Nhóm gồm các thành viên:

Nguyễn Sơn Rin – 1751010122

Nguyễn Thị Cẩm Tú – 1751010178

Nguyễn Hoàng Duy Lộc – 1851010070

Nguyễn Hoàng Thuận – 1851010132

Phan Thị Thúy Hằng - 1851050042

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

*RAID (Redundant Arrays of Inexpensive Disks)* là hình thức ghép nhiều ổ đĩa cứng vật lý thành một hệ thống ổ đĩa cứng có chức gia tăng tốc độ đọc/ghi dữ liệu hoặc nhằm tăng thêm sự an toàn của dữ liệu chứa trên hệ thống đĩa hoặc kết hợp cả hai yếu tố trên.

| **Loại** | **Thông tin** | **Ưu điểm** | **Nhược điểm** | **Đối tượng** |
| --- | --- | --- | --- | --- |
| RAID 0 | Raid 0 là loại Raid khá phổ biến do có khả năng nâng cao hiệu suất tốc độ đọc ghi trao đổi dữ liệu của ổ cứng. Để tiến hành setup Raid 0 thì server cần tối thiểu 2 ổ đĩa (Disk 0, Disk 1).  Raid 0 sẽ lưu trữ như sau. Giả sử bạn có 1 file A dung lượng 100MB. Khi tiến hành lưu trữ thay vì file A sẽ được lưu vào 1 ổ cứng duy nhất, Raid 0 sẽ giúp lưu vào 2 ổ đĩa disk 0, disk 1 mỗi ổ 50MB *(Striping)* giúp giảm thời gian đọc ghi xuống 1 nửa so với lý thuyết | Tốc độ đọc ghi nhanh (gấp đôi bình thường theo lý thuyết). | Tiềm ẩn rủi ro về dữ liệu. Lý do dữ liệu được chia đôi lưu trên 2 ổ đĩa.Trường hợp 1 trong 2 ổ đĩa bị hỏng thì nguy cơ mất dữ liệu rất cao. Về ổ cứng yêu cầu phải 2 ổ cùng dung lượng, nếu 2 ổ khác dung lượng thì lấy ổ thấp nhất. | Thích hợp với những dịch vụ cần lưu trữ và truy xuất với tốc độ cao. Chẳng hạn như dịch vụ video streaming, chạy cơ sở dữ liệu... (đối với hình thức lưu trữ này Vinahost khuyến cáo khách hàng nên có hình thức sao lưu backup của mình.) |
| RAID 1 | Raid 1 là loại Raid cơ bản được sử dụng khá nhiều hiện nay do khả năng đạt an toàn về dữ liệu. để tiến hành setup Raid 1 thì cũng giống như Raid 0, server cần tối thiểu 2 ổ cứng để lưu trữ.  Không giống như Raid 0, Raid 1 đảm bảo an toàn hơn về dữ liệu do dữ liệu được ghi vào 2 ổ giống hệt nhau *(Mirroring)*. | An toàn về dữ liệu, trường hợp 1 trong 2 ổ đĩa bị hỏng thì dữ liệu vẫn có khả năng đáp ứng dịch vụ. | Hiệu suất không cao, Nâng cao chi phí (giả sử khách hàng sử dụng 2 ổ cứng 500GB. Khi sử dụng Raid 1 thì dung lượng lưu trữ có thể sử dụng chỉ được 500GB). Về ổ cứng yêu cầu phải 2 ổ cùng dung lượng, nếu 2 ổ khác dung lượng thì lấy ổ thấp nhất. | Các dịch vụ lưu trữ, các website vừa và nhỏ không yêu cầu quá cao về tốc độ đọc ghi (in/out) của ổ cứng. Các đối tượng yêu cầu sự an toàn về dữ liệu như các dịch vụ kế toán,lưu trữ thông tin khách hàng, bất động sản v.v… |
