

Editions ENI

Red Hat Enterprise Linux CentOS

**Mise en production
et administration de serveurs**

(2^e édition)

Collection
Ressources Informatiques

Table des matières

Les éléments à télécharger sont disponibles à l'adresse suivante :
<http://www.editions-eni.fr>
Saisissez la référence ENI de l'ouvrage **RI2RED** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le bouton de téléchargement.

Avant-propos

Chapitre 1

Présentation de Red Hat

1. Red Hat : l'entreprise	21
2. Historique	21
3. Un mot sur la souscription	23
4. Red Hat : le système d'exploitation	26
4.1 Historique des versions	26
4.2 Particularités de Red Hat	28
4.3 Les différentes versions existantes	29
4.3.1 Red Hat Enterprise Desktop	29
4.3.2 Red Hat Enterprise Linux pour serveurs	29
4.3.3 Versions courantes	30
5. Les sites web Red Hat	32
5.1 redhat.com : le site principal	32
5.2 Red Hat Store	34
5.3 Portail Client (Customer Portal) : assistance technique, téléchargement et gestion des serveurs	36
5.4 Red Hat Network : administrer vos serveurs (jusqu'à RHEL 6.X)	37
5.5 CentOS	38

2 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

5.6	Autres sites relatifs à Red Hat	39
5.6.1	La formation et la certification	39
5.6.2	La communauté	39
5.6.3	Documentation en ligne	39
6.	En pratique, commencer avec Red Hat	40
6.1	Les différents éléments administratifs	40
6.1.1	Red Hat Login et Account number	40
6.1.2	Subscription number, Installation number, Registration number	40
6.1.3	Login Red Hat, numéro de contrat et numéro d'installation	41
6.2	Étapes jusqu'à l'obtention du système	42
6.2.1	Résumé des étapes	42
6.2.2	Étape 1 : Création d'un login Red Hat	42
6.2.3	Étape 2 : Achat de RHEL et de la souscription	43
6.2.4	Étape 3 : Téléchargement de RHEL	45

Chapitre 2

Déploiement d'un serveur Red Hat

1.	Préparer le déploiement d'un serveur Red Hat	49
1.1	Services à mettre en place	49
1.2	HCL	49
1.3	RAID matériel	51
1.4	RAID logiciel	51
1.5	Partitionnement et types de système de fichiers	52
1.6	Autres éléments nécessaires à l'installation	52
1.7	Interface graphique ou pas ?	54
1.8	Documentation de la configuration du serveur	55
2.	Installation d'un système Red Hat	56
2.1	Installation par DVD	56
2.2	Se procurer le DVD d'installation	56
2.3	Vérifier l'intégrité du DVD	57

- 2.4 Installation du système d'exploitation par DVD 58
 - 2.4.1 Installation du système par DVD
pour RHEL/CentOS 5 et 6. 58
 - 2.4.2 Installation du système par DVD
pour RHEL/CentOS 7 87
- 3. Autres types d'installation 101
 - 3.1 Installation à distance avec VNC 102
 - 3.2 Installation par le réseau (RHEL 7) 106
 - 3.2.1 Installation par le réseau avec média d'amorçage
et serveur HTTP 106
 - 3.2.2 Installation par le réseau avec PXE/BOOTP 110
 - 3.2.3 Installation automatisée avec Kickstart 116
 - 3.2.4 Exemple de combinaison :
Installation PXE/VNC listener 121
- 4. Prise en main du système 129
 - 4.1 Ligne de commande 129
 - 4.1.1 Les shells en général 129
 - 4.1.2 Le bash. 131
 - 4.1.3 Aide en ligne 135
 - 4.2 Commandes de base 140
 - 4.2.1 Comprendre l'arborescence et s'y déplacer 140
 - 4.2.2 Manipulation des fichiers et répertoires 145
 - 4.2.3 Rechercher des fichiers 151
 - 4.2.4 Afficher et éditer le contenu d'un fichier 154
 - 4.2.5 Éditeur de fichiers vi 157
 - 4.2.6 Utilisation du shell 159
 - 4.2.7 Outils Red Hat en ligne de commande 160
 - 4.3 Présentation de l'interface graphique 163
 - 4.3.1 GNOME 163
 - 4.3.2 GNOME pour RHEL 5/6 164
 - 4.3.3 GNOME pour RHEL 7 165

4 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

5.	Structure de RHEL	167
5.1	Structure générale	167
5.2	L'espace utilisateur	168
5.3	Focus sur l'interface graphique en espace utilisateur	170
5.4	Le noyau	173

Chapitre 3

Démarrage du système

1.	La séquence de démarrage	177
1.1	Pourquoi il faut la connaître	177
1.2	De l'appui sur le bouton ON jusqu'à l'invite de connexion . . .	178
2.	BIOS	179
3.	UEFI	179
4.	Chargeur de démarrage GRUB	180
4.1	Présentation	180
4.2	GRUB Legacy (RHEL 5/6)	181
4.3	Les interfaces	182
4.3.1	Interface Menu	183
4.3.2	Éditeur d'interface	184
4.3.3	Ligne de commande	186
4.4	Fichier de configuration /boot/grub/grub.conf	186
4.4.1	Particularités de GRUB	187
4.4.2	Structure du fichier de configuration	188
4.5	GRUB 2 (RHEL 7)	190
4.5.1	Les interfaces	190
4.5.2	Fichiers de configuration	193
5.	Lancement du noyau et du processus père	201
5.1	Rôle du noyau (kernel)	201
5.2	Sélection au démarrage	202
5.2.1	Répertoire /boot	202
5.2.2	Informations sur le noyau existant	204

