HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA CÔNG NGHỆ THÔNG TIN

ĐỀ TÀI THỰC TẬP CƠ SỞ

QUẢN TRỊ TRÊN WINDOW SERVER 2008

Giáo viên hướng dẫn: Nguyễn Văn Phác

Sinh viên thực hiện:

- Lê Thị Bích Hằng
- Trần Thế Linh
- Phan Thị Thúy An
- Vũ Đình Bắc

HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA CÔNG NGHỆ THÔNG TIN

ĐỀ TÀI THỰC TẬP CƠ SỞ

QUẢN TRỊ TRÊN WINDOWS SERVER 2008

Nhận xét của giảng viên hướng dẫn:.....

.....

.....

.....

.....

.....

.....

Điểm chuyên cần của nhóm:.....

Điểm chấm kết quả bản in hoàn chỉnh của báo cáo thực tập.....

MỤC LỤC

LỜI NÓI ĐẦU

Microsoft Windows Server 2008 là thế hệ kế tiếp của hệ điều hành Windows Server, có thể giúp các chuyên gia công nghệ thông tin có thể kiểm soát tối đa cơ sở hạ tầng của họ và cung cấp khả năng quản lý và hiệu lực chưa từng có, là sản phẩm hơn hẳn trong việc đảm bảo độ an toàn, khả năng tin cậy và môi trường máy chủ vững chắc hơn các phiên bản trước đây. Windows Server 2008 cung cấp những giá trị mới cho các tổ chức bằng việc bảo đảm tất cả người dùng đều có thể có được những thành phần bổ sung từ các dịch vụ từ mạng. Windows Server 2008 cũng cung cấp nhiều tính năng vượt trội bên trong hệ điều hành và khả năng chuẩn đoán, cho phép các quản trị viên tăng được thời gian hỗ trợ cho công việc của doanh nghiệp.

Windows Server 2008 xây dựng trên sự thành công và sức mạnh của hệ điều hành đã có trước đó là Windows Server 2003 và những cách tân có trong bản Service Pack 1 và Windows Server 2003 R2. Mặc dù vậy Windows Server 2008 hoàn toàn hơn hẳn các hệ điều hành tiền nhiệm. Windows Server 2008 được thiết kế để cung cấp cho các tổ chức có được nền tảng sản xuất tốt nhất cho ứng dụng, mạng và các dịch vụ web từ nhóm làm việc đến những trung tâm dữ liệu với tính năng động, tính năng mới có giá trị và những cải thiện mạnh mẽ cho hệ điều hành cơ bản.

CHƯƠNG 1: TỔNG QUAN VỀ WINDOWS SERVER 2008

1.1. Giới thiệu Windows Server 2008

Window Server 2008 chính thức phát hành cho các nhà sản xuất vào ngày 4/2/2008 và chính thức đưa ra thị trường vào 27/2/2008.

Microsoft Windows Server 2008 là hệ điều hành máy chủ Windows thế hệ tiếp theo của hãng Microsoft. Sản phẩm này có khả năng hỗ trợ các chuyên gia công nghệ thông tin trong việc kiểm soát một cách tối ưu hạ tầng máy chủ nhờ việc cung cấp khả năng sẵn sàng và khả năng quản lý chưa từng có, đồng thời tạo nên một môi trường máy chủ an toàn, tin cậy và hiệu quả hơn trước rất nhiều.

Bằng việc đưa vào những tính năng mới, Windows Server 2008 đem đến sự cải thiện mạnh mẽ cho nền tảng hệ điều hành, hơn hẳn so với Windows Server 2003. Các tính năng được cải thiện đáng chú ý nhất bao gồm các tính năng an ninh nâng cao, truy cập ứng dụng từ xa, quản lý server tập trung, các công cụ giám sát hiệu năng và độ tin cậy, failover clustering, triển khai và hệ thống file. Các cải thiện này cùng với rất nhiều tính năng khác sẽ giúp tối ưu hóa độ linh hoạt, tính sẵn sàng và việc điều khiển đối với các máy chủ.

1.2. Các tính năng của Windows Server 2008

Active Directory được mở rộng với các dịch vụ nhận dạng, chứng thực và quản lý quyền. AD dưới phiên bản Windows Server trước kia cho phép người quản trị có thể quản lý tập trung các máy tính trong mạng, để thiết lập các chính sách cho các nhóm & người dùng, và để triển khai tập trung các ứng dụng tới các máy tính. Vai trò này trong Windows Server 2008 được chuyển sang tên Active Directory Domain Services (ADDS). Một loạt các dịch vụ khác được giới thiệu trong phiên bản này như : Active Directory Federation Services (ADFS), Active Directory Lightweight Directory Services (AD LDS), Active Directory Certificate Services (ADCS), và Active Directory Rights Management Services (ADRMS).

Terminal Services : hỗ trợ phiên bản Remote Desktop Protocol 6.0 với nhiều cải tiến :

- Chia sẻ ứng dụng đơn qua kết nối mạng, thay vì toàn bộ Desktop (Terminal Services RemoteApp).
- Client có thể kết nối RDP qua HTTPS mà không cần khởi tạo phiên VPN trước (Terminal Services Gateway).

- Quản trị viên có thể cung cấp truy nhập vào Terminal Services Sessions qua giao diện Web (Terminal Services Web Access).

Windows PowerShell : Đây là hệ điều hành đầu tiên cung cấp Windows PowerShell, bộ lệnh mở rộng mới của Microsoft và công nghệ tạo kịch bản công việc. PowerShell dựa trên công nghệ lập trình hướng đối tượng và phiên bản .NET 2.0, cung cấp hơn 120 ứng dụng quản trị hệ thống, có cú pháp chặt chẽ và hỗ trợ khả năng làm việc với các thành phần hệ thống như Windows Registry, hệ thống chứng chỉ, hoặc Windows Management Instrumentation.Ngôn ngữ kịch bản PowerShell được thiết kế dành cho các nhà quản trị viên IT, và có thể sử dụng trong lệnh cmd.exe hoặc Windows Scripting Host.

Self-Healing NTFS : Trong các phiên bản Windows trước, nếu hệ điều hành phát hiện các lỗi trong file hệ thống của ổ đĩa NTFS, nó đánh dấu ổ đĩa là "dirty"; để sửa lỗi trên ổ đĩa đó, ổ đĩa phải ở chế độ offline. Với hệ thống NTFS tự sửa lỗi, một tiến trình NTFS "worker" sẽ được chạy ở chế độ nền, tiến hành các sửa chữa trên vùng dữ liệu bị lỗi, không cần toàn bộ ổ đĩa phải ngừng làm việc. Hệ điều hành giờ cũng cung cấp tính năng S.M.A.R.T (Self-Monitoring, Analysis, and Reporting Technology) để phát hiện khi nào ổ đĩa có thể bị hỏng.

Hyper – V : là một hệ thống ảo hóa cho phép tạo ra các server ảo trên hệ thống ở mức hệ điều hành. Nó có thể hiểu là một máy chủ vật lý được chia làm nhiều máy tính nhỏ hơn, và các hệ điều hành chạy độc lập trên các máy tính đó. Phiên bản này chỉ cung cấp khả năng hoạt động trên các kiến trúc x86-64 bit.

Windows System Resource Manager : Cung cấp khả năng quản lý tài nguyên và có thể sử dụng để điều khiển số lượng các tài nguyên mà một tiến trình hoặc một người sử dụng có thể dùng dựa trên độ ưu tiên.

Server Manager : là một công cụ quản trị dựa theo vai trò dành cho Windows Server 2008. Nó bao gồm cả Manage Your Server và Security Configuration Wizard ở Windows Server 2003. Công cụ sẽ được mặc định chạy khi khởi động Windows, cho phép người dùng dễ dàng thêm, bớt các dịch vụ dựa theo việc xác định vai trò của Server. Hiện tại phiên bản này chưa cho phép công cụ này được sử dụng từ xa, nhưng cũng đang có một số ứng dụng thay thế được xây dựng để đáp ứng nhu cầu này.

1.3. Một số nâng cấp mới của Windows Server 2008

1.3.1. Cải tiến trên lõi hệ điều hành

- Một hệ điều hành nhiều thành phần đầy đủ
- Cải tiến khả năng hot-patching, cho phép việc kết nối các thành phần không thuộc lõi có thể diễn ra mà không cần khởi động lại máy.
- Hỗ trợ việc khởi động từ các firmware tương thích EFI (Extensible Firmware Interface).
- Phân hoạch phần cứng động.
- Hỗ trợ việc thêm bớt nóng các bộ xử lý và bộ nhớ động, theo khả năng của phần cứng.
- Hỗ trợ việc thay thế nóng các bộ xử lý và bộ nhớ, theo khả năng của phần cứng.

1.3.2. Cải tiến của AD

- Có chế độ hoạt động Domain chỉ đọc (Read Only Domain Controller - RODC). Chế độ này dành cho các chi nhánh khi mà DC chạy trên các máy server có độ an toàn vật lý không cao. Khi đó các RODC chỉ lưu trữ một bản sao chỉ đọc của AD, và nó chuyển mọi yêu cầu cập nhật lên một máy DC chính. Máy này sẽ tự động tiến hành các cập nhật cần thiết.
- AD có khả năng khởi động lại cho phép dịch vụ ADDS có thể STOP và RESTART trong giao diện Management Console mà không cần khởi động lại cả server.

1.3.3. Các chính sách cải tiến

- Mọi cải tiến của Group Policy trong Windows Vista đều được cập nhật. Group Policy Management Console được tích hợp sẵn. Các đối tượng GP được đánh chỉ mục để dễ dàng tìm kiếm và nhận xét.
- Có cơ chế bảo vệ truy cập mạng với Network Access Protection cho phép admin buộc các máy tính kết nối vào mạng phải đáp ứng yêu cầu về sức khỏe hệ thống, và giới hạn truy cập mạng với các máy tính không thoả yêu cầu. NAP còn cung cấp thư viện hàm API cho phép các hãng phần mềm và các nhà phát triển xây dựng nhiều giải pháp cho việc đánh giá tình trạng sức khỏe và giới hạn truy cập mạng.
- Các chính sách có thể được tạo ra để đảm bảo các ứng dụng cần băng thông cao có thể có chất lượng mạng tốt hơn.

- Cơ chế thiết lập mật khẩu cho phép tạo ra nhiều chính sách mật khẩu trên các nhóm và người dùng thay vì 1 thiết lập duy nhất trên toàn bộ domain.

1.3.4. Các cải tiến trong quản lý ổ đĩa và file

- Cung cấp khả năng thay đổi kích thước phân vùng mà không phải dừng server, kể cả phân vùng hệ thống (không áp dụng trên striped volumes).
- Shadow Copy hỗ trợ các ổ đĩa quang, ổ đĩa mạng.
- Distributed File System cải tiến, giúp cho việc thiết lập hệ thống chạy trên nhiều DC hiệu quả hơn.
- Cải tiến Failover Clustering.
- Internet Storage Naming Server cho phép đăng ký, hủy đăng ký tập trung và truy xuất tới các ổ đĩa cứng iSCS.

1.3.5. Cải tiến giao thức và mã hóa

- Hỗ trợ mã hóa 128 và 256 bit cho giao thức chứng thực Keberos.
- Hàm API mã hóa mới hỗ trợ mã hóa vòng ellip và cải tiến quản lý chứng chỉ.
- Giao thức VPN mới Secure Socket Tunneling Protocol.
- AuthIP, một phần mở rộng của giao thức mã hóa IKE sử dụng trong mạng VPN Ipsec.
- Giao thức Server Message Block 2.0 trong bộ TCP/IP mới cung cấp một loạt các cải tiến trong truyền thông như hiệu suất lớn hơn khi kết nối đến các file chia sẻ qua các liên kết có độ trễ cao và bảo mật tốt hơn trong các chứng thực hai chiều và chữ ký số.

