Linux Administrateur

Sébastien Jeudy

(www.neosysta.com)

SOMMAIRE

OBJECTIFS DU SUPPORT

Maîtriser l'administration du système Linux Ubuntu au quotidien, sous ses aspects les plus importants :

- Distributions
- Installations & Partionnements
- Amorçages & Noyaux
- Logiciels & Préférences Système
- Paquets
- Arborescence & Commandes Système
- Sauvegardes & Journalisations
- Processus & Urgences
- Tâches Administratives
- Groupes & Utilisateurs
- Serveurs
- Sécurités
- Réseaux
- Partages & Connexions Distantes
- Routages & Proxy
- Impressions

 ***Sources** : http://www.ubuntu-fr.org & http://fr.wikipedia.org*

1 Rappel UNIX

UNIX (dérivé de Unics) est un système d'exploitation sécurisé, multitâches et multi-utilisateurs, imaginé en 1969 par Ken Thompson (Laboratoires Bell, USA). Il est conceptuellement ouvert et fondé sur une approche par laquelle il offre de nombreux petits outils chacun dotés d'une mission spécifique.

UNIX a donné naissance à une famille de systèmes, dont les plus populaires en 2010 sont GNU/Linux, BSD et Mac OSX. On nomme « famille Unix » l'ensemble de ces systèmes. On dit encore qu'ils sont de « type Unix » et on les qualifie d'Unices (en anglais, UNIX étant invariable en français).

Il existe un ensemble de standards réunis sous la norme POSIX qui vise à unifier certains aspects de leur fonctionnement.

2 La distribution Linux Ubuntu

2.1 Origines

Linux Ubuntu est un système d'exploitation libre et gratuit, hérité d'UNIX.

Dans un jargon plus technique, Ubuntu est une "distribution GNU/Linux très globalement libre basée sur Debian". C'est Mark Shuttleworth, un entrepreneur sud-africain ayant fait fortune lors de l'explosion de la bulle Internet, qui est à l'origine d'Ubuntu. Depuis la première version stable d'Ubuntu, sortie en 2004, la popularité de cette distribution ne cesse de croître ; elle continue de s'améliorer en terme de fonctionnalités et de stabilité, et séduit chaque jour de nombreux utilisateurs, tant parmi les débutants que parmi les plus chevronnés.

Canonical Ltd est la société fondée (et financée) par l'entrepreneur sud-africain Mark Shuttleworth, et dont l'objet est la promotion de projets open source. Canonical est basée sur l'Île de Man. Canonical est le sponsor officiel du système d'exploitation libre Ubuntu auquel elle assure le support technique et la certification.

2.2 Pourquoi choisir Ubuntu ?

Voici ce qui fait la force et le succès d'Ubuntu :

- **Disponible gratuitement et librement :** Tout un chacun peut télécharger gratuitement et légalement une copie d'Ubuntu et l'installer pour lui-même et d'autres personnes. Il peut aussi obtenir le code ayant servi à construire Ubuntu, l'étudier, le modifier et le redistribuer ensuite (avec ou sans rétribution financière) en toute légalité ;

- **Le parfum Ubuntu :** Thème graphique et sonore particulier ;

- **Toujours à la pointe :** Une nouvelle version tous les six mois propulse Ubuntu continuellement vers l'avant ;

- **Le système des dépôts de logiciels** permet d'installer en quelques clics, avec une facilité déconcertante, des logiciels extrêmement variés. Les dépôts contiennent des paquets logiciels dont le nombre est passé à 23 000. Dans ce cadre, on peut dire que Ubuntu est parfaitement adapté pour exploiter Internet. Des miroirs du dépôt Ubuntu sont disponibles localement pour accélérer les transferts. La compatibilité générale (mais imparfaite) avec les paquets Debian permet une bonne interaction entre les 2 distributions ;

- **Les mises à jour de sécurité sont simplifiées et gérées graphiquement :** Une tâche de notification prévient lorsqu'une mise à jour est disponible. En quelques clics, machine et logiciels sont sécurisées ;

- **Une vaste communauté contributive :**

  - Une communauté francophone proposant une documentation fournie et des forums actifs ;

  - Launchpad (https://launchpad.net), une plateforme de coordination permettant de fédérer toute la communauté internationale sur les évolutions, les bogues, la traduction (localisation) et la documentation d'Ubuntu ;

  - Les groupes d'utilisateurs Linux supportant généralement Debian offrent naturellement le même suivi avec Ubuntu. En effet, ces 2 distributions sont très voisines et se manipulent pratiquement de la même façon.

2.3 Variantes officielles

Ces variantes d'Ubuntu sont soutenues officiellement par Canonical et la communauté Ubuntu :

- **Ubuntu :** Édition destinée à un usage bureautique ou domestique, avec l'environnement de bureau GNOME

- **Kubuntu :** Édition destinée à un usage bureautique ou domestique, avec l'environnement de bureau KDE

- **Edubuntu :** Édition destinée au milieu scolaire

- **Ubuntu Édition Serveur :** Édition destinée aux serveurs informatiques (en général, sans interface graphique)

Toutes les variantes officielles sont basées sur la variante initiale, Ubuntu. Elles partagent donc toutes le même mode de fonctionnement. En fait, elles forment toutes une seule et même distribution.

2.4 Historique des versions

La numérotation des versions d'Ubuntu est basée sur l'année et le mois de sa sortie [A.MM] :

Version	Nom	Date de sortie
Ubuntu 4.10	The Warty Warthog (le phacochère verruqueux)	20/10/04
Ubuntu 5.04	The Hoary Hedgehog (le hérisson vénérable)	08/04/05
Ubuntu 5.10	The Breezy Badger (le blaireau jovial)	13/10/05
Ubuntu 6.06 LTS (*)	The Dapper Drake (le canard pimpant)	01/06/06
Ubuntu 6.10	The Edgy Eft (la salamandre énervée)	26/10/06
Ubuntu 7.04	The Feisty Fawn (le faon courageux)	19/04/07
Ubuntu 7.10	The Gutsy Gibbon (le gibbon fougueux)	18/10/07
Ubuntu 8.04 LTS (*)	The Hardy Heron (le héron robuste)	24/04/08
Ubuntu 8.10	The Intrepid Ibex (le bouquetin intrépide)	30/10/08
Ubuntu 9.04	The Jaunty Jackalope (le jackalope enjoué)	23/04/09
Ubuntu 9.10	The Karmic Koala (le koala karmique)	29/10/09
Ubuntu 10.04 LTS (*)	The Lucid Lynx (le lynx lucide)	29/04/10
Ubuntu 10.10	The Maverick Meerkat (le suricate rebelle)	28/10/10

Des versions stables d'Ubuntu sortent deux fois par an, aux mois d'avril et d'octobre. Le développement d'Ubuntu est lié au développement de l'environnement de bureau GNOME.

(*) LTS = Long Term Support (soutien à long terme).

3 Installation d'Ubuntu

3.1 Téléchargement

Ubuntu est une distribution GNU/Linux libre et gratuite. On peut en obtenir une copie pour utilisation et installation en téléchargeant gratuitement et légalement une image CD ou DVD Ubuntu, à graver soi-même sur un CD ou un DVD.

- **Lien de téléchargement : http://www.ubuntu-fr.org/telechargement**

Le CD-ROM d'installation d'Ubuntu (aussi appelé "Desktop CD" ou "Live CD") est un média permettant de tester Ubuntu ainsi que de l'installer. Le CD-ROM d'installation d'Ubuntu dispose aussi de quelques outils utiles pour la réparation et la restauration du système.

Pour accéder au menu de démarrage et aux outils fournis par le CD-ROM d'installation d'Ubuntu, celui-ci doit être inséré dans le lecteur de CD-ROM avant même qu'un système d'exploitation soit chargé.

Pour qu'une session live ou l'installateur d'Ubuntu puisse être chargé, l'ordre d'amorçage du BIOS doit être réglé de telle façon que le lecteur de CD-ROM soit au-haut de cette liste.

3.2 Tester sans installation (Live CD)

Le terme « session live » désigne l'exécution d'un système d'exploitation sans qu'il soit installé sur l'ordinateur qui lui sert d'hôte. Cela correspond au premier choix dans le menu du CD-ROM d'Ubuntu : « Essayer Ubuntu sans rien changer sur votre ordinateur ».

Fonctionnement : les fichiers essentiels d'Ubuntu sont copiés dans la mémoire vive (RAM) de l'ordinateur, puis Ubuntu est chargé depuis cette mémoire vive. Les fichiers non essentiels sont récupérés à la volée depuis le CD-ROM d'Ubuntu et copiés également en mémoire vive. Ceci a deux conséquences :

- Comme tout ce qui concerne Ubuntu ne se trouve qu'en mémoire vive et dans le CD-ROM d'Ubuntu, rien - absolument rien - du contenu des disques durs de l'ordinateur n'est modifié.

- Puisque la mémoire vive est une mémoire volatile, à la mise sous tension suivante de l'ordinateur, toutes les traces d'Ubuntu sont effacées.

De plus, puisque la plupart des fichiers non essentiels sont récupérés à la volée depuis le CD-ROM d'Ubuntu, une « session live » est nécessairement moins réactive qu'un système installé de manière permanente sur le disque dur. Cependant, la « session live » est un mode extrêmement pratique pour tester Ubuntu et ses outils, vérifier la compatibilité de son matériel et réparer un système corrompu.

Le CD-ROM d'installation d'Ubuntu est parfois appelé « Live CD », parce qu'il permet de charger une « session live » d'Ubuntu sur un ordinateur.

3.3 Installer avec le CD-ROM d'installation Ubuntu

En choisissant l'entrée de menu « Installer Ubuntu », l'installateur d'Ubuntu se charge directement. Il suffit ensuite de suivre les instructions à l'écran, telles que décrites ci-dessous :

- **Étape 1 :** Sélection de la langue

Choisir la langue dans laquelle on souhaite poursuivre l'installation. C'est aussi avec cette langue que le système sera paramétrée par défaut.

- **Étape 2 :** Emplacement géographique

Sélectionner le lieu de résidence. Cela permettra à Ubuntu de régler automatiquement l'horloge à l'heure locale, de se synchroniser régulièrement avec des serveurs de temps et d'ajuster l'heure aux passages à l'heure avancée d'été. Choisir ensuite la région dans la liste Région puis la ville de résidence dans le menu déroulant Ville.

- **Étape 3 :** Disposition du clavier

Paramétrer la disposition des touches du clavier. Par défaut, la disposition sélectionnée correspond à celle choisie pour la session live en cours. Pour définir une autre disposition de clavier, sélectionner d'abord le pays dans le menu de gauche. Puis, sélectionner un agencement de clavier dans le menu de droite.

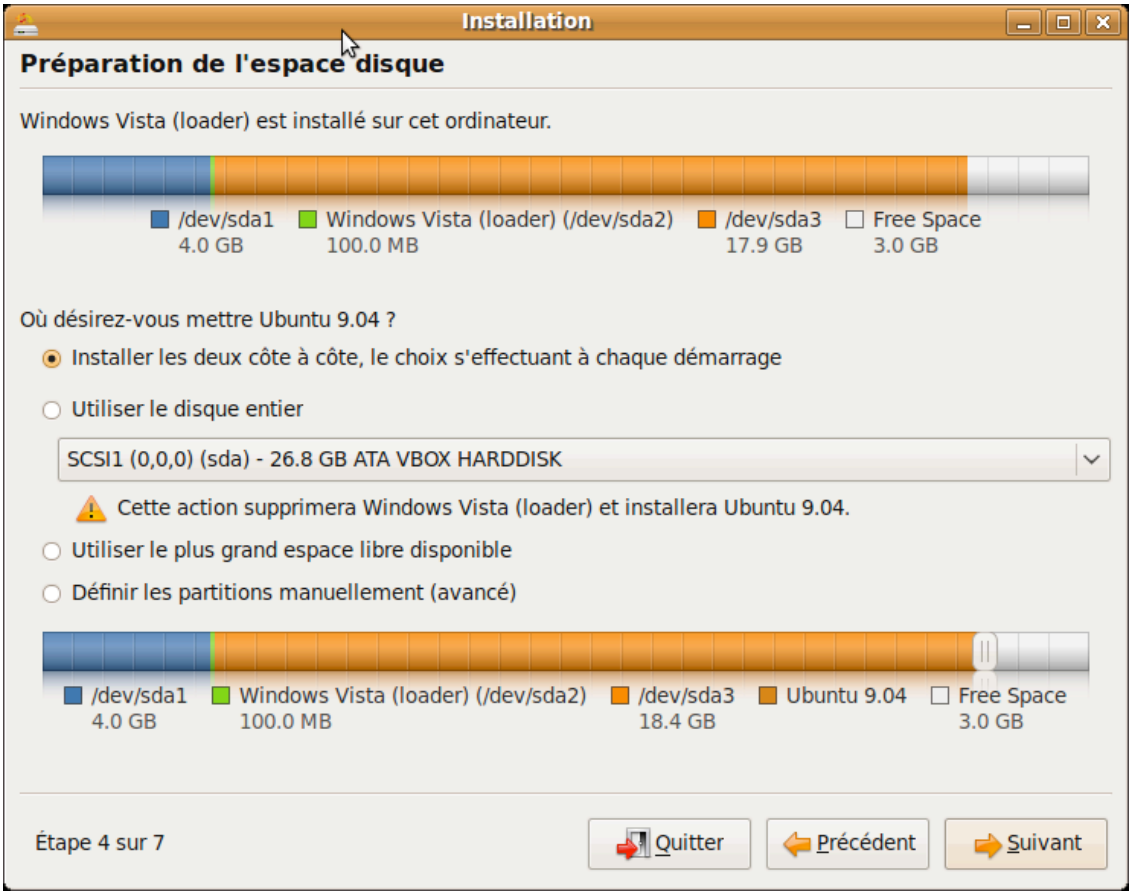
- **Étape 4 :** Partitionnement

Ubuntu ne peut pas être installé dans la même partition de disque dur qu'un autre système d'exploitation ; il doit avoir sa zone bien à lui. C'est donc ici qu'on définit où Ubuntu doit s'installer et quel espace on lui accorde.

La jauge du dessus affiche l'état actuel du disque dur principal et la jauge du bas, l'état qu'il aurait si on appliquait l'option de partitionnement sélectionné. Jusqu'à quatre options sont proposées :

- Installer les deux côte à côte, le choix s'effectuant à chaque démarrage : Cette option apparaît si au moins une partition existe sur le disque dur et que celle-ci contient un système d'exploitation. Elle redimensionne la partition disposant du plus grand espace non utilisé et installe Ubuntu dans l'espace qui sera libéré. Par défaut, l'installateur n'accorde aucun espace à Ubuntu. Se servir du curseur pour attribuer de l'espace à Ubuntu.

Noter que cette option fait fi de tout espace actuellement non alloué à une partition. Elle se contente de redimensionner une partition existante et installe Ubuntu uniquement dans l'espace disque qui vient d'être libéré.



- Utiliser le disque entier : Cette option permet de formater un disque dur entier et d'installer Ubuntu sur l'ensemble de ce disque.

Attention : Cette option efface toutes les données et tous les systèmes d'exploitation actuellement présents dans ce disque dur. Avec plus d'un disque dur, choisir le disque dur de son choix dans la liste proposée.

- Utiliser le plus grand espace disponible : Cette option apparaît si on dispose d'espace libre non alloué sur le disque dur. Par défaut, elle attribue automatiquement à Ubuntu tout l'espace qui n'est assigné à aucune partition, laissant intactes les partitions existantes. On ne voit pas cette option si tout l'espace de votre disque dur est attribué à des partitions, même si l'une d'entre elle est inutilisée ou non formatée. À l'aide du curseur, on peut réduire l'espace attribué à Ubuntu et même agrandir cet espace en empiétant celui d'une partition existante.

Si un système d'exploitation est présent dans une autre partition du disque dur, un multi-amorçage sera paramétré pour choisir de charger l'un ou l'autre des systèmes d'exploitation à la mise sous tension de l'ordinateur.

- Définir les partitions manuellement (avancé) : Cette option offre la plus grande flexibilité. Elle permet de redimensionner à loisir les partitions de son disque dur et d'en créer des nouvelles, aux tailles désirées, pour Ubuntu. C'est un mode qui est particulièrement utile pour les experts (détaillé

dans un chapitre spécifique).

- **Étape 5 :** Identité

Créer son compte utilisateur. Ce compte sera aussi paramétré comme étant administrateur du système Ubuntu.

Saisir son nom complet (il sera utilisé à quelques endroits, comme le client de courrier électronique), puis un identifiant (en anglais, login name) plus court.

Entrer un mot de passe, puis répéter ce même mot de passe pour le confirmer. Saisir un mot de passe est obligatoire. Ce mot de passe évitera que tout le monde puisse effectuer des tâches administratives sur l'ordinateur. Choisir un mot de passe fort (composé d'au moins 8 caractères variés contenant chiffres, lettres majuscules, lettres minuscules et caractères de typographie).

Spécifier un nom à donner à l'ordinateur : ce nom sera utilisé à l'intérieur du réseau domestique ou d'entreprise uniquement, afin de partager et accéder aux autres ordinateurs du réseau auquel on fait partie.

Enfin, choisir si une session utilisateur doit être automatiquement ouverte à chaque lancement d'Ubuntu, si la saisie du mot de passe utilisateur doit être obligatoire avant que la session s'ouvre, ou si la saisie du mot de passe est nécessaire pour ouvrir une session et déverrouiller l'accès aux données personnelles de compte.

- **Étape 6 :** Migrer des documents et des paramètres

Cette étape n'est proposée que si un ou des systèmes Microsoft Windows sont installés sur l'ordinateur et que des données peuvent en être importées. Un assistant permet d'importer les données de ses comptes utilisateur.

Rien n'est effacé du système Windows. Les données sont simplement dupliquées, afin d'être aussi exploitables depuis Ubuntu. De plus, tous les documents et paramètres seront importés dans le compte créé durant l'installation d'Ubuntu.

- **Étape 7 :** Confirmer l'installation et options avancées

Confirmer les réglages et démarrer l'installation. Attention : C'est la dernière possibilité pour arrêter la procédure d'installation sans rien modifier sur l'ordinateur.

Si l'installation est annulée à cette étape, aucun changement sur l'ordinateur n'est appliqué.

L'installation peut prendre quelques minutes selon la vélocité du matériel. Il est possible que, vers la fin de l'installation (vers 82%), le processus semble inactif si on est ou pas connecté à Internet (récupération de paquets supplémentaires).

Une fenêtre indiquera que l'installation est terminée et proposera alors de redémarrer l'ordinateur sur le nouveau système d'exploitation Ubuntu.

Mise en pratique : Installation d'Ubuntu sur le poste de travail.

4 Partitions et systèmes de fichiers

4.1 Généralités

Puisque les disques emmagasinent de grandes capacités de données, il est important d'organiser ces données de manière à y accéder rapidement. La partition est une zone du disque, définie par l'administrateur de l'ordinateur, dans laquelle doivent être contenues des données similaires : une partition système d'exploitation et logiciels, une partition données personnelles, une partition d'échange ou swap, etc.

À l'intérieur de la partition, un système de fichiers doit être créé. Celui-ci sert à organiser les données à l'intérieur d'une partition.

Un disque doit être divisé en au moins une partition (soit une zone d'organisation occupant la totalité de l'espace de stockage disponible). Un disque dur (dans les ordinateurs de type IBM-PC) ne peut d'ordinaire contenir qu'un maximum de 4 partitions (limite du MBR) : les partitions primaires.

Pour de nombreux administrateurs de systèmes GNU/Linux, cette limite est vite atteinte. Mais il est possible de transformer une partition primaire en une partition étendue. Une partition étendue est une sorte de conteneur à partitions. Dans ce conteneur, on peut créer des lecteurs logiques, des sous-partitions du conteneur. C'est ainsi que l'on procède pour s'affranchir de cette limitation des périphériques de stockage.

Pour être utilisable, une partition dans laquelle on enregistre directement des données doit être formatée. On doit doc attribuer un système de fichiers aux partitions primaires et aux lecteurs logiques. La partition étendue n'étant qu'un conteneur à partitions, elle n'a pas à être formatée.

4.2 Définitions pour Linux Ubuntu

Historiquement, les disques durs ou les lecteurs CD/DVD étaient nommés "hdX" ou "sdX" selon le type de branchement sur lesquels ils étaient branchés : dans le premier cas des nappes de type IDE, dans le second cas des nappes SCSI ou SATA. Depuis la version 6.06 d'Ubuntu, tous ces types de branchement sont confondus : peu importe le type de nappe utilisé, tous les disques durs sont nommés "sdX".

Dans la dénomination "sdX", la lettre X représente la nappe et la position sur laquelle est branché physiquement le disque dur :

- "a" pour le maître de la nappe IDE primaire ou l'ID0 du connecteur primaire SATA
- "b" pour l'esclave de la nappe IDE primaire ou l'ID1 du connecteur primaire SATA
- "c" pour le maître de la nappe IDE secondaire ou l'ID0 du connecteur secondaire SATA
- "d" pour l'esclave de la nappe IDE secondaire ou l'ID1 du connecteur secondaire SATA

Comme les partitions sont une partie d'un disque dur, elles sont nommées comme leur disque dur suivies d'un suffixe numérique représentant leur position sur le disque dur. Par exemple, "sda1" est la première partition du disque dur "sda" ; "sda2" est la seconde partition du disque dur "sda" ; "sdb1" est la première partition du disque dur "sdb" ; etc.

