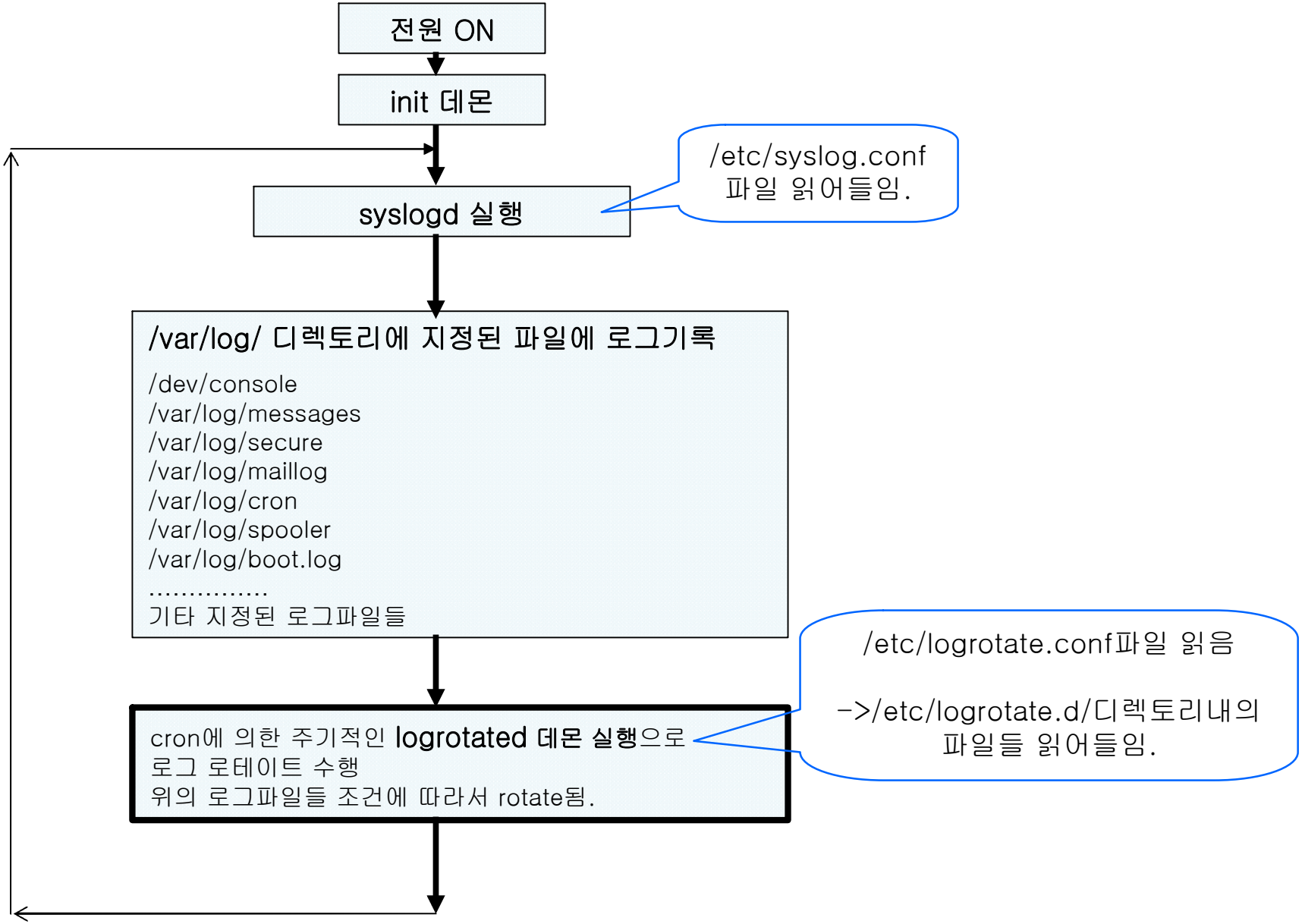
# 로그시스템의 이해와 활용

1. 리눅스 로그시스템 흐름도
2. 로그파일의 종류와 내용
3. /etc/syslog.conf 파일의 예
4. /etc/syslog.conf 파일의 이해와 활용
5. syslogd와 klogd의 시작과 종료
6. 로그파일의 로테이트를 위한 logrotated
7. 로테이트된 로그파일들의 실제 예
8. logrotated 관련 파일들
9. logrotated 설정파일의 이해와 활용
10. 활용1 : 중요로그기록 이중저장
11. 활용2 : 중요로그파일 원격실시간 저장

