



Ressourcesinformatiques

UBUNTU

Administration d'un système Linux

5^e édition

Yann BARDOT
Luc DÉMARET



Avant-propos

Chapitre 1 Ubuntu et Linux

1. Affirmation du modèle open source	21
1.1 Principe et avenir du modèle	21
1.1.1 Open source et capitalisme financier	22
1.1.2 Open source et logiciel libre	23
1.2 Place de Linux dans le modèle	24
1.3 Principaux outils open source	26
2. Ubuntu : les raisons d'un succès	28
2.1 Point de départ	28
2.1.1 Les origines	28
2.1.2 Le fondateur d'Ubuntu : Mark Shuttleworth	29
2.2 Qualités de la distribution	30
2.2.1 Points forts de la distribution	31
2.2.2 Un mot sur la distribution pour les serveurs	31
2.2.3 Pourquoi adopter Ubuntu ?	32
3. Déclinaisons d'Ubuntu	33
3.1 Historique des versions supportées	34
3.2 Nouveautés de la version 18.04	35
3.3 Déclinaisons d'une même version	37
3.3.1 Suivant la destination	38
3.3.2 Suivant l'environnement graphique	40
3.3.3 Suivant les fonctionnalités	44
4. Administrateur système Ubuntu	46
4.1 Rôle de base	47
4.2 Missions étendues	48
5. Conventions typographiques	48
5.1 Terminologie anglaise	48
5.2 Exemples	49

5.3	Commandes et code	49
5.3.1	Présentation	49
5.3.2	Exécution	49
5.4	Touches du clavier	50

Chapitre 2

Prérequis à l'installation

1.	Essayer Ubuntu sans l'installer	51
1.1	Depuis Windows	51
1.1.1	Sur les anciennes versions	51
1.1.2	Dans une machine virtuelle	52
1.2	Depuis un LiveCD	62
2.	Le matériel	63
2.1	L'architecture	63
2.1.1	Cas classiques	63
2.1.2	Cas spéciaux	64
2.1.3	32 ou 64 bits ?	65
2.1.4	Accès Internet	65
2.2	Les besoins d'Ubuntu	65
2.2.1	Linux en général	65
2.2.2	Ubuntu Desktop	67
2.2.3	Ubuntu Server	67
2.2.4	Lubuntu	67
2.2.5	Xubuntu	67
2.2.6	Kubuntu	68
2.2.7	Edubuntu	68
2.3	Compatibilité du matériel	68
2.3.1	Vérifier son matériel	68
2.3.2	Listes de compatibilité matérielle	75

- 3. Les supports de stockage 76
 - 3.1 Trouver de la place 76
 - 3.1.1 Installer Ubuntu sur un disque inutilisé 77
 - 3.1.2 Repartitionner un disque 77
 - 3.2 Schéma de partitionnement. 83
 - 3.2.1 Nombre minimal de partitions. 83
 - 3.2.2 Séparation des données. 84
 - 3.2.3 Partitionnement d'un serveur 85
 - 3.2.4 Cas du swap. 85
 - 3.3 Choisir un système de fichiers. 86
 - 3.3.1 Le journal 87
 - 3.3.2 ext2fs 87
 - 3.3.3 ext3fs 88
 - 3.3.4 ext4fs 88
 - 3.3.5 btrfs 88
 - 3.3.6 Compatibilité avec Windows 89

Chapitre 3
Installation

- 1. Installation normale d'un poste de travail 91
 - 1.1 Préalable à l'installation 91
 - 1.2 Processus d'installation. 92
 - 1.2.1 Écran de bienvenue 92
 - 1.2.2 Disposition du clavier 94
 - 1.2.3 Type d'installation (paquets) 95
 - 1.2.4 Type d'installation (disque) 96
 - 1.2.5 Emplacement géographique 97
 - 1.2.6 Personnalisation et identité du Super Utilisateur 98
 - 1.2.7 Phase finale 100

