로그 관리

로그(log)

- 시스템 운영 중에 발생하는 이벤트를 기록한 파일

  - 운영체제 또는 소프트웨어마다 로그 파일의 형식이 다름

- 컴퓨터 또는 프로그램의 사용 기록
- Logging(로깅) : 로그를 기록하는 행위
- 리눅스(유닉스) 시스템은 로그의 분산 관리
- 리눅스의 로그 파일은 기본적으로 /var/log 디렉터리에 존재

리눅스 로그 종류

❶ 텍스트 기반 로그

로그종류	로그 파일 위치	설명
시스템 로그	/var/log/messages	시스템에서 발생하는 전반적인 로그 기록
인증로그	/var/log/secure	인증 시스템(PAM 등)이 발생시키는 로그
메일로그	/var/log/mailog	메일 로그
부팅로그	/var/log/boot.log	시스템 부팅 시의 로그
크론로그	/var/log/cron	작업 스케쥴링 로그

❷ 텍스트 기반 로그(애플리케이션 로그)

로그종류	로그 파일 위치	설명
Apache 웹 서버	/var/log/httpd	아파치 웹 서버가 발생시킨 로그
Samba 서버	/var/log/samba	삼바 서버가 발생시킨 로그
SMTP 서버	/var/log/maillog	Sendmail이나 Postfix 같은 메일 서버가 발생시킴
FTP 서버	/var/log/xferlog	VSFTP나 Proftp 서버가 발생시킨 로그

❸ 바이너리 로그

로그파일	설명	로그 확인 명령어
/var/run/utmp	사용자의 현재 로그인 정보를 기록	who , w, user, finger
/var/log/wtmp	성공한 로그인과 로그아웃, 시스템 재부팅 정보	last
/var/log/btmp	사용자의 로그인 실패를 기록	lastb
/var/log/lastlog	가장 최근 로그인 정보를 기록	lastlog
/usr/account/pacct	시스템에 로그인한 사용자가 수행한 프로그램 정보 기록 로그인해서 로그오프 할 때까지 입력 정보 등을 기록 시스템 자원을 많이 소모하므로 기본적으로 동작 안함	acctcom lastcomm

로그 관련 주요 파일

❶ /var/log/messages

- 시스템에서 발생하는 표준 메시지가 기록되는 파일
- 대부분의 로그가 이 파일에 쌓이고, root만이 읽을 수 있도록 설정
- 이 로그는 날짜 및 시간, 메시지가 발생한 호스트명, 메시지를 발생한 내부 시스템이나 응용프로그램의 이름, 발생된 메시지(:으로 구분) 순으로 기록

#cat /var/log/messages

```
Mar 24 08:12:17 localhost org.gnome.Shell.desktop[2372]: Window manager warning: W13 (root@local)
Mar 24 08:16:17 localhost org.gnome.Shell.desktop[2372]: Window manager warning: last_user_time (1
nding inaccurate timestamps in messages such as _NET_ACTIVE_WINDOW.  Trying to work around...
Mar 24 08:16:17 localhost org.gnome.Shell.desktop[2372]: Window manager warning: W13 (root@local)
Mar 24 08:16:48 localhost org.gnome.Shell.desktop[2372]: Window manager warning: last_user_time (1
nding inaccurate timestamps in messages such as _NET_ACTIVE_WINDOW.  Trying to work around...
Mar 24 08:16:48 localhost org.gnome.Shell.desktop[2372]: Window manager warning: W13 (root@local)
```

a) 시간　　b) 컴퓨터명　　c) 프로세스　　d) 설명

❷ /var/log/wtmp

- 사용자의 로그인과 로그아웃 정보를 가지고 있는 로그 파일

  - 사용자 로그인, 로그아웃, 시스템 종료(shutdown), 부팅(booting), 재부팅(reboot) 정보

  - 콘솔, telnet, ftp 등 통한 로그인 정보

- 파일 위치 : /var/log (텍스트가 아닌 바이너리 형태로 로그가 저장됨)

