



Linux Utilisateur



Session du 27 juin au 1er juillet 2005

Table des matières

Installation de la distribution.....	2
Préparation.....	2
C'est parti !.....	2
Partitionnement :.....	2
Choix des paquetages.....	3
Mot de passe Root.....	3
Utilisateurs.....	3
Gestionnaire de démarrage.....	3
Vérification des paramètres système.....	4
Mise à jour sur Internet.....	4
Le système de droits.....	4
Sauvetage.....	5
VI.....	5
Récupération de fichiers effacés.....	6
Bash.....	6
Truc pour le montage usb.....	10
Firewall.....	11
WIFI.....	14
DHCP.....	16
CUPS.....	17

Webographie.....	18
------------------	----

Installation de la distribution

Quelques conseils rapides.

Préparation

Si vous avez un système Windows sur votre machine et que vous ne voulez pas l'effacer, sauvegardez vos données (pas les programmes) et défragmentez vos partitions.

Repérez les différents périphériques de votre machine notamment la carte graphique et la quantité de mémoire dont elle dispose et l'interface réseau. Si vous ne trouvez pas ces caractéristiques ne vous inquiétez pas outre mesure, la plupart du temps la détection automatique fonctionne bien. Si vous disposez de périphériques externes, veillez à ce qu'ils soient reliés à la machine et sous tension.

Configurez le BIOS de votre machine pour qu'elle démarre sur le lecteur de cdrom.

C'est parti !

Mettez la machine sous tension et insérez rapidement le premier cdrom (avant que la machine ne « boote »).

Lorsque vous arrivez au choix de la langue veillez à bien choisir Europe=>Français car par défaut c'est le français d'amérique qui est sélectionné.

Partitionnement :

C'est la partie la plus délicate de l'installation surtout si un autre système d'exploitation est installé sur votre machine et qu'il vous faut modifier la taille des partitions existantes (si vous avez décidé d'effacer votre ancien système, aucun souci). Tout d'abord vérifiez l'endroit où vous avez rangé les sauvegardes que vous faites régulièrement. Si vous ne vous souvenez plus de la date de votre dernière sauvegarde, redémarrez sous votre ancien système et sauvegardez vos données ! Profitez-en pour défragmenter vos partitions windows si ce n'est pas déjà fait.

Assurez-vous que l'alimentation électrique de votre machine est stable, une coupure secteur pendant l'opération de partitionnement peut avoir des effets catastrophiques.

Pour une utilisation domestique, une partition racine et une partition /home sont raisonnables. Si vous comptez utiliser votre machine comme serveur de données, il peut être utile d'avoir une partition /var séparée. Enfin si vous avez un disque ide et un ou plusieurs disques exotiques (SATA,...) il est prudent de créer une petite partition /boot

(100 à 200 Mo) sur un disque ide.

La partition de swap doit en principe être égale au double de la RAM installé sur votre machine.

Choix des paquetages

Les choix proposés permettent d'installer rapidement une machine standard. Si vous disposez de peu d'espace disque, il faut cocher la sélection individuelle des paquetages. Prévoyez café, bière, sandwichs. Les paquetages standards sont déjà présélectionnés et la plupart du temps il n'y a qu'à décocher ceux dont vous ne voulez pas, après avoir lu les explications sur leur utilité. Vous pourrez toujours rajouter par la suite ce qui vous manque, ce n'est pas bloquant. Les dépendances des paquetages sont bien gérées par l'outil et dorénavant l'installation ne commence pas si vous n'avez pas suffisamment d'espace disque.

Mot de passe Root

Après l'installation des paquetages, vous devez choisir le mot de passe de l'administrateur du système. Dans le cas d'une machine familiale celui-ci n'est pas d'une importance capitale. Cependant, si vous désirez que votre installation soit pérenne, il vaut mieux que vous soyez seul à le connaître et que les enfants ne le devinent pas. Pour une utilisation professionnelle il faut choisir des mots de passe robustes.

En cas d'oubli il est possible de le changer (si vous pouvez le faire, d'autres aussi !)