Quant à "/dev", il désigne un répertoire sous GNU/Linux qui est utilisé afin de communiquer avec ces partitions. Ainsi, "/dev/sda1" est un fichier qui permet d'interagir avec le contenu de la partition "sda1". Ceci est monté à l'aide de la commande Unix « mount ».

4.3 Format des partitions et systèmes de fichiers (outil GParted)

Formater une partition, c'est y créer un système de fichiers. Le formatage est une procédure qui consiste à créer un fichier d'index neuf (par des zéros) dans lequel viendront se loger les informations de localisation des données informatiques dans la partition.

De nombreux attributs différents sont nécessaires afin de définir un système de fichiers. Ils incluent entre autres la taille maximale que peut avoir un fichier dans ce système de fichiers, la taille maximale d'une partition et la journalisation ou non du système de fichiers.

- **ext2fs (Extended File System) :** Extended File System est le système de fichiers natif de Linux. Dans ses versions 1 et 2, on peut le considérer comme désuet car il ne dispose pas de la journalisation.
- **ext3fs :** ext3 est essentiellement ext2 avec la gestion de la journalisation (gestion de la corruption des fichiers par enregistrement intermédiaire et journal).
- **ext4fs :** ext4 est le successeur du système de fichiers ext3 (futur Btrfs).
- **FAT (File Allocation Table) :** Développé par Microsoft, ce système de fichiers se rencontre moins fréquemment aujourd'hui.
- **FAT32 :** Ce système de fichiers, aussi créé par Microsoft, est une évolution de son prédécesseur.
- **NTFS (New Technology File System) :** Ce système de fichiers a aussi été développé par Microsoft, et il reste très peu documenté.

Les systèmes de fichiers créés par Microsoft (FAT, FAT32 et NTFS) ne gèrent pas les droits d'accès aux fichiers comme les systèmes de fichiers de type Unix (ext2, ext3, etc). Il pourrait être possible d'installer Linux sur l'un de ces systèmes de fichiers, mais comme ils ne gèrent pas les droits d'accès, il en résulterait un système d'exploitation hautement non-sécurisé...

Pour l'échange de données entre systèmes Linux et Windows (lecture/écriture des partitions), il est alors nécessaire de passer par des pilotes comme « ntfs-3g » (Ubuntu), ou « Ext2IFS » et « Ext2fsd » (Windows).

4.4 Le swap

Le swap (parfois appelé mémoire virtuelle) est un espace réservé sur le disque dur servant à décharger la mémoire physique (RAM) lorsque celle-ci arrive à saturation. Le swap peut être un fichier, on parle alors de fichier d'échange, ou une partition dédiée à cet usage, on parle alors de partition d'échange. En général, il est conseillé de créer une partition swap complétant la mémoire vive, dont la taille est au moins de : 1 Gio moins la mémoire vive.

5 Vérification de fichiers et partitions (outil fsck)

5.1 Généralités

« fsck » est l'outil de contrôle d'intégrité et de réparation pour les systèmes de fichiers Linux. C'est un programme en mode console. Il se décompose en plusieurs sous-programmes, appelés automatiquement en fonction du type de la partition :

fsck.ext2 / fsck.minix / fsck.nfs / fsck.vfat / fsck.cramfs / fsck.ext3 / fsck.msdos / fsck.reiserfs / fstobdf

Si « fsck » est le marteau, le fichier « /etc/fstab » est l'enclume. La liste des partitions et les objets des vérifications s'y trouvent. Pour le consulter en ligne de commande :

cat /etc/fstab

L'outil « fsck » lance par défaut « e2fsck » qui ne vérifie que la ou les partitions de type « ext2 » et « ext3 ». En cas d'arrêt brutal notamment, « fsck » lancera une vérification au démarrage suivant. Tandis que l'outil « tune2fs » permet de configurer la fréquence des contrôles d'intégrité (via fsck), de changer le nom de la partition et bien d'autres choses.

Important : « fsck » ne doit être lancé que sur une partition non montée. En pratique, cela veut dire qu'il faut utiliser « fsck » à un stade premier du démarrage, antérieur au montage du système de fichiers.

5.2 Utilisation

Pour utiliser « fsck », il faut connaître au préalable le partitionnement du disque dur, à l'aide de l'outil GParted par exemple. Une fois la partition à examiner choisie, il faut obligatoirement la démonter pour la rendre non accessible. Remarque : on peut également faire le "check fsck" avec un Live CD.

Si la partition est "/dev/sda1", taper en ligne de commande :

sudo umount /dev/sda1

Puis lancer la vérification :

sudo fsck /dev/sda1

Si des corrections doivent être effectuées, « fsck » demande de les confirmer :

I-noeud 2392126, i_blocs est 192, devrait être 224. Corriger<o>? **oui**

 ***Mise en pratique : Vérifier une partition démontée à l'aide de l'outil « fsck ».***

6 Repartitionner un disque dur déjà équipé d'un système d'exploitation

Ce chapitre concerne la modification de partitions afin de libérer de la place pour l'installation d'Ubuntu sur un disque dur déjà équipé d'un autre système d'exploitation (Windows 2000, XP, Vista, etc).

6.1 Recommandations

Défragmenter les partitions Windows avant toute manipulation.

Sauvegarder les données importantes (sur CD, DVD, disque dur externe, etc).

Quelque soit l'outil de partitionnement utilisé, il vaut mieux créer des partitions Windows avec des outils Windows et des partitions Linux avec des outils Linux.

6.2 Ubuntu et Windows sur le même disque dur

- **Avec un seul disque dur :**

On prépare un espace libre qui va accueillir Ubuntu. Compter 4/6 Go minimum, 8/10 Go recommandé. On peut aller jusqu'à 10/15 Go, mais au-delà il vaut mieux créer une partition annexe (pour installer jeux, vidéos, musiques, documents,...). Exemple :

- 10-15 Go de / (pour la partition racine, contenant programmes et fichiers système)
- 10-300+ Go de données (sur une autre partition, lisible aussi bien par Windows que Linux)

- **Avec deux disques durs (Système/Partage) :**

C'est la solution de base si on possède 2 disques durs. Celle-ci est préférable dans la mesure où il ne faudra pas toucher à GRUB.

6.3 Pour Windows Vista

Windows Vista a des difficultés à être complètement redimensionné, même en utilisant le partitionneur « Maison ». Voici comment utiliser cet outil mis à disposition par Microsoft :

1) Ouvrir l'outil de partitionnement de Windows Vista : Ordinateur (clic-droit) => Gérer => Stockage (double-clic) => Gestion des disques. L'initialisation prend normalement un certain temps.

2) Cliquer sur la partition C: (ou autre) à modifier, puis sélectionner "Réduire le volume...". Choisir pour le champ "Quantité d'espace à réduire" l'espace à libérer pour Ubuntu, puis cliquer sur "Réduire".

3) Une fois la procédure terminée, fermer le programme.

Ce programme ne gère que les partitions de type NTFS (Windows), à utiliser exclusivement pour l'espace disque de Windows Vista. Par contre, utiliser l'outil GParted pour les partitions Linux.

Remarques :

- Par défaut, Windows ne défragmente pas les fichiers de plus de 64 Mo. Lancer "Defrag C: -W" pour forcer une défragmentation. Cela aidera à libérer de l'espace pour Linux (remplacer C: par l'identifiant du lecteur souhaité).

- Ne pas créer d'espace vide à l'intérieur d'une partition, mais bien de l'espace libre 'complet' (non alloué), c'est-à-dire non contenu dans une partition (souvent à la 'fin' du disque).

- Ne pas partitionner l'espace aménagé ici depuis Vista (partitions pour Ubuntu, /, /home, swap,...), car cela sera correctement préparé lors de l'installation Ubuntu dans l'espace vide créé.

6.4 Pour Windows XP

Cette méthode est réservée à Windows XP, car Windows Vista intègre déjà un partitionneur (voir paragraphe précédent).

- **Utiliser GParted depuis le Live CD d'Ubuntu :**

Gparted est un outil graphique d'Ubuntu relativement intuitif qui permet de créer, modifier et supprimer les partitions de son ou ses disques durs internes et externes. Pour l'utiliser :

1) Démarrer avec le Live CD.

2) Lancer l'outil GParted : Système => Administration => Éditeur de partition (GParted).

3) Agrandir la fenêtre.

4) En haut à droite, sélectionner le disque à repartitionner. Pour l'identifier, se baser sur sa taille.

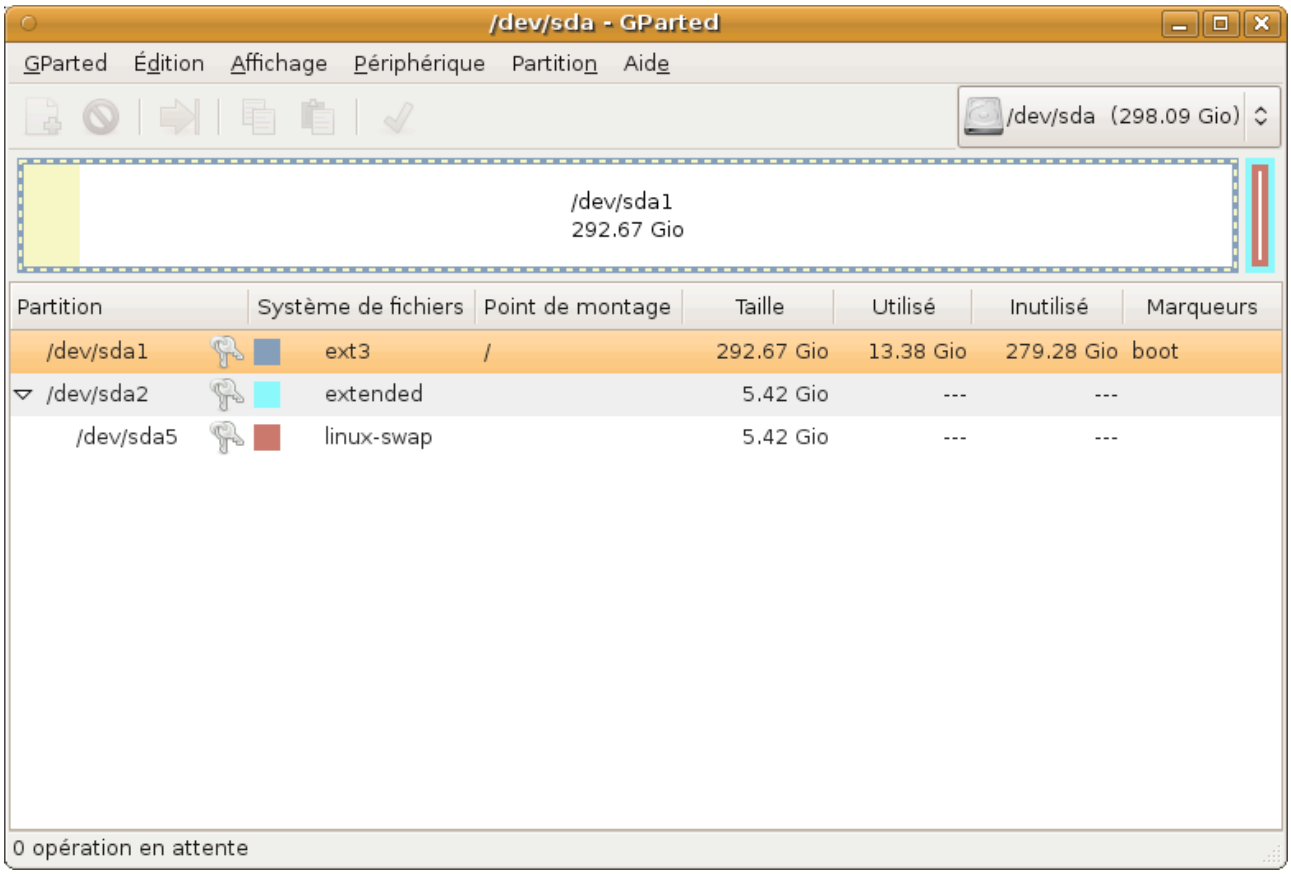
5) La(es) partition(s) du disque s'affiche(nt).

6) Choisir la partition à modifier et faire "Redimensionner" (clic droit).

7) Utiliser la réglette à l'aide de la souris pour diminuer l'espace de la partition principale.

8) Il reste un espace "non alloué", celui-ci sera occupé automatiquement par Ubuntu lors de son installation.

9) Pour appliquer les changements : Édition => "Appliquer toutes les opérations".



Si Windows Vista est installé sur le système, et que malgré les recommandations cette méthode a été utilisée, il se peut qu'il ne veuille plus démarrer. Une solution simple existe : l'outil « ntfsfix », ou sinon remettre en situation d'origine et recommencer en suivant les recommandations.

Mise en pratique : Tester le repartionnement avec GParted.

7 Sauvegarder le MBR du disque dur

7.1 Qu'est-ce que le MBR ?

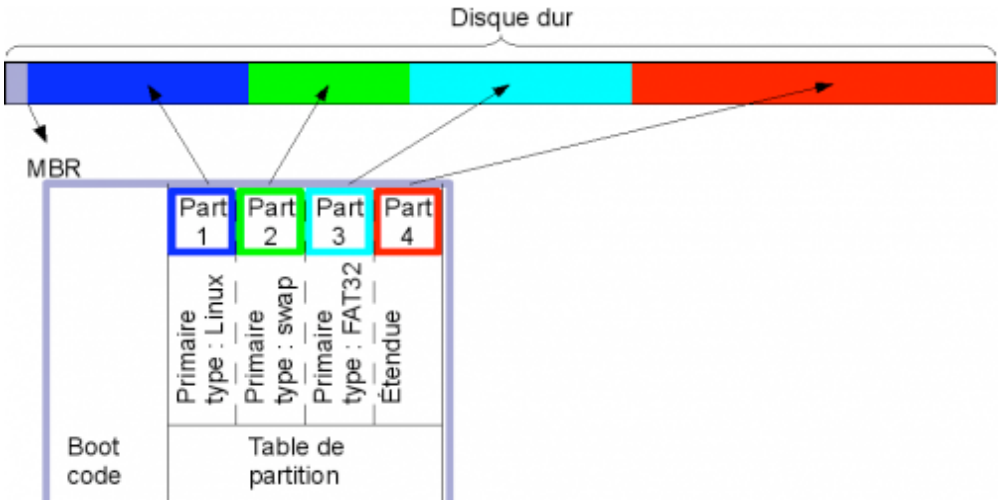
Le MBR est le premier secteur du disque. On trouve aussi au début de chaque partition étendue un EBR qui est son équivalent pour décrire les partitions logiques emboitées.

Le Master Boot Record, zone d'amorçage principale, est une zone de 512 octets découpés ainsi :

- Les 446 premiers octets sont le bootloader, code exécutable qui permet l'accès initial aux informations du disque ainsi que les messages d'erreur.

- Les 64 octets suivants contiennent l'arrangement du disque dur : la table des partitions (64 octets, soit 16 octets pour chacune des partitions primaires possibles : 4 max).

- Et enfin 2 octets 55AA signifiant que le secteur est amorçable.



Lors du démarrage de l'ordinateur, le BIOS scrute successivement les différents périphériques à la recherche de cette signature pour charger le secteur en mémoire.

Dans certains cas (manipulation hasardeuse des partitions, extinction brutale lors d'un redimensionnement, virus de MBR attrapé avec un autre OS,...), il arrive de perdre ces informations. Dans le meilleur des cas, une ou plusieurs partitions sont inaccessibles. Dans le pire des cas, le disque apparaît comme "non formaté".

Il suffit alors d'écrire à nouveau ce MBR en lieu et place de celui qui est corrompu. Encore faut-il en avoir fait une copie avant. Il est évident qu'un fichier de sauvegarde de ce type ne doit pas être conservé sur le disque qu'il faudrait réparer, mais sur un autre support de sauvegarde (CD, clé USB, etc).

7.2 Procédure de sauvegarde du MBR

1) Booter l'ordinateur sur un Live CD Ubuntu.

2) Choisir le mode Session Live permettant de tester Ubuntu sans rien changer à l'ordinateur.

3) Saisir dans un terminal la commande suivante qui va créer un fichier nommé mbr512.img dans le Dossier Personnel :

sudo dd if=/dev/sda of=~/mbr512.img bs=512 count=1

4) Copier ce fichier sur le support de stockage externe (disquette ou clé USB), ou se l'envoyer par e-mail. L'important est d'en avoir une copie de sauvegarde disponible au besoin.

7.3 Procédure de restauration du MBR

À partir d'un Live CD, copier le fichier à restaurer (mbr512.img) dans le Dossier Personnel, puis :

- Pour restaurer le MBR sans restaurer la table des partitions (par exemple si Windows a écrasé le menu GRUB), saisir dans un terminal :

sudo dd if=~/mbr512.img of=/dev/sda bs=446 count=1

- Pour restaurer le MBR et la table des partitions (par exemple en cas d'erreur lors du partitionnement du disque), saisir dans un terminal :

sudo dd if=~/mbr512.img of=/dev/sda bs=512 count=1

- Pour ne restaurer que la table des partitions (par exemple en cas d'erreur lors du partitionnement du disque et si l'on désire garder le bootloader que l'on a pu modifier), saisir dans un terminal :

sudo dd if=~/mbr512.img of=/dev/sda bs=1 skip=446 count=66

Mise en pratique : Sauvegarder puis restaurer le MBR du disque dur.

8 Démarrer Ubuntu en mode récupération (recovery mode)

8.1 Généralités

Le mode récupération (en anglais recovery mode) est une méthode de démarrage d'Ubuntu permettant d'effectuer certaines tâches d'administration et de récupération du système. Ce mode est très utile lorsqu'aucune session n'est en mesure d'être ouverte, ou lorsque le mot de passe du compte utilisateur principal est oublié afin de le réinitialiser.

Suivant le comportement normal d'Ubuntu, le mode récupération charge le système Ubuntu directement en session super-utilisateur (root session) sans nécessité de mot de passe.

Remarque :

Ceci représente une certaine vulnérabilité pour le système, car tout utilisateur ayant un accès physique à l'ordinateur peut démarrer en mode de secours. Dans un parc informatique avec un large accès d'utilisateurs (entreprise, bibliothèque, université, cybercafé, etc), l'administrateur du parc informatique doit bloquer l'accès au mode récupération autant que d'empêcher quiconque de démarrer un système à partir d'un CD-ROM ou d'un autre périphérique portable.

Conseil :

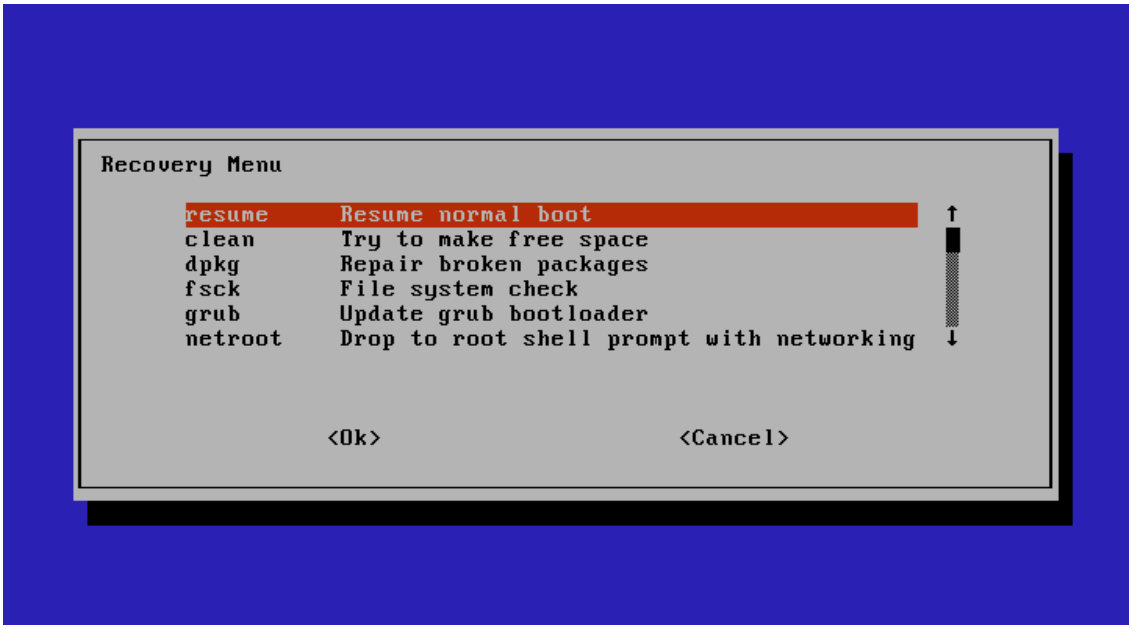
Pour empêcher un intrus de changer l'ordre de "boot" et démarrer sur un Live CD ou Live-USB par exemple (ce qui lui confère un équivalent des droits "root" sur la machine), il suffit de mettre un mot de passe au BIOS. Pour cela, il faut trouver "Administrator password" ou "Password" dans le menu du BIOS (l'interface change suivant les cartes-mères) et définir un mot de passe.

8.2 Démarrer le mode récupération

Le démarrage en mode récupération se choisit dans le menu d'amorçage du système d'exploitation (premières secondes de démarrage de l'ordinateur) : sélectionner la ligne "Ubuntu, kernel 2.6.x (recovery mode)", où x est la version la plus récente du noyau Linux installé sur l'ordinateur.

