

# Serveur WEB ISPconfig – Ubuntu 14.04.1

Pré-requis:

[NAS – VirtualBox serveurs virtuels – Ubuntu 16.04.1](#)

Après avoir configuré votre machine physique (host1), vous êtes maintenant à l'étape d'assembler la machine virtuelle.

Vous avez donc réussie à lancer la machine virtuelle et vous y êtes connecté par l'application rdesktop ou par ssh.

*Cette portion du howto est une traduction et adaptation de: [howtoforge\\_perfect-server-ubuntu-14.04-apache2-php-mysql-pureftpd-bind-dovecot-ispconfig-3](#)*

À l'invite de l'assistant d'installation, appuyer sur ENTRER

```
Choisir la langue > Français  
Choisir le clavier > Canada
```

À la demande du lieu:

```
Choisir > Canada  
Choisir le nom de machine (à votre choix) > ns1
```

```
Choisir le disque souhaité > sda  
Choisir > partitionnement assisté
```

Le partitionnement assisté, déterminera les éléments suivants :

1. Partition primaire
2. Partition swap (2x la mémoire vive app.) probablement sda5
3. Point de montage racine (/) probablement sda1
4. Amorçable

Terminer le partitionnement pour ce disque.

Pour le disque de données (web et courriels)

On ne fait rien pour le moment

Fuseau horaire:

```
Choisir > Est Eastern
Usager et mots de passe:
Utilisateur > (à votre choix, noter et conserver)
Identifiant >
Mot de passe: (à votre choix, noter et conserver)
```

Installation des applications :

```
À la demande d'utiliser du proxy:
Choisir > pas de proxy
```

```
À la demande de sélection de logiciels:
Choisir > openSSH
```

Éjection du CD (automatique)

Redémarrage

---

Ubuntu a été installé avec les options décrite plus haut.

---

Donc voici les étapes à réaliser dans l'OS de la machine virtuelle (ns1)

Au redémarrage, il faut configurer notre autre disque dur :

- mail sera de 80G
- Web sera de 240G

Passer au compte super-utilisateur pour faire la configuration (exit pour en sortir)

```
sudo su
```

Changer la config du clavier si nécessaire:

```
apt-get install console-data
```

```
dpkg-reconfigure console-data
```

Si vous êtes connecté par rdesktop, il est préférable de se connecter en SSH pour pouvoir faire des Copier-coller plus aisément. Comme vous n'avez pas encore une IP fixe, il faut trouver avec quelle IP ns1 s'est connecter au réseau.

Trouver votre adresse ip :

```
ifconfig
```

```
ssh info1af@votreIP
```

```
mkfs -t ext4 /dev/sdb1
```

```
mkfs -t ext4 /dev/sdb2
```

Noter le numéro de blkid pour éditer le montage automatique des disques dans fstab

```
blkid
```

```
nano /etc/fstab
```

```
#Montage locaux des disques du serveur ns1
```

```
#/dev/sdb1 - Mail
```

```
UUID=b387ac6f-3607-4189-916a-b1d0b45531e2 /var/vmail ext4 defaults 0 2
```

```
#/dev/sdb2 - Web
```

```
UUID=fa35cd5c-2114-46ba-8a54-b11c2e653508 /var/www ext4 defaults 0 2
```

Il faut créer les répertoires de montages :

```
mkdir /var/vmail
```

```
mkdir /var/www
```

Monter les partitions avec le fichier /etc/fstab

```
mount -a
```

Créer des fichiers témoins sur les partitions montées :

```
touch /var/vmail/mount_ok-vmail
```

```
touch /var/www/mount_ok-www
```

Vérifier que les fichiers sont bien là :

```
ls /var/vmail
```

```
ls /var/www
```

Démonter les partitions :

```
umount /var/vmail /var/www
```

Vérifier qu'il n'y a plus rien dans le point de montage :

```
ls /var/vmail
```

```
ls /var/www
```

Remonter les partitions :

```
mount -a
```

---

Assemblage logiciel :

Nous avons besoin d'un serveur web, serveur DNS, serveur courriel et une base de données MySQL, mais je ne le installe pas maintenant afin d'avoir le plein contrôle lors de l'installation manuel.

Entre temps, simplement sélectionner server SSH. Ainsi il sera possible de continuer la configuration à partir d'une session SSH via un terminal.

Ubuntu 14.04LTS a configuré notre système de façon à utiliser DHCP pour obtenir les paramètres du réseau. Il nous faut donc modifier celui-ci afin d'utiliser une adresse IP statique.

Éditer `/etc/network/interfaces` et ajuster le contenu à vos besoins. (Dans cet exemple, j'utilise l'adresse IP 192.168.0.10) (S.V.P. noter que j'ai remplacé `allow-hotplug eth0` avec `auto eth0` ; autrement le redémarrage du réseau ne fonctionnera pas et nous devons alors redémarrer tout le système):

```
nano /etc/network/interfaces
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.0.10
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.1
#dns-nameservers 192.168.0.10 192.168.0.12
dns-nameservers
```

Redémarrer le réseau :

```
service networking restart
```

Éditer ensuite `/etc/hosts`

```
nano /etc/hosts
```

```
127.0.0.1 localhost
192.168.0.10 ns1.infolaf.net ns1

# The following lines are desirable for IPv6 capable hosts
::1
ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Exécuter :

```
echo ns1.infolaf.net > /etc/hostname
```

```
service hostname restart
```

ensuite :

```
hostname
```

```
hostname -f
```

Les deux commandes doivent retourner ns1.infolaf.net

Mise à jour du système Ubuntu:

Pour mettre à jour la base de données des mises à jours, exécuter :

```
apt-get update
```

Pour appliquer les mises à jour, exécuter :

```
apt-get upgrade
```

Redémarrer le système si un noyau a été installé.

bin/sh est un lien symbolique vers /bin/dash mais nous devons utiliser /bin/bash et non /bin/dash . Alors nous faisons ce qui suit :

```
dpkg-reconfigure dash
```

```
Use dash as the default system shell (/bin/sh)? <- no Si cela n'est pas fait,  
l'installation de ISPConfig échouera.
```

AppArmor est une extension de sécurité (semblable à SELinux) son rôle est d'améliorer la sécurité mais comme il cause souvent plus de problème qu'il n'en règle, nous allons le désactiver.

Procéder comme suit:

```
service apparmor stop
```

```
update-rc.d -f apparmor remove
```

```
apt-get remove apparmor apparmor-utils
```

Synchronisation de l'horloge système :

C'est une bonne idée de synchroniser l'horloge système avec un serveur NTP (network time protocol) via Internet. Exécuter :

```
apt-get install ntp ntpdate
```

ainsi votre système sera toujours en synchronisme.

Avant d'installer postfix, nous devons arrêter et enlever sendmail :

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

Installation de Postfix, Dovecot, MySQL, phpMyAdmin, rkhunter, binutils

