Installation d’un serveur Linux sur un Raspberry

Stéphane Apiou

Version 0.9, 2020-04-20

Table of Contents

Chapter 1. Avant propos

Ce document est disponible sur le site ReadTheDocs et sur Github.

Cette documentation décrit la méthode que j'ai utilisé pour installer une homebox (site auto hébergé) avec un raspberry PI Elle est le résultat de très nombreuses heures de travail pour collecter la documentation nécessaire. Sur mon serveur, j'ai installé un Linux Debian 10. Cette documentation est facilement transposable pour des versions différentes de Debian.

Dans ce document, je montre la configuration de nombreux types de sites web et services dans un domaine en utilisant ISPConfig.

Sont installés:

- un panel ISPConfig
- un configurateur Webmin
- un serveur apache avec sa configuration let's encrypt et les plugins PHP, python et ruby
- un serveur de mail avec antispam, sécurisation d'envoi des mails et autoconfiguration pour Outlook, Thunderbird, Android.
- un webmail roundcube,
- un serveur de mailing list mailman,
- un serveur ftp et sftp sécurisé.
- un serveur de base de données et son interface web d'administration phpmyadmin.
- des outils de sécurisation, de mise à jour automatique et d'audit du serveur
- un outil de Monitoring Munin
- un outil de Monitoring Monit
- un sous domaine pointant sur un site auto-hébergé (l'installation du site n'est pas décrite ici; Se référer à Yunohost),
- un site CMS sous Joomla,
- un site CMS sous Concrete5,
- un site WIKI sous Mediawiki,
- un site Wordpress,
- un site Microweber,
- un site Photo sous Piwigo,
- un site Collaboratif sous Nextcloud,
- un site Gitea et son repository GIT,
- un serveur et un site de partage de fichiers Seafile,
- un serveur Grafana, Prometheus, Loki, Promtail pour gérer les statistiques et les logs du serveur,
- un serveur de sauvegardes Borg

- un serveur de VPN Pritunl,

Dans ce document nous configurons un nom de domaine principal. Pour la clarté du texte, il sera nommé "example.com". Il est à remplacer évidemment par votre nom de domaine principal.

Je suppose dans ce document que vous savez vous connecter à distance sur un serveur en mode terminal, que vous savez vous servir de `ssh` pour Linux ou de `putty` pour Windows, que vous avez des notions élémentaires de Shell Unix et que vous savez vous servir de l'éditeur `vi`. Si `vi` est trop compliqué pour vous, je vous suggère d'utiliser l'éditeur de commande `nano` à la place et de remplacer `vi` par `nano` dans toutes les lignes de commande.

Dans le document, on peut trouver des textes entourés de <texte>. Cela signifie que vous devez mettre ici votre propre texte selon vos préférences.

A propos des mots de passe: il est conseillé de saisir des mots de passe de 10 caractères contenant des majuscules/minuscules/nombres/caractères spéciaux. Une autre façon de faire est de saisir de longues phrases. Par exemple: 'J'aime manger de la mousse au chocolat parfumée à la menthe'. Ce dernier exemple a un taux de complexité est bien meilleur que les mots de passe classiques. Il est aussi plus facile à retenir que 'Az3~1ym_a&'.

Le coût pour mettre en oeuvre ce type de serveur est relativement faible:

- Compter 15-18€TTC/an pour un nom de domaine classique (mais il peut y avoir des promos)
- Comptez 26€ pour acheter une carte Raspberry PI 3 A+ (1Go de Ram) et 61€ pour un PI 4 avec 4Go de Ram. A cela il faut ajouter un boitier, une alim et une flash de 64 ou 128 Go (prenez les cartes SD les plus rapide possible en écriture). Vous en aurez donc pour 110€ si vous achetez tout le kit.

Par rapport à une solution VPS directement dans le cloud, ce budget correspond à 7 mois d'abonnement.

Chapter 2. Choix du registrar

Pour rappel, un registrar est une société auprès de laquelle vous pourrez acheter un nom de domaine sur une durée déterminée. Vous devrez fournir pour votre enregistrement un ensemble de données personnelles qui permettront de vous identifier en tant que propriétaire de ce nom de domaine.

Pour ma part j'ai choisi Gandi car il ne sont pas très cher et leur interface d'administration est simple d'usage. Vous pouvez très bien prendre aussi vos DNS chez OVH.

Une fois votre domaine enregistré et votre compte créé vous pouvez vous loguer sur la plateforme de gestion de Gandi.

Allez dans Nom de domaine et sélectionnez le nom de domaine que vous voulez administrer. La vue générale vous montre les services actifs. Il faut une fois la configuration des DNS effectuée être dans le mode suivant:

- Serveurs de noms: Externes
- Emails: Inactif
- DNSSEC: Actif (cela sera activé dans une seconde étape de ce guide)

Vous ne devez avoir aucune boite mail active sur ce domaine. A regardez dans le menu "Boites & redirections Mails". Vous devez reconfigurer les 'Enregistrements DNS' en mode externes. Dans le menu "serveurs de noms", vous devez configurer les serveurs de noms externe. Mettre 3 DNS:

- le nom de votre machine OVH: VPSxxxxxx.ovh.net
- et deux DNS de votre domaine: ns1.<example.com> et ns2.<example.com>

Pour que tout cela fonctionne bien, ajoutez des Glue records:

- un pour ns1.<example.com> lié à l'adresse <IP> du serveur OVH
- un pour ns2.<example.com> lié à l'adresse <IP> du serveur OVH

Il y a la possibilité chez OVH d'utiliser un DNS secondaire. Je ne l'ai pas mis en oeuvre.

Avoir un DNS sur au moins deux machines distinctes est la configuration recommandée.

Le menu restant est associé à DNSSEC; nous y reviendrons plus tard.

Chapter 3. Installation du linux sur votre raspberry.

C'est la première étape.

Il vous faudra un lecteur de flash microSD - USB que vous brancherez sur votre PC.

Il existe maintenant un outil nommé Rasberry PI Imager pour la plateforme qui vous convient. C'est le moyen de plus simple de flasher votre raspberry.

Pour Windows, très simple, il suffit de lancer le programme téléchargé. Pour Linux, appliquer la procédure suivante:

1. Loguez vous comme root
2. Tapez:

```
cd /tmp
wget https://downloads.raspberrypi.org/imager/imager_amd64.deb
dpkg -i imager_amd64.deb
```

3. Lancez le programme.

Suivez la procédure ci dessous commune à toutes les plateformes:

1. Sélectionnez `Choose OS` et dans la liste choisissez `Raspbian`
2. Sélectionnez `CHoose SD CARD` et sélectionnez votre lecteur de carte SD
3. Cliquez sur `Write`
4. Attendez la fin du chargement et de l'écriture sur la flash.
5. Vous avez deux façons d'installer:
   - avec un écran et un clavier qui est la méthode la plus facile
   - en mode Headless qui est plus complexe mais ne nécessite pas d'écran ni de clavier
6. Vous devez choisir l'une des méthodes décrites dans les deux chapitres suivants.

3.1. Installation avec écran et clavier

Pour ce type d'installation, il vous faut un clavier+souris et un écran.

1. Enlevez la carte SD de votre lecteur et insérez la dans votre raspberry PI.
2. Brancher un clavier, une souris et un écran (ou utilisez un écran 3,5" configuré selon la procédure en annexe).
3. Branchez votre Raspberry sur votre réseau Ethernet filaire (vous pouvez aussi utiliser le wifi)
4. Démarrez votre Raspberry.

5. Après l'écran de démarrage arc en ciel, vous devez assez rapidement arriver sur le bureau
6. Un programme doit se lancer automatiquement.
7. Sélectionnez le clavier et la langue en français
8. Tapez votre nouveau mot de passe pour le login `pi`
9. Choisissez un full screen sans bords
10. Choisissez votre connexion wifi et entrez le mot de passe
11. Bien noter votre adresse IP elle vous sera utile ensuite
12. Les mises à jours de paquets Debian ainsi que l'installation des traductions en français vont s'installer.
13. Une fois les installations terminées, le Raspberry va rebooter.
14. Une fois rebooté, sélectionnez dans le menu `Préférences` → `Configuration du Raspberry PI`
    - Dans l'onglet `Display` Cliquez sur `Set Resolution` et choisissez `31: 1920x1080`
    - Dans l'onglet `Interfaces` activez `SSH` et `VNC`
    - Cliquez sur `Valider`
15. Cliquez sur l'icône `VNC` dans la barre en haut à Droite
    - Dans la fenêtre cliquez sur le menu burger en haut à Droite.
    - Choisissez `Options` puis l'onglet `Sécurité`
    - Dans le champ Authentification choisissez l'option `mot de passe VNC`
    - Tapez votre mot de passe dans les deux champs et cliquez `Valider` puis `OK`
16. Vous pouvez maintenant rebooter votre Raspberry sans écran et sans clavier pour continuer la configuration.
17. Vous avez deux options: connexion en mode SSH ou au travers d'une connexion VNC

3.2. Installation Headless

Pour ce type d'installation, pas besoin d'écran et de clavier et de souris. Tout s'effectue à distance.

Dans la suite, je suppose que vous possèdez un PC fonctionnant avec un Linux (la procédure peut être adaptée avec une machine windows en utilisant la ligne de commande et putty)

1. Avant d'enlever votre flash SD du lecteur, appliquez la procédure ci après:
    - Sur la flash, 2 partitions ont été crées. Montez la partition boot
    - sur cette partition, créez un fichier `wpa_supplicant.conf` et éditez le avec un éditeur de text (Nano ou vi sous linux ou Notepad sous windows).
    - Mettez y le texte suivant:

```
ctrl_interface=DIR=/var/run/wpa_supplicant GROUP=netdev
update_config=1
country=US
network={
    ssid="YOURSSID" ①
    psk="YOURPASSWORD" ②
    key_mgmt=WPA-PSK
    scan_ssid=1
}
```

① remplacez `YOURSSID` par le nom SSID de votre wifi local

② remplacez `YOURPASSWORD` par le mot de passe de votre wifi local

- sauvez le fichier
- Sur la même partition créez un fichier `ssh` (vide et sans extension). Il servira à indiquer au raspberry d'activer ssh au prochain boot
- démontez la partition
- au boot sur la carte SD, le fichier sera recopié dans votre configuration et le réseau wifi sera ainsi accessible

2. Enlevez la carte SD de votre lecteur et insérez la dans votre Raspberry PI.
3. Démarrez votre raspberry.
4. Attendez environ 2 minutes le temps que le premier boot se termine. Tout pendant la procédure de boot, la petite led d'accès disque doit clignoter.
5. Vous devez maintenant découvrir l'adresse IP de votre Raspberry, pour cela tapez la commande suivante:

```
ping raspberrypi.local
```

6. Si le Raspberry a démarré correctement, cette commande doit montrer l'adresse IP du raspberry et une réponse correcte au ping

```
PING raspberrypi.local (192.168.3.212) 56(84) bytes of data.
64 bytes from raspberrypi.local (192.168.0.212): icmp_seq=1 ttl=64 time=1.32 ms
```

1. Si vous n'obtenez aucun résultat essayer la commande `nmap` sur le subnet de votre réseau local
   - On obtient l'adresse local du subnet en tapant:

```
hostname -I
```

   - l'adresse IP de votre PC est affichée comme premier mot. Par exemple :`192.168.3.10`
   - le subnet se déduit de cette adresse en gardant les 3 premiers nombres (cas général de la

plupart des utilisateurs).

- Tapez:

```
nmap -sn 192.168.3.0/24
```

- la commande affiche alors les adresses IP et mac de toutes les machines présentes sur le réseau.
- le Raspberry se reconnait par son nom de machine qui contient le terme `raspberry` ou par son adresse mac qui est reconnue du type `Raspberry Pi Foundation`

2. vous pouvez alors directement vous connecter. Tapez:

```
ssh pi@adresse_ip ①
```

① adresse_ip est l'adresse IP du Raspberry pi découverte précédemment ou raspberrypi.local

3. Se loguer avec le mot de passe `raspberry`
4. Tapez :

```
sudo raspi-config
```

5. Choisissez `1 Change User Password` → tapez votre nouveau mot de passe 2 fois
6. Sur l'étape suivante, il ne faut pas se louper ou vous serez obligé d'éteindre votre raspberry, retirer la flash et la reprogrammer avec le fichier `wpa_supplicant.conf` dans la partition `boot`
7. Choisissez `2 Network Options` → `N2 Wi-fi` → Tapez votre nom de SSID (attention aux majuscules) → Tapez votre mot de passe
8. Choisissez `4 Localisation Options` → `I1 Change Locale` → Sélectionnez votre langue: `fr_FR.UTF-8 UTF-8` → puis la locale par défaut `fr_FR.UTF-8 UTF-8`
9. Choisissez `4 Localisation Options` → `I2 Change Timezone` → Choisissez votre timezone (par exemple: `Europe` → `Paris`)
10. Choisissez `4 Localisation Options` → `I3 Change Keyboard Layout` → Choisissez votre mapping clavier
11. Choisissez `4 Localisation Options` → `I4 Change Wi-fi Country` → choisissez votre pays de norme wifi
12. choisissez `5 Interfacing Options` → `P2 SSH` → choisissez `yes`
13. choisissez `5 Interfacing Options` → `P3 VNC` → choisissez `yes`
14. choisissez `7 Advanced Options` → `A5 Resolution` → choisissez `DMT Mode 82 1920x1080 60Hz 16:9`
15. choisissez `8 Update` ; Une mise a jour du système va s'effectuer
16. Tapez ensuite 2 fois sur la touche `TAB` pour sélectionner `Finish`. Tapez `entrée`.
17. Rebootez le système en tapant:

```
sudo reboot
```

18. Vous allez perdre votre connexion avec le raspberry
19. si vous arrivez à vous reloguer en tapant (attendre 30 secondes après le reboot avant d'essayer):

```
ssh pi@adresse_ip ①
```

① adresse_ip est l'adresse IP du Raspberry pi découverte précédemment ou raspberrypi.local

C'est que vous avez terminé avec succès la configuration initiale.

20. RealVNC dans sa configuration par défaut ne permet pas à un utilisateur de se connecter simplement. Il faut donc ruser la première fois.
21. Dans un autre terminal sur votre poste local, tapez:

```
apt install realvnc-vnc-viewer
vncviewer adresse_ip:5900 ①
```

① adresse_ip est l'adresse IP du Raspberry pi découverte précédemment ou raspberrypi.local

22. Une demande de login et de mot de passe est affiché tapez `pi` dans le login et le mot de passe que vous avez choisi dans le champ mot de passe. Cliquez sur `OK`
23. le bureau va s'afficher et un programme se lance automatiquement. Arrêter ce programme puisque vous avez déjà fait la configuration initiale.
24. Cliquez sur l'icone `VNC` dans la barre en haut à Droite
    - Dans la fenêtre cliquez sur le menu burger en haut à Droite.
    - Choisissez `Options` puis l'onglet `Sécurité`
    - Dans le champ Authentification choisissez l'option `mot de passe VNC`
    - Tapez votre mot de passe dans les deux champs et cliquez `Valider` puis `OK`
25. Vous avez terminé l'installation initiale de Raspbian. Vous pouvez maintenant rebooter votre raspberry pour continuer la configuration.
26. Vous avez deux options: connexion en mode SSH ou au travers d'une connection VNC

Chapter 4. Se loguer root sur le serveur

A de nombreux endroit dans la documentation, il est demandé de se loguer root sur le serveur. Pour se loguer root, et dans l'hypothèse que vous avez mis en place un compte sudo:

1. De votre machine locale, loguez vous avec votre compte `<sudo_username>`. Tapez :

   ```
   ssh <sudo_username>@<example.com> ①
   ```

   ① Mettez ici <sudo_username> par votre nom de login et <example.com> par votre nom de domaine. Au début votre nom de domaine acheté n'est pas encore configuré. Il faut donc utiliser le nom de machine (par exemple pour un VPS OVH: VPSxxxxxx.ovh.net) ou votre adresse IP.

   ou utilisez putty si vous êtes sous Windows.

2. Tapez votre mot de passe s'il est demandé. Si vous avez installé une clé de connexion ce ne devrait pas être le cas.
3. Loguez-vous `root`. Tapez :

   ```
   sudo bash
   ```

   Un mot de passe vous est demandé. Tapez le mot de passe demandé.

4. Dans le cas contraire (pas de sudo créé et connexion en root directe sur le serveur):
   a. Se loguer root sur le serveur distant. Tapez:

      ```
      ssh root@<example.com> ①
      ```

      ① remplacer ici <example.com> par votre nom de domaine.