본 자료는 강좌의 간단한 참고자료용입니다. 강좌의 실제내용은 강좌를 직접 보시기 바랍니다.

# 리눅스 로그시스템 흐름도



# 로그파일의 종류와 내용

| 로그파일 종류 | 관련데몬 | 의미와 내용 |
|---|---|---|
| /dev/console | kernel | 콘솔에 뿌려지는 메시지들(콘솔로그) |
| /var/log/messages | 거의 모든 데몬 | 시스템로그파일 |
| /var/log/secure | xinetd | 보안인증에 관한 메시지 로그파일. tcpd로그파일(xinetd) |
| /var/log/maillog | sendmail,pop등 | 메일로그파일(메일관련로그데몬에 의해 기록됨) |
| /var/log/cron | crond | 크론로그파일로서 crond에 의해 기록되는 파일 |
| /var/log/xferlog | proftpd, vsftpd | ftp로그파일, ftp데몬에 의해서 기록되는 로그파일 |
| /var/log/dmesg | kernel | 부팅될 당시에 각종 메시지들을 저장하고 있는 로그파일<br>즉, 부팅시의 로그파일을 부팅후에 확인하고자 할 때사용. |
| /var/log/wtmp<br>/var/log/utmp | | 시스템에 로그인 기록이 저장되는 파일.<br>wtmp는 전체 로그인기록을 하는 파일.<br>utmp는 현재 로그인사용자에 대한 기록하는 파일. |
| /var/log/lastlog | | 각계정들의 가장 최근로그인기록을 하는 파일. |
| 기타 로그파일들 | ㅇ 관련데몬은 반드시 그런 것은 아님.<br>ㅇ syslogd데몬에 의해 각 로그파일의 기록내용이 달라질 수 있음.<br>ㅇ 즉, **로그파일**과 **관련데몬**, 그리고 **기록내용**은 /etc/syslog.conf파일의 설정내용에 따라서 달라질 수 있음. | |

# /etc/syslog.conf 파일의 예

```
[root@edu /]# cat /etc/syslog.conf
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                                 /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none                /var/log/messages

# The authpriv file has restricted access.
authpriv.*                                              /var/log/secure

# Log all the mail messages in one place.
mail.*                                                  /var/log/maillog


# Log cron stuff
cron.*                                                  /var/log/cron

# Everybody gets emergency messages
*.emerg                                                 *

# Save news errors of level crit and higher in a special file.
uucp,news.crit                                          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                                /var/log/boot.log
[root@edu /]#
```

# /etc/syslog.conf 파일의 이해와 활용

○ /etc/syslog.conf파일의 각행의 형식(포맷)

```
서비스종류.우선순위;서비스종류.우선순위;서비스종류.우선순위        로그파일위치
```

○ 각행의 의미

서비스종류(데몬)에 대하여 우선순위의 상황이 발생하면 로그파일위치의 파일에 그 내용을 기록한다.

○ 규 칙

- 서비스종류는 facility, 우선순위는 priority, 로그파일위치는 logfile-location을 각각 의미함.
- 서비스종류와 우선순위는 .(점)으로 구분함.
- "서비스종류.우선순위" 그리고 "서비스종류.우선순위" 사이에는 ;(세미콜론)으로 구분함.
- 서비스종류에는 mail, cron, kern, uucp등과 같은 해당 서비스의 종류를 의미함.
- 우선순위에는 지정된 서비스종류의 상황정도를 의미 함.(다음페이지 참조)
- 로그파일위치는 서비스종류와 우선순위에 의해서 발생되는 로그가 기록될 파일의 위치를 의미함.
- 서비스종류 자리에 *가 설정되면 모든 서비스를 의미함.
- 우선순위 자리에 *가 설정되면 모든 우선순위(상황)을 의미함.
- 로그파일위치 자리에 *가 설정되면 모든 로그파일을 의미함.

