[Linux System Log]

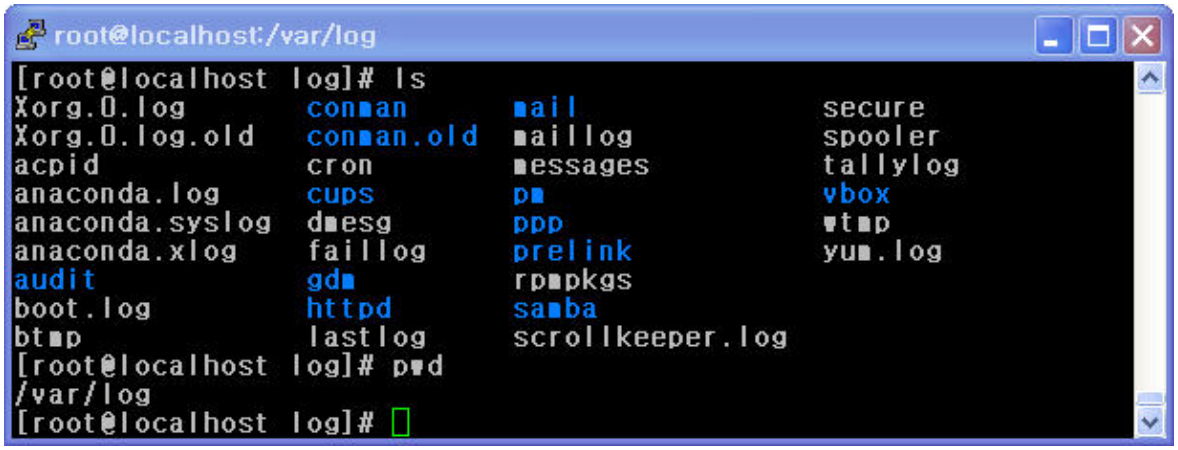
[01] 리눅스 시스템 로그

현재의 시스템에서 일어나고 있는 모든 작업이 로그파일에 기록이 된다.
그러므로 문제가 발생하였을 경우 가장 먼저 해야 할 일이 로그분석이다.
로그 파일은 시비스하고 있는 상황에 따라 하루에 몇 기가씩 쌓일 수도 있다.
이에 대해서 정확하게 분석하는 작업과 함께 주기적으로 파일을 로테이션시켜 부하를 줄여야 한다.

리눅스의 system log는 기본적으로 syslogd(/sbin/syslogd) 데몬과 그 데몬의 설정 파일인 syslog.conf(/etc/syslog.conf) 파일에 의해서 기록이 되고, cron과 logrotated에 의해서 주기적으로 로테이션 된다.
(log는 정책상 다른 서버에 저장하는게 보안상 좋다.)

[02] 로그 파일의 종류

리눅스에서 로그 파일은 일반적으로 /var/log/에 기록이 된다.
로그 파일은 운영하는 서비스에 따라서 차이가 나며 syslog.conf 설정에 따라 다르다.



- boot.log : 부팅 및 각종 서비스 시작 및 중지에 대한 기록
- cron.log : cron(작업 스케줄러링) 활동 관련 기록
- dmesg : 시스템이 부팅할 때 출력되는 메시지들이 기록된다. dmesg 명령어로 확인
- lastlog : 사용자의 마지막 로그인 시간 기록(last 명령 이용하여 확인)
- maillog : 메일과 관련된 로그를 기록한다. 이 파일을 이용하여 어떤 메일들이 오고 가는지 확인할 수 있고, 메일이 오고간 시간, 호스트, 데몬, 유저, 크기 등을 확인할 수 있다.
- messages : kernel error, reboot message, log fail 등 시스템 콘솔에서 출력된 결과를 기록하고 syslog에 의하여 생성된 메시지도 기록
- secure : log 인증 및 보안 관련 주요 로그(telnet, ssh log 기록)
- wtmp : 사용자 로그인, logout time, system 종료 시간 등 기록(last 명령 이용하여 확인)
- xferlog : FTP 서버의 데이터 전송관련 로그를 기록한다. 이 파일을 이용하면 불법파일이 전송되었는지 여부를 확인할 수 있으며, 전송 상황을 모니터링 할 수 있다.
- utmp : 현재 로그인한 사용자에 대한 상태 기록(redhat 에서는 /var/run에 있다. w,who 등을 이용하여 확인)
- history : 각 계정의 home directory에 있으며 사용자가 shell에서 작업것을 기록

