



Ressourcesinformatiques

 + QUIZ

Version en ligne

OFFERTE !

pendant 1 an

UBUNTU

Administration d'un système Linux

6^e édition

Yann BARDOT





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 35
 - 3.2 Nouveautés de la version 20.04 36
 - 3.3 Déclinaisons d'une même version 39
 - 3.3.1 Suivant la destination 39
 - 3.3.2 Suivant l'environnement graphique 42
 - 3.3.3 Suivant les fonctionnalités 45
- 4. Administrateur système Ubuntu. 48
 - 4.1 Rôle de base. 49
 - 4.2 Missions étendues 50
- 5. Conventions typographiques. 50
 - 5.1 Terminologie anglaise. 50
 - 5.2 Exemples 51

5.3	Commandes et code	51
5.3.1	Présentation	51
5.3.2	Exécution	51
5.4	Touches du clavier	52

Chapitre 2

Prérequis à l'installation

1.	Essayer Ubuntu sans l'installer	53
1.1	Depuis Windows	53
1.1.1	Sur les anciennes versions	53
1.1.2	Avec WSL	54
1.1.3	Dans une machine virtuelle	56
1.2	Depuis un LiveCD	68
2.	Le matériel	70
2.1	L'architecture	70
2.1.1	Cas classiques	70
2.1.2	Cas spéciaux	70
2.1.3	Accès Internet	71
2.2	Les besoins d'Ubuntu	71
2.2.1	Linux en général	71
2.2.2	Ubuntu Desktop	73
2.2.3	Ubuntu Server	73
2.2.4	Lubuntu	73
2.2.5	Xubuntu	73
2.2.6	Kubuntu	74
2.3	Compatibilité du matériel	74
2.3.1	Vérifier son matériel	74
2.3.2	Listes de compatibilité matérielle	81
3.	Les supports de stockage	82
3.1	Trouver de la place	82
3.1.1	Installer Ubuntu sur un disque inutilisé	83
3.1.2	Repartitionner un disque	83

- 3.2 Schéma de partitionnement. 89
 - 3.2.1 Nombre minimal de partitions 89
 - 3.2.2 Séparation des données 90
 - 3.2.3 Partitionnement d'un serveur 91
 - 3.2.4 Cas du swap 91
- 3.3 Choisir un système de fichiers. 92
 - 3.3.1 Le journal 93
 - 3.3.2 ext2fs. 93
 - 3.3.3 ext3fs. 94
 - 3.3.4 ext4fs. 94
 - 3.3.5 btrfs. 94
 - 3.3.6 ZFS 95
 - 3.3.7 Compatibilité avec Windows 95

Chapitre 3
Installation

- 1. Installation normale d'un poste de travail 97
 - 1.1 Préalable à l'installation 97
 - 1.2 Processus d'installation. 98
 - 1.2.1 Écran de bienvenue. 98
 - 1.2.2 Disposition du clavier. 100
 - 1.2.3 Type d'installation (paquets). 101
 - 1.2.4 Type d'installation (disque). 102
 - 1.2.5 Emplacement géographique. 103
 - 1.2.6 Personnalisation et identité du super-utilisateur 104
 - 1.2.7 Phase finale 105
- 2. Installation d'un serveur avec Subiquity. 107
 - 2.1 Préalable à l'installation 107
 - 2.2 Installation 108
 - 2.2.1 Sélection de la langue. 108
 - 2.2.2 Sélection du clavier. 109
 - 2.2.3 Configuration du réseau. 110

2.2.4	Configuration du proxy	112
2.2.5	Configuration du miroir	113
2.2.6	Configuration du système de fichiers	114
2.2.7	Configuration du profil	117
2.2.8	Configuration des logiciels.	118
3.	Installation d'un serveur en mode expert	120
3.1	Préalable à l'installation	120
3.2	Première phase du processus d'installation.	120
3.2.1	Sélection de la langue	120
3.2.2	Options de boot	121
3.3	Deuxième phase du menu d'installation.	125
3.3.1	Choisir la langue	126
3.3.2	Configurer le clavier	127
3.3.3	Détecter et monter le CD	128
3.3.4	Charger un fichier de configuration	128
3.3.5	Charger des composants d'installation à partir du CD .	129
3.4	Troisième phase du menu d'installation	130
3.4.1	Détecter le matériel réseau.	130
3.4.2	Configurer le réseau	131
3.4.3	Créer les utilisateurs et choisir les mots de passe	132
3.4.4	Configurer l'horloge	133
3.4.5	Détecter les disques	133
3.4.6	Partitionner les disques	134
3.4.7	Installer le système.	141
3.4.8	Configurer l'outil de gestion des paquets	143
3.4.9	Choisir et installer des logiciels	145
3.4.10	Installer le programme de démarrage GRUB sur un disque dur	148
3.4.11	Terminer l'installation	148
4.	Installations spécifiques	150
4.1	Utilisation du LVM	150
4.1.1	Principe	150
4.1.2	Installation avec LVM	151

