Варианты реализации журналирования процессов в службах на примере clamd

```
[hostX:~] # rcsdiff /usr/local/etc/clamd.conf
14c14
< LogFile /var/log/clamav/clamd.log
>
# LogFile /var/log/clamav/clamd.log
43c43
< #LogSyslog yes
>
LogSyslog yes
48c48
< #LogFacility LOG_MAIL
>
LogFacility LOG_LOCAL6
[hostX:~] # /usr/local/etc/rc.d/clamavclamd
reload
```

Пример использования syslogd

```
man syslog.conf
[hostX:~] # shutdown p
17:30
[hostX:~] # logger t
clamd p
kern.emerg 'Kernel Panic'
[hostX:~] # cat syslog.conf
...
local6.* /var/log/clamd.log
...
[hostX:~] # touch /var/log/clamd.log
[hostX:~] # /etc/rc.d/syslogd reload
[hostX:~] # clamdscan virus.zip
```

Ротация файлов регистрации

```
[hostX:~] # cat /etc/newsyslog.conf
...
/var/log/clamd.log 600 7 10 * J
[hostX:~] # cat logger.sh
while :
66
do
logger t
clamd p
local7.info "Message 1"
logger t
clamd p
```

local7.info "Message 2"
done
[hostX:~] # sh logger.sh
...
<Ctrl>C
[hostX:~] # tail f
/var/log/clamd.log
...
<Ctrl>C
[hostX:~] # newsyslog
[hostX:~] # ls l
/var/log/clamd.log*
Использование syslogd в сети
Настройка сервера
[hostX:~] # cat /etc/rc.conf
...
syslogd_flags="a
192.168.X.0/24"
Сокращенная форма 192.168.X/24 не распознается!
[hostX:~] # /etc/rc.d/syslogd restart
Настройка клиента
[gate:~] # cat /etc/syslog.conf
. @hostX
...
[gate:~] # /etc/rc.d/syslogd restart
Передача сообщений syslogd в программу
[hostX:~] # cat syslog.sh
#!/bin/sh
while read m
do
if expr "$m" : '.*login.*' > /dev/null
then
echo $m | mail s
login root
fi
done
67
[hostX:~] # chmod +x syslog.sh
[hostX:~] # cat /etc/syslog.conf
...
auth.* | /root/syslog.sh
...
68