

Installation d'un serveur Web sur un Raspberry

Guide de l'hébergement à domicile

Stéphane Apiou

STATUT DU DOCUMENT

Type	Nom	Titre
Auteur	Stéphane Apiou	CTO
Vérificateur	Stéphane Apiou	CTO
Approbateur	Stéphane Apiou	CTO

HISTORIQUE DES MODIFICATIONS

Date	Indice	Nature de la modification	Par
2024-10-20	1.8	mise à jour de doc sur vaultwarden, borg backup, certificats, docker-mirror, ajout de wireguard	SA
2024-04-17	V1.7	Debian 12, Mise à jour de la doc sur webmin, rspamd, pritunl, nextcloud, mealie, borg-backup, vaultwarden	SA
2024-03-14	V1.6	Passage sur Contabo, Debian 12, Raspberry pi 5, ajout du Motd, Correction du générateur readthedocs	SA
2021-05-19	V1.3	Création du document	SA

SOMMAIRE

Avant propos.....	9
Se loguer root sur le serveur.....	12
Gestion des mots de passe.....	12
Choix du registrar.....	14
Installation du linux sur votre Raspberry Pi.....	16
Installation avec écran et clavier.....	18
Installation Headless.....	19
Connexion au travers du réseau.....	19
Installation Headless de Ubuntu 64.....	21
Configuration de VNC.....	24
Configuration basique.....	25
Vérification du nom de serveur.....	25
Mettre l'éditeur de votre choix.....	27
Installation d'un repository pour /etc.....	27
Mise à jour des sources de paquets Debian ou Ubuntu.....	29
Installation des paquets de base.....	30
Passage de la locale en FR.....	30
Installer l'outil Debfoster.....	31
Création d'un fichier keeper dans /etc.....	33
Installation des mises à jours automatiques.....	34
Interdire le login direct en root.....	35
Création d'une clé de connexion ssh locale.....	37
Sudo sans mot de passe.....	38
Configuration du Motd.....	39
Installation de Neofetch.....	39
Configuration du MOTD avec Neofetch.....	40
Mise à jour de packages.....	41
Installer l'outil dselect.....	44
Ajouter un fichier de swap.....	44
Installation initiale des outils.....	45
Installation et configuration de ISPConfig.....	45

Configuration Manuelle des outils.....	47
Configuration manuelle de Postfix.....	48
Configuration manuelle de MariaDB.....	49
Configuration manuelle d'Apache.....	51
Configuration manuelle d' Awstats.....	52
Configuration manuelle de Fail2ban.....	52
Installation et configuration manuelle de PureFTPD.....	53
Installation et configuration manuelle de Phpmyadmin.....	55
<i>Installation de Phpmyadmin.....</i>	55
<i>Upgrade de Phpmyadmin.....</i>	59
Installation manuelle du webmail Roundcube.....	59
Installation manuelle de Let's Encrypt.....	60
Suite de l'installation.....	61
Déblocage de port de firewall.....	61
<i>Déblocage et suppression de règles de Firewall avec ISPconfig.....</i>	61
<i>Déblocage de Firewall UFW.....</i>	62
Scan des vulnérabilités.....	63
<i>Installation d'un scanner de vulnérabilités Lynis.....</i>	63
<i>Upgrade de Lynis.....</i>	63
Installation du système d'administration Webmin.....	64
Configuration d'un domaine.....	66
Login initial.....	66
Création de la zone DNS d'un domaine.....	70
Activation de DNSSEC.....	71
Exemple de configuration de domaine.....	73
Création d'un sous domaine.....	74
Création d'un site web.....	76
Création d'un Site Vhost.....	78
Associer des certificats reconnu à vos outils.....	81
Surveillance du serveur avec Munin et Monit.....	83
Note préliminaire.....	83
Installation et configuration de Munin.....	83
Activez les plugins de Munin.....	87
Installer et configurer Monit.....	87
Configuration de la messagerie.....	92

Configuration de l'antispam rspamd.....	92
Création du serveur de messagerie.....	104
Finaliser la sécurisation de votre serveur de mail.....	105
Surveillance du statut de Spammer.....	107
Création de l'autoconfig pour Thunderbird et Android.....	109
Création d'autodiscover pour Outlook.....	112
Création d'une boite mail.....	117
Configuration de votre client de messagerie.....	118
Mise en oeuvre du site web de webmail.....	119
Transfert de vos boites mails IMAP.....	120
Installation de Docker et des outils associés.....	121
A propos des Raspberry Pi.....	121
Installation de Docker.....	122
Installation de docker swarm.....	123
Choix des images docker.....	123
Considérations de sécurité.....	124
Mise à jour automatique des images.....	125
Surveillance et redémarrage de container.....	126
Configuration d'un repository local Docker.....	126
Configuration de Docker-mirror.....	127
Outils web de gestion des containers.....	129
Installation de Yacht.....	129
Upgrade d'un container dans Yacht.....	131
Upgrade de Yacht.....	131
Installation de Portainer.....	132
Upgrade d'un container dans Portainer.....	135
Upgrade de Portainer.....	135
Installation des CMS Joomla.....	135
Création du site web de Joomla.....	136
Création des bases de données.....	136
Création de l'application Joomla.....	137
Update de Joomla.....	139
Installation des CMS Concrete5.....	139
Création du site web de Concrete5.....	139

Création des bases de données.....	140
Création de l'application Concrete5.....	141
Update de concrete5.....	142
Installation du portail wiki Mediawiki.....	143
Création du site web de Mediawiki.....	143
Création des bases de données.....	143
Création de l'application Mediawiki.....	144
Update du serveur Mediawiki.....	147
Installation d'un gestionnaire de Blog Wordpress.....	148
Création du site web de Wordpress.....	148
Création des bases de données.....	149
Création de l'application Wordpress.....	150
Update de wordpress.....	151
Installation du CMS Micro Weber.....	152
Création du site web de Microweber.....	152
Création des bases de données.....	153
Installation de Microweber.....	153
Update de Microweber.....	155
Installation de Mealie.....	155
Prérequis.....	155
Installation du serveur Mealie.....	155
Création du site web de mealie.....	156
Configuration du site mealie.....	157
Upgrade de Mealie.....	157
Installation du gestionnaire de photos Piwigo.....	158
Création du site web de Piwigo.....	158
Création des bases de données.....	159
Installation de Piwigo.....	160
Update de Piwigo.....	161
Installation du système collaboratif Nextcloud.....	161
Installation initiale.....	161
Création du site web de Nextcloud.....	162
Création des bases de données.....	163
Installation de Nextcloud.....	164

Upgrade de Nextcloud.....	165
Installation du gestionnaire de projet Gitea.....	165
Création du site web de Gitea.....	165
Création des bases de données.....	167
Téléchargez et installez Gitea.....	168
Activer une connexion SSH dédiée.....	170
Update de Gitea.....	170
Installation de vaultwarden.....	171
Prérequis.....	171
Installation du serveur vaultwarden.....	171
Création du site web de vaultwarden.....	172
Configuration du site vaultwarden.....	173
Upgrade de vaultwarden.....	174
Installation de Heimdall.....	175
Prérequis.....	175
Installation du serveur Heimdall.....	175
Création du site web de heimdall.....	176
Configuration du site heimdall.....	177
Upgrade de Heimdall.....	178
Installation du système de partage de fichiers Seafile.....	178
Création du site web de Seafile.....	178
Création de bases de données.....	180
Téléchargez et installez Seafile.....	181
Lancement initial.....	182
Lancement automatique de Seafile.....	183
Upgrade de Seafile.....	185
Installation du système de monitoring Grafana.....	187
Création du site web de Grafana.....	187
Installation de Grafana.....	188
Installation et configuration de Loki.....	191
Installation et configuration de Promtail.....	193
Upgrade de Grafana.....	195
Installation du système de backup BorgBackup.....	196
Introduction.....	197

Installation du serveur de stockage.....	197
Installation sur le serveur sauvegardé.....	198
Lister les backups.....	200
Obtenir les infos sur un backup.....	201
Vérifier un backup.....	201
Restaurer un backup.....	202
Supprimer vos vieux backups.....	203
Restauration d'urgence.....	205
Installation de Borgweb.....	207
Création du site web de Borgweb.....	209
Installation d'un serveur de VPN Wireguard.....	211
Création du site web de Wireguard.....	211
Installation de Wireguard.....	213
Update de Wireguard.....	213
Installation d'un serveur de bureau à distance Guacamole.....	214
Création du site web de Guacamole.....	215
Création des bases de données.....	216
Installation du Guacamole.....	217
Upgrade de Guacamole.....	223
Annexe.....	224
Installation de Hestia.....	224
Configuration d'un écran 3.5 inch RPI LCD (A).....	225
Pour commencer.....	225
Basculer entre l'affichage LCD et HDMI.....	226
Paramètres d'orientation de l'écran.....	226
Calibrage de l'écran tactile.....	226
Installer un clavier virtuel.....	228
Ressources.....	229
<i>Manuel utilisateur.....</i>	229
<i>Images.....</i>	229
<i>Driver.....</i>	229
<i>Fichiers de configuration de référence.....</i>	230

Avant propos

Ce document est disponible sur le site [ReadTheDocs](#)



et sur [Github](#). Sur Github vous trouverez aussi les versions PDF, EPUB, HTML, Docbook et AsciiDoc de ce document

Cette documentation décrit la méthode que j'ai utilisé pour installer une homebox (site auto hébergé) avec un raspberry PI.

Elle est le résultat de très nombreuses heures de travail pour collecter la documentation nécessaire. Sur mon serveur, j'ai installé un Ubuntu pour Raspberry. Cette documentation décrit aussi l'installation pour une Raspbian.

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

Sont installés:

- un panel [ISPConfig](#),
- un configurateur [Webmin](#),
- un serveur apache avec sa configuration let's encrypt et les plugins PHP, Python et Ruby,
- un serveur de mail avec antispam, sécurisation d'envoi des mails et autoconfiguration pour Outlook, Thunderbird, Android,
- un webmail [roundcube](#),
- un serveur de mailing list [mailman](#),

- un serveur ftp et sftp sécurisé,
- un serveur de base de données MariaDB 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](#),
- l'installation de [Docker](#) et des outils [Portainer](#) et [Yacht](#),
- un sous domaine pointant sur un site auto-hébergé (l'installation du site n'est pas décrite ici; Se référer à [Yunohost](#)) par exemple,
- un site CMS sous [Joomla](#),
- un site CMS sous [Concrete5](#),
- un site WIKI sous [Mediawiki](#),
- un site de blog [Wordpress](#),
- un site [Microweber](#),
- un site Photo sous [Piwigo](#),
- un site de partage de recettes de cuisine [Mealie](#)
- un site Collaboratif sous [Nextcloud](#),
- un site [Gitea](#) et son repository GIT,
- un serveur de mots de passe [Bitwarden](#),
- un dashboard pour vos sites web [Heimdall](#),
- un serveur et un site de partage de fichiers [Seafile](#),
- un serveur [Grafana](#), [Prometheus](#), [Loki](#), Promtail pour gérer les statistiques et les logs du serveur,
- un serveur de sauvegardes [BorgBackup](#),

- un serveur de VPN [Wireguard \(wg-easy\)](#),
- un serveur de bureau à distance [Guacamole](#)

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 texte `nano` à la place et de remplacer `vi` par `nano` dans toutes les lignes de commande.

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

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

- Compter 15-18€TTC/an pour un nom de domaine classique (mais il peut y avoir des promos)
- Comptez 47€ pour acheter une carte Raspberry PI 4 (1Go de Ram) et 67€ pour un PI 4 avec 4Go de Ram ou 94€ pour un PI 5 avec 8Go de Ram. A cela il faut ajouter un boitier, une alim et une flash de 64 ou 128 Go (prenez les cartes SD les plus rapide possible en écriture).

Vous en aurez donc entre 80€ pour une petite Configuration Raspberry PI 4 1Go, flash de 64 Go et 160€ pour une configuration Raspberry PI 5 8 Go et une flash de 512 Go.

Il existe aussi des kits permettant de mettre en oeuvre des cartes NVME avec un gros gain de performance disque.

Par rapport à une solution VPS directement dans le cloud, ce budget correspond à 7-16 mois d'abonnement selon la configuration. Si vous avez la Fibre chez vous, il est nettement plus rentable d'utiliser un Raspberry que de prendre un abonnement VPS.

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>
```

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

ou utilisez putty si vous êtes sous Windows.

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

3. Loguez-vous root. Tapez :

```
sudo bash
```

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

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

1. Se loguer root sur le serveur distant. Tapez:

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

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

Tapez ensuite votre mot de passe root

Gestion des mots de passe

A propos des mots de passe: il est conseillé de saisir des mots de passe de 12 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 bien meilleur qu'un mot de passe classique. Il est aussi plus facile à retenir que 'Az3~1ym_a&!'.

Cependant, si vous êtes en manque d'inspiration et que vous souhaitez générer des mots de passe, voici quelques méthodes:

1. En se basant sur la date. Tapez:

```
date +%s | sha256sum | base64 | head -c 32 ; echo
```

- remplacez 32 par la valeur qui vous convient pour générer un mot de passe d'une taille différente de 32 caractères

2. En se basant sur les nombres aléatoires système. Tapez l'une des deux lignes ci dessous :

```
tr -cd '[:graph:]' < /dev/urandom | head -c 32; echo  
tr -cd A-Za-z0-9 < /dev/urandom | head -c 32;echo
```

- remplacez 32 par la valeur qui vous convient pour générer un mot de passe d'une taille différente de 32 caractères

3. En utilisant Openssl. Tapez :

```
openssl rand -base64 32 | cut -c-32
```

- remplacez 32 par la valeur qui vous convient pour générer un mot de passe d'une taille différente de 32 caractères

4. En utilisant gpg. Tapez :

```
gpg --gen-random --armor 1 32 | cut -c-32
```

- remplacez 32 par la valeur qui vous convient pour générer un mot de passe d'une taille différente de 32 caractères

5. En utilisant pwgen pour générer des mots de passe qui suivent des règles de longueur et types de caractères.

1. Pour installer l'outil, tapez:

```
apt install pwgen
```

2. Ensuite tapez :

```
pwgen -Bcny 32 -1
```

- remplacez 32 par la valeur qui vous convient pour générer un mot de passe d'une taille différente de 32 caractères. La commande crée un mot de passe non ambigu avec au moins une majuscule , une valeur numérique, un symbole.

6. En utilisant apg pour générer des mots de passe prononcables tel que:

```
7quiGrikCod+ (SEVEN-qui-Grik-Cod-PLUS_SIGN)
```

1. Pour installer l'outil, tapez:

```
apt install apg
```

2. Ensuite tapez :

```
apg
```

7. En utilisant xkcdpass pour générer des passphrases comme: context smashup spiffy cuddly throttle landfall

1. Pour installer l'outil, tapez:

```
apt install xkcdpass
```

2. Ensuite tapez :

```
xkcdpass
```

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: Inactif (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".

Ajoutez des Glue records:

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

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:

- les deux DNS de votre domaine: ns1.<example.com> et ns2.<example.com>
- puis enfin le nom de votre machine définie par votre hébergeur de VPS:
vmixxxxxxx.contaboserver.net

Ajoutez des Glue records:

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

i Note

Il y a la possibilité chez OVH d'utiliser un DNS secondaire. Dans ce cas, enregistrez votre nom de domaine sur le serveur de dns secondaire de votre hébergeur. Notez ensuite le nom de domaine de ce DNS secondaire et ajoutez une entrée supplémentaire sur le serveur de votre registrar avec l'adresse DNS secondaire.

i Note

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

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

Installation du linux sur votre Raspberry Pi

C'est la première étape.

Il vous faut bien choisir le type de linux que vous souhaitez installer:

- Debian 64: C'est la distribution la plus connue et celle qui offre le plus de possibilités juste après l'installation (notamment pour faire de la domotique, utiliser le GPIO ...).
- Ubuntu 64: Elle est plus proche d'une Ubuntu standard.

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

Il existe maintenant un outil nommé [Raspberry PI Imager](#) pour la plateforme qui vous convient. C'est le moyen de plus simple de flasher votre Raspberry pi.

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

1. [Loguez vous comme root](#)

2. Tapez:

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

3. Lancez le programme.

Suivez la procédure ci dessous commune à toutes les plateformes:

1. Vous avez deux façons d'installer:

- avec un écran et un clavier qui est la méthode la plus facile

- en mode Headless qui est plus complexe mais ne nécessite pas d'écran ni de clavier. L'installation s'effectue automatiquement.
2. Sélectionnez Choisir le modèle et dans la liste choisissez votre type de Raspberry
3. Sélectionnez Choisir l'OS et dans la liste choisissez Raspberry Pi OS (64-bit) ou Other general-purpose OS → `Ubuntu` → `Ubuntu Desktop 64`
4. Sélectionnez Choisir le Stockage et sélectionnez votre lecteur de carte SD
5. Cliquez sur Suivant
6. Cliquez sur Modifier Réglages si vous souhaitez installer en mode headless le Raspberry sinon cliquez sur Non et allez à l'étape 10
7. Dans l'onglet Général
- Donnez le nom de votre Raspberry dans Nom d'hôte
 - Donnez votre utilisateur sudo dans nom d'utilisateur
 - Donnez votre mot de passe dans Mot de passe. Utilisez un générateur de mot de passe pour en obtenir un suffisamment complexe
 - Donnez votre SSID Wifi dans SSID
 - Donner le mot de passe de votre wifi dans Mot de passe. Vous pouvez l'afficher si vous voulez vérifier que la saisie est correcte.
 - Dans Pays Wi-fi mettez FR
 - Dans Fuseau horaire mettez votre pays Europe/Paris par exemple
 - Dans type de clavier mettez fr si vous avez un clavier Azerty
8. Dans l'onglet `Services`
- Activez Activer SSH
 - Sélectionnez Utiliser un mot de passe pour l'authentification
9. Cliquez sur Enregistrer

10. Cliquez sur Oui

11. Dans la fenêtre suivant intitulée Attention cliquez sur Oui

12. Attendez la fin du chargement et de l'écriture sur la flash.

13. En fonction de la méthode choisie, allez au chapitre suivant ou celui encore après.

Installation avec écran et clavier

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

1. Enlevez la carte SD de votre lecteur et insérez la dans votre raspberry PI.
2. Brancher un clavier, une souris et un écran (ou utilisez un écran 3,5" configuré selon la procédure en annexe).
3. Branchez votre Raspberry sur votre réseau Ethernet filaire (vous pouvez aussi utiliser le wifi)
4. Démarrez votre raspberry. Attention, les Raspberry PI 5 ont un bouton On
5. Attendez environ 2 minutes le temps que le premier boot se termine. Tout pendant la procédure de boot, la petite led d'accès disque doit clignoter. Vous devez assez rapidement arriver sur le bureau
6. Un écran de configuration doit s'afficher automatiquement.
7. Sélectionnez le clavier et la langue en français
8. Tapez votre nouveau mot de passe et votre compte utilisateur
9. Choisissez votre connexion wifi et entrez le mot de passe
10. Les mises à jours de paquets Debian ainsi que l'installation des traductions en français vont s'installer.
11. Une fois les installations terminées, le Raspberry va rebooter.
12. Une fois rebooté, sélectionnez dans le menu Préférences → `Configuration du Raspberry PI`

- Dans l'onglet Display Cliquez sur Set Resolution et choisissez 31: 1920x1080
- Dans l'onglet Interfaces activez SSH et VNC
- Cliquez sur Valider

13. Cliquez sur l'icône VNC dans la barre en haut à Droite

- Dans la fenêtre cliquez sur le menu burger en haut à Droite.
- Choisissez Options puis l'onglet Sécurité
- Dans le champ Authentification choisissez l'option mot de passe VNC
- Tapez votre mot de passe dans les deux champs et cliquez Valider puis OK

14. Vous pouvez maintenant rebooter votre Raspberry sans écran et sans clavier pour continuer la configuration.

15. Vous avez deux options: connexion en mode SSH ou au travers d'une connexion VNC

Allez au chapitre [Connexion au travers du réseau.](#)

Installation Headless

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

1. Enlevez la carte SD de votre lecteur et insérez la dans votre raspberry PI.
2. Démarrez votre raspberry. Attention, les Raspberry PI 5 ont un bouton on
3. Attendez environ 2 minutes le temps que le premier boot se termine. Tout pendant la procédure de boot, la petite led d'accès disque doit clignoter.

Connexion au travers du réseau

1. Vous devez maintenant découvrir l'adresse IP de votre Raspberry, pour cela tapez la commande suivante:

```
ping raspberrypi.local
```

- Attention remplacez raspberrypi par le nom d'Hôte que vous avez choisi lors de la configuration
2. Si le Raspberry a démarré correctement, cette commande doit montrer l'adresse IP du raspberry et une réponse correcte au ping

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

1. Vous pouvez aussi utiliser la commande suivante:

```
arp -na | grep -Pi "(b8:27:eb) | (dc:a6:32) | (e4:5f:01) | (d8:3a:dd)"
```

2. Elle vous donnera l'adresse IP de tous les raspberry de votre réseau et présents dans le cache ARP de votre PC.
3. Ensuite testez l'adresse ip trouvée

```
ping 192.168.0.100
```

- mettez ici l'adresse IP qui a été découverte.
4. Si le Raspberry a démarré correctement, cette commande doit montrer l'adresse IP du raspberry et une réponse correcte au ping

```
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=1.49 ms
```

1. Si vous n'obtenez aucun résultat essayez la commande nmap sur le subnet de votre réseau local

- On obtient l'adresse local du subnet en tapant:

```
hostname -I
```

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

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

- En suite à l'exemple de hostname reçu dans l'étape précédente, nous avons remplacé le 10 à la fin de l'adresse IP par 0.
- la commande affiche alors les adresses IP et mac de toutes les machines présentes sur le réseau.
- le Raspberry se reconnaît par son nom de machine qui contient le terme raspberry ou par son adresse mac qui est reconnue du type Raspberry Pi Foundation

2. vous pouvez alors directement vous connecter. Tapez:

```
ssh username@adresse_ip
```

- username est le nom d'utilisateur défini lors de la configuration.
- adresse_ip est l'adresse IP du Raspberry pi découverte précédemment ou raspberrypi.local ou nom d'hôte.local

3. Se loguer avec le mot de passe défini pendant la configuration

Installation Headless de Ubuntu 64

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

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

1. Avant d'enlever votre flash SD du lecteur, appliquez la procédure ci après:

- Sur la flash, 2 partitions ont été créées. Montez la partition system-boot
- sur cette partition, editez le fichier network-config et éditez le avec un éditeur de text (Nano ou vi sous linux ou Notepad sous windows).
- Mettez y le texte suivant:

```
version: 2
ethernets:
    eth0:
        dhcp4: true
```

```

        optional: true
wifis:
    wlan0:
        dhcp4: true
        optional: true
        access-points:
            YOURSSID:
                password: "YOURPASSWORD"

```

- remplacez `YOURSSID` par le nom SSID de votre wifi local
 - remplacez `YOURPASSWORD` par le mot de passe de votre wifi local
 - sauvez le fichier
 - démontez la partition
 - au boot sur la carte SD, le fichier sera recopié dans votre configuration et le réseau wifi sera ainsi accessible
2. Enlevez la carte SD de votre lecteur et insérez la dans votre Raspberry PI.
 3. Démarrez votre raspberry.
 4. Attendez environ 2 minutes le temps que le premier boot se termine. Tout pendant la procédure de boot, la petite led d'accès disque doit clignoter.
 5. Vous devez maintenant découvrir l'adresse IP de votre Raspberry, pour cela tapez la commande suivante: +

```
arp -na | grep -Pi "(b8:27:eb) | (dc:a6:32) | (e4:5f:01) | (d8:3a:dd)"
```

1. Ensuite testez l'adresse ip trouvée


```
ping 192.168.0.100
```

 - mettez ici l'adresse IP qui a été découverte.
2. Si le Raspberry a démarré correctement, cette commande doit montrer l'adresse IP du raspberry et une réponse correcte au ping

```
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=1.49 ms
```

1. Si vous n'obtenez aucun résultat essayer la commande `nmap` sur le subnet de votre réseau local

- On obtient l'adresse local du subnet en tapant:

```
hostname -I
```

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

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

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

2. vous pouvez alors directement vous connecter. Tapez:

```
ssh ubuntu@adresse_ip
```

- adresse_ip est l'adresse IP du Raspberry pi découverte précédemment

3. Se loguer avec le mot de passe ubuntu

4. Un nouveau mot de passe vous sera demandé puis vous serez déconnecté.

5. Reconnectez vous.

6. Installez la langue française. Tapez :

```
apt install language-pack-fr manpages-fr
```

7. Installer la locale qui vous plaît. Tapez :

```
dpkg-reconfigure locales
```

8. Choisissez votre langue locale. Par exemple: fr_FR.UTF-8

9. Installer la la timezone qui vous plaît. Tapez :

```
dpkg-reconfigure tzdata
```

10. Choisissez votre Timezone. Par exemple: Europe/Paris

Configuration de VNC

VNC permet de prendre le contrôle à distance et en mode graphique du raspberry pi.

Il peut être lancé à la demande ou automatiquement au démarrage du raspberry pour un utilisateur standard.

L'installation est simple:

1. Sur le bureau du raspberry aller dans le menu →Préférences→Configuration du raspberry Pi
2. Dans la fenêtre qui s'ouvre allez dans l'onglet interfaces et cliquez sur VNC.
3. Cliquez sur Valider
4. Le raspberry PI a des problèmes de lenteurs lorsque vous ne branchez pas d'écran au moment du boot de votre raspberry. C'est typiquement le cas pour les configurations Headless. Pour corriger cela il faut forcer une résolution avec une autodétection de l'écran. Il faut modifier la conf de boot.
5. [Loguez vous comme root sur le serveur](#)
6. Tapez,
`vi /boot/firmware/cmdline.txt`
7. Puis sur la ligne présenté à l'écran, ajoutez au bout le texte suivant précédé d'un espace. Vous pouvez changer la résolution (1024x768) comme vous voulez :
`video=HDMI-A-1:1024x768@60D`
8. Le driver graphique définit par défaut n'est pas le bon pour un Raspberry PI 4 ou 5. Tapez
`vi /boot/firmware/config.txt`
9. Cherchez la ligne `dtoverlay=vc4-kms-v3d` et replacez la avec :
`gpu_mem=128`
`dtoverlay=vc4-kms-v3d-pi4`
`hdmi_force_hotplug=1`
 - pour un raspberry PI 5 remplacez -pi4 par -pi5.

10. Si la ligne n'est pas trouvé c'est que la configuration est plus récente. il faut alors rajouter ces lignes directement dans le fichier vers la fin.

11. Rebootez

Enfin sur votre machine Hôte:

1. Installez Tigervnc-viewer; c'est le seul qui est compatible avec les certificats de ce VNC
2. Sélectionnez l'adresse IP de votre raspberry
3. Connectez vous, acceptez les certificats
4. Entrez le login et mot de passe de votre compte sudo du raspberry.
5. C'est fait Si vous ne souhaitez pas démarrer automatiquement x11vnc, ne créez pas le fichier 'vnc server.desktop' dans le répertoire autostart.

Configuration basique

Vérification du nom de serveur

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

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

```
cat /etc/hostname
```

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

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

```
vi /etc/hostname
```

Changez la valeur, sauvegardez et rebootez. Tapez :

```
reboot
```

- b. Loguez vous comme root sur le serveur

3. Vérifier le fichier hosts. Tapez :

```
cat /etc/hosts
```

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

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

Tapez:

```
vi /etc/hosts
```

b. Changez la ou les lignes, sauvegardez.

i Note

Le FQDN (nom de machine avec le nom de domaine) doit être déclaré avant le hostname simple dans le fichier `hosts`. Pour que la configuration de votre serveur de mail soit correcte vous devez installer un FQDN contenant l'adresse de mail comme `mail.example.com`

c. Rebootez. Tapez :

```
reboot
```

d. Loguez vous comme root sur le serveur

4. Vérifiez que tout est correctement configuré.

a. Tapez :

```
hostname
```

La sortie doit afficher le nom de host.

b. Tapez ensuite :

```
hostname -f
```

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

c. Reconfigurez les clés SSH server si vous avez changé le Hostname.

Tapez:

```
rm -v /etc/ssh/ssh_host_*
```

```
dpkg-reconfigure openssh-server
```

d. Les nouvelles clés vont être regénérées.

e. Déconnectez vous de votre session SSH et reconnectez vous.

f. Sur votre poste de travail, la clé d'authentification du serveur aura changée. il vous faudra annuler l'ancien puis accepter la nouvelle.

g. Tapez :