- 4.2 Utilisation du RAID logiciel 154
 - 4.2.1 Principe 154
 - 4.2.2 Installation avec RAID 155

Chapitre 4
Prise en main de la distribution

- 1. Présentation de l'interface graphique 161
 - 1.1 L'écran de connexion 161
 - 1.2 L'environnement 163
- 2. Présentation des menus et outils 165
 - 2.1 Menus 165
 - 2.2 Applications 172
- 3. Raccourcis-clavier 181

Chapitre 5
Utiliser la ligne de commandes

- 1. Le shell 185
 - 1.1 Rôle 185
 - 1.2 Le shell et l'administrateur 188
 - 1.3 Bash : le shell par défaut 188
 - 1.4 Utiliser le shell 189
 - 1.4.1 Pour débiter 189
 - 1.4.2 Syntaxe générale 189
 - 1.4.3 Aide 190
 - 1.4.4 Exemple avec cal 190
 - 1.4.5 Chaîner les commandes 192
 - 1.4.6 Grouper les commandes 193
 - 1.4.7 Afficher du texte avec echo 194
 - 1.4.8 L'historique de commandes 194

2.	L'éditeur vi.	195
2.1	Fonctionnement	195
2.2	Commandes de base.	196
2.2.1	Saisie	196
2.2.2	Sortie et sauvegarde	196
2.2.3	Déplacement.	197
2.2.4	Correction	197
2.2.5	Recherche simple	198
2.2.6	Copier-coller	198
2.2.7	Recherche et remplacement.	199
2.2.8	Autres commandes.	199
3.	Gestion des fichiers.	199
3.1	Système de fichiers FHS.	199
3.2	Types de fichiers.	203
3.3	Nomenclature des fichiers	204
3.4	Chemins	204
3.4.1	Représentation	204
3.4.2	Se déplacer	205
3.5	Commandes de base.	205
3.5.1	Lister	205
3.5.2	Créer des fichiers vides.	207
3.5.3	Créer des répertoires.	207
3.5.4	Supprimer des répertoires	207
3.5.5	Copier des fichiers	207
3.5.6	Déplacer et renommer un fichier.	208
3.5.7	Supprimer un fichier ou une arborescence	208
3.5.8	Liens symboliques	209
3.6	Caractères de substitution.	210
3.7	Verrouillage de caractères.	210
4.	Recherche	211
4.1	Rechercher des fichiers.	211
4.1.1	Critères de recherche	211
4.1.2	Commandes	212

- 4.2 Retrouver des exécutables 213
- 5. Redirections 213
 - 5.1 Les canaux..... 213
 - 5.2 En sortie..... 214
 - 5.3 En entrée..... 214
 - 5.4 Jouer avec les canaux 215
- 6. Quelques filtres et utilitaires 215
 - 6.1 Les tubes ou pipes..... 215
 - 6.2 Rechercher des lignes 216
 - 6.3 Couper des champs..... 216
 - 6.4 Compter les lignes 217
 - 6.5 Trier..... 218
 - 6.6 Supprimer les doublons 219
 - 6.7 Découper et recoller un fichier..... 219
 - 6.7.1 Découper..... 219
 - 6.7.2 Recoller 220
 - 6.8 Afficher du texte..... 220
 - 6.8.1 En pleine page..... 220
 - 6.8.2 Début d'un fichier..... 220
 - 6.8.3 Fin et attente de fichier 221
 - 6.9 Dupliquer le canal de sortie standard 221
 - 6.10 Mettre un script en attente 222
- 7. Variables 222
 - 7.1 Nomenclature..... 222
 - 7.2 Déclaration et affectation 222
 - 7.3 Accès et affichage 222
 - 7.4 Accolades..... 223
 - 7.5 Variables système 224
 - 7.6 Variables spéciales 225
- 8. Effectuer des tests..... 225
 - 8.1 Sur des chaînes 225
 - 8.2 Sur des valeurs numériques 226

