Serveur Linux

Installation et configuration

2ème Bachelier en Informatique

Projet Linux

Auteur :

Terencio Agozzino

Auteur :

Alexandre Ducobu

Enseignants :

Antoine Malaise

Julien De Bodt

Année académique 2016 - 2017

Serveur Linux

Installation et configuration

2ème Bachelier en Informatique

Projet Linux

Auteur :

Terencio Agozzino

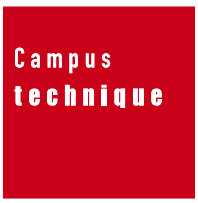
Auteur :

Alexandre Ducobu

Enseignants :

Antoine Malaise

Julien De Bodt



Année académique 2016 - 2017

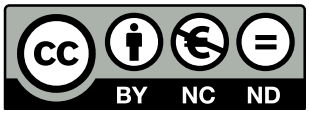


Table des matières

1 Présentation générale du projet

1.1 Introduction

Dans le cadre de ce projet, il nous a été demandé d'administrer un serveur sous Linux.

Le choix de la distribution ainsi que la gestion des sauvegardes est libre et devra être justifié.

Le serveur devra contenir :

- un partage NFS qui permettra aux utilisateurs du réseaux local d'y stocker des fichiers ;
- un partage Samba qui permettra aux utilisateurs de Windows d'accéder à ce même partage ;
- un serveur Web, FTP, MySQL et DNS qui permettra un hébergement multi-utilisateurs ;
  - le serveur FTP permettra à chaque utilisateur d'accéder à son dossier Web ;
  - le serveur DNS contient une zone qui sera indispensable pour les sites Web de l'utilisateur ;
  - le serveur DNS fera également office de DNS cache pour le réseau local.
- un serveur NTP pour que les machines du réseau local puissent se synchroniser ;
- le support du module SSH.

1.2 Déontologie

En tant qu'administrateurs du serveur, nous serons tenus de suivre de nombreuses règles telles que :

— la documentation des actions entreprises sur le serveur ;

— l'automatisation des installations et configurations au travers de scripts ;

— la sécurité : mise en place de mots de passe forts, du SSH, etc. ;

— la vigilance et la prévoyance, par exemple par la mise en place de sauvegardes avant et après chaque changement sur le serveur ;

— le contrôle du bon fonctionnement de chaque élément.

1.3 Sécurité

Du côté de la sécurité, quelques contraintes seront prises en compte :

— mise en place d'une politique utilisateur ;

— mise en place de quotas ;

— partitionnement et gestion du disque (LVM et RAID) ;

— mise en place d'une stratégie de sauvegarde ;

— désactivation des éléments inutiles et des mises à jours ;

— mise en place d'un antivirus, d'un firewall, etc.

2 Choix

2.1 Distribution

Le choix de la distribution s'est naturellement porté sur Debian, pour ses nombreux avantages. En voici quelques exemples :

— Large communauté : grâce à cela, les erreurs et problèmes rencontrés ont souvent plusieurs solutions connues et éprouvées.

— Plusieurs architectures et noyaux : Debian supporte la majorité des architectures de processeurs comme AMD, Armel, i386, MIPS, etc. Elle supporte aussi de nombreux noyaux tels que FreeBSD et GNU Hurd.

— Sécurité : vu que la distribution est open-source, cela signifie que les *backdoors* sont presque inexistantes. De surcroît, lorsqu'une faille de sécurité est détectée, celle-ci est rapidement corrigée par la communauté.

  En outre, Debian comprend de nombreux logiciels de sécurité tels que GPG (et PGP), SSH et autres.

— Stabilité : les serveurs doivent avoir le plus grand temps d'accessibilité ($\approx 99.999\%$). Sous Debian, il existe de nombreux exemples de machines qui tournent sans arrêt pendant des années, mis à part lors de pannes ou de mises à jour liées au matériel.

— Système de paquets : grâce au système de paquets, les distributions Linux ont la possibilité d'installer de nombreux logiciels par une seule ligne de commande.

