LXD – Apache – multi PHP – ISPconfig

Référence: Ubuntu 22.04 – PHP 8.1 et 7.4

Instructions de configuration du conteneur lxd: lxdvm-ns1

Ce Howto est la suite du tuto: LXD – Configuration de l'hôte et conteneur

> *Cette portion du howto est une traduction et adaptation de: howtoforge_perfect-server-ubuntu-20.04-apache2-php-mariadb-pureftpd-bind-dovecot-ispconfig-3*

Les commandes de ce tutoriel doivent être exécutées avec les permissions root. Ceci évite d'ajouter sudo devant chacune des commandes. Pour devenir root taper:

`sudo -s`

Déactiver cloud-init:
`touch /etc/cloud/cloud-init.disabled`
`nano /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg`

```
network: {config: disabled}
```

Ubuntu 22.04 a configuré notre système de façon à utiliser DHCP. Il nous faut donc modifier celui-ci afin d'utiliser une adresse IP statique.

sur lxdvm-ns1, configurer le réseau avec une adresse IP fixe:

`ls /etc/netplan`

```
>50-cloud-init.yaml
```

`nano /etc/netplan/50-static-public-ip.yaml`

```
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.0.4/24]
      nameservers:
        addresses:
          - 192.168.0.6
          - 208.67.220.220
      routes:
        - to: default
          via: 192.168.0.1
```

Appliquer les changements

`netplan apply`

Vérifier le résultat des modifications:

`ip addr show dev eth0`

```
5: eth0@if3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
group default qlen 1000
link/ether 00:16:3e:34:df:eb brd ff:ff:ff:ff:ff:ff link-netnsid 0
inet 192.168.0.4/24 brd 192.168.0.255 scope global eth0
valid_lft forever preferred_lft forever
inet6 fe80::216:3eff:fe34:dfeb/64 scope link
valid_lft forever preferred_lft forever
```

`nano /etc/hosts`

```
127.0.0.1 localhost
192.168.0.4 lxdvm-ns1.infolaf.ca lxdvm-ns1

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

`echo lxdvm-ns1 > /etc/hostname`
`hostname lxdvm-ns1`

`hostname`
`hostname -f`

Voici la sortie des deux commandes précédentes:

```
root@lxdvm-ns1:/home/infolaf# hostname
lxdvm-ns1
root@lxdvm-ns1:/home/infolaf# hostname -f
lxdvm-ns1.infolaf.ca
```

Modifier /etc/apt/sources.list. Mettre en commentaires l'utilisation du CD et s'assurer que les dépôts universe et multiverse sont activés. Voici l'allure attendue après les modifications:

`nano /etc/apt/sources.list`

```
deb http://archive.ubuntu.com/ubuntu jammy-updates universe
deb http://archive.ubuntu.com/ubuntu jammy-updates multiverse
```

`apt update`
`apt full-upgrade`
`reboot`

3. Modifier l’interpréteur de commande par défaut.

/bin/sh est un lien symbolique vers /bin/dash, mais nous souhaitons plutôt /bin/bash, et non pas /bin/dash. Donc lancer la commande suivante:

`dpkg-reconfigure dash`

```
Use dash as the default system shell (/bin/sh)? <-- No
```

```
Removing 'diversion of /bin/sh to /bin/sh.distrib by dash'
Adding 'diversion of /bin/sh to /bin/sh.distrib by bash'
Removing 'diversion of /usr/share/man/man1/sh.1.gz to
/usr/share/man/man1/sh.distrib.1.gz by dash'
Adding 'diversion of /usr/share/man/man1/sh.1.gz to
/usr/share/man/man1/sh.distrib.1.gz by bash'
```

Si cette étape n’est pas respectée, l’installation de ISPConfig échoura.

4. Désactiver AppArmor

`service apparmor stop`
`update-rc.d -f apparmor remove`
`apt remove apparmor apparmor-utils`

5. Synchroniser l’horloge système

`apt -y install ntp`

6. Installation de Postfix, Dovecot, MariaDB, rkhunter et binutils

Afin d’installer postfix, nous devons être certain que sendmail n’est pas installé et fonctionnel. Pour arrêter et retirer sendmail, exécuter cette commande:

`service sendmail stop; update-rc.d -f sendmail remove`

Le message d’erreur:

```
Failed to stop sendmail.service: Unit sendmail.service not loaded.
```

est normal, celui-ci indique simplement que sendmail n'était pas installé et qu'il n'y a donc rien à retirer.

Installons Postfix, Dovecot, MariaDB (remplace MySQL), rkhunter, et binutils:

```
apt -y install postfix postfix-mysql postfix-doc mariadb-client mariadb-server
openssl getmail6 rkhunter binutils dovecot-imapd dovecot-pop3d dovecot-mysql
dovecot-sieve sudo patch
```

Les questions suivantes seront posées:

```
General type of mail configuration: <-- Internet Site
System mail name: <-- lxdvm-ns1.infolaf.ca
```

Il est important d'utiliser un sous domaine comme « system mail name » tel que server1.example.com ou server1.yourdomain.com et non pas un domaine qui sera utilisé comme domaine de courriel (c.à.d. yourdomain.tld) dans une étape ultérieure.

Ensuite, ouvrons les ports (submission ports) requis pour les connexion SSL-TLS dans Postfix:

```
nano /etc/postfix/master.cf
```

Décommenter les sections submission et smtps telle qu'indiquée et ajouter la

ligne suivante aux deux sections et laisser tout le reste en commentaires.

```
 -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

```
[...]
submission inet n - y - - smtpd
-o syslog_name=postfix/submission
-o smtpd_tls_security_level=encrypt
-o smtpd_sasl_auth_enable=yes
-o smtpd_tls_auth_only=yes
-o smtpd_client_restrictions=permit_sasl_authenticated,reject
# -o smtpd_reject_unlisted_recipient=no
# -o smtpd_client_restrictions=$mua_client_restrictions
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
# -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
smtps inet n - y - - smtpd
-o syslog_name=postfix/smtps
-o smtpd_tls_wrappermode=yes
-o smtpd_sasl_auth_enable=yes
-o smtpd_client_restrictions=permit_sasl_authenticated,reject
# -o smtpd_reject_unlisted_recipient=no
# -o smtpd_client_restrictions=$mua_client_restrictions
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
# -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
[...]
```

NOTE: L’absence d’espaces vides devant les lignes « -o …. » est important!

Redémarrage de Postfix suite aux modifications:

`service postfix restart`

MySQL doit être à l’écoute de toutes les interfaces, pas seulement localhost. En conséquence, éditons /etc/mysql/mariadb.conf.d/50-server.cnf et commenter la

ligne bind-address = 127.0.0.1:

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

```
[...]
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address = 127.0.0.1

[...]
```

La méthode d'authentification est maintenant différente pour MariaDB. Il n'y a plus de mot de passe root et donc pas de sécurisation à effectuer lors de l'installation comme au paravant.

ISPconfig requiert un utilisateur et un mot de passe pour MariaDB lors de l'installation.

Définir la méthode d'authentification par mot de passe (password authentication method) pour MariaDB à native ainsi, nous pourrons plus tard utiliser ISPconfig et PHPMyAdmin pour se connecter comme utilisateur root:

`mysql`
`ALTER USER root@localhost IDENTIFIED VIA mysql_native_password USING PASSWORD("votremotdepasse");`
`\q`

Normalement mySQL refusera la connection:
`mysql`

Normalement mySQL acceptera la connection:
`mysql -pvotremotdepasse`

Ouvrir le fichier /etc/security/limits.conf avec l'éditeur nano:

`nano /etc/security/limits.conf`

Ajouter les lignes suivantes à la fin du fichier.

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

Ensuite, créer un nouveau répertoire /etc/systemd/system/mysql.service.d/

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

Créer un nouveau fichier dans ce répertoire:

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

copier les lignes suivantes dans ce fichier:

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

Enregistrer et fermer l'éditeur nano.

Ajouter des paramètres à my.cnf
`nano /etc/mysql/my.cnf`

```
max_allowed_packet = 128M

[mysqld]
wait_timeout = 86400
interactive_timeout = 86400
innodb_log_file_size = 128MB
```

Rechargeons systemd et effectuons un redémarrage de MariaDB:

`systemctl daemon-reload`
`service mariadb restart`

Vérifions que la connexion réseau pour MySQL est bien active avec la commande suivante:

`netstat -tap | grep mysql`

La sortie de cette commande doit ressembler à ceci:

```
tcp 0 0 0.0.0.0:mysql 0.0.0.0:* LISTEN 234/mariadbd
tcp6 0 0 [::]:mysql [::]:* LISTEN 234/mariadbd
```