Utilisateurs

Créez maintenant vos utilisateurs. Un pour vous et un pour chaque personne susceptible d'utiliser la machine. Si vous êtes seul à utiliser la machine ne vous croyez pas dispensé de créer votre compte. La robustesse de Linux est aussi fondée sur le fait que personne ne travaille avec les droits d'administrateur ! Les machines utilisées en permanence par « root » se dégradent assez vite par accumulation de petites erreurs impossibles à réaliser par un utilisateur standard.

Vous aurez la possibilité de sélectionner un compte qui sera connecté automatiquement au démarrage, sans avoir à taper le mot de passe. C'est pratique pour de jeunes enfants. Ce compte NE DOIT PAS être le votre !

Gestionnaire de démarrage

L'installation du gestionnaire de démarrage sur la MBR est généralement une bonne

solution.

Vérification des paramètres système

Vous pouvez maintenant vérifier que votre matériel a bien été détecté et configuré. Les éventuels problèmes sont indiqués en rouge. Vérifiez particulièrement l'interface graphique même si il n'y a plus guère de soucis dorénavant. Vous aurez le choix de démarrer directement en mode graphique plutôt qu'en mode texte. Si vous avez des doutes sur votre interface, il faut dire non, quitte à changer une fois votre carte correctement configurée. C'est aussi le moment de paramétrer votre souris.

Mise à jour sur Internet

Dites non, vous le ferez plus tard.

Le système de droits

Les êtres humains sont répartis en 3 catégories : moi, mon groupe et les autres.

Les permissions sont :

- **lecture**, je peux lire donc copier le fichier ou lister le contenu du répertoire
- **écriture**, je peux modifier ou effacer le fichier ou créer / supprimer un fichier dans le répertoire
- **exécution**, je peux lancer le programme ou traverser le répertoire

	<i>propriétaire</i>	<i>groupe</i>	<i>autres</i>
lecture	4	4	4
écriture	2	2	2
exécution	1	1	1

Il existe 2 autres bits :

- le bit **S**, appliqué à un fichier exécutable il fait en sorte que le programme s'exécute avec les droits du propriétaire ou de son groupe et non pas ceux de celui qui le lance.
- le bit **T**, appliqué à un fichier exécutable il maintient en mémoire le programme après la fin de son exécution. Appliqué à un répertoire dans lequel tout le monde peut écrire, il n'autorise la suppression que des fichiers dont on est propriétaire (/tmp).

Ces bits constituent le premier digit octal (optionnel) Suid vaut 4, Guid vaut 2 et T vaut 1.

Sauvetage

Si vous avez oublié le mot de passe de root, supprimé le gestionnaire de démarrage ou une autre grosse bêtise, tout n'est pas perdu.

Démarrez votre machine avec le dvd et tapez <F1>. puis « rescue ».

Un menu s'affiche qui permet :

- de restaurer le gestionnaire de démarrage
- de restaurer le chargeur de démarrage de Windows (drôle d'idée)
- de monter vos partitions Linux dans /mnt. Après ceci, retournez au menu et choisissez d'aller sur une console. Vous aurez alors le loisir de réparer votre système. Sur l'écran s'affiche une aide bien utile notamment pour configurer votre clavier (par défaut en QWERTY).

Si vous avez perdu votre mot de passe root, modifiez les droits de /mnt/etc/shadow en 600 (chmod 600 /mnt/etc/shadow) puis éditez le avec vi. Supprimez alors le mot de passe de root (le mot de passe crypté, pas toute la ligne !), exemple :

```
root:$1$PgbdUpt5$VTzjNZ15m//ajifewjJIs0:12826:0:99999:7:::
```

devient

```
root::12826:0:99999:7:::
```

sauvegardez (<ESC>:wq), remettez les droits d'origine (chmod 400 /mnt/etc/shadow) puis rebootez normalement. N'oubliez pas de redéfinir le mot de passe de root ! (su puis passwd).

Si votre machine est configurée pour démarrer en mode graphique et que le mode graphique ne marche plus :

Editez le fichier /mnt/etc/inittab et changez le niveau d'exécution au démarrage.

```
id:5:initdefault:
```

devient

```
id:3:initdefault:
```

VI

Lorsque vous êtes en mode « rescue », vous n'avez pas vraiment d'autre choix que d'utiliser VI. Voici le minimum à savoir :

ouvrir un fichier : vi <nom du fichier>

Passer en mode insertion : « i »

Se déplacer avec les flèches du clavier, supprimer, écrire puis...