1.3.6. Một số tính năng khác

- Windows Deployment Services thay thế cho Automated Deployment Services và Remote Installation Services.
- IIS 7 thay thế cho IIS 6, tăng cường khả năng bảo mật, cải tiến công cụ chuẩn đoán, hỗ trợ quản trị.
- Có thành phần "Desktop Experience" cung cấp khả năng cải tiến giao diện như Windows Aero của Windows Vista, cho cả người dùng tại chỗ và người dùng truy cập từ xa.

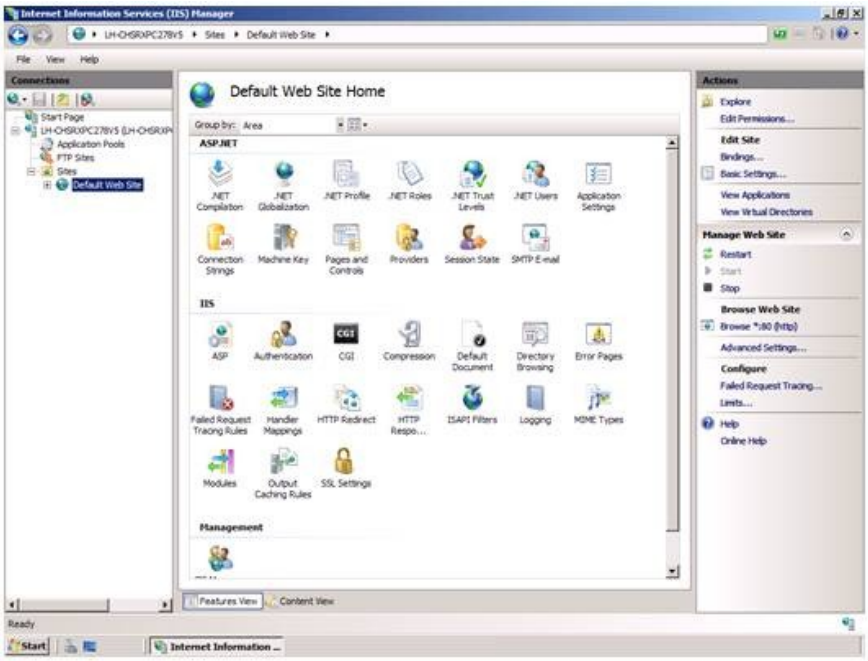
1.4. Các lợi ích của Windows Server 2008

Windows Server 2008 mang lại lợi ích trong bốn lĩnh vực chính:

1.5. Web:

Windows Server 2008 cung cấp một nền tảng đồng nhất để triển khai dịch vụ Web nhờ việc tích hợp Internet Information Services 7.0 (IIS 7.0), ASP .NET, Windows Communication Foundation và Microsoft Windows SharePoint Services. Là bản nâng cấp của IIS 6.0, IIS 7.0 đóng vai trò chính trong việc tích hợp các công nghệ trên nền tảng Web. IIS 7.0 đem lại các lợi ích lớn, bao gồm các tính năng phân tích và quản trị hiệu quả hơn, nâng cao tính bảo mật và giảm chi phí hỗ trợ.

Với giao diện quản trị thân thiện và tiện dụng, IIS 7.0 giúp việc quản lý các tác vụ máy chủ Web đơn giản hơn trước rất nhiều. Người quản trị sẽ không cần phải truy cập quá nhiều mức vào cây thư mục quản trị, các tác vụ thực hiện được bố trí rất thuận tiện và dễ dùng.



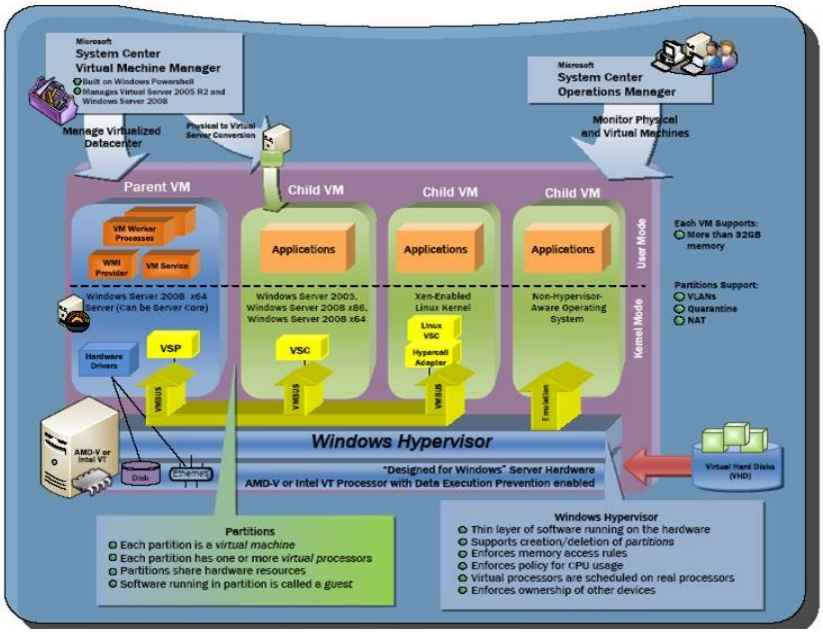
Hình 1.1: Giao diện quản trị IIS 7.0

IIS 7.0 còn hỗ trợ việc sao chép giữa các site, cho phép copy dễ dàng các thiết lập của trang web giữa các máy chủ Web khác nhau mà không phải cấu hình gì thêm. Bên cạnh đó, chính sách phân quyền quản trị các ứng dụng và các site được thực hiện rất rõ ràng, giúp bạn có thể điều khiển các phần khác nhau của máy chủ Web một cách an toàn và thuận tiện.

1.5.1. Ảo hóa:

Phiên bản 64 bits của Windows Server 2008 được tích hợp sẵn công nghệ ảo hóa. Khác với sản phẩm Microsoft Virtual Server 2005 khi

các máy ảo được dựng trên nền hệ điều hành với nhiều tính năng hạn chế, công nghệ ảo hóa hypervisor trong Windows Server 2008 cho phép các máy ảo tương tác trực tiếp với phần cứng máy chủ một cách hiệu quả hơn. Ảo hóa dựng sẵn có khả năng ảo hóa nhiều hệ điều hành khác nhau như Windows, Linux… trên cùng một phần cưng máy chủ, cho phép bạn giảm chi phí, tăng hiệu suất sử dụng phần cứng, tối ưu hóa hạ tầng và nâng cao tính sẵn sàng của máy chủ. Hơn nữa, cùng với chính sách bản quyền linh hoạt, việc sử dụng ảo hóa sẽ tiết kiệm đáng kể chi phí mua sắm bản quyền phần mềm.



Hình 1.2: Windows Server Virtualization

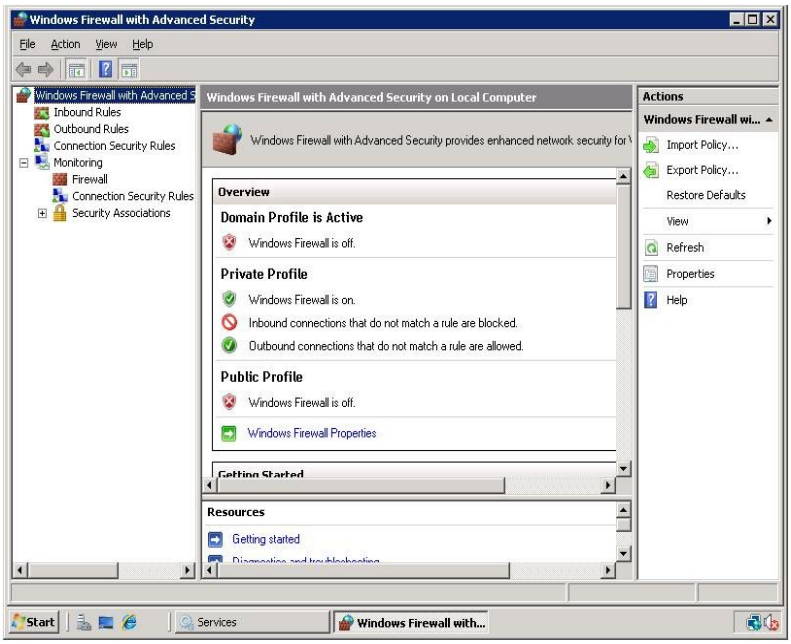
Bên cạnh đó, công nghệ ảo hóa trong Windows Server 2008 còn giúp bạn tích hợp và tập trung các ứng dụng phục vụ cho việc truy cập từ xa một cách dễ dàng bằng cách sử dụng Terminal Services. Người dùng từ xa (và cả người dùng từ ngoài Internet) sẽ không phải sử dụng các kết nối VPN mà vẫn có thể truy cập tới các ứng dụng trong hệ thống mạng nội bộ và sử dụng các ứng dụng đó mà không cần quan tâm vị trí hiện tại của họ ở đâu.

1.5.2. Bảo mật

Windows Server 2008 là hệ điều hành máy chủ Windows an toàn nhất từ trước tới nay. Các tính năng an ninh bao gồm Network Access Protection, Read-Only Domain Controller, BitLocker, Windows Firewall… cung cấp các mức bảo vệ chưa từng có cho hệ thống mạng, dữ liệu và công việc của tổ chức.

Network Access Protection (NAP). Chúng ta đều biết rằng, một trong những nguyên nhân gây ảnh hưởng lớn tới hoạt động của hệ thống công nghệ thông tin của tổ chức xuất phát từ sự thiếu an toàn của

máy trạm. Kẻ gian có thể lợi dụng những lỗ hổng an ninh của máy trạm để từ đó gây hại cho hệ thống của tổ chức. Nhờ có NAP, người quản trị có thể thiết lập các chính sách mạng đối với các máy trạm khi máy trạm đó muốn kết nối vào hệ thống mạng của tổ chức. Chỉ khi các máy trạm đó đáp ứng đầy đủ các yêu cầu an ninh như máy trạm đã cài đặt phần mềm diệt virus và đã cập nhật bản mới nhất, máy trạm đã cài đặt các bản vá lỗi hệ thống, hay đã cài đặt phần mềm firewall thì mới được phép kết nối vào hệ thống mạng của tổ chức. Nếu chưa thỏa mãn các điều kiện đó thì máy trạm sẽ được cách ly trong một vùng mạng riêng, tại đó máy trạm sẽ được cập nhật và sửa lỗi các yêu cầu an ninh, đến khi nào thỏa mãn chính sách đặt ra mới được kết nối vào mạng của tổ chức. NAP có thể được sử dụng để kiểm soát khi máy trạm muốn truy nhập vào hệ thống mạng thông qua DHCP, IPSec, VPN, và qua kết nối không dây 802.1x. Nhờ cách thức mới này, quản trị viên có thể hạn chế ở mức cơ bản những tác hại từ máy trạm đối với hệ thống mạng chung.



