

Collection
Ressources Informatiques

UBUNTU

Administration d'un système Linux

Gilles CHAMILLARD

 INFORMATIQUE TECHNIQUE



UBUNTU

Administration d'un système Linux

Gilles CHAMILLARD



Résumé

Ce livre sur Ubuntu présente de façon progressive tous les atouts de cette distribution de Linux.

Le **technicien ou l'administrateur système** trouveront les réponses aux questions qu'ils se posent, vis à vis des autres distributions Linux ou pour la **mise en place des outils spécifiques** Ubuntu. Le lecteur simplement désireux de s'informer trouvera, quant à lui, les bases nécessaires pour une **mise en pratique facile et complète** de la distribution.

L'ouvrage peut être lu de deux façons : chapitre après chapitre dans l'optique de la découverte du système, ou en ciblant les chapitres liés à des concepts, à une pratique ou à un thème. Ce livre sert de base à l'apprentissage du système Linux dans le cadre de la **formation de technicien supérieur en informatique**. L'auteur a donc choisi, ponctuellement, de poser des séries de **questions (corrigées)** destinées à vérifier l'appropriation des acquis.

La version traitée dans le livre est la **LTS** (Long Term Support) en version 8.04 au moment de l'écriture.

L'auteur

Gilles Chamillard est professeur en BTS informatique de gestion, option Administrateur de réseaux locaux d'entreprise et assure des formations Technicien Micro Réseaux et Internet au Conservatoire National des Arts et Métiers (CNAM de Paris). Convaincu qu'une pratique réussie apporte ou améliore les qualifications professionnelles, il donne au lecteur dans cet ouvrage toutes les clefs pour atteindre ce but.

Ce livre numérique a été conçu et est diffusé dans le respect des droits d'auteur. Toutes les marques citées ont été déposées par leur éditeur respectif. La loi du 11 Mars 1957 n'autorisant aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective", et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, "toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayant cause, est illicite" (alinéa 1er de l'article 40). Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal. Copyright Editions ENI

Chapitre 1 : Ubuntu et Linux

A. Affirmation du modèle OpenSource.	7
1. Principe du modèle, son avenir	7
a. OpenSource et capitalisme financier	7
b. OpenSource et logiciel libre	9
2. Place de Linux dans le modèle	10
3. Principaux outils OpenSource	11
B. Ubuntu : les raisons d'un succès.	13
1. Point de départ	13
a. Les origines	13
b. Plus de renseignements sur le fondateur...	14
2. Qualités de la distribution.	14
a. Points forts de la distribution	15
b. Un mot sur la distribution pour les serveurs.	16
c. Pourquoi l'adopter ?	16
C. Déclinaisons Ubuntu.	17
1. Historique des versions.	18
2. Déclinaisons d'une même version	18
a. Suivant la destination	19
b. Suivant l'environnement graphique.	23
c. Suivant les fonctionnalités	26
D. Administrateur système Ubuntu	30
1. Rôle de base	31
2. Missions étendues	31

E. Conventions typographiques.	32
1. Terminologie anglaise	32
2. Exemples	32
3. Commandes et code	32
a. Présentation	32
b. Exécution	33

Chapitre 2 : Préalable à l'installation

A. Avant l'installation	37
1. Implantations de la distribution	37
a. Type d'implantations	37
b. Spécifications	38
2. Outils pour l'administrateur	40
a. Utilisation de la distribution Ubuntu live	40
b. Utilisation d'un logiciel de virtualisation	40
3. Ressources nécessaires	42
a. Liste des images de la distribution Hardy Heron 8.04	42
b. Vérification de l'empreinte d'une image ISO	44
B. Découverte de la distribution	45
1. Fonctionnement du matériel	46
a. Informations et tests	47
b. Autres informations	50
2. Arborescence des fichiers	51
a. Structure du système	51
b. Types de système de fichiers	53
C. Plan de partitionnement	54
1. Principes d'identification	54
a. Identification des périphériques	54
b. Étiquette et UUID	55
2. Choix des partitions	56

D. Initialisation du système	56
1. Processus de démarrage	56
2. Chargeurs de démarrage	58
a. GRUB	58
b. LILO	59
E. Dépôts logiciels	60
1. Types de dépôts	60
2. Serveurs miroirs	61

Chapitre 3 : Processus d'installation

A. Installation normale d'un poste de travail	65
1. Préalable à l'installation	65
2. Processus d'installation	65
a. Écran de bienvenue	66
b. Écran de l'emplacement géographique	67
c. Écran de disposition du clavier	67
d. Écran de préparation de l'espace disque	68
e. Écran de l'identité du "super" utilisateur	69
f. Écran de "Prêt à installer"	70
 B. Installation en mode expert d'un serveur	 71
1. Préalable à l'installation	71
2. Première phase du processus d'installation	71
a. Sélection de la langue	71
b. Passage en mode texte	71
3. Deuxième phase du menu d'installation	77
a. Ligne "Choisir la langue"	77
b. Ligne "Configurer le clavier"	78
c. Ligne "Détecter et monter le CD"	78
d. Ligne "Charger un fichier de configuration"	79
e. Ligne "Charger des composants d'installation à partir du CD"	80

4.	Troisième phase du menu d'installation	81
a.	Ligne "Détecter le matériel réseau".	81
b.	Ligne "Configurer le réseau"	82
c.	Ligne "Configurer l'horloge"	82
d.	Ligne "Détecter les disques"	82
e.	Ligne "Partitionner les disques"	82
f.	Ligne "Installer le système de base"	86
g.	Ligne "Créer les utilisateurs et choisir les mots de passe" .	88
h.	Ligne "Configurer l'outil de gestion des paquets"	88
i.	Ligne "Choisir et installer des logiciels"	89
j.	Ligne "Installer le programme de démarrage GRUB sur un disque dur"	90
k.	Ligne "Terminer l'installation"	91

Chapitre 4 : Installations particulières

A. Installations particulières d'un poste de travail	95
1. Avec Windows sous la forme d'une application	95
a. Principes de fonctionnement	96
b. Conditions de ressources.	96
c. Processus d'installation	97
d. Pourquoi utiliser Wubi ?	99
2. Avec un autre système en "dual boot".	100
a. Avant l'implantation.	101
b. Situation n°1 : aucun espace libre.	101
c. Situation n°2 : un espace libre existant.	103
d. Démarrage et échanges entre les systèmes	105
e. Pourquoi disposer d'un double système d'exploitation ? . .	109
3. Supplément : avec Windows en machine virtuelle Jeos	109
a. Principes de fonctionnement	109
b. Différences d'installation	110
c. Intérêt de Jeos	110
B. Installations particulières d'un serveur	110
1. Avec un système de disques RAID	110
a. Partitionnement en RAID 1.	111
b. Maintenance.	114
c. Partitionnement en RAID 5.	117

2.	Avec un système de partitions en LVM	117
a.	Principes de fonctionnement	117
b.	Partitionnement en RAID 5 avec LVM	117
c.	Maintenance.	121
d.	Manipulations	122

Chapitre 5 : Gestion des droits utilisateurs

A. Ouverture d'une session	127
1. Sur un serveur	127
a. Phase de démarrage	127
b. Rétablir le compte de l'administrateur	128
2. Sur un poste de travail	130
a. Interface GDM	130
b. Réglages de l'interface	132
3. Authentification locale	133
a. Principes d'une connexion	133
b. Fichiers de connexion	133
B. Droits des utilisateurs	138
1. Utilisateurs et attributs de fichiers	138
a. Principes	138
b. Changement des attributs de fichiers	139
c. Changement de propriétaire ou de groupe	140
d. Droits supplémentaires	141
2. Entraînement	142
C. Droits par l'interface graphique	143
1. Droits et espace de travail	143
a. Dossier personnel de l'utilisateur	143
b. Modification des droits	144
2. La commande <code>gsudo</code> et PolicyKit	145

➤ Chapitre 6 : Prise en main de la distribution

A. Démarrage et premiers réglages	151
1. Réglages du chargeur de démarrage	151
a. Fichier /boot/grub/menu.lst	151
b. Cas d'un double système au démarrage	154
2. Connexion au réseau	154
a. Fichier /etc/network/interfaces.	155
b. Network Manager.	158
3. Réglages particuliers	160
a. Changement de l'image splash de GRUB	160
b. Changement de thème pour GDM	162
c. Autres réglages.	163
B. Sources de paquets logiciels	164
1. Principe des paquetages	164
a. Manuellement avec le fichier sources.list	165
b. Sources et interface graphique	168
c. Cas d'un serveur mandataire	169
2. Interfaces de gestion de paquets	170
a. Utilitaire dpkg	171
b. Utilitaire Apt.	172
c. Utilitaire Aptitude.	173
d. Utilitaire Wajig	175
e. Gestion graphique	176

C. Services au démarrage	177
1. Niveaux d'exécution	177
a. Détails sur les niveaux d'exécution.	177
b. Upstart en remplacement d'inittab.	178
2. Utilitaires de gestion des services	180
a. Méthode update-rc	180
b. Méthode sysv-rc-conf	181
c. Méthode sysvconfig	182
d. Méthode par l'interface graphique	183

Chapitre 7 : Session de travail en mode console

A. Contexte d'une session de travail	187
1. Interpréteur de commandes	187
a. Englobement ou expressions rationnelles du shell	187
b. Redirections	188
c. Tubes	189
2. VIM ou l'éditeur de l'administrateur.	190
a. Éditeur et traitement de texte.	190
b. L'éditeur de texte VI.	191
c. Utilisation optimisée de VIM	193
B. Environnement et cadre de travail	196
1. Outils de base	196
a. Fichiers de session	196
b. Manuel en ligne	198
c. Complétion	198
d. Historique des commandes.	199
2. Travailler sur les répertoires	199
a. Organisation des fichiers.	199
b. Commandes usuelles	201

3.	Travailler sur les fichiers	205
a.	Types de fichiers	205
b.	Processus de création d'un fichier	206
c.	Pointeur sur un fichier : le lien	206
d.	Commandes usuelles	207
4.	Entraînement	209

Chapitre 8 : Session de travail en mode graphique

A. Système X Windows Xorg.	213
1. Gestion de l'installation.	213
a. Serveur X minimal	213
b. Composants d'un environnement graphique	215
c. Gestionnaire de fenêtres FluxBox	216
2. Configuration du serveur Xorg	217
a. Configuration manuelle par le fichier xorg.conf.	217
b. Utiliser la commande de configuration dpkg-reconfigure.	222
c. Utiliser la commande graphique displayconfig-gtk	223
B. Environnement et cadre de travail	223
1. Paramétrage d'une session graphique à l'ouverture	224
2. Organisation du bureau.	224
3. Autres préférences.	226
C. Personnalisation du bureau GNOME	227
1. Avoir un bureau en 3D.	227
a. Réglages par défaut.	227
b. Effets spéciaux.	228
2. Lanceur d'applications	231
a. GNOME-do	231
b. AWN	233
3. Gadgets de bureau	234

Chapitre 9 : Administration des ressources

A. Gestionnaire de périphériques UDEV	239
1. Découverte des périphériques	239
a. Enregistrement d'un périphérique	239
b. Découverte dynamique	240
2. Fonctionnement d'UDEV	240
a. Fichiers de base	240
b. Principe d'une règle	242
c. Problème en cas de changement de carte réseau	244
B. Ajout de périphériques au système	244
1. Impression et imprimantes	244
a. Connecter une imprimante	245
b. Devenir un serveur d'impression	248
2. Branchement d'un scanner	248
3. Ajout d'un disque supplémentaire	249
C. Ajout de ressources au système	252
1. Connexion à distance	252
a. Prise de contrôle à distance avec Vinagre	252
b. Ouverture d'une session à distance avec SSH	254
c. Partage de fichiers sur le réseau	255

2.	Méthodes supplémentaires d'ajout de programmes	258
a.	Par les sources.	259
b.	Installation d'un logiciel au format binaire	261
c.	Autres possibilités d'installations	262
1.	Logiciels Windows avec Wine sous Ubuntu	262
a.	Principe et installation.	262
b.	Configuration et installation d'un programme	263

Chapitre 10 : Maintenance de base du système

A. Administration des utilisateurs.	269
1. Principes, commandes et tâches	269
a. Principales commandes	269
b. Exemples d'utilisation	270
2. Gestion avancée des utilisateurs	273
a. Utilisateur modèle	273
b. Utilisation des quotas de disque	273
c. Accorder des droits supplémentaires avec sudo	274
B. Problèmes de maintenance	276
1. "Sur quelle version Ubuntu suis-je exactement ?"	277
2. "J'ai perdu mon mot de passe administrateur..."	277
3. "Le serveur graphique ne répond plus..."	279
4. "J'ai un programme qui bloque, impossible de l'arrêter..."	279
5. "La console n'est pas/plus en français..."	279
6. "GRUB fait une erreur au démarrage du système..."	282
7. "À quoi sert le mode Recovery ?"	283
C. Administration des ressources	284
1. Planification des tâches	284
a. Fonctionnement de cron	285
b. Définir une crontable personnelle	286

2.	Surveillance du système par les processus	286
a.	Notion de processus	286
b.	Vérification et surveillance des processus	287
c.	"Tuer" un processus	290
d.	Moniteur du système en mode graphique	291
3.	Surveillance du système par les journaux	292
a.	Consignation des évènements	292
b.	Archivage des fichiers journaux	294

Chapitre 11 : Maintenance avancée du système

A. Manipulations en ligne de commandes	299
1. Expressions régulières	299
a. Expressions régulières atomiques ou ERA	299
b. Expressions régulières simples ou ERS	300
c. Expressions régulières étendues ou ERE	302
d. Utilisation des expressions régulières avec grep	302
2. Commandes d'édition ou filtres de fichiers	303
3. Entraînement	308
4. Montage et démontage manuel d'un système de fichiers	310
a. Principes de montage	311
b. Démontage	312
5. Stratégies et outils de sauvegarde	312
a. Principes de la sauvegarde de données.	312
b. Commandes et outils de sauvegarde	313
 B. Interventions sur le noyau	 316
1. Principes.	316
a. Les méthodes	317
b. Préparation de l'environnement	317
2. Changer le noyau par Aptitude.	318
a. Modification pour GRUB.	319
b. Nettoyage	319

- 3.** Construction d'un autre noyau 320
 - a.** Charger les sources 320
 - b.** Compiler le nouveau noyau. 321
- 4.** Accélérer le démarrage du système. 324
 - a.** Principe. 324
 - b.** Méthodologie de réalisation 324

Chapitre 12 : Sécurisation du système

A. Gestion des profils utilisateurs	331
1. ACL avec Apparmor	331
2. Administration des profils	332
a. Fonctionnement d'Apparmor	332
b. Commandes	334
c. Création d'un profil	336
B. Politique d'authentification	338
1. Modules PAM	338
a. Principes	338
b. Configuration et structure des fichiers	339
c. Exemple du fichier /etc/pam.d/login	340
2. Utilisation de PAM pour une configuration à un annuaire	343
a. Connexion à un serveur LDAP	343
b. Connexion à un serveur Active Directory	346
3. Plus de sécurité avec PAM	350
a. Restriction horaire	350
b. Mots de passe renforcés	350
C. Politique d'accès	352
1. Réglages essentiels	353
a. Désactivation/Activation d'IPv6	353
b. Fichier sysctl.conf et routage	353

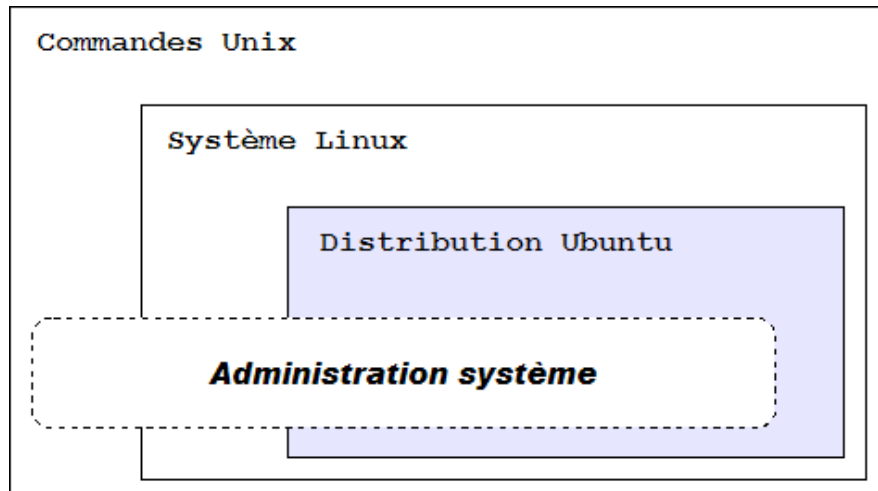
2.	Mise en place de règles de pare-feu	356
a.	En ligne de commandes avec UFW	356
b.	Par une interface graphique avec FireStarter	359
c.	Configuration	360

Annexes

A. Services courants de la distribution Ubuntu	365
B. Corrections des entraînements.	369
1. Chapitre Gestion des droits utilisateurs	369
2. Chapitre Session de travail en mode console.	370
3. Chapitre Maintenance avancée du système	373

Avant-propos

La singularité de rédaction d'un ouvrage sur Linux et son administration ne réside pas dans son thème, mais dans la présentation de son contenu. Schématiquement, l'administration système UNIX/Linux, pour une distribution, se retrouve dans trois éléments imbriqués :



Pour cet ouvrage, l'accent a été mis résolument sur le dernier élément : celui de la distribution **Linux Ubuntu**. Cela induit trois remarques :

- l'ouvrage traite des notions d'administration d'un système UNIX/Linux à travers le prisme de la distribution Ubuntu. Il ne concurrence pas, mais complète les autres manuels dans cette matière.
- l'ouvrage peut s'adresser à des utilisateurs ayant des connaissances limitées du système Linux. Toutes les informations présentées sont exploitables sans formation préalable, même si une connaissance légère du système Linux est appréciée pour la compréhension plus rapide du système et la recherche d'approfondissements.
- l'obsolescence rapide des ouvrages en informatique est tempérée ici par le support d'une version LTS (*Long Time Support*) d'Ubuntu. Dite de longue durée (5 ans), cette distribution apporte la pérennité d'une utilisation dans le milieu professionnel.

Vous trouverez dans cet ouvrage un cheminement logique, basé sur la découverte du système Ubuntu jusqu'à sa maîtrise plus avancée. Quelquefois, vous trouverez des exercices simples sous forme de questions dans un but d'apprentissage plus théorique.

Le premier chapitre **Ubuntu et Linux** traite de la place particulière qu'occupe la distribution Ubuntu au sein du monde Linux. Il répond entre autres aux questions : *Pourquoi l'utiliser ?* et *Quels en sont les avantages ?*

Les trois chapitres suivants **Préalable à l'installation, Processus d'installation, Installations particulières** concernent tout ce qui se rapporte aux installations des différentes - et nombreuses - déclinaisons de cette distribution si prolifique et actuellement en pointe dans le monde Linux.

Les chapitres cinq et six **Gestion des droits utilisateurs, Prise en main de la distribution** répondent à la nécessité de la maîtrise de base de la distribution et de la gestion des utilisateurs. Ce dernier domaine constituant à lui seul la démonstration parfaite de la transversalité Unix/Linux-Ubuntu.

Des chapitres sept et huit **Session de travail en mode console, Session de travail en mode graphique** découlent respectivement les deux modes de fonctionnement de la distribution : en mode console dans le cadre d'un serveur et en mode graphique dans le cadre d'un poste de travail.

Le chapitre neuf **Administration des ressources** parlera des ressources, internes ou externes au système, avec notamment ce qui a trait à la gestion des périphériques.

Les chapitres dix et onze **Maintenance de base du système, Maintenance avancée du système** abordent, concrètement et en deux paliers, la maintenance du système, base du travail courant de l'administrateur. Les utilisateurs ayant une tendance naturelle à effectuer des tâches donnant des sueurs froides à tout administrateur, il convient d'adopter un plan de travail le plus rigoureux et le plus complet possible.

Enfin, le dernier chapitre **Sécurisation du système** - très important - donnera les clefs d'une sécurité globale du système. Aucun système ne peut se targuer d'être LE système sans failles, mais la distribution Ubuntu (et dans son cadre général, le système Linux) comporte l'essentiel des contrôles permettant de dire qu'elle est parmi l'un des systèmes actuels les plus sûrs, aussi bien dans une activité professionnelle que dans une utilisation personnelle.

Affirmation du modèle OpenSource

La nature aime les contre-pouvoirs. Aussi la montée en puissance d'une éthique communautaire face au modèle commercial n'est pas aussi illogique que l'on pourrait le croire. Le modèle OpenSource dépasse moralement la notion de logiciel propriétaire en lui attribuant une dimension morale basée sur le partage.

1. Principe du modèle, son avenir

Le modèle OpenSource repose sur deux idées fortes : le travail en collaboration et l'implication des acteurs. En cela, Internet contribue beaucoup au développement du modèle en permettant à une communauté de partager et de développer ensemble des sources de logiciels librement distribuables. Économiquement, le modèle OpenSource dépasse aussi le modèle classique du logiciel propriétaire (+80 % de croissance en 2007) sur deux plans :

- Le développement de plus en plus complexe des logiciels nécessite une communauté apte à aider, améliorer, contribuer. Cela n'est plus à la portée d'une seule entreprise (même la plus forte...). On le voit clairement avec la généralisation de la distribution massive de versions bêta (pré-versions) comme par exemple Microsoft avec Vista et son logiciel phare Office12.
- La mondialisation des échanges implique une stratégie commerciale plus active avec beaucoup de relais d'opinions, de références. Le modèle OpenSource trouve naturellement sa place dans le nouveau média de distribution qu'est Internet. La généralisation de sites "miroirs" de sites officiels en est la preuve : en France, des sites comme drupalfr.org pour le CMS (*Content Management System* ou système de gestion de contenu) Drupal ou apachefrance.com pour le logiciel serveur WEB APACHE...

a. OpenSource et capitalisme financier

La rentabilité financière des "start-up" attire de plus en plus d'investisseurs comme l'a montré l'introduction en bourse de Google. Mais que peut-on dire du modèle OpenSource ? C'est d'ailleurs une question récurrente : *comment peut-on gagner de l'argent en distribuant librement ses sources ?*

La réponse se situe intrinsèquement par rapport au produit. Quand on achète un téléviseur, la part de responsabilité contractuelle de l'entreprise s'arrête naturellement lors du transfert de propriété. Bien sûr, suivant la technicité du produit (on ne compare pas une boîte de petits pois à un téléviseur), la mise en place d'un service après-vente pour d'éventuelles réparations s'impose, avec éventuellement l'introduction de sociétés tiers car l'entreprise peut déléguer cette activité et ne pas l'effectuer elle-même. On ne parle pas, là, de la responsabilité légale qui traite du respect de la nature et de la fonctionnalité de la chose vendue.

Dans le cas d'un logiciel informatique, l'accompagnement pour l'utilisateur est essentiel. Il faut une offre de support technique, des possibilités d'extensions, des certifications, de la formation... C'est là que se trouve la **rentabilité du modèle OpenSource**.

Toujours dans le cas d'un logiciel, la fourniture d'un produit exempt d'erreurs (*bugs* ou bogues en français) est impossible, vu la complexité d'un développement. La société commerciale se trouve confrontée à deux choix :

- soit elle privilégie la qualité du programme et allonge le temps de développement entraînant *ipso facto* une augmentation des coûts avec un possible problème financier vis-à-vis de la rentabilité.
- soit elle minimise le contrôle qualité au risque de livrer un produit imparfait capable de mécontenter les acheteurs et ainsi mettre à mal une image marketing à long terme.

Toute la difficulté réside par une direction d'entreprise à placer le curseur au bon endroit... Une communauté de développeurs répond de fait à ce problème par la mise en place d'échanges, de retours sur les versions bêta. C'est là que se trouve la **justification d'existence du modèle OpenSource**.

L'entreprise commerciale fait de même, mais la demande impérative de rentabilité liée au couple vente du produit et retour sur investissement rend plus accessoire voire annexe ce qui est fondamental pour le modèle OpenSource.

Exemples de réussite :

Automatic, n°2 des entreprises sur le marché de la publication de blogs avec Wordpress, a pu attirer 29,5 millions de dollars pour financer son développement. Dès l'origine, le code du logiciel Wordpress a été mis à la disposition de tous gratuitement.

Le SGBD (Système de Gestion de Bases de Données) MySQL a obtenu de la société Sun Microsystems un milliard de dollars pour son rachat sans abandonner ses idéaux dans le domaine de l'OpenSource.

L'entreprise Emertec, spécialiste des logiciels dits "embarqués" sous technologie JAVA et la téléphonie mobile, a pu lever une des plus importantes mises dans le secteur du capital-risque avec 23 millions d'euros.

b. OpenSource et logiciel libre

Il ne faut pas confondre logiciel OpenSource et logiciel libre. Les différences apparaissent minimes (surtout pour les néophytes) mais elles existent et sont essentiellement axées sur le contenu de la licence.

En réalité, il n'existe pas une licence OpenSource ou libre, mais plusieurs. Certains acteurs utilisent à tort ou à raison (le débat est loin d'être clos) une licence dérivée de la licence générale, la licence GPL (ou *General Public License*) :

- licence BSD (*Berkeley Software Distribution*)
- licence publique adaptative
- licence Mozilla Public (MPL)
- licence Apache Software
- licence de documentation libre (GFDL - *GNU Free Documentation License*)
- etc.

Vous trouverez une liste de ces licences sur le site : <http://www.opensource.org/licenses/alphabetical>

Concrètement, un logiciel libre signifie "... pour les utilisateurs d'exécuter, de copier, de distribuer, d'étudier, de modifier et d'améliorer le logiciel". Un des aspects essentiels concerne donc la liberté de redistribuer les sources : ce qui va à l'encontre fondamentalement du modèle commercial.

Un logiciel OpenSource permet quelques restrictions comme par exemple :

- l'interdiction de tirer profit d'une modifications des sources.
- la prise en compte de limitations liées à une partie du code tiré d'un logiciel d'une autre licence (cas des pilotes de périphériques propriétaires dans une distribution Linux ou de DRM (*Digital Rights Management*), signatures numériques).

Au final, la distinction peut être apportée par Richard Stallman le "gourou" du logiciel libre et de la licence GNU (*GNU's Not Unix*, jeu de mot récursif) : pour lui, "... l'OpenSource est une méthodologie de développement ..." alors que le "... logiciel libre est un mouvement social ...".

Voici l'adresse du site Internet pour le système GNU : <http://www.gnu.org>

2. Place de Linux dans le modèle

Les distributions à base de noyau Linux constituent le fer de lance du modèle OpenSource. À l'origine, le projet GNU désigne un système d'exploitation entièrement libre à base de noyau UNIX. Le concepteur du noyau Linux Linus Torvalds, aime à répéter d'ailleurs qu'il ne faut pas confondre **distribution Linux** et **noyau Linux**, *a fortiori* **système GNU** et **noyau Linux**.

Dans la pratique, les distributions Linux constituent une alternative mondiale dans le domaine du système d'exploitation face au géant Windows et le particulier Mac OS. Comme toujours dans le monde libre, la pluralité des offres abonde. Un site Internet essaye d'en recenser l'éventail : <http://distrowatch.com>

Un premier tri fait apparaître des distributions principales (ou majeures, moins d'une dizaine) et des distributions secondaires (ou mineures, plus de trois cents). Un second tri ne retient que les distributions :

- **Debian**, la distribution de référence .
- **Red Hat**, l'autre distribution de référence maintenant commerciale et pour les serveurs d'entreprise.
- **Gentoo**, la distribution à partir des sources.
- **Slackware**, la distribution la plus ancienne.

Il faut ajouter à cette liste pour diverses raisons :

- **Ubuntu**, la distribution la plus aboutie basée sur la distribution Debian.
- **Fedora**, la version communautaire et grand public de la distribution Red Hat.
- **Centos**, la version communautaire strictement équivalente à la version commerciale de la Red Hat Entreprise recompilée à partir des sources.
- **OpenSuse**, au préalable basée sur une distribution Slackware, maintenant autonome et passée sous contrôle de l'entreprise Novell.
- **Mandriva**, la distribution d'origine française basée sur une distribution Red Hat.

L'intérêt des autres distributions réside plus dans le phénomène de mode et, nettement plus important, la spécialisation du système. On trouve, par exemple, des distributions Linux orientées vers la sécurité, le domaine scientifique, l'éducation, etc.

Une distribution pratique par exemple pour la création d'un petit pare-feu (*firewall*) **IPCop Firewall**, avec pour site Internet : <http://www.ipcop.org/>

3. Principaux outils OpenSource

Beaucoup de logiciels OpenSource ne se contentent pas d'être des succès mais souvent disputent des parts de leadership ou représentent une véritable alternative. Un simple florilège de produits suffit pour le montrer :

Navigation WEB

Le logiciel **Firefox** approche les 18 % du marché contre certes 80 % à **Internet Explorer** mais ce dernier est installé par défaut sur les plates-formes Windows. La version 3 de Firefox a fait l'objet d'une inscription au livre Guinness des Records avec plus de huit millions de téléchargements dans les 24 heures qui ont suivi sa date de lancement.

Messagerie

Le logiciel **Thunderbird** de la même fondation que **Firefox** (Mozilla) est un client de messagerie sûr et fiable. Il est axé sur la sécurité avec par exemple une protection contre les attaques par hameçonnage ou courrier frauduleux (*phishing*). Il concurrence plus qu'avantageusement le logiciel **Outlook Express**.

Serveur WEB

Le serveur **APACHE** de fondation Apache Software est leader dans son domaine avec environ 68 % de part de marché.

Bureautique

La suite **OpenOffice**, véritable concurrent de **Microsoft Office**, réussit une percée importante dans les administrations et collectivités désireuses d'éviter une hémorragie de fonds face à de plus en plus de versions sans réelle avancée technologique.

Graphisme

Maintenant porté sur Windows, le logiciel **GIMP** (*The GNU Image Manipulation Program*) est comme son nom l'indique LE logiciel de manipulation d'image par nature sous système Linux/Unix.

Utilitaire

7-Zip, réservé à la plate-forme Windows, supporte quasiment tous les formats de compression de données et s'intègre de façon simple au bureau. Pour Linux, les outils de (dé)compression sont intégrés de façon native avec le système.

Langage

Le langage incontournable actuellement pour le développement WEB est le **PHP** mais on peut citer aussi **PERL**, **Python**, **Ruby**, etc. On ne peut concevoir l'apparition et l'utilisation d'un langage par la communauté des développeurs autrement que par l'OpenSource.

CMS, système de gestion de contenu pour Internet

S'il ne faut en citer qu'un (car ils sont très nombreux) : **Drupal**. Il est employé pour la réalisation de nombreux sites Internet comme Rue89, Mediapart (information numérique), FnacLive (musique en ligne), etc. **Egroupware** dans le domaine plus spécialisé du serveur collaboratif apporte les services de calendrier, bloc-notes, gestion de projets, relation clients, etc. **GPLI**, dans le domaine de l'inventaire, du support technique aux utilisateurs...

Progiciel de gestion/ERP (Entreprise Resource Planning)

Face au poids lourds comme **SAP**, des solutions OpenSource commencent à voir le jour. Citons **Compiere** de plus en plus implanté dans les PMI/PME avec ses modules de gestion financière, de stocks, d'achats et ventes, d'e-commerce, TinyErp...

Vous en saurez plus sur le libre et ses déclinaisons logicielles en allant sur :

<http://www.framasoft.net/>

<http://www.logiciellibre.net/>

Ubuntu : les raisons d'un succès

1. Point de départ

a. Les origines

Historiquement, Ubuntu est née de ce qui aurait pu être une ambiguïté : le multimillionnaire **Mark Shuttleworth** fonde en 2005 la **Ubuntu Foundation** dont le but avéré est de contribuer à la popularisation du système d'exploitation Linux. Voir une seule personne porter financièrement à ce point (10 millions de dollars par an) un projet OpenSource avait de quoi laisser sceptique sur les motivations réelles en regard d'un modèle comme le système Windows et de son charismatique leader Bill Gates.

Considérez en plus l'adresse du site de la distribution : <http://www.ubuntu.com>

Cette adresse possède comme nom de domaine Internet l'extension **.com** (liée aux sociétés commerciales) et non en **.org** (pour les organisations). Force est de constater maintenant que la distribution Ubuntu est maintenant un succès, non seulement au sens du système d'exploitation Linux mais aussi à celui du modèle OpenSource.

Les (mauvaises ?) arrière-pensées restent toujours : sur la toile, certains pensent toujours que la société **Canonical**, entreprise commerciale de Mark Shuttleworth qui sponsorise la fondation Ubuntu, cache des buts financiers certes avoués mais qui se traduiront à terme sur des verrouillages de licence contraire à la licence du monde libre. La récente apparition de la distribution **Gobuntu**, système d'exploitation 100 % libre, peut paradoxalement faire craindre aux puristes de la Free Software Fondation une accélération de la dépendance de la distribution Ubuntu vis-à-vis du monde propriétaire. Selon des déclarations récentes de Mark Shuttleworth, la préférence irait vers une cohabitation pacifique entre Windows et Ubuntu à l'image du navigateur Web Firefox, présent avec succès sur les deux plates-formes.

Toute la discussion est là : bien sûr, Canonical, par le biais de partenariat avec d'autres entreprises commerciales, fait des bénéfices. Bien sûr, l'émergence d'un leader a de quoi alimenter les peurs de la montée en puissance d'un Windows bis. Mais pour l'instant, toutes les preuves du contraire sont là : **liberté d'utilisation, liberté des choix logiciels** même non libres, promotion et affirmation du postulat **logiciels libres convergent vers un meilleur schéma de développement d'applications**.

En France par exemple, Ubuntu a adhéré à l'APRIL (association pour "la promotion et la défense du libre").

b. Plus de renseignements sur le fondateur...

Mark Shuttleworth, d'origine sud-africaine, a fait fortune dans la finance, la gestion et la sécurité des Systèmes d'Information. Impliqué dans le monde libre, il collabore au développement de la distribution **Debian** dans les années 1990 et supporte activement par l'intermédiaire de sa fondation, la **Shuttleworth Foundation**, des projets éducatifs. Il fait partie des "patrons" de l'environnement graphique KDE (*K Desktop Environment*) ce qui représente le plus haut niveau de parrainage.

Son site personnel, sous la forme d'un blog, se situe à l'adresse suivante : <http://www.markshuttleworth.com/>

Au registre de l'anecdote, il fait partie du cercle très fermé des touristes de l'espace en participant à la mission russe Soyouz TM-34 de 2002 au prix d'un versement d'environ 20 millions de dollars. On peut aussi parler de pied de nez linguistique : *shuttle* (première partie de son nom) signifiant en français navette spatiale !

2. Qualités de la distribution

D'emblée, Ubuntu est sympathique avec son logo représentant schématiquement trois personnes se tenant la main :



Le mot Ubuntu, d'origine africaine, a pour signification "*humanité aux autres*" : ce qui place d'emblée cette distribution dans une optique communautaire proche de la demande de Richard Stallman avec son mouvement social.

Au niveau technique, Ubuntu se base sur la distribution majeure **Debian** dont la popularité et la robustesse ne sont plus à démontrer. Pour comprendre la relation entre Ubuntu et Debian, il faut indiquer le schéma de développement de cette dernière. On a pour Debian :

- la branche **stable**, actuellement représentée par la distribution **Etch**.

- la branche **testing**, actuellement représentée par la distribution **Lenny**.
- la branche **unstable**, ayant toujours pour nom **Sid**.

Les noms des versions de distribution sont basés sur les personnages du film d'animation *Toy Story* sorti en 1996. Sid est le garçon dont le passe-temps favori est de casser ses jouets... Comme Ubuntu se base sur cette dernière, doit-on conclure qu'Ubuntu ne serait pas stable ? Évidemment non, ce serait méconnaître l'excellent travail des développeurs Ubuntu. Un compromis serait de dire qu'Ubuntu se base sur une version stable de la branche instable de la Debian...

Chez Ubuntu, l'accent est mis - et c'est ce qui fait en partie son succès - sur les fonctionnalités alors que chez Debian, on recherche à tout prix la fiabilité et ce, sur toutes les plates-formes. Ceci explique pour Debian, le rythme de sortie assez long entre deux versions (environ trois ans...).

a. Points forts de la distribution

Pourquoi Ubuntu et non une autre ? Parce qu'Ubuntu a su, à l'inverse de ses concurrents (que sont Fedora, Mandriva, OpenSUSE, PCLinuxOS ou MEPIS Linux), apporter :

- une **procédure d'installation** facile et impressionnante par sa qualité, les matériels sont bien reconnus comme par exemple sur les ordinateurs portables,
- un **bureau classique** mais ergonomique, apportant un ensemble de bases cohérent et immédiatement fonctionnel (exemple : la suite bureautique),
- une **mise à jour simple** et accessible, même pour le non-initié,
- un **système rapide et sécurisé**,
- une **documentation agréable et complète**,
- une **communauté active** et parfaitement dans l'esprit du monde libre.

Dans de nombreux blogs professionnels (blogs.zdnet.com par exemple), de plus en plus d'articles posent la question : Ubuntu devient-elle la distribution de référence dans le monde Linux ?

b. Un mot sur la distribution pour les serveurs

À la lecture des précédentes lignes, on pourrait croire que la distribution Ubuntu se réserve aux postes de travail et non aux serveurs. Ce serait une erreur car pour l'avoir pratiqué sur un **PowerEdge 2900 64 bits de Dell** (processeur Xeon, disques durs SAS), ce système d'exploitation a toute sa place dans le cercle très fermé des distributions serveurs OpenSource (xBSD, Centos, Debian, Solaris...).

Sur ce matériel, la distribution **Debian Etch** a par exemple posé problème avec le contrôleur **PERC 5/i** (contrôleur matériel RAID 5).

Dans le cadre d'une utilisation sur des serveurs en milieu professionnel, la demande de support à long terme (LTS) est quasi-existentielle... Il faut donc utiliser une distribution Ubuntu avec le support LTS soit une distribution disposant d'un support à long terme sur cinq ans pour les serveurs.

C'est le cas pour la distribution Ubuntu utilisée dans cet ouvrage.

c. Pourquoi l'adopter ?

Pour l'informatique en entreprise, seul compte le TCO ou **coût total de possession** (*Total Cost of Ownership*) : c'est dire l'intégration de l'ensemble des coûts du produit. Dans ce domaine, les courbes d'un système basé sur Linux et Windows se croisent : Linux est moins cher à l'achat (principal avantage concurrentiel du logiciel libre) mais un peu plus onéreux en termes de support et d'utilisation. Pour Windows, c'est l'inverse : plus cher à l'achat mais moins dans sa pratique. Cette tendance s'explique pour Linux par le niveau de qualification globalement plus élevée des professionnels et par une mise en place de solutions plus robustes mais plus "pointues", donc prenant davantage de temps. Les logiciels Windows, plus orientés "clefs en mains", nécessitent moins de compréhension et de manipulations...

À chacun de faire en fonction de ses besoins sans porter de jugement, ni d'anathème. Il est certain qu'une entreprise de type PME/PMI a tout intérêt à utiliser des logiciels qui ne nécessitent pas de maintenance sérieuse, à

la différence d'une grande entreprise disposant pour cela d'un personnel qualifié.

Ce qui fait maintenant changer la balance en faveur de Linux, c'est la demande de plus en plus importante concernant un standard ouvert et où les investissements ne sont plus liés à la sortie inhérente de nouvelles versions de systèmes liées ipso facto à de nouveaux matériels.

Exemples d'implantation :

L'assemblée Nationale a choisi Ubuntu pour les postes de travail mis à la disposition des députés. Cela a malheureusement entraîné une réaction du patron de Mandriva qui aurait préféré la sienne, plus française... Après un an d'utilisation et après d'inévitables ajustement (sur les synchronisations avec les agendas des députés), le retour d'expérience semble positif.

La Gendarmerie Nationale va migrer ses 70.000 postes de travail sur Ubuntu, ce qui constitue une pénétration sans précédent dans l'administration française. À terme, c'est-à-dire à l'horizon 2013, la quasi-totalité du parc se situera sous Linux. L'importance est de montrer, outre l'aspect factuel des économies, que la Gendarmerie Nationale fait confiance à la technologie et au niveau de sécurité utilisé par le système Linux.

Certains constructeurs comme Dell proposent maintenant à la vente des machines, portables ou ordinateurs de bureau, avec Ubuntu pré-installée. Soyons réalistes : l'offre est pour l'instant réduite à deux ordinateurs de bureau et un portable...

Déclinaisons Ubuntu

Le rythme de sortie des distributions choisi par Canonical peut paraître élevé avec deux versions stables tous les six mois. En fait, rappelez-vous que Ubuntu se base sur une version instable de la Debian, ce qui semble donc en définitive normal. L'évolution des matériels est telle que ce rythme convient afin de "coller" au plus près à la réalité. Tous les systèmes d'exploitation sont à la même enseigne : définir un rythme de sortie d'une version majeure tous les trois ans environ. Le tout est de choisir entre les deux sorties, soit la publication de versions intermédiaires, soit la mise à la disposition de "service pack" : ce qui revient, en définitive, au même...

Avec Ubuntu, on distingue les distributions majeures (tous les deux ans) des distributions mineures. Seule une distribution majeure se voit qualifiée LTS c'est-à-dire avec un support plus long qui se partage en :

- trois ans pour la version poste de travail (*desktop*).
- cinq ans pour la version serveur (*server*).

Ce support concerne les mises à jour normales et de sécurité. Une version mineure aura, quant à elle, un support de 18 mois. Le numéro de sortie correspond à une numérotation de la forme Y.MM (année/mois) et les noms sont choisis dans un bréviaire animalier délicieusement rétrograde (voulu par Mark Suttleworth) affublés d'un adjectif haut en couleur : **Feisty Fawn** (faon téméraire), **Gutsy Gibbon** (gibbon courageux), **Hardy Heron** (héron robuste)...

1. Historique des versions

Nom	Version	Support	Date de Sortie	Arrêt du support
Warthy Warthog	4.10		20/10/2004	30/04/2006
Hoary Hedgehog	5.04		08/04/2005	31/10/2006
Breezy Badger	5.10		13/10/2005	13/04/2007
Dapper Drake	6.06	LTS	01/06/2006	06/2009 (desktop) 06/2011 (server)
Edgy Eft	6.10		26/10/2006	25/04/2008
Feisty Fawn	7.04		19/04/2007	10/2008
Gutsy Gibbon	7.10		18/10/2007	04/2009
Hardy Heron	8.04	LTS	24/04/2008	04/2011 (desktop) 04/2013 (server)
Intrepid Ibex	8.10		30/10/2008	04/2010

La distribution qui constitue la base de cet ouvrage se base sur la **Hardy Heron** qui dispose donc du support à long terme et qualifiée de distribution majeure. Cette distribution est seulement la deuxième dans ce support et devrait donc perdurer. Elle convient donc parfaitement à une utilisation en tant que serveur.

2. Déclinaisons d'une même version

Le projet Ubuntu, très actif, comporte beaucoup de branches et de distributions dérivées. Le classement fait par Canonical porte sur la notion de dérivée (indépendamment des architectures supportées Intel x86 et AMD64). On aura :

- la version normale, de base pour les postes de travail,

- les versions totalement supportées par Canonical, les versions serveurs, celle avec l'environnement KDE et celle orientée éducation,
- les versions reconnues et faisant l'objet de contributions de la part de Canonical avec l'environnement XFCE , la version 100 % libre, la version orientée production multimédia et celle pour les terminaux mobiles.

On peut facilement s'y perdre aussi je propose, à la place, un classement par trois critères :

- le critère de la **destination**, suivant ce que l'on veut faire avec la distribution,
- le critère de l'**environnement** graphique, suivant le cadre de travail voulu pour la distribution,
- le critère des **fonctionnalités**, suivant la spécialisation de la distribution.

a. Suivant la destination

Server Edition

Distribution robuste d'un déploiement facile, sans environnement graphique et disposant des logiciels permettant, d'une part, la construction d'un serveur sécurisé et, d'autre part, le choix de composants à l'installation comme la plate-forme LAMP (*Linux/Apache/MySQL/PHP*), DNS, MAIL, etc.

Le menu d'installation propose plusieurs choix et un seul mode (normal par la touche [F4]) d'installation :

- **Installer Ubuntu Server**
- **Vérifier le CD**
- **Réparer un système endommagé**
- **Tester la mémoire**
- **Démarrer à partir du premier disque dur**

L'installation se déroule en **mode graphique** (par défaut) ou en **mode texte** en appuyant au préalable sur la touche [Echap].

Alternate Edition

Cette distribution spéciale, dérivée de la précédente, s'emploie dans des situations particulières : en cas de manque de mémoire par exemple ou de mauvaise reconnaissance des résolutions de l'écran. Au premier écran, vous disposez des mêmes choix que la distribution serveur, mais l'appui de la touche [F4] provoque l'affichage d'un sous-menu offrant quatre modes supplémentaires :

- l'installation normale
- l'installation de type OEM (pour les intégrateurs ou *Original Equipment Manufacturer*)
- l'installation en ligne de commande (installation minimaliste)
- l'installation en serveur LTSP (*Linux Terminal Server Project*)

Ce dernier mode fournit une architecture client/serveur permettant l'utilisation de terminaux baptisés "clients légers" (éventuellement sans disque dur ou *diskless*).



L'installation OEM construit un système avec un minimum de demandes d'informations. L'utilisateur n'a plus ensuite qu'à personnaliser sa distribution (les sources sur une partition à part). Elle est destinée aux intégrateurs (ou aux constructeurs) comme le montre l'écran ci-dessous après installation et avant le premier démarrage :

[!] Configuration de oem-config

Quand vous démarrerez le nouveau système, vous serez capable de vous connecter en tant qu'utilisateur 'oem' avec le mot de passe que vous avez choisi auparavant; cet utilisateur possède également les privilèges d'administrateur en utilisant 'sudo'. Vous serez alors capable de faire toutes les modifications supplémentaires dont vous avez besoin pour votre système.

Une fois que le système est configuré à votre convenance, lancez 'oem-config-prepare'. Cela va amener le système à effacer l'utilisateur temporaire 'oem' et poser les diverses questions de configuration pour l'utilisateur final au prochain démarrage.

Prêt à configurer pour l'utilisateur final

<Continuer>

Desktop Edition

Cette fois-ci, la forme classique de la distribution Ubuntu. Avec l'environnement graphique par défaut GNOME et un ensemble de logiciels permettant la configuration d'un poste de travail immédiatement opérationnel : traitement de textes, édition graphique et multimédia, navigation Internet, réception de messages, etc.

Le menu d'installation propose, là encore, plusieurs choix et un quatre modes :

- **Essayer Ubuntu sans rien changer sur votre ordinateur**
- **Installer Ubuntu**
- **Vérifier le CD**
- **Tester la mémoire**
- **Démarrer à partir du premier disque dur**

Là aussi, l'installation se déroule soit en **mode graphique** (par défaut et recommandé) ou en **mode texte** en appuyant au préalable sur la touche [Echap].

La première ligne du menu montre la possibilité d'essayer Ubuntu sans l'installer sous la forme d'une **distribution live**. Les quatre choix d'installation portent sur :

- l'installation normale,
- l'installation en mode graphique sans échec lorsque la détection de la carte graphique et/ou l'écran se passe mal,
- l'utilisation d'un CD-Rom supplémentaire contenant des mises à jour de pilotes de périphériques,
- l'installation de type OEM (pour les intégrateurs).



Une distribution LIVE s'exécute sur un support amovible comme un CD-Rom ou une clé USB. Le système de fichiers (unionFS et maintenant auFS) est pour partie sur le support, et pour partie en mémoire. Destinée essentiellement à faire découvrir une distribution car elle ne touche pas au système d'exploitation installé sur le disque dur (elle n'installe rien) ; on peut l'utiliser à des fins didactiques ou pour une population d'utilisateurs nomades.

JeOS Server Edition

Pour les francophones, **Jeos** se prononce "Juice". Cette version spéciale et très récente (car seulement disponible à

partir de la version 7.10 Gutsy) est dérivée de la version serveur et a pour univers la **virtualisation**. À partir de la version 8.10 Intrepid Ibex, cette déclinaison est incluse dans la version serveur.

L'idée originale s'appuie sur les produits de la société **VMware**, leader en ce domaine avec leur produit phare VMware ESX Server. L'optimisation de la distribution est poussée à l'extrême pour les machines virtuelles (applications logicielles non liées à un fournisseur ou *virtual appliances*). La suppression de drivers inutiles allège l'ensemble et fournit un noyau (*kernel*) ajusté pour un environnement virtuel.

Pour information, le site de la société VMware se trouve à l'adresse : <http://www.vmware.com>

Spécifications techniques

- image ISO d'environ 100 Mo
- contenu installé d'environ 300 Mo
- optimisé pour VMware ESX, Server et KVM
- mémoire de fonctionnement nécessaire 128 Mo
- pas d'environnement graphique.

C'est une véritable et bonne initiative. Nul doute que d'autres distributions suivront cet exemple. Vous trouverez plus de détails sur le site Ubuntu : <http://www.ubuntu.com/products/whatisubuntu/serveredition/jeos>

Gobuntu Alternate Edition

Cette variante de la distribution de base, avec une installation uniquement en mode texte, répond aux critiques envers Ubuntu par rapport à son manque de conformité aux standards de la Free Software Foundation. Utiliser **Gobuntu**, c'est être sûr d'utiliser une distribution Linux 100 % OpenSource avec uniquement des logiciels libres. La contrepartie de cela fait que cette distribution ne s'installera pas correctement ou impartialement sur des matériels aux pilotes propriétaires.

Un conseil : si vous n'êtes pas un "linuxien" convaincu ou n'œuvrant pas dans un cadre juridique contraignant, évitez cette variante. Concrètement, une version Gobuntu **ne doit jamais** être installée sur un portable par exemple.

Gobuntu dispose de son propre logo :



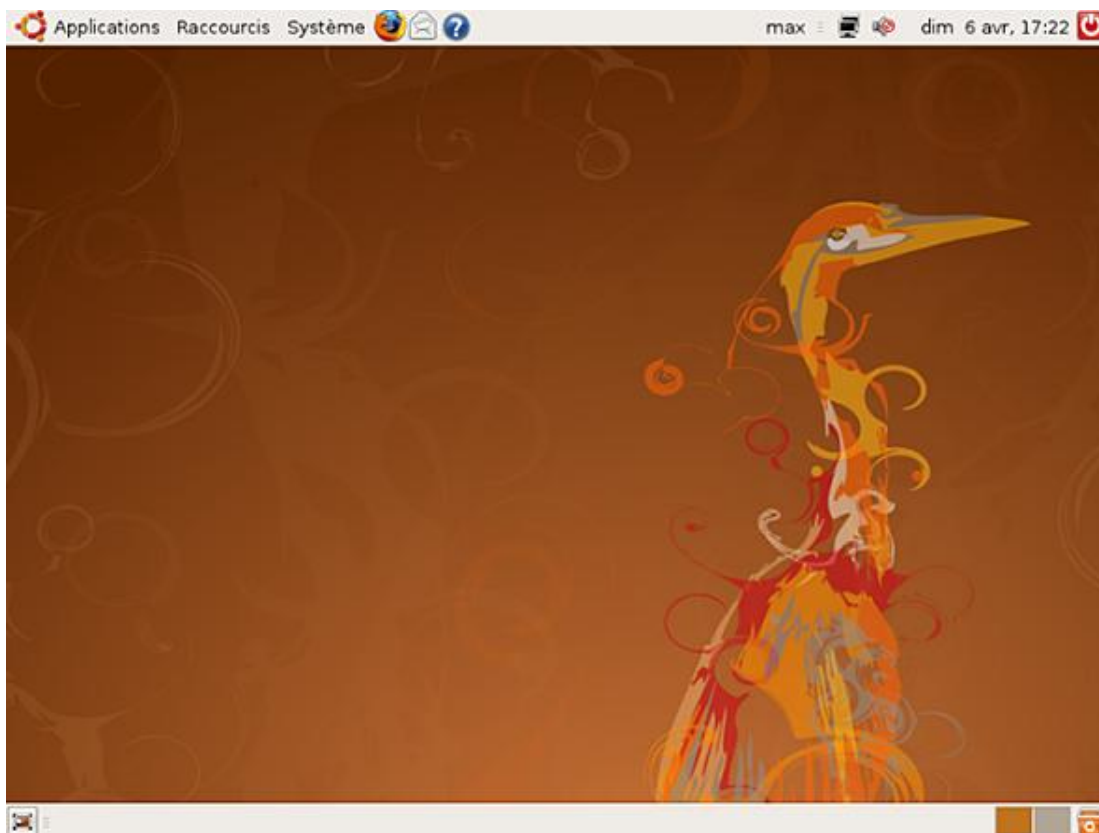
Le lien pour le téléchargement de cette version reste au moment de la rédaction de ces lignes, bloqué sur la version 7.10 Gutsy. Le véritable lien pour la version 8.04 Hardy se trouve à l'adresse suivante : <http://cdimage.ubuntu.com/gobuntu/releases/8.04.1/release/>

b. Suivant l'environnement graphique

Ubuntu Desktop Edition

La distribution générique désigne la version en poste de travail (déjà vue dans le point précédent). Elle supporte les architectures x86 (Pentium, Celeron, Athlon, Sempron), 64 bits ADM ou Intel (AMD64 et EM64T soit processeurs Athlon64, Opteron, Xeon et Core 2) et UltraSPARC T1.

L'environnement graphique par défaut GNOME s'adapte aussi bien sur un ordinateur de bureau que sur un portable :



Elle dispose des outils logiciels comme la suite bureautique **OpenOffice**, **Xsane** (acquisition d'images), des outils Web avec **Firefox** (navigateur Internet), **Evolution** et **Pidgin** (courrier et messagerie) ; des outils multimédia avec **Brasero** (gravure de disque), **F-Spot** (gestionnaire de photos), **GIMP** (éditeur d'images), **Rhythmbox** (lecteur de musique) et **Totem** (lecteur vidéo), etc.

Kubuntu

Les utilisateurs Linux se divisent *grosso modo* en deux camps : les adeptes de l'environnement graphique GNOME et ceux qui ne jurent que pas l'environnement KDE (*K Desktop Environment*). **Kubuntu** répond aux désirs de ces derniers.



Le site Internet de cette distribution : <http://www.kubuntu.org/>

Réputé pour être très complet, ses détracteurs le trouvent gourmand en ressources. Il demande un minimum de 256 Mo de mémoire vive (RAM) et un espace disque de 3 Go. Il installe plus d'applications que GNOME, dont les noms ont pour principale caractéristique de commencer par la lettre k : **kate**, **kmail**, **Kaffeine**, etc.

La nouvelle version KDE 4 remédiera en partie (semble-t-il), à ce problème. Notez que la distribution KUbuntu Hardy Heron possède deux déclinaisons :

- Celle avec la **version 3.5** (3.5.9 en septembre 2008) supportée par Canonical.
- Celle avec la **version 4** (4.1 en septembre 2008) nommée **Kubuntu Remix** et supportée uniquement par la communauté.

L'implication de cette déclinaison fait que dans la version Remix ne dispose pas du support LTS.

Xubuntu Desktop Edition

À l'écart des deux "grands" que sont GNOME et KDE, d'autres environnements graphiques existent. **Xubuntu** a pour environnement graphique **XFCE** dont la volonté affichée est d'être le plus "léger" possible. En voici le sigle :



Le site Internet de cette distribution : <http://www.xubuntu.org/>

XFCE utilise les mêmes librairies GTK que GNOME et de l'avis de son concepteur - un français - Olivier Fourdan, est "... conçu pour la productivité" en équilibrant idéalement l'exécution des applications et la consommation des ressources systèmes.

Sur un serveur devant disposer absolument d'une interface graphique, Xubuntu reste un bon compromis, car il n'obère pas ou peu les ressources de l'ordinateur.

Voici son bureau somme toute plus classique et épuré par rapport à GNOME :



c. Suivant les fonctionnalités

Edubuntu

La société Canonical dans la droite ligne de son slogan *l'humanité envers les autres*, soutient des projets de formation et d'éducation comme, par exemple, le projet **Computer for Every Child** en République de Macédoine. Une des manifestations de ce soutien aboutit à une distribution sous bureau GNOME, spécialement adaptée au milieu éducatif et intitulée **Edubuntu** :



Voici l'adresse de son site Internet : <http://www.edubuntu.org/>

L'éventail des applications pédagogiques va au niveau scolaire de l'école maternelle au secondaire. De plus, Edubuntu adopte l'architecture LTSP (*Linux Terminal Server Project*) car le monde scolaire (il faut se placer ici dans une optique mondialiste) ne dispose pas beaucoup de moyens...

Jusqu'à la version 7.10 Gutsy, Edubuntu provenait d'une version complète mais dérivée de la distribution de base. À partir de la version 8.04 Hardy, la part consacrée à Edubuntu passe par un CD-Rom supplémentaire (*add-on*) qui s'installe au-dessus d'une version existante. Si vous désirez l'architecture LTSP, il faudra installer Edubuntu au-dessus d'une version Alternate.

Ubuntu-Studio

Cette distribution, basée sur une version **alternate**, a pour objectifs la création numérique et l'édition multimédia.

Son logo personnalisé :



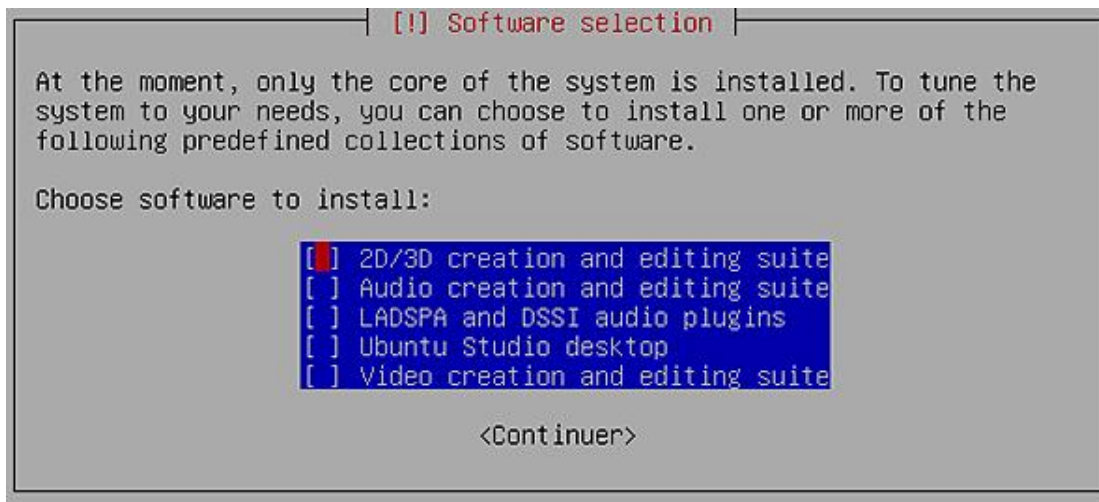
Le site Internet de cette déclinaison de Ubuntu présente, en accord avec son contenu, un design plus recherché : <http://ubuntustudio.org/>



Les particularités méritent d'être détaillées :

- Emploi de logiciels spécifiques pour l'audio, la vidéo et le graphisme.
- Utilisation d'un noyau dit "*lowlatency*" (meilleur temps de réponse).
- Support de distribution par DVD-Rom car la taille dépasse un gigaoctet.
- Installation en mode texte et non en mode graphique.

Dans un but de facilité, l'installation (en mode texte) vous propose un choix parmi une collection de logiciels regroupant des fonctionnalités par thème :



Pour information, la totalité des choix apporte les logiciels :

- **Blender** (création d'objets 3D)
- Éditeur d'images : **GIMP, Inkscape** (images vectorielles)
- Gestionnaire de photos : **F-Spot**
- Créateur de panorama : **Hugin**
- Mise en page graphique et publication : **Scribus**
- Création d'animations : **Stopmotion**
- Composition et animations 2D : **Synfig Studio**
- Et une multitude d'outils de production : audio, synthétiseur, mixeur, etc. (près de 40) et vidéo : éditeur, lecteur, montage.

Mythbuntu

Axée aussi sur le multimédia mais basée toujours sur une version **Alternate** et avec l'environnement graphique XFCE, cette déclinaison se rapporte à la lecture de flux fournis par une carte tuner TV :



Une des phases principales de l'installation consiste à choisir dans la liste le matériel de capture TV utilisé (comme par exemple les clés **Pinacle**) pour le paramétrage du paquetage **LIRC** (encodage/décodage des signaux infrarouges de la télécommande) :

If you choose a remote, but already have a configuration file in /etc/lirc/lircd.conf, the existing file will be renamed to /etc/lirc/lircd.conf.dpkg-old and the community configurations loaded into /etc/lirc/lircd.conf. This process will only happen once, and subsequent instantiations of this configuration will not overwrite your /etc/lirc/lircd.conf file again.

Choose a remote if you would like to preload a configuration:

Packard Bell receiver
PCMAK serial receiver
PCMAK USB receiver
Phoebe Tv Master + FM (card 22)
Pinnacle Systems PCTV (pro) receiver
Pinnacle Systems PCTV Sat receiver
Pinnacle Systems PCTV Sat receiver
Pixelview PlayTV MPEG2
PixelView PlayTV PAK (card 50)
Pixelview PlayTV pro (card 37)
PixelView RemoteMaster RC2000/RC3000
Prolink Pixelview PV-BT878P+ (Rev.4C8E card 70)



Administrateur système Ubuntu

Les responsabilités d'administrateur Ubuntu s'apparentent à celles d'un administrateur système sur Linux, d'autant plus que la distribution suit la certification LSB (version 3.2 du 28 janvier 2008).

 Le sigle LSB désigne un ensemble de spécifications destiné à unifier les différentes distributions Linux (www.linux-foundation.org). Parallèlement, existe le projet Freedesktop.org (www.freedesktop.org) qui travaille sur la compatibilité des programmes au sein d'environnements de bureau comme GNOME ou KDE.

Les différences portent sur l'utilisation d'outils spécifiques à la distribution Debian dont est issue Ubuntu :

- L'emploi du gestionnaire de mise à jour Aptitude et des paquets logiciels au format .deb.
- La configuration réseau située dans un emplacement et une forme différente.
- La gestion du noyau avec une méthode de compilation basée sur la création d'un paquet.

1. Rôle de base

Qu'il soit en entreprise ou en situation d'utilisation personnelle, l'administrateur système effectue des tâches communes :

- Installer, configurer et faire évoluer le matériel : une nouvelle carte réseau, un nouveau disque, etc.
- Installer le système et les applications : installation de la distribution sur un ou plusieurs postes en même temps (par exemple avec CloneZilla).
- Gérer les utilisateurs : ce qui comprend l'ajout, la suppression d'un profil, la mise en place de quotas, la gestion des droits spécifiques ou par groupe...

La distribution Ubuntu, résolument moderne, apporte de nouveaux outils pour effectuer ces tâches : **Upstart** (gestion des scripts de niveau), **Udev** (découverte des périphériques), **Apparmor** (gestion de profils utilisateurs), etc. Un des apports de cet ouvrage consistera à vous faire découvrir ces nouveaux outils.

2. Missions étendues

Ensuite, en fonction des responsabilités et de la situation, d'autres tâches s'ajoutent :

- Optimiser et réparer le système : suivant les demandes des utilisateurs, les ressources matérielles, les mauvaises manipulations et/ou les pannes.
- Sécuriser le système : par les mises à jours liées à la distribution ainsi que celles liées aux applications, par la mise en place d'une protection des informations (cryptage par exemple), par les sauvegardes régulières des données...
- Faciliter le travail des utilisateurs par le biais d'une documentation.

 Ubuntu "désactive" le compte `root` ou compte de l'administrateur système et promeut au rang d'administrateur un "super" utilisateur. Les tâches administratives sont alors effectuées par la commande `sudo`. Ce point sera développé en détail dans le chapitre sur la gestion des utilisateurs.

Conventions typographiques

L'écriture d'un ouvrage informatique comprend nombre de symboles, vocables, acronymes, définitions, etc. qui le distinguent d'un roman. Prenez le temps de découvrir, ici, la présentation des éléments distinctifs de l'ouvrage en dehors de la police normale utilisée pour le texte.

1. Terminologie anglaise

L'utilisation de mots en langue anglaise a été limitée au maximum mais beaucoup de termes perdent leur signification une fois traduits. Une traduction ou explication accompagne chaque terme anglais en police italique :

L'administrateur système Linux s'appelle le *root*.



Cette remarque se remarque...

2. Exemples

Les exemples illustrant le texte sont rédigés avec la même police que le texte mais en italique.

Voici un exemple de ligne exemple.

3. Commandes et code

a. Présentation

Les commandes ou le code sont présentés avec la police Courier, en italique pour les éléments facultatifs.

commande *[options]* arguments

Tout ce qui est optionnel se trouve entre crochets.

Les extraits de fichier texte (exemple : fichier de configuration) ont la même facture que le code mais avec un encadré :

```
# Fichier de configuration
element = valeur
```

b. Exécution

Sur une distribution Linux, se pose la question de l'identité de l'utilisateur, c'est-à-dire ici, celui qui exécute la commande. Comme beaucoup de commandes se font en mode console (mode texte), se pose la question du prompt ou invite de commandes. Diverses représentations sont possibles :

- *[root]#*
- *[util]\$*
- *root:~#*
- *util:~\$*

Les deux premières lignes se réfèrent implicitement à respectivement une connexion en *root* (l'administrateur) et dans son répertoire personnel, et une connexion par un utilisateur nommé *util*, toujours dans son répertoire personnel. Les deux dernières lignes introduisent le symbole *~* (tilde) qui, dans la règle technique de Linux, exprime par convention le répertoire personnel de l'utilisateur.

Quid d'un changement de répertoire ? Est-ce utile de garder cette invite à partir du moment où l'utilisateur ne change pas ? Ensuite sous Ubuntu, vous verrez qu'effectuer une commande d'administration nécessite des droits supplémentaires avec une autre commande (sudo)...

La solution adoptée dans cet ouvrage vise **au plus simple** et ne montre que la commande (suivie du symbole `sudo`). Le texte, au préalable, sera suffisamment explicite et lèvera toute ambiguïté sur l'identité de l'utilisateur et le lieu de l'exécution de la commande.

Avant l'installation

L'utilisation normale d'un système Linux passe par son installation sur un ordinateur. Cette évidence un peu simpliste, cache en fait pour Ubuntu une diversité de situations. Avec en premier rang, la coexistence pacifique (ainsi l'a voulu Mark Shuttleworth) avec d'autres systèmes d'exploitation (Windows, par exemple)...

1. Implantations de la distribution

a. Type d'implantations

La forme d'implantation d'une distribution Linux Ubuntu se résume au choix entre :

- L'installation en **poste de travail**, liée intimement à un environnement graphique (Ubuntu Gnome, Kubuntu KDE, Xubuntu XFCE...).
- L'installation en tant que **serveur** (sans environnement graphique) avec une gestion des commandes en mode console texte.

À partir de ces deux types d'implantations, des variations sont possibles. Elles sont décrites dans le tableau ci-dessous.



Je ne tiens pas compte des versions dérivées comme Gubuntu, Ubuntu-Studio, Edubuntu, etc. Seules sont prises en compte la version poste de travail de base (desktop avec GNOME) et la version serveur.

Type d'implantation	Forme d'installation
Serveur	<i>Normale</i>
	Avec la technologie RAID , technique de sauvegarde des données utilisée avec plusieurs disques physiques.
	Sur un système de partitions LVM (<i>Logical Volume Manager</i>). Le partitionnement des disques s'effectue de façon logique dans le but d'apporter plus de souplesse dans la gestion des partitions (variation de taille, suppression, etc.).
Poste de travail	<i>Normale</i>
	Avec un double démarrage (<i>dual boot</i>) . Ubuntu cohabite parfaitement avec un autre système d'exploitation sur la même machine ; le chargeur de démarrage de Linux (GRUB ou LILO) se chargeant de proposer le choix à l'allumage de la machine.
	En cohabitation avec Windows . L'installation d'Ubuntu s'effectue dans un gros fichier (la partition est dans ce cas virtuelle) et se gère comme une application ; le chargeur de démarrage utilisé est cette fois-ci celui de Windows.

Vous verrez dans le chapitre Processus d'installation, les deux premiers niveaux d'installation (dite "*normale*") du plus simple au plus compliqué : en poste de travail avec un déroulement de base et en serveur en situation d'expert. Les autres implantations seront détaillées dans le quatrième chapitre Installations particulières.

b. Spécifications

Chaque système d'exploitation requiert un niveau de ressources pour fonctionner. Ce niveau se décompose en trois parties : le **minimum de base** sans lequel le système ne peut fonctionner, le **niveau recommandé** pour un

fonctionnement sans limitation ni ralentissement et les **exigences particulières** dues aux effets visuels du bureau.

Les types d'ordinateur vont du PC classique à base d'x86 et de la famille Pentium, Athlon, Sempron ; à base d'AMD 64bit, Intel64 Xeon EMT64 ou autres ; à base de Sun UltraSPARC. Concrètement pour la version 8.04 **Hardy Heron**, distribution utilisée pour cet ouvrage, les ressources demandées se situent :

Pour le minimum de base

- 300 MHz x86 (166 MHz dans le cas Xubuntu)
- 64 Mo de RAM (utilisation du CD-Rom Alternate)
- 4 Go d'espace disque (1,5 Go dans le cas Xubuntu)
- Carte VGA avec résolution 640x480

Pour le niveau recommandé

- 700 MHz x86 (300 MHz dans le cas Xubuntu)
- 384 Mo de RAM (256 Mo dans le cas Xubuntu)
- 8 Go d'espace disque
- Carte VGA avec résolution 1024x768 (800x600 dans le cas Xubuntu)

Pour une exigence particulière

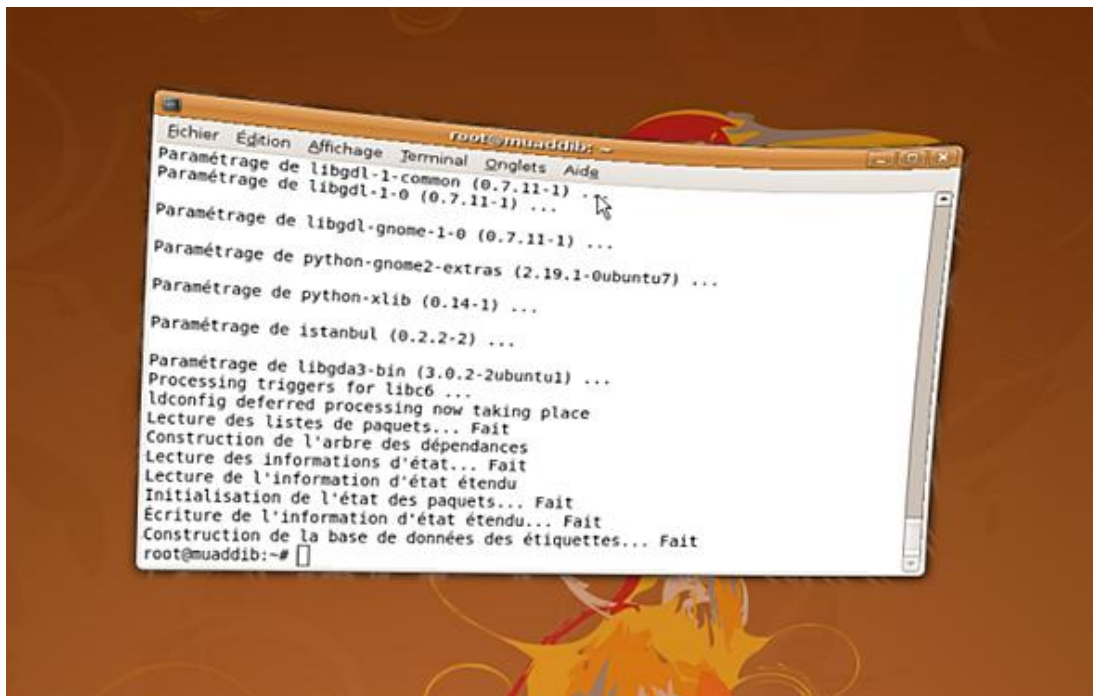
Certains effets visuels du bureau améliorent le rendu et le travail du bureau : fenêtres translucides, bureau en 3D, effets d'ombrages, animations, etc. Leurs emplois dépendent de la carte graphique (sans problème pour tous les modèles récents ATI, Intel, nVidia ; à vérifier pour les puces graphiques ou "*chipsets*" intégrés dans la carte mère) mais surtout de la volonté de l'utilisateur... On peut citer, en exemple, l'effet "fenêtre molle" : indispensable ou gadget ?

- 1,2 GHz x86
- 384 Mo de RAM

Voici le lien à partir du Wiki de la distribution **Gentoo**, indiquant la compatibilité des cartes graphiques support XGL et donc les effets visuels :

http://gentoo-wiki.com/HARDWARE_Video_Card_Support_Under_XGL

Voici une capture d'écran montrant l'effet "fenêtre molle" :



Il n'est pas fait mention d'un lecteur de CD-Rom/DVD-Rom et d'un équipement réseau dans les ressources nécessaires mais cela coule de source... Le premier s'utilisant comme support d'installation, le deuxième permettant l'accès au Web et aux mises à jour du système.

2. Outils pour l'administrateur

a. Utilisation de la distribution Ubuntu live

La distribution de base au démarrage du CD-Rom possède comme première ligne "*Essayer Ubuntu sans rien changer sur votre ordinateur*". Vous pouvez utiliser cette option pour démarrer et exploiter la distribution Ubuntu sans rien installer (ni altérer) sur votre disque dur.

Pour l'administrateur, l'intérêt est évident : tester facilement et rapidement un nouveau système d'exploitation, en comprendre les principales fonctionnalités, sans toucher à la machine support. Cette manipulation constitue un excellent départ pour la détection et l'identification du matériel avant toute installation : si la distribution live démarre correctement, il est quasiment sûr que son installation ne posera pas de problèmes...

Cette distribution servira de base aux explications de ce chapitre...

b. Utilisation d'un logiciel de virtualisation

Parallèlement à l'utilisation d'une distribution live, la virtualisation complète la panoplie de l'administrateur en lui offrant des ressources systèmes supplémentaires. La virtualisation fait fonctionner de manière logicielle plusieurs systèmes d'exploitation sur une seule machine physique.

Les acteurs présents sur le marché

Ils sont nombreux et appartiennent à la fois au monde libre et au monde commercial. Dans ce dernier cas, les éditeurs proposent aussi une solution non payante. Voici une sélection de logiciels de virtualisation sans licence payante :

- Solution avec **Xen** (OpenSource) : <http://www.citrixserver.com>

Récemment rachetée par Citrix, elle est plutôt réservée à des utilisateurs confirmés, voire experts (Système hôte de base : Linux).

- Solution avec **Virtual PC** (société Microsoft) : <http://www.microsoft.com/france/windows/xp/virtualpc/default.mspx>

Force est de constater que Microsoft ne virtualise correctement que ... du système Microsoft (Système hôte de base : Windows).

- Solution avec **VirtualBox** (société Innotek, récemment gratuit) : <http://www.virtualbox.org>

Performant et abouti, ce logiciel est correct dans l'utilisation de machines virtuelles autonomes et se réserve donc à l'utilisation d'un seul serveur (par exemple pour les développeurs avec un besoin d'un serveur Linux pour une application SGBD, WEB, JAVA, etc. (Système hôte de base : Windows ou Linux).

- Solution avec **VMware Server** (société VMware) : <http://www.vmware.com>

Le leader en la matière. La version VMware Workstation plus complète est payante (environ \$189). Cette version serveur se réserve à des utilisations moins professionnelles que la version VMware ESX, beaucoup plus onéreuse (Système hôte de base : Windows ou Linux).

Je vous conseille comme choix la troisième ou la quatrième solution.

Ressources matérielles nécessaires

L'utilisation d'un logiciel de virtualisation nécessite un minimum de configuration sur un PC :

- 2 Go de mémoire vive (RAM),
- 100 Go d'espace disque (idéalement un deuxième disque),
- un deuxième écran (optionnel, pour le confort).

Le premier point est essentiel si l'on veut disposer de plus d'une machine virtuelle en fonction en même temps. N'oubliez pas que vous avez aussi les ressources prises par le système hôte.

L'espace disque découle du nombre de machines virtuelles avec en moyenne une dizaine de Go par machine. L'utilisation d'un deuxième disque apporte uniquement un confort supplémentaire. Les machines virtuelles sont enregistrées sous la forme d'un gros fichier qu'il faut parfois vérifier et défragmenter. Un deuxième disque permet de ne pas surcharger votre disque principal et bloquer votre travail. Un deuxième écran (surtout sur un portable) vous offre le confort de ne pas constamment basculer de votre espace de travail aux écrans de machines virtuelles.

Si vous n'utilisez qu'une machine virtuelle, comme par exemple pour la découverte du système Ubuntu, les ressources se réduisent à 1 Go de RAM et une quinzaine de Go pour le disque. On peut même faire tourner une machine virtuelle à 256 Mo sur un système hôte qui en dispose 512.



La démarche de création d'une machine dépend du logiciel utilisé et sort du cadre de l'ouvrage. Vous trouverez facilement des tutoriels sur Internet.

3. Ressources nécessaires

L'installation de la distribution Ubuntu s'effectue à l'aide d'une image ISO, gravée ou non sur un CD-Rom/DVD-Rom. Pour obtenir celles-ci, trois méthodes sont possibles :

- Le **téléchargement** des images via le site officiel de la distribution suivant le choix d'un site miroir, géographiquement, le plus proche de vous : la possibilité par le biais de **BitTorrent** (ou avec **Jigdo** comme pour la Debian à partir de l'accès direct du site miroir).

Site officiel de la distribution : <http://www.ubuntu.com/getubuntu/download>

- L'**achat** des CD-Rom/DVD-Rom depuis la boutique en ligne de la société Canonical ou d'un distributeur dont la liste est fournie sur le site.

Site de la société Canonical : <https://shop.canonical.com>

- La **demande d'envoi gratuite** sponsorisée par cette même société Canonical des CD-Rom/DVD-Rom dans le plus pur esprit monde libre... Seul bémol : le délai assez long de livraison qui peut aller jusqu'à dix semaines.

a. Liste des images de la distribution Hardy Heron 8.04

Lors de la première méthode, et après le choix du serveur le plus proche de vous (ligne **Choose a location near you**), cliquez sur le lien **Start download** pour télécharger l'image ISO de la version choisie.

Pour obtenir la liste des images disponibles, vous devez cliquer sur le lien "**complete list of download locations**" en bas de cette page de téléchargement. Une liste des miroirs apparaît par continent.

Voici un extrait de la liste des images ISO tiré du site FTP France de Free et qui concerne les versions classiques (d'autres liens sont fournis pour Xubuntu, Kubuntu et Edubuntu) :

Ubuntu Releases

The following releases of Ubuntu are available:

- [Ubuntu 6.06.2 LTS \(Dapper Drake\)](#)
- [Ubuntu 6.10 \(Edgy Eft\)](#)
- [Ubuntu 7.04 \(Feisty Fawn\)](#)
- [Ubuntu 7.10 \(Gutsy Gibbon\)](#)
- [Ubuntu 8.04.1 LTS \(Hardy Heron\)](#)

Releases of [Kubuntu](#) and [Edubuntu](#) are also available here.

We are happy to provide hosting for the following projects via the [cdimage server](#). While they are not from their communities.

- [Gobuntu](#)
- [Mythbuntu](#)
- [UbuntuStudio](#)
- [Xubuntu](#)

For old releases, see old-releases.ubuntu.com.