- 로그 출력 명령어 : **last**

```
[root@localhost ~]# last
gildong  pts/0        :0               Mon Oct  2 09:
gildong  pts/1        :0               Mon Oct  2 08:39   still logged in
gildong  pts/0        :0               Sun Oct  1 14:21 - 09:17  (18:55)
gildong  :0           :0               Sun Oct  1 14:21   still logged in
(unknown :0           :0               Sun Oct  1 14:19 - 14:21  (00:01)
user02   :0           :0               Sun Oct  1 14:19 - 14:19  (00:00)
(unknown :0           :0               Sun Oct  1 14:19 - 14:19  (00:00)
gildong  pts/0        :0               Sun Oct  1 13:39 - 14:19  (00:39)
gildong  :0           :0               Sun Oct  1 13:37 - 14:19  (00:41)
(unknown :0           :0               Sun Oct  1 13:37 - 13:37  (00:00)
reboot   system boot  3.10.0-123.el7.x Sun Oct  1 13:37 - 15:05 (1+01:28)
gildong  pts/2        :0               Sun Oct  1 10:01 - crash  (03:36)
gildong  pts/1        :0               Sun Oct  1 10:01 - crash  (03:36)
gildong  pts/0        :0               Sun Oct  1 09:57 - crash  (03:40)
gildong  pts/0        :0               Sun Oct  1 08:45 - 09:53  (01:08)
gildong  :0           :0               Sun Oct  1 08:44 - crash  (04:52)
```

* last 계정명 ⟶ 계정명의 로그정보
* last console ⟶ 콘솔로 로그인한 사용자 확인
* last reboot | more ⟶ 재부팅 시간 정보 확인

$ last → /var/log/wtmp가 만들어진 후 관련 정보를 출력

$ last gildong → gildong 사용자의 로그인 정보를 출력

$ last reboot → 시스템이 재부팅된 정보를 출력

$ last -1 reboot → 가장 최근에 재부팅한 정보 하나만 출력

$ last -f /var/log/wtmp.1 → /var/log/wtmp.1 파일의 정보를 출력

$ last 2 → /dev/tty2로 로그인한 정보를 출력

❸ /var/log/btmp

- 모든 로그인 실패 정보를 기록하는 로그 파일
- 파일 위치 : /var/log (텍스트가 아닌 바이너리 형태로 로그가 저장됨)
- 로그 출력 명령어 : **lastb**
- 기본적인 사용법은 last 명령과 동일하지만, root만 사용가능

```
[root@localhost ~]# lastb
test03   pts/0                Mon Oct  2 09:23 - 09:23  (00:00)
test01   pts/0                Mon Oct  2 09:19 - 09:19  (00:00)
test03   pts/0                Mon Oct  2 08:56 - 08:56  (00:00)
test01   pts/0                Mon Oct  2 08:00 - 08:00  (00:00)

btmp begins Mon Oct  2 08:00:20 2023
```