| RAID 10 | Raid 10 là sự kết hợp giữa 2 loại raid phổ biến và Raid 1 và Raid 0. Để setup Raid 10 khách hàng cần sử dụng tối thiểu 4 ổ cứng (Disk 0, Disk 1, Disk 2, Disk 3).  Đối với Raid 10 dữ liệu sẽ được lưu đồng thời vào 4 ổ cứng. 2 ổ dạng Striping (Raid 0) và 2 ổ (Mirroring) Raid 1. | Đây là 1 hình thức lưu trữ nhanh nhẹn và an toàn, vừa nâng cao hiệu suất mà lại đảm bảo dữ liệu không bị thất thoát khi 1 trong số 4 ổ cứng bị hỏng. | Chi phí cao. Đối với Raid 10 dung lượng sẵn sàng sử dụng chỉ bằng ½ dung lượng của 4 ổ. (giống như raid 1). | Raid 10 thích hợp với tất cả các đối tượng sử dụng (từ những yêu cầu về hiệu suất đến việc đảm bảo an toàn dữ liệu). Về ổ cứng yêu cầu phải 4 ổ cùng dung lượng, nếu 4 ổ khác dung lượng thì lấy ổ thấp nhất. |
| RAID 5 | Raid 5 cũng là một loại Raid được phổ biến khá rộng rãi. Nguyên tắc cơ bản của Raid 5 cũng gần giống với 2 loại raid lưu trữ truyền thống là Raid 1 và Raid 0. Tức là cũng có tách ra lưu trữ các ổ cứng riêng biệt và vẫn có phương án dự phòng khi có sự cố phát sinh đối với 1 ổ cứng bất kì trong cụm.  Để setup Raid 5 ta cần tối thiểu 3 ổ cứng. Theo như hình minh họa phương án lưu trữ của Raid 5 như sau. Giả sử có 1 file A thì khi lưu trữ sẽ tách ra 3 phần A1, A2, A3. Ba phần nãy sẽ tương ứng lưu trên ổ đĩa Disk 0, Disk 1, Disk 2, còn ổ đĩa Disk 3 sẽ giữ bản sao lưu backup của 3 phần này. Tương tự các file sau cũng vậy và tùy theo tiến trình thực hiện mà bản sao lưu có thể được lưu ở bất kì 1 trong những ổ trong cụm Raid. | Nâng cao hiệu suất, an toàn dữ liệu, tiết kiệm chi phí hơn so với hình thức lưu trữ Raid 10. | Chi phí phát sinh thêm 1 ổ so với hình thức lưu trữ thông thường. (tổng dung lượng ổ cứng sau cùng sẽ bằng tổng dung lượng đĩa sử dụng trừ đi 1 ổ. Giả sử bạn có 4 ổ 500GB thì dung lượng sử dụng sau cùng khi triển khai Raid 5 bạn chỉ còn 1500GB). | Tất cả những website, dịch vụ, ứng dụng có số lượng truy cập và yêu cầu tài nguyên từ nhỏ đến vừa và lớn. |