Quitter le mode insertion : <ESC>

Passer en mode commande : « : »

Sauvegarder : « w »

Quitter : « q »

Si vous voulez (ou devez) quitter sans sauvegarder : « :q! »

Récupération de fichiers effacés

Fichier détruit par inadvertance sur un système de fichiers ext2 ?

Lire le HOWTO intitulé "Ext2-undeletion"

Laurent Foucher résume cela (mots-clés : restaurer, undelete) :

voici les manip à faire pour récupérer un fichier (ici : sur hda2)

```
echo lsdel | debugfs /dev/hda2 > liste.txt
```

cela permet de connaître les inodes des fichiers perdus.

puis lancer debugfs /dev/hda2 et dans la ligne de commande de debugfs, lancer :

```
dump ((No_inode)) /mnt/recovered.000
```

Bash

Un script qui affiche le chemin d'un fichier passé en paramètre.

```
echo `basename $1`
```

un script qui renvoie les paramètres passés si il y en a deux ou un message d'insulte dans le cas contraire

```
#!/bin/bash
```

```
if [ $# -eq 2 ]
```

```
    then echo $1 $2
```

```
else
```

```
    echo "Insulte"
```

```
fi
```

un script test-fichier, qui précisera le type du fichier passé en paramètre, ses permissions d'accès pour l'utilisateur

```
#!/bin/bash

if [ ! -e $1 ]
then
    echo "Le fichier $1 n'existe pas"
    exit 1
fi
# Info sur le type de fichier
echo -n "Le fichier $1 est un "
if [ -f $1 ]
then
    echo "fichier ordinaire"
elif [ -d $1 ]
then
    echo "répertoire"
else
    echo "truc bizarre"
fi
# Infos sur les droits d'accès
echo -n "qui est accessible par `id -un` en "
if [ -r $1 ]
then
    echo -n " lecture"
fi
if [ -x $1 ]
then
    echo -n " execution"
fi
if [ -w $1 ]
then
    echo -n " ecriture"
```

```
fi
```

un script bash `listedir.sh` permettant d'afficher le contenu d'un répertoire passé en paramètre, en séparant les fichiers et les (sous)répertoires.

```
#!/bin/bash
```

```
# Liste le contenu du repertoire specifie en argument
```

```
# Verification du nombre d'arguments
```

```
if [ $# -ne 1 ]
```

```
then
```

```
    echo "Erreur: usage: $0 <repertoire>"
```

```
fi
```

```
# Affichage des fichiers
```

```
echo "----- Fichiers dans $1 -----"
```

```
for nom in $1/*
```

```
do
```

```
    if [ -f $nom ]
```

```
    then
```

```
        echo `basename $nom`
```

```
    fi
```

```
done
```

```
# Affichage des repertoires
```

```
echo "----- Repertoires dans $1 -----"
```

```
for nom in $1/*
```

```
do
```

```
    if [ -d $nom ]
```

```
    then
```

```
        echo `basename $nom`
```

```
    fi
```

```
done
```

```
if [ ! -e $1 ]
then
    echo -n repertoire ?
    read truc
else
    truc=$1
fi
```

Puis changer chaque occurrence de \$1 par \$truc

Exemple de « case » :

```
#!/bin/bash
# Verification du nombre d'arguments
case $# in
    1) echo "un paramètre";;
    2) echo "deux paramètres";;
    3) echo "trois paramètres";;
    *) echo "autre" ;;
esac
```

Autre exemple :

```
#!/bin/bash

# Verification du nombre d'arguments
case $# in
    1) if [ -f $1 ]
        then
            if [ -r $1 ]
            then echo "$1 est lisible par `id -un`"
            else echo "$1 n'est pas lisible par `id -un`"
        fi
    fi
fi
```

```
        fi
        else echo "$1 n'est pas un fichier"
        fi;;
2) if [ -f $1 ] && [ -f $2 ]
    then if [ $1 -nt $2 ]
        then echo "$1 est plus récent que $2"
        else echo "$2 est plus récent que $1"
        fi
    fi;;
*) echo "Que veux tu que je fasse du 3ème paramètre ?" ;;
esac
```

