đặt Functional Level. Ví dụ: mức tối thiểu để kết nối một DC chạy Windows Server 2012 với một forest đang tồn tại là forest đó phải có functional level từ Windows Server 2003 trở lên. Vì vậy, người quản trị mạng cần xem xét kĩ hiện trạng hệ thống trước khi cấu hình tùy chọn này.



Hình 2-8 Cấu hình functional level

Tiếp theo chúng ta cần cấu hình mật khẩu Directory Services Restore Mode (DSRM). Đây là mật khẩu cho phép thực hiện các tác vụ liên quan đến việc bảo trì hệ thống và khôi phục khi có sự cố. Chúng ta có thể truy cập vào chế độ này bằng cách ấn F8 khi khởi động Windows. Sau khi lựa chọn chế độ DSRM, sẽ có một thông báo yêu cầu đăng nhập, tuy nhiên lúc này dịch vụ Active Directory chưa được chạy, vì vậy chúng ta không thể sử dụng tài khoản trên domain để đăng nhập mà thay vào đó chúng ta phải sử dụng một tài khoản quản trị đặc biệt với mật khẩu đã được cài đặt ở trên. Cần phải chú ý rằng mật khẩu DSRM này là hoàn toàn khác với mật khẩu của tài khoản Administrator để quản trị hệ thống. Nó cung cấp khả năng truy cập cục bộ vào máy chủ DC và có thể truy cập đến cơ sở dữ liệu của Active Directory. Chính vì vậy, người quản trị cần chú ý trong việc đặt mật khẩu này và bảo mật cho nó.

Bước cuối cùng trong quá trình cài đặt là cấu hình vị trí lưu trữ các thư mục chứa cơ sở dữ liệu của Active Directory. Có 3 thư mục quan trọng cần phải quan tâm đó là: thư mục chứa cơ sở dữ liệu ,thư mục chứa log của hệ thống và thư mục SYSVOL. Thông thường, thư mục chứa cơ sở dữ liệu và log của hệ thống được lưu chung vào một thư mục được đặt tên là NTDS. SYSVOL là một thư mục chia sẻ giúp phân tán những cấu hình, chính sách được thực thi trên toàn hệ thống. Cần phải chú ý rằng, dung lượng của những thư mục này là rất lớn. Chính vì vậy, nó cần phải được lưu trữ ở trong các phân vùng được định dạng theo kiểu NTFS. Chi tiết về kiểu định dạng phân vùng của Windows Server sẽ được nhắc đến trong các phần sau.



Hình 2-9 Cấu hình vị trí lưu CSDL AD

Active Directory là một cơ sở dữ liệu có kích thước khá lớn, chính vì vậy các nhà phát triển đã chia nó thành 2 phần: cơ sở dữ liệu chính và nhật kí thay đổi. Những thay đổi đối với cơ sở dữ liệu sẽ được ghi vào nhật kí. Việc này giúp cung cấp khả năng phục hồi và chống chịu lỗi rất tốt cho AD, nó sẽ đảm bảo cơ sở dữ liệu ở trạng thái nhất quán khi máy chủ được khởi động lại. Mọi thay đổi được ghi vào nhật kí đều được đưa vào cơ sở dữ liệu và mọi thay đổi chưa được ghi vào nhật kí sẽ bị bỏ qua.

Trong thực tế triển khai hệ thống Active Directory, để đảm bảo về mặt hiệu suất, người ta thường chia thư mục cơ sở dữ liệu, nhật kí thay đổi và SYSVOL sang các ổ đĩa khác nhau. Ví dụ như:

C:\ drive: Hệ điều hành

D:\ drive: Active Directory database file và SYSVOL

E:\ drive: Log file

Với ví dụ này, mỗi ổ đĩa logic cần được lưu trữ trong một ổ đĩa vật lý riêng biệt. Nếu chúng ta chỉ sử dụng một ổ đĩa vật lý để tạo thành ba phân vùng logic thì sẽ không mang lại sự khác biệt nào về mặt hiệu suất. Ngoài ra, nếu các ổ đĩa vật lý có tốc độ đọc ghi dữ liệu khác nhau, thì chúng ta nên ưu tiên ổ đĩa có tốc độ nhanh nhất dành cho hệ điều hành, ổ đĩa có tốc độ nhanh thứ hai cho Log file và ổ đĩa chậm nhất sẽ được sử dụng để lưu trữ AD, SYSVOL. Chúng ta cũng có thể sử dụng thêm các giải pháp khác nhau như RAID để tăng hiệu năng của các ổ đĩa. Phần cấu hình đĩa lưu trữ này sẽ được nhắc đến trong các chương sau.

Sau khi thực hiện xong các cấu hình cần thiết, người quản trị có thể xem lại các cấu hình mình đã thực hiện ở trong mục Review Options, tiếp theo đó, hệ thống sẽ được chuyển sang bước kiểm tra các trạng thái của máy chủ Prerequisites Check. Bước này sẽ được hệ điều hành thực hiện một cách tự động, mục đích của nó là kiểm tra lại các điều kiện cần thiết của hệ thống cho việc triển khai AD. Nếu hệ thống tồn tại lỗi khiến cho việc triển khai AD không thể thực hiện được thì người quản trị cần phải hủy bỏ quá trình nâng cấp máy chủ lên Domain Controller và thực hiện sửa lỗi. Trong trường hợp hệ thống chỉ xuất hiện các cảnh báo chung, hoặc không có lỗi thì người quản trị có thể ấn nút cho phép bắt đầu quá trình nâng cấp máy chủ lên Domain Controller, quá trình này sẽ được thực hiện tự động và máy chủ sẽ tự khởi động lại sau khi hoàn thành.

2.4 Quản trị các thành phần trong AD DS

2.4.1 SID và ACL

A. SID

Tuy hệ thống **Windows Server** dựa vào tài khoản người dùng (**user account**) để mô tả các quyền hệ thống (**rights**) và quyền truy cập (**permission**) nhưng thực sự bên

trong hệ thống mỗi tài khoản được đặc trưng bởi một con số nhận dạng bảo mật **SID** (**Security Identifier**). **SID** là thành phần nhận dạng không trùng lặp, được hệ thống tạo ra đồng thời với tài khoản và dùng riêng cho hệ thống xử lý, người dùng không cần quan tâm đến các giá trị này.

Một SID bao gồm 02 trường cố định và tối đa là 15 trường bổ sung, các trường được phân tách nhau bởi dấu gạch ngang có dạng như sau:

S-v-id-s1-s2-s3-s4-s5-s6-s7-s8-s9-s10-s11-s12-s13-s14-s15

Trong đó, trường cố định đầu tiên (v) mô tả phiên bản của cấu trúc SID. Mặc định hiện Microsoft đang để giá trị là 1. Trường thứ hai (id) là thông tin định danh, nó giúp xác định vị trí của SID trong hệ thống. Các trường còn lại từ s1 đến s15 là các trường bổ sung không bắt buộc. Các trường này sẽ được sử dụng để xác định các đối tượng sử dụng SID trên toàn domain. Nó thường được gọi là RID (Relative Identifier), RID giúp đảm bảo việc không bao giờ có một SID nào trùng nhau trong một domain. Nó thực hiện bằng cách tạo ra một không gian giá trị riêng biệt của một domain, khi domain cần tạo ra một SID mới thì một giá trị RID trong không gian đó sẽ được lấy ra để sử dụng.

B. ACL và ACE

Active Directory là dịch vụ hoạt động dựa trên các đối tượng, có nghĩa là người dùng, nhóm, máy tính, các tài nguyên mạng đều được định nghĩa dưới dạng đối tượng và được kiểm soát hoạt động truy cập dựa vào bộ mô tả bảo mật ACE. Chức năng của bộ mô tả bảo mật bao gồm:

- Liệt kê người dùng và nhóm nào được cấp quyền truy cập đối tượng.
- Định rõ quyền truy cập cho người dùng và nhóm.
- Theo dõi các sự kiện xảy ra trên đối tượng.
- Định rõ quyền sở hữu của đối tượng.

Các thông tin của một đối tượng Active Directory trong bộ mô tả bảo mật được xem là mục kiểm soát hoạt động truy cập ACE (Access Control Entry). Một ACL (Access Control List) chứa nhiều ACE, nó là danh sách tất cả người dùng và nhóm có quyền truy cập đến đối tượng. ACL có đặc tính kế thừa, có nghĩa là thành viên của một nhóm thì được thừa hưởng các quyền truy cập đã cấp cho nhóm này.

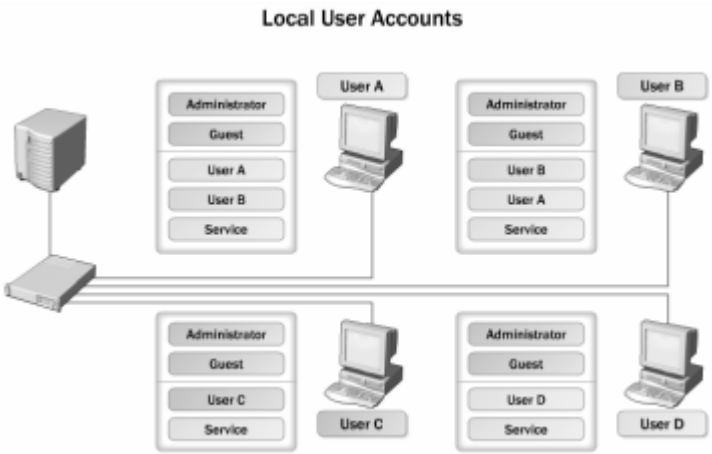
2.4.2 Quản trị tài khoản người dùng

Tài khoản người dùng (user account) là một đối tượng quan trọng đại diện cho người dùng trên mạng, chúng được phân biệt với nhau thông qua chuỗi nhận dạng username. Chuỗi nhận dạng này giúp hệ thống mạng phân biệt giữa người này và người khác trên mạng từ đó người dùng có thể đăng nhập vào mạng và truy cập các tài nguyên mạng mà mình được phép. Có hai loại tài khoản người dùng trong AD là tài khoản người

dùng cục bộ (local user account) và tài khoản người dùng trên domain (domain user account)

A. Tài khoản người dùng cục bộ

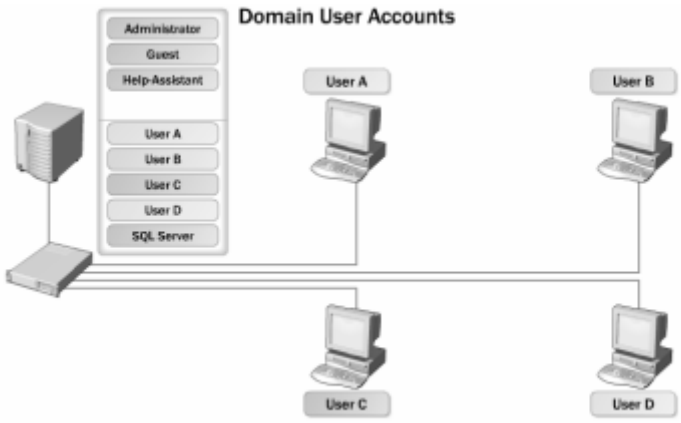
Tài khoản người dùng cục bộ (**local user account**) là tài khoản người dùng được định nghĩa trên máy cục bộ và chỉ được phép logon, truy cập các tài nguyên trên máy tính cục bộ. Nếu muốn truy cập các tài nguyên trên mạng thì người dùng này phải chứng thực lại với máy **domain controller** hoặc máy tính chứa tài nguyên chia sẻ. Chúng ta tạo tài khoản người dùng cục bộ với công cụ **Local Users and Group** trong **Computer Management** (**COMPMGMT.MSC**). Các tài khoản cục bộ tạo ra trên máy **stand-alone server**, **member server** hoặc các máy trạm đều được lưu trữ trong tập tin cơ sở dữ liệu **SAM** (**Security Accounts Manager**). Tập tin **SAM** này được đặt trong thư mục **\Windows\system32\config**.



Hình 2-10 Tài khoản người dùng cục bộ

B. Tài khoản người dùng miền

Tài khoản người dùng miền (**domain user account**) là tài khoản người dùng được định nghĩa trên **Active Directory** và được phép đăng nhập (**logon**) vào mạng trên bất kỳ máy trạm nào thuộc vùng. Đồng thời với tài khoản này người dùng có thể truy cập đến các tài nguyên trên mạng. Chúng ta tạo tài khoản người dùng miền với công cụ **Active Directory Users and Computer** (**DSA.MSC**). Khác với tài khoản người dùng cục bộ, tài khoản người dùng miền không chứa trong các tập tin cơ sở dữ liệu **SAM** mà chứa trong tập tin **NTDS.DIT**, theo mặc định thì tập tin này chứa trong thư mục **\Windows\NTDS**.



Hình 2-11 Tài khoản người dùng miền

C. Yêu cầu về tài khoản người dùng:

Mỗi username phải từ 1 đến 20 ký tự (trên Windows Server 2003 thì tên đăng nhập có thể dài đến 104 ký tự, tuy nhiên khi đăng nhập từ các máy cài hệ điều hành Windows NT 4.0 về trước thì mặc định chỉ hiểu 20 ký tự).

Mỗi username là chuỗi duy nhất của mỗi người dùng có nghĩa là tất cả tên của người dùng và nhóm không được trùng nhau.

Username không chứa các ký tự sau: " / \ [ ] : ; | = , + * ? < >

Trong một username có thể chứa các ký tự đặc biệt bao gồm: dấu chấm câu, khoảng trắng, dấu gạch ngang, dấu gạch dưới. Tuy nhiên, nên tránh các khoảng trắng vì những tên như thế phải đặt trong dấu ngoặc khi dùng các kịch bản hay dòng lệnh.

D. Tài khoản người dùng tạo sẵn.

Tài khoản người dùng tạo sẵn (**Built-in**) là những tài khoản người dùng mà khi ta cài đặt **Windows Server** thì mặc định được tạo ra. Tài khoản này là hệ thống nên chúng ta không có quyền xóa đi nhưng vẫn có quyền đổi tên (chú ý thao tác đổi tên trên những tài khoản hệ thống phức tạp một chút so với việc đổi tên một tài khoản bình thường do nhà quản trị tạo ra). Tất cả các tài khoản người dùng tạo sẵn này đều nằm trong **Container Users** của công cụ **Active Directory User and Computer**. Sau đây là bảng mô tả các tài khoản người dùng được tạo sẵn:

Tên tài khoản	Mô tả
Administrator	**Administrator** là một tài khoản đặc biệt, có toàn quyền trên máy tính hiện tại. Bạn có thể đặt mật khẩu cho tài khoản này trong lúc cài đặt **Windows Server 2003**. Tài khoản này có thể thi hành tất cả các tác vụ như tạo tài khoản người dùng, nhóm, quản lý các tập tin hệ thống và cấu hình máy in…
Guest	Tài khoản **Guest** cho phép người dùng truy cập vào các máy tính nếu họ không có một tài khoản và mật mã riêng. Mặc định là tài khoản này không được sử dụng, nếu được sử dụng thì thông thường nó bị giới hạn về quyền, ví dụ như là chỉ được truy cập **Internet** hoặc in ấn.
ILS_Anonymous_ User	Là tài khoản đặc biệt được dùng cho dịch vụ **ILS**. **ILS** hỗ trợ cho các ứng dụng điện thoại có các đặc tính như: **caller ID**, **video conferencing**, **conference calling**, và **faxing**. Muốn sử dụng **ILS** thì dịch vụ **IIS** phải được cài đặt.
IUSR_computer-name	Là tài khoản đặc biệt được dùng trong các truy cập giấu tên trong dịch vụ **IIS** trên máy tính có cài **IIS**.
IWAM_computer-name	Là tài khoản đặc biệt được dùng cho **IIS** khởi động các tiến trình của các ứng dụng trên máy có cài **IIS**.
Krbtgt	Là tài khoản đặc biệt được dùng cho dịch vụ trung tâm phân phối khóa (**Key Distribution Center**)
TSInternetUser	Là tài khoản đặc biệt được dùng cho **Terminal Services**.

2.4.3 Quản trị tài khoản nhóm

Tài khoản nhóm (**group account**) là một đối tượng đại diện cho một nhóm người nào đó, dùng cho việc quản lý chung các đối tượng người dùng. Việc phân bổ các người dùng vào nhóm giúp chúng ta dễ dàng cấp quyền trên các tài nguyên mạng như thư mục chia sẻ, máy in. Chú ý là tài khoản người dùng có thể đăng nhập vào mạng nhưng tài khoản nhóm không được phép đăng nhập mà chỉ dùng để quản lý. Tài khoản nhóm được chia làm hai loại: nhóm bảo mật (**security group**) và nhóm phân phối (**distribution group**).

A. Nhóm bảo mật

Nhóm bảo mật là loại nhóm được dùng để cấp phát các quyền hệ thống (**rights**) và quyền truy cập (**permission**). Giống như các tài khoản người dùng, các nhóm bảo mật đều được chỉ định các **SID**. Có ba loại nhóm bảo mật chính là: **local**, **global** và **universal**. Tuy nhiên nếu chúng ta khảo sát kỹ thì có thể phân thành bốn loại như sau: **local**, **domain local**, **global** và **universal**.

Local group (nhóm cục bộ) là loại nhóm có trên các máy **stand-alone Server**, **member server**, **Win2K Pro** hay **WinXP**. Các nhóm cục bộ này chỉ có ý nghĩa và phạm vi hoạt động ngay tại trên máy chứa nó thôi.

Domain local group (nhóm cục bộ miền) là loại nhóm cục bộ đặc biệt vì chúng là **local group** nhưng nằm trên máy **Domain Controller**. Các máy **Domain Controller** có một cơ sở dữ liệu **Active Directory** chung và được sao chép đồng bộ với nhau do đó một **local group** trên một **Domain Controller** này thì cũng sẽ có mặt trên các **Domain Controller** anh em của nó, như vậy **local group** này có mặt trên miền nên được gọi với cái tên nhóm cục bộ miền. Các nhóm trong mục **Built-in** của **Active Directory** là các **domain local**.

Global group (nhóm toàn cục hay nhóm toàn mạng) là loại nhóm nằm trong **Active Directory** và được tạo trên các **Domain Controller**. Chúng dùng để cấp phát những quyền hệ thống và quyền truy cập vượt qua những ranh giới của một miền. Một nhóm **global** có thể đặt vào trong một nhóm **local** của các **server** thành viên trong miền. Chú ý khi tạo nhiều nhóm **global** thì có thể làm tăng tải trọng công việc của **Global Catalog**.

Universal group (nhóm phổ quát) là loại nhóm có chức năng giống như **global group** nhưng nó dùng để cấp quyền cho các đối tượng trên khắp các miền trong một rừng và giữa các miền có thiết lập quan hệ tin cậy với nhau. Loại nhóm này tiện lợi hơn hai nhóm **global group** và **local group** vì chúng dễ dàng lồng các nhóm vào nhau. Nhưng chú ý là loại nhóm này chỉ có thể dùng được khi hệ thống của chúng ta phải hoạt động ở chế độ Windows 2003 native functional level hoặc Windows Server 2008 functional level có nghĩa là tất cả các máy Domain Controller trong mạng đều phải là Windows Server 2003 hoặc Windows 2008 Server trở lên.

B. Nhóm phân phối

Nhóm phân phối là một loại nhóm phi bảo mật, không có **SID** và không xuất hiện trong các **ACL** (**Access Control List**). Loại nhóm này không được dùng bởi các nhà quản trị mà được dùng bởi các phần mềm và dịch vụ. Chúng được dùng để phân phối thư (**e-mail**) hoặc các tin nhắn (**message**). Chúng ta sẽ gặp lại loại nhóm này khi làm việc với phần mềm **MS Exchange**.

C. Các nhóm tạo sẵn đặc biệt

Ngoài các nhóm tạo sẵn đã trình bày ở trên, hệ thống **Windows Server** còn có một số nhóm tạo sẵn đặc biệt, chúng không xuất hiện trên cửa sổ của công cụ **Active Directory User and Computer**, mà chúng chỉ xuất hiện trên các **ACL** của các tài nguyên và đối tượng. Ý nghĩa của nhóm đặc biệt này là:

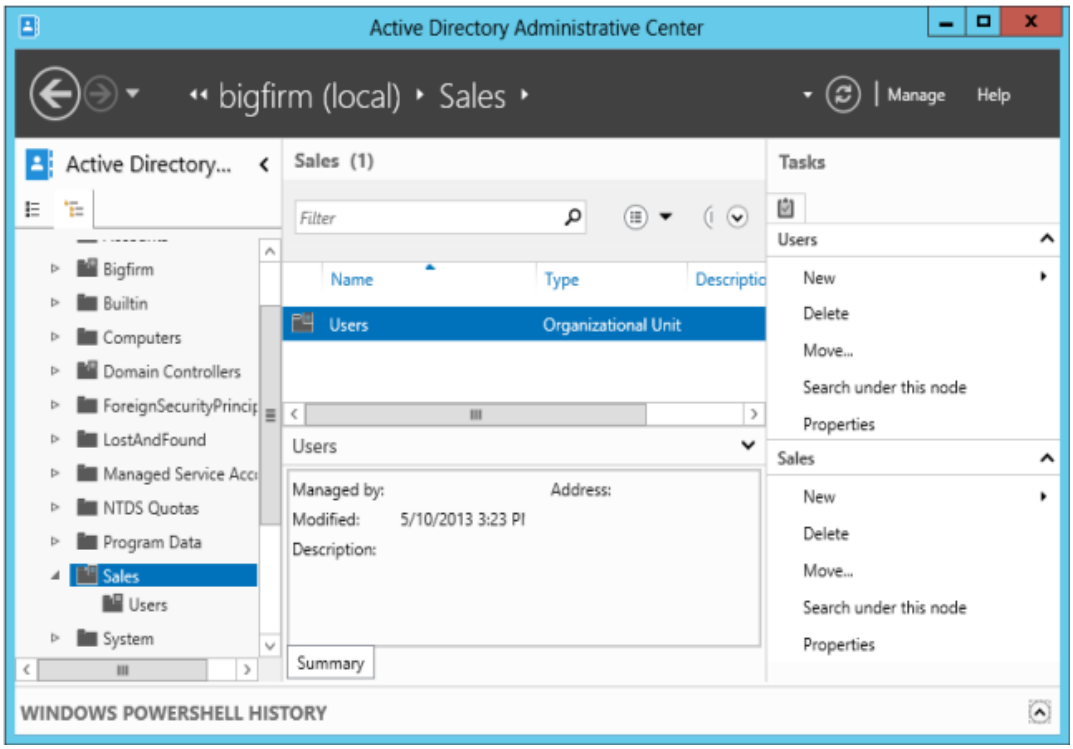
- **Interactive**: đại diện cho những người dùng đang sử dụng máy tại chỗ.
- **Network**: đại diện cho tất cả những **user** đang nối kết mạng đến một máy tính khác.
- **Everyone**: đại diện cho tất cả mọi người dùng.

- **System**: đại diện cho hệ điều hành.
- **Creator owner**: đại diện cho những người tạo ra, những người sở hữu một tài nguyên nào đó như: thư mục, tập tin, tác vụ in ấn (**print job**)…
- **Authenticated users**: đại diện cho những người dùng đã được hệ thống xác thực, nhóm này được dùng như một giải pháp thay thế an toàn hơn cho nhóm **everyone**.
- **Anonymous logon**: đại diện cho một người dùng đã đăng nhập vào hệ thống một cách nặc danh, chẳng hạn một người sử dụng dịch vụ **FTP**.
- **Service**: đại diện cho một tài khoản mà đã đăng nhập với tư cách như một dịch vụ.
- **Dialup**: đại diện cho những người đang truy cập hệ thống thông qua **Dial-up Networking**.

Các nhóm tạo sẵn đặc biệt này sẽ giúp quản trị viên dễ dàng thực hiện các tác vụ quản lý, theo dõi giám sát truy cập và xử lý sự cố khi cần.

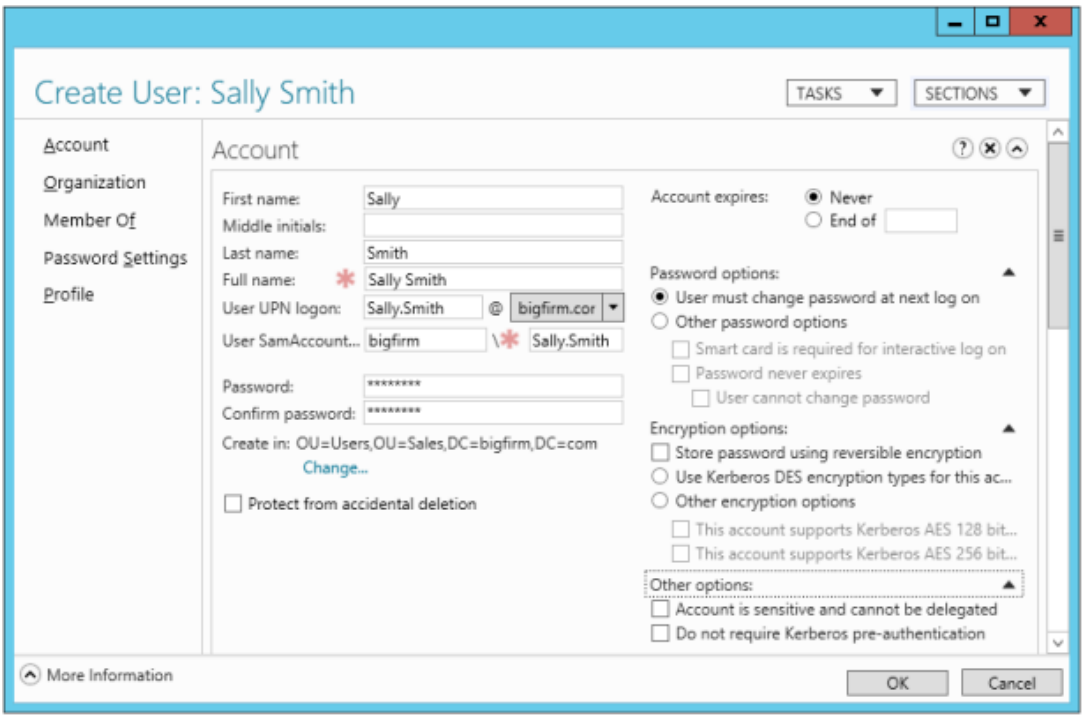
2.4.4 Bộ công cụ quản trị

Windows Server 2012 cung cấp một bộ quản trị cho AD với tên gọi Active Directory Administrative Center. Người quản trị có thể mở giao diện quản trị này bằng cách ấn vào biểu tượng Active Directory Administrative Center hoặc ấn WIN + R và chạy lệnh dsac.exe. Giao diện của bộ công cụ giống như hình …



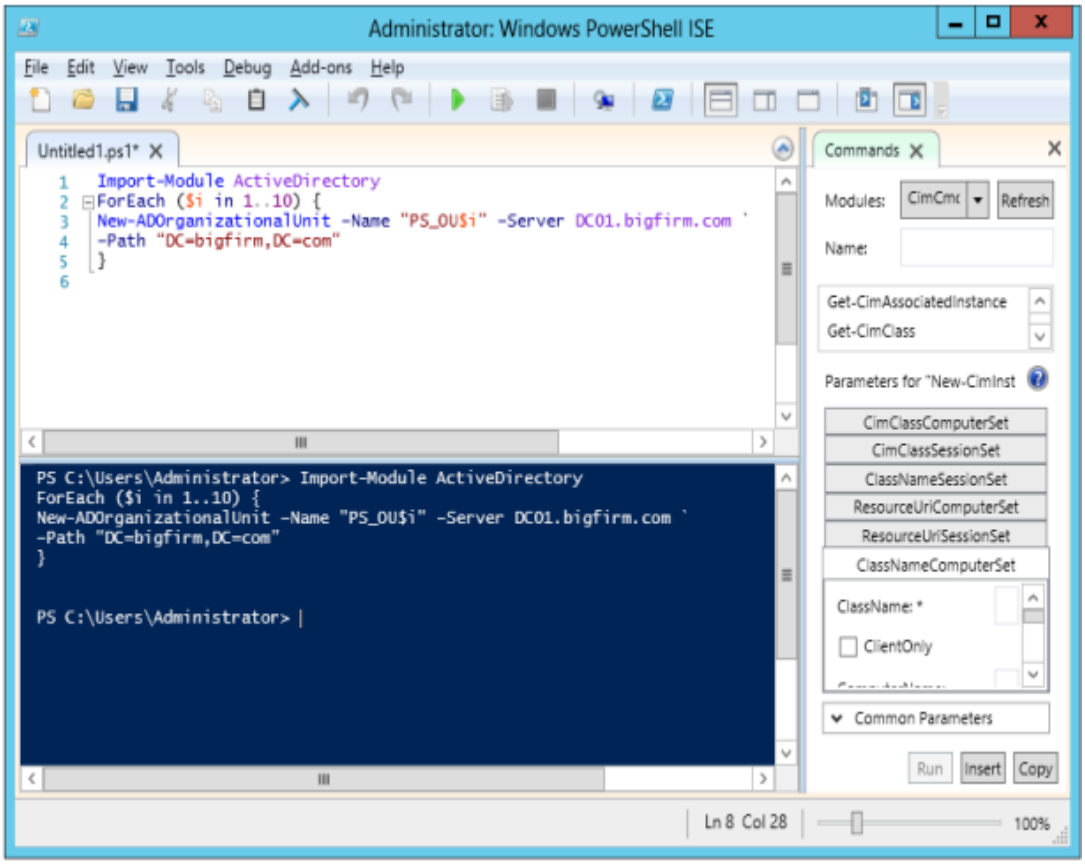
Hình 2-12 Công cụ quản trị AD

Từ giao diện này, chúng ta có thể tạo và quản lý các Object trong AD như OU, User và Group. Hình dưới mô tả giao diện khi chúng ta tạo mới một User mới trong Active Directory. Các giao diện tạo mới Group và OU tương tự như vậy. Trong giao diện này, người quản trị có thể tiến hành cấu hình thêm thông tin cho User mới, cũng như thực hiện một số yêu cầu cơ bản về bảo mật. Ví dụ như tùy chọn User must change password at next logon sẽ bắt buộc người dùng thay đổi mật khẩu ở lần đăng nhập tiếp theo. Điều này giúp tránh thói quen sử dụng mật khẩu mặc định của đa số người dùng dẫn đến việc mất an toàn trong hệ thống. Ngoài ra còn có các tùy chọn khác liên quan đến các chính sách lưu trữ và mã khóa mật khẩu của người dùng. Tùy vào vị trí cũng như quyền hạn của người dùng đó trong hệ thống, quản trị viên có thể cân nhắc để thực hiện những cấu hình sao cho phù hợp.



Hình 2-13 Khởi tạo user

Ngoài việc thực hiện cấu hình bằng giao diện, người quản trị cũng có thể thực hiện thông qua các câu lệnh với công cụ Windows Power Shell như hình dưới.



Hình 2-14 Windows Powershell

Việc sử dụng công cụ dòng lệnh như Windows PowerShell sẽ giúp tự động hóa các tác vụ quản trị một cách rất hiệu quả. Ví dụ như khi người quản trị cần tạo nhiều tài khoản người dùng, việc sử dụng giao diện sẽ tốn rất nhiều thời gian và công sức. Với Windows PowerShell người quản trị chỉ cần thực thi một đoạn lệnh như hình …

```
PS C:\Users\Administrator> Import-CSV c:\users.csv | foreach
 {New-ADUser -Name $_.Name -SamAccountName $_.SamAccountName -GivenName
 $_.GivenName -Surname $_.Surname -DisplayName $_.DisplayName -Path $_.Path
 -UserPrincipalName $_.UserPrincipalName -AccountPassword (ConvertTo-SecureString
 -AsPlainText $_.AccountPassword -Force) -Enabled $true -ChangePasswordAtLogon 1}
```

Hình 2-15 Ví dụ về câu lệnh trong PowerShell

Câu lệnh này sẽ thực hiện lấy lần lượt thông tin của từng người dùng từ file users.csv và khởi tạo người dùng đó trên hệ thống. Ngoài ra, Windows PowerShell cũng hỗ trợ thực hiện nhiều tác vụ tự động hóa khác nhau như khóa và mở khóa tài khoản người dùng, thay đổi mật khẩu, tạo nhóm,v.v. Chính vì vậy, thông thạo công cụ Windows PowerShell sẽ giúp ích rất nhiều cho việc quản trị hệ thống Active Directory trong Windows Server.

CHƯƠNG 3 GROUP POLICY (CHÍNH SÁCH NHÓM)

3.1 Giới thiệu về GPO, vai trò của GPO trong hệ thống mạng

Khi nói đến việc quản trị Active Directory, một thành phần không thể không nhắc đến chính là Group Policy. Đây là một công cụ quản lý tập trung cho phép người quản trị mạng thiết lập và áp dụng các cài đặt, hướng dẫn và hạn chế lên các thành phần trong Active Directory. Group Policy không phải là một công nghệ mới xuất hiện, nó đã có mặt trên Windows 2000, tuy nhiên với mỗi một phiên bản mới của Windows, Group Policy lại được cải tiến mạnh mẽ và đem lại nhiều hơn những cơ chế, công cụ để kiểm soát hệ thống máy tính chạy Windows. Group Policy hiện có hơn 5000 tùy chọn cài đặt khác nhau, giúp quản trị viên có thể dễ dàng kiểm soát từng thành phần trong hệ thống mạng.

Quản trị viên có thể cấu hình và triển khai Group Policy bằng cách tạo ra các Group Policy objects (GPOs). GPOs là một tập hợp các cài đặt chính sách có thể được áp dụng cho người dùng và máy tính trong hạ tầng Active Directory. Các Policy có thể được tạo ra bằng công cụ Group Policy Management Editor (GPME). Một GPOs có thể áp dụng rất nhiều chính sách khác nhau cho hệ thống, từ việc giới hạn hoặc chỉ định cài đặt một phần mềm lên máy trạm, cấu hình hạn ngạch đĩa cứng, giới hạn việc truy cập thư mục và phần mềm Explorer, quy định các chính sách về mật khẩu và khóa tài khoản.v.v. Có thể nói rằng GPOs được phép can thiệp đến hầu hết các tính năng trong một hệ điều hành Windows.

Một GPOs có hai phần chính:

Computer Configuration: Đây là các chính sách dành riêng cho việc quản trị các máy tính trong mô hình AD bao gồm: Đặt hạn ngạch cho đĩa cứng, cấu hình kiểm soát truy cập và cấu hình giám sát sự kiện.

User Configuration: Đây là các chính sách dành riêng cho việc quản trị User trong mô hình AD bao gồm: Cấu hình các ứng dụng, quản lý tùy chọn trong hệ điều hành, quản lý thư mục.

