

Version numérique

OFFERTE !

www.editions-eni.fr

Debian GNU/Linux

Maîtrisez la sécurité
des infrastructures



informatique technique

Fichiers complémentaires
à télécharger



ε
Collection

epsilon

Philippe PIERRE

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

Avant-propos

- 1. Objectifs 9
- 2. Public visé 10
- 3. Prérequis et connaissances nécessaires 11
- 4. Structure de l'ouvrage 11
- 5. Normes et règles de nommage 13

Chapitre 1 Outils de sauvegarde

- 1. Gestion de sauvegarde simple 15
 - 1.1 Généralités sur les sauvegardes 15
 - 1.1.1 Les supports 16
 - 1.1.2 Plan de reprise informatique 18
 - 1.1.3 Politique de sauvegarde 20
 - 1.2 Suite OpenSSH 21
 - 1.3 Tunnels SSH 25
 - 1.3.1 Tunnels SOCKS 25
 - 1.3.2 Tunnels par port 26
 - 1.3.3 Tunnels X 27
 - 1.3.4 Tunnels IP 27
 - 1.4 Commande de copie sécurisée 28
 - 1.5 Automatisation de sauvegarde avec copie sécurisée 30
 - 1.6 Échanges de fichiers sécurisés 33
 - 1.6.1 Échanges via sftp 33
 - 1.6.2 Échanges via vsftp 34
- 2. Synchronisation avec rsync 38
 - 2.1 Présentation 38
 - 2.2 Quelques cas d'utilisation simple 41

2 _____ Debian GNU/Linux

Maîtrisez la sécurité des infrastructures

2.3	Sauvegarde complète de machine	42
2.4	Somme de contrôle et mode avancé	44
2.5	Utilisation en tant que service	46
3.	Sauvegarde UrBackup	47
3.1	Fonctionnalités et architecture	47
3.2	Interface applicative	48
3.3	Fonctionnement sécurisé	51
3.4	Nouveaux clients	53
4.	Outil AMANDA	56
4.1	Architecture AMANDA	56
4.2	Configuration du serveur AMANDA	58
4.3	Configuration des clients	64
4.4	Vérification des bandes	66
5.	Sauvegarde d'entreprise	68
5.1	Solution BACULA	68
5.2	Installation	70
5.3	Configuration des services	71
5.3.1	Service de stockage	71
5.3.2	Service du directeur	73
5.3.3	Configuration des clients	79
5.4	Sauvegarde des postes client	80
5.5	Changement de répertoire de sauvegarde	89
6.	Gestionnaire de clonage	90
6.1	Installation	90
6.2	Utilisation et sauvegarde	92
6.3	Méthode de restauration	94

Chapitre 2

Outils d'audit et d'analyse

1.	Gestion de ressource	97
1.1	Équipements et matériels	97
1.2	Environnement	105
1.3	Réseau	112

- 2. Analyse du réseau 118
 - 2.1 Renifleur réseau 119
 - 2.2 Outil nmap 120
 - 2.3 Utilisation de nmap 120
 - 2.4 L’outil nmap et le Wi-Fi 123
- 3. Analyse des paquets 124
 - 3.1 Généralités et définitions 124
 - 3.2 L’outil tcpdump 125
 - 3.3 L’outil wireshark 127
 - 3.4 L’outil scapy 135
- 4. Détection d’intrusion 139
 - 4.1 Utilisation d’un IDS 139
 - 4.2 Outil snort 142
 - 4.3 Gestion d’un IDS via pfsense 148
 - 4.4 Outil suricata 152
- 5. Test de pénétration 155
 - 5.1 Présentation 155
 - 5.2 Installation 156
 - 5.3 Initialisation 157
 - 5.4 Configuration 159
 - 5.5 Rapport d’audit 163
- 6. Utilitaire de test et de détection d’intrusion 164
 - 6.1 Les audits pentesting 164
 - 6.2 Outil Backbox en live-CD sur VirtualBox 166
 - 6.3 Exploration de BackBox 168
 - 6.4 Configuration de backbox 171