# /etc/syslog.conf 파일의 이해와 활용

○ 서비스종류(facility,데몬종류)

해당 로그파일에 기록할 서비스의종류, 즉, 데몬종류를 의미함.

| 서비스 종류 | 설 명 |
|---|---|
| auth | 로그인과 같이 사용자 인증에 관한 메시지 |
| authpriv | 보안 및 승인에 관한 메시지 |
| cron | crond데몬과 atd데몬에 의해 발생되는 메시지 |
| daemon | telnet, ftp등과 같은 데몬에 의한 메시지 |
| kern | kernel에 의한 메시지로서 커널메시지라고함 |
| lpr | 프린터데몬인 lpd에 의해 발생되는 메시지 |
| mail | sendmail, pop, qmail등과 같은 메일 관련 메시지 |
| news | innd등과 같은 뉴스시스템에 의해 발생되는 메시지 |
| uucp | uucp에 의한 시스템에 의한 메시지 |
| * | 모든 서비스에 의해 발생되는 메시지 |

# /etc/syslog.conf 파일의 이해와 활용

ㅇ 우선순위 (priority, 상황정도)

- 지정한 서비스의 종류에 대한 우선순위(상황정도)를 의미함.

| 우선순위(상황정도) | | 설 명 |
|---|---|---|
| 9 | * | 모든상황의 메시지(all) |
| 8 | debug | debugging에 관한 메시지(가장 낮은 단계) |
| 7 | info | 단순한 프로그램에 대한 정보 메시지(information) |
| 6 | notice | 에러가 아닌 알림에 대한 메시지 |
| 5 | warn | 주의를 요하는 메시지(warning) |
| 4 | err | 에러로 인한 메시지(error) |
| 3 | crit | 급한상황은 아니지만 치명적인 시스템 문제 발생 메시지(critical) |
| 2 | alert | 즉각적인 조치를 해야하는 메시지 |
| 1 | emerg | 매우 위험한 상황의 메시지(가장 높은 단계, emergency) |
| 0 | none | 해당사항없음. 메시지없음.(기록될 내용이 없음) |

- 주의사항

. 각 우선순위들은 포함관계를 나타냄. (매주 중요함.)
예) 9단계인 *는 모든 메시지를 의미함.(1부터 9까지의 모든 상황을 포함됨.)
8단계인 debug는 1부터 8까지의 상황을 모두 포함함.)

# syslogd와 klogd의 시작과 종료

○ syslogd 데몬과 klogd 데몬 실행확인

```
[root@edu log]# ps -ef | grep syslogd
root      3070     1  0 15:37 ?        00:00:00 syslogd -m 0
root      3078  1977  0 15:38 pts/0    00:00:00 grep syslogd
[root@edu log]#
[root@edu log]# ps -ef | grep klogd
root      3072     1  0 15:37 ?        00:00:00 klogd -x
root      3080  1977  0 15:38 pts/0    00:00:00 grep klogd
[root@edu log]#
```

○ syslogd 서비스의 시작 : /etc/rc.d/init.d/syslog start

```
[root@edu log]# /etc/rc.d/init.d/syslog start
Starting system logger: [  OK  ]
Starting kernel logger: [  OK  ]
[root@edu log]#
```

○ syslogd 서비스의 종료 : /etc/rc.d/init.d/syslog stop

```
[root@edu log]# /etc/rc.d/init.d/syslog stop
Shutting down kernel logger: [  OK  ]
Shutting down system logger: [  OK  ]
[root@edu log]#
```