Hình 1.3: Giao diện quản trị Windows Firewall

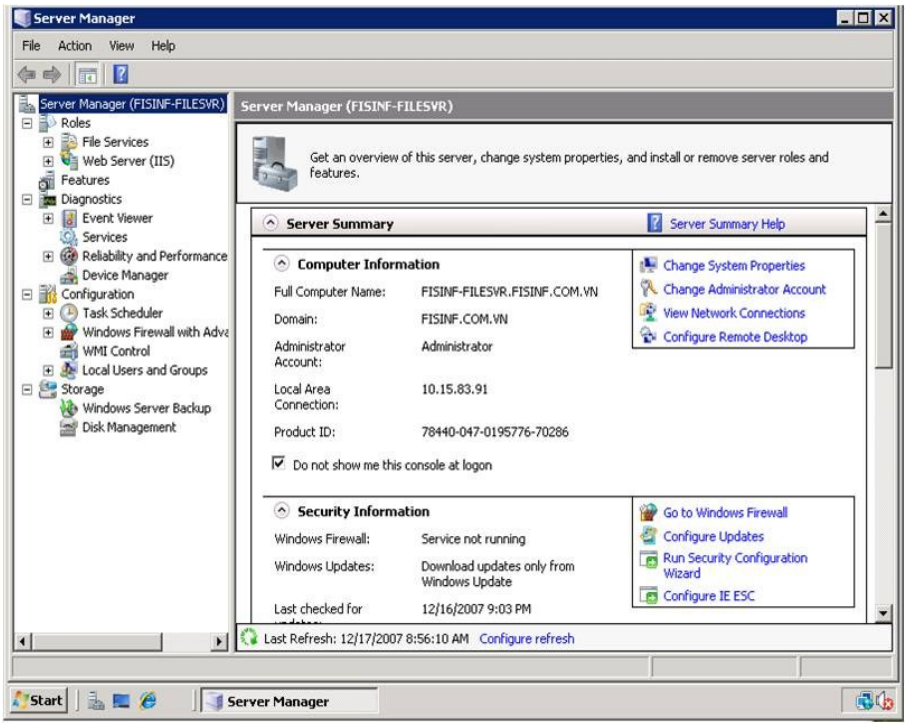
Trong các phiên bản Windows Server trước, Windows Firewall và IPSec được cấu hình một cách riêng rẽ, do đó rất dễ dẫn đến việc trùng lặp các luật cho các thông tin vào ra. Để khắc phục nhược điểm này, Windows Firewall trong Windows Server 2008 đã kết hợp cả hai dịch vụ mạng này lại trên một giao diện cấu hình chung. Sự kết hợp này sẽ giúp đơn giản hóa các thao tác cấu hình, và tránh được sự trùng lặp các luật.

1.5.3. Nền tảng vững chắc cho các hoạt động của tổ chức

Windows Server 2008 cũng là hệ điều hành máy chủ Windows linh hoạt và mạnh mẽ nhất từ trước tới nay. Với các công nghệ và tính

năng mới như Server Core, PowerShell, Windows Deployment Services và các công nghệ mạng, Failover Clustering nâng cao, Windows Server 2008 mang đến cho bạn một nền tảng Windows linh hoạt và tin cậy cho tất cả các yêu cầu về khối lượng công việc và ứng dụng.

Server Manager: Là một tính năng mới có trong Windows Server 2008. Đây là một trong những tính năng nổi trội, được thiết kế để nhân viên quản trị có một cái nhìn tổng quan nhất về toàn bộ quá trình cài đặt, cấu hình, quản lý các roles (vai trò, chức năng của server) và tính năng trong máy chủ chạy Windows Server 2008. Server Manager thay thế và hợp nhất một số tính năng từ Windows Server 2003 như Manage Your Server, Configure Your Server, Add or Remove Windows Components. Người quản trị có thể sử dụng công cụ này để kiểm soát, thay đổi, cài đặt các roles và tính năng trên máy chủ, quản lý các tác vụ, các services (các dịch vụ chạy trên máy chủ), tài khoản người dùng, cũng như xác định, giám sát các sự kiện, phục vụ việc tìm và sửa lỗi hệ thống.



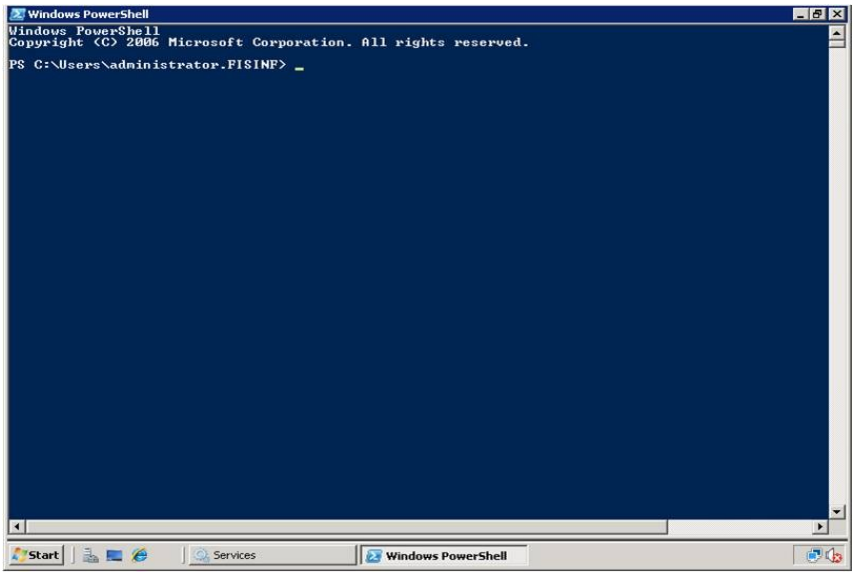
Hình 1.4: Giao diện quản trị Server Manage

Server Core: Là một chức năng mới trong Windows Server 2008. Máy chủ chạy Server Core sẽ chỉ cài đặt một môi trường tối thiểu để chạy các ứng dụng cơ bản, cần thiết như các roles AD DS, AD LDS, DHCP Server, DNS Server, File Services, và Streaming Media Services. Server Core không có giao diện đồ họa như truyền thống. Khi cấu hình server, ta có thể quản lý nó thông qua cửa sổ command-line (cục bộ) hay qua kết nối Terminal Server. Ta cũng có thể quản lý từ xa bằng

cách sử dụng Microsoft Management Console (MMC) hoặc các công cụ command-line hỗ trợ từ xa.

Việc triển khai Server Core đem lại nhiều lợi ích như giảm chi phí bảo trì, giảm chi phí quản lý và giảm việc bị tấn công do nó chỉ cài đặt tối thiểu các ứng dụng yêu cầu, bề mặt tấn công giảm. Hơn thế, Server Core không yêu cầu máy chủ có cấu hình cao. Server Core thường được áp dụng trong trường hợp yêu cầu độ an toàn, ổn định cao.

Windows PowerShell: Là môt tiện ích mới, sử dụng dòng lệnh của Windows giúp cho các nhân viên IT có thể thực hiện các tác vụ một cách tự động. Với trên 120 công cụ dòng lệnh chuẩn, cùng với các ứng dụng và kịch bản sẵn có, Windows PowerShell cho phép các quản trị viên dễ dàng kiểm soát hệ thống và tăng tốc các quá trình tự động trong các nhiệm vụ quản trị theo định kỳ một cách an toàn, đặc biệt thông qua nhiều máy chủ. Vì làm việc với mã lệnh và hạ tầng IT sẵn có, Windows PowerShell rất dễ sử dụng. Nó cho phép người dùng có thể tự động hóa quá trình quản trị các tác vụ, quản trị hệ thống (ví dụ như Active Directory, Internet Information Server (IIS 7.0), Terminal Server…), cũng như triển khai các roles của máy chủ. Đồng thời Windows PowerShell cho phép cải thiện khả năng quản lý hệ thống nhằm phù hợp với môi trường hệ thống.

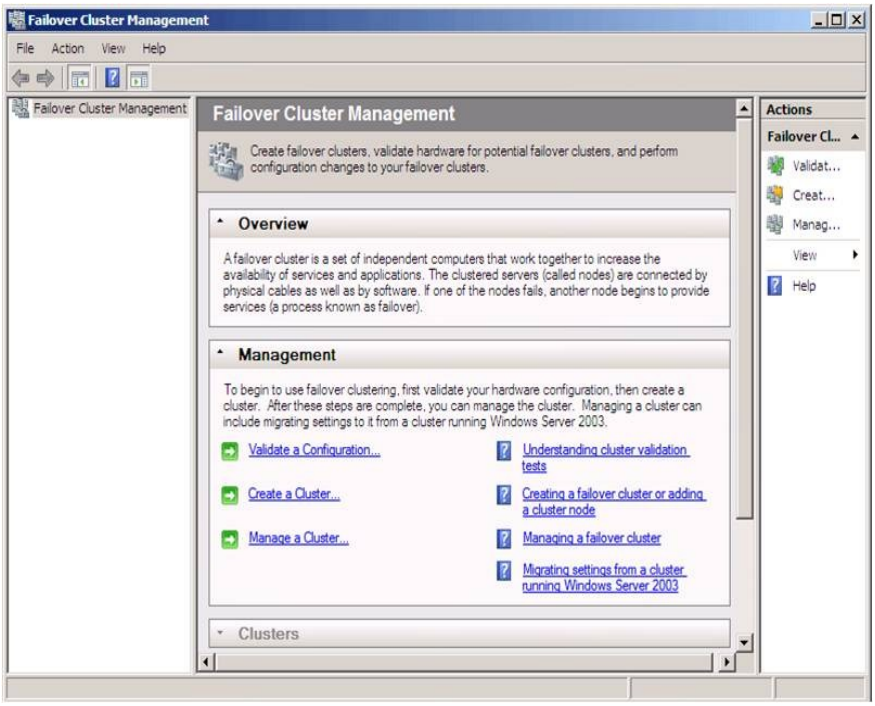


Hình 1.5: Giao diện Windows PowerShell

Windows Deployment Services (WDS): Là phiên bản nâng cấp của Remote Installation Services (RIS) có trong Windows Server 2003. WDS hỗ trợ việc triển khai nhanh chóng các hệ điều hành Windows thông qua việc cài đặt qua mạng mà không cần tới trực tiếp các máy

tính cũng như không cần các đĩa CD cài đặt. Việc sử dụng WDS sẽ đem lại cho tổ chức nhiều lợi ích như giảm chi phí tổng thể và giảm phức tạp khi triển khai, có thể triển khai khi các máy tính chưa có hệ điều hành, cũng như hỗ trợ được cả trong môi trường hỗ hợp có cả Windows XP và Windows Server 2003.

Failover Clustering: Tính năng Failover Clustering trong Windows Server 2008 được cải thiện làm cho việc cấu hình các nhóm máy chủ cùng thực hiện một chức năng dễ dàng hơn trước rất nhiều. Người dùng Windows Server 2003 có thể gặp nhiều rắc rối khi tiến hành cài đặt cluster cho máy chủ, nhưng với Windows Server 2008, việc cài đặt và cấu hình đơn giản và trực quan hơn.



Hình 1.6: Giao diện cấu hình Failover Cluster

Bằng việc sử dụng Validate Tool, một công cụ mới của tính năng Failover Clustering, bạn có thể kiểm tra tính tương thích của các máy chủ trước khi tiến hành cài đặt cluster. Công cụ này sẽ kiểm tra toàn bộ phần cứng, phần mềm của máy chủ và đưa ra các báo cáo rất rõ ràng, giúp bạn dễ dàng xác định được xem các cấu hình và thiết lập đã phù hợp yêu cầu cài đặt hay chưa. Mặt khác, với khả năng tự động chuyển đổi dự phòng trong nhóm các máy chủ chạy cluster với nhau của Windows Server 2008, các quản trị viên có thể thực hiện cài đặt, chuyển đổi cũng như quản lý các nhiệm vụ hoạt động dễ dàng hơn. Vì vậy, tính sẵn sàng và ổn định của hệ thống sẽ được nâng cao.

Windows Server 2008 và Windows Vista cùng hỗ trợ nhau: Tương tự như Windows XP ra đời cùng với dòng hệ điều hành máy

chủ của nó là Windows Server 2003, Windows Vista ra đời là sự kết hợp hoàn hảo với Windows Server 2008. Cả hai đều là một phần trong một dự án của Microsoft, chia sẻ khá nhiều công nghệ như: bảo mật, lưu trữ, quản lý, mạng… Microsoft sẽ kết hợp hai hệ điều hành này nhằm tạo ra một hệ thống an toàn từ máy trạm cho tới máy chủ.

