NAS – VirtualBox serveurs virtuels – Ubuntu 16.04.1

Présentation du projet

Afin de combler mon désir d'autonomie face à l'hébergement WEB et l'infonuagique, j'ai rassemblé ici un bon nombre d'informations pour réaliser soit même à la maison son hébergement web ainsi que le partage de contenu multimédia dématérialisé.

Vous trouverez dans ce document les instructions afin d'assembler les logiciels d'une machine hôte *UBUNTU 16.04 LTS* qui fournira des services de partage de fichiers et contenu multimédia pour un réseau domestique. De plus cet hôte assurera l'hébergement d'un système invité sous VirtualBox de Oracle.

La machine virtuelle et l'assemblage de celle-ci est détaillée dans un autre tuto qui fait suite à celui-ci. Afin de vous donner un aperçu des services, voici une liste des logiciels qui seront installés dans le système virtuel.

1. Devecot – Serveur de courriel IMAP
2. Postfix – Agent de livraison
3. Getmail – Récupérateur de compte POP externe (Gmail – Yahoo – FAI)
4. Amavis, Spamassasin, Clamav – Filtrage et antivirus
5. Bind – Serveur de nom primaire (DNS)
6. PureFTP – Serveur FTP
7. Apache2 – Serveur WEB
8. ISPConfig – System Provider (ISP) avec gestion d'usagers et domaines virtuels
9. OpenLDAP – Serveur d'annuaire (annuaire seulement)
10. Rsync – Sauvegarde des bases de données MySQL ainsi que les sites web pour une restauration d'urgence si nécessaire ou une migration de serveur
11. IMAPSYNC – Sauvegarde des comptes courriel externe (Gmail et Yahoo) vers un compte courriel local de notre serveur imap.

12. PHPmyAdmin (MySQL)
13. PHPldapAdmin (LDAP)
14. PhpVirtualBox seront également installées pour effectuer plus facilement la gestion de ces services

ISPConfig3 est le cerveau de ce système et c'est seulement à l'installation de celui-ci que l'ensemble des scripts de gestion des usagers virtuels sous MySQL sera mis en place automatiquement. L'apprentissage de ISPConfig est assez laborieux si vous n'avez jamais rien lu sur la configuration d'un serveur de nom (DNS).

Personnellement c'est ce que j'ai trouvé le plus difficile à apprendre. Je ne peux pas vraiment reproduire dans ce document les étapes d'entrées de données de ISPConfig, car le document d'aide doit être acheté sur howtoforge contre une somme minimale. Je dois vous aviser cependant que celui-ci n'est pas éloquent sur la façon de faire. Il faut lire ailleurs sur le web surtout pour le DNS pour arriver à faire quelque chose qui fonctionne. Je fournirai un exemple de fichier de zone DNS qui fonctionne afin de vous inspirer.

Cette portion du howto est une traduction et adaptation de: howtoforge_perfect-server-ubuntu-14.04-apache2-php-mysql-pureftpd-bind-dovecot-ispconfig-3.

Suivre le Serveur WEB ISPconfig – Ubuntu 14.04.1

Hôte – Serveur physique

Pré-requis important

Avant de vous lancer dans l'aventure, il faut posséder une adresse IP publique statique ou alors qui ne change vraiment pas souvent, car la propagation des adresses IP au travers des DNS peut prendre jusqu'à plusieurs jours.

Si vous désirez le faire en réseau local privé seulement alors il n'y a pas de problème, car votre adresse IP du réseau local pourra être statique facilement en configurant votre routeur domestique.

Le résultat n’est sûrement pas parfait, mais fonctionne bien et j’ai testé celui-ci sur plusieurs années.

Vous devrez être un peu débrouillard, car toutes les sections ne seront pas détaillées. Dans certains cas (comme l’installation de l’OS), seulement les particularités seront énoncées.

Services de l’hôte

Comme toute cette installation est à la maison, un serveur de fichiers ainsi que des services optionnels pour la diffusion de contenus stockés sur l’hôte pourront être installés au choix.

