

Raphaël Hertzog

Roland Mas

Cahiers
de **l'Admin**
Debian
Lenny

Collection dirigée par Nat Makarévitch

© Groupe Eyrolles, 2009,
ISBN : 978-2-212-12443-9

EYROLLES



Table des matières

1. LE PROJET DEBIAN.....	1
Qu'est-ce que Debian ? • 2	
Un système d'exploitation multi-plates-formes • 2	
La qualité des logiciels libres • 3	
Le cadre : une association • 4	
Les textes fondateurs • 4	
L'engagement vis-à-vis des utilisateurs • 5	
Les principes du logiciel libre selon Debian • 6	
Fonctionnement du projet Debian • 8	
Les développeurs Debian • 8	
Le rôle actif des utilisateurs • 12	
Équipes et sous-projets • 14	
Sous-projets Debian existants • 14	
Équipes administratives • 15	
Équipes de développement, équipes transversales • 16	
Rôle d'une distribution • 18	
L'installateur : debian-installer • 18	
La bibliothèque de logiciels • 19	
Cycle de vie d'une release • 19	
Le statut Experimental • 19	
Le statut Unstable • 20	
La migration vers Testing • 21	
La promotion de Testing en Stable • 22	
2. PRÉSENTATION DE L'ÉTUDE DE CAS	27
Des besoins informatiques en forte hausse • 28	
Plan directeur • 28	
Pourquoi une distribution GNU/Linux ? • 30	
Pourquoi la distribution Debian ? • 31	
Distributions communautaires et commerciales • 31	
Pourquoi Debian Lenny ? • 33	
3. PRISE EN COMPTE DE L'EXISTANT ET MIGRATION	35
Coexistence en environnement hétérogène • 36	
Intégration avec des machines Windows • 36	
Intégration avec des machines Mac OS • 36	
Intégration avec d'autres machines Linux/Unix • 36	
Démarche de migration • 36	
Recenser et identifier les services • 37	
Réseau et processus • 38	
Conserver la configuration • 38	
Prendre en main un serveur Debian existant • 39	
Installer Debian • 40	
Installer et configurer les services sélectionnés • 41	
4. INSTALLATION.....	43
Méthodes d'installation • 44	
Installation depuis un CD-Rom/DVD-Rom • 44	
Démarrage depuis une clé USB • 45	
Installation par boot réseau • 46	
Autres méthodes d'installation • 46	
Étapes du programme d'installation • 47	
Exécution du programme d'installation • 47	
Choix de la langue • 48	
Choix du pays • 49	
Choix de la disposition du clavier • 49	
Détection du matériel • 50	
Chargement des composants • 50	
Détection du matériel réseau • 50	
Configuration du réseau • 51	
Configuration de l'horloge • 51	
Détection des disques et autres périphériques • 51	
Démarrage de l'outil de partitionnement • 51	
Partitionnement assisté • 52	
Partitionnement manuel • 54	
Emploi du RAID logiciel • 55	
Emploi de LVM (Logical Volume Manager) • 55	
Chiffrement de partitions • 56	
Mot de passe administrateur • 57	
Création du premier utilisateur • 57	
Installation du système de base Debian • 58	
Configuration de l'outil de gestion des paquets (apt) • 59	
Concours de popularité des paquets • 59	
Sélection des paquets à installer • 60	
Installation du chargeur d'amorçage GRUB • 60	
Terminer l'installation et redémarrer • 61	
Après le premier démarrage • 61	
Installation de logiciels supplémentaires • 62	

