

PERMESSI LINUX

Il sistema operativo Linux, noto per la sua robustezza e sicurezza, utilizza un sistema di permessi per controllare l'accesso ai file e alle directory. Questo sistema consente di definire chi può leggere, scrivere ed eseguire un file, proteggendo così i dati da accessi non autorizzati o modifiche accidentali. I permessi in Linux sono organizzati in base a tre categorie di utenti: il proprietario, il gruppo e gli altri. La gestione dei permessi è cruciale per garantire l'integrità e la sicurezza dei sistemi, e rappresenta un aspetto fondamentale per ogni amministratore di sistema. In questa relazione, verranno esaminati i vari tipi di permessi, le modalità di visualizzazione e modifica, nonché l'importanza della loro configurazione corretta.

Tipi di permessi:

1. **Lettura (r - read):** Consente di leggere il contenuto del file o, nel caso di una directory, di elencarne il contenuto.
2. **Scrittura (w - write):** Consente di modificare il contenuto di un file o, nel caso di una directory, di aggiungere o rimuovere file al suo interno.
3. **Esecuzione (x - execute):** Consente di eseguire un file (se è un programma o uno script) o di accedere ai file all'interno di una directory.

Categorie di utenti:

1. **Proprietario (owner):** L'utente che ha creato il file o la directory, di solito il primo responsabile dei permessi.
2. **Gruppo (group):** Un gruppo di utenti che possono condividere certi permessi su un file o una directory.
3. **Altri (others):** Tutti gli altri utenti del sistema che non appartengono né al gruppo né sono il proprietario.

Esercizio:

Creazione di un File e di una Directory:

Ho aperto il terminale e ho creato un nuovo file chiamato **S10L2.txt** e una nuova directory chiamata **S10L2_dir**.

- Comando per la creazione del file=**touch S10L2.txt**

- Comando per la creazione della Directory=**mkdir S10L2_dir**

```
carmine@carmine: ~/Desktop
File Actions Edit View Help
zsh: corrupt history file /home/carmin/.zsh_history
(carmine@carmine)-[~/Desktop]
$ touch S10L2.txt

(carmine@carmine)-[~/Desktop]
$ mkdir S10L2_dir

(carmine@carmine)-[~/Desktop]
$
```

Verifica dei Permessi:

Ho controllato i permessi attuali del file e della directory con il comando **ls -l**.

- **ls -l S10L2.txt**
- **ls -l S10L2_dir**

```
(carmine@carmine)-[~/Desktop]
$ ls -l S10L2.txt
-rw-rw-r-- 1 carmine carmine 0 Dec  3 15:38 S10L2.txt

(carmine@carmine)-[~/Desktop]
$ ls -l S10L2_dir
total 0

(carmine@carmine)-[~/Desktop]
$
```

Modifica dei Permessi:

Ho impostato i permessi di lettura e scrittura per l'utente (**rw-**), e solo lettura per il gruppo e gli altri (**r--**) per il file. Per la directory, ho impostato i permessi di lettura, scrittura ed esecuzione per l'utente (**rwx**), e solo lettura ed esecuzione per il gruppo e gli altri (**r-x**).

- **chmod u=rw,g=r,o=r esempio.txt**
- **chmod u=rwx,g=rx,o=rx esempio_dir**

```
(carmine@carmine)-[~/Desktop]
$ chmod u=rw,g=r,o=r S10L2.txt

(carmine@carmine)-[~/Desktop]
$ chmod u=rwx,g=rx,o=rx S10L2_dir
```

Verifica dei nuovi permessi

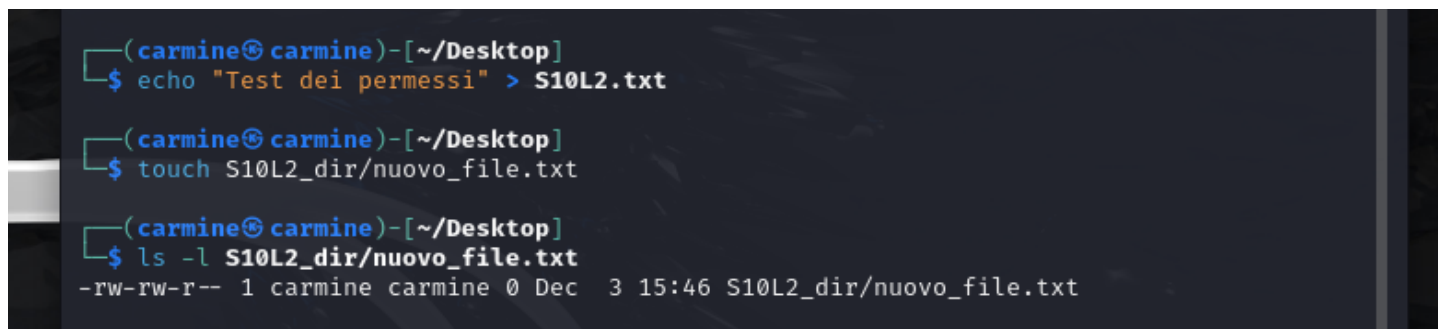
- **ls -l esempio.txt**
- **ls -l esempio_dir**

```
(carmine@carmine)-[~/Desktop]
$ ls -l S10L2.txt
-rw-r--r-- 1 carmine carmine 0 Dec  3 15:38 S10L2.txt

(carmine@carmine)-[~/Desktop]
$ ls -l S10L2_dir
total 0
```

Ho provato a scrivere nel file **S10L2.txt** e a creare un nuovo file all'interno della directory **S10L2_dir**.

- **echo "Test dei permessi" > L10S2.txt**
- **touch S10L2_dir/nuovo_file.txt**
- **ls -l S10L2_dir/nuovo_file.txt**



```
(carmine@carmine)~[~/Desktop]
$ echo "Test dei permessi" > S10L2.txt

(carmine@carmine)~[~/Desktop]
$ touch S10L2_dir/nuovo_file.txt

(carmine@carmine)~[~/Desktop]
$ ls -l S10L2_dir/nuovo_file.txt
-rw-rw-r-- 1 carmine carmine 0 Dec  3 15:46 S10L2_dir/nuovo_file.txt
```

Conclusioni

In conclusione, il sistema di permessi di Linux rappresenta una componente fondamentale nella gestione della sicurezza e dell'accesso ai file e alle directory. La possibilità di definire permessi distinti per il proprietario, il gruppo e gli altri utenti consente di avere un controllo granulare su chi può eseguire determinate operazioni sui file. La comprensione e la corretta configurazione di questi permessi sono essenziali per garantire la protezione dei dati e per prevenire accessi non autorizzati o modifiche accidentali.

La flessibilità offerta dai permessi, consente agli amministratori di sistema di personalizzare l'accesso in base alle necessità specifiche di ciascun utente o gruppo. Con l'uso dei permessi simbolici e numerici, è possibile applicare modifiche rapide e precise ai file e alle directory.

In un contesto di sicurezza informatica, la gestione appropriata dei permessi è cruciale, poiché consente di limitare l'accesso a file sensibili e di assicurare che solo gli utenti autorizzati possano modificarli o eseguirli. Pertanto, una buona conoscenza dei permessi di Linux è indispensabile per ogni amministratore di sistema e per chiunque desideri garantire l'integrità e la sicurezza del proprio ambiente di lavoro.