

BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP.HCM



KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM

ĐỒ ÁN MÔN HỌC: QUẢN TRỊ MẠNG

ĐỀ TÀI:

QUẢN LÝ ĐĨA TRÊN WINDOWS SERVER 2008

Giảng viên hướng dẫn : ThS.Tù Thanh Trí

Sinh viên thực hiện : Trần Tiến Đạt

Nguyễn Trường Thuận

Lớp : 03ĐHCNTT2

Khóa : 2014 – 2018

TP. Hồ Chí Minh, tháng 3 năm 2017

BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP.HCM

KHOA: HỆ THỐNG THÔNG TIN VÀ VIỄN THÁM



ĐỒ ÁN MÔN HỌC: QUẢN TRỊ MẠNG

ĐỀ TÀI:

QUẢN LÝ ĐĨA TRÊN WINDOWS SERVER 2008

Giảng viên hướng dẫn : ThS.Tù Thanh Trí

Sinh viên thực hiện : Trần Tiến Đạt

Nguyễn Trường Thuận

Lớp : 03ĐHCNTT2

Khóa : 2014 – 2018

TP. Hồ Chí Minh, tháng 3 năm 2017

MỞ ĐẦU

- Lý do chọn đề tài

Cùng với phát triển của công nghệ thông tin thì số lượng người biết sử dụng máy tính ngày càng nhiều. Các dịch vụ trên máy tính đã thâm nhập vào hầu hết các lĩnh vực trong xã hội. Các nhu cầu quản lý trên máy tính dần trở nên quan trọng đối với người sử dụng. Đối với doanh nghiệp thì việc quản lý càng trở nên được xem trọng. Nhận thấy được tầm quan trọng của việc quản lý, vì vậy nhóm em chọn đề tài "Nghiên cứu và ứng dụng quản lý đĩa trên Server 2008" cho đồ án lần này.

- Mục đích nghiên cứu

Mục đích của đồ án là nghiên cứu, ứng dụng vào thực tiễn việc quản lý đĩa trên Windows Server 2008 R2.

- Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu của đồ án là việc quản lý đĩa trên Windows Server 2008 R2 hiện nay.

Phạm vi nghiên cứu: Các thuộc tính, cũng như ứng dụng của việc quản lý đĩa

- Phương pháp nghiên cứu

Phương pháp phân tích, phương pháp mô hình hóa, giải thuật, phương pháp mô phỏng, thực nghiệm, phân tích, đánh giá, ...

- Đồ án được chia thành 4 chương:
 - Chương 1: Tổng quan về Window Server 2008 R2

Khái quát một số đặc điểm chính của Windows Server 2008 R2, các thuộc tính cũng như các khả năng của hệ điều hành

- Chương 2: Quản lý đĩa

Phân tích cấu hình hệ thống thông tin và cấu hình đĩa lưu trữ

Phân tích việc mã hóa dữ liệu EFS

- Chương 3: Thực nghiệm

Trong chương này nhóm sẽ mô phỏng việc tạo các loại đĩa và tạo nên 1 file EFS và mã hoá chúng, thiết lập hạn ngạch

- Chương 4: Kết luận

LỜI CẢM ƠN

Chân thành cảm ơn thầy **TÙ THANH TRÍ** đã tạo cơ hội cho nhóm để tìm hiểu về đề tài “Nghiên cứu và ứng dụng quản lý đĩa trên Server 2008”.

Trong quá trình thực hiện đồ án nhóm đã có nhiều cố gắng và nỗ lực để thực hiện đồ án một cách hoàn chỉnh nhất, tuy nhiên vẫn xảy ra một số thiếu sót vì kiến thức chuyên môn trong lĩnh vực chưa sâu rộng, tài liệu chưa đầy đủ rõ ràng, và một số vấn đề khác. Chúng em rất mong nhận được sự đóng góp của thầy để nhóm nâng cao kiến thức về chuyên môn cũng như khả năng viết báo cáo và xây dựng đồ án.

Xin chân thành cảm ơn thầy.

NHẬN XÉT

Điểm sinh viên 1 :

ĐIỂM

Điểm sinh viên 2 :

Mục Lục

[Chương 1 Tổng quan Windows Server 2008 R2 1](#)

[**1.1 Giới thiệu về Windows Server 2008 R2 1**](#)

[**1.1.1 Ứng dụng nền tảng Web 1**](#)

[**1.1.2 Ảo hóa 2**](#)

[**1.1.3 Linh hoạt và khả năng mở rộng 3**](#)

[**1.1.4 Hoạt động tốt hơn khi kết hợp với Client 4**](#)

[Chương 2 Quản lý đĩa 7](#)

[**2.1 Cấu hình hệ thống tập tin 7**](#)

[**2.1.1 File system là gì? 7**](#)

[**2.1.2 Các loại File system 7**](#)

[**2.2 Cấu hình đĩa lưu trữ 9**](#)

[**2.2.1 Basic Disk 9**](#)

[**2.2.2 Dynamic Disk 12**](#)

2.3 Chương trình Disk Manager 16

2.3.1 Công cụ quản lý Disk Management 16

2.3.2 Thuộc tính của Volume (hoặc Đĩa) cục bộ 16

2.4 Mã hóa dữ liệu EFS 17

2.4.1 Nén dữ liệu 17

2.4.2 Tổng quan về mã hóa EFS 18

2.4.3 Thuật toán 3DES 20

2.4.4 Phương thức mã hóa dữ liệu của EFS 22

2.2.5 Quá trình mã hóa tập tin của EFS 22

2.4.6 Quá trình giải mã tập tin của EFS 23

2.5 Thiết lập hạn ngạch đĩa 23

Chương 3 Thực nghiệm 26

3.1 Convert Basic Disk to Dynamic Disk 26

3.2 Tạo phân vùng cho Basic Disk 28

3.3 Tạo các loại Volume cho Dynamic Disk 30

3.3.1 Tạo Spanned Volume 30

3.3.2 Tạo Striped Volume 32

3.3.3 Tạo Mirrored Volume 35

3.3.4 Tạo RAID-5 Volume 40

3.4 Mã hóa 42

3.5 Cấu hình hạn ngạch đĩa 55

Chương 4 Kết luận 62

4.1 Thuận lợi và khó khăn 62

4.2 Hướng phát triển 63

4.3 Tổng kết 63

Mục lục hình ảnh

Hình 1.1.1 Internet Information Services (IIS) 7.5 1

Hình 1.1.2a Microsoft® Hyper-V™ 2

Hình 1.1.2b Presentation Virtualization 3

Hình 1.1.3 Linh hoạt và khả năng mở rộng 4

Hình 1.1.4a Direct Access 5

Hình 1.1.4b BranchCache 6

Hình 2.2.1a Basic Disk 10

Hình 2.2.1b MBR (master boot record) 11

Hình 2.2.1c GPT (GUIDs partition table) 12

Hình 2.2.2a Dynamic Disk 13

Hình 2.2.2b Simple Volume 13

Hình 2.2.2c Spanned Volume 14

Hình 2.2.2d Striped Volume 14

[Hình 2.2.2e Mirror volume \(RAID-1\) 15](#)

[Hình 2.2.2f RAID-5 volume 15](#)

[Hình 2.3.1 Disk Management 16](#)

[Hình 2.3.2 Thuộc tính của Volume/ đĩa cục bộ 17](#)

[Hình 2.4.2 Mã hóa EFS 19](#)

[Hình 2.4.3a Symmetric Encryption: 3DES 20](#)

[Hình 2.4.3b Thuật toán 3DES 20](#)

[Hình 2.5.1 Thiết lập hạn ngạch đĩa 24](#)

[Hình 3.1a Convert Basic Disk to Dynamic Disk 26](#)

[Hình 3.1b Chọn đĩa để convert 27](#)

[Hình 3.1c Sau khi convert sang Dynamic Disk 27](#)

[Hình 3.2a New Simple Volume 28](#)

[Hình 3.2b Specify Volume Size 28](#)

[Hình 3.2c Format Partition 29](#)

[Hình 3.2d Hoàn tất tạo Simple Volume 29](#)

[Hình 3.3.1a New Spanned Volume 30](#)

[Hình 3.3.1b Select Disks \(Spanned Volume\) 31](#)

[Hình 3.3.1c Format Volume \(Spanned Volume\) 31](#)

[Hình 3.3.1d Tao thành công Spanned Volume 32](#)

[Hình 3.3.2a New Striped Volume 33](#)

[Hình 3.3.2b Select Disk \(Striped Volume\) 33](#)

[Hình 3.3.2c Format Volume \(Striped Volume\) 34](#)

[Hình 3.3.2d Đã tạo thành công Striped Volume 35](#)

[Hình 3.3.3a New Mirrored Volume 36](#)

[Hình 3.3.3b Select Disks \(Mirrored Volume\) 36](#)

[Hình 3.3.3c Format Volume \(Mirrored Volume\) 37](#)

[Hình 3.3.3d Đã tạo thành công Mirrored Volume 38](#)

[Hình 3.3.3e Tao Mirror để dự phòng 39](#)

[Hình 3.3.3f Add Mirror 39](#)

[Hình 3.3.3g Đã Add Mirror thành công 40](#)

[Hình 3.3.4a New RAID-5 Volume 40](#)

[Hình 3.3.4b Select Disks \(RAID-5 Volume\) 41](#)

[Hình 3.3.4c Format Volume \(RAID-5 Volume\) 41](#)

[Hình 3.3.4d Đã tạo thành công RAID-5 Volume 42](#)

[Hình 3.3.5a Remove Mirror 43](#)

[Hình 3.3.5b Repair RAID-5 Volume 44](#)

[Hình 3.4.1 Tao File PC01 45](#)

[Hình 3.4.2 Properties folder 45](#)

[Hình 3.4.3 Advanced Attributes 46](#)

[Hình 3.4.4 Confirm Attribute Changes 46](#)

[Hình 3.4.5 Tập tin đã được mã hóa 47](#)

[Hình 3.4.6 Access is denied 47](#)

[Hình 3.4.7 Error Applying Attributes 48](#)

[Hình 3.4.8 Run MMC 48](#)

[Hình 3.4.9 Console Root 48](#)

[Hình 3.4.10 Add or Remove Snap-ins 49](#)

[Hình 3.4.11 Certificates 49](#)

[Hình 3.4.12 Export 50](#)

[Hình 3.4.13 Certificate Export Wizard 50](#)

[Hình 3.4.14 Export Private Key 51](#)

[Hình 3.4.15 Export File Format 51](#)

[Hình 3.4.16 Pasword 52](#)

[Hình 3.4.17 File to export 52](#)

[Hình 3.4.18 Finish export 53](#)

[Hình 3.4.19 The export was successful 53](#)

[Hình 3.4.20 Certificate Import Wizad 54](#)

[Hình 3.4.21 File to import 54](#)

[Hình 3.4.22 Pasword Import 55](#)

[Hình 3.4.23 Certificate Store 55](#)

[Hình 3.4.24 Finish Import 56](#)

[Hình 3.4.25 The import was successful 56](#)

[Hình 3.4.26 Certificates đã được import 57](#)

[Hình 3.4.26 Giải mã thành công 57](#)

[Hình 3.5.1 Tab Quota 58](#)

[Hình 3.5.2 Enable quota management 59](#)

[Hình 3.5.3 Tùy chỉnh giới hạn cho phép và cảnh báo 60](#)

[Hình 3.5.4 Áp dụng hạn ngạch 60](#)

[Hình 3.5.5 Copy Item \(PC01\) 61](#)

[Hình 3.5.6 Quota Entries for Quota \(D:\) 62](#)

[Hình 3.5.7 New Quota Entry 62](#)

[Hình 3.5.8 Select Users 63](#)

[Hình 3.5.9 Add New Quota Entry 63](#)

[Hình 3.5.10 Thiết lập thành công 63](#)

[Hình 3.5.11 Copy Item \(PC02\) 64](#)

Chương 1 Tổng quan Windows Server 2008 R2

•

1. Giới thiệu về Windows Server 2008 R2

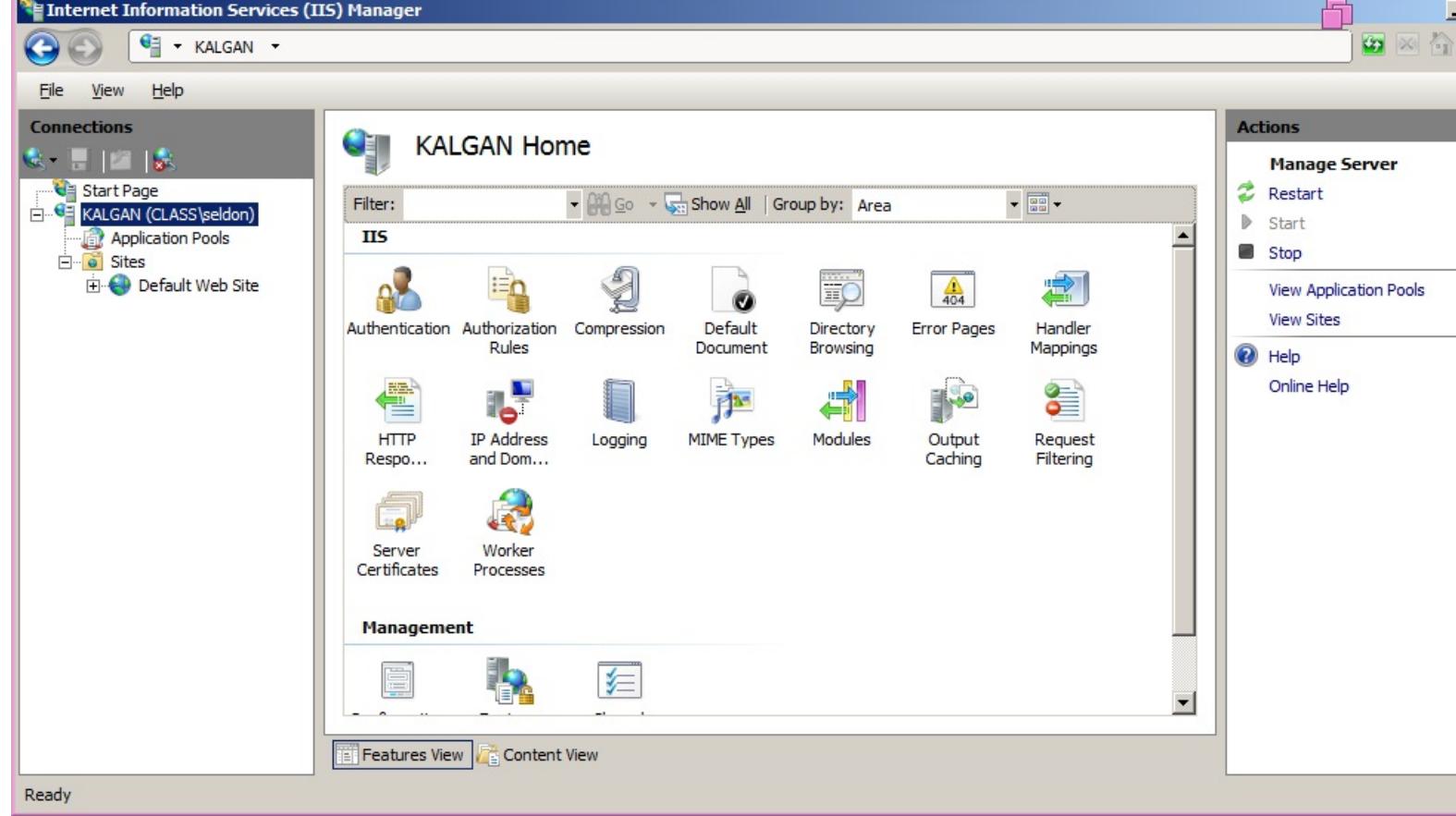
Sự ra đời của Windows Server 2008 R2 dựa trên sự thành công của phiên bản trước đó là Windows Server 2008 và sản phẩm mới này được cải tiến thêm một số công nghệ và tính năng nổi trội giúp chúng ta, những người tham gia quản lý hệ thống già tăng sự ổn định, linh hoạt cho hạ tầng các server trong hệ thống của

mình. Mặc khác Virtualization tools, web resources, tích hợp với client Windows 7... trong dòng hệ điều hành mới này được cải tiến đáng kể, và đó sẽ là một phần quan trọng không thể bỏ qua nếu bạn có kế hoạch triển khai hoặc nâng cấp mới hệ thống.

Như đã đề cập bên trên thì ở phiên bản Windows Server 2008 R2 Microsoft đã có những cải tiến đáng kể trong công nghệ và tính năng mới, hỗ trợ trong việc quản lý và vận hành hệ thống. Sau đây tôi sẽ liệt kê một vài tính năng được tập trung thay đổi:

1. Ứng dụng nền tảng Web

Windows Server 2008 R2 tập hợp những cải tiến mạnh mẽ dành cho nền tảng ứng dụng Web. Nó đưa ra nhiều cập nhật cho web server role, Internet Information Services (IIS) 7.5, hỗ trợ tối đa cho .NET trên nền server core. Thiết kế tập trung vào cải tiến IIS 7.5 cho phép người quản trị Web dễ dàng triển khai và quản lý các ứng dụng web, tăng độ tin cậy và khả năng mở rộng dễ dàng.Thêm vào đó, IIS 7.5 còn có khả năng sắp xếp hợp lý và cung cấp nhiều khả năng tùy chỉnh trong môi trường Web.



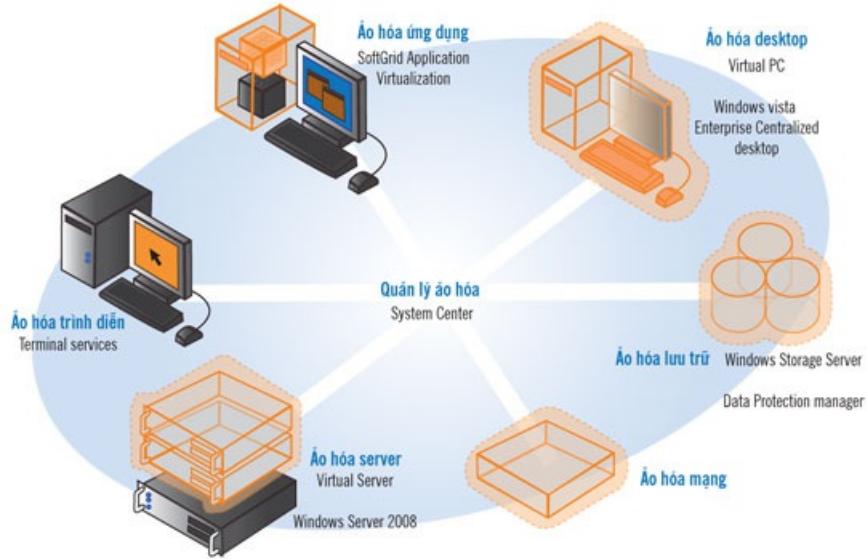
Hình 1.1.1 Internet Information Services (IIS) 7.5

1. Ảo hóa

Nhờ sự hoạt động có hiệu quả của công nghệ ảo hóa mà các trung tâm tổ chức có hoạt động liên quan đến lĩnh vực công nghệ thông tin đã tiết kiệm được rất lớn các chi phí về tiêu thụ năng lượng và công tác quản lý bảo trì trên diện rộng trong toàn hệ thống. Windows Server 2008 R2 cung cấp 2 loại hình về ảo hóa:

- Client và Server ảo hóa cung cấp bởi Hyper-V:

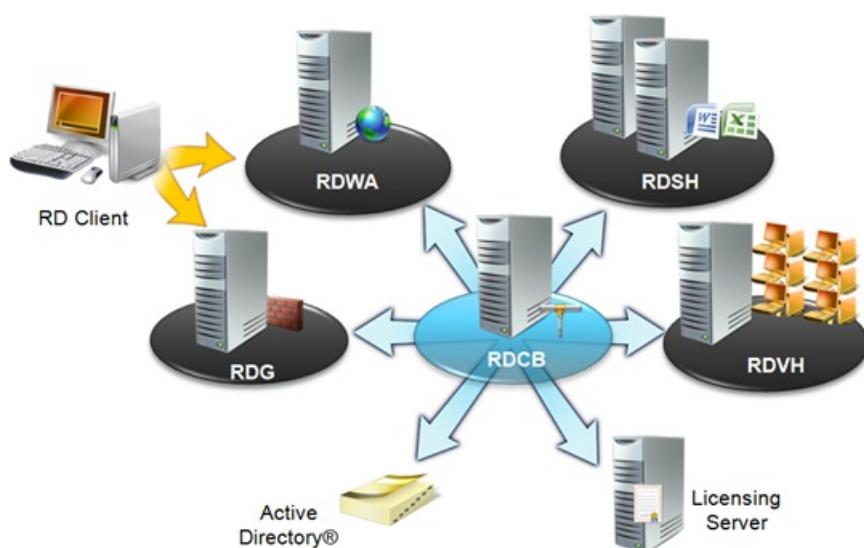
Microsoft® Hyper-V™ ảo hóa các tài nguyên hệ thống của máy tính vật lý. Nghĩa đơn giản là bạn có thể tạo ra thêm một hay nhiều máy tính ảo sử dụng tài nguyên vật lý từ 1 máy tính thật. Từ môi trường ảo hóa này bạn có thể chạy các hệ điều hành, ứng dụng và liên kết với các Client trong hệ thống một cách dễ dàng. Hyper-V tích hợp trong Windows Server 2008 R2, nó cung cấp độ tin cậy cao và tùy biến trong giải pháp về ảo hóa giúp cải thiện việc sử dụng máy chủ và giảm chi phí vận hành hệ thống.



Hình 1.1.2a Microsoft® Hyper-V™

- Presentation Virtualization:

Dịch vụ kết nối từ xa (Terminal Services) chắc không còn xa lạ với chúng ta trong những phiên bản trước đây của Windows Server. Nó giúp chúng ta có thể chạy những ứng dụng tại 1 vị trí xác định nhưng công việc đó được xử lý và điều khiển tại 1 vị trí khác. Trong Windows Server 2008 R2 tên gọi Terminal Services được thay thế bằng Remote Desktop Services (RDS). Để mở rộng những tính năng của RDS, Microsoft đã đầu tư phát triển vào Virtual Desktop Infrastructure (VDI) cùng với những đối tác như Citrix, Unisys, HP, Quest, Ericom và một vài đơn vị liên kết khác.

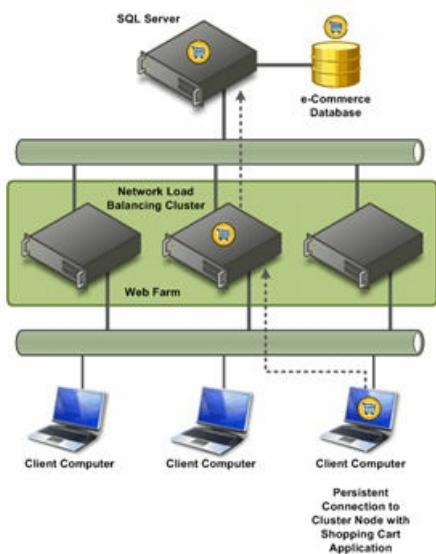


Hình 1.1.2b Presentation Virtualization

-
-

1. Linh hoạt và khả năng mở rộng

Windows Server 2008 R2 chỉ hỗ trợ trên nền vi xử lý 64 bit, điều này có nghĩa nó tận dụng tối đa khả năng xử lý và khả năng nâng cấp hầu như là không giới hạn cho hoạt động của hệ thống. Một loạt tính năng mới được cập nhật sẵn có trong windows, bao gồm tận dụng cấu trúc CPU, tăng thêm thành phần hệ thống, cải thiện hiệu suất và khả năng mở rộng cho ứng dụng – dịch vụ. Hyper-V cũng nằm trong tính năng tương thích ưu việt này, khả năng tương thích này cho phép các máy ảo di chuyển giữa các hệ thống khác nhau chỉ cần kiến trúc bộ vi xử lý trong hệ thống di chuyển đến và hệ thống cũ cùng nhà sản xuất.



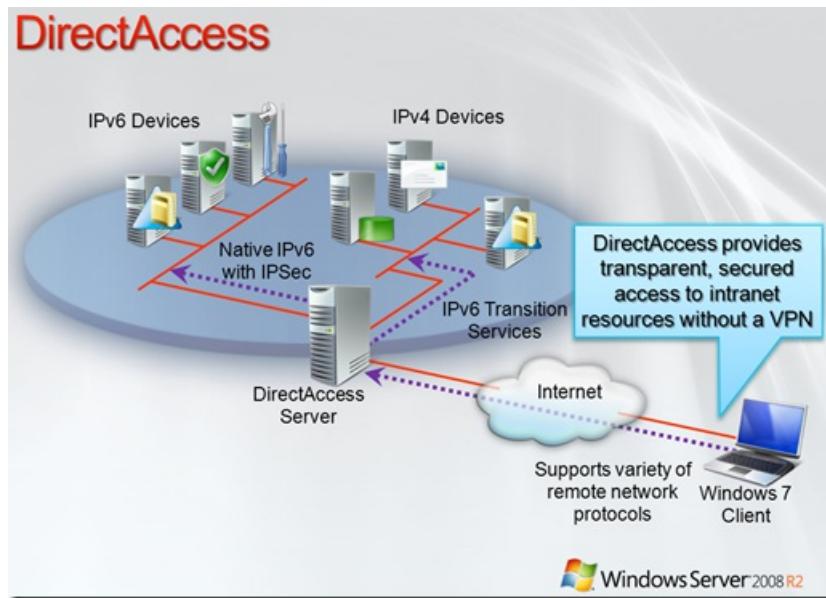
Hình 1.1.3 Linh hoạt và khả năng mở rộng

- - - 1. Hoạt động tốt hơn khi kết hợp với Client**

Windows Server 2008 R2 có một vài tính năng được thiết kế đặc biệt dành cho client sử dụng Windows 7, tạo sự tiện lợi tối đa và an toàn cho người dùng dựa trên công nghệ mới.

- **Đơn giản hóa các kết nối từ xa cho các máy tính sử dụng tính năng DirectAccess:**

Một trong những vấn đề thường phải đối mặt trong các tổ chức là kết nối từ xa cho người sử dụng thiết bị di động. Giải pháp được đưa ra và sử dụng rộng rãi hiện nay là mạng riêng ảo(VPN). Tùy theo loại VPN, mà người dùng có thể phải cài đặt phần mềm VPN client trên máy tính để kết nối vào tổ chức công ty của họ. Tính năng DirectAccess trong Windows Server 2008 R2 cho phép các máy tính client sử dụng Windows 7 kết nối trực tiếp với mạng nội bộ mà không có sự phức tạp của việc thiết lập kết nối VPN.



