Cheatsheet 3: il comando `lsof`

Laboratorio di Reti e Sistemi Distribuiti @ UniME

February 26, 2025

1 Introduzione

Il comando `lsof` (List Open Files) è uno strumento potente su sistemi Unix e Linux che elenca i file aperti dai processi. Poiché in Unix/Linux "tutto è un file", `lsof` può mostrare non solo file regolari, ma anche directory, dispositivi, socket, pipe e altro ancora. Questo documento descrive i più comuni utilizzi di `lsof`, con particolare attenzione ai socket.

2 Sintassi di Base

La sintassi generale del comando `lsof` è:

```
lsof [opzioni] [nome]
```

Dove:

- `[opzioni]` sono i flag che modificano il comportamento del comando.
- `[nome]` è un file, directory, dispositivo o altro oggetto di cui si vogliono ottenere informazioni.

3 Utilizzi Comuni

3.1 Elencare tutti i file aperti

Per elencare tutti i file aperti sul sistema, si esegue:

```
lsof
```

Questo comando produce un output dettagliato che include:

- Il nome del processo (`COMMAND`).
- Il PID del processo (`PID`).
- L'utente che ha aperto il file (`USER`).
- Il tipo di file (`TYPE`).
- Il file aperto (`NAME`).

3.2 Filtrare per utente

Per elencare i file aperti da un utente specifico, si utilizza l'opzione `-u`:

```
lsof -u username
```

Ad esempio, per vedere i file aperti dall'utente `root`:

```
lsof -u root
```

3.3 Filtrare per processo

Per elencare i file aperti da un processo specifico, si utilizza l'opzione `-p` con il PID del processo:

```
lsof -p PID
```

Ad esempio, per vedere i file aperti dal processo con PID `1234`:

```
lsof -p 1234
```

3.4 Filtrare per file o directory

Per elencare i processi che hanno aperto un file o una directory specifica, si passa il percorso come argomento:

```
lsof /path/to/file
```

Ad esempio, per vedere chi ha aperto il file `/var/log/syslog`:

```
lsof /var/log/syslog
```

3.5 Elencare i file aperti su una porta di rete

Per trovare i processi che stanno utilizzando una specifica porta di rete, si utilizza l'opzione `-i`:

```
lsof -i :porta
```

Ad esempio, per vedere i processi che utilizzano la porta `80`:

```
lsof -i :80
```

3.6 Elencare i file aperti su un protocollo di rete

Si possono filtrare i file aperti per protocollo di rete (ad esempio, TCP o UDP) con l'opzione `-i`:

```
lsof -i TCP
```

Per vedere solo i file aperti su connessioni UDP:

```
lsof -i UDP
```

3.7 Elencare i file aperti da un comando specifico

Per elencare i file aperti da un comando specifico, si utilizza l'opzione `-c`:

```
lsof -c nome_comando
```

Ad esempio, per vedere i file aperti da `nginx`:

```
lsof -c nginx
```

3.8 Elencare i file aperti in una directory

Per elencare i file aperti in una directory specifica, si utilizza l'opzione `+D`:

```
lsof +D /path/to/directory
```

Ad esempio, per vedere i file aperti nella directory `/var/log`:

```
lsof +D /var/log
```

3.9 Elencare i file aperti da un filesystem specifico

Per elencare i file aperti su un filesystem specifico, si utilizza l'opzione `/mount/point`:

```
lsof /mount/point
```

Ad esempio, per vedere i file aperti sul filesystem montato in `/home`:

```
lsof /home
```

3.10 Killare i processi che hanno aperto un file

Si possono combinare `lsof` con altri comandi per killare i processi che hanno aperto un file. Ad esempio, per killare tutti i processi che hanno aperto `/var/log/syslog`:

```
kill -9 $(lsof -t /var/log/syslog)
```

L'opzione `-t` di `lsof` restituisce solo i PID dei processi.

4 Esempi Specifici per i Socket

4.1 Elencare i socket aperti

Per elencare tutti i socket aperti sul sistema, si utilizza l'opzione `-i` senza specificare una porta:

```
lsof -i
```

Questo comando mostra tutti i socket aperti, inclusi quelli TCP e UDP.

4.2 Elencare i socket TCP aperti

Per elencare solo i socket TCP aperti, si utilizza:

```
lsof -i TCP
```

4.3 Elencare i socket UDP aperti

Per elencare solo i socket UDP aperti, si utilizza:

```
lsof -i UDP
```

4.4 Elencare i socket aperti su una porta specifica

Per trovare i processi che stanno utilizzando una specifica porta di rete, si utilizza l'opzione `-i` con il numero di porta:

```
lsof -i :porta
```

Ad esempio, per vedere i processi che utilizzano la porta `8080`:

```
lsof -i :8080
```

4.5 Elencare i socket aperti da un processo specifico

Per elencare i socket aperti da un processo specifico, si utilizza l'opzione `-p` con il PID del processo:

```
lsof -p PID -i
```

Ad esempio, per vedere i socket aperti dal processo con PID `5678`:

```
lsof -p 5678 -i
```

5 Output di Esempio

Ecco un esempio di output di `lsof` relativo ai socket:

```
COMMAND   PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd      1234  root    3u  IPv4  12345      0t0  TCP *:ssh (LISTEN)
nginx     5678  www     4u  IPv4  67890      0t0  TCP *:http (LISTEN)
```

Dove:

- `COMMAND`: Nome del comando.
- `PID`: ID del processo.
- `USER`: Utente che ha aperto il socket.

- `FD`: File descriptor (ad esempio, `3u` per un socket in ascolto).
- `TYPE`: Tipo di file (ad esempio, `IPv4` per un socket IPv4).
- `NAME`: Indirizzo e porta del socket (ad esempio, `*:ssh` per un socket in ascolto sulla porta SSH).