

Debian GNU/Linux

Vers une administration
de haute sécurité

→ Informatique technique

Téléchargement
www.editions-eni.fr



The logo for the Epsilon Collection, featuring a stylized Greek letter epsilon (ε) and the word "Collection" below it.

epsilon

Philippe PIERRE

Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>
Saisissez la référence de l'ouvrage **EPDEBS** dans la zone de recherche
et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Avant-propos

1. Objectifs	15
2. Public visé	16
3. Prérequis et connaissances nécessaires	16
4. Structure de l'ouvrage	16

Partie 1 : Le noyau

Chapitre 1

Sécurisation à l'initialisation

1. Pourquoi Debian ?	19
1.1 Sécurité du système d'information	21
1.2 Sécurité de l'information.	22
1.3 Où trouver la distribution Debian ?	23
2. Comment sécuriser ?	25
2.1 Sécurité et sûreté de fonctionnement	25
2.2 Supervision et surveillance	26
2.3 Traçabilité	26
2.4 Considération du coût et du risque	27
3. Chiffrer le gestionnaire de volumes logiques (LVM)	28
4. Sécuriser le BIOS.	30
4.1 Démarrage	30
4.2 Paramétrage	31
4.3 Cas des machines virtuelles	32
4.4 Utilisation d'UEFI	33
5. Sécuriser le bootloader	34
5.1 Les options	35
5.2 Restreindre l'accès au bootloader	38
5.3 Sécurisation en version antérieure	40
6. Sécuriser le noyau Linux	41
6.1 Les modules	42
6.2 initrd.	43
6.3 Les pseudo-systèmes de fichiers	45
6.3.1 /proc	45
6.3.2 /sys	46
6.3.3 Paramétrages particuliers	46

2 _____ Debian GNU/Linux

Vers une administration de haute sécurité

6.4	Sécurisation et compilation du noyau	47
6.5	Suppression des anciens noyaux	52
7.	Gestion de démarrage et améliorations	52
7.1	Phase d'initialisation init	53
7.2	Scripts d'initialisation avec en-têtes LSB	55
7.3	Parallélisation avec systemd	59

Chapitre 2 Installation

1.	Comment et quoi installer ?	67
1.1	Différents types d'installation	68
1.1.1	Cas d'une machine virtuelle VirtualBox	68
1.1.2	Cas d'une machine virtuelle VMware	73
1.1.3	Cas d'un serveur physique	78
1.2	Mécanisme de boot on SAN	82
1.3	Phase de démarrage	84
1.4	Création de compte d'administration autre que root	87
1.5	Sélection de logiciels minima	89
2.	Système d'exploitation et applications	91
2.1	Le noyau Linux	92
2.2	Les anneaux de protection	92
2.2.1	Architecture 32 bits sans virtualisation	93
2.2.2	Architecture 32 bits virtualisée	93
2.2.3	Architecture 64 bits sans virtualisation	94
2.2.4	Architecture 64 bits virtualisée	95
3.	Noyau Linux	95
3.1	Comment identifier un noyau Linux ?	97
3.2	Comment compiler un noyau Linux ?	97
3.3	Comment mettre à niveau le système ?	101
3.4	Configurer un mandataire de cache	103
4.	Mise à jour de sécurité	105
5.	Activation du pare-feu interne	109
6.	Installation automatisée	114
6.1	Éléments de configuration	114
6.2	Mise en œuvre de la préconfiguration	115
6.3	Fichier preseed.cfg	117
6.4	Cas particulier de l'installation Jessie (Debian 8.x)	121
6.5	Fonctions clonage et clichés	124
7.	Installation des compléments	125
7.1	Installation des « add-on guests » sous VirtualBox	126
7.2	Installation des VMTtools	128

Partie 2 : Le système d'exploitation

Chapitre 3

Sécurisation du système d'exploitation

- 1. Connexions et consoles 131
- 2. Commandes bas niveau 133
 - 2.1 Les différentes combinaisons 134
 - 2.2 Les consoles distantes 135
 - 2.3 L'intégrité d'un disque..... 135
 - 2.3.1 Intégrité de niveau logique 135
 - 2.3.2 Intégrité de niveau physique 137
- 3. Gestion des partitions 138
 - 3.1 Partitionnement LVM standard 138
 - 3.2 Partitionnement de type RAID 145
 - 3.3 Montages CIFS 158
 - 3.4 Chiffrement de partition 159
- 4. Serveur de temps 165
- 5. Gestion des services 168
 - 5.1 Niveau de service..... 168
 - 5.2 Activation et désactivation d'un service 169
 - 5.3 Services de base 170
 - 5.4 Service de création de périphériques 171
- 6. Gestion des ressources 176
 - 6.1 Matériel 176
 - 6.2 Disques..... 179
 - 6.3 Mémoire..... 180
 - 6.4 CPU 182
- 7. Paramétrage régional et internationalisation 183