5.3	Installation d'un nouveau noyau	204
5.4	Paramétrage du noyau	207
5.5	Modules du noyau	210
5.5.1	Lister les modules chargés	211
5.5.2	Afficher les informations sur un module	211
5.5.3	Charger un module	212
5.5.4	Décharger un module	212
5.5.5	Chargement de modules au démarrage	212
6.	Lancement du système	214
6.1	Avec /sbin/init (RHEL 5 et 6)	214
6.1.1	Démarrage général	214
6.1.2	Niveaux d'exécution	215
6.2	Démarrage System V Init (RHEL 5.X)	219
6.3	Démarrage Upstart (RHEL 6.X)	221
6.4	Démarrage systemd (RHEL 7)	223
6.5	Gestion des services avec systemd	227
7.	Éteindre le système	228
8.	Notions de cryptographie	229

Chapitre 4

Installation de logiciels

1.	Introduction et historique	237
2.	Installation avec le gestionnaire de paquets YUM	240
2.1	Introduction à YUM	240
2.1.1	Chercher et installer des paquets	241
2.1.2	Mise à jour de paquets	246
2.1.3	Plug-ins yum	247
2.1.4	Réinitialiser yum	249
2.1.5	yum et la cryptographie	249
2.2	Rappel des commandes yum	252
2.3	Gestion des abonnements	253

6 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

2.4	Red Hat Network	253
2.4.1	Enregistrement du système	253
2.4.2	Supprimer un système du Red Hat Network	256
2.4.3	Gestion des abonnements	258
2.4.4	Politiques de mises à jour et sécurité	262
2.5	Utilisation de dépôts de logiciels externes	263
2.5.1	Présentation et installation du dépôt EPEL	265
2.5.2	Présentation et installation du dépôt RPMForge	267
2.5.3	Utiliser EPEL ou RPMForge ?	269
3.	RPM : installation de paquets indépendants	278
3.1	Où trouver des RPM ?	279
3.1.1	Rapatrier un RPM sur votre serveur Red Hat Enterprise Linux	280
3.1.2	Nomenclature de nommage des paquets	281
3.2	Installation et mise à jour : option -U	281
3.2.1	Résolution de dépendances	282
3.2.2	Forcer l'installation d'un paquet sans ses dépendances	283
3.3	Désinstallation : option -e	283
3.4	Requête : option -q	284
4.	Compilation à partir des sources	286
4.1	Compilation : pourquoi ?	286
4.2	Les pré-requis pour la compilation	287
4.2.1	Quels paquets installer ?	287
4.2.2	Où trouver des logiciels ?	289
4.3	Les étapes de la compilation	290
4.3.1	Préalable	290
4.3.2	Pré-test de compilation et résolution de dépendances	292
4.3.3	Compilation	294
4.3.4	Installation	294
4.3.5	Les options de compilation	295

Chapitre 5
Partitions et système de fichiers

- 1. Partitionner un disque 297
 - 1.1 Structure d'un disque dur 297
 - 1.1.1 Introduction aux disques durs et partitions 297
 - 1.1.2 Concepts de partitionnement 299
 - 1.1.3 La logique de nommage des partitions
 sous Linux Red Hat 302
 - 1.1.4 Idées de partitionnement 303
 - 1.2 Le partitionnement en pratique 303
 - 1.2.1 Utiliser fdisk pas à pas 304
 - 1.2.2 Avec parted 310
 - 1.2.3 Partitionnement graphique : GParted 314
- 2. Logical Volume Manager 315
 - 2.1 Présentation et composants 315
 - 2.2 Notions avancées 318
 - 2.2.1 Extensions 318
 - 2.2.2 Clichés (snapshots) 322
 - 2.3 Administration de LVM 322
 - 2.3.1 Étape 1 : Volumes physiques (PV) 322
 - 2.3.2 Étape 2 : Groupe de volumes (VG) 324
 - 2.3.3 Étape 3 : Volumes logiques (LV) 326
 - 2.4 Administration avancée de LVM 328
 - 2.4.1 Supprimer un volume logique 328
 - 2.4.2 Étendre un volume logique 331
 - 2.4.3 Réduire un volume logique 334
- 3. RAID 336
 - 3.1 Présentation 336
 - 3.1.1 Qu'est-ce que le RAID ? 336
 - 3.1.2 Niveaux de RAID 336
 - 3.1.3 RAID physique ou logiciel ? 338

8 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

3.2	RAID logiciel : mise en œuvre	339
3.2.1	Création de volume RAID	339
3.2.2	Surveillance du RAID	344
4.	Installer un système de fichiers	345
4.1	Présentation	345
4.2	Structure des données sous Linux	349
4.2.1	Extended File System	349
4.2.2	Superbloc	350
4.2.3	Inodes	350
4.2.4	Table des inodes	351
4.2.5	Tables des blocs	352
4.2.6	Illustration de la structure du système de fichiers	352
4.2.7	Liens symboliques et liens physiques	355
4.2.8	Fragmentation	359
4.2.9	Descripteurs de fichiers (File Descriptors)	359
4.3	Les systèmes de fichiers sous Red Hat Enterprise Linux	362
4.3.1	ext3	362
4.3.2	ext4	363
4.3.3	XFS	363
4.3.4	GFS2	363
4.3.5	L'espace Swap	364
4.3.6	Connaître le type de système de fichiers d'une partition	364
4.4	Création du système de fichiers	365
4.4.1	Création d'un système de fichiers en ext3	366
4.4.2	Utilitaires de gestion de partitions ext3/ext4 : e2fsprogs	367
4.5	Création d'un système de fichiers en XFS	368
5.	Monter le système de fichiers	371
5.1	Montage manuel	372