Mặc dù là hai phần cấu hình riêng trong GPOs, tuy nhiên có những tùy chọn sẽ được tồn tại trong cả hai phần Computer Configuration và User Configuration. Tùy thuộc vào điều kiện sử dụng, người quản trị có thể tạo ra một chính sách áp dụng trên cả hai phần hoặc tạo ra các chính sách riêng biệt áp dụng cho từng loại.

Các GPOs đượp áp dụng lên các đối tượng được gọi là LSDOU trong đó L – local, S – site, D – domain, OU – Organizational Unit. Mối quan hệ của GPOs với LSDOU được gọi là liên kết, đó có thể là quan hệ một – nhiều (một GPOs liên kết với

nhiều OU) hoặc là một quan hệ nhiều – một (nhiều GPOs liên kết với một OU). Khi đã áp dụng liên kết, các User Configuration sẽ ảnh hưởng đến người dùng, các Computer Configuration sẽ ảnh hưởng đến các máy tính. Các GPOs có khả năng tích lũy và kế thừa, khi đã liên kết nó với một OUs, các OUs con bên trong nó cũng sẽ chịu các chính sách đó theo thứ tự.

GPOs được chia thành hai phần Group Policy container (GPC) và Group Policy template (GPT). Các GPC được lưu trữ trong thư mục SYSVOL cùng với cơ sở dữ liệu của AD. Đường dẫn cụ thể của nó là Windows\SYSVOL\sysvol\<Domain Name>\Policies\GUID\ trong đó GUID là chỉ số định danh duy nhất dành cho GPO. Thư mục này chứa các cài đặt quản trị, cài đặt bảo mật, thông tin về các ứng dụng, các cài đặt cho hệ điều hành, các kịch bản đăng nhập, đăng xuất, và rất nhiều tùy chọn khác.

Chính sách nhóm được cập nhật trong nền mỗi 90 phút tại các máy trạm, tuy nhiên sẽ có thêm 30 phút ngẫu nhiên để các máy thực hiện việc yêu cầu cập nhật từ máy chủ. Điều này giúp máy chủ tránh được việc bị quá tải do có quá nhiều kết nối yêu cầu cập nhật cùng lúc. Mặt khác, các máy chủ miền sẽ được tự động cập nhật chính sách nhóm sau mỗi năm phút. Quản trị viên cũng có thể sử dụng một Policy trong bộ chính sách nhóm để quy định điều này. Ngoài ra có một số chính sách nhóm sẽ chỉ được áp dụng nếu như có trạng thái đăng nhập hoặc khởi động lại hệ thống. Ví dụ như các chính sách nhóm liên quan đến việc cài đặt phần mềm, chuyển hướng thư mục hoặc các tác vụ tự động khi người dùng đăng nhập.v.v. Quản trị cũng có thể thực hiện ép buộc việc cập nhật chính sách nhóm trên các máy trạm với câu lệnh trong PowerShell.

Enforced và Block Inheritance

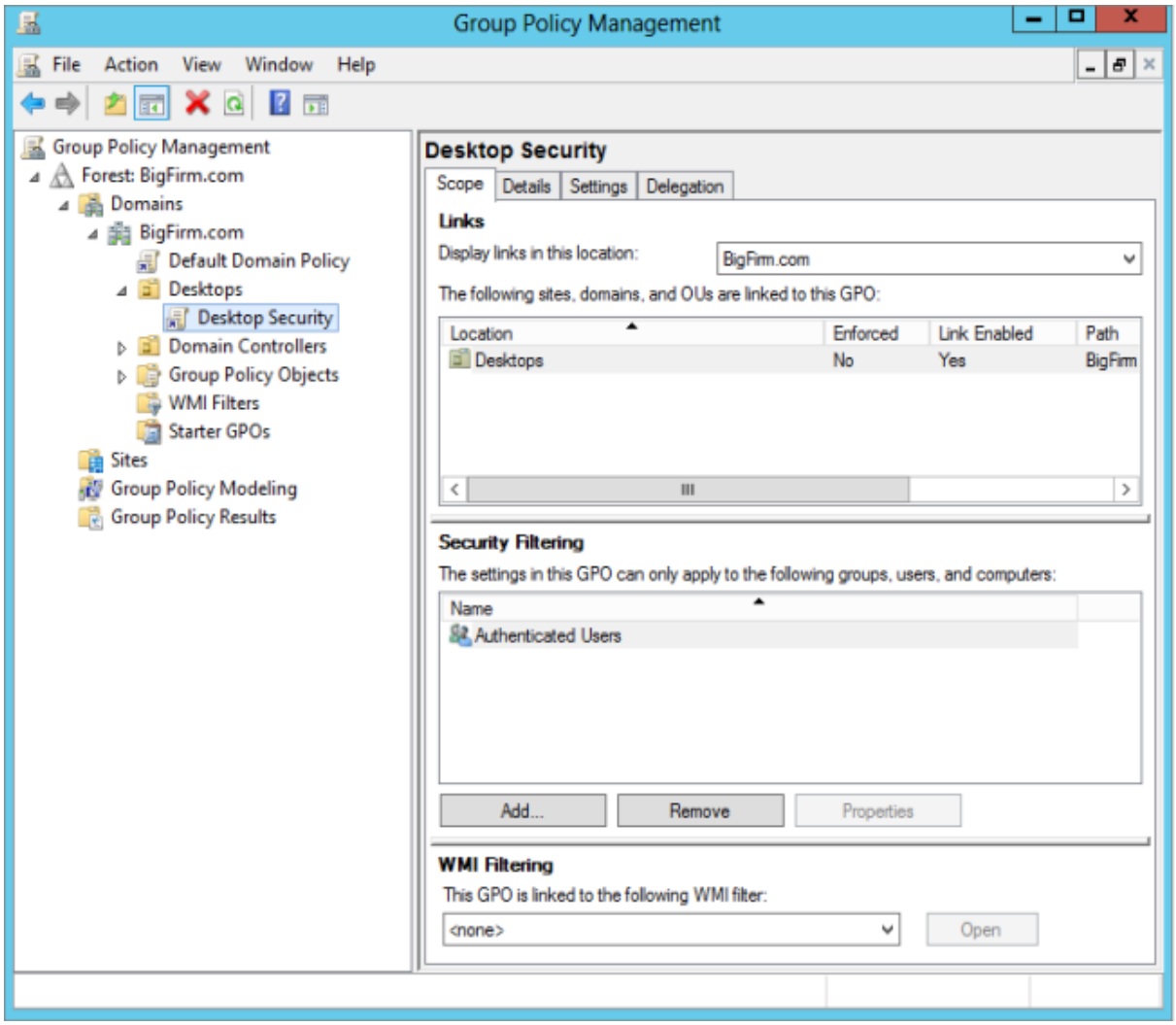
Block Inheritance là một thiết lập đặc biệt trong việc cấu hình GPOs trên AD. Nó cho phép một OU hoặc một miền từ chối các policy ở các GPOs áp dụng trên cấp cao hơn. Khi thiết lập này được bật các OU cấp thấp hơn sẽ không phải thực hiện các chính sách được áp dụng cho OU cấp trên.

Tuy nhiên, có những chính sách mà người quản trị muốn bắt buộc phải thực thi ở trên toàn miền hoặc trên một OU nhất định, thì lúc đó quản trị viên cần thực hiện bật tùy chọn Enforced ở chính sách đó. Khi tùy chọn Enforced được bật trên một chính sách thì chính sách đó sẽ luôn được thực thi ở tất cả các đơn vị mà nó được áp dụng.

Do sự mâu thuẫn giữa hai tùy chọn này, người quản trị cần kiểm tra các chính sách đang được áp dụng trên một đối tượng nhất định. Đặc biệt là thứ tự của các chính sách, chính sách đứng ở trên cùng sẽ được thực thi cuối cùng. Vì vậy cần xem xét nếu như chính sách này thực thi những cài đặt phủ định với các chính sách trước đó.

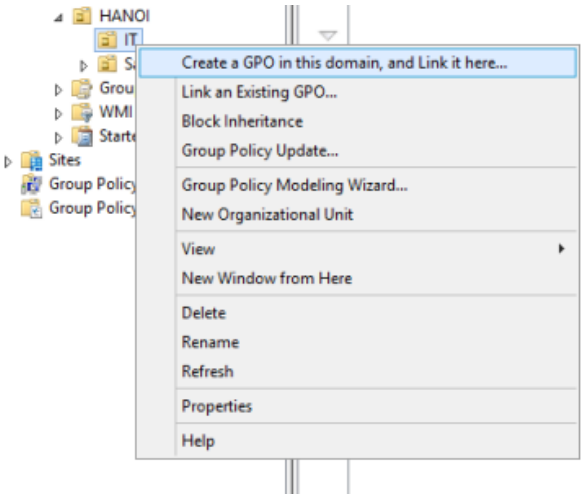
Khởi tạo một GPO

Chúng ta có thể khởi tạo một GPO bằng cách đi đến công cụ Group Policy Management trong Server Manager, hoặc truy cập vào lối tắt thông qua lệnh gpedit.msc trên cửa sổ Run. Công cụ có giao diện như hình 3-1.



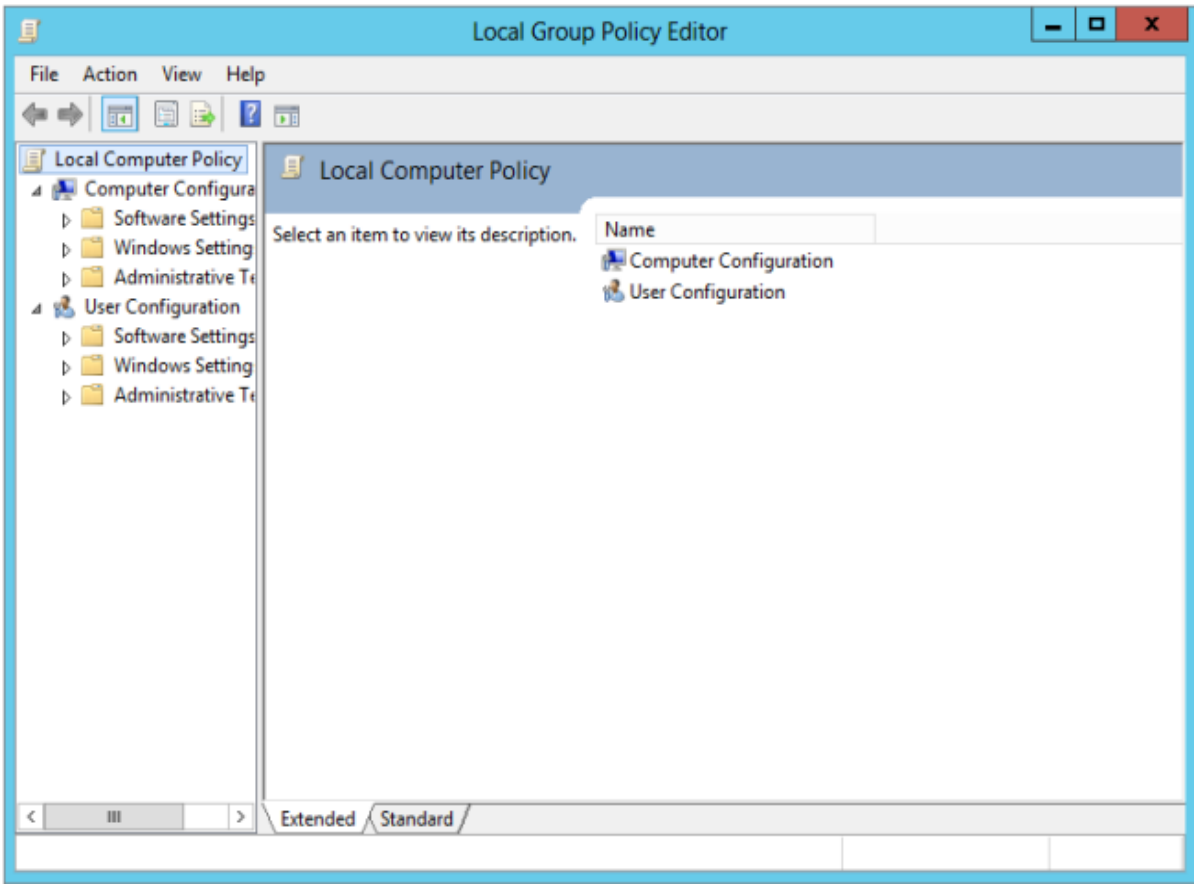
Hình 3-1 Công cụ quản trị Group Policy

Chúng ta có thể tạo một GPO mới cho một OU hoặc một domain trong forest bằng cách click chuột phải vào tên OU hoặc domain muốn tạo và chọn Create a GPOs in this domain, and Link it here như hình



Hình 3-2 Thao tác khởi tạo GPO

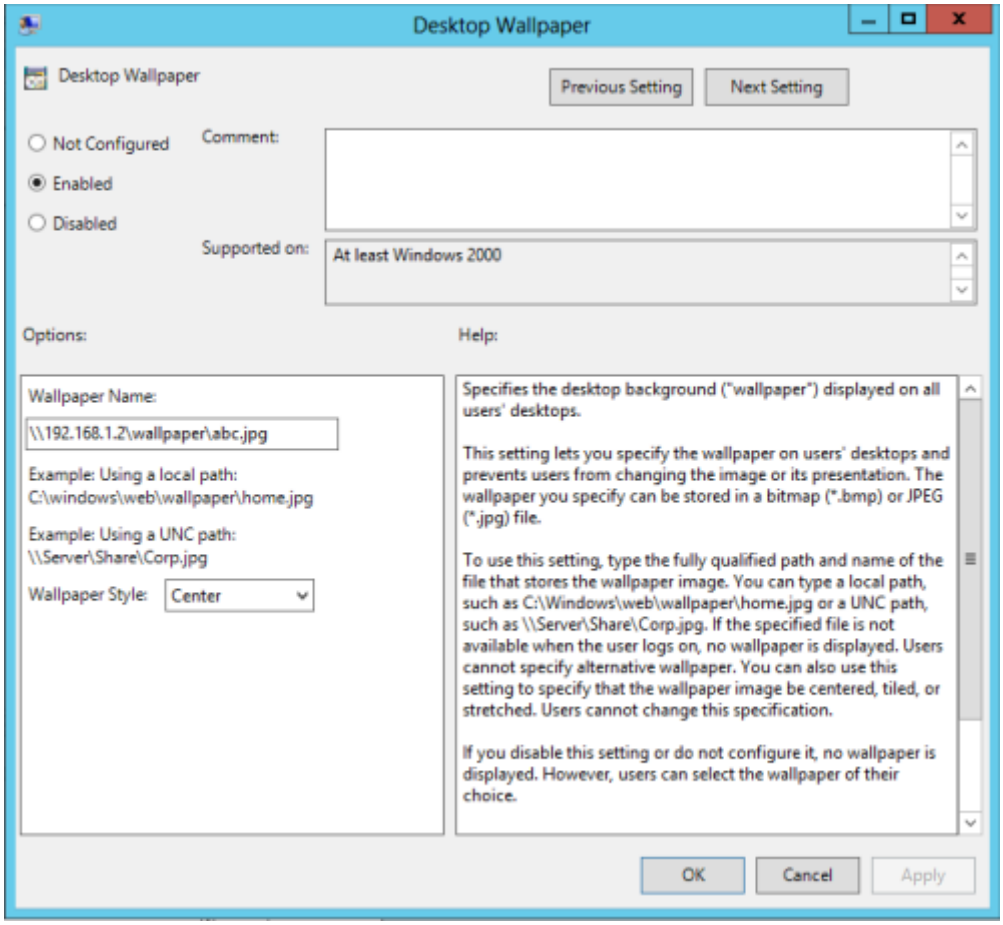
Sau khi khởi tạo xong chúng ta có thể chuột phải vào GPO đó và lựa chọn Edit để bắt đầu cấu hình các chính sách cho nó. Giao diện cấu hình chính sách giống như hình dưới.



Hình 3-3 Giao diện cấu hình GPO

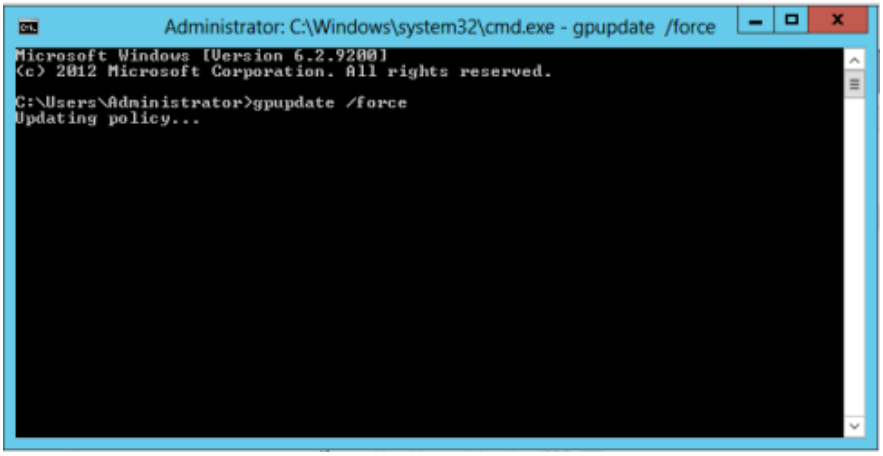
Trong đó menu bên trái là các tùy chọn cấu hình được phân chia theo từng phần, bên phải là các cấu hình chi tiết và giải thích nếu có. Người quản trị sẽ phải thực hiện tìm kiếm những tùy chọn cấu hình phù hợp với chính sách mà mình đang muốn áp dụng.

Một cấu hình ban đầu sẽ có ba tùy chọn như hình 3-4. Tùy chọn Not Configured thể hiện việc cấu hình này chưa được thực hiện và sẽ không có hành động nào được thực hiện. Tùy chọn Enabled sẽ tiến hành thực thi cấu hình này. Và tùy chọn Disabled sẽ tiến hành ngăn chặn việc thực thi cấu hình này.



Hình 3-4 Giao diện cấu hình chính sách

Sau khi cấu hình xong một GPOs, chúng ta có thể để cho các máy tính tự động cập nhật GPOs mới sau mỗi 90 phút. Hoặc chúng ta thực hiện việc yêu cầu cập nhật với câu lệnh gpupdate /force như trong hình 3-5.



Hình 3-5 Cập nhật GPO

3.2 Cấu hình GPO cho máy chủ cục bộ

Chính sách cục bộ (**Local Policies**) cho phép chúng ta thiết lập các chính sách giám sát các đối tượng trên mạng như người dùng và tài nguyên dùng chung. Đồng thời dựa vào công cụ này chúng ta có thể cấp quyền hệ thống cho các người dùng và thiết lập các lựa chọn bảo mật.

Chính sách cục bộ bao gồm ba phần: Các chính sách kiểm toán (Audit Policy), Gán quyền hệ thống cho người dùng (User Rights Assignment) và các tùy chọn bảo mật (Security Options).

Audit Policy

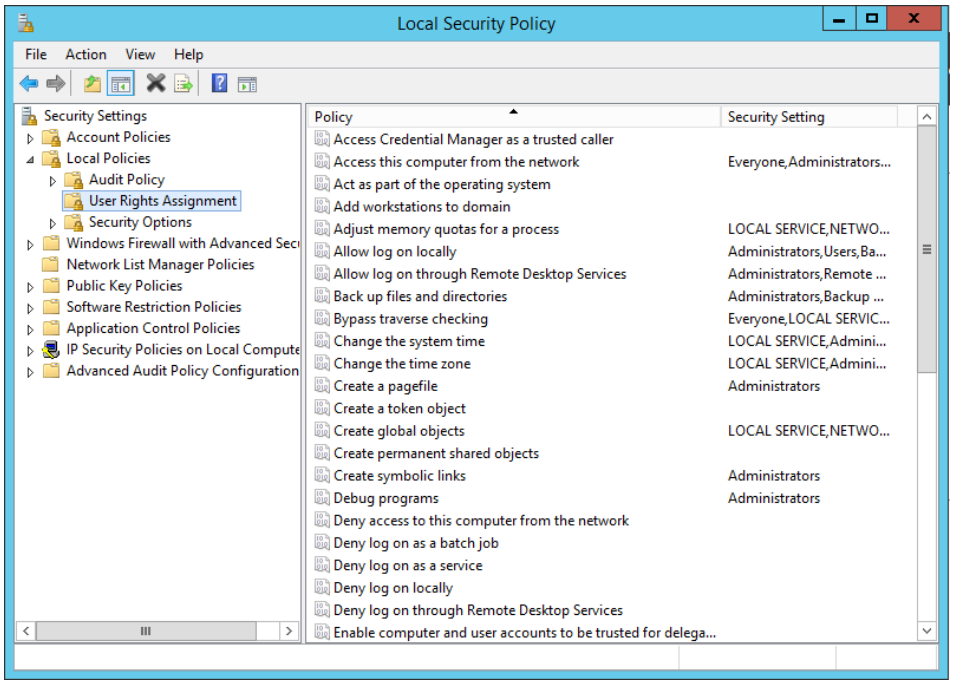
Chính sách kiểm toán giúp chúng ta có thể giám sát và ghi nhận các sự kiện xảy ra trong hệ thống, trên các đối tượng cũng như đối với người dùng. Chúng ta có thể xem lại nhật kí các sự kiện thông qua công cụ Event Viewer. Các tùy chọn kiểm toán được thể hiện trong hình 3-6. Chi tiết về các tùy chọn này sẽ được bàn đến trong các chương sau.

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Hình 3-6 Các chính sách kiểm toán

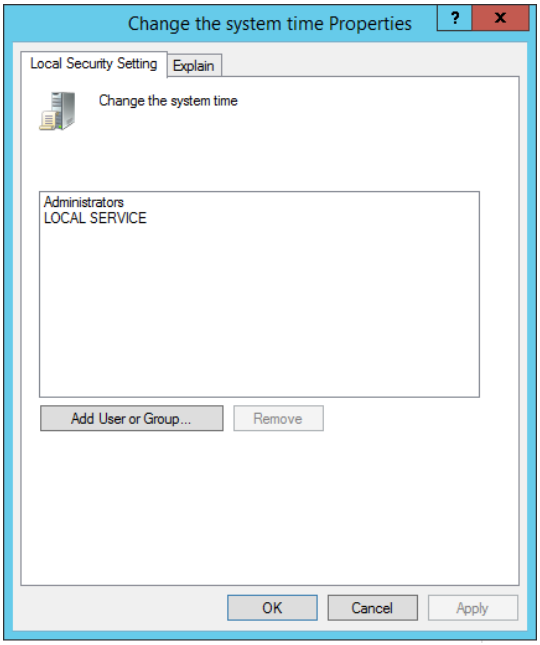
User Rights Assignment

Đối với các hệ thống Windows Server, chúng ta có hai cách cấp quyền hệ thống cho người dùng đó là: Thêm tài khoản người dùng đó vào các nhóm tạo sẵn (built-in) để kế thừa quyền, hoặc sử dụng Local Policy để gán các quyền hạn bằng cài đặt User Rights Assignment.



Hình 3-7 Quyền hệ thống

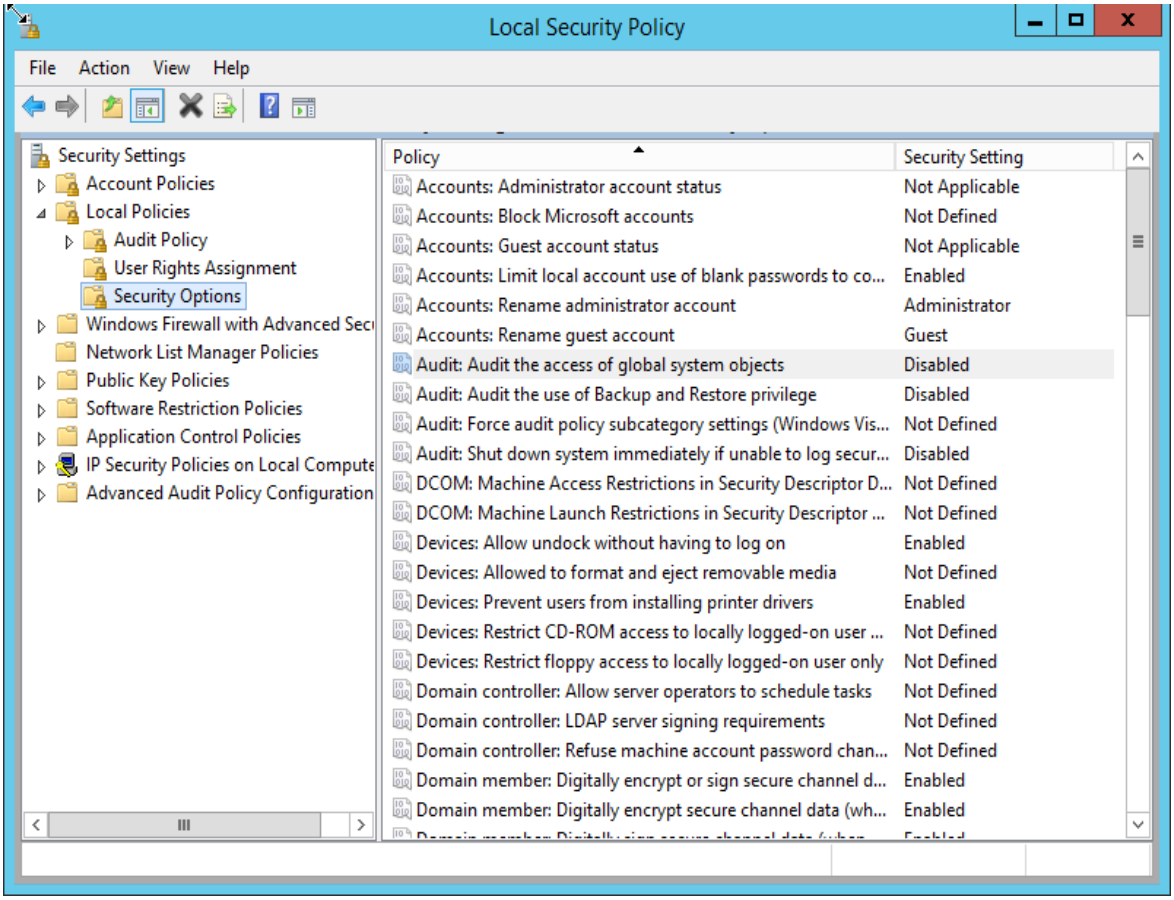
Cài đặt User Rights Assignment trong Local Security Policy có chứa rất nhiều tùy chọn cấu hình các hành động đối với hệ thống, cụ thể như các thao tác: đăng nhập, đăng xuất, khởi động lại hoặc tắt máy, các thao tác thay đổi cấu hình ngày giờ, cấu hình mạng,v.v. Để thêm hoặc bớt một quyền hệ thống cho người dùng hoặc nhóm, chúng ta click chọn vào quyền được chọn, nó sẽ xuất hiện một hộp thoại chứa danh sách người dùng và nhóm hiện tại đang có quyền này. Chúng ta có thể nhấp chuột vào nút Add để thêm người dùng và nhóm vào danh sách.



Hình 3-8 Thêm quyền hệ thống cho người dùng

Security Options

Đây là các tùy chọn cho phép người quản trị máy chủ khai báo thêm các thông số hoặc các quy tắc nhằm tăng tính bảo mật cho hệ thống như: không cho phép đổi tên tài khoản người dùng tạo sẵn, giám sát việc truy cập các đối tượng, không cho phép hiển thi các tài khoản đã logon trước đó,.v.v



Hình 3-9 Các tùy chọn bảo mật

Để cấu hình một tùy chọn thì người quản chỉ chỉ cần nhập chuột vào tên tùy chọn đó và lựa chọn Enable hoặc Disabled. Các tùy chọn được để ở dạng Not Defined là các cấu hình mặc định và chưa được thực thi trên hệ thống.

Account Policies

Bộ chính sách tài khoản là tập hợp các cấu hình liên quan đến việc khởi tạo, quản lý và sử dụng tài khoản của người dùng. Bộ chính sách tài khoản tồn tại trong nhóm các chính sách cục bộ và sẽ được nâng cấp lên thành chính sách dành cho toàn domain trong mô hình Active Directory.

Bộ chính sách tài khoản bao gồm ba cấu hình: Password Policy, Account Lockout Policy và Keberos Policy

Password Policy: Là tập hợp các chính sách quy định việc khởi tạo và lưu trữ mật khẩu của tài khoản người dùng, nó bao gồm các tùy chọn như sau:

Enforce Password History: Tùy chọn này chỉ định số lượng mật khẩu khác nhau liên tiếp mà người dùng cần sử dụng trước khi sử dụng lại một mật khẩu cũ. Ví dụ: Giả sử tùy chọn này được đặt bằng 05, thì người dùng sẽ phải nhập 05 mật khẩu khác nhau cho mỗi lần thay đổi mật khẩu kế tiếp, trước khi được sử dụng lại mật khẩu cũ. Giá trị mặc định của tùy chọn này là 0 đối với stand-alone server và 24 đối với domain server.

Maximum Password Age: Tùy chọn này quy định thời gian tối đa tính theo ngày mà một mật khẩu của người dùng được tồn tại trong hệ thống. Khi hết thời gian này, hệ thống sẽ yêu cầu người dùng tạo mật khẩu mới. Thời gian này thường được đặt mặc định trong khoảng 30~90 ngày.

Minimum Password Age: Tùy chọn này quy định thời gian tối thiểu một mật khẩu phải tồn tại trong hệ thống trước khi hệ thống cho phép người dùng thay đổi mật khẩu mới.

Minimum Password Length: Tùy chọn này quy định độ dài tối thiểu của một mật khẩu do người dùng tạo ra. Giá trị mặc định trên domain server là 7, còn trên stand-alone server là 0 tức là cho phép không có mật khẩu.

Passwords must meet complexity requirements: Tùy chọn này yêu cầu mật khẩu của người dùng phải đáp ứng các tiêu chuẩn về độ phức tạp. Cụ thể như là: phải có độ dài tối thiểu là 6 kí tự, không chứa tên người dùng hoặc một phần của tên người dung, phải bao gồm một kí tự viết hoa (A-Z), kí tự viết thường (a-z), kí tự số (0-9) và kí tự đặc biệt (@,#,$,%).

Store passwords using reversible encryption: Đây là một tùy chọn khá đặc biệt, vì nó cho phép lưu trữ mật khẩu dưới dạng mã hóa có thể đảo ngược. Điều này khác với thông thường khi mà mã hóa trong AD được lưu dưới dạng hàm băm một chiều.

Account Lockout Policy: Đây là các chính sách hạn chế những người dùng đăng nhập thất bại nhiều lần liên tục. Có 3 tùy chọn cấu hình chính bao gồm:

Account Lockout Duration: Tùy chọn này sẽ xác định thời gian tài khoản bị khóa khi đăng nhập thất bại vượt quá số lần quy định.

Account Lockout Threshold: Tùy chọn này xác định số lần người dùng có thể đăng nhập thất bại trước khi tài khoản bị khóa.

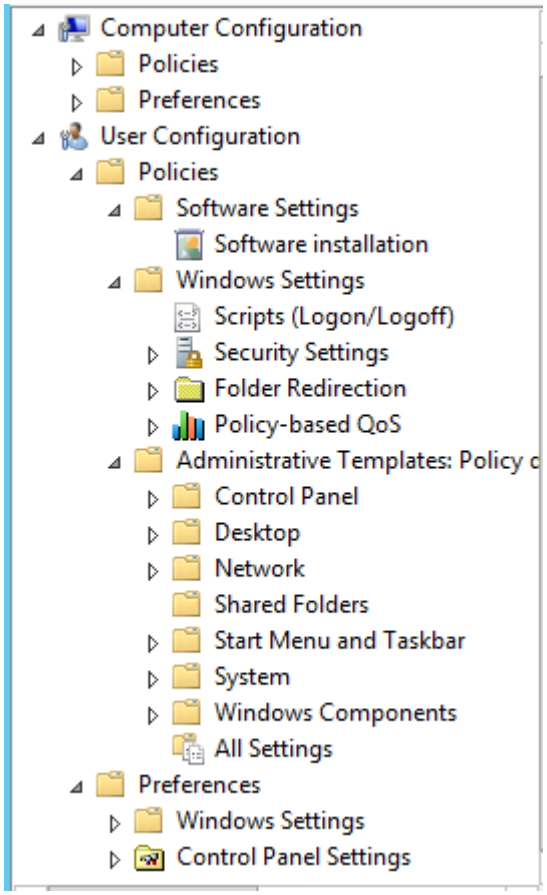
Reset Account Lockout Counter After: Tùy chọn này xác định khoảng thời gian mà bộ đếm số lần đăng nhập thất bại được xóa và đếm lại từ đầu. Ví dụ nếu chúng ta đặt tùy chọn này là 2 phút và ngưỡng đăng nhập thất bại là 3 lần. Thì sau 2 lần nhập sai, chúng ta có thể chờ 2 phút để bộ đếm bị xóa và chúng ta có thể thử lại 3 lần.

Kerberos Policy: Phần cuối cùng trong các chính sách tài khoản là các quy định về hệ thống xác thực và phân phối khóa sử dụng cơ chế Kerberos. Các tùy chọn này cho

phép người quản trị cấu hình thông tin về thời hạn sử dụng khóa, thời gian gia hạn sử dụng.v.v.

3.3 Cấu hình GPO cho máy trạm và người dùng

Group Policy cung cấp cho người quản trị rất nhiều tùy chọn trong việc quản lý hệ thống các máy trạm trong mạng và người dùng. Có thể kể đến như việc giới hạn truy cập vào một số công cụ trong Windows, tiến hành cài đặt phần mềm từ xa, thiết lập các kịch bản tự động hóa khi khởi động máy tính, giới hạn sử dụng phần mềm và bao gồm cả cài đặt hệ điều hành thông qua mạng LAN. Mỗi chính sách lại được phân chia vào các thư mục tùy theo đặc thù của nó. Ví dụ như chính sách về giới hạn quyền truy cập và sử dụng các công cụ quản trị hệ điều hành Windows như Control Panel sẽ được đặt trong thư mục Administrative Templates. Các chính sách liên quan đến phần mềm sẽ được đặt trong thư mục Software Settings. Chi tiết về cấu trúc thư mục chứa các bộ chính sách nhóm được thể hiện trong hình 3-10.



Hình 3-10 Cấu trúc thư mục chứa GPO

Tùy vào mỗi chính sách, người quản trị có thể chỉ cần kích hoạt hoặc vô hiệu hóa chính sách. Cũng có thể cần tiến hành cấu hình thêm các thông tin bổ sung.