      Tapez ensuite votre mot de passe root

Chapter 5. Configuration basique

5.1. Mettre l'éditeur de votre choix

En fonction de vos préférences en terme d'éditeur, choisissez celui qui vous convient pour les outils utilisant un éditeur de façon automatique tels que `crontab`.

Pour les débutants, il est conseillé d'utiliser nano.

Loguez vous comme root et tapez:

```
update-alternatives  --config editor
```

5.2. Installation d'un repository pour `/etc`

Si vous souhaitez gérer en gestion de configuration le contenu de votre répertoire `/etc`, installez `etckeeper`.

Cette installation est optionnelle.

1. Loguez vous comme root sur le serveur
2. Tapez :

   ```
   apt update
   apt install etckeeper
   ```

3. Vous pouvez créer un repository privé dans le cloud pour stocker votre configuration de serveur (autre serveur privé de confiance ou repository privé `Gitlab` ou `Github`).
4. Ajoutez ce repository distant. Pour `Gitlab` et `Github`, une fois le repository créé, demandez l'affichage de la commande git pour une communication en ssh. Tapez ensuite sur votre serveur :

   ```
   cd /etc
   git remote add origin git@github.com:username/etc_keeper.git ①
   ```

   ① remplacer l'url par celle qui correspond au chemin de votre repository

5. modifier le fichier de configuration de `etckeeper`. tapez:

   ```
   vi /etc/etckeeper/etckeeper.conf
   ```

6. Recherchez la ligne contenant `PUSH_REMOTE` et ajoutez y tous les repositories distant sur lesquels vous souhaitez pousser les modifications. Pour notre configuration, mettez:

```
PUSH_REMOTE="origin"
```

7. Pour éviter demandes de mot de passe de la part de `github` ou `gitlab`, il est nécessaire de déclarer une clé publique sur leur site. Créez une clé sur votre serveur pour l'utilisateur root:
   a. Créer un répertoire `/root/.ssh` s'il n'existe pas. tapez :

   ```
   cd /root
   mkdir -p .ssh
   ```

   b. Allez dans le répertoire. Tapez :

   ```
   cd /root/.ssh
   ```

   c. Générez vous clés. Tapez :

   ```
   ssh-keygen -t rsa
   ```

   d. Un ensemble de questions apparaît. Si un texte vous explique que le fichier existe déjà, arrêtez la procédure. Cela signifie que vous avez déjà créé une clé et que vous risquez de perdre la connexion à d'autres serveurs si vous en générez une nouvelle. Sinon, appuyez sur Entrée à chaque fois pour accepter les valeurs par défaut.

   e. Allez sur `gitlab` ou `github` dans la rubriques "settings" et le menu "SSH keys". Ajoutez la clé que vous aurez affiché avec la commande suivante:

   ```
   cat /root/.ssh/id_rsa.pub
   ```

8. Effectuez un premier push. Tapez:

```
cd /etc
git push -u origin master
```

9. aucun mot de passe ne doit vous être demandé. Si ce n'est pas le cas, re-vérifier les étapes précédentes.
10. Lancer `etckeeper`. Tapez:

```
etckeeper commit
```

11. Tout le contenu de `/etc` est poussé sur le repository. Saisissez un commentaire.
12. C'est fait !

5.3. Mise à jour des sources de paquets Debian

1. Loguez vous comme root sur le serveur
2. Modifier la liste standard de paquets
   a. Éditer le fichier `/etc/apt/sources.list`. Tapez:

   ```
   vi /etc/apt/sources.list
   ```

   b. Dé-commenter les lignes débutant par `deb` et contenant le terme `backports`. Par exemple pour `#deb http://deb.debian.org/debian buster-backports main contrib non-free` enlever le # en début de ligne
   c. Ajouter sur toutes les lignes les paquets `contrib` et `non-free` . en ajoutant ces textes après chaque mot `main` du fichier `source.list`
   d. Le fichier doit ressembler à ceci:

   ```
   deb http://raspbian.raspberrypi.org/raspbian/ buster main contrib non-free rpi
   # Uncomment line below then 'apt-get update' to enable 'apt-get source'
   #deb-src http://raspbian.raspberrypi.org/raspbian/ buster main contrib non-free
   rpi
   ```

3. Effectuer une mise à niveau du système
   a. Mettez à jour la liste des paquets. Tapez:

   ```
   apt update
   ```

   b. Installez les nouveautés. Tapez:

   ```
   apt dist-upgrade
   ```

4. Effectuez du ménage. Tapez:

   ```
   apt autoremove
   ```

5.4. Installation des paquets de base

1. Loguez vous comme root sur le serveur
2. Tapez:

```
apt install curl wget ntpdate apt-transport-https apt-listchanges apt-file apt-
rdepends man
```

5.5. Installer l'outil Debfoster

L'outil `debfoster` permet de ne conserver que les paquets essentiels.

Cette installation est optionnelle.

Il maintient un fichier `keepers` présent dans `/var/lib/debfoster`

En répondant aux questions de conservations de paquets, `debfoster` maintient la liste des paquets uniques nécessaires au système. Tous les autres paquets seront supprimés.

1. Loguez vous comme root sur le serveur
2. Ajouter le paquet `debfoster`. Tapez :

   ```
   apt install debfoster
   ```

3. Lancez `debfoster`. Tapez :

   ```
   debfoster
   ```

4. Répondez au questions pour chaque paquet
5. Acceptez la liste des modifications proposées à la fin. Les paquets superflus seront supprimés

Ci dessous une petite liste de paquets à conserver sur une installation basique:

alacarte	apparmor	apt-listchanges	arandr
avahi-daemon	binutils-arm-linux-gnueabihf	blueman	bluetooth
cifs-utils	console-setup	debconf-utils	debfoster
debian-reference-en	dphys-swapfile	ed	etckeeper
ethtool	fake-hwclock	fbset	ffmpeg
firmware-atheros	firmware-brcm80211	firmware-libertas	firmware-misc-nonfree
firmware-realtek	gldriver-test	hardlink	htop
hunspell-en-gb	hunspell-fr	hyphen-en-gb	hyphen-fr
keyutils	locales	lxde	mythes-fr
ncdu	omxplayer	pi-package	piclone
piwiz	pkg-config	python-pip	qpdfview

raspberrypi-net-mods	raspberrypi-ui-mods	raspi-copies-and-fills	read-edid
realvnc-vnc-server	realvnc-vnc-viewer	rng-tools	rp-prefapps
rpi-update	rsync	ssh	ssh-import-id
strace	sudo	tree	ttf-bitstream-vera
usb-modeswitch	usbutils	v4l-utils	vl805fw
wamerican	wfrench	wireless-tools	wpasupplicant
xcompmgr	xfonts-100dpi	xinit	xml-core
xsel	xserver-xorg-video-fbdev	zip	

5.6. Création d'un fichier keeper dans /etc

Vous pourriez être intéressé après l'installation de `debfoster` et de `etckeeper` de construire automatiquement un fichier qui contient la liste des paquets qui permettent de réinstaller le système:

1. Loguez vous comme root sur le serveur
2. Tapez:

```
vi /etc/etckeeper/pre-commit.d/35debfoster
```

3. Saisissez dans le fichier:

```
#!/bin/sh
set -e

# Make sure sort always sorts in same order.
LANG=C
export LANG

shellquote() {
        # Single quotes text, escaping existing single quotes.
        sed -e "s/'/'\"'\"'/g" -e "s/^/'/" -e "s/$/'/"
}


if [ "$VCS" = git ] || [ "$VCS" = hg ] || [ "$VCS" = bzr ] || [ "$VCS" = darcs ];
then
        # Make sure the file is not readable by others, since it can leak
        # information about contents of non-readable directories in /etc.
        debfoster -q -k /etc/keepers
        chmod 600 /etc/keepers
        sed -i "1i\\# debfoster file" /etc/keepers
        sed -i "1i\\# Generated by etckeeper.  Do not edit."  /etc/keepers

        # stage the file as part of the current commit
        if [ "$VCS" = git ]; then
                # this will do nothing if the keepers file is unchanged.
                git add keepers
        fi
        # hg, bzr and darcs add not done, they will automatically
        # include the file in the current commit
fi
```

4. Sauvez et tapez:

```
chmod 755 /etc/etckeeper/pre-commit.d/35debfoster
```

5. Exécutez maintenant `etckeeper`

```
etckeeper commit
```

6. Le fichier keepers est créé et sauvegardé automatiquement.

5.7. Installation des mises à jours automatiques

Si vous souhaitez installer automatiquement les paquets Debian de correction de bugs de sécurité, cette installation est pour vous.

Cette installation est optionnelle.

L'installation automatique de paquets peut conduire dans certains cas très rare à des dysfonctionnements du serveur. Il est important de regarder périodiquement les logs d'installation

Tapez:

```
apt install unattended-upgrades
```

5.8. Vérification du nom de serveur

Cette partie consiste à vérifier que le serveur a un hostname correctement configuré.

1. Loguez vous comme root sur le serveur
2. vérifier que le hostname est bien celui attendu (c'est à dire configuré par votre hébergeur). Tapez :

   ```
   cat /etc/hostname
   ```

   Le nom du hostname (sans le domaine) doit s'afficher.

   a. Si ce n'est pas le cas, changer ce nom en éditant le fichier. Tapez :

      ```
      vi /etc/hostname
      ```

      Changez la valeur, sauvegardez et rebootez. Tapez :

      ```
      reboot
      ```

   b. Loguez vous comme root sur le serveur
3. Vérifier le fichier `hosts`. Tapez :

   ```
   cat /etc/hosts
   ```

   Si le fichier contient plusieurs lignes avec la même adresse de loopback en `127.x.y.z`, en gardez une seule et celle avec le hostname et le nom de domaine complet.

   a. si ce n'est pas le cas, changer les lignes en éditant le fichier. Tapez:

      ```
      vi /etc/hosts
      ```

   b. Changez la ou les lignes, sauvegardez.

Le FQDN (nom de machine avant le nom de domaine) doit être déclaré avant le hostname simple dans le fichier `hosts`.

c. Rebootez. Tapez :

```
reboot
```

d. Loguez vous comme root sur le serveur

4. Vérifiez que tout est correctement configuré.

a. Tapez :

```
hostname
```

La sortie doit afficher le nom de host.

b. Tapez ensuite :

```
hostname -f
```

La sortie doit afficher le nom de host avec le nom de domaine.

5.9. Interdire le login direct en root

Il est toujours vivement déconseillé d'autoriser la possibilité de se connecter directement en SSH en tant que root. De ce fait, notre première action sera de désactiver le login direct en root et d'autoriser le sudo. Respectez bien les étapes de cette procédure:

1. Loguez vous comme root sur le serveur
2. Ajoutez un utilisateur standard qui sera nommé par la suite en tant que <sudo_username>

a. Tapez :

```
adduser <sudo_username>
```

b. Répondez aux questions qui vont sont posées: habituellement le nom complet d'utilisateur et le mot de passe.

c. Donner les attributs sudo à l'utilisateur `<sudo_username>`. Tapez :

```
usermod -a -G sudo <sudo_username>
```

d. Dans une autre fenêtre, se connecter sur le serveur avec votre nouveau compte `<sudo_username>`:

```
ssh <sudo_username>@<example.com> ①
```

① remplacer ici <sudo_username> par votre login et <example.com> par votre nom de domaine

e. une fois logué, tapez:

```
sudo bash
```

Tapez le mot de passe de votre utilisateur. Vous devez avoir accès au compte root. Si ce n'est pas le cas, revérifiez la procédure et repassez toutes les étapes.

Tout pendant que ces premières étapes ne donnent pas satisfaction ne passez pas à la suite sous peine de perdre la possibilité d'accéder à votre serveur.

1. Il faut maintenant modifier la configuration de sshd.
   a. Editez le fichier `/etc/ssh/sshd_config`, Tapez:

```
vi /etc/ssh/sshd_config
```

il faut rechercher la ligne: `PermitRootLogin yes` et la remplacer par:

```
PermitRootLogin no
```

   b. Redémarrez le serveur ssh. Tapez :

```
service sshd restart
```

2. Faites maintenant l'essai de vous re-loguer avec le compte root.Tapez :

```
ssh root@<example.com> ①
```

① Remplacer ici <example.com> par votre nom de domaine

3. Ce ne devrait plus être possible: le serveur vous l'indique par un message `Permission denied, please try again.`

5.10. Création d'une clé de connexion ssh locale

Pour créer une clé et la déployer:

1. Créez une clé sur votre machine locale (et pas sur le serveur distant!):
   a. Ouvrir un terminal

b. Créer un répertoire `~/.ssh` s'il n'existe pas. tapez :

```
mkdir -p $HOME/.ssh
```

c. Allez dans le répertoire. Tapez :

```
cd ~/.ssh
```

d. Générez vous clés. Tapez :

```
ssh-keygen -t rsa
```

e. Un ensemble de questions apparaît. Si un texte vous explique que le fichier existe déjà, arrêtez la procédure. Cela signifie que vous avez déjà créé une clé et que vous risquez de perdre la connexion à d'autres serveurs si vous en générez une nouvelle. Sinon, appuyez sur Entrée à chaque fois pour accepter les valeurs par défaut.

2. Sur votre PC local afficher la clé à l'écran. Elle sera copiée-collée par la suite:

```
cat /root/.ssh/id_rsa.pub
```

3. Déployez votre clé:

a. Loguez vous sur votre serveur distant. Tapez :

```
ssh <sudo_username>@<example.com> ①
```

① remplacer ici <sudo_username> par votre login et <example.com> par votre nom de domaine

Entrez votre mot de passe

b. Créer un répertoire `~/.ssh` s'il n'existe pas. tapez: :

```
mkdir -p $HOME/.ssh
```

c. Éditez le fichier `~/.ssh/authorized_keys` tapez:

```
vi ~/.ssh/authorized_keys
```

et coller dans ce fichier le texte contenu dans le votre fichier local `~/.ssh/id_rsa.pub`. Remarque: il peut y avoir déjà des clés dans le fichier `authorized_keys`.

d. Sécurisez votre fichier de clés. Tapez: :

```
chmod 600 ~/.ssh/authorized_keys
```

e. Sécurisez le répertoire SSH; Tapez :

```
chmod 700 ~/.ssh
```

f. Déconnectez vous de votre session

4. Vérifiez que tout fonctionne en vous connectant. Tapez: :

```
ssh <sudo_username>@<example.com> ①
```

① remplacer ici <sudo_username> par votre login et <example.com> par votre nom de domaine

La session doit s'ouvrir sans demander de mot de passe.

5.11. Sudo sans mot de passe

Avant tout, il faut bien se rendre compte que cela constitue potentiellement une faille de sécurité et qu'en conséquence, le compte possédant cette propriété devra être autant sécurisé qu'un compte root. L'intérêt étant d'interdire le compte root en connexion ssh tout en gardant la facilité de se loguer root sur le système au travers d'un super-compte.

1. Loguez vous comme root sur le serveur
2. Ajoutez un groupe sudonp et y affecter un utilisateur. Tapez :

```
addgroup --system sudonp
```

a. Ajouter l'utilisateur: :

```
usermod -a -G sudonp <sudo_username>
```

b. Éventuellement retirez l'utilisateur du groupe sudo s'il a été ajouté auparavant :

```
gpasswd -d <sudo_username> sudo
```

c. Éditez le fichier sudoers. Tapez :

```
vi /etc/sudoers
```

d. Ajouter dans le fichier la ligne suivante:

```
%sudonp ALL=(ALL:ALL) NOPASSWD: ALL
```

L'utilisateur nom_d_utilisateur pourra se logger root sans mot de passe au travers de la commande `sudo bash`

5.12. Installer l'outil dselect

L'outil `dselect` permet de choisir de façon interactive les paquets que l'on souhaite installer.

1. Loguez vous comme root sur le serveur
2. Ajouter le paquet `dselect`. Tapez :

```
apt install dselect
```

5.13. Ajouter un fichier de swap

Pour un serveur VPS de 2 Go de RAM, la taille du fichier de swap sera de 1 Go. Si vous avez beaucoup d'outils et de serveurs à installer il peut être nécessaire d'avoir 4 Go de RAM au total.