Phiên bản chính thức của Windows Server 2008 được Microsoft ra mắt vào tháng 2/2008. Với những tính năng nổi trội và những lợi ích lớn như đã trình bày ở trên, Windows Server 2008 hứa hẹn sẽ đem đến cho các tổ chức, doanh nghiệp một nền tảng hệ điều hành máy chủ an toàn, ổn định và hiệu quả nhất.

1.6. Các phiên bản Window Server 2008

- ***Windows Web Server 2008***: dành cho các hệ thống dựa trên bộ xử lý Itanium được tối ưu hóa cho các trung tâm dữ liệu lớn, các ứng dụng nghiệp vụ riêng, ứng dụng tùy biến mang lại độ sẵn sàng và khả năng mở rộng cao cho tới 64 bộ xử lý để đáp ứng nhu cầu cho các giải pháp khắt khe và quan trọng.
- ***Windows Server 2008 Standard***: là hệ điều hành Windows Server mạnh nhất hiện nay. Với các khả năng ảo hóa và Web dựng sẵn và tăng cường, phiên bản này được thiết kế để tăng độ tin cậy và linh hoạt của cơ sở hạ tầng máy chủ của bạn đồng thời giúp tiết kiệm thời gian và giảm chi phí. Các công cụ mạnh mẽ giúp bạn kiểm soát máy chủ tốt hơn, và sắp xếp hợp lý các tác vụ cấu hình và quản lý. Thêm vào đó, các tính năng bảo mật được cải tiến làm tăng sức mạnh cho hệ điều hành để giúp bạn bảo vệ dữ liệu và mạng, và tạo ra một nền tảng vững chắc và đáng tin cậy cho doanh nghiệp của bạn.
- ***Windows Server 2008 Standard without Hyper-V***
- ***Windows Server 2008 Enterprise***: đem tới một nền tảng cấp doanh nghiệp để triển khai các ứng dụng quan trọng đối với hoạt động kinh doanh. Phiên bản này giúp cải thiện tính sẵn có nhờ các khả năng clustering và cắm nóng bộ xử lý, giúp cải thiện tính bảo mật với các đặc tính được củng cố để quản lý nhận dạng, và giảm bớt chi phí cho cơ sở hạ tầng hệ thống bằng cách hợp nhất ứng dụng với các quyền cấp phép ảo hóa. Windows Server 2008 Enterprise mang lại nền tảng cho một cơ sở hạ tầng CNTT có độ năng động và khả năng mở rộng cao.
- ***Windows Server 2008 Enterprise without Hyper-V***
- ***Windows Server 2008 Datacenter***: đem tới một nền tảng cấp

doanh nghiệp để triển khai các ứng dụng quan trọng đối với hoạt động kinh doanh và ảo hóa ở quy mô lớn trên các máy chủ lớn và nhỏ. Phiên bản này cải thiện tính sẵn có nhờ các khả năng clustering và phân vùng phần cứng động, giảm bớt chi phí cho cơ sở hạ tầng hệ thống bằng cách hợp nhất các ứng dụng với các quyền cấp phép ảo hóa không hạn chế, và mở rộng từ 2 tới 64 bộ xử lý. Windows Server 2008 Datacenter mang lại một nền tảng để từ đó xây dựng các giải pháp mở rộng và ảo hóa cấp doanh nghiệp.

- ***Windows Server 2008 Datacenter without Hyper-V***
- ***Windows Server 2008 for Itanium-Based Systems***: dành cho các hệ thống dựa trên bộ xử lý Itanium được tối ưu hóa cho các trung tâm dữ liệu lớn, các ứng dụng nghiệp vụ riêng, ứng dụng tùy biến mang lại độ sẵn sàng và khả năng mở rộng cao cho tới 64 bộ xử lý để đáp ứng nhu cầu cho các giải pháp khắt khe và quan trọng
- ***Windows HPC Server 2008*** : Được xây dựng dựa trên Windows Server 2008, công nghệ 64-bit, Windows HPC Server 2008 có thể mở rộng tới hàng nghìn lõi xử lý và chứa các console quản lý giúp bạn chủ động theo dõi và duy trì tình trạng an toàn và tính ổn định của hệ thống. Khả năng tương kết và linh hoạt trong điều khiển công việc cho phép tích hợp giữa các nền tảng HPC trên nền Windows và Linux, hỗ trợ các tải làm việc theo mẻ và các tải làm việc theo ứng dụng hướng dịch vụ (SOA). Năng suất được cải thiện, hiệu năng có thể tùy biến, và dễ sử dụng là một số đặc trưng khiến Windows HPC Server 2008 trở thành sản phẩm tốt nhất cho các môi trường Windows.

CHƯƠNG 2: CÀI ĐẶT CÁC DỊCH VỤ MẠNG TRÊN WINDOWS SERVER 2008

2.1. Cài đặt và cấu hình máy chủ Windows Server 2008

2.1.1. Xác định yêu cầu phần cứng

2.1.2.

Phần cứng/Cấu hình **Tối thiểu** **Đề nghị** **Tối ưu** Bộ nhớ RAM 512MB 1GB 2GB Bộ vi xử lý 1Ghz 2Ghz 3Ghz Ở cứng(trống) 10GB 40GB 80GB			

Ti

ến hành cài đặt Windows Server 2008

Toàn bộ việc cài đặt Windows Server 2008 chỉ qua ba phần:

- Cài đặt hệ điều hành
- Khởi tạo cấu hình Initial Configuration Tasks
- Cài đặt Server Manager

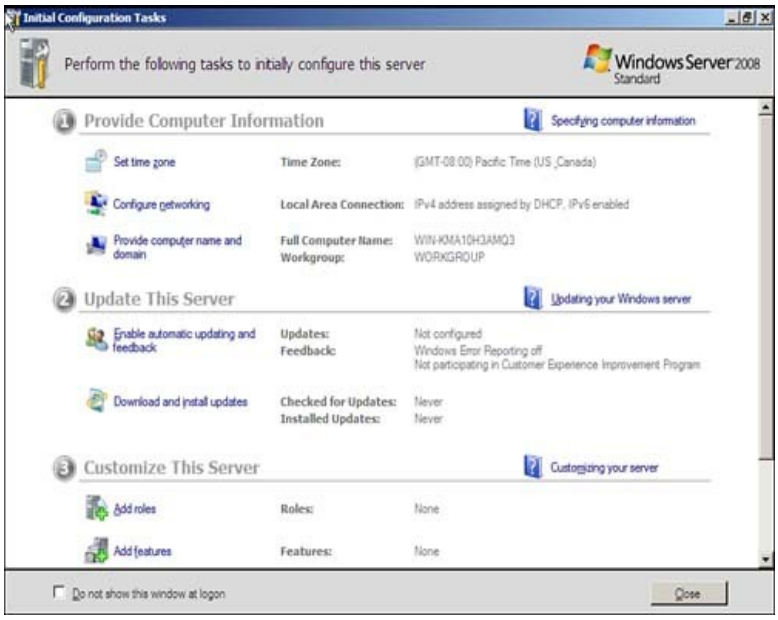
2.1.2.1. Cài đặt hệ điều hành

1. Cho đĩa cài đặt Windows Server 2008 vào ổ và khởi động máy chủ từ đĩa cài.
2. Khi được yêu cầu chọn ngôn ngữ, thời gian, đơn vị tiền tệ và thông tin bàn phím, bạn hãy đưa ra lựa chọn thích hợp rồi click **Next**.
3. Tùy chọn Install Now xuất hiện. Nếu chưa chắc chắn về yêu cầu phần cứng, có thể click vào liên kết*What to Know Before Installing Windows* để biết thêm chi tiết.
4. Nhập khóa kích hoạt sản phẩm (product key) và đánh dấu kiểm vào ô *Automatically Activate Windows When I'm Online*. Click **Next**.
5. Nếu chưa nhập khóa sản phẩm ở mục trước, bây giờ bạn sẽ phải lựa chọn ấn bản Windows Server 2008 sắp cài đặt và đánh dấu kiểm vào ô *I Have Selected an Edition of Windows That I Purchased*. Nếu bạn đã nhập khóa sản phẩm hợp lệ, trình cài đặt sẽ tự động nhận diện được ấn bản Windows Server 2008 bạn sắp cài đặt. Click **Next**.
6. Đọc các điều khoản quy định và chấp nhận bằng cách đánh dấu ô kiểm. Click **Next**.
7. Ở cửa sổ mới xuất hiện, do bạn khởi động máy từ đĩa cài nên tùy chọn Upgrade (nâng cấp) đã bị vô hiệu. Click **Custom (Advanced)**.
8. Trên cửa sổ tiếp theo, bạn cần lựa chọn vị trí cài đặt Windows. Nếu có driver của các thiết bị lưu trữ bên thứ ba, cần cài đặt ngay bằng cách click liên kết *Load Driver*.
9. Khi quá trình cài đặt hoàn tất, hãy thay đổi mật khẩu tài khoản quản trị administrator trước khi đăng nhập. Sau khi mật khẩu được thay đổi và bạn đã đăng nhập vào hệ điều hành, như vậy là bạn đã xong phần 1 của việc cài đặt.

2.1.2.2. Khởi tạo cấu hình

Sau khi bạn đăng nhập vào hệ điều hành, cửa sổ Initial Configuration Tasks Wizard xuất hiện, gồm ba mục:

- Provide computer information (Cung cấp thông tin hệ thống)
- Update this server (Cập nhật máy chủ)
- Customize this server (Tùy biến máy chủ)



Hình 2.1: Initial Configuration Tasks Wizard

Trong mục Provide Computer Information, bạn có thể thực hiện những việc sau:

- Thay đổi múi giờ
- Thiết lập cấu hình mạng trên giao diện card giao tiếp mạng (NIC). Bạn cũng có thể gán địa chỉ IP tĩnh, subnet mask, default gateway (cổng mặc định) và máy chủ DNS/WINS. Trong nhiều môi trường, có lẽ bạn sẽ được nhóm hai card giao tiếp mạng cho mạng LAN dữ liệu sản xuất (sử dụng phần mềm bên thứ ba) và có một card giao tiếp mạng riêng biệt dành riêng cho việc sao lưu dữ liệu được kết nối với mạng LAN sao lưu. Ngoài ra, bạn có thể để mặc cho các thiết lập tự động được gán bởi máy chủ DHCP, tất nhiên trong trường hợp bạn có máy chủ DHCP đã được cấu hình.

Lưu ý: Trên thực tế, bạn sẽ thường gán địa chỉ IP tĩnh cho máy chủ cơ sở hạ tầng. Trong trường hợp này, bạn sẽ cần thu thập thông tin đó cùng với địa chỉ IP hợp lệ cho default gateway và cho máy chủ DNS/WINS trước khi cài đặt.

Trong mục Update This Server, bạn có thể thực hiện những việc

sau:

- Cho phép tự động cập nhật và phản hồi
- Cấu hình việc tải về và cài đặt những cập nhật của hệ điều hành

Trong mục Customize This Server, bạn có thể thực hiện những việc sau:

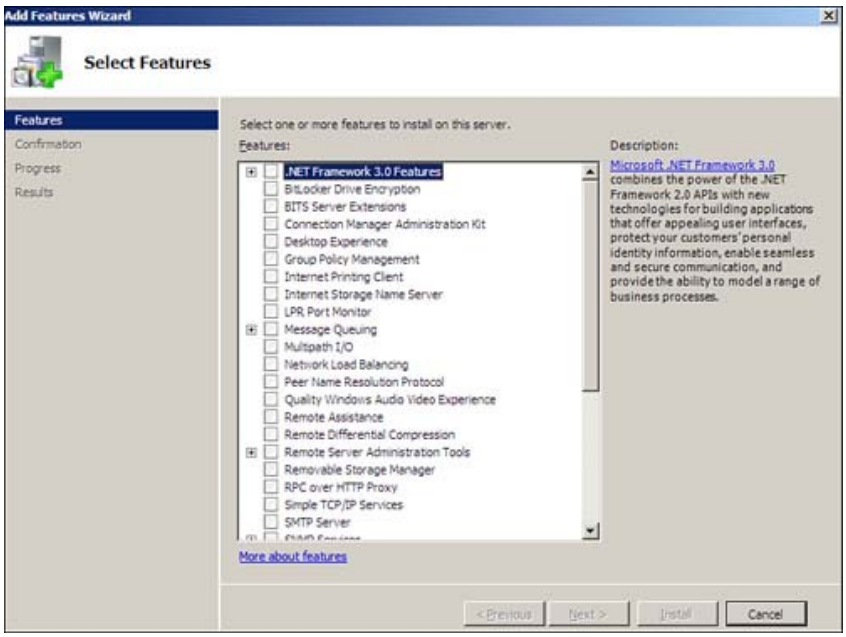
1. Thêm vai trò (role) máy chủ.