Hình 1.1.4a Direct Access

- **Đảm bảo kết nối bảo mật cho máy tính cá nhân và công cộng:**

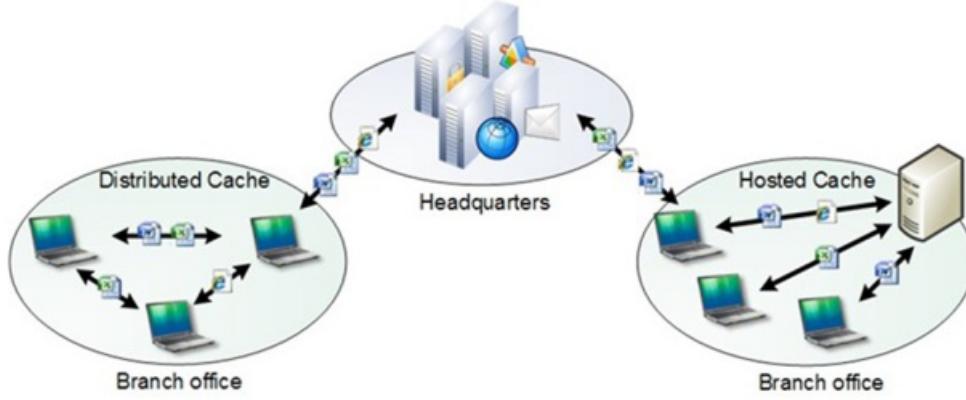
Vấn đề này được đề cập đến khi người dùng kết nối vào hệ thống mạng của tổ chức, cty họ nhưng máy tính đó không thuộc sở hữu tổ chức của người dùng mà nó thuộc về công cộng hoặc địa điểm cho thuê truy cập Internet. Hầu hết người dùng cũng không thể tự kết nối vào hệ thống của tổ chức dựa trên các công cụ có sẵn trên máy tính. Sự tích hợp của Remote Workspace, Presentation Virtualization và Remote Desktop Gateway cho phép người dùng sử dụng Windows 7 không phải cài thêm phần mềm nào trên máy tính mà vẫn kết nối vào hệ thống thao tác công việc như đang trên máy tính nội bộ.

- **Cải thiện hiệu suất làm việc trong các văn phòng chi nhánh:**

Thực tế thì hiện nay việc thành lập các chi nhánh phục vụ cho việc phát triển kinh doanh của các tổ chức là điều không thể thiếu. Để giảm thiểu chi phí cho hoạt động và quản lý của văn phòng chi nhánh các tổ chức đang tìm cách tập trung các ứng dụng về khu trung tâm. Tuy nhiên điều này cũng còn phụ thuộc vào liên kết WAN giữa các văn phòng chi nhánh và trung tâm ứng dụng, tuy nhiên liên kết này cũng là một phần chi phí hoạt động của doanh nghiệp.

Tính năng BranchCache trong Windows Server 2008 R2 và Windows 7 giúp giảm sự liên kết WAN bằng cách thường xuyên sử dụng thông tin từ bộ nhớ đệm cho các người dùng tại các văn phòng chi nhánh. Khi người dùng từ văn phòng chi nhánh gửi yêu cầu lấy dữ liệu từ các văn phòng trung tâm của họ, một bản sao nội dung văn bản đó sẽ được sao lưu lại tại văn phòng chi nhánh. Yêu cầu tiếp theo cũng với nội dung văn bản vừa rồi thì người dùng tiếp theo sẽ được cung cấp

tức thời thông qua Cache từ văn phòng chi nhánh, qua đó giảm việc sử dụng kết nối WAN cũng như chi phí kết nối.



Hình 1.1.4b BranchCache

Chương 2 Quản lý đĩa

2.1 Cấu hình hệ thống tập tin

2.1.1 File system là gì?

File system hay hệ thống tập tin có chức năng tổ chức và kiểm soát các tập tin và siêu dữ liệu tương ứng. Hệ thống tập tin sắp xếp dữ liệu được lưu trên đĩa cứng của máy tính, kiểm soát thường xuyên vị trí vật lý. Cho phép người dùng truy cập người dùng truy cập nhanh chóng và an toàn khi cần thiết.

File system làm việc như một hệ chỉ mục số, cho phép máy tính nhanh chóng tìm thấy một tập tin nào đó, bất chấp kích thước hay cấu hình của ổ đĩa lưu trữ.

Mọi hệ điều hành từ MS-DOS cho đến Windows 95, Windows Linux hay Windows Server 2008 đều có hệ thống tập tin riêng.

2.1.2 Các loại File system

Các hệ thống File trong Windows Server 2008 gồm 2 hệ thống chính là FAT và NTFS, trong đó NTFS là hệ thống file với nhiều đặc tính hiện đại mà hệ thống FAT không có.

- FAT được chia làm 2 loại: FAT16 và FAT32

FAT16 (File Allocation Table 16 bits): Với hệ điều hành MS-DOS, hệ thống tập tin FAT được công bố vào năm 1981 đưa ra một cách thức mới về việc tổ chức và quản lý tập tin trên đĩa cứng, đĩa mềm. Tuy nhiên, khi dung lượng đĩa cứng ngày càng tăng nhanh, FAT16 đã bộc lộ nhiều hạn chế. Với không gian địa chỉ 16bit, FAT16 chỉ hỗ trợ đến 65.536 clusters trên một partition, gây ra sự lãng phí dung lượng đáng kể (đến 50% dung lượng với những ổ đĩa cứng trên 2GB). FAT16 không hỗ trợ các partition lớn hơn 2GB.

FAT32 (File Allocation Table 32bits): được giới thiệu trong phiên bản Windows 95 Service Pack 2 (OSR 2), được xem là phiên bản mở rộng của FAT16. Do sử dụng không gian địa chỉ 32 bit nên FAT32 hỗ trợ nhiều clusters trên một partition, do vậy không gian đĩa cứng được tận dụng nhiều hơn. Với khả năng hỗ trợ kích thước của phân vùng từ 2GB lên 2TB và chiều dài tối đa của tên tập tin được mở rộng đến 255 ký tự đã làm cho FAT16 nhanh chóng bị lãng quên. Tuy nhiên, nhược điểm của FAT32 là tính bảo mật và khả năng chịu lỗi (Fault Tolerance) không cao.

- Khái niệm NTFS

NTFS (New Technology File System): được giới thiệu cùng với phiên bản Windows NT đầu tiên, Microsoft đã thay thế hệ thống file FAT MS-DOS bằng một hệ thống file mới 32-bit nhanh hơn, bảo mật hơn. Với không gian địa chỉ 64 bit, khả năng thay đổi kích thước của cluster độc lập với dung lượng đĩa cứng, NTFS hầu như đã loại trừ được những hạn chế về số cluster, kích thước tối đa của tập tin trên một phân vùng đĩa cứng.

NTFS sử dụng bảng quản lý tập tin MFT (Master File Table) thay cho bảng FAT quen thuộc nhằm tăng cường khả năng lưu trữ, tính bảo mật cho tập tin và thư mục, khả năng mã hóa dữ liệu đến từng tập tin. Ngoài ra, NTFS có khả năng chịu lỗi cao, cho phép người dùng đóng một ứng dụng “chết” (not responding) mà không làm ảnh hưởng đến những ứng dụng khác. Tuy nhiên, NTFS lại không thích hợp với những ổ đĩa có dung lượng thấp (dưới 400 MB) và không sử dụng được trên đĩa mềm.

Hệ thống file NTFS có khả năng hoạt động cao và có khả năng tự sửa chữa. Nhờ có tính năng lưu giữ lại các thông tin xử lý, NTFS có khả năng phục hồi file cao hơn trong những trường hợp ổ đĩa có sự cố. Nó hỗ trợ chế độ bảo mật ở mức độ file, nén và kiểm định. Nó cũng hỗ trợ các ổ đĩa lớn và các giải pháp lưu trữ mạnh mẽ như RAID.

NTFS hiện có các phiên bản: v1.0, v1.1, v1.2 ở các phiên bản Windows NT 3.1, Windows NT 3.5, Windows 3.51 và Windows NT 4. Phiên bản v3.0 của Windows 2000 và phiên bản v3.1 của Windows XP, Windows Server 2003, Windows Vista và Windows Server 2008.

Chức năng quan trọng nhất của NTFS là khả năng mã hóa file và folder để bảo vệ các dữ liệu nhạy cảm của người dùng máy tính.

Đáng tiếc là NTFS và FAT không tương thích với nhau. Hậu quả là chỉ có các hệ điều hành Windows NT/2000/XP mới “nhìn” thấy các ổ đĩa được định dạng với hệ thống file NTFS.

Trong khi đó, tính tương thích giữa các phiên bản NTFS cao hơn. Tuy có hệ thống file NTFS 1.1, Windows NT SP4 trở lên (với drive NTFS.SYS mới) có thể truy xuất các ổ đĩa NTFS 5.0. Trong Windows 2000 có chức năng tự chuyển đổi các file NTFS cũ thành NTFS 5.0.

Để nhận biết một ổ cứng đã sử dụng NTFS hay chưa, ta nhấp chuột phải vào ổ đĩa nào đó trong My Computer rồi chọn properties. Nhìn vào type có là NTFS chưa.

Để chuyển FAT thành NTFS file system thì có thể làm như sau: chọn Start → Run → CMD. Trong CMD: Convert [ổ đĩa:] /FS:NTFS

Bảng so sánh FAT và NTFS

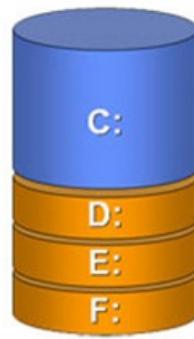
Khả năng	FAT16	FAT32	NTFS
		Windows 95 OSR2,	
Hệ điều hành hỗ trợ	Hầu hết các hệ điều hành	Windows 98,	Windows 2000, 2003, 2008
		Windows 2000, 2003	
Hỗ trợ tên tập tin dài	Windows: 256 ký tự, Dos: 8.3 ký tự	256 ký tự	
Sử dụng hiệu quả đĩa	Không	Có	Có
Hỗ trợ nén đĩa	Không	Không	Có
Hỗ trợ hạn ngạch	Không	Không	Có
Hỗ trợ mã hóa	Không	Không	Có
Hỗ trợ bảo mật cục bộ	Không	Không	Có
Hỗ trợ bảo mật trên mạng	Có	Có	Có
Kích thước Volume tối đa được hỗ trợ	4GB	32GB	1024GB

2.2 Cấu hình đĩa lưu trữ

Windows Server 2008 hỗ trợ 2 loại đĩa lưu trữ: Basic và Dynamic.

2.2.1 Basic Disk

Basic disk là một ổ cứng vật lý bao gồm các phân vùng chính (primary partition) và các phân vùng mở rộng (extended partition) hoặc các ổ đĩa luân lý (logical drive), và toàn bộ không gian cấp cho partition được sử dụng trọn vẹn. Các phân vùng và các ổ đĩa luân lý được xem hiểu như là basic volume.



Hình 2.2.1a Basic Disk

Số phân vùng (partition) ta tạo nên một basic tùy thuộc vào loại phân vùng của ổ đĩa (disk's partition type). Có hai phương thức để lưu trữ thông tin phân vùng trên ổ đĩa: MBR disk (master boot record) và GPT disk (GUIDs partition table).

• MBR (master boot record)

Lần đầu tiên được giới thiệu trong IBM PC DOS 2.0 vào năm 1983.

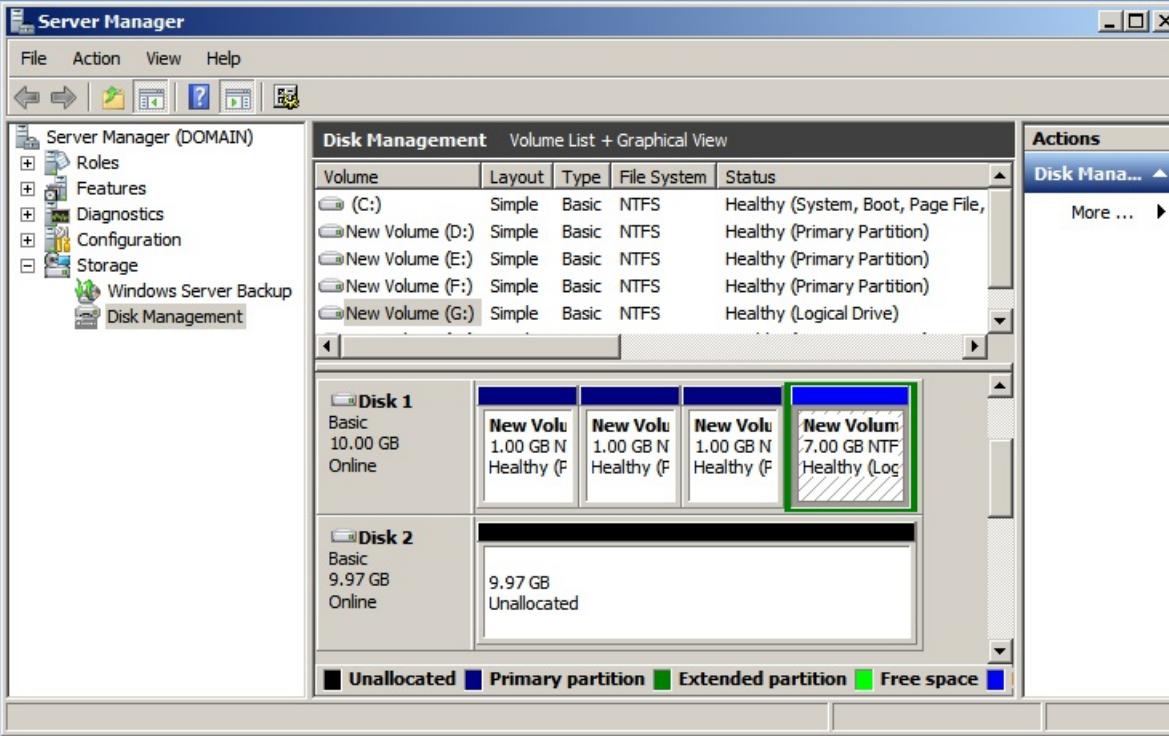
Nó được gọi là master boot record bởi vì MBR là sector khởi động đặc biệt ở vị trí bắt đầu của ổ đĩa. Sector bao gồm boot loader cho hệ điều hành được cài đặt và thông tin về những phân vùng logic của ổ đĩa.

Về boot loader, chúng ta có thể hiểu nó là chương trình khởi động hệ thống và hệ điều hành đã được lập trình sẵn và cài đặt trong ROM. Nói rõ hơn, Boot loader là một đoạn mã nhỏ được thực thi trước khi hệ điều hành bắt đầu chạy và nó cho phép nhà sản xuất thiết bị quyết định những tính năng nào người sử dụng được phép dùng hoặc bị hạn chế.

MBR trở thành chuẩn công nghiệp cho mọi người sử dụng để phân vùng và khởi động từ các ổ đĩa.

Chúng ta có thể tạo được bốn phân vùng chính (primary partition) hoặc ba phân vùng chính (primary partition) và một phân vùng mở rộng (extended partition). Trong phân vùng mở rộng ta có thể tạo vô hạn ổ đĩa luân lý (logical drive). Và mỗi phân vùng được giới hạn đến 2TB (tera byte).

Một trong số những thiếu sót lớn nhất của MBR disk là hạn chế việc sử dụng partition table. MBR disk chỉ có một partition table để theo dõi tất cả các khối trong phân vùng đó. Nếu partition này bị lỗi, toàn bộ đĩa phải phục hồi từ bản sao lưu.



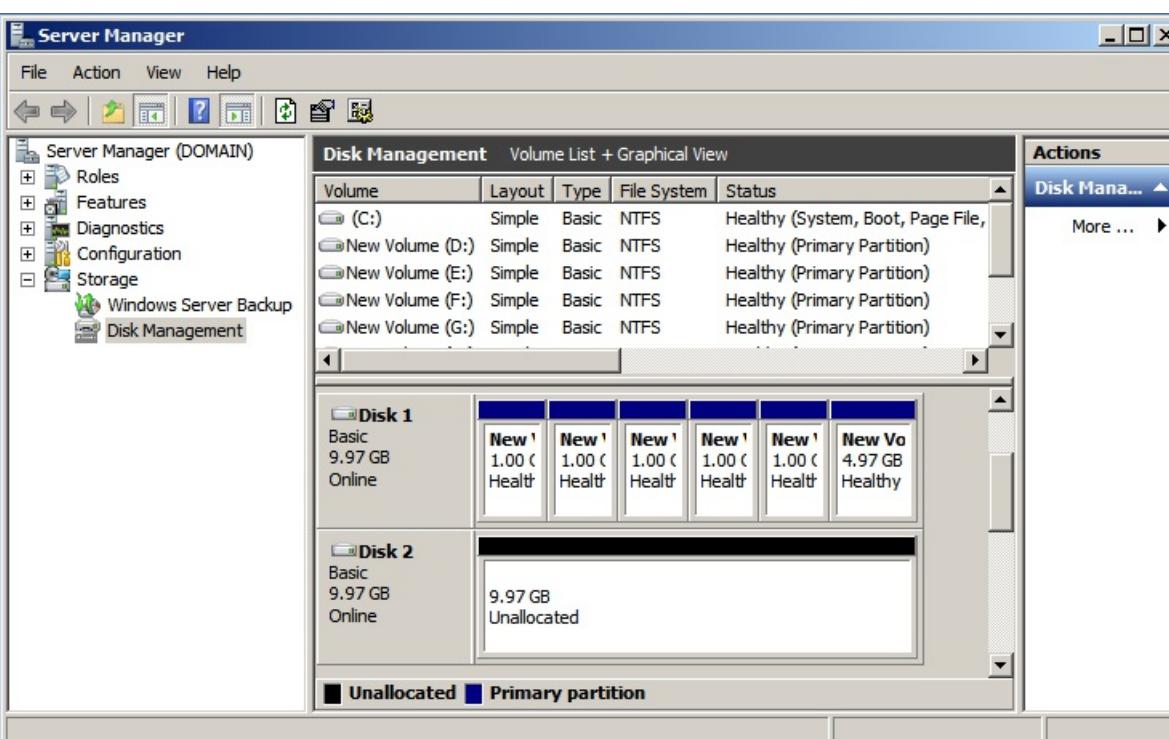
Hình 2.2.1b MBR (master boot record)

- **GPT (GUIDs partition table)**

Đây là một dạng chuẩn mới đang dần thay thế chuẩn MBR. GPT thay thế các hệ thống phân vùng MBR xa xỉ bằng các tính năng giao diện hiện đại hơn.

Lí do được gọi là GUID Partition Table bởi lẽ mỗi phân vùng trên ổ đĩa của bạn có một "globally unique identifier" hay viết tắt là GUID.

Hệ thống này không giới hạn của MBR. Ổ đĩa có thể nhiều hơn, lớn hơn nhiều và kích thước giới hạn nhưng lại phụ thuộc vào hệ điều hành và hệ thống tập tin của nó. Chúng ta có thể tạo lên đến 128 phân vùng chính (primary partition). Bởi vì GPT disk không giới hạn bốn phân vùng chính nên chúng ta không cần tạo phân vùng mở rộng (extended partition) hay các ổ đĩa luận lý (logical drive).



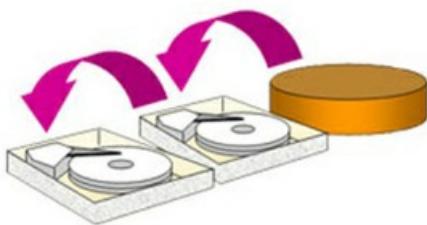
Hình 2.2.1c GPT (GUIDs partition table)

2.2.2 Dynamic Disk

Dynamic disk có một đặc trưng mà ở Basic disk không có. Nó được chia thành các volume dynamic để lưu trữ dữ liệu và có thể hỗ trợ lên tới 2000 volume trên một ổ đĩa. Volume disk không chứa các ổ đĩa logic hay partition.

Giống như basic disk, Dynamic được hỗ trợ cả hai loại phân vùng MBR và GPT. Dynamic cho thấy sự linh hoạt trong việc quản lý khối lượng bởi vì chúng sử dụng cơ sở dữ liệu để theo dõi thông tin dynamic volume trên đĩa và các dynamic khác trên máy.

Vị trí của cơ sở dữ liệu được xác định bởi kiểu phân vùng trên ổ đĩa. Đối với MBR thì cơ sở dữ liệu chứa trong 1MB (megabyte) cuối cùng của ổ đĩa. Đối với GPT thì cơ sở dữ liệu được ẩn trong một phân vùng dành riêng 1 MB (megabyte).

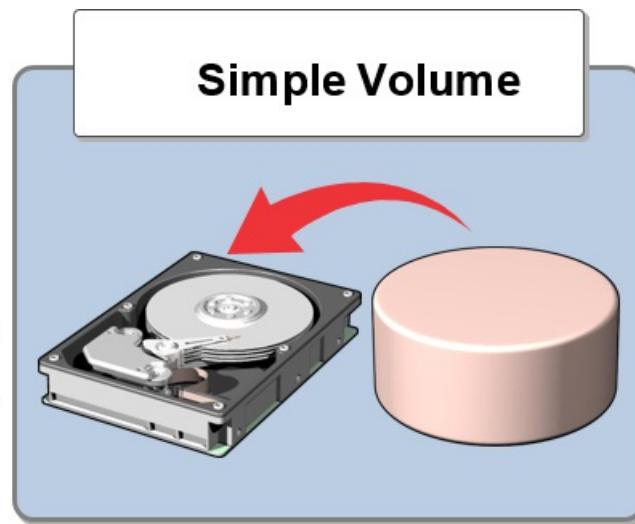


Hình 2.2.2a Dynamic Disk

Dynamic đã hỗ trợ 5 loại volume dynamic từ windows server 2003 và windows 2000 bao gồm các loại: Simple volume, spaned volume, striped volume (RAID-0), mirrored volume (RAID-1), RAID-5 volume.

- **Simple Volume**

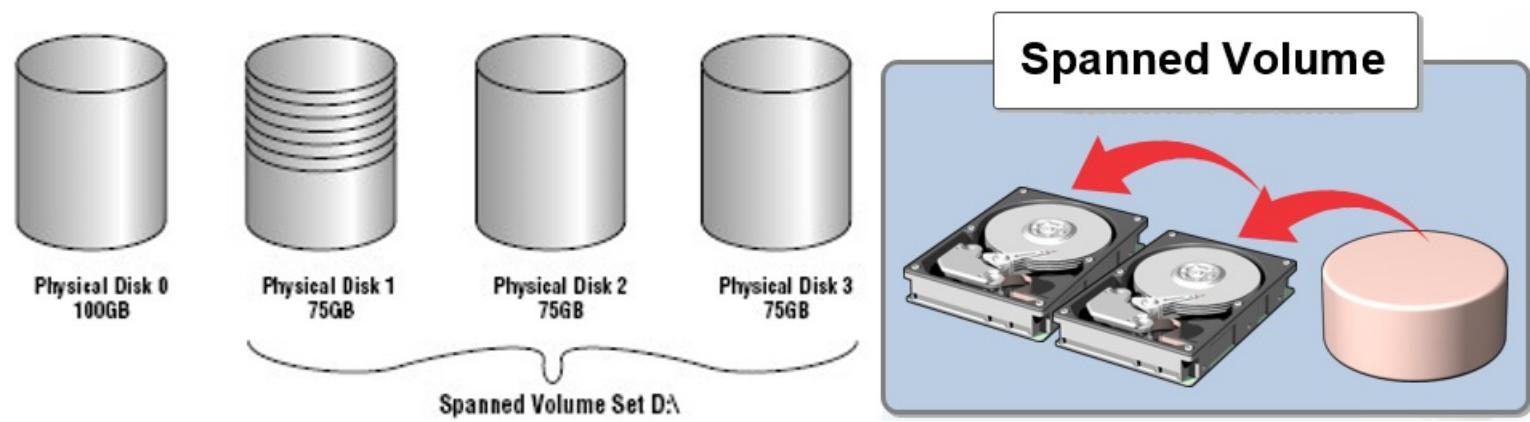
Dữ liệu trên **simple volume** chỉ được lưu trữ trên 1 ổ cứng vật lý, do đó vấn đề an toàn dữ liệu (Fault Tolerancing), và tăng tốc độ xử lý (Load Balancing) không được đảm bảo, khi ổ cứng vật lý hỏng, thì dữ liệu có nguy cơ bị mất.



Hình 2.2.2b Simple Volume

- **Spanned Volume**

Dữ liệu trên **spanned volume** được chép phân bổ trên 2 ổ cứng vật lý trở lên, các ổ cứng **không nhất thiết phải giống nhau** và chúng được ghép lại thành một Volume duy nhất, tuy vậy chúng không có khả năng đáp ứng vấn đề an toàn dữ liệu (Fault Tolerancing), và tốc độ xử lý dữ liệu (Load Balancing), vì chưa có sự thay đổi về cơ chế (dữ liệu được chép đầy trên spanned volume ở disk 1 mới chép sang các disk còn lại).