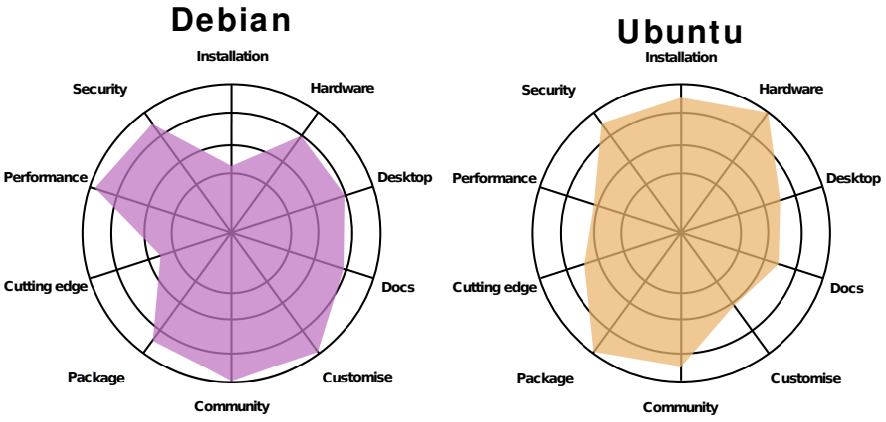


FIGURE 1 – Différences entre Debian et Ubuntu

De même, la distribution Debian est plus professionnel et celle-ci possède le *leadership* depuis des années.

Remarque : depuis mai 2016, Ubuntu a les mêmes parts de marché que Debian.

La distribution Ubuntu n'a pas été choisi pour les raisons suivantes :

— Dérivé de Debian : de ce fait, un administrateur sachant configurer un serveur sous Debian pourra facilitement s'adapter aux serveur sous Ubuntu.

— Vise le grand public. Par conséquent, est beaucoup moins utilisé dans le milieu professionnel.

— Assez récent sur le marché du serveur.

— Moins performant que Debian.

Concernant les autres distributions, CentOS est en baisse, mais reste au-dessus de Red Hat et de Fedora qui sont en chute libre.

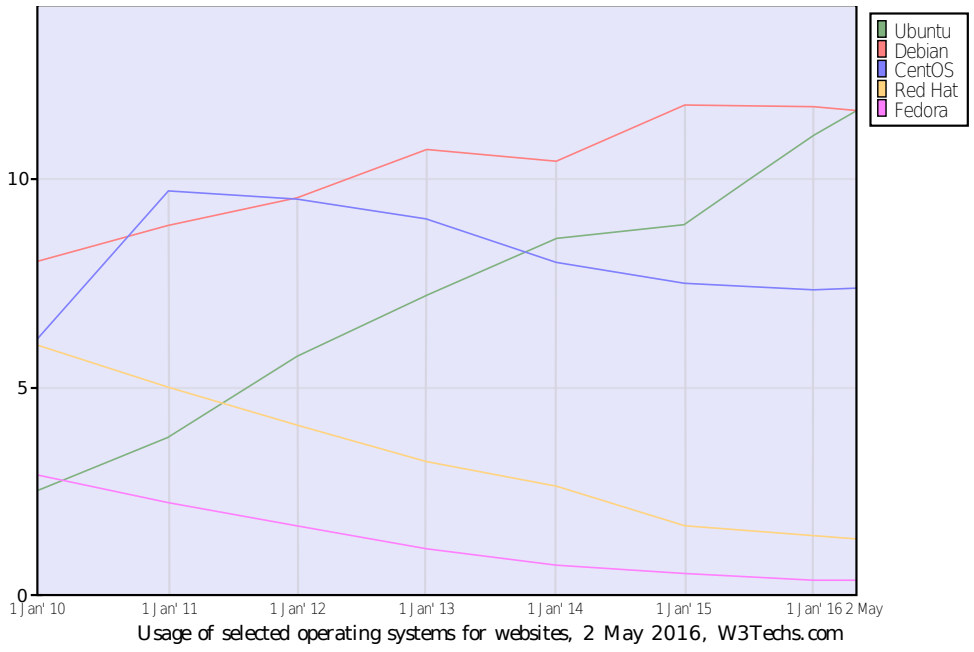


FIGURE 2 – Parts de marché des distributions Linux

2.2 Langue

Pour le choix de la langue lors de l'installation, il a été préféré d'utiliser l'anglais vu que la majorité des documentations et forums sont disponibles dans cette langue. De plus, cela permet d'éviter une mauvaise traduction concernant les nouvelles mises à jour et de toucher un plus large public possible.