5.2	Montage automatique /etc/fstab	374
5.2.1	Commande mount et /etc/fstab	374
5.2.2	Les options de montage	375
5.2.3	Déplacer /home sur une autre partition	376
6.	Système de fichiers chiffré	378
6.1	Installation	378
6.2	Création d'un système de fichiers chiffré	378
7.	L'arborescence du système de fichiers ext3/ext4	381
7.1	Une arborescence conforme au FHS	381
7.1.1	Le répertoire /dev	381
7.1.2	Le répertoire /boot	382
7.1.3	Le répertoire /etc.	382
7.1.4	Les répertoires /lib et /lib64	382
7.1.5	Le répertoire /mnt et /media	383
7.1.6	Le répertoire /proc	383
7.1.7	Le répertoire /sbin.	383
7.1.8	Le répertoire /var	383
7.1.9	Le répertoire /home	384
7.1.10	Le répertoire /tmp.	384
7.2	Vérifier l'espace disque disponible	384
7.2.1	Utilisation des systèmes de fichiers.	384
7.2.2	Afficher la taille des répertoires	385

Chapitre 6

Gestion des utilisateurs et des groupes

1.	Utilisateurs et groupes	387
1.1	Utilisateurs, groupes et fichiers	387
1.1.1	Utilisateurs, groupes et rôles	387
1.1.2	Fichiers et permissions	388

10 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

1.2	Gestion des utilisateurs et des groupes	389
1.2.1	Ajout d'un utilisateur en ligne de commande	389
1.2.2	Modification des paramètres du compte utilisateur . . .	390
1.2.3	Ajout et modification : options avancées	391
1.2.4	Suppression d'un utilisateur en ligne de commande . . .	392
1.2.5	Gestion des utilisateurs et des groupes via l'interface graphique	392
1.2.6	La séquence en détail	392
1.2.7	Mot de passe	395
1.2.8	Temporisateurs du compte utilisateur	401
1.3	Personnalisation du compte utilisateur	403
1.3.1	Fichiers de lancement	403
1.3.2	Variables d'environnement	405
1.3.3	Alias de commandes	406
2.	Droits sur les fichiers et répertoires	406
2.1	Présentation	406
2.2	Afficher les droits	407
2.3	Droits sur les fichiers	409
2.4	Droits sur les répertoires	409
2.5	Droits spéciaux	412
2.6	Modification des propriétaires et des droits sur les fichiers . .	417
2.6.1	Modification de propriétaire	417
2.6.2	Modification de droits	419
2.6.3	Droits par défaut avec umask	423
3.	Gestion avancée des disques et des utilisateurs	424
3.1	Quotas de disque par utilisateur ou groupe	424
3.1.1	Activation des quotas sur les systèmes de fichiers	425
3.1.2	Analyse du disque	426
3.1.3	Assignation de quotas	426
3.1.4	Délai de grâce	428
3.1.5	Activer les quotas	428

3.2	Droits pour plusieurs utilisateurs : les ACL	429
3.2.1	Principe des ACL	429
3.2.2	Modifier les ACL sur les fichiers	429
3.3	Attributs étendus	431
3.3.1	Modifier les attributs étendus	432
3.3.2	Lister les attributs étendus	432
4.	Autres types d'authentification	433
4.1	PAM : modules d'authentification	433
4.1.1	Introduction	433
4.1.2	Fonctionnement	433
4.1.3	Configuration	434
4.2	NSS	436
4.2.1	Introduction	436
4.2.2	Configuration	437
4.3	RHEL 6 : System Security Services Daemon (SSSD)	437
5.	Sécurité de l'administration : sudo	438
5.1	Présentation	438
5.2	Configuration de sudo	440
5.2.1	Utiliser sudo	442
5.2.2	Autre usage	444
5.2.3	Désactiver le compte root	444
5.3	SELinux	445
5.3.1	Contrôle du mode SELinux (RHEL 5)	446
5.3.2	Contrôle du mode SELinux (RHEL 6 et 7)	447
5.3.3	Contextes de sécurité : visualisation	447
5.3.4	Rétablissement du contexte de sécurité par défaut	450

12 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

Chapitre 7 Réseau

1. Configuration du réseau pour RHEL 5 et 6	451
1.1 Hostname	453
1.1.1 Configuration dynamique	453
1.1.2 Configuration statique	454
1.1.3 Diagnostic	454
1.2 Adresse IP et masque	455
1.2.1 Configuration dynamique	455
1.2.2 Configuration statique	458
1.2.3 Scripts de contrôle des interfaces	459
1.2.4 Diagnostic	460
1.3 Passerelle par défaut	461
1.3.1 Configuration dynamique	461
1.3.2 Configuration statique	462
1.3.3 Diagnostic	462
1.4 Adresse des serveurs DNS	463
1.4.1 Configuration dynamique	464
1.4.2 Configuration statique	464
1.5 Configuration réseau IPv6	465
1.5.1 Activation d'IPv6	465
1.5.2 Configuration manuelle de la passerelle par défaut ...	466
1.5.3 Configuration manuelle de l'interface	466
1.5.4 Vérification	467
1.6 Configuration réseau : résumé	467
1.7 Configuration du réseau avec NetworkManager (RHEL 7) ...	468
1.7.1 Service NetworkManager	469
1.7.2 L'outil en ligne de commande nmcli	469
1.7.3 Paramétrer le hostname	475
1.7.4 Paramétrer une interface	475
1.7.5 L'interface en mode texte nmtui	487