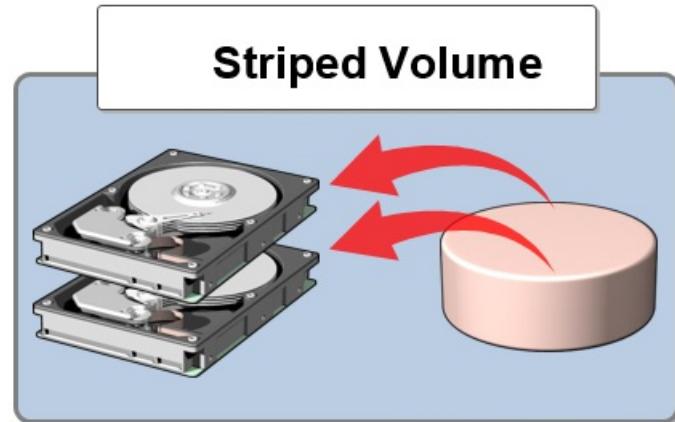
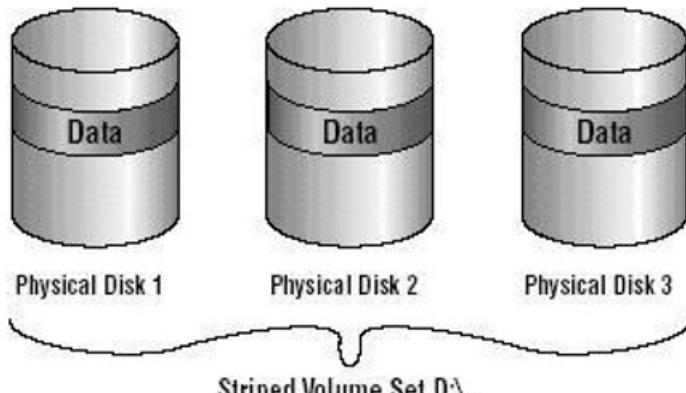


Hình 2.2.2c Spanned Volume

- **Striped volume (RAID-0)**

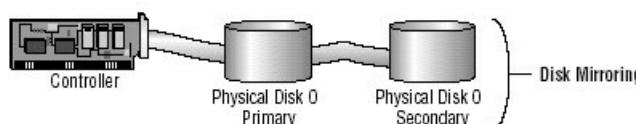
Dữ liệu trên **striped volume** có thể được trao đổi cùng lúc trên 2 ổ cứng vật lý trở lên, **dung lượng trên các ổ cứng vật lý của striped volume phải bằng nhau**. Striped Volume có sự thay đổi trong cơ chế hoạt động, dữ liệu khi được chép trên striped được chia ra và chép đều trên các disk, vì thế striped đáp ứng được vấn đề tốc độ xử lý dữ liệu (Load Balancing), tuy nhiên striped không đáp ứng được vấn đề an toàn dữ liệu (Fault Tolerancing).

Hình 2.2.2d Striped Volume



- **Mirror volume (RAID-1)**

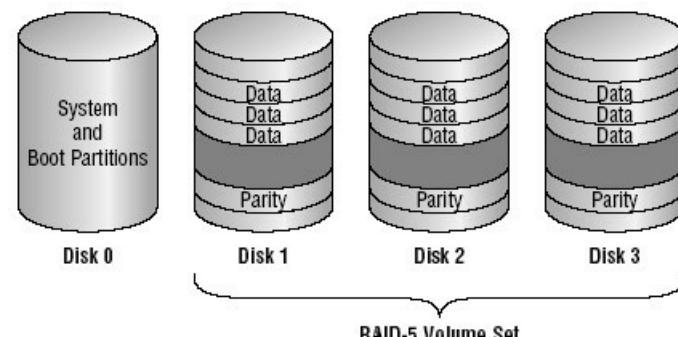
Mirror volume chỉ yêu cầu 2 ổ cứng vật lý, dữ liệu khi chép trên mirror sẽ được backup sang đĩa cứng vật lý thứ 2 (vì thế dung lượng trên mirror volume chỉ bằng 1/2 dung lượng khi ta cấu hình). Do đó Mirror Volume đáp ứng nhu cầu an toàn dữ liệu (Fault Tolerancing), nhưng không làm tăng tốc độ truy xuất dữ liệu.



Hình 2.2.2e Mirror volume(RAID-1)

- **RAID-5 volume**

Raid-5 Volume là giải pháp kết hợp các loại volume (Striped Volume RAID-0, Mirror Volume RAID-1) mà ta đã đề cập ở trên. **Raid-5 đáp ứng cho chúng ta cả 2 vấn đề an toàn dữ liệu (Fault Tolerancing), và tăng tốc độ xử lý dữ liệu (Load Balancing).** Để đáp ứng 2 vấn đề trên, Raid-5 đòi hỏi phải sử dụng 3 ổ đĩa cứng vật lý, và sử dụng thuật toán Parity (khi 1 trong 3 đĩa bị hỏng, thuật toán Parity sẽ tự chép những bit bị mất). Vì phải chứa thêm bit Parity nên dung lượng của Raid-5 Volume sẽ chỉ bằng 2/3 dung lượng ta cấu hình (1/3 còn lại là để chứa bit Parity).



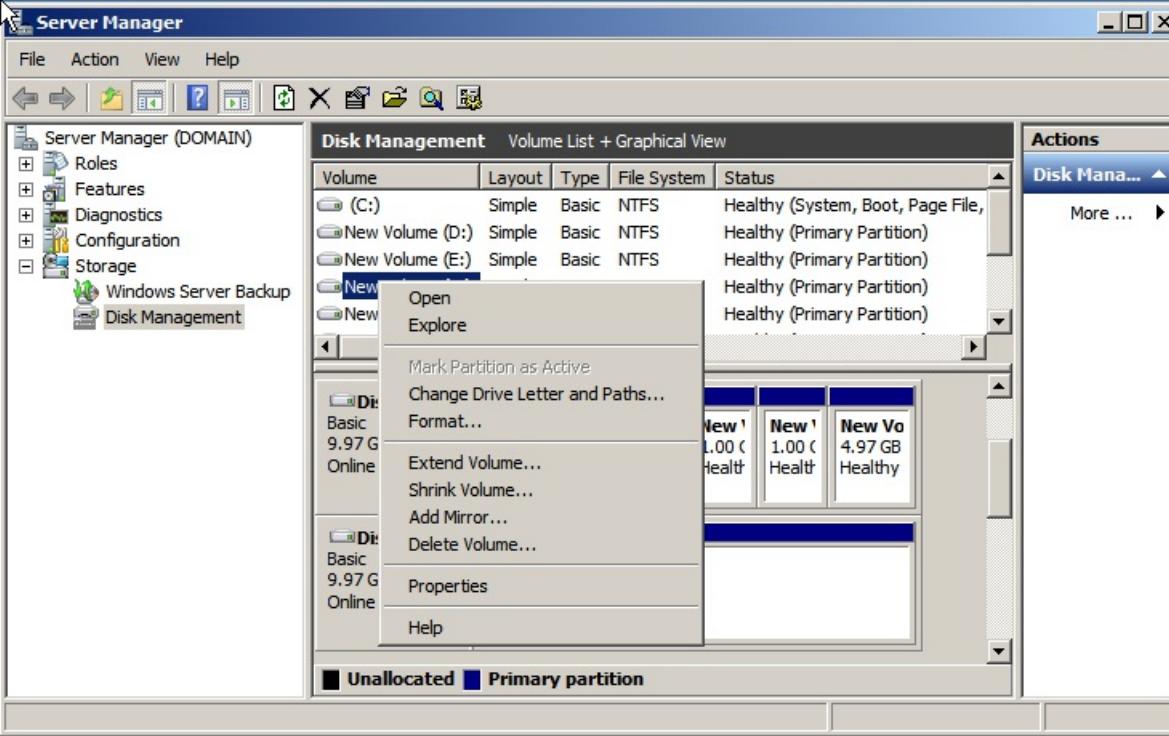
Hình 2.2.2f RAID-5 volume

2.3 Chương trình Disk Manager

2.3.1 Công cụ quản lý đĩa Disk Management

Disk Management là một công cụ quản lý dung lượng ổ cứng mạnh trong Windows. Không những thế, nó còn quản lý tất cả các thiết bị lưu trữ khác như: **Đĩa mềm, đĩa flash...**

Tuy không giàu tính năng nhưng nó khá hữu ích trong việc giúp bạn thiết lập hệ thống đĩa trong Windows một cách hiệu quả nhất. Vì vậy, nếu muốn thiết lập lại phân vùng ổ cứng, chẳng hạn như: Tạo ổ đĩa mới, định dạng, giảm hoặc tăng dung lượng đĩa hiện thời thì Disk Management là công cụ ta cần.

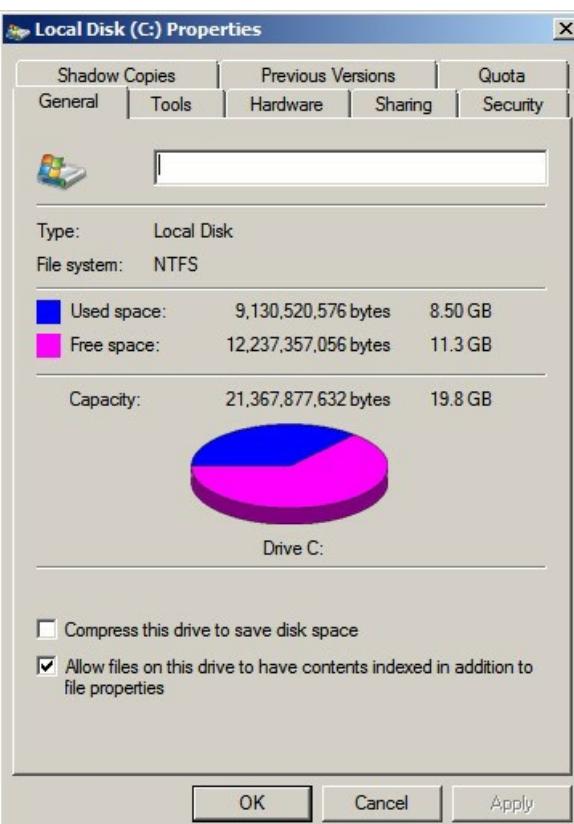


Hình 2.3.1 Disk Management

2.3.2 Thuộc tính của Volume (hoặc Đĩa) cục bộ

Tab general: Cung cấp các thông tin như nhãn đĩa, loại, hệ thống thông tin, dung lượng. Disk cleanup để xoá tập tin không cần thiết.

Tab tool: Nút check now để kích hoạt chương trình check disk dùng để kiểm tra lỗi. Nút Backup no sẽ mở chương trình backup Wizard. Nút defragment Now mở chương trình disk defragment, dùng để dồn các tập tin trên đĩa thành một khối liên tục.



Tab hardware: Liệt kê các ổ đĩa vật lý windows nhận diện được.

Tab sharing: Cho phép chia sẻ hoặc không chia sẻ ổ đĩa cục bộ này

Tab security: Thiết lập quyền truy cập lên ổ đĩa

Tab quota: Thiết lập hạn ngạch đĩa.

Tab Shadow Copies: Khôi phục dữ liệu lỗi.

Hình 2.3.2 Thuộc tính của Volume/ đĩa cục bộ

2.4 Mã hóa dữ liệu EFS

2.4.1 Nén dữ liệu

Nén dữ liệu là việc chuyển định dạng thông tin sử dụng ít bit hơn cách thể hiện ở dữ liệu ở gốc. Tuỳ theo dữ liệu có bị thay đổi trước và sau khi giải nén hay không. Người ta chia nén thành hai loại: **Nguyên vẹn (lossless)** và **bị mất dữ liệu (lossy)**.

Việc nén dữ liệu là cần thiết vì giảm được nguồn tài nguyên cũng như dung lượng lưu trữ hay băng thông đường truyền.

- **Nén không mất dữ liệu**

Dữ liệu, đặc biệt là văn bản, đồ họa luôn chứa trong nó những chuỗi thông tin giống hệt nhau lặp đi lặp lại. Việc nén dữ liệu thực hiện bằng cách thay thế nhiều kí tự thông tin lặp đi lặp lại bằng các kí tự khác, và chỉ tạo ra một bản sao của những đoạn dữ liệu bị lặp lại này. Cũng có cách tinh tế hơn là sử dụng những đoạn mã có độ dài khác nhau mã hoá cho các kí tự khác nhau giúp cho các kí tự này chiếm ít chỗ hơn. Dù sử dụng cách nào đi nữa cũng phải làm sao thu nhỏ được kích thước file và giữ được sự toàn vẹn của dữ liệu.

- **Nén mất dữ liệu**

Trường hợp gặp nhất trong nén hình ảnh và âm thanh. Đối với hình ảnh, nhiều giải thuật được đặt ra để đáp ứng nhu cầu giảm thiểu kích thước file sao cho vẫn duy trì ở chất lượng có thể chấp nhận được. Đối với âm thanh, có nhiều chuẩn nén khác nhau: window media, mp3, Real G2, ACC, nhưng thông dụng nhất vẫn là MP3. Nén theo chuẩn MP3, kích thước file audio có thể được thu nhỏ đi 8 lần so với kích thước ban đầu.

2.4.2 Tổng quan về mã hóa EFS

EFS (Encrypting File System) được tích hợp vào trong hệ thống tập tin (file system), cho phép người dùng mã hóa dữ liệu, thông tin cá nhân được lưu trữ trên máy tính nhằm bảo vệ sự riêng tư, tránh người dùng khác khi sử dụng máy tính truy cập một cách cố ý hay vô ý. Đặc biệt, EFS thường được sử dụng để bảo vệ những dữ liệu quan trọng, “nhạy cảm” trên những máy tính xách tay hoặc máy tính có nhiều người sử dụng. Cả hai trường hợp trên đều dễ bị tấn công do những hạn chế của ACL (Access Control Lists).

Trên một máy tính dùng chung, kẻ tấn công có thể lấy được quyền truy cập vào hệ thống thông qua việc sử dụng một hệ điều hành khác nếu máy cài nhiều hệ điều hành. Một trường hợp khác với máy tính bị đánh cắp, bằng cách tháo ổ cứng và gắn vào máy tính khác, kẻ tấn công có thể dễ dàng truy cập những tập tin lưu trữ. Sử dụng EFS để mã hóa những tập tin, nội dung hiển thị chỉ là những ký tự vô nghĩa nếu kẻ tấn công không có khóa để giải mã.

Tính năng EFS được tích hợp chặt chẽ với hệ thống tập tin NTFS. Khi mở một tập tin, EFS sẽ thực hiện quá trình giải mã, dữ liệu được đọc từ nơi lưu trữ sau khi so khớp khóa mã hóa tập tin; khi người dùng lưu những thay đổi của tập tin, EFS sẽ mã hóa dữ liệu và ghi chúng vào nơi lưu trữ cần thiết. Với thuật toán mã hóa đối xứng 3DES, quá trình mã hóa và giải mã diễn ra ngầm bên dưới, thậm chí người dùng cũng không nhận ra sự khác biệt khi làm việc với những tập tin được mã hóa.

EFS hỗ trợ lớp mã hóa bảo mật thông tin. Mỗi tập tin có một khóa mã hóa riêng, và khóa này được sử dụng để giải mã các dữ liệu trong các tập tin. Khóa này cũng được mã hóa và cung cấp cho những người dùng có quyền truy cập dữ liệu. Chỉ những người dùng được phép hoặc được chỉ định mới có quyền giải mã những tập tin này. Những tài khoản người dùng khác trong hệ thống; thậm chí có thể chiếm quyền kiểm soát tập tin (Take Ownership Permission) vẫn không thể đọc được nội dung nếu không có khóa truy cập (access key). Ngay cả tài khoản thuộc nhóm Administrators cũng không thể mở tập tin này nếu tài khoản đó không được chỉ định quyền giải mã.

Một khi đã chọn mã hóa tập tin, quá trình xử lý mã hóa và giải mã dữ liệu thực hiện hoàn toàn trong suốt, ta không cần làm theo bất cứ thao tác nào. Ta cần phải quyết định mã hóa thư mục nào chứa tập tin này. Nếu lựa chọn mã hóa một thư mục, tất cả các tập tin và thư mục con sẽ được mã hóa đồng thời. Do đó, khi mã hóa một thư mục, ta cần phải biết được những tập tin, thư mục nào ở trong đó.

Nếu chọn giải mã thư mục thôi, thì các tập tin và thư mục con bên trong vẫn bị mã hóa. Tuy nhiên, các tập tin và thư mục mới sẽ không được tự động mã hóa.

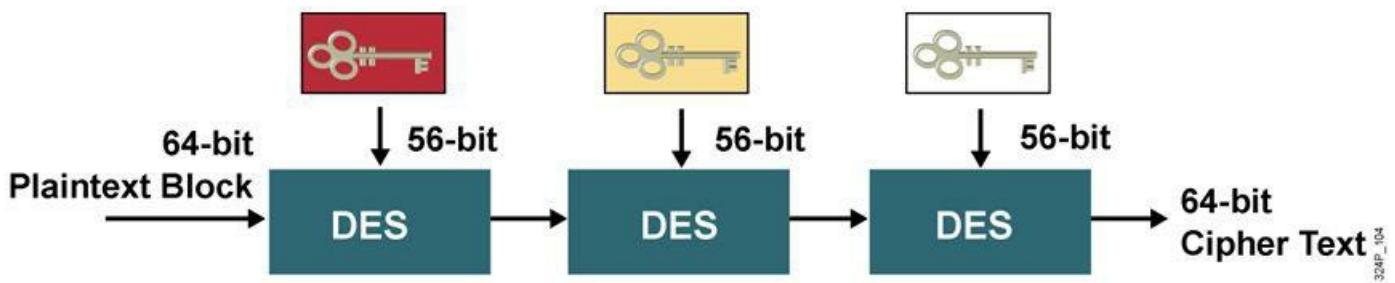


Hình 2.4.2 Mã hóa EFS

2.4.3 Thuật toán 3DES

Triple Data Encryption Standard (3DES) là DES được bổ sung thêm một số tính năng cao cấp, nó thực hiện mã hóa dữ liệu thông qua việc xử lý mỗi block 3 lần và mỗi lần với một khóa khác nhau. Trước hết nó sẽ dùng một khóa để mã hóa plain-text thành ciphertext, sau đó lại tiếp tục dùng một khóa khác để mã hóa ciphertext, và tiếp tục mã hóa ciphertext này với khóa thứ 3, nghĩa là 3DES sử dụng một khóa 168 bit, do đó an toàn hơn và tất nhiên xử lý chậm hơn DES.

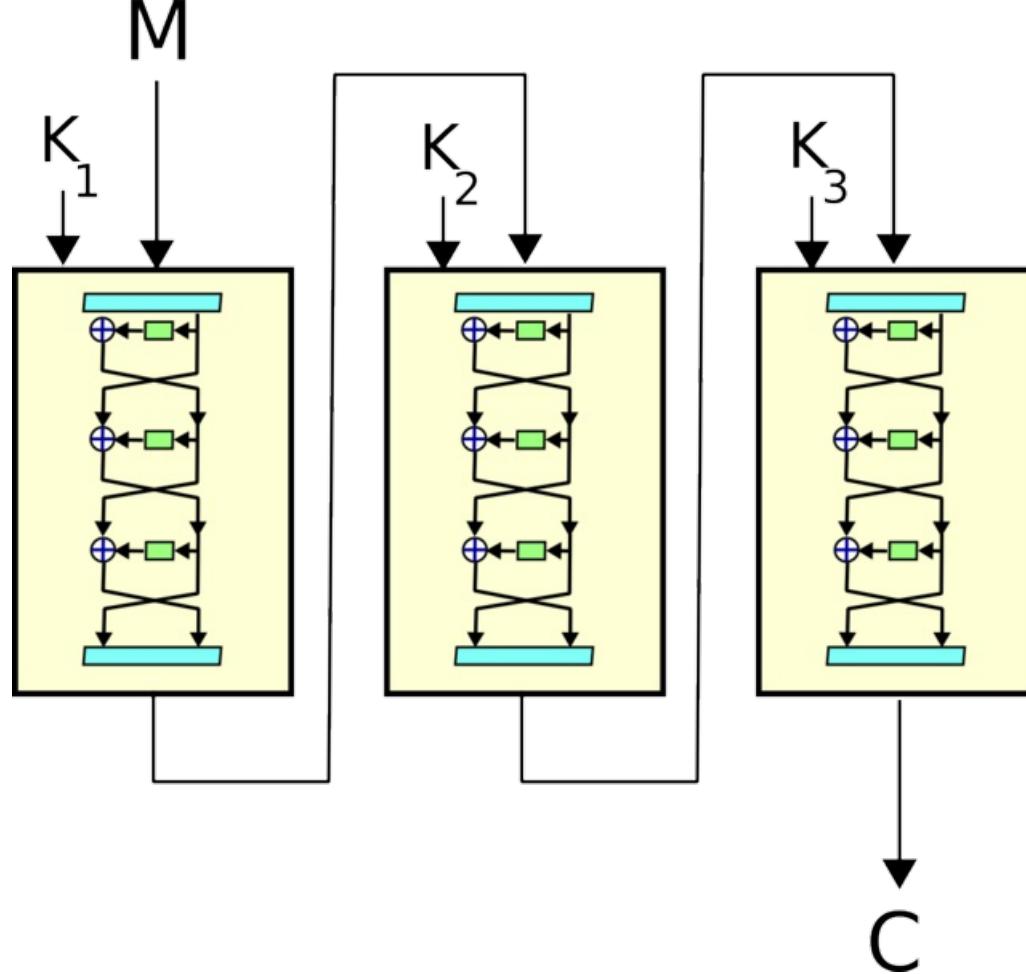
Symmetric Encryption: 3DES



- **168-bit total key length**
- **Mode of operation decides how to process DES three times**
- **Normally: encrypt, decrypt, encrypt**
- **3DES requires more processing than DES**

Hình 2.4.3a Symmetric Encryption: 3DES

Thuật toán mã hóa 3DES thực ra là mã hóa cùng 1 thông tin qua 3 lần mã hóa DES với 3 chìa khóa khác nhau. Do đó, chiều dài mã khóa sẽ lớn hơn và an toàn cao hơn so với DES.



Hình 2.4.3b Thuật toán 3DES

Ta có $EK(I)$ và $DK(I)$ là tượng trưng cho quá trình mã hóa vào giải mã I với khóa là K. Mỗi hệ thống mã hóa hay giải mã triple-Des là 1 hợp tác các quá trình giải mã và mã hóa trên Des.

- Quá trình mã hóa Triple Des, ta mã hóa I thành O:

$$O = EK3(DK2(EK1(I)))$$

hay

$$I \rightarrow DES \rightarrow EK1 \rightarrow DES \rightarrow DK2 \rightarrow DES \rightarrow EK3 \rightarrow O$$

- Quá trình giải mã 3DES, ta giải mã O thành I:

$$I = DK1(EK2(DK3(O)))$$

Hay

$$I \rightarrow DES \rightarrow DK3 \rightarrow DES \rightarrow EK2 \rightarrow DES \rightarrow DK1 \rightarrow O$$

- Những tiêu chuẩn kèm theo:
- Key: khóa K1, K2, K3 độc lập
- Key: khóa K1=K3, K2 độc lập
- Key: khóa K1=K2=K3

Một bản rõ được mã hóa bằng 3DES có thể giải mã bằng DES và một bản rõ mã hóa bằng DES có thể được giải mã bằng 3DES. Triple Des cũng có các chế độ ECB, CBC, CFB, OFB. Về cơ bản cũng giống DES, chỉ việc thay các hàm mã hóa của DES thành 3DES. Với khóa K1=K2=K3 thì TECB, TCBC, TCFB và TOFB cũng tương ứng với các chế độ ECB, CBC, CFB và OFB của DES.

- **Ưu nhược điểm của 3DES:**
- **Ưu điểm:** Khác với DES, thuật toán mã hóa 3DES được mã hóa 3 lần DES với kích thước không gian khóa 168 bit cho nên an toàn hơn rất nhiều so với DES.
- **Nhược điểm:** Vì 3DES sử dụng 3 lần mã hóa DES cho nên tốc độ mã hóa sẽ chậm hơn rất nhiều so với DES. Phần mềm ứng dụng tỏ ra rất chậm đối với hình ảnh số và một số ứng dụng dữ liệu tốc độ cao.

2.4.4 Phương thức mã hóa dữ liệu của EFS

EFS sử dụng kết hợp khóa công khai và khóa mã hóa đối xứng để bảo mật tập tin. Phương pháp mã hóa công khai (public key encryption) sử dụng một cặp khóa public key/private key (thông tin mã hóa bởi public key có thể được giải mã bằng private key) và khóa mã hóa FEK (file encryption key) để mã hóa và giải mã dữ liệu.

Khi người dùng mã hóa một tập tin, EFS tạo ra một FEK để mã hóa dữ liệu; FEK này sẽ được mã hóa với public key sau khi kết thúc “nhiệm vụ” của mình và được lưu giữ trong header của dữ liệu đã mã hóa. Khi cần giải mã, EFS sử dụng private key (ứng với mỗi người dùng) để giải mã FEK và sử dụng FEK để giải mã dữ liệu.

Việc mã hóa và giải mã trong Windows XP có thể sử dụng bằng nhiều cách khác nhau: tùy chọn thuộc tính mã hóa trong Advanced Properties; có thể sao chép tập tin cần mã hóa vào thư mục đã mã hóa hoặc sử dụng dòng lệnh “Cipher.exe” trong cửa sổ DOS – Prompt ...

2.2.5 Quá trình mã hóa tập tin của EFS

Khi cần mã hóa EFS sẽ thực hiện các bước như sau:

- Mở tập tin cần mã hóa và sao chép tất cả dữ liệu vào một tập tin tạm thời trong thư mục TEMP của hệ thống.
- Một FEK ngẫu nhiên được tạo ra để mã hóa dữ liệu bằng thuật toán DESX hoặc 3DES (tùy vào việc áp dụng chính sách bảo mật) và FEK này được mã hóa với public key và lưu vào DDF (Data Decrypting Field - vùng dành để giải mã).
- Nếu sử dụng Recovery Agent (được thiết lập trong Group Policy), DRF (Data Recovery Field - vùng khôi phục dữ liệu) được tạo ra để chứa FEK mã hóa bằng public key của Data Recovery Agent (tác nhân phục hồi dữ liệu).
- Kết thúc quá trình mã hóa, EFS sẽ ghi những dữ liệu đã mã hóa cùng với DDF và DRF vào tập tin và xóa bỏ tập tin tạm.

2.4.6 Quá trình giải mã tập tin của EFS

Khi ứng dụng cần truy cập một tập tin mã hóa, quá trình giải mã được thực hiện như sau:

- NTFS sẽ ghi nhận tập tin cần giải mã và gửi yêu cầu đến EFS driver.
- EFS driver sẽ khôi phục DDF và gửi nó đến EFS service.
- Với private key của người dùng, EFS service sử dụng chìa khóa này để giải mã DDF nhằm có được FEK và gửi FEK này cho EFS driver.
- EFS driver sử dụng FEK để giải mã nội dung tập tin mà ứng dụng yêu cầu.