2.3 Noyau

Un noyau (monolithique[1]) modulaire a été choisi afin de gérer les modules. En effet, celui-ci facilite l'ajout et la suppression de modules à chaud. Ces modules, pas toujours indispensables, peuvent être la source de failles et de bugs.

2.4 Partitionnement

Le partionnement du disque a été réalisé avec une partition racine, */boot*, et un groupe de volume LVM nommé *VolGroup*. De sucroît, deux disques de 10 Go en RAID 1 ont été utilisés.

Label	Type	Taille (Mo)	Format
/boot	primary	512	ext4
VolGroup	logical	20958	lvm
LVsrv (/srv)	lvm	6144	ext4
LVswap (/swap)	lvm	4096	swap
LVhome (/home)	lvm	2048	ext4
LVroot (/root)	lvm	2048	ext4
LVusr (/usr)	lvm	2048	ext4
LVopt (/opt)	lvm	2048	ext4
LVvar (/var)	lvm	1024	ext4
LVtmp (/tmp)	lvm	1024	ext4

TABLE 1 – Tableau du partitionnement *(avec LVM)*

1. Les fonctions du système et pilotes sont regroupées dans le kernel space généré à la compilation.

2.5 Sauvegardes

Dans le milieu de l'entreprise, deux types de sauvegarde sont principalement utilisées : incrémentielle [2] et différentielle [3].

Afin de trouver un compromis, ces deux types de sauvegardes ont été utilisés :

1. différentielle : afin de restaurer les données plus rapidement par rapport à la sauvegarde incrémentielle ;
2. incrémentielle : pour une rapidité de sauvegarde et un stockage en mémoire plus économe que la sauvegarde différentielle.

Dans le but d'éviter de perturber l'accès au serveur, tous les jours à deux heures du matin, une sauvegarde incrémentielle est lancée à l'aide d'un *cron* [4], dans le but d'enregistrer les données modifiées et créées en cette journée.

```
1 crontab -e 0 2 * * * /usr/bin/backup-make.sh -i
```

Quant à la sauvegarde différentielle, celle-ci s'opère uniquement le dimanche à 2 heures du matin. Le dimanche étant un jour de congé pour la majorité du monde, ce qui aura un impact mineur sur les performances du serveur.

```
1 crontab -e 0 2 * * 0 /usr/bin/backup-make.sh -d
```

Remarque : à défaut d'utiliser *fcron* n'étant plus disponible sur Debian, le serveur doit être alimenté à l'heure de l'exécution du *cron*. Néanmoins, cela ne pose pas de difficultés, vu que le rôle du serveur est de fournir une disponibilité permanente.

2. Sauvegarde exclusivement les données modifiées ou ajoutées depuis la précédente sauvegarde.
3. Sauvegarde les données modifiées ou ajoutées en référence à la dernière sauvegarde complète.
4. Gestionnaire des tâches sous Linux devant être exécutées à un moment précis.

3 Services

3.1 NTP

Le NTP (*Network Time Protocol*), est le protocole utilisé afin de synchroniser les machines du reseau local en fonction de l'horloge du serveur.

3.1.1 Principe

Bien que tout équipement informatique dispose d'une horloge, celle-ci dérive comme toute montre ordinaire, ce qui peut amener a des erreurs de synchronisation.
La nécessité de synchroniser des équipements en réseau paraît alors évidente.

Chaque machine peut être à la fois serveur et cliente. Celle-ci sélectionnera un serveur de temps dans sa configuration, et récupérera l'heure, ainsi qu'un numéro de strate, *n*, et se déclarera de strate *n + 1*.

L'architecture du réseau est en arborescence, et divisée en trois couches :

1. les plus précises sources (horloges atomiques, récepteurs GPS, ...) sont de *strate 0* ;
2. les serveurs diffusant l'heure des sources sont de *strate 1* ;
3. les serveurs de *strate 2* sont généralement accessibles au public.