Chapitre 4

Sécurisation de l'environnement

- 1. Systèmes de fichiers 187
 - 1.1 Présentation et types..... 187
 - 1.2 Opérations sur les systèmes de fichiers 194
 - 1.2.1 Opérations sous VirtualBox 194
 - 1.2.2 Opérations sous VMware 199
 - 1.2.3 Opérations sur un serveur physique..... 204
 - 1.3 Attributs spécifiques lsattr/chattr 213
 - 1.4 Amélioration du système de fichiers 215
 - 1.5 Chiffrer le système de fichiers 217

4 _____ Debian GNU/Linux

Vers une administration de haute sécurité

2.	Utilisateurs et groupes	219
2.1	Gestion des quotas	220
2.2	Limites utilisateurs	223
2.3	Notion de privilèges	225
2.4	Authentification standard	228
3.	Gestion de processus	231
3.1	Qu'est-ce qu'un processus ?	231
3.2	Sécurisation avec chroot	234
3.3	De l'utilisation des bibliothèques dynamiques	236
3.4	Confinement de processus	237
3.4.1	SELinux	238
3.4.2	cgroups	245
4.	Sécurisation des accès utilisateurs	247
4.1	SSH	248
4.2	PAM	255
4.3	Patch GRSEC	259
5.	Gestion de notifications et des variables	260
5.1	Notifications à l'utilisateur	260
5.2	Environnement utilisateur (/etc/skel)	261
5.3	Configuration générale et paramétrage	262
6.	Gestionnaire de fenêtre	264
6.1	Display manager	265
6.2	Fonctionnalités Xauth	266
6.3	Tunnel X11	267
7.	Gestion des menus	268
7.1	Personnalisation	268
7.2	Sécuriser XWindow avec ldm	270
7.3	Que faire en cas d'attaque ?	270

Chapitre 5

Sécurisation du système

1.	Gestionnaire de paquets	271
1.1	Outils à disposition	272
1.1.1	Outil dpkg	272
1.1.2	Outil dselect	273
1.1.3	Outil aptitude	275
1.2	Utilisation avancée d'aptitude	277
2.	Agents de support constructeur	282
3.	Outils de soumission de tâches	284
3.1	Outil at	285
3.2	Outil cron	286

3.3	Mise à jour sécurité via cron-apt	288
4.	Gestion des journaux et traces système	290
4.1	Système courant de logs	290
4.2	Personnaliser logcheck	294
4.3	Utilisation d'un hôte d'archivage centralisé	296
4.4	Centralisation des journaux de trace avec logAnalyzer	299
5.	Dépannage	307
6.	Déclaration et remontée de bugs	308
6.1	Remontée d'un nouveau bug	308
6.2	Modification de rapport	311
6.3	Suivi de version	311
6.4	Intégrité et reporting	313
7.	Installation d'un bastion harden	314
7.1	La suite harden	314
7.2	L'outil tripwire	315
7.3	Configuration de tripwire	319

Partie 3 : L'infrastructure

Chapitre 6

Sécurisation du réseau

1.	Configuration d'interface réseau	323
1.1	Configuration du réseau	323
1.2	Pare-feu netfilter	332
1.2.1	Les tables netfilter	332
1.2.2	Les chaînes netfilter	333
1.2.3	Les actions netfilter	333
1.2.4	Le traitement des règles netfilter	333
1.3	Le réseau et ses routes	336
1.4	La commande netstat	338
1.5	Les outils réseau	338
2.	Mise en œuvre du bonding	341
3.	Sécurisation des ports de service	345
3.1	Scan des ports d'écoute avec nmap	345
3.2	Mise en place d'un wrappers	346
4.	Partages Linux	347
4.1	Paramétrage serveur	347
4.2	Paramétrage client	349
5.	Partages hétérogènes depuis Windows	351
5.1	Montages samba	351
5.2	Montages cifs	354
5.3	Mise en œuvre de Samba 4	356

6 --- Debian GNU/Linux

Vers une administration de haute sécurité

5.4	Administration de Samba 4	361
6.	Configuration des transferts de fichiers	364
6.1	Installation et configuration de vsftpd	365
6.2	Utilisation de comptes virtuels	370
6.3	Chiffrement SSL	372
6.4	Configuration pour Internet	374
7.	Réseaux et connexions sans fil	375
7.1	Les modes de fonctionnement du Wi-Fi (802.11)	375
7.1.1	Le mode infrastructure	376
7.1.2	Le mode ad-hoc	377
7.2	Installation d'outils	378
7.3	Configuration de carte Wi-Fi	379
7.4	Installation et configuration Bluetooth	381