1. BIND – Serveur de nom secondaire privé (DNS)
2. Postfix – Agent de livraison de courriels satellite pour host1 (courriels internes de la machine, message d’application, etc.)
3. SAMBA – Serveur de fichiers (NAS) en partage SAMBA sur le réseau local.
4. NFS – Serveur de fichiers (NAS) en partage NFS sur le réseau local.
5. Logitech Media Server 7.9 – Serveur pour écoute de musique (mp3, flac, dsd, wav, ogg, aac, etc.) au travers des clients (Squeezebox ou piCorePlayer)
6. Mediatomb – Serveur DLNA pour les films sur le téléviseur HD via WD Live ou Kodi
7. BlissHQ – Organisateur de médiathèque de musique (complète les métadonnées des fichiers audio et organise).
8. Deluged – Serveur Bittorrent
9. SABnzbd – Client Usenet
10. Rkhunter – Vérificateur de rootkit sur les machines.
11. HDD 320GB – Données pour le serveur virtuel de courriel (ns1) et serveur virtuel web (ns1) afin d’éviter la croissance du disque dur de la machine virtuelle

---

Les irritants à contourner

Les fournisseurs bloquent des ports pour des raisons de sécurité et ou pour vous faire payer des forfaits affaire ou d'hébergement WEB.

Ports bloqués vers le FAI (Fournisseur Accès internet) :

- 25 = smtp
- 139 = bios
- 445 = smb
- 444

Ports bloqués venant du FAI :

- 25 = smtp
- 80 = http
- 135
- 161-162
- 389 = ldap
- 445
- 1080 = proxy

Mon FAI bloque les ports requis (25-80-389) entre lui et moi, je dois donc établir une redirection de certains ports dans la configuration de mon routeur:

- (8080) vers le port 80 pour les pages web
- (2525) vers le port 25 pour le serveur de courriel et le port
- (8085) vers le port 389 pour le serveur LDAP (pour un accès de l'extérieur à mon annuaire)

> *Afin de contourner le blocage du port 80, il est possible d'utiliser le port 443 pour les sites sécurisés (https://). Il faudra alors mettre en place les certificats requis (autosigné ou signé par une autorité de certification (COMODO).*

Après la configuration des serveurs, il est souhaitable de configurer certains paramètres dans le routeur.

1. Indiquer les DNS 192.168.0.10 et 192.168.0.12 (ainsi tous les clients du réseau vont interroger votre DNS public et privé afin de permettre que les noms de machines soient utilisés plutôt que des ip)
2. Indiqué le nom de domaine « reseau.maison »
3. Les redirections de ports (22,389,80,21,443,53,993,465,)

Les services payants requis

Pour avoir une redondance de DNS public, il faut 2 serveurs de nom pour le domaine. Comme il ne m'est pas possible d'avoir deux IP externes de mon FAI, j'ai donc décidé d'utiliser le service de DNS secondaire loué de dyn.com pour la redondance du DNS public.

Je veux la même redondance pour mon réseau local sans devoir publier mes informations locales dans le DNS public. J'ai donc recours à une machine virtuelle qui utilise la même carte réseau que la machine physique, mais configurée en pont. J'obtiens ainsi de mon routeur une autre adresse IP pour mon second serveur de nom privé.

J'ai acheté sur une base annuelle les services suivants de dyn.com :

- Secondary DNS qui se synchronise avec mon serveur DNS primaire.
- Nom de domaine (FQDN) infolaf.net

J'ai aussi acheté sur une base annuelle les services suivants de Duocircle.com :

- Email Gateway Domains qui permet de recevoir les courriels de mon domaine (infolaf.net) et les réacheminer sur le port 2525 (car le FAI bloque le port 25)

- Outbound SMTP qui permet d’envoyer les courriels de mon domaine (infolaf.net) via le port 465 en SSL (car le FAI bloque le port 25)

Voici un peu de détail sur la configuration à effectuer avec ces services.

> *Get started with DuoCircle Email Gateway*
>
> 1. *To finish allowing Duocircle Email Gateway to receive mail for your domain, you first need to have your MX records point to our mail servers: mx1.mailhop.org and mx2.mailhop.org. This can be done through your DNS provider.*
> 2. *If your mail server is using anti-spam settings or devices, you want to add our IPs in the « trusted forwarder » section of that server or device.*
> 3. *Then, once your server is setup and you have configured port forwarding in your router, you should be all set to receive email relayed through the Duocircle Email Gateway service.*
>
> *Get Started with Duocircle Outbound SMTP*
>
> 1. *Set outbound.mailhop.org as the Outgoing SMTP Server in your mail server or mail client*
> 2. *Make sure it authenticates with your Duocircle username and password (do not use your email address as the username)*
> 3. *You’ll need to set your server or client to connect to us on one of the following ports: 25, 2525, 10025, 465, 10465*
>
> *That’s all there is to it! Get Started with Dyn Secondary DNS*
>
> 1. *Configure your Primary nameserver to allow our nameservers to transfer your zone file. Our IPs are:*
>   - *204.13.249.76*

