

Trong Linux, toàn bộ log file của server được lưu trong thư mục `/var/log`.

Để di chuyển đến thư mục này bạn dùng lệnh:

```
cd /var/log/
```

Dùng `ls -l` để liệt kê hết file trong thư mục này bạn sẽ thấy một số file log chính:

**`/var/log/auth.log`**: Lưu các log về xác thực

**`/var/log/boot.log`** : Log các hoạt động trong quá trình khởi động hệ thống

**`/var/log/cron`**: Log lưu các lịch hoạt động tự động

**`/var/log/dmesg`** : Giống log message bên dưới nhưng chủ yếu là log bộ đệm

**`/var/log/message`**: Log lưu thông tin chung của hệ thống

**`/var/log/httpd/`**: Thư mục chứa log của dịch vụ Apache

**`/var/log/maillog`**: Các log hoạt động mail trên máy chủ

**`/var/log/secure`**: Log bảo mật

**`/var/log/wtmp`** : Ghi log đăng nhập

**`/var/log/yum.log`**: Các log của Yum

Nếu bạn cài thêm các phần mềm khác, sẽ có các file log với tên tương ứng ở đây.

Để xem file log chúng ta thường dùng lệnh `tail` hoặc `less`

```
more -f /var/log/secure
```

```
tail -n 30 /var/log/secure //xem 30 dòng đầu của log
```