Chapitre 7

Sécurité et services d'infrastructure

1.	Mise en œuvre d'OpenSSH	383
1.1	Cryptographie asymétrique	383
1.2	Service de transfert de fichiers sftp	386
1.3	Authentification par clé SSH	388
1.4	Copie de fichiers sécurisée	390
1.5	Sécurisation de commandes via ssh	392
1.6	Tunnel SSH	392
1.6.1	Tunnel socks	393
1.6.2	Tunnel par port	393
1.6.3	Tunnel X	394
1.6.4	Tunnel IP	395
1.7	Utilisation d'OpenSSL	395
1.7.1	Installation d'une autorité de certification	395
1.7.2	Gestion de certificats d'une autorité de certification	398
1.7.3	Génération de certificat pour un serveur	399
2.	Sécurisation du serveur de noms DNS	401
2.1	Généralités sur le serveur de noms	401
2.2	Attaques visant le serveur de noms	402
2.3	Recommandations générales	403
2.3.1	Opter pour la redondance	403
2.3.2	Veiller à tenir à jour la version	403
2.3.3	Effectuer une surveillance accrue	403
2.3.4	Sécuriser les flux d'échanges	404
2.3.5	Prévoir un plan de reprise	404
2.4	Mise en œuvre d'un serveur DNS simple	404

- 2.5 Emprisonnement du serveur de noms 407
- 2.6 Création d'un serveur secondaire 409
- 2.7 Mise en place du protocole TSIG 413
- 2.8 Utilisation de DNSSEC..... 415
- 3. Mise en œuvre d'un annuaire OpenLDAP 418
 - 3.1 Architecture d'un annuaire LDAP 418
 - 3.2 Sécurité d'utilisation 422
 - 3.2.1 Authentification 422
 - 3.2.2 Contrôle d'accès 423
 - 3.3 Sécurisation du backend 424
 - 3.4 Installation d'un serveur LDAP minimal 426
 - 3.5 Gestion des schémas 435
 - 3.6 Réplication des données 436
 - 3.7 Chiffrement des échanges 439
- 4. Alternative de l'annuaire LDAP : NIS 443
 - 4.1 Service NIS 443
 - 4.2 Restriction d'utilisateurs ou de groupes 446
 - 4.3 Sécurisation du service NIS 447
 - 4.4 Initialisation d'un serveur NIS esclave 448
- 5. Service d'adressage dynamique DHCP 448
 - 5.1 Sécurisation du service DHCP 450
 - 5.2 Utilisation du failover 451
- 6. Service de messagerie postfix..... 452
 - 6.1 Agents de messagerie 452
 - 6.2 Installation basique 453
 - 6.3 Déport de postfix et configuration 457
 - 6.4 Ajout de la gestion MySQL 459
 - 6.5 Installation de SASL 462
 - 6.6 Installation de SpamAssassin..... 465
 - 6.7 Utilisation de GnuPG 466
- 7. Administration graphique Webmin 473
 - 7.1 Installation et configuration de Webmin 473
 - 7.2 Sécurisation de l'outil 474

Partie 4 : Les applications

Chapitre 8

Sécurisation des bases de données

- 1. PostgreSQL 479
 - 1.1 Généralités et installation..... 479
 - 1.1.1 Introduction 479
 - 1.1.2 Installation 479

8 **Debian GNU/Linux**

Vers une administration de haute sécurité

1.1.3	Architecture du moteur PostgreSQL	480
1.2	Paramétrage et initialisation	481
1.3	Axes de sécurisation	484
1.3.1	Restriction de connexions	484
1.3.2	Ouverture de flux	485
1.3.3	Sauvegardes	485
1.3.4	Chiffrement	488
1.3.5	Réplication	492
1.4	Points faibles	493
2.	Oracle MySQL	494
2.1	Généralités et installation	494
2.1.1	Introduction	494
2.1.2	Installation	495
2.1.3	Architecture du moteur MySQL	495
2.2	Paramétrage et initialisation	496
2.3	Axes de sécurisation	501
2.3.1	Optimiseur MySQLTuner	501
2.3.2	Administration et outils	501
2.3.3	Réplication de bases	507
2.3.4	Amélioration des sauvegardes/restaurations	511
2.3.5	Réinitialisation du mot de passe root	513
2.3.6	Limitation du nombre de connexions utilisateurs	513
2.3.7	Optimisation et caches	514
2.4	Points faibles	515
3.	MariaDB	516
3.1	Généralités et installation	516
3.1.1	Introduction	516
3.1.2	Installation	516
3.2	Paramétrage et initialisation	518
3.3	Axes de sécurisation	519
3.3.1	Réinitialisation du mot de passe root	519
3.3.2	Restriction d'accès extérieurs	520
3.3.3	Migration MySQL vers MariaDB	520
4.	SQLite	522
4.1	Généralités et installation	522
4.1.1	Introduction	522
4.1.2	Installation	523
4.2	Utilisation et optimisation	523
4.2.1	Manipulation des commandes	523
4.2.2	Manipulation des objets	524
4.2.3	Optimisations	526

