

2 SERVER LINUX

Perché è stato necessario eseguire ps come root (premettendo il comando con sudo)?

Il comando **ps** ha bisogno del **sudo** per visualizzare tutti i processi eseguiti in background perché la maggior parte sono di proprietà dell' utente root.

come viene rappresentata la gerarchia dei processi con ps ?

La gerarchia dei processi ha una struttura padre-figlio. il processo padre è incolonnato a sinistra mentre i figli sottostanti sono spostati verso destra.

```
595 492 492 ? 00:00:00 polkit-gnome-au
600 492 492 ? 00:00:01 xfce4-power-man
439 439 439 ? 00:00:02 syslog-ng
440 440 440 ? 00:00:00 vsftpd
448 448 448 ? 00:00:00 polkitd
483 483 483 ? 00:00:00 systemd
485 483 483 ? 00:00:00 (sd-pam)
506 506 506 ? 00:00:00 dbus-broker-lau
507 506 506 ? 00:00:00 dbus-broker
517 517 517 ? 00:00:00 at-spi-bus-lau
523 517 517 ? 00:00:00 dbus-broker-lau
524 517 517 ? 00:00:00 dbus-broker
534 534 534 ? 00:00:00 at-spi2-registr
549 549 549 ? 00:00:00 gpg-agent
566 566 566 ? 00:00:00 dconf-service
606 606 606 ? 00:00:00 xfce4-notifyd
540 540 540 ? 00:00:00 ssh-agent
621 618 618 ? 00:00:00 VBoxClient
622 618 618 ? 00:00:00 VBoxClient
632 631 631 ? 00:00:00 VBoxClient
634 631 631 ? 00:00:03 VBoxClient
645 643 643 ? 00:00:00 VBoxClient
649 643 643 ? 00:00:03 VBoxClient
687 687 687 ? 00:00:01 upowerd
698 697 697 ? 00:00:00 VBoxClient
699 697 697 ? 00:00:01 VBoxClient
725 492 492 ? 00:00:03 xfce4-terminal
731 731 731 pts/0 00:00:00 bash
823 823 731 pts/0 00:00:00 sudo
825 825 825 pts/1 00:00:00 sudo
826 826 825 pts/1 00:00:00 ps
808 808 808 ? 00:00:00 nginx
809 808 808 ? 00:00:00 nginx
[analyst@secOps ~]$
```

Qual è il significato delle opzioni -t, -u, -n, -a e -p in netstat? L'ordine delle opzioni è importante per netstat?

Il comando **netstat** restituisce informazioni sulla rete, le diverse opzioni sono correlate a queste informazioni:

- **-t** restituisce il tcp
- **-u** l'udp
- **-n** visualizza le connessioni rete attive sulla macchina
- **-a** visualizza tutte le connessioni attive
- **-p** i programmi attivi sulla rete

l'ordine in cui si scrivono le opzioni non è importante per netstat.

Basandosi sull'output di netstat mostrato al punto (d), qual è il protocollo di Livello 4, lo stato della connessione e il PID del processo in esecuzione sulla porta 80? Sebbene i numeri di porta siano solo una convenzione, puoi indovinare che tipo di servizio è in esecuzione sulla porta 80 TCP?

In sudo **netstat -tunap** alla porta 80 abbiamo un tcp in ascolto su un PID 808 che è il servizio http del master process del server web nginx.

da queste analisi si deduce che c'è un servizio **http** in ascolto sulla porta 80 che è di proprietà del servizio **nginx**

Il processo PID 395 è nginx. Come si potrebbe concludere questo dall'output sopra?

- **Cos'è nginx? Qual è la sua funzione? Usa google per saperne di più su nginx)**
- **La seconda riga mostra che il processo 396 è di proprietà di un utente chiamato http e ha il processo numero 395 come processo genitore. Cosa significa? È un comportamento comune?**
- **Perché l'ultima riga mostra `grep 395`?**

nginx è un server web per richieste http sulla porta 80.
il comportamento è molto comune.

nell'ultima riga vedo 808 perché per andare a cercare il **pid 808**, il comando **grep** avvia un processo che lo include nella ricerca, come se stesse cercando se stesso.

2.1 TELNET

Perché l'errore è stato inviato come pagina web?

Con **telnet** non riesco a connettermi alla porta 68 perché è un servizio che utilizza come protocollo **l'UDP** mentre telnet usufruisce del protocollo **TCP**, in sostanza non parlano la stessa lingua.

Quali sono i vantaggi di usare netstat?

Vantaggi nell'usare telnet, è sicuro?

Il vantaggio di netstat è che possiamo comprendere quali porte e quali servizi sono operativi su una data macchina.

Telnet è sicuramente un modo veloce per far comunicare due computer ma non è assolutamente sicuro perché i messaggi sono visibili in chiaro