Tapez :

1. Loguez vous comme root sur le serveur
2. Tout d'abord, si l'outil `dphys-swapfile` est installé et configuré sur la machine, commencez par désactiver le swap. Tapez:

```
dphys-swapfile uninstall
```

3. Tapez:

```
cd /
fallocate -l 2G /swapfile
chmod 600 /swapfile
mkswap /swapfile
swapon /swapfile
```

4. Enfin ajoutez une entrée dans le fichier fstab. Tapez :

```
vi /etc/fstab
```

5. Ajoutez la ligne:

```
/swapfile swap swap defaults 0 0
```

6. Enfin vous pouvez être tenté de limiter le swap (surtout utile sur les systèmes avec peu de RAM et du SSD. Tapez:

```
vi /etc/systctl.conf
```

7. Ajoutez ou modifiez la ligne:

```
vm.swappiness = 5
```

8. Le paramètre sera actif au prochain reboot

Chapter 6. Installation initiale des outils

La procédure d'installation ci-dessous configure ISPconfig avec les fonctionnalités suivantes: Postfix, Dovecot, MariaDB, rkHunter, Apache, PHP, Let's Encrypt, PureFTPd, Bind, Webalizer, AWStats, fail2Ban, UFW Firewall, PHPMyadmin, RoundCube.

Pour les systèmes ayant 2 Go de RAM ou plus, il est fortement conseillé d'installer les outils ci après : Amavisd, SPamAssassin, ClamAV, Mailman.

1. Loguez vous comme root sur le serveur
2. Changez le Shell par défaut. Tapez :

   ```
   dpkg-reconfigure dash
   ```

   A la question `utilisez dash comme shell par défaut` répondez `non`. C'est bash qui doit être utilisé.

3. Installation de quelques paquets debian. ;-)
   a. Tapez :

      ```
      apt install patch ntp postfix postfix-mysql postfix-doc mariadb-client mariadb-
      server openssl getmail4 rkhunter binutils dovecot-imapd dovecot-pop3d dovecot-
      mysql dovecot-sieve dovecot-lmtpd unzip bzip2 arj nomarch lzop cabextract p7zip
      p7zip-full unrar lrzip libnet-ldap-perl libauthen-sasl-perl clamav-docs daemon
      libio-string-perl libio-socket-ssl-perl libnet-ident-perl zip libnet-dns-perl
      libdbd-mysql-perl postgrey apache2 apache2-doc apache2-utils libapache2-mod-php
      php php-common php-gd php-mysql php-imap php-cli php-cgi libapache2-mod-fcgid
      apache2-suexec-pristine php-pear mcrypt  imagemagick libruby libapache2-mod-
      python php-curl php-intl php-pspell php-recode php-sqlite3 php-tidy php-xmlrpc
      php-xsl memcached php-memcache php-imagick php-gettext php-zip php-mbstring
      memcached libapache2-mod-passenger php-soap php-fpm php-opcache php-apcu bind9
      dnsutils haveged webalizer awstats geoip-database libclass-dbi-mysql-perl
      libtimedate-perl fail2ban ufw anacron
      ```

   b. Pour les systèmes avec plus de mémoire tapez :

      ```
      apt install amavisd-new spamassassin clamav clamav-daemon
      ```

4. Aux questions posées répondez:
   a. `Type principal de configuration de mail`: ← Sélectionnez `Site Internet`
   b. `Nom de courrier`: ← Entrez votre nom de host. Par exemple: mail.example.com

6.1. Configuration de Postfix

1. Editez le master.cf file de postfix. Tapez :

```
vi /etc/postfix/master.cf
```

2. Ajoutez dans le fichier:

```
submission inet n - - - - smtpd
 -o syslog_name=postfix/submission
 -o smtpd_tls_security_level=encrypt
 -o smtpd_sasl_auth_enable=yes
 -o smtpd_client_restrictions=permit_sasl_authenticated,reject

smtps inet n - - - - smtpd
 -o syslog_name=postfix/smtps
 -o smtpd_tls_wrappermode=yes
 -o smtpd_sasl_auth_enable=yes
 -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

3. Sauvegardez et relancez Postfix:

```
systemctl restart postfix
```

4. Si vous avez installé `SpamAssassin`, désactiver `SpamAssassin` puisque `amavisd` utilise celui ci en sous jacent. Tapez :

```
systemctl stop spamassassin
systemctl disable spamassassin
```

6.2. Configuration de MariaDB

1. Sécurisez votre installation MariaDB. Tapez :

```
mysql_secure_installation
```

Répondez au questions ainsi:

a. `Enter current password for root`: ← Tapez Entrée
b. `Set root password? [Y/n]`: ← Tapez `Y`
c. `New password:`: ← Tapez votre mot de passe root MariaDB
d. `Re-enter New password:`: ← Tapez votre mot de passe root MariaDB
e. `Remove anonymous users? [Y/n]`: ← Tapez `Y`
f. `Disallow root login remotely? [Y/n]`: ← Tapez `Y`
g. `Remove test database and access to it? [Y/n]`: ← Tapez `Y`

h. `Reload privilege tables now? [Y/n]`: ← Tapez `Y`

2. MariaDB doit pouvoir être atteint par toutes les interfaces et pas seulement localhost.
3. Éditez le fichier de configuration. :

```
vi /etc/mysql/mariadb.conf.d/50-server.cnf
```

4. Commentez la ligne `bind-address`:

```
#bind-address           = 127.0.0.1
```

5. Modifiez la méthode d'accès à la base MariaDB pour utiliser la méthode de login native.
   a. Tapez :

```
echo "update mysql.user set plugin = 'mysql_native_password' where user='root';"
| mysql -u root
```

6. Editez le fichier debian.cnf. Tapez :

```
vi /etc/mysql/debian.cnf
```

   a. Aux deux endroits du fichier ou le mot clé `password` est présent, mettez le mot de passe root de votre base de données.

```
password = votre_mot_de_passe
```

7. Pour éviter l'erreur `Error in accept: Too many open files`, augmenter la limite du nombre de fichiers ouverts.
   a. Editer le fichier: :

```
vi /etc/security/limits.conf
```

   b. Ajoutez à la fin du fichier les deux lignes:

```
mysql soft nofile 65535
mysql hard nofile 65535
```

8. Créez ensuite un nouveau répertoire. Tapez:

```
mkdir -p /etc/systemd/system/mysql.service.d/
```

a. Editer le fichier limits.conf. :

```
vi /etc/systemd/system/mysql.service.d/limits.conf
```

b. Ajoutez dans le fichier les lignes suivantes:

```
[Service]
LimitNOFILE=infinity
```

9. Redémarrez votre serveur MariaDB. Tapez: :

```
systemctl daemon-reload
systemctl restart mariadb
```

10. vérifiez maintenant que MariaDB est accessible sur toutes les interfaces réseau. Tapez :

```
netstat -tap | grep mysql
```

11. La sortie doit être du type: `tcp6 0 0 [::]:mysql [::]:* LISTEN 13708/mysqld`
12. Pour les serveur avec peu de ressources quelques éléments de tuning. Editez le fichier 50-server.cnf:

```
vi /etc/mysql/mariadb.conf.d/50-server.cnf
```

6.3. Configuration d'Apache

1. Installez les modules Apache nécessaires. Tapez :

```
a2enmod suexec rewrite ssl proxy_http actions include dav_fs dav auth_digest cgi
headers actions proxy_fcgi alias speling
```

2. Pour ne pas être confronté aux problèmes de sécurité de type HTTPOXY, il est nécessaire de créer un petit module dans apache.

a. Éditez le fichier httpoxy.conf: :

```
vi /etc/apache2/conf-available/httpoxy.conf
```

b. Collez les lignes suivantes:

```
<IfModule mod_headers.c>
    RequestHeader unset Proxy early
</IfModule>
```

3. Activez le module en tapant :

```
a2enconf httpoxy
systemctl restart apache2
```

4. Désactiver la documentation apache en tapant:

```
a2disconf apache2-doc
systemctl restart apache2
```

6.4. Installation et Configuration de Mailman

1. Tapez :

```
apt-get install mailman
```

2. Sélectionnez un langage:
   a. `Languages to support:` ← Tapez `en (English)`
   b. `Missing site list :` ← Tapez `Ok`
3. Créez une mailing list. Tapez:

```
newlist mailman
```

4. ensuite éditez le fichier aliases: :

```
vi /etc/aliases
```

   et ajoutez les lignes affichées à l'écran:

```
## mailman mailing list
mailman:              "|/var/lib/mailman/mail/mailman post mailman"
mailman-admin:        "|/var/lib/mailman/mail/mailman admin mailman"
mailman-bounces:      "|/var/lib/mailman/mail/mailman bounces mailman"
mailman-confirm:      "|/var/lib/mailman/mail/mailman confirm mailman"
mailman-join:         "|/var/lib/mailman/mail/mailman join mailman"
mailman-leave:        "|/var/lib/mailman/mail/mailman leave mailman"
mailman-owner:        "|/var/lib/mailman/mail/mailman owner mailman"
mailman-request:      "|/var/lib/mailman/mail/mailman request mailman"
mailman-subscribe:    "|/var/lib/mailman/mail/mailman subscribe mailman"
mailman-unsubscribe:  "|/var/lib/mailman/mail/mailman unsubscribe mailman"
```

5. Exécutez :

```
newaliases
```

et redémarrez postfix: :

```
systemctl restart postfix
```

6. Activez la page web de mailman dans apache: :

```
ln -s /etc/mailman/apache.conf /etc/apache2/conf-enabled/mailman.conf
```

7. Redémarrez apache :

```
systemctl restart apache2
```

puis redémarrez le demon mailman :

```
systemctl restart mailman
```

8. Le site web de mailman est accessible
   a. Vous pouvez accéder à la page admin Mailman à http://<server1.example.com>/cgi-bin/mailman/admin/
   b. La page web utilisateur de la mailing list est accessible ici http://<server1.example.com/cgi-bin>/mailman/listinfo/.
   c. Sous http://<server1.example.com>/pipermail/mailman vous avez accès aux archives.

6.5. Configuration d' Awstats

1. configurer la tache cron d'awstats: Éditez le fichier :

```
vi /etc/cron.d/awstats
```

Et commentez toutes les lignes:

```
#MAILTO=root
#*/10 * * * * www-data [ -x /usr/share/awstats/tools/update.sh ] &&
/usr/share/awstats/tools/update.sh
# Generate static reports:
#10 03 * * * www-data [ -x /usr/share/awstats/tools/buildstatic.sh ] &&
/usr/share/awstats/tools/buildstatic.sh
```

6.6. Configuration de Fail2ban

1. Editez le fichier jail.local :

```
vi /etc/fail2ban/jail.local
```

Ajoutez les lignes suivantes:

```
[dovecot]
enabled = true
filter = dovecot
logpath = /var/log/mail.log
maxretry = 5

[postfix-sasl]
enabled = true
port = smtp
filter = postfix[mode=auth]
logpath = /var/log/mail.log
maxretry = 3
```

2. Redémarrez Fail2ban: :

```
systemctl restart fail2ban
```

6.7. Installation et configuration de PureFTPd

1. Tapez: :

```
apt-get install pure-ftpd-common pure-ftpd-mysql
```

2. Éditez le fichier de conf: :

```
vi /etc/default/pure-ftpd-common
```

3. Changez les lignes ainsi:

```
STANDALONE_OR_INETD=standalone
VIRTUALCHROOT=true
```

4. Autorisez les connexions TLS. Tapez:

```
echo 1 > /etc/pure-ftpd/conf/TLS
```

5. Créez un certificat SSL.
   a. Tapez :

```
mkdir -p /etc/ssl/private/
```

   b. Puis créez le certificat auto signé. Tapez :

```
openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout
/etc/ssl/private/pure-ftpd.pem -out /etc/ssl/private/pure-ftpd.pem
```

   et répondez aux questions de la manière suivante:

   i. `Country Name (2 letter code) [AU]:` ← Entrez le code pays à 2 lettres
   ii. `State or Province Name (full name) [Some-State]:` ← Entrer le nom d'état
   iii. `Locality Name (eg, city) []:` ← Entrer votre ville
   iv. `Organization Name (eg, company) [Internet Widgits Pty Ltd]:` ← Entrez votre entreprise ou tapez entrée
   v. `Organizational Unit Name (eg, section) []:` ← Tapez entrée
   vi. `Common Name (e.g. server FQDN or YOUR name) []:` ← Enter le nom d'hôte de votre serveur. Dans notre cas: server1.example.com
   vii. `Email Address []:` ← Tapez entrée

c. Puis tapez :

```
chmod 600 /etc/ssl/private/pure-ftpd.pem
```

d. et redémarrez pure-ftpd en tapant: :

```
systemctl restart pure-ftpd-mysql
```

e. En Option: Activer les quotas si votre kernel le permet.

- Installez les paquets de gestion des quotas. Tapez:

```
apt install quota quotatool
```

- Editez `fstab`. Tapez:

```
vi /etc/fstab
```

- Inserez le texte ci dessous pour chaque directive de montage

```
UUID=45576b38-39e8-4994-b8c1-ea4870e2e614 / ext4 errors=remount-
ro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0 1
```

- Pour le Raspberry, éditez le fichier rc.local pour créer /dev/root à chaque reboot:

```
ln -s /dev/mmblk0p7 /dev/root
vi /etc/rc.local
```

- Ajoutez avant `exit 0`:

```
ln -s /dev/mmcblk0p7 /dev/root
```

- Pour activer les quotas, tapez:

```
mount -o remount /
quotacheck -avugm
quotaon -avug
```

6.8. Installation et configuration de phpmyadmin

1. Installez phpmyadmin. Exécutez:

```
mkdir /usr/share/phpmyadmin
mkdir /etc/phpmyadmin
mkdir -p /var/lib/phpmyadmin/tmp
chown -R www-data:www-data /var/lib/phpmyadmin
touch /etc/phpmyadmin/htpasswd.setup
cd /tmp
wget https://files.phpmyadmin.net/phpMyAdmin/4.9.0.1/phpMyAdmin-4.9.0.1-all-
languages.tar.gz
tar xfz phpMyAdmin-4.9.0.1-all-languages.tar.gz
mv phpMyAdmin-4.9.0.1-all-languages/* /usr/share/phpmyadmin/
rm phpMyAdmin-4.9.0.1-all-languages.tar.gz
rm -rf phpMyAdmin-4.9.0.1-all-languages
cp /usr/share/phpmyadmin/config.sample.inc.php
/usr/share/phpmyadmin/config.inc.php
```

2. Éditez le fichier :

```
vi /usr/share/phpmyadmin/config.inc.php
```

   a. Modifier l'entrée `blowfish_secret` en ajoutant votre propre chaîne de 32 caractères.

   b. Éditez le fichier: :

```
vi /etc/apache2/conf-available/phpmyadmin.conf
```

   c. Ajoutez les lignes suivantes:

```
# phpMyAdmin default Apache configuration

Alias /phpmyadmin /usr/share/phpmyadmin

<Directory /usr/share/phpmyadmin>
 Options FollowSymLinks
 DirectoryIndex index.php

 <IfModule mod_php7.c>
 AddType application/x-httpd-php .php

 php_flag magic_quotes_gpc Off
 php_flag track_vars On
 php_flag register_globals Off
 php_value include_path .
 </IfModule>

</Directory>

# Authorize for setup
<Directory /usr/share/phpmyadmin/setup>
 <IfModule mod_authn_file.c>
 AuthType Basic
 AuthName "phpMyAdmin Setup"
 AuthUserFile /etc/phpmyadmin/htpasswd.setup
 </IfModule>
 Require valid-user
</Directory>

# Disallow web access to directories that don't need it
<Directory /usr/share/phpmyadmin/libraries>
 Order Deny,Allow
 Deny from All
</Directory>
<Directory /usr/share/phpmyadmin/setup/lib>
 Order Deny,Allow
 Deny from All
</Directory>
```

3. Activez le module et redémarrez apache. Tapez :

```
a2enconf phpmyadmin
systemctl restart apache2
```

4. Créer la base de donnée phpmyadmin.
    a. Tapez :

```
mysql -u root -p
```

puis entrer le mot de passe root

b. Créez une base phpmyadmin. Tapez :

```
CREATE DATABASE phpmyadmin;
```

c. Créez un utilisateur phpmyadmin. Tapez :

```
CREATE USER 'pma'@'localhost' IDENTIFIED BY 'mypassword'; ①
```

① `mypassword` doit être remplacé par un mot de passe choisi.

d. Accordez des privilèges et sauvez:

```
GRANT ALL PRIVILEGES ON phpmyadmin.* TO 'pma'@'localhost' IDENTIFIED BY
'mypassword' WITH GRANT OPTION; ①
```

① `mypassword` doit être remplacé par un mot de passe choisi.

e. Flusher les privilèges:

```
FLUSH PRIVILEGES;
```

f. et enfin

```
EXIT;
```

5. Chargez les tables sql dans la base phpmyadmin:

```
mysql -u root -p phpmyadmin < /usr/share/phpmyadmin/sql/create_tables.sql
```

6. Enfin ajoutez les mots de passe nécessaires dans le fichier de config.

a. Tapez:

```
vi /usr/share/phpmyadmin/config.inc.php
```

b. Rechercher le texte contenant `controlhost` . Ci-dessous, un exemple:

```
/* User used to manipulate with storage */
$cfg['Servers'][$i]['controlhost'] = 'localhost';
$cfg['Servers'][$i]['controlport'] = '';
$cfg['Servers'][$i]['controluser'] = 'pma';
$cfg['Servers'][$i]['controlpass'] = 'mypassword'; ①


/* Storage database and tables */
$cfg['Servers'][$i]['pmadb'] = 'phpmyadmin';
$cfg['Servers'][$i]['bookmarktable'] = 'pma__bookmark';
$cfg['Servers'][$i]['relation'] = 'pma__relation';
$cfg['Servers'][$i]['table_info'] = 'pma__table_info';
$cfg['Servers'][$i]['table_coords'] = 'pma__table_coords';
$cfg['Servers'][$i]['pdf_pages'] = 'pma__pdf_pages';
$cfg['Servers'][$i]['column_info'] = 'pma__column_info';
$cfg['Servers'][$i]['history'] = 'pma__history';
$cfg['Servers'][$i]['table_uiprefs'] = 'pma__table_uiprefs';
$cfg['Servers'][$i]['tracking'] = 'pma__tracking';
$cfg['Servers'][$i]['userconfig'] = 'pma__userconfig';
$cfg['Servers'][$i]['recent'] = 'pma__recent';
$cfg['Servers'][$i]['favorite'] = 'pma__favorite';
$cfg['Servers'][$i]['users'] = 'pma__users';
$cfg['Servers'][$i]['usergroups'] = 'pma__usergroups';
$cfg['Servers'][$i]['navigationhiding'] = 'pma__navigationhiding';
$cfg['Servers'][$i]['savedsearches'] = 'pma__savedsearches';
$cfg['Servers'][$i]['central_columns'] = 'pma__central_columns';
$cfg['Servers'][$i]['designer_settings'] = 'pma__designer_settings';
$cfg['Servers'][$i]['export_templates'] = 'pma__export_templates';
```

① A tous les endroit ou vous voyez dans le texte ci dessus le mot `mypassword` mettez celui choisi. N'oubliez pas de dé-commenter les lignes.

6.9. Installation et configuration de Roundcube

1. Tapez:

```
apt-get install roundcube roundcube-core roundcube-mysql roundcube-plugins
```

2. Répondez aux question
   - `Utiliser dbconfig_common` ← Répondre `Oui`
   - `Mot de passe Mysql pour db Roundcube` ← Tapez un mot de passe
3. Éditez le fichier php de roundcube: :

```
vi /etc/roundcube/config.inc.php
```

et définissez les hosts par défaut comme localhost

```
$config['default_host'] = 'localhost';
$config['smtp_server'] = 'localhost';
```

4. Éditez la configuration apache pour roundcube: :

```
vi /etc/apache2/conf-enabled/roundcube.conf
```

et ajouter au début les lignes suivantes:

```
Alias /roundcube /var/lib/roundcube
Alias /webmail /var/lib/roundcube
```

5. Redémarrez Apache:

```
systemctl reload apache2
```

6.10. Installation de Let's Encrypt

Installez Let's Encrypt. Tapez:

```
cd /usr/local/bin
wget https://dl.eff.org/certbot-auto
chmod a+x certbot-auto
./certbot-auto --install-only
```

Une façon alternative de l'installer est:

```
apt install python3-certbot-apache
```

6.11. Installation d'un scanner de vulnérabilités

1. Loguez vous comme root sur le serveur
2. installer Git. Tapez :

```
apt install git
```

3. installer Lynis
   a. Tapez :

```
cd
git clone https://github.com/CISOfy/lynis
```

b. Executez :

```
cd lynis;./lynis audit system
```

4. L'outil vous listera dans une forme très synthétique la liste des vulnérabilités et des améliorations de sécurité à appliquer.

Chapter 7. Installation d'un Panel

Il existe plusieurs type de panel de contrôle pour les VPS. La plupart sont payant.

Pour citer les plus connus:

- payant: cPanel (leader du type), Plesk
- gratuit: Yunohost (un excellent système d'autohébergement packagé) , Ajenti, Froxlor, Centos web panel, Webmin et Usermin, ISPConfig, HestiaCP, VestaCP ,

Ci après nous allons en présenter 3 différents (ISPConfig, Webmin et HestiaCP). Ils sont incompatibles entre eux.

On peut faire cohabiter ISPConfig et Webmin en prenant les précautions suivantes:

- ISPConfig est le maitre de la configuration: toute modification sur les sites webs, mailboxes et DNS doit impérativement être effectuées du coté d'ISPConfig
- Les modifications réalisées au niveau de webmin pour ces sites webs, mailboxes et DNS seront au mieux écrasées par ISPConfig au pire elles risquent de conduire à des incompatibilités qui engendreront des dysfonctionnement d'ISPConfig (impossibilité de mettre à jour les configurations)
- Le reste des modifications peuvent être configurées au niveau de webmin sans trop de contraintes.

Pour rappel, HestiaCP (tout comme VestaCP) sont incompatibles d'ISPConfig et de Webmin. Ils doivent être utilisés seuls

7.1. Installation et configuration de ISPConfig

ISPConfig est un système de configuration de sites web totalement compatible avec Webmin.

Pour installer ISPConfig, vous devez suivre la procédure ci-dessous. ISPConfig 3.1 a été utilisé dans ce tutoriel.

1. Loguez vous comme root sur le serveur
2. Tapez:

```
cd /tmp
```

3. Cherchez la dernière version d'ISPConfig sur le site ISPConfig
4. Installez cette version en tapant: :

```
wget <la_version_a_telecharger>.tar.gz
```

5. Décompressez la version en tapant: :

```
tar xfz <la_version>.tar.gz
```

6. Enfin allez dans le répertoire d'installation: :

```
cd ispconfig3_install/install/
```

7. Lancez l'installation: :

```
php -q install.php
```

et répondez aux questions:

a. `Select language (en,de) [en]:` ← Tapez entrée
b. `Installation mode (standard,expert) [standard]:` ← Tapez entrée
c. `Full qualified hostname (FQDN) of the server, eg server1.domain.tld [server1.example.com]:` ← Tapez entrée
d. `MySQL server hostname [localhost]:` ← Tapez entrée
e. `MySQL server port [3306]:` ← Tapez entrée
f. `MySQL root username [root]:` ← Tapez entrée
g. `MySQL root password []:` ← Enter your MySQL root password
h. `MySQL database to create [dbispconfig]:` ← Tapez entrée
i. `MySQL charset [utf8]:` ← Tapez entrée
j. `Country Name (2 letter code) [AU]:` ← Entrez le code pays à 2 lettres
k. `State or Province Name (full name) [Some-State]:` ← Entrer le nom d'état
l. `Locality Name (eg, city) []:` ← Entrer votre ville
m. `Organization Name (eg, company) [Internet Widgits Pty Ltd]:` ← Entrez votre entreprise ou tapez entrée
n. `Organizational Unit Name (eg, section) []:` ← Tapez entrée
o. `Common Name (e.g. server FQDN or YOUR name) []:` ← Enter le nom d'hôte de votre serveur. Dans notre cas: server1.example.com
p. `Email Address []:` ← Tapez entrée
q. `ISPConfig Port [8080]:` ← Tapez entrée
r. `Admin password [admin]:` ← Tapez entrée
s. `Do you want a secure (SSL) connection to the ISPConfig web interface (y,n) [y]:` ←- Tapez entrée
t. `Country Name (2 letter code) [AU]:` ← Entrez le code pays à 2 lettres
u. `State or Province Name (full name) [Some-State]:` ← Entrer le nom d'état

v. `Locality Name (eg, city) []:` ← Entrer votre ville

w. `Organization Name (eg, company) [Internet Widgits Pty Ltd]:` ← Entrez votre entreprise ou tapez entrée

x. `Organizational Unit Name (eg, section) []:` ← Tapez entrée

y. `Common Name (e.g. server FQDN or YOUR name) []:` ← Enter le nom d'hôte de votre serveur. Dans notre cas: server1.example.com

z. `Email Address []:` ← Tapez entrée

8. Sécurisez Apache

a. Il est maintenant recommandé de désactiver les protocoles TLS 1.0 et TLS 1.1. Ce n'est pas la configuration par défaut d'ISPconfig

b. Loguez vous comme root sur le serveur.

c. Copier le fichier `vhost.conf.master` dans la zone custom

```
cp /usr/local/ispconfig/server/conf/vhost.conf.master
/usr/local/ispconfig/server/conf-custom/vhost.conf.master
```

d. Editer le fichier dans la zone custom. Tapez:

```
vi /usr/local/ispconfig/server/conf-custom/vhost.conf.master
```

e. Remplacez la ligne `SSLProtocol All` par:

```
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
```

9. L'installation est terminée. Vous accédez au serveur à l'adresse: https://example.com:8080/ .

Lors de votre première connexion, votre domaine n'est pas encore configuré. Il faudra alors utiliser le nom DNS donné par votre hébergeur. Pour OVH, elle s'écrit VPSxxxxxx.ovh.net

10. Loguez vous comme admin et avec le mot de passe que vous avez choisi. Vous pouvez décider de le changer au premier login

Si le message "Possible attack detected. This action has been logged.". Cela signifie que vous avez des cookies d'une précédente installation qui sont configurés. Effacer les cookies de ce site de votre navigateur.

7.2. Installation de Webmin

Webmin est un outil généraliste de configuration de votre serveur. Son usage peut être assez complexe mais il permet une configuration plus précise des fonctionnalités.

1. Loguez vous comme root sur le serveur
2. Ajoutez le repository Webmin
   a. allez dans le répertoire des repositories. Tapez :

   ```
   cd /etc/apt/sources.list.d
   ```

   b. Tapez: :

   ```
   echo "deb http://download.webmin.com/download/repository sarge contrib" >>
   webmin.list
   ```

   c. Ajoutez la clé. Tapez :

   ```
   curl -fsSL http://www.webmin.com/jcameron-key.asc | sudo apt-key add -
   ```

   Le message `OK` s'affiche
3. Mise à jour. Tapez :

   ```
   apt update
   ```

4. Installation de Webmin. Tapez :

   ```
   apt install webmin
   ```

   ```
   Débloquez le port 10000 dans votre firewall
   ```

   a. Allez sur le site ispconfig https://example.com:8080/
   b. Loguez-vous et cliquez sur la rubrique `System` et le menu `Firewall`. Cliquez sur votre serveur.
   c. dans la rubrique `Open TCP ports:`, ajoutez le port 10000
   d. Cliquez sur `save`
5. Connectez vous avec votre navigateur sur l'url https://<example.com>:10000. Un message indique un problème de sécurité. Cela vient du certificat auto-signé. Cliquez sur 'Avancé' puis 'Accepter le risque et poursuivre'.
6. Loguez-vous `root`. Tapez le mot de passe de `root`. Le dashboard s'affiche.
7. Restreignez l'adressage IP
   a. Obtenez votre adresse IP en allant par exemples sur le site https://www.showmyip.com/
   b. Sur votre URL Webmin ou vous êtes logué, allez dans Webmin→Webmin Configuration

c. Dans l'écran choisir l'icône `Ip Access Control`.

d. Choisissez `Only allow from listed addresses`

e. Puis dans le champ `Allowed IP addresses` tapez votre adresse IP récupérée sur showmyip

f. Cliquez sur `Save`

g. Vous devriez avoir une brève déconnexion le temps que le serveur Webmin redémarre puis une reconnexion.

8. Si vous n'arrivez pas à vous reconnecter c'est que l'adresse IP n'est pas la bonne. Le seul moyen de se reconnecter est de:

   a. Loguez vous comme root sur le serveur

   b. Éditez le fichier /etc/webmin/miniserv.conf et supprimez la ligne `allow= ⋯`

   c. Tapez :

   ```
   service webmin restart
   ```

   d. Connectez vous sur l'url de votre site Webmin. Tout doit fonctionner

9. Passez en Français. Pour les personnes non anglophone. Les traductions française ont des problèmes d'encodage de caractère ce n'est donc pas recommandé. La suite de mon tutoriel suppose que vous êtes resté en anglais.

   a. Sur votre url Webmin ou vous êtes logué, allez dans Webmin → Webmin Configuration

   b. Dans l'écran choisir l'icône `Language and Locale`.

   c. Choisir `Display Language` à `French (FR.UTF-8)`

Chapter 8. Configuration d'un domaine

Cette configuration est réalisée avec le Panel ISPConfig installé dans le chapitre précédent. L'étape "login initial" n'est à appliquer qu'une seule fois. Une fois votre premier domaine configuré, vous pourrez vous loguer à ISPconfig en utilisant ce domaine à l'adresse: https://example.com:8080/ .

8.1. Login initial

Cette procédure n'est à appliquer que lorsqu'aucun domaine n'est encore créé.

Vous devrez tout d'abord vous loguer sur le serveur ISPConfig. Comme vous n'avez pas encore configuré de nom de de domaine, vous devrez vous loguer de prime abord sur le site http://vpsxxxxxx.ovh.net:8080/ pour un vps chez ovh par exemple ou sur http://raspberrypi.local:8080/ pour un Raspberry.

Utiliser le login: Admin et le mot de passe que vous avez configuré lors de l'installation d'ISPConfig

1. Aller dans la rubrique `System`
    a. Dans le menu `Main config`
        i. Dans l'onglet `Sites`, configurer:
            A. `Create subdomains as web site:` ← Yes
            B. `Create aliasdomains as web site:` ← Yes
        ii. Dans l'onglet `Mail` :
            A. `Administrator's e-mail :` ← adresse mail de l'administrateur. par exemple admin@example.com
            B. `Administrator's name :` ← nom de l'administrateur
    b. Dans le menu `Firewall`
        i. Cliquez sur `Add Firewall Record`
        ii. Acceptez les valeurs par défaut en cliquant sur `Save`

Il est possible de basculer le site ISPConfig entièrement en Français. J'ai pour ma part gardé la version anglaise du site. Vous trouverez donc tous les libellés dans la suite de la documentation en anglais.

2. Aller dans la rubrique `DNS`
    a. Dans le menu `Template`
        i. Cliquez sur `Add new record`
        ii. Remplissez les champs comme ci-après:
            - `Name` ← Tapez `Template IPV4 autoNS`
            - `Fields` ← Cochez `Domain`, `IP Address`, `Email`, `DKIM`, `DNSSEC`
            - `Template` ← remplissez comme ci dessous:

```
[ZONE]
origin={DOMAIN}.
ns=ns1.{DOMAIN}.
mbox={EMAIL}.
refresh=7200
retry=540
expire=604800
minimum=3600
ttl=3600

[DNS_RECORDS]
A|{DOMAIN}.|{IP}|0|3600
A|www|{IP}|0|3600
A|mail|{IP}|0|3600
A|autoconfig|{IP}|0|3600
A|autodiscover|{IP}|0|3600
A|webmail|{IP}|0|3600
A|ns1|{IP}|0|3600
CNAME|ftp|{DOMAIN}|0|3600
CNAME|smtp|{DOMAIN}|0|3600
CNAME|pop3|{DOMAIN}|0|3600
CNAME|imap|{DOMAIN}|0|3600
SRV|_pop3._tcp|0 0 .|0|3600
SRV|_imap._tcp|0 0 .|0|3600
SRV|_pop3s._tcp|1 995 mail.{DOMAIN}|0|3600
SRV|_imaps._tcp|1 993 mail.{DOMAIN}|0|3600
SRV|_submission._tcp|1 465 mail.{DOMAIN}|0|3600
SRV|_autodiscover._tcp|1 443 autodiscover.{DOMAIN}|0|3600
NS|{DOMAIN}.|ns1.{DOMAIN}.|0|3600
MX|{DOMAIN}.|mail.{DOMAIN}.|10|3600
TXT|{DOMAIN}.|v=spf1 mx a ~all|0|3600
```

iii. Cliquez sur `Save`

iv. Cliquez sur `Add new record`

v. Remplissez les champs comme ci-après:

- `Name` ← Tapez `Template IPV6 autoNS`
- `Fields` ← Cochez `Domain`, `IP Address`, `IPV6 Address`, `Email`, `DKIM`, `DNSSEC`
- `Template` ← remplissez comme ci dessous:

```
[ZONE]
origin={DOMAIN}.
ns=ns1.{DOMAIN}.
mbox={EMAIL}.
refresh=7200
retry=540
expire=604800
minimum=3600
ttl=3600

