Table des matières

[Configuration d’un serveur DNS primaire 2](#_Toc134105154)

[1. Vérifications préalables à l’installation 2](#_Toc134105155)

[Fichier ‘ hostname ’ 2](#_Toc134105156)

[Fichier ‘ hosts ’ 2](#_Toc134105157)

[Fichier ‘ interfaces ’ 3](#_Toc134105158)

[Fichier ‘ /etc/resolv.conf ’ 3](#_Toc134105159)

[2. Installation de BIND9 4](#_Toc134105160)

[Mise à jour 4](#_Toc134105161)

[Installation des paquets 4](#_Toc134105162)

[3. Compréhension du fonctionnement de BIND9 4](#_Toc134105163)

[Fichier ‘ named.conf ‘ 5](#_Toc134105164)

[Fichier ‘named.conf.options’ 5](#_Toc134105165)

[Fichier ‘named.conf.local’ 5](#_Toc134105166)

[Fichier ‘named.conf.default-zones’ 6](#_Toc134105167)

[4. Configuration de Bind9 7](#_Toc134105168)

[Fichier ‘ named.conf.local ‘ 7](#_Toc134105169)

[Création du fichier de zone interne 8](#_Toc134105170)

[Vérifications 11](#_Toc134105171)

[Paramétrer le serveur DNS sur les machines clientes 13](#_Toc134105172)

[Explication complémentaire 14](#_Toc134105173)

Objectifs :

Comprendre le fonctionnement d’un serveur DNS.

Être capable d’installer et de configurer un serveur DNS.

Être capable de lier une machine cliente à un serveur DNS.

Matériel à avoir :

Une machine Debian 11 « propre » qui servira de serveur DNS ainsi qu’une machine cliente Windows (OS au choix).

Consignes :

Installez les deux machines.

Configurez-les en IP fixe. Les machines doivent communiquer entre elles, et avoir accès à Internet.

Une fois cela effectué et vérifié par divers tests de ping, vous pouvez poursuivre ce TP.

# Configuration d’un serveur DNS primaire

DNS = Domain Name Server = Résolution de noms. L’une des deux machines Debian va devenir un serveur DNS, c’est-à-dire qu’il fera la translation entre une adresse IP et un nom de machine, et inversement.

Pour cela, il faut utiliser le paquet ‘Bind9’.

Avant de se lancer dans l’installation, il est essentiel de vérifier les fichiers de base, que vous devriez avoir vérifiés et modifiés si besoin juste après votre installation.

## Vérifications préalables à l’installation

Toutes les informations notées sur ce TP sont les miennes, à vous d’adapter les fichiers de configurations avec vos informations, tels que nom de machine, nom de domaine, adresse IP, sous réseau …

### Fichier ‘ hostname ’

Doit contenir le nom de votre machine.

srvdns

### Fichier ‘ hosts ’

Doit ressembler à cela, avec vos propres informations.

127.0.0.1 localhost.localdomain localhost

192.168.15.150 srvdns.pxvp.lan srvdns

La 2e ligne est obligatoire, afin que la machine qui devient serveur DNS puisse faire sa propre résolution de nom dans son domaine d’appartenance.

### Fichier ‘ interfaces ’

Doit ressembler à cela, avec vos propres informations.

auto eth0

iface eth0 inet static

address 192.168.15.150

netmask 255.255.255.0

gateway 192.168.15.254

### Fichier ‘ /etc/resolv.conf ’

Modifier le fichier resolv.conf afin qu’il ressemble à cela, avec vos informations.

Les paramètres signifient :

* nameserver : obligatoire : indique à la suite de ce paramètre les adresses IP des serveurs de noms utilisés sur cette machine. Une ligne nameserver par adresse IP. À noter que l’adresse IP du serveur DNS saisie en 1er, sera la 1ère interrogée, et ainsi de suite, donc mettez obligatoirement en 1er l’adresse du votre serveur DNS, à savoir votre Box, parce que vous avez besoin de recourir à la résolution de nom. Ensuite, lorsque vous aurez fini de transformer votre machine en un vrai serveur DNS, vous reviendrez sur ce fichier, et en tout premier, vous rajouterez une ligne nameserver cette fois-ci en mettant l’adresse IP de votre propre machine. Comme cela, ce sera elle qui sera utilisée pour la résolution de nom !
* search : optionnel : liste de recherche pour les noms d’hôtes. Par défaut, ne contiens que le nom du domaine local. On peut lister les chemins de recherche des domaines désirés, séparés par des espaces. Les noms de domaines saisis ici doivent être identiques à ceux saisis sur la ligne dns-search dans le fichier /etc/network/interfaces.
* domain : très optionnel : indique le nom du domaine local.

nameserver 192.168.15.254

nameserver 8.8.8.8

search pxvp.lan

domain pxvp.lan

Une fois tous ces fichiers vérifiés et modifiés, redémarrez les services correspondants. Ou redémarrez la machine si vous en avez la possibilité.

