Quelques commandes pratiques d'audit système



Je me suis retrouvé dans des situations ou une machine n'avait pas le comportement habituel ou ces performances n'étaient pas au niveau du service qu'on demande à la machine.

Je vous propose quelques outils Linux qui pourraient vous aider a diagnostiqué des problèmes ou à faire un audit sur un serveur Linux.

Ces commandes m'ont sauvé la vie plusieurs fois et j'espère qu'elles feront pareille pour vous.

I/O disque

hdparm

Test la rapidité des disques dur avec hdparm.

Avec un disque sdb.

```
hdparm -Tt /dev/sdb
```

Options possibles pour hdparm.

```
hdparm --help
```

iostat

Générer des rapports statistiques sur l'entrée et la sortie des disques et fournir des mesures du débit, de l'utilisation, des longueurs de file d'attente, des taux de transaction et de la durée de service.

```
iostat interval count
```



il faudra peut-être l'installer :

```
apt install sysstat
```

Options usuelles:

- -x : extended statistics
- -t : Afficher le temps de chaque rapport

- -c : affiche l'usage CPU (sans -d)
- -d : affiche le rapport de l'utilisation disque (sans -c)
- -p device : affiche les statistiques des devices block et de leurs partitions (sans -x)
- -k : kilobytes (bytes par défaut)
- -m : megabytes (bytes par défaut)

Statistiques CPU exécutées toutes les 6 secondes 5 fois. Si rien n'est mentionné, cela ne s'arrête pas.

```
iostat -xtc 6 5
```

Détails des valeurs de retour affichées avec -c (CPU Utilization Report) à voir dans le man du système.

Statistiques disques exécutées toutes les 6 secondes 5 fois. Si rien n'est mentionné en nombre de fois, cela ne s'arrête pas.

```
iostat -xtd 6 5
```

Détails de valeurs de retour affichées avec -d (Device Utilization Report) à voir dans le man du système.

Les colonnes r/s, w/s, kr/s, et kw/s montrent respectivement les read et write par secondes en octets et kilo-octets.

Sur Solaris, les colonnes importantes à observer sont : svc_t, wait %w et %b – plus le temps de traitement est élevé, plus la performance s'en ressent bien évidemment.
Couplés l'un à l'autre, le temps de traitement et le temps d'occupation donnent une bonne impression sur l'état des entrées/sorties d'un disque.
Un taux d'occupation de plus de deux-tiers et un temps de traitement de plus de 50 millisecondes sont les indicateurs d'un goulot d'étranglement.

Que faire ? Voilà quelques pistes à explorer :

- répartir la charge sur plusieurs disques en utilisant un meilleur partitionnement;
- distribuer le swap (la pagination) sur plusieurs disques, ce qui a d'autant plus de sens que le swapping est important sur son système;
- faire figurer dans la mesure du possible les données liées sur la même partition;
- augmenter la mémoire (RAM) pour diminuer la pagination; c'est le cas par exemple lors de l'utilisation de SGBD qui sont très gourmands en mémoire, mais peu demandeurs de capacités de traitement rapides par le processeur;
- utiliser autant que faire se peut les ressources en cache des applications développées; php a par exemple un système de cache plutôt efficace aujourd'hui, très utile pour les requêtes et traitements récurrents;
- bien entendu, éviter d'écrire des requêtes qui parcourent les tables inutilement; cela demande donc une modélisation a priori qui arbitre entre un modèle E/R approprié et les capacités matérielles requises, sans oublier la manière dont on écrit les applications;
- si le disque est utilisé à 100%, on peut répartir le système de fichier sur deux disques ou plus en utilisant l'utilitaire de gestion des volumes disques que l'on trouve sous Solaris (le Volume Manager);
- déplacer le système de fichier vers un autre disque ou contrôleur plus rapide.