**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 một dịch vụ thư mục (directory service) đã ađăng ký bản quyền bởi Microsoft, nó là một phần không thể thiếu trong kiến trúc Windows. Giống như các dịch vụ thư mục khác, chẳng hạn như **Novell Directory Services (NDS)**, **Active Directory** là một hệ thống chuẩn và tập trung, dùng để tự động hóa việc quản lý mạng dữ liệu người dùng, bảo mật và các nguồn tài nguyên được phân phối, cho phép tương tác với các thư mục khác. Thêm vào đó, Active Directory được thiết kế đặc biệt cho các môi trường kết nối mạng được phân bổ theo một kiểu nào đó.

**Active Directory** có thể được coi là một điểm phát triển mới so với **Windows 2000 Server** và được nâng cao và hoàn thiện tốt hơn trong **Windows Server 2003**, trở thành một phần quan trọng của hệ điều hành. **Windows Server 2003 Active Directory** cung cấp một tham chiếu, được gọi là **directory service**, đến tất cả các đối tượng trong một mạng, gồm có **user, groups, computer, printer, policy và permission**.

**- Các tính năng:**

**Active Directory Domain Service** sử dụng bố cục tầng cấp bao gồm các domain, tree và forest kết hợp với các thành phần mạng.

**Domain** là tập hợp của một nhóm đối tượng, có thể là người dùng hoặc thiết bị, chia sẻ cùng một cơ sở dữ liệu AD. [Domain](https://bizflycloud.vn/tin-tuc/domain-la-gi-hosting-la-gi-moi-lien-he-giua-domain-va-hosting-20180625175213708.htm) có một hệ thống cấu trúc tên miền gọi là [DNS](https://bizflycloud.vn/tin-tuc/dns-server-la-gi-tac-dung-cua-dns-server-20180608161356343.htm).

**Tree** là một hoặc nhiều nhóm domain hợp lại. Cấu trúc cây sử dụng một vùng tên liền kề để thu thập một tập hợp các domain trong một hệ thống phân cấp logic. Tree có thể được xem là một mối quan hệ tin cậy khi một kết nối an toàn, hoặc đảm bảo, được chia sẻ giữa hai domain. Nhiều domain có thể cùng được trust khi một domain có thể trust domain thứ 2 và domain thứ hai có thể trust domain thứ ba. Do tính chất phân cấp của kiểu setup này, domain thứ nhất hoàn toàn có thể trust domain thứ ba mà không cần độ trust phải thực sự rõ ràng.

**Forest** là là một nhóm gồm nhiều tree. Một forest thường bao gồm các danh mục chia sẻ, lược đồ thư mục, thông tin ứng dụng và cấu hình miền. Lược đồ xác định thuộc tính và lớp của đối tượng trong một forest. Ngoài ra, các global catalog servers (máy chủ danh mục chung) sẽ cung cấp danh sách tất cả các đối tượng trong một forest.

**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?**

Server Manager/Add roles để cài Web Server sau đó chọn FTP publishing service.

Chọn tên miền trong DNS sau đó tạo các Alias web1 và web2.

Vào ổ C:/inetpub tạo thư mục web1 và web2 chứa file .htm để hiện nội dung trang web.

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

* Tạo website mới với Site name: web1, Physical path trỏ đến thư mục web1, port: 8080.
* Tạo website mới với Site name: web2, Physical path trỏ đến thư mục web2, port: 9005

Administrative tools/Windows firewall with advance security, chuột phải inbound rule chọn New rule -> rule type: custom -> program: all programs -> Name: AllowAll

Quay lại 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://[địa chỉ IP máy server]:8080/ để kiểm tra web1

Nhập <http://web2.ou.edu.vn:9005/> để kiểm tra web2.

**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 gồm 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 ->Name: DenyApplication.

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:chuột phải Additional rule chọn new Path rule -> Path:browse đến đúng file cần hạn chế sử dụng -> chọn security level đúng với yêu cầu hạn chế chọn Apply.
* -Hash rule:chuột phải Additional rule chọn new Hash rule ->Browse đến đúng file cần hạn chế sử dụng -> chọn security level đúng với yêu cầu hạn chế chọn Apply.

Software Deployment có hai dạng Assigning software: gán phần mềm cho users hoặc computers được cài đặt khi đăng nhập và Publishing software: công bố phần mềm cho users được hiển thị từ hộp thoại Add or remove programs cài đặt bởi users.

* Các bước cài đặt:

Tạo điểm phân phối: tạo shared folder chứa file cài đặt phần mềm dạng .msi

Tạo GPO -> edit -> User configuration -> software settings ->software installation -> new -> package -> nhập địa chỉ UNC của file .msi-> assigned

Hoặc -> published

**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 FTProot1 cho FTP1 và folder FTProot2 cho FTP2

**Thiết lập FTP site sử dụng port 5000 chỉ cho các user u1 có quyền đọc, u2  có quyền ghi**

Mở IIS 6.0 Manager chuột phải FTP Sites chọn New -> FTP Site -> Description: FTP1 -> TCP port: 5000-> Do not isolate user -> Browse đến folder FTProot1 -> 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 FTProot1 chọn chuột phải properties -> security -> add u1 với quyền read và u2 với quyền write.