Name	Last modified	Size	Description
 6.06	2008-Jan-21 20:22:24	-	
 6.06.2	2008-Jan-21 20:22:24	-	Ubuntu 6.06.2 LTS (Dapper Drake)
 7.04	2008-May-17 14:52:25	-	Ubuntu 7.04 (Feisty Fawn)
 7.10	2008-May-17 14:52:58	-	Ubuntu 7.10 (Gutsy Gibbon)
 8.04	2008-Jul-03 23:36:25	-	
 8.04.1	2008-Jul-03 23:36:25	-	Ubuntu 8.04.1 LTS (Hardy Heron)
 dapper	2008-Jan-21 20:22:24	-	Ubuntu 6.06.2 LTS (Dapper Drake)
 edubuntu	2008-Jul-04 00:57:35	-	Edubuntu Releases

Une fois choisie et téléchargée, l'image ISO se grave classiquement sur un CD-Rom. Une version intermédiaire existe parfois suivant la distribution. C'est le cas de la 8.04 Hardy Heron avec la version 8.04.1.



Il vaut mieux choisir un support CD-Rom plutôt qu'un DVD-Rom afin de ne pas encombrer inutilement les serveurs. Les logiciels non installés au départ le seront via le mécanisme de gestion de paquets (toujours à jour).

b. Vérification de l'empreinte d'une image ISO

Une bonne pratique : vérifier la bonne qualité de l'image par MD5SUM. Cet utilitaire construit une empreinte à partir des données de l'image. L'intégrité des données se trouve alors vérifiée (le fichier des empreintes se trouve en premier dans la liste des images). Alors que l'utilitaire se trouve installé nativement sur Linux, pour Windows, il faut le chercher sur le site **Fourmilab** de John Walker : <http://www.fourmilab.ch/md5>

Contrôle MD5SUM sous Windows

Après le téléchargement et la décompression de l'archive (format **zip**), l'exécutable se nomme **md5.exe**. Voici l'exemple du calcul de l'empreinte de l'image ISO (cela prend quelques secondes) de la version de base à partir d'une console de commandes DOS :



```
C:\WINDOWS\system32\cmd.exe
C:\>md5.exe G:\isos\ubuntu-8.04.1-desktop-i386.iso
C69E34E92D5402D1B87E6BABC739F774 G:\isos\ubuntu-8.04.1-desktop-i386.iso
C:\>
```

Il suffit de comparer cette empreinte avec celle trouvée dans le fichier MD5SUMS du répertoire sur **Free** de la Ubuntu 8.04.1 LTS (Hardy Heron) :

```
38e3f4d0774a143bd24f1f2e42e80d63 *ubuntu-8.04.1-alternate-amd64.iso
bbd21ded02c06b41c59485266833937a *ubuntu-8.04.1-alternate-i386.iso
b78ef719e3361e726b89bab78c526ad0 *ubuntu-8.04.1-desktop-amd64.iso
c69e34e92d5402d1b87e6babc739f774 *ubuntu-8.04.1-desktop-i386.iso
e7351d79903588699a383ae77854f734 *ubuntu-8.04.1-server-amd64.iso
7232c6004ba438890cd09aded162dc8e *ubuntu-8.04.1-server-i386.iso
```

Les deux concordent (quatrième ligne du fichier), le fichier a donc correctement été téléchargé.

Plus de commandes MD5SUM sous Linux Ubuntu

Sous Ubuntu, l'utilitaire présent par défaut se nomme **md5sum**. Les commandes ci-dessous sont réalisées en mode console sous Linux Ubuntu et en **root** (mettre **sudo** devant chaque commande dans le cas contraire).

Définir l'empreinte d'un fichier :

```
md5sum image1.iso
```

Définir l'empreinte d'un fichier et l'envoyer (redirection) dans un autre :

```
md5sum image1.iso > images.sum
```

En mettre une autre :

```
md5sum image2.iso >> images.sum
```

Faire le contrôle (autrement que visuel) :

```
md5sum -c images.sum
```

Deux lignes sont retournées avec la mention OK pour chaque empreinte.

Découverte de la distribution

Rappel : La suite de ce chapitre se base sur la fonctionnalité live de la distribution de base.

- Téléchargez l'image ISO desktop par la méthode de votre choix (normalement, par bittorrent ou jigdo).
- Vérifiez l'intégrité de l'image par md5sum.
- Gravez l'image sur un CD-Rom.

Deux remarques :

- Vous téléchargerez l'image spécifique à votre matériel : version 32 ou 64 bits (**ubuntu-8.04.1-desktop-i386.iso** ou **ubuntu-8.04.1-desktop-amd64.iso**) ; en cas de doute, prenez la première.
- Vous pouvez graver l'image sur un support physique ou bien employer un logiciel de virtualisation et utiliser le fichier ISO.

Il suffit ensuite de redémarrer l'ordinateur (ou la machine virtuelle) avec le lecteur de CD-Rom en premier dans la liste du BIOS. Le choix à prendre se trouve à la première ligne "Essayer Ubuntu sans rien changer sur votre ordinateur" après la demande de la langue :



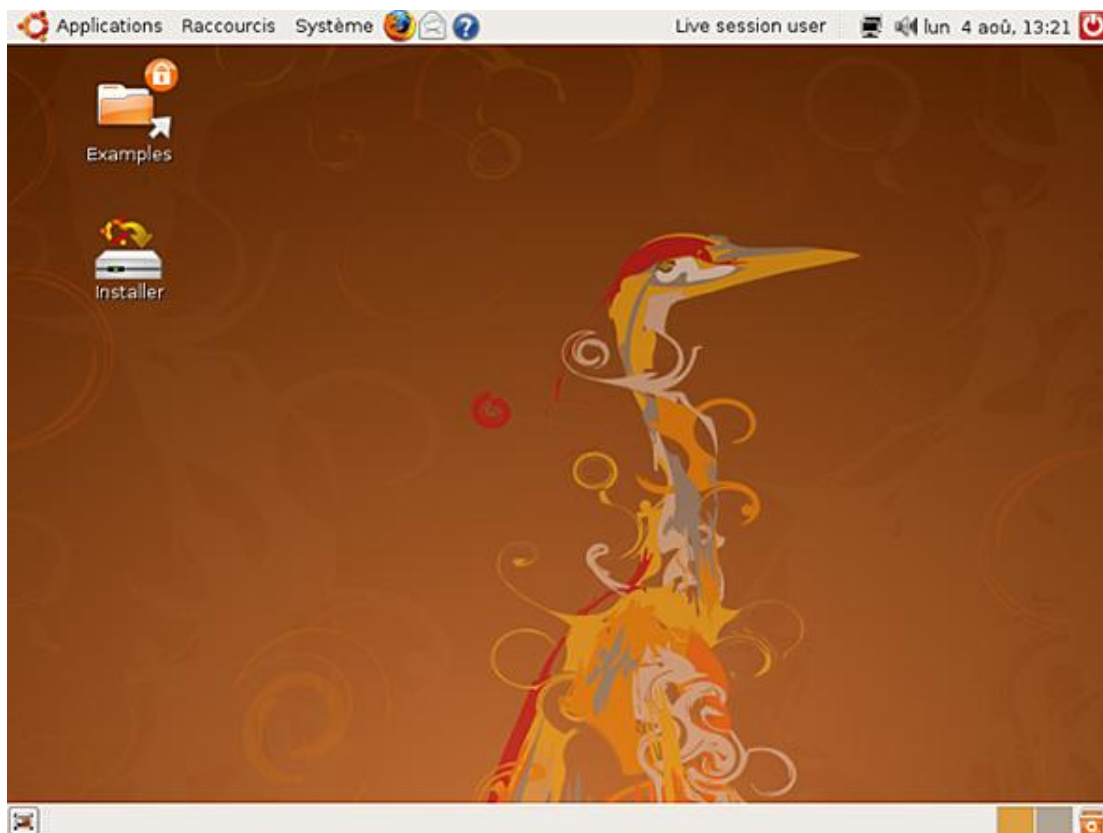
Essayer Ubuntu sans rien changer sur votre ordinateur
Installer Ubuntu
Vérifier le CD
Tester la mémoire
Démarrer à partir du premier disque dur

Appuyez sur F4 pour sélectionner un mode de démarrage et d'installation alternatif.

F1 Aide F2 Langue F3 Clavier F4 Modes F5 Accessibilité F6 Autres options

1. Fonctionnement du matériel

Une fois démarré, si démarrage correct il y a eu, le bureau GNOME apparaît. Dans le cas contraire au premier écran, appuyez sur la touche [F4] et choisissez le **mode graphique sans échec** car la plupart des problèmes viennent d'une mauvaise reconnaissance des caractéristiques de l'écran.



Le dossier **Exemples** sur le bureau contient un ensemble de fichiers permettant de tester les possibilités d'édition multimédia d'Ubuntu : fichiers png, xcf, ogg, rtf, etc. Le deuxième dossier offre le choix de l'installation de la distribution sur le disque dur.

a. Informations et tests

Pour connaître les matériels détectés par Ubuntu :

- Ouvrez une console en mode commande par les menus **Applications - Accessoires - Terminal**.
- Tapez la commande **lspci**.

Cette commande montre les informations sur les périphériques sur bus PCI de l'ordinateur :

```
ubuntu@ubuntu:~$ lspci
00:00.0 Host bridge: Intel Corporation Mobile 945GM/PM/GMS, 943/940GML and 945GT Express Memory Controller Hub (rev 03)
00:01.0 PCI bridge: Intel Corporation Mobile 945GM/PM/GMS, 943/940GML and 945GT Express PCI Express Root Port (rev 03)
00:1b.0 Audio device: Intel Corporation 82801G (ICH7 Family) High Definition Audio Controller (rev 02)
00:1c.0 PCI bridge: Intel Corporation 82801G (ICH7 Family) PCI Express Port 1 (rev 02)
00:1c.1 PCI bridge: Intel Corporation 82801G (ICH7 Family) PCI Express Port 2 (rev 02)
00:1c.2 PCI bridge: Intel Corporation 82801G (ICH7 Family) PCI Express Port 3 (rev 02)
00:1c.3 PCI bridge: Intel Corporation 82801G (ICH7 Family) PCI Express Port 4 (rev 02)
00:1d.0 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controller #1 (rev 02)
00:1d.1 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controller #2 (rev 02)
00:1d.2 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controller #3 (rev 02)
00:1d.3 USB Controller: Intel Corporation 82801G (ICH7 Family) USB UHCI Controller #4 (rev 02)
00:1d.7 USB Controller: Intel Corporation 82801G (ICH7 Family) USB2 EHCI Controller (rev 02)
00:1e.0 PCI bridge: Intel Corporation 82801 Mobile PCI Bridge (rev e2)
00:1f.0 ISA bridge: Intel Corporation 82801GBM (ICH7-M) LPC Interface Bridge (rev 02)
00:1f.1 IDE interface: Intel Corporation 82801G (ICH7 Family) IDE Controller (rev 02)
00:1f.2 IDE interface: Intel Corporation 82801GBM/GHM (ICH7 Family) SATA IDE Controller (rev 02)
00:1f.3 SMBus: Intel Corporation 82801G (ICH7 Family) SMBus Controller (rev 02)
01:00.0 VGA compatible controller: nVidia Corporation G70 [GeForce Go 7600] (rev a1)
02:00.0 Ethernet controller: Intel Corporation 82573L Gigabit Ethernet Controller
06:00.0 Network controller: Intel Corporation PRO/Wireless 3945ABG Network Connection (rev 02)
08:00.0 Mass storage controller: Silicon Image, Inc. SiI 3132 Serial ATA Raid II Controller (rev 01)
0a:03.0 CardBus bridge: Texas Instruments PCIxx12 Cardbus Controller
0a:03.1 FireWire (IEEE 1394): Texas Instruments PCIxx12 OHCI Compliant IEEE 1394 Host Controller
0a:03.2 Mass storage controller: Texas Instruments 5-in-1 Multimedia Card Reader (SD/MMC/MS/MS PRO/xD)
0a:08.0 Ethernet controller: Intel Corporation PRO/100 VE Network Connection (rev 02)
ubuntu@ubuntu:~$
```



Les renseignements ci-dessus proviennent d'une machine virtuelle avec le logiciel VMware Workstation, ce qui fait que beaucoup de lignes se rapportent à ce type de matériel.

Les lignes retournées informent l'administrateur sur les pilotes correctement détectés par le système (ces informations seront revues dans le chapitre traitant des périphériques et celui des modules du noyau). Une approche plus simple est proposée par Canonical avec le test des différents paramètres de votre système.

Créer son compte chez launchpad

Canonical a ouvert un site afin de gérer au mieux l'ensemble de ses services et le développement des projets OpenSource liés ou non à Ubuntu. Le site **Launchpad** favorise le travail communautaire par le partage facile du code, des rapports d'erreurs, des traductions, etc. d'un projet OpenSource. Tout naturellement, le projet Ubuntu est inscrit dans la catégorie distribution.

Voici l'adresse du site de Launchpad : <https://launchpad.net/>

Vous remarquerez le protocole `https` au lieu du classique `http`, car la gestion de projets demande des échanges sécurisés avec SSL (*Secure Socket Layer*, protocole de sécurisation des échanges sur Internet).

Afin de participer aux différents projets, ou simplement de s'inscrire comme membre de la communauté Ubuntu, vous devez créer un compte. L'inscription est gratuite et ne demande qu'une adresse e-mail afin de vous envoyer la procédure à suivre pour compléter votre compte : le nom dans la base des utilisateurs de Launchpad et le mot de passe personnel.

Une fois votre compte créé, vous pourrez participer à Rosetta, le système de traduction en ligne, Malone, le système de gestion de rapports d'erreurs, etc. Accessoirement, vous pouvez même créer votre page Wiki :



Test de votre matériel

L'envoi à Launchpad du résultat de ce test nécessite un compte ; aussi est-ce la raison (la seule ?) pour laquelle vous devez en créer un.

- Lancez l'application par le menu **Système - Administration - Test du matériel**.

Une série de questions et de manipulations se succèdent sur :

- le test de la carte son
- la détection de la résolution de l'écran
- le test vidéo des couleurs

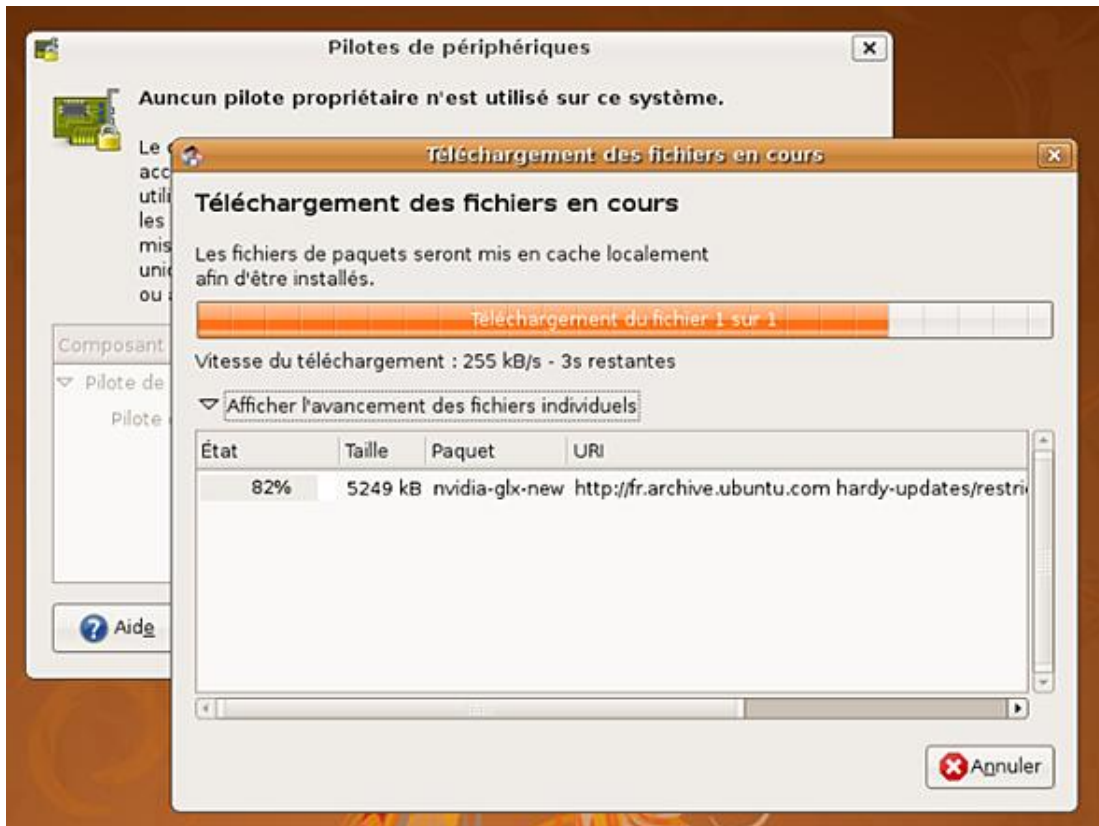
- le test du bon fonctionnement de la souris
- la détection de la carte réseau
- la vérification de la connexion Internet
- le test du clavier

Au final, un rapport est construit et sera envoyé à Launchpad si vous avez indiqué, au préalable, l'adresse électronique de votre compte.

b. Autres informations

Les renseignements concernant les autres matériels sont au niveau des menus **Système - Administration**. La ligne **Pilotes de périphériques** indique notamment si l'ordinateur devrait ou non employer des pilotes en accès restreint, c'est-à-dire des pilotes avec une licence propriétaire. L'activation de ces pilotes sera **rendu nécessaire** pour en obtenir le fonctionnement complet. L'exemple le plus courant concerne la carte graphique avec la possibilité d'activer les effets 3D du bureau (gestionnaire de fenêtres avancé Compiz) .

Voici l'exemple d'utilisation (et de son téléchargement) du pilote pour une carte Nvidia sur un portable :



Attention : cette manipulation s'adresse à un système physiquement installé et non à une distribution live comme c'est le cas ici.

2. Arborescence des fichiers

a. Structure du système

À la différence du système Windows, la structure de fichiers sous Linux ne se base pas par rapport aux périphériques : les lecteurs C, D, etc. englobés dans un ensemble à la tête duquel on trouve un bureau. Avec Linux et Ubuntu, le point de départ de la structure s'appelle tout simplement **la racine** et est noté par une barre oblique (/). Tout le reste est contenu dans cette racine : les fichiers de données, les fichiers répertoires ou les

périphériques ; ces derniers étant considérés comme des fichiers spéciaux. Devant la multiplicité des distributions Linux la dernière normalisation FHS 2.3 de 2004 tente d'uniformiser cette structure : <http://www.pathname.com/fhs>

La plupart des distributions Linux comme Ubuntu suivent l'essentiel du standard :

/

répertoire racine, base du système de fichiers.

/bin

contient les fichiers binaires exécutables.

/boot

contient les fichiers nécessaires au démarrage.

/cdrom

lien vers le répertoire /media/cdrom.

/dev

contient les fichiers spéciaux descripteurs de périphériques.

/etc

contient les fichiers de configuration utilisés par les programmes.

/home

contient les données propres à chaque utilisateur du type /home/nom_utilisateur.

/initrd

répertoire utilisé par le système pour le démarrage du noyau et des modules via un disque virtuel en RAM.

/lib

contient les bibliothèques du système et des binaires.

/lost+found

répertoire contenant les fichiers orphelins ou endommagés après une vérification, il indique que le répertoire courant est sur une partition dédiée.

/media

répertoire de montage des périphériques temporaires comme le CD-Rom, les clés USB, etc.

/mnt

répertoire ayant autrefois le rôle de /media, sert maintenant d'espace de montage de test pour l'administrateur.

/opt

contient les paquetages logiciels supplémentaires et particuliers (comme la taille) nécessitant un espace d'installation différent.

/proc

interface contenant un système de fichiers virtuel pour les informations sur le noyau et les processus.

/root

répertoire spécifique et séparé de l'administrateur.

/sbin

contient les fichiers binaires exécutables plus spécialement pour l'administrateur.

/srv

contient les données des services offertes par le système, comme par exemple le système LTSP.

/sys

contient les informations en provenance de /proc donc de la part des gestionnaires de périphériques sous la forme d'un pseudo-système de fichiers.

/tmp

espace de stockage des fichiers temporaires.

/usr

contient les données statiques exploitées par les utilisateurs : sources, exécutables, documentation, bibliothèques, etc.

/var

contient des fichiers à variables comme par exemple les journaux, les bases de données...



La distribution live possède un répertoire en plus : `rofs` indiquant un système de fichiers en lecture seule (à partir d'un fichier compressé sur le CD-Rom) et un répertoire en moins `lost+found` qui évidemment ne s'impose pas dans ce cas.

L'arborescence s'obtient sur la distribution live par les menus **Raccourcis - Poste de travail**. L'item **Système de fichiers** affiche les icônes des répertoires de l'arborescence.

b. Types de système de fichiers

Pour chaque partition Linux et au moment de l'installation du système, il faut choisir un type de système de fichiers. Mis à part le type `swap` spécial ou partition d'échanges destiné à augmenter virtuellement la taille de la mémoire présente sur l'ordinateur (sous Windows, cette fonctionnalité est dévolue à un fichier d'échange), Ubuntu propose les cinq types suivants :

Type de système de fichiers	Commentaires
ext2fs	Système de fichiers historique de Linux, devenu obsolète. Utilisé encore sur les disquettes.
ext3fs	Système de fichiers par défaut d'Ubuntu. Il gère la journalisation.
ReiserFS	Système alternatif maintenant mûre avec la version 4. Plus rapide dans le cas d'un système avec beaucoup de petits fichiers, il est à déconseiller pour les portables car gourmand en énergie.
JFS	Système alternatif porté par IBM, plus à l'aise dans la manipulation des gros fichiers.
XFS	Système alternatif porté par SGI (<i>Silicon Graphics Inc</i>) plutôt sur les Unix (<i>Irix</i>). Performant en cas d'une grande arborescence de fichiers.

À noter que tous ces systèmes gèrent les droits d'accès utilisateurs. À part ext2FS, tous supportent la fonctionnalité de journalisation rendant moins problématique un arrêt brutal et intempestif du système. Le journal enregistre les opérations d'écriture sur le disque dans le but de faciliter la synchronisation entre les opérations effectuées et celles en cours ; il facilite le maintien de l'intégrité des données.

Le choix entre tel ou tel système fait et fera toujours couler beaucoup d'encre... Chaque système possède des atouts indéniables par rapport aux autres. En termes de performances, les derniers tests ou "*benchmarks*" montrent un léger avantage à XFS. Pourquoi alors utiliser par défaut ext3FS ? Parce qu'il s'appuie sur le système traditionnel ext2FS de Linux et qu'il est le plus équilibré dans toutes les situations, en tant que serveur ou en tant que poste de travail.

Plan de partitionnement

1. Principes d'identification

a. Identification des périphériques

Du point de vue de l'environnement sous Linux/Ubuntu :

- Les disques durs IDE ou CD-Rom sont nommés `hd` suivi d'une lettre (de `a` à `d` avec un maximum de quatre par contrôleur, soit `hda`, `hdb`...) et d'un chiffre comme `hda2` qui indique la deuxième partition sur le premier disque maître IDE.
- Les périphériques SCSI (*Small Computer System Interface*) et les disques SATA (*Serial ATA*) sont nommés `sd` avec la même séquence que les disques IDE (avec un nombre de limitations plus élevé).
- L'archaïque lecteur de disquettes est représenté par `fd` ; `fd0` pour le premier lecteur.

La liste complète des identifiants se trouve dans le répertoire `/etc/dev`. Le clavier et l'écran, périphériques d'entrée/sortie par défaut ne sont pas représentés par un descripteur fichier dans le système mais par un lien (`stdin` pour standard in et `stdout` pour standard out).

b. Étiquette et UUID

L'UUID (*Universal Unique Identifier*) est une nouvelle technique pour identifier une unité de stockage, devenue nécessaire par l'apparition des périphériques USB. Le codage de longueur variable par des caractères alpha-numériques se calcule par un algorithme. Il garantit un identifiant unique pour chaque volume. La commande `vol_id` en mode console retourne cet identifiant :

```
vol_id --uuid /dev/sda1
```

On retrouve les UUID dans le fichier `/etc/fstab` servant de base au montage du système de fichiers. La commande `blkid` construit un UUID (ce point est vu dans un chapitre ultérieur traitant de l'ajout d'un nouveau disque).

Un label ou étiquette constitue un moyen plus pratique de manipulation, mais ne remplace pas l'UUID. C'est à considérer comme un alias plus compréhensible que l'UUID. Pour obtenir la totalité des renseignements (et l'étiquette), la commande se lance sans option :

```
vol_id /dev/sda1
```



Cette commande ne rend aucun résultat sur une distribution Live car le système (une partie, en fait) se trouve en mémoire. Le retour de la simple commande `df` le prouve.

2. Choix des partitions

L'axiome de base sur la sécurité d'un système impose une répartition des données sur plusieurs partitions. Ainsi en cas de problème, la sauvegarde et la restauration des données sont plus aisées. Les partitions dites "sensibles" suggérées par l'installateur Ubuntu sont `/home`, `/usr`, `/var` et `/tmp`. On peut rajouter à cette liste le répertoire `/boot` pour trois raisons :

- Pour plus de facilité en cas de changement de noyau et/ou de mise à jour du système.
- Avec l'utilisation de RAID ou LVM , car devant obligatoirement être séparé.
- La nécessité de l'emplacement au début de la géométrie physique du disque pour des disques et/ou chargeurs de démarrage anciens.

Forte de ce constat, la création des partitions correspond aux cas suivants :

- Deux partitions : une de `swap` et le système de fichiers dans son entier ; ce type de schéma convient aux postes de travail dont la sécurité des données n'est pas essentielle (ou exportées d'un serveur qui lui les sauvegarde).
- Trois partitions : `swap`, racine et `/home` ; la sécurité est axée sur la sauvegarde des données des utilisateurs plutôt que sur le système. On peut envisager un système RAID pour le répertoire des utilisateurs.
- Plus de trois partitions : situation d'un serveur où toutes les combinaisons sont possibles et fonctions du degré de sécurité attendu ; une attention particulière est à noter concernant le répertoire `/var` qui contient quand même les bases de données, journaux, etc.

Initialisation du système

1. Processus de démarrage

Le premier secteur d'un disque dur porte le nom de MBR (*Master Boot Record*). Une fois donné le contrôle par le BIOS, le programme contenu dans ce secteur :

- lit la table des partitions,
- contrôle la partition indiquée comme active,
- lit le premier secteur de celle-ci nommé secteur de boot.

Le deuxième programme contenu dans le secteur de boot :

- lit la première partie du système d'exploitation trouvé,
- lance ce système d'exploitation.

L'ensemble de ces deux programmes constitue le chargeur de démarrage. Sous Ubuntu deux sont proposés : **GRUB** (*GRand Unified Bootloader*) celui installé par défaut et **LILO** (*LI*nux *LO*ader) plus classique et maintenant aussi performant que GRUB depuis les versions permettant l'adressage au delà des premiers 1024 cylindres du disque pour le noyau. Les deux programmes forment un tout mais peuvent être dissociés c'est-à-dire n'être présents que dans un des deux.

Exemple :

La partie GRUB contenue dans le MBR peut lancer un autre système d'exploitation comme Windows (cf. le chapitre sur l'installation de Ubuntu en dual boot ou double démarrage).

Ubuntu utilise le mécanisme `initrd` (*INITial Ram Disk*) qui contient un système de fichiers et le monte en mémoire (`/dev/ram0`) afin de charger des modules pour le noyau. Cette démarche rend plus polyvalent et adaptatif le démarrage du système à la différence des noyaux de type UNIX préférant une approche statique (le noyau est alors plus gros). Ensuite, le système de fichiers du disque est monté avec en suivant la libération de la RAM et l'exécution de la commande `init`, père de tous les autres processus.

À partir de la distribution LIVE :

- Ouvrez une console en mode commande par les menus **Applications - Accessoires - Terminal**.
- Tapez la commande `ps aux | less` (la barre s'obtient par [Alt Gr] 6 ; pour quitter tapez `q`).

La première ligne donne un PID, c'est-à-dire un numéro de processus à 1.

2. Chargeurs de démarrage

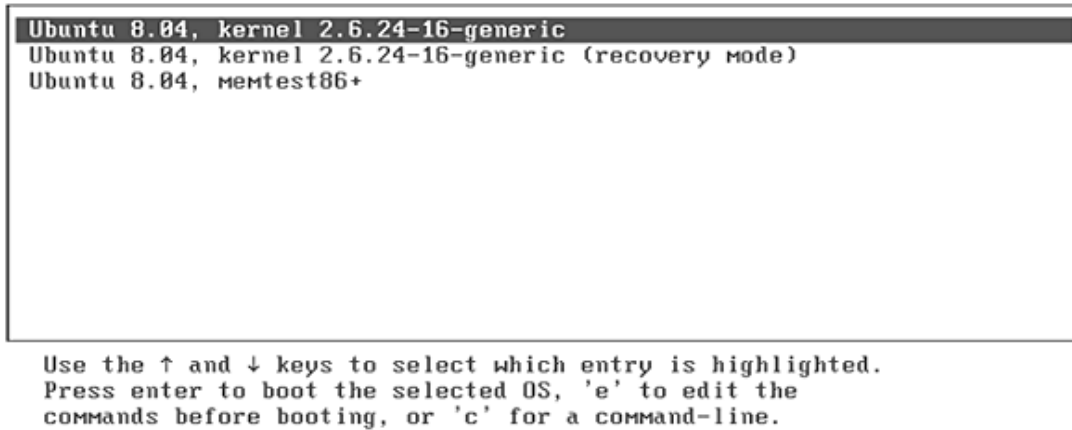
a. GRUB

GRUB est un projet GNU en version 0.97 sur Ubuntu. Une fois installé, les composants se trouvent dans le répertoire `/etc/grub` :

- `stage1` et `stage2`, respectivement le premier programme (MBR) et le deuxième (secteur de boot) du chargeur de démarrage.
- `XXX_stage1_5` (`e2fs_stage1_5`, `reiserfs_stage1_5`, etc.) programme intermédiaire (pont) entre `stage1` et `stage2` dépendant du système de fichiers ; `stage1_5` est appelé par `stage1` et appelle `stage2`.
- `installed-version`, contenant le numéro de version.

- `menu.lst`, le fichier de configuration.
- `default`, à ne pas modifier car résultant de la commande `grub-set-default` et définissant dans le fichier de configuration le système à charger après un laps de temps prédéfini.

Écran de démarrage GRUB sur une Hardy Heron :



Adresse du site Internet pour GRUB : <http://www.gnu.org/software/grub>



Vous reverrez d'autres aspects de GRUB dans le chapitre traitant sur les installations particulières, dans celui de la prise en main de la distribution et plus particulièrement son dépannage dans le chapitre traitant sur la maintenance de base du système.

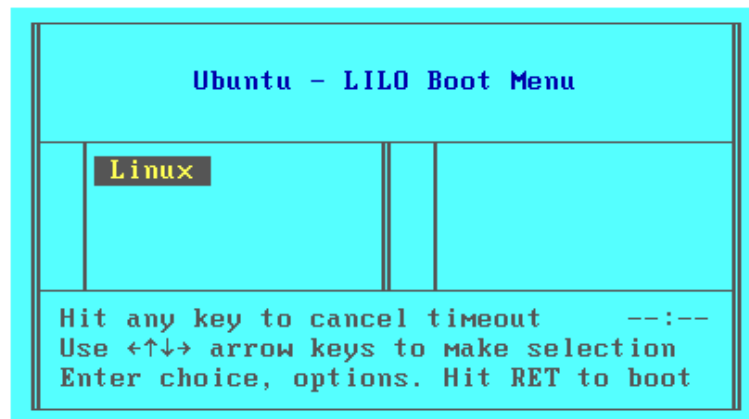
b. LILO

LILO sous licence BSD, en version 1.22.8 se charge avec le paquet de même nom et à besoin de la dépendance `mbr` (utilitaire pour démarrer un système à partir d'un disque). Après installation, le système dispose des commandes :

- `lilo_find_mbr` : commande retournant l'UUID de la partition active (avec le MBR), très utile pour identifier la bonne partition.
 - `liloconfig` : le script de configuration aboutissant à la création du fichier `/etc/lilo.conf`.
 - `lilo` : la commande installant le chargeur de démarrage.
- Pour installer LILO à la place de GRUB sur Ubuntu, il faut choisir impérativement une installation en mode expert.

Adresse du site Internet pour LILO : <http://lilo.go.dyndns.org>

Écran de démarrage LILO sur une Hardy Heron :



boot: _

Dépôts logiciels

1. Types de dépôts

Ubuntu comme Debian utilise des serveurs externes à des fins d'installations de logiciels et de mise à jour du système. Même si les deux distributions sont très proches, **il est fortement déconseillé** d'utiliser les dépôts logiciels de Debian pour Ubuntu, chacun des systèmes ayant des raffinements différents. D'ailleurs, les catégories de dépôts sont différentes :

- **Debian Etch 4.0** : la distribution (etch), les mises à jour (etch/updates), les temporaires (etch/volatile) comme les définitions de virus.
- **Ubuntu Hardy Heron** : la distribution (hardy), les mises à jour (hardy-updates), les mises à jour de sécurité (hardy-security).



Les logiciels ou paquets du CD-Rom ne couvrent pas l'ensemble de la distribution. Ils permettent de construire un système avec les fonctionnalités de base.

Pour chaque catégorie de dépôts, les logiciels se répartissent en fonction de la licence (sections) :

	Debian	Ubuntu
Logiciels libres maintenus officiellement	main	main
Logiciels non libres maintenus officiellement	non free	restricted
Logiciels libres mais ayant une source non libre	contrib	x
Logiciels libres non maintenus officiellement	x	universe
Logiciels non libres non maintenus officiellement	x	multiverse
Logiciels rétroportés construits à partir de la version de développement	etch-backports	backports
Logiciels commerciaux libres et non libres maintenus officiellement	x	partner

D'autres dépôts existent comme les dépôts concernant le multimédia (codecs, lecteurs, etc.) ou des applications spécifiques avec la virtualisation et le dépôt de la société **Innotek** (*Virtual Box*). Pour faire fonctionner ces dépôts, l'importation d'une clé GPG (*GNU Privacy Guard*) est nécessaire pour l'authentification. Pour les dépôts officiels, ces clés sont déjà présentes dans le répertoire `/var/lib/apt/lists/`.

2. Serveurs miroirs

L'utilisation d'un serveur miroir est fortement recommandé car cela réduit les temps de connexion en évitant la surcharge des serveurs maîtres. L'adresse d'un miroir officiel Ubuntu pour un pays se compose comme suit :

`code_pays.archive.ubuntu.com`

Soit pour la France : `fr.archive.ubuntu.com` qui est le serveur **FTP d'Oleane**. Parallèlement, il existe d'autres serveurs secondaires qui rendent le même service, voire mieux, en cas de saturation du serveur officiel.

Le site Launchpad , déjà vu, héberge des projets de développement communautaire avec bien sûr le projet Ubuntu.

On trouve pour celui-ci deux ressources importantes :

- les paquetages avec la possibilité d'une recherche ou de voir la liste entière.
- les miroirs officiels de la distribution par pays.

Pour ces derniers, on trouve deux renseignements supplémentaires :

- la vitesse de la bande passante.
- l'état de synchronisation : de "une semaine" (*One week behind*) au meilleur : "à jour" (*Up to date*).

Dernier renseignement utile si l'on désire créer son propre serveur miroir : les protocoles disponibles et la présence de rsync.



Les serveurs français sont, à la rédaction de l'ouvrage, au nombre de sept. Le choix de l'un ou l'autre dépend du goût de chacun. Il ne faut pas penser prendre un serveur et s'y tenir car les conditions d'accès varient... Un choix personnel : le serveur de l'association **CRIHAN** à l'initiative du Conseil Régional de Haute-Normandie qui réunit à la fois de bonnes qualités de transfert et de synchronisation à jour. Notez que l'on peut parfaitement utiliser un serveur d'un autre pays, cela n'influe en rien les paramètres régionaux du système installé.

Sur la distribution, les ajustements concernant les sources de logiciels se trouvent par les menus **Administration - Système - Sources de logiciels**.



Il est bien entendu inutile de mettre à jour la distribution live...

Installation normale d'un poste de travail

L'installateur Ubuntu a considérablement évolué depuis les premières versions pour aboutir à un total de seulement sept écrans entre le début et la fin du processus. Dans le cas d'une installation autonome sur une machine (*stand alone*), les choix proposés par défaut suffisent : ce qui en fait l'une des distributions (si ce n'est la distribution...) la plus simple et rapide à installer.

 Les notions techniques (heure GMT, partitionnement, etc.) sont détaillées dans le deuxième paragraphe traitant de l'installation en mode expert de la version serveur.

1. Préalable à l'installation

Pré-requis : l'image ISO gravée sur un CD-Rom et téléchargée à partir d'un des sites miroirs vu au chapitre précédent, soit : `ubuntu-8.04.1-desktop-i386.iso`

Pour un démarrage du CD-Rom à partir du lecteur, le BIOS de la machine se paramètre soit :

- En "dur" dans le `setup`, accessible suivant le modèle de carte mère par les touches [Suppr] ou [F2] (pour les plus courantes AWARD ou AMI).
- À la volée par le choix donné dans un menu de démarrage (`Boot`), appelé par les touches [F11], [F12] voire [Echap] (les plus courantes).

 Préférez le deuxième choix car, somme toute, une installation constitue un cas particulier de démarrage : le lancement normal se faisant à partir du disque dur. Dans le cas d'un serveur normalement jamais éteint, cela peut éviter une mauvaise surprise dans le cas - rare - d'un reboot intempestif avec un CD-Rom laissé dans le lecteur...

2. Processus d'installation

La demande de la langue apparaît immédiatement afin de personnaliser le menu d'accueil. Vous pouvez changer la langue à nouveau en appuyant sur la touche [F2].

Rappel : l'option **Essayer Ubuntu sans rien changer sur votre ordinateur** fera démarrer la distribution en live avec un chargement uniquement en mémoire vive (RAM).

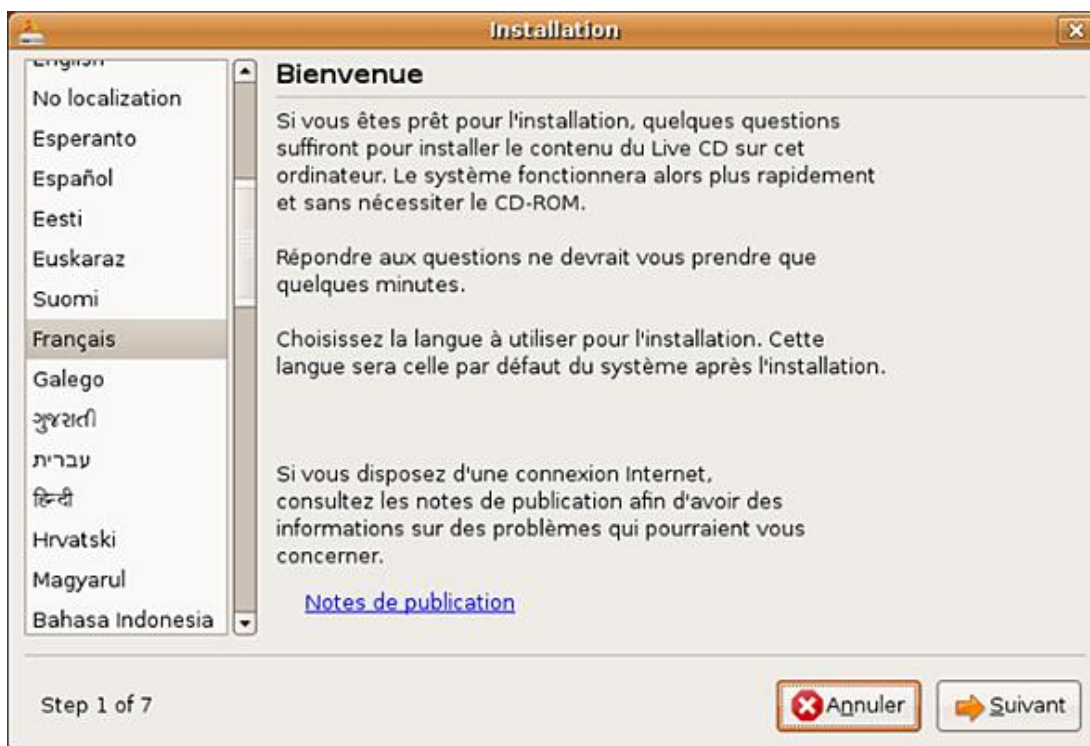
- Choisissez et validez la ligne **Installer ubuntu**.

a. Écran de bienvenue

La demande de la langue se positionne automatiquement en fonction du choix précédent.

- Choisissez la ligne **Français**, cliquez sur le bouton **Suivant**.

 Le lien **Notes de publications** lance le navigateur Web Firefox et charge la page des informations de la version. Cela suppose une connexion Internet... que vous n'avez pas ici. Cette option n'est valable que si vous lancez l'installation à partir du bureau lors d'un démarrage en live.



b. Écran de l'emplacement géographique

La détection du fuseau horaire est automatique. Il peut arriver que l'heure ne coïncide pas mais cela se réglera après l'installation.

- Acceptez la détection de paramètres ville (**Paris**) et l'heure, cliquez sur le bouton **Suivant**.

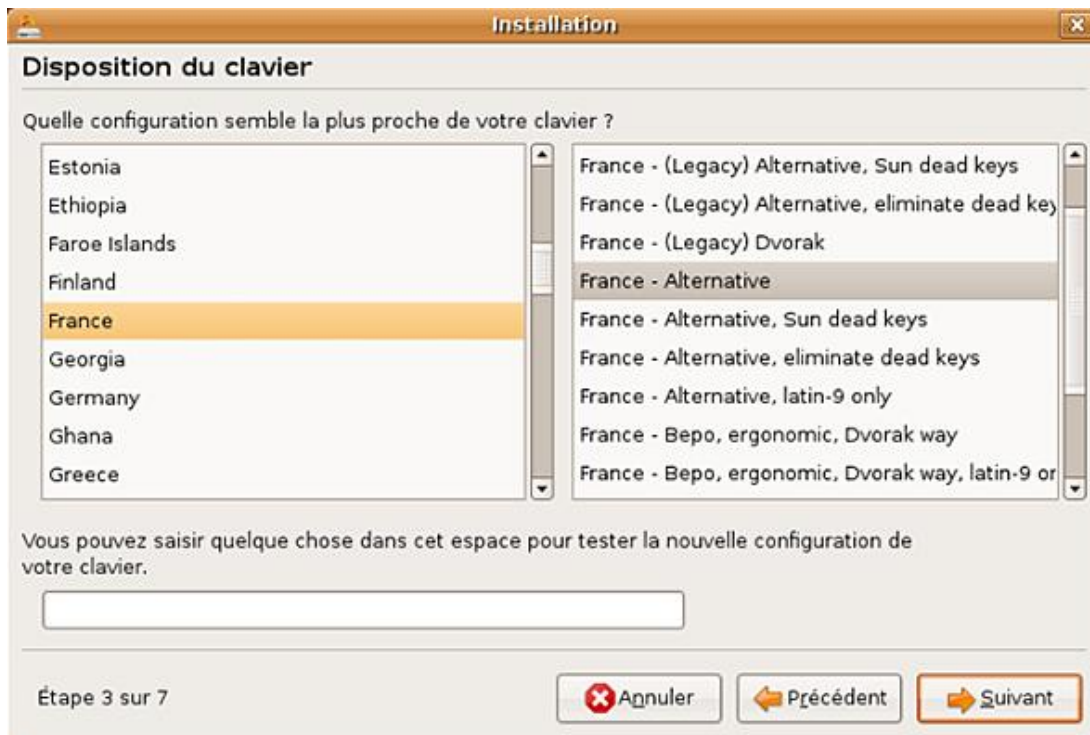


c. Écran de disposition du clavier

Le choix par défaut **France - Alternative** correspond à la disposition **latin-9** pour un clavier de type 105 touches

(modèle courant).

- Acceptez les choix **France, France - Alternative**, cliquez sur le bouton **Suivant**.



d. Écran de préparation de l'espace disque

Le choix **Assisté - utiliser un disque entier** créera deux partitions :

- une partition principale avec le système de fichiers complet.
- une partition étendue pour la partition swap.



Rappel : le choix manuel de création des différentes partitions est décrit dans le paragraphe suivant.

- Choisissez le choix **Assisté - utiliser un disque entier**, cliquez sur le bouton **Suivant**.



e. Écran de l'identité du "super" utilisateur

Le système multi-utilisateur Linux nécessite au moins un compte pour ouvrir une session. Sur Ubuntu, le compte de l'administrateur étant suspendu, les renseignements demandés pour la première fois correspondent à l'utilisateur principal doté de droits étendus (le "super" utilisateur).

- Entrez le nom patronymique, le nom de connexion (login) si différent, le mot de passe et sa vérification, le nom de machine et cliquez sur le bouton **Suivant**.



f. Écran de "Prêt à installer"

Le bouton **Avancé** vous permet de :

- modifier les paramètres du chargeur de démarrage (déconseillé dans cet exemple).
- participer aux statistiques d'utilisation des paquets (facultatif).
- paramétrer un serveur mandataire (proxy), c'est-à-dire l'adresse d'un ordinateur représentant la "porte de sortie" pour Internet de votre réseau (généralement dans une situation en entreprise).

Attention : à l'issue de cet écran, le formatage du disque commence. Les données présentes à l'origine sont irrémédiablement perdues.

- Entrez éventuellement les coordonnées d'un serveur mandataire par le bouton **Avancé**, sinon cliquez sur le bouton **Installer**.

L'état d'avancement de l'installation du système s'apprécie par une barre de progression. Dans sa phase finale, un téléchargement externe des paquets linguistiques, dont le temps varie en fonction de la vitesse de votre connexion, s'effectue.

La dernière demande propose un simple bouton **Redémarrer maintenant** qui fera éjecter le CD-Rom. Après un appui sur la touche [Entrée] (*Enter*), le système redémarre et aboutit à l'écran de connexion pour l'ouverture d'une session.

Vous êtes maintenant prêt à ouvrir une session en tant qu'utilisateur.

Installation en mode expert d'un serveur

La procédure décrite ci-dessous concerne, cette fois-ci, l'installation de la version serveur Ubuntu en mode **expert**. Dans ce mode, l'administrateur maîtrise l'installation au niveau le plus bas.

1. Préalable à l'installation

Pré-requis : l'image ISO gravée sur un CD-Rom et téléchargée à partir d'un des sites miroirs vu au chapitre précédent, soit : ubuntu-8.04.1-server-i386.iso

Les autres éléments sont identiques à ceux de l'installation en poste de travail.

2. Première phase du processus d'installation

a. Sélection de la langue

La version serveur, pour la distribution **Hardy Heron**, propose immédiatement (comme pour l'installation en poste de travail) le choix de la langue dans un menu lié par défaut au premier écran général. Notez que quelques phrases cependant ne seront pas traduites et restent en langue anglaise : elles s'avèrent inutiles en mode texte. Il faudra à nouveau redéfinir les paramètres régionaux.

b. Passage en mode texte

À l'instar de sa grande sœur (la distribution Debian), Ubuntu propose une installation en mode expert (au sens Debian on indique une priorité définie à `low` au niveau de l'installateur `debconf`). Ce changement de priorité, transparent pour l'opérateur, se trouve uniquement disponible en mode texte.

- Quittez l'installateur graphique en utilisant la touche [Echap], validez par **OK**.

Après la demande de confirmation, une simple ligne de commande avec le terme `boot` apparaît. L'appui de la touche [F1] fait apparaître l'aide et les possibilités de l'installation :

Welcome to Ubuntu!

This is an installation CD-ROM for Ubuntu 8.04.
It was built on 20080423.2.

HELP INDEX

KEY	TOPIC
-----	-------

<F1>	This page, the help index.
<F2>	Prerequisites for installing Ubuntu.
<F3>	Boot methods for special ways of using this CD-ROM
<F4>	Additional boot methods; rescue mode.
<F5>	Special boot parameters, overview.
<F6>	Special boot parameters for special machines.
<F7>	Special boot parameters for selected disk controllers.
<F8>	Special boot parameters for the install system.
<F9>	How to get help.
<F10>	Copyrights and warranties.

Press F2 through F10 for details, or ENTER to boot: _

Les écrans <F2>, <F9> et <F10> sont de simples écrans d'informations. L'écran <F4> concerne la réparation d'un

système endommagé comme proposé lors de l’affichage graphique du premier écran. L’écran <F5> donne une courte information sur les écrans <F6>, <F7> et <F8>. En cela il diffère de l’installation en mode graphique où l’appui de la touche <F5> concernait des modes d’installation adaptés à des personnes handicapées (contraste élevé, loupe, terminal en braille, etc.).

L’écran <F6> traite des paramètres à passer au noyau Linux lors de l’installation concernant des particularités matérielles :

SPECIAL BOOT PARAMETERS - VARIOUS HARDWARE

F6

You can use the following boot parameters at the **boot:** prompt, in combination with the boot method (see <F3>).

If you use hex numbers you have to use the 0x prefix (e.g., 0x300).

HARDWARE	PARAMETER TO SPECIFY
IBM PS/1 or ValuePoint (IDE disk)	hd=cylinders,heads,sectors
Some IBM ThinkPads	floppy.floppy=thinkpad
IBM Pentium Microchannel	mca-pentium no-hlt
Protect I/O port regions	reserve=iobase,extent[,...]
Workaround faulty FPU (old machines)	no387
Laptops with screen display problems	vga=771
Use first serial port at 9600 baud	console=ttyS0,9600n8
Force use of generic IDE driver	generic.all_generic_ide=1

If you experience lockups or other hardware failures, disable buggy APIC interrupt routing

noapic nolapic

For example:

boot: install vga=771 noapic nolapic

Press F1 for the help index, or ENTER to boot: _

Les paramètres utilisés se rapportent parfois au contrôleur programmable d’interruptions IO-APIC (*I/O Advanced Programmable Interrupt Controller*) posant problème dans la gestion de l’horloge système sur certains matériels. L’exemple donné avec les paramètres `noapic` et `nolapic` indique au noyau de ne pas utiliser ce contrôleur.

➤ J’ai personnellement rencontré ce type de problème sur une architecture 64 bits, sujet à ce type de réglage.

L’option **vga=771** représente un écran en 8 bits et 800x600, toujours en cas de problème d’affichage et en utilisant le mode framebuffer.

➤ Le framebuffer est une technique qui utilise la carte graphique sans pilote attitré. Par défaut dans le noyau Linux, ses paramètres les plus utilisés sont présentés dans le tableau ci-dessous :

	640x480	800x600	1024x768	1280x1024
8 bits	769	771	773	775
16 bits	785	788	791	794
32 bits	786	789	792	795

Une autre numérotation donne le nombre de lignes et de colonnes (mode 6 pour vga = 775) :

0	80x25
1	80x50
2	80x43
3	80x28
4	80x30

5	80x34
6	80x60

L'écran <F7> traite des paramètres à passer au noyau Linux en cas de contrôleurs disques spécifiques :

SPECIAL BOOT PARAMETERS - VARIOUS DISK DRIVES

F7

You can use the following boot parameters at the **boot:** prompt, in combination with the boot method (see <F3>).

HARDWARE	PARAMETER TO SPECIFY
Adaptec 151x, 152x	aha152x.aha152x=iobase[,irq[,scsi-id[,reconnect]]]
Adaptec 1542	aha1542.aha1542=iobase[,buson,busoff[,dmaspeed]]
Adaptec 274x, 284x	aic7xxx.aic7xxx=no_reset (enabled if non-zero)
BusLogic SCSI Hosts	BusLogic.BusLogic=iobase
Certain DELL machines	aic7xxx.aic7xxx=no_probe

This list is incomplete, see the kernel's kernel-parameters.txt file for more.

For example:

```
boot: install aic7xxx.aic7xxx=no_probe
```

Press F1 for the help index, or ENTER to boot: _

L'écran <F8> traite des paramètres à passer au noyau Linux lors de problèmes concernant l'installation proprement dite. L'option fb désactive le framebuffer si la carte graphique ne le supporte pas. On peut ainsi imposer une configuration nationale pour le clavier comme bootkbd=fr.



Ceci ne concerne pas paradoxalement l'installation en mode texte, le clavier étant configuré par défaut pour la langue anglaise et donc en QWERTY. Le choix de langue sera à nouveau proposé pour cela.

SPECIAL BOOT PARAMETERS - INSTALLATION SYSTEM

F8

You can use the following boot parameters at the **boot:** prompt, in combination with the boot method (see <F3>). These parameters control how the installer works.

RESULT	PARAMETER
Verbose debugging	DEBCONF_DEBUG=5
Debug boot sequence	BOOT_DEBUG=2:3
Disable framebuffer	fb=false
Don't probe for USB	debian-installer/probe/usb=false
Don't start PCMCIA	hw-detect/start_pcmcia=false
Force static network config	netcfg/disable_dhcp=true
Set keyboard map	bootkbd=es
Use Braille tty	brltty=driver,device,gettexttable
Use high contrast accessibility theme	theme=dark
Use special tasks	tasks="kde-desktop, standard"

For example:

```
boot: install fb=false
```

Press F1 for the help index, or ENTER to boot: _

Enfin, l'écran <F3> donne les niveaux de contrôles de l'installation :

Available boot methods:

```

install
    Start the installation -- this is the default CD-ROM install.
expert
    Start the installation in expert mode, for maximum control.
cli, cli-expert
    Minimal command-line system install.
memtest
    Perform a memory test.

```

To use one of these boot methods, type it at the prompt, optionally followed by any boot parameters. For example:

```
boot: install acpi=off
```

If unsure, you should use the default boot method, with no special parameters, by simply pressing enter at the boot prompt.

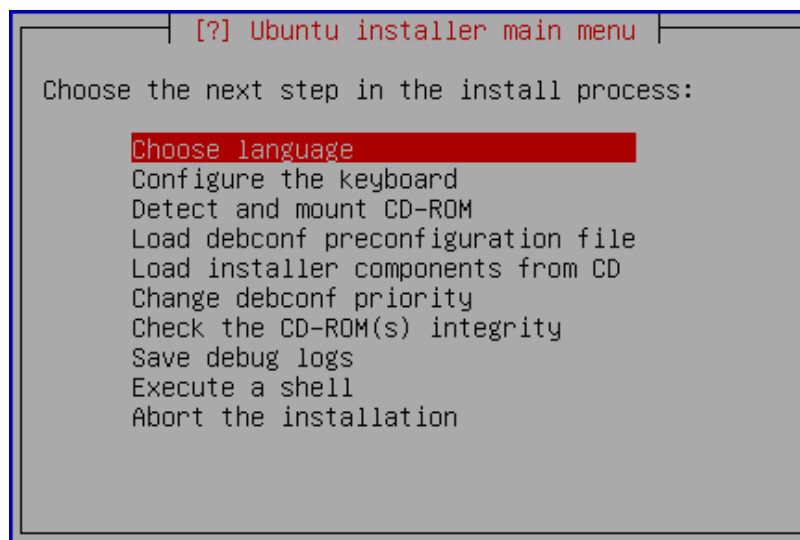
Press F1 for the help index, or ENTER to boot: _

Pour une totale maîtrise de l'installation, le choix se porte sur **expert**. Les options **cli** et **cli-expert** ne sont pas opérationnelles.

- Tapez **expert** à l'invite du boot.

3. Deuxième phase du menu d'installation

L'écran principal du menu ne contient pas toutes les phases d'installation. Il apporte les réglages nécessaires au départ de l'environnement de l'installation :



a. Ligne "Choisir la langue"

La première ligne traite respectivement du choix de la langue, du pays d'origine et des paramètres régionaux.

- Sélectionnez **French**, **France** et **fr_FR.UTF-8**.
- Décochez **en_US.UTF-8** et cochez en plus **fr_FR** et **fr_FR@euro** à l'écran des paramètres supplémentaires pour une couverture complète de la langue française.



Les RFC (*Request For Comments* signifie littéralement "demande de commentaires") définissent, par un travail participatif des spécialistes, les standards de l'Internet. Vous voulez tout savoir de la nouvelle norme officielle IPv6 ? Consultez la RFC 2460. Savoir lire une RFC (la lecture peut être rébarbative) fait partie intégrante de la panoplie du bon administrateur système. Ne pas en lire enlève une dimension professionnelle appréciée à votre profil.

La norme UTF-8, standard défini dans la RFC 3629, code les caractères sur une suite de quatre octets dans un souci d'universalité.

b. Ligne "Configurer le clavier"

La deuxième ligne du menu concerne le paramétrage du clavier.

- Sélectionnez **Generic 105-key (Intl) PC**.
- L'agencement du clavier (layout) peut être ignoré, indiquez **Non** dans ce cas.
- Sélectionnez **France** et **France - Alternative** pour l'origine du clavier et sa disposition.
- Gardez la **Touche Alt de droite** pour la touche **AltGr**.
- Sélectionnez ensuite **Pas de touche « compose »** car UTF-8 est unicode, **UTF-8, latin1 et latin5 (...)**.
- Validez par défaut le type de police (on ne peut rien mettre d'autre), et **16** comme taille de police.
- Validez **/dev/tty[1-6]** afin de disposer de six consoles virtuelles.



Une console virtuelle ouvre un terminal de type texte offrant la possibilité de nouvelles sessions de travail. Pour plus de détails, voir le chapitre Session en mode console.

c. Ligne "Détecter et monter le CD"

La troisième ligne du menu détecte et monte le support d'installation (CD-Rom). Il propose aussi le chargement de modules complémentaires pour le noyau comme USB et le démarrage des services de cartes PC comme les cartes PCMCIA (carte au format "cartes de crédit" que l'on trouve généralement sur les portables).

- Sélectionnez ou non par la barre d'espace l'option **USB storage** (certainement inutile dans le cadre d'un serveur).
- Sélectionnez ou non le démarrage des services de cartes PC (toujours inutile pour un serveur).

Le dernier écran fait état d'un utilitaire `hdparm` qui s'utilise avec les périphériques IDE (contrôleur au BUS-AT ou ATA) délaissé maintenant pour l'EIDE (*Enhanced IDE* ou ATA2) et le S-ATA (Serial ATA ou SATA). Le lecteur CD-Rom fait partie des périphériques IDE et la commande `hdparm` permet, par exemple, le réglage du nombre de secteurs lus par anticipation ; cela peut influencer sur la vitesse de lecture suivant la taille et le nombre des fichiers.

- Il n'est pas nécessaire d'activer `hdparm` dans le cadre d'une installation, validez la ligne vide.

L'examen du répertoire d'installation sur le CD-Rom s'effectue et le résultat d'un bon déroulement s'affiche :

```
[.] Détecter et monter le CD
      Un CD a été détecté
La détection automatique du CD s'est bien déroulée. Un lecteur de
CD-ROM a été identifié et ce lecteur contient le CD : Ubuntu-Server
8.04 "Hardy Heron" - Release i386 (20080423.2). Vous pouvez
poursuivre l'installation.

      <Continuer>
```

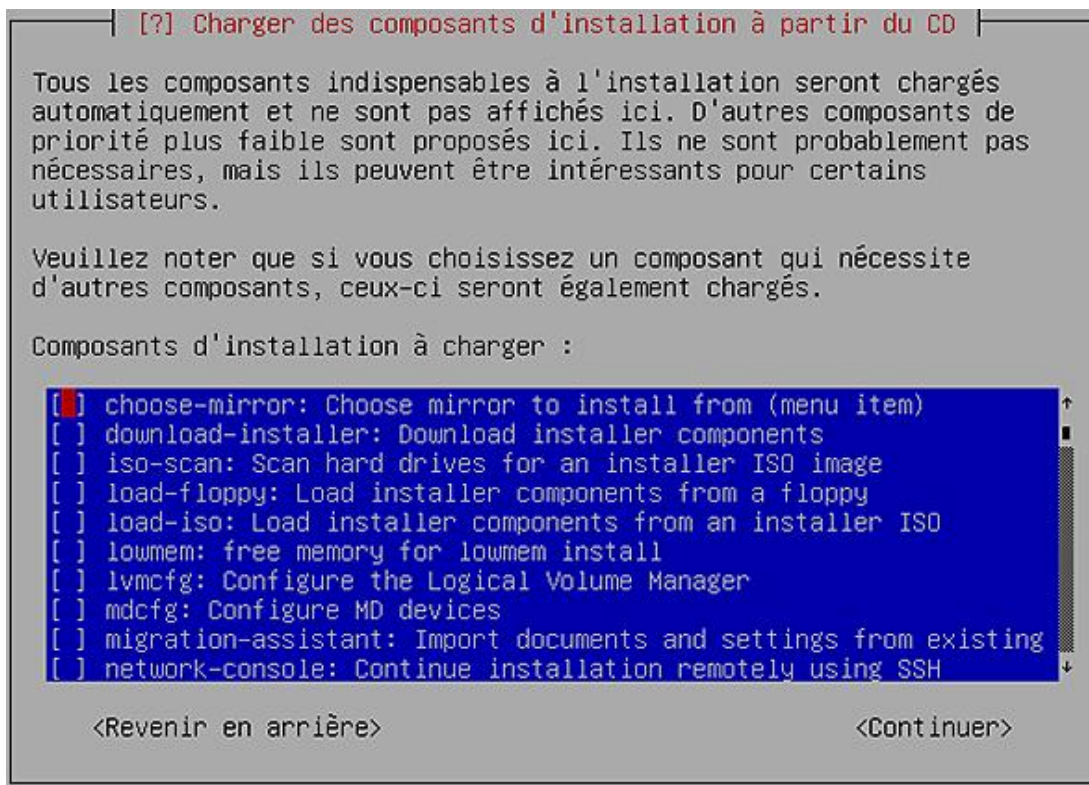

d. Ligne "Charger un fichier de configuration"

Cette ligne ne propose aucun menu et n'est là que dans un souci de compatibilité. Elle fait référence à l'utilitaire de configuration de paquets `debconf` qui accepte de définir des options dans un fichier afin de réduire le temps d'installation des paquets logiciels.

- Validez ou passez à la ligne suivante.

e. Ligne "Charger des composants d'installation à partir du CD"

Cette ligne propose des composants d'installation supplémentaires généralement non nécessaires :



Voici une sélection de trois choix intéressants :

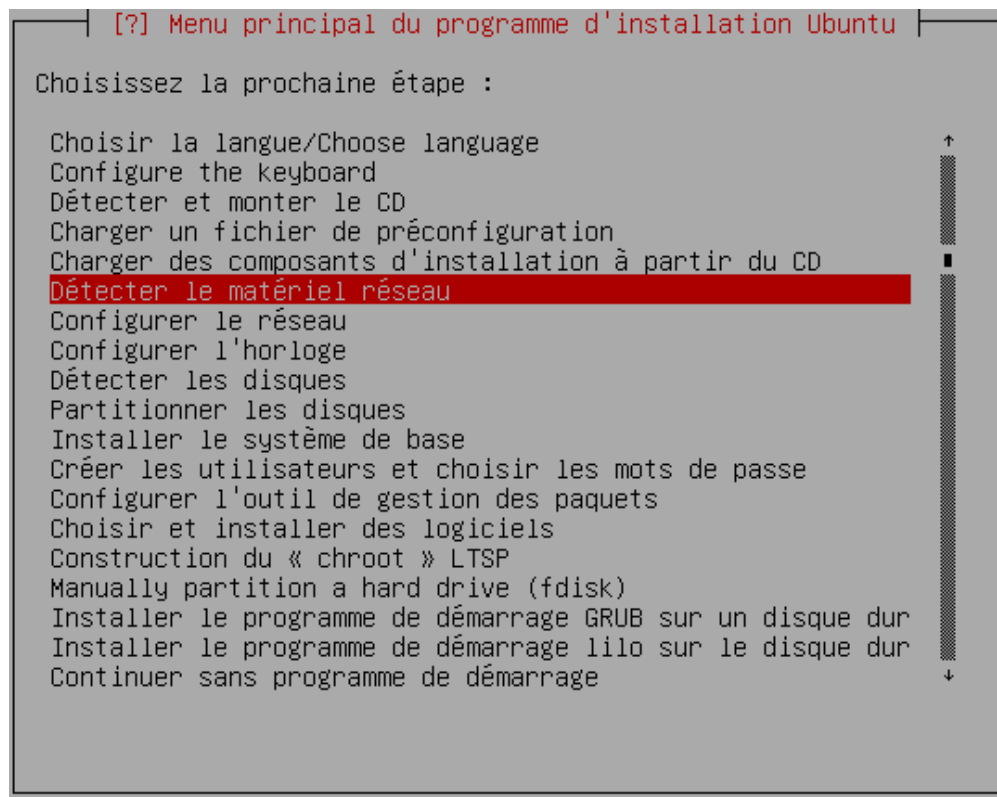
- l'utilitaire `choose-mirror` pour utiliser un miroir (local par exemple),
- l'utilitaire `lvmcfd` en cas de configuration LVM,
- l'utilitaire `mdcfd` en cas de configuration RAID.

L'activation du chargement de l'un ou l'autre de ces composants ajouteront au menu d'installation les lignes **Choisir un miroir de l'archive Ubuntu** et **Configurer les périphériques multi-disque**. Curieusement, le fait de ne pas ajouter les deux derniers utilitaires ne gênera en rien la mise en place du RAID ou de LVM. Leur utilité s'apprécie uniquement lorsque l'on modifie une configuration système déjà existante.

- Il n'est pas nécessaire de charger des composants supplémentaires dans le cadre d'une installation, validez sur **Continuer**.

4. Troisième phase du menu d'installation

Le menu d'installation entre dans sa deuxième phase. Vous noterez l'ajout de plusieurs lignes :



Il faut prendre la structure du menu d'installation comme un enchaînement de tâches interdépendantes, la réalisation d'une tâche étant subordonnée à la précédente. Quelques lignes dans le menu sont cependant optionnelles comme la construction du "chroot" (racine du système emprisonné) LTSP par exemple.

a. Ligne "Détecter le matériel réseau"

La détection recherche le matériel réseau présent dans la machine. Il demande à nouveau le chargement du module USB ainsi que les services de cartes PC car le matériel réseau pourrait être de ce type.

b. Ligne "Configurer le réseau"

Le choix se pose entre une configuration par DHCP (l'adresse IP est donnée par un serveur situé sur le réseau) ou manuellement auquel cas il s'agit de renseigner :

- l'adresse IP *exemple* : 192.168.3.10
- le masque de sous-réseau *exemple* : 255.255.255.0
- la passerelle *exemple* : 192.168.3.1
- le serveur de noms (DNS) *exemple* : suivant votre fournisseur d'accès.

En cas de choix DHCP ou de configuration non obtenue, un sous-menu offre trois choix : la possibilité d'essayer à nouveau (avec ou pas de nom d'hôte DHCP), d'effectuer une configuration manuelle ou de ne pas configurer le réseau.

Un dernier écran demande le nom du système et le domaine DNS associé (localdomain par défaut).

- Entrez le type de configuration adapté à votre situation.

c. Ligne "Configurer l'horloge"

L'horloge système peut être réglée en cas de bonne configuration du réseau, par un serveur de temps, appelé serveur NTP (*Network Time Protocol*). Ensuite l'installateur détecte normalement le fuseau horaire (Europe/Paris en

France).

- Utilisez un serveur NTP si vous le désirez (votre réseau d'entreprise en possède peut-être un propre).

d. Ligne "Détecter les disques"

La détection des périphériques de stockage s'effectue avec là encore les demandes pour USB, les services PC et cartes PCMCIA.

e. Ligne "Partitionner les disques"

Trois cas se distinguent :

- le partitionnement simple (généralement un seul disque)
- l'utilisation RAID logiciel (au minimum deux disques)
- LVM (idem RAID)

Rappel : ces deux derniers cas seront abordés dans le chapitre suivant. Attention : une fois effectué, le partitionnement efface les données présentes sur le (ou les) disque(s) utilisé(s). L'outil **partman** dans le choix **Assisté - utiliser un disque entier** donne trois schémas de partitionnement :

Tout dans une seule partition	Partitions / (~30%), et /home (~67.5%) séparée	Partitions / (~3%), /home (~35%), /usr (~35%), /var (~17.5%) et /tmp (~3%) séparées
-------------------------------	--	---

Dans tous les cas, la partition racine (/) est primaire alors que les autres partitions (même la swap) sont logiques.

- Choisissez et validez la méthode de partitionnement **Manuel**.



La situation de l'exemple se présente sous la forme d'un disque de 8,6 Go avec 512 Mo de RAM. Cette situation est fictive et correspond à l'outil de virtualisation (VMware) utilisé pour la démonstration :

```
| [!!!] Partitionner les disques |
Voici la table des partitions et les points de montage actuellement
configurés. Vous pouvez choisir une partition et modifier ses
caractéristiques (système de fichiers, point de montage, etc.), un
espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Partitionnement assisté
Aide pour le partitionnement

SCSI3 (0,0,0) (sda) - 8.6 GB VMware, VMware Virtual S

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

<Revenir en arrière>
```

Le plan de partition retenu fait état de quatre partitions : la partition d'échanges (swap), la partition racine (/), une partition pour le boot (/boot) et une partition pour les répertoires des utilisateurs (/home).

Pour la partition /boot

- Positionnez-vous sur la ligne concernant le disque, validez puis **accepter en cas de nouveau disque l'écriture d'une nouvelle table de partitions**, type MSDOS.
- Positionnez-vous sur la ligne de la partition marquée comme **espace libre**, validez puis **Créer une nouvelle partition**, taille 100 Mo (pour l'exemple donné).

Attention : la notation anglaise indique GB pour giga bytes ou MB pour mega bytes. En langue française, on note Go et Mo dans le texte **mais pas** pour la configuration.

- Choisissez le type primaire avec un emplacement au début.
- Choisissez comme point de montage /boot dans la liste.
- Validez sur la ligne **Fin du paramétrage de cette partition**.

Voici ce que donne le résultat de ces réglages :

```

[!!!] Partitionner les disques

Vous modifiez la partition n° 1 sur SCSI3 (0,0,0) (sda). Aucun
système de fichiers n'a été détecté sur cette partition.

Caractéristiques de la partition :

Utiliser comme :      système de fichiers journalisé ext3
Point de montage :    /boot
Options de montage :  relatime
Étiquette :           aucune
Blocs réservés :      5%
Utilisation habituelle : standard
Indicateur d'amorçage : absent

Copier les données d'une autre partition
Supprimer la partition
Fin du paramétrage de cette partition

<Revenir en arrière>

```

Note : les partitions restantes seront logiques, la partition étendue sera créée automatiquement à la première partition logique.

Pour la partition swap

- Positionnez-vous sur la ligne de la partition marquée comme **espace libre**, validez puis **Créer une nouvelle partition**, taille 1 Go (GB).

 La taille d'une partition d'échanges se calcule comme suit : le double de la taille RAM installée dans la machine avec un maximum de 2 Go. Exemples : 256 Mo de RAM donne une partition de swap de 512 Mo ; 4 Go de RAM donne une partition de swap de 2 Go.

- Choisissez le type **logique** avec un emplacement au début (c'est-à-dire juste après la fin de la partition précédente).
- Choisissez **espace d'échange (swap)** dans la liste donnée par la ligne **Utiliser comme**.
- Validez sur la ligne **Fin du paramétrage de cette partition**.

Pour la partition /home

- Positionnez-vous sur la ligne de la partition marquée comme **espace libre**, validez puis **Créer une nouvelle partition**, taille 2 Go (GB).
- Choisissez le type **logique** avec toujours un emplacement au début.
- Choisissez comme point de montage **/home** dans la liste.
- Validez sur la ligne **Fin du paramétrage de cette partition**.

Pour la partition /

- Positionnez-vous sur la ligne de la partition marquée comme **espace libre**, validez puis **Créer une nouvelle partition**.
- Validez la taille restante et toujours le type **logique**.
- Validez sur la ligne **Fin du paramétrage de cette partition**.

Le résultat de tout ceci donne l'écran suivant :

```

[!!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement
configurés. Vous pouvez choisir une partition et modifier ses
caractéristiques (système de fichiers, point de montage, etc.), un
espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Partitionnement assisté
Aide pour le partitionnement

SCSI3 (0,0,0) (sda) - 8.6 GB VMware, VMware Virtual S
n° 1 primaire  98.7 MB  f ext3    /boot
n° 5 logique   1.0 GB   f swap   swap
n° 6 logique   2.0 GB   f ext3    /home
n° 7 logique   5.5 GB   f ext3    /

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements
<Revenir en arrière>

```

- Validez sur la ligne **Terminer le partitionnement et appliquer les changements** et confirmez la demande.

f. Ligne "Installer le système de base"

Comme son intitulé l'indique, le système de base s'installe. On peut, en attendant, vérifier que le plan de partitionnement est correct en allant sur la console BusyBox contenant un environnement de commande minimum et par l'utilitaire `fdisk`.

Pour plus de renseignements sur la console BusyBox : <http://www.busybox.net>

- Ouvrez une deuxième console par [Alt][F2] et la touche [Entrée] pour l'activer.
- Listez les commandes en tapant `help`.

Please press Enter to activate this console.

```
BusyBox v1.1.3 (Debian 1:1.1.3-5ubuntu12) Built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

```
~ # help
```

```
Built-in commands:
```

```
_____
. : bg break cd chdir command continue echo eval exec exit export
false fg getopts hash help jobs kill let local pwd read readonly
return set shift times trap true type ulimit umask unset wait
```

```
~ #
```

L'utilitaire `fdisk` va servir à voir le plan de partitionnement :

- Tapez `fdisk /dev/sda`, puis `p` pour afficher la structure des partitions.
- Quittez l'utilitaire par en tapant `q`.

```
~ # fdisk /dev/sda
```

```
The number of cylinders for this disk is set to 1044.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)
```

```
Command (m for help): p
```

```
Disk /dev/sda: 8589 MB, 8589934592 bytes
255 heads, 63 sectors/track, 1044 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0x000ead88
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1		1	12	96358+	83	Linux
/dev/sda2		13	1044	8289540	5	Extended
/dev/sda5		13	134	979933+	82	Linux swap / Solaris
/dev/sda6		135	377	1951866	83	Linux
/dev/sda7		378	1044	5357646	83	Linux

```
Command (m for help): q
```

```
~ #
```

- Revenez sur la console par `[Alt][F1]`.

g. Ligne "Créer les utilisateurs et choisir les mots de passe"

Ubuntu a pour politique de désactiver le compte de l'administrateur, partant du principe que cela contribue à une meilleure sécurité. Cet aspect sera revu dans la gestion des comptes. Concernant une utilisation en serveur, on peut supposer qu'un administrateur correctement formé sait ce qu'il fait.

De plus, la gestion des utilisateurs dans une entreprise fait l'objet, très souvent, d'une recherche sur un serveur

d'annuaire de type LDAP (Linux) ou Active Directory (Windows). Cette option rend inutile la création de comptes utilisateurs séparés de la politique d'authentification de l'entreprise.

- Activez les mots de passe cachés.
- Activez le compte de l'administrateur en autorisant les connexions.
- Indiquez avec son mot de passe et sa vérification.
- Créez éventuellement un utilisateur ordinaire.

h. Ligne "Configurer l'outil de gestion des paquets"

L'utilisation d'un serveur miroir pour une installation de type serveur se base essentiellement sur les mises à jour et non sur les logiciels supplémentaires par rapport au contenu du CD-Rom. Il est aussi plus courant, dans le cadre d'une entreprise, de disposer d'un serveur local. Ce choix se trouve à la ligne "Saisie manuelle" tout en haut de la liste des pays.

Les points abordés sont alors :

- le nom du miroir : le mieux est d'indiquer l'adresse IP au lieu du nom DNS avec le port (optionnel en cas de port 80).
- le répertoire du miroir : par défaut nommé /ubuntu/, à changer si différent.
- le mandataire HTTP (proxy) : à indiquer en cas de présence dans l'entreprise.
- l'utilisation des logiciels à diffusion restreinte (non libres).

À ce stade, la recherche du miroir se fait et un problème est sanctionné par un écran de couleur rouge avec la mention indisponible ou corrompu. La validation sur **Continuer** permet de modifier les renseignements en cas d'erreur de frappe alors que le **Retour en arrière** redonne les possibilités de choix de l'outil de gestion des paquets. La réussite d'une connexion au serveur miroir entraîne la prise en compte des dépôts qu'il contient et déroule en fonction de leur présence une autre série de questions :

- la demande d'utilisation des logiciels à diffusion restreinte (restricted).
 - la demande d'utilisation des logiciels à composante universe.
 - la demande d'utilisation des logiciels à composante multiverse.
 - la demande d'utilisation des logiciels rétro-portés (backports).
- À chaque étape, indiquez vos choix et validez.



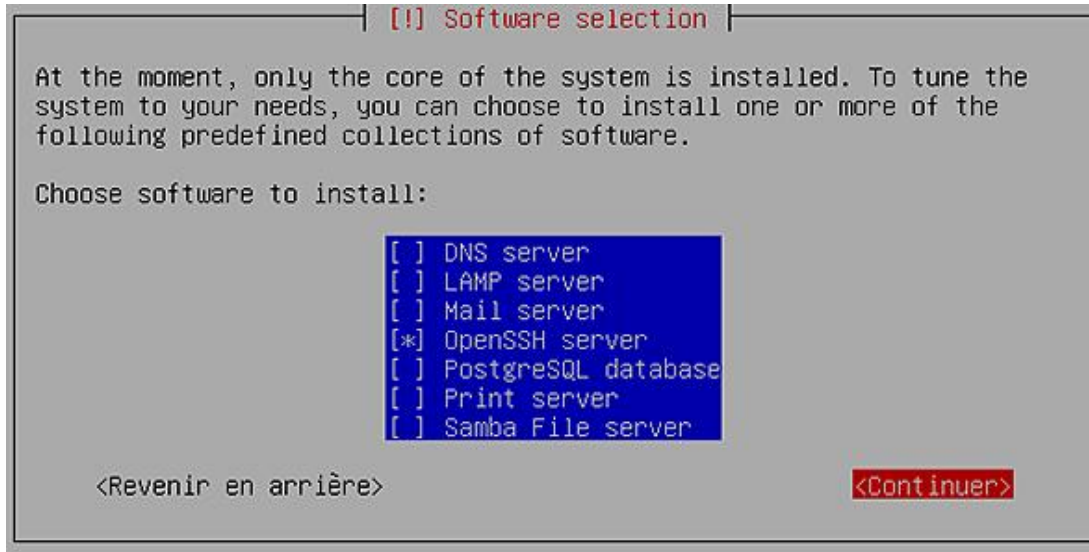
Conseil : validez les choix par défaut, ce qui correspond aux trois premières lignes. L'utilisation des logiciels rétro-portés, sources de conflits et d'erreurs ne s'imposent pas sur un serveur.

i. Ligne "Choisir et installer des logiciels"

L'installateur propose maintenant des "collections" de paquetages logiciels destinées à offrir des fonctionnalités couramment employées sur un serveur d'entreprise :

- serveur DNS ou serveur de noms de domaine avec **Bind**.
- serveur LAMP, acronyme de Linux, **Apache** (serveur Web), **MySQL** (SGBD) et **PHP** (langage de programmation pour HTML).

- serveur de Mails avec le MTA (*Mail Transfer Agent*) **Postfix**.
- serveur **SSH** (*Secure Shell*) pour des connexions distantes sécurisées avec **OpenSSH**.
- serveur **PostgreSQL**, autre serveur de base de données.
- serveur d'impression.
- serveur **SAMBA**, le protocole d'intégration des systèmes Windows avec Linux.



Un des choix indispensables pour un serveur est l'installation du serveur OpenSSH. L'administrateur gère ainsi ses serveurs de façon sécurisée centralisée à partir d'un autre système.

- Choisissez les logiciels désirés et validez.

j. Ligne "Installer le programme de démarrage GRUB sur un disque dur"



On passe les deux lignes concernant la construction du "chroot" LTSP (client de serveur léger) et le formatage manuel par `fdisk`.

En mode expert (et uniquement dans ce cas), le choix vous est laissé entre l'installation de GRUB ou LILO, sur le secteur d'amorçage principal (MBR) et le secteur d'amorçage (`boot`) du disque.

