

Jean-Louis Cech
390 descente des Princes des Baux
84100 Orange

09 81 88 04 18
06 59 71 48 37
jl.cech@free.fr

Orange : 7 mai 2014

Installation Serveur

Matériel vendu par :

R.C. Electronic

53 rue Victor Hugo

84100 Orange

info@rcelectronic.com

04 90 34 60 23

Table des matières

Configuration serveur.....	3
Liminaire Installation serveur.....	3
Version installée.....	3
Remarques sur l'écran TV HD.....	3
Remarques sur le partitionnement.....	3
Installation serveur.....	4
Services complémentaires.....	4
Personnalisation de l'arborescence.....	5
Restauration des données.....	5
Mise en place disque externe.....	5
Modification /etc/fstab.....	5
Modification de /etc/passwd.....	6
Compte root.....	6
Compte www-data.....	6
Compte jlc.....	6
Restauration des données.....	7
Récupération du backup.....	7
Site WEB.....	8
Comptes « root » et « jlc ».....	8
Service vsftp.....	9
Service samba.....	10
Services apache2 et php5.....	10
Service fail2ban.....	10
Service ssh.....	10
Vim.....	10

Configuration serveur

Référence serveur : DC3217IYE Intel (format Pont l'évêque)

Disque SSD 120 Go
4 Go RAM
Clavier / Souris USB wireless
Lecteur / Graveur de DVD amovible USB
Ecran TV HD via HDMI
Disque dur externe 2 To.USB

Cette configuration est choisie pour son absence de pièces en mouvement, ventilateur et disque dur, ainsi que pour son alimentation mono tension (18v) qui permet l'insertion d'un accumulateur tampon qui fera office d'alimentation secourue.

A l'usage, l'interface audio-video HDMI rend cette machine idéale pour une utilisation multimedia.

Liminaire Installation serveur

Avant toute installation, mettre hors service le disque externe de sauvegarde et multimedia.

Remarque sur les conceptions typographiques :

Les commandes à passer au clavier sont affichées en gras, cadrées gauche, par exemple :

```
sudo vi /etc/vstpd.conf
```

Version installée

KDE Ubuntu 14.04 LTS

Seule quelques ajustements des fichiers de configuration seront à appliquer, service par service. Ces ajustements sont décrits, service par service, plus bas.

Remarques sur l'écran TV HD

Le serveur est connecté sur une TV HD Panasonic via une interface HDMI. Si globalement l'image est de qualité satisfaisante, en particulier en ce qui concerne le centre de l'écran, le pourtour déborde et n'est donc pas une IHM idéale (Interface Homme Machine) même si le pointeur de la souris peut s'y déplacer librement et pointer les icônes et commandes.

Pour information, aucun des réglages disponibles par le menu de la TV HD ne permet de visualiser l'intégralité de l'écran.

Remarques sur le partitionnement

Le partitionnement du SSD provoque des erreurs en fin d'installation. Les raisons de ce plantage ne sont pas explicites, il convient de laisser le processus d'installation utiliser la

totalité de l'espace à sa convenance et ne pas tenter d'utiliser un mode de partitionnement manuel.

Installation serveur

Attention : pour tout ce qui suit, les commandes sont passées par le terminal.

Rien de particulier à signaler, l'installation se déroule sans soucis majeurs.

Attention : l'utilisateur principal est identifié par « jlc » qui est défini lors de l'installation. Dans un premier temps il sera le seul « sudoer ».

Il reste à installer les services complémentaires et préparer l'arborescence pour la bonne exécution des scripts spécifiques.

Pour optimiser l'IHM, créer un alias du terminal sur le bureau, les accès au menu démarrer, sur ma TV HD Panasonic, sont hors écran. L'ensemble de la configuration sera faite par des commandes sous terminal.