- 4.3 Axes de sécurisation 526
 - 4.3.1 Restriction d'accès 526
 - 4.3.2 Installation de SQLCipher 526
 - 4.3.3 Intégration dans les applications web 527
- 4.4 Points faibles 528
- 5. NoSQL..... 529
 - 5.1 Généralités et installation 529
 - 5.1.1 Introduction 529
 - 5.1.2 Mise en œuvre de MongoDB 530
 - 5.1.3 Manipulation sous MongoDB 531
 - 5.2 Axes de sécurisation 533
 - 5.3 Points faibles 535
- 6. Oracle 535
 - 6.1 Généralités et installation 535
 - 6.1.1 Architecture Oracle 536
 - 6.1.2 Mise en œuvre d'Oracle Express 538
 - 6.1.3 Réglages et tuning sous Oracle 541
 - 6.2 Axes de sécurisation 543
 - 6.3 Points faibles 553
- 7. Firebird 553
 - 7.1 Généralités et installation 553
 - 7.2 Axes de sécurisation 558
 - 7.3 Points faibles 559

Chapitre 9
Sauvegardes

- 1. Fonction élémentaire 561
 - 1.1 Architecture AMANDA 563
 - 1.2 Vérification des bandes 565
 - 1.3 Configuration du serveur 565
 - 1.4 Configuration des clients 570
 - 1.5 Utilitaire de restauration amrecover 573
 - 1.6 Solution alternative : Backup-PC 574
 - 1.6.1 Sauvegarde de postes Windows 576
 - 1.6.2 Sauvegarde de postes Linux 577
 - 1.6.3 Sauvegarde de postes éteints 582
 - 1.6.4 Changement de répertoire de sauvegarde 583
- 2. Gestionnaire de récupération 584
 - 2.1 Image ISO Clonezilla Live 584
 - 2.2 Le fichier de menus 585
 - 2.3 Les fonctions d'accès aux images ISO 587

2.4	Le fichier de personnalisation	588
3.	Gestionnaire de clonage	598
3.1	Installation	598
3.2	Utilisation et sauvegarde	599
3.3	Méthode de restauration	603
4.	Sauvegarde d'entreprise	605
4.1	Solution BACULA	605
4.2	Installation	606
4.3	Configuration des services	608
4.3.1	Service de stockage	608
4.3.2	Service du directeur	609
4.3.3	Configuration des clients	615
4.4	Installation d'OpenMediaVault	615
4.4.1	Emprisonnement d'OpenMediaVault	616
4.4.2	Installation d'OpenMediaVault	617
4.4.3	Installation alternative	619
5.	Sauvegardes et synchronisations avancées	627
5.1	Utilitaire rsync	627
5.2	Interface graphique grsync	629
5.3	Alternative avancée unison	631
6.	Sauvegardes différentielles	634
6.1	Installation et utilisation	634
6.2	Restauration	636
6.3	Solution alternative : Areca	636
7.	Plan de reprise informatique	642
7.1	Définitions et méthodes	642
7.2	Politique de sauvegarde	644
7.3	Sauvegardes dans les nuages	645
7.3.1	Fonctionnalités	645
7.3.2	Mise en œuvre d'une stratégie	647
7.3.3	Comment restaurer	649
7.4	Conclusion	650

Chapitre 10

Sécurité des applications

1.	Vérification des rootkits	651
2.	Surveillance des journaux de traces	657
3.	Attaques brute force et déni de services	664
3.1	Installation et paramétrage	664
3.1.1	Protection contre les attaques brute force	665
3.1.2	Protection contre les attaques DoS	665

3.2	Interface cliente	667
3.3	Configuration fail2ban avancée	667
3.4	Interface web	669
4.	Serveur d'impression	671
4.1	Généralités	671
4.2	Installation	672
4.3	Utilisation	673
4.4	Sécurisation	678
5.	Serveur web	680
5.1	Généralités	680
5.2	Vérification des prérequis	681
5.3	Installation et paramétrage	682
5.4	Sécurisation	686
5.4.1	Points basiques	686
5.4.2	Limitation des informations diffusées	686
5.4.3	Limitation des accès	688
5.4.4	Limitation des modules	689
5.4.5	Fichier .htaccess	690
5.4.6	Limitation des attaques DoS	691
5.5	Chiffrement et certificat	696
6.	Mise en œuvre d'un domaine Kerberos	698
6.1	Principe et généralités	698
6.2	Installation et paramétrage	700
6.3	Tests initiaux	702
6.4	Kerberisation des services	704
6.4.1	Support Kerberos	704
6.4.2	Support PAM	707
6.4.3	Configuration des clients Kerberos	708
6.4.4	Cadre d'utilisation	708
7.	Mise en œuvre d'OpenVPN	710
7.1	Généralités	710
7.2	Installation et configuration	711
7.2.1	Prérequis	711
7.2.2	Infrastructure à clés publiques	712
7.2.3	Démarrage du service OpenVPN	720