3.4 Xử lý sự cố với GPOs

Group Policy là một bộ công cụ rất hữu ích cho việc quản trị hệ thống, tuy nhiên sức mạnh của nó cũng đi kèm với sự phức tạp. Đặc biệt với các mô hình AD có quy mô lớn, có cấu trúc phức tạp, sẽ xuất hiện tình huống policy đã được cấu hình nhưng lại không hoạt động. Khi đó người quản trị cần sử dụng những công cụ hỗ trợ để kiểm tra trạng thái hoạt động của các policy.

Công cụ Resultant Set of Policy Tool (RSOP): Đây là một bộ công cụ được tích hợp sẵn trong Windows Server nó cho phép thực hiện thử nghiệm các policy trên hệ thống. Sử dụng RSOP chúng ta sẽ biết được chính sách mà chúng ta triển khai có tác động như thế nào đến người dùng hoặc máy tính trong mạng. RSOP có thể được khởi chạy thông qua câu lệnh rsop.msc.

Công cụ Group Policy Result: Đây là một công cụ có sẵn trong tùy chọn của bộ công cụ quản trị Group Policy. Công cụ này cho phép truy vấn đến từng người dùng, máy tính trong AD để kiểm tra tác động của những Group Policy đến đối tượng đó. Nó cũng cung cấp một bảng thông tin tổng quan như hình … giúp quản trị viên dễ dàng kiểm soát trạng thái của từng Policy.

Câu lệnh gpresult trong PowerShell: Câu lệnh này giúp hiển thị trạng thái áp dụng các chính sách của một máy tính trong hệ thống.

Công cụ Event Viewer: hoạt động của Group Policy trong hệ thống đều được lưu trữ dưới dạng các log file. Công cụ Event Viewer sẽ giúp chúng ta tìm được và kiểm tra những log file đó thông qua đường dẫn Applications and Services Logs\Microsoft\Windows\GroupPolicy.

CHƯƠNG 4 QUẢN TRỊ TÀI NGUYÊN VÀ PHÂN QUYỀN

4.1 Quản trị ổ đĩa

4.1.1 Ổ đĩa vật lý

Ổ đĩa cứng trên máy chủ đóng vai trò cực kỳ quan trọng trong việc lưu trữ dữ liệu và đảm bảo hoạt động ổn định của hệ thống. Khi chọn ổ đĩa cứng cho máy chủ, cần xem xét các yếu tố sau:

Hiệu suất:

Tốc độ đọc/ghi: Ổ đĩa nhanh giúp tăng hiệu suất xử lý dữ liệu và tải trọng công việc.

Chỉ số IOPS (Input/Output Operations Per Second): Số lần đọc/ghi mà ổ đĩa có thể thực hiện trong một giây. Đây là yếu tố quan trọng cho các ứng dụng đòi hỏi hiệu suất cao.

Dung lượng:

Lớn và linh hoạt: Cần đáp ứng nhu cầu lưu trữ hiện tại và tương lai của hệ thống mà không gặp vấn đề về không gian lưu trữ.

Độ tin cậy và tuổi thọ:

MTBF (Mean Time Between Failures): Thời gian trung bình giữa các lỗi hoạt động. Càng cao càng tốt, vì nó đảm bảo ổ đĩa ít gặp sự cố.

TBW (Total Bytes Written): Số lượng dữ liệu có thể được ghi trên ổ đĩa trước khi nó trở nên không tin cậy. Đây là một yếu tố quan trọng đối với SSD.

Loại ổ đĩa:

SSD (Solid State Drive): Nhanh hơn HDD, ít tiêu tốn năng lượng, không gây tiếng ồn, thích hợp cho các ứng dụng yêu cầu tốc độ cao.

HDD (Hard Disk Drive): Dung lượng lớn hơn, giá thành thấp hơn, phù hợp cho việc lưu trữ dữ liệu lớn với chi phí hợp lý.

Giao diện kết nối:

SATA: Phổ biến cho các ổ đĩa thông thường.

SAS (Serial Attached SCSI): Hỗ trợ hiệu suất cao, độ tin cậy và tính tương thích với các hệ thống chuyên nghiệp.

Tính khả dụng và backup:

Redundancy (sự dự phòng): Có thể sử dụng RAID (Redundant Array of Independent Disks) để tăng tính khả dụng và bảo vệ dữ liệu trong trường hợp ổ đĩa gặp sự cố.

Backup: Quy trình sao lưu dữ liệu định kỳ để đảm bảo an toàn cho thông tin quan trọng.

Khi chọn ổ đĩa cứng cho máy chủ, cần phải đánh giá kỹ lưỡng các yếu tố trên để đảm bảo rằng hệ thống có thể hoạt động ổn định, đáng tin cậy và phù hợp với mục tiêu sử dụng cụ thể.

4.1.2 Cấu hình ổ đĩa vật lý

Trên Windows, có hai loại cơ bản khi đề cập đến quản lý đĩa lưu trữ: Basic Disk (đĩa cơ bản) và Dynamic Disk (đĩa động).

A, Basic storage

Là kiểu cấu hình đĩa lưu trữ cơ bản. Bao gồm các **partition primary** và **extended**. **Partition** tạo ra đầu tiên trên đĩa được gọi là **partition primary** và toàn bộ không gian cấp cho **partition** được sử dụng trọn vẹn. Mỗi ổ đĩa vật lý có tối đa bốn **partition**. Chúng ta có thể tạo ba **partition primary** và một **partition extended**. Với **partition extended**, chúng ta có thể tạo ra nhiều **partition logical**.

A, Dynamic Storage

Đây là một tính năng mới của **Windows Server**. Đĩa lưu trữ dynamic chia thành các **volume dynamic**. **Volume dynamic** cung cấp khả năng hỗ trợ RAID mềm trên Windows mà không cần sử dụng phần cứng. Ưu điểm của công nghệ **Dynamic storage** so với công nghệ **Basic storage**:

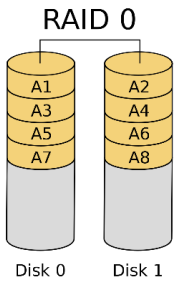
- Cho phép ghép nhiều ổ đĩa vật lý để tạo thành các ổ đĩa **logic** (**Volume**).
- Cho phép ghép nhiều vùng trống không liên tục trên nhiều đĩa cứng vật lý để tạo ổ đĩa **logic**.
- Có thể tạo ra các ổ đĩa logic có khả năng dung lỗi cao và tăng tốc độ truy xuất…

4.1.3 RAID

RAID (Redundant Array of Independent Disks) là một phương pháp kết hợp nhiều ổ đĩa cứng vật lý thành một hệ thống lưu trữ logic. Mục tiêu chính của RAID là cải thiện hiệu suất, độ tin cậy hoặc cả hai, tùy thuộc vào cấu hình cụ thể của nó. Trên các hệ thống máy chủ RAID có thể được cung cấp thông qua phần cứng bằng một thiết bị đặc biệt gọi là RAID card, hoặc được cấu hình trên phần mềm thông qua hệ điều hành.

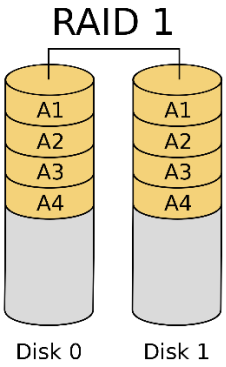
Có 4 loại cấu hình RAID phổ biến như sau:

RAID 0: Phân chia dữ liệu thành các đoạn nhỏ và lưu trữ lần lượt trên các ổ đĩa khác nhau. Nó cải thiện tốc độ đọc/ghi bằng cách phân tán dữ liệu trên nhiều ổ đĩa. Tuy nhiên, không có tính năng dự phòng nên nếu một ổ đĩa hỏng, toàn bộ dữ liệu có thể mất.



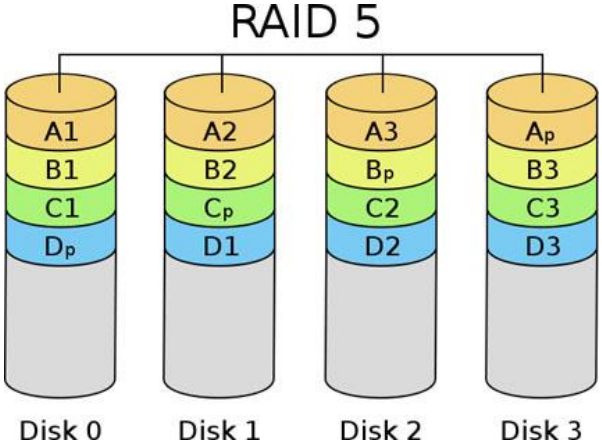
Hình 4-1 RAID 0

RAID 1: Dữ liệu được sao chép đồng thời trên hai ổ đĩa khác nhau. Đây là cấu hình có độ tin cậy cao vì nếu một ổ đĩa hỏng, dữ liệu vẫn được bảo toàn trên ổ đĩa còn lại. Tuy nhiên, hiệu suất không được đảm bảo do phải mất thời gian nhân bản dữ liệu. Do vậy, trong các hệ thống triển khai RAID 1 cần sử dụng thêm các ổ đĩa có tốc độ truy xuất cao làm bộ nhớ đệm. RAID 1 cũng là kiểu RAID thông dụng nhất được sử dụng trong các hệ thống lưu trữ hiện nay.



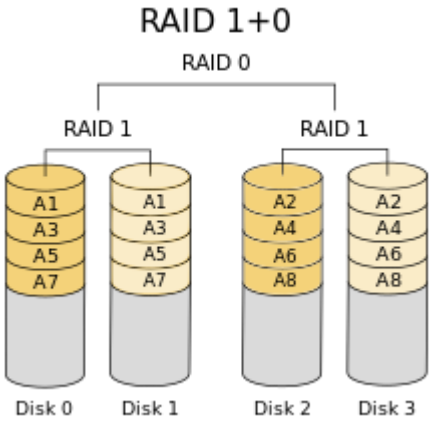
Hình 4-2 RAID 1

RAID 5: Dữ liệu được chia thành các khối nhỏ và phân tán trên nhiều ổ đĩa, cùng với dữ liệu kiểm tra (parity) được lưu trữ trên các ổ đĩa khác nhau. Nếu một ổ đĩa hỏng, dữ liệu có thể được khôi phục từ thông tin parity. RAID 5 chỉ hoạt động với cụm từ 3 ổ đĩa vật lý trở lên.



Hình 4-3 RAID 5

RAID 10: Kết hợp cả hai cấu trúc RAID 0 và RAID 1. Dữ liệu được phân chia và lưu trữ đồng thời trên nhiều ổ đĩa và cũng được sao chép đồng thời trên các ổ đĩa khác nhau.



Hình 4-4 RAID 10

Mỗi loại cấu hình RAID sẽ mang lại những lợi ích khác nhau về hiệu suất hoạt động, độ tin cậy, an toàn dữ liệu. Tuy nhiên đi kèm với nó cũng là những yêu cầu khác nhau về quy mô triển khai, loại ổ cứng, độ phức tạp khi triển khai. Chính vì vậy người quản trị cần có đánh giá tổng thể về yêu cầu lưu trữ dữ liệu trên hệ thống của mình để lựa chọn được kiểu cấu hình phù hợp.

4.1.4 Các mô hình triển khai hệ thống lưu trữ

A, DAS – Direct-Attached Storage

DAS là hệ thống lưu trữ mà các thiết bị lưu trữ (ổ đĩa cứng, băng, hoặc các thiết bị lưu trữ khác) được kết nối trực tiếp với một máy tính hoặc máy chủ cụ thể.

Kết nối được thực hiện thông qua giao diện như USB, SATA, SCSI hoặc Thunderbolt.

DAS thường dùng cho việc lưu trữ cá nhân, hoặc để mở rộng dung lượng lưu trữ cho máy tính cá nhân hoặc máy chủ cụ thể.

Ưu điểm:

Thiết lập dễ dàng: Các giải pháp DAS bên trong và bên ngoài đều dễ dàng thiết lập, cấu hình và truy cập. Bộ nhớ gắn trực tiếp bên trong được cài đặt sẵn trong máy tính hoặc máy chủ mới và có thể được sử dụng ngay lập tức. Bộ nhớ ngoài plug-and-play có thể được sử dụng ngay sau khi nó được gắn vào bằng cổng USB.

Chi phí thấp: Không giống như NAS và SAN, DAS không yêu cầu phần cứng hoặc phần mềm để chạy và quản lý hệ thống lưu trữ, làm cho nó trở thành một lựa chọn rất hợp lý khi so sánh với NAS và SAN yêu cầu phần cứng và phần mềm để chạy và

quản lý hệ thống lưu trữ. Để thiết lập một hệ thống DAS, chi phí duy nhất của bạn là những chi phí liên quan đến ổ đĩa và bất kỳ vỏ ổ đĩa nào bạn cần.

Hiệu suất cao: Do bộ lưu trữ được kết nối trực tiếp với máy chủ DAS nên DAS có thể cung cấp khả năng truy cập dữ liệu nhanh chóng và hỗ trợ các hoạt động I / O hiệu suất cao. Và, bởi vì nó không được kết nối với mạng, hệ thống DAS không bị ảnh hưởng bởi các vấn đề băng thông hoặc độ trễ mạng.

Nhược điểm:

Khả năng truy cập hạn chế: Bộ nhớ gắn trực tiếp chỉ có thể truy cập được đối với các ứng dụng chạy trên máy tính hoặc máy chủ mà DAS được kết nối. Vì nó không sử dụng phần cứng mạng để chia sẻ tài nguyên lưu trữ nên nhóm người dùng khác trên mạng không thể truy cập bộ nhớ, điều này có thể ảnh hưởng đến năng suất và sự cộng tác.

Khả năng mở rộng hạn chế: DAS có thể khó mở rộng quy mô vì các tùy chọn bị giới hạn ở số lượng ổ đĩa bên trong, dung lượng của các thiết bị DAS bên ngoài và tính khả dụng của các cổng bên ngoài trên các thiết bị riêng lẻ.

Không có quản lý trung tâm và sao lưu: DAS không cung cấp cơ chế quản lý trung tâm và sao lưu. Điều này ít có vấn đề hơn khi chỉ có một số máy tính sử dụng DAS, nhưng việc đảm bảo khả năng lưu trữ và bảo vệ DAS có thể trở nên tốn kém và phức tạp hơn khi mạng doanh nghiệp phát triển.

B, NAS – Network Attached Storage

NAS là một hệ thống lưu trữ dữ liệu có kết nối mạng, có thể truy cập qua mạng LAN (Local Area Network) hoặc Internet.

Thiết bị NAS thường chạy trên phần mềm và phần cứng đặc biệt được thiết kế để cung cấp dịch vụ lưu trữ dữ liệu cho nhiều thiết bị trong mạng.

NAS thường được sử dụng để chia sẻ dữ liệu, sao lưu dữ liệu, phục vụ media và các nhu cầu lưu trữ gia đình hoặc doanh nghiệp nhỏ.

Ưu điểm:

Khả năng mở rộng: NAS cho phép các tổ chức mở rộng dung lượng lưu trữ mà không cần thay thế hoặc nâng cấp các máy chủ hiện có hoặc tắt mạng. Có thể dễ dàng tăng dung lượng lưu trữ bằng cách thêm thiết bị NAS khác, ổ cứng khác hoặc ổ cứng có dung lượng lớn hơn.

Khả năng truy cập lớn hơn: NAS tạo ra một hệ thống lưu trữ tập trung giúp các thiết bị nối mạng truy cập dữ liệu dễ dàng hơn. Người dùng có thể cộng tác và chia sẻ tệp từ nhiều vị trí cho dù họ đang sử dụng PC hay Mac hoặc sử dụng các hệ điều hành khác nhau như Windows, Unix hoặc Mac OS.

Hiệu suất: Mặc dù mức hiệu suất của thiết bị lưu trữ NAS không cao bằng hệ thống SAN, nhưng các hệ thống này vẫn mang lại một số lợi ích về hiệu suất. Vì NAS loại bỏ trách nhiệm cung cấp tệp khỏi các thiết bị được nối mạng khác và được kết nối với mạng LAN, nên nó có thể lưu trữ và phân phát tệp nhanh hơn, góp phần tăng hiệu suất.

Nhược điểm:

Tăng lưu lượng mạng LAN: Sử dụng NAS nhiều có thể làm tăng lưu lượng mạng và gây tắc nghẽn trên mạng LAN, ảnh hưởng đến những người dùng khác. Điều này làm cho NAS không phù hợp với các ứng dụng thực hiện các hoạt động truyền dữ liệu chuyên sâu.

Hạn chế về hiệu suất: NAS bị giới hạn bởi băng thông của mạng doanh nghiệp và các giao thức SMB và NFS (Hệ thống tệp mạng) của nó không đủ nhanh để hỗ trợ các ứng dụng hiệu suất cao. Khi nhiều khách hàng tham gia vào mạng và truy cập vào hệ thống tệp NAS, hiệu suất có thể giảm xuống mức không phù hợp. Điều này làm cho NAS phù hợp hơn với các mạng nhỏ hơn.

Bảo mật và độ tin cậy: NAS không thể được định cấu hình để có tính sẵn sàng cao, làm tăng khả năng nó có thể trở thành một điểm lỗi duy nhất khi mạng phát triển. Vì NAS chỉ cung cấp sao lưu dữ liệu tại chỗ, cả dữ liệu doanh nghiệp và NAS đều có thể bị mất nếu xảy ra sự kiện tự nhiên, tấn công mạng hoặc do lỗi của con người.

C, SAN – Storage Area Network

SAN là một hệ thống lưu trữ độc lập, được kết nối với mạng LAN hoặc WAN (Wide Area Network).

Nó sử dụng giao thức truyền tải dữ liệu như Fibre Channel hoặc iSCSI để kết nối các thiết bị lưu trữ với các máy chủ.

SAN thường được sử dụng trong môi trường doanh nghiệp, data center hoặc các ứng dụng đòi hỏi hiệu suất cao, tính sẵn sàng và khả năng mở rộng.

SAN hoạt động với hai thiết bị chuyên dụng:

SAN Switch – được cấu tạo bởi nhiều giao tiếp fibre cung cấp cơ chế chuyển tiếp dữ liệu từ các hệ thống máy chủ xuống hệ thống lưu trữ.

Hình 4-5 Thiết bị SAN Switch

SAN Storage: có cấu tạo như một máy chủ vật lý, nhưng bổ sung thêm rất nhiều khe cắm ổ cứng để có thể tăng tối đa năng lực lưu trữ dữ liệu.

Hình 4-6 Thiết bị SAN Storage

Ưu điểm của SAN:

Cải thiện hiệu suất: SAN cung cấp hiệu suất cao hơn so với DAS và NAS vì quá trình xử lý lưu trữ được thực hiện trên một mạng tách biệt với mạng cục bộ (LAN). Di chuyển các tác vụ lưu trữ sang một SAN chuyên dụng đảm bảo rằng hiệu suất trên SAN không bị ảnh hưởng bởi tắc nghẽn lưu lượng trên mạng LAN. Nó cũng loại bỏ lưu lượng lưu trữ khỏi mạng LAN để giải phóng băng thông và cải thiện hiệu suất.

Khả năng mở rộng lớn hơn: SAN có thể bao gồm hàng nghìn thiết bị lưu trữ SAN và máy chủ lưu trữ có thể được mở rộng để đáp ứng nhu cầu kinh doanh đang phát triển.

Các tổ chức có thể thêm máy chủ và thiết bị lưu trữ mới để xây dựng SAN khi nhu cầu dung lượng tăng lên.

Cải thiện tính khả dụng: Lưu trữ SAN có thể truy cập thông qua nhiều đường dẫn và vẫn độc lập với các ứng dụng mà nó hỗ trợ. Kết cấu mạng SAN có thể sử dụng các đường dẫn thay thế để duy trì tính khả dụng của bộ nhớ nếu xảy ra lỗi giao tiếp, đảm bảo rằng không có điểm lỗi nào giữa máy chủ và thiết bị lưu trữ.

Nhược điểm:

Chi phí: Chi phí thiết lập và duy trì cơ sở hạ tầng cáp quang để hỗ trợ SAN có thể rất đáng kể. Bộ nhớ dự phòng hiệu suất cao tốn kém và có thể mất một thời gian trước khi bạn thấy lợi tức đầu tư. SAN cũng yêu cầu bảo trì và quản lý liên tục, phát sinh thêm chi phí. Điều này làm cho SAN phù hợp hơn với các tổ chức lớn hơn có thể đủ khả năng đầu tư chi phí vốn ban đầu.

Phức tạp hơn để thiết lập và duy trì: Sự phức tạp của SAN có thể yêu cầu chuyên môn cụ thể để quản lý và duy trì. Do đó, sẽ cần duy trì chuyên viên quản trị được đào tạo để hỗ trợ SAN hoặc thuê hỗ trợ bên ngoài cho nhà cung cấp bên thứ ba.

4.2 Cơ chế phân quyền và bảo mật tập tin

4.2.1 Hệ thống tập tin trên Windows Server

Hệ thống tập tin quản lý việc lưu trữ và định vị các tập tin trên đĩa cứng. Các hệ thống Windows trước đây hỗ trợ hai hệ thống tập tin là FAT và NTFS. Tuy nhiên, với sự phát triển của các hệ thống công nghệ thông tin, hệ thống tập tin FAT tỏ ra không còn phù hợp với việc quản lý và định vị tập tin. Do vậy, từ phiên bản Windows Server 2012, Microsoft đã giới thiệu hệ thống tập tin mới có tên gọi ReFS và duy trì nó cùng với NTFS là hai hệ thống tập tin chính trong hệ điều hành.

NTFS (New Technology File System):

NTFS là hệ thống tập tin tiêu chuẩn và mặc định cho hệ điều hành Windows Server 2012.

Nó cung cấp nhiều tính năng như phân quyền truy cập, mã hóa dữ liệu, nén tập tin, kiểm tra và sửa chữa lỗi, và hỗ trợ dung lượng lưu trữ lớn.

NTFS cũng hỗ trợ Shadow Copies (bản sao bóng đèn) để sao lưu dữ liệu và khôi phục phiên bản trước đó của tập tin.

ReFS (Resilient File System):

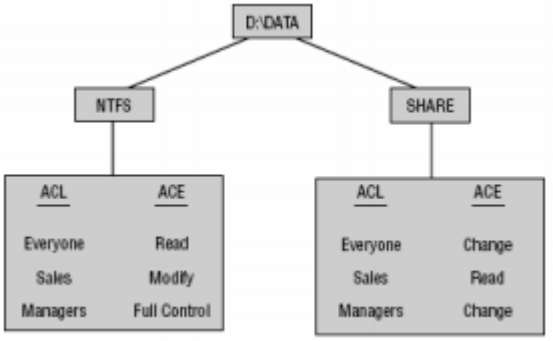
ReFS là một hệ thống tập tin mới ra mắt trong Windows Server 2012 (cũng như Windows 8).

Nó được thiết kế để cung cấp tính năng độ bền cao hơn và khả năng chịu lỗi tốt hơn so với NTFS.

ReFS hỗ trợ tính năng như bảo vệ dữ liệu, kiểm tra và sửa chữa tự động, tính năng phân quyền tập tin (File Permission), và khả năng mở rộng dung lượng lưu trữ lớn.

4.2.2 Quyền truy cập NTFS

Hệ thống **Windows Server** dùng các **ACL** (**Access Control List**) để quản lý các quyền truy cập của đối tượng cục bộ và các đối tượng trên **Active Directory**. Một **ACL** có thể chứa nhiều **ACE** (**Access Control Entry**) đại diện cho một người dùng hay một nhóm người.



Hình 4-7 Cấu trúc ACL trong Windows

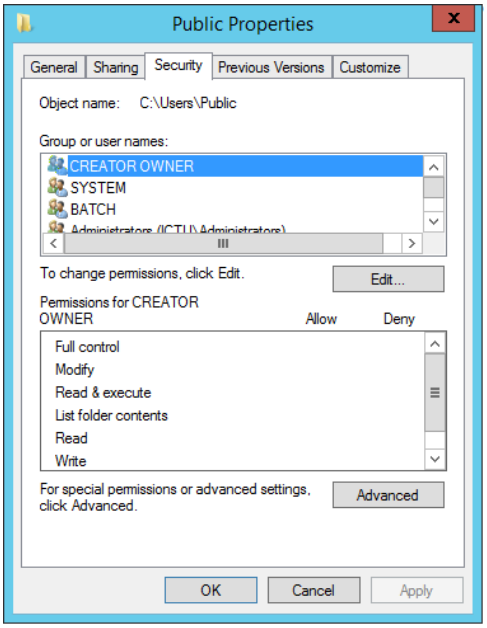
A, Các quyền truy cập NTFS

Tên quyền	Chức năng
Traverse Folder/Execute File	Duyệt các thư mục và thi hành các tập tin chương trình trong thư mục
List Folder/Read Data	Liệt kê nội dung của thư mục và đọc dữ liệu của các tập tin trong thư mục
Read Attributes	Đọc các thuộc tính của các tập tin và thư mục
Read Extended Attributes	Đọc các thuộc tính mở rộng của các tập tin và thư mục
Create File/Write Data	Tạo các tập tin mới và ghi dữ liệu lên các tập tin này
Create Folder/Append Data	Tạo thư mục mới và chèn thêm dữ liệu vào các tập tin
Write Attributes	Thay đổi thuộc tính của các tập tin và thư mục
Write Extendd Attributes	Thay đổi thuộc tính mở rộng của các tập tin và thư mục
Delete Subfolders and Files	Xóa thư mục con và các tập tin
Delete	Xóa các tập tin
Read Permissions	Đọc các quyền trên các tập tin và thư mục
Change Permissions	Thay đổi quyền trên các tập tin và thư mục
Take Ownership	Tước quyền sở hữu của các tập tin và thư mục

B, Gán quyền truy cập trên thư mục

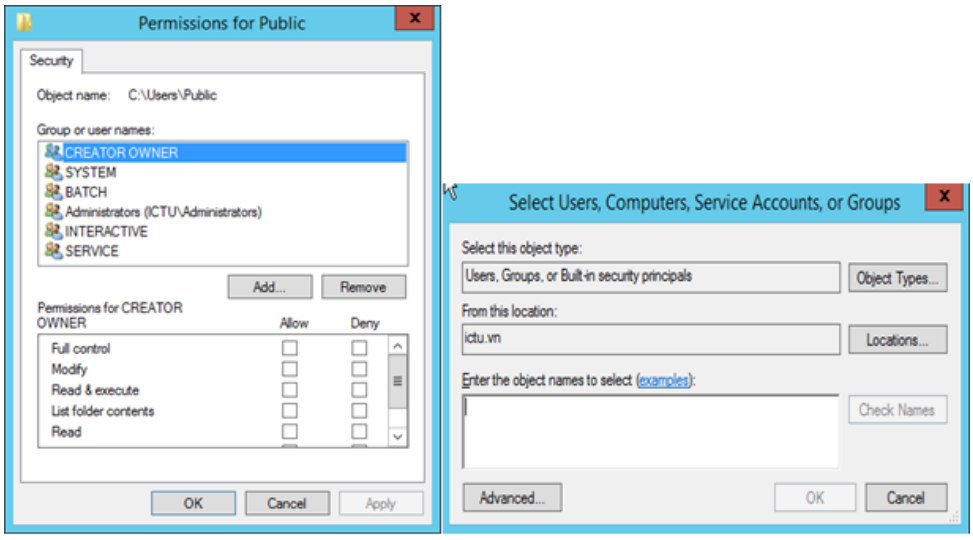
Chúng ta muốn gán quyền **NTFS**, thông qua **Windows Explorer** chúng ta nhấp phải chuột vào tập tin hay thư mục cần cấu hình quyền truy cập rồi chọn **Properties**.

Hộp thoại **Properties** xuất hiện. Nếu ổ đĩa của chúng ta định dạng là **FAT** thì hộp thoại chỉ có hai **Tab** là **General** và **Sharing**. Nhưng nếu đĩa có định dạng là **NTFS** thì trong hộp thoại sẽ có thêm một **Tab** là **Security**. **Tab** này cho phép ta có thể quy định quyền truy cập cho từng người dùng hoặc một nhóm người dùng lên các tập tin và thư mục. Chúng ta nhấp chuột vào **Tab Security** để cấp quyền cho các người dùng.



Hình 4-8 Quyền truy cập NTFS

Muốn cấp quyền truy cập cho một người dùng, chúng ta nhấp chuột vào nút **Add**, hộp thoại chọn lựa người dùng và nhóm xuất hiện, chúng ta chọn người dùng và nhóm cần cấp quyền, nhấp chuột vào nút **Add** để thêm vào danh sách, sau đó nhấp chuột vào nút **OK** để trở lại hộp thoại chính.

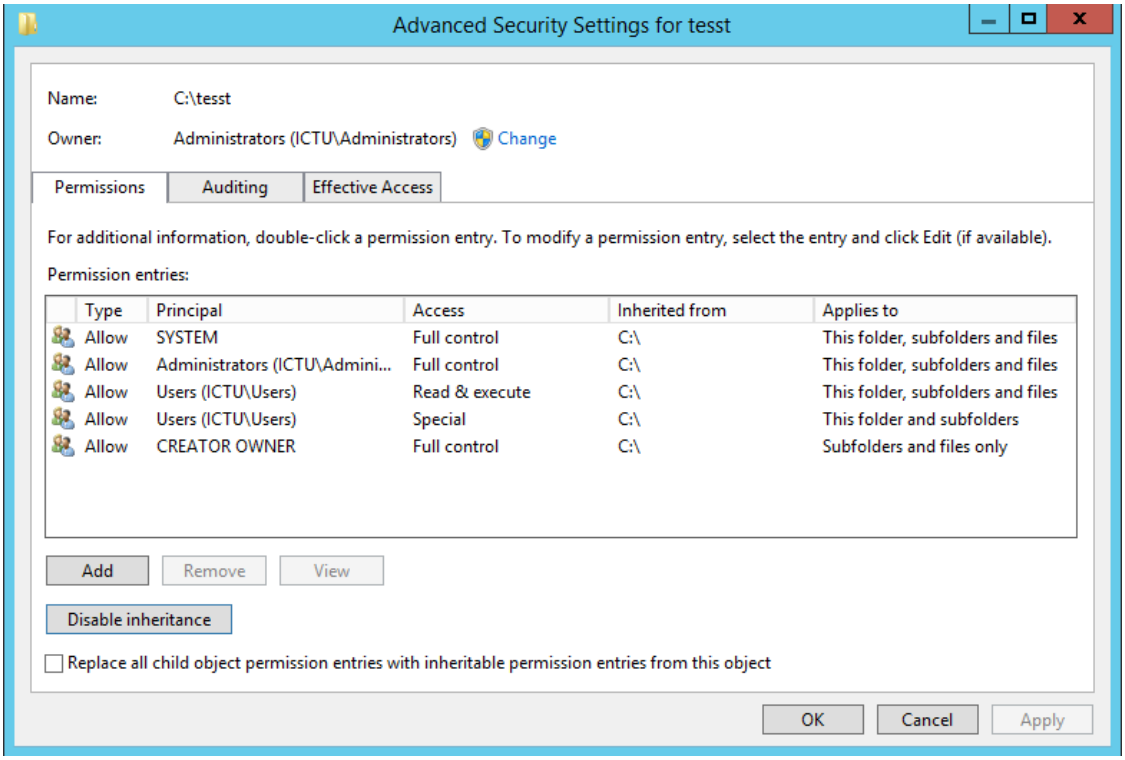


Hình 4-9 Cấu hình quyền truy cập NTFS

Hộp thoại chính sẽ xuất hiện các người dùng và nhóm mà chúng ta mới thêm vào, sau đó chọn người dùng và nhóm để cấp quyền. Trong hộp thoại đã hiện sẵn danh sách quyền, chúng ta muốn cho người dùng đó có quyền gì thì chúng ta đánh dấu vào phần **Allow**, còn ngược lại muốn cấm quyền đó thì đánh dấu vào mục **Deny**.

C, Kế thừa và thay thế quyền của các đối tượng con

Trong hộp thoại chính trên, chúng ta có thể nhấp chuột vào nút **Advanced** để cấu hình chi tiết hơn cho các quyền truy cập của người dùng. Khi nhấp chuột vào nút **Advanced**, hộp thoại **Advanced Security Settings** xuất hiện, trong hộp thoại, nếu chúng ta ấn vào nút **Enable inheritance** thì thư mục hiện tại được thừa hưởng danh sách quyền truy cập từ thư mục cha, chúng ta muốn xóa những quyền thừa hưởng từ thư mục cha chúng ta phải ấn vào nút Disable inheritance ở cùng vị trí. Nếu danh sách quyền truy cập của thư mục cha thay đổi thì danh sách quyền truy cập của thư mục hiện tại cũng thay đổi theo. Ngoài ra nếu chúng ta đánh dấu vào mục **Replace permission entries on all child objects with entries shown here that apply to child objects** thì danh sách quyền truy cập của thư mục hiện tại sẽ được áp dụng xuống các tập tin và thư mục con có nghĩa là các tập tin và thư mục con sẽ được thay thế quyền truy cấp giống như các quyền đang hiển thị trong hộp thoại.