*Vào máy client truy cập thử bằng đường dẫn: ftp://[địa chỉ IP máy server]:port/*

**Thiết lập FTP site port 5001 u1,u2 đều có quyền ghi**

Chuột phải FTP Sites chọn New -> FTP Site -> Description: FTP2 -> TCP port: 5001-> chọn isolate user -> Browse đến folder FTProot2 -> 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 FTProot2 chọn chuột phải properties -> security -> add u1 và u2 với quyền write.

*Vào máy client truy cập thử bằng đường dẫn: ftp://[địa chỉ IP máy server]:port/*

**Thiết lập FTP isolated áp dụng trong hê thống miền sử dụng Active Directory**

FTP isolated Tạo FTP home cho từng users trong FTProot của FTP site add từng user vào security của folder của chính user đó.

Mở IIS 6.0 Manager chuột 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.

Dùng ADSI 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.

*Đăng nhập vào ftp://[địa chỉ ip máy server]/ để kiểm tra bên máy client*

**Câu 6: Trình bày các quyền NTFS permission, special permission áp dụng cho File và Folder trên Windows Server?**

**Standard permission gồm 6 bộ quyền:**

**– Read:** cho phép user đọc nội dung file.

**– List folder contents:** liệt kê nội dung folder (user có thể mở folder để xem có các file, sub folder nào trong đó).

**– Read and execute:** Có thể đọc nội dung các file ( file \*.doc, ppt. xls v.v) và thực thi các file nếu file đó là chương trình (.exe, .bat v.v).

**\* Khi phân quyển user thì ta nên cho cả 3 quyền này.**

**– Write:** chỉnh sửa, tạo mới dữ liệu.

**+ Nếu user có quyền write trên file thì user có thể chỉnh sửa dữ liệu, nếu là folder thì có thể tạo mới các đối tượng trong folder, chép dữ liệu vào folder. Nhưng không thể xóa các đối tượng.**

**– Modify:** bằng các quyền ở trên gộp lại và thêm quyền delete ( đọc, chỉnh sửa, xóa các đối tượng).

**– Full control:** gồm

+ Modify

+ Quyền change permission (là quyền được cho phép thiết lập lại các bộ quyền).

+ Quyền Take Ownership

--------------------

Special Permission gồm 14 quyền:

**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, chỉnh 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, hidden).

**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 mở 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 ?**

**Thiết lập NTFS Permissions:**

Nên đặt folder permissions, hạn chế sử dụng file permissions

Nên đặt permissions cho group, hạn chế đặt cho user

Các loại NTFS Permission (câu 6)

Các bước thực hiện: • Right-click Folder/File

• Chọn Sharing and Security

• Chọn Security Tab

• Đặt permissions theo yêu cầu cho user/group (deny permission ưu tiên hơn allow permissions)

**Thiết lập Shared Permissions:**

Đặt quyền truy xuất cho folder, không đặt cho file

Kiểm soát truy xuất cho FAT volume

Các loại Shared Permissions: • Read • Change • Full Control

Các bước thực hiện: • Right-click Folder

• Trong Folder Properties chọn Sharing

• Thiết lập các Permissions theo yêu cầu

• Có thể thiết lập nhiều shared folder cho cùng một folder với các permission khác nhau

**Minh họa việc kết hợp của NTFS Permissions và Shared Permissions**

NTFS permissions dùng kết hợp với Shared Permissions theo nguyên tắc **More Restrictive** => **Effective Permissions sẽ chọn quyền thấp hơn**

| **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** |