2.	Installation d'un serveur avec Subiquity	101
2.1	Préalable à l'installation	101
2.2	Installation	102
2.2.1	Sélection de la langue	102
2.2.2	Sélection du clavier	103
2.2.3	Choix de la version	104
2.2.4	Configuration du réseau	105
2.2.5	Configuration du proxy	108
2.2.6	Configuration du système de fichiers	109
2.2.7	Configuration du profil	115
3.	Installation en mode expert d'un serveur	117
3.1	Préalable à l'installation	117
3.2	Première phase du processus d'installation	117
3.2.1	Sélection de la langue	117
3.2.2	Options de boot	118
3.3	Deuxième phase du menu d'installation	122
3.3.1	Choisir la langue	123
3.3.2	Configurer le clavier	124
3.3.3	Détecter et monter le CD	125
3.3.4	Charger un fichier de configuration	125
3.3.5	Charger des composants d'installation à partir du CD	126
3.4	Troisième phase du menu d'installation	127
3.4.1	Détecter le matériel réseau	127
3.4.2	Configurer le réseau	128
3.4.3	Créer les utilisateurs et choisir les mots de passe	129
3.4.4	Configurer l'horloge	130
3.4.5	Détecter les disques	130
3.4.6	Partitionner les disques	131
3.4.7	Installer le système de base	137
3.4.8	Configurer l'outil de gestion des paquets	139
3.4.9	Choisir et installer des logiciels	141
3.4.10	Installer le programme de démarrage GRUB sur un disque dur	143

- 3.4.11 Terminer l'installation. 143
- 4. Installations spécifiques 144
 - 4.1 Utilisation du LVM 144
 - 4.1.1 Principe. 144
 - 4.1.2 Installation avec LVM. 146
 - 4.2 Utilisation du RAID logiciel. 149
 - 4.2.1 Principe. 149
 - 4.2.2 Installation avec RAID 150

Chapitre 4
Prise en main de la distribution

- 1. Présentation de l'interface graphique 159
 - 1.1 L'écran de connexion 159
 - 1.2 L'environnement 161
- 2. Présentation des menus et outils 163
 - 2.1 Menus 163
 - 2.2 Applications 168
- 3. Raccourcis-clavier 178

Chapitre 5
Utiliser la ligne de commandes

- 1. Le shell 181
 - 1.1 Rôle 181
 - 1.2 Le shell et l'administrateur 184
 - 1.3 Bash : le shell par défaut. 184
 - 1.4 Utiliser le shell 185
 - 1.4.1 Pour débiter. 185
 - 1.4.2 Syntaxe générale 185
 - 1.4.3 Aide. 186
 - 1.4.4 Exemple avec cal 186
 - 1.4.5 Chaîner les commandes 188

1.4.6	Grouper les commandes	189
1.4.7	Afficher du texte avec echo.	190
1.4.8	L'historique de commandes	190
2.	L'éditeur vi.	191
2.1	Fonctionnement	191
2.2	Commandes de base.	192
2.2.1	Saisie.	192
2.2.2	Sortie et sauvegarde.	192
2.2.3	Déplacement	193
2.2.4	Correction	193
2.2.5	Recherche simple.	194
2.2.6	Copier-coller.	194
2.2.7	Recherche et remplacement	195
2.2.8	Autres commandes	195
3.	Gestion des fichiers.	195
3.1	Système de fichiers FHS.	195
3.2	Types de fichiers.	198
3.3	Nomenclature des fichiers	199
3.4	Chemins	199
3.4.1	Représentation.	199
3.4.2	Se déplacer	200
3.5	Commandes de base.	200
3.5.1	Lister.	200
3.5.2	Créer des fichiers vides	202
3.5.3	Créer des répertoires	202
3.5.4	Supprimer des répertoires	202
3.5.5	Copier des fichiers	202
3.5.6	Déplacer et renommer un fichier	203
3.5.7	Supprimer un fichier ou une arborescence.	203
3.5.8	Liens symboliques	204
3.6	Caractères de substitution	205
3.7	Verrouillage de caractères.	205

4.	Recherche	206
4.1	Rechercher des fichiers	206
4.1.1	Critères de recherche	206
4.1.2	Commandes	207
4.2	Retrouver des exécutables	208
5.	Redirections	208
5.1	Les canaux	208
5.2	En sortie	209
5.3	En entrée	209
5.4	Jouer avec les canaux	210
6.	Quelques filtres et utilitaires	210
6.1	Les tubes ou pipes	210
6.2	Rechercher des lignes	211
6.3	Couper des champs	211
6.4	Compter les lignes	212
6.5	Trier	213
6.6	Supprimer les doublons	214
6.7	Découper et recoller un fichier	214
6.7.1	Découper	214
6.7.2	Recoller	215
6.8	Afficher du texte	215
6.8.1	En pleine page	215
6.8.2	Début d'un fichier	215
6.8.3	Fin et attente de fichier	216
6.9	Dupliquer le canal de sortie standard	216
6.10	Mettre un script en attente	217
7.	Variables	217
7.1	Nomenclature	217
7.2	Déclaration et affectation	217
7.3	Accès et affichage	217
7.4	Accolades	218
7.5	Variables système	219