[DNS_RECORDS]
A|{DOMAIN}.|{IP}|0|3600
A|www|{IP}|0|3600
A|mail|{IP}|0|3600
A|autoconfig|{IP}|0|3600
A|autodiscover|{IP}|0|3600
A|webmail|{IP}|0|3600
A|ns1|{IP}|0|3600
AAAA|{DOMAIN}.|{IPV6}|0|3600
AAAA|www|{IPV6}|0|3600
AAAA|mail|{IPV6}|0|3600
AAAA|autoconfig|{IPV6}|0|3600
AAAA|autodiscover|{IPV6}|0|3600
AAAA|webmail|{IPV6}|0|3600
AAAA|ns1|{IPV6}|0|3600
CNAME|ftp|{DOMAIN}|0|3600
CNAME|smtp|{DOMAIN}|0|3600
CNAME|pop3|{DOMAIN}|0|3600
CNAME|imap|{DOMAIN}|0|3600
SRV|_pop3._tcp|0 0 .|0|3600
SRV|_imap._tcp|0 0 .|0|3600
SRV|_pop3s._tcp|1 995 mail.{DOMAIN}|0|3600
SRV|_imaps._tcp|1 993 mail.{DOMAIN}|0|3600
SRV|_submission._tcp|1 465 mail.{DOMAIN}|0|3600
SRV|_autodiscover._tcp|1 443 autodiscover.{DOMAIN}|0|3600
NS|{DOMAIN}.|ns1.{DOMAIN}.|0|3600
MX|{DOMAIN}.|mail.{DOMAIN}.|10|3600
TXT|{DOMAIN}.|v=spf1 mx a ~all|0|3600
```

8.2. Création de la zone DNS d'un domaine

1. Allez dans `DNS`
   a. Cliquez sur `Add dns-zone`
   b. Cliquez sur `Dns zone wizard`
   c. Choisir le template `IPV4 autoNS` ou `IPV6 autoNS` selon que vous soyez IPV4 ou IPV4+V6
   d. Remplissez les champs:

- `Domain :` ← tapez le nom de votre domaine `example.com`
- `IP Address:` ← prendre l'adresse IPV4 du serveur sélectionnée
- `IPV6 Address:` ← prendre l'adresse IPV6 du serveur sélectionnée
- `Email:` ← votre Email valide exemple admin@example.com
- `DKIM:` ← Yes

Si votre serveur est chez vous, il est probablement installé derrière un routeur ADSL configuré au préalable avec une DMZ qui pointe sur ce serveur. Dans ce cas, vous ne devrez pas indiquer l'adresse IP locale de votre serveur mais l'adresse IP de votre routeur ADSL telle qu'elle est vue sur internet. On suppose aussi que cette adresse IP est statique et non pas allouée dynamiquement par l'opérateur.

e. Cliquez sur `Create DNS-record`

Attendez quelques minutes le temps que les enregistrements DNS se propagent et faites une essai de votre nom de domaine sur le site ZoneMaster.

Dans le champ Nom de domaine saisissez votre nom de domaine et tapez sur check. Tout doit est OK sauf pour les serveurs de noms ns1 et ns2. Si ce n'est pas le cas, votre nom de domaine doit être mal configuré chez votre registrar. Il vous faut vérifier la configuration initiale.

Zonemaster a bien repéré que l'on a essayé de mettre des noms de host différents pour les serveurs de DNS. Ils ont cependant tous la même adresse IP. Cela apparait comme une erreur suite au test. De la même manière, il indique dans la rubrique connectivité qu'il n'y a pas de redondance de serveur DNS. Une manière de corriger ce problème est de définir un DNS secondaire chez OVH en utilisant le service qu'ils mettent à disposition.

Vous pouvez maintenant essayer les différents Hostname munis de leur nom de domaine dans votre navigateur. Par exemple: http://webmail.example.com

Ils doivent afficher une page web basique (Apache2, ou de parking).Si ce n'est pas le cas revérifier la configuration du DNS dans ISPConfig.

8.3. Activation de DNSSEC

Vous pouvez maintenant activer DNSSEC afin d'augmenter la sécurité de résolution de nom de domaine:

1. Allez dans la rubrique `DNS`
   a. puis dans le menu `Zones`
   b. choisissez la zone correspondant à votre domaine
   c. dans l'onglet `DNS Zone` allez tout en bas et activer la coche `Sign Zone (DNSSEC)`
   d. cliquez sur `Save`

e. Une fois fait, retourner dans le même onglet. La boite `DNSSEC DS-Data for registry: `contient les informations que vous devez coller dans le site web de votre registrar pour sécuriser votre zone.

f. Gardez cette fenêtre ouverte dans votre navigateur et ouvrez un autre onglet sur le site de votre registrar.

Si vous êtes chez Gandi, il vous faut:

1. Sélectionner le menu `nom de domaine`
2. Choisir votre nom de domaine "example.com"
3. Allez dans l'onglet DNSSEC. Il doit permettre d'ajouter des clés puisque vous fonctionner avec des DNS externes.
4. Effacez éventuellement toutes les clés si vous n'êtes pas sur de celles-ci.
5. puis cliquez sur `Ajouter une clé externe`
   a. Sélectionnez d'abord le flag `257 (KSK)`. puis l'algorithme `7 (RSASHA1-NSEC3-SHA1)`
   b. Collez ensuite la clé de votre site ISPConfig. Elle doit ressembler à cela:

```
example.com. IN DNSKEY 257 3 7
AwEAAcs+xTC5GlyC8CSufM9U7z5uazLNmNP3vG2txzNIGM1VJHWCpRYQVZjsBZqx5vZuOFBwp0F6cpF8
YdW9QibZc82UAeIYAstgRSwnCLYsIV+3Zq0NpCcnGTkPLknxxZuN3MD5tARkxBM5c5fME0NgMU+kcx4x
aTVm2Go6bEeFuhgNfRogzXKqLV6h2bMCajudfJbbTbJlehym2YegLI+yYCpYr6b+jWHorRoUVDJ41OPX
Ltz2s8wtycyINpZsdmLNJhNNaeGqOok3+c5uazLNmNP3vG2txzNIGLM1VJHWCpRYQVZjsBZkqx5vZuOF
Bgwp0F6cpF8YdW9QbZc82UAeIYAstKgRSwnCLYsIV+3Zq0NpCcnGTkPLkn
```

   c. Cliquez sur `Ajouter`
   d. Entrez la deuxième clé. Cliquez sur `Ajouter une clé externe`
   e. Sélectionnez d'abord le flag `256 (ZSK)`. puis l'algorithme `7 (RSASHA1-NSEC3-SHA1)`
   f. Collez ensuite la clé de votre site ISPConfig. Elle doit ressembler à cela:

```
example.com. IN DNSKEY 256 3 7
AwEAAcs+xTC5GlyC8CSufM9U7z5uazLNmNP3vG2txzNIGM1VJHWCpRYQVZjsBZqx5vZuOFBwp0F6cpF8
YdW9QibZc82UAeIYAstgRSwnCLYsIV+3Zq0NpCcnGTkPLknxxZuN3MD5tARkxBM5c5fME0NgMU+kcx4x
aTVm2Go6bEeFuhgNfRogzXKqLV6h2bMCajudfJbbTbJlehym2YegLI+yYCpYr6b+jWHorRoUVDJ41OPX
Ltz2s8wtycyINpZsdmLNJhNNaeGqOok3+c5uazLNmNP3vG2txzNIGLM1VJHWCpRYQVZjsBZkqx5vZuOF
Bgwp0F6cpF8YdW9QbZc82UAeIYAstKgRSwnCLYsIV+3Zq0NpCcnGTkPLkn
```

   g. Cliquez sur `Ajouter`
   h. Les deux clés doivent maintenant apparaître dans l'onglet `DNSSEC`
   i. Vous devez attendre quelques minutes (une heure dans certains cas) pour que les clés se propagent. Pendant ce temps vous pouvez avoir quelques problèmes d'accès à vos sites webs
   j. Allez sur le site DNSSEC Analyzer.

k. Entrez votre nom de domaine "example.com" et tapez sur "entrée".

Le site doit afficher pour les différentes zones le statut des certificats. Tout doit être au vert. Si ce n'est pas le cas, réessayer dans une heure. S'il y a encore des problèmes vérifiez votre configuration dans ISPConfig, chez votre registrar (rubrique DNSSEC) ou regardez les logs d'ISPConfig sur votre serveur pour y débusquer une erreur.

Une erreur classique est de croiser les certificats avec leurs types. Vérifiez bien que vous avez mis les bons certificats avec les bons types.

Une fois que vous activez DNSSEC, vous pourriez faire face au problème suivant: les nouveaux enregistrements que vous renseignez ne sont pas actifs. Une analyse des logs montre que la commande `dnssec-signzone` retourne l'erreur `fatal: 'example.com': found DS RRset without NS RRset`. Cela signifie que vous avez saisi une ou deux entrées DS dans vos enregistrements. Il faut les supprimer pour que tout redevienne fonctionnel.

8.4. Exemple de configuration de domaine

Une fois la configuration terminé, les différents enregistrements du domaines ressemblent à l'exemple ci-dessous. Il peut y avoir des enregistrements supplémentaires pour les configurations SPF, DKIM et Let's encrypt.

```
example.com.          3600 A             1.2.3.4
www                   3600 A             1.2.3.4
mail                  3600 A             1.2.3.4
ns1                   3600 A             1.2.3.4
ns2                   3600 A             1.2.3.4
webmail               3600 A             1.2.3.4
autoconfig            3600 A             1.2.3.4
autodiscover          3600 A             1.2.3.4
ftp                   3600 CNAME         example.com.
smtp                  3600 CNAME         mail.example.com.
pop3                  3600 CNAME         mail.example.com.
imap                  3600 CNAME         mail.example.com.
example.com.          3600 NS            ns1.example.com.
example.com.          3600 NS            ns2.example.com.
example.com.          3600 MX    10      mail.example.com.
_pop3s._tcp           3600 SRV   10 1 995 mail.example.com.
_imaps._tcp           3600 SRV   0  1 993 mail.example.com.
_submission._tcp      3600 SRV   0  1 465 mail.example.com.
_imap._tcp            3600 SRV   0  0 0   .
_pop3._tcp            3600 SRV   0  0 0   .
_autodiscover._tcp    3600 SRV   0 0 443  autoconfig.example.com.
example.com.          3600 TXT           "v=spf1 mx a ~all"
```

8.5. Création d'un sous domaine

Supposons que vous êtes en train de créer un sous domain nommé sub.example.com . Dans ce sous domaines vous allez créer un ensemble de site web par exemple mail.sub.example.com ou blog.sub.example.com.

Un cas assez classique est que ce sous domaine est délégué à une machine tierce.

Par exemple: example.com est installé sur un VPS quelque part sur internet et sub.example.com est hébergé chez vous sur votre Raspberry.

On suppose que votre domain a été configuré en suivant la procédure du chapitre précédent.

Rien de bien sorcier pour votre sous domaine: Vous devez le créer sur votre Raspberry selon la même procédure mais avec le nom du sous domaine (sub.example.com donc).

Vous aurez des actions complémentaires à effectuer sur votre domaine:

1. Allez dans `DNS` de votre serveur de domaine principal
2. Sélectionner le menu `Zones` puis le domaine example.com
3. Choisissez l'onglet `Records` et créez:
   - un enregistrement de type `NS` avec une `Zone` ← `sub.example.com.` et un `nameserver Hostname` ← `ns1.sub.example.com.`
   - un enregistrement de type `NS` avec une `Zone` ← `sub.example.com.` et un `nameserver Hostname` ← `ns2.sub.example.com.`
   - un enregistrement de type `NS` avec une `Zone` ← `sub.example.com.` et un `nameserver Hostname` ← `ns3.example.com.` .

     Ce dernier type d'enregistrement se nomme un Glue record pour faire le lien vers le serveur secondaire.

   - un enregistrement de type `A` avec un `Hostname` ← ns3 et une `IP-address` ← Adresse IP de votre routeur ADSL ou est connecté le Raspberry.

     Ce dernier enregistrement en complétant le Glue record fait le lien avec l'adresse IP de sub.example.com
4. Si vous avez activé DNSSEC sur votre serveur DNS de sub.example.com vous devrez récupérer les entrées DS du champ `DNSSEC DS-Data for registry` de votre domaine sub.example.com et créer dans votre domaine example.com les deux entrées suivantes:
   - un enregistrement de type `DS` avec une `Zone` ← `sub.example.com` et un champ `data` contenant `xxxxx 7 1 <votre_digest_recupérée>`
   - un enregistrement de type `DS` avec une `Zone` ← `sub.example.com` et un champ `data` contenant `xxxxx 7 2 <votre_digest_recupérée>`

8.6. Création d'un site web

Dans la suite le site web sera nommé "example.com".

Vous devez avoir avant tout défini le "record" DNS associé au site.

1. Aller dans "Sites"
    a. Aller dans le menu "Website" pour définir un site web
        i. Cliquez sur "Add new website"
        ii. Saisissez les informations:
            - `Domain:` ← mettre `example.com`
            - `Auto-subdomain:` ← sélectionner `www` ou `*` si l'on veut un certificat let's encrypt wildcard
            - `SSL:` ← yes
            - `Let's Encrypt:` ← yes
            - `Php:` ← Sélectionez `php-fpm`
            - Sélectionnez éventuellement aussi les coches `Perl`, `Python`, `Ruby` en fonction des technologies déployées sur votre site. Cela est indiqué dans la procédure d'installation du site.
        iii. Dans l'onglet `redirect` du même écran
            - `SEO Redirect:` ← Sélectionner `domain.tld ⇒www.domain.tld`
            - `Rewrite http to https:` ← yes
        iv. Dans l'onglet `Statistics` du même écran
            - `Set Webstatistics password:` ← saisissez un mot de passe
            - `Repeat Password:` ← ressaisissez le mot de passe
        v. Dans l'onglet `Backup` du même écran
            - `Backup interval:` ← saisir `weekly`
            - `Number of backup copies:` ← saisir `1`
        vi. Dans l'onglet `Options`, il peut être utile pour certains types de site qui sont des redirections d'autres sites de saisir dans la zone `Apache Directives:`

```
ProxyPass "/.well-known/acme-challenge" http://localhost:80/.well-known/acme-challenge
ProxyPassReverse "/.well-known/acme-challenge" http://localhost:80/.well-known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# redirect from server
#

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / http://localhost[:port_number_if_any]/[path_if_any]
ProxyPassReverse / http://localhost[:port_number_if_any]/[path_if_any]
```

2. Vous pouvez maintenant tester la qualité de la connexion de votre site en allant sur: SSL Server Test. Saisissez votre nom de domaine et cliquez sur `Submit`. Votre site doit au moins être de `Grade A`.

8.7. Création d'un Site Vhost

Dans la suite le sous-domaine sera nommé "mail.example.com".

Vous devez avoir avant tout défini le "record" DNS associé au site. Vous ne pouvez définir un sous-domaine que si vous avez défini le site web racine auparavant.

1. Aller dans "Sites"
   a. Aller dans le menu "Subdomain(vhost)" pour définir un sous-domaine
      i. Cliquez sur "Add Subdomain" pour un nouveau sous domaine
      ii. Saisissez les informations:
         - `Hostname:` ← saisir `mail`
         - `Domain:` ← mettre `example.com`
         - `web folder:` ← saisir `mail`
         - `Auto-subdomain:` ← sélectionner `wwww` ou `*` si l'on veut un certificat let's encrypt wildcard
         - `SSL:` ← yes
         - `Let's Encrypt:` ← yes
         - `Php:` ← Sélectionez `php-fpm`
         - Sélectionnez éventuellement aussi les coches `Perl`, `Python`, `Ruby` en fonction des technologies déployées sur votre site. Cela est indiqué dans la procédure d'installation du site.
      iii. Dans l'onglet `redirect` du même écran
         - `Rewrite http to https:` ← yes
      iv. Dans l'onglet `Statistics` du même écran

- `Set Webstatistics password:` ← saisissez un mot de passe
- `Repeat Password:` ← ressaisissez le mot de passe

v. Dans l'onglet `Options`, il peut être utile pour certains types de site qui sont des redirections d'autres sites de saisir dans la zone `Apache Directives:`

```
ProxyPass "/.well-known/acme-challenge" http://localhost:80/.well-
known/acme-challenge
ProxyPassReverse "/.well-known/acme-challenge" http://localhost:80/.well-
known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# redirect from server
#

