LINUX LOGS

Trình bày: Nguyễn Xuân Việt – FPT CIO

NỘI DUNG CHÍNH

01 Các distro phổ biến trong Linux

02 Các file log quan trọng trong Linux

03 Các ví dụ về log trong Linux

Các distro phổ biến trong Linux

- CentOS (*Version mới nhất cho kiến trúc x86_64 là phiên bản Centos 8.0-1905, phát hành ngày 24-09-2019*)
- Ubuntu (*Version mới nhất Ubuntu 21.10 – Impish Indri, phát hành ngày 14-10-2021)*
- RedHat (*Version mới nhất RHEL 8.4 – phát hành ngày 18-05-2021*)

LINUX LOG

- File log là 1 tập hợp các bản ghi mà hệ thống duy trì để kiểm tra các thông tin, sự kiện theo thời gian của hệ điều hành, ứng dụng phục vụ công tác điều tra khi xảy ra sự cố.
- Trên hệ thống Linux, các file log thông thường được lưu tại đường dẫn **/var/log**
- Để kiểm tra log, có thể sử dụng các công cụ sau:
  - ✓ Vi or vim
  - ✓ Tail
  - ✓ Grep
  - ✓ cat

CÁC FILE LOG QUAN TRỌNG

File log chứa nhật kí hoạt động của hệ thống, được sử dụng để lưu trữ các thông tin liên quan đến hệ thống như: mail, cron, daemon, kern, auth…

- **Centos, Redhat**: /var/log/messages
- **Ubuntu:** /var/log/syslog

CÁC FILE LOG QUAN TRỌNG

File log chứa thông tin thông tin xác thực trên hệ thống, ghi nhận các vấn đề liên quan đến cơ chế ủy quyền của người dùng. File này giúp xác định:

- Các lần thử đăng nhập thất bại
- Điều tra các cuộc tấn công và các lỗ hổng liên quan đến cơ chế ủy quyền

Các file này nằm tại:

- **Centos, Redhat:** /var/log/audit/audit.log
- **Ubuntu:** /var/log/auth.log

CÁC FILE LOG QUAN TRỌNG

Các file log quan trọng khác:

- **/var/log/secure:** Chứa các thông tin xác thực trên hệ thống. Giúp xác định thông tin đăng nhập sudo, đăng nhập SSH
- **/var/log/boot.log**: Chứa các thông tin liên quan đến quá trình khởi động của hệ thống. Giúp xác định thời gian ngừng hoạt động đột ngột của hệ thống
- **/var/log/dmesg**: Chứa các thông tin về bộ kernel của hệ thống. Giúp xác định các lỗi liên quan đến phần cứng và trình điều khiển.
- **/var/log/daemon.log**: Chứa thông tin các tiến trình nền khác nhau chạy trên hệ thống
- **/var/log/lastlog**: Chứa thông tin đăng nhập gần đây của tất cả người dùng
- **/var/log/yum.log - /var/log/dpkg.log**: Chứa các thông tin cài đặt từ gói yum hay gói dpkg trên OS Centos và Ubuntu

CÁC VÍ DỤ VỀ LOG LINUX

Đường dẫn lưu trữ log: **/var/log**

```
[                    ]# cd /var/log
[                    ]# ls
anaconda          boot.log-20191106  cron-20210815  grubby             maillog-20210829  mysqld.log       secure-20210808  spooler-20210822  vmware-install.log   vmware-network.log      yum.log-20200108
app_protect       boot.log-20200108  cron-20210822  grubby_prune_debug messages          nginx            secure-20210815  spooler-20210829  vmware-network.1.log vmware-vgauthsvc.log.0  yum.log-20210101
audit             boot.log-20200116  cron-20210829  lastlog            messages-20210808 nginx-plus-backup secure-20210822  sudo_history      vmware-network.2.log vmware-vmsvc.log        zabbix
boot.log          btmp               dmesg          maillog            messages-20210815 ntpstats         secure-20210829  tallylog          vmware-network.3.log wtmp
boot.log-20010212 btmp-20210801      dmesg.old      maillog-20210808   messages-20210822 ppp              spooler          tuned             vmware-network.4.log wtmp-20010212
boot.log-20180720 cron               eset           maillog-20210815   messages-20210829 rhsm             spooler-20210808 users_history     vmware-network.5.log yum.log
boot.log-20191105 cron-20210808      firewalld      maillog-20210822   modsec_audit.log  secure           spooler-20210815 vmware-imc        vmware-network.6.log yum.log-20191105
```

CÁC VÍ DỤ VỀ LOG LINUX

Kiểm tra việc Login: kiểm tra việc login thành công hay thất bại tại đường dẫn ***/var/log/secure.***