7.6	Variables spéciales	220
8.	Effectuer des tests	220
8.1	Sur des chaînes	220
8.2	Sur des valeurs numériques	221
8.3	Sur les fichiers	221
8.4	Critères ET OU NON	222
9.	Processus	222
9.1	Lancer des programmes	222
9.2	Lister les processus	223
9.3	Arrêter un processus	225
10.	Divers	226
10.1	Calculs	226
10.2	Longueur d'une chaîne	226
10.3	Substitution de commande	227

Chapitre 6

Configuration du système

1.	Démarrage	229
1.1	Le chargeur de démarrage	229
1.2	GRUB2 remplace GRUB	230
1.3	Configuration de GRUB2	231
1.3.1	Fichier /etc/default/grub	231
1.3.2	Autres fichiers	233
1.3.3	Mise à jour de GRUB	233
1.3.4	Construction des menus	234
1.4	Démarrage et édition	236
1.5	Changement de l'image splash de GRUB	236
2.	Services au démarrage	237
2.1	Niveaux d'exécution	237
2.2	systemd en remplacement d'upstart	238
2.3	Utilitaires de gestion des services	240

2.3.1	Anciennes méthodes	240
2.3.2	sysv-rc-conf	241
2.3.3	initctl	241
2.3.4	systemctl	242
2.4	Actions sur un service	243
3.	Connexion au réseau	246
3.1	Nouvelle configuration	246
3.1.1	Fichier /etc/netplan/*.yam	246
3.1.2	Cas d'une connexion sans fil	248
3.2	Ancienne configuration	248
3.2.1	Fichier /etc/network/interfaces	248
3.2.2	Routes statiques et autres commandes	249
3.2.3	Cas d'une connexion sans fil	250
3.3	Commandes utiles pour le réseau	252
3.3.1	ping	252
3.3.2	ifconfig	252
3.3.3	ip	253
3.3.4	arp	254
3.3.5	route	254
3.4	Network Manager	255
4.	Les périphériques	259
4.1	Découverte des périphériques	259
4.1.1	Fichiers périphériques	259
4.1.2	Découverte dynamique	260
4.2	Fonctionnement d'udev	260
4.3	Principe d'une règle	262
4.4	Exemple des cartes réseau	264

Chapitre 7**Mise à jour du système**

1. Les dépôts de paquets logiciels.	265
1.1 Types de dépôts	265
1.2 Serveurs miroirs	266
1.3 Launchpad.	268
1.4 Remonter les problèmes.	269
1.5 Le fichier sources.list	269
1.5.1 Structure	269
1.5.2 Dépôts officiels	272
1.5.3 Backports	272
1.5.4 Dépôt partenaire ou commercial	273
1.5.5 Medibuntu	273
1.5.6 Les dépôts PPA.	273
1.6 Gestion des dépôts avec l'interface graphique	274
1.7 Cas d'un serveur mandataire	275
2. Principe des paquets	276
2.1 Interfaces de gestion de paquets	276
2.2 snap	278
2.3 Les gestionnaires graphiques	278
2.3.1 Logiciels Ubuntu	278
2.3.2 Gestionnaire de mises à jour.	279
2.3.3 Gestionnaire de paquets Synaptic	280
2.4 Les gestionnaires en mode console	282
2.4.1 Utilitaire dpkg	282
2.4.2 Utilitaire apt	283
2.4.3 Utilitaire aptitude	284
2.4.4 Utilitaire snap	287
2.4.5 Résumé de séquence de mise à jour d'un système.	287

- 2.5 Mise à niveau de la distribution 288
 - 2.5.1 Cas des versions LTS 288
 - 2.5.2 Notifications 289
 - 2.5.3 Canonical Livepatch 290
 - 2.5.4 Vers une version en développement. 293
 - 2.5.5 Vers une version finale 293

