

Avant-propos

Chapitre 1

Démarrage du système

- 1. Démarrage du système 29
 - 1.1 Personnalisation du démarrage du système 29
 - 1.1.1 Compétences principales..... 29
 - 1.1.2 Éléments mis en œuvre 30
 - 1.2 Récupération du système..... 30
 - 1.2.1 Compétences principales..... 30
 - 1.2.2 Éléments mis en œuvre 31
 - 1.3 Chargeurs d'amorçage alternatifs 31
 - 1.3.1 Compétences principales..... 31
 - 1.3.2 Éléments mis en œuvre 31
- 2. Personnalisation du démarrage du système..... 32
 - 2.1 init System V 32
 - 2.2 Le processus init 33
 - 2.2.1 Processus enfants d'init 33
 - 2.2.2 Configuration du processus init 33
 - 2.3 Les niveaux d'exécution init System V 35
 - 2.3.1 Les différents niveaux d'exécution (run levels) 36
 - 2.3.2 Configuration des différents niveaux d'exécution..... 37
 - 2.3.3 Scripts de gestion des services..... 37
 - 2.3.4 Niveaux d'exécution et services 39
 - 2.4 Gestion des niveaux d'exécution init system V 40
 - 2.4.1 Niveau d'exécution courant 40
 - 2.4.2 Changer de niveau d'exécution..... 41
 - 2.4.3 Commandes de gestion du contenu des niveaux d'exécution . 41
 - 2.4.4 Script indépendant du niveau d'exécution : /etc/rc.local 42
 - 2.5 systemd 42
 - 2.5.1 Démarrage de systemd 42
 - 2.5.2 Répertoire de travail de systemd 44
 - 2.5.3 Répertoires de configuration de systemd..... 45
 - 2.5.4 La commande systemctl 46

2.6	Les cibles systemd	46
2.6.1	Cible par défaut	47
2.6.2	Configuration des cibles	48
2.6.3	Cibles et niveaux d'exécution	49
2.6.4	Modifier la cible lors du chargement du noyau	49
2.7	Gestion des services par systemd	49
2.7.1	Liste et état des services	51
2.7.2	Démarrage et arrêt des services	52
2.7.3	Activation et désactivation des services	53
2.7.4	Journal de systemd	53
2.8	Arrêt et redémarrage du système par systemd	54
3.	Récupération du système	54
3.1	Amorçage du système	55
3.1.1	BIOS	55
3.1.2	UEFI	55
3.1.3	NVMe	56
3.2	Le gestionnaire de démarrage GRUB	56
3.2.1	Configuration de GRUB Legacy	57
3.2.2	Configuration de GRUB 2	58
3.2.3	Configuration de GRUB 2 en mode UEFI	60
3.2.4	Utilisation de GRUB en mode interactif	61
3.2.5	Réinstallation depuis un système non démarrable	61
3.2.6	Shell de secours au démarrage	61
3.2.7	Modes systemd rescue et emergency	62
4.	Chargeurs d'amorçage alternatifs	62
4.1	SYSLINUX et EXTLINUX	63
4.2	ISOLINUX	63
4.3	PXELINUX	64
4.4	systemd-boot	65
4.5	U-Boot	65

Chapitre 2

Systèmes de fichiers et périphériques

1. Système de fichiers et périphériques	67
1.1 Administration du système de fichiers Linux	67
1.1.1 Compétences principales	67
1.1.2 Éléments mis en œuvre	67
1.2 Maintenance du système de fichiers Linux	68
1.2.1 Compétences principales	68
1.2.2 Éléments mis en œuvre	68
1.3 Création et configuration de systèmes de fichiers optionnels	69
1.3.1 Compétences principales	69
1.3.2 Éléments mis en œuvre	69
2. Administration du système de fichiers Linux	69
2.1 Composants du système de fichiers Linux	70
2.2 Systèmes de fichiers physiques	70
2.3 Systèmes de fichiers virtuels	71
2.3.1 Le système de fichiers virtuel proc	71
2.3.2 Le système de fichiers virtuel sys	73
2.4 Identification des systèmes de fichiers	74
2.4.1 Fichier spécial en mode bloc	74
2.4.2 Label	74
2.4.3 UUID	75
2.4.4 Visualiser les identifiants	75
2.4.5 Gestion du label d'un système de fichiers	76
2.4.6 Gestion de l'UUID d'un système de fichiers	76
2.5 Montage et démontage des systèmes de fichiers	78
2.5.1 Configuration du montage des systèmes de fichiers	78
2.5.2 Monter un système de fichiers : mount	79
2.5.3 Démonteur un système de fichiers : umount	81
2.5.4 Suivi des systèmes de fichiers montés	83
2.5.5 Vidage des caches d'entrées-sorties	84
2.6 Montage par systemd	84
2.6.1 Unité de montage systemd	85
2.6.2 Activation de l'unité de montage	86
2.6.3 Montage/démontage manuel de l'unité de montage	86
2.6.4 Montage/démontage automatique de l'unité de montage	86

