2022-01-06

리눅스 로그 분석

201812745 김종원

A Table of Contents.

로그(Log)란?

운영 체제나 다른 소프트웨어가 실행 중에 발생하는 이벤트나 각기 다른 사용자의 통신 소프트웨어 간의 메시지를 기록한 파일

로그

로그의 유형

유형	경로	
시스템 로그	**/var/log/messages**	**시스템 전반적인 로그**
보안 로그	**/var/log/secure**	**su, ssh, 텔넷 등으로 시스템에 접속된 내용이 기록**
메일 로그	/var/log/maillog	메일로그
크론 로그	/var/log/cron	작업 스케줄링 로그
부팅 로그	/var/log/boot.log	시스템 부팅시의 로그
Dmesg 로그	/var/log/dmesg	부팅 시 기록되는 로그
Utmp 로그	**/var/log/utmp**	**현재 시스템에 로그인한 각 사용자의 상태를 출력**
Wtmp 로그	**/var/log/wtmp**	**로그인, 로그아웃, 시스템의 재부팅에 대한 정보**
Btmp 로그	**/var/log/btmp**	**실패한 로그인 시도를 기록**
Last 로그	**/var/log/lastlog**	**계정 사용자들이 마지막으로 로그인한 정보**
Su 로그	/var/log/sulog	su 명령어를 통한 로그인 시 정보 기록
Pacct 로그	/var/account/pacct	로그인한 모든 사용자의 실행한 프로그램 정보 기록
아나콘다	/var/log/anaconda	리눅스 설치 시 installer 과정에 대한 로그

로그

messages

시스템의 전반적인 로그

```
[root@localhost log]# cat -n messages
```

날짜 및 시간 컴퓨터 관련 프로그램 메시지

```
  4519  Jan  5 23:37:44 localhost systemd[8476]: Stopped target Default.
  4520  Jan  5 23:37:44 localhost systemd[8476]: Stopping Sound Service...
  4521  Jan  5 23:37:44 localhost systemd[8476]: Stopping D-Bus User Message Bus...
  4522  Jan  5 23:37:44 localhost systemd[8476]: Stopped Sound Service.
  4523  Jan  5 23:37:44 localhost systemd[8476]: Stopped D-Bus User Message Bus.
  4524  Jan  5 23:37:44 localhost systemd[8476]: Stopped target Basic System.
  4525  Jan  5 23:37:44 localhost systemd[8476]: Stopped target Paths.
  4526  Jan  5 23:37:44 localhost systemd[8476]: Stopped target Sockets.
  4527  Jan  5 23:37:44 localhost systemd[8476]: Closed D-Bus User Message Bus Socket.
  4528  Jan  5 23:37:44 localhost systemd[8476]: Closed Multimedia System.
  4529  Jan  5 23:37:44 localhost systemd[8476]: Stopped target Timers.
  4530  Jan  5 23:37:44 localhost systemd[8476]: Closed Sound System.
  4531  Jan  5 23:37:44 localhost systemd[8476]: Reached target Shutdown.
  4532  Jan  5 23:37:44 localhost systemd[8476]: Starting Exit the Session...
  4533  Jan  5 23:37:44 localhost systemd[1]: user@42.service: Killing process 9002 (systemctl) wi
th signal SIGKILL.
  4534  Jan  5 23:37:44 localhost systemd[1]: user@42.service: Succeeded.
  4535  Jan  5 23:37:44 localhost systemd[1]: Stopped User Manager for UID 42.
  4536  Jan  5 23:37:44 localhost systemd[1]: Stopping User runtime directory /run/user/42...
  4537  Jan  5 23:37:44 localhost systemd[1]: run-user-42.mount: Succeeded.
  4538  Jan  5 23:37:44 localhost systemd[1]: user-runtime-dir@42.service: Succeeded.
  4539  Jan  5 23:37:44 localhost systemd[1]: Stopped User runtime directory /run/user/42.
  4540  Jan  5 23:37:44 localhost systemd[1]: Removed slice User Slice of UID 42.
  4541  Jan  5 23:38:09 localhost journal[8648]: Service not used for 60 seconds. Shutting down..
  4542  Jan  5 23:38:09 localhost systemd[1]: geoclue.service: Succeeded.
  4543  Jan  5 23:38:10 localhost systemd[1]: realmd.service: Succeeded.
```