Chapitre 8

Découverte de l'environnement de travail

- 1. Xorg 295
 - 1.1 Présentation 295
 - 1.1.1 X Window 295
 - 1.1.2 Le gestionnaire de fenêtres 296
 - 1.1.3 Les widgets et les toolkits 297
 - 1.1.4 Wayland 298
 - 1.2 Installation et tests. 298
 - 1.2.1 Installer Xorg 298
 - 1.2.2 Installer un gestionnaire de fenêtres 299
 - 1.2.3 Installer un environnement de bureau. 301
 - 1.3 Configuration détaillée du serveur Xorg. 302
 - 1.3.1 Configuration manuelle par le fichier xorg.conf 302
 - 1.3.2 Utiliser la commande de configuration
dpkg-reconfigure 307
 - 1.3.3 Générer automatiquement un fichier xorg.conf 308
- 2. L'environnement de bureau 309
 - 2.1 Connexion avec GDM (Gnome Desktop Manager). 309
 - 2.1.1 Pourquoi remplacer LightDM par GDM ? 309
 - 2.1.2 Le gestionnaire de sessions 309
 - 2.1.3 Utiliser GDM. 309
 - 2.1.4 Le compte invité 312

2.2	Personnaliser GDM	313
2.2.1	Le fichier custom.conf	313
2.2.2	Tweaks	315
2.2.3	Changer l'environnement par défaut	317
2.2.4	Changer de gestionnaire de session	317
3.	Travailler avec d'autres environnements	318
3.1	Installer LXDE	319
3.2	Installer KDE	320
3.3	Installer XFCE	321

Chapitre 9

Les droits des utilisateurs

1.	Gérer les utilisateurs	323
1.1	Principe	323
1.1.1	Linux en général	323
1.1.2	Ubuntu en particulier	324
1.1.3	Rétablir le compte root	325
1.2	Les fichiers	326
1.2.1	/etc/passwd	326
1.2.2	/etc/group	328
1.2.3	/etc/shadow	328
1.2.4	/etc/gshadow	329
1.3	Ouverture de session	330
1.3.1	En mode console	330
1.3.2	En mode graphique	331
1.4	Gérer les utilisateurs	331
1.4.1	En mode console	331
1.4.2	En mode graphique	334
2.	Droits des utilisateurs	337
2.1	Utilisateurs et attributs de fichiers	337
2.1.1	Principes	337
2.1.2	Changement des attributs de fichiers	339

2.1.3	Le masque	340
2.1.4	Changement de propriétaire ou de groupe	342
2.1.5	Droits supplémentaires	342
2.2	Gérer les droits depuis l'interface graphique	344
2.2.1	Dossier personnel de l'utilisateur	344
2.2.2	Modification des droits	345
2.3	La commande sudo et PolKit	347
2.3.1	sudo	347
2.3.2	Tâches administratives avec PolKit	347
3.	Gestion avancée des utilisateurs	350
3.1	Sécurité des mots de passe	350
3.1.1	Changer de mot de passe	350
3.1.2	Gérer les informations de validité	351
3.2	Vérifier la cohérence des fichiers	353
3.3	Actions de l'utilisateur	354
3.3.1	Changer de shell	354
3.3.2	Changer le commentaire	354
3.3.3	Changer de groupe principal	355
3.3.4	Changer d'identité	355
3.4	Configuration avancée	356
3.4.1	/etc/default/useradd	356
3.4.2	/etc/login.defs	356
3.5	Notifications à l'utilisateur	357
3.5.1	/etc/issue	357
3.5.2	/etc/update-motd.d	358
3.6	Environnement utilisateur	359
3.6.1	/etc/skel	359
3.6.2	Scripts de configuration	359
4.	Exercices	360
4.1	Gestion des utilisateurs	360
4.2	Gestion des droits	361

