Aide-mémoire administrateur Linux

Table of Contents

section 1- Informations système

uname - Identification du système.

-a : toutes les informations. dmesg - Messages du noyau (et ceux du boot). uptime - Durée et charge du système. free - Occupation de la mémoire. vmstat - Détails sur l'utilisation de la mémoire. ipcs - Utilisation des ressources IPC System V. ipcrm - Suppression de ressources IPC System V. ldconfig - Valider les bibliothèques dynamiques. init - Changement de niveau de fonctionnement :

0 : arrêt. 1 : mono-utilisateur, 3 : multi-utilisateurs mode texte, 5 : multi-utilisateurs mode graphique, 6 : redémarrer.

section 2- Utilisateurs

useradd - Ajout d'un utilisateur :

```
useradd -m -p "" linus
```

crée un compte linus, avec répertoire personnel et mot de passe vide.

userdel - Suppression d'un compte utilisateur :

```
userdel -r linus
```

supprime le compte et le contenu de son répertoire.

```
passwd - Modification d'un mot de passe :
passwd linus
```

section 3 - Partitions et systèmes de fichiers

fdisk - Édition de la table des partitions :

```
fdisk /dev/hda
```

mkswap - Création d'une zone de swap :

```
mkswap /dev/hda2
mkswap /boot/swap_file
```

swapon - Activation d'une zone de swap :

```
swapon /dev/hda2
```

-a active toutes les zones de swap de /etc/fstab.

swapoff - Désactivation d'une zone de swap :

```
swapoff /dev/hda2
```

mkfs - Création d'un système de fichiers :

```
mkfs.ext2 /dev/hda3
mkfs.ext3 /dev/hda4
mkfs.vfat /dev/hda5
```

fsck - Vérification d'un système de fichiers :

```
fsck.ext2 -p /dev/hda3
```

réparation automatique d'un système ext2/ext3,

```
fsck.vfat /dev/hda4
```

vérification d'une partition Windows.

mount - Insertion de partition dans le système :

```
mount -t vfat /dev/hda4 /mnt/dos/
```

monter une partition Windows,

```
mount -a
```

monter toutes les partitions de /etc/fstab, **mount** 192.1.1.254:/home /home/users/

Montage d'un répertoire distant par NFS.

```
Options avec -o ou dans /etc/fstab :
```

default : rw,suid,dev,exec,auto,nouser,async,

remount : changer les attributs d'un système monté, rw : lecture-écriture, ro : lecture seule, noauto : ne pas monter automatiquement avec -a, nodev : interdire les fichiers spéciaux, noexec : pas de fichiers exécutables, nosuid ; ignorer les bits Set-UID/GID, sync : écritures synchrones, user : peut être monté par un utilisateur. Types de systèmes de fichiers courants : ext2, ext3, msdos, vfat, proc, iso9660, udf, smb.

umount - Démontage d'un système de fichiers :

-a : démonte tous les systèmes dans /etc/mtab.

```
umount /dev/hda4
umount /mnt/dos
umount -a
```

df - Taux d'occupation des systèmes de fichiers montés.

```
df -h
```

section 4- Distribution/installation de logiciel

tar - Gestion d'archives : -c : création d'archive, -x : extraction d'archive, -t : consultation d'archive, -f : nom du fichier archive, -v : mode volubile, -z : (dé)compresser avec g(un)zip, -j : (dé)compresser avec b(un)zip2. tar -czf archive.tar.gz distrib/

crée une archive compressée du répertoire distrib/,

```
tar -tvf archive.tar
```

liste le contenu de l'archive,

```
tar -xjf archive.tar.bz2
```

extrait le contenu d'une archive compressée. installation classique

```
tar -xzf application-1.01.tar.gz
cd application-1.01
./configure
make && make install
```

rpm - Gestion des paquetages RedHat :

```
-h : affichage de la progression du travail.
rpm -ivh paquet.rpm
```

- installation d'un paquetage,

  ```
  rpm -Uvh paquet.rpm
  ```

- mise à jour/installation d'un paquetage,

  ```
  rpm -Fvh paquet.rpm
  ```

- mise à jour d'un paquetage déjà installé,

  ```
  rpm -e paquet
  ```

- désinstallation d'un paquetage,

```
rpm -qa
```

- liste de tous les paquetages installés,

```
rpm -qf /chemin/fichier
```

- recherche du paquetage auquel appartient le fichier,

```
rpm -qip paquet.rpm
```

