

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

## Avant-propos

1. Présentation de Kubernetes	39
1.1 Un peu d'histoire	39
1.2 Qu'est-ce qu'un container ?	40
1.3 Les containers avant Docker	40
1.4 Pourquoi utiliser des containers ?	41
1.5 Problèmes introduits avec les containers	42
1.6 À quoi va servir Kubernetes ?	42
1.7 Ressources externes	43
2. Un mot sur l'application	43
2.1 Rien ne sert de courir	43
2.2 Les douze facteurs applicatifs	44
2.3 Microservices vs Monolithes	44

## Chapitre 1

### Introduction

1. Cibles et objectifs de l'ouvrage	45
2. Prérequis techniques et ressources documentaires	46
2.1 Prérequis techniques	46
2.2 Ressources documentaires	46
2.3 Récupération des fichiers d'exemples	47
3. Présentation générale	47
3.1 Prérequis	48
3.2 Utilisation de Kubernetes	48
3.3 Installation et configuration de Kubernetes	48

# 2 \_\_\_\_\_ **Kubernetes**

Plateforme de déploiement de vos applications

3.4	Extension du cluster Kubernetes et notions avancées . . . . .	49
3.5	Déploiement et intégration continue . . . . .	49
3.6	Conventions utilisées . . . . .	50

## **Chapitre 2**

### **Installation de l'environnement Kubernetes**

1.	Objectifs du chapitre et prérequis . . . . .	51
2.	Alternative à l'installation en local . . . . .	52
2.1	Pourquoi ces alternatives ? . . . . .	52
2.2	Utilisation d'un service managé . . . . .	52
2.3	Service Katacoda . . . . .	53
3.	Mise en place de la commande kubectl . . . . .	53
3.1	À quoi sert kubectl ? . . . . .	53
3.2	Installation de kubectl . . . . .	54
3.2.1	Installation sous Debian/Ubuntu . . . . .	54
3.2.2	Installation sous CentOS/RHEL ou Fedora . . . . .	54
3.3	Vérification de l'installation . . . . .	55
3.4	Configuration de l'autocomplétion . . . . .	55
3.4.1	Présentation du mécanisme d'auto-complétion . . . . .	55
3.4.2	Fichier profile à modifier . . . . .	56
3.4.3	Autocomplétion sur kubectl . . . . .	56
3.4.4	Utilisation de la variable SHELL . . . . .	57
4.	Mise en place de Minikube . . . . .	57
4.1	Pourquoi faire appel à Minikube ? . . . . .	57
4.2	Téléchargement et installation de Minikube . . . . .	57
4.3	Vérification de l'installation de Minikube . . . . .	58
4.4	Mise en place de l'auto-complétion . . . . .	59
5.	Installation du cluster Kubernetes avec Minikube . . . . .	59
5.1	Choix de l'hyperviseur . . . . .	59
5.2	Préparation de l'hyperviseur VirtualBox . . . . .	59
5.2.1	Installation de VirtualBox . . . . .	59

- 5.3 Préparation de l'hyperviseur KVM/libvirt ..... 60
  - 5.3.1 Installation de KVM et libvirt ..... 60
  - 5.3.2 Installation du driver KVM pour Minikube ..... 60
- 5.4 Configuration de l'utilisateur courant ..... 61
- 5.5 Déploiement du cluster avec Minikube ..... 62
  - 5.5.1 Création de la machine Minikube ..... 62
  - 5.5.2 Arrêt/démarrage de la machine Minikube ..... 65
  - 5.5.3 Container runtime alternatif ..... 66
  - 5.5.4 Extensions de Minikube ..... 67
  - 5.5.5 Suppression de la machine Minikube ..... 68
- 6. Quelques notions sur le format YAML ..... 68
  - 6.1 Déclaration de couples clés/valeurs ..... 69
  - 6.2 Les tableaux en YAML ..... 70
  - 6.3 Les structures clé/valeur ou table de hachage ..... 71
  - 6.4 Tableau de table de hachage ..... 72

**Chapitre 3**  
**Tableau de bord et ligne de commande**

- 1. Objectifs du chapitre et prérequis ..... 75
- 2. Préambule ..... 76
  - 2.1 Origine du nom et du logo ..... 76
  - 2.2 Pourquoi utiliser Kubernetes ? ..... 76
  - 2.3 Origine de Kubernetes ..... 77
  - 2.4 Fondation CNCF ..... 77
  - 2.5 Les orchestrateurs du marché ..... 78
- 3. Le tableau de bord de Kubernetes (dashboard) ..... 78
  - 3.1 Présentation ..... 78
  - 3.2 Tableau de bord Kubernetes sur service managé ..... 79
  - 3.3 Déploiement du dashboard sur Minikube ..... 79
  - 3.4 Accès au dashboard sur Minikube ..... 79
  - 3.5 Structure du tableau de bord ..... 80

# 4 **Kubernetes**

Plateforme de déploiement de vos applications

3.6	Création d'un déploiement	81
3.6.1	Un petit mot sur MailHog	81
3.6.2	Lancement du déploiement	82
3.7	État d'un déploiement	84
3.7.1	Consultation de l'état du déploiement	84
3.7.2	Consultation du gestionnaire de réplicats	86
3.7.3	Consultation de l'état d'un pod	87
3.7.4	Journal d'activité du container	88
3.7.5	Scalabilité	89
3.7.6	Mise à jour de l'application	90
3.7.7	Pour résumer	92
4.	Présentation de l'outil kubectl	92
4.1	Préambule	92
4.2	Consultation des éléments	92
4.3	Liste des pods	93
4.4	Liste des machines d'un cluster	94
4.4.1	Connexion à la machine Minikube	94
4.4.2	Liste des nœuds d'un cluster	95
4.4.3	Affichage des caractéristiques étendues	95
5.	Le moteur Docker de Minikube	96
5.1	Initialisation de l'environnement	96
5.2	Installation de Docker	97
5.3	Vérification de la communication avec le moteur Docker	97
5.4	Les containers associés aux pods	98

## **Chapitre 4**

### **Automatisation et publication d'une application**

1.	Objectifs du chapitre et prérequis	101
2.	Gestion par kubectl d'une application	101
2.1	Suppression d'un déploiement	101
2.2	Création d'un déploiement	102
2.3	État du déploiement	103

2.4	Mécanisme des réplicats. . . . .	105
2.4.1	Consultation des réplicats . . . . .	105
2.4.2	Description des réplicats . . . . .	106
2.5	État du pod . . . . .	107
2.5.1	Liste des pods . . . . .	107
2.5.2	Détails de l'état d'un pod . . . . .	108
2.6	Accès aux logs des containers . . . . .	109
2.7	Accéder à l'application MailHog . . . . .	110
3.	Exposition de services. . . . .	111
3.1	Pourquoi utiliser un service ? . . . . .	111
3.2	Exposition d'un déploiement via un service . . . . .	112
3.3	Vérification du service mailhog . . . . .	112
3.4	Que faire en cas d'absence de shell ? . . . . .	113
3.5	Résilience et scalabilité. . . . .	116
3.5.1	Origine du besoin . . . . .	116
3.5.2	Scalabilité manuelle . . . . .	116
3.5.3	Nombre de pods associés à un déploiement . . . . .	116
3.5.4	Arrêter temporairement une application . . . . .	117
4.	Automatisation de déploiement par fichier YAML . . . . .	118
4.1	Mécanisme de création et mise à jour . . . . .	118
4.2	Structure YAML d'un déploiement . . . . .	119
4.2.1	Quelques rappels. . . . .	119
4.2.2	Récupération d'une structure au format YAML . . . . .	119
4.2.3	Édition d'un déploiement. . . . .	121
4.2.4	Squelette pour un déploiement . . . . .	121
4.2.5	Création d'un déploiement à l'aide d'un fichier . . . . .	123
4.2.6	Suppression des éléments d'un fichier . . . . .	124
4.2.7	Gestion de l'idempotence et de la réentrance . . . . .	124
4.3	Création du service . . . . .	126
4.3.1	Définition du service . . . . .	126
4.3.2	Application de la définition du service . . . . .	127
4.3.3	Gestion de la réentrance. . . . .	127
4.4	Mécanisme de sélecteur et labels . . . . .	128

# 6 **Kubernetes**

Plateforme de déploiement de vos applications

4.5	Regroupement de la création des éléments. . . . .	129
4.5.1	Création d'un groupe d'objets . . . . .	129
4.5.2	Consultation de l'état d'un groupe d'objets . . . . .	130
4.6	Structure des objets . . . . .	131
4.6.1	Interrogation de Kubernetes avec kubectl . . . . .	131
4.6.2	Référence de l'API en ligne. . . . .	132
5.	Ingress et reverse proxy . . . . .	132
5.1	Origine du besoin . . . . .	132
5.2	Activation du contrôleur Ingress dans Minikube. . . . .	133
5.3	Déclaration d'une règle Ingress . . . . .	134
5.4	Consultation des règles Ingress . . . . .	134
5.5	Désactivation de la redirection HTTP vers HTTPS . . . . .	136
5.6	Hôte virtuel et nip.io . . . . .	137
5.6.1	Hôte virtuel par défaut. . . . .	137
5.6.2	Présentation du mécanisme de nip.io . . . . .	138
5.6.3	Création d'un hôte virtuel pour mailhog . . . . .	139

## **Chapitre 5**

### **Cycle de vie d'un container dans Kubernetes**

1.	Objectifs du chapitre et prérequis . . . . .	141
2.	Gestion des crashes d'application . . . . .	142
2.1	Consultation de l'état des pods . . . . .	142
2.2	Connexion au pod . . . . .	142
2.3	Container associé à MailHog. . . . .	143
2.4	Comportement en cas de crash . . . . .	145
2.5	État du container après redémarrage du pod . . . . .	146
2.6	Container vu depuis Docker (Minikube) . . . . .	146
2.7	Attention au nettoyage . . . . .	148
3.	État d'un container. . . . .	148
3.1	Pourquoi scruter l'état d'un container ? . . . . .	148
3.2	Readiness vs Liveness . . . . .	149
3.3	Utilisation et bonne pratique . . . . .	150

3.4	Structure des champs de surveillance . . . . .	150
3.5	Vérification de la présence d'un port. . . . .	151
3.5.1	Définition de la surveillance . . . . .	151
3.5.2	Test d'indisponibilité sur un pod non prêt . . . . .	153
3.5.3	État des pods en cas d'indisponibilité . . . . .	153
3.5.4	Test d'indisponibilité sur un pod en mauvaise santé. . . . .	154
3.5.5	État des pods en cas de problème sur un pod . . . . .	154
3.5.6	Attention à la consistance des tests . . . . .	155
3.5.7	Uniformisation des tests . . . . .	157
3.6	Surveillance HTTP . . . . .	157
3.6.1	Pourquoi privilégier ce type de surveillance ? . . . . .	157
3.6.2	Surveillance de l'application MailHog. . . . .	158
3.7	Point d'entrée de surveillance HTTP d'une application. . . . .	158
3.7.1	Un mot sur les frameworks modernes . . . . .	158
3.7.2	Présentation de l'application Flask . . . . .	159
3.7.3	Exemple de déclaration . . . . .	159
3.7.4	Déploiement de l'application Flask . . . . .	160
3.7.5	Consultation de l'état de l'application . . . . .	161
3.8	Lancement d'un shell . . . . .	162
3.8.1	Principe de fonctionnement. . . . .	162
3.8.2	Exemple de surveillance d'une base Postgres . . . . .	163
3.8.3	Déclaration de la commande . . . . .	163
4.	Définition de la capacité d'un pod. . . . .	164
4.1	Pourquoi définir une capacité ? . . . . .	164
4.2	Réservation et surallocation. . . . .	164
4.3	Allocation de ressources à un container . . . . .	165
4.4	Allocation de ressources à l'application MailHog. . . . .	166
4.5	Comportement en cas de saturation des ressources. . . . .	167
4.5.1	Demande trop importante de CPU . . . . .	167
4.5.2	Dépassement de la mémoire allouée . . . . .	168
4.6	Priorité d'un pod . . . . .	169
4.6.1	Présentation du mécanisme . . . . .	169
4.6.2	Consultation des types par défaut . . . . .	169

4.6.3	Consultation des priorités des pods . . . . .	170
4.6.4	Création d'une classe de priorité . . . . .	171
4.6.5	Affectation d'une classe de priorité personnalisée . . . . .	172
4.6.6	Remarque sur les classes de priorité par défaut . . . . .	173

## **Chapitre 6** **Persistance des données**

1.	Objectifs du chapitre et prérequis . . . . .	175
2.	Persistance des données . . . . .	175
2.1	Origine du besoin . . . . .	175
2.2	Utilisation d'un volume persistant externe . . . . .	176
2.3	Volumes persistants . . . . .	177
2.3.1	Structure du volume persistant . . . . .	177
2.3.2	Création du volume persistant . . . . .	178
2.4	Persistance de données avec MailHog . . . . .	178
2.4.1	Opérations à réaliser . . . . .	178
2.4.2	Déclaration de l'objet PersistentVolumeClaim . . . . .	179
2.4.3	État des objets de volume persistant . . . . .	180
2.4.4	État de la demande de volume persistant . . . . .	181
2.4.5	Déclaration du point de montage . . . . .	181
2.4.6	Ajout d'un point de montage sur le container . . . . .	182
2.4.7	Options de lancement de MailHog . . . . .	182
2.4.8	Déclaration entière suite aux modifications . . . . .	183
2.5	Test de la persistance . . . . .	185
2.5.1	Installation de mhsendmail . . . . .	185
2.5.2	Ouverture de la communication avec le port SMTP . . . . .	186
2.5.3	Envoi d'un mail . . . . .	186
2.5.4	Droits du répertoire de persistance des données . . . . .	187
2.5.5	Consultation de l'interface MailHog . . . . .	188
2.5.6	Suppression des pods . . . . .	189
2.5.7	Vérification du fonctionnement de la persistance . . . . .	189