Chapitre 10

Tâches d'administration

1. Surveillance et performances	363
1.1 Surveillance des processus	363
1.1.1 Les différents états d'un processus	363
1.1.2 La commande top	365
1.1.3 La charge moyenne	366
1.2 Les processeurs	367
1.2.1 La charge des processeurs	367
1.2.2 Surveillance de la charge CPU	367
1.3 La gestion de la mémoire	368
1.3.1 Voir l'état de la mémoire	368
1.3.2 Interpréter la consommation mémoire	369
1.3.3 Mémoire et architecture	370
1.3.4 L'OOM Killer	370
1.3.5 Interpréter le swap	371
1.4 Les performances des disques	372
1.4.1 Occupation	372
1.4.2 Surveillance de la charge	373
1.5 Surveillance globale	374
1.5.1 En direct	374
1.5.2 En différé	375
1.6 Autres commandes	376
1.6.1 La commande strace	376
1.6.2 La commande lsof	376
1.7 Surveillance depuis l'interface graphique	376
2. Surveillance avec les journaux	378
2.1 Consignation des événements	378
2.2 Archivage des fichiers journaux	381

3. Planification des tâches	382
3.1 cron	382
3.1.1 Fonctionnement de cron	382
3.1.2 Définir une crontable personnelle	383
3.2 anacron	385
3.3 at	386
4. Archivage et sauvegarde	387
4.1 Principes de la sauvegarde de données	387
4.2 Commandes et outils de sauvegarde	388
4.2.1 La commande tar (tape archiver)	388
4.2.2 La commande dd (device to device)	389
4.2.3 Les commandes dump et restore	390
5. Interventions sur le noyau	391
5.1 proc et sys	392
5.2 Paramètres dynamiques	393
5.3 Changer de noyau	394
5.3.1 Les méthodes	394
5.3.2 Préparation de l'environnement	394
5.4 Changer le noyau avec apt	395
5.4.1 En mise à jour	395
5.4.2 Dernières versions	395
5.5 Construction d'un autre noyau	396
5.5.1 Charger les sources	396
5.5.2 Compiler le nouveau noyau	397
5.6 Accélérer le démarrage du système	400
5.6.1 Principe	400
5.6.2 Méthodologie de réalisation	400
6. Mise en pratique	404
6.1 Consommation de ressources	404
6.2 Sauvegarde automatique	406

Chapitre 11

Disques et systèmes de fichiers

1. Introduction	407
1.1 Nomenclature	407
1.1.1 IDE	407
1.1.2 SCSI, SATA, USB, FireWire, etc.	408
1.2 Fonctionnement d'un système de fichiers	408
1.2.1 Principe.	408
1.2.2 Les inodes	408
1.2.3 Les noms des fichiers	409
1.2.4 Le journal	409
1.2.5 Le système de fichiers ext4	410
2. Partitionnement	410
2.1 Découpage logique	410
2.2 Organisation d'un disque	410
2.2.1 Le MBR.	410
2.2.2 Le GPT	411
2.2.3 Les partitions	411
2.2.4 Les types de partitions	412
2.3 Travailler avec les partitions	414
2.3.1 Lister.	414
2.3.2 Supprimer.	415
2.3.3 Créer.	415
2.3.4 Enregistrer	416
2.3.5 Synchronisation des disques.	417
3. Manipuler les systèmes de fichiers	417
3.1 Créer un système de fichiers	417
3.2 Accéder aux systèmes de fichiers.	420
3.2.1 mount.	420
3.2.2 umount	423
3.2.3 /etc/fstab	424
3.2.4 CD-Rom et images ISO.	425

3.3	Contrôler le système de fichiers	426
4.	Les quotas disques	427
4.1	Définitions	427
4.2	Mise en place	428
5.	RAID	429
5.1	Création d'un RAID	429
5.1.1	RAID0	429
5.1.2	RAID1	429
5.1.3	RAID0+1	430
5.2	État du RAID	430
5.3	Simulation d'une panne	431
5.4	Remplacement d'un disque	431
5.5	Arrêt et relance manuels	432
6.	LVM	432
6.1	Volumes physiques (PV)	432
6.1.1	Créer un volume physique	432
6.1.2	Détails d'un volume physique	433
6.2	Groupes de volumes (VG)	433
6.2.1	Créer un groupe de volumes	433
6.2.2	Détails d'un groupe de volumes	434
6.3	Volumes logiques (LV)	435
6.3.1	Créer un volume logique	435
6.3.2	Détails d'un volume logique	435
6.3.3	Accès au volume logique	436
6.4	Agrandissements et réductions	436
6.4.1	Les groupes de volumes	436
6.4.2	Agrandir un volume logique	437
6.4.3	Réduire un volume logique	438
6.4.4	Réduire un groupe de volumes	439
6.5	Suppression d'un groupe de volumes	439
7.	Mise en pratique	440