> - *208.78.69.76*
> - *91.198.22.76*
> - *203.62.195.76*
>
> 2. *Add NS records for our nameservers in your domain’s zone file. Our nameservers are:*
>   - *ns1200.dns.dyn.com 208.76.58.200*
>   - *ns2167.dns.dyn.com 208.76.59.167*
>   - *ns3173.dns.dyn.com 208.76.60.173*
>   - *ns4154.dns.dyn.com 208.76.61.154*
> 3. *Add our nameservers, as listed above, to the delegation of your domain through your registrar*
> 4. *Once the delegation change propagates and your Secondary DNS zone activates, you should see our servers query your primary server to retrieve your zone file.*

Le matériel

host1 : Ubuntu 16.04LTS

host1 est mon serveur physique qui servira d’hôte à ns1 qui tournera sur une machine virtuelle (VirtualBox).

Composantes matérielles de host1

1. SUPERMICRO MBD-X11SAE-M-O (motherboard), 2133MHz, Intel® E3-1200 v5 series, 6th Gen. Core i3/i5/i7
2. Intel Xeon E3-1230 v5 SkyLake 3.4 GHz 8MB L3 Cache LGA 1151 80W BX80662E31230V5 Server Processor
3. Crucial 32GB (2 x 16GB) 288-Pin DDR4 SDRAM DDR4 2133 (PC4 17000) Desktop Memory Model non-ECC CT2K16G4DFD8213
4. Carte vidéo Asus PCIE Radeon R5 230 1GB
5. Carte réseau Intel I219LM Gigabit Network Controller
6. Case ATX ANTEC SONATA
7. Ubuntu 16.04LTS sur disque Samsung SSD 850 EVO MZ-75E500 500GB SATA3

8. Données (nas1) sur disque HGST Ultrastar 7K6000 HUS726040ALE610 (0F23005) 4TB 7200 RPM 128MB Cache SATA 6.0Gb/s 3.5″ Enterprise Hard Drive
9. Données (nas2) sur disque Seagate 2TB SATA3 3.5″ Enterprise Hard Drive (RE3)
10. Données (nas3) sur disque Seagate 2TB SATA3 (RE3)
11. Données (mail & web) sur disque Western Digital 320GB SATA2 (WD3200YS RE)

Note d'installation

Sécurité des données:

Dans la première version de mon système, j'avais utilisé le RAID 5 logiciel pour la sécurité des données, mais maintenant (2016) les disques durs étant plus gros et abordable, je préfère plutôt utiliser RSYNC pour faire une sauvegarde régulièrement.

Choisir les adresses IP:

J'ai utilisé des adresses IPs statiques pour les serveurs. Il s'agit de choisir des adresses en dehors du champ d'action du serveur DHCP du routeur.

- ns1.infolaf.net = 192.168.0.10
- host1.reseau.maison = 192.168.0.12

Créer un média d'installation:

Afin d'installer Ubuntu 16.04 sur la machine physique (host1), récupérer d'abord l'ISO d'installation sur le site d'UBUNTU et copier celle-ci sur une clef USB comportant suffisamment d'espace:

```
sudo dd bs=4M if=[ur .iso] of=/dev/sd[that 1 letter]
```

```
sudo dd bs=4M if="/home/lafontaj/ubuntu-16.04.1-server-amd64.iso" of=/dev/sdc && sync
```

Créer les partitions:

Vous pouvez utiliser l'outil de partitionnement inclus avec Ubuntu mais de mon coté, je préfère créer les partitions avec gdisk à partir d'un autre ordinateur.