[03] 로그 관련 명령어

lastlog
/var/log/lastlog 파일의 내용을 보여주는 명령어
/etc/passwd 파일에 선언되어 있는 계정중 로그인이 되는 계정만 접근한 흔적이 남아야 한다.

```
사용자명          포트      ~로부터          최근정보
root              pts/3     192.168.133.1    금 10월 10 16:49:24 +0900 2008
bin                                          **한번도 로그인한 적이 없습니다**
hsqldb                                       **한번도 로그인한 적이 없습니다**
xfs                                          **한번도 로그인한 적이 없습니다**
gdm                                          **한번도 로그인한 적이 없습니다**
doom              pts/1     192.168.133.1    금 10월 10 16:17:53 +0900 2008
```

last
특정 계정에 접근한 시간과 종료 시간에 대한 부분이 나와 있다.
/var/log/wtmp 파일을 참고하여 내용을 보여준다.

```
root     pts/0        :0.0             Fri Oct  3 15:29 - down    (00:26)
root     :0                            Fri Oct  3 15:28 - down    (00:27)
reboot   system boot  2.6.18-53.el5    Fri Oct  3 15:27           (00:28)
root     pts/0        :0.0             Fri Oct  3 15:23 - down    (00:00)
root     :0                            Fri Oct  3 15:22 - down    (00:01)
reboot   system boot  2.6.18-53.el5    Sat Oct  4 00:18           (-8:-54)
```

[TIP] # last 유저명을 하게 되면 특정 사용자의 정보를 확인할 수 있다.

lastb
접근하지 못한 계정, ip, service에 대한 정보를 보여주는 명령어이다.
무차별 대입공격을 확인 할 수 있다. /var/log/btmp 파일을 참고한다.
(기본적으로 /var/log/btmp는 존재하지 않으므로, 파일을 생성해 줘야 한다.)

w
/var/log/utmp 파일에 대한 정보를 참고하여 실시간으로 접근한 유저의 정보를 보여주는 명령어

```
[root@localhost log]# w
 18:11:44 up  3:22,  3 users,  load average: 0.05, 0.07, 0.03
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    192.168.133.1     15:41    0.00s  1.66s  0.07s w
root     pts/1    192.168.133.1     16:31    1:40m  0.22s  0.22s -bash
root     pts/2    192.168.133.1     16:49    1:22m  0.22s  0.22s -bash
```

who
w 명령어와 마찬가지로 /var/log/utmp 파일의 내용을 참고한다.

```
[root@localhost log]# who
root     pts/0        2008-10-10 15:41 (192.168.133.1)
root     pts/1        2008-10-10 16:31 (192.168.133.1)
```

```
root       pts/2          2008-10-10 16:49 (192.168.133.1)
```

[04] 로그 관리 프로그램 syslogd

syslogd는 리눅스의 시스템 로그를 기록하는 프로그램이다.
환경 설정은 /etc/syslog.conf 파일로 한다.

(01) syslogd 데몬 확인

```
[root@localhost log]# ps -ef | grep syslogd
root       1868       1   0 14:50 ?          00:00:00 syslogd -m 0
root       5034   4925   0 18:31 pts/0      00:00:00 grep syslogd
```

(02) 환경 설정 파일 /etc/syslog.conf

```
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# 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
```

위의 파일의 설정들을 자세하게 알아보자. 이 파일의 설정에는 왼쪽에 메시지를 보내는 서브 시스템의 이름을 입력하고 오른쪽에는 그 메시지를 받는 파일이나 장치등을 입력한다.

<형식>

서브시스템.메시지 종류	출력 장치

※ 서브 시스템

auth, authpriv, cron, daemon, kern, lpr, mail, news, syslog, user, uucp, local0 ~ local7

※ 메시지 종류(중요도 순서)

emerg : 시스템 패닉(시스템 충돌: 자동차가 움직일 수 없는 경우)
alert : 치명적인 에러, 즉시 알려야 하는 내용
(변조된 시스템 데이터베이스: 자동차는 가지만 일부 장비가 파손된 경우)
crit : 치명적인 에러(하드웨어 에러, critical error)
err : 에러(일반적인 에러 상태)
warn : 경고 메시지(시스템 요구 상황 에러)
notice : 알림 메시지(정상적인 상태지만 중대한 상황)
info : 정보 메시지
debug : 디버그 메시지(실행중인 프로세서의 디버깅 정보)
none : 모든 메시지를 무시한다.