Khi bạn chọn một vai trò, trình hướng dẫn sẽ giúp bạn hoàn thành việc cài đặt vai trò. Bạn có thể lựa chọn các vai trò sau:

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Application Server
- DHCP Server
- DNS Server
- Fax Server
- File Services
- Network Policy and Access Services
- Print Services
- Terminal Services
- UDDI Services
- Web Server (IIS)
- Windows Deployment Services

2. Thêm tính năng.

Cũng như thêm vai trò, khi bạn lựa chọn tính năng, trình hướng dẫn sẽ giúp bạn hoàn thành việc cài đặt tính năng đó. Có rất nhiều tính năng cho bạn lựa chọn.



Hình 2.2: Lựa chọn tính năng bạn muốn cài đặt

2.1.2.3. Cài đặt Server Manager

Server Manager cho bạn một cái nhìn toàn cục về máy chủ. Khi nhìn vào phần chi tiết mặc định, bạn có thể thấy thông tin máy tính, thông tin bảo mật và bản tóm tắt các vai trò và tính năng đã cài đặt. Nhìn xuống phía dưới, bạn sẽ thấy tài nguyên và phần hỗ trợ. Phía bên trái cửa sổ là các công cụ giúp bạn thêm/bớt và cấu hình các vai trò cũng như các tính năng. Bạn cũng sẽ thấy các tùy chọn để chẩn đoán, cấu hình và quản lý ổ đĩa. Sau khi xác lập các thay đổi trong Server Manager, công việc cài đặt thủ công của bạn đã thực sự hoàn tất.

2.2. Cài đặt máy chủ quản trị miền Domain Controller

Nếu bạn đến từ thế giới Windows Server 2003 thì bạn sẽ thấy bước này có rất nhiều khác biệt. Bạn sẽ vẫn cần chạy **dcpromo** từ nhắc lệnh **Run,**tuy nhiên cần phải cài đặt **Active Directory Domain Controller** role. Các role máy chủ là một khái niệm mới trong Windows Server 2008 – nơi các dịch vụ máy chủ được xem như các "role". Active Directory Domain Controller role có khác biệt đôi chút vì nó là một quá trình hai bước để cài đặt Active Directory DC: đầu tiên bạn cài đặt role, sau đó chạy **dcpromo**.

1. Vào **Server Manager** và kích nút **Roles** trong panel bên trái của giao diện điều khiển. Sau đó kích vào liên kết**Add Roles** trong phần panel bên phải.
2. Thao tác đó sẽ làm xuất hiện trang **Before You Begin**. Nếu đây là lần đầu tiên bạn cài đặt một role bằng cách sử dụng Server

Manager, hãy đọc các thông tin trong trang này. Nếu bạn đã quen với Server Manager rồi, khi đó hãy kích **Next** để tiếp tục.

3. Chọn **Active Directory Domain Services** bằng cách đặt một dấu tích vào hộp kiểm. Lưu ý rằng wizard sẽ hiển thị cho bạn số lượng các tính năng sẽ được cài đặt cùng với Active Directory Server Role. Kích nút **Add Required Features** để cài đặt thêm các tính năng này với Active Directory Server Role.
4. Sau khi chọn **Active Directory DC Server Role**, bạn sẽ thấy các thông tin về Server Role.
5. Kích **Install** để cài đặt các file yêu cầu nhằm chạy **dcpromo**.
6. Cài đặt được thực hiện thành công. Kích **Close**.
7. Lúc này hãy vào menu **Start**, đánh **dcpromo** vào hộp tìm kiếm. Khi đó bạn sẽ tìm thấy nó trong danh sách như thể hiện trong hình bên dưới. Kích **dcpromo**.
8. Thao tác này sẽ khởi chạy **Welcome to the Active Directory Domain Service Installation Wizard**. Chúng ta không cần các tùy chọn nâng cao trong kịch bản này, chính vì vậy chỉ cần kích **Next.**
9. Trong trang **Operating System Compatibility**, bạn sẽ được cảnh báo rằng các máy khách NT và non-Microsoft SMB sẽ gặp các vấn đề với một số thuật toán mật mã được sử dụng bởi Windows Server 2008. Chúng ta không có vấn đề này trong mạng thử nghiệm, chính vì vậy hãy kích **Next**.
10. Trong trang **Choose a Deployment Configuration** chọn tùy chọn **Create a new domain in a new forest.**Chúng ta thực hiện như vậy vì đây là một miền mới nằm trong một forest mới.
11. Trong trang **Name the Forest Root Domain**, nhập vào tên của miền trong hộp nhập liệu **FQDN of the forest room domain**. Trong ví dụ này chúng tôi sẽ đặt tên cho miền là **fflab.net**. Tuy nhiên các bạn có thể đặt bất cứ tên nào tùy chọn ý thích của mình. Kích **Next.**
12. Trong trang **Set Forest Functional Level**, chọn tùy chọn **Windows Server 2008.**
13. Trong trang **Additional Domain Controller Options**, chúng ta chỉ có một lựa chọn đó là **DNS server**. Tùy chọn Global catalog được tích mặc định vì đây chỉ là một DC trong miền này, vì vậy nó phải là một máy chủ Global Catalog. Tùy chọn Read-only domain controller (RODC) bị hủy chọn vì bạn phải có một non-RODC khác trong mạng để kích hoạt tùy chọn này. Chọn tùy chọn **DNS**

server và kích **Next**.

14. Một hộp thoại sẽ xuất hiện nói rằng không thể tạo đại biểu cho máy chủ DNS này vì không thể tìm thấy vùng xác thực hoặc nó không chạy Windows DNS server. Lý do cho điều này là vì đây là DC đầu tiên trên mạng. Bạn không nên lo lắng về điều này và chỉ cần kích **Yes** để tiếp tục.
15. Để lại thư mục Database, Log Files và SYSVOL trong các location mặc định của chúng và kích **Next**.
16. Trong **Directory Service Restore Mode Administrator Password**, nhập một mật khẩu mạnh vào các hộp nhập liệu **Password** và **Confirm password.**
17. Xác nhận các thông tin trên trang **Summary** và kích **Next**.
18. Active Directory sẽ cài đặt. DC đầu tiên sẽ cài đặt khá nhanh. Đặt một dấu kiểm vào hộp chọn **Reboot on completion** để máy tính sẽ tự động khởi động lại khi cài đặt DC được hoàn tất.
19. Máy tính sẽ tự động khởi động lại vì chúng ta đã chọn tùy chọn đó. Cài đặt sẽ hoàn tất khi bạn đăng nhập.

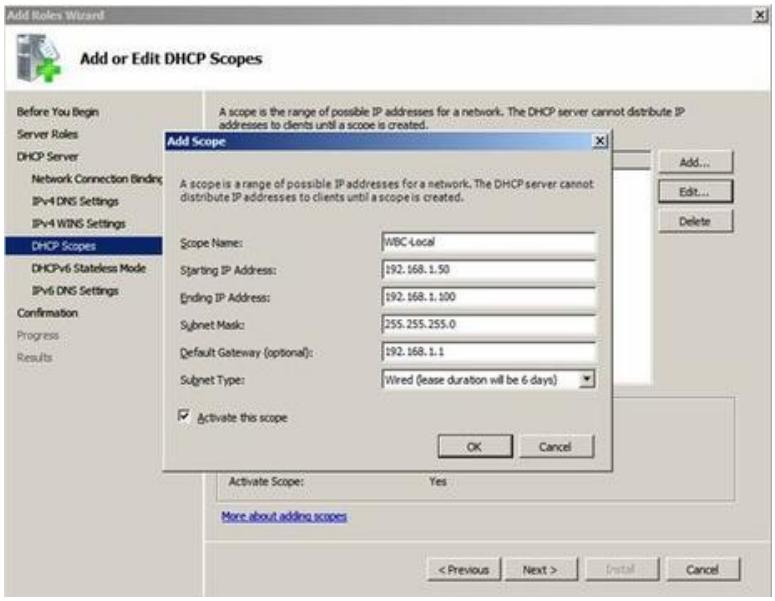
2.3. Cấu hình máy chủ DHCP

Dynamic Host Configuration Protocol (DHCP) bản chất là một dịch vụ cơ sở hạ tầng có trên bất kì một hệ thống mạng nào nhằm cung cấp địa chỉ IP và thông tin DNS server tới các "PC client" hay một số thiết bị khác. DHCP được sử dụng để giúp bạn không phải ấn định địa chỉ IP tĩnh cho tất cả các thiết bị có trong hệ thống mạng của mình và giúp bạn quản lí mọi vấn đề mà địa chỉ IP tĩnh có thể tạo ra. Qua từng thời kì, DHCP ngày càng phát triển để có thể thích hợp trong từng dịch vụ mạng mới giống như "Windows Health Service" hay "Network Access Protection (NAP)". Tuy nhiên, trước khi bạn có thể sử dụng nó để tim kiếm các tiện ích thú vị mà DHCP mang lại cho mình, trước hết bạn cần cài đặt và cấu hình các đặc tính cơ bản. Sau đây, hãy xem hướng dẫn và tiến hành những gì bạn cần làm.

1. Bắt đầu quá trình cài đặt DHCP, bạn có thể click **Add Roles** từ của sổ **Initial Configuration Tasks** hay từ **Server Manager \ Roles \ Add Roles.**
2. Tiếp theo, bạn chọn **DHCP Server Role** mà bạn muốn thêm vào và click **Next.**
3. Nếu bạn không có một địa chỉ IP tĩnh để gán cho server của mình, bạn sẽ nhận được một thông báo rằng bạn sẽ không thể tiếp tục

tiến hành quá trình cài đặt DHCP với một địa chỉ IP động. Do đó, đến điểm này, bạn sẽ bắt đầu cập nhật thông tin cho IP mạng bao gồm: thông tin về phạm vi và thông tin về DNS. Nếu bạn chỉ muốn cài đặt server DHCP với không một cấu hình nào cho bộ chỉ báo hay các thiết đặt cần có, bạn có thể chỉ click Next mà không cần bận tâm gì đến các câu hỏi có được trong tiến trình cài đặt.