```
apt-get install postfix postfix-mysql postfix-doc mysql-client mysql-server openssl  
getmail4 rkhunter binutils dovecot-imapd dovecot-pop3d dovecot-mysql dovecot-sieve  
sudo
```

Les questions suivantes vous seront posées:

```
Création d'un certificat SSL auto-signé <- oui  
Commonname <- ns1.infolaf.net
```

```
New password for the MySQL "root" user: <-- yourrootsqlpassword
```

```
Repeat password for the MySQL "root" user: <-- yourrootsqlpassword
```

```
General type of mail configuration: <-- Internet Site
```

```
System mail name: <-- ns1.infolaf.net
```

Ensuite, ouvrir les ports TLS/SSL et submission dans Postfix:

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

Dès-commenter les sections submission et smtps tel qu'indiqué et ajouter la ligne qui suit au deux sections et laisser le reste en commentaires

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

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

```
nano /etc/aliases
```



```
postmaster: root
clamav: root
infolaf: root
root: postmaster@infolaf.net
```

`newaliases`

Redémarrer Postfix:

```
service postfix restart
```

MySQL doit écouter sur toutes les interfaces réseaux, pas seulement localhost, alors nous éditons `/etc/mysql/my.cnf` et mettons en commentaire la ligne `bind-address = 127.0.0.1` :

```
nano /etc/mysql/my.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
[...]
```

Ensuite redémarrons MySQL:

```
service mysql restart
```

Maintenant, il faut vérifier que le réseau est actif. Exécuter :

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

La sortie au terminal devrait correspondre à ceci:

```
tcp 0 0 *:mysql *.* LISTEN 26757/mysqld
```

Afin d'installer `amavisd-new`, `SpamAssassin`, et `ClamAV`, nous exécutons :

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

L'installation de ISPConfig 3 utilise amavisd qui se charge à l'interne des bibliothèques de filtres de SpamAssassin, Nous pouvons donc arrêter SpamAssassin pour libérer un peu de RAM:

```
service spamassassin stop
```

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

Apache2, PHP5, phpMyAdmin, FCGI, suExec, Pear, and mcrypt doivent être installés comme indiqué:

```
apt-get install apache2 apache2-doc apache2-utils libapache2-mod-php5 php5 php5-  
common php5-gd php5-mysql php5-imap phpmyadmin php5-cli php5-cgi libapache2-mod-  
fcgid apache2-suexec php-pear php-auth php5-mcrypt mcrypt php5-imagick  
imagemagick libapache2-mod-suphp libruby libapache2-mod-python php5-curl php5-  
intl php5-memcache php5-memcached php5-ming php5-ps php5-pspell php5-recode php5-  
snmp php5-sqlite php5-tidy php5-xmllrpc php5-xsl memcached snmp
```

Les questions suivantes seront affichées:

```
Web server to reconfigure automatically: <- apache2  
Configure database for phpmyadmin with dbconfig-common? <- no
```

The PHP5 mcrypt module has to be enabled manually:

```
php5enmod mcrypt
```

Afin d'activer les modules Apache suexec , rewrite , ssl , actions , et include (plus dav , dav\_fs , et auth\_digest si vous désirez utiliser WebDAV), Exécuter:

```
a2enmod suexec rewrite ssl actions include cgi
```

```
a2enmod dav_fs dav auth_digest
```

Ensuite éditer */etc/apache2/mods-available/suphp.conf* ...

```
nano /etc/apache2/mods-available/suphp.conf
```

...et mettre en commentaire la section `<FilesMatch "\.ph(p3?|tml)$">` et ajouter la ligne `AddType application/x-httpd-suPHP .php .php3 .php4 .php5 .phtml` sinon tout les fichiers PHP seront lancer avec SuPHP:

```
<IfModule mod_suPHP.c>
#   <FilesMatch "\.ph(p3?|tml)$">
#       SetHandler application/x-httpd-suPHP
#   </FilesMatch>
      AddType application/x-httpd-suPHP .php .php3 .php4 .php5 .phtml
      suPHP_AddHandler application/x-httpd-suPHP

  <Directory />
    suPHP_Engine on
  </Directory>

  # By default, disable suPHP for debian packaged web applications as files
  # are owned by root and cannot be executed by suPHP because of min_uid.
  <Directory /usr/share>
    suPHP_Engine off
  </Directory>

  # # Use a specific php config file (a dir which contains a php.ini file)
  #   suPHP_ConfigPath /etc/php5/cgi/suPHP/
  # # Tells mod_suPHP NOT to handle requests with the type <mime-type>.
  #   suPHP_RemoveHandler <mime-type>
</IfModule>
```

Redémarrer Apache:

```
service apache2 restart
```

Si vous désirez héberger des fichiers Ruby avec l'extention `.rb` sur vos sites web créés avec ISPConfig, vous devez mettre en commentaire la ligne `application/x-ruby rb` dans `/etc/mime.types`:

```
nano /etc/mime.types
```

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

(Ceci est requis seulement pour les fichiers .rb ; Les fichiers Ruby avec l'extension .rbx fonctionne nativement.)

Redémarrer Apache:

```
service apache2 restart
```

Xcache est un opcode cacher PHP gratuit et libre pour mettre en cache et optimiser les codes PHP intermédiaire. Il est similaire à d'autres opcode cachés PHP tel que : eAccelerator et APC. Il est fortement recommandé d'avoir un de ceux-ci d'installé pour accélérer les pages PHP.

Xcache peut être installé de la façon suivante:

```
apt-get install php5-xcache
```

Redémarrer Apache:

```
service apache2 restart
```

Débutant avec ISPConfig 3.0.5, il est possible d'utiliser un mode PHP supplémentaire avec Apache: PHP-FPM.

Afin d'utiliser PHP-FPM avec Apache, il est nécessaire d'installer le module Apache mod\_fastcgi (S.V.P. ne pas s'embrouiller avec mod\_fcgid – Ils sont assez similaire, mais il est impossible d'utiliser PHP-FPM avec mod\_fcgid).

L'installation de PHP-FPM et mod\_fastcgi se fait de la façon suivante:

```
apt-get install libapache2-mod-fastcgi php5-fpm
```

Activer le module et redémarrer Apache:

```
a2enmod actions fastcgi alias
```

```
service apache2 restart
```

Versions additionnelles de PHP

Débutant avec ISPConfig 3.0.5, il est possible d'utiliser de multiple version

de PHP sur un seul serveur (sélectionnable dans ISPConfig) exécuté par FastCGI et PHP-FPM. Pour apprendre comment construire ces versions additionnelles de PHP (PHP-FPM et FastCGI) et comment configurer ISPConfig, veuillez s.v.p. consulter ce tutoriel: [How To Use Multiple PHP Versions \(PHP-FPM & FastCGI\) With ISPConfig 3 \(Debian Wheezy\)](#).

### Installation de Mailman

Depuis la version 3.0.4, ISPConfig vous permet également de gérer (création/modifier/supprimer) des listes d'envois Mailman. Si vous désirez utiliser cette fonctions, installer Mailman :