Chapitre 12

Sécurisation système et réseau

1. Politique d'authentification	445
1.1 Modules PAM	445
1.1.1 Principes	445
1.1.2 Configuration et structure des fichiers	446
1.1.3 Exemple du fichier /etc/pam.d/login	448
1.2 Utilisation de PAM pour une connexion à un annuaire	449
1.2.1 Connexion à un serveur LDAP	449
1.2.2 Connexion à un serveur Active Directory	455
1.3 Plus de sécurité avec PAM	460
1.3.1 Restriction horaire	460
1.3.2 Mots de passe renforcés	461
2. Pare-feu avec UFW	463
2.1 Activation et statut	463
2.2 Règles par défaut	464
2.3 Gestion des règles	464
2.3.1 Règles simples	464
2.3.2 Suppression	465
2.3.3 Applications	465
2.3.4 Règles plus complexes	466
2.4 Interface graphique	467
3. OpenSSH	468
3.1 Présentation	468
3.2 Configuration	468
3.3 Utilisation	469
3.4 Connexion par clés	469
3.4.1 Côté client	469
3.4.2 Côté serveur	470

- 4. Partage de fichiers 471
 - 4.1 Partage public 471
 - 4.2 Partage Samba 471
 - 4.2.1 Paramètres du serveur 472
 - 4.2.2 Partage d'un dossier 473
 - 4.2.3 Samba et pare-feu 475
- 5. Ubuntu One 475

Chapitre 13
Support et dépannage

- 1. Dépanner les problèmes courants 477
 - 1.1 Sur quel système suis-je ? 477
 - 1.2 Perte du mot de passe 478
 - 1.2.1 Le mot de passe utilisateur 478
 - 1.2.2 Vous n'avez plus aucun mot de passe 478
 - 1.2.3 Vous avez le CD d'installation d'Ubuntu Server 482
 - 1.3 Le serveur graphique ne répond plus 483
 - 1.4 Un programme est bloqué 483
 - 1.5 La langue n'est pas le français 484
 - 1.5.1 Corriger depuis la console 484
 - 1.5.2 Corriger depuis l'interface graphique 484
 - 1.5.3 Le problème des locales 485
 - 1.6 GRUB fait une erreur au démarrage du système 486
 - 1.7 Le mode de dépannage 487
- 2. Problèmes d'instabilité (plantages, blocages) 488
 - 2.1 Isoler l'origine du problème 488
 - 2.2 Les problèmes matériels 489
 - 2.2.1 L'overclocking 489
 - 2.2.2 La mémoire 490
 - 2.2.3 L'alimentation électrique 492
 - 2.2.4 La surchauffe du processeur 493
 - 2.2.5 La carte graphique 494

2.3	Les plantages logiciels	494
3.	Trouver de l'aide	495
3.1	Sur le bureau	495
3.2	Aide en ligne	497
	Index	499



Chapitre 9

Les droits des utilisateurs

1. Gérer les utilisateurs

La gestion des droits est un point crucial de l'administration de votre système d'exploitation Ubuntu. Elle est fortement liée au système de fichiers (car rappelez-vous qu'Unix est construit autour des systèmes de fichiers) et c'est pourquoi vous trouvez ici beaucoup de manipulations en mode console.

Une erreur dans les droits et c'est toute la sécurité de votre installation qui est en jeu.

1.1 Principe

1.1.1 Linux en général

Les utilisateurs sont référencés par :

- Un **login**, ou nom de connexion.
- Un **UID** (*User ID*), identifiant numérique unique de l'utilisateur, codé sur 32 bits.
- Un **GID** (*Group ID*), identifiant du groupe principal auquel appartient l'utilisateur.
- Divers autres groupes secondaires.

Ces informations sur votre compte utilisateur sont obtenues avec la commande `ID`. Dans l'exemple ci-dessous, l'utilisateur `eni` a comme `uid` 1000 et comme `gid` 1000. Il fait partie d'un grand nombre de groupes.

```
$ id
uid=1000(en) gid=1000(en)
groupes=1000(seb),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),10
9(lpadmin),124(sambashare)
```

Les utilisateurs ont des droits sur tout ce qui leur appartient et sur ce qui appartient à leurs groupes.

Une commande est exécutée avec les droits de l'utilisateur.