7. Installation de Amavisd-new, SpamAssassin et Clamav

```
apt -y install amavisd-new spamassassin clamav clamav-daemon unzip bzip2 arj
nomarch lzop cabextract apt-listchanges libnet-ldap-perl libauthen-sasl-perl
clamav-docs daemon libio-string-perl libio-socket-ssl-perl libnet-ident-perl zip
libnet-dns-perl postgrey
```

Lors de l'installation d'ISPConfig 3, amavisd est installé et les librairies de filtres de SpamAssassin sont alors chargées, nous pouvons donc arrêter SpamAssassin pour libérer un peu de RAM:

`service spamassassin stop`
`update-rc.d -f spamassassin remove`

Démarrer ClamAV:

`freshclam`
`service clamav-daemon start`

Cette erreur peut être ignorée lors du premier démarrage de freshclam.

```
ERROR: /var/log/clamav/freshclam.log is locked by another process
ERROR: Problem with internal logger (UpdateLogFile =
/var/log/clamav/freshclam.log).
```

8. Installation d’Apache, PHP, phpMyAdmin, FCGI, SuExec, Pear

Apache 2, PHP 8.1, PHP 7.4, phpMyAdmin, FCGI, suExec et Pear sont intallés comme suit:

Ajouter le dépôt pour avoir accès à PHP 7.4 ainsi que des mises à jour pour PHP 8.1

`sudo add-apt-repository ppa:ondrej/php`

`sudo apt update`

`sudo apt full-upgrade`

```
apt -y install apache2 apache2-doc apache2-utils libapache2-mod-php php8.1
php8.1-common php8.1-gd php8.1-mysql php8.1-imap phpmyadmin php8.1-cli php8.1-cgi
libapache2-mod-fcgid apache2-suexec-pristine php-pear libruby libapache2-mod-
python php8.1-curl php8.1-intl php8.1-pspell php8.1-sqlite3 php8.1-tidy php8.1-
xmlrpc php8.1-xsl memcached php-memcache php-imagick php8.1-zip php8.1-mbstring
php-soap php8.1-soap php8.1-opcache php-apcu php8.1-fpm libapache2-reload-perl
```

```
apt -y install php7.4 php7.4-cli php7.4-cgi php7.4-fpm php7.4-gd php7.4-mysql
php7.4-imap php7.4-curl php7.4-intl php7.4-pspell php7.4-sqlite3 php7.4-tidy
php7.4-xmlrpc php7.4-xsl php7.4-zip php7.4-mbstring php7.4-soap php7.4-opcache
php7.4-common php7.4-json php7.4-readline php7.4-xml
```

Répondre aux questions suivantes:

```
Web server to reconfigure automatically: <-- apache2
Configure database for phpmyadmin with dbconfig-common? <-- Yes
MySQL application password for phpmyadmin: <-- Press enter
Password of the database's administrative user: <-- root mysql password
```

Afin d’être en mesure d’importer de grosses tables dans phpmyadmin, il faut faire les ajustements suivants au fichier php.in

`sudo nano /etc/php/8.1/apache2/php.ini`

```
;;;;;;;;;;;;;;;;;;;
; Resource Limits ;
```

```
;;;;;;;;;;;;;;;;;;
memory_limit = 512M

;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;

upload_max_filesize = 10G
post_max_size = 10G
```

Il faut aussi modifier cette configuration pour PHP-FPM 7.4
`sudo nano /etc/php/7.4/fpm/php.ini`

```
;;;;;;;;;;;;;;;;;;
; Resource Limits ;
;;;;;;;;;;;;;;;;;;
memory_limit = 512M

;;;;;;;;;;;;;;;;
; File Uploads ;
;;;;;;;;;;;;;;;;

upload_max_filesize = 10G
post_max_size = 10G
```

`restart php7.4-fpm.service`
`restart php8.1-fpm.service`

Vérier que PHP 8.1 est bien la version qui tourne par défaut pour Apache:
`php --version`

```
Copyright (c) The PHP Group
Zend Engine v4.1.2, Copyright (c) Zend Technologies
    with Zend OPcache v8.1.2-1ubuntu2.9, Copyright (c), by Zend Technologies
```