- Choisissez le chargeur d'amorçage, de préférence GRUB sur le MBR.

Pour GRUB, un mot de passe au démarrage interdit toute utilisation de la ligne de commande du chargeur ou une modification des entrées du menu. Cette fonctionnalité semble peu intéressante car facilement évitable. En matière de sécurité, la politique à adopter doit porter sur d'autres points : voir pour cela le chapitre sur la sécurité en fin d'ouvrage.

Pour éviter une prise de contrôle au démarrage, le confinement physique du serveur s'impose avec filtrage des accès. On peut mettre toutes les sécurités connues sur un serveur, elles ne résistent pas si une personne mal intentionnée a accès au matériel.

k. Ligne "Terminer l'installation"

Cette dernière ligne, avant de terminer réellement l'installation, précise le réglage de l'horloge système. Tout serveur Linux se règle normalement sur l'heure universelle (UTC ou heure de Greenwich) afin d'être harmonisé avec les serveurs du monde entier. Le système prend ensuite en compte le fuseau horaire du pays (GMT + 1 pour Paris) et ajuste aussi en fonction de l'heure d'été (GMT +2). L'heure système indiquée dans le BIOS de la machine désigne donc impérativement l'heure UTC.



Un petit distinguo : les systèmes Windows, à la différence de Linux, demandent que l'horloge CMOS (horloge système dans le BIOS) soit réglée sur l'heure locale avec donc la prise en compte du fuseau horaire. En cas de cohabitation des deux systèmes, changez le réglage sous Linux (plus accommodant...).

- Indiquez le réglage de l'heure en UTC et validez la fin de l'installation après avoir retiré le CD-Rom de la distribution.

Le système redémarre, l'écran est en mode texte car il n'y a pas eu d'installation de serveur graphique.

Vous êtes normalement prêt à ouvrir une session en administrateur (`root`).

Installations particulières d'un poste de travail

Parallèlement à l'installation normale où le système Ubuntu occupe seul l'espace disque de l'ordinateur, deux variantes d'installations existent :

- l'une moderne, mêlant intimement le système Windows à Ubuntu ;
- l'autre classique, s'appuyant sur le chargeur de démarrage de Linux et pouvant prendre en charge deux systèmes d'exploitation ou plus (plus de deux étant parfois un peu lourd), quels qu'ils soient.

1. Avec Windows sous la forme d'une application

Mark Shuttleworth décrit lui-même l'intérêt de faire tourner une distribution Ubuntu sur Windows : il faut montrer la puissance des logiciels libres sur cette plate-forme incontournable au niveau mondial. En quelque sorte, sa démarche s'apparente à faire entrer le loup dans la bergerie.



Le projet sur MacOS existe mais se trouve encore à l'état de développement (à la rédaction de ces lignes) et se nomme **Mubi**. Le projet **Lubi**, lui, se charge des plates-formes Linux car l'envie d'essayer la distribution Ubuntu sur une autre distribution est aussi naturelle. Mais là, cela s'appelle de la concurrence ou plutôt, dans un univers non commercial, de la sainte émulation.

Existant depuis la version 7.04 Feisty Fawn, le programme **Wubi** apparaît sur les CD-Rom de la version desktop (et ses variantes) 8.04 Hardy Heron. Officiellement supporté par la distribution, le projet fut initié et toujours maintenu par Agostino Russo.

Deux sites Internet décrivent le projet :

<http://wubi-installer.org>

Le site du projet

<https://launchpad.net/~ago>

Le profil d'Agostino Russo

a. Principes de fonctionnement

Wubi installe la distribution Ubuntu de la même façon qu'une application. Ce programme peut donc être désinstallé facilement car il ne modifie en aucune façon les partitions existantes. Il utilise un fichier virtuel comme les logiciels de virtualisation de type **VMware** ou **VirtualBox**, mais la comparaison s'arrête là car :

- Wubi utilise le chargeur de démarrage (*boot manager*) de Windows, où l'on décide d'utiliser l'un ou l'autre de façon exclusive.
- Les pilotes s'appuient sur le matériel de l'ordinateur et ne sont pas émulés (on peut donc par exemple avoir les effets 3D de Compiz Fusion).
- Le disque dur avec ses partitions sont ceux de Windows comme le montre l'utilitaire `fdisk` et il n'y a pas de partition swap.
- Le répertoire `/host` à la racine contient l'arborescence (accessible) de la partition Windows où Wubi a installé Ubuntu.
- Le système de fichiers de type NTFS et non ext3FS est monté sur `/host/ubuntu/disks/root.disk`.

Tout se passe comme une installation en *dual-boot* (double amorçage) avec cette différence que le système est contenu dans un fichier et non dans une partition. Un utilitaire nommé **LPVM** permettra de transférer ce fichier virtuel dans une partition dédiée (non disponible actuellement sur la 8.04).

b. Conditions de ressources

Wubi tourne sur les plates-formes Windows 98, 2000, XP et Vista. Il requiert pour fonctionner au minimum :

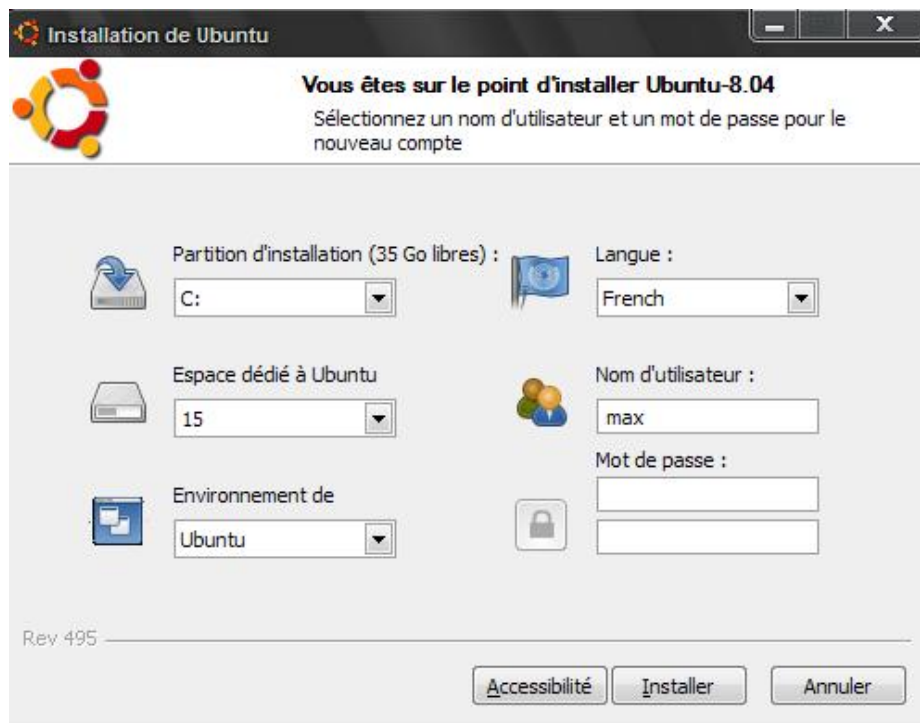
- 256 Mo de mémoire
- 5 Go d'espace disque
- 1 GHz pour le processeur

c. Processus d'installation

L'insertion du CD-Rom de la distribution version desktop à partir d'une plate-forme Windows fait démarrer automatiquement le menu d'installation (umenu.exe) :



Le premier choix concerne l'utilisation du CD-Rom en LIVE et nécessite un redémarrage. Il est préférable d'utiliser le CD-Rom car Wubi reconnaît de façon automatique comme support d'installation ce média. L'utilisation solitaire de Wubi entraîne un téléchargement à partir d'un serveur miroir par Internet. Le second choix lance Wubi (wubi.exe) et affiche le seul écran de personnalisation :



À ce stade, vous pouvez choisir :

- la partition d'installation (C ou une autre)
- l'espace dédié à la distribution
- la langue (par défaut celle du système Windows)
- le nom de l'utilisateur (par défaut celui de la session Windows)
- le mot de passe et sa vérification.

Un bouton **Accessibilité** propose la modification des paramètres de visibilité et de mobilité. Ubuntu, dans son esprit communautaire, pense toujours aux personnes à handicap. Le bouton **Installer** démarre l'installation ou plutôt prépare l'installation car celle-ci ne sera effective qu'au cours d'une deuxième phase. Une fois terminée, le CD-Rom est éjecté et une demande de redémarrage s'affiche.

Le fichier boot.ini (fichier caché) de Windows est modifié et la section [operating systems] comporte un système d'exploitation supplémentaire. En voici un exemple à partir d'un système Windows XP, édition Media Center :

```
[boot loader]
timeout=15
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows XP Media Center
Edition" /fastdetect /NoExecute=OptIn /noguiboot
c:\wubldr.mbr="Ubuntu"
```

Le choix de la ligne Ubuntu conduit à un menu GRUB d'installation de la distribution. L'utilitaire **Grub4Dos** propose alors une installation normale et des variantes :

- en mode graphique sans échec
- des solutions de contournements
- en mode détaillée
- en LiveCD

Le choix de l'installation normale conduit à une distribution Ubuntu classique en poste de travail, bureau GNOME (pour la version de base).

d. Pourquoi utiliser Wubi ?

Comme dans toutes formes d'implantation de système, des avantages et des inconvénients se dégagent.

Avantages

- La distribution sous forme d'application avec une gestion facile et non "traumatisante" pour l'utilisateur.
- Des fonctionnalités complètes comme le bureau 3D pour apprécier pleinement la distribution.
- La possibilité de sauvegarder des données personnelles dans un espace de travail mixte.

Inconvénients

- Des performances réduites : pas de mémoire d'échanges (swap), un support sur un système de fichiers NTFS et donc soumis à fragmentation.
- La dépendance vis-à-vis de Windows, comme dans le cas de la virtualisation, une panne du système principal (système hôte) entraîne une panne de Ubuntu.

En résumé, il existe une place pour une implantation de ce type et elle dépasse la notion de test du système plutôt réservée à une distribution LIVECD. Un utilisateur désireux de s'initier rapidement à Linux mais travaillant pour la plupart du temps sous Windows trouvera un cadre adapté à son cas. Une utilisation plus professionnelle demande à ce que les systèmes soient distinctement séparés, ce qui est présenté maintenant dans le paragraphe suivant.

2. Avec un autre système en "dual boot"

Dans cette situation, deux systèmes d'exploitation sont installés sur un ordinateur de façon indépendante, le démarrage de l'un ou de l'autre s'effectuant par un choix du chargeur de démarrage. En fonctionnement, l'un ou l'autre des systèmes possède toutes les ressources de la machine.

Première démarche de mixité de plusieurs systèmes, essentiellement entre Linux et Windows ce type d'implantation pose des difficultés sur :

- Le schéma de partitionnement entre partitions Linux et partitions Windows.
- Le chargeur de démarrage, son choix et sa configuration (classiquement GRUB).

Le premier point fait état de la limitation à quatre partitions principales de la table du MBR. Le second ajoute une "brique" logicielle supplémentaire rendant plus complexe le lancement des systèmes.



Ce type d'implantation correspond à une utilisation en poste de travail. Un serveur en situation professionnelle ne s'éteint jamais... donc pas de double démarrage ! Si vous avez un serveur Windows et l'obligation d'offrir aussi les services d'un serveur Linux, utilisez une machine virtuelle.

a. Avant l'implantation

Deux cas de figures seront vus :

- Le schéma de partitionnement actuel de l'ordinateur ne comporte aucun espace ou partition susceptible d'être utilisé pour Ubuntu.
- Un espace libre est disponible et suffisant (ou vous ajoutez un autre disque).

Sans utilitaire de gestion de partitions, point de salut ! Autrefois parent pauvre dans cette catégorie, le monde

OpenSource dispose maintenant d'un logiciel tout à fait au point : **GParted**.

L'utilitaire GParted

Basé sur le célèbre **PartitionMagic** et appartenant maintenant à la société Norton Symantec, GParted "clone" avec une interface en GTK (bibliothèque logicielle) cet outil de partitionnement. Il se trouve installé sur la version desktop d'Ubuntu et pour y accéder, il suffit de démarrer la station de travail avec le CD-Rom en live.

Voici l'adresse du site Internet de GParted : <http://gparted.sourceforge.net/>

b. Situation n°1 : aucun espace libre

L'exemple suivant traite d'une installation sur un disque dur de 8 Go entièrement occupé en NTFS par Windows XP version Professionnel. Un conseil : lors de l'installation, une option donne la possibilité de créer les partitions nécessaires directement au moment du partitionnement (on parlera de partitionnement "à la volée"). Ne la choisissez pas : il est préférable d'effectuer ces étapes en **deux fois** afin de s'éviter quelques complications.

Pré-requis : le CD-Rom de la version desktop, un système Windows installé sur la totalité du disque, sur une partition (plusieurs partitions utilisées ne changent rien à la démarche, elles la compliquent simplement) avec un taux d'occupation du disque par Windows inférieur à 50 % (dans l'exemple, on partage le disque en deux).

- Démarrez le système avec le CD-Rom Ubuntu en **situation live d'essai** (première ligne).

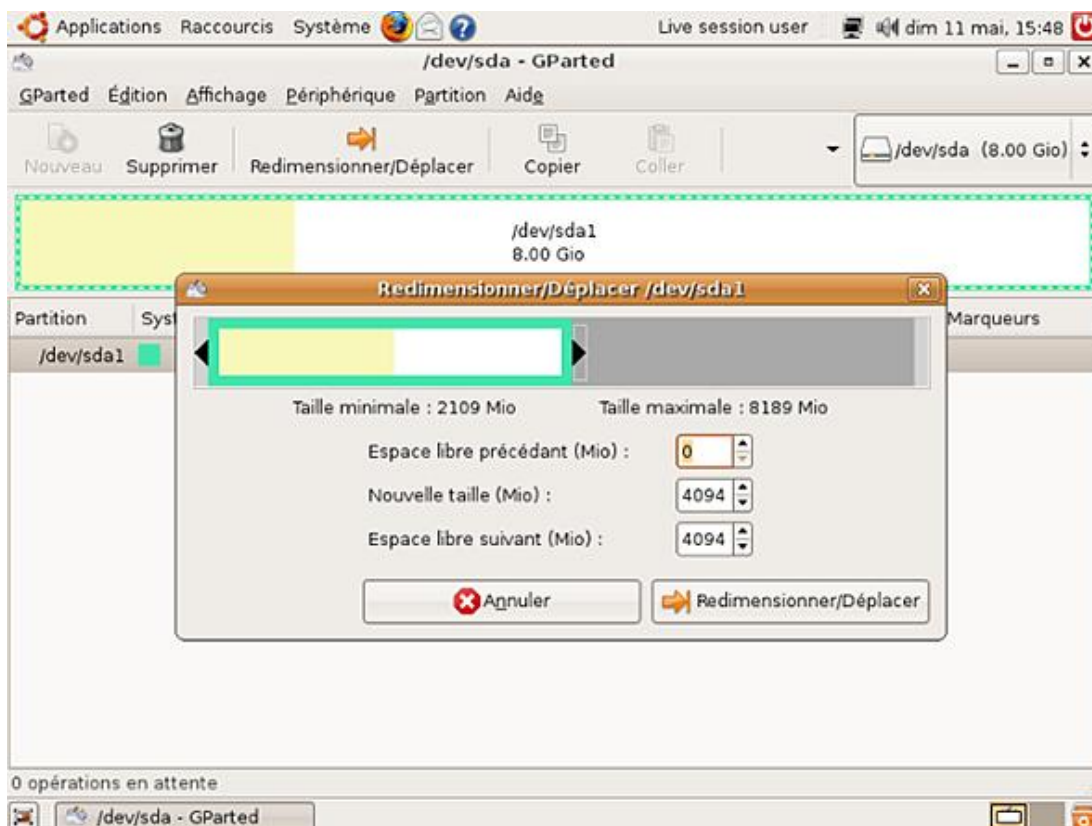
Le système une fois lancé, montre comme vu dans un chapitre précédent, le bureau GNOME.

- Lancez l'utilitaire GParted par les menus **Système - Administration - Éditeur de partition**.

Au lancement du logiciel, la bande représente votre disque dur. Il montre le découpage en partition et présente normalement une occupation totale du disque.

- Cliquez par le bouton droit de la souris sur cette bande et choisissez l'option **Redimensionner/Déplacer**.
- Redimensionnez par le curseur la partition initiale à la taille voulue.
- Validez votre action par le bouton **Redimensionner/Déplacer**.

L'exemple ci-dessous montre un redimensionnement à la moitié d'un disque d'une taille initiale de 8 Go :



L'ordre est donné mais non réalisé. À ce stade, la structure des partitions est encore intacte et modifiable.

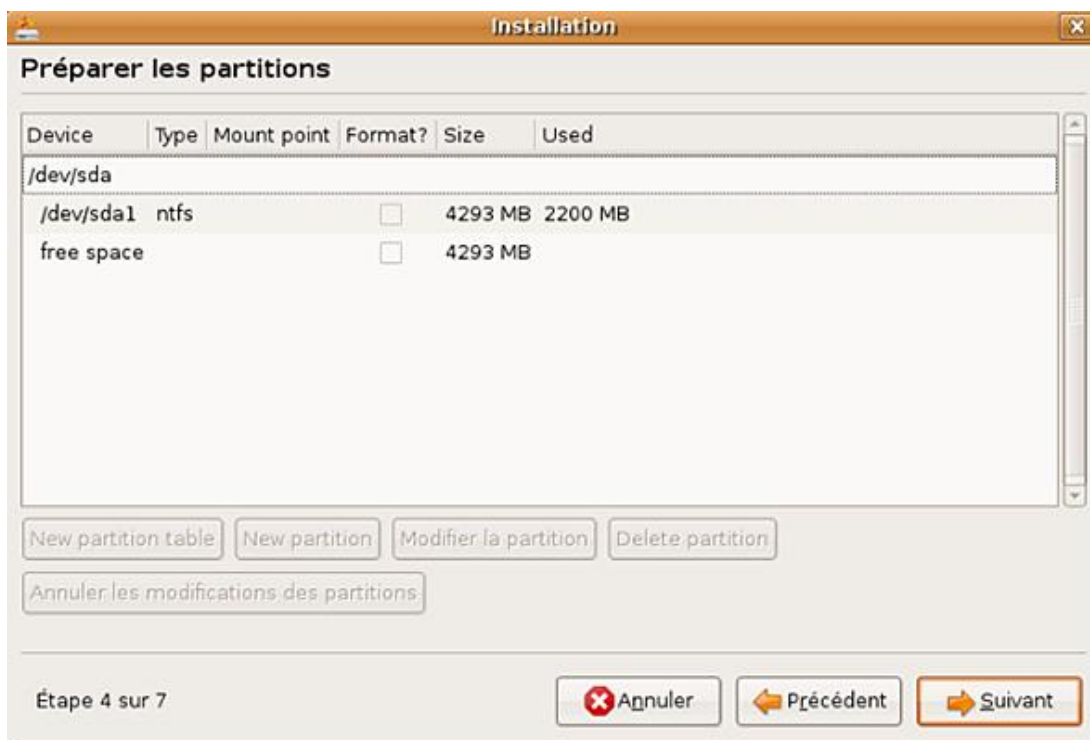
- Par le menu **Édition**, ligne **Appliquer toutes les opérations**, entérinez votre demande puis confirmez.

L'espace disque se modifie en laissant la place pour la distribution Ubuntu (structure minimale : une partition swap et la partition racine).

Vous entrez maintenant dans le cas de la situation n°2.

c. Situation n°2 : un espace libre existant

C'est la suite logique de la manipulation précédente. Le démarrage classique de l'installation peut alors commencer. Un changement important : dans ce type de manipulation vous devez choisir obligatoirement un **partitionnement manuel**. Voici, pour rappel, l'écran de préparation du partitionnement lors d'une installation en poste de travail :



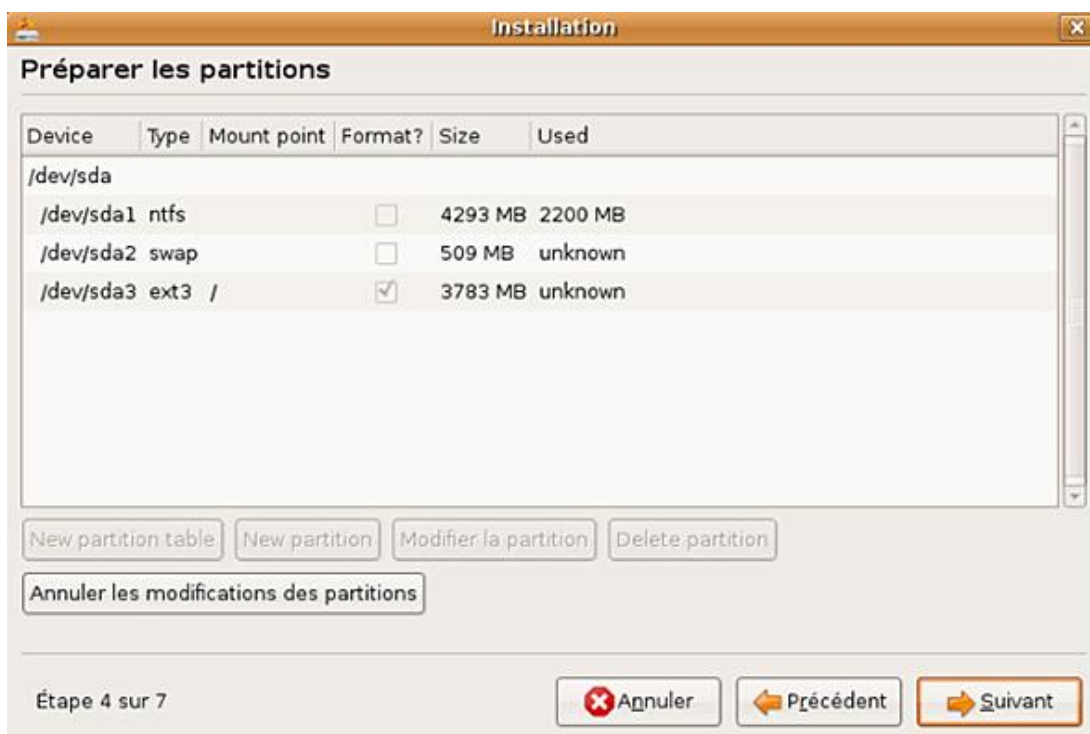
Le schéma de partition simple comprend une partition d'échanges (swap) et la partition du système :

- Partition swap de 512 Mo en primaire, emplacement au début.
- Partition / du reste en primaire, emplacement au début, **ext3FS**.

Une fois positionné sur la ligne de l'espace libre :

- Cliquez sur **New partition**, créez la partition swap, répétez l'opération pour la partition système.

Soit le résultat ci-après :



L'installation se déroule ensuite normalement avec cependant encore un écran supplémentaire par rapport à une

installation normale : la demande d'importation des documents et paramètres d'un ou des utilisateurs du système Windows. Le programme d'installation détecte en effet le deuxième système et est capable d'en importer les environnements (profils : arrière-plan du bureau, etc.).

- Suivant votre désir, cochez ou non la (ou les) case(s) des comptes du système Windows.

d. Démarrage et échanges entre les systèmes

Le chargeur de démarrage GRUB propose une série de choix au démarrage, avec la première ligne comme choix par défaut en surbrillance :

```
Ubuntu 8.04.1, kernel 2.6.24-19-generic
Ubuntu 8.04.1, kernel 2.6.24-19-generic (recovery mode)
Ubuntu 8.04.1, memtest86+
Other operating systems:
Windows XP Professionnel
```

La première ligne démarre Ubuntu alors que la dernière lance le système Windows. Les autres lignes servent respectivement :

- Au lancement de Ubuntu en mode récupération (différent du mode sans échec).
- Au test de la mémoire vive installée sur la machine.
- À définir une séparation entre les systèmes (ne lance rien).

Note : les options du fichier de configuration GRUB sont expliquées dans le chapitre Prise en main de la distribution.



Le mode de récupération offre les fonctionnalités de récupération des paquetages logiciels "cassés", de réparation du serveur graphique, du lancement d'une console en mode administrateur (sans demande de mot de passe) et bien sûr de revenir à un démarrage normal.

Échanges Ubuntu/Windows

L'indépendance des deux systèmes dans la forme n'empêche pas l'échange d'informations. Cette fonctionnalité n'est valable que dans un seul sens, car si maintenant Ubuntu lit et écrit sur des partitions NTFS (type Windows XP, Vista ; les partitions Fat et Fat 32 ne posaient aucun problème), l'inverse n'est toujours pas d'actualité...

La partition NTFS est accessible à partir du bureau Ubuntu. Dans l'exemple, cela se caractérise par la présence d'un lecteur de disque dans **Raccourcis/Poste de travail** intitulé **Média 4,3 Gio** :



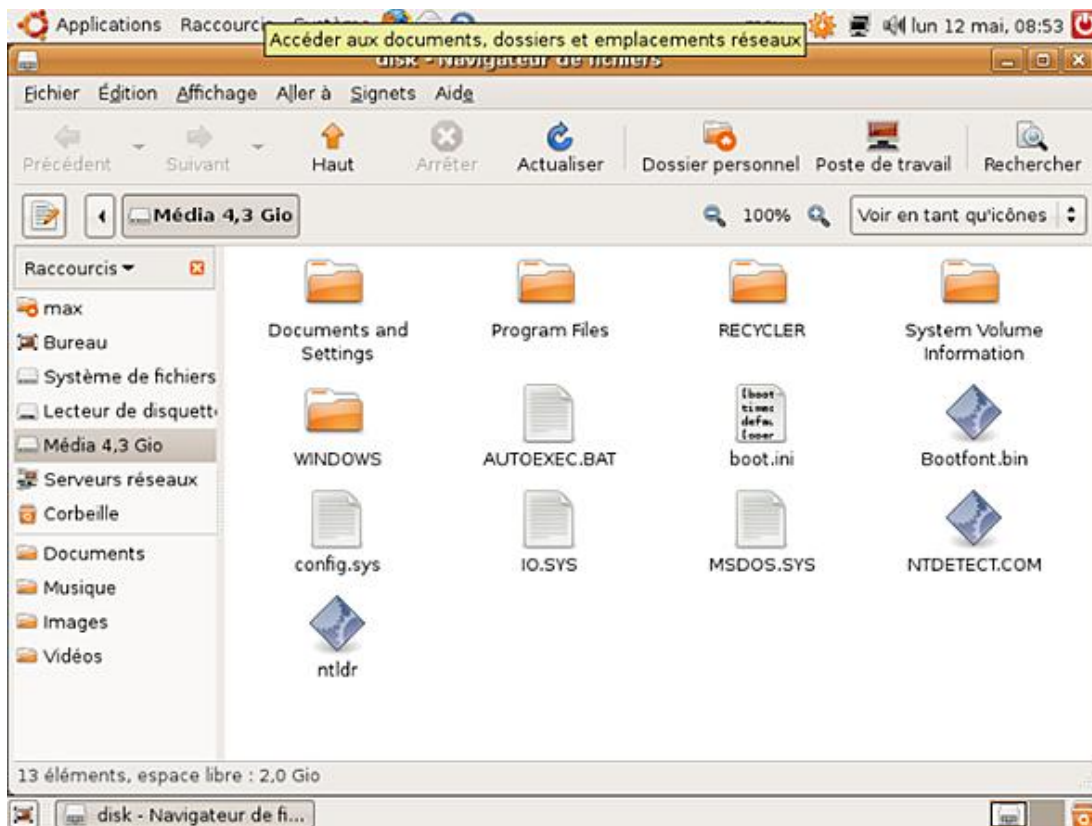
L'accès pour celui-ci nécessite un montage :

- Cliquez avec le bouton droit de la souris sur **Média 4,3 Gio** (ou une appellation différente suivant votre configuration).
- Entrez le mot de passe de l'utilisateur principal.
- Fermez le poste de travail.

L'icône du **Média 4,3 Gio** apparaît sur le Bureau et un double clic de la souris en affiche le contenu.



Vous avez accès à TOUT ! Fichiers et répertoires systèmes cachés de Windows (*System Volume Information*, *Recycler*, etc.) comme le montre l'image ci-dessous. Attention donc à ne pas effacer des éléments essentiels, d'autant plus que le passage à la corbeille se révèle impossible.



La lecture et l'écriture sur une partition NTFS à partir de Linux est désormais du passé. Sur Ubuntu Hardy Heron, le paquet logiciel **ntfs-3g** en version 1.2216 en licence GPL fonctionne avec **FUSE**, une bibliothèque d'implémentation d'un système de fichiers.

Adresse du site Internet du projet **ntfs-3g** : <http://www.ntfs-3g.org>

Le point sur FUSE

FUSE (*Filesystem in Userspace*) apporte une API (bibliothèque) pour l'implémentation simple et sécurisée d'un système de fichiers par un utilisateur. La démarche Debian/Ubuntu qui consiste à reporter sur un "super-utilisateur" les tâches de l'administrateur complique le montage d'un système de fichiers existant. En effet, pour faire traditionnellement cette opération sur un système Linux, il faut :

- soit être administrateur (le root) ;
- soit disposer d'un point de montage dans le fichier `/etc/fstab`.

Beaucoup de systèmes de fichiers (média, réseau, etc.) doivent aussi pouvoir être montés par un utilisateur classique. Ubuntu utilise pour FUSE les paquets logiciels :

- `gvfs-fuse`, le serveur
- `libfuse2`, la bibliothèque
- `fuse-utils`, les utilitaires

FUSE est chargé comme module pour le noyau : on le voit par sa présence dans le fichier `/etc/modules` (intégré par défaut sur Ubuntu Hardy Heron). L'appartenance au groupe **fuse** (`/etc/group`) accorde la possibilité de montage, on peut le vérifier avec la commande `id`.

Affichage des groupes de l'utilisateur privilégié de nom **max** :

```
id
uid=1000(max), gid=1000(max), groupes=4(adm),
20(dialout), 24(cdrom), 25(floppy), 29(audio), 30(dip),
44(video), 46(plugdev), 107(fuse), 109(lpadmin),
115(admin), 1000(max)
```



Attention : le montage des périphériques USB correspond à une autre logique : celle des droits de l'administrateur à rattacher au système de fichiers existant un autre système externe (au lieu d'interne). Ce point sera revu dans le chapitre sur les droits des utilisateurs, car même avec FUSE, la gestion de tâches se gère par la nouvelle bibliothèque **PolicyKit** sur Ubuntu.

e. Pourquoi disposer d'un double système d'exploitation ?

À la différence de l'installation avec Wubi, l'utilisateur dispose d'une version Ubuntu pleine et entière. Cette implantation plus lourde que la précédente dépasse une situation de test et se réserve aux utilisateurs confirmés n'ayant pas peur de modifier la structure de partitions. Une autre réserve concerne l'espace disque qui doit être suffisamment conséquent pour les deux systèmes d'exploitation.

3. Supplément : avec Windows en machine virtuelle Jeos

La variante **Jeos** (on prononce "Juice") dérive d'une version serveur pour une installation avec un logiciel de virtualisation. Cette nouveauté n'est pas anodine car le marché de la virtualisation en entreprise prend de l'ampleur :

- Elle réduit les coûts des infrastructures par la baisse physique des équipements et de leur maintenance.
- Elle augmente la productivité par la mise en place facile de plates-formes de test dans le cas de développement d'applications.

La société VMware et sa suite Infrastructure (ESX, VirtualCenter, Backup, etc.) obtient les meilleures parts de marché par rapport à Virtual Server de Microsoft. Il était donc naturel que Jeos s'appuie sur cette technologie.

a. Principes de fonctionnement

Le principe de base a été de retirer du noyau tous les éléments inutiles comme les pilotes de périphériques afin d'obtenir une empreinte légère (inférieure à 300 Mo installée) tant au niveau de la taille du système (l'image ISO jeos-8.04.1-jeos-i386.iso ne fait d'ailleurs qu'une centaine de Mo) qu'en mémoire à l'exécution. Comme pour toute distribution serveur et pour obtenir des résultats de cette taille, il n'y a pas d'environnement graphique d'installer. Le résultat donne de meilleures performances qu'avec une distribution non Jeos.

Caractéristiques

- l'adresse de téléchargement : <http://cdimage.ubuntu.com/jeos/>
- processeurs : Intel ou AMD en architecture x86
- mémoire minimum requise : 128 Mo
- noyau (Hardy) : 2.6.24-16-virtual

b. Différences d'installation

Les différences se mesurent surtout lors de la création de la machine virtuelle où il faut respecter les points suivants :

- Pour la préparation de la machine virtuelle : un choix en configuration "*custom*" afin de pouvoir choisir le type IDE pour le disque VMware.
- Au cours de l'installation : une configuration réseau manuelle et non par DHCP.

c. Intérêt de Jeos

Bien que version serveur, Jeos est placé dans la partie déclinaison d'implantation d'un poste de travail. Pourquoi ? Parce que sa destination fonctionnelle (serveur de test, DNS, de dépôts logiciels, etc.) range son utilisation dans un côté applicatif, surtout si le serveur hôte appartient au système d'exploitation Windows.

Au final, l'intérêt de Jeos rejoint, comme indiqué précédemment, celui de l'utilisation de machine virtuelle.

Installations particulières d'un serveur

Note : toutes les manipulations présentées dans ce paragraphe le sont :

- avec une version de type serveur
- en mode expert
- à l'installation (il est illogique et plutôt "amateur" de réaliser ce genre de manipulations sur un système existant).

Pour des raisons de test, l'outil de virtualisation VMware est utilisé.

1. Avec un système de disques RAID

La recherche d'une tolérance de pannes conduit à l'utilisation de la technologie **RAID**. Ubuntu supporte le RAID logiciel (pilote **md** pour *Multiple Devices*) dans ces deux formes les plus utilisées :

- **RAID 1** ou disques en "miroir", l'écriture sur un disque s'effectue de la même façon en parallèle sur un autre disque de même taille, qui peut ainsi suppléer le premier en cas de panne.
- **RAID 5** ou disques en bandes avec parité, l'écriture se décompose en morceaux uniformes et s'effectue sur plusieurs disques. Une part de chaque disque est réservée à un espace de contrôle. En cas de panne d'un disque, les données sont recrées à l'aide des espaces de contrôle des autres disques comme une empreinte "en négatif". Là aussi, dans un souci d'uniformisation et de pleine capacité, il vaut mieux utiliser des disques identiques.

L'utilisation de l'une ou l'autre des formules correspond au degré de sécurité attendu. Pour des données non sensibles, une simple sauvegarde automatisée journalière sur un support différent suffit. Pour des données plus sensibles, RAID 1 a pour avantage la simplicité et pour inconvénient un coût plus élevé car la capacité réelle de stockage est divisée par 2. RAID 5 apporte une sécurité plus élevée, le nombre de supports divise le risque de pannes, et ce avec une bonne performance dans la lecture/écriture des données. Utilisable à partir de trois disques au moins car l'espace utile se calcule comme étant égal à $n-1$ disques, un nombre élevé de disques rentabilise le procédé mais le rend aussi plus cher.

a. Partitionnement en RAID 1

Après le démarrage de l'installation, le point de départ se situe à l'écran de partitionnement des disques avec un **choix manuel**. La situation de l'exemple se présente sous la forme de deux disques de 8.6 Go chacun. Comme il est inutile de cloner la partition d'échanges, la structure sera la suivante :

- disque 1 : partition swap 512 Mo, partition en RAID 1 du reste
- disque 2 : partition swap 512 Mo, partition en RAID 1 du reste

La RAM du serveur s'élève à 512 Mo, compte tenu des règles, le total de la swap est bien de 1 Go, réparti sur les deux disques. Ainsi, non seulement on atteint notre objectif, mais on définit bien deux partitions RAID équivalentes pour la mise en miroir.

Pour le disque n°1, partition swap :

- Positionnez-vous sur la ligne concernant le disque, validez, acceptez en cas de nouveau disque l'écriture d'une nouvelle table de partitions, type MSDOS.
- Positionnez-vous sur la ligne de la partition marquée comme espace libre, validez puis **Créer une nouvelle partition**, taille 512 Mo.
- Choisissez un type primaire pour la partition avec un emplacement au début.

- Dans le choix **Utiliser comme**, validez et choisir l'espace d'échange "swap".
- Terminez par une validation sur **Fin du paramétrage de cette partition**.

Pour le disque n°1, partition RAID :

- Positionnez-vous sur la ligne de la partition marquée comme espace libre, validez, choisissez **Créer une nouvelle partition**, acceptez la taille par défaut (le reste du disque soit 8.1 Go) et toujours de type primaire.
- Choisissez l'utilisation comme système de fichiers **volume physique pour RAID**.
- Important : validez la ligne **Indicateur d'amorçage** pour y mettre la valeur **présent**.
- Terminez par une validation sur **Fin du paramétrage de cette partition**.

Pour le disque n°2, partition swap et RAID :

- Effectuez les mêmes manipulations que pour le disque 1.

Voici le résultat à obtenir :

```

| [!!!] Partitionner les disques |
Voici la table des partitions et les points de montage actuellement
configurés. Vous pouvez choisir une partition et modifier ses
caractéristiques (système de fichiers, point de montage, etc.), un
espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Configurer le RAID logiciel
Partitionnement assisté
Aide pour le partitionnement

SCSI3 (0,0,0) (sda) - 8.6 GB VMware, VMware Virtual S
n° 1 primaire 509.9 MB f swap swap
n° 2 primaire 8.1 GB B K raid
SCSI3 (0,1,0) (sdb) - 8.6 GB VMware, VMware Virtual S
n° 1 primaire 509.9 MB f swap swap
n° 2 primaire 8.1 GB B K raid

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

<Revenir en arrière>

```

- Validez sur **Configurer le RAID logiciel**, accepter la demande d'application pour les changements et la configuration RAID.

Un menu supplémentaire apparaît afin de déterminer quelle structure à appliquer au volume RAID.

- Choisissez l'option **Créer un périphérique multidisque**.
- Choisissez le type **RAID1** pour la mise en miroir.
- Validez la valeur par défaut (soit 2) concernant le nombre de périphériques actifs pour l'ensemble RAID1, avec 0 comme périphérique de réserve.

Avec une demande en RAID1, la proposition concerne la partition sda2 du premier disque et la partition sdb2 du

deuxième disque :



- Cochez les périphériques /dev/sda2 et /dev/sdb2, validez.
- De retour sur la configuration des périphériques multidisque, validez par **Terminer**.

Une nouvelle ligne concernant le périphérique RAID1 n°0 apparaît. Il suffit maintenant d'y créer la partition du système.

- Validez sur la ligne n°1 du périphérique RAID1 n°0.
- Créez la partition / en ext3.

Le résultat final de tout ceci donne comme écran :



La fin de l'installation se déroule conformément à celle d'un serveur simple.

b. Maintenance

Le système de fichiers se trouve sur le périphérique /dev/md0 (on le vérifie par la commande df). La commande mdadm offre l'ensemble des opérations nécessaires à la gestion du RAID (création, modification, information). Elle se trouve aussi lancée au démarrage sous la forme d'un service afin de superviser (mode monitor) les périphériques RAID.

Le propre d'un système RAID est de se faire oublier... jusqu'à la panne. De même, la création d'un système RAID sur un système existant n'est pas courante. Un bon administrateur pense et gère, avant l'installation, la structure de partitions de son serveur. Aussi, on emploie la commande mdadm d'abord pour obtenir des informations :

- Tapez la commande mdadm --detail /dev/md0

```
root@demo:~# mdadm --detail /dev/md0
/dev/md0:
    Version : 00.90.03
  Creation Time : Wed May 14 10:04:24 2008
    Raid Level : raid1
    Array Size : 7887808 (7.52 GiB 8.08 GB)
  Used Dev Size : 7887808 (7.52 GiB 8.08 GB)
    Raid Devices : 2
    Total Devices : 2
 Preferred Minor : 0
 Persistence : Superblock is persistent

    Update Time : Wed May 14 08:26:17 2008
      State : clean
 Active Devices : 2
Working Devices : 2
 Failed Devices : 0
 Spare Devices : 0

    UUID : 3aee75d2:d55e0b27:d77ac47e:9b4c343c
    Events : 0.4

   Number Major Minor RaidDevice State
        0     8      2        0     active sync  /dev/sda2
        1     8     18        1     active sync  /dev/sdb2
root@demo:~#
```

L'information "Persistence" indique le bloc présent sur chaque disque contenant la description du RAID pour le noyau. L'état d'activation des disques est montré avec la bonne synchronisation des deux disques (autre possibilité concernant le bon fonctionnement avec cat /proc/mdstat). Le fichier de configuration /etc/mdadm/mdadm.conf, quant à lui, décrit cette structure RAID.

L'essentiel du travail de l'administrateur dans le cadre du RAID consiste à réparer une situation bloquée et pour en voir le détail, il faut provoquer une panne.

Simulation de panne n°1 sur le deuxième disque

Cette panne peut être simulée de façon logicielle par la commande mdadm.

- Tapez mdadm /dev/md0 --fail /dev/sdb2 --remove /dev/sdb2

Le retour indique une mise en défaut de /dev/sdb2 (faulty) et son retrait de /dev/md0. La confirmation en est donnée toujours par cat /proc/mdstat où l'on voit le deuxième absent (2/1 [U_] au lieu de 2/2 [UU]). Pour remettre le miroir en route :

- Tapez mdadm /dev/md0 --add /dev/sdb2
- Visualisation de la progression par cat /proc/mdstat


```

root@deno:~# cat /proc/mdstat
Personalities : [linear] [multipath] [raid0] [raid1] [raid6] [raid5] [raid4] [raid10]
md0 : active raid1 sdb2[2] sda2[0]
      7887808 blocks [2/1] [U_]
      [==>.....] recovery = 12.4% (985984/7887808) finish=1.9min speed=57999K/sec

unused devices: <none>
root@deno:~#

```

Simulation de panne n°2 sur le premier disque

Cette panne plus violente consiste à débrancher carrément le premier disque. Avant d'effectuer cette opération, l'administrateur pré-positionne la configuration de GRUB de manière à ce que le système puisse démarrer à partir du deuxième disque (c'est l'explication du paramètre présent dans l'indicateur d'amorçage au moment de l'installation).

- Tapez la commande `grub-install hd1`

Le menu de démarrage `/boot/grub/menu.lst` comporte une section supplémentaire pour la deuxième partition du deuxième disque à rajouter à la fin :

```

title      Ubuntu 8.04, kernel 2.6.24-16-server
root       (hd1,1)
kernel     /boot/vmlinuz-2.6.24-16-server root=/dev/md0 ro
initrd     /boot/initrd.img-2.6.24-16-server
quiet

```

Cette entrée du menu peut être sélectionnée à la place du premier disque sans problème, même en l'absence de panne. Ensuite, débranchez le premier disque. Le choix sur la nouvelle entrée fait démarrer votre système.



Si vous obtenez une erreur GRUB au démarrage, c'est qu'il y a eu une mauvaise manipulation... Utilisez alors le CD-Rom de la version serveur avec l'option **Réparer un système endommagé**. Après avoir monté le shell sur `/dev/md0`, réinstallez GRUB.

La remise en état s'effectue de la même façon que pour la première panne.

c. Partitionnement en RAID 5

Pour une meilleure gestion de l'espace disque, le partitionnement en RAID 5 se marie mieux avec un partitionnement logique par LVM. Ce point sera donc développé dans le paragraphe suivant.

2. Avec un système de partitions en LVM

Toutes les structures vues précédemment associent physiquement la partition à l'emplacement sur le disque. Ubuntu supporte LVM (*Logical Volume Manager*) pour gérer les opérations sur les partitions sans altérer le système de fichiers déjà existant. LVM est apporté par le paquet logiciel `lvm2`. En clair, LVM répond à un problème récurrent : *comment toucher au système de fichiers sans toucher aux partitions ?*

a. Principes de fonctionnement

Au lieu de définir une partition sur un disque, LVM se construit d'abord avec un groupe de disques physiques (maximum 256 disques, avec un minimum de 1). Avec la technique du RAID 5, la démarche fait que l'on crée d'abord le RAID et ensuite le groupe physique. On biaise un peu le sens de LVM car il n'existera qu'un seul volume physique pour un groupe de volume (voir l'exemple). Ensuite, on aura autant de groupes logiques (maximum 256) que de partitions désirées.

b. Partitionnement en RAID 5 avec LVM

L'exemple va concerner, cette fois, un système à trois disques et toujours à l'étape du partitionnement en **choix manuel**. Comme LVM ne supporte pas le `/boot`, ce répertoire sera sur une partition physique séparée. Le reste (soit l'espace libre du disque 1, le disque 2 et le 3) sera regroupé d'abord dans un ensemble RAID 5 avant d'être intégré dans un groupe de volumes physiques avec LVM (techniquement, il faut réserver RAID 5 sur trois disques de tailles identiques, mais peu importe ici pour le test).

Pour le disque n°1, partition

- Positionnez-vous sur la ligne concernant le **premier** disque (`sda`), validez, acceptez en cas de nouveau disque l'écriture d'une nouvelle table de partitions, type MSDOS.
- Positionnez-vous sur la ligne de la partition marquée comme espace libre, validez, choisissez **Créer une nouvelle partition**, taille 100 Mo (cela est suffisant pour le noyau).
- Choisissez un type primaire pour la partition avec un emplacement au début.
- Dans le choix **Utiliser comme**, validez **système de fichiers journalisé ext3**, point de montage `/boot`.
- Terminez par une validation sur **Fin du paramétrage de cette partition**.

Pour le disque n°1, partition RAID

- Positionnez-vous sur la ligne de la partition marquée comme espace libre (toujours sur le premier disque), validez, choisissez **Créer une nouvelle partition**, acceptez la taille par défaut (le reste du disque soit 8.5 Go) et toujours de type primaire.
- Choisissez l'utilisation comme système de fichiers **volume physique pour RAID**.
- Important : validez la ligne **Indicateur d'amorçage** pour y mettre la valeur **présent**.
- Terminez par une validation sur **Fin du paramétrage de cette partition**.

Pour le disque n°2 et n°3

- Répétez les opérations précédentes concernant une partition RAID pour la totalité du disque.

Avant la configuration LVM, l'écran présente les détails suivants :

```
| [!!!] Partitionner les disques |
Voici la table des partitions et les points de montage actuellement
configurés. Vous pouvez choisir une partition et modifier ses
caractéristiques (système de fichiers, point de montage, etc.), un
espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Configurer le RAID logiciel
Partitionnement assisté
Aide pour le partitionnement

SCSI3 (0,0,0) (sda) - 8.6 GB VMware, VMware Virtual S
n° 1 primaire 98.7 MB f ext3 /boot
n° 2 primaire 8.5 GB B K raid
SCSI3 (0,1,0) (sdb) - 8.6 GB VMware, VMware Virtual S
n° 1 primaire 8.6 GB B K raid
SCSI3 (0,2,0) (sdc) - 8.6 GB VMware, VMware Virtual S
n° 1 primaire 8.6 GB B K raid

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

<Revenir en arrière>
```

La mise en RAID 5 peut s'effectuer.

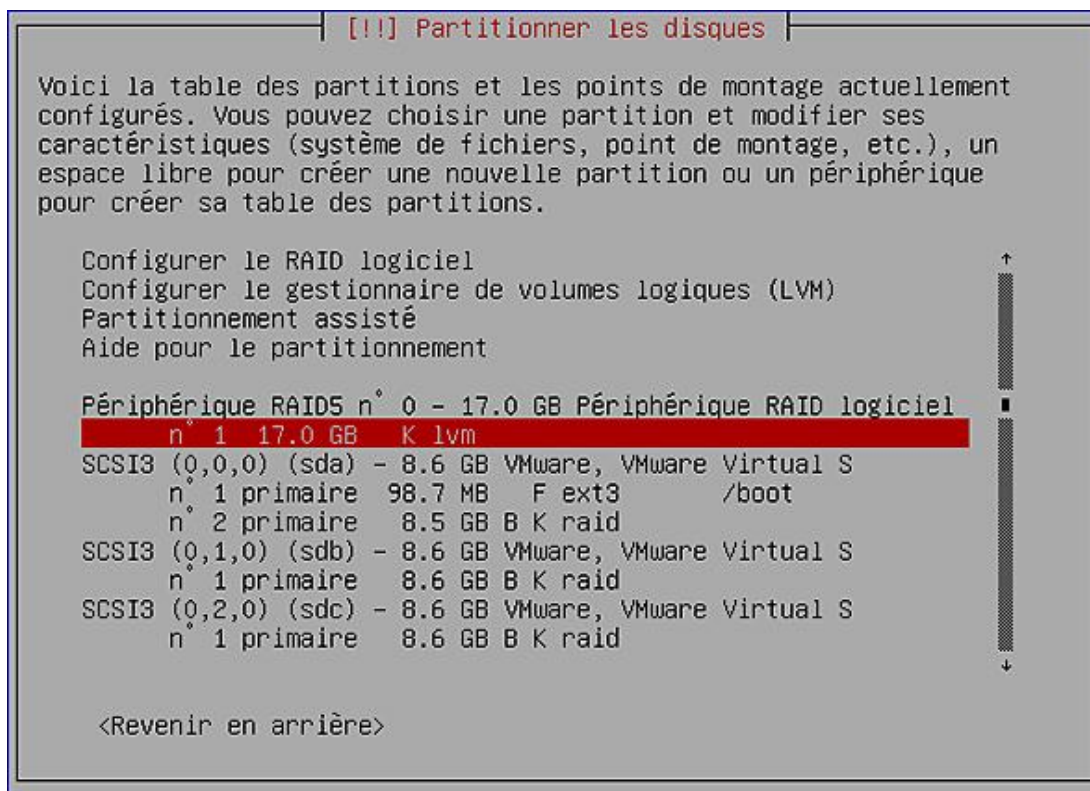
- Choisissez la ligne **Configurer le RAID logiciel** et validez les changements.
- Choisissez l'option **Créer un périphérique multidisque**.
- Choisissez le type **RAID5** pour le niveau du RAID.
- Validez la valeur par défaut (soit 3) concernant le nombre de périphériques actifs pour l'ensemble RAID5, avec 0 périphériques de réserve.
- Cochez les trois périphériques /dev/sda2, /dev/sdb1 et /dev/sdc1.
- Validez et choisissez **Terminer la configuration multidisque**.

Le périphérique RAID n°0 comporte au final un espace de 17 Go. Il faut maintenant compléter LVM et déterminer le groupe de volumes.

Création du groupe LVM physique

- Validez la ligne n°1 17.0 GB du périphérique RAID 5 et choisissez une utilisation comme **volume physique pour LVM**.
- Terminez par une validation sur **Fin du paramétrage de cette partition**.

Une nouvelle ligne de configuration s'est positionnée, celle qui a trait à LVM :



- Validez la ligne **Configurer le gestionnaire de volumes logiques**, répondez **Oui** à l'écriture des modifications (si demandé).

Une synthèse de la configuration LVM s'affiche et montre :

- 1 volume physique libre
- aucun volume physique utilisé

- aucun groupe de volumes
- aucun volumes logiques

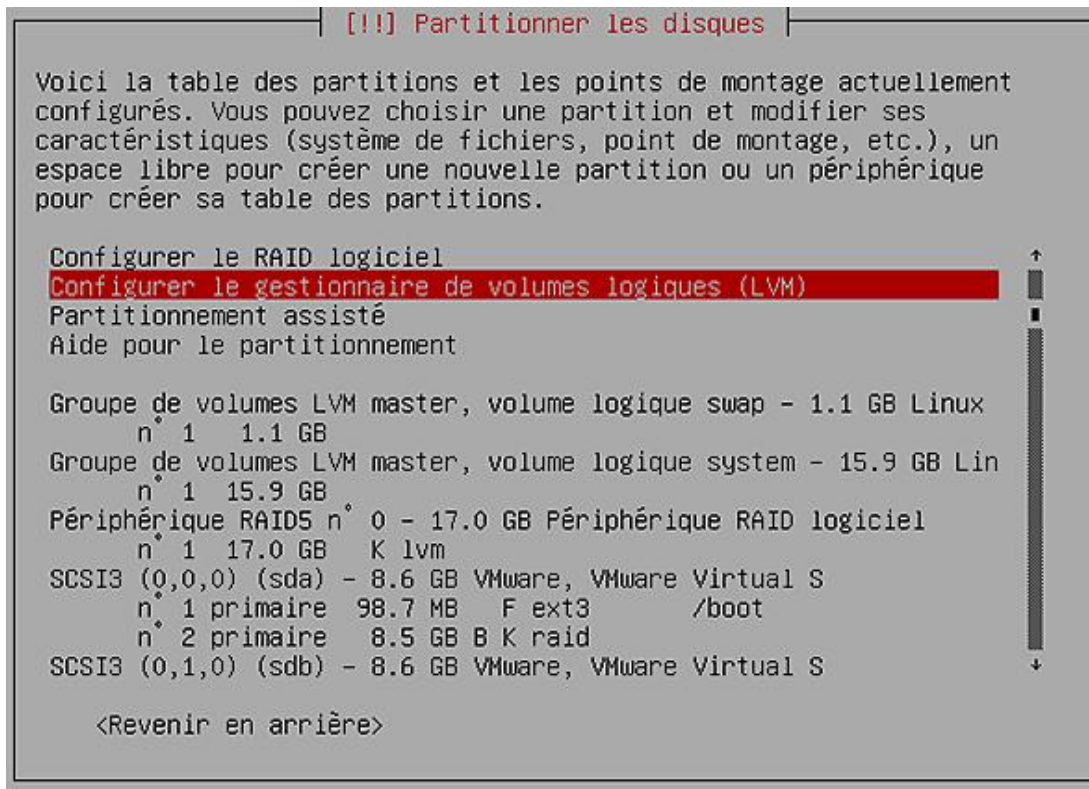
Il faut affecter à la configuration LVM au moins un volume physique :

- Validez la ligne **Créer un groupe de volumes** et donnez-lui un nom.
- Cochez le périphérique pour le groupe c'est-à-dire /dev/md0.

À ce stade, il ne reste plus de volume physique de libre : un est utilisé et un groupe de volumes est créé. La manipulation suivante va créer deux volumes logiques : celui que l'on réservera à la partition d'échange et celle pour le système de fichiers. On gardera pour la démonstration un espace libre de 2 Go.

- Validez la ligne **Créer un volume logique** sur le volume physique et donnez-lui un nom (exemple swap), taille de 1024 Mo.
- Recommencez pour un deuxième volume avec une taille du reste, normalement 15900 Mo (exemple de nom : **system**).
- Validez par **Terminer**.

L'écran affiche les informations suivantes :



Il ne reste plus qu'à définir sur le volume logique `swap` la partition étendue et sur le volume logique `system`, le point de montage / pour le système de fichiers en `ext3`.

Le fin de l'installation est conforme à la procédure déjà vue en terminant le partitionnement et application des changements.

c. Maintenance

La maintenance au niveau de RAID ne diffère pas ou peu de celle vue avec le RAID 1. Pour LVM, l'application du principal avantage porte sur la modification facile du système de fichiers.

Hypothèse :

Vous désirez séparer l'espace de travail des utilisateurs en affectant une partition à la racine /home ; taille désirée 3 Go. Il faut donc redimensionner le système de fichiers principal en le réduisant de la valeur voulue et affecter celle-ci au point de montage /home.

Note : toutes les manipulations se font en `root`, directement en se connectant sous ce compte si à l'installation celui-ci a été créé, ou par la commande `sudo -i` à partir de l'utilisateur principal. Nous sommes en mode console (texte) bien évidemment car pour la version serveur, il n'y a pas d'environnement graphique.

d. Manipulations

Deux problèmes se posent immédiatement :

- la **taille du système de fichiers** (le contenu) par rapport à la nouvelle taille du volume logique (le contenant) ; on comprend aisément que si le premier est supérieur au deuxième, cela ne pourra se faire...
- le **démontage du système de fichiers**, obligatoire pour pouvoir effectuer les manipulations ; or vous êtes dans le système, il va falloir travailler sur une position "extérieure".



Le dernier problème ne se pose pas si vous désirez modifier des points de montage à l'intérieur du système de fichiers. Ici, ce qui nous bloque, c'est que l'on désire travailler directement à la racine soit /.

Vérification de l'espace disque occupé :

```
df -h
```

Le retour affiche une taille arrondie de 15.532 Go utilisée et 14 Go disponible. Ce sont les chiffres en rapport avec l'exemple et largement suffisants quant à l'espace car situés juste après une installation. En cas d'occupation trop importante, il aurait fallu supprimer quelques fichiers...

Pour travailler en dehors du système, vous allez réutiliser le CD-Rom de la distribution serveur :

- Mettez le CD-Rom, redémarrez par la commande `reboot` et choisissez l'option **Réparer un système endommagé**.
- Choisissez le pays **France**, et entrez un nom de machine quelconque.

La plupart des éléments se détecte automatiquement comme le matériel et la configuration réseau (d'ailleurs non nécessaires), etc. L'écran le plus important montre le choix du périphérique à monter comme système de fichiers racine. Dans l'exemple, les quatre partitions normales, les deux volumes logiques et le volume RAID sont affichées :

```

| [!!!] Entrer dans le mode de récupération |
|
| Veuillez choisir un périphérique qui sera utilisé comme système de
| fichiers racine. Vous pourrez ensuite choisir entre plusieurs
| opérations de récupération à effectuer sur ce système de fichiers.
|
| Périphérique à monter comme système de fichiers racine (/) :
|
| /dev/sda1
| /dev/sda2
| /dev/sdb1
| /dev/sdc1
| /dev/master/swap
| /dev/master/system
| /dev/md0
|
| <Revenir en arrière>
```

- Choisissez le volume logique LVM `/dev/master/system` correspondant au système de fichiers racine.
- Choisissez **Exécuter un shell dans le contexte de l'installateur** et validez par **Continuer**.

On ne prend pas l'exécution dans le volume logique lui-même car vous n'avez pas intrinsèquement à réparer le système et vous vous retrouveriez dans la même situation qu'un démarrage normale de la distribution. L'exécution de la dernière action vous place dans la console **BusyBox**, déjà vue lors de l'installation.

Le point de montage `/target` comprend votre système, tapez `mount` et validez pour le vérifier. Il faut le "démonter" :

```
umount -l /target
```

Avant de redéfinir la taille du système à 12 Go (15 - 3 pour `/home`), une vérification de la structure s'impose :

```
e2fsck -f /dev/master/system
resize2fs -p /dev/master/system 11G
```

Pourquoi 11 Go au lieu de 12 ? Parce qu'il faudra réadapter la taille du système à la taille du volume logique et vous ne devez pas prendre le risque d'ajuster à l'octet près le deuxième sur le premier, au risque de perdre des données. On le voit nettement avec la réduction effective à 11,81 Go :

```
~ # lvresize -L -3G /dev/master/system
File descriptor 3 left open
File descriptor 4 left open
File descriptor 5 left open
File descriptor 6 left open
WARNING: Reducing active logical volume to 11.81 GB
THIS MAY DESTROY YOUR DATA (filesystem etc.)
Do you really want to reduce system? [y/n]: y
Reducing logical volume system to 11.81 GB
Logical volume system successfully resized
~ #
```

Il ne vous reste plus qu'à indiquer au système de réoccuper tout l'espace du volume logique :

```
resize2fs /dev/master/system
```

Après le redémarrage, l'appel de la commande `df -h` montre cette fois pour `/dev/mapper/master-system` une taille de 12 Go, une utilisation toujours à 532 Mo et total utilisable à 11 Go.

Passez ensuite à la création du nouveau volume logique LVM que vous nommerez `home` :

```
lvcreate -n home -L 3g master
```

Pour finir, un système de fichiers `ext3` doit être créé sur ce volume logique avant d'être monté :

```
mkfs.ext3 /dev/master/home
mount /dev/master/home /home
```

L'appel une dernière fois de la commande `df -h` montre un système de fichiers supplémentaire `/dev/mapper/master-home`, d'une taille de 3 Go, une utilisation à 69 Mo et un espace disponible de 2,8 Go.

Ce simple tour d'horizon aborde les premières notions de LVM. D'autres commandes existent comme `vgdisplay`, qui affiche les renseignements sur le volume physique ou d'autres notions comme le "snapshot", littéralement un instantané d'un volume logique pour une sauvegarde d'intégrité des données.

Une bonne adresse Internet pour en savoir plus : <http://linux.developpez.com/lvm/>

Ouverture d'une session

Quel que soit le matériel, le démarrage du système lance une série de tests et de détection de matériel. Le mécanisme `initrd` laisse ensuite la place au système de fichiers monté puis exécute la commande `init`, père de tous les autres processus. La différence entre un serveur et un poste de travail c'est que dans le premier on voit - et on recherche - plus d'informations, alors que pour le deuxième, la discrétion prime.

1. Sur un serveur

a. Phase de démarrage

Le démarrage affiche une succession de lignes et se termine par une invite :

```
* Activating swap... [ OK ]
* Checking root file system...
fsck 1.40.8 (13-Mar-2008)
/dev/sda1: clean, 17446/499712 files, 150276/1994060 blocks [ OK ]

* Checking file systems...
fsck 1.40.8 (13-Mar-2008) [ OK ]

* Mounting local filesystems... [ OK ]
* Activating swapfile swap... [ OK ]
$Mounting securityfs on /sys/kernel/security: done.
Loading AppArmor profiles : done.
* Checking minimum space in /tmp... [ OK ]
* Skipping firewall: ufw (not enabled)... [ OK ]
* Configuring network interfaces... [ OK ]
* Setting up console font and keymap... [ OK ]
* Starting system log daemon... [ OK ]
* Starting kernel log daemon... [ OK ]
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Running local boot scripts (/etc/rc.local) [ OK ]

Ubuntu 8.04.1 serveur tty1

serveur login: _
```

Cette phase importante donne à l'administrateur des renseignements importants sur la bonne reconnaissance du matériel et le lancement des services de base. Le résultat à droite par l'affichage du mot **[OK]** ne laisse planer aucune ambiguïté...

L'ouverture de session se fait par l'entrée du `login` soit `root` et de son mot de passe, **compte normalement activé à l'installation**. La saisie du mot de passe s'effectue "en aveugle", c'est-à-dire sans affichage de retour de frappe, dans un but de sécurité (pour qu'on ne puisse déterminer la longueur du mot de passe). Une fois vérifiée, vous vous trouvez dans l'espace de travail de l'utilisateur (`/root`).

Lors d'une connexion réussie, l'identifiant s'affiche avant le prompt ainsi que le répertoire dans lequel vous vous trouvez (un tilde ou `~` indique le répertoire de l'utilisateur). Le dernier symbole se détermine comme un dièse dans le cas d'un statut administrateur (`root`) alors qu'un dollar indique un statut utilisateur.

La fermeture de la session se fait par :

- `exit` : le plus usité
- `<Ctrl + D>` : classique
- `logout` : explicite

Si les droits de l'utilisateur le permettent :

- `reboot` ou `<Ctrl + Alt + Suppr>` : redémarrage du système
- `poweroff` ou `shutdown -f now` : arrêt du système

b. Rétablir le compte de l'administrateur

Appelé `root` en anglais, il dispose de tous les pouvoirs et d'un répertoire séparé : `/root`. Les travaux d'administration se font à l'aide de ce compte. Sous Ubuntu, un utilisateur spécial peut prendre temporairement les droits administrateurs pour une commande par la commande `sudo` (do = faire) alors que le changement complet d'identité se fait par la commande `su`.



Attention : le répertoire de base du système noté `/`, s'appelle aussi `root` mais signifie racine. Il ne faut pas les confondre.

Seules les installations de la distribution Ubuntu en mode expert (CD-Rom de la version `server` ou `alternate`) propose l'utilisation classique du compte de l'administrateur (le `root`). Dans le cas contraire, un utilisateur spécial doté de pouvoirs avec le mécanisme `sudo` a été créé.

Ubuntu défend une politique restrictive sur les droits utilisateurs partant de deux principes :

- L'utilisateur courant, dans sa session de travail, ne doit pas avoir accès aux fichiers et processus systèmes, ni pouvoir les modifier.
- Le compte `root` est "désactivé" car facilement repérable aux attaques externes et trop dangereux dans une utilisation courante.

Pour lancer et travailler sous OpenOffice ou d'autres applications, nul besoin est de disposer des privilèges liés à l'administration du système. Toute la perception de cette limitation repose sur :

- D'une part, la nature du système : un serveur ou un poste de travail.
- D'autre part, la nature des opérations effectuées : tâches d'administration ou tâches plus courantes.

Le raisonnement est simpliste mais réel : si vous êtes un administrateur système sur une distribution serveur, l'utilisation de `sudo` pour prendre les droits va vite se révéler fastidieuse, n'en déplaie aux tenants du dogme... Dans tous les autres cas, on ne change rien pour suivre les préceptes cités plus haut.

Pour lancer une opération nécessitant les droits de l'administrateur, on fait précéder le terme `sudo` avant la commande :

```
sudo visudo
```

Le choix de l'exemple n'est pas anodin car il montre le contenu du fichier `sudoers` avec la commande spéciale `visudo`. Plusieurs remarques sont à faire :

- Le fichier `/etc/sudoers` ouvert par cette commande contient la configuration de l'outil `sudo`.
- La commande `visudo` édite dans un mode plus sécurisé le fichier en interdisant les éditions multiples, vérifie et détecte les erreurs de syntaxe.
- Sans la commande `sudo`, l'édition du fichier est impossible (permission refusée) car seul le `root` en a le droit.

Voici l'adresse du site Internet de `sudo` : <http://www.gratisoft.us/sudo>

L'utilisation temporaire de droits administrateurs par ce mécanisme est un choix d'administration sur la distribution Ubuntu. En voici les avantages, tous liés à une meilleure recherche de la sécurité :

- L'exécution de tâches critiques pour le système fait l'objet d'une demande d'autorisation supplémentaire, propre à la réflexion.
- Les droits de l'utilisateur privilégié sont modulables et étendus à d'autres utilisateurs.
- Le compte `root`, aisément repérable par un attaquant se trouve bloqué.

L'ouverture sans la commande `sudo` interdit la modification du fichier des caractéristiques utilisateurs. Quelquefois, l'ouverture elle-même est impossible.

Si malgré tout, la fatigue liée à l'emploi systématique de la commande `sudo` l'emporte sur le désir de sécurité (on peut l'imaginer sur un système non en réseau ou protégé par un pare-feu), le rétablissement du compte administrateur système est facile :

```
sudo passwd root
```

Après la saisie du mot de passe de l'utilisateur privilégié, la demande et sa confirmation du mot de passe `root` rétablira simplement le compte.



La seule différence réside dans l'absence du fichier caché `.bash_logout` effectuant un nettoyage de l'écran lors de la déconnexion. Il suffit de le copier à partir d'un compte utilisateur dans le répertoire `/root` pour y remédier.

Utilisation de sudo en tant qu'administrateur

Alors que la commande `sudo -V` en tant qu'utilisateur ne retourne que le nom du programme et sa version, lancée en tant qu'administrateur (ou `sudo sudo`), elle affiche (liste assez longue) les variables d'environnement toujours intéressantes :

```
sudo -V
```

L'édition et la modification d'un fichier peuvent se faire par le biais d'un tampon situé dans `/var/tmp/` :

```
sudo -e (ou sudoedit)
```

La syntaxe est vérifiée et en cas de problème, des choix d'enregistrements sont proposés.



Une utilisation plus complète de la commande `sudo` vous est fournie lors de la gestion des comptes utilisateurs dans le chapitre Maintenance de base du système.

2. Sur un poste de travail

a. Interface GDM

L'environnement de bureau GNOME associe le gestionnaire **GDM** (*Gnome Display Manager*) pour l'ouverture d'une session graphique. Ce service dispose d'un espace personnel sur le site de GNOME : <http://www.gnome.org/projects/gdm>

Suivant le même principe du mode console, l'interface autorise les sessions, et donc les autorisations multiples. Sur une machine utilisée par un utilisateur unique, la session peut être ouverte automatiquement par GDM avec la dispense d'entrée de l'identifiant et du mot de passe :



Une session s'ouvre classiquement en indiquant son identifiant (login) et le mot de passe de l'utilisateur. Un sous-menu d'options est disponible avant la connexion et propose les actions suivantes :

Sélectionner une langue

Changement de la langue pour la session.

Sélectionner une session

Changement de type de session (distant ou local).

Connexion distante via XDMCP

Ouvre une session à distance à partir d'un serveur via le protocole XDMCP (via un terminal à distance, rarement utilisé).

Redémarrer

Redémarre le système.

Éteindre

Éteint le système.

Mettre en veille

Fonctions et données vitales préservées en mémoire mais réduites au minimum pour économiser l'énergie.

Hiberner

Fonctions et données vitales préservées sur le disque et éteintes pour ne plus consommer d'énergie.



L'interface GDM se change sans difficulté. Voir pour cela le chapitre suivant Prise en main de la distribution.

b. Réglages de l'interface

L'utilitaire GDM s'exécute avec les **droits utilisateurs de même nom** tels que définis dans le fichier `/etc/gdm/gdm.conf`. Le lancement du client graphique (client X) s'effectue lui, avec les droits de l'utilisateur connecté et aboutit au même résultat qu'une console texte avec la commande `startx`.

L'écran de connexion comporte beaucoup de paramètres et la configuration de celui-ci se lance par le menu **Système/Administration/Fenêtre de connexion**, soit le programme **gdmsetup** (nécessite le droit administration). Les changements les plus courants concernent :

- L'onglet **Général** : l'interdiction/autorisation des connexions multiples.
- L'onglet **Locale** : le changement du thème.
- L'onglet **Distante** : l'activation/désactivation d'une connexion distante.
- L'onglet **Accessibilité** : l'activation/désactivation des sons de connexion (les fameux roulements de tambour africain Ubuntu).
- L'onglet **Sécurité** : l'activation/désactivation de la connexion automatique avec l'accès ou non pour le `root` (désactivé par défaut).
- L'onglet **Utilisateurs** : inclure/exclure les utilisateurs dans le navigateur de figures avec personnalisation des images.

3. Authentification locale

a. Principes d'une connexion

Comme tout système Linux, Ubuntu autorise une authentification multi-utilisateur par le biais du programme `login`. Son réglage se trouve dans le fichier `/etc/login.defs` que l'on ne change généralement pas, certaines options étant réécrites par le module d'authentification PAM (voir le chapitre sur la sécurité). Les consoles de connexion sont, quant à elles, définies dans le fichier `/etc/securetty`.

Le principe local constitue le schéma de base d'une authentification, mais il peut y en avoir d'autres dites distribuées :

- par un serveur d'annuaire de type **LDAP** (*Lightweight Directory Access Protocol*).
- par un contrôleur de domaine de type **Samba** ou serveur **Active Directory** (Windows).

Le mécanisme de connexion repose sur trois fichiers :

- `/etc/passwd`, contenant les informations d'un utilisateur.
- `/etc/shadow`, contenant les mots de passe cryptés.
- `/etc/group`, contenant les informations des groupes d'utilisateurs.

Cela introduit les trois grandes catégories de classement d'utilisateurs sous Ubuntu Linux : les **utilisateurs** normaux, les **groupes** d'utilisateurs et le **reste du monde** (ou plus simplement ceux qui n'appartiennent pas aux deux premières catégories).

b. Fichiers de connexion

L'ajout manuel d'un utilisateur à partir des fichiers correspond à :

- l'ajout de la ligne utilisateur dans le fichier `/etc/passwd`.

- l'ajout du groupe de base de l'utilisateur dans le fichier `/etc/group` (généralement du même nom).
- l'ajout du mot de passe crypté avec la commande `mkpasswd` (le cryptage MD5 se combinant avec un algorithme de hachage).
- la création du répertoire dans `/home`.
- la copie des fichiers du profil utilisateur provenant du répertoire `/etc/skel`.

Structure du fichier `/etc/passwd`

Ce fichier texte comprenant sept champs séparés par le caractère deux points (:), accessible par tous en lecture, possède la structure suivante :

- (1) **Nom de connexion** : identifiant de l'utilisateur ou nom du démon (*daemon* ou processus en cours).
- (2) **Caractère** : ancienne place du mot de passe (avant l'utilisation de la suite *shadow*) un x indiquant un mot de passe crypté dans `/etc/shadow`, une étoile (*) interdit la connexion au compte.
- (3) **Numéro de l'utilisateur** : UID (*user identifier* ou du processus) ou véritable identifiant pour le système (UID du root à 0, Ubuntu commence les UID utilisateurs à partir de 1000).
- (4) **Numéro du groupe** : GID (*group identifier* ou du processus), même principe de numérotation que pour les UID.
- (5) **Détail** : commentaire (en général vide), l'ajout ou la modification de ce champ s'exécute par la commande `chfn`.
- (6) **Répertoire d'accueil** : pour un utilisateur situé dans `/home`.
- (7) **Programme** : à lancer à la connexion (dans le cas d'un utilisateur, il s'agit du shell ou gestionnaire de commandes).