# kern.*	/dev/console

모든 커널 메시지를 콘솔화면에 출력하라는 뜻이다. 기본적으로 주석으로 되어 있다.

*.info;mail.none;authpriv.none;cron.none	/var/log/messages

메일, 인증, 크론을 제외한 모든 정보들을 /var/log/messages에 기록한다.

authpriv.*	/var/log/secure

개인적인 인증에 대한 정보들을 /var/log/secure에 기록한다.

mail.*	/var/log/maillog

메일과 관련된 정보들을 /var/log/maillog에 기록한다.

cron.*	/var/log/cron

크론과 관련된 정보들을 /var/log/cron에 기록한다.

*.emerg	/*

모든 유저들이 긴급 메시지를 받을 수 있게 한다.

uucp,news.crit	/var/log/spooler

메일과 뉴스에 관한 에러들을 /var/log/spooler에 기록한다.

local7.*	/var/log/boot.log

시스템이 부팅될 때 데몬의 메시지들을 /var/log/boot.log에 기록한다.

[TIP]

본인은 위 설정을 외부 서버로 설정 “@:아이피”을 했었는데, syslog가 일정 시간에만 System

Down 되는 경우가 있었다. 원인을 알아보니 위의 설정을 잘못해서 그런경우를 알게 되었다.

[TIP]
pkill -hup PID 하면 서비스 중단 없이 재시작할 수 있다.
로그에 관해서 자주 쓰이는 명령어이므로 꼭 알아두자.

```
# pkill -hup
pkill: No matching criteria specified
Usage: pkill [-SIGNAL] [-fvx] [-n|-o] [-P PPIDLIST] [-g PGRPLIST] [-s SIDLIST]
        [-u EUIDLIST] [-U UIDLIST] [-G GIDLIST] [-t TERMLIST] [PATTERN]
```

[05] logrotate

로그파일은 특정한 파일에 지속적으로 기록이 된다. 이것은 시간이 지나면 지날수록 그 파일의 크기가 커져 시스템에서 많은 공간을 차지하며, 시스템 성능저하의 원인을 제공하기도 한다.
이런 문제점을 해결하기 위하여 logrotate를 이용하여 로그를 정기적으로 잘라서 보관하도록 한다.

※ CentOS 5.1에는 기본적으로 설치되어 있다. 확인해 보자.

```
# rpm -qa | grep logrotate
logrotate-3.7.4-7
```