2.6.5	Exemples	86
2.7	Gestion des zones de swap	88
2.7.1	Taille de la zone de swap	89
2.7.2	Configuration du swap	90
2.7.3	Visualisation des espaces de swap	90
2.7.4	Activation d'un espace de swap	90
2.7.5	Désactivation d'un espace de swap	91
3.	Maintenance des systèmes de fichiers Linux	92
3.1	Création et contrôle des systèmes de fichiers	92
3.1.1	Création d'un système de fichiers : mkfs	93
3.1.2	Vérification des systèmes de fichiers	94
3.2	Création d'une zone de swap	95
3.2.1	Choix des espaces de swap	95
3.2.2	Nature de l'espace de swap	96
3.2.3	Création de l'espace de swap : mkswap	96
3.2.4	Contrôle du swap	98
3.3	Les principaux types de systèmes de fichiers Linux	98
3.3.1	Systèmes de fichiers de type ext*	98
3.3.2	Systèmes de fichiers de type XFS	99
3.3.3	Systèmes de fichiers de type Btrfs	100
3.3.4	Systèmes de fichiers de type ZFS	101
3.4	Gestion des systèmes de fichiers de type ext2, ext3 et ext4	103
3.4.1	Création d'un système de fichiers ext*	103
3.4.2	Vérification d'un système de fichiers ext*	105
3.4.3	Gestion des paramètres d'un système de fichiers avec tune2fs	105
3.4.4	Débogage d'un système de fichiers ext*	108
3.4.5	Sauvegarde de système de fichiers ext*	110
3.4.6	Restauration de système de fichiers ext*	111
3.5	Gestion de base des systèmes de fichiers de type Btrfs	113
3.5.1	Création de système de fichiers Btrfs	113
3.5.2	Conversion de système de fichiers ext* en Btrfs	114
3.5.3	Informations sur un système de fichiers Btrfs	115
3.5.4	Montage d'un système de fichiers Btrfs	117
3.5.5	Sous-volumes Btrfs	118
3.5.6	Instantanés Btrfs	120

3.6	Gestion des systèmes de fichiers de type XFS	122
3.6.1	Création de système de fichiers XFS	122
3.6.2	Gestion du label d'un système de fichiers XFS	123
3.6.3	Informations sur un système de fichiers XFS	123
3.6.4	Extension d'un système de fichiers XFS	124
3.6.5	Sauvegarde d'un système de fichiers XFS	125
3.6.6	Restauration d'un système de fichiers XFS	127
3.6.7	Réorganiser un système de fichiers XFS	129
3.6.8	Vérifier un système de fichiers XFS	130
3.6.9	Réparer un système de fichiers XFS	130
3.7	Surveillance des périphériques SMART	131
3.7.1	Le paquet smartmontools	131
3.7.2	Le daemon smartd	131
3.7.3	La commande smartctl	132
4.	Création et configuration de systèmes de fichiers optionnels	136
4.1	Service d'automontage	136
4.1.1	Configuration du service autofs/automount	137
4.1.2	Démarrage et arrêt du service	139
4.1.3	Exemple	140
4.2	Automontage par systemd	142
4.2.1	Unité de montage automatique systemd	142
4.2.2	Exemple de montage automatique par systemd	142
4.3	Systèmes de fichiers de périphériques amovibles	144
4.3.1	Lister les informations d'un CD-ROM/DVD	145
4.3.2	Copie d'un CD-ROM/DVD dans une image ISO	147
4.3.3	Création d'une image ISO	149
4.4	Chiffrement de systèmes de fichiers	151
4.4.1	Principes du chiffrement Linux	151
4.4.2	Chiffrement d'un fichier	152
4.4.3	Chiffrement de l'espace de stockage	154
4.4.4	Utilisation d'un espace de stockage chiffré	155
4.4.5	Chiffrement au niveau système de fichiers	156

Chapitre 3**Gestion des périphériques de stockage**

1. Gestion des périphériques de stockage	159
1.1 Configuration des disques RAID	159
1.1.1 Compétences principales	159
1.1.2 Éléments mis en œuvre	159
1.2 Optimiser l'accès aux périphériques de stockage	160
1.2.1 Compétences principales	160
1.2.2 Éléments mis en œuvre	160
1.3 Logical Volume Manager	160
1.3.1 Compétences principales	161
1.3.2 Éléments mis en œuvre	161
2. Configuration des disques RAID	161
2.1 Les principaux niveaux de RAID	162
2.1.1 Le RAID 0	162
2.1.2 Le RAID 1	162
2.1.3 Le RAID 5	163
2.2 Configuration du RAID	164
2.2.1 Création d'un volume RAID	164
2.2.2 Type de partition RAID	166
2.2.3 État d'un volume RAID	167
2.2.4 Arrêt et suppression d'un volume RAID	169
2.3 Exploitation d'un volume RAID	170
2.3.1 Remplacement d'un espace disque	170
2.3.2 Exemple d'utilisation d'un volume RAID 1	170
3. Optimiser l'accès aux périphériques de stockage	174
3.1 Gestion des disques durs locaux	174
3.1.1 Détermination des fichiers spéciaux	174
3.1.2 Le service udev	175
3.1.3 Interagir avec le service udev	175
3.1.4 Les liens symboliques dans /dev/disk	178
3.1.5 Le système de fichiers virtuel sysfs	179
3.1.6 La commande dmesg	180
3.1.7 Les commandes ls*	180

3.2	Gestion bas niveau des périphériques de stockage	182
3.2.1	La commande hdparm.	182
3.2.2	La commande sdparm	183
3.2.3	Gestion des disques SSD	184
3.2.4	Gestion des blocs défectueux	186
3.2.5	Identifiant SCSI.	186
3.3	Les réseaux de stockage SAN	187
3.4	Gestion des disques iSCSI	187
3.4.1	Terminologie	188
3.4.2	Paquets logiciels iSCSI.	189
3.4.3	Linux en tant que client iSCSI	190
3.4.4	Linux en tant que serveur iSCSI.	194
4.	Logical Volume Manager	198
4.1	Architecture des volumes logiques	199
4.2	Configuration du gestionnaire LVM.	200
4.3	Syntaxe générale des commandes LVM	203
4.4	Les volumes physiques	205
4.4.1	Création d'un volume physique	205
4.4.2	Informations sur les volumes physiques	206
4.4.3	Suppression d'un volume physique	208
4.5	Les groupes de volumes	208
4.5.1	Création d'un groupe de volumes	208
4.5.2	Informations sur les groupes de volumes.	210
4.5.3	Ajout/retrait d'un volume physique.	211
4.5.4	Suppression de groupes de volumes	214
4.6	Les volumes logiques	214
4.6.1	Création d'un volume logique.	214
4.6.2	Informations sur les volumes logiques.	217
4.6.3	Extension d'un volume logique.	219
4.6.4	Réduction d'un volume logique	220
4.6.5	Suppression de volumes logiques	222
4.6.6	Volumes logiques et système de fichiers	222
4.7	Instantané LVM (snapshot).	226
4.7.1	Création d'un volume logique instantané	226