Hình 4-10 Cấu hình kế thừa quyền truy cập NTFS

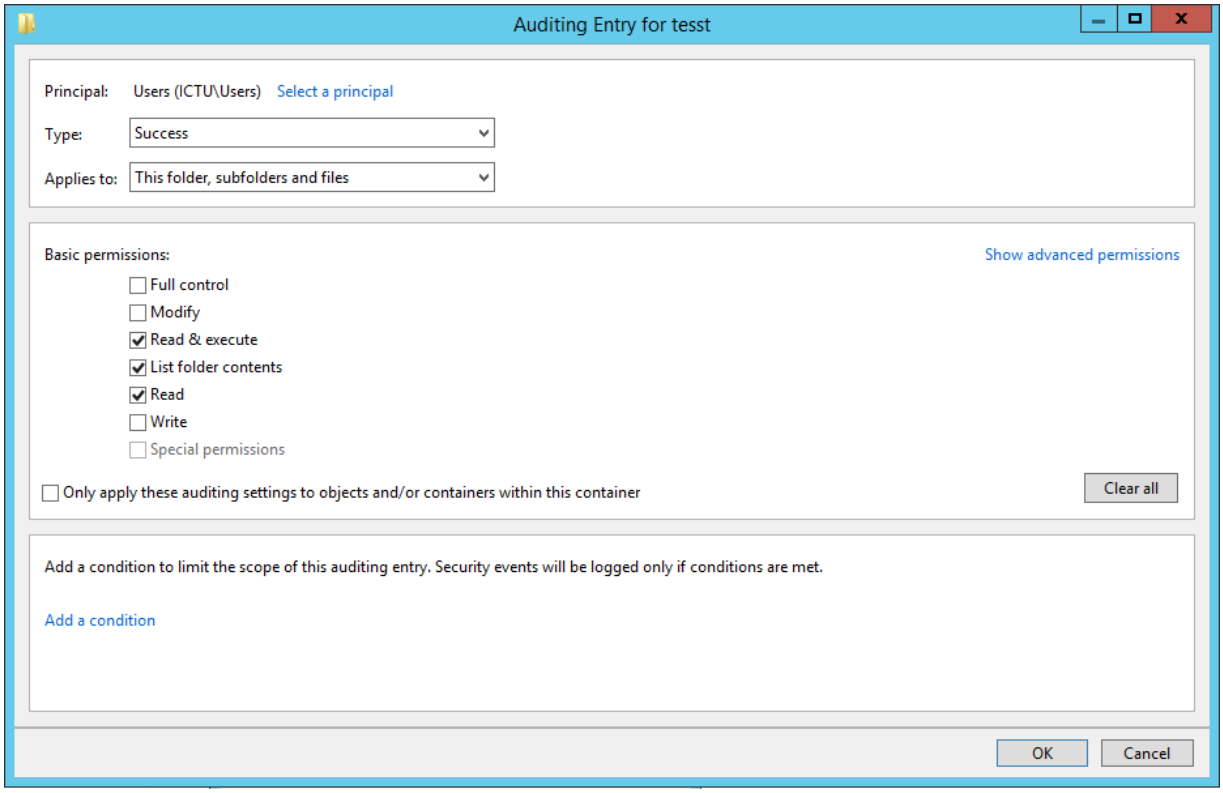
D, Di chuyển và sao chép tập tin và thư mục

Khi chúng ta sao chép (**copy**) một tập tin hay thư mục sang một vị trí mới thì quyền truy cập trên tập tin hay thư mục này sẽ thay đổi theo quyền trên thư mục cha

chứa chúng, nhưng ngược lại nếu chúng ta di chuyển (**move**) một tập tin hay thư mục sang bất kì vị trí nào thì các quyền trên chúng vẫn được giữ nguyên.

E, Kiểm soát truy cập thư mục

Chúng ta muốn kiểm soát và ghi nhận lại các người dùng thao tác trên thư mục hiện tại, trong hộp thoại **Advanced Security Settings**, chọn **Tab Auditing**, nhấp chuột vào nút **Add** để chọn người dùng cần giám sát, sau đó chúng ta muốn giám sát việc truy xuất thành công thì chọn **Successful** trong mục Type, ngược lại giám sát việc truy xuất không thành công thì đánh dấu vào mục **Fail**.

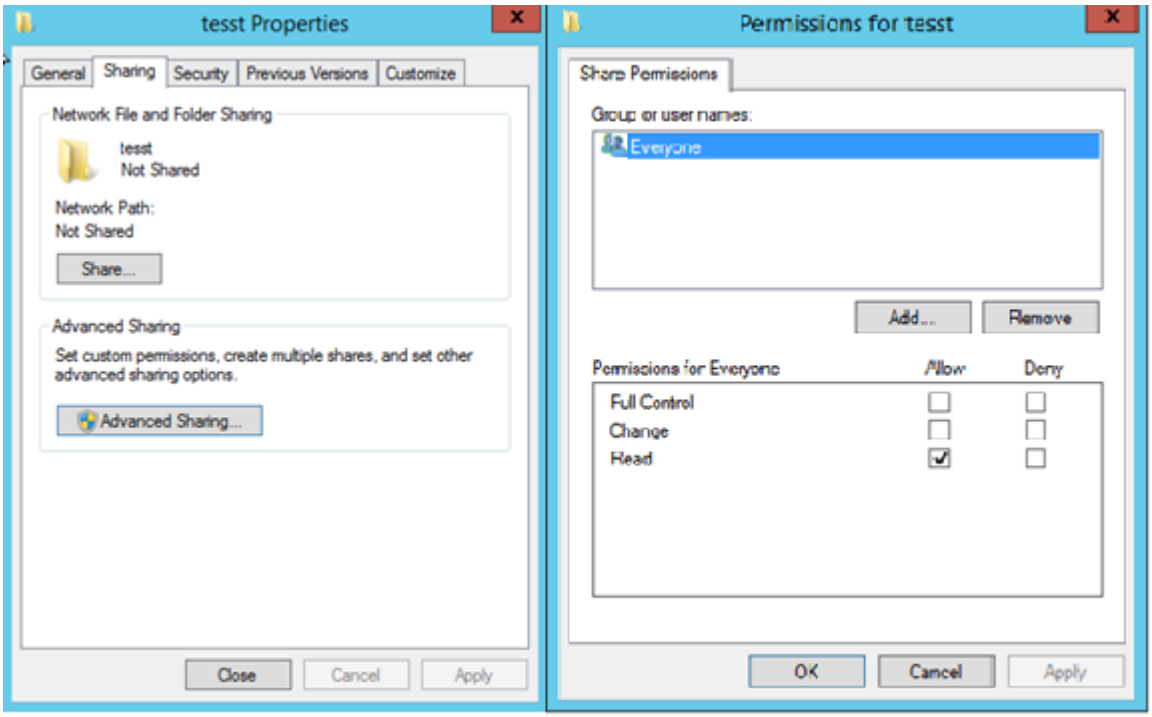


Hình 4-11 Cấu hình kiểm soát truy cập thư mục

4.3 Dịch vụ chia sẻ và quản lý tập tin

A, Chia sẻ thư mục dùng chung

Các tài nguyên chia sẻ là các tài nguyên trên mạng mà các người dùng có thể truy xuất và sử dụng thông qua mạng. Muốn chia sẻ một thư mục dùng chung trên mạng, chúng ta phải **logon** vào hệ thống với vai trò người quản trị (**Administrators**) hoặc là thành viên của nhóm **Server Operators**, tiếp theo trong **Explorer** chúng ta nhấp phải chuột trên thư mục đó và chọn **Properties**, hộp thoại **Properties** xuất hiện, chọn **Tab Sharing**.



Hình 4-12 Cấu hình chia sẻ thư mục

B, Cấu hình share permissions

Chúng ta muốn cấp quyền cho các người dùng truy cập qua mạng thì dùng **Share Permissions**. **Share Permissions** chỉ có hiệu lực khi người dùng truy cập qua mạng chứ không có hiệu lực khi người dùng truy cập cục bộ. Khác với **NTFS Permissions** là quản lý người dùng truy cập dưới cấp độ truy xuất đĩa. Trong hộp thoại **Share Permissions**, chứa danh sách các quyền sau:

Full Control: cho phép người dùng có toàn quyền trên thư mục chia sẻ.

Change: cho phép người dùng thay đổi dữ liệu trên tập tin và xóa tập tin trong thư mục chia sẻ.

Read: cho phép người dùng xem và thi hành các tập tin trong thư mục chia sẻ.

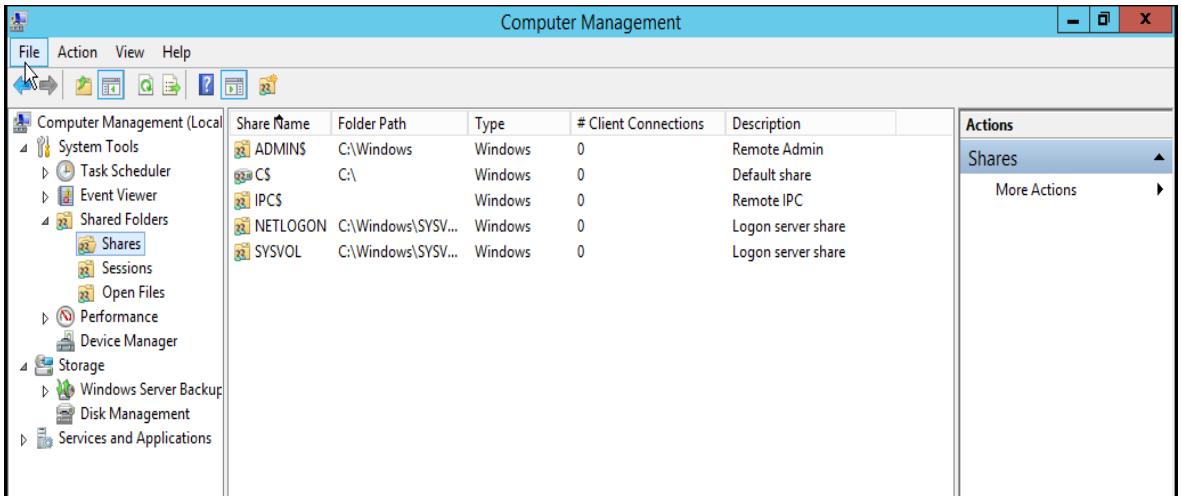
Chúng ta muốn cấp quyền cho người dùng thì nhấp chuột vào nút **Add**.

Hộp thoại chọn người dùng và nhóm xuất hiện, chúng ta nhấp đôi chuột vào các tài khoản người dùng và nhóm cần chọn, sau đó chọn **OK**. Trong hộp thoại xuất hiện, muốn cấp quyền cho người dùng chúng ta đánh dấu vào mục **Allow**, ngược lại khóa quyền thì đánh dấu vào mục **Deny**.

C, Quản lý các thư mục dùng chung.

Trong một hệ thống mạng AD có số lượng người dùng lớn, việc có quá nhiều thư mục chia sẻ sẽ ảnh hưởng đến hiệu năng hệ thống và các vấn đề bảo mật. Công cụ **Computer Management** cho phép chúng ta quản lý các thư mục đang được chia sẻ trên

hệ thống. Từ cửa sổ **Computer Management**, chúng ta truy cập vào menu **Shared Folders**.



Hình 4-13 Cấu hình quản lý thư mục chia sẻ

Ở menu Shares sẽ hiển thị danh sách các thư mục đang được chia sẻ trên hệ thống, đường dẫn, kiểu của thư mục, số Client đang kết nối đến thư mục đó và chú thích. Các thư mục có tên với dấu $ ở cuối là các thư mục chia sẻ bị ẩn.

Menu Sessions ở bên dưới có tác dụng hiển thị danh sách người dùng đang truy cập đến các thư mục dùng chung trong hệ thống. Các thông tin mà menu này cung cấp bao gồm:

- Tên tài khoản người dùng đang kết nối vào tài nguyên chia sẻ.
- Tên máy tính có người dùng kết nối từ đó.
- Hệ điều hành mà máy trạm đang sử dụng để kết nối.
- Số tập tin mà người dùng đang mở.
- Thời gian kết nối của người dùng.
- Thời gian chờ xử lý của kết nối.
- Phải là truy cập của người dùng **Guest** không?

Menu Open Files hiển thị danh sách các tập tin đang được mở trong các thư mục dùng chung. Nó cũng cho biết đường dẫn của tập tin đó, tên tài khoản người dùng đang truy cập tập tin đó, hệ điều hành mà người dùng sử dụng, trạng thái tập tin có đang bị khóa hay không và trạng thái mở sử dụng tập tin (Read hay Write).

CHƯƠNG 5 QUẢN TRỊ DỊCH VỤ MẠNG

5.1 Dịch vụ DNS

5.1.1 Tổng quan về hệ thống DNS

DNS (Domain Name System) là dịch vụ giúp phân giải tên miền thành địa chỉ IP và ngược lại. Điều này giúp cho người dùng có thể truy cập các trang web bằng tên thay vì phải dùng địa chỉ IP.

Khi một người dùng nhập một tên miền vào trình duyệt, giao thức DNS được kích hoạt. Trước tiên, trình duyệt sẽ gửi yêu cầu tới máy chủ DNS gần nhất. Máy chủ DNS này sau đó sẽ tìm kiếm trong cơ sở dữ liệu của nó hoặc liên hệ với các máy chủ DNS khác để tìm địa chỉ IP tương ứng với tên miền được yêu cầu. Khi tìm thấy, máy chủ DNS trả về địa chỉ IP cho trình duyệt, giúp trình duyệt thực hiện kết nối với máy chủ hoặc dịch vụ mạng tương ứng.

Dịch vụ DNS hoạt động theo mô hình Client-Server. Phần Server được gọi là máy chủ phục vụ tên hay còn gọi là Name Server , chứa CSDL về thông tin phân giải tên cho các tên miền.

Phần Client là trình phân giải (Resolver), chứa các hàm thư viện dùng để tạo truy vấn (query) gửi tới Name Server.

DNS giúp tăng tính khả dụng và linh hoạt của Internet, cho phép người dùng truy cập vào các trang web và dịch vụ bằng cách sử dụng tên miền dễ nhớ thay vì phải ghi nhớ các địa chỉ IP phức tạp. Nó cũng hỗ trợ các chức năng như cân bằng tải hoặc sử dụng bộ nhớ đệm để tăng tốc độ truy vấn. Chính vì vậy, nó là một hệ thống định danh quan trọng trong cơ sở hạ tầng Internet đóng vai trò kết nối người dùng với các dịch vụ và tài nguyên trên mạng.

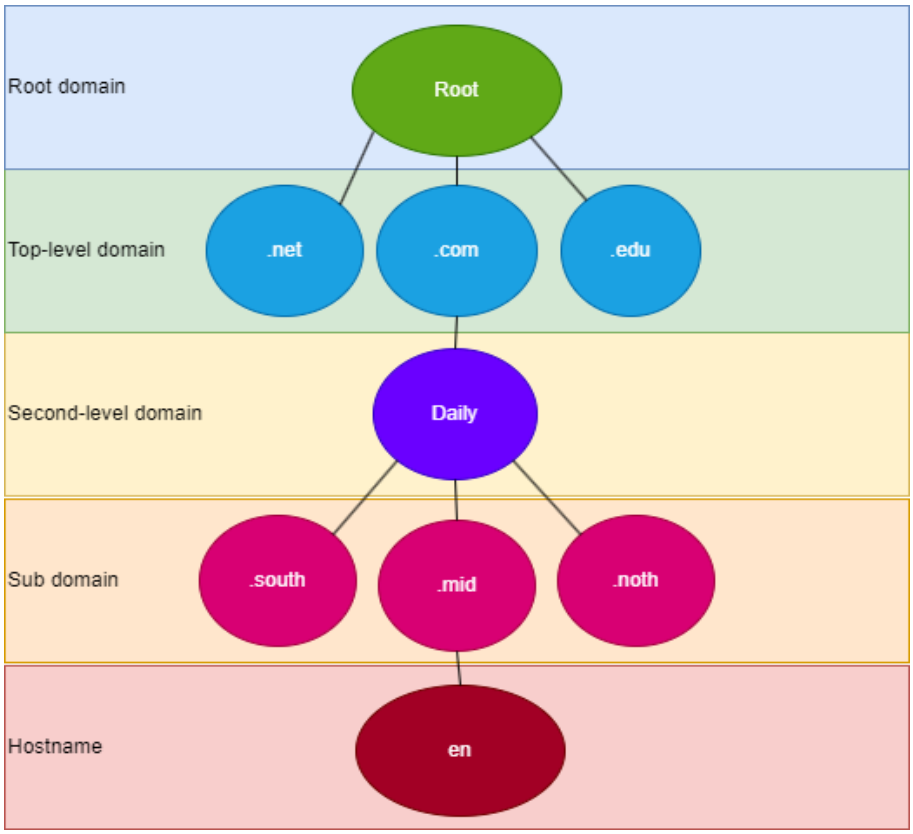
5.1.2 Cấu trúc hệ thống DNS

Do vai trò định dạng trong cơ sở hạ tầng DNS, người ta đã thiết kế một kiến trúc giúp cho toàn bộ các máy chủ DNS trên Internet được liên kết với nhau thành một cơ sở dữ liệu tên miền trên toàn cầu.

Cơ sở dữ liệu của DNS là một cây đảo ngược. Mỗi nút trên cây là một miền (Domain). Mỗi Domain có thể phân chia thành các vùng nhỏ hơn được gọi là miền con (Sub Domain).

Mỗi Domain có một tên riêng gọi là Domain Name. Domain Name này chỉ cho ta biết được vị trí của nó trong cơ sở dữ liệu DNS. Một tên DNS name mà chúng ta

thường gọi là tên miền là một chuỗi đi ngược từ dưới lên gốc của cây Domain và được ngăn cách nhau bằng dấu ".". Hình 5.2 là một ví dụ về một cây Domain Name



Hình 5-1 Ví dụ về cơ sở dữ liệu DNS

Trong ví dụ về cơ sở dữ liệu về DNS này thì ta có các Top-level Domain là .net, .com, .edu; Second-level Domain là Daily; có các Subdomain là: south, mid, north; có một host là en. Nên host sẽ có Domain Name là en.mid.Daily.com.

Đối với cơ sở dữ liệu DNS, root domain đóng vai trò rất quan trọng. Root domain là gốc của hệ thống DNS, root domain không có tên chính thức và nhãn của nó trong hệ thống DNS là một chuỗi trống. Tất cả các domain trên hệ thống DNS đều kết thúc bằng chuỗi trống này, và do đó phần kết thúc của các domain đều dừng ở dấu phân cách nhãn ".". Ví dụ: "www.example.com.". Chính vì sự đồng nhất này nên các trình phân giải tên miền ngày nay không yêu cầu phải đưa dấu chấm cuối cùng vào khi thực hiện truy vấn.

Khi các máy tính trên Internet cần thực hiện truy vấn một tên miền, nó sẽ sử dụng các dịch vụ có tên gọi là Resolver để thực hiện phân giải tên miền. Resolver sẽ chia tên miền thành các phần theo dấu "." phân cách nhãn từ phải qua trái. Các top-level domain sẽ được phân giải bởi Root domain. Chính vì vậy có thể nói Root domain là "trái tim" của toàn bộ hệ thống DNS. Mặc dù các tổ chức có thể triển khai hệ thống DNS nội bộ với root domain riêng, tuy nhiên thuật ngữ "root name server" thường được dùng để chỉ 13 cụm máy chủ đóng vai trò là Root domain cho hệ thống tên miền chính thức trên toàn

cầu. Các cụm máy chủ này có quy định chung về tên miền có dạng như sau: <kí tự>.root-servers.net, trong đó kí tự là một chữ cái latinh theo thứ tự từ a đến m. Mỗi cụm máy chủ này sẽ có một dải địa chỉ IP public riêng và được vận hành bởi một tổ chức riêng bao gồm các công ty cung cấp dịch vụ Internet, các tổ chức chính phủ, các tổ chức quốc tế và được đặt ở khắp các thành phố trên thế giới. Điều này để đảm bảo sự hoạt động thông suốt của hệ thống tên miền trên Internet.

Thành phần tiếp theo trong Domain Tree là các tên miền cấp cao, hay còn gọi là top-level domain (TLD). Các tên miền cấp cao được xếp ngay sau root domain. Do quy định của root domain nên ta có thể coi tên miền cấp cao là phần cuối cùng trong một tên miền. Ví dụ đối với tên miền "www.example.com" thì phần .com chính là tên miền cấp cao. Trách nhiệm quản lý các tên miền cấp cao được thực hiện bởi ICANN một tổ chức phi lợi nhuận được thành lập tại Hoa Kỳ vào năm 1998 nhằm thực hiện quản lý việc cấp phát tên miền trên Internet. Bảng 5.2 liệt kê các Top-level Domain thông dụng được phân chia theo các lĩnh vực.

Tên miền	Mô tả
.com	Các tổ chức thương mại
.org	Các tổ chức phi lợi nhuận
.net	Các tổ chức hỗ trợ về mạng
.edu	Các tổ chức giáo dục
.gov	Các tổ chức thuộc chính phủ
.mil	Các tổ chức quân sự

Bảng 5-1 Các Top-level Domain thông dụng

Ngoài các tên miền cấp cao được phân nhóm theo các lĩnh vực khác nhau, còn có các tên miền cấp cao của các quốc gia. Bảng 5.3 bên dưới liệt kê một số Top-level Domain của các quốc gia.

Tên miền	Quốc gia
.vn	Việt Nam
.us	Mỹ
.uk	Anh

.jp	Nhật
.ru	Nga
.cn	Trung Quốc

Bảng 5-2 Top-level của các quốc gia

Các thành phần bên dưới tên miền cấp cao được gọi là các tên miền cấp 2 hay second-level domain, nó nằm ngay trước tên miền cấp cao trong một domain đầy đủ. Tên miền cấp 2 thường được sử dụng để bổ trợ cho tên miền cấp cao trong một không gian tên. Ví dụ tên miền: "www.ictu.edu.vn" thì ".edu" chính là miền cấp 2 nằm trong không gian miền ".vn" nhằm giúp bổ sung thông tin cho TLD.

Ngoài ra trong cấu trúc Domain Tree còn có tên miền phụ hay sub domain. Nó là một phân vùng bổ sung nằm dưới tên miền cấp 2. Tên miền phụ được sử dụng để chia nhỏ và tổ chức tên miền chính thành các tên miền con. Ví dụ trong domain: "mail.example.com" thì "mail" là phần tên miền phụ của domain "example.com".

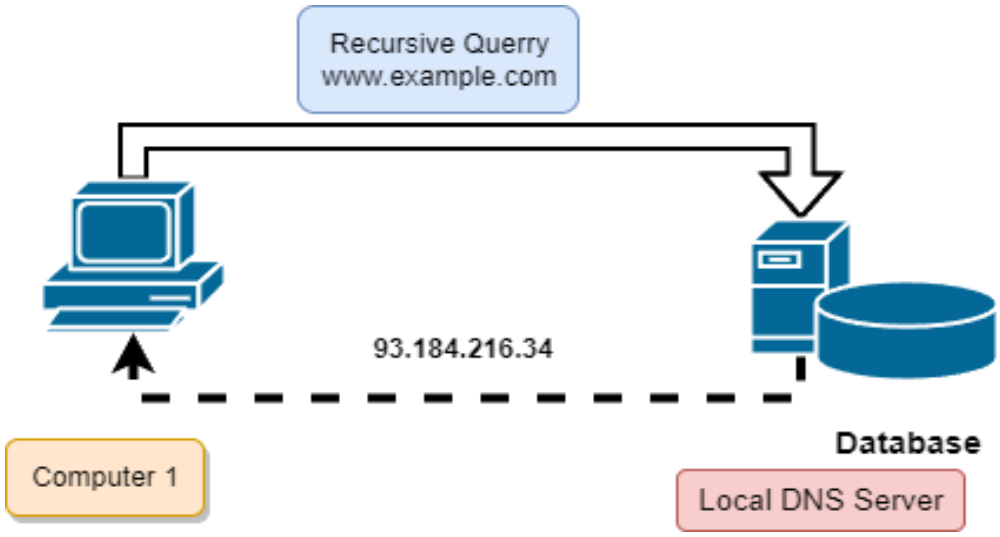
Phần cuối cùng của một tên miền là hostname, nó là chuỗi định danh duy nhất được gán cho một máy tính, máy chủ hoặc thiết bị trong mạng. Hostname có thể được đặt tên theo một số quy tắc nhất định được quy định bởi người quản trị mạng, hoặc đại diện cho loại dịch vụ mà máy chủ đó đang cung cấp.

Kết hợp tất cả các thành phần trong một domain tree ta sẽ có được một tên miền hoàn chỉnh FQDN (Fully Qualified Domain Name). Một FQDN bao gồm hai phần, phần DNS Suffix và phần hostname. Ví dụ trong domain: "www.example.com" thì "www" là hostname, "example.com" là DNS Suffix của domain đó. DNS Suffix của mỗi domain thuộc domain namespace của domain đó. Mỗi domain namespace có thể được sở hữu bởi một tổ chức, công ty hoặc quốc gia khác nhau. Ví dụ: quốc gia Việt Nam sở hữu domain namespace ".vn". Tổ chức ICTU đặt tại Việt Nam có thể đăng kí domain namespace "edu.vn" để sở hữu tên miền: "ictu.edu.vn".

5.1.3 Quá trình truy vấn DNS

Truy vấn (Query) là gửi câu yêu cầu phân giải tên miền đến máy DNS Server. Có 2 loại truy vấn là: Truy vấn đệ quy (Recursive) và truy vấn tương tác (Interactive)

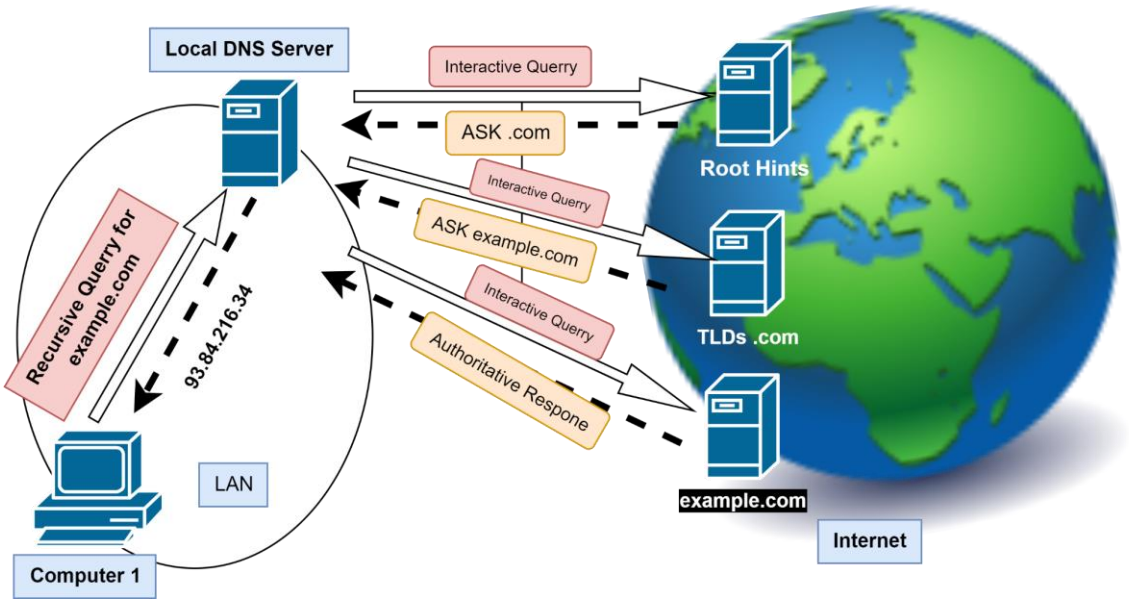
Truy vấn đệ quy là kiểu truy vấn mà Client yêu cầu Server cung cấp câu trả lời đầy đủ cho câu truy vấn phân giải một tên miền nào đó. Hình 5.4 mô tả quá trình truy vấn đệ quy.



Hình 5-2 Truy vấn đệ quy (Recursive)

Như hình 5.2, máy Computer1 gửi câu truy vấn phân giải tên miền www.example.com thành địa chỉ IP đến máy Local DNS Server. Máy Local DNS Server này sẽ tìm trong cơ sở dữ liệu của nó và nếu có kết quả tương ứng thì nó sẽ gửi về địa chỉ IP tương ứng với tên miền cho máy Computer1 (trong ví dụ này là 172.16.64.1).

Truy vấn tương tác là kiểu truy vấn mà Client sẽ nhận được các câu trả lời tốt nhất mà DNS Server cung cấp tại thời điểm đó. Trong trường hợp DNS Server không tìm thấy kết quả, nó sẽ trả lời với tên miền và địa chỉ IP của DNS Server gần nhất mà nó biết. Hình 5.5 mô tả quá trình truy vấn tương tác

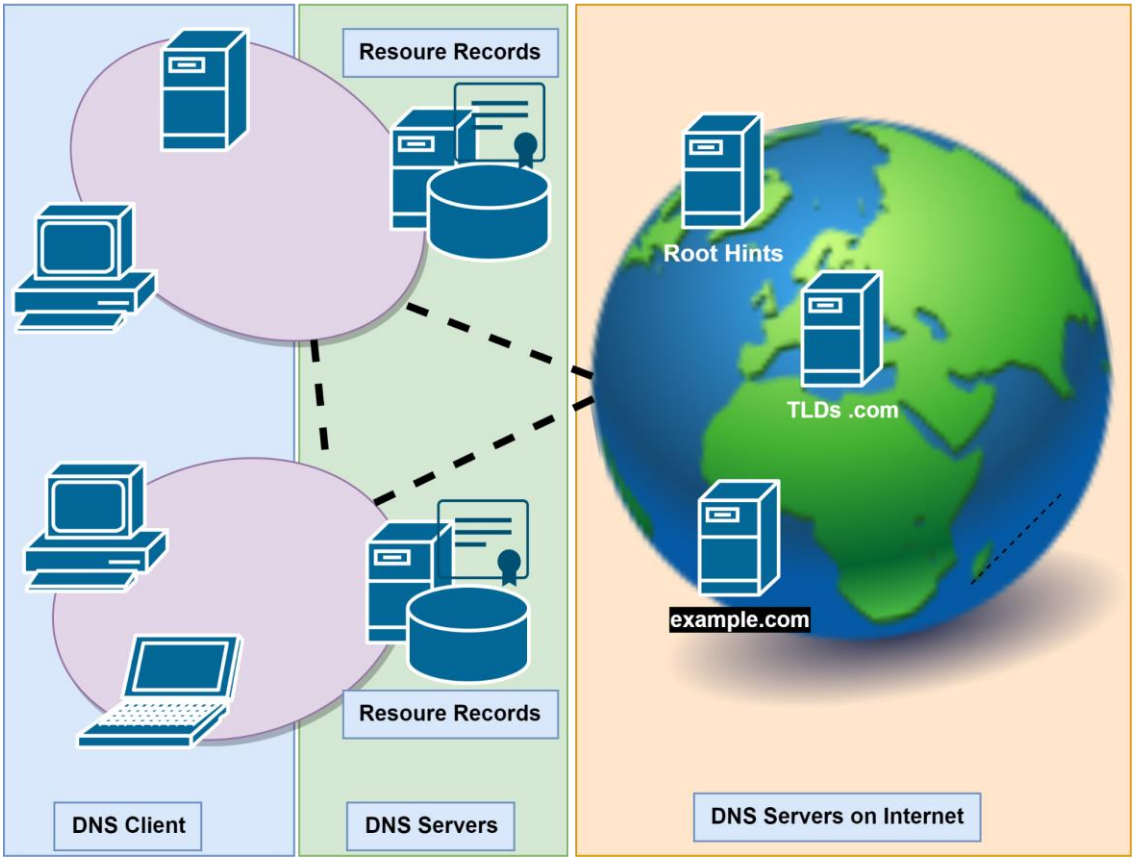


Hình 5-3 Truy vấn tương tác

Theo hình 5.3, máy Computer1 gửi yêu cầu truy vấn phân giải tên miền mail1.matraders.com thành địa chỉ IP đến Local DNS Server. Máy Local DNS Server

tìm trong cơ sở dữ liệu của mình xem có câu trả lời để gửi về cho DNS client không? Nếu có thì nó gửi trả về, còn nếu không có thì nó chuyển tiếp câu truy vấn ra ngoài Internet đến máy Root Hint Server, là máy quản lý dấu ".". Máy Root Hint Server cung cấp tên và địa chỉ IP của máy Server quản lý tên miền ".com" cho máy Local DNS Server và máy Local này sẽ gửi câu truy vấn đến máy quản lý tên miền ".com"; rồi câu truy vấn tiếp tục được chuyển đến máy Server quản lý tên miền là "example.com"; máy Server này lưu trữ thông tin về địa chỉ IP tương ứng với tên miền là www.example.com; nó trả về địa chỉ IP tương ứng với tên miền cho máy Local DNS Server và máy Local này gửi câu trả lời về cho máy Computer 1.

Tiếp theo, chúng ta cùng tìm hiểu về quá trình phân giải tên miền thành địa chỉ IP thông qua sơ đồ như hình 5.4



Hình 5-4 Các thành phần tham gia phân giải tên miền

Quá trình phân giải tên miền như sau:

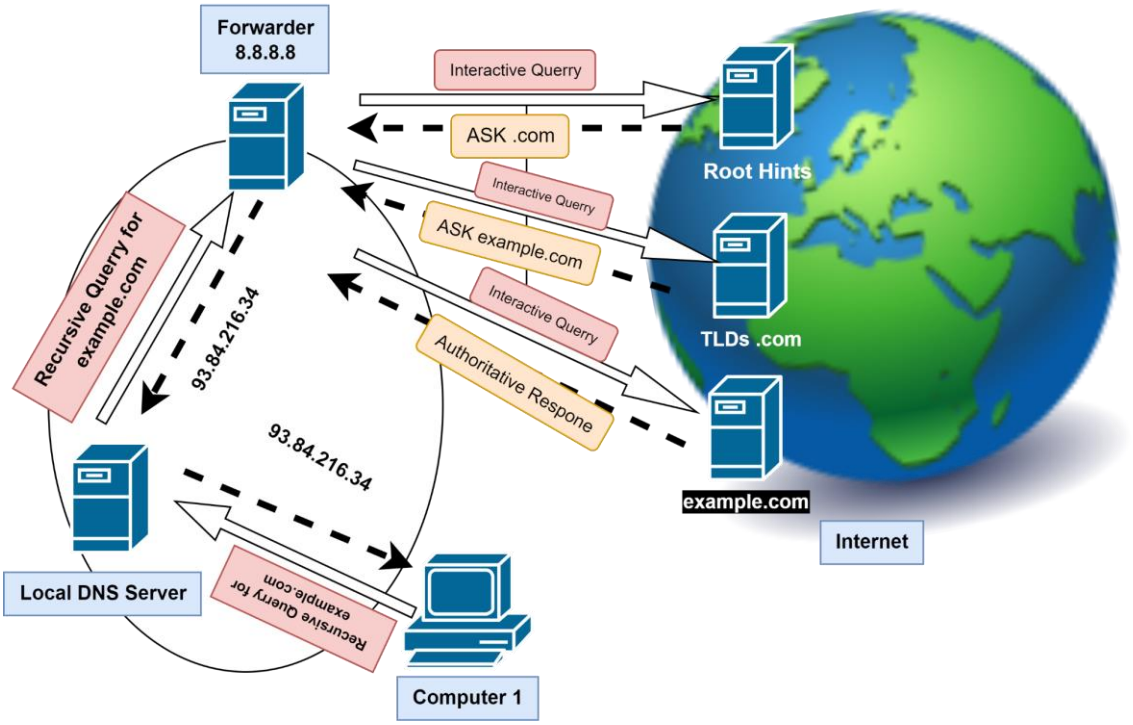
- Đầu tiên, DNS Clients kiểm tra trong Cache của xem có lưu thông tin về địa chỉ IP tương ứng với tên miền nó muốn truy vấn hay không?

- Client gửi truy vấn lên máy Local DNS Server. Nếu DNS Server này có chứa kết quả trong cơ sở dữ liệu của nó thì nó sẽ trả lời về Client. Quá trình này gọi là quá trình truy vấn đến Server có thẩm quyền (Authoritative DNS Server)

- Nếu máy Authoritative DNS Server không có câu trả lời, câu truy vấn DNS (DNS query) sẽ được chuyển (Forward) tới một máy DNS Server khác được chỉ định từ trước hoặc chuyển thẳng nó lên Root hints Server. Rồi câu truy vấn sẽ tiếp tục được gửi đến các Server quản lý tên miền theo đuôi từ phải qua trái đến khi nào đến được server quản lý tên miền tương ứng mà client đang cần truy vấn.

