# 1.1 시스템 로그 분석 및 관리

## 시스템 로그의 개요

- 로그
  - 시스템에서 일어나는 모든 사건이나 이벤트 등은 각 서비스별로 기록됨
  - 로그 분석은 시스템 보안에 중요한 역할
- 로그 기록 패키지
  - 리눅스 초기에는 syslog 패키지를 사용
  - syslogd 데몬이 /etc/syslog.conf 설정 파일을 기반으로 서비스별 로그 파일을 /var/log 디렉터리에 생성
  - 최근 리눅스 배포판에서는 rsyslog 패키지로 대체
  - rsyslogd 데몬이 /etc/rsyslog.conf 설정 파일을 기반으로 서비스별 로그 파일을 /var/log 디렉터리에 생성
  - rsyslogd는 syslog의 성능을 대폭 강화한 패키지로 멀티스레드 지원, TCP 지원, SSL 및 TLS 지원, MySQL 등과 같은 데이터베이스 지원, 보내는 목록 제한, 메시지 일부 필터링, 출력 포맷 제어 등 다양한 기능을 지원

---

## rsyslog

- rsyslog 개요
  - rsyslog는 rsyslog 데몬이 동작하면서 로그를 기록
  - 관련 환경 설정은 /etc/rsyslog.conf 파일을 통해 제어

| 파일명 | 설명 |
| --- | --- |
| /etc/rsyslog.conf | rsyslogd 데몬의 환경 설정 파일 |
| /etc/sysconfig/rsyslog | rsyslogd 데몬의 실행과 관련된 옵션이 설정되는 파일 |
| /sbin/rsyslogd | 실제 rsyslogd 데몬 실행 명령 |

- **/etc/rsyslog.conf** 파일
  - [기본 구성 형식]
    - **facility.priority  action**

- facility: 일종의 서비스를 의미, 메시지를 발생시키는 프로그램의 유형
- priority: 위험의 정보. 설정한 수준보다 높아야 메시지를 보낸다. 설정값 앞에 =을 사용할 경우에는 해당 레벨의 위험도와 같은 경우에만 메시지를 기록. !는 제외시킬 때 사용
- action: 메시지를 보낼 목적지나 행동들에 관한 설정으로 보통 파일명을 적는다.

◦ [facility 종류]

| facility | 설명 |
|---|---|
| cron | cron, at과 같은 스케줄링 프로그램이 발생한 메시지 |
| auth, security | login과 같이 인증 프로그램 유형이 발생한 메시지 |
| authpriv | ssh와 같이 인증이 필요한 프로그램 유형이 발생한 메시지로 사용자 추가 시에도 메시지가 발생 |
| daemon | telnet, ftp 등과 같은 여러 데몬이 발생한 메시지 |
| kern | 커널이 발생한 메시지 |
| lpr | 프린트 유형의 프로그램이 발생한 메시지 |
| mail | 메일 시스템이 발생한 메시지 |
| mark | syslogd에 의해 만들어지는 날짜 유형 |
| news | 유즈넷 프로그램 유형이 발생한 메시지 |
| syslog | syslog 프로그램 유형이 발생한 메시지 |
| user | 사용자 프로세스 |
| uucp | UUDP(Unix to Unix Copy Prototol) 시스템이 발생한 메시지 |
| local0 ~ local7 | 여분으로 남겨둔 유형 |
| * | 모든 facility를 의미 |

◦ [facility 종류]

| priority | 설명 |
|---|---|
| none | 지정한 facility 제외, 보통 앞에 다른 facility에 대한 설정을 하고 ;뒤에 특정 facility를 제외할 때 사용 |
| debug | 프로그램을 디버깅할 때 발생하는 메시지 |
| info | 통계, 기본 정보 메시지 |
| notice | 특별한 주의를 필요로 하나 에러는 아닌 메시지 |
| warning, warn | 주의가 필요한 경고 메시지 |
| | |

| | |
|---|---|
| error | 에러를 발생하는 경우의 메시지 |
| crit | 크게 급하지는 않지만 시스템에 문제가 생기는 단계의 메시지 |
| alert | 즉각적인 조정을 해야하는 경우 |
| emerg, panic | 모든 사용자에게 전달해야 할 위험한 상황 |

- [action 종류]

| action | 설명 |
|---|---|
| file | 지정한 파일에 로그를 기록 |
| @host | 지정한 호스트로 메시지를 전달 |
| user | 지정한 사용자가 로그인한 경우 해당 사용자의 터미널로 전달 |
| * | 현재 로그인 되어 있는 모든 사용자의 화면으로 전달 |
| 콘솔 또는 터미널 | 지정한 터미널로 메시지 전달 |

- 사용 예
  - *.=crit;kern.none /var/log/critical
  - *.ermerg *
  - authpriv.* root,lima
  - authpriv.* /dev/tty2
  - mail.*;mail.! =info /var/log/maillog
  - uucp,news.crit /var/log/news

---

# 로그 파일 관리: logrotate

- **logrotate** 개요
  - 로그 파일은 계속적으로 덧붙여지면서 쌓이는 형태라 파일의 크기가 계속 커지게 된다.
  - 이를 방지하기 위해 로그 파일을 여러 개로 분할해주는 프로그램이 logrotate이다.
  - 로그 파일의 자동 로테이션 기능, 압축 기능, 제거 등을 지원
  - 각각의 로그 파일은 하루, 일주일, 한달 단위로 로테이션을 할 수 있다.
  - 시스템과 관련된 기본적인 로그 설정은 /etc/logrotate.conf에서 제어하고, 응용 프로그램은 /etc/logrotate.d 디렉터리에 위치하여 로그 파일은 관리

    - 명령행에서 logrotate를 직접 사용이 가능하지만, 현재 리눅스에서는 /etc/cron.daily 디렉터리에 등록되어서 cron에 의해 스케줄링되어 실행되고 있다.
    - 사용법
        - **logrotate 옵션 설정파일**
        - 주요 옵션
            - -f: 강제로 환경 설정 파일을 읽어들여 실행(—force)
        - 사용 예
            - logrotate -f /etc/logrotate.conf
- /etc/logrotate.conf의 주요 설정
    - weekly
    - rotate 4
        - 최대 4번까지 로테이트, 기본로그파일, 로그파일.1, 로그파일.2, 로그파일.3, 로그파일.4 현태로 생성
    - create
    - dateext
    - compress
    - include /etc/logrotate.d
    - nomissingok
        - 로그 파일이 존재하지 않는 경우에 에러 메시지를 출력. 기본값
    - missingok
        - 로그 파일이 존재하지 않는 경우에 에러 메시지를 출력하지 않고 다음 파일로 이동
    - /var/log/wtmp {
        - monthly
        - create 0644 root utmp
        - minsize 1M
        - rotate 1
        - }

        - 로그 파일명을 명기하면 별도로 지정이 가능
        - /var/log/wtmp는 한달마다 로테이트, 파일 크기가 1M가 되면 그 이전이라도 로테이트를 실행, 파일 생성시에 허가권 0644, 소유자는 root, 소유그룹은 utmp로 결정. 또한 로테이션으로 생성되는 로그 파일은 1개만 생성
- 관련 파일: /var/lib/logrotate.status(CentOS 6)
    - 각 로그 파일별로 로테이션된 날짜가 기록된 파일