Installation d’un serveur Linux sur un Raspberry

Stéphane Apiou

Version 1.0, 2020-03-27

Table of Contents

Chapter 1. Avant propos

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

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

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

Sont installés:

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

- un serveur de VPN Pritunl,

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

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

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

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

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

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

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

Chapter 2. Choix du registrar

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

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

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

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

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

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

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

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

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

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

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

Chapter 3. Installation du linux sur votre raspberry.

C'est la première étape.

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

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

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

1. Loguez vous comme `root`
2. Tapez:

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

3. Lancez le programme.

Suivez la procédure ci dessous commune à toutes les plateformes:

1. Sélectionnez `Choose OS` et dans la liste choisissez `Raspbian`
2. Sélectionnez `CHoose SD CARD` et sélectionnez votre lecteur de carte SD
3. Cliquez sur `Write`
4. Attendez la fin du chargement et de l'écriture sur la flash.
5. Enlevez la carte SD de votre lecteur et insèrez la dans votre raspberry PI.
6. Brancher un clavier, une souris et un écran (ou utilisez un écran 3,5" configuré selon la procédure en annexe).
7. Branchez votre Rasberry sur votre réseau ethernet filaire (vous pouvez aussi utiliser le wifi)
8. Démarrez votre raspberry.
9. Après l'écran de démarrage arc en ciel, vous devez assez rapidement arriver sur le bureau
10. Un programme doit se lancer automatiquement.
11. Sélectionnez le clavier et la langue en français
12. Tapez votre nouveau mot de passe root
13. Choisissez un full screen sans bords
14. Choississez votre connexion wifi et entrez le mot de passe
15. Bien noter votre adresse IP elle vous sera utile ensuite
16. Les mises à jours de paquets debian ainsi que l'installation des traductions en français vont

s’installer.

17. Une fois les installations terminées, le raspberry va rebooter.
18. 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`
19. Cliquez sur l’icone `VNC` dans la barre en haut à Droite
    - Dans la fenêtre cliquez sur le menu burger en haut à Droite.
    - Choisissez `Options` puis l’onglet `Sécurité`
    - Dans le champ Authentification choisissez l’option `mot de passe VNC`
    - Tapez votre mot de passe dans les deux champs et cliquez `Valider` puis `OK`
20. Vous pouvez maintenant rebooter votre raspberry sans écran et sans clavier pour continuer la configuration.
21. Vous avez deux options: connexion en mode SSH ou au travers d’une connection VNC

Chapter 4. Se loguer root sur le serveur

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

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

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

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

   ou utilisez putty si vous êtes sous Windows.

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

   ```
   sudo bash
   ```

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

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

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

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

      Tapez ensuite votre mot de passe root

Chapter 5. Configuration basique

5.1. Mettre l'éditeur de votre choix

En fonction de vos préférences en terme d'éditeur, choisissez celui qui vous convient.

Loguez vous comme `root` et tapez:

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

Pour les débutants, il est conseillé d'utiliser nano

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

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

Cette installation est optionnelle.

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

   ```
   apt update
   apt install etckeeper
   ```

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

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

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

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

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

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

```
PUSH_REMOTE="origin"
```

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

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

   b. Allez dans le répertoire. Tapez :

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

   c. Générez vous clés. Tapez :

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

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

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

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

8. Effectuez un premier push. Tapez:

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

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

```
etckeeper commit
```

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

5.3. Mise à jour des sources de paquets Debian

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

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

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

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

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

```
apt update
```

   b. Installez les nouveautés. Tapez:

```
apt dist-upgrade
```

4. Effectuez du ménage. Tapez:

```
apt autoremove
```

5.4. Installation des paquets de base

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

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

5.5. Installer l'outil Debfoster

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

Cette installation est optionnelle.