lastb → 로그인에 실패한 정보를 출력

lastb gildong → gildong 사용자의 로그인 실패 기록을 출력

lastb -3 → 가장 최근에 로그인에 실패한 3개 기록을 출력

lastb -f /var/log/btmp.1 → /var/log/btmp.1의 로그 기록을 출력

lastb 3 → /dev/tty3에서의 로그인 실패한 기록을 출력

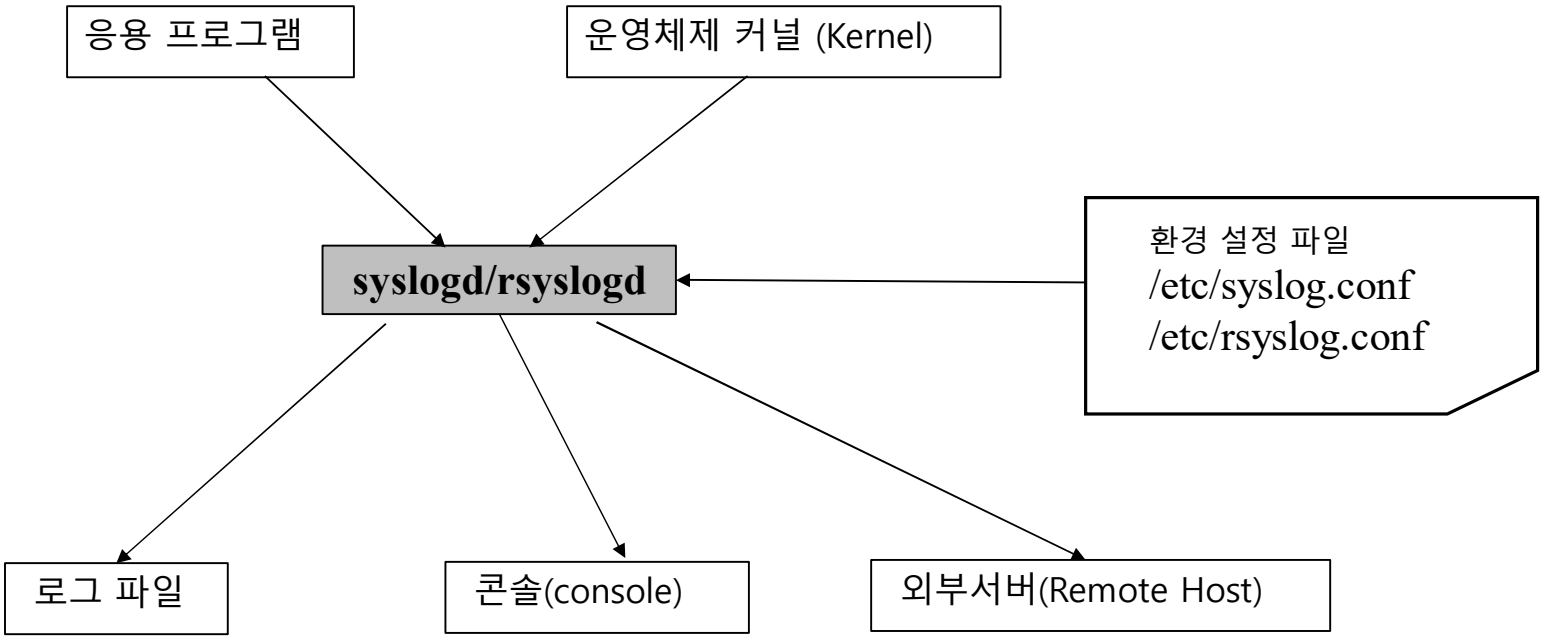
rsyslog 개요

- rsyslogd 데몬이 동작하면서 로그를 기록
- 데몬 동작은 /etc/rc.d/init.d/rsyslog라는 스크립트를 이용
- 환경 설정은 /etc/rsyslog.conf 파일을 통해서 제어

파일명	설명
/etc/rc.d/init.d/rsyslog	rsyslogd 데몬을 동작 시키는 스크립트 start, stop, restart 등의 인자값을 사용
/etc/rsyslog.conf	rsyslogd 데몬의 환경설정파일
/etc/sysconfig/rsyslog	rsyslogd 데몬 실행과 관련된 옵션이 설정되는 파일
/sbin/rsyslogd	실제 rsyslogd 데몬 실행 명령

syslog/rsyslog

- 로그를 중앙 집중적으로 관리하는 패키지
  - rsyslogd 데몬은 /etc/rsyslog.conf 설정파일을 참조하여 로그를 남김
  - /etc/rsyslog.conf 파일에는 “어디에서 로그가 생성이 되면 어디에 로그를 남겨라”설정



파일 /etc/rsyslog.conf

[facility].[priority] [action]

❶ Facility

- 일종의 서비스를 의미, 메시지를 발생시키는 프로그램의 유형

❷ Priority

- 위험 정도를 나타냄, 설정한 수준보다 높아야 메시지를 보냄

❸ Action

- 메시지를 보낼 목적지나 행동들에 관한 설정으로 일반적으로 파일명을 적음

* facility 종류(what)