Chapitre 4

Configuration du réseau

1.	Configuration du réseau	229
1.1	Configuration de base du réseau	229
1.1.1	Compétences principales	229
1.1.2	Éléments mis en œuvre	229
1.2	Configuration avancée du réseau	230
1.2.1	Compétences principales	230
1.2.2	Éléments mis en œuvre	230
1.3	Dépannage réseau	230
1.3.1	Compétences principales	231
1.3.2	Éléments mis en œuvre	231
2.	Configuration de base du réseau	232
2.1	Adresses IPv4 et IPv6	232
2.2	Paramétrage de base d'une connexion IPv4	233
2.2.1	Réseau/sous-réseau	233
2.2.2	Adresse IP	234
2.2.3	Masque de sous-réseau	234
2.2.4	Passerelle par défaut	234
2.3	Paramétrage de base d'une connexion IPv6	235
2.3.1	Adresse IPv6	235
2.3.2	Masque de sous-réseau	238
2.3.3	Passerelle par défaut	239
2.4	Configurer dynamiquement une interface réseau Ethernet	239
2.4.1	Nom d'une interface réseau	239
2.4.2	La commande ip	240
2.4.3	Gérer les adresses IP : ip address	242
2.4.4	Gérer les adresses IP : ifconfig	245
2.4.5	Configurer la passerelle par défaut : ip route	249
2.4.6	Configurer la passerelle par défaut : route	251
2.4.7	ping et ping6	253
2.4.8	Résolution d'adresse IPv4/MAC avec ARP	256
2.4.9	Résolution d'adresse IPv6/MAC avec NDP	258
2.5	Configurer une interface réseau sans fil	259
2.5.1	La commande iw	260
2.5.2	Les commandes iwconfig et iwlist	264

3.	Configuration avancée du réseau	265
3.1	Connexion à un réseau sans fil	266
3.1.1	Réseaux sans fil non sécurisés	266
3.1.2	Réseaux sans fil sécurisés	271
3.1.3	Configuration d'une connexion sécurisée WPA/WPA2	272
3.2	Connexion sur plusieurs réseaux	275
3.2.1	Configuration multi-réseau (multihomed)	276
3.2.2	Configuration d'une interface multi-réseau	278
3.2.3	Routage statique par un serveur multi-réseau	280
3.3	Outils de diagnostic et de suivi de l'activité réseau	283
3.3.1	Suivi de l'activité avec netstat	284
3.3.2	Suivi de l'activité avec ss	287
3.3.3	Suivi des sockets ouverts avec lsof -i	289
3.3.4	Tests de communication avec ncat (nc)	290
3.3.5	Tester les ports ouverts distants : la commande nmap	293
3.3.6	Capture du trafic réseau : tcpdump	297
4.	Dépannage du réseau	300
4.1	Le service NetworkManager	301
4.2	Configuration du démarrage du réseau	302
4.3	Configuration réseau de type Debian	303
4.3.1	Le fichier /etc/network/interfaces	303
4.3.2	Interface avec plusieurs adresses IP de même version	306
4.3.3	Démarrage du réseau par le script networking	307
4.4	Configuration réseau de type Red Hat	308
4.4.1	Les fichiers /etc/sysconfig/network-scripts/ifcfg*	308
4.4.2	Interface avec plusieurs adresses IP de même version	310
4.4.3	Démarrage du réseau	311
4.5	Contrôle du routage	312
4.5.1	Les commandes ip route et route	312
4.5.2	traceroute	313
4.6	Configuration de la résolution de noms d'hôtes	314
4.6.1	Configuration du nom d'hôte	314
4.6.2	Configuration de la résolution de noms	315
4.6.3	Configuration d'un client DNS	316
4.7	Restriction d'accès aux services réseau	317
4.7.1	Configuration de TCP Wrappers	318

4.8	Fichiers journaux.	319
4.8.1	Fichiers journaux du système	319
4.8.2	Le journal de systemd	320

Chapitre 5

Maintenance du système

1.	Maintenance du système.	323
1.1	Compilation et installation de programmes à partir des sources . . .	323
1.1.1	Compétences principales.	323
1.1.2	Éléments mis en œuvre	324
1.2	Sauvegardes	324
1.2.1	Compétences principales.	324
1.2.2	Éléments mis en œuvre	324
1.3	Informers les utilisateurs d'événements système	325
1.3.1	Compétences principales.	325
1.3.2	Éléments mis en œuvre	325
2.	Compilation et installation de programmes à partir des sources	325
2.1	Installation à partir de fichiers sources	326
2.1.1	Récupération des sources.	326
2.1.2	Décompression des sources	326
2.1.3	Restauration du fichier d'archivage.	327
2.1.4	Configuration de la compilation.	329
2.1.5	Compilation	333
2.1.6	Installation des exécutables.	335
2.1.7	Nettoyage des sources	337
2.1.8	Désinstallation d'un programme.	338
2.2	Installation de correctifs logiciels (patches)	339
3.	Sauvegardes	342
3.1	Que faut-il sauvegarder ?	342
3.1.1	Systèmes de fichiers.	342
3.1.2	Répertoires	343
3.2	Sur quels médias sauvegarder ?	344
3.2.1	Bande ou cartouche magnétique.	344
3.2.2	Disque dur	345
3.2.3	Disque optique.	345

- 3.2.4 Réseau 345
- 3.3 Stratégies de sauvegardes 346
- 3.4 Les commandes de sauvegarde et de restauration 347
 - 3.4.1 La commande tar 347
 - 3.4.2 La commande cpio 354
- 3.5 Les logiciels de sauvegarde 357
 - 3.5.1 Bacula et Bareos 357
 - 3.5.2 AMANDA 357
 - 3.5.3 BackupPC 357
 - 3.5.4 Logiciels commerciaux 357
- 3.6 Duplication de disque : la commande dd 358
- 3.7 Synchronisation de données : la commande rsync 359
 - 3.7.1 Syntaxe 360
 - 3.7.2 Exemple 360
- 4. Informer les utilisateurs 362
 - 4.1 Les fichiers /etc/issue et /etc/issue.net 362
 - 4.2 Le fichier /etc/motd 363
 - 4.3 La commande wall 364
 - 4.4 Prévenir avant l'arrêt du système 365
 - 4.4.1 Arrêt du système avec la commande shutdown 365
 - 4.4.2 Arrêt du système avec la commande systemctl 366

