목차

터미널 명령어 로깅 3
PROMPT_COMMAND 이용하는 방식 3
별도의 로그 파일로 기록 저장 4
참조링크 4

Last update: 2025/08/06 01:41	터미널 명령어 로깅	https://atl.kr/dokuwiki/doku.php/%ED%84%B0%EB%AF%B8%EB%84%90_%EB%AA%85%EB%A0%B9%EC%96%B4_%EB%A1%9C%EA%B9%85

터미널 명령어 로깅

사용자가 터미널로 접속하여 명령어를 입력한것을 모두 로그로 남기는 방법에 대해 설명한다.

/etc/profile.d/cmd_log.sh

```
#!/bin/bash
function logging
{
    #stat="$?"
    cmd=$(history|tail -1)
    srcip=`who -m | awk -F'(' '{print $2}' | awk -F')' '{print $1}'`

    if [ "$cmd" != "$cmd_old" ]; then
        #logger -p local6.info "[2] STAT=$stat"
        logger -p local6.info "PID= $$, SRC=$srcip, PWD=$PWD, CMD=$cmd"
    fi
    cmd_old=$cmd
}
trap logging DEBUG
```

위와같이 스크립트를 생성해 두면 된다. 위의 방식은 시스템의 로그 파일messages 또는 syslog에 출력이 된다. 별도의 파일로 기록하려면 맨 아래 내용을 참고한다.

PROMPT_COMMAND 이용하는 방식

단, 이 방식은 SSH/Telnet등과 같이 원격에서 쉘로 접속하는경우와 CLI접속시에만 적용되며 Xwindows 환경에서는 적용되지 않는다.

또다른 방식으로 아래처럼 구현해도 된다.

/etc/profile.d/command-logging.sh

```
#!/bin/bash
# Script to log user commands to syslog
export PROMPT_COMMAND='history -a; logger -p local6.info -t bash-commands
"USER=$USER IP=$(who -m | awk "{print \$5}" | tr -d "()") PWD=$PWD
CMD=$(history 1 | sed "s/^[ ]*[0-9]\+[ ]*//")"'
```

그리고 해당 스크립트에 실행권한을 부여한다.

```
# 스크립트에 실행 권한 부여
chmod +x /etc/profile.d/command-logging.sh
```

별도의 로그 파일로 기록 저장

명령어 로그를 /var/log/command.log에 기록한다.

/etc/rsyslog.d/command-logging.conf

```

# Rule for command logging
local6.* /var/log/command.log
```

참조링크

- http://coffeenix.net/board_view.php?bd_code=1659
- http://hanbyoru.tistory.com/227

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/%ED%84%B0%EB%AF%B8%EB%84%90_%EB%AA%85%EB%A0%B9%EC%96%B4_%EB%A1%9C%EA%B9%85

Last update: **2025/08/06 01:41**