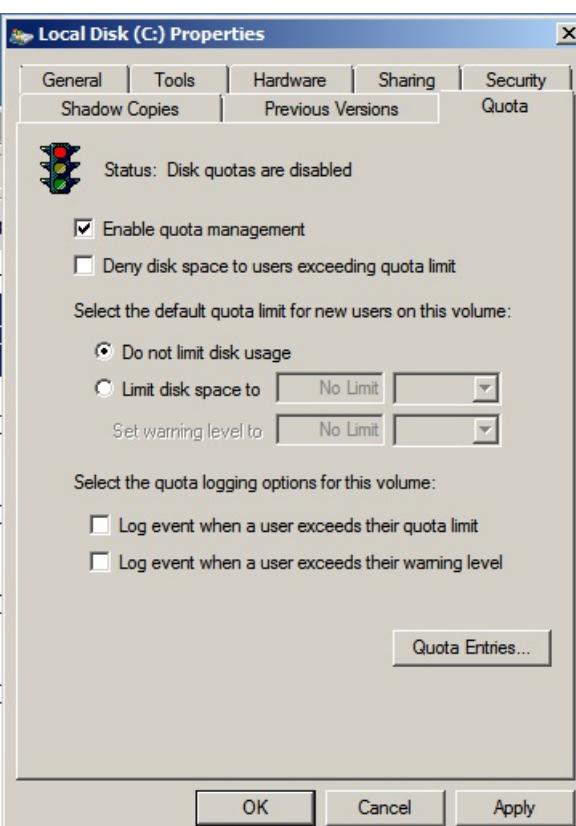
2.5 Thiết lập hạn ngạch đĩa

Hạn ngạch đĩa được dùng để chỉ định dung lượng không gian đĩa tối đa một người dùng có thể sử dụng trên một volume NTFS. Ta có thể áp dụng hạn ngạch đĩa cho tất cả người dùng hoặc chỉ đối với từng người dùng riêng biệt.

Một số vấn đề cần lưu ý khi thiết lập hạn ngạch đĩa:

- Chỉ có thể áp dụng trên các **volume NTFS**.
- Lượng không gian chiếm dụng được tính theo các tập tin và thư mục do người dùng sở hữu.
- Khi người dùng cài đặt một chương trình, lượng không gian đĩa còn trống mà chương trình thấy được tính toán dựa vào hạn ngạch đĩa của người dùng, không phải là lượng không gian còn trống trên volume.
- Được tính toán trên kích thước thật sự của tập tin trong trường hợp tập tin hoặc thư mục được nén.
- Cấu hình hạn ngạch đĩa**

Cấu hình hạn ngạch đĩa bằng hộp thoại Volume Properties, trong tab quota. Theo mặc định tính năng hạn ngạch không được kích hoạt.



Hình 2.5.1 Thiết lập hạn ngạch đĩa

Các mục trong hộp thoại có ý nghĩa như sau:

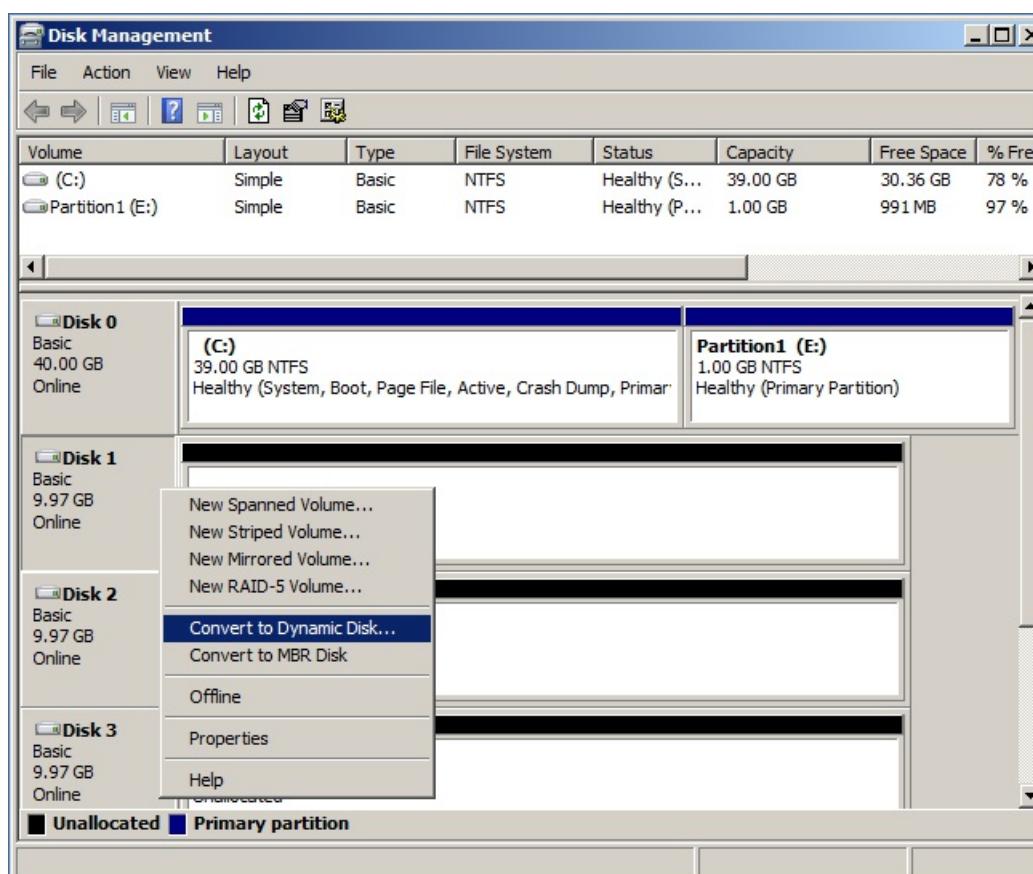
- **Enable quota management:** thực hiện hoặc không thực hiện quản lý hạn ngạch đĩa.
- **Deny disk space to user exceeding quota limit:** người dùng sẽ không thể tiếp tục sử dụng khi vượt quá hạn ngạch và nhận được thông báo **out of disk space**.
- **Select the default quota limit for new users on this volume:** định nghĩa các giới hạn sử dụng. Các lựa chọn bao gồm “không định nghĩa giới hạn” (**Do not limit this space**), “giới hạn cho phép” (**Limit disk space to**) và “giới hạn cảnh báo” (**Set warning level to**).
- **Select the quota logging options for this volume:** có ghi nhận lại các sự kiện liên quan đến sử dụng hạn ngạch đĩa. Có thể ghi nhận khi người dùng vượt quá giới hạn cho phép hoặc vượt quá giới hạn cảnh báo.
- **Biểu tượng đèn giao thông trong hộp thoại có các trạng thái sau:**
 - Đèn đỏ cho biết tính năng quản lý hạn ngạch không được kích hoạt.
 - Đèn vàng cho biết Windows Server 2008 đang xây dựng lại thông tin hạn ngạch.
 - Đèn xanh cho biết tính năng quản lý đang có tác dụng.
- **Thiết lập hạn ngạch mặc định**

Khi thiết lập hạn ngạch mặc định áp dụng cho người dùng mới trên volume, chỉ những người dùng chưa bao giờ tạo tập tin trên volume đó mới chịu ảnh hưởng. Có nghĩa là những người dùng đã sở hữu các tập tin hoặc thư mục trên volume này đều không bị chính sách hạn ngạch quy định. Như vậy, nếu muốn áp đặt hạn ngạch cho tất cả người dùng thì phải chỉ định hạn ngạch ngay từ khi tạo lập volume.

Chương 3 Thực nghiệm

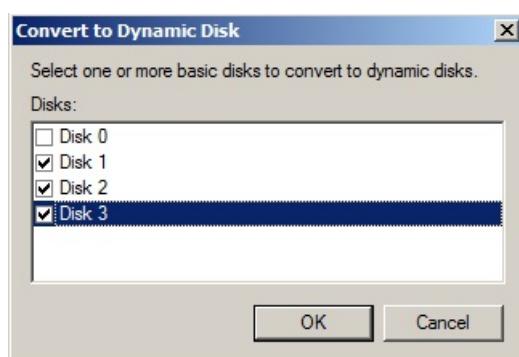
3.1 Convert Basic Disk to Dynamic Disk

Đầu tiên chúng ta cần nâng cấp lần lượt từng ổ đĩa lên **Dynamic** bằng cách nhấp phải vào ổ đĩa chọn **Convert to Dynamic Disk...**



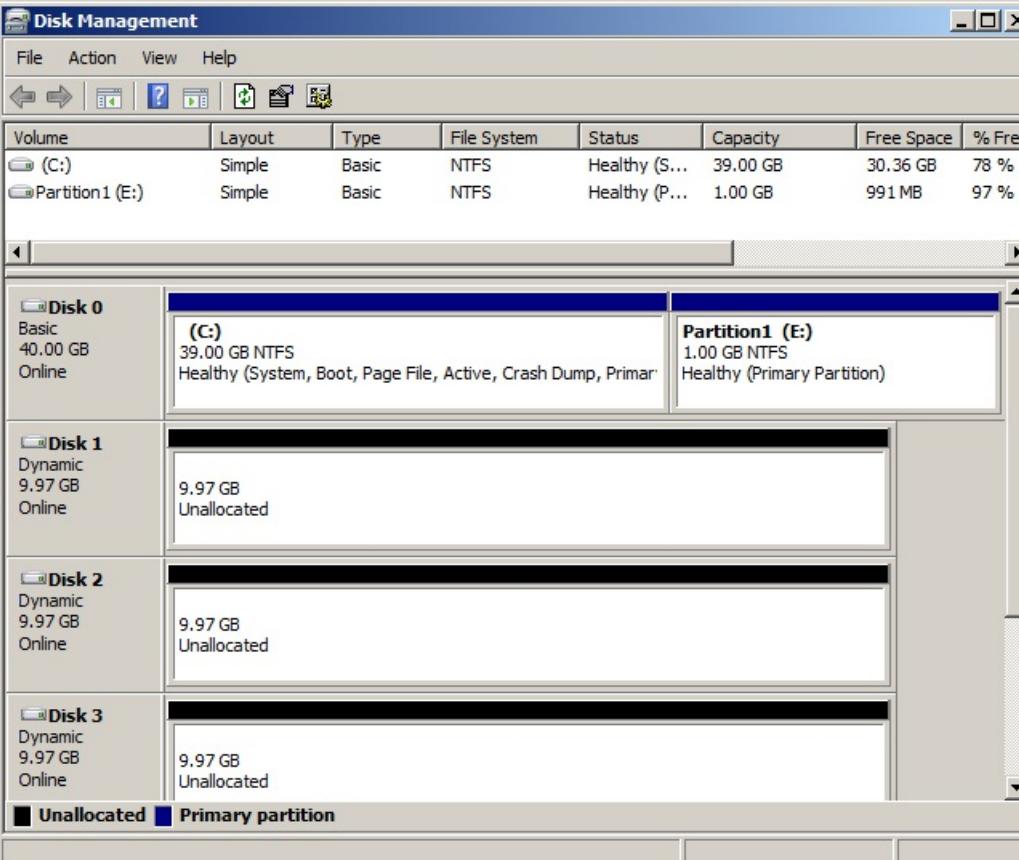
Hình 3.1a Convert Basic Disk to Dynamic Disk

Ở đây chúng ta chỉ nâng cấp **Disk 1, Disk 2 & Disk 3**. Sau đó chọn **OK** để tiến hành **Convert**.



Hình 3.1b Chọn đĩa để convert

Sau khi **Convert** thành công ta đã có 3 **Dynamic Disk**



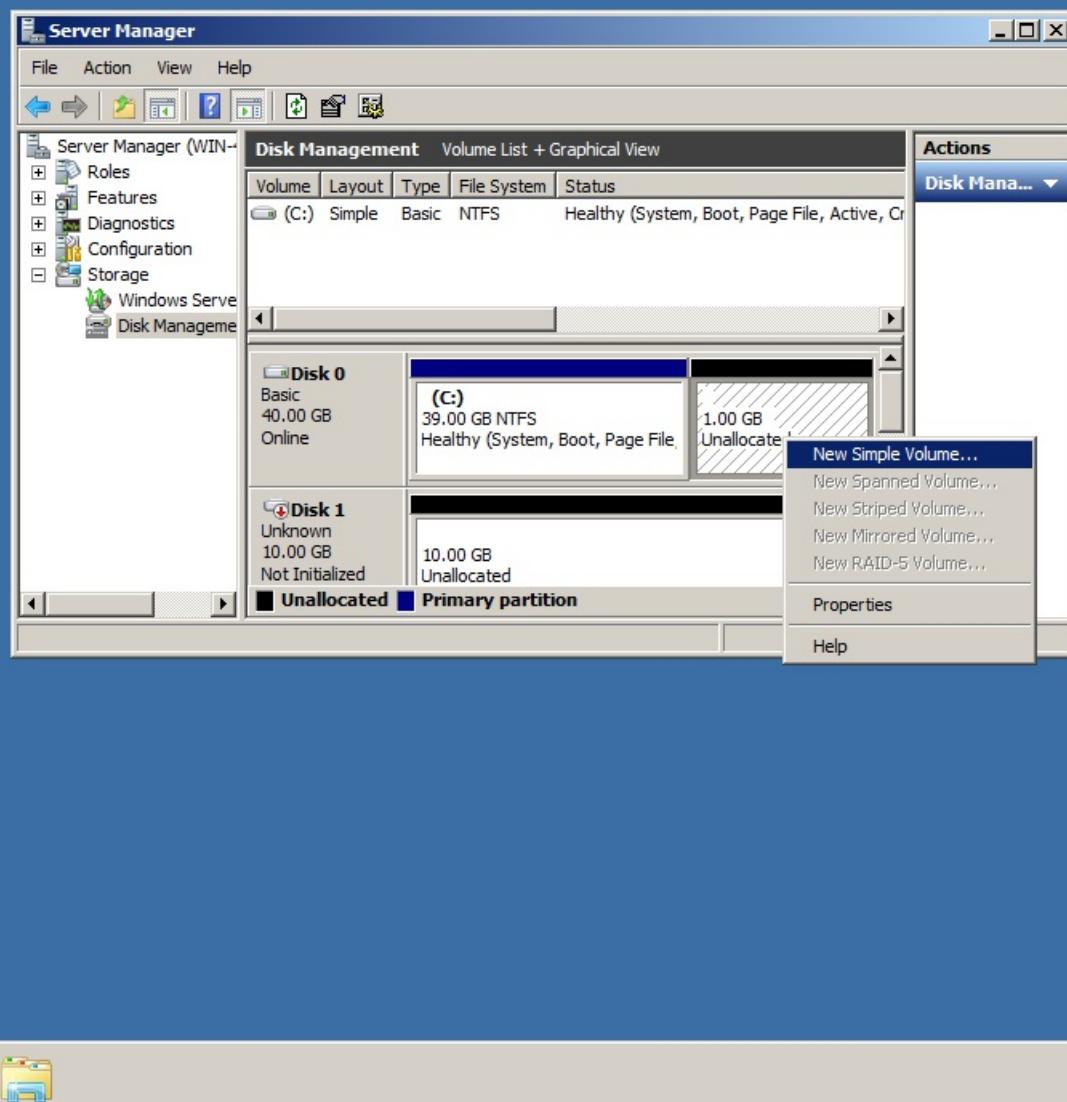
Hình 3.1c Sau khi convert sang Dynamic Disk

3.2 Tạo phân vùng cho Basic Disk

Để tạo một phân vùng mới bạn nhấp phải vào phần **Unallocated** chọn **New Simple Volume...**

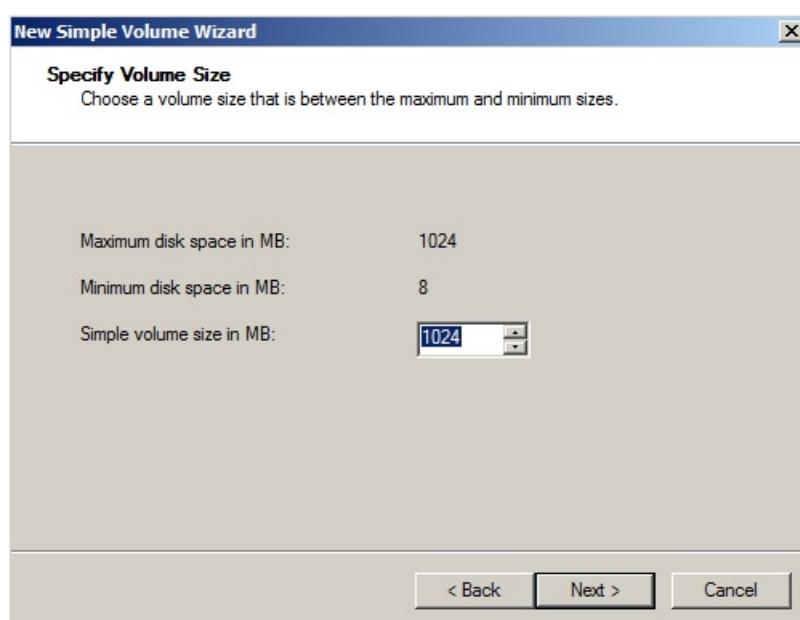


Recycle Bin



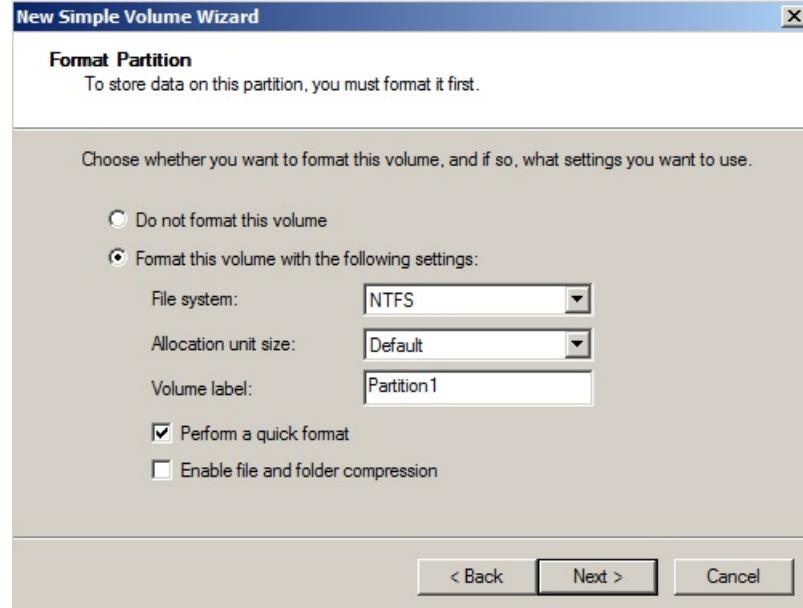
Hình 3.2a New Simple Volume

Tiến hành tạo **Primary Partition** cho **Disk 0** với dung lượng **1024MB**



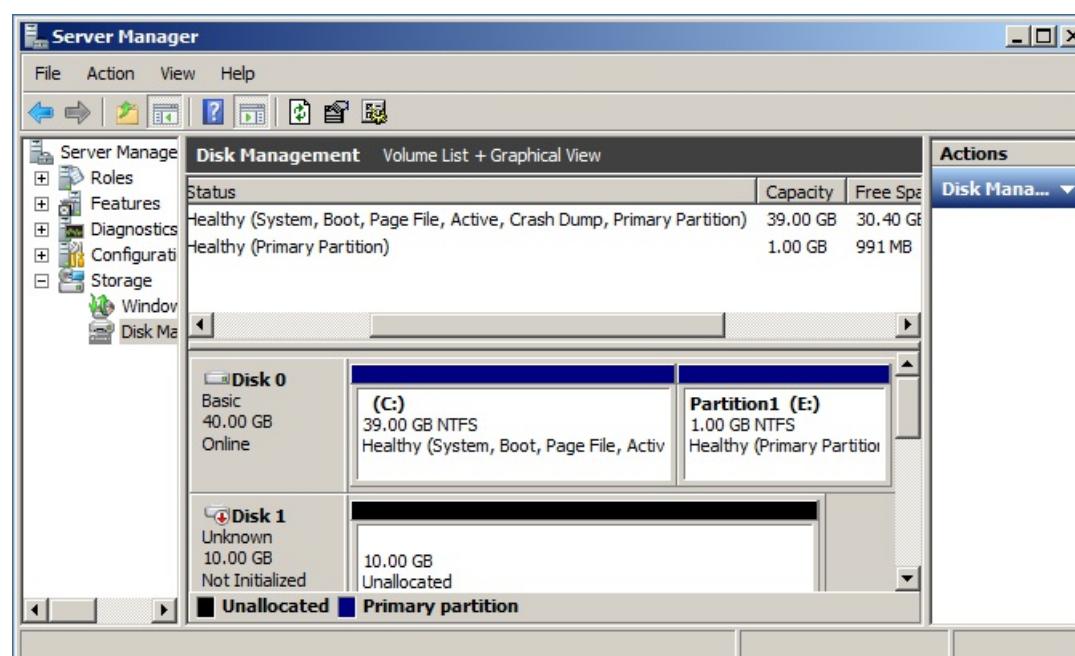
Hình 3.2b Specify Volume Size

Đặt tên cho nó là **Partition1** với định dạng ở dạng **NTFS**



Hình 3.2c Format Partition

Sau khi kết thúc, kết quả cho thấy ta đã tạo được 1 phân vùng mới

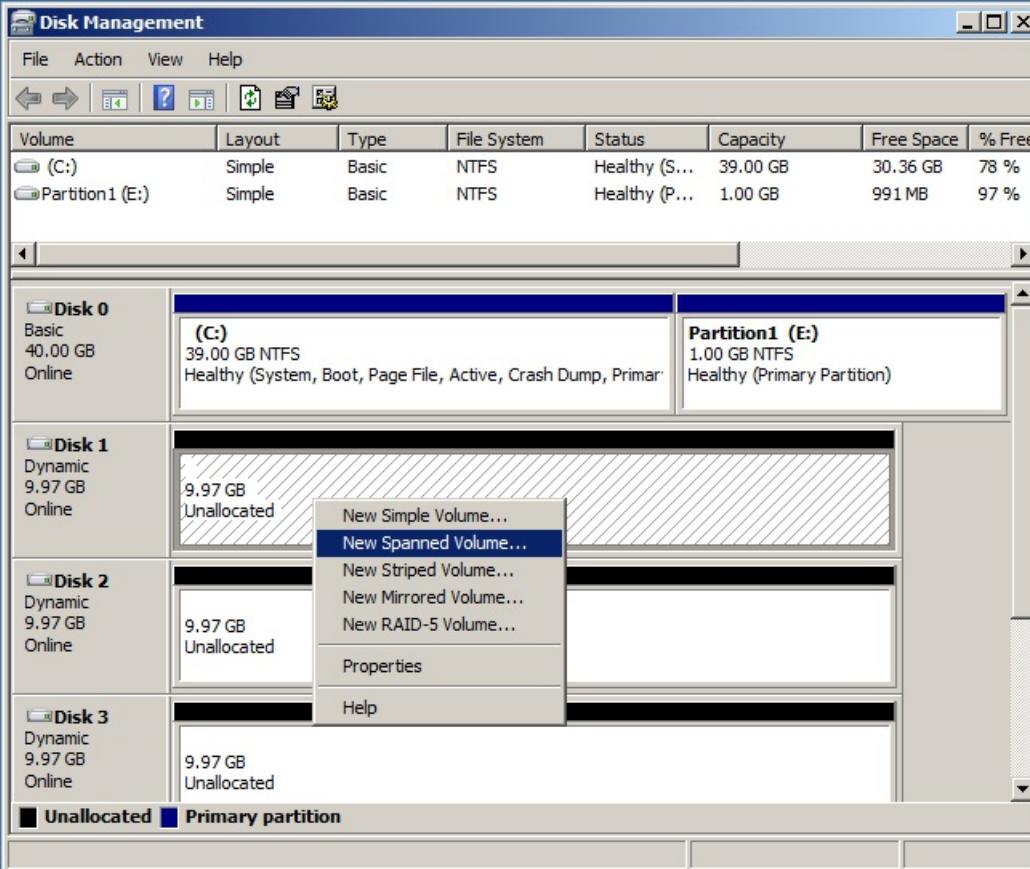


Hình 3.2d Hoàn tất tạo Simple Volume

3.3 Tạo các loại Volume cho Dynamic Disk

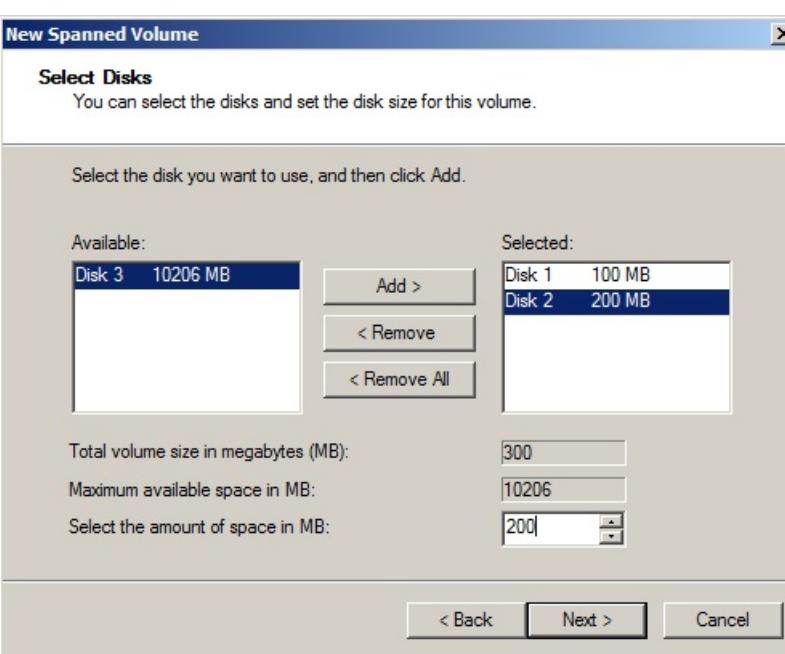
3.3.1 Tạo Spanned Volume

Tạo **Spanned Volume**: nhấp phải chuột vào **Unallocated** chọn **New Spanned Volume**.



