

Guide d'installation d'un serveur LAMP

Cedric Malherbe

ced at 404consulting dot com

Guide d'installation d'un serveur LAMP

par Cedric Malherbe

Publié 2004-10-26

Guide d'installation, configuration et sécurisation d'un serveur Linux Apache MySQL PHP

Table des matières

A propos de ce document	i
1. Objectif	i
2. Historique	i
1. Introduction.....	1
1.1. But de l'installation	1
1.2. Configuration matérielle requise	1
1.3. Choix du système d'exploitation	1
2. Procédure d'installation de Debian GNU/Linux Sarge	2
2.1. Boot option	2
2.2. Choix de la langue	2
2.3. Choix du clavier	2
2.4. Nom de la machine.....	2
2.5. Configuration réseau	2
2.6. Partitionnement du disque dur.....	2
2.7. Installation des paquets	3
2.8. Système d'amorçage (boot loader).....	3
2.9. Fin de l'installation.....	3
3. Configuration post-installation	4
3.1. Configuration de l'heure.....	4
3.2. Mot de passe administrateur (root).....	4
3.3. Création d'utilisateur(s).....	4
3.4. Configuration d'APT	4
3.5. Configuration du serveur de courrier.....	4
3.6. Fin.....	5
4. Installation d'applications serveurs	6
4.1. Serveur HTTP.....	6
4.2. Base de données	6
4.3. Serveur FTP.....	6
5. Sécurisation du système.....	7
5.1. Points de montage	7
5.2. Sécurisation de base	7
5.2.1. GRUB	7
5.2.2. Mot de passe	7
5.2.3. Login.....	8
5.3. Sécurisation des services	8
5.3.1. Désactiver les services inutiles	8
5.3.2. SSH.....	8
5.3.3. FTP	9
5.4. Mise en place d'un pare-feu	9
5.5. Mise à jour de sécurité	11
6. Quota.....	13
7. Sauvegarde.....	15
7.1. Sauvegarde des fichiers	15
7.2. Sauvegarde de la base de données.....	15
7.3. Automatiser les sauvegardes avec <i>cron</i>	15
8. Plus d'information	18

Liste des tableaux

1. Historique du document.....	i
2-1. Partitionnement.....	3
5-1. Sécuriser les points de montage.....	7

A propos de ce document

1. Objectif

Ce document discute de la mise en service d'un serveur web sous Debian GNU/Linux. Les points abordés sont l'installation, la configuration des services et la sécurisation de la machine.

Ce guide se veut simple et n'aborde qu'une partie de la configuration d'un serveur. Il se focalise sur la mise en place d'un hébergement dédié de pages dynamiques.

2. Historique

Tableau 1. Historique du document

Date	Modification
2004-07-05	Première version publique
2004-08-09	Correction et amélioration de la partie sur les quotas, des scripts iptables (pare-feu), mise-à-jour de sécurité et nom de machine.
2004-10-26	Petite correction dans la partie concernant la sécurisation de SSH.

Chapitre 1. Introduction

1.1. But de l'installation

Mettre en place un serveur web dédié pour l'hébergement de contenus dynamiques (PHP, CGI...) en relation avec des bases de données (SQL).

1.2. Configuration matérielle requise

Ce guide ne discute que de l'installation sur une architecture Intel x86 (et compatible), mais d'autres architectures sont envisageable (PowerPC, Sparc, Alpha...).

- Processeur: Pentium 2 ou équivalent
- Mémoire: 32-64Mo minimum
- Disque dur: 500Mo à plusieurs Go suivant les besoins
- Carte réseau: 10/100Mbits

1.3. Choix du système d'exploitation

Le choix du système d'exploitation s'est porté sur GNU/Linux étant donné ses besoins matériels faibles, sa stabilité et son coût de déploiement et de maintenance.

La distribution retenue est Debian GNU/Linux pour sa stabilité, sa facilité de mise à jour (apt) et son suivi de sécurité (debian security).