- 3. Classes de stockage . . . . . 190
  - 3.1 Origine du besoin . . . . . 190
  - 3.2 Liste des classes de stockage . . . . . 191
  - 3.3 Détail d’une classe de stockage . . . . . 192
  - 3.4 Classe de stockage par défaut . . . . . 192
  - 3.5 Les différentes classes de stockage . . . . . 193
    - 3.5.1 Les différentes familles . . . . . 193
    - 3.5.2 Origine de ces familles . . . . . 193
  - 3.6 Caractéristiques des classes de stockage . . . . . 194
    - 3.6.1 Modes d’accès . . . . . 194
    - 3.6.2 Caractéristiques de certains pilotes . . . . . 195
    - 3.6.3 Liste des pilotes chargés . . . . . 196
  - 3.7 Déclaration d’une classe de stockage . . . . . 197
    - 3.7.1 Structure de la déclaration . . . . . 197
    - 3.7.2 Exemple de déclaration . . . . . 197
  - 3.8 Test de création automatique d’un volume persistant . . . . . 198

**Chapitre 7**

**Hébergement d’application en cluster**

- 1. Objectifs du chapitre et prérequis . . . . . 201
- 2. Déploiement d’une base de données MariaDB . . . . . 201
  - 2.1 Origine du besoin . . . . . 201
  - 2.2 Déploiement . . . . . 202
    - 2.2.1 Choix de l’image Docker . . . . . 202
    - 2.2.2 Version initiale du fichier de déploiement . . . . . 202
    - 2.2.3 Gestion de la réentrance . . . . . 203
  - 2.3 Volume persistant . . . . . 204
    - 2.3.1 Demande de volume persistant . . . . . 204
    - 2.3.2 État de la demande de volume persistant . . . . . 204
    - 2.3.3 Ajout d’une persistance sur le container de MariaDB . . 205
    - 2.3.4 Consultation de l’état du déploiement . . . . . 206
  - 2.4 Configuration de la base de données . . . . . 207

2.5	Consultation de l'état du pod	208
2.5.1	Liste des pods	208
2.5.2	Connexion au container	209
2.6	Surveillance de la base de données	209
2.6.1	Définition des commandes de surveillance	209
2.6.2	Application de la modification	211
2.6.3	Vérification du déploiement	211
2.7	Mécanisme de déploiement	212
3.	Mise en place d'un StatefulSet	214
3.1	Augmentation du nombre de pods associés au déploiement	214
3.2	Présentation du type StatefulSet	216
3.2.1	Caractéristiques	216
3.2.2	Limitations	216
3.3	Déclaration du premier objet StatefulSet	217
3.3.1	Purge de l'ancien déploiement	217
3.3.2	Modifications à réaliser	217
3.3.3	Création du StatefulSet	218
3.3.4	État des volumes persistants	219
3.3.5	Suppression des anciens objets PV/PVC	220
3.4	Scalabilité de l'objet StatefulSet	220
3.5	Pods et volumes persistants d'un objet StatefulSet	220
3.6	Réduction de la taille du StatefulSet	221
4.	Base et compte de test	222
4.1	Variables d'environnement du container	222
4.2	ConfigMap et secret	223
4.2.1	Pourquoi y faire appel ?	223
4.2.2	Structure d'un objet ConfigMap	223
4.2.3	Déclaration d'un objet Secret	224
4.2.4	Rattachement au container	225

**Chapitre 8**

**Mise en place d'une réplication entre pods**

- 1. Objectifs du chapitre et prérequis ..... 227
- 2. Synchronisation des pods MariaDB ..... 228
  - 2.1 Exposition de la problématique ..... 228
  - 2.2 Principe de fonctionnement de la synchronisation ..... 228
    - 2.2.1 Opérations à réaliser ..... 228
    - 2.2.2 Nombre de réplicats ..... 229
  - 2.3 Identifiants des serveurs ..... 229
    - 2.3.1 Connexion aux pods ..... 229
    - 2.3.2 Connexion à la base de données ..... 229
    - 2.3.3 Identifiants des serveurs ..... 230
    - 2.3.4 ID du maître ..... 230
    - 2.3.5 Création du compte de réplication sur le maître ..... 231
    - 2.3.6 Configuration de l'esclave ..... 232
  - 2.4 Activation de la synchronisation ..... 232
    - 2.4.1 Activer les journaux pour la réplication ..... 232
    - 2.4.2 Commande docker-entrypoint.sh ..... 233
    - 2.4.3 Consultation de l'état du maître ..... 234
    - 2.4.4 Configuration de l'esclave ..... 234
  - 2.5 Test de la réplication ..... 236
    - 2.5.1 Connexion au maître ..... 236
    - 2.5.2 Création d'une table ..... 236
    - 2.5.3 Connexion à l'esclave ..... 237
- 3. Automatisation de la synchronisation ..... 238
  - 3.1 Scripts de démarrage et synchronisation ..... 238
    - 3.1.1 Script de démarrage ..... 238
    - 3.1.2 Configuration de la synchronisation ..... 239
    - 3.1.3 Scripts SQL additionnels ..... 240
    - 3.1.4 Script d'arrêt de la base ..... 240
  - 3.2 Scripts et objet ConfigMap ..... 241
  - 3.3 Création du ConfigMap ..... 241

3.4	Montage du ConfigMap . . . . .	244
3.4.1	Référencement du ConfigMap dans la liste des volumes . . . . .	244
3.4.2	Point de montage du ConfigMap . . . . .	245
3.5	Démarrage et arrêt du container . . . . .	245
3.5.1	Commande de démarrage . . . . .	245
3.5.2	Commande d'arrêt de la base . . . . .	246
3.6	Résumé des modifications . . . . .	246
3.7	État du déploiement . . . . .	248
3.7.1	État des pods . . . . .	248
3.7.2	Journaux d'activité du pod esclave . . . . .	248
3.7.3	Test de la synchronisation . . . . .	248
3.7.4	Vérification du fonctionnement de la synchronisation . . . . .	249

## **Chapitre 9**

### **Gestion des briques internes de Kubernetes**

1.	Objectifs du chapitre et prérequis . . . . .	251
2.	Espace de noms kube-system . . . . .	251
2.1	Pods présents dans l'espace de noms kube-system . . . . .	251
2.2	CoreDNS . . . . .	252
2.3	etcd . . . . .	253
2.4	Le gestionnaire d'extensions de Minikube . . . . .	253
2.5	Le serveur d'API . . . . .	253
2.6	Le proxy Kubernetes (kube-proxy) . . . . .	254
2.7	Le gestionnaire de tâches (scheduler) . . . . .	254
2.8	Le gestionnaire de contrôle (controller manager) . . . . .	254
2.9	Kubelet . . . . .	254
3.	Configuration des serveurs maîtres . . . . .	255
3.1	Principe de lancement des pods système . . . . .	255
3.2	Contenu du répertoire /etc/kubernetes/manifests . . . . .	255
3.3	Contenu des fichiers . . . . .	256

- 3.4 Désactivation d'un pod système ..... 257
- 3.5 Réactivation du pod système. .... 258
- 4. Monitoring des containers du cluster avec Glances ..... 259
  - 4.1 Origine du besoin ..... 259
  - 4.2 Consultation des DaemonSets ..... 259
  - 4.3 Présentation de Glances ..... 260
  - 4.4 Définition du DaemonSet ..... 260
    - 4.4.1 Structure de la déclaration ..... 260
    - 4.4.2 Champ volumes ..... 261
    - 4.4.3 Champ containers ..... 261
  - 4.5 Création du DaemonSet. .... 262
    - 4.5.1 Déclaration complète ..... 262
    - 4.5.2 Création du DaemonSet. .... 262
    - 4.5.3 Consultation des pods ..... 263
  - 4.6 Annotations de tolérance ..... 264
    - 4.6.1 Présentation du mécanisme ..... 264
    - 4.6.2 Récupération des annotations taints ..... 264
    - 4.6.3 Tolérances de lancement ..... 265
    - 4.6.4 Modification du DaemonSet ..... 266
  - 4.7 Connexion à Glances ..... 267

**Chapitre 10**

**Helm - Gestionnaire de package**

- 1. Objectifs du chapitre et prérequis ..... 269
- 2. Présentation de Helm ..... 269
  - 2.1 Pourquoi faire appel à Helm ? ..... 269
  - 2.2 Principe de fonctionnement. .... 270
- 3. Déploiement de Helm ..... 271
  - 3.1 Installation du client Helm ..... 271
  - 3.2 Consultation de la version de Helm ..... 271
  - 3.3 Configuration du client Helm ..... 272

3.4	Initialisation de la partie serveur (Tiller) avec Helm 2.x . . . . .	272
3.4.1	Un mot sur la sécurité (Helm 2.x) . . . . .	272
3.4.2	Le compte de service de Tiller (Helm 2.x) . . . . .	273
3.4.3	Création du compte de service . . . . .	273
3.4.4	Attribution des droits d'administrateur au compte de service . . . . .	275
3.4.5	Initialisation de Tiller . . . . .	276
3.5	Suppression de Tiller (Helm 2) . . . . .	278
4.	Déploiement d'une application avec Helm . . . . .	278
4.1	Déterminer le package à déployer . . . . .	278
4.2	Installation du package Wordpress . . . . .	280
4.2.1	Un peu de vocabulaire . . . . .	280
4.2.2	Installation avec Tiller . . . . .	280
4.2.3	Installation sans Tiller . . . . .	282
4.3	Corrections de l'installation . . . . .	283
4.3.1	Quelques remarques . . . . .	283
4.3.2	Spécification du nom et espace de noms . . . . .	283
4.3.3	Lancement de l'installation . . . . .	283
4.3.4	Mise à jour et réentrance . . . . .	284
4.4	Éléments déployés avec Helm . . . . .	285
4.5	Suppression d'un déploiement . . . . .	286
4.6	Annulation de la suppression . . . . .	287
4.7	Purge d'un chart Helm . . . . .	288
5.	Cycle de vie d'une application déployée avec Helm . . . . .	289
5.1	Ouverture du port vers WordPress . . . . .	289
5.2	Connexion à WordPress . . . . .	290
5.3	Configuration d'un chart Helm . . . . .	291
5.3.1	Consultation des options d'un chart . . . . .	291
5.3.2	Configuration de la publication (Minikube) . . . . .	293
5.4	Historique de déploiement . . . . .	295
5.5	Retour arrière . . . . .	296
5.6	Portail Helm Hub . . . . .	297

**Chapitre 11**  
**Contextes et outils tiers Kubernetes**

- 1. Objectifs du chapitre et prérequis ..... 299
- 2. Gestion des contextes avec kubectl ..... 300
  - 2.1 Origine du besoin ..... 300
  - 2.2 Lister les contextes ..... 300
  - 2.3 Variable d’environnement KUBECONFIG ..... 301
    - 2.3.1 Spécifier l’emplacement du fichier ..... 301
    - 2.3.2 Spécifier plusieurs fichiers ..... 301
  - 2.4 Changement de contexte ..... 302
  - 2.5 Créer un contexte ..... 302
  - 2.6 Supprimer un contexte ..... 304
  - 2.7 Outils de gestion de contexte ..... 304
    - 2.7.1 Présentation de kubectx et kubens ..... 304
    - 2.7.2 Installation de kubectx et kubens ..... 305
    - 2.7.3 Mise en place de l’autocomplétion ..... 305
    - 2.7.4 Test des commandes ..... 306
  - 2.8 Contexte dans le prompt utilisateur ..... 306
    - 2.8.1 Pourquoi afficher le contexte ? ..... 306
    - 2.8.2 Activation à l’aide de oh-my-zsh ..... 307
    - 2.8.3 Activation avec bash ..... 307
    - 2.8.4 Exemple d’affichage ..... 307
  - 2.9 Changement des couleurs du terminal avec Konsole ..... 308
    - 2.9.1 Principe de fonctionnement ..... 308
    - 2.9.2 Création de la fonction ..... 308
    - 2.9.3 Ajout de l’appel dans l’invite de commande ..... 309
- 3. Utilitaires Kubernetes ..... 310
  - 3.1 K9s : interface texte de suivi ..... 310
    - 3.1.1 Contexte ..... 310
    - 3.1.2 Installation de k9s ..... 311
    - 3.1.3 Lancement de k9s ..... 311
  - 3.2 Kubespy : espionnage de l’activité ..... 312
    - 3.2.1 Présentation de Kubespy ..... 312

3.2.2	Installation de Kubespy . . . . .	312
3.2.3	Observation d'un déploiement avec Kubespy . . . . .	312
3.3	Krew : gestionnaire d'extensions. . . . .	313
3.3.1	Présentation du mécanisme d'extensions . . . . .	313
3.3.2	Installation de Krew . . . . .	314
3.3.3	Test de l'extension . . . . .	314
3.4	Sniff : capture du trafic réseau d'un pod . . . . .	315
3.4.1	Principe de fonctionnement. . . . .	315
3.4.2	Installation de Sniff et Wireshark . . . . .	316
3.4.3	Lancement d'une séance de capture . . . . .	316
3.5	Kube Hunter : outil d'analyse du cluster . . . . .	317
3.5.1	Présentation de Kube Hunter . . . . .	317
3.5.2	Lancement de l'analyse . . . . .	317
3.5.3	Résultat de l'analyse. . . . .	318
3.5.4	Publication de rapports HTML . . . . .	319
3.5.5	Lancement à intervalles réguliers . . . . .	321

**Chapitre 12****Services managés Kubernetes**

1.	Objectifs du chapitre et prérequis . . . . .	325
2.	Service managé de Google : GKE . . . . .	326
2.1	Présentation du service Google . . . . .	326
2.2	Administration depuis la console Google . . . . .	326
2.3	Installation de la commande gcloud en local . . . . .	328
2.3.1	Installation sur Debian/Ubuntu . . . . .	328
2.3.2	Mise en place de l'autocomplétion . . . . .	329
2.4	Configuration de l'environnement . . . . .	330
2.4.1	Authentification auprès de Google Cloud . . . . .	330
2.4.2	Projet associé avec le contexte courant . . . . .	332
2.4.3	Activation de l'API . . . . .	332
2.5	Gestion du cluster GKE . . . . .	333
2.5.1	Consultation de la liste des clusters . . . . .	333