```
ssh-keygen -f "$HOME/.ssh/known_hosts" -R hostname
```

■ remplacer hostname par l'adresse IP ou le nom de machine

h. Reloguez vous comme root sur le serveur

Mettre l'éditeur de votre choix

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

Pour les débutants, il est conseillé d'utiliser `nano` pour les utilisateurs avancés, vous pouvez utiliser `vim`

[Loguez vous comme root .](#)

Si vous voulez installer `vim`, tapez:

```
apt install vim
```

Pour Sélectionner votre éditeur par défaut, tapez:

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

choisissez le chiffre correspondant à Nano ou Vim.basic et quittez.

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. Elle permet de garder dans un repository GIT toutes les modifications qui sont effectuées dans `/etc` soit par vous soit au moment de l'installation de paquets.

1. [Loguez vous comme root sur le serveur](#)

2. Tapez :

```
apt update  
apt install etckeeper
```

3. Vous pouvez créer un repository privé dans le cloud pour stocker votre configuration de serveur (autre serveur privé de confiance ou repository privé Gitlab ou Github).

4. Ajoutez ce repository distant. Pour Gitlab et Github, une fois le repository créé, demandez l'affichage de la commande git pour une communication en ssh. Tapez ensuite sur votre serveur :

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

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

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

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

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

```
PUSH_REMOTE="origin"
```

7. Pour éviter des 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:

1. Créer un répertoire `/root/.ssh` s'il n'existe pas. tapez :

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

2. Allez dans le répertoire. Tapez :

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

3. Générez vous clés. Tapez :

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

4. 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.

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

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

8. Effectuez un premier push. Tapez:

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

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

10. Lancer `etckeeper`. Tapez:

```
etckeeper commit
```

11. Tout le contenu de `/etc` est poussé sur le repository. Saisissez un commentaire.

12. C'est fait !

Mise à jour des sources de paquets Debian ou Ubuntu

1. [Loguez vous comme root sur le serveur](#)

2. Selon la distribution installée suivez la procédure ci-après ou celle suivante.

3. Modifier la liste standard de paquets Debian

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 bookworm-backports main contrib non-free` enlever le `#` en début de ligne

c. Ajouter sur toutes les lignes les paquets `contrib` et `non-free`. en ajoutant ces textes après chaque mot `main` du fichier `source.list`

d. Le fichier doit ressembler à ceci:

```
deb http://deb.debian.org/debian bookworm main contrib non-free  
non-free-firmware
```

```
## Major bug fix updates produced after the final release of the  
## distribution.
```

```
deb http://security.debian.org/debian-security bookworm-security  
main contrib non-free non-free-firmware
```

```
deb http://deb.debian.org/debian bookworm-updates main contrib  
non-free non-free-firmware
```

```
## N.B. software from this repository may not have been tested as
```

```
## extensively as that contained in the main release, although it
includes
## newer versions of some applications which may provide useful
features.
deb http://deb.debian.org/debian bookworm-backports main contrib
non-free non-free-firmware
```

4. Modifier la liste standard de paquets Ubuntu

- Éditer le fichier /etc/apt/sources.list. Tapez:

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

- Dé-commenter les lignes débutant par `deb` enlever le `#` en début de ligne

5. Effectuer une mise à niveau du système

- Mettez à jour la liste des paquets. Tapez:

```
apt update
```

- Installez les nouveautés. Tapez:

```
apt dist-upgrade
```

6. Effectuez du ménage. Tapez:

```
apt autoremove
```

Installation des paquets de base

- Loguez vous comme root sur le serveur

- Tapez:

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

Passage de la locale en FR

- Loguez vous comme root sur le serveur

- Tapez:

```
apt install locales
```

- Tapez ensuite:

```
dpkg-reconfigure locales
```

1. Dans l'écran qui apparait, sélectionnez: `fr_FR.UTF_8`
2. Tapez ensuite sur la ligne de commande: `locale`
3. Le texte suivant apparait:

```
LANG=fr_FR.UTF-8
LC_CTYPE="fr_FR.UTF-8"
LC_NUMERIC="fr_FR.UTF-8"
LC_TIME="fr_FR.UTF-8"
LC_COLLATE="fr_FR.UTF-8"
LC_MONETARY="fr_FR.UTF-8"
LC_MESSAGES="fr_FR.UTF-8"
LC_PAPER="fr_FR.UTF-8"
LC_NAME="fr_FR.UTF-8"
LC_ADDRESS="fr_FR.UTF-8"
LC_TELEPHONE="fr_FR.UTF-8"
LC_MEASUREMENT="fr_FR.UTF-8"
LC_IDENTIFICATION="fr_FR.UTF-8"
LC_ALL=
```

1. Tapez ensuite la ligne suivante pour installer l'environnement en français:

```
apt install task-french
```

Installer l'outil Debfoster

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

Cette installation est optionnelle.

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

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

1. [Loguez vous comme root sur le serveur](#)
2. Ajouter le paquet `debfoster`. Tapez :

```
apt install debfoster
```

3. Lancez `debfoster`. Tapez :

```
debfoster
```

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

Ci-dessous une petite liste de paquets à conserver sur une installation basique Debian 64 pour Raspberry Pi:

apt-file	apt-listchanges	apt-rdepends	apt-transport-https
avahi-daemon	build-essential	cifs-utils	console-setup
crda	debconf-utils	debconf	dphys-swapfile
dselect	ethtool	fake-hwclock	fbset
firmware-atheros	firmware-brcm80211	firmware-libertas	firmware-misc-nonfree
firmware-realtek	gdb	hardlink	htop
libpam-chksshpwd	libraspberrypi-doc	locales	man-db
mkvtoolnix	ncdu	nfs-common	ntpdate
p7zip-full	pi-bluetooth	pkg-config	python-is-python3
raspberrypi-net-mods	raspinfo	rng-tools	rpi-update
rsync	ssh	ssh-import-id	strace
sudo	udisks2	usb-modeswitch	userconf-pi
v4l-utils	wireless-tools	wpa_supplicant	zip

La même liste pour un Ubuntu pour Raspberry Pi:

apt-file	apt-listchanges	apt-rdepends	apt-transport-https

cloud-init	debfoster	etckeeper	language-pack-fr
linux-firmware-raspi2	linux-raspi	manpages-fr	ntpdate
openssh-server	u-boot-rpi	ubuntu-server	ubuntu-standard
wpasupplicant			

Création d'un fichier keeper dans /etc

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

1. Loguez vous comme root sur le serveur

2. Tapez:

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

3. Saisissez dans le fichier:

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

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

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

if [ "$VCS" = git ] || [ "$VCS" = hg ] || [ "$VCS" = bzr ] || [
"$VCS" = darcs ]; then
    # Make sure the file is not readable by others, since it can
    # leak
    # information about contents of non-readable directories
    # in /etc.
```

```
debfoster -q -k /etc/keepers
chmod 600 /etc/keepers
sed -i "li\\# debfoster file" /etc/keepers
    sed -i "li\\# Generated by etckeeper. Do not edit."
/etc/keepers

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

4. Sauvez et tapez:

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

5. Exécutez maintenant etckeeper

```
etckeeper commit
```

6. Le fichier keepers est créé et sauvegardé automatiquement.

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.



Warning

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.

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. Tapez:

```
apt install unattended-upgrades
```

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.

Avec les versions récentes de Debian Bookworm pour raspberry pi, il n'est plus nécessaire de créer le compte sudo qui est créé par défaut lors de la procédure d'installation standard. Cette procédure est cependant indispensable pour l'installation d'une distribution debian standard.

Une remarque tout de même pour le raspberry pi: le compte sudo permet de se logger root sans aucun mot de passe. C'est considéré comme une faille de sécurité. Pour corriger cela, [Loguez vous comme root sur le serveur](#) et tapez:

```
rm -f /etc/sudoers.d/010_pi-nopasswd
```

La procédure suivante s'applique pour la création du compte sudo sur une debian standard.

Notre première action sera de désactiver le login direct en root et d'autoriser le sudo.

Respectez bien les étapes de cette procédure:

1. [Loguez vous comme root sur le serveur](#)

2. Installez l'outil sudo s'il n'est pas déjà présent. Tapez:

```
apt install sudo
```

3. Ajoutez un utilisateur standard qui sera nommé par la suite en tant que <sudo_username>

a. Tapez :

```
adduser <sudo_username>
```

■ remplacer ici <sudo_username> par votre login

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>
```

- remplacer ici <sudo_username> par votre login

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

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

- 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, vérifiez la procédure et repassez toutes les étapes.

! Important

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>
```

- 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.

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  
chmod 700 ~/.ssh
```

- c. Allez dans le répertoire. Tapez :

```
cd ~/.ssh
```

- d. Générez vous clés. Tapez :

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

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

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

```
cat ~/.ssh/id_rsa.pub
```

3. Déployez votre clé:

- a. Loguez vous sur votre serveur distant. Tapez :

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

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

Entrez votre mot de passe

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

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

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

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

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

d. Sécurisez votre fichier de clés. Tapez: :

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

e. Sécurisez le répertoire SSH; Tapez :

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

f. Déconnectez vous de votre session

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

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

- 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.

Sudo sans mot de passe

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

1. [Loguez vous comme root sur le serveur](#)

2. Ajoutez un groupe sudonp et y affecter un utilisateur. Tapez :

```
addgroup --system sudonp
```

a. Ajouter l'utilisateur: :

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

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

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

c. Éditez le fichier sudoers. Tapez :

```
vi /etc/sudoers.d/010_sudonp
```

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

Configuration du Motd

Le motd est affiché au moment où l'utilisateur se loggue en ssh. Nous allons configurer l'affichage de plusieurs informations importantes.

Installation de Neofetch

Neofetch affiche au démarrage de votre système des informations sur le fonctionnement de celui-ci.

Nous allons créer une configuration système:

1. Loguez vous comme root sur le serveur

2. Installez le package neofetch. Tapez :

```
apt install neofetch
```

3. Editez ensuite le fichier /etc/neofetch.conf. Tapez:

```
vi /etc/neofetch.conf
```

4. Mettez ensuite dans le fichier la configuration suivante:

```
print_info() {  
    info title  
    info underline  
  
    info "OS" distro  
    info "Host" model  
    info "Kernel" kernel  
    info "Uptime" uptime  
    info "Packages" packages  
    info "Shell" shell  
    info "Resolution" resolution  
    info "DE" de
```

```

    info "WM" wm
    info "WM Theme" wm_theme
    info "Theme" theme
    info "Icons" icons
    info "Terminal" term
    info "Terminal Font" term_font
    info "CPU" cpu
    info "CPU Usage" cpu_usage
    prin "CPU Temp" "$(vcgencmd measure_temp | awk -F '=' '{print $2}')"
    prin "Load" "$(cat /proc/loadavg | awk '{print $1, $2, $3}')"
    info "GPU" gpu
    info "GPU Driver" gpu_driver # Linux/macOS only
    info "Memory" memory
    info "Disk" disk
    info "Local IP" local_ip
    info "Public IP" public_ip
    info "Users" users
    info "Locale" locale # This only works on glibc systems.

    info cols
}

title_fqdn="on"
memory_percent="on"
memory_unit="mib"
package_managers="on"
image_backend="ascii"
cpu_temp="on"

    ○ Cette ligne est à retirer si vous n'utilisez pas de Raspberry PI 4 ou 5

```

Configuration du MOTD avec Neofetch

Pour afficher les informations au moment du login ssh, vous devez modifier le fichier Motd:

1. [Loguez vous comme root sur le serveur](#)
2. Editez le fichier Neofetch du MOTD

```
vi /etc/update-motd.d/20-neofetch
```

3. Mettez ensuite dans le fichier la configuration suivante:

```
#!/bin/sh
neofetch --config /etc/neofetch.conf
```

4. Changez les permissions du fichier 20-neofetch. Tapez:

```
chmod 755 /etc/update-motd.d/20-neofetch
```

5. A notez que vous pouvez utiliser Neofetch pour votre fichier .bash_profile

Mise à jour de packages

Vous pouvez ajouter la liste des mises à jours dans le fichier MOTD:

1. Installez le package python de gestion APT. Tapez :

```
apt install python3-apt
```

2. Editez le fichier MOTD

```
vi /etc/update-motd.d/30-updates
```

3. Dans le fichier mettez le contenu suivant:

```
#!/usr/bin/python3
import sys
import subprocess
import apt_pkg

DISTRO = subprocess.Popen(["lsb_release", "-c", "-s"],
                        stdout=subprocess.PIPE).communicate()
[0].strip()

class OpNullProgress(object):
    '''apt progress handler which supresses any output.'''
    def update(self):
        pass
    def done(self):
        pass

    def is_security_upgrade(pkg):
        '''
        Checks to see if a package comes from a DISTRO-security source.
        '''

        security_package_sources = [("Ubuntu", "%s-security" % DISTRO),
                                    ("Debian", "%s-security" % DISTRO)]
```

```
for (file, index) in pkg.file_list:
    for origin, archive in security_package_sources:
        if (file.archive == archive and file.origin == origin):
            return True
    return False

# init apt and config
apt_pkg.init()

# open the apt cache
try:
    cache = apt_pkg.Cache(OpNullProgress())
except SystemError as e:
    sys.stderr.write("Error: Opening the cache (%s)" % e)
    sys.exit(-1)

# setup a DepCache instance to interact with the repo
depcache = apt_pkg.DepCache(cache)

# take into account apt policies
depcache.read_pinfile()

# initialise it
depcache.init()

# give up if packages are broken
if depcache.broken_count > 0:
    sys.stderr.write("Error: Broken packages exist.")
    sys.exit(-1)

# mark possible packages
try:
    # run distro-upgrade
    depcache.upgrade(True)
    # reset if packages get marked as deleted -> we don't want to
    # break anything
    if depcache.del_count > 0:
        depcache.init()

    # then a standard upgrade
```

```

    depcache.upgrade()

except SystemError as e:
    sys.stderr.write("Error: Couldn't mark the upgrade (%s)" % e)
    sys.exit(-1)

# run around the packages
upgrades = 0
security_upgrades = 0
for pkg in cache.packages:
    candidate = depcache.get_candidate_ver(pkg)
    current = pkg.current_ver

    # skip packages not marked as upgraded/installed
    if not (depcache.marked_install(pkg) or
            depcache.marked_upgrade(pkg)):
        continue

    # increment the upgrade counter
    upgrades += 1

    # keep another count for security upgrades
    if is_security_upgrade(candidate):
        security_upgrades += 1

    # double check for security upgrades masked by another package
    for version in pkg.version_list:
        if (current and apt_pkg.version_compare(version.ver_str,
        current.ver_str) <= 0):
            continue
        if is_security_upgrade(version):
            security_upgrades += 1
            break

print("%d updates to install." % upgrades)
print("%d are security updates." % security_upgrades)
print("") # leave a trailing blank line

```

4. Changez les permissions du fichier 30-updates. Tapez:

```
chmod 755 /etc/update-motd.d/30-updates
```

Installer l'outil `dselect`

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

1. [Loguez vous comme root sur le serveur](#)
2. Ajouter le paquet `dselect`. Tapez :

```
apt install dselect
```

Ajouter un fichier de swap

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

Enfin pour un Raspberry PI 3 avec 1 Go de Ram, il faut ajouter 1 Go de swap.

Tapez :

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

```
dphys-swapfile uninstall
```

3. Pour installer un swap de 4Go, tapez:

```
cd /
fallocate -l 4G /swapfile
chmod 600 /swapfile
mkswap /swapfile
swapon /swapfile
```

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

```
vi /etc/fstab
```

5. Ajoutez la ligne:

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

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

```
vi /etc/sysctl.conf
```

7. Ajoutez ou modifiez la ligne:

```
vm.swappiness = 5
```

8. Le paramètre sera actif au prochain reboot

Installation initiale des outils

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

L'installation est simplifiée grâce à l'utilisation de l'autoinstalleur d'ISPConfig.

cet installeur fonction pour les version de Debian 10, 11 et 12 et Ubuntu 20.04 à 24.04

1. [Loguez vous comme root sur le serveur](#)

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 a été utilisé dans ce tutoriel.

1. Tapez:

```
hostname -f
```

2. La sortie doit être du type:

```
mail.example.com
```

3. Si ce n'est pas le cas corrigez le FQDN en vous référant au chapitre [Vérification du nom de serveur](#).

4. Nous allons maintenant installer [ISPConfig](#) avec l'autoinstalleur.

5. Mettez à jour le système. tapez:

```
apt update && apt dist-upgrade
```

6. Exécutez l'autoinstalleur en tapant:

```
wget -O - https://get.ispconfig.org | sh -s -- --use-ftp-ports=40110-40210 --unattended-upgrades
```

- vous pouvez remplacer l'éventail de ports FTP par d'autres si vous voulez.

7. Au bout d'un moment vous verrez s'afficher:

```
WARNING! This script will reconfigure your complete server!  
It should be run on a freshly installed server and all current  
configuration that you have done will most likely be lost!  
Type 'yes' if you really want to continue
```

8. Répondez 'yes'. L'installation démarre.

9. Lorsque l'installation se termine vous verrez:

```
[INFO] Your ISPConfig admin password is: 5GvfSSSYsdfdYC  
[INFO] Your MySQL root password is: kkAkft82d!kafMwqxdtYs
```

10. Notez ces informations, elles vous serviront pour vous connecter au panel ISPConfig ou à votre base mysql (PhpMyAdmin).

11. L'installation est terminée. Vous accédez au serveur à l'adresse:

<https://example.com:8080/>.

Note981267

Lors de votre première connexion, votre domaine n'est pas encore configuré. Il faudra alors utiliser le nom DNS donné par votre hébergeur pour votre machine. Pour Contabo, elle s'écrit vmixxxxxx.contaboserver.net.

12.. Loguez vous avec le login `admin` et le mot de passe que vous avez récupéré plus haut.

i Note

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.

Vous pouvez passer maintenant à la suite de la configuration.

Configuration Manuelle des outils

Ce chapitre décrit comment configurer manuellement Postfix, Mariadb, Apache, Awstats, Fail2ban, Pureftpd, Phpmyadmin, Roundcube, Letsencrypt manuellement.

Ce chapitre est à sauter si vous avez installé ISPConfig. Vous devez poursuivre vers [Suite de l'installation](#)

Commencez l'installation:

1. [Loguez vous comme root sur le serveur](#)

2. Installez quelques outils de base. Tapez :

```
apt install packages ssh, openssh-server, nano, vim-nox, lsb-release,  
apt-transport-https, ca-certificates, wget, git, gnupg, software-  
properties-common, curl, cron, ntp
```

3. Installez ensuite:

```
apt install dbconfig-common, postfix, postfix-mysql, mariadb-client,  
mariadb-server, openssl, rkhunter, binutils, sudo, getmail6, rsyslog  
dovecot-imapd, dovecot-pop3d, dovecot-mysql, dovecot-sieve, dovecot-  
managesieved, dovecot-lmtpd
```

4. Puis installez:

```
apt install software-properties-common update-inetd dnsutils  
resolvconf clamav clamav-daemon zip unzip bzip2 xz-utils lzip  
borgbackup arj nomarch lzop cabextract apt-listchanges libnet-ldap-  
perl libauthen-sasl-perl daemon libio-string-perl libio-socket-ssl-  
perl libnet-ident-perl libnet-dns-perl libdbd-mysql-perl bind9 rspamd  
redis-server postgrey p7zip p7zip-full unrar-free lrzip
```

5. Installez:

```
apt install apache2 apache2-utils libapache2-mod-fcgid apache2-  
suexec-pristine libapache2-mod-python libapache2-mod-passenger
```

6. Installez:

```
apt install php php-pear php-memcache php-imagick mcrypt imagemagick  
libruby memcached php-apcu jailkit
```

7. Déterminer votre version de php. Tapez:

```
LC_ALL='C' apt list -a 'php*' | grep -E 'php[0-9]+.[0-9]+/' | grep '\  
[installed\]' | sed 's/(.*\)\/.*/\1/'
```

8. En fonction de la version affichée Installez les packages PHP :

```
for i in php#-gd php#-mysql php#-imap php#-cli php#-curl php#-intl
php#-pspell php#-sqlite3 php#-tidy php#-xsl php#-zip php#-mbstring
php#-soap php#-opcache php#-cgi php#-fpm php#-xmlrpc

do
echo $i | sed 's/#/version/'
done | xargs apt install -y
```

- remplacer ici version par la version affichée plus haut. Par exemple 8.3

9. Installez:

```
apt install haveged geoip-database libclass-dbi-mysql-perl
libtimedate-perl build-essential autoconf automake libtool flex bison
debhelper binutils quota quotatool
```

10. Installez:

```
apt install pure-ftpd-common pure-ftpd-mysql awstats goaccess awffull
```

Configuration manuelle de Postfix

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur

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

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

3. Ajoutez ou modifiez dans le fichier:

```
append_dot_mydomain = yes
mydestination = mail.example.com, localhost, localhost.localdomain
```

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

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

5. Ajoutez dans le fichier:

```
submission inet n - y - - 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
```

```
submissions      inet  n   -     y     - - smtpd
```

```
-o syslog_name=postfix/submissions  
-o smtpd_tls_wrappermode=yes  
-o smtpd_sasl_auth_enable=yes  
-o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

6. Sauvegardez et relancez Postfix:

```
systemctl restart postfix
```

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

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

i Note

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

i Note

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

Configuration manuelle de MariaDB

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. 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
3. MariaDB doit pouvoir être atteint par toutes les interfaces et pas seulement localhost.
4. Éditez le fichier de configuration. :
- ```
vi /etc/mysql/mariadb.conf.d/50-server.cnf
```
5. Commentez la ligne bind-address:
- ```
#bind-address      = 127.0.0.1
```
6. 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
```
7. Editez le fichier debian.cnf. Tapez :
- ```
vi /etc/mysql/debian.cnf
```
- a. Aux deux endroits du fichier où le mot clé password est présent, mettez le mot de passe root de votre base de données.
- ```
password = votre_mot_de_passe
```
- i** Note  
Dans les versions récentes de Debian et Ubuntu, le mot clé password n'est pas présent. Il n'y a rien à faire.
8. 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
```

## 9. 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
```

## 10. Redémarrez votre serveur MariaDB. Tapez::

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

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

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

## 12.La sortie doit être du type:

```
tcp 0 0 0.0.0.0:mysql 0.0.0.0:* LISTEN 1146/mariadb
tcp6 0 0 :::mysql :::* LISTEN 1146/mariadb
```

## ***Configuration manuelle d'Apache***

Suivez la procédure suivante:

### 1. Loguez vous comme root sur le serveur

### 2. 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
```

### 3. 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>
```

4. Activez le module en tapant :

```
a2enconf httpoxy
systemctl restart apache2
```

5. Désactiver la documentation apache en tapant:

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

## ***Configuration manuelle d'Awstats***

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. Configurer la tache cron d'awstats: Éditez le fichier :

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

3. 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
```

## ***Configuration manuelle de Fail2ban***

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. Editez le fichier jail.local :

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

Ajoutez les lignes suivantes:

```
[pure-ftpd]
enabled = true
```

```

port = ftp
filter = pure-ftpd
logpath = /var/log/syslog
maxretry = 3

[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

```

### 3. Redémarrez Fail2ban:

```
systemctl restart fail2ban
```

## ***Installation et configuration manuelle de PureFTPD***

Suivez la procédure suivante:

### 1. Loguez vous comme root sur le serveur

### 2. Tapez:

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

### 3. Éditez le fichier de conf:

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

### 4. Changez les lignes ainsi:

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

### 5. Autorisez les connexions TLS. Tapez:

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

### 6. 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] : ← Entrer 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] : ← Entrer votre entreprise ou tapez entrée
- v. Organizational Unit Name (eg, section) [] : ← Tapez entrée
- vi. Common Name (e.g. server FQDN or YOUR name) [] : ← Enter le nom d'hôte de votre serveur. Dans notre cas: server1.example.com
- vii. Email Address [] : ← Tapez entrée

c. Puis tapez :

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

d. et redémarrez pure-ftpd en tapant: :

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

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

- Installez les paquets de gestion des quotas. Tapez:

```
apt install quota quotatool
```

- Editez fstab. Tapez:

```
vi /etc/fstab
```

- Inserez le texte ci dessous pour chaque directive de montage autre que

```
/proc OU /swapfile :
```

```
usrquota=quota.user,grpquota=quota.group,jqfmt=vfsv0
```

- Par exemple pour une ligne de la table contenant:

```
UUID=45576b38-39e8-4994-b8c1-ea4870e2e614 /
errors=remount-ro 0 1
```

- Vous obtiendrez:

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

- Pour une Raspbian:

- Editez le fichier rc.local pour créer /dev/root à chaque reboot:

```
ln -s /dev/mmcblk0p7 /dev/root
vi /etc/rc.local
```

- Ajoutez avant exit 0:

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

- Pour activer les quotas, tapez:

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

## ***Installation et configuration manuelle de Phpmyadmin***

### **Installation de Phpmyadmin**

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur
2. allez sur le site de [phpMyAdmin](#) et copier l'adresse du lien vers la dernière version de l'outil.
3. 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
```

```
version=`wget -O - https://www.phpmyadmin.net/home_page/version.txt
2> /dev/null | head -n 1`
echo https://files.phpmyadmin.net/phpMyAdmin/#/phpMyAdmin-#-all-
languages.tar.gz | sed 's/#/$version/g' | xargs wget -O
phpmyadmin.tar.gz
tar xfz phpmyadmin.tar.gz
mv phpMyAdmin-$version-all-languages/* /usr/share/phpmyadmin/
rm phpMyAdmin-$version-all-languages.tar.gz
rm -rf phpMyAdmin-$version-all-languages
cp /usr/share/phpmyadmin/config.sample.inc.php
/usr/share/phpmyadmin/config.inc.php
```

4. Créez votre chaîne aléatoire en base64. Tapez:

```
tr -dc A-Za-z0-9 < /dev/urandom | head -c${1:-32};echo;
```

5. Copiez le texte généré

6. Éditez le fichier :

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

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

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 SymLinksIfOwnerMatch
```

```
 DirectoryIndex index.php
```

```
 # limit libapache2-mod-php to files and directories
```

```
 necessary by pma
```

```
 <IfModule mod_php7.c>
```

```
 php_admin_value upload_tmp_dir
```

```
 /var/lib/phpmyadmin/tmp
```

```
 php_admin_value open_basedir
/usr/share/phpmyadmin/:/etc/phpmyadmin/:/var/lib/phpmyadmin/:/usr/
share/php/:/usr/share/javascript/
</IfModule>

PHP 8+
<IfModule mod_php.c>
 php_admin_value upload_tmp_dir
/var/lib/phpmyadmin/tmp
 php_admin_value open_basedir
/usr/share/phpmyadmin/:/etc/phpmyadmin/:/var/lib/phpmyadmin/:/usr/
share/php/:/usr/share/javascript/
</IfModule>

</Directory>

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

Disallow web access to directories that don't need it
<Directory /usr/share/phpmyadmin/templates>
 Require all denied
</Directory>
<Directory /usr/share/phpmyadmin/libraries>
 Require all denied
</Directory>
<Directory /usr/share/phpmyadmin/setup/lib>
 Require all denied
</Directory>
```

## 7. Activez le module et redémarrez apache. Tapez :

```
a2enconf phpmyadmin
systemctl restart apache2
```

## 8. Créez 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';
```

- 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;
```

- mypassword doit être remplacé par le mot de passe choisi plus haut.

### e. Flusher les privilèges:

```
FLUSH PRIVILEGES;
```

### f. et enfin

```
EXIT;
```

## 9. Chargez les tables sql dans la base phpmyadmin:

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

## 10. 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 controlpass . 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';
```

- 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.