○ syslogd 서비스의 재시작 : /etc/rc.d/init.d/syslog restart

```
[root@edu log]# /etc/rc.d/init.d/syslog restart
Shutting down kernel logger: [  OK  ]
Shutting down system logger: [  OK  ]
Starting system logger: [  OK  ]
Starting kernel logger: [  OK  ]
[root@edu log]#
```

# 로그파일의 로테이트를 위한 logrotated

○ 로그자동관리를 위한 로테이트 처리

- crond에 의해서 주기적으로 실행되는 logrotated 데몬에 의해 수행됨.
- 로테이트(rotate)작업내용
  . 로그파일 자르기(rotate), 보관하고, 삭제하고, 압축하고, 메일로 보내기등.
- 단, 해당 조건체크의 실행은 crond에 의해 주기적으로 자동실행되지만,
  . 로테이트작업이 발생하기 위해서는 해당 조건에 해당되어야 함.
  . 해당조건은 /etc/logrotate.conf파일과 /etc/logrotate.d/ 디렉토리내에 있는 파일들에서 설정.

○ 로테이트(rotate) 처리

- 특정날짜 또는 특정용량이상이 되었을 때 로그파일을 로테이트(교체)한다.(size)
- 로테이트작업 직전과 직후에 특정작업을 수행할 수 있다.(prerotate/endscript,postrotate/endscript)
- 로테이트 작업을 하면서 압축을 하거나 하지않을 수 있다.(compress, nocompress)
- 로테이트 후에 보관할 파일의 수를 지정할 수 있다.(rotate)
- 로테이트 후에 생성되는 파일의 소유주와 퍼미션등을 설정할 수 있다.(create)
- 로테이트 후에 생성되는 파일의 확장자 임의로 지정할 수 있다.(extension)

# 로테이트된 로그파일의 실제 예

```
[root@edu]# ls -l /var/log/
합계 45620
-rw-------  1 root root      275  2월 14 11:40 boot.log
-rw-------  1 root root      324  2월 11 10:09 boot.log.1
-rw-------  1 root root      269  2월  3 09:43 boot.log.2
-rw-------  1 root root      721  1월 27 16:03 boot.log.3
-rw-------  1 root root     1046  1월 20 20:15 boot.log.4
-rw-------  1 root root   179056  2월 14 22:40 cron
-rw-------  1 root root   451656  2월 12 04:02 cron.1
-rw-------  1 root root   451951  2월  5 04:02 cron.2
-rw-------  1 root root   451647  1월 29 04:02 cron.3
-rw-------  1 root root   451656  1월 22 04:02 cron.4
-rw-r--r--  1 root root    15922 12월 12 22:05 dmesg
-r--------  1 root root 19136220  2월 14 22:40 lastlog
-rw-------  1 root root  1818881  2월 14 22:39 maillog
-rw-------  1 root root  4950358  2월 12 04:02 maillog.1
-rw-------  1 root root  4716323  2월  5 04:02 maillog.2
-rw-------  1 root root  5114028  1월 29 04:02 maillog.3
-rw-------  1 root root  5058371  1월 22 04:02 maillog.4
-rw-------  1 root root   517495  2월 14 22:40 messages
-rw-------  1 root root   998580  2월 10 15:52 messages.1
-rw-------  1 root root  1653245  2월  5 04:00 messages.2
-rw-------  1 root root  1276373  1월 29 04:00 messages.3
-rw-------  1 root root  1602436  1월 22 04:00 messages.4
-rw-------  1 root root    81232  2월 14 22:40 secure
-rw-------  1 root root   208676  2월 12 04:00 secure.1
-rw-------  1 root root   435757  2월  5 04:00 secure.2
-rw-------  1 root root   229603  1월 29 04:00 secure.3
-rw-------  1 root root   230319  1월 22 04:00 secure.4
-rw-rw-r--  1 root utmp  2136960  2월 14 22:40 wtmp
-rw-r--r--  1 root root  8569951  2월 14 22:35 xferlog
[mons@su020.suidc.com ~]$
```

