Câu 1:

RAID là gì ?  Phân biệt các loại RAID 0, RAID 1, RAID 5, RAID 6, RAID 01, RAID 10 ?

RAID là viết tắt của Redundant Array of Inexpensive Disks (Hệ thống đĩa dự phòng). Đây là hệ thống hoạt động bằng cách kết nối một dãy các ổ cứng có chi phí thấp lại với nhau để hình thành một thiết bị nhớ đơn có dung lượng lớn hỗ trợ hiệu quả cao và đáng tin cậy hơn so với các giải pháp trước đây. RAID được sử dụng và triển khai thành phương pháp lưu trữ trong doanh nghiệp và các máy chủ

- RAID chỉ nên làm việc với các loại ổ cứng dung lượng bằng nhau.  
- Sử dụng RAID sẽ tốn số lượng ổ nhiều hơn bình thường, nhưng đổi lại là dữ liệu sẽ an toàn hơn.  
- RAID có thể dùng cho bất kỳ hệ điều hành nào, từ **Window 98, window 2000, window XP, Window 10, window server 2016, MAC OS X, Linux...vv**

**Raid 0:**

RAID 0 sử dụng một kĩ thuật gọi là “striping”. “Striping” phân chia khối dữ liệu đơn và trải chúng qua các ổ cứng.

Tác dụng của striping là làm tăng hiệu quả thực thi. Có thể ghi được hai khối dữ liệu cùng lúc tới hai ổ cứng, hơn hẳn so với một ổ cứng như trước đây. Nếu một ổ cứng bị lỗi thì sẽ gây nguy hiểm cho dữ liệu.

Raid 1 :

Cung cấp phương pháp dự phòng dữ liệu đơn giản bằng kĩ thuật “mirroring” (nhân bản dữ liệu). Kĩ thuật này cần 2 ổ cứng riêng biệt có cùng dung lượng. Một ổ sẽ là ổ hoạt động, ổ còn lại là ổ dự phòng. Khi dữ liệu được ghi vào ổ hoạt động thì đồng thời nó cũng được ghi vào ổ dự phòng. Nếu một ổ gặp sự cố, ổ còn lại vẫn còn hoạt động. Hạn chế của kĩ thuật này là dung lượng RAID chỉ bằng dung lượng nhỏ nhất của hai ổ cứng nếu như dung lượng lưu trữ trên hai ổ được sử dụng độc lập.

Raid 5 :

 Phương pháp này sử dụng phân chia “parity” (chẵn lẻ) để duy trì dự phòng dữ liệu. Cần ít nhất 3 ổ cứng có năng xuất cao như nhau để áp dụng RAID 5.

Parity” là là một phép toán nhị phân so sánh 2 khối dữ liệu với một khối dữ liệu thứ 3 dựa trên 2 khối đầu tiên. Cách giải thích đơn giản nhất là chẵn và lẻ. Nếu tổng của 2 khối dữ liệu là chẵn thì số bit là chẵn, nếu tổng của 2 khối dữ liệu là lẻ thì số bit là lẻ. Do đó phép toán 0+0 and 1+1 đều bằng 0 còn 0+1 or 1+0 sẽ bằng 1. Dựa trên phép toán nhị phân này, một ổ trong dãy bị trục trặc thì thì sẽ cho phép các bit “parity” khôi phục lại dữ liệu khi ổ đó được thay thế.

Raid 6 :

RAID 6 phần nào giống như RAID 5 nhưng lại được sử dụng lặp lại nhiều hơn số lần sự phân tách dữ liệu để ghi vào các đĩa cứng khác nhau. Ví dụ như ở RAID 5 thì mỗi một dữ liệu được tách thành hai vị trí lưu trữ trên hai đĩa cứng khác nhau, nhưng ở RAID 6 thì mỗi dữ liệu lại được lưu trữ ở ít nhất ba vị trí (trở lên), điều này giúp cho sự an toàn của dữ liệu tăng lên so với RAID 5.  
  
