# Esplorazione dei Filesystem in Linux

Questa parte dell'attività ha approfondito la gestione e il montaggio dei filesystem nel sistema operativo Linux, in particolare utilizzando il filesystem ext4. L'obiettivo principale è stato esplorare come Linux riconosce e gestisce le unità di memoria.

1. **Avvio del Terminale e Visualizzazione dei Filesystem Montati**: Dopo aver avviato il terminale sulla VM CyberOps Workstation, è stato utilizzato il comando lsblk per elencare i dispositivi di blocco presenti. Il risultato ha mostrato tre dispositivi: sda, sdb e sr0, dove sda e sdb sono dischi rigidi, ognuno con una singola partizione (sda1 e sdb1 rispettivamente). Si è quindi usato il comando mount per visualizzare i dettagli sui filesystem montati, con particolare attenzione al filesystem radice (/), montato su /dev/sda1 e formattato in ext4.
2. **Montaggio Manuale e Smontaggio di Filesystem**: È stato montato manualmente il filesystem /dev/sdb1 sulla directory second_drive nella home dell'utente. Utilizzando mount, è stato confermato che /dev/sdb1 fosse correttamente montato. Successivamente, è stato utilizzato il comando umount per smontare il filesystem, riportando la directory second_drive al suo stato iniziale.

## Part 2: Permessi sui File

Nella seconda parte dell'attività, è stata esplorata la gestione dei permessi sui file, che in Linux vengono rappresentati da un set di definizioni che specificano cosa possono fare gli utenti e i gruppi con un determinato file.

1. **Visualizzazione dei Permessi sui File**: Dopo essersi spostati nella directory /home/analyst/lab.support.files/scripts/, è stato utilizzato ls -l per elencare i file presenti e i relativi permessi. Ad esempio, per il file cyops.mn, i permessi erano -rw-r--r--, indicando che l'utente proprietario analyst può leggere e scrivere sul file, mentre altri utenti possono solo leggerlo.
2. **Creazione di File e Permessi delle Directory**: È stato tentato di creare un file vuoto nella directory /mnt utilizzando touch, ma l'operazione è fallita a causa dei permessi della directory, posseduta dall'utente root. Per eseguire correttamente l'operazione, è stato necessario specificare i permessi di scrittura tramite sudo o modificare i permessi della directory /mnt.

In sintesi, questa attività ha fornito un'esperienza pratica su come Linux gestisce i filesystem e implementa i permessi, consentendo di comprendere meglio la sicurezza e la gestione dei file e delle directory nel sistema operativo Linux.