# logrotated 관련 파일들

| 구 분 | 위치 및 실행방법 | 설 명 |
|---|---|---|
| logrotated데몬 | /usr/sbin/logrotate | logrotated 데몬파일 |
| logrotated 주로그 파일 | /etc/logrotate.conf | logrotated의 주된 설정파일<br>개별 설정파일들에는 이 파일의 설정파일의 내용이 global하게 적용됨. |
| 개별 설정파일 | /etc/logrotate.d/* | 개별 설정파일들의 저장 위치<br>/etc/logrotate.conf파일에서 불러들임. |
| cron 실행 | /etc/cron.daily/logrotate | crond 데몬에 의해/etc/cron.daily/logrotate 파일을 실행함.<br>이 파일의 실행으로 logrotated 데몬이 주기적(1일 1회, 주로 새벽 4시)으로 실행됨. |
| 상황파일 | /var/lib/logrotate.status | logrotate한 작업내역을 보관한 파일 |

- /etc/logrotate.conf파일은 logrotated데몬의 주 설정파일로서 global하게 적용되는 파일임.
- /etc/logrotate.d/ 디렉토리내에 존재하는 파일들은 개별 로그파일의 개별 logrotate설정파일
- /etc/logrotate.d/ 디렉토리내에 로그파일에 대한 추가파일을 설정해 두면 그 로그파일을 로테이트(rotate)처리를 할 수 있음.

# logrotated 설정파일의 이해와 활용

○ /etc/logrotate.conf 파일의 예

```
[root@fileserver1 /]# cat /etc/logrotate.conf

weekly
rotate 4
create 0600 root root

include /etc/logrotate.d

/var/log/wtmp {
    monthly
    create 0664 root utmp
    rotate 1
}
```

- logrotated 데몬이 실행되면서 /etc/logrotate.conf파일을 읽어들여서 그 내용을 적용함.

- 위의 “include /etc/logrotate.d” 설정으로 인하여 /etc/logrotate.d 디렉토리에 존재하는 개별로그파일들을 모두 읽어들여 적용함.

# logrotated 설정파일의 이해와 활용

○ /etc/logrotate.d/ 디렉토리내의 파일의 예

```
[root@fileserver1 /]# cat /etc/logrotate.d/syslog
/var/log/messages /var/log/secure /var/log/maillog /var/log/spooler /var/log/boot.log /var/log/cron
{
monthly
compress
rotate 4
mail  admin@superuser.co.kr
errors admin@superuser.co.kr
postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
endscript
}
[root@fileserver1 /]#
```

# logrotated 설정파일의 이해와 활용

- daily
  해당 로그파일을 매일 로테이트 함.

- weekly
  해당 로그파일을 매주 로테이트 함.

- monthly
  해당 로그파일을 매월 로테이트 함.

- rotate 숫자
  현재 로그파일을 제외한 숫자만큼까지의 로테이트된 파일을 보관함. 이전 로테이트된 파일은 삭제함.
  예) “rotate 2”일 경우 해당로그파일이 secure라면
  secure 파일(현재파일)과 secure.1파일, secure.2파일까지만 보관됨. 그 이전파일은 자동삭제.

- compress
  순환된 로그파일이 gzip에 의해 압축됨. 예) messages.1.gz, secure.1.gz

- nocompress
  순환된 로그파일이 압축되지 않고 원본상태로 저장됨. 예) messages.1, secure.1

- create 퍼미션 소유자 소유그룹
  순환된 로그파일이 지정된 퍼미션을 가지고, 지정된 소유자와 소유그룹으로 생성됨.
  예) create 600 root wheel

# logrotated 설정파일의 이해와 활용

- errors 메일주소
  로테이트 실행시 문제(에러)가 발생하면 관련 내용을 지정된 메일주소로 메일 발송함.

- mail 메일주소
  로테이트된 후에 삭제되는 로테이트된 파일들을 지정한 메일주소로 보내게 됨.

- extension 확장자명
  로테이트된 파일뒤에 지정된 확장자명을 붙여주게 됨. (로테이트파일의 개별 구분을 위한 것)
  예) “extension kkk”라고 설정되었다면 messages.1.kkk, 또는 messages.1.ext.gz로 생성됨.