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / http://localhost[:port_number_if_any]/[path_if_any]
ProxyPassReverse / http://localhost[:port_number_if_any]/[path_if_any]
```

2. Vous pouvez maintenant tester la qualité de la connexion de votre site en allant sur: SSL Server Test. Saisissez votre nom de domaine et cliquez sur `Submit`. Votre site doit au moins être de `Grade A`.

Chapter 9. Associer des certificats reconnu à vos outils

Cette action est à effectuer une fois que vous avez créé votre domaine principal et que vous avez généré vos premiers certificats let's encrypt dans ISPConfig, vous pouvez maintenant, affecter ce certificat aux services de base:

1. Vous devez avoir créé au préalable un site pour les domaines example.com et mail.example.com
2. Loguez vous comme root sur le serveur
3. Liez le certificat d'ISPconfig avec celui du domaine crée.
    - Tapez :

```
cd /usr/local/ispconfig/interface/ssl/
mv ispserver.crt ispserver.crt-$(date +"%y%m%d%H%M%S").bak
mv ispserver.key ispserver.key-$(date +"%y%m%d%H%M%S").bak
ln -s /etc/letsencrypt/live/example.com/fullchain.pem ispserver.crt ①
ln -s /etc/letsencrypt/live/example.com/privkey.pem ispserver.key ①
cat ispserver.{key,crt} > ispserver.pem
chmod 600 ispserver.pem
systemctl restart apache2
```

① remplacer <example.com> par votre nom de domaine

4. Liez le certificat Postfix et Dovecot avec celui de let's encrypt
    - Tapez :

```
cd /etc/postfix/
mv smtpd.cert smtpd.cert-$(date +"%y%m%d%H%M%S").bak
mv smtpd.key smtpd.key-$(date +"%y%m%d%H%M%S").bak
ln -s /etc/letsencrypt/live/mail.example.com/fullchain.pem smtpd.cert ①
ln -s /etc/letsencrypt/live/mail.example.com/privkey.pem smtpd.key ①
service postfix restart
service dovecot restart
```

① remplacer <example.com> par votre nom de domaine

5. Liez le certificat pour Pureftd
    - Tapez :

```
cd /etc/ssl/private/
mv pure-ftpd.pem pure-ftpd.pem-$(date +"%y%m%d%H%M%S").bak
ln -s /usr/local/ispconfig/interface/ssl/ispserver.pem pure-ftpd.pem
chmod 600 pure-ftpd.pem
service pure-ftpd-mysql restart
```

6. Création d'un script de renouvellement automatique du fichier pem

   a. Installez incron. Tapez :

   ```
   apt install -y incron
   ```

   b. Créez le fichier d'exécution périodique. Tapez :

   ```
   vi /etc/init.d/le_ispc_pem.sh
   ```

   et coller dans le fichier le code suivant:

   ```
   #!/bin/sh
   ### BEGIN INIT INFO
   # Provides: LE ISPSERVER.PEM AUTO UPDATER
   # Required-Start: $local_fs $network
   # Required-Stop: $local_fs
   # Default-Start: 2 3 4 5
   # Default-Stop: 0 1 6
   # Short-Description: LE ISPSERVER.PEM AUTO UPDATER
   # Description: Update ispserver.pem automatically after ISPC LE SSL certs are
   renewed.
   ### END INIT INFO
   cd /usr/local/ispconfig/interface/ssl/
   mv ispserver.pem ispserver.pem-$(date +"%y%m%d%H%M%S").bak
   cat ispserver.{key,crt} > ispserver.pem
   chmod 600 ispserver.pem
   chmod 600 /etc/ssl/private/pure-ftpd.pem
   service pure-ftpd-mysql restart
   service monit restart
   service postfix restart
   service dovecot restart
   service apache2 restart
   exit 1
   ```

   c. Sauvez et quittez. Tapez ensuite:

   ```
   chmod +x /etc/init.d/le_ispc_pem.sh
   echo "root" >> /etc/incron.allow
   incrontab -e.
   ```

   et ajoutez les lignes ci dessous dans le fichier:

   ```
   /etc/letsencrypt/archive/example.com/ IN_MODIFY /etc/init.d/le_ispc_pem.sh ①
   ```

   ① Remplacer example.com par votre nom de domaine.

Chapter 10. Surveillance du serveur avec Munin et Monit

10.1. Note préliminaire

Installez tout d'abord les paquets indispensables pour faire fonctionner Munin avec Apache puis activez le module fcgid:

```
apt-get install apache2 libcgi-fast-perl libapache2-mod-fcgid
a2enmod fcgid
```

10.2. Installation et configuration de Munin

Suivez les étapes ci-après:

1. Installer le paquet Munin:

   ```
   apt-get install munin munin-node munin-plugins-extra logtail libcache-cache-perl
   ```

2. Votre configuration de Munin va utiliser une base de données MariaDB. Vous devez activer quelques plugins. Tapez:

   ```
   cd /etc/munin/plugins
   ln -s /usr/share/munin/plugins/mysql_ mysql_
   ln -s /usr/share/munin/plugins/mysql_bytes mysql_bytes
   ln -s /usr/share/munin/plugins/mysql_innodb mysql_innodb
   ln -s /usr/share/munin/plugins/mysql_isam_space_ mysql_isam_space_
   ln -s /usr/share/munin/plugins/mysql_queries mysql_queries
   ln -s /usr/share/munin/plugins/mysql_slowqueries mysql_slowqueries
   ln -s /usr/share/munin/plugins/mysql_threads mysql_threads
   ```

3. Créez la base de données MariaDB de Munin. Tapez:

   ```
   mysql -p
   ```

4. Tapez le mot de passe mysql de root , puis dans mysql tapez:

```
CREATE SCHEMA munin_innodb;
USE munin_innodb
CREATE TABLE something (anything int) ENGINE=InnoDB;
GRANT SELECT ON munin_innodb.* TO 'munin'@'localhost' IDENTIFIED BY 'munin';
FLUSH PRIVILEGES;
EXIT;
```

5. Editez ensuite le fichier de configuration de Munin. Tapez:

```
vi /etc/munin/munin.conf
```

6. Décommentez les lignes débutant par: `bdir`, `htmldir`, `logdir`, `rundir`, and `tmpldir`. Les valeurs par défaut sont correctes.
7. Munin utilisera l'adresse `munin.example.com`. Toujours dans le fichier de configuration de munin, remplacer la directive `[localhost.localdomain]` par `[munin.example.com]`.
8. Un fois les commentaires enlevés et la ligne modifiée, le fichier de configuration doit ressembler à celui-ci:

```
# Example configuration file for Munin, generated by 'make build'
# The next three variables specifies where the location of the RRD
# databases, the HTML output, logs and the lock/pid files. They all
# must be writable by the user running munin-cron. They are all
# defaulted to the values you see here.
#
dbdir /var/lib/munin
htmldir /var/cache/munin/www
logdir /var/log/munin
rundir /var/run/munin
# Where to look for the HTML templates
#
tmpldir /etc/munin/templates
# Where to look for the static www files
#
#staticdir /etc/munin/static
# temporary cgi files are here. note that it has to be writable by
# the cgi user (usually nobody or httpd).
#
# cgitmpdir /var/lib/munin/cgi-tmp

# (Exactly one) directory to include all files from.
includedir /etc/munin/munin-conf.d
[...]
# a simple host tree
[server1.example.com]
 address 127.0.0.1
 use_node_name yes
[...]
```

9. Activez Munin dans Apache. Tapez:

```
a2enconf munin
```

10. Editez le fichier munin.conf d'Apache:

```
vi /etc/apache2/conf-enabled/munin.conf
```

11. Nous allons maintenant activer le module Munin dans Apache et définir une authentification basique.
12. Modifiez le fichier pour qu'il ressemble à celui ci-dessous:

```
ScriptAlias /munin-cgi/munin-cgi-graph /usr/lib/munin/cgi/munin-cgi-graph
Alias /munin/static/ /var/cache/munin/www/static/

<Directory /var/cache/munin/www>
    Options FollowSymLinks SymLinksIfOwnerMatch
    AuthUserFile /etc/munin/munin-htpasswd
    AuthName "Munin"
    AuthType Basic
    Require valid-user

</Directory>

<Directory /usr/lib/munin/cgi>
    AuthUserFile /etc/munin/munin-htpasswd
    AuthName "Munin"
    AuthType Basic
    Require valid-user
    Options FollowSymLinks SymLinksIfOwnerMatch
    <IfModule mod_fcgid.c>
        SetHandler fcgid-script
    </IfModule>
    <IfModule !mod_fcgid.c>
        SetHandler cgi-script
    </IfModule>
</Directory>

# ***** SETTINGS FOR CGI/CRON STRATEGIES *****

# pick _one_ of the following lines depending on your "html_strategy"
# html_strategy: cron (default)
Alias /munin /var/cache/munin/www
# html_strategy: cgi (requires the apache module "cgid" or "fcgid")
#ScriptAlias /munin /usr/lib/munin/cgi/munin-cgi-html
```

13. Créez ensuite le fichier de mot de passe de munin:

```
htpasswd -c /etc/munin/munin-htpasswd admin
```

14. Tapez votre mot de passe
15. Redémarrez apache. Tapez:

```
service apache2 restart
```

16. Redémarrez Munin. Tapez:

```
service munin-node restart
```

17. Attendez quelques minutes afin que Munin produise ses premiers fichiers de sortie. et allez ensuite sur l'URL: http://example.com/munin/.

10.3. Activez les plugins de Munin

Dans Debian 10, tous les plugins complémentaires sont déjà activés.Vous pouvez être tenté de vérifier:

1. Pour vérifier que la configuration est correcte. Tapez:

```
munin-node-configure --suggest
```

2. Une liste de plugins doit s'afficher à l'écran. La colonne `used` indique que le plugins est activé. La colonne `Suggestions` indique que le serveur fait fonctionner un service qui peut être monitoré par ce module. Il faut créer un lien symbolique du module de `/usr/share/munin/plugins` dans `/etc/munin/plugins` pour l'activer.
3. Par exemple pour activer les modules apache_*:

```
cd /etc/munin/plugins
ln -s /usr/share/munin/plugins/apache_accesses
ln -s /usr/share/munin/plugins/apache_processes
ln -s /usr/share/munin/plugins/apache_volume
rm /usr/share/munin/plugins/mysql_
```

4. Redémarrez ensuite le service Munin. Tapez:

```
service munin-node restart
```

10.4. Installer et configurer Monit

Pour installer et configurer Monit, vous devez appliquer la procédure suivante:

1. Tapez:

```
apt install monit
```

2. Maintenant nous devons éditer le fichier `monitrc` qui définira les services que l'on souhaite monitorer. Il existe de nombreux exemples sur le web et vous pourrez trouver de nombreuses configuration sur http://mmonit.com/monit/documentation/.
3. Editez le fichier monitrc. Tapez:

```
cp /etc/monit/monitrc /etc/monit/monitrc_orig
vi /etc/monit/monitrc
```

4. Le fichier contient déjà de nombreux exemples. Nous configurer une surveillance de sshd, apache, mysql, proftpd, postfix, memcached, named, ntpd, mailman, amavisd, dovecot. Monit sera activé sur le port 2812 et nous allons donner à l'utilisateur admin un mot de passe. Le certificat HTTPS sera celui généré avec let's encrypt pour le site ISPConfig. Collez le contenu ci dessous dans le fichier monitrc:

```
set daemon 60
set logfile syslog facility log_daemon
set mailserver localhost
set mail-format { from: monit@fpvview.site }
set alert stef@fpvview.site
set httpd port 2812 and
 SSL ENABLE
 PEMFILE /usr/local/ispconfig/interface/ssl/ispserver.pem
 allow admin:"my_password" ①

check process sshd with pidfile /var/run/sshd.pid
 start program "/usr/sbin/service ssh start"
 stop program "/usr/sbin/service ssh stop"
 if failed port 22 protocol ssh then restart
 if 5 restarts within 5 cycles then timeout

check process apache with pidfile /var/run/apache2/apache2.pid
 group www
 start program = "/usr/sbin/service apache2 start"
 stop program = "/usr/sbin/service apache2 stop"
 if failed host localhost port 80 protocol http
 and request "/monit/token" then restart
 if cpu is greater than 60% for 2 cycles then alert
 if cpu > 80% for 5 cycles then restart
 if totalmem > 500 MB for 5 cycles then restart
 if children > 250 then restart
 if loadavg(5min) greater than 10 for 8 cycles then stop
 if 3 restarts within 5 cycles then timeout

#
---------------------------------------------------------------------------
----------
# NOTE: Replace example.pid with the pid name of your server, the name depends on
the hostname
#
---------------------------------------------------------------------------
----------
check process mysql with pidfile /var/run/mysqld/mysqld.pid
 group database
 start program = "/usr/sbin/service mysql start"
```

```
 stop program = "/usr/sbin/service mysql stop"
 if failed host 127.0.0.1 port 3306 then restart
 if 5 restarts within 5 cycles then timeout

check process pureftpd with pidfile /var/run/pure-ftpd/pure-ftpd.pid
 start program = "/usr/sbin/service pure-ftpd-mysql start"
 stop program = "/usr/sbin/service pure-ftpd-mysql stop"
 if failed port 21 protocol ftp then restart
 if 5 restarts within 5 cycles then timeout

check process postfix with pidfile /var/spool/postfix/pid/master.pid
 group mail
 start program = "/usr/sbin/service postfix start"
 stop program = "/usr/sbin/service postfix stop"
 if failed port 25 protocol smtp then restart
 if 5 restarts within 5 cycles then timeout

check process memcached with pidfile /var/run/memcached/memcached.pid
 start program = "/usr/sbin/service memcached start"
 stop program = "/usr/sbin/service memcached stop"
 if failed host 127.0.0.1 port 11211 then restart

check process named with pidfile /var/run/named/named.pid
 start program = "/usr/sbin/service bind9 start"
 stop program = "/usr/sbin/service bind9 stop"
 if failed host 127.0.0.1 port 53 type tcp protocol dns then restart
 if failed host 127.0.0.1 port 53 type udp protocol dns then restart
 if 5 restarts within 5 cycles then timeout

check process ntpd with pidfile /var/run/ntpd.pid
 start program = "/usr/sbin/service ntp start"
 stop program = "/usr/sbin/service ntp stop"
 if failed host 127.0.0.1 port 123 type udp then restart
 if 5 restarts within 5 cycles then timeout

check process mailman with pidfile /var/run/mailman/mailman.pid
 group mail
 start program = "/usr/sbin/service mailman start"
 stop program = "/usr/sbin/service mailman stop"

check process amavisd with pidfile /var/run/amavis/amavisd.pid
 group mail
 start program = "/usr/sbin/service amavis start"
 stop program = "/usr/sbin/service amavis stop"
 if failed port 10024 protocol smtp then restart
 if 5 restarts within 5 cycles then timeout

check process dovecot with pidfile /var/run/dovecot/master.pid
 group mail
 start program = "/usr/sbin/service dovecot start"
 stop program = "/usr/sbin/service dovecot stop"
```

```
  if failed host localhost port 993 type tcpssl sslauto protocol imap then restart
  if 5 restarts within 5 cycles then timeout
```

① remplacez my_password par votre mot de passe

5. La configuration est assez claire à lire. pour obtenir des précisions, référez vous à la documentation de monit http://mmonit.com/monit/documentation/monit.html.
6. Dans la configuration pour apache, la configuration indique que monit doit allez chercher sur le port 80 un fichier dans `/monit/token`. Nous devons donc créer ce fichier. Tapez:

```
mkdir /var/www/html/monit
echo "hello" > /var/www/html/monit/token
```

7. Tapez :

```
service monit restart
```

8. Pour monitorer le statut des process en ligne de commande, tapez:

```
monit status
```

9. Débloquez le port 2812 dans votre firewall
   a. Allez sur le site ispconfig https://example.com:8080/
   b. Loguez-vous et cliquez sur la rubrique `System` et le menu `Firewall`. Cliquez sur votre serveur.
   c. dans la rubrique `Open TCP ports:`, ajoutez le port 2812
   d. Cliquez sur `save`
10. Maintenant naviguez sur le site https://example.com:2812/
11. Rentrez le login `admin` et votre mot de passe `my_password`. Monit affiche alors les informations de monitoring du serveur.

Chapter 11. Configuration de la messagerie

11.1. Installation de rspamd à la place d' Amavis-new

`rspamd` est réputé de meilleure qualité que `Amavis` dans la chasse aux spams. Vous pouvez décider de l'installer à la place d'Amavis. Cette installation reste optionnelle.

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur
2. Installez les paquets debian. tapez:

```
apt-get install rspamd redis-server
```

3. Activez l'apprentissage automatique

```
echo "autolearn = true;" > /etc/rspamd/local.d/classifier-bayes.conf
echo 'backend = "redis";' >> /etc/rspamd/local.d/classifier-bayes.conf
echo "new_schema = true;" >> /etc/rspamd/local.d/classifier-bayes.conf
echo "expire = 8640000;" >> /etc/rspamd/local.d/classifier-bayes.conf
```

4. Activez Redis dans la configuration de Rspamd. Tapez:

```
echo 'servers = "127.0.0.1";' > /etc/rspamd/local.d/redis.conf
```

5. Fixer des métriques assez élevées pour analyser les spams

```
echo "actions {" > /etc/rspamd/local.d/metrics.conf
echo 'add_header = 5;' >> /etc/rspamd/local.d/metrics.conf
echo "greylist = 25;" >> /etc/rspamd/local.d/metrics.conf
echo "reject = 50;" >> /etc/rspamd/local.d/metrics.conf
echo "}" >> /etc/rspamd/local.d/metrics.conf
```

6. Augmentez la taille de l'historique de Rspamd, activez la compression.

