

Trouver d'où vient la charge sur un serveur

Diagnostic de base

Premièrement, il faut trouver d'où vient la charge.... Est-ce que c'est un site web/utilisateur qui en est la cause? un problème serveur? une attaque sur une adresse IP?

Commandes

Nombre de connexions par IPs

```
netstat -tn 2>/dev/null | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr | head
```

Nombre de connexions par IPs sur le port 80

Changer :80 dans la commande pour :21 pour le FTP par exemple...

```
netstat -tn 2>/dev/null | grep :80 | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr | head
```

Trouver toutes les connexions sur le serveur pour une adresse IP

Remplacer 185.185.251.27 par l'adresse IP que vous souhaitez chercher.

```
netstat -tn 2>/dev/null | grep 185.185.251.27
```

Nombre de connexion par statut

```
netstat -an|awk '/tcp/ {print $6}'|sort|uniq -c
```

Trouver une adresse IP dans les logs apache

Remplacer 185.185.251.27 par l'adresse IP que vous souhaitez chercher.

```
grep -rnw '/var/log/httpd' -e '185.185.251.27'
```

From:

<https://wiki.proletaire.net/> - **Wiki**

Permanent link:

https://wiki.proletaire.net/linux/debug_charge?rev=1588592229

Last update: **2020/05/04 11:37**