Exemple de fichier sous Ubuntu (serveur) :

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuid:x:100:101::/var/lib/libuid:/bin/sh
dhcpc:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
max:x:1000:1000:max,,,:/home/max:/bin/bash
~
```



Pour éditer le fichier `/etc/passwd`, on utilise de préférence la commande `vi pw` qui interdit toute autre édition en même temps et passe par un fichier temporaire.

Structure du fichier `/etc/shadow`

Le processus d'authentification utilise le fichier des mots de passe cryptés pour vérifier que l'utilisateur est bien celui qu'il prétend être. Ce fichier, en lecture uniquement par le `root` et le groupe `shadow`, comprend 9 champs, séparés par le symbole deux points (`:`), avec :

- (1) **Nom de l'utilisateur** : le groupe de base est du même nom que l'utilisateur.
- (2) **Mot de passe** : mot de passe chiffré par un algorithme mathématique, une étoile signifie que le compte a été désactivé ou qu'il s'agit d'un processus.
- (3) **Date de changement** : en fait le nombre de jours entre le 01/01/1970 et la date ou le changement de mot de passe a été effectué.
- (4) **Intervalle avant changement** : classiquement un 0 car non utilisé, ce champ indique le nombre de jours avant de pouvoir changer le mot de passe.
- (5) **Intervalle de changement** : classiquement 99999 car peu utilisé, il représente le nombre de jours après quoi un changement de mot passe est obligatoire.
- (6) **Délai d'expiration** : nombre de jours indiquant le délai accordé à un utilisateur avant que son mot de passe n'expire.
- (7) **Expiration du compte** : nombre de jours avant l'expiration du mot de passe et donc désactivation du compte, vide car peu utilisé.
- (8) **Date de désactivation** : en fait le nombre de jours entre le 01/01/1970 et la date de désactivation du compte, vide car peu utilisé.
- (9) **Indicateur** : non utilisé.

Exemple de fichier sous Ubuntu (serveur) :

```
root:$1$qn3AweE7$EAWynH0v1sODbXZ.j/220//:14044:0:99999:7:::
daemon:!:14044:0:99999:7:::
bin:!:14044:0:99999:7:::
sys:!:14044:0:99999:7:::
sync:!:14044:0:99999:7:::
games:!:14044:0:99999:7:::
man:!:14044:0:99999:7:::
lp:!:14044:0:99999:7:::
mail:!:14044:0:99999:7:::
news:!:14044:0:99999:7:::
uucp:!:14044:0:99999:7:::
proxy:!:14044:0:99999:7:::
www-data:!:14044:0:99999:7:::
backup:!:14044:0:99999:7:::
list:!:14044:0:99999:7:::
irc:!:14044:0:99999:7:::
gnats:!:14044:0:99999:7:::
nobody:!:14044:0:99999:7:::
libuid:!:14044:0:99999:7:::
dhcp:!:14044:0:99999:7:::
syslog:!:14044:0:99999:7:::
klog:!:14044:0:99999:7:::
max:$1$5Mj/by.J$rqo.NociSqZIrJP1QeZH10:14044:0:99999:7:::
```

Structure du fichier /etc/group

Ce fichier, complément du fichier /etc/passwd comprend 4 champs, séparés par le symbole deux points (:), avec :

- (1) **Nom du groupe** : le groupe de base est du même nom que l'utilisateur.
- (2) **Caractère** : pour remplacer un mot de passe de groupe (non attribué maintenant).
- (3) **Numéro du groupe** : c'est-à-dire l'identifiant GID.
- (4) **Utilisateurs du groupe** : liste des membres supplémentaires du groupe séparés par une virgule.

Exemple de fichier sous Ubuntu (extrait d'un serveur) :

```
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:max
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:max
fax:x:21:
voice:x:22:
cdrom:x:24:max
floppy:x:25:max
tape:x:26:
sudo:x:27:
audio:x:29:max
dip:x:30:max
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:max
sasl:x:45:
plugdev:x:46:max
staff:x:50:
"/etc/group" 52L, 653C
```

Droits des utilisateurs

Le mécanisme permettant au système d'être multi-utilisateur induit un accès sélectif et des niveaux de protection sur les fichiers. Le principe de base s'énonce ainsi : le propriétaire d'un fichier définit son droit d'accès. Tout fichier ou répertoire sur Ubuntu appartient à un utilisateur et à un groupe.

1. Utilisateurs et attributs de fichiers

a. Principes

Sous Ubuntu Linux, voici l'identification des types d'utilisateurs :

- Le propriétaire du fichier noté user.
- Le groupe d'appartenance du propriétaire noté group.
- Les autres ou le reste du monde noté other.

Pour visualiser l'appartenance d'un fichier, la commande `ls` option `-l` (format long) montre pour chaque fichier un ensemble d'arguments associés.

Exemple :

```
touch essai.txt
```

```
ls -l essai.txt
```

La première commande crée un fichier texte vide. Les deux sont effectuées par l'administrateur (le créateur du fichier est le propriétaire) :

```
-rw-r--r-- 1 root root 0 sept 24 16:21 essai.txt
```

Le premier bloc de dix caractères informe de la signification des droits :

- La première lettre donne l'indication du type de fichier. Les plus courants sont un tiret (-) pour l'attribut d'un fichier ordinaire et un (d) pour un répertoire.
- Les trois lettres suivantes indiquent le propriétaire avec dans l'ordre : r ou - (droit en lecture ou non), w ou - (droit en écriture ou non), x ou - (droit en exécution ou non).
- Les trois lettres suivantes donnent exactement la même signification mais pour le groupe.
- Les trois dernières lettres s'appliquent au reste du monde.

La suite de l'affichage donne respectivement le nombre de liens (cette notion est vue dans le chapitre Session de travail en mode console), le propriétaire du fichier, le groupe d'appartenance, la taille du fichier en octets, la date et l'heure de la dernière modification du fichier et enfin le nom du fichier.

Plus précisément :

- Dans le cas d'un fichier : le droit de lecture (r) autorise la visualisation du contenu, le droit d'écriture (w) autorise la modification du contenu et le droit d'exécution (x) autorise (pour les fichiers exécutables évidemment) ... son exécution.
- Dans le cas d'un répertoire : le droit de lecture (r) autorise le listing des fichiers qu'il contient, le droit d'écriture (w) autorise la création, modification et suppression des fichiers et le droit d'exécution (x) autorise la possibilité d'y aller ou de le "traverser".

b. Changement des attributs de fichiers

Rappel du principe de base : seul le propriétaire peut changer son droit d'accès au fichier. Seul l'administrateur système (root) possède tous les pouvoirs. Cela rend le système fiable car l'infection et la propagation d'un virus ne peut se faire que dans l'espace de propriété de l'utilisateur, d'où le fait de ne pas effectuer des opérations courantes ou à risque comme la lecture de courriers sous l'identité du root.

Le changement d'attributs s'effectue avec la commande `chmod` (change mode). On distingue traditionnellement deux modes d'utilisation.

Méthode par le nombre octal (base huit)

Le nombre octal se donne par trois bits, positionnés à 0 ou 1, représentatifs de puissances de 2 :

```
chmod nombre_octal nom_fichier
```

Exemple :

```
chmod 644 essai.txt
```

Qui s'explique de la façon suivante : il ne faut pas lire 644 mais 6 (le premier pour le propriétaire), 4 (le deuxième pour le groupe) et 4 (le dernier pour le reste du monde). En binaire 6 se code sur 110, soit en représentant les puissance de 2 :

$$1*2^2 + 1*2^1 + 0*2^0 = 110 \text{ (ou } 4 + 2 + 0 = 6)$$

Un bit positionné à 1 donne la permission, 0 donne une interdiction. 110 donne donc la permission en lecture , en écriture et non en exécution soit dans notre exemple :

rw-

Notez un chiffre couramment utilisé pour les scripts exécutables : 755 ce qui donne tous les droits pour le propriétaire, les droits en lecture et exécution pour le groupe et le reste du monde.

Méthode par la définition symbolique

On aura cette fois la commande :

```
chmod [qui][opération][type_permission] nom_fichier
```

Avec :

qui : u pour user

opération : - pour une interdiction, + pour une permission

type_permission : rwx lecture, écriture et exécution

Exemple :

```
chmod o-r essai.txt
```

Cet exemple ôte la permission en lecture pour le reste du monde.

c. Changement de propriétaire ou de groupe

Pour "donner" un fichier à un autre utilisateur, il faut bien sûr en être propriétaire et avoir les droits (sauf le root) : on ne peut donner que ce qui nous appartient ! La commande :

```
chown [options] nouveau_propriétaire nom_fichier
```

s'utilise pour changer le propriétaire d'un fichier (change owner), alors que :

```
chgrp [options] nouveau_groupe nom_fichier
```

s'utilise pour changer le groupe d'un fichier (change group).

Exemples (on donne à max le fichier de léon) :


```
chown max essai.txt
```

```
chgrp max essai.txt
```

```
chown max.max essai.txt
```

La dernière commande exploite une fonctionnalité de la commande `chown` qui permet d'effectuer un raccourci en changeant en même temps le propriétaire et le groupe.

d. Droits supplémentaires

Parallèlement aux droits standards, des droits étendus existent et répondent à des besoins spécifiques :

- Pour un répertoire, restreindre la suppression au seul propriétaire : droit **sticky bit**.
- Pour un fichier binaire, exécution sous l'identité du propriétaire : droit **SUID** (`setuid`) ou sous l'identité du groupe : droit **SGID** (`setgid`).

Ce dernier point permet d'exécuter un programme (normalement un binaire et non un fichier de commandes) à partir d'un utilisateur quelconque nécessitant les droits d'un autre.

Pour affecter ou retirer ces droits, on utilise la commande `chmod` avec cette fois-ci sur quatre bits, le premier indiquant la nature du droit ou par une lettre spécifique en notation symbolique :

Droit	En octal	En symbolique
Sticky bit	1000	o+t
SUID	4000	u+s
SGID	2000	g+s

Le champ d'application du droit par la notation symbolique se fait clairement : `u` pour le SUID et `g` pour le SGID. Dans le cas du **sticky bit**, l'application porte sur le "reste du monde" soit `o`, partant du principe qu'un fichier sous Ubuntu appartient à un groupe du même nom que le propriétaire.

Exemples de commandes :

```
chmod o+t /home/donald/programmes/
```

```
chmod 4755 liste.sh
```

```
ls -l /usr/bin/chage
```

La première commande positionne le droit **sticky bit** pour le répertoire `programmes` situé dans le répertoire de l'utilisateur `donald`. La deuxième commande met les droits en exécution pour le fichier comprenant des commandes shell et positionne en même temps le droit SUID. Enfin la dernière commande montre que le droit SGID est mis pour la commande `chage` (modifie les informations de validité d'un mot de passe) pour le groupe `shadow` (note : le fichier `/etc/shadow` a pour propriétaire le `root` et comme groupe `shadow`).



Si le fichier/répertoire n'a pas les droits en exécution, le `s` et `t` apparaissent en majuscules.

2. Entraînement

L'utilisation et la compréhension des droits utilisateurs nécessitent un minimum de pratique. Afin de vous aider dans la maîtrise des commandes, voici une liste de **questions/exercices** (les solutions se trouvent en **Annexe 2**) :

Cadre de travail

Session ouverte en `root` sur une version Ubuntu serveur.

Questions

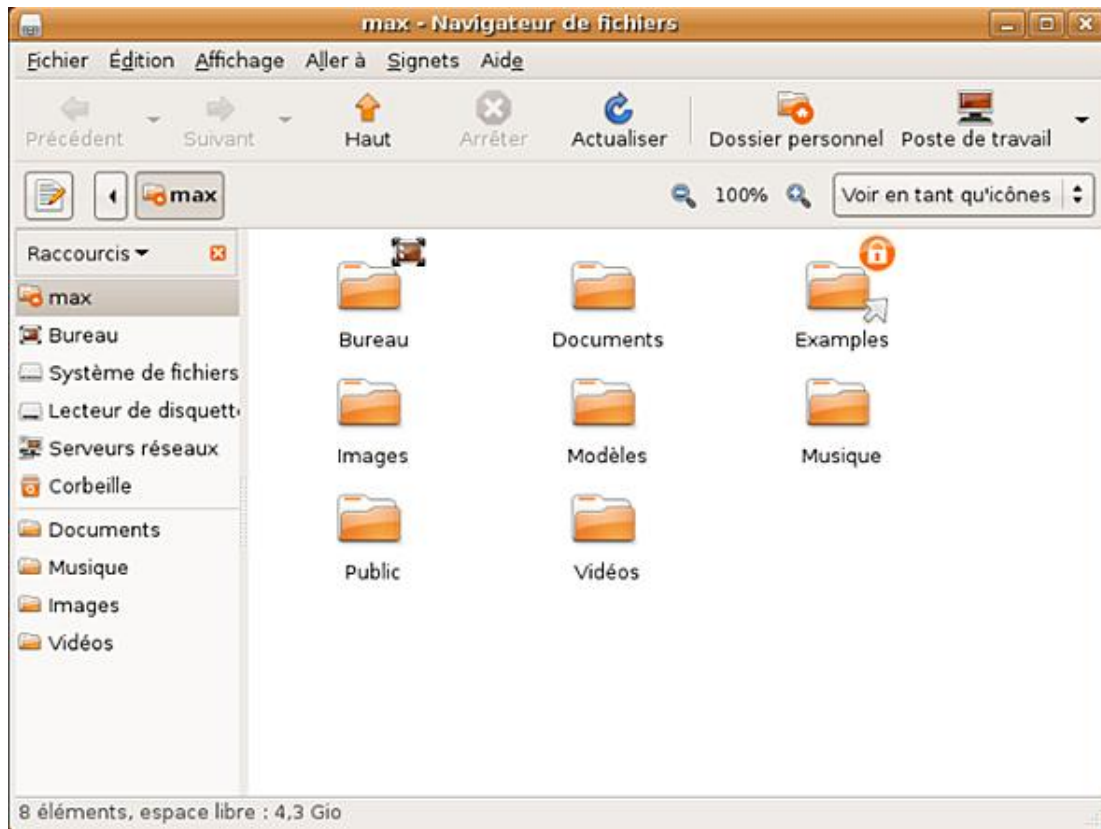
- Vérifiez l'endroit où vous êtes, votre identité de compte avec notamment l'UID et le GID par la commande `id`.
- Quelles sont les permissions en octal de votre répertoire personnel ? et celles du répertoire parent ?
- À quel groupe appartenez-vous ?
- Créez un fichier par la commande `touch liste.sh`.
- À qui appartient-il ? À quel groupe ?
- Quels sont les droits de ce fichier en octal ?
- Ajoutez le droit en écriture pour le groupe par la méthode octale.
- Enlevez le droit en écriture pour le groupe par la méthode symbolique.
- Le fichier `liste.sh` contiendra des commandes shell. Aussi, donnez-lui les permissions que l'on donne généralement à un programme, c'est-à-dire 755 et vérifiez-le.

Droits par l'interface graphique

1. Droits et espace de travail

a. Dossier personnel de l'utilisateur

Toujours dans le répertoire /home de l'arborescence, l'accès au dossier personnel de l'utilisateur en mode graphique sous Ubuntu se fait par les menus **Raccourcis - Dossier personnel** :



Le contenu comporte classiquement des dossiers thématiques **Documents**, **Images**, **Musique**, etc. que l'on retrouve aussi sous forme de raccourcis dans le menu général. Les icônes s'affichent quelquefois avec des éléments supplémentaires se positionnant à droite puis vers le bas (si plusieurs) :

- Les **emblèmes**, sous la forme d'un symbole dans un disque orange, destinés à préciser la nature d'un contenu (le dossier **Exemples** contenant divers fichiers de démonstration, installé par défaut par la distribution dans chaque répertoire utilisateur, le montre avec un petit cadenas signifiant une lecture seule).
- Les **déterminants**, sous la forme d'autres symboles, destinés à qualifier le contenu (tableau pour le bureau, flèche pour un lien...).

Pour afficher les fichiers et dossier cachés du répertoire, cochez la ligne **Afficher les fichiers cachés** du menu **Affichage**.

b. Modification des droits

La modification des droits en mode graphique est plus simple. À partir d'une session ouverte par un utilisateur, Il suffit d'ouvrir **Raccourcis - Dossier personnel** et sur un répertoire ou fichier de visualiser les propriétés par un clic droit sur le dossier. Les permissions se situent au niveau de l'onglet de même nom.

Exemple sur le dossier Images d'un utilisateur :



Notes :

- En mode graphique, le transfert de la propriété d'un dossier ou fichier se limite au groupe.
- Les associations d'ouverture avec une application se gère dans l'onglet **Ouvrir avec** du menu **Propriétés**.



Le contexte SELinux définissant une véritable politique d'accès suivant un modèle multiniveaux par des descripteurs de fichiers, sera vu dans le chapitre Sécurisation du système.

2. La commande **gsudo** et PolicyKit

Au sein d'une session graphique, une application se lance avec les droits associés à l'utilisateur. Pour effectuer des opérations d'ordre administrative, la voie classique consiste à utiliser la commande **gsudo** équivalent graphique de la commande **sudo** dans une console. **Gsudo** s'utilise donc pour ouvrir avec les droits administrateurs une application graphique, partant du principe qu'une modification en mode console reste toujours possible avec **sudo**.

Exemple avec le fichier `/etc/passwd` :

- Ouvrir le fichier par `gsudo gedit /etc/passwd` (application graphique)
- Ouvrir le fichier par `sudo vim /etc/passwd` (application texte)

Tâches administratives avec PolicyKit

Concernant la gestion administrateur en mode graphique, c'est-à-dire les applications se trouvant dans le menu **Système - Administration**, Ubuntu apporte un nouveau mécanisme appelé **PolicyKit** tendant à remplacer efficacement la commande `sudo` :

<http://hal.freedesktop.org/docs/PolicyKit/>

Cette interface logicielle basée sur **D-Bus**, accorde partiellement les droits administrateurs d'une application en fonction d'une tâche précise en non en totalité comme le faisait `sudo`.



Le projet D-Bus centralise, par le biais d'un enregistrement, les services d'autres applications. Il mutualise en quelque sorte les ressources des programmes entre eux. Couplé avec le service d'abstraction matérielle HAL (*Hardware Abstraction Layer*), il gère la notification d'événements du noyau et permet ainsi le branchement "à chaud" des périphériques comme les clés USB.

Un exemple concret : les mises à jour. La visualisation de la bonne synchronisation du système ne demande pas d'autorisation alors que la vérification, elle, la demande. Deux cas de figures :

- Soit l'application demande immédiatement une authentification avec privilèges.
- Soit des parties sont accessibles librement, d'autres le sont après déverrouillage.

Exemple sur les réglages du réseau :

Cette interface (`network-admin`), gérant les différentes cartes et connexions réseau de la machine, s'obtient par le menu **Système - Administration - Réseau**. La visualisation des éléments est libre, mais la modification impose de déverrouiller l'application par la mention d'un utilisateur possédant les droits pour cela :



La gestion du trousseau se fait avec l'application `polkit-gnome-authorization` obtenue par le menu **Système - Administration - Autorisations**. Vous pouvez définir de façon très fine le niveau d'implication des utilisateurs à la gestion du système et ce, pour différentes actions.

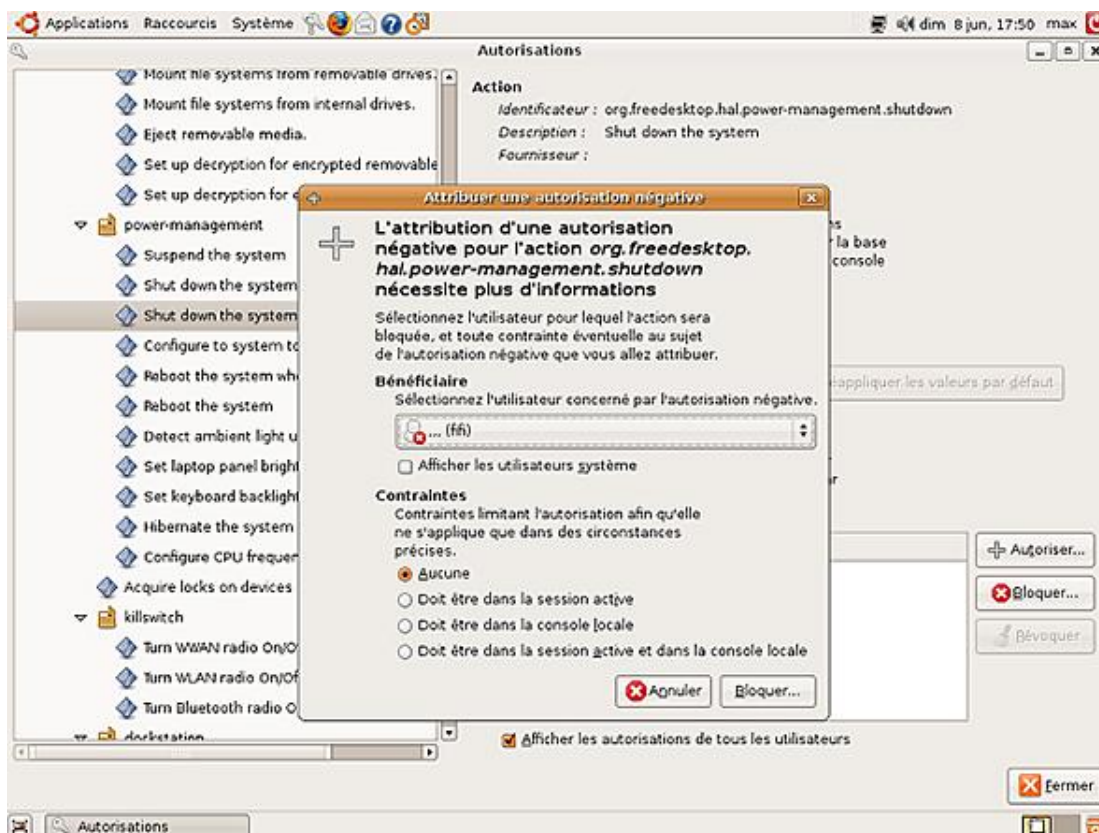
Suivant ce principe, vous pouvez par exemple interdire à un utilisateur d'arrêter le système et l'autoriser à un autre (branche **power-management**). Au niveau de la branche **policykit**, vous pouvez définir un autre utilisateur doté de super-pouvoirs dans le but de déléguer une partie des tâches administratives.

Ubuntu, avec PolicyKit, introduit le concept de gestion partagé de système.

Exemple :

On désire bloquer la possibilité à l'utilisateur `fifi` d'arrêter le système.

- Lancez l'application par **Système - Administration - Autorisations**.
- Cliquez sur l'action **Shut down the system** dans la branche **power-management**.
- Cliquez sur le bouton **Bloquer** et définissez **fifi** comme utilisateur "bénéficiaire" de l'autorisation négative. Au besoin, cochez la case sur l'affichage des utilisateurs système.
- Ne donnez pas de contrainte et validez par le bouton **Bloquer**.



Démarrage et premiers réglages

1. Réglages du chargeur de démarrage

Plus de renseignements peuvent être donnés au démarrage par l'intermédiaire des options passées au chargeur de démarrage GRUB . L'utilisation d'un éditeur de texte s'avère indispensable pour modifier celles-ci. Dans l'attente d'un éditeur plus conforme au statut d'un administrateur (**VIM** pour ne pas le nommer), vous utiliserez nano , éditeur simple et installé par défaut dans la version serveur.

L'éditeur de texte nano :

```
GNU nano 2.0.7      New Buffer

-

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^X Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^U Where Is   ^U Next Page  ^U UnCut Text ^T To Spell
```

Nano supporte les touches de mouvement du curseur et l'ensemble de ses commandes (faciles à comprendre) commence par la touche [Ctrl], ce qui se traduit en visuel par l'accent circonflexe.

a. Fichier /boot/grub/menu.lst

- Éditez le fichier (*note* : les lignes en commentaires commencent par le caractère dièse) :

```
nano /boot/grub/menu.lst
```

Voici une sélection des options importantes du fichier (pour un serveur) :

```
default 0
timeout 3
hiddenmenu
#color cyan/blue white/blue

title      Ubuntu 8.04.1, kernel 2.6.24-19-server
root       (hd0,0)
kernel     /boot/vmlinuz-2.6.24-19-server root=UUID=b8abd298-
af27-4557-b563-78ed1aece7f9 ro quiet splash
initrd     /boot/initrd.img-2.6.24-19-server
quiet

title      Ubuntu 8.04.1, kernel 2.6.24-19-server (recovery mode)
root       (hd0,0)
kernel     /boot/vmlinuz-2.6.24-19-server root=UUID=b8abd298-
af27-4557-b563-78ed1aece7f9 ro single
initrd     /boot/initrd.img-2.6.24-19-server

title      Ubuntu 8.04.1, memtest86+
root       (hd0,0)
```



```
kernel    /boot/memtest86+.bin
quiet
```



Attention : l'éditeur n'affiche pas la ligne complète lorsque celle-ci dépasse le cadre. Il indique en fin de ligne le caractère dollar ce qui peut prêter à confusion... Pour voir la ligne dans sa totalité, positionnez-vous dessus avec le curseur et appuyez sur la touche [Fin].

Pour les quatre premières lignes :

- `default 0` : numéro d'ordre de la ligne ce choix par défaut commençant par le mot-clé `title`, indice de départ à 0.
- `timeout 3` : nombre de secondes avant le démarrage automatique du choix par défaut.
- `hiddenmenu` : l'option affiche ou non le menu ; pour un serveur, cette option ne devrait jamais être activée au contraire d'un poste de travail.
- `color cyan/blue white/blue` : couleurs du menu ; si le bleu vous insupporte d'autres couleurs existent (`light-green/brown, blink-red/blue, etc.`).

Ensuite, le fichier se lit par paragraphe, avec en premier lieu :

- `title` : début d'une entrée ou choix système, il est suivi d'un texte modifiable (on peut le franciser) visible dans le menu.
- `root` : indique la partition racine à monter (une variation `rootnoverify`, ne tente pas de le faire par exemple pour des OS non accessibles par GRUB) ; tout disque chez GRUB porte l'indication `hd`, avec un indice de départ à 0 (premier disque), suivi d'une virgule et du numéro de la partition (toujours à l'indice de départ 0, 3 signifiant par exemple la quatrième partition du disque).

Les autres lignes se rapportent spécifiquement au système : `kernel` et `initrd` : pour Linux, elles indiquent respectivement l'image du noyau et celle du système à utiliser. Pour la ligne commençant par `kernel`, les paramètres :

- `ro`, indique en lecture seule (avant de monter le système sur le disque).
- `quiet`, donne moins d'informations : à enlever pour un serveur.
- `splash`, affiche lors du démarrage l'image graphique de progression (non disponible pour un serveur).

Réglages sur un serveur

- Effacez la ligne `hiddenmenu`, enlevez le commentaire pour la ligne `color`, enlevez à la ligne `kernel` les paramètres `quiet` et `splash`.
- Effacez toutes les lignes en commentaire pour avoir une vision plus claire du contenu.
- Sortez de l'éditeur par [Ctrl] **X**, validez la demande d'écriture des changements et redémarrez.

Réglages sur un poste de travail

Peu de choses à faire, à part réduire le `timeout` à 0 secondes pour accélérer le démarrage.

b. Cas d'un double système au démarrage

Essentiellement on l'a vu dans un chapitre précédent, cette technique s'utilise pour un amorçage proposant Windows et Linux. Les lignes supplémentaires tiennent toujours sous la forme d'un paragraphe classique d'une entrée dans GRUB :


```
title      Other operating systems:
root

title      Windows XP Media Center Edition
root      (hd0,0)
savedefault
makeactive
chainloader +1
```

Le premier paragraphe n'est là que pour la forme. Il ne sert à rien, si ce n'est qu'à séparer les entrées. Le deuxième paragraphe, outre les deux lignes `title` et `root`, comprend :

- `savedefault`, en liaison avec la ligne `default` avec comme paramètre `saved`. GRUB choisira, lors d'un prochain démarrage, l'entrée système sauvegardée (utile uniquement pour des tests).
- `makeactive`, positionne la partition comme active (nécessaire pour un système Windows).
- `chainloader`, charge le premier secteur de la partition indiquée par le paramètre `root`.

Pour terminer, le paquetage logiciel `grub-doc` apporte sur Ubuntu tous les renseignements complémentaires sur ce chargeur de démarrage.



Il ne reste plus qu'à voir comment résoudre les problèmes de démarrage, ce sera vu dans le chapitre Maintenance de base du système.

2. Connexion au réseau

Le branchement au réseau de l'entreprise ou à Internet constitue une condition *sine qua none* du bon fonctionnement de la distribution Ubuntu par les mises à jour ou l'installation de logiciels via les dépôts.

a. Fichier `/etc/network/interfaces`

C'est le fichier de base pour la configuration des interfaces réseaux sur une distribution de type serveur. Il sert de sources d'informations pour les programmes `ifup` et `ifdown` permettant respectivement d'activer et de désactiver une interface réseau. Chaque interface suit le plan de déclaration suivant :

```
auto|allow-*|mapping INT
iface INT inet loopback|static|dhcp|ppp
```

Le paramètre `auto` identifie le matériel présent, `allow-hotplug` ou `allow-auto` autorisent une activation par d'autres processus, `mapping` permet la fabrication d'alias.

`Loopback` identifie la boucle locale et se doit d'être toujours présente. `Static` et `dhcp` donne la méthode d'adressage de la carte. **PPP** (*Point to Point Protocol*) traite de l'adressage par un modem. Un adressage statique comporte d'autres renseignements comme le montre l'exemple d'un système comportant deux cartes réseau `eth0` et `eth1`, l'une en `dhcp`, l'autre en statique :

```
# Boucle locale
auto lo
iface lo inet loopback

# Eth0
auto eth0
iface eth0 inet dhcp

# Eth1
auto eth1
iface eth1 inet static
    address 192.168.3.1
    netmask 255.255.255.0
    network 192.168.3.0
    broadcast 192.168.3.255
```

La ligne gateway suivie de l'IP d'une passerelle peut s'ajouter à la suite de la ligne broadcast. Dans l'exemple, on suppose que la passerelle (gateway) est fournie par la configuration DHCP.



L'attribution de plusieurs adresses réseaux à la même carte porte plus sur l'administration réseau, aussi cette fonctionnalité ne sera pas vue ici.

Cas d'une connexion sans fil

Pour le Wi-Fi, la connexion par clé WEP (*Wired Equivalent Privacy*) apporte une faible sécurité. On lui préfère la technique du **WPA** (*Wi-Fi Protected Access*), d'un cryptage plus sûr. Sur Ubuntu, le service wpa_supplicant se charge de la connexion sans fil.

Exemple pour une interface Wi-Fi se nommant wlan0 :

```
auto wlan0
iface wlan0 inet dhcp
    wpa-driver wext
    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
```

La ligne wpa-conf indique au système de trouver la configuration dans le fichier adéquat. Le paramètre wpa-driver, optionnel, utilise le pilote générique wext (à changer suivant la configuration et si la présence de la ligne est demandée).

La suite se passe au niveau du fichier de configuration wpa_supplicant.conf et, parce que la connexion Wi-Fi part du principe de l'itinérant, voyez l'exemple avec commentaires d'un fichier avec deux configurations, pour un portable nomade :

```
# Emplacement du programme de traitement
ctrl_interface=/var/run/wpa_supplicant
# Groupe Linux pour le contrôle
ctrl_interface_group=root
# Mode de sélection (classique) du point d'accès
ap_scan=1

# Réseau de type familial avec clé WPA
network={
    # Identification du réseau
    ssid="DUNE"
    # Scanne les requêtes du réseau dans un but d'actualisation
    scan_ssid=1
    # Authentification du réseau
    key_mgmt=WPA-PSK
    # Cryptage des données
    pairwise=TKIP
    # phrase de mot de passe
    psk="la mer est calme ce soir"
}

# Réactivation rapide pour EAP
fast_reauth=1
# Version de transport pour EAP
eapol_version=1
# Réseau de type professionnel avec contrôle par certificats
network={
    ssid="ADV"
    # Pas de scan de requêtes (inutile)
    scan_ssid=0
    # Type d'infrastructure, managed par défaut
    mode=0
    key_mgmt=WPA-EAP
    pairwise=TKIP
    # Système d'authentification, OPEN pour WPA
    auth_alg=OPEN
    # Authentification par certificats
    eap=TLS
    # Identité et emplacement des certificats
    identity="chamillg"
    ca_cert="/etc/wpa_supplicant/certificats/root-ca.crt"
```

```
client_cert="/etc/wpa_supplicant/certificats/chamillg.crt"
private_key="/etc/wpa_supplicant/certificats/chamillg.key"
}
```

Toutes ces options et d'autres exemples se retrouvent dans la documentation et le manuel en ligne.

Commandes utiles pour le réseau

ping

Cette commande connue de tous existe sur tous les systèmes. Elle vérifie si une machine distante répond :

```
ping <IP>
```

On peut aussi utiliser le nom de la machine, si celle-ci est renseignée dans le fichier `/etc/hosts` contenant les correspondances "en dur" entre une adresse IP et un nom de machine ou dans un serveur DNS. La commande ne s'arrête pas, utilisez alors [Ctrl] **C**.

ifconfig

Autre commande essentielle, `ifconfig` affiche la configuration réelle des cartes réseau, mais aussi change celles-ci "à la volée".

Exemple :

```
ifconfig eth0 192.168.0.2 netmask 255.255.255.0 broadcast 192.168.0.255
```

Le `netmask` et `broadcast` proposés sont ceux correspondant à une adresse de classe C. Au redémarrage de la machine, ce changement sera perdu.

arp

Cette commande met en correspondance des adresses IP avec des adresses **MAC** (*Media Access Control address*). Les options possibles importantes sont :

- `arp -a` : toutes les entrées ARP de la table
- `arp -d machine` : supprimer une entrée de la table
- `arp -s machine mac` : ajouter une nouvelle entrée dans la table

route

Cette commande affiche, ajoute ou enlève les routes se trouvant déclarées sur votre machine. Ainsi pour indiquer à votre machine où aller trouver les adresses qui ne sont pas les adresses de votre réseau local, vous devez lui indiquer la passerelle (gateway) vers laquelle elle doit envoyer tous les paquets. Pour voir les routes indiquées :

- `route -n` : on peut aussi utiliser la commande `netstat -nr`

L'option `-n` permet de ne pas avoir la résolution des noms.

Exemple pour ajouter une route par défaut :

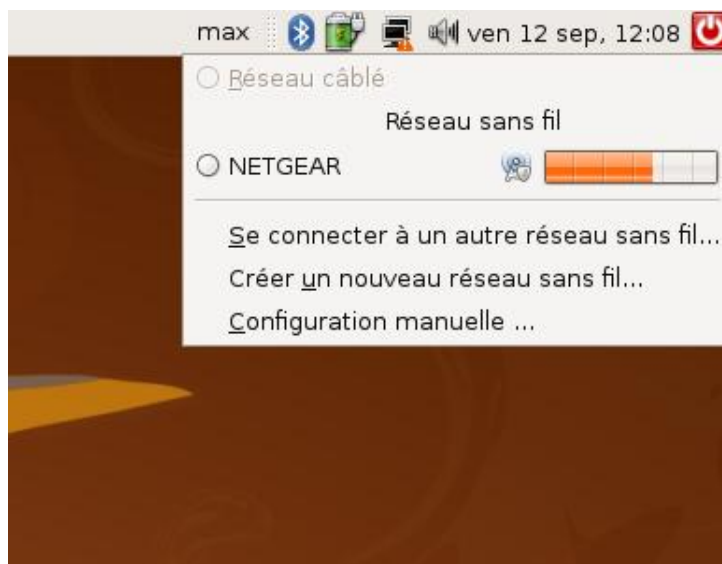
```
route add default gateway 192.168.0.1
```

En clair : la passerelle vers qui j'envoie tous les paquets qui ne sont pas pour le réseau local. La passerelle correspond la plupart du temps à votre routeur. Pour plus de renseignements sur la syntaxe, voir le manuel en ligne.

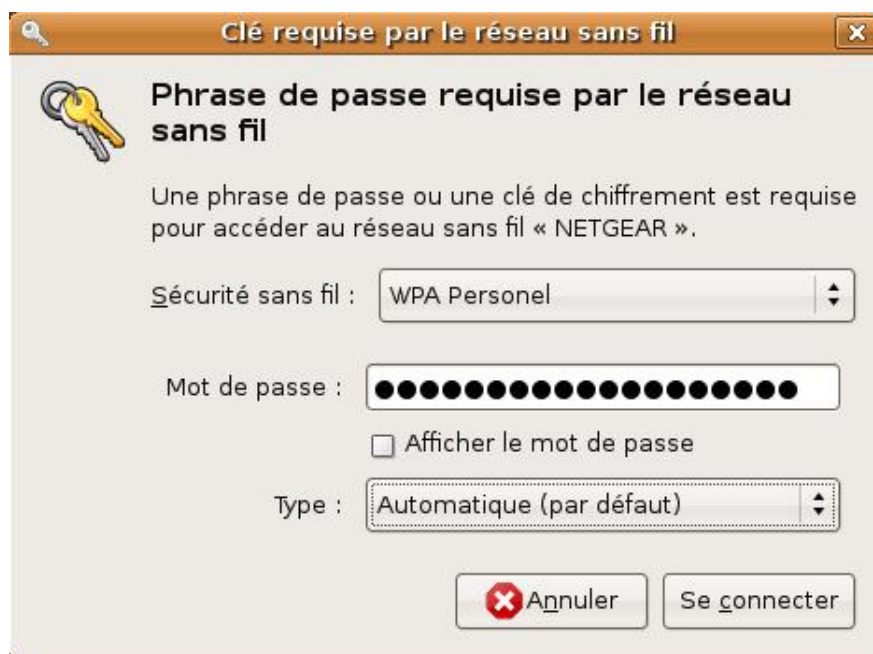
b. Network Manager

Cet applet (GNOME ou KDE) se charge par défaut avec la version poste de travail et gère les connexions réseaux automatiquement. Respectueux du système, il s'efface devant une connexion manuelle écrite dans le fichier `/etc/network/interfaces`.

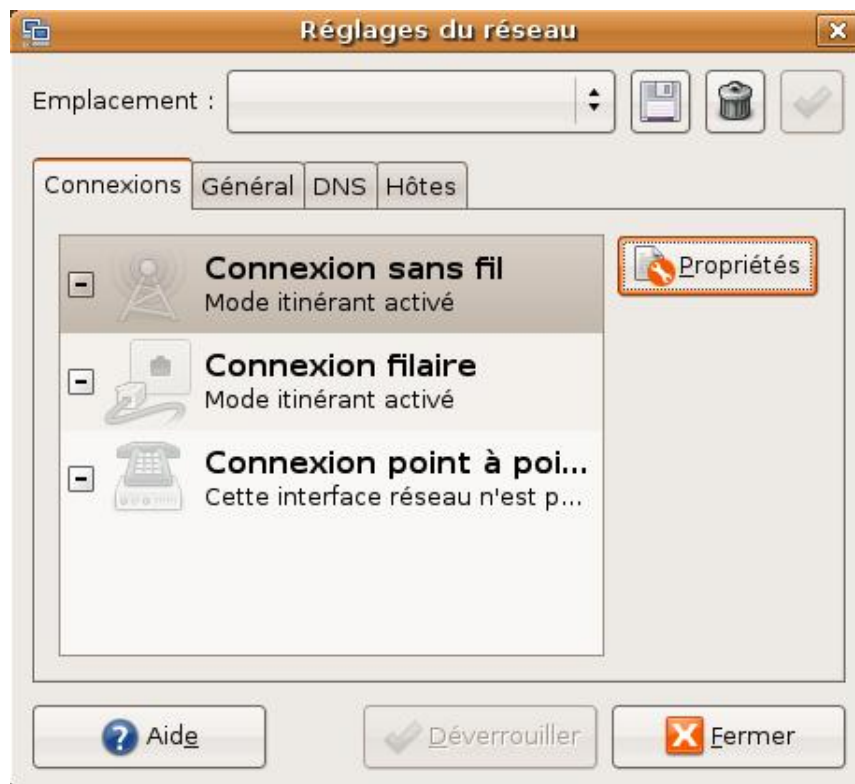
Lors d'une première connexion, Network Manager (clic droit de la souris sur l'icône) détecte les réseaux sans fil mais ne s'y connecte pas :



La connexion s'établit après avoir fourni les paramètres d'authentification :



La connexion s'enregistre pour les sessions suivantes. Il reste toujours la ressource de modifier les paramètres manuellement :



3. Réglages particuliers

Ces réglages, au nombre de deux, s'appliquent plutôt à un poste de travail lorsque l'administrateur désire adapter le visuel des ordinateurs à la signalétique de l'entreprise.

a. Changement de l'image splash de GRUB

La configuration d'un poste de travail avec affichage du menu GRUB ne comporte pas par défaut d'image de fond. L'image se définit obligatoirement au format spécial XPM (pixmap X) :

- format d'image "visible" par un éditeur de texte
- résolution : 640 x 480 pixels
- bits par pixels/couleur : 4/16 (RVB)

L'image est compressée, ce qui donne en fait une extension à `xpm.gz`. Ubuntu possède une collection d'images de démonstration :

```
sudo aptitude install grub-splashimages
```

Pour changer l'image de fond, deux lignes supplémentaires apparaissent dans le fichier `/boot/grub/menu.lst` : celle ayant trait à l'image et une autre pour la couleur du cadre menu (facultative) :

```
default 0
timeout 10
splashimage=(hd0,0)/boot/grub/splashimages/fiesta.xpm.gz
foreground FF0000

title      Ubuntu 8.04.1, kernel 2.6.24-19-generic
root       (hd0,0)
kernel     /boot/vmlinuz-2.6.24-19-generic root=UUID=b8abd298-
af27-4557-b563-78ed1aace7f9 ro quiet splash
initrd     /boot/initrd.img-2.6.24-19-generic
```

```

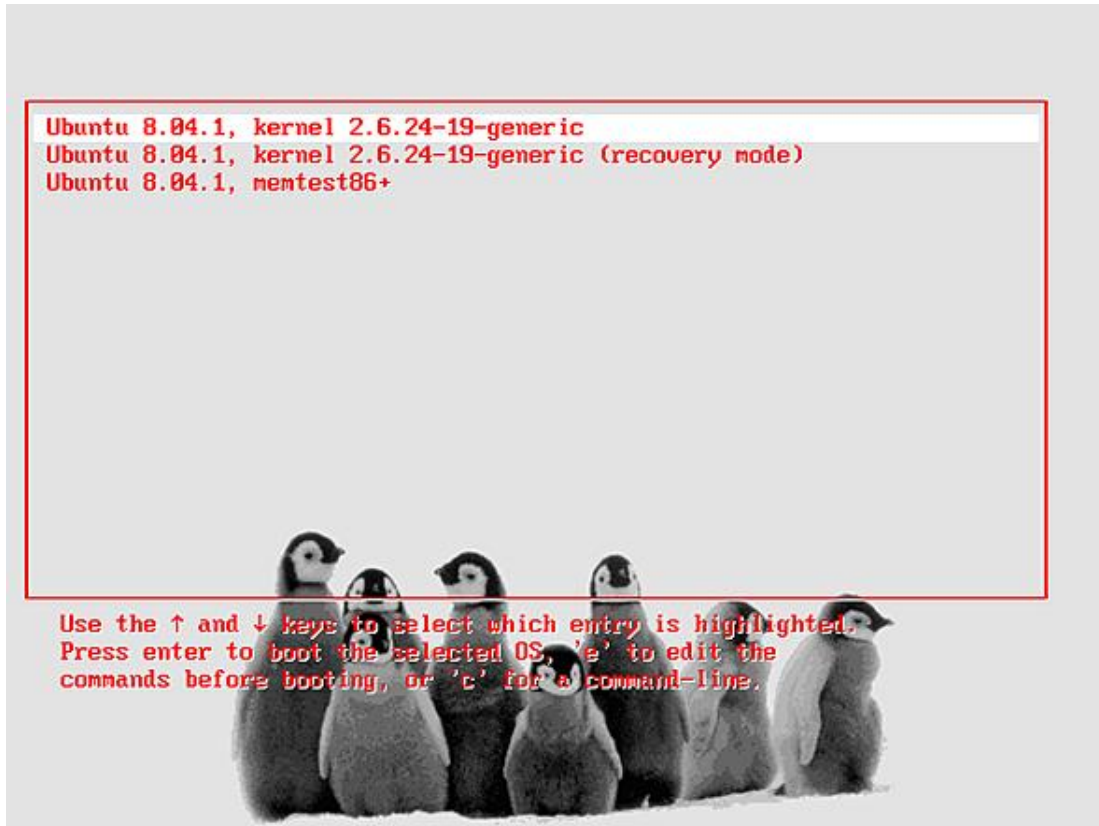
quiet

title      Ubuntu 8.04.1, kernel 2.6.24-19-generic (recovery mode)
root       (hd0,0)
kernel     /boot/vmlinuz-2.6.24-19-server root=UUID=b8abd298-
af27-4557-b563-78ed1aece7f9 ro single
initrd     /boot/initrd.img-2.6.24-19-generic

title      Ubuntu 8.04.1, memtest86+
root       (hd0,0)
kernel     /boot/memtest86+.bin
quiet

```

Les images compressées se trouvent dans le répertoire `/boot/grub/splashimages` et il est tout à fait possible, à l'aide d'un éditeur (GIMP par exemple), de créer pour une entreprise sa propre image personnalisée. Voici comme exemple l'utilisation de l'image `fiesta` avec un cadre rouge :



D'autres réglages sont possibles. Consultez pour cela la documentation de GRUB :

<http://www.gnu.org/software/grub/manual/>

b. Changement de thème pour GDM

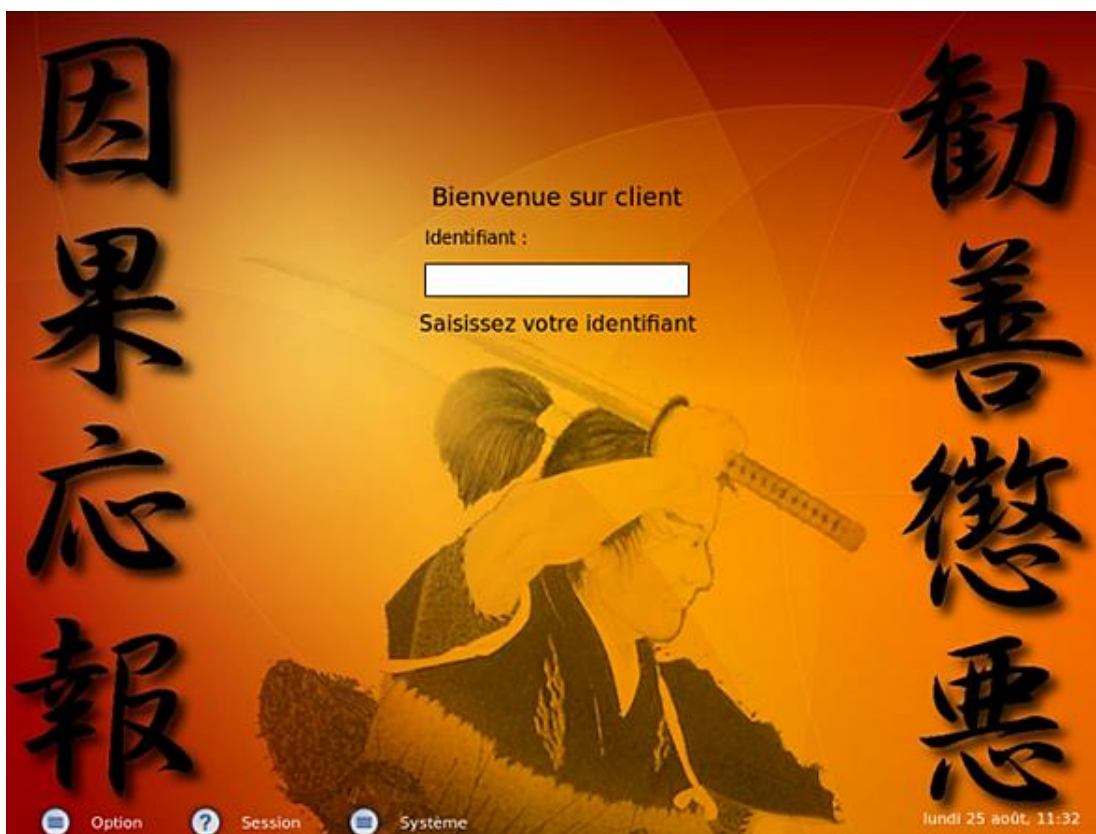
Le changement de thème est simple. Outre les thèmes déjà proposés, le téléchargement de nouveaux thèmes aboutit à un paquet sous forme d'archive (`tar.gz`) qu'il suffit d'un "glisser/déplacer" (*drag and drop*) sur l'onglet **Locale** au niveau de la liste des thèmes pour l'installer. Vous trouverez des nouveaux thèmes à cette adresse : <http://art.gnome.org>

Exemple avec le thème Orange Musashi :

- Téléchargez le thème **GDM-OrangeMurashi.tar.gz** dans la catégorie Desktop **Themes - Login Manager**.
- Faites-le glisser du bureau à la liste des thèmes, menus **Administration - Fenêtre de connexion**, onglet **Locale**.
- Sélectionnez-le et redémarrez la machine.



Vérifiez bien la bonne sélection du thème car la première fois le comportement de GDM ne prend pas forcément en compte le changement.



c. Autres réglages

Connexion automatique sans donner le mot de passe

La connexion automatique cochée dans l'onglet **Sécurité** avec sélection d'un utilisateur nécessite un redémarrage du service GDM pour être prise en compte. Il est évident que, dans ce cas, vous ne voyez plus l'écran et le thème GDM.

Résolution de l'écran GDM

Il arrive quelquefois d'avoir une résolution d'écran au niveau de GDM trop grande et qui ne correspond pas à celle du bureau. Il convient de vérifier deux choses :

- la taille de l'image utilisée pour le thème en fond d'écran afin qu'elle soit adaptée à la résolution souhaitée.
- la résolution maximale limitée à celle désirée dans le fichier `xorg.conf` au niveau de la sous-section `Display` (voir le chapitre Session de travail en mode graphique).

Utiliser une autre interface

Un seul gestionnaire graphique de session est utilisé par défaut, indépendamment de leur nombre (`xdm`, `gdm` et `kdm`). Les gestionnaires s'installent par défaut avec leur environnement attribué : `kdm` pour KDE, etc. Par contre, `opter` - non conseillé - pour `kdm` dans un environnement GNOME ne permettra plus d'utiliser `gdmsetup` car il détectera un gestionnaire en fonctionnement. Pour remettre le gestionnaire par défaut, on passe par la commande d'administration :

```
update-alternatives --config x-session-manager
```

Le choix de l'interface s'effectue en tapant le numéro du gestionnaire de session `/usr/bin/gnome-session` ou `/usr/bin/startkde`.

Sources de paquets logiciels

1. Principe des paquetages

La gestion des logiciels sous Ubuntu est centralisée sur des serveurs de dépôts (voir le chapitre Préalable à l'installation) et se gère par un gestionnaire, appelé gestionnaire de paquets. Comme toujours sous Linux, il n'y a pas une mais plusieurs manières de construire, obtenir et gérer ces paquets logiciels.

Ubuntu utilise la philosophie Debian en matière de paquets. Aussi un logiciel aura pour extension `.deb` (Rappel : ne pas utiliser de logiciels Debian pour une distribution Ubuntu, l'extension est la même mais pas son contenu). Son nom renseigne sans ambiguïté sur son numéro de version, sa distribution (parfois) et sa catégorie (processeur i386).

Exemple :

```
dhcp3-common_3.0.6.dfsg-1ubuntu9_i386.deb
```

a. Manuellement avec le fichier `sources.list`

Dépôts indispensables

Bien régler son fichier de sources de logiciels fait partie des tous premiers réglages de l'administrateur. Deux adresses sont couramment utilisées en France :

- `fr.archive.ubuntu.com` (serveur Oléane).
- `security.ubuntu.com` (serveur canonical à Auckland).

Comme indiqué dans le chapitre Préalable à l'installation, il est parfois utile de changer de sources car il arrive que le serveur Oléane soit surchargé. Quoi qu'il en soit, il est très important de disposer d'un fichier de sources bien réglé : en voici un modèle minimal :

```
# Sources Hardy Heron 8.04.1

# Sections principale et à diffusion restreinte
deb http://fr.archive.ubuntu.com/ubuntu/ hardy main restricted
deb http://fr.archive.ubuntu.com/ubuntu/ hardy-updates main restricted
deb http://security.ubuntu.com/ubuntu hardy-security main restricted

# Sections universe et multiverse
deb http://fr.archive.ubuntu.com/ubuntu/ hardy universe multiverse
deb http://fr.archive.ubuntu.com/ubuntu/ hardy-updates universe multiverse
deb http://security.ubuntu.com/ubuntu hardy-security universe multiverse
```

Le fichier prend en compte les quatre sections sur deux paragraphes et pour chaque type de sources : **normales, nouvelles, mises à jour de sécurité**. Volontairement compact, certains administrateurs lui préfèrent une version plus détaillée pour chaque section : c'est une affaire de goût !

Voici maintenant les lignes à rajouter (avec les droits administrateurs bien sûr) en cas de besoin des sources de logiciels (on peut les intégrer au fichier et les laisser commentées si on ne les utilise pas) :

```
# Sections principale et à diffusion restreinte (sources)
# A activer en cas de besoin en décommentant la ligne
#deb-src http://fr.archive.ubuntu.com/ubuntu/ hardy main restricted
universe multiverse
#deb-src http://fr.archive.ubuntu.com/ubuntu/ hardy-updates main
restricted universe multiverse
#deb-src http://security.ubuntu.com/ubuntu hardy-security main
restricted universe multiverse
```

La différence réside dans la dénomination du paquet `deb-src` au lieu de `deb`, avec cette fois-ci la démonstration des quatre sections en même temps. Les sources permettent la compilation d'un logiciel dans un but d'adaptation à la plate-forme (voir le chapitre Maintenance avancée du système).

Dépôts secondaires

À côté des dépôts indispensables, se trouvent les dépôts des logiciels **rétro-portés** (*backports*) c'est-à-dire des logiciels de la prochaine version Ubuntu adaptés à la version courante :

```
# Logiciels backports
# A activer en cas de besoin en décommentant la ligne
#deb http://fr.archive.ubuntu.com/ubuntu/ hardy-backports main
restricted universe multiverse
#deb-src http://fr.archive.ubuntu.com/ubuntu/ hardy-backports main
restricted universe multiverse
```

Il existe aussi les logiciels **commerciaux** payants en partenariat avec la société Canonical :

```
# Logiciels commerciaux
# A activer en cas de besoin en décommentant la ligne
#deb http://archive.canonical.com/ubuntu hardy partner
#deb-src http://archive.ubuntu.com/ubuntu hardy partner
```

Autre possibilité : les dépôts "Proposed" apportant des **logiciels à tester** ou des **mise à jour non encore intégrées** dans les dépôts principaux. On peut comparer ceux-ci à la déclinaison **Sid** de la distribution Debian :

```
# Logiciels proposed
# A activer en cas de besoin en décommentant la ligne
#deb http://fr.archive.ubuntu.com/ubuntu/ hardy-proposed main
restricted universe multiverse
#deb-src http://fr.archive.ubuntu.com/ubuntu/ hardy-proposed main
restricted universe multiverse
```

Tout ces dépôts, outre le fait qu'il n'y a pas à proprement parlé de mises à jour, sont sous la responsabilité de l'administrateur car ils peuvent induire des problèmes sur le système (surtout le premier !). Le risque est important pour un serveur, moindre sur un poste de travail et peut contribuer à résoudre des situations de pilotes non encore adaptés à un matériel récent.

Dépôts accessoires

Enfin, on trouve des dépôts spécifiques généralement liés à une application (codecs multimédia par exemple) ou pour des raisons légales (dépôt **Médibuntu**). Ces dépôts se structurent de la même façon que les autres. Exemple de **DRBL** (*Diskless Remote Boot in Linux*) pour la fourniture d'un environnement sans disque :

```
# Sources DRBL
deb http://free.nhcc.org.tw/ubuntu hardy main restricted universe multiverse
deb http://free.nhcc.org.tw/drbl-core drbl stable
```

Vous devrez alors importer une clé **GPG** (*GNU Privacy Guard*) chargée de vérifier l'authenticité des transactions car ces logiciels ne viennent pas des dépôts officiels. Deux étapes : la récupération sur le serveur par l'outil `wget` et l'installation par l'utilitaire `apt-key`. Ce qui donne toujours pour l'exemple DRBL :

```
sudo wget http://drbl.nhcc.org.tw/GPG-KEY-DRBL
```

```
sudo apt-key add GPG-KEY-DRBL
```

La première commande récupère la clé, tandis que la deuxième ajoute à la liste la clé déclarée fiable.

Autre exemple : le dépôt Médibuntu qui propose des logiciels ne pouvant être inclus dans la distribution (droits des licences, disparités légales entre pays, etc.) :

```
sudo wget http://fr.packages.medibuntu.org/medibuntu-key.gpg
```

```
sudo apt-key add medibuntu-key.gpg
```

Et l'ajout du dépôt dans le fichier `sources.list` :

```
# Sources Medibuntu
deb http://fr.packages.medibuntu.org/ hardy free non-free
#deb-src http://fr.packages.medibuntu.org/ hardy free non-free
```

Dès lors, une application comme le célèbre Skype (logiciel propriétaire de voix IP) est possible après une mise à jour nécessaire.

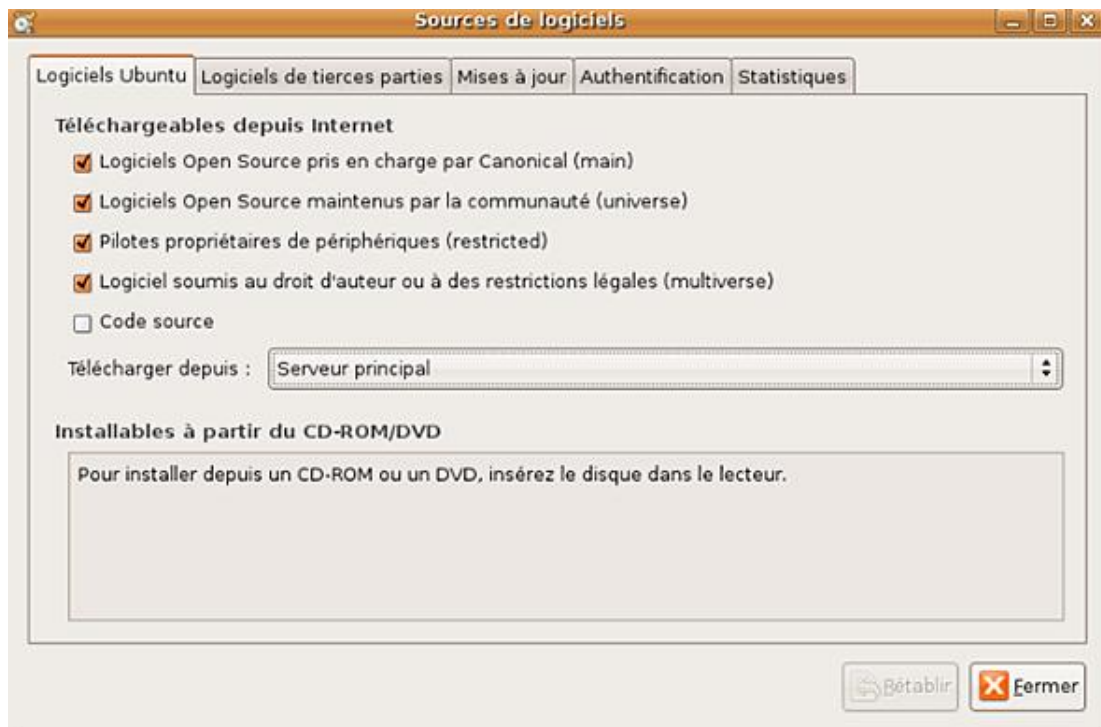


Une application graphique gère plus simplement le chiffrement et les "trousseaux" de clefs : seahorse-preferences. Elle sera vue dans le chapitre Session de travail en mode graphique.

b. Sources et interface graphique

Une application graphique (update-manager) règle précisément toutes ces options par le menu **Système - Administration - Sources de logiciels**. L'avantage de l'interface graphique est qu'elle permet de choisir facilement parmi une liste un autre serveur que le serveur national. Les onglets présentés dans l'application sont au nombre de cinq :

- **Logiciels Ubuntu** : donne le choix des quatre sections (main, universe, restricted, multiverse), des sources et du serveur de téléchargement. Une fonction permet de rechercher le meilleur serveur mais, après plusieurs tests, le doute est permis... (ce qui est vrai à un instant T peut ne plus l'être à T+1). Préférez un serveur en relation avec votre fournisseur d'accès (votre FAI est Free : choisissez ftp.free.fr) ou remettez-vous en au serveur national (fr.archive.ubuntu.com).
- **Logiciels de tierces parties** : indique l'adresse de serveurs extérieurs pour des logiciels spécifiques. L'adresse d'un serveur miroir local s'écrit aussi ici avec le même format de ligne vu dans le fichier sources.list (exemple : deb http://192.168.3.3/hardy hardy main restricted universe multiverse).
- **Mises à jour** : concerne les quatre niveaux de mises à jour (security, updates, proposed, backports).
- **Authentification** : contient les clés de signatures fiables, soit celle du CD-Rom d'installation et du ou des serveurs utilisés.
- **Statistiques** : laisse le choix de participer à l'étude statistique d'utilisation des paquets : à ne pas utiliser si vous êtes peu concerné par le projet Ubuntu et un peu paranoïaque...

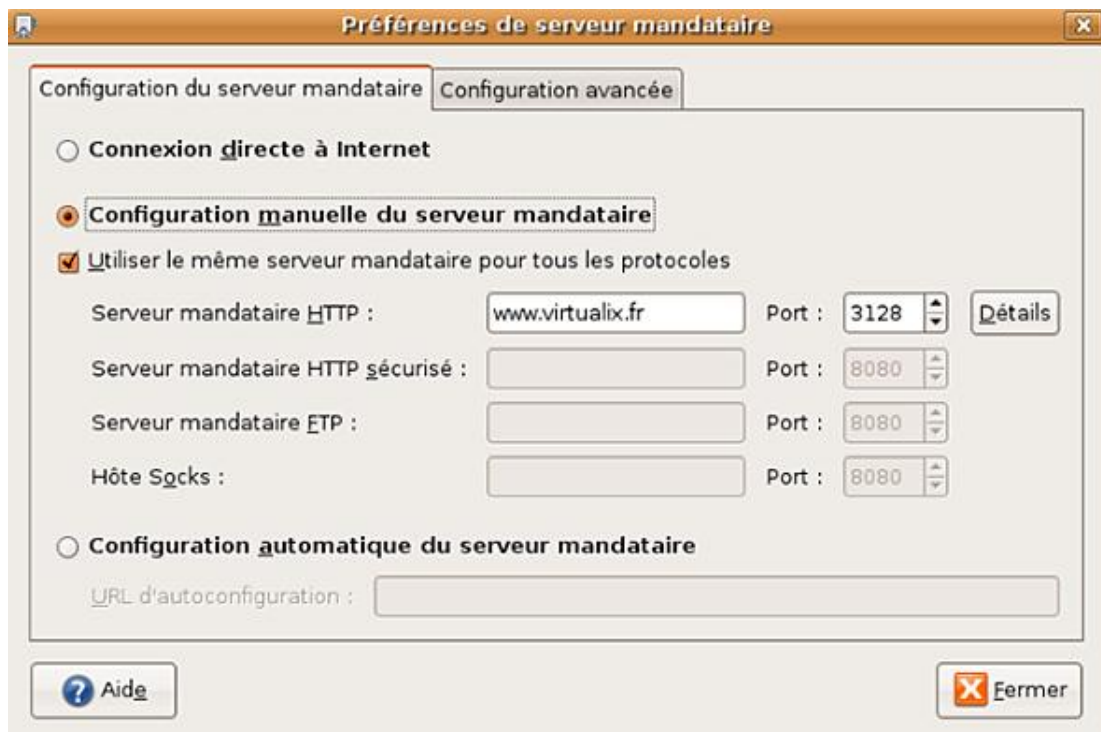


c. Cas d'un serveur mandataire

S'il existe sur le réseau un serveur mandataire (proxy), un réglage supplémentaire est à mettre dans un fichier (à créer) nommé /etc/apt/apt.conf. En voici un exemple où le serveur proxy se nomme www.virtualix.fr, port 3128 (pas de demande d'authentification utilisateur) :

```
Acquire::http::Proxy "http://www.virtualix.fr:3128";
```

Cette démarche s'applique sur un serveur. Dans le cas d'une Ubuntu en mode graphique (et seulement dans ce cas), la gestion du serveur mandataire passe par le menu **Système - Préférences - Serveur mandataire** :



Cette configuration ne fonctionne plus si vous sortez de l'environnement graphique, auquel cas il faut écrire le fichier `/etc/apt/apt.conf`. L'environnement pris en compte est celui de GNOME et sa suite **Evolution**. Attention : un navigateur comme **Firefox** se paramètre individuellement et indépendamment dans l'application par le menu **Edition - Préférences**, onglets **Avancé/Réseau**, bouton **Paramètres**.

2. Interfaces de gestion de paquets

L'administrateur ne choisit pas une seule interface de gestion de paquets mais plusieurs en fonction de son besoin. Classée de la plus spartiate à la plus conviviale, chaque interface comporte des avantages. Il n'est pas question ici de fournir un *motus operandi* complet de chaque interface mais d'en montrer tactiquement les principales utilisations. L'approche dans cet ouvrage se veut plus didactique que théorique, aussi vous verrez que :

- la commande détermine le choix de l'interface la mieux adaptée.
- seules les meilleures interfaces sont utilisées.

Suivant ce principe, l'utilitaire `dselect` "front-end" trop orienté Debian ne sera pas évoqué ou des bizarreries comme **Gdebi**, interface graphique de **dpkg** qu'il vaut mieux oublier...



Ces commandes, essentiellement d'ordre administratif pour un serveur, se tapent en mode console sous le compte du `root` ou, à défaut, en précédant la commande par le mot-clé `sudo`. La gestion graphique, réservée à un poste de travail, utilise l'outil **Synaptic**.

a. Utilitaire **dpkg**

Premier utilitaire dit de bas niveau de gestion de paquets **dpkg** (*debian package*) s'utilise pour installer un paquet le plus souvent "solitaire" c'est-à-dire sans dépendances à gérer. Auquel cas une interface plus évoluée est nécessaire. Ensuite, l'utilité de `dpkg` tourne autour de sa capacité à donner des informations.

Commandes usuelles

Rechercher un ou plusieurs paquets :

```
dpkg -l debconf
```

Variante avec un motif (tous les paquets commençant par deb).

```
dpkg -l deb*
```

Une description de tous les paquets se trouve dans `/var/lib/dpkg/available`.

Installer un paquet (exemple avec le logiciel de virtualisation **VirtualBox** dans sa version non OSE c'est-à-dire non OpenSource) :

```
dpkg -i virtualbox_1.6.0-30421-Ubuntu_hardy_i386.deb
```

Les options `-r` et `-P` suppriment et purgent respectivement le paquet avec la commande `dpkg`.

Connaître l'appartenance d'un fichier à un paquetage installé :

```
dpkg -S /etc/apache2/apache2.conf
```

Cette commande retourne `apache2.2-common`, paquet du serveur Web Apache.

Connaître la liste complète des paquetages installés :

```
dpkg --get-selections
```

Si l'on effectue une redirection de la commande dans un fichier, cette commande réinstalle une distribution avec pour copie conforme l'ensemble des éléments :

```
dpkg --get-selections > liste_paquetages.txt
```

La reprise :

```
dpkg --get-selections < liste_paquetages.txt
```

```
apt-get dselect-upgrade
```

b. Utilitaire Apt

Utilitaire phare et incontournable de la gestion de paquets même si l'équipe Debian demande à utiliser **Aptitude** plutôt que **Apt** (*Advanced Packaging Tool*) pour la raison d'une meilleure gestion des dépendances. Mais les habitudes sont là et beaucoup d'administrateurs soutiennent encore l'utilisation d'Apt et de sa commande principale : `apt-get`.

Comme je soutiens l'utilisation d'Aptitude, certaines commandes ne seront pas volontairement présentées (exemple : installation de paquets). Attention : le choix de l'outil importe peu mais il est impératif, sous peine de problème, dans la base des paquets, **de ne pas mélanger les deux méthodes**. Autrement dit si vous utilisez `apt-get` : gardez cette méthode !

Recherche d'un paquetage ou d'un fichier appartenant à un paquetage non installé :

```
apt-cache search dos2unix
```

La recherche par `apt-cache` donne de meilleurs résultats que par Aptitude. L'exemple de `dos2unix` le montre. Cet utilitaire utilisé pour adapter les fichiers texte du format Windows au format Unix (principalement pour les caractères de fin de ligne comme les retours chariots) appartient au paquetage `tofrodos`. La commande `apt-cache` retourne deux paquets alors qu'Aptitude ne trouve rien !



Le nom passé dans la commande peut être tronqué, dans l'exemple `dos2` retournera la même chose ; cela est utile si l'on ne connaît pas exactement la syntaxe de ce que l'on cherche.

Installation d'une nouvelle clé GPG :

```
apt-key add medibuntu-key.gpg
```

Ajoute la clé à la liste des clés fiables. Le paramètre `list`, seul, affiche la liste du trousseau (fichier `/etc/apt/trusted.gpg`) alors que le paramètre `del` supprime une clé de cette liste.

c. Utilitaire Aptitude

Promu utilitaire principal de gestion de paquets, **Aptitude** dans sa version en mode commande (l'interface semi-graphique n'apporte pas grand chose de plus) remplace `apt-get` et ne change pas beaucoup les usages. Il apporte par contre une meilleure gestion des dépendances, serpent de mer de toute interface de gestion de paquets.

Installe un paquet logiciel en gérant les dépendances liées :

```
aptitude install paquet
```

À l'inverse, cette option désinstalle un paquet logiciel :

```
aptitude remove paquet
```

Cette variante désinstalle un paquet logiciel et tente de supprimer en plus les fichiers de configuration et les répertoires créés sauf s'ils ne sont pas vides :

```
aptitude purge paquet
```

Cette commande fondamentale met à jour la liste des paquets logiciels disponibles par rapport à la liste contenue dans `/etc/apt/sources.list` :

```
aptitude update
```

Mettre à jour le système de façon très propre avec uniquement les paquets logiciels installés ; de plus, seuls les paquets non utilisés seront désinstallés :

```
aptitude safe-upgrade
```

Cette autre option met à jour le système en enlevant les anciennes versions des paquets installés à la différence de la commande précédente. Réputée plus "abrasive" pour le système, elle est quand même à employer par rapport à `safe-upgrade` car elle rend le système plus cohérent :

```
aptitude full-upgrade
```

Donner des informations sur un paquet :

```
aptitude show paquet
```

```
root@ubuntu:~# aptitude show squid
Package: squid
State: not installed
Version: 2.6.18-1ubuntu3
Priority: optionnel
Section: web
Maintainer: Ubuntu Core Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Uncompressed Size: 1622k
Depends: adduser, libc6 (>= 2.4), libdb4.6, libldap-2.4-2 (>= 2.4.7), libpam0g (>= 0.
        logrotate (>= 3.5.4-1), lsb-base, netbase, squid-common (>= 2.6.18-1ubuntu3)
        1.0-11ubuntu1)
PreDepends: debconf (>= 1.2.9) | debconf-2.0
Suggests: logcheck-database, resolvconf (>= 0.40), smbclient, squid-cgi, squidclient,
Conflicts: sarg (< 1.1.1-2), squid-novm
Replaces: squid-novm
Description: Internet object cache (WWW proxy cache)
 This package provides the Squid Internet Object Cache developed by the National Labo
 Applied Networking Research (NLNR) and Internet volunteers.
Homepage: http://www.squid-cache.org/
```

L'exemple montre des renseignements sur le paquet **Squid** (logiciel pour la création d'un serveur mandataire). Elle affiche aussi d'autres renseignements intéressants : l'état, les dépendances, les paquets suggérés et les conflits. Enfin, elle indique éventuellement la page Web de l'application.

Cette option, moins connue, télécharge simplement le paquet logiciel dans le répertoire courant, cela est utile en cas de traitement non immédiat :

```
aptitude download paquet
```

Supprimer le cache pour libérer de la place sur le disque dur :

```
aptitude clean
```

L'exécution de cette dernière option (voir le manuel en ligne pour toutes les options possibles) vide le répertoire `/var/cache/apt/archives`, c'est-à-dire là où les paquets logiciels ont été chargés.

Résumé de séquence de mise à jour d'un système

Pour mettre à jour un système Ubuntu, voici la séquence des trois commandes à exécuter les unes à la suite des autres :

```
aptitude update
```

```
aptitude full-upgrade# ou safe-upgrade
```

```
aptitude clean
```



Aptitude reste par excellence l'outil de l'administrateur, aussi la pratique courante consiste à s'arrêter là.

d. Utilitaire Wajig

Parallèlement à l'utilisation d'Aptitude, existe un autre utilitaire que l'on pourrait qualifier "d'exotique" s'il ne disposait pas de qualités certaines. Basé sur le langage Python, l'installation a comme dépendance le paquetage `dselect` et beaucoup de paquets suggérés qu'il est nécessaire de prendre (exemples : `wget`, `fping`) :

```
aptitude install wajig wget fping
```

Wajig comme Aptitude effectue la mise à jour des sources :

```
wajig update
```

Il donne un renseignement double : le nombre de logiciels à mettre à jour et les nouveaux. On voit les nouveautés par un simple :

```
wajig new
```

```
root@jeos:~# wajig new
Package      Description
=====
fglrx-amdcccle-envy  Dummy package for easy transition
fglrx-control-envy   Control panel for the ati graphics accelerators
fglrx-kernel-source-envy  Ati binary kernel module source
nvidia-glx-dev-envy  Nvidia binary xfree86 4.x/x.org driver development files
nvidia-glx-envy      Nvidia binary xfree86 4.x/x.org driver
nvidia-glx-legacy-dev-envy  Nvidia binary xfree86 4.x/x.org 'legacy' driver development files
nvidia-glx-legacy-envy  Nvidia binary xfree86 4.x/x.org 'legacy' driver
nvidia-glx-new-dev-envy  Nvidia binary xfree86 4.x/x.org 'new' driver development files
nvidia-glx-new-envy   Nvidia binary xfree86 4.x/x.org 'new' driver
nvidia-kernel-source-envy  Nvidia binary kernel module source
nvidia-legacy-kernel-source-envy  Nvidia binary 'legacy' kernel module source
nvidia-new-kernel-source-envy  Nvidia binary 'new' kernel module source
openssh-blacklist   List of blacklisted openssh rsa and dsa keys
openssl-blacklist   List of blacklisted openssl rsa keys
openvpn-blacklist    List of blacklisted openvpn rsa shared keys
xorg-driver-fglrx-dev-envy  Video driver for ati graphics accelerators (devel files)
xorg-driver-fglrx-envy   Video driver for ati graphics accelerators
root@jeos:~# _
```

Les paquetages à mettre à jour sont montrés avec les numéros de version : ce qui est intéressant pour l'administrateur :

```
wajig newupgrade
```



```

root@jeos:~# wajig newupgrade
Package                Available                Installed
=====
libssl0.9.8            0.9.8g-4ubuntu3.1        0.9.8g-4ubuntu3
openssh-client          1:4.7p1-8ubuntu1.2        1:4.7p1-8ubuntu1
openssh-server          1:4.7p1-8ubuntu1.2        1:4.7p1-8ubuntu1
root@jeos:~# _

```

Wajig utilise bien sûr les commandes `install`, `remove`, `purge` et `upgrade` pour la gestion des paquets. La liste complète des commandes se trouve par un simple `wajig list-commands` ou à cette adresse Internet : <http://www.togaware.com/wajig>

e. Gestion graphique

Dernier utilitaire en situation graphique : **Synaptic**. Il se lance par le menu **Système - Administration - Gestionnaire de paquets Synaptic**. Même dans le cas d'un poste de travail, l'utilisation de Synaptic est à déconseiller car peu intuitif. On perd beaucoup moins de temps à gérer les paquets avec **Aptitude** en ligne de commande.

Mise à jour du système

Les mises à jour de sécurité s'installent :

- sans confirmation
- en téléchargement en arrière-plan
- avec un simple avertissement

Le choix de ces trois options se trouvent dans le menu **Système - Administration - Sources de logiciels**, onglet **Mises à jour**.

Pour le reste, l'application `update-manager` (menu **Gestionnaire de mises à jour**) détecte par défaut automatiquement les mises à jour et les installe après fourniture du mot de passe de l'utilisateur privilégié.

Services au démarrage

1. Niveaux d'exécution

Ubuntu s'inspire des niveaux d'exécution (runlevel) de type System V Unix pour pouvoir configurer l'accès aux services. Chaque niveau d'exécution se trouve dans un répertoire de type `/etc/rcN.d` où N identifie le numéro d'ordre. La distribution Ubuntu distingue les niveaux d'exécution suivants :

- 0 pour l'arrêt du système.
- 1 pour le mode `single` ou mono-utilisateur.
- de 2 à 5 pour un mode multi-utilisateur.
- 6 pour le redémarrage du système.

Par défaut, Ubuntu comporte un réglage sur le niveau 2. Le mode 1 se réserve plus particulièrement à la maintenance, comme le changement du mot de passe administrateur en cas d'oubli.

a. Détails sur les niveaux d'exécution

La commande `telinit` change le niveau d'exécution :

```
telinit 3
```

Rien ne se passe car les niveaux de 3 à 5 sur Ubuntu sont identiques au niveau 2. La commande `runlevel` montre le niveau d'exécution courant :

```
runlevel
```

Le retour affiche `2 3`, c'est-à-dire les niveaux précédents et actuels. Un `N 2` (N pour normal) aurait été la sortie si la commande `telinit` n'avait pas changé cela.

Sur Ubuntu, c'est le script `/etc/init.d/rcS` qui exécute les actions pour le niveau qui lui est passé en argument. Par exemple, un passage de l'argument 2 fera exécuter les scripts du répertoire `/etc/rc2.d`. Les répertoires contiennent des scripts du type `Snnxxx` ou `Knnxxx` : S pour Start et K pour Kill. La numérotation implique un lancement ordonné du plus petit au plus grand : `S90halt` pour le dernier script du niveau 0.



Les scripts contenus dans les répertoires `/etc/rcN.d` sont pour la plupart des pointeurs sur des fichiers regroupés dans `/etc/init.d`.

b. Upstart en remplacement d'initd

Sur Ubuntu, une nouvelle méthode d'engagement des scripts de niveau a vu le jour : en remplaçant le traditionnel fichier `/etc/inittab` par `upstart`. On passe d'un aspect plus statique et figé à une méthode plus dynamique, basée sur la notion de tâches (jobs) et d'évènements. Vous trouverez plus de renseignements à l'adresse Internet : <http://upstart.ubuntu.com/>

Les tâches résident dans le répertoire `/etc/events.d` :


```

root@ubuntu:~# ls -l /etc/event.d/
total 76
-rw-r--r-- 1 root root 260 2008-04-11 15:49 control-alt-delete
-rw-r--r-- 1 root root 299 2008-04-11 15:49 logd
-rw-r--r-- 1 root root 552 2008-04-11 15:49 rc0
-rw-r--r-- 1 root root 342 2008-04-11 15:49 rc1
-rw-r--r-- 1 root root 403 2008-04-11 15:49 rc2
-rw-r--r-- 1 root root 403 2008-04-11 15:49 rc3
-rw-r--r-- 1 root root 403 2008-04-11 15:49 rc4
-rw-r--r-- 1 root root 403 2008-04-11 15:49 rc5
-rw-r--r-- 1 root root 422 2008-04-11 15:49 rc6
-rw-r--r-- 1 root root 485 2008-04-11 15:49 rc-default
-rw-r--r-- 1 root root 392 2008-04-11 15:49 rcS
-rw-r--r-- 1 root root 575 2008-04-11 15:49 rcS-sulogin
-rw-r--r-- 1 root root 558 2008-04-11 15:49 sulogin
-rw-r--r-- 1 root root 306 2008-04-11 15:49 tty1
-rw-r--r-- 1 root root 300 2008-04-11 15:49 tty2
-rw-r--r-- 1 root root 300 2008-04-11 15:49 tty3
-rw-r--r-- 1 root root 300 2008-04-11 15:49 tty4
-rw-r--r-- 1 root root 300 2008-04-11 15:49 tty5
-rw-r--r-- 1 root root 300 2008-04-11 15:49 tty6
root@ubuntu:~# _

```

Le script rc-default montre bien que le niveau par défaut d'Ubuntu est le niveau 2. La commande `initctl` contrôle et communique avec le processus `init`. Avec l'option `list`, elle montre la liste des tâches en fonctionnement ou en attente :

```
initctl list
```

```

root@ubuntu:~# initctl list
control-alt-delete (stop) waiting
logd (stop) waiting
rc-default (stop) waiting
rc0 (stop) waiting
rc1 (stop) waiting
rc2 (stop) waiting
rc3 (stop) waiting
rc4 (stop) waiting
rc5 (stop) waiting
rc6 (stop) waiting
rcS (stop) waiting
rcS-sulogin (stop) waiting
sulogin (stop) waiting
tty1 (start) running, process 4238
tty2 (start) running, process 4080
tty3 (start) running, process 4081
tty4 (start) running, process 4075
tty5 (start) running, process 4076
tty6 (start) running, process 4085
root@ubuntu:~#

```

Upstart, à la différence d'`inittab`, lance ou arrête une tâche parmi d'autres dans un niveau d'exécution au lieu de changer globalement tout le niveau. On ajoute ou modifie sans problème un script dans le répertoire des événements.

Pour ne plus avoir les consoles `tty4`, `tty5` et `tty6`, il suffit de supprimer les fichiers correspondants dans le répertoire des événements.

Exemple :

Vous désirez sauvegarder un fichier avant l'arrêt ou le redémarrage de la machine, et ce quel que soit l'utilisateur connecté. L'ajout de la commande de sauvegarde dans le script `/etc/event.d/rc0` (avant la ligne `exec /etc/init.d/rc 0`) le fera (nécessite un redémarrage pour la prise en compte). On peut aussi moduler l'évènement `control-alt-delete` pour l'interdire ou effectuer un traitement préalable, par exemple.

Jusqu'à un certain point Upstart peut même remplacer un utilitaire de type `cron`, `atd` ou `anacron` et donc de lancer un événement dans un intervalle de temps (voir les détails dans la documentation sur le site).

2. Utilitaires de gestion des services

Optimiser son système revient en partie à ne charger que les services nécessaires à réel fonctionnement. L'administrateur doit :

- identifier les services lancés ;
- recenser les services inutiles ;
- gérer le lancement des services au démarrage.

Vous trouverez en **Annexe 1** une liste commentée (non exhaustive) des services de la distribution Ubuntu afin de vous aider pour les deux premiers points.

a. Méthode update-rc

L'outil `update-rc.d` gère les services en ligne de commande. Son utilisation n'est pas triviale. Voici un exemple d'emploi sur une distribution Ubuntu en version poste de travail et où l'on désire aboutir au démarrage à une console texte et non graphique (dans ce cas précis et parce que nous sommes en poste de travail, il faut passer en mode console par un terminal et en tapant `sudo -i` pour passer en administrateur).

Cela consiste à enlever le service GDM (le lanceur de session graphique de GNOME, pour KDE c'est KDM) de tous les niveaux de démarrage :

```
update-rc.d -f gdm remove
```

Notez les messages de retour car il nous donne des indications sur les ordres d'exécution :

```
root@dsk:~# update-rc.d -f gdm remove
Removing any system startup links for /etc/init.d/gdm ...
/etc/rc0.d/K01gdm
/etc/rc1.d/K01gdm
/etc/rc2.d/S30gdm
/etc/rc3.d/S30gdm
/etc/rc4.d/S30gdm
/etc/rc5.d/S30gdm
/etc/rc6.d/K01gdm
root@dsk:~#
```

La remise du service GDM pour le niveau 2 est plus complexe (il faut respecter les espaces et les points) :

```
update-rc.d gdm start 30 2 . stop 01 0 1 6 .
```

Le service GDM est remis en numérotation 30, niveau 2 pour son lancement ; numérotation 01, niveaux 0, 1 et 6 pour son arrêt. On laisse de côté les niveaux 3, 4 et 5 de lancement, facultatifs.

b. Méthode sysv-rc-conf

Utilisée sur un serveur et apportée par le paquet logiciel de même nom (non installé par défaut), elle se base sur la librairie `curses` pour apporter plus de convivialité dans la manipulation des services en rapport avec le niveau d'exécution.

Installation et lancement de l'outil :

```
aptitude install sysv-rc-conf
```

```
sysv-rc-conf
```

SysV Runlevel Config -: stop service =/+ : start service h: help q: quit								
service	1	2	3	4	5	0	6	S
exim4	[]	[X]	[X]	[X]	[X]	[]	[]	[]
gdm	[]	[X]	[]	[]	[]	[]	[]	[]
hal	[]	[X]	[X]	[X]	[X]	[]	[]	[]
halt	[]	[]	[]	[]	[]	[X]	[]	[]
hotkey-se\$	[]	[X]	[X]	[X]	[X]	[]	[]	[]
keyboard-\$	[]	[]	[]	[]	[]	[]	[]	[X]
killprocs	[X]	[]	[]	[]	[]	[]	[]	[]
klogd	[]	[X]	[X]	[X]	[X]	[]	[]	[]
laptop-mo\$	[]	[]	[]	[]	[]	[]	[]	[]
linux-res\$	[]	[]	[]	[]	[]	[X]	[X]	[X]
loopback	[]	[]	[]	[]	[]	[]	[]	[X]
module-in\$	[]	[]	[]	[]	[]	[]	[]	[X]
mountover\$	[]	[]	[]	[]	[]	[]	[]	[X]
mysql	[]	[X]	[X]	[X]	[X]	[]	[]	[]
mysql-ndb	[]	[X]	[X]	[X]	[X]	[]	[]	[]
mysql-ndb\$	[]	[X]	[X]	[X]	[X]	[]	[]	[]
nbd-server	[]	[X]	[X]	[X]	[X]	[]	[]	[]
networking	[]	[]	[]	[]	[]	[]	[]	[X]
nfs-common	[]	[X]	[X]	[X]	[X]	[]	[]	[X]
nfs-kerne\$	[]	[X]	[X]	[X]	[X]	[]	[]	[]
nvidia-ke\$	[]	[]	[]	[]	[]	[]	[]	[]

Use the arrow keys or mouse to move around. ^n: next pg ^p: prev pg
space: toggle service on / off

La suppression ou la remise en place du service GDM s'effectue simplement à l'aide de la barre d'espace (sortie par la lettre q).

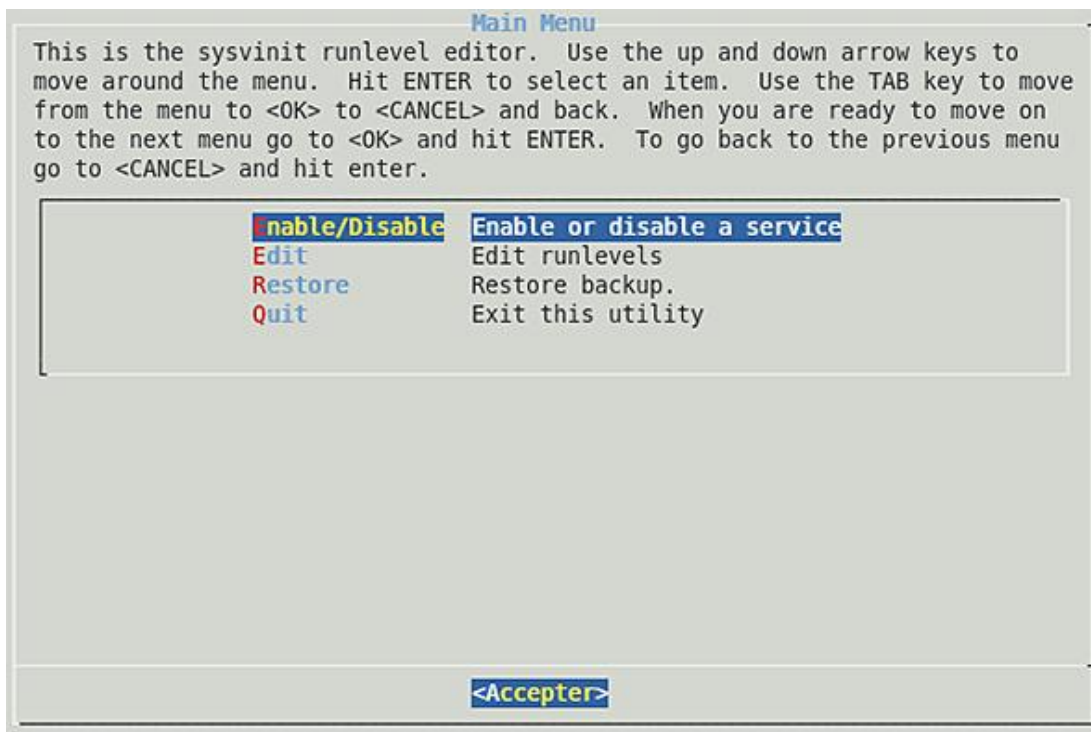
c. Méthode sysvconfig

Je préfère cette méthode, car elle possède une interface encore plus claire et directement liée au niveau d'exécution courant (ce qui est somme toute suffisant dans la plupart des cas). On retrouve cependant la présentation à la façon sysv-rc-conf dans la ligne Edit runlevels.

Installation et lancement de l'outil :

```
aptitude install sysvconfig
```

```
sysvconfig
```



Pour enlever le service GDM :

- Validez **Enable or disable a service**.
- Décochez le service GDM et acceptez.
- Validez **Finish and save files** et acceptez.
- Sortez par **Exit this utility**.

Cette commande dispose de la possibilité de revenir à une situation précédente par la restauration d'un backup. Du point de vue de l'administrateur et sur une version serveur Ubuntu, c'est l'outil à utiliser par rapport aux deux précédents.

d. Méthode par l'interface graphique

Sur un poste de travail et avec GNOME , la gestion des services passe par le menu **Système - Administration - Services**, ou commande **services-admin**. Un déverrouillage de l'application est nécessaire par l'entrée du mot de passe du super-utilisateur pour y effectuer des modifications car au départ tout s'affiche, mais en gris.

- Déverrouillez l'application par l'appui du bouton de même nom.

À noter que, cette fois-ci, les noms des services sont traduits et quelques-uns sont commentés :



Les modifications seront, là encore, prises en compte lors d'un prochain redémarrage de la machine.

Contexte d'une session de travail

1. Interpréteur de commandes

La connexion réussie d'un utilisateur (ici le `root` car on se base sur une version serveur) a activé l'interpréteur de commandes approprié (indiqué dans le fichier `/etc/passwd`). L'interpréteur de commandes (ou `shell`) représente l'interface entre l'utilisateur et le système d'exploitation. Comme toujours, et Ubuntu ne déroge pas à la règle, il existe non pas un mais plusieurs interpréteurs de commandes. Le `shell` par défaut sous Ubuntu est le `BASH` ou *Bourne Again Shell*.

Pour expliquer les notions qui suivent, la commande basique (et essentielle) `ls` qui liste les fichiers d'un répertoire sera utilisée.

a. Englobement ou expressions rationnelles du shell

L'englobement dans une commande du shell consiste à taper un ou plusieurs caractères spéciaux signifiant une sélection particulière à appliquer à cette commande. Caractère spécial le plus courant : le caractère "étoile" qui remplace une suite de caractères quelconques :

```
ls b*e
```

Cela affiche la liste de tous les fichiers du répertoire courant commençant par un `b` et finissant par un `e`.