Chapitre 3
Outils de surveillance et supervision

- 1. Surveillance basique 175
 - 1.1 Présentation et définitions 175
 - 1.2 Installation de Glances 178
 - 1.3 Modes d’utilisation 180
 - 1.4 Configuration de Glances 182
 - 1.5 Alternative à Glances 184

2.	Supervision d'un système de calcul	188
2.1	Fonctionnalités	188
2.2	Installation	190
2.3	Configuration	191
2.3.1	Le fichier gmetad.conf	191
2.3.2	Le fichier gmond.conf	192
2.4	Sécurisation	194
2.5	État et statistiques	198
2.6	Alternative légère : cacti	199
3.	Supervision évoluée	207
3.1	Généralités	207
3.2	Installation	208
3.3	Configuration	209
3.4	Initialisation	211
3.5	Utilisation	216
4.	Supervision complète.	218
4.1	Présentation.	218
4.2	Installation	220
4.3	Configuration Apache2	221
5.	Alternative à Nagios	227
5.1	Généralités	227
5.2	Prérequis d'installation	228
5.3	Installation et configuration	229

Chapitre 4 **Services système et administration**

1.	Introduction	237
2.	Serveur de temps	237
2.1	Présentation.	237
2.2	Installation du serveur NTP	238
2.3	Installation du client NTP	241
2.4	Démarrage et vérifications	242
2.5	Sécurisation NTP	244

- 3. Matrices RAID 245
 - 3.1 Installation mdadm 247
 - 3.2 Création de matrices RAID 247
 - 3.3 Cas d'usage 251
- 4. Partages Linux 261
 - 4.1 Paramétrage serveur 262
 - 4.2 Paramétrage client 264
 - 4.3 Partages hétérogènes depuis Windows 266
 - 4.3.1 Montages SAMBA 266
 - 4.3.2 Montages cifs 270
- 5. Outils d'administration. 272
 - 5.1 Gestion des applications AMP. 272
 - 5.2 Utilisation de l'outil phpMyAdmin. 274
 - 5.3 Sécurisation de phpMyAdmin. 275
 - 5.4 Mise en œuvre de webmin. 277
 - 5.5 Sécurisation de webmin 278
 - 5.6 Notifications des nouvelles mises à jour 283
- 6. Les mécanismes de wrapper 284
 - 6.1 Principe de fonctionnement. 284
 - 6.2 Installation du wrapper 287
 - 6.3 Configuration du fichier inetd.conf. 287
 - 6.4 Les utilitaires du wrapper. 288
- 7. Les mécanismes de statistiques. 291
 - 7.1 Notion de comptabilité 291
 - 7.2 Service accton 291
 - 7.3 Les statistiques de la comptabilité. 292
 - 7.4 Utilisation de LBSA 293

Chapitre 5
De la redondance au cluster

- 1. Redondance 295
 - 1.1 Présentation des volumes SAN 296
 - 1.2 Snapshot sur LVM 304
 - 1.3 Carte d'interface réseau et bonding. 304
 - 1.4 Synchronisation des disques 309

6 **Debian GNU/Linux**

Maîtrisez la sécurité des infrastructures

1.5	Duplication des services	314
2.	Mise en œuvre d'un cluster	320
2.1	Utilisation de LVS	320
2.2	Utilisation de KeepAlived	323
2.3	Utilisation de heartbeat	328
3.	Haute disponibilité	329
3.1	Architecture à initialiser	329
3.2	Installation de corosync	331
3.3	Configuration de corosync	332
3.4	Configuration de pacemaker	334
4.	Application aux bases de données	335
4.1	Installation	336
4.2	Utilisation et configuration	338
4.3	Système maître/esclave : londiste	342
4.4	Réplication PostgreSQL	346
4.5	Mise en œuvre de la réplication	348

Chapitre 6

Loadbalancing et qualité de service

1.	Équilibrage de charge	357
1.1	Comment optimiser le trafic ?	357
1.2	Équilibrage de charge pfsense	359
1.3	Installation de pfsense	360
1.4	Configuration et accès aux fonctionnalités	365
2.	Configuration de pfsense	366
2.1	Configuration de base	366
2.2	Configuration d'interface réseau	369
2.3	Fonctionnalités supplémentaires	372
2.4	Activation de l'équilibrage de charge	373
2.5	Gestion des règles d'accès	377
3.	Sécurisation de pfsense	381
3.1	Déploiement d'un tunnel VPN site-à-site	381
3.2	Mise en œuvre	385
3.3	Tests de la configuration	391