Exemple de « while »

```
#!/bin/bash
while
    echo -n "tapez quelque chose : "
    read mot
    [ $mot != "fin" ];
do
    echo "vous avez tapé $mot"
    echo "tapez \"fin\" pour finir";
done
```

Truc pour le montage usb

Après avoir inséré un périphérique usb, tapez la commande « dmesg » :

```
Initializing USB Mass Storage driver...
scsi2 : SCSI emulation for USB Mass Storage devices
usbcore: registered new driver usb-storage
USB Mass Storage support registered.
usb-storage: device found at 2
```

```
usb-storage: waiting for device to settle before scanning
  Vendor: OTi           Model: Flash Disk           Rev: 2.00
  Type:   Direct-Access           ANSI SCSI revision:
02
SCSI device sdb: 256000 512-byte hdwr sectors (131 MB)
sdb: Write Protect is off
sdb: Mode Sense: 03 00 00 00
sdb: assuming drive cache: write through
SCSI device sdb: 256000 512-byte hdwr sectors (131 MB)
sdb: Write Protect is off
sdb: Mode Sense: 03 00 00 00
sdb: assuming drive cache: write through
  sdb: sdb1
Attached scsi removable disk sdb at scsi2, channel 0, id 0, lun 0
usb-storage: device scan complete
```

Le périphérique usb est reconnu comme un disque scsi et porte le doux nom de « sdb ».

Pour le monter il vous reste à taper :

```
mount /dev/sdb1 /le_repertoire_de_votre_choix
```

Les éventuels messages d'erreur vous indiquent pourquoi ça ne fonctionne pas, le cas échéant.

Firewall

corrigé du TP

Exercice 1 : le routeur jette icmp en provenance du poste de travail

1. Effacez toutes les règles qui pourraient exister
2. Ecrivez les règles correspondantes
3. Testez

```
iptables -F
iptables -A INPUT -s adresse_IP_du_poste_de_travail -p icmp -j
DROP
```

Exercice 2 : le routeur retourne les pings à destination du poste de travail en prétendant qu'il n'existe pas

1. Effacez les règles précédentes
2. Ecrivez les règles correspondantes
3. Testez

```
iptables -F
iptables -A FORWARD -i eth_externe -p icmp -j REJECT --reject-with
icmp-host-unreachable
/*note eth_externe désigne l'interface reliée au "backbone" de la
salle et eth_interne désigne l'interface reliée au poste de
travail*/
```

Exercice 3 : le routeur interdit tout au poste de travail sauf le web

1. Effacez les règles précédentes
2. Ecrivez les règles correspondantes
3. Testez

```
iptables -F
iptables -P FORWARD DROP
iptables -A FORWARD -i eth_interne -p tcp --destination-port www
-j ACCEPT
iptables -A FORWARD -i eth_externe -p tcp --source-port www -j
ACCEPT
```

Ces règles fonctionnent mais dans la vraie vie il faudrait aussi autoriser udp 53 (DNS) dans les deux sens (et https 443)!

```
iptables -A FORWARD -p udp --source-port 53 -j ACCEPT
iptables -A FORWARD -p udp --destination-port 53 -j ACCEPT
```

Exercice 4 : le routeur interdit les connexions TCP venant de l'extérieur vers le poste de travail

1. Effacez les règles précédentes
2. Vérifiez que l'on peut se connecter sur le poste de travail par ssh
3. Vérifiez que l'on peut se connecter sur le poste de travail sur un serveur web (au besoin installez-le)
4. Ecrivez les règles correspondantes
5. Testez

```
iptables -F
iptables -P FORWARD ACCEPT
iptables -A FORWARD -i eth_externe -p tcp --syn -j DROP
ou
iptables -A FORWARD -i eth_externe -p tcp --syn -j REJECT --
reject-with icmp-host-unreachable
```

Exercice 5 : le routeur n'autorise, venant de l'extérieur, que les connexions web