Partie 5 : La surveillance**Chapitre 11****Supervision**

1. Gestion locale	721
1.1 Principe d'action	721
1.2 Installation de Glances	722
1.3 Configuration de Glances	724
2. Visualisation des métriques du système	726
2.1 Description	726
2.2 Installation	728
2.2.1 Utilisation des sources	728
2.2.2 Installation du package web frontal	729
2.3 Configuration	730
2.3.1 Le fichier gmetad.conf	730
2.3.2 Le fichier gmond.conf	731
2.4 Sécurisation	732
2.4.1 Les flux unicast	733
2.4.2 Option deaf	733
2.4.3 Mise en œuvre d'ACL	734
2.4.4 Interface web	734
2.5 Personnalisation de métriques	735
2.6 État et statistiques	737
2.7 Alternative légère	738
2.7.1 Installation	738
2.7.2 Initialisation	740
2.7.3 Configuration	743
3. Supervision historisée	745
3.1 Généralités	745
3.2 Comment ça marche ?	746
3.3 Installation	746
3.4 Configuration	747
3.4.1 Côté serveur	747
3.4.2 Côté client	753
3.5 Avantages et inconvénients	754
4. Supervision orientée métier	754
4.1 Présentation	754
4.2 Installation	755
4.3 Configuration	758
5. Supervision générique	761
5.1 Généralités	761
5.2 Prérequis d'installation	762

- 5.3 Installation et configuration 762
- 6. Diagnostic réseau et sniffers 767
 - 6.1 Outil netstat 768
 - 6.2 Outil tcpdump 770
 - 6.3 Outil ntop 772
 - 6.4 Outil wireshark 776

Chapitre 12
Sécurité

- 1. Système antiviral 781
 - 1.1 Généralités 781
 - 1.2 Installation d'Avast pour station 782
 - 1.3 Autres solutions pour stations Linux 786
 - 1.4 Solution open source 792
- 2. Mise en œuvre de proxy 793
 - 2.1 Généralités 793
 - 2.2 Le proxy squid 795
 - 2.3 Le proxy HAProxy 800
 - 2.4 Le proxy SOCKS 803
- 3. Serveur d'audit 807
 - 3.1 Le framework W3AF 807
 - 3.2 L'outil Helix 813
 - 3.3 L'audit Lynis 819
 - 3.4 Audit interne 821
- 4. Serveur pot de miel 824
- 5. Scrutation de proximité 827
- 6. Système de détection d'intrusion 830
 - 6.1 IDS SNORT 831
 - 6.2 HIDS AIDE 834
 - 6.3 IDS OpenVAS 836
 - 6.4 IDS hybride Prelude 839
- 7. Système de wrappers TCP 845

Partie 6 : La haute disponibilité

Chapitre 13

Haute disponibilité et virtualisation

- 1. SAN et multipathing 851
 - 1.1 Architecture à mettre en œuvre 851
 - 1.1.1 Architecture réseau 851
 - 1.1.2 Architecture SAN 852
 - 1.1.3 Déclaration d'un serveur 854

1.1.4	Le multipathing sur un serveur Debian	856
1.2	Installation du multipath et configuration	856
1.3	Sauvegardes et synchronisation	860
2.	Réplication de bases de données	864
2.1	Installation	864
2.2	Utilisation et configuration	865
2.3	Système maître/esclave : londiste	869
3.	Synchronisation des disques	873
3.1	Installation et configuration	874
3.2	Dépannage en cas de défaillance	876
4.	Système de distribution	877
4.1	Installation et configuration xcat	877
4.2	Installation et configuration FAI	883
5.	Mise en cluster	887
5.1	Utilisation de LVS	888
5.2	Utilisation de KeepAlived	890
5.3	Utilisation de heartbeat	894
6.	Équilibrage de charge	895
6.1	Installation	895
6.2	Configuration	900
7.	Mise en œuvre de qualité de service	906
7.1	Généralités	906
7.2	Approche directe	907
7.3	Mise en œuvre de trickle	908