```
ls /etc/*.conf
```

Liste tous les fichiers du répertoire `/etc` ayant pour extension `.conf`.

Autres caractères d'englobement

`?` : remplace un seul caractère

`[...]` : correspond aux caractères entre crochets soit :

`[1-9]` : pour des chiffres

`[GER]` : pour un `G`, un `E` ou un `R`

`[a-z]` : pour tout l'alphabet en minuscule

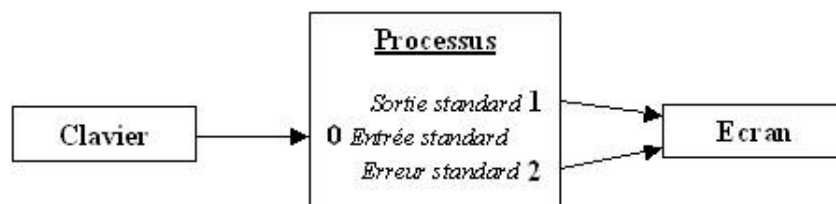
`[!...]` : même chose mais en exclusion

```
ls b[!0-9]e
```

Cette commande liste les fichiers commençant par un `b`, avec une deuxième lettre qui ne peut être un chiffre et se terminant par un `e`.

b. Redirections

Le système Linux Ubuntu comporte une entrée dite standard réservée au clavier par défaut et une sortie standard consacrée à l'écran. Pour compléter cet équilibre, une sortie d'erreur standard (toujours l'écran par défaut) est ajoutée. Pour le shell, les codes associés à ces flux correspondent respectivement à 0, 1 et 2.



Le principe de redirection consiste redéfinir ces flux standards. L'utilisateur réalise ce type d'opérations constamment sans le savoir lorsqu'il imprime un document. La sortie est redirigée vers l'imprimante et non plus vers l'écran. Les redirections possibles sont :

- un **fichier** : utile pour enregistrer des informations ou des événements comme les erreurs.
- un **tube** : on redirige la sortie de la commande vers l'entrée d'une autre (voir le détail plus bas).
- un **périphérique** : classique comme l'imprimante.

La redirection utilise le caractère > pour fonctionner, précédé ou non (implicite pour le 0 ou 1) du code de flux. Un double >> détermine un ajout pour un fichier alors que le caractère > simple détruit le fichier si existant avant de le remplacer par le contenu du flux.

En voici une syntaxe plus précise :

```
0<nom_de_fichier
    nom_de_fichier comme entrée standard, code 0 optionnel
1>nom_de_fichier
    nom_de_fichier comme sortie standard, code 1 optionnel
1>>nom_de_fichier
    idem en ajout au fichier et non en création, code 1 optionnel
2>erreurs
    dirige les erreurs vers le fichier erreurs
```

Exemples :

```
ls /etc/*.conf > liste.txt
```

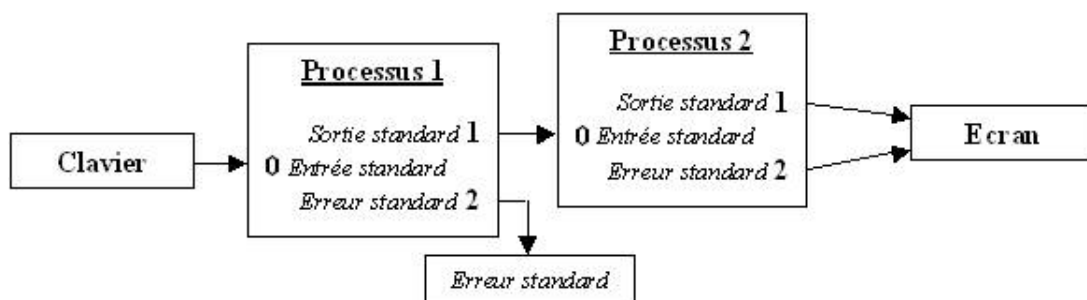
```
ls /usr/local/etc/*.conf >> liste.txt
```

```
ls /home/max/ > liste_max.txt 2> erreurs.txt
```

Le premier exemple envoie la liste des fichiers du répertoire /etc ayant l'extension .conf dans le fichier liste.txt (il n'y a plus d'affichage à l'écran). Le deuxième exemple ajoute à ce fichier la liste des fichiers de même extension trouvée dans /usr/local/etc. Le dernier exemple envoie la liste des fichiers du répertoire max dans le fichier liste_max.txt et un message d'erreur dans le fichier erreurs.txt si l'utilisateur max n'existe pas (dans ce cas, le fichier liste_max.txt est vide).

c. Tubes

Un tube combine une redirection d'entrée et de sortie, ou plus exactement relie la sortie standard d'une commande à l'entrée standard d'une autre commande. Ceci se matérialise dans la ligne de commande par les deux tirets verticaux | (touche [Alt Gr] 6).



Cette technique s'emploie couramment dans les tâches administratives. Des exemples plus concrets sont décrits dans les chapitres sur la maintenance. Avec la commande `ls`, on utilise typiquement un tube avec la commande `less`.

Cette commande découpe en page la sortie à l'écran pour les fichiers très longs qui, sans cela, défileraient jusqu'à la fin. Le déplacement se réalise à l'aide des touches [Page Up] et [Page Down] (les flèches du pavé numérique pour les pages) car on peut remonter dans le fichier à l'inverse d'une autre commande similaire, la commande `more`.

Exemple :

```
ls -l /etc/ | less
```

L'affichage du répertoire /etc/ dépasse la capacité de l'écran. L'affichage entier est passé en entrée de la commande `less` et fractionné. Pour sortir à tout moment du tube, on tape la lettre `q`.



Un truc très utile pour les administrateurs : même si vous n'avez pas fait de tube, l'utilisation des touches [Page Up] et [Page Down] permettent de revenir en arrière et en avant de l'affichage. La seule limite réside dans la taille du tampon (buffer) de la sortie écran.

2. VIM ou l'éditeur de l'administrateur

a. Éditeur et traitement de texte

Un éditeur de texte sert à créer et/ou modifier des fichiers texte sans mise en forme. Une simple mise en page pour la lisibilité suffit à la différence d'un traitement de texte qui peut utiliser outre une présentation élaborée, des objets comme des images, des graphiques, etc. On peut dissocier donc l'écriture (faite par un éditeur de texte) de la mise en page définitive (faite par un compilateur de texte comme **LaTeX** par exemple). Dans le cas d'un traitement de texte, ces deux étapes sont simultanées.

Comment choisir son éditeur ? Certains sont très simples, voire spartiates, d'autres simples mais graphiques et avec une souris, d'autres plus complexes... Le choix est simple car fonction de l'environnement :

Pour la console texte

- **vi** (ou en fait **vim**)
- **pico** (ou **nano** déjà utilisé dans le précédent chapitre)
- **joe**

Tous ces éditeurs possèdent leurs raccourcis de commandes et, il faut le dire, souvent abscons. Voici par exemple les commandes de l'éditeur **joe** :

Help Screen		turn off with ^KH	more help with ESC . (^[.)			
CURSOR	GO TO	BLOCK	DELETE	MISC	EXIT	
^B left	^U prev. screen	^KB begin	^D char.	^KJ reformat	^KX save	
^P up	^N down	^KK end	^Y line	^KA center	^C abort	
^Z previous word	^A beg. of line	^KM move	^W >word	^T options	^KZ shell	
^X next word	^E end of line	^KC copy	^O word<	^R refresh	FILE	
SEARCH	^KU top of file	^KW file	^J >line	SPELL	^KE edit	
^KF find text	^KV end of file	^KY delete	^_ undo	^IN word	^KR insert	
^L find next	^KL to line No.	^K/ filter	^_ redo	^IL file	^KD save	
IU	Sans nom	Rou 1	Col 1	10:44	Ctrl-K H for help	

Pour l'environnement graphique (liste non exhaustive)

- **gedit** (environnement GNOME)
- **kate** (environnement KDE)
- **gvim** (version graphique de **vim**)
- **xemacs** (version graphique d'**emacs**)

b. L'éditeur de texte VI

Le principe d'utilisation d'un éditeur de texte pour un administrateur se rapporte essentiellement à sa rapidité. L'administrateur système ne programme pas, il crée certes des scripts (courts) mais son activité essentielle avec un éditeur de texte réside dans l'édition de fichiers de logs, (journaux), dans l'édition et la modification de fichiers de configuration de services.

Pourquoi VI (on prononce vi-aïe) ou plutôt VIM (**Vi IMproved** soit **VI** amélioré) ? Parce qu'il fait partie intégrante de tout environnement Unix/Linux et qu'il représente un outil de base incontournable : quelle que soit la distribution, quel que soit le système, il existe une version de VI . Son apprentissage fait partie de la fondation même de la

fonction d'administrateur. Ne pas connaître VIM et se prétendre administrateur système fera immédiatement naître une suspicion vis-à-vis de vos capacités réelles dans la fonction.

Lancement de VIM

L'installation de la distribution Ubuntu, qu'elle soit serveur ou poste de travail, propose une version de base de VIM (`vim-common` et `vim-tiny`). Dans cette version, certaines manipulations ne sont pas possibles comme par exemple l'utilisation des touches de curseur pour naviguer dans le texte. Le gestionnaire de paquets doit normalement être correctement configuré pour pouvoir installer le paquetage VIM afin d'obtenir la version complète :

```
aptitude install vim
```



➤ L'utilisation de l'éditeur VIM permet de mettre en lumière un comportement de Linux : la notion d'alternatives. En fonction de l'installation des logiciels, une même commande aboutit au lancement d'un logiciel différent. Sous Ubuntu, ce changement de comportement est visible dans le dossier `/etc/alternatives`. Dans le cas de VIM, avant l'installation du logiciel, les commandes `vi` ou `vim` suivent le lien `/usr/bin/vim.tiny` ; après l'installation, le lien se transforme en `/usr/bin/vim.basic`. Cette situation se retrouve dans l'exploitation d'un service de messagerie ou le choix du logiciel serveur n'influence pas les commandes de gestion du courrier. Si l'on revient dans le domaine des éditeurs de texte, les commandes `pico`, `editor` et `nano` aboutissent sous Ubuntu à ce même éditeur `nano`.

Une fois l'installation effectuée, la syntaxe générale de lancement de VIM est la suivante :

```
vi(m) [options] [chemin/nom_de_fichier]
```

En fonction ou non de la présence d'un nom de fichier à la suite de la commande, on aura :

- Si le fichier existe, l'éditeur l'ouvre en modification.
- Si le fichier n'existe pas, l'éditeur l'ouvre en création.
- Si aucun nom de fichier, la demande se fera à la sortie de l'éditeur.
- Pour être sûr d'ouvrir un fichier uniquement en lecture, on utilise l'option -R.

Voici l'écran d'accueil de VIM, l'écran s'efface et la colonne la plus à gauche affiche des ~ (tildes) :

```

      UIM - Vi Amélioré

      version 7.1.138
      par Bran Moolenaar et al.
      Vim est un logiciel libre

      Aidez les enfants pauvres d'Ouganda !
      tapez :help iccf<Entrée> pour plus d'informations

      tapez :q<Entrée> pour sortir du programme
      tapez :help<Entrée> ou <F1> pour accéder à l'aide en ligne
      tapez :help version?<Entrée> pour lire les notes de mise à jour
  
```



Notez l'appel humanitaire pour les enfants du centre ougandais de Kibaale. Cela a toujours été la règle pour VI et cela montre une fois de plus que logiciel libre rime avec esprit d'entraide communautaire.

Coloration syntaxique

L'éditeur VI possède la capacité de la coloration syntaxique en fonction du langage utilisé (BASH ou Perl, les plus utilisés par l'administrateur). Pour activer cette fonctionnalité, il suffit de modifier le fichier de configuration de VI :

- Éditez par VI le fichier `/etc/vim/vimrc` et supprimez le guillemet (") de commentaire sur la ligne `syntax on`.
- Lancez par exemple le fichier `.bashrc` dans votre répertoire de travail pour en voir le résultat.

c. Utilisation optimisée de VIM

Il existe beaucoup de littérature sur VI décrivant en détail et en totalité les commandes de l'éditeur. Pourtant même si VI constitue le premier élément de la trousse à outils de l'administrateur, il n'en reste pas moins vrai qu'il ne déroge pas à la règle classique qui consiste à ce qu'un utilisateur ne connaisse et ne tire profit en général que d'une partie d'un logiciel. Concrètement, l'apprentissage de VI est difficile et rébarbatif... Mais une fois maîtrisé, l'outil se révèle **indispensable**.

La présentation qui suit n'est pas exhaustive mais constitue la base de l'utilisation de VI tel qu'un administrateur le pratique au jour le jour. En clair : toutes les commandes ne sont pas décrites, mais l'essentiel est là.



Les débutants désireux de suivre une progression tireront profit du tutoriel fourni avec l'éditeur. Pour le lancer, soyez dans une console texte bien sûr et tapez la commande `vimtutor` :

===== Bienvenue dans le Tutoriel de VIM - Version 1.5.fr.2 =====

Vin est un éditeur très puissant qui a trop de commandes pour pouvoir toutes les expliquer dans un cours comme celui-ci, qui est conçu pour en décrire suffisamment afin de vous permettre d'utiliser simplement Vin.

Le temps requis pour suivre ce cours est d'environ 25 à 30 minutes, selon le temps que vous passerez à expérimenter. Les commandes utilisées dans les leçons modifieront le texte. Faites une copie de ce fichier afin de vous entraîner dessus (si vous avez lancé "vintutor" ceci est déjà une copie).

Il est important de garder en tête que ce cours est conçu pour apprendre par la pratique. Cela signifie que vous devez exécuter les commandes pour les apprendre correctement. Si vous vous contentez de lire le texte, vous oublierez les commandes !

Maintenant, vérifiez que votre clavier n'est PAS verouillé en majuscules, et appuyez la touche **j** le nombre de fois suffisant pour que la leçon 1.1 remplisse complètement l'écran.

Leçon 1.1 : DÉPLACEMENT DU CURSEUR
"/tnp/tutorXP4066" [converti] 809 lignes, 30059 caractères

Les états de VI

On distingue sous VI deux états principaux :

- **mode commande** : saisie d'une commande.
- **mode saisie** : saisie d'un texte dans le buffer.

Au démarrage, VI se positionne automatiquement en mode commande. L'utilisation de VI implique que l'on passe fréquemment d'un mode à l'autre. En fait pour savoir où l'on est, il suffit de taper deux fois sur la touche [Echap] : vous êtes alors sûr d'être en mode commande.

Pour passer d'un mode à l'autre :

- du mode commande en mode saisie : appui d'une commande codée sur une seule lettre.
- du mode saisie en mode commande : appui de la touche [Echap] (bip si vous y êtes déjà).

Les autres modes de fonctionnement

Le mode **ex**, qui traite en partie de la façon de sortir de VI (des combinaisons sont possibles) :

Fonctions	Touches
normalement sans sauvegarde	:q

obligatoirement sans sauvegarde	:q!
avec sauvegarde	:wq ou :x
avec sauvegarde mais sans sortie	:w
avec sauvegarde, sortie et indication du fichier	:wq <i>nom_de_fichier</i>
pour le fichier d'aide	:h (sortie par :q)

VI possède aussi la possibilité de travailler avec plusieurs fichiers à l'écran, mais nous ne le verrons pas. C'est un choix personnel : si l'on commence à utiliser VI comme un traitement de texte, alors autant en utiliser un et graphique de préférence ! VI doit rester ce qu'il est : un éditeur en mode console, simple et surtout rapide à utiliser.

Les commandes essentielles

Rappel : si vous n'êtes pas sûr de l'être, tapez deux fois sur [Echap], vous serez en mode commande. Un bip vous le signale. Vous avez, en mode saisie ou commande, la possibilité de vous déplacer avec toutes les flèches de direction, sauts de page, [Suppr], [Inser], etc.

En mode commande :

Fonctions	Touches
Insère du texte devant le curseur	i
efface et supprime la ligne entière (variante : <i>ndd</i> supprime <i>n</i> lignes)	dd 3dd (pour 3 lignes)
cherche le motif toto dans le texte à partir de curseur	/toto
idem sauf que la recherche se fait en arrière, vers le début du texte	?toto
répète la dernière commande de recherche	n
copie la ligne dans le Presse-papiers (variante : <i>nyy</i> copie <i>n</i> lignes)	yy 3yy (pour 3 lignes)
colle le contenu du Presse-papiers derrière le curseur	p
annule la dernière commande	u
répète la dernière commande	.

En mode ex :

Fonctions	Touches
aller à la ligne <i>n</i>	:n
aller à la dernière ligne	:\$
déplacer les lignes de <i>n1</i> à <i>n2</i> en <i>n3</i> (:2,4 m 8 déplace les lignes 2 à 4 après la ligne 8)	: <i>n1</i> , <i>n2</i> m <i>n3</i>
remplace chaîne1 par chaîne2 de <i>n1</i> à <i>n2</i> (si <i>n2</i> =\$ alors fin de fichier)	: <i>n1</i> , <i>n2</i> s/chaine1/chaine2

insère un fichier à la ligne courante	:r <i>nom_de_fichier</i>
afficher les numéros de ligne (nonu pour l'enlever)	:set nu



Toutes les éditions de fichiers dans l'ouvrage sont faites par l'éditeur VIM.

Environnement et cadre de travail

1. Outils de base

a. Fichiers de session

Une fois la connexion réussie, l'utilisateur Ubuntu se trouve donc dans un répertoire nommé le répertoire de travail, c'est-à-dire celui où il se situe (rappel : `/root` pour l'administrateur et `/home/noms_de_l'utilisateur` pour les autres). Au départ, le répertoire courant se confond avec le répertoire de l'utilisateur. Il comprend cinq fichiers cachés (le point devant le nom du fichier indique cet état) qu'un simple `ls` ne peut montrer. Il faut lui ajouter l'option `-a` :

```
ls -a
```

La sortie de la commande montre :

- Un simple point : indique le répertoire lui-même.
- Un double point : indique le répertoire parent.
- Le fichier `.bash_logout` : script d'exécution de commandes juste avant la fin de session.
- Le fichier `.bashrc` : script d'exécution de commandes juste avant le début de session.
- Le fichier `.profile` : script de positionnement de l'environnement utilisateur, il lance notamment `.bashrc`.

Avec les trois derniers fichiers, il est facile de modifier les informations lors de l'entrée et la sortie d'une session avec des commandes de l'interpréteur de commandes (shell) BASH.

Exemple :

Éditez le fichier `.profile` et ajoutez-y les deux lignes ci-dessous en fin de fichier :

```
echo " Bienvenue $USER. "  
echo -n " Nous sommes le " ; date
```

Explications :

La prochaine session de travail affichera, après l'identification réussie, un message de bienvenue avec le nom de l'utilisateur (variable d'environnement `$USER`). La deuxième ligne affiche la date et l'heure du jour.



L'apprentissage du shell BASH, avec l'écriture de scripts dépasse le cadre de cet ouvrage. Il mérite à lui seul un manuel...

b. Manuel en ligne

L'utilisateur, qu'il soit administrateur ou utilisateur, dispose d'un manuel en ligne expliquant et donnant des renseignements sur toutes les commandes Linux. Pour l'appeler il suffit de taper le mot-clé `man` suivi de la commande désirée :

```
man ls
```

La sortie équivaut à un affichage filtré par la commande `less`. On se déplace donc dans le manuel avec les touches [Page Up] et [Page Down]. Pour rechercher dans les pages un mot, on utilise la commande de recherche de VIM (d'où son utilité). La sortie du manuel - souvent en langue anglaise, car tout n'est pas traduit - s'effectue classiquement par le caractère `q`.

Sur Ubuntu la prise en compte des pages françaises du manuel en ligne passe par un paquet logiciel :

```
aptitude install manpages-fr
```

Une bonne pratique pour l'administrateur consiste à ouvrir (et laisser ouverte) une console supplémentaire (la sixième par exemple avec [Alt][F6]) réservée à l'utilisation du manuel en ligne.



Une raison évidente d'apprendre l'éditeur VIM : la commande de recherche d'un mot dans l'afficheur du manuel est la même ! Cela peut être utile dans le cas d'une trop abondante documentation...

c. Complétion

Le mécanisme de complétion (mot peu usité dans la langue française), évite beaucoup de fatigue à l'administrateur. En tapant partiellement une commande, suivi de deux frappes sur la touche de tabulation, celle-ci se trouve naturellement complétée en fonction des prémices de la demande. Elle complète à la fois les commandes et les arguments de ces commandes.

Exemple :

Si l'on tape juste la lettre `l` suivie de deux tabulations, toutes les commandes commençant par `l` vont s'afficher. Si l'on tape `ls` puis un espace, suivi de deux tabulations, cette fois ce sera la liste des fichiers et répertoires qui s'affichera.

Autre exemple : un `cat /etc/net` et deux tabulations complèteront la commande avec le mot `network` mais s'arrêteront là. Deux touches de tabulations supplémentaires montreront qu'il y a en fait le choix entre `/etc/network/` (sous-répertoire) et `/etc/networks` (fichier).

d. Historique des commandes

Autre outil important pour l'administrateur : la mise en mémoire des commandes tapées dans la console. Au lieu du fichier `.bash_history`, on lui préfère directement la commande `history` qui indique en plus un numéro d'indice :

- Tapez `history` et notez le numéro d'une commande quelconque.

En premier lieu, vous voyez la syntaxe exacte de la commande recherchée (utilisez le mécanisme des [Page Up]/[Page Down] si la liste est trop longue). Mais en plus, il n'est pas nécessaire de la retaper entièrement si vous ne désirez pas faire de modifications. Exemple, j'ai une commande de téléchargement d'un répertoire (très longue) que je veux refaire et que voici :

```
lftp -c "open http://archive.ubuntu.com/ubuntu/dists/hardy/main/installer-i386/current/images/netboot/; mirror"
```

En tapant la commande `history` dans la console je repère cette commande et je note son indice : 169. Pour relancer la commande sans la retaper, il suffit de noter un point d'exclamation suivi du numéro : `!169`

Autre méthode

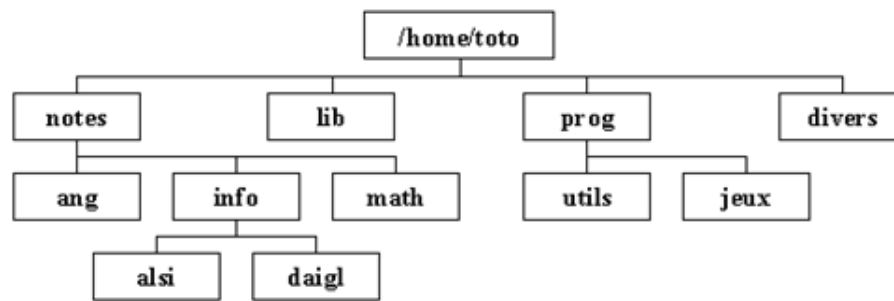
Plus simple, elle se réserve aux commandes tapées il y a peu de temps. En appuyant sur les flèches de direction (haut et bas) vous faites tout simplement défiler les commandes. Il suffit de valider à nouveau la commande pour qu'elle s'exécute.

2. Travailler sur les répertoires

a. Organisation des fichiers

La hiérarchie des répertoires sous Linux commence à la racine (notée par `/`) et se divise en répertoires, chacun séparé du précédent par une barre oblique `/` (slash ou barre de division). Travailler au sein de son espace, c'est-à-dire son répertoire de travail, revient à en gérer les sous-répertoires et fichiers. Pour l'administrateur, le champ d'investigation s'étend à tout le système alors que l'utilisateur se limite à son répertoire personnel.

Prenons l'exemple d'un étudiant nommé toto :



Cette arborescence montre la structure des répertoires de l'utilisateur. Un document `/home/toto/document.txt` indique que le fichier `document.txt` se trouve dans le répertoire `toto`, lui-même dans le répertoire `home` qui, on l'a vu, est dans la racine matérialisée par la barre de division.

Notions de chemin absolu et de chemin relatif

Cette notion, très importante, donne deux façons différentes pour se situer au sein de l'arborescence des fichiers :

- le chemin **absolu** commence avec la spécification du répertoire racine.
- le chemin **relatif** commence avec le répertoire de travail c'est-à-dire celui **où l'on est** (à ne pas confondre avec le répertoire de l'utilisateur).

Exemple :

Si vous vous situez dans le répertoire `/home/toto`, la référence au fichier `cours.txt` situé dans le répertoire `alsi` se note :

- `/home/toto/notes/info/alsi/cours.txt` (chemin absolu)
- `notes/info/alsi/cours.txt` (chemin relatif)

Notez bien l'absence du `/` au début dans le chemin relatif car le départ ou répertoire de travail se note `/home/toto/`.

Les abréviations utiles

La première abréviation se traduit par un double point (`..`) et fait référence au répertoire parent de celui dans lequel on est.

Exemple :

Si vous êtes dans `/home/toto/ang`, la référence au fichier `script.sh` situé dans `prog` se note :

- `/home/toto/prog/script.sh` (chemin absolu : ne change pas)
- `../../prog/script.sh` (chemin relatif)

En lisant de la droite vers la gauche, le premier double point indique en fait le répertoire parent de `ang`, c'est-à-dire `notes` ; le deuxième indique `toto` (là où vous vous situez).

La deuxième abréviation, un seul point (`.`) fait référence au répertoire de travail lui-même.

Exemple :

En reprenant le même exemple :

- `./prog/chose.txt` (chemin absolu)
- `notes/info/alsi/truc.txt` (chemin relatif : ne change pas)

Le point au niveau du chemin absolu remplace la séquence `/home/toto`.

b. Commandes usuelles

1) Par rapport à l'arborescence du système de fichiers :

<code>pwd</code>	<i># retourne le chemin absolu du répertoire dans lequel # vous vous trouvez</i>
<code>cd</code>	<i># cette commande permet de se déplacer dans le système de # fichiers</i>

Exemples :

Je suis dans `/home/toto/prog/utils` et je veux aller dans le répertoire `alsi` :

- `cd /home/toto/notes/info/alsi` (par le chemin absolu)
- ou `cd ../notes/info/alsi` (par le chemin absolu)
- `cd ../../notes/info/alsi` (par le chemin relatif)

Je veux simplement remonter d'un niveau :

- `cd /home/toto/prog` (par le chemin absolu)
- ou `cd ../prog` (par le chemin absolu)
- `cd ..` (par le chemin relatif)



Les utilisateurs du système Windows et du DOS notent la présence obligatoire sur Ubuntu de l'espace entre la commande et le double point. Espace non nécessaire sur le système de Microsoft.

2) Lister le contenu des répertoires (déjà vu) :

`ls [options]` *# liste fichiers et répertoires*

Les options les plus courantes :

- a : liste tous les fichiers, y compris ceux cachés (commençant par un point)
- i : liste les fichiers et leurs inodes (voir le concept plus bas)
- s : liste les fichiers et leur taille en kilo-octets
- l : liste les fichiers avec plus de détails (format dit long)

Toutes les combinaisons d'options sont possibles.

Exemple :

`ls -ail /var` (liste le contenu du répertoire `/var`)


```

root@hardy:/etc# ls -ail /var/
total 48
 97537 drwxr-xr-x 14 root root 4096 2008-05-22 18:06 .
      2 drwxr-xr-x 22 root root 4096 2008-05-22 18:11 ..
105666 drwxr-xr-x  2 root root 4096 2008-05-22 17:47 backups
 97544 drwxr-xr-x  8 root root 4096 2008-05-22 18:06 cache
 97540 drwxr-xr-x 23 root root 4096 2008-05-25 11:26 lib
105669 drwxrusr-x  2 root staff 4096 2008-04-15 07:53 local
 5712  drwxrwxrwt  4 root root   100 2008-05-27 18:19 lock
105670 drwxr-xr-x  9 root root 4096 2008-05-27 11:27 log
105759 drwxrusr-x  2 root mail 4096 2008-05-22 17:46 mail
105758 drwxr-xr-x  2 root root 4096 2008-05-22 17:46 opt
 5708  drwxr-xr-x  8 root root   360 2008-05-27 11:28 run
105671 drwxr-xr-x  3 root root 4096 2008-05-22 17:53 spool
105672 drwxrwxrwt  2 root root 4096 2008-05-26 18:05 tmp
106903 drwxr-xr-x  2 root root 4096 2008-05-22 18:29 www
root@hardy:/etc#

```

3) Commandes sur les répertoires et les fichiers :

```

mkdir    # crée un répertoire
rmdir    # supprime un répertoire (attention : le répertoire doit
          # être vide)
touch    # crée un fichier de type texte (ASCII) vide
rm       # efface un fichier
cp       # copie un fichier ou répertoire
mv       # même démarche que la copie mais simplement un
          # déplacement

```

Exemples :

```

mkdir geosi : crée le répertoire geosi.
rmdir geosi : supprime le répertoire geosi.
touch essai.txt : crée le fichier vide essai.txt.
rm essai.txt : supprime le fichier essai.txt.
rm -f essai.txt : la même chose sans demande de confirmation.
cp essai.txt notes/ang : copie le fichier dans le répertoire ang.
cp essai.txt notes/ang/test.txt : cette fois en changeant le nom.

```

4) La recherche d'un fichier :

```
find # cherche un fichier
```

C'est une commande plus complexe que les précédentes. En voici la forme d'utilisation la plus courante :

```

find -name toc.txt      # cherche le fichier toc.txt dans le
                        # répertoire courant
find /home -name "test*" # cherche tous les fichiers ou répertoire
                        # commençant par test à partir d
                        # répertoire home (l'étoile remplace le
                        # reste)

```

On lui préfère l'outil `locate`, couplé avec la commande `updatedb` plus simple d'utilisation. La commande `find` retourne beaucoup d'erreurs en allant chercher là où elle ne possède pas les droits suffisants. Sur une distribution serveur Ubuntu, le paquetage logiciel (de nom `locate`) est installé par défaut. La première étape consiste à lancer la simple commande `updatedb` destinée à répertorier dans une base l'ensemble des fichiers :

```
updatedb
```

Ensuite pour chercher, la commande `locate` est suivie du nom du fichier (partiel ou complet), précédé éventuellement d'une indication de répertoire :

locate [rep] motif

Exemple :

locate /etc "conf" : recherche tous les éléments contenant le motif conf dans son intitulé.

L'avantage réside dans la rapidité de la recherche, l'inconvénient dans l'obligation de relancer périodiquement la commande updatedb afin de mettre à jour la base d'index.

5) Commandes particulières :

```
cat          # concatène des fichiers et les affiche sur la
              # sortie standard (écran par défaut)
```

Bien que plutôt réservée sur les fichiers cette commande très puissante possède bien d'autres fonctionnalités... Nous ne voyons pour l'instant que :

```
cat nom_de_fichier      # affiche le contenu d'un fichier
cat > nom_de_fichier     # crée un fichier
```

Dans ce dernier cas, vous tapez directement les lignes de texte désirées par le clavier à la suite de la commande. La fin de saisie s'effectue par [Ctrl] d. L'administrateur utilise la commande cat sur des petits fichiers afin d'en visualiser rapidement le contenu.

```
Clear        # efface toute la console et replace le curseur
              # en haut à gauche de l'écran
whoami       # donne le nom de l'utilisateur courant
hostname     # donne le nom de la machine
```

Ces trois dernières commandes ne posent aucune difficulté.

3. Travailler sur les fichiers

a. Types de fichiers

Un fichier au sens UNIX (et Linux) représente à la fois une source de données (à lire) ou une destination pour ces données (à écrire). La structure arborescente se compose de nœuds ou répertoires et de feuilles ou fichiers. On peut donc avoir :

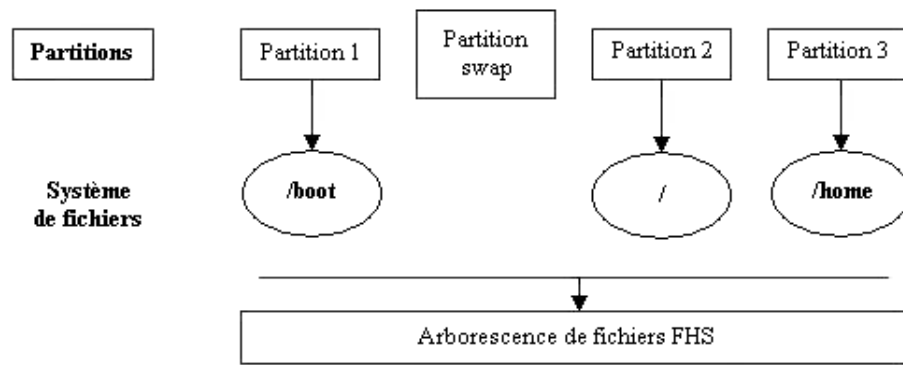
- le fichier **répertoire** : fichier particulier contenant des références vers d'autres fichiers (pointeurs). Au sens littéral du terme, un fichier répertoire ne "contient" pas ses fichiers, mais seulement les liens vers ceux-ci. Un fichier répertoire contient au minimum une référence : celle du répertoire qui le contient (parent), sauf pour la racine principale / évidemment.
- le fichier **ordinaire** : fichier contenant des données. Les plus nombreux, ils peuvent être de type texte ou binaire.
- le fichier **spécial** : fichier dit de "dispositif", il représente un périphérique physique : clavier, écran, disques durs, lecteur USB, etc.

D'autres "types" de fichiers (encore que cela soit impropre comme appellation) existent :

- Les **liens** : pointeurs vers d'autres fichiers.
- Les **tubes** : redirection des entrées/sorties.
- Les **sockets** : canaux de communication inter-processus.

On l'a vu, le système de fichiers Linux se construit en arborescence et il utilise pour enregistrer chaque élément une table des **i-nœuds** ou **inodes**. Chaque création de système de fichiers (sur une partition) sous Linux s'accompagne d'une table des inodes.

En voici un exemple :



La partition swap ne donne pas lieu à une table des inodes. Elle est employée par le système comme extension de la mémoire RAM (mémoire virtuelle). Le *Filesystem Hierarchy Standard* définit l'organisation du système de fichiers commune (théoriquement) à toutes les distributions.

Il ne faut pas confondre organisation du système de fichiers et type de systèmes. L'apparition de systèmes de fichiers journalisés plus robustes, comme **ReiserFS** ou **ext3fs** (intégrés au noyau) ou **jfs** (IBM, maintenant très performant) ou **xfs** (plus robuste) ne change rien dans l'arborescence FHS, ni fondamentalement dans le principe des inodes. En gros, ce nouveau type de fichiers utilise le principe du cache tiré du monde des SGBD.

b. Processus de création d'un fichier

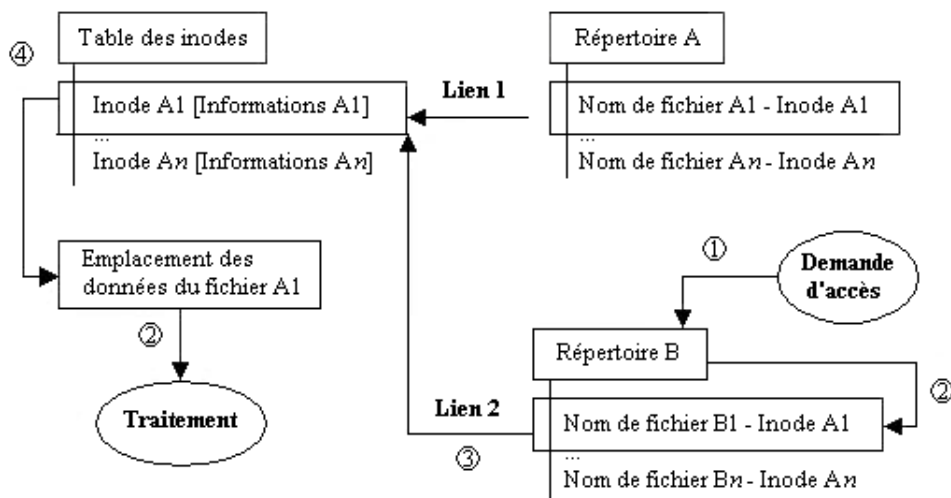
Une fois définie la table des inodes (créée à l'initialisation du système de fichiers), le processus de création d'un fichier est donc le suivant :

- Détermination de l'espace sur le disque pour stocker les données du fichier.
- Création d'un inode unique (appelé aussi nœud d'index) contenant des informations : emplacement, propriétaire, etc.
- Mise en place dans le fichier répertoire du couple **inumber** (numéro) et nom de fichier.

c. Pointeur sur un fichier : le lien

Quand un utilisateur désire manipuler un fichier, le système recherche le nom dans le fichier répertoire, trouve l'inumber et récupère les données correspondantes dans la table des inodes.

Cette relation entre le nom de fichier et son inode s'appelle un lien. Sous Linux, un même fichier peut disposer de plusieurs liens et donc de plusieurs noms différents. C'est un mécanisme important et, même si vous n'en voyez pas l'intérêt de prime abord, il est important d'en connaître les mécanismes. Les liens multiples sont possibles car ce n'est pas le nom qui identifie un fichier mais son inumber. Le plus simple consiste à examiner le schéma suivant :



On constate :

- L'existence de deux noms de fichiers différents avec le même inode.
- Une modification du fichier B1 (départ de la demande en) entraîne une modification sur A1 car, en fait, le fichier de données est unique.
- La possibilité de créer un lien avec la commande `ln` (voir ci-dessous), ce qui incrémente un compteur.
- Une copie du fichier créée (un fichier avec un inode différent), ce n'est donc pas un lien supplémentaire. Ce type de liens s'appelle liens "en durs" et ne peuvent s'appliquer que dans le système de fichier. Pour créer un lien entre deux fichiers dans deux systèmes différents, on utilisera des liens dits "symboliques".

d. Commandes usuelles

1) Commandes classiques :

<code>cmp</code>	# compare deux fichiers, affiche un message en cas # de différence (plutôt pour les fichiers binaires)
<code>diff</code>	# trouve les différences entre des fichiers
<code>file</code>	# donne le type d'un fichier
<code>head</code>	# affiche le début d'un fichier
<code>basename</code>	# élimine le chemin d'accès d'un fichier
<code>paste</code>	# regroupe les lignes de plusieurs fichiers
<code>stat</code>	# affiche des renseignements et statistiques sur un # fichier ou répertoire
<code>tail</code>	# affiche les dernières lignes d'un fichier
<code>whereis</code>	# recherche les fichiers exécutables, les sources et les # pages de manuel
<code>which</code>	# localise une commande

La plupart des commandes sont à découvrir à l'aide du manuel en ligne, mais l'une d'entre elles mérite qu'on s'y arrête. Il s'agit de la commande `tail`, très utile à l'administrateur pour voir le contenu des journaux, plus précisément pour voir en temps réel le résultat d'une manipulation.

On veut voir par exemple en temps réel ce qui se passe sur la machine à partir du journal général :

- Ouvrez une console supplémentaire avec une connexion en administrateur ([Alt][F2]).
- Tapez la commande `tail -f /var/log/syslog`.

Le résultat affiche la fin du fichier du démon général `syslog` et ne se ferme pas. Une manipulation ultérieure sur une autre console entraînant un message sera visible immédiatement en s'inscrivant à la fin du fichier.

2) Commandes sur les liens :

La commande `ls` avec l'option `-l` pour inode liste les liens :

<code>ls -li</code>	# liste les fichiers avec les numéros d'inodes du # répertoire courant
---------------------	---

Il existe aussi la commande spécifique `ln` qui crée un lien supplémentaire :

```
ln [-s] fichier_source fichier_cible
```

Exemple :

`ln nafnaf.txt nifnif.txt` : crée un nouveau pointeur sur le fichier `nafnaf.txt`.

L'option `-s` permet de créer un lien symbolique (à ne pas utiliser pour l'instant !). Par analogie, on peut dire que cette notion s'apparente au raccourci sur un bureau graphique.

3) Autres commandes spécifiques au système de fichiers :

<code>du</code>	# affiche des statistiques d'utilisation du disque
<code>df</code>	# donne la quantité d'espace occupé des systèmes de

	# fichiers
badblocks	# recherche des blocs défectueux sur un périphérique
fdisk	# utilitaire de manipulation de la table de
	# partition d'un disque
mount	# monte un système de fichiers
umount	# démonte un système de fichiers

Exemples d'utilisation :

du -hs /etc : affiche en Ko ou Mo le poids total du répertoire /etc.

df -h : affiche par système de fichiers la taille, le poids, l'utilisation et son pourcentage.

4. Entraînement

Comme pour la compréhension des droits utilisateurs, les notions abordées dans ce chapitre nécessitent un minimum de pratique. Afin de vous aider dans la maîtrise des commandes, voici une liste de **questions/exercices** (les solutions se trouvent toujours en Annexe) :

Cadre de travail

Session ouverte en `root` sur une version Ubuntu serveur.

Exercices

- Tapez la commande permettant de voir dans quel répertoire vous êtes.
- Listez normalement le contenu de votre répertoire.
- Listez le contenu du répertoire avec les fichiers cachés et le format long.
- Utilisez le manuel en ligne pour connaître et comprendre la commande `sleep`.
- Tapez maintenant `sleep --help`, quelle en est l'utilité ?
- Si vous tapez `sleep 360`, quelle combinaison de touches permet de l'interrompre ? Testez-la.
- Quelle est la taille du répertoire `/usr` ?
- Allez dans le répertoire `/etc` par le chemin absolu.
- Faites un tube avec d'un côté la commande `ls *.conf`, de l'autre `wc -l`, quel en est le résultat ?
- Tapez tout simplement `cd` et validez. Que s'est-il passé ? Que signifie le tilde (`~`) ?
- Allez dans votre répertoire et créez deux sous-répertoires : `hobbit` et `elfe`, vérifiez la création par la commande appropriée.
- Allez dans `hobbit` et créez trois fichiers `merry`, `pipin` et `gollum` par la commande `touch`.
- Sans changer de répertoire, créez le sous-répertoire `elfedesbois` dans `elfe` et par le chemin relatif.
- Sans changer de répertoire, créez le fichier `legolas` dans votre répertoire personnel et par le chemin absolu.
- Allez dans `elfedesbois` obligatoirement en trois commandes (niveau par niveau).
- Sans changer de répertoire, déplacez `legolas` pour le mettre là où vous êtes et par le chemin relatif.
- Sans changer de répertoire renommez `gollum` en `sam` par le chemin absolu.

- Trouvez, par la commande `find`, le fichier `interfaces` à partir de `/etc`.
- Retournez dans votre répertoire et créez le fichier `riri.txt`.
- Dupliquez-le par la commande `cp` en changeant son nom en `fifi.txt`.
- Créez un lien par `ln` en changeant son nom en `loulou.txt`.
- Éditez les inodes par `ls` et l'option adéquate et concluez.
- Par VIM, mettez une phrase dans `riri.txt`.
- Éditez `fifi.txt` et `loulou.txt` ; concluez.
- Effacez `riri.txt`, que s'est-il passé pour `fifi.txt` ?
- Quel est le type du fichier `/etc/passwd` ?

Système X Windows Xorg

1. Gestion de l'installation

Le système graphique Xorg, projet Linux autonome, est un **fork** d'X11, le standard d'interface graphique (GUI pour *Graphical User Interface*). Il fonctionne en mode client/serveur afin d'ouvrir une console graphique (terminal X), aussi bien sur la machine qu'à partir d'un ordinateur distant.

Voici l'adresse du site Xorg sur Internet : <http://xorg.freedesktop.org/wiki/>

Un fork définit un nouveau processus enfant au sens de la programmation système (langage C) et une variante d'un projet informatique dans le cas d'Xorg.



La démarche qui suit montre l'installation de A jusqu'à Z d'un serveur graphique et des ses composants à partir d'une distribution en mode serveur. Étant entendu que sur une version poste de travail, tout est déjà fait.

a. Serveur X minimal

La version sur une distribution Ubuntu Hardy Heron porte le numéro **X11R7.3**, en licence libre adaptée par l'X.Org Foundation, à la fois OpenSource et logiciel libre. Les applications graphiques se situent dans le répertoire `/usr/X11R6/bin`. Sur Ubuntu 8.04.1 et à **partir d'une version serveur**, l'environnement graphique s'obtient avec le paquet du même nom (96 dépendances) :

```
aptitude install xorg
```

Peu de différences avec le paquet `xserver-org`, si ce n'est qu'il est plus complet car installant cinq paquetages supplémentaires, `xorg` installant d'ailleurs `xserver-org` en dépendance.

Xorg installe un terminal X (il s'intitule `xterm`) qui se lance par défaut lorsque l'on démarre le serveur X par le script `startx`. Mais il faut le reconnaître : peu enthousiasmant, et n'offrant au premier abord aucune différence avec une console de type texte. Parfaitement fonctionnel, il lance les applications graphiques. Par exemple, dans le terminal, installez le navigateur Web Firefox, et lancez-le :

```
startx
```

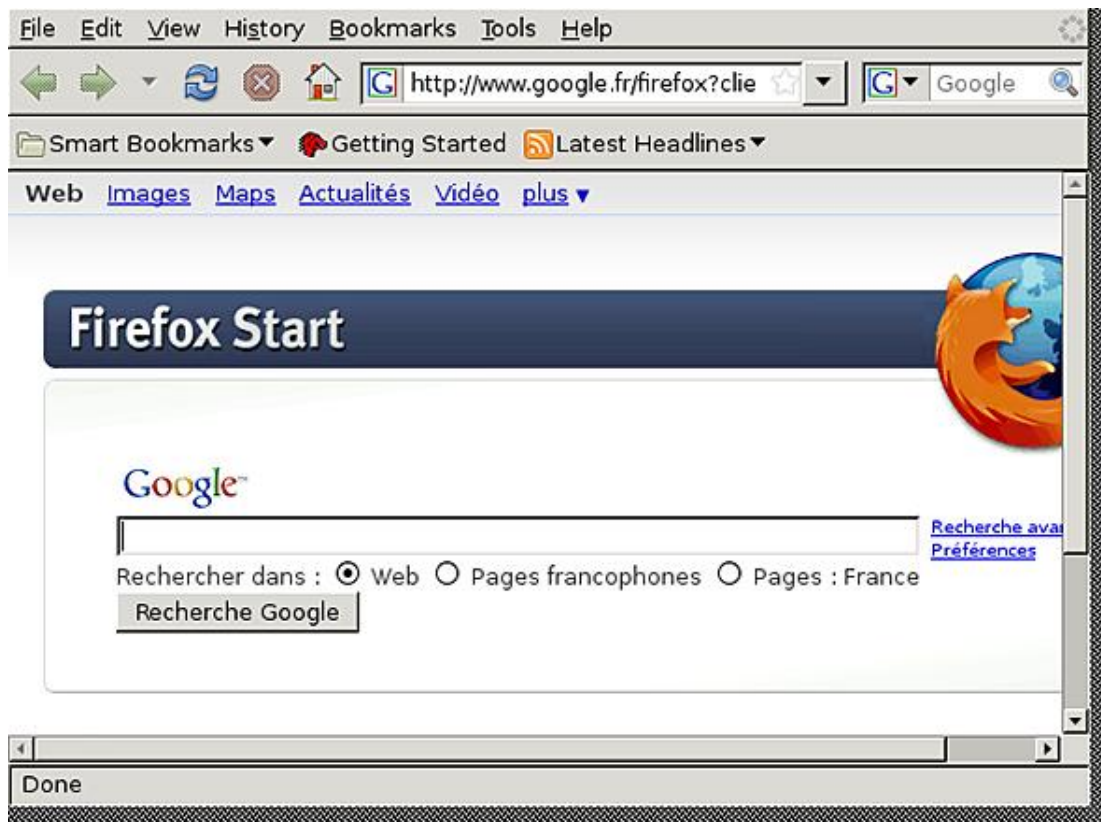
```
aptitude install firefox
```

```
firefox &
```



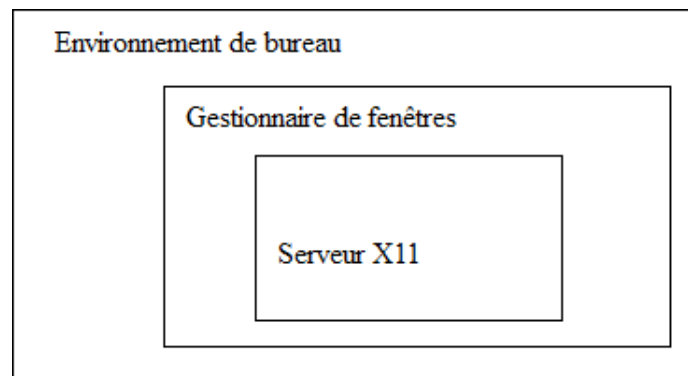
Le "et" commercial (&) ou esperluette détache l'application graphique de la console qui peut alors être à nouveau utilisée. L'exemple présenté le montre en revenant sur la ligne de commande avant le lancement de Firefox. Après, le navigateur remplit entièrement l'espace.

La sortie du serveur graphique se fait par la commande `exit` dans la console.



b. Composants d'un environnement graphique

Jusqu'à présent, les aspects graphiques du serveur X ne paraissent pas probants. En fait, le serveur constitue le noyau d'un ensemble en trois couches :



Le gestionnaire de fenêtres (*window manager*) se charge de dessiner les fenêtres et leurs interactions avec le serveur X11. L'environnement de bureau (*desktop manager*) fournit un cadre de développement d'applications. Les deux vont souvent par paires :

- l'environnement GNOME avec le gestionnaire de fenêtres **Metacity**.
- l'environnement KDE avec le gestionnaire de fenêtres **Kwin**.
- l'environnement XFCE avec le gestionnaire de fenêtres **Xfwm4**.

Pour ne citer que les trois principaux. Si l'on désire des environnements plus légers encore que XFCE, on a le choix sous Ubuntu : FluxBox, Enlightenment, Fvwm, IceWM, WindowMaker, etc.

Xorg gère la présence de plusieurs environnements de bureau en même temps sur le serveur et fait fonctionner - même si cela n'est pas conseillé - des applications d'un environnement de bureau à partir d'un autre. Exemple : éditeur de texte **Kate** ou le logiciel de gravure **K3b** de KDE sur GNOME. Il suffit d'installer les bibliothèques correspondantes :

- GNOME fonctionne avec les librairies QT (dérivées)
- KDE fonctionne avec les librairies GTK/GTK+

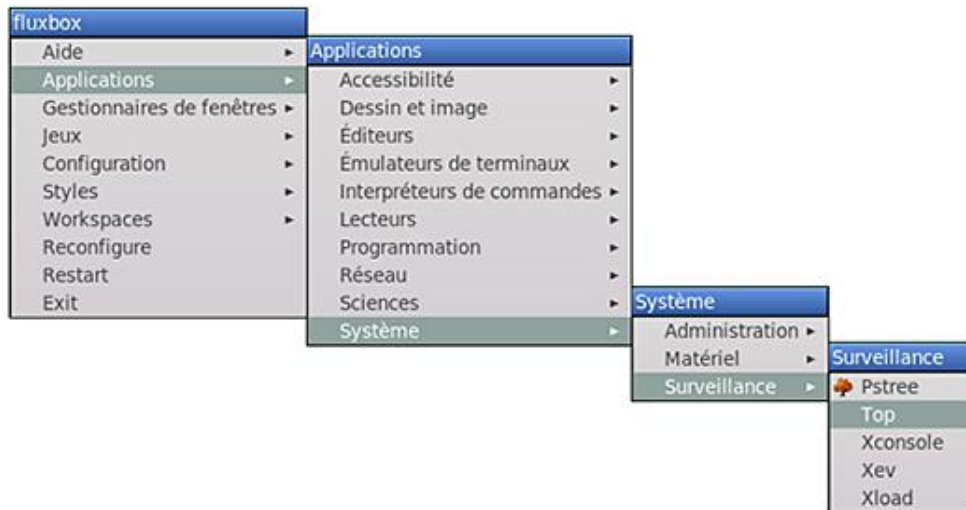
c. Gestionnaire de fenêtres FluxBox

Ce gestionnaire récent se distingue sur Ubuntu avec une version spécialement orientée. Voici l'adresse de son site Internet : <http://fluxbox.org/>

Indépendamment, il est tout à fait possible de l'installer sur une version serveur car vraiment légère et peu gourmande en ressources. En reprenant l'exemple, on aura :

```
aptitude install fluxbox
```

```
startx
```



Ce type de gestionnaire est idéal pour un serveur où l'administrateur désire faire de la virtualisation et donc disposer d'un cadre graphique le plus léger possible.

La configuration de FluxBox se trouve dans le répertoire personnel de l'utilisateur et dans le sous-répertoire caché .fluxbox. Il comporte :

- les répertoires background, pixmaps, styles
- les fichiers init, keys, menu, slitlist et startup

La configuration de FluxBox, simple dans l'ensemble devrait se faire dans son acceptation minimale, partant du principe que si l'on désire un environnement avec fonds d'écran, icônes, lanceurs, etc. Il vaut mieux utiliser un autre gestionnaire comme XFCE. La documentation se trouve naturellement sur le site officiel.

2. Configuration du serveur Xorg

a. Configuration manuelle par le fichier xorg.conf

Le fichier de configuration générale d'Xorg se trouve dans `/etc/X11/xorg.conf` et est composé de sections de la forme :

```
Section "Nom de la section"  
    Entrée1 de la section  
    Entrée2 de la section  
    ...  
EndSection
```

Avec comme noms des sections :

Files

Chemin des fichiers.

ServerFlags

Valeurs de paramétrage du serveur.

Module

Module en chargement dynamique.

InputDevice

Description de périphérique d'entrée.

Device

Description de périphérique graphique.

VideoAdaptor

Description de l'adaptateur vidéo.

Monitor

Description du moniteur vidéo.

Modes

Description des modes vidéo possibles.

Screen

Description de l'écran.

ServerLayout

Présentation.

DRI

Configuration spécifique pour DRI.

Vendor

Configuration spécifique du vendeur.

Normalement, la détection initiale ne pose pas de problème et le serveur graphique a de grandes chances d'être bien configuré. Il arrive cependant que l'on soit amené à modifier les configurations pour des raisons diverses :

mauvaise détection des capacités de l'écran, adaptation à un pilote graphique particulier, etc.

Plus précisément, il est important de détailler la configuration de quatre sections :

Section Inputdevice

Statut : obligatoirement présent par deux fois ; l'une pour le clavier, l'autre pour un pointeur, (classiquement, une souris).

Exemple de section :

```
Section "InputDevice"
    Identifier "Generic Keyboard"
    Driver      "kbd"
    Option      "XkbRules"      "xorg"
    Option      "XkbModel"      "pc105"
    Option      "XkbLayout"     "fr"
    Option      "XkbVariant"    "oss"
EndSection
```

Entrées de la section :

Identifier : entrée obligatoire spécifiant le nom unique du périphérique d'entrée.

Driver : entrée obligatoire spécifiant le nom du pilote du périphérique d'entrée.

Option :

CorePointer : entrée facultative désignant une souris.

CoreKeyboard : entrée facultative désignant un clavier.

AlwaysCore : valeur booléenne.

SendCoreEvents : option équivalente à la précédente et permettant au périphérique de générer des évènements.

HistorySize : donne la taille de l'historique, à 0 par défaut.

SendDragEvents : valeur booléenne (non documentée).

Section Monitor

Statut : obligatoirement présent une fois, cette section peut être multiple en cas de moniteurs différents.

Exemple de section

```
Section "Monitor"
    Identifier "Generic Monitor"
    Option      "DPMS"
    HorizSync   30-96
    VertRefresh 50-150
EndSection
```

Entrées de la section :

Identifier : entrée obligatoire spécifiant le nom unique du moniteur.

Option "DPMS" : entrée signifiant *Display Power Management System* et visant la faculté d'extinction automatique de l'écran.

VendorName : entrée facultative désignant la marque du moniteur.

ModelName : entrée facultative désignant le modèle du moniteur.

HorizSync : intervalle de valeurs définissant clairement les bornes techniques ou fréquences horizontales du moniteur (très important selon moi pour ne pas mettre en péril le matériel).

VertRefresh : même principe, avec pour cette fois la définition des fréquences maximales verticales.

DisplaySize : largeur et hauteur en millimètres de l'image pour le moniteur utilisées pour calculer le pitch (valeur entre deux pixels) de l'écran.

Section Screen

Statut : obligatoirement présent une fois, cette section pour être viable, comporte la référence à un pilote de carte graphique et à un moniteur ; elle comporte éventuellement des sous-sections destinées à offrir un éventail de modes à l'utilisateur.



Les définitions inscrites dans cette section l'emportent sur l'outil de configuration dans le bureau GNOME. Autrement dit, si vous limitez la résolution dans le fichier à 1024x768, vous ne pourrez en aucun cas en définir une plus grande dans l'outil de configuration gnome-display-properties.

Exemple de section :

```
Section "Screen"
    Identifier "Default Screen"
    Device      "Generic Video Card"
    Monitor     "Generic Monitor"
    DefaultDepth 24
    SubSection "Display"
        Depth    4
        Modes     "1024x768" "800x600" "640x480"
    EndSubSection
    SubSection "Display"
        Depth    8
        Modes     "1024x768" "800x600" "640x480"
    EndSubSection
    SubSection "Display"
        Depth    16
        Modes     "1024x768" "800x600" "640x480"
    EndSubSection
    SubSection "Display"
        Depth    24
        Modes     "1024x768" "800x600" "640x480"
    EndSubSection
EndSection
```

Entrées de la section :

Identifiant : entrée obligatoire spécifiant le nom unique de l'écran.

Device : entrée obligatoire indiquant l'identifiant du pilote de la carte défini au préalable dans une section Device.

Monitor : même remarque, cette fois pour l'identifiant d'un moniteur de la section Monitor.

ModelName : entrée facultative désignant le modèle du moniteur.

DefaultDepth : valeur représentant le nombre de couleurs par défaut.

SubSection "Display" : sous-section définissant, à chaque fois, la profondeur de couleur et les modes de résolution possibles ; se termine obligatoirement par l'instruction EndSubSection.

Section ServerLayout

Statut : section obligatoire effectuant la liaison entre les différents éléments du fichier afin de définir une "mise en page" du serveur graphique ; elle se remplit donc avec les identifiants des autres sections.

Exemple de section

```
Section "ServerLayout"
    Identifier "Default Layout"
    Screen      "Default Screen"
    InputDevice "Generic Keyboard"
    InputDevice "Configured Mouse"
EndSection
```

Entrées de la section :

Identifiant : entrée obligatoire spécifiant le nom unique de la présentation.

Screen : entrée donnant l'identifiant de la section Screen.

InputDevice : entrées donnant les identifiants classiquement au nombre de deux, pour le clavier et la souris.



D'autres options existent pour ces sections, mais ne sont pas vues car peu courantes.

Autres exemples de section

Ces deux sections dépendent des spécifications matérielles que l'on ne peut inventer. Il faut se reporter aux manuels des équipements considérés.

Section `InputDevice` pour une tablette de souris sensitive :

```
Section "InputDevice"
    Identifier "Synaptics Touchpad"
    Driver     "synaptics"
    Option     "SendCoreEvents"      "true"
    Option     "Device"               "/dev/psaux"
    Option     "Protocol"              "auto-dev"
    Option     "HorizEdgeScroll"       "0"
EndSection
```

Section `Device` pour un pilote de carte graphique **Nvidia** :

```
Section "Device"
    Identifier "Configured Video Device"
    Driver     "nvidia"
    Option     "NoLogo"               "True"
EndSection
```

b. Utiliser la commande de configuration `dpkg-reconfigure`

À partir de l'utilitaire `dpkg`, la commande `dpkg-reconfigure` se base sur `debconf` pour configurer à nouveau un paquet déjà installé. Pour le serveur graphique, la commande complète sera :

```
dpkg-reconfigure -phigh xserver-xorg
```

L'option `phigh` indique une priorité élevée pour la configuration, c'est-à-dire la plus complète (niveau expert). Les questions posées concernent :

- L'utilisation de l'interface de mise en tampon (`framebuffer`) : non par défaut car dépendant du matériel installé (à tester donc).
- La recherche automatique de la disposition du clavier : non par défaut car il vaut mieux affiner par des entrées manuelles.
- La disposition du clavier : pour les français, le type `fr`.
- Le jeu de définitions XKB : `xorg` par défaut, ce qui correspond à la plupart des cas (claviers Sun exceptés).
- Le type de clavier : les claviers modernes européens utilisent le type `pc105`.
- La gestion des touches : à la suite du type `pc105`, le jeu `latin9` respecte les caractères français.
- La définition d'option : celle par défaut `lv3;ralt_switch` indique que l'appui de la touche `[Alt]` côté droit (`[Alt Gr]`) entraîne le troisième caractère de niveau de la touche appuyée (exemple | pour `[Alt Gr]` **6**).

Au final la base `debconf` sera mise à jour, le fichier `xorg.conf` réécrit et le fichier précédent sauvegardé avec une extension comportant la date de modification suivi d'un index.

À l'inverse, l'utilitaire `dexconf` reconfigure le fichier de configuration `xorg.conf` à partir des informations de la base issues de `debconf`. Il ne positionne aucune valeur dans la base à la différence de la commande `dpkg-reconfigure`. Pour en voir le fonctionnement, il suffit de modifier une valeur dans le fichier `xorg.conf`, de lancer sans argument la commande `dexconf` et d'éditer à nouveau le fichier `xorg.conf` : les modifications ont disparu.

Pour l'administrateur, cela permet de revenir à un fichier `xorg.conf` propre après des modifications manuelles hasardeuses et qui ne fonctionnent pas.



En fonction des fabricants et des types de cartes, certains outils existent pour une configuration adaptée avec toujours par exemple pour les cartes Nvidia, le paquet `nvidia-settings`.

c. Utiliser la commande graphique `displayconfig-gtk`

Quelquefois dans certaines situations matérielles, la commande `dpkg-reconfigure` n'aboutit pas au résultat voulu en ne posant pas les questions concernant la carte graphique. Une autre commande existe, plus performante mais dans un environnement graphique : la commande `displayconfig-gtk` :

- Dans un terminal avec les droits administrateurs, lancez la commande `displayconfig-gtk &`.

L'onglet intéressant est celui de la carte graphique où l'on peut choisir son modèle. Pour connaître celui-ci, il suffit de taper la commande `lspci` (toujours dans un terminal) et identifier la ligne traitant du contrôleur VGA.

La validation des préférences d'affichage et d'écran entraîne l'écriture d'un nouveau fichier `xorg.conf` (l'ancien est sauvegardé dans le répertoire de façon à pouvoir le reprendre en cas de problèmes).

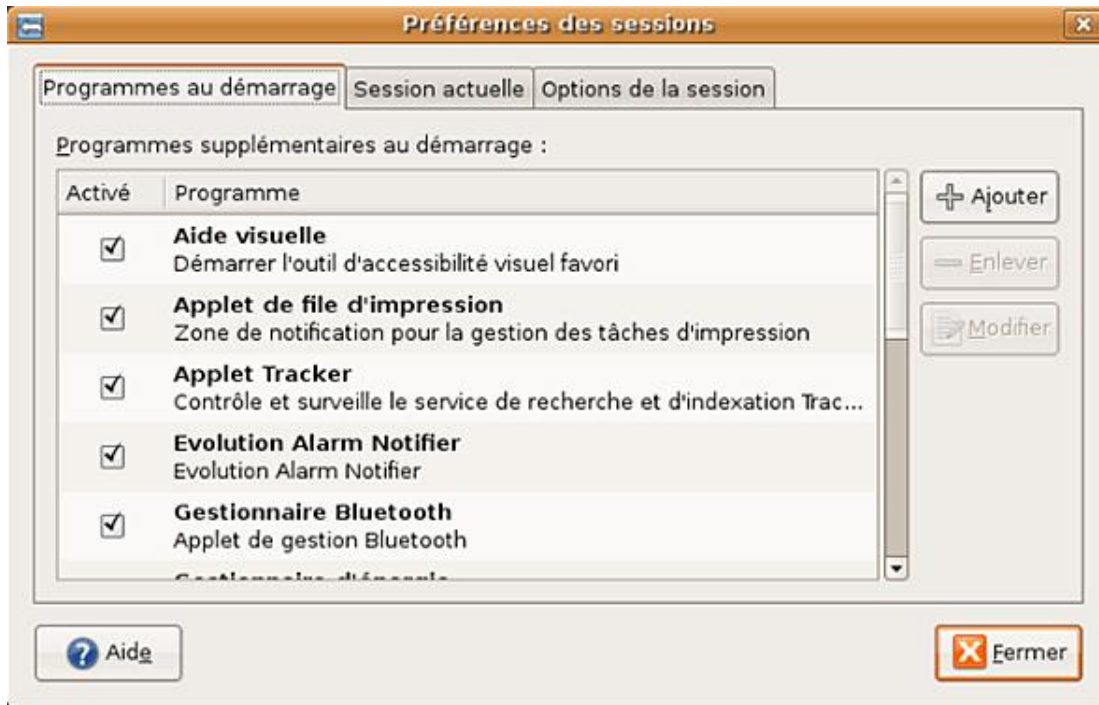
Environnement et cadre de travail

Peu de différence, dans le fond, sur une session graphique par rapport à une session en mode texte. Par contre, l'emploi de la commande `sudo` dans un terminal s'impose lors de commandes d'administration (voire `sudo -i` pour être tranquille une fois pour toutes), par le fait qu'une session graphique est par nature ouverte par un utilisateur. Comme indiqué dans le chapitre Prise en main de la distribution, la préférence va pour l'installation de logiciels à un terminal avec Aptitude, plutôt que par l'outil Synaptic.

1. Paramétrage d'une session graphique à l'ouverture

Il est possible de régler finement les programmes (applets) GNOME lancés au démarrage d'une session (à ne pas confondre avec les services lancés au démarrage de la machine) :

Lancez le programme `gnome-session-properties` par les menus **Système - Préférences - Sessions** :



Certains programmes tournent en tâche de fond et ne se manifestent (les alarmes de notification de nouvelles mises à jour, par exemple) qu'en cas de besoin. Dans le cas d'une machine à faibles performances graphiques, enlever des applets au démarrage libérera des ressources.

Le dernier onglet vous évite de rouvrir les applications courantes : un développeur démarrera automatiquement son environnement de travail (IDE) favori.

2. Organisation du bureau

On appelle tableau de bord les bandes horizontales en haut et en bas de l'écran. Chacune se règle indépendamment l'une de l'autre par un clic droit de la souris sur un espace libre de la bande choisie, amenant un menu avec les actions principales suivantes :

- L'ajout ou la suppression d'un tableau de bord. Attention : la suppression entraîne aussi celle de son contenu ; il ne faut donc surtout pas les enlever en totalité ou vous ne pourrez plus rien faire.
- La modification des propriétés du tableau de bord avec la disposition, la taille, etc.
- L'ajout d'éléments au tableau de bord : un choix à faire parmi une liste.

Gnome-dictionary : l'applet dictionnaire

La liste est longue dans le choix des propositions et s'il ne faut en retenir qu'une, je conseille la recherche dans un **dictionnaire** :

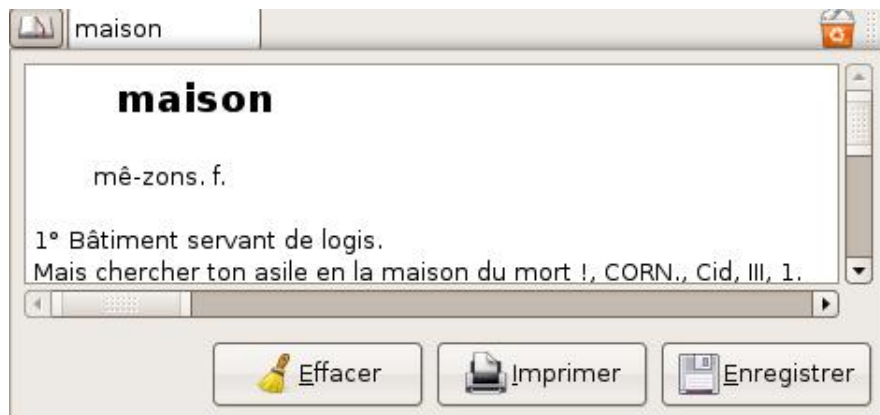
- Cliquez avec le bouton droit de la souris dans le tableau de bord désiré et choisissez **Ajoutez au tableau de bord**.
- Choisissez la ligne **Rechercher dans un dictionnaire** et validez par le bouton **Ajouter**.

Si vous tapez un mot dans la petite fenêtre à droite du livre, vous ne trouverez rien ! En fait, le mot a été introduit en français alors que le dictionnaire est par défaut un dictionnaire anglais.

Deux remarques :

- Le dictionnaire est en ligne sur Internet avec utilisation d'un protocole particulier (port 2628 ou 2629 par SSL).
 - Très peu de dictionnaires en français existent (je n'en ai trouvé qu'un et partiel), la liste se cherche à l'adresse : <http://luetzschemastahmeln.de/dictd/index.php>
- Cliquez avec le bouton droit de la souris dans le tableau de bord désiré et choisissez **Préférences**.
 - Cliquez sur le bouton **Ajouter** et indiquez **Dictionnaire français** pour la description, **vocabulary.aioe.org** pour le nom d'hôte (autres éléments inchangés).
 - Validez et fermez.

Une nouvelle recherche avec un mot français devrait retourner cette fois une définition en français (exemple : maison). Par contre, d'autres mots en français risquent de retourner des définitions anglaises, surtout si les termes se rejoignent.



3. Autres préférences

L'essentiel des réglages du bureau se trouve dans les menus **Système - Préférences**. Citons pour les principaux :

- **Apparence** : réglages de l'aspect visuel du bureau, le fonds d'écran, etc.
- **Applications Préférées** : associations entre fichier et applications.
- **Menu principal** : choix des applications dans les différents menus.

Exemple :

Vous décidez d'utiliser le lecteur multimédia **VLC Media Player** (<http://www.videolan.org/vlc>) en lieu et place du lecteur **Rhythmbox**. En voici la démarche :

- aptitude install vlc

- Menus **Système - Préférences - Applications préférés**, onglet **Multimédia**.

- Choisissez **Personnalisé** dans la liste et indiquez en commande `vlc %U`.

Note : GNOME lancera VLC lorsqu'il décide à votre place, alors qu'au niveau du système de fichiers, un double clic sur l'icône d'une vidéo lance toujours le lecteur vidéo. Pour qu'il lance VLC à la place, vous devez faire le changement par un clic droit sur l'icône, menu **Propriétés**, onglet **Ouvrir avec** et choisir le bon lecteur.

- **A propos de moi** : renseignements sur l'utilisateur.
- **Bureau à distance** : basé sur l'outil **Vinagre**, contrôle d'accès à distance du bureau.
- **Menu principal** : gère les applications du menu principal ; on peut par exemple enlever le menu **Jeux...**
- **Recherche et indexation** : équivalent graphique de l'outil **locate**, **Tracker** indexe les fichiers du système dans le but d'en faciliter la recherche.

Les autres réglages ne présentent pas de difficultés.

Personnalisation du bureau GNOME

Le système X Window apporte la dimension graphique nécessaire à l'utilisation du système Ubuntu Desktop. La nouvelle mouture du système graphique Xorg basée pour Ubuntu sur le gestionnaire de fenêtres en **3D Compiz Fusion** dépasse par sa rapidité, son ergonomie - et on peut le dire, sa primauté - le système Windows car il fût réalisé (anciennement Beryl et Compiz) avant la sortie de Vista et son interface graphique Aero.

1. Avoir un bureau en 3D

La mise en place d'un bureau 3D est intimement liée à la présence d'une carte graphique performante. Pour mettre en place le pilote adapté, la procédure d'utilisation se trouve dans les menus **Système - Administration**, ligne **Pilotes de périphériques** (déjà vu au chapitre Préalable à l'installation). N'oubliez pas d'effectuer une mise à jour des sources de logiciels avant d'activer le pilote propriétaire (dépôt restricted, cas des deux grands que sont ATI et Nvidia).

a. Réglages par défaut

Les paquetages logiciels concernés sous Ubuntu commencent tous par le mot `compiz` (sauf la librairie). Suivant l'environnement de bureau, le paquetage adéquat est chargé par défaut : `compiz-gnome` pour l'environnement de même nom :

- `compiz` : le paquetage OpenGL de l'environnement.
- `compiz-core` : base du paquetage OpenGL.
- `compiz-plugins` : effets et propriétés de base du bureau 3D.
- `compiz-gnome` : cadre GNOME pour les fenêtres.
- `compiz-fusion-plugins-extra` et `main` : collection de plug-ins supplémentaires.
- `compizconfig-backend-gconf` : librairie pour les plug-ins.
- `libcompizconfig0` : librairie de base.

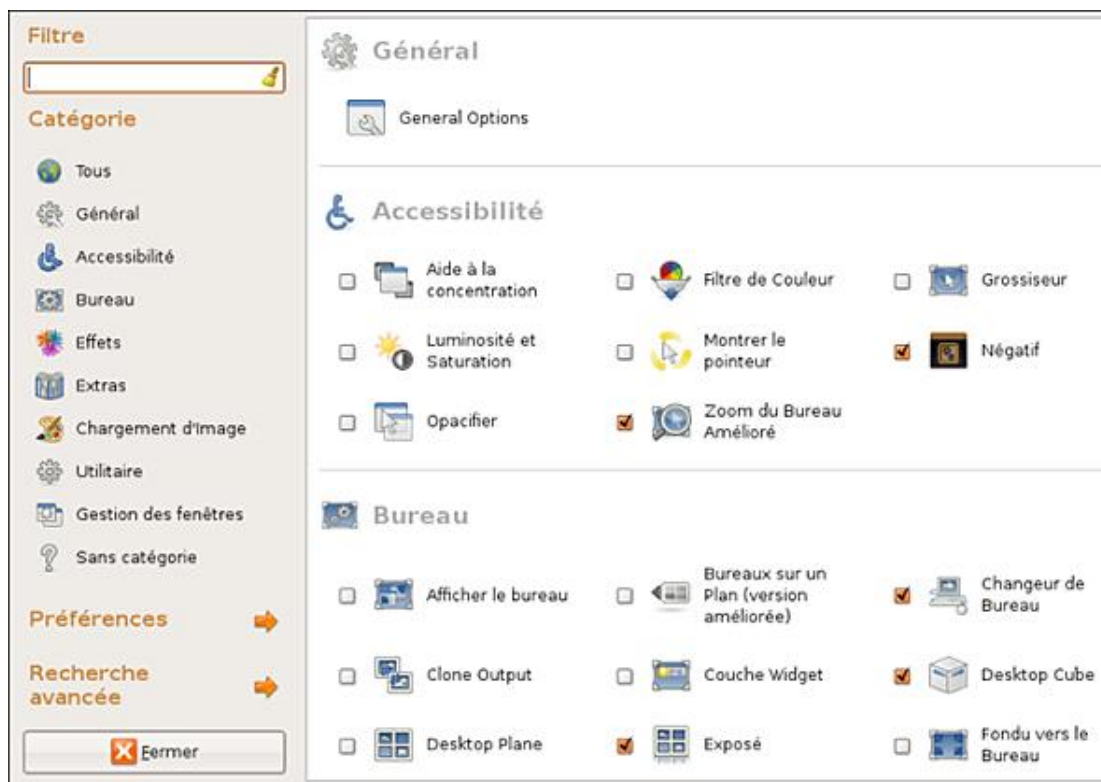
La mise en place du bureau 3D se trouve par **Système - Préférences - Apparence** avec sélection de l'onglet **Effets visuels**. Trois choix sont possibles : aucun effet, des effets dits normaux et des extras. La sélection du deuxième et du troisième choix entraîne immédiatement le bureau 3D à moins que la carte graphique ne le supporte pas (affichage d'un message d'erreur, cas en fait des puces - *chipsets* - graphiques intégrés sur la carte mère).

b. Effets spéciaux

L'utilitaire de configuration n'est pas installé par défaut, aussi il faut le faire manuellement si l'on veut gérer les effets supplémentaires :