1.8	Configuration graphique	487
1.8.1	Les différents éléments.	487
1.8.2	Utiliser le gestionnaire réseau (RHEL 5/6)	489
1.8.3	Utiliser le gestionnaire réseau (RHEL 7)	492
1.9	Diagnostic et dépannage du réseau	493
1.9.1	Accessibilité d'une machine : ping.	493
1.9.2	Chemin des paquets : traceroute.	494
1.9.3	Ports ouverts sur la machine	495
1.9.4	Analyse de réseau : nmap.	498
1.9.5	Analyse de protocoles : TCPdump et Wireshark	499
1.9.6	Forgeur de paquets : ncat et hping	500
1.10	Création de routes statiques	501
1.11	Interface Bonding (RHEL 5/6)	506
1.11.1	Configuration de l'Interface Bonding	506
1.11.2	Vérification	508
1.12	Interface Teaming (RHEL 7)	509
1.13	Affectation de plusieurs adresses IP à une interface.	515
1.14	VLAN Tagging 802.1Q.	516
1.14.1	Configuration	518
1.14.2	Vérification	522
2.	Configuration du pare-feu pour un serveur	523
2.1	Introduction	523
2.2	Configuration graphique	524
2.2.1	Red Hat Enterprise Linux 5	524
2.2.2	Red Hat Enterprise Linux 6	525
2.3	Configuration en ligne de commande avec RHEL 5 et 6	526
2.3.1	Filtrage.	527
2.3.2	Configuration : ajout ou modification de règles.	528
2.3.3	Critères de base.	528
2.3.4	Actions	529
2.3.5	Politique par défaut	530
2.3.6	Listage des règles.	530
2.3.7	Sauvegarde des règles	530

14 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

2.3.8	Contrôle du service IPTables	531
2.4	Configuration en ligne de commande pour RHEL 7	532
2.4.1	Présentation de firewalld	532
2.4.2	Configuration en ligne de commande firewall-cmd.	535
2.5	Autres mécanismes de sécurité	544
2.5.1	TCP Wrappers.	544
2.5.2	xinetd	545
3.	Accès sécurisé au serveur	547
3.1	SSH pour l'administration à distance	547
3.1.1	Présentation	547
3.1.2	Utilisation simple	547
3.1.3	Prise en main graphique à distance	549
3.1.4	Connexion SSH simple avec PuTTY sous Windows	551
3.1.5	Prise en main à distance sous Windows	553
3.1.6	Authentification à clé publique	555
3.1.7	Authentification à clé publique avec PuTTY sous Windows.	564
3.1.8	Authentification avec clé publique et agent	570
3.1.9	Lancement de commandes automatiques sur serveurs distants.	571
3.1.10	Rapatrier des fichiers	575
3.1.11	Tunneling simple	577
3.2	Création de VPN avec RHEL	581
3.2.1	Introduction	581
3.2.2	VPN IPsec	585
3.2.3	VPN SSL avec OpenVPN	595
3.2.4	VPN avec authentification par certificats.	604

Chapitre 8
Les scripts bash

- 1. Introduction 613
- 2. Préalable 614
 - 2.1 Transformer un fichier en script bash 614
 - 2.2 Commentaires dans un script 617
 - 2.3 Déboguer un script 617
- 3. Traitement de base 618
 - 3.1 Variables 618
 - 3.2 Arguments du script 620
 - 3.3 Script interactif 622
 - 3.4 Appel d'un autre fichier dans le script 623
 - 3.5 Une commande dans une commande ou dans un texte 625
 - 3.6 Échappement de caractères spéciaux 626
- 4. Traitement avancé 630
 - 4.1 Tests et comparaisons 630
 - 4.2 Les instructions conditionnelles 633
 - 4.3 Boucles conditionnelles 638
 - 4.4 Fonctions 641
 - 4.5 Sortie de script ou de commande 643
 - 4.6 Redirections 646
 - 4.7 Tubes et filtres 650
- 5. Outils 653
 - 5.1 Sed : éditeur de données en flux 653
 - 5.2 Tableau de commandes utiles 657

16 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

Chapitre 9

Services de production courants

1. Services de production	659
2. Apache	660
2.1 Présentation	660
2.2 Configuration	660
2.2.1 Installation	660
2.2.2 Fichiers et répertoires importants	663
2.2.3 Nouveau site web avec VirtualHost	663
2.2.4 Ajout d'un site web	667
3. PHP et MySQL (MariaDB)	668
3.1 Installation de PHP	669
3.2 Installation de MariaDB	670
3.3 phpMyAdmin	672
3.3.1 Nouvelle configuration de phpMyAdmin	674
3.3.2 Administration d'une base de données	677
4. DNS	677
4.1 Présentation de BIND et de DNS	677
4.2 Configuration	681
4.2.1 Installation	681
4.2.2 Fichiers et répertoires importants	682
4.2.3 Configuration d'une zone	682
4.2.4 Zone inverse	688
4.2.5 Vérification	689
5. FTP	691
5.1 Présentation	691
5.2 Configuration	692
5.2.1 Installation	692
5.2.2 Configuration pour utilisateurs anonymes	693
5.2.3 Configuration pour utilisateurs classiques	694
5.2.4 Configuration pour utilisateurs virtuels	695