Chúng ta đã nói về máy Root Hint Server là máy mà Local DNS Server khi nhận được câu truy vấn từ Client mà nó không tìm thấy trong cơ sở dữ liệu của nó sẽ chuyển tiếp đến. Vậy máy Root Hint Server là gì? Root Hint Server hay còn gọi là Root Name Server là những máy DNS Server gốc quản lý các Root Domain. Nó quản lý những tên miền là Top-Level Domain trên Internet. Tên máy và địa chỉ IP tương ứng của các máy Root Name Server cũng được công bố rộng rãi khắp thế giới.

Cơ chế forwarder là cơ chế chuyển hướng câu truy vấn khi máy Name Server cục bộ không tìm thấy câu trả lời. Cơ chế Forwarder do người quản trị chủ động cấu hình. Cơ chế này được thể hiện như hình 5.5

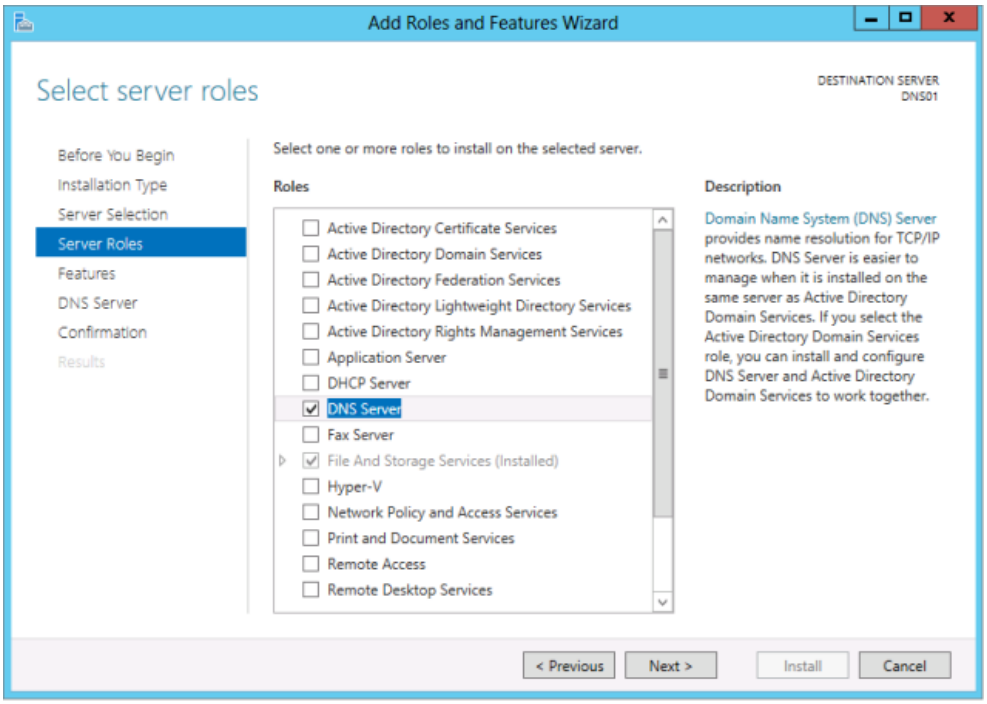


Hình 5-5 Cơ chế Forwarder

5.1.4 Cài đặt và quản trị DNS Server

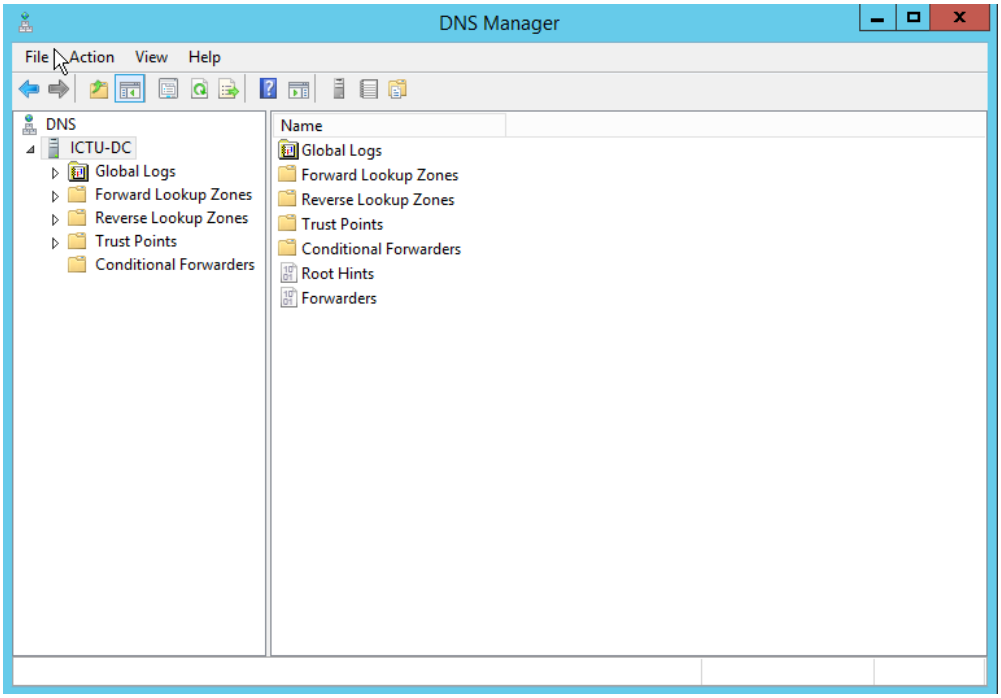
A, Cài đặt máy chủ chạy Windows Server làm DNS Server

Các bước cài đặt máy chủ Windows Server làm DNS Server khá đơn giản, người quản trị chỉ cần cài đặt Role có tên là DNS Server như trong hình 5-6



Hình 5-6 Cài đặt DNS Server

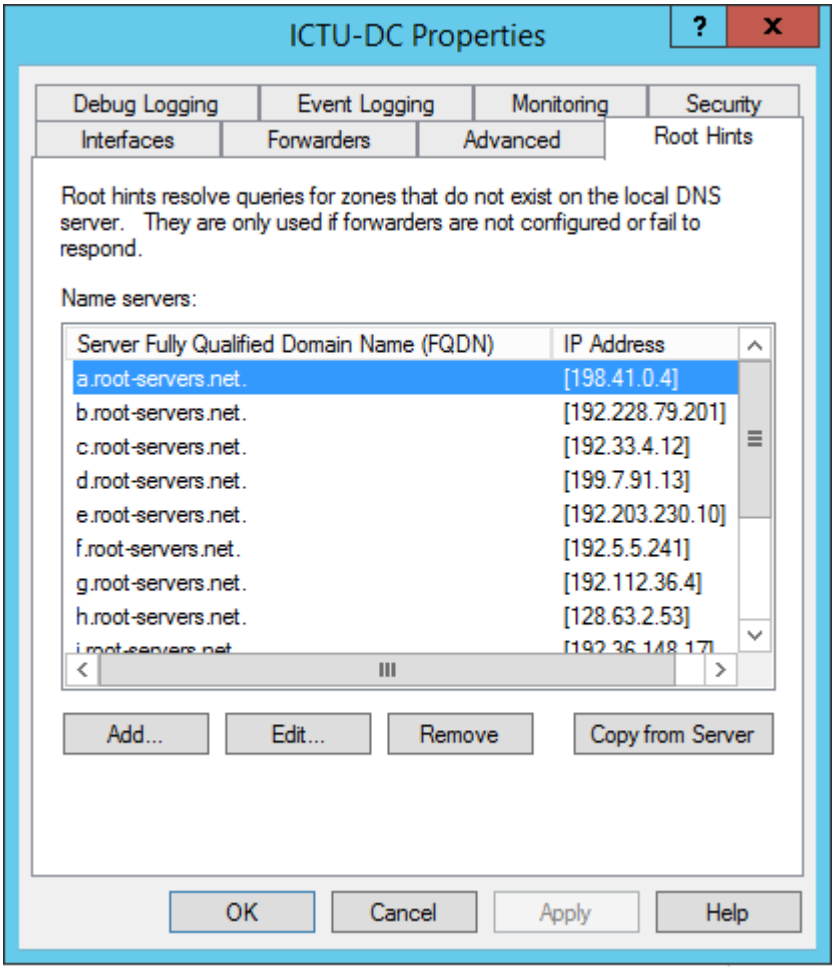
Sau khi cài đặt Role DNS xong, để quản trị máy chủ DNS chúng ta cần mở giao diện DNS Manager có sẵn trong bộ công cụ. Giao diện DNS Manager như hình 5-7.



Hình 5-7 DNS Manager

Để DNS Server hoạt động, người quản trị cần thực hiện hai cấu hình quan trọng đó là cấu hình Root Hints và cấu hình Forwarders.

Cấu hình Root Hints là cấu hình cho phép liên kết DNS Server cục bộ với hệ thống các máy chủ Root name DNS trên toàn thế giới. Điều này giúp đảm bảo DNS Server có thể phân giải được mọi yêu cầu từ người dùng. Cấu hình Root Hints được thể hiện ở hình dưới.



Hình 5-8 Cấu hình Root Hints

Cấu hình Forwarders là cấu hình liên kết máy chủ DNS Server này với các DNS Server khác, có thể là DNS Server cục bộ khác trong hệ thống, cũng có thể là các DNS Server đến từ bên thứ ba. Khi cấu hình forwarders xong nếu có truy vấn không nằm trong cơ sở dữ liệu thì máy chủ DNS Server cục bộ sẽ hỏi máy chủ được chỉ định trong Forwarders trước sau đó nếu không có câu trả lời mới gửi truy vấn đến Root Hints, điều này sẽ giúp tăng tốc độ truy vấn trong hệ thống.

B, Quản trị máy chủ DNS

Để máy chủ DNS thực hiện được nhiệm vụ phân giải tên miền trong hệ thống, người quản trị cần thực hiện khởi tạo và cấu hình các Zone trong máy chủ DNS. Zone là một thuật ngữ đề cập đến phạm vi tên miền mà máy chủ quản lý. Có một số loại zone cơ bản như sau:

Forward Lookup Zone: Đây là loại zone phổ biến nhất trong DNS. Nó ánh xạ tên miền sang địa chỉ IP. Khi bạn nhập tên miền vào trình duyệt web, forward lookup zone sẽ giúp máy tính dịch tên miền đó thành địa chỉ IP tương ứng để kết nối.

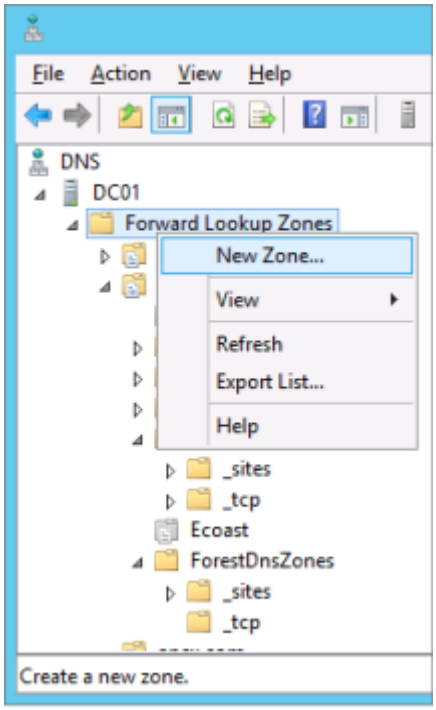
Reverse Lookup Zone: Ngược lại với forward lookup zone, reverse lookup zone cho phép tra cứu địa chỉ IP để tìm tên miền tương ứng. Khi bạn có địa chỉ IP và muốn biết tên miền của nó, reverse lookup zone sẽ cung cấp thông tin này.

Primary Zone: Là zone chứa dữ liệu thực sự của tên miền. Nó thường được lưu trữ trên máy chủ DNS và là nơi cập nhật, thêm mới hoặc chỉnh sửa các bản ghi DNS.

Secondary Zone: Đây là bản sao dự phòng của primary zone. Secondary zone lấy dữ liệu từ primary zone và giữ cho phép truy cập nhanh hơn. Nó hữu ích khi cần đảm bảo sự liên tục và cung cấp dữ liệu khi máy chủ primary gặp sự cố.

Stub Zone: Stub zone chứa thông tin DNS cơ bản như tên miền và bản ghi NS (Name Server) chỉ định cho zone đó. Nó được sử dụng để chuyển tiếp truy vấn DNS từ một domain đến một name server khác.

Khởi tạo các zone thông qua giao diện như hình



Hình 5-9 Khởi tạo Zone

Các zone sau khi được cấu hình xong sẽ có dạng như hình 5-10, trong đó ở bên phải là các bản ghi DNS đã được khởi tạo. Có các loại bản ghi DNS phổ biến như sau:

A Record (Address Record): Liên kết một địa chỉ IP v4 với một tên miền.

AAAA Record (IPv6 Address Record): Tương tự như A record, nhưng dùng để ánh xạ địa chỉ IPv6 với tên miền.

CNAME Record (Canonical Name Record): Chỉ định một tên miền phụ (alias) cho một tên miền chính (canonical name). Thường được sử dụng để tạo các bí danh cho các tên miền chính.

MX Record (Mail Exchange Record): Chỉ định máy chủ email (mail server) có trách nhiệm nhận email cho tên miền được xác định.

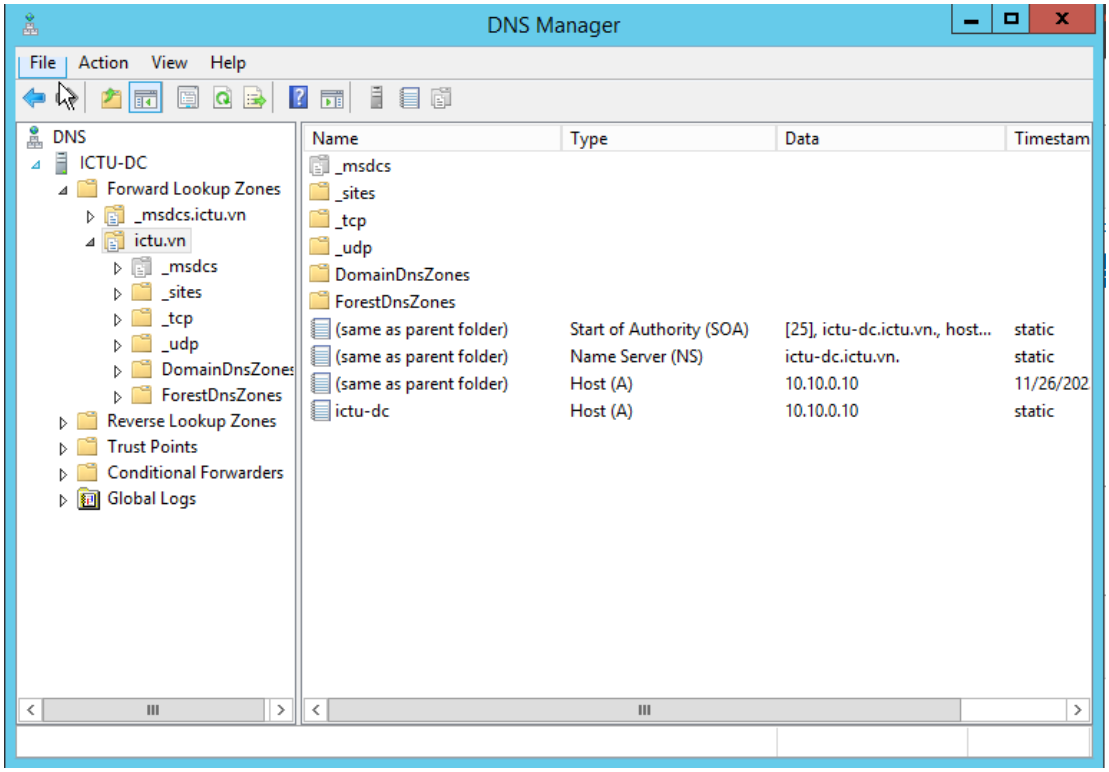
TXT Record (Text Record): Chứa văn bản không định dạng hoặc thông tin mô tả liên quan đến tên miền.

PTR Record (Pointer Record): Thường được sử dụng trong reverse DNS lookup, ánh xạ địa chỉ IP về tên miền.

NS Record (Name Server Record): Xác định name server cho tên miền cụ thể, chỉ ra nơi lưu trữ thông tin DNS cho tên miền đó.

SOA Record (Start of Authority Record): Chứa thông tin quản lý cho một zone cụ thể, bao gồm thông tin về máy chủ chính quản lý zone đó.

SRV Record (Service Record): Chứa thông tin về dịch vụ cụ thể nằm trong một tên miền nhất định, thường được sử dụng cho các dịch vụ như VoIP, Active Directory, và các dịch vụ mạng khác.



Hình 5-10 Giao diện quản lý DNS

5.2 Dịch vụ DHCP

Mỗi thiết bị trên mạng có dùng bộ giao thức **TCP/IP** đều phải có một địa chỉ **IP** hợp lệ, phân biệt. Để hỗ trợ cho vấn đề theo dõi và cấp phát các địa chỉ **IP** được chính xác, tổ chức **IETF** (**Internet Engineering Task Force**) đã phát triển ra giao thức **DHCP** (**Dynamic Host Configuration Protocol**). Giao thức này được mô tả trong các **RFC** 1533, 1534, 1541 và 1542. Chúng ta có thể tìm thấy các **RFC** này tại địa chỉ **http://www.ietf.org/rfc.html**. Để có thể làm một **DHCP Server**, máy tính **Windows Server 2003** phải đáp ứng các điều kiện sau:

- Đã cài dịch vụ **DHCP**.
- Mỗi **interface** phải được cấu hình bằng một địa chỉ IP tĩnh.
- Đã chuẩn bị sẵn danh sách các địa chỉ **IP** định cấp phát cho các máy **client**.

Dịch vụ **DHCP** này cho phép chúng ta cấp động các thông số cấu hình mạng cho các máy trạm (**client**). Các hệ điều hành của **Microsoft** và các hệ điều hành khác như **Unix** hoặc **Macintosh** đều hỗ trợ cơ chế nhận các thông số động, có nghĩa là trên các hệ điều hành này phải có một **DHCP Client**. Cơ chế sử dụng các thông số mạng được cấp phát động có ưu điểm hơn so với cơ chế khai báo tĩnh các thông số mạng như:

- Khắc phục được tình trạng đụng địa chỉ **IP** và giảm chi phí quản trị cho hệ thống mạng.
- Giúp cho các nhà cung cấp dịch vụ (**ISP**) tiết kiệm được số lượng địa chỉ **IP** thật (**Public IP**).
- Phù hợp cho các máy tính thường xuyên di chuyển qua lại giữa các mạng.
- Kết hợp với hệ thống mạng không dây (**Wireless**) cung cấp các điểm **Hotspot** như: nhà ga, sân bay, trường học…

5.2.1 Nguyên lý hoạt động của giao thức DHCP

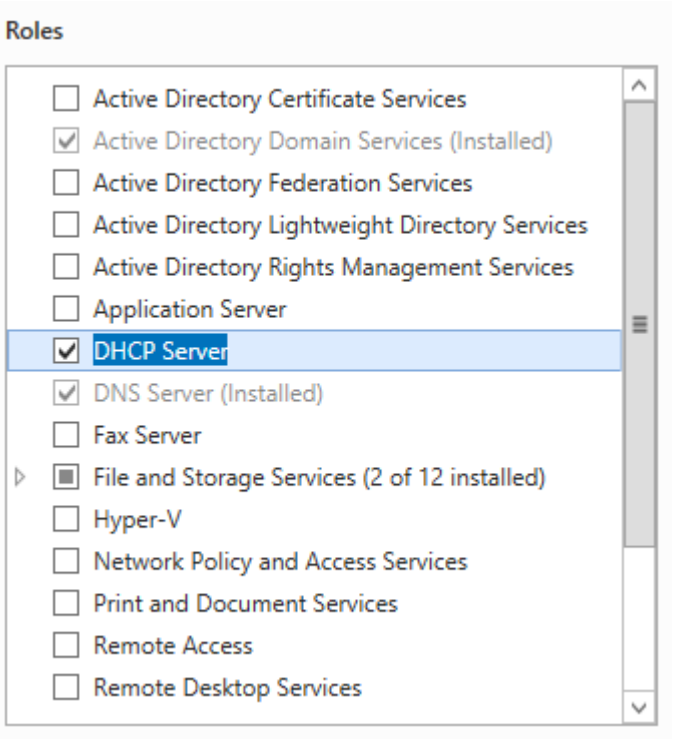
Giao thức **DHCP** làm việc theo mô hình **client/server**. Theo đó, quá trình tương tác giữa **DHCP** client và **server** diễn ra theo các bước sau:

- Khi máy client khởi động, máy sẽ gửi **broadcast** gói tin **DHCPDISCOVER**, yêu cầu một **server** phục vụ mình. Gói tin này cũng chứa địa chỉ **MAC** của máy **client**.
- Các máy **Server** trên mạng khi nhận được gói tin yêu cầu đó, nếu còn khả năng cung cấp địa chỉ **IP**, đều gửi lại cho máy **Client** gói tin **DHCPOFFER**, đề nghị cho thuê một địa chỉ **IP** trong một khoản thời gian nhất định, kèm theo là một **subnet mask** và địa chỉ của **Server**. **Server** sẽ không cấp phát địa chỉ **IP** vừa đề nghị cho những **Client** khác trong suốt quá trình thương thuyết.

- Máy **Client** sẽ lựa chọn một trong những lời đề nghị (**DHCPOFFER**) và gửi **broadcast** lại gói tin **DHCPREQUEST** chấp nhận lời đề nghị đó. Điều này cho phép các lời đề nghị không được chấp nhận sẽ được các **Server** rút lại và dùng đề cấp phát cho **Client** khác.
- Máy **Server** được **Client** chấp nhận sẽ gửi ngược lại một gói tin **DHCPACK** như là một lời xác nhận, cho biết là địa chỉ **IP** đó, **subnet mask** đó và thời hạn cho sử dụng đó sẽ chính thức được áp dụng. Ngoài ra **Server** còn gửi kèm theo những thông tin cấu hình bổ sung như địa chỉ của **gateway** mặc định, địa chỉ **DNS Server**, …

5.2.2 Cài đặt máy chủ DHCP Server

Giống như các dịch vụ khác, để nâng cấp máy chủ thành DHCP Server, cần cài đặt Role DHCP như hình

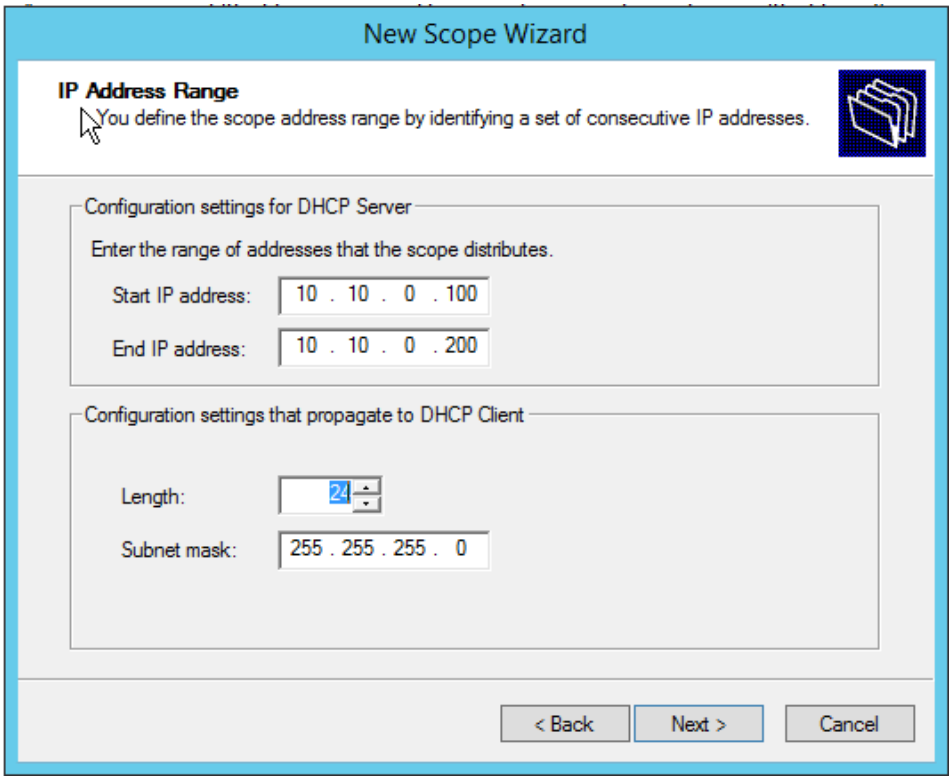


Hình 5-11 Cài đặt DHCP Server

Cần phải lưu ý là, máy chủ sử dụng để làm DHCP Server cần được cấu hình địa chỉ IP tĩnh, cố định.

Chúng ta cũng cần lên kế hoạch về dải mạng sẽ sử dụng, số lượng địa chỉ IP, subnet mask, các thông tin về DNS Server và Gateway để có thể cấu hình lên DHCP Server khi hoàn thiện.

Hình … mô tả giao diện cấu hình dải địa chỉ IP để cấp phát trong mạng.



Hình 5-12 Cấu hình tạo Scope

Sau đó chúng ta cần cấu hình các thông số như sau:

Exclusion and Delay: dải địa chỉ loại trừ, khi cấu hình tùy chọn này những địa chỉ IP được nhập vào sẽ không được máy chủ DHCP mang ra cấp cho Client, mà sẽ được để dành riêng cho các dịch vụ đặc biệt cho người quản trị cấu hình.

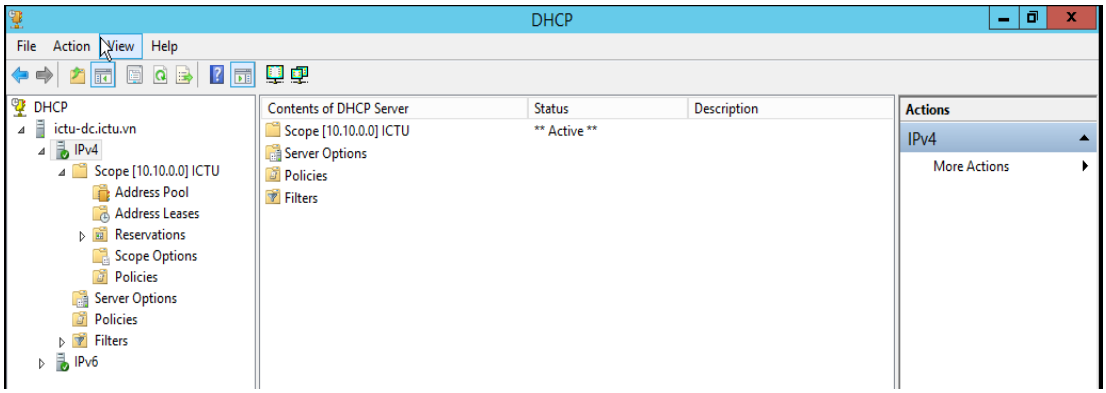
Lease Duration: Thời gian cho thuê địa chỉ IP.

Router: Đây là địa chỉ cổng mặc định cho các kết nối mạng.

DNS: Địa chỉ máy chủ DNS Server nội bộ trong mạng.

Một máy chủ DHCP khi hoàn thiện việc cấu hình sẽ có giao diện quản lý như hình

..



Hình 5-13 Quản lý DHCP Server

5.3 Dịch vụ VPN

VPN là mạng riêng ảo, Virtual Private Network, là một công nghệ mạng giúp tạo kết nối mạng an toàn khi tham gia vào mạng công cộng như Internet hoặc mạng riêng do một nhà cung cấp dịch vụ sở hữu. Các tập đoàn lớn, các cơ sở giáo dục và cơ quan chính phủ sử dụng công nghệ VPN để cho phép người dùng từ xa kết nối an toàn đến mạng riêng của cơ quan mình.

Hình 5-14 Sử dụng VPN kết nối Internet

Một hệ thống VPN có thể kết nối được nhiều site khác nhau, dựa trên khu vực, diện tích địa lý... tượng tự như chuẩn **Wide Area Network (WAN)**. Bên cạnh đó, VPN còn được dùng để "khuếch tán", mở rộng các mô hình Intranet nhằm truyền tải thông tin, dữ liệu tốt hơn. Ví dụ, các trường học vẫn phải dùng VPN để nối giữa các khuôn viên của trường (hoặc giữa các chi nhánh với trụ sở chính) lại với nhau.

Các giao thức thường được sử dụng trong VPN

Bản chất của giao thức VPN là một tập hợp các giao thức. Có một số chức năng mà mọi VPN phải giải quyết được:

- Tunnelling (kỹ thuật truyền dữ liệMu qua nhiều mạng có giao thức khác nhau) - Chức năng cơ bản của VPN là phân phối các gói (packet) từ điểm này đến điểm khác mà không để lộ chúng cho bất kỳ ai trên đường truyền. Để làm điều này, VPN đóng gói tất cả dữ liệu theo định dạng mà cả máy khách và máy chủ đều hiểu được. Bên gửi dữ liệu đặt nó vào định dạng tunnelling và bên nhận trích xuất để có được thông tin.

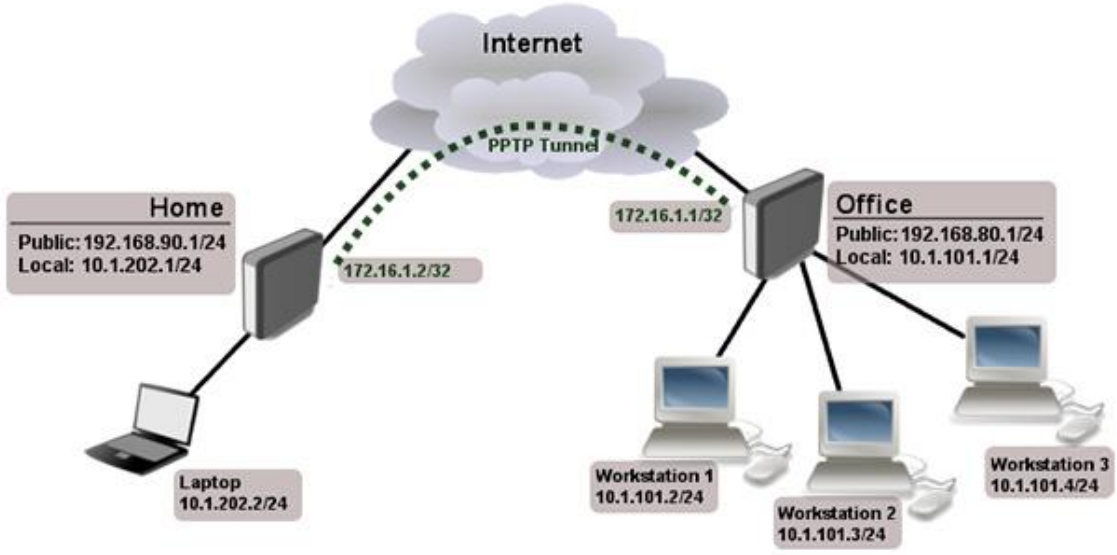
- Mã hóa: Tunnelling không cung cấp tính năng bảo vệ. Bất cứ ai cũng có thể trích xuất dữ liệu. Dữ liệu cũng cần phải được mã hóa trên đường truyền. Bên nhận sẽ biết cách giải mã dữ liệu từ một người gửi nhất định.

- Xác thực. Để bảo mật, VPN phải xác nhận danh tính của bất kỳ client nào cố gắng "giao tiếp" với nó. Client cần xác nhận rằng nó đã đến đúng máy chủ dự định.

- Quản lý phiên: Một khi người dùng được xác thực, VPN cần duy trì phiên để client có thể tiếp tục "giao tiếp" với nó trong một khoảng thời gian.

Nói chung các giao thức VPN coi việc tạo tunnel, xác thực và quản lý phiên như một gói. Điểm yếu trong bất kỳ chức năng nào đều là những lỗ hổng bảo mật tiềm ẩn trong giao thức. Mã hóa là một chuyên ngành, nó cũng rất khó, nên thay vì cố gắng tạo ra cái mới, các VPN thường sử dụng kết hợp nhiều giao thức mã hóa đáng tin cậy.

- **Giao thức PPTP:** Giao thức cũ nhất vẫn đang được sử dụng là PPTP (Point-to-Point Tunneling Protocol). PPTP lần đầu tiên được sử dụng vào năm 1995. PPTP không chỉ định giao thức mã hóa nhưng có thể sử dụng một số giao thức như MPPE-128 mạnh mẽ. Việc thiếu sự tiêu chuẩn hóa về giao thức mạnh là một rủi ro, vì nó chỉ có thể sử dụng tiêu chuẩn mã hóa mạnh nhất mà cả 2 phía cùng hỗ trợ. Nếu một phía chỉ hỗ trợ tiêu chuẩn yếu hơn thì kết nối phải sử dụng mã hóa yếu hơn người dùng mong đợi.



Hình 5-15 Giao thức PPTP

Tuy nhiên, vấn đề thực sự với PPTP là quá trình xác thực. PPTP sử dụng giao thức MS-CHAP, có thể dễ dàng bị crack trong giai đoạn hiện nay. Kẻ tấn công có thể đăng nhập và mạo danh người dùng được ủy quyền.

- **Giao thức IPSEC**: Được dùng để bảo mật các giao tiếp, các luồng dữ liệu trong môi trường Internet (môi trường bên ngoài VPN). Đây là điểm mấu chốt, lượng traffic qua IPSec được dùng chủ yếu bởi các Transport mode, hoặc các tunnel (hay gọi là hầm - khái niệm này hay dùng trong Proxy, SOCKS) để MÃ HÓA dữ liệu trong VPN. Sự khác biệt giữa các mode này là: Transport mode chỉ có nhiệm vụ mã hóa dữ liệu bên trong các gói (data package - hoặc còn biết dưới từ payload). Trong khi các Tunnel mã hóa toàn bộ các data package đó.
- **Giao thức L2TP:** Được dùng để bảo mật các giao tiếp, các luồng dữ liệu trong môi trường Internet (môi trường bên ngoài VPN). Đây là điểm mấu chốt, lượng traffic qua IPSec được dùng chủ yếu bởi các Transport mode, hoặc các tunnel (hay gọi là hầm - khái niệm này hay dùng trong Proxy, SOCKS) để MÃ HÓA dữ liệu trong VPN. Sự khác biệt giữa các mode này là: Transport mode chỉ có nhiệm vụ mã hóa dữ liệu bên trong các gói (data package - hoặc còn biết dưới từ payload). Trong khi các Tunnel mã hóa toàn bộ các data package đó.

