25. System Log

Log File

- System Log
  - 리눅스 운영시 발생하는 이벤트들에 대한 정보를 기록한 것을 말한다.
- Log File
  - 접속한 사용자 정보, 접속 이력 정보, su 명령을 사용한 정보, 부팅시 출력되는 로그 정보, 커널 또는 프로세스에 의해 만들어지는 메시지 정보 등 수많은 정보들이 시스템 운영시 만들어지는데 이러한 정보를 기록한 파일을 의미한다.

/var/run/utmp

- 현재 접속한 사용자 정보를 가지고 있는 데이터 파일이다.
- who 또는 w 같은 명령에 의해 참조된다.

```
[root@itserver ~]# file /var/run/utmp
```

/var/log/wtmp

- 사용자들이 접속한 이력 정보를 가지고 있는 파일이다.
- last 명령을 통해 사용자 접속 이력을 확인할 수 있다.

```
[root@itserver ~]# file /var/log/wtmp
```

/var/log/sulog

- su 명령을 사용한 사용자 전환에 관련된 로그 파일이다.
- 기본적으로 없는 파일이다. 생성 및 설정을 해야 한다.

```
[root@itserver ~]# vi /etc/login.defs
# su command log file
SULOG_FILE=/var/log/sulog
[root@itserver ~]# vi /etc/rsyslog.conf
# su command log
authpriv.info   /var/log/sulog
[root@itserver ~]# touch /var/log/sulog
[root@itserver ~]# service rsyslog restart
```

/var/log/secure

- SSH, FTP, su 명령 등 사용자 인증 관련 기록을 가지고 있는 로그 파일이다.

```
[root@itserver ~]# grep -i ssh /var/log/secure | grep -i fail
```

/var/log/cron

- 사용자들의 cron 사용 기록 정보를 가지고 있는 로그 파일이다.

```
[root@itserver ~]# head -5 /var/log/cron
```

/var/log/dmesg

- 부팅시 시스템에 의해 출력되는 로그 정보를 가지고 있는 파일이다.
- dmesg 명령을 통해 내용을 확인할 수 있다.

[root@itserver ~]# head -5 /var/log/dmesg

/var/log/lastlog

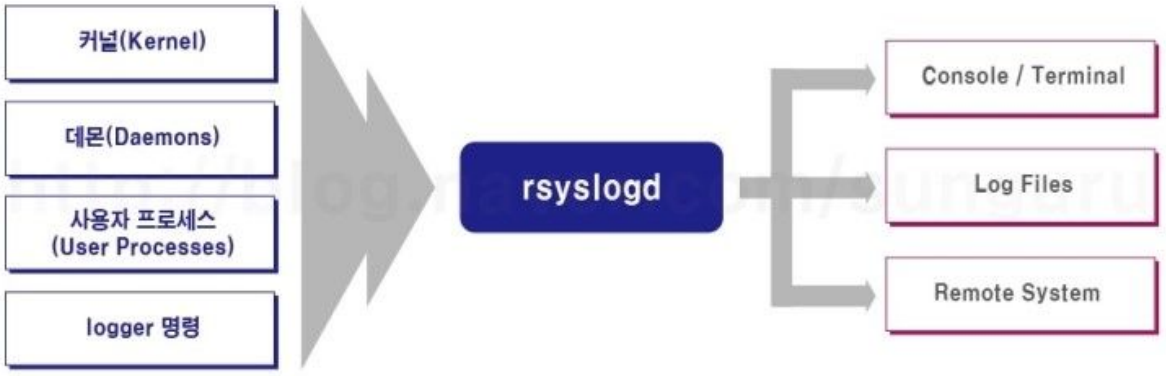
- 사용자들이 마지막으로 로그인한 접속 정보를 가지고 있는 로그 파일이다.
- lastlog 명령을 통해 내용을 확인할 수 있다.

rsyslogd

rsyslogd

- 메시지 로깅을 지원하는 시스템 유틸리티이다.
- 이전에 사용하던 syslogd의 확장버전으로 생각할 수 있다.
- 커널, 데몬, 사용자 프로세스들은 동작 중에 수많은 메시지를 만들어낸다. 각 프로그램들마다 메시지를 관리하기에는 어려움이 있기 때문에 일정한 규칙을 통해 메시지를 기록, 관리하기 위해 만든 것이 로그 시스템이다.
- rsyslogd는 메시지를 생성하는 대상, 위험 수준, 메시지 전달 대상을 가지고 규칙을 만들어낸다. 로컬 시스템의 로그 파일에 저장할 수도 있고, 원격지의 로그 서버에 메시지를 전달하여 저장할 수도 있다.