Je branche donc le nouveau disque SSD vierge via un adaptateur USB.

```
sudo apt install gdisk
```

Pour identifier le bon disque:

```
sudo fsisk -l
```

Supposons qu'il s'agit de sdc:

```
sudo gdisk /dev/sdc
```

En suivant l'excellent tuto de gdisk:« Partitioning Advice—General suggestions on how to lay out your GPT partitions »

- Créer une table des partitions de type gpt (automatique)
- Créer une première partition de 200M de type EFI
- Créer une 2e partition (/) espacé de +129M avec la 1er (début) de +25G de type Linux filesystem – 8300
- Créer une 3e partition (swap) espacé de +129M avec la 2e (début) de +64G de type Linux swap
- Créer une 4e partition (/home) espacé de +129M avec la 3e (début) et avec un espace à la fin de -129M de type Linux filesystem – 8300
- Appliquer les changements

Lors de l'installation d'UBUNTU, en mode manuel, il faudra simplement indiquer la fonction de chacune des partitions pour que le montage s'effectue correctement

1. /
2. swap
3. /home

Le formatage se fera lors de l'installation de Ubuntu.

Installation:

Assurez-vous que votre Bios est à jour et qu'il reconnaît bien votre processeur et mémoire vive.

Assurez-vous que votre Bios permet l'initialisation à partir du CDROM ou USB. Insérer la clef USB ou CD/DVD Ubuntu Linux et redémarrer l'ordinateur.

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): host1
```

Partitionnement des disques durs pour l'installation de l'OS, si vous n'avez pas utilisé l'outil gdisk alors suiver cette procédure sinon choissiser l'option manuelle.

Voici quelques explications d'appellation dans le monde Linux: Les disques s'appellent sda, sdb, etc. Les partitions s'identifient en ajoutant un chiffre au disque (sda1, sda2, sdb1, sdb2, etc.)

> *note: Si comme moi vous rencontrez des problèmes à cause d'un disque qui a déjà servi dans un ensemble RAID, il faudra sans doute utiliser la commande:*
>
> *mdadm --misc --zero-superblock /dev/sdd1*
> *sudo mkfs.ext4 -j /dev/sdd1*
> *sudo mkfs.ext4 -j /dev/sdd2*

L’outil de partitionnement s’ouvre.

Pour l’os :

```
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 chaque disque dur de donnée (nas1, nas2, nas3)

```
Choisir le disque souhaité: sdb
Choisir: partitionnement manuel
Choisir: ne pas formater ce disque (si données déjà présente, sinon choisir EXT4)
Choisir le point de montage: /media/nas1
Terminer le partitionnement pour ce disque.
```

Pour le disque de données (web et courriels)

Celui-ci n’est pas configuré sur la machine physique, mais le sera une fois sur Virtualbox en créant un fichier .vmdk (ceci sera expliqué plus loin)

```
Fuseau horaire:
Choisir: Toronto
```

```
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 Samba-server
```

Éjection du CD (automatique)

Redémarrage

La plupart des commandes qui suivent doivent être exécutées en mode super-utilisateur :

`sudo su`

Ubuntu 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 192.168.0.12)

(S.V.P., noter que j'ai remplacé *allow-hotplug eth0* avec *auto eth0* autrement le redémarrage du réseau ne fonctionnera pas et nous devrons 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
#allow-hotplug eth0
#iface eth0 inet dhcp
auto eth0
iface eth0 inet static
address 192.168.0.12
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*

> *note: Il est important de choisir un nom de domaine qui n'est pas réservé à moins d'en être le propriétaire (ex: .org, .com, .ca, etc.) . Moi, j'ai choisi un système avec une zone intranet distincte de la zone internet. Ainsi seulement certaine machine seront connu du monde extérieur.*

`nano /etc/hosts`

```
127.0.1.1 host1.reseau.maison
127.0.0.1 localhost.localdomain localhost
192.168.0.12 host1.reseau.maison host1
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Exécuter :

`echo host1.reseau.maison > /etc/hostname`

`service hostname restart`

Ensuite :

`hostname` `hostname -f`

Les deux commandes doivent retourner:

```
host1.reseau.maison
```

Mise à jour du système Ubuntu:

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

`apt update`

Pour appliquer les mises à jour, exécuter :

`apt full-upgrade`

Redémarrer le système si un noyau a été installé.

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 install ntp ntpdate`

Il est nécessaire de configurer un partage NFS pour Linux et Samba pour Windows ainsi que la gestion des permissions afin que l'utilisateur squeezeboxserver puisse écrire les listes de lecture et accéder aux répertoires et fichiers audio.

Le meilleur choix est par gestion d'ACL, suivre ce lien: *Partages ACL pour Linux et Windows*

Méthode alternative de contrôle des permissions par sgid, suivre le lien: *Partage NFS et Samba par sgid*

Installation de postfix mode satellite:

`apt install postfix`

Éventuellement, les DNS pointeront vers le serveur de courriel fonctionnel et celui-ci pourra être rejoint par les machines du réseau local à mail.reseau.maison

Deux questions vous seront posées, répondre comme suit :