2.5.2	Versions et régions disponibles . . . . .	334
2.6	Création d'un cluster . . . . .	334
2.6.1	Options de création . . . . .	334
2.6.2	Lancement de la création du cluster . . . . .	335
2.6.3	Récupération du fichier d'accès au cluster . . . . .	336
2.7	Consultation du cluster . . . . .	336
2.7.1	Liste des nœuds. . . . .	336
2.7.2	Services démarrés . . . . .	337
2.8	Délégation des droits d'accès . . . . .	338
2.8.1	Configuration des accès . . . . .	338
2.8.2	Principe du mécanisme sous-jacent. . . . .	339
2.9	Configuration de Helm/Tiller 2.x . . . . .	341
2.10	Suppression d'un cluster GKE . . . . .	341
3.	Service managé Microsoft Azure : AKS . . . . .	342
3.1	Présentation du service Azure . . . . .	342
3.2	Administration depuis la console Azure . . . . .	342
3.2.1	Présentation de la console . . . . .	342
3.2.2	Consultation du tableau de bord Kubernetes. . . . .	344
3.3	Installation de la commande az en local. . . . .	345
3.3.1	Installation sur Debian/Ubuntu . . . . .	345
3.3.2	Mise en place de l'autocomplétion . . . . .	346
3.4	Authentification auprès du service Azure. . . . .	347
3.5	Emplacement de déploiement . . . . .	348
3.5.1	Liste des emplacements . . . . .	348
3.5.2	Versions disponibles de Kubernetes . . . . .	349
3.6	Création d'un cluster . . . . .	350
3.6.1	Création d'un groupe de ressources. . . . .	350
3.6.2	Lancement de la création du cluster . . . . .	350
3.6.3	Récupération du fichier de connexion. . . . .	352
3.6.4	Zone DNS par défaut . . . . .	352
3.7	Consultation de la liste des clusters . . . . .	353
3.8	Délégation des droits d'accès . . . . .	353
3.9	Configuration de Helm/Tiller 2.x . . . . .	354

3.10	Suppression d'un cluster AKS	354
4.	Service managé d'Amazon : EKS	355
4.1	Présentation du service Amazon AWS	355
4.2	Introduction de la commande eksctl	356
4.3	Configuration des accès Amazon	356
4.4	Installation des binaires	360
4.4.1	Installation d'eksctl à l'aide de snap	360
4.4.2	Installation de l'outil aws cli	361
4.4.3	Vérification de la communication avec AWS	362
4.5	Création du cluster EKS	363
4.5.1	Aide en ligne d'eksctl	363
4.5.2	Options intéressantes à la création d'un cluster	363
4.5.3	Lancement de la création du cluster	364
4.6	Configuration des accès kubectl	366
4.7	Installation de aws-iam-authenticator	366
4.8	Délégation des droits d'accès	367
4.8.1	Configuration des accès	367
4.8.2	Principe du mécanisme sous-jacent	368
4.9	Configuration de Helm/Tiller 2.x	369
4.10	Suppression du cluster	370
5.	Accès en lecture-écriture multiple	370
5.1	Origine du besoin	370
5.2	Serveur NFS déployé dans Kubernetes	371
5.2.1	Limitations	371
5.2.2	Déploiement d'un serveur NFS	372
5.2.3	Vérification du déploiement	372
5.2.4	Test de création de volume persistant (PVC)	373
5.3	Service managé Amazon : EFS	373
5.3.1	Consultation des instances EFS	373
5.3.2	Création d'une instance EFS	374
5.3.3	Déploiement de la classe de stockage EFS	374
5.4	Service managé Google : Filestore	376
5.4.1	Consultation des instances Filestore	376

- 5.4.2 Création d'une instance Filestore ..... 376
- 5.5 Classe de stockage NFS ..... 377
  - 5.5.1 Installation du chart ..... 377
  - 5.5.2 Vérification de l'installation du chart ..... 378
  - 5.5.3 Test de création d'une demande  
de volume persistant (PVC) ..... 378
- 5.6 Classe de stockage Azure ..... 379

**Chapitre 13**

**Installation de Kubernetes en interne**

- 1. Objectifs du chapitre et prérequis ..... 381
- 2. Installation à l'aide de Kubespray ..... 382
  - 2.1 Origine du besoin ..... 382
  - 2.2 Pourquoi Kubespray ? ..... 382
  - 2.3 Principe de Kubespray ..... 382
  - 2.4 Prérequis des machines à administrer avec Ansible ..... 383
    - 2.4.1 Échange de clés SSH ..... 383
    - 2.4.2 Escalade de droits sudo ..... 383
  - 2.5 Structure du cluster ..... 385
    - 2.5.1 Architecture du cluster Kubespray ..... 385
    - 2.5.2 Groupes de machines ..... 385
  - 2.6 Préparation des éléments d'installation ..... 386
    - 2.6.1 Clonage du dépôt Git ..... 386
    - 2.6.2 Installation des prérequis ..... 386
  - 2.7 Préparation de l'inventaire Ansible ..... 387
    - 2.7.1 Qu'est-ce qu'un inventaire ? ..... 387
    - 2.7.2 Fichier d'inventaire d'exemple ..... 387
    - 2.7.3 Test de la communication Ansible/SSH ..... 389
  - 2.8 Installation du cluster ..... 390
    - 2.8.1 Configuration du cluster ..... 390
    - 2.8.2 Lancement de l'installation ..... 391
    - 2.8.3 Mise à jour du cluster ..... 392

2.9	Accès au cluster	392
2.9.1	Configuration de l'accès au cluster	392
2.9.2	Utilisation d'un répartiteur de charge	392
2.9.3	Vérification de la communication avec le cluster	393
3.	Environnement embarqué avec k3s	394
3.1	Présentation et but du projet	394
3.2	Installation de k3s	395
3.3	Lancement de k3s	395
3.4	Communication avec le cluster	395

## Chapitre 14

### Exposition des applications sur Internet

1.	Objectifs du chapitre et prérequis	397
2.	Gestion des entrées DNS	398
2.1	Principe de fonctionnement	398
2.2	Prérequis	399
2.3	Retour sur le fonctionnement du domaine DNS nip.io	399
2.4	Activation du service DNS	400
2.4.1	Console Cloud DNS Google	400
2.4.2	Service DNS Zones d'Azure	403
2.4.3	Service Route 53 d'AWS	404
2.5	Configuration DNS	405
2.5.1	Opération à réaliser	405
2.5.2	Console DNS OVH	405
2.5.3	Vérification de la délégation	407
2.6	Gestionnaire de DNS	408
2.6.1	Présentation de la brique external-dns	408
2.6.2	Création du compte d'administration DNS de Google Cloud	408
2.6.3	Création du compte d'administration DNS service Azure	410

- 2.6.4 Création du compte d'administration
      - DNS Amazon (Route 53) . . . . . 411
    - 2.6.5 Création d'un secret (Google et Azure) . . . . . 414
    - 2.6.6 Déploiement d'external-dns . . . . . 415
    - 2.6.7 Vérification du fonctionnement d'external-dns . . . . . 416
  - 3. Exposition de services et répartition de charge . . . . . 417
    - 3.1 Présentation du mécanisme . . . . . 417
    - 3.2 Retour sur la notion de service . . . . . 417
      - 3.2.1 Rôle d'un service . . . . . 417
      - 3.2.2 Structure d'un service . . . . . 418
      - 3.2.3 Type ClusterIP . . . . . 418
      - 3.2.4 Type NodePort et LoadBalancer . . . . . 419
      - 3.2.5 Type ExternalName . . . . . 419
    - 3.3 Service associé au proxy inverse . . . . . 419
  - 4. Le contrôleur Ingress . . . . . 420
    - 4.1 Principe de fonctionnement . . . . . 420
    - 4.2 Le rôle du contrôleur Ingress . . . . . 421
    - 4.3 Structure d'une règle Ingress . . . . . 421
    - 4.4 Droits nécessaires pour un contrôleur . . . . . 422
  - 5. Le contrôleur Ingress Google . . . . . 423
    - 5.1 Prérequis . . . . . 423
    - 5.2 Présentation du contrôleur GLBC . . . . . 423
    - 5.3 Déploiement de MailHog . . . . . 424
      - 5.3.1 Préparation de la règle Ingress . . . . . 424
      - 5.3.2 Déploiement de l'application MailHog . . . . . 425
      - 5.3.3 Consultation de l'état de l'objet Ingress . . . . . 425
      - 5.3.4 Consultation du journal d'activité d'external-dns . . . . . 425
      - 5.3.5 Consultation de MailHog . . . . . 427
  - 6. Le contrôleur Ingress Nginx . . . . . 429
    - 6.1 Pourquoi changer de contrôleur Ingress ? . . . . . 429
    - 6.2 Présentation du logiciel Nginx . . . . . 430
    - 6.3 Installation d'Ingress Nginx sur GKE (Google) . . . . . 430
      - 6.3.1 Détermination du chart Helm à installer . . . . . 430

6.3.2	Espace de noms et configuration du chart	431
6.4	Utilisation du contrôleur	432
6.4.1	Utilisation de l'annotation kubernetes.io/ingress.class	432
6.4.2	Vérification du déploiement	433
6.5	Annotations Ingress Nginx	434
7.	Le contrôleur Ingress Traefik	435
7.1	Présentation de Traefik	435
7.2	Installation du chart Helm	435
7.3	Utilisation du nouveau contrôleur Ingress	437
7.3.1	Sélectionner le contrôleur Ingress Traefik	437
7.3.2	Création de la règle Ingress faisant appel à Traefik	437
7.3.3	État des règles Ingress	438
7.4	Tableau de bord de Traefik	439
7.5	Annotations Ingress Traefik	440

## Chapitre 15

### Sécurisation : accès aux applications

1.	Objectifs du chapitre et prérequis	441
2.	Mise en place de Let's Encrypt	442
2.1	Présentation de Let's Encrypt	442
2.2	Installation du chart Helm cert-manager	442
2.2.1	Présentation du chart Helm	442
2.2.2	Prérequis avant installation	443
2.3	L'émetteur de certificats (issuer)	444
2.3.1	Principe du protocole ACME	444
2.3.2	Structure de la déclaration d'un émetteur	445
2.3.3	Exemple de déclaration Issuer Google	446
2.3.4	Exemple de déclaration Issuer Azure	447
2.3.5	Exemple de déclaration Issuer Amazon	447
2.3.6	Limitations et certificats avec joker	448
2.4	Exemples de déclarations	449
2.4.1	Serveur Let's Encrypt de test	449

- 2.4.2 Serveur Let's Encrypt de production . . . . . 450
- 2.5 Déclaration des certificats . . . . . 450
  - 2.5.1 État des émetteurs de certificats . . . . . 450
  - 2.5.2 Structure d'un certificat . . . . . 451
  - 2.5.3 Certificat de test . . . . . 452
  - 2.5.4 État du certificat . . . . . 452
  - 2.5.5 Journal d'activité de cert-manager . . . . . 453
  - 2.5.6 Consultation du secret . . . . . 455
  - 2.5.7 Certificat de production . . . . . 456
  - 2.5.8 Marche à suivre en cas de problèmes . . . . . 458
- 2.6 Rattachement du certificat à la règle Ingress . . . . . 458
- 2.7 Automatisation de la gestion des certificats . . . . . 460
  - 2.7.1 Certificat par défaut du contrôleur Ingress Nginx . . . . . 460
  - 2.7.2 Mécanisme d'annotations . . . . . 461
  - 2.7.3 Émetteur de certificats par défaut . . . . . 462
- 3. Protection de l'accès aux applications . . . . . 463
  - 3.1 Origine du besoin . . . . . 463
  - 3.2 Mot de passe simple (HTTP basic) . . . . . 463
    - 3.2.1 Principe de fonctionnement . . . . . 463
    - 3.2.2 Création du secret à l'aide de htpasswd . . . . . 463
    - 3.2.3 Import du secret . . . . . 464
    - 3.2.4 Configuration de l'authentification . . . . . 464
- 4. Authentification basée sur OAuth2 . . . . . 467
  - 4.1 À propos du protocole OAuth2 . . . . . 467
  - 4.2 Principe de la solution . . . . . 467
  - 4.3 Création d'un identifiant GitHub . . . . . 468
  - 4.4 Déploiement du proxy . . . . . 469
    - 4.4.1 À propos du proxy . . . . . 469
    - 4.4.2 Configuration du chart Helm . . . . . 470
    - 4.4.3 Déploiement du chart Helm . . . . . 471
    - 4.4.4 État du déploiement . . . . . 471
  - 4.5 Déclaration des règles Ingress . . . . . 471
    - 4.5.1 Description des règles Ingress . . . . . 471

4.5.2	Annotations Ingress de MailHog . . . . .	472
4.5.3	Description Ingress du proxy OAuth . . . . .	472
4.5.4	Déclaration des règles Ingress . . . . .	472
4.6	Tests de connexion . . . . .	474
4.7	Restriction des accès . . . . .	475
4.7.1	Mécanisme d'autorisation . . . . .	475
4.7.2	Restriction par domaine e-mail . . . . .	476
4.7.3	Restriction par organisation GitHub . . . . .	476

## **Chapitre 16**

### **Polices réseau**

1.	Objectifs du chapitre et prérequis . . . . .	479
2.	Les polices réseau (network policies) . . . . .	479
2.1	Présentation du mécanisme . . . . .	479
2.2	Kubernetes Network Plugins . . . . .	480
2.3	Polices réseau sur services managés et installation maison . . . . .	480
2.4	Installation de Calico sur Minikube . . . . .	481
2.4.1	Activation de CNI sur Minikube . . . . .	481
2.4.2	Installation de Calico . . . . .	481
2.5	Connexions entrantes . . . . .	482
2.5.1	Test de la connexion en interne . . . . .	482
2.5.2	Bloquer les accès internes . . . . .	482
2.5.3	Test de la règle . . . . .	484
2.6	Connexions sortantes . . . . .	484
2.6.1	Test des connexions externes . . . . .	484
2.6.2	Restriction sur les règles sortantes . . . . .	485
2.6.3	Test de la règle . . . . .	485
3.	Protection de l'application WordPress . . . . .	486
3.1	Contexte . . . . .	486
3.2	Déploiement de WordPress . . . . .	486
3.3	Restriction des accès . . . . .	487
3.3.1	Référencement de l'ensemble des flux . . . . .	487