- Mise à jour du système • 63
- 5. SYSTÈME DE PAQUETAGE, OUTILS ET PRINCIPES FONDAMENTAUX 65**
- Structure d'un paquet binaire • 66**
- Méta-informations d'un paquet • 68**
- Description : fichier control • 68
 - Dépendances : champ Depends • 69
 - Conflits : champ Conflicts • 70
 - Incompatibilités : champ Breaks • 70
 - Éléments fournis : champ Provides • 71
 - La fourniture d'un « service » • 71
 - L'interchangeabilité avec un autre paquet • 71
 - Limitations actuelles • 72
 - Remplacements : champ Replaces • 72
 - Scripts de configuration • 73
 - Installation et mise à jour • 73
 - Suppression de paquet • 74
 - Sommes de contrôle, liste des fichiers de configuration • 75
- Structure d'un paquet source • 76**
- Format • 76
 - Utilité chez Debian • 78
- Manipuler des paquets avec dpkg • 79**
- Installation de paquets • 79
 - Suppression de paquet • 81
 - Autres fonctionnalités de dpkg • 82
 - Journal de dpkg • 84
- Cohabitation avec d'autres systèmes de paquetages • 85**
- 6. MAINTENANCE ET MISE À JOUR : LES OUTILS APT 89**
- Renseigner le fichier sources.list • 90**
- Ressources non officielles : apt-get.org, mentors.debian.net et backports.org • 92
- Commandes aptitude et apt-get • 93**
- Initialisation • 93
 - Installation et suppression • 94
 - Mise à jour • 95
 - Options de configuration • 96
 - Gérer les priorités associées aux paquets • 96
 - Travailler avec plusieurs distributions • 99
- Commande apt-cache • 101**
- Frontaux : aptitude, synaptic, gnome-apt • 101**
- aptitude • 101
 - Suivi des paquets installés automatiquement • 103
 - Gestion des recommandations, suggestions et tâches • 104
 - Meilleurs algorithmes de résolution • 105
 - synaptic • 105
- Vérification d'authenticité des paquets • 106**
- Mise à jour d'une distribution à la suivante • 107**
- Démarche à suivre • 108
 - Gérer les problèmes consécutifs à une mise à jour • 109
- Maintenir un système à jour • 110**
- Mise à jour automatique • 112**
- Configuration de dpkg • 112
 - Configuration d'APT • 112
 - Configuration de debconf • 113
 - Gestion des interactions en ligne de commande • 113
 - La combinaison miracle • 113
- Recherche de paquets • 114**
- 7. RÉOLUTION DE PROBLÈMES ET SOURCES D'INFORMATION 119**
- Les sources de documentation • 120**
- Les pages de manuel • 120
 - Documentation au format info • 122
 - La documentation spécifique • 122
 - Les sites web • 123
 - Les tutoriels (HOWTO) • 123
- Procédures type • 124**
- Configuration d'un logiciel • 124
 - Surveiller l'activité des démons • 125
 - Demander de l'aide sur une liste de diffusion • 126
 - Signaler un bogue en cas de problème incompréhensible • 126
- 8. CONFIGURATION DE BASE : RÉSEAU, COMPTES, IMPRESSION...129**
- Francisation du système • 130**
- Définir la langue par défaut • 130
 - Configurer le clavier en mode console • 131
 - Migration vers UTF-8 • 132
 - Configurer le clavier en mode graphique • 133
- Configuration du réseau • 134**
- Interface Ethernet • 134
 - Connexion PPP par modem téléphonique • 135
 - Connexion par modem ADSL • 135
 - Modem fonctionnant avec PPPoE • 136
 - Modem fonctionnant avec PPTP • 136
 - Modem fonctionnant avec DHCP • 136
 - Configuration réseau itinérante • 136
- Attribution et résolution des noms • 137**
- Résolution de noms • 138
 - Configuration des serveur DNS • 138
 - Fichier /etc/hosts • 138
- Base de données des utilisateurs et des groupes • 139**
- Liste des utilisateurs : /etc/passwd • 139
 - Le fichier des mots de passe chiffrés et cachés : /etc/shadow • 140
 - Modifier un compte ou mot de passe existant • 140

