25. System Log

Chapter 25 System Log

- **Log**
  - 커널과 리눅스 시스템이 제공하는 여러 서비스와 응용프로그램이 발생시키는 메시지
- **Log File**
  - 로그를 저장하고 있는 파일

주요 Log File

- 대부분의 로그 파일은 **/var/log** 디렉터리에 있다.

로그 파일 관리

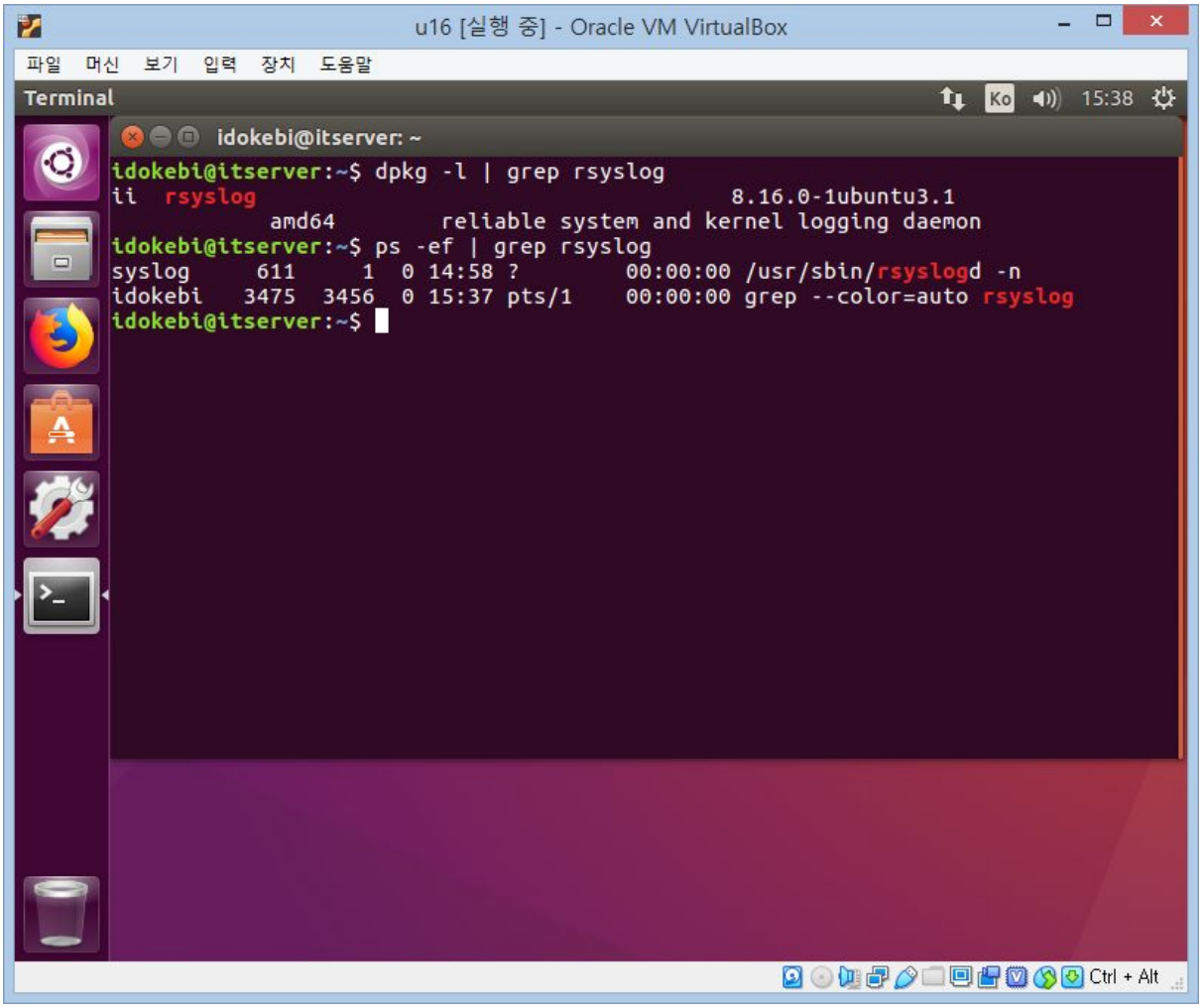
- 같은 파일명에 번호가 붙은 파일을 여러 개 볼 수 있다.
  - 로그를 계속 한 파일에 저장할 경우 파일의 크기가 너무 커져서 파일의 내용을 보거나 관리할 때 불편하기 때문
  - 시스템 관리자는 번호가 큰 로그 파일은 백업을 하고 삭제해야 한다.
- 로그 파일의 소유자는 거의 대부분 root 계정이고, 접근 권한은 대부분의 경우 root 계정만 읽고 쓸 수 있게 설정되어 있다.