```
aptitude install compizconfig-settings-manager
```

L'application se lance par les menus **Système - Préférences - Advanced Desktop Effects Settings** :



Les effets parlent d'eux-mêmes ainsi la sélection de Desktop Cube et de Rotate Cube fait apparaître par certaines touches le fameux "effet Cube" (il faut pour cela quatre espaces de travail. Pour en ajouter : clic droit sur le tableau de bord/espaces de travail, **Préférences**, 4 colonnes) :



Les effets s'obtiennent par une combinaison de touches. Le paramétrage et les descriptifs des effets font appel à des boutons dont la traduction est la suivante :

Super key	Touche du clavier avec le logo Windows (!)
Button1	Bouton gauche de la souris
Button2	Bouton du milieu (ou molette) de la souris
Button3	Bouton droit de la souris

Button4	Molette actionnée vers le haut
Button5	Molette actionnée vers le bas

Les combinaisons les plus courantes avec en supplément les touches [Alt], [Ctrl] et [Shift] (majuscules) aboutissent aux effets décrits ci-dessous :

Action	Combinaison
Rotation du cube	[Ctrl][Alt][Flèche à gauche] ou [Flèche à droite] (clavier), [Ctrl] [Alt] clic gauche de la souris et déplacement (souris)
Cube "à plat"	[Ctrl] [Alt][Flèche en bas]
Sélecteur de fenêtres	[Ctrl][Alt][Tab] (gauche à droite), [Shift][Ctrl][Alt] [Tab] (droite à gauche)
Visualisation de tous les bureaux	[Super key] E, même chose pour revenir à l'état initial
Visualisation de toutes les fenêtres	[Alt][Shift][Flèche en haut]
Réglage de l'opacité	[Alt][Button4] plus d'opacité, [Alt][Button5] moins d'opacité

À cela, s'ajoute des combinaisons fonctionnelles si l'effet correspondant est activé :

Effet de feu	[Shift][Super key][Button1] : une flamme ! [Shift] [Super key] c annulation
Effet de pluie	[Shift][F9] : il pleut !, [Ctrl][Super key] : une goutte... avec en plus la souris [Button1] : que d'eau !
Blur Windows	Mettre any dans Alpha blur windows
Flou cinétique	[Ctrl][F12]

Rigoureusement inutiles, ces effets apportent néanmoins un peu d'ambiance qui fait maintenant dire que Linux n'est plus le système barbare et peu moderne. Parallèlement, d'autres effets ou fonctionnalités sont plus intéressants, comme l'effet de zoom sur une fenêtre pour les déficients visuels.

Vous trouverez d'autres renseignements directement sur le site de Compiz :

<http://www.compiz-fusion.org>

2. Lanceur d'applications

a. GNOME-do

La constante recherche de productivité sur poste de travail informatique aboutit à des applications facilitant le travail de l'utilisateur. **GNOME-do** en est une (son équivalent sous KDE s'appelle **Katapult**). Issue du monde MacOS, cette fonctionnalité associe actions entrées au clavier à applications.

Voici l'adresse du site Internet de GNOME-do : <http://do-davebsd.com>

- Installez tout d'abord GNOME-do et ses dépendances :

```
aptitude install gnome-do
```

- Lancez le programme en choisissant les menus **Applications - Accessoires - GNOME-do**.

Au lancement, deux carrés aux angles arrondis apparaissent à l'écran et disparaissent dès la prochaine manipulation. Il faut alors utiliser la combinaison de touches [Super key][Espace] pour les afficher à nouveau. Ensuite ce que vous tapez au clavier détermine le type de travail que vous désirez.

Exemple, vous tapez la lettre **a** et vous obtenez :



GNOME-do détecte et associe votre demande à ce qu'il connaît, soit le lancement de l'aide en ligne. Si vous tapez ensuite un **r** :



Cette fois, l'action suppose une recherche parmi les artistes des bandes musicales sauvegardées. Enfin si l'on tape le mot **arabesque**, la recherche sur Internet apparaît en deuxième choix (accessible par la touche de tabulation) :



La validation lancera le navigateur Firefox sur un moteur de recherche search.creativecommons avec le mot arabesque.

Tout ceci appelle plusieurs remarques :

- GNOME-do se spécialise de fait dans les objets musicaux, vidéos.
- Pour une présence continue, GNOME-do se met dans les programmes au démarrage.
- La démarche d'utilisation particulière comporte ses détracteurs comme ses "aficionados".

En conclusion, ce type d'outil s'essaye et se garde en fonction des besoins...



Il existe un outil similaire, via une applet de tableau de bord, qui s'intitule Deskbar : la barre d'action "tout en un". Plus simple, elle remplace avantageusement (à mon sens) GNOME-do.

b. AWN

Avec l'activation du bureau Compiz et comme toujours d'inspiration MacOS, voici le lanceur d'applications **Avant-Window-Navigator** (AWN). Il se présente sous la forme d'une barre (paramétrable) en bas du bureau avec un déroulement d'icônes, agrandies lors du passage de la souris.

Le passage obligé avec l'installation du programme :

```
aptitude install avant-window-navigator
```

Il est quasiment obligatoire de mettre l'application au démarrage de la session. La mise en place du lanceur impose une refonte importante du bureau :

- Le tableau de bord du bas doit être supprimé ou masqué automatiquement (clic droit, ligne **Propriétés**).
- Les espaces de travail doivent être remis sur le tableau de bord supérieur sous peine de ne plus être accessibles.

Suite de la mise en place :

- Lancez le gestionnaire AWN par **Système - Préférences - Awn manager**.
- Les nouveaux lanceurs se mettent dans le menu **Launchers** et le bouton **Ajouter**.

Astuce : pour savoir ce qu'il faut renseigner dans la fenêtre **Créer un lanceur**, positionnez-vous dans le menu **Applications** et dans un sous-menu sur un logiciel ; ajoutez le lanceur au tableau de bord. Il ne reste qu'à en voir les propriétés (par un clic droit de la souris sur l'icône) pour savoir quoi recopier dans AWN.



D'autres lanceurs d'application existent comme Cairo Dock maintenant dans les dépôts depuis la version Ubuntu 8.10 Intrepid Ibex, Simdock, et autres... Le plus abouti demeure toujours AWN.

3. Gadgets de bureau

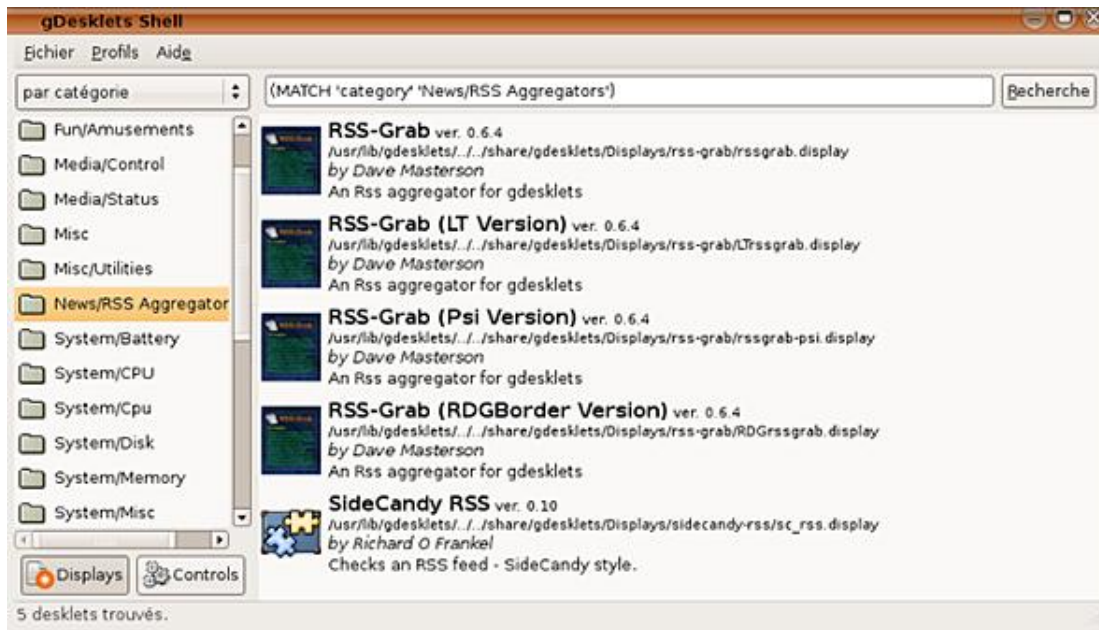
Pour finir ce tour d'horizon de la personnalisation du bureau GNOME, Ubuntu supporte les **widgets**, c'est-à-dire de petites applications affichant des informations et que l'on classe grossièrement en deux catégories :

- celles apportant des informations tirées du système : horloge, calendrier, contrôles comme l'occupation du disque, les fréquences du processeur, etc.
- celles apportant des informations de l'extérieur : météo, flux RSS (syndication de contenu) comme l'état des embouteillages avec le site Sytadin, jeux, sorties de films, etc.

Rigoureusement inutiles ou rigoureusement essentiels selon les opinions, les widgets se programment en langage Python (pour **gDesklets**) ou en JavaScript (plus côté WEB). Sur Ubuntu, on préfère gDesklets à aDesklets, tous deux dans le dépôt universe :

aptitude install gdesklets

Le lancement de gDesklets se réalise par les menus **Applications - Accessoires - gDesklets**. Il faut distinguer deux étapes : le lancement du programme et le choix/positionnement des widgets choisis dans la liste :



- Choisissez un widget et double cliquez dessus : le widget se pose sur le bureau.
- Placez-le à l'endroit désiré, un clic de souris le fige.

Chaque widget possède un menu de personnalisation par un clic droit de la souris (par exemple le choix de la ville dans un widget météo). Voici, par exemple, un bureau avec deux widgets, Calendar et Clock :



Remarques :

- Les widgets peuvent se superposer comme dans l'exemple ci-dessus.
- Chaque widget utilise des ressources de la machine : trop peut nuire.

- Le lancement de gDesklets doit se faire au démarrage de la session.
- On peut installer des widgets supplémentaires ou créer les siens.

La dernière remarque apporte la limite à cette fonctionnalité : certains widgets fonctionnent mal. D'autre part cela pose un problème de sécurité : dans la pratique, l'utilisateur du système autorise un programme avec des échanges avec l'extérieur avec pour seul contrôle la bonne foi du programmeur.

Gestionnaire de périphériques UDEV

1. Découverte des périphériques

a. Enregistrement d'un périphérique

Le répertoire `/dev` contient, sous la forme d'un fichier spécial, tout périphérique système que l'on appelle nœud (*node* en anglais). Concrètement, cela signifie que le contenu peut y être lu suivant la catégorie du périphérique. Le mode bloc, où les données sont inscrites en groupes continus sur un support persistant ; et le mode caractère, où les données sont lues octet par octet en fonction d'un flux.

Note : toutes les commandes sont à faire en mode console et avec les droits d'administration.

Démonstration pour le mode bloc

- Tapez la commande `less -f /dev/sda`

Le périphérique `sda` représente votre disque (changez par `hda` si vous disposez d'un disque IDE). Le contenu affiché par la commande `less` ou l'option `-f` force l'ouverture d'un fichier non-texte, représente tout simplement le contenu de votre disque. Les caractères en ASCII sont d'ailleurs lisibles.

- Quittez par la lettre `q`.

Démonstration pour le mode caractère

La souris est un périphérique usuel pour le mode caractère. Dans une console texte, il faut installer le paquet `gpm` pour disposer de la souris (avec les présentations semi-graphiques et la bibliothèque `curse`).

- Tapez la commande `aptitude install gpm`

Une fois installé, en bougeant la souris, le pavé se déplace à l'écran.

- Tapez la commande `cat /dev/mouse`

En bougeant cette fois la souris, des caractères s'affichent en temps réel, correspondant aux caractères liés au protocole de la souris.

- Quittez par `[Ctrl] c`.

b. Découverte dynamique

L'affichage par la commande `ls` du répertoire `/dev` retourne une longue liste de périphériques définis par le système ; certains étant utilisés, d'autres pas. La gestion du répertoire `/dev`, celle des droits et des permissions, de l'identification des fichiers de périphériques, autrefois du ressort de **devfs** (*DEVice File System*) est maintenant dévolu à **udev** (*Userspace implementation od DEVfs*). Udev apporte :

- l'emploi de règles au niveau de l'utilisateur à la différence de `devfs` fonctionnant, lui, au niveau du noyau.
- une gestion dynamique des périphériques réellement présents avec la prise en compte de la connexion "à chaud" (*hotplug*).
- une association avec `sysfs`, le système de fichiers du noyau à partir de la version 2.6.

2. Fonctionnement d'UDEV

a. Fichiers de base

Udev crée et enlève les nœuds dans /dev, à partir des événements envoyés par le noyau en cas de découverte de périphériques. La commande `df` montre bien udev comme système de fichiers pour /dev. La liste des périphériques toujours attendus et gérés par udev se trouve dans /lib/udev/devices :

```
root@ubuntu:~# ls -l /lib/udev/devices/
total 12
crw----- 1 root root    5, 1 2008-05-16 08:31 console
lrwxrwxrwx 1 root root    11 2008-05-16 08:31 core -> /proc/kcore
lrwxrwxrwx 1 root root    13 2008-05-16 08:31 fd -> /proc/self/fd
crw-r----- 1 root kmem    1, 2 2008-05-16 08:31 kmem
brw----- 1 root root    7, 0 2008-05-16 08:31 loop0
lrwxrwxrwx 1 root root    13 2008-05-16 08:31 MAKEDEV -> /sbin/MAKEDEV
drwxr-xr-x 2 root root  4096 2008-05-16 08:31 net
crw----- 1 root root    1, 3 2008-05-16 08:31 null
crw----- 1 root root 108, 0 2008-05-16 08:31 ppp
drwxr-xr-x 2 root root  4096 2008-04-11 14:21 pts
drwxr-xr-x 2 root root  4096 2008-04-11 14:21 shm
lrwxrwxrwx 1 root root    24 2008-05-16 08:31 sndstat -> /proc/asound/oss/sndstat
lrwxrwxrwx 1 root root    15 2008-05-16 08:31 stderr -> /proc/self/fd/2
lrwxrwxrwx 1 root root    15 2008-05-16 08:31 stdin -> /proc/self/fd/0
lrwxrwxrwx 1 root root    15 2008-05-16 08:31 stdout -> /proc/self/fd/1
root@ubuntu:~#
```

Les noms persistants donnés par udev sont situés dans /dev/disk :

```
root@ubuntu:~# ls -l /dev/disk
total 0
drwxr-xr-x 2 root root 120 2008-05-16 10:16 by-id
drwxr-xr-x 2 root root 140 2008-05-16 10:16 by-path
drwxr-xr-x 2 root root  80 2008-05-16 10:16 by-uuid
root@ubuntu:~# ls -lR /dev/disk
/dev/disk:
total 0
drwxr-xr-x 2 root root 120 2008-05-16 10:16 by-id
drwxr-xr-x 2 root root 140 2008-05-16 10:16 by-path
drwxr-xr-x 2 root root  80 2008-05-16 10:16 by-uuid

/dev/disk/by-id:
total 0
lrwxrwxrwx 1 root root    9 2008-05-16 10:16 edd-int13_dev80 -> ../../sda
lrwxrwxrwx 1 root root   10 2008-05-16 10:16 edd-int13_dev80-part1 -> ../../sda1
lrwxrwxrwx 1 root root   10 2008-05-16 10:16 edd-int13_dev80-part2 -> ../../sda2
lrwxrwxrwx 1 root root   10 2008-05-16 10:16 edd-int13_dev80-part5 -> ../../sda5

/dev/disk/by-path:
total 0
lrwxrwxrwx 1 root root   10 2008-05-16 10:16 pci-0000:00:07.1-scsi-1:0:0:0 -> ../../scd0
lrwxrwxrwx 1 root root    9 2008-05-16 10:16 pci-0000:00:10.0-scsi-0:0:0:0 -> ../../sda
lrwxrwxrwx 1 root root   10 2008-05-16 10:16 pci-0000:00:10.0-scsi-0:0:0:0-part1 -> ../../sda1
lrwxrwxrwx 1 root root   10 2008-05-16 10:16 pci-0000:00:10.0-scsi-0:0:0:0-part2 -> ../../sda2
lrwxrwxrwx 1 root root   10 2008-05-16 10:16 pci-0000:00:10.0-scsi-0:0:0:0-part5 -> ../../sda5

/dev/disk/by-uuid:
total 0
lrwxrwxrwx 1 root root   10 2008-05-16 10:16 49b50a9d-3569-4f46-97e3-6775106ceb54 -> ../../sda5
lrwxrwxrwx 1 root root   10 2008-05-16 10:16 98186f7c-8f1e-4225-aabc-05eedc89b1f8 -> ../../sda1
root@ubuntu:~#
```

On voit bien par exemple les UUID de chaque partition du disque dur dans le sous-répertoire /dev/disk/by-uuid. Sur Ubuntu, toutes les règles d'udev (extension `rules`) sont quant à elles situées dans /etc/udev/rules.d :

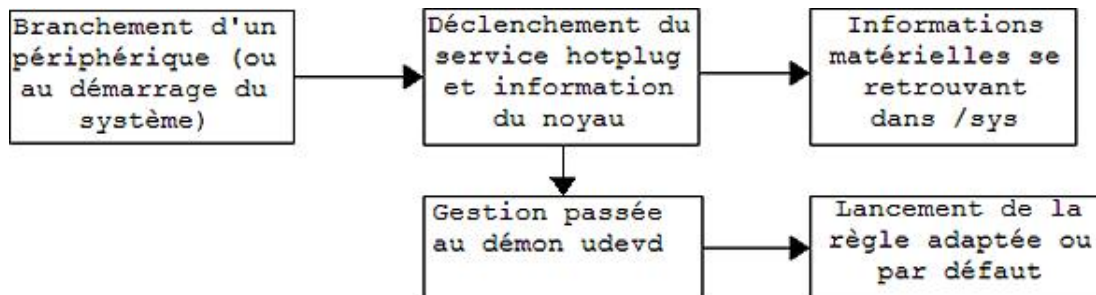
```

root@ubuntu:~# ls -l /etc/udev/rules.d/
total 96
-rw-r--r-- 1 root root 400 2008-04-11 14:21 05-options.rules
-rw-r--r-- 1 root root 191 2008-04-11 14:21 05-udev-early.rules
-rw-r--r-- 1 root root 3215 2008-04-11 14:21 20-names.rules
-rw-r--r-- 1 root root 119 2008-04-11 14:21 30-cdrom_id.rules
-rw-r--r-- 1 root root 814 2008-04-11 14:21 40-basic-permissions.rules
-rw-r--r-- 1 root root 3109 2008-04-11 14:21 40-permissions.rules
-rw-r--r-- 1 root root 30 2008-02-26 19:25 45-fuse.rules
-rw-r--r-- 1 root root 1431 2008-04-11 14:21 60-persistent-input.rules
-rw-r--r-- 1 root root 3468 2008-04-11 14:21 60-persistent-storage.rules
-rw-r--r-- 1 root root 1222 2008-04-11 14:21 60-persistent-storage-tape.rules
-rw-r--r-- 1 root root 649 2008-04-11 14:21 60-symlinks.rules
-rw-r--r-- 1 root root 411 2008-04-11 14:21 61-persistent-storage-edd.rules
-rw-r--r-- 1 root root 465 2008-05-16 08:44 70-persistent-cd.rules
-rw-r--r-- 1 root root 375 2008-05-16 08:31 70-persistent-net.rules
-rw-r--r-- 1 root root 390 2008-04-11 14:21 75-cd-aliases-generator.rules
-rw-r--r-- 1 root root 2251 2008-04-11 14:21 75-persistent-net-generator.rules
-rw-r--r-- 1 root root 563 2008-04-11 14:21 80-programs.rules
-rw-r--r-- 1 root root 84 2008-03-28 23:26 85-hdparm.rules
-rw-r--r-- 1 root root 126 2008-04-15 05:36 85-hwclock.rules
-rw-r--r-- 1 root root 708 2007-09-20 02:25 85-ifupdown.rules
-rw-r--r-- 1 root root 950 2007-10-23 19:03 85-pcmcia.rules
-rw-r--r-- 1 root root 3017 2008-04-11 14:21 90-modprobe.rules
-rw-r--r-- 1 root root 233 2008-04-11 14:21 95-udev-late.rules
-rw-r--r-- 1 root root 1224 2008-04-11 14:21 README
root@ubuntu:~# _

```

b. Principe d'une règle

Le fonctionnement d'udev déterminant une règle s'établit dans le schéma suivant :



Les règles s'appliquent normalement dans l'ordre de numérotation des fichiers. Une règle comporte une série de clés sous la forme de paires clés/valeurs et s'applique si et seulement si toutes les assertions données par les valeurs sont exactes. Exemples de clés :

- **KERNEL** : nom donné au périphérique par le noyau.
- **SUBSYSTEM** : nom donné au sous-système du périphérique.
- **DRIVER** : pilote concerné par le périphérique.

Les renseignements sont donnés par la commande `udevinfo` dont voici un extrait d'une sortie sur un disque SCSI :

```
root@ubuntu:/etc/udev/rules.d# udevinfo -a -p /sys/class/scsi_device/1:0:0:0/
```

Udevinfo starts with the device specified by the devpath and then walks up the chain of parent devices. It prints for every device found, all possible attributes in the udev rules key format. A rule to match, can be composed by the attributes of the device and the attributes from one single parent device.

```
looking at device '/class/scsi_device/1:0:0:0':
```

```
  KERNEL=="1:0:0:0"
  SUBSYSTEM=="scsi_device"
  DRIVER==""
```

```
looking at parent device '/devices/pci0000:00/0000:00:07.1/host1/target1:0:0:1:0:0:0':
```

```
  KERNELS=="1:0:0:0"
  SUBSYSTEMS=="scsi"
  DRIVERS=="sr"
  ATTRS{device_blocked}=="0"
  ATTRS{type}=="5"
  ATTRS{scsi_level}=="6"
  ATTRS{vendor}=="NECUMWar"
  ATTRS{model}=="VMware IDE CDR10"
  ATTRS{rev}=="1.00"
  ATTRS{state}=="running"
```

Grâce à ces règles, on peut gérer les permissions de chaque périphérique, exécuter des programmes en fonction d'évènements, etc. L'exemple typique d'administration des périphériques USB concerne l'attribution d'un nom persistant et ce, en fonction du fichier spécial dans /dev. Une clé USB peut se voir ainsi attribuer un nom associé au périphérique /dev/sdc quel que soit le nombre de périphériques USB branché.

Pour plus de renseignements sur les commandes d'udev, reportez-vous au manuel en ligne et à l'adresse : <http://www.kernel.org/pub/linux/utils/kernel/hotplug/udev.html>

c. Problème en cas de changement de carte réseau

Le mieux est parfois l'ennemi du bien et un problème se pose pour la carte réseau. La règle d'attribution d'udev pour une interface réseau indique naturellement l'utilisation de son adresse MAC. Or dans certains cas, lors du changement de carte réseau ou dans le cadre de la virtualisation de serveur, cette attribution de nom deviendra obsolète. Une nouvelle carte ou un changement verra le nom basé sur l'adresse MAC attribué à eth1 et non eth0.

Les services, comme par exemple un serveur DHCP, basés sur eth0 ne fonctionneront plus.

Les fichiers des règles Ubuntu concernés sont :

- 75-persistent-net.generator.rules : règle établissant le nom et lançant le programme /lib/udev/write_net_rules.
- 70-persistent-net.rules : généré par la règle ci-dessus.

Solution n°1

Détruire la (ou les) ligne(s) de la règle du fichier 70-persistent-net.rules et redémarrer le système. Ce fichier reconstruit contiendra la bonne association.

Solution n°2

Encore plus radical : détruire les deux fichiers de règles. Ceci est à éviter pour respecter les règles de noms des périphériques dans le cadre d'une gestion par udev.

Ajout de périphériques au système

1. Impression et imprimantes

L'impression de documents incombe sous Ubuntu au système d'impression CUPS (*Common Unix Printing System*) et plus exactement au service (daemon) cupsys. Installé pour démarrer par défaut sur une version en poste de travail (cela concerne a priori moins un serveur), ce service a bien évolué pour rendre très facile maintenant l'installation d'une imprimante. Statistiquement la première situation demandée en entreprise au niveau d'un poste de travail, l'impression fut longtemps le casse-tête des administrateurs.

Trois situations se présentent :

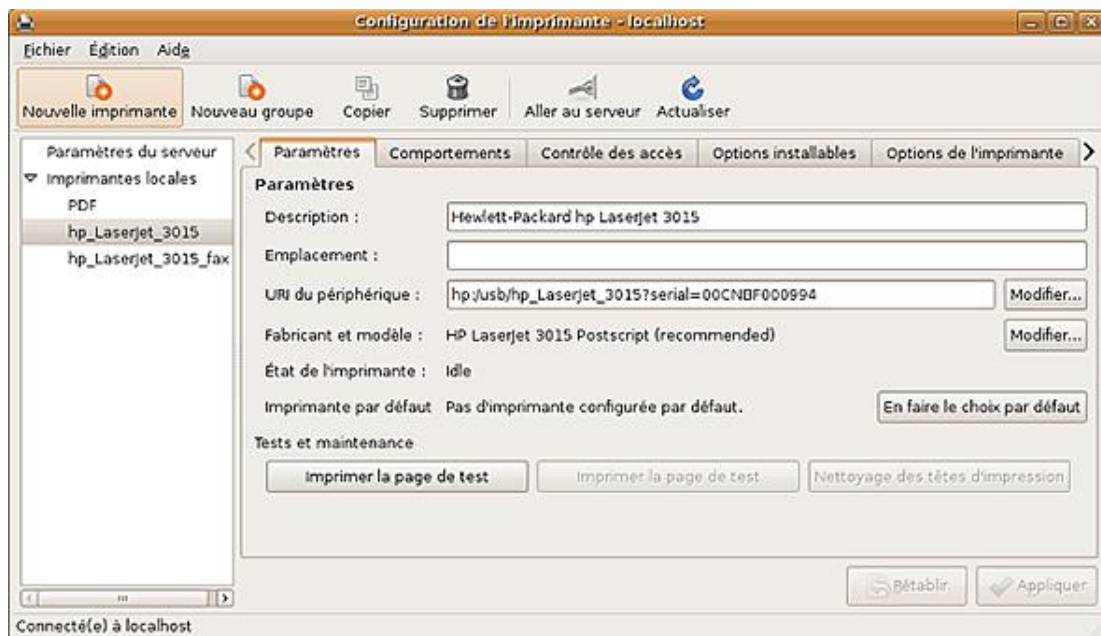
- Connexion par l'intermédiaire d'un port USB (le plus courant actuellement),
- Connexion par l'intermédiaire d'un câble parallèle,
- Connexion à travers le réseau.

Quoi qu'il en soit, la connexion d'une imprimante à un système Linux dépend avant tout de son pilote et de la bonne volonté du fabricant pour le système Linux. Ubuntu propose pour les matériels Hewlett Packard par exemple, un ensemble de paquets logiciels supplémentaires, certains installés par défaut (hplip).

a. Connecter une imprimante

Connexion par l'intermédiaire d'un port USB

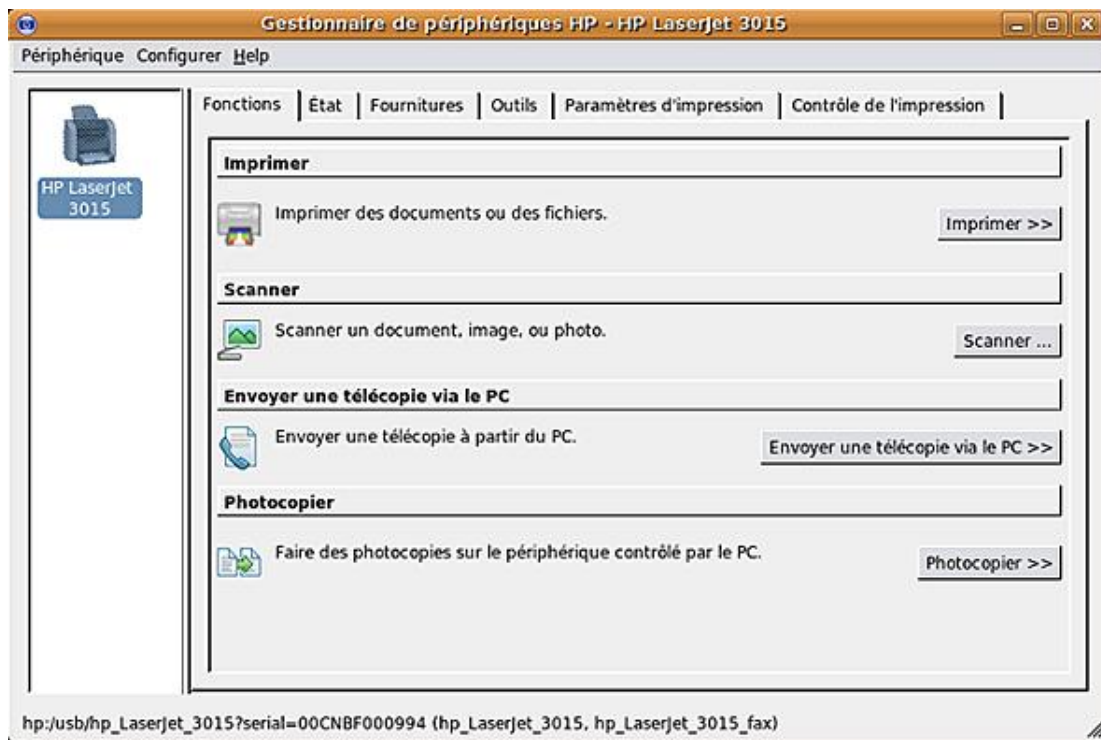
C'est le cas pratique des imprimantes modernes aujourd'hui. Le branchement de l'imprimante implique une détection automatique du système Ubuntu et l'affichage d'un message vous indiquant le modèle d'imprimante détectée. Il n'y a donc rien à faire, si ce n'est la sélectionner par défaut à partir des menus **Système - Administration - Impression**. En voici un exemple pour une imprimante multifonctions HP LaserJet 3015 :



Si vous disposez d'un matériel Hewlett Packard (pour plus de renseignements allez sur le site <http://hplip.sourceforge.net/install/index.html>), installez en plus le logiciel de gestion :

```
aptitude install hplip-gui
```

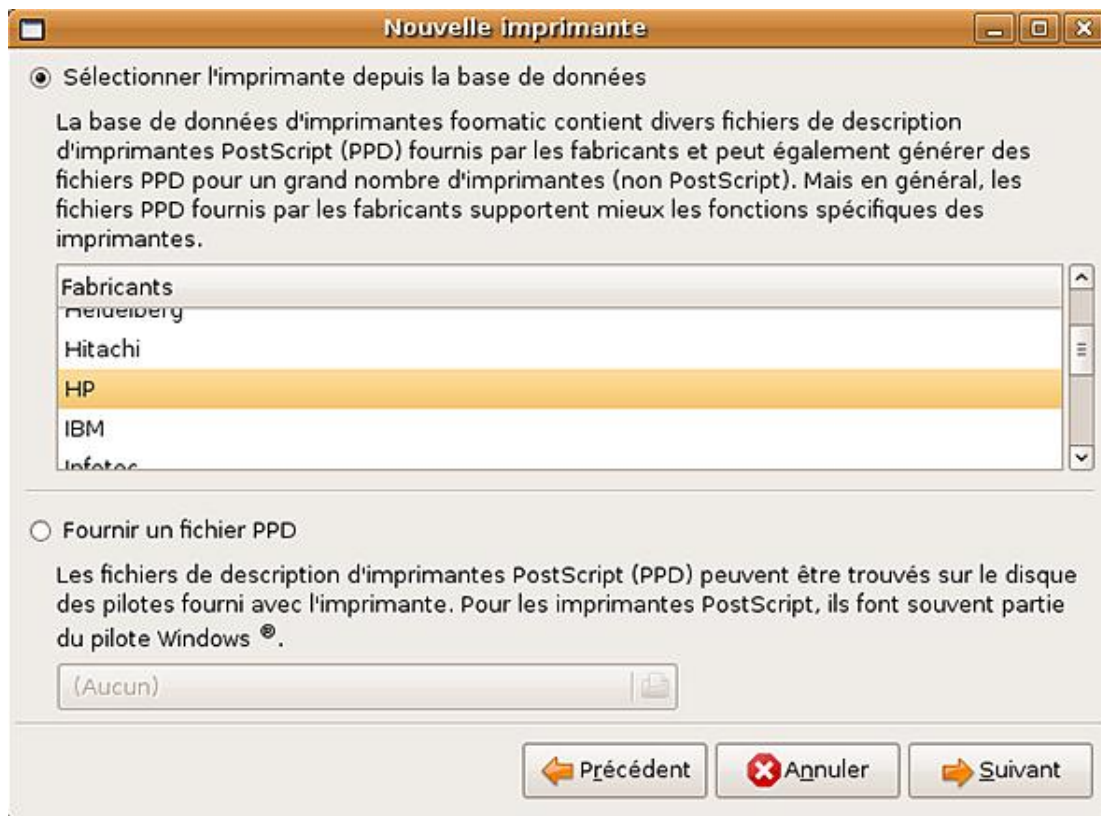
Il se lance par les menus **Système - Préférences - HPLIP Toolbox** et vous offre une gestion plus complète de votre matériel comme c'est le cas dans l'exemple avec la détection de cette imprimante multifonctions imprimante / scanner / fax / photocopieuse :



Connexion par l'intermédiaire d'un port parallèle

Le branchement de l'imprimante dans ce type de configuration oblige l'installation du pilote approprié. Installez l'imprimante par les menus **Système - Administration - Impression**, bouton **Nouvelle imprimante**, ligne **LPD/LPR Host or Printer** (LPD/LPR Line Printer Request, le demandeur et Line Printer Daemon, le serveur).

Indiquez localhost au niveau de l'hôte et cliquez sur le bouton **Suivant**. Il ne vous reste plus qu'à trouver le modèle de votre imprimante :



Connexion d'une imprimante réseau

Plusieurs cas de figure se distinguent lorsque vous ajoutez une nouvelle imprimante, toujours par les menus **Système - Administration - Impression** :

- AppSocket/HP Jet Direct, pour les imprimantes utilisant une API de type socket sur protocole TCP/UDP et le port 9100.
- *Internet Printing Protocole (IPP)*, pour l'utilisation du protocole basé sur HTTP.
- Windows Printer via SAMBA, impression via le protocole SMB sur des imprimantes installées dans un réseau Windows.

On met l'adresse IP de l'imprimante dans le premier et le deuxième cas alors qu'une recherche lance l'explorateur SMB sur le réseau. L'adresse de l'imprimante se décompose dans de cas comme suit :

smb://nom_domaine/nom_serveur:port/nom_imprimante

Note : le port est optionnel, par défaut normalement le port 139.

b. Devenir un serveur d'impression

Pour offrir le partage de l'imprimante, il suffit de cocher la case **Partager les imprimantes publiées connectées à ce système** dans les **Paramètres du serveur** à partir du menu d'administration. Sur un client Windows, la recherche de l'imprimante sur le réseau détectera automatiquement le matériel.



Assurez-vous que vos droits utilisateurs vous permettent de gérer les imprimantes par les menus **Système - Administration - Utilisateurs et groupes**, onglet **Privilèges utilisateur**.

2. Branchement d'un scanner

L'utilisation d'un scanner est trivial car maintenant ce matériel se présente avec une connexion sur port USB, que la distribution détecte sans problème. Ubuntu s'appuie sur la bibliothèque logicielle SANE (*Scanner Access Now Easy*) et le logiciel **Xsane**, installés par défaut sur la distribution poste de travail.

Pour un lancement automatique de Xsane, un simple réglage est à faire dans les menus **Système - Préférences - Périphériques et médias amovibles**, onglet **Imprimante et scanner**, en cochant la case **Lancer automatiquement un programme lors de la connexion d'un scanner**.

Sinon, le lancement de l'application Xsane montre la détection automatique du matériel présent, ici un scanner de marque Hewlett-Packard Scanjet 3800 :



3. Ajout d'un disque supplémentaire

Même si cette procédure se rencontre le plus souvent dans les cas de virtualisation de serveurs, la méthodologie reste la même dans le cas d'un disque dur physique classique. Deux raisons principales se dégagent de l'ajout d'un nouveau disque :

- Augmenter la capacité de stockage du système.
- Construire un système RAID.

En premier lieu, il faut insérer le disque dans la machine physiquement ou virtuellement. Après reconnaissance dans le BIOS, on démarre le système. Classiquement, un deuxième disque s'appelle sdb (forme SATA ou SCSI) ou hdb (pour un IDE).

Première étape : création de la partition

Cette étape utilise l'utilitaire de base **Fdisk**, chargé sous Ubuntu de manipuler la table de partition d'un disque.

```
fdisk /dev/sdb
```

Fdisk suffit à l'administrateur pour effectuer les principales tâches sur la table de partitions. Une fois lancée, l'invite de commande n'attend qu'une seule lettre (une lettre = une action) dont les principales sont :

- a pour indiquer une partition amorçable
- d pour détruire une partition
- l pour afficher les types possibles d'une partition

- `m` pour afficher l'aide
- `n` pour créer une partition
- `p` pour afficher la tables des partitions
- `q` pour quitter fdisk
- `t` pour changer le type d'une partition
- `v` pour vérifier la table des partitions
- `w` pour écrire la table des partitions et sortir

Des sous-actions découlent parfois d'une action principale. Fdisk ne peut agrandir une partition existante comme le fait **Gparted** (version GNOME de Parted).

- Pour créer une partition primaire de la taille du disque, vous tapez les séquences :
 - `n` pour nouvelle partition,
 - `p` pour une partition primaire,
 - `1` pour la première partition parmi les quatre possibles.
- Validez à vide ou `1` pour First cylinder car on se positionne au début du disque.
- Validez à vide ou la valeur par défaut car la partition occupe l'ensemble du disque.

Dans de rares cas, le renseignement se donne à partir des cylindres ; mais trop compliqué à calculer ! Heureusement Fdisk propose de noter la taille en octets, kilo-octets ou megaoctets (exemple pour 1 Go : +1024M).

Un appel de la structure par la lettre commande `P` montre la partition en `sdb1` :

- `p` pour l'affichage de la structure des partitions.

```
Command (m for help): p
```

```
Disk /dev/sdb: 2147 MB, 2147483648 bytes
255 heads, 63 sectors/track, 261 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Disk identifier: 0xab75f785
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sdb1		1	261	2096451	83	Linux

```
Command (m for help):
```

Linux (code 82) s'applique par défaut de la partition. À ce stade, aucun changement n'est encore appliqué, pour cela on utilise la commande `w` :

- Tapez `w` pour écrire et rendre définitive la structure de la table des partitions.

Deuxième étape : création du système de fichiers

Votre partition existe, mais ne contient pas de système de fichiers :

```
mkfs.ext3 /dev/sdb1
```

La commande construit entre autres la table des inodes et le journal associé. Un message vous indique que le système sera vérifié tous les 21 montages (comprendre à l'allumage de la machine) ou tous les 180 jours. Vous avez la possibilité de modifier ces réglages par la commande `tune2fs`.

Troisième étape : montage du périphérique

Dans une phase de test, le montage du nouveau système se fait manuellement en créant d'abord le point de montage :

```
mkdir /travail
```

```
mount /dev/sdb1 /travail
```

La vérification de tout ceci se fait avec un classique `df -h` :

```
root@serveur:~# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        6,6G  571M   5,7G   9% /
varrun          252M   40K  252M   1% /var/run
varlock         252M    0  252M   0% /var/lock
udev            252M   52K  252M   1% /dev
devshm          252M    0  252M   0% /dev/shm
/dev/sda2       950M   18M  885M   2% /home
/dev/sdb1       4,0G   73M   3,7G   2% /travail
root@serveur:~# _
```

Pour que ce montage perdure lors d'un redémarrage du système, la modification du fichier `/etc/fstab` s'impose en ajoutant la ligne suivante :

<code>/dev/sdb1 /travail</code>	<code>ext3</code>	<code>relatime</code>	<code>0</code>	<code>2</code>
---------------------------------	-------------------	-----------------------	----------------	----------------

À l'ancienne mode, un label se définissait par la commande `e2label`. Maintenant, on indique plutôt l'**UUID** qui se récupère avec la commande :

```
vol_id -u /dev/sdb1 > travail.uuid
```

J'ai créé une redirection dans un fichier de manière à le récupérer plus facilement... Ouvrez à nouveau le fichier `/etc/fstab` avec VIM, remplacez `/dev/sdb1` par `UUID=` et tapez les touche [Echap] + : + r travail.uuid afin de lire le numéro. Il ne reste plus qu'à compléter la ligne.

Ajout de ressources au système

1. Connexion à distance

L'administrateur ne dispose pas du don d'ubiquité, aussi certaines tâches doivent se réaliser à distance. Il convient de distinguer deux cas de figures : la prise de contrôle à distance d'un poste de travail dans un but de maintenance et l'ouverture de session à distance dans un but d'administration de serveur.

a. Prise de contrôle à distance avec Vinagre

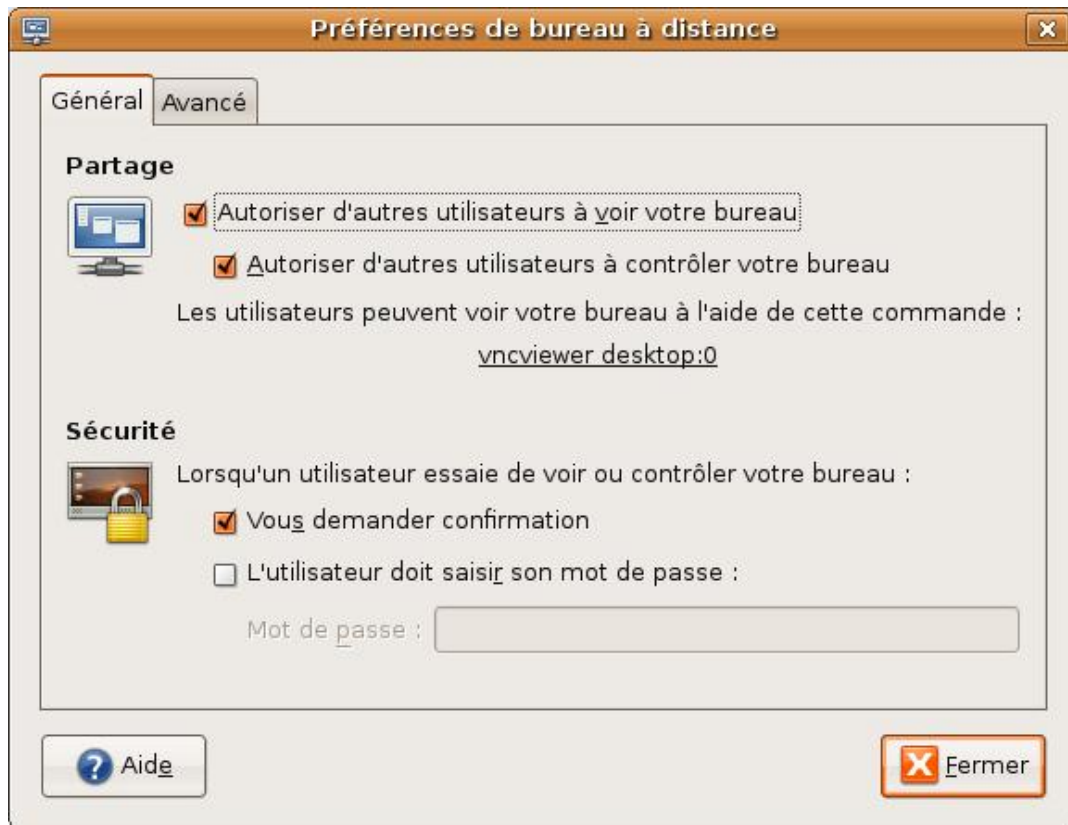
Cas typique de l'assistance utilisateur, Ubuntu offre cette possibilité avec l'outil **Vinagre** (de la famille des clients VNC) dont le site Internet est à l'adresse suivante :

<http://www.gnome.org/projects/vinagre/>

Cette manipulation nécessite deux postes avec GNOME installé sur les deux comme bureaux. Vinagre s'appuie sur le protocole TCP avec le port 5900. En premier lieu, le **client** doit autoriser la connexion du bureau à distance :

- Autorisez la prise de contrôle en cochant la case **Autoriser d'autres utilisateurs à voir votre bureau** dans les menus **Système - Préférences - Bureau à distance**.

Le réglage des paramètres de sécurité : chiffrement, mot de passe, etc. se trouve dans l'onglet **Avancé**.



Sur le serveur, la prise de contrôle débute le lancement de l'outil **Vinagre** à partir des menus **Applications - Internet - Visionneur de bureaux distants**. La demande par le bouton **Se connecter** ouvre une fenêtre demandant le nom de l'hôte (ou adresse IP de la machine distante, plus approprié dans le cas d'une prise de contrôle par Internet via une adresse IP publique) et le port 5900.

b. Ouverture d'une session à distance avec SSH

SSH ouvre un tunnel chiffré pour vos échanges de données. Il sécurise la relation par l'encryptage des données et autorise l'administrateur à effectuer diverses manipulations à distance. Ubuntu supporte OpenSSH, mise en application libre et en OpenSource des protocoles SSH (*Secure Shell*). SSH remplace les outils *rlogin*, *rsh* et *rcp* nettement moins sécurisés.

Le protocole SSH existe en deux versions SSH1 et SSH2. SSH1 utilise une paire de clés de type RSA1 pour l'authentification, tandis que SSH2 utilise DSA ou RSA (différent de RSA1). Les authentifications traitées ici seront par mot de passe et par clé asymétrique.

Ubuntu installe par défaut sur le client le paquetage openssh-client tandis qu'il faut installer sur le serveur la partie serveur :

```
aptitude install openssh-server
```

L'installation entraîne la création des clés RSA et DSA dans le répertoire de configuration /etc/ssh.

Attention : il existe une ambiguïté dans les termes, en fait le serveur représente la machine sur laquelle on se connecte et le client celle à partir de laquelle on va se connecter.

Exemple de connexion d'un client sur un serveur :

```
max@desktop:~$ ssh donald@192.168.0.2
The authenticity of host '192.168.0.2 (192.168.0.2)' can't be established.
RSA key fingerprint is f8:80:1b:cc:df:bc:47:68:12:a4:2b:ba:23:7c:c8:ad.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.2' (RSA) to the list of known hosts.
donald@192.168.0.2's password:
Added user donald.

Linux muaddib 2.6.24-19-generic #1 SMP Wed Aug 20 22:56:21 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
donald@muaddib:~$ █
```

L'exemple montre une première connexion d'une machine cliente SSH nommée desktop par l'utilisateur max sur une machine serveur SSH nommée muaddib sur le compte de l'utilisateur donald. La syntaxe de la commande SSH est la suivante :

```
ssh (nom_utilisateur@)nom_hôte
```

Le nom de l'utilisateur peut être omis : dans ce cas, le protocole établit une connexion en root. Le nom d'hôte est indifféremment un nom de machine ou une adresse IP (en cas de non-résolution DNS). Lors de la première demande, le système enregistre la clé d'authentification dans un fichier d'hôtes connus (répertoire caché .ssh dans celui de l'utilisateur sur la machine client, fichier know_hosts).



Référez-vous à la documentation SSH pour plus de renseignements avec notamment la connexion par clés.

Utilitaires SSH

Ils sont au nombre de deux :

- la commande scp pour transférer un fichier ou un répertoire.
- la commande sftp de même facture, pour ouvrir une session FTP interactive sécurisée.

Syntaxe de la commande scp correspondant au transfert d'un fichier distant vers un système est la suivante :

```
scp fichier_local login@IP_distante:/chemin/fichier_distant
```

Et son contraire :

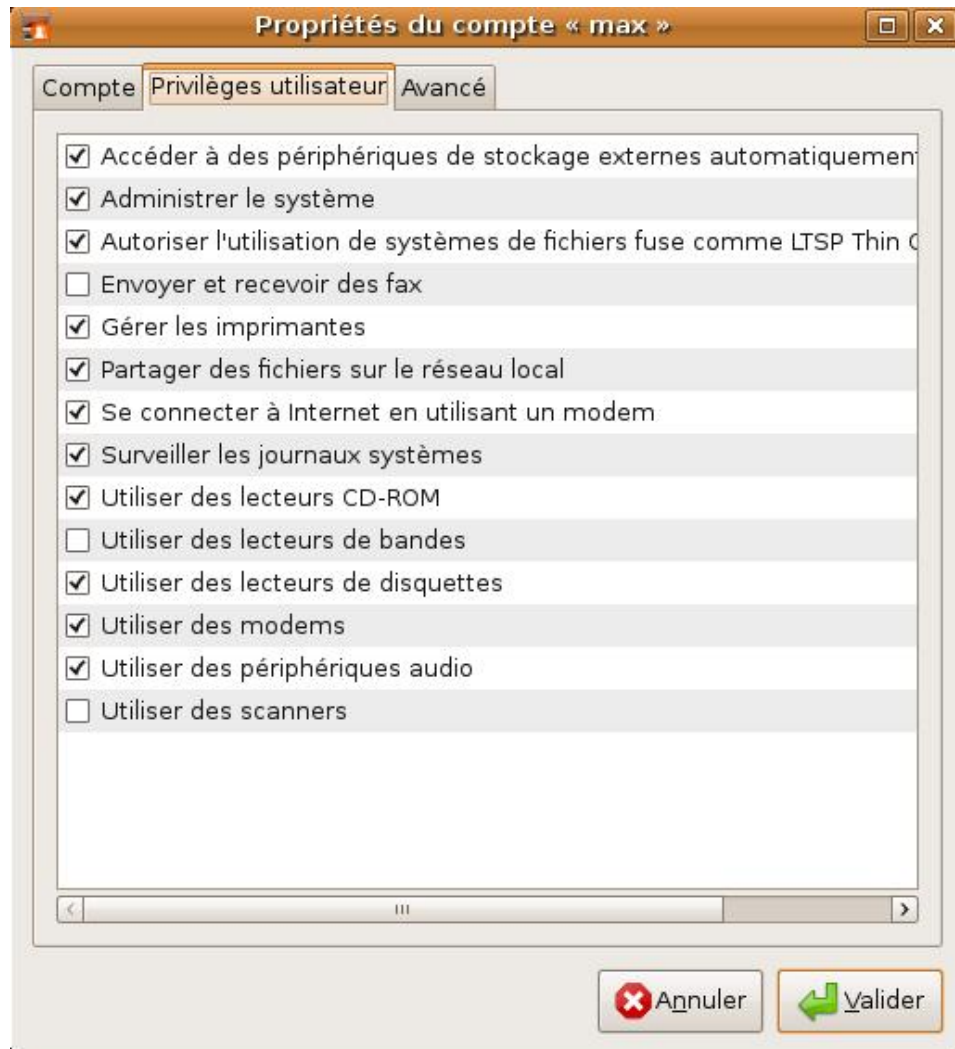
```
scp utilisateur@IP_distante:/chemin/fichier_distant fichier_local
```

La copie d'un répertoire nécessite l'option -r (pour une copie récursive).

c. Partage de fichiers sur le réseau

Un utilisateur dispose de la faculté de partager un espace de son répertoire sur le réseau. Il existe déjà d'ailleurs un répertoire nommé **Public** dans le dossier personnel.

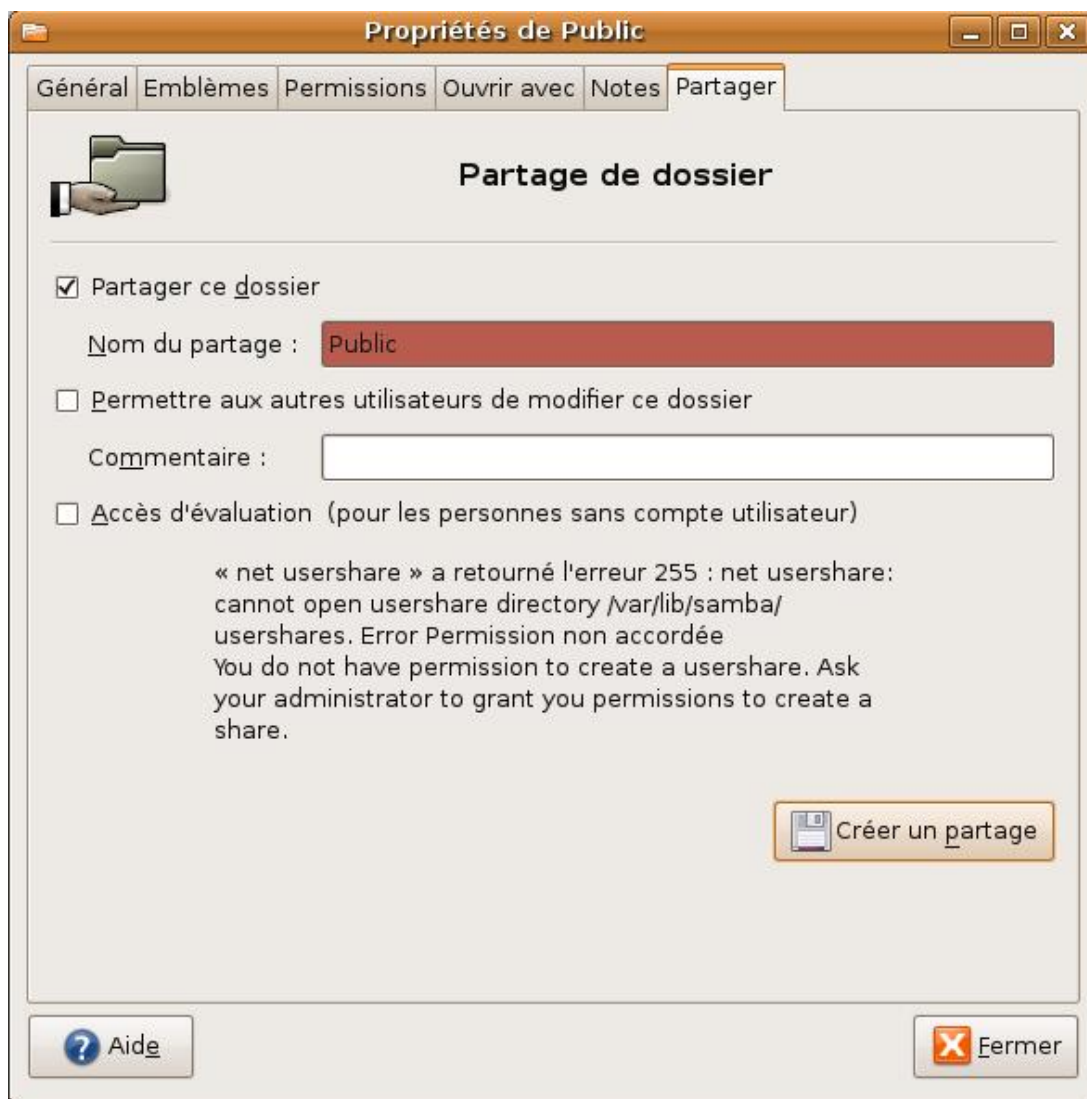
Le droit d'exercer le partage se vérifie dans l'application users-admin à partir des menus **Système - Administration - Utilisateurs et groupes**. La modification des propriétés nécessite le déverrouillage de l'application par le mot de passe. Tout se vérifie ensuite avec l'onglet **Privilèges utilisateur** et la case (qui doit être cochée) **Partager des fichiers sur le réseau local** :



La manipulation suivante s'effectue par un clic droit de la souris sur l'icône du répertoire **Public** dans la fenêtre du dossier personnel et le choix de la ligne **Option de partage**.

- Cochez la case **Partager ce dossier**.

La première fois, le système installe le service de partage (logiciel SAMBA) nécessaire à un partage de fichiers par le protocole smb sur le réseau. Un problème cependant : la création du partage ne se fait pas pour un problème de permission :



Ceci est normal car le droit de partage s'attribue par l'appartenance au groupe **sambashare**. Il faut vous déconnecter et rouvrir une session afin que votre profil soit actualisé avec l'enregistrement de l'appartenance à ce groupe.

- Fermez votre session et connectez-vous à nouveau.
- Effectuez cette fois le partage du répertoire **Public**.

Sur un poste Windows, le répertoire est visible dans les **Favoris réseau** et sur un poste Linux Ubuntu au niveau des serveurs réseaux. Pour se situer dans le même groupe de travail que les ordinateurs Windows, éditez le fichier `/etc/samba/smb.conf` et changez la ligne `workgroup = WORKGROUP` par `workgroup = votre_nom_de_réseau`.

Relancez ensuite le service samba par `/etc/init.d/samba restart`.

2. Méthodes supplémentaires d'ajout de programmes

Il a été vu dans le chapitre Prise en main de la distribution le principe de la gestion centralisée des sources de logiciels au travers l'outil principal **Aptitude** et le fichier de configuration `/etc/apt/sources.list`. La mise en pratique de cette gestion montre en réalité deux possibilités supplémentaires d'installation de logiciels, en dehors de la voie royale apportée par **Aptitude**. Enfin le cas très particulier d'utilisation de logiciels issus du monde Windows complètera ce thème.

Rappel de la démarche d'installation d'un logiciel (en mode console) sur Ubuntu :

Vérification de la présence du logiciel (exemple : le serveur WEB Apache) :

```
aptitude search apache2
```

Ou `apt-get search apache2` lorsque l'on n'est pas sûr du nom du logiciel.

Éventuellement vérification des informations du logiciel :

```
aptitude show apache2
```

Installation proprement dite :

```
aptitude install apache2
```

Rappel de la démarche de désinstallation d'un logiciel :

Pour désinstaller en laissant les fichiers de configuration :

```
aptitude remove apache2
```

Pour une désinstallation complète :

```
aptitude purge apache2
```

a. Par les sources

L'installation par les sources nécessitent une compilation des différents fichiers par divers outils (compilateur GCC pour des sources en C par exemple). Cette méthode s'emploie lorsque l'administrateur désire un paquetage plus récent (pilote de périphériques ou autre) qui n'existe pas encore dans les dépôts ou trop propriétaire pour y être.

Ubuntu dispose d'un paquetage descriptif sous forme de liste, contenant l'ensemble des logiciels nécessaires à la compilation des sources d'un programme :

```
aptitude install build-essential
```

Les sources contiennent parfois un script d'installation écrit en BASH ou en PERL.

Exemple n°1 :

Logiciel serveur WEB NanoWeb écrit en PHP avec script d'installation.

À côté d'Apache LE serveur web incontournable (il existe d'autres serveurs dont NanoWeb), écrit en PHP apporte robustesse et petite taille. Il se trouve dans les dépôts Ubuntu mais (à la rédaction de ces lignes) en version 2.2.8. Or, il existe sur le site (<http://nanoweb.si.kz>) en version 2.2.9 que vous devez télécharger :

```
wget  
http://nanoweb.si.kz/downloads/dist/nanoweb_2.2.9.tgz
```

Les sources se trouvent toujours au format d'archives compressées `tar.gz` ou `tgz`, (voire `lzma` ou `bz2`) qu'il faut remettre état :

```
tar -zxvf nanoweb_2.2.9.tgz
```

Avec pour la commande `tar`, utilitaire d'archivage :

- L'option `z` pour décompresser l'archive
- L'option `x` pour extraire
- L'option `v` pour afficher plus d'informations
- L'option `f` pour indiquer le nom de l'archive qui suit.

Il ne reste plus qu'à se positionner dans le répertoire d'installation et lancer le script existant (il faut au préalable avoir installé les paquetages `php5` et `php5-cli`) :

```
cd nanoweb_2.2.9
```

```
./install-sh
```


Intéressant : le script d'installation vous indique les différents répertoires d'installation et autres renseignements utiles lors d'une désinstallation. En effet, on ne peut utiliser la commande `aptitude remove` pour des sources.

Exemple n°2 :

Outil logiciel Netcat "couteau suisse" de l'administrateur pour lire et écrire des connexions réseau.

Ce logiciel se trouve dans les dépôts, mais on désire effectuer une compilation afin de l'installer dans un endroit bien précis à l'abri des regards. La séquence de compilation d'un logiciel passe traditionnellement par quatre étapes :

- L'étape de **configuration** : commande `configure` (création du fichier Makefile avec dépendances et options définies).
- L'étape de **compilation** : commande `make`.
- L'étape de **vérification** : commande `make check`.
- L'étape d'**installation** : commande `make install`.

Les sources se récupèrent sur le site de **Netcat** : <http://netcat.sourceforge.net/>

Ce qui donne pour le traitement :

```
tar -zxvf netcat-0.7.1.tar.gz
```

```
cd netcat-0.7.1
```

```
./configure --prefix=/root/netcat/
```

```
make
```

```
make check
```

```
make install
```

Le logiciel se trouve ainsi installé dans l'espace de l'administrateur, avec l'exécutable dans le répertoire **/root/netcat/bin**.



La notion de compilation est juste effleurée et nécessite à elle seule un ouvrage - il en existe d'ailleurs - pour en comprendre toutes les arcanes.

b. Installation d'un logiciel au format binaire

Dans de rares cas, généralement liés à une politique restrictive des droits concernant la licence du logiciel, le programme se trouve en téléchargement sur le site de l'éditeur sous la forme d'un exécutable à l'extension `.bin` (pour binaire bien sûr) et non dans un dépôt Ubuntu.

Le langage JAVA de Sun Microsystems fut un exemple célèbre, car proposé très longtemps sous forme binaire. Il est maintenant intégré dans les dépôts Ubuntu sous deux formes :

- la version en OpenSource du langage Java portée par le projet IcedTea (<http://openjdk.java.net>).
- la version sous forme de paquets de Sun Microsystems (avec acceptation de la licence).

Exemple d'installation :

Le lecteur multimédia (déclinaison basique, version 11 française) de la société RealNetworks (<http://france.real.com/player/select/>) est fourni pour les distributions Linux sous la forme d'un binaire pour processeur i686 :

RealPlayer11GOLD.bin 7,15 Mo

Une fois téléchargé ce fichier, les droits afférents sont à 644 (soit en lecture et écriture uniquement pour le propriétaire). Il faut véritablement le transformer en binaire en lui donnant les droits d'exécution et en le lançant :


```
chmod 755 RealPlayer11GOLD.bin
```

```
./RealPlayer11GOLD.bin
```

Le processus consiste à valider des options d'installation par défaut. Il est évidemment préférable d'effectuer l'installation sous l'identité de l'administrateur ou avec la commande `sudo` car, dans ce cas, un lanceur est rajouté au menu **Application - Son et vidéo - RealPlayer 11**. Le lecteur sera opérationnel pour tous les utilisateurs du système et installé dans le répertoire :

```
/opt/real/RealPlayer
```

Dans le cas contraire, l'installateur détecte la restriction des droits et propose une installation dans le répertoire de l'utilisateur, sans rajout au menu.

Certains binaires conditionnent plus clairement l'acceptation à une licence pendant le processus d'installation.

c. Autres possibilités d'installations

Il n'existe pas de contradiction majeure pour installer un paquet logiciel a priori destiné à une autre distribution :

- Au format `deb` pour la distribution **Debian** (méthode d'installation sensiblement équivalente).
- Au format `rpm`, issu de la distribution façon **Red Hat** (conversion avec l'application **Alien**).

Pour ne citer que les plus courantes. Comme il avait déjà été indiqué au début de l'ouvrage, ces méthodes sont à proscrire pour des problèmes de stabilité. Il est rare de ne pas trouver le logiciel dans les sources nombreuses des dépôts Ubuntu ou en compilation à partir de l'éditeur. Si vraiment la chose est impossible pour un logiciel très spécifique : changez de distribution !

3. Logiciels Windows avec Wine sous Ubuntu

Le logiciel **Wine** (<http://www.winehq.org/>) part d'une idée généreuse (certains parleront de fantasme) visant à faire cohabiter le système Windows avec Linux. Brisons tout de suite le rêve : il est illusoire de penser faire fonctionner tout les logiciels Windows avec Wine, son nom l'indique bien : *Wine Is Not an Emulator* (acronyme récursif typique !). Depuis ses débuts chaotiques, le projet Wine progresse de jour en jour au rythme de ses sorties mensuelles très fréquentes.

Autre remarque : le logo basé sur un verre de vin ne tire sa justification que par son homonymie avec le mot traduit en anglais.

a. Principe et installation

Wine se différencie de **WineLib** dont l'optique consiste à compiler les logiciels Windows sous Linux. **Wine** réimplante l'API de Windows en traduisant les appels aux fonctions systèmes en appels reconnaissables par Linux. C'est pour cela qu'un gros travail de programmation se fait et que des nouvelles applications (et API) ne peuvent être prises en compte immédiatement par **Wine**. Une liste de logiciels compatibles se consulte sur le site :

```
http://appdb.winehq.org/appbrowse.php?catId=0
```

Du point de vue de sa justification, disons qu'il est plus simple d'utiliser **Wine** pour un ou deux logiciels Windows n'ayant pas d'équivalent Linux (ou alors vous y êtes trop habitué...) que de monter une solution virtuelle plus lourde en ressources et en temps d'accès.

La mise en place de **Wine** s'effectue de deux façons : soit par le dépôt **universe**, soit par l'ajout d'un dépôt supplémentaire afin de disposer de la dernière version stable. Comme le projet est très actif (il y a une différence de version importante), il vaut mieux choisir la deuxième solution et intégrer le dépôt dans le fichier `/etc/apt/sources.list` :

```
deb http://wine.budgetdedicated.com/apt hardy main
```

Ensuite, vous devez télécharger la clé publique de vérification du dépôt et l'installer :

```
wget -q http://wine.budgetdedicated.com/apt/387EE263.gpg
```

```
apt-key add 387EE263.gpg
```

L'installation classique du packaging se fait après une mise à jour des sources :

```
aptitude update
```

```
aptitude install wine
```

Un nouveau menu général s'installe et préfigure un environnement "à la Windows" avec la structure de type **Program Files** et un disque C situés dans un répertoire caché de chaque utilisateur. Le menu **Applications - Wine - Browse C:\Drive** permet d'y aller directement. Une application (célèbre) existe déjà :



b. Configuration et installation d'un programme

La configuration spécifique de **Wine** se trouve dans le menu **Applications - Wine - Configure Wine** (programme **winecfg**) avec par exemple le choix de la version de Windows ou, plus intéressant un surclassement de bibliothèques de type DLL, nécessaire pour certains programmes. Pour fonctionner, un logiciel utilisera soit une version distribuée par **Wine**, soit une version native apportée par le programme lui-même.

Un exemple de ce type de sur-classement se montre avec l'installation de Microsoft Visio, utilitaire de création de diagrammes. Comme alternative OpenSource il existe **Dia**, mais on peut lui préférer (surtout si l'on possède déjà la licence) le logiciel de Microsoft, plus visuel et plus complet.

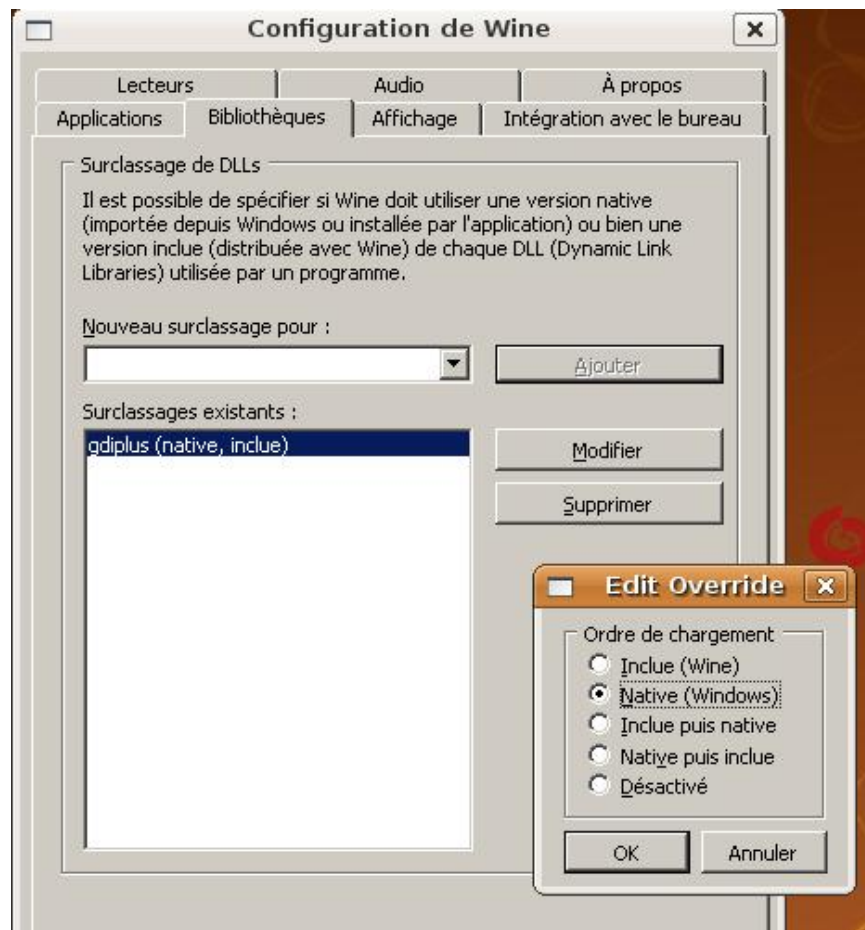
Installation de Microsoft Visio

Une fois inséré, l'installation démarre par le lancement sur le CD-Rom du programme **setup.exe** classique, maintenant utilisable par le programme **Wine**. L'installation ne présente pas de difficultés et demande bien sûr le numéro de licence avant de pouvoir continuer. Le programme s'installe dans un nouveau menu **Wine - Programmes - Microsoft Office - Microsoft Office Visio 2003** (on prend ici la version XP du logiciel).

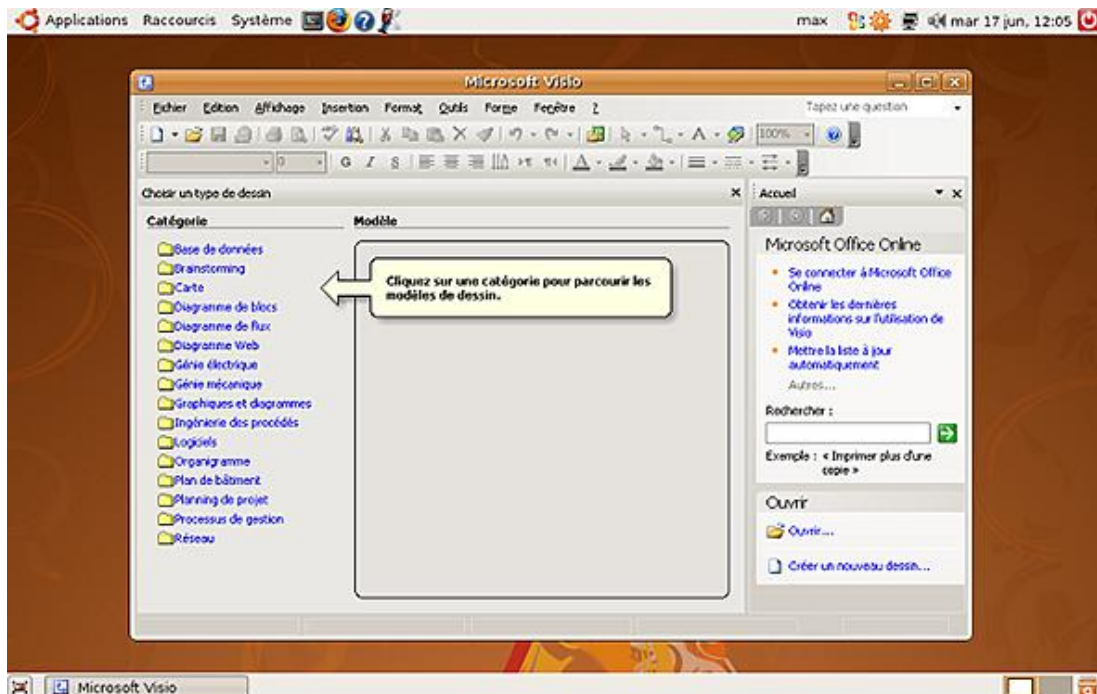
Le lancement immédiat de **Visio** aboutit à une erreur (caché derrière l'écran de démarrage) indiquant *IOPL not enabled*. Pour résoudre ce problème de bibliothèque :

- Lancez l'utilitaire de configuration **Wine** par le menu **Wine - Configure Wine**.
- Cliquez sur l'onglet **Bibliothèques**.
- Dans **Nouveau surclassement pour**, choisissez la DLL **gdiplus** et ajoutez-la.
- Cliquez sur le bouton **Modifier** pour indiquer un choix sur **Native (Windows)**.
- Validez et lancez à nouveau le programme.

L'écran de configuration :



Le lancement de Visio :



L'erreur est maintenant corrigée.

Administration des utilisateurs

Il a été vu dans le chapitre Gestion des droits utilisateurs tout ce qui concernait les droits des utilisateurs. L'approche de ce paragraphe concerne plus spécialement le travail d'administration des comptes utilisateurs. L'administration des comptes utilisateurs, outre le fait qu'elle occupe dans une bonne part du temps de l'administrateur, consiste à s'occuper des tâches de création, de suppression, de modification et de consultation. Il faut évidemment être connecté en `root`...

1. Principes, commandes et tâches

La gestion des utilisateurs sous Linux/Ubuntu a pour principe l'indépendance, c'est-à-dire protéger l'utilisateur contre les accès indésirables des autres et lui octroyer un cadre de travail cohérent.

a. Principales commandes

Voici sous forme de liste récapitulative les principales commandes concernant la gestion des utilisateurs :

- **gestion des comptes utilisateurs :**
 - `adduser` : ajouter un utilisateur (préféré à `useradd` en ligne de commande).
 - `usermod` : modifier un utilisateur.
 - `deluser` : supprimer un utilisateur (préféré à `userdel` en ligne de commande).
- **gestion des groupes :**
 - `addgroup` : ajouter un groupe (préféré à `groupadd` en ligne de commande).
 - `groupmod` : modifier la définition d'un groupe.
 - `delgroup` : supprimer un groupe (préféré à `groupdel` en ligne de commande).
 - `groups` : afficher le groupe d'appartenance de l'utilisateur.
- **administration des utilisateurs :**
 - `passwd` : changer le mot de passe de l'utilisateur.
 - `chfn` : modifier les informations de l'utilisateur (champ numéro 5 du fichier `/etc/passwd`).
 - `chsh` : changer le shell (interpréteur de commandes) de l'utilisateur.
 - `id` : affiche l'identifiant de l'utilisateur (`whoami` affiche le nom de connexion).
 - `last` : afficher la liste des connexions utilisateurs.
 - `su` : passer sous l'identité de l'administrateur (`root`).
 - `sudo` : obtenir des droits étendus.
 - `who` : montrer qui est connecté.

Rappel : il existe deux types d'utilisateurs sous Linux, les utilisateurs systèmes (virtuels) ou propriétaires de processus et les utilisateurs humains dont le `root` (l'administrateur) en est un type particulier.



Les commandes préférées le sont car elles suivent la charte Debian alors que les autres correspondent à la norme POSIX (*Portable Operating System for Computer Environment*), standard UNIX. Par contre, l'administrateur utilise les commandes POSIX plutôt dans les scripts SHELL d'automatisation de création/modification d'utilisateurs.

b. Exemples d'utilisation

Création d'un nouvel utilisateur

Être utilisateur signifie être connu du poste local, de pouvoir s'y connecter, d'avoir un accès complet sur son répertoire personnel et de disposer de certains droits (réseaux ou autres). Syntaxe de la commande :

```
adduser login_utilisateur
```

Avec pour effet :

- la création du répertoire personnel /home/login_utilisateur,
- tout ce qui concerne la gestion et l'authentification des utilisateurs est inscrit dans un seul fichier /etc/passwd,
- la gestion des groupes est assurée par /etc/group,
- les mots de passe cryptés sont placés dans /etc/shadow, par sécurité lisible seulement par le root.

Pour les options, vous vous référerez au manuel en ligne.

Rappel : la maîtrise de la commande `adduser` (commande POSIX) est indispensable pour écrire des scripts de génération automatique de comptes.

Exemple :

```
useradd toto -u 1200 -p moi -g 1000 -s /bin/bash
```

Cette commande crée en une seule fois l'utilisateur `toto` avec le numéro d'identifiant 1200, le mot de passe `moi`, le numéro de groupe 1000 et le shell `/bin/bash`.

Rappel : la gestion des mots de passe cryptés par l'installation (courante maintenant) de la `shadow`-suite fait que le fichier `/etc/shadow` ne contient plus que le mot de passe crypté et pour des raisons de sécurité ne peut être ouvert en lecture que par son propriétaire le root.

Ajout/modification d'un mot de passe

Par défaut, la simple commande `useradd` crée un compte sans mot de passe (à la différence de `adduser`). Pour le créer ou le modifier, on aura :

```
passwd login_utilisateur
```

Suivi de deux demandes (l'autre pour la vérification). Il est possible d'avoir des messages si votre mot de passe est trop court, trop simple ("azerty") ou basé sur uniquement des lettres...

À noter :

- l'option `-d` pour supprimer le mot de passe
- l'option `-l` pour le verrouiller
- l'option `-u` pour le déverrouiller

Supprimer un utilisateur

Supprimer le compte d'un utilisateur comporte l'obligation que celui-ci ne soit pas connecté :

```
userdel [-r] login_utilisateur
```

L'option `-r` supprime aussi le répertoire personnel (non effacé par défaut), les fichiers de l'utilisateur et toute trace de l'utilisateur dans les fichiers de configuration.

Modifier un utilisateur

La commande de modification d'un compte utilisateur s'applique en fonction des options désirées.

Exemples :

```
usermod -G nom_groupe login_utilisateur
usermod -L login_utilisateur
usermod -e MM/JJ/AA login_utilisateur
```

La première ligne ajoute `login_utilisateur` dans le groupe (existant bien sûr !). La deuxième bloque le compte de l'utilisateur (voir le résultat dans le fichier `/etc/passwd`). La dernière change la date d'expiration du compte. Voir le manuel pour les autres options.

Gestion des groupes

Un groupe comporte un ensemble d'utilisateurs partageant les mêmes fichiers et répertoires et ce, avec des droits d'accès. Chaque utilisateur fait partie d'au moins un groupe, dit groupe primaire. Sur Ubuntu, celui-ci est automatiquement identique au `login` de l'utilisateur par défaut, par souci de sécurité. Un utilisateur peut faire partie de plusieurs autres groupes, appelés groupes secondaires.

Explications sur les commandes principales :

- pour créer un nouveau groupe : `addgroup nom_du_groupe`
- pour lister tous les groupes d'un utilisateur : `groups nom_du_groupe`
- pour supprimer un groupe : `delgroup nom_du_groupe`
- pour ajouter un utilisateur à un groupe : `usermod nom_du_groupe` (ou `groupmod` avec l'option `-n`).