Bloquer un compte • 140	Syntaxe du sélecteur • 177
Liste des groupes : /etc/group • 141	Syntaxe des actions • 178
Création de comptes • 141	Le super-serveur inetd • 178
Environnement des interpréteurs de commandes • 142	Planification de tâches : cron et atd • 180
Configuration de l'impression • 144	Format d'un fichier crontab • 181
Configuration du chargeur d'amorçage • 144	Emploi de la commande at • 182
Identifier ses disques • 144	Planification asynchrone : anacron • 183
Configuration de LILO • 146	Les quotas • 184
Configuration de GRUB • 147	Sauvegarde • 185
Cas des Macintosh (PowerPC) : configuration de Yaboot • 148	Sauvegarde avec rsync • 185
Autres configurations : synchronisation, logs, partages... • 149	Restauration des machines non sauvegardées • 187
Fuseau horaire • 149	Branchements « à chaud » : hotplug • 188
Synchronisation horaire • 150	Introduction • 188
Pour les stations de travail • 151	La problématique du nommage • 188
Pour les serveurs • 151	Fonctionnement de udev • 189
Rotation des fichiers de logs • 151	Cas pratique • 191
Partage des droits d'administration • 152	Gestion de l'énergie • 192
Liste des points de montage • 152	Gestion avancée de l'énergie : APM • 192
locate et updatedb • 154	Économie d'énergie moderne : ACPI • 192
Compilation d'un noyau • 155	Cartes pour portables : PCMCIA • 193
Introduction et prérequis • 155	
Récupérer les sources • 155	10. INFRASTRUCTURE RÉSEAU 195
Configuration du noyau • 156	Passerelle • 196
Compilation et génération du paquet • 157	Réseau privé virtuel • 197
Compilation de modules externes • 158	OpenVPN • 198
Emploi d'un patch sur le noyau • 159	Infrastructure de clés publiques easy-rsa • 198
Installation d'un noyau • 160	Configuration du serveur OpenVPN • 202
Caractéristiques d'un paquet Debian du noyau • 160	Configuration du client OpenVPN • 203
Installation avec dpkg • 161	Réseau privé virtuel avec SSH • 203
9. SERVICES UNIX 163	IPsec • 204
Démarrage du système • 164	PPTP • 204
Connexion à distance • 167	Configuration du client • 205
Connexion à distance : telnet • 167	Configuration du serveur • 205
Connexion à distance sécurisée : SSH • 168	Qualité de service • 208
Authentification par clé • 169	Principe et fonctionnement • 208
Utiliser des applications X11 à distance • 170	Configuration et mise en œuvre • 208
Créer des tunnels chiffrés avec le port forwarding • 170	Minimiser le temps de latence : wondershaper • 208
Accéder à distance à des bureaux graphiques • 171	Configuration standard • 209
Gestion des droits • 172	Routage dynamique • 210
Interfaces d'administration • 174	IPv6 • 210
Administrer sur interface web : webmin • 175	Serveur de noms (DNS) • 212
Configuration des paquets : debconf • 176	Principe et fonctionnement • 212
Les événements système de syslog • 176	Configuration • 213
Principe et fonctionnement • 176	DHCP • 215
Le fichier de configuration • 177	Présentation • 215
	Configuration • 215
	DHCP et DNS • 216