3.1.2 Configuration du serveur

La totalité de l'implémentation se trouve dans le fichier */etc/ntp.conf*

Voici les différentes étapes et options qui ont été effectuées :

— activation des statistiques NTP ;

— ajout de trois serveurs (un belge et deux européens) ;

— activation de l'échange de l'heure avec tout le monde (aucune modification n'est acceptée) ;

— activation de la synchronisation avec les machines du réseau local.

```
...

# Adjust time server.
ntpdate 1.be.pool.ntp.org

driftfile /var/lib/ntp/ntp.drift

# Statistics loopstats peerstats clockstats.
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# You do need to talk to an NTP server or two (or three).
server 1.be.pool.ntp.org iburst
server 3.europe.pool.ntp.org
server 2.europe.pool.ntp.org

# By default, exchange time with everybody, but don't
# allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery

# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict 10.1.0.0 mask 255.255.0.0 nomodify notrap nopeer
restrict ::1

# To provide time to the local subnet.
broadcast 10.1.255.255

...
```

Remarque : l'adresse de diffusion (*broadcast*) a été adapté en fonction du réseau.

3.1.3 Configuration du client

Tout comme le serveur, la totalité de l'implémentation se trouve dans le fichier */etc/ntp.conf*

Sur le client, la configuration est beaucoup plus simple :

— activation des statistiques NTP ;

— ajout du serveur local.

```
...

# Adjust time server.
ntpdate 1.be.pool.ntp.org

# File containing the average deviation.
driftfile /var/lib/ntp/ntp.drift

# Desired Statistics.
statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# You do need to talk to an NTP server or two (or three).
server 10.1.214.184 prefer

...
```

Remarque : l'adresse IP "10.1.214.184" étant celle du serveur NTP.

3.2 SSH

Le SSH (*Secure Shell*), est un protocole de communication sécurisé. Celui-ci impose un échange de clés de chiffrement en début de connexion.

3.2.1 Type d'authentification

Il existe plusieurs manières de s'authentifier sur le serveur via SSH.

Les deux authentifications les plus utilisées sont :

1. par mot de passe ;
2. par clés publiques et privées du client.

L'identification automatique par clés a été mise en place pour ce serveur. De ce fait, il est nul nécessaire d'entrer le mot de passe à chaque connexion à distance.
Cette méthode est plus complexe à mettre en place, mais elle est surtout plus pratique.

On remarque rapidement son utilité si on se connecte fréquemment au serveur, car plus aucun mot de passe n'est demandé.

3.2.2 Implémentation

La majorité de l'implémentation se trouve dans le fichier */etc/ssh/sshd_config*.
Le serveur a été configuré respectant ces critères :

— installation de *openssh* ;

```
# Installation of OpenSSH.
apt-get install openssh-server -y
```

— changement de port et passage à la version 2 de SSH pour plus de sécurité ;

```
# Using port number 62000
Port 62000
# Using Protocol 2 of SSH.
Protocol 2
```

— ajout d'une bannière (disponible dans le fichier */etc/ssh-banner/banner*) ;

```
The debianThink server is for authorized personnel only.
WARNING! Access to this device is restricted to those
individuals with specific permissions. If you are not an
authorized user, disconnect now.  Any attempts to gain
unauthorized access will be prosecuted to the fullest
extent of the law.

All access and use may (not will) be monitored
and/or recorded.
```

— connexion en tant que **root** ;

```
# Privilege separation for security.
UsePrivilegeSeparation yes
```

— déconnexion après 120 secondes d'inactivité ;

```
# Deactivation of the login in root and disconnection
# after 120 seconds if no connections.
LoginGraceTime 120
PermitRootLogin no
StrictModes yes
```

— désactivation de la connexion par mot de passe, vu que l'authentification passe par les clés RSA.

```
# We deny the authentication by password.
PasswordAuthentication no
```

Ensuite, une génération et un chiffrement d'une paire de clés publique / privée sur la machine cliente a été nécessaire.

```
ssh-keygen -t rsa -b 4096 -C $email -f "/$USER/.ssh/id_rsa" \
-N ""
```

Une fois cela fait, la clé publique de celle-ci a été enregistrée sur le serveur dans le fichier */etc/ssh/ssh_host_rsa_key* afin d'accepter sa connection au serveur.