Conclusion

1.	Autour de la sécurité	911
2.	Un mot sur Linux Debian	912
3.	Pour conclure	913

Index	915
-----------------	-----

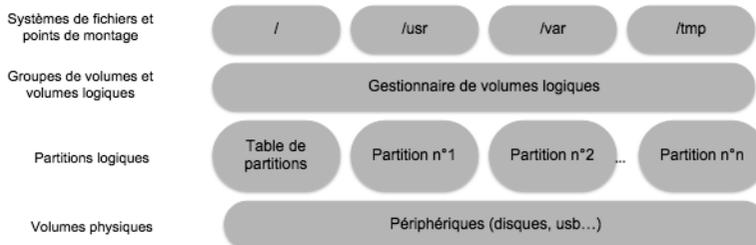
Chapitre 4

Sécurisation de l'environnement

1. Systèmes de fichiers

1.1 Présentation et types

Il a été vu dans les chapitres précédents comment les périphériques étaient partitionnés afin de présenter les données stockées sur les volumes logiques. Ces derniers doivent être présentés à leur point de montage pour pouvoir accéder aux informations s'y trouvant.



Donc, les données sont accessibles aux utilisateurs ainsi qu'aux programmes via une architecture structurée, selon un modèle arborescent de répertoires et de fichiers. On appelle système de fichiers le format de présentation de ces données sous forme de succession de blocs organisés.

Les formats les plus courants sur des systèmes GNU/Linux sont ext2, ext3 et ext4. Mais, il faut aussi souligner que les lecteurs CD/DVD ont leur propre système de fichiers :

- Système de fichiers ISO9660 (pour les lecteurs CD et les formats Joliet et Rock Ridge).
- Système de fichiers *Universal Disk Format* ou UDF (pour les lecteurs DVD).

Voici quelques systèmes de fichiers bien connus pour être utilisés sous Linux Debian :

Nom FS	Commentaire
ext2	Système de fichiers initial (pas de journalisation).
ext3	Système de fichiers évolués (avec journalisation).
ext4	Système de fichiers journalisé étendu à 1024 Po.
btrfs	Amélioration d'ext4 16 Eo basé sur les références arrière (back reference) pour la protection des données et la compression.

Lorsque l'on a créé les volumes logiques à l'aide de la commande `lvcreate`, il devient alors possible de créer un ou plusieurs systèmes de fichiers. Pour cela, il suffit d'utiliser la commande `mkfs`. En réalité, cette commande est une interface permettant de formater le système de fichiers selon le type souhaité : `ext2`, `ext3`, `btrfs` ou autres.

Option	Format long	Commentaire
<code>-V</code>	<code>--version</code>	Permet de lister toutes les commandes exécutées.
<code>-t <Type></code>	<code>--type</code>	Indique le type de système de fichiers à créer.
<code>-v</code>	<code>--verbose</code>	Affiche plus d'informations (mode verbeux).
<code>-b</code>		Donne la taille en blocs multiples de 512 octets.
<code>-c</code>		Vérifie les blocs défectueux avant la création du système de fichiers.
<code>-i</code>		Fournit le ratio octets/inodes.
<code>-m</code>		Vérifie les blocs défectueux avant la création du système de fichiers.
<code>-L</code>		Décrit le label du système de fichiers.
<code>-J</code>		Permet de créer une journalisation au système de fichiers (pour <code>ext2</code>).

Lorsque l'on précise un type de système de fichiers, le programme fait alors appel à une commande dédiée au formatage :

- `mkfs.ext2`
- `mkfs.ext3`
- `mkfs.ext4`
- ...

Ensuite, lorsque le système de fichiers est créé, on peut générer un point de montage : généralement un répertoire suffit, pour monter le périphérique de type bloc, ou la partition, sur laquelle le système de fichiers existe. La commande `mount` permet d'attacher le répertoire racine du système de fichiers, au répertoire appelé « point de montage ».

Chaque montage réussi provoque l'écriture d'une ligne correspondante dans le fichier `/etc/mtab`.

```
root@Philo:/home/uadmin# more /etc/mtab
rootfs / rootfs rw 0 0
sysfs /sys sysfs rw,nosuid,nodev,noexec,relatime 0 0
proc /proc proc rw,nosuid,nodev,noexec,relatime 0 0
udev /dev devtmpfs rw,relatime,size=10240k,nr_inodes=30340,mode=755 0 0
devpts /dev/pts devpts rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000 0 0
tmpfs /run tmpfs rw,nosuid,noexec,relatime,size=25444k,mode=755 0 0
/dev/mapper/Philo-root / ext4 rw,relatime,errors=remount-ro,user_xattr,barrier=1,data=ordered 0 0
tmpfs /run/lock tmpfs rw,nosuid,nodev,noexec,relatime,size=5120k 0 0
tmpfs /run/shm tmpfs rw,nosuid,nodev,noexec,relatime,size=50880k 0 0
/dev/sdal /boot ext2 rw,relatime,errors=continue 0 0
/dev/mapper/Philo-home /home ext4 rw,relatime,user_xattr,barrier=1,data=ordered 0 0
/dev/mapper/Philo-tmp /tmp ext4 rw,relatime,user_xattr,barrier=1,data=ordered 0 0
/dev/mapper/Philo-usr /usr ext4 rw,relatime,user_xattr,barrier=1,data=ordered 0 0
/dev/mapper/Philo-var /var ext4 rw,relatime,user_xattr,barrier=1,data=ordered 0 0
rpc_pipefs /var/lib/nfs/rpc_pipefs rpc_pipefs rw,relatime 0 0
binfmt_misc /proc/sys/fs/binfmt_misc binfmt_misc rw,nosuid,nodev,noexec,relatime 0 0
```