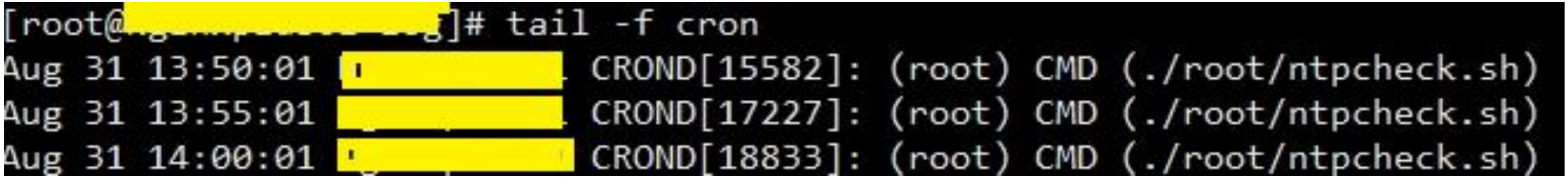
- *Ví dụ: Account dangbh với quyền root uid=0 login failed lúc 11:36:32 và thành công lúc 11:36:39 từ IP 10.0.4.51*

```
[redacted]# tail -f secure
Aug 30 14:14:33 [redacted] sudo:  dangbh : TTY=pts/0 ; PWD=/home/dangbh ; USER=root ; COMMAND=/bin/bash
Aug 30 14:14:33 [redacted] sudo: pam_unix(sudo:session): session opened for user root by dangbh(uid=0)
Aug 30 21:00:02 [redacted] sshd[10099]: pam_unix(sshd:session): session closed for user dangbh
Aug 30 21:00:02 [redacted] sudo: pam_unix(sudo:session): session closed for user root
Aug 31 11:36:30 [redacted] sshd[4641]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.0.4.51  user=dangbh
Aug 31 11:36:32 [redacted] sshd[4641]: Failed password for dangbh from 10.0.4.51 port 58922 ssh2
Aug 31 11:36:39 [redacted] sshd[4641]: Accepted password for dangbh from 10.0.4.51 port 58922 ssh2
Aug 31 11:36:39 [redacted] sshd[4641]: pam_unix(sshd:session): session opened for user dangbh by (uid=0)
Aug 31 11:36:54 [redacted] sudo:  dangbh : TTY=pts/0 ; PWD=/home/dangbh ; USER=root ; COMMAND=/bin/bash
Aug 31 11:36:54 [redacted] sudo: pam_unix(sudo:session): session opened for user root by dangbh(uid=0)
```

CÁC VÍ DỤ VỀ LOG LINUX

Kiểm tra các công việc chạy theo lịch trình: tại đường dẫn **/var/log/cron**

- *Ví dụ: Script ntpcheck.sh chạy 5 phút/lần. Đây là script để đồng bộ về mặt date/time đến ntpserver. Script này chạy với quyền root*



CÁC VÍ DỤ VỀ LOG LINUX

Kiểm tra các gói cài đặt: tại đường dẫn **/var/log/yum.log**

- Các gói được update và cài đặt vào hệ thống từ thời gian nào

```
[root@                log]# tail -f yum.log
Jun 29 17:50:36 Updated: app-protect-attack-signatures-2021.06.24-1.el7.ngx.x86_64
Jun 29 17:55:21 Updated: app-protect-threat-campaigns-2021.06.27-1.el7.ngx.x86_64
Jul 03 12:37:05 Installed: kernel-devel-3.10.0-1160.31.1.el7.x86_64
Jul 03 12:37:37 Installed: efs-8.0.375.0-1.x86_64
Jul 09 16:07:34 Updated: app-protect-attack-signatures-2021.07.01-1.el7.ngx.x86_64
Jul 09 16:13:02 Updated: app-protect-attack-signatures-2021.07.08-1.el7.ngx.x86_64
Jul 09 16:16:48 Updated: app-protect-threat-campaigns-2021.07.07-1.el7.ngx.x86_64
Aug 05 08:16:41 Updated: app-protect-attack-signatures-2021.07.29-1.el7.ngx.x86_64
Aug 05 08:17:49 Updated: app-protect-threat-campaigns-2021.08.03-1.el7.ngx.x86_64
Aug 27 08:37:12 Updated: app-protect-threat-campaigns-2021.08.23-1.el7.ngx.x86_64
```

CÁC VÍ DỤ VỀ LOG LINUX

Kiểm tra quá trình khởi động của hệ thống tại đường dẫn ***/var/log/boot.log***

- *Kiểm tra các vấn đề liên quan đến tắt máy không đúng cách, khởi động lại hoặc lỗi khởi động*
- *Xác định thời gian ngừng hoạt động của hệ thống do tắt máy đột xuất*

Thank You !