

Linux Operating System and Applications

Syslog, Crontab

Nội dung



- Dịch vụ syslogd
 - /etc/syslog.conf
 - /etc/sysconfig/syslog
 - /etc/logrotate.conf
 - /etc/logrotate.d/
- Dịch vụ crond
 - /etc/crontab

Dịch vụ Syslogd

- ☐ Người quản trị có nhu cầu thường xuyên theo dõi các sự kiện xảy ra trong hệ thống.
- ☐ Khi có sự cố, người quản trị có nhu cầu tìm lại các sự kiện xảy ra trước thời điểm đó trong hệ thống.
- ☐ Một hệ thống luôn có nhu cầu cần lưu log.
- ☐ Có thể lưu log cục bộ, hoặc lưu log tập trung.

Log

- ❑ Thư mục log mặc định: /var/log
- ❑ Xem danh sách file log: `# ls -l /var/log`

```
total 1472
-rw-----. 1 root root  4524 Nov 15 16:04 anaconda.ifcfg.log
-rw-----. 1 root root 59041 Nov 15 16:04 anaconda.log
-rw-----. 1 root root 42763 Nov 15 16:04 anaconda.program.log
-rw-----. 1 root root 299910 Nov 15 16:04 anaconda.storage.log
-rw-----. 1 root root 40669 Nov 15 16:04 anaconda.syslog
-rw-----. 1 root root 57061 Nov 15 16:04 anaconda.xlog
-rw-----. 1 root root  1829 Nov 15 16:04 anaconda.yum.log
drwxr-x---. 2 root root  4096 Nov 15 16:11 audit
-rw-r--r-- 1 root root  2252 Dec  9 10:27 boot.log
-rw----- 1 root utmp    384 Dec  9 10:31 btmp
-rw-----. 1 root utmp  1920 Nov 28 09:28 btmp-20131202
drwxr-xr-x 2 root root  4096 Nov 29 15:47 ConsoleKit
-rw----- 1 root root  2288 Dec  9 11:01 cron
-rw-----. 1 root root  8809 Dec  2 17:09 cron-20131202
-rw-r--r-- 1 root root 21510 Dec  9 10:27 dmesg
```

Một số file log thường gặp



- ☐ wtmp
- ☐ utmp
- ☐ dmesg
- ☐ messages
- ☐ maillog or mail.log
- ☐ spooler
- ☐ auth.log or secure

- ☐ Các file **wtmp** và **utmp** lưu thông tin users logging in và out vào/khỏi hệ thống. Không thể dùng lệnh “cat” để đọc các file này, phải truy xuất thông qua các lệnh đặc biệt.

Users logged in vào hệ thống

- ❑ Xác định user hiện đang logged in vào hệ thống: `# who`

```
root      tty1      2013-12-09 10:44
root      pts/0      2013-12-09 10:29 (10.0.2.2)
sysadmin  pts/1      2013-12-09 10:31 (10.0.2.2)
joeblog   pts/2      2013-12-09 10:39 (10.0.2.2)
```

- ❑ Xác định lịch sử login của một user: `# last | grep sysadmin`

```
sysadmin pts/1      10.0.2.2      Mon Dec  9 10:31  still logged in
sysadmin pts/0      10.0.2.2      Fri Nov 29 15:42 - crash (00:01)
sysadmin pts/0      10.0.2.2      Thu Nov 28 17:06 - 17:13 (00:06)
sysadmin pts/0      10.0.2.2      Thu Nov 28 16:17 - 17:05 (00:48)
sysadmin pts/0      10.0.2.2      Thu Nov 28 09:29 - crash (06:04)
sysadmin pts/0      10.0.2.2      Wed Nov 27 16:37 - down (00:29)
sysadmin tty1      Wed Nov 27 14:05 - down (00:36)
sysadmin tty1      Wed Nov 27 13:49 - 14:04 (00:15)
```

Last reboot

❏ # last reboot

```
reboot    system boot  2.6.32-358.el6.x Mon Dec  9 10:27 - 10:47  (00:19)
reboot    system boot  2.6.32-358.el6.x Fri Dec  6 16:37 - 10:47  (2+18:10)
reboot    system boot  2.6.32-358.el6.x Fri Dec  6 16:28 - 16:36  (00:08)      reboot
reboot    system boot  2.6.32-358.el6.x Mon Dec  2 17:00 - 16:36  (3+23:36)
reboot    system boot  2.6.32-358.el6.x Fri Nov 29 16:01 - 16:36  (7+00:34)
reboot    system boot  2.6.32-358.el6.x Fri Nov 29 15:43 - 16:36  (7+00:53)
...
...
wtmp begins Fri Nov 15 16:11:54 2013
```

Lần cuối các user log in vào hệ thống là khi nào?