RAID 6 yêu cầu tối thiểu 4 ổ cứng.  
Trong RAID 6, ta thấy rằng khả năng chịu đựng rủi ro hư hỏng cứng được tăng lên rất nhiều. Nếu với 4 ổ cứng thì chúng cho phép hư hỏng đồng thời đến 2 ổ cứng mà hệ thống vẫn làm việc bình thường, điều này tạo ra một xác xuất an toàn rất lớn. Chính do đó mà RAID 6 thường chỉ được sử dụng trong các máy chủ chứa dữ liệu cực kỳ quan trọng.

Raid 0+1:

Sự kết hợp này chỉ áp dụng với các hệ thống có ít nhất 4 ổ cứng. Các kĩ thuật “mirroring” và “striping” kết hợp với nhau tạo ra hiệu quả dự phòng. Thiết lập đầu tiên của các ổ được kích hoạt và các dữ liệu sẽ được phân chia qua đó, thiết lập thứ hai sẽ phản chiếu những dữ liệu này sang ổ thứ hai. Hiệu quả thực thi của RAID 0 được tăng lên vì ổ cứng chỉ phải mất một nửa thời gian thực hiện so với một ổ riêng lẻ mà vẫn đảm bảo sự dự phòng. Hạn chế chính của phương pháp này là giá thành bởi nó cần phải có ít nhất 4 ổ cứng.

Raid 10 :

Thay vì phân chia dữ liệu giữa các thiết lập ổ đĩa rồi phản chiếu chúng thì hai ổ cứng đầu tiên sẽ được phản chiếu với nhau. Đây là thiết lập RAID lồng. Hai cặp ổ 1 và 2, 3 và 4 sẽ phản chiếu lẫn nhau. Sau đó chúng sẽ được thiết lập thành các dãy phân chia dữ liệu. RAID 10 cần tối thiểu là 4 ổ cứng để thực hiện chức năng của mình. Tuy nhiên dữ liệu được bảo vệ bằng RAID 10 an toàn hơn RAID 0+1 rất nhiều.

Câu 2:

AD (Active Directory) là gì ? Nêu các chức năng của Active Directory? Phân biệt sự khác nhau giữa tài khoản người dùng cục bộ và tài khoản người dùng miền ?

**Active Directory** là tổ chức có thứ bậc lưu trữ và quản lý thông tin về tài nguyên trên mạng.

Chức năng : kiểm soát quyền truy cập của các user (local user, domain user)

Domain user accounts : là các tài khoản được lưu trữ trong AD, các thiết lập được áp dụng trên toàn domain. Đăng nhập từ bất kì máy tính nào vào domain cũng sẽ được áp dụng các thiết lập đó.

Local user accounts : chỉ đăng nhập trong máy không thể dùng đăng nhập vào miền.

Câu 3:

Trình bày quá trình thiết lập cấu hình  Web server [web1.ou.edu.vn](http://web1.ou.edu.vn/), [web2.ou.edu.vn](http://web2.ou.edu.vn/). Yêu  cầu : [web1.ou.edu.vn](http://web1.ou.edu.vn/) chạy port 8080, [web2.ou.edu.vn](http://web2.ou.edu.vn/) sử dụng host header name chạy port 9005 ?

cài Web Server sau đó cài FTP publishing service.

trong DNS, tạo các record web1 và web2.

Vào ổ C:/inetpub tạo thư mục Web1 và Web2 và tạo file trang chủ .htm/.html để hiện nội dung trang web.

Vào IIS Manager vừa mới cài đặt, chuột phải vào Sites chọn New website

* Site name: web1, Physical path trỏ đến thư mục Web1, port: 8080.
* Site name: web2, Physical path trỏ đến thư mục Web2, port: 9005

Tìm Windows firewall with advance security trong Start menu, click phải inbound rule chọn New rule ==> rule type: custom ==> program: all programs ==> Name: AllowAll

Ở bên IIS Manager chọn Web2 sau đó chọn bindings chọn binding có port 9005 sau đó chọn edit nhập Host name: web2.ou.edu.vn

Qua máy Client kiểm tra bằng Internet Explorer nhập http://[server\_name]:8080/ để kiểm tra web1

Câu 4:

Software Restriction policies là gì ? Cho  ví dụ triển khai minh  họa ?