- 3.4 Sauvegarde/restauration de la configuration 392
- 3.5 Installation d'Open-VM-Tools 394
- 4. Qualité de service. 396
 - 4.1 Généralités 396
 - 4.2 Approche directe 397
 - 4.3 Mise en œuvre de trickle 404
 - 4.4 Mise en œuvre de wondershaper 406
- 5. Intégration d'un bac à sable 407
 - 5.1 Le sandbox. 407
 - 5.2 Utilisation de seccomp 410
 - 5.3 Mise en œuvre de firejail 411
 - 5.4 Compléments de firejail 412

Chapitre 7
Outils forensic

- 1. La science de l'analyse forensic 415
 - 1.1 Le contexte 415
 - 1.2 Les objectifs. 416
 - 1.3 Catégorisation des outils 418
 - 1.4 Dans quels cas utiliser l'analyse forensic ? 427
- 2. Kali linux 429
 - 2.1 Fonctions et rôles 429
 - 2.2 Installation de la suite Kali Linux 430
 - 2.3 Configuration et exploitation 437
 - 2.4 Exemples d'utilisation 441
- 3. Caine live 447
 - 3.1 Fonctions et rôles 447
 - 3.2 Initialisation de Caine Live 450
 - 3.3 Configuration et exploitation 459
 - 3.4 Exemples d'utilisation 461
- 4. Deft Linux 464
 - 4.1 Fonctions et rôles 464
 - 4.2 Installation de Deft Linux 468
 - 4.3 Configuration et exploitation 474

4.4	Exemples d'utilisation.....	480
5.	Helix.....	483
5.1	Fonctions et rôles.....	483
5.2	Installation d'Helix.....	486
5.3	Configuration et exploitation.....	489
5.4	Exemples d'utilisation.....	490
5.5	Liste d'outils d'analyses forensic.....	492

Conclusion

1.	Niveaux évolutifs.....	495
2.	Gestion de statistiques et de journaux.....	496
3.	Bilan des opérations.....	498
4.	Pour conclure.....	499

Glossaire.....	501
Index.....	515



Chapitre 3

△ Outils de surveillance et supervision

1. Surveillance basique

1.1 Présentation et définitions

Après s'être intéressé à l'analyse des différentes machines d'une infrastructure, il est temps d'étudier la mise en place d'instruments de supervision sur les machines de l'environnement de production. Avant de commencer, il est important de bien distinguer l'analyse et la supervision. Dans le premier cas, comme abordé dans le chapitre précédent, il s'agit plus de récupérer de l'information, ponctuellement. Alors que dans le cas présent nous chercherons à garder un œil (voire les deux, de préférence) sur l'évolution de l'exploitation des machines du parc informatique. La définition exacte de la supervision informatique est la suivante : il s'agit de la surveillance du bon fonctionnement d'un système et/ou d'une activité. C'est pourquoi il est primordial de posséder un mécanisme connecté en permanence, remontant les alertes en cas d'incidents. Cela doit permettre de rapporter, alerter et surveiller les fonctionnements aussi bien normaux qu'anormaux des systèmes informatiques. Cette préoccupation doit répondre aux points suivants :

- surveillance technique : gestion du réseau, de l'infrastructure et des machines sous-jacentes
- surveillance applicative : gestion des applications et des processus métiers
- surveillance des contrats de services : gestion des indicateurs contractuels, type SLA
- surveillance métier : inspection des processus métiers de l'entreprise via des KPI

Dans ce dernier cas, nous devons bien sûr nous assurer que l'ensemble des fonctionnalités mises en œuvre par les informaticiens respecte bien les préoccupations du cœur de métier. En d'autres termes, l'informatique n'est que l'outil permettant d'aider l'entreprise à être plus rentable et plus réactive. Le système de supervision est là pour envoyer des messages sur la console, aux administrateurs et aux utilisateurs, en cas de dysfonctionnement. Ce genre d'activité doit se faire après avoir sécurisé l'écosystème et de façon systématique 24h/24, 7j/7. Plusieurs méthodes de supervision sont à distinguer :