4. Tiếp theo,nhập **Parent Domain**, **Primary DNS Server**, và **Alternate DNS Server** và click **Next.**
5. Sau đó, điều chỉnh cấu hình phạm vi một DHCP cho Server DHCP mới.
6. Quay trở lại màn hình Add Scope, click Next.
7. Chọn Disable DHCPv6 stateless mode cho server này và click Next. Sau đó,cấu hình DHCP Installation Selections và click **Install.**



Hình 2.3: Cấu hình máy chủ DHCP

2.4. Cấu hình máy chủ bảo vệ truy cập mạng

Network Access Protection là một hệ thống chính sách thi hành (Health Policy Enforcement) được xây dựng trong các hệ điều hành Windows Server 2008, Windows Vista và Windows XP Services Park 3 . Mục đích của NAP là bảo đảm các máy tính tuân theo yêu cầu bảo mật trong tổ chức của bạn. Khi một người dùng nào đó kết nối vào mạng, máy tính của người dùng có thể được mang ra so sánh với một chính sách mà bạn đã thiết lập Các nội dung bên trong của chính sách này sẽ

khác nhau tùy theo mỗi tổ chức, bạn có thể yêu cầu hệ điều hành của người dùng phải có đầy đủ các bản vá bảo mật mới nhất và máy tính phải đang chạy phần mềm chông virus được cập nhật một cách kịp thời,…và nhiều vấn đề tương tự như vậy. Nếu một máy tính có hội tụ đủ các tiêu chuẩn cần thiết mà bạn đã thiết lập trong chính sách thì máy tính này hoàn toàn có thể kết nối vào mạng theo cách thông thường. Nếu máy tính này không hội tụ đủ các yếu tố cần thiết thì bạn có thể chọn để từ chối sự truy cập mạng cho người dùng, sửa vấn đề lập tức hoặc tiếp tục và cho người dùng sự truy cập nhưng lưu ý về trạng thái của máy tính của người dùng.

Việc triển khai cấu hình máy chủ NAP gồm các bước:

- Cài đặt và cấu hình DHCP server
- Cài đặt Network Policy and Access Service
- Cấu hình NAP health policy server

1. ***Cài đặt và cấu hình DHCP Server (xem phần 2.3)***
2. ***Cài đặt Network Policy anh Access Service***

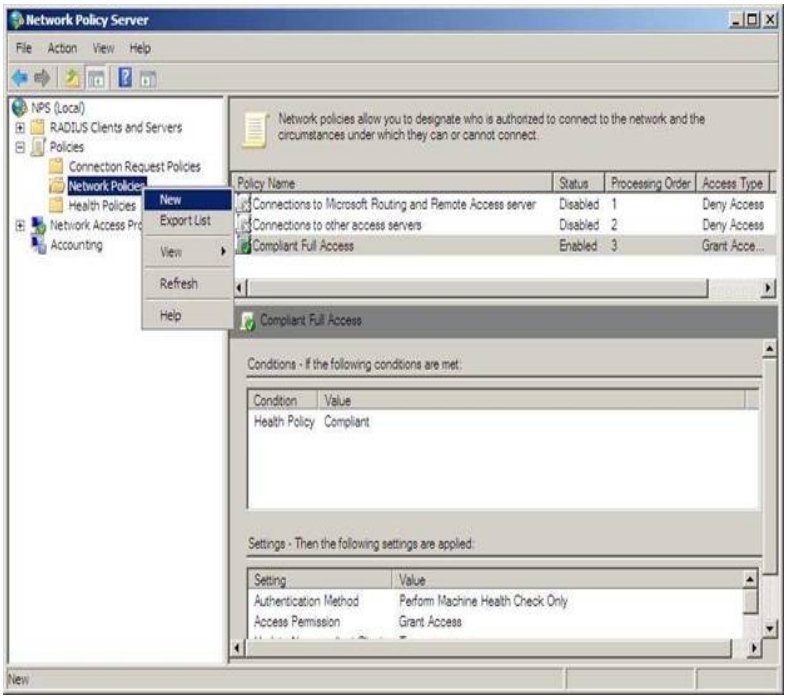
- Mở **Server Manager** từ Administrative Tools, bạn có thể click **Add Roles** từ của sổ **Initial Configuration Tasks** hay từ **Server Manager \ Roles \ Add Roles.**
- Trong cửa **sổ Before You Begin**, chọn **Next.**
- Trong cửa sổ **Select Server Roles**, đánh dấu chọn vào ô **Network Policy and Access Services**, chọn **Next.**
- Trong cửa sổ **Network Policy and Access Services**, chọn **Next.**
- Trong cửa sổ **Select Role Services**, đánh dấu chọn vào ô **Network Policy Server**, chọn **Next.**
- Trong cửa sổ **Confirm Installation Selections**, chọn **Install.**

3. Cấu hình NAP health policy server

- Trên máy Server, mở **Network Policy Server** từ **Administrative Tools**, bung **Network Access Protection**, chọn**System Health Validators**, right click **Windows Security Health Validators** chọn **Properties.**
- Trong cửa sổ **Windows Security Health Validators Properties**, chọn **Configure…**
- Trong cửa sổ **Windows Security Health Validators**, bỏ tất cả các ô chọn, trừ ô **A firewall is enable for all network connections**, chọn **OK**.

- Trong cửa sổ **Windows Security Health Validators Properties**, chọn **OK.**
- Trong cửa sổ **Network Access Policy**, **bung Network Access Protection**, right click **Remediation Server Groups** chọn**New.**
- Trong cửa sổ **New Remediation Server Group**, nhập **Rem1** vào ô **Group Name**, chọn **Add.**
- Trong cửa sổ **Add New Server**, nhập IP của máy Server vào ô **IP address or DNS name**, chọn **Resolve**, chọn **OK.**
- Trong cửa sổ **New Remediation Server Group**, kiểm tra đã add được địa chỉ của máy Server vào ô **Remediation Server,** chọn **OK.**
- Trong cửa sổ **Network Policy Server**, bung **Policies**, right click **Health Policies** chọn **New.**
- Trong cửa sổ **Create New Health Policy**, nhập **Compliant** vào ô **Policy name**, trong ô **Client SHV checks** chọn **Clientpasses all SHV checks**, kiểm tra có đánh dấu chọn ô **Windows Security Health Validator**, chọn **OK.**
- Trong cửa sổ **Network Policy Server**, bung **Policies**, right click **Health Policies** chọn **New**.
- Trong cửa sổ **Create New Health Policy**, nhập **NonCompliant** vào ô **Policy name**, trong ô **Client SHV checks** chọn**Client fails one or more SHV checks**, kiểm tra có đánh dấu chọn ô **Windows Security Health Validator**, chọn **OK.**
- Kiểm tra đã tạo thành công 2 Health Policies: **Complient** và **NonComplient.**
- Trong cửa sổ **Network Policy Server**, bung **Policies**, vào **Network Policies**, lần lượt disable 2 policy đang có.
- Right click **Network Policies** chọn **New.**
- Trong cửa sổ **Specify Network Policy Name and Connection Type**, nhập **Complian Full-Access** vào ô **Policy name**, chọn **Next.**
- Trong cửa sổ **Specify Conditions**, chọn **Add.**
- Trong cửa sổ **Select condition**, chọn mục **Health Policies**, chọn **Add.**
- Trong cửa sổ **Health Policies**, bung **Health policies** chọn **Compliant**, chọn **OK.**
- Trong cửa sổ **Specify Conditions**, chọn **Next.**

- Trong cửa sổ **Specify Access Permission**, chọn **Access granted**, chọn **Next.**
- Trong cửa sổ **Configure Authentication Methods**, bỏ trắng các ô chọn, chỉ đánh dấu chọn vào ô **Perform machine health check only,** chọn **Next.**
- Trong cửa sổ **Configure Constraints**, giữ cấu hình mặc định, chọn **Next.**
- Trong cửa sổ **Configure Settings**, chọn mục **NAP Enforcement**, kiểm tra đảm bảo đang chọn **Allow full network access**, chọn **Next.**
- Trong cửa sổ **Completing New Network Policy**, chọn **Finish.**
- Right click **Network Policies** chọn **New.**
- Trong cửa sổ **Specify Network Policy Name and Connection Type**, nhập **NonCompliant Restricted** vào ô **Policy name**, chọn **Next.**
- Trong cửa sổ **Specify Conditions**, chọn **Add.**
- Trong cửa sổ **Select condition**, chọn mục **Health Policies**, chọn **Add.**
- Trong cửa sổ **Health Policies**, bung **Health policies** chọn **Non-Compliant**, chọn **OK.**
- Trong cửa sổ **Specify Conditions**, chọn **Next.**
- Trong cửa sổ **Specify Access Permission**, chọn **Access granted**, chọn **Next.**
- Trong cửa sổ **Configure Authentication Methods**, bỏ trắng các ô chọn, chỉ đánh dấu chọn vào ô **Perform machine health check only**, chọn **Next.**
- Trong cửa sổ **Configure Constraints**, giữ cấu hình mặc định, chọn **Next.**
- Trong cửa sổ **Configure Settings**, chọn mục **NAP Enforcement**, chọn **Allow limited access**, đánh dấu chọn ô **Enable auto-remediation of client computers**, chọn **Next.**
- Trong cửa sổ **Completing New Network Policy**, chọn **Finish.**
- Kiểm tra đã tạo thành công 2 Network Policies.



Hình 2.4: Cấu hình NAP health policy server

2.5. Cấu hình máy chủ định tuyến và truy cập từ xa

Với Windows Server 2008, có một số các thay đổi trong việc kết nối mạng cũng như Routing và Remote Access. Trong Windows Server 2008 thực sự đã có những dịch vụ mạng đã được remove và một số khác bạn phải sử dụng thay. OSPF đã không tồn tại trong Windows Server 2008 mặc dù theo quan điểm của chúng tôi thì đây có thể là giao thức định tuyến động tốt nhất đã được tạo. Tuy nhiên chúng ta cần phải hiểu sự quyết định của Microsoft trong việc remove nó vì có thể đến 99% các quản trị viên máy chủ Windows không sử dụng đến nó. Vậy chúng ta còn lại những gì? Với sự remove của OSPF khiến chúng ta chỉ còn lại 1) định tuyến tĩnh hoặc 2) định tuyến động với RIPV2. Chúng ta hãy đi tìm ra cách chúng làm việc như thế nào.

Nên sử dụng định tuyến động hay tĩnh?

Câu hỏi đặt ra bạn nên sử dụng định tuyến động hay định tuyến tĩnh thực sự là một câu hỏi làm đau đầu các quản trị viên. Cách định tuyến nào đi chăng nữa thì kết quả cuối cùng của nó vẫn là nhằm mục đích định tuyến đúng lưu lượng mạng.

Với định tuyến tĩnh, bạn phải tạo một entry trên máy chủ Windows Server cho mỗi một mạng, mỗi một mạng này sẽ được định tuyến bởi máy chủ đó. Như vậy, với một mạng đơn giản có một máy chủ Windows Server thì việc định tuyến lưu lượng giữa hai mạng bằng

phương pháp định tuyến tĩnh là một phương pháp ơ no brainer. Bạn có thể cấu hình nó chỉ cần bằng hai lệnh đơn giản **route add.**

Trong trường hợp khác, trên một mạng ở đó bạn muốn hệ thống Windows Server 2008 định tuyến tới 25 mạng hoặc trao đổi các tuyến với mạng Cisco có sử dụng RIP thì cách thực hiện là chọn phương pháp định tuyến động.

Tuy nhiên định tuyến động cung cấp cho bạn những tính năng gì ở đây? Chúng ta hãy liệt kê ra các tính năng của chúng.