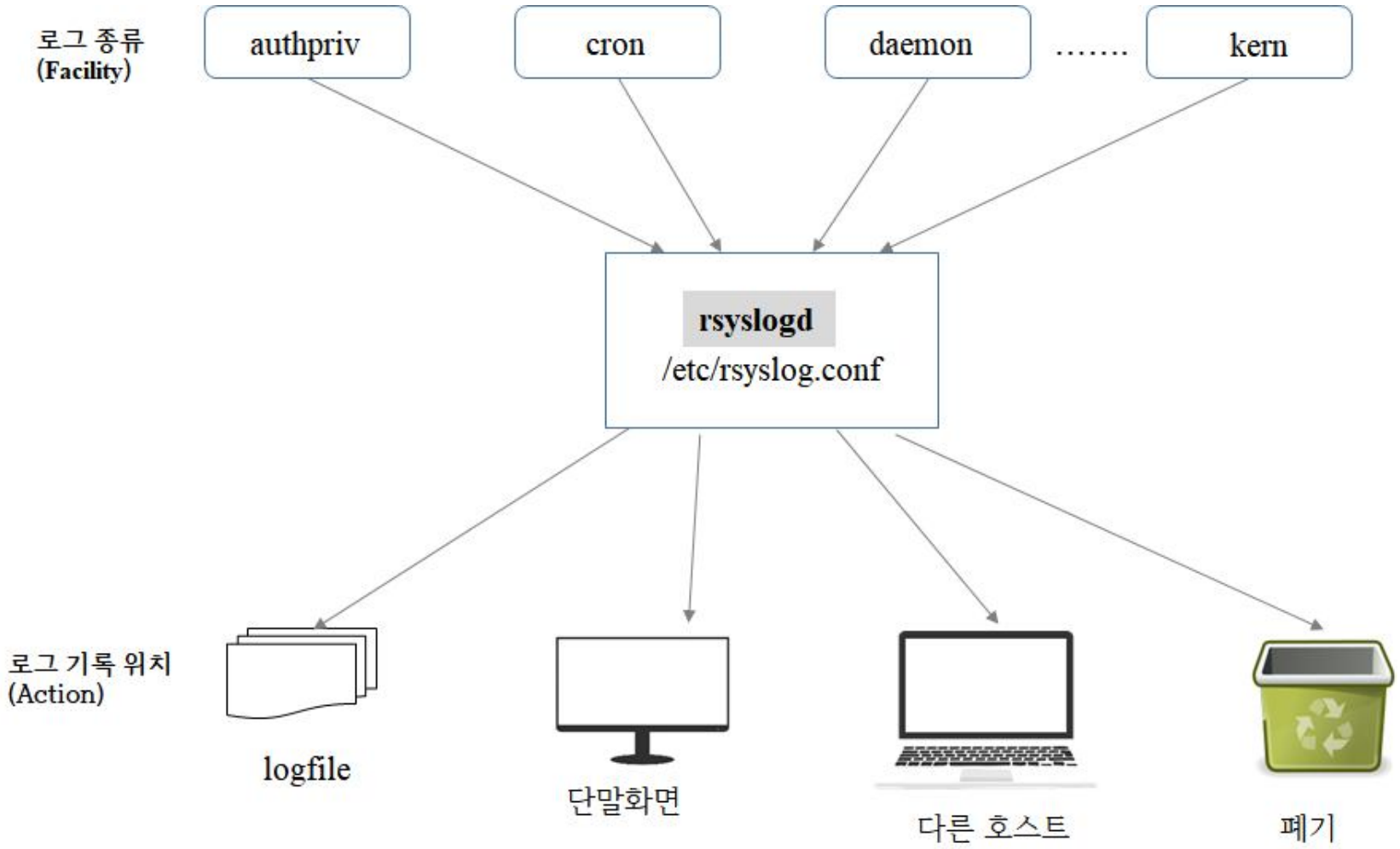
cron	cron, at과 같은 스케줄링 프로그램이 발생한 메시지
auth, security	login과 같이 인증프로그램 유형이 발생한 메시지
authpriv	ssh와 같이 인증을 필요한 프로그램 유형이 발생한 메시지 사용자 추가 시에도 메시지가 발생
daemon	telnet, ftp 등과 같이 여러 데몬이 발생한 메시지
kern	커널이 발생한 메시지
lpr	프린트 유형의 프로그램이 발생한 메시지
mail	mail 시스템이 발생한 메시지
mark	syslogd에 의해 만들어지는 날짜 유형
news	유즈넷 뉴스 프로그램 유형이 발생한 메시지
syslog	syslog 프로그램이 유형이 발생한 메시지
user	사용자 프로세스
uucp	UUCP(UNIX to UNIX Copy Protocol)시스템이 발생한 메시지
local0 ~ local7	여분으로 남겨둔 유형
*	모든 facility를 의미

* priority 종류 (심각수준,level)

none	로그로 기록하지 않음
debug	프로그램을 개발 또는 테스트 할 때 발생하는 메시지
info	사용자가 알아둬야 할 기본정보 메시지
notice	특별한 주의를 필요하나 에러는 아닌 메시지
warning, warn	주의가 필요한 경고 메시지(무시해도 됨)
error, err	에러가 발생하는 경우의 처리가 필요한 경우 발생 메시지 소프트웨어 상에서 발생하는 오류 메시지
crit	크게 급하지는 않지만 시스템에 문제가 생기는 단계의 메시지 하드웨어 장치에 문제가 발생 시 생성
alert	즉각적인 조정을 해야 하는 상황 시스템 DB에 손상 등 즉시 수정해야 되는 상황
emerg, panic	모든 사용자들에게 전달되는 패닉 상황 블루스크린, 커널 패닉 등에서 발생