Part 1,

로그

secure

su, ssh, 텔넷 등으로 시스템에 접속된 내용이 기록

```
[root@localhost log]# cat secure
Jan  5 10:48:07 localhost polkitd[863]: Loading rules from directory /etc/polkit-1/rules.d
Jan  5 10:48:07 localhost polkitd[863]: Loading rules from directory /usr/share/polkit-1/rules.d
Jan  5 10:48:07 localhost polkitd[863]: Finished loading, compiling and executing 11 rules
Jan  5 10:48:07 localhost polkitd[863]: Acquired the name org.freedesktop.PolicyKit1 on the system bus
Jan  5 10:48:08 localhost sshd[1059]: Server listening on 0.0.0.0 port 22.
Jan  5 10:48:08 localhost sshd[1059]: Server listening on :: port 22.
Jan  5 10:48:48 localhost useradd[5859]: new group: name=user, GID=1000
Jan  5 10:48:48 localhost useradd[5859]: new user: name=user, UID=1000, GID=1000, home=/home/user, shell=/bin/bash
Jan  5 10:48:48 localhost chage[5872]: changed password expiry for user
Jan  5 10:48:50 localhost systemd[5921]: pam_unix(systemd-user:session): session opened for user gdm by (uid=0)
Jan  5 10:48:50 localhost gdm-launch-environment][5915]: pam_unix(gdm-launch-environment:session): session opened for user gdm
 by (uid=0)
Jan  5 10:48:53 localhost polkitd[863]: Registered Authentication Agent for unix-session:c1 (system bus name :1.79 [/usr/bin/g
nome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale ko_KR.UTF-8)
```

Part 1,

로그

utmp

현재 시스템에 로그인한 각 사용자의 상태를 출력

```
[root@localhost ~]# w
 13:57:06 up  1:58,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
user     tty4     tty4             12:03    1:58m 28.28s  0.00s /usr/libexec/gsd-disk-utility-not
```

wtmp

로그인, 로그아웃, 시스템의 재부팅에 대한 정보

```
[root@localhost ~]# last
user     tty4         tty4             Thu Jan  6 12:03   still logged in
user2    tty3         tty3             Thu Jan  6 12:02 - 12:04  (00:02)
user     tty2         tty2             Thu Jan  6 11:59 - 12:01  (00:02)
reboot   system boot  4.18.0-348.el8.x Thu Jan  6 11:58   still running
user     tty2         tty2             Thu Jan  6 00:49 - down   (11:08)
reboot   system boot  4.18.0-348.el8.x Thu Jan  6 00:48 - 11:57  (11:09)
```

btmp

실패한 로그인 시도를 기록

```
[root@localhost user]# lastb
root     pts/0                        Thu Jan  6 14:06 - 14:06  (00:00)
root     pts/0                        Thu Jan  6 14:06 - 14:06  (00:00)
root     pts/0                        Thu Jan  6 14:06 - 14:06  (00:00)
```

로그

lastlog

계정 사용자들이 마지막으로 로그인한 정보

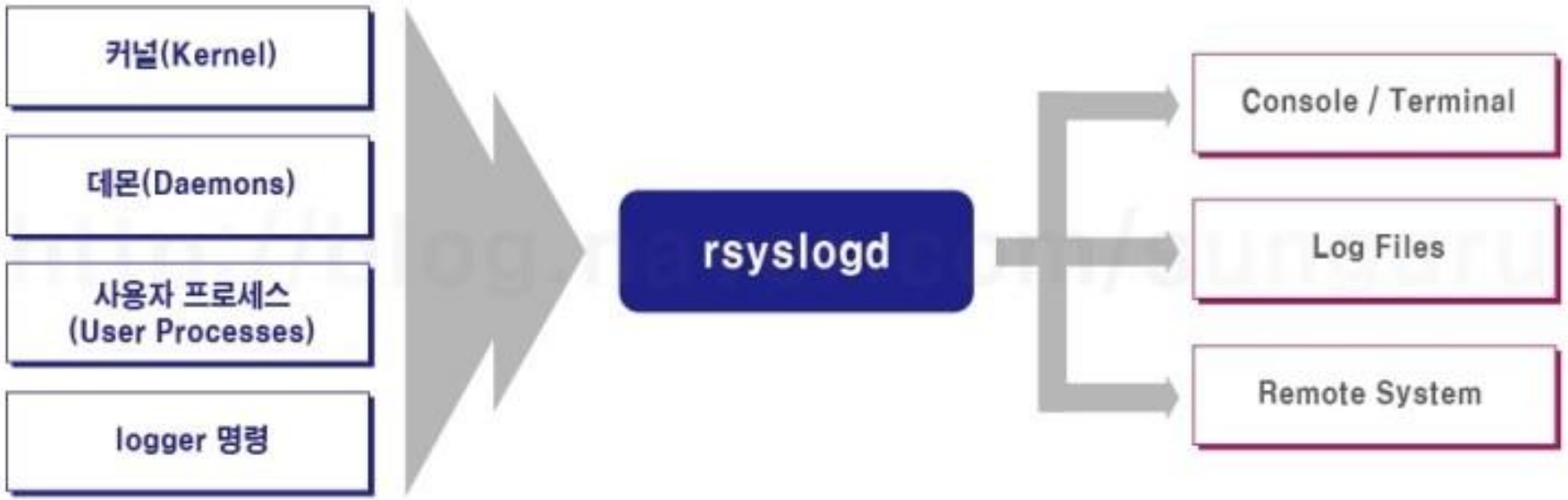
```
[root@localhost user]# lastlog
사용자이름         포트     어디서           최근정보
root             pts/0                     목  1월  6 14:06:42 +0900 2022
bin                                        **한번도 로그인한 적이 없습니다**
daemon                                     **한번도 로그인한 적이 없습니다**
adm                                        **한번도 로그인한 적이 없습니다**
lp                                         **한번도 로그인한 적이 없습니다**
sync                                       **한번도 로그인한 적이 없습니다**
shutdown                                   **한번도 로그인한 적이 없습니다**
gdm              tty1                      목  1월  6 14:02:41 +0900 2022
clevis                                     **한번도 로그인한 적이 없습니다**
gnome-initial-setup                           **한번도 로그인한 적이 없습니다
tcpdump                                    **한번도 로그인한 적이 없습니다**
sshd                                       **한번도 로그인한 적이 없습니다**
user             tty2                      목  1월  6 14:05:00 +0900 2022
user2            tty3                      목  1월  6 12:02:16 +0900 2022
```