```
apt-get install mailman
```

Sélectionner au moins une langue:

```
Languages to support: <-- en (English) Missing site list <-- Ok
```

Avant de lancer Mailman, une première liste nommée mailman doit être créée :

```
newlist mailman
```

```
Enter the email of the person running the list: <-- admin email address, e.g.
listadmin@example.com
```

```
Initial mailman password: <-- admin password for the mailman list
```

To finish creating your mailing list, you must edit your */etc/aliases* (or equivalent) file by adding the following lines, and possibly running the ``newaliases'` program:

```
## 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"
```

```
Hit enter to notify mailman owner... <-- ENTER
```

Éditer ensuite */etc/aliases* ...

```
nano /etc/aliases
```

... et ajouter les lignes suivantes :

```
[...]
## 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"
```

Exécuter

```
newaliases
```

ensuite redémarrer Postfix:

```
service postfix restart
```

Finalement, nous devons activer la configuration de Mailman dans Apache:

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

```
a2enconf mailman.conf
```

 (a2disconf pour enlever une configuration)

Ceci définit l'alias `/cgi-bin/mailman/` pour tous les vhosts Apache, ce qui signifie que vous pouvez accéder aux listes de diffusion par l'interface d'administration de Mailman à l'URL `http://cgi-bin/mailman/admin/`. La page web des utilisateurs à l'URL `http://cgi-bin/mailman/listinfo/`.

Sous `http://pipermail` vous trouverez les listes de diffusion archivées.

Redémarrer Apache:

```
service apache2 restart
```

Sauter directement au démarrage de mailman. Ce qui suit peut permettre le débogage s'il y a problème avec mailman

```
cd /usr/lib/mailman/bin  
./check_perms
```

*Les permissions ne sont pas correctement fixé. Alors pour fixer le tout...*

```
./check_perms -f
```

```
Mauvais gid pour /var/lib/mailman/cgi-bin (Obtenu: root, Attendu list)  
Mauvais gid pour /var/lib/mailman/locks (Obtenu: root, Attendu list)  
Mauvais gid pour /var/lib/mailman/scripts (Obtenu: root, Attendu list)  
Mauvais gid pour /var/lib/mailman/mail (Obtenu: root, Attendu list)  
Mauvais gid pour /var/lib/mailman/Mailman (Obtenu: root, Attendu list)  
Mauvais gid pour /var/lib/mailman/cron (Obtenu: root, Attendu list)  
Mauvais gid pour /var/lib/mailman/templates (Obtenu: root, Attendu list)  
Mauvais gid pour /var/lib/mailman/logs (Obtenu: root, Attendu list)  
Mauvais gid pour /var/lib/mailman/icons (Obtenu: root, Attendu list)  
Mauvais gid pour /var/lib/mailman/bin (Obtenu: root, Attendu list)  
Problemes trouves : 10
```

*Mais, il s'agit de liens symboliques et l'outil contrôle les permissions des liens, pas des fichiers visés. Bref, c'est bon.*

*Une partie de la doc d'installation est dans /usr/lib/mailman/bin/postfix-to-mailman.py qui est un lien vers /etc/mailman/postfix-to-mailman.py. Attention, cette doc doit être transposée au contexte « serveur virtuel avec conf en MySQL » – ce que je fais dans cet article.*

```
Dans /etc/mailman/mm_cfg.py, j'adapte ces paramètres là :
```

```
DEFAULT_SERVER_LANGUAGE = 'fr'  
MTA='Postfix'
```

Démarrer Mailman:

```
service mailman start
```

Installer PureFTPd et Quota :

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

Éditer le fichier /etc/default/pure-ftpd-common ...

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

... ajuster start mode à standalone et VIRTUALCHROOT=true :

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

Maintenant configurons PureFTPd pour permettre les sessions FTP et TLS. FTP n'est pas un protocole sécuritaire car les mots de passe et les données sont transférés en texte clair.

En utilisant TLS, l'ensemble des communications peuvent alors être cryptées, rendant ainsi FTP beaucoup plus sécuritaire.

Pour installer TLS sessions, exécuter :

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

Afin de permettre l'utilisation de TLS, nous devons créer un certificat SSL. Celui-ci sera créé dans /etc/ssl/private/ , donc il faut premièrement créer ce répertoire:

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

Ensuite, nous générons le certificat SSL comme indiqué:



```
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]: <-- Enter your Country Name (e.g., "CA").  
State or Province Name (full name) [Some-State]: <-- Enter your State or Province  
Name.  
Locality Name (eg, city) []: <-- Enter your City.  
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter your  
Organization Name (e.g., the name of your company).  
Organizational Unit Name (eg, section) []: <-- Enter your Organizational Unit  
Name (e.g. "IT Department").  
Common Name (eg, YOUR name) []: <-- Enter the Fully Qualified Domain Name of the  
system (e.g. "server1.example.com").  
Email Address []: <-- Enter your Email Address.
```

Changer les permissions du certificat SSL:

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

Redémarrer PureFTPd:

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

Éditer `/etc/fstab` . Le mien ressemble à celui-ci (J'ai ajouté

```
,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0
```

 à la partition qui a le point de montage `/` et `/var/vmail` et `/var/www` ):

```
nano /etc/fstab
```

```
# /etc/fstab: static file system information.  
#  
# Use 'blkid' to print the universally unique identifier for a  
# device; this may be used with UUID= as a more robust way to name devices  
# that works even if disks are added and removed. See fstab(5).  
#  
#     # / was on /dev/sda1 during installation  
UUID=19113f17-f269-4840-96ec-7cc1221fb9bf / ext4 errors=remount-  
ro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0 1  
# swap was on /dev/sda5 during installation  
UUID=998f7d49-6c82-4fd4-a47e-dc909449dc8a none swap sw 0 0  
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
```

```
#Montage locaux des disques du serveur ns1

#/dev/sdb1 - Mail
UUID=114ca2a0-a741-4602-8bdd-c30c95f29b73 /var/vmail ext4
defaults,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0 2

#/dev/sdc1 - Web
UUID=ebccdb3a-f1b8-4430-9cb4-dc5e9b6bb123 /var/www ext4
defaults,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0 2
```

Pour activer quota, exécuter ces commandes:

```
mount -o remount /
```

```
mount -o remount /var/vmail
```

```
mount -o remount /var/www
```

```
quotacheck -avugm
```

```
quotaon -avug
```

Installation du serveur DNS BIND

BIND s'installe ainsi:

```
apt-get install bind9 dnsutils
```

Installation de Vlogger, Webalizer, et AWstats

Vlogger, webalizer, et AWstats peuvent être installés ainsi:

```
apt-get install vlogger webalizer awstats geop-database libclass-dbi-mysql-perl
```

Ouvrir /etc/cron.d/awstats

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

... et mettre tout en commentaires dans ce fichier:

```
#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
```

## Installation de Jailkit

Jailkit est requis seulement si vous désirez avec des usagers SSH en chroot. L'installation se fait comme suit ( important: Jailkit doit être installé avant ISPConfig – Il ne peut pas être installé par la suite! ):

```
apt-get install build-essential autoconf automake1.9 libtool flex bison debhelper
binutils-gold
```

```
cd /tmp
```

```
wget http://olivier.sessink.nl/jailkit/jailkit-2.17.tar.gz
```

```
tar xvfz jailkit-2.17.tar.gz
```

```
cd jailkit-2.17
```

```
./debian/rules binary
```

Vous pouvez désormais installer le paquet .deb de Jailkit comme suit:

```
cd ..
```

```
dpkg -i jailkit_2.17-1_*.deb
```

```
rm -rf jailkit-2.17*
```

## Installation de fail2ban

Ceci est optionnel mais recommandé, parce que le module Monitor de ISPConfig tente d'afficher le log:

```
apt-get install fail2ban
```

Afin que fail2ban surveille PureFTPd et Dovecot, il faut créer le fichier /etc/fail2ban/jail.local :

```
nano /etc/fail2ban/jail.local
```

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

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

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

Créer ensuite les deux fichiers de filtre suivants:

```
nano /etc/fail2ban/filter.d/pureftpd.conf
```

```
[Definition]
failregex = .*pure-ftp: \(.*@\) \[WARNING\] Authentication failed for user.*
ignoreregex =
```

```
nano /etc/fail2ban/filter.d/dovecot-pop3imap.conf
```

```
[Definition]
failregex = (?: pop3-login|imap-login): .*(?:Authentication failure|Aborted login
```

```
\(auth failed|Aborted login \(\(tried to use disabled|Disconnected \(\(auth
failed|Aborted login \(\d+ authentication attempts).*rip=(?P\S*),.*
ignoreregex =
```

Add the missing ignoreregex line in the postfix-sasl file:

```
echo "ignoreregex =" >> /etc/fail2ban/filter.d/postfix-sasl.conf
```

Redémarrer fail2ban:

```
service fail2ban restart
```

Installation de ISPConfig 3

Afin d'installer la dernière version stable de ISPConfig 3 , effectuer ceci:

```
cd /tmp
```

```
wget http://www.ispconfig.org/downloads/ISPConfig-3-stable.tar.gz
```

```
tar xzf ISPConfig-3-stable.tar.gz
```

```
cd ispconfig3_install/install/
```

L'étape suivante consiste à exécuter

```
php -q install.php ou bien php -q update.php pour un update
```

Ceci démarrera l'installation de ISPConfig 3. L'assistant d'installation configurera tous les services pour vous : Postfix, Dovecot, etc.

```
root@nsl:/tmp/ispconfig3_install/install# php -q install.php
```

```
PHP Deprecated: Comments starting with '#' are deprecated in
/etc/php5/cli/conf.d/ming.ini on line 1 in Unknown on line 0
```

```
-----
_____
--
____
|_ _/ __| __ \ / _ \
/ _(_)
/_ \
```

```
| | \ `--.| | / / | / \ _ _ _ | | _ _ _ / /
| | `--. \ _ / | | / _ \ | ' \ | _ | / _ ` | | _ |
_| | / \ / / | | \ \ ^ ( ) | | | | | | ( | | _ \ \
\ \ ^ _ \ \ ^ _ | \ \ ^ _ / | | | | | | \ \ , | \ \ /
_ / |
| _ /
```

-----  
>> Initial configuration

Operating System: Debian or compatible, unknown version.

Following will be a few questions for primary configuration so be careful.

Default values are in [brackets] and can be accepted with .

Tap in "quit" (without the quotes) to stop the installer.

Select language (en,de) [en]: <-- ENTER Installation mode (standard,expert)

[standard]: <-- ENTER Full qualified hostname (FQDN) of the server, eg

server1.domain.tld [server1.example.com]: <-- ENTER MySQL server hostname

[localhost]: <-- ENTER MySQL root username [root]: <-- ENTER MySQL root password

[: <-- yourrootsqlpassword MySQL database to create [dbispconfig]: <-- ENTER

MySQL charset [utf8]: <-- ENTER 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 State or Province Name (full name) [Some-State]: <-- ENTER Locality Name (eg, city) []: <--

ENTER Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- ENTER

Organizational Unit Name (eg, section) []: <-- ENTER Common Name (e.g. server

FQDN or YOUR name) []: <-- ENTER Email Address []: <-- ENTER Configuring Jailkit

Configuring Dovecot Configuring Spamassassin Configuring Amavisd Configuring

Getmail Configuring Pureftpd Configuring BIND Configuring Apache Configuring

Vlogger Configuring Apps vhost Configuring Bastille Firewall Configuring Fail2ban

Installing ISPConfig ISPConfig Port [8080]: <-- ENTER Do you want a secure (SSL)

connection to the ISPConfig web interface (y,n) [y]: <-- 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 State or Province Name (full name) [Some-State]:
<-- ENTER Locality Name (eg, city) []: <-- ENTER Organization Name (eg, company)
[Internet Widgits Pty Ltd]: <-- ENTER Organizational Unit Name (eg, section) []:
<-- ENTER Common Name (e.g. server FQDN or YOUR name) []: <-- ENTER Email Address
[]: <-- ENTER Please enter the following 'extra' attributes to be sent with your
certificate request A challenge password []: <-- ENTER An optional company name
[]: <-- ENTER writing RSA key Configuring DBServer Installing ISPConfig crontab
no crontab for root no crontab for getmail Restarting services ... Stopping MySQL
database server: mysqld. Starting MySQL database server: mysqld .. Checking for
tables which need an upgrade, are corrupt or were not closed cleanly.. Stopping
Postfix Mail Transport Agent: postfix. Starting Postfix Mail Transport Agent:
postfix. Stopping amavisd: amavisd-new. Starting amavisd: amavisd-new. Stopping
ClamAV daemon: clamd. Starting ClamAV daemon: clamd . Restarting IMAP/POP3 mail
server: dovecot. [Tue May 07 02:36:22 2013] [warn] NameVirtualHost *:443 has no
VirtualHosts [Tue May 07 02:36:22 2013] [warn] NameVirtualHost *:80 has no
VirtualHosts [Tue May 07 02:36:23 2013] [warn] NameVirtualHost *:443 has no
VirtualHosts [Tue May 07 02:36:23 2013] [warn] NameVirtualHost *:80 has no
VirtualHosts Restarting web server: apache2 ... waiting . Restarting ftp server:
Running: /usr/sbin/pure-ftpd-mysql-virtualchroot -l mysql:/etc/pure-
ftpd/db/mysql.conf -l pam -H -O clf:/var/log/pure-ftpd/transfer.log -Y 1 -D -u
1000 -A -E -b -8 UTF-8 -B Installation completed.
root@server1:/tmp/ispconfig3_install/install#

```

L'assistant d'installation configure automatiquement tous les services sous-jacents, aucune configuration manuelle n'est requise.