Outils de diagnostic réseau • 217	
Diagnostic local : netstat • 217	
Diagnostic distant : nmap • 218	
Les sniffers : tcpdump et wireshark • 220	
11. SERVICES RÉSEAU : POSTFIX, APACHE, NFS, SAMBA, SQUID, LDAP..... 223	
Serveur de messagerie électronique • 224	
Installation de Postfix • 224	
Configuration de domaines virtuels • 227	
Domaine virtuel d'alias • 227	
Domaine virtuel de boîtes aux lettres • 228	
Restrictions à la réception et à l'envoi • 229	
Restreindre l'accès en fonction de l'adresse IP • 229	
Vérifier la validité de la commande EHLO ou HELO • 230	
Accepter ou refuser en fonction de l'émetteur (annoncé) • 231	
Accepter ou refuser en fonction du destinataire • 231	
Restrictions associées à la commande DATA • 232	
Application des restrictions • 232	
Filtrer en fonction du contenu du message • 233	
Mise en place du greylisting • 233	
Personnalisation des filtres en fonction du destinataire • 235	
Intégration d'un antivirus • 236	
Installation et configuration de l'antivirus • 236	
Configuration de Postfix avec l'antivirus • 237	
SMTP authentifié • 238	
Serveur web (HTTP) • 240	
Installation d'Apache • 240	
Configuration d'hôtes virtuels • 240	
Directives courantes • 242	
Requérir une authentification • 243	
Restrictions d'accès • 243	
Analyseur de logs • 243	
Serveur de fichiers FTP • 245	
Serveur de fichiers NFS • 246	
Sécuriser NFS (au mieux) • 247	
Serveur NFS • 248	
Client NFS • 249	
Partage Windows avec Samba • 250	
Samba en serveur • 250	
Configuration avec debconf • 250	
Configuration manuelle • 251	
Modifications à smb.conf • 251	
Ajout des utilisateurs • 253	
Transformation en contrôleur de domaines • 253	
Samba en client • 254	
Le programme smbclient • 254	
Monter un partage Windows • 254	
Imprimer sur une imprimante partagée • 255	
Mandataire HTTP/FTP • 255	
Installation • 256	
Configuration d'un cache • 256	
Configuration d'un filtre • 256	
Annuaire LDAP • 257	
Installation • 257	
Remplissage de l'annuaire • 259	
Utiliser LDAP pour gérer les comptes • 260	
Configuration de NSS • 260	
Configuration de PAM • 261	
Sécuriser les échanges de données LDAP • 263	
Configuration côté serveur • 263	
Configuration côté client • 264	
12. ADMINISTRATION AVANCÉE 267	
RAID et LVM • 268	
RAID logiciel • 268	
Différents niveaux de RAID • 269	
Mise en place du RAID • 272	
Sauvegarde de la configuration • 277	
LVM • 278	
Concepts de LVM • 278	
Mise en place de LVM • 279	
LVM au fil du temps • 284	
RAID ou LVM ? • 285	
Virtualisation avec Xen • 288	
Installation automatisée • 294	
SystemImager • 295	
Fully Automatic Installer (FAI) • 296	
Debian-installer avec préconfiguration • 297	
Employer un fichier de préconfiguration • 297	
Créer un fichier de préconfiguration • 298	
Créer un média de démarrage adapté • 298	
Démarrage depuis le réseau • 299	
Préparer une clé USB amorçable • 299	
Créer une image de CD-Rom • 299	
Simple-CDD : la solution tout en un • 300	
Définir des profils • 300	
Configuration et fonctionnement de build-simple-cdd • 301	
Générer une image ISO • 302	
Supervision • 302	
Mise en œuvre de Munin • 302	