Une fois l'installation terminée affecter à l'interface LAN les paramètres suivants :

Adresse IP fixe : 192.168.1.22
Masque réseau : 255.255.255.0
Adresse DNS : 208.67.222.222 (ici le DNS Open Source)
Nom machine : piccolo

Services complémentaires

Par la commande

apt-get install « service »

installer les services suivants :

- ssh
- vim
- vsftp
- samba
- apache2
- php5
- fail2ban

Personnalisation de l'arborescence

En tant que « root » créer les répertoires suivants :

```
/mnt/nas  
/mnt/bu  
/mnt/restore
```

Appliquer les droits suivants aux répertoires ainsi créés :

```
chown www-data:users mnt/nas  
chmod 775 /mnt/nas
```

Restauration des données

Mise en place disque externe

Le disque USB externe est reconnu directement par le système, ses deux partitions sont référencée sous les « devices » suivants :

```
/dev/sdb1 pour la partition de multimedia  
/dev/sdb2 pour la partition de sauvegarde.
```

Modification /etc/fstab

Modifier /etc/fstab en ajoutant les lignes suivantes

```
/dev/sdb1 /mnt/nas auto rw 0 0  
/dev/sdb2 /mnt/bu auto rw 0 0
```

puis pour activer le montage « multimedia » passer

```
mount -a
```

Une fois cette commande passée, les deux partitions sont montées et utilisables. On le vérifie par la commande

```
df
```

qui doit fournir l'affichage suivant :

Sys. de fichiers	blocks de 1K	Utilisé	Disponible	Uti%	Monté sur
/dev/sda1	111219488	20904448	84642288	20%	/
none	4	0	4	0%	/sys/fs/cgroup
udev	1962636	4	1962632	1%	/dev
tmpfs	394676	2276	392400	1%	/run
none	5120	4	5116	1%	/run/lock
none	1973376	220	1973156	1%	/run/shm
none	102400	36	102364	1%	/run/user
/dev/sdb1	1031992064	129890116	849673148	14%	/mnt/nas
/dev/sdb2	890605628	191765028	653593724	23%	/mnt/bu

Modification de /etc/passwd

Compte root

Afin de rendre « root » utilisable en tant que compte d'administration, passer la commande

```
passwd root
```

pour lui affecter un mot de passe.

Compte www-data

Dans le répertoire /home créer

```
mkdir /home/webedit
```

et l'assigner à

```
chmod 750 /home/www-data
```

```
chown www-data:users /home/webedit
```

Dans le fichier /etc/passwd

L'éditer et modifier ses paramètres de www-data comme suit

```
www-data:x:33:33:www-data:/home/webedit:/bin/bash
```

Créer le mot de passe associé à www-data

```
passwd www-data
```

et assigner le mot de passe.

Dans le répertoire /home/webedit créer le lien symbolique vers le site Web en tant que www-data

```
su www-data
```

```
ln -s /var/www/html www
```

Le compte système www-data devient un utilisateur « standard » ce qui permet d'utiliser des logiciels de création de sites web via des accès FTP protégés par les couples mdp (Mots de passe) ID.

Compte jlc

Modifier le groupe de « jlc » en users en modifiant le groupe de 1000 en 100 dans /etc/passwd la ligne de jlc.

Restauration des données

Les opérations suivantes se font en tant que « root »

Récupération du backup

Toutes les commandes de la récupération des fichiers se fait en tant que root.

Créer le répertoire d'accroche /mnt/bu qui servira aussi ensuite au opérations de sauvegarde automatiques.

Si /dev/sdb2 n'est pas montée dans /mnt/bu monter la partition de backup par

```
mount /dev/sdb2 /mnt/bu
```

Dans ce qui suit le préfixe 5.tar est donné à titre d'exemple.

Créer le répertoire /mnt/restore qui servira aux opération de restauration des fichiers.

Copier la sauvegarde choisie dans /mnt/restore :

```
cp /mnt/bu/daily/5.tar.gz /mnt/restore
```

Puis passer les commandes suivantes

```
cd /mnt/restore
```

```
gunzip 5.tar.gz
```

```
tar -xvzf 5.tar
```

Vérifier que les fichiers dans /mnt/restore sont utilisables et disponibles.