```
echo "nrows = 2500;" > /etc/rspamd/local.d/history_redis.conf
echo "compress = true;" >> /etc/rspamd/local.d/history_redis.conf
echo "subject_privacy = false;" >> /etc/rspamd/local.d/history_redis.conf
```

7. Activez la mise à jour automatique de rspamd

```
echo 'enabled = true;' > /etc/rspamd/local.d/redis.conf
```

8. Enrichissez les headers des mails spams. Tapez:

```
vi /etc/rspamd/local.d/milter_headers.conf
```

9. inserez le texte suivant:

```
# local.d/milter_headers.conf:

# Options

# Add "extended Rspamd headers" (default false) (enables x-spamd-result, x-rspamd-
server & x-rspamd-queue-id routines)
extended_spam_headers = true;

# List of headers to be enabled for authenticated users (default empty)
# authenticated_headers = ["authentication-results"];

# List of headers to be enabled for local IPs (default empty)
local_headers = ["x-spamd-bar"];

# Set false to always add headers for local IPs (default true)
# skip_local = true;

# Set false to always add headers for authenticated users (default true)
# skip_authenticated = true;

# Routines to use- this is the only required setting (may be omitted if using
extended_spam_headers)
use = ["x-spamd-bar", "x-spam-level", "authentication-results"];

# this is where we may configure our selected routines
routines {
  # settings for x-spamd-bar routine
  x-spamd-bar {
    # effectively disables negative spambar
    negative = "";
  }
  # other routines...
}
custom {
  # user-defined routines: more on these later
}
```

10. Créez un mot de passe. Tapez:

```
rspamadm pw
```

11. Entrez votre mot de passe. Une hashphrase est générée.
12. Copiez la.
13. Remplacez celle déjà présente dans `/etc/rspamd/local.d/worker-controller.inc`

```
vi /etc/rspamd/local.d/worker-controller.inc
```

14. Remplacez le texte entre guillemets sur la ligne `password = "$2$g95yw……dq3c5byy";` par le texte copié.
15. Sauvez
16. Redémarrez Rspamd

```
systemctl restart rspamd
```

17. Loguez vous dans ISPConfig
18. Activer Rspamd dans ISPConfig
    a. Allez dans la rubrique `system` → menu `Server Config` → Sélectionnez votre serveur → Onglet `Mail`
    b. Dans le champ `Content Filter`, sélectionnez `Rspamd`
    c. Dans le champ `Rspamd Password`, tapez votre mot de passe
    d. Cliquez sur `Save`
    e. Revenez dans la rubrique `system` → menu `Server Config` → Sélectionnez votre serveur → Onglet `Mail`
    f. Vous pouvez voir le mot de passe de connexion au serveur web Rspamd.
19. Rendre le site rspamd accessible dans un host
20. Activez le module proxy dans apache

```
a2enmod proxy
systemctl restart apache2
```

21. Allez dans la rubrique `DNS`, sélectionnez le menu `Zones`, Sélectionnez votre Zone, Allez dans l'onglet `Records`.
    a. Cliquez sur `A` et saisissez:
        - `Hostname:` ← Tapez `rspamd`
        - `IP-Address:` ← Double cliquez et sélectionnez l'adresse IP de votre serveur
    b. Cliquez sur `Save`
22. Créer un sub-domain (vhost) dans le configurateur de `sites`.
    a. Lui donner le nom `rspamd`.
    b. Le faire pointer vers le web folder `rspamd`.

c. Activer let's encrypt ssl

d. Activer `Fast CGI` pour PHP

e. Laisser le reste par défaut.

f. Dans l'onglet Options:

g. Dans la boite `Apache Directives:` saisir le texte suivant:

```
ProxyPass "/.well-known/acme-challenge" http://localhost:80/.well-known/acme-
challenge
ProxyPassReverse "/.well-known/acme-challenge" http://localhost:80/.well-
known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# rspamd httpserver
#

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / http://localhost:11334/
ProxyPassReverse / http://localhost:11334/
```

23. en pointant sur le site rspampd.example.com, et en utilisant le mot de passe saisi plus haut vous pouvez accèder aux fonctions de l'outil.

24. Activer l'apprentissage par déplacement

    a. Couplé avec Dovecot, Rspamd nous propose de pouvoir apprendre également en fonction des actions des utilisateurs. Si un mail est déplacé vers le répertoire Junk, il sera appris comme tel et au contraire, s'il est sorti du répertoire Junk vers autre chose que la corbeille, il sera appris comme Ham.

    b. Editez le fichier Dovecot.conf (remarques ISPConfig n'utilise pas aujourd'hui le contenu du répertoire conf.d). Tapez:

```
vi /etc/dovecot/dovecot.conf
```

    c. Insérez dans le groupe plugin et le protocol imap déjà existants dans le fichier :

```
plugin {
  sieve_plugins = sieve_imapsieve sieve_extprograms

  imapsieve_mailbox1_name = Junk
  imapsieve_mailbox1_causes = COPY
  imapsieve_mailbox1_before = file:/etc/dovecot/sieve/report-spam.sieve

  imapsieve_mailbox2_name = *
  imapsieve_mailbox2_from = Junk
  imapsieve_mailbox2_causes = COPY
  imapsieve_mailbox2_before = file:/etc/dovecot/sieve/report-ham.sieve

  sieve_pipe_bin_dir = /etc/dovecot/sieve

  sieve_global_extensions = +vnd.dovecot.pipe
}

protocol imap {
  mail_plugins = quota imap_quota imap_sieve
}
```

d. Redémarrez dovecot. Tapez:

```
service dovecot restart
```

e. Créez un répertoire sieve et éditez report-ham.sieve. Tapez:

```
mkdir -p /etc/dovecot/sieve/
vi /etc/dovecot/sieve/report-ham.sieve
```

f. Insérez le texte suivant:

```
require ["vnd.dovecot.pipe", "copy", "imapsieve", "environment", "variables"];

if environment :matches "imap.mailbox" "*" {
set "mailbox" "${1}";
}

if string "${mailbox}" "Trash" {
stop;
}

if environment :matches "imap.email" "*" {
set "email" "${1}";
}

pipe :copy "train-ham.sh" [ "${email}" ];
```

g. Editez report-spam.sieve. Tapez:

```
vi /etc/dovecot/sieve/report-spam.sieve
```

h. Insérez le texte suivant:

```
require ["vnd.dovecot.pipe", "copy", "imapsieve", "environment", "variables"];

if environment :matches "imap.email" "*" {
set "email" "${1}";
}

pipe :copy "train-spam.sh" [ "${email}" ];
```

i. Créez les scripts et rétablissez les droits et permissions. Compilez les règles. Tapez:

```
echo "exec /usr/bin/rspamc learn_ham" > /etc/dovecot/sieve/train-ham.sh
echo "exec /usr/bin/rspamc learn_spam" > /etc/dovecot/sieve/train-spam.sh
sievec /etc/dovecot/sieve/report-ham.sieve
sievec /etc/dovecot/sieve/report-spam.sieve
chmod +x /etc/dovecot/sieve/train-*
chown -R vmail:vmail /etc/dovecot/sieve
```

j. Redémarrez dovecot. Tapez:

```
service dovecot restart
```

k. Lorsque vous déplacer un mail du répertoire Inbox vers le répertoire Junk ou vice-versa, les fichiers `/var/log/mail.log` et `/var/log/rspamd/rspamd.log` doivent montrer les actions de

recalcul des spams.

25. Enfin, vous pouvez désactiver amavisd si vous le souhaitez. tapez:

```
systemctl stop amavisd-new
systemctl disable amavisd-new
```

11.2. Création du serveur de messagerie

Pour créer un serveur de messagerie:

1. Assurez vous d'avoir créé le domaine DNS. Si ce n'est pas le cas déroulez tout d'abord la procédure de création de domaines
2. Aller dans la rubrique `Email`. Sélectionnez ensuite le menu `Domain`
3. Cliquez sur `Add new Domain`
4. Saisissez le nom de domaine.
5. Cliquez sur `DomainKeys Indentified Mail (DKIM)`
6. Cliquez sur `enable DKIM`
7. Cliquez sur `Generate DKIM Private-key`
8. Une fois cela fait, retourner dans la gestion des `Records` de domaine et activer le type DMARC
9. Garder le paramétrage par défaut et sauvegardez.
10. Faites de même pour les enregistrements SPF mais sélectionnez le mécanisme softfail.
11. Votre serveur est créé et protégé Contre les spams (entrants et sortants).

11.3. Finaliser la sécurisation de votre serveur de mail

Afin de mieux sécuriser votre serveur de mail, appliquez les opérations suivantes:

1. editez le fichier main.cf

```
vi /etc/postfix/main.cf
```

2. Rechercher `myhostname` et replacer le texte par:

```
myhostname = mail.example.com ①
```

① Remplacer example.com par votre nom de domaine.

3. Redémarrez Postfix. Tapez:

```
service postfix restart
```

4. Vous pouvez le tester en allant sur le site MxToolbox.
    - Entrez le nom de host de votre serveur de mail: mail.example.com .
    - cliquez sur `test Email Server`
    - Tout doit être correct sauf éventuellement le reverse DNS qui doit être configuré pour pointer vers mail.example.com .

11.4. Création de l'autoconfig pour Thunderbird et Android

La procédure est utilisé par Thunderbird et Android pour configurer automatiquement les paramètres de la messagerie.

Appliquez la procédure suivante:

1. Créer un sub-domain (vhost) dans le configurateur de sites.
    a. Lui donner le nom `autoconfig`.
    b. Le faire pointer vers le web folder `autoconfig`.
    c. Activer let's encrypt ssl
    d. Activer `php-FPM`
    e. Laisser le reste par défaut.
    f. Dans l'onglet Options:
    g. Dans la boite `Apache Directives:` saisir le texte suivant:

```
AddType application/x-httpd-php .php .php3 .php4 .php5 .xml

CheckSpelling On
CheckCaseOnly Off
```

    h. Sauver.
2. Loguez vous comme root sur le serveur
3. Dans le répertoire `/var/www/autoconfig.example.com/autoconfig/` créer un répertoire mail. Lui donner les permissions 755 et affecter les mêmes possesseurs que pour autres fichiers du répertoire. Tapez:

```
mkdir -p /var/www/autoconfig.example.com/autoconfig/mail
chmod 755 /var/www/autoconfig.example.com/autoconfig/mail
chown web1:client0 /var/www/autoconfig.example.com/autoconfig/mail ①
```

① remplacer web1:client0 par les permissions du répertoire `/var/www/autoconfig.example.com`

    a. A l'intérieur de ce répertoire, Editez un fichier `config-v1.1.xml`. Tapez:

```
vi /var/www/autoconfig.example.com/autoconfig/mail/config-v1.1.xml
```

4. Y coller:

```
<?php
header('Content-Type: application/xml');
?>
<?xml version="1.0" encoding="UTF-8"?>

<clientConfig version="1.1">
 <emailProvider id="example.com"> ①
   <domain>example.com</domain>
   <displayName>Example Mail</displayName> ②
   <displayShortName>Example</displayShortName> ③
   <incomingServer type="imap">
     <hostname>mail.example.com</hostname> ①
     <port>993</port>
     <socketType>SSL</socketType>
     <authentication>password-cleartext</authentication>
     <username>%EMAILADDRESS%</username>
   </incomingServer>
   <incomingServer type="pop3">
     <hostname>mail.example.com</hostname> ①
     <port>995</port>
     <socketType>SSL</socketType>
     <authentication>password-cleartext</authentication>
     <username>%EMAILADDRESS%</username>
   </incomingServer>
   <outgoingServer type="smtp">
     <hostname>mail.example.com</hostname> ①
     <port>465</port>
     <socketType>SSL</socketType>
     <authentication>password-cleartext</authentication>
     <username>%EMAILADDRESS%</username>
   </outgoingServer>
   <outgoingServer type="smtp">
     <hostname>mail.example.com</hostname> ①
     <port>587</port>
     <socketType>STARTTLS</socketType>
     <authentication>password-cleartext</authentication>
     <username>%EMAILADDRESS%</username>
   </outgoingServer>
 </emailProvider>
</clientConfig>
```

① mettre à la place de example.com votre nom de domaine

② mettre ici votre libellé long pour votre nom de messagerie

③ mettre ici un libellé court pour votre nom de messagerie

5. Donner la permission en lecture seule et affecter les groupes d'appartenance. Tapez:

```
chmod 644 /var/www/autoconfig.example.com/autoconfig/mail/config-v1.1.xml
chown web1:client0 /var/www/autoconfig.example.com/autoconfig/mail/config-v1.1.xml
①
```

① remplacer web1:client0 par les permissions du répertoire `/var/www/autoconfig.example.com`

11.5. Création d'autodiscover pour Outlook

Outlook utilise un autre mécanisme pour se configurer automatiquement. Il est basé sur l'utilisation du nom de sous-domaine `autodiscover`.

Appliquez la procédure suivante:

1. Créer un sub-domain (vhost) dans le configurateur de sites.
   a. Lui donner le nom `autodiscover`.
   b. Le faire pointer vers le web folder `autodiscover`.
   c. Activer let's encrypt ssl
   d. Activer `php-FPM`
   e. Laisser le reste par défaut.
   f. Dans l'onglet Options:
   g. Dans la boite `Apache Directives:` saisir le texte suivant:

```
CheckSpelling On
CheckCaseOnly On
RewriteEngine On
ProxyPass "/" http://autoconfig.example.com/ ①
ProxyPassReverse "/" http://autoconfig.example.com/ ①
RewriteRule ^/ - [QSA,L]
```

① remplacer example.com par votre nom de domaine

   h. Sauver.
2. Loguez vous comme root sur le serveur
3. Dans le répertoire `/var/www/autoconfig.example.com/autoconfig/`, créer un répertoire `Autodiscover`. Lui donner les permissions 755 et affecter les mêmes possesseurs que pour autres fichiers du répertoire. Tapez:

```
mkdir -p /var/www/autoconfig.example.com/autoconfig/Autodiscover/
chmod 755 /var/www/autoconfig.example.com/autoconfig/Autodiscover/
chown web1:client0 /var/www/autoconfig.example.com/autoconfig/Autodiscover/ ①
```

① remplacer web1:client0 par les permissions du répertoire `/var/www/autoconfig.example.com`

a. A l'intérieur de ce répertoire, Editez un fichier `Autodiscover.xml`. Tapez:

```
vi /var/www/autoconfig.example.com/autoconfig/Autodiscover/Autodiscover.xml
```

4. Y coller:

```
<?php
 $raw = file_get_contents('php://input');
 $matches = array();
 preg_match('/<EMailAddress>(.*)<\/EMailAddress>/', $raw, $matches);
 header('Content-Type: application/xml');
?>
 <Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
   <Response
xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/20
06a">
     <User>
       <DisplayName>Example Mail</DisplayName> ②
     </User>
     <Account>
       <AccountType>email</AccountType>
       <Action>settings</Action>
       <Protocol>
         <Type>IMAP</Type>
         <Server>mail.example.com</Server> ①
         <Port>993</Port>
         <DomainRequired>off</DomainRequired>
         <SPA>off</SPA>
         <SSL>on</SSL>
         <AuthRequired>on</AuthRequired>
         <LoginName><?php echo $matches[1]; ?></LoginName>
       </Protocol>
       <Protocol>
         <Type>SMTP</Type>
         <Server>mail.example.com</Server> ①
         <Port>465</Port>
         <DomainRequired>off</DomainRequired>
         <SPA>off</SPA>
         <SSL>on</SSL>
         <AuthRequired>on</AuthRequired>
         <LoginName><?php echo $matches[1]; ?></LoginName>
       </Protocol>
     </Account>
   </Response>
 </Autodiscover>
```

① mettre à la place de example.com votre nom de domaine

② mettre ici votre libellé long pour votre nom de messagerie

5. Changez les permissions comme pour le répertoire