❑ # lastlog

Username	Port	From	Latest
root	tty1		Mon Dec 9 10:44:30 +1100 2013
bin			**Never logged in**
daemon			**Never logged in**
adm			**Never logged in**
lp			**Never logged in**
sync			**Never logged in**
shutdown			**Never logged in**
halt			**Never logged in**
mail			**Never logged in**
uucp			**Never logged in**
operator			**Never logged in**
games			**Never logged in**
gopher			**Never logged in**
ftp			**Never logged in**
nobody			**Never logged in**
vcsa			**Never logged in**
saslauth			**Never logged in**

Dịch vụ Syslogd




❑ **Log** trong hệ thống được **syslog** được mô tả như sau:

- **facility**: cho biết ứng dụng nào phát sinh ra thông điệp
 - **syslog** định nghĩa các facility có sẵn: authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp
 - **syslog** dành facility từ local0 -> local7 cho người dùng định nghĩa
- **level**: mức độ nghiêm trọng của thông điệp

debug < info < notice < warn < err < crit, alert < emerg
- **action**: thông điệp sẽ được xử lí như thế nào? Lưu hay không, lưu ở đâu?

Facilities



- ☐ **auth** or **authpriv**: Messages coming from authorization and security related events
 - ☐ **kern**: Any message coming from the Linux kernel
 - ☐ **mail**: Messages generated by the mail subsystem
 - ☐ **cron**: Cron daemon related messages
 - ☐ **daemon**: Messages coming from daemons
 - ☐ **news**: Messages coming from network news subsystem
 - ☐ **lpr**: Printing related log messages
 - ☐ **user**: Log messages coming from user programs
 - ☐ **local0 to local7**: Reserved for local use
- 

Dịch vụ Syslogd

Severity Level	Keyword	Description
0	emergencies	System unusable
1	alerts	Immediate action required
2	critical	Critical condition
3	errors	Error conditions
4	warnings	Warning conditions
5	notifications	Normal but significant conditions
6	informational	Informational messages
7	debugging	Debugging messages

❑ Tập tin cấu hình: /etc/rsyslog.conf

Dịch vụ Syslogd

```
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                                /var/log/secure

# Log all the mail messages in one place.
mail.*                                                    /var/log/maillog

# Log cron stuff
cron.*                                                    /var/log/cron

# Everybody gets emergency messages
*.emerg                                                    *

# Save news errors of level crit and higher in a special file.
uucp,news,crit                                           /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                  /var/log/boot.log
```

The diagram illustrates the mapping of syslogd configuration to facility, level, and action. It features three labels at the bottom: 'facility' (in blue), 'level' (in blue), and 'action' (in blue). Red lines and brackets connect specific parts of the configuration to these labels:

- A bracket under 'local7.*' in the last line points to the 'facility' label.
- A red circle around 'crit' in the line 'uucp,news,crit' has a line pointing to the 'level' label.
- A bracket under '/var/log/boot.log' in the last line points to the 'action' label.

Dịch vụ Syslogd



- ❑ Khởi động lại dịch vụ khi thay đổi rsyslog.conf

```
# service rsyslog restart
```

- ❑ Xem những dòng mới của file log

```
# tail -f /var/log/messages
```

```
# grep string /var/log/messages | more
```

- Có khả năng lưu các log vào các máy ở xa
- 

Dịch vụ Syslogd - Logrotate

- ❑ **Logrotate**: tiện ích để quản lí các log, tránh trường hợp ghi log quá nhiều dẫn đến cạn kiệt dung lượng ổ cứng.
- ❑ Các tập tin cấu hình:
 - /etc/logrotate.conf: định nghĩa các option dùng chung cho việc quản lí log
 - /etc/logrotate.d/: cấu hình cho phép mỗi dịch vụ có thể định nghĩa cách thức quản lí log riêng phù hợp với dịch vụ đó
- Kích hoạt lại logrotate:

```
[root@bigboy tmp]# logrotate -f <configure file>
```

Dịch vụ Syslogd - Logrotate

❑ File /etc/logrotate.conf

```
# global options
# rotate log files weekly
weekly
# keep 4 weeks worth of backlogs
rotate 4
# send errors to root
errors root
# create new (empty) log files after rotating old ones
create
# compress log files
compress
# specific files
/var/log/wtmp {
    monthly
    create 0664 root utmp
    rotate 1
}
```

❑ File /etc/logrotate.d/radiusd

```
/data/radius/log/radius.log {
    rotate 10
    size=30M
}
```