Các giao thức kể trên đều được ra đời và phát triển từ cách đây khá lâu. Qua thời gian sử dụng, chúng đều bộc lộ những lỗ hổng bảo mật khá nguy hiểm. Ngày nay, các nhà nghiên cứu đã phát triển và công bố một số phương thức bảo mật an toàn hơn so với ba giao thức trên. Có thể kể đến một vài cái tên trong số đó như: IKEv2 (Internet Key Exchange), SSTP (Securre Socket Tunneling Protocol), OpenVPN, SoftEther.

5.4 Dịch vụ NPS và NAP

5.4.1 NPS

NPS hay Network Policy Server là một tính năng mới ra đời trên Windows Server 2008 nhằm thay thế IAS (Internet Authentication Service) cho phép sử dụng Windows Server 2008 để chứng thực Client sử dụng giao thức 802.1x.

NPS không chỉ là một sự thay thế cho IAS mà nó còn thực hiện nhiều hơn những gì IAS đã từng làm. Trong khi nhiều chúng ta trong số chúng ta có thể mới chỉ xem để thực hiện những thứ tương tự mà IAS đã thực hiện được trong Windows 2003 thì khi cài đặt NPS chúng ta sẽ thấy được rất nhiều chức năng mới trong đó.

Chức năng của NPS

- Định tuyến lưu lượng cho LAN và WAN
- Cho phép truy cập vào các tài nguyên nội bộ thông qua kết nối VPN hoặc dial-up.

- Tạo và ép buộc sự truy cập mạng thông qua các kết nối VPN hoặc dial-up.

Tuy nhiên NPS còn có thể cung cấp các chức năng khác như:

- Các dịch vụ VPN
- Các dịch vụ Dial-up
- Truy cập được bảo vệ 802.11
- Routing & Remote Access (RRAS)
- Đăng ký chứng thực thông qua Windows Active Directory
- Điều khiển truy cập mạng bằng các chính sách

Những gì mà NPS thực hiện trên là tất cả các chức năng có liên quan đến NAP. Ví dụ - System Health Validators, Remediation Server Groups, Health Polices,…

5.4.2 NAP

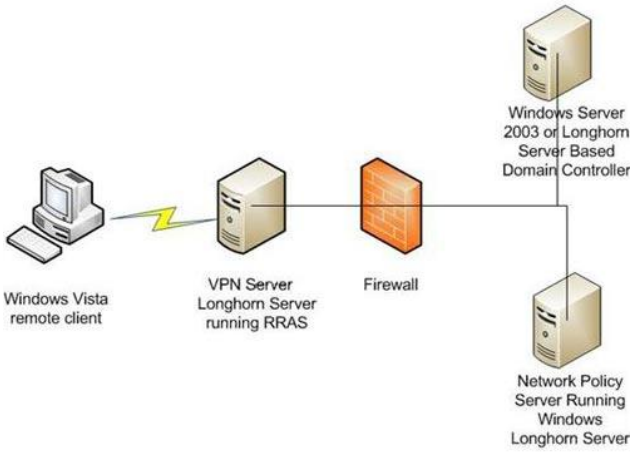
Định nghĩa

Một khía cạnh bảo mật mạng gây khó chịu cho nhiều quản trị viên đó là việc không thể kiểm soát cấu hình của các máy tính từ xa. Mặc dù mạng của một công ty có thể đang hoạt động an toàn nhưng vẫn không có gì để ngăn chặn người dùng từ xa truy cập vào mạng thông qua một máy tính đã bị nhiễm virus hay có các lỗ hổng chưa được nâng cấp bản vá kịp thời.

NAP là một tính năng nhằm bảo đảm máy tính của người dùng từ xa tuân theo các yêu cầu bảo mật trong tổ chức. NAP sẽ không làm gì để ngăn chặn truy cập trái phép đến mạng. Nếu một người xâm phạm có một máy tính đáp ứng được các chính sách bảo mật của công ty thì NAP sẽ không thực hiện bất hoạt động gì để ngừng hoạt động truy cập của người này. Việc ngăn chặn truy nhập của người này là công việc của các kỹ thuật bảo mật khác. NAP đơn giản chỉ được thiết kế để ngăn chặn người dùng đăng nhập vào mạng khi sử dụng các máy tính không bảo đảm.

Mô hình triển khai NAP

Việc thi hành NAP cần sử dụng một số máy chủ, mỗi một máy chủ có một vai trò riêng. Có thể xem ở hình dưới để có cái nhìn tổng quát về vấn đề này.



Hình 5-16 Sơ đồ hoạt động của NAP

Mô hình trên bao gồm các thành phần sau:

- Một máy chủ đóng vai trò là VPN RRAS Server cho phép Client truy cập từ xa vào mạng nội bộ
- Một máy chủ đóng vai trò là máy chủ điều khiển miền có chứa dịch vụ thư mục và DNS

Cuối cùng là máy chủ chính sách NPS cho phép cấu hình các chính sách được áp dụng.

5.5 Dịch vụ Web với IIS

Word Wide Web (thường được gọi tắt là Web) là mạng lưới nguồn thông tin cho phép mọi người khai thác thông tin qua một số công cụ hoặc là chương trình hoạt động cùng các giao thức mạng. World Wide Web là một trong số các dịch vụ của Internet nhằm giúp cho việc trao đổi thông tin trở nên thuận tiện và dễ dàng. Sở dĩ Web trở nên phổ biến vì Web cung cấp cho người sử dụng khả năng truy cập dễ dàng, từ đó người sử dụng có thể khai thác các thông tin đa dạng trên Internet (văn bản, hình ảnh, âm thanh, video).

Những thông tin trên web được biểu diễn trên các trang web (webpage), theo đúng nghĩa đen của từ "trang" mà chúng ta có thể nhìn thấy trên màn hình máy tính. Mọi thông tin đều có thể biểu thị trên trang Web, đồng thời có khả năng liên kết với những trang Web khác và dẫn người dùng đến những nguồn thông tin khác. Khả năng này của Web có được là nhờ thông qua các siêu liên kết (hyperlink). Bằng những siêu liên kết này, các trang Web có thể liên kết với nhau thành một mạng lưới rộng lớn, và đó cũng là nguồn gốc của thuật ngữ web (nghĩa là mạng nhện trong tiếng Anh). Tập hợp các trang web dưới cùng một tên miền tạo thành một website.

Trên Internet hiện nay có hàng triệu website đang hoạt động với đủ các hình thức và chức năng khác nhau. Tuy nhiên, có thể phân biệt một số loại website thường gặp:

-Website giới thiệu: là loại website căn bản và đơn giản nhất, dùng để giới thiệu về một cá nhân hay một đơn vị. Website loại này chứa ít trang, ít tốn kém và dễ làm nhất.

-Website lưu trữ thông tin: còn gọi là thư viện điện tử, chứa các thông tin chuyên môn được sắp xếp thành nhiều đề mục, nhiều tiêu đề dễ tra cứu. Website lưu trữ phải được cập nhật thường xuyên thông tin mới và được sắp xếp sao cho người xem tìm ngay được thông tin mình muốn tìm.

-Website truyền dữ liệu: là loại website được thiết kế đặc biệt để thu nhận thông tin từ xa. Một cơ quan hay một doanh nghiệp làm công tác quản lý chương trình có nhiều đơn vị vệ tinh thay vì phải đến tận đơn vị ở quận huyện, tỉnh thành khác để ghi chép thông tin thì nay có thể ngồi tại chỗ để nhận thông tin qua mạng Internet và chỉ việc kiểm chứng, đánh giá thông tin trước khi nhập vào kho thông tin chung. Website này thuộc hàng cao cấp có nhiều chương trình lồng trong trang web, đòi hỏi nhà thiết kế phải có trình độ nhất định trong cả lĩnh vực điện toán lẫn chuyên môn.

-Website thương mại: chứa thông tin hàng hoá và dịch vụ, chứa nhiều form và chứa các script tính toán để người tiêu dùng có thể mua và trả tiền ngay qua website. Hiện nay bên cạnh thuật ngữ website còn thường sử dụng thuật ngữ ứng dụng web (TA: web application hay web app). Trong đa số các trường hợp hai thuật ngữ này có mối liên hệ chặt chẽ với nhau và khó phân biệt. Nếu một website cung cấp nhiều chức năng tập trung vào một mảng nào đó (gần giống như một ứng dụng cho máy desktop) thì cũng được gọi là một ứng dụng web.

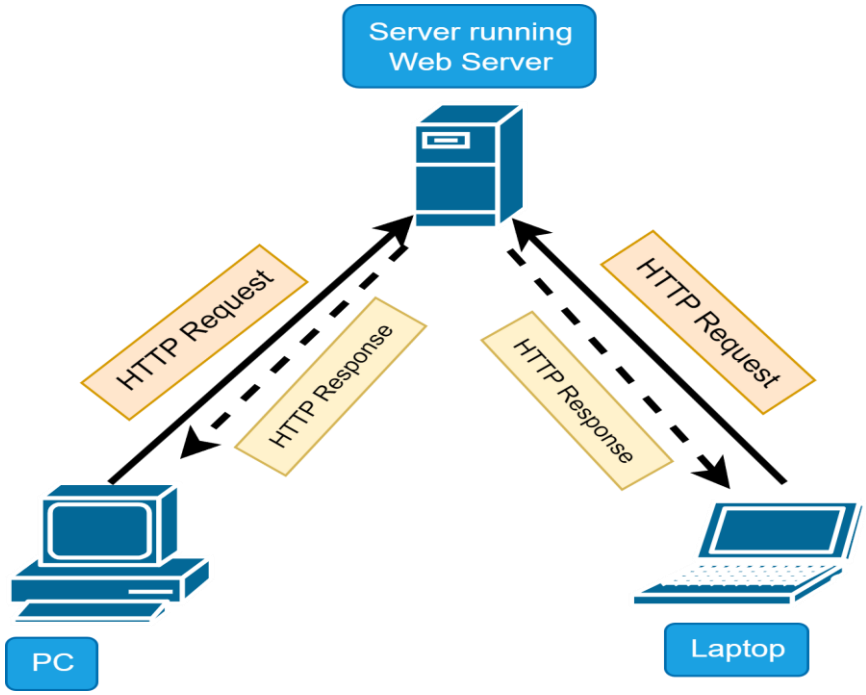
Tổng hợp các ứng dụng web của một tổ chức như thư điện tử, chia sẻ tài liệu, lịch công tác, v.v., thông qua giao diện Web tạo thành một hệ thống lớn gọi là cổng thông tin điện tử (TA: web portal). Cổng thông tin là công cụ đắc lực cho các hoạt động của mọi doanh nghiệp, giúp người dùng có thể tận dụng tối đa những tài nguyên có sẵn và nâng cao giá trị của thông tin.

5.5.1 Giao thức HTTP

Một hệ thống Web là một hệ thống cung cấp thông tin trên mạng Internet thông qua các thành phần như Máy chủ, trình duyệt và nội dung thông tin. Trong phần này sẽ giới thiệu một cách cơ bản nguyên lý hoạt động của một hệ thống Web cũng như các thông tin liên quan tới các cách thức xác định vị trí nguồn thông tin, cách thức trao đổi dữ liệu giữa máy chủ với trình duyệt và cách thức thể hiện thông tin.

Từ khía cạnh kiến trúc ứng dụng mạng, hệ thống web là một dạng chương trình hoạt động theo mô hình chủ - khách với hai thành phần: Chương trình khách (client), thường được gọi là trình duyệt web (web browser), chạy trên máy tính của người dùng đầu cuối; Chương trình chủ, gọi là web server, được cài đặt và chạy trên máy có cấu

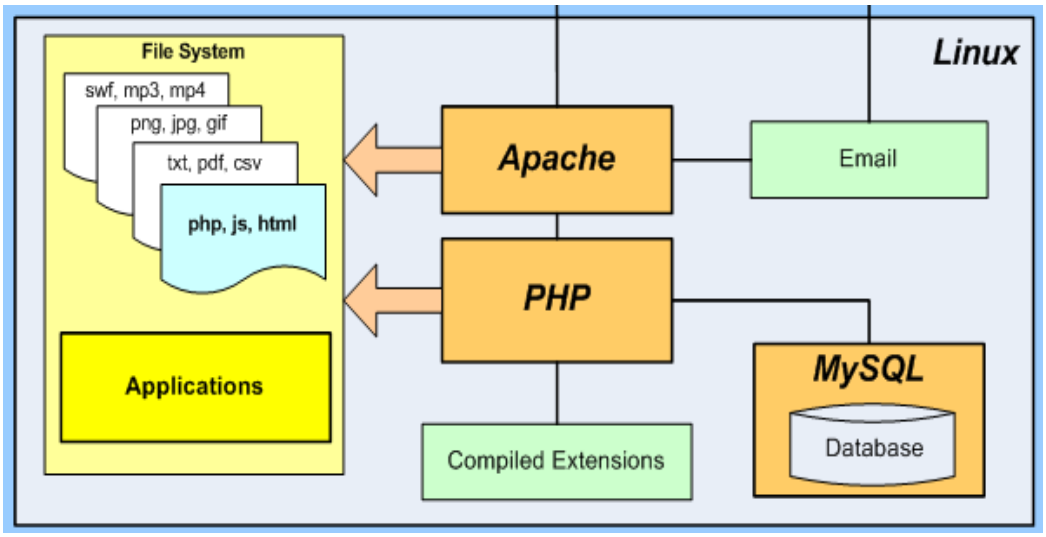
hình mạnh (máy này cũng thường được gọi là web server). Chương trình khách và chương trình chủ trao đổi dữ liệu với nhau thông qua giao thức HTTP theo nhu cầu của người sử dụng (client), trong đó trình duyệt sẽ gửi cho server các thông điệp đặc biệt theo cấu trúc quy định của HTTP (gọi là HTTP request), server sẽ gửi lại cho trình duyệt các dữ liệu theo yêu cầu (gọi là HTTP response). Hình 5.16 trình bày mô hình hoạt động của hệ thống web .



Hình 5-17 Mô hình hoạt động của chương trình Web

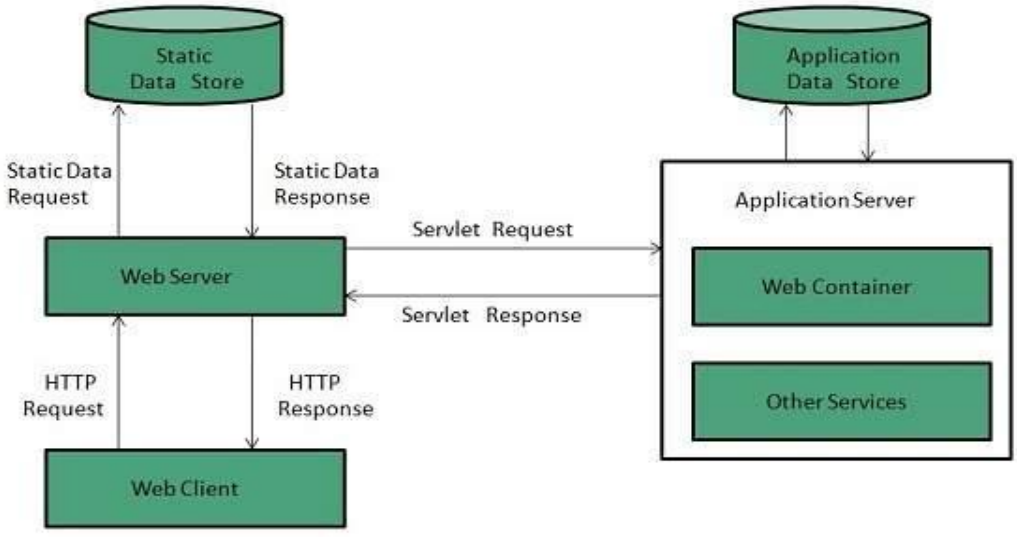
Như vậy, một hệ thống Web gồm có 2 thành phần: Trình duyệt Web chạy trên máy client và Web Server chạy trên máy Server.

Trong đó, Web Server có thể được hiểu theo hai nghĩa: một chương trình ứng dụng có chức năng chính là lưu trữ, xử lý và cung cấp các trang web cho các chương trình khách theo yêu cầu từ các chương trình này; một máy tính cấu hình cao có cài đặt chương trình máy chủ web và một số chương trình hỗ trợ khác cho việc xử lý và phục vụ web (vd.: database server, v.v.). Trên thực tế, chương trình ứng dụng máy chủ web cũng cần phải có các chương trình khác hỗ trợ để có thể hoàn thành nhiệm vụ xử lý các ứng dụng web hiện đại, trong đó có máy chủ cơ sở dữ liệu (TA: Database Server) và chương trình hỗ trợ thực thi mã nguồn viết bằng các ngôn ngữ lập trình cho server (vd.: trình thông dịch ngôn ngữ PHP đối với Apache) như hình 5.17.



Hình 5-18 Cấu trúc thường gặp của một web server với Apache, MySQL, PHP

Khi client gửi yêu cầu tải một trang web, chương trình máy chủ web sẽ tìm kiếm trang theo yêu cầu. Nếu trang yêu cầu được tìm thấy, chương trình máy chủ sẽ gửi lại cho client với một HTTP response, trong đó nội dung trang web (dưới dạng HTML) được chứa trong khối dữ liệu của gói tin HTTP response. Nếu trang web yêu cầu không được tìm thấy, máy chủ web sẽ gửi các thông báo "HTTP: Error 404 Not found". Nếu client yêu cầu cho một số tài nguyên khác thì máy chủ web sẽ liên lạc với các máy chủ ứng dụng và lưu trữ dữ liệu để tự tạo ra dữ liệu HTML theo yêu cầu và gửi dữ liệu này lại cho client.



Hình 5-19 Sơ đồ nguyên tắc hoạt động của một hệ thống máy chủ Web

Chương trình máy chủ web thường có kiến trúc xử lý đồng thời (Concurrent) hoặc đơn luồng hướng sự kiện (Single-Process-Event-Driven). Kiến trúc xử lý đồng thời cho phép các máy chủ web xử lý nhiều yêu cầu của khách hàng cùng một lúc. Nó có thể đạt được bằng cách sử dụng các phương pháp xử lý đa tiến trình (Multi-processing), xử lý

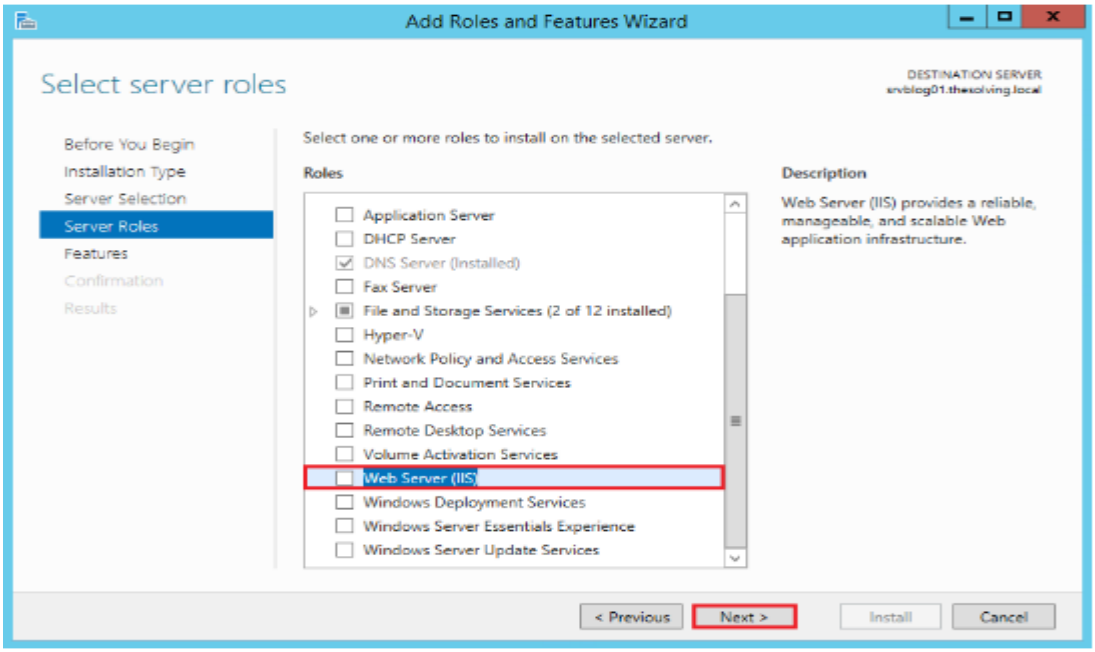
đa luồng (Multi-threading), và phương pháp lai (Hybrid). Có một số Web Server thông dụng bao gồm: IIS, Apache,…

5.5.2 Cài đặt và cấu hình IIS trên Windows Server

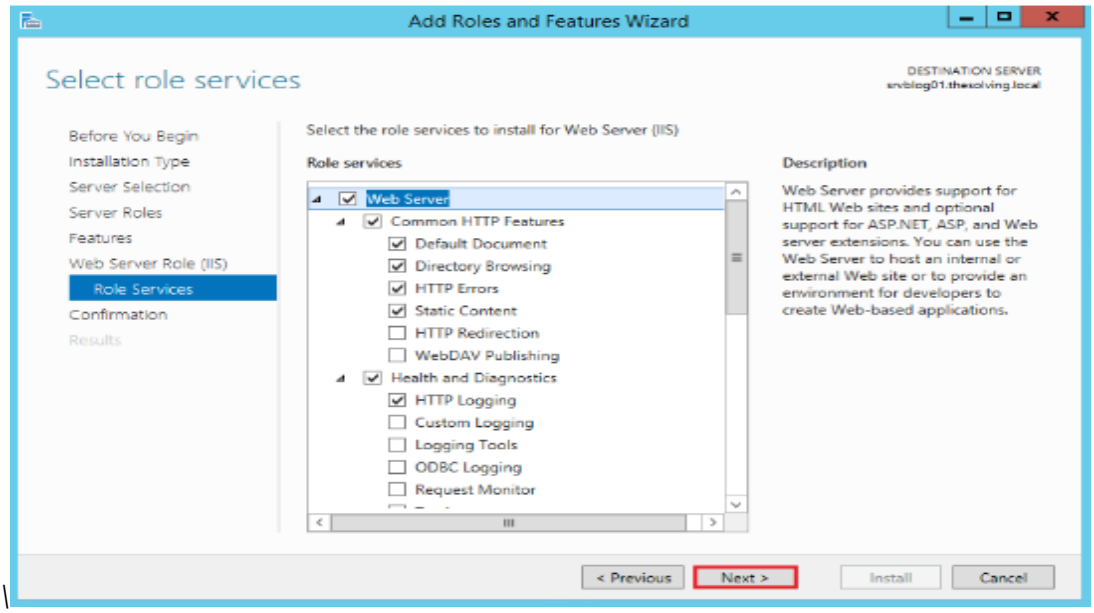
Bây giờ, chúng ta sẽ tìm hiểu về cách cài đặt IIS trên máy server để lưu trữ trang web. Quá trình cài đặt và cấu hình gồm 2 bước:

-Bước 1: Cài đặt Web Server (IIS) role

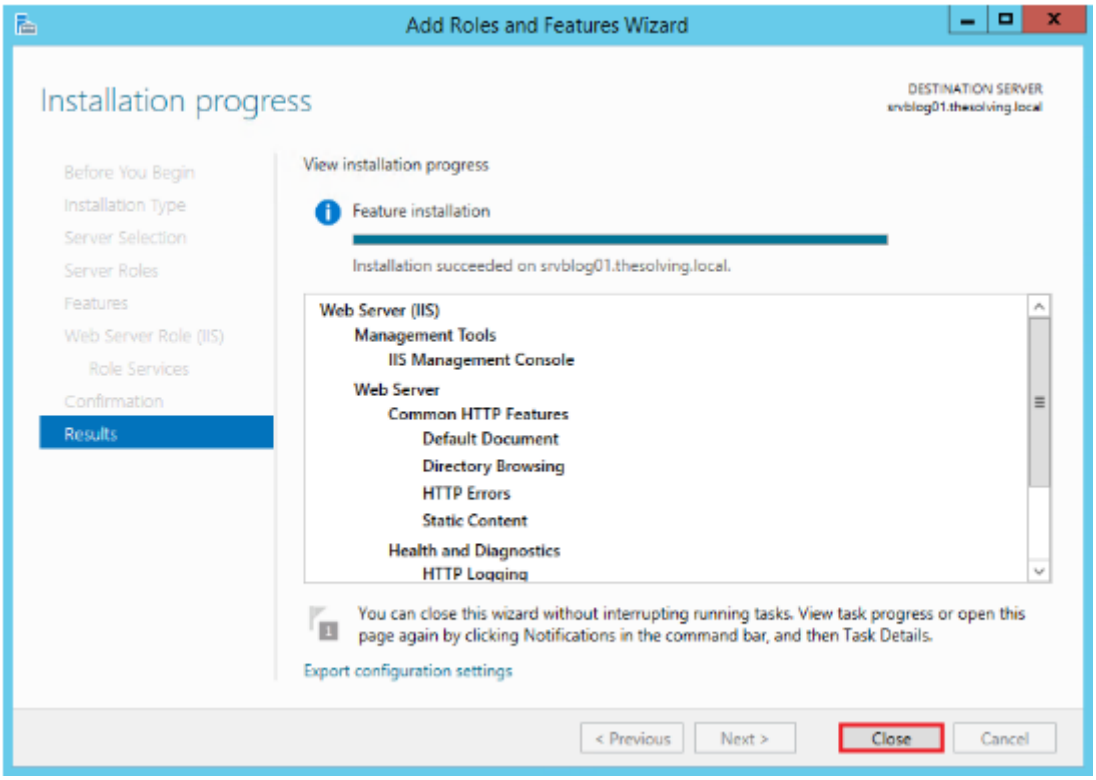
Mở Server Manager và click Add Roles and Features như hình 5.20



Hình 5-20 Server Roles



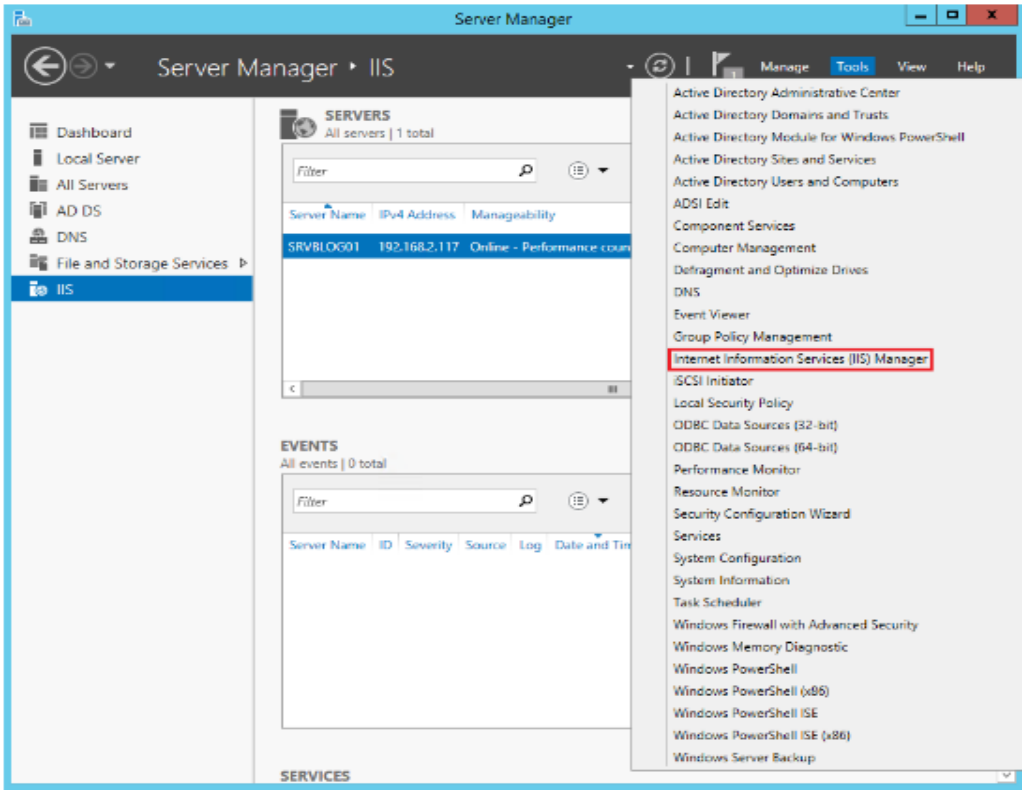
Hình 5-21 Lựa chọn các Roles Service cho IIS



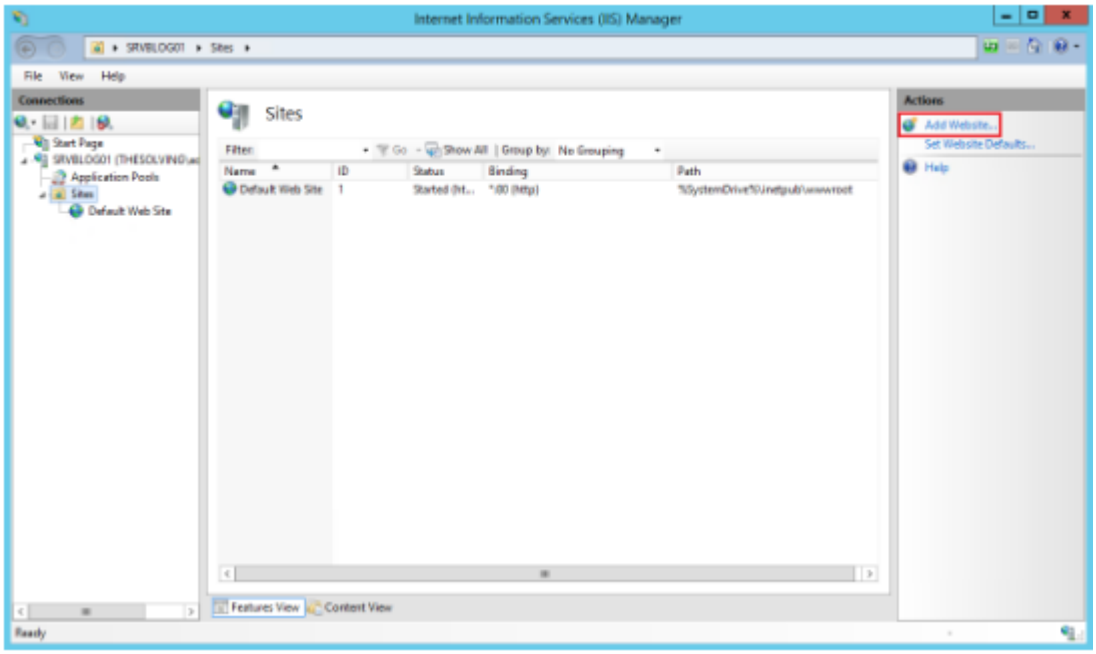
Hình 5-22 Hoàn thành cài đặt Roles IIS

-Bước 2: Cấu hình IIS

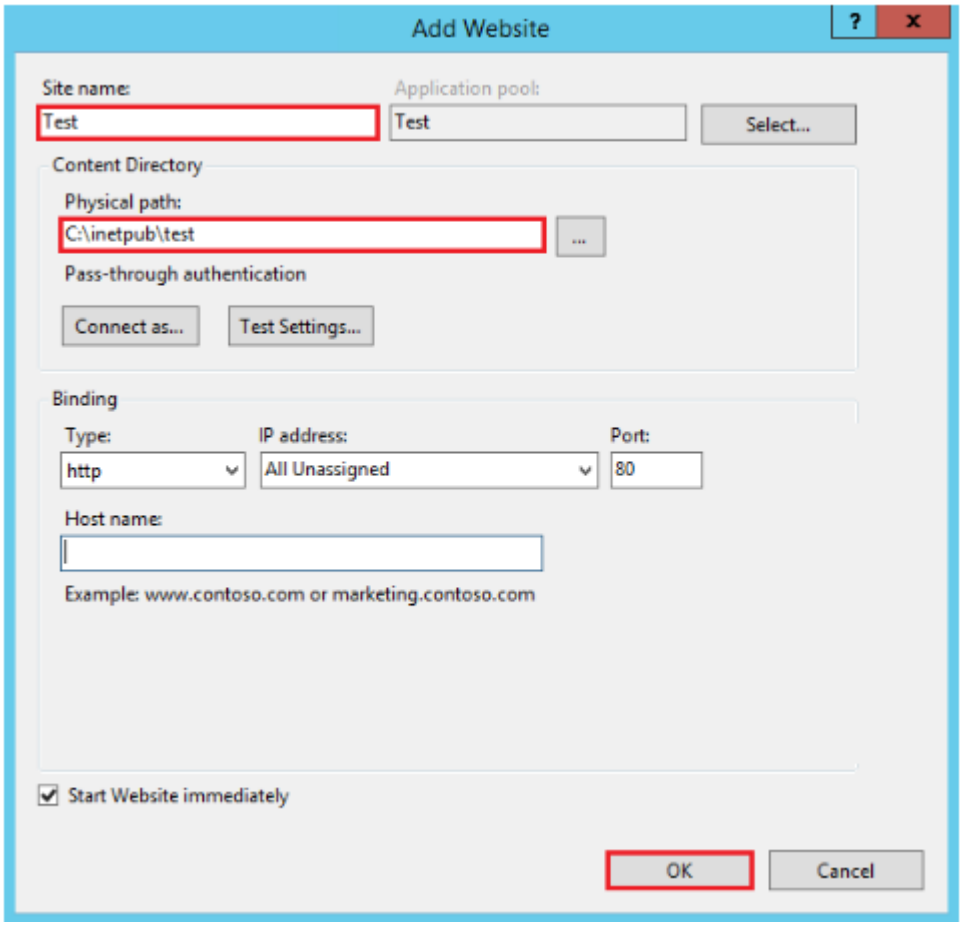
Trở lại tab Server Manager, lựa chọn Internet Information Services (IIS) từ menu Tools:



Hình 5-23 Cấu hình IIS



Hình 5.28: Click Add Website



Hình 5.29: Chỉ rõ tên site và đường dẫn

CHƯƠNG 6 GIÁM SÁT VÀ KIỂM SOÁT TRUY CẬP

6.1 Giám sát máy chủ

Giám sát hệ thống máy chủ là quá trình theo dõi, kiểm tra và quản lý các máy chủ và tài nguyên của chúng để đảm bảo chúng hoạt động hiệu quả, an toàn và không bị sự cố. Việc giám sát này thường được thực hiện thông qua việc sử dụng các công cụ và phần mềm để theo dõi các thông số kỹ thuật, tài nguyên và hoạt động của máy chủ như CPU, bộ nhớ, dung lượng đĩa, tình trạng mạng, và các dịch vụ đang chạy trên máy chủ.