Remarque : Utiliser la touche [Echap] pendant la phase "GRUB Loading" pour accéder au menu d'amorçage du système.

8.3 Les options du mode récupération



- **resume :** Reprendre le chargement normal
- **clean :** Tenter de libérer de l'espace disque
- **dpkg :** Réparer les paquets brisés
- **fsck :** Vérification de l'intégrité des systèmes de fichiers
- **grub :** Mettre à jour le chargeur d'amorçage GRUB
- **netroot :** Ouvrir une session super-utilisateur avec gestion du réseau
- **root :** Ouvrir une session super-utilisateur
- **xfix :** Tenter de réparer les problèmes de session graphique

Mise en pratique : Démarrer et quitter Ubuntu en mode récupération.

9 Le chargeur d'amorçage GRUB

9.1 Généralités

GRUB (GRand Unified Bootloader) est un programme informatique permettant de charger un système d'exploitation. Il peut amorcer par lui-même des systèmes compatibles avec la norme POSIX (GNU/Linux, *BSD, Mac OSX, etc) et possède la capacité d'enchaîner vers un autre amorceur pour les systèmes non compatibles avec la norme POSIX (Microsoft Windows).

Le projet GRUB a créé un successeur : GRUB 2. Pour bien distinguer les deux logiciels, incompatibles entre eux, GNU GRUB a été renommé GRUB Legacy.

Pour éviter tout problème, il faut toujours installer GRUB sur la partition d'installation du système. De même, Il est fortement recommandé de ne pas installer GRUB sur le MBR, mais sur la racine de la partition (car cela pourrait rendre impossible le redémarrage de Windows en dual-boot). Sur un PC standard en dual-boot, on aura en général le schéma :

Grub a besoin d'un dossier /boot/ valide.
Son emplacement est défini lors de son installation

9.2 Fonctionnement

Le MBR (Master Boot Record) est le premier secteur du disque (512 octets). Il est chargé en mémoire par le BIOS à la mise sous tension de la machine. À cause de la faible taille du MBR, celui-ci contient seulement la première phase du programme GRUB qui va lui-même charger la suite du programme installé dans le dossier /boot/, jusqu'à ce que la totalité du noyau Linux soit chargé en mémoire. Ensuite, les différentes applications du système sont chargées par le noyau (gestionnaire de fenêtres, etc), jusqu'à ce que l'utilisateur se trouve devant son écran de login.

Le MBR ne pointe donc que sur un seul dossier /boot/.
La commande /sbin/grub-install est uniquement utilisée pour installer la première phase du programme GRUB dans le MBR (ou dans une partition). Inutile lors des mises à jour du GRUB.

9.3 Configuration GRUB Legacy

Les fichiers nécessaires au démarrage du système Linux Ubuntu se situent dans le répertoire /boot/ (à la racine), notamment les différents noyaux installés ou kernels.

Les fichiers relatifs au GRUB se situent dans le répertoire /boot/grub/, notamment son fichier de

configuration « menu.lst » et les différentes parties du programme (stage1, stage2,...).

La configuration des options et paramètres des démarrages systèmes se fait donc en éditant ce fichier texte : **sudo gedit /boot/grub/menu.lst**

Après modification d'un paramètre, il faut obligatoirement mettre à jour GRUB et « menu.lst » avec la commande (dans /sbin/) : **sudo update-grub**

Update-grub examine le répertoire /boot/ et y recherche tous les fichiers dont le nom commence par "vmlinuz-". Ces fichiers seront supposés constituer des noyaux et donneront lieu à des entrées dans le fichier « menu.lst ».

Update-grub, pour chacune des entrées introduites, ajoutera en outre les lignes « initrd » correspondant à chacun des noyaux identifiés sous forme d'images compressées (à partir de l'analyse du nom complet des fichiers commençant par "initrd" trouvés dans /boot/. Exemple : /boot/vmlinuz-2.6.22-14-generic et /boot/initrd.img-2.6.22-14-generic).

Remarques :

- Chaque entrée de noyau Ubuntu est doublée d'une entrée en mode "recovery" pour permettre certaines récupérations. Si la valeur est fixée à 1, deux entrées seront préservées : noyau en lancement "normal" et noyau en "mode recovery".
- Seules les entrées directement gérées par update-grub sont concernées, soient les entrées correspondant à des noyaux Linux (fichiers identifiés par un début de nom en vmlinuz, situés dans le répertoire /boot/). Les entrées spécifiques correspondant à memtest86+ ou aux entrées Windows ne sont pas concernées.
- Update-grub conserve les sections identifiant d'autres systèmes d'exploitation (Windows par exemple).

Rappel : Pour entrer dans le menu de GRUB, appuyer sur « Echap » au démarrage de la machine (phase "GRUB Loading"). Pour augmenter ce délai d'entrée, éditer « /boot/grub/menu.lst » puis augmenter le nombre de secondes dans la section timeout. Pour supprimer ce délai, ajouter un # en début de ligne (à éviter !).

9.4 Configuration GRUB 2 (grub-pc)

GRUB 2 est le chargeur d'amorçage installé par défaut avec Linux Ubuntu 9.10 et ultérieures. Par contre, en effectuant une mise à niveau d'une version antérieure d'Ubuntu vers la version 9.10, le chargeur d'amorçage est toujours GRUB Legacy.

Fichier utilisé par le système : /boot/grub/grub.cfg. Il est auto-généré par « update-grub » et ne doit pas être modifié manuellement. C'est lui qui est lu au démarrage comme l'était « menu.lst » avec GRUB Legacy (configuration similaire).

9.5 Exemple de configuration type

En général, la structure de « /boot/grub/menu.lst » est la suivante :

```
default N
timeout sec
color   couleur1 couleur2

# la configuration pour l'OS dont le Grub est installé

title          Le libellé d'OS
root            (hd<disque>,<partition>)
kernel          /boot/vmlinuz-2.x.x.xx root=/dev/hdLN options
initrd         /boot/initrd.img-2.x.x.xx

# à partir d'ici à éditer pour les autres OS

# pour la grande famille GNU/Linux
# pour chaque OS à ajouter dans Grub il faut écrire le bloc suivant

title          Le libellé d'OS supplementaires
root            (hd<disque>,<partition>)
kernel          /boot/vmlinuz-2.x.x.xx root=/dev/hdLN options
initrd         /boot/initrd.img-2.x.x.xx
rootnoverify    (hd<disque>,<partition>)

# pour la famille Windows

title          Le libellé d'OS
root            (hd<disque>,<partition>)
chainloader     +1
```

Mise en pratique : Visualiser et éditer un GRUB.

10 Le noyau du système d'exploitation Linux

10.1 Généralités

Un noyau de système d'exploitation (abrégé noyau, ou kernel en anglais, de l'allemand kern), est la partie fondamentale de certains systèmes d'exploitation tel Linux. Il gère les ressources de l'ordinateur et permet aux différents composants - matériels et logiciels - d'être reconnus et de communiquer entre eux.

Le noyau est le coeur du système, mais ne constitue pas la distribution complète. Celui-ci est composé d'un ou plusieurs fichiers et programmes présents dans /boot/.

Pour connaître la version de son noyau Linux, son nom, la version du compilateur utilisé, taper dans une console : **cat /proc/version**

Le noyau Linux est en constante évolution.

10.2 Versions

Chaque nouvelle version d'Ubuntu inclut le plus souvent une nouvelle version du noyau Linux par rapport à la précédente. Si cela permet de corriger des bugs et de proposer de nouvelles fonctionnalités, il arrive que cela entraine des régressions. Dans ce cas, on peut être amené à installer d'autres versions du noyau Linux, plus récentes ou plus anciennes.

Pour Ubuntu, plusieurs types de noyaux précompilés sont proposés :

- **generic :** le noyau est compilé avec les options nécessaires à une utilisation bureautique.
- **server :** le noyau est compilé avec les options nécessaires à une utilisation sur un serveur.
- **virtual :** le noyau est compilé avec les options nécessaires à une utilisation via une machine virtuelle.

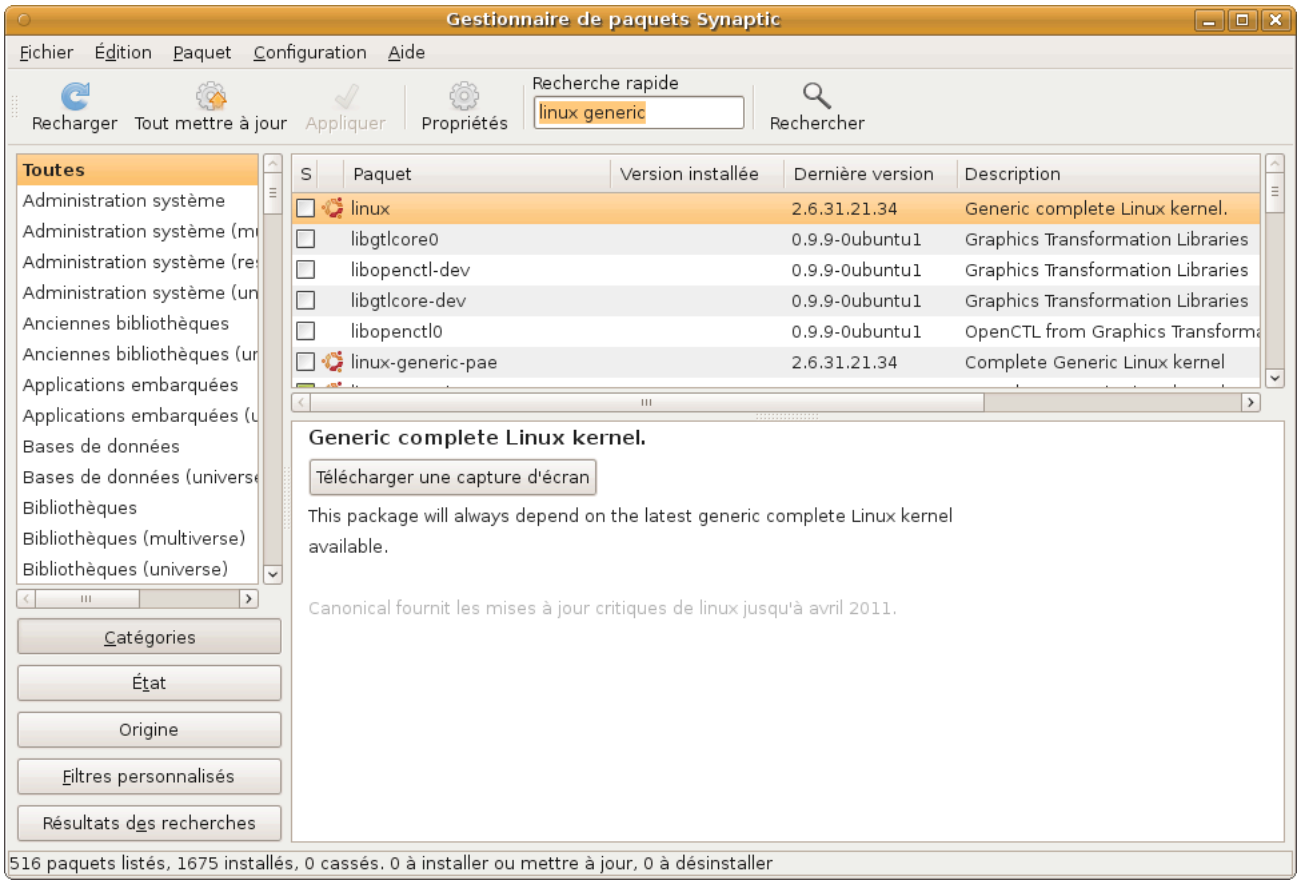
Rappel : Après l'installation, penser à mettre à jour le menu GRUB pour pouvoir choisir le nouveau noyau au démarrage (à l'aide de la commande « update-grub »).

10.3 Installation

Le noyau à installer doit être prévu pour la même architecture que celui déjà pré-installé. Le plus souvent il s'agit de l'architecture i386.

Pour certaines versions d'Ubuntu, plusieurs versions du noyau Linux sont disponibles dans les dépôts. Le paquet « linux-generic » (apt://linux-generic) pointe toujours sur la version la plus récente dans le dépôt.

Une version antérieure peut être installée en passant par le gestionnaire de paquets (Synaptic) et en cherchant les paquets souhaités « linux-image-<numéro_version>-generic » (mots clés : « linux generic »). La même installation peut être effectuée à l'aide de la commande « apt-get ».



La dernière possibilité est de télécharger les sources du noyau Linux soit depuis les dépôts, soit sur le site http://www.kernel.org, et de les compiler soi-même.

Pour se faire, de nombreuses options doivent être définies si l'on souhaite avoir un support complet du matériel. Plusieurs outils sont disponibles pour assister dans cette tache, de même que plusieurs tutoriels sur Internet.

Il est également possible de passer différents paramètres au noyau Linux en modifiant la ligne du menu GRUB. Pour connaître les différents paramètres possibles, consulter la page « kernel-parameters » sur kernel.org

***Mise en pratique* : Vérifier et télécharger la dernière version du noyau Linux.**

11 Logiciels fournis avec Ubuntu & Préférences Système

La distribution Ubuntu est fournie avec un certain nombre de logiciels gratuits, accessibles par défaut dans le menu « Applications » de l'environnement de bureau GNOME. En voici l'essentiel :

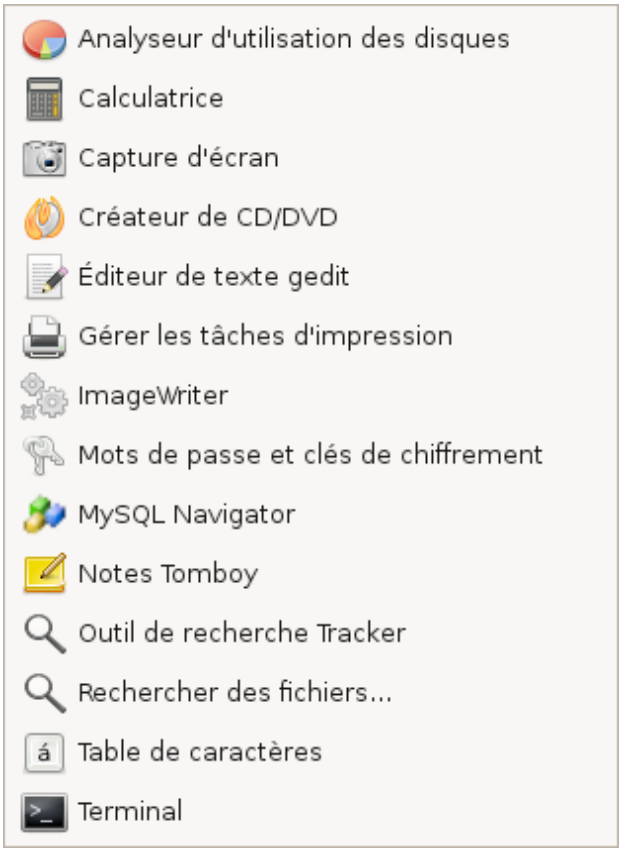
- **Navigation Internet :** Le navigateur par défaut sur Ubuntu est Firefox.
- **Bureautique :** La suite bureautique installée par défaut sous Ubuntu est la célèbre OpenOffice.org, existant aussi sous Windows et Mac OSX, compatible avec les documents créés par Microsoft Office (Word, Excel, PowerPoint, etc).
- **Navigateur de fichiers :** L'explorateur de fichiers par défaut sous Ubuntu s'appelle Nautilus. Il permet d'accéder facilement aux fichiers de l'ordinateur.
- **Fichiers compressés :** Le logiciel de compression/décompression intégré à Ubuntu s'appelle File-Roller, un clone de WinZip. Faire un clic-droit sur une archive (fichier ZIP par exemple) et choisir "Extraire ici" pour la décompresser. Par défaut, il ne supporte que les formats libres mais peut gérer les formats propriétaires (comme unrar pour le format rar).
- **Sécurité (antivirus et pare-feu) :** Pas besoin d'antivirus pour une utilisation standard d'Ubuntu (la sécurité est l'un des gros avantages des sytèmes Unix/Linux). De même, un pare-feu est déjà intégré à Ubuntu par défaut (accessible en Administration).
- **Lecture de musiques et vidéos :** Totem est le lecteur multimédia installé par défaut sur Ubuntu. Il est recommandé d'installer le lecteur VLC, ou encore MPlayer.
- **Gravure de CD :** Le logiciel de gravure par défaut est Brasero, pour CD et DVD.
- **Messagerie instantanée :** Pour discuter en temps réel avec vos contacts MSN, Yahoo, Jabber, ICQ, IRC, et autres, Ubuntu intègre par défaut un logiciel nommé Empathy. Pour utiliser la webcam avec le protocole MSN, il existe le logiciel aMSN.
- **Graphisme :** Le célèbre éditeur d'images GIMP est également fourni avec Ubuntu, tout comme le logiciel de modélisation 3D Blender.

Cette liste peut être largement complétée par la Logithèque Linux, toute aussi riche et professionnelle sur Ubuntu, accessible librement et gratuitement depuis Internet. Pour cela, utiliser l'outil « Applications / Logithèque Linux » ou le gestionnaire de paquets Synaptic.

A recommander :

Wine, un programme permettant d'utiliser des logiciels écrits pour Microsoft Windows sur d'autres systèmes d'exploitation sans installer Windows (disponible pour Linux, BSD, Solaris et Mac OSX). Wine est un acronyme signifiant "Wine Is Not an Emulator" (Wine n'est pas un émulateur).

De nombreux outils et accessoires sont également disponibles depuis le menu « Applications / Accessoires » :



Remarque : Sur Ubuntu, Gedit est l'éditeur de prédilection pour l'écriture de fichiers texte brut (fichiers systèmes, scripts Shell,...). Gedit peut-être remplacé par l'éditeur Nano en mode texte.

- **Utiliser le menu Système / Préférences :**

Ubuntu fournit une vaste palette d'applications faciles à utiliser pour permettre aux utilisateurs de personnaliser leur bureau selon leurs exigences particulières :

Affichage / Apparence / Applications au démarrage / Applications préférées / À propos de moi / Bluetooth / Bureau à distance / Clavier / Connexions réseau / Contrôleur de volume / Économiseur d'écran / Fenêtres / Gestionnaire de fichiers / Gestion d'énergie / Imprimante par défaut / Menus et barres d'outils / Périphériques Palm OS / Raccourcis clavier / Sélecteur du système multimédia / Serveur Mandataire / Souris / ...

***Mise en pratique* : Découverte des logiciels et des préférences Ubuntu.**

12 Le gestionnaire de paquets

12.1 Généralités

Le gestionnaire de paquets est un système qui permet d'installer des logiciels, de les maintenir à jour et de les désinstaller. Son travail est de n'utiliser que des éléments compatibles entre eux, les installations sans utiliser de gestionnaire de paquets sont donc déconseillées.

Un paquet est un bout de logiciel prêt à être installé (package en anglais), une sorte d'archive. Dont on peut établir les besoins, les compatibilités et les incompatibilités. C'est la plus petite unité d'agencement au sein du système Ubuntu, comme une brique élémentaire.

Un logiciel courant est généralement proposé sous forme de plusieurs paquets, selon les besoins de compatibilité, les imbrications et les agencements envisagés.

Un dépôt est l'endroit où sont stockés les paquets (serveur). Sous Ubuntu, il existe 4 dépôts principaux pour séparer les paquets libres ou non, et soutenus par Ubuntu ou pas :

	libre	**non libre**
soutenu	main	restricted
non soutenu	universe	multiverse

Par défaut, seuls les dépôts des paquets soutenus par Ubuntu sont activés. Pour activer « Universe » et « Multiverse », il faut cocher les cases correspondantes dans « Sources de logiciels » (Système => Administration).

Pour ajouter et supprimer des paquets, il existe donc des programmes. Certains utilisent les interfaces graphiques, d'autres des outils en ligne de commande.

Remarque : Le « Gestionnaire de mises à jour » (Système => Administration) est l'outil graphique qui s'occupe de la mise à jour complète du système par rapport à la sélection des paquets déjà installés sur celui-ci. Il peut être paramétré et planifié.

