GABRIELE ROMANATO

Come creare uno script Bash per salvare le informazioni del comando netstat in un file CSV

Il comando netstat è uno strumento potente che fornisce informazioni sulle connessioni di rete, le interfacce di rete e altre statistiche di sistema legate alla rete. Se vuoi salvare queste informazioni in un formato strutturato, come un file CSV, puoi farlo facilmente utilizzando uno script Bash. Questo articolo spiegherà come creare uno script Bash che esegue il comando netstat, filtra e formatta i risultati, e li salva in un file CSV.

Il comando `netstat` genera un output che può variare a seconda delle opzioni utilizzate. Ad esempio, il comando `netstat -tun` mostra le connessioni TCP e UDP attive, insieme ai numeri di porta e indirizzi IP associati:

```
Proto Recv-Q Send-Q Local Address           Foreign Address
State
tcp        0      0 192.168.1.10:22
192.168.1.100:54512     ESTABLISHED
tcp        0      0 192.168.1.10:80
192.168.1.101:60912     TIME_WAIT
udp        0      0 0.0.0.0:68              0.0.0.0:*
```

Per salvare queste informazioni in un file CSV, dovremo rimuovere l'intestazione e formattare l'output in modo che ogni campo sia separato da una virgola.

```
#!/bin/bash

# Nome del file CSV di output
output_file="netstat_output.csv"
```

```
# Aggiungi l'intestazione al file CSV
echo "Protocol,Recv-Q,Send-Q,Local Address,Foreign
Address,State" > $output_file

# Esegui il comando netstat e formatta l'output in formato
CSV
netstat -tun | tail -n +3 | awk '{print
$1","$2","$3","$4","$5","$6}' >> $output_file

# Mostra un messaggio di completamento
echo "Le informazioni di netstat sono state salvate in
$output_file."
```

Spiegazione dello script:

- `output_file="netstat_output.csv"`: Definisce il nome del file CSV in cui verranno salvati i dati.
- `echo "Protocol,Recv-Q,Send-Q,Local Address,Foreign Address,State" > $output_file`: Aggiunge un'intestazione al file CSV con i nomi delle colonne.
- `netstat -tun | tail -n +3 | awk '{print $1","$2","$3","$4","$5","$6}' >> $output_file`:
  - `netstat -tun`: Esegue il comando `netstat` per mostrare le connessioni TCP e UDP.
  - `tail -n +3`: Rimuove le prime due righe dell'output di `netstat`, che di solito includono l'intestazione.
  - `awk '{print $1","$2","$3","$4","$5","$6}'`: Usa `awk` per formattare l'output, separando ogni campo con una virgola.
- `>> $output_file`: Aggiunge i dati formattati al file CSV.

Miglioramenti e opzioni avanzate:

- **Aggiungere un timestamp ai dati raccolti** per tracciare quando sono state registrate le informazioni.
- **Filtrare l'output di `netstat`** per mostrare solo le connessioni attive (`ESTABLISHED`), in ascolto (`LISTEN`), o in uno stato specifico.

- **Programmare lo script** per eseguire automaticamente la raccolta dei dati a intervalli regolari utilizzando `cron`.

Conclusione

Salvare le informazioni di `netstat` in un file CSV con uno script Bash è un processo semplice e utile per monitorare le connessioni di rete. Questo script può essere adattato per soddisfare esigenze specifiche e automatizzare la raccolta dei dati di rete.