Chapitre 2. Procédure d'installation de Debian GNU/Linux Sarge

2.1. Boot option

4 types d'installation sont disponible:

- *linux* (choix par défaut)
- *expert* (pour chaque étape de l'installation, une confirmation est demandé)
- *linux26* (idem que *linux* mais installation du kernel 2.6 au lieu du 2.4)
- *expert26* (idem que *expert* mais installation du kernel 2.6 au lieu du 2.4)

La suite du document décrit l'installation de Debian GNU/Linux en mode *linux* / *linux26*.

2.2. Choix de la langue

Choisir la langue souhaité et sa variante. Par exemple: *fr_BE*

2.3. Choix du clavier

Dépend souvent de la langue. 105 touches + support Euro: *Belgique Latin 1*

2.4. Nom de la machine

A votre convenance. Il ne s'agit pas du nom de domaine qualifié, ne mettez donc pas *monsite.com* ici.

2.5. Configuration réseau

Vous avez le choix entre la configuration automatique via *DHCP* ou un réglage manuel.

En cas de configuration manuel, entrer l'adresse IP de votre machine (adresse statique), le masque de sous-réseau (netmask) et éventuellement l'adresse de broadcast, l'adresse de votre passerelle (gateway) et les serveurs de noms (résolution DNS).

2.6. Partitionnement du disque dur

Exemple de partitionnement pour un disque dur d'environ 5Go:

Tableau 2-1. Partitionnement

Point de montage	Système de fichiers	Taille	Type	spécificité
/boot	ext2	50Mo	primaire	amorçable
/	Reiser FS	150Mo	logique	
/usr	Reiser FS	2Go	logique	
/var	Reiser FS	1.5Go	logique	
/tmp	ext2	100Mo	logique	
/home	Reiser FS	1Go	logique	
/swap	Swap	200Mo	logique	

Pour un serveur, la taille de la partition `/var` doit être suffisamment grande pour stocker les logs et les emails en attente. 1Go ne sera pas de trop si vous comptez fournir un service email.

La taille de la partition `/home` doit refléter le nombre d'utilisateurs dont vous souhaitez fournir un compte et un espace de stockage.

2.7. Installation des paquets

L'installation des paquets de base se fait automatiquement, aucune intervention n'est donc nécessaire pendant quelques minutes.

2.8. Système d'amorçage (boot loader)

GRUB (choix par défaut)

Si votre machine comporte plusieurs systèmes d'exploitations, ceux-ci seront automatiquement détectés et leur entrée respective ajoutée au menu de GRUB.

2.9. Fin de l'installation

L'installation de base est maintenant terminée. Retirez le CD, le système va redémarrer.

Chapitre 3. Configuration post-installation

3.1. Configuration de l'heure

L'horloge matérielle est-elle réglée sur GMT? *Oui*

Choix du fuseau horaire: *Europe/Brussels*

3.2. Mot de passe administrateur (root)

La complexité du mot de passe root est la clé de la sécurité de votre système. N'hésitez pas à mélanger minuscules, majuscules et chiffres.

3.3. Création d'utilisateur(s)

Créez au moins un utilisateur pour se connecter à la machine, même si vous (l'administrateur) êtes le seul à l'y accéder.

On ne se connecte jamais en root!

3.4. Configuration d'APT

APT vous permet de mettre à jour votre système et d'installer des paquets supplémentaires. Plusieurs options vous sont proposées (cdrom, ftp, http, sauter l'étape). Si votre réseau fonctionne, choisissez ftp (ou http si un pare-feu éventuel bloque l'accès sur le port 21)

- Méthode: *FTP*
- Version de Debian¹: *stable*
- Pays: *Belgique*
- Choix du serveur: *ftp.debian.skynet.be*
- Mise à jour de sécurité (security.debian.org)? *Oui*

3.5. Configuration du serveur de courrier

Exim 4 est installé par défaut.

Choisissez la configuration "*pour site internet*".

Configurez les alias mail (root & postmaster) vers le compte utilisateur de l'administrateur.