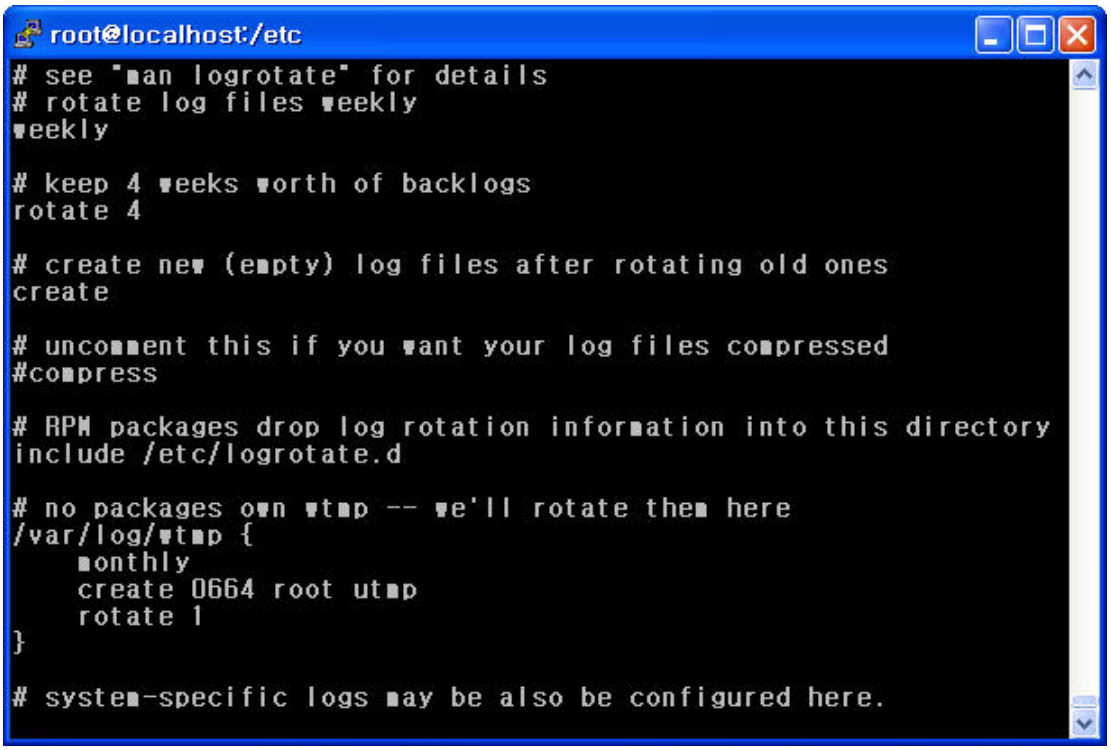
logrotate는 기본적으로 /etc/cron.daily 디렉토리에 포함되어 있어서 하루에 한번 실행된다.

```
[root@localhost /]# cd /etc/cron.daily/
[root@localhost cron.daily]# ls
0anacron    cups          makewhatis.cron  prelink   tmpwatch
0logwatch   logrotate     mlocate.cron     rpm
```

```
[root@localhost cron.daily]# ls -F /etc/cron*
/etc/cron.deny   /etc/crontab

/etc/cron.d:
sa-update

/etc/cron.daily:
0anacron*    cups*          makewhatis.cron*  prelink*   tmpwatch*
0logwatch@   logrotate*     mlocate.cron*     rpm*

/etc/cron.hourly:

/etc/cron.monthly:
0anacron*

/etc/cron.weekly:
0anacron*   makewhatis.cron*
```

환경 설정 파일인 /etc/logrotate.conf 파일을 읽어들여 로그를 관리한다.

vi /etc/logrotate.conf



<설명>

weekly

로그 파일을 변경할 기간을 정한다. 기본 설정은 주단위로 로그 파일을 변경한다.

daily : 매일 변경

weekly : 매주 변경

monthly : 매달 변경

rotate 4

순환될 파일의 개수를 지정한다. 0부터 시작하게 되며 위에서 weekly로 설정했기 때문에 4주간 유지된다.

create

로그 파일을 백업하고 새로운 파일을 생성할 것인지 설정한다.

#compress

백업할 로그를 압축하도록 변경한다. 주석을 해제하면 백업 파일을 gzip으로 압축한다.

include /etc/logrotate.d

RPM 패키지들이 로그 순환 정보를 가진 파일들이 저장된 디렉토리를 불러온다. 이 디렉토리에 있는 파일들이 모두 포함된다.

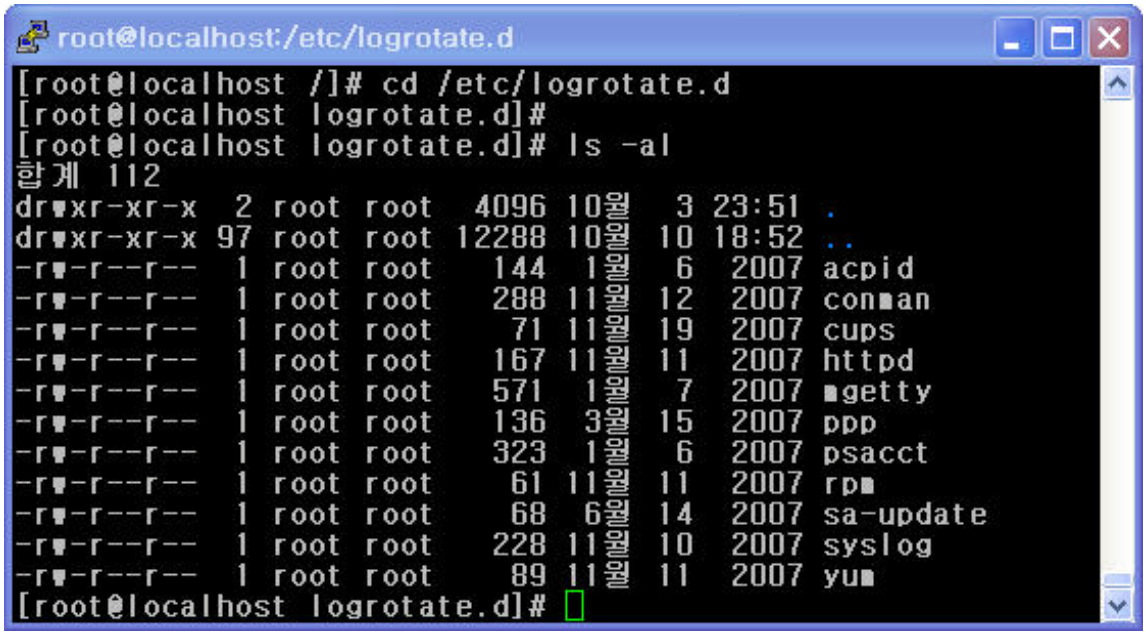
```
/var/log/wtmp {
    monthly
```

```
    create 0664 root utmp
    rotate 1
}
```