- 3.3.2 Restriction de tous les accès . . . . . 487
- 3.3.3 Autorisation de l'accès du contrôleur Ingress  
sur WordPress . . . . . 488
- 3.3.4 Autorisation de l'accès entre WordPress et MariaDB . . . 489
- 3.3.5 Test des règles réseau . . . . . 491
- 3.4 Ressources externes . . . . . 492

**Chapitre 17**  
**Montée en charge automatique**

- 1. Objectifs du chapitre et prérequis . . . . . 493
- 2. Le serveur de métriques . . . . . 494
  - 2.1 Présentation de la brique metrics-server . . . . . 494
  - 2.2 Activation du serveur de métriques . . . . . 494
    - 2.2.1 Vérification de la présence du serveur de métriques . . . 494
    - 2.2.2 Activation sous Minikube . . . . . 495
    - 2.2.3 Activation sur Amazon EKS . . . . . 495
  - 2.3 Consultation de la consommation des pods et des nœuds . . . 496
    - 2.3.1 État des nœuds d'un cluster . . . . . 496
    - 2.3.2 État des pods . . . . . 496
- 3. Activation de la montée en charge automatique . . . . . 497
  - 3.1 Test avec l'application MailHog . . . . . 497
  - 3.2 Lancement d'un bench . . . . . 498
    - 3.2.1 Présentation d'Apache Bench . . . . . 498
    - 3.2.2 Installation d'Apache Bench . . . . . 498
    - 3.2.3 Lancement du test initial . . . . . 499
  - 3.3 Gestion de la montée en charge . . . . . 499
  - 3.4 Lancement du test . . . . . 501
    - 3.4.1 Test à froid : montée en charge des pods . . . . . 501
    - 3.4.2 Test à chaud . . . . . 501
    - 3.4.3 Diminution du nombre de pods . . . . . 502
- 4. Scalabilité des nœuds d'un cluster . . . . . 502
  - 4.1 Contexte . . . . . 502

4.2	Présentation de l'autoscaler . . . . .	503
4.3	Activation de l'autoscaler avec Google Cloud . . . . .	503
4.4	Activation de l'autoscaler avec Azure AKS . . . . .	504
4.5	Activation de l'autoscaler avec Amazon EKS . . . . .	506
4.5.1	Présentation du mécanisme de l'ASG . . . . .	506
4.5.2	Affichage des tags d'un groupe ASG . . . . .	506
4.5.3	Activation de l'autoscaler. . . . .	507
4.5.4	Vérification de l'activation du mécanisme de l'autoscaler . . . . .	508
4.6	Test de montée en charge . . . . .	508
4.6.1	Déploiement de WordPress . . . . .	508
4.6.2	Pods en attente de ressources. . . . .	509
4.6.3	État des nœuds . . . . .	510
4.6.4	Démarrage du pod . . . . .	510
4.6.5	Nettoyage des déploiements . . . . .	511

## **Chapitre 18**

### **Surveillance à l'aide de Prometheus**

1.	Objectifs du chapitre et prérequis . . . . .	513
2.	Mise en place de Prometheus. . . . .	514
2.1	À propos de Prometheus . . . . .	514
2.2	Fonctionnement de Prometheus . . . . .	515
2.2.1	Architecture de Prometheus . . . . .	515
2.2.2	Le moteur Prometheus . . . . .	515
2.2.3	Les exporteurs Prometheus . . . . .	516
2.3	Installation de Prometheus . . . . .	517
2.3.1	Choix du chart Prometheus . . . . .	517
2.3.2	Qu'est-ce qu'un opérateur ? . . . . .	517
2.3.3	Déploiement de l'opérateur Prometheus. . . . .	518
2.3.4	Pods démarrés . . . . .	519
2.3.5	Objets déploiements. . . . .	520
2.3.6	Nouvelles ressources Prometheus . . . . .	521

- 2.3.7 DaemonSet : node exporter . . . . . 522
- 2.4 Priorisation des briques de surveillance . . . . . 522
  - 2.4.1 Problème de la surveillance . . . . . 522
  - 2.4.2 Déclaration des classes de priorité . . . . . 522
  - 2.4.3 Modification du déploiement de Prometheus . . . . . 523
- 3. Utilisation de Prometheus . . . . . 524
  - 3.1 Fonctionnement des métriques . . . . . 524
    - 3.1.1 Consultation des métriques de Prometheus . . . . . 524
    - 3.1.2 Présentation de l'interface de Prometheus . . . . . 525
    - 3.1.3 Métriques de Kubernetes . . . . . 526
    - 3.1.4 Déclaration des points de collecte dans Kubernetes . . . . . 527
    - 3.1.5 Consultation des points de collecte dans Prometheus . . . . . 528
  - 3.2 Définition des alertes . . . . . 529
    - 3.2.1 Consultation de la liste des alertes . . . . . 529
    - 3.2.2 Structure d'une règle d'alerte . . . . . 530
    - 3.2.3 Définition d'alertes . . . . . 531
  - 3.3 Gestionnaire d'alertes . . . . . 532
    - 3.3.1 Rôle du gestionnaire d'alertes . . . . . 532
    - 3.3.2 Consultation du gestionnaire d'alertes . . . . . 533
    - 3.3.3 Configuration des alertes . . . . . 533
    - 3.3.4 Désactivation des alertes scheduler  
et manager (clusters managés) . . . . . 534
    - 3.3.5 Configuration de l'envoi des notifications . . . . . 536
    - 3.3.6 Adresse de l'API de Slack . . . . . 537
- 4. Tableaux de bord Grafana . . . . . 540
  - 4.1 Présentation de Grafana . . . . . 540
  - 4.2 Configuration de Grafana . . . . . 540
    - 4.2.1 Branchement au moteur Prometheus . . . . . 540
    - 4.2.2 Définition des tableaux de bord . . . . . 541
  - 4.3 Interface Grafana . . . . . 542
  - 4.4 Sécurisation de l'accès à Grafana . . . . . 543
- 5. Suppression du chart de Prometheus . . . . . 544

**Chapitre 19****Centralisation des journaux d'activité**

1. Objectifs du chapitre et prérequis . . . . .	545
2. Principe de la centralisation des journaux. . . . .	546
2.1 Architecture . . . . .	546
2.2 Caractéristiques de l'agent déployé. . . . .	547
2.3 Mécanisme de centralisation des journaux. . . . .	547
3. Centralisation dans le cloud. . . . .	548
3.1 Centralisation à l'aide d'un service managé . . . . .	548
3.2 Google Stackdriver . . . . .	548
3.2.1 Présentation de Stackdriver . . . . .	548
3.2.2 Pod Fluentd (cluster GKE) . . . . .	549
3.2.3 Consultation des journaux . . . . .	549
3.3 Azure Monitor . . . . .	550
3.3.1 Présentation d'Azure Monitor . . . . .	550
3.3.2 Consultation des journaux . . . . .	550
3.4 Amazon Cloudwatch . . . . .	551
3.4.1 Présentation de Cloudwatch . . . . .	551
3.4.2 Activation de Cloudwatch sur le centre de contrôle . . . . .	551
3.4.3 Configuration de Cloudwatch. . . . .	553
3.4.4 Création de la police de communication avec Cloudwatch . . . . .	553
3.4.5 Création d'un compte et rattachement à la police. . . . .	555
3.4.6 Création d'une clé d'accès . . . . .	555
3.4.7 Envoi des journaux dans Cloudwatch . . . . .	556
3.4.8 État des pods déployés . . . . .	557
3.4.9 Consultation des journaux dans Cloudwatch . . . . .	558
4. Centralisation des journaux avec Loki . . . . .	559
4.1 Présentation de Loki . . . . .	559
4.1.1 Origine de Loki . . . . .	559
4.1.2 Loki vs Elasticsearch. . . . .	560
4.1.3 Conseil d'utilisation . . . . .	560

4.2	Installation de Loki . . . . .	560
4.3	Configuration de la source de données Grafana . . . . .	561
4.4	Consultation des journaux dans Grafana . . . . .	563
4.4.1	Vérification des sources de données . . . . .	563
4.4.2	Consultation des journaux . . . . .	563
5.	Centralisation des journaux avec Elasticsearch . . . . .	565
5.1	Avertissements et limitations . . . . .	565
5.2	À propos d'Elasticsearch. . . . .	565
5.3	Déploiement des briques Elasticsearch . . . . .	565
5.3.1	Installation d'Elasticsearch . . . . .	565
5.3.2	Installation de l'agent fluent-bit . . . . .	567
5.3.3	Installation de Kibana . . . . .	568
5.3.4	Installation de Cerebro. . . . .	568
5.4	État des différentes briques . . . . .	569
5.4.1	État du moteur Elasticsearch . . . . .	569
5.4.2	Agent fluent-bit . . . . .	569
6.	Gestion d'Elasticsearch. . . . .	570
6.1	Accès à l'interface Cerebro. . . . .	570
6.2	Utilisation de Kibana . . . . .	572
6.2.1	Accéder à l'interface de Kibana . . . . .	572
6.2.2	Création de l'index . . . . .	573
6.3	Branchement sur Grafana . . . . .	575
6.3.1	Source de données Elasticsearch . . . . .	575
6.3.2	Création d'un objet ConfigMap . . . . .	575

## Chapitre 20

### Maillage de services avec Istio

1.	Objectifs du chapitre et prérequis . . . . .	577
2.	Présentation d'Istio . . . . .	578
2.1	Micro-services et mise en réseau de services . . . . .	578
2.2	Présentation d'Istio. . . . .	579
2.3	Principe de fonctionnement. . . . .	579

3.	Installation d'Istio	581
3.1	Configuration d'external-dns	581
3.2	Dépôt des charts Istio	582
3.3	Installation du chart istio-init	583
3.4	Installation du chart Istio	583
3.4.1	Activation des tableaux de bord	583
3.4.2	Activation du mécanisme SDS	585
3.4.3	Configuration d'Istio	585
3.4.4	Installation d'Istio	587
3.5	Configuration du gateway Istio	588
3.5.1	Présentation du mécanisme	588
3.5.2	Configuration du gateway	588
3.5.3	Génération du certificat	589
4.	Utilisation d'Istio	590
4.1	Injection de pods dans le maillage de services	590
4.1.1	Installation d'istiocli	591
4.1.2	Injection du sidecar à l'aide d'istiocli	591
4.1.3	Injection du sidecar par annotation	592
4.1.4	Désactivation du sidecar par annotation	592
4.2	Déploiement d'une application de test	593
4.2.1	Principe de l'exposition d'application avec Istio	593
4.2.2	Préparation du fichier de déploiement MailHog	593
4.2.3	Déclaration du service MailHog	595
4.2.4	Création du gateway	596
4.2.5	Création du service virtuel (VirtualService)	597
4.3	Sécurisation des flux	599
4.3.1	Activation de Mutual TLS (mTLS)	599
4.3.2	Consultation des polices du service MailHog	600
4.3.3	Forcer l'utilisation de mTLS	600
5.	Tableaux de bord	603
5.1	Présentation des différentes briques	603
5.2	Interface Kiali	604
5.3	Interface Grafana	605

5.4 Interface Jaeger . . . . .	607
--------------------------------	-----

## Chapitre 21

### Compilation et stockage d'image Docker

1. Objectifs du chapitre et prérequis . . . . .	609
2. Création d'une image Docker . . . . .	610
2.1 Application d'exemple Flask Healthcheck . . . . .	610
2.1.1 Présentation de l'application . . . . .	610
2.1.2 Présentation des dépendances . . . . .	610
2.1.3 Description des dépendances . . . . .	610
2.1.4 Installation des dépendances . . . . .	611
2.1.5 Initialisation de l'application . . . . .	611
2.1.6 Fonction racine . . . . .	612
2.1.7 Lancement du programme . . . . .	612
2.2 Environnement de compilation . . . . .	615
2.3 Le fichier Dockerfile . . . . .	616
2.3.1 Présentation du format . . . . .	616
2.3.2 Création de l'image . . . . .	616
2.3.3 Compilation et tag de l'image . . . . .	617
2.3.4 Authentification sur le registre d'images Docker . . . . .	618
2.3.5 Pousser l'image sur le registre . . . . .	619
3. Image Docker multi-étape (multi-stage) . . . . .	620
3.1 Origine du besoin . . . . .	620
3.2 Exemple de compilation avec Maven . . . . .	621
4. Analyse d'images . . . . .	621
4.1 Historique des commandes . . . . .	621
4.2 Analyse de l'image : Dive . . . . .	622
4.2.1 Présentation de Dive . . . . .	622
4.2.2 Installation de Dive . . . . .	622
4.2.3 Consultation du contenu d'une image . . . . .	622
5. Utilisation de registres Docker privés . . . . .	623
5.1 Origine du besoin . . . . .	623

5.2	Déploiement d'image d'un registre privé . . . . .	624
5.2.1	Exposition de la problématique . . . . .	624
5.2.2	Création du secret . . . . .	624
5.2.3	Utilisation du secret . . . . .	625
5.2.4	Recopie d'un secret entre espaces de noms . . . . .	626
5.3	Erreurs de récupération des images . . . . .	627
5.3.1	Détection des erreurs . . . . .	627
5.3.2	Erreur sur le nom de l'image . . . . .	627
5.3.3	Secret absent ou non spécifié . . . . .	627
5.3.4	Identifiants invalides . . . . .	628
5.4	Services de registres managés . . . . .	628
5.4.1	Solutions managées . . . . .	628
5.4.2	Service Google Container Registry . . . . .	628
5.4.3	GitLab.com . . . . .	630

