

Esercitazione a supporto della lezione del 20-aprile-2007 (Corso Docenti)

1- Loggarsi come root sul proprio computer. Trovare la posizione del file messages, che contiene il log dei principali eventi del sistema.

```
nemorino60@valentino:~$ su -  
Password:  
valentino:~# updatedb  
valentino:~# locate messages
```

escludendo la "home" i messaggi a video sono assimilabili a questi:

```
/usr/include/c++/4.1.2/i486-linux-gnu/64/bits/messages_members.h  
/usr/include/c++/4.1.2/i486-linux-gnu/bits/messages_members.h  
/usr/include/glib-2.0/glib/gmessages.h  
/usr/include/kde/kxmessages.h  
/usr/share/djvu/osi/de/messages.xml  
/usr/share/djvu/osi/en/messages.xml  
/usr/share/djvu/osi/fr/messages.xml  
/usr/share/djvu/osi/ja/messages.xml  
/usr/share/djvu/osi/zh/messages.xml  
/var/log/messages  
/var/log/messages.0  
/var/log/messages.1.gz
```

l'unico file che presenta unicamente i caratteri della stringa "messages" è il file:

```
/var/log/messages
```

il file si trova in /var/log

2- Creare una nuova directory chiamata test in /tmp/. Copiare il file messages nella nuova directory /tmp/test.

```
valentino:~# mkdir /tmp/test  
valentino:~# cp /var/log/messages /tmp/test
```

verifico che il file copia si trovi effettivamente nella directory destinazione - uso il parametro "-l" per evidenziare più informazioni:

```
valentino:~# ls -l /tmp/test  
totale 108  
-rw-r----- 1 root root 103386 2007-05-11 16:38 messages
```

3- Provare a visualizzare, in modalità continua, le ultime righe di /tmp/test/messages. Provare a loggarsi su altre console del sistema per vedere se il file cambia.

Per visualizzare il file messages utilizzo il comando tail:

```
valentino:~# tail /tmp/test/messages
```

```
May 12 07:22:15 valentino kernel: Vendor: ChipsBnk Model: Flash Disk Rev: 2.00  
May 12 07:22:15 valentino kernel: Type: Direct-Access ANSI  
SCSI revision: 02  
May 12 07:22:15 valentino kernel: SCSI device sda: 516352 512-byte hdwr sectors (264 MB)  
May 12 07:22:15 valentino kernel: sda: Write Protect is off  
May 12 07:22:15 valentino kernel: SCSI device sda: 516352 512-byte hdwr sectors (264 MB)  
May 12 07:22:15 valentino kernel: sda: Write Protect is off
```

```
May 12 07:22:15 valentino kernel: sda: sda1
May 12 07:22:15 valentino kernel: sd 0:0:0:0: Attached scsi removable disk sda
May 12 07:38:03 valentino syslogd 1.4.1#20: restart.
May 12 08:00:30 valentino -- MARK --
```

Utilizzando altre console come root il file non cambia.
Ma con il comando exit esco da root e torno ad essere utente nemorino60:

```
valentino:~# exit
logout
nemorino60@valentino:~$ tail /tmp/test/messages
tail: impossibile aprire `/tmp/test/messages' per la lettura: Permission denied
```

Come utente nemorino60 non ho i diritti di accesso al file riservato esclusivamente a root!

4- Rimuovere il file /tmp/test/messages. Creare un link simbolico fra il messages nella posizione originaria e /tmp/test/messages

Come root:

```
valentino:~# rm /tmp/test/messages
valentino:~# ln -s /var/log/messages /tmp/test/messages
valentino:~# ls -l /tmp/test
totale 0
lrwxrwxrwx 1 root root 17 2007-05-12 08:03 messages -> /var/log/messages
```

5- Provare a visualizzare, in modalità continua, le ultime righe di /tmp/test/messages. Provare a loggarsi su altre console del sistema per vedere se il file cambia.

```
valentino:~# tail /tmp/test/messages
May 12 07:22:15 valentino kernel: Vendor: ChipsBnk Model: Flash Disk Rev: 2.00
May 12 07:22:15 valentino kernel: Type: Direct-Access ANSI
SCSI revision: 02
May 12 07:22:15 valentino kernel: SCSI device sda: 516352 512-byte hdwr sectors (264 MB)
May 12 07:22:15 valentino kernel: sda: Write Protect is off
May 12 07:22:15 valentino kernel: SCSI device sda: 516352 512-byte hdwr sectors (264 MB)
May 12 07:22:15 valentino kernel: sda: Write Protect is off
May 12 07:22:15 valentino kernel: sda: sda1
May 12 07:22:15 valentino kernel: sd 0:0:0:0: Attached scsi removable disk sda
May 12 07:38:03 valentino syslogd 1.4.1#20: restart.
May 12 08:00:30 valentino -- MARK --
```

Il link simbolico mi ha permesso di visualizzare le ultime righe del file messages lo stesso risultato che avremmo avuto con il comando:

```
valentino:~# tail /var/log/messages
```

Tutti i comandi rivolti al link simbolico operano sul file "puntato" dal link!!!