Si requis ajuster PHP 8.1 comme version par défaut:

```
update-alternatives --config php
update-alternatives --config php-cgi
update-alternatives --config php-fpm.sock
systemctl restart apache2.service
```

Vérifier les versions PHP disponible sur le système
`ls -al /etc/php`

```
total 11
drwxr-xr-x   4 root root   4 déc 21 21:22 .
drwxr-xr-x 130 root root 242 déc 21 19:26 ..
drwxr-xr-x   6 root root   6 déc 21 21:22 7.4
drwxr-xr-x   7 root root   7 déc 20 16:04 8.1
```

Vérifier les versions PHP actives sur le système
`ls -al /run/php`

```
total 8
drwxr-xr-x  2 www-data www-data 140 déc 22 15:03 .
drwxr-xr-x 31 root     root     920 déc 22 12:01 ..
-rw-r--r--  1 root     root       6 déc 22 15:03 php7.4-fpm.pid
srw-rw----  1 www-data www-data   0 déc 22 15:03 php7.4-fpm.sock
-rw-r--r--  1 root     root       3 déc 21 21:29 php8.1-fpm.pid
srw-rw----  1 www-data www-data   0 déc 21 19:57 php8.1-fpm.sock
lrwxrwxrwx  1 root     root      30 déc 21 19:57 php-fpm.sock ->
/etc/alternatives/php-fpm.sock
```

C’est possible de vérifier que PHPMyAdmin est fonctionnel:

http://192.168.0.4/phpmyadmin/

Exécuter les commandes suivantes pour activer les modules Apache: suexec, rewrite, ssl, actions et include (plus dav, dav_fs et auth_digest si vous désirez utiliser WebDAV):

`a2enmod suexec rewrite ssl actions include cgi alias proxy_fcgi`

`a2enmod dav_fs dav auth_digest headers`

Pour s'assurer que le serveur ne puisse pas être attaqué via la vulnerabilité HTTPOXY, désactiver globalement l'entête HTTP_PROXY dans apache. Créer un nouveau fichier httpoxy.conf file avec nano:

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

Coller les lignes suivantes ans le fichier:

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

Activer le fichier de configuration:

`a2enconf httpoxy`

Redémarrer Apache:

`service apache2 restart`

Si vous voulez héberger sur vos sites crées avec ISPConfig, des fichiers Ruby avec l'extension .rb, vous devez mettre en commentaire la ligne application/x-ruby rb in /etc/mime.types:

`nano /etc/mime.types`

```
[...]
#application/x-ruby rb
[...]
```

(Ceci n'est requis que pour les fichiers .rb; Les fichiers Ruby avec l'extension .rbx fonctionnent « out of the box ».)

Redémarrer Apache:

```
service apache2 restart
```

9. Installation de Let’s Encrypt

ISPConfig 3.2 supporte nativement la création de certificat SSL gratuit « Certificate Authority Let’s encrypt ». La fonction de création Let’s Encrypt vous permet de générer vos certificats SSL gratuits pour vos sites web directement dans ISPConfig.

Ajoutons le support pour Let’s encrypt.

```
apt install certbot
```

10. Mailman pas requis dans ce projet

11. Installation de PureFTPd

PureFTPd et quota peuvent être installés avec la commande suivante:

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

Édition du fichier /etc/default/pure-ftpd-common…

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

… vérifier que mode de démarrage est ajusté sur « standalone » et ajusté VIRTUALCHROOT=true:

```
[...]
STANDALONE_OR_INETD=standalone
[...]
VIRTUALCHROOT=true
[...]
```

Configurons PureFTPd pour permettre les sessions FTP et TLS. FTP est un protocol vraiment non sécuritaire parce que tous les mots de passe et données sont transférés en texte clair. En utilisant plutôt TLS, l’ensemble des

communications sont cryptées et donc beaucoup plus sécuritaire.