## Installation de BIND9

BIND 9 est un paquet pouvant être installé sur les machines Debian. Il permet de faire de ces machines des serveurs DNS.

### Mise à jour

Faites la commande suivante afin de mettre à jour le cache de votre machine, contenant les informations des paquets disponibles sur le miroir. Cela permettra d’installer le dernier paquet disponible.

apt update

Si besoin, faites un upgrade.

### Installation des paquets

Le paquet principal est bind9. Le paquet bind9utils est nécessaire pour garder une installation de BIND fonctionnelle, tandis que le paquet dnsutils est très pratique pour tester et débugger le service DNS.

apt install bind9 bind9utils dnsutils

Si vous voulez installer la documentation de BIND9, cela se fait avec le paquet bind9-doc.

À l’installation du paquet BIND9, le service associé s’est lancé automatiquement. Afin de pouvoir configurer le serveur BIND en toute tranquillité, il faut arrêter le service BIND9

systemctl stop bind9

## Compréhension du fonctionnement de BIND9

Les fichiers de configuration de Bind se trouvent dans /etc/bind.

Le fichier named.conf est le fichier de configuration principal de Bind.

Le fichier named.conf.options permet de définir toutes les options du serveur DNS.

Le fichier named.conf.local permet de déclarer toutes les zones locales du serveur DNS.

Le fichier named.conf.default-zones contient les zones par défaut. Nous n’y toucherons pas.

Regardons ces fichiers de configurations, et comprenons-les.

### Fichier ‘ named.conf ‘

Ce fichier est LE fichier de configuration de Bind. En réalité, tout est centralisé en lui, il indique à Bind qu’il doit utiliser les 3 autres fichiers que nous allons voir grâce à la commande « include ».

Il vous faut donc vérifier que les lignes include du fichier /etc/bind/named.conf ressemble à celles ci-dessous. Sinon, modifiez-les en conséquence, car sans l’un de ses fichiers, Bind aurait du mal à fonctionner correctement.

// This is the primary configuration file for the BIND DNS server named.

// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";

include "/etc/bind/named.conf.local";

include "/etc/bind/named.conf.default-zones";

### Fichier ‘named.conf.options’

Ce fichier permet de configurer les options de votre serveur DNS. Nous le configurerons plus tard, lorsque nous aurons besoin de sécuriser notre serveur. Le fichier par défaut, sans tous les commentaires, ressemble à ça :

options {

directory "/var/cache/bind";

dnssec-validation auto;

listen-on-v6 { any; };

};

Certains préfèrent travailler depuis le dossier /var/cache/bind plutôt que dans /etc/bind directement. C’est une question de préférence. La ligne directory, sert à indiquer de prendre en compte le dossier précisé. Sachant que la valeur par défaut est yes, dnssec-validation auto, autorise l’utilisation de dnssec qui permet de sécuriser les échanges DNS. Tandis que, la dernière option active la résolution DNS pour les adresses IPv6.

### Fichier ‘named.conf.local’

Ce fichier est par défaut uniquement composé de commentaires. Donc, il n’est pas actif.

Dès que nous passerons à la configuration, nous allons paramétrer ce fichier.

À l’intérieur, nous devrons déclarer les zones locales que nous utiliserons.

C’est-à-dire la zone directe de notre domaine, et si on en a besoin, la zone inverse, qui n’est pas obligatoire.

**Dans le cas où nous aurions le DNS à configurer pour plusieurs domaines, nous devrions déclarer une zone directe par domaine qui en a besoin.**

### Fichier ‘named.conf.default-zones’

Ci-dessous, vous trouverez le contenu de ce fichier.

Il permet d’indiquer à votre serveur où il doit trouver les informations concernant les zones par défauts, c’est-à-dire la zone racine « . », et les zones locales inverses, de transfert et broadcast.

Nous ne toucherons jamais à ce fichier.

