1.2 로그 관련 파일

로그 관련 주요 파일

- **/var/log/messages**
  - 시스템에서 발생하는 표준 메시지가 기록되는 파일
  - 대부분의 로그가 이 파일에 쌓이고, root만이 읽을 수 있도록 설정
  - 날짜 및 시간, 메시지가 발생한 호스트명, 메시지를 발생한 내부 시스템이나 응용 프로그램의 이름, 발생된 메시지(: 으로 구분) 순으로 기록
- **/var/log/secure**
  - 인증에 기반한 접속과 관련된 로그가 기록되는 파일
  - 보통 login(telnet, ssh), tcp wrappers, xinetd 관련 로그가 쌓인다.
- **/var/log/dmesg**
  - 시스템이 부팅할 때 출력되었던 로그가 기록
  - 커널 부트 메시지 로그라고 한다.
- **/var/log/maillog**
  - sendmail, dovecot 등 메일 관련 작업이 기록되는 로그 파일
- **/var/log/xferlog**
  - FTP 접속과 관련된 작업이 기록되는 파일
  - 로그 포맷: 총 14개 영역으로 구성
    - current-time
    - transfer-time
    - remote-host
    - file-size
    - filename
    - transfer-type
    - special-action-flag
    - direction

        - access-mode
        - username
        - service-name
        - authentication-method
        - authentication-user-id
        - comletion-status
- **/var/log/cron**
    - cron 관련 정보가 기록되는 파일
- **/var/log/boot.log**
    - 부팅 시 발생되는 메시지가 기록되는 파일로 보통 부팅 시 동작하는 데몬 관련 정보가 기록
- **/var/log/lastlog**
    - telnet이나 ssh를 이용해서 접속한 각 사용자의 마지막 정보가 기록되는 파일-바이너리 파일
    - lastlog라는 명령으로 확인
- **/var/log/wtmp**
    - console, telnet, ftp 등 이용하여 접속한 사용자 기록, 시스템을 재부팅한 기록 등의 로그가 쌓이는 파일-바이너리 파일
    - last라는 명령으로 확인
- **/var/log/btmp**
    - wtmp와 반대되는 로그로 접속이 실패한 경우에 기록-바이너리 파일
    - lastb라는 명령으로 확인
- 참고 자료

  utmp

  : 현재 로그인한 사용자 상태 정보를 담고 있는 로그파일

  Path: /var/run/utmp

  Cmd: w, who

  wtmp

  : 성공한 로그인/로그아웃 정보 로그파일

: system boot / shutdown 정보 로그파일

Path: /var/log/wtmp

Cmd: last

btmp

: 실패한 로그인 정보를 담고 있는 로그파일

Path: /var/log/btmp

Cmd: lastb

last log

: 마지막으로 성공한 로그인 정보를 담고있는 로그파일

Path: /var/log/lastlog

Cmd: lastlog

관련 명령어

- **last**
  - 사용자의 로그인 정보, 재부팅한 정보는 /var/log/wtmp 파일에 저장-바이너리 파일
  - 이 파일의 내용을 출력
  - 사용법
    - **last 옵션 사용자명**
    - 옵션
      - -f 파일명: 로그 로테이션 설정이 되어 있는 경우, 기본 로그 파일 이외의 다른 로그 파일의 기록을 볼 경우에 사용
      - -n 숫자: 가장 최근부터 해당 숫자값 만큼만 출력(-숫자와 같다)
      - -t YYYYMMDDHHMMSS: 지정된 시간 이전에 로그인한 기록을 출력
      - -R: IP주소나 호스트명을 출력하지 않는다.
      - -a: 호스트명이나 IP 주소 필드를 맨 마지막에 출력. 일반적으로 -d 옵션과 함께 사용
      - -d: 리눅스는 외부에서 접속한 기록을 IP주소뿐만 아니라, 호스트 이름도 저장. 호스트 이름이 존재하는 경우에 IP주소를 호스트 이름으로 변환하여 출력

        - -F: 로그인 및 로그아웃 시간을 출력
        - -i: 접속한 호스트의 IP 주소로만 출력
        - -w: 사용자의 전체 이름이나 전체 도메인 이름 전부 출력
    - 사용 예
        - last
        - last lima
        - last reboot
        - last -1 boot
        - last -f /var/log/wtmp.1
        - last 2
- **lastlog**
    - 각각의 사용자가 마지막으로 로그인한 정보를 출력해주는 명령
    - 바이너리 파일인 /var/log/lastlog의 내용을 출력
    - 사용법
        - **lastlog 옵션**
        - 옵션
            - -u 사용자명: 특정 사용자에 대한 정보만 출력
            - -t 날짜: 오늘부터 지정한 날짜만큼 거슬려 올라가 그 이후에 로그인한 사용자의 정보를 출력
    - 사용 예
        - lastlog
        - lastlog -u lima
        - lastlog -t 3
- **lastb**
    - last와 반대되는 개념의 명령으로 로그인에 실패한 정보를 /var/log/btmp에 기록하는데, 이 파일의 내요을 출력
    - 기본적인 사용법은 last와 동일하지만, root만 사용 가능
    - 사용법

        - **lastb 옵션 사용자명**
        - 옵션
            - -f 파일명
            - -n 숫자
            - -t YYYYMMDDHHMMSS
            - -R
            - -a
            - -d
            - -F
            - -i
            - -w
    - 사용 예
        - lastb
        - lastb lima
        - lastb -3
        - lastb -f /var/log/btmp.1
        - lastb 3
- **dmesg**
    - 커널 링 버퍼의 내용을 출력하고 제어하는 명령
    - 커널 링 버퍼: 커널의 동작과 관련된 메시지를 기록해주는 영역
    - 사용법
        - **dmesg 옵션**
        - 옵션
            - -c: 커널 링 버퍼에 저장된 메시즈를 출력한 후에 지운다
    - 사용 예
        - dmesg
        - dmesg -c

- 커널 링 버퍼에 저장된 메시지를 전부 지운다