Les informations sur les comptes locaux sont stockées dans `/etc/passwd` et `/etc/shadow`. Les groupes sont dans `/etc/group` et `/etc/gshadow`.

Le mot de passe, crypté, est le deuxième champ de chaque ligne du fichier `/etc/shadow`. Seul l'administrateur peut lire le contenu de ce fichier.

L'administrateur du système est appelé **root** et porte toujours l'`uid` 0. Il est le seul, sauf mécanismes spécifiques, à pouvoir exécuter les tâches administratives les plus importantes.

Pour passer `root`, un utilisateur peut utiliser la commande `su`. Il saisit le mot de passe `root` et devient celui-ci. En fermant le shell `root` il reprend ses droits par défaut.

```
$ su
Mot de passe : xxxxxxxx
#
```

1.1.2 Ubuntu en particulier

À moins d'avoir installé Ubuntu en mode expert, vous avez remarqué que :

- à aucun moment vous n'avez saisi le mot de passe du compte `root`.
- un seul compte, le vôtre, a été créé, et qu'il dispose de droits particuliers.

Ce mécanisme utilise les droits `sudo`. C'est une fonctionnalité d'Unix qui permet de donner des droits supplémentaires à des utilisateurs, sur tout le système ou des commandes en particulier.

Le compte que vous avez créé lors de l'installation dispose de ces droits : ils lui permettent d'utiliser toutes les commandes en tant qu'administrateur, à condition de les faire précéder de la commande `sudo` et de saisir son mot de passe :

```
┌ $ sudo apt update
└ [sudo] password for seb:
```

Pour rester `root`, ce qui est plus pratique si vous avez beaucoup de commandes à taper, tapez :

```
┌ $ sudo -i
└ #
```

Ubuntu a donc une politique des droits plus restrictive que les autres distributions Linux :

- L'utilisateur courant ne doit pas avoir accès aux fichiers et processus du système et ne peut pas les modifier.
- Le compte `root` est désactivé car il est trop dangereux pour une utilisation courante du système.

Personne n'est à l'abri d'une mauvaise manipulation aux conséquences très graves. Pour utiliser LibreOffice, écouter de la musique, surfer sur le web et envoyer des mails, nul besoin d'être `root`.

Si vos actions nécessitent une action de l'administrateur, Ubuntu demandera votre mot de passe et les commandes associées seront jouées par `sudo`.

1.1.3 Rétablir le compte `root`

Il ne faut pas élever la règle de l'utilisation de `sudo` à un rang de dogme. Si elle est plus sécurisante, elle devient vite ennuyeuse, notamment si vous devez configurer un serveur ou utiliser temporairement un grand nombre de commandes. Dans ce cas, deux solutions :

- Faites un `sudo -i`.
- Rétablissez le compte `root`.

Pour rétablir le compte `root`, il suffit de lui donner un mot de passe.

```
┌ $ sudo passwd root
└ [sudo] password for eni:
```



```
Entrez le nouveau mot de passe UNIX :
Retapez le nouveau mot de passe UNIX :
passwd : le mot de passe a été mis à jour avec succès
```

Vous pouvez alors vous connecter en tant que root ou taper la commande `su` (sans passer par `sudo`) : saisissez le mot de passe que vous lui avez donné.

Pour annuler cette action, vous devez verrouiller le compte. Cette commande ajoute un point d'exclamation devant le mot de passe crypté de root dans **/etc/shadow**.

```
$ sudo passwd -l root
```

Même root rétabli, toutes les actions effectuées par `sudo` via la console ou l'interface continuent de demander votre mot de passe et pas celui de root. Pour demander le mot de passe de root, faites ceci :

Éditez **/etc/sudoers** avec `visudo`.

```
$ sudo visudo
```

▣ Modifiez la ligne suivante comme ceci :

```
Defaults          env_reset,rootpw
```

▣ Sauvegardez le fichier.

1.2 Les fichiers

1.2.1 /etc/passwd

Le fichier **/etc/passwd** contient la liste des utilisateurs du système local. Il est lisible par tout le monde. Les informations qu'il contient sont publiques et utiles tant pour le système que pour les utilisateurs. Chaque ligne représente un utilisateur et est composée de sept champs.

```
login:password:UID:GID:comment:homedir:shell
```

- Champ 1 : le login ou nom d'utilisateur.
- Champ 2 : sur les vieilles versions, le mot de passe crypté. Si un x est présent, le mot de passe est placé dans **/etc/shadow**. Si c'est un point d'exclamation, le compte est verrouillé.

