1. **CHỦ ĐỀ: QUẢN LÝ NGƯỜI DÙNG VÀ MÁY TÍNH**
2. Windows
3. Quản lí người dùng và nhóm

- Để sử dụng được máy tính sử dụng hệ điều hành Microsoft Windows, mỗi một người dùng cần phải có tài khoản riêng còn gọi là tài khoản người dùng. Tài khoản này được sử dụng khi:

* Người dùng truy nhập vào mạng,
* Cho phép người dùng đăng nhập vào máy hay miền thư mục động.

- Tài khoản cho phép người dùng truy nhập vào máy tính cụ thể được gọi là tài khoản cục bộ (local account). Tài khoản này chỉ có giá trị đối với một máy tính duy nhất. Khi người dùng muốn sử dụng các tài nguyên trong mạng của một miền (domain) người dùng cần tài khoản miền (domain account). Tài khoản này được tạo trên máy chủ miền và được phép truy nhập vào các tài nguyên của miền. Các thông tin người dùng được lưu trong cơ sở dữ liệu miền và được sao chép tới các máy chủ miền.

- Để thuận tiện cho việc quản trị, Windows tạo sẵn một số tài khoản như quản trị (Administrator) và khách (Guest). Ngoài ra, các người dùng có vai trò và yêu cầu truy tương tự nhau có thể được xếp vào nhóm người dùng (User group). Điều này giúp cho việc quản trị được dễ dàng và thuận tiện. Tương tự như tài khoản người dùng, nhóm người dùng cũng phân biệt nhóm cục bộ và nhóm miền. Cụ thể như sau:

* Nhóm miền cục bộ (Domain local group) tương ứng với nhóm tài khoản ở bất kỳ miền nào có giá trị cục bộ.
* Nhóm toàn thể (Global group) chứa tài khoản người dùng và nhóm toàn thể khác áp dụng cho một miền cụ thể.
* Nhóm vạn năng (Universal group) áp dụng cho nhiều miền, chứa các nhóm toàn thể của các miền khác.

- Để đơn giản cho công việc quản trị Windows Server cung cấp các nhóm tạo sẵn:

* Domain Admins: dùng cho các thành viên làm nhiệm vụ quản trị.
* Domain Users: nhóm người dùng miền.
* Account Operators: thành viên nhóm có thể tạo, xóa và sửa nhóm và tài khoản người dùng.
* Backup Operators: Sao lưu và khôi phục máy chủ miền.
* Authenticated Users: người dùng hợp lệ.
* Everyone: bao gồm tất cả các người dùng.

- Để quản trị người dùng cục bộ, người dùng quản trị truy nhập “Local User and Group” của “Server manager” như trong Hình 2-6 dưới đây. “Active Directory Users and Computers” cung cấp chức năng quản lý các máy tính và người dùng trong miền. Mỗi tài khoản người dùng cần cung cấp các thông tin cơ bản sau:

* Tên người dùng: được dùng để định danh người sử dụng khi truy nhập vào mạng.
* Mật khẩu: được gán cho từng tài khoản người dùng và đảm bảo chỉ người dùng được phép mới truy nhập được vào mạng.
* Các thuộc tính của tài khoản người dùng như họ tên, số điện thoại, thư điện tử.
  1. Tạo Users và Groups với local account

\* Users:

- Tạo user mới bằng cách: vào Computer Managerment -> Local Users and Groups -> Users -> Nhập users -> Create

- Xoá user bằng cách : Users cần xóa -> Delete -> Yes

\* Groups:

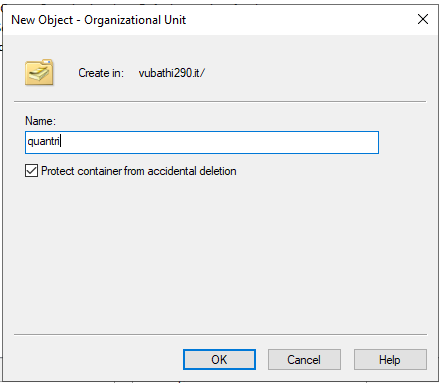
- Tạo Tạo Group mới bằng cách: Computer Managerment -> Local Users and Groups -> New Group -> Nhập group -> Create

- Add các user vào một Group: Group cần add -> Add to Group -> Add -> Nhập tên user cần add -> OK -> Apply -> Ok

|  |  |
| --- | --- |
|  |  |

* 1. Tạo Users và Groups trên Domain account (Tài khoản được tạo trên máy chủ miền và được phép truy cập vào các tài nguyên của miền)

\* Tạo Tạo OU: Active Direstory Users and Computers -> vubathi290.it, sau đó ấn chuột phải chọn New -> Organizational Unit. Để chứa Users và Groups



\* Users:

- Tại OU quantri -> chuột phải chọn New -> User -> Nhập users -> Create

- Xóa user bằng cách : Users cần xóa -> Delete -> Yes

|  |  |
| --- | --- |
|  |  |

\*Groups:

- Tạo Group mới: Tại OU quantri -> chuột phải chọn New -> Groups -> New Group -> Nhập group -> Create