- 6. NFS 696
 - 6.1 Présentation 696
 - 6.2 Configuration 697
 - 6.2.1 Installation 697
 - 6.2.2 Configuration 698
 - 6.3 Accès à un partage NFS 699
- 7. DHCP 699
 - 7.1 Présentation 699
 - 7.2 Configuration 700
 - 7.2.1 Installation 700
 - 7.2.2 Fichier et répertoire importants 700
 - 7.2.3 Configuration de démarrage 701
 - 7.2.4 Configuration 701
- 8. Services RHEL 7 704
 - 8.1 Virtualisation avec KVM/Qemu 704
 - 8.1.1 Présentation 704
 - 8.1.2 Installation de l'hyperviseur KVM 705
 - 8.1.3 Virt-manager en mode graphique 706
 - 8.2 Conteneurs avec Docker, isolation d'applications 714
 - 8.2.1 Présentation et installation 714
 - 8.2.2 Images Docker 717
 - 8.2.3 Conteneurs 720
 - 8.2.4 Images maison 725
 - 8.2.5 Registres et partage des images 729

Chapitre 10

Maintenance du système en production

- 1. Analyse du système 733
 - 1.1 Nécessité d'analyser son système 733
 - 1.2 Le standard Syslog 734
 - 1.2.1 Présentation et explication 734
 - 1.2.2 Syslogd (RHEL 5.X) 736

18 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

1.2.3	Rsyslog (RHEL 6)	740
1.2.4	Journald (RHEL 7)	741
1.2.5	Vérification des logs et du fonctionnement	746
1.2.6	Bonnes pratiques	748
1.3	Outils d'analyse système	749
1.4	Outils d'analyse des logs	754
1.5	Outils de surveillance externes	755
1.5.1	Supervision proactive (météologie) : Cacti	755
1.5.2	Supervision réactive : Nagios	756
1.5.3	Cacti ou Nagios ?	758
2.	Programmation de tâches	758
2.1	Présentation	758
2.2	Programmation périodique avec Cron	759
2.2.1	Présentation	759
2.2.2	Configuration du service	759
2.2.3	Programmation de tâches	760
2.3	Programmation périodique avec systemd (RHEL 7)	763
2.4	Programmation périodique avec Anacron	766
2.4.1	Présentation	766
2.4.2	Configuration	766
2.5	Programmation ponctuelle de commandes	768
2.5.1	En fonction d'une heure : at	768
2.5.2	En fonction de la charge processeur : batch	769
3.	Gestion des processus	769
3.1	Contrôle des jobs	769
3.2	Consoles multiples avec screen	775
3.3	Contrôle des processus	777
4.	Mise en place des sauvegardes et de l'archivage	780
4.1	Plan de reprise d'activité	780
4.2	Politiques d'archivage et de sauvegardes	780

- 4.3 Différents outils : tar, cpio, rsync 782
 - 4.3.1 Utilisation de tar. 783
 - 4.3.2 Utilisation de cpio 784
 - 4.3.3 Utilisation de rsync 786
- 4.4 Solutions intégrées 787
 - 4.4.1 Solutions libres 787
 - 4.4.2 Solutions commerciales 787
- 5. Dépannage d'un système RHEL 787
 - 5.1 Mode de secours 788
 - 5.2 Mode mono-utilisateur 789
 - 5.3 Écraser un mot de passe perdu..... 790

Chapitre 11

Aide-mémoire des principales commandes

- 1. Démarrage..... 793
 - 1.1 GRUB2 793
 - 1.2 Noyau et modules. 794
 - 1.3 Init et services..... 794
- 2. Installation de logiciels..... 795
 - 2.1 Abonnement 795
 - 2.2 YUM (dépôts de paquets) 796
 - 2.3 RPM (paquets indépendants) 797
 - 2.4 Compilation à partir des sources..... 798
- 3. Partitions et systèmes de fichiers..... 798
 - 3.1 Partitionnement 798
 - 3.2 Logical Volume Manager 799
 - 3.3 RAID logiciel..... 800
 - 3.4 Système de fichiers..... 800
 - 3.5 Quotas..... 801

20 — Red Hat Enterprise Linux/CentOS

Mise en production et administration de serveurs

4. Utilisateurs et groupes	802
4.1 Utilisateurs	802
4.2 Fichiers des utilisateurs	803
4.3 Droits.	803
4.4 File ACL.	804
4.5 Attributs étendus	804
4.6 sudo	804
4.7 SELinux	805
5. Réseau	805
5.1 Interface	805
5.2 Interface RHEL 7	806
5.3 Diagnostic	807
5.4 Routes	807
5.5 Pare-feu	808
5.6 SSH	810
6. Shell Bash	810
7. Scripting Bash	814
7.1 sed (éditeur de données en flux)	819
7.2 Regular Expression (expressions rationnelles)	820
7.3 Autres commandes	822
8. Pour éditer/exporter	823
Index	825