8.3	Sur les fichiers	226
8.4	Critères ET OU NON	227
9.	Processus	228
9.1	Lancer des programmes	228
9.2	Lister les processus	229
9.3	Arrêter un processus	230
10.	Divers	232
10.1	Calculs	232
10.2	Longueur d'une chaîne	232
10.3	Substitution de commande	232
11.	Mise en pratique	233
11.1	Énoncé	233
11.2	Correction	234

Chapitre 6

Configuration du système

1.	Démarrage	237
1.1	Le chargeur de démarrage	237
1.2	GRUB2 remplace GRUB	238
1.3	Configuration de GRUB2	239
1.3.1	Fichier /etc/default/grub	239
1.3.2	Autres fichiers	241
1.3.3	Mise à jour de GRUB	241
1.3.4	Construction des menus	242
1.4	Démarrage et édition	244
1.5	Changement de l'image splash de GRUB	244
2.	Services au démarrage	245
2.1	Niveaux d'exécution	245
2.2	systemd en remplacement d'upstart	246

2.3	Utilitaires de gestion des services	248
2.3.1	Anciennes méthodes	249
2.3.2	systemctl	250
2.4	Actions sur un service	251
3.	Connexion au réseau	254
3.1	netplan	254
3.1.1	Présentation	254
3.1.2	Cas d'une connexion filaire	254
3.1.3	Cas d'une connexion sans fil	256
3.2	Network Manager	256
3.2.1	Configuration graphique	257
3.2.2	Configuration en mode console	260
3.2.3	Désactivation	261
3.3	Ancienne configuration	261
3.3.1	Fichier /etc/network/interfaces	261
3.3.2	Routes statiques et autres commandes	263
3.3.3	Cas d'une connexion sans fil	263
3.4	Commandes utiles pour le réseau	266
3.4.1	ping	266
3.4.2	ip	266
3.4.3	arp	267
3.4.4	ifconfig	267
3.4.5	route	268
4.	Les périphériques	269
4.1	Découverte des périphériques	269
4.1.1	Fichiers périphériques	269
4.1.2	Découverte dynamique	270
4.2	Fonctionnement d'udev	270
4.3	Principe d'une règle	272
4.4	Exemple des cartes réseau	274
5.	Mise en pratique	275
5.1	Énoncés	275
5.2	Corrigés	275

Chapitre 7**Mise à jour du système**

1. Les dépôts de paquets logiciels.	277
1.1 Types de dépôts	277
1.2 Serveurs miroirs	278
1.3 Launchpad.	280
1.4 Remonter les problèmes.	281
1.5 Le fichier sources.list	282
1.5.1 Structure	282
1.5.2 Dépôts officiels	284
1.5.3 Backports.	285
1.5.4 Dépôt partenaire ou commercial.	285
1.5.5 Medibuntu	285
1.5.6 Les dépôts PPA	285
1.6 Gestion des dépôts avec l'interface graphique	286
1.7 Cas d'un serveur mandataire	287
2. Principe des paquets	289
2.1 Interfaces de gestion de paquets	289
2.2 snap	290
2.3 Les gestionnaires graphiques	291
2.3.1 Logiciel	291
2.3.2 Gestionnaire de mises à jour	292
2.3.3 Gestionnaire de paquets Synaptic	292
2.4 Les gestionnaires en mode console	294
2.4.1 Utilitaire dpkg.	294
2.4.2 Utilitaire apt	295
2.4.3 Utilitaire aptitude.	297
2.4.4 Utilitaire snap	299
2.4.5 Résumé de séquence de mise à jour d'un système	300
2.5 Mise à niveau de la distribution	300
2.5.1 Cas des versions LTS	300
2.5.2 Notifications	301
2.5.3 Canonical Livepatch.	302

- 2.5.4 Vers une version en développement 305
- 2.5.5 Vers une version finale 305
- 3. Mise en pratique 306