Chapitre 6
Le noyau Linux

- 1. Le noyau Linux 367
 - 1.1 Les composants du noyau 367
 - 1.1.1 Compétences principales 367
 - 1.1.2 Éléments mis en œuvre 367
 - 1.2 Compilation du noyau 368
 - 1.2.1 Compétences principales 368
 - 1.2.2 Éléments mis en œuvre 368
 - 1.3 Gestion et dépannage du noyau 369
 - 1.3.1 Compétences principales 369
 - 1.3.2 Éléments mis en œuvre 369

2.	Les composants du noyau	370
2.1	Le noyau	371
2.2	Les modules de noyau	371
2.3	Les versions du noyau	372
2.4	Les fichiers images du noyau	373
2.5	Le fichier disque virtuel complémentaire du noyau	374
2.6	La documentation du noyau	374
3.	Compilation du noyau	376
3.1	Téléchargement des sources du noyau	377
3.1.1	Paquet logiciel	377
3.1.2	Fichier archive compressé	379
3.2	Configuration et compilation du noyau	382
3.2.1	Nettoyage du répertoire de compilation	382
3.2.2	Génération du fichier de réponse	382
3.2.3	Exemple de configuration	383
3.2.4	Compilation du noyau	384
3.2.5	Compilation des modules de noyau	385
3.2.6	Gestion des modules de noyau par DKMS	386
3.3	Installation du nouveau noyau	386
3.3.1	Installation des modules	386
3.3.2	Installation du noyau	387
3.3.3	Création du fichier disque virtuel des modules	387
3.3.4	Configuration du gestionnaire de démarrage	388
4.	Gestion et dépannage du noyau	389
4.1	Gestion des modules de noyau LKM	390
4.1.1	Emplacement des modules	390
4.1.2	Liste des modules LKM chargés en mémoire	392
4.1.3	Déchargement d'un module	393
4.1.4	Chargement d'un module	394
4.1.5	Chargement des modules au démarrage du système	395
4.1.6	Configuration du chargement des modules	395
4.1.7	Installation manuelle d'un module LKM	395
4.1.8	Paramétrage des modules : modinfo, modprobe	396
4.2	Configuration dynamique via /proc/sys	397
4.3	La commande sysctl	400
4.3.1	Visualisation des paramètres du noyau et des modules	400
4.3.2	Modification des paramètres du noyau et des modules	401

Chapitre 7**Planification des ressources**

1. Planification des ressources.	403
1.1 Mesure de l'utilisation des ressources et dépannage.	403
1.1.1 Compétences principales.	403
1.1.2 Éléments mis en œuvre	404
1.2 Gestion prévisionnelle des ressources	404
1.2.1 Compétences principales.	404
1.2.2 Éléments mis en œuvre	405
2. Mesure de l'utilisation des ressources et dépannage	405
2.1 Types de ressources	405
2.2 Sources d'information sur les ressources.	405
2.2.1 Les pseudo-systèmes de fichiers proc et sysfs	405
2.2.2 Les journaux du système.	411
2.2.3 Les commandes de suivi instantané	412
2.3 Surveillance et suivi des ressources processeur.	413
2.3.1 Informations sur les ressources processeur	413
2.3.2 Utilisation des ressources processeur	416
2.3.3 Diagnostiquer une surutilisation du processeur	424
2.4 Surveillance et suivi de la mémoire vive	426
2.4.1 Informations sur la mémoire	426
2.4.2 Utilisation de la mémoire	427
2.4.3 Diagnostiquer une surconsommation de la mémoire	432
2.5 Surveillance et suivi des ressources disques	433
2.5.1 Informations sur les ressources disques	433
2.5.2 Utilisation des ressources disques.	440
2.6 Surveillance et suivi des ressources réseau	445
2.6.1 Informations sur les ressources réseau	446
2.6.2 Suivi et diagnostic des ressources réseau	448
3. Gestion prévisionnelle des ressources.	454
3.1 Le paquet sysstat	454
3.1.1 La collecte d'informations avec sysstat	454
3.1.2 La commande sar	454

3.2	Le démon collectd	456
3.2.1	Installation	457
3.2.2	Configuration	457
3.2.3	Exploitation des données de collectd	460
3.3	Les solutions de supervision	462

Chapitre 8

Domain Name Server

1.	Domain Name Server	465
1.1	Configuration de base d'un serveur DNS	465
1.1.1	Compétences principales	465
1.1.2	Éléments mis en œuvre	466
1.2	Création et gestion des zones DNS	466
1.2.1	Compétences principales	466
1.2.2	Éléments mis en œuvre	466
1.3	Sécuriser un serveur DNS	467
1.3.1	Compétences principales	467
1.3.2	Éléments mis en œuvre	467
2.	Configuration de base d'un serveur DNS	467
2.1	Principes de DNS	468
2.1.1	Clients et serveurs DNS	468
2.1.2	Noms de domaines complets (FQDN)	469
2.2	Les types de serveurs DNS	469
2.2.1	Serveur de noms DNS primaire ou secondaire	470
2.2.2	Serveur DNS de cache ou transitaire (forwarder)	470
2.2.3	Serveur de cache	470
2.2.4	Serveur transitaire (forwarder)	470
2.3	Gestion de l'arborescence DNS par les serveurs DNS	471
2.3.1	Autorité et délégation d'autorité	471
2.3.2	Les serveurs DNS de la racine (root servers)	471
2.3.3	Les domaines de premier niveau (Top Level Domains)	472
2.3.4	Le domaine de résolution inverse in-addr.arpa	472
2.4	Mécanisme de la résolution de noms	473
2.4.1	Exemple	474