Vous pourrez changer cette configuration après l'installation via la commande:

```
machine:~# dpkg-reconfigure exim4-config
```

3.6. Fin

A ce stade, votre système Debian GNU/Linux est utilisable, mais dépourvu d'applications et encore peu sécurisé. Les étapes suivantes ont pour but de remédier à ces manquements.

Notes

1. La distribution Debian se compose de trois branches distinctes: *stable*, *testing* et *unstable*.

Stable est la version "super" stable, longuement testé et dispose de mise à jour de sécurité. La branche *unstable* profite des dernières nouveautés logiciels mais ne garanti pas que le système soit pleinement fonctionnel. *Testing* se situe entre les deux, elle recoit au fur et à fur les paquets de la version *unstable* si ceci sont considérés comme suffisamment solide. Elle ne dispose cependant d'aucune mise à jour de sécurité.

Pour une utilisation serveur, le choix de la branche *stable* s'impose de lui-même.

Chapitre 4. Installation d'applications serveurs

4.1. Serveur HTTP

Installez Apache 1.3 et PHP 4:

```
machine:~# apt-get install apache apache-utils php4
```

Editez `/etc/apache/httpd.conf` et modifiez les options suivantes comme décrites:

```
MaxClients 25
ServerAdmin votre@adresse.email
ServerName www.votre-domain.com
DocumentRoot /var/www
AddType application/x-httpd-php .php
```

La valeur de *MaxClients* dépend de la quantité de mémoire vive de votre serveur. La valeur par défaut (150) est souvent bien trop élevée pour une petite configuration.

4.2. Base de données

Installez MySQL 4:

```
machine:~# apt-get install mysql-server mysql-common php4-mysql
```

Par défaut, aucun mot de passe pour MySQL n'est défini. Pour ajouter un mot de passe, exécutez la commande suivante:

```
machine:~# mysqladmin -u root password mot_de_passe
```

4.3. Serveur FTP

Intallez ProFTP:

```
machine:~# apt-get install proftpd
```

Chapitre 5. Sécurisation du système

5.1. Points de montage

Editez `/etc/fstab` et modifiez les options comme décrit:

Tableau 5-1. Sécuriser les points de montage

Point de montage	Options
/boot	defaults,ro
/usr	defaults,ro,nodev
/var	defaults,nodev
/tmp	defaults,nosuid,noexec,nodev

`/usr` étant en lecture seul (*ro*), il sera impossible d'installer ou de mettre à jour votre système sans remonter la partition en lecture/écriture. L'option *noexec* de la partition `/tmp` peut également poser des problèmes.

Pour contourner ces problèmes et ne pas devoir effectuer les changements manuellement à chaque fois, rajoutez ceci dans le fichier de configuration d'APT (`/etc/apt/apt.conf`):

```
DPkg
{
  Pre-Invoke { "mount /usr -o remount,rw" };
  Pre-Invoke { "mount /tmp -o remount,exec" };
  Post-Invoke { "mount /usr -o remount,ro" };
  Post-Invoke { "mount /tmp -o remount,noexec" };
};
```

5.2. Sécurisation de base

5.2.1. GRUB

Ajoutez un mot de passe. Editez `/boot/grub/menu.lst` et rajoutez la ligne suivante:

```
password --md5 hash_du_mot_de_passe
```

Pour générer le hash de votre mot de passe, utilisez le programme **grub-md5-crypt**.

5.2.2. Mot de passe

Activer le mode *shadow password* si vous l'avez désactivé lors de l'installation:

```
machine:~# shadowconfig on
```

De manière générale, utilisez des mots de passe suffisamment long et complexe (mélangez majuscules, minuscules, chiffres...).

Pour générer de bon mots de passe, utilisez **apg** (**apt-get install apg**). Ce programme a l'avantage de créer des mots de passe prononçable tout en étant suffisamment complexe.

5.2.3. Login

Pour une politique de sécurité accrue, bloquez l'accès au compte administrateur depuis l'extérieur.

