

..... 3

..... 3

[illegible]

Step 1) 1. utmp, wtmp ,btm
IP, 2. sulog
su 3. xferlog
ftp 가

Step 2)

Step 3)

```
Step 1) vi /etc/rsyslog.conf
```

```
#vi /etc/rsyslog.conf
```

Step 2)

```

*.info;mail.none;authpriv.none;cron.none    /var/log/messages
authpriv.*                                    /var/log/secure
mail.*                                         /var/log/maillog
cron.*                                         /var/log/cron
*.alert                                        /dev/console
*.emerg                                        *
```

Step 3) RSYSLOG

```
#ps -ef | grep rsyslogd
root 7524 6970 0 Apr 23 - 0:02 /usr/sbin/rsyslogd
#kill -HUP [PID]
```

auth	
authpriv	
cron	cron, at
daemon	telnet, ftpd
kern	
lpr	
mail	
news	
syslog	syslog
user	
uucp	
local0	

4 ()	Emergency [emerg]	
3	Alert [alert]	
2	Critical [crit]	가
1	Error [err]	
0	Warnnig [warning]	
-1	Notice [notice]	가
-2	Information [info]	
-3 ()	Debug [debug]	

From:

<https://atl.kr/dokuwiki/> - AllThatLinux!

Permanent link:

https://atl.kr/dokuwiki/doku.php/%EB%A1%9C%EA%B7%B8_%EA%B4%80%EB%A6%ACLast update: **2022/01/18 01:12**