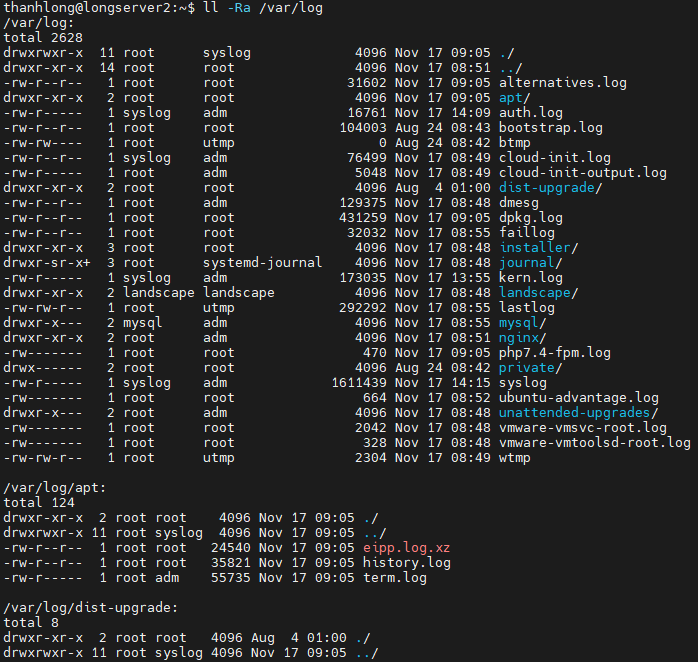
Các file log hệ thống trong linux, mysql

1. Kiểm tra các file log

* File log của hệ thống linux được lưu trong thư mục /var/log
* Muốn muốn xem hết các file hệ thống bạn có thể dùng lệnh:

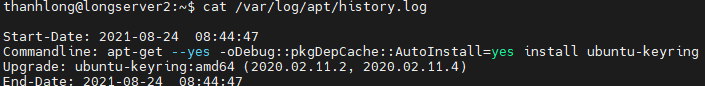
ll -Ra /var/log

để hiển thị ra các thư mục, file log và file log đệ quy của các thư mục ấy.



* Muốn xem chi tiết 1 file log bạn dùng lệnh:

cat [đường dẫn đến file log]



* + - Ngoài ra có thể sử dụng soạn thảo **vi, tail –f**.