Vous avez la possibilité de permettre à l'assistant d'installation de créer un vhost SSL afin d'accéder au panneau de contrôle de ISPConfig via https:// à la place de http:// . Pour réaliser cette opération, appuyer sur ENTRÉE lorsque vous apercevez cette question: Do you want a secure (SSL) connection to the ISPConfig web interface (y,n) [y]: .

Par la suite, vous pourrez accéder à ISPConfig 3 à l'URL `http(s)://server1.example.com:8080/` ou `http(s)://192.168.0.100:8080/` ( http ou https selon votre choix pendant l'installation). Effectuer votre authentification avec le nom d'utilisateur : admin et le mot de passe : admin (Vous devriez changer le mot de passe par défaut lors de votre première connexion):

À titre de référence seulement si on a utilisé le mode expert de ISPconfig lors de l'installation:

si on as deux serveur de nom que l'on veut piloter dans ISPConfig (Utiliser l'installation expert de ispcnfig)  
Pour la connexion du serveur DNS secondaire il faut autoriser le tout dans mysql du master.

Run twice for every slave server on the master before ispcnfig is installed, once for the IP « 192.168.0.11 » and a second time for the hostname « ns2.infolaf.net ». If you dont do that, you get the forbidden error that you described above. Also make sure that you add the lines in the /etc/hosts files for all servers on each server.

Just correct these things in the mysql server on the master and check all hosts fiels, then restart mysql and proceed with the installation of ispcnfig on the slaves. No need to reinstall the master or slaves.

```
CREATE USER 'root'@'ns2.infolaf.net' IDENTIFIED BY '';  
GRANT ALL PRIVILEGES ON * . * TO 'root'@'ns2.infolaf.net' IDENTIFIED BY '' WITH  
GRANT OPTION MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0  
MAX_UPDATES_PER_HOUR 0 MAX_USER_CONNECTIONS 0 ;
```

```
CREATE USER 'root'@'192.168.0.11' IDENTIFIED BY '';  
GRANT ALL PRIVILEGES ON * . * TO 'root'@'192.168.0.11' IDENTIFIED BY '' WITH GRANT  
OPTION MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0  
MAX_USER_CONNECTIONS 0 ;
```

Ajout du mode canonical dans MySQL :

Créer la table mail\_canonical dans la base de données dbispcnfig :

Le mode canonical permet de changer l'adresse de réponse d'un courriel envoyé à partir d'une adresse sans FQDN (@reseau.maison) afin que le destinataire puisse répondre au courriel vers une adresse réellement joignable sur internet @infolaf.net

L'opération suivante permet d'ajouter ce mode dans la table dbispcnfig mais



sans pouvoir l'éditer dans l'interface web de ISPConfig. Afin d'ajouter les données, on doit éditer directement la table mail\_canonical à partir de phpmyadmin.

Sélectionner la table et appuyer sur insérer. Dans Email, ajouter l'adresse sans FQDN (prenom.nom@reseau.maison). Dans canonical ajouter le courriel de réponse (prenom.nom@infolaf.net)

Afin d'ajouter le mode canonical à postfix il faut effectuer les opérations suivantes soit dans phpmyadmin sur la table dbispconfig et exécuter la commande SQL suivante :

```
CREATE TABLE mail_canonical (email varchar(80) NOT NULL, canonical TEXT NOT NULL,  
PRIMARY KEY (email) ) ENGINE=MyISAM;
```

ou avec le shell :

```
mysql -u root -p  
USE dbispconfig;  
CREATE TABLE mail_canonical (email varchar(80) NOT NULL, canonical TEXT NOT NULL,  
PRIMARY KEY (email) ) ENGINE=MyISAM;
```

Créer le fichier suivant et adapter le password (Le récupérer dans /etc/postfix/mysql-virtual\_relaydomains.cf)

```
sudo nano /etc/postfix/mysql-virtual_sender_canonical_maps.cf  
user = ispconfig  
password = fa8c47a339ddd7a49573e976ae99d593  
dbname = dbispconfig  
table = mail_canonical  
select_field = canonical  
where_field = email  
#query = SELECT canonical FROM canonical WHERE email='%s'  
hosts = 127.0.0.1
```

Effectuer les commandes suivantes

```
sudo chmod o= /etc/postfix/mysql-virtual_sender_canonical_maps.cf
sudo chgrp postfix /etc/postfix/mysql-virtual_sender_canonical_maps.cf
sudo postconf -e 'sender_canonical_maps = proxy:mysql:/etc/postfix/mysql-
virtual_sender_canonical_maps.cf'
sudo service postfix restart
```

Quelques problèmes avec MySQL après 1 an d'utilisation: Fatal error: cannot allocate memory for the buffer pool

référence:

<http://www.webtrafficexchange.com/solved-mysql-crash-fatal-error-cannot-allocate-memory-buffer-pool>

Le problème est relatif au fait que le serveur n'a pas assez de mémoire à sa disposition pour en allouer au processus MySQL. Il y a quelques solutions à ce problème.

- (1) Augmenter la RAM physique. Ajouter 1GB de RAM additionnelle devrait régler le problème.
- (2) Allouer de l'espace SWAP. Si votre serveur n'utilise pas automatiquement le swap, voici comment l'activer. En allouant 512MB comme fichier d'échange (swap), il a été possible de résoudre ce problème. Suivre la procédure suivante:

## Passer au compte root et faire les commandes suivantes:

```
sudo su
dd if=/dev/zero of=/swap.dat bs=1024 count=512k
mkswap /swap.dat
swapon /swap.dat
```

## Modifier le fichier /etc/fstab, en ajoutant la ligne suivante.

```
/swap.dat none swap sw 0 0
```

- (3) Réduire la grosseur du buffer pour MySQL:

## Modifier le fichier /etc/mysql/my.cnf, en ajoutant la ligne suivante sous la

section [mysqld].

```
[mysqld]
```

```
innodb_buffer_pool_size=64M
```

Redémarrer mysql:

```
sudo service mysql restart
```

Surveiller le processus MySQL pour une semaine environ afin de s'assurer que le serveur tourne sans problème d'allocation de mémoire.