- 2.5 Zones DNS 474
 - 2.5.1 Enregistrement de zone (type SOA)..... 475
 - 2.5.2 Enregistrements de ressources 475
 - 2.5.3 Zone de résolution inverse in-addr.arpa. 476
- 2.6 Les serveurs DNS sur Linux 476
 - 2.6.1 BIND..... 476
 - 2.6.2 Autres logiciels serveurs DNS..... 476
- 2.7 Configuration de base d'un serveur primaire DNS BIND 477
 - 2.7.1 Le fichier named.conf 477
 - 2.7.2 Les fichiers de zone par défaut 480
 - 2.7.3 Exemple 480
- 2.8 Configuration d'un serveur de cache ou transitaire 481
 - 2.8.1 Configuration du serveur de cache..... 481
 - 2.8.2 Configuration d'un serveur transitaire (forwarder)..... 482
- 2.9 Suivi d'un serveur DNS BIND 483
 - 2.9.1 Rechargement de la configuration du serveur 483
 - 2.9.2 Contrôle du fichier de configuration : named-checkconf 484
 - 2.9.3 La commande rndc 484
- 2.10 Test d'un serveur DNS BIND 486
 - 2.10.1 La commande host..... 486
 - 2.10.2 La commande dig..... 487
- 3. Création et gestion des zones DNS 489
 - 3.1 Fichier de zone de recherche 489
 - 3.1.1 Enregistrement de zone (type SOA)..... 490
 - 3.1.2 Enregistrements de ressources 492
 - 3.1.3 Exemple de fichier 493
 - 3.2 Fichier de zone de recherche inverse 494
 - 3.2.1 Déclaration de la zone dans named.conf 494
 - 3.2.2 Enregistrement SOA 494
 - 3.2.3 Enregistrements de ressources 494
 - 3.2.4 Exemple de fichier 495
 - 3.3 Gestion de zones secondaires..... 495
 - 3.3.1 Déclaration de la zone secondaire dans named.conf. 496
 - 3.4 Délégation de zone 496
 - 3.5 Contrôle d'un fichier de zone..... 497

3.6	Tests d'un serveur DNS	498
3.6.1	La commande nslookup	498
3.6.2	La commande dig	499
4.	Sécuriser un serveur DNS	502
4.1	Contrôle des clients autorisés	502
4.1.1	L'option allow-query	502
4.1.2	L'option blackhole	504
4.2	Utilisation d'un compte de service	505
4.3	BIND en mode chroot jail	506
4.3.1	Création de l'environnement nécessaire	506
4.3.2	Création de l'environnement chroot jail	507
4.3.3	Lancement du programme en mode chroot jail	507
4.4	Serveurs DNS fractionnés (split DNS)	508
4.5	Échange sécurisé entre serveurs DNS	509
4.6	Contrôle des transferts de zone	509
4.7	Transactions sécurisées TSIG	510
4.7.1	Génération de clés de transaction d'hôtes	510
4.7.2	Configuration de TSIG dans named.conf	511
4.8	DNSSEC	513
4.9	DANE	513

Chapitre 9

Services HTTP

1.	Services HTTP	515
1.1	Configuration de base d'un serveur Apache	515
1.1.1	Compétences principales	515
1.1.2	Éléments mis en œuvre	516
1.2	Configuration HTTPS d'un serveur Apache	516
1.2.1	Compétences principales	516
1.2.2	Éléments mis en œuvre	516
1.3	Serveur proxy et de cache Squid	517
1.3.1	Compétences principales	517
1.3.2	Éléments mis en œuvre	517

- 1.4 Nginx serveur HTTP et reverse proxy..... 517
 - 1.4.1 Compétences principales..... 517
 - 1.4.2 Éléments mis en œuvre..... 517
- 2. Remarques concernant la sécurité..... 518
 - 2.1 iptables..... 518
 - 2.2 firewalld..... 519
 - 2.3 SELinux..... 519
- 3. Configuration de base d'un serveur HTTP Apache..... 520
 - 3.1 Fichier de configuration..... 521
 - 3.1.1 Format du fichier de configuration..... 521
 - 3.1.2 Directives globales et directives de section..... 522
 - 3.1.3 Directives de base..... 522
 - 3.1.4 Validation de la syntaxe..... 524
 - 3.2 Démarrage et arrêt du serveur HTTP Apache..... 524
 - 3.2.1 Arrêt/démarrage par systemd..... 525
 - 3.2.2 Test du serveur HTTP Apache..... 526
 - 3.2.3 Arrêt/démarrage ponctuel..... 527
 - 3.3 Fichiers journaux..... 528
 - 3.4 Les modules Apache..... 529
 - 3.4.1 Directive de chargement d'un module..... 530
 - 3.4.2 Liste des modules inclus et chargés..... 530
 - 3.4.3 Configuration des modules..... 532
 - 3.4.4 Configuration du module Perl..... 532
 - 3.4.5 Configuration du module PHP..... 535
 - 3.5 Contrôle des ressources allouées au serveur..... 539
 - 3.6 Hôtes virtuels d'un serveur Apache..... 540
 - 3.6.1 Organisation des hôtes virtuels..... 541
 - 3.6.2 Hôtes virtuels sur adresse IP..... 542
 - 3.6.3 Hôtes virtuels sur numéro de port..... 544
 - 3.6.4 Hôtes virtuels sur nom d'hôte..... 544
 - 3.7 Contrôle des droits d'accès utilisateurs..... 546
 - 3.7.1 Section de déclaration d'un répertoire : Directory..... 546
 - 3.7.2 Directive de contrôle d'accès : Require..... 547
 - 3.7.3 Directives d'authentification..... 548
 - 3.7.4 Méthode d'authentification locale : AuthType Basic..... 548
 - 3.7.5 Authentification par annuaire LDAP..... 551
 - 3.7.6 Contrôle d'accès par fichier .htaccess..... 552