Torno come utente nemorino60 ed eseguo lo stesso comando:

```
valentino:~# exit
logout
nemorino60@valentino:~$ tail /tmp/test/messages
tail: impossibile aprire `/tmp/test/messages' per la lettura: Permission denied
```

Ottingo lo stesso risultato ottenuto al punto 3.

6- Spiegare perchè i comportamenti sono diversi nei punti 3 e 5.

Per nemorino60 l'accesso al file è negato perchè il proprietario esclusivo è root (e gruppo: adm) come si vede:

```
nemorino60@valentino:~$ su -  
Password:  
valentino:~# ls -l /var/log/messages  
-rw-r----- 1 root adm 135232 2007-05-12 08:20 /var/log/messages
```

7- Visualizzare i permessi del file messages originario. Provare ad entrare sul sistema come utente normale. Provare a visualizzare il contenuto del messages originario.

come si vede:

```
nemorino60@valentino:~$ su -  
Password:  
valentino:~# ls -l /var/log/messages  
-rw-r----- 1 root adm 135232 2007-05-12 08:20 /var/log/messages
```

8- Si riesce a visualizzarlo? Spiegare perchè.

E' sufficiente osservare che la maschera "-rw-r-----" associata al file indica che i primi tre simboli riservati al proprietario sono rw- (l=read lettura e w=write scrittura) riservati a root. Il simbolo "-" indica che non essendoci il carattere x (execute) il file non è eseguibile per root. La presenza dei simboli "r--" per "gruppo" significa che come gruppo adm il file è accessibile in lettura mentre i simboli "---" indicano che il file non è accessibile per gli altri utenti.

9- Dalla shell aperta come root rendere leggibile a tutti gli utenti il file messages originario. Passare alla shell aperta come utente normale e visualizzarne il contenuto.

Cambiando i permessi di accesso ai file (e solo root lo può fare) la situazione cambia e anche l'utente nemorino60 può visualizzare il contenuto del file.

```
valentino:~# chmod +r /var/log/messages  
valentino:~# ls -l /var/log/messages  
-rw-r--r-- 1 root adm 137381 2007-05-12 08:33 /var/log/messages
```

come si vede la maschera riservata agli altri utenti è cambiata in "r--", esco da root e visualizzo la coda del file messages originale

```
valentino:~# exit  
logout  
nemorino60@valentino:~$ tail /var/log/messages
```

```
May 12 08:33:34 valentino gconfd (root-5396): L'indirizzo "xml:readonly:/var/lib/gconf/defaults" è stato risolto ad una sorgente di configurazione in sola lettura in posizione 4  
May 12 08:33:34 valentino gconfd (root-5396): Il server GConf non è utilizzato, arresto  
May 12 08:33:34 valentino gconfd (root-5396): Uscita
```

Nel frattempo si sono aggiunte delle righe di LOG perchè il sistema ha notificato alcune operazioni ma in sostanza l'utente nemorino60 riesce a leggerne il contenuto.

10- Reimpostare i permessi precedenti sul file messages (contenente riservate informazioni sul sistema che non tutti gli utenti devono vedere).

Potremmo usare il comando "chmod -r /var/log/messages" ma ciò toglierebbe TUTTI i

permessi di lettura. In realtà dobbiamo agire solo sui permessi di "altri utenti" quindi useremo la numerazione:

```
valentino:~# chmod 640 /var/log/messages
valentino:~# ls -l /var/log/messages
-rw-r----- 1 root adm 137418 2007-05-12 09:00 /var/log/messages
```

"-rw-r-----" = 640 si traduce in:
6 = 4+2+0 cioè 4="r" 2="w" e 0="-" per l'utente proprietario root
4 = 4+0+0 cioè 4="r" 0="-" e 0="-" per il gruppo proprietario adm
0 = 0+0+0 cioè 0="-" 0="-" e 0="-" per il resto degli utenti

se avessimo usato il comando "chmod -r /var/log/messages" avremmo ottenuto il risultato seguente:

```
valentino:~# chmod -r /var/log/messages
valentino:~# ls -l /var/log/messages
--w----- 1 root adm 137381 2007-05-12 08:33 /var/log/messages
```

l'equivalente di "chmod 200 /var/log/messages" secondo il seguente schema:

"--w-----" = 200 si traduce in:
2 = 0+2+0 cioè 0="-" 2="w" e 0="-" per l'utente proprietario root
0 = 0+0+0 cioè 0="-" 0="-" e 0="-" per il gruppo proprietario adm
0 = 0+0+0 cioè 0="-" 0="-" e 0="-" per il resto degli utenti

11- Copiare il messages originario in /tmp/test/messages2

```
valentino:~# cp /var/log/messages /tmp/test/messages2
```

12- Visualizzare le righe di /tmp/test/messages2 che contengono la parola root

uso il filtro grep per estrarre solo le righe che contengono la parola root:

```
valentino:~# cat /tmp/test/messages2 | grep "root"
```

13- Cancellare la directory /tmp/test/ e il relativo contenuto.

uso il parametro -R (recursive) del comando rm:

```
valentino:~# rm -R /tmp/test
```

```
-----
valentino.stampone@gmail.com
http://www.valentino.stampone.name
-----
```