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

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

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

   ```
   apt install debfoster
   ```

3. Lancez `debfoster`. Tapez :

   ```
   debfoster
   ```

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

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

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

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

5.6. Création d'un fichier keeper dans /etc

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

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

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

3. Saisissez dans le fichier:

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

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

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


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

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

4. Sauvez et tapez:

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

5. Exécutez maintenant `etckeeper`

```
etckeeper commit
```

6. Le fichier keepers est créé et sauvegardé automatiquement.

5.7. Installation des mises à jours automatiques

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

Cette installation est optionnelle.

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

Tapez:

```
apt install unattended-upgrades
```

5.8. Vérification du nom de serveur

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

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

   ```
   cat /etc/hostname
   ```

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

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

      ```
      vi /etc/hostname
      ```

      Changez la valeur, sauvegardez et rebootez. Tapez :

      ```
      reboot
      ```

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

   ```
   cat /etc/hosts
   ```

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

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

      ```
      vi /etc/hosts
      ```

   b. Changez la ou les lignes, sauvegardez.

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

c. Rebootez. Tapez :

```
reboot
```

d. Loguez vous comme `root` sur le serveur

4. Vérifiez que tout est correctement configuré.

a. Tapez :

```
hostname
```

La sortie doit afficher le nom de host.

b. Tapez ensuite :

```
hostname -f
```

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

5.9. Interdire le login direct en root

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

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

a. Tapez :

```
adduser <sudo_username>
```

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

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

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

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

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

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

e. une fois logué, tapez:

```
sudo bash
```

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

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

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

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

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

```
PermitRootLogin no
```

   b. Redémarrez le serveur ssh. Tapez :

```
service sshd restart
```

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

```
ssh root@<example.com> ①
```

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

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

5.10. Création d'une clé de connexion ssh locale

Pour créer une clé et la déployer:

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

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

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

c. Allez dans le répertoire. Tapez :

```
cd ~/.ssh
```

d. Générez vous clés. Tapez :

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

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

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

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

3. Déployez votre clé:

a. Loguez vous sur votre serveur distant. Tapez :

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

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

Entrez votre mot de passe

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

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

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

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

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

d. Sécurisez votre fichier de clés. Tapez: :

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

e. Sécurisez le répertoire SSH; Tapez :

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

f. Déconnectez vous de votre session

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

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

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

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

5.11. Sudo sans mot de passe

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

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

```
addgroup --system sudonp
```

a. Ajouter l'utilisateur: :

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

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

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

c. Éditez le fichier sudoers. Tapez :

```
vi /etc/sudoers
```

d. Ajouter dans le fichier la ligne suivante:

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

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

5.12. Installer l'outil dselect

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

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

```
apt install dselect
```

5.13. Ajouter un fichier de swap

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

Tapez :

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

```
dphys-swapfile uninstall
```

3. Tapez:

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

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

```
vi /etc/fstab
```

5. Ajoutez la ligne:

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

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

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

7. Ajoutez ou modifiez la ligne:

```
vm.swappiness = 5
```

8. Le paramètre sera actif au prochain reboot

Chapter 6. Installation initiale des outils

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

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

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

   ```
   dpkg-reconfigure dash
   ```

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

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

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

   b. Pour les systèmes avec plus de mémoire tapez :

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

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

6.1. Configuration de Postfix

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

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

2. Ajoutez dans le fichier:

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

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

3. Sauvegardez et relancez Postfix:

```
systemctl restart postfix
```

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

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

6.2. Configuration de MariaDB

1. Sécurisez votre installation MariaDB. Tapez :

```
mysql_secure_installation
```

Répondez au questions ainsi:

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

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

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

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

4. Commentez la ligne `bind-address`:

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

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

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

6. Editez le fichier debian.cnf. Tapez :

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

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

```
password = votre_mot_de_passe
```

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

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

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

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

8. Créez ensuite un nouveau répertoire. Tapez:

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

a. Editer le fichier limits.conf. :

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

b. Ajoutez dans le fichier les lignes suivantes:

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

9. Redémarrez votre serveur MariaDB. Tapez: :

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

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

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

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

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

6.3. Configuration d'Apache

1. Installez les modules Apache nécessaires. Tapez :

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

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

a. Éditez le fichier httpoxy.conf: :