Editez `/etc/security/access.conf` et ajoutez la ligne suivante:

```
-:wheel:ALL EXCEPT LOCAL
```

Pour se connecter à distance, il faudra alors passer par un compte utilisateur, puis se connecter en root via la commande **su**.

5.3. Sécurisation des services

5.3.1. Désactiver les services inutiles

Editez `/etc/inetd.conf` et commentez tous les services inutiles:

- echo
- chargen
- discard
- daytime
- time

Relancer le démon *inet* avec la commande suivante:

```
machine:~# /etc/init.d/inetd restart
```

5.3.2. SSH

Editez `/etc/ssh/sshd_config` et ajoutez les options suivantes:

```
Protocol 2
AllowGroups staff
PermitRootLogin no
PermitEmptyPasswords no
```

N'oubliez pas de vous ajouter au groupe `staff` (désormais le seul groupe à pouvoir se connecter au serveur via ssh):

```
machine:~# adduser votre_login staff
```

5.3.3. FTP

Editez `/etc/proftpd.conf` et ajoutez les options suivantes:

```
DefaultRoot ~
DenyFilter \*.*/*
```

L'option `DefaultRoot ~` enferme les utilisateurs dans leur répertoire personnel, les empêchant ainsi de se balader dans l'arborescence système.

Dans le même ordre d'idée mais en excluant le groupe `staff` de la directive: `DefaultRoot ~ !staff`.

5.4. Mise en place d'un pare-feu

But du pare-feu: bloquer toute connexion au serveur sur les ports autre que 21 (ftp), 22 (ssh) et 80/443 (http).

Nous utiliserons `netfilter/iptables` comme pare-feu:

```
machine:~# apt-get install iptables
```

Voici les règles du pare-feu à placer dans un fichier nommé `firewall-start` (par exemple). Nous le copierons dans le dossier `/etc/network/if-pre-up.d/` afin qu'il soit activé à chaque démarrage de l'interface réseau.

```
#!/bin/sh
# Configuration du pare-feu

modprobe ip_conntrack_ftp
```

```
# Configuration:
# Indiquez l'adresse IP de votre serveur ici:
IPADDRESS=adresse_ip_de_votre_serveur

#
# Parametrage au niveau du noyau
#

echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo 1 > /proc/sys/net/ipv4/tcp_syncookies #this violate a RFC!
echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/all/send_redirects

#
# Vider les regles de filtrage
#

iptables -F

#
# Politique par défaut
#

# bloquer les paquets entrants
iptables -P INPUT DROP

# accepter les paquets sortants
iptables -P OUTPUT ACCEPT

# bloquer les transferts
iptables -P FORWARD DROP

#
# Filtres de base
#

# accepter le trafic sur l'interface loopback
iptables -A INPUT -i lo -j ACCEPT

# bloquer le spoofing de l'adresse loopback
iptables -A INPUT -s 127.0.0.0/8 -j DROP
iptables -A INPUT -d 127.0.0.0/8 -j DROP

# bloquer les tentatives de spoofing de l'adresse IP locale
iptables -A INPUT -s $IPADDRESS -j DROP

# s'assurer que les connexions TCP commencent avec des paquets syn
iptables -A INPUT -p tcp -m tcp ! --syn -m state --state NEW -j DROP

# protection contre le ping flood
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP

# accepter les autres requetes icmp
iptables -A INPUT -p icmp -j ACCEPT

# accepter les connexions pre-etablies
```

```
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#
# connexions aux serveurs
#

# accepter les connexions ssh
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# accepter les connexions web
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT

# accepter les connexions ftp
iptables -A INPUT -p tcp --dport 21 -j ACCEPT
```

Et maintenant le fichier `firewall-stop` pour arrêter le pare-feu, à placer dans le dossier `/etc/network/if-post-down.d/`

```
#!/bin/sh
# Configuration sans pare-feu

echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo 0 > /proc/sys/net/ipv4/tcp_syncookies
echo 1 > /proc/sys/net/ipv4/conf/all/accept_redirects
echo 1 > /proc/sys/net/ipv4/conf/all/send_redirects

# Vider les regles de filtrage
iptables -F

# Politique par défaut: tout accepter
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

Assurez-vous que ces scripts soient exécutable:

```
machine:~# chmod 755 /etc/network/if-pre-up.d/firewall-start
machine:~# chmod 755 /etc/network/if-post-down.d/firewall-stop
```

Cette configuration vous permet également d'arrêter et de redémarrer le pare-feu manuellement avec les commandes suivantes:

```
machine:~# sh /etc/network/if-post-down.d/firewall-stop
machine:~# sh /etc/network/if-pre-up.d/firewall-start
```

5.5. Mise à jour de sécurité

Si vous n'avez pas configuré les mises à jour de sécurité pendant l'installation de Debian, éditez `/etc/apt/sources.list` et ajoutez la ligne suivante:

```
deb http://security.debian.org/ sarge/updates main
```

Pour une mise à jour manuelle, exécutez:

```
machine:~# apt-get update
machine:~# apt-get upgrade
```

Pour automatiser la mise à jour, installez **cron-apt**:

```
machine:~# apt-get install cron-apt
```

Éditez `/etc/cron-apt/action.d/3-download` et appliquez les options suivantes:

```
upgrade -u -y
autoclean -y
```

La mise à jour se fera toutes les nuits à 4h00.

Chapitre 6. Quota

Attention, le support des quotas sur les partitions Reiser FS n'est disponible qu'à partir de la version 2.6.7 du noyau Linux. Il vous faudra donc appliquer un patch si vous possédez un noyau plus ancien.

```
machine:~# apt-get install quota
```

Editez `/etc/fstab` et ajoutez les options suivantes à la partition voulue:

```
usrquota,grpquota
```

Préparation de la partition (*/home* en exemple):

```
machine:~# touch /home/quota.user /home/quota.group
machine:~# chmod 600 /home/quota.*
machine:~# mount -o remount /home
```

Activer les quotas:

```
machine:~# quotacheck -avugm
machine:~# quotaon -a
```

Définir les quotas pour un utilisateur:

```
machine:~# edquota -u albert
```

```
Disk quotas for user albert (uid XXXX):
Filesystem      blocks      soft      hard    inodes      soft      hard
/dev/hdaX        24          0          0         7           0         0
```

Les valeurs de *blocks* et *inodes* représentent respectivement le nombre de blocs et de fichiers que l'utilisateur possède. Ces valeurs sont générées automatiquement, ne les modifiez pas.

Par contre, vous pouvez régler les valeurs limites *soft* et *hard*, à la fois pour les blocs et pour les inodes en remplaçant les zéros par les valeurs de votre choix (0 = pas de limite).

Pour définir des quotas sur les groupes, même principe, avec la commande suivante:

```
machine:~# edquota -g un groupe
```

Vous pouvez également définir une période de "grace" avant de faire respecter les quotas:

```
machine:~# edquota -t
```

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
Filesystem      Block grace period  Inode grace period
/dev/hdaX       7days               7days
```

Automatiser la vérification des quotas avec *cron*:

```
user@machine:~$ su
Password:
machine:~# crontab -e
```

Ajoutez-y les lignes suivantes:

```
# verification des quotas tous les dimanches a 3h30
30 3 * * 0 /sbin/quotacheck -avugm
```

Vous pouvez activer/désactiver les quotas à tout moment avec les commandes **quotaon** et **quotaoff**.

