Installation d’un VPS

Stéphane Apiou

Version 1.0, 2020-03-27

Table of Contents

1. Avant propos . . . 1
2. Choix du VPS . . . 3
3. Choix du registrar . . . 4
4. Se loguer root sur le serveur . . . 5
5. Installation basique . . . 6
   5.1. Mise à jour des sources de paquets Debian . . . 6
   5.2. Installation des paquets de base . . . 6
   5.3. Installation d'un repository pour `/etc` . . . 7
   5.4. Installer l'outil Debfoster . . . 8
   5.5. Création d'un fichier keeper dans /etc . . . 9
   5.6. Installation des mises à jours automatiques . . . 10
   5.7. Vérification du nom de serveur . . . 11
   5.8. Interdire le login direct en root . . . 12
   5.9. Création d'une clé de connexion ssh locale . . . 13
   5.10. Sudo sans mot de passe . . . 15
   5.11. Installer l'outil dselect . . . 15
   5.12. Ajouter un fichier de swap . . . 16
6. Installation initiale des outils . . . 17
   6.1. Configuration de Postfix . . . 17
   6.2. Configuration de MariaDB . . . 18
   6.3. Configuration d'Apache . . . 20
   6.4. Installation et Configuration de Mailman . . . 20
   6.5. Configuration d' Awstats . . . 22
   6.6. Configuration de Fail2ban . . . 22
   6.7. Installation et configuration de PureFTPd . . . 23
   6.8. Installation et configuration de phpmyadmin . . . 24
   6.9. Installation et configuration de Roundcube . . . 27
   6.10. Installation de Let's Encrypt . . . 28
   6.11. Installation d'un scanner de vulnérabilités . . . 28
7. Installation d'un Panel . . . 30
   7.1. Installation de Webmin . . . 30
   7.2. Installation et configuration de ISPConfig . . . 32
8. Configuration d'un domaine . . . 35
   8.1. Login initial . . . 35
   8.2. Création de la zone DNS d'un domaine . . . 35
   8.3. Ajout d'enregistrements DNS . . . 36
   8.4. Activation de DNSSEC . . . 37
   8.5. Exemple de configuration de domaine . . . 38

8.6. Création d’un site web . . . 39
8.7. Création d’un Site Vhost . . . 40
8.8. Associer des certificats reconnu à vos outils . . . 41
9. Surveillance du serveur avec Munin et Monit . . . 44
9.1. Note préliminaire . . . 44
9.2. Installation et configuration de Munin . . . 44
9.3. Activez les plugins de Munin . . . 47
9.4. Installer et configurer Monit . . . 47
10. Configuration de la messagerie . . . 51
10.1. Installation de rspamd à la place d' Amavis-new . . . 51
10.2. Création du serveur de messagerie . . . 53
10.3. Création de l’autoconfig pour Thunderbird et Android . . . 54
10.4. Création d’autodiscover pour Outlook . . . 56
10.5. Création d’une boite mail . . . 58
10.6. Configuration de votre client de messagerie. . . . 58
10.7. Mise en oeuvre du site web de webmail . . . 59
10.8. Transfert de vos boites mails IMAP . . . 60
11. Installation de Joomla . . . 62
11.1. Création du site web de Joomla . . . 62
11.2. Création de l’application Joomla . . . 62
12. Installation de Mediawiki . . . 64
12.1. Création du site web de Mediawiki . . . 64
12.2. Création de l’application Mediawiki . . . 64
13. Installation de Wordpress . . . 66
13.1. Création du site web de Wordpress . . . 66
13.2. Création de l’application Wordpress . . . 66
14. Pritunl . . . 68
15. Installation et configuration de Gitea . . . 69
15.1. Création du site web de Gitea . . . 69
15.2. Création des bases de données . . . 70
15.3. Téléchargez et installez Gitea . . . 71
15.4. Activer une connexion SSH dédiée . . . 72
16. Installation de Seafile . . . 74
16.1. Création du site web de Seafile . . . 74
16.2. Création de bases de données . . . 75
16.3. Téléchargez et installez Seafile . . . 76
16.4. Lancement initial . . . 77
16.5. Lancement automatique de Seafile . . . 78
17. Installation d’un serveur de VPN Pritunl . . . 81
17.1. Création du site web de Pritunl . . . 81
17.2. Installation de Pritunl . . . 82

17.3. Configuration de Pritunl 82
17.4. Se connecter au serveur de VPN 84
17.5. Réparer une base Pritunl 84
17.6. Mot de passe perdu 85
18. Annexe 86
18.1. Installation de Hestia 86

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 un serveur VPS sur la plate-forme OVH. 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 ou à Ubuntu ou toute autre distribution basée sur l'un ou l'autre. En revanche si vous utilisez CentOS, il y aura des différences beaucoup plus importantes notamment liées au gestionnaire de paquets `yum`, le nommage des paquets, les configurations par défaut et aux différences dans l'arborescence présente dans /etc.

Dans ce document, je configure de nombreux sites web et services de mon domaine en utilisant ISPConfig.

Sont installés:

- un panel ISPConfig
- un configurateur Webmin
- 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 sous Joomla,
- un site Mediawiki,
- un site Wordpress
- un site Gitea et son repository GIT,
- un serveur et un site de partage de fichiers Seafile,
- un serveur de VPN pritunl,
- un site Nextcloud
- à venir: concrete5, gitlab, piwigo, borg

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.

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 et 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) * Compter 5€TTC/mois pour un VPS de base. Une machine plus sérieuse sera à 15€/mois

Le budget est donc de 6-7€TTC/mois pour une offre d'entrée de gamme. Il faut plus sérieusement compter sur 16€/mois tout compris.

Chapter 2. Choix du VPS

Cette partie du guide s'adresse aux utilisateurs d'OVH. J'ai pour ma part choisi un serveur VPS SSD chez OVH avec 2Go de RAM. Au moment ou j'écris ce document il possède un seul coeur et 20 Go de disque.