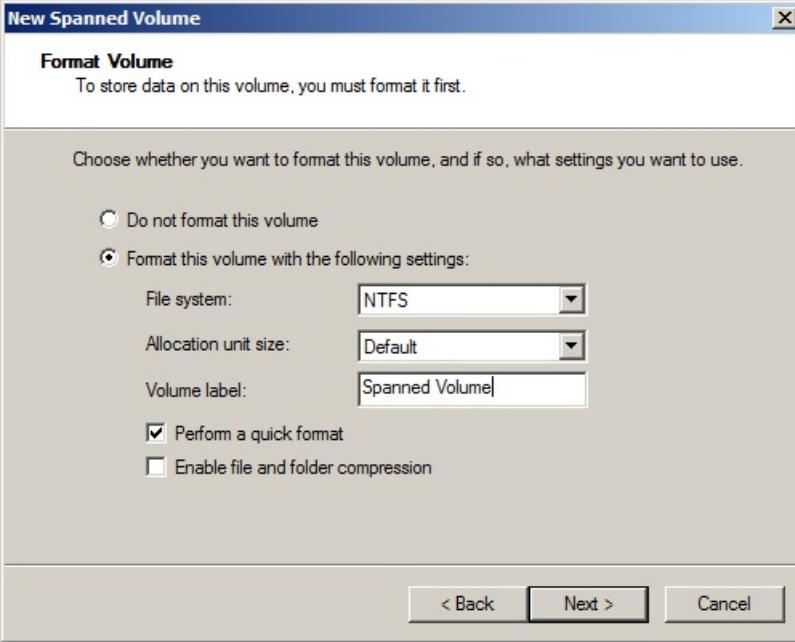
Hình 3.3.1a New Spanned Volume

Chọn **Disk 1** với 100MB và **Disk 2** với 200MB



Hình 3.3.1b Select Disks (Spanned Volume)

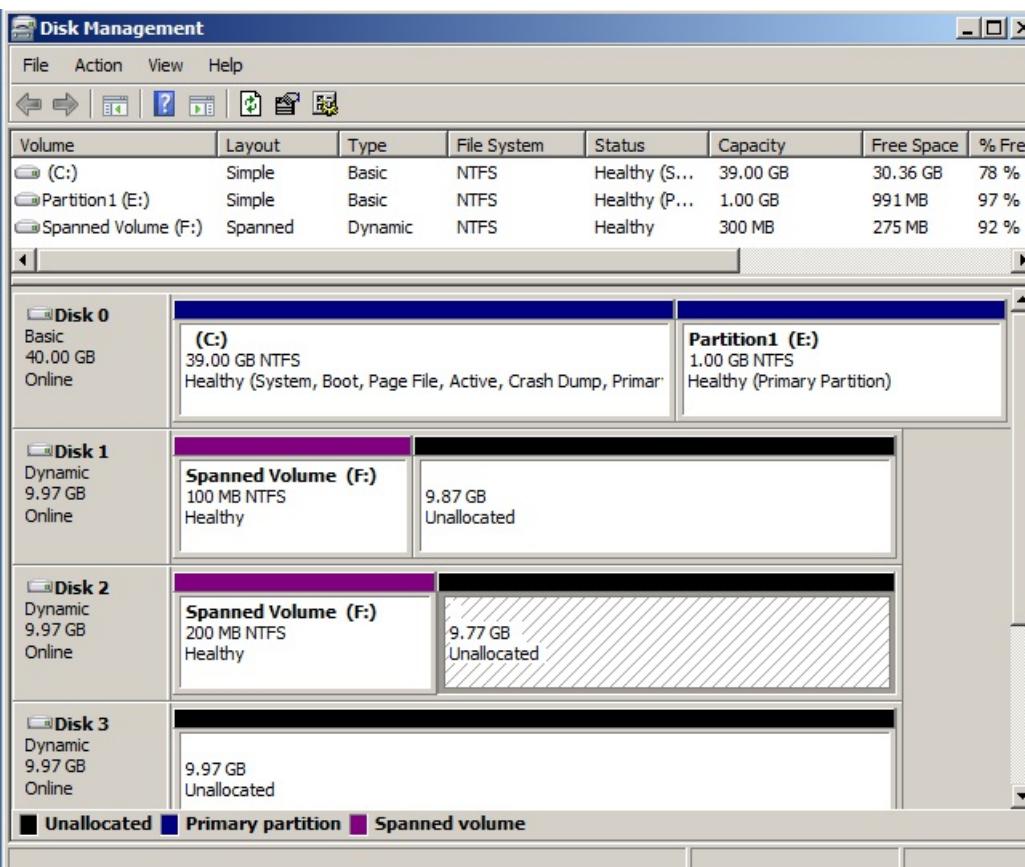
Đặt tên là **Spanned Volume** với định dạng **NTFS**



Hình 3.3.1c Format Volume (Spanned Volume)

Sau khi tạo thành công ta được một **Spanned Volume** với **100MB** trong **Disk 1** và **200MB** trong **Disk 2**. Tuy nhiên, trong **My Computer** chỉ hiển thị 1 ổ **Spanned Volume(F)** với dung lượng **300MB**.

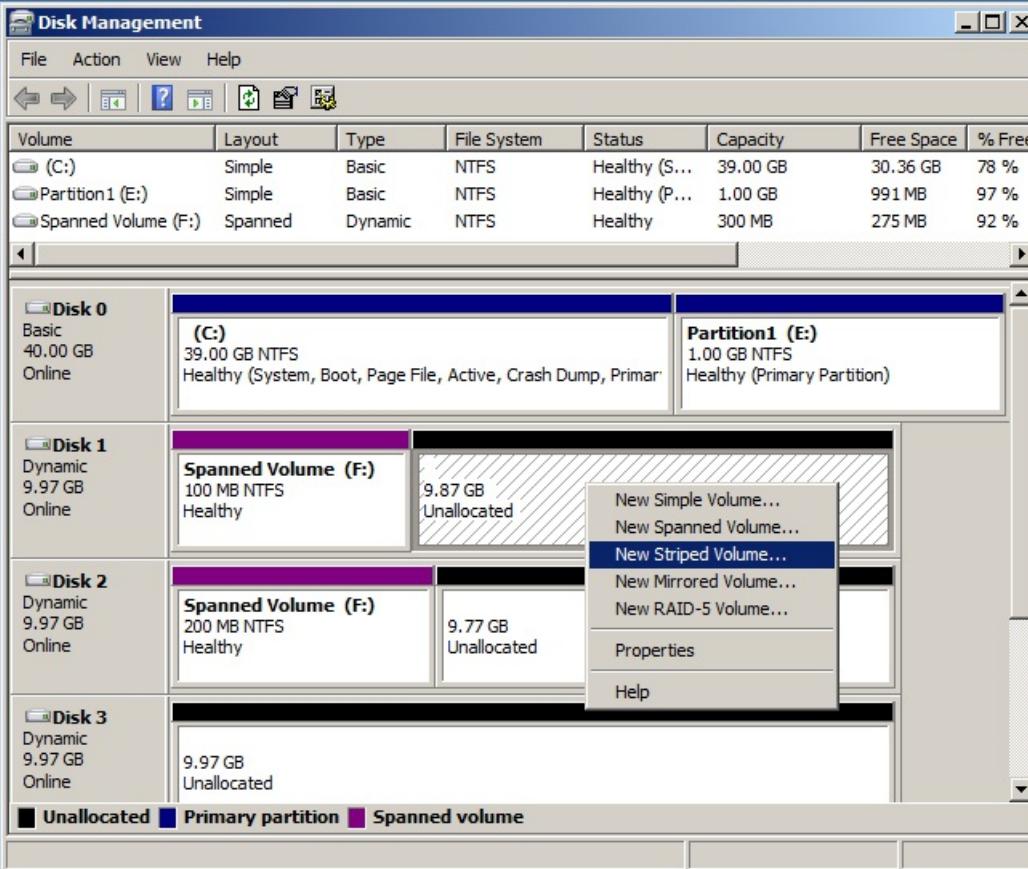
→ Ta khai thác được **300MB** nhưng một trong hai ổ cứng hỏng thì dữ liệu mất hoàn toàn.



Hình 3.3.1d Tạo thành công Spanned Volume

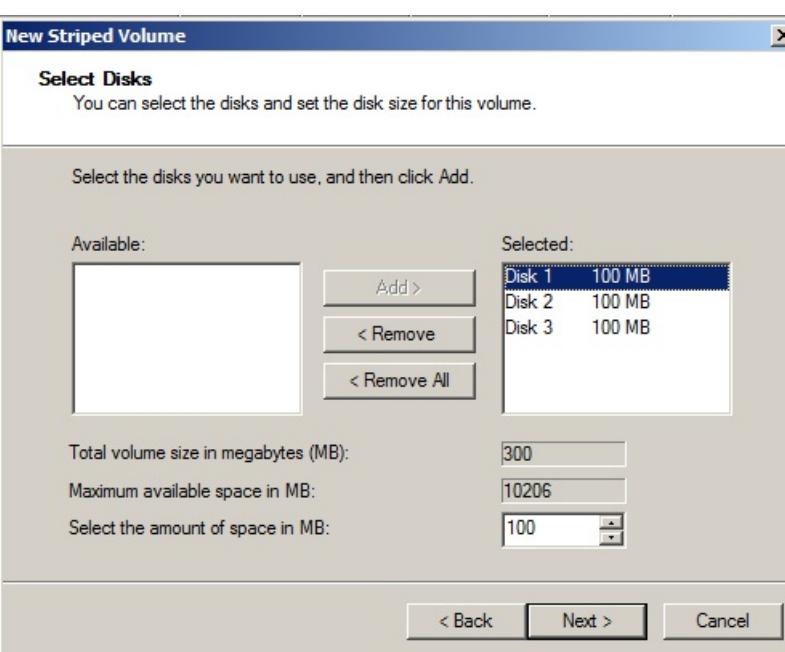
3.3.2 Tạo Striped Volume

Tạo **Striped Volume**: click phải chuột vào **Unallocated** chọn **New Striped Volume**



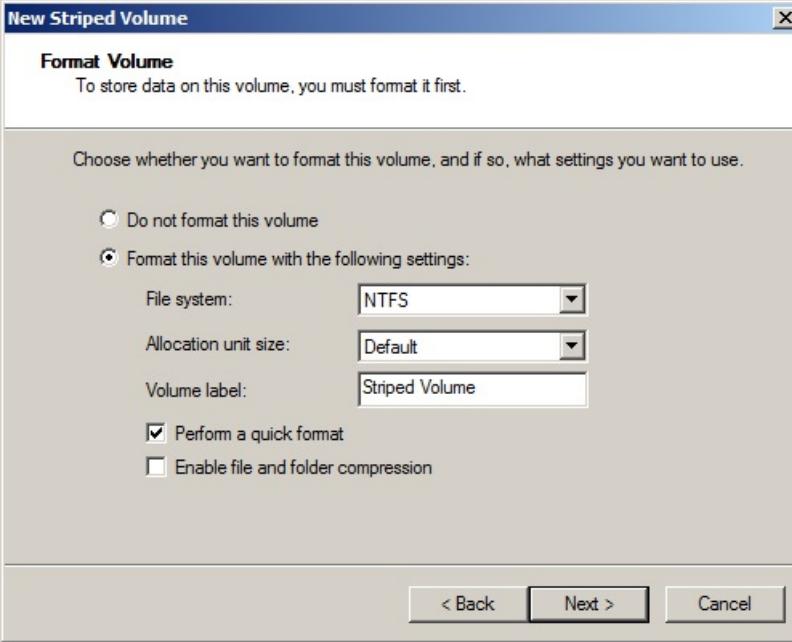
Hình 3.3.2a New Striped Volume

Chọn dung lượng của 3 **Disk 1, Disk 2, Disk 3** là **100MB**



Hình 3.3.2b Select Disk (Striped Volume)

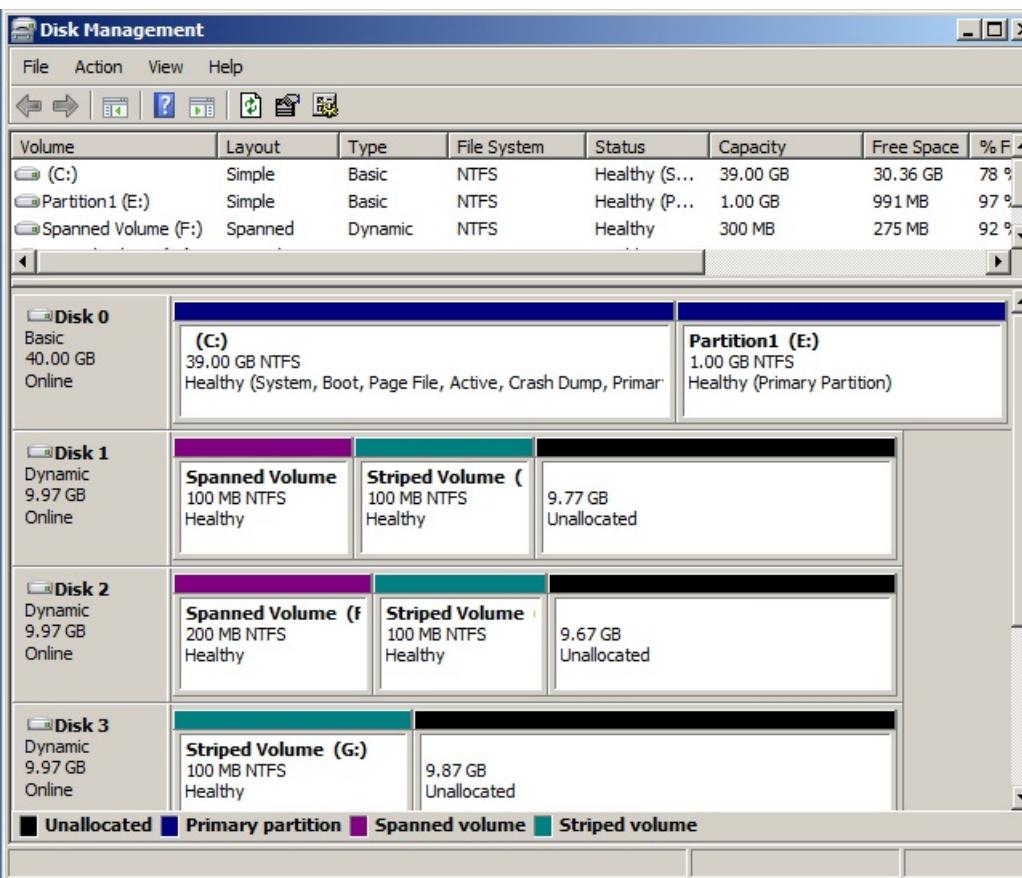
Đặt tên là **Striped Volume** với định dạng **NTFS**



Hình 3.3.2c Format Volume (Striped Volume)

Sau khi tạo thành công ta có một **Striped Volume** được phân tán tại 3 ổ cứng với dung lượng mỗi ổ cứng là **100MB**. Tuy nhiên, trong **My computer** chỉ hiển thị một ổ **Striped Volume(G)** với dung lượng **300MB** mà thôi.

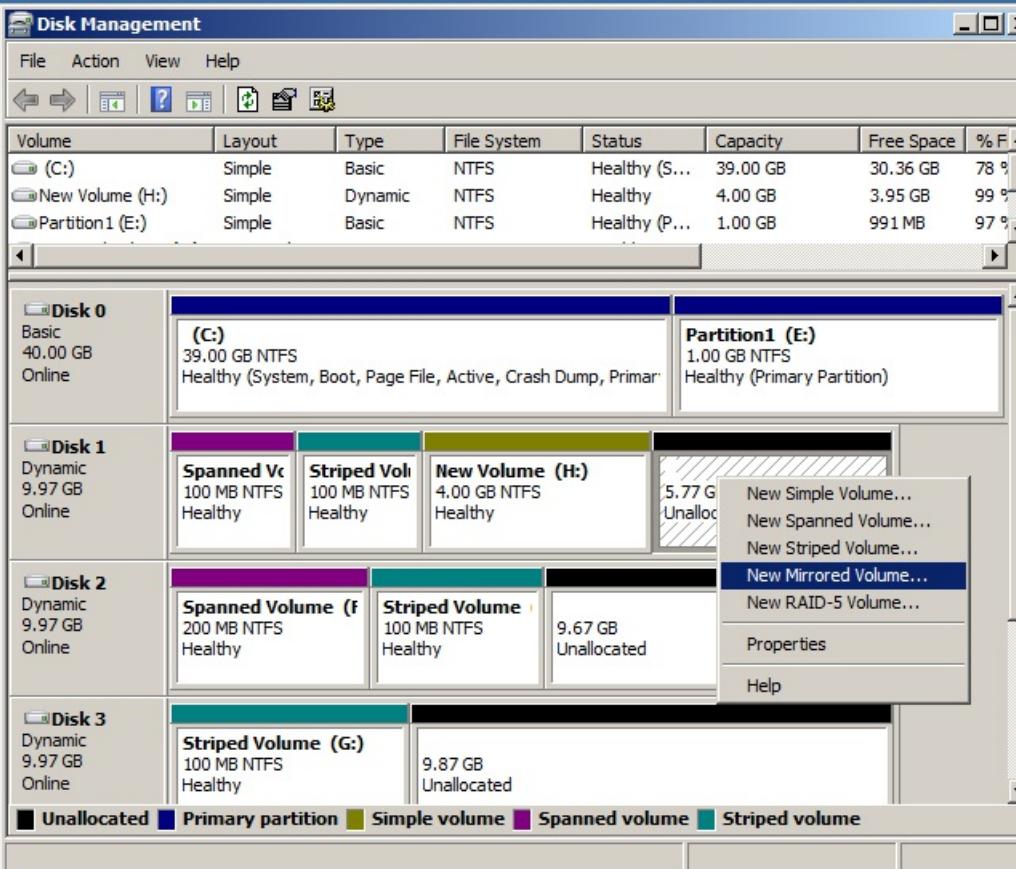
→Ta khai thác được **300MB**, với tùy chọn này khi ghi chép dữ liệu lên đĩa cứng chúng sẽ trãi đều lên cả 3 ổ nên tốc độ ghi chép là cực nhanh vì mỗi ổ cứng chỉ làm 1/3 công việc mà thôi, nhưng một trong ba ổ cứng bị hỏng thì dữ liệu hoàn toàn mất trắng.



Hình 3.3.2d Đã tạo thành công Striped Volume

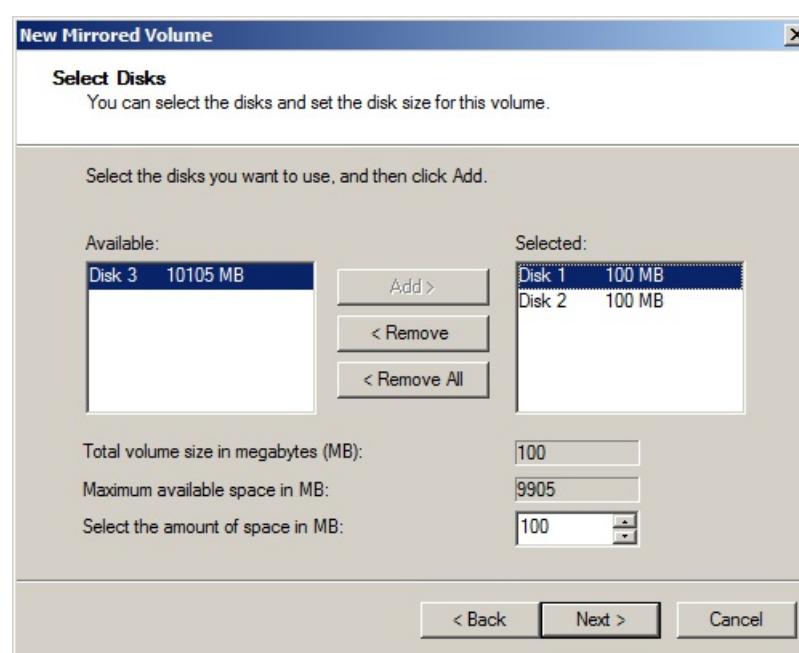
3.3.3 Tạo Mirrored Volume

Tạo **Mirrored Volume**: Chuột phải vào **Unallocated** chọn **New Mirrored Volume**



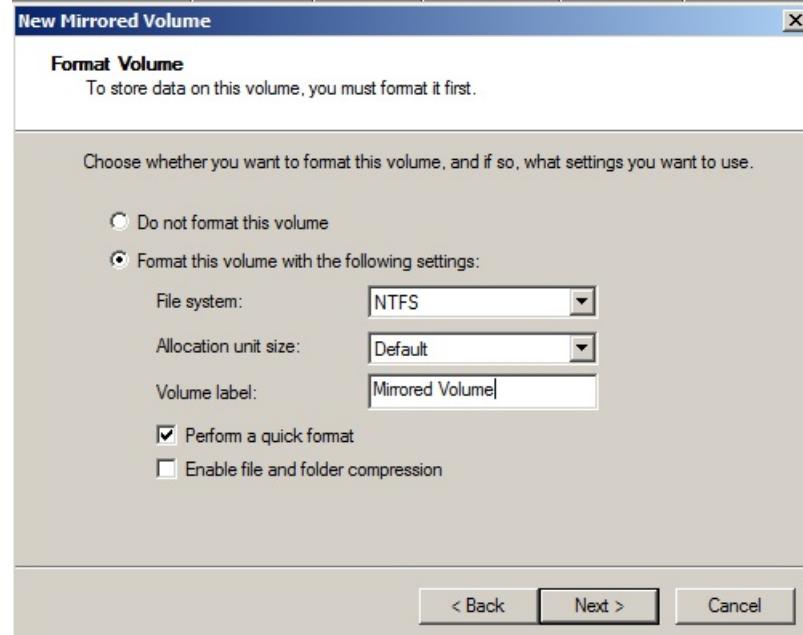
Hình 3.3.3a New Mirrored Volume

Chọn Disk 1 với 100MB và Disk 2 với 100MB



Hình 3.3.3b Select Disks (Mirrored Volume)

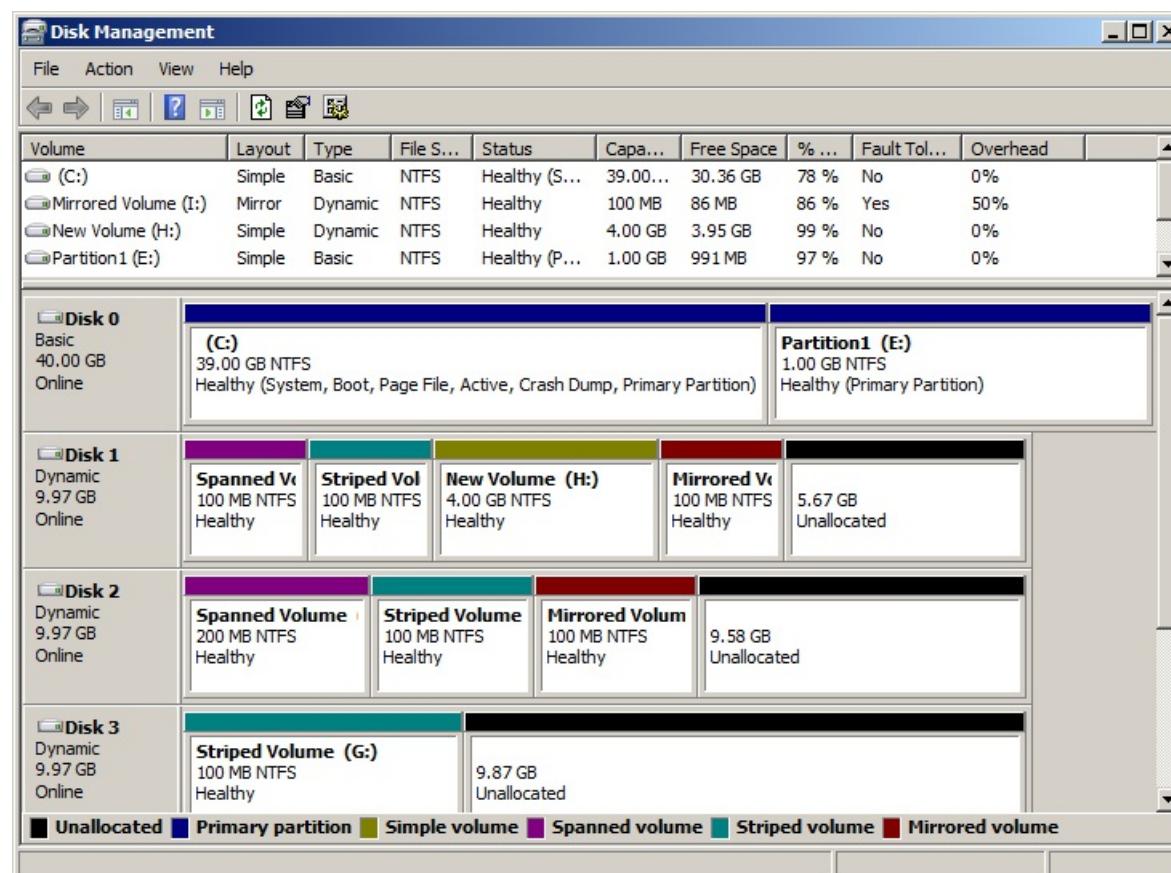
Đặt tên là **Mirrored Volume** với định dạng NTFS



Hình 3.3.3c Format Volume (Mirrored Volume)

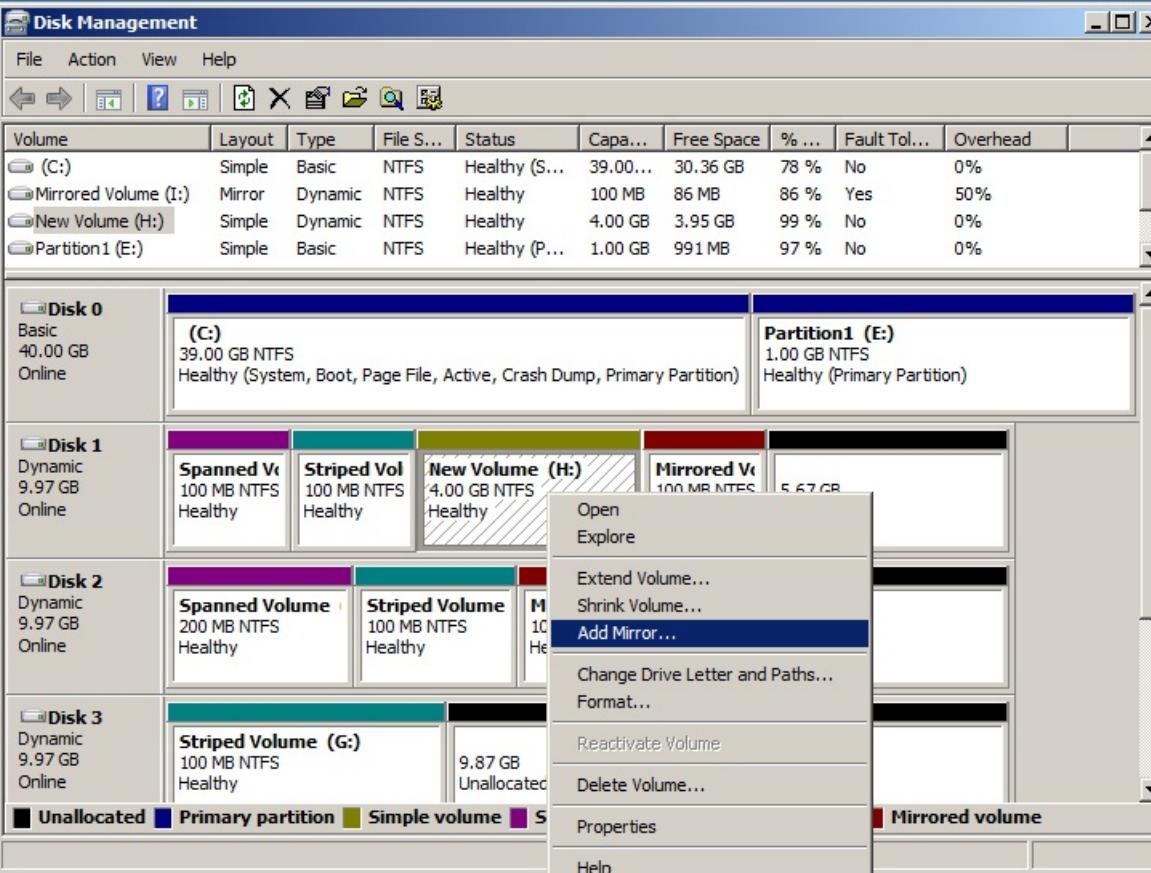
Sau khi tạo thành công ta có 1 **Mirrored Volume** phân tán tại 2 ổ **Disk 1 100MB, Disk 2 100MB**, tuy nhiên **My computer** chỉ hiển thị 1 ổ **Mirrored Volume(I)** với dung lượng **100MB**.