```
chmod 644 /var/www/autoconfig.example.com/autoconfig/Autodiscover/Autodiscover.xml
chown web1:client0
/var/www/autoconfig.example.com/autoconfig/Autodiscover/Autodiscover.xml ①
```

① remplacer web1:client0 par les permissions du répertoire `/var/www/autoconfig.example.com`

6. Pointer votre navigateur sur le site https://autodiscover.example.com/Autodiscover/Autodiscover.xml.
7. Le contenu du fichier xml doit s'afficher
8. Vous pouvez faire aussi un test sur le Testeur de connectivité Microsoft.
   a. choisissez: `Découverte automatique Outlook`
   b. cliquez sur `suivant`
   c. Entrez votre adresse de courrier: `user@example.com`, un domain: `example\user`, un mot de passe tiré au hazard, Cochez les deux cases en dessous.
   d. Cliquez sur `effectuer un test`
   e. Le résultat doit être: `Test de connectivité réussi`

11.6. Création d'une boite mail

Pour créer une boite de messagerie:

1. Aller dans la rubrique `Email`. Sélectionnez ensuite le menu `Email Mailbox`
2. Cliquez sur `Add new Mailbox`
3. Remplissez les champs suivants:
   a. `Name:` ← mettez votre prénom et votre nom
   b. `Email:` ← mail_name @ example.com
   c. `Password:` ← saisissez un mot de passe ou générez en un
   d. `Repeat Password` ← saisissez une deuxième fois votre mot de passe
   e. `Quota (0 for unlimited):` ← mettez éventuellement un quota ou laissez 0 pour illimité.
   f. `Spamfilter:` ← Sélectionnez `Normal`
4. Dans l'onglet Backup:
   a. `Backup interval:` Sélectionnez `Daily`
   b. `Number of backup copies:` Sélectionnez 1
5. Cliquez sur `Save`

Notez que si vous créez une adresse mail nommée mail_name@example.com, vous pouvez utilisez toutes les variantes (nommées tag) derrière le caractère "+". Ainsi mail_name+nospam@example.com sera bien redirigé vers votre boite et l'extension +nospam vous permettre de trier automatiquement les mails que vous ne voulez pas recevoir.

Il est possible de changer ce caractère spécial en le modifiant dans le fichier `/etc/postfix/main.cf` sur la ligne commençant par `recipient_delimiter`.

11.7. Configuration de votre client de messagerie.

Saisir l'adresse mail et votre mot de passe doit suffire pour configurer automatiquement votre client de messagerie.

Si vous avez besoin de configurer votre client manuellement, voici les informations à saisir:

Paramètre	**Valeur**
Type de serveur	IMAP
Nom de serveur IMAP	mail.example.com
Nom d'utilisateur IMAP	user@example.com
Port IMAP	993
Sécurité IMAP	SSL/TLS
Authentification IMAP	Normal Password
Nom de serveur SMTP	mail.example.com
Nom d'utilisateur SMTP	user@example.com
Port SMTP	465
Sécurité SMTP	SSL/TLS
Authentification SMTP	Normal Password

11.8. Mise en oeuvre du site web de webmail

On suppose que vous avez install roundcube lors de la procédure d'installation initiale et que vous avez déjà créé le host mail.example.com.

Il vous reste à appliquer la procédure suivante:

1. Créer un sub-domain (vhost) dans le configurateur de sites.
    a. Lui donner le nom `mail`.
    b. Le faire pointer vers le web folder `mail`.
    c. Activer let's encrypt ssl
    d. Activer `Fast CGI` pour PHP
    e. Laisser le reste par défaut.
    f. Dans l'onglet Options:
    g. Dans la boite `Apache Directives:` saisir le texte suivant:

```
ProxyPass "/.well-known/acme-challenge" http://localhost:80/.well-known/acme-challenge
ProxyPassReverse "/.well-known/acme-challenge" http://localhost:80/.well-known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# roundcube httpserver

SSLProxyEngine On
SSLProxyCheckPeerCN Off
SSLProxyCheckPeerName Off
SSLProxyVerify none

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / https://localhost:8080/webmail/
ProxyPassReverse / https://localhost:8080/webmail/
ProxyPreserveHost On
```

2. C'est fait, vous pouvez accéder à Roundcube directement sur https://mail.example.com

11.9. Transfert de vos boites mails IMAP

Si vous faites une migration d'un ancien serveur vers un nouveau serveur vous souhaiterez probablement migrer aussi vos boites mail.

La procédure ci dessous est à appliquer pour chaque compte mail IMAP. Elle peut facilement être scriptée:

1. Téléchargez imapsync du repository. Tapez:

```
wget https://raw.githubusercontent.com/imapsync/imapsync/master/imapsync
chmod 755 imapsync
```

2. Installez les packages perls éventuellement manquants:

```
apt install libregexp-common-perl libfile-tail-perl libsys-meminfo-perl libunicode-string-perl libmail-imapclient-perl libio-tee-perl libio-socket-inet6-perl libfile-copy-recursive-perl
```

3. Créez deux fichiers temporaires qui contiennent les mots de passe du 1er et 2eme serveur. Tapez:

```
echo "passwdsrc" > secretsrc ①
echo "passwddst" > secretdst ②
chmod 600 secretsrc
chmod 600 secretdst
```

① passwdsrc est à remplacer par le mot de passe du compte sur le serveur source

② passwddst est à remplacer par le mot de passe du compte sur le serveur destination

4. Nous pouvons maintenant lancer la commande. Tapez:

```
./imapsync --host1 imap.examplesrc.com --user1 usersrc@examplesrc.com --passfile1
/etc/secretsrc --host2 imap.exampledst.com --user2 userdst@exampledst.com
--passfile2 /etc/secretdst
```

5. Un fois la synchronisation effectuée, vous pouvez supprimer le fichier des mots de passe. tapez:

```
rm secretsrc
rm secretdst
```

11.10. Annexe

11.11. Configuration d'un écran 3.5inch RPi LCD (A)

11.11.1. Pour commencer

Le RPi LCD peut être piloté de deux manières :

1. installer le pilote sur votre Raspbian OS.
2. utiliser le fichier image prêt à l'emploi ou lle pilote LCD est préinstallé.
3. Téléchargez la dernière image sur le site web de Raspberry Pi et écrivez-la sur la carte SD.
4. Connectez l'écran LCD RPi à Raspberry Pi et connectez le Pi au réseau.
5. Configurez votre Pi :

```
sudo raspi-config
```

6. configurez ainsi :
   - Sélectionnez "Expand Filesystem".
   - Boot Option → Desktop Autologin (peut différer selon la révision Raspbian)
7. Ouvrez le terminal du Raspberry Pi (Vous devrez peut-être connecter un clavier et un écran LCD HDMI à Pi pour l'installation du pilote). Tapez:

```
git clone https://github.com/waveshare/LCD-show.git
cd LCD-show/
```

Note: Une connexion réseau est nécessaire lors de l'installation du pilote sur votre Pi, sinon l'installation ne fonctionnera pas correctement.

```
chmod +x LCD35-show
./LCD35-show
```

8. Après le redémarrage du système, le RPi LCD est prêt à l'emploi.

11.11.2. Basculer entre l'affichage LCD et HDMI

Une fois que l'écran LCD est activé, les paramètres par défaut pour HDMI sont modifiés. Si vous souhaitez utiliser un autre moniteur HDMI, veuillez exécuter la commande suivante :

```
cd LCD-show/
./LCD-hdmi
```

Cela permet de basculer le mode sur l'affichage LCD :

```
chmod +x LCD35-show
./LCD35-show
```

11.11.3. Paramètres d'orientation de l'écran

Une fois le pilote tactile installé, l'orientation de l'écran peut être définie par ces commandes :

- Rotation de 0 degrés

```
cd LCD-show/
./LCD35-show 0
```

- Rotation de 90 degrés

```
cd LCD-show/
./LCD35-show 90
```

- Rotation de 180 degrés

```
cd LCD-show/
./LCD35-show 180
```

- Rotation de 270 degrés

```
cd LCD-show/
./LCD35-show 270
```

11.11.4. Calibrage de l'écran tactile

Cet écran LCD peut être calibré à l'aide d'un programme appelé `xinput_calibrator` . Il n'est pas préinstallé sur le système d'exploitation Raspbian original. Vous devez donc le télécharger et installer le programme manuellement.

```
sudo apt-get install -y xinput-calibrator
```

Entrez les commandes suivantes pour le calibrage de l'écran tactile :

```
sudo DISPLAY=:0.0 xinput_calibrator
```

ou Sélectionnez Menu → Preferences → Calibrate Touchscreen.

Après l'exécution de ces commandes, l'écran LCD affiche une invite pour un calibrage en quatre points. Cliquez sur les points un par un pour terminer le calibrage tactile. Ensuite, les nouvelles données de calibrage seront affichées dans le terminal, comme indiqué ci-dessous. Veuillez obtenir ces données pour une utilisation ultérieure.

```
Doing dynamic recalibration:
Setting new calibration data: 3919, 208, 236, 3913
```

Tapez la commande suivante pour éditer 99-calibration.conf:

```
sudo nano /etc/X11/xorg.conf.d/99-calibration.conf
```

Ensuite, les anciennes données d'étalonnage seront affichées dans le terminal :

```
Section "InputClass"
Identifier  "calibration"
MatchProduct    "ADS7846 Touchscreen"
Option  "Calibration"   "160 3723 3896 181"
Option  "SwapAxes"  "1"
EndSection
```

Modifiez les données d'étalonnage en fonction des nouvelles données d'étalonnage affichées plus haut :

```
Section "InputClass"
Identifier  "calibration"
MatchProduct    "ADS7846 Touchscreen"
Option  "Calibration"   "3919 208 236 3913"
Option  "SwapAxes"  "1"
EndSection
```

Appuyez sur les touches Ctrl+X, et sélectionnez l'option Y pour enregistrer la modification.

La modification sera valide après le redémarrage du système. Entrez la commande suivante pour le redémarrage du système :

```
sudo reboot
```

Notices: En cas de toucher imprécis, veuillez procéder à un nouvel étalonnage de l'écran et redémarrer le système.

11.11.5. Installer un clavier virtuel

1. Installer matchbox-keyboard

   ```
   sudo apt-get install update
   sudo apt-get install matchbox-keyboard
   sudo nano /usr/bin/toggle-matchbox-keyboard.sh
   ```

2. Copiez les commandes ci-dessous dans toggle-matchbox-keyboard.sh et sauvegardez.

   ```
   #!/bin/bash
   #This script toggle the virtual keyboard
   PID=`pidof matchbox-keyboard`
   if [ ! -e $PID ]; then
   killall matchbox-keyboard
   else
   matchbox-keyboard -s 50 extended&
   fi
   ```

3. Exécutez les commandes:

   ```
   sudo chmod +x /usr/bin/toggle-matchbox-keyboard.sh
   sudo mkdir /usr/local/share/applications
   sudo nano /usr/local/share/applications/toggle-matchbox-keyboard.desktop
   ```

4. Copiez les commandes ci-dessous dans toggle-matchbox-keyboard.desktop et sauvegardez.

```
[Desktop Entry]
Name=Toggle Matchbox Keyboard
Comment=Toggle Matchbox Keyboard`
Exec=toggle-matchbox-keyboard.sh
Type=Application
Icon=matchbox-keyboard.png
Categories=Panel;Utility;MB
X-MB-INPUT-MECHANSIM=True
```

5. Exécutez les commandes ci dessous.

   NOTE: Notez que vous devez utiliser les droits d'utilisateur "Pi" au lieu de root pour exécuter cette commande

```
nano ~/.config/lxpanel/LXDE-pi/panels/panel
```

6. Trouvez la déclaration qui est similaire à celle ci-dessous : (Elle peut être différente dans une autre version)

```
Plugin {
  type = launchbar
  Config {
    Button {
      id=lxde-screenlock.desktop
    }
    Button {
      id=lxde-logout.desktop
    }
  }
}
```

7. Ajoutez ces déclarations pour ajouter une option de bouton :

```
Button {
  id=/usr/local/share/applications/toggle-matchbox-keyboard.desktop
}
```

8. redémarrez votre Raspberry Pi. Si le clavier virtuel est correctement installé, vous pouvez constater qu'il y a une icône de clavier sur la gauche de la barre

```
sudo reboot
```

11.11.6. Ressources

Manuel utilisateur

- RPiLCD User Manual

Images

Description : si vous avez eu du mal à installer le pilote, essayez l'image avec le pilote préinstallé.

- RPi-35inch-LCD-(A)-Raspbian-180326.7z

Driver

Le pilote peut être téléchargé sur github

```
git clone https://github.com/waveshare/LCD-show.git
```

Fichiers de configuration de référence

/boot/cmdline.txt

```
dwc_otg.lpm_enable=0 console=tty1 console=ttyAMA0,115200 root=/dev/mmcblk0p7
rootfstype=ext4 elevator=deadline rootwait fbcon=map:10 fbcon=font:ProFont6x11
logo.nologo
```

/boot/config.txt

```
# For more options and information see
# http://www.raspberrypi.org/documentation/configuration/config-txt.md
# Some settings may impact device functionality. See link above for details

# uncomment if you get no picture on HDMI for a default "safe" mode
#hdmi_safe=1

# uncomment this if your display has a black border of unused pixels visible
# and your display can output without overscan
#disable_overscan=1

# uncomment the following to adjust overscan. Use positive numbers if console
# goes off screen, and negative if there is too much border
#overscan_left=16
#overscan_right=16
#overscan_top=16
#overscan_bottom=16

# uncomment to force a console size. By default it will be display's size minus
# overscan.
```

```
#framebuffer_width=1280
#framebuffer_height=720

# uncomment if hdmi display is not detected and composite is being output
hdmi_force_hotplug=1

# uncomment to force a specific HDMI mode (this will force VGA)
#hdmi_group=1
#hdmi_mode=1

# uncomment to force a HDMI mode rather than DVI. This can make audio work in
# DMT (computer monitor) modes
#hdmi_drive=2

# uncomment to increase signal to HDMI, if you have interference, blanking, or
# no display
#config_hdmi_boost=4

# uncomment for composite PAL
#sdtv_mode=2

#uncomment to overclock the arm. 700 MHz is the default.
#arm_freq=800

# Uncomment some or all of these to enable the optional hardware interfaces
dtparam=i2c_arm=on
#dtparam=i2s=on
dtparam=spi=on
enable_uart=1
# Uncomment this to enable the lirc-rpi module
#dtoverlay=lirc-rpi

# Additional overlays and parameters are documented /boot/overlays/README

# Enable audio (loads snd_bcm2835)
dtparam=audio=on
dtoverlay=tft35a
#dtoverlay=ads7846,cs=1,penirq=17,penirq_pull=2,speed=1000000,keep_vref_on=1,swapxy=1,
pmax=255,xohms=60,xmin=200,xmax=3900,ymin=200,ymax=3900
```

/etc/inittab

Ajouter:

```
#Spawn a getty on Raspberry Pi serial line
T0:23:respawn:/sbin/getty -L ttyAMA0 115200 vt100
```

/usr/share/X11/xorg.conf/99-fbturbo.conf

```
Section "Device"
        Identifier      "Allwinner A10/A13/A20 FBDEV"
        Driver          "fbturbo"
        Option          "fbdev" "/dev/fb1"

        Option          "SwapbuffersWait" "true"
EndSection
```

/usr/share/X11/xorg.conf.d/40-libinput.conf /usr/share/X11/xorg.conf.d/45-evdev.conf

```
Section "InputClass"
        Identifier "libinput pointer catchall"
        MatchIsPointer "on"
        MatchDevicePath "/dev/input/event*"
        Driver "libinput"
EndSection

Section "InputClass"
        Identifier "libinput keyboard catchall"
        MatchIsKeyboard "on"
        MatchDevicePath "/dev/input/event*"
        Driver "libinput"
EndSection

Section "InputClass"
        Identifier "libinput touchpad catchall"
        MatchIsTouchpad "on"
        MatchDevicePath "/dev/input/event*"
        Driver "libinput"
EndSection

Section "InputClass"
        Identifier "libinput touchscreen catchall"
        MatchIsTouchscreen "on"
        MatchDevicePath "/dev/input/event*"
        Driver "libinput"
EndSection

Section "InputClass"
        Identifier "libinput tablet catchall"
        MatchIsTablet "on"
        MatchDevicePath "/dev/input/event*"
        Driver "libinput"
EndSection
```

/etc/X11/xorg.conf.d/99-calibration.conf

```
Section "InputClass"
        Identifier      "calibration"
        MatchProduct    "ADS7846 Touchscreen"
        Option  "Calibration"   "3936 227 268 3880"
        Option  "SwapAxes"      "1"
EndSection
```