로그 관리

로그 파일

- 리눅스에서는 시스템이 운영되는 전반적인 사항을 로그파일에 기록하게 된다.
- 이 로그파일을 분석하여 시스템의 문제를 분석하고 해결할 수 있다.
- 로그 파일은 시비스하고 있는 상황에 따라 하루에 몇 기가씩 쌓일 수도 있다.
- 이에 대해서 정확하게 분석하는 작업과 함께 주기적으로 파일을 로테이션시켜 부하를 줄여야 한다.
- RHEL7 의 system log 는 기본적으로 rsyslogd 데몬과 그 데몬의 설정 파일인 /etc/rsyslog.conf 파일에 의해서 기록된다.
- /etc/rsyslog.conf 파일에는 어떤 프로그램의 로그가 어디에 기록 될지 명시되어 있다.

주요 로그 파일

- 기본적으로 로그 파일은 /var/log 라는 디렉토리에 위치한다. 물론 다른 곳에 위치하는 로그 파일들도 있다.
- 로그를 확인하려면 간단히 vi 편집기나 cat 명령어 등을 이용하여 파일의 내용을 확인하면 된다.

/var/log/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.
- 다음은 maillog 파일의 내용중 일부이다.

```
[root@localhost log]# cat maillog | more
Nov 12 20:32:28 localhost sendmail[8070]: alias database /etc/aliases r
ebuilt by root
Nov 12 20:32:28 localhost sendmail[8070]: /etc/aliases: 76 aliases, lon
gest 10 bytes, 765 bytes total
Nov 12 20:32:28 localhost sendmail[8075]: starting daemon (8.13.8): SMT
P+queueing@01:00:00
Nov 12 20:32:28 localhost sm-msp-queue[8083]: starting daemon (8.13.8):
 queueing@01:00:00
```

/var/log/messages

- 메일, 뉴스 등을 제외하고 전체적인 로그를 기록하는 파일이다.

```
[root@localhost log]# cat messages | more
Nov 12 11:16:34 localhost syslogd 1.4.1: restart.
Nov 12 11:20:07 localhost dhclient: DHCPREQUEST on eth0 to 192.168.133.
254 port 67
Nov 12 11:20:07 localhost dhclient: DHCPACK from 192.168.133.254
Nov 12 11:20:07 localhost dhclient: bound to 192.168.133.142 -- renewal
 in 866 seconds.
Nov 12 11:26:37 localhost init: Trying to re-exec init
Nov 12 11:34:33 localhost dhclient: DHCPREQUEST on eth0 to 192.168.133.
254 port 67
```

/var/log/secure

- 유저에 대한 접속을 기록한다.

```
[root@localhost log]# cat secure | more
Nov 12 12:25:22 localhost sshd[8431]: pam_unix(sshd:session): session c
losed for user root
Nov 12 12:25:25 localhost sshd[7906]: Received signal 15; terminating.
Nov 12 20:32:23 localhost sshd[7900]: Server listening on :: port 22.
Nov 12 20:32:23 localhost sshd[7900]: error: Bind to port 22 on 0.0.0.0
 failed: Address already in use.
```

/var/log/lastlog

- 계정 사용자들이 마지막으로 로그인한 정보를 기록한다.
- 기록된 사항들은 lastlog 명령어를 사용하여 확인할 수 있다.

```
[root@localhost log]# lastlog
사용자명         포트     ~로부터          최근정보
root             pts/1    192.168.133.1    금 11월 14 14:42:43 +0900 2008
bin                                        **한번도 로그인한 적이 없습니다**
daemon                                     **한번도 로그인한 적이 없습니다**
adm                                        **한번도 로그인한 적이 없습니다**
lp                                         **한번도 로그인한 적이 없습니다**
sync                                       **한번도 로그인한 적이 없습니다**
shutdown                                   **한번도 로그인한 적이 없습니다**
```

/var/log/boot.log

- 부팅시 서비스 데몬들의 실행 상태를 기록하는 파일이다.

```
[root@localhost log]# cat boot.log
Nov  9 20:33:51 localhost NET[8937]: /sbin/dhclient-script : updated
f
Nov  9 20:34:01 localhost NET[9247]: /sbin/dhclient-script : updated
f
Nov  9 20:40:24 localhost NET[9419]: /sbin/dhclient-script : updated
f
Nov  9 20:40:35 localhost NET[9729]: /sbin/dhclient-script : updated
f
```