위의 설정은 wtmp에 대한 설정을 하는 것이다.
한달 단위로 순환을 하며, 백업은 한달을 보관하고, 백업 파일은 root 사용자와 utmp 그룹의 소유로 644 퍼미션을 부여한다.

[06] /etc/logrotate.d

이곳에는 데몬들의 로그 순환 설정을 담고 있는 파일들이 있다.

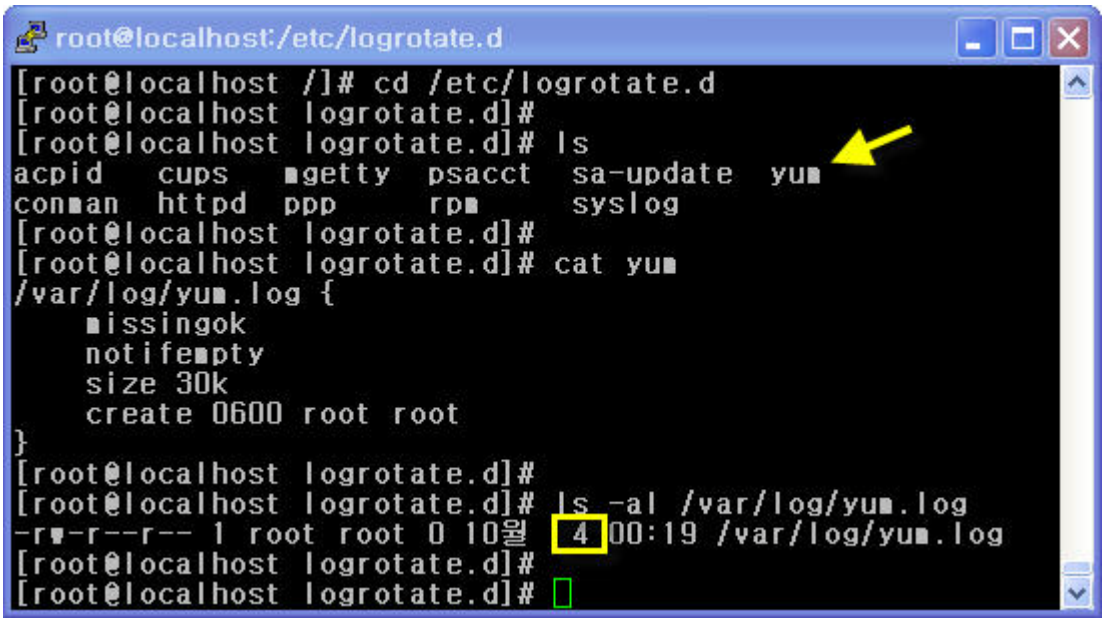


위의 파일중 yum 파일을 살펴보자.

vi /etc/logrotate.d/yum

```
[root@localhost logrotate.d]# cat yum
/var/log/yum.log {
    missingok
    notifempty
    size 30k
    create 0600 root root
}
```

- notifempty : 로그 파일이 비어있는 경우 순환을 하지 않는다.
- size 30k : 로그 파일의 크기가 30k를 넘지 않도록 한다.
- create 0600 root root : 순환되어 생성된 파일의 퍼미션을 0600으로 소유자를 root로, 그룹을 root로 지정한다.



http://cafe.naver.com/linuxlog
krintiz@naver.com