## Upgrade de Phpmyadmin

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur
2. allez sur le site de [phpMyAdmin](#) et copier l'adresse du lien vers la dernière version de l'outil.
3. Mettez à jour phpmyadmin. Exécutez:

```
mv /usr/share/phpmyadmin /usr/share/phpmyadmin.old
mkdir /usr/share/phpmyadmin
cd /tmp
version=`wget -O - https://www.phpmyadmin.net/home_page/version.txt
2> /dev/null | head -n 1`
echo https://files.phpmyadmin.net/phpMyAdmin/#/phpMyAdmin-#-all-
languages.tar.gz | sed 's/#/$version/g' | xargs wget -O
phpmyadmin.tar.gz
tar xfz phpmyadmin.tar.gz
mv phpMyAdmin-$version-all-languages/* /usr/share/phpmyadmin/
rm phpMyAdmin-$version-all-languages.tar.gz
rm -rf phpMyAdmin-$version-all-languages
cp /usr/share/phpmyadmin.old/config.inc.php
/usr/share/phpmyadmin/config.inc.php
```

4. Redémarrez apache. Tapez :

```
systemctl restart apache2
```

5. Vérifiez que tout fonctionne correctement sur le site phpmyadmin

6. Supprimez l'ancien répertoire

```
rm -rf /usr/share/phpmyadmin.old
```

## Installation manuelle du webmail Roundcube

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur

2. Tapez:

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

3. Répondez aux question

- Utiliser dbconfig\_common ← Répondre Oui
- Mot de passe Mysql pour db Roundcube ← Tapez un mot de passe

4. Éditez le fichier php de roundcube :

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

5. Et chercher les éléments de \$config si dessous, et s'ils sont trouvés, remplacez les par les valeurs indiquées :

```
$config['default_host'] = 'localhost';
$config['smtp_server'] = 'localhost';
$config['imap_host'] = ["localhost:143"];
$config['smtp_host'] = 'localhost:25';
```

6. 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/public_html
Alias /webmail /var/lib/roundcube/public_html
```

7. Redémarrez Apache:

```
systemctl reload apache2
```

## ***Installation manuelle de Let's Encrypt***

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur

2. Installez Let's Encrypt. Tapez:

```
cd /tmp ; wget -O - https://get.acme.sh 2>/dev/null | sh 2>/dev/null
```

3. Une façon alternative de l'installer est:

```
apt install certbot
```

## Suite de l'installation

Les chapitres suivants doivent être suivis que ISPConfig soit installé ou pas.

### **Déblocage de port de firewall**

Par défaut, une fois le firewall activé, TOUS les ports sont bloqués en entrée de votre équipement. Cela veut dire qu'il ne sera pas possible de connecter une machine externe sur votre équipement sans avoir effectué une opération de déblocage du port du firewall.

Il existe deux manières de débloquer un port. Elle dépend de ce que vous avez configuré.

### **Déblocage et suppression de règles de Firewall avec ISPconfig**

Appliquez les opérations suivantes pour Débloquez le firewall:

1. Allez sur le site ispconfig <https://example.com:8080/>
2. Loguez-vous et cliquez sur la rubrique `System` et le menu `Firewall`. Cliquez sur votre serveur.
3. dans la rubrique `Open TCP ports:`, ajoutez le numéro de port xxxx que vous souhaitez débloquer
4. Cliquez sur `save`

Appliquez les opérations suivantes bloquer (en lever une règle de déblocage) de firewall:

1. Allez sur le site ispconfig <https://example.com:8080/>
2. Loguez-vous et cliquez sur la rubrique `System` et le menu `Firewall`. Cliquez sur votre serveur.
3. dans la rubrique `Open TCP ports:`, Supprimer le port xxxx
4. Cliquez sur `save`

Remarque: si vous utilisez VNC, il faut débloquer le port dans le firewall de ISPConfig.  
Appliquez la méthode de déblocage pour le port 5900.

Remarque: si vous avez besoin de débloquer un port UDP vous devez aller dans la rubrique Open UDP Ports.

## Déblocage de Firewall UFW

### Important981267

Si vous avez installé ISPconfig vous ne devez pas utiliser cette méthode !

Tout d'abord, à la première utilisation, il vous faut appliquer la procédure suivante:

1. Installez ufw. Tapez:

```
apt install ufw
```

2. Autorisez SSH si vous ne voulez pas perdre votre connexion SSH à l'activation du firewall. Tapez:

```
ufw allow 22/tcp
ufw allow 80/tcp
ufw allow 443/tcp
ufw allow 5900/tcp
```

- Cette ligne autorise VNC et est utile si vous utilisez ce protocole sur votre Système. Il est fortement déconseillé pour un serveur visible sur internet d'autoriser ce protocole.

3. Activez le firewall. tapez:

```
ufw enable
```

4. C'est prêt !

Appliquez les opérations suivantes pour Débloquez le firewall:

1. Loguez vous comme root sur le serveur

2. Tapez:

```
ufw allow xxxx/tcp
```

- remplacez xxxx par le numero de port que vous souhaitez débloquer

Appliquez les opérations suivantes bloquer (en lever une règle de déblocage) de firewall:

1. Loguez vous comme root sur le serveur

2. Tapez:

```
ufw delete allow xxxx/tcp
```

- remplacez xxxx par le numero de port que vous souhaitez débloquer

## Scan des vulnérabilités

### Installation d'un scanner de vulnérabilités Lynis

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur

2. installer Git. Tapez :

```
apt install git
```

3. installer Lynis

- a. Tapez :

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

- b. Executez :

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

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

## Upgrade de Lynis

Pour effectuer la mise à jour de Lynis appliquez la procédure suivante:

1. Loguez vous comme root sur le serveur

2. Tapez :

```
cd
cd lynis
```

```
git pull
```

## ***Installation du système d'administration Webmin***

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

1. [Loguez vous comme root sur le serveur](#)

2. Lancez le script de configuration de webmin:

```
curl https://raw.githubusercontent.com/webmin/webmin/master/setup-repos.sh -o setup-repos.sh
sh setup-repos.sh
rm setup-repos.sh
```

3. Mise à jour. Tapez :

```
apt update
```

4. Installation de Webmin. Tapez :

```
apt install webmin
```

5. [Debloquez le port 10000 sur votre firewall](#)

6. Changer le nom du user admin

7. Editez le fichier `miniserv.users`. Tapez:

```
vi /etc/webmin/miniserv.users
```

8. Dans le fichier remplacer le texte `root` par le nom de votre `<sudo_username>`.

9. De la même manière, éditer le fichier `webmin.acl`. Tapez:

```
vi /etc/webmin/webmin.acl
```

10. Dans le fichier remplacer le texte `root` par le nom de votre `<sudo_username>`.

11. Tapez :

```
service webmin restart
```

12. 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'.

13. Loguez-vous <sudo\_username>. Tapez le mot de passe de <sudo\_username>. Le dashboard s'affiche.

14. Restreignez l'adressage IP

- a. Obtenez votre adresse IP en allant par exemple sur le site <https://www.showmyip.com/>
- b. Sur votre URL Webmin où 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.

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

- a. Loguez vous comme root sur le serveur
- b. Éditez le fichier /etc/webmin/miniserv.conf et supprimez la ligne allow= ...
- c. Tapez :  

```
service webmin restart
```
- d. Connectez vous sur l'url de votre site Webmin. Tout doit fonctionner

16. Compléments de configuration

- a. Pour augmenter la sécurité, vous pouvez désactiver le login sudo\_username et créer un autre compte admin en allant dans: Webmin → Webmin Users → Create a new privileged user. Pour le user sudo\_username, modifier le Password en mettant No password accepted

b. Allez dans Webmin → Webmin Configuration → SSL Encryption → onglet Let's Encrypt → Request Certificate. Attention cette opération ne fonctionne que si le serveur est disponible sur internet.

17. 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)

## 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/>.

### ***Login initial***

**i** Note

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://vmixxxxxx.contaboserver.net:8080/> pour un vps chez contabo par exemple ou sur <http://raspberrypi.local:8080/> pour un Raspberry.

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

1. Aller dans la rubrique System

a. Dans le menu `Main config`

i. Dans l'onglet `Sites`, configurer:

A. `Create subdomains as web site:` ← Yes

B. `Create aliasdomains as web site:` ← Yes

ii. Dans l'onglet `Mail`:

A. `Administrator's e-mail` : ← adresse mail de l'administrateur. par exemple [admin@example.com](mailto:admin@example.com)

B. `Administrator's name` : ← nom de l'administrateur

iii. Cliquez sur `Save`

b. Dans le menu `Firewall`

i. Cliquez sur `Add Firewall Record`

ii. Acceptez les valeurs par défaut en cliquant sur `Save`

**i** Note

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

2. Aller dans la rubrique `DNS`

a. Dans le menu `Templates`

i. Cliquez sur `Add new record`

ii. Remplissez les champs comme ci-après:

- `Name` ← Tapez `Template IPV4 autoNS`
- `Fields` ← Cochez `Domain, IP Address, Email, DKIM, DNSSEC`
- `Template` ← remplissez comme ci dessous:  
`[ZONE]`  
`origin={DOMAIN}.`

```
ns=ns1.{DOMAIN} .
mbox={EMAIL} .
refresh=7200
retry=540
expire=604800
minimum=3600
ttl=3600
xfer=
also_notify=
dnssec_wanted=N
dnssec_algo=ECDSAP256SHA256

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

iii. Cliquez sur Save

iv. Cliquez sur Add new record

v. Remplissez les champs comme ci-après:

- Name ← Tapez Template IPV6 autoNS

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

```
[ZONE]
origin={DOMAIN}.

ns=ns1.{DOMAIN}.

mbox={EMAIL}.

refresh=7200
retry=540
expire=604800
minimum=3600
ttl=3600
xfer=
also_notify=
dnssec_wanted=N
dnssec_algo=ECDSAP256SHA256

[DNS_RECORDS]
A|{DOMAIN} . |{IP}|0|3600
A|www|{IP}|0|3600
A|mail|{IP}|0|3600
A|autoconfig|{IP}|0|3600
A|autodiscover|{IP}|0|3600
A|webmail|{IP}|0|3600
A|ns1|{IP}|0|3600
AAAA|{DOMAIN} . |{IPV6}|0|3600
AAAA|www|{IPV6}|0|3600
AAAA|mail|{IPV6}|0|3600
AAAA|autoconfig|{IPV6}|0|3600
AAAA|autodiscover|{IPV6}|0|3600
AAAA|webmail|{IPV6}|0|3600
AAAA|ns1|{IPV6}|0|3600
CNAME|ftp|{DOMAIN}|0|3600
CNAME|smtp|{DOMAIN}|0|3600
CNAME|pop3|{DOMAIN}|0|3600
CNAME|imap|{DOMAIN}|0|3600
SRV|_pop3._tcp|0 0 .|0|3600
SRV|_imap._tcp|0 0 .|0|3600
SRV|_pop3s._tcp|1 995 mail.{DOMAIN}|0|3600
SRV|_imaps._tcp|1 993 mail.{DOMAIN}|0|3600
```

```
SRV|_submission._tcp|1 465 mail.{DOMAIN}|0|3600
SRV|_autodiscover._tcp|1 443 autodiscover.{DOMAIN}|0|3600
NS|{DOMAIN}.|ns1.{DOMAIN}.|0|3600
MX|{DOMAIN}.|mail.{DOMAIN}.|10|3600
TXT|{DOMAIN}.|v=spf1 mx a ~all|0|3600
```

## Création de la zone DNS d'un domaine

1. Allez dans DNS
  - a. Cliquez sur Add dns-zone
  - b. Cliquez sur Dns zone wizard
  - c. Choisir le template IPV4 autoNS ou `IPV6 autoNS` selon que vous soyez IPV4 ou IPV4+V6
  - d. Remplissez les champs:
    - Domain : ← tapez le nom de votre domaine example.com
    - IP Address: ← prendre l'adresse IPV4 du serveur sélectionnée
    - IPV6 Address: ← prendre l'adresse IPV6 du serveur sélectionnée
    - Email: ← votre Email valide exemple admin@example.com
    - DKIM: ← Yes

### i Note

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

- e. Cliquez sur Create DNS-record

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

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

**i** Note

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 apparaît 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.

## **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 **zones settings** 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 boîte '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 fonctionnez 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 13 (ECDSAP256SHA256)
  - b. Collez ensuite la clé de votre site ISPConfig. Elle doit ressembler à cela:

```
example.com. IN DNSKEY 257 3 13
CGI4g4NzPkOXeuRzA1ZdB7N5/WJ2su5Q6teGDjVeYq2kwnxbFsYJhjq
QVcqDqm7gzFqP16QC/zK1eC0zrPE9g==
```
  - 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 13 (ECDSAP256SHA256)
  - f. Collez ensuite la clé de votre site ISPConfig. Elle doit ressembler à cela:

```
example.com. IN DNSKEY 256 3 13
YFzB4DJmq0I7K6J17ynU4A+dracTW7qkrMnK5ZIbEO/DtjgJyDPaZn9f
uvJ/KriFY/sdf89XHb4u8q+MQCm/cg==
```
  - 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.

✓ Tip

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

⚠ Warning

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.

## ***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"

```

## **Création d'un sous domaine**

Supposons que vous êtes en train de créer un sous domaine nommé `sub.example.com`.

Dans ce sous domaines vous allez créer un ensemble de site web par exemple `mail.sub.example.com` ou `blog.sub.example.com`.

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

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

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

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

Vous aurez des actions complémentaires à effectuer sur votre domaine:

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

- un enregistrement de type NS avec une Zone  $\leftarrow$  sub.example.com. et un nameserver Hostname  $\leftarrow$  ns2.sub.example.com.
- un enregistrement de type A avec une IP\_Address  $\leftarrow$  IPV4\_NS1 et un Hostname  $\leftarrow$  ns1.sub.example.com.
- un enregistrement de type A avec une IP\_Address  $\leftarrow$  IPV4\_NS2 et un Hostname  $\leftarrow$  ns2.sub.example.com.

Ces deux derniers types d'enregistrement se nomment un Glue record pour faire le lien vers le serveur secondaire.

- Si vous connaissez pas l'adresse IPV4, tapez dans un terminal texte de votre serveur 'sub.example.com':

```
wget -qO- http://ipecho.net/plain; echo
```

4. Si vous avez activé DNSSEC sur votre serveur DNS de sub.example.com vous devrez récupérer les entrées DS du champ DNSSEC DS-Data for registry de votre domaine sub.example.com et créer dans votre domaine example.com les deux entrées suivantes:

- un enregistrement de type DS avec une Zone  $\leftarrow$  sub.example.com. et un champ data contenant xxxxx 7 1 <votre\_digest\_recupérée>
- un enregistrement de type DS avec une Zone  $\leftarrow$  sub.example.com. et un champ data contenant xxxxx 7 2 <votre\_digest\_recupérée>

5. Allez sur le site [DNSSEC Analyzer](#).

6. Entrez votre nom de domaine sub.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 de votre domaine et de votre sous-domaine, chez votre registrar (rubrique DNSSEC) ou regardez les logs d'ISPConfig sur votre serveur pour y débusquer une erreur.

## 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:

- `Client`: ← laisser vide ou mettre le client que vous avez créé.
- `IPv4-Address`: ← mettre \*. Si vous mettez votre adresse IPV4 vous allez rencontrer quelques disfonctionnements.
- `Domain`: ← mettre `example.com`
- `Auto-subdomain`: ← sélectionner `www` ou \* si l'on veut un certificat let's encrypt wildcard
- `SSL`: ← yes
- `Let's Encrypt`: ← yes
- `Php`: ← Sélectionnez `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: ← **ressaissez 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 (locaux, d'autres machines ou de container docker) de saisir dans la zone **Apache Directives**:
- Pour un site en HTTP (attention dans ce cas, ce site doit être local ou dans un container pour des raisons de sécurité) :
- ```

<Proxy *>
    Order deny,allow
    Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

# Original httpserver
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPassMatch ^/(.+)/websocket
ws://localhost[:port_number_if_any]/$1/websocket
keepalive=On # If websocket is in use

ProxyPass /
http://localhost[:port_number_if_any]/[path_if_any]
ProxyPassReverse /
http://localhost[:port_number_if_any]/[path_if_any]

RedirectMatch ^/$ https://www.example.com

```
- remplacer `example.com` par votre nom de domaine

- Pour un site en HTTPS :

```

<Proxy *>
    Order deny,allow
    Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

# redirect from server
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
SSLProxyEngine On # Comment this out if no https required
ProxyPreserveHost On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off

ProxyPass /
https://localhost[:port_number_if_any]/[path_if_any]
ProxyPassReverse /
https://localhost[:port_number_if_any]/[path_if_any]

RedirectMatch ^/$ https://www.example.com
    ○ remplacer example.com par votre nom de domaine

```

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.

Création d'un Site Vhost

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

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

1. Aller dans "Sites"

- a. Aller dans le menu "Subdomain(vhost)" pour définir un sous-domaine
 - i. Cliquez sur "Add Subdomain" pour un nouveau sous domaine
 - ii. Saisissez les informations:
 - Hostname: ← saisir mail
 - Domain: ← mettre example.com
 - web folder: ← saisir mail
 - Auto-subdomain: ← sélectionner www ou * si l'on veut un certificat let's encrypt wildcard
 - SSL: ← yes
 - Let's Encrypt: ← yes
 - Php: ← Sélectionnez 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 généré
 - Repeat Password: ← Ressaissez 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 (locaux, d'autres machines ou de container docker) de saisir dans la zone Apache Directives:
 - Pour un site en HTTP (attention dans ce cas, ce site doit être local ou dans un container pour des raisons de sécurité):

```

<Proxy *>
    Order deny,allow
    Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

# yacht httpserver
#

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPass / http://localhost[:port_number_if_any]/[path_if_any]
ProxyPassReverse / http://localhost[:port_number_if_any]/[path_if_any]

RedirectMatch ^/$ https://sub.example.com
    ○ remplacer example.com par votre nom de domaine

• Pour un site en HTTPS :

<Proxy *>
    Order deny,allow
    Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

# redirect from server
#

SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
SSLProxyEngine On # Comment this out if no https required
ProxyPreserveHost On

```

```

ProxyPass /
  https://localhost[:port_number_if_any]/[path_if_any]
  ProxyPassReverse /
    https://localhost[:port_number_if_any]/[path_if_any]

  RedirectMatch ^/$ https://sub.example.com
    ○ remplacer example.com par votre nom de domaine

```

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.

Associer des certificats reconnus à vos outils

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

1. Vous devez avoir créé au préalable un site pour les domaines example.com et mail.example.com
2. [Loguez vous comme root sur le serveur](#)
3. Liez le certificat d'ISPconfig avec celui du domaine créé.

- 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 /var/www/clients/<clientx>/<webx>/ssl/<example.com>-le.crt
ispserver.crt
ln -s /var/www/clients/<clientx>/<webx>/ssl/<example.com>-le.key
ispserver.key
cat ispserver.{key,crt} > ispserver.pem
chmod 600 ispserver.pem
systemctl restart apache2

```

- remplacer <example.com> par votre nom de domaine, <clientx> par votre numéro de client, <webx> par votre numéro de serveur web. L'information est facilement retrouvé en cliquant sur l'interface

d'ISPconfig dans Sites → `Website` → `<example.com>`. Le champ Document Root donne le début du chemin /var/www/clients/<clientx>/<webx>/

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

- Tapez :

```
cd /etc/postfix/
mv smtpd.cert smtpd.cert-$(date +"%y%m%d%H%M%S").bak
mv smtpd.key smtpd.key-$(date +"%y%m%d%H%M%S").bak
ln -s /var/www/clients/client0/web1/ssl/mail.example.com-le.crt
smtpd.cert
ln -s /var/www/clients/client0/web1/ssl/mail.example.com-le.key
smtpd.key
service postfix restart
service dovecot restart
■ remplacer <example.com> par votre nom de domaine
```

5. Liez le certificat pour Pureftd

- Tapez :

```
cd /etc/ssl/private/
mv pure-ftpd.pem pure-ftpd.pem-$(date +"%y%m%d%H%M%S").bak
ln -s /usr/local/ispconfig/interface/ssl/ispserver.pem pure-
ftpd.pem
ln -s /usr/local/ispconfig/interface/ssl/dhparam4096.pem pure-
ftpd-dhparams.pem
chmod 600 pure-ftpd.pem
service pure-ftpd-mysql restart
```

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

1. Installez la cron. Tapez :

```
crontab -e
```

2. Ajoutez la ligne suivante:

```
00 02 1 * * /usr/local/bin/certif_update.sh
```

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

```
/usr/local/bin/certif_update.sh
```

et coller dans le fichier le code suivant:

```

#!/bin/bash

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
cd /etc/postfix
cat smtpd.{key,cert} > smtpd.pem
chmod 600 smtpd.pem
service pure-ftpd-mysql restart
service monit restart
service postfix restart
service dovecot restart
service apache2 restart

```

4. Sauvez et quittez. Tapez ensuite:

```
chmod +x /usr/local/bin/certif_update.sh
```

Surveillance du serveur avec Munin et Monit

Note préliminaire

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

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

Installation et configuration de Munin

Suivez les étapes ci-après:

1. Installer le paquet Munin:

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

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

```
cd /etc/munin/plugins
ln -s /usr/share/munin/plugins/mysql_ mysql_
```

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

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

```
mysql -p
```

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

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

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

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

6. Décommentez les lignes débutant par: dbdir, htmldir, logdir, rundir, and tmpldir. Les valeurs par défaut sont correctes.

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

8. Un fois les commentaires enlevés et la ligne modifiée, le fichier de configuration doit ressembler à celui-ci:

```
# Example configuration file for Munin, generated by 'make build'
# The next three variables specifies where the location of the RRD
# databases, the HTML output, logs and the lock/pid files. They all
# must be writable by the user running munin-cron. They are all
# defaulted to the values you see here.
#
dbdir /var/lib/munin
htmldir /var/cache/munin/www
logdir /var/log/munin
rundir /var/run/munin
```

```

# Where to look for the HTML templates
#
tmpldir /etc/munin/templates
# Where to look for the static www files
#
#staticdir /etc/munin/static
# temporary cgi files are here. note that it has to be writable by
# the cgi user (usually nobody or httpd).
#
# cgitmpdir /var/lib/munin/cgi-tmp

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

```

- mettre à la place de `example.com` votre nom de domaine

9. Activez Munin dans Apache. Tapez:

```
a2enconf munin
```

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

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

11. Nous allons maintenant activer le module Munin dans Apache et définir une authentification basique.

12. Modifiez le fichier pour qu'il ressemble à celui ci-dessous:

```

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

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

```

```

</Directory>

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

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

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

```

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

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

14. Tapez votre mot de passe généré

15. Redémarrez apache. Tapez:

```
service apache2 restart
```

16. Vérifiez bien que IPV6 est activé. Si ce n'est pas le cas, le redémarrage de Munin peut survenir.

17. Redémarrez Munin. Tapez:

```
service munin-node restart
```

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

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 plugin est activé. La colonne `Suggestions` indique que le serveur fait fonctionner un service qui peut être monitoré par ce module. Il faut créer un lien symbolique du module de `/usr/share/munin/plugins` dans `/etc/munin/plugins` pour l'activer.

3. Par exemple pour activer les modules apache_*:

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

4. Une autre manière simple de configurer munin est de taper:

```
cd /etc/munin/plugins
munin-node-configure --shell --families=contrib,auto | sh -x
```

5. Redémarrez ensuite le service Munin. Tapez:

```
service munin-node restart
```

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 configurations sur <http://mmonit.com/monit/documentation/>.

3. Changez la configuration de Monit. Tapez:

```
vi /etc/monit/conf.d/monitrc.local
```

4. Ajoutez dans le fichier cette configuration :

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


- remplacez my_password par votre mot de passe généré
- remplacer example.com par votre domaine et nom@example.com par votre email

```

5. Activez les modules standards :

```
cd /etc/monit/conf-enabled
```

6. Créez ensuite un fichier pour Mariadb. Tapez:

```
vi /etc/monit/conf-enabled/mariadb
```

7. Ajoutez dans le fichier cette configuration :

```
check process mysqld with pidfile /var/run/mysqld/mysqld.pid
group database
group mysql
start program = "/etc/init.d/mariadb start"
stop program = "/etc/init.d/mariadb stop"
if failed host localhost port 3306 protocol mysql with timeout 15
seconds for 3 times within 4 cycles then restart
if failed unixsocket /var/run/mysqld/mysqld.sock protocol mysql
for 3 times within 4 cycles then restart
if 5 restarts with 5 cycles then timeout
depend mysql_bin
depend mysql_rc

check file mysql_bin with path /usr/sbin/mysqld
group mysql
include /etc/monit/templates/rootbin
```

```
check file mysql_rc with path /etc/init.d/mariadb
group mysql
include /etc/monit/templates/rootbin
```

8. Créez ensuite un fichier pour Pureftpd. Tapez:

```
vi /etc/monit/conf-enabled/pureftpd
```

9. Ajoutez dans le fichier cette configuration :

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

10. Créez ensuite un fichier pour named. Tapez:

```
vi /etc/monit/conf-enabled/named
```

11. Ajoutez dans le fichier cette configuration :

```
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
```

12. Créez ensuite un fichier pour sshd. Tapez:

```
vi /etc/monit/conf-enabled/sshd
```

13. Ajoutez dans le fichier cette configuration :

```
check process sshd with pidfile /var/run/sshd.pid
start program = "/etc/init.d/ssh start"
stop program = "/etc/init.d/ssh stop"
if failed host localhost port 22 with proto ssh then restart
if 5 restarts within 5 cycles then timeout
```

14. Créez ensuite un fichier pour apache. Tapez:

```
vi /etc/monit/conf-enabled/apache2
```

15. Ajoutez dans le fichier cette configuration :

```
check process apache with pidfile /var/run/apache2/apache2.pid
start program = "/etc/init.d/apache2 start"
stop program = "/etc/init.d/apache2 stop"
```

```

    if 4 restarts within 20 cycles then timeout
        if failed host localhost port 80 with protocol http and request
        "/server-status" with timeout 25 seconds for 4 times within 5 cycles
        then restart

```

16. Créez ensuite un fichier pour memcached. Tapez:

```
vi /etc/monit/conf-enabled/memcached
```

17. Ajoutez dans le fichier cette configuration :

```

check process memcached with pidfile
/var/run/memcached/memcached.pid
    start program = "/etc/init.d/memcached start"
    stop program = "/etc/init.d/memcached stop"
    if failed host 127.0.0.1 port 11211 and protocol memcache then
        restart
    if cpu > 60% for 2 cycles then alert
    if cpu > 98% for 5 cycles then restart
    if 5 restarts within 20 cycles then timeout

```

18. Créez ensuite un fichier pour ntpd. Tapez:

```
vi /etc/monit/conf-enabled/ntp
```

19. Ajoutez dans le fichier cette configuration :

```

check process ntpd with pidfile /var/run/ntp.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

```

20. Créez ensuite un fichier pour dovecot. Tapez:

```
vi /etc/monit/conf-enabled/dovecot
```

21. Ajoutez dans le fichier cette configuration :

```

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

```

22. Créez ensuite un fichier pour postfix. Tapez:

```
vi /etc/monit/conf-enabled/postfix
```

23. Ajoutez dans le fichier cette configuration :

```
check process postfix with pidfile /var/spool/postfix/pid/master.pid
  start program = "/etc/init.d/postfix start"
  stop  program = "/etc/init.d/postfix stop"
  if failed host localhost port 25 with protocol smtp for 2 times
within 3 cycles then restart
  if 5 restarts with 5 cycles then timeout
```

24. Créez ensuite un fichier pour redis. Tapez:

```
vi /etc/monit/conf-enabled/redis
```

25. Ajoutez dans le fichier cette configuration :

```
check process redis with pidfile /var/run/redis/redis-server.pid
  start program = "/usr/sbin/service redis-server start" with timeout
60 seconds
  stop program  = "/usr/sbin/service redis-server stop" with timeout
60 seconds
  if failed host 127.0.0.1 port 6379 then restart
  if totalmem > 500 Mb then alert
  if cpu > 60% for 2 cycles then alert
  if cpu > 98% for 5 cycles then restart
  if 2 restarts within 2 cycles then alert
```

26. 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>.

27. Redémarrez apache. Tapez:

```
service apache2 restart
```

28. Dans la configuration pour apache, la configuration indique que monit doit aller 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
```

29. Tapez :

```
service monit restart
```

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

```
monit status
```

31. Debloquez le port 2812 sur votre firewall

32. Maintenant naviguez sur le site <https://example.com:2812/>

33. Rentrez le login `admin` et votre mot de passe `my_password`. Monit affiche alors les informations de monitoring du serveur.

Configuration de la messagerie

Configuration de l'antispam rspamd

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

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur

2. Installez les paquets debian. tapez:

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

3. Loguez vous dans ISPConfig

4. Activer Rspamd dans ISPConfig

a. Allez dans la rubrique `System` → menu `Server Config` → Sélectionnez votre serveur → Onglet `Mail`

b. Dans le champ `Content Filter`, sélectionnez `Rspamd`

c. Dans le champ `Rspamd Password`, tapez votre mot de passe

d. Cliquez sur `Save`

e. Revenez dans la rubrique `System` → menu `Server Config` → Sélectionnez votre serveur → Onglet `Mail`

f. Vous pouvez voir le mot de passe de connexion au serveur web Rspamd.