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

b. Collez les lignes suivantes:

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

3. Activez le module en tapant :

```
a2enconf httpoxy
systemctl restart apache2
```

4. Désactiver la documentation apache en tapant:

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

6.4. Installation et Configuration de Mailman

1. Tapez :

```
apt-get install mailman
```

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

```
newlist mailman
```

4. ensuite éditez le fichier aliases: :

```
vi /etc/aliases
```

   et ajoutez les lignes affichées à l'écran:

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

5. Exécutez :

```
newaliases
```

et redémarrez postfix: :

```
systemctl restart postfix
```

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

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

7. Redémarrez apache :

```
systemctl restart apache2
```

puis redémarrez le demon mailman :

```
systemctl restart mailman
```

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

6.5. Configuration d' Awstats

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

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

Et commentez toutes les lignes:

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

6.6. Configuration de Fail2ban

1. Editez le fichier jail.local :

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

Ajoutez les lignes suivantes:

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

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

2. Redémarrez Fail2ban: :

```
systemctl restart fail2ban
```

6.7. Installation et configuration de PureFTPd

1. Tapez: :

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

2. Éditez le fichier de conf: :

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

3. Changez les lignes ainsi:

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

4. Autorisez les connexions TLS. Tapez:

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

5. Créez un certificat SSL.
   a. Tapez :

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

   b. Puis créez le certificat auto signé. Tapez :

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

   et répondez aux questions de la manière suivante:

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

c. Puis tapez :

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

d. et redémarrez pure-ftpd en tapant: :

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

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

- Installez les paquets de gestion des quotas. Tapez:

```
apt install quota quotatool
```

- Editez `fstab`. Tapez:

```
vi /etc/fstab
```

- Inserez le texte ci dessous pour chaque directive de montage

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

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

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

- Ajoutez avant `exit 0`:

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

- Pour activer les quotas, tapez:

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

6.8. Annexe

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

6.9.1. Pour commencer

Le RPi LCD peut être piloté de deux manières :

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

   ```
   sudo raspi-config
   ```

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

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

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

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

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

6.9.2. Basculer entre l'affichage LCD et HDMI

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

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

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

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

6.9.3. Paramètres d'orientation de l'écran

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

- Rotation de 0 degrés

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

- Rotation de 90 degrés

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

- Rotation de 180 degrés

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

- Rotation de 270 degrés

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

6.9.4. Calibrage de l'écran tactile

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

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

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

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

ou Sélectionnez Menu → Preferences → Calibrate Touchscreen.

Après l'exécution de ces commandes, l'écran LCD affiche une invite pour un calibrage en quatre

points. Cliquez sur les points un par un pour terminer le calibrage tactile. Ensuite, les nouvelles données de calibrage seront affichées dans le terminal, comme indiqué ci-dessous. Veuillez obtenir ces données pour une utilisation ultérieure.

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

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

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

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

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

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

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

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

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

```
sudo reboot
```

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

6.9.5. Installer un clavier virtuel

1. Installer matchbox-keyboard

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

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

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

3. Exécutez les commandes:

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

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

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

5. Exécutez les commandes ci dessous.

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

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

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

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

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

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

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

```
sudo reboot
```

6.9.6. Ressources

Manuel utilisateur

- RPiLCD User Manual

Images

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

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

Driver

Le pilote peut être téléchargé sur github

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

Fichiers de configuration de référence

/boot/cmdline.txt

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

/boot/config.txt

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

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

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

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

# uncomment to force a console size. By default it will be display's size minus
# overscan.
#framebuffer_width=1280
#framebuffer_height=720

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

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

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

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

# uncomment for composite PAL
#sdtv_mode=2

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

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

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

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

/etc/inittab

Ajouter:

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

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

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

        Option          "SwapbuffersWait" "true"
EndSection
```

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

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

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

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

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

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

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

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