

..... 3

..... 3

가 가 가 가

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

Step 1) vi "/etc/syslog.conf" #vi /etc/syslog.conf * CentOS 6.x
 : 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) SYSLOG #ps -ef | grep syslogd root 7524 6970 0 Apr 23 - 0:02
 /usr/sbin/syslogd #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%AC?rev=1641520098

Last update: 2022/01/07 01:48

