

Quản Lý Tài Khoản Người Dùng và Nhóm trong Linux

1. Quản Lý Người Dùng

1.1 Tạo Người Dùng Mới

```
# Tạo người dùng cơ bản
useradd username

# Tạo người dùng với các tùy chọn
useradd -m -d /home/username -s /bin/bash -c "Full Name" username

# Các tùy chọn phổ biến:
# -m: Tạo thư mục home
# -d: Chỉ định đường dẫn thư mục home
# -s: Chỉ định shell mặc định
# -c: Thêm comment (thường là tên đầy đủ)
# -u: Chỉ định UID
# -g: Chỉ định nhóm chính
# -G: Chỉ định các nhóm phụ

# Đặt mật khẩu
passwd username
```

1.2 Chỉnh Sửa Người Dùng

```
# Đổi tên người dùng
usermod -l newname oldname

# Thay đổi thư mục home
usermod -d /newhome -m username

# Thay đổi shell
usermod -s /bin/zsh username

# Khóa và mở khóa tài khoản
usermod -L username # Khóa
usermod -U username # Mở khóa

# Thêm vào nhóm
usermod -aG groupname username
```

1.3 Xóa Người Dùng

```
# Xóa người dùng
userdel username

# Xóa người dùng và thư mục home
userdel -r username

# Xóa người dùng và backup thư mục home
mv /home/username /home/username.bak
userdel username
```

2. Quản Lý Nhóm

2.1 Tạo và Xóa Nhóm

```
# Tạo nhóm mới
groupadd groupname

# Tạo nhóm với GID cụ thể
groupadd -g 1500 groupname

# Xóa nhóm
groupdel groupname
```

2.2 Quản Lý Thành Viên Nhóm

```
# Thêm người dùng vào nhóm
usermod -aG groupname username

# Xóa người dùng khỏi nhóm
gpasswd -d username groupname

# Đặt người dùng làm admin nhóm
gpasswd -A username groupname
```

3. Quản Lý Mật Khẩu và Thời Hạn

3.1 Quản Lý Mật Khẩu

```
# Đổi mật khẩu
passwd username

# Đặt quy tắc mật khẩu
chage -M 90 username # Hết hạn sau 90 ngày
chage -m 7 username  # Tối thiểu 7 ngày giữa các lần đổi
chage -W 7 username  # Cảnh báo trước 7 ngày
```

```
# Xem thông tin mật khẩu  
chage -l username
```

3.2 Quản Lý Thời Hạn Tài Khoản

```
# Đặt ngày hết hạn  
chage -E 2024-12-31 username  
  
# Bắt buộc đổi mật khẩu khi đăng nhập  
chage -d 0 username  
  
# Vô hiệu hóa hết hạn  
chage -I -1 username
```

4. Công Cụ Kiểm Tra và Giám Sát

4.1 Kiểm Tra Thông Tin

```
# Xem thông tin người dùng  
id username  
  
# Xem nhóm của người dùng  
groups username  
  
# Xem người dùng đang đăng nhập  
who  
w  
  
# Xem lịch sử đăng nhập  
last username
```

4.2 Quản Lý File Hệ Thống

```
# Kiểm tra /etc/passwd  
grep username /etc/passwd  
  
# Kiểm tra /etc/group  
grep groupname /etc/group  
  
# Sao lưu file quan trọng  
cp /etc/passwd /etc/passwd.bak  
cp /etc/shadow /etc/shadow.bak  
cp /etc/group /etc/group.bak
```

5. Ví Dụ Thực Tế

5.1 Tạo Tài Khoản Nhân Viên Mới

```
#!/bin/bash

# Tạo người dùng mới
useradd -m -s /bin/bash -c "John Doe" john
# Đặt mật khẩu
echo "john:InitialPassword123" | chpasswd
# Thêm vào nhóm
usermod -aG developers,staff john
# Bắt buộc đổi mật khẩu khi đăng nhập
chage -d 0 john
```

5.2 Vô Hiệu Hóa Tài Khoản Cũ

```
#!/bin/bash

# Khóa tài khoản
usermod -L olduser
# Sao lưu thư mục home
tar -czf /backup/olduser.tar.gz /home/olduser
# Xóa tài khoản và thư mục
userdel -r olduser
```

6. Lời Khuyên Bảo Mật

1. Mật Khẩu

- Sử dụng mật khẩu mạnh
- Thay đổi định kỳ
- Cấu hình chính sách mật khẩu

2. Quyền Truy Cập

- Tuân thủ nguyên tắc "least privilege"
- Kiểm tra quyền thường xuyên
- Ghi log các thay đổi quan trọng

3. Kiểm Soát

- Giám sát hoạt động đăng nhập
- Rà soát tài khoản định kỳ
- Backup file cấu hình quan trọng