3.3 NFS

Le NFS (*Network File System*), est un protocole qui permet à un ordinateur d'accéder à des fichiers distants via un réseau.
Ce système de fichiers en réseau permet de partager des données principalement entre systèmes UNIX.

3.3.1 Constatation

Avant de commencer, il est à remarquer que, quelle que soit sa version, NFS est à déployer dans un réseau local et n'a pas de vocation à être ouvert sur Internet.
En effet, les données qui circulent sur le réseau ne sont pas chiffrées et les droits d'accès sont accordés en fonction de l'adresse IP du client qui peut être usurpée.

3.3.2 Configuration côté serveur

La totalité de l'implémentation se trouve dans le fichier */etc/exports*.

Voici les différentes étapes et options qui ont été effectuées :

— installation des différents services indispensables au NFS ;

```
# Installation of NFS.
apt-get install nfs-kernel-server nfs-common -y
```

— création du dossier de partage, et ajout de droits spécifiques ;

```
mkdir /srv/share
chmod 777 /srv/share
```

— activation du partage sur le réseau local et configuration dudit partage (autorise la lecture et l'écriture, retire les droit **root** à distance et désactivation de la vérification de sous-répertoires) ;

```
/srv/share  10.1.0.0/16(rw,no_subtree_check,root_squash)
```

— mises à jour de la tables des systèmes de fichiers partagés.

```
# Update the table of exported file systems.
exportfs -av
```

3.3.3 Configuration côté client

Sur le client, la configuration est similaire :

— installation des différents services indispensables au NFS ;

```
# Installation of NFS.
apt-get install nfs-common -y
```

— création du dossier de partage, et ajout de droits spécifiques ;

```
mkdir /mnt/share/users
chmod 777 /mnt/share/users
```

— installation d'AutoFS ;

```
# Installation of AutoFS.
apt-get install AutoFS
```

— configuration d'AutoFS

Contenu du fichier */etc/auto.master* :

```
/mnt/share    /etc/auto.nfs    --ghost,timeout=30
```

Contenu du fichier */etc/auto.nfs* :

```
users -noexec,nosuid,rw,ghost \
10.1.214.184:/srv/share/users
```

Remarque : l'adresse IP "10.1.214.184" étant celle du serveur NFS.

La configuration ci-dessus permet la création d'un point de montage lors de l'accès au répertoire.

3.4 Samba

Samba est un outil permettant de partager des dossiers et des imprimantes à travers un réseau local.

Son utilisation est conseillée pour partager de manière simple des ressources entre plusieurs ordinateurs.

Celui-ci est compatible avec les systèmes d'exploitation suivants : Windows, macOS, ainsi que des systèmes GNU/Linux, *BSD et Solaris dans lesquels une implémentation de Samba est installée.

3.4.1 Configuration

La configuration du serveur Samba se déroule en trois parties, mais tout d'abord, il est nécessaire de créer le dossier de partage et de lui donner les droits appropriés.

```
mkdir -p /srv/share/users/
chown -R root:users /srv/share/users/
chmod -R 775 /srv/share/users/
```

La totalité de l'implémentation se trouve dans le fichier */etc/samba/smb.conf*.

1. configuration de Samba (désignation du *workgroup*, choix du nom de *netbios*, etc.) ;

```
# Installation of Samba.
apt-get install libcups2 samba samba-common cups
# If you don't know the name of the workgroup
# run this command on the Windows client to get
# the workgroup name: net config workstation.
[global]
workgroup = WORKGROUP
server string = Samba Server %v
netbios name = debian
security = user
map to guest = bad user
dns proxy = no
```

2. configuration du partage pour le groupe « *users* » (désignation du chemin, des droits, etc.) ;

```
[users]
comment = All Users
path = /srv/share/users
valid users = @users
force group = users
create mask = 0660
directory mask = 0771
writable = yes
```

3. configuration du partage du dossier « *home* » des utilisateurs (désignation des droits, vérification de l'identité, etc.).

```
[homes]
comment = Home Directories
browseable = no
valid users = %S
writable = yes
create mask = 0700
directory mask = 0700
```

3.5 Quotas

Dans le but de mieux gérer l'espace personnel de chaque utilisateur, des quotas ont été mis en place sur la partition */home*.