## Chapitre 22

### Usine logicielle

1.	Objectifs du chapitre et prérequis . . . . .	633
2.	Compilation à l'aide de GitLab . . . . .	634
2.1	Application à compiler . . . . .	634
2.2	Mécanisme de pipeline GitLab . . . . .	634
2.3	Adresse et contenu du dépôt . . . . .	634
2.4	Structure du fichier <code>.gitlab-ci.yml</code> . . . . .	635
2.5	Exemple de fichier <code>.gitlab-ci.yml</code> de compilation d'image . . . . .	636
2.6	Pour la suite . . . . .	638
3.	Déploiement continu avec Jenkins . . . . .	639
3.1	À propos de Jenkins . . . . .	639
3.2	Installation de Jenkins . . . . .	639
3.2.1	Configuration du chart . . . . .	639
3.2.2	Vérification de l'installation . . . . .	640
3.2.3	Connexion à l'interface de Jenkins . . . . .	640
3.2.4	Installation d'extensions . . . . .	641



4. Pipeline de déploiement continu avec Jenkins . . . . .	642
4.1 Prérequis . . . . .	642
4.2 Présentation du mécanisme de déploiement continu . . . . .	642
4.3 Stockage des identifiants Docker. . . . .	643
4.4 Création de l'environnement develop . . . . .	643
4.5 Création du pipeline . . . . .	643
4.5.1 Création du pod de compilation . . . . .	643
4.5.2 Squelette du pipeline de déploiement . . . . .	646
4.5.3 Récupération du code source . . . . .	647
4.5.4 Vérifications et tests. . . . .	647
4.5.5 Compilation de l'image Docker. . . . .	648
4.5.6 Connexion au registre et publication . . . . .	648
4.5.7 Mise à jour du déploiement de test . . . . .	649
4.5.8 Programme complet . . . . .	650
4.6 Lancement de la compilation. . . . .	652
4.6.1 Création du job . . . . .	652
4.6.2 Lancement du build . . . . .	653
4.7 Compte de service. . . . .	654
4.7.1 Opérations à réaliser. . . . .	654
4.7.2 Création d'un compte de service . . . . .	654
4.7.3 Création du rôle de mise à jour . . . . .	654
4.7.4 Affectation du rôle au compte de service . . . . .	655
4.7.5 Affectation du compte de service . . . . .	656
4.7.6 Relance de la compilation . . . . .	656
4.8 Mécanisme de Webhook . . . . .	657
4.8.1 Présentation du mécanisme . . . . .	657
4.8.2 Déclenchement du Webhook. . . . .	657
4.8.3 Création du Webhook . . . . .	658
5. Un mot sur Jenkins X. . . . .	659

**Chapitre 23****Packager son application avec Helm**

1. Objectifs du chapitre et prérequis . . . . .	661
2. Helm . . . . .	661
2.1 Origine du besoin . . . . .	661
2.2 Création d'un chart . . . . .	662
2.3 Contenu d'un package . . . . .	662
2.3.1 Structure d'un package . . . . .	662
2.3.2 Variables .Values, .Chart et .Release . . . . .	663
2.4 Adaptation à l'application MailHog . . . . .	663
2.4.1 Résumé des travaux à réaliser . . . . .	663
2.4.2 Utilisation de l'image de MailHog . . . . .	664
2.4.3 Correction sur les ports de service . . . . .	664
2.4.4 Ajout d'un ConfigMap . . . . .	665
2.4.5 Ajout du volume persistant . . . . .	666
2.4.6 Montage du volume dans le container . . . . .	667
2.4.7 Test de déploiement . . . . .	668
2.5 Dépendances . . . . .	669
2.5.1 Déclaration des dépendances . . . . .	669
2.5.2 Récupération des dépendances . . . . .	670
2.5.3 Déploiement du chart avec les dépendances . . . . .	671
3. Template Go . . . . .	671
3.1 Principe de fonctionnement . . . . .	671
3.2 Substitution du contenu d'une variable . . . . .	672
3.3 Blocs conditionnels . . . . .	672
3.4 Gestion des conditions . . . . .	673
3.4.1 Les valeurs de vrai ou faux . . . . .	673
3.4.2 Opérateurs de comparaison . . . . .	673
3.4.3 Conditions multiples et négation . . . . .	674
3.5 Itération . . . . .	674
3.5.1 Affichage du contenu d'un tableau . . . . .	674
3.5.2 Suppression des sauts de lignes surnuméraires . . . . .	675
3.5.3 Itération sur un groupe fixe d'éléments . . . . .	676

3.5.4	Itération sur un tableau de hachage	676
3.5.5	Accéder à une variable globale depuis une boucle	677
3.6	Filtres	677
3.7	Valeurs par défaut	678
3.8	Fonction template	678
3.8.1	Exemple de définition de fonction	678
3.8.2	Passage de paramètres et contexte global	679
3.9	Redéploiement sur changement de configuration	680
3.9.1	Exposition de la problématique	680
3.9.2	Principe de la solution	680
3.9.3	Exemple d'implémentation	680

## Chapitre 24

### Restriction et délégation d'accès

1.	Objectifs du chapitre et prérequis	683
2.	Mise en place de quotas	684
2.1	Origine du besoin	684
2.2	Quotas par défaut sur un espace de noms	684
2.2.1	Création d'un espace de noms	684
2.2.2	Structure d'un objet LimitRange	685
2.2.3	Exemple de définition de limitations	686
2.2.4	Vérification de l'application des limitations	687
2.2.5	Test du mécanisme	688
2.2.6	Analyse du problème	688
2.3	Quotas globaux sur un espace de noms	689
2.3.1	Présentation des quotas de ressources (ResourceQuota)	689
2.3.2	Structure d'un quota de ressources	690
2.3.3	Exemples de restriction de consommation CPU et mémoire	690
2.3.4	Champs pour positionner des limitations (champ hard)	691
2.3.5	Test du mécanisme	692

2.3.6	Nettoyage en fin d'exercice . . . . .	693
3.	Authentification et autorisation . . . . .	694
3.1	Origine du besoin . . . . .	694
3.2	Prérequis . . . . .	695
3.3	Activation des accès anonymes . . . . .	695
3.3.1	Activation des accès anonymes sur Minikube . . . . .	695
3.3.2	Création du fichier d'accès. . . . .	696
3.3.3	Affectation des droits en lecture . . . . .	697
3.3.4	Suppression des droits d'accès anonymes. . . . .	698
3.4	Principe de l'authentification par certificat . . . . .	698
3.5	Problème de la révocation des certificats . . . . .	699
3.6	Génération du certificat . . . . .	699
3.6.1	Création de la clé et du certificat client . . . . .	699
3.6.2	Emplacement de la PKI . . . . .	700
3.6.3	Signature du certificat . . . . .	702
3.7	Authentification par certificat. . . . .	703
3.7.1	Récupération des informations de connexion au cluster . . . . .	703
3.7.2	Utilisation du certificat pour l'authentification. . . . .	704
3.7.3	Test de la connexion . . . . .	705
3.8	Quelques exemples d'erreurs de manipulation. . . . .	706
3.8.1	Problème d'autorité de certification . . . . .	706
3.8.2	Problème de couple clé/certificat. . . . .	707
3.8.3	Pas d'identifiant renseigné. . . . .	707
3.8.4	Utilisation de la demande de certificat à la place du certificat. . . . .	707
3.9	Attributions de droits administrateur sur le cluster. . . . .	707
3.9.1	Contexte et opérations à réaliser. . . . .	707
3.9.2	Affectation des droits administrateur à un utilisateur . . . . .	708
3.9.3	Test du nouvel administrateur . . . . .	709
3.9.4	Création de nouveaux utilisateurs . . . . .	710
3.9.5	Affectation des droits administrateur à un groupe . . . . .	711
3.9.6	Administrateur d'un espace de noms . . . . .	711

- 4. Mécanismes d'authentification externes ..... 713
  - 4.1 Présentation du mécanisme ..... 713
  - 4.2 Communication entre le fournisseur OAuth2 et le cluster ... 714
  - 4.3 Création des identifiants ..... 715
  - 4.4 Modification des options de démarrage (Minikube) ..... 716
  - 4.5 Configuration des accès clients ..... 718
    - 4.5.1 Présentation de l'outil k8s-oidc-helper ..... 718
    - 4.5.2 Installation du compilateur Go ..... 718
    - 4.5.3 Installation de k8s-oidc-helper ..... 718
    - 4.5.4 Génération des identifiants d'accès ..... 718
    - 4.5.5 Renseignement du cluster et contexte ..... 720
    - 4.5.6 Test de connexion ..... 721
  - 4.6 Attribution des droits d'accès ..... 722

**Chapitre 25**  
**Les opérateurs Kubernetes**

- 1. Objectifs du chapitre et prérequis ..... 723
- 2. Utilisation des opérateurs ..... 724
  - 2.1 Présentation du principe ..... 724
  - 2.2 L'opérateur de Prometheus ..... 724
    - 2.2.1 Retour sur le chart prometheus-operator ..... 724
    - 2.2.2 Structure d'un objet Prometheus ..... 725
  - 2.3 Ressources externes sur les opérateurs existants ..... 727
  - 2.4 Présentation de l'opérateur MySQL ..... 727
    - 2.4.1 Justification du choix de MySQL ..... 727
    - 2.4.2 Choix de l'opérateur ..... 728
  - 2.5 Déploiement de l'opérateur ..... 728
  - 2.6 Création d'une instance MysqlCluster ..... 729
    - 2.6.1 Création d'un secret pour l'instance MysqlCluster ... 729
    - 2.6.2 Création du cluster ..... 730

2.7	Objets créés au déploiement du cluster	731
2.7.1	Volumes persistants	731
2.7.2	Services MySQL	732
2.8	Tableau de bord de l'opérateur	732
2.9	Test de la réplication	735
2.9.1	Connexion aux instances maître et esclave	735
2.9.2	Création d'une table	736
2.9.3	Alimentation de la table	736
2.9.4	Changement du nombre de réplicats	737
2.10	Pour conclure	738

## Annexes

1.	bash vs zsh	739
1.1	Les shells Unix	739
1.2	zsh et oh-my-zsh	740
1.3	Tester zsh et oh-my-zsh	740
1.4	Configurer zsh comme shell pour l'utilisateur courant	741
2.	Déploiement du tableau de bord Kubernetes	742
2.1	Installation du tableau de bord (application dashboard)	742
2.2	Création du compte d'accès	742
2.3	Récupération du jeton de connexion	743
2.4	Décodage du contenu du jeton	744
2.5	Connexion au tableau de bord	746

Index	747
-------	-----

Avant-propos

Chapitre 1  
Présentation de Linux

- 1. Bienvenue dans le monde Unix ..... 31
  - 1.1 Un nouveau monde ..... 31
  - 1.2 Histoire des ordinateurs ..... 32
    - 1.2.1 Complexité des ordinateurs ..... 32
    - 1.2.2 L'intelligence ..... 32
  - 1.3 Le système d'exploitation ..... 33
  - 1.4 Le système Unix, une brève histoire ..... 36
    - 1.4.1 De MULTICS à UNIX ..... 36
    - 1.4.2 Le langage C ..... 39
    - 1.4.3 Les licences et l'avènement de BSD et System V ..... 39
    - 1.4.4 La guerre des Unix ..... 41
    - 1.4.5 La standardisation ..... 41
    - 1.4.6 Unix est un standard ..... 42
    - 1.4.7 Unix sur les ordinateurs personnels ..... 43
- 2. Le logiciel libre ..... 44
  - 2.1 Les origines du logiciel libre ..... 44
  - 2.2 Le projet GNU et la FSF ..... 45
  - 2.3 L'open source ..... 47
  - 2.4 GNU/Linux ..... 48
    - 2.4.1 Linus Torvalds ..... 48
    - 2.4.2 L'accident ..... 49
    - 2.4.3 La première version officielle ..... 49
    - 2.4.4 Le succès communautaire ..... 49
    - 2.4.5 Les années 1994-1997 ..... 50
    - 2.4.6 À partir de 1998 : l'explosion ..... 50
    - 2.4.7 Aujourd'hui et demain ..... 51
- 3. Quel matériel pour Linux ? ..... 52
  - 3.1 L'architecture ..... 52
  - 3.2 Un point sur les SSD ..... 56
  - 3.3 Compatibilité du matériel ..... 57

4.	Choisir une distribution	60
4.1	Debian	60
4.2	Ubuntu	61
4.3	Red Hat, Fedora et CentOS	62
4.4	openSUSE	64
4.5	Les autres	65
4.6	Les LiveCD ou LiveUSB	66
5.	Obtenir de l'aide	67
5.1	L'aide propre aux commandes	67
5.2	L'aide interne au shell	68
5.3	Le manuel en ligne de commande	68
5.3.1	Accès	68
5.3.2	Structure d'une page	69
5.3.3	Navigation	70
5.3.4	Les sections	70
5.3.5	Rechercher par correspondance	71
5.4	Les pages info	72
5.5	Rechercher de l'aide sur Internet	72

## Chapitre 2

### Installation de Linux et des logiciels

1.	Installer une Ubuntu	75
1.1	Support d'installation	75
1.2	Boot sur le support	76
1.3	Choix des langues et pays	78
1.4	Configuration des interfaces réseau	79
1.5	Miroir d'installation	80
1.6	Partitionnement des disques	81
1.7	Utilisateur et hôte	83
1.8	Configuration SSH	84
1.9	Installation	84
1.10	Fin d'installation et redémarrage	86
2.	Installation de CentOS	86
2.1	Support d'installation	86
2.2	Boot sur le support	87