Statistiques disques du device et des partitions de sda exécutées toutes les 6 secondes 5 fois.

```
iostat -p sda 6 5
```

dd

Pour tester les temps d'accès disques (io). dd est une commande unix permettant de copier un fichier avec ou sans conversion(s) au passage, en ne sélectionnant qu'une partie de données à copier.
Il est particulièrement adapté à la copie sur des périphériques blocs tel que des disques durs ou des lecteurs CD-ROM.

```
time dd if=/dev/hda1 of=/file400Mo bs=1M count=400
```

CPU

mpstat

Statistiques CPU.

Usage.

```
mpstat <interval> <count>
```

Exécuter `mpstat` de manière infini toutes les 8 secondes.

```
mpstat 8
```

Load average

Affichage du load average.

```
top
uptime
cat /proc/loadavg
```

```
Load average of 1 means a single CPU system is loaded all the time while on
a 4 CPU system it means it was idle 75% of the time.
```

Mémoire

free

```
free -m
```

```
             total       used       free     shared    buffers     cached
Mem:          7983       5861       2121          0        382       1885
-/+ buffers/cache:       3593       4390
Swap:         3999        338       3661
```

Mémoire par processus

Analyser la mémoire utilisée par un processus 1234.

```
cat /proc/1234/smaps
```

Utilisation de la commande ps.

```
ps -efo pid,user,args,rss,%cpu,%mem,vsz --sort %mem
ps -efo pid,user,args,rss,pcpu,pmem,vsz --sort pmem
ps -efo pid,user,command,args,rss,pmem,vsz,size,pcpu,time,psr --sort pmem
```

Réseau

netstat

Statistiques réseaux.

Liste des statistiques par interfaces.

```
netstat -i
```

Etat des connexions.

```
netstat
```

Statistique en continue.

```
netstat -c
```

Liste les connexions établies.

```
netstat -tap
```

Liste les ports en écoute.

```
netstat -tulp
```

iftop

top des interfaces réseau.

Services

- apachetop : top Apache.
- mytop : top MySQL.
- ftptop : liste des connexions au serveur FTP.

Outils polyvalents

sysreport

Outil d'aspiration de toutes les configurations d'un système.

Entrer la commande suivante, un nom et un numéro de ticket et un fichier /tmp/sosreport-<nom>.<num_ticket>-<cle>.tar.bz2.

```
sysreport
```

Décompresser le fichier et toutes les informations systèmes sont contenues dans le dossier et peuvent être consultées.

vmstat

Statistiques processeurs, mémoires, IO.

Usage.

```
vmstat <delay> <count>
```

Exécution de vmstat toutes les 5 secondes de manière illimité.

```
vmstat 5
```

Voir le man du système pour le détail de chaque colonne.

top/htop

x : afficher le script exécuté par le processus au lieu du nom du process.

htop est un top un peu moins austère avec quelques couleurs.

sar

Compteur de l'activité système.

```
sar -o datafile interval count >/dev/null 2>&1 &
```

nmon

nmon est un outil de benchmark pour les administrateurs systèmes.
ça peut afficher la charge CPU, mémoire, réseau, disques (mini graphiques ou chiffres), fichier systèmes, NFS, top processus, les ressources.

Options usuelles:

- -h aide complète
- -f format de sortie de feuille de calcul [note: défaut -s300 -c288] optionnel
- -s <secondes> délai l'actualisation de l'écran [défaut 2]
- -c <nombre> délai de rafraîchissements [1 millions par défaut]
- -d <disques> pour augmenter le nombre de disque [défaut 256]
- -t tableau comprend les meilleurs processus
- -x planification de la capacité (15 min pendant 1 jour = 900 -fdt -s -c 96)

Si toi aussi tu as des outils intéressant viens les partagés
source: ouieuthoutca.org

From:
https://www.ksh-linux.info/ - **Know Sharing**

Permanent link:
https://www.ksh-linux.info/systeme/quelques-commandes-pratique-d-audit-systeme

Last update: **05/09/2025 21:17**