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

Pour permettre l'utilisation de TLS, nous devons créer un certificat SSL. Le certificat sera créé dans le répertoire /etc/ssl/private/, donc il faut au préalable créer celui-ci:

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

Ensuite, la création du certificat SSL:

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

```
Country Name (2 letter code) [AU]:CA
State or Province Name (full name) [Some-State]:QC
Locality Name (eg, city) []:Lachine
Organization Name (eg, company) [Internet Widgits Pty Ltd]:infolaf
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:lxdvm-ns1.infolaf.ca
Email Address []:postmaster@infolaf.ca
```

Modification des permissions du certificat SSL:

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

Re-démarrage de PureFTPd:

```
service pure-ftpd-mysql restart
```

12. Installation de BIND DNS Server

BIND sera installé comme suit:

```
apt -y install bind9 dnsutils haveged
```

Activer et démarrer le service haveged:

```
systemctl enable haveged
systemctl start haveged
```

13. Installation de Vlogger, Webalizer, AWStats et GoAccess

Vlogger, Webalizer, and AWStats seront installés comme suit:

```
apt -y install vlogger webalizer awstats geoip-database libclass-dbi-mysql-perl
```

Installer la version la plus récente de GoAccess directement de son dépot:

```
echo "deb https://deb.goaccess.io/ $(lsb_release -cs) main" | sudo tee -a
/etc/apt/sources.list.d/goaccess.list
wget -O - https://deb.goaccess.io/gnugpg.key | sudo apt-key --keyring
/etc/apt/trusted.gpg.d/goaccess.gpg add -
sudo apt update
sudo apt install goaccess
```

Ouvrir ensuite /etc/cron.d/awstats

```
nano /etc/cron.d/awstats
```

… mettre en commentaires l'ensemble des 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
```

14. Installation de Jailkit

Jailkit est utilisé par ISPConfig pour confiner le shell des utilisateurs et les cronjobs.

```
apt -y install jailkit
```

15. Installation de fail2ban et UFW

Ceci est optionel mais recommandé car ISPConfig monitor traite les logs:

`apt -y install fail2ban`

Afin que fail2ban observe les services PureFTPd et Dovecot, Créer le fichier /etc/fail2ban/jail.local:

`nano /etc/fail2ban/jail.local`

```
[pure-ftpd]
enabled = true
port = ftp
filter = pure-ftpd
logpath = /var/log/syslog
maxretry = 3

[dovecot]
enabled = true
filter = dovecot
action = iptables-multiport[name=dovecot-pop3imap, port="pop3,pop3s,imap,imaps",
protocol=tcp]
logpath = /var/log/mail.log
maxretry = 5

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

Redémarrer fail2ban:

`service fail2ban restart`

Pour l’installation du coupe-feu UFW, exécuter cette commande:

`apt-get install ufw`

16. Installation de Roundcube Webmail – Non requis dans ce projet

17. Installation de ISPConfig 3.2

Utilisons la version stable de ISPConfig 3.2

```
cd /tmp
wget -O ispconfig.tar.gz
https://www.ispconfig.org/downloads/ISPConfig-3-stable.tar.gz
tar xfz ispconfig.tar.gz
cd ispconfig3*/install/
```