- Add các user vào một Group: Group cần add -> Add to Group -> Add -> Nhập tên user cần add -> OK -> Apply -> Ok

|  |  |
| --- | --- |
|  |  |

1. Quản lý quyền truy nhập

Quản trị viên có thể cấp các quyền khác nhau cho người dùng hoặc nhóm để truy nhập và sử dụng tài nguyên trong hệ thống. Các quyền tiêu biểu gồm:

* + Toàn quyền kiểm soát (Full control) : bao gồm quyền đọc, ghi, sửa và thực thi đối tượng tài nguyên. thay đổi thuộc tính và quyền; cũng như lấy quyền sở hữu các đối tượng tài nguyên.
  + Sửa (Modify): cho phép đọc ghi sửa và thay đổi thuộc tính đối tượng tài nguyên.
  + Đọc (Read): Hiển thị dữ liệu, thuộc tính, chủ sở hữu và quyền của các đối tượng tài nguyên.
  + Ghi (Write): Ghi và thêm dữ liệu vào đối tượng tài nguyên và đọc hay thay đổi các thuộc tính tài nguyên.

Quản trị viên truy cập Local User and Group thông qua Server Manager để quản lý người dùng và nhóm trên máy tính cục bộ. Đối với quản lý người dùng và máy tính trong miền, công cụ Active Directory Users and Computers được sử dụng.

II. Linux(Ubuntu)

1. Quản lý người dùng và nhóm

Trong Linux có 3 dạng đối tượng:

* + User: tài khoản người dùng. User gồm user và super user (root). Root có quyền cao nhất trong hệ thống.
  + Group: nhóm người dùng.
  + Other: Những người dùng khác trong hệ thống.

\*Users:

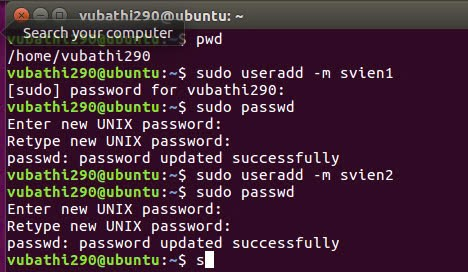
- Thông tin người dùng: Lưu trong file /etc/passwd, bao gồm tên, UID, GID, mô tả và thư mục riêng. Mật khẩu được mã hóa trong file /etc/shadow.

- Các lệnh quản lý:

* useradd: Thêm người dùng.
* userdel: Xóa người dùng.
* groupadd: Thêm nhóm

- Một số thao tác với user:

* Thêm user mới: # sudo useradd -m (tên user)
* Đặt mật khẩu cho user: # sudo passwd (tên user)
* Thêm user vào một Group: # sudo usermod -a -G (tên Group tên user)
* Thêm nhiều user vào 1 Group:# sudo gpasswd -M (tên 1, tên 2, tên Group)
* Xóa user khỏi 1 Group: # sudo gpasswd -d (tên user tên Group)
* Xóa user: # sudo userdel (tên user)

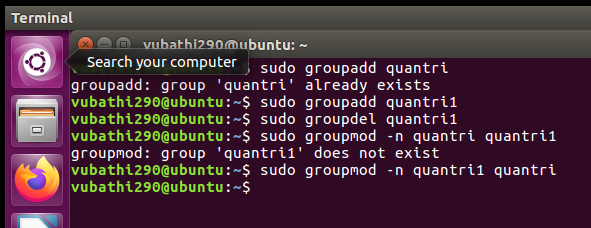


\*Groups:

- Nhóm người dùng được lưu trong file /etc/group, mỗi dòng trong file có cấu trúc như sau: Tên nhóm; Mật khẩu nhóm: tùy chọn cho phép người dùng ngoài nhóm tham gia vào; Số định danh nhóm; Các thành viên.

- Một số thao tác với groups:

* + Thêm Group mới: # sudo groupadd (tên Group)
  + Xóa Group: # sudo groupdel (tên Group)
  + Thay đổi tên Group: # sudo groupmod -n Newname Oldname



1. Quản lý quyền truy cập

- Hệ thống file của Linux/Unix cho phép cài đặt một số quyền truy nhập tới file và thư mục.

- Các quyền phổ biến được dùng đó là đọc (r), ghi (w) và thực thi (x). Ý nghĩa cụ thể của các quyền này đôi khi lệ thuộc vào đối tượng giám sát cụ thể.

- Để tăng cường tính an toàn, Linux/Unix bổ sung thêm ba kiểu đặc quyền hay nhóm đặc quyền. Đó là chủ sở hữu file, nhóm sở hữu file, và những người dùng còn lại.

Như vậy, có thể chia nhỏ hơn quyền truy nhập tới các file và thư mục chia sẻ.