Chapitre 7. Sauvegarde

7.1. Sauvegarde des fichiers

Installez *rdiff-backup*

```
machine:~# apt-get install rdiff-backup
```

Pour effectuer une sauvegarde manuelle:

```
user@machine:~$ rdiff-backup /repertoire/a/sauvegarder /destination/de/la/sauvegarde
```

Pour restaurer les données, utilisez la commande suivante:

```
user@machine:~$ cp -a /repertoire/de/sauvegarde /emplacement/du/site
```

7.2. Sauvegarde de la base de données

Pour effectuer une sauvegarde de toutes les bases en une archive au format gzip:

```
user@machine:~$ mysqldump -u root --password --all-databases | gzip > backup.sql.gz  
Enter password:
```

Pour restaurer les bases, utilisez les commandes suivantes:

```
machine:~# gzip -d backup.sql.gz  
machine:~# mysql -u root < backup.sql
```

7.3. Automatiser les sauvegardes avec *cron*

Pour automatiser ces tâches, nous allons créer deux scripts maison regroupant les procédures à effectuer.

Dans le répertoire `/usr/local/bin/`, créez un fichier `sauvegarde_site` avec le contenu suivant:

```
#!/bin/sh  
# sauvegarde des fichiers/repertoires  
# hebdomadaire, sur les 4 dernieres semaines  
  
# A modifier:
```

```

SOURCE=/var/www
DESTINATION=/mnt/backup

DATE=`date +%Y-%m-%d`
WEEK=`date +%W`
let "DEL=$WEEK-4"

# backup de la semaine
/usr/bin/rsync -avz $SOURCE $DESTINATION/$WEEK.$DATE

# efface le backup vieux de 4 semaines
rm -rf $DESTINATION/$DEL.*

```

Toujours dans le répertoire `/usr/local/bin/`, créez un fichier `sauvegarde_bdd` avec le contenu suivant:

```

#!/bin/sh
# sauvegarde des bases de données
# hebdomadaire, sur les 4 dernières semaines

# A modifier:
USER=root
PASS=mot_de_passe_sql
DESTINATION=/mnt/backup

DATE=`date +%Y-%m-%d`
WEEK=`date +%W`
let "DEL=$WEEK-4"

# backup de la semaine
mysqldump -u $USER --password=$PASS --all-databases | gzip > $DESTINATION/$WEEK.$DATE.sql.gz

# efface le backup vieux de 4 semaines
rm -rf $DESTINATION/$DEL.*.sql.gz

```

Assurez-vous que les scripts soient exécutables:

```

machine:~# chmod 700 /usr/local/bin/sauvegarde_site
machine:~# chmod 700 /usr/local/bin/sauvegarde_bdd

```

Pour planifier l'exécution de ces scripts, procédez comme ceci:

```

user@machine:~$ su
Password:
machine:~# crontab -e

```

Ajoutez ensuite les lignes suivantes:

```

# backup des fichiers tous les samedi a 3h00
0 3 * * 6 /usr/local/bin/sauvegarde_site

# backup de la base de données tous les samedi a 3h00

```

```
0 3 * * 6 /usr/local/bin/sauvegarde_bdd
```

Il vous est également possible d'éditer directement le fichier `/var/spool/cron/crontabs/root` même si ce n'est pas conseillé (relancez le démon cron après modification).

La syntaxe fonctionne de la manière suivante:

```
0 3 * * 6 /usr/local/bin/sauvegarde_site
| | | | |
| | | | | |-----> programme à exécuter
| | | | |-----> jour de la semaine (0 pour dimanche, 1 pour lundi, etc.)
| | | |-----> mois (1-12)
| | |-----> jour (1-31)
| |-----> heure (0-23)
|-----> minute (0-59)

* est une wilcard = toujours "vrai"
```

La commande **crontab -l** permet de connaître toutes les entrées déjà configurées. La commande **crontab -r** permet de les effacer.

Chapitre 8. Plus d'information

Documentations, tutoriaux, howto...

- Formation Linux (<http://people.via.ecp.fr/~alexis/formation-linux/>) [fr]
- Debian Reference (<http://qref.sourceforge.net>) [en]
- Securing Debian Manual (<http://www.debian.org/doc/manuals/securing-debian-howto/>) [en]
- A ProFTP User's Guide (<http://proftpd.linux.co.uk/localsite/Userguide/linked/userguide.html>) [en]
- rdiff-backup documentation (<http://rdiff-backup.stanford.edu/docs.html>) [en]