Editions ENI

LDAP

Planification et mise en oeuvre d'un annuaire OpenLDAP

Collection
Expert IT

Table des matières

Avant-propos

Chapitre 1
Un annuaire, un choix évident

- 1. Le casse-tête de la gestion des identifiants électroniques en entreprise. 15
- 2. La centralisation des identités électroniques 16
- 3. Les annuaires. 17
- 4. Annuaires vs mécanismes d'authentification 18
- 5. Annuaire vs base de données 18

Chapitre 2
Les concepts de base LDAP

- 1. Introduction 21
- 2. LDAP : Protocole ou normalisation des systèmes d'annuaires informatiques 21
- 3. Modèle de stockage des informations 25
 - 3.1 Les attributs 26
 - 3.2 Les classes d'objets et les schémas 29
- 4. Modèle d'organisation des informations 35
 - 4.1 La structure arborescente (DIT) 35
 - 4.2 Le format LDIF 38
- 5. Modèle fonctionnel 39
 - 5.1 Les opérations de type requête 40
 - 5.2 La syntaxe du filtre de recherche 42
 - 5.3 Comparaison. 44
 - 5.4 Les opérations de mise à jour 44
 - 5.5 Les opérations d'authentification 44
- 6. Modèle de sécurisation et de confidentialité des informations 45

Chapitre 3**Planification de l'intégration d'un annuaire LDAP**

1. Introduction	47
2. Source et contenu de l'annuaire	49
2.1 Utilisation principale de l'annuaire	49
2.2 Recensement des différents systèmes d'information utilisés dans votre entreprise	49
2.3 Vérifier la compatibilité avec le protocole LDAP	50
3. Modélisation et définition du contenu de l'annuaire	52
3.1 Connaissance des schémas utilisés par les clients LDAP	52
3.2 Modélisation	53
4. Stockage physique des données	55
4.1 Disques locaux ou architecture de stockage de données	55
4.2 Base de données, moteurs de stockage (backend)	57
4.3 Le format LDIF	57
5. Sécurisation de l'annuaire	58
5.1 Objectif	58
5.2 Étude de l'authentification à l'annuaire	59
5.3 Étude de l'autorisation au contenu de l'annuaire	61
6. Conception de l'infrastructure du service d'annuaire	62
6.1 Les différentes topologies	62
6.1.1 Un service d'annuaire local	63
6.1.2 Un service d'annuaire local avec référent(s)	63
6.1.3 Un service d'annuaire local et répliqué	65
6.1.4 Un service d'annuaire distribué et répliqué	66
6.1.5 Un service d'annuaire distribué et répliqué avec référents	67
6.2 La haute disponibilité des annuaires	68
6.2.1 Configuration de multiples serveurs LDAP	69
6.2.2 Configuration de la mise en cache LDAP	70

- 6.2.3 Ajout d'un équipement matériel ou applicatif de type commutateur IP avec ou sans équilibrage de charge en "Front-end" 72
- 6.3 Présentation d'un cluster de répartition de charge (load-balancing cluster) 73
 - 6.3.1 Fonction de haute disponibilité en mode "actif/passif" (clustering) 74
 - 6.3.2 Fonction de répartition de charge (load-balancing) 77
 - 6.3.3 Méthode de réponse du "load-balancer" 78
 - 6.3.4 Exemple de configuration pour la fonction cluster à répartition de charge en mode dispatcher (sous AIX) . . 81
- 6.4 Un service d'annuaire local avec délégation d'authentification (PTA) 85

Chapitre 4

Installation/configuration d'un serveur OpenLDAP

- 1. Introduction 87
- 2. Présentation de l'architecture LDAP à intégrer 87
- 3. Installation du serveur OpenLDAP 90
 - 3.1 Les prérequis applicatifs 90
 - 3.2 À partir de packages RPM (exemple de la distribution Red Hat) 90
 - 3.3 Depuis les sources du code 93
- 4. Configuration du serveur OpenLDAP 95
 - 4.1 Organisation des fichiers de configuration 96
 - 4.2 Présentation des entrées de configuration 98
 - 4.2.1 "dn: cn=config" 99
 - 4.2.2 "dn: cn=module, cn=config" 100
 - 4.2.3 "dn: cn=schema, cn=config" 101
 - 4.2.4 "dn: olcBackend=<type>, cn=config" 101
 - 4.2.5 "dn: Database={x}<type>, cn=config" 102

4.3	Présentation des backend disponibles	103
4.3.1	Les backend locaux	103
4.3.2	Les proxy backend	104
4.3.3	Les backend dynamiques	104
4.4	Configuration initiale par le fichier "slapd.conf"	104
4.4.1	Création du fichier "/etc/openldap/slapd.conf"	105
4.4.2	Conversion de l'ancien (slapd.conf) au nouveau format de configuration (olc, cn=config)	108

Chapitre 5

Installer et configurer un navigateur LDAP

1.	Introduction	111
2.	Présentation de Apache Directory Studio	111
3.	Installation sous Linux	112
4.	Configuration d'une connexion à un annuaire	113
5.	Quelques exemples d'utilisation	118
6.	Première connexion au DIT de configuration	125

Chapitre 6

Démarrage du serveur OpenLDAP

1.	Introduction	129
2.	Le service "slapd"	129
3.	Présentation des options de démarrage du processus "slapd"	130
4.	Vérification du démarrage automatique du service "slapd"	133
5.	Démarrage et arrêt du processus "slapd" en ligne de commande	133