[root@itserver ~]# service rsyslog status
[root@itserver ~]# chkconfig --list rsyslog
[root@itserver ~]# ps -ef | grep rsyslogd | grep -v grep



rsyslogd 서비스 시작/종료

- service rsyslog {stop | start | status}

/etc/rsyslog.conf

- rsyslogd 데몬 프로세스의 구성 파일이다.
- 파일의 주석 기호는 #이다.
- 일반적으로 다음과 같이 메시지 처리 규칙(Rules)이 설정되어 있다.
  FacilityLevel.SecureLevel Action

1. **Facility Level**
   - Facility는 메시지를 생성하는 대상을 나타낸다.

Facility 번호	키워드	설명

0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9		clock daemon
10	authpriv	security/authorization messages
11	ftp	FTP daemon
12	-	NTP subsystem
13	-	log audit
14	-	log alert
15	cron	clock daemon
16	local0	local use 0
17	local1	local use 1
18	local2	local use 2
19	local3	local use 3
20	local4	local use 4
21	local5	local use 5
22	local6	local use 6
23	local7	local use 7

2. Security Level

- 메시지의 중요도를 나타낸다.

Code	Security	키워드	설명	세부 설명

0	Emergency	emerg	시스템 사용불능	Panic 상황이며 보통 이런 메시지면 시스템 리부팅이 된다. 메모리/CPU 오류 많이 발생한다.
1	Alert	alert	즉각 조치 필요	즉각조치가 필요한 상황을 나타낸다.
2	Critical	crit	위기 상황	//
3	Error	err	오류 상황	긴급장애는 아니지만 조치가 필요한 상황을 나타낸다. 하드디스크 오류시 많이 발생한다.
4	Warning	warn	경고 상황	긴급장애는 아니지만 조치가 필요한 상황을 나타낸다. 파일시스템사용량 많을 때 발생한다.
5	Notice	notice	정상이지만 알림상황	이벤트 정도의 메시지이다.
6	Information	info	일반 정보 메시지	정상 운영 메시지이다.
7	Debug	debug	디버그레벨 메시지	응용프로그램 디버깅을 위한 것으로3. 개발자들에게 유용하다.

3. Action

- 메시지 전달 메시지를 나타낸다.
- 대부분 파일을 설정하며 콘솔이나 원격지 시스템이 설정될 수도 있다. 메시지를 보관한 파일을 로그 파일, 네트워크를 통해 메시지들을 저장, 관리하는 시스템을 로그 서버라고 한다.

/var/log/messages

- 시스템 주요 메시지 정보가 저장되는 로그 파일이다.
- 보관 주기 및 파일 개수 설정에 따라 로그 보관기간이 달라진다.

/etc/logrotate.conf

- logrotate 명령에 대한 설정 파일로 로그 파일 저장 주기 및 압축 여부 등을 설정할 수 있다.
- logrotate는 시스템 로그 파일을 전환, 압축하기 위해 사용되는 명령이다. 이는 로그 파일이 방대해지는 것을 방지하기 위해 사용하며 cron에 의해 매일 실행된다.
- logrotate.conf 설정 정보

설정 정보	내 용
weekly	로그 파일을 바꾸는 교체 주기를 나타낸다. 설정값은 daily, weekly, monthly가 있다.
rotate N	교체 파일 개수를 설정한다. 로그 파일 교체주기가 weekly이고 rotate 4로 되어 있다면 로그는 한달간(4 weeks) 보관된다.
create	지난 로그 파일 교체 후 새 로그파일을 생성한다.

compress	로그 파일을 압축한다. 기본값은 비압축이다.

logger 명령

- **logger**
  - /etc/rsyslog.conf 파일의 내용을 변경하였다면 rsyslogd 데몬이 변경한 설정정보대로 정상적으로 동작하는지 확인하기 위해 사용하는 명령이다.

기능	강제적으로 rsyslogd 데몬에 메시지를 전달하기 위해 사용하는 명령이다.
형식	**logger 옵션 메시지**
옵션	-i: 메시지에 logger 프로세스의 PID를 남김 -f 파일명: 파일의 내용을 메시지 내용으로 사용 -p PRIORITY: 메시지의 우선순위를 출력. 즉 Facility.Security를 표시 -t TAG: 메시지에 태그를 명시. 일반적으로 TAG는 프로세스이름임 메시지: 로그로 남길 메시지를 표시