Chapitre 8
Découverte de l'environnement de travail

- 1. Xorg 307
 - 1.1 Présentation 307
 - 1.1.1 X Window 307
 - 1.1.2 Le gestionnaire de fenêtres 308
 - 1.1.3 Les widgets et les toolkits 309
 - 1.1.4 Wayland 310
 - 1.2 Installation et tests 310
 - 1.2.1 Installer Xorg 310
 - 1.2.2 Installer un gestionnaire de fenêtres 311
 - 1.2.3 Installer un environnement de bureau 312
 - 1.3 Configuration détaillée du serveur Xorg 313
 - 1.3.1 Générer automatiquement un fichier xorg.conf 313
 - 1.3.2 Configuration manuelle par le fichier xorg.conf 314
 - 1.3.3 Utiliser la commande
de configuration dpkg-reconfigure 318
- 2. L'environnement de bureau 319
 - 2.1 Connexion avec GDM (Gnome Desktop Manager) 319
 - 2.1.1 Pourquoi remplacer LightDM par GDM ? 319
 - 2.1.2 Le gestionnaire de sessions 320
 - 2.1.3 Utiliser GDM 320
 - 2.1.4 Le compte invité 323
 - 2.2 Personnaliser GDM 323
 - 2.2.1 Le fichier custom.conf 323
 - 2.2.2 Tweaks 325
 - 2.2.3 Changer l'environnement par défaut 326
 - 2.2.4 Changer de gestionnaire de session 327

3. Travailler avec d'autres environnements	328
3.1 Installer LXDE	328
3.2 Installer KDE.	329
3.3 Installer XFCE.	331
4. Mise en pratique.	332

Chapitre 9

Les droits des utilisateurs

1. Gérer les utilisateurs	333
1.1 Principe	333
1.1.1 Linux en général	333
1.1.2 Ubuntu en particulier.	334
1.1.3 Rétablir le compte root	335
1.2 Les fichiers.	336
1.2.1 /etc/passwd.	336
1.2.2 /etc/group	338
1.2.3 /etc/shadow	338
1.2.4 /etc/gshadow	339
1.3 Ouverture de session	340
1.3.1 En mode console.	340
1.3.2 En mode graphique.	341
1.4 Gérer les utilisateurs.	341
1.4.1 En mode console.	341
1.4.2 En mode graphique.	344
2. Droits des utilisateurs	346
2.1 Utilisateurs et attributs de fichiers	346
2.1.1 Principes	346
2.1.2 Changement des attributs de fichiers	348
2.1.3 Le masque	349
2.1.4 Changement de propriétaire ou de groupe	351
2.1.5 Droits supplémentaires	351

2.2	Gérer les droits depuis l'interface graphique	353
2.2.1	Dossier personnel de l'utilisateur	353
2.2.2	Modification des droits	354
2.3	La commande sudo et PolKit	356
2.3.1	sudo	356
2.3.2	Tâches administratives avec PolKit	357
3.	Gestion avancée des utilisateurs	359
3.1	Sécurité des mots de passe	359
3.1.1	Changer de mot de passe	359
3.1.2	Gérer les informations de validité	361
3.2	Vérifier la cohérence des fichiers	363
3.3	Actions de l'utilisateur	363
3.3.1	Changer de shell	363
3.3.2	Changer le commentaire	364
3.3.3	Changer de groupe principal	364
3.3.4	Changer d'identité	364
3.4	Configuration avancée	365
3.4.1	/etc/default/useradd	365
3.4.2	/etc/login.defs	366
3.5	Notifications à l'utilisateur	367
3.5.1	/etc/issue	367
3.5.2	/etc/update-motd.d	368
3.6	Environnement utilisateur	368
3.6.1	/etc/skel	368
3.6.2	Scripts de configuration	369
4.	Mise en pratique	369
4.1	Gestion des utilisateurs	369
4.2	Gestion des droits	371

Chapitre 10

Tâches d'administration

1. Surveillance et performances	373
1.1 Surveillance des processus	373
1.1.1 Les différents états d'un processus	373
1.1.2 La commande top	375
1.1.3 La charge moyenne	376
1.2 Les processeurs	377
1.2.1 La charge des processeurs	377
1.2.2 Surveillance de la charge CPU	378
1.3 La gestion de la mémoire	378
1.3.1 Voir l'état de la mémoire	378
1.3.2 Interpréter la consommation mémoire	379
1.3.3 Mémoire et architecture	381
1.3.4 L'OOM Killer	381
1.3.5 Interpréter le swap	382
1.4 Les performances des disques	383
1.4.1 Occupation	383
1.4.2 Surveillance de la charge	385
1.5 Surveillance globale	386
1.5.1 En direct	386
1.5.2 En différé	386
1.6 Autres commandes	387
1.6.1 La commande strace	387
1.6.2 La commande lsof	387
1.7 Surveillance depuis l'interface graphique	388
2. Surveillance avec les journaux	390
2.1 Consignation des événements	390
2.2 Archivage des fichiers journaux	392