5. Activez l'apprentissage automatique. Tapez:

```
vi /etc/rspamd/local.d/classifier-bayes.conf
```

6. insérez le texte suivant:

```

backend = "redis";
servers = "127.0.0.1";
expire = 8640000;
autolearn {
    spam_threshold = 6.0; # When to learn spam (score >= threshold and
    action is reject)
    junk_threshold = 4.0; # When to learn spam (score >= threshold and
    action is rewrite subject or add header, and has two or more positive
    results)
    ham_threshold = -0.5; # When to learn ham (score <= threshold and
    action is no action, and score is negative or has three or more
    negative results)
    check_balance = true; # Check spam and ham balance
    min_balance = 0.9; # Keep diff for spam/ham learns for at least
    this value
}

per_user = false;
per_language = true;

```

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

```

echo 'write_servers = "127.0.0.1";' > /etc/rspamd/local.d/redis.conf
echo 'read_servers = "127.0.0.1";' >> /etc/rspamd/local.d/redis.conf

```

8. Fixer des métriques assez élevées pour analyser les spams

```

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

```

9. 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

```

- à basculer à true si vous avez des utilisateurs de votre serveur de mail souhaitant une compatibilité RGPD.

10. Assignez un calcul automatique de réputation aux URLs

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

11. Vérifiez si l'émetteur est bien un serveur de mail. Tapez :

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

12. Insérez le texte suivant:

```
enabled = true;  
key_prefix = "rmx";  
symbol_bad_mx = "MX_INVALID";  
symbol_no_mx = "MX_MISSING";  
symbol_good_mx = "MX_GOOD";  
expire = 86400;  
expire_novalid = 7200;  
greylist_invalid = false;
```

13. Activez l'analyse par réseau de neurone. Tapez:

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

14. Insérez le texte suivant:

```
enabled = true;  
  
rules {  
    "LONG" {  
        train {  
            max_trains = 5000;  
            max_usages = 200;  
            max_iterations = 25;  
            learning_rate = 0.01,  
            spam_score = 10;  
            ham_score = -2;  
        }  
        symbol_spam = "NEURAL_SPAM_LONG";  
        symbol_ham = "NEURAL_HAM_LONG";  
        ann_expire = 100d;  
    }  
    "SHORT" {  
        train {  
            max_trains = 100;  
            max_usages = 2;  
            max_iterations = 25;  
            learning_rate = 0.01,  
            spam_score = 10;
```

```

        ham_score = -2;
    }
symbol_spam = "NEURAL_SPAM_SHORT";
symbol_ham = "NEURAL_HAM_SHORT";
ann_expire = 1d;
}
}

```

15. Créez les groupes associés. Tapez:

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

16. Insérez le texte suivant:

```

symbols = {
    "NEURAL_SPAM_LONG" {
        weight = 1.0; # sample weight
        description = "Neural network spam (long)";
    }
    "NEURAL_HAM_LONG" {
        weight = -2.0; # sample weight
        description = "Neural network ham (long)";
    }
    "NEURAL_SPAM_SHORT" {
        weight = 0.5; # sample weight
        description = "Neural network spam (short)";
    }
    "NEURAL_HAM_SHORT" {
        weight = -1.0; # sample weight
        description = "Neural network ham (short)";
    }
}

```

17. Enrichissez les headers des mails spams. Tapez:

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

18. Insérez le texte suivant:

```

# local.d/milter_headers.conf:

# Options

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

```

```

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

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

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

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

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

# this is where we may configure our selected routines
routines {
    remove-headers {
        headers {
            "X-Spam" = 0;
            "X-Spamd-Bar" = 0;
            "X-Spam-Level" = 0;
            "X-Spam-Status" = 0;
            "X-Spam-Flag" = 0;
        }
    }
    # other routines...
}

custom {
    # user-defined routines: more on these later
}

```

19. Créez une configuration pour le protocole arc. Tapez:

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

20. Insérez le texte suivant:

```
sign_authenticated = false;
```

```

sign_inbound = true;
sign_local = false;
use_domain = "header";
try_fallback = false;
use_esld = false;
path_map = "/etc/rspamd/local.d/dkim_domains.map";
selector_map = "/etc/rspamd/local.d/dkim_selectors.map";

```

21. Créez un mot de passe. Tapez:

```
rspamadm pw
```

22. Entrez votre mot de passe généré. Une hash phrase est générée.

23. Copiez la.

24. Remplacez celle déjà présente dans /etc/rspamd/local.d/worker-controller.inc

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

25. Remplacez le texte entre guillemets sur la ligne password = "\$2\$g95yw.....dq3c5byy"; par le texte copié.

26. Si vous avez installé l'antivirus Clamav, Créez un fichier pour la configuration:

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

27. Insérez le texte suivant :

```

clamav {
    # If set force this action if any virus is found (default unset:
    no action is forced)
    #action = "reject";
    # Scan mime_parts separately - otherwise the complete mail will
    be transferred to AV Scanner
    scan_mime_parts = true;
    # Scanning Text is suitable for some av scanner databases (e.g.
    Sanesecurity)
    scan_text_mime = true;
    scan_image_mime = true;
    # If `max_size` is set, messages > n bytes in size are not
    scanned
    #max_size = 20000000;
    # symbol to add (add it to metric if you want non-zero weight)
    symbol = "CLAM_VIRUS";
    # type of scanner: "clamav", "fprot", "sophos" or "savapi"
}

```

```

type = "clamav";
# For "savapi" you must also specify the following variable
#product_id = 12345;
# You can enable logging for clean messages
#log_clean = true;
# servers to query (if port is unspecified, scanner-specific
default is used)
# can be specified multiple times to pool servers
# can be set to a path to a unix socket
# Enable this in local.d/antivirus.conf
#servers = "127.0.0.1:3310";
servers = "/var/run/clamav/clamd.ctl";
# if `patterns` is specified virus name will be matched against
provided regexes and the related
# symbol will be yielded if a match is found. If no match is
found, default symbol is yielded.
patterns {
    # symbol_name = "pattern";
    JUST_EICAR = "^Eicar-Test-Signature$";
}
patterns_fail {
    # symbol_name = "pattern";
    CLAM_PROTOCOL_ERROR = '^unhandled response';
}
# `whitelist` points to a map of IP addresses. Mail from these
addresses is not scanned.
whitelist = "/etc/rspamd/antivirus.wl";
}

```

28. Définissez des groupes:

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

29. Insérez le texte suivant :

```

group "antivirus" {
    .include(try=true;      priority=1;      duplicate=merge)
"$LOCAL_CONFDIR/local.d/antivirus_group.conf"
        .include(try=true;      priority=10)
"$LOCAL_CONFDIR/override.d/antivirus_group.conf"
}

```

30. Définissez les détections de virus :

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

31. Insérez le texte suivant :

```
subject = "****SPAM*** %s";
symbols = {
    "CLAM_VIRUS" {
        weight = 50;
        description = "Clamav has found a virus.";
    }
    "JUST_EICAR" {
        weight = 50;
        description = "Clamav has found a virus.";
    }
    "R_DUMMY" {
        weight = 0.0;
        description = "Dummy symbol";
    }
}
```

32. Ajuster les permissions. Tapez:

```
chmod 755 /etc/rspamd/local.d/maps.d
```

33. Redémarrez Rspamd

```
systemctl restart rspamd
```

34. Rendre le site rspamd accessible dans un host

35. Activez le module proxy dans apache

```
a2enmod proxy
systemctl restart apache2
```

36. 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

37. 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. Sélectionnez `None` dans Auto-subdomain
- d. Activer let's encrypt SSL
- e. Activer PHP-FPM pour PHP
- f. Dans l'onglet Redirect Cochez la case `Rewrite HTTP to HTTPS`
- g. Laisser le reste par défaut.
- h. Dans l'onglet Options:

- i. Dans la boite Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

# redirect from server
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
SSLProxyEngine On # Comment this out if no https required
ProxyPreserveHost On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off

ProxyPass /rspamd https://example.com:8081/rspamd/
ProxyPass / https://example.com:8081/rspamd/
ProxyPassReverse / https://example.com:8081/rspamd/

RedirectMatch ^/$ https://rspamd.example.com
```

- remplacer `example.com` par votre nom de domaine

38.en pointant sur le site `rspamd.example.com`, et en utilisant le mot de passe saisi plus haut vous pouvez accéder aux fonctions de l'outil.

39.Activer l'apprentissage par déplacement

- a. Couplé avec Dovecot, Rspamd nous propose de pouvoir apprendre également en fonction des actions des utilisateurs. Si un mail est déplacé vers le répertoire Junk, il sera appris comme tel et au contraire, s'il est sorti du répertoire Junk vers autre chose que la corbeille, il sera appris comme Ham.
- b. Editez le fichier Dovecot.conf (remarques ISPConfig n'utilise pas aujourd'hui le contenu du répertoire conf.d). Tapez:

```
vi /etc/dovecot/conf.d/99-ispconfig-custom-config.conf
```

- c. Ajoutez le texte suivant:

```
plugin {
    sieve_plugins = sieve_imapsieve sieve_extprograms

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

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

    sieve_pipe_bin_dir = /etc/dovecot/sieve

    sieve_global_extensions = +vnd.dovecot.pipe
}

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

- d. Redémarrez dovecot. Tapez:

```
service dovecot restart
```

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

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

- f. Insérez le texte suivant:

```
require ["vnd.dovecot.pipe", "copy", "imapsieve", "environment",  
"variables"];  
  
if environment :matches "imap.mailbox" "*" {  
set "mailbox" "${1}";  
}  
  
if string "${mailbox}" "Trash" {  
stop;  
}  
  
if environment :matches "imap.email" "*" {  
set "email" "${1}";  
}  
  
pipe :copy "train-ham.sh" [ "${email}" ];
```

- g. Editez report-spam.sieve. Tapez:

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

- h. Insérez le texte suivant:

```
require ["vnd.dovecot.pipe", "copy", "imapsieve", "environment",  
"variables"];  
  
if environment :matches "imap.email" "*" {  
set "email" "${1}";  
}  
  
pipe :copy "train-spam.sh" [ "${email}" ];
```

- i. Créez les scripts et rétablissez les droits et permissions. Compilez les règles.

Tapez:

```
echo "exec /usr/bin/rspamd learn_ham" > /etc/dovecot/sieve/train-  
ham.sh
```

```

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

```

- j. On en profite pour ajouter un petit script qui informe l'utilisateur de l'atteinte de son quota. On édite le fichier 90-quota.conf :

```
vi /etc/dovecot/conf.d/90-quota.conf
```

- k. Insérez le texte suivant:

```

plugin {
    quota = maildir:User quota
    quota_warning = storage=90%% quota-warning 90 %u
}

service quota-warning {
    executable = script /usr/local/bin/quota-warning.sh
    user = vmail
    unix_listener quota-warning {
        user = vmail
    }
}

```

- l. Créer le fichier de script :

```
vi /usr/local/bin/quota-warning.sh
```

- m. Insérez le texte suivant:

```

#!/usr/bin/env bash

PERCENT=${1}
USER=${2}

cat      <<      EOF      |      /usr/sbin/sendmail      $USER      -O
"plugin/quota=maildir:User quota:noenforcing"
From: postmaster@example.com

Votre Boite est plein à plus de ${PERCENT}. Faut faire du ménage
mon ami !
EOF

```

- remplacer example.com par votre nom de domaine.

n. Changez les permissions :

```
chmod +x /usr/local/bin/quota-warning.sh  
chown vmail /usr/local/bin/quota-warning.sh
```

o. Redémarrez dovecot. Tapez:

```
service dovecot restart
```

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

40. Enfin, vous pouvez désactiver amavisd si vous le souhaitez et s'il est installé sur votre système. tapez:

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

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 Save
6. Attendez quelques secondes la fin de configuration puis rouvrez la configuration de votre serveur de mail et
7. Cliquez sur DomainKeys Identified Mail (DKIM)
8. Cliquez sur enable DKIM
9. Cliquez sur Generate DKIM Private-key

- 10.Une fois cela fait, retourner dans la gestion des `Records de domaine` et activer le type DMARC
- 11.Garder le paramétrage par défaut et sauvegardez.
- 12.Faites de même pour les enregistrements SPF mais sélectionnez le mécanisme softfail.
- 13.Votre serveur est créé et protégé Contre les spams (entrants et sortants).

Finaliser la sécurisation de votre serveur de mail

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

1. Loguez vous comme root sur le serveur

2. editez le fichier main.cf

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

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

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

- Remplacer `example.com` par votre nom de domaine.

4. Redémarrez Postfix. Tapez:

```
service postfix restart
```

5. Vous pouvez ajouter une signature DKIM. Si vous utilisez ISPConfig, cette opération est effectuée automatiquement et cette étape est à sauter :

- DKIM est une méthode d'authentification du courrier électronique conçue pour détecter l'usurpation d'adresse électronique. Elle permet au serveur de réception de vérifier l'origine d'un courrier électronique en y apposant une signature numérique. La vérification de la signature est effectuée à l'aide de la clé publique du signataire publiée dans le DNS. Elle peut être utilisée pour détecter les courriels frauduleux.
- Créez un nouveau répertoire pour stocker la clé DKIM et générez une nouvelle paire de clés DKIM à l'aide de l'utilitaire `rspamadm`. Dans l'exemple suivant, nous utilisons `mail` comme sélecteur DKIM. Il générera une paire de

clés qui pourra être utilisée pour tous les domaines gérés par le serveur de messagerie:

```
mkdir /var/lib/rspamd/dkim/
rspamadm dkim_keygen -d example.com -s default -k toto -b 2048
/var/lib/rspamd/dkim/example.com.dkim.key >
/var/lib/rspamd/dkim/example.com.dkim.key.pub
```

- remplacez `example.com` par votre nom de domaine.
- Vous trouverez deux fichiers dans le répertoire :
 - `mail.key` - Le fichier de clé privée
 - `mail.pub` - Le fichier de clé publique
- Editez le fichier `dkim_domains.map` et ajoutez:


```
example.com /var/lib/rspamd/dkim/example.com.dkim.key
```

 - remplacez `example.com` par votre nom de domaine.
- Editez le fichier `dkim_selectors.map` et ajoutez:


```
example.com default
```

 - remplacez `example.com` par votre nom de domaine.
- Ajoutez une entrée DNS avec le texte suivant:


```
default._domainkey.example.com. 3600 IN TXT "v=DKIM1; t=s;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAtBdWvMULDmlAzZWTMhyh
eOmcewA4DFx+nMHI+3baOuJWt3/v7CdrX+egisWD5jwRzi/wN18kWR4kG/
5rQKpIQLjurQrzqP09i1Bub90+VZWw0ldCAVNjKtkoFfgEErePMnKX/
9Qjje+rqrH9oHSC+RK0z2Dvj3+WQIDAQAB"
```

 - remplacez `example.com` par votre nom de domaine et remplacez le contenu derrière `p=` par le contenu derrière `p=` présent dans le fichier `/var/lib/rspamd/dkim/exaple.com.dkim.key.pub`

- Ajouter si ce n'est pas le cas une entrée DNS pour le SPF:

```
v=spf1 mx a a:mail.example.com a:mail.other.example.com
include:mail.toto.com -all
```

- remplacez `example.com` par votre nom de domaine. Vous pouvez rajouter autant d'entrée `a:` ou `include:` que nécessaires si vous avez

des serveur de mail secondaires qui peuvent relayer des mails pour ce domaine. La valeur -all interdira tout autre domaine ou adresse IP à envoyer des mails

6. Vous pouvez le tester en allant sur le site [MxToolbox](#).

- Entrez le nom de host de votre serveur de mail: mail.example.com .
- cliquez sur test Email Server
- Tout doit être correct sauf éventuellement le reverse DNS qui doit être configuré pour pointer vers mail.example.com .

7. Testez votre email sur le site [Phishing Scoreboard](#)

- Entrez votre adresse mail: admin@example.com
- Entrez votre nom de domaine: example.com
- Entrez votre clé dkim: default

8. Enfin, vous pouvez tester votre statut de spammer potentiel en envoyant allant sur le site [Newsletter Spam test](#)

- suivez les instructions (envoi d'un email à l'adresse donnée)
- le site vous donnera des informations intéressantes sur la configuration du serveur et des informations complémentaires liées au contenu du mail. Pour ces dernières ne pas en tenir compte.

Surveillance du statut de Spammer

Il est nécessaire aujourd'hui de surveiller le statut de votre serveur de mail et de vérifier notamment si votre configuration SPF, DKIM et DMARC est correctement comprise par les serveurs de mails les plus connus comme Gmail, Yahoo, Hotmail ...

Pour cela un peu de configuration est nécessaire.

En premier, il faut créer un compte:

1. Allez sur le site [Dmarcian](#)

2. Cliquez sur Sign up Free
3. Choisissez votre région, Europe par exemple.
4. Enregistrez votre compte (mail, mot de passe) et votre nom de domaine example.com
5. notez bien l'adresse email qui va vous être donnée par dmrcian de la forme xyzabcd@ag.dmarcian.eu pour la réception de messages de type abuse et de la forme xyzabcd@fr.dmarcian.eu pour des forensic. Notez bien ces deux adresses.

Ensuite, vous devez modifier votre configuration DMARC:

1. Allez dans DNS de votre serveur de domaine principal
2. Sélectionnez le menu Zones puis le domaine example.com
3. Choisissez l'onglet Records et éditez l'entrée TXT nommée _dmarc
4. modifiez le champ Text avec :
v=DMARC1;p=reject;sp=quarantine;pct=100;ruamailto:abuse@example.com;
rufmailto:forensic@example.com. On remplacera bien le domaine
example.com par son propre domaine.
5. Allez ensuite dans Email
6. Allez dans le menu Email Forward
7. cliquez sur Add new Email Forward
8. Saisissez dans Email la valeur abuse
9. Saisissez dans Destination Email sur 2 lignes l'adresse de votre mail de réception interne et l'adresse mail qui vous a été fournie par dmrcian.com pour l'adresse abuse (de la forme xyzabcd@ag.dmarcian.eu)
10. Cliquez sur Save
11. cliquez sur Add new Email Forward
12. Saisissez dans Email la valeur forensic

13.Saisissez dans Destination Email sur 2 lignes l'adresse de votre mail de réception interne et l'adresse mail qui vous a été fournie par dmarcian.com pour l'adresse forensic (de la forme xyzabcd@fr.dmarcian.eu)

14.Cliquez sur Save

15.le site dmarcian.com va commencer à recevoir tous les comptes rendus de mails refusés par les destinataires de messagerie et élaborer des statistiques ainsi que des comptes rendus que vous pourrez consulter sur votre compte.

Il est intéressant de vérifier votre statut de spammer en vérifiant les différentes blacklist qui existent.

Pour cela allez sur le site [Email Blacklist Check](#) entrez votre nom de domaine example.com et cliquez sur le bouton Blacklist Check.

Tous les sites doivent indiquer que votre domaine n'est pas blacklisted.

Création de l'autoconfig pour Thunderbird et Android

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

Appliquez la procédure suivante:

1. Créez 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. Mettre dans Auto-SubDomain la valeur None
 - d. Sélectionnez None dans Auto-subdomain
 - e. Activer let's encrypt SSL
 - f. Activer PHP-FPM pour PHP
 - g. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS
 - h. Laisser le reste par défaut.

i. Dans l'onglet Options:

j. Dans la boîte Apache Directives: saisir le texte suivant:

```
<FilesMatch ".+\.xml$">
    SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost"
</FilesMatch>

<FilesMatch ".+\.json$">
    SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost"
</FilesMatch>

AddHandler application/x-httpd-php .php .xml .json

<IfModule mod_speling.c>
    CheckCaseOnly on
    CheckSpelling on
</IfModule>
```

- Mettez bien ici la version de PHP que vous avez choisi. Dans l'exemple c'est la 8.2

k. Sauver.

2. Loguez vous comme root sur le serveur

3. Editez le fichier le fichier /etc/php/8.2/fpm/pool.d/www.conf (mettez votre version choisie à la place de 8.2).

4. Dans le fichier, recherchez security.limit_extension et ajoutez:

```
security.limit_extensions = .php .php3 .php4 .php5 .php7 .xml .json
```

1. 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:

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

- remplacer web1:client0 par les permissions du répertoire /var/www/autoconfig.example.com
 - remplacez example.com par votre nom de domaine
2. A l'intérieur de ce répertoire, Editez un fichier config-v1.1.xml. Tapez:
- ```
vi autoconfig/mail/config-v1.1.xml
```
3. Y coller:

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

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

```
<hostname>mail.example.com</hostname>
<port>587</port>
<socketType>STARTTLS</socketType>
<authentication>password-cleartext</authentication>
<username>%EMAILADDRESS%</username>
</outgoingServer>
</emailProvider>
</clientConfig>
```

- mettre à la place de `example.com` votre nom de domaine
- mettre ici votre libellé long pour votre nom de messagerie
- mettre ici un libellé court pour votre nom de messagerie

#### 4. Donner la permission en lecture seule et affecter les groupes d'appartenance.

Tapez:

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

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

### ***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`. Cette méthode ne fonctionne pas avec les versions récentes de Outlook.

Appliquez la procédure suivante:

1. Créez un [sub-domain \(vhost\)](#) dans le configurateur de sites.
  - a. Lui donner le nom `autodiscover`.
  - b. Le faire pointer vers le web folder `autoconfig`.
  - c. Mettre dans `Auto-SubDomain` la valeur `None`
  - d. Sélectionnez `None` dans `Auto-subdomain`
  - e. Activer `let's encrypt SSL`

f. Activer PHP-FPM pour PHP

g. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS

h. Laisser le reste par défaut.

i. Dans l'onglet Options:

j. Dans la boîte Apache Directives: saisir le texte suivant:

```
<FilesMatch ".+\.xml$">
 SetHandler
 "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost"
</FilesMatch>

<FilesMatch ".+\.json$">
 SetHandler
 "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost"
</FilesMatch>

AddHandler application/x-httpd-php .php .xml .json

<IfModule mod_speling.c>
 CheckCaseOnly on
 CheckSpelling on
</IfModule>
```

- Mettez bien ici la version de PHP que vous avez choisi. Dans l'exemple c'est la 8.2

k. Sauver.

## 2. Loguez vous comme root sur le serveur

3. Editez le fichier le fichier /etc/php/8.2/fpm/pool.d/www.conf (mettez votre version choisie à la place de 8.2).

4. Dans le fichier, recherchez security.limit\_extension et ajoutez:

```
security.limit_extensions = .php .php3 .php4 .php5 .php7 .xml .json
```

1. 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:

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

- remplacer web1:client0 par les permissions du répertoire /var/www/autoconfig.example.com
- remplacez example.com par votre nom de domaine

```

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

```
vi autoconfig/Autodiscover/Autodiscover.xml
```

3. Y coller:

```
<?php
$postData = file_get_contents('php://input'); //Autodiscover requests
are HTTP posts with XML content
$xml = simplexml_load_string($postData);
$user = $xml->Request->EMailAddress; //copy the email address from
the request into a variable

//set Content-Type
header("Content-Type: application/xml");
?>
<?php echo '<?xml version="1.0" encoding="utf-8" ?>'; ?>
<Autodiscover
xmlns="http://schemas.microsoft.com/exchange/autodiscover/responseschema/2006">
 <ResponseAccountAccountTypeAccountTypeActionActionProtocolTypeTypeServerServerPortPortLoginNameLoginNameDomainRequiredDomainRequiredSPASPASSLSSL

```

```

<AuthRequired>on</AuthRequired>
<DomainRequired>on</DomainRequired>
</Protocol>
<Protocol>
 <Type>IMAP</Type>
 <Server>mail.example.com</Server>
 <Port>993</Port>
 <DomainRequired>on</DomainRequired>
 <LoginName><?php echo $user; ?></LoginName>
 <SPA>off</SPA>
 <SSL>on</SSL>
 <Encryption>Auto</Encryption>
 <AuthRequired>on</AuthRequired>
</Protocol>
<Protocol>
 <Type>SMTP</Type>
 <Server>mail.example.com</Server>
 <Port>465</Port>
 <DomainRequired>on</DomainRequired>
 <LoginName><?php echo $user; ?></LoginName>
 <SPA>off</SPA>
 <Encryption>Auto</Encryption>
 <!-- if your server requires encryption other than
SSL -->
 <AuthRequired>on</AuthRequired>
 <UsePOPAuth>on</UsePOPAuth>
 <SMTPLast>off</SMTPLast>
</Protocol>
</Account>
</Response>
</Autodiscover>

```

- mettre à la place de `example.com` votre nom de domaine

#### 4. Changez les permissions comme pour le répertoire

```

chmod 644 autoconfig/Autodiscover/Autodiscover.xml
chown web1:client0 autoconfig/Autodiscover/Autodiscover.xml

```

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

5. Pointer votre navigateur sur le site  
[https://autodiscover.example.com/Autodiscover/Autodiscover.xml.](https://autodiscover.example.com/Autodiscover/Autodiscover.xml)

6. Le contenu du fichier xml doit s'afficher

7. Dans le répertoire /var/www/autoconfig.<example.com>/autoconfig/, Editez un fichier autodiscover.json. Tapez:

```
vi autoconfig/Autodiscover/autodiscover.json
```

8. Y coller:

```
<?php
header('Content-type: application/json');
echo
'{"Protocol":"AutodiscoverV1","Url":"https://autodiscover.example.com
/Autodiscover/Autodiscover.xml"}';
?>
```

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

9. Changez les permissions comme pour le répertoire

```
chmod 644 autoconfig/Autodiscover/autodiscover.json
chown web1:client0 autoconfig/Autodiscover/autodiscover.json
cp -pr autoconfig/Autodiscover autoconfig/autodiscover
```

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

10. Pointer votre navigateur sur le site  
<https://autodiscover.example.com/autodiscover/autodiscover.json>

11. Le contenu du fichier json doit s'afficher

12. Vous pouvez faire aussi un test sur le [Testeur de connectivité Microsoft](#).

1. choisissez: Découverte automatique Outlook

2. cliquez sur suivant

3. 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.

4. Cliquez sur effectuer un test
5. Le résultat doit être: Test de connectivité réussi

## 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: ← saisir le <mail\_name> mail\_name@example.com
  - c. Password: ← Saisissez un mot de passe généré ou générez en un en cliquant sur le bouton
  - 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

### i Note

Notez que si vous créez une adresse mail nommée mail\_name@example.com, vous pouvez utiliser toutes les variantes (nommées tag) derrière le caractère "+". Ainsi mail\_name+nospam@example.com sera bien redirigé vers votre boite et

l'extension `+nospam` vous permettre de trier automatiquement les mails que vous ne voulez pas recevoir.

**i Note**

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

## **Configuration de votre client de messagerie.**

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

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

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

## 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. Sélectionnez None dans Auto-subdomain
  - d. Activer let's encrypt SSL
  - e. Activer PHP-FPM pour PHP
  - f. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS
  - g. Laisser le reste par défaut.
  - h. Dans l'onglet Options:
  - i. Dans la boite Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

redirect from server
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
SSLProxyEngine On # Comment this out if no https required
ProxyPreserveHost On
SSLProxyVerify none
SSLProxyCheckPeerCN off
```

```
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off

ProxyPass /webmail https://localhost:8080/webmail/
ProxyPass / https://localhost:8080/webmail/
ProxyPassReverse / https://localhost:8080/webmail/

RedirectMatch ^/$ https://mail.example.com
```

- remplacer `example.com` par votre nom de domaine

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

## **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.

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)

2. Téléchargez imapsync du repository. Tapez:

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

3. Installez les packages perl 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 libencode-imaputf7-perl
```

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

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

```
chmod 600 secretdst
```

- passwdsrc est à remplacer par le mot de passe du compte sur le serveur source
- passwddst est à remplacer par le mot de passe du compte sur le serveur destination

#### 5. Nous pouvons maintenant lancer la commande. Tapez:

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

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

```
rm secretsrc
rm secretdst
```

## Installation de Docker et des outils associés

Le logiciel Docker est une technologie de conteneurisation qui permet la création et l'utilisation de conteneurs Linux. En clair, Docker permet d'installer et de configurer rapidement toute une appli web complexe dans un environnement isolé et avec tout son écosystème de bibliothèques logicielles spécifiques.

Il est ainsi possible d'effectuer rapidement des installations, de suivre des mises à jours et d'isoler ces environnements du système principal.

## A propos des Raspberry Pi



### Warning

Les raspberry utilisent une architecture ARM, tous les conteneurs ne seront pas forcément compatibles "out of the box" ( Exemple pour MySQL). Sur le [Docker Hub](#), il faut choisir par un Raspberry Pi 4 ou 5 en Ubuntu une architecture de type ARM64 et pour un Raspberry Pi 3 en Raspbian une architecture de type ARM.

## Installation de Docker

L'installation de Docker est relativement simple.