```
General type of mail configuration : Satellite
System mail name: host1.reseau.maison
SMTP server: mail.reseau.maison
```

Éditer le fichier *main.cf*

`nano /etc/postfix/main.cf`

```
# See /usr/share/postfix/main.cf.dist for a commented, more complete version
# Debian specific: Specifying a file name will cause the first
# line of that file to be used as the name. The Debian default
# is /etc/mailname.
#myorigin = /etc/mailname
smtpd_banner = $myhostname ESMTP $mail_name (Ubuntu)
```

```
biff = no
# appending .domain is the MUA's job.
append_dot_mydomain = no
# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h
readme_directory = no
# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.
myhostname = host1.reseau.maison
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = host1.reseau.maison, localhost.reseau.maison, localhost
relayhost = mail.reseau.maison
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = loopback-only
```

Le nom de domaine (myhostname) correspond au nom de serveur de mail interne (host1.reseau.maison).

Le nom de domaine (mydomain) correspond à un domaine. (reseau.maison)

Les alias (alias_map) servent à simplifier l’écriture des en-têtes des courriers ainsi en tapant toto cela signifie pour le serveur de mail toto@ns1.reseau.maison.

On peut même rediriger le courrier de root vers sa propre adresse. C’est relativement intéressant, car certains programmes envoient des mails internes pour prévenir des défaillances (exemple fail2ban). Pour cela il faut ouvrir le fichier /etc/aliases, on voit apparaitre le nom de l’utilisateur et l’adresse email associée.

`nano /etc/aliases`

```
postmaster: root
root: postmaster@infolaf.net
nas: postmaster@infolaf.net
vmail: postmaster@infolaf.net
```

`newaliases`

Sur le courriel apparait le nom du serveur qui a envoyé le mail (myorigin). Ici c'est le nom de notre domaine situé dans /etc/mailname (host1.reseau.maison). C'est ce nom qu'il faudra modifier pour envoyer un mail.

mydestinations indique les autres noms possibles pour envoyer des courriels sur le réseau interne. Ainsi pour envoyer un courrier à toto, on peut écrire toto@host1.reseau.maison, mais aussi toto@localhost. Le courrier sera acheminé de la même façon.

`nano /etc/mailname`

ajouter :

`host1.reseau.maison`

`service postfix restart` ou `service postfix reload`

Pour voir si le SMTP-AUTH fonctionne correctement, exécuter la commande suivante:

```
telnet localhost 25
quit
```

À tester uniquement lorsque le serveur de courrier sur NS1 sera fonctionnel:

`sudo apt install mailutils`

`echo "test de host1" | mailx -s test root`

RKHUNTER: Installer sur host1 et ns1

Installation de RKHUNTER (cherche root kit) sur host1 :

`apt install rkhunter`

Modifier le fichier de configuration pour recevoir les courriels

`sudo nano /etc/rkhunter.conf`

```
MAIL-ON-WARNING=postmaster@infolaf.net
MAIL_CMD=mail -s "[rkhunter] Avertissements trouvés pour ${HOST_NAME}"
```

Éditer */etc/default/rkhunter*

`nano /etc/default/rkhunter`

```
# Defaults for rkhunter automatic tasks
# sourced by /etc/cron.*/rkhunter and /etc/apt/apt.conf.d/90rkhunter
#
# This is a POSIX shell fragment
#
# Set this to yes to enable rkhunter daily runs
# (default: true)
CRON_DAILY_RUN="true"

# Set this to yes to enable rkhunter weekly database updates
# (default: true)
CRON_DB_UPDATE="true"

# Set this to yes to enable reports of weekly database updates
# (default: false)
DB_UPDATE_EMAIL="true"
```

```
# Set this to the email address where reports and run output should be sent
# (default: root)
REPORT_EMAIL="root"