2. Gestion avancée des utilisateurs

a. Utilisateur modèle

Le répertoire `/etc/skel` (et son contenu) sert de modèle pour les utilisateurs lors d'une création. Pour examiner les valeurs par défaut appliquées par `useradd`, on a la commande :

```
useradd -D
```

L'édition du fichier `/etc/default/useradd` donne le même résultat, soit pour Ubuntu :

```
GROUP=100          # identifiant du groupe primaire
HOME=/home          # racine des répertoires personnels
INACTIVE=-1         # nombre de jours avant destruction du
                    # compte
EXPIRE=             # nombre de jours avant expiration du mot
                    # de passe (vide par défaut)
SHELL=/bin/bash     # shell de connexion attribué au compte
SKEL=/etc/skel       # fichiers recopiés par défaut dans
                    # chaque répertoire personnel
```

Le répertoire `/etc/skel` contient, on le voit, les fichiers recopiés par défaut dans chaque répertoire personnel. Il suffit pour l'administrateur d'effectuer une modification dans ce répertoire pour qu'elle se répercute à chaque création future d'utilisateur.

Le fichier `/etc/login.defs` contient toutes les informations spécifiques à l'ordinateur pendant le processus de

connexion (comme par exemple lors de la commande `/bin/login`). Se reporter au manuel en ligne et au fichier pour connaître et comprendre ses différents paramètres.

b. Utilisation des quotas de disque

Installer des quotas de disque consiste à fixer des limites de capacité de stockage pour chaque utilisateur. On **ne peut utiliser** les quotas sur une partition `root`, ou plus exactement une partition qui contient par exemple `/proc`. Le plus simple pour affecter des quotas utilisateurs, c'est d'avoir une **partition /home spécifique**.

Première étape : installation du paquetage

```
aptitude install quota
```

Deuxième étape : modification du fichier `/etc/fstab` avec `usrquota` pour la partition `/home`

```
UUID=votre_numéro /home ext3 relatime,usrquota 0 2
```

- Redémarrez le système.

Troisième étape : initialisation de la table de quotas

```
touch /home/quota.user
```

```
chmod 600 /home/quota.user
```

```
quotacheck -cu /home
```

Le fichier `quota.user` a été créé dans `/home` et contient la table des quotas.

Quatrième étape : fixation des quotas

La commande `edquota -u nom_utilisateur` sert à fixer par Nano les limites `soft` et `hard` (espace disque et nombre de fichiers pour les deux).

Exemple avec un utilisateur nouvellement créé :

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/sda2	20	8182	10240	6	512	1024

L'exemple montre pour une limite d'espace disque à 8 Mo en `soft` et 10 Mo en `hard` et un nombre de fichiers à 512 en `soft` et 1024 en `hard`. Un dépassement de la limite `soft` affiche un message d'alerte et l'utilisateur ne peut dépasser la limite `hard`.

D'autres commandes existent :

- la génération de rapports : `repquota -a`
- l'affichage d'information pour un utilisateur : `quota -u utilisateur`
- le paramètre `grace` qui fixe la période possible du dépassement de la limite `soft` : `edquota -t`

c. Accorder des droits supplémentaires avec sudo

Rappel : la commande `su nom_utilisateur` démarre un nouveau processus avec un nouveau shell avec l'identité de l'utilisateur, après bien sûr demande et validation du mot de passe approprié. Une utilisation courante consiste, en étant un utilisateur ordinaire, à passer en `root` afin d'effectuer une tâche d'administration. Dans ce cas, la commande `su` sans le nom de l'utilisateur suffit.

Une autre possibilité existe avec la commande `sudo`, on l'a vu (commande `sudo -i`). Cette commande permet à des utilisateurs indiqués dans le fichier `/etc/sudoers` de lancer des commandes de superutilisateur. Pour accorder des droits, il faut modifier le fichier `/etc/sudoers` par la commande `visudo` et bien sûr en étant en `root`.

Configuration de sudo

```
visudo
```

```
# /etc/sudoers
# This file MUST be edited with the 'visudo' command as root.
# See the man page for details on how to write a sudoers file.

Defaults    env_reset
# Host alias specification
# User alias specification
# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down
# %sudo    ALL=NOPASSWD: ALL

# Members of the admin group may gain root privileges
%admin    ALL=(ALL) ALL
```

Ce fichier contient deux types d'entrées : les **alias** ou plus simplement les variables et les spécifications des utilisateurs. En cas de multiples entrées pour un utilisateur, les règles s'appliquent dans l'ordre de lecture. La syntaxe des entrées ou règles vient de la forme EBNF (*Extended Backus-Naur Form*), nom barbare pour une lecture assez simple : en gros sous la forme de paires "champs = valeurs".

L'étude complète de cette syntaxe `sudo` ne présente pas véritablement d'intérêt. Aussi, son apprentissage se limite à l'étude de quelques exemples.

Exemples :

```
donald    ALL = (ALL) ALL
```

L'utilisateur `donald` peut lancer toutes les commandes sur toutes les machines.

```
Donald    ALL = NOPASSWD: ALL
```

L'utilisateur `donald` peut lancer toutes les commandes sur toutes les machines sans demande de mot de passe.

```
Host_Alias    RESEAU = 192.168.3.0/255.255.255.0
donald        RESEAU = (ALL) ALL
```

L'utilisateur `donald` peut lancer toutes les commandes sur toutes les machines du réseau donné par l'alias.

```
%info        ALL = (ALL) ALL
```

Tous les utilisateurs du groupe `info` peuvent lancer toutes les commandes sur toutes les machines.

```
Cmnd_Alias    REBOOT = /sbin/reboot
donald        ALL = ALL, !REBOOT
```

L'utilisateur `donald` ne peut relancer le système. Notez la syntaxe qui autorise tout d'abord toutes les commandes pour ensuite restreindre spécifiquement le `reboot`.

```
User_Alias    WEB = donald, riri, fifi, loulou
WEB           srvweb = (www-data) ALL, (root) /bin/su www-data
```

Sur la machine `srvweb`, tous les utilisateurs listés dans `WEB` peuvent lancer toutes les commandes sous l'identité `www-data` (c'est le propriétaire des pages Web sous Apache) ou simplement se transférer sous ce compte.

```
donald    ALL=NOPASSWD: /usr/bin/vim /etc/passwd
```

Donne à `donald` le droit d'éditer et de modifier le fichier `/etc/passwd` sans demande de mot de passe.

Problèmes de maintenance

L'administration d'un système Linux comporte plusieurs aléas revenant de façon récurrente. À la manière d'une FAQ (*Frequently Asked Questions*), genre popularisé sur Internet pour apporter les réponses aux utilisateurs, voici une petite liste de questions et de leurs réponses. On parle là uniquement de problèmes de maintenance.

1. "Sur quelle version Ubuntu suis-je exactement ?"

De cette question anodine va découler deux réponses. La première renvoie l'identification du noyau en cours, du type de version et de quelques informations complémentaires :

```
uname -r
```

Exemple :

```
Linux srvfrw 2.6.24-19-server #1 SMP Wed Jun 18 15:18:00 UTC 2008  
i686 GNU/Linux
```

L'option `-a` renvoie une version réduite. Cette information est utile car le système peut contenir plusieurs noyaux, présents au démarrage dans l'écran de GRUB, et l'administrateur évoluant entre l'un ou l'autre en fonction des besoins (choix différents de modules par exemple).

Pour la demande d'identification de la version, la commande s'énonce comme :

```
lsb_release -a
```

Exemple :

```
No LSB modules are available  
Distributor ID: Ubuntu  
Description:    Ubuntu 8.04.1  
Release:        8.04  
Codename:       Hardy
```

Les modules LSB font référence aux normes de la **Free Standards Group**. Ubuntu dispose simplement du paquetage `lsb-base` installé (pour la norme LSB 3.2).

2. "J'ai perdu mon mot de passe administrateur..."

L'être humain est faillible, l'administrateur système est un être humain donc un administrateur est faillible. Ce syllogisme facile montre qu'il existe des défaillances quel que soit le sérieux et la compétence de l'administrateur.

- À partir d'un CD-Rom de la distribution Ubuntu serveur et en redémarrant la machine, choisissez l'option **Réparer un système endommagé**.

Après la question classique du choix de la langue, suit une série de détections de la configuration puis une demande sur le nom de la machine (facultatif, car sans effet pour la suite). Le cheminement du mode de récupération aboutit enfin à un écran de choix du système racine.

Exemple pour un système avec trois partitions : `/boot`, `swap` et `/`

```
[!!] Entrer dans le mode de récupération

Veillez choisir un périphérique qui sera utilisé comme système de
fichiers racine. Vous pourrez ensuite choisir entre plusieurs
opérations de récupération à effectuer sur ce système de fichiers.

Périphérique à monter comme système de fichiers racine (/) :

/dev/sda1
/dev/sda2
/dev/sda3

<Revenir en arrière>
```

L'administrateur doit savoir où se situe le montage du système de fichiers racine (dans l'exemple /dev/sda3). S'en suivent les options ci-dessous :

```
[!!] Entrer dans le mode de récupération

Opérations du mode de récupération

Exécuter un shell dans /dev/sda3
Exécuter un shell dans le contexte de l'installateur
Réinstallation du programme de démarrage GRUB
Changer de système de fichiers racine
Redémarrer le système

<Revenir en arrière>
```

On s'aperçoit que la réinstallation de GRUB est possible en cas de problème de cet ordre. Pour changer un mot de passe nous avons besoin d'un shell aussi est-ce le premier choix à prendre. Après l'information sur le montage du système, un prompt (invite de commande) s'offre en `root` pour lancer la commande `passwd` afin de changer le mot de passe.

Il ne reste plus alors qu'à sortir du montage par un simple `exit`.



La relative simplicité de passer outre une règle de sécurité essentielle comme le changement de mot de passe de l'administrateur, met en exergue la nécessité absolue de protéger physiquement les accès aux serveurs...

3. "Le serveur graphique ne répond plus..."

Cas typique d'un problème graphique, il arrive que la souris ne réponde plus, ni le clavier. Xorg porte sa part avec son constant développement et sa constitution modulaire (version 7.3 sur Hardy Heron) et les pilotes propriétaires de cartes graphiques, une autre...

Quoi qu'il en soit, une simple combinaison de touches permet d'arrêter le serveur graphique et de revenir :

- soit en mode console si le serveur a été lancé par la commande `startx`
- soit sur GDM en poste de travail.

[Ctrl][Alt][FlècheRetour]

Note : la touche [Retour arrière] ou *backspace* indique la touche unique avec une flèche gauche généralement en haut à droite du clavier et non la flèche de direction.

4. "J'ai un programme qui bloque, impossible de l'arrêter..."

Il suffit de "tuer" son processus. Cette opération s'effectue en ligne de commande avec les droits administrateurs (voir le troisième paragraphe de ce chapitre) ou plus facilement avec le moniteur graphique par les menus **Système - Administration - Moniteur système**, onglet **Processus** et le bouton **Terminer le processus**.

5. "La console n'est pas/plus en français..."

Accessoirement, vous avez bien un clavier **azerty** mais pas les caractères accentués. Cela arrive parfois lorsque la configuration initiale n'a pas été correctement terminée.

Le plus simple est de faire un :

```
dpkg-reconfigure console-setup
```

Cette relance de la configuration écrit un nouveau fichier `/etc/default/console-setup` qui, pour les français ressemble à ceci :

```
VERBOSE_OUTPUT=no
ACTIVE_CONSOLES="/dev/tty[1-6]"
CHARMAP="UTF-8"
CODESET="Lat15"
FONTFACE="VGA"
FONTSIZE="16"
XKBMODEL="pc105"
XKBLayout="fr"
XKBVARIANT="oss"
XKBOPTIONS="lv3:ralt_switch"
BOOTTIME_KMAP_MD5="aaaaaaaaaaaaaaaaaaaaaaaaaaaa"
```

Note : ne tenez pas compte de la clé MD5 et n'y touchez pas. Elle intervient si l'on change le fichier `/etc/console-setup/boottime.kmap.gz` et en ne la changeant pas, `debconf` (l'utilitaire de configuration système) ne modifiera pas dans votre dos ce fichier. Une manière "brutale" pour changer de configuration clavier consiste à renommer un jeu de clavier (paquetage `console-data`, emplacement `/usr/share/keymaps`) en `boottime.kmap.gz`, mais je ne vous la conseille pas...

Une autre façon de changer sa configuration circule sur Internet : la commande `setupcon`. Cela ne sert malheureusement à rien si le fichier `/etc/default/console-setup` est faux, car la commande l'utilise...

Par l'interface graphique

Vérifiez la prise en charge complète du français par l'application **gnome-language-selector** (menus **Système - Administration - Prise en charge linguistique**). Vérifiez surtout que la case pour le français est **cochée** et non **grisée**.

Le problème des locales

Il ne faut pas confondre la configuration du clavier et celle de l'environnement du système même si les deux sont liées (la première dépend parfois de la deuxième). Une bonne pratique consiste à réutiliser la commande `dpkg-reconfigure` :

```
dpkg-reconfigure locales
```

Or, voici ce qui se passe généralement :

```

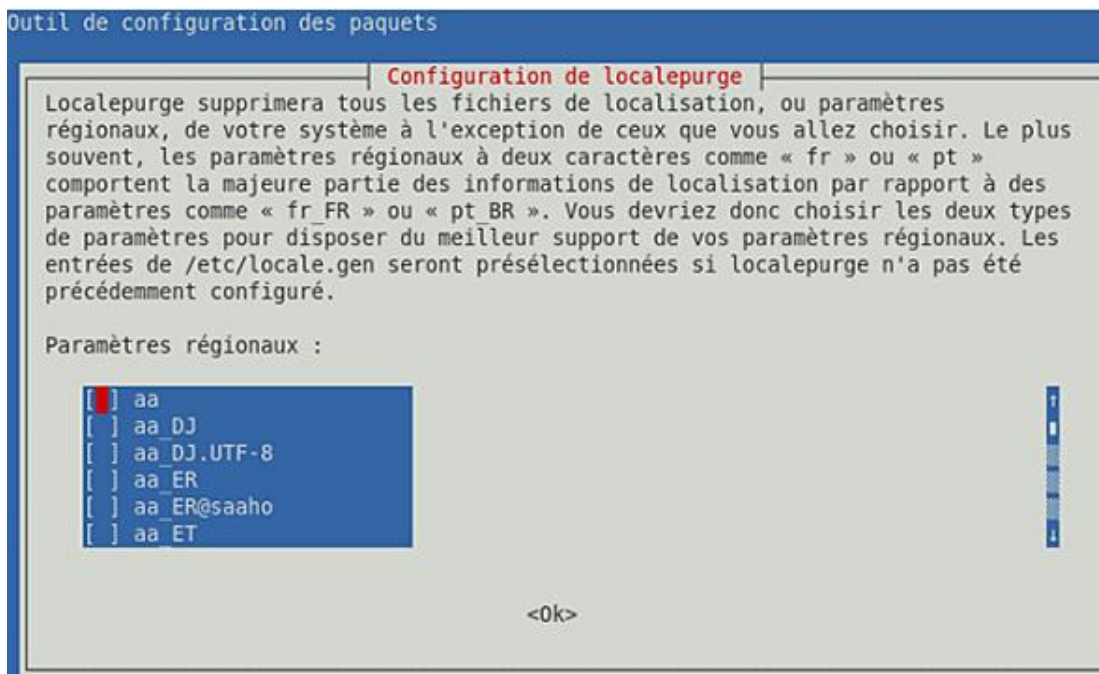
root@host:~# dpkg-reconfigure locales
Generating locales...
  en_AU.UTF-8... up-to-date
  en_BW.UTF-8... up-to-date
  en_CA.UTF-8... up-to-date
  en_DK.UTF-8... up-to-date
  en_GB.UTF-8... up-to-date
  en_HK.UTF-8... up-to-date
  en_IE.UTF-8... up-to-date
  en_IN.UTF-8... up-to-date
  en_NZ.UTF-8... up-to-date
  en_PH.UTF-8... up-to-date
  en_SG.UTF-8... up-to-date
  en_US.UTF-8... up-to-date
  en_ZA.UTF-8... up-to-date
  en_ZW.UTF-8... up-to-date
  fr_BE.UTF-8... done
  fr_CA.UTF-8... done
  fr_CH.UTF-8... done
  fr_FR.UTF-8... done
  fr_LU.UTF-8... done
Generation complete.
root@host:~# _

```

La commande, on le voit, régénère la configuration en fonction des locales présentes sur le système dans le répertoire `/usr/lib/locale`, ce qui ne fait pas forcément notre affaire si la localisation demandée est absente ou incomplètement configurée.

Supprimer les locales directement du répertoire `/usr/lib/locale/` n'est pas une bonne solution, le mieux est de passer par le paquet logiciel `localepurge` :

```
aptitude install localepurge
```



Attention ! Comme le message l'indique, l'outil `localepurge` supprimera tous les autres fichiers de localisation que ceux choisis, cela permet en plus de libérer de l'espace sur le disque. Pour une localisation française complète, vous devez choisir :

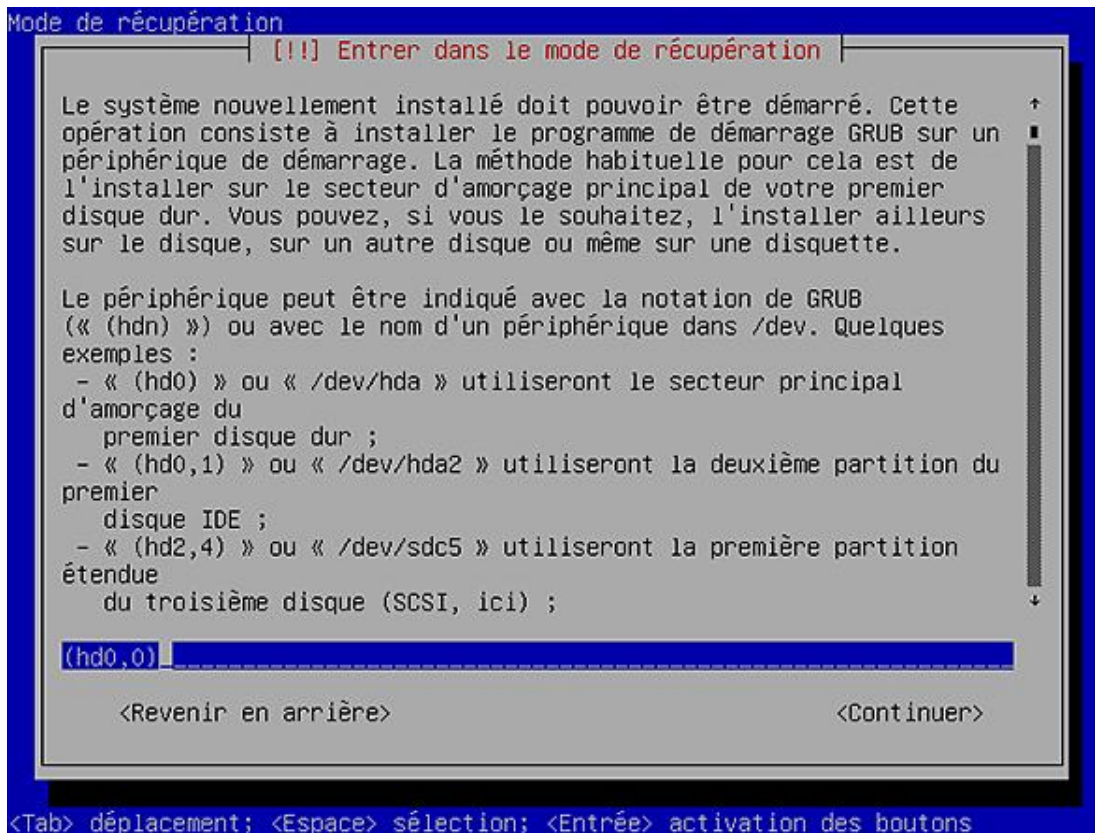
```

fr
fr_FR
fr_FR@euro
fr_FR.UTF-8

```

6. "GRUB fait une erreur au démarrage du système..."

Peu importe la raison pour laquelle GRUB ne fonctionne plus, il faut tout simplement le réinstaller. Pour cela on applique la même démarche qu'à la deuxième question (Perte du mot de passe). L'opération du mode de récupération est cette fois-ci la troisième ligne. La pratique veut que le chargeur de démarrage s'installe sur le MBR du premier disque du système et que l'on préfère la notation GRUB :



Le même résultat est obtenu en mode console avec la commande `grub-install`.

7. "À quoi sert le mode Recovery ?"

Le chargeur GRUB donne dans sa configuration une deuxième entrée par le mode `single` :

Ubuntu 8.04.1, kernel 2.6.24-19-server (recovery mode)

Ce qui correspond dans le fichier `/boot/grub/menu.lst` au mode `single` pour la ligne du noyau :

```
title      Ubuntu 8.04, kernel 2.6.24-19-virtual (recovery mode)
root       (hd0,0)
kernel     /boot/vmlinuz-2.6.24-19-virtual
root=UUID=f153c6f5-836c-47bb-98b0-24b470ca26e5 ro single
initrd     /boot/initrd.img-2.6.24-19-virtual
```

Si l'on choisit cette configuration de démarrage, trois choix de maintenance s'affichent :

- la **réparation des paquetages "cassés"**, ce qui arrive dans une tentative d'installation ou de désinstallation (en mode console la commande `aptitude -f install` tente la même chose) et la mise à jour du système.
- l'**ouverture d'une console** avec une invite de commandes en `root` après saisie du mot de passe. Le niveau d'exécution est 1, le démarrage des services est donc minimal : ce qui en permet la réparation.

- la **tentative de réparation du serveur graphique**, ce qui correspond à la commande `dpkg-reconfigure xserver-xorg` avec une nouvelle détection du matériel.

Administration des ressources

1. Planification des tâches

Ubuntu propose trois outils de programmation de tâche correspondant à trois sortes de tâches à réaliser :

- **atd** : ce service exécute un travail donné à un moment donné, et ce, une seule fois (présent sur Ubuntu server et desktop par défaut).
- **crond** : ce service exécute un travail (ou plus) à des horaires précis suivant un intervalle de temps défini (présent sur Ubuntu server et desktop par défaut).
- **anacron** : ce démon exécute un travail (ou plus) après un laps de temps déterminé (présent sur Ubuntu desktop par défaut).

L'utilitaire de base reste pour l'administrateur le service `cron`.

a. Fonctionnement de cron

Le service `cron` travaille à partir du fichier `/etc/crontab` qui contient les entrées correspondant aux répertoires respectifs et contenant les scripts à exécuter :

- pour les heures : `/etc/cron.hourly/`
- pour les jours : `/etc/cron.daily/`
- pour les semaines : `/etc/cron.weekly`
- pour les mois : `/etc/cron.monthly`

Exemple de fichier `/etc/crontab` :

```
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

Les quatre dernières lignes montrent la périodicité sous un schéma minute / heure / jour / mois / jour de la semaine, ce qui donne :

- la 17^{ème} minute de chaque heure pour `/etc/cron.hourly`
- chaque jour à 6 heures 25 pour `/etc/cron.daily`
- chaque semaine le dimanche à 6 heures 47 pour `/etc/cron.weekly`
- le premier de chaque mois à 6 heures 52 pour `/etc/monthly`



Les services concernant les fichiers journaux `logrotate` et `syslogd` (voir le troisième paragraphe) se trouvent - et s'exécutent chaque jour - dans le répertoire `/etc/cron.daily`.

b. Définir une crontable personnelle

Un utilisateur crée un fichier particulier de requête appelé `crontab` avec la commande `crontab`. Ce fichier se placera dans le répertoire `/var/spool/cron/crontabs/` avec comme nom celui de l'utilisateur.

Exemple de fichier utilisateur :

```
# Exemple de tâche personnelle
01 08 * * * rm *.*.*~
```

Ce qui aura pour effet de supprimer tous les fichiers cachés se terminant par un tilde (fichiers temporaires d'éditeur de texte) dans le répertoire de l'utilisateur par défaut tous les jours à 8 heures et 1 minute et si la machine est allumée. On peut définir une fréquence (intervalle ou "pas") et d'autres fonctionnalités, voir dans ce cas le manuel en ligne.

Syntaxe d'utilisation de la commande

```
crontab -e
# édite par nano (ou VIM) et modifie la crontab active
# elle ne doit pas l'être directement par un éditeur de textes

crontab -l
# liste la crontab active

crontab -r
# arrête la crontab active
```



L'administrateur change accessoirement les droits pour autoriser ou non la commande `crontab`. Sur Ubuntu, tous les utilisateurs ont par défaut le droit de l'exécuter.

2. Surveillance du système par les processus

a. Notion de processus

Un processus se traduit par l'exécution d'un programme à un instant donné : l'exécution du shell en est un dès que vous vous connectez. À chaque processus correspond un PID (*Process IDentifier*). De plus, un processus peut lancer un autre processus : dans ce cas on parlera de processus "père" et de processus "fils". Parce que Linux est multitâche, plusieurs processus peuvent s'exécuter en même temps.

Rappel : au démarrage du système, le BIOS lance le programme de démarrage (`bootstrap`), qui charge ensuite le noyau Linux et charge enfin le programme `init`, père de tous les autres. Ce premier processus a donc un PID à 1.

Il existe une relation entre types de commandes d'un shell et processus :

- Les **commandes internes** (comme `ls`) ne donnent pas lieu à une création de nouveau processus.
- Les **commandes externes** se trouvant dans différents répertoires font l'objet de la création d'un processus fils.
- Les **commandes définies par une fonction** (ou alias) renomment en fait une commande du shell.

b. Vérification et surveillance des processus

Plusieurs commandes constituent la trousse à outils de l'administrateur.

La commande

Syntaxe :

ps [-options]

Parmi les options les plus courantes :

- L'option `a` affiche les processus pour tous les utilisateurs.
- L'option `x` affiche les processus sans terminal de contrôle (services).
- L'option `u` affiche en regard de chaque processus le nom de l'utilisateur et son heure de lancement.

Exemple :

```
root@srvfai:~# ps -au
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root      4125  0.0  0.0   1716    512 tty4      Ss+   08:29   0:00 /sbin/getty 38400 tty4
root      4126  0.0  0.1   1716    516 tty5      Ss+   08:29   0:00 /sbin/getty 38400 tty5
root      4131  0.0  0.1   1716    516 tty3      Ss+   08:29   0:00 /sbin/getty 38400 tty3
root      4132  0.0  0.0   1716    512 tty6      Ss+   08:29   0:00 /sbin/getty 38400 tty6
root      4549  0.0  0.2   2568   1212 tty1      Ss    08:30   0:00 /bin/login --
root      4550  0.0  0.3   4164   1820 tty1      R     08:30   0:00 -bash
root      7290  0.0  0.2   2568   1212 tty2      Ss    10:42   0:00 /bin/login --
max       7298  0.0  0.5   5488   2900 tty2      S+    10:42   0:00 -bash
root      7480  0.0  0.1   2644   1012 tty1      R+    10:59   0:00 ps -au
root@srvfai:~# _
```

Plus pratique, la commande `ps` s'utilise avec un "tube" pour éviter un affichage inutile et accéder plus rapidement à l'information. Voici un exemple pour rechercher les processus en relation avec `dhcp` :

```
ps -aux | grep dhcp
```

Une autre commande dérivée affiche les processus sous forme d'arborescence, ce qui permet visuellement de voir la filiation d'un processus envers un autre :

pstree [-options]

On a coutume de l'utiliser avec les options `u` (UID) et `p` (PID) :

```
root@srvfai:~# pstree -up
init(1)
├── atd(4494,daemon)
├── cron(4507)
├── dd(4197)
├── dhclient3(4095,dhcp)
├── exim4(5850,Debian-exim)
├── getty(4125)
├── getty(4126)
├── getty(4131)
├── getty(4132)
├── in.tftpd(4442)
├── klogd(4199,klog)
├── login(4549)──bash(4550)──pstree(7538)
├── login(7290)──bash(7298,max)
├── portmap(3849,daemon)
├── rpc.idmapd(3888)
├── rpc.mountd(4436)
├── rpc.statd(3867,statd)
├── sshd(4221)
├── syslogd(4176,syslog)
├── udevd(2481)
└── vmware-guestd(4354)
root@srvfai:~# _
```

La commande

Syntaxe :

top [-options]

La commande `ps` n'offre qu'un aperçu "instantané" du système. **Top** fournit un résumé mis à jour des processus actifs et de leur utilisation en ressources. Le résultat de la commande peut être assez long (en fonction des processus ouverts) et sachez que la commande ne retourne pas au prompt (arrêt de la commande par [Ctrl] **C**). Elle actualise la page toutes les dix secondes. Comme elle utilise des ressources en temps processeur, vous ne devez l'utiliser que pour pister un processus bloqué.

Exemple :

```
top - 11:21:33 up 2:51, 2 users, load average: 0.00, 0.05, 0.03
Tasks: 58 total, 1 running, 57 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.0%us, 0.0%sy, 0.0%ni,100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 515448k total, 251408k used, 264040k free, 42576k buffers
Swap: 409616k total, 0k used, 409616k free, 174960k cached
```

PID	USER	PR	NI	VRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4305	root	20	0	0	0	0	S	0.3	0.0	0:00.17	vmmemctl
7690	root	20	0	2308	1072	856	R	0.3	0.2	0:00.02	top
1	root	20	0	1808	836	612	S	0.0	0.2	0:01.09	init
2	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	kthreadd
3	root	RT	-5	0	0	0	S	0.0	0.0	0:00.00	migration/0
4	root	15	-5	0	0	0	S	0.0	0.0	0:00.03	ksoftirqd/0
5	root	RT	-5	0	0	0	S	0.0	0.0	0:00.00	watchdog/0
6	root	15	-5	0	0	0	S	0.0	0.0	0:05.16	events/0
7	root	15	-5	0	0	0	S	0.0	0.0	0:00.02	khelper
41	root	15	-5	0	0	0	S	0.0	0.0	0:00.02	kblockd/0
44	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	kacpid
45	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	kacpi_notify
108	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	kseriod
146	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pdf_lush
147	root	20	0	0	0	0	S	0.0	0.0	0:00.21	pdf_lush
148	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	kswapd0
190	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	aio/0
1341	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	ata/0
1342	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	ata_aux
1348	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	scsi_eh_0
1351	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	scsi_eh_1
2094	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	scsi_eh_2
2305	root	15	-5	0	0	0	S	0.0	0.0	0:00.15	kjournald
2481	root	16	-4	2216	652	384	S	0.0	0.1	0:00.31	udev
2739	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	kpsmoused
3849	daemon	20	0	1836	524	428	S	0.0	0.1	0:00.00	portmap
3867	statd	20	0	1900	716	616	S	0.0	0.1	0:00.00	rpc.statd
3873	root	15	-5	0	0	0	S	0.0	0.0	0:00.00	rpciod/0
3888	root	20	0	3652	564	316	S	0.0	0.1	0:00.00	rpc.idmapd
4095	dhcpc	18	-2	2440	772	452	S	0.0	0.1	0:00.03	dhclient3

Une meilleure utilisation de `top` consiste à l'effectuer dans une console différente. On comprend facilement les renseignements traitant de l'occupation processeur, mémoire et swap.

La commande

Cette commande plus difficile d'accès (plutôt pour les administrateurs chevronnés) affiche les appels système et les signaux POSIX (échanges entre le noyau et les processus). Si vous voulez en voir une démonstration, tapez :

```
strace touch essai.txt
```

La commande montre les informations pour la commande `touch` créant un fichier vide `essai.txt`. Strace s'utilise aussi sur des processus déjà ouverts.

La commande

Cette commande liste les fichiers ouverts et les processus actifs :

- `lsof -i` : indique les processus de type Internet.

- `lsof -ni tcp:25` : même chose mais pour un seul protocole.
- `lsof -ni @192.168.0.1:25` : même chose mais pour une seule machine.
- `lsof -i -a -p 1234` : tous les ports réseau ouverts par le processus 1234 (-a est interprété comme l'opérateur ET).
- `lsof -p -u 1000` : tous les fichiers ouverts par l'utilisateur d'id 1000.

Bien sûr, il existe d'autres commandes pour faire cela, mais celle-ci est très complète.

c. "Tuer" un processus

Ubuntu stocke les processus ouverts dans le répertoire `/var/run`. La fin d'un processus se termine généralement normalement, mais il peut arriver d'avoir un processus bloqué, auquel cas il n'est pas nécessaire de redémarrer la machine. L'administrateur utilise la commande :

```
kill [-s signal]
```

On peut "tuer" un processus en ligne de commande par la commande `kill` ou `killall`. La première passe en argument le numéro de processus alors que la deuxième passe le nom de la commande. Concrètement `kill` envoie un signal à un processus et pas seulement celui qui lui demande de s'arrêter (voir la page de manuel plus de détails). Celui qui "tue" un processus est le signal 9. La commande s'écrit donc :

```
kill -9 n°_de_PID
```

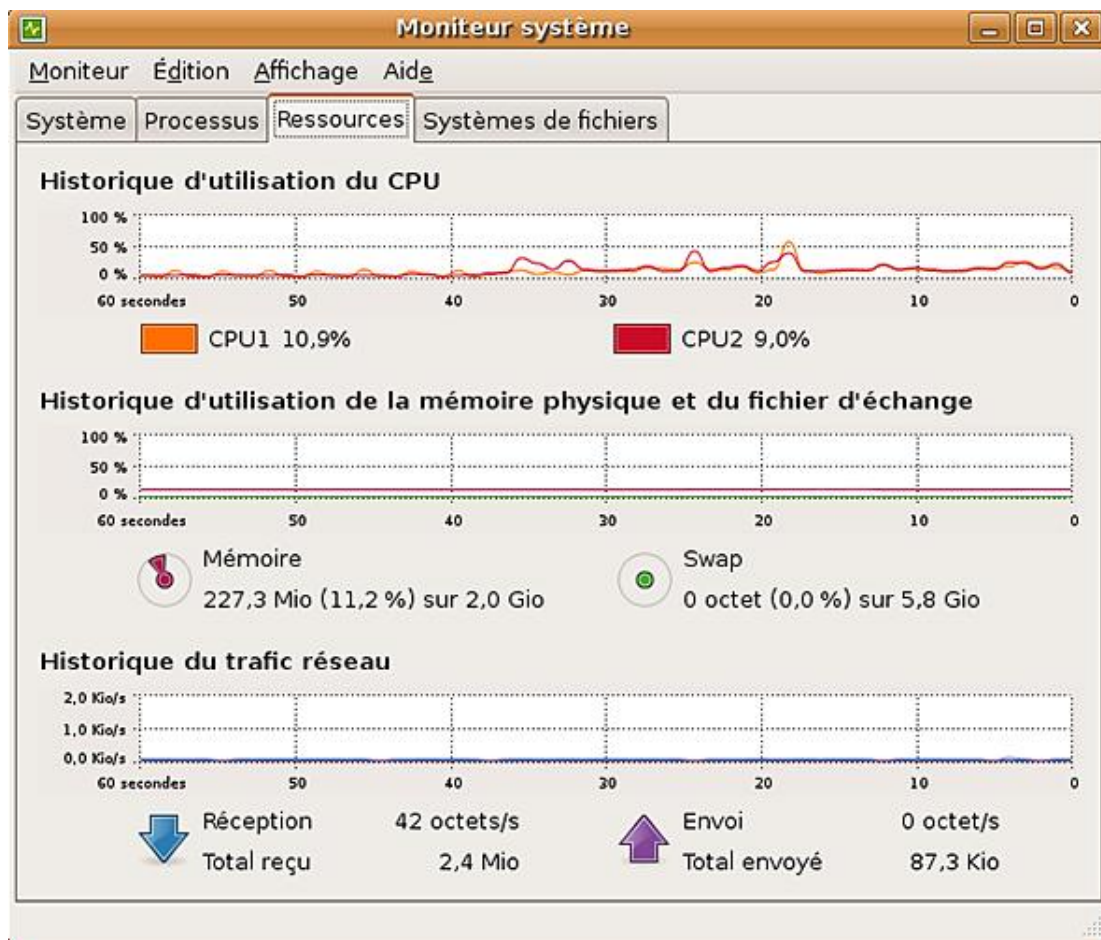
Attention de bien identifier le bon processus ! Outre les instabilités engendrées par une manipulation erronée, la réussite en dépend. Par exemple, dans le cas du serveur WEB Apache, plusieurs processus sont en jeu :

```
root      8215  0.0  0.5  10472  2584 ?        Ss   11:41   0:00 /usr/sbin/apache2 -k start
uuu-data  8216  0.0  0.3  10244  1784 ?        S    11:41   0:00 /usr/sbin/apache2 -k start
uuu-data  8218  0.0  0.4 231808  2400 ?        Sl   11:41   0:00 /usr/sbin/apache2 -k start
uuu-data  8222  0.0  0.4 231808  2404 ?        Sl   11:41   0:00 /usr/sbin/apache2 -k start
root      8535  0.0  0.1   2644  1008 tty1    R+   11:41   0:00 ps aux
```

Sur les quatre processus pour Apache, seul celui sous l'identité du `root` compte (processus père). C'est donc celui-là qu'il faut détruire par un `kill -9 8215`.

d. Moniteur du système en mode graphique

Sous GNOME, l'application **gnome-system-monitor** (menus **Système - Administration - Moniteur système**) rend plus agréable les opérations de surveillance et de gestion des ressources systèmes :



3. Surveillance du système par les journaux

a. Consignation des évènements

Ubuntu consigne les évènements de son activité par l'intermédiaire de deux services généraux : syslogd et klogd. La commande `ps aux | grep logd` montre (parmi d'autres lignes) les deux processus en cours :

```
syslogd 5256 0.0 0.0 1936 684 ? Ss 07:46 0:00 /sbin/syslogd -u syslo
...
klogd 5314 0.0 0.0 3860 2776 ? Ss 07:46 0:00 /sbin/klogd -P /var/run
```

Les fichiers journaux se trouvent dans le répertoire `/var/log` :


```

root@muaddib:~# ls /var/log/
acpid          dmesg          lastlog        samba
apache2        dmesg.0        lpr.log        scrollkeeper.log
apparmor        dmesg.1.gz     mail.err       syslog
apt            dmesg.2.gz     mail.info      syslog.0
aptitude       dmesg.3.gz     mail.log       syslog.1.gz
auth.log       dmesg.4.gz     mail.warn      syslog.2.gz
auth.log.0     dpkg.log       messages       syslog.3.gz
boot           exim4          messages.0     udev
bootstrap.log  faillog        messages.1.gz  unattended-upgrades
btmpt          fontconfig.log mysql           user.log
cups           fsck           mysql.err      user.log.0
daemon.log     gdm           mysql.log      wtmp
daemon.log.0   installer     mysql.log.1.gz wvdialconf.log
debug          kern.log       mysql.log.2.gz Xorg.0.log
debug.0        kern.log.0     news           Xorg.0.log.old
dist-upgrade   kern.log.1.gz pycentral.log
root@muaddib:~#

```

Le répertoire comporte plusieurs autres journaux car, pour des raisons de lisibilité, les consignations se rapportant à d'autres services font l'objet d'un ou de plusieurs fichiers séparés. Ainsi, au lieu de "fouiller" dans le fichier `syslog`, l'administrateur accède directement aux informations de l'application. Certaines gèrent même leurs journaux sans passer par le démon `syslog`.

Ceci se gère par la configuration dans le fichier `/etc/syslog.conf` dont voici un extrait :

```

# /etc/syslog.conf      Configuration file for syslogd.
#
#                       For more information see syslog.conf(5)
#                       manpage.
#
# First some standard logfiles.  Log by facility.
#
auth,authpriv.*      /var/log/auth.log
*.*;auth,authpriv.none -/var/log/syslog
#cron.*              /var/log/cron.log
daemon.*             -/var/log/daemon.log
kern.*               -/var/log/kern.log
lpr.*                -/var/log/lpr.log
mail.*               -/var/log/mail.log
user.*              -/var/log/user.log
#
# Logging for the mail system.  Split it up so that
# it is easy to write scripts to parse these files.
#
mail.info            -/var/log/mail.info
mail.warn            -/var/log/mail.warn
mail.err             /var/log/mail.err

```

Peu de modifications ou changements sont à apporter dans ce fichier, ainsi que la configuration par défaut dans `/etc/default/syslogd`. Cela dépend essentiellement de l'application. Aussi, vous vous reporterez au manuel de celle-ci. La structure d'une ligne suit la base :

```
fonction.priorité      fichier
```

Dans l'exemple, les événements du service de courrier (mail) comportent trois priorités : `info`, `warn` et `err`. Le tiret devant les fichiers de logs des deux premiers informe le démon `syslog` de ne pas synchroniser le fichier après chaque message. L'astérisque comme priorité lui indique d'inscrire tout ce qui concerne la fonction. Il n'est pas contradictoire d'avoir les deux comme le montre l'exemple `mail`. Tous les messages seront inscrits dans `mail.log` et une ventilation de ceux-ci se fera dans les trois autres par priorité.

La pratique courante de l'administrateur consiste à ouvrir une console supplémentaire et à taper la commande :

```
tail -f /var/log/syslog
```

Cela ouvrira la fin du fichier sans le refermer. Toute nouvelle inscription s'affichera en temps réel : ce qui est, pour un administrateur, très utile.

Pour être complet, sachez qu'en mode graphique un utilitaire **gnome-system-log** affiche ou surveille les journaux système par les menus **Système - Administration - Visionneur de journaux système**.

b. Archivage des fichiers journaux

De par l'obligation légale dans certaines activités de garder trace des informations et simplement du fait que l'administrateur puisse les revoir, les fichiers journaux sont archivés suivant des règles définies pour le programme logrotate dans `/etc/logrotate.conf` :

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here
/var/log/wtmp {
    missingok
    monthly
    create 0664 root wtmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0664 root wtmp
    rotate 1
}

# system-specific logs may be configured here
```

Ubuntu transforme donc les fichiers journaux en archive (numéro.gz) avec, on le voit, une fréquence hebdomadaire qui n'excède pas 4 semaines. Les fichiers wtmp et btmp utilisés par les programmes login, shutdown, etc. font l'objet d'un archivage séparé. Vous pouvez mettre vos propres règles d'archivage là où le message le spécifie.

L'exécution de logrotate s'effectue par cron et, vu la fréquence, plus exactement par cron.weekly.

Manipulations en ligne de commandes

L'administrateur sur un serveur utilise la ligne de commandes pour ses manipulations de fichiers textes, scripts, périphériques, etc. Certaines techniques s'apparentent aux figures imposées du patineur artistique : peu valorisantes et attractives, elles sont néanmoins nécessaires pour maîtriser son métier. Pour suivre l'esprit de l'ouvrage résolument tourné vers la distribution Ubuntu et non sur l'apprentissage du système Linux, les paragraphes suivants ne présenteront qu'une base de ces techniques.

1. Expressions régulières

Une expression régulière (ou rationnelle) décrit de façon générique une chaîne de caractères contenue dans un fichier ou nom de fichier. En fait, on peut simplifier en disant qu'une expression régulière est une manière plus compacte (mais pas forcément plus lisible...) de définir un modèle (pattern) de chaîne de caractères. Les objectifs s'identifient comme une demande de sélection suivant ce critère, ou d'effectuer des traitements comme des substitutions sur les chaînes trouvées. Leur utilisation s'étend à partir de certains filtres shell (grep, sed, awk...) à des langages de scripts pour administrateurs : perl, python...

Attention ! Certains caractères spéciaux ressemblent aux caractères génériques de désignation de fichiers (caractères d'englobements) : elles ne se confondent pas avec les 'jokers' ou caractères spéciaux du shell. Même s'il existe des similitudes, ils ont une interprétation différente.

a. Expressions régulières atomiques ou ERA

L'ERA représente un seul caractère du type `ch` (type normal) ou `sp` (type spécial). Concrètement, si vous voulez rechercher toutes les lignes d'un fichier qui contient la chaîne de caractères coucou (qui n'est, après tout, qu'une succession de caractères, soit `c o u c o u`), vous aurez la syntaxe suivante :

(commande de recherche) `'coucou' [nom_de_fichier]`

Cela affiche les lignes d'un fichier contenant le mot "coucou". Vous pouvez aussi utiliser une ERA avec un type spécial :

`^` : indique le début d'une ligne.

`$` : indique la fin d'une ligne.

`.` : indique tout caractère sauf nouvelle ligne (new line ou retour chariot).

`*` : indique la répétition de 0 à n fois du caractère.

`[]` : indique un ensemble de caractères.

`[^]` : correspond à l'un des caractères non inclus dans l'ensemble.

`\<` : correspond au début de mot.

`\>` : correspond à la fin de mot.

`\` : enlève la signification spéciale du caractère suivant.

Exemples :

`i` : le caractère i.

`.` : un caractère quelconque.

`\.` : le caractère `.` : ce n'est plus un caractère spécial car précédé de `\`.

`[aceg]` : soit a, c, e ou g.

`[^aceg]` : tous les caractères autres que a, c, e ou g.

[a-f] : tout caractère compris entre a et f suivant l'ordre alphabétique.

[^a-f] : tout caractère n'appartenant pas à l'intervalle a-f.

\<p : tous les mots commençant par p.

e\> : tous les mots finissant par p.

Certains caractères comme \$, *, [etc. ont une signification particulière pour le shell : vous devez donc mettre en quotes l'expression régulière.

b. Expressions régulières simples ou ERS

L'ERS s'obtient en juxtaposant (concaténation) des ERA. L'ERA de droite s'applique à l'ERA de gauche. Dans certains cas, l'ERA se "multiplie" par d'autres expressions :

x? : recherche dans la chaîne une fois au maximum le caractère représenté par x.

x* : recherche dans la chaîne 0 ou plus le caractère représenté par x.

x+ : recherche dans la chaîne au moins une fois le caractère représenté par x.

x\|y : recherche dans la chaîne le caractère représenté par x ou y.

x\[n\] : recherche dans la chaîne précisément n fois le caractère représenté par x.

x\[n,\] : recherche dans la chaîne contenant au moins n fois le représenté par le caractère x.

x\[,\m\] : recherche dans la chaîne 0 ou m fois le caractère représenté par x.

x\[n,m\] : recherche dans la chaîne de n à m fois le caractère représenté par x.

Exemples :

Prenons comme test le fichier texte (les numéros de lignes ne font pas partie du fichier, elles sont là pour identifier les lignes) suivant :

```
1   mars
2
3   le marsupilami
4   marsupial
5   barre mars
6   martinet 1515
7   une mare
8   bien
9   mar
```

'mars' : chaîne mars (retourne les lignes 1,3,4 et 5).

'mars.' : chaîne mars suivie de n'importe quel caractère (lignes 3 et 4).

'mars*' : chaîne mar, ou mars ou marss ou marsss... (toutes sauf la 2 et 8).

Rappel : * n'a pas la même signification qu'en shell. Cet ERA s'applique au caractère de gauche, le s et demande un nombre n de s.

'[mars]' : lignes contenant (sans exclusive) des m, a, r, s (toutes sauf la 2 et 8).

'[^mar]' : lignes ne contenant pas exclusivement des m, a, r (toutes sauf la 2).

'[r]{2\}' : lignes où les chaînes (mots) ayant 2 r se suivant (ligne 5).

Notez le \ enlevant la signification spéciale des accolades. On peut spécifier un opérateur logique de cette façon :

'rs\$\\al\$' : lignes se terminant par rs **ou** al (lignes 1,4,5).

c. Expressions régulières étendues ou ERE

L'ERE s'obtient en juxtaposant (concaténation) des ERA ou des ERS.

Exemples d'ERE sur le même fichier :

'[^a-zA-Z]' : chaînes contenant a contrario des espaces ou des chiffres (lignes 3,5,6,7).

'^mar' : lignes commençant par m, a, ou r (lignes 1,4,6).

'mars\$' : même chose mais en fin de ligne (1,5) avec s.

'[0-9]' : désigne un chiffre quelconque (6).

'^[^m]' : ligne ne commençant pas par un m (3,5,7,8).

'ar\\{2,\\}' : ligne contenant au moins deux fois ar (5).

d. Utilisation des expressions régulières avec grep

Cette commande se décline en fait sur trois niveaux :

- grep utilise les expressions régulières simples (par défaut grep -G).
- egrep utilise les expressions régulières étendues (ou grep -E).
- fgrep n'utilise pas d'expression régulière mais recherche une chaîne littérale (ou grep -F).

Syntaxe :

grep [-options] expression [fichier]

Avec grep, les motifs doivent être saisis entre guillemets (exemple : "UnMotif") ou entre apostrophes si le motif contient un "\$" (exemple : '\$UnMotif'). Ces commandes disposent aussi d'options (voir le manuel en ligne pour plus de détails).

Exemples d'utilisation :

sans expressions régulières

grep 'es' fichier.txt	# toutes les lignes contenant 'es'
grep -n 'es' fichier.txt	# toutes les lignes numérotées contenant 'es'
grep -i 'il' fichier.txt	# toutes les lignes contenant 'il' en minuscules ou majuscules
grep -l 'Z' *	# tous les noms de fichiers contenant 'Z'

avec expressions régulières

grep 'ss.' fichier.txt	# toutes les lignes contenant ss plus un caractère quelconque
grep '[0-9]' fichier.txt	# toutes les lignes contenant un caractère numérique
grep '^print' fichier.pl	# toutes les lignes contenant print en début de ligne
grep '^[^a-z]' fichier.txt	# les lignes ne contenant pas des minuscules en début de ligne

Exemple montrant les caractères spéciaux dans une expression régulière :

```
grep '\\home\\a[a-z]*' test.txt
```

Si on suppose que `test.txt` contient un listing de noms de fichiers avec leur répertoire, la commande retournera les fichiers contenant la séquence `\home\`, commençant par `a` et suivi de zéro ou plusieurs minuscules `alphonse`, `albert`, `aurélien`, `andré`...

En décomposé :

- on a `\\` qui donne `\` pour le *back slash* ou symbole de division inversé
- `home` pour ... `home`
- `\\` pour encore le *back slash*
- `a` pour la lettre ... `a`
- `[a-z]` pour les minuscules avec `*` s'appliquant donc zéro ou plusieurs minuscules appartenant à l'intervalle.

2. Commandes d'édition ou filtres de fichiers

Pour voir ces quelques commandes (il ne sera pas exposé ici les commandes `sed` et `awk`), la base de travail portera sur le fichier texte `neveux.txt` contenant les lignes :

```
riri:rouge:1
fifi:vert:2
loulou:bleu:3
```



La syntaxe de ce fichier se rapproche de celle de beaucoup de fichiers de données sous Linux, à commencer par un des premiers d'entre eux : le fichier `/etc/passwd`.

La commande

Cette commande coupe en plusieurs champs les lignes d'un fichier ou de l'entrée standard :

```
cut -cliste {position des caractères} fichier
cut -fliste [-dx] {position des champs, x séparateur} fichier
```

Note : liste `-n` équivaut à `1-n` et `p-` à `p-x` (ou `x` représente le dernier).

Avec la commande `cut`, le premier champ a comme numéro 1, le deuxième 2 est ainsi de suite.

Exemples :

```
cut -c10 neveux.txt
# Affichage en colonne du 10ème caractère de chaque ligne e, :, e
cut -c1-4 neveux.txt
# Affichage en colonne des caractères entre le 1er et 4ème caractère
# de chaque ligne riri, fifi, loul
cut -f2 -d: neveux.txt
# Affichage en colonne du deuxième champ de toutes les lignes avec
# comme séparateur les deux points rouge,vert,bleu
cut -f1,3 -d: neveux.txt
# Affichage en colonne du premier et troisième champ de toutes les
# lignes avec comme séparateur les deux points
```

La commande

Cette commande assez simple, compte le nombre de lignes, mots et caractères dans un fichier :

```
wc [-wcl] fichier
```

On a l'option `-w` pour les mots, `-c` pour les caractères et `-l` pour les lignes.

Exemple :

```
wc -wcl neveux.txt
# L'ensemble donne : 3 3 39 neveux.txt. L'ordre de sortie est
# toujours ligne, mot et caractère, séparateur du mot : l'espace
```

La commande

Cette commande lit mais surtout tri le contenu d'un fichier. Par défaut le tri porte sur un seul champ (premier caractère de la ligne) selon l'ordre lexicographique (table ASCII) :

```
sort [-options] [+pos1 [-pos2]] fichier
```

Les principales options :

- d : trie par ordre alphanumérique (caractères, chiffres et espace).
- o : fichier_résultat renvoie le résultat du tri dans le fichier indiqué.
- tx : donne le séparateur (x) au lieu de l'espace ou tabulation (par défaut).
- f : pas de différence entre minuscule et majuscule.
- u : supprime les lignes doublons.
- n : trie sur des chiffres.
- r : renverse l'ordre de tri.

Exemples :

```
sort -o resultat.tri test.txt
# Tri du fichier selon l'ordre lexicographique, résultat dans
# resultat.tri
sort -t: +3n -4 -o res.tri /etc/passwd
# Tri numérique sur le 3ème champ, pos1 et pos2 sont sous la forme
# numéros de champ : +pos1 enlève du tri les champs de 1 à pos1 et
# -pos2 les champs qui suivent pos2 (jusqu'à la fin de la ligne si
# pos2 est omis)
```

Soit sur le fichier neveux.txt :

```
sort neveux.txt
# Affiche le fichier trié par ordre alphabétique
sort -rn -t: +2 neveux.txt
# Affiche le fichier en sens inverse trié numériquement sur le
# 3ème champ
```

La commande

Très utilisée en programmation, la commande `split` coupe un fichier en morceau (en plusieurs fichiers) et ce par nombre de lignes :

```
split -l nombre_de_lignes fichier [fichier1 fichier2 ...]
```

Exemple :

```
split -l 1 neveux.txt
# Découpe en trois fichiers parce que trois lignes dans xaa, xab,
# xac par défaut en cas d'absence de noms de fichiers de sortie
```

Il existe la commande inverse `paste` qui regroupe les fichiers par ligne (voir le manuel en ligne pour plus de renseignements).

La commande

La commande `cmp` indique si deux fichiers sont identiques :

```
cmp fichier1 fichier2
```

Si les deux fichiers sont identiques, la commande ne génère aucune sortie. Dans le cas contraire la commande indique la position de la première différence (ligne et caractère).

Exemple d'utilisation :

(on a un autre fichier *neveux1.txt* avec 4 au lieu de 2 en fin de deuxième ligne) :

```
cmp neveux.txt neveux1.txt
```

Retourne :

```
neveux.txt neveux1.txt sont différents: octet 24, ligne 2
```

La commande `diff` recherche aussi les différences entre deux fichiers et `comm` qui affiche les lignes communes (voir le manuel pour plus de renseignements).

La commande

Cette commande, déjà vue, édite un fichier par la fin, son inverse est `head` :

```
tail -f /var/log/messages
# Montre la fin du fichier
```

Autre utilisation :

```
tail -50 /var/log/syslog
# Montre les 50 dernières lignes du fichier
```

La commande

Cette commande aux multiples usages affiche, crée, copie et concatène des fichiers. Elle s'emploie seule ou avec des commandes spéciales (comme les filtres) en utilisant les mécanismes de redirections. Les principales fonctionnalités de cette commande sont :

- La lecture au clavier : lecture des données au clavier et affichage en écho à l'écran, la fin de saisie par `<ctrl -d>`.

```
cat
# saisie d'un texte quelconque, fin par <ctrl-d>
```

- Copie de fichier : copie du fichier *nifnif.txt* dans le fichier *nafnaf.txt* en utilisant la redirection de la sortie standard (alternative à la commande `cp`).

```
cat nifnif >nafnaf
```

- Affichage d'un fichier : affichage à l'écran du contenu du fichier *mechantloup.txt*

```
cat mechantloup.txt
```

- Création d'un fichier : création du fichier *noufnouf.txt* avec lecture au clavier par l'entrée standard et redirection de la sortie standard, fin par `<ctrl -d>`.

```
cat >noufnouf.txt
```

- Concaténation de fichier : regroupement dans le fichier *maisonbriques.txt* par la redirection de la sortie standard.

```
cat nifnif.txt nafnaf.txt noufnouf.txt >maisonbriques.txt
```

La commande

La commande `tr` convertit une chaîne de caractères en une autre de taille égale. Les options sont les suivantes :

`-c` : les caractères qui ne sont pas dans la chaîne d'origine sont convertis selon les caractères de la chaîne de destination.

-d : destruction des caractères appartenant à la chaîne d'origine.

-s : si la chaîne de destination contient une suite contiguë de caractères identiques, cette suite est réduite à un caractère unique.

Cette commande, plus complexe qu'elle en a l'air, nécessite un fichier (ou une commande par un tube) en entrée standard, sortie à votre convenance. Nous ne l'utiliserons que dans le cas d'une substitution d'éléments. Exemple d'utilisation :

```
tr ":" "#" <neveux.txt neveux.txt
# Remplace les deux points par le caractère dièse
```

La commande

Cette commande très utilisée par l'administrateur, outre son utilisation avec les expressions régulières (voir plus haut), accompagne souvent d'autres commandes dans un tube.

Principales options :

-n : fait précéder chaque ligne d'un numéro de ligne.

-v : affiche toutes les lignes sauf celles contenant "expression".

-i : pas de distinction entre minuscules et majuscules.

-c : affiche le nombre de lignes contenant "expression".

Utilisation de `grep` avec un tube et la commande `wc` :

```
grep "le" test.txt | wc -l
# Compte le nombre de lignes contenant le mot le dans le fichier
```

Ou par exemple pour interroger la base de données des paquetages avec un mot :

```
dpkg -l | grep -i bind
# dpkg -l retourne tous les paquetages, grep les filtre sans
# distinction des majuscules/minuscules et affiche tous les
# paquetages contenant le mot bind
```

3. Entraînement

Toujours pour vous aider dans la maîtrise des commandes, voici une liste d'exercices (les solutions se trouvent toujours en Annexe) :

Cadre de travail

Session ouverte en `root` sur une version Ubuntu serveur. Reprenez l'exemple du fichier des ERS et ajoutez-lui quelques lignes de façon à ce qu'il contienne ceci :

```
mars
le marsupilami
marsupial
barre mars
martinet 1515
une mare
bien
mar
mar mare
langage
language
Language
Language
le le le langage gage ge jjjjjjjava jjjaaavvvaaa jaaavvaaaaa jaavvaaaaa
05.06.07.08
0 1 2 3 5 6 7 8 9
0123456789
riri 05-55-35-22-55 23 ans
fifi 10-23-22-55-63 35 ans
```

Donnez-lui pour nom test1.txt.

Exercices - Partie 1

- Affichez les lignes contenant la chaîne ar.
- Affichez les lignes dont au moins une chaîne contient au minimum 3 j consécutifs.
- Affichez les lignes ayant au moins une chaîne se terminant par age.
- Affichez les lignes ayant au moins une chaîne se terminant par guage ou gage.
- Affichez les lignes se terminant par age ou ava.
- Affichez les lignes vides.
- Affichez les lignes contenant les sous-chaînes 35 ET ans (vous ferez un "tube").
- Affichez les lignes ne commençant pas par un chiffre.
- Affichez les lignes ne contenant que des chiffres.
- Affichez les lignes commençant par une voyelle ou un chiffre.
- Affichez les lignes ne se terminant pas par un chiffre.
- Affichez les lignes faisant moins de 10 caractères.

Voici maintenant un autre fichier nommé test2.txt :

```
riri:rouge:1:caneton  
fifi:vert:2:caneton  
loulou:bleu:3:caneton  
donald:jaune:4:canard  
trouvetou:violet:5:canard  
daisy:rose:6:canard  
picsou:or:7:canard
```

Exercices - Partie 2

- Affichez à l'écran par cat le contenu du fichier.
- Quel est le nombre de mots, de lignes et de caractères de ctest2.txt ?
- Combien de lignes contient ce fichier ?
- Affichez à l'écran le deuxième champ de toutes les lignes.
- Quel est le nombre de canards ?
- Envoyez le fichier test2.txt avec uniquement le premier champs de toutes les lignes dans un fichier noms.txt.
- Triez le fichier noms.txt par ordre alphabétique.

- Coupez le fichier test2.txt en **deux fichiers** test2aa et test2ab (voir l'option nécessaire dans le manuel en ligne).
- Réunissez-les dans un fichier disney.txt.

4. Montage et démontage manuel d'un système de fichiers

Pour un serveur, le montage d'un système de fichiers ne se réalise pas de façon automatique. La base du procédé se situe dans le fichier /etc/fstab déjà vu lors du montage d'un disque dur supplémentaire (chapitre Administration des ressources).

Ubuntu suit la tendance générale qui consiste à abandonner le répertoire /mnt pour le répertoire /media. Afin de faciliter les multiplications de périphériques, le répertoire /media/cdrom est en fait un lien vers /media/cdrom0.

a. Principes de montage

Le répertoire qui rattache le système de fichiers externe au système général s'appelle un point de montage et **doit exister au préalable**. Le montage passe par la commande `mount`. Assez complexe, elle mérite un passage vers les pages de manuels :

`mount [options] [-t type] périphérique répertoire`

La commande seule affiche les systèmes de fichiers et les attributs de montage :

```
root@serveur:~# mount
/dev/sda3 on / type ext3 (rw,relatime,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
/sys on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,noexec,nosuid,nodev,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
devshm on /dev/shm type tmpfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/sda2 on /home type ext3 (rw,relatime,usrquota)
securityfs on /sys/kernel/security type securityfs (rw)
root@serveur:~# _
```

On voit bien les répertoires physiques sur les partitions et les montages systèmes comme par exemple /dev/shm espace mémoire partagé pour les échanges entre les processus.

Montage du lecteur de disquette

Ce type de périphérique, bientôt obsolète, se monte avec la commande (le type est détecté) :

`mount /dev/fd0 /media/floppy0`

Si la ligne du lecteur de disquettes se trouve présente dans le fichier /etc/fstab, un simple `mount /media/floppy0` suffit. Ne jamais enlever la disquette avant de la démonter sous peine de perte de données (le lecteur de CD-Rom, lui, ne peut pas s'ouvrir).

Montage du lecteur de CD-Rom

La commande complète nécessite le type :

`mount -t iso9660 /dev/cd0 /media/cdrom0`

Le montage d'autres partitions, notamment celles d'un système différent ne pose plus de problème : Ubuntu reconnaît la plupart des systèmes de fichiers avec maintenant le système NTFS en lecture **et écriture**.

b. Démontage

Le contraire de la commande `mount` est `umount` (et non pas `unmount`) :

umount point_de_montage

Attention : pour démonter un périphérique, vous ne devez être dedans.

5. Stratégies et outils de sauvegarde

La sauvegarde des données fait partie intégrante du travail de l'administrateur système. La question n'est pas de savoir pourquoi sauvegarder mais quand, comment et quoi sauvegarder. Corollaire de la pratique des sauvegardes : la manipulation d'archives.

a. Principes de la sauvegarde de données

Il faut distinguer les différentes méthodes : la méthode dite incrémentielle s'applique à sauvegarder les fichiers modifiés (ou susceptible de l'avoir été) depuis la dernière sauvegarde. Cette pratique suffit dans de nombreux cas, mais ce n'est pas la seule : on peut envisager une sauvegarde complète à intervalles réguliers, jour, semaine, mois...

En fait, pour une meilleure efficacité on utilise trois méthodes en même temps :

- la sauvegarde **complète**, qui comme son nom l'indique sauvegarde toutes les données à un instant T ;
- la sauvegarde **incrémentielle**, qui ne sauvegarde que les données modifiées depuis la dernière sauvegarde complète ;
- la sauvegarde **différentielle**, qui ne sauvegarde que les données modifiées depuis la dernière sauvegarde (qu'importe son type).

Les unités de temps généralement utilisées sont le jour, la semaine et le mois. Voici un exemple de cycle de sauvegarde :

	Dim	Lun	Mar	Mer	Jeu	Ven	Sam
Semaine 1	C	D	D	I	D	D	D
Semaine 2	C	D	D	I	D	D	D
Semaine 3	C	D	D	I	D	D	D
Semaine 4	C	D	D	I	D	D	D

Et en utilisant, bien entendu, des supports de sauvegarde différents.

b. Commandes et outils de sauvegarde

Note : Les exemples portent sur la sauvegarde du répertoire des utilisateurs : /home.

La commande

Cet utilitaire lit les fichiers et les enregistre de façon séquentielle dans le fichier de sortie. Il utilise pour compresser en ligne les données un utilitaire externe : `gzip`. Citons quelques problèmes épineux : la restauration des données (les archives corrompues ne sont pas récupérables), la sauvegarde de système entier (pour `/proc` ou les répertoires `nfs`) et l'impossibilité de sauvegarde sur plusieurs bandes.

Syntaxe (simplifiée, vu la complexité de la commande) :

```
tar [-options] archive répertoire/fichier
```

Exemple d'utilisation classique :


```
tar -cvzpf home.tar.gz /home
```

Où :

c (--create) : indique le mode création.

v (--verbose) : indique le mode "verbeux". Dans l'exemple, la liste complète des fichiers.

z (--gzip) : indique l'utilisation de gzip.

p (--same-permissions) : garde les mêmes permissions et droits.

f (--file) : utilise le nom du fichier archive qui suit.

La restauration se réalise par :

```
tar -zxvf home.tar.gz
```

Où :

z (--gunzip) : indique l'utilisation de gunzip.

x (--extract) : indique l'extraction des fichiers de l'archive.

Les deux dernières options sont déjà vues, l'absence de répertoire de sortie indique le répertoire courant. Pour une sauvegarde incrémentielle ou différentielle, on utilise l'option :

-g fichier (--listed-incremental)

Ce qui donnerait :

```
tar -cvzp -g /root/incrs.lst -f home.tar.gz /home
```

Où incrs.lst est le fichier stockant les informations de la sauvegarde incrémentielle. Si on ne change pas le fichier incrs.lst, tar effectuera une sauvegarde différentielle la fois suivante. Si l'on se base par rapport au premier incrs.lst (copié pour sauvegarde), on effectue une sauvegarde incrémentielle. Utiliser un autre nom (ou effacement) pour le fichier de sauvegarde incrémentielle revient à faire une sauvegarde complète.

La commande

Cette commande copie tout simplement son fichier spécifié en entrée sur celui en sortie. Créé initialement pour le support bande magnétique, on l'utilise maintenant soit pour dupliquer une bande (entre deux lecteurs), soit pour écrire une image amorçable sur une disquette. On peut aussi l'utiliser pour effectuer des conversions de types de bandes, mais cela ne sera pas vu ici.

Syntaxe :

```
dd [options] if=fichier_entrée of=fichier_sortie [bs=taille_de_bloc]
```

Les commandes

Ces commandes s'utilisent pour les sauvegardes incrémentielles du système Linux. Attention, dump opère sur un niveau plus bas que les autres commandes de sauvegarde : celui des inodes ; il prend en charge explicitement le système de fichiers utilisé.

Syntaxe principale :

```
dump [n]uf périphérique_sauvegarde système_à_sauvegarder
```

Où :

n : représente le niveau incrémentiel de 0 à 9, le niveau 0 définissant une sauvegarde complète alors qu'un niveau n définit une sauvegarde différentielle par rapport au niveau n-1.

u : stocke l'historique des sauvegardes dans /etc/dumpdates.

f : ce paramètre signifie que le nom de fichier (au sens Linux, c'est-à-dire un fichier de périphérique) qui suit est celui de la sauvegarde.

Exemples d'utilisation :

```
dump -0uf /dev/st0 /home
```

```
# Sauvegarde complète dans un lecteur de bandes de /home
dump -0f /opt/sauv /home
# Sauvegarde du répertoire /home dans un fichier sauv (pas de u)
```

Un dump supplémentaire sur un même niveau donnera une sauvegarde incrémentielle. La sauvegarde à distance s'effectue en rajoutant simplement le nom du serveur (et en utilisant `ssh`) devant le périphérique comme :

```
dump 0uf serveur:/dev/st0 /home
```

La commande `restore` extrait la sauvegarde effectuée avec `dump`.

Syntaxe :

```
restore -t -f /dev/st0
```

Cette commande affiche la liste des fichiers (l'option `t`) et restaure de façon non interactive l'ensemble des fichiers présents sur une bande. Il existe la possibilité d'une restauration interactive (option `i`) :

```
restore -i -f /dev/st0
```

Une invite apparaît : `restore>` ; la commande `ls` permet de voir l'ensemble des fichiers. Si l'on restaure uniquement le répertoire de l'utilisateur `donald`, on tape :

```
restore> add donald
restore> extract
```

Note : voir l'option `-s` si une bande renferme plusieurs archives.

Interventions sur le noyau

Comme le rappelle souvent son créateur Linus Torvalds, le champ de définition de Linux se circonscrit au noyau (kernel) et non comme malheureusement l'usage populaire le fait, à une distribution. Maintenu par une communauté de développeurs (et pour "patron" incontesté, son créateur) en licence GNU, le noyau gère les ressources physiques, puis logiques d'un système informatique. Le système Linux Ubuntu est conforme à la norme POSIX, cette API (bibliothèque logicielle ou interface) régissant les demandes de services des processus au noyau.

1. Principes

Le noyau Linux est dit modulaire car il gère de façon dynamique les pilotes de périphériques en fonction des besoins, à l'inverse du noyau de type BSD (FreeBSD, NetBSD et OpenBSD).

Quelques informations complémentaires :

- le site WEB officiel du noyau : <http://www.kernel.org>
- la version initiale du noyau Ubuntu Hardy Heron : 2.6.24-16

Le numéro tient compte d'une version majeure (2.6) et d'une révision concernant la correction d'erreurs ou l'ajout de fonctionnalités (24). Le dernier chiffre indique une variation dans la configuration ; vous pouvez parfaitement définir votre propre variation en cas de compilation différente du noyau.

a. Les méthodes

Une modification du noyau n'est pas une opération anodine, elle relève plutôt de la tâche complexe et exceptionnelle. En effet, rares sont les besoins réels d'une modification. On peut cependant classer trois motivations :

- Le remplacement du noyau pour une version supérieure.
- L'ajout d'une fonctionnalité ou d'un composant.
- Le retrait d'éléments dans le but d'alléger le noyau.

Cette proposition de travail correspond dans ce chapitre à une méthodologie d'enchaînement logique :

- On se base tout d'abord sur un remplacement d'un noyau pour une version plus récente dans le cadre d'une politique de mise à jour.
- On ajoute ou on supprime une fonctionnalité sur ce nouveau noyau afin d'adapter celui-ci à une situation particulière.
- On améliore le noyau afin d'obtenir une version optimisée pour disposer d'un système plus rapide.

Le dernier traitement fait état d'une modification non pas au niveau du noyau par `initrd` afin d'accélérer le démarrage du système en supprimant les modules inutiles.

b. Préparation de l'environnement

La compilation du noyau nécessite l'installation de paquets spécifiques, à l'instar d'un jardinier préparant son terrain avant toute plantation. La compilation en tant que telle ne présente pas de difficultés. Les raisons des trop fréquents échecs tiennent pour la plupart d'un manque de préparation avant cette compilation.

Les outils de compilation

Ubuntu utilise un paquetage logiciel déjà vu `build-essential`, liste des paquetages considérés comme indispensable pour compiler des logiciels. On peut lui adjoindre le paquet `bin86`, chargé sous Linux de créer le secteur de boot 16 bits et les configurations binaires.

```
aptitude install build-essential bin86
```

Comme toujours, la mise à jour propre du système s'impose :

```
aptitude update
```

```
aptitude safe-upgrade
```

```
aptitude clean
```

Le processus de compilation du noyau possède des outils qui lui sont propres, auquel on ajoute un paquet logiciel particulier permettant d'éviter d'être le **root** lors de la construction du paquet. Plus exactement, on accorde les droits administrateurs au processus de construction du paquet.

```
aptitude install linux-kernel-devel fakeroot
```

Toutes les options de compilation sont regroupées dans un fichier de configuration qu'il est plus simple de gérer via une interface :

- de type texte : avec une interface ncurses
- de type graphique : avec une interface GTK+ (Gnome) ou QT (KDE)

Dans la situation d'un serveur, on passe par l'interface texte et ncurses :

```
aptitude install libncurses5-dev
```

2. Changer le noyau par Aptitude

Le changement de noyau par **Aptitude** et les dépôts Ubuntu s'effectuent de façon triviale lorsqu'il en existe un nouveau : il suffit de lancer la commande `aptitude` avec l'option `full-upgrade`. Elle reste la meilleure méthode et la plus simple d'effectuer un changement sur le noyau, ce qui n'empêche pas un minimum de travail et de méthode.

Vérifiez la version de votre noyau (version courte) :

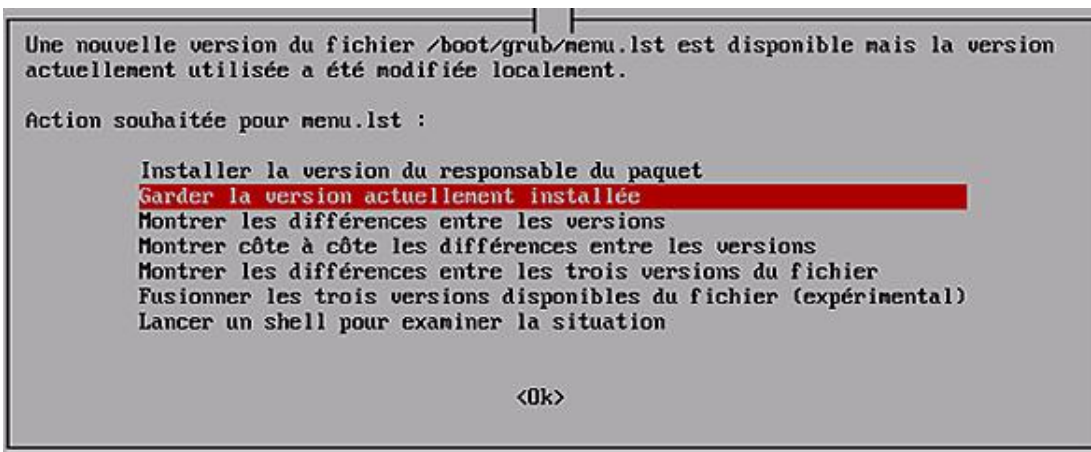
```
uname -r
```

Rappel : l'option `safe-upgrade` ne met à jour que les paquets installés. L'ambiguïté réside dans le numéro de paquet. Si l'on prend exemple sur une distribution serveur initiale avec le noyau 2.6.24-16, le système considère que ce dernier comme installé alors que le noyau 2.6.24-19-server (notre noyau de mise à jour au moment de la rédaction de l'ouvrage, il peut changer bien sûr) ne l'est pas. Un `safe-upgrade` ne changera donc pas la version du noyau alors qu'un `full-upgrade` le fera :

```
aptitude full-upgrade
```

a. Modification pour GRUB

Lors de l'installation, une demande concerne le fichier `/boot/grub/menu.lst` : elle consiste à offrir une nouvelle ligne de menu pour GRUB au démarrage du système.



- Choisissez non pas de garder la version installée (cela ne changerait rien) mais **Installer la version du responsable du paquet**.

Ce choix lance l'utilitaire update-grub qui remplit à la suite du fichier initial les éléments de démarrage du nouveau noyau.

- Redémarrez votre système et choisissez la nouvelle configuration.

b. Nettoyage

Pour ne pas encombrer le système, un nettoyage des précédents paquets s'impose, l'ensemble totalisant près de 90 Mo :

```
aptitude purge linux-image-2.6.24-16-server
```

```
aptitude purge linux-ubuntu-modules-2.6.24-16-server
```

```
aptitude purge linux-restricted-modules-2.6.24-16-server
```

La dernière commande est à omettre si vous n'aviez pas installé de pilotes propriétaires en accès réservé. Si vous aviez installé les en-têtes du noyau :

```
aptitude purge linux-headers-2.6.24-16-server
```

Dans le même ordre d'idée, si vous en avez besoin pour la nouvelle version du noyau :

```
aptitude install linux-headers-`uname -r`
```



L'utilisation de la commande `uname` permet de s'affranchir de la version installée et apporte la certitude d'installer la bonne version.



Attention : les caractères encadrant la commande ne sont pas des apostrophes mais des apostrophes inversées (touches [Alt Gr] 7, suivies d'un espace pour la matérialisation du caractère).

L'ancien répertoire des modules peut ne pas être vide et donc avoir échappé au nettoyage :

```
rm -Rf /lib/modules/2.6.24-16-server/
```

3. Construction d'un autre noyau

a. Charger les sources

Pour Ubuntu comme pour les autres distributions Linux, la véritable source (sans jeu de mots) et la plus récente se trouve sur le site kernel.org. Malgré son intérêt indéniable, cette méthode est à proscrire car ne comportant pas les réglages nécessaires spécifiques à la distribution Ubuntu. On lui préfère le chargement par les dépôts Ubuntu.

Honnêtement, très rares sont les cas où une demande ne saurait être satisfaite par l'installation des dernières sources stables. Par contre, là encore, deux possibilités existent :

- Soit classiquement par `aptitude install linux-source`,
- Soit par l'utilitaire GIT, système de contrôle de version chargé de gérer le code source par les développeurs du noyau Ubuntu.

Le premier ne donnera au mieux que le code source du noyau en cours : autant utiliser les sources sur kernel.ubuntu.com. Le paquetage `git-core` étant installé, la première étape charge une copie locale des sources du noyau à partir du dépôt :

```
git-clone git://kernel.ubuntu.com/ubuntu/ubuntu-hardy.git ubuntu-hardy
```

La totalité prend environ 190 Mo, ce qui peut nécessiter un peu de temps... :

```
root@serveur:~# git-clone git://kernel.ubuntu.com/ubuntu/ubuntu-hardy.git ubuntu
-hardy
Initialized empty Git repository in /root/ubuntu-hardy/.git/
remote: Counting objects: 654683, done.
remote: Compressing objects: 100% (131202/131202), done.
remote: Total 654683 (delta 532869), reused 643791 (delta 522354)
Receiving objects: 100% (654683/654683), 190.44 MiB | 50 KiB/s, done.
Resolving deltas: 100% (532869/532869), done.
Checking out files: 100% (23870/23870), done.
root@serveur:~# _
```

Plus tard, pour garder l'arborescence à jour vous devrez faire :

```
cd /root/ubuntu-hardy
```

```
git pull
```



Linus Torvalds conseille de prendre un utilisateur différent du `root` et de compiler le noyau en dehors du répertoire des sources, ce qui n'est pas le cas ici.

Il ne reste plus qu'à mettre en place l'arborescence dans le répertoire des sources (attention : bien mettre le chemin absolu) :

```
ln -s /root/ubuntu-hardy/ /usr/src/linux
```

```
cd /usr/src/linux
```

b. Compiler le nouveau noyau

L'idée de base réside dans la construction d'un noyau sous la forme d'un paquetage logiciel, facile à installer et... à désinstaller. Les fichiers de configuration, standards pour toutes les architectures, se trouvent dans le répertoire `/usr/src/linux/debian/config`. On y trouve d'ailleurs le fichier `config.generic` et `config.server` pour les images de mêmes noms et le fichier `config` pour tous.



Dans le cas de l'installation des sources par `aptitude install linux-source`, vous auriez pu prendre le fichier de configuration `config-*` se trouvant dans `/boot` puisque, vraisemblablement, la version est identique. Dans l'exemple, la version installée est la version 2.6.24-19 alors que celle par `git` porte le numéro 2.6.24-3.