주요 로그 파일

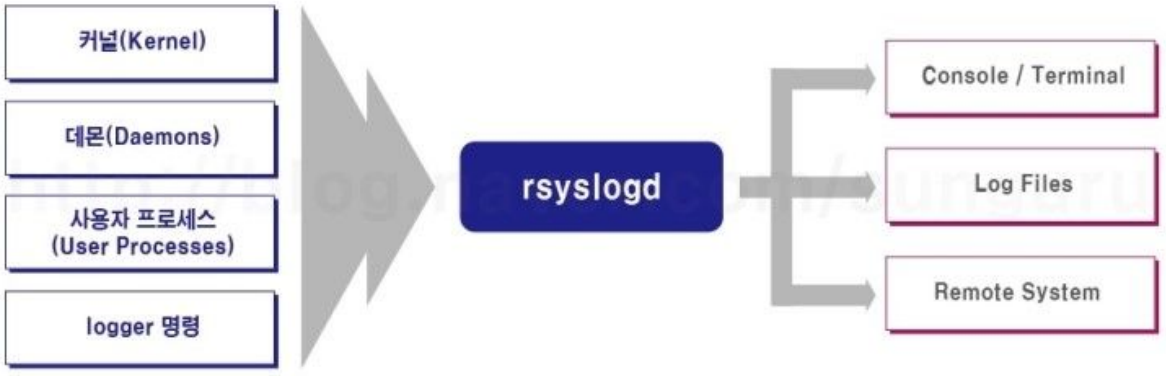
로그 파일	내용
/var/log/boot.log	부팅시 서비스 데몬의 실행 상태를 기록
/var/log/apache2/*	아파치 웹 서버와 관련된 로그를 기록
/var/log/apt/*	apt-get 명령으로 패키지를 설치하고 삭제한 로그를 기록
/var/log/auth.log	telnet, ssh, su, sudo 등의 사용자 로그인 인증을 기록
/var/log/dmesg	각 계정의 가장 최근 로그인 정보를 기록하고 lastlog 명령으로 확인
/var/log/lastlog	실패한 로그인 기록(바이너리 파일) last-f btmp 또는 last 명령으로 확인 가능
/var/log/btmp	로그인 기록이며 last 명령으로 내용을 확인
/var/log/syslog	syslog가 생성하는 공통 로그를 기록
/var/log/ufw.log	방화벽이 생성하는 로그를 기록

로그 관리 데몬

- 리눅스 시스템의 로그 파일 중 일부는 로그 관리 데몬에 의해 통제된다.
- 현재 시스템에서 로그 관리 데몬으로 rsyslog가 동작 중임을 확인된다.



- rsyslog 서비스를 제공하는 데몬은 rsyslogd이고, rsyslog 서비스를 설정하는 파일은 /etc.rsyslog.d 디렉터리에 있는 *.conf 파일이다.
- 이 중 50-default.conf는 어떤 로그를 어떻게 처리할 것인지 기본 규칙을 설정한 파일이다.
- rsyslog의 규칙 파일은 텍스트 파일이므로 관리자가 vi로 수정할 수 있다.



선택자

- rsyslog의 선택자는 기능명과 우선순위를 기반으로 다음과 같은 형식이다.
- **기능명.우선순위**

- **Facility[기능]**
  - 로그 메시지를 생성하는 프로그램을 지정한 것

기능명	관련 프로그램
*	모든 기능
auth	인증 관련 명령
authpriv	보다 민감한 보안 메시지
cron	cron 데몬
daemon	일반 시스템 데몬
kern	시스템 커널
security	auth와 동일, 사용하지 않음
syslog	rsyslog 데몬 내부 메시지
user	사용자 프로세스
local0~7	8가지 로컬 메시지
mark	일정 주기로 타임 스탬프 메시지 생성(rsyslog 내부용)

- **Security Level[우선 순위]**
  - 메시지의 심각도를 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.

Action[동작]

- 선택자가 선택한 메시지를 어떻게 처리할지를 정의한 것이다.
- 로그 파일의 경로 앞에 붙은 -는 특별한 의미가 없으므로 신경쓰지 않아도 된다.

로그 관리 도구

- wtmp 같은 일부 파일을 제외하고 대부분의 로그 파일은 일반 텍스트 파일이다.
- 따라서 vi 같은 편집기로 파일의 내용을 확인할 수 있다.
- GNOME은 로그를 관리할 수 있는 GUI 도구인 로그뷰어를 제공한다.
    - GNOME 로그 뷰어: gnome-system-log