À la création de chaque utilisateur, un quota avec une limite dure [5] de 500 Mo et une limite douce [6] de 400 Mo, lui sera attribué.

Remarque : lors du dépassement de la limite douce, l'utilisateur sera averti.

```
# Installation of quotatool, useful for scripts.
apt-get install -y quota quotatool

# Add this to /etc/fstab to the /home line.
usrquota,grpquota

fuser -k /dev/mapper/VolGroup-LVhome
# Create the file 'aquota.user' and aquota.group' and
# initialize all the partition that contains quotas.
quotacheck -cguvf /dev/mapper/VolGroup-LVhome
quotacheck -vagum

# Unmout the /home partition.
umount -l /dev/mapper/VolGroup-LVhome

# Activate quota.
quotaon -avug

# Mount the /home partition.
mount /dev/mapper/VolGroup-LVhome
```

5. Limite que nul ne peut dépasser.
6. Limite que l'utilisateur (ou groupe) peut dépasser pendant un certain laps de temps.

3.6 Base de données

Le serveur utilise MariaDB, un fork communautaire de MySQL édité sous licence GPL.

MySQL est un système de gestion de bases de données relationnelles. Il fait partie des logiciels de gestion de base de données les plus utilisés au monde, autant par le grand public que par des professionnels.

3.6.1 Mise en place

La totalité de l'implémentation se trouve dans le fichier */usr/bin/deepblue.sql*

La base de données a été installée et configurée sur le serveur en différentes étapes :

— installation de MariaDB par APT (*Advanced Package Tool*) ;

```
apt-get install -y mariadb-server
```

— configuration sécurisée de l'installation de MariaDB ;

```
mysql_secure_installation
```

— création de la base de données, nommée *deepblue* ;

```
CREATE DATABASE IF NOT EXISTS deepblue
CHARACTER SET 'utf8'
COLLATE utf8_general_ci;
```

— création de la table « *users* » contenant les différents utilisateurs.

```
USE deepblue;

CREATE TABLE IF NOT EXISTS users (
    id INT NOT NULL AUTO_INCREMENT,
    username VARCHAR(30) NOT NULL,
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    updated_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP,
    CONSTRAINT pk_users PRIMARY KEY(id)
) ENGINE=InnoDB;
```

3.7 Serveur Web

Pour la création du serveur Web, Apache a été utilisé.

3.7.1 Configuration côté serveur

La totalité de l'implémentation se trouve dans les fichiers
/etc/apache2/mods-available/mpm_prefork.conf
/etc/apache2/mods-available/mpm_event.conf

Voici les différentes étapes et options qui ont été effectuées :

— installation de la version 2 d'Apache ;

```
# Installation of Apache 2.
apt-get install -y apache2 apache2-doc apache2-utils
```

— configuration des modules multiprocessus (MPMs) ;

```
# prefork MPM.
<IfModule mpm_prefork_module>
        StartServers                4
        MinSpareServers             20
        MaxSpareServers             40
        MaxRequestWorkers           200
        MaxConnectionsPerChild      4500
</IfModule>
```

— désactivation du module d'évenement et activation de divers modules ;

```
# On Debian 8, the event module is enabled by default.
# This will need to be disabled, and the prefork
# module enabled.
a2dismod mpm_event
a2enmod mpm_prefork
a2enmod userdir
a2enmod rewrite
```

— configuration du module d'évenement ;

```
# event MPM.
<IfModule mpm_event_module>
        StartServers                2
        MinSpareServers             25
        MaxSpareServers             75
        ThreadLimit                 64
        ThreadsPerChild             25
        MaxRequestWorkers           150
        MaxConnectionsPerChild      3000
</IfModule>
```

— configuration du serveur Apache ;

```
# Disable the default Apache virtual host.
a2dissite 000-default.conf

# Creation of the Web folder.
mkdir -p /srv/www/example/www
```

— masquage de la version de PHP pour les utilisateurs ;

```
# Hide the version of PHP for users.
min_info
```

— installation du support PHP.

```
# Install PHP support.
apt-get install -y php5 php-pear
```

Remarque : les dossiers des sites Web ainsi que des logs sont créés lors de l'ajout d'un utilisateur.