L’étape suivante est d’éxécuter:

```
php -q install.php
```

Ceci va démarrer l’installation de ISPConfig 3. L’assistant d’installation va configurer pour vous tout les services comme Postfix, Dovecot, etc.

```
# php -q install.php

--------------------------------------------------------------------------------
_____ _____________ _____ __ _ ____
|_ _/ ___| ___ \ / __ \ / _(_) /__ \
| | \ `--.| |_/ / | / \/ ___ _ __ | |_ _ __ _ _/ /
| | `--. \ __/ | | / _ \| '_ \| _| |/ _` | |_ |
_| |_/\__/ / | | \__/\ (_) | | | | | | | (_| | ___\ \
\___/\____/\_| \____/\___/|_| |_|_| |_|\__, | \____/
__/ |
|___/
--------------------------------------------------------------------------------

>> Initial configuration

Operating System: Ubuntu 20.04.1 LTS (Focal Fossa)

Following will be a few questions for primary configuration so be careful.
Default values are in [brackets] and can be accepted with <ENTER>.
Tap in "quit" (without the quotes) to stop the installer.
```

```
Select language (en,de) [en]: <-- Hit Enter

Installation mode (standard,expert) [standard]: <-- Hit Enter

Full qualified hostname (FQDN) of the server, eg server1.domain.tld
[server1.canomi.com]: <-- Hit Enter

MySQL server hostname [localhost]: <-- Hit Enter

MySQL server port [3306]: <-- Hit Enter

MySQL root username [root]: <-- Hit Enter

MySQL root password []: <-- Enter your MySQL root password

MySQL database to create [dbispconfig]: <-- Hit Enter

MySQL charset [utf8]: <-- Hit Enter

Configuring Postgrey
Configuring Postfix
Generating a 4096 bit RSA private key
.....................................................................++
.....................................................................
.....................................................++
writing new private key to 'smtpd.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: <-- Enter 2 letter country code
State or Province Name (full name) [Some-State]: <-- Enter the name of the state
Locality Name (eg, city) []: <-- Enter your city
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter company
name or press enter
Organizational Unit Name (eg, section) []: <-- Hit Enter
Common Name (e.g. server FQDN or YOUR name) []: <-- Enter the server hostname, in
my case: server1.example.com
```

```
Email Address []: <-- Hit Enter
Configuring Mailman
Configuring Dovecot
Configuring Spamassassin
Configuring Amavisd
Configuring Getmail
Configuring BIND
Configuring Jailkit
Configuring Pureftpd
Configuring Apache
Configuring vlogger
Configuring Metronome XMPP Server
writing new private key to 'localhost.key'
-----
Country Name (2 letter code) [AU]: <-- Enter 2 letter country code
Locality Name (eg, city) []: <-- Enter your city
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter company
name or press enter
Organizational Unit Name (eg, section) []: <-- Hit Enter
Common Name (e.g. server FQDN or YOUR name) [server1.canomi.com]: <-- Enter the
server hostname, in my case: server1.example.com
Email Address []: <-- Hit Enter

Configuring Ubuntu Firewall
Configuring Fail2ban
[INFO] service OpenVZ not detected
Configuring Apps vhost
Installing ISPConfig
ISPConfig Port [8080]:

Admin password [admin]:

Do you want a secure (SSL) connection to the ISPConfig web interface (y,n) [y]:
<-- Hit Enter

Generating RSA private key, 4096 bit long modulus
.......................++
.....................................................................................
.............................................++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: <-- Enter 2 letter country code
State or Province Name (full name) [Some-State]: <-- Enter the name of the state
Locality Name (eg, city) []: <-- Enter your city
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter company
name or press enter
Organizational Unit Name (eg, section) []: <-- Hit Enter
Common Name (e.g. server FQDN or YOUR name) []: <-- Enter the server hostname, in
my case: server1.example.com
Email Address []: <-- Hit Enter

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: <-- Hit Enter
An optional company name []: <-- Hit Enter
writing RSA key

Symlink ISPConfig LE SSL certs to postfix? (y,n) [y]: <-- Hit Enter

Symlink ISPConfig LE SSL certs to pureftpd? Creating dhparam file takes some
times. (y,n) [y]: <-- Hit Enter

Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
.....................................................................+.....................
.....................................................................+.....
.....

Configuring DBServer
Installing ISPConfig crontab
no crontab for root
no crontab for getmail
Detect IP addresses
Restarting services ...
Installation completed.
```

Il n’y a aucune configuration manuelle à effectuer car l’assistant d’installation a effectuée toute les configurations automatiquement.

Vous pouvez dorénavent accéder à ISPConfig 3 à l’URL: http(s)://server1.example.com:8080/ ou http(s)://192.168.0.4:8080/ (HTTP ou HTTPS selon des choix effectués durant l’installation). Authentifiez-vous avec l’utilisateur « admin » en utilisant le mot de passe « admin » (vous devez changer le mot de passe par défaut une fois votre première connexion à ISPConfig):

Activer PHP versions dans ISPConfig

Dans l’interface d’ISPConfig 3, Il est possible de configurer une version additionelle de PHP sous l’onglet System > Additional PHP Versions.

Indiquer:

PHP Name:PHP 7.4

onglet FastCGI settings:

Path to the PHP FastCGI binary:php-cgi7.4
Path to the php.ini directory:/etc/php/7.4/cgi

onglet PHP-FPM settings:

Path to the PHP-FPM init script:php-cgi7.4
Path to the php.ini directory:/etc/php/7.4/fpm
Path to the PHP-FPM pool directory:/etc/php/7.4/fpm/pool.d
PHP-FPM socket directory: laissez vide

18. Installation de rsync sur lsdvm-ns1 afin d’assurer la sauvegarde des sites, fichiers de configuration.

Cette étape, vient compléter la première étape réalisé sur la machine physique qui héberge le conteneur

```
apt install rsync
```

`nano /etc/rsyncd.conf`

Sauvegarder et fermer

`cp /lib/systemd/system/rsync.service /etc/systemd/system/rsync.service`

Redémarrer le service.