Il faut suivre les étapes suivantes:

1. Loguez vous comme root sur le serveur

2. Désinstallez les éventuelles anciennes versions de docker. tapez:

```
apt remove --purge docker docker.io containerd runc docker-doc
docker-compose podman-docker
```

- docker-engine n'existe pas dans une distribution ubuntu. C'est à enlever.

3. Tapez:

```
Add Docker's official GPG key:
apt-get update
apt-get install ca-certificates curl
install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/debian/gpg -o
/etc/apt/keyrings/docker.asc
chmod a+r /etc/apt/keyrings/docker.asc
```

```
Add the repository to Apt sources:
echo \
 "deb [arch=$(dpkg --print-architecture)
signed-by=/etc/apt/keyrings/docker.asc]
https://download.docker.com/linux/debian \
$(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \
tee /etc/apt/sources.list.d/docker.list > /dev/null
```

4. Une fois installé avec succès, tapez:

```
apt update
```

5. Si vous obtenez une erreur c'est que vous avez ajouté un repository qui n'est pas supporté par Docker. Vérifiez les fichier `/etc/apt/sources.list`.

6. Une fois mis à jour avec succès, tapez:

```
apt-get install docker-ce docker-ce-cli containerd.io docker-buildx-
plugin docker-compose-plugin
```

7. vérifiez que votre installation de Docker est fonctionnelle. Tapez:

```
docker run hello-world
```

8. Cette commande exécute un conteneur simple. Si aucune erreur n'apparaît c'est que l'installation est réussie.

## ***Installation de docker swarm***

Docker contient nativement le mode Swarm afin de gérer un ensemble de Docker Engines. Cette installation est optionnelle puisque l'on peut faire fonctionner Docker sans cette Option.

Il y a deux types de machines: les **Managers** et les **Workers**.

Les managers : Ce sont les nodes gestionnaires de votre cluster. Ils distribuent les tâches aux nodes workers et ils effectuent également les fonctions d'orchestration et de gestion.

Les workers : Ils vont exécuter les tâches confiées par les managers. Un agent s'exécute sur chaque nœud et rend compte des tâches qui lui sont affectées. Il informe ainsi les nodes managers de l'état des tâches affectées.

Il faut suivre les étapes suivantes:

1. [Loguez vous comme root sur le serveur](#)

2. Tapez:

```
docker swarm init
```

3. Le résultat de la commande donne la commande `docker swarm join` à exécuter sur un "worker" pour lui faire rejoindre le "swarm". A noter que le "manager" que nous venons de créer est aussi un worker. De ce fait, un swarm peut être installé de façon standalone sur un VPS.

4. Vous pouvez maintenant vérifier l'état de votre cluster. Tapez:

```
docker node ls
```

## ***Choix des images docker***

Les images docker sont accessibles sur le [Docker Hub](#).

Mais voilà, c'est un peu la jungle. Un bon moyen de trouver des images à jour d'un point de vue sécurité et non compromises est de ne sélectionner que des images "Docker Certified" ou "Verified Publisher" ou "Official Images".

Du moins on est sûr que ces images ont été à minima vérifiées par les équipes Docker.

Pour mémoire: **Le nombre de chargement d'une image n'est pas un gage de qualité !**

Si vous n'utilisez pas une image du type mentionné ci dessus, l'accès facile au fichier Dockerfile est un gage de qualité et de transparence. En tout cas, il vous sera facilement possible de regarder comment l'image est construite et quels sont les packages dockers de base et si ces packages dockers de base sont récents et certifiés.

Pour les plateformes de type Raspberry, il faut bien vérifier que l'image docker que vous chargez est compatible de votre plateforme. Sur Docker Hub, vous devez allez sur l'onglet Tag de votre package et vérifier que le champ OS/ARCH contient bien votre plateforme.

Pour un Raspberry Pi 4 ou 5 ce doit être: `Linux/arm64`

Pour un Raspberry Pi 3 ce doit être: `Linux/arm`

Par exemple pour les docker de `Yacht` et de `Portainer` décrits ci après, on peut voir que les containers sont multiplateforme et conviennent très bien pour de l'Intel ou de l'ARM.

## ***Considérations de sécurité***

A propos de l'export des ports sous docker.

Par défaut lorsque vous lancez un container docker, l'option pour exporter un port de votre docker vers votre machine est `-p dst_port:src_port`. Si vous indiquez uniquement le port de destination comme par exemple dans `-p 80:8080` qui exporte le port 8080 de votre docker vers le port 80 de votre machine réelle, vous exporter vers le port 80 de l'adresse IP 0.0.0.0 ce qui en pratique indique que vous n'utilisez pas les règles du firewall; le port est exporté automatiquement sur toutes les interfaces.

De ce fait, vous exposez tous les ports interne de votre système docker à tout internet et le firewall ne bloque rien pour ces ports.

Il est donc indispensable pour une machine directement exposée sur internet d'indiquer l'adresse du loopback en indiquant systématiquement l'adresse IP soit `-p 127.0.0.1:80:8080`. Ainsi les règles du firewall sont appliquées et vous pourrez par votre configuration d'ISPconfig n'exposer que les ports et noms de domaines nécessaires.

#### ! Important

Dans tout ce qui suit nous omettrons d'utiliser cette adresse en 127.0.0.1 . Pensez bien donc à ajouter cette adresse systématiquement pour un serveur présent sur le web !

## ***Mise à jour automatique des images***

Vos images docker peuvent être mise à jour automatiquement si vous les avez installés à partir du docker hub ou de n'importe quel autre repository compatible.

Un outil automatise cette mise à jour c'est [watchtower](#).

Pour l'installer, rien de plus simple:

1. Tapez:

```
docker run -d --name watchtower -v /var/run/docker.sock:/var/run/docker.sock containrrr/watchtower --cleanup --interval 86400
```

2. l'option cleanup effectue le ménage des images inutiles et interval indique en secondes le temps à attendre entre deux vérifications (ici 24h)
3. si vous voulez vous connecter à un repository avec un login et un mot de passe, vous pouvez ajouter au lancement du docker les options suivantes:  
`-e REPO_USER=username -e REPO_PASS=password`
4. Si vous désirez ne mettre à jour que certains containers, vous pouvez passer l'option `--label-enable` et ensuite désigner les container à mettre à jour en leur passant le label `-l com.centurylinklabs.watchtower.enable=true`

5. Enfin dernière option très utile la possibilité de décider de la période de mise à jour à l'aide d'une expression de type cron. Comme exemple: `--schedule "0 0 4 * *"` mettra à jour à 0h0 tous les 4 de chaque mois.
6. Enfin lorsqu'une mise à jour s'effectue vous pouvez être notifié par mail, slack ou d'autres outils tels que shoutrrr. Se référer à la [documentation](#)

## **Surveillance et redémarrage de container**

Il peut arriver que certains container s'arrêtent brusquement suite à un bug.

Autoheal est un outil qui redémarre ces container automatiquement en se basant sur l'attribut healthcheck des containers.

La documentation est [ici](#).

Pour l'installer:

1. tapez:

```
docker run -d --name autoheal --restart=always -e AUTOHEAL_CONTAINER_LABEL=all /var/run/docker.sock:/var/run/docker.sock willfarrell/autoheal
```

2. La variable d'environnement AUTOHEAL\_CONTAINER\_LABEL indique que tous les containers seront vérifiés. Si vous souhaitez uniquement indiquer les container à vérifier, il vous faut ajouter pour les container concernés l'option `-l autoheal=true`

## **Configuration d'un repository local Docker**

L'outil Registry est un système de dépôt local pour Docker

Si vous avez plusieurs machines utilisant docker sur votre réseau, les déploiements et les mises à jour seront considérablement accélérées par l'utilisation de ce système de cache. Ce cache évitera aussi d'atteindre la limite d'accès sur le repository principal de docker

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)

2. Créez un volume et lancer le repository. Tapez:

```
docker volume create registry
docker run -d -p 5000:5000 --restart always --name registry --volume
registry:/var/lib/registry registry:2
```

3. Loguez vous comme root sur le poste client

4. Tapez:

```
vi /etc/docker/daemon.json
```

5. Dans le fichier, ajoutez:

```
{
 "insecure-registries" : ["docker.example.com:5000"],
}
```

- remplacer docker.example.com par le nom ou l'adresse ip de votre cache docker. Si vous en avez plusieurs vous devez tous les lister en les séparant par des virgules. Le numéro de port doit correspondre à celui choisi au lancement du container.

6. Sauvegarder le fichier et redémarrez le démon docker. Tapez:

```
systemctl restart docker
```

## Configuration de Docker-mirror

L'outil Docker-mirror est un système de cache de fichier Dockers.

Si vous avez plusieurs machines utilisant docker sur votre réseau, les déploiements et les mises à jour seront considérablement accélérées par l'utilisation de ce système de cache.

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur

2. Obtenez une configuration initiale pour le fichier config.yml. Tapez:

```
docker run -it --rm --entrypoint cat registry:
2 /etc/docker/registry/config.yml > /etc/docker-mirror.yml
```

3. Ajoutez ceci dans le fichier config.yml. Tapez:

```
vi /etc/docker-mirror-1.yml
```

#### 4. Dans ce fichier, ajoutez les lignes suivantes :

```
proxy:
 remoteurl: https://registry-1.docker.io
```

#### 5. Démarrez ensuite le service docker. Tapez:

```
docker volume create registry-proxy1
docker run -d --restart=always -p 5001:5000 --name docker-registry-
proxy-1 -v registry-proxy1:/var/lib/registry -v /etc/docker-
mirror-1.yml:/etc/docker/registry/config.yml registry:2
```

Si vous avez plusieurs miroirs à configurer, il faut créer un proxy sur chaque. Ainsi si vous voulez créer un miroir pour `ghcr.io` il vous faudra créer une autre fichier `docker-mirror-2.yml` avec la deuxième adresse `remoteurl`.

+

```
proxy:
 remoteurl: https://ghcr.io
```

#### 1. Lancer le tout par:

```
docker volume create registry-proxy2
docker run -d --restart=always -p 5002:5000 --name docker-registry-
proxy-2 -v registry-proxy2:/var/lib/registry -v /etc/docker-
mirror-2.yml:/etc/docker/registry/config.yml registry:2
```

Et ainsi de suite pour chaque proxy que vous voulez mettre en place.

Sur le poste client, soit passez l'option `--registry-mirror` lorsque vous lancez le démon `dockerd` ou sinon éditez le fichier `/etc/docker/daemon.json` et ajoutez la clé `registry-mirrors` pour rendre le changement persistant:

#### 1. Loguez vous comme root sur le poste client

#### 2. Tapez:

```
vi /etc/docker/daemon.json
```

#### 3. Dans le fichier, ajoutez:

```
{
 "insecure-registries" : ["docker.example.com:5001",
 "docker.example.com:5002"],
 "registry-mirrors": ["http://docker.example.com:5001",
 "docker.example.com:5002"]
}
```

- remplacer `docker.example.com` par le nom ou l'adresse ip de votre cache docker. Si vous en avez plusieurs vous devez tous les lister en les séparant par des virgules comme présenté dans l'exemple

4. Sauvegarder le fichier et redémarrez le démon docker. Tapez:

```
systemctl restart docker
```

## Outils web de gestion des containers

### *Installation de Yacht*

Yacht est un outil d'administration de vos instances docker sous forme de site web. Yacht est très facile d'utilisation mais manque de possibilités du moins dans la version actuelle. Si vous souhaitez administrer de façon plus avancée vos instances docker, il est conseillé d'utiliser Portainer.

Yacht s'installe comme un conteneur docker pour simplifier son déploiement.

Pour la création du site web, il faut suivre les étapes suivantes:

1. Allez dans ISPConfig dans la rubrique DNS, sélectionnez le menu Zones, Sélectionnez votre Zone, Allez dans l'onglet Records.
  - a. Cliquez sur A et saisissez:
    - Hostname: ← Tapez yacht
    - IP-Address: ← Double cliquez et sélectionnez l'adresse IP de votre serveur
  - b. Cliquez sur Save
2. Créer un sub-domain (vhost) dans le configateur de sites.
  - a. Lui donner le nom `yacht`.
  - b. Le faire pointer vers le web folder `yacht`.
  - c. Sélectionnez `None` dans Auto-subdomain
  - d. Activer let's encrypt SSL

e. Activer PHP-FPM pour PHP

f. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS

g. Laisser le reste par défaut.

h. Dans l'onglet Options:

i. Dans la boîte Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

yacht httpserver
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPass / http://localhost:8061/
ProxyPassReverse / http://localhost:8061/

RedirectMatch ^/$ https://yacht.example.com
```

■ remplacer example.com par votre nom de domaine

3. Puis sur votre serveur, Loguez vous comme root sur le serveur

4. Tapez:

```
docker volume create yacht_data
docker run -d -p 8061:8000 --name=yacht -v
/var/run/docker.sock:/var/run/docker.sock --restart=always -v
yacht_data:/config selfhostedpro/yacht
```

5. Ouvrez un navigateur et pointez sur <http://yacht.example.com>

6. L'utilisateur par défaut est login: admin@yacht.local et mot de passe: pass.

7. Une fois loggué, Cliquez sur l'utilisateur en haut à droite et `user`.
8. Cliquez sur `change password`
9. Modifier votre Email de login et saisissez un nouveau mot de passe.
10. Cliquez ensuite sur `Templates` dans la barre vertical de gauche puis sur `New templates`
11. Copiez la suggestion de template proposée.
12. Saisissez un titre `Yacht` dans le champ `Title` puis collez l'URL du json dans le champ `URL`
13. Cliquez sur `Submit`.
14. Allez dans `Templates` → `View Templates`.
15. cliquez sur `Yacht`; vous avez maintenant accès à une foule de templates.
16. Vous pouvez maintenant administrer vos machines docker. Référez vous à la documentation de [Yacht](#) pour installer de nouvelles machines docker

## ***Upgrade d'un container dans Yacht***

Plutôt que d'effectuer des mises à jour automatiques avec Watchtower, vous préférerez mettre à jour manuellement avec Yacht.

Appliquez la procédure suivante:

1. Ouvrez un navigateur et pointez sur <http://yacht.example.com>
2. Loguez vous en tant qu'`admin``
3. Allez dans l'onglet `Applications`
4. Cliquez sur le bouton `Updates`

## ***Upgrade de Yacht***

Rien a faire pour la mise à jour si vous utilisez `Watchtower` Vous pouvez aussi appliquer la procédure de mise à jour des [containers à l'aide de Portainer](#)

Sinon, effectuez les opérations suivantes:

1. [Loguez vous comme root sur le serveur](#)

2. Allez dans le répertoire de root

3. Mettez à jour le docker de Yacht. Tapez:

```
docker pull selfhostedpro/yacht
docker stop yacht
docker rm yacht
docker run -d -p 8061:8000 --name=yacht -v /var/run/docker.sock:/var/run/docker.sock --restart=always -v yacht_data:/config selfhostedpro/yacht
```

## ***Installation de Portainer***

Portainer est un outil d'administration de vos instances docker sous forme de site web. Portainer est plus complexe à utiliser que Yacht, mais offre cependant beaucoup plus de possibilités.

Portainer s'installe comme un conteneur docker pour simplifier son déploiement. Portainer gère une bonne partie des éléments de docker : conteneurs, images, volumes, réseaux, utilisateurs

Pour la création du site web, il faut suivre les étapes suivantes:

1. Allez dans ISPConfig dans la rubrique DNS, sélectionnez le menu Zones, Sélectionnez votre Zone, Allez dans l'onglet Records.

a. Cliquez sur **A** et saisissez:

- Hostname: ← Tapez portainer
- 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 portainer.

- b. Le faire pointer vers le web folder portainer.
- c. Sélectionnez None dans Auto-subdomain
- d. Activer let's encrypt SSL
- e. Activer PHP-FPM pour PHP
- f. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS
- g. Laisser le reste par défaut.
- h. Dans l'onglet Options:

- i. Dans la boite Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

portainer httpserver
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPass / http://localhost:9050/
ProxyPassReverse / http://localhost:9050/

RedirectMatch ^/$ https://portainer.example.com
■ remplacer example.com par votre nom de domaine
```

3. Puis sur votre serveur, Loguez vous comme root sur le serveur

4. Tapez:

```
docker volume create portainer_data
```

```
docker run -d -p 9050:9000 --name=portainer --restart=always -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest
```

5. Si vous utiliser **traefik**, il vous faut lancer docker avec la commande suivante:

```
docker run -d -p 9050:9000 --name=portainer --restart=always -l 'traefik.http.routers.portainer.rule=Host(`portainer.example.com`)' -l "traefik.enable=true" -l "traefik.http.routers.portainer.service=myportainersvc" -l "traefik.http.services.myportainersvc.loadbalancer.server.port=9000" -v /var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data portainer/portainer-ce:latest
```

- remplacez `example.com` par votre nom de domaine.

6. Ouvrez un navigateur et pointez sur <http://portainer.example.com>

7. Créez votre utilisateur de `admin` avec un mot de passe sécurisé.

8. Ajoutez un endpoint Local

9. Vous pouvez maintenant administrer vos machines docker. Référez vous à la documentation de [portainer](#) pour installer de nouvelles machines docker

Portainer offre la possibilité d'installer des templates par défaut. Vous pouvez soit garder le repository par défaut : <https://raw.githubusercontent.com/portainer/templates/master/templates-2.0.json> ou utiliser un autre repository comme : [https://raw.githubusercontent.com/Qballjos/portainer\\_templates/master/Template/template.json](https://raw.githubusercontent.com/Qballjos/portainer_templates/master/Template/template.json):

1. allez sur votre site web portainer.
2. puis dans le menu Settings
3. Dans la zone App Templates saisissez le repository de votre choix dans le champ URL
4. Cliquez sur Save Settings
5. retournez dans le menu App Templates; vos nouveau templates sont maintenant affichés.

## Upgrade d'un container dans Portainer

Plutôt que d'effectuer des mises à jour automatiques avec Watchtower, vous préférerez mettre à jour manuellement avec Portainer.

Appliquez la procédure suivante:

1. Ouvrez un navigateur et pointez sur <http://portainer.example.com>
2. Loguez vous en tant qu' admin
3. Allez dans l'onglet Containers
4. Double-cliquez sur le container à mettre à jour
5. Dans le nouvel écran Container details cliquez sur l'icone recreate
6. Sélectionnez Pull latest image et cliquez recreate

## Upgrade de Portainer

Rien a faire pour la mise à jour si vous utilisez Watchtower Vous pouvez aussi appliquer la procédure de mise à jour des containers à l'aide de [Yacht](#)

Sinon, effectuez les opérations suivantes:

1. [Loguez vous comme root sur le serveur](#)
2. Allez dans le répertoire de root
3. Mettez à jour le docker de Yacht. Tapez:

```
docker pull portainer/portainer-ce
docker stop portainer
docker rm portainer
docker run -d -p 9050:9000 --name=portainer --restart=always -v
/var/run/docker.sock:/var/run/docker.sock -v portainer_data:/data
portainer/portainer-ce
```

## Installation des CMS Joomla

Joomla est un CMS très connu écrit en PHP. Il est fréquemment mis à jour et inclut une foule de plugins

## 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 configateur de sites.
  - a. Lui donner le nom joomla.
  - b. Le faire pointer vers le web folder joomla.
  - c. Pour Auto-Subdomain sélectionnez None
  - d. Activer let's encrypt ssl
  - e. Activer PHP-FPM pour PHP
  - f. Laisser le reste par défaut.

## 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 joomla par exemple
- Database password: ← saisir un mot de passe généré 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 joomla
- Database user: ← Saisir ici le nom d'utilisateur créé: `cxjoomla.x`: est le numéro de client.

e. Cliquez sur `save`

## ***Création de l'application Joomla***

La procédure d'installation officielle de Joomla se trouve [ici](#)

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. allez sur le site de [Joomla](#) et copier l'adresse du lien vers la dernière version de l'outil en format tarball.
3. Installez Joomla. Exécutez:

```
cd /tmp
wget -O joomla.tar.gz https://downloads.joomla.org/cms/joomla3/3-9-
26/Joomla_3-9-26-Stable-Full_Package.tar.gz?format=gz
cd /var/www/joomla.example.com/joomla/
tar -xvzf /tmp/joomla.tar.gz
rm /tmp/joomla.tar.gz
```

```
chown -R web[x]:client[y] /var/www/joomla.example.com/joomla
```

- Remplacez [x] et [y] par les numéros de site web et de client. Ces informations sont consultables dans ISPConfig en consultant les informations du Web Domain→onglet Options→champs Linux User et Linux Group.
- mettre ici votre site web à la place de joomla.example.com et le répertoire d'installation à la place de joomla
- coller ici l'adresse de téléchargement récupérée sur le site de Joomla.

4. Pointez votre navigateur sur <https://joomla.example.com>.

5. Dans l'onglet configuration :

1. Choisissez votre langue fr.
2. Nom du site ← mettez le nom de votre site web
3. Description ← mettez une description courte de votre site
4. Email ← indiquez votre email d'admin
5. Saisissez le identifiant du compte administrateur
6. Saisissez 2 fois un mot de passe généré dans mot de passe

6. Cliquez suivant

1. Choisissez une base MySQLi
2. mettez Localhost comme Nom du serveur
3. Dans le nom d'utilisateur mettez cxjoomla comme créé plus haut
4. Dans le mot de passe saisissez le mot de passe de créé pour la base.
5. Dans le nom de la base de données mettez cxjoomla comme créé plus haut
6. Vous pouvez laisser le prefixe des tables ou mettre à vide si votre base est dédiée.

7. Cliquez suivant

1. Dans l'écran suivant, vous choisissez le type de site

2. Vérifiez votre configuration

8. Cliquez suivant

9. L'installation s'effectue. Une fois terminée avec succès, vous pouvez décider d'installer des langues

10. N'oubliez pas ensuite de supprimer le répertoire `installation` en cliquant sur le bouton Supprimer le répertoire

11. Cliquez ensuite sur le bouton Administration pour continuer à configurer votre site ou sur Site pour voir votre installation par défaut

### ***Update de Joomla***

La mise à jour de Joomla s'effectue au travers du portail d'administration Joomla vous prévient d'un mise à jour du moteur et vous propose de le mettre à jour. Cliquez sur le lien qui vous est présenté dans l'interface.

## **Installation des CMS Concrete5**

Concrete5 est un CMS très connu écrit en PHP. Il est fréquemment mis à jour et permet une configuration wysiwyg

### ***Création du site web de Concrete5***

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 Concrete5

- IP-Address: ← Double cliquez et sélectionnez l'adresse IP de votre serveur
- b. Cliquez sur `Save`
2. Créez un sub-domain (vhost) dans le configurateur de sites.
- a. Lui donner le nom `Concrete5`.
  - b. Le faire pointer vers le web folder `Concrete5`.
  - c. Pour `Auto-Subdomain` sélectionnez `None`
  - d. Activer let's encrypt ssl
  - e. Activer `PHP-FPM` pour PHP
  - f. Laisser le reste par défaut.

## 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 `Concrete5` par exemple
      - `Database password:` ← saisir un mot de passe généré 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 `Concrete5`
  - Database user: ← Saisir ici le nom d'utilisateur créé: `cxConcrete5.` x: est le numéro de client.
- e. Cliquez sur `save`

## ***Création de l'application Concrete5***

La procédure d'installation officielle de Concrete5 se trouve [ici](#)

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. allez sur le site de [Concrete5](#) et téléchargez la dernière version de l'outil en format zip.
3. Uploader ce fichier dans votre répertoire `/tmp` de votre serveur au moyen de filezilla
4. Installez Concrete5. Exécutez:

```
cd /tmp
unzip concrete5-8.5.5.zip
mv concrete5-8.5.5/* /var/www/concrete5.example.com/concrete5/
rm -rf concrete5-8.5.5
rm concrete5-8.5.5.zip
chown -R web[x]:client[y] /var/www/concrete5.example.com/concrete5
```

- Remplacez [x] et [y] par les numéros de site web et de client. Ces informations sont consultables dans ISPConfig en consultant les informations du Web Domain→onglet Options→champs Linux User et Linux Group.

- mettre ici votre site web à la place de concrete5.example.com et le répertoire d'installation à la place de concrete5

- le nom du fichier zip dépend de la version que vous avez téléchargé. De même le nom du répertoire est dépendant de la version.

5. Pointez votre navigateur sur <https://concrete5.example.com>.

6. Choisissez votre langue français.

7. Le système check que la configuration est correcte.

8. Cliquez sur continuer l'installation

9. Nom ← saisissez le nom de votre site

10. Adresse de courriel administrateur ← indiquez votre email d'admin

11. Saisissez 2 fois un mot de passe généré dans Mot de passe administrateur

12. Choisissez le point de départ

13. mettez Localhost comme Serveur

14. Dans le Utilisateur MySQL mettez cxconcrete5 comme créé plus haut

15. Dans le Mot de passe MySQL saisissez le mot de passe de créé pour la base.

16. Dans le nom de la base de données mettez cxconcrete5 comme créé plus haut

17. Cliquez sur la case à cocher de la politique de confidentialité

18. Cliquez Installer Concrete5

19. L'installation s'effectue. Une fois terminée avec succès, Cliquez sur Modifier votre site

## **Update de concrete5**

La mise à jour de concrete5 s'effectue au travers du portail d'administration concrete5 vous prévient d'un mise à jour du moteur et vous propose de le mettre à jour. Cliquez sur le lien qui vous est présenté dans l'interface.

## Installation du portail wiki Mediawiki

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

### ***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 configateur de sites.
  - a. Lui donner le nom `mediawiki`.
  - b. Le faire pointer vers le web folder `mediawiki`.
  - c. Pour `Auto-Subdomain` sélectionnez `None`
  - d. Activer let's encrypt ssl
  - e. Activer `PHP-FPM` pour PHP
  - f. Laisser le reste par défaut.

### ***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 mediawiki par exemple
- Database password: ← saisir un mot de passe généré 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 mediawiki
- Database user: ← Saisir ici le nom d'utilisateur créé: cxmediawiki. x: est le numéro de client.

e. Cliquez sur save

## **Création de l'application Mediawiki**

La procédure d'installation officielle de Mediawiki se trouve [ici](#)

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. allez sur le site de [Mediawiki](#) et copier l'adresse du lien vers la dernière version de l'outil en format tarball.
3. Installez Mediawiki. Exécutez:

```
cd /tmp
wget https://releases.wikimedia.org/mediawiki/1.35/mediawiki-1.35.2.tar.gz -O mediawiki.tar.gz
tar -xvzf mediawiki.tar.gz
mv mediawiki-1.35.2/* /var/www/mediawiki.example.com/mediawiki/
rm mediawiki.tar.gz
rm -rf mediawiki-1.35.2
chown -R web[x]:client[y] /var/www/mediawiki.example.com/mediawiki
```

- Remplacez [x] et [y] par les numéros de site web et de client. Ces informations sont consultables dans ISPConfig en consultant les informations du Web Domain→onglet Options→champs Linux User et Linux Group.
- mettre ici votre site web à la place de mediawiki.example.com et le répertoire d'installation à la place de mediawiki
- coller ici l'adresse de téléchargement récupérée sur le site de Mediawiki.
- le nom du fichier tar.gz dépend de la version que vous avez téléchargé. De même le nom du répertoire est dépendant de la version.

4. Pointez votre navigateur sur <https://mediawiki.example.com>.
5. Cliquez sur set up the wiki. La procédure d'installation se déclenche :
6. Choisissez votre langue fr. Cliquez sur continuer
  1. L'environnement est vérifié. Assurez vous que le texte L'environnement a été vérifié. Vous pouvez installer MediaWiki. s'affiche.
  2. Choisissez une base MariaDB
  3. mettez Localhost comme nom d'hote de la Base
  4. Dans le nom de la base de données mettez cxmediawiki comme créé plus haut
  5. Dans le nom d'utilisateur de la base de données mettez cxmediawiki comme créé plus haut
  6. Dans le mot de passe saisissez le mot de passe de créé pour la base.