4.	Configuration HTTPS d'un serveur Apache	553
4.1	Cryptographie et certificats	553
4.1.1	Cryptographie symétrique	553
4.1.2	Cryptographie asymétrique.	554
4.1.3	Les certificats numériques X.509	554
4.2	Fonctionnement d'une connexion HTTPS	554
4.3	Configuration SSL d'un serveur Apache	555
4.3.1	Génération d'un certificat autosigné.	556
4.3.2	Chargement du module SSL	558
4.3.3	Configuration des clés du serveur.	559
4.3.4	Activation du mode HTTPS	560
4.3.5	Test du serveur HTTPS	560
4.3.6	Authentification des clients par certificat	562
4.3.7	Utilisation de SSL avec les hôtes virtuels	562
4.3.8	Directives renforçant la sécurité des échanges du serveur.	562
5.	Serveur proxy et de cache Squid	563
5.1	Rôles des serveurs proxy	563
5.1.1	Protection des clients	564
5.1.2	Serveurs de cache	564
5.1.3	Filtrage et journalisation	564
5.1.4	Limites	564
5.2	Configuration de base du serveur proxy Squid	565
5.2.1	Le fichier de configuration squid.conf	566
5.2.2	Gestion du cache	568
5.2.3	Listes de contrôle d'accès	569
5.2.4	Directives de contrôle d'accès : http_access	570
5.3	Exemple de serveur Squid	570
5.3.1	Configuration et démarrage du serveur	571
5.3.2	Configuration et test du client	572
5.3.3	Configuration et test d'un client interdit	573
5.3.4	Configuration et test d'une URL interdite	574
6.	Nginx serveur HTTP et reverse proxy	575
6.1	Nginx et les serveurs web	575
6.2	Fichier de configuration	576
6.2.1	Format du fichier de configuration	576
6.2.2	Directives générales	577
6.2.3	Règles de syntaxe	580

6.2.4	Validation de la syntaxe	581
6.2.5	Configuration par défaut de type Debian	582
6.2.6	Démarrage et arrêt du serveur	582
6.3	Les modules Nginx	583
6.3.1	Chargement des modules	583
6.3.2	Visualisation des modules	583
6.3.3	Choix des modules	585
6.4	Gestion des ressources	586
6.5	Nginx et les expressions régulières	588
6.5.1	Expressions régulières simples	589
6.6	Hôtes virtuels	593
6.6.1	Configuration globale	593
6.6.2	Configuration des hôtes virtuels	594
6.6.3	Hôtes virtuels sur adresse IP/numéro de port	594
6.6.4	Hôtes virtuels sur nom d'hôte	595
6.7	Les filtres d'URI : le bloc de type location	597
6.7.1	Définition d'un bloc location de sélection d'URI	597
6.7.2	Syntaxe	598
6.7.3	Priorité de sélection	598
6.7.4	Exemples de sélection	599
6.7.5	Bloc de location nommé	601
6.8	Restrictions de l'accès utilisateur	601
6.8.1	Contrôle par adresse IP	602
6.8.2	Contrôle par authentification	604
6.8.3	Contrôle par authentification locale	606
6.8.4	Choix de la portée de la restriction d'accès simple	606
6.8.5	Directives d'authentification	606
6.8.6	Création d'une base de compte locale	607
6.9	Authentification par LDAP	608
6.9.1	Utilisation de PAM	608
6.9.2	Sous-requête	608
6.9.3	Module LDAP	608
6.10	Configuration de Nginx avec SSL	609
6.10.1	Configuration d'un serveur virtuel SSL	609
6.10.2	Optimisation d'un serveur SSL	611

6.11	Gestion des pages dynamiques	612
6.11.1	Les modules FastCGI	612
6.11.2	Configuration de FastCGI	613
6.12	Nginx en reverse proxy	613
6.12.1	Reverse proxy	614
6.12.2	Le module ngx_http_proxy	614
6.12.3	Déclaration du serveur cible	614
6.12.4	Sélection des demandes à rediriger	615
6.13	Répartition de charge	617
6.13.1	Définition d'une grappe de serveurs	618
6.13.2	Utilisation d'une grappe de serveurs	619

Chapitre 10

Serveurs de fichiers

1.	Serveurs de fichiers	621
1.1	Configuration d'un serveur Samba	621
1.1.1	Compétences principales	621
1.1.2	Éléments mis en œuvre	622
1.2	Configuration d'un serveur NFS	622
1.2.1	Compétences principales	622
1.2.2	Éléments mis en œuvre	622
2.	Configuration d'un serveur Samba	623
2.1	Configuration du serveur Samba	626
2.1.1	Les daemons Samba	626
2.1.2	Le fichier de configuration smb.conf	626
2.1.3	La commande testparm	628
2.1.4	Configuration globale	630
2.2	Partage de répertoire	630
2.3	Partage d'imprimantes	632
2.4	Modèles de sécurité	633
2.5	Gestion des comptes utilisateurs Samba	634
2.5.1	Authentification des utilisateurs Samba	634
2.5.2	Gestion des utilisateurs et des mots de passe Samba	634
2.5.3	Mapping des comptes utilisateurs Samba	635
2.5.4	Synchronisation avec les mots de passe Linux	636

- 2.6 Arrêt/démarrage du serveur Samba 636
- 2.7 Le client Samba 636
 - 2.7.1 La commande smbclient 636
 - 2.7.2 Montage d'un partage SMB 637
- 2.8 Suivi de l'état du serveur Samba 638
- 3. Configuration d'un serveur NFS 640
 - 3.1 NFS version 4 640
 - 3.2 Le service rpcbind/portmapper 641
 - 3.2.1 Principe de fonctionnement 641
 - 3.2.2 Sécurisation du service 641
 - 3.3 Arrêt/démarrage du serveur NFS 641
 - 3.4 Configuration des répertoires partagés 645
 - 3.4.1 Le fichier de déclaration des partages : /etc/exports 645
 - 3.4.2 Partage dynamique d'un répertoire 647
 - 3.5 Gestion des comptes utilisateurs clients 647
 - 3.5.1 Droits d'accès de l'utilisateur client 647
 - 3.5.2 Le cas particulier du super-utilisateur 648
 - 3.6 Suivi du serveur NFS 648
 - 3.6.1 Gestion des partages : exportfs 648
 - 3.6.2 showmount 649
 - 3.6.3 nfsstat 650
 - 3.6.4 rpcinfo 651
 - 3.7 Mise en œuvre du client NFS 651
 - 3.7.1 Montage d'un répertoire partagé NFS 651
 - 3.7.2 Affichage des partages des serveurs 654