Chapitre 7
Les schémas

- 1. Introduction 135
- 2. Les schémas contenus dans OpenLDAP 135
- 3. Extension de schéma 138
- 4. Ajout du schéma "sudo" 140
- 5. Suppression d'un schéma 142

Chapitre 8
Préparation des données de l'annuaire

- 1. Introduction 145
- 2. Choix du suffixe 145
- 3. Structure et nommage des entrées 145
- 4. Configuration de la structure LDAP au format LDIF 148

Chapitre 9
Provisionner l'annuaire LDAP

- 1. Introduction 151
- 2. Les méthodes de chargement de l'annuaire 151
 - 2.1 Chargement des données en ligne 152
 - 2.2 Chargement des données hors ligne 153
- 3. Présentation des commandes LDAP 155
 - 3.1 La commande ldapsearch 156
 - 3.2 La commande ldapdelete 160
 - 3.3 La commande "ldapadd" 161
 - 3.4 La commande ldapmodify 162
 - 3.5 Les commandes ldapmodrdn, slapasswd, ldapwhoami, ldapurl 164
 - 3.6 Configuration des commandes LDAP 164

Chapitre 10**Sécuriser un annuaire OpenLDAP**

1. Introduction	167
2. Authentification (ou ouverture de session LDAP)	168
2.1 L'authentification de base ou simple	169
2.2 L'authentification SASL	170
2.3 Consulter les mécanismes SASL disponibles sur OpenLDAP .	173
3. La politique de mot de passe	175
4. Le stockage des mots de passe	175
4.1 Rappel sur les algorithmes de cryptage de type condensé . . .	176
4.2 Revue des fonctions de hachage supportées par OpenLDAP .	178
4.2.1 CRYPT	178
4.2.2 MD5	179
4.2.3 SMD5	179
4.2.4 SHA "Secure Hash Algorithm"	179
4.2.5 SSHA	180
4.2.6 PTA	181
4.3 Configuration du service PTA	182
4.3.1 Configuration du service saslauthd	184
5. La configuration réseau	192
5.1 Sélectionner son (ou ses) interface(s) réseau et son (ou ses) port(s) d'écoute(s)	192
5.2 Sélectionner les réseaux autorisés	193
6. Fixer des limites aux opérations LDAP	194
6.1 Le type de limites	194
6.2 Les limites hard ou soft	194
6.3 La portée des limites	195
6.3.1 Les limites globales	195
6.3.2 Les limites par base de données	196

- 7. Confidentialité et intégrité des communications 197
 - 7.1 Présentation de SSL et TLS 197
 - 7.1.1 Son fonctionnement. 198
 - 7.2 StartTLS 201
 - 7.3 Présentation du programme OpenSSL 202
 - 7.3.1 Commande de création de certificats 203
 - 7.3.2 Commande de contrôle des certificats 204
 - 7.3.3 Recherche de pannes 204
 - 7.3.4 Commandes de conversion de certificats 205
- 8. Configuration du LDAPS avec SSL/TLS 206

Chapitre 11
Protection des données de l'annuaire

- 1. Compréhension de la sécurité d'un annuaire 215
- 2. Configuration générale des ACL 216
 - 2.1 Les entrées ciblées (à quoi ?) 216
 - 2.2 Les entrées accréditées (qui a accès ?) 219
 - 2.3 Les droits accordés (pour faire quoi ?) 220
 - 2.4 Évaluation des droits 221
 - 2.5 Exemples de configuration d'ACL 222
- 3. Configuration des ACL dans l'annuaire de démonstration 225
 - 3.1 Configuration des ACL standard. 226
 - 3.2 Cloisonnement de l'annuaire par client 227
 - 3.3 Pour aller plus loin dans le cloisonnement 229

Chapitre 12**Ajout de fonctionnalités appelées "overlay"**

1. Introduction	235
2. Ajouter un overlay	236
2.1 Vérification de son existence dans l'annuaire	236
2.2 Charger le module de l'overlay dans l'annuaire	237
2.3 Créer un overlay pour la base de données désirée	237
3. AccessLog	238
3.1 Présentation	238
3.2 Exemple de configuration	239
4. Audit logging	241
4.1 Présentation	241
4.2 Exemple de configuration	241
5. Constraint	242
5.1 Présentation	242
5.2 Exemple de configuration	242
6. Dynamic Lists	243
6.1 Présentation	243
6.2 Exemple de configuration	244
7. Password Policy	246
7.1 Présentation	246
7.2 Exemple de configuration	247
8. L'intégrité référentielle	253
8.1 Présentation	253
8.2 Exemple de configuration	255
9. Sync Provider	256
9.1 Présentation	256
9.2 Exemple de configuration	256
10. Attribute Uniqueness	257
10.1 Présentation	257
10.2 Exemple de configuration	258

- 11. Reverse Group Membership Maintenance 259
 - 11.1 Présentation 259
 - 11.2 Exemple de configuration 259