* Action 종류(where)

file	지정한 파일에 로그를 기록
@host	지정한 호스트로 메시지를 전달
user	지정한 사용자가 로그인한 경우 해당 사용자의 터미널로 전달
*	현재 로그인되어 있는 모든 사용자의 화면으로 전달
콘솔 또는 터미널	지정한 터미널로 메시지를 전달


로그 종류
(Facility)
authpriv
cron
daemon
.....
kern
rsyslogd
/etc/rsyslog.conf
로그 기록 위치
(Action)
logfile
단말화면
다른 호스트
폐기

systemctl stop/start/restart rsyslog ⟶ rsyslogd 동작 중단/시작/재시작

systemctl enable rsyslog ⟶ 부팅 시 rsyslogd 활성화

systemctl –l status rsyslog ⟶ rsyslogd 상태 정보 확인

ls –l /etc/rsyslog.conf

ps -ef | grep rsyslog ⟶ rsyslogd 동작 확인

```
[root@localhost ~]# ls -l /etc/rsyslog.conf
-rw-r--r--. 1 root root 3232  3월 26  2014 /etc/rsyslog.conf
[root@localhost ~]#
[root@localhost ~]# ps -ef | grep rsyslog
root         943       1  0 04:48 ?        00:00:00 /usr/sbin/rsyslogd -n
root       37124   17009  0 15:45 pts/1    00:00:00 grep --color=auto rsyslog
[root@localhost ~]#
```

```
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
  GNU nano 2.3.1                                File: /etc/rsyslog.conf

$OmitLocalLogging on

# File to store the position in the journal
$IMJournalStateFile imjournal.state


#### 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
```

#nano /etc/rsyslog.conf

```
  GNU nano 2.3.1                                        File: /etc/rsyslog.conf

# 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

*.notice                                                        /var/log/test.log
```

#touch /var/log/test.log

```
[root@localhost ~]# touch /var/log/test.log
[root@localhost ~]# ls -l /var/log/test.log
-rw-r--r--. 1 root root 0 10월  2 15:57 /var/log/test.log
[root@localhost ~]#
```

#systemctl restart rsyslog

#systemctl status rsyslog

```
[root@localhost ~]# nano /etc/rsyslog.conf
[root@localhost ~]# systemctl restart rsyslog
[root@localhost ~]# systemctl status rsyslog
rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled)
   Active: active (running) since 월 2023-10-02 16:01:05 KST; 6s ago
 Main PID: 38416 (rsyslogd)
   CGroup: /system.slice/rsyslog.service
           └─38416 /usr/sbin/rsyslogd -n

10월 02 16:01:05 localhost.localdomain systemd[1]: Started System Logging Service.
[root@localhost ~]#
```

#logger –p local1.notice logging test

#logger –p local1.notice Hello~

#cat /var/log/test.log

```
[root@localhost ~]# logger -p local1.notice logging test
[root@localhost ~]# cat /var/log/test.log
Oct  2 16:04:03 localhost gildong: logging test
[root@localhost ~]# logger -p local1.notice Hello~~
[root@localhost ~]# cat /var/log/test.log
Oct  2 16:04:03 localhost gildong: logging test
Oct  2 16:05:31 localhost gildong: Hello~~
[root@localhost ~]#
```

❶ *.=crit;kern.none /var/log/critical

→ 모든 facility가 발생하는 메시지 중에 crit 수준의 메시지만 /var/log/critical에 기록

→ 커널이 발생하는 메시지는 제외

❷ *.emerg *

→ 모든 emerg 수준 이상의 문제가 발생하면 모든 사용자에게 메시지를 전달

❸ authpriv.* root,gildong

→ 인증 관련 로그를 root 및 gildong 사용자의 터미널로 전송

❹ mail.*;mail.!=info /var/log/maillog

→ mail 관련한 모든 정보는 /var/log/maillog에 기록하는데, info 수준의 로그는 제외