Part 2,

로그 관리

rsyslogd

rsyslogd : 리눅스 및 유닉스에서 메시지 로깅을 지원하는 시스템 로그 데몬



Part 2,

로그 관리

Syslog의 구성

형식 : [Facility].[Level] [Action]

Facility

kern : 커널이 발생한 메시지
user : 사용자 프로세스
mail : mail 시스템 관련 서비스
daemon : telnetd, ftpd, httpd과 관련된 서비스
auth : 로그인과 같은 인증 관련 서비스
syslog : syslog 관련 서비스
cron : 예약작업 관련 서비스, crond, atd
* : 모든 서비스를 의미

Level

emerge : 일반적으로 모든 사용자에게 전달되는 패닉 상황(블루스크린, 커널 패닉)
alert : 시스템 DB에 손상 등 즉시 수정해야 되는 상황
crit : 하드웨어 장치 오류 등 중대한 상황에 대한 경고
err : 하드웨어 장치 이외의 오류
warning : 경고 메시지, 무시해도 됨
notice : 특별한 처리가 필요할 수 있는 비오류 상황
info : 정보 메시지
debug : 프로그램 개발 또는 테스트 할 때 사용
none : 로그로 기록 X

Action

File : 지정한 파일에 로그 기록
@host : 지정한 호스트로 메시지 전달
User : 지정한 사용자가 로그인 한 경우, 해당 사용자의 터미널로 전달
* : 현재 로그인 되어 있는 모든 사용자의 화면으로 전달
콘솔 또는 터미널 : 지정한 터미널로 메시지 전달

Part 2,

로그 관리

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
```

Part 2,

로그 관리

logrotate

logrotate : 누적된 로그로 인해 파일시스템이 가득차는 것을 방지하기 위해 존재

Part 2,

로그 관리

중요성

- **침해 사고 발생 시 사고의 근원을 명확하게 규명**

언제, 어떻게, 어디서 접속이 시도되었고, 어떤 명령이 수행되었는지 모두 로그에 남아 있기 때문에 침입자가 침입 흔적을 지우지 못하도록 로그 파일의 무결성 관리가 중요.

-> 별도의 로그 관리 시스템으로 무결성 강화

- **침해 시도를 조기에 탐지하여 사고를 예방**

사후 대응이 아닌 실시간 탐지로 사전 예방에 하는 방향으로, 접속 로그, 명령어 로그를 실시간으로 로그분석 시스템을 전송.

Part 3,

로그 분석 사례

개요

/etc/passwd 파일 삭제로 인한 서버 접속 장애에 대한 분석

장애 발생 일자

2016년 7월 28일 목요일

장애 내용

/etc/passwd 파일 삭제로 인하여 부팅 후 로그인 및 원격접속 시 접속 불가

점검 항목

Last	로그인 내역 확인
/var/log/secure	접속권한부여와 관련된 내용의 로그 확인
/home/user/.bash_history	해당 유저의 명령어 입력 히스토리
/root/.bash_history	root 명령어 입력 히스토리

Part 3,

로그 분석 사례

점검 내용

/var/log/messages

```
jul 28 16:52:33 linux200 xinetd(4321) : START : telnet pid=4991 from=172;16.6.11
jul 28 16:53:50 linux200 xinetd(4321) : EXIT : telnet status=1 pid=4991 duration=77(sec)
```

/var/log/secure

```
Jul 28 16:52:53 linux200 su pam unix(su-l :session): ssesion  opend for user root by user01(uid=500)
```

Part 3,

로그 분석 사례

점검 내용

/var/log/wtmp

last | head -10 명령어로 접속기록 확인 결과 IP:182.168.6.11 사용자 16시 52분~16시 53분 user01로 접속을 한 흔적 발생

/root/.bash_history

.bash_histor를 이용하여 53분에 사용된 명령어 검색 결과, /etc/passwd파일을 삭제하고 접속을 종료한 것을 확인.

분석 결과

-> **16시 52분 33초에 IP:172.16.6.11 사용자가 텔넷을 이용하여 user01로 접속 후 “su” 명령어를 통해 root로 로그인하여, /etc/passwd 파일을 삭제하고 빠져나갔음.**