Au premier login de ISPConfig, veuillez vous assurez que la fonction SLI est coché sous le menu `>System >Server Config >SSL Settings`

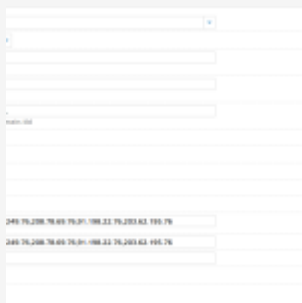
---

Voici des captures d'écran des entrées DNS d'iSPConfig pour illustrer une configuration fonctionnelle:

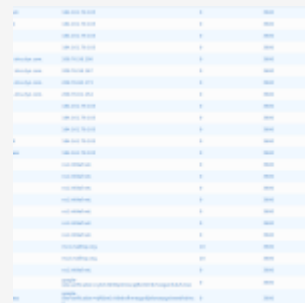
Pour la zone public:

infolaf.net

**Zone**



**Enregistrements**



142.189.131.in-addr.arpa

**Zone**

**Enregistrements**

ns1.infolaf.com.	0	3600
ns2.infolaf.com.	0	3600
ns3.infolaf.com.	0	3600
ns4.infolaf.com.	0	3600
ns5.infolaf.com.	0	3600
ns6.infolaf.com.	0	3600
ns7.infolaf.com.	0	3600
ns8.infolaf.com.	0	3600
ns9.infolaf.com.	0	3600
ns10.infolaf.com.	0	3600
ns11.infolaf.com.	0	3600
ns12.infolaf.com.	0	3600
ns13.infolaf.com.	0	3600
ns14.infolaf.com.	0	3600
ns15.infolaf.com.	0	3600
ns16.infolaf.com.	0	3600
ns17.infolaf.com.	0	3600
ns18.infolaf.com.	0	3600
ns19.infolaf.com.	0	3600
ns20.infolaf.com.	0	3600
ns21.infolaf.com.	0	3600
ns22.infolaf.com.	0	3600
ns23.infolaf.com.	0	3600
ns24.infolaf.com.	0	3600
ns25.infolaf.com.	0	3600
ns26.infolaf.com.	0	3600
ns27.infolaf.com.	0	3600
ns28.infolaf.com.	0	3600
ns29.infolaf.com.	0	3600
ns30.infolaf.com.	0	3600
ns31.infolaf.com.	0	3600
ns32.infolaf.com.	0	3600
ns33.infolaf.com.	0	3600
ns34.infolaf.com.	0	3600
ns35.infolaf.com.	0	3600
ns36.infolaf.com.	0	3600
ns37.infolaf.com.	0	3600
ns38.infolaf.com.	0	3600
ns39.infolaf.com.	0	3600
ns40.infolaf.com.	0	3600
ns41.infolaf.com.	0	3600
ns42.infolaf.com.	0	3600
ns43.infolaf.com.	0	3600
ns44.infolaf.com.	0	3600
ns45.infolaf.com.	0	3600
ns46.infolaf.com.	0	3600
ns47.infolaf.com.	0	3600
ns48.infolaf.com.	0	3600
ns49.infolaf.com.	0	3600
ns50.infolaf.com.	0	3600

Pour la zone privé:

reseau.maison

### Zone

### Enregistrements

ns1.reseau.maison.	0	3600
ns2.reseau.maison.	0	3600
ns3.reseau.maison.	0	3600
ns4.reseau.maison.	0	3600
ns5.reseau.maison.	0	3600
ns6.reseau.maison.	0	3600
ns7.reseau.maison.	0	3600
ns8.reseau.maison.	0	3600
ns9.reseau.maison.	0	3600
ns10.reseau.maison.	0	3600
ns11.reseau.maison.	0	3600
ns12.reseau.maison.	0	3600
ns13.reseau.maison.	0	3600
ns14.reseau.maison.	0	3600
ns15.reseau.maison.	0	3600
ns16.reseau.maison.	0	3600
ns17.reseau.maison.	0	3600
ns18.reseau.maison.	0	3600
ns19.reseau.maison.	0	3600
ns20.reseau.maison.	0	3600
ns21.reseau.maison.	0	3600
ns22.reseau.maison.	0	3600
ns23.reseau.maison.	0	3600
ns24.reseau.maison.	0	3600
ns25.reseau.maison.	0	3600
ns26.reseau.maison.	0	3600
ns27.reseau.maison.	0	3600
ns28.reseau.maison.	0	3600
ns29.reseau.maison.	0	3600
ns30.reseau.maison.	0	3600
ns31.reseau.maison.	0	3600
ns32.reseau.maison.	0	3600
ns33.reseau.maison.	0	3600
ns34.reseau.maison.	0	3600
ns35.reseau.maison.	0	3600
ns36.reseau.maison.	0	3600
ns37.reseau.maison.	0	3600
ns38.reseau.maison.	0	3600
ns39.reseau.maison.	0	3600
ns40.reseau.maison.	0	3600
ns41.reseau.maison.	0	3600
ns42.reseau.maison.	0	3600
ns43.reseau.maison.	0	3600
ns44.reseau.maison.	0	3600
ns45.reseau.maison.	0	3600
ns46.reseau.maison.	0	3600
ns47.reseau.maison.	0	3600
ns48.reseau.maison.	0	3600
ns49.reseau.maison.	0	3600
ns50.reseau.maison.	0	3600