1. Effacez les règles précédentes
2. Vérifiez que l'on peut se connecter sur le poste de travail par ssh
3. Vérifiez que l'on peut se connecter sur le poste de travail sur un serveur web
4. Ecrivez les règles correspondantes
5. Testez

```
iptables -F
iptables -P FORWARD DROP
iptables -A FORWARD -i eth_interne -j ACCEPT
iptables -A FORWARD -i eth_externe -p tcp -m state --state
ESTABLISHED, RELATED -j ACCEPT
iptables -A FORWARD -i eth_externe -p tcp --destination-port www
-j ACCEPT
Un firewall qui se base sur l'état des connexions TCP s'appelle
"statefull".
```

Exercice 6 : masquering (NAT)

Vous allez maintenant masquer les adresses IP de notre réseau local. Deux raisons pour cela :

1. Votre FAI ne vous donne (loue ?) qu'une seule adresse IP et vous avez tout un réseau à connecter à Internet. Utilisez dans ce cas un adressage "privé" pour votre réseau local.
2. Vous voulez cacher le réseau local au reste du monde.

Utilisez la chaîne POSTROUTING, qui s'applique après la décision de routage.

Faites des captures sur toutes les interfaces et expliquez ce qui se passe.

```
iptables -t nat -A POSTROUTING -o eth_externe -j MASQUERADE
```

Maintenant, renvoyez les demandes de connexion externes (ssh) sur le port 1234 TCP vers le poste de travail (port 22 TCP).

```
iptables -t nat -A PREROUTING -p tcp --dport 1234 -i eth_externe
-j DNAT --to adresse_IP-poste_de_travail:22
```

Exercice 7 : prévenir le "Deny of Service"

Le DoS est une attaque qui consiste à noyer une machine sous une avalanche de paquets dans le but de la mettre à genoux. Une parade est de limiter certains traffic. Essayez de limiter les "ping".

```
iptables -P INPUT ACCEPT
```

```
iptables -A INPUT -p icmp -m limit --limit 3/hour -j ACCEPT
```

```
iptables -A INPUT -p icmp -j DROP
```

Ces règles acceptent 5 pings à la suite (à cause de la réserve **--limit-burst**) puis droppent pendant 20 minutes (1/3 d'heure).

Exercice 8 : "logger"

Enregistrez dans le journal les pings reçus de la station de travail (le journal est dans /var/log/message, vous le visualisez facilement avec tail). Vous pouvez limiter la fréquence.

```
iptables -A INPUT -p icmp -m limit --limit 1/minute -j LOG --log-prefix "Bonjour les cocos"
```

Pour en savoir plus, lire l'excellent Packet Filtering HOWTO ainsi que le nat HOWTO :

<http://www.netfilter.org/documentation/HOWTO/fr/packet-filtering-HOWTO.html>

<http://www.netfilter.org/documentation/HOWTO/fr/NAT-HOWTO.html>

ainsi que les exemples de www.lea-linux.org

WIFI

Votre interface est détectée par le système, le driver fourni avec votre distribution fonctionne et vous pouvez utiliser les outils graphiques. Allez vite jouer au loto !

La commande « lspci » vous indique les périphériques trouvés sur le bus. Repérez votre interface et notez son identification.

```
02:02.0 Network controller: Broadcom Corporation BCM4306 802.11b/g Wireless LANController (rev 03)
```

Tapez ensuite « lspci -n »

```
02:02.0 Class 0280: 14e4:4320 (rev 03)
```

Notez l'avant dernier et dernier nombre, dans ce cas « 14e4:4320 »

Coller ceci dans un bon moteur de recherche.

1. il existe un driver sur internet :

1. télécharger la dernière version, voire une version cvs
 2. le compiler / installer en suivant les instructions fournies
2. il n'existe pas de driver
1. vérifier que « ndiswrapper » est installé (sinon l'installer)
 2. copier les driver Windows dans un répertoire quelconque (fichier .inf et .sys)
 3. installer le driver par « ndiswrapper -i <chemin vers votre fichier inf> »

Devenez root et lancez votre module driver par :

```
modprobe <driver ou ndiswrapper>
```

Détectez les réseaux wifi présents dans votre environnement :

```
iwlist scan
```