Trình bày dạng triển khai phần mềm (Software Deployment) sử dụng chính sách nhóm ? Cho ví dụ minh họa ?

-Software Restriction policies: chính sách nhóm dùng để hạn chế sử dụng phần mềm.

Có hai cách để hạn chế sử dụng phần mềm là Path rule hoặc Hash Rule.

Vào Group policy management chọn OU cần được hạn chế sử dụng phần mềm chuột phải chọn Create a GPO in this domain

Chuột phải vào GPO mới tạo chọn edit ==> User configuration==> policies ==> Windows Settings ==> Security settings==>chuột phải Software restriction policies ==> New Software restriction policies ==>Additional rules ==> Tạo 1 trong 2 cái Path rule hoặc Hash rule.

* Path rule : điền đường dẫn tới file đó vào.
* Hash rule: Chọn file đó để có được mô tả về ứng dụng đó

-Các bước cài đặt Software Deployment :

Tạo GPO ==> edit ==> User configuration ==> software settings ==>software installation ==> new ==> package ==> chọn file ứng dụng==> assigned Hoặc ==> published

Assigned :Bắt buộc cài.

Published : Khuyến cáo cài nằm trong Add or Remove Programs.

Câu 5:

FTP là gì ? Trình bày thiết lập FTP site sử dụng port 5000 chỉ cho các user u1 có quyền đọc, u2  có quyền ghi ? Với  FTP site port 5001 u1,u2 đều có quyền ghi ?  
Minh họa quá trình  thiết lập FTP isolated áp dụng trong hê thống miền sử dụng Active Directory ?

FTP được dùng để đưa file lên mạng, quản lý file.

Tạo folder FTP1 và FTP 2.

**Thiết lập FTP site 1**

Mở IIS 6.0 Manager click phải FTP Sites chọn New ==> FTP Site ==> Description: FTP1 ==> TCP port: 5000==> Do not isolate user ==> Chọn folder FTP1 ==> chọn read và write ==> finish ==> chuột phải FTP site mới tạo ==> explore ==>chuột phải FTP site ==> chọn properties ==> Security accounts ==> bỏ chọn Allow anonymous connectors.

Vào folder FTP1 cấu hình NTFS như đề yêu cầu (bỏ quyền user và thêm quyền cho u1, u2 trong tab Security)

Qua client truy cập trong My Document với đường truy cập là ftp://[địa chỉ IP]:port.

**Thiết lập FTP site 2**

Chuột phải FTP Sites chọn New ==> FTP Site ==> Description: FTP2 ==> TCP port: 5001==> chọn isolate user ==> Chọn folder FTP2 ==> chọn read và write ==> finish ==> chuột phải FTP site mới tạo ==> explore ==>chuột phải FTP site ==> chọn properties ==> Security accounts ==> bỏ chọn Allow anonymous connectors.

Vào folder FTP2 cấu hình NTFS theo yêu cầu của đề(bỏ quyền user và thêm quyền cho u1, u2 trong tab Security).

Qua client truy cập trong My Document với đường truy cập là ftp://[địa chỉ IP]:port.

**Thiết lập FTP isolated using AD.**

Tạo FTP home cho từng users trong FTProot của FTP site.

Cấu hình NTFS cho từng user để có quyền thao tác trên folder của chính user đó.

Mở IIS 6.0 Manager click phải FTP Sites chọn New ==> FTP Site ==> Description: FTP1 ==> isolate user using active directory ==> Username: TEST/Administrator Password: nhập pass của admin miền Active directory domain: test.com ==> allow read và write.

Mở ADSI edit để đặt giá trị cho msIIS-FTPRoot và msIIS-FTPDir của folder của từng user.

Chuột phải vào FTP site mới tạo chọn Browse đăng nhập vào từng user để kiểm tra.

Qua client truy cập trong My Document với đường truy cập là ftp://[địa chỉ IP]:port.