- la méthode locale, à l'aide d'outils spécialisés
- la méthode externe type ASP (*Application Service Provider*), au travers d'Internet
- la méthode SaaS (*Software as a Service*) via un Cloud privé ou hybride

Ces deux dernières techniques permettent à l'utilisateur :

- d'éviter les intégrations d'infrastructures techniques.
- de pouvoir se passer de compétences spécifiques dédiées au fonctionnement de ces solutions.
- d'éviter un investissement dans un logiciel particulier, spécialisé.
- de disposer d'une solution simple, même avec une informatique répartie géographiquement.
- de consulter n'importe où et à tout moment les données collectées.

La seule contrainte de ce genre de solution est la forte dépendance à un fournisseur d'accès à Internet ou prestataire de Cloud. En fait, le choix de la solution dépend fortement du besoin et des contraintes imposées par les utilisateurs. Dans le cas le plus simple, après avoir correctement sécurisé l'ensemble des couches du système d'exploitation Linux Debian, l'étape suivante consiste à s'intéresser à la détection d'incidents (de préférence avant l'utilisateur), voire même d'anticiper les pannes en s'appuyant alors sur la supervision du système. Mais, outre les méthodes évoquées précédemment, il existe différents niveaux de supervision :

La supervision locale

Pour certaines entités, relativement petites, il est quelquefois plus intéressant de gérer les différents aspects de la supervision, en local : c'est-à-dire, sur chaque serveur du réseau. Cela permet d'avoir individuellement un tableau de bord pour chaque machine et de pouvoir valider tous les échelons : système, réseau, performances disques, ressources mémoire... et également de valider les éventuels goulots d'étranglement de façon rapide. Cela s'apparente à un mode dit "dashboard" dans lequel nous pourrions utiliser indifféremment :

- Glances
- lynis

La gestion des métriques du système

Dans le cadre de clusters de calculs ou de groupements de machines plus importantes, nous pouvons aussi nous intéresser uniquement à l'aspect système en remontant essentiellement les métriques telles que CPU, performances disques, utilisation de la mémoire, occupation disques... mais sans pour autant nous préoccuper du réseau et de l'environnement extérieur (même si celui-ci reste indéfectiblement lié à la machine). Ainsi, nous pouvons facilement déterminer les points d'amélioration d'un serveur et prédire ses défaillances. Cela correspond plus à un mode de supervision système qui pourra être géré par :

- ganglia
- cacti

La supervision avec gestion d'état

Au sein d'infrastructures assez conséquentes, la supervision devient plus délicate et nécessite très souvent de pouvoir constituer des rapports généraux, mais également de zoomer spécifiquement sur certaines métriques au travers du temps afin de connaître les fréquences d'usure et d'utilisation des équipements. Cela correspond plus à un mode basique que pourront fournir :

- zabbix
- munin

La supervision orientée métier

Très rapidement, les informaticiens ont eu besoin d'orienter leur surveillance autour d'applications spécifiques et de les corréliser à leurs équipements. C'est pourquoi certains logiciels s'articulent autour des préoccupations métier, plus proches des utilisateurs, comme les outils :

- nagios
- centreon

La supervision universelle modulaire

Étant donné que la préoccupation finale reste néanmoins l'utilisateur et ses applications, il a également fallu orienter la supervision universelle vers des aspects plus métiers que Nagios. C'est dans cette vision qu'est né Shinken.

■ Remarque

On pourra aussi détailler l'aspect analyse du trafic réseau permettant de vérifier les types de paquets transitant entre les différentes machines de l'entreprise, y compris ceux entrant ou sortant du LAN. De plus, il existe de nombreuses autres solutions commerciales telles que WhatsUpGold, ou encore PRTG.