7. Cliquez sur `continuer`

1. Dans l'écran suivant, cliquez `continuer` sans rien changer

2. Saisissez le nom du wiki

3. Saisissez le nom d'utilisateur du compte administrateur

4. Saisissez 2 fois un mot de passe généré

5. Saisissez Adresse de courriel ← votre Email.

8. Cliquez sur `continuer`

1. Répondez en fonction de vos besoins aux questions suivantes.

9. Cliquez sur `continuer`

10. Lisez le texte et cliquez sur `continuer`

11. L'installation s'effectue et se termine avec succès. Cliquez sur `continuer`

12. Le fichier LocalSettings.php vous est proposé au téléchargement. Enregistrez le et ouvrez le dans un éditeur. Copier tout le contenu du fichier dans le presse-papier

13. Loguez vous comme root sur le serveur

14. Créez le fichier LocalSettings.php. Tapez:

```
vi /var/www/mediawiki.example.com/mediawiki/LocalSettings.php
```

- mettre ici votre site web à la place de mediawiki.example.com et le répertoire d'installation à la place de mediawiki

15. Coller tout le texte dans le fichier édité. Sauvegardez et quittez.

16. Tapez:

```
chown -R web[x]:client[y]
/var/www/mediawiki.example.com/mediawiki/LocalSettings.php
chmod 644 /var/www/mediawiki.example.com/mediawiki/LocalSettings.php
```

- Remplacez [x] et [y] par les numéros de site web et de client. Ces informations sont consultables dans ISPConfig en consultant les

informations du Web Domain→onglet Options→champs Linux User et Linux Group.

- mettre ici votre site web à la place de mediawiki.example.com et le répertoire d'installation à la place de mediawiki

17. Dans votre navigateur cliquez sur accéder à votre wiki

18. C'est fait

## ***Update du serveur Mediawiki***

La procédure de mise à jour officielle de Mediawiki se trouve [ici](#)

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. allez sur le site de [Mediawiki](#) et copier l'adresse du lien vers la dernière version de l'outil en format tarball.
3. Mettez à jour Mediawiki. Exécutez:

```
mkdir /tmp/mediawiki.old
mv /var/www/mediawiki.example.com/mediawiki/* /tmp/mediawiki.old
cd /tmp
wget https://releases.wikimedia.org/mediawiki/1.35/mediawiki-1.35.2.tar.gz
tar -xvzf mediawiki.tar.gz
mv mediawiki-1.35.2/* /var/www/mediawiki.example.com/mediawiki/
rm mediawiki.tar.gz
rm -rf mediawiki-1.35.2
cp /tmp/mediawiki.old/LocalSettings.php
/var/www/mediawiki.example.com/mediawiki/LocalSettings.php
cp -r /tmp/mediawiki.old/images/*
/var/www/mediawiki.example.com/mediawiki/images/
chown -R web[x]:client[y] /var/www/mediawiki.example.com/mediawiki
```

- Remplacez [x] et [y] par les numéros de site web et de client. Ces informations sont consultables dans ISPConfig en consultant les informations du Web Domain→onglet Options→champs Linux User et Linux Group.

- mettre ici votre site web à la place de mediawiki.example.com et le répertoire d'installation à la place de mediawiki
  - coller ici l'adresse de téléchargement récupérée sur le site de Mediawiki.
  - le nom du fichier tar.gz dépend de la version que vous avez téléchargé. De même le nom du répertoire est dépendant de la version.
4. vous pouvez aussi copier vos logos du répertoire resources/assets de l'ancien mediawiki.
  5. Mettez à jour vos extensions avec les dernières versions compatibles.
  6. Suivez les recommandations de mise à jour de Mediawiki pour le fichier LocalSettings.php
  7. exécuter le script d'update. Tapez:  

```
cd /var/www/mediawiki.example.com/mediawiki/maintenance
php update.php
```
  8. Vérifiez que tout s'est bien passé. Se référer à la documentation de Mediawiki pour résoudre les problèmes.
  9. Redémarrez apache. Tapez :  

```
systemctl restart apache2
```
  10. Vérifiez que tout fonctionne correctement sur le site phpmyadmin
  11. Supprimez l'ancien répertoire  

```
rm -rf /tmp/mediawiki.old
```

## Installation d'un gestionnaire de Blog Wordpress

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

### **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 `Add` et saisissez:

- Hostname: ← Tapez `wordpress`
- IP-Address: ← Double cliquez et sélectionnez l'adresse IP de votre serveur

b. Cliquez sur `Save`

2. Créez 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. Pour `Auto-Subdomain` sélectionnez `None`
- d. Activer let's encrypt ssl
- e. Activer `PHP-FPM` pour PHP
- f. Laisser le reste par défaut.

## **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 `wordpress` par exemple
      - `Database password:` ← saisir un mot de passe généré 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 wordpress
  - Database user: ← Saisir ici le nom d'utilisateur créé: cxwordpress. x: est le numéro de client.
- e. Cliquez sur save

## ***Création de l'application Wordpress***

La procédure d'installation officielle de Wordpress se trouve [ici](#)

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. allez sur le site de [Wordpress](#) et copier l'adresse du lien vers la dernière version de l'outil en format tarball.
3. Installez Wordpress. Exécutez:

```
cd /tmp
wget -O wordpress.tar.gz https://wordpress.org/latest.tar.gz
tar -xvzf wordpress.tar.gz
mv wordpress/* /var/www/wordpress.example.com/wordpress/
rm wordpress.tar.gz
rm -rf wordpress
chown -R web[x]:client[y] /var/www/wordpress.example.com/wordpress
```

- Remplacez [x] et [y] par les numéros de site web et de client. Ces informations sont consultables dans ISPConfig en consultant les informations du Web Domain→onglet Options→champs Linux User et Linux Group.

- mettre ici votre site web à la place de wordpress.example.com et le répertoire d'installation à la place de wordpress
4. Pointez votre navigateur sur <https://wordpress.example.com>.
  5. Choisissez votre langue français. Cliquez sur continuer.
  6. Lisez le texte et cliquez sur C'est parti !
  7. Dans le nom de la base de données mettez cxwordpress comme créé plus haut
  8. Dans le Identifiant mettez cxwordpress comme créé plus haut
  9. Dans le Mot de passe saisissez le mot de passe de créé pour la base.
  10. mettez Localhost comme Adresse de la base de données
  11. Vous pouvez laisser le préfixe des tables ou mettre à vide si votre base est dédiée.
  12. Cliquez sur Envoyer.
  13. Cliquez ensuite sur Lancer l'installation
  14. Titre du site ← mettez le nom de votre site web
  15. Saisissez le identifiant du compte administrateur
    1. Saisissez un mot de passe généré dans mot de passe
    2. Votre e-mail ← indiquez votre email d'admin
  16. Cliquez Installer Wordpress
  17. C'est fini.
  18. Vous pouvez ensuite cliquer sur Se connecter pour administrer votre site

## **Update de wordpress**

La mise à jour de wordpress s'effectue directement dans le site web en allant sur Dashboard et l'item updates. Il n'y a rien d'autre à faire.

## Installation du CMS Micro Weber

Microweber est un système de gestion de contenu et un constructeur de sites web Open Source. Il est basé sur le langage de programmation PHP et le framework web Laravel 5, utilisant le glisser-déposer et permettant aux utilisateurs de créer rapidement du contenu, tout en programmant et en gérant plusieurs affichages. Il dispose d'une fonction d'édition en direct qui permet aux utilisateurs de visualiser leurs modifications telles qu'elles apparaîtraient.

### ***Création du site web de Microweber***

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 microweber
    - 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 microweber.
  - b. Le faire pointer vers le web folder microweber.
  - c. Activer let's encrypt ssl
  - d. Activer PHP-FPM pour PHP
  - e. Laisser le reste par défaut.
  - f. Cliquez sur Save
3. Loguez vous comme root sur le serveur

## 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 microweber par exemple
      - Database password: ← Saisissez un mot de passe généré 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 microweber
    - Database user: ← Saisir ici le nom d'utilisateur créé: cxmicroweber. x: est le numéro de client.
  - e. Cliquez sur save

## Installation de Microweber

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur

## 2. Tapez:

```
cd /var/www/microweber.example.com/microweber
wget
https://raw.githubusercontent.com/microweber-dev/webinstall/master/
webinstall.php
```

- mettre à la place de `example.com` votre nom de domaine

## 3. Un fois téléchargé, faites pointer votre navigateur vers <http://microweber.example.com/netinstall.php>

## 4. Indique . comme répertoire d'installation et cliquez sur Télécharger et décompresser microweber

## 5. Une fois le téléchargement terminé cliquez sur Installer Microweber. Rechargez la page si besoin.

## 6. Répondez aux questions suivantes:

- Database Engine ← MySQL
- Hostname ← Laissez localhost
- Username ← entrez `cxmicroweber`. x est le numéro de client; habituellement c'est 0
- Password ← Tapez votre mot de passe
- Database ← entrez `cxmicroweber`. x est le numéro de client; habituellement c'est 0
- Préfix des noms de tables ← Laissez le champ vide
- Website Default Language ← French
- Admin username ← tapez admin
- Admin password ← Tapez votre mot de passe
- Repeat password ← Tapez votre mot de passe
- Admin email ← Tapez votre adresse mail d'administrateur

7. Tapez `Install`
8. Vous êtes redirigé sur le site Microweber ou vous pourrez vous loguer et commencer à utiliser l'outil

## ***Update de Microweber***

La mise à jour de Microweber s'effectue directement dans le site web en allant sur Dashboard et l'item `updates`. Il n'y a rien d'autre à faire.

## **Installation de Mealie**

le logiciel `Mealie` est un gestionnaire de recettes et un planificateur de repas auto-hébergés avec un backend RestAPI et une application frontale responsive construite en Vue pour une expérience utilisateur agréable pour toute la famille.

### ***Prérequis***

Il vous faudra tout d'abord installer `docker` en vous référant au chapitre qui y est consacré.

### ***Installation du serveur Mealie***

Nous allons installer Mealie à partir de son container Docker.

Ouvrez un terminal et suivez la procédure:

1. [Loguez vous comme root sur le serveur](#)
2. Allez dans le répertoire de root
3. Créez le docker de Mealie. Tapez:

```
docker volume create mealie_data
docker run -d -p 1282:9000 --name=mealie --restart=always -v
mealie_data:/app/data/ -e PGID=1000 -e PUID=1000 ghcr.io/mealie-
recipes/mealie:latest
```

## Création du site web de mealie

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 mealie
    - IP-Address: ← Double cliquez et sélectionnez l'adresse IP de votre serveur
  - b. Cliquez sur Save
2. Créer un sub-domain (vhost) dans le configIBUTEUR de sites.
  - a. Lui donner le nom mealie.
  - b. Le faire pointer vers le web folder mealie.
  - c. Sélectionnez None dans Auto-subdomain
  - d. Activer let's encrypt SSL
  - e. Activer PHP-FPM pour PHP
  - f. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS
  - g. Laisser le reste par défaut.
  - h. Dans l'onglet Options:
  - i. Dans la boite Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !
```

```
mealie httpserver
#
SetEnvIf Authorization "(.*)" HTTP__AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPass / http://localhost:1282/
ProxyPassReverse / http://localhost:1282/

RedirectMatch ^/$ https://mealie.example.com
```

- remplacer `example.com` par votre nom de domaine

## ***Configuration du site mealie***

Votre site web `mealie` est installé et opérationnel.

1. Pointez votre navigateur sur votre site web `mealie`
2. Loggez vous avec le mail `changeme@email.com` et le mot de passe `MyPassword`
3. Vous devez ensuite aller dans le menu de configuration de l'utilisateur pour changer ce mail et ce mot de passe par défaut
4. Vous pouvez maintenant ajouter des utilisateurs et des recettes de cuisine.
5. C'est prêt !

## ***Upgrade de Mealie***

Rien à faire pour la mise à jour si vous utilisez `Watchtower`. Vous pouvez aussi appliquer la procédure de mise à jour des containers à l'aide de [Portainer](#) ou à l'aide [Yacht](#).

Sinon, effectuez les opérations suivantes:

1. [Loguez vous comme root sur le serveur](#)
2. Allez dans le répertoire de root
3. Mettez à jour le docker de Mealie. Tapez:

```
docker pull hkotel/mealie:latest
```

```
docker stop mealie
docker rm mealie
docker run -d -p 1282:9000 --name=mealie --restart=always -v
mealie_data:/app/data/ -e PGID=1000 -e PUID=1000 ghcr.io/mealie-
recipes/mealie:latest
```

## Installation du gestionnaire de photos Piwigo

Piwigo est une application web pour gérer votre collection de photos, et autres médias. Doté de puissantes fonctionnalités, il gère des galeries partout dans le monde. Elle est écrite en PHP et nécessite une base de données MySQL.

Piwigo était auparavant connu sous le nom PhpWebGallery.

### ***Création du site web de Piwigo***

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

f. Cliquez sur `Save`

### 3. Loguez vous comme root sur le serveur

## **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 `piwigo` par exemple
      - `Database password:` ← saisir un mot de passe généré 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 `piwigo`
    - `Database user:` ← Saisir ici le nom d'utilisateur créé: `cxiwigox`: x: est le numéro de client.
  - e. Cliquez sur `save`

## Installation de Piwigo

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)

2. Tapez la commande suivante:

```
cd /var/www/piwigo.example.com/piwigo
wget http://piwigo.org/download/dlcounter.php?code=netinstall -O
piwigo-netinstall.php
```

○ mettre à la place de `example.com` votre nom de domaine

3. Un fois téléchargé, faites pointer votre navigateur vers  
[http://piwigo.example.com/piwigo-netinstall.php](#)

4. Choisissez votre Langue à Français

5. Indique . comme répertoire d'installation et cliquez sur Télécharger et décompresser Piwigo

6. Une fois le téléchargement terminé cliquez sur Installer Piwigo. Rechargez la page si besoin.

7. Répondez aux questions suivantes:

○ Langue par défaut de la galerie ← Français

○ Hôte ← Laissez localhost

○ Utilisateur ← entrez cxpiwigo. x est le numero de client; habituellement c'est 0

○ Mot de passe ← Tapez votre mot de passe

○ Nom de la Base de données ← entrez cxpiwigo. x est le numero de client; habituellement c'est 0

○ Préfix des noms de tables ← Laissez le champ vide

○ Nom d'Utilisateur ← tapez admin

○ Mot de passe ← Tapez [votre mot de passe généré](#)

- Mot de passe [confirmer] ← Retapez votre mot de passe
  - Adresse e-mail ← Tapez votre adresse mail d'administrateur
8. Tapez Démarrer l'installation
9. Vous êtes redirigé sur le site piwigo ou vous pourrez vous loguer et commencer à utiliser l'outil

## ***Update de Piwigo***

La mise à jour de Piwigo s'effectue directement dans le site web en allant sur Dashboard Admin et l'item Mises à jour. Il n'y a rien d'autre à faire.

## **Installation du système collaboratif Nextcloud**

NextCloud est un serveur d'hébergement et de partage de fichiers gratuit et open source, fork du projet ownCloud. Il est très similaire aux autres systèmes de partage de fichiers des services comme Google Drive, Dropbox et iCloud ou Seafile. NextCloud vous permet de stocker des fichiers, des documents, des photos, des films et des vidéos à partir de la centrale l'emplacement. Avec NextCloud, vous pouvez partager des fichiers, des contacts et tout autre les médias avec vos amis et vos clients. NextCloud s'intègre avec le courrier, calendrier, contacts et autres fonctionnalités qui aideront vos équipes à obtenir leur travail est plus rapide et plus facile. Vous pouvez installer le client NextCloud sur un ou plusieurs PC pour synchroniser les fichiers avec votre serveur Nextcloud. Des clients sont disponibles pour la plupart des systèmes d'exploitation, y compris Windows, macOS, FreeBSD, et Linux.

### ***Installation initiale***

NextCloud est écrit en PHP et utilise une base de données MariaDB pour stocker ses données.

Pour installer, Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)

## 2. Installez quelques paquets de base. Tapez:

```
apt-get install php-cgi php-curl
```

## 3. Une fois installé, éditez le fichier php.ini pour changer quelques limitations.

Tapez:

```
vi /etc/php/8.2/fpm/php.ini
```

- remplacer 8.2 par votre version de php

### 1. Cherchez les champs ci dessous et changez les valeurs comme suit:

```
memory_limit = 512M
upload_max_filesize = 500M
post_max_size = 500M
max_execution_time = 300
```

### 2. Sauvez et redémarrez apache. Tapez:

```
systemctl restart apache2
```

## ***Création du site web de Nextcloud***

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 nextcloud
- IP-Address: ← Double cliquez et sélectionnez l'adresse IP de votre serveur

#### b. Cliquez sur Save

### 2. Créer un sub-domain (vhost) dans le configateur de sites.

#### a. Lui donner le nom nextcloud.

#### b. Le faire pointer vers le web folder nextcloud.

#### c. Sélectionnez None dans Auto-subdomain

#### d. Activer let's encrypt SSL

- e. Activer PHP-FPM pour PHP
- f. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS
- g. Aller dans l'onglet Statistics pour Webstatistics program sélectionnez None
- h. Laisser le reste par défaut.
- i. Cliquez sur Save

## **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 nextcloud par exemple
      - Database password: ← saisir un mot de passe généré 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 nextcloud

- Database user: ← Saisir ici le nom d'utilisateur créé: cxnextcloud. x: est le numéro de client.
- e. Cliquez sur `save`

## ***Installation de Nextcloud***

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur

2. Tapez la commande suivante:

```
cd /var/www/nextcloud.example.com/nextcloud
wget https://download.nextcloud.com/server/installer/setup-nextcloud.php
```

- mettre à la place de `example.com` votre nom de domaine
  1. Un fois téléchargé, faites pointer votre navigateur vers <http://nextcloud.example.com/setup-nextcloud.php>
  2. Indique . comme répertoire d'installation et cliquez sur `Next`
  3. Une fois le téléchargement terminé cliquez sur `Next`. Rechargez la page si besoin.
  4. Répondez aux questions suivantes:
    - Login Admin ← tapez `admin`
    - Password Admin ← Tapez votre mot de passe
    - ouvrez Stockage et base de données
    - Configurer la base de données ← cliquez sur `MariaDB`
    - Utilisateur de la Base de données ← entrez `cxnextcloud`. x est le numero de client; habituellement c'est 0
    - Password de la Base de données ← Tapez votre mot de passe
    - Nom de la Base de données ← entrez `cxnextcloud`. x est le numéro de client; habituellement c'est 0

- nom du serveur ← Laissez Localhost

5. Tapez Next
6. Vous êtes redirigé sur le site nextcloud ou vous pourrez vous loguer et commencer à utiliser l'outil

## ***Upgrade de Nextcloud***

La mise à jour de nextcloud se fait directement dans nextcloud avec l'outil de mise à jour intégré à l'interface. Il faut se connecter en mode Admin

## **Installation du gestionnaire de projet 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.

### ***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 configutateur de sites.
  - a. Lui donner le nom gitea.
  - b. Le faire pointer vers le web folder gitea.

- c. Sélectionnez `None` dans Auto-subdomain
- d. Activer `let's encrypt SSL`
- e. Activer `PHP-FPM` pour `PHP`
- f. Dans l'onglet `Redirect` Cochez la case `Rewrite HTTP to HTTPS`
- g. Laisser le reste par défaut.
- h. Dans l'onglet Options:

- i. Dans la boîte `Apache Directives`: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

gitea httpserver
#
SetEnvIf Authorization "(.*)" HTTP__AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPass / http://localhost:3000/
ProxyPassReverse / http://localhost:3000/

RedirectMatch ^/$ https://gitea.example.com
```

■ remplacer `example.com` par votre nom de domaine

- j. Cliquez sur `Save`

### 3. Loguez vous comme 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
```

## **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: ← Saisissez un mot de passe généré 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

## Téléchargez et installez Gitea

Appliquez les opérations suivantes:

1. Loguez vous comme root sur le serveur

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

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

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

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

4. Coller le texte suivant:

```
[Unit]
Description=Gitea (Git with a cup of tea)
After=syslog.target
After=network.target
Requires=mysql.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
```

5. Recharge la base de systemd. Tapez:

```
systemctl daemon-reload
```

6. Activez et démarrez Gitea. Tapez:

```
systemctl enable gitea.service
```

```
systemctl start gitea.service
```

7. 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

8. Laissez le reste et cliquez sur **Install Gitea**.

9. 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
```

10. Redémarrez gitea.

11. [Loguez vous comme root sur le serveur](#)

12. Tapez:

```
systemctl restart gitea.service
```

## ***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
```

- mettez ici le numéro de port que vous souhaitez

4. [Debloquez le port 2222 sur votre firewall](#)

5. Redémarrez gitea. Tapez:

```
systemctl restart gitea.service
```

6. Enjoy !

## ***Update de Gitea***

Appliquez les opérations suivantes:

1. [Loguez vous comme root sur le serveur](#)
2. Téléchargez gitea du [site de chargement](#). Tapez pour un système 64 bits:

```
service gitea stop
wget https://dl.gitea.io/gitea/main/gitea-main-linux-amd64 -O
/usr/local/bin/gitea
chmod 755 /usr/local/bin/gitea
service gitea start
```

## Installation de vaultwarden

le logiciel `vaultwarden` est un gestionnaire de mots de passe relativement complet et gratuit. Il peut être installé sur votre serveur VPS de manière indépendante de l'éditeur `vaultwarden`.

Il reste cependant un bémol puisque l'installation s'effectue à l'aide de containers dockers qui sont eux générés par l'éditeur de `vaultwarden`.

### **Prérequis**

Il vous faudra tout d'abord installer `docker` en vous référant au chapitre qui y est consacré.

### **Installation du serveur vaultwarden**

Nous allons installer Vaultwarden qui est la version libre de `vaultwarden` et compatible avec les APIs. Cette version est plus complète que la version officielle, consomme moins de ressources et est plus rapide.

Ouvrez un terminal et suivez la procédure:

1. [Loguez vous comme root sur le serveur](#)
2. Allez dans le répertoire de root
3. Installez `argon2`  
`apt install argon2`
4. Créez un [mot de passe](#)

5. Créez un code de hashage valide à partir de celui ci et notez le. tapez:

```
echo -n "MySecretPassword" | argon2 "$ (openssl rand -base64 32)" -e
-id -k 19456 -t 2 -p 1
```

6. Créez le docker de Vaultwarden. Tapez:

```
docker volume create vaultwarden_data
docker run -d -p 1280:80 --name=vaultwarden --restart=always -v
vaultwarden_data:/data:rw -e ROCKET_ENV=staging -e ROCKET_PORT=80 -e
ROCKET_WORKERS=10 -e SMTP_HOST=mail.example.com -e
SMTP_FROM=mailname@example.com -e SMTP_PORT=587 -e SMTP_SSL=true -e
SMTP_USERNAME=mailname@example.com -e SMTP_PASSWORD=mailpassword -e
WEBSOCKET_ENABLED=true -e ADMIN_TOKEN=Hashcode -e
SIGNUPS_ALLOWED=false -e DOMAIN=https://vaultwarden.example.com
vaultwarden/server:latest
```

- ici il faut remplacer `example.com` par votre nom de domaine. Il faut aussi remplacer `mailname@example.com` par une boite mail valide sur le serveur et `mailpassword` par le mot de passe de cette boite mail valide. `Hashcode` doit être remplacé par le code de hashage généré. Ce code protège l'accès `admin` de `vaultwarden`.

## ***Création du site web de vaultwarden***

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 `vaultwarden`
- `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 `vaultwarden`.

- b. Le faire pointer vers le web folder `vaultwarden`.
- c. Mettre `None` dans Auto-Subdomain
- d. Activer let's encrypt ssl
- e. Activer PHP-PFM pour PHP
- f. Laisser le reste par défaut.
- g. Dans l'onglet Options:

- h. Dans la boite Apache Directives: saisir le texte suivant:

```
<Proxy *>
 Order deny,allow
 Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

vaultwarden httpserver
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPass / http://localhost:1280/
ProxyPassReverse / http://localhost:1280/

RedirectMatch ^/$ https://vaultwarden.example.com
```

## **Configuration du site vaultwarden**

Votre site web `vaultwarden` est installé et opérationnel.

1. Pointez votre navigateur sur votre site web `vaultwarden`
2. Créez un compte avec votre login et choisissez un mot de passe.

3. Loggez vous sur le site vous pouvez maintenant créer des droits d'accès ou importer ceux d'un autre outil tel que `lastpass` ou `1password`.
4. Vous pouvez aussi vous connecter en tant qu'admin en allant sur l'url  
<https://vaultwarden.example.com/admin>
5. Une fenêtre apparaît vous demandant le code de hachage que vous avez configuré à l'installation. Saisissez le.
6. vous pouvez maintenant configurer des options dans vaultwarden.
7. une option qu'il est important de configurer est la désactivation de la création de compte. Pour cela:
  - allez dans General Settings
  - désactivez `Allow new signups`. Cliquez sur `Save` (en bas à gauche).
8. Les utilisateurs non invités ne pourront plus créer de compte sur votre serveur.
9. Une autre façon de faire est de démarrer le container docker avec l'option `-e SIGNUPS_ALLOWED=false`

Sur votre smartphone ou dans votre navigateur, configurez vaultwarden pour pointer vers votre serveur en y configurant l'URL: <https://vaultwarden.example.com>. Loguez vous.

Tout est prêt!

## ***Upgrade de vaultwarden***

Rien à faire pour la mise à jour si vous utilisez `Watchtower`. Vous pouvez aussi appliquer la procédure de mise à jour des containers à l'aide de [Portainer](#) ou à l'aide [Yacht](#).

Sinon, effectuez les opérations suivantes:

1. [Loguez vous comme root sur le serveur](#)
2. Allez dans le répertoire de root
3. Mettez à jour le docker de Bitwarden\_rs. Tapez:

```
docker pull vaultwarden/server:latest
```

```
docker stop vaultwarden
docker rm vaultwarden
docker run -d -p 1280:80 --name=vaultwarden --restart=always -v
vaultwarden_data:/data:rw -e ROCKET_ENV=staging -e ROCKET_PORT=80 -e
ROCKET_WORKERS=10 -e SMTP_HOST=mail.example.com -e
SMTP_FROM=mailname@example.com -e SMTP_PORT=587 -e SMTP_SSL=true -e
SMTP_USERNAME=mailname@example.com -e SMTP_PASSWORD=mailpassword -e
WEBSOCKET_ENABLED=true -e ADMIN_TOKEN=Hashcode -e
SIGNUPS_ALLOWED=false -e DOMAIN=https://vaultwarden.example.com
vaultwarden/server:latest
```

- ici il faut remplacer `example.com` par votre nom de domaine. Il faut aussi remplacer `mailname@example.com` par une boite mail valide sur le serveur et `mailpassword` par le mot de passe de cette boite mail valide. `Hashcode` doit être remplacé par le code de hashage généré. Ce code protège l'accès `admin` de `vaultwarden`.

## Installation de Heimdall

le logiciel `Heimdall` est un logiciel de portail offrant de nombreuses possibilités de configuration.

### Prérequis

Il vous faudra tout d'abord installer `docker` en vous référant au chapitre qui y est consacré.

### Installation du serveur Heimdall

Nous allons installer Heimdall à partir de son container Docker.

Ouvrez un terminal et suivez la procédure:

1. [Loguez vous comme root sur le serveur](#)
2. Allez dans le répertoire de root
3. Créez le docker de heimdall. Tapez:

```
docker volume create heimdall_data
```

```
docker run -d -p 1281:443 --name=heimdall --restart=always -v
heimdall_data:/config:rw -e PGID=1000 -e PUID=1000
linuxserver/heimdall
```

## Création du site web de heimdall

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 heimdall
    - 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 heimdall.
  - b. Le faire pointer vers le web folder heimdall.
  - c. Sélectionnez None dans Auto-subdomain
  - d. Activer let's encrypt SSL
  - e. Activer PHP-FPM pour PHP
  - f. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS
  - g. Laisser le reste par défaut.
  - h. Dans l'onglet Options:
  - i. Dans la boite Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>
```

```
ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

redirect from server
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
SSLProxyEngine On # Comment this out if no https required
ProxyPreserveHost On
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off

ProxyPass / https://localhost:1281/
ProxyPassReverse / https://localhost:1281/

RedirectMatch ^/$ https://heimdall.example.com
```

- remplacer `example.com` par votre nom de domaine

## **Configuration du site heimdall**

Votre site web `heimdall` est installé et opérationnel.

1. Pointez votre navigateur sur votre site web `heimdall`
2. Créez un compte avec votre login et choisissez un mot de passe.
3. Sélectionnez l'icone User (3 éme icone en forme de portrait à droite).
4. Sélectionnez Admin et cliquez sur l'icone modifier
5. Tapez un mot de passe, le confirmer. Sélectionnez "Allow logging in from a specific URL". Cliquez sur "Enregistrez"
6. Une URL est maintenant disponible vous pouvez la mettre comme page d'accueil de votre navigateur

Tout est prêt!

## Upgrade de Heimdall

Rien à faire pour la mise à jour si vous utilisez Watchtower. Vous pouvez aussi appliquer la procédure de mise à jour des containers à l'aide de [Portainer](#) ou à l'aide [Yacht](#).