Les informations concernant les différents montages peuvent être consultées dans le fichier `/proc/mounts`. Il s'agit d'une copie virtuelle du fichier `mtab`.

L'ordre de montage répond à une syntaxe bien particulière permettant de monter aussi bien des systèmes de fichiers à partir de périphérique, de label ou encore d'identifiant :

```
# mount -t ext4 /dev/sdb1 /mnt/data
# mount -t ext4 -L DATA /data2
# mount -t ext3 -U 66f6ce4b8-635c-4103-9a81-977fb7bb29fe /home
```

L'ensemble des ordres de montages peuvent être effectués automatiquement dès lors que leurs paramètres sont indiqués dans le fichier `/etc/fstab`.

Ce dernier contient les noms des périphériques et leur point de montage et les options du montage à réaliser. Le format de ce fichier est le suivant :

Champ	Commentaire
Périphérique	Périphérique à monter. Cela peut être sous forme de nom, de label ou d'UUID.
Point de montage	Répertoire d'accès au système de fichiers monté
Type de système	Type du système de fichiers : ext2, ext3, ext4...
options	Options de montage, séparées par des virgules.
dump	Fréquence de dump pour les outils de sauvegarde système.
fsck	Fréquence de vérification fsck du système : 0 = à ignorer, 1 = en premier, 2 = en second... Les systèmes de même valeur sont parallélisés.

Pour monter l'ensemble des partitions proposées dans le fichier `/etc/fstab`, on peut exécuter la commande suivante :

```
# mount -a
```

A contrario, il est possible de monter un volume unitaire en le précisant derrière la commande `mount` :

```
# mount /data
Pour réaliser un démontage, on peut alors invoquer la commande
umount de la façon suivante :
# umount /mnt/perso
```

Remarque

Toutefois, il n'existe pas de commande permettant le démontage de l'intégralité des partitions.

Il existe de nombreuses options concernant les montages et leurs propriétés et permettant de sécuriser les accès :

Option	Commentaire
<code>defaults</code>	Reprend l'ensemble des options : <code>rw</code> , <code>suid</code> , <code>dev</code> , <code>exec</code> , <code>auto</code> , <code>noauto</code> et <code>async</code> .
<code>sync/async</code>	Active ou désactive les écritures synchrones. Ceci est préférable avec des supports externes.
<code>exec/noexec</code>	Exécute (ou non) les fichiers binaires sur le support.
<code>noatime</code>	Empêche la mise à jour de l'horodatage lors de chaque accès aux fichiers. Cette option est utile pour des supports externes, des pages web ou des forums de news.
<code>auto/noauto</code>	Monte automatiquement (explicitement depuis <code>fstab</code>) le système de fichiers.
<code>user/nouser</code>	Autorise (ou non) les utilisateurs standards à effectuer les montages.
<code>remount</code>	Autorise la remontée du système afin de prendre en compte de nouvelles options.
<code>ro/rw</code>	Réalise le montage en lecture seule ou en lecture-écriture.
<code>dev/nodev</code>	Permet d'interpréter (ou non) les fichiers spéciaux.
<code>noload</code>	Évite de charger le journal (valable pour les systèmes de fichiers journalisés).
<code>usrquota/grpquota</code>	Permet d'être ignorée par l'option du système de fichiers et n'est prise en compte que par le sous-système de gestion de quotas.
<code>acl</code>	Autorise l'utilisation de contrôle d'accès (ou <i>Access Control Lists</i>).
<code>user_xattr</code>	Accepte les attributs étendus sur les fichiers : encodage de texte, champs d'indexation... (valable pour les systèmes de fichiers <code>ext3</code> , <code>ext4</code> ...).
<code>umask</code>	Permet pour les systèmes de fichiers NAT/NTFS d'appliquer un masque différent de la valeur par défaut.