Dịch vụ Syslogd - Logrotate

❑ Một số tham số thường dùng

- ✓ Compress/nocompress : nén/không nén những file log đã sử dụng
- ✓ create mode owner group: tạo file log mới có thuộc tính (mode, owner group).
- ✓ nocreate : không tạo file log mới.
mail address : khi hết chu kỳ sử dụng file log sẽ được gửi tới địa chỉ (address).
- ✓ daily : chu kỳ sử dụng file log theo ngày
- ✓ weekly : chu kỳ sử dụng file log theo tuần.
- ✓ monthly : chu kỳ sử dụng file log theo tháng.
rotate count : xác định số lần luân phiên sử dụng file log.
- ✓ size size : chu kỳ sử dụng file log được xác định theo kích thước.
- ✓ include /etc/logrotate.d : đọc thêm các thông tin cấu hình tại các file trong thư mục /etc/logrotate. Các tham số khai báo ở các file này có độ ưu tiên cao hơn các tham số khai báo trong file /etc/logrotate.conf.

Testing the Rotation

❑ # ls -l /var/log

```
total 800
...
-rw----- 1 root root    359 Dec 17 18:25 maillog
-rw-----. 1 root root   1830 Dec 16 16:35 maillog-20131216
-rw----- 1 root root  30554 Dec 17 18:25 messages
-rw-----. 1 root root 180429 Dec 16 16:35 messages-20131216
-rw----- 1 root root    591 Dec 17 18:28 secure
-rw-----. 1 root root   4187 Dec 16 16:41 secure-20131216
...
...
```

❑ # ls -l /var/log/message*


```
-rw----- 1 root root    148 Dec 17 18:34 /var/log/messages
-rw-----. 1 root root 180429 Dec 16 16:35 /var/log/messages-20131216
-rw----- 1 root root  30554 Dec 17 18:25 /var/log/messages-20131217
```

Dịch vụ Cron

- ❑ Các dịch vụ cần chạy định kì, chạy vào một thời điểm nào đó cụ thể trong ngày -> cần các thao tác lập lịch.
- ❑ Service crond là service định kì gọi thực thi các tác vụ được định nghĩa sẵn.
- ❑ Chạy trực tiếp bằng lệnh crontab.
- ❑ Chạy bằng service crond, với file cấu hình là */etc/crontab*
- ❑ Mỗi người dùng có một cron schedule riêng, file này thường nằm ở */var/spool/cron*
- ❑ Khởi động lại: *service crond restart*

Dịch vụ Cron



- ☐ Crontab -e: tạo và chỉnh sửa file crontab
 - ☐ Crontab -l: hiển thị file crontab
 - ☐ Crontab -r: xóa file crontab
- 

Dịch vụ Cron

❑ File /etc/crontab có cấu trúc như sau:

minute hour day month dayofweek [user] command



- trường nào có dấu "*": mọi lúc
- trường nào có dấu "/": mỗi lúc

Dịch vụ Cron

0 0 * * * – chạy script mỗi 0:00 AM

0 * * * * – chạy script mỗi giờ (vào phút đầu tiên của giờ)

* / 15 * * * * – chạy script mỗi 15 ph

5 8 * * * – chạy script mỗi ngày vào 8h5ph sáng

5 8 15 * * – chạy script mỗi 8h5ph sang ngày 15 hằng tháng

5 8 * * 1 – chạy script mỗi thứ hai hàng tuần, 8h5ph

30 0 1 1,6,12 * chạy script vào 0h30ph sang ngày 1 của tháng 1, tháng 6 và tháng 12.

0 20 * 10 1-5 8h tối mỗi ngày trong tuần(thứ 2 tới thứ 6) của tháng 10

0 0 1,10,15 * * nửa đêm của ngày 1, 10 và 15 hằng tháng.

5,10 0 10 * 1 vào 12h5, 12h10 mỗi thứ hai và vào ngày 10 hằng tháng

Ví dụ Crontab



- ☐ Schedule a cron to execute at 2am daily
 - `0 2 * * * /bin/sh backup.sh`
 - ☐ Schedule a cron to execute twice a day
 - `0 5,17 * * * /scripts/script.sh`
 - ☐ Schedule a cron to execute on every minutes
 - `* * * * * /scripts/script.sh`
 - ☐ Schedule a cron to execute on every Sunday at 5 PM
 - `0 17 * * * sun /scripts/script.sh`
 - ☐ Schedule a cron to execute on every 10 minutes
 - `*/10 * * * * /scripts/monitor.sh`
 - ☐ Cron that runs PHP script
 - `* * * * * root /usr/bin/php /var/www/html/project/test.php`
- 

Ví dụ Crontab (tiếp)



Q&A