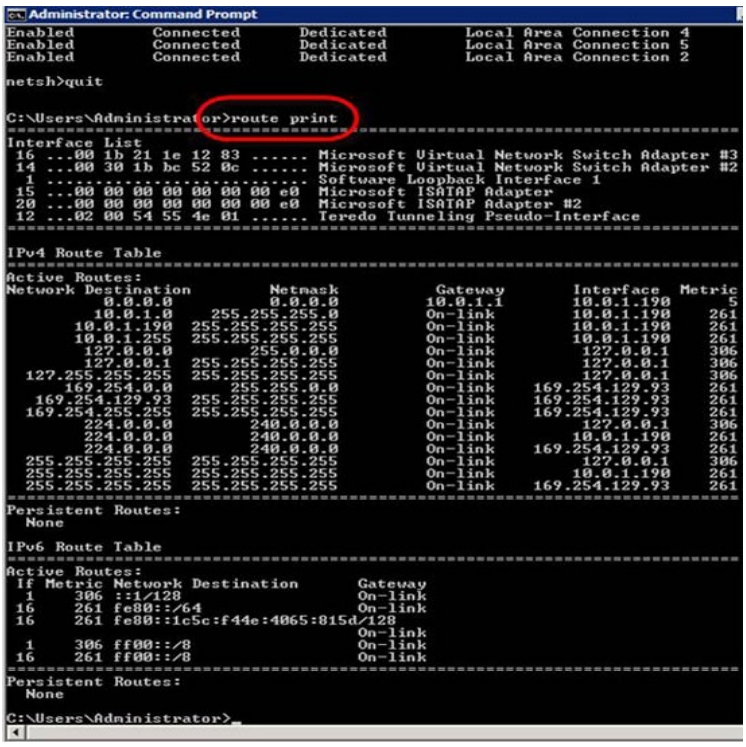
- Khả năng tự động bổ sung các mạng bằng cách học hỏi chúng từ các RIP router khác
- Khả năng tự động remove các tuyến từ bảng định tuyến khi một RIP liền kề khác xóa chúng
- Khả năng chọn tuyến tốt nhất dựa trên metric định tuyến
- Giảm việc cấu hình của các hệ thống định tuyến của Windows Server có nhiều tuyến tĩnh cần được bổ sung.

  Vậy cách cấu hình định tuyến động và định tuyến tĩnh như thế nào trong Windows Server 2008?

2.5.1. Định tuyến tĩnh trong Windows Server 2008

Định tuyến tĩnh trong Windows Server không phải là mới. Bạn có thể cấu hình định tuyến tĩnh trong Windows 2008 Server bằng cách sử dụng lệnh route hoặc sử dụng giao diện quản trị người dùng. Tuy nhiên, nếu bạn sử dụng giao diện GUI thì các tuyến này sẽ không được liệt kê trong giao diện GUI khi bạn đánh **route print**. Chúng ta hãy đi xem xét một số ví dụ về cách cấu hình định tuyến tĩnh bằng lệnh **route:**

- Hiển thị bảng định tuyến tĩnh sử dụng lệnh **route print**.



Hình 2.5: Hiển thị bản định tuyến IP trong Windows Server 2008

Trong phần đầu ra của lệnh **route print**, thứ quan trọng nhất mà bạn sẽ thấy ở đây là danh sách giao diện. Các giao diện Windows Server IP được dán nhãn bằng số giao diện. Số giao diện trong hình 1 là 16, 14, 1, 15, 20, và 12. Các số giao diện này được sử dụng bất cứ khi nào bạn bổ sung hoặc xóa các tuyến trong bảng định tuyến. Bảng này thể hiện cho chúng ta thấy được các đích đến của mạng, network mask, default gateway, interface, và metric.

- Thêm một tuyến tĩnh bằng lệnh **route add**:

  route add 1.1.1.0 mask 255.255.255.0 10.0.1.1 if 1

- Xóa một tuyến tĩnh bằng lệnh **route delete**:

2.5.2. Đinh tuyến động trong Windows Server 2008 bằng RIPV2

2.5.2.1. Cài đặt RIPV2

- Mở Sever Manager,add Role chọn **Network Policy and Access Sevices** rồi chọn **Routing and Remote Access** để Install.
- Sau khi đã cài đặt xong,mở cửa sổ Routing and Remote Access,right click vào tên máy chủ chọn **Configure and Enable Routing and Remote Access**.

- Sau đó chọn cài đặt **LAN ROUTING**, tiếp đến chọn khởi chạy dịch vụ. Bạn có thể thấy **Network Interfaces** được điều khiển bởi RRAS và các cấu hình cụ thể cho IPV4 và IPV6.
- Tại đây, mở rộng phần **IPV4**, vào **General**, sau đó vào **New Routing Protocol.**
- Tiếp đến, chọn **RIPV2** với tư cách là giao thức định tuyến của mình.Như vậy là đã hoàn tất việc cài đặt **RIPV2**.

2.5.2.2. Cấu hình RIPv2

- Vào phần **RIP** ở cửa sổ **Routing and Remote Access** chọn **New Interface** sau đó chọn giao diện mà bạn muốn bổ sung trong RIP**.**
- Sau khi chọn giao diện, bạn sẽ có tùy chọn cấu hình một loạt các thuộc tính kết nối RIP. Khi bạn đã bổ sung thêm các giao diện RIP, hãy kiểm tra xem bạn có gửi và nhận các đáp trả trên các giao diện RIP không. Bạn cũng có thể kiểm tra xem mình có bất kỳ RIP lân cận nào không bằng cách kích phải vào giao thức RIP, sau đó click **Show Neighbors.**

2.6. Cài đặt và cấu hình hệ thống quản lý tài nguyên phân tán (DFS)

DFS (Distributed File System) là một hệ thống tập hợp các tài nguyên chia sẻ từ nhiều các máy chủ lưu trữ khác nhau. Điều này giúp cho bạn quản lý các tài nguyên chia sẻ trong công ty một cách hiệu quả và khoa học, giúp cho người dùng có thể tìm kiếm một tài nguyên chia sẻ nào đó một cách dễ dàng.

Có 2 loại DFS là:

- **Domain-based namespace**: Hoạt động trên môi trường Active Directory, có tính dung lỗi cao. Cho phép đồng bộ dữ liệu dùng chung giữa các Servertrong hệ thống Domain.

- **Stand-alone namespace**: Hoạt động trên môi trường Workgroup, không có tính dung lỗi vì DFS chỉ hoạt động trên một máy tính độc lập.

2.6.1. Các bước cấu hình

- Vào công cụ **Server Manager** ,chọn **Roles**,**Add Roles**, chọn vào mục **File Services** để cài đặt vai trò của các dịch vụ về tập tin.
- Trong hộp thoại **Selected Role Services**, cho phép ta lựa chọn chi tiết các dịch vụ về tập tin. Ta chọn vào các mục như **Distributed File System, File Server Resource Manager**.
- Trong hộp thoại **Create a DFS Namespace**, ta chọn vào mục

Create a namespace later using the DFS Management snap-in Server Manager để có thể tạo tên Namespace sau.

- Trong hộp thoại **Set Report Options**, cho phép lưu trữ các báo cáo về hệ thống DFS, ta để mặc định các báo cáo sẽ được lưu trữ trong đường dẫn Code: **C:\StorageReports**. Sau đó tiến hành cài đặt.
- Sau khi cài đặt xong, trong **Server Manage**r, vào **Roles\ File Services**. Vào mục **System Services**, ta chọn 2 mục **DFS Namespace** và **File Server Storage Report Manager** rồi chọn **Start** để khởi động 2 dịch vụ trên.

2.6.2. Cấu hình dịch vụ DFS

1. ***Tạo Namespace***

- Vào **Administrative Tools** ,chọn **DFS Management**.
- Trong hộp thoại **Namespace Server**,chọn **Browse** và chỉ định máy Server là gốc cây DFS.
- Trong hộp thoại **Namespace Name and Settings**, đặt tên cho namespace.
- Trong hộp thoại **Namespace Type**, cho phép lựa chọn kiểu của namespace trên miền **(Domain-based)** hay máy đơn **(Stand-alone).**
- Trong hộp thoại **Review Settings and Create Namespace**, chọn **Create** để tạo mới một namespace trên cây **DFS**.
- Sau khi tạo xong,trong cửa sổ giao diện công cụ **DFS Management**, sẽ thấy được một namespace tên **Public_Data** đã được tạo trên kiểu **Domain-based**.

2. ***Thêm một tài khoản máy vào Namespace***

- Để tạo thêm một namespace Server, chuyển sang một máy member server khác, cài đặt **Role File Service** giống như máy đầu tiên. Sau đó, chuyển về máy tính hiện hành, chọn **Add Namespace Server**.
- Trong hộp thoại **Add Namespace Server**, chọn **Browse**.
- Trong hộp thoại **Select Computer**, chọn **Advanced**.
- Trong hộp thoại kế tiếp, chọn nút **Find Now** và lựa chọn tài khoản máy Server cần thêm vào. Chọn **OK** để hoàn tất.

3. ***Đồng bộ dữ liệu giữa các máy Server trong một Namespace***

- Trong cửa sổ chính của công cụ **DFS Management**,right click

mục **Replication** chọn **New Replication Group**.

- Trong hộp thoại **Replication Group Type**, chọn mục **Multipurpose replication group** để cho phép 2 hoặc nhiều hơn các Server trong namespace đồng bộ dữ liệu với nhau. Nếu chọn mục **Replication group for data collection** thì sẽ có được sự đồng bộ 2 chiều từ các Server trong namespace, ngoài ra còn có thể lựa chọn các loại dữ liệu để đồng bộ.
- Trong hộp thoại **Name and Domain**, trong mục **Name of replication group** nhập vào tên của nhóm đồng bộ dữ liệu.
- Trong **Replication Group Members**, chọn nút **Add** để thêm vào các máy Server tham gia nhóm **Replication group**.
- Trong hộp thoại **Topology Selection**, chọn kiểu kiến trúc đồng bộ của các máy trong **Replication group**, chọn **Full mesh**.
- Trong hộp **thoại Replication Group Schedule and Bandwith**, có thể chọn vào mục **Replicate continuously using the specified banwidth** để định thời gian đồng bộ 24/7.Bạn cũng có thể chọn vào mục **Bandwidth** để định băng thông đồng bộ. Ngoài ra, bạn có thể chọn vào mục **Replicate during the specified days and times**, chọn nút **Edit Schedule** để lập lịch chỉ định thời gian đồng bộ giữa các Server và băng thông tương ứng.
- Trong hộp thoại **Primary Member**, chọn một **Server** trong nhóm **Replication** làm máy chính.
- Trong hộp thoại **Folders to Replicate**, chọn nút **Add** để lựa chọn một thư mục trên máy **Primary** mà muốn đồng bộ với các máy thành viên khác trong nhóm **Replication**.
- Trong hộp thoại **Add Folder to Replicate**, chọn nút **Browse** để chỉ ra thư mục để đồng bộ dữ liệu.
- Trong hộp thoại **Local Path of Public_Data on Other Members**, cho phép nhập vào đường dẫn mà thư mục đồng bộ dữ liệu sẽ lưu trữ trên máy member khác, chọn **Edit**.
- Trong hộp thoại **Edit**, chọn nút **Browse**.
- Chọn đường dẫn **C:\DFSRoots\Public_Data**. Chọn **OK**.
- Trong hộp thoại **Review Settings** and **Create Replication Group**, chọn **Create**.
- Trong hộp thoại **Confirmation**, chọn **Close** để hoàn tất.
- Trong hộp thoại **Replication Delay**, chọn **OK**.