Attention, les ordinateurs portables nécessitent de démarrer l'interface par un bouton !

```
wlan0 Scan completed :
```

```
Cell 01 - Address: 00:12:44:BA:95:30
```

```
ESSID:"tsunami"
```

```
Protocol:IEEE 802.11b
```

```
Mode:Managed
```

```
Frequency:2.417 GHz (Channel 2)
```

```
Quality:0/100 Signal level:-36 dBm Noise level:-256 dBm
```

```
Encryption key:off
```

```
.....
```

```
Bit Rate:54 Mb/s
```

```
Extra:bcn_int=100
```

```
Extra:atim=0
```

Nous avons donc un réseau nommé « tsunami » sur le canal 2, sans cryptage. Si votre interface s'appelle wlan0 tapez « iwconfig wlan0 essid "tsunami" channel 2 ».

```
iwconfig wlan0
```

```
wlan0 IEEE 802.11g ESSID:"tsunami"
```

```
Mode:Managed Frequency:2.417 GHz Access Point:  
00:12:44:BA:95:30
```

```
Bit Rate:54 Mb/s Tx-Power:25 dBm
```

```
RTS thr:2347 B Fragment thr:2346 B
```

```
Encryption key:off
```

```
Power Management:off
Link Quality:100/100 Signal level:-10 dBm Noise
level:-256 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:2097 Missed
beacon:0
```

Si vous avez un serveur dhcp, vous pouvez maintenant tenter « dhclient wlan0 » pour faire attribuer une adresse à votre interface. Vous pouvez quitter root et mener une existence normale mais sans fil !

Si vous ne voulez pas avoir à lancer votre module à chaque utilisation, insérez la ligne suivante dans le fichier /etc/modprobe.conf

```
alias wlan0 <ndiswrapper ou le nom de votre driver>
```

DHCP

Le paquetage Mandriva pour le serveur dhcp s'appelle : dhcp-server...

Le fichier de configuration est : /etc/dhcpd.conf

Exemple de configuration simple

```
ddns-update-style interim;
ignore client-updates;
#Les 2 lignes précédentes servent à ignorer la mise à jour
#automatique de dns, fonction encore expérimentale

#définition d'un réseau
subnet 10.2.10.0 netmask 255.255.255.0 {
#plage d'adresses servies
    range dynamic-bootp 10.2.10.50 10.2.10.100;
#durée du bail en secondes
    default-lease-time 21600;
#durée maximum si le client ne se contente pas de la valeur par défaut
    max-lease-time 43200;

    # si une machine nécessite une adresse fixe
    host toto {
        #Cette machine charge sa configuration en tftp
```

```
    next-server truc.machin.com;
    #Elle est identifiée par son adresse MAC
    hardware ethernet 12:34:56:78:AB:CD;
    #Enfin son adresse fixe qui doit être en dehors de la plage servie...
    fixed-address 10.2.10.49;
}

#Vous pouvez répéter les adressages fixes tant que vous voulez
}

Votre serveur peut servir d'autres réseaux à conditions qu'ils soient accessibles
```

CUPS

Common Unix Printing System. C'est le serveur d'impression le plus utilisé par les grandes distributions.

On configure les imprimantes directement connectées par l'interface web 127.0.0.1:631. Les serveurs CUPS des différentes machines du réseau communiquant entre eux vont apprendre quelles sont les imprimantes accessibles.

Le serveur se configure dans le fichier `/etc/cups/cupsd.conf` :

```
#L'imprimante locale
<Location /printers/epson>
Order Deny,Allow
Deny From All
Allow From 127.0.0.1
AuthType None
Allow from 192.168.0.0/255.255.255.0
#Le réseau local peut utiliser l'imprimante on aurait pu mettre Allow from @LOCAL
</Location>
Browsing On # on autorise à causer
BrowseProtocols cups
BrowseOrder Deny,Allow
BrowseAllow from @LOCAL # on acquiert les imprimantes du réseau
```

BrowseAddress 192.168.0.255 # on cause en broadcast sur le réseau local

Listen 192.168.0.1:631

Listen 127.0.0.1:631

#Le serveur est accessible de la machine locale (par ses 2 adresses)

Voilà !

Webographie

www.lea-linux.org

www.linux-french.org