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

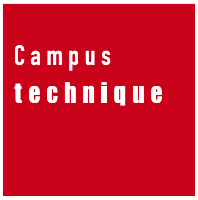
2ème Bachelier en Informatique

Projet Linux

Auteur :
Terencio Agozzino

Auteur :
Alexandre Ducobu

Enseignants :
Antoine Malaise
Julien De Bodt



Année académique 2016 - 2017

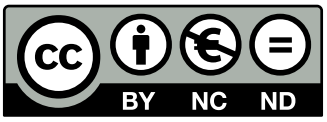


Table des matières

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** permettra aux utilisateurs Windows d'accéder à ce même partage ;
- un serveur **Web**, **FTP**, **MySQL** et **DNS** qui permettra un hébergement multi-utilisateurs ;
  - le FTP permettra à chaque utilisateur d'accéder à son dossier Web ;
  - il faudra créer une zone dans le DNS pour nos sites ;
  - le DNS fera également office de DNS cache pour le réseau local ;
- un **serveur de temps** pour que les machines du réseau local puissent se synchroniser ;
- une connexion en **SSH** au serveur.

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 changements sur le serveur ;

— le contrôle du bon fonctionnement de chaque élément.

1.3 Sécurité

Du côté de la sécurité, nous avons quelques contraintes reprises ci-dessous :

— 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

Notre 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 : nous savons que 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 matérielles.

— 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. Le système de paquets de Debian est l'outil central de mise à jour, installation, suppression et recherche de paquets.

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

À titre d'information, depuis mai 2016, Ubuntu a les mêmes parts de marché que Debian.

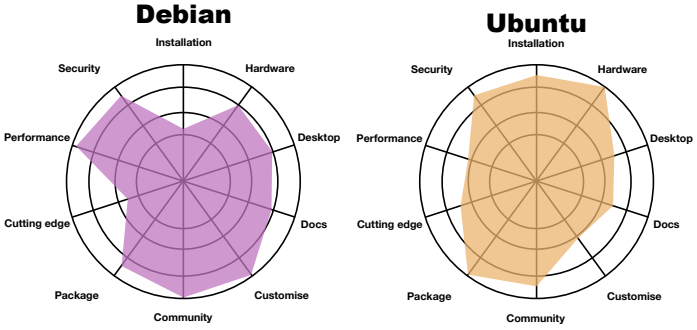


FIGURE 1 – Différences entre Debian et Ubuntu

Nous n'avons pas choisi Ubuntu pour les raisons suivantes :

— C'est un dérivé de Debian : de ce fait, un administrateur sachant configurer un serveur Debian pourra faciliter s'adapter au serveur Ubuntu.

— Il vise le grand public et, de ce fait, est beaucoup moins utilisé dans le milieu professionnel.

— Celui-ci est 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, lui, est en chute libre.

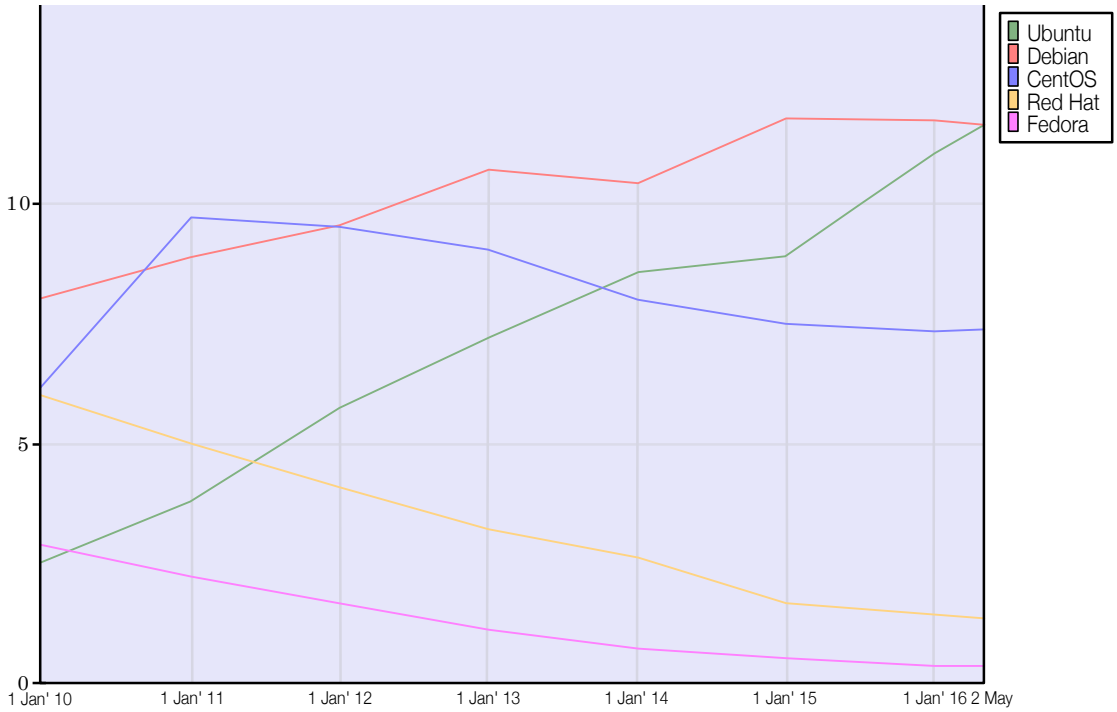


FIGURE 2 – Parts de marché des distributions Linux

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) 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

Afin de posséder assez d'espace de stockage, nous avons choisi d'utiliser deux disques de 20 Go en RAID 1.
Nous avons alors partitionné le disque de cette manière, avec un partition racine, */boot*, et un groupe de volume LVM nommé *VolGroup* :

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

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

3 Services

3.1 NTP

Le **NTP**, ou ***Network Time Protocol***, est le protocole que nous avons utilisé afin de synchroniser les machines du reseau local avec l'horloge du serveur.