Câu 6:

Trình bày các quyền NTFS permission, special permission áp dụng cho File và Folder trên Windows Server ?

|  |  |  |
| --- | --- | --- |
| Permission | Folder | File |
| Full control | Toàn quyền, thêm hoặc loại bỏ quyền truy cập khác | Toàn quyền, thêm hoặc loại bỏ quyền truy cập khác |
| Modify | Kết hợp từ Write và Read, có thể xoá và xem nội dung các tập tin con | Có thể sửa đổi các nội dung trong tập tin |
| Read And execute | Đọc và thực hiện tập tin | Đọc và thực hiện tập tin |
| List Folder Content | Xem nội dung thư mục nhưng không thực thi hay tác động gì được | Không có phân quyền này |
| Read | Đọc nội dung | Đọc nội dung |
| Write | Tạo tập tin và ghi | Tạo tập tin và ghi |

Full control: toàn quyền, giống Full control của standar permission.

Traverse folder/ execute file: Quyền thực thi file + quyền đi vào folder, ta chỉ vào được khi dùng lệnh “cd”. VD: cd C:\Data nếu ta sử dụng quyền Traverse folder/ execute cho folder Data).

List folder / Read data: Đi vào thư mục và đọc dữ liệu trên thư mục đó.

Read Attributes: đọc thuộc tính folder và file ( Read only, Hiden v.v).

Read Attributes: đọc thuộc tính mở rộng (Archive, Encrypt).

Create file/ Write data: tạo file và ghi, chỉnh sửa dữ liệu.

Create folder/ Append data:

– Cho phép tạo folder

– Ghi ghi dữ liệu vào phía cuối file ( ghi nối tiếp) , chứ không xóa, chình sửa phần dữ liệu sẵn có (chỉ áp dụng cho file).

Write Attributes: Cho phép thay đổi các thuộc tính của file, folder (read-only, hiden).

Write Extended Attributes: Cho phép chỉnh sửa các thuộc tính mở rộng của file, folder. Thuộc tính mở rộng được xác định bởi các chương trình (program), các chương trình khác nhau có các thuộc tính mờ rộng khác nhau.

Delete Subfolders and files: Xóa các folder con và các file.

Delete: Cho phép xóa tài nguyên (folder, subfolder, file).

Change permission: Cho phép thay đổi các quyền hạn đối vối file, folder.

Read permission: cho phép user, group thấy các quyền hạn mà ta đã cấu hình.

Take Ownership: Cho phép lấy quyền sở hữu file, folder của người khác.

Ngoài ra ta còn có 7 thành phần có thể liên kết với 14 bộ quyền special permission

This folder only: chỉ áp dụng quyền vào folder này ( các subfolder, file không bị áp đặt)

This folder, subfolders, files: áp lên folder, các folder con và các file trong các folder.

This folder and subfolders: áp lên folder và subfolders.

This folder and files: áp lên folder và các file ( subfolder không bị áp quyền).

Subfolder and files only: chỉ subfolder và các file bên trong mới bị áp đặt quyền.

Subfolder only: chỉ có quyền trên subfolder.

Files only: chỉ áp đặt quyền trên các file.

Câu 7:

Trình bày các thiết lập quyền cho 2 dạng Share permission, NTFS permission ?

Minh họa việc kết hợp của 2 loại permission trên và cho biết quyền nào sẽ được áp dụng ở mỗi trường hợp, giải thích ?

Các bước thực hiện NTFS: Click phải Folder/File 🡺 Chọn Properties 🡺 Chọn Security Tab 🡺 Cấu hình permissions theo yêu cầu cho user/group

Các bước thực hiện Sharing: click phải Folder 🡺 trong Folder Properties chọn Sharing 🡺Cấu hình Permission theo yêu cầu 🡺 có thể thiết lập nhiều shared folder cho cùng một folder với các permission khác nhau.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Groups | Shared Permissions | NTFS Permissions | Effective Permissions | Giải thích |
| Everyone | Full control | Read | Read | Read < Full control |
| Administrators | Full control | Full control | Full control | 2 quyền giống nhau |
| Manager | Change | Full control | Change | Change < Full control |

Theo nguyên tắc **More Restrictive** => **Effective Permissions sẽ chọn quyền thấp hơn.**

Câu 8:   
Trình bày các bước thiết lập địa chỉ IP động cho máy trạm khi kết nối vào hệ thống mạng có máy chủ DHCP ?  
  