La supervision industrielle

Il existe des solutions pour le contrôle de processus et d'automatisation. Ici, on s'intéresse uniquement à la partie spécifique du processus de supervision au sein d'un corps de métiers. En ce cas, seront utilisés des outils comme :

- `Proview` : pour le contrôle de processus et/ou d'automatisation
- `Lintouch` : pour la création des applications SCADA pour clients individuels
- `Energoscada` : pour le contrôle de la supervision énergétique des bâtiments

1.2 Installation de Glances

Lorsqu'un serveur est mis en production au sein d'une petite entité, nous souhaiterons surveiller a minima l'utilisation des ressources de celui-ci : RAM, CPU, disques... Pour cela, nous installerons un utilitaire, appelé `Glances` sur le serveur en question. Il s'agit d'un programme développé en Python par Nicolas HENNION, effectuant une surveillance des serveurs en mode texte (comparable en cela à l'utilitaire `htop`, ou `pstree`). Cela signifie que pour l'installer, nous devons passer par le gestionnaire d'installation Python officiel, appelé `pip` :

```
# apt-get install python-dev python-pip
```

■ Remarque

Depuis la version Debian 8 (Jessie), il existe un package `glances` installable directement, mais jusqu'à la version Wheezy, il est nécessaire de passer par l'assistant Python.

Il ne reste plus alors qu'à installer le programme `glances`, en installant le package éponyme :

```
# apt-get install glances
```

Invoquons la commande `glances` pour pouvoir vérifier le bon fonctionnement :

```
debian (debian 8.8 64bit / Linux 3.16.0-4-amd64) Uptime: 0:01:10
CPU      0.7% nice:  0.0%  LOAD  1-core MEM   39.2% SWAP   0.0%
user:    0.7% irq:  0.0%  1 min: 1.70 total: 1000M total: 2.00G
system:  0.0% iowait: 0.0%  5 min: 0.51 used:  392M used:  0
idle:    99.3% steal: 0.0% 15 min: 0.18 free:  608M free:  2.00G

NETWORK  Rx/s Tx/s TASKS 153 (278 thr), 1 run, 152 slp, 0 oth
eth0     0b   0b
lo       520b 520b

DISK I/O R/s  W/s
dm-0     0    0
dm-1     0    0
dm-2     0   18K
dm-3     0    0
dm-4     0   29K
sda1     0    0
sda2     0    0
sda5     0   47K
sr0      0    0

FILE SYS  Used Total Warning or critical alerts (one entry)
2017-08-17 21:13:43 2017-08-17 21:13:33 (0:00:03) - CRITICAL on CPU USER
```

Remarque

Il arrive parfois que l'affichage se fasse sur un fond clair avec des caractères presque blancs. Pour optimiser l'affichage pour un fond blanc, il faut utiliser l'option `--theme-white`.

Comme nous le constatons sur cette capture, l'écran est alors fractionné en sept grandes familles permettant de disposer en un coup d'œil des principales métriques du système :

- CPU
- LOAD
- MEM
- SWAP
- NETWORK
- TASKS
- DISK I/O

La première ligne de l'écran contient à la fois le nom du serveur, sa distribution, ainsi que sa version et l'architecture du serveur. Les codes couleur parlent d'eux-mêmes :

- Le vert : pour signifier que la statistique est acceptable.
- Le bleu : pour signifier qu'il faut faire attention (à surveiller).
- Le violet : pour signifier que la statistique est en alerte.

– Le rouge : pour signifier que la statistique est critique.

Nous pouvons nous assurer de la bonne installation de l'outil en vérifiant la version de celui-ci :

```
root@debian:/home/phil# glances -V
Glances v2.1.1 with psutil v2.1.1
```

1.3 Modes d'utilisation

Suite à la demande de nombreuses personnes, Glances v2 intègre, en plus du mode "standalone" (permettant de superviser une machine localement), et de son mode client/serveur (option `-s`), permettant de surveiller n'importe quelle machine distante, un mode web. En lançant le programme en mode serveur web (c'est-à-dire en utilisant l'option `-w`), nous pouvons alors interroger l'application depuis n'importe quel navigateur web présent sur le système local ou distant. Ainsi, en ouvrant un navigateur web avec l'adresse `http://localhost:61208` (ou `http://debian.mydmn.org/61208`), nous devrions alors pouvoir visualiser la même interface que précédemment, mais au travers du navigateur :