Chapitre 11

Gestion des clients réseau

- 1. Gestion des clients réseau 655
 - 1.1 Configuration DHCP 655
 - 1.1.1 Compétences principales 655
 - 1.1.2 Éléments mis en œuvre 655
 - 1.2 Authentification par PAM 656
 - 1.2.1 Compétences principales 656
 - 1.2.2 Éléments mis en œuvre 656

1.3	Utilisation d'un client LDAP	656
1.3.1	Compétences principales	656
1.3.2	Éléments mis en œuvre	657
1.4	Configuration d'un serveur OpenLDAP	657
1.4.1	Compétences principales	657
1.4.2	Éléments mis en œuvre	657
2.	Configuration DHCP	658
2.1	Le protocole DHCP	658
2.1.1	Recherche d'un serveur DHCP : DHCPDISCOVER	658
2.1.2	Offre de bail par le serveur : DHCPOFFER	658
2.1.3	Acceptation de l'offre : DHCPREQUEST	658
2.1.4	Accusé de réception du serveur : DHCPACK	659
2.1.5	Durée du bail	659
2.2	Le serveur DHCP Linux	660
2.3	Configuration du serveur DHCP	661
2.3.1	Directives générales	662
2.3.2	Paramètres optionnels transmis aux clients	662
2.3.3	Déclaration d'une plage d'adresses	663
2.3.4	Paramètres spécifiques à un client	664
2.3.5	Paramètres spécifiques à un client BOOTP	664
2.3.6	Suivi des baux DHCP	665
2.4	Configuration du client	666
2.5	Agent-relais DHCP	667
2.6	DHCP et IP version 6	667
2.6.1	Principes de DHCPv6	668
2.6.2	Gestion des messages routeurs IPv6	668
3.	Authentification par PAM	669
3.1	Le principe	670
3.2	Les modules PAM	670
3.2.1	Les types d'action de PAM	670
3.2.2	Les piles de modules	671
3.2.3	Les principaux modules PAM	671
3.3	Configuration de PAM	672
3.3.1	Structure des fichiers de configuration	673
3.3.2	Enchaînement des modules	673
3.3.3	Exemple	674

- 3.4 Configuration PAM pour SSSD 675
 - 3.4.1 Configuration NSS 675
 - 3.4.2 Configuration PAM 676
- 4. Configuration d'un serveur OpenLDAP 676
 - 4.1 Généralités 677
 - 4.1.1 Structure et terminologie 677
 - 4.1.2 Schéma 678
 - 4.1.3 Désignation des objets 678
 - 4.1.4 Authentification auprès d'un annuaire LDAP 679
 - 4.1.5 Le format LDIF 679
 - 4.2 Le serveur OpenLDAP 679
 - 4.2.1 Gestion du service 680
 - 4.2.2 Configuration du service d'annuaire 681
 - 4.2.3 Génération d'un mot de passe chiffré : slappasswd 682
 - 4.2.4 Contrôle de la configuration : slaptest 682
 - 4.2.5 Démarrage du serveur 683
 - 4.2.6 Utilitaires LDIF 683
 - 4.2.7 Indexation de l'annuaire 685
- 5. Utilisation d'un client LDAP 686
 - 5.1 Fichier de configuration du client 686
 - 5.2 Interrogation de l'annuaire : ldapsearch 687
 - 5.3 Gestion du mot de passe : ldappasswd 689
 - 5.4 Ajout d'objets dans un annuaire avec ldapadd 690
 - 5.5 Modification d'objets : ldapmodify 692
 - 5.6 Suppression d'objets : ldapdelete 693
 - 5.7 Outils graphiques 694

Chapitre 12
Services e-mail

- 1. Services e-mail 695
 - 1.1 Utilisation des serveurs de messagerie 695
 - 1.1.1 Compétences principales 695
 - 1.1.2 Éléments mis en œuvre 695

1.2	Gestion de la distribution des e-mails	696
1.2.1	Compétences principales	696
1.2.2	Éléments mis en œuvre	696
1.3	Gestion de l'accès aux boîtes e-mail	696
1.3.1	Compétences principales	696
1.3.2	Éléments mis en œuvre	696
2.	Utilisation des serveurs de messagerie	697
2.1	Le protocole SMTP	697
2.1.1	Syntaxe du protocole	697
2.1.2	Exemple	698
2.2	Les principaux serveurs de messagerie	698
2.2.1	sendmail	698
2.2.2	Exim	699
2.2.3	Postfix	699
2.3	Configuration de base de Postfix	699
2.3.1	Gestion des comptes de messagerie	699
2.3.2	Alias de messagerie	700
2.3.3	Le fichier de configuration de Postfix	701
2.3.4	Paramètres actifs	702
2.3.5	La commande postfix	702
2.3.6	Test de fonctionnement du serveur	703
2.4	La commande mail	704
2.5	Configuration de Postfix pour TLS	705
2.6	Gestion de domaines virtuels	705
2.6.1	Définition des domaines virtuels	705
2.6.2	Gestion des comptes de messagerie des domaines virtuels	705
2.7	Gestion de quotas	706
3.	Gestion de la distribution des e-mails	706
3.1	Formats de stockage des messages	706
3.1.1	Le format mbox	706
3.1.2	Le format maildir	708
3.1.3	Utilisation du format maildir par Postfix	708
3.2	procmail	709
3.2.1	Paramétrage de Postfix	709
3.2.2	Configuration de procmail	709