Chapitre 9

- Champ 3 : le User ID.
- Champ 4 : le GID, c'est-à-dire le groupe principal.
- Champ 5 : un commentaire ou descriptif. C'est un champ d'information qui contient souvent le prénom et le nom de l'utilisateur, mais qui peut contenir autre chose.
- Champ 6 : le répertoire de travail, personnel, de l'utilisateur. C'est le répertoire dans lequel il arrive lorsqu'il se connecte.
- Champ 7 : le shell par défaut de l'utilisateur. Mais ce peut être toute autre commande, y compris une commande interdisant la connexion.

```
root@eni-VirtualBox: ~
Fichier Édition Affichage Rechercher Terminal Aide
root@eni-VirtualBox:~#
root@eni-VirtualBox:~#
root@eni-VirtualBox:~# pwd
/root
root@eni-VirtualBox:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
ircd:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:/:home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/:nonexistent:/usr/sbin/nologin
_apt:x:104:65534:/:nonexistent:/usr/sbin/nologin
uuid:x:105:111:/:run/uuid:/usr/sbin/nologin
avahi-autoipd:x:106:112:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:107:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
rtkit:x:109:114:RealtimeKit,,,:/proc:/usr/sbin/nologin
speech-dispatcher:x:110:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
whoopsie:x:111:117:/:nonexistent:/bin/false
kernoops:x:112:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:113:119:/:var/lib/saned:/usr/sbin/nologin
pulse:x:114:120:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
avahi:x:115:122:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
colord:x:116:123:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
hplip:x:117:7:HPLIP system user,,,:/var/run/hplip:/bin/false
geoclue:x:118:124:/:var/lib/geoclue:/usr/sbin/nologin
gnome-initial-setup:x:119:65534:/:run/gnome-initial-setup:/bin/false
gdm:x:120:125:Gnome Display Manager:/var/lib/gdm3:/bin/false
eni:x:1000:1000:eni,,,:/home/eni:/bin/bash
vboxadd:x:999:1:/:var/run/vboxadd:/bin/false
lightdm:x:121:127:Light Display Manager:/var/lib/lightdm:/bin/false
sddm:x:122:129:Simple Desktop Display Manager:/var/lib/sddm:/bin/false
root@eni-VirtualBox:~#
```

1.2.2 /etc/group

Le fichier **/etc/group** contient la définition des groupes d'utilisateurs et pour chacun, la liste des utilisateurs dont il est le groupe secondaire. Chaque ligne est composée de quatre champs :

```
group:password:GID:user1,user2,...
```

- Champ 1 : le nom du groupe.
- Champ 2 : le mot de passe associé. Voyez l'explication ci-après.
- Champ 3 : le Group ID.
- Champ 4 : la liste des utilisateurs appartenant à ce groupe.

Il est inutile de replacer dans le quatrième champ les utilisateurs ayant ce groupe pour groupe principal, c'est induit.

Vous pouvez être surpris de voir la présence d'un champ de mot de passe pour les groupes. Il est peu utilisé. Un utilisateur a le droit de changer de groupe afin de prendre, temporairement tout du moins, un groupe secondaire comme groupe principal avec la commande `newgrp`.

L'administrateur peut mettre en place un mot de passe sur le groupe pour protéger l'accès à ce groupe en tant que groupe principal.

1.2.3 /etc/shadow

C'est là que sont stockés, entre autres, les mots de passe cryptés des utilisateurs. Il contient toutes les informations sur les mots de passe et leur validité dans le temps. Chaque ligne est composée de 9 champs séparés par des « : » :

```
bean:$2a$10$AjADxPEfE5iUJcltzYA4wOZO.f2UZ0qP/8EnOFY.P.m10Hifs7J8i:  
15141:0:99999:7:::
```

- Champ 1 : le login.
- Champ 2 : le mot de passé crypté. Le `xx` initial indique le type de cryptage.
- Champ 3 : nombre de jours depuis le 1er janvier 1970 du dernier changement de mot de passe.
- Champ 4 : nombre de jours avant lesquels le mot de passe ne peut pas être changé (0 : il peut être changé n'importe quand).