→ Ta chỉ khai thác được **100MB** mà thôi, với tùy chọn này khi ghi chép dữ liệu lên đĩa cứng nó sẽ ghi chép cẩn thận với cùng một thông tin lên cả 2 ổ cứng nên có tốc độ chậm hơn nhưng một trong 2 ổ cứng bị hỏng thì dữ liệu ở kia vẫn còn. Trong các dạng ta làm trước đó thì chỉ có mỗi dạng **Mirrored** là có khả năng chịu lỗi mà thôi, tuy nhiên nó sẽ mất đi **50%** dung lượng.



Hình 3.3.3d Đã tạo thành công Mirrored Volume

Dạng **Mirrored** dùng để dự phòng các dữ liệu quan trọng, với dạng này ta còn có thể tạo dự phòng cho một ổ đĩa có trước nàò mà không cần phải khôi tạo từ 2 phân vùng trắng như các dạng khác. Để thực hiện ta nhấp phải vào một phân vùng **New Volume(H)** của **Disk 1** muốn tạo bản dự phòng chọn **Add Mirror...**



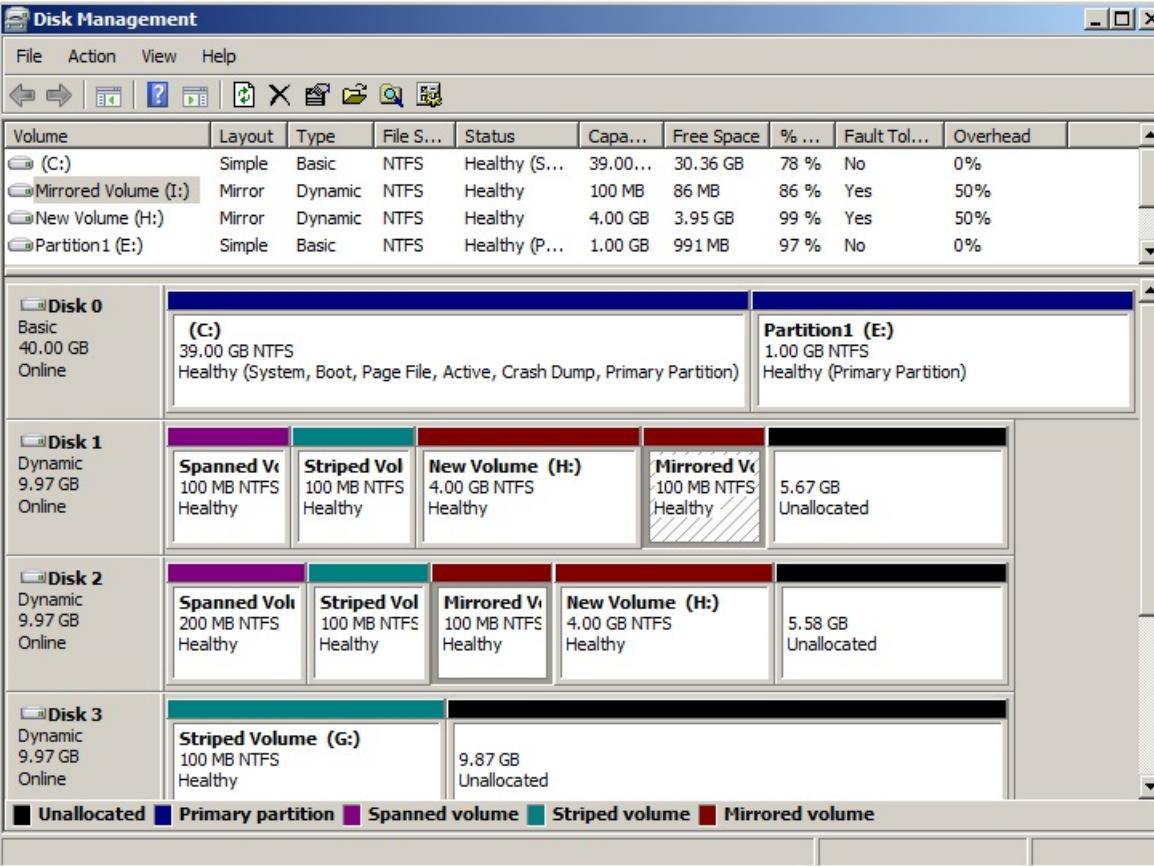
Hình 3.3.3e Tạo Mirror để dự phòng

Cửa sổ **Add Mirror** Sẽ yêu cầu chỉ định ô tạo dự phòng, ở đây là **Disk 2** hoặc **Disk 3**, ta chọn **Disk 2**.



Hình 3.3.3f Add Mirror

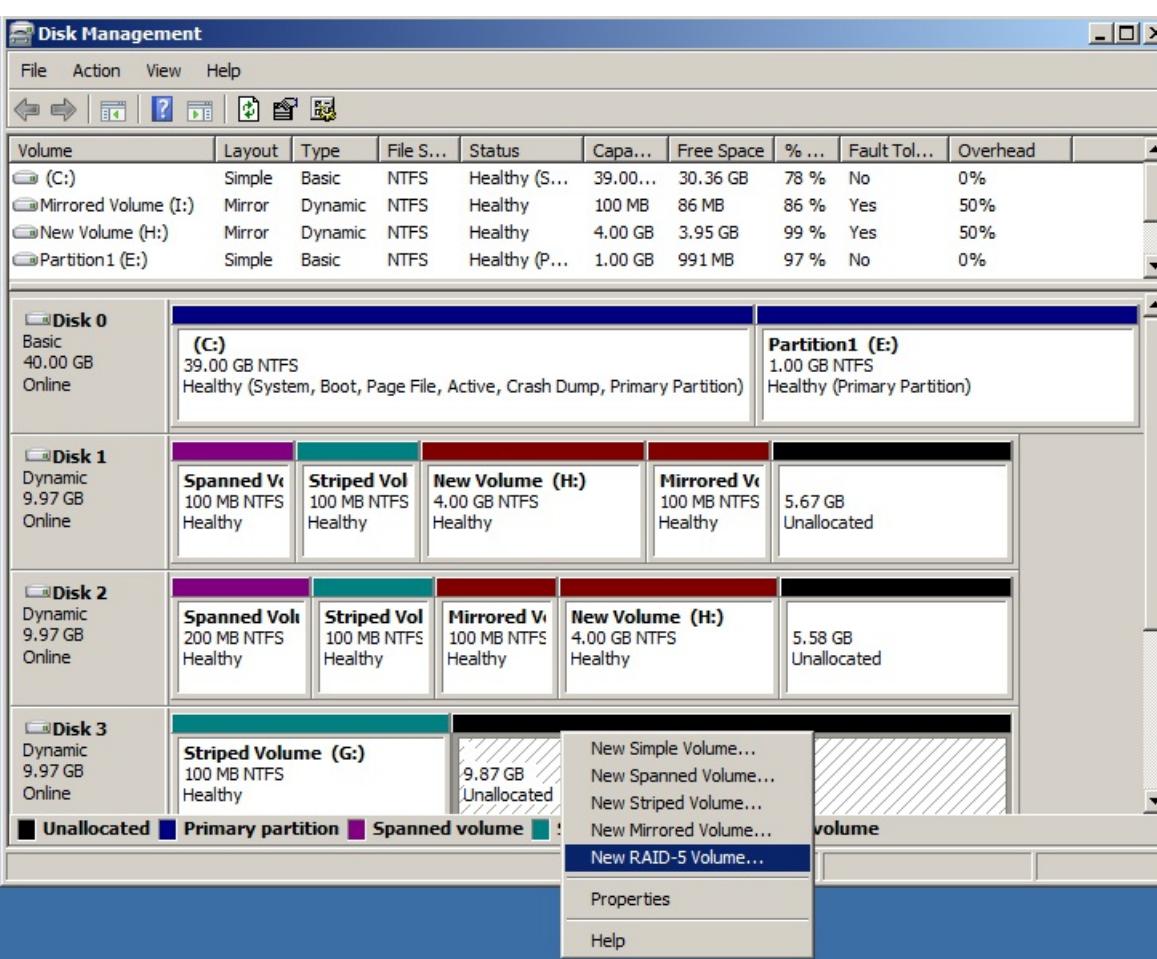
Sau đó **Add Mirror**, windows sẽ tự động tạo một phân vùng mới trên **Disk 2** và copy toàn bộ dữ liệu từ **New Volume(H)** của **Disk 1** sang.



Hình 3.3.3g Đã Add Mirror thành công

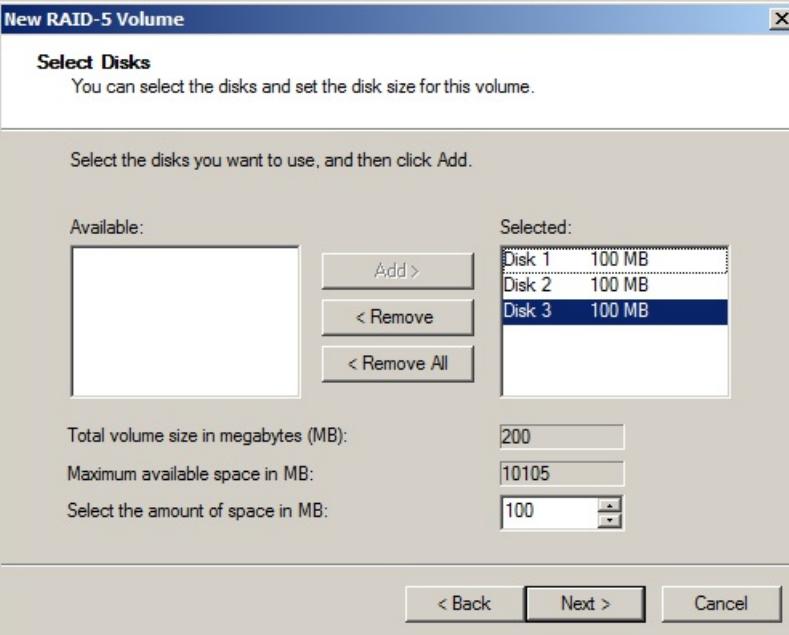
3.3.4 Tạo RAID-5 Volume

Tạo RAID-5: chuột phải vào Unallocated chọn New RAID-5 Volume



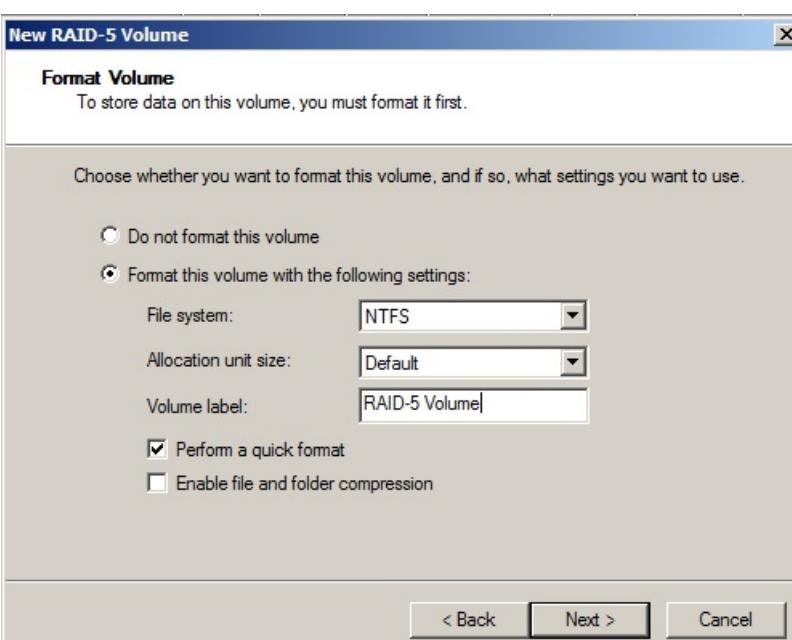
Hình 3.3.4a New RAID-5 Volume

Chọn **Disk 1, Disk 2, Disk 3** với dung lượng mỗi ổ cứng là **100MB**



Hình 3.3.4b Select Disks (RAID-5 Volume)

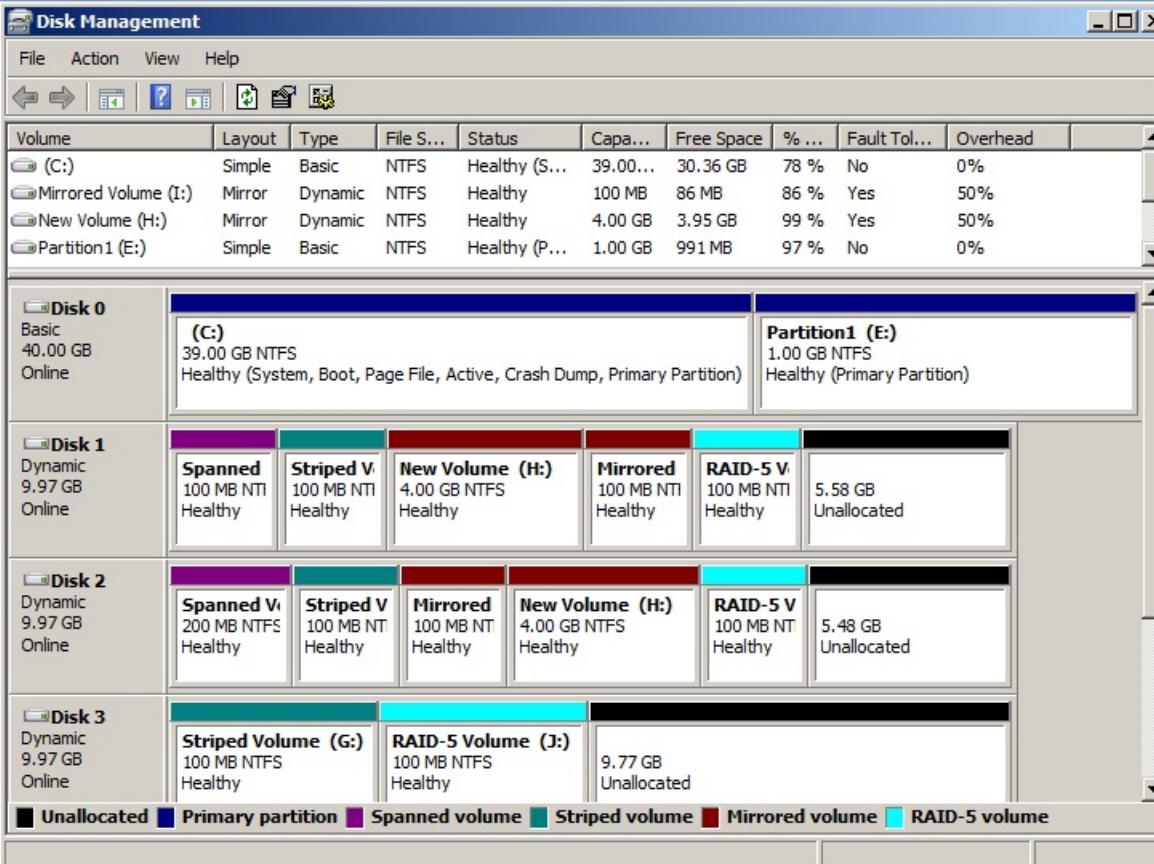
Đặt tên là **RAID-5 Volume** với định dạng là **NTFS**



Hình 3.3.4c Format Volume (RAID-5 Volume)

Sau khi tạo thành công ta được **RAID-5 Volume** phân tán tại 3 **Disk 1, 2, 3** với dung lượng mỗi ổ chiếm **100MB**, tuy nhiên trong **My Computer** chỉ hiển thị 1 ổ **RAID-5 Volume(J)** với dung lượng là **200MB** mà thôi.

→ Chúng ta chỉ khai thác được **200Mb** mà thôi, với tùy chọn này khi ghi chép dữ liệu lên đĩa cứng chúng sẽ ghi chép lên 2 ổ cứng cùng một lúc & một ổ dùng làm file ảnh để phục hồi nếu một trong 2 ổ trên bị lỗi nên có tốc độ **khá nhanh** nhưng một trong 2 ổ cứng bị hỏng thì **dữ liệu vẫn còn**. Dạng **RAID-5** có khả năng chịu lỗi tốt, tuy nhiên nó sẽ mất đi **33%** dung lượng.



Hình 3.3.4d Đã tạo thành công RAID-5 Volume

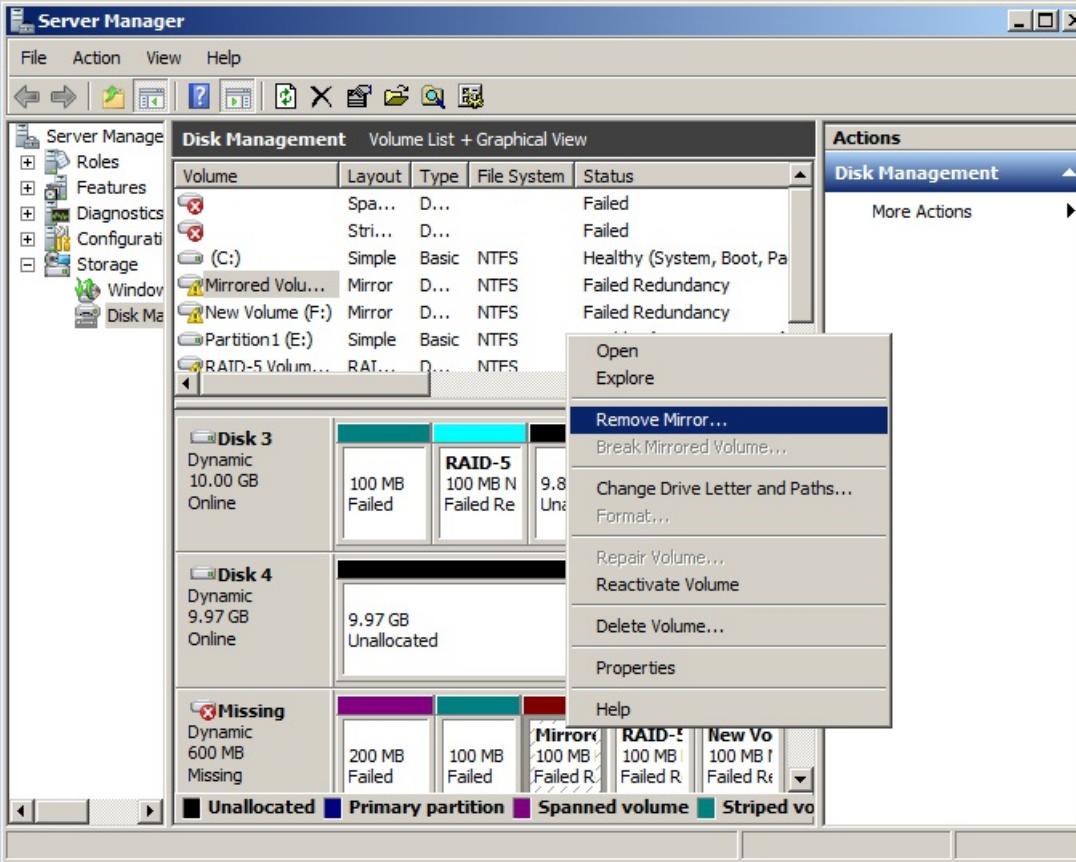
3.3.5 Kiểm lỗi

Tiến hành chép một tệp thử nghiệm vào các phân vùng. Sau đó, gỡ Disk 2 ra khỏi máy tính và rút ra nhận xét:

- Partition1 không bị ảnh hưởng do đĩa bị hỏng là Disk 2, nếu Disk 0 hỏng thì dữ liệu trên phân vùng Partition1 sẽ mất trắng.
- Spanned Volume được định dạng theo spanned nên khi Disk 2 hỏng dữ liệu trên phân vùng này cũng mất đi.
- Striped Volume được định dạng theo striped nên khi một trong các ổ đĩa hỏng dữ liệu sẽ mất đi. Trong trường hợp này, Disk 2 hỏng nên đương nhiên dữ liệu trên phân vùng này cũng mất hết.
- Phân vùng Mirrored Volume dữ liệu vẫn còn nguyên vẹn vì một trong các ổ disk hỏng thì dữ liệu vẫn được an toàn. Nhưng ta phải tiến hành Add Mirror lại cho phân vùng này.
- RAID-5 Volume được định dạng theo RAID-5 nên dữ liệu vẫn được an toàn. Tuy vậy ta phải tiến hành ngay việc Repair Volume cho phân vùng.

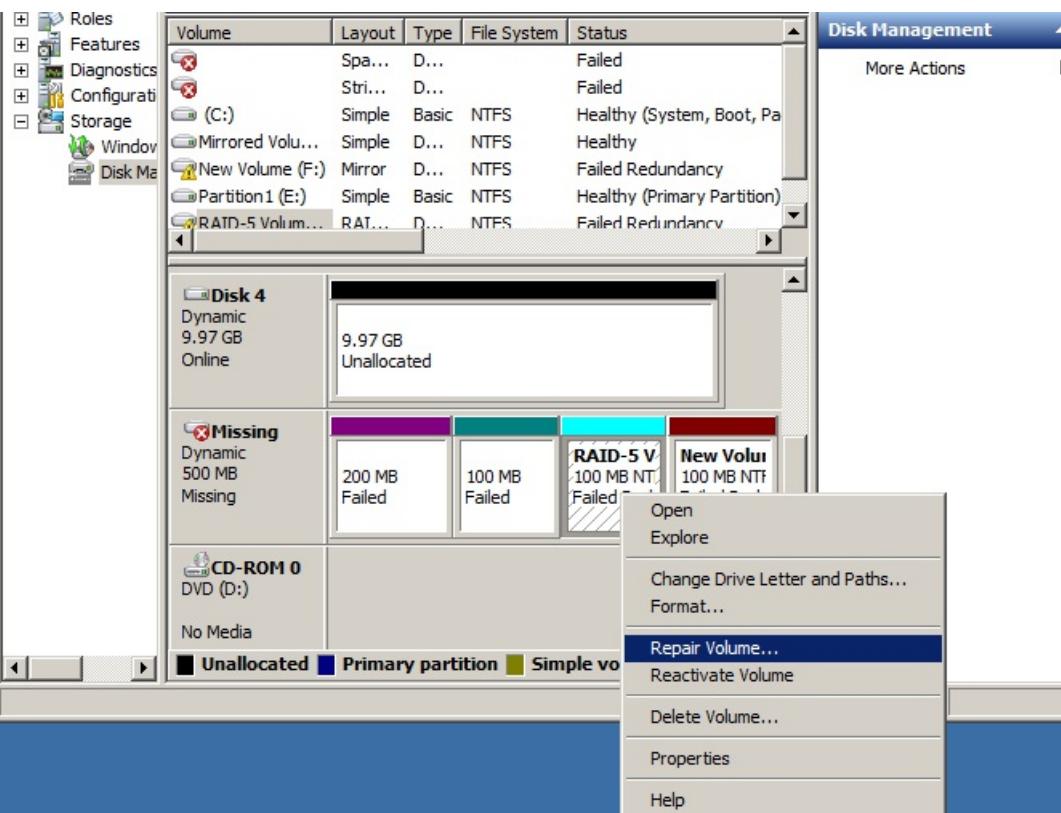
Ta gắn thêm một ổ đĩa vào thay thế cho Disk 2 bị hỏng → Convert Disk 4 này sang Dynamic. Do các phân vùng dạng Spanned và Stripped cơ bản không thể phục hồi được nên ta chỉ đề cập đến phân vùng mirrored và RAID-5.

- Sửa lỗi cho Mirrored Volume
- Ta tiến hành Remove mirror bằng cách click phải chuột vào Mirrored Volume của ổ Missing. Sau đó click chọn vào ô đang missing và tiến hành xóa.



Hình 3.3.5a Remove Mirror

- Sau khi remove mirror ta tiến hành add lại mirror cho volume, chọn nơi add là Disk 4 để gỡ lỗi cho phân vùng.
- Gỡ lỗi cho RAID-5 Volume
- Ta chọn Repair Volume bằng cách click phải chuột vào RAID-5 Volume bị missing. Sau đó chọn repair vào Disk 4 để khôi phục lại RAID-5.