Việc giám sát hệ thống máy chủ là cực kỳ quan trọng vì nó mang lại nhiều lợi ích như sau:

Đảm bảo sự ổn định và hiệu suất: Theo dõi thông số kỹ thuật giúp nhận biết vấn đề sớm và giải quyết trước khi gây ra sự cố nghiêm trọng, từ đó tối ưu hóa hiệu suất của máy chủ.

Phát hiện sự cố và can thiệp kịp thời: Qua việc giám sát liên tục, người quản trị có thể nhận biết các dấu hiệu bất thường, từ đó có thể can thiệp kịp thời để ngăn chặn sự cố trước khi nó ảnh hưởng đến hoạt động của hệ thống.

Tối ưu hóa tài nguyên: Bằng cách theo dõi việc sử dụng tài nguyên như CPU, bộ nhớ, và lưu trữ, người quản trị có thể tối ưu hóa việc phân phối tài nguyên, tránh tình trạng lãng phí và đảm bảo hệ thống hoạt động hiệu quả.

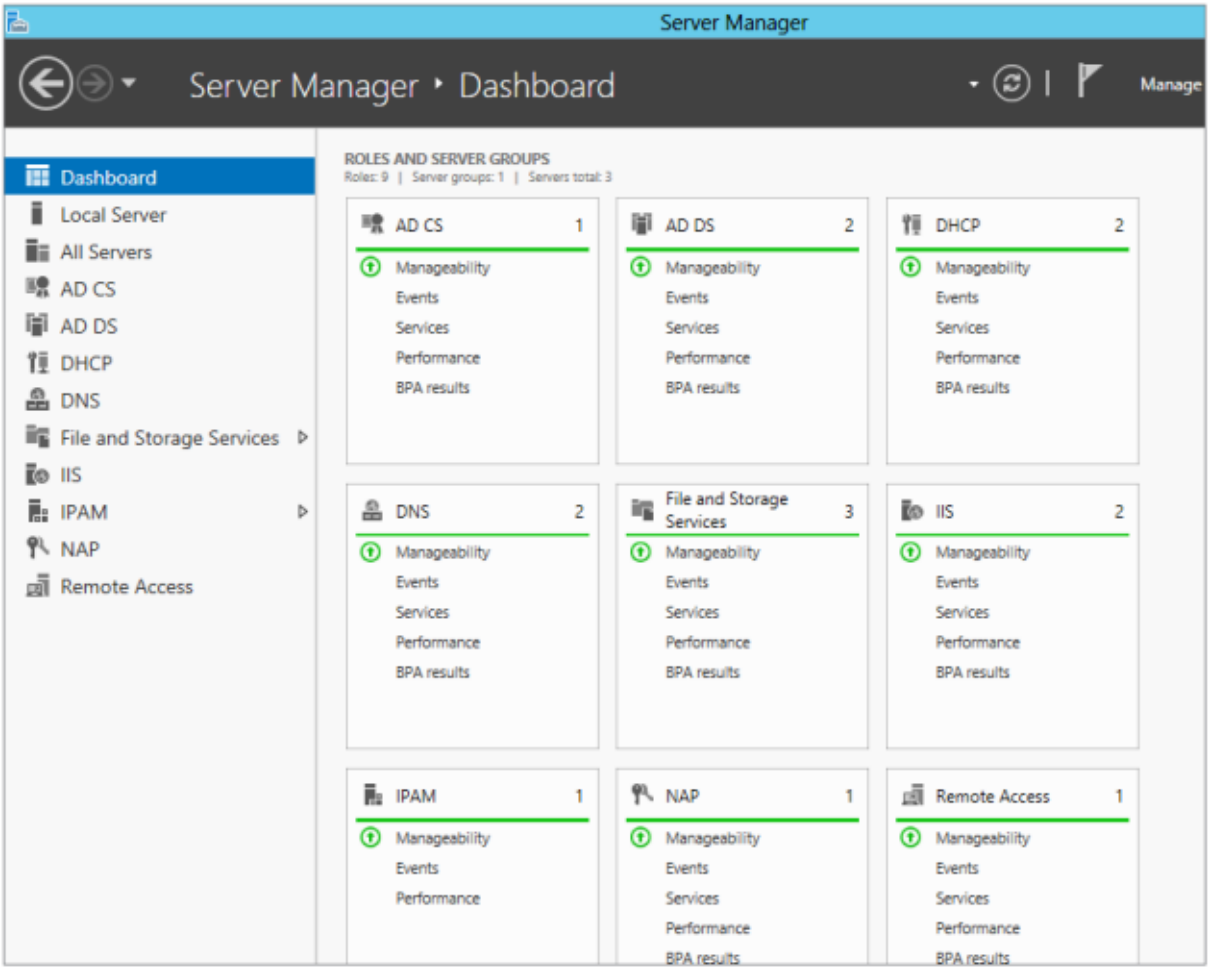
Bảo mật và tuân thủ quy định: Giám sát cũng giúp phát hiện các hành vi không đáng tin cậy hoặc tấn công từ bên ngoài, giúp tăng cường bảo mật hệ thống. Nó cũng có thể hỗ trợ việc tuân thủ các quy định bảo mật và chứng nhận.

Dự đoán và lập kế hoạch: Dữ liệu từ việc giám sát có thể được sử dụng để dự đoán xu hướng sử dụng tài nguyên, từ đó lập kế hoạch mở rộng hoặc nâng cấp hệ thống một cách có hệ thống và linh hoạt.

Trong chương này, chúng ta sẽ cùng tìm hiểu về các công cụ hoặc phương pháp hiệu quả để có thể giám sát hoạt động của hệ thống Windows Server. Các công cụ có thể kể đến như là: công cụ Server Manager, công cụ Best Practices Analyzer, Event View, Performance Monitor, Resource Monitor. Ngoài ra chúng ta cũng có thể sử dụng những công cụ đến từ bên thứ ba.

A, Sử dụng Server Manager để giám sát nhiều máy chủ

Server Manager là một công cụ tổng hợp cho phép quản trị rất nhiều khía cạnh trong các hệ thống máy chủ. Chúng ta cũng có thể sử dụng Server Manager để theo dõi trạng thái của nhiều máy chủ trong hệ thống cùng lúc. Chỉ đơn giản bằng việc truy cập vào Dashboard của Server Manager như hình ..



Hình 6-1 Server Manager Dashboard

Trong giao diện này, hệ thống đưa ra một vài tùy chọn chính để theo dõi cơ bản trong hệ thống. Cụ thể như sau:

Tùy chọn Manageability: Cung cấp những thông tin cơ bản về hệ thống và những lỗi nghiêm trọng đang tồn tại.

Tùy chọn Event: Một giao diện tập trung về các lỗi, lỗ hổng và cảnh báo sự kiện trong hệ thống.

Tùy chọn Services: Tổng quát về các dịch vụ đang chạy hoặc đang không chạy trong máy chủ.

Tùy chọn Performance: Cung cấp thông tin về hiệu suất hoạt động của phần cứng trong hệ thống.

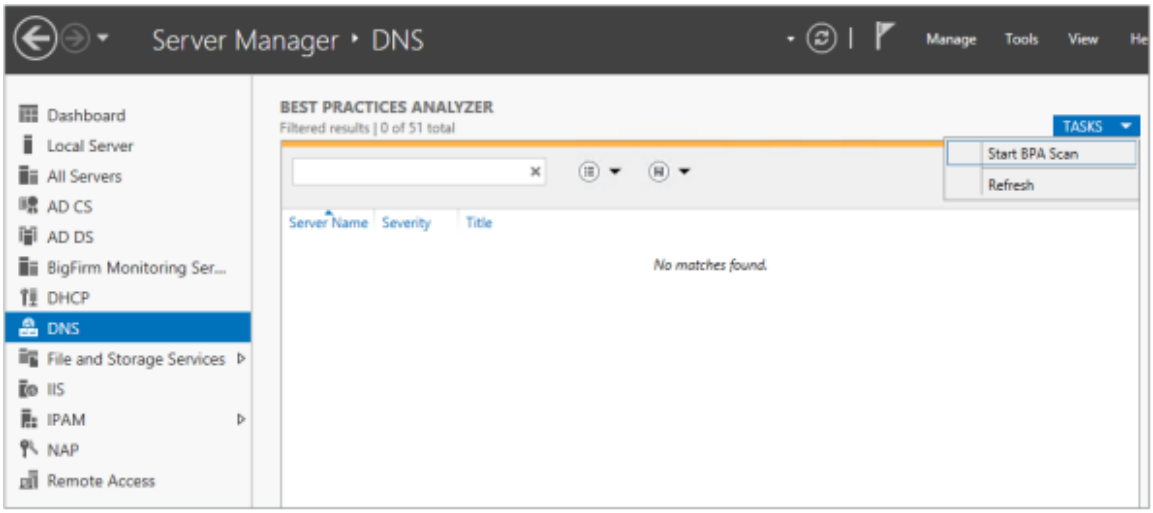
B, Sử dụng công cụ Best Practices Analyzer

Best Practices Analyzer (BPA) là một công cụ tích hợp trong Windows Server để kiểm tra cấu hình hệ thống và cung cấp các khuyến nghị về cách tối ưu hóa cài đặt. Nó giúp người quản trị hệ thống xác định và sửa các vấn đề tiềm ẩn, đánh giá tuân thủ các quy tắc và nguyên tắc tốt nhất (best practices) được đề xuất bởi Microsoft.

Công cụ BPA kiểm tra cấu hình của hệ thống, dịch vụ, ứng dụng và các vai trò cụ thể (ví dụ: Domain Controller, DNS Server, File Server, etc.) trong Windows Server. Sau đó, nó cung cấp các báo cáo chi tiết về việc tuân thủ các nguyên tắc tốt nhất và đưa ra các khuyến nghị để cải thiện hoặc điều chỉnh cài đặt để tối ưu hóa hiệu suất, bảo mật và sẵn sàng của hệ thống.

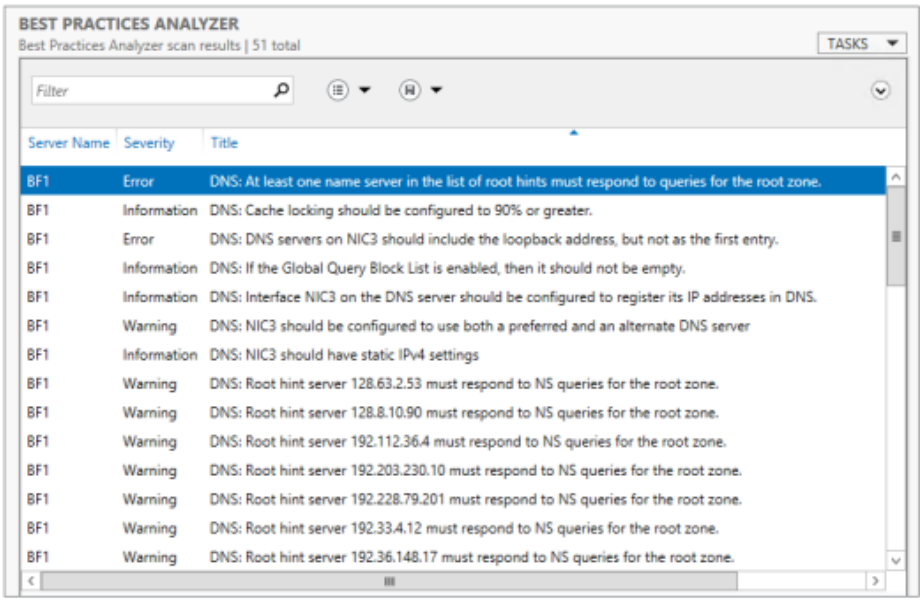
Công cụ này thường đi kèm với mỗi phiên bản Windows Server và có thể được chạy từ Giao diện người dùng hoặc thông qua PowerShell.

Chúng ta có thể khởi chạy BPA từ giao diện Server Manager như hình 6-2



Hình 6-2 Công cụ BPA

Sau khi công cụ dò quét tự động được thực thi, kết quả sẽ được hiển thị như hình .. từ đó người quản trị có thể dễ dàng nắm được các lỗi hoặc cảnh báo đang còn tồn tại trong hệ thống.



Hình 6-3 Kết quả BPA Scan

C, Giám sát hệ thống với công cụ Event Viewer

Event Viewer trong Windows Server 2012 R2 là một công cụ quan trọng giúp người quản trị hệ thống theo dõi, kiểm tra và phân tích các sự kiện và lỗi trên hệ thống. Được tích hợp sẵn trong Windows Server, Event Viewer cung cấp thông tin chi tiết về các sự kiện hệ thống, ứng dụng và bảo mật, giúp người dùng hiểu rõ hơn về hoạt động của máy chủ.

Các chức năng chính của Event Viewer bao gồm:

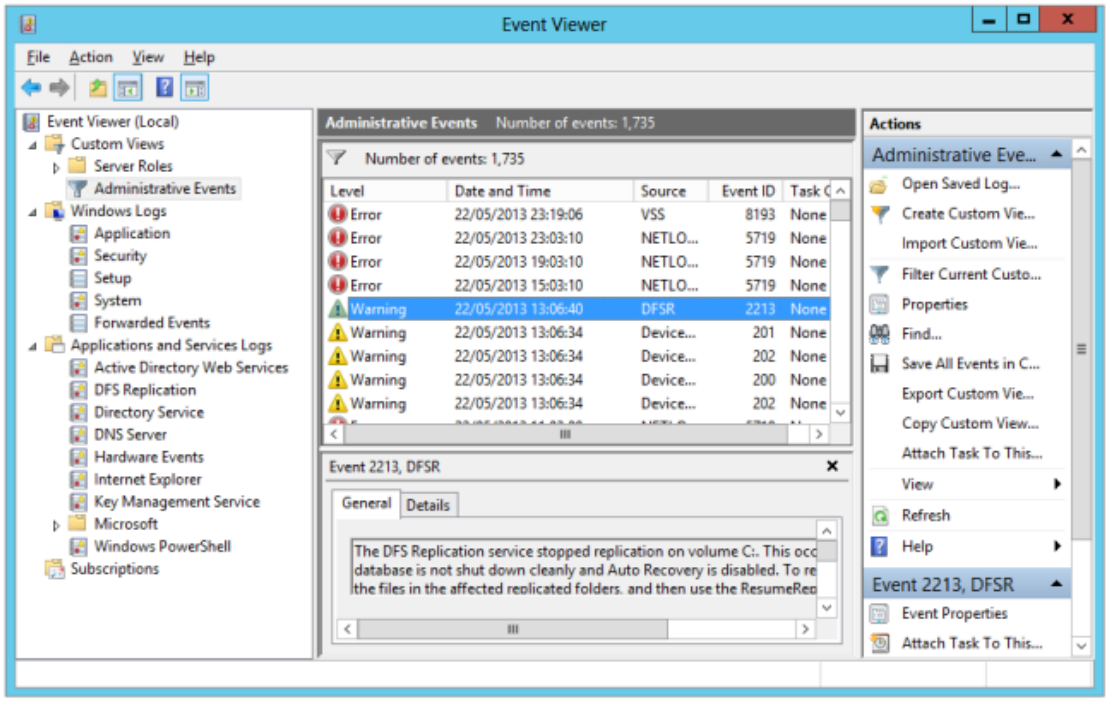
Xem và Quản lý Sự kiện: Hiển thị các sự kiện đã được ghi lại trên hệ thống, bao gồm thông tin về lỗi, cảnh báo, thông tin hoạt động, và sự kiện bảo mật. Người quản trị có thể lọc và tìm kiếm sự kiện theo loại, nguồn, thời gian và mức độ quan trọng.

Xác định Vấn đề và Đánh giá Tình trạng Hệ thống: Giúp xác định nguyên nhân của các sự cố hệ thống, từ đó cung cấp thông tin quan trọng để giải quyết vấn đề và cải thiện hiệu suất hệ thống.

Ghi nhận Sự kiện Quan trọng: Theo dõi các sự kiện quan trọng như lỗi ứng dụng, lưu lượng mạng, đăng nhập vào hệ thống, để bảo vệ và giám sát bảo mật.

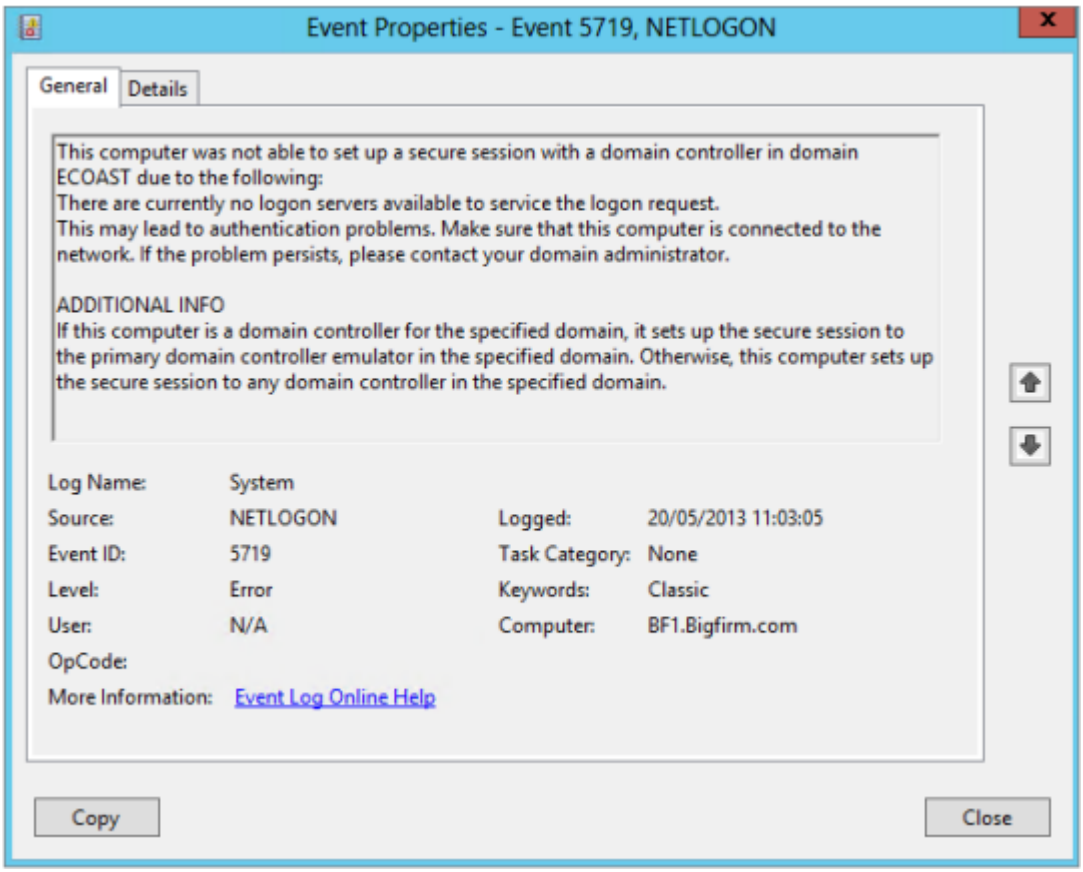
Tạo Báo cáo và Thống kê: Cung cấp khả năng tạo báo cáo và thống kê về các sự kiện và hoạt động của hệ thống, giúp hiểu rõ hơn về tình trạng hoạt động của máy chủ.

Chúng ta có thể khởi chạy Event Viewer từ màn hình Start của Windows Server 2012 R2 bằng cách nhập eventvwr và sau đó nhấn Enter hoặc thông qua Server Manager ➢ Tools ➢ Event Viewer. Giao diện của Event Viewer như hình 6-4.



Hình 6-4 Event Viewer

Khi người quản trị lựa chọn vào một sự kiện, sẽ có thể xem được chi tiết các thông tin được hệ thống ghi nhận cho sự kiện đó giống như hình 6-5. Ngoài ra, hệ thống còn cung cấp đường dẫn để thực hiện tra cứu trực tuyến, giúp người quản trị dễ dàng theo dõi và xử lý sự cố.



Hình 6-5 Chi tiết một Event trong hệ thống

6.2 Kiểm soát truy cập

6.2.1 Audit Policy

Thiết lập chính sách kiểm toán là một khía cạnh quan trọng của bảo mật. Giám sát việc tạo hoặc sửa đổi các đối tượng cung cấp cho chúng ta một cách để theo dõi các vấn đề bảo mật tiềm ẩn, giúp đảm bảo trách nhiệm giải trình của người dùng và cung cấp bằng chứng trong trường hợp vi phạm bảo mật.

Có chín loại sự kiện khác nhau mà chúng ta có thể kiểm tra. Nếu chúng ta kiểm tra bất kỳ loại sự kiện nào trong số này, Windows® sẽ ghi lại các sự kiện đó trong Nhật ký bảo mật mà chúng ta có thể tìm thấy trong Trình xem sự kiện.

Sự kiện đăng nhập tài khoản. Kiểm tra điều này để xem từng trường hợp người dùng đăng nhập hoặc đăng xuất khỏi một máy tính khác mà máy tính này được sử dụng để xác thực tài khoản. Các sự kiện đăng nhập tài khoản được tạo trong Nhật ký bảo mật của bộ điều khiển miền khi tài khoản người dùng miền được xác thực trên bộ điều khiển

miền. Các sự kiện này tách biệt với các sự kiện Logon, được tạo trong Nhật ký bảo mật cục bộ khi người dùng cục bộ được xác thực trên máy tính cục bộ. Các sự kiện đăng xuất tài khoản không được theo dõi trên bộ điều khiển miền.

Quản lý tài khoản. Kiểm tra điều này để xem khi ai đó đã thay đổi tên tài khoản, bật hoặc tắt tài khoản, tạo hoặc xóa tài khoản, thay đổi mật khẩu hoặc thay đổi nhóm người dùng.

Truy cập dịch vụ thư mục. Kiểm tra điều này để xem khi ai đó truy cập đối tượng dịch vụ thư mục Active Directory® có danh sách kiểm soát truy cập hệ thống (SACL) riêng.

Đăng nhập sự kiện. Kiểm tra điều này để xem khi ai đó đã đăng nhập hoặc tắt máy tính của chúng ta (trong khi thực tế trên máy tính của chúng ta hoặc bằng cách cố gắng đăng nhập qua mạng).

Quyền truy cập đối tượng. Kiểm tra điều này để xem khi ai đó đã sử dụng tệp, thư mục, máy in hoặc đối tượng khác. Mặc dù chúng ta cũng có thể kiểm tra các khóa sổ đăng ký, nhưng chúng tôi khuyên chúng ta không nên làm như vậy trừ khi chúng ta có kiến thức máy tính nâng cao và biết cách sử dụng sổ đăng ký.

Thay đổi chính sách. Kiểm tra điều này để xem các nỗ lực thay đổi chính sách bảo mật cục bộ và để xem liệu ai đó đã thay đổi việc chuyển nhượng quyền người dùng, chính sách kiểm tra hoặc chính sách tin cậy hay chưa.

Đặc quyền sử dụng. Kiểm tra điều này để xem khi ai đó thực hiện quyền người dùng.

Theo dõi quy trình. Kiểm tra điều này để xem khi nào xảy ra các sự kiện như kích hoạt chương trình hoặc thoát quy trình.

Sự kiện hệ thống. Kiểm tra điều này để xem khi ai đó đã tắt hoặc khởi động lại máy tính hoặc khi một quy trình hoặc chương trình cố gắng thực hiện điều gì đó mà nó không có quyền thực hiện. Ví dụ: nếu phần mềm độc hại cố gắng thay đổi cài đặt trên máy tính của chúng ta mà không có sự cho phép của chúng ta, kiểm tra sự kiện hệ thống sẽ ghi lại cài đặt đó.

Khi chúng ta thực hiện chính sách kiểm toán:

Chỉ định danh mục sự kiện mà chúng ta muốn kiểm tra. Các danh mục sự kiện mà chúng ta chọn cấu thành chính sách kiểm toán của chúng ta.

Đặt kích thước và hoạt động của Nhật ký bảo mật. Chúng ta có thể xem Nhật ký bảo mật bằng Trình xem sự kiện.

Nếu chúng ta muốn kiểm tra quyền truy cập dịch vụ thư mục hoặc quyền truy cập đối tượng, hãy xác định đối tượng nào chúng ta muốn kiểm tra quyền truy cập và loại quyền truy cập chúng ta muốn kiểm tra. Ví dụ: nếu chúng ta muốn kiểm tra bất kỳ nỗ

lực nào của người dùng để mở một tệp cụ thể, chúng ta có thể định cấu hình cài đặt chính sách kiểm tra trong danh mục sự kiện truy cập đối tượng để cả nỗ lực đọc tệp thành công và thất bại đều được ghi lại.

Nhật ký bảo mật ghi lại sự kiện kiểm tra bất cứ khi nào người dùng thực hiện các hành động cụ thể nhất định. Ví dụ: việc sửa đổi tệp hoặc chính sách có thể kích hoạt sự kiện hiển thị hành động đã được thực hiện, tài khoản người dùng được liên kết và ngày giờ của hành động. Những sự kiện này có thể là nỗ lực thực hiện hành động thành công và thất bại.

Các phân tích bảo mật thường xuyên cho phép quản trị viên theo dõi và xác định xem các biện pháp bảo mật thích hợp có hiệu lực đối với từng máy tính như một phần của chương trình quản lý rủi ro doanh nghiệp hay không. Các phân tích như vậy tập trung vào thông tin cụ thể cao về tất cả các khía cạnh của máy tính liên quan đến bảo mật, mà quản trị viên có thể sử dụng để điều chỉnh mức độ bảo mật. Quan trọng hơn, thông tin này có thể giúp phát hiện bất kỳ sơ suất bảo mật nào có thể xảy ra trong máy tính theo thời gian. Ví dụ: các cấp độ bảo mật có thể được thay đổi tạm thời để có thể giải quyết ngay lập tức sự cố quản trị hoặc mạng. Tuy nhiên, những thay đổi như vậy thường bị lãng quên và không bao giờ được hoàn tác. Nếu các cấp độ bảo mật không được đặt lại đúng cách, máy tính có thể không còn đáp ứng các yêu cầu về bảo mật doanh nghiệp.

Việc thiết lập và kích hoạt chính sách kiểm tra ghi lại các sai lệch so với chính sách bảo mật doanh nghiệp của chúng ta là cực kỳ quan trọng đối với bất kỳ mạng doanh nghiệp nào, vì nhật ký kiểm tra có thể cung cấp dấu hiệu duy nhất cho thấy đã xảy ra vi phạm bảo mật bằng cách ghi lại các thay đổi về quyền đối với tệp, cài đặt chương trình và báo cáo đặc quyền. Nếu vi phạm được phát hiện theo cách khác, cài đặt kiểm tra thích hợp có thể tạo nhật ký kiểm tra có thể chứa thông tin quan trọng về vi phạm, cách nó xảy ra và hệ thống nào bị ảnh hưởng.

Trong nhiều trường hợp, các sự kiện thất bại có nhiều thông tin hơn các sự kiện thành công vì các sự kiện thất bại thường chỉ ra lỗi. Ví dụ: người dùng đăng nhập thành công vào máy tính thường được coi là bình thường. Tuy nhiên, nếu ai đó cố gắng đăng nhập vào máy tính nhiều lần không thành công, điều đó có thể cho thấy kẻ tấn công cố gắng đột nhập vào máy tính bằng thông tin đăng nhập tài khoản của người khác. Mục Nhật ký sự kiện của Chính sách nhóm được sử dụng để xác định các thuộc tính liên quan đến nhật ký Ứng dụng, Bảo mật và Hệ thống, chẳng hạn như kích thước nhật ký tối đa, quyền truy cập cho từng nhật ký, cài đặt và phương pháp lưu giữ. Các sự kiện kiểm toán được lưu trữ trong Nhật ký sự kiện bảo mật. Để biết thêm thông tin về Nhật ký sự kiện, hãy xem phần Nhật ký sự kiện trong hướng dẫn này.

Trước khi thực hiện bất kỳ quy trình đánh giá nào, tổ chức phải xác định cách thức họ sẽ thu thập, tổ chức và phân tích dữ liệu. Sẽ có rất ít giá trị trong khối lượng lớn dữ liệu kiểm toán nếu không có kế hoạch cơ bản để sử dụng nó. Cũng cần lưu ý rằng cài đặt kiểm tra có thể ảnh hưởng đến hiệu suất máy tính. Ảnh hưởng của một tổ hợp cài đặt nhất định có thể không đáng kể trên máy tính người dùng cuối nhưng khá đáng chú ý trên một máy chủ bận. Do đó, chúng ta nên thực hiện một số kiểm tra hiệu suất trước khi triển khai cài đặt kiểm tra mới trong môi trường sản xuất của mình. Cân nhắc cuối cùng là dung lượng lưu trữ mà chúng ta có thể phân bổ để lưu trữ dữ liệu được thu thập trong quá trình kiểm tra. Tùy thuộc vào cài đặt chúng ta chọn, dữ liệu kiểm tra có thể tích lũy nhanh chóng và có thể lấp đầy dung lượng đĩa trống.

Chúng ta có thể định cấu hình cài đặt chính sách Kiểm tra ở vị trí sau trong Trình chỉnh sửa Đối tượng Chính sách Nhóm của Windows Server® 2003 hoặc Bảng Điều khiển Quản lý Chính sách Nhóm trong Windows Vista với Gói Dịch vụ 1 (SP1):

Cấu hình máy tính \ Cài đặt Windows \ Cài đặt bảo mật \ Chính sách cục bộ \ Chính sách kiểm tra

6.2.2 Cài đặt các chính sách giám sát và kiểm soát truy cập

Các lỗ hổng, biện pháp đối phó và tác động tiềm ẩn của tất cả các cài đặt kiểm tra là giống hệt nhau. Các tùy chọn cho từng cài đặt kiểm tra cũng giống hệt nhau:

- Trạng thái thành công. Sự kiện kiểm tra được tạo ra khi hành động được yêu cầu thành công.
- Trang thái thất bại. Một sự kiện kiểm tra được tạo ra khi hành động được yêu cầu không thành công.
- Không có Kiểm toán. Không có sự kiện kiểm tra nào được tạo cho hành động liên quan.

Tính dễ bị tổn thương

Nếu cài đặt kiểm tra không được định cấu hình, có thể khó hoặc không thể xác định điều gì đã xảy ra trong sự cố bảo mật. Tuy nhiên, nếu cài đặt kiểm tra được định cấu hình để các sự kiện được tạo cho tất cả các hoạt động, Nhật ký bảo mật sẽ chứa đầy dữ liệu và khó sử dụng. Ngoài ra, chúng ta có thể sử dụng một lượng lớn dung lượng lưu trữ dữ liệu cũng như ảnh hưởng xấu đến hiệu suất tổng thể của máy tính nếu chúng ta định cấu hình cài đặt kiểm tra cho một số lượng lớn các đối tượng.

Nếu sử dụng kiểm tra lỗi và Kiểm tra: Tắt hệ thống ngay lập tức nếu không thể ghi cài đặt kiểm tra bảo mật trong phần Tùy chọn bảo mật của Chính sách nhóm được bật, kẻ tấn công có thể tạo ra hàng triệu sự kiện thất bại, chẳng hạn như lỗi đăng nhập để điền vào Nhật ký bảo mật và buộc máy tính phải tắt, tạo ra từ chối dịch vụ (DoS).

Nếu nhật ký bảo mật được phép ghi đè, kẻ tấn công có thể ghi đè một phần hoặc toàn bộ hoạt động của chúng bằng cách tạo ra một số lượng lớn các sự kiện để bằng chứng về sự xâm nhập của chúng bị ghi đè.

Biện pháp đối phó

Bật cài đặt chính sách Kiểm tra hỗ trợ chính sách bảo mật của tổ chức cho tất cả các máy tính trong tổ chức của chúng ta. Xác định các thành phần mà chúng ta cần cho một chính sách kiểm toán cho phép tổ chức của chúng ta quy trách nhiệm cho người dùng về các hành động của họ trong khi sử dụng tài nguyên của tổ chức và cho phép các bộ phận CNTT phát hiện hoạt động trái phép một cách hiệu quả và sau đó theo dõi các sự kiện đó trong các tệp nhật ký.

Tác động tiềm tàng

Nếu không có cài đặt kiểm tra nào được định cấu hình hoặc nếu cài đặt kiểm tra quá lỏng lẻo trên các máy tính trong tổ chức của chúng ta, các sự cố bảo mật có thể không được phát hiện hoặc không có đủ bằng chứng để phân tích pháp y mạng sau khi sự cố bảo mật xảy ra. Tuy nhiên, nếu cài đặt kiểm tra quá chi tiết, các mục nhập cực kỳ quan trọng trong Nhật ký bảo mật có thể bị che khuất bởi số lượng lớn mục nhập nhật ký được tạo bởi các hoạt động thông thường và hiệu suất máy tính, đồng thời dung lượng lưu trữ dữ liệu có sẵn có thể bị ảnh hưởng nghiêm trọng. Các công ty hoạt động trong một số ngành được quản lý nhất định có thể có nghĩa vụ pháp lý để ghi lại các sự kiện hoặc hoạt động nhất định.

Kiểm tra sự kiện đăng nhập tài khoản

Cài đặt chính sách này cho phép kiểm tra từng trường hợp đăng nhập hoặc đăng xuất của người dùng trên một máy tính khác với máy tính ghi lại sự kiện và xác thực tài khoản. Kiểm toán thành công cung cấp thông tin hữu ích cho mục đích kế toán và pháp y sau sự cố để chúng ta có thể xác định ai đã đăng nhập thành công vào máy tính nào.

Kiểm tra thất bại rất hữu ích cho việc phát hiện xâm nhập. Tuy nhiên, cấu hình này của thiết lập chính sách cũng tạo ra khả năng tấn công DoS. Khi Kiểm tra: Tắt hệ thống ngay lập tức nếu không thể ghi lại cài đặt kiểm tra bảo mật trong phần Tùy chọn bảo mật của Chính sách nhóm cũng được bật, kẻ tấn công có thể tạo ra hàng triệu lần đăng nhập thất bại để điền vào Nhật ký bảo mật và buộc máy tính phải tắt .

Nếu chúng ta định cấu hình cài đặt sự kiện đăng nhập tài khoản Kiểm tra thành Thành công trên bộ điều khiển miền, thì một sự kiện sẽ được ghi lại cho từng người dùng được xác thực dựa trên bộ điều khiển miền đó, ngay cả khi người dùng thực sự đăng nhập vào một máy trạm hoặc máy chủ được tham gia vào miền.

Theo mặc định, các sự kiện đăng nhập Auditaccount được đặt thành Thành công.