Configuration des hôtes à superviser • 302	En temps réel • 341
Configuration du grapheur • 304	Historique • 341
Mise en œuvre de Nagios • 305	Détection des changements • 342
Installation • 305	Audit des paquets : l'outil debsums et ses limites • 342
Configuration • 305	Surveillance des fichiers : AIDE • 343
13. STATION DE TRAVAIL..... 311	Détection d'intrusion (IDS/NIDS) • 344
Configuration du serveur X11 • 312	Introduction à SELinux • 345
Détection automatique • 312	Les principes • 345
Script de configuration • 313	La mise en route • 346
Personnalisation de l'interface graphique • 313	La gestion d'un système SELinux • 347
Choix d'un gestionnaire d'écran (display manager) • 313	Gestion des modules SELinux • 348
Choix d'un gestionnaire de fenêtres • 314	Gestion des identités • 348
Gestion des menus • 315	Gestion des contextes de fichiers, des ports et des booléens • 349
Bureaux graphiques • 315	L'adaptation des règles • 350
GNOME • 316	Rédiger un fichier .fc • 351
KDE • 317	Rédiger un fichier .if • 351
Xfce et autres • 318	Rédiger un fichier .te • 352
Outils • 319	Compilation des fichiers • 355
Courrier électronique • 319	Autres considérations sur la sécurité • 355
Evolution • 319	Risques inhérents aux applications web • 355
KMail • 320	Savoir à quoi s'attendre • 355
Thunderbird et Icedove • 320	Bien choisir les logiciels • 357
Navigateurs web • 321	Gérer une machine dans son ensemble • 358
Développement • 322	Les utilisateurs sont des acteurs • 358
Outils pour GTK+ sur GNOME • 322	Sécurité physique • 358
Outils pour Qt sur KDE • 323	Responsabilité juridique • 359
Travail collaboratif • 323	En cas de piratage • 360
Travail en groupe : groupware • 323	Détection et constater le piratage • 360
Messagerie instantanée • 323	Mettre le serveur hors-ligne • 361
Configuration du serveur • 324	Préserver tout ce qui peut constituer une preuve • 361
Clients Jabber • 326	Réinstaller • 362
Travail collaboratif avec GForge • 326	Analyser à froid • 362
Suites bureautiques • 327	Reconstituer le scénario de l'attaque • 363
L'émulation Windows : Wine • 327	
14. SÉCURITÉ..... 331	15. CONCEPTION D'UN PAQUET DEBIAN..... 367
Définir une politique de sécurité • 332	Recompiler un paquet depuis ses sources • 368
Pare-feu ou filtre de paquets • 333	Récupérer les sources • 368
Fonctionnement de netfilter • 334	Effectuer les modifications • 368
Syntaxe d'iptables • 336	Démarrer la recompilation • 370
Les commandes • 336	Construire son premier paquet • 371
Les règles • 336	Méta-paquet ou faux paquet • 371
Créer les règles • 337	Simple archive de fichiers • 372
Installer les règles à chaque démarrage • 339	Créer une archive de paquets pour APT • 376
Supervision : prévention, détection, dissuasion • 339	Devenir mainteneur de paquet • 377
Surveillance des logs avec logcheck • 340	Apprendre à faire des paquets • 377
Surveillance de l'activité • 341	Les règles • 378

Les procédures • 378	
Les outils • 378	
Le programme lintian • 378	
devscripts • 379	
debhelper et dh-make • 379	
dupload et dput • 379	
Processus d'acceptation • 380	
Prérequis • 380	
Inscription • 380	
Acceptation des principes • 381	
Vérification des compétences • 382	
Approbation finale • 382	
16. CONCLUSION : L'AVENIR DE DEBIAN	385
Développements à venir • 386	
Avenir de Debian • 386	
Avenir de ce livre • 387	
A. DISTRIBUTIONS DÉRIVÉES	389
Ubuntu Linux • 390	
Knoppix • 391	
SimplyMEPIS • 391	
Xandros • 391	
Linspire et Freespire • 392	
Sidux • 392	
Damn Small Linux • 393	
Et d'autres encore • 393	
B. PETIT COURS DE RATTRAPAGE.....	395
Interpréteur de commandes et commandes de base • 396	
Déplacement dans l'arborescence et gestion des fichiers • 396	
Consultation et modification des fichiers texte • 397	
Recherche de fichiers et dans les fichiers • 397	
Gestion des processus • 397	
Informations système : mémoire, espace disque, identité • 398	
Organisation de l'arborescence des fichiers • 398	
La racine • 398	
Le répertoire personnel de l'utilisateur • 399	
Fonctionnement d'un ordinateur :	
les différentes couches en jeu • 400	
Au plus bas niveau : le matériel • 400	
Le démarreur : le BIOS • 401	
Le noyau • 402	
L'espace utilisateur • 402	
Quelques fonctions remplies par le noyau • 403	
Pilotage du matériel • 403	
Systèmes de fichiers • 404	
Fonctions partagées • 405	
Gestion des processus • 405	
Gestion des permissions • 406	
L'espace utilisateur • 407	
Processus • 407	
Démons • 408	
Communications entre processus • 408	
Bibliothèques • 410	
GLOSSAIRE	411
INDEX	431