3.8 FTP

Un serveur FTP (*File Transfer Protocol*), permet de transférer des fichiers par Internet ou par le biais d'un réseau informatique local (intranet). Pour ce serveur, il sera disponible au travers du réseau local.

3.8.1 Choix du serveur

Pour un maximum de sécurité, VsFTPd (*Very Secure FTP Daemon*) a été utilisé.
Ce serveur FTP est fortement axé sécurité : c'est l'un des premiers logiciels serveurs à mettre en œuvre la séparation des privilèges, minimisant ainsi les risques de piratage.

Dans sa configuration par défaut, VsFTPd est très restrictif :

— Seul le compte anonyme est autorisé à se connecter au serveur, et en lecture seule ;

— Les utilisateurs ne peuvent accéder qu'à leur compte.

3.8.2 Configuration

La totalité de l'implémentation se trouve dans les fichiers
/etc/vsftpd.conf
/etc/pam.d/vsftpd

Voici les différentes étapes et options qui ont été effectuées :

— installation de vsFTPd

```
1 # Installation of vsftpd.
2 apt-get install vsftpd -y
```

— choix du port et du monitoring

```
1 # Change the number of port to transmit:
2 listen_port=52152
3
4 # Basic monitoring
5 setproctitle_enable=YES
```

— configuration de vsFTPd ;

```
# Set vsftpd in standalone mode.
listen=YES

# Block the not allowed users.
anonymous_enable=NO

# Allow the local connections
local_enable=YES
write_enable=YES
local_umask=022

# Allow connection for guests users.
guest_enable=YES

# Default user for connections.
guest_username=apache

# Avoid local users go to /root.
chroot_local_user=YES

# Send virtual users into the default folder.
local_root=/srv/www/

# PAM manages the authentifications of the system.
# We can set a login and a password to all the systems.
pam_service_name=vsftpd

# Create a default folder for users.
user_config_dir=/etc/vsftpd/vsftpd_conf_users
```

— configuration de PAM ;

```
# Create the configuration file.
################ PAM VSFTPD CONFIGURATION ###############

# Authentification"
auth required /lib/x86_64-linux-gnu/security/pam_userdb.so
    db=/etc/vsftpd/login
account required /lib64/security/pam_userdb.so
    db=/etc/vsftpd/login
```

3.9 DNS

Le DNS (*Domain Name System*), est un service permettant de résoudre un nom de domaine.
De fait, les serveurs étant identifiés par leur adresse IP, il a fallu créer un processus afin d'associer leur adresse à un nom plus simple à retenir, le « nom de domaine ».

3.9.1 Sélection du DNS

Il a été choisi d'utiliser BIND9 (*Berkeley Internet Name Daemon*).
Celui-ci est le serveur DNS le plus utilisé sur Internet, spécialement sur les systèmes de type UNIX et est devenu de facto un standard.

3.9.2 Mise en place

La majorité de l'implémentation se trouve dans le fichier */etc/bind/named.conf.options*.

Le DNS a été installé et configuré sur le serveur en différentes étapes :

— installation de BIND9 ;

```
# Installation of bind9.
apt-get install bind9 bind9utils bind9-doc -y
```

— création des ACL (*Access Control List*) définissant le réseau local ;

```
acl goodclients {
  10.1.0.0/16;
  localhost;
  localnets;
};
```

— création et configuration du serveur DNS en lui-même :

- acceptation des requêtes uniquement pour le réseau interne ;

```
recursion yes;
allow-query { goodclients; };
```

- configuration des forwarders ;

```
forwarders {
  8.8.8.8;
  8.8.4.4;
};
forward only;
```

- activation de *DNSSEC* qui sécurise les données envoyées par le DNS ;

```
dnssec-enable yes;
dnssec-validation yes;
```

- implémentation de la RFC1035[7][8].

```
# Conform to RFC1035
auth-nxdomain no;
listen-on-v6 { any; };
```

7. http://abcdrfc.free.fr/rfc-vf/rfc1035.html
8. http://www.bortzmeyer.org/1035.html

3.10 iptables

iptables permet de configurer les règles du pare-feu en IPv4.

3.10.1 Écriture du script

Le script est */bin/script/iptables/iptables-conf.sh*.