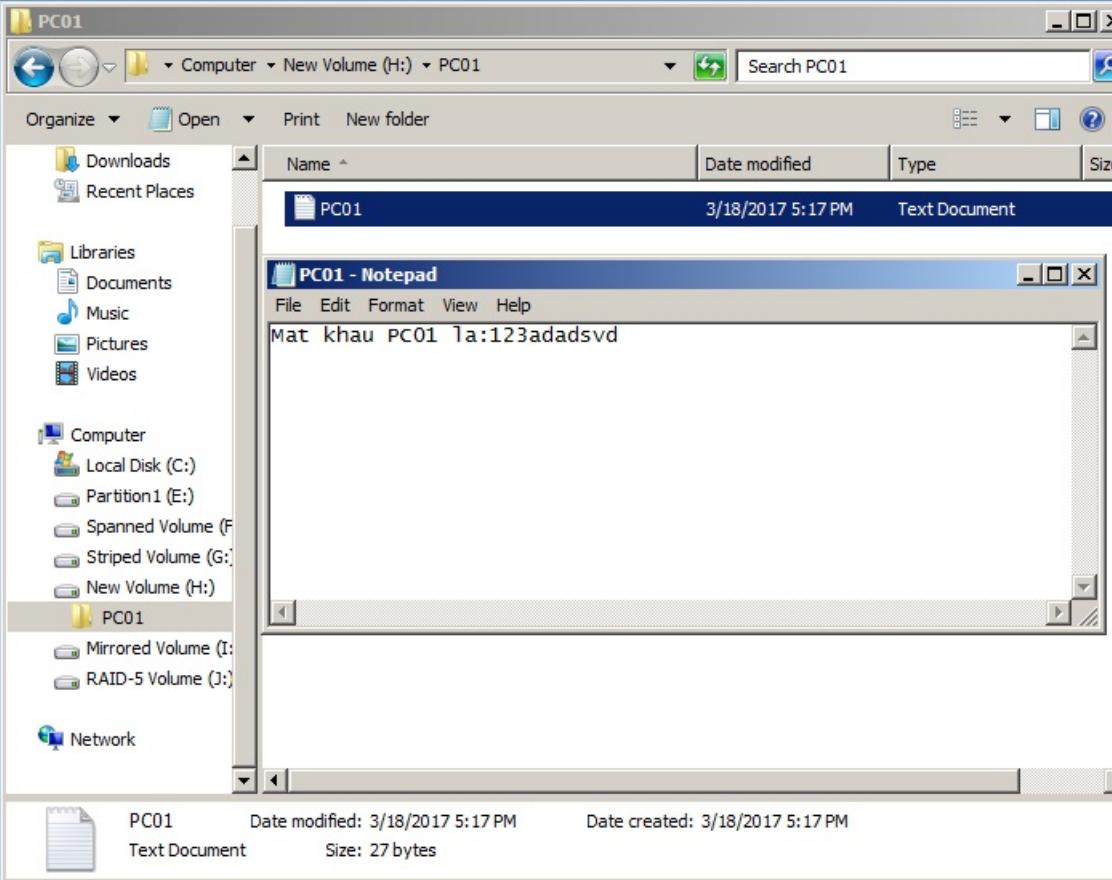


Hình 3.3.5b Repair RAID-5 Volume

3.4 Mã hóa

Sử Dụng máy tính Windows Server 2008 R2. Tạo 2 User: PC01 và PC02.

Đăng nhập vào PC01. Trong ổ đĩa H, tạo file dữ liệu PC01 trong thư mục PC01.



Hình 3.4.1 Tạo File PC01

Click phải vào thư mục PC01 chọn Properties → Advanced



Hình 3.4.2 Properties folder

Trong hộp thoại Advanced Attributes → check vào mục Encrypt contents to secure data để tiến hành mã hóa dữ liệu → Chọn OK



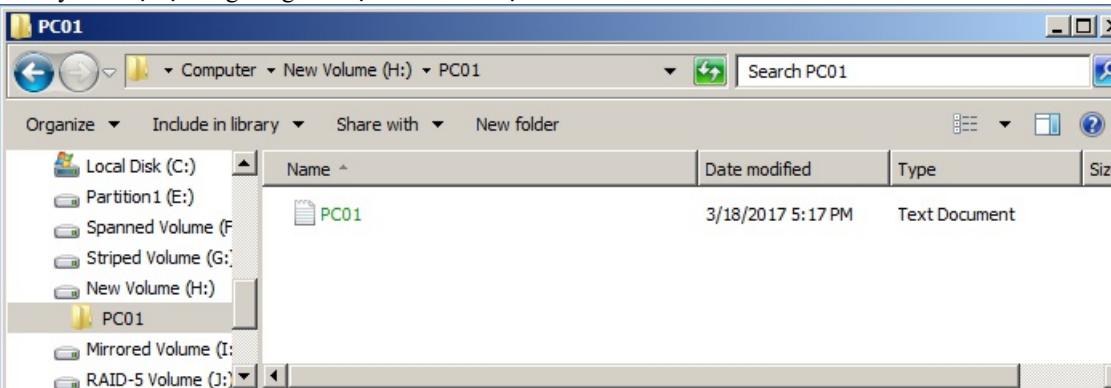
Hình 3.4.3 Advanced Attributes

Trong hộp thoại **Confirm Attribute Changes**, chọn **Apply changes to this folder, subfolders and files** → OK



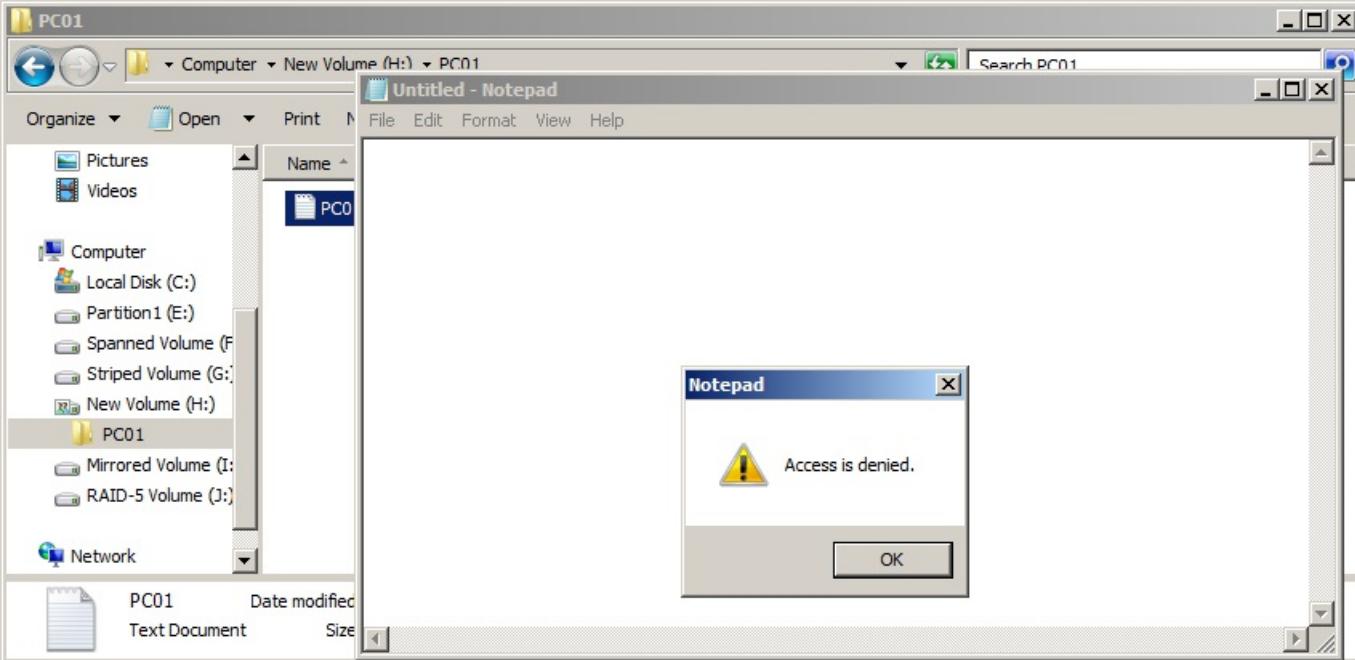
Hình 3.4.4 Confirm Attribute Changes

Ta thấy toàn bộ nội dung trong thư mục PC01 đã được mã hóa.



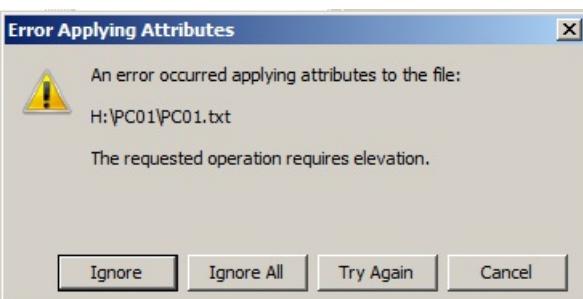
Hình 3.4.5 Tập tin đã được mã hóa

Ta đăng xuất khỏi PC01. Tiến hành đăng nhập vào PC02, truy xuất vào ổ (H) → thư mục PC01 → file PC01, ta nhận thông báo **Access is denied**.



Hình 3.4.6 Access is denied

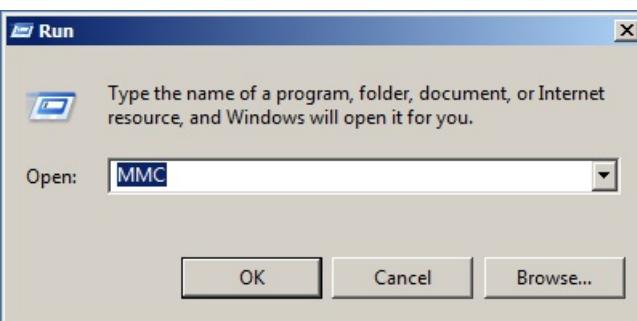
Ta thử bỏ chức năng mã hóa của thư mục ra và hệ thống báo lỗi không cho giải mã thư mục này. Chỉ duy nhất tài khoản **PC01** mới có thể giải mã cho thư mục **PC01** này.



Hình 3.4.7 Error Applying Attributes

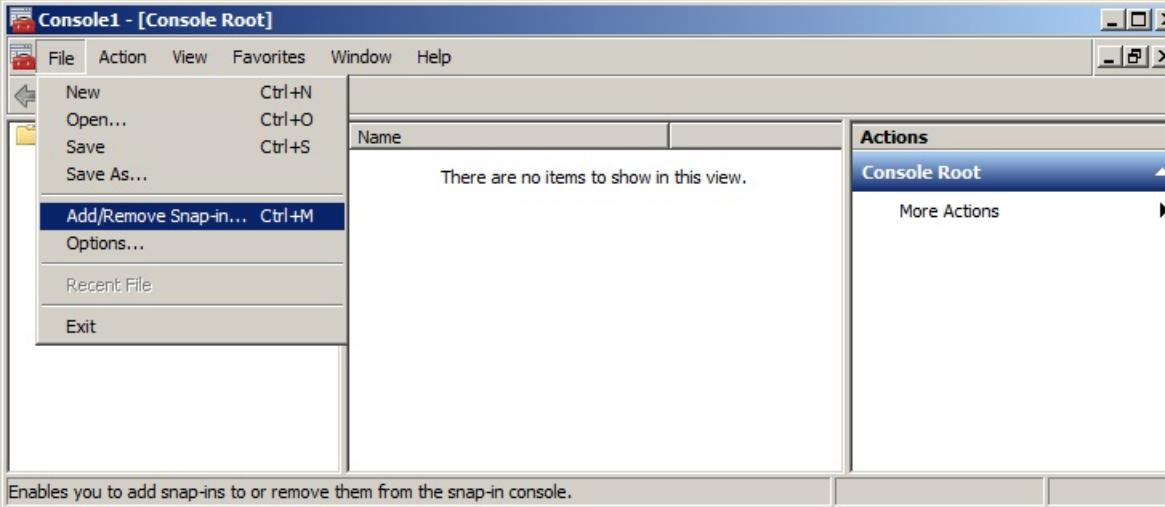
Để giải mã dữ liệu, ta phải tiến hành trích xuất Certificate của User **PC01** dùng mã hóa, **import Certificate** này vào **ngăn chứa Certificate** của User **PC02**.

Ta đăng nhập vào **PC01**, chọn **Start → Run → MMC → OK**



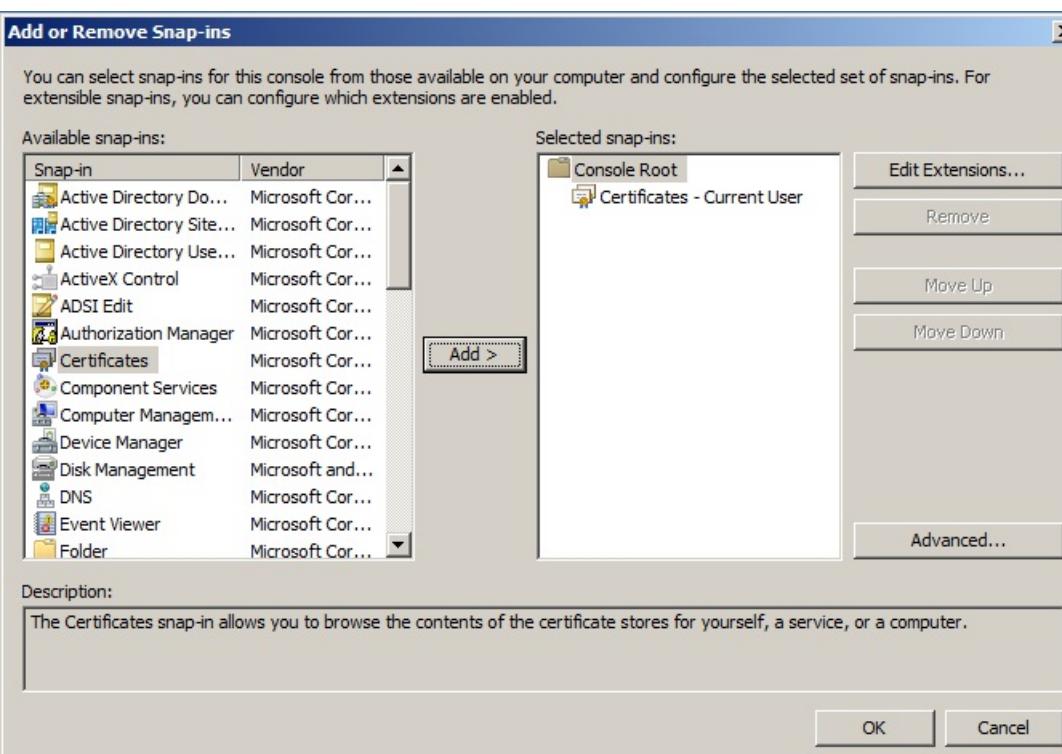
Hình 3.4.8 Run MMC

Ta vào **File → Chọn Add/Remove Snap-in**



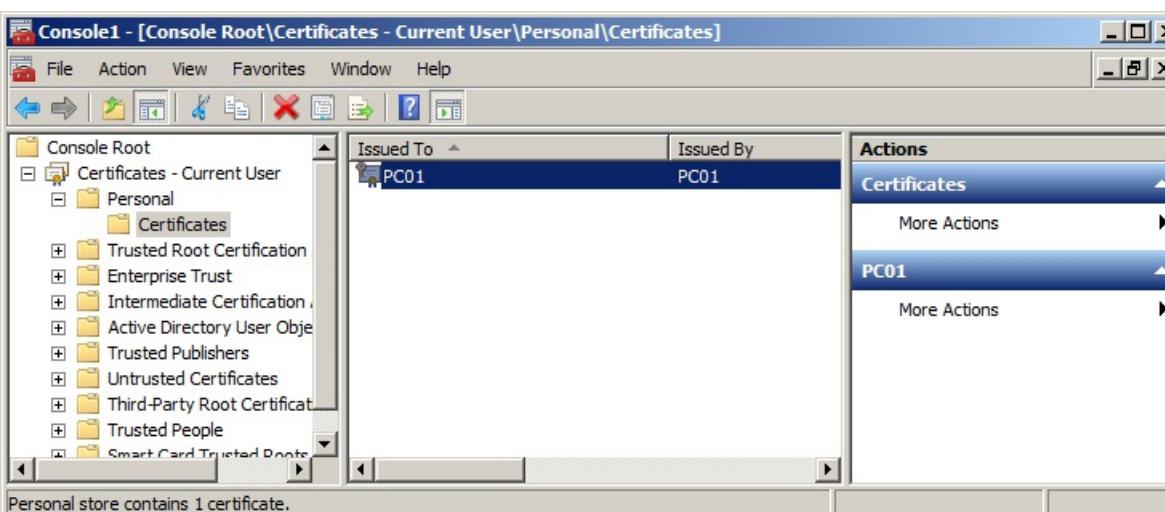
Hình 3.4.9 Console Root

Trong hộp thoại **Add or Remove Snap-ins** → Chọn **Certificates** → **Add** → **OK**



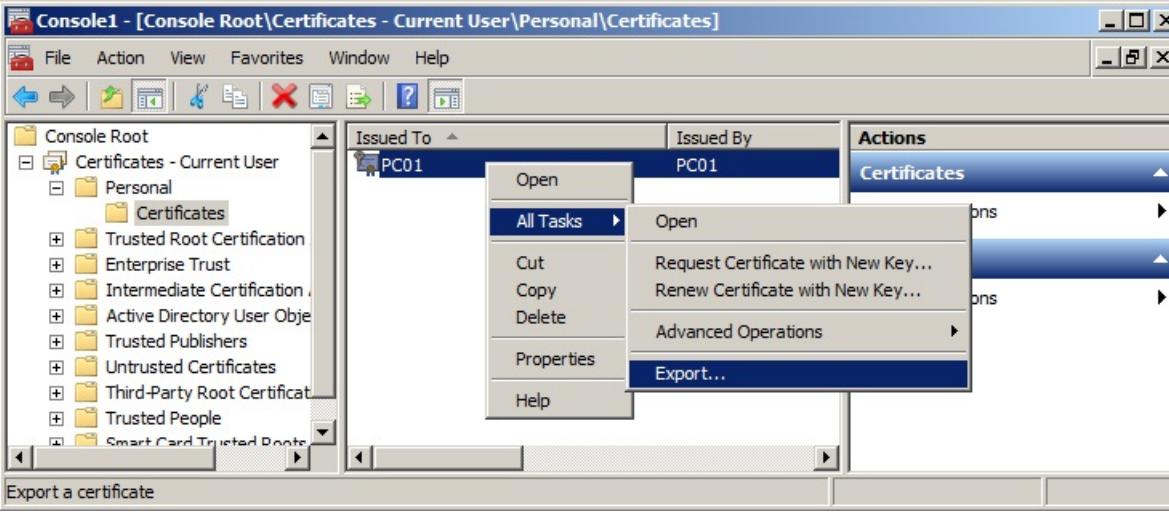
Hình 3.4.10 Add or Remove Snap-ins

Lúc này ngăn chứa Certificate hiện ra ta chọn vào **Certificates – Current User** → **Personal** → **Certificates**



Hình 3.4.11 Certificates

Phải chuột vào PC01 chọn **All Tasks** → **Export**



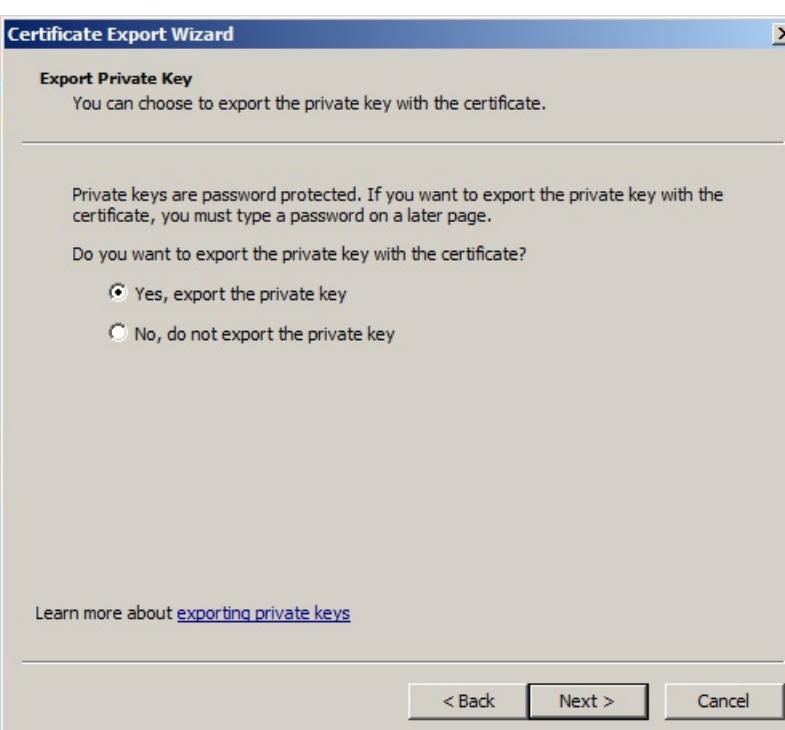
Hình 3.4.12 Export

Hộp thoại **Certificate Export Wizard** xuất hiện → Next



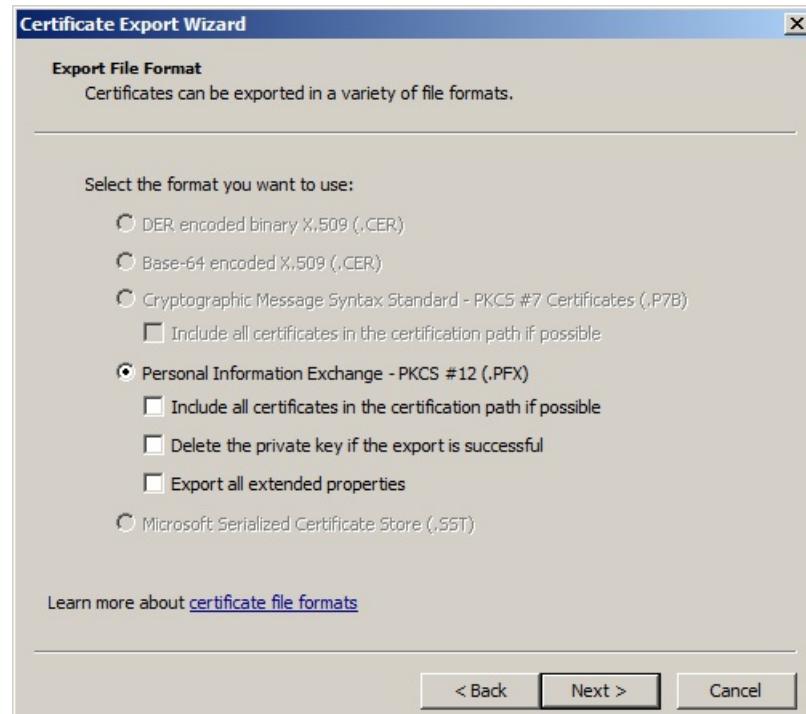
Hình 3.4.13 Certificate Export Wizard

Trong hộp thoại **Export Private Key**, click chọn vào Yes, export the private key → Next



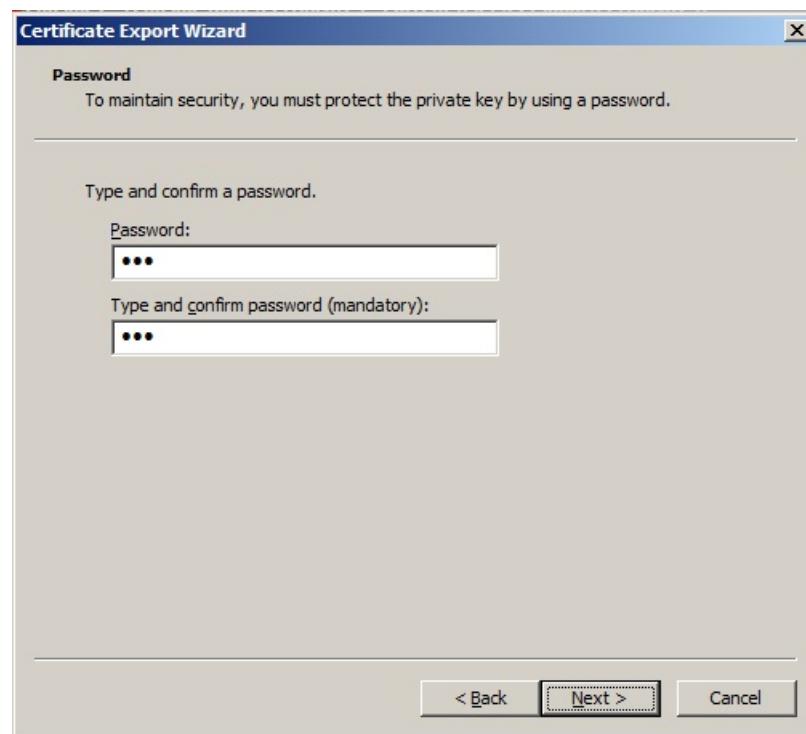
Hình 3.4.14 Export Private Key

Trong hộp thoại **Export File Format**, click chọn **Next**



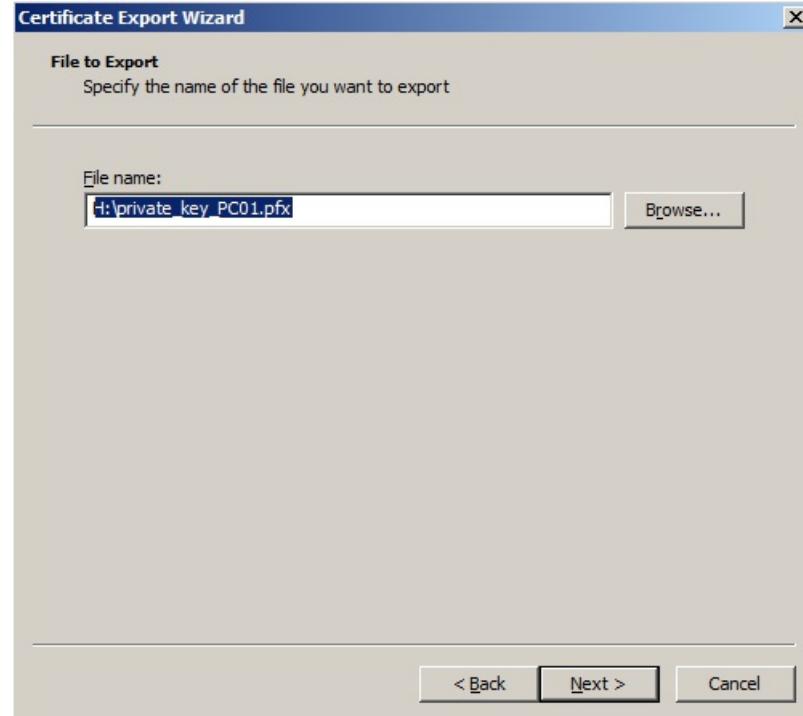
Hình 3.4.15 Export File Format

Trong hộp thoại **Password** ta tiến hành nhập vào Password để bảo vệ pravite key (Nếu muốn) → Next



Hình 3.4.16 Pasword

Trong hộp thoại **File to export**, click vào **Browse** để chọn nơi lưu Certificate đã export → Ta chọn đường dẫn **H:\private_key_PC01.pfx** → Next



Hình 3.4.17 File to export

Chọn **Finish** để hoàn tất quá trình Export Certificate



Hình 3.4.18 Finish export

Hệ thống thông báo export thành công.