- 2.3 Langue d'installation . . . . . 89
- 2.4 Résumé de l'installation . . . . . 90
- 2.5 Clavier . . . . . 90
- 2.6 Destination de l'installation . . . . . 91
- 2.7 Configuration du réseau . . . . . 95
- 2.8 Horloge . . . . . 96
- 2.9 Source d'installation . . . . . 97
- 2.10 Sélection de logiciels . . . . . 98
- 2.11 Utilisateurs . . . . . 99
- 2.12 Fin de l'installation . . . . . 100
- 3. Red Hat Package Manager . . . . . 101
  - 3.1 Notion de package . . . . . 101
  - 3.2 Le gestionnaire RPM . . . . . 102
  - 3.3 Installation, mise à jour et suppression . . . . . 103
  - 3.4 Cas du noyau . . . . . 104
  - 3.5 Requêtes RPM . . . . . 104
  - 3.6 Vérification des packages . . . . . 106
  - 3.7 Les dépendances . . . . . 107
  - 3.8 Extraction du contenu . . . . . 107
  - 3.9 Mises à jour automatisées . . . . . 108
- 4. YUM . . . . . 108
  - 4.1 Configuration des dépôts . . . . . 108
  - 4.2 Utilisation des dépôts . . . . . 110
    - 4.2.1 Rafraîchir le cache . . . . . 110
    - 4.2.2 Lister les packages . . . . . 110
    - 4.2.3 Installer des packages . . . . . 112
    - 4.2.4 Mises à jour . . . . . 112
    - 4.2.5 Rechercher un package . . . . . 113
    - 4.2.6 Supprimer un package . . . . . 113
    - 4.2.7 Télécharger un package . . . . . 113
  - 4.3 La commande dnf . . . . . 114
- 5. Debian Package . . . . . 114
  - 5.1 dpkg : le gestionnaire de paquets Debian . . . . . 114
  - 5.2 Installation, mise à jour et suppression . . . . . 115

5.3	Requêtes dpkg . . . . .	117
5.3.1	Lister les paquets . . . . .	117
5.3.2	Trouver un paquet contenant un fichier . . . . .	118
5.3.3	Lister le contenu d'un paquet . . . . .	118
5.4	Convertir des packages . . . . .	119
5.5	Reconfigurer un package . . . . .	120
6.	Gestionnaire APT . . . . .	121
6.1	Principe . . . . .	121
6.2	Les dépôts . . . . .	121
6.2.1	Configuration . . . . .	121
6.2.2	Mise à jour de la base . . . . .	123
6.3	Mise à jour de la distribution . . . . .	124
6.4	Rechercher et installer un package individuel . . . . .	125
6.5	Client graphique . . . . .	126
7.	Gestionnaire aptitude . . . . .	127
7.1	apt ou aptitude ? . . . . .	127
7.2	Installation . . . . .	127
7.3	Utilisation . . . . .	128
8.	Zypper . . . . .	129
8.1	Gestion des dépôts . . . . .	129
8.2	Gérer les packages . . . . .	131
9.	Snappy . . . . .	133
9.1	Images logicielles . . . . .	133
9.2	Utiliser Snap . . . . .	134
10.	Installer depuis les sources . . . . .	136
10.1	Obtenir les sources . . . . .	136
10.2	Prérequis et dépendances . . . . .	136
10.3	Exemple d'installation . . . . .	137
10.4	Désinstallation . . . . .	141
10.5	Les bases du Makefile . . . . .	141
10.5.1	Bases . . . . .	141
10.5.2	Makefile intermédiaire . . . . .	143
10.5.3	Un peu plus complexe . . . . .	144

11. Gérer les bibliothèques partagées . . . . .	146
11.1 Principe . . . . .	146
11.2 Lieu de stockage . . . . .	147
11.3 Quelles bibliothèques liées ? . . . . .	148
11.4 Configurer le cache de l'éditeur de liens . . . . .	149

## Chapitre 3

### Le shell et les commandes GNU

1. Le shell bash . . . . .	151
1.1 Rôle . . . . .	151
1.2 Bash : le shell par défaut . . . . .	152
1.2.1 Un shell puissant et libre . . . . .	152
1.2.2 L'invite de commandes . . . . .	153
1.3 Utiliser le shell . . . . .	154
1.3.1 La saisie . . . . .	154
1.3.2 Syntaxe générale des commandes . . . . .	155
1.3.3 Premier exemple concret avec cal . . . . .	155
1.3.4 Chaîner les commandes . . . . .	157
1.3.5 Afficher du texte avec echo . . . . .	157
1.3.6 Commandes internes et externes . . . . .	158
1.3.7 Quelques raccourcis utiles . . . . .	159
1.4 Rappel de l'historique . . . . .	159
2. La gestion des fichiers . . . . .	160
2.1 Le système de fichiers . . . . .	160
2.2 Les divers types de fichiers . . . . .	161
2.2.1 Les fichiers ordinaires ou réguliers . . . . .	161
2.2.2 Les catalogues . . . . .	162
2.2.3 Les fichiers spéciaux . . . . .	162
2.3 Nomenclature des fichiers . . . . .	163
2.4 Les chemins . . . . .	164
2.4.1 Structure et nom de chemin . . . . .	164
2.4.2 Répertoire personnel . . . . .	164
2.4.3 Chemin relatif . . . . .	165
2.4.4 Le tilde . . . . .	166
2.4.5 cd . . . . .	166

2.5	Les commandes de base	167
2.5.1	Lister les fichiers et les répertoires	167
2.5.2	Gérer les fichiers et les répertoires	169
2.5.3	Wildcards : caractères de substitution	174
2.5.4	Verrouillage de caractères	176
3.	Rechercher des fichiers	176
3.1	Considérations générales	176
3.2	Critères de recherche	177
3.2.1	-name	177
3.2.2	-type	177
3.2.3	-user et -group	178
3.2.4	-size	178
3.2.5	-atime, -mtime et -ctime	179
3.2.6	-perm.	180
3.2.7	-links et -inum	180
3.2.8	-regex et -iregex	181
3.2.9	-depth, -maxdepth, -mindepth	181
3.3	Commandes	182
3.3.1	-ls	182
3.3.2	-exec	182
3.3.3	-ok	183
3.4	Critères AND / OR / NOT	183
3.5	Retrouver des exécutables	184
3.5.1	whereis	184
3.5.2	which	184
3.5.3	locate	185
4.	L'éditeur vi	186
4.1	Présentation	186
4.2	Fonctionnement	186
4.3	Les commandes	187
4.3.1	La saisie	187
4.3.2	Quitter et sauvegarder	188
4.3.3	Déplacement	188
4.3.4	La correction	189
4.3.5	Recherche dans le texte	189
4.3.6	Commandes de remplacement	190
4.3.7	Copier-coller	191

4.3.8	Substitution.....	191
4.3.9	Autres.....	192
5.	Redirections.....	193
5.1	Principe.....	193
5.2	En sortie.....	193
5.3	En entrée.....	194
5.4	Documents en ligne.....	194
5.5	Les canaux standards.....	195
5.6	Ouverture de canaux.....	196
5.7	Filtre : définition.....	196
5.8	Pipelines / tubes.....	197
6.	Les filtres et utilitaires.....	197
6.1	Extraction des noms et chemins.....	197
6.2	Recherche de lignes.....	198
6.2.1	grep.....	198
6.2.2	egrep.....	199
6.2.3	fgrep.....	200
6.2.4	sed.....	200
6.2.5	Expressions régulières.....	201
6.3	Colonnes et champs.....	201
6.3.1	Colonnes.....	201
6.3.2	Champs.....	202
6.4	Décompte de lignes.....	204
6.5	Tri de lignes.....	205
6.6	Suppression des doublons.....	206
6.7	Jointure de deux fichiers.....	207
6.7.1	Sur des champs communs.....	207
6.7.2	Ligne à ligne.....	207
6.8	Découpage d'un fichier en morceaux.....	208
6.8.1	Découper.....	208
6.8.2	Reconstruire.....	209
6.9	Remplacement de caractères.....	209
6.9.1	Liste de caractères.....	209
6.9.2	Tabulations et espaces.....	211
6.10	xargs.....	212

6.11	Visualisation de texte	213
6.11.1	En pleine page	213
6.11.2	Début d'un fichier	214
6.11.3	Fin et attente de fichier	215
6.11.4	Formater une sortie	215
6.12	Duplication du canal de sortie standard	215
6.13	Comparaison de fichiers	216
6.13.1	diff	216
6.13.2	cmp	218
6.14	Délai d'attente	218
6.15	Contrôler le flux	218
6.16	Les sommes de contrôle	219
7.	Les processus	220
7.1	Définition et environnement	220
7.2	États d'un processus	221
7.3	Lancement en tâche de fond	222
7.4	Background, foreground, jobs	223
7.5	Liste des processus	223
7.6	Arrêt d'un processus / signaux	225
7.7	nohup	227
7.8	nice et renice	227
7.9	time	228
7.10	exec	228
8.	Plus loin avec le bash	229
8.1	Alias	229
8.2	Groupement de commandes	230
8.3	Liaison et exécution conditionnelle	231
9.	Les variables	232
9.1	Nomenclature	232
9.2	Déclaration et affectation	232
9.3	Accès et affichage	232
9.4	Suppression et protection	234
9.5	Export	234
9.6	Accolades	235
9.7	Accolades et remplacement conditionnel	235
9.8	Variables système	236

9.9	Variables spéciales	237
9.10	Longueur d'une chaîne	237
9.11	Tableaux et champs	238
9.12	Variables typées	238
10.	Configuration de bash	239
10.1	Fichiers de configuration	239
10.1.1	Shell de connexion	240
10.1.2	Shell simple	240
10.1.3	Mode Bourne shell	240
10.1.4	Mode non interactif	240
10.2	Commandes set	241
11.	Programmation shell	241
11.1	Structure et exécution d'un script	241
11.2	Arguments d'un script	243
11.2.1	Paramètres de position	243
11.2.2	Redéfinition des paramètres	244
11.2.3	Réorganisation des paramètres	244
11.2.4	Sortie de script	245
11.3	Environnement du processus	245
11.4	Substitution de commande	246
11.5	Tests de conditions	247
11.5.1	Tests sur une chaîne	247
11.5.2	Tests sur les valeurs numériques	247
11.5.3	Tests sur les fichiers	248
11.5.4	Tests combinés par des critères ET, OU, NON	249
11.5.5	Syntaxe allégée	250
11.6	if ... then ... else	250
11.7	Choix multiples case	251
11.8	Saisie de l'utilisateur	253
11.9	Les boucles	254
11.9.1	Boucle for	254
11.9.2	Boucle while	257
11.9.3	Boucle until	258
11.9.4	true et false	259
11.9.5	break et continue	259
11.9.6	Boucle select	259
11.10	Les fonctions	260

11.11	Calculs et expressions . . . . .	261
11.11.1	expr . . . . .	261
11.11.2	Calculs avec bash . . . . .	263
11.11.3	Calculs de nombres réels . . . . .	263
11.12	Une variable dans une autre variable . . . . .	264
11.13	Traitement des signaux . . . . .	265
11.14	Commande « : » . . . . .	266
12.	Multiplexeurs de terminal . . . . .	267
12.1	Présentation . . . . .	267
12.2	Utilisation . . . . .	267
12.2.1	Installation et aide . . . . .	267
12.2.2	Fenêtres . . . . .	267
12.2.3	Détacher et rattacher . . . . .	268
12.2.4	Tout fermer . . . . .	269
12.3	Alternatives . . . . .	269

## Chapitre 4

### Les disques et le système de fichiers

1.	Représentation des disques . . . . .	271
1.1	Nomenclature . . . . .	271
1.1.1	IDE . . . . .	271
1.1.2	SCSI, SATA, USB, FIREWIRE, etc. . . . .	272
1.2	Cas spéciaux . . . . .	273
1.2.1	Contrôleurs spécifiques . . . . .	273
1.2.2	Virtualisation . . . . .	273
1.2.3	SAN, iSCSI, multipathing . . . . .	273
2.	Manipulations de bas niveau . . . . .	274
2.1	Informations . . . . .	274
2.2	Modification des valeurs . . . . .	275
3.	Choisir un système de fichiers . . . . .	277
3.1	Principe . . . . .	277
3.1.1	Définition . . . . .	277
3.1.2	Représentation . . . . .	277
3.1.3	Les métadonnées . . . . .	278
3.1.4	Les noms des fichiers . . . . .	278



3.1.5	Le journal	279
3.2	Les systèmes de fichiers sous Linux	279
3.2.1	ext2	279
3.2.2	ext3	280
3.2.3	ext4	280
3.2.4	BTRFS	280
3.2.5	XFS	281
3.2.6	VFAT (FAT32)	282
3.2.7	exFAT	282
3.2.8	FUSE	283
4.	Partitionnement	284
4.1	Découpage logique	284
4.2	Partitionnement MBR	284
4.2.1	MBR et BIOS	284
4.2.2	MBR	285
4.2.3	Les partitions	285
4.2.4	EBR	287
4.2.5	PBR	287
4.2.6	Types de partitions	287
4.3	Partitionnement GPT	288
4.3.1	GPT et UEFI	288
4.3.2	GUID	289
4.3.3	LBA 0	290
4.3.4	LBA 1	290
4.3.5	LBA 2 à 33	291
4.3.6	Types de partitions	291
4.3.7	UEFI Boot manager	292
4.3.8	La partition système EFI	293
4.4	Manipuler les partitions	293
4.4.1	Outils disponibles	293
4.4.2	Manipuler les partitions MBR	294
4.4.3	Manipuler les partitions GPT	299
5.	Manipuler les systèmes de fichiers	300
5.1	Définitions de base	300
5.1.1	Bloc	300
5.1.2	Superbloc	301
5.1.3	Table d'inodes	301

5.1.4	Tables catalogues	303
5.1.5	Hard link	304
5.2	Créer un système de fichiers	305
5.2.1	mkfs, syntaxe générale	305
5.2.2	Un premier exemple en ext2	306
5.2.3	ext2, ext3 et ext4	307
5.2.4	XFS	310
5.2.5	BTRFS	310
5.2.6	VFAT	312
6.	Accéder aux systèmes de fichiers	313
6.1	mount	313
6.1.1	Montage par périphérique	313
6.1.2	Options de montage	316
6.1.3	umount	318
6.1.4	/etc/fstab	319
6.1.5	Cas des CD et images ISO	321
7.	Contrôler le système de fichiers	322
7.1	Statistiques d'occupation	322
7.1.1	Par système de fichiers	322
7.1.2	Par arborescence	323
7.2	Vérifier, régler et réparer	324
7.2.1	fsck	324
7.2.2	badblocks	325
7.2.3	dumpe2fs	325
7.2.4	tune2fs	327
7.2.5	debugfs	329
7.3	XFS	330
7.3.1	xfs_info	330
7.3.2	xfs_growfs	330
7.3.3	xfs_repair	330
7.3.4	xfs_db et xfs_admin	332
7.3.5	xfs_fsr	332