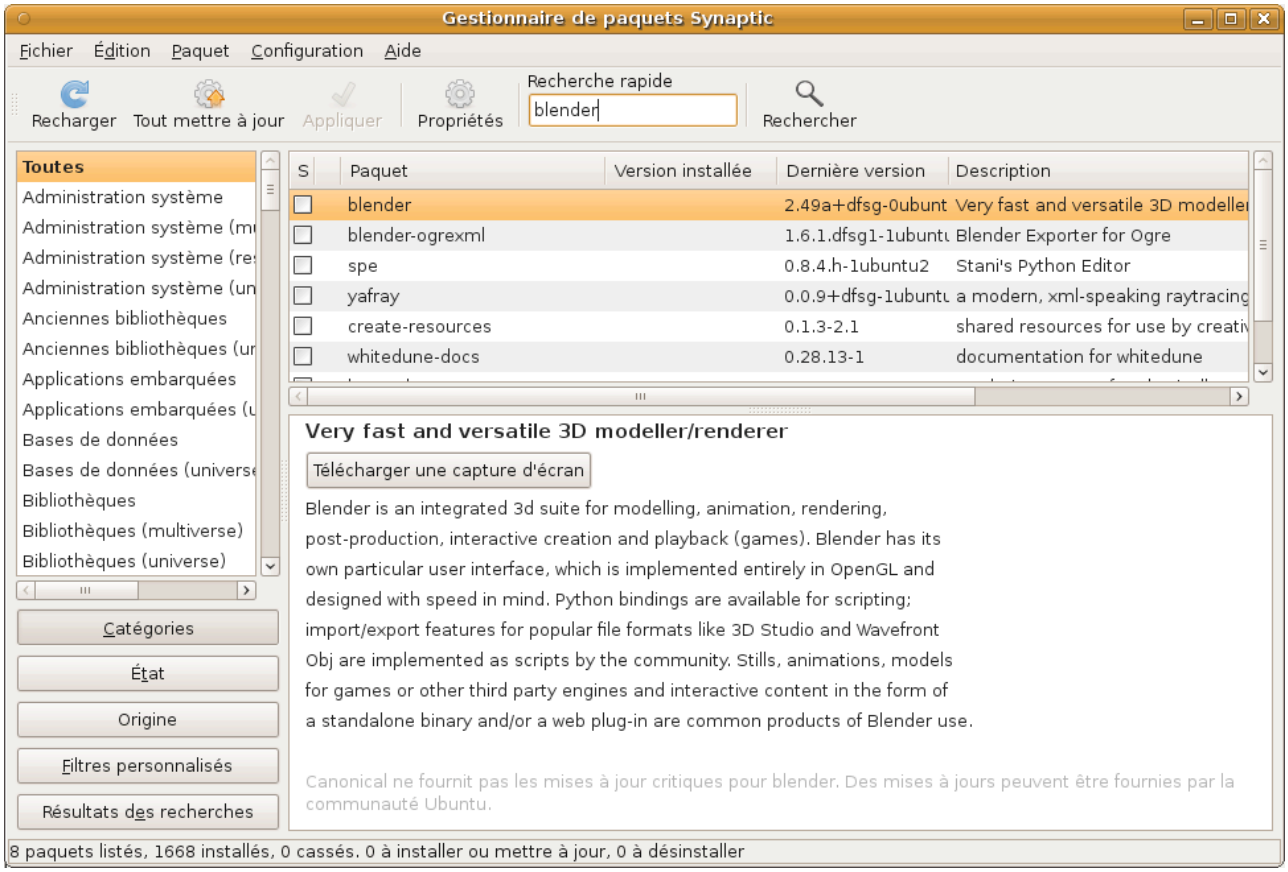
12.2 Par l'interface graphique (outil Synaptic)

Il existe plusieurs outils graphiques pour le système de gestion de paquets. Ils sont, suivant le cas, orientés pour une utilisation très simple et intuitive ou, au contraire, avancée. Chaque interface s'intègre à un environnement GNOME, KDE ou Xfce.

Remarque : L'arrivée de la version 9.10 d'Ubuntu (Karmic) introduit un tout nouveau système graphique qui unifie les solutions décrites ci-dessous : la « Logithèque Ubuntu » avec interface unique et tout en un (menu « Applications »).

- **Le gestionnaire de paquets « Synaptic » :**

Le « Gestionnaire de paquets Synaptic » se trouve dans le menu Système => Administration. Le système demande d'abord de confirmer son mot de passe. Cette sécurité est prévue pour éviter que n'importe quel utilisateur installe (ou désinstalle) n'importe quoi sur la machine.



Dans la fenêtre principale, on retrouve les actions exécutables dans la barre d'outils en haut. Les catégories de logiciels, à gauche, et la liste des paquets (applications et bibliothèques) disponibles à l'installation depuis les dépôts APT configurés, à droite, occupent la majeure partie de l'interface. Chaque application est précédée d'un carré indiquant le statut actuel du paquet :

- **vert** = installé
- **rouge** = cassé
- **blanc** = non installé

12.3 En ligne de commande (outil apt-get)

Apt-get est un outil à utiliser en ligne de commande, à l'aide du terminal Linux. Il permet d'effectuer l'installation et la désinstallation facile de paquets en provenance d'un dépôt APT. Il faut disposer des droits d'administration (sudo).

Installation simple :

sudo apt-get install <paquet(s)>

Installation avec réponse « oui » :

sudo apt-get install -y <paquet(s)>

Forcer une installation :

sudo apt-get -f install

Trouver un paquet (dépend des dépôts configurés) :

apt-cache search <word1 word2 ...>

Obtention des codes sources (dans dossier personnel) :

apt-get source <paquet(s)>

Suppression de paquets (autoremove = avec dépendances logicielles) :

sudo apt-get remove <paquet(s)>

sudo apt-get autoremove <paquet(s)>

Suppression + purge (paquets indiqués + leurs fichiers de configuration) :

sudo apt-get remove --purge <paquet(s)>

sudo apt-get autoremove --purge <paquet(s)>

Nettoyage « à zéro » des paquets à récupérer (libérer de l'espace disque) :

sudo apt-get clean

sudo apt-get autoclean (que les obsolètes)

Mise à jour dépôts (d'après le fichier de configuration /etc/apt/sources.list) :

sudo apt-get update

Mise à jour paquets (vers les dernières versions) :

sudo apt-get upgrade

sudo apt-get dist-upgrade (que le nécessaire)

Bloquer la mise à jour d'un paquet :

Insérer les lignes suivantes dans le fichier texte /etc/apt/preferences (le créer si inexistant) :

Package: nom du paquet
Pin: version du paquet à conserver (ex : version 0.8.8)
Pin-priority: 1001

La priorité du pin à 1001 bloque les futures mises à jour.

Obtenir la liste des derniers paquets installés sur le système :

cat /var/log/dpkg.log

 ***Mise en pratique : Rechercher et installer des paquets avec Synaptic et apt-get.***

13 Arborescence des répertoires à la racine de Linux Ubuntu

La liste standard (norme Unix/FHS) des répertoires à la racine du système Linux Ubuntu est obtenue par la commande « ls -la / » :

Répertoire	Contenu
/	Racine du système
/bin	Exécutables des commandes essentielles
/boot	Fichiers statiques du chargeur d'amorçage
/dev	Fichiers spéciaux des périphériques
/etc	Fichiers de configuration
/home	Répertoires personnels des utilisateurs
/lib	Bibliothèques partagées essentielles et modules du noyau
/media	Contient les points de montages pour les médias amovibles
/mnt	Point de montage pour monter temporairement un système de fichiers
/proc	Répertoire virtuel pour les informations système (noyaux 2.4 et 2.6)
/root	Répertoire personnel du super-utilisateur
/sbin	Exécutables système essentiels
/srv	Données pour les services du système
/tmp	Fichiers temporaires
/usr	Hiérarchie secondaire
/var	Données variables et diverses
/opt, /usr/local	Paquets pour applications supplémentaires, installées hors gestionnaire de paquets

Mise en pratique : Visualiser l'essentiel des répertoires à la racine du système.

14 Les commandes de base en mode console

Accéder au Terminal et au Shell Unix depuis le menu de l'environnement graphique Ubuntu :

« Applications / Accessoires / Terminal »

Rappel : La syntaxe générale d'une commande Unix est : **cde_-opt(s)_arg1_arg2_...**

Commande « man » : manuel

> Affiche les pages du manuel système.

Chaque argument donné a man est généralement le nom d'un programme, d'un utilitaire ou d'une fonction.

> Ex :

man man

Affiche les informations pour l'utilisation de man ('q' pour quitter).

Commande « ls » : list segment

> Permet de lister un répertoire.

> Options :

-l : Permet un affichage détaillé du répertoire (permissions d'accès, le nombre de liens physiques, le nom du propriétaire et du groupe, la taille en octets, et l'horodatage).

-h : Associé avec -l affiche la taille des fichiers avec un suffixe correspondant à l'unité (K, M, G).

-a : Permet l'affichage des fichiers et répertoires cachés (ceux qui commencent par un . (point)).

> Ex :

ls -a

Affiche tous les fichiers et répertoires cachés du répertoire courant.

ls /etc/

Affiche le contenu du répertoire /etc/.

Commande « pwd » : print working directory

> Affiche le répertoire en cours depuis la racine.

Commande « cd » : change directory

> Permet de se promener dans les répertoires.

> Ex :

cd

Permet de revenir au répertoire /home/utilisateur (identique à cd ~).

cd -

Permet de revenir au répertoire précédent.

cd ..

Permet de remonter au répertoire parent.

cd /

Permet de remonter à la racine de l'ensemble du système de fichiers.

cd /usr/bin/

Se place dans le répertoire /usr/bin/.

Commande « cat » : concatenate

> Affiche le contenu d'un fichier.

> Options :

-n : Affiche les numéros de ligne.

-v : Affiche les caractères de contrôles.

> Ex :

cat -n monFichier

Affiche monFichier en numérotant les lignes à partir de 1.

cat > monFichier

Ecrit dans monFichier (CTRL+D pour sauver).

Commande « more » : plus

> Affiche un fichier page par page.

> Options :

-s : Regroupe les lignes vides consécutives en une seule.

-f : Ne coupe pas les lignes longues.

> Ex :

more -sf monFichier

Affiche monFichier page par page en concaténant les lignes vides sans compter les lignes longues.

Commande « mv » : move

> Permet de déplacer ou renommer des fichiers et des répertoires.

> Options :

-f : Ecrase les fichiers de destination sans confirmation.

-i : Demande confirmation avant d'écraser.

-u : N'écrase pas le fichier de destination si celui-ci est plus récent.

> Ex :

mv monFichier unRep/

Déplace monFichier dans le répertoire unRep.

mv unRep/monFichier

Déplace le fichier monFichier du répertoire unRep là où on se trouve.

mv unRep monRep

Renomme unRep en monRep.

Commande « cp » : copy

> Permet de copier des fichiers ou des répertoires.

> Options :

-a : Archive. Copie en gardant les droits, dates, propriétaires, groupes, etc.

-i : Demande une confirmation avant d'écraser.

-f : Si le fichier de destination existe et ne peut être ouvert alors le détruire et essayer à nouveau.

-r : Copie un répertoire et tout son contenu.

-u : Ne copie que les fichiers plus récents ou qui n'existent pas.

-v : permet de suivre les copies réalisées en temps réel.

> Ex :

cp monFichier sousrep/

Copie monFichier dans sousrep.

cp -r monRep/ ailleurs/

Copie le répertoire monRep vers ailleurs en créant le répertoire s'il n'existe pas.

Commande « rm » : remove

> Permet d'effacer des fichiers.

> Options :

-f : Ne demande pas de confirmation avant d'effacer.

-r : Efface récursivement les fichiers ainsi que les répertoires.

> Ex :

rm CeFichier

Efface le fichier CeFichier.

rm -rf /tmp/LeRep

Efface le répertoire /tmp/LeRep ainsi que tous ses fichiers sans demander de confirmation.

Commande « mkdir » : make directory

> Crée un répertoire vide.

> Options :

-p : Crée les répertoires parents s'ils n'existent pas.

> Ex :

mkdir photos

Crée le répertoire photos.

mkdir -p photos/2005/noel

Crée le répertoire noel et, s'ils n'existent pas, les répertoires 2005 et photos.

Commande « rmdir » : remove directory

> Supprime un répertoire (vide).

> Options :

-p : Supprime les répertoires parents s'ils deviennent vides.

> Ex :

rmdir LeRep

Supprime le répertoire LeRep.

Commande « ln » : link

> Crée un lien (physique ou symbolique) vers un fichier (ou un répertoire).

> Options :

-s : Crée un lien symbolique (similaire au raccourci Windows).

-f : Force l'écrasement du fichier de destination s'il existe.

-d : Crée un lien sur un répertoire (uniquement en mode sudo ou root).

> Ex :

ln -s Rep1/Rep2/Monfichier MonLien

Crée un lien symbolique MonLien de Rep1/Rep2/Monfichier dans le répertoire où on se trouve.

ln Monfichier unRep/AutreNom

Crée un lien physique AutreNom de Monfichier dans le répertoire unRep.

> Notes :

Vérifiez que vous vous trouvez bien dans le répertoire dans lequel vous souhaitez créer le lien avant de faire cette commande.

Commande « find » : rechercher

> Permet de chercher des fichiers et éventuellement d'exécuter des commandes sur ceux-ci ; la recherche est récursive c'est-à-dire qu'elle concerne le répertoire de départ et toute sa descendance.

> Options :

-name : Recherche d'un fichier par son nom.

-iname : Même chose que name mais insensible à la casse.

-type : Recherche de fichier d'un certain type.

-atime : Recherche par date de dernier accès.

-mtime : Recherche par date de dernière modification.

-link : Recherche du nombre de liens au fichier.

-user : Recherche de fichiers appartenant à l'utilisateur donné.

-group : Recherche de fichiers appartenant au groupe donné.

> Ex :

find monfichier*

Recherche un fichier commençant par "monfichier".

find *monfichier*.ogg

Recherche un fichier contenant "monfichier" et ayant pour extention ".ogg".

find /home/ -name monfichier

Recherche le fichier monfichier dans toute la descendance de /home/.

find . -name "*.c"

Recherche tous les fichiers ayant une extension '.c' depuis le répertoire courant.

Commande « grep » : global regular expression print

> Recherche une chaîne de caractères dans des fichiers (ou depuis la console si aucun fichier n'est indiqué) ; Souvent utilisé en filtre avec d'autres commandes.

> Options :

-c : Retourne le nombre de lignes au lieu des lignes elles mêmes.

-n : Retourne les lignes préfixées par leur numéro.

-i : Insensible à la casse.

-r : Recherche récursivement dans tous les sous-répertoires ; On peut utiliser la commande rgrep.

-G : Recherche en utilisant une expression rationnelle basique (option par défaut).

-E : Recherche en utilisant une expression rationnelle étendue ; On peut utiliser la commande egrep.

-F : Recherche en utilisant une chaîne fixe ; On peut utiliser la commande fgrep.

> Ex :

grep -n montexte monfichier

Retourne toutes les lignes ainsi que leur numéro ou montexte apparait dans monfichier.

Commande « chmod » : change mode

> Modifie les permissions d'accès à un fichier ou à un répertoire.

Type d'autorisations (une autorisation d'exécution sur un répertoire autorise son ouverture) :

+ : Ajoute une permission.

- : Enlève une permission.

= : Autorise uniquement l'autorisation indiquée.

r : Lecture ; Valeur octale 4.

w : Ecriture ; Valeur octale 2.

x : Execution ; Valeur octale 1.

s : Utilise les droits du propriétaire ou du groupe lors de l'exécution.

u : Propriétaire du fichier.

g : Groupe propriétaire du fichier.

o : Tous les autres utilisateurs.

> Options :

-R : Récursif, modifie les autorisation d'un répertoire et tout ce qu'il contient.

-c : Ne montrer que les fichiers ayant été réellement modifiés.

-f : Ne pas afficher les messages d'erreur.

> Ex :

chmod ugo+x monRep

Ajoute l'exécution (ouverture) du répertoire monRep à tous (propriétaire, groupe, autres).

chmod go-wx monRep

Supprime l'autorisation de lecture et d'écriture de monRep au groupe et aux autres.

chmod u=rw,go=r MonFichier

Fixe l'autorisation de lecture et d'écriture au propriétaire de MonFichier et une autorisation de lecture au groupe et aux autres.

chmod 644 MonFichier

Exactement la même chose que ci-dessus mais en utilisant les valeurs octales (Nota : 6 = 4+2 = lecture + écriture).

chmod u=rw,g=r,o= MonFichier

Fixe l'autorisation d'ouverture et de lecture de MonFichier au propriétaire, uniquement la lecture au groupe et interdit tout accès aux autres.

chmod 640 MonFichier

Exactement la même chose que ci-dessus mais en utilisant les valeurs octales.

Commande « chown » : change owner

> Change le propriétaire et le groupe propriétaire d'un fichier.

> Options :

-R : Modifie récursivement un répertoire et tout ce qu'il contient.

> Ex :

chown autreUtilisateur MonFichier

Change le propriétaire de MonFichier en autreUtilisateur.

chown -R lui:nous monRep

Change le propriétaire en lui et le groupe propriétaire en nous du répertoire monRep ainsi que tout ce qu'il contient.

Commande « chgrp » : change group

> Change le groupe propriétaire d'un fichier.

> Options :

-R : Change récursivement un répertoire et tout ce qu'il contient.

-h : Change le groupe propriétaire d'un lien symbolique et seulement lui (ne touche pas à la destination du lien).

-L : Si fournie avec R , change le groupe propriétaire d'un répertoire et des fichiers qu'il contient s'il est pointé par un lien symbolique rencontré lors de l'exécution.

> Ex :

chgrp unGroupe MonFichier

Change le groupe propriétaire du fichier MonFichier en unGroupe.

chgrp -R unGroupe monRep

Change le groupe propriétaire du répertoire monRep ainsi que tout ce qu'il contient en unGroupe.

Commande « sudo » : substitute user do

> Permet d'exécuter des commandes en tant que super-utilisateur (administrateur root), en précisant le mot de passe de l'utilisateur courant. Nécessaire pour toutes les tâches d'administration système.

> Options :

-s : Importe les variables d'environnement du shell.

-k : Lorsque l'on utilise sudo, garde en mémoire le mot de passe. Cette option déconnecte l'utilisateur et forcera à redemander un mot de passe si sudo est exécuté avant le timeout défini.

> Ex :

$ sudo reboot

Lance la commande reboot avec les droits de l'utilisateur root.

Commande « ps » : processes snapshot

> Affiche les processus en cours.

> Options :

-u : Affiche les processus de l'utilisateur qui exécute la commande.

-au : Affiche les processus de tous les utilisateurs.

-aux : Affiche l'intégralité des processus du système. Équivalent à ps -A

-faux : Affiche tous les processus du système en les regroupant par enchaînement d'exécution.

> Ex :

ps -u

Tous les processus de l'utilisateur courant.

ps -aux

Tous les processus en cours.

Commande « kill » / « killall » : kill / kill all (tuer / tuer tous)

> Permet d'envoyer un signal à un processus ; kill ne comprend que les PID (Process Identifier, numéro d'ordre du processus), killall quant à lui comprend le nom du processus.

> Options :

-s : Indique quel signal s à envoyer au processus ; Le signal peut être identifié soit par son nom (exemple : SIGTERM) soit par son numéro (exemple : 9) ; Cette option peut être remplacée par le numéro du signal : -s 9 est équivalent à -9.

-l : Affiche la liste des signaux connus.

> Les signaux les plus courants sont :

HUP signal 1 : signal de fin d'exécution ou le processus doit relire son fichier de configuration.

TERM signal 15 : Le signal Terminate indique à un processus qu'il doit s'arrêter.

KILL signal 9 : Le signal Kill indique au système qu'il doit arrêter un processus qui ne répond plus.

> Ex :

kill -15 14774 : Envoie le signal 15, ou TERM, au processus ayant le numéro 14774 ce qui a pour effet de terminer proprement le processus.

kill -9 7804 : Envoie le signal 9, ou KILL, au processus ayant le numéro 7804 ce qui a pour effet de tuer le processus.

killall -TERM firefox-bin : Envoie le signal TERM, ou 15, au processus firefox-bin ce qui a pour effet de le fermer.

> Il est conseillé de lancer des signaux de faible importance avant de lancer la grosse artillerie. En pratique, tester dans l'ordre et deux fois chacune de ces commandes :

kill pid (envoie le signal 15, TERM)

kill -INT pid (envoie le signal 2, INT)

kill -KILL pid (envoie le signal 9, KILL)

Commande « su » : substitute user

> Changer de session utilisateur sans nécessairement se déconnecter de sa session graphique courante. Sous Ubuntu, le compte système root est bloqué (su root : impossible).

> Ex :

su NomUSER

Ouvre une nouvelle session sous l'utilisateur NomUSER après avoir saisi son mot de passe.

Commande « passwd » : password

> Permet de modifier le mot de passe d'un utilisateur.

> Options :

-S : Affiche l'état d'un compte (nom du compte, bloqué (L), si l'utilisateur n'a pas de mot de passe (NP) ou a un mot de passe utilisable (P), date de dernière modification du mot de passe, durée minimum avant modification, durée maximum de validité, durée d'avertissement, durée d'inactivité autorisée).

> Ex :

passwd NomUser

Demande à changer le mot de passe de l'utilisateur NomUSER.

Commande « groups » : groups

> Affiche les groupes auxquels appartient un utilisateur.

> Ex :

groups

Affiche la liste des groupes auxquels appartient l'utilisateur ayant tapé la commande.

groups NomUSER

Affiche tous les groupes auxquels appartient l'utilisateur NomUSER.

Commande « groupadd » : add group

> Crée un nouveau groupe utilisateurs.

> Ex :

groupadd NomGROUPE

Crée le nouveau groupe utilisateurs NomGROUPE.

Commande « adduser » : add user

> Ajoute un utilisateur, ou un groupe, au système.

> Options :

--disabled-login : Empêche l'utilisateur de se connecter.

--disabled-password : Un peu comme </del>disabled-login sauf qu'il est possible de se connecter via une clé RSA SSH, pratique pour créer un utilisateur qui ne se connectera que via SSH.

--system : Crée un utilisateur système.

--group : Avec --system crée un groupe avec le même ID que l'utilisateur système, sans un groupe avec le nom donné sera créé.

--home : Permet de fixer le répertoire HOME de l'utilisateur.

--no-create-home : Ne crée pas de répertoire HOME.