Voici comment il est structuré :

— *suppression des règles par défaut*

```
# Flushing all rules from all tables.
iptables -F ; iptables -X
iptables -t nat -F ; iptables -t nat -X
iptables -t mangle -F ; iptables -t mangle -X
iptables -t raw -F ; iptables -t raw -X
```

— mise en place de règles par défaut

```
# Setting default filter policy.
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP

# Allow loopback access.
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

— acceptation des différents services tels que les *ping*, le *DNS*, *HTTP(S)*, *NTP*, *NFS*, *Samba* et *SSH*. Voici la configuration du DNS :

```
# Allow DNS (53)
iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT
iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT
```

3.11 SELinux

SELinux (*Security-Enhanced Linux*) permet de définir des politiques d'accès à différents éléments du système d'exploitation. Ces éléments peuvent être des processus (*démons*), ou encore des fichiers.

Références

[1] ASTUCES-INFO.COM. Debian : Ajouter des quotas sur le disque dur, Site, [en ligne]. https ://www.astuces-info.com, (consulté le 23 mai 2017).

[2] COUTAREL, J. Installation du serveur Web Apache sur un serveur dédié Kimsufi sous Ubuntu Server 14.04 LTS, Site, [en ligne]. https ://justincoutarel.fr, (consulté le 17 mai 2017).

[3] DUCEA, M. Apache Tips & Tricks : Hide Apache Software Version, Site, [en ligne]. http ://www.ducea.com, (consulté le 17 mai 2017).

[4] GELBMANN, M. Ubuntu became the most popular Linux distribution for web servers, Site, [en ligne]. http ://www.w3techs.com, (consulté le 15 février 2017).

[5] KROUT, E. Apache Web Server on Debian 8 (Jessie), Site, [en ligne]. https ://www.linode.com, (consulté le 17 mai 2017).

[6] LA COMMUNAUTÉ DE WIKIPÉDIA. MariaDB, Site, [en ligne]. https ://fr.wikipedia.org, (consulté le 23 mai 2017).

[7] LA COMMUNAUTÉ DE WIKIPÉDIA. Network File System, Site, [en ligne]. https ://fr.wikipedia.org, (consulté le 23 mai 2017).

[8] LA COMMUNAUTÉ DE WIKIPÉDIA. Samba (informatique), Site, [en ligne]. https ://fr.wikipedia.org, (consulté le 23 mai 2017).

[9] LA COMMUNAUTÉ DE WIKIPÉDIA. Secure Shell, Site, [en ligne]. https ://fr.wikipedia.org, (consulté le 23 mai 2017).

[10] LA COMMUNAUTÉ DE WIKIPÉDIA. BIND, Site, [en ligne]. https ://fr.wikipedia.org, (consulté le 27 mai 2017).

[11] LA COMMUNAUTÉ DE WIKIPÉDIA. Domain Name System, Site, [en ligne]. https ://fr.wikipedia.org, (consulté le 27 mai 2017).

[12] LA COMMUNAUTÉ DE WIKIPÉDIA. Serveur FTP, Site, [en ligne]. https ://fr.wikipedia.org, (consulté le 27 mai 2017).

[13] LA COMMUNAUTÉ DE WIKIPÉDIA. VsFTPd, Site, [en ligne]. https ://fr.wikipedia.org, (consulté le 27 mai 2017).

[14] LaTeX. A document preparation system. (consulté le 15 février 2017).

[15] MEUH. NTP - Clock is not syncing to low stratum server, Site, [en ligne]. http ://stackoverflow.com, (consulté le 28 mars 2017).

[16] RUCHI. NTP Server and Client Configuration in debian, Site, [en ligne]. http ://www.debianadmin.com, (consulté le 23 mars 2017).

[17] SVERDLOV, E. How To Create a New User and Grant Permissions in MySQL, Site, [en ligne]. https ://www.digitalocean.com, (consulté le 23 mai 2017).

[18] THE DEBIAN COMMUNITY. NTP, Site, [en ligne]. https ://wiki.debian.org/NTP, (consulté le 23 mars 2017).

[19] THE DEBIAN SUPPORT. Configuration serveur NTP, Site, [en ligne]. https ://www.debian-fr.org, (consulté le 23 mars 2017).