- 8. Le swap. . . . . 333
  - 8.1 Pourquoi créer un swap ? . . . . . 333
  - 8.2 Taille optimale . . . . . 333
  - 8.3 Créer une partition de swap . . . . . 334
  - 8.4 Activer et désactiver le swap. . . . . 334
    - 8.4.1 Activation dynamique. . . . . 334
    - 8.4.2 Dans /etc/fstab . . . . . 335
  - 8.5 En cas d'urgence : fichier de swap. . . . . 335
  - 8.6 État de la mémoire. . . . . 336
    - 8.6.1 free . . . . . 336
    - 8.6.2 Mémoire réservée. . . . . 337
    - 8.6.3 meminfo. . . . . 338
    - 8.6.4 swap utilisé et mémoire libre . . . . . 338
- 9. Les quotas disques . . . . . 339
  - 9.1 Définitions . . . . . 339
  - 9.2 Mise en place sur ext4 . . . . . 340
  - 9.3 Mise en place sur XFS . . . . . 342
- 10. Les droits d'accès . . . . . 343
  - 10.1 Les droits de base . . . . . 343
    - 10.1.1 Droits et utilisateurs . . . . . 343
    - 10.1.2 Signification. . . . . 344
  - 10.2 Modification des droits . . . . . 345
    - 10.2.1 Par symboles . . . . . 345
    - 10.2.2 Par base 8 . . . . . 346
  - 10.3 Masque des droits . . . . . 347
    - 10.3.1 Restreindre des droits automatiquement . . . . . 347
    - 10.3.2 Calcul de masque. . . . . 348
  - 10.4 Changer de propriétaire et de groupe. . . . . 348
  - 10.5 Droits d'accès étendus . . . . . 349
    - 10.5.1 SUID et SGID . . . . . 349
    - 10.5.2 Real / effectif . . . . . 350
    - 10.5.3 Sticky bit . . . . . 350
    - 10.5.4 Droits et répertoires . . . . . 351

## Chapitre 5

### Boot, services, noyau et périphériques

1.	Processus de démarrage . . . . .	353
1.1	Le BIOS et l'UEFI . . . . .	353
1.1.1	BIOS . . . . .	353
1.1.2	UEFI . . . . .	354
1.1.3	Réglages basiques . . . . .	355
1.2	Le chargeur de démarrage . . . . .	357
1.3	GRUB . . . . .	358
1.3.1	Configuration . . . . .	358
1.3.2	Installation . . . . .	359
1.3.3	Démarrage et édition . . . . .	360
1.4	GRUB2 . . . . .	360
1.4.1	GRUB2 remplace GRUB . . . . .	360
1.4.2	Configuration . . . . .	361
1.4.3	Démarrage et édition . . . . .	364
1.4.4	Cas de GPT et UEFI . . . . .	364
1.5	Initialisation du noyau . . . . .	366
2.	init System V . . . . .	367
2.1	init System V en 2020 . . . . .	367
2.2	Rôle . . . . .	367
2.3	Niveaux d'exécution . . . . .	368
2.4	/etc/inittab . . . . .	369
2.5	Changement de niveau . . . . .	371
2.6	Paramétrage système de base . . . . .	372
2.7	Niveaux d'exécution . . . . .	373
2.8	Gestion des niveaux et des services . . . . .	373
2.8.1	Services dans init.d . . . . .	373
2.8.2	Contrôle manuel des services . . . . .	375
2.8.3	Modification des niveaux d'exécution . . . . .	376
2.9	Consoles virtuelles . . . . .	378
2.10	Les logins . . . . .	379
2.11	Arrêt . . . . .	380
3.	systemd . . . . .	382
3.1	Principe . . . . .	382
3.2	Unités cibles et services . . . . .	383

3.3	Configuration	383
3.4	Cibles	384
3.4.1	Équivalence avec init System V	384
3.4.2	Connaître la cible par défaut	384
3.4.3	Changer de cible par défaut	384
3.4.4	Passer d'une cible à l'autre	385
3.4.5	Mode secours et urgence	385
3.4.6	Cibles actives et dépendances	385
3.4.7	Lister toutes les cibles	386
3.5	Services	387
3.5.1	Actions	387
3.5.2	Statut	388
3.5.3	Activation	389
3.5.4	Masquage	390
3.5.5	Dépendances	390
3.6	Compatibilité avec System V	391
3.7	Actions système	392
3.8	Gestion de la console	392
3.9	Interface graphique	393
4.	upstart	394
4.1	Principe	394
4.2	Fichiers	394
4.3	Niveau par défaut	395
4.4	Compatibilité System V	395
4.5	Commandes de contrôle	396
4.6	Activation et désactivation d'un service	397
5.	Consulter les traces du système	397
5.1	dmesg	397
5.2	/var/log/messages ou /var/log/syslog	399
5.3	journalctl	400
6.	Services et modules noyau	400
6.1	Présentation	400
6.2	uname	402
6.3	Gestion des modules	403
6.3.1	lsmod	404
6.3.2	depmod	405

6.3.3	modinfo	406
6.3.4	insmod	407
6.3.5	rmmod	408
6.3.6	modprobe	408
6.3.7	modprobe.d	409
6.4	Chargement des modules au boot	411
6.4.1	initrd et initramfs	411
6.4.2	Modules persistants	416
6.5	Paramètres dynamiques	417
6.5.1	/proc et /sys	417
6.5.2	sysctl	421
7.	Compiler un noyau	422
7.1	Obtenir les sources	422
7.1.1	Sources officielles	422
7.1.2	Sources de la distribution	423
7.2	Les outils nécessaires	423
7.3	Configuration	424
7.3.1	Le .config	424
7.3.2	Récupérer la configuration du noyau	425
7.3.3	make oldconfig	426
7.3.4	make menuconfig	427
7.3.5	make xconfig	428
7.3.6	Pistes d'optimisations	429
7.4	Compilation	431
7.5	Installation	432
7.6	Test	434
7.7	Autres options	434
8.	Les fichiers périphériques	435
8.1	Introduction	435
8.2	Fichiers spéciaux	436
8.3	Créer un fichier spécial	437
8.4	Connaître son matériel	438
8.4.1	Bus PCI	438
8.4.2	Bus USB	439
8.4.3	Ressources matérielles	440
8.4.4	Autres outils	443

- 8.5 Le support de l'USB et du hotplug ..... 446
  - 8.5.1 Les modules ..... 446
  - 8.5.2 Chargement ..... 447
  - 8.5.3 hotplug, usbmgr ..... 447
  - 8.5.4 udev ..... 448

**Chapitre 6**  
**Les tâches administratives**

- 1. Administration des utilisateurs ..... 451
  - 1.1 Principe ..... 451
    - 1.1.1 Identification et authentification ..... 451
    - 1.1.2 Les utilisateurs ..... 451
    - 1.1.3 Les groupes ..... 453
    - 1.1.4 Les mots de passe ..... 453
  - 1.2 Les fichiers ..... 454
    - 1.2.1 /etc/passwd ..... 454
    - 1.2.2 /etc/group ..... 454
    - 1.2.3 /etc/shadow ..... 455
    - 1.2.4 /etc/gshadow ..... 456
  - 1.3 Gestion des utilisateurs ..... 456
    - 1.3.1 Ajout ..... 456
    - 1.3.2 Sécurité des mots de passe ..... 459
    - 1.3.3 Modification ..... 462
    - 1.3.4 Suppression ..... 462
  - 1.4 Gestion des groupes ..... 463
    - 1.4.1 Ajout ..... 463
    - 1.4.2 Modification ..... 463
    - 1.4.3 Suppression ..... 463
    - 1.4.4 Mot de passe ..... 464
  - 1.5 Commandes additionnelles ..... 464
    - 1.5.1 Conversion des fichiers ..... 464
    - 1.5.2 Vérifier la cohérence ..... 465
    - 1.5.3 Vérifier les connexions ..... 466
    - 1.5.4 Actions de l'utilisateur ..... 466
    - 1.5.5 Interroger le système ..... 469
  - 1.6 Configuration avancée ..... 470

1.7	Notifications à l'utilisateur	473
1.7.1	/etc/issue	473
1.7.2	/etc/issue.net	473
1.7.3	/etc/motd	473
1.7.4	wall, write et mesg	474
1.8	L'environnement utilisateur	475
1.8.1	/etc/skel	475
1.8.2	Scripts de configuration	475
1.8.3	Groupes privés et setgid	476
1.9	Aperçu de PAM	477
2.	L'impression	480
2.1	Principe	480
2.2	System V	480
2.3	BSD	481
2.4	CUPS	482
2.4.1	Présentation	482
2.4.2	Ajout d'une imprimante	484
3.	Automatisation	489
3.1	Avec cron	489
3.1.1	Présentation	489
3.1.2	Formalisme	490
3.1.3	Exemples	490
3.1.4	crontab système	491
3.1.5	Contrôle d'accès	491
3.2	Avec at	492
3.2.1	Présentation	492
3.2.2	Formalisme	492
3.2.3	Contrôle des tâches	493
3.2.4	Contrôle d'accès	494
3.3	Avec anacron	494
3.4	Avec systemd	495
4.	Les traces (logs) du système	497
4.1	Principe	497
4.2	Les messages	498
4.3	Configuration de syslog	499
4.4	Cas de rsyslog	501



- 4.5 systemd et journald . . . . . 501
- 4.6 Les fichiers de traces . . . . . 503
- 4.7 journalctl . . . . . 504
- 4.8 Émettre des messages . . . . . 505
- 4.9 Rotation des logs . . . . . 506
  - 4.9.1 logrotate . . . . . 506
  - 4.9.2 journald . . . . . 507
- 5. Archivage et backup . . . . . 509
  - 5.1 Les outils de sauvegarde . . . . . 509
    - 5.1.1 Commandes, plans, scripts . . . . . 509
    - 5.1.2 Autres commandes . . . . . 510
  - 5.2 tar . . . . . 510
    - 5.2.1 Archiver . . . . . 510
    - 5.2.2 Lister . . . . . 511
    - 5.2.3 Restauration . . . . . 511
    - 5.2.4 Autres paramètres . . . . . 512
  - 5.3 cpio . . . . . 513
    - 5.3.1 Archiver . . . . . 513
    - 5.3.2 Lister . . . . . 514
    - 5.3.3 Restaurer . . . . . 515
  - 5.4 dd . . . . . 515
- 6. L'horloge . . . . . 517
  - 6.1 Connaître l'heure . . . . . 517
    - 6.1.1 date . . . . . 517
    - 6.1.2 hwclock . . . . . 518
  - 6.2 Modifier l'horloge matérielle . . . . . 519
    - 6.2.1 Via date . . . . . 519
    - 6.2.2 Via hwclock . . . . . 519
  - 6.3 NTP . . . . . 519
    - 6.3.1 Principe . . . . . 519
    - 6.3.2 Client NTP . . . . . 520
    - 6.3.3 Dérive temporelle . . . . . 521
  - 6.4 timedatectl . . . . . 522
  - 6.5 chrony . . . . . 523

7. Les paramètres régionaux .....	525
7.1 i18n et l10n .....	525
7.2 Réglages locaux .....	526
7.2.1 Outils de la distribution .....	526
7.2.2 Variables d'environnement .....	526
7.2.3 Fuseaux horaires .....	528
7.3 Codage des caractères .....	529

## Chapitre 7

### Le réseau

1. TCP/IP .....	531
1.1 Bases .....	531
1.2 Adressage .....	532
1.2.1 Classes .....	532
1.2.2 Sous-réseaux .....	533
1.2.3 Routage .....	534
1.2.4 IPv6 .....	535
1.3 Cas particuliers .....	536
1.3.1 NetworkManager .....	536
1.3.2 Nommage des interfaces .....	537
1.4 Configuration .....	537
1.4.1 Cas général et historique .....	537
1.4.2 Cas des distributions de type Red Hat .....	538
1.4.3 Machines de type Debian et Ubuntu .....	540
1.4.4 Routage .....	541
1.4.5 iproute2 .....	542
1.4.6 Network Manager .....	543
1.4.7 netplan .....	545
1.4.8 Les ports .....	547
1.5 Outils réseau .....	548
1.5.1 Ping .....	548
1.5.2 Traceroute .....	549
1.5.3 tracepath .....	550
1.5.4 Whois .....	550
1.5.5 Netstat .....	551
1.5.6 IPTraf .....	553

1.6	Fichiers généraux . . . . .	554
1.6.1	/etc/resolv.conf . . . . .	554
1.6.2	/etc/hosts et /etc/networks . . . . .	555
1.6.3	/etc/nsswitch.conf . . . . .	555
1.6.4	/etc/services . . . . .	556
1.6.5	/etc/protocols . . . . .	557
2.	Services réseau xinetd . . . . .	558
2.1	Présentation . . . . .	558
2.2	Configuration . . . . .	558
2.3	Démarrage et arrêt des services . . . . .	560
2.4	Conversion vers systemd . . . . .	561
3.	OpenSSH . . . . .	562
3.1	Présentation . . . . .	562
3.2	Configuration . . . . .	563
3.3	Utilisation . . . . .	563
3.4	Clés et connexion automatique . . . . .	563
3.4.1	Type de chiffrement . . . . .	564
3.4.2	Côté client . . . . .	564
3.4.3	Côté serveur . . . . .	565
3.4.4	Copie automatique . . . . .	565
3.5	Passphrase et agent SSH . . . . .	566
3.6	Authentification de l'hôte . . . . .	567
4.	Monter un serveur DHCP . . . . .	568
4.1	Présentation . . . . .	568
4.2	Démarrage du serveur dhcpd . . . . .	568
4.3	Informations de base . . . . .	569
4.4	Côté client . . . . .	570
5.	Serveur DNS . . . . .	570
5.1	Présentation . . . . .	570
5.2	Lancement . . . . .	572
5.3	Configuration de Bind . . . . .	572
5.3.1	Configuration générale . . . . .	572
5.3.2	Section globale . . . . .	573
5.3.3	Section de zones . . . . .	573
5.3.4	Zone de résolution . . . . .	574
5.3.5	Zone de résolution inverse . . . . .	574