> Ex :

adduser NomUSER

Crée l'utilisateur NomUSER.

adduser --disabled-password --no-create-home UserSSH

Crée un utilisateur UserSSH sans mot de passe qui ne pourra pas se connecter directement sur la machine et sans lui créer de répertoire home.

adduser --disabled-password --home /home/NomUSER NomUSER

Même chose qu'au dessus sauf qu'on lui donne le même répertoire HOME qu'à l'utilisateur NomUSER créé en premier.

adduser seb lpadmin

Ajoute l'utilisateur seb (créé préalablement) dans le groupe "lpadmin".

adduser anna --ingroup users

Crée l'utilisateur anna et l'ajoute au groupe "users".

Commande « deluser » : delete user

> Supprime un utilisateur du système.

> Option :

--system : Ne supprime l'utilisateur que si c'est un utilisateur système.

--remove-home : Supprime l'utilisateur ainsi que son répertoire dans le home.

> Ex :

deluser UserSSH

Supprime l'utilisateur UserSSH.

deluser --remove-home bob

Supprime l'utilisateur bob ainsi que le répertoire /home/bob.

deluser seb lpadmin

Supprime l'utilisateur seb du groupe "lpadmin".

Commande « usermod » : user modification

> Modifie le groupe d'appartenance d'un utilisateur.

> Options :

-G, --groups GROUPE1[,GROUPE2,...[,GROUPEN]]] : Ajouter l'utilisateur aux groupes précédents. Si l'utilisateur fait actuellement partie d'un groupe qui n'est pas listé, l'utilisateur sera supprimé du groupe. Ce comportement peut être changé avec l'option -a, qui permet d'ajouter l'utilisateur à une liste de groupes supplémentaires.

> Ex :

usermod -aG toto machin

Ajoute l'utilisateur machin au groupe toto sans supprimer machin de son groupe originel.

sudo usermod -d /home/nouveau_login -m -l nouveau_login ancien_login

Permet de renommer le répertoire (dossier) utilisateur et de changer son nom. Pratique lorsque le pc change de mains.

Commande « uname » : unix name

> Affiche des informations sur le système.

> Options :

-s : Affiche le nom du noyau.

-n : Affiche le nom de la machine (hostname).

-r : Affiche la révision du noyau.

-v : Affiche la version du noyau.

-m : Affiche le type de processeur de la machine (i386, i686, etc.).

-o : Affiche le nom du système d'exploitation.

-a : Afficher les informations en utilisant les options -snrvmo.

> Ex :

uname -a

Affiche tout.

Commande « top » : top

> Montre la charge CPU.

> Options :

-u : affiche les processus pour un utilisateur donné.

> Ex :

top

top -u root

Commande « free » : mémoire libre

> Affiche la mémoire disponible / utilisée du système.

> Options :

-b : Affiche la mémoire en bytes.

-k : Affiche la mémoire en kilo octet.

-m : Affiche la mémoire en méga octet.

-g : Affiche la mémoire en giga octet.

-s : Spécifie le délai de réaffichage de la mémoire.

-t : Affiche la ligne des totaux.

> Ex :

free -m -s 5

Affiche la mémoire du système en méga octet toutes les 5 secondes.

Commande « df » : disk free

> Affiche la quantité d'espace disque utilisé par les systèmes de fichiers.

> Options :

-a : Affiche tous les systèmes de fichiers, y compris ceux de 0 blocs (par exemple : proc, sysfs, usbfs et tmpfs).

-h : Ajoute aux valeur un M pour mébioctet (2^20 octets) pour que ce soit plus lisible.

-H : Pareil que -h mais en mégaoctets (10^6 octets).

-T : Affiche le type du système de fichier.

> Ex :

df -h

Affiche la quantité d'espace disque utilisé en mébioctets par les systèmes de fichiers.

df /home

Affiche la quantité d'espace disque utilisé par la partition /home (si elle existe).

df -T -h

Affichage le nom des partitions et leur point de montage.

Commande « fdisk » : infos disques

> Affiche les infos des disques.

> Options les plus fréquentes :

-l Informations détaillées des disques.

> Ex :

sudo fdisk -l

Commande « du » : directory usage

> Affiche l'espace disque utilisé par répertoires.

> Options :

-a : Afficher pour tous les fichiers et pas uniquement les répertoires.

-c : Faire un total après avoir tout affiché.

-h : Ajoute un suffixe correspondant à l'unité (K, M, G).

-H : Idem que -h mais en puissance de 10.

> Ex :

du -ch /home/NomUSER

Affiche la taille des répertoires contenus dans /home/NomUSER en utilisant un suffixe puis le total.

Commande « uptime » : uptime

> Indique depuis quand le système fonctionne.

> Ex :

uptime

Affiche l'heure actuelle, la durée depuis laquelle le système fonctionne, le nombre d'utilisateurs actuellement connectés, et la charge système moyenne.

Commande « lspci » : list pci

> Liste tous les périphériques PCI

> Option :

-v : Affiche des informations plus détaillées.

> Ex :

lspci

Commande « lsusb » : list usb

> Liste tous les périphériques USB.

> Option :

-v : Affiche des informations plus détaillées.

> Ex :

lsusb

Commande « mount » : mount

> Monter un système de fichiers.

> Options :

-a : Monter tous les systèmes de fichier déclarés dans le fichier /etc/fstab.

-t : Précise le type de fichier à monter.

-o : Ajouter une option. Options adjointe à -o les plus fréquentes :

auto : Permet d'être monté par -a.

async : Les entrées/sorties sur le système de fichiers seront asynchrones.

defaults : Utilise les options rw, suid, dev, exec, auto, nouser, et async.

dev : Interprète les fichiers spéciaux de périphériques du système présent dans /dev/.

exec : Permet l'exécution de fichiers binaires du système monté.

noauto : Empêche d'être monté avec -a.

nodev : Ne pas interpréter les fichiers spéciaux de périphériques du système.

noexec : Empêche l'exécution de fichiers binaires du système monté.

nouser : Ne pas autoriser d'autres utilisateurs que root (ou sudo) à monter le système de fichiers (comportement par défaut).

ro : Monte le système en lecture seule.

rw : Monte le système en lecture et écriture.

suid : Prend en compte les bits SetUID ou SetGID du système monté.

user : Permet aux utilisateurs ordinaires à monter et démonter le système de fichiers (implique noexec, nosuid, et nodev sauf si surchargées).

> Ex :

mount

Liste tous les systèmes de fichiers actuellement montés.

mount -a

Monte tous les systèmes de fichiers déclarés dans le fichier /etc/fstab.

mount /mnt/maPartion

Monte le système de fichiers ad-hoc déclarés dans le fichier /etc/fstab.

mount -t iso9660 monFichier.iso /mnt/monIso -o loop

Monte dans un périphérique boucle (loop) le fichier iso monFichier.iso dans le répertoire /mnt/monIso.

mount -t vfat -o defaults,rw,user,umask=022,uid=1000 /dev/sda1 /mnt/Mondisk/

Monte un disque dur USB (/dev/sda1) formaté en FAT32 (-t vfat) en lecture écriture (rw) dans le répertoire /mnt/Mondisk/ ; tous les utilisateurs peuvent le démonter (user), les droits d'exécution (uid=1000) sont fixés à l'utilisateur ayant l'UID 1000 (sous Ubuntu, l'uid 1000 correspond au premier utilisateur créé) et la création d'un fichier s'effectuera avec les permissions 644 (rw-r--r--) et pour un répertoire 755 (rwxr-xr-x) (umask 022).

Commande « umount » : unmout

> Démonte un système de fichiers.

> Options :

-a : Démonte tous les systèmes de fichiers présents dans /etc/mtab.

-d : Si le système monté est un périphérique loop, libérer le périphérique.

-f : Forcer le démontage.

-r : Si impossible de démonter, monter en lecture seule.

> Ex :

umount /mnt/Mondisk

Démonte le système de fichiers monté dans /mnt/Mondisk.

umount -f /dev/cdrom

Force le démontage du périphérique CDROM.

umount -d /mnt/monIso

Démonte et libère le périphérique loop.

umount -a

Démonte tous les systèmes de fichiers montés (à l'exception de /proc) ; ne sert que lorsque l'on veut redémarrer ou

éteindre sa machine manuellement et proprement.

Commande « apt-get » : avanced package tool - get

> Permet l'installation et le retrait de packages en tenant compte des dépendances, ainsi que le téléchargement des packages s'ils sont sur une source réseau.

> Commandes les plus fréquentes :

update : Met à jour la liste des packages disponibles en fonction des sources fournies.

upgrade : Met à jour tous les packages déjà installés.

dist-upgrade : Pareil que précédent mais permet également de passer à une version n+1 simplement de la distribution.

install : Installe un ou plusieurs packages.

remove : Supprime un ou plusieurs packages.

clean : Efface du disque dur les packages téléchargés.

> Options :

-f : Utilisée avec install ou remove cette option permet de réparer un système dont les dépendances sont défectueuses.

-m : Ignore les paquets manquants (a éviter si on ne sait pas exactement ce que l'on fait).

-s : Fait une simulation des actions à mener sans rien toucher au système.

-y : Répond automatiquement oui à toutes les questions.

-u : Affiche les paquets mis à jour.

--purge : A utiliser conjointement avec remove pour supprimer tout ce qui peut l'être (fichiers de configuration par exemple).

--reinstall : Réinstaller les paquets avec leur version plus récente.

> Ex :

apt-get update

Met à jour la liste de packages.

apt-get upgrade

Met à jour tous les packages installés.

apt-get install package1 package2

Installe package1 et package2.

apt-get --purge remove package3

Supprime package3 ainsi que tous les fichiers de configuration.

Mise en pratique : Tester les commandes en mode console.

15 Sauvegarde incrémentielle et journalisation (outils rdiff-backup & cron)

15.1 Généralités

Réaliser des sauvegardes différentielles journalières de son « /home », ou supprimer les sauvegardes vieilles d'une semaine, ceci est possible à l'aide de l'outil « rdiff-backup ».

Rdiff-backup peut être utilisé sur Linux, Mac OSX et Windows, ce qui permet d'installer ce logiciel sur n'importe quel ordinateur puis de sauvegarder ces systèmes sur serveur via SSH.

15.2 Installation

Pour installer « rdiff-backup », il suffit de lancer la commande suivante :

```
sudo apt-get install rdiff-backup
```

15.3 Utilisation

Sauvegarder :

rdiff-backup --exclude /home/mon_login/.aMule /home/mon_login /repertoire_de_sauvegarde

Ici, on sauvegarde tout le « /home/mon_login » sauf le répertoire « /home/mon_login/.aMule » dans le dossier de destination « /repertoire_de_sauvegarde ». Si « /repertoire_de_sauvegarde » n'est pas vide, un message indique qu'il faut utiliser l'option « --force » et dans ce cas, son contenu est supprimé.

Exemples :

Sauvegarder uniquement les répertoires « /usr/local » et « /var » :

```
rdiff-backup --include /usr/local --include /var --exclude '**' / /backup
```

Idem, mais avec la liste des répertoires à sauver dans un fichier nommé « include-list.txt » :

```
/varfichiers à lancer au démarrage
/usr/bin/gzip
```

La commande est alors :

```
rdiff-backup --include-globbing-filelist include-list.txt --exclude '**' / /backup
```

Restaurer une sauvegarde :

rdiff-backup -r now /repertoire_de_sauvegarde /repertoire_de_restauration

L'option « -r now » permet de remettre la version de la sauvegarde la plus récente. On peut remonter dans les sauvegardes, par exemple remettre le répertoire d'il y a 3 jours avec l'option « -r 3D ».

Supprimer des sauvegardes :

Pour supprimer les différences accumulées au fur et à mesure que l'on a ajouté des sauvegardes :

rdiff-backup --remove-older-than 1W --force /repertoire_de_sauvegarde

Ici on enlève toutes les modifications enregistrées vieilles de plus d'une semaine. On peut mettre D(ay),W(eek), M(onth) et Y(ear). S'il il y a plusieurs sauvegardes à supprimer, la commande échoue. C'est pourquoi il faut rajouter le paramètre « --force » pour ne pas prendre en compte cette erreur.

Voir la liste des sauvegardes :

Liste simple :

rdiff-backup -l /repertoire_de_sauvegarde

Liste en tableau avec la taille de chaque incrément :

rdiff-backup --list-increment-size /repertoire_de_sauvegarde

Voir les statistiques des sauvegardes :

rdiff-backup-statistics /repertoire_de_sauvegarde

Sauvegarder sur une machine distante via SSH :

Remplacer « /repertoire_de_sauvegarde » par :

<utilisateur>@<adresse_ip_de_la_machine_distante>::<repertoire_de_sauvegarde_sur_la_machine_distante>

15.4 Automatiser les sauvegardes

Comment faire pour que les commandes précédentes se lancent de façon automatique, c'est-à-dire pour qu'on n'ait pas à le faire manuellement chaque jour ?

Journaliser les tâches :

Actuellement, on dispose de trois outils de journalisation de tâches sous Linux :

- **at :** Permet de définir des tâches à réaliser à un instant précis et si la machine est éteinte à ce moment-là, la tâche sera réalisée au prochain démarrage. Utilisable par tout le monde.
- **cron :** Peut définir des tâches périodiques, mais c'est un « daemon » donc si la machine est éteinte, la commande ne se lancera pas du tout. Utilisable par tout le monde.
- **anacron :** Lance des tâches de façon périodique et si l'ordinateur n'est pas allumé au moment voulu, la tâche s'exécutera au prochain démarrage. Utilisable uniquement par root.

« cron » utilise la « crontab » qui permet d'indiquer les tâches que l'on veut réaliser et à quelle fréquence. « cron » est présent dans le dossier « /etc/init.d/ » (fichiers lancés au démarrage).

Editer la « crontab » :

```
sudo crontab -e                (pour visualiser : sudo crontab -l)
```

Pour journaliser la tâche, on indique à « cron » d'exécuter le script « ~/sauve_mon_dossier.sh » chaque jour à 20h00. Pour cela, on ajoute la ligne suivante dans « crontab » :

```
00   20   *   *   *   ~/sauve_mon_dossier.sh
```

Celle-ci signifie : tous les jours à 20h00 lance le script « ~/sauv_mon_dossier.sh » (en indiquant d'abord les minutes et ensuite les heures).

Ecrire le script Shell à exécuter :

Ensuite, il reste à écrire le script pour lancer les sauvegardes. On édite donc le fichier « ~/sauv_mon_dossier.sh » et on y insère les lignes suivantes :

```
#!/bin/sh
nice -n 19 rdiff-backup --exclude /home/login/.aMule /home/login /mnt/save && nice -n 19 rdiff-backup --remove-older-than 1W --force /mnt/save
```

Le « nice -n 19 » signifie que les commandes s'exécutent avec la priorité la plus petite par rapport aux autres processus, ceci afin d'éviter que l'ordinateur ne se mette à ralentir tous les jours à 20h00. On sauvegarde le script et on lui rajoute les droits d'exécution :

```
sudo chmod ugo+x ~/sauv_mon_dossier.sh
```

On peut alors vérifier que le script fonctionne bien en le lançant directement :

```
~/sauve_mon_dossier.sh
```

Normalement « rdiff-backup » se lance, fait sa sauvegarde et informe ensuite qu'il a ou non supprimé les sauvegardes plus vieilles d'une semaine.

Mise en pratique : Créer, restaurer et supprimer des sauvegardes.

15.5 Lancer une tâche au démarrage (processus init)

« init » est le premier processus, exécuté par le noyau, qui est père de tous les autres (son PID est donc 1).

Au démarrage, il lance divers scripts contenus dans « /etc/init.d/ » ou « /etc/rc*.d/ ».

C'est dans le dossier « /etc/init.d/ » qu'il faut enregistrer les fichiers à lancer au démarrage. Il faut ensuite ajouter le fichier à la liste des processus exécutés au démarrage :

```
sudo update-rc.d mon-fichier defaults
```

- **Plus d'informations :**

Taper dans un terminal :

```
ls -l /etc/init.d/ (pour voir les scripts lancés au démarrage)
init --help
cat /etc/init.d/README
man init
info init
man update-rc.d
```

Mise en pratique : Ecrire un script Shell exécuté au démarrage.

16 Que faire en cas de gel du système ?

16.1 Généralités

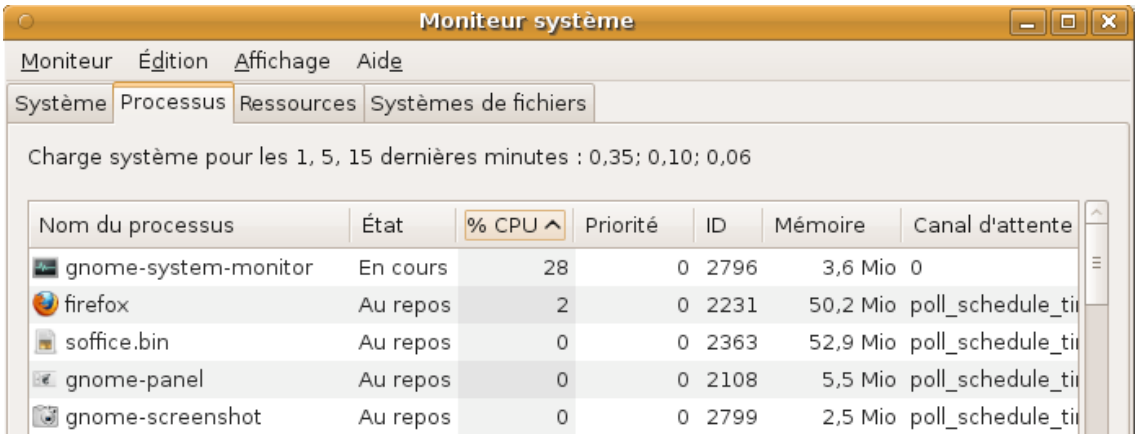
Lorsque l'ordinateur ne répond plus aux commandes et que les périphériques d'entrée comme le clavier et/ou la souris semblent bloqués, on dit que le système "gèle" (freeze en anglais). Cela peut signifier qu'une erreur critique est survenue dans la configuration logicielle ou matérielle.

Dans le cas d'un gel du système, la priorité sera d'identifier le processus coupable et de le mettre hors d'état de nuire le cas échéant. Si cela n'est pas possible, la priorité sera alors d'éteindre le système correctement.

16.2 Tuer un processus avec le moniteur système

Cette manipulation est possible quand le système gèle : un processus prend "100%" du processeur (bug ou procédure non désirée). On peut "tuer" facilement les processus avec le moniteur système.

Aller dans Système => Administration => Moniteur Système => Cliquer sur l'onglet « Processus » :



- Essayer de terminer le processus.
- Si cela ne fonctionne pas, faire un clic-droit sur le processus et cliquer sur terminer.

16.3 Tuer un processus depuis un terminal virtuel

6 consoles textes, nommés "terminaux virtuels", sont accessibles via les combinaisons de touches Alt-Ctrl-F1, Alt-Ctrl-F2,… Alt-Ctrl-F6. Cela peut prendre plusieurs secondes. L'écran devient noir et invite à entrer son « login » (nom d'utilisateur) puis son « password » (mot de passe). Un Shell Unix est alors disponible, exactement comme dans une fenêtre terminal. On peut à tout moment revenir à l'écran graphique par Alt-Ctrl-F7.

La commande « top » va permettre de voir les processus qui utilisent le plus de ressources. Par défaut, les processus sont classés par ordre d'utilisation du processeur (colonne %CPU). On peut les classer par utilisation de la mémoire (colonne %MEM) en appuyant sur la touche 'M', et revenir au classement initial par la touche 'P' (lettres majuscules). Si un processus occupe trop de ressources (plus de 90% du CPU par exemple), on peut le "tuer" de la manière suivante : noter son PID (première colonne), puis appuyer respectivement sur la touche 'k', la touche '9', entrer ce numéro et appuyer sur « Entrée ».

La commande « ps -A » (ou « ps aux ») peut également aider à identifier les "processus fous". En particulier, si on a un soupçon sur un programme, on peut identifier son PID en tapant : « ps -A | grep nom_du_prog ». Il suffit ensuite d'écrire « kill PID » ou « kill -9 PID » pour tuer le processus (en remplaçant PID par le numéro concerné).

Si rien ne paraît suspect, ou si tuer les processus gourmands ne change rien, exécuter la commande « sudo pkill X », ou la commande « sudo pkill -9 X » si la première n'a aucun effet.

16.4 Tuer un processus depuis un autre ordinateur

Si un serveur SSH est configuré sur la machine, essayer de s'y connecter par « ssh » à partir d'une autre machine. Il est recommandé de se connecter en tant qu'utilisateur non privilégié, puis d'utiliser la commande « sudo » pour devenir root. Les commandes à utiliser sont évidemment les mêmes que depuis un terminal virtuel.

16.5 Autres solutions

Tenter d'arrêter l'ordinateur à l'aide de l'ACPI (Advanced Configuration and Power Interface), en appuyant sur le bouton « Marche / Arrêt » pendant moins d'une seconde. Après un temps de latence éventuellement long (plusieurs minutes), le système s'arrête correctement et l'ordinateur est prêt à être redémarré.

Enfin, si rien de ce qui précède ne fonctionne, presser le bouton « reset » de la machine. Avec un peu de chance, GNU/Linux se contentera uniquement d'une vérification du disque au redémarrage. Si ce n'est pas le cas, démarrer temporairement (le temps d'une session) sur l'option "recovery mode" de GRUB, ou même simplement sur une version antérieure du noyau peut parfois résoudre les problèmes.

Pour éteindre un ordinateur "gelé", on peut aussi appuyer 5 secondes sur la touche « Arrêter » de l'unité centrale. Dans tous les cas, ne jamais débrancher l'ordinateur "à chaud".