Kiểm toán quản lý tài khoản

Cài đặt chính sách này cho phép kiểm tra từng sự kiện quản lý tài khoản trên máy tính. Ví dụ về các sự kiện quản lý tài khoản bao gồm:

Tài khoản hoặc nhóm người dùng được tạo, thay đổi hoặc xóa.

Tài khoản người dùng được đổi tên, vô hiệu hóa hoặc kích hoạt.

Mật khẩu được đặt hoặc thay đổi.

Đánh giá thành công nên được kích hoạt trên tất cả các máy tính trong doanh nghiệp của chúng ta. Khi một tổ chức phản ứng với các sự cố bảo mật, điều quan trọng là họ có thể theo dõi ai đã tạo, thay đổi hoặc xóa tài khoản. Kiểm tra không thành công tạo ra một sự kiện khi bất kỳ hành động quản lý tài khoản nào không thành công.

Kiểm tra quyền truy cập dịch vụ thư mục

Cài đặt chính sách này cho phép kiểm tra quyền truy cập của người dùng vào một đối tượng Active Directory có SACL được liên kết. SACL là danh sách người dùng và nhóm mà các hành động trên một đối tượng sẽ được kiểm tra trên mạng dựa trên Windows.

Kiểm tra thành công tạo ra một sự kiện khi người dùng truy cập thành công đối tượng Active Directory có SACL chỉ ra rằng người dùng cần được kiểm tra cho hành động được yêu cầu. Kiểm tra thất bại tạo ra một sự kiện cho mỗi lần thử không thành công. (Cả hai loại sự kiện đều được tạo trước khi người dùng được thông báo rằng yêu cầu thành công hay không thành công.) Nếu chúng ta bật cài đặt chính sách này và định cấu hình SACL trên các đối tượng thư mục, một lượng lớn các mục nhập có thể được tạo trong Nhật ký bảo mật trên bộ điều khiển miền. Chúng ta chỉ nên bật các cài đặt này nếu chúng ta thực sự có ý định sử dụng thông tin được tạo.

Kiểm tra sự kiện đăng nhập

Cài đặt chính sách này cho phép kiểm tra từng trường hợp đăng nhập, đăng xuất của người dùng hoặc kết nối mạng với máy tính ghi lại sự kiện. Nếu chúng ta ghi các sự kiện đăng nhập tài khoản thành công trên bộ điều khiển miền, các nỗ lực đăng nhập máy trạm không tạo ra các sự kiện đăng nhập. Chỉ những nỗ lực đăng nhập mạng và tương tác vào bộ điều khiển miền mới tạo ra các sự kiện đăng nhập trên bộ điều khiển miền. Tóm lại, "sự kiện đăng nhập tài khoản" được tạo khi tài khoản tồn tại, trên bộ điều khiển miền nếu tài khoản là tài khoản miền hoặc trên máy tính cục bộ nếu tài khoản là tài khoản máy tính cục bộ và "sự kiện đăng nhập" được tạo trên máy tính nơi người dùng đang đăng nhập hoặc tắt.

Kiểm toán thành công cung cấp thông tin hữu ích cho mục đích rà soát và điều tra sau sự cố để chúng ta có thể xác định ai đã đăng nhập thành công vào máy tính nào. Kiểm tra thất bại rất hữu ích cho việc phát hiện xâm nhập. Tuy nhiên, cấu hình của các sự kiện thất bại cũng tạo ra một điều kiện DoS tiềm ẩn. Khi Kiểm tra: Tắt hệ thống ngay

lập tức nếu không thể ghi lại cài đặt kiểm tra bảo mật trong phần Tùy chọn bảo mật của Chính sách nhóm cũng được bật, kẻ tấn công có thể tạo ra hàng triệu lần đăng nhập thất bại để điền vào Nhật ký bảo mật và buộc máy chủ phải tắt .

Quyền truy cập đối tượng kiểm tra

Cài đặt chính sách này cho phép kiểm tra sự kiện được tạo bởi người dùng truy cập một đối tượng — ví dụ: tệp, thư mục, khóa đăng ký hoặc máy in — có SACL chỉ định yêu cầu kiểm tra.

Kiểm tra thành công tạo ra một sự kiện khi người dùng truy cập thành công một đối tượng có SACL. Kiểm tra thất bại tạo ra một sự kiện cho mỗi lần thử không thành công (một số sự kiện hỏng hóc sẽ xảy ra trong quá trình hoạt động bình thường của máy tính). Ví dụ, nhiều ứng dụng (chẳng hạn như Microsoft Word) luôn cố gắng mở tệp với cả đặc quyền đọc và ghi. Nếu các ứng dụng không thể làm như vậy, thì chúng sẽ cố gắng mở các tệp bằng đặc quyền chỉ đọc. Nếu chúng ta bật kiểm tra lỗi và SACL thích hợp trên tệp, sự kiện lỗi sẽ được ghi lại khi sự kiện đó xảy ra.

Trong Windows Server 2003 với Gói Dịch vụ 1 (SP1), chúng ta có thể kiểm tra quyền truy cập vào các đối tượng được lưu trữ trong siêu dữ liệu Dịch vụ Thông tin Internet (IIS). Để bật kiểm tra đối tượng siêu dữ liệu, chúng ta phải bật quyền truy cập đối tượng Kiểm tra trên máy tính mục tiêu, sau đó đặt SACL trên các đối tượng siêu dữ liệu cụ thể có quyền truy cập mà chúng ta muốn kiểm tra.

Nếu chúng ta định cấu hình cài đặt chính sách truy cập đối tượng Kiểm tra và định cấu hình SACL trên các đối tượng, thì một lượng lớn các mục nhập có thể được tạo trong Nhật ký bảo mật trên máy tính trong tổ chức của chúng ta. Do đó, chúng ta chỉ nên bật các cài đặt này nếu chúng ta thực sự có ý định sử dụng thông tin được ghi lại.

Thay đổi chính sách kiểm toán

Cài đặt chính sách này cho phép kiểm tra mọi tỷ lệ thay đổi đối với chính sách chuyển nhượng quyền người dùng, chính sách Tường lửa của Windows, chính sách Kiểm tra hoặc chính sách tin cậy.

Kiểm tra thành công rất hữu ích cho mục đích kế toán và có thể giúp chúng ta xác định ai đã sửa đổi thành công các chính sách trong miền hoặc trên từng máy tính. Đánh giá thất bại tạo ra một sự kiện khi một thay đổi đối với chính sách chuyển nhượng quyền người dùng, chính sách Đánh giá hoặc chính sách tin cậy không thành công.

Nếu chúng ta bật cài đặt thay đổi chính sách Kiểm tra trong Windows Vista và Windows Server 2003 với SP1, thì việc ghi nhật ký các thay đổi cấu hình cho thành phần Tường lửa của Windows cũng được bật.

Sử dụng đặc quyền kiểm tra

Cài đặt chính sách này cho phép kiểm tra từng trường hợp của người dùng thực hiện quyền người dùng.

Đánh giá thành công tạo ra một sự kiện khi việc thực thi quyền của người dùng thành công. Đánh giá thất bại tạo ra một sự kiện cho một bài tập không thành công. Nếu chúng ta bật cài đặt chính sách này, khối lượng sự kiện được tạo có thể rất lớn và cồng kềnh. Chúng ta chỉ nên bật cài đặt này nếu chúng ta định sử dụng thông tin được tạo.

Các sự kiện đánh giá không được tạo để sử dụng các quyền của người dùng sau, ngay cả khi đánh giá thành công hoặc đánh giá thất bại được chỉ định cho cài đặt chính sách sử dụng đặc quyền Đánh giá:

Bỏ qua kiểm tra ngang

Chương trình gỡ lỗi

Tạo một đối tượng mã thông báo

Thay thế mã thông báo cấp quy trình

Tạo kiểm tra bảo mật

Sao lưu tệp và thư mục

Khôi phục tệp và thư mục

Theo dõi quá trình kiểm tra

Cài đặt chính sách này cho phép kiểm tra thông tin theo dõi chi tiết cho các sự kiện như kích hoạt chương trình, thoát quy trình, xử lý trùng lặp và truy cập đối tượng gián tiếp.

Đánh giá thành công tạo ra một sự kiện khi quá trình được theo dõi thành công. Đánh giá thất bại tạo ra một sự kiện khi quá trình không thành công.

Nếu chúng ta bật theo dõi quá trình Kiểm tra trong Windows Vista và Windows Server 2003 với SP1, Windows cũng sẽ ghi lại thông tin về chế độ hoạt động và trạng thái của cấu phần Tường lửa của Windows.

Khi được bật, cài đặt theo dõi quy trình Kiểm tra sẽ tạo ra một số lượng lớn các sự kiện. Cài đặt chính sách này thường được định cấu hình thành Không kiểm tra. Tuy nhiên, thông tin mà thiết lập chính sách này tạo ra có thể rất hữu ích trong quá trình ứng phó sự cố vì nó cung cấp nhật ký chi tiết về các quá trình đã được bắt đầu và khi chúng được bắt đầu.

Sự kiện hệ thống kiểm tra

Cài đặt chính sách này cho phép kiểm tra việc khởi động lại hoặc tắt máy tính của người dùng hoặc các sự kiện ảnh hưởng đến bảo mật máy tính hoặc Nhật ký bảo mật.

Kiểm tra thành công tạo ra một sự kiện khi một sự kiện chạy thành công. Kiểm toán thất bại tạo ra một sự kiện khi một sự kiện không thành công.

Bởi vì một số sự kiện bổ sung được ghi lại nếu cả kiểm tra thất bại và thành công đều được bật cho các sự kiện hệ thống và bởi vì tất cả các sự kiện như vậy đều rất quan trọng, chúng ta nên định cấu hình cài đặt chính sách này thành Bật trên tất cả các máy tính trong tổ chức của mình.

CHƯƠNG 7 SAO LƯU VÀ KHÔI PHỤC DỮ LIỆU

7.1 Sao lưu và khôi phục dữ liệu sử dụng windows server backup

Từ Windows Server 2008, công cụ NTBackup không còn được Windows hỗ trợ mà thay vào đó là Windows Server Backup. Windows Server Backup là công cụ sao lưu và phục hồi dữ liệu được Microsoft phát triển mới hoàn toàn với cơ chế hoạt động và nhiều tính năng rất khác biệt so với "người tiền nhiệm" NTBackup.

Xét về khả năng sao lưu, Windows Server Backup là công cụ khá mạnh mẽ bởi nó hỗ trợ sao lưu nhiều dạng dữ liệu:

- Full server (All volume): Sao lưu tất cả các volume của server.
- Selected volume: Sao lưu một volume xác định.
- System state: Sao lưu dữ liệu System state của Windows (bao gồm Active Directory).
- File/Folder: Sao lưu dữ liệu dạng file/folder.
- Bare-metal recovery: Tạo bản sao lưu để phục hồi Bare-metal.

Chúng ta có thể sử dụng Windows Server Backup để sao lưu dữ liệu của Local server hoặc Remote server. Windows Server Backup hỗ trợ chạy thủ công một lần (One-time Backup) hoặc chạy tự động theo lịch sao lưu (Schedule Backup). Về giao diện, Windows Server Backup hỗ trợ 3 giao diện là MMC Snap-in, Command-line và Windows PowerShell.

Một số điểm khác nhau của Windows Server Backup so với NTBackup

Windows Server Backup là tính năng được Microsoft phát triển mới hoàn toàn với một số thay đổi trong quan điểm thiết kế so với NTBackup. Do đó, công cụ này có một số điểm khác biệt đáng lưu ý sau:

1. Không hỗ trợ Tape

Windows Server Backup hoàn toàn không hỗ trợ thiết bị Tape. Chúng ta không thể đọc/ghi dữ liệu từ Windows Server Backup từ/xuống Tape. Theo quan điểm của Microsoft thì Tape đang đi theo con đường của Floppy-disk bởi thiết bị lưu trữ Disk ngày càng rẻ trong khi sử dụng lại đơn giản hơn nhiều. Vì thế, Microsoft chỉ hỗ trợ thiết bị lưu trữ Disk hoặc DVD với Windows Server Backup. Vì thế, những doanh nghiệp khi nâng cấp lên Windows Server 2008 chắc chắn phải từ bỏ thiết bị Tape đang có hoặc phải tìm kiếm một giải pháp sao lưu khác có hỗ trợ Tape. Điều này gây ra không ít bất tiện và lãng phí.

Mặc dù chúng ta Windows Server Backup không hỗ trợ Tape nhưng Microsoft có cung cấp một phiên bản NTBackup với Windows Server 2008 có thể sử dụng để phục hồi các dữ liệu sao lưu vào Tape trước đó (gọi là Restore-only NTBackup –

http://www.microsoft.com/en-us/download/details.aspx?id=4220). Nhờ đó, chúng ta có thể phục hồi dữ liệu đã được sao lưu vào Tape bằng NTBackup.

Lưu ý là chúng ta có thể phục hồi dữ liệu từ Tape với phiên bản NTBackup này, nhưng không thể ghi dữ liệu vào nó. Để sử dụng phiên bản NTBackup này trên Windows Server 2008, chúng ta cần tìm đúng driver cho Tape drive sử dụng. Vì Microsoft không hỗ trợ Tape nữa nên nhiều nhà sản xuất Tape không cũng không cung cấp driver cho Windows Server 2008.

2. Sao lưu dạng Block-level

Thay vì sao lưu theo cơ chế File-level như NTBackup, Windows Server Backup sử dụng cơ chế Block-level. Với cơ chế này, Windows Server Backup chỉ sao lưu những block dữ liệu thay đổi trong file chứ không sao lưu toàn bộ file. Bên cạnh đó, Windows Server Backup xử lý dữ liệu ở cấp độ Image-base nên không phải mất thời gian cho các thao tác mở/đóng từng file như với NTBackup. Nhờ vậy, so với NTBackup thì Windows Server Backup sao lưu nhanh và tốn ít dung lượng hơn.

Bên cạnh cách thức sao chép dữ liệu, Windows Server Backup còn thay đổi cách thức quản lý các block dữ liệu của mỗi lần sao lưu. Nhờ đó, khi phục hồi chúng ta không cần thực hiện phục hồi bản Full backup và nhiều bản Incremental backup sau đó mà chỉ cần lựa chọn phiên bản cần phục hồi (bởi các bản sao lưu đều là bản Full backup).

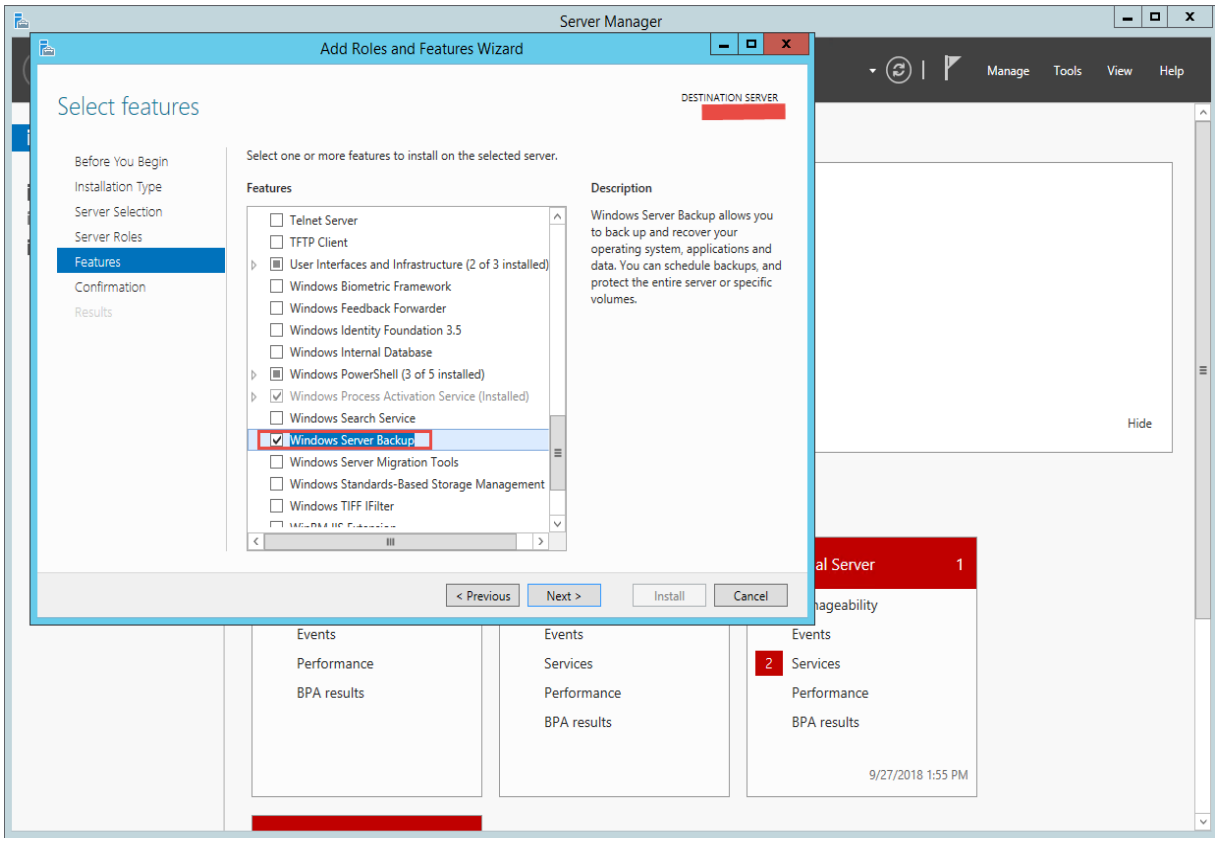
3. Tự động quản lý dung lượng

Điểm mạnh của Windows Server Backup là khả năng tự quản lý dung lượng vùng lưu trữ chứa file sao lưu. Khi vùng lưu trữ bị đầy, Window Server Backup sẽ tự động xóa phiên bản cũ để giải phóng dung lượng cho phiên bản mới. Quá trình này diễn ra hoàn toàn tự động mà chúng ta không cần phải thao tác.

Mặc định không được cài đặt sẵn: Windows Server Backup không được cài đặt sẵn trong Windows như NTBackup. Thay vào đó, chúng ta cần sử dụng công cụ Add roles and features trong Server Manager để cài đặt tính năng này. Windows hoàn toàn không cảnh báo gì về việc chúng ta đã cài đặt hay sao lưu dữ liệu chưa. Do đó, tốt nhất chúng ta nên cài đặt Windows Server Backup ngay sau khi cài đặt Windows. Và cấu hình để sao lưu ngay sau đó. Tránh để tình trạng mất dữ liệu xảy ra rồi khi đó mới cuống cuồng lo chuyện sao lưu.

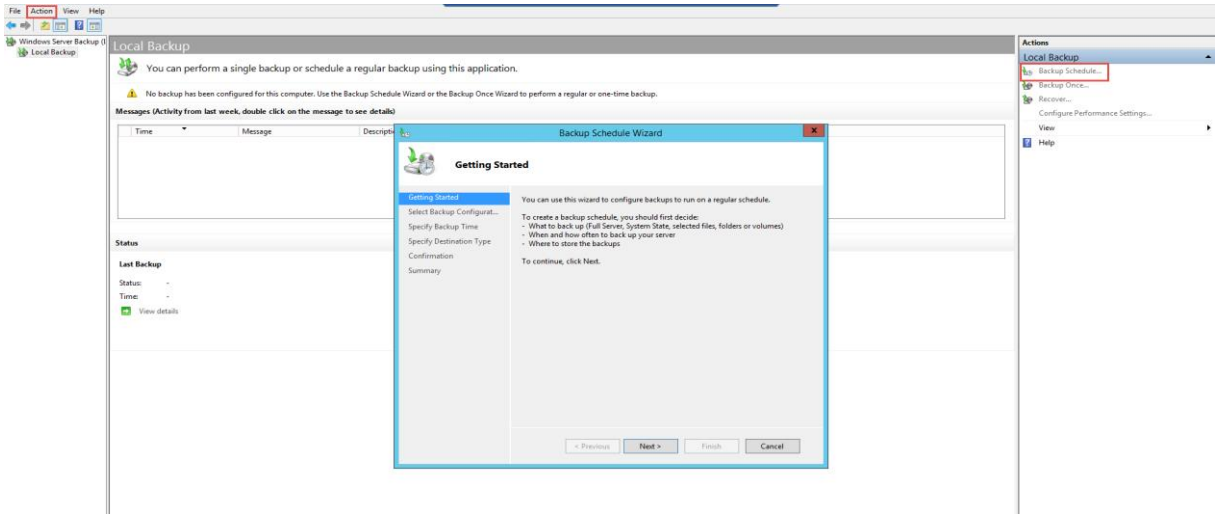
Một số thao tác với Windows Server Backup:

Bước 1: Cài đặt Features Windows Server Backup. Hình 7-1.



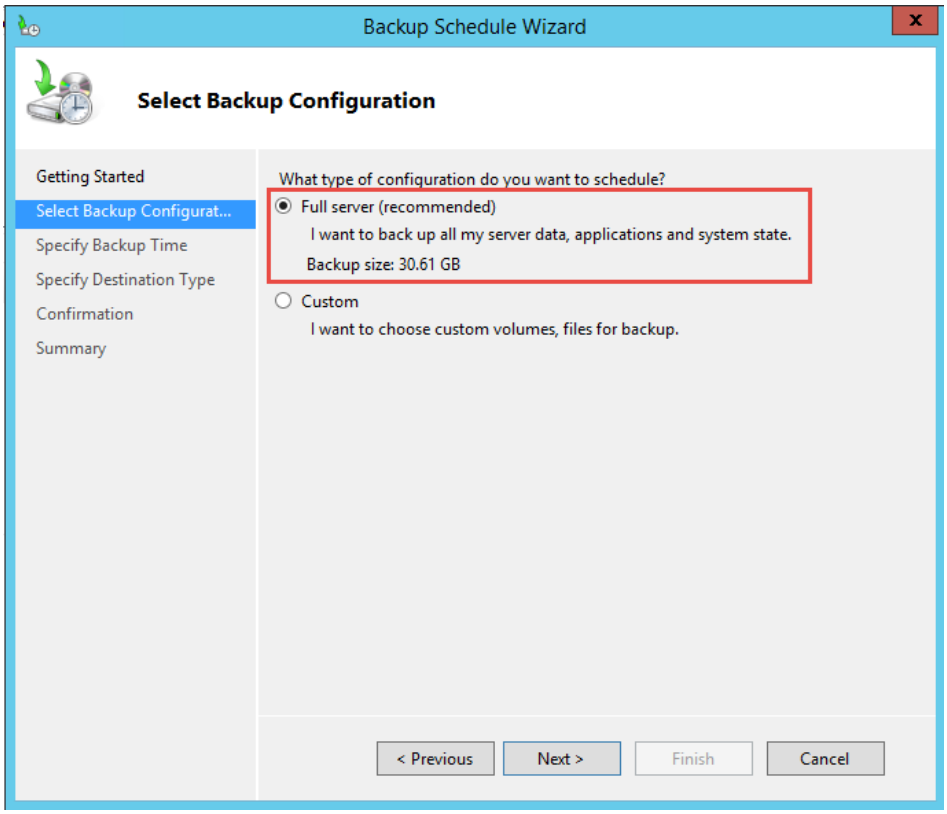
Hình 7-1 Cài đặt tính năng sao lưu dữ liệu

Bước 2: Khởi tạo kế hoạch sao lưu dữ liệu



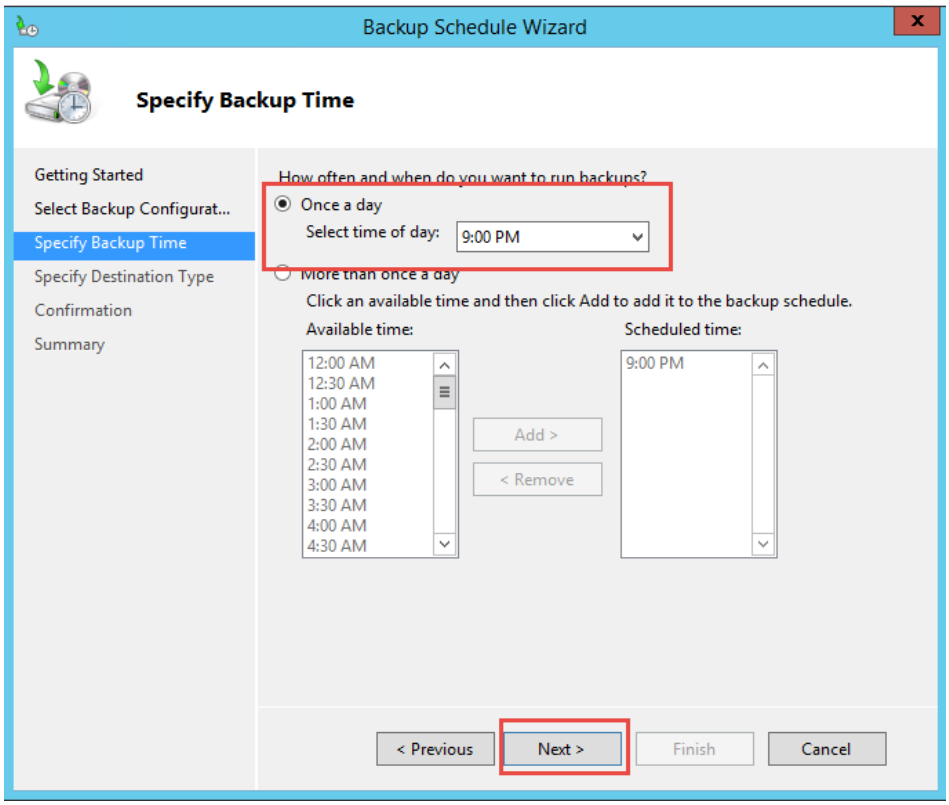
Hình 7-2 Khởi tạo lịch biểu sao lưu

Bước 3: Cấu hình lịch biểu sao lưu và lựa chọn kiểu sao lưu



Hình 7-3 Cấu hình sao lưu dữ liệu

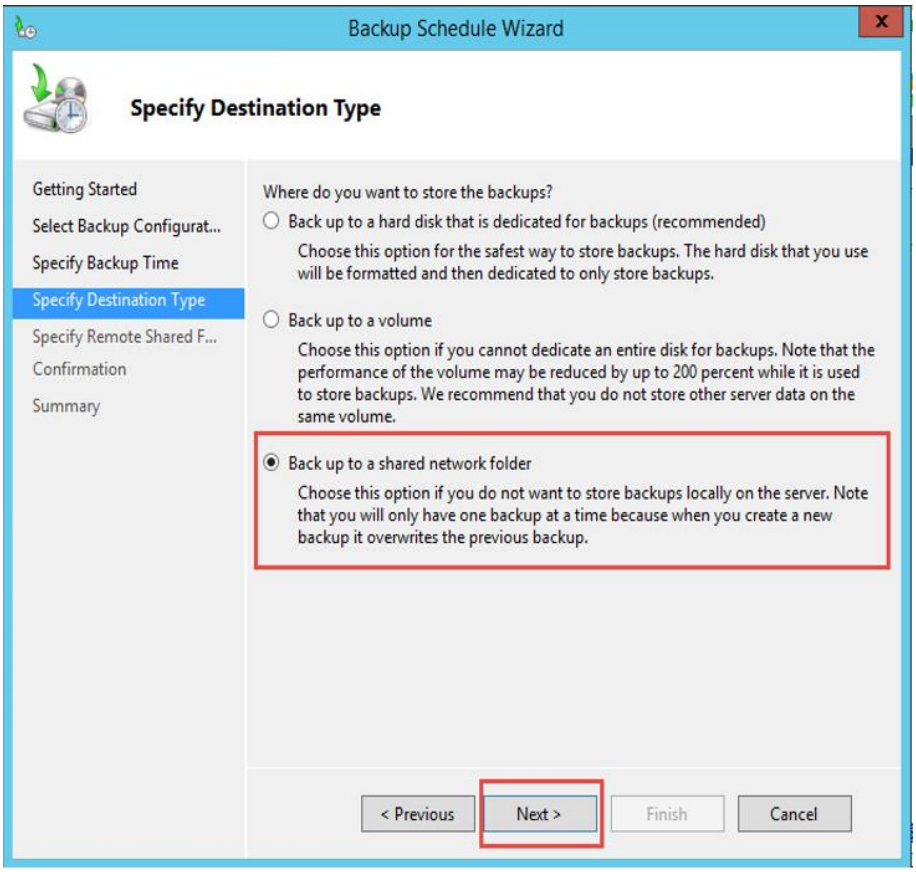
Người quản trị có thể lựa chọn sao lưu toàn bộ máy chủ hoặc chỉ sao lưu một phần.



Hình 7-4 Cấu hình thời gian thực hiện sao lưu

Có thể cấu hình thực hiện việc sao lưu một lần trong một ngày hoặc nhiều lần trong ngày.

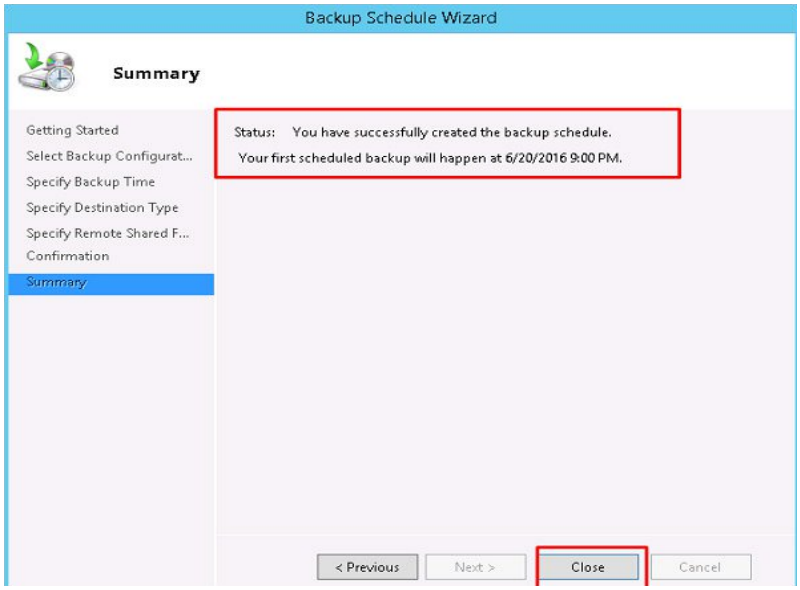
Bước 4: Lựa chọn vị trí lưu dữ liệu



Hình 7-5 Lựa chọn vị trí lưu bản sao

Có thể sao lưu vào một ổ đĩa vật lý, một ổ đĩa logic hoặc một ổ đĩa trên mạng.

Bước 5: Hoàn thành việc sao lưu



Hình 7-6 Hoàn thành sao lưu

7.2 Các giải pháp sao lưu và khôi phục dữ liệu khác

Tự động sao lưu và phục hồi dữ liệu trên máy chủ Windows Server là một phần quan trọng của việc bảo vệ và duy trì tính ổn định cho môi trường doanh nghiệp. Dưới đây là một số phần mềm chuyên dụng được thiết kế để cung cấp giải pháp sao lưu và phục hồi dữ liệu mạnh mẽ cho máy chủ Windows Server:

Acronis Backup: Acronis Backup đã lâu được biết đến là một trong những phần mềm hàng đầu trong lĩnh vực sao lưu và phục hồi dữ liệu. Với khả năng tạo bản sao lưu toàn bộ hệ thống, dữ liệu và ứng dụng, Acronis Backup cung cấp một giải pháp toàn diện để bảo vệ máy chủ Windows Server của bạn. Nó hỗ trợ nhiều phương pháp sao lưu như sao lưu máy ảo, sao lưu trực tiếp lên các dịch vụ đám mây phổ biến và khả năng phục hồi linh hoạt.

Veritas Backup Exec: Đối với môi trường doanh nghiệp, Veritas Backup Exec là một lựa chọn đáng cân nhắc. Với tích hợp đa nền tảng, phần mềm này cho phép sao lưu dữ liệu trên các hệ điều hành khác nhau và ứng dụng đa dạng. Veritas Backup Exec cung cấp khả năng sao lưu và phục hồi dữ liệu trên môi trường Windows Server một cách hiệu quả, bổ sung thêm tích hợp với các giải pháp đám mây.

Veeam Backup & Replication: Dành cho môi trường ảo hóa, Veeam Backup & Replication đã chứng tỏ khả năng mạnh mẽ trong việc sao lưu và phục hồi máy chủ Windows Server chạy trên nền tảng VMware và Hyper-V. Với khả năng sao lưu liên tục, nén dữ liệu thông minh và tích hợp với các dịch vụ đám mây lớn, Veeam đem lại hiệu suất cao và tính linh hoạt trong việc bảo vệ dữ liệu.

Symantec System Recovery: Symantec System Recovery cung cấp một phương pháp toàn diện để tạo sao lưu hệ thống và phục hồi dữ liệu trên máy chủ Windows. Khả năng sao lưu trực tiếp lên các ổ đĩa cục bộ và lưu trữ đám mây giúp đảm bảo sự an toàn cho dữ liệu của bạn.

BackupAssist: Được thiết kế cho sự đa dạng trong việc sao lưu dữ liệu, BackupAssist cung cấp nhiều tính năng bảo vệ, bao gồm sao lưu toàn bộ hệ thống và dữ liệu cơ sở dữ liệu. Khả năng sao lưu lên các dịch vụ đám mây phổ biến như Amazon S3 và Microsoft Azure giúp bạn duy trì dữ liệu an toàn và dễ dàng phục hồi.

Tất cả những phần mềm trên đều đem lại sự linh hoạt và khả năng tùy chỉnh để chúng ta có thể lựa chọn giải pháp sao lưu và phục hồi dữ liệu phù hợp với nhu cầu cụ thể của máy chủ Windows Server. Trước khi quyết định, hãy xem xét cẩn thận các tính năng, tích hợp với hạ tầng hiện có và khả năng hỗ trợ kỹ thuật để đảm bảo rằng chúng ta đã chọn lựa đúng phần mềm.

TÀI LIỆU THAM KHẢO

[1] Brian Desmond, Joe Richards, Robbie Allen, and Alistair G. Lowe-Norris, *Active Directory – Fifth Edition*, O'REILLY, 2013.

[2] Mark Minasi Kevin Greene Christian Booth Robert Butler John McCabe Robert Panek Michael Rice Stefan Roth, *Mastering Windows Server 2012*, SYBEX, 2014.

[3]. Mitch Tulloch, *Training Guide Installing and Configuring Windows Server 2012 R2*, Microsoft Press,2014.

[4]. Mitch Tulloch, *Introducing Windows Server 2012 R2*, Microsoft Press, 2013.

[5]. Microsoft System Center Team, *Introducing Microsoft System Center 2012 R2*, Microsoft Press, 2014.