5.3.6	Exemple	575
5.3.7	Zones spéciales	576
5.4	Fichiers de zones	576
5.4.1	Définitions	576
5.4.2	Zone	577
5.4.3	Zone de résolution inverse	580
5.5	Diagnostic des problèmes de configuration	580
5.6	Interrogation dig, host et getent	580
6.	Courrier électronique	584
6.1	Principe	584
6.2	postfix	585
6.2.1	Configuration simple	585
6.2.2	Alias d'utilisateurs	586
6.2.3	Test	586
6.3	Autres MTAs	587
6.3.1	exim	587
6.3.2	qmail	587
7.	Service HTTP Apache	587
7.1	Présentation	587
7.2	Arrêt/Relance	588
7.3	Configuration	588
7.4	Directives générales	589
7.5	Les répertoires, alias et emplacements	589
7.5.1	Directory	589
7.5.2	Alias	590
7.6	Hôtes virtuels	591
8.	Partage de fichiers	592
8.1	NFS	592
8.1.1	Lancement	592
8.1.2	Cas de NFS4	593
8.1.3	Partage côté serveur	593
8.1.4	Montage côté client	595

- 9. Partages Windows avec Samba . . . . . 596
  - 9.1 Présentation . . . . . 596
  - 9.2 Configuration . . . . . 597
  - 9.3 Partage de fichiers . . . . . 598
  - 9.4 Méthodes d'authentification. . . . . 599
  - 9.5 Correspondance des noms et des mots de passe . . . . . 599
  - 9.6 Clients SAMBA . . . . . 599

**Chapitre 8**  
**La sécurité**

- 1. Bases de sécurité . . . . . 601
  - 1.1 Sécurité informatique . . . . . 601
  - 1.2 Contrôler les droits d'endossement . . . . . 604
  - 1.3 Vérifier les packages. . . . . 605
  - 1.4 Politique de mot de passe . . . . . 606
  - 1.5 Stocker ses mots de passe . . . . . 607
  - 1.6 Interdire les connexions . . . . . 608
    - 1.6.1 /bin/false . . . . . 608
    - 1.6.2 /etc/nologin . . . . . 609
    - 1.6.3 /etc/securetty. . . . . 609
  - 1.7 Tester les mots de passe . . . . . 610
  - 1.8 Rechercher des rootkits . . . . . 612
    - 1.8.1 Principe du rootkit. . . . . 612
    - 1.8.2 Chkrootkit et rkhunter . . . . . 613
  - 1.9 Les virus . . . . . 615
  - 1.10 Les limites de l'utilisateur . . . . . 617
  - 1.11 Les droits SUDO . . . . . 618
    - 1.11.1 Donner des privilèges étendus . . . . . 618
    - 1.11.2 Syntaxe de /etc/sudoers . . . . . 619
  - 1.12 Audit plus complet . . . . . 621
  - 1.13 Les bulletins de sécurité. . . . . 622
    - 1.13.1 CERT : Computer Emergency Response Team. . . . . 622
    - 1.13.2 SecurityFocus. . . . . 624
    - 1.13.3 Les bulletins des distributions . . . . . 625
    - 1.13.4 Les correctifs . . . . . 625

2.	Sécurité des services et du réseau	626
2.1	Vérifier les ports ouverts	626
2.1.1	Les sockets	626
2.1.2	Informations depuis netstat	627
2.1.3	L'outil nmap	627
2.2	Supprimer les services inutiles	629
2.2.1	Généralités	629
2.2.2	Services standalone	630
2.2.3	Services xinetd	630
2.3	Les tcp_wrappers	631
2.4	Netfilter	633
2.4.1	Présentation	633
2.4.2	Vie d'un paquet	634
2.4.3	Principe des règles	635
2.4.4	Cibles de règles	635
2.4.5	Premier exemple	635
2.4.6	Opérations de base	636
2.4.7	Critères de correspondance	637
2.4.8	Tables	638
2.4.9	Sauvegarder ses réglages	639
2.5	UFW	639
2.5.1	Activation et statut	640
2.5.2	Règles par défaut	641
2.5.3	Gestion des règles	641
2.5.4	Limitations	643
2.6	firewalld	643
2.6.1	Activation	644
2.6.2	Zones	644
2.6.3	Services	646
2.6.4	Règles personnalisées	647
2.6.5	Règles riches	647
2.7	GPG	647
2.7.1	Un clone de PGP	647
2.7.2	Générer les clés	648
2.7.3	Générer une clé de révocation	651
2.7.4	Gérer le trousseau	652
2.7.5	Exporter la clé publique	653

- 2.7.6 Importer une clé ..... 654
- 2.7.7 Signer une clé..... 655
- 2.7.8 Signer et chiffrer ..... 657

**Chapitre 9**  
**X Window**

- 1. Comment fonctionne un environnement graphique ? ..... 661
  - 1.1 X Window System..... 661
    - 1.1.1 Un modèle client/serveur ..... 661
    - 1.1.2 Le gestionnaire de fenêtres ..... 663
    - 1.1.3 Les widgets et les toolkits ..... 664
    - 1.1.4 Les bureaux virtuels..... 666
  - 1.2 Les environnements de bureau ..... 666
- 2. Xorg ..... 669
  - 2.1 Conditions générales et Wayland ..... 669
  - 2.2 Présentation ..... 670
  - 2.3 Installation..... 671
  - 2.4 Configuration ..... 672
    - 2.4.1 Via la distribution ..... 672
    - 2.4.2 Xorgcfg ..... 672
    - 2.4.3 Xorgconfig ..... 673
    - 2.4.4 X..... 674
  - 2.5 Structure de xorg.conf..... 674
    - 2.5.1 Découpage ..... 674
    - 2.5.2 Valeurs booléennes ..... 674
    - 2.5.3 Section InputDevice ou InputClass ..... 674
    - 2.5.4 Section Monitor..... 676
    - 2.5.5 Section Modes ..... 677
    - 2.5.6 Section Device ..... 678
    - 2.5.7 Section Screen ..... 678
    - 2.5.8 Section ServerLayout..... 679
    - 2.5.9 Section Files ..... 680
    - 2.5.10 Section Modules ..... 681
    - 2.5.11 Section ServerFlags ..... 682
    - 2.5.12 Section Extensions ..... 682

2.5.13	xorg.conf.d .....	682
2.6	Tester et lancer X .....	683
2.6.1	Vérifier la configuration .....	683
2.6.2	Les traces .....	684
2.6.3	Tester le serveur .....	685
3.	Le Display Manager .....	686
3.1	Principe .....	686
3.2	XDM .....	687
3.2.1	Configuration générale .....	687
3.2.2	Setup : Xsetup .....	688
3.2.3	Chooser : RunChooser .....	690
3.2.4	Startup : Xstartup .....	690
3.2.5	Session : Xsession .....	690
3.2.6	Reset : Xreset .....	692
3.2.7	Resources : Xresources .....	692
3.2.8	Servers : Xservers .....	692
3.2.9	AccessFile : Xaccess et XDMCP .....	693
3.3	gdm et kdm .....	693
3.4	LightDM .....	695
3.4.1	Utilisation .....	695
3.4.2	Connexion .....	696
3.4.3	Personnaliser LightDM .....	697
3.5	Display Manager au boot .....	698
3.5.1	System V et inittab .....	698
3.5.2	System V et services .....	699
3.5.3	Cible systemd .....	699
3.5.4	service upstart .....	700
3.5.5	/etc/sysconfig .....	700
3.5.6	Anciennes versions Ubuntu et Debian .....	701
4.	Window Manager et environnement personnel .....	702
4.1	Via le Display Manager .....	702
4.2	startx .....	703
4.3	Les terminaux .....	703
4.4	Les gestionnaires de fenêtres .....	705
4.4.1	twm .....	705
4.4.2	IceWM .....	705
4.4.3	Fvwm .....	706



- 4.4.4 CDE ..... 706
- 4.4.5 WindowMaker ..... 707
- 4.4.6 Enlightenment ..... 707
- 4.4.7 Xfce ..... 708
- 4.4.8 KDE et GNOME ..... 708
- 4.4.9 Les autres ..... 708
- 4.5 Exporter ses fenêtres ..... 709
- 5. Bureau distant ..... 710
  - 5.1 RDP ..... 710
  - 5.2 VNC ..... 711
  - 5.3 Spice ..... 713
- 6. Accessibilité ..... 713
  - 6.1 Assistance au clavier et à la souris ..... 713
  - 6.2 Assistance visuelle et auditive ..... 716

**Chapitre 10**

**Partitionnement avancé : RAID, LVM et BTRFS**

- 1. Partitionnement avancé RAID logiciel ..... 717
  - 1.1 Définitions ..... 717
  - 1.2 Précautions et considérations d'usage ..... 718
    - 1.2.1 Disque de secours ..... 718
    - 1.2.2 Disque défectueux ..... 718
    - 1.2.3 Boot ..... 719
    - 1.2.4 Swap ..... 719
    - 1.2.5 Périphériques ..... 719
    - 1.2.6 IDE et SATA ..... 719
    - 1.2.7 Hot Swap ..... 720
  - 1.3 RAID avec mdadm ..... 720
    - 1.3.1 Préparation ..... 720
    - 1.3.2 Création ..... 721
    - 1.3.3 Sauvegarder la configuration ..... 723
  - 1.4 État du RAID ..... 723
  - 1.5 Simuler une panne ..... 724
  - 1.6 Remplacer un disque ..... 725
  - 1.7 Arrêt et relance manuels ..... 726

1.8	Destruction du RAID	726
2.	Initiation au LVM	727
2.1	Principe	727
2.2	Les volumes physiques	728
2.2.1	Créer un volume physique	728
2.2.2	Voir les volumes physiques	729
2.3	Les groupes de volumes	729
2.3.1	Créer un groupe de volumes	729
2.3.2	Propriétés d'un groupe de volumes	730
2.4	Les volumes logiques	731
2.4.1	Créer un volume logique	731
2.4.2	Propriétés d'un volume logique	732
2.4.3	Accès au volume logique	733
2.5	Agrandissements et réductions	733
2.5.1	Les groupes de volumes	733
2.5.2	Agrandir un volume logique	735
2.5.3	Réduire un volume logique	738
2.5.4	Déplacer le contenu d'un volume physique	740
2.5.5	Réduire un groupe de volumes	742
2.6	Supprimer un groupe de volumes	742
2.6.1	Étapes	742
2.6.2	Supprimer un volume logique	742
2.6.3	Retirer tous les volumes physiques	743
2.6.4	Détruire un groupe de volumes	743
2.6.5	Supprimer un volume physique	743
2.7	Commandes supplémentaires	743
3.	Utilisation étendue de BTRFS	744
3.1	Les subvolumes	744
3.1.1	Un système de fichiers dans un autre système de fichiers	744
3.1.2	Création	745
3.1.3	Montage	745
3.1.4	Destruction	746
3.2	Les snapshots	746
3.2.1	Principe	746
3.2.2	Création	747
3.2.3	Montage	747
3.2.4	Destruction	747

3.2.5 Opérations sur les ID ..... 748  
 3.3 Utiliser plusieurs disques. .... 749

**Chapitre 11**  
**Machines virtuelles, containers et cloud**

1. La virtualisation ..... 751  
 1.1 Définition ..... 751  
 1.2 Le cloud ..... 752  
 1.3 Intérêt ..... 752  
 1.4 Apprentissage ..... 754  
 1.5 Choix de la solution. .... 754  
 2. Méthodes de virtualisation ..... 754  
 2.1 L'isolation ..... 754  
 2.2 Noyau en espace utilisateur ..... 756  
 2.3 Hyperviseur de type 2 ..... 756  
 2.4 Hyperviseur de type 1 ..... 757  
 2.5 Virtualisation matérielle ..... 758  
 3. Paravirtualisation. .... 758  
 3.1 Principe ..... 758  
 3.2 Virtio ..... 759  
 3.3 Assistance matérielle ..... 759  
     3.3.1 Anneaux de protection ..... 759  
     3.3.2 Anneaux et virtualisation ..... 760  
 3.4 AMD-V et Intel-VT ..... 760  
 3.5 Virtualisation de la mémoire ..... 761  
 3.6 Virtualisation des périphériques ..... 762  
 3.7 Sécurité ..... 763  
 3.8 Considérations pratiques ..... 764  
 4. Les containers ..... 765  
 4.1 Principe ..... 765  
 4.2 Container et Machine virtuelle ..... 766  
 4.3 Les espaces de nommage ..... 767  
 4.4 Les groupes de contrôle ..... 768  
 4.5 Montage en union ..... 768  
 4.6 Image applicative ..... 769

4.7	Les couches d'images	769
4.8	Le projet OCI	770
4.9	Docker	771
4.10	Un exemple complet	772
4.10.1	Créer une image	772
4.10.2	Démarrer un container	774
4.10.3	Arrêt du container	774
4.10.4	Exposition du container	774
4.10.5	Dynamisme	775
4.10.6	Accéder au container	775
4.10.7	Traces	776
4.10.8	Supprimer le container et l'image	776
4.11	Sécurité	777
5.	Le cloud	777
5.1	Principe	777
5.2	Services Cloud	778
5.3	Fournisseurs	779
5.4	Exemple d'AWS	779
5.5	Zones géographiques	781
5.6	Tester	782
5.7	cloud-init	786
6.	Systèmes invités	787
6.1	Hyperviseur et additions	787
6.2	L'accès à la console ou l'affichage	791
6.2.1	Spice et KVM	791
6.2.2	Client Spice	792
6.2.3	Autres cas	793
	Index	795