

.....	3
PROMPT_COMMAND	3
.....	4
.....	4

Last update: 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
2025/08/06 01:41

가

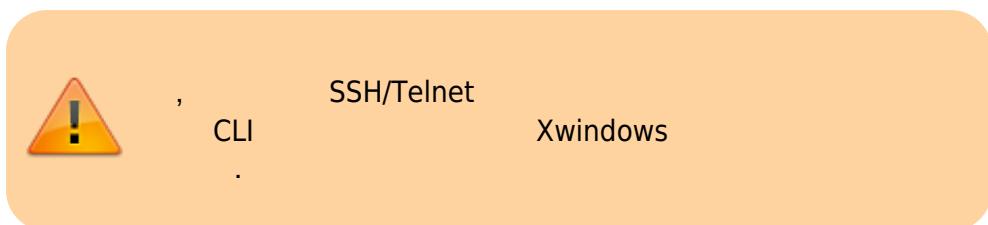
/etc/profile.d/cmd_log.sh

```
#!/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
```

messages syslog

PROMPT_COMMAND



/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]\+[ \ ]*//")"'
```

Last update: 2025/08/06 01:41
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

```
# chmod +x /etc/profile.d/command-logging.sh
```

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

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

- 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