// prime the server with knowledge of the root servers

zone "." {

type hint;

file "/etc/bind/db.root";

};

// be authoritative for the localhost forward and reverse zones, and for

// broadcast zones as per RFC 1912

zone "localhost" {

type master;

file "/etc/bind/db.local";

};

zone "127.in-addr.arpa" {

type master;

file "/etc/bind/db.127";

};

zone "0.in-addr.arpa" {

type master;

file "/etc/bind/db.0";

};

zone "255.in-addr.arpa" {

type master;

file "/etc/bind/db.255";

};

À présent, vous connaissez les 4 fichiers par défaut du DNS. Il vous faut les connaitre, et surtout savoir à quoi ils servent.

Passons à la configuration de notre serveur.

## Configuration de Bind9

Mettre en place un serveur DNS signifie mettre en place des zones qui permettent de réaliser une résolution de noms.

Nous allons configurer un serveur DNS classique. C’est-à-dire, simplement une zone directe qui permet de résoudre un nom de domaine en une adresse IP. C’est l’utilisation la plus courante.

Pour cela, nous allons, un peu plus tard, créer un fichier dit « de zone directe » dans lequel nous allons mettre en place son paramétrage et ses enregistrements. Mais ce fichier, le serveur DNS a besoin de savoir qui il est, et où il se trouve. Donc, pour cela, commençons par remplir le fichier de déclaration de zone locale, c’est-à-dire le fichier named.conf.local.

### Fichier ‘ named.conf.local ‘

Avant de le modifier, sauvegardez le fichier existant, par précaution.

mv /etc/bind/named.conf.local /etc/bind/named.conf.local.old

Créez un nouveau fichier vierge named.conf.local et configurez-le.

nano /etc/bind/named.conf.local

Dans ce fichier, nous déclarons la zone locale associée au domaine, et précisions le fichier dans lequel cette zone est paramétrée.

//Zone de résolution de domaine pxvp.lan

zone "pxvp.lan**.**"{

type master;

file "/etc/bind/db.pxvp.lan";

};

Il s’agit de déclarer un serveur DNS primaire, c’est-à-dire qu’il est le maître. A contrario des serveurs secondaire, esclave, qui ne sont qu’une copie, une sauvegarde du serveur primaire, et qui prendra le relais en cas de chute du premier.

Si vous avez besoin de créer une zone inverse (ce que nous ferons plus tard), il faudra l’indiquer ici, de la même façon. Avec son nom de zone et le fichier associé.

Dans le cas où vous souhaitez configurer une zone différemment des autres, avec d’autres options, vous pouvez directement les inscrire dans la déclaration de la zone correspondante, et non dans le fichier options, sinon elles s’appliqueront pour toutes les zones.

### Création du fichier de zone interne

Créez le fichier de zone interne ou zone directe, que vous avez indiqué sur la ligne ‘file’ dans le fichier named.conf.local.

nano /etc/bind/db.pxvp.lan

Remplissez ce fichier comme ci-dessous.

Vous devez comprendre ce fichier, savoir identifier et expliquer chaque paramètre, son utilité et sa configuration, et ainsi pouvoir adapter le fichier en fonction de vos besoins. Et surtout, savoir ce que vous faites ! Chaque paramètre de ces fichiers de configuration est très important. Vous devez les comprendre et les connaitre.

Pour chaque fichier de zone que vous rencontrerez, vous aurez une ligne qui s’appelle ‘serial number’. Vous devez y saisir un numéro qui servira de numéro de série à votre fichier. Par convention, on note ce numéro avec la date et l’heure de dernière modification, car le numéro de série DOIT CHANGER à CHAQUE MODIFICATION, s’il y a une erreur, cela permet de savoir sur quelle version du fichier. Et cela permet aussi à un serveur dns esclave, s’il a un numéro inférieur au maitre, de se mettre à jour. Exemple 2017100801 : Le 08 Octobre 2017 modification n°1.

; BIND fichier de résolution de zone interne;

$ORIGIN pxvp.lan.