- informations sur un paquetage,

```
rpm -qlp paquet.rpm
```

- liste des fichiers contenus dans le paquetage.

```
apt - Gestion des paquetages Debian :
apt-get install application
```

- installation de l'application et ressources éventuelles,

```
apt-get remove application
```

- suppression application et dépendances éventuelles,

```
apt-get update
```

- mise à jour de la base de données interne,

```
apt-get upgrade
```

section 5 - Gestion des processus

1. application & lance l'application à l'arrière-plan, ramène à l'avant-plan le job numéro 1, (Ctrl-Z) endort l'application à l'avant-plan,

```
bg
```

- relance à l'arrière-plan un job endormi.

```
ps - État des processus :
```

```
ps -ef
ou
ps -aux
```

- affichage long de tous les processus du système.

```
top - Affichage continu des processus du système.
```

```
-d délai de rafraîchissement.
```

- renice - Changer la courtoisie d'un processus :

```
renice +5 12857
```

- augmente la courtoisie du processus 12857 de 5 unités,

```
renice -5 -u root
```

- diminue de 5 la courtoisie de tous les processus de root.

```
kill - Envoyer un signal à un processus :
kill -15 12857
-l (lettre l) : liste des signaux disponibles.
killall - Tuer tous les processus du même nom :
killall -9 boucle_fork
```

- fuser - Liste des processus accédant à un fichier :

```
fuser -k -m /dev/hda5
```

tue tous les processus accédant à la partition indiquée.

section 6 - Utilitaires réseau

- ifconfig - Configuration des interfaces réseau

```
ifconfig -a
```

- affiche la configuration de toutes les interfaces réseau,

```
ifconfig eth0 192.1.1.50
```

- configure la première interface ethernet.

```
route - Gestion de la table de routage du noyau :
route add -net 192.1.1.0 eth0
```

- ajoute une route statique via l'interface eth0,

```
route add -net 172.1.1.0 gw 192.1.1.5
```

- ajoute un réseau accessible par une passerelle,

```
route add default eth1
```

- ajoute une route par défaut,

```
route del default
```

- supprime la route par défaut.

```
socklist - Liste des sockets actives.
```

- netstat - Statistiques réseau :

```
netstat -r
```

- affiche la table de routage du noyau,

```
netstat -i
```

- affiche l'état des différentes interfaces,

```
netstat -a
```

- affiche l'état des sockets du système.

```
arp - Gestion de la table ARP du noyau :
```

-a affiche toutes les entrées dans le cache ARP,

```
arp -d hote
```

- supprime les entrées concernant l'hôte indiqué.

```
ping - demande d'écho vers d'autres hôtes :
ping -c 1 -w 2 192.1.1.53
une seule requête et attend au plus 2 secondes,
ping -b 192.1.1.255
```

- requête diffusée en broadcast à tous les hôtes du sous-réseau.
- traceroute - Chemin pour joindre un hôte :

```
traceroute www.destination.com
-n ne pas traduire les adresses numériques en noms.
tcpdump - Examen du trafic réseau :
tcpdump -i eth0
```

- affiche tout ce qui circule sur eth0, tcpdump -i eth0 port telnet affiche les message depuis / vers le port 23 (telnet).
- telnet - Connexion TCP/IP : telnet mail.isp.com pop-3
- connexion sur port 110 (Pop/3) du serveur de courrier.

```
rsh - Exécution d'un shell distant.
ssh - Exécution sécurisée d'un shell distant.
ssh usera@192.168.1.54
```

- ftp - Transferts de fichiers :

Commandes usuelles :

```
open ftp.serveur.org
cd /chemin/distant/
lcd /chemin/local/
get fichier
put fichier
prompt
mget \*.c
mput \*.h
wget - Rapatrier le contenu d'une URL :
```

- wget http://www.site.com/repertoire/ -c reprendre un transfert déjà entamé, -r charger récursivement les liens, -l niveau maximal de récursion, -k convertir les liens en pointeurs locaux.

section 7 - Signaux fréquemment utilisés

```
0 : pseudo signal vérifiant la présence d'un processus,
1 (SIGHUP) : fin de connexion,
2 (SIGINT, Ctrl-C) : fin immédiate du programme,
3 (SIGQUIT, Ctrl-\) : fin immédiate avec fichier core,
9 (SIGKILL) : fin obligatoire et immédiate,
15 (SIGTERM) : fin normale.
```

section 8 - Gestion des modules du noyau

1. lsmodListe des modules chargés. modinfoInformations sur un fichier module.