CHƯƠNG 3: QUẢN TRỊ HỆ THỐNG TRÊN WINDOWS SERVER 2008

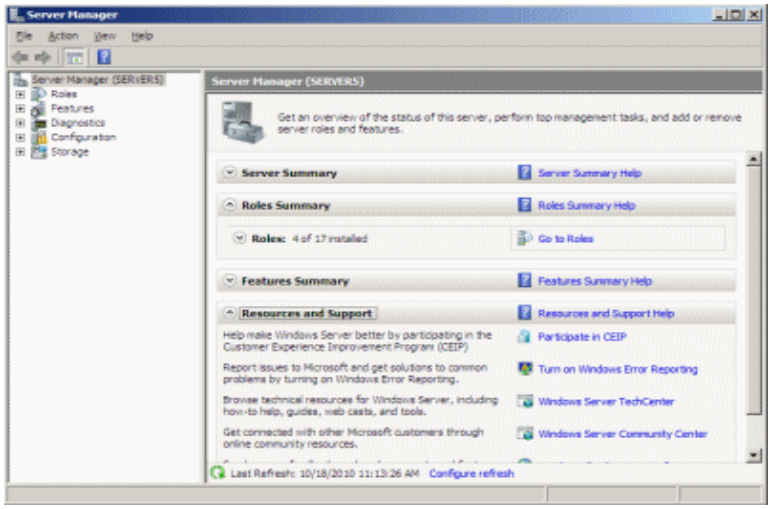
3.1. Sử dụng công cụ quản trị Server Manager trên Windows Server 2008

Server Manager là một công cụ che phép bạn thực hiện hầu hết các thao tác quản trị trên Windows Server 2008, từ các dịch vụ server như Active Directory, DNS, DHCP, … đến các thành phần của hệ thống như .NET Framework 3.0, Network Load Balancing, Group Policy Management, … ; từ hệ thống firewall, quản lý user và group đến các dịch vụ sao lưu hệ thống, quản lý đĩa, …

3.1.1. Giới thiệu về Server Manage

Có thể nói rằng công cụ này là kết quả của sự kết hợp hoàn hảo các công cụ quản lý trên những phiên bản Windows trước đó. Theo mặc định, Server Manager sẽ tự động khởi động ngay sau khi bạn đăng nhập vào hệ thống. Nếu đã đóng cửa sổ này, bạn có thể thực hiện một trong những cách sau để mở lại :

- Kích chuột phải vào biểu tượng **Computer** trên desktop, chọn **Manage**.
- Từ menu **Start**, chọn **Programs/Administrative Tools/Server Manager**.
- Từ menu **Start**, chọn **Control Panel/Administrative Tools/Server Manager**.
- Kích chọn biểu tượng **Server Manager** trên **Quick Launch** của Taskbar.



Hình 3.1: Giao diện chính của Server Manager

3.1.2. Các thành phần trong Server Manager

Khi làm việc với Server Manager, bạn sẽ tương tác với 5 thành phần chính :

- **Roles** cho phép bổ sung và loại bỏ các dịch vụ của server. Tại đây bạn cũng có thể quản lý chi tiết dữ liệu tương ứng với mỗi dịch vụ.
- **Features** cho phép bổ sung và loại bỏ các thành phần trên Windows Server 2008. Chức năng này tương tự như **Add/Remove Windows Components** trong các phiên bản Windows trước đó.
- **Diagnostics** tích hợp các thành phần **Event Viewer, Reliability and Performance** và **Device Manager**.
- **Configuration** bao gồm các công cụ **Local Users And Group, Task Scheduler, Windows Firewall with Advanced Security, WMI Control**và **Services**. WMI Control được dùng để quản lý các dịch vụ Windows Management Instrumentation.
- **Storage** tích hợp hai công cụ **Windows Server Backup** và **Disk Management**.

3.1.3. Quản trị hệ thống với Server Manager

- **Quản lý các dịch vụ Server (Roles)**

Để mở các cửa sổ quản lý các dịch vụ server, bạn chọn mục **Roles** ở khung bên trái của màn hình**Server Manager**. Trên Windows Server 2008 nói chung, bạn có thể triển khai tất cả 16 dịch vụ server, từ Active Directory Domain Services đến các server như DHCP, DNS, Web, …
Lưu ý : ngoài 16 dịch vụ server có mặt trên tất cả các phiên bản Windows Server 2008, Microsoft còn cung cấp một dịch vụ server nữa, đó là Hyper-V. Hyper-V là công nghệ ảo hóa chỉ chạy trên các nền tảng hệ điều hành 64-bit.

Để cài đặt một dịch vụ server bất kỳ, bạn đánh dấu chọn vào ô tương ứng trên hộp thoại **Select Server Roles**. Tiếp theo, bấm nút **Install** để bắt đầu. Trong tiến trình cài đặt, tùy theo đặc điểm riêng của từng dịch vụ server, bạn sẽ điền thông tin và thực hiện các thao tác cần thiết để hoàn thành tiến trình.

Các dịch vụ Server trên Windows Server 2008 Sau khi cài đặt xong, thông tin và trạng thái của các dịch vụ server sẽ hiển thị trong khung **Roles Summary** thuộc cửa sổ **Server Manager**. Tại đây bạn cũng có thể thực hiện các thao tác bổ sung và loại bỏ các dịch vụ

server này. Nếu muốn quản lý chi tiết dữ liệu tương ứng với mỗi dịch vụ server, bạn kích chọn dịch vụ đó ở ngay dưới mục **Roles**.

- **Quản lý các thành phần (Features)**

Để mở cửa sổ quản lý các thành phần, bạn chọn mục **Features** ở khung bên trái của màn hình **Server Manager**. Trên Windows Server 2008 bạn có thể tương tác với tất cả 35 thành phần. Để cài đặt một thành phần bất kỳ, bạn đánh dấu chọn vào ô tương ứng trên hộp thoại **Select Features**. Tiếp theo, bấm nút **Install** để bắt đầu. Trong tiến trình cài đặt, tùy theo đặc điểm riêng của từng thành phần, bạn sẽ điền thông tin và thực hiện các thao tác cần thiết để hoàn thành tiến trình.

Các thành phần trên Windows Server 2008 Sau khi cài đặt xong, thông tin và trạng thái của các thành phần sẽ hiển thị trong khung **Features Summary** thuộc cửa sổ **Server Manager**. Tại đây, bạn cũng có thể thực hiện các thao tác bổ sung và loại bỏ các thành phần này.

Task Scheduler là công cụ cho phép bạn lập lịch để thực thi các nhiệm vụ trên hệ thống theo yêu cầu của mình.

3.2. Tài khoản người dùng, tài khoản máy tính, nhóm và đơn vị tổ chức

3.2.1. Tài khoản người dùng(User Acount)

Trong hệ thống mạng Windows Server 2008, người dùng muốn truy cập vào tài nguyên mạng cần phải có một user acount.Với user acount này,người dùng sẽ được chứng thực và cấp phát quyền truy cập.

Một user acount là một đối tượng chứa tất cả các thông tin định nghĩa một người dùng trong Windows Server 2008.

Windows Server 2008 có 3 kiểu user acount:

- **User acount domain**: được tạo trên máy chủ DC.User này có thể logon vào bất kỳ các máy Client nào trên mạng.User được tạo trên DC thì mặc định tài khoản này sẽ là Domain user,thuy nhiên có thể gán quyền cho user vào nhóm [Member of] để có các quyền khác.
- **Built in acount**: là các tài khoản được tạo sẵn khi cài hệ điều hành và thăng cấp thành DC.Mục đích là để trao quyền đặc biệt cho người dùng trên hệ điều hành.Ví dụ một số Built in acount:
  - Administrator
  - Account operator

- Backup operator
- Print operator
- Guest

- **Local user acount:** 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.

3.2.2. Tài khoản máy tính(Computer Acount)

- **Computer acount:** Dùng để xác định một máy tính trong Domain**,** cung cấp các thông tin để người quản trị có thể xác định và kiểm tra quyền truy cập các tài nguyên trên mạng**.**
- Computer Account sẽ được tạo ra khi một máy tính tham gia vào domain

3.2.3. Nhóm(Group)

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).

- **Nhóm bảo mật**

Nhóm bảo mật là loại nhóm được dùng để cấp phát các quyền hệ thống (rights) và quyền truy cập(permission). 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.

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.

- **Nhóm phân phối.**

Nhóm phân phối là một loại nhóm phi bảo mật,không cấp phép truy cập tài nguyên.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 phố thư (e-mail) hoặc các tin nhắn (message). Bạn sẽ gặp lại loại nhóm này khi làm việc với phần mềm MS Exchange.

3.2.4. Đơn vị tổ chức(OU-Organizational Unit)

OU là đơn vị tổ chức nằm dưới cấp độ miền. nó được xem là một vật chứa các đối tượng được dùng để sắp xếp các đối tượng khác nhau phục vụ cho mục đích quản trị của bạn. Việc sử dụng OU có hai công dụng chính sau:

- Trao quyền kiếm soát một tập hợp các tài khoản người dùng, máy tính hay các thiết bị mạng cho một nhóm người hay một phụ tá quản trị viên nào đó (sub-administrator), từ đó giảm bớt công tác quản trị cho người quản trị toàn bộ hệ thống.
- Kiểm soát và khóa bớt một số chức năng trên các máy trạm của người dùng trong OU thông qua việc sử dụng các đối tượng chính sách nhóm (GPO).

3.3. Quản trị môi trường làm việc người dùng, máy tính sử dụng chính sách nhóm

- Triển khai phần mềm ứng dụng: bạn có thể gom tất cả các tập tin cần thiết để cài đặt một phần mềm nào đó vào trong một gói (package), đặt nó lên Server, rồi dùng chính sách nhóm hướng một hoặc nhiều máy trạm đến gói phần mềm đó. Hệ thống sẽ tự

động cài đặt phần mềm này đến tất cả các máy trạm mà không cần sự can thiệp nào của người dùng.

- Gán các quyền hệ thống cho người dùng: chức năng này tương tự với chức năng của chính sách hệ thống. Nó có thể cấp cho một hoặc một nhóm người nào đó có quyền tắt máy server, đổi giờ hệ thống hay backup dữ liệu…
- Giới hạn những ứng dụng mà người dùng được phép thi hành: chúng ta có thể kiểm soát máy trạm của một người dùng nào đó và cho phép người dùng này chỉ chạy được một vài ứng dụng nào đó thôi như: Outlook Express, Word hay Internet Explorer.
- Kiểm soát các thiết lập hệ thống: bạn có thể dùng chính sách nhóm để qui định hạn ngạch đĩa cho một người dùng nào đó. Người dùng này chỉ được phép lưu trữ tối đa bao nhiêu MB trên đĩa cứng theo qui định.
- Thiết lập các kịch bản đăng nhập, đăng xuất, khởi động và tắt máy.

3.4. Quản lý và cấp phép quyền truy cập tài nguyên

Windows Server 2008 có 2 cơ chế cấp phát quyền:

- Folder Permission
- NTFS(New Technology File System)

3.4.1. Folder Permission

- Read: quyền này cho phép user có thể xem nội dung và thuộc tính file.
- Change:ngoài xem nội dung và thuộc tính file người dùng còn có thể xóa hay tao tạo file,xóa thư mục(do user đó tạo ra).
- Full control: bao gồm cả quyền read và change;thêm vào đó user còn có thể thay đổi chủ sở hữu của thư mục hoặc file(do user đó tạo ra).

3.4.2. NTFS

Hỗ trợ người dùng nhiều quyền hơn.

- Read
- Write: user có khả năng thay đổi nội dung file nhưng không thể xóa.
- Modify = Read + Write và có khả năng xóa file,thư mục.
- Full = Read + Write + Modify và có khảanawn thay đổi chủ sở hữu

trên các file và folder.

----------HẾT----------

KẾT QUẢ ĐẠT ĐƯỢC VÀ HƯỚNG PHÁT TRIỂN CỦA ĐỀ TÀI

Dưới sự hướng dẫn tận tình của thầy giáo hướng dẫn và sự tìm tòi nghiên cứu của các thành viên trong nhóm,cơ bản chúng em đã xây dựng được một hệ thống mạng Windows Server 2008 và quản trị nó một cách cơ bản nhất,tổng quan nhất.

Để thực sự trở thành những nhà quản trị viên giỏi,nhóm em sẽ tích cực tìm hiểu chuyên sâu về quản trị hệ thống mạng Windows Server 2008,tìm hiểu về những sự cố có thể xảy ra trong một hệ thống mạng và cách khắc phục chúng.

Kính mong các thầy cô đóng góp ý kiến để bài báo cáo thực tập của nhóm em được hoàn chỉnh hơn.

Chúng em xin trân thành cảm ơn!

TÀI LIỆU THAM KHẢO

1. www.Microsoft.com
2. www.Quantrimang.com.vn
3. Windows Server 2008 unleashed
4. www.itnews.com.vn