# Linux Filesystem e Settaggio Permessi

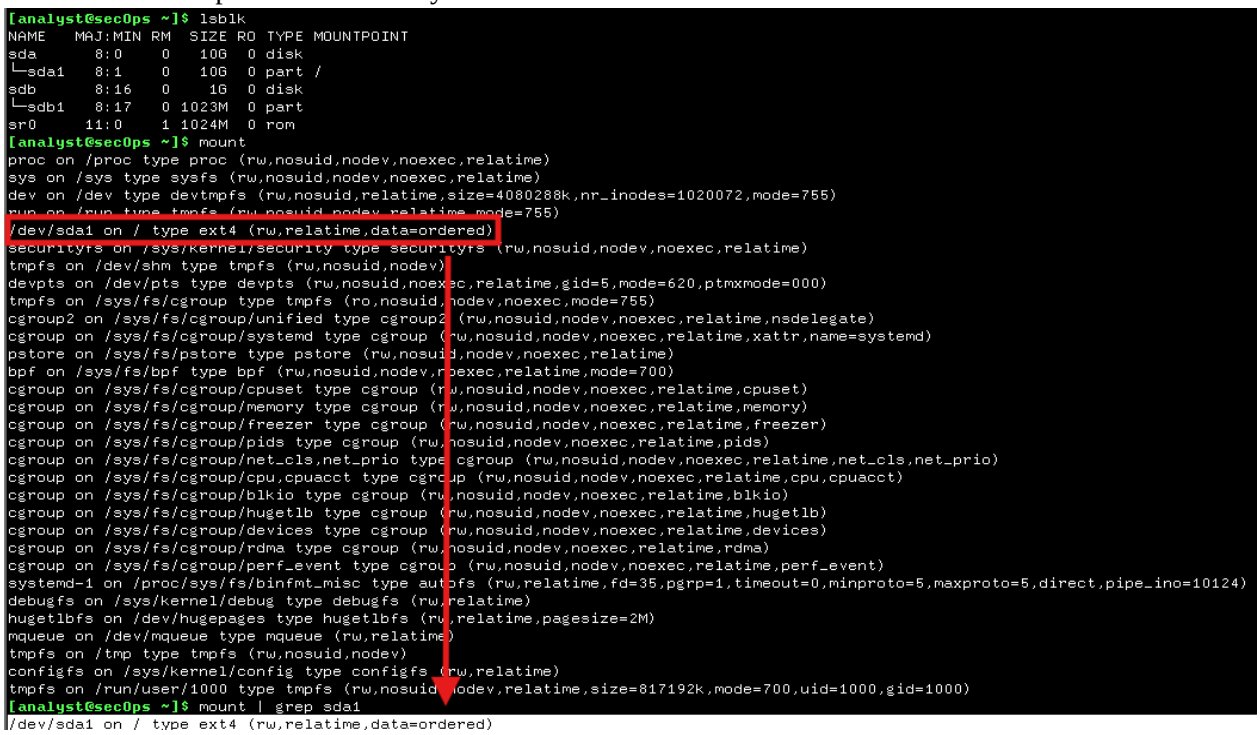
## Part 1: Exploring Filesystems in Linux

1. **Visualizza dispositivi a blocchi**

   Comando: lsblk mostra i dispositivi: sr0, sda (10GB) e sdb (1GB).

2. **Visualizza filesystem montati**

   Comando: mount per elencare i filesystem montati.



3. **Montaggio manuale di /dev/sdb1**

Creazione della directory second_drive in home/analyst, montaggio di /dev/sdb1.

```
[analyst@secOps ~]$ cd /
[analyst@secOps /]$ ls -l
total 52
lrwxrwxrwx   1 root root     7 Jan  5  2018 bin -> usr/bin
drwxr-xr-x   3 root root  4096 Apr 16  2018 boot
drwxr-xr-x  19 root root  3120 Oct 28 05:21 dev
drwxr-xr-x  58 root root  4096 Apr 17  2018 etc
drwxr-xr-x   3 root root  4096 Mar 20  2018 home
lrwxrwxrwx   1 root root     7 Jan  5  2018 lib -> usr/lib
lrwxrwxrwx   1 root root     7 Jan  5  2018 lib64 -> usr/lib
drwx------   2 root root 16384 Mar 20  2018 lost+found
drwxr-xr-x   2 root root  4096 Jan  5  2018 mnt
drwxr-xr-x   2 root root  4096 Jan  5  2018 opt
dr-xr-xr-x 143 root root     0 Oct 28 05:21 proc
drwxr-x---   7 root root  4096 Apr 17  2018 root
drwxr-xr-x  17 root root   480 Oct 28 05:21 run
lrwxrwxrwx   1 root root     7 Jan  5  2018 sbin -> usr/bin
drwxr-xr-x   6 root root  4096 Mar 24  2018 srv
dr-xr-xr-x  13 root root     0 Oct 28 05:21 sys
drwxrwxrwt   8 root root   200 Oct 28 05:21 tmp
drwxr-xr-x   9 root root  4096 Apr 17  2018 usr
drwxr-xr-x  12 root root  4096 Apr 17  2018 var
[analyst@secOps /]$ cd ~
[analyst@secOps ~]$ ls -l
total 16
drwxr-xr-x 2 analyst analyst 4096 Mar 22  2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 Mar 22  2018 Downloads
drwxr-xr-x 9 analyst analyst 4096 Jul 19  2018 lab.support.files
drwxr-xr-x 2 analyst analyst 4096 Mar 21  2018 second_drive
[analyst@secOps ~]$ ls -l second_drive/
total 0
[analyst@secOps ~]$ sudo mount /dev/sdb1 ~/second_drive/
[sudo] password for analyst:
[analyst@secOps ~]$ ls -l second_drive/
total 20
drwx------ 2 root    root    16384 Mar 26  2018 lost+found
-rw-r--r-- 1 analyst analyst   183 Mar 26  2018 myFile.txt
```