3.	Planification des tâches	394
3.1	cron	394
3.1.1	Fonctionnement de cron	394
3.1.2	Définir une crontable personnelle	396
3.2	anacron	397
3.3	at	399
4.	Archivage et sauvegarde	399
4.1	Principes de la sauvegarde de données	400
4.2	Commandes et outils de sauvegarde	401
4.2.1	La commande tar (tape archiver)	401
4.2.2	La commande dd (device to device)	402
4.2.3	Les commandes dump et restore	403
5.	Interventions sur le noyau	404
5.1	Présentation	404
5.2	/proc et /sys	405
5.3	Paramètres dynamiques	406
5.4	Changer de noyau	407
5.4.1	Les méthodes	407
5.4.2	Préparation de l'environnement	407
5.5	Changer le noyau avec apt	408
5.5.1	En mise à jour	408
5.5.2	Dernières versions	408
5.6	Construction d'un autre noyau	409
5.6.1	Charger les sources	409
5.6.2	Compiler le nouveau noyau	410
5.7	Accélérer le démarrage du système	413
5.7.1	Principe	413
5.7.2	Méthodologie de réalisation	413
6.	Mise en pratique	418
6.1	Consommation de ressources	418
6.2	Sauvegarde automatique	420

Chapitre 11

Disques et systèmes de fichiers

1. Introduction	421
1.1 Nomenclature	421
1.1.1 IDE	421
1.1.2 SCSI, SATA, USB, FireWire, etc.	422
1.2 Fonctionnement d'un système de fichiers	422
1.2.1 Principe	422
1.2.2 Les inodes	422
1.2.3 Les noms des fichiers	423
1.2.4 Le journal	423
1.2.5 Le système de fichiers ext4	424
2. Partitionnement	424
2.1 Découpage logique	424
2.2 Organisation d'un disque	424
2.2.1 Le MBR	424
2.2.2 Le GPT	425
2.2.3 Les partitions	425
2.2.4 Les types de partitions	426
2.3 Travailler avec les partitions	428
2.3.1 Lister	428
2.3.2 Supprimer	429
2.3.3 Créer	429
2.3.4 Enregistrer	430
2.3.5 Synchronisation des disques	431
3. Manipuler les systèmes de fichiers	431
3.1 Créer un système de fichiers	431
3.2 Accéder aux systèmes de fichiers	434
3.2.1 mount	434
3.2.2 umount	437
3.2.3 /etc/fstab	438
3.2.4 CD-Rom et images ISO	440

- 3.3 Contrôler le système de fichiers. 440
- 4. Les quotas disques 441
 - 4.1 Définitions 441
 - 4.2 Mise en place. 442
- 5. RAID 443
 - 5.1 Création d'un RAID 443
 - 5.1.1 RAID0 443
 - 5.1.2 RAID1 444
 - 5.1.3 RAID0+1 444
 - 5.2 État du RAID 445
 - 5.3 Simulation d'une panne 446
 - 5.4 Remplacement d'un disque 446
 - 5.5 Arrêt et relance manuels 446
- 6. LVM. 447
 - 6.1 Volumes physiques (PV) 447
 - 6.1.1 Créer un volume physique. 447
 - 6.1.2 Détails d'un volume physique 447
 - 6.2 Groupes de volumes (VG) 448
 - 6.2.1 Créer un groupe de volumes 448
 - 6.2.2 Détails d'un groupe de volumes 448
 - 6.3 Volumes logiques (LV) 449
 - 6.3.1 Créer un volume logique 449
 - 6.3.2 Détails d'un volume logique 450
 - 6.3.3 Accès au volume logique 450
 - 6.4 Agrandissements et réductions 451
 - 6.4.1 Les groupes de volumes 451
 - 6.4.2 Agrandir un volume logique 451
 - 6.4.3 Réduire un volume logique 453
 - 6.4.4 Réduire un groupe de volumes 453
 - 6.5 Suppression d'un groupe de volumes 454

7. Cas particulier de ZFS	454
7.1 Présentation de ZFS	454
7.2 Création de pools	455
7.3 Clichés instantanés	458
8. Mise en pratique	459