Au final, essayer de trouver ce qui a provoqué le blocage, car cela peut endommager sévèrement le système de fichiers, et préférer un système de fichiers journalisés (plus robuste aux "crashs").

 ***Mise en pratique : Lancer et tuer des processus longs.***

17 Combinaisons de touches système

En cas d'urgence, un certain nombre de touches sont directement accessibles par le système pour aider à débloquer la situation :

Combinaison	Effet	Signification
Alt SysRq 0-9	Détermine le niveau de log de la console	
Alt SysRq b	Redémarre l'ordinateur	reBoot
Alt SysRq c	Redémarre via kexec pour faire un crashdump	Crashdump
Alt SysRq e	Envoie un signal de terminaison (SIGTERM) à tous les processus (sauf init)	tErm
Alt SysRq f	Tue le processus qui consomme le plus de mémoire (via oom-killer)	
Alt SysRq i	Envoie un signal de fin (SIGKILL, plus ferme que SIGTERM) à tous les processus (sauf init)	kIll
Alt SysRq k	Tue tous les processus de la console virtuelle courante	Key
Alt SysRq l	Envoie un signal de fin (SIGKILL, plus ferme que SIGTERM) à tous les processus (même init)	kilL
Alt SysRq m	Affiche le contenu actuel de la mémoire	Memory
Alt SysRq o	Éteint le systeme via APM	Out
Alt SysRq p	Affiche sur la console les registres et drapeaux actuels	Print
Alt SysRq r	Bascule la gestion du clavier de mode brute (raw) à XLATE	Raw
Alt SysRq s	Synchronise les disques (tente d'écrire toutes les données non sauvegardées)	sync
Alt SysRq t	Affiche une liste des tâches actuellement en cours et leur description	Task
Alt SysRq u	Tente de remonter tous les systèmes de fichiers montés en lecture seule. Ceci retire le marquage « dirty flag » et évitera ainsi une vérification du système de fichiers au redémarrage.	Umount

Mise en pratique : Tester quelques combinaisons de touches.

18 Effectuer des tâches administratives (sudo)

18.1 Généralités

Par défaut, l'accès direct au compte système root est désactivé sous Linux Ubuntu. La logique du système est d'utiliser « sudo » pour effectuer toutes les tâches administratives. Il est totalement déconseillé d'activer l'accès et d'utiliser directement le compte root sous Ubuntu. Rappelons aussi que « sudo » n'est pas moins sécurisé que l'utilisation d'un compte root.

« sudo » est l'outil permettant à un utilisateur d'exécuter des tâches d'administration (par défaut le premier utilisateur, celui qui a été créé lors de l'installation du système). A la demande, c'est le mot de passe de l'utilisateur actif dans la session qu'il faut saisir.

Remarque : Sur les systèmes d'exploitation "à contrôle d'accès discrétionnaire" (MVS, Windows NT/2000/XP,…), le compte système et le compte administrateur sont différents. Par contre, Unix, depuis sa création en 1969, n'a jamais mis en place cette différence. root est à la fois le super-utilisateur du système et le système lui-même.

18.2 Définition de « sudo »

Certaines situations peuvent amener l'utilisateur à effectuer des tâches administratives, particulièrement lors de la résolution de problèmes de fonctionnement du système ou d'installation logiciels. L'utilitaire « sudo » (pour Substitute User Do) permet à un administrateur système de donner à un utilisateur (ou un groupe d'utilisateurs) la possibilité d'exécuter une ou toutes les commandes en tant que super-utilisateur, tout en gardant une trace des commandes tapées et des arguments.

Par défaut, le compte super-utilisateur n'a pas de mot de passe sous Ubuntu. Aucun mot de passe n'est associé au compte root et root n'en a pas besoin. Sous les systèmes Unix (dont Linux fait partie), on ne peut pas se connecter directement à un compte utilisateur sans mot de passe. Ceci signifie qu'on ne peut pas se connecter en tant que root ou utiliser la commande « su root ».

L'installateur d'Ubuntu configure plutôt l'utilitaire « sudo » de façon à ce que l'utilisateur créé durant l'installation puisse effectuer toutes les tâches d'administration nécessaires.

Tous les programmes d'administration dans les menus d'applications utilisent un système graphique associé à « sudo » demandant le mot de passe utilisateur pour s'exécuter : « gksudo » sous GNOME et « kdesu » sous KDE. Que ce soient « gksudo », « kdesu », ou « sudo » dans un terminal, c'est le mot de passe de l'utilisateur actif qui est requis.

18.3 Utilisation de « sudo »

L'utilitaire « sudo » s'utilise en ligne de commande, dans un terminal. Il sert à exécuter, en mode super-utilisateur, des commandes ou des applications en console. Pour lancer des applications graphiques avec les privilèges d'administration, il est de mise d'utiliser les pendants graphiques « gksudo » pour GNOME, ou « kdesudo » pour KDE.

Syntaxe : sudo <commande>

Ainsi, on doit faire précéder chacune des commandes à exécuter en mode super-utilisateur par « sudo ». Le mot de passe demandé est celui de l'utilisateur courant. La commande sera exécutée si le mot de passe entré est correct et que l'utilisateur courant peut effectuer des tâches d'administration (fichier /etc/sudoers).

Au bout d'un laps de temps, il faut entrer de nouveau le mot de passe. Pour terminer la session « sudo » avant la fin des 15 minutes par défaut, entrer la commande « sudo -k ».

« sudo » conserve une trace de toutes les commandes exécutées dans le fichier journal :

```
cat /var/log/auth.log
```

18.4 Configuration de « sudo »

La configuration de « sudo » se fait dans le fichier « /etc/sudoers ». Les utilisateurs définis dans ce fichier ont donc les droits « sudo ».

Ce fichier doit être modifié impérativement avec la commande « visudo ». Si on édite le fichier directement, il est possible que le système refuse de fonctionner correctement par la suite. Avec « visudo » le système vérifie la syntaxe du fichier avant d'accepter les modifications.

Syntaxe : sudo visudo

On peut modifier l'éditeur à utiliser (par défaut « vi ») :

```
sudo EDITOR="/bin/nano" visudo
sudo EDITOR="/usr/bin/gedit" visudo
```

Ajout des privilèges super-utilisateur à un utilisateur :

```
sudo adduser <login> admin
```

"admin" est un groupe défini du système. Il existe également d'autres groupes relatifs à l'administration du système, dont "adm" qui autorise la lecture des fichiers de log sans avoir à utiliser « sudo », et "staff" qui donne des droits d'écriture dans « /usr/local » et « /home » (un « sudo » bridé en quelque sorte).

Toujours demander le mot de passe :

Pour ceux qui veulent profiter d'une sécurité accrue et appliquer un délai nul à « sudo », modifier la ligne :

```
Defaults        !lecture,tty_tickets,!fqdn
```

En ajoutant timestamp_timeout=0 :

```
Defaults        !lecture,tty_tickets,!fqdn,timestamp_timeout=0
```

« sudo » demandera désormais le mot de passe à chaque opération. Au besoin, on peut ouvrir un terminal root et effectuer plusieurs opérations d'administration sans devoir taper un mot de passe à chaque fois, grâce à la commande :

```
sudo -i
```

Fichier « /etc/sudoers » corrompu :

Il peut arriver lors de certaines manipulations de corrompre le fichier « /etc/sudoers » :

```
sudoers file: syntax error, line 19
sudo: parse error in /etc/sudoers near line 19
```

Ou d'avoir modifié par mégarde les droits du fichier :

```
sudo: bad permissions (ou autre)
```

Dans ce cas, on ne peut le corriger puisqu'on a besoin de « sudo » pour le modifier. Pour retrouver des droits d'administrateur et le corriger :

- Utiliser un Live CD
- Redémarrer en « recovery mode »

Rappel : Ce mode est disponible à l'écran de GRUB lors du démarrage de l'ordinateur. Il se lance directement en mode texte et en tant qu'administrateur (root sans mot de passe).

 ***Mise en pratique : Utiliser « sudo » et définir un utilisateur dans « /etc/sudoers ».***

19 Gestion des groupes et des utilisateurs

19.1 Rappel

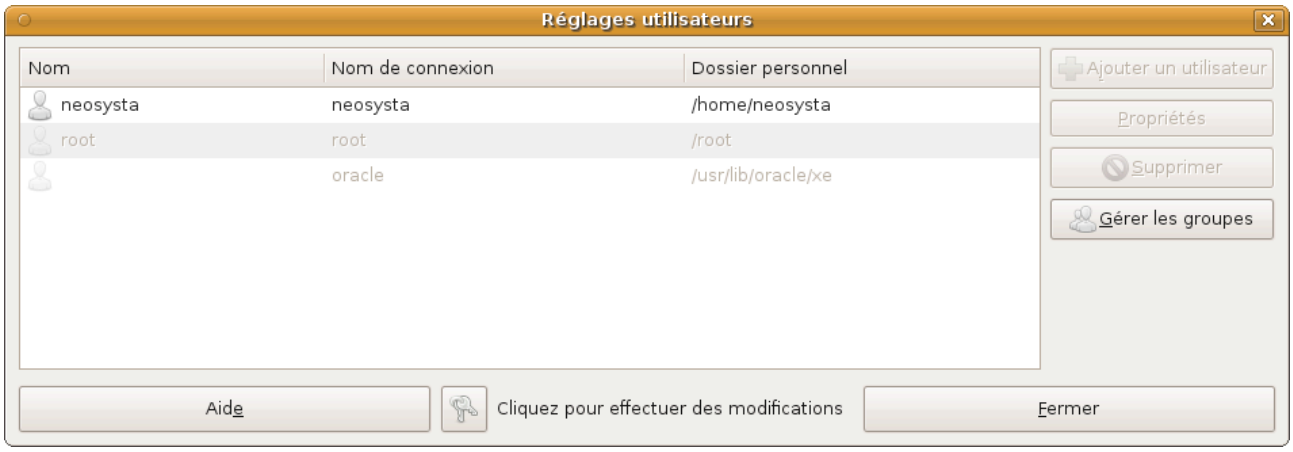
Sous les systèmes d'exploitation Unix et Linux comme Ubuntu, l'utilisation du système passe toujours par l'identification (login avec mot de passe) d'un utilisateur (unique) appartenant à un groupe (unique) ayant certains droits sur les fichiers. Tous les fichiers ont des droits définis.

Cette organisation sécurise intégralement les systèmes Unix et Linux.

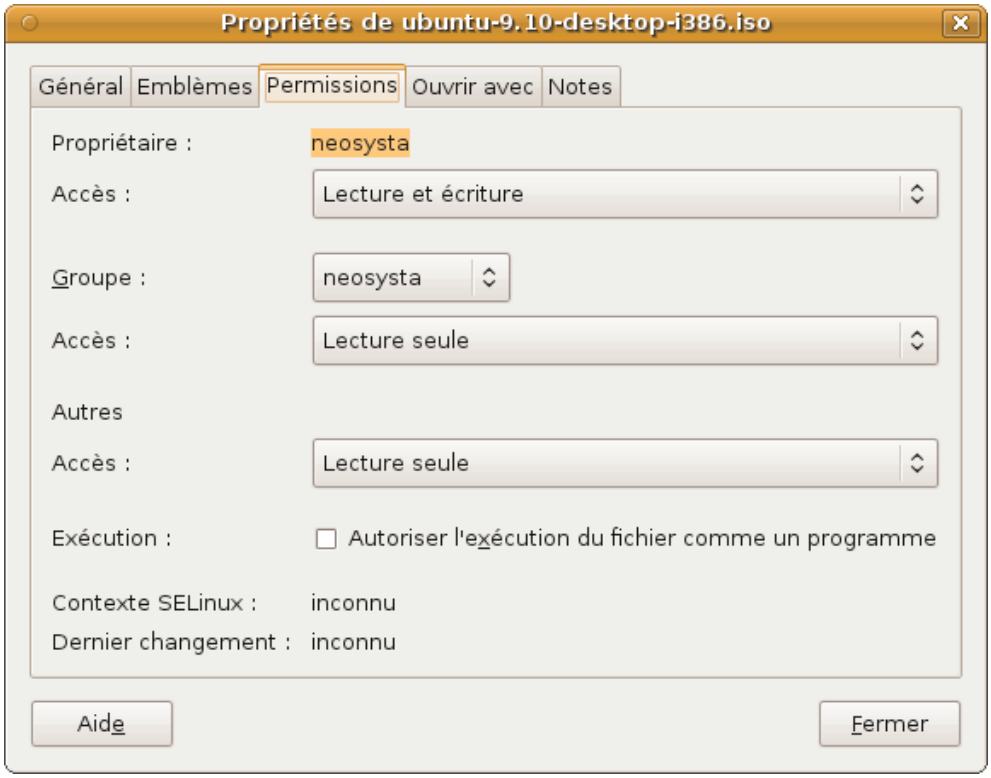
19.2 Par l'interface graphique

Par l'interface graphique de Linux Ubuntu (GNOME), la définition des utilisateurs et des groupes est accessible depuis le menu :

Système => Administration => Utilisateurs et groupes



La définition des droits sur les fichiers est accessible en faisant un clic-droit sur le fichier puis « Propriétés » et onglet « Permissions » :



19.3 En ligne de commande

Chaque fichier possède des droits ou permissions de lecture (r = read), d'écriture (w = write), d'exécution (x = execute), ou pas (-), pour son propriétaire (u = user), son groupe (g = group) et les autres utilisateurs (o = other). Définitions vérifiables par la commande « ls -la ».

La procédure et les commandes nécessaires à la définition des utilisateurs et des groupes, ainsi qu'à la définition de leurs droits sur les fichiers, sont les suivantes :

1) Syntaxe de la commande créant le nouveau groupe d'utilisateurs nommé « groupetest » :

sudo groupadd groupetest

2) Syntaxe de la commande affichant le contenu du fichier des groupes d'utilisateurs (avec leurs GID) :

cat /etc/group (ou : sudo cat /etc/group)

3) Syntaxe de la commande créant le nouvel utilisateur nommé « usertest » appartenant au groupe « groupetest » (si GID = 1111) :

sudo adduser --gid 1111 usertest

4) Syntaxe de la commande affichant le contenu du fichier des utilisateurs (avec leurs UID) :

cat /etc/passwd **(ou : sudo cat /etc/passwd)**

5) Syntaxe de la commande affichant le contenu du fichier des mots de passe utilisateurs :

sudo cat /etc/shadow

6) Syntaxe de la commande affectant l'utilisateur « usertest » comme propriétaire du fichier « fichtest » :

sudo chown usertest fichtest

7) Syntaxe de la commande affectant le groupe « groupetest » comme groupe d'utilisateurs au fichier « fichtest » :

sudo chgrp groupetest fichtest

8) Syntaxe de la commande donnant par exemple tous les droits à tout le monde sur le fichier « fichtest » :

chmod ugo+rwx fichtest **(ou : sudo chmod ugo+rwx fichtest)**

9) Syntaxe de la commande permettant de changer le mot de passe de l'utilisateur « usertest » :

sudo passwd usertest

10) Syntaxe de la commande permettant de se connecter à la session de l'utilisateur « usertest » :

su usertest **(« exit » pour quitter sa session)**

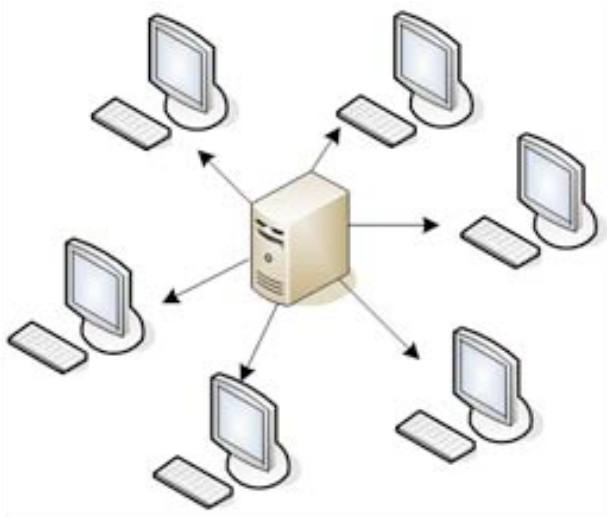
Rappel :

Le répertoire d'accueil à l'ouverture d'une "session terminal utilisateur" est « /home/utilisateur/ » (dossier personnel de l'utilisateur), et le programme Shell lancé par défaut « /bin/bash ».

 ***Mise en pratique : Tester les commandes de gestion des groupes et utilisateurs.***

20 Caractéristiques générales d'un serveur (rappel)

En informatique, un serveur est un ordinateur (et l'ensemble des logiciels installés) dont le rôle est de répondre de manière automatique à des demandes envoyées par des clients - ordinateur et logiciel - via un réseau (local ou Internet). Les programmes du serveur sont des services en fonction et accessibles par les clients via des ports ouverts ou fermés faisant office de portes d'entrée au système depuis l'extérieur.



La mise en place d'un serveur se fait en deux étapes :

1) Installation (et configuration) du système d'exploitation
2) Installation (et configuration) de l'une ou des application(s) adaptée(s) au(x) service(s) désiré(s)

Dans le cas de Linux Ubuntu, n'importe quelle variante du système peut donc servir de base pour mettre en place un serveur. Cependant, les serveurs de production sont très souvent configurés pour avoir une efficacité maximale.

Ainsi, la variante serveur d'Ubuntu (Ubuntu Server Edition) possède un noyau optimisé et est dépourvue d'environnement graphique, gourmand en ressources et superflu dans le cas d'un serveur amené à être manipulé assez rarement. Cette variante est donc la plus adaptée pour la mise en place d'un serveur utilisé de manière intensive.

Les deux principales caractéristiques à prendre en compte dans le cas d'un serveur de production sont :

- **Une très haute disponibilité :** Dans l'idéal, un client doit pouvoir accéder à un serveur n'importe quand et facilement.
- **Une grande sécurité :** Condition requise pour une bonne qualité du service, fiabilité et garantie.

21 Configuration Netfilter & Iptables

21.1 Généralités

« Netfilter » est un module du noyau Linux (depuis les branches 2.4 et 2.6) qui offre la possibilité de contrôler, modifier et filtrer les paquets d'adresses IP, et de suivre les connexions. Il fournit ainsi les fonctions de pare-feu, de partage de connexions Internet et d'autorisation du trafic réseau.

« Iptables » est l'interface en ligne de commande permettant de configurer « Netfilter ».

21.2 Configuration du pare-feu avec Iptables

Rappel : Pour les réseaux informatiques, un pare-feu (firewall en anglais) est un logiciel et/ou un matériel qui a pour fonction de faire respecter la politique de sécurité du réseau. Cette politique définissant quels sont les types de communication autorisés ou interdits.

La configuration du pare-feu est la suivante :

- On bloque tout le trafic entrant par défaut.
- On autorise au cas par cas : le trafic appartenant ou lié à des connexions déjà établies et le trafic à destination des serveurs (Web, SSH, etc) qu'on souhaite mettre à disposition.