/var/log/dmesg

- 시스템이 부팅할 때 출력되는 메시지들이 기록된다. dmesg 명령어로도 확인할 수 있다.

```
[root@localhost log]# dmesg
Linux version 2.6.18-92.el5 (mockbuild@builder16.centos.org) (gcc versi
on 4.1.2 20071124 (Red Hat 4.1.2-42)) #1 SMP Tue Jun 10 18:49:47 EDT 20
08
BIOS-provided physical RAM map:
 BIOS-e820: 0000000000000000 - 000000000009f800 (usable)
 BIOS-e820: 000000000009f800 - 00000000000a0000 (reserved)
 BIOS-e820: 00000000000dc000 - 0000000000100000 (reserved)
 BIOS-e820: 0000000000100000 - 00000000fef0000 (usable)
 BIOS-e820: 00000000fef0000 - 00000000feff000 (ACPI data)
 BIOS-e820: 00000000feff000 - 00000000ff00000 (ACPI NVS)
 BIOS-e820: 00000000ff00000 - 0000000010000000 (usable)
 BIOS-e820: 00000000fec00000 - 00000000fec10000 (reserved)
 BIOS-e820: 00000000fee00000 - 00000000fee01000 (reserved)
 BIOS-e820: 00000000fffe0000 - 0000000100000000 (reserved)
0MB HIGHMEM available.
256MB LOWMEM available.
found SMP MP-table at 000f6c90
Memory for crash kernel (0x0 to 0x0) notwithin permissible range
disabling kdump
Using x86 segment limits to approximate NX protection
On node 0 totalpages: 65536
```

/var/log/cron

- cron 과 관련된 메시지들이 저장된다.
- 이 파일을 통해 예약한 작업이 정상적으로 실행되고 있는지 확인할 수 있다.

/var/log/wtmp

- 사용자들이 접속한 정보를 기록한다.
- 바이너리 파일로 로그의 확인은 #last 명령어를 이용하여 확인할 수 있다.
- 쉘프롬프트에 last 를 입력하면 전체 접속 정보를 확인할 수 있다.

```
[root@localhost log]# last
root     pts/1        192.168.133.1    Fri Nov 14 14:42   still logged in
reboot   system boot  2.6.18-92.el5    Fri Nov 14 14:40          (00:12)
root     pts/1        192.168.133.1    Fri Nov 14 03:07 - down   (00:00)
```

- #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.)

- 만약 root 사용자명의 최근 접속 정보를 5 개만 출력하려면 아래와 같이 하면 된다.

```
# last -n 5 root
root     pts/1        192.168.133.1    Fri Nov 14 14:42   still logged in
root     pts/1        192.168.133.1    Fri Nov 14 03:07 - down   (00:00)
root     pts/1        192.168.133.1    Fri Nov 14 02:56 - down   (00:04)
root     :0                            Fri Nov 14 02:56 - down   (00:04)
root     :0                            Fri Nov 14 02:56 - 02:56  (00:00)

wtmp begins Mon Nov  3 17:00:19 2008
```

/var/log/xferlog

- FTP 서버의 데이터 전송관련 로그를 기록한다.
- 이 파일을 이용하면 불법 파일이 전송되었는지 여부를 확인할 수 있으며, 전송 상황을 모니터링 할 수 있다.

로그 관리를 위한 프로그램

로그 관리 프로그램 rsyslogd

- rsyslogd 는 리눅스의 시스템 로그를 기록하는 서비스이다.
- rsyslogd 데몬 확인

```
# ps -ef | grep rsyslogd
root          876        1  0 Mar10 ?          00:00:00 /usr/sbin/rsyslogd -nroot
```

- 환경 설정 파일 /etc/rsyslog.conf

```
#### RULES ####

# 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                                                 :omusrmsg:*

# 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
```

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 logrotate 를 이용하여 로그를 정기적으로 잘라서 보관하도록 한다.
- logrotate 는 기본적으로 /etc/cron.daily 디렉토리에 포함되어 있어서 하루에 한번 실행된다.

```
# cd /etc/cron.daily/
# ls
0anacron    cups          makewhatis.cron   prelink   tmpwatch
0logwatch   logrotate     mlocate.cron      rpm
```

- 환경 설정 파일인 /etc/logrotate.conf 파일을 읽어들여 로그를 관리한다.
- **# cat /etc/logrotate.conf**

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
        minsize 1M
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0600 root utmp
    rotate 1
}
```

```
# system-specific logs may be also be configured here.
```

- 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. 0 부터 시작하게 되며 위에서 weekly 로 설정했기 때문에 4 주간 유지된다.

- create

  로그 파일을 백업하고 새로운 파일을 생성할 것인지 설정한다.

- compress

  백업할 로그를 압축하도록 변경한다. 주석을 해제하면 백업 파일을 gzip 으로 압축한다.

- include /etc/logrotate.d

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

/etc/logrotate.d

- 데몬들의 로그 순환 설정을 담고 있는 파일들이 있다.

cat /etc/logrotate.d/yum

```
/var/log/yum.log {
    missingok
    notifempty
    size 30k
    yearly
    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.