Choisissez d'installer une image Linux seule avec Debian 10. Une fois l'installation effectuée, vous recevez un Email sur l'adresse mail de votre compte OVH avec vos identifiants de login root. Ils serviront à vous connecter sur le serveur.

En vous loguant sur la plateforme d'administration d'OVH, vous accèderez aux informations de votre serveur dans le menu Server→VPS. A cet endroit votre VPS doit y être indiqué.

En cliquant dessus un ensemble de menus doivent apparaitre pour administrer celui-ci. Vous y trouverez notamment:

- Son adresse <IP> et le nom de la machine chez OVH. Elle est du type "VPSxxxxxx.ovh.net".
- La possibilité de le redémarrer
- La possibilité de le reinstaller (avec perte complète de données)
- un KVM pour en prendre le controle console directement dans le navigateur
- un menu de configuration de reverse DNS (qui nous sera utile par la suite) pour définir le domaine par défaut
- le statut des services principaux (http, ftp, ssh ...)
- enfin des choix pour souscrire à un backup régulier, ajouter des disques ou effecter un snapshot de la VM associée au VPS.

Chapter 3. 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.

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

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 de votre VPS (pour ovh: VPSxxxxxx.ovh.net).

   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. Installation basique

5.1. Mise à jour des sources de paquets Debian

1. Se loguer `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`
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
   ```

5.2. Installation des paquets de base

Tapez:

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

5.3. 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. Tapez :

```
apt install etckeeper
```

2. 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`).
3. 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

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

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

5. 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"
```

6. 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
```

7. Effectuez un premier push. Tapez:

```
git push -u origin master
```

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

```
etckeeper commit
```

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

5.4. 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. Se loguer `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

5.5. 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 systeme:

1. Loguez vous comme `root`
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`

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

6. Le fichier keepers est créé et sauvegardé automatiquement.

5.6. 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
```

5.7. Vérification du nom de serveur

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

1. Se loguer `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. Se loguer`root` de nouveau 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
      ```

      Changez la ou les lignes, sauvegardez et rebootez. Tapez :

```
reboot
```

b. Se logger `root` de nouveau 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.

5.8. 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. Se loguer `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.`

5.9. 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. 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

3. 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.

5.10. 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. 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 -G sudo <sudo_username>
```

   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`

5.11. Installer l'outil dselect

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

1. Se loguer `root` sur le serveur
2. Ajouter le paquet `dselect`. Tapez :

```
apt install dselect
```

5.12. Ajouter un fichier de swap

Pour un serveur VPS de 2 Go de RAM, la taille du fichier de swap sera de 1 Go:

1. Tapez:

```
fallocate -l 1G /swapfile
chmod 600 /swapfile
mkswap /swapfile
swapon /swapfile
```

2. Enfin ajoutez une entrée dans le fichier fstab. Tapez `vi /etc/fstab` et ajoutez la ligne:

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

Chapter 6. Installation initiale des outils

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

1. Se loguer `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 amavisd-new spamassassin clamav clamav-daemon
   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 php7.3 php7.3-common
   php7.3-gd php7.3-mysql php7.3-imap php7.3-cli php7.3-cgi libapache2-mod-fcgid
   apache2-suexec-pristine php-pear mcrypt  imagemagick libruby libapache2-mod-
   python php7.3-curl php7.3-intl php7.3-pspell php7.3-recode php7.3-sqlite3
   php7.3-tidy php7.3-xmlrpc php7.3-xsl memcached php-memcache php-imagick php-
   gettext php7.3-zip php7.3-mbstring memcached libapache2-mod-passenger php7.3-
   soap php7.3-fpm php7.3-opcache php-apcu bind9 dnsutils haveged webalizer awstats
   geoip-database libclass-dbi-mysql-perl libtimedate-perl fail2ban ufw anacron
   ```

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`

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.

   b. `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. Désactiver SpamAssassin puisque amavisd utilise celui ci en sous jacent. Tapez :

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

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
```

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: :

```
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` et `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
```

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;` puis tapez `FLUSH PRIVILEGES;` 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. 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';
```

3. 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
```

4. 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
```

6.11. Installation d'un scanner de vulnérabilités

1. installer Git. Tapez :

```
apt install git
```

2. installer Lynis
   a. Tapez :

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

   b. Executez :

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

3. 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 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. Se logger `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 `root` sur 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)`

7.2. 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. Tapez:

```
cd /tmp
```

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

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

4. Décompressez la version en tapant: :

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

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

```
cd ispconfig3_install/install/
```

6. 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. une deuxième série de question du même type est posée répondre de la même manière !

7. 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. Se loguer `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`

f. Régénérez la configuration des serveurs web. Allez dans `Tools` → `Resync`. Sélectionnez `Websites`.cliquez sur `start`

8. 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

9. 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.

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/ .

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

1. Aller dans l'onglet `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

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.

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 par défaut.
    d. Remplissez les champs:
        - `Domain :` ← tapez le nom de votre domaine `example.com`
        - `IP Address:` ← prendre l'adresse du serveur sélectionnée
        - `NS1 :` ← ns1.example.com
        - `NS2 :` ← ns2.example.com

- `Email:` ← votre Email valide exemple admin@example.com
- `DKIM:` ← Yes

e. Cliquez sur `Create DNS-record`

8.3. Ajout d'enregistrements DNS

Allez maintenant dans l'onglet `Records` de la zone DNS. J'y ai ajouté quelques enregistrements complémentaires:

1. Des enregistrements de type A (définissent des domaines principaux) :
   - `Hostname:` ← `autoconfig` et `IP-Address:` ← <IP> de votre serveur
   - `Hostname:` ← `autodicover` et `IP-Address:` ← <IP> de votre serveur
   - `Hostname:` ← `webmail` et `IP-Address:` ← <IP> de votre serveur
2. Des enregistrements de type CNAME (définissent des alias de domaines) :
   - `Hostname:` ← `ftp` et `IP-Address:` ← `example.com`
   - `Hostname:` ← `smtp` et `IP-Address:` ← `example.com`
   - `Hostname:` ← `pop3` et `IP-Address:` ← `example.com`
   - `Hostname:` ← `imap` et `IP-Address:` ← `example.com`
3. Des enregistrements de type SRV (définissent des services) :
   - `Hostname:` ← `_pop3._tcp`, `Target:` ← `.`, `Weight:` ← 0, `Port:` ← 0
   - `Hostname:` ← `_imap._tcp`, `Target:` ← `.`, `Weight:` ← 0, `Port:` ← 0
   - `Hostname:` ← `_pop3s._tcp`, `Target:` ← `mail.example.com`, `Weight:` ← 1, `Port:` ← 995, `Priority:` ← 10
   - `Hostname:` ← `_imaps._tcp`, `Target:` ← `mail.example.com`, `Weight:` ← 1, `Port:` ← 993
   - `Hostname:` ← `_submission._tcp`, `Target:` ← `mail.example.com`, `Weight:` ← 1, `Port:` ← 465
   - `Hostname:` ← `_autodiscover._tcp`, `Target:` ← `autoconfig.example.com`, `Weight:` ← 0, `Port:` ← 443

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.

8.4. 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.

8.5. 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"
```

8.6. 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 `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
            - `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://127.0.0.1:80/.well-
known/acme-challenge
ProxyPassReverse "/.well-known/acme-challenge" http://127.0.0.1:80/.well-
known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# redirect from server
#

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / http://127.0.0.1[:port_number_if_any]/[path_if_any]
ProxyPassReverse / http://127.0.0.1[: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 "site.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 `site`
         - `Domain:` ← mettre `example.com`
         - `web folder:` ← saisir `site`
         - `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

- 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://127.0.0.1:80/.well-
known/acme-challenge
ProxyPassReverse "/.well-known/acme-challenge" http://127.0.0.1:80/.well-
known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# redirect from server
#

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / http://127.0.0.1[:port_number_if_any]/[path_if_any]
ProxyPassReverse / http://127.0.0.1[: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.

8.8. Associer des certificats reconnu à vos outils

Comme vous avec créé votre premier domaine avec SSL et 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
2. 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

3. 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
ln -s /etc/letsencrypt/live/mail.example.com/privkey.pem smtpd.key
service postfix restart
service dovecot restart
```

4. 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
```

5. 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 9. Surveillance du serveur avec Munin et Monit

9.1. Note préliminaire

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

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

9.2. Installation et configuration de Munin

Suivez les étapes ci-après:

1. Installer le paquet Munin:

   ```
   apt-get install munin munin-node munin-plugins-extra
   ```

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

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

4. Décommentez les lignes débutant par: `bdir`, `htmldir`, `logdir`, `rundir`, and `tmpldir`. Les valeurs par défaut sont correctes.

5. Munin utilisera l'adresse `munin.example.com`. Toujours dans le fichier de configuration de munin, remplacer la directive `[localhost.localdomain]` par `[munin.example.com]`.

6. 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
[...]
```

7. Activez Munin dans Apache. Tapez:

```
a2enconf munin
```

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

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

9. Nous allons maintenant activer le module Munin dans Apache et définir une authentification basique.
10. 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
```

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

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

12. Tapez votre mot de passe
13. Redémarrez apache. Tapez:

```
service apache2 restart
```

14. Redémarrez Munin. Tapez:

```
service munin-node restart
```

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

9.3. 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 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
```

4. Redémarrez ensuite le service Munin. Tapez:

```
service munin-node restart
```

9.4. 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 proftpd 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 10. Configuration de la messagerie

10.1. 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 sur le serveur en tant que `root`
2. Installez les paquets debian. tapez:

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

   Activez Redis dans la configuration de Rspamd. Tapez:

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

3. 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
   ```

4. Créez un mot de passe:

   ```
   rspamadm pw
   ```

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

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

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

    ```
    systemctl restart rspamd
    ```

11. Loguez vous dans ISPConfig
12. 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. Cliquez sur `Save`
    d. Revenez dans la rubrique `system` → menu `Server Config` → Sélectionnez votre serveur → Onglet `Mail`
    e. Vous pouvez voir le mot de passe de connexion au serveur web Rspamd.
13. Rendre le site rspamd accessible dans un host
14. Activez le module proxy dans apache

```
a2enmod proxy
systemctl restart apache2
```

15. 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`
16. 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://127.0.0.1:80/.well-known/acme-challenge
ProxyPassReverse "/.well-known/acme-challenge" http://127.0.0.1:80/.well-known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# rspamd httpserver
#

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / http://127.0.0.1:11334/
ProxyPassReverse / http://127.0.0.1:11334/
```

17. 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.
18. Enfin, vous pouvez désactiver amavisd si vous le souhaitez. tapez:

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

10.2. 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).
12. 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 ne doit pas pointer sur le nom

de domaine.

10.3. 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 sur le serveur en tant que `root`
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/
chmod 755 /var/www/autoconfig.example.com/autoconfig/
chown web1:client0 /var/www/autoconfig.example.com/autoconfig/ 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/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> ①
   <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-encrypted</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-encrypted</authentication>
     <username>%EMAILADDRESS%</username>
   </outgoingServer>
   <outgoingServer type="smtp">
     <hostname>mail.example.com</hostname> ①
     <port>587</port>
     <socketType>STARTTLS</socketType>
     <authentication>password-encrypted</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 600 /var/www/autoconfig.example.com/autoconfig/config-v1.1.xml
chown web1:client0 /var/www/autoconfig.example.com/autoconfig/config-v1.1.xml ①
```

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

10.4. 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 sur le serveur en tant que `root`
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. Pointer votre navigateur sur le site https://autodiscover.example.com/Autodiscover/Autodiscover.xml.
6. Le contenu du fichier xml doit s'afficher
7. 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`

10.5. 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 @ votre_domaine
    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`

10.6. 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

Paramètre	Valeur
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

10.7. 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://127.0.0.1:80/.well-known/acme-challenge
ProxyPassReverse "/.well-known/acme-challenge" http://127.0.0.1:80/.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

10.8. 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
```

Chapter 11. Installation de Joomla

Joomla est un CMS très connu écrit en PHP. Il est fréquemment mis à jour.

L'installation s'effectue à 100% avec ISPConfig.

11.1. Création du site web de Joomla

Appliquez les opérations suivantes Dans ISPConfig:

1. 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 `joomla`
      - `IP-Address:` ← Double cliquez et sélectionnez l'adresse IP de votre serveur
   b. Cliquez sur `Save`
2. Créer un sub-domain (vhost) dans le configurateur de sites.
   a. Lui donner le nom `joomla`.
   b. Le faire pointer vers le web folder `joomla`.
   c. Activer let's encrypt ssl
   d. Activer `PHP-FPM` pour PHP
   e. Laisser le reste par défaut.

11.2. Création de l'application Joomla

Appliquez les opérations suivantes dans ISPConfig:

1. Allez dans la rubrique `Sites`, le menu `Update Packagelist`.
2. Cliquez sur `Update Packagelist`
3. Allez dans la rubrique `Sites`, le menu `Available packages`.
4. Faites une recherche par `Name`. Tapez `joomla`
5. Cliquez sur le package `joomla`
6. Cliquez sur `Install this package`
7. Remplissez tous les champs:
   - `Install location:` ← choisissez votre domain (`example.com`) et laissez vide le chemin.
   - `New database password` ← gardez ce qui est remplit
   - `Administrator's login` ← gardez ce qui est remplit: `admin`
   - `Password` et `Repeat Password` ← Tapez votre mot de passe
   - `Default site language:` ← choisissez `French`

    - `I accept the license` ← cochez la case
8. Cliquez sur `Install`
9. Pointez votre navigateur sur https://example.com/ et loguez vous `admin` avec votre mot de passe saisi, c'est fait !
10. N'oubliez pas d'administrer le site et de le mettre à jour avec la dernière version de Joomla.

Chapter 12. Installation de Mediawiki

Mediawiki est le portail wiki mondialement connu et utilisé notamment pour le site wikipedia.

L'installation s'effectue à 100% avec ISPConfig.

12.1. Création du site web de Mediawiki

Appliquez les opérations suivantes Dans ISPConfig:

1. 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 `mediawiki`
      - `IP-Address:` ← Double cliquez et sélectionnez l'adresse IP de votre serveur
   b. Cliquez sur `Save`
2. Créer un sub-domain (vhost) dans le configurateur de sites.
   a. Lui donner le nom `mediawiki`.
   b. Le faire pointer vers le web folder `mediawiki`.
   c. Activer let's encrypt ssl
   d. Activer `PHP-FPM` pour PHP
   e. Laisser le reste par défaut.

12.2. Création de l'application Mediawiki

Appliquez les opérations suivantes dans ISPConfig:

1. Allez dans la rubrique `Sites`, le menu `Update Packagelist`.
2. Cliquez sur `Update Packagelist`
3. Allez dans la rubrique `Sites`, le menu `Available packages`.
4. Faites une recherche par `Name`. Tapez `mediawiki`
5. Cliquez sur le package `mediawiki`
6. Cliquez sur `Install this package`
7. Remplissez tous les champs:
   - `Install location:` ← choisissez votre domain (`example.com`) et laissez vide le chemin.
   - `New database password` ← gardez ce qui est remplit
   - `Administrator's login` ← gardez ce qui est remplit: `admin`
   - `Password` et `Repeat Password` ← Tapez votre mot de passe
   - `Default site language:` ← choisissez `French`

    - `I accept the license` ← cochez la case
8. Cliquez sur `Install`
9. Pointez votre navigateur sur https://example.com/ et loguez vous `admin` avec votre mot de passe saisi, c'est fait !
10. N'oubliez pas d'administrer le site et de le mettre à jour avec la dernière version de Mediawiki.

Chapter 13. Installation de Wordpress

Wordpress est un CMS très connu écrit en PHP. Il est fréquemment mis à jour.

L'installation s'effectue à 100% avec ISPConfig.

13.1. Création du site web de Wordpress

Appliquez les opérations suivantes Dans ISPConfig:

1. 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 `wordpress`
      - `IP-Address:` ← Double cliquez et sélectionnez l'adresse IP de votre serveur
   b. Cliquez sur `Save`
2. Créer un sub-domain (vhost) dans le configurateur de sites.
   a. Lui donner le nom `wordpress`.
   b. Le faire pointer vers le web folder `wordpress`.
   c. Activer let's encrypt ssl
   d. Activer `PHP-FPM` pour PHP
   e. Laisser le reste par défaut.

13.2. Création de l'application Wordpress

Appliquez les opérations suivantes dans ISPConfig:

1. Allez dans la rubrique `Sites`, le menu `Update Packagelist`.
2. Cliquez sur `Update Packagelist`
3. Allez dans la rubrique `Sites`, le menu `Available packages`.
4. Faites une recherche par `Name`. Tapez `wordpress`
5. Cliquez sur le package `wordpress`
6. Cliquez sur `Install this package`
7. Remplissez tous les champs:
   - `Install location:` ← choisissez votre domain (`example.com`) et laissez vide le chemin.
   - `New database password` ← gardez ce qui est remplit
   - `Administrator s login` ← gardez ce qui est remplit: `admin`
   - `Password` et `Repeat Password` ← Tapez votre mot de passe
   - `Default site language:` ← choisissez `French`

    - `I accept the license` ← cochez la case
8. Cliquez sur `Install`
9. Pointez votre navigateur sur https://example.com/ et loguez vous `admin` avec votre mot de passe saisi, c'est fait !
10. N'oubliez pas d'administrer le site et de le mettre à jour avec la dernière version de Wordpress.

Chapter 14. Pritunl

sudo tee /etc/apt/sources.list.d/mongodb-org-4.2.list << EOF deb http://repo.mongodb.org/apt/debian buster/mongodb-org/4.2 main EOF

sudo tee /etc/apt/sources.list.d/pritunl.list << EOF deb http://repo.pritunl.com/stable/apt buster main EOF

sudo apt-get install dirmngr sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv E162F504A20CDF15827F718D4B7C549A058F8B6B sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv 7568D9BB55FF9E5287D586017AE645C0CF8E292A sudo apt-get update sudo apt-get --assume-yes install pritunl mongodb-org sudo systemctl start mongod pritunl sudo systemctl enable mongod pritunl

Chapter 15. Installation et configuration de Gitea

Gitea est un système simple d'hébergement de code basé sur Git. C'est un fork de Gogs. Il montre des fonctionnalités similaires à gitlab ou github tout en gardant un code plus simple.

15.1. Création du site web de Gitea

Appliquez les opérations suivantes Dans ISPConfig:

1. 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 `gitea`
      - `IP-Address:` ← Double cliquez et sélectionnez l'adresse IP de votre serveur
   b. Cliquez sur `Save`
2. Créer un sub-domain (vhost) dans le configurateur de sites.
   a. Lui donner le nom `gitea`.
   b. Le faire pointer vers le web folder `gitea`.
   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://127.0.0.1:80/.well-known/acme-
challenge
ProxyPassReverse "/.well-known/acme-challenge" http://127.0.0.1:80/.well-
known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# gitea httpserver
#

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / http://localhost:3000/ ①
ProxyPassReverse / http://localhost:3000/ ①
```

   ① mettez le nom de votre domaine à la place de example.com

   h. Cliquez sur `Save`
3. Loguez vous `root` sur le serveur

4. Créez un utilisateur `Gitea`. Tapez:

```
adduser --system --disabled-password --group --shell /bin/bash --home /home/gitea
gitea
```

5. Créez la structure de répertoire de `Gitea`. Tapez:

```
mkdir -p /var/lib/gitea/{data,log} /etc/gitea /run/gitea
```

6. Donnez les bonnes permissions aux répertoires. Tapez:

```
chown -R gitea:gitea /var/lib/gitea
chown -R gitea:gitea /run/gitea
chown -R root:gitea /etc/gitea
chmod -R 750 /var/lib/gitea
chmod 770 /etc/gitea
```

15.2. Création des bases de données

Appliquez les opérations suivantes dans ISPConfig :

1. Créez une base de données mysql. Aller dans le menu `Database` pour définir un utilisateur MariaDB
2. Aller dans la rubrique `Sites`
   a. Aller dans le menu `Database users` pour définir un utilisateur MariaDB
      i. Cliquez sur `Add new User` pour créer un nouvel utilisateur
      ii. Saisissez les informations:
         - `Database user:` ← saisir votre nom d'utilisateur `gitea` par exemple
         - `Database password:` ← saisir un mot de passe ou en générer un en cliquant sur le bouton
         - `Repeat Password:` ← saisir de nouveau le mot de passe
   b. Cliquez sur `save`
   c. Cliquez sur `Add new Database` pour créer une nouvelle base de données
   d. Saisissez les informations:
      - `Site:` ← sélectionner le site `example.com`
      - `Database name:` ← Saisissez le nom de la base de données `gitea`
      - `Database user:` ← Saisir ici le nom d'utilisateur créé: `cxgitea`. x: est le numéro de client.
   e. Cliquez sur `save`

15.3. Téléchargez et installez Gitea

Appliquez les opérations suivantes:

1. Téléchargez gitea du site de chargement. Tapez pour un système 64 bits:

```
wget https://dl.gitea.io/gitea/master/gitea-master-linux-amd64 -O
/usr/local/bin/gitea
chmod 755 /usr/local/bin/gitea
```

2. Créez maintenant une entrée pour le launcher systemd. Tapez:

```
vi /etc/systemd/system/gitea.service
```

3. y Coller le texte suivant:

```
[Unit]
Description=Gitea (Git with a cup of tea)
After=syslog.target
After=network.target
Requires=mysqld.service
[Service]
Type=simple
User=gitea
Group=gitea
WorkingDirectory=/var/lib/gitea/
RuntimeDirectory=gitea
ExecStart=/usr/local/bin/gitea web -c /etc/gitea/app.ini
Restart=always
Environment=USER=gitea HOME=/home/gitea GITEA_WORK_DIR=/var/lib/gitea
[Install]
WantedBy=multi-user.target
```

4. Recharge la base de systemd. Tapez:

```
systemctl daemon-reload
```

5. Activez et démarrez `Gitea`. Tapez:

```
systemctl enable gitea.service
systemctl start gitea.service
```

6. Ouvrez votre navigateur sur l'url: https://gitea.example.com/install et remplissez les paramètres comme ci-après :

- `Type de base de données:` ← Sélectionnez `MySQL`
- `Nom d'utilisateur:` ← Tapez `c0gitea`
- `Mot de passe:` ← Tapez le mot de passe saisi lors de la création de la base
- `Nom de base de données:` ← Tapez `c0gitea`
- `Titre du site:` ← mettez une titre de votre choix
- `Emplacement racine des dépôts:` ← saisissez `/home/gitea/gitea-repositories`
- `Répertoire racine Git LFS:` ← Tapez `/var/lib/gitea/data/lfs`
- `Exécuter avec le compte d'un autre utilisateur :` ← Tapez `gitea`
- `Domaine du serveur SSH:` ← Tapez votre domaine. exemple : `gitea.example.com`
- `Port du serveur SSH:` ← Tapez 22
- `Port d'écoute HTTP de Gitea:` ← Tapez 3000
- `URL de base de Gitea:` ← Tapez l'URL de votre domaine. Exemple: `https://gitea.example.com`
- `Chemin des fichiers log:` ← Tapez `/var/lib/gitea/log`
- `Hôte SMTP:` ← Tapez `localhost`
- `Envoyer les e-mails en tant que:` ← Tapez `gitea@gitea.example.com`
- `Exiger la confirmation de l'e-mail lors de l'inscription:` ← cochez la case
- `Activez les notifications par e-mail:` ← cochez la case
- `Désactiver le formulaire d'inscription:` ← cochez la case
- `Masquer les adresses e-mail par défaut:` ← cochez la case

7. Laissez le reste et cliquez sur `Install Gitea`.
8. Restreignez les permissions sur le fichier de configuration de gitea. Tapez:

```
chmod 750 /etc/gitea
chown root:gitea /etc/gitea/app.ini
chmod 640 /etc/gitea/app.ini
```

9. Redémarrez `gitea`. Sur le serveur en tant que `root`. Tapez:

```
systemctl restart gitea.service
```

15.4. Activer une connexion SSH dédiée

En option, vous pouvez avoir envie de dédier une connexion SSH pour Gitea:

1. Loguez vous comme `root` sur le serveur.
2. Éditez le fichier de configuration. Tapez:

```
vi /etc/gitea/app.ini
```

3. Trouvez les lignes suivantes et les remplacer dans le fichier. Chercher et remplacez:

```
START_SSH_SERVER = true
SSH_PORT = 2222 ①
```

① mettez ici le numéro de port que vous souhaitez

4. Débloquez le port 2222 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 222
   d. Cliquez sur `save`
5. Redémarrez `gitea`. Tapez:

```
systemctl restart gitea.service
```

6. Enjoy !

Chapter 16. Installation de Seafile

Seafile est un système de partage de fichier simple et efficace. Il existe des clients de connexion pour Windows, Linux, Android, IOS.

Cette installation est optionnelle.

16.1. Création du site web de Seafile

Appliquez la procédure suivante:

1. 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 `seafile`
      - `IP-Address:` ← Double cliquez et sélectionnez l'adresse IP de votre serveur
   b. Cliquez sur `Save`
2. Créer un sub-domain (vhost) dans le configurateur de sites.
   a. Lui donner le nom `seafile`.
   b. Le faire pointer vers le web folder `seafile`.
   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:

```
Alias /media {DOCROOT}/private/seafile/seafile-server-latest/seahub/media
RewriteEngine On

<Location /media>
Require all granted
</Location>

Alias /.well-known {DOCROOT}/private/seafile/.well-known
RewriteEngine On

<Location /.well-known>
Require all granted
</Location>

ProxyPass "/.well-known/acme-challenge" http://127.0.0.1:80/.well-known/acme-
challenge
ProxyPassReverse "/.well-known/acme-challenge" http://127.0.0.1:80/.well-
known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# seafile httpserver
#
ProxyPass /seafhttp http://127.0.0.1:8092
ProxyPassReverse /seafhttp http://127.0.0.1:8092
RewriteRule ^/seafhttp - [QSA,L]
#
# seahub
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / http://127.0.0.1:8090/
ProxyPassReverse / http://127.0.0.1:8090/
```

16.2. Création de bases de données

1. Loguez vous sur ISPConfig
2. Aller dans la rubrique `Sites`
   a. Aller dans le menu `Database users` pour définir un utilisateur MariaDB
      i. Cliquez sur `Add new User` pour créer un nouvel utilisateur
      ii. Saisissez les informations:
         - `Database user:` ← saisir votre nom d'utilisateur `seafile` par exemple
         - `Database password:` ← saisir un mot de passe ou en générer un en cliquant sur le bouton
         - `Repeat Password:` ← saisir de nouveau le mot de passe
   b. Aller dans le menu `Database` pour définir les bases de données

c. Appliquer l'opération ci après 3 fois d'affilée pour créer les trois bases suivantes: `ccnetdb`, `seafiledb`, `seahubdb`

   i. Cliquez sur `Add new Database` pour créer une nouvelle base de données

   ii. Saisissez les informations:

      - `Site:` ← sélectionner le site `example.com`
      - `Database name:` ← Saisissez le nom de la base de données
      - `Database user:` ← Saisir ici le nom d'utilisateur créé: `cxseafile`. x: est le numéro de client.

   iii. Cliquez sur `save`

d. Les trois bases de données doivent apparaitre dans la liste des bases

16.3. Téléchargez et installez Seafile

Appliquez la procédure suivante:

1. Loguez vous comme `root` sur le serveur
2. Installez quelques paquets Debian complémentaires. Tapez:

```
apt-get install python2.7 python-setuptools python-simplejson python-pil python-
mysqldb python-flup
```

3. Je préfère faire tourner mes serveurs dans le répertoire privé plutot que dans le répertoire web pour des questions de sécurité. Tapez:

```
cd /var/www/seafile.example.com/private
mkdir seafile
cd seafile
wget https://download.seadrive.org/seafile-server_7.0.5_x86-64.tar.gz
tar zxvf seafile-server_7.0.5_x86-64.tar.gz
mkdir installed
mv seafile-server_* installed
cd seafile-server-*
./setup-seafile-mysql.sh
cd ../..
chown -R web1:client0 seafile ①
```

① choisissez le user et le groupe de votre site web. Ces informations sont consultables dans ISPConfig en consultant les informations du Web Domain → onlget `Options` → champs Linux User et Linux Group.

4. A ce moment, vous devez répondre à un certain nombre de questions.
5. Choisissez le mode de configuration 2) pour indiquer vous même les informations sur les bases de données créées.

6. Vous devrez ensuite donner le nom d'utilisateur pour la base de données, le mot de passe ainsi que le nom des 3 bases de données.
7. Si tout est saisi correctement le programme doit donner une synthèse de ce qui a été configuré

16.4. Lancement initial

Nous allons effectuer un premier lancement du serveur Seafile:

1. allez dans le répertoire contenant les configurations et éditez `gunicorn.conf`. Tapez:

```
cd /var/www/seafile.example.com/private/seafile/conf
vi gunicorn.conf
```

2. Repèrez le texte `bind=` et mettez un numéro de port 8090 à la place de 8000. Comme ceci:

```
bind = "127.0.0.1:8090"
```

3. Editez le fichier `seafile.conf`. Tapez:

```
vi seafile.conf
```

4. mettez un port 8092 au lieu du port 8080 saisi pour l'entrée `fileserver`. Le fichier doit contenir ceci:

```
[fileserver]
port = 8092
```

5. Editez le fichier `ccnet.conf`. Tapez:

```
vi ccnet.conf
```

6. modifier l'entrée SERVICE_URL. Le fichier doit contenir ceci:

```
SERVICE_URL = https://seafile.example.com
```

7. Editez le fichier `seahub_settings.py`. Tapez:

```
vi seahub_settings.py
```

8. modifier l'entrée FILE_SERVER_ROOT. Le fichier doit contenir ceci:

```
FILE_SERVER_ROOT = 'https://seafile.example.com/seafhttp'
```

9. Démarrez Seafile. Tapez:

```
sudo -u web1 ./seafile.sh start ①
sudo -u web1 ./seahub.sh start 8090 ①
```

① remplacer le nom de user web1 par celui correspondant à celui du site web installé (indiqué dans le champ `Options` → `linux user` du web domain). (Si vous n'avez qu'un site, web1 est le bon).

10. Débloquez le port 8090 et 8092 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 8090 et 8092
    d. Cliquez sur `save`
11. Faites pointer votre navigateur sur https://seafile.example.com
12. La page de login de Seafile doit s'afficher

16.5. Lancement automatique de Seafile

Afin de s'assurer que Seafile tourne en permanence, on doit créer un script de lancement automatique de Seafile:

1. Créer un script de lancement automatique. Tapez:

```
cd /var/www/seafile.example.com/private/seafile
touch startseafile.sh
chmod +x startseafile.sh
vi startseafile.sh
```

2. Coller le texte suivant de le fichier ouvert:

```
#!/bin/bash

# Change the value of "seafile_dir" to your path of seafile installation
seafile_dir=/var/www/seafile.example.com/private/seafile ①
script_path=${seafile_dir}/seafile-server-latest
seafile_init_log=${seafile_dir}/logs/seafile.init.log
seahub_init_log=${seafile_dir}/logs/seahub.init.log

case "$1" in
start)
${script_path}/seafile.sh start >> ${seafile_init_log}
${script_path}/seahub.sh start 8090 >> ${seahub_init_log}
;;
restart)
${script_path}/seafile.sh restart >> ${seafile_init_log}
${script_path}/seahub.sh restart 8090 >> ${seahub_init_log}
;;
stop)
${script_path}/seahub.sh stop >> ${seahub_init_log}
${script_path}/seafile.sh stop >> ${seafile_init_log}
;;
*)
echo "Usage: /etc/init.d/seafile {start|stop|restart}"
exit 1
;;
esac
```

① remplacer example.com par votre nom de domaine

3. Créer un job cron dans ISPConfig pour démarrer Seafile au démarrage
   a. Allez dans la rubrique `Sites` puis dans le menu `Cron Jobs`. Cliquez sur `Add cron Job`. Saisisssez les champs:
      - `Parent Website:` ← mettre `example.com`
      - `Minutes:` ← mettre *
      - `Hours:` ← mettre *
      - `Days of month:` ← mettre *
      - `Months:` ← mettre `@reboot`
      - `Days of week:` ← mettre *
      - `Command to run:` ← mettre `/var/www/seafile.example.com/private/seafile/startseafile.sh start`
4. Créer un second job cron dans ISPConfig pour redémarrer Seafile tous les jours
   a. Allez dans la rubrique `Sites` puis dans le menu `Cron Jobs`. Cliquez sur `Add cron Job`. Saisisssez les champs:
      - `Parent Website:` ← mettre `example.com`

- `Minutes:` ← mettre 45
- `Hours:` ← mettre 20
- `Days of month:` ← mettre *
- `Months:` ← mettre *
- `Days of week:` ← mettre *
- `Command to run:` ← mettre `/var/www/seafile.example.com/private/seafile/startseafile.sh restart`

5. Arretez le serveur précédemment lancé en tant que root. Tapez:
6. Enjoy !

Chapter 17. Installation d'un serveur de VPN Pritunl

Pritunl est un serveur VPN basé sur OpenVPN.

17.1. Création du site web de Pritunl

Appliquez la procédure suivante:

1. 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 `pritunl`
      - `IP-Address:` ← Double cliquez et sélectionnez l'adresse IP de votre serveur
   b. Cliquez sur `Save`
2. Créer un sub-domain (vhost) dans le configurateur de sites.
   a. Lui donner le nom `pritunl`.
   b. Le faire pointer vers le web folder `pritunl`.
   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://127.0.0.1:80/.well-known/acme-
challenge
ProxyPassReverse "/.well-known/acme-challenge" http://127.0.0.1:80/.well-
known/acme-challenge
RewriteRule ^/.well-known/acme-challenge - [QSA,L]

# Pritunl httpserver
#
  SSLProxyEngine On
  SSLProxyCheckPeerCN Off
  SSLProxyCheckPeerName Off
  SSLProxyVerify none

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPass / https://127.0.0.1:8070/
ProxyPassReverse / https://127.0.0.1:8070/
ProxyPreserveHost On
```

17.2. Installation de Pritunl

Veuillez suivre la procédure suivante:

1. Loguez vous comme `root` sur le serveur
2. Ajoutez des repositories Debian. Tapez:

```
tee /etc/apt/sources.list.d/mongodb-org.list << EOF
deb http://repo.mongodb.org/apt/debian buster/mongodb-org/4.2 main
EOF
tee /etc/apt/sources.list.d/pritunl.list << EOF
deb http://repo.pritunl.com/stable/apt buster main
EOF
apt-get install dirmngr
apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv
E162F504A20CDF15827F718D4B7C549A058F8B6B
apt-key adv --keyserver hkp://keyserver.ubuntu.com --recv
7568D9BB55FF9E5287D586017AE645C0CF8E292A
apt-get update
apt-get --assume-yes install pritunl mongodb-org
```

3. Pritunl utilise en standard le port 80 et 443. Ces deux ports sont utilisés dans notre configuration par le serveur apache
4. On commence par arrêter apache. Tapez:

Plus aucun site web ne sera servit. Danger donc.

```
systemctl stop apache2
```

5. Démarrez Mongodb ainsi que Pritunl. Tapez:

```
systemctl start mongod pritunl
systemctl enable mongod pritunl
```

17.3. Configuration de Pritunl

Votre service Pritunl est actif. Vous devez maitenant le configurer pour qu'il fonctionne:

1. pointez votre navigateur sur le site web de Pritunl: https://example.com
2. Accepter le certificat non sécurisé. La page de setup de Pritunl s'affiche.
3. Obtenez la clé d'activation. Tapez:

```
pritunl setup-key
```

4. copier la clé dans la page web. Cliquez sur `Save`
5. La page web s'affiche en erreur. Pas d'inquiétude à avoir.
6. Arrêtez le serveur Pritunl. Tapez:

```
systemctl stop pritunl
```

7. Configurez le serveur pour qu'il n'utilise plus le port 80 et le port 443

```
pritunl set app.server_port 8070
pritunl set app.redirect_server false
```

8. Redémarrez apache et pritunl

```
systemctl start apache2
systemctl start pritunl
```

9. Pointez maintenant votre navigateur sur le site https://pritunl.example.com . La page de login de pritunl doit s'afficher. Si ce n'est pas le cas, revérifier votre configuration de site web dans ISPConfig et que le port 8070 est bien activé.
10. Sur le serveur, tapez:

```
pritunl default-password
```

11. Entrez dans la page web la valeur de `username` et de `password` affichés dans le terminal.
12. Une boite de dialogue `initial setup` s'affiche. Ne changez rien mais tapez votre mot de passe.
13. Vous êtes maintenant connecté sur le site web.
14. Cliquez sur l'onglet `Users`
    a. Cliquez sur `Add Organization`
    b. Entrez votre nom d'organisation. Par exemple `Personnel`
    c. Cliquez sur `Add`
    d. Cliquez sur `Add User`
    e. Remplissez les champs:
        - `Name: ` ← Tapez votre nom de login (pas de caractère accentué pas d'espace)
        - `Select an organization: ` ← sélectionnez votre organisation
        - `Email: ` ← Tapez votre adresse Email
        - `Pin:` ← entrez votre code Pin (que des nombres; au moins 6 chiffres)

f. Cliquez sur `Add`

15. Allez sur l'onglet `Servers`
    a. Cliquez sur `Add Server`
    b. Remplissez les champs:
        - `Name:` ← donnez un nom à votre serveur (pas de caractère accentué pas d'espace)
        - laissez le reste tel quel mais notez bien le numéro de port UDP indiqué
    c. Cliquez sur `Add`
    d. Cliquez sur `Attach Organization`
    e. Sélectionnez le `server` et l' `organization`.
    f. Cliquez sur `Attach`
16. Débloquez le port VPN 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 UDP ports:`, ajoutez le port UDP du VPN que vous avez noté.
    d. Cliquez sur `save`
17. Retourner dans l'interface de Pritunl. retournez sur l'onglet `Servers`
    a. Cliquez sur `Start server`
18. Votre serveur de VPN est opérationnel.

17.4. Se connecter au serveur de VPN

Comme Pritunl est compatible OpenVPN n'importe quel logiciel compatible OpenVPN peut être utilisé. Pritunl founit un client compatible pour Linux, macOS, and Windows.

Pour se connecter à l'aide du client, vous devez charger un fichier de configuration qui est téléchargeable dans l'onglet utilisateur du serveur web. Ce fichier est à importer dans le logiciel client de Pritunl. Une fois fait, une compte apparait dans le logiciel client. Vous pourrez vous connecter en cliquant sur le bouton `Connect` du compte utilisateur.

17.5. Réparer une base Pritunl

Si jamais votre base est corrompue, vous pourrez la réparer en tapant:

```
systemctl stop pritunl
pritunl repair-database
systemctl start pritunl
```

17.6. Mot de passe perdu

Vous pouvez regénérer un mot de passe en tapant:

```
pritunl reset-password
```

Chapter 18. Annexe

18.1. Installation de Hestia

Hestia est basé sur VestaCP. C'est une alternative opensource et plus moderne de cet outiL. La documentation est proposée ici: https://docs.hestiacp.com/

Attention Hestia n'est pas compatible de Webmin dans le sens que webmin est incapable de lire et d'interpréter les fichiers créés par Hestia.

De même, Hestia est principalement compatible de PHP. Si vous utilisez des système web basés sur des applicatifs écrits en Python ou en Ruby, la configuration sera à faire à la main avec tous les problèmes de compatibilité que cela impose.

Pour installer:

1. Se logger `root` sur le serveur
2. Télécharger le package et lancez l'installeur
   a. Tapez :

   ```
   wget https://raw.githubusercontent.com/hestiacp/hestiacp/release/install/hst-install.sh
   ```

   b. Lancez l'installeur. Tapez :

   ```
   bash hst-install.sh -g yes -o yes
   ```

   c. Si le système n'est pas compatible, HestiaCP vous le dira. Sinon, il vous informe de la configuration qui sera installée. Tapez `Y` pour continuer.
   d. Entrez votre adresse mail standard et indépendante du futur serveur qui sera installé. ce peut être une adresse gmail.com par exemple.
3. Hestia est installé. Il est important de bien noter le mot de passe du compte admin de Hestia ainsi que le numéro de port du site web