$TTL 3D

@ IN SOA srvdns.pxvp.lan. email.pxvp.lan. (

2017100822 ;serial number

8H ;refresh

2H ;retry

4W ;expiration

3D ) ;minimum

@ IN NS srvdns.pxvp.lan.

srvdns IN A 192.168.15.150

;

serveur IN CNAME srvdns.pxvp.lan.

serveur IN CNAME srvdns

**Ces deux dernières lignes sont strictement équivalentes**. Elles permettent d’identifier votre machine sous le nom « serveur ». La deuxième ligne peut uniquement être écrite sous ce format raccourci, car au début du document nous avons configuré la variable $ORIGIN qui va rajouter son contenu automatiquement à la suite d’un nom. Cela permet de faciliter l’écriture et la lecture du document. Mais la première façon d’écrire est l’originale, la plus complète. Il s’agit du nom FQDN de la machine :

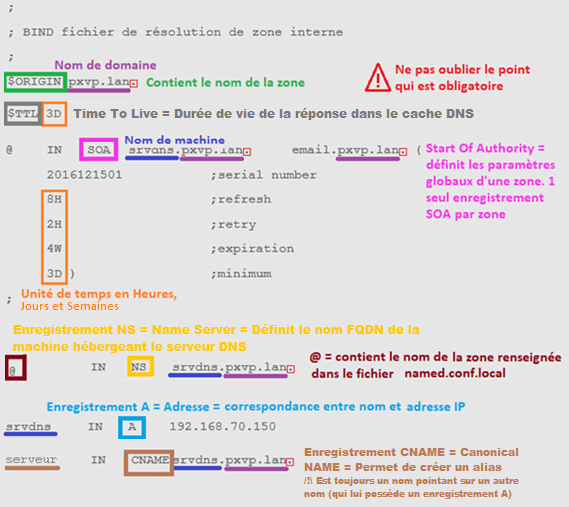
[nomdela machine].[nom du domaine].[tld].

À noter que le dernier point représente la racine, internet. Il ne faut surtout pas l’oublier.

**Attention, vous ne devez pas écrire les deux lignes. Cela provoquerait une erreur. Choisissez l’écriture que vous préférez et utilisez celle-là.**

L’enregistrement de type SOA, ou Start Of Authority, est l’enregistrement fondamental définissant des informations importantes faisant autorité sur la zone pour laquelle il est configuré : le @ en début de ligne, qui fait référence à $ORIGIN. Le premier nom qui est donné srvdns.pxvp.lan. définis quel est le FQDN du serveur de noms primaire (master) faisant autorité pour cette zone. Il doit correspondre à un enregistrement de type A, défini plus loin dans le fichier de zone (mais jamais à un CNAME (alias)). La valeur email.pxvp.lan. fais référence à l’adresse mail de contact pour cette zone (le @ de l’adresse mail est remplacé par un point).

Comme vu précédemment, le premier chiffre est le numéro de série du fichier.  
Le deuxième chiffre, 8H, refresh, est le time to refresh pour le serveur secondaire. Elle définit la fréquence à laquelle un serveur secondaire peut vérifier si le fichier de zone du serveur DNS maitre a été mis à jour.  
Le troisième chiffre, 2H, retry, est le time to retry. Lorsqu’un serveur DNS secondaire tente de vérifier auprès du DNS maitre si des mises à jour pour la zone sont disponibles (le time-to-refresh) mais que le maitre ne répond pas, le serveur secondaire tentera à nouveau la mise à jours au bout du temps indiqué par le time-to-retry.  
Le quatrième chiffre, 4W, expire, est le time to expire, qui définit le temps au bout duquel un serveur DNS secondaire cesse de résoudre les requêtes de la zone s’il n’arrive pas à joindre le serveur DNS maitre pour mettre à jour sa base de données avant le temps imparti.  
Le cinquième chiffre, 3D, minimum, c’est le minimum TTL, qui définit le temps avant qu’un serveur distant puisse réitérer sa requête s’il a reçu une réponse négative (NXDOMAIN ou NODATA) lors d’une requête DNS pour cette zone.

Petit récapitulatif du fichier, que vous pouvez compléter. Vous devez le comprendre et savoir de réexpliquer.

Par contre, bonne nouvelle, vous n’avez pas à le connaitre par cœur. Par exemple, quand vous avez une zone à créer, comme vous venez de le faire. Vous pouvez copier l’un des fichiers existants par défaut, par exemple le fichier « db.local » ou « db.empty » et modifier les informations à l’intérieur pour qu’il corresponde à votre attente !

# Vérifications

Vous venez de configurer votre zone directe et vous avez dit à votre serveur DNS où se trouvait ce fichier. À présent, il faut tester que votre serveur fonctionne.

Pour cela, avant de lancer ou relancer BIND, nous vérifions la validité de nos fichiers de configuration avec les deux outils fournis avec BIND :  *named-checkconf* et  *named-checkzone*. Vous devez connaitre ces commandes.