Site WEB

Via un poste extérieur vérifier que le serveur apache fonctionne.

Attention :

- la nouvelle version d'Apache2 autorise en natif l'exécution de serveurs virtuels, la racine des sites est déplacée dans `/var/www/html`
- Les scripts qui modifient les fichiers du site web en automatique doivent prendre en compte cette organisation. Par exemple les fichiers de log visualisés dans le site à l'adresse publique <http://cech.fr/log> qui se trouvaient en `/var/www/log/` sont désormais en `/var/www/html/log/`

Supprimer le fichier `index.html` par défaut par

```
rm /var/www/html/index.html
```

Copier le site par

```
cp -Rp /mnt/restore/www/* /var/www/html/
```

Relancer le navigateur sur <http://cech.fr> le site devrait apparaître.

Dans la partie supérieure de la page d'accueil, si la date est correctement affichée, la fonction « PHP » du serveur web est présumée fonctionner correctement.

Comptes « root » et « jlc »

Copier dans leur répertoires respectifs depuis `/mnt/restore` les données de `root` et `jlc` en préservant les attributs par

```
cp -Rp /mnt/restore/root/* /root/
```

et

```
cp -Rp /mnt/restore/home/jlc/* /home/jlc/
```

Relancer les action de scheduleur des deux comptes pour chacun par

```
su root
```

```
crontab /root/admin/schedule
```

```
su jlc
```

```
crontab /home/jlc/admin/schedule
```

et vérifier leur bonne initialisation pour chacun des deux comptes par

```
crontab -l
```


Service vsftpd

Le fichier de configuration par défaut ne permet pas l'écriture, il faudra l'adapter tout en préservant le fichier original.

L'ensemble des commandes suivantes sont passées en tant que root :

```
mv /etc/vsftpd.conf /root/admin/vsftpd.original
```

```
cat /root/admion/vsftpd.original | grep -v '#' > /etc/vsftpd.conf
```

Y ajouter les deux lignes suivantes :

```
write_enable=YES
```

```
xferlog_file=/var/log/auth.log
```

Relancer vsftpd.

Attention : le service vsftpd se comporte de façon particulière, pour le relancer il faut simplement le tuer par un « kill ». La séquence suivante est une capture d'écran, le process à tuer est le 16735, ce numéro ne vaut que pour cet exemple.

```
root@picolo:~# ps -ef | grep ftp
root  16735 1      0 mai06 ?          00:00:00 /usr/sbin/vsftpd
root  23228 23203 0 10:07 pts/14    00:00:00 grep --color=auto ftp
root@picolo:~# kill 16735
```

Vérifier que vsftpd est automatiquement relancé avec un nouveau numéro de process

```
root@picolo:~# ps -ef | grep ftp
root  23232      1 0 10:08 ?          00:00:00 /usr/sbin/vsftpd
root  23235 23203 0 10:08 pts/14    00:00:00 grep --color=auto ftp
```

Le process est changé, la nouvelle configuration de /ect/vsftpd.conf est bien prise en compte avec les paramètres suivants :

```
listen=YES
anonymous_enable=NO
local_enable=YES
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
#
# Ajout
write_enable=YES
xferlog_file=/var/log/auth.log
```

Service samba

Remplacer le fichier de configuration smb.conf par le fichier de sauvegarde :

```
cp -p /mnt/restote/etc/samba/smb.conf /etc/samba/
```

Relancer le service par :

```
service samba restart
```

Créer le premier compte :

```
smbpasswd -a jlc
```

et lui assigner le mot de passe.

Services apache2 et php5

Les services apache2 et php5 devraient fonctionner sans aucune adaptation.

Service fail2ban

Modifier /etc/fail2ban/jail.conf et relancer.

Service ssh

Fonctionne sans adaptation.

Lors de la première connexion, il est normal qu'un message d'erreur signale que la signature n'est pas conforme. Dans ce cas il faut modifier sur le poste client la liste des serveurs ssh autorisés.

Vim

Rien à paramétrer.