0.168.192.in-addr.arpa

### Zone

### Enregistrements

ns1.0.168.192.in-addr.arpa.	0	3600
ns2.0.168.192.in-addr.arpa.	0	3600
ns3.0.168.192.in-addr.arpa.	0	3600
ns4.0.168.192.in-addr.arpa.	0	3600
ns5.0.168.192.in-addr.arpa.	0	3600
ns6.0.168.192.in-addr.arpa.	0	3600
ns7.0.168.192.in-addr.arpa.	0	3600
ns8.0.168.192.in-addr.arpa.	0	3600
ns9.0.168.192.in-addr.arpa.	0	3600
ns10.0.168.192.in-addr.arpa.	0	3600
ns11.0.168.192.in-addr.arpa.	0	3600
ns12.0.168.192.in-addr.arpa.	0	3600
ns13.0.168.192.in-addr.arpa.	0	3600
ns14.0.168.192.in-addr.arpa.	0	3600
ns15.0.168.192.in-addr.arpa.	0	3600
ns16.0.168.192.in-addr.arpa.	0	3600
ns17.0.168.192.in-addr.arpa.	0	3600
ns18.0.168.192.in-addr.arpa.	0	3600
ns19.0.168.192.in-addr.arpa.	0	3600
ns20.0.168.192.in-addr.arpa.	0	3600
ns21.0.168.192.in-addr.arpa.	0	3600
ns22.0.168.192.in-addr.arpa.	0	3600
ns23.0.168.192.in-addr.arpa.	0	3600
ns24.0.168.192.in-addr.arpa.	0	3600
ns25.0.168.192.in-addr.arpa.	0	3600
ns26.0.168.192.in-addr.arpa.	0	3600
ns27.0.168.192.in-addr.arpa.	0	3600
ns28.0.168.192.in-addr.arpa.	0	3600
ns29.0.168.192.in-addr.arpa.	0	3600
ns30.0.168.192.in-addr.arpa.	0	3600
ns31.0.168.192.in-addr.arpa.	0	3600
ns32.0.168.192.in-addr.arpa.	0	3600
ns33.0.168.192.in-addr.arpa.	0	3600
ns34.0.168.192.in-addr.arpa.	0	3600
ns35.0.168.192.in-addr.arpa.	0	3600
ns36.0.168.192.in-addr.arpa.	0	3600
ns37.0.168.192.in-addr.arpa.	0	3600
ns38.0.168.192.in-addr.arpa.	0	3600
ns39.0.168.192.in-addr.arpa.	0	3600
ns40.0.168.192.in-addr.arpa.	0	3600
ns41.0.168.192.in-addr.arpa.	0	3600
ns42.0.168.192.in-addr.arpa.	0	3600
ns43.0.168.192.in-addr.arpa.	0	3600
ns44.0.168.192.in-addr.arpa.	0	3600
ns45.0.168.192.in-addr.arpa.	0	3600
ns46.0.168.192.in-addr.arpa.	0	3600
ns47.0.168.192.in-addr.arpa.	0	3600
ns48.0.168.192.in-addr.arpa.	0	3600
ns49.0.168.192.in-addr.arpa.	0	3600
ns50.0.168.192.in-addr.arpa.	0	3600

Voici le résultat obtenu pour les fichiers bind après la configuration dans ispsconfig :

```
sudo nano /etc/bind/pri.infolaf.net
```

```
$TTL 3600
@ IN SOA ns1.infolaf.net. postmaster.infolaf.net. (
```

```
2015021902 ; serial, todays date + todays serial #
86400 ; refresh, seconds
7200 ; retry, seconds
3600000 ; expire, seconds
172800 ) ; minimum, seconds
;

magasin 3600 A 184.161.79.103
mdp 3600 A 184.161.79.103
ns1 3600 A 184.161.79.103
ns1200.dns.dyn.com. 3600 A 208.76.58.200
ns2167.dns.dyn.com. 3600 A 208.76.59.167
ns3173.dns.dyn.com. 3600 A 208.76.60.173
ns4154.dns.dyn.com. 3600 A 208.76.61.154
nuage 3600 A 184.161.79.103
photos 3600 A 184.161.79.103
piwik 3600 A 184.161.79.103
webmail 3600 A 184.161.79.103
wordpress 3600 A 184.161.79.103
ftp 3600 CNAME ns1.infolaf.net.
imap 3600 CNAME ns1.infolaf.net.
ldap 3600 CNAME ns1.infolaf.net.
listes 3600 CNAME ns1.infolaf.net.
mail 3600 CNAME ns1.infolaf.net.
pop 3600 CNAME ns1.infolaf.net.
smtp 3600 CNAME ns1.infolaf.net.
@ 3600 MX 10 mx1.mailhop.org.
@ 3600 MX 20 mx2.mailhop.org.
@ 3600 NS ns1.infolaf.net.
photos 3600 TXT "google-site-verification=rykrk3dl3bptimwcjzjlfvx9m9c5xogenfu0vf-
cbcs"
wordpress 3600 TXT "google-site-
verification=ejf0bw1nk0ebvfhmezpp6jielsnaeygxtvewdlvdmca"
```

```
sudo nano pri.142.189.131.in-addr.arpa
```

```
$TTL 3600
@ IN SOA ns1.infolaf.net. postmaster.infolaf.net. (
2015020101 ; serial, todays date + todays serial #
86400 ; refresh, seconds
7200 ; retry, seconds
```

```
3600000 ; expire, seconds
172800 ) ; minimum, seconds
;

@ 3600 NS ns2167.dns.dyn.com.
@ 3600 NS ns1200.dns.dyn.com.
@ 3600 NS ns3173.dns.dyn.com.
@ 3600 NS ns4154.dns.dyn.com.
@ 3600 NS ns1.infolaf.net.
103 3600 PTR listes.infolaf.net.
103 3600 PTR ftp.infolaf.net.
103 3600 PTR mdp.infolaf.net.
103 3600 PTR ns1.infolaf.net.
103 3600 PTR pop.infolaf.net.
103 3600 PTR imap.infolaf.net.
103 3600 PTR ldap.infolaf.net.
103 3600 PTR mail.infolaf.net.
103 3600 PTR smtp.infolaf.net.
103 3600 PTR nuage.infolaf.net.
103 3600 PTR magasin.infolaf.net.
103 3600 PTR photos.infolaf.net.
103 3600 PTR webmail.infolaf.net.
103 3600 PTR wordpress.infolaf.net.
```

```
sudo nano /etc/bind/pri.reseau.maison
```

```
$TTL 3600
@ IN SOA ns1.infolaf.net. postmaster.reseau.maison. (
2015020119 ; serial, todays date + todays serial #
86400 ; refresh, seconds
7200 ; retry, seconds
3600000 ; expire, seconds
172800 ) ; minimum, seconds
;

nas1 3600 A 192.168.0.12
ns1 3600 A 192.168.0.10
routeur 3600 A 192.168.0.1
solydx-ltsp 3600 A 192.168.0.11
solydx-n73 3600 A 192.168.0.105
solydx-ss 3600 A 192.168.0.110
```

```
solydx-t500 3600 A 192.168.0.103
win7-sous-sol 3600 A 192.168.0.110
ftp 3600 CNAME ns1.reseau.maison.
imap 3600 CNAME ns1.reseau.maison.
ldap 3600 CNAME ns1.reseau.maison.
mail 3600 CNAME ns1.reseau.maison.
pop 3600 CNAME ns1.reseau.maison.
smtp 3600 CNAME ns1.reseau.maison.
virtualbox 3600 CNAME ns1.reseau.maison.
@ 3600 MX 10 ns1.infolaf.net.
@ 3600 NS ns1.reseau.maison.
reseau.maison. 3600 NS ns1.infolaf.net.
```

```
sudo nano pri.0.168.192.in-addr.arpa
```

```
$TTL 3600
@ IN SOA ns1.infolaf.net. postmaster.reseau.maison. (
2015012502 ; serial, todays date + todays serial #
86400 ; refresh, seconds
7200 ; retry, seconds
3600000 ; expire, seconds
172800 ) ; minimum, seconds
;

. 3600 MX 10 ns1.infolaf.net.
@ 3600 NS ns1.reseau.maison.
@ 3600 NS ns1.infolaf.net.
10 3600 PTR ftp.reseau.maison.
10 3600 PTR ns1.infolaf.net.
10 3600 PTR pop.reseau.maison.
10 3600 PTR imap.reseau.maison.
10 3600 PTR ldap.reseau.maison.
10 3600 PTR mail.reseau.maison.
10 3600 PTR smtp.reseau.maison.
10 3600 PTR mysql.maison.
10 3600 PTR virtualbox.reseau.maison.
10 3600 PTR lists.reseau.maison
103 3600 PTR win7-t500.reseau.maison.
103 3600 PTR solydx-t500.reseau.maison.
105 3600 PTR solydx-n73.reseau.maison.
11 3600 PTR solydx-ltsp.reseau.maison.
```

```
110 3600 PTR solydx-ss.reseau.maison.  
110 3600 PTR win7-sous-sol.reseau.maison.  
12 3600 PTR nas1.reseau.maison.
```

