Installation d’un VPS

Stéphane Apiou

Version 1.0, 2020-03-27

Table of Contents

Chapter 1. Avant propos

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

Cette documentation décrit la méthode que j'ai utilisé pour installer 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 serveur de mail avec antispam, * 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. * un serveur et un site de partage de fichiers Seafile, * un site sous Joomla, * un sous domaine pointant sur un site autohébergé (l'installation du site n'est pas décrite ici; Se référer à Yunohost), * un site Gitea et son repository GIT, * un serveur de VPN pritunl, * un site Mediawiki, * un site Nextcloud * un site Wordpress * des outils de sécurisation, mise à jour automatique et d'audit du serveur * A venir: strut, 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. Donc que vous savez vous servir de `ssh` pour Linux ou de `putty` pour Windows

Dans le document, on peut trouver des textes entourés de <texte>. Cela signifie que vous devez mettre ici votre propre texte selon vos préférences. Si le texte ne doit pas contenir d'espace, la phrase contient elle même des _ ou des - pour l'indiquer en fonction de ce qui est autorisé.

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'. Le taux de complexité est bien meilleur et les mots de passe sont plus facile à retenir que 'Az3~1ym_a&'

Le cout pour avoir 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 15€/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. 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.

5.2. 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.`

5.3. Création d'une clé de connexion ssh

Pour créer une clé et la déployer:

1. Créez une clé sur votre machine locale:
   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.

5.4. 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`

5.5. 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
```

5.6. 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`

5.7. Installation des paquets de base

1. tapez:

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

2. Si vous souhaitez installer automatiquement les paquets Debian de correction de bugs de sécurité, tapez:

```
apt install unattended-upgrades
```

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
   ```

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.
```

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 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. Installer quelques outils Debian

7.1. Installer l'outil debfoster

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

7.2. 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 `deselect`. Tapez :

```
apt install deselect
```

Chapter 8. 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

8.1. 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
```

5. Autorisation de Webmin au niveau du firewall
   a. Loguez vous Admin sur le site Hestia: https://<example.com>:8083
   b. Allez dans Server→Firewall, puis Add Rule
   c. Sélectionnez Action: `Allow`, Protocol: `TCP`, Port: `10000`, IP Address: `0.0.0.0/0`, Service: `WEBMIN`
   d. Cliquez sur Save, puis Back
   e. Constatez que le service Webmin sur le port 10000 est autorisé
6. 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'.
7. Loguez-vous `root`. Tapez le mot de passe de `root`. Le dashboard s'affiche.
8. 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.
9. 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
10. 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)`

8.2. 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. 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

8. 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 9. Configuration d'un premier 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/ .

9.1. Login initial

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.

9.2. 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`

9.3. 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.

9.4. 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.

9.5. 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"
```

Chapter 10. 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]
```

Chapter 11. Création d'un sous-domaine (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]
```

Chapter 12. Configuration de la messagerie

12.1. Création du serveur de messagerie

Pour créer la messagerie, aller dans email→domain→cliquez sur add new domain. Sélectionner le nom de domaine et créer des identifiants DKIM. Une fois cela fait, retourner dans la gestion des records de domaine et activer le type DMARC. Garder le paramétrage par défaut et sauvegardez. Faites de même pour les enregistrements SPF et sélectionner le mécanisme softfail.

Chapter 13. Annexe

13.1. 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