Hướng dẫn kiểm tra trạng thái SSH trên Linux

Phương pháp kiểm tra

1. Kiểm tra gói SSH đã được cài đặt

Trên các hệ thống dựa trên Debian/Ubuntu:

```
dpkg -l | grep ssh
```

Trên các hệ thống dựa trên RHEL/CentOS/AlmaLinux:

```
rpm -qa | grep ssh
```

Kết quả sẽ hiển thị danh sách các gói SSH được cài đặt. Bạn cần tìm gói "openssh-server" trong kết quả.

2. Kiểm tra trạng thái dịch vụ SSH

Sử dụng systemctl để kiểm tra trạng thái:

```
systemctl status sshd
```

Hoặc:

```
service sshd status
```

Kết quả sẽ cho thấy SSH có đang chạy (active/running) hay không.

3. Kiểm tra cổng SSH

Xem có tiến trình nào đang lắng nghe trên cổng SSH (mặc định là 22):

```
netstat -tuln | grep 22
```

Hoặc sử dụng lệnh ss:

```
ss -tuln | grep 22
```

4. Kiểm tra tường lửa

Kiểm tra xem cổng SSH có được mở trong tường lửa không:

```
sudo firewall-cmd --list-all
```

Cách xử lý khi SSH chưa được cài đặt

1. Cài đặt SSH Server

Trên Debian/Ubuntu:

```
sudo apt update
sudo apt install openssh-server
```

Trên RHEL/CentOS/AlmaLinux:

```
sudo dnf install openssh-server
```

2. Khởi động dịch vụ SSH

```
sudo systemctl start sshd
sudo systemctl enable sshd
```

3. Mở cổng trong tường lửa

```
sudo firewall-cmd --permanent --add-service=ssh
sudo firewall-cmd --reload
```

Kiểm tra kết nối SSH

Sau khi cài đặt và khởi động, bạn có thể kiểm tra kết nối SSH từ máy khác:

```
ssh username@địa_chỉ_IP
```

Các lỗi thường gặp và cách khắc phục

1. **Dịch vụ không chạy**

```
sudo systemctl restart sshd
```

2. **Cổng 22 bị chặn**

```
sudo ufw allow 22
```

hoặc

```
sudo firewall-cmd --permanent --add-port=22/tcp
sudo firewall-cmd --reload
```

3. **Xem log để debug**

```
sudo tail -f /var/log/auth.log    # Trên Ubuntu
sudo tail -f /var/log/secure      # Trên RHEL/CentOS
```

Lưu ý về bảo mật

1. Luôn cập nhật SSH lên phiên bản mới nhất
2. Sử dụng xác thực key thay vì mật khẩu
3. Thay đổi cổng mặc định nếu cần
4. Giới hạn quyền truy cập SSH cho các tài khoản cụ thể