En tapant « sudo iptables -L », une liste des règles actuelles est affichée. Au départ (pas encore de configuration), les chaines devraient être vides :

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Pour l'instant, tout passe dans toutes les directions (policy ACCEPT). Pour cette configuration basique, seul le trafic entrant (chaine INPUT) est concerné. Si la configuration a déjà été modifiée et qu'on souhaite la réinitialiser, taper :

```
sudo iptables -F
sudo iptables -X
```

Autoriser le trafic entrant d'une connexion déjà établie :

Pour permettre à une connexion déjà ouverte de recevoir du trafic :

```
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Pour permettre le trafic entrant sur un port spécifique :

Pour permettre le trafic entrant sur le port 22 (traditionnellement utilisé par SSH), on doit indiquer à « Iptables » tout le trafic TCP sur le port 22 du réseau :

```
sudo iptables -A INPUT -p tcp -i eth0 --dport ssh -j ACCEPT
```

Cette commande ajoute une règle (-A) à la chaine contrôlant le trafic entrant INPUT, avec le protocole (-p) TCP, pour autoriser le trafic (-j ACCEPT) vers l'interface (-i) eth0 et à destination du port (--dport) SSH (on aurait pu mettre 22).

Maintenant, on peut vérifier les règles « Iptables » : sudo iptables -L

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
```

Accepter tout le trafic Web (www) entrant (port 80) :

```
sudo iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT
```

En vérifiant les règles : sudo iptables -L

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:www
```

On a exceptionnellement autorisé le trafic TCP pour SSH et les ports Web, mais comme rien n'a encore été bloqué, tout le trafic passe quand même.

Bloquer le trafic :

Les autorisations étant configurées, il faut maintenant bloquer le reste en modifiant la politique par défaut (policy) de la chaine INPUT. Cette décision (DROP) s'applique lorsqu'aucune règle n'a été appliquée à un paquet. Si la tentative de connexion n'est permise par aucune des règles précédentes, elle sera donc rejetée :

```
sudo iptables -P INPUT DROP
sudo iptables -L

Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere            state RELATED,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh
```

```
ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:www
```

Autoriser le trafic local :

Avec cette configuration, même l'interface locale (loopback) est bloquée. On pourrait écrire les règles de rejet seulement pour « eth0 » en spécifiant « -i eth0 », mais on peut également ajouter une règle pour loopback. Par exemple, en l'insérant en 2ème position :

```
sudo iptables -I INPUT 2 -i lo -j ACCEPT
```

Pour lister les règles plus en détail :

```
sudo iptables -L -v -n
```

Autoriser les requêtes ICMP (ping) :

Il peut être utile de valider les réponses aux requêtes "ping", ne serait-ce que pour s'assurer que le poste est toujours en activité. On autorise donc le PC à faire des "pings" sur des IP externes et à répondre aux requêtes "ping" :

```
sudo iptables -A OUTPUT -p icmp -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT

sudo iptables -A INPUT -p icmp -j ACCEPT
```

Supprimer une règle :

On peut supprimer une seule entrée plutôt que de tout réinitialiser. Tout d'abord, lister l'ensemble des règles avec affichage des lignes :

```
sudo iptables -L --line-numbers

Chain INPUT (policy DROP)
num  target     prot opt source               destination
1    DROP       icmp --  anywhere             anywhere
2    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
3    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:www
4    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:webmin

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     tcp  --  anywhere             anywhere             tcp spt:www
2    ACCEPT     tcp  --  anywhere             anywhere             tcp spt:12345
```

Si on souhaite supprimer la ligne 2 de la chaine OUTPUT :

sudo iptables -D chaine numéro_de_ligne

sudo iptables -D OUTPUT 2

Appliquer les règles au démarrage :

Une fois les règles testées, il reste à les appliquer au démarrage. Pour cela, éditer un fichier en « root » et l'enregistrer sous « /etc/init.d/monIptables ». La première ligne de ce fichier doit être :

#!/bin/bash

Cette ligne indique que le fichier doit être enregistré en tant que script Shell. Le reste du fichier doit contenir les commandes « Iptables » souhaitées. Puis rendre ce script exécutable :

sudo chmod ugo+x /etc/init.d/monIptables

Pour indiquer au système de l'utiliser au démarrage :

sudo update-rc.d monIptables defaults

Au prochain redémarrage, vérifier que les règles sont bien utilisées avec :

sudo iptables -L

 ***Mise en pratique : Tester quelques configurations du pare-feu avec « Iptables ».***

22 Configuration du pare-feu avec UFW

22.1 Généralités

Rappel : Pour les réseaux informatiques, un pare-feu (firewall en anglais) est un logiciel et/ou un matériel qui a pour fonction de faire respecter la politique de sécurité du réseau. Cette politique définissant quels sont les types de communication autorisés ou interdits.

Linux Ubuntu possède déjà par défaut un pare-feu nommé « UFW », ainsi qu'une interface graphique simple : « Gufw ».

22.2 Utilisation

L'outil « UFW » n'est pas activé par défaut (fichier de configuration par défaut : /etc/default/ufw).

Activer le pare-feu :

sudo ufw enable

Désactiver le pare-feu :

sudo ufw disable

Autoriser le trafic entrant suivant les règles par défaut :

sudo ufw default allow

Refuser le trafic entrant suivant les règles par défaut :

sudo ufw default deny

Afficher l'état actuel des règles :

sudo ufw status

Activer la journalisation :

sudo ufw logging on

Désactiver la journalisation :

sudo ufw logging off

Autoriser une règle :

sudo ufw allow [règle]

Refuser une règle :

sudo ufw deny [règle]

Supprimer une règle :

sudo ufw delete allow [règle]

Voici quelques exemples pour comprendre la syntaxe des règles de configuration :

- Ouverture du port 53 en TCP et UDP : sudo ufw allow 53
- Ouverture du port 25 en TCP uniquement : sudo ufw allow 25/tcp

Utilisation des ports et services disponibles :

« UFW » regarde dans sa liste de services connus pour appliquer les règles standards associées à ces services (apache2, smtp, imaps, etc). Pour avoir la liste de ces services :

less /etc/services

Exemple (autoriser le service SMTP) :

sudo ufw allow smtp

L'écriture de règles plus complexes est également possible :

- Refuser le protocole (proto) TCP à (to) tout le monde (any) sur le port (port) 80 :
  sudo ufw deny proto tcp to any port 80
- Refuser à (to) l'adresse 192.168.0.1 de recevoir sur le port (port) 25 les données provenant (from) du réseau de classe A et utilisant le protocole (proto) TCP :
  sudo ufw deny proto tcp from 10.0.0.0/8 to 192.168.0.1 port 25
- Refuser les données provenant (from) de 1.2.3.4 utilisant le protocole (proto) UDP sur le port (port) 514 :
  sudo ufw deny proto udp from 1.2.3.4 to any port 514

Configuration IPv6 (protocole adresses IP) :

« UFW » prend en charge les adresses IPv6, mais nécessite une configuration complémentaire pour activer ce support. Pour cela, il suffit de modifier le fichier « /etc/default/ufw » en précisant :
IPV6=yes

Il ne reste plus qu'à désactiver et réactiver de nouveau « UFW » :

sudo ufw disable
sudo ufw enable

 ***Mise en pratique : Tester quelques configurations du pare-feu avec « UFM ».***

23 Configuration d'un réseau statique et dynamique

23.1 Généralités

D'une manière générale, l'utilisation des paramètres automatiques (comme le DHCP) avec une connexion filaire (type Ethernet) permet d'être connecté sans aucune autre manipulation que celle de brancher le câble réseau. Mais il existe de nombreux cas de figures (WiFi, ADSL, Réglage réseau particulier, etc) qui peuvent nécessiter une intervention particulière.

Indépendamment des paramétrages, pour accéder à un réseau (local ou Internet) il faut que le matériel qui sert à se connecter puisse être utilisé par Linux Ubuntu. Il existe plusieurs cas de figure en fonction du type de connexion :

- La connexion Ethernet (par fil) est normalement fonctionnelle et utilisable dès le premier démarrage.
- La connexion WiFi (sans fil), que le module soit intégré ou en USB externe, est généralement fonctionnel au démarrage mais nécessite parfois une configuration particulière.

Si le matériel est correctement pris en charge par Ubuntu, il doit être paramétré en fonction du réseau pour que la connexion soit efficace et opérationnelle selon le besoin.

Convention :

Avec un réseau de moins de 256 machines, on peut choisir d'établir le réseau dans la plage d'adresses IP 192.168.X.Y (par exemple) :

- Le X représente alors l'identification du réseau (par exemple : 10).
- Le Y permet de distinguer les machines les unes des autres au sein du réseau 192.168.10.Y : chaque machine doit avoir une valeur différente.

Pour des cas simples (un seul réseau), on peut choisir la numération suivante : 10.0.1.Y

Le serveur ICS (DHCP & DNS) :

Ce chapitre documente les façons de mettre en place la fonction ICS (Internet Connection Sharing ou Partage de Connexion Internet) sur l'une des machines du réseau, qu'elle soit dédiée au rôle de serveur, ou qu'elle soit le PC d'un utilisateur. Dans les deux cas de figure, cette machine sera nommée « serveur ICS » (IP : 192.168.10.1), même si c'est un simple poste de travail utilisateur.

23.2 Les principales commandes réseau

Connaître le module d'une carte (eth0) :

```
ethtool -i eth0
udevinfo -a -p /sys/class/net/eth0/
```

Liste des interfaces détectées par le noyau :

```
ifconfig
ip link show
```

Informations sur le sans-fil (wlan0) :

```
iwconfig
```

Informations sur le routage :

```
route -n
```

Outils supplémentaires :

```
mii-tool eth0
mii-diag -a
```

Connexions Internet actives (seulement serveurs) :

```
sudo netstat -lp --inet
```

Tester l'adresse locale et autres IP :

```
ping -c4 localhost
ping -c4 Adresse_IP
```

Configurer une adresse réseau :

```
ifconfig eth0 192.168.10.1 netmask 255.255.255.0 broadcast 192.168.10.255
```

Ajouter une passerelle par défaut :

```
route add default gw nom_passerelle
```

Empêcher le ping :

```
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
```

23.3 Configuration statique (IP fixes)

Cette méthode est la plus simple à mettre en place, mais aussi la plus lourde à tenir à jour, surtout avec des modifications de parc assez régulières (des machines qui viennent et repartent du réseau régulièrement): Il va falloir noter la liste de toutes les valeurs d'IP déjà utilisées afin de ne pas ré-attribuer une même valeur à une nouvelle machine.

1) Fixer l'adresse IP des machines :

Une fois qu'on a déterminé quelle adresse IP on souhaitait donner à une machine, il faut faire en sorte que cette machine prenne cette adresse IP et n'en change plus. Avec les droits d'administrateur, éditer le fichier « /etc/network/interfaces » pour modifier le fichier ainsi :

```
iface eth0 inet dhcp
```

Il deviendra alors :

```
auto eth0
iface eth0 inet static
        address 192.168.10.2
        netmask 255.255.255.0
        gateway 192.168.10.1
```

Redémarrer ensuite le réseau :

```
sudo /etc/init.d/networking restart
```

2) Activer le partage de connexions :

Sur la machine ICS, voici les commandes à exécuter :

```
# activation du "pontage" entre les deux cartes réseaux
echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward
sudo iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth1 -j MASQUERADE
```

Remarque : La commande « sudo echo 1 > /proc/sys/net/ipv4/ip_forward » ne fonctionne pas. Les redirections (>) sont indépendantes de « sudo », seul « echo » sera exécuté en root...

La commande « iptables » permet à toutes les machines du réseau local d'aller sur Internet en se faisant passer pour la machine réellement connectée à internet. Ce mécanisme s'appelle NAT (Network Address Translation) ou masquage d'adresse IP (Masquerading).

Maintenant qu'on a fixé les adresses IP locales et qu'on a activé le partage de connexions, toutes les machines sont capables d'aller sur Internet, mais seulement de la façon la plus basique qui soit: Avec la commande « ping 212.27.33.233 », cette machine qui n'est pas du tout sur le réseau local va répondre (on obtient des lignes « Réponse de 212.27.33.233 : octets=32 temps=22 ms TTL=51 »).

Toutefois, on ne peut pas encore utiliser de noms pour s'adresser aux autres machines du réseau local, ni pour s'adresser aux machines qui sont sur Internet.

Remarque : Ces deux commandes sont "volatiles", leur effet disparaitra au prochain redémarrage du serveur ICS. Pour rendre leur effet permanent, il faut les activer dans un script de démarrage de la machine (voir la configuration dynamique), ou modifier le fichier « /etc/network/options ».

Le contenu du fichier est le suivant :

```
ip_forward=no
spoofprotect=yes
syncookies=no
```

Il suffit de changer le paramètre « ip_forward » en 'yes'. L'option « spoofprotect » active la protection contre l'"ip spoofing". Enfin, la dernière option « syncookies » protège la machine des attaques de type "SYN flood".

3) Renseigner le fichier « /etc/hosts » :

On va s'occuper de donner des noms aux machines du réseau local. En fait, elles possède déjà chacune un nom, mais il n'y a qu'elles-mêmes qui le connaissent. Il faut faire en sorte que toutes les machines du réseau sachent que par exemple la machine « 192.168.10.3 » s'appelle « aragorn ». Pour cela, faire le tour de toutes les machines du réseau afin d'éditer le fichier « /etc/hosts ».

Voici par exemple le fichier « /etc/hosts » d'une machine nommée « pippin » :

```
127.0.0.1       localhost.localdomain   localhost       pippin
192.168.10.1    serveurICS
192.168.10.2    gandalf
192.168.10.3    aragorn
192.168.10.4    boromir

# Ce qui suit fait partie de l'installation par défaut d'Ubuntu. A laisser tel quel.
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Le fichier « /etc/hosts » de la machine « boromir » sera différent. Il devra ressembler à ceci :

```
127.0.0.1       localhost.localdomain   localhost       boromir
192.168.10.1    serveurICS
192.168.10.2    gandalf
192.168.10.3    aragorn
192.168.10.5    pippin
```

...

A ce stade de la configuration, les machines sont capables de communiquer entre elles et on peut les interpeler par leur nom : « ping gandalf » fonctionnera et ça sera la machine « gandalf » qui répondra. Mais toujours vérifier la cohérence du tout.

4) Configurer la résolution DNS :

Il reste à configurer la résolution DNS (Domain Name System ou système des noms de domaine) pour pouvoir taper « ping mon-domaine.local » au lieu de « ping 192.168.10.1 ». Si on veut pouvoir naviguer sur Internet, cette configuration est obligatoire (sinon URL introuvables).

Pour cela, il faut renseigner le fichier « /etc/resolv.conf » de chaque machine. Si le serveur ICS a bien fait son travail lorsqu'il s'est connecté à Internet, son fichier « /etc/resolv.conf » est déjà renseigné (voir la configuration dynamique). Il suffit donc de noter le contenu du fichier « /etc/resolv.conf » de la machine ICS, puis de le recopier sur toutes les autres machines.

Rappel :

Le fichier « /etc/resolv.conf » permet d'indiquer le ou les domaines de recherche et les différents serveurs DNS à utiliser pour la navigation Internet.

Par exemple, dans un réseau local, on pourrait avoir un serveur DNS à l'adresse « 192.168.10.1 » chargé de gérer le domaine « mon-domaine.local ». En cas de défaillance du DNS local, on peut faire appel aux serveurs DNS du fournisseur d'accès à Internet (ex : Free) :

```
nameserver 192.168.10.1
nameserver 212.27.32.176
nameserver 212.27.32.177
search mon-domaine.local
```

La première ligne indique l'adresse du serveur DNS du réseau local. En cas de défaillance de ce serveur, les serveurs suivants seront utilisés (serveurs DNS du FAI).
La dernière ligne permet d'indiquer le nom du domaine géré par le serveur DNS local. Par exemple, si on cherche à contacter le serveur « MonServeur », le système cherchera à contacter l'adresse complète « MonServeur.mon-domaine.local » car le nom du serveur indiqué ne comporte pas le domaine de recherche.

Remarque :

Un serveur DHCP réécrit habituellement « resolv.conf » avec ses propres informations DNS à chaque connexion (voir la configuration dynamique).

 ***Mise en pratique : Configurer un réseau avec IP fixes.***

23.4 Configuration dynamique (serveurs DHCP & DNS)

L'idée de cette solution, c'est de concentrer (quasiment) tout le paramétrage sur le seul serveur ICS. De plus, on va optimiser le réseau en allant interroger les DNS du fournisseur d'accès à Internet que lorsque c'est strictement nécessaire. Pour cela, on va utiliser un outil appelé « dnsmasq ». Ce logiciel regroupe un serveur DHCP et un serveur relais DNS :

- Le serveur DHCP permet de ne plus renseigner les adresses IP sur chaque machine. Chaque machine devient "cliente DHCP" et le serveur distribue les adresses IP disponibles dans une plage d'adresses qu'on lui a spécifiée.

- Le relais DNS évite de passer par la liaison Internet à chaque fois qu'il y a un nom de domaine à atteindre : toutes les machines interrogent le serveur relais DNS. Si on lui a déjà posé la question, il répond tout de suite. Sinon, c'est lui qui interroge les serveurs DNS du fournisseur d'accès et qui donne ensuite la réponse (mais il la garde en mémoire pour question ultérieure).

Le relais DNS va mémoriser les noms des machines locales. C'est très important, car les machines étant en DHCP, on ne saura pas quelles seront leurs adresses IP à l'avance. Par contre, leur nom sera toujours à jour. Le démarrage du serveur sera également sécurisé.

1) L'outil « dnsmasq » :

Sur la machine ICS, effectuer les actions suivantes :

- Installer le paquet « dnsmasq » (il faut avoir accès aux dépôts « Universe »).
- Sauvegarder le fichier de configuration original :
  sudo cp -p /etc/dnsmasq.conf /etc/dnsmasq.conf.ori
- Editer le fichier « /etc/dnsmasq.conf » en fonction du besoin réel. Si on a une adresse IP dynamique (le FAI change cette adresse tous les jours), commenter la ligne "no-poll" (avec un # devant) :

```
# Configuration file for dnsmasq.
#
# pour éviter de fournir du trafic DHCP/DNS inutile du coté internet
##domain-needed
bogus-priv
# pour permettre à dnsmasq de suivre vos changements d'IP:
# commentez cette ligne si vous avez une IP qui change
no-poll
# pour limiter l'écoute de requêtes DHCP du coté réseau local
interface=eth0
# nom de votre domaine pour dnsmasq
domain=inet
# activez le serveur DHCP:
dhcp-range=192.168.10.100,192.168.10.150,255.255.255.0,12h
```

2) Configuration « Iptables » :

Créer le fichier de démarrage d'« Iptables » en éditant le fichier « /etc/init.d/iptables » :

```
#!/bin/sh
#
# Script de démarrage qui lance l'interface réseau internet,
# met en place un firewall basique et un partage de connexion
#

start() {
# init du la périphérique internet (ici derriere un modem ADSL ethernet, DHCP client)

/sbin/ifup eth1

# Dans cette partie, on met en place le firewall
#vidage des chaines
iptables -F
#destruction des chaines personnelles
iptables -X

#stratégies par défaut
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

#init des tables NAT et MANGLE (pas forcément nécessaire)
iptables -t nat -F
iptables -t nat -X
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT

iptables -t mangle -F
iptables -t mangle -X
iptables -t mangle -P PREROUTING ACCEPT
iptables -t mangle -P OUTPUT ACCEPT


# Acceptation de toutes les connexions en local (un process avec l'autre)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# PORT FORWARDING:
# attention : on ne peut pas mettre un nom de machine en destination, il faut mettre
# l'adresse IP.
# exemple : on veut qu'un serveur HTTP installé sur une machine du réseau local soit
# visible depuis l'extérieur.
###iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to-destination
###192.168.10.121:80
###iptables -A FORWARD -p tcp -i eth1 --dport 80 -j ACCEPT
```

```
#création d'une nouvelle règle
iptables -N MAregle

#définition de la règle : accepter les nouvelles connexions ne venant pas de l'interface
# internet et accepter toutes les connexions établies et reliées
#(ex: une demande de page HTML provoque l'ouverture
# d'une connexion reliée pour acheminer cette page vers l'ordinateur)

iptables -A MAregle -m state --state NEW -i! eth1 -j ACCEPT
iptables -A MAregle -m state --state ESTABLISHED,RELATED -j ACCEPT

#application de la règle au partage de connexion
iptables -A INPUT -j MAregle
iptables -A FORWARD -j MAregle

# activation du forwarding dans le noyau
# mise en place du partage de connexion sur le réseau local

echo 1 >/proc/sys/net/ipv4/ip_forward
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth1 -j MASQUERADE

}

stop() {
        echo 0 >/proc/sys/net/ipv4/ip_forward
        ifdown eth1
}

case "$1" in
 start)
        start
        ;;

stop)
        stop
        ;;
restart)
        stop && start
        ;;
*)
        echo "Usage $0 {start|stop|restart}"
        exit 1
esac

exit 0
```

Une fois le script créé, il faut le rendre exécutable :

```
sudo chmod ugo+x /etc/init.d/iptables
```

Puis, intégrer ce script dans les séquences de démarrage et d'arrêt de la machine ICS :

```
sudo update-rc.d iptables start 99 2 . stop 00 2 0 1 6 .
```

Attention : Les points font partie de la syntaxe.

3) Ajustements du serveur ICS :

Il reste à effectuer quelques ajustements sur le serveur ICS.

Interfaces :

Il faut modifier le fichier « /etc/network/interfaces ». En effet, on a pu voir que le script « Iptables » s'occupait de démarrer l'interface « eth1 ». Il ne faut donc plus la faire démarrer au "boot" du serveur ICS. Dans le principe, il faut retirer la mention « eth1 » de la ligne qui commence par « auto ».

Le fichier contient également le paramétrage en IP fixe pour « eth0 » (« eth0 » doit être en IP fixe). Pour simplifier, on considère que toutes les machines sont connectées au réseau local (loopback) par l'interface réseau « eth0 » , y compris le serveur ICS.

```
# The loopback network interface
auto lo eth0
iface lo inet loopback

# This is a list of hotpluggable network interfaces.
# They will be activated automatically by the hotplug subsystem.
mapping hotplug
        script grep
        map eth0

# The primary network interface
iface eth0 inet static
        address 192.168.10.1
        netmask 255.255.255.0
# Interface vers internet : eth1
# cette interface est demarree par le script iptables
# donc elle est absente de la ligne "auto"
iface eth1 inet dhcp
```

Hôtes :

Il faut aussi modifier le fichier « /etc/hosts » du serveur ICS :

```
127.0.0.1       localhost.localdomain   localhost
192.168.10.1    serveurICS
```

Remarque :

Après une installation d'Ubuntu, « serveurICS » est sur la même ligne que « localhost ». Sur toutes les machines du réseau, c'est désiré : cela permet à chaque machine de se reconnaître elle-même. L'ennui, c'est que toutes les informations contenues dans le fichier « /etc/hosts » du serveur ICS vont être disponibles à travers le réseau local (via le relais DNS).

Si on ne modifiait pas « /etc/hosts », un « ping serveurICS » à partir de « gandalf » donnerait :

Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128

Sauf que « 127.0.0.1 » n'est pas le serveur ICS, mais « gandalf » lui-même...

dhcclient :

Cette manipulation est à faire sous réserve que le serveur ICS est configuré en "DHCP client" auprès du fournisseur d'accès à Internet. C'est grâce au "DHCP client" que le fichier « /etc/resolv.conf » est automatiquement renseigné sur le serveur ICS. De même, l'adresse IP de la carte « eth1 », ainsi que la "route" par défaut, sont fournies via DHCP.