Vérification de la syntaxe des fichiers :

named-checkconf -z

Lisez bien les lignes que vous obtenez en résultat, s’il y a une erreur, elle sera identifiée ici. Si aucune erreur n’apparait, alors vos fichiers de configuration sont bons, sinon vérifiez l’erreur et corrigez-la redémarrer le service Bind, et relancer le test pour voir si tout est bon.

Si vous n’avez pas d’erreur, la commande devrait vous renvoyer cela :

zone pxvp.lan/IN: loaded serial 2016121501

zone localhost/IN: loaded serial 2

zone 127.in-addr.arpa/IN: loaded serial 1

zone 0.in-addr.arpa/IN: loaded serial 1

zone 255.in-addr.arpa/IN: loaded serial 1

Vérification de la zone interne :

named-checkzone pxvp.lan /etc/bind/db.pxvp.lan

zone pxvp.lan/IN: loaded serial 2016121501

OK

Après toutes ces modifications, il est temps de rallumer le service BIND9, si vous l’aviez bien éteint au début du TP. Sinon redémarrez-le.

sysetmctl start bind9

ou

systemctl restart bind9

Vérifier le statut du service, s’il y a des erreurs elles seront décrites à ce moment-là. Lisez bien les informations pour comprendre d’où pourrez venir l’erreur, et ensuite la corriger.

systemctl status bind9.service

● bind9.service - BIND Domain Name Server

Loaded: loaded (/lib/systemd/system/bind9.service; enabled)

Drop-In: /run/systemd/generator/bind9.service.d

└─50-insserv.conf-$named.conf

Active: active (running) since ven. 2017-09-15 18:36:46 CEST; 1min 10s ago

Docs: man:named(8)

Process: 525 ExecStop=/usr/sbin/rndc stop (code=exited, status=0/SUCCESS)

Main PID: 530 (named)

CGroup: /system.slice/bind9.service

└─530 /usr/sbin/named -f -u bind

sept. 15 18:36:46 srvdns.pxvp.lan named[530]: command channel listening on...3

sept. 15 18:36:46 srvdns.pxvp.lan named[530]: managed-keys-zone: loaded se...3

sept. 15 18:36:46 srvdns.pxvp.lan named[530]: zone 0.in-addr.arpa/IN: load...1

sept. 15 18:36:46 srvdns.pxvp.lan named[530]: zone pxvp.lan/IN: loaded ser...1

sept. 15 18:36:46 srvdns.pxvp.lan named[530]: zone localhost/IN: loaded se...2

sept. 15 18:36:46 srvdns.pxvp.lan named[530]: zone 127.in-addr.arpa/IN: lo...1

sept. 15 18:36:46 srvdns.pxvp.lan named[530]: zone 255.in-addr.arpa/IN: lo...1

sept. 15 18:36:46 srvdns.pxvp.lan named[530]: all zones loaded

sept. 15 18:36:46 srvdns.pxvp.lan named[530]: running

Hint: Some lines were ellipsized, use -l to show in full.

Le serveur DNS est bien configuré et bien actif, les vérifications sont correctes.

Testons à présent le bon fonctionnement du serveur, afin de vérifier qu’il joue bien son rôle.

Pour cela, en local dans une premier temps, indiquez dans le resolv.conf l’adresse IP de votre serveur DNS. Ensuite, utilisez dessus la commande dig, elle permet de diagnostiquer les dysfonctionnements dans la résolution de nom et de vérifier qu’elle fonctionne correctement.

dig srvdns.pxvp.lan

; <<>> DiG 9.9.5-9+deb8u14-Debian <<>> srvdns.pxvp.lan

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60019

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

;; QUESTION SECTION:

;srvdns.pxvp.lan. IN A

;; ANSWER SECTION:

srvdns.pxvp.lan. 259200 IN A 192.168.0.150

;; Query time: 2 msec

;; SERVER: 127.0.0.1#53(127.0.0.1)

;; WHEN: Fri Sep 15 18:41:20 CEST 2017

;; MSG SIZE rcvd: 77

Pour confirmer que cela fonctionne, vous devez avoir QUERY: 1, ANSWER: 1 et dans la partie ANSWER vous devez voir clairement la résolution de nom.

Bravo ! votre serveur DNS est maintenant fonctionnel, testez-le en condition réelle depuis votre machine cliente