- 3.3 Sieve..... 710
 - 3.3.1 Composants d'un filtre Sieve 710
 - 3.3.2 La structure if. 711
 - 3.3.3 Les commandes d'action 711
 - 3.3.4 Les critères de sélection 712
 - 3.3.5 Les opérateurs de comparaison 712
 - 3.3.6 L'extension vacation 713
 - 3.3.7 Exemple 713
- 4. Gestion de l'accès aux boîtes e-mail 714
 - 4.1 Le protocole POP3. 714
 - 4.2 Le protocole IMAP4 714
 - 4.3 Serveurs courrier imap et courrier pop..... 715
 - 4.3.1 Format de stockage des messages 715
 - 4.3.2 Configuration des services 715
 - 4.3.3 Validation de l'authentification 715
 - 4.4 Le serveur Dovecot 716
 - 4.4.1 Configuration..... 716
 - 4.4.2 Visualisation de la configuration courante : doveconf 716
 - 4.4.3 La commande dovecadm. 718

Chapitre 13
Sécurité du système

- 1. Sécurité du système..... 719
 - 1.1 Configuration d'un routeur 719
 - 1.1.1 Compétences principales..... 719
 - 1.1.2 Éléments mis en œuvre 720
 - 1.2 Gestion des serveurs FTP 720
 - 1.2.1 Compétences principales..... 720
 - 1.2.2 Éléments mis en œuvre 720
 - 1.2.3 Shell sécurisé (SSH) 720
 - 1.2.4 Compétences principales..... 721
 - 1.2.5 Éléments mis en œuvre 721
 - 1.3 Tâches de sécurité..... 721
 - 1.3.1 Compétences principales..... 721
 - 1.3.2 Éléments mis en œuvre 721

1.4	OpenVPN	722
1.4.1	Compétences principales	722
1.4.2	Éléments mis en œuvre	722
2.	Configuration d'un routeur	722
2.1	Configuration d'un serveur Linux en tant que routeur	722
2.1.1	Activation du routage	723
2.1.2	La table de routage	723
2.1.3	Gestion des routes statiques	724
2.1.4	Modifier la table de routage : ip route	724
2.1.5	Modifier la table de routage : route	726
2.2	iptables	727
2.2.1	Les tables	728
2.2.2	Les chaînes	728
2.2.3	Les cibles (targets)	728
2.2.4	Les critères de sélection	729
2.2.5	Le traitement des règles	729
2.3	Administration d'un pare-feu avec iptables	730
2.3.1	Stratégies de chaînes	730
2.3.2	Création de règles	731
2.3.3	Gestion des règles	732
2.3.4	Gestion des flux retour	733
2.3.5	Exemple de configuration	734
2.4	Gestion du NAT (Network Address Translation)	735
2.4.1	Principe de la traduction d'adresses NAT	735
2.4.2	Configuration NAT d'un routeur iptables	735
2.4.3	Connexion d'un réseau privé à un réseau public	735
2.5	Sauvegardes et restauration des règles de filtrage	736
2.5.1	Sauvegarde des règles courantes	736
2.5.2	Restauration des règles de filtrage	737
3.	Gestion des serveurs FTP	737
3.1	Le protocole FTP	737
3.1.1	Principes de fonctionnement	737
3.1.2	Modes FTP actif et FTP passif	738
3.2	Les clients FTP	738
3.2.1	Les clients FTP graphiques	738
3.2.2	Le client FTP en ligne de commande	738
3.2.3	Mode anonyme	739

- 3.2.4 Mode compte utilisateur 740
 - 3.3 Le serveur FTP Pure-FTPD 740
 - 3.3.1 Options de fonctionnement 740
 - 3.4 Le serveur FTP vsftpd 741
 - 3.4.1 Configuration du serveur FTP 741
 - 3.4.2 Liste d'utilisateurs autorisés ou interdits 742
 - 3.5 Le serveur FTP ProFTPD 742
- 4. Shell sécurisé (SSH) 743
 - 4.1 Utilisations de OpenSSH 743
 - 4.1.1 Configuration du serveur OpenSSH 743
 - 4.1.2 Chiffrement des communications 744
 - 4.2 Gestion des authentifications 744
 - 4.2.1 Authentification par mot de passe et empreinte numérique . 744
 - 4.2.2 Authentification par clés 745
 - 4.2.3 Création de la paire de clés sur le client 745
 - 4.2.4 L'agent SSH 748
 - 4.3 Confidentialité des communications 749
 - 4.3.1 Session interactive avec SSH 749
 - 4.3.2 Copie de fichiers 749
 - 4.3.3 Utilisation d'applications dans des tunnels SSH 750
 - 4.3.4 Renvoi de sessions X11 via SSH 750
- 5. Tâches de sécurité 751
 - 5.1 Commandes de test et de surveillance 751
 - 5.1.1 La commande nc 751
 - 5.1.2 La commande nmap 751
 - 5.2 Les systèmes IDS (Intrusion Detection System) 752
 - 5.2.1 Techniques d'analyse 752
 - 5.2.2 Sources d'information 752
 - 5.3 Fail2Ban 753
 - 5.4 Snort 753
 - 5.4.1 Les composants 753
 - 5.4.2 Gestion des sources d'information 754
 - 5.4.3 Gestion des alertes 754
 - 5.5 OpenVAS 754
 - 5.5.1 Le serveur OpenVAS 754
 - 5.5.2 Les clients OpenVAS 755
 - 5.5.3 Base de données de vulnérabilités 755

6. OpenVPN.....	755
6.1 Les principes d'OpenVPN.....	755
6.1.1 Authentification.....	755
6.1.2 Confidentialité.....	755
6.1.3 Types de fonctionnement réseau.....	756
6.2 Création d'un tunnel point-à-point.....	756
6.2.1 Authentification par clé partagée.....	756
6.2.2 Fichiers de configuration.....	757
6.2.3 Mise en œuvre du tunnel VPN.....	758
Index.....	761