Comme « /etc/resolv.conf » a été alimenté par DHCP, il contient donc les DNS du fournisseur d'accès. Aucune chance que celui-ci ne connaisse la machine "pippin". Donc à partir du serveur ICS, un « ping pippin » n'a aucune chance d'aboutir. Voici ce qu'il faut faire :

- Editer le fichier « /etc/dhcp3/dhclient.conf »
- Rechercher et décommenter la ligne « prepend domain-name-servers 127.0.0.1 »
- Sauvegarder la modification

En clair, cette modification indique ceci au serveur ICS : "Pour rechercher un nom, adresse-toi d'abord à toi-même, et si tu n'y arrives pas, alors fait comme d'habitude".

4) Pour les autres machines :

Pour que tout fonctionne, il faut que les autres machines du réseau s'intègrent correctement dans celui-ci.

Si les cartes « eth0 » ont été configurées en dur, il faut les remettre en DHCP. Pour cela, modifier le fichier « /etc/dhcp3/dhclient.conf » :

- Editer le fichier « /etc/dhcp3/dhclient.conf »
- Rechercher la ligne contenant « send host-name »
- La compléter et la décommenter : send host-name "monpc"
  où « monpc » est le nom du poste (attention à la syntaxe avec guillemets)

Cette modification est nécessaire pour que les machines inscrivent leurs noms dans le serveur DNS relais (installé sur le serveur ICS).

5) Comment ça marche ?

Rebooter le serveur ICS, puis rebooter les autres machines du réseau local.

Quand une machine du réseau local démarre, voici ce qu'elle fait :

- Recherche d'un serveur DHCP, le serveur ICS répond.
- Le serveur ICS fournit une adresse DHCP dans la plage 192.168.10.100 à 192.168.10.150.
- Le serveur ICS renseigne le fichier « /etc/resolv.conf » de la machine : il se met lui-même 192.168.10.1, car il est serveur relais DNS.
- Le serveur ICS renseigne la "route" par défaut. Il se nomme lui-même en "route" par défaut car c'est lui qui effectue le partage de la connexion Internet.

À ce stade, on peut également installer une machine Windows dans le réseau local : en laissant le paramétrage TCP/IP et les DNS sur "obtenir automatiquement" (par défaut), elle sera reconnue par tout le réseau.

Quand on fait un « ping gandalf », ce n'est pas forcément l'IP « 192.168.10.103 » qui va répondre (par exemple), mais on sera certain que c'est bien la machine « gandalf ». On est maintenant en IP dynamiques.

6) En cas de problème :

Quelques pièges à éviter :

- La plage DHCP n'était pas dans le même réseau local que l'interface Ethernet (ex : plage 192.168.0.100-192.168.0.150 alors que l'interface est en 192.168.1.1).
- Le réseau local référencé dans la commande POSTROUTING du script « Iptables » ne correspondait pas au réseau local dans lequel était la patte locale du serveur.
- Confondre « eth0 » et « eth1 » dans « Iptables », du coup, le serveur n'était pas joignable en local…

Mise en pratique : Configurer un réseau avec IP dynamiques.

24 Partage de bureau à distance avec VNC

24.1 Généralités

Cette option permet de configurer et d'utiliser le bureau d'un ordinateur à distance (via un réseau), et ce, en prenant le contrôle du clavier et de la souris de cette machine. En anglais, c'est le « Virtual Network Computing » ou VNC.

VNC est indépendant de la plateforme : un client VNC installé sur n'importe quel système d'exploitation peut se connecter à un serveur VNC installé sur un autre système d'exploitation.

24.2 Utilisation

Sous Linux Ubuntu, on peut configurer ces paramètres "serveur" via le menu GNOME : « Système / Préférences / Bureau à distance » (en autorisant le partage).

Une fois ce service activé, on peut aller sur une autre machine "cliente", ouvrir le menu « Applications / Internet / Visionneur de bureaux distants » et « Se connecter » en VNC : entrer alors l'adresse IP ou le nom de la machine hôte (ex : 127.0.0.1 ou localhost) pour voir apparaître son écran de bureau et l'utiliser à distance.

L'application Ubuntu qui gère le partage de bureau à distance est « vino », un véritable client/serveur VNC. Malheureusement, celle-ci transporte en continu le pointeur de souris, ce qui rend la connexion lente avec un décalage d'affichage.

Une alternative est d'utiliser « x11vnc » comme serveur VNC.

Remarques :

Pour des raisons de sécurité, il peut être nécessaire de désactiver le bureau à distance (VNC n'étant pas un protocole sécurisé).

« vino » peut également utiliser le protocole « Secure Shell » ou SSH (sécurisé).

Dans tous les cas, il est fortement recommandé de spécifier un mot de passe lors de l'ouverture du service.

Mise en pratique : Tester un partage de bureau à distance.

25 Connexions distantes sécurisées avec SSH

25.1 Généralités

SSH (Secure Shell) est à la fois un programme informatique et un protocole de communication sécurisé. Il permet de se connecter à un ordinateur distant afin d'obtenir un Shell avec ligne de commande (console), et possède un protocole de transfert de fichiers complet. Idéal pour un « partage de fichiers sécurisé ».

SSH peut également être utilisé pour transférer des ports TCP d'une machine vers une autre, créant ainsi un tunnel. Cette méthode est couramment utilisée afin de sécuriser une connexion qui ne l'est pas (par exemple le protocole email POP3) en la faisant transférer par le biais du tunnel chiffré SSH.

Habituellement, le protocole SSH utilise le port 22.

OpenSSH est une version libre de la suite de protocole de SSH. Beaucoup d'utilisateurs de VNC, Telnet, Rlogin, FTP, ou d'autres programmes similaires, ne se rendent pas compte que leur mot de passe est transmis en clair à travers les réseaux. OpenSSH chiffre tout le trafic à l'aide de clés de chiffrement (mot de passe y compris). OpenSSH fournit également une variété de méthodes d'authentification. Comme son nom l'indique, OpenSSH est développé dans le cadre du projet OpenBSD.

25.2 Installation

Installation du serveur SSH :

Pour accéder à son PC depuis un autre endroit (à distance), on doit le transformer en serveur au préalable.

Installer le paquet « apt://openssh-server » sur le poste concerné. Par défaut, il se lance au démarrage.

Pour l'activer après une fausse manipulation :

```
sudo /etc/init.d/ssh start
```

Pour l'arrêter :

```
sudo /etc/init.d/ssh stop
```

Installation du client SSH :

Sur le poste client (qui va prendre l'accès à distance), « openssh-client » installé par défaut sous Linux Ubuntu, doit être présent.

Remarque : Pour prendre le contrôle sur un poste équipé de Windows, installer « PuTTY » qui est

disponible sous licence MIT (type BSD).

25.3 Utilisation

Se connecter à un ordinateur distant via SSH :

Pour ouvrir une session sur un ordinateur distant ayant un serveur SSH, saisir la commande :

```
ssh <username>@<ipaddress> -p <num_port>

ssh phyrex@192.168.23.42 -p 12345
```

L'option « -p xxx » est facultative. Si rien n'est précisé, c'est le port 22 par défaut qui sera utilisé.

Pour se connecter avec SSH en IPv6 depuis un terminal :

```
ssh -6 <nom>@<adresse ipv6>
```

Soit par exemple pour un lien Internet :

```
ssh -6 alfred@2a01:e35:2431::2e57
```

On peut aussi appeler un ordinateur par son nom :

```
ssh utilisateur@nom_machine
```

A partir du moment où celui-ci est "résolu" par DNS sur la machine. Cela peut se faire sur le réseau local par le fichier « /etc/hosts » (éventuellement distribué d'un serveur vers les clients locaux au travers d'un partage NIS), ou par un service de DNS si on accède à une machine distante pour laquelle on a enregistré un nom de domaine (serveur loué).

Authentification par mot de passe :

L'authentification par mot de passe (transmis chiffré) est le mode d'identification par défaut.

Suite à l'installation du paquet « openssh-server », il peut parfois être nécessaire de modifier le fichier de configuration SSH « sshd_config », notamment si on rencontre le problème suivant :

```
moi@maison:~$ ssh user@domain.com
Permission denied (publickey).
```

Dans ce cas, modifier le fichier « /etc/ssh/sshd_config » de la manière suivante (avec sudo) :

```
# Change to yes to enable tunnelled clear text passwords
PasswordAuthentication yes
```

Puis redémarrer le service SSH avec la commande :

sudo /etc/init.d/ssh restart

Navigation via « sftp » (secure file transfer protocol) et « Nautilus » :

En utilisant le navigateur de fichiers « Nautilus » d'Ubuntu, on peut également accéder aux emplacements à distance par l'intermédiaire de SSH et visualiser, éditer ou copier des fichiers.

Ouvrir « Nautilus », puis dans la fenêtre « Emplacement » (Ctrl–L), entrer l'URL suivante :

ssh://username@hostname:port

(remplacer « username », « hostname » et « port » en conséquence).

La copie de fichiers se fait par le glisser-déposer directement dans la fenêtre de « Nautilus », comme avec le système de fichiers local.

Pour accéder directement à un répertoire donné (pratique avec l'utilisation des signets), il suffit de rajouter le chemin en fin d'URL :

ssh://username@hostname:port/le/chemin/voulu/

Enfin, il est également possible d'avoir accès à SSH dans « Nautilus » par :

« Fichier => Se connecter à un serveur... » et choisir le « Type de service » SSH.

Puis de renseigner les valeurs de « Serveur », « Port », « Nom d'utilisateur » (et « Dossier).

Remarque : De la même façon, « Nautilus » permet de se connecter à un serveur FTP simple.

Copier des fichiers via SSH :

Pour copier un fichier à partir d'un ordinateur sur un autre avec SSH, utiliser la commande « scp » :

scp <fichier> <username>@<ipaddress>:<DestinationDirectory>
scp -6 <élément> <nom>@[addresse ipv6]:<destination>

Exemples :

scp fichier.txt hornbeck@192.168.1.103:/home/hornbeck
scp -6 fichier.txt albertine@[2a01:e35:2431::2a34]:/home/albertine

Ou copier un répertoire vers un ordinateur :

scp -r répertoire hornbeck@192.168.1.103:/home/hornbeck/
scp -6r répertoire/ albertine@[2a01:e35:2431::2a34]:/home/albertine

Copier des fichiers à partir d'ordinateurs à distance sur son disque local :

scp hornbeck@192.168.1.103:/home/hornbeck/urls.txt .

Le point à la fin de commande indique le répertoire courant pour destination. On peut aussi le renommer en le copiant (« mon.txt ») sur le disque local :

scp hornbeck@192.168.1.103:/home/hornbeck/urls.txt ./mon.txt

Copier un fichier d'un ordinateur vers un autre tout en étant sur un troisième ordinateur :

scp nom@ordi1:chemin/fichier nom@ordi2:chemin/fichier

Monter un répertoire distant en utilisant « sshfs » :

« sshfs » est un outil permettant d'utiliser le protocole SSH comme un système de fichiers et ainsi monter un répertoire distant en SSH. Pour l'utiliser, il suffit d'installer le paquet « apt://sshfs » puis de saisir la commande de montage :

sshfs <username>@<ipaddress>:/RepertoireDistant /Emplacement de montage

 ***Mise en pratique : Installer et utiliser un serveur SSH.***

26 Le routage sous Linux

26.1 Généralités

Le routage est fort utile pour créer un sous-réseau et ainsi cacher des ordinateurs derrière un seul.

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, selon un ensemble de règles formant la table de routage. Les premiers routeurs étaient de simples ordinateurs ordinaires.

Pré-requis :

Pour faire un routeur de son ordinateur, il faut :

- deux cartes réseau installées (si on veut séparer les réseaux)
- deux réseaux différents à relier (on peut les créer soi-même)

Il n'est pas obligatoire d'utiliser 2 cartes réseau ou plus afin de séparer les réseaux. L'utilisation de plusieurs cartes réseau transforme juste l'ordinateur concerné en « bastion ».

Cette façon de faire est recommandée si l'on souhaite séparer physiquement 2 réseaux distincts, et permet un contrôle total des échanges entre les 2 réseaux au niveau de la machine.

26.2 Installation d'un réseau (rappel)

Pour créer un réseau, il suffit d'associer une adresse IP à l'une des interfaces du système. Par exemple, on peut associer l'adresse IP « 190.1.1.173 » à l'interface « eth0 » en tapant la commande :

```
sudo ifconfig eth0 add 190.1.1.173
```

Pour vérifier cette association :

```
ifconfig
```

Remarque : On peut associer autant de réseaux que l'on souhaite à une interface.

On peut maintenant communiquer avec toutes les machines qui sont sur le même réseau que nous (ayant une autre adresse IP du réseau et reliées directement ou indirectement à la même carte réseau).

Pour que Linux Ubuntu se souvienne de cette association au redémarrage de l'ordinateur, il faut modifier le fichier « /etc/network/interfaces » (en précisant la commande « up » suivie de la nouvelle "route"). Par exemple, pour supprimer la "route" « default », rajouter dans le fichier interface :

up route del default

Remarque : Lorsqu'on associe une adresse IP à une interface, la table de routage est automatiquement mise à jour.

26.3 Description du routage

Pour visualiser la table de routage actuelle :

route -n

```
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
10.0.1.0        0.0.0.0         255.255.255.0   U     2      0        0 wlan0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlan0
0.0.0.0         10.0.1.1        0.0.0.0         UG    0      0        0 wlan0
```

Le tableau ci-dessus s'affiche avec une ligne par route. Les colonnes indiquent chacune une information sur la route paramétrée :

1. **La destination (Réseau) :** C'est une adresse IP qui indique quels sont les paquets de données qui vont suivre cette route selon leur destination.
2. **La passerelle (Gateway) :** C'est une adresse IP qui indique par où les paquets vont passer pour arriver à destination. Ils seront envoyés à cette adresse.
3. **Le masque de sous-réseau (Genmask) :** C'est une suite de 4 octets (comme une adresse IP) qui permet d'indiquer quelle est la taille de chaque partie de l'adresse IP (partie réseau et partie hôte). Par exemple « 255.255.255.0 », comme ci-dessus, indique que les 3 premiers octets seront utilisés pour le réseau et le dernier pour les adresses d'hôtes.
4. **Les indicateurs :** Ils correspondent à l'état de la route (ici 'U' signifie que la route est active (Up) et 'G' que la route est une passerelle « Gateway »). Il existe d'autres indicateurs mais ils sont moins courants (taper « man route » pour les découvrir).
5. **Les sauts (Metric) :** C'est un nombre qui indique combien d'intermédiaires il reste avant d'arriver à la destination. Cette information n'est plus utilisée (sauf par des programmes comme « routed RIP »).
6. **Les références (Ref) :** C'est un nombre qui indique le nombre de références associées à cette route. Cette information n'est pas utilisée.
7. **L'utilisation (Use) :** C'est un compteur d'utilisation de la route.
8. **L'interface réseau (Iface) :** C'est le nom de l'interface réseau qui sera utilisée pour cette route. Pour avoir la liste des interfaces disponibles taper « ifconfig ».

Remarque : La dernière ligne de la table correspond à ce que l'on nomme plus couramment la passerelle par défaut.

26.4 Modification du routage

Nous allons maintenant voir comment mettre en oeuvre le routage entre 2 réseaux, en utilisant les commandes « ifconfig » et « route ».

Objectif :

Faire communiquer 2 ordinateurs qui ne sont pas sur le même réseau, mais qui sont tous les 2 connectés au même routeur.

Données :

- Le réseau A : 190.1.1.0/255.255.255.0 (de 190.1.1.1 à 190.1.1.254)
- L'adresse IP du poste A sur le réseau A : 190.1.1.2
- Le réseau B : 193.17.1.0/255.255.255.0 (de 193.17.1.1 à 193.17.1.254)
- L'adresse IP du poste B sur le réseau B : 193.17.1.2

Solution :

Il faut tout d'abord avoir une adresse IP sur le réseau de destination afin de communiquer avec par le biais de l'interface qui y est connectée. Attention de ne pas prendre une adresse IP déjà utilisée !

1) Sur le routeur, paramétrer l'interface réseau connectée au réseau A comme dit précédemment (par exemple : 190.1.1.1).

2) Sur le routeur, paramétrer l'interface réseau connectée au réseau B (par exemple : 193.17.1.1).

3) Si besoin, configurer la table de routage du poste A :

```
sudo route add -net 193.17.1.0 netmask 255.255.255.0 gw 190.1.1.1
```

4) Si besoin, configurer la table de routage du poste B :

```
sudo route add -net 190.1.1.0 netmask 255.255.255.0 gw 193.17.1.1
```

Astuce : Il est possible de ne pas toucher aux tables de routage des postes clients, si le routeur est déjà leur route par défaut.

Maintenant, si on fait un « ping » du poste A ou du poste B vers son homologue du réseau opposé, on peut remarquer qu'ils peuvent communiquer ensembles.

 ***Mise en pratique : Configurer un routage.***

27 Configuration d'un proxy Web léger

27.1 Généralités

Un proxy, "serveur mandataire" ou "bastion" en bon français, est un serveur informatique dont le rôle est de servir de relais entre un client (vous) et un serveur (le site Web que vous souhaitez consulter).

Les entreprises utilisent très souvent un proxy, afin de pouvoir contrôler les sorties de leurs employés sur Internet. Quand vous vous connectez à Internet à partir du travail, il se peut qu'une boite de dialogue s'ouvre et vous demande un identifiant (et un mot de passe) pour surfer sur Internet : c'est le proxy qui demande cette authentification pour vous autoriser ou non l'accès au site désiré.

Tinyproxy est un proxy Web très léger. Il ne crée pas de cache des pages visitées.

27.2 Installation

Tinyproxy est très simple d'installation puisqu'il est présent dans le dépot « Universe ». Il suffit donc d'installer le paquet « tinyproxy » (apt://tinyproxy).

27.3 Configuration

Le fichier de configuration à modifier est « /etc/tinyproxy/tinyproxy.conf ».

Pour modifier les restrictions d'accès, adapter les lignes comme ceci :

```
# The following is the authorization controls. If there are any access
# control keywords then the default action is to DENY. Otherwise, the
# default action is ALLOW.
#
# Also the order of the controls are important. The incoming connections
# are tested against the controls based on order.
#
Allow 127.0.0.1
Allow 192.168.1.0/25
```

Pour personnaliser les pages d'erreur :

```
cd /usr/share/tinyproxy
```

Tinyproxy s'exécute comme un service « daemon ». Pour l'arrêter, le démarrer et le redémarrer :

```
sudo /etc/init.d/tinyproxy stop
sudo /etc/init.d/tinyproxy start
sudo /etc/init.d/tinyproxy restart
```

Attention : Depuis la version 1.8.1, lorsque l'on veut le faire tourner sur un port < 1024, il faut spécifier :

« User root »

Site officiel : http://tinyproxy.sourceforge.net

Mise en pratique : Configurer un proxy.

28 Installation d'une imprimante

28.1 Pré-requis

Pour l'installation, s'assurer d'avoir connecté l'imprimante à l'aide d'un port USB ou parallèle.

Remarque : Pour l'installation d'une imprimante par port série, utiliser plutôt « CUPS » afin de déterminer la bonne configuration.

28.2 Par port USB

Si on dispose d'une imprimante USB, elle est automatiquement détectée. On peut alors lancer une impression directement.

Pour savoir si l'imprimante a bien été (ou mal) détectée, ouvrir le gestionnaire de configuration des imprimantes :

- **Pour Ubuntu :** Système => Administration => Impression
- **Pour Kubuntu :** Menu K => Paramètres du système => Imprimantes
- **Pour Xubuntu :** Applications => Paramètres => Impression

Dans la fenêtre qui s'affiche, choisir l'imprimante dans la liste, puis dans l'onglet « Paramètres », cliquer sur « Imprimer la page de test ».

Si cela ne fonctionne pas, cliquer sur « Modifier… » en face de la ligne « Fabricant et modèle » et choisir le bon pilote. Si celui-ci n'est pas présent, essayer le modèle le plus proche, sinon l'installer.

28.3 Par port parallèle

Ouvrir le gestionnaire de configuration des imprimantes :

- **Pour Ubuntu :** Système => Administration => Impression
- **Pour Kubuntu :** Menu K => Paramètres du système => Imprimantes
- **Pour Xubuntu :** Applications => Paramètres => Impression

Puis :

- Cliquer sur : Édition => Nouvelle imprimante
- Cliquer sur : « LPT #1 » et faire « Suivant »
- Choisir la marque de l'imprimante et faire « Suivant »
- Choisir le modèle de l'imprimante et faire « Suivant »
- Donner un nom à l'imprimante et faire « Appliquer »

Voilà, l'imprimante est installée.

28.4 Commandes utiles

La suite « lp* » est présente sur la plupart des distributions Linux. Elle consiste en un ensemble de commandes permettant d'interagir avec les imprimantes :

- **lp :** permet d'imprimer un (ou des) fichier(s).
- **lpr :** permet d'imprimer un (ou des) fichier(s).
- **lpq :** permet d'afficher la file d'attente d'une imprimante.
- **lprm :** permet de supprimer des jobs de la file d'attente (voir aussi la commande « cancel »).
- **lpstat :** permet d'afficher des informations détaillées sur le serveur d'impression. Par exemple, pour voir l'imprimante par défaut : lpstat -d
- **lpoptions :** permet d'afficher ou de modifier la configuration du serveur d'impression. Par exemple, pour changer l'imprimante par défaut : lpoptions -d autreimprimante (commande « CUPS » seulement).
- **lpmove :** permet de déplacer un job (une impression) de la file d'attente d'une imprimante à une autre imprimante.
- **lpc :** permet de contrôler interactivement les imprimantes.

 ***Mise en pratique : Tester une impression (si possible).***