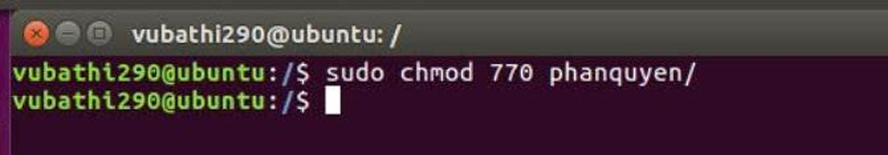
- Với một file, quyền đọc thông báo cho hệ thống biết là file đó có thể đọc được từ người dùng. Quyền ghi có nghĩa là người dùng có thể thay đổi nội dung. Và quyền thực thi cho phép người dùng chạy file đó.

- Với thư mục, quyền ghi thông báo cho hệ thống biết nội dung của thư mục có thể được liệt kê (xem); Quyền ghi tới thư mục là nội dung của thư mục đó có thể bị người dùng thay đổi; Quyền thực thi thư mục cho phép người dùng di chuyển vào bên trong thư mục đó.

- Các lệnh quản lý quyền:

* chmod: Thay đổi quyền truy nhập.
* chown: Thay đổi chủ sở hữu.

|  |  |
| --- | --- |
|  |  |



III. So sánh quản lý người dùng và máy tính trong Windows và Linux:

|  |  |  |
| --- | --- | --- |
| Tiêu chí | Điểm giống nhau | Điểm khác nhau |
| Mục tiêu | - Đều nhằm quản lý tài khoản người dùng, phân quyền truy cập và bảo mật tài nguyên hệ thống. | - **Windows**: Phù hợp với người dùng phổ thông và doanh nghiệp.  - **Linux**: Tập trung vào quản trị chuyên sâu và tính linh hoạt. |
| Cách tạo tài khoản | - Cả hai đều hỗ trợ tạo tài khoản mới với thông tin như tên người dùng, mật khẩu. | - **Windows**: Qua GUI hoặc lệnh net user.  - **Linux**: Qua lệnh adduser username hoặc GUI trong Settings. |
| Phân quyền | - Cả hai đều có thể phân quyền người dùng vào các nhóm (Group) để kiểm soát quyền hạn. | - **Windows**: Qua GUI dễ dàng hoặc sử dụng Active Directory.  - **Linux**: Qua dòng lệnh như usermod hoặc chỉnh file /etc/group. |
| Quản lý nhóm | - Đều hỗ trợ tạo, chỉnh sửa, và xóa nhóm người dùng để phân quyền. | - **Windows**: Quản lý nhóm qua GUI trong Computer Management.  - **Linux**: Quản lý chi tiết qua lệnh groupadd, groupmod, groupdel. |
| Thay đổi thông tin người dùng | - Có thể thay đổi tên, mật khẩu hoặc các thông tin liên quan đến người dùng. | - **Windows**: Thay đổi dễ dàng qua GUI.  - **Linux**: Sử dụng dòng lệnh như usermod, passwd username. |
| Xóa tài khoản | - Đều cho phép xóa tài khoản người dùng khi không còn sử dụng. | - **Windows**: Qua lệnh net user username /delete hoặc GUI.  - **Linux**: Qua lệnh deluser username. |
| Công cụ quản lý từ xa | - Đều hỗ trợ quản lý người dùng và máy tính từ xa. | - **Windows**: Qua Remote Desktop, Active Directory, PowerShell.  - **Linux**: Qua SSH, Webmin, Cockpit, hoặc công cụ tự động hóa như Ansible. |
| Quản lý máy tính | - Cả hai đều có thể theo dõi, cấu hình và bảo trì máy tính trong hệ thống. | - **Windows**: Quản lý qua GUI dễ dàng.  - **Linux**: Dùng dòng lệnh như lsblk, df hoặc công cụ quản lý như Samba, Cockpit. |
| Tính bảo mật | - Đều có cơ chế bảo mật, phân quyền truy cập tài nguyên để bảo vệ hệ thống khỏi truy cập trái phép. | - **Windows**: Tích hợp Windows Defender, BitLocker, UAC.  - **Linux**: Bảo mật mạnh mẽ với SELinux, AppArmor, và quản lý quyền sudo chi tiết. |
| Tính linh hoạt | - Cả hai đều cho phép tùy chỉnh cấu hình hệ thống để đáp ứng nhu cầu khác nhau. | - **Windows**: Ít linh hoạt, cài đặt cố định.  - **Linux**: Tùy chỉnh sâu qua các tệp cấu hình và mã nguồn mở. |
| Chi phí | - Đều yêu cầu chi phí triển khai (cả trực tiếp và gián tiếp, như đào tạo hoặc bảo trì). | - **Windows**: Có chi phí bản quyền cao.  - **Linux**: Hầu hết miễn phí và mã nguồn mở. |

**Nhận xét chung:**

* **Điểm giống nhau**: Windows và Linux đều cung cấp các chức năng quản lý cơ bản cho người dùng và máy tính, bao gồm tạo tài khoản, phân quyền, bảo mật, và quản lý tài nguyên.
* **Điểm khác nhau**: Sự khác biệt chủ yếu nằm ở cách thực hiện: **Windows** nhấn mạnh vào tính đơn giản và giao diện trực quan, trong khi **Linux** tập trung vào khả năng tùy chỉnh và linh hoạt thông qua dòng lệnh.