Hình 3.4.19 The export was successful

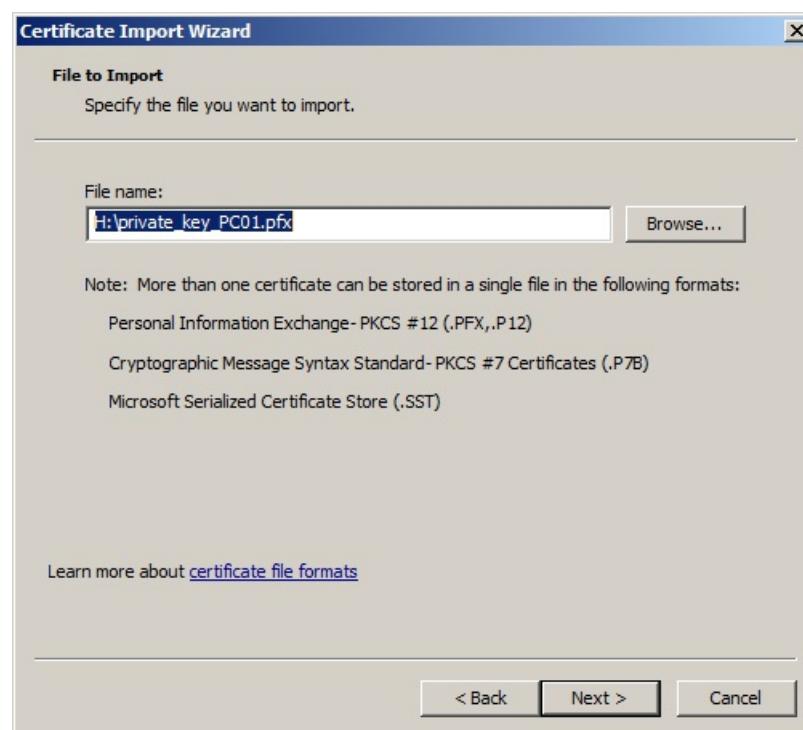
Tiếp theo ta đăng nhập vào PC02 để tiến hành Import Certificate của PC01 vào PC02.

Trong PC02, ta chọn **Start → Run → MMC**. Cửa sổ **Console** hiện ra, click chọn **File → Add/Remove Snap-in**. Trong hộp thoại **Add or Remove Snap-ins → Certificates → Add → OK**. Sau đó chọn **Certificates – Current User → Personal**. Phải chuột vào **Personal** chọn **All Tasks → Import**. Cửa sổ **Certificate Import Wizard** mở ra, chọn **Next**.



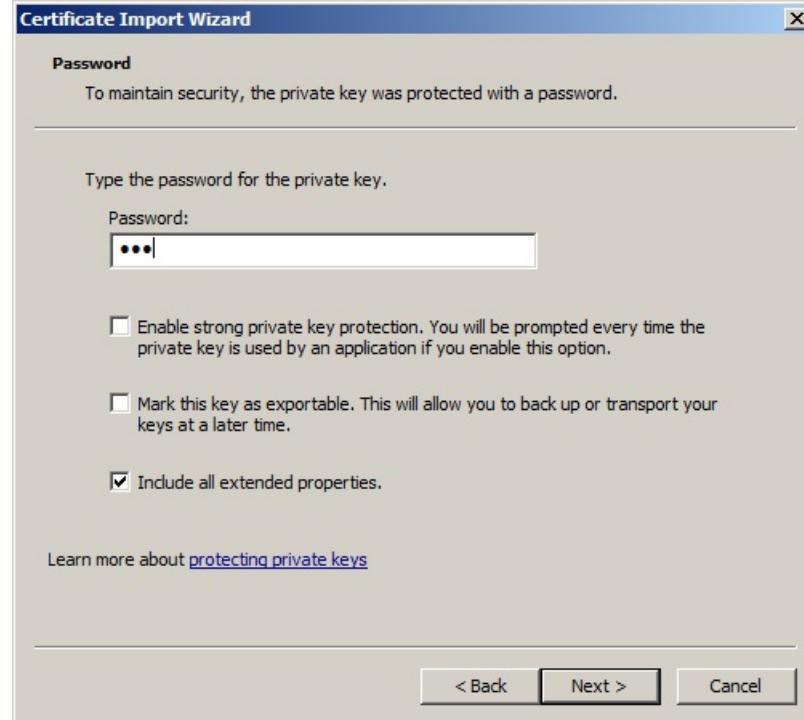
Hình 3.4.20 Certificate Import Wizard

Trong hộp thoại **File to Import**, ta chọn **Browse** để chọn đường dẫn đến Certificate đã export từ PC01. Sau đó chọn **Next**.



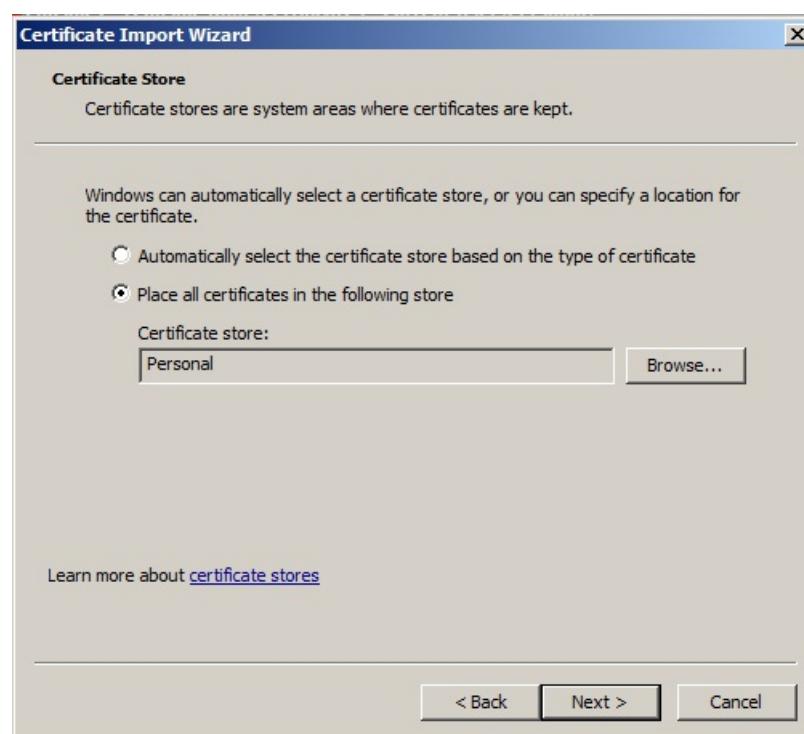
Hình 3.4.21 File to import

Hộp thoại **Password** mở ra, nhập password bảo vệ private key → **Next**.



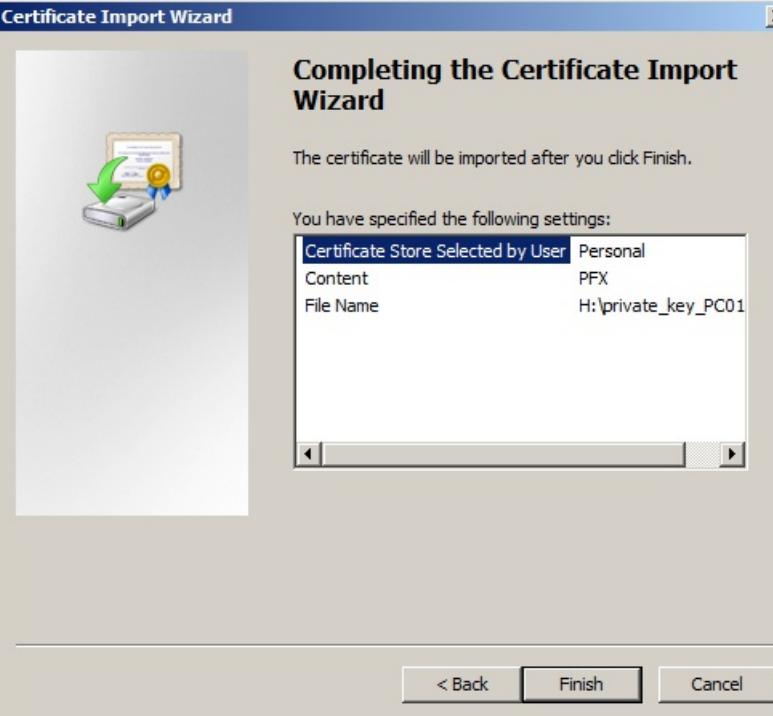
Hình 3.4.22 Pasword Import

Trong hộp thoại **Certificates Store** → Chọn **Nexxt**.



Hình 3.4.23 Certificate Store

Chọn **Finish** để kết thúc quá trình Import Certificate.



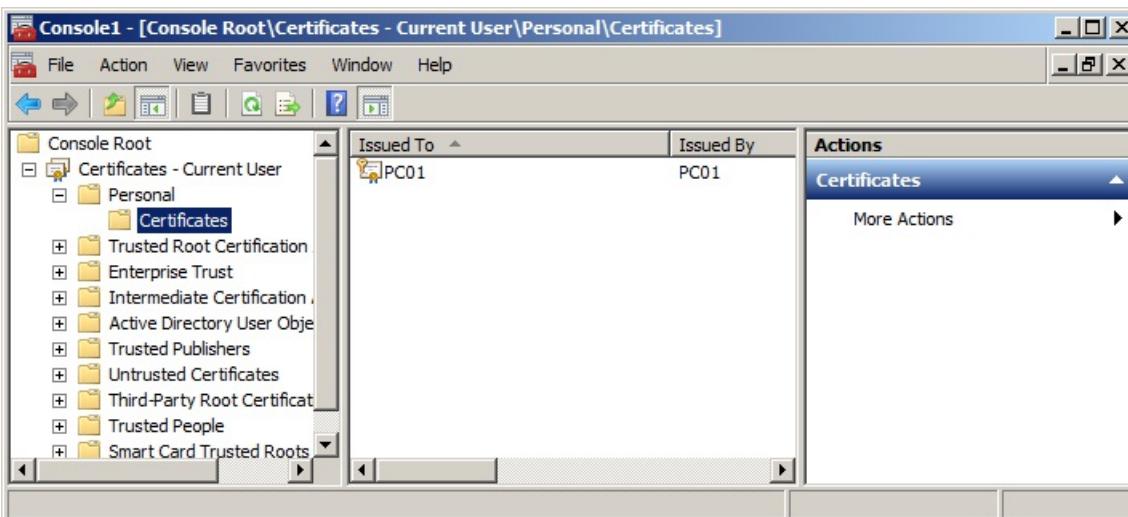
Hình 3.4.24 Finish Import

Hệ thống thông báo import thành công.



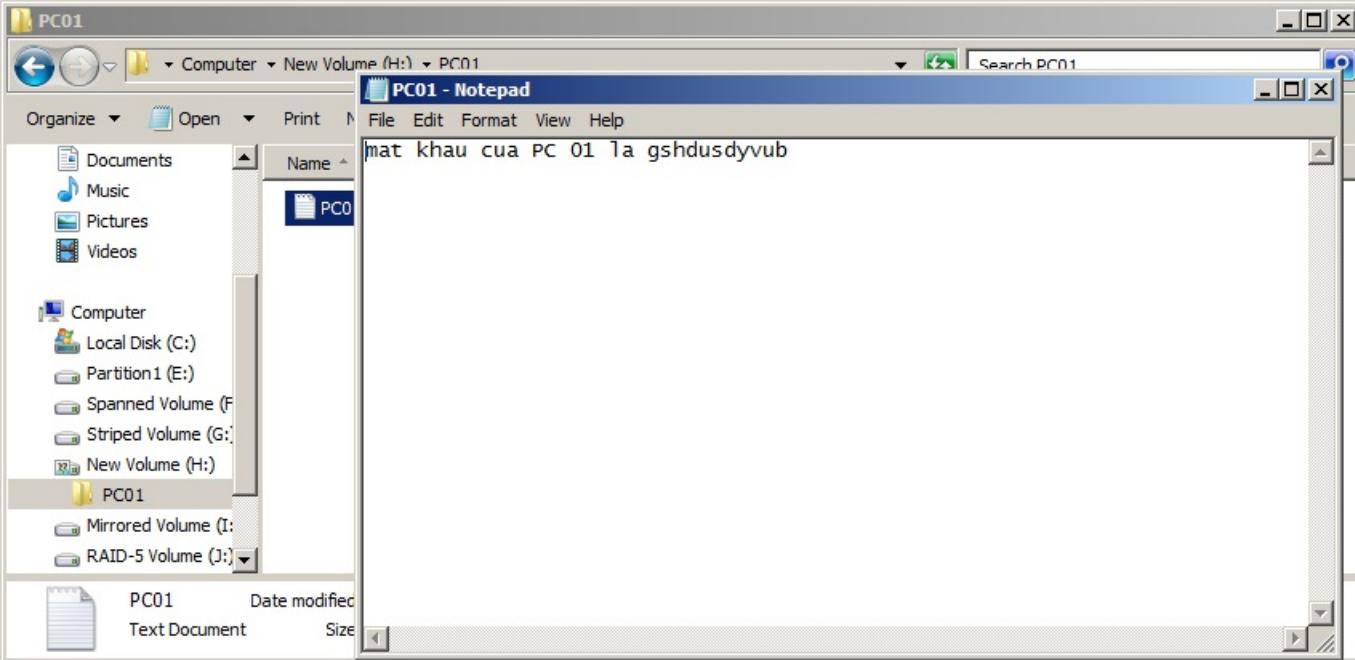
Hình 3.4.25 The import was successful

Lúc này ta thấy Certificate đã xuất hiện trong ngăn chứa của PC02



Hình 3.4.26 Certificates đã được import

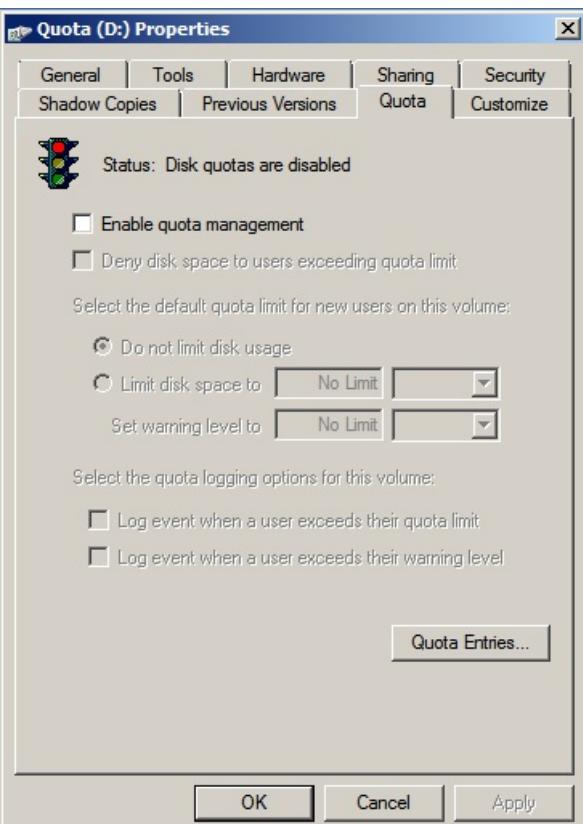
Ta tiến hành truy cập vào file PC01 trong thư mục PC01 bằng user PC02. Kết quả ta đã giải mã thành công.



Hình 3.4.26 Giải mã thành công

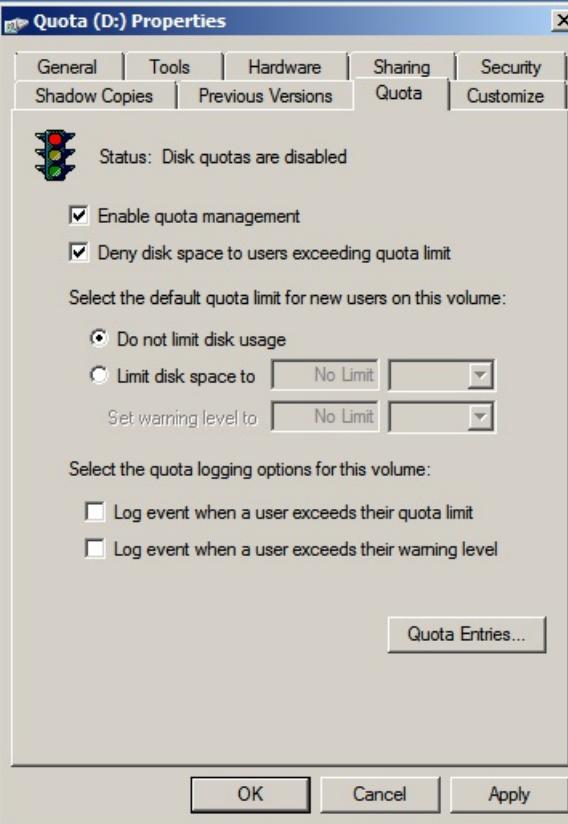
3.5 Cấu hình hạn ngạch đĩa

Tạo User PC01. Đăng nhập vào tài khoản Administrator. Phải chuột vào đĩa Quota(D) → Properties → Tab quota



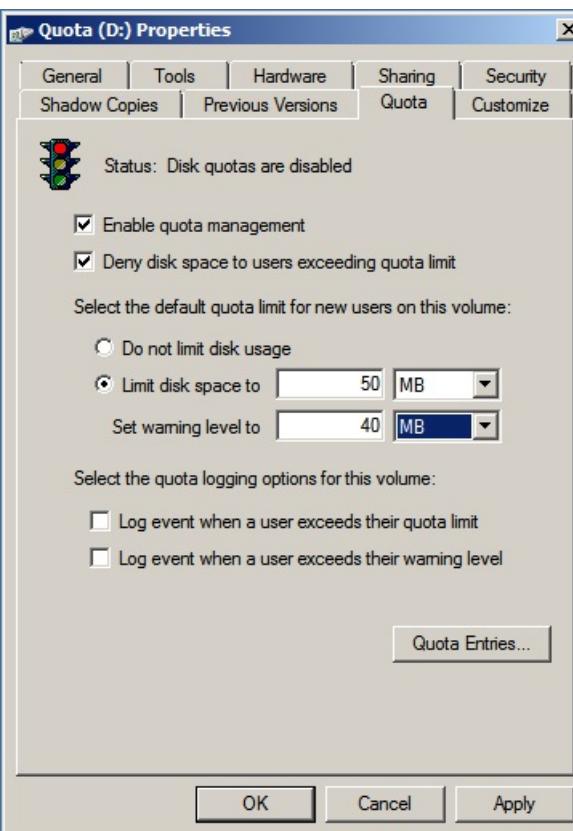
Hình 3.5.1 Tab Quota

Click chọn vào **Enable quota management** → Sau đó click tiếp vào **Deny disk space to users exceeding quota limit**



Hình 3.5.2 Enable quota management

Click chọn vào **Limit disk space to** tùy chỉnh **50MB**, ở mục **Set warning level to** tùy chỉnh **40MB** → Sau đó **Apply**



Hình 3.5.3 Tùy chỉnh giới hạn cho phép và cảnh báo

Click chọn **OK** khi Disk Quota thông báo



Hình 3.5.4 Áp dụng hạn ngạch

Tiến hành đăng nhập bằng User **PC01** → Copy một thư mục bất kì lớn hơn 50MB vào ổ đĩa đã thiết lập hạn ngạch. Ta được cảnh báo



Hình 3.5.5 Copy Item (PC01)

Như vậy hạn ngạch vừa thiết lập đã áp dụng cho PC01

- **Trường hợp ta muốn chỉ định hạn ngạch cho từng cá nhân**

Ta đăng nhập vào Administrator.

Trong Tab Quota của hộp thoại Properties → Chọn Quota Entries, hộp thoại Quota Entries for Quota (D:) hiện ra

Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
War...	PC01	PC01@trant...	49.27 MB	50 MB	40 MB	98
OK	BUILTIN\Administrators		71 KB	No Limit	No Limit	N/A
OK	NT AUTHORITY\SYSTEM		20 MB	No Limit	No Limit	N/A

3 total item(s), 1 selected.

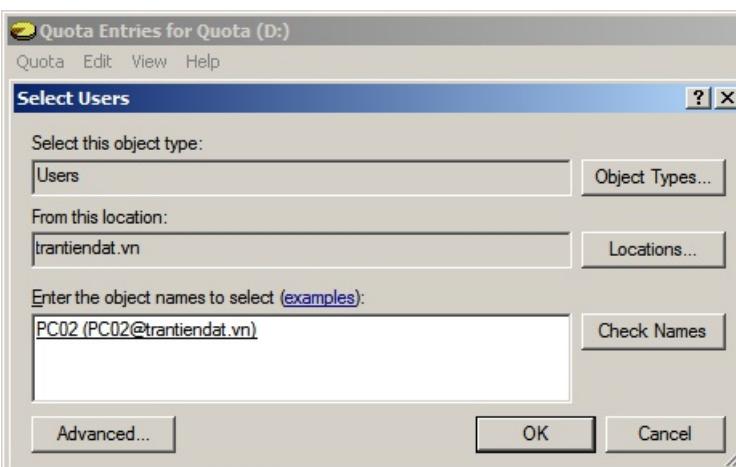
Hình 3.5.6 Quota Entries for Quota (D:)

Ta add thêm User PC02 vào, chọn Quota → New Quota Entry

Quota Entries for Quota (D:)					
Quota		Edit View Help			
New Quota Entry...					
Import...					
Export...					
Delete Quota Entry...					
Properties					
Close					
Adds a new quota entry.					

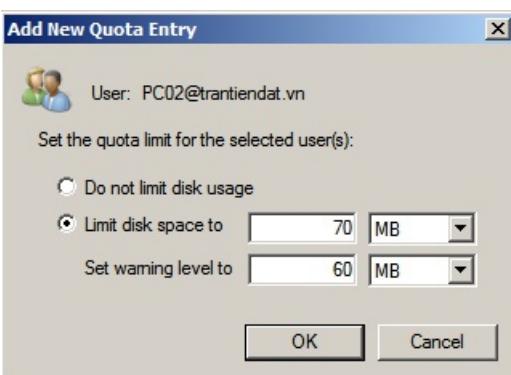
Hình 3.5.7 New Quota Entry

Nhập vào User PC02 → OK



Hình 3.5.8 Select Users

Thiết lập giới hạn Limit disk space to: 70MB, Set warning level to: 60MB → OK



Hình 3.5.9 Add New Quota Entry

Sau khi thiết lập thành công cho PC02

Quota Entries for Quota (D:)						
Quota		Edit View Help				
Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
OK	PC02	PC02@trant...	0 bytes	70 MB	60 MB	0
War...	PC01	PC01@trant...	49.27 MB	50 MB	40 MB	98
OK	BUILTIN\Admin...		71 KB	No Limit	No Limit	N/A
OK	NT AUTHORITY\SYSTEM		20 MB	No Limit	No Limit	N/A
4 total item(s), 1 selected.						

Hình 3.5.10 Thiết lập thành công

Ta tiến hành đăng nhập vào PC02. Ta thấy dung lượng ổ Quota (D:) chỉ có dung lượng là **70MB** và copy 1 file có dung lượng **>70MB** vào ta được kết quả.



Hình 3.5.11 Copy Item (PC02)

Như vậy ta đã thiết lập thành công hạn ngạch cho User **PC02**

Chương 4 Kết luận

4.1 Thuận lợi và khó khăn

Trong quá trình cài đặt và thử nghiệm do chưa thật sự hiểu rõ về cơ chế chuyển đổi từ Basic Disk sang Dynamic Disk nên khi tiến hành convert bằng máy tính thật dẫn đến lỗi. Sau khi convert thành công từ Basic sang Dynamic tiến hành restart lại windows thì không boot vào hệ điều hành được nữa. Dẫn đến việc cài lại windows. Trong quá trình cài lại windows lại gặp một số khó khăn do Dynamic Disk không thể cài hệ điều hành vào được. Do đó phải dùng Hiren boot mới khắc phục được.

Từ việc sử dụng máy tính thật không đạt được kết quả thì chúng em đã dùng máy ảo. Việc tiếp cận đài tài bằng sử dụng máy ảo tốn nhiều thời gian hơn do nhiều yếu tố khách quan khác.

Thay vào đó thì thử nghiệm các chuyển đổi và khởi tạo phân vùng từ Dynamic Disk và Basic Disk thành công khi sử dụng máy ảo.

4.2 Hướng phát triển

Từ những thành công đã đạt được chúng em đưa ra hướng phát triển cho đài tài:

- Tiến hành triển khai RAID-5 cho File Server để tăng khả năng dung lối cho Server.
- Triển khai mã hóa EFS cho các user trong Domain để mã hóa dữ liệu người dùng, dữ liệu trên File Server, nâng cao khả năng bảo mật dữ liệu.
- Triển khai Disk Quota cho các user trong Domain giới hạn dung lượng truy xuất trên file hệ thống, File Server, cũng như mức độ cho phép lưu trữ dữ liệu cho từng user.

4.3 Tổng kết

Sau khi kết thúc đài tài nhóm chúng em đã đạt được những mục tiêu cơ bản sau:

- Hiểu về những đổi mới trên windows server 2008R2 so với windows server 2008 cũng như với các phiên bản windows server trước.
- Hiểu về cơ cấu hệ thống tập tin, các loại File system.
- Hiểu về các loại đĩa lưu trữ Dynamic Disk, Basic Disk.
- Tạo và nắm bắt cơ chế hoạt động cũng như chức năng của từng loại phân vùng của các loại đĩa.
- Sử dụng công cụ Disk Manager để quản lý đĩa trên Windows Server 2008
- Mã hóa và giải mã được các tập tin thư mục bằng EFS
- Cấu hình thiết lập hạn ngạch đĩa cho các user.

Tài liệu tham khảo

<http://sinhvienit.net/forum/windows-server-2008-part-7-disk-management.25389.html>

<http://thegioitinhoc.vn/tin-hoc-can-ban/88464-phan-biet-basic-disk-va-dynamic-disk.html>

<http://tmdpc.vn/tin-cong-nghe/tim-hieu-cong-nghe-basic-disk-va-dynamic-disk/>

<https://quantrimang.com/ma-hoa-du-lieu-voi-efs-17543>

<https://technet.microsoft.com/en-us/library/cc940351.aspx>

<http://vforum.vn/diendan/showthread.php?70767-So-sanh-su-khac-biet-giua-GPT-va-MBR-khi-phan-vung-o-dia>

https://vi.wikipedia.org/wiki/N%C3%A9n_d%E1%BB%AF_l%E1%BB%87u