Giải thích các thông số cấu hình mà máy client nhận được từ DHCP Server ?

DHCP Discover : xin địa chỉ IP. Client gửi gói tin này tới DHCP Relay Agent hay DHCP server trong nội bộ mạng.

DHCP Relay Agent nhận được yêu cầu sẽ gửi lên DHCP server qua unicast. DHCP server tạo gói tin DHCP offer để lưu thông tin cấu hình mà client yêu cầu.

DHCP RA lúc này broadcast ra client và Client gửi gói DHCP Request lên lại DHCP Server để xác nhận lấy địa chỉ hay không.

DHCP server nào nhận được gói này sẽ phải cấp IP cho client.

### DHCP Discover: ****DHCP Client**** là một gói được gửi đến DHCP server từ một thiết bị Client khi muốn truy cập mạng để yêu cầu thông tin địa chỉ IP.

### DHCP Offer: ****DHCP Offer**** là gói tin chứa địa chỉ IP và thông tin cấu hình TCP/IP bổ sung. Nó được DHCP server gửi về cho Client sau khi nhận được DHCP Discover.

### DHCP Request: ****DHCP Request**** là gói được DHCP client phản hồi với máy chủ sau khi nhận được DHCP Offer để thể hiện sự chấp nhận đối với địa chỉ IP.

### DHCP Acknowledge: ****DHCP Acknowledge**** là một gói được DHCP server gửi đến cho Client để xác thực việc chấp nhận DHCP Request và định hướng các tham số tùy chọn cho phép Client tham gia mạng TCP/IP và hoàn thành hệ thống khởi động.

Câu 9:  
Email server là gì ? Trình bày quá trình thiết  lập, cấu hình email server ở 2 sites [**mail.ou.org**](http://mail.ou.org/)**&**[**mail.ou.info**](http://mail.ou.info/) để người dùng ở các sites trên có  thể thực hiện việc gửi nhận email qua lại với nhau ?

Email Server là hệ thống Mail Server được thiết kế cho các tổ chức hoặc ISP xử lý khối lượng thư lớn, yêu cầu kiểm soát và linh hoạt hơn đối với các dịch vụ thư. Nó bổ sung các tính năng như hợp tác, đồng bộ hóa Outlook, quản trị từ xa, Webmail và Quản trị web nâng cao hơn và kết nối cơ sở dữ liệu, cung cấp sức mạnh và kiểm soát cần thiết cho các hoạt động quy mô lớn.

Trình bày :

Vô DNS :

Tạo 2 zone từ forward lookup zone là ou.org, ou.info

Tạo 2 record Host tên mail cho 2 zone xong tạo thêm record Mail Exchanger

Qua 2 máy Client cài MDaemon cấu hình tên miền lần lượt là ou.org, ou.info.

Tạo tài khoản tắt tính năng Strong password.

Lên IE của 2 máy Client để gửi thư qua lại.

Câu  10:  
DFS là gì ? Hãy trình bày quá trình thiết lập cấu hình hệ thống DFS. Cho ví dụ ?

**Distributed File System (DFS)** là một giải pháp cho phép người quản trị tập trung các dữ liệu nằm rời rạc trên các file server về một thư mục chung và thực hiện các tính năng replicate nhằm đảm bảo dữ liệu luôn sẵn sang khi có sự cố về file server. Bao gồm 2 tính năng : **DFS Namespace** và **DFS Replication**.

Thiết lập :

Tạo các folder Shared như yêu cầu.

Cài dịch vụ Distributed File System trong roles File service.

Namespaces ==> Thêm server DFS ==> Thêm máy chủ server\_name.

- Name: DFS

- Edit Settings:

+ Namespace server: server\_name

+ Shared folder: DFS

+ Local path of shared folder: C:\DFSRoots\DFS

+ Tích chọn User custom permissions: Customize.. chọn Everyone, chỉ cho quyền READ

Ở mục namespace vừa tạo Click New Folder để thêm các folder đã share trên các máy.

Qua client nhập đường dẫn của namespace để kiểm tra.