4. **Smontaggio del filesystem**

   Usa umount per smontare /dev/sdb1.

```
[analyst@secOps ~]$ sudo umount /dev/sdb1
```

**Part 2: File Permissions**

1. **Verifica e modifica permessi file**

   Comando: ls -l su cyops.mn per verificare i permessi (proprietario: analyst, gruppo: analyst, permessi -rw-r--r--).

```
[analyst@secOps ~]$ cd lab.support.files/scripts/
[analyst@secOps scripts]$ ls -l
total 60
-rwxr-xr-x 1 analyst analyst  952 Mar 21  2018 configure_as_dhcp.sh
-rwxr-xr-x 1 analyst analyst 1153 Mar 21  2018 configure_as_static.sh
-rwxr-xr-x 1 analyst analyst 3459 Mar 21  2018 cyberops_extended_topo_no_fw.py
-rwxr-xr-x 1 analyst analyst 4062 Mar 21  2018 cyberops_extended_topo.py
-rwxr-xr-x 1 analyst analyst 3669 Mar 21  2018 cyberops_topo.py
-rw-r--r-- 1 analyst analyst 2871 Mar 21  2018 cyops.mn
-rwxr-xr-x 1 analyst analyst  458 Mar 21  2018 fw_rules
-rwxr-xr-x 1 analyst analyst   70 Mar 21  2018 mal_server_start.sh
drwxr-xr-x 2 analyst analyst 4096 Mar 21  2018 net_configuration_files
-rwxr-xr-x 1 analyst analyst   65 Mar 21  2018 reg_server_start.sh
-rwxr-xr-x 1 analyst analyst  189 Mar 21  2018 start_ELK.sh
-rwxr-xr-x 1 analyst analyst   85 Mar 21  2018 start_miniedit.sh
-rwxr-xr-x 1 analyst analyst   76 Mar 21  2018 start_pox.sh
-rwxr-xr-x 1 analyst analyst  106 Mar 21  2018 start_snort.sh
-rwxr-xr-x 1 analyst analyst   61 Mar 21  2018 start_tftpd.sh
```

2. **Modifica dei permessi della directory /mnt**

   Il comando touch fallisce su /mnt perché possiede permessi limitati (drwxr-xr-x).

3. **Modifica permessi di myFile.txt**

   Comando: chmod 665 myFile.txt per settare i permessi a -rw-rw-r-x.

4. **Cambio del proprietario del file**

   Comando chown per cambiare il proprietario del file myFile.txt a root.

```
[analyst@secOps scripts]$ sudo mount /dev/sdb1 ~/second_drive/
[analyst@secOps scripts]$ cd ~/second_drive/
[analyst@secOps second_drive]$ ls -l
total 20
drwx------ 2 root    root    16384 Mar 26  2018 lost+found
-rw-r--r-- 1 analyst analyst   183 Mar 26  2018 myFile.txt
[analyst@secOps second_drive]$ sudo chmod 665 myFile.txt
[analyst@secOps second_drive]$ sudo chown analyst myFile.txt
[analyst@secOps second_drive]$ echo test >> myFile.txt
[analyst@secOps second_drive]$ cat myFile.txt
This is a file stored in the /dev/sdb1 disk.
```

**Part 3: Symbolic Links and other Special File Types**

1. **Esame dei tipi di file**

   Comando: ls -l in /home/analyst per visualizzare file (indicati da -) e directory (indicate da d).

2. **Creazione di symbolic e hard link**

   Comando ln -s per creare link simbolico a file1.txt, ln per link hard a file2.txt.

3. **Effetti sui link dopo rinomina dei file originali**

   Comando: rinomina file1.txt e file2.txt per osservare i cambiamenti. Il link simbolico file1symbolic si rompe, mentre il link hard file2hard rimane funzionante.