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

Nombre de connexions

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

Il est possible de savoir le nombre de connexions pour d'autre services... Il suffit de changer *:80* dans la commande pour le port sur lequel vous souhaitez avoir le nombre de connexion. Ex: *: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
```

Exemple de résultat

Le première rangé de chiffres indique le nombre de connexions et la seconde l'adresse IP.

```
69 54.36.38.246
67 91.134.14.17
67 178.32.213.61
63 54.38.25.183
55 69.70.205.10
10 70.55.210.193
8 198.251.83.14
6 135.19.240.224
5 174.94.120.132
5 142.169.78.98
```

On voit ici que les 5 premier résultats sont “louche” et ont un nombre important de connexions au serveur. On va donc vérifier le propriétaire de l'adresse IP via le BGP Toolkit de Hurricane Electric.

Dans cet exemple, tous les IPs “louche” appartiennent à OVH... Solution ⇒ Firewall Block.

Trouver une adresse IP dans les logs

Vous pouvez savoir quel site/service est la cible des adresses IP avec la commande suivante

Remplacer 54.36.38.246 par l'adresse IP que vous souhaitez chercher.

Serveur Web:

```
grep -rnw '/var/log/httpd' -e '54.36.38.246'
```

- Examples de résultats et solutions

Serveur Mail (exim):

```
grep -rnw '/var/log/exim' -e '54.36.38.246'
```

FTP:

```
grep -rnw '/var/log/pureftpd.log' -e '54.36.38.246'
```

DirectAdmin:

```
grep -rnw '/var/log/directadmin' -e '54.36.38.246'
```

SSH:

```
grep -rnw '/var/log/secure' -e '54.36.38.246'
```