Principe

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

Chaque machine peut être à la fois serveur et client.
Elle 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 sources les plus précises *(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.

Configuration du serveur

Voici les différentes étapes et options que nous avons 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.

Configuration du client

Sur le client, la configuration est beaucoup plus simple :

- activation des statistiques NTP ;
- ajout du serveur local.

3.2 SSH

Le **SSH**, ou ***Secure Shell***, est un protocole de communication sécurisé. Il impose un échange de clés de chiffrement en début de connexion.

Type d'authentification

Il y a plusieurs façons de s'authentifier sur le serveur via SSH.
Les deux plus utilisées sont :

— l'authentification par mot de passe ;

— l'authentification par clés publique et privée du client.

Nous avons décidé de mettre en place une **identification automatique par clés**. Ainsi on évite d'entrer le mot de passe à chaque connexion à distance.
Cette méthode est plus complexe à mettre en place, mais elle surtout plus pratique.

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

Implémentation

Tout d'abord, nous avons configuré le serveur :

- installation de *openssh* ;
- changement de port et passage à la version 2 de SSH pour plus de sécurité ;
- ajout d'une bannière ;
- désactivation de la connexion en tant que **root** ;
- déconnexion après 120 secondes d'inactivité ;
- désactivation de la connexion par mot de passe, vu que l'authentification passe par les clés RSA.

Ensuite, il nous a fallu générer et chiffrer une paire de clés publique / privée sur la machine client.
Une fois cela fait, la clé publique a été enregistrée sur le serveur afin de l'accepter dans le futur.

3.3 NFS

Le **NFS**, ou ***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.

Constatation

Avant de commencer, il est à remarquer que, quelle que soit sa version, NFS est a 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)*.

Configuration côté serveur

Voici les différentes étapes et options que nous avons effectuées :

- installation des différents services indispensables au NFS ;
- création du dossier de partage, et ajout de droits spécifiques ;
- activation du partage sur le réseau local et configuration dudit partage *(autorise la lecture et l'écriture, retire les droit* ***root*** *à distance et et désactivation de la vérification de sous-répertoires)* ;
- mise à jour de la tables des systèmes de fichiers partagés.

Configuration côté client

Sur le client, la configuration est similaire :

- installation des différents services indispensables au NFS ;
- création du dossier de partage, et ajout de droits spécifiques ;
- installation d'*AutoFS* ;
- configuration d'AutoFS *(création d'un point de montage lors de l'accès au répertoire, durée d'activité après le dernier accès au dossier partagé ⇒ au moins 30 secondes pour un partage samba, etc.)*.

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
Il 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.

Configuration

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

1. configuration de Samba *(désignation du* ***workgroup****, choix du nom de* ***netbios****, etc.)* ;
2. configuration du partage pour le groupe « *users* » *(désignation du chemin, des droits, etc.)* ;
3. configuration du partage du dossier « *home* » des utilisateurs *(désignation des droits, vérification de l'identité, etc.)* ;

3.5 Base de données

MariaDB est 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.

Mise en place

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

- installation de MariaDB par **APT** ***(Advanced Package Tool)*** ;
- configuration sécurisée de l'installation de MariaDB ;
- création de la base de données, nommée *deepblue* ;
- création de la table « *users* » contenant les différents utilisateurs.

Remarque : le mot de passe de la base de données est formé de 10 caractères et est composé de lettres *(majuscules et minuscules)* et de chiffres, dans le but d'éviter les attaques par force brute et/ou par dictionnaire.

3.6 Serveur Web

3.7 FTP

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

Choix du serveur

Pour un maximum de sécurité, notre choix s'est porté sur **vsFTPd**, ou ***Very Secure FTP Daemon***.
Ce serveur FTP est fortement axé sécurité : c'est l'un des premiers logiciels serveurs à mettre en uvre 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.

Configuration

À terminer

3.8 DNS

Le **DNS**, ou ***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* ».

Sélection du DNS

Nous avons choisi d'utiliser **BIND**, pour ***Berkeley Internet Name Daemon***.
C'est *le* serveur DNS le plus utilisé sur Internet, spécialement sur les systèmes de type UNIX et est devenu de facto un standard.

Mise en place

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

- installation de BIND9 ;
- création des ACL *(**Access Control List**)* définissant le réseau local ;
- création et configuration du serveur DNS en lui-même :
  - acceptation des requêtes uniquement pour le réseau interne ;
  - configuration des forwarders ;
  - activation de ***DNSSEC*** qui sécurise les données envoyées par le DNS ;
  - activation de l'écoute des requêtes IPv6 ;
  - implémentation de la RFC1035 [1] [2].

1. `http://abcdrfc.free.fr/rfc-vf/rfc1035.html`
2. `http://www.bortzmeyer.org/1035.html`

Gestion

4 Sauvegardes

Dans le milieu de l'entreprise, deux types de sauvegarde sont utilisées : incrémentielle et différentielle.

La méthode de sauvegarde choisie est la différentielle, afin de restaurer les données plus rapidement par rapport à la sauvegarde incrémentielle. De plus, cette méthode est plus fiable, car seule la sauvegarde complète est nécessaire pour reconstituer les données sauvegardées.

Il est à remarqué que la sauvegarde incrémentielle est plus économe en terme de stockage.

Pour terminer, nous prévoyons d'effectuer une sauvegarde complète une fois toutes les semaines.

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).