`systemctl restart rsync`

`nano /etc/rsyncd.conf`

```
log file = /var/log/rsync.log

[cumulus]
uid = web1
gid = client1
path = /var/www/clients/client1/web1/web
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup cumulus.infolaf.net
read only = true
auth users = test
secrets file = /etc/rsyncd.scrt

[photos]
uid = web2
gid = client1
path = /var/www/clients/client1/web2/web
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup photos.infolaf.ca
read only = true
auth users = test
secrets file = /etc/rsyncd.scrt

[matomo]
uid = web3
gid = client1
path = /var/www/clients/client1/web3/web
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup matomo.infolaf.ca
```

```
read only = true
auth users = test
secrets file = /etc/rsyncd.scrt

[courriel]
uid = vmail
gid = vmail
path = /var/vmail
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup courriel
read only = true
auth users = test
secrets file = /etc/rsyncd.scrt

[mysql]
uid = infolaf
gid = infolaf
path = /home/infolaf/backups/mysql_DB
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup mysql
read only = true
auth users = test
secrets file = /etc/rsyncd.scrt

[scripts_NS1]
uid = infolaf
gid = infolaf
path = /home/infolaf/scripts/
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup scripts_NS1
read only = true
auth users = test
secrets file = /etc/rsyncd.scrt

[rsync_NS1]
uid = root
gid = root
path = /etc/
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup rsync_NS1
read only = true
auth users = test
```

```
secrets file = /etc/rsyncd.scrt

[bind_NS1]
uid = root
gid = root
path = /etc/bind
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup bind_NS1
read only = true
auth users = test
secrets file = /etc/rsyncd.scrt

[crontab_NS1]
uid = root
gid = root
path = /var/spool/cron/crontabs/
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup crontab_NS1
read only = true
auth users = test
secrets file = /etc/rsyncd.scrt

[www-full]
uid = root
gid = root
path = /var/www/
hosts allow = 192.168.0.11 #ici votre IP
comment = Backup full path of www disk
read only = true
auth users = test
secrets file = /etc/rsyncd.scrt
```

Le fichier secret /etc/rsyncd.scrt devra contenir dans cet exemple les permissions 640:

```
personne1:motdepasse1
personne2:motdepasse2
```

`nano /etc/rsyncd.scrt`

```
test:votremotdepasse
```

`chmod 640 /etc/rsyncd.scrt`

Vous pouvez maintenant lancer rsync:

`service rsync start`

Redevenir un utilisateur normal pour ne pas créer les fichiers suivants comme root

`exit`

`mkdir -p /home/infolaf/backups/mysql_DB`

`mkdir /home/infolaf/scripts/`

`nano /home/infolaf/scripts/backup_mysql.sh`

```
#mysql> -uroot -p<motdepasse> -e FLUSH TABLES WITH READ LOCK;
mysqldump -uroot -p<motdepasse> --databases c1photos >
/home/infolaf/backups/mysql_DB/c1photos.sql
mysqldump -uroot -p<motdepasse> --databases dbispconfig >
/home/infolaf/backups/mysql_DB/dbispconfig.sql
mysqldump -uroot -p<motdepasse> --databases c1matomo >
/home/infolaf/backups/mysql_DB/c1matomo.sql
mysqldump -uroot -p<motdepasse> --databases c1nextcloud >
/home/infolaf/backups/mysql_DB/c1nextcloud.sql
#mysql> -uroot -p<motdepasse> -e UNLOCK TABLES;

echo "Bonjour,"
echo ""
echo "Ce message vous confirme que les bases de donnees MySQL de vos sites web
sont bien sauvegardee localement dans ~/backups/mysql_DB/"
echo ""
echo "La sauvegarde sera complete lorsque host1 lancera son script de sauvegarde
des sites web"
echo ""
echo "Message produit par le script de sauvegarde execute par CRON sur
```

```
infolaf@192.168.0.4"

chmod 777 /home/infolaf/scripts/backup_mysql.sh
```

Nons n’avons pas à créer le fichier de mot de passe d’exécution automatique. Car rsync n’est pas lancer de lxdvm-ns1

et on ajoute les commandes suivantes dans crontab :

`crontab -e`

```
# m h dom mon dow command
MAILTO=root
00 00 * * 0-7 sh /home/infolaf/scripts/backup_mysql.sh
```