   ```
   insmod - Insertion d'un module dans le noyau :
   insmod module.o
   ```

2. rmmod - Suppression d'un modulé chargé :

   ```
   rmmod module
   ```

3. depmod - Vérification des dépendances :

   ```
   depmod -an
   ```

4. modprobe - Chargement gérant les dépendances :

   ```
   modprobe module.o
   ```

section 9 - Compilation d’un noyau Linux

```
ftp ftp.kernel.org
```

récupérer le noyau désiré (connexion anonymous) depuis le répertoire /pub/linux/kernel/,

```
tar -xjf linux-XXXX.tar.bz2
cd linux-XXXX
make mrproper
make menuconfig
choisir et sauver la configuration désirée, puis
make dep clean bzImage (jusqu'au noyau 2.4)
```

ou :

make (depuis noyau 2.6)

```
Puis, sous compte root :
```

make modules && make modules_install

```
    cp System.map /boot/System.map-XXXX
    cd arch/i386/boot/
    cp bzImage /boot/vmlinuz-XXXX
    vi /etc/lilo.conf
    ajouter l'entrée pour le nouveau noyau, puis
    /sbin/lilo
ou
    vi /boot/grub/grub.conf
    /sbin/init 6
```

section 10 - CHEAT

Reseaux

```
netstat -nat | awk '{print $6}' | sort | uniq -c | sort -r
```

Liste processus en ECOUTE

```
netstat -apn | grep LISTEN | awk '{ print $7 }' | sort | uniq -c | sort -nr | head -n
10
```

Info:

ESTABLISHED

```
The socket has an established connection.
```

SYN_SENT

```
The socket is actively attempting to establish a connection.
```

SYN_RECV

```
A connection request has been received from the network.
```

FIN_WAIT1

```
The socket is closed, and the connection is shutting down.
```

FIN_WAIT2

```
Connection is closed, and the socket is waiting for a shutdown
from the remote end.
```

TIME_WAIT

```
The socket is waiting after close to handle packets still in
the network.
```

CLOSE

```
The socket is not being used.
```

CLOSE_WAIT

```
The remote end has shut down, waiting for the socket to close.
```

LAST_ACK

```
The remote end has shut down, and the socket is closed.
 Waiting for acknowledgement.
```

LISTEN The socket is listening for incoming connections.

```
Such sockets are not included in the output unless you
specify the --listening
(-l) or --all (-a) option.
```

CLOSING

```
Both sockets are shut down but we still don't have all our
data sent.
```

UNKNOWN

```
The state of the socket is unknown.
```

script:

```
\#!/bin/bash
\#
\#    vvvv vvvv-- the code from above
RED='\033[0;31m'
NC='\033[0m' # No Color
echo ""
echo -en "${RED} ALL TCP Connections Count: ${NC}\n"
netstat -nat | awk '{print $6}' | sort | uniq -c | sort -r
echo ""
echo -en "${RED} Top CLOSE_WAIT state TCP Connections: ${NC}\n"
netstat -apn | grep CLOSE_WAIT | awk '{ print $7 }' | sort | uniq -c | sort -nr | head
-n 10
```

1. Time zone reconfigurer Time Zone

```
sudo dpkg-reconfigure tzdata
```

2. Configurér CLI, clavier avec accents

```
sudo apt install locales
sudo dpkg-reconfigure localces
```

3. executer des packets 32 bites sur une machine 64 bites

```
dpkg --add-acrhitecture i386
```

4. sécuriser TOP

pour cacher les informations à d'autres utilisateurs, dans le cas ou la machine est partagé avec d'autres utilisateurs. Il faut lancer la commandes:

```
sudo mount -o remount,rw,hidepid=2 /proc
```

[IMPORTANT]: et pour le mettre en permanance en cas de reboot, il faut modifier la line dans /etc/fstab

```
nano /etc/fstab
```

modifier la ligne /proc en rajoutant dans la colone 'type'

```
defaults,hidepid=2
```

5. changer paramètre SSH (modification de port, etc...)

```
nano /etc/ssh/sshd_config
```

1. changer le port 22 en port 'xxx'
2. vous pouvez desactiver le 'PermitRootLogin' aussi

```
service ssh restart
```