Chapitre 12

Sécurisation système et réseau

1. Politique d'authentification	463
1.1 Modules PAM	463
1.1.1 Principes	463
1.1.2 Configuration et structure des fichiers	464
1.1.3 Exemple du fichier /etc/pam.d/login	466
1.2 Utilisation de PAM pour une connexion à un annuaire	467
1.2.1 Connexion à un serveur LDAP	467
1.2.2 Connexion à un serveur Active Directory	473
1.3 Plus de sécurité avec PAM	478
1.3.1 Restriction horaire	478
1.3.2 Mots de passe renforcés	479
2. Pare-feu avec UFW	481
2.1 Activation et statut	481
2.2 Règles par défaut	482
2.3 Gestion des règles	483
2.3.1 Règles simples	483
2.3.2 Suppression	483
2.3.3 Applications	484
2.3.4 Règles plus complexes	485
2.4 Interface graphique	485
3. OpenSSH	486
3.1 Présentation	486
3.2 Configuration	487

- 3.3 Utilisation 487
- 3.4 Connexion par clés 488
 - 3.4.1 Côté client 488
 - 3.4.2 Côté serveur 489
- 4. Partage de fichiers 490
 - 4.1 Partage webdav 490
 - 4.2 Partage Samba 491
 - 4.2.1 Paramètres du serveur 492
 - 4.2.2 Partage d'un dossier 494
 - 4.2.3 Samba et pare-feu 496

Chapitre 13
Support et dépannage

- 1. Dépanner les problèmes courants 497
 - 1.1 Sur quel système suis-je ? 497
 - 1.2 Perte du mot de passe 498
 - 1.2.1 Le mot de passe utilisateur 498
 - 1.2.2 Vous n'avez plus aucun mot de passe 499
 - 1.2.3 Vous avez le média d'installation d'Ubuntu Server 503
 - 1.3 Le serveur graphique ne répond plus 505
 - 1.4 Magic System Keys et crash 506
 - 1.5 Un programme est bloqué 508
 - 1.6 La langue n'est pas le français 509
 - 1.6.1 Corriger depuis la console 509
 - 1.6.2 Corriger depuis l'interface graphique 509
 - 1.6.3 Le problème des locales 510
 - 1.7 GRUB fait une erreur au démarrage du système 511
 - 1.8 Le mode de dépannage 512
 - 1.9 Utilisation du LiveCD 514

2.	Problèmes d'instabilité (plantages, blocages)	515
2.1	Isoler l'origine du problème	515
2.2	Les problèmes matériels	516
2.2.1	L'overclocking	516
2.2.2	La mémoire	517
2.2.3	L'alimentation électrique	519
2.2.4	La surchauffe du processeur	520
2.2.5	La carte graphique	521
2.3	Les plantages logiciels	521
3.	Trouver de l'aide	522
3.1	Sur le bureau	522
3.2	Aide en ligne	524
	Index	525

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(en),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 eni:
```

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. Actuellement, 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
irc: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).

- Champ 5 : nombre de jours après lesquels le mot de passe doit être changé.
- Champ 6 : nombre de jours avant l'expiration du mot de passe durant lesquels l'utilisateur doit être prévenu.
- Champ 7 : nombre de jours, après l'expiration du mot de passe, après lesquels le compte est désactivé.
- Champ 8 : nombre de jours depuis le 1er janvier 1970 à partir du moment où le compte a été désactivé.
- Champ 9 : réservé.

Dans l'exemple de la ligne `bean`, le mot de passe a été changé 15141 jours après le 01/01/1970. Le mot de passe doit être changé avant 0 jour mais il est toujours valide car le champ suivant indique qu'il faut le changer au bout de 99999 jours (273 ans) et le champ 5 est vide (pas d'obligation de changement de mot de passe). Le compte est désactivé après 7 jours, ce qui évidemment ne risque pas d'arriver...

Les valeurs courantes pour le cryptage des mots de passe sont les suivantes :

- \$1\$: MD5
- \$2a\$: Blowfish
- \$5\$: SHA-256
- \$6\$: SHA-512
- Autre : DES

Pour connaître la date en fonction du 01/01/1970, utilisez la commande `date` comme ceci, en ajoutant le nombre de jours désiré :

```
$ date --date "1 jan 1970 +15141days"  
jeu. juin 16 00:00:00 CEST 2011
```

1.2.4 /etc/gshadow

Le fichier `/etc/gshadow` est le pendant du fichier précédent mais pour les groupes. Sa syntaxe est la suivante :

```
groupe:password:admins:members
```