Sinon, effectuez les opérations suivantes:

1. [Loguez vous comme root sur le serveur](#)
2. Allez dans le répertoire de root
3. Mettez à jour le docker de heimdall. Tapez:

```
docker pull linuxserver/heimdall
docker stop heimdall
docker rm heimdall
docker run -d -p 1281:443 --name=heimdall --restart=always -v
heimdall_data:/config:rw -e PGID=1000 -e PUID=1000
linuxserver/heimdall
```

## Installation du système de partage de fichiers Seafile

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

Cette installation est optionnelle.

### 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. Sélectionnez `None` dans Auto-subdomain
  - d. Activer `let's encrypt SSL`
  - e. Activer `PHP-FPM` pour PHP
  - f. Dans l'onglet Redirect Cochez la case `Rewrite HTTP to HTTPS`
  - g. Laisser le reste par défaut.
  - h. Dans l'onglet Options:
  - i. Dans la boite Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

Seafile configuration

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

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

seafile httpserver
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPreserveHost On
```

```

ProxyPass /seafhttp http://localhost:8092
ProxyPassReverse /seafhttp http://localhost:8092
RewriteRule ^/seafhttp - [QSA,L]

#
seahub
#
SetEnvIf Authorization "(.*)" HTTP__AUTHORIZATION=$1
ProxyPreserveHost On
ProxyPass / http://localhost:8090/
ProxyPassReverse / http://localhost:8090/

```

## **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 votre mot de passe généré ou en générer un en cliquant sur le bouton
      - Repeat Password: ← Resaisir 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 apparaître dans la liste des bases

## **Téléchargez et installez Seafile**

Appliquez la procédure suivante:

1. Loguez vous comme root sur le serveur

2. Installez quelques paquets Debian complémentaires. Tapez:

```
apt install python3 python3-setuptools python3-pip default-
libmysqlclient-dev
pip3 install --timeout=3600 Pillow pylibmc captcha jinja2 future
mysqlclient sqlalchemy==1.4.3 psd-tools django-pylibmc django-simple-
captcha python3-ldap
```

3. Allez sur le site de téléchargement de [Seafile](#) et copier le lien de téléchargement pour Server for generic Linux

4. Il est préférable d'exécuter les serveurs dans un répertoire privé plutôt que dans le répertoire web pour des questions de sécurité. Tapez:

```
cd /var/lib
mkdir seafile
cd seafile
wget
https://s3.eu-central-1.amazonaws.com/download.seadrive.org/seafile-
server_7.1.3_x86-64.tar.gz
tar zxvf seafile-server_7.1.3_x86-64.tar.gz
mkdir installed
mv seafile-server_* installed
cd seafile-server-*
./setup-seafile-mysql.sh
cd ../..
chown -R web1:client0 seafile
```

- choisissez le user et le groupe de votre site web. Ces informations sont consultables dans ISPConfig en consultant les informations du Web Domain→onglet Options→champs Linux User et Linux Group.
  - coller ici l'adresse de téléchargement récupérée sur le site de Seafile.
  - le nom du fichier tar.gz dépend de la version que vous avez téléchargé. De même le nom du répertoire est dépendant de la version.
5. A ce moment, vous devez répondre à un certain nombre de questions.
  6. Choisissez le mode de configuration 2) pour indiquer vous même les informations sur les bases de données créées.
  7. 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.
  8. Si tout est saisi correctement le programme doit donner une synthèse de ce qui a été configuré

## ***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/lib/seafile/conf
vi gunicorn.conf
```
2. Repérez 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 8082 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
```

- mettre à la place de `example.com` votre nom de domaine

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'
```

- mettre à la place de `example.com` votre nom de domaine

9. Démarrez Seafile. Tapez:

```
cd /var/lib/seafile/seafile-server-latest
sudo -u web1 ./seafile.sh start
sudo -u web1 ./seahub.sh start 8090
```

- 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 sur votre firewall](#)

11. Faites pointer votre navigateur sur <https://seafile.example.com>

12. La page de login de Seafile doit s'afficher

## **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/lib/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 "seafolder_dir" to your path of seafolder
installation
seafolder_dir=/var/lib/seafolder
script_path=${seafolder_dir}/seafolder-server-latest
seafolder_init_log=${seafolder_dir}/logs/seafolder.init.log
seahub_init_log=${seafolder_dir}/logs/seahub.init.log
seafgc_init_log=${seafolder_dir}/logs/seafgc.init.log

case "$1" in
start)
${script_path}/seafolder.sh start >> ${seafolder_init_log}
${script_path}/seahub.sh start 8090 >> ${seahub_init_log}
;;
restart)
${script_path}/seafolder.sh restart >> ${seafolder_init_log}
${script_path}/seahub.sh restart 8090 >> ${seahub_init_log}
;;
reload)
${script_path}/seahub.sh stop >> ${seahub_init_log}
${script_path}/seafolder.sh stop >> ${seafolder_init_log}
${script_path}/seaf-gc.sh >> ${seafgc_init_log}
${script_path}/seafolder.sh start >> ${seafolder_init_log}
${script_path}/seahub.sh start 8090 >> ${seahub_init_log}
;;
stop)
${script_path}/seahub.sh stop >> ${seahub_init_log}
${script_path}/seafolder.sh stop >> ${seafolder_init_log}
;;
*)
echo "Usage: /etc/init.d/seafolder {start|stop|restart|reload}"
exit 1
;;
esac

```

## 3. Créer un job cron dans ISPConfig pour démarrer Seafolder au démarrage

- Allez dans la rubrique **Sites** puis dans le menu **Cron Jobs**. Cliquez sur **Add cron Job**. Saisissez 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/lib/seafolder/startseafolder.sh start

#### 4. Créer un second job cron dans ISPConfig pour redémarrer Seafolder tous les jours

a. Allez dans la rubrique `Sites` puis dans le menu `Cron Jobs`. Cliquez sur `Add cron Job`. Saisissez 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/lib/seafolder/startseafolder.sh reload

#### 5. Arrez le serveur précédemment lancé en tant que root. Tapez:

#### 6. Enjoy !

## Upgrade de Seafolder

La procédure de mise à jour officielle de Seafolder se trouve [ici](#)

Suivez la procédure suivante:

1. Loguez vous comme root sur le serveur
2. Allez sur le site de téléchargement de [Seafile](#) et copier le lien de téléchargement pour Server for generic Linux
3. Il est préférable d'exécuter les serveurs dans un répertoire privé plutôt que dans le répertoire web pour des questions de sécurité. Tapez:

```
cd /var/lib/seafile
wget
https://s3.eu-central-1.amazonaws.com/download.seadrive.org/seafile-
server_7.1.3_x86-64.tar.gz
tar zxvf seafile-server_7.1.3_x86-64.tar.gz
./startseafile.sh stop
mv seafile-server_* installed
cd seafile-server-7.1.3
cd upgrade
./upgrade_7.1.2.sh
./setup-seafile-mysql.sh
cd ../../..
chown -R web1:client0 seafile
cd seafile/seafile-server-latest
sudo -u web1 ./seafile.sh start
sudo -u web1 ./seahub.sh start 8090
```

- coller ici l'adresse de téléchargement récupérée sur le site de Seafile.
  - choisissez le user et le groupe de votre site web. Ces informations sont consultables dans ISPConfig en consultant les informations du Web Domain→onglet Options→champs Linux User et Linux Group.
  - le nom du fichier tar.gz dépend de la version que vous avez téléchargé. De même le nom du répertoire est dépendant de la version.
  - exédez tous les scripts d'upgrade dont le numéro de version est supérieur ou égal au numéro de version du seafile installé préalablement.
4. Vérifiez que vous savez accéder à Seafile tant sur le site web qu'avec vos applis PC et smartphone

## Installation du système de monitoring Grafana

Grafana est un logiciel de visualisation et d'analyse à code source ouvert. Il vous permet d'interroger, de visualiser, d'alerter et d'explorer vos mesures, quel que soit l'endroit où elles sont stockées. En clair, il vous fournit des outils pour transformer vos données de base de données de séries chronologiques (TSDB) en de magnifiques graphiques et visualisations. Grafana s'appuie sur Prometheus afin d'obtenir des métriques. Loki est aussi installé pour réaliser une analyse précise des fichiers de logs.

Cette installation est optionnelle puisque Munin est déjà installé sur votre système.

### Création du site web de Grafana

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 `grafana`
    - `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 `grafana`.
  - b. Le faire pointer vers le web folder `grafana`.
  - c. Sélectionnez `None` dans `Auto-subdomain`
  - d. Activer `let's encrypt SSL`
  - e. Activer `PHP-FPM` pour PHP
  - f. Dans l'onglet `Redirect` Cochez la case `Rewrite HTTP to HTTPS`

g. Laisser le reste par défaut.

h. Dans l'onglet Options:

i. Dans la boîte Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

grafana httpserver
#
SetEnvIf Authorization "(.*)" HTTP__AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPass / http://localhost:3100/
ProxyPassReverse / http://localhost:3100/

RedirectMatch ^/$ https://grafana.example.com

■ remplacer example.com par votre nom de domaine
```

## Installation de Grafana

1. Loguez vous comme root sur le serveur

2. Tapez:

```
echo "deb https://packages.grafana.com/oss/deb stable main"
>>/etc/apt/sources.list.d/grafana.list
cd /etc/apt/trusted.gpg.d
wget https://packages.grafana.com/gpg.key grafana.asc
```

3. Installez les paquets. Tapez:

```
apt update
apt install grafana prometheus prometheus-mysqld-exporter prometheus-
apache-exporter prometheus-bind-exporter prometheus-process-exporter
```

#### 4. Editez la configuration de Prometheus. Tapez:

```
vi /etc/prometheus/prometheus.yml
```

#### 5. Ajoutez les lignes suivantes:

```
- job_name: 'prometheus'

 # Override the global default and scrape targets from this job
 every 5 seconds.

 scrape_interval: 5s
 scrape_timeout: 5s

 # metrics_path defaults to '/metrics'
 # scheme defaults to 'http'.

 static_configs:
 - targets: ['localhost:9090']

 - job_name: node
 # If prometheus-node-exporter is installed, grab stats about the
 local
 # machine by default.

 static_configs:
 - targets: ['localhost:9100']

 - job_name: dns-master
 static_configs:
 - targets: ['localhost:9119']
 labels:
 alias: dns-master

 - job_name: apache
 static_configs:
 - targets: ['localhost:9117']

 - job_name: process
 static_configs:
 - targets: ['localhost:9256']

 - job_name: mysql
 static_configs:
 - targets: ['localhost:9104']
```

**6. Editez la configuration de prometheus-process-exporter. Tapez:**

```
vi etc/default/prometheus-process-exporter
```

**7. Ajoutez les lignes suivantes:**

```
ARGS="-procnames postgres,dovecot,apache2,sshd,php-fpm7.3,rsync,named,mysqld"
```

**8. Editez la configuration de prometheus-mysqld-exporter. Tapez:**

```
vi etc/default/prometheus-mysqld-exporter
```

**9. Ajoutez les lignes suivantes:**

```
ARGS='--config.my-cnf /etc/mysql/debian.cnf --
collect.info_schema.tables.databases="*"
collect.auto_increment.columns
collect.perf_schema.file_instances.filter=".**"
collect.info_schema.tablestats'
```

**10. Ajuster les permissions du fichier de conf de mysql pour donner l'accès à prometheus. Tapez:**

```
chmod 644 /etc/mysql/debian.cnf
```

**11. Ajustez la configuration de bind pour servir des statistiques. Tapez:**

```
vi /etc/bind/named.conf
```

**12. Ajouter dans le fichier:**

```
statistics-channels {
 inet 127.0.0.1 port 8053 allow { 127.0.0.1; };
};
```

**13. Activez dans mysql quelques statistiques. Tapez:**

```
mysql -p
```

**14. tapez votre mot de passe root pour mysql. puis taper:**

```
INSTALL PLUGIN QUERY_RESPONSE_TIME_AUDIT SONAME
'query_response_time.so';
INSTALL PLUGIN QUERY_RESPONSE_TIME SONAME 'query_response_time.so';
INSTALL PLUGIN QUERY_RESPONSE_TIME_READ SONAME
'query_response_time.so';
INSTALL PLUGIN QUERY_RESPONSE_TIME_WRITE SONAME
'query_response_time.so';
SET GLOBAL query_response_time_stats=ON;
SET GLOBAL userstat=ON;
```

## 15. Redémarrez les services. Taper:

```
service prometheus restart
service prometheus-mysqld-exporter restart
service prometheus-process-exporter restart
```

## ***Installation et configuration de Loki***

Pour installer Loki, appliquez la procédure suivante:

### 1. Loguez vous comme root sur le serveur

### 2. allez sur le site de [Loki](#) et copier l'adresse du lien vers la dernière version de loki-linux-amd64.zip (ou loki-linux-arm.zip pour raspberry pi 3 ou loki-linux-arm64.zip pour raspberry pi 4 ou 5)

### 3. Tapez:

```
cd /usr/local/bin
curl -fSL https://github.com/grafana/loki/releases/download/v1.4.1/loki-linux-amd64.zip
gunzip loki.gz
chmod a+x loki
```

### 4. Créez le fichier de configuration de loki

```
vi /etc/config-loki.yml
```

### 5. Ajoutez le texte ci dessous dans le fichier

```
auth_enabled: false

server:
 http_listen_port: 3100
 log_level: "warn"

ingester:
 lifecycler:
 address: 127.0.0.1
 ring:
 kvstore:
 store: inmemory
 replication_factor: 1
 final_sleep: 0s
```

```
 chunk_idle_period: 5m
 chunk_retain_period: 30s

 schema_config:
 configs:
 - from: 2010-01-01
 store: boltdb
 object_store: filesystem
 schema: v9
 index:
 prefix: index_
 period: 168h

 storage_config:
 boltdb:
 directory: /tmp/loki/index

 filesystem:
 directory: /tmp/loki/chunks

 limits_config:
 enforce_metric_name: false
 reject_old_samples: true
 reject_old_samples_max_age: 168h

 chunk_store_config:
 max_look_back_period: 0

 table_manager:
 chunk_tables_provisioning:
 inactive_read_throughput: 0
 inactive_write_throughput: 0
 provisioned_read_throughput: 0
 provisioned_write_throughput: 0
 index_tables_provisioning:
 inactive_read_throughput: 0
 inactive_write_throughput: 0
 provisioned_read_throughput: 0
 provisioned_write_throughput: 0
 retention_deletes_enabled: false
 retention_period: 0
```

6. [Débloquez le port 3100 sur votre firewall](#)

7. Testez maintenant la configuration de Loki. Tapez:

```
loki -config.file /etc/config-loki.yml
```

8. Ouvrez un navigateur et visitez: <http://example.com:3100/metrics>

9. Maintenant arrêtez Loki en tapant **CTRL-C**.

10. [Bloquez le port 3100 sur votre firewall](#)

11. Configurez un service Loki afin de le faire tourner en arrière plan. Tapez:

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

12. Ajoutez le texte ci dessous et sauvez:

```
[Unit]
Description=Loki service
After=network.target

[Service]
Type=simple
ExecStart=/usr/local/bin/loki -config.file /etc/config-loki.yml

[Install]
WantedBy=multi-user.target
```

13. Maintenant lancez le service et vérifiez que tout est fonctionnel. Tapez: Now start and check the service is running.

```
sudo service loki start
sudo service loki status
```

## ***Installation et configuration de Promtail***

Installez maintenant Promtail:

1. allez sur le site de [Loki](#) et copier l'adresse du lien vers la dernière version de promtail-linux-amd64.zip (ou promtail-linux-arm.zip pour raspberry pi 3 ou promtail-linux-arm64.zip pour raspberry pi 4 ou 5)
2. [Loguez vous comme root sur le serveur](#)
3. Tapez:

```
cd /usr/local/bin
curl -fSL -o promtail.zip
https://github.com/grafana/loki/releases/download/v1.4.1/promtail-
linux-amd64.zip
gunzip promtail.zip
chmod a+x promtail
```

#### 4. Créez la configuration de Promtail. Tapez:

```
mkdir -p /var/log/journal
vi /etc/config-promtail.yml
```

#### 5. Et ajoutez le texte suivant puis sauvez:

```
server:
 http_listen_port: 9080
 grpc_listen_port: 0

positions:
 filename: /tmp/positions.yaml

clients:
 - url: http://127.0.0.1:3100/api/prom/push

scrape_configs:
 - job_name: system
 static_configs:
 - targets:
 - localhost
 labels:
 job: varlogs
 __path__: /var/log/{*.log, */*.log}
```

#### 6. [Débloquez le port 9800 sur votre firewall](#)

#### 7. testez que Promtail fonctionne. Tapez:

```
promtail -config.file /etc/config-promtail.yml
```

#### 8. Ouvrez un navigateur et visitez: <http://example.com:9080>

#### 9. Maintenant arrêtez Promtail en tapant **CTRL-C**.

#### 10. [Bloquez le port 9800 sur votre firewall](#)

#### 11. Configurez un service Promtail afin de le faire tourner en arrière plan. Tapez:

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

## 12. Ajoutez le texte ci dessous et sauvez:

```
[Unit]
Description=Promtail service
After=network.target

[Service]
Type=simple
ExecStart=/usr/local/bin/promtail -config.file /etc/config-promtail.yml

[Install]
WantedBy=multi-user.target
```

## 13. Maintenant lancez le service et vérifiez que tout est fonctionnel. Tapez:

```
sudo service promtail start
sudo service promtail status
```

## 14. Allez sur votre site grafana <http://grafana.example.com> et ajoutez une source de données de type loki

## 15. Mettez l'URL suivante: <http://127.0.0.1:3100>. Laissez tout le reste tel quel.

## 16. vous pouvez maintenant explorer vos logs en utilisant le menu explore sur la gauche. Dans la zone texte "Log Labels" essayez ces exemples un à un:

```
{job="varlogs"}
```

## **Upgrade de Grafana**

Comme grafana est installé à partir de paquets Debian, la mise à jour s'effectue automatiquement avec le système.

Il reste cependant Loki et Promtail à mettre à jour.

Appliquez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. allez sur le site de [Loki](#) et copier l'adresse du lien vers la dernière version de loki-linux-amd64.zip (ou loki-linux-arm.zip pour raspberry pi 3 ou loki-linux-arm64.zip pour raspberry pi 4 ou 5)

3. allez sur le site de [Loki](#) et copier l'adresse du lien vers la dernière version de promtail-linux-amd64.zip (ou promtail-linux-arm.zip pour raspberry pi 3 ou promtail-linux-arm64.zip pour raspberry pi 4)

4. Mettez à jour Loki et Promtail à jour. Exécutez:

```
cd /usr/local/bin
curl -fSL -o loki.gz
https://github.com/grafana/loki/releases/download/v2.2.1/loki-linux-
amd64.zip
gunzip loki.gz
chmod a+x loki
curl -fSL -o promtail.zip
https://github.com/grafana/loki/releases/download/v2.2.1/promtail-
linux-amd64.zip
gunzip promtail.zip
chmod a+x promtail
```

5. redémarrez les service. Tapez:

```
sudo service loki restart
sudo service loki status
sudo service promtail restart
sudo service promtail status
```

6. Allez sur votre site Grafana <http://grafana.example.com>

7. Vérifiez que tout fonctionne

## Installation du système de backup BorgBackup

BorgBackup est un système de backup simple mais offrant des fonctionnalités avancées telles que le backup incrémental, la déduplication de données, la compression, l'authentification, l'encryption.

Borg backup est un système de backup offsite. Cela signifie que vous devez avoir accès à un espace de stockage sur un autre site pour effectuer cette sauvegarde.

Pour le moment, BorgBackup n'utilise pas de mécanisme de type RClone et il n'est donc pas encore possible de sauvegarder sur google drive ou autres espaces partagés.

## Introduction

BorgBackup permet de stocker des backups sur un serveur distant. Nous nommerons le serveur sur lequel les sauvegardes seront stockées : serveur de stockage et identifié par <storing\_srv>. Nous nommerons le serveur qu'il faut sauvegarder: serveur sauvegardé et identifié par <example.com>

## Installation du serveur de stockage

Il est préférable pour des questions de sécurité de créer un compte utilisateur spécifique.

Suivez la procédure suivante:

1. Loguez vous comme root sur <storing\_srv>.

2. Tapez:

```
apt install borgbackup
```

3. Générez un mot de passe long

**!** Important

Sauvegardez précieusement ce mot de passe. Il vous sera indispensable pour récupérer vos backup après un crash du serveur. Sans celui-ci, impossible de récupérer votre installation !

4. Créez un compte utilisateur. Tapez:

```
adduser borgbackup
```

5. Copiez-collez le mot de passe généré lorsqu'il est demandé

6. se loguer comme borgbackup

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

```
mkdir -p $HOME/.ssh
chmod 700 ~/.ssh
```

8. Allez dans le répertoire. Tapez :

```
cd ~/.ssh
```

9. Générez vous clés. Tapez :

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

10. 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.

11. Créez maintenant le répertoire pour recevoir les sauvegardes

```
cd
mkdir borgbackup
chmod 700 borgbackup
```

## ***Installation sur le serveur sauvegardé***

Suivez la procédure suivante:

1. [Loguez vous comme root sur <example.com>.](#)

2. Tapez:

```
apt install borgbackup
```

3. Copiez la clé publique de root sur le <storing\_srv>. Tapez:

```
ssh-copy-id -i ~/.ssh/id_*.pub borgbackup@<storing_srv>
```

4. Coller le mot de passe généré plus haut lorsqu'il est demandé

5. Affichez votre adresse IP. tapez:

```
wget -qO- http://ipecho.net/plain; echo
```

6. Faites un essai de connexion en tapant:

```
ssh borgbackup@<storing_srv>
```

7. Aucun mot de passe ne doit être demandée et vous devez être connecté en tant que borgbackup sur le <storing\_srv>

8. Si vous êtes très attaché à la sécurité, vous pouvez restreindre l'accès au seul serveur <example.com>. Tapez sur la ligne de commande du <storing\_srv> :

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

9. Ajoutez en première ligne du fichier :

```
from="SERVERIPADDRESS", command="borg serve --restrict-to-path
/home/borgbackup/borgbackup/", no-pty,no-agent-forwarding,no-port-
forwarding,no-X11-forwarding,no-user-rc
```

- remplacez SERVERIPADDRESS par l'adresse IP affichée plus tôt.

10. Fusionnez cette ligne avec la suivante qui démarre par ssh en prenant bien garde de laissez un espace entre no-user-rc et ssh-rsa

11. Déconnectez vous en tapant :

```
exit
```

12. De retour sur le serveur <example.com>

13. [Créez un mot de passe pour le dépôt borg backup.](#)

**!** Important

Sauvegardez précieusement ce mot de passe. Il vous sera indispensable pour récupérer vos backup après un crash du serveur. Sans celui-ci, impossible de récupérer votre installation !

14. Puis tapez:

```
export BORG_PASSPHRASE='mot_passe'
```

- mot\_passe doit être remplacé par celui généré plus haut

15. Initialisez le dépôt borg. Tapez:

```
borg init -e repokey-blake2
borgbackup@<storing_srv>:/home/borgbackup/borgbackup/
```

16. Tout est maintenant prêt pour faire un backup

17. avec le mode `repokey`, une clé de cryptage est stockée dans le repository de backup. Il est conseillé de la sauvegarder. Pour cela, tapez:

```
borg key export borgbackup@<storing_srv>:/home/borgbackup/borgbackup/
```

18. Notez bien la clé qui sert à décrypter le repository dans un endroit sécurisé  
==== Effectuer un backup

Nous allons créer tout d'abord un script de backup pour sauvegarder tout le serveur sauf les répertoires système:

1. Loguez vous comme root sur <example.com>.

2. Tapez:

```
vi /usr/local/bin/borgbackup.sh
```

3. Insérez dans le fichier le texte suivant:

```
#!/bin/sh
export BORG_PASSPHRASE='mot_passe'
cd / && /usr/bin/borg create --stats --progress --compress zstd
borgbackup@<storing_srv>:/home/borgbackup/borgbackup/:`hostname`-
`date +%Y-%m-%d-%H-%M-%S` ./ --exclude=dev --exclude=proc --
exclude=run --exclude=root/.cache/ --exclude=mnt/borgmount --
exclude=sys --exclude=swapfile --exclude=tmp && cd
```

- mot\_passe doit être remplacé par celui généré plus haut
- en fonction de la puissance de votre machine, vous pouvez remplacer l'algorithme de compression zstd par un algorithme lz4 (rapide) ou lzma (très lent mais performant en taille).

4. changez les permissions du script. Tapez:

```
chmod 700 /usr/local/bin/borgbackup.sh
```

5. vous pouvez maintenant effectuer une première sauvegarde en tapant:

```
/usr/local/bin/borgbackup.sh
```

## ***Lister les backups***

Nous allons créer un script de listage :

1. Loguez vous comme root sur <example.com>.

2. Tapez:

```
vi /usr/local/bin/borglist.sh
```

3. Insérez dans le fichier le texte suivant:

```
#!/bin/sh
export BORG_PASSPHRASE='mot_passe'
/usr/bin/borg list
borgbackup@<storing_srv>:/home/borgbackup/borgbackup/
```

- mot\_passe doit être remplacé par celui généré plus haut.

4. changez les permissions du script. Tapez:

```
chmod 700 /usr/local/bin/borglist.sh
```

5. vous pouvez maintenant lister vos backup en tapant:

```
/usr/local/bin/borglist.sh
```

## **Obtenir les infos sur un backup**

Nous allons créer un script de listage :

1. Loguez vous comme root sur <example.com>.

2. Tapez:

```
vi /usr/local/bin/borginfo.sh
```

3. Insérez dans le fichier le texte suivant:

```
#!/bin/sh
export BORG_PASSPHRASE='mot_passe'
/usr/bin/borg info --progress
borgbackup@<storing_srv>:/home/borgbackup/borgbackup/::$1
```

- mot\_passe doit être remplacé par celui généré plus haut.

4. changez les permissions du script. Tapez:

```
chmod 700 /usr/local/bin/borginfo.sh
```

5. vous pouvez maintenant lister vos backup en tapant:

```
/usr/local/bin/borginfo.sh
```

## **Vérifier un backup**

Nous allons créer un script de vérification :

1. Loguez vous comme root sur <example.com>.

2. Tapez:

```
vi /usr/local/bin/borgcheck.sh
```

3. Insérez dans le fichier le texte suivant:

```
#!/bin/sh
export BORG_PASSPHRASE='mot_passe'
```

```
/usr/bin/borg check --progress
borgbackup@<storing_srv>:/home/borgbackup/borgbackup/::$1
```

- mot\_passe doit être remplacé par celui généré plus haut.

4. changez les permissions du script. Tapez:

```
chmod 700 /usr/local/bin/borgcheck.sh
```

5. vous pouvez maintenant vérifier un de vos backup en tapant:

```
/usr/local/bin/borgcheck.sh <nom_de_sauvegarde>
```

- le nom de sauvegarde est récupéré en utilisant la commande borglist.sh

## **Restaurer un backup**

Nous allons créer un script de montage sous forme de système de fichier :

1. Loguez vous comme root sur <example.com>.

2. Tapez:

```
vi /usr/local/bin/borgmount.sh
```

3. Insérez dans le fichier le texte suivant:

```
#!/bin/sh
mkdir -p /mnt/borgbackup
export BORG_PASSPHRASE='mot_passe'
/usr/bin/borg mount
borgbackup@<storing_srv>:/home/borgbackup/borgbackup/ /mnt/borgbackup
```

- mot\_passe doit être remplacé par celui généré plus haut.