- ifempty
  로테이트하고자 하는 원본파일의 용량이 0이라 하더라도 로테이트 시킴.(기본값)

- notifempty
  로테이트하고자 하는 원본파일의 용량이 0이라면 로테이트하지 않음.

- prerotate/endscript
  로테이트를 수행하기 이전에 prerotate와 endscript 사이의 내용을 실행함.

- postrotate/endscript
  로테이트를 수행한 후에 postrotate와 endscript 사이의 내용을 실행함.
  거의 대부분 syslogd 데몬을 재시작하기 위한 것임.

- size 용량크기
  로테이트의 수행결과 로테이트된 파일의 크기가 지정한 용량크기 이상을 넘지 않도록 함.
  예) size 200K, size 1024M

# 활용1 : 중요로그기록 이중저장

○ 시스템로그파일(messages)들 중요한 기록들을 별도 위치에 이중저장 한다.

**1단계** : 별도로 저장 파일명과 저장위치를 결정하고 디렉토리를 생성한다.

예) /var/tmp/..hidden/..messages
/var/tmp/..hidden/..secure

```
[root@edu /]# mkdir /var/tmp/..hidden
```

**2단계** : /etc/syslog.conf 파일의 내용을 수정한다.

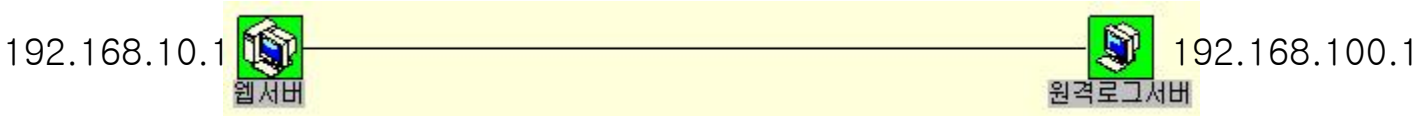
```
*.info;mail.none;authpriv.none;cron.none        /var/log/messages
*.info;mail.none;authpriv.none;cron.none        /var/tmp/..hidden/..messages

authpriv.*                                      /var/log/secure
authpriv.*                                      /var/tmp/..hidden/..secure
```

**3단계** : syslogd 데몬을 재시작한다.

```
[root@edu /]# /etc/rc.d/init.d/syslog restart
Shutting down kernel logger: [  OK  ]
Shutting down system logger: [  OK  ]
Starting system logger: [  OK  ]
Starting kernel logger: [  OK  ]
[root@edu /]#
```

**4단계** : /var/tmp/..hidden/디렉토리에 ..messages파일과 ..secure파일이 생성되어 해당 로그가 기록되고 있는가를 확인한다.

# 활용2 : 중요로그파일 원격실시간 저장




ㅇ 웹서버 설정내용

- 작업1 : 원격로그서버에 대한 호스트 설정 : /etc/hosts 설정

  192.168.100.1 logserver

- 작업2 : syslog.conf파일 수정 : /etc/syslog.conf 설정

  *.info;mail.none;authpriv.none;cron.none /var/log/messages
  *.info;mail.none;authpriv.none;cron.none @logserver
  authpriv.* /var/log/secure
  authpriv.* @logserver

- 작업3 : syslogd 데몬 재시작 : /etc/rc.d/init.d/syslog restart

ㅇ 원격로그서버 설정내용

- 작업1 : 웹서버에 대한 호스트 설정 : /etc/hosts 설정

  192.168.10.1 webserver

- 작업2 : 원격에서 들어오는 로그메시지를 저장할 수 있도록 syslogd 데몬 재시작
  방법1 : /sbin/syslogd –r –m 0
  방법2 : /etc/sysconfig/syslog 파일내에 설정된 SYSLOGD_OPTIONS="-m 0"을
  SYSLOGD_OPTIONS="-r –m 0"로 변경한다.

- 확인작업 : 로그파일에 웹서버의 로그내용이 실시간으로 저장되고 있는가를 확인한다.