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?

Pour débuter, j'aime toujours (si possible) fermer le serveur web... Si la charge diminue drastiquement après l'arrêt du serveur web, on sait immédiatement que c'est le site d'un utilisateur qui est le problème de notre charge.

Le système devrait vouloir repartir le serveur http par lui-même. Donc idéalement, on ouvre 2 terminal... un pour envoyer notre commande stop au httpd et un pour vérifier la charge...et comme ça, on peut renvoyer la commande stop au besoin tout en vérifiant la charge...

Arret du serveur Web

```
systemctl stop httpd
```

Vous pouvez vérifier la charge et plein d'autre trucs avec htop

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'
```