Une fois cette manipulation effectuée, vous lancez le menu de configuration. Dans ce menu, une étoile indique une option activée, un M un chargement par module (chargé en fonction du besoin) :

```
make menuconfig
```

```
.config - Linux Kernel v2.6.24.3 Configuration

----- Linux Kernel Configuration -----
Arrow keys navigate the menu. <Enter> selects submenus ---.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </>
for Search. Legend: [*] built-in [ ] excluded <M> module < >

+-----+
|  _ General setup _<---> |
|  [*] Enable loadable module support ---> |
|  [*] Enable the block layer ---> |
|      Processor type and features ---> |
|      Power management options ---> |
|      Bus options (PCI etc.) ---> |
|      Executable file formats / Emulations ---> |
|      Networking ---> |
|      Device Drivers ---> |
|      Firmware Drivers ---> |
|      File systems ---> |
+-----+

<Select>  < Exit >  < Help >
```

Exemple :

Dans le cas d'un serveur, il n'est pas nécessaire de garder le support pour la radio amateur, les systèmes utilisant l'infrarouge et le bluetooth dans le menu **Networking** :

```
.config - Linux Kernel v2.6.24.3 Configuration

----- Networking -----
Arrow keys navigate the menu. <Enter> selects submenus ---.
Highlighted letters are hotkeys. Pressing <Y> includes, <N> excludes,
<M> modularizes features. Press <Esc><Esc> to exit, <?> for Help, </>
for Search. Legend: [*] built-in [ ] excluded <M> module < >

+-----+
|  -- Networking support |
|      Networking options ---> |
|      [ ] Amateur Radio support ---> |
|      < > IrDA (infrared) subsystem support ---> |
|      <_> Bluetooth subsystem support ---> |
|      {M} RxRPC session sockets |
|      [ ] RxRPC dynamic debugging |
|      <M> RxRPC Kerberos security |
|      Wireless ---> |
|      {M} RF switch subsystem support ---> |
|      <M> Plan 9 Resource Sharing Support (9P2000) (Experimental) -- |
+-----+

<Select>  < Exit >  < Help >
```

La sortie après modifications propose automatiquement la sauvegarde de la configuration et écrit le fichier .config dans /usr/src/linux.

Ce fichier de configuration fait état d'une configuration du noyau ayant trait à la virtualisation par XEN. Comme vous ne disposez pas des sources de celui-ci, vous devez en effacer la référence dans le fichier de configuration. On peut passer par le menu (voir ce qui suit), mais vous pouvez (autre méthode) éditer directement le fichier :

- Éditez le fichier /usr/src/linux/.config par VIM.
- Effectuez une recherche sur XEN par les touches [Echap] /XEN.
- Supprimez la ligne commençant par CONFIG_XEN=y.

Maintenant, vous pouvez lancer l'utilitaire de construction de paquets Debian du noyau à partir des sources. D'abord avec l'option clean pour vérification :

```
make-kpkg clean
```


Puis pour la construction des paquets pour le noyau (sur une seule ligne et cela va être un peu long...) :

```
fakeroot make-kpkg --initrd
--append-to-version=perso24 kernel_image
kernel_headers modules_image
```

La commande `make-kpkg` regroupe plusieurs commandes : `make dep`, `make bzimage`, `make modules`. À la fin, le résultat se trouve sous la forme de deux paquets que vous installerez par la commande `dpkg -i` :

```
linux-headers-2.6.24.3perso24_2.6.24.3perso24-10.00.Custom_i386.deb
linux-image-2.6.24.3perso24_2.6.24.3perso24-10.00.Custom_i386.deb
root@srvtest:~#
```



Depuis la version Hardy Heron, une nouvelle façon de compiler les sources utilise la commande `AUTOBUILD=1 fakeroot debian/rules binary-debs`. Par expérience, réservez cette méthode si vous installez les sources par `apt-get build-dep linux-image-`uname -r`` et `apt-get source linux-image-`uname -r`` au lieu de `git`. Vous trouverez plus de renseignements sur le WIKI Ubuntu : <https://help.ubuntu.com/community/Kernel/Compile>

4. Accélérer le démarrage du système

a. Principe

Ubuntu utilise le mécanisme `initrd` (voir le chapitre Préalable à l'installation) qui charge un système de fichiers et le monte en mémoire pour détecter et charger les pilotes nécessaires au système de fichiers sur le disque dur. Le fichier au format compressé contenant ce FS de départ se trouve dans le répertoire `/boot` et a pour nom `initrd.img-(numéro du noyau)`.

Au fur et à mesure des versions Ubuntu, cette image `initrd` a tendance à prendre du poids pour la recherche d'une meilleure compatibilité matérielle. Sur votre système, le chargement de la distribution comporte des pilotes a fortiori connus de vous, on peut donc éliminer les pilotes inutiles. Le but est d'accélérer le chargement du système sachant que l'on ne touche pas aux sources du noyau à la différence de la précédente méthode.

b. Méthodologie de réalisation

La démarche consiste à récupérer le système de fichiers, le décompresser, enlever les éléments inutiles, le compresser à nouveau et le faire prendre en compte par le système. Je prends l'exemple d'une distribution en poste de travail, avec un noyau `2.6.24-29-generic` (en `root` bien sûr).

- Copiez le fichier `initrd` dans un répertoire particulier :

```
mkdir /root/initrd

cd /root/initrd

cp /boot/initrd.img-2.6.24-generic .
```

- Déterminez le type exact du fichier (surtout sa méthode de compression) :

```
file initrd.img-2.6.24-19-generic
```

Le retour de la commande annonce normalement un fichier compressé au format `gzip`. La commande effectuant la décompression est un peu compliquée :

```
gunzip < initrd.img-2.6.24-19-generic | cpio -i -make-directories
```

Explications :

`gunzip` : commande de restauration.

`< initrd.img-2.6.24-19-generic` : redirection de l'entrée standard pour le fichier `initrd` "alimente" la commande

gunzip.

| `cpio -i -make-directories` : tube, c'est-à-dire envoi du résultat de la sortie de la commande `gunzip` en entrée de la commande `cpio`.

La commande `cpio` extrait les éléments de l'archive en créant les répertoires si besoin. On se passe maintenant du fichier initial :

```
rm initrd.img-2.6.24-19-generic
```

Le répertoire contient les éléments suivants :

```
root@desktop:~/initrd# ls
bin  conf  etc  init  lib  modules  sbin  scripts  usr  var
root@desktop:~/initrd#
```

Initramfs possède un fichier de configuration situé dans `conf/initramfs.conf` :

```
#
# initramfs.conf
# Configuration file for mkinitramfs(8). See initramfs.conf(5).
#
#
# MODULES: [ most | netboot | dep | list ]
#
# most - Add all framebuffer, acpi, filesystem, and harddrive drivers.
#
# dep - Try and guess which modules to load.
#
# netboot - Add the base modules, network modules, but skip block devices.
#
# list - Only include modules from the 'additional modules' list
#
MODULES=most

#
# BUSYBOX: [ y | n ]
#
# Use busybox if available.
#
BUSYBOX=y

#
# NFS Section of the config.
#
#
#
# BOOT: [ local | nfs ]
#
# local - Boot off of local media (harddrive, USB stick).
#
# nfs - Boot using an NFS drive as the root of the drive.
#
BOOT=local

#
# DEVICE: ...
#
# Specify the network interface, like eth0
#
DEVICE=eth0

#
# NFSROOT: [ auto | HOST:MOUNT ]
#
NFSROOT=auto
```

On y retrouve l'utilisation de la `busybox` comme alternative à un problème de chargement et le démarrage par NFS. La section qui nous intéresse est la première avec les choix pour les modules :

- `most` : charge tous les pilotes.
- `dep` : détecte les pilotes nécessaires à charger.
- `Netboot` : utilise les modules liés au réseau.
- `List` : ne prend que les modules d'une liste additionnelle.

Le deuxième choix suffit largement :

`MODULES=dep`

La suite se passe dans le répertoire `lib/modules/2.6.24-19-generic/kernel`. Des pilotes sont inutiles s'ils sont absents de votre système.

Dans `fs`, on peut supprimer les systèmes de fichiers non utilisés :

- `jfs`
- `reiserfs`
- `xfs`

Dans `drivers`, les pilotes non utilisés :

- `ieee1394` (suivant équipement)
- `parport` (les imprimantes ne sont plus sur port parallèle)
- `virtio` (pour la virtualisation)

Une fois ces modifications (ou d'autres) effectuées, il faut refaire l'opération inverse, c'est-à-dire remettre le système de fichiers dans une archive :

```
cd /root/initrd
```

```
find ./ | cpio -H newc -o > ../initrdnouveau
```

Par rapport à l'ancien fichier, nous sommes passés de 42165 blocs à 39449 blocs. Ensuite, la compression :

```
cd ..
```

```
gzip initrdnouveau
```

Pour remplacer le nouveau système `initrd` :

```
cd /boot
```

```
cp /root/initrdnouveau.gz .
```

Modifiez l'entrée dans `/boot/grub/menu.lst` (ou mieux : dupliquez l'entrée pour plus de sécurité) au niveau de la ligne :

```
initrd /boot/initrdnouveau.gz
```

Redémarrez avec votre nouvel `initrd`. La vitesse de démarrage n'est pas foncièrement évidente sans chronomètre, mais en tout cas, votre processus `initrd` est plus "propre" et adapté à votre configuration.

Gestion des profils utilisateurs

Dans le cadre d'un système multi-utilisateur, la capacité à gérer de manière fine et sécurisée chaque profil se pose de façon redondante. La réponse passe par le triptyque utilisateur - droit - application, ou plus exactement par la question : quels sont les droits globaux des utilisateurs et quels sont leurs droits vis-à-vis de chaque application ? On le voit nettement, la réponse dépasse le classique schéma Propriétaire/Groupe/Reste du monde vu au chapitre Gestion des droits utilisateurs.

1. ACL avec Apparmor

Gérer la sécurité des données revient à assurer leur confidentialité, leur intégrité et leur disponibilité au travers d'un contrôle d'accès, le plus souvent logiciel.

Ubuntu comporte une approche, au travers d'un logiciel nommé **Apparmor**, destinée à associer un profil de sécurité à chaque application. Il suit la norme POSIX 1003.1e (ajoutée à celle classique des permissions donnée par POSIX.1) et introduit la gestion des ACL (*Access Control List*) sous Linux.

Il s'agit donc de définir les droits de chaque utilisateur sur une application et donc d'en permettre une restriction. On passe d'une gestion de type DAC (*Discretionary Access Control*) à une gestion de type MAC (*Mandatory Access Control*) définie par l'administrateur système, elle-même englobée dans une approche de contrôle d'accès par rôle (RBAC ou *Role-Based Access Control*).

SELinux ou Apparmor ?

Cette mise en place sur Linux se traduit sur Linux par une bibliothèque de sécurité (framework) constituée de modules (LSM) et par le choix entre deux techniques :

- **SELinux**, développé par la NSA, l'agence de sécurité américaine, et implanté surtout sur les systèmes Red Hat, Fedora.
- **Apparmor**, développé par Novell et intégré sur OpenSuse (racheté par Novell) et les systèmes Debian, Ubuntu.

Le choix entre l'une ou l'autre des techniques mérite un développement plus long hors de propos dans cet ouvrage. Sachez simplement que SELinux sécurise l'ensemble du système avec une interdépendance lourde sur le système de fichiers alors que Apparmor s'intègre plus facilement grâce à son mécanisme de profils. La lourdeur de la première technique s'oppose à la lisibilité de la deuxième, mais Apparmor ne protège que quelques processus. Aussi, on peut dire que le SELinux est plus strict au sens de la sécurité.

Ubuntu depuis Hardy Heron fait le choix d'Apparmor. La documentation complète se situe sur le site de Novell : <http://www.novell.com/documentation/apparmor/>

2. Administration des profils

Apparmor (licence GPL) se trouve installé et chargé par défaut sur la distribution Ubuntu. Par contre, si certains profils proviennent automatiquement lors de l'installation de certains paquets, d'autres profils se trouvent dans un paquet supplémentaire :

```
aptitude install apparmor-profiles
```

Ces profils se chargent dans le répertoire `/etc/apparmor.d/`. Vous êtes toujours connecté en root.

a. Fonctionnement d'Apparmor

La commande `apparmor_status` permet de faire le point sur les profils existants qui viennent d'être installés :

```

root@server:~# apparmor_status
apparmor module is loaded.
12 profiles are loaded.
1 profiles are in enforce mode.
  /usr/sbin/avahi-daemon
11 profiles are in complain mode.
  /usr/sbin/ntpd
  /usr/sbin/identd
  /usr/sbin/nmbd
  /sbin/klogd
  /usr/sbin/smbd
  /sbin/syslogd
  /sbin/syslog-ng
  /usr/sbin/traceroute
  /usr/sbin/nscd
  /usr/sbin/mdnsd
  /bin/ping
2 processes have profiles defined.
0 processes are in enforce mode :
0 processes are in complain mode.
2 processes are unconfined but have a profile defined.
  /sbin/klogd (3994)
  /sbin/syslogd (3973)

```

Le résultat de cette commande montre les deux modes de fonctionnement d'**Apparmor** :

- Le mode *complaining/learning* : réservé à l'apprentissage ou aux tests, on autorise la violation de profil avec enregistrement de l'événement.
- Le mode *enforced/confined* : le profil s'applique dans toute sa rigueur, on enregistre toute violation éventuelle.



Un profil ne s'applique qu'à un processus en fonctionnement.

Le résultat de la commande `apparmor_status` s'explique donc de la façon suivante :

- 12 profils se trouvent dans le répertoire `/etc/apparmor.d` et sont chargés,
- 11 sont en mode apprentissage et 1 en mode appliqué,
- Seuls deux processus sont en cours (`klogd` et `syslogd`) mais dont les profils sont définis (ils ne sont pas en *learning*) ne s'appliquent pas.

La vérification est facile :

```
ps aZ | grep syslogd
```

La commande d'interrogation sur les processus en cours et plus particulièrement sur le démon `syslogd` retourne :

```
unconfined      4548 tty1  S+          0:00 grep syslogd
```

Il faut bien comprendre qu'un processus peut être soit en mode *complain* contre *enforce* (suivant qu'il est ou non autorisé à suivre le profil), soit en mode *Learning* ou *confined* (suivant qu'un profil est ou non défini).

Une autre façon de suivre les profils consiste à visualiser le fichier `/sys/kernel/security/apparmor/profiles` (essayez par `cat`) :

```

/usr/sbin/traceroute (complain)
/usr/sbin/smbd (complain)
/usr/sbin/ntpd (complain)
/usr/sbin/nscd (complain)
/usr/sbin/nmbd (complain)
/usr/sbin/mdnsd (complain)
/usr/sbin/identd (complain)

```

```
/usr/sbin/avahi-daemon (enforce)
/sbin/syslogd (complain)
/sbin/syslog-ng (complain)
/sbin/klogd (complain)
/bin/ping (complain)
```

b. Commandes

L'exemple pris pour ces commandes concerne l'utilitaire traceroute (le profil est présent mais pas l'utilitaire) :

```
aptitude install traceroute
```

Pour passer en mode enforce le profil :

```
aa-enforce usr.sbin.traceroute
```

Pour revenir en mode complain : aa-complain.

Pour charger un profil : redémarrez le service apparmor ou aa-logprof.

Le premier lancement de cette dernière commande fait état d'une demande sur l'activation d'un dépôt de profil externe. Répondez non à cette question, cela positionnera à no la variable enabled dans le fichier /etc/apparmor/repository.conf. À la date d'écriture de ces lignes le dépôt hardy n'était pas présent ; seule la version gutsy existait (voir le fichier /etc/apparmor/logprof.conf. Comme Novell se réfère à OpenSuse, les développements se rapportent à cette distribution ou celles d'obédience Red Hat comme la Fedora. Les profils "en stock" sont visibles à l'adresse : <http://apparmor.opensuse.org>

Pour l'affichage de la démarche d'application d'un profil, nous allons utiliser la commande bien connue ping, dont voici le profil dans /etc/apparmor.d/bin.ping :

```
# Last Modified: Thu Aug  2 14:28:48 2007
# $Id: bin.ping 935 2007-08-20 01:28:20 DominicReynolds_ $
# -----
#
# Copyright (C) 2002-2005 Novell/SUSE
#
# This program is free software; you can redistribute it and/or
# modify it under the terms of version 2 of the GNU General Public
# License published by the Free Software Foundation.
# -----
#
#include <tunables/global>
/bin/ping flags=(complain) {
    #include <abstractions/base>
    #include <abstractions/containers>
    #include <abstractions/nameservice>

    capability net_raw,
    capability setuid,
    network inet raw,

    /bin/ping mixr,
    /etc/modules.conf r,
}
```

Sans entrer dans les détails de configuration (que vous trouverez dans la documentation Novell citée plus haut), sachez que :

- La directive include permet l'insertion de données issues d'autres fichiers (ici en commentaire).
- La section /bin/ping donne son nom au profil.
- La présence de la directive flags indique le mode complain (absente en cas de enforce).
- La directive capability permet l'accessibilité CAP_NET_RAW Posix.

- Les options `r`, `m`, `ix` définissent respectivement la permission en lecture, l'autorisation de protocole pour les appels `mmap` et `inherit` execute pour l'exécution.

Vous verrez plus loin que la définition de ces éléments est facilitée par la commande `aa-genprof`.



Les commandes préfixées par `aa-` se révèlent en fait des liens vers d'autres commandes. Gardez cette écriture afin d'éviter des confusions.

Vérification du processus

On va montrer le statut de la commande `ping` dans son fonctionnement :

- Ouvrez une deuxième console.
- Faites un `ping` sur une adresse IP de votre réseau local.
- Sur la deuxième console, tapez la commande :

```
ps aZ | grep ping
```

Le résultat au niveau de la deuxième ligne montre un statut `unconfined`.

Passage en mode `enforce` :

```
aa-enforce /bin/ping
```

Vous pouvez le vérifier par la commande `apparmor_status`.

c. Création d'un profil

Voici un script simple, nommé `test.sh` :

```
#!/bin/bash
exec ls -ail
```

- Donnez-lui les droits en exécution :

```
chmod 755 test.sh
```

- Générez le profil :

```
aa-genprof /root/test.sh
```

Le profilage est en cours par une mise sur écoute avec, en retour de messages, l'indication que l'application est démarrée en mode `complain`. À ce stade, deux solutions :

- Soit lancer le programme dans une autre console, revenir dans la première et appuyer sur (S) pour Scan (**meilleure solution**).
- Soit appuyer directement sur (F) pour Finish, lancer le programme et ensuite la commande `aa-logprof`.

Une série de questions traite des exécutions et permissions nécessaires au bon déroulement du programme. La plupart du temps, il s'agit de répondre (I) pour `Inherit` (héritage du programme principal), (A) pour `allow` dans les cas de permissions :

Répertoire: /	-> Allow en mode <code>r</code> pour lecture
Répertoire: /bin/bash	-> Allow en mode <code>r</code> pour lecture
Execute : /bin/ls	-> Inherit en mode <code>x</code> pour exécution
Répertoire : /dev/tty	-> Allow en mode <code>r</code> pour lecture
Fichier : /etc/group	-> Allow en mode <code>r</code> pour lecture
Fichier : /etc/nsswitch.conf	-> Allow en mode <code>r</code> pour lecture

```

Fichier : /etc/passwd          -> Allow en mode r pour lecture
Répertoire : /root/           -> Allow en mode r pour lecture
Fichier : /root/.aptitude      -> Allow en mode r pour lecture
Fichier : /root/test.sh        -> Allow en mode r pour lecture
Fichier : /root/.viminfo       -> Allow en mode r pour lecture
Fichier : /root/.bash_history  -> Allow en mode r pour lecture
Fichier : /root/.bashrc        -> Allow en mode r pour lecture
Fichier : /root/.profile       -> Allow en mode r pour lecture

```

On voit nettement la succession d'opérations, du lancement du script à l'affichage respectif de la commande `ls` (dans le répertoire `/root` il n'y a que 6 fichiers).

Au final, (S) pour sauvegarder le profil :

```

# Last Modified: Fri Jun 20 19:09:25 2008
#include <tunables/global>
/root/test.sh {
    #include <abstractions/base>

    / r,
    /bin/ls ixr,
    /etc/group r,
    /etc/nsswitch.conf r,
    /etc/passwd r,
    /proc/*/mounts r,
    /root/ r,
    /root/.aptitude/ r,
    /root/.bash_history r,
    /root/.bashrc r,
    /root/.profile r,
    /root/.viminfo r,
    /root/test.sh mr,
}

```

Pour faire prendre en compte uniquement le profil :

```
cat /etc/apparmor.d/root.test.sh | apparmor_parser -r
```

Supposons maintenant que l'on change la seule ligne du programme par celle-ci, au combien malveillante :

```
rm *.*
```

L'exécution à nouveau du programme retournera la phase suivante :

```
./test.sh: line 2: /bin/rm: Permission denied
```

On en voit tout l'intérêt par exemple pour des scripts exécutés à partir d'un serveur.

Politique d'authentification

L'authentification sur un système Linux ne concerne pas uniquement une personne physique. On trouve à la fois des utilisateurs et des applications, chacun avec sa propre méthode de demande d'authentification. Les bibliothèques PAM (*Pluggable Authentication Modules*) apportent un mécanisme d'authentification simple, souple et unifié.

1. Modules PAM

a. Principes

PAM décrit la manière de développer des programmes indépendamment de la vérification de l'identité. Ces programmes utilisent pour cela des modules qui se chargent de la demande d'exécution. Une politique d'authentification peut, par exemple, autoriser un simple utilisateur à exécuter une commande en local, mais pas à distance.

L'identification se rapporte au login, l'authentification se vérifie par la saisie du mot de passe de l'utilisateur. En cas de changement de type d'authentification, tous les programmes s'y rapportant doivent être modifiés pour le nouveau fonctionnement. C'est ce que simplifie PAM : les directives des interfaces de modules s'additionnent avec un ordonnancement suivant l'ordre de déclaration.



Modifier sans précaution le mécanisme d'authentification sur un système aboutit parfois à son blocage. Soyez prudent et attentif, sinon la seule ressource sera de vous connecter en mode `rescue` (voir le chapitre Maintenance de base du système) afin de remettre les bons fichiers de configuration PAM.

La source de documentation principale pour PAM se trouve à l'adresse :

<http://www.kernel.org/pub/linux/libs/pam>

Par contre, la multiplicité des modules fait qu'il vaut mieux rechercher directement les informations s'y rapportant. Exemple pour le module `pam_mount` (il permet le montage de volumes pour une session utilisateur) :

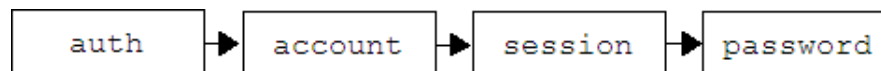
<http://pam-mount.sourceforge.net/>

b. Configuration et structure des fichiers

Les nombreux modules PAM se situent dans le répertoire `/lib/security`, le fichier de configuration générale dans `/etc/pam.conf` et les fichiers de configuration des services dans `/etc/pam.d`. Le fichier de configuration générale sous Ubuntu est vide et utilisé uniquement si le répertoire `/etc/pam.d` n'existe pas.

Les quatre primitives PAM

Le processus de connexion répond à la suite logique de quatre étapes :



Avec :

- **auth** : pour l'identification du compte.
- **account** : pour la vérification de l'autorisation.
- **session** : pour le contrôle des ressources liées au compte.
- **password** : pour la vérification de l'authentification.

Syntaxe d'une ligne d'un fichier PAM

Chaque fichier possède des lignes applicables à des modules (l'ensemble constitue une requête) avec :

- soit une inclusion :

```
@include fichier
```

- soit une structure de la forme :

```
primitive    contrôle    module    arguments
```

Le contrôle se décrit par les directives :

- **required** : le contrôle doit réussir mais l'enchaînement est vérifié.
- **requisite** : le contrôle doit réussir pour continuer l'enchaînement.
- **sufficient** : la validation du contrôle suffit pour valider la requête.
- **optional** : le contrôle doit réussir seulement dans le cas où c'est le seul.

Les modules sont nombreux (nous avons déjà vu `pam_mount.so`). Une authentification normale Unix utilise le module `pam_unix.so` ; une authentification LDAP (*Lightweight Directory Access Protocol* ou service d'annuaire) utilise le module `pam_ldap.so`. La commande `aptitude search libpam` vous donne la liste non exhaustive mais appliquée à Ubuntu, des modules PAM possibles sur ce système.

Les arguments dépendent du module concerné, il faut se reporter à la documentation propre à chaque module. Par exemple, l'argument `use_first_pass`, commun à plusieurs modules, permet de ne pas retaper le mot de passe quand deux modules l'exigent :

```
...
auth required pam_unix.so nullok_secure
auth required pam_ldap.so use_first_pass
...
```

c. Exemple du fichier `/etc/pam.d/login`

Certainement le fichier le plus utilisé, il montre les règles de connexion à une session en mode console. Remarquez les quatre inclusions de fichiers, communes à tous les services.

```
#
# The PAM configuration file for the Shadow `login' service
#

# Outputs an issue file prior to each login prompt (Replaces the
# ISSUE_FILE option from login.defs). Uncomment for use
# auth      required    pam_issue.so issue=/etc/issue

# Disallows root logins except on tty's listed in /etc/securetty
# (Replaces the `CONSOLE' setting from login.defs)
auth      requisite    pam_securetty.so

# Disallows other than root logins when /etc/nologin exists
# (Replaces the `NOLOGINS_FILE' option from login.defs)
auth      requisite    pam_nologin.so

# SELinux needs to be the first session rule. This ensures that any
# lingering context has been cleared. Without out this it is
# possible that a module could execute code in the wrong domain.
# (When SELinux is disabled, this returns success.)
session   required    pam_selinux.so close

# This module parses environment configuration file(s)
# and also allows you to use an extended config
# file /etc/security/pam_env.conf.
#
# parsing /etc/environment needs "readenv=1"
session   required    pam_env.so readenv=1
```

```

# locale variables are also kept into /etc/default/locale in etc
# reading this file *in addition to /etc/environment* does not hurt
session      required    pam_env.so readenv=1 envfile=/etc/default/locale

# Standard Un*x authentication.
@include common-auth

# This allows certain extra groups to be granted to a user
# based on things like time of day, tty, service, and user.
# Please edit /etc/security/group.conf to fit your needs
# (Replaces the `CONSOLE_GROUPS' option in login.defs)
auth          optional    pam_group.so

# Uncomment and edit /etc/security/time.conf if you need to set
# time restraint on logins.
# (Replaces the `PORTTIME_CHECKS_ENAB' option from login.defs
# as well as /etc/porttime)
# account      requisite    pam_time.so

# Uncomment and edit /etc/security/access.conf if you need to
# set access limits.
# (Replaces /etc/login.access file)
# account      required      pam_access.so

# Sets up user limits according to /etc/security/limits.conf
# (Replaces the use of /etc/limits in old login)
session       required      pam_limits.so

# Prints the last login info upon succesful login
# (Replaces the `LASTLOG_ENAB' option from login.defs)
session       optional      pam_lastlog.so

# Prints the motd upon succesful login
# (Replaces the `MOTD_FILE' option in login.defs)
session       optional      pam_motd.so

# Prints the status of the user's mailbox upon succesful login
# (Replaces the `MAIL_CHECK_ENAB' option from login.defs).
#
# This also defines the MAIL environment variable
# However, userdel also needs MAIL_DIR and MAIL_FILE variables
# in /etc/login.defs to make sure that removing a user
# also removes the user's mail spool file.
# See comments in /etc/login.defs
session       optional      pam_mail.so standard

# Standard Un*x account and session
@include common-account
@include common-session
@include common-password

# SELinux needs to intervene at login time to ensure that the
# process starts in the proper default security context. Only
# sessions which are intended to run in the user's context should be
# run after this. (When SELinux is disabled, this returns success.)
session       required      pam_selinux.so open

```

Exemple de modification

Vous désirez filtrer la connexion du root suivant la console. La toute première ligne du fichier login nous montre que ce filtrage se règle au niveau du module pam_securetty.so et de son fichier de configuration /etc/securetty.

- Ouvrez le fichier par VIM et supprimez par exemple la ligne tty4, sauvegardez.
- Ouvrez la quatrième console, tapez comme login le mot root : un message indiquant login incorrect apparaît.

Autre exemple :

Voici ce fichier chargé de la connexion pour une session graphique (type GNOME), expurgé des commentaires :

```
##PAM-1.0
auth    requisite    pam_nologin.so
auth    required     pam_env.so readenv=1
auth    required     pam_env.so readenv=1 envfile=/etc/default/locale
@include common-auth
auth    optional     pam_gnome_keyring.so
@include common-account
session required     pam_limits.so
@include common-session
session optional     pam_gnome_keyring.so auto_start
@include common-password
```

Remarquez les quatre inclusions identiques à celles du fichier `/etc/pam.d/login`.

Tout le mécanisme d'authentification ne passe pas forcément par PAM. Par exemple, si vous désirez vous connecter en `root` à partir de `gdm` (bloqué par défaut), vous cochez la case **Autoriser la connexion locale de l'administrateur système** dans l'onglet **Sécurité** du programme **gdmsetup (Système - Administration - Fenêtre de connexion)**. Cela revient à mettre manuellement la directive `AllowRoot=true` dans le fichier `/etc/gdm/gdm.conf-custom` au niveau de la section `[security]`.

À l'inverse, notez que la connexion automatique par `gdm` sans introduction de mot de passe utilise les modules PAM dans `/etc/pam.d/gdm-autologin`.

2. Utilisation de PAM pour une configuration à un annuaire

En entreprise, le mécanisme d'authentification repose naturellement sur un service d'annuaire de type **LDAP** (*Lightweight Directory Access Protocol*) (Linux) ou **Active Directory** (Windows). On intègre dans cette situation des modules PAM complémentaires, nécessaires à la connexion utilisateur.

a. Connexion à un serveur LDAP



L'exemple traité utilise une version Ubuntu sans session graphique.

Depuis la version Gutsy l'authentification LDAP, plus simple, s'effectue par un outil (optionnel) gérant des profils de connexion centralisés. L'installation du méta-paquetage suivant suffit pour toutes les dépendances :

```
aptitude install ldap-auth-client
```

Questions posées lors de l'installation :

- **l'URL du serveur LDAP** : comme par exemple `ldap://ldap.virtualix.fr` ; mettre l'IP du serveur résout parfois des problèmes de traduction DNS.
- **le nom qualifiant la base** : à partir de notre exemple `dc=virtualix,dc=fr` ; classiquement déduit du nom DNS.
- **la version LDAP utilisée** : usuellement on répond la 3.
- **l'administrateur local comme administrateur de la base** : par défaut sur oui (inutile, voire dangereux), répondre **non**.
- **une obligation de connexion de la base** : usuellement, répondre non.

En cas d'erreur, ces paramètres sont modifiables à partir du fichier `/etc/ldap.conf`.

Exemples de modification :

Certains serveurs LDAP nécessitent l'emploi :

- de la directive `host` comme `host ldap.virtualix.fr`,

- de la directive `soft` comme `bind_policy soft`.

Ces directives (et d'autres) sont données par l'administrateur réseau, gestionnaire du serveur LDAP.

Trois profils sont fournis par défaut dans le répertoire `/etc/auth-client-config/profile.d/` :

- `acc-cracklib` : pour forcer des mots de passe plus complexes ;
- `acc-default` : pour une authentification utilisant le protocole Kerberos ;
- `ldap-auth-config` : modèle pour une configuration de base utilisant un serveur LDAP.

Le script `auth-client-config`, en langage Python, positionne les différents fichiers avec une section décrite dans un fichier présent dans `/etc/auth-client-config/profile.d/` (voir le modèle). L'installation se réalise alors par :

```
auth-client-config -a -p votre_profil
```

Je lui préfère cependant la configuration manuelle, plus didactique, avec tout d'abord la modification du fichier de configuration des bases de données du système en lui ajoutant la possibilité LDAP pour `passwd` et `group` :

```
passwd:      compat ldap
group:       compat ldap
...
```

Vous pouvez dès à présent tester la bonne réponse du serveur LDAP par la commande `getent passwd` ou `getent group`, qui doit retourner normalement les comptes de l'annuaire.

Ensuite, suivant l'enchaînement des inclusions PAM, modifiez (ne mettez que ces lignes) :

- le fichier `/etc/pam.d/common-auth`

```
auth      sufficient      pam_ldap.so
auth      sufficient      pam_unix.so nullok_secure use_first_pass
```

- le fichier `/etc/pam.d/common-account`

```
account    sufficient      pam_ldap.so
account    required        pam_unix.so
```

- le fichier `/etc/pam.d/common-session`

```
session    required        pam_mkhomedir.so skel=/etc/skel
session    required        pam_unix.so
session    optional        pam_ldap.so
session    optional        pam_foreground.so
```

- le fichier `/etc/pam.d/common-password`

```
password    requisite      pam_unix.so nullok obscure min=4 max=8 md5
```

Les modules `libpam-mkhomedir` et `libpam-foreground` doivent être, au préalable, installés. La connexion avec un utilisateur de l'annuaire entraîne, la première fois, la création de son répertoire personnel :

```

root@fai:~# login fougeron
Password:
Linux fai 2.6.24-19-server #1 SMP Wed Jun 18 15:18:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Creating directory '/home/fougeron'.
fougeron@fai:~$ id
uid=4000(fougeron) gid=1000(users) groups=1000(users),2038(Classe_IG12),5001(Eleves)
fougeron@fai:~$

```



Pour le montage automatique d'un répertoire utilisateur avec `pam_mount`, veuillez vous reporter à un ouvrage traitant d'Ubuntu et de l'administration réseau avec l'installation d'un serveur LDAP.

b. Connexion à un serveur Active Directory

Je prends comme exemple un serveur Windows 2003 édition entreprise avec comme domaine `virtualix.local`. Ce type de serveur utilise **Kerberos** (<http://web.mit.edu/Kerberos/>) comme protocole d'authentification réseau par défaut.

Vous devez commencer par installer les paquets liés au protocole Kerberos :

```
aptitude install krb5-user libpam-krb5
```

Renseignez dans le fichier `/etc/hosts` le nom de votre serveur Active Directory (le mien se nomme `win2k3see` ayant pour adresse IP `192.168.3.101`) :

```

127.0.0.1          desktop.virtualix.local      desktop
192.168.3.101     win2k3see.virtualix.local    win2k3see

```

Vérifiez par un `ping` la bonne réponse de votre serveur.

Un point important : synchronisez les heures systèmes entre votre serveur et votre client, que ce soit le deuxième par rapport au premier ou les deux sur l'heure universelle.

La configuration de Kerberos se fait de préférence manuellement à partir de son fichier. Ce protocole fait appel à la notion de royaume (REALM) confondu généralement avec le domaine DNS mais toujours exprimé **en majuscules**. Le fichier résultant, en fonction de notre exemple, donne ceci :

Fichier **`/etc/krb5.conf`**

```

[login]
    default = FILE666:/var/log/krb5lib.log

[libdefaults]
    default_realm = VIRTUALIX.LOCAL
    kdc_timesync = 1
    ccache_type = 4
    forwardable = true
    proxiable = true

[realms]
    VIRTUALIX.LOCAL = {
        admin_server = win2k3see.virtualix.local
        default_domain = VIRTUALIX.LOCAL
        kdc = win2k3see.virtualix.local
    }

[domain_realm]
    virtualix.local = VIRTUALIX.LOCAL
    .virtualix.local = VIRTUALIX.LOCAL

```

D'ores et déjà vous pouvez obtenir votre "ticket" (Kerberos fonctionne ainsi en lieu et place d'un échange de mots de passe) pour un utilisateur présent dans la base Active Directory du serveur. Voici mon exemple pour un utilisateur nommé **filochard** :

```
root@desktop:~# kinit filochard@VIRTUALIX.LOCAL
Password for filochard@VIRTUALIX.LOCAL:
root@desktop:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: filochard@VIRTUALIX.LOCAL

Valid starting    Expires          Service principal
06/30/08 16:57:25 07/01/08 02:57:26  krbtgt/VIRTUALIX.LOCAL@VIRTUALIX.LOCAL
                renew until 07/01/08 16:57:25

Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
root@desktop:~# █
```

La commande `klist` montre les tickets obtenus et en cours.

La démarche suivante concerne l'authentification en utilisant les paquetages `winbind` et `SAMBA` (LE logiciel d'intégration des plates-formes Linux/WINDOWS) :

`aptitude install winbind samba`

La configuration du (long) fichier `SAMBA` diffère de celle d'un serveur :

Fichier `/etc/samba/smb.conf`

```
[global]
security = ads
realm = VIRTUALIX.LOCAL
password server = 192.168.3.101
workgroup = VIRTUALIX
encrypt passwords = true
domain master = no
local master = no
winbind use default domain = yes
idmap uid = 10000-20000
idmap gid = 10000-20000
template shell = /bin/bash
template homedir = /home/%D/%U
winbind enum groups = yes
winbind enum users = yes
client use spnego = yes
client ntlmv2 auth = yes
```

Il faut ensuite relancer, dans l'ordre, les services :

`/etc/init.d/samba restart`

`/etc/init.d/winbind restart`

Le domaine Active Directory est désormais joignable pour l'utilisateur. Vous validez la demande de mot de passe à blanc car vous disposez du ticket correspondant :

```
root@desktop:/etc/samba# net ads join
Password:
Using short domain name -- VIRTUALIX
DNS update failed!
Joined 'DESKTOP' to realm 'VIRTUALIX.LOCAL'
root@desktop:/etc/samba# █
```

Et PAM dans tout ça ?

De la même façon pour une connexion utilisateur, vous modifiez le fichier `/etc/nsswitch.conf`, cette fois pour

winbind au lieu de ldap :

```
passwd:      compat winbind
group:       compat winbind
...
```

La commande `getent group`, par exemple, retourne alors les groupes de la machine locale et ceux du serveur Active Directory :

```
haldaemon:x:123:
max:x:1000:
winbindd_priv:x:124:
smbashare:x:125:max
ordinateurs du domaine:x:10002:
contrôleurs de domaine:x:10003:
administrateurs du schéma:x:10004:administrateur
administrateurs de l'entreprise:x:10005:administrateur
admins du domaine:x:10006:administrateur
utilise. du domaine:x:10000:
invités du domaine:x:10001:
propriétaires créateurs de la stratégie de groupe:x:10007:administrateur
dnsupdateproxy:x:10008:
root@desktop:/etc/samba#
```



En cas de non-fonctionnement, n'hésitez pas à relancez les services `samba` et `winbind`.

Suivant la même procédure vue plus haut, remplacez `pam_ldap.so` par `pam_winbind.so` dans les fichiers `common-*` là où il y est fait référence. La recherche des utilisateurs et des groupes se fait par la commande `wbinfo` :

```
root@desktop:~# wbinfo -u
administrateur
invité
krbtgt
filochard
root@desktop:~# wbinfo -g
ordinateurs du domaine
contrôleurs de domaine
administrateurs du schéma
administrateurs de l'entreprise
admins du domaine
utilise. du domaine
invités du domaine
propriétaires créateurs de la stratégie de groupe
dnsupdateproxy
root@desktop:~#
```

La connexion à l'utilisateur `filochard` est possible par la commande `login` :


```

root@desktop:~# login filochard
Password:
Dernière connexion : lundi 30 juin 2008 à 18:40:46 CEST sur pts/0
Linux desktop 2.6.24-19-generic #1 SMP Wed Jun 18 14:43:41 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
filochard@desktop:~$ pwd
/home/VIRTUALIX/filochard
filochard@desktop:~$

```

Comme GDM utilise les modules inclus, la connexion par l'interface graphique est tout à fait possible.



La même remarque vue pour LDAP s'impose avec Active Directory : le montage du profil et de son répertoire utilisateur à la connexion passe par le module `pam_mount`. Sa mise en œuvre est de l'ordre de l'administration réseau.

3. Plus de sécurité avec PAM

a. Restriction horaire

L'administrateur système applique la politique de sécurité de l'entreprise. Elle porte notamment sur la restriction d'accès des utilisateurs. Dans le cadre normal d'une utilisation des comptes, on peut envisager naturellement la non-possibilité de connexion des utilisateurs en dehors des heures de bureau et donc l'usurpation éventuelle d'un compte. PAM dispose d'un module `pam_time` pour cela, couplé avec l'utilitaire `cron`.

La modification du fichier `/etc/pam.d/gdm` ne suffit pas car elle n'interdira pas une connexion à partir d'une console en mode texte. Par le biais des inclusions la place de `pam_time` se situe dans le fichier `common-account`.

Ajoutez cette ligne à la fin du fichier `/etc/pam.d/common-account` :

```
account required      pam_time.so
```

La modification suivante passe par le fichier `/etc/security/time.conf`. Le fichier contient des explications en commentaires très claires sur le format d'une entrée. Dans notre exemple, nous ne voulons autoriser que la période entre 08h00 et 20h00 à tous les utilisateurs et du lundi au vendredi :

```
login;*;*;Wk0800-2000
```

Le premier champ traitant du service `login`, une mesure de sécurité plus sévère aurait été de mettre une étoile (willcard) afin d'interdire tous les services, comme `ssh` par exemple.

Cas d'une connexion non fermée

Tout le monde ne quitte pas proprement sa session de travail : il arrive fréquemment que le poste reste en l'état au départ de l'employé. Aussi, un mécanisme de déconnexion doit être couplé à cette mesure de sécurité (et d'économie en électricité). La mise en place de l'arrêt du poste se fait par `cron` (voir le chapitre Maintenance de base).

b. Mots de passe renforcés

Longtemps considérée comme accessoire, la politique des mots de passe a été le parent pauvre de la sécurité, partant du faux principe - surtout sur Linux/Unix - que le système est difficilement inviolable à partir du moment où l'administrateur gère et surveille les comptes des utilisateurs.

Même si les dégâts d'un piratage restent circonscrit à un compte utilisateur par le biais de la suppression du compte

administrateur et de la gestion des droits par profils, la perte de donnée (ou le vol) pour un utilisateur n'est pas acceptable. La politique à mettre en place pour les mots de passe consiste en quelques règles :

- forcer le changement à intervalle régulier,
- augmenter la complexité et la longueur,
- garder un historique dans le but d'éviter une réutilisation.

C'est le but du module PAM `libpam-cracklib`, non installé par défaut (il devrait pourtant l'être) :

```
aptitude install libpam-cracklib
```

Le fichier `/etc/pam.d/common-password` donne en exemple les deux lignes essentielles à mettre pour positionner un renforcement de la sécurité avec `pam_cracklib.so` :

```
password required pam_cracklib.so retry=3 minlen=6 difok=3
password required pam_unix.so use_authok nullok md5
```

La première ligne

Les options du module `pam_cracklib` s'expliquent de la façon suivante :

- **retry=3** : trois essais possibles avant une relance du programme `passwd`. Cette option est facultative car la demande de connexion n'étant pas bloquée, rien n'empêche l'utilisateur de recommencer.
- **minlen=6** : impose un nombre minimum de caractères pour la longueur d'un mot de passe.
- **difok=3** : impose un nombre minimum de caractères différents lors d'un changement de mot de passe.

Par défaut, `pam_cracklib` vérifie si le mot de passe se base trop sur un mot courant ou si certains caractères se retrouvent trop souvent (en liaison aussi avec le paramètre `difok`). Attention toutefois, il arrive que le programme accepte certains mots en se trompant avec des mots d'écriture identique suivant les langues anglaise et française.

Les options supplémentaires `dcredit`, `ucredit`, `lcredit` et `ocredit` expriment respectivement l'obligation de lettres en minuscules, majuscules, chiffres et autres caractères alphanumériques.

La deuxième ligne

Les options de la deuxième ligne montrent l'utilisation du codage classique MD5, `use_authok` indiquant au module `pam_unix` de ne pas utiliser ses propres contrôles (rôle dédié à `pam_cracklib`) et `nullok` d'autoriser (contradiction évidente) les mots de passe vides !

Au niveau de ce module, l'option `remember` sauvegarde un nombre d'anciens mots de passe (et interdit la réutilisation) dans le fichier `/etc/security/opasswd` uniquement accessible à l'administrateur.

Un résultat possible

En fonction de ces remarques, vous pouvez modifier plus clairement ces deux lignes en ceci :

```
password required pam_cracklib.so retry=3 minlen=8 difok=3 ucredit=2
password required pam_unix.so use_authok md5 remember=24
```



N'oubliez pas que la durée de vie d'un mot de passe se règle dans le fichier `/etc/login.defs` au niveau de la variable `PASS_MAX_DAYS`.

Politique d'accès

Différents comportements du système s'ajustent en modifiant des paramètres pris en compte par le noyau. On classe ces comportements dans deux catégories : les ajustements relatifs à la sécurité et ceux relatifs à l'ajout de fonctionnalités.

IPv6, protocole Internet adopté comme standard par l'IETF (*Internet Engineering Task Force*), bien que lancé en 1990 n'est qu'imparfaitement intégré sur le réseau des réseaux entraînant parfois des problèmes d'implantation. Même si certains fournisseurs d'accès comme Free commencent à proposer l'activation d'IPv6, la gestion de ce protocole ne sera pris en compte que dans la prochaine version de ce manuel. Le pare-feu d'Ubuntu **ufw**, désactive d'ailleurs par défaut ce protocole.

1. Réglages essentiels

a. Désactivation/Activation d'IPv6

La méthode consistant à supprimer l'alias dans le fichier `/etc/modprobe.d/aliases` est à proscrire pour deux raisons : d'abord parce que le commentaire en tête du fichier l'indique (!) et ensuite parce qu'une modification induira des problèmes lors d'une mise à jour via le paquetage `module-init-tools`. Il faut lui préférer la méthode de la liste noire et, avec Ubuntu, la création de son propre fichier `blacklist` :

Fichier `/etc/modprobe.d/blacklist-admin` :

```
blacklist ipv6
```

Un dernier réglage porte sur le fichier `/etc/hosts` où il ne doit pas rester de lignes concernant Ipv6 : le mieux étant de les mettre en commentaire (on peut en avoir besoin lors d'un rétablissement de la configuration) :

```
# 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
```

b. Fichier `sysctl.conf` et routage

Le fichier `/etc/sysctl.conf` constitue le "pendant" de la commande `sysctl` et traite des ajustements systèmes pour modifier des paramètres du noyau. Concrètement pour modifier "à la volée", c'est-à-dire lorsque le système est en fonctionnement et jusqu'à un prochain redémarrage, on peut :

- soit utiliser la commande `sysctl` ;
- soit écrire directement dans les variables fichiers du répertoire `/proc`.

Le fichier `/etc/sysctl.conf` est utilisé pour prendre en compte ces changements au démarrage du système. Vous trouverez ci-dessous, une sélection de variables à gérer, généralement utiles pour l'administrateur d'un système.

Transformation du système en routeur

Sur une machine de type Ubuntu Linux, on parlera de routage logiciel pour la commutation de paquets entre réseaux différents, d'un port d'entrée vers un port de sortie (nombre d'interfaces réseau minimum : 2). Comme il est préférable de garder la main sur la fonctionnalité afin de pouvoir l'interrompre le cas échéant, on utilise l'écriture directe dans la variable, voire à l'intérieur d'un script gérant les règles d'un pare-feu.

```
sysctl net.ipv4.ip_forward
```

Ou (ipv6 comme ipv4) :

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



La commande `sysctl -a` affiche l'ensemble des paramètres passés au noyau.

Ajustements liés à la sécurité réseau

Tous les réglages suivants s'inscrivent dans le fichier `/etc/sysctl.conf` afin de protéger le système au démarrage.

Protection contre les attaques de type spoofing

Ce réglage protège contre les arrivées de paquets provenant d'une source usurpée. Pour l'interface de `loopback`, le bouclage attendu interdit une source autre qu'elle-même. Sur un système à plusieurs interfaces cela revient à vérifier la cohérence entre les interfaces et la table de routage.

Sur Ubuntu, ce réglage est activé par défaut (mettez des espaces entre le signe égal pour avoir la coloration syntaxique de VIM).

```
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
```

Protection contre les attaques de type syn flooding

Ce réglage active un numéro de séquence destiné à rendre non nécessaire la sauvegarde du SYN initial dans la séquence `three-way handshake` pour une connexion TCP. Afin d'éviter trop de connexions ouvertes et donc un déni de service, Ubuntu gère une liste (*backlog*) d'une longueur de 1024 (voir le contenu pour cela de `/proc/sys/net/ipv4/tcp_max_syn_backlog`).

Activer les `syncookies` permet de protéger au mieux la surcharge d'un serveur :

```
net.ipv4.tcp_syncookies = 1
```

Redirection ICMP

L'utilisation de la redirection ICMP pour informer d'une route plus adaptée est inutile si votre réseau est bien configuré. Cela peut même s'avérer dangereux par le biais d'injection de routes dans la table de routage. Les trois variables (en commentaire) sur Ubuntu sont positionnées par défaut (faire un `sysctl -a | grep redirects`) à 1 pour l'acceptation, 1 pour l'émission et 1 pour la redirection via une passerelle par défaut reconnue. Pour un routeur, seule l'émission garde la position booléenne à "vrai".

```
net/ipv4/conf/all/accept_redirects = 0
net/ipv4/conf/all/secure_redirects = 0
net/ipv4/conf/all/send_redirects = 1
```



Vous ne devez pas interdire les PING : d'abord, parce que cela va à l'encontre de la RFC 792, ensuite parce que cela ne sert maintenant à rien, si ce n'est qu'à satisfaire une tendance paranoïaque...

Surveiller les "martiens"

Cette appellation fantaisiste dénomme les paquets sur le réseau ayant des adresses sources/destination invalides. Mettre la valeur permet d'inscrire dans les logs ces paquets :

```
net/ipv4/conf/all/log_martians = 1
```

Autres paramètres

Trois derniers paramètres en commentaire dans le fichier `sysctl.conf` restent en l'état par défaut (à ne pas changer donc) avec respectivement :

- ne pas autoriser la fonctionnalité du ping en broadcast soit sur l'ensemble des machines du réseau.
- ne pas autoriser l'enregistrement dans les logs des paquets ICMP mal formés.
- ne pas autoriser l'inscription de passerelles à l'intérieur d'un paquet IP.

```
net/ipv4/icmp_echo_ignore_broadcasts = 1
net/ipv4/icmp_ignore_bogus_error_responses = 1
net/ipv4/conf/all/accept_source_route = 0
```

2. Mise en place de règles de pare-feu

a. En ligne de commandes avec UFW

La gestion d'un pare-feu sous Ubuntu s'apparente à celle d'une distribution Linux traditionnelle avec l'utilisation de **Netfilter** (le module du noyau pour le filtrage des paquets IP) et **IPtables** (l'interface de configuration en ligne de commandes). Ayant toujours le souci de "démocratiser" leur distribution, ou tout au moins de la rendre plus accessible, les développeurs Ubuntu ont introduit une nouvelle interface plus agréable à utiliser : **UFW**. Dans l'esprit de l'ouvrage, vous n'aurez pas ici une thématique sur IPtables (vu et revu dans nombres de livres sur Linux) mais sur la spécificité Ubuntu avec l'utilisation de ce nouvel outil, UFW.

UFW ne veut pas dire Ubuntu Firewall mais *Uncomplicated Firewall* (le mot anglais n'est pas cette fois-ci un faux ami).

Le service UFW se met en place non pas par un démarrage par `/etc/init.d/ufw start` mais par la commande :

```
ufw enable
```

Cette commande positionne la valeur `ENABLED` à `yes` dans le fichier `/etc/ufw/ufw.conf` (il ne contient d'ailleurs que cette ligne). Le lancement manuel (ou au démarrage du système) facultatif sans cette valeur à `yes` indiquera un service non démarré (skipped).

On voit tout de suite son fonctionnement avec les règles mises en place à partir de l'ancienne interface IPtables (toujours opérationnelle) :

```
iptables -L
```

Ce qui donne en sortie (extrait) :

```
Chain INPUT (policy DROP)
target     prot opt source                destination
ufw-before-input  all  --  anywhere              anywhere
ufw-after-input   all  --  anywhere              anywhere

Chain FORWARD (policy DROP)
target     prot opt source                destination
ufw-before-forward all  --  anywhere              anywhere
ufw-after-forward all  --  anywhere              anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ufw-before-output all  --  anywhere              anywhere
ufw-after-output  all  --  anywhere              anywhere

Chain ufw-after-forward (1 references)
target     prot opt source                destination
LOG        all  --  anywhere              anywhere          limit: avg 3/min burst 10 LOG level war
ning prefix '[UFW BLOCK FORWARD]: '
RETURN     all  --  anywhere              anywhere

Chain ufw-after-input (1 references)
target     prot opt source                destination
RETURN     udp  --  anywhere              anywhere          udp dpt:netbios-ns
RETURN     udp  --  anywhere              anywhere          udp dpt:netbios-dgm
RETURN     tcp  --  anywhere              anywhere          tcp dpt:netbios-ssn
RETURN     tcp  --  anywhere              anywhere          tcp dpt:microsoft-ds
RETURN     udp  --  anywhere              anywhere          udp dpt:bootps
RETURN     udp  --  anywhere              anywhere          udp dpt:bootpc
LOG        all  --  anywhere              anywhere          limit: avg 3/min burst 10 LOG level war
ning prefix '[UFW BLOCK INPUT]: '
RETURN     all  --  anywhere              anywhere

Chain ufw-after-output (1 references)
target     prot opt source                destination
RETURN     all  --  anywhere              anywhere
:_
```

Il en ressort qu'UFW introduit les chaînes `ufw-before-*` et `ufw-after-*` dans les trois chaînes principales INPUT, OUTPUT et FORWARD (table filter ou table contenant les règles de filtrage des paquets en entrée ou en sortie dans la machine, et ceux routés d'une interface à l'autre).

Une sous-chaîne est aussi présente dans les trois : `ufw-user-*` et dans les nouvelles versions d'UFW, les chaînes `ufw-user-limit` et `ufw-user-limit-accept`.



Le fichier `sysctl.conf` pris en compte après l'établissement d'UFW est celui qui se trouve dans le répertoire `/etc/ufw` et non le fichier se trouvant dans `/etc`.

Fonctionnement d'UFW

L'établissement des règles par défaut fait que le système accepte tout sur l'interface de la boucle locale (*loopback*) et en sortie. En entrée, toujours en ACCEPT par défaut, la règle est configurable et n'accepte que quelques services (ICMP, udp). Les paquets jetés sont enregistrés (LOG) avec une limite.

Syntaxe générale (et complète) :

```
ufw allow|deny [proto <protocole>]
  [from <adresse> [port <port>]] [to <adresse> [port <port>]]
```

Exemple :

Une fois UFW lancé avec les règles par défaut, un ping venant d'une autre machine fonctionne mais pas d'autres services. Autrement dit, si vous avez par exemple un service Apache (WEB), il n'est plus accessible à partir d'autres postes. Il faut le rétablir :

```
ufw allow proto tcp from 192.168.3.1 to 192.168.3.134 port 80
```

Ce qui se traduit par : accepter pour le protocole TCP les demandes faites par la machine d'IP 192.168.3.1 pour 192.168.3.134 (IP du serveur WEB) sur le port 80.

Un exemple plus simple :

```
ufw allow ssh
```

Dans ce cas, la permission est donnée pour une connexion SSH à partir de n'importe quel poste externe. Voir le manuel en ligne d'UFW pour plus d'exemples. On aurait pu remplacer la commande par :

```
ufw allow to any port 22 from any
```

Ou :

```
ufw allow proto tcp to any port 22 from any
```

```
ufw allow proto udp to any port 22 from any
```

La vérification de ces règles se fait par la commande :

```
ufw status
```

Ce qui donne après les deux règles précédentes :

```
root@server:/etc# ufw status
Firewall loaded

To Action From
--
192.168.3.134 80:tcp ALLOW 192.168.3.1
22:tcp ALLOW Anywhere
22:udp ALLOW Anywhere

root@server:/etc#
```

Destruction d'une règle

La suppression d'une règle simple dans sa syntaxe de base, **nécessite de connaître la règle exacte précédemment utilisée** :

ufw delete allow|deny règle

L'outil graphique GUFw

Suite logique d'UFW, le développement d'un outil graphique sous GNOME permettant le paramétrage des règles autrement que par les lignes de commandes. Encore en développement, **GUFw** apparaît dans les dépôts de la version **8.10 Intrepid Ibex**. Pour l'instant, en environnement graphique, l'outil **FireStarter** (voir ci-dessous) remporte plus les suffrages de ceux qui désirent s'initier et établir un pare-feu sans trop de complications.

b. Par une interface graphique avec FireStarter

Dans le cas d'un poste de travail, le travail d'une équipe de développeurs (<http://www.fs-security.com/>) a abouti au projet **FireStarter** en OpenSource.

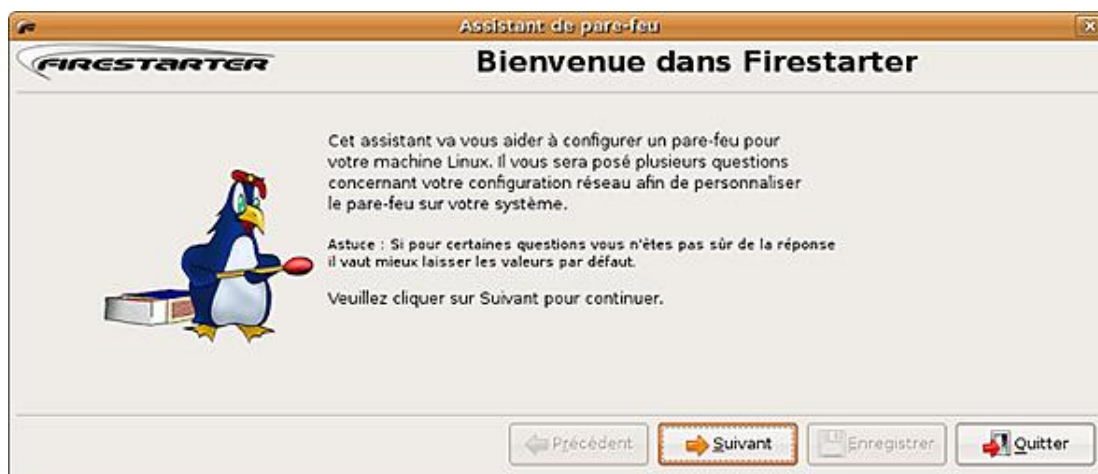
L'établissement de règles de pare-feu se fait par une interface graphique (Gnome sous GTK) et d'un assistant pour la configuration d'un pare-feu, ce qui en facilite considérablement la mise en place. Ses principales qualités :

- Utilisable pour les postes de travail ou une passerelle.
- Gestion en temps réel des événements comme les tentatives d'intrusion.
- Offre le partage de connexion Internet (plus le service DHCP si besoin).
- Gestion des ports simple, en entrée comme en sortie.
- Gestion de listes noires et/ou blanches pour les flux.
- Protection contre les attaques de type flooding, broadcasting, spoofing, DoS...
- Possibilité d'écrire des scripts utilisateur (*rulesets*) avant ou après activation du pare-feu.

Disponible sous Ubuntu dans le dépôt Universe, l'application s'installe classiquement et se trouve, une fois chargée, dans le menu **Système - Administration - FireStarter** (vous devez entrer le mot de passe d'administration bien sûr au lancement) :

```
aptitude install firestarter
```

Le premier lancement de l'application fait intervenir l'assistant de configuration :



c. Configuration

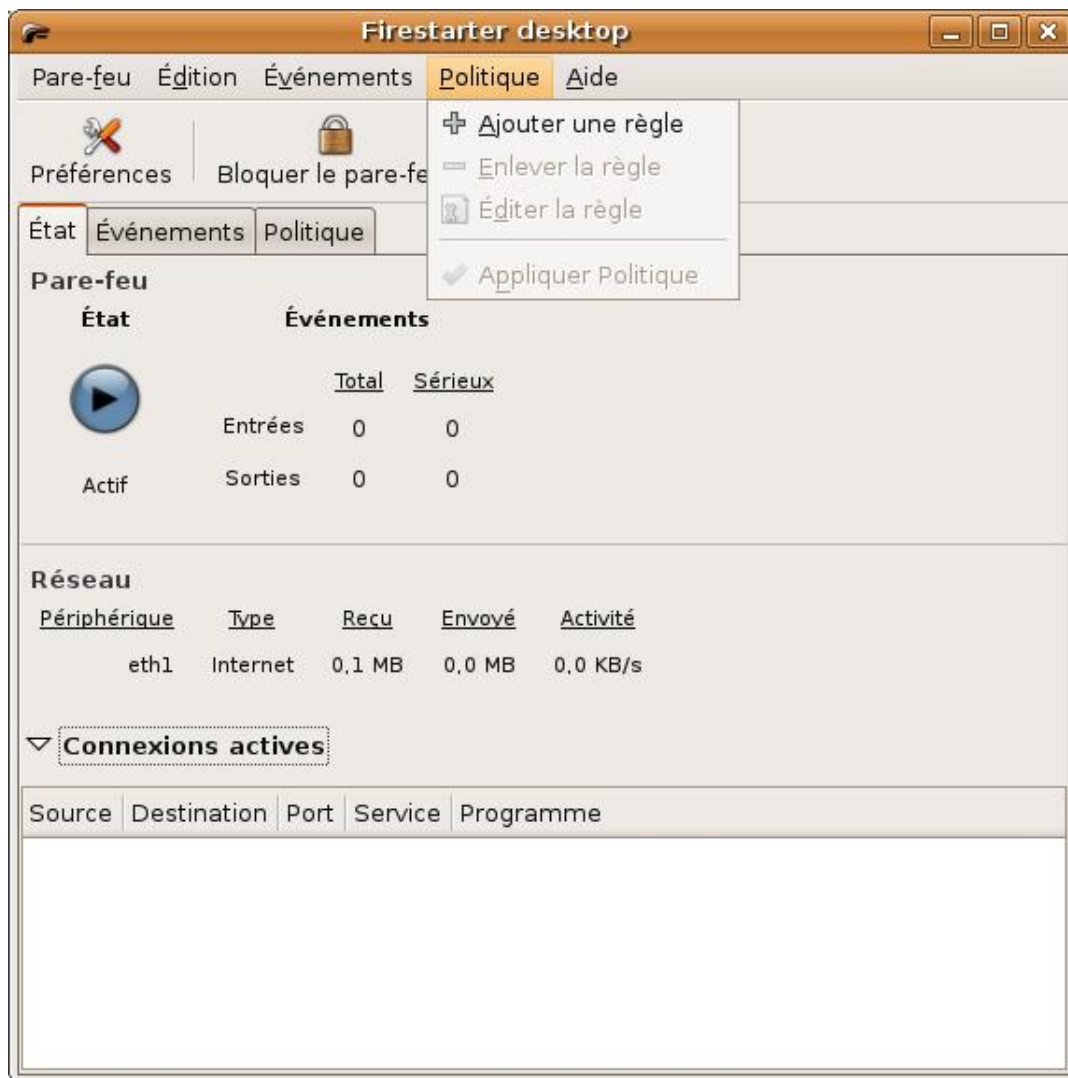
Les étapes de configuration concernent :

- **La configuration des périphériques réseaux.** Vous vérifiez la bonne détection de la carte et cochez le

lancement du pare-feu à la connexion. Indiquez aussi si l'adresse IP est donnée par DHCP (acceptable dans le cas d'un poste de travail au lieu d'une IP fixe).

- **L'autorisation du partage de la connexion Internet.** Cela revient à définir la translation d'adresses (NAT) et à s'appuyer sur un serveur DHCP. Deux remarques importantes : ce dernier **n'est pas installé par défaut** avec FireStarter, vous devez le faire en utilisant le paquet logiciel `dhcp3-server` ; enfin la translation d'adresses est possible si vous avez deux interfaces réseau.
- **Le démarrage du pare-feu.** L'option est cochée par défaut, vous enregistrez les paramètres par l'appui du bouton de même nom, ce qui fait quitter l'assistant. Le menu **Pare-feu - Lancer l'assistant** relance l'assistant.

L'écran de **FireStarter** montre l'état du pare-feu et d'autres renseignements comme les événements, les connexions actives, etc. L'un des menus les plus importants traite de la politique et des règles à ajouter :

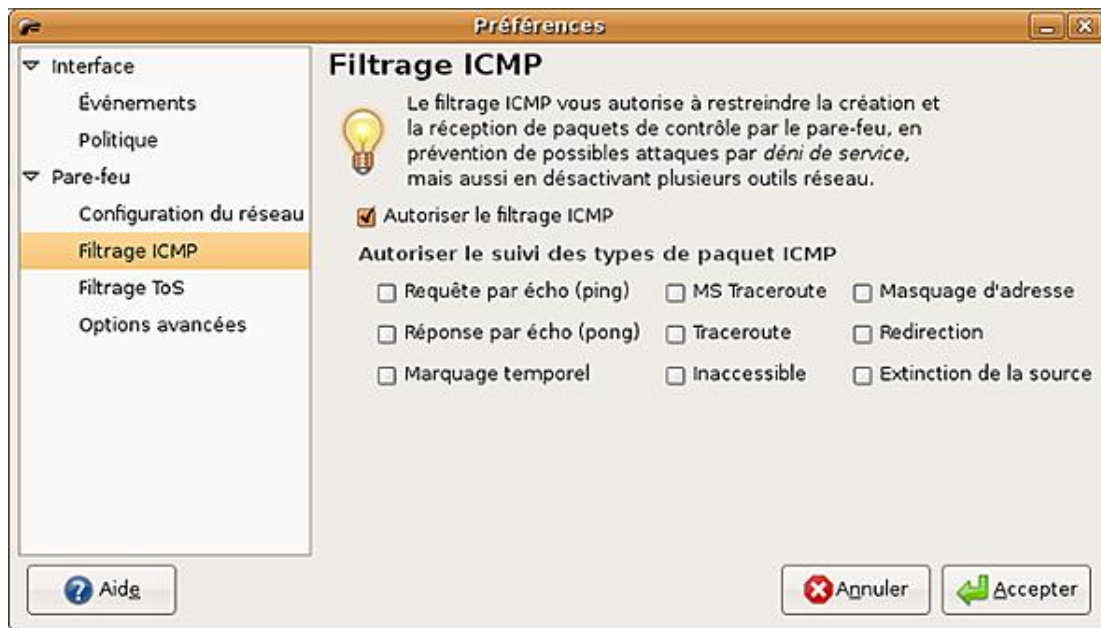


Vous pouvez par ce menu, ajouter une politique sur le trafic entrant et/ou sortant, en fonction ou non d'un service (clic droit de la souris pour faire apparaître le menu conceptuel à partir de l'onglet **Politique** et dans la zone choisie), suivant des permissions par rapport à la liste noire et/ou blanche.



Attention : certaines options ne sont disponibles et visibles qu'en cas de partage de la connexion Internet.

Vous vous reporterez avec profit à la documentation de **FireStarter** et à son manuel en ligne. Concernant les blocages de base vus dans le premier paragraphe, leur configuration se situe au niveau du menu **Édition - Préférences**. Par exemple, vous trouverez sur la ligne Filtrage ICMP le suivi des types de paquets :



Dès lors, le filtrage mis en place provoque des événements (réglez les colonnes visibles dans le menu **Événements - Montrer la colonne**).

Corrections des entraînements

1. Chapitre Gestion des droits utilisateurs

Réponses

- Vérifiez l'endroit où vous êtes, votre identité de compte avec notamment l'UID et le GID par la commande `id`.

`pwd`

`id`

- Quelles sont les permissions en octal de votre répertoire personnel ? et celles du répertoire parent ?

`755 (drwxr-xr-x)` visible par `ls -al /root`

même chose

- À quel groupe appartenez-vous ?

`root` (le `GID`)

- Créez un fichier par la commande `touch liste.sh`.

Pas de correction nécessaire...

- À qui appartient-il ? À quel groupe ?

au `root`, groupe `root` (`ls -l`)

- Quels sont les droits de ce fichier en octal ?

`644 (rw-r--r--)`

- Ajoutez le droit en écriture pour le groupe par la méthode octale.

`chmod 664 liste.sh`

- Enlevez le droit en écriture pour le groupe par la méthode symbolique.

`chmod g-w liste.sh`

- Le fichier `liste.sh` contiendra des commandes shell. Aussi, donnez-lui les permissions que l'on donne généralement à un programme, c'est-à-dire `755` et vérifiez-le.

`chmod 755 liste.sh` ou `chmod ugo+x liste.sh`

2. Chapitre Session de travail en mode console

- Tapez la commande permettant de voir dans quel répertoire vous êtes.

`pwd` (dans `/root`)

- Listez normalement le contenu de votre répertoire.

`ls`

- Listez le contenu du répertoire avec les fichiers cachés et le format long.

`ls -al`

- Utilisez le manuel en ligne pour connaître et comprendre la commande `sleep`.

`man sleep`

- Tapez maintenant `sleep --help`, quelle en est l'utilité ?

donne une aide plus concise

- Si vous tapez `sleep 360`, quelle combinaison de touches permet de l'interrompre ? Testez-la

`[Ctrl] c`

- Quelle est la taille du répertoire `/usr` ?

`du -hs /usr`

- Allez dans le répertoire `/etc` par le chemin absolu.

`cd /etc`

- Faites un tube avec d'un côté la commande `ls *.conf`, de l'autre `wc -l`, quel en est le résultat ?

`ls *.conf | wc -l` (donne 22 fichiers sur mon serveur)

- Tapez tout simplement `cd` et validez. Que s'est-il passé ? Et que signifie le tilde (`~`) ?

L'utilisateur se retrouve dans son répertoire, le tilde indique son espace personnel.

- Allez dans votre répertoire et créez deux sous-répertoires : `hobbit` et `elfe`, vérifiez la création par la commande appropriée.

`mkdir hobbit elfe`

- Allez dans `hobbit` et créez trois fichiers `merry`, `pipin` et `gollum` par la commande `touch`.

`cd hobbit`

`touch merry pipin gollum`

- Sans changer de répertoire créez le sous-répertoire `elfedesbois` dans `elfe` et par le chemin relatif.

`mkdir ../elfe/elfedesbois`

- Sans changer de répertoire, créez le fichier `legolas` dans votre répertoire personnel et par le chemin absolu.

`touch /root/legolas`

- Allez dans `elfedesbois` obligatoirement en trois commandes (niveau par niveau).

`cd ..`

`cd elfe/`

`cd elfedesbois/`

- Sans changer de répertoire, déplacez `legolas` pour le mettre là où vous êtes et par le chemin relatif.

```
mv ../../legolas .
```

- Sans changer de répertoire renommez `gollum` en `sam` par le chemin absolu.

```
mv /root/hobbit/gollum /root/hobbit/sam
```

- Trouvez, par la commande `find`, le fichier `interfaces` à partir de `/etc`.

```
find /etc -name interfaces
```

- Retournez dans votre répertoire et créez le fichier `riri.txt`.

```
cd
```

```
touch riri.txt
```

- Dupliquez-le par la commande `cp` en changeant son nom en `fifi.txt`.

```
cp riri.txt fifi.txt
```

- Créez un lien par `ln` en changeant son nom en `loulou.txt`.

```
ln riri.txt loulou.txt
```

- Éditez les inodes par `ls` et l'option adéquate et concluez.

```
ls -i
```

et les inodes de `riri.txt` et `loulou.txt` sont identiques.

- Par VIM, mettez une phrase dans `riri.txt`.

Pas de correction nécessaire...

- Éditez `fifi.txt` et `loulou.txt` ; concluez

Le contenu est le même car ce sont en fait les mêmes fichiers.

- Effacez `riri.txt`, que s'est-il passé pour `fifi.txt` ?

Rien pour `fifi.txt` mais le nombre de lien de `loulou.txt` est passé de 2 à 1.

- Quel est le type du fichier `/etc/passwd` ?

```
file /etc/passwd
```

ce qui donne le type ASCII text.

3. Chapitre Maintenance avancée du système

Exercices - Partie 1

- Affichez les lignes contenant la chaîne `ar`.

```
grep -n 'ar' test1.txt (1, 3, 4, 5, 6, 7, 9, 10)
```

- Affichez les lignes dont au moins une chaîne contient au minimum 3 j consécutifs.

```
grep -n '[j]\{3,\}' test1.txt (15)
```

- Affichez les lignes ayant au moins une chaîne se terminant par age.

```
grep -n 'age\>' test1.txt (11, 12, 13, 14, 15)
```

- Affichez les lignes ayant au moins une chaîne se terminant par guage ou gage.

```
grep -n 'g[u]*age\>' test1.txt (11, 12, 13, 14, 15)
```

- Affichez les lignes (pas les mots) se terminant par age ou ava.

```
grep -n 'age$\|ava$' test1.txt (11, 12, 13, 14)
```

- Affichez les lignes vides.

```
grep -n '^$' test1.txt (2, attention aux caractères invisibles)
```

- Affichez les lignes contenant les sous-chaînes 35 ET ans (vous ferez un "tube").

```
grep -n 'age$\|ava$' test1.txt (11, 12, 13, 14)
```

- Affichez les lignes ne commençant pas par un chiffre.

```
grep -n "^[^0-9]" test1.txt (toutes sauf la 2, 16, 17, 18, 22)
```

- Affichez les lignes ne contenant que des chiffres.

```
grep -n '^[0-9]$_' test1.txt (aucune, l'espace est  
considéré comme un caractère)
```

- Affichez les lignes commençant par une voyelle ou un chiffre.

```
grep -n '^[aeiouy]\|^[0-9]' test1.txt (7, 16, 17, 18, 22)
```

- Affichez les lignes ne se terminant pas par un chiffre.

```
grep -n '^[^0-9]$_' test1.txt (toutes sauf la 2, 6, 16, 18, 22)
```

- Affichez les lignes faisant moins de 10 caractères.

```
grep -n '^\.{1,10}$' test1.txt (1, 4, 5, 7, 8, 9, 10,  
11, 12, 13, 14, 18, 22)
```

Exercices - Partie 2

- Affichez à l'écran par cat le contenu du fichier.

```
cat test2.txt
```

- Quel est le nombre de mots, de lignes et de caractères de test2.txt ?

```
wc -wlc test2.txt
```

- Combien de lignes contient ce fichier ?

```
wc -l test2.txt
```

- Affichez à l'écran le deuxième champ de toutes les lignes.

```
cut -f2 -d: test2.txt
```

- Quel est le nombre de canards ?

```
grep 'canard' test2.txt | wc -l
```

- Envoyez le fichier test2.txt avec uniquement le premier champs de toutes les lignes dans un fichier noms.txt.

```
cut -f1 -d: test2.txt > noms.txt
```

- Triez le fichier noms.txt par ordre alphabétique.

```
sort -o noms.txt noms.txt
```

- Coupez le fichier test2.txt en **deux fichiers** test2aa et test2ab (voir l'option nécessaire dans le manuel en ligne).

```
split -l 4 test2.txt test2
```

- Réunissez-les dans un fichier disney.txt.

```
paste test2aa test2ab > disney.txt
```

Services courants de la distribution Ubuntu

(Version Hardy Heron 8.04)

Nom du service	Description
acpi-support	Script utilisé par acpid
acpid	Gestion de l'énergie
alsa-utils	Gestion des paramètres audio
anacron	Planificateur d'évènements
apmd	Gestion de l'énergie (plus ancien)
apparmor	Confinement d'un programme dans un profil de sécurité limité en ressources
apport	Support de rapports automatiques de défaillance
atd	Planificateur de tâches
avahi-daemon	Découverte de service DNS multicast
bluetooth	Gestion des périphériques bluetooth
bootclean	Script de nettoyage
bootlogd	Service d'enregistrement des messages au boot
bootmisc.sh	Script de lancement de programmes au démarrage
brltty	Gestion d'affichage en braille
checkfs.sh	Script de vérification des systèmes de fichiers au démarrage
checkroot.sh	Script de vérification du système de fichiers racine au démarrage
console-screen.sh	Script définissant des paramètres spécifiques pour la console
console-setup	Service de gestion spécifique de la police et du clavier en mode console
cron	Utilitaire d'exécution de tâches périodiques
cryptdisks	Script de setup pour le cryptage des périphériques de bloc
cryptdisks-early	Script de mise en place du cryptage des périphériques de bloc
cupsys	Service pour l'impression
dbus	Bus de communication système
dhcdd	Contrôle D-Bus pour le client DHCP

dirmngr	Service de gestion et de chargement des listes de révocation de certificats (CRLs)
dns-clean	Script de nettoyage au démarrage des messages laissé par 0dns-up
gdm	Gestionnaire de connexion graphique Gnome
glibc.sh	Script vérifiant les versions des bibliothèques C par rapport au noyau
hal	Service maintenant en permanence une liste des ressources connectées
halt	Script plus complet pour la commande halt
hostname.sh	Script positionnant le nom de machine au lieu de le faire directement
hotkey-setup	Gestion des touches spéciales
hwclock.sh	Script pour l'ajustement de l'heure CMOS (matérielle) à l'heure système
hwclockfirst.sh	Identique au précédent, avec une variante de préférence
kdm	Gestionnaire de connexion graphique KDE
keyboard-setup	Script préliminaire de gestion du clavier
killprocs	Script utilisé par le processus init afin de basculer en mode single
klogd	Enregistreur d'activité
laptop-mode	Script de mise en place d'utilitaires pour un ordinateur portable
linux-restricted-modules-common	Script de préparation pour les pilotes sous licence restreinte
lisa	Service simple de mise en place d'un voisinage réseau via TCP/IP
loopback	Script de mise en place de l'interface de la boucle locale
module-init-tools	Utilitaires d'initialisation des modules listés dans /etc/modules
mountall-bootclean.sh	Script nettoyant les systèmes de fichiers temporaires après un mountall
mountall.sh	Script montant tous les systèmes de fichiers locaux dans /etc/fstab
mountdevsubfs.sh	Script montant les systèmes de fichiers spéciaux
mountkernfs.sh	Script montant un noyau pour les systèmes de fichiers virtuels

mountnfs-bootclean.sh	Script identique à mountall-bootclean mais pour NFS
mountoverflowtmp	Script pour le montage tmpfs sur /tmp en cas de problème d'espace disque lors d'une connexion
mtab.sh	Script de mise à jour du fichier mtab en cas de systèmes de fichiers virtuels
networking	Service de configuration des interfaces réseaux
nvidia-kernel	Noyau spécifique pour les cartes graphiques NVidia
pcmciautils	Ensemble d'utilitaires pour les cartes de type PCMCIA
policykit	Gestion centralisée des polices de caractères
postfix	Service de messagerie (MUA)
powernowd	Gestionnaire de la fréquence et voltage du CPU
powernowd.early	Script de préparation du script précédent
pppd-dns	Script de restauration du fichier de résolution DNS resolv.conf en cas de crash
procps	Script de positionnement d'options pour le noyau au démarrage
pulseaudio	Service de lancement du serveur de son pulseaudio
rc.local	Script de lancement des services personnalisés au démarrage
readahead	Service de chargement en mémoire des programmes de façon à accélérer les performances au démarrage
readahead-desktop	Identique au précédent mais pour la version poste de travail
reboot	Script de redémarrage
rmnologin	Service de nettoyage afin de permettre une connexion utilisateur après une perte brutale de session
rsync	Service de gestion synchronisée de sauvegarde de fichiers
screen-cleanup	Script de suppression d'écrans résiduels au démarrage
sendsigs	Service tuant tous les processus en vue de passer au niveau 0
single	Mode de récupération (runlevel 1)
stop-bootlogd	Script d'arrêt d'enregistrement des logs au démarrage
stop-bootlogd-single	Identique au précédent, mais pour le mode single
stop-readahead	Script d'arrêt du script readahead

sysklogd	Enregistreur d'activité
udev	Service dynamique de découverte et de nommage de périphériques
udev-finnish	Script de finalisation du lancement du service udev
ufw	Programme de gestion du pare-feu
umountfs	Script de démontage des systèmes de fichiers
umountnfs.sh	Identique au précédent, mais pour les systèmes de fichiers NFS
umountroot	Service de montage du système de fichiers principal (root) en lecture seulement
urandom	Fichier spécial de caractères pour la fourniture d'une interface avec le générateur de nombres aléatoires du noyau
usplash	Utilisation d'un écran graphique au démarrage et à l'arrêt du système
vbesave	Service de sauvegarde des états de la vidéo (mode hibernation)
waitnfs.sh	Script de temporisation pour le montage de système de fichiers NFS
wpa-ifupdown	Script de gestion du service de cryptage WPA (Wi-Fi)
x11-common	Infrastructure du système de fichiers, requise pour une autre installation du système graphique
xserver-xorg-input-wacom	Service de fourniture du pilote de périphérique Wacom (tablette avec stylet)