Hướng Dẫn Sử Dụng và Quản Lý Sudo

1. Giới Thiệu về Sudo

Khái Niệm

- **Sudo** (SuperUser DO) cho phép người dùng thường thực thi lệnh với quyền của người dùng khác (thường là root)
- Tăng cường bảo mật bằng cách kiểm soát quyền truy cập root
- Ghi log tất cả các hoạt động sudo

Cách Hoạt Động

```
# Cú pháp cơ bản
sudo command

# Ví dụ
sudo apt update     # Cập nhật hệ thống
sudo -u user2 cmd   # Chạy lệnh với quyền của user2
```

2. Quản Lý Quyền Sudo

Kiểm Tra Quyền

```
# Xem quyền sudo hiện tại
sudo -l

# Kiểm tra thành viên nhóm sudo
groups username
```

Cấp Quyền Sudo

Sử dụng visudo

```
# Mở file cấu hình
sudo visudo

# Cú pháp cơ bản
username ALL=(ALL) ALL

# Cho phép không cần mật khẩu
username ALL=(ALL) NOPASSWD: ALL
```

Qua Nhóm

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

# Cấu hình cho cả nhóm
%developers ALL=(ALL) ALL
```

3. Cấu Hình Chi Tiết

Giới Hạn Lệnh

```
# Cho phép chỉ chạy lệnh cụ thể
username ALL=(ALL) /bin/systemctl restart apache2

# Cho phép nhiều lệnh
username ALL=(ALL) /sbin/reboot, /sbin/shutdown
```

Cấu Hình Nâng Cao

```
# Giới hạn theo host
username host1=(ALL) ALL

# Giới hạn theo người dùng
username ALL=(apache,nginx) ALL
```

4. Bảo Mật và Giám Sát

Theo Dõi Log

```
# Xem log sudo
grep sudo /var/log/auth.log

# Theo dõi realtime
tail -f /var/log/auth.log | grep sudo
```

Chính Sách Bảo Mật

```
# Cấu hình timeout
Defaults timestamp_timeout=15
```

```
# Giới hạn số lần thử mật khẩu
Defaults passwd_tries=3
```

5. Xử Lý Lỗi Thường Gặp

Lỗi Quyền Truy Cập

```
user is not in the sudoers file
→ Thêm user vào file sudoers hoặc nhóm sudo
```

Lỗi Mật Khẩu

```
Sorry, try again
→ Kiểm tra mật khẩu và cấu hình sudo
```

6. Ví Dụ Thực Tế

Quản Lý Dịch Vụ Web

```
# Cấu hình cho nhóm web admin
%webadmin ALL=(ALL) /bin/systemctl restart apache2, /bin/systemctl restart nginx

# File sudoers
Cmnd_Alias WEB = /bin/systemctl restart apache2, /bin/systemctl restart nginx
%webadmin ALL=(ALL) WEB
```

Quản Lý Backup

```
# Script backup với sudo
#!/bin/bash
sudo tar -czf /backup/system-$(date +%Y%m%d).tar.gz /etc
```

7. Best Practices

Nguyên Tắc Cơ Bản

1. **Tối Thiểu Hóa Quyền**
    - Chỉ cấp quyền cần thiết
    - Giới hạn theo chức năng
2. **Giám Sát**

- Kiểm tra log thường xuyên
- Cấu hình cảnh báo

3. **Cập Nhật**
   - Cập nhật sudo thường xuyên
   - Rà soát cấu hình định kỳ

Mẫu Cấu Hình An Toàn

```
# /etc/sudoers
Defaults env_reset
Defaults mail_badpass
Defaults
secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Nhóm admin
%admin ALL=(ALL) ALL

# Giới hạn lệnh cho nhóm dev
Cmnd_Alias SERVICES = /bin/systemctl restart, /bin/systemctl status
%developers ALL=(ALL) SERVICES
```

8. Câu Lệnh Hữu Ích

Quản Lý Người Dùng

```
# Thêm user vào nhóm sudo
sudo usermod -aG sudo username

# Xóa user khỏi nhóm sudo
sudo deluser username sudo

# Kiểm tra cấu hình
sudo visudo -c
```

Kiểm Tra Hệ Thống

```
# Xem người dùng sudo
getent group sudo

# Kiểm tra phiên bản sudo
sudo -V
```