`sudo nano /etc/bind/named.conf.local` (Sur le NS1)

```
zone "0.168.192.in-addr.arpa" {  
    type master;  
    allow-transfer {192.168.0.12;};  
    file "/etc/bind/pri.0.168.192.in-addr.arpa";  
};  
zone "reseau.maison" {  
    type master;  
    allow-transfer {192.168.0.12;};  
    file "/etc/bind/pri.reseau.maison";  
};  
zone "infolaf.net" {  
    type master;  
    allow-transfer  
    {192.168.0.12;204.13.249.76;208.78.69.76;91.198.22.76;203.62.195.76;};  
    also-notify  
    {192.168.0.12;204.13.249.76;208.78.69.76;91.198.22.76;203.62.195.76;};  
    file "/etc/bind/pri.infolaf.net";  
};  
zone "142.189.131.in-addr.arpa" {  
    type master;  
    allow-transfer  
    {192.168.0.12;204.13.249.76;208.78.69.76;91.198.22.76;203.62.195.76;};  
    also-notify  
    {192.168.0.12;204.13.249.76;208.78.69.76;91.198.22.76;203.62.195.76;};  
    file "/etc/bind/pri.142.189.131.in-addr.arpa";  
};
```

`sudo nano /etc/bind/named.conf.local` (Sur le nas1 – DNS esclave)

```
//  
// Do any local configuration here  
//
```



```
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "reseau.maison" {
type slave;
file "/etc/bind/pri.reseau.maison";
masters { 192.168.0.10; };
};
zone "0.168.192.in-addr.arpa" {
type slave;
file "/etc/bind/pri.0.168.192.in-addr.arpa";
masters { 192.168.0.10; };
};
zone "infolaf.net" {
type slave;
file "/etc/bind/pri.infolaf.net";
masters { 192.168.0.10; };
};
zone "142.189.131.in-addr.arpa" {
type slave;
file "/etc/bind/pri.142.189.131.in-addr.arpa";
masters { 192.168.0.10; };
};
```

Il doit maintenant être possible de faire un ping sur infolaf.net et la requête doit être résolue :

```
ping infolaf.net
```

L'utilitaire named-checkzone (inclus dans le package BIND9) peut également être utilisé :

```
named-checkzone infolaf.net /etc/bind/pri.infolaf.net
```

```
named-checkzone 142.189.131.in-addr.arpa /etc/bind/pri.142.189.131.in-addr.arpa
```

```
named-checkzone reseau.maison /etc/bind/pri.reseau.maison
```

```
named-checkzone 0.168.192.in-addr.arpa /etc/bind/pri.0.168.192.in-addr.arpa
```

Utiliser cet utilitaire est un bon moyen de s'assurer de l'absence d'erreurs avant le redémarrage de bind.

Pour tester la recherche inversée, l'utilitaire dig peut être utilisé :

```
dig /etc/bind/pri.0.168.192.in-addr.arpa
```

Éditer aussi le fichier suivant du DNS secondaire :

```
sudo nano /etc/bind/named.conf.options
```

```
options {
  directory "/var/cache/bind";

  // If there is a firewall between you and nameservers you want
  // to talk to, you may need to fix the firewall to allow multiple
  // ports to talk. See http://www.kb.cert.org/vuls/id/800113

  // If your ISP provided one or more IP addresses for stable
  // nameservers, you probably want to use them as forwarders.
  // Uncomment the following block, and insert the addresses replacing
  // the all-0's placeholder.

  // forwarders {
  // 0.0.0.0;
  // };

  auth-nxdomain no; # conform to RFC1035
  listen-on-v6 { none; };
  allow-query { none; };
  allow-recursion { 184.161.79.103; 192.168.0.0/24; localnets; };
  allow-transfer { none; };
};
```

Changer les permissions sur le répertoire de bind pour permettre la synchro.

```
sudo chmod 775 /etc/bind
```

Apparmor fixe les droits d'accès des programmes.

J'ai donc modifié sur le serveur primaire (nas.reseau.maison) :

```
sudo nano /etc/apparmor.d/usr.sbin.named
```

en remplaçant :

```
/etc/bind/** r,
```

par

```
/etc/bind/** rw,
```

pour autoriser named à écrire dans /etc/bind. Sans oublier de relancer :

```
sudo /etc/init.d/apparmor restart
```

Vérifier les fichiers de configurations sur serveur secondaire:

```
sudo named-checkzone infolaf.net /etc/bind/pri.infolaf.net
```

```
sudo named-checkzone reseau.maison /etc/bind/pri.reseau.maison
```

```
sudo named-checkzone 142.189.131.in-addr.arpa /etc/bind/pri.142.189.131.in-addr.arpa
```

```
sudo named-checkzone 0.168.192.in-addr.arpa /etc/bind/pri.0.168.192.in-addr.arpa
```

```
sudo named-checkconf /etc/bind/named.conf
```

```
sudo /etc/init.d/bind9 reload
```

TRÈS IMPORTANT surtout si vous ne voulez pas utiliser les DNS de votre ISP:

Une fois la configuration de votre DNS effectué et testé, il faut mettre celui-ci actif sur votre réseau en modifiant /etc/network/interfaces et en indiquant aussi dans votre routeur les IP de vos DNS afin que tous les clients de votre réseau puissent interroger le DNS privé pour fonctionner avec les noms de machine au lieu des IP lors des connexions SSH et autres types.

```
nano /etc/network/interfaces
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5). # The
loopback network interface
auto lo
iface lo inet loopback # The primary network interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
```

```
address 192.168.0.10
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.1
dns-nameservers 192.168.0.10 192.168.0.12
#dns-nameservers
```

Redémarrer le réseau :

```
service networking restart
```

---

Pour la suite de la configuration:

[Outils de récupération de l'hébergement](#)