Chapitre 13
Configuration de clients LDAP

- 1. Introduction 261
- 2. Prérequis 261
- 3. Les systèmes d'exploitation 262
 - 3.1 Les serveurs Linux Red Hat (cas d'un RHEL6) 262
 - 3.1.1 Installation des packages 262
 - 3.1.2 Configuration du service "sssd" 264
 - 3.1.3 Ajout du certificat de l'autorité de certification 265
 - 3.1.4 Mise à jour du fichier /etc/hosts 266
 - 3.1.5 Dissimulation du mot de passe du Bind user 266
 - 3.1.6 Redémarrage du service "sssd" 266
 - 3.1.7 Vérifier le bon fonctionnement de la configuration 267
 - 3.1.8 Observation du mécanisme PAM 268
 - 3.2 Les serveurs IBM AIX 270
 - 3.2.1 Prérequis 270
 - 3.2.2 Installation et configuration des paquetages de cryptographie (gsk) 271
 - 3.2.3 Installation et configuration des paquetages du client LDAP 272
 - 3.2.4 Paramétrage système 272
 - 3.2.5 Vérification de l'installation du client LDAP 272
- 4. Les équipements Hardwares 274
 - 4.1 Cas d'une interface HP iLO 274
 - 4.1.1 Configuration 275
 - 4.2 Cas d'un Routeur (Cisco ASA) 278
 - 4.2.1 Les méthodes d'authentification à l'annuaire LDAP 279
 - 4.2.2 Les informations à rechercher 280

4.2.3	La configuration	280
5.	Les applications et utilitaires	284
5.1	Cas de l'application de monitoring OP5	284
5.2	Cas du programme sudo	289

Chapitre 14

Sauvegarder/restaurer un annuaire OpenLDAP

1.	Les données de l'annuaire.	293
2.	Les stratégies de sauvegarde.	294
3.	Méthode de sauvegarde des données de l'annuaire.	296
3.1	Sauvegarde hors-ligne au niveau des répertoires du système de fichiers	296
3.2	Sauvegarde hors-ligne au niveau de la base de données.	296
3.3	Sauvegarde en ligne au format LDIF	299
4.	Restauration de l'annuaire	300
4.1	Restauration totale.	300
4.2	Restauration partielle.	302
4.2.1	Restauration en ligne de type "import/export"	302
4.2.2	Restauration hors-ligne	303
5.	Exemple de script de sauvegarde	304
6.	Migration d'annuaire OpenLDAP	306

Chapitre 15

La réplication

1.	Introduction	307
2.	Fonctionnement du protocole de réplication "LDAP Sync".	308
2.1	Réplication en mode "refreshOnly" ou "Pull-based"	309
2.2	Réplication en mode "refreshAndPersist" ou "Push-based"	311

- 3. Configuration du "Syncrepl" en utilisant OLC 312
 - 3.1 Configuration du provider 312
 - 3.2 Configuration du consumer 313
- 4. Les problèmes liés à la réplication LDAP Sync 314
 - 4.1 SessionLog 315
 - 4.2 Delta-syncrepl ou AccessLog 316
 - 4.2.1 Exemple de configuration 317
- 5. Les différentes architectures de réplication 320
 - 5.1 Architecture de réplication simple "provider/consumer" 320
 - 5.2 Architecture de réplication "Peer to peer" ou "multi-Peer" . . . 321
 - 5.2.1 Exemple de configuration 322
 - 5.3 Architecture de réplication "miroir" 325
 - 5.4 Architecture avec un proxy de réplication 327
 - 5.5 Configuration du NTP 328
 - 5.6 Réaliser la première synchronisation 329

Chapitre 16
Surveillance d'un annuaire OpenLDAP

- 1. Surveiller le service LDAP 331
 - 1.1 Le processus "slapd" 331
 - 1.2 Les systèmes de fichiers 331
- 2. Surveiller la réplication 332
- 3. Surveiller les connexions au serveur LDAP 334
- 4. Surveiller les modifications du contenu de l'annuaire 336

Chapitre 17

Amélioration des performances

1. Considérations matérielles 339
 - 1.1 La mémoire ou RAM 339
 - 1.2 Le stockage 340
 - 1.3 Le réseau 341
2. Au niveau du processus "slapd" 341
 - 2.1 Paramétrage des threads. 341
3. Au niveau du backend 342
 - 3.1 Paramétrage du cache (ou la zone tampon) 342
 - 3.2 Paramétrage des index 346
 - 3.2.1 Syntaxe 347
 - 3.2.2 Exemples de configuration. 348
 - 3.2.3 Application 349
4. Changer de backend 349

Chapitre 18

Dépannage

1. Liste de contrôle (checklist) 353
2. Activer le mode "debug" 355
3. Activer et modifier la verbosité des logs 356

Chapitre 19

L'autogestion des comptes utilisateurs

1. Problématique 361
2. Infrastructure de gestion des identités 362
 - 2.1 Fonctionnement général 362
 - 2.2 Création/modification de compte 364
 - 2.3 Suppression de compte. 365

- 3. Présentation ITIM 366
 - 3.1 Bannière de connexion 368
 - 3.2 Espace de gestion des comptes de l'utilisateur 368
 - 3.3 Workflow 370
 - 3.4 Approbation 371
- 4. Intégration du serveur OpenLDAP dans ITIM. 373

Annexe

- 1. Le schéma "sudo" pour OpenLDAP 375
- 2. Quelques problèmes rencontrés. 377
 - 2.1 Cas 1 377
 - 2.2 Cas 2 378
 - 2.3 Cas 3 : reconfigurer le "checksum"
dans les fichiers de configuration 378
- 3. Déverrouiller les comptes. 379

- Index 383