Lorsque l'on effectue le montage d'un système de fichiers utilisant l'option `sync`, cela permet de s'affranchir de toute forme de cache en écriture attachée au disque. Cela permet alors de fiabiliser les opérations d'écritures. En fait, cette option permet de vider ponctuellement le cache sur un système de fichiers ne bénéficiant pas de cette option de montage. Lorsqu'un système de fichiers est en cours, il est possible d'avoir des informations concernant le processus actif sur tel ou tel point de montage. Il suffit juste d'utiliser la commande `lsdf`, permettant de lister les sockets ou les processus attachés à un fichier ou un point de montage, en l'occurrence :

```
root@Philo:/home/uadmin# lsdf /tmp
COMMAND  PID  USER  FD  TYPE  DEVICE  SIZE/OFF  NODE NAME
gnome-ter 3259 uadmin 17w  REG  254,5   9437    14 /tmp/vteI1ARJX (deleted)
gnome-ter 3259 uadmin 18u  REG  254,5   1504    18 /tmp/vte8LARJX (deleted)
```

Lorsqu'un point de montage semble occupé et qu'il n'est alors pas possible de libérer la ressource, on peut interroger le point de montage à l'aide de la commande `fuser` pour forcer la libération du point de montage et démonter celui-ci :

```
■ # fuser -km /mnt/data
```

On peut également modifier certains paramètres du système de fichiers en utilisant la commande `tune2fs` :

```
■ # tune2fs -j /dev/sdb1 (pour journaliser le système de fichiers)
■ # tune2fs -O^has_journal /dev/sdb1 (pour supprimer la
journalisation)
```

ou encore `e2label`, permettant de générer un label à un système de fichiers existant :

```
■ # e2label /dev/sdb1 LABEL
```

■ Remarque

La commande seule avec le nom du périphérique permet de lister le label du système pour ce même périphérique :

```
■ # e2label /dev/sdb1
```

ATTENTION : ces commandes sont propres au type du système de fichiers manipulé. En effet, pour un système `reiserfs`, la commande sera plutôt `reiserfstune`.

La commande `tune2fs` est très complète et permet de réaliser de nombreuses tâches. Voici les options principales :

Option	Commentaire
<code>-c <N></code>	Détermine le nombre de montages avant lequel la vérification <code>fsck</code> sera effectuée. La valeur 0 permet de désactiver cette vérification automatique.
<code>-i <N></code>	Représente l'intervalle entre deux vérifications <code>fsck</code> : d(ay), w(eek), m(onth). Par défaut l'unité est le jour.
<code>-j</code>	Active la journalisation (valable uniquement sur des systèmes non journalisés).

Option	Commentaire
-L	Modifie le label.
-e <Err>	Permet de décrire le comportement du noyau en cas d'erreur. Les valeurs sont continue, panic et remount-ro. Par défaut, la valeur est continue.
-m <N>	Permet d'empêcher le remplissage du système de fichiers en laissant (par défaut) 5 % de réservation au système afin de laisser travailler les daemons klogd et syslogd.
-o ^	Ajoute ou supprime l'option de montage indiquée (voir ci-dessus pour la journalisation).
-u <UUID>	Modifie la valeur de l'UUID selon un format hexadécimal. On peut le supprimer avec l'option clear ou en générer un nouveau avec l'option random.
-s [0 1]	Active ou désactive le bit <i>sparse super feature</i> sur les disques de grande taille. En activant cette option, on réduit le nombre de blocs de secours et on optimise ainsi l'espace occupé sur les disques.
-l	Liste la configuration et le paramétrage d'un périphérique.

Exemple : configuration du système de fichiers /dev/sda1

```

root@Philo:/home/uadmin# tune2fs -l /dev/sda1
tune2fs 1.42.5 (29-Jul-2012)
Filesystem volume name: <none>
Last mounted on: <not available>
Filesystem UUID: 33936108-2eb9-44dd-a5a0-ae6447566f4a
Filesystem magic number: 0xEF53
Filesystem revision #: 1 (dynamic)
Filesystem features: filetype sparse_super
Default mount options: (none)
Filesystem state: not clean
Errors behavior: Continue
Filesystem OS type: Linux
Inode count: 124496
Block count: 248832
Reserved block count: 12441
Free blocks: 215303
Free inodes: 124256
First block: 1
Block size: 1024
Fragment size: 1024
Blocks per group: 8192
Fragments per group: 8192
Inodes per group: 4016
Inode blocks per group: 502
Last mount time: n/a
Last write time: Mon Aug 4 18:02:19 2014
Mount count: 9
Maximum mount count: 30
Last checked: Thu Jan 1 01:00:00 1970
Check interval: 0 (<none>)
Reserved blocks uid: 0 (user root)
Reserved blocks gid: 0 (group root)
First inode: 11
Inode size: 128

```