1. Các file trong linux
   1. System logs

* Trong file log này sẽ chứa nhật ký hoạt động hệ thống (System Logs). Nó chủ yếu được sử dụng để lưu trữ các thông tin liên quan đến hệ thống. chúng ta có thể theo dõi các lỗi khởi động trừ kernel, lỗi dịch vụ liên quan đến ứng dụng và thông báo được ghi lại trong quá trình khởi động hệ thống.
* Đây là file log đầu tiên mà các quản trị viên Linux nên kiểm tra nếu có sự cố trên hệ thống.
  + - Các bản phân phối Linux thuộc họ Redhat, như CentOS hoặc RHEL được lưu trữ trong: **/var/log/message** .
    - Trong khi Ubuntu và các hệ thống dựa trên Debian khác được lưu trữ trong **/var/log/syslog** .
  1. File auth.log (secure)
* Chứa thông tin xác thực trên hệ thống trong máy chủ được ghi lại. Trong file này giúp ta các định được:
  + Các lần thử đăng nhập thất bại
  + Điều tra các cuộc tấn công và các lỗ hổng liên quan đến cơ chế ủy quyền của người dùng.
    - Trong Ubuntu, Debian : **/var/log/auth.log**
    - Trong RedHat và CentOS:  **/var/log/secure**
  1. File boot.log
* Là nơi lưu trữ tất cả thông tin liên quan đến khởi động và mọi thống báo được ghi lại trong quá trình khởi động bao gồm tập lệnh khởi tạo hệ thống. Chúng ta nên phân tích file log này để kiểm tra các vấn đề liên quan đến tắt máy không đúng cách, khởi động lại hoặc lỗi khởi động. Và cũng có thể hữu ích để xác định thời gian ngừng hoạt động của hệ thống do tắt máy đột xuất.
  + Đường dẫn: **/var/log/boot.log**
  1. File dmesg
* Tại đây các thông tin về bộ kernel được ghi nhận. Khi hệ thống khởi động các thông tin liên quan đến các thiết bị phần cứng và trình điều khiển của chúng được ghi lại ở đây. Vì kernel phát hiện các thiết bị phần cứng vật lý được liên kết trong quá trình khởi động, nó sẽ ghi lại trạng thái thiết bị, lỗi phần cứng và các thông báo chung khác
  + Đường dẫn: **/var/log/dmesg**
  1. File kern.log
* Đây là một file log vô cùng quan trọng chính là nơi chứa các thông tin được ghi bởi kernel. Thông qua file log này giúp cho chúng ta có thể khắc phục các lỗi và cảnh báo liên quan đến kernel. Kernel log có thể hữu ích trong việc khắc phục sự cố kernel và có ích trong việc gỡ lỗi các vấn đề phần cứng.
  + Đường dẫn: **/var/log/kern.log**
  1. File faillog
* Trong file này sẽ chứa các thông tin người dùng đã đăng nhập thất bại. Chúng ta có thể sử dụng lệnh faillog để hiển thị nội dung của file. Nó là file log vô cùng hữu ích để chúng ta có thể tìm ra bất kỳ vi phạm bảo mật liên quan đến việc hack username hoặc passwrod của người dùng cừng như các cuộc tấn công.
  + Đường dẫn: **/var/log/faillog**
  1. File cron
* Nơi lưu trữ tất cả các thông tin liên quan đến [Crond](https://blogd.net/linux/quan-ly-cron-tren-linux/) (công việc cron), ví dụ như khi tiến trình nền cron khởi tạo một công việc, các thông báo lỗi liên quan,... Bất cứ khi nào một công việc cron chạy, tệp nhật ký này ghi lại tất cả các thông tin liên quan bao gồm thực thi thành công và thông báo lỗi trong trường hợp thất bại.
  + Đường dẫn: **/var/log/cron**
  1. File maillog (mail.log)
* Nơi đây sẽ lưu trữ các thông tin từ máy chủ mail đang chạy trên hệ thống bao gồm các thông tin về postfix, smtpd, MailScanner, SpamAssassain hoặc bất kỳ dịch vụ liên quan đến email nào khác. TRong file log này sẽ ghi lại tất cả các email đã được gửi hoặc nhận trong một khoảng thời gian cụ thể. Thông qua file log giúp chúng ta có thể kêểm tra các vấn đề gửi thư thất bại, nhận thông tin về spam có thể bị chặn bởi máy chủ mail.
  + Đường dẫn: **/var/log/maillog** (mail.log)
  1. File httpd
* Tại đây là nơi lưu trữ của các file **error\_log** và **access\_log**của tiến trình nền httpd Apache. Các **error\_log** chứa tất cả các lỗi gặp phải httpd. Những lỗi này bao gồm các vấn đề về bộ nhớ và các lỗi liên quan đến hệ thống khác, access\_log chứa một bản ghi của tất cả các yêu cầu nhận được qua HTTP. Giúp bạn theo dõi mọi trang được phục vụ và mọi tệp được tải bởi Apache. Ghi lại địa chỉ IP và ID người dùng của tất cả các máy khách thực hiện yêu cầu kết nối đến máy chủ. Lưu trữ thông tin về trạng thái của các yêu cầu truy cập cho dù phản hồi đã được gửi thành công hay yêu cầu dẫn đến lỗi.
  + Đường dẫn: **/var/log/httpd**

1. Cài đặt và đọc file log của mysql
   1. Cài đặt

* Để bật chế độ lưu log của MySQL ta chỉnh sửa tệp cấu hình MySQL nằm trong:

/var/mysql/my.cnf