# Set this to yes to enable automatic database updates
# (default: false)
APT_AUTOGEN="true"

# Nicenesses range from -20 (most favorable scheduling) to 19 (least favorable)
# (default: 0)
NICE="0"

# Should daily check be run when running on battery
# powermgmt-base is required to detect if running on battery or on AC power
# (default: false)
RUN_CHECK_ON_BATTERY="false"
```

OpenSSH

`nano /etc/ssh/sshd_config`

```
PermitRootLogin prohibit-password
```

Configuration de Bind (host1)

La copie des zones privée et publique se fera automatiquement lorsque ISPConfig sera configuré sur NS1, mais il faut préparer le terrain pour que host1 accepte la connexion avec NS1

`sudo apt install bind9`

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

entre le serveur de nom primaire et secondaire.

`chmod 775 /etc/bind`

Apparmor fixe les droits d’accès des programmes, J’ai donc modifié la configuration de apparmor sur le serveur primaire (host1.reseau.maison) afin d’autoriser named à écrire dans le répertoire /etc/bind:

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

en remplaçant :

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

par

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

Sans oublier de relancer :

`sudo service apparmor restart`

Adapter selon vos besoins sur host1 :

`nano /etc/bind/named.conf.local`

```
// // 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; }; };
```

`nano /etc/bind/named.conf.options` `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; // };
//======================================================================== // If
BIND logs error messages about the root key being expired, // you will need to
update your keys. See https://www.isc.org/bind-keys
//========================================================================
dnssec-validation auto; auth-nxdomain no; # conform to RFC1035 listen-on-v6 {
any; }; allow-query { none; }; allow-recursion { 184.162.98.153; 192.168.0.0/24;
localnets; }; allow-transfer { none; }; };
```

Les fichiers suivants sont ici à titre d’exemple de fichiers fonctionnels. Ces informations doivent être ajouté à ISPConfig afin qu’il crée lui même les fichiers avec ses scripts internes.

```
/etc/bind/pri.reseau.maison
/etc/bind/pri.0.168.192.in-addr.arpa
/etc/bind/pri.infolaf.net
/etc/bind/pri.142.189.131.in-addr.arpa
```

/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
;

host1          3600     A            192.168.0.12
ns1            3600     A            192.168.0.10
routeur        3600     A            192.168.0.1
solydx-n73     3600     A            192.168.0.105
```

```
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           host1.reseau.maison.
reseau.maison. 3600     NS           ns1.infolaf.net.
```

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

```
$TTL 3600
@ IN SOA ns1.infolaf.net. postmaster.reseau.maison. (
2015020101 ; 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.infolaf.net.
@   3600     NS            host1.reseau.maison.
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           virtualbox.reseau.maison.
105 3600     PTR           solydx-n73.reseau.maison.
12  3600     PTR           nas1.reseau.maison.
```

/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-cbsc"
wordpress               3600     TXT "google-site-
verification=ejf0bw1nk0ebvfhmezpp6jielsnaeygxtvewdlvdmca"
```

/etc/bind/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.
153     3600     PTR    listes.infolaf.net.
153     3600     PTR    ftp.infolaf.net.
153     3600     PTR    mdp.infolaf.net.
153     3600     PTR    ns1.infolaf.net.
153     3600     PTR    pop.infolaf.net.
153     3600     PTR    imap.infolaf.net.
153     3600     PTR    ldap.infolaf.net.
153     3600     PTR    mail.infolaf.net.
153     3600     PTR    smtp.infolaf.net.
153     3600     PTR    nuage.infolaf.net.
153     3600     PTR    magasin.infolaf.net.
153     3600     PTR    photos.infolaf.net.
153     3600     PTR    webmail.infolaf.net.
153     3600     PTR    wordpress.infolaf.net.
```

Installer Logitech Media Server selon le HOWTO

Installer Mediatomb selon le HOWTO

Maintenant il est temps de passer à l’installation du serveur vituel pour ns1 :

Installer VirtualBox :

```
mkdir /home/nas/downloads
```

```
sudo su
```

Sous 16.04, les headers sont déjà installés, mais voici la commande au cas où:

```
apt install linux-generic linux-image-generic linux-headers-generic linux-signed-generic dkms
```

vous pouvez procéder à l'installation de VirtualBox de deux façons, mais la version des dépôts xenial est bogué au 2016-11-15.

```
apt install virtualbox
```

alors vous êtes mieux de télécharger la version du site Oracle, Windows 10 n'est supporté qu'à partir de la version 4.3.30.

```
cd /home/nas/downloads
```

```
wget http://download.virtualbox.org/virtualbox/5.1.10/virtualbox-5.1_5.1.10-112026~Ubuntu~xenial_amd64.deb
```

```
dpkg -i /home/nas/downloads/virtualbox-5.1_5.1.10-112026~Ubuntu~xenial_amd64.deb
```

Ajouter l'utilisateur VirtualBox (nas) au GROUP *vboxusers* et *disk* :

Avant de débuter, nous devons avoir l'assurance que l'utilisateur qui a lancé VirtualBox est un membre du groupe disk.

```
usermod -aG vboxusers nas
```

```
usermod -aG disk nas
```

Afin de pouvoir ajouter et démarrer des machines virtuelles, il faut ajuster les paramêtres de démarrage des interfaces VirtualBox. Si vous utilisez phpvirtualbox, le username est probablement vbox au départ. Si l'interface graphique VirtualBox est utilisée, vous utilisez alors le nom d'utilisateur qui est authentifié dans la session actuelle du bureau Linux

`sudo nano /etc/default/virtualbox`

```
VBOXWEB_USER=nas
VBOXWEB_HOST=192.168.0.12
```

L’étape suivante ne pourra être configuré qu’une fois le serveur web (NS1) lancé dans la machine virtuelle. Donc il faudra revenir à cette portion une fois phpvirtualbox installé sur le serveur web.

Configurer l’interface de phpVirtualBox sur le serveur web ou il est installé en modifiant le fichier *config.php* à l’aide de Filezilla.

```
/* Username / Password for system user that runs VirtualBox */
var $username = 'nas';
var $password = 'votremotdepasse';

/* SOAP URL of vboxwebsrv (not phpVirtualBox's URL) */
var $location = 'http://192.168.0.12:18083/';
```

De retour sur le serveur physique (host1)

`sudo service vboxweb-service restart`

Dans le cas actuel, le serveur web n’est pas encore en fonction, je vais utiliser des commandes à la console puisque j’utilise une version sans environnement de bureau.

Je suis authentifié sous le nom d’utilisateur root sinon faire:

`sudo su`

Installation du paquet d’extension pour l’USB :

```
VBoxManage extpack install --replace
Oracle_VM_VirtualBox_Extension_Pack-5.1.10-112026.vbox-extpack
```

Sortir de l’environnement super-utilisateur :

`exit`

Ensuite, il faut créer un système invité sous VitualBox :

La configuration du système invité choisi comporte deux disques durs virtuels :

1. 10G de type .vdi – dynamique pour l’OS
2. 320G de type .vmdk – (Raw hard drive) Disque physique branché à la carte mère comme /dev/sde pour le stockage des courriels et sites web.

```
VBoxManage createvm --name serveur-ubuntu-14.04.1_ns1.infolaf.net --ostype
Ubuntu_64 --register
```

```
VBoxManage createhd --filename "/home/nas/VirtualBox VMs/serveur-
ubuntu-14.04.1_ns1.infolaf.net/serveur-ubuntu-14.04.1_ns1.infolaf.net.vdi" --size
10240 --format VDI --variant Standard
```

Au moment de faire la commande suivante, il faut s’assurer de la carte réseau qui est en utilisation « eth0,eth1 ou eno1 » sur le serveur physique et adapter la commande suivante en fonction de celle-ci. À défaut de cela la machine virtuelle ne pourra se connecter au réseau. Il faut aussi adapter la quantité de mémoire à allouer à la machine virtuelle pour en laisser suffisamment à la machine hôte.

```
VBoxManage modifyvm serveur-ubuntu-14.04.1_ns1.infolaf.net --memory 3072 --boot1
disk --clipboard bidirectional --acpi on --ioapic on --cpus 2 --pae on --hwvirtex
on --hwvirtexexcl on --nestedpaging on --largepages on --vtxvpid on --rtcuseutc
on --vram 12 --accelerate3d off --vrde on --vrdeport 3389 --vrdeaddress
192.168.0.12 --floppy disabled --audio none --nic1 bridged --bridgeadapter1 eth0
--nictype1 82540EM --cableconnected1 on --usb off --macaddress1 0800279DDB6E
```

```
VBoxManage storagectl serveur-ubuntu-14.04.1_ns1.infolaf.net --name "Contrôleur
SATA" --add sata --controller IntelAhci --bootable on --portcount 2
```

```
VBoxManage storageattach serveur-ubuntu-14.04.1_ns1.infolaf.net --storagectl
"Contrôleur SATA" --port 0 --device 0 --type hdd --medium "/home/nas/VirtualBox
VMs/serveur-ubuntu-14.04.1_ns1.infolaf.net/serveur-
ubuntu-14.04.1_ns1.infolaf.net.vdi" --nonrotational on
```

Préparation du disque dur physique :

Afin d’identifier le bon disque

`sudo fdisk -l`

`parted /dev/sdf` (320GB)

```
mklabel gpt
mkpart mail
fstype : ext4
début : 0% (1 cylindre possible)
fin : 81920 (80GB)
mkpart web
fstype : ext4
début : 81920
fin : -1s (Ce qui reste)
```

Quitter parted et taper les commandes suivantes dans le shell:

`mkfs -t ext4 /dev/sdf1`

`mkfs -t ext4 /dev/sdf2`

La commande pour créer le disque dur physique de type .vmdk (Raw hard drive)

```
VBoxManage internalcommands createrawvmdk -filename "/home/nas/VirtualBox
```

```
VMs/serveur-ubuntu-14.04.1_ns1.infolaf.net/mail-web-sdf.vmdk" -rawdisk /dev/sdf
```

`chown nas:nas mail-web-sdf.vmdk`

```
VBoxManage storageattach serveur-ubuntu-14.04.1_ns1.infolaf.net --storagectl
"Contrôleur SATA" --port 1 --device 0 --type hdd --medium "/home/nas/VirtualBox
VMs/serveur-ubuntu-14.04.1_ns1.infolaf.net/mail-web-sdf.vmdk
```

Attacher le CD d'installation de Ubuntu: Télécharger l'iso de Ubuntu et sauvegardez le à un endroit accessible.

```
VBoxManage storagectl serveur-ubuntu-14.04.1_ns1.infolaf.net --name "Contrôleur
IDE" --add ide --controller PIIX4 --bootable on   VBoxManage storageattach
serveur-ubuntu-14.04.1_ns1.infolaf.net --storagectl "Contrôleur IDE" --port 0 --
device 0 --type dvddrive --medium "/home/nas/downloads/ubuntu-14.04.1-server-
amd64.iso"
```

C'est maintenant le temps de procéder l'installation de notre Ubuntu sur le système virtuel. Faite l'installation sur /dev/sda en utilisant tout l'espace disponible. Installez-y le boot loader lorsque le moment sera venu.

Démarrer la VM :

`VBoxHeadless -startvm serveur-ubuntu-14.04.1_ns1.infolaf.net &`

Pour voir la machine en action d'un autre poste de travail avec interface graphique:

`sudo apt install rdesktop` `rdesktop -a 16 -N 192.168.0.12:3389`

Pour éteindre la machine virtuelle, il est préférable d'éteindre avec un sudo poweroff dans la VM plutôt que d'utiliser la commande brutale suivante:

```
VBoxManage controlvm serveur-ubuntu-14.04.1_ns1.infolaf.net poweroff
```

Détacher le CD après l'installation : En général c'est automatique

```
VBoxManage storageattach serveur-ubuntu-14.04.1_ns1.infolaf.net --storagectl
"Contrôleur IDE" --port 0 --device 0 --medium "none"
```

> ## *Compactage du disque virtuel à l'occasion*
>
> *Dans la machine virtuelle, lancer la commande suivante dans le répertoire qui correspond au disque vdi à compacter:*
>
> `dd if=/dev/zero of=EMPTY bs=1M`
>
> *Ceci va remplir de zero l'espace vide il faut ensuite effacer le fichier EMPTY avec la commande suivante:*
>
> `rm EMPTY`
>
> *Il faut ensuite éteindre la machine virtuelle:*
>
> `sudo poweroff`
>
> *Ensuite sur l'ordinateur hôte lancer la commande pour compacter:*
>
> *Compacter le disque dur VDI:*
>
> ```
> VBoxManage modifyvdi "/home/nas/VirtualBox VMs/serveur-
> ubuntu-14.04.1_ns1.infolaf.net/serveur-ubuntu-14.04.1_ns1.infolaf.net.vdi"
> compact
> ```

Suivre le Serveur WEB ISPconfig – Ubuntu 14.04.1

Suivre le Outils de récupération de l’hébergement