4. changez les permissions du script. Tapez:

```
chmod 700 /usr/local/bin/borgmount.sh
```

5. vous pouvez maintenant monter vos backups et effectuer des opérations de fichiers. Tapez:

```
/usr/local/bin/borgmount.sh
```

6. Pour créer un script pour démonter les backups. Tapez:

```
vi /usr/local/bin/borgumount.sh
```

7. Insérez dans le fichier le texte suivant:

```
#!/bin/sh
```

```
umount /mnt/borgbackup
rmdir /mnt/borgbackup
```

#### 8. changez les permissions du script. Tapez:

```
chmod 700 /usr/local/bin/borgumount.sh
```

#### 9. vous pouvez maintenant demonter vos backups. Tapez:

```
/usr/local/bin/borgumount.sh
```

### **Supprimer vos vieux backups**

Nous allons créer un script de ménage des backups :

#### 1. Loguez vous comme root sur <example.com>.

#### 2. Tapez:

```
vi /usr/local/bin/borgprune.sh
```

#### 3. Insérez dans le fichier le texte suivant:

```
#!/bin/sh
```

```
Nettoyage des anciens backups
On conserve
- une archive par jour les 7 derniers jours,
- une archive par semaine pour les 4 dernières semaines,
- une archive par mois pour les 6 derniers mois.
```

```
export BORG_PASSPHRASE='mot_passe'
/usr/bin/borg prune --stats --progress
borgbackup@<storing_srv>:/home/borgbackup/borgbackup --prefix
`hostname` --keep-daily=7 --keep-weekly=4 --keep-monthly=12
```

- mot\_passe doit être remplacé par celui généré plus haut.
- Le nettoyage des sauvegardes va conserver 7 sauvegardes journalières, 4 à la semaine et 12 au mois

#### 4. changez les permissions du script. Tapez:

```
chmod 700 /usr/local/bin/borgprune.sh
```

#### 5. vous pouvez maintenant effectuer du ménage:

```
/usr/local/bin/borgprune.sh
```

6. Pour récupérer l'espace libéré par la suppression des sauvegardes inutiles, créez le script suivant:

```
vi /usr/local/bin/borgcompact.sh
```

7. Insérez dans le fichier le texte suivant:

```
#!/bin/sh
```

```
export BORG_PASSPHRASE='mot_passe'
/usr/bin/borg compact --progress
borgbackup@<storing_srv>:/home/borgbackup/borgbackup/
```

- mot\_passe doit être remplacé par celui généré plus haut.

8. changez les permissions du script. Tapez:

```
chmod 700 /usr/local/bin/borgcompact.sh
```

9. vous pouvez maintenant effectuer du ménage:

```
/usr/local/bin/borgcompact.sh
```

==== Automatisez votre sauvegarde

10. Pour créer un script automatisé de backup. Tapez:

```
mkdir -p /var/log/borg
vi /usr/local/bin/borgcron.sh
```

11. Insérez dans le fichier le texte suivant:

```
#!/bin/sh
#
Script de sauvegarde.
#
set -e

LOG_PATH=/var/log/borg/cron.log

/usr/local/bin/borgbackup.sh >> ${LOG_PATH} 2>&1
/usr/local/bin/borgprune.sh >> ${LOG_PATH} 2>&1
/usr/local/bin/borgcompact.sh >> ${LOG_PATH} 2>&1
```

12. changez les permissions du script. Tapez:

```
chmod 700 /usr/local/bin/borgcron.sh
```

13. vous pouvez ensuite planifier votre backup à 1h du matin. Tapez:

```
crontab -e
```

#### 14. Inserez ensuite le texte suivant:

```
Backup via Borg to backup server
00 01 * * * /usr/local/bin/borgcron.sh
```

### ***Restauration d'urgence.***

En cas de crash du serveur, l'intérêt du backup offsite est de pouvoir remonter la dernière sauvegarde sans souci. Pour cela il faut avoir un moyen de booter le serveur dans un mode rescue (boot du VPS en mode rescue, utilisation d'un clé USB bootable, boot réseau ou autre moyen).

On suppose dans ce qu'il suit que vous avez booté sur un linux de type debian ou ubuntu dont la version n'est pas la toute dernière et dans laquelle borg-backup n'est pas obligatoirement présent du moins dans une version suffisamment récente.

1. loguez vous root sur votre serveur. A noter que, comme vous êtes en mode rescue, l'accès au mode est indiqué par votre hébergeur ou, si vous avez booté sur une clé USB en local, l'accès root s'effectue souvent avec une commande  
`sudo bash`

2. Montez votre partition racine. Sur un VPS, la partition est souvent déjà montée dans le répertoire /mnt. Sur un PC c'est souvent /dev/sda1. Sur un Raspberry Pi cette partition est /dev/mmcblk0p7. Tapez la commande:

```
mkdir -p /mnt/root
mount /dev/mmcblk0p7 /mnt/root
```

3. Installez borgbackup. Tapez:

```
apt install python3-pip libssl-dev cython3 gcc g++ libpython3-dev
libacl1-dev python3-llfuse libfuse-dev
pip3 install -U pip setuptools wheel
pip3 install pkgconfig
pip3 install borgbackup[llfuse]
```

4. Si la compilation échoue, c'est qu'il manque des packages. lisez attentivement les logs et installez les packages manquant.
5. Munissez vous du mot de passe <mot\_passe> des archives borg et tapez:

```
mkdir -p /mnt/borgbackup
```

```
export BORG_PASSPHRASE='mot_passe'
borg list borgbackup@<storing_srv>:/home/borgbackup/borgbackup/
```

- remplacez mot\_passe par votre mot de passe de borg

6. tapez le mot de passe du compte borgbackup.

7. la liste des sauvegardes est affichées à l'écran.

8. Choisissez l'archive qui vous convient et tapez:

```
cd /mnt/root
borg extract --list
borgbackup@<storing_srv>:/home/borgbackup/borgbackup/::<votre_archive>
```

9. tapez le mot de passe du compte borgbackup.

10. la restauration s'effectue et peut prendre des heures ! soyez patient.

11. il peut être nécessaire de réinstaller le bootloader (non utile sur VPS ou raspberry). Tapez:

```
cd /mnt/root
chroot . bash
mkdir -p dev proc run sys tmp
mount -t devtmpfs dev /dev
mount -t proc proc /proc
grub_install /dev/sda
umount /proc
umount /dev
sync
exit
```

- tapez ici le nom de device de votre disque de boot

12. Créez votre fichier de swap en suivant [la procédure](#). Attention le fichier de swap doit être installé dans /mnt/root/swapfile

13. vous pouvez maintenant rebooter votre machine en mode normal.

14. une autre façon de remonter la sauvegarde est d'extraire un fichier tar.xz directement du serveur de stockage et de transférer cette archive sur la machine en mode rescue puis de décompresser. La commande de génération d'archive est:

```
borg export-tar --list
borgbackup@<storing_srv>:/home/borgbackup/borgbackup/:<votre_archive
> restore.tar.xz
```

## Installation de Borgweb

Borgweb existe en version officielle. Cette version n'a pas trop d'intérêt pour nous étant donnée qu'elle n'interroge pas le serveur de stockage pour obtenir les informations des backups réalisés. Il existe un clone de repository qui implémente une fonctionnalité qui liste tous les backups effectués sur le serveur de stockage

Suivez la procédure suivante sur le serveur de stockage:

1. Loguez vous comme root sur <storing\_srv>.

2. Installez pip pour python3 et NPM. Tapez:

```
apt install python3-pip npm
```

3. Installer le logiciel dans le répertoire /var/lib/borgweb. Tapez:

```
mkdir -p /var/lib/borgweb
cd /var/lib/borgweb
git clone https://github.com/vche/borgweb.git
```

4. Dans la version testée, le fichier README.rst est utilisé par l'installeur mais plus présent dans le repo. Tapez:

```
cd borgweb
touch README.rst
```

5. Lancez l'installation. Tapez:

```
pip3 install -e .
cd js
npm install
```

6. Editez la configuration. Comme la variable d'environnement BORG\_CONFIG semble n'avoir aucun effet, éditez directement le fichier de configuration du repository. Tapez:

```
cd /var/lib/borgweb/borgweb/borgweb
vi config.py
```

7. Mettez ce texte dans le fichier édité:

```
class Config(object):
```

```
"""This is the basic configuration class for BorgWeb."""

#: builtin web server configuration
HOST = '127.0.0.1' # use 0.0.0.0 to bind to all interfaces
PORT = 5000 # ports < 1024 need root
DEBUG=False

#: borg / borgweb configuration
LOG_DIR = '/var/log/borg'
BORG_PATH="/usr/bin/borg"

Repo status cache configuration. TTL in secs
STATUS_CACHE_TTL=43200
STATUS_CACHE_PATH="/tmp/borgweb.cache"

BACKUP_REPOS = {
 # Repo name
 "example.com": {
 # Repo absolute path
 "repo_path": "/home/borgbackup/borgbackup",
 # Repo logs absolute path, or relative to the main
 LOG_DIR
 "log_path": "/var/log/borg/",
 # Repo password
 "repo_pwd": "your_password",
 # Command/script to run to manually start a backup.
 # If left empty or not specified, the backup won't be
 # manually runnable
 "script": "script",
 # Filled with discovered backups in the repo
 "backups": []
 }
}
```

- Insérez ici le mot de passe du dépôt Borg Backup
- Mettez ici le nom de votre domaine sauvegardé

8. Créez un service `systemd`. Editez le fichier de service. Tapez:

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

9. Insérez dans le fichier le texte suivant:

```
[Unit]
Description=Borgweb Daemon
After=syslog.target network.target

[Service]
WorkingDirectory=/var/lib/borgweb
User=root
Group=root
UMask=0002
Restart=on-failure
RestartSec=5
Type=simple
ExecStart=/usr/local/bin/borgweb
KillSignal=SIGINT
TimeoutStopSec=20
SyslogIdentifier=borgweb

[Install]
WantedBy=multi-user.target
```

10. Recharge la base de `systemd`. Tapez:

```
systemctl daemon-reload
```

11. Activez et démarrez `borgweb`. Tapez:

```
systemctl enable borgweb.service
systemctl start borgweb.service
```

## **Création du site web de Borgweb**

Appliquez les opérations suivantes Dans ISPConfig de votre serveur de stockage

<storing\_srv>:

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 borgweb
- IP-Address: ← Double cliquez et sélectionnez l'adresse IP de votre serveur

b. Cliquez sur Save

## 2. Créez un sub-domain (vhost) dans le configurateur de sites.

- a. Lui donner le nom borgweb.
- b. Le faire pointer vers le web folder borgweb.
- c. Sélectionnez None dans Auto-subdomain
- d. Activer let's encrypt SSL
- e. Activer PHP-FPM pour PHP
- f. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS
- g. Laisser le reste par défaut.
- h. Dans l'onglet Options:
- i. Dans la boîte Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

borgweb httpserver
#
<Location />
 AllowOverride AuthConfig
 AuthUserFile /var/lib/borgweb/borgweb-htpasswd
 AuthName "Borgweb"
 AuthType Basic
 Require valid-user

</Location>
```

```

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

borgweb httpserver
#
SetEnvIf Authorization "(.*)" HTTP__AUTHORIZATION=$1
ProxyPreserveHost On
ProxyPass / http://localhost:5000/
ProxyPassReverse / http://localhost:5000/

RedirectMatch ^/$ https://borgweb.example.com

```

- remplacer example.com par votre nom de domaine

3. Loguez vous comme root sur <storing\_srv>.

4. Créez ensuite le fichier de mot de passe de borgweb dans votre <storing\_srv>:

```
htpasswd -c /var/lib/borgweb/borgweb-htpasswd admin
```

5. Tapez votre mot de passe généré

6. Redémarrez apache. Tapez:

```
service apache2 restart
```

7. Pointez votre navigateur sur [https://borgweb.storing\\_srv](https://borgweb.storing_srv) , un mot de passe vous est demandé. Tapez admin pour le user et le password saisi. Vous accédez aux informations de sauvegarde de votre site.

## Installation d'un serveur de VPN Wireguard

### ***Création du site web de Wireguard***

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 wireguard
  - IP-Address: ← Double cliquez et sélectionnez l'adresse IP de votre serveur
- b. Cliquez sur Save
2. Créez un sub-domain (vhost) dans le configurateur de sites.
- a. Lui donner le nom wireguard.
  - b. Le faire pointer vers le web folder wireguard.
  - c. Sélectionnez None dans Auto-subdomain
  - d. Activer let's encrypt SSL
  - e. Activer PHP-FPM pour PHP
  - f. Dans l'onglet Redirect Cochez la case Rewrite HTTP to HTTPS
  - g. Laisser le reste par défaut.
  - h. Dans l'onglet Options:
  - i. Dans la boîte Apache Directives: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

wireguard httpserver
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPass / http://localhost:51821/
ProxyPassReverse / http://localhost:51821/
```

```
RedirectMatch ^/$ https://wireguard.example.com
```

- remplacer `example.com` par votre nom de domaine

## ***Installation de Wireguard***

Nous allons installer wg-easy qui est un container qui implémente wireguard dans un docker.

1. Loguez vous comme root sur le serveur

2. Installez Wireguard. Tapez:

```
docker run -d \
--name=wg-easy \
-e LANG=fr \
-e WG_HOST=Public_IP \
-e PASSWORD=mot_de_passe \
-e PORT=51821 \
-e WG_PORT=51820 \
-v /etc/wg-easy:/etc/wireguard \
-p 51820:51820/udp \
-p 51821:51821/tcp \
--cap-add=NET_ADMIN \
--cap-add=SYS_MODULE \
--sysctl="net.ipv4.conf.all.src_valid_mark=1" \
--sysctl="net.ipv4.ip_forward=1" \
--restart unless-stopped \
ghcr.io/wg-easy/wg-easy
```

- saisir votre adresse IP publique donnée par exemple sur le site <https://www.showmyip.com/>. Attention ce doit être une IP V4
- saisir un mot de passe généré

3. Configurez votre firewall pour ouvrir le port 51820 en mode UDP

## ***Update de Wireguard***

Rien a faire pour la mise à jour si vous utilisez Watchtower

Sinon, effectuez les opérations suivantes:

1. Loguez vous comme root sur le serveur
2. Allez dans le répertoire de root
3. Mettez à jour le docker de wg-easy. Tapez:

```
docker pull ghcr.io/wg-easy/wg-easy
docker stop wg-easy
docker rm wg-easy
docker run -d \
--name=wg-easy \
-e LANG=fr \
-e WG_HOST=Public_IP \
-e PASSWORD=mot_de_passe \
-e PORT=51821 \
-e WG_PORT=51820 \
-v /etc/wg-easy:/etc/wireguard \
-p 51820:51820/udp \
-p 51821:51821/tcp \
--cap-add=NET_ADMIN \
--cap-add=SYS_MODULE \
--sysctl="net.ipv4.conf.all.src_valid_mark=1" \
--sysctl="net.ipv4.ip_forward=1" \
--restart unless-stopped \
ghcr.io/wg-easy/wg-easy
```

- saisir votre adresse IP publique donnée par exemple sur le site <https://www.showmyip.com/>. Attention ce doit être une IP V4
- saisir un mot de passe généré

## Installation d'un serveur de bureau à distance Guacamole

Apache Guacamole est un logiciel opensource et une application web de bureau à distance qui vous permet d'accéder à vos machines de bureau par le biais d'un navigateur web. Il s'agit d'une appli web html5 qui prend en charge des protocoles standard comme VNC, RDP et SSH. Vous n'avez pas besoin d'installer et d'utiliser des logiciels ou des plugins sur le serveur. Avec Guacamole, vous pouvez facilement passer d'un bureau d'une machine à l'autre avec le même navigateur.

Guacamole est assez ancien et d'un point de vue protocole, il ne saura pas se connecter avec des serveurs VNC utilisants les stack cryptos récentes. Il faut se mettre en version compatible 3.8 de serveur VNC.

## **Création du site web de Guacamole**

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 `guacamole`
    - IP-Address: ← Double cliquez et sélectionnez l'adresse IP de votre serveur
  - b. Cliquez sur `Save`
2. Créer un [sub-domain \(vhost\)](#) dans le configutateur de sites.
  - a. Lui donner le nom `guacamole`.
  - b. Le faire pointer vers le web folder `guacamole`.
  - c. Sélectionnez `None` dans Auto-subdomain
  - d. Activer `let's encrypt SSL`
  - e. Activer `PHP-FPM` pour PHP
  - f. Dans l'onglet Redirect Cochez la case `Rewrite HTTP to HTTPS`
  - g. Laisser le reste par défaut.
  - h. Dans l'onglet Options:
    - i. Dans la boite `Apache Directives`: saisir le texte suivant:

```
<Proxy *>
Order deny,allow
Allow from all
```

```
</Proxy>

ProxyRequests Off
ProxyPass /stats !
ProxyPass /.well-known/acme-challenge !

guacamole httpserver
#
SetEnvIf Authorization "(.*)" HTTP_AUTHORIZATION=$1
ProxyPreserveHost On

ProxyPass /guacamole http://localhost:8085/guacamole
ProxyPassReverse /guacamole http://localhost:8085/guacamole

RedirectMatch ^/$ https://guacamole.example.com
 ■ remplacer example.com par votre nom de domaine

j. Cliquez sur Save
```

## 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 guacamole par exemple
      - Database password: ← Saisissez un mot de passe généré 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 guacamole
  - Database user: ← Saisir ici le nom d'utilisateur créé: cxguacamole. x: est le numéro de client.
- e. Cliquez sur save

## ***Installation du Guacamole***

Suivez la procédure suivante:

1. [Loguez vous comme root sur le serveur](#)
2. Guacamole n'est pas compatible aujourd'hui (version 1.5.5) de Tomcat10. Or c'est la version présente dans la dernière version de Debian. Je vous conseille donc d'installer tomcat9 de la version de debian précédente.
3. Tapez:

```
echo "deb http://deb.debian.org/debian/ bullseye main" >
/etc/apt/sources.list.d/bullseye.list
apt update
apt install tomcat9 tomcat9-admin tomcat9-common tomcat9-user
sed -i 's/^/#/' /etc/apt/sources.list.d/bullseye.list
apt install gcc g++ libossp-uuid-dev libavcodec-dev libpango1.0-dev
libssh2-1-dev libcairo2-dev libjpeg-dev libpng-dev libavutil-dev
libavformat-dev libswscale-dev libvncserver-dev libssl-dev libvorbis-
dev libwebp-dev freerdp2-dev libtelnet-dev libswscale-dev libossp-
uuid-dev libwebsockets-dev libpulse-dev libmariadb-java
```

4. Par ailleurs, Guacamole pose des problèmes de compatibilités avec IP V6.
5. Editez votre fichier /etc/hosts et commentez:

```
#:::1 localhost ip6-localhost ip6-loopback
```

6. Téléchargez la dernière version de Guacamole en allant sur le site web et en récupérant le [lien de téléchargement](#).

7. tapez:

```
cd /tmp
curl -fSL -o guacamole-server.tar.gz
'https://apache.org/dyn/closer.lua/guacamole/1.5.5/source/guacamole-
server-1.5.5.tar.gz?action=download'
tar xfz guacamole-server.tar.gz
cd guacamole-server-*
```

- insérez ici l'adresse du package serveur à charger

8. Lancez la configuration. Tapez:

```
./configure --with-init-dir=/etc/init.d
```

9. Vous devez obtenir, à la fin de la configuration, une table de ce type:

```

guacamole-server version 1.5.5

```

Library status:

```
freerdp2 yes
pango yes
libavcodec yes
libavformat..... yes
libavutil yes
libssh2 yes
libssl yes
libswscale yes
libtelnet yes
libVNCServer yes
libvorbis yes
libpulse yes
libwebsockets yes
libwebp yes
wsock32 no
```

Protocol support:

```

Kubernetes yes
RDP yes
SSH yes
Telnet yes
VNC yes

Services / tools:
```

```

guacd yes
guacenc yes
guaclog yes
```

10. Si ce n'est pas le cas, c'est qu'une bibliothèque n'est pas installée correctement.

11. Lancez la compilation et l'installation. Tapez:

```

make
make install
ldconfig
```

12. Activez le démon de gestion guacd. Tapez:

```

systemctl daemon-reload
systemctl enable guacd
systemctl start guacd
```

13. Téléchargez le dernier client war de Guacamole en allant sur le site web et en récupérant le [lien de téléchargement](#). Récupérez le lien puis tapez:

```

mkdir -p /usr/local/share/guacamole
cd /usr/local/share/guacamole
curl -fSL -o guacamole.war
'https://apache.org/dyn/closer.lua/guacamole/1.5.5/binary/guacamole-1
.5.5.war?action=download'
ln -s /usr/local/share/guacamole/guacamole.war
/var/lib/tomcat9/webapps/
systemctl restart tomcat9
systemctl restart guacd
 ○ insérez ici l'adresse du war à charger
```

14. Editez le fichier server.xml. Tapez:

```
vi /etc/tomcat9/server.xml
```

15. Chercher `Connector port="8080" protocol="HTTP/1.1` et remplacer partout le port 8080 par 8085

16. Créez les répertoires de configuration de guacamole. Tapez:

```
mkdir -p /etc/guacamole
mkdir -p /etc/guacamole/{extensions,lib}
```

17. Récupérez le driver mysql/mariadb pour java. Sur la plupart des Linux, il est présent dans `/usr/share/java`. Pour le copier, tapez:

```
ln -s /usr/share/java/mariadb-java-client.jar /etc/guacamole/lib/
```

18. Il se peut que ce driver ne soit pas présent: allez sur le site [Mysql](#) et téléchargez la version Platform independant. Tapez:

```
curl -fSL -o mysql-java.tar.gz
'https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-
j-8.3.0.tar.gz'
tar xfz mysql-java.tar.gz
cd mysql-connector-java-*
cp mysql-connector-java-*.jar /etc/guacamole/lib/mysql-connector-
java.jar
```

- Collez ici le lien récupéré sur le site de Mysql.

19. Editez le fichier `guacamole.properties`. Tapez:

```
vi /etc/guacamole/guacamole.properties
```

20. Ajoutez dans le fichier:

```
mysql-hostname: localhost
mysql-port: 3306
mysql-database: cxguacamole
mysql-username: cxguacamole
mysql-password: <mot_de_passe>
```

- mettez ici le nom de la base de données, le nom de l'utilisateur de la base et son mot\_de\_passe tels qu'ils ont été saisis dans le chapitre de création de la base de données.

21. Vous devez maintenant télécharger les plugins mysql pour Guacamole. Allez sur le site web de guacamole et récupérez le [lien de téléchargement de guacamole-auth-jdbc](#). Tapez:

```
cd /tmp
curl -fSL -o guacamole-auth-jdbc.tar.gz
'https://apache.org/dyn/closer.lua/guacamole/1.5.5/binary/guacamole-
auth-jdbc-1.5.5.tar.gz?action=download'
tar xfv guacamole-auth-jdbc.tar.gz
cd guacamole-auth-jdbc-*/mysql
cp guacamole-auth-jdbc-mysql-*.jar /usr/local/share/guacamole/
ln -s /usr/local/share/guacamole/guacamole-auth-jdbc-mysql-*.jar
/etc/guacamole/extensions

- insérez ici l'adresse du fichier guacamole-auth-jdbc à charger

```

## 22. Créez les tables de la base:

```
cd schema
cat *.sql | mysql -u cxguacamole -p cxguacamole

- mettez derrière le -u le nom d'utilisateur de la base de données et derrière
le -p le nom de la base de données. Un mot de passe vous sera demandé.

```

## 23. Redémarrez tomcat et guacd. Tapez:

```
systemctl restart tomcat9
systemctl restart guacd
```

## 24. Allez sur le site de [guacamole.example.com/guacamole](http://guacamole.example.com/guacamole)

### 25. Loguez vous avec le compte: **guacadmin** et password: **guacadmin**

26. Commencez par cliquez sur **guacadmin** → paramètres → utilisateurs → Nouvel Utilisateur

- Identifiant ← Tapez **admin**
- Mot de passe ← Tapez votre [mot de passe généré](#)
- Répétez mot de passe ← Retapez votre mot de passe
- Permissions ← activer toutes les options

## 27. Deconnectez vous et reconnectez vous avec le login **admin**

## 28. cliquez sur **admin** → paramètres → utilisateurs → **guacadmin**

## 29. Supprimez ce compte utilisateur

30. Si vous avez activé VNC. Cliquez sur Admin → Paramètres → Utilisateurs → Connexions → Nouvelle Connexion

- Nom ← Tapez Local server VNC
- Protocole ← Sélectionnez VNC
- Paramètres → Nom d'hôte ← Tapez Localhost
- Cochez SFTP → Activer SFTP
- SFTP → Nom d'hôte ← Tapez Localhost
- Paramètres → port ← Tapez 5900
- Paramètres → Mot de passe ← Tapez votre mot de passe VNC de votre machine locale.
- SFTP → Mot de passe ← Tapez un mot de passe sur votre Hôte

31. Cliquez sur Admin → Paramètres → Utilisateurs → Connexions → Nouvelle Connexion

- Nom ← Tapez Local server SSH
- Protocole ← Sélectionnez SSH
- Paramètres → Nom d'hôte ← Tapez Localhost
- Paramètres → port ← Tapez 22
- Paramètres → Identifiant ← Tapez un login sur votre Hôte
- Paramètres → Mot de passe ← Tapez votre mot de passe de compte
- Cochez SFTP → Activer SFTP
- SFTP → File browser root directory ← Tapez /

32. Vous pouvez maintenant vérifier vos connexions en vous loguant avec l'un des deux profils.

33.l'appui simultané sur SHIFT CTRL ALT fait apparaître un menu pour effectuer des chargements de fichiers ou contrôler votre connexion

## **Upgrade de Guacamole**

Il est nécessaire de regénérer les logiciels avec les dernières versions.

Appliquez la procédure suivante:

1. Loguez vous comme root sur le serveur

2. Arrêtez le serveur guacamole

```
systemctl stop guacd
```

3. Téléchargez la dernière version de Guacamole en allant sur le site web et en récupérant le lien de téléchargement.

4. tapez:

```
cd /tmp
curl -fSL -o guacamole-server.tar.gz
'http://apache.org/dyn/closer.cgi?
action=download&filename=guacamole/1.2.0/source/guacamole-
server-1.2.0.tar.gz'
tar xfz guacamole-server.tar.gz
cd guacamole-server-*
```

○ insérez ici l'adresse du package serveur à charger

5. Lancez la configuration. Tapez:

```
./configure --with-init-dir=/etc/init.d
```

6. Lancez la compilation et l'installation. Tapez:

```
make
make install
ldconfig
```

7. Téléchargez le dernier client war de Guacamole en allant sur le site web et en récupérant le lien de téléchargement. Récupérez le lien puis tapez:

```
cd /usr/local/share/guacamole
curl -fSL -o guacamole.war 'http://apache.org/dyn/closer.cgi?
action=download&filename=guacamole/1.2.0/binary/guacamole-1.2.0.war'
systemctl daemon-reload
```

```
systemctl restart tomcat9
systemctl start guacd
 ○ insérez ici l'adresse du war à charger
```

8. Allez sur le site de `guacamole.example.com/guacamole`

9. Vérifiez que tout fonctionne

## Annexe

### ***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. [Loguez vous comme root sur le serveur](#)
2. Télécharger le package et lancez l'installateur

a. Tapez :

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

b. Lancez l'installateur. 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

## **Configuration d'un écran 3.5 inch RPI LCD (A)**

### **Pour commencer**

Le RPi LCD peut être piloté de deux manières :

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

#### **5. Configurez votre Pi :**

```
sudo raspi-config
```

#### **6. configuez ainsi :**

- Sélectionnez "Expand Filesystem".
- Boot Option → Desktop Autologin (peut différer selon la révision Raspbian)

#### **7. Ouvrez le terminal du Raspberry PI (Vous devrez peut-être connecter un clavier et un écran LCD HDMI à PI pour l'installation du pilote). Tapez:**

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

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

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

#### **8. Après le redémarrage du système, le RPI LCD est prêt à l'emploi.**

## Basculer entre l'affichage LCD et HDMI

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

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

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

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

## Paramètres d'orientation de l'écran

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

- Rotation de 0 degrés

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

- Rotation de 90 degrés

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

- Rotation de 180 degrés

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

- Rotation de 270 degrés

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

## Calibrage de l'écran tactile

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

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

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

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

ou Sélectionnez Menu → Preferences → Calibrate Touchscreen.

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

Doing dynamic recalibration:

```
Setting new calibration data: 3919, 208, 236, 3913
```

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

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

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

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

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

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

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

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

```
sudo reboot
```

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

## Installer un clavier virtuel

### 1. Installer matchbox-keyboard

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

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

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

### 3. Exécutez les commandes:

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

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

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

### 5. Exécutez les commandes ci dessous.

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

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

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

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

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

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

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

Ressources

Manuel utilisateur

- [RPiLCD User Manual](#)

Images

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

- [RPi-35inch-LCD-\(A\)-Raspbian-180326.7z](#)

Driver

Le pilote peut être téléchargé sur github

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

Fichiers de configuration de référence

/boot/cmdline.txt

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

/boot/config.txt

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

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

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

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

# uncomment to force a console size. By default it will be display's size
# minus
# overscan.
#framebuffer_width=1280
#framebuffer_height=720

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

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

```

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

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

# uncomment for composite PAL
#sdtv_mode=2

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

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

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

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

/etc/inittab

```

Ajouter:

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

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

```
Section "Device"
    Identifier      "Allwinner A10/A13/A20 FBDEV"
    Driver          "fbturbo"
```

```
option          "fbdev"  "/dev/fb1"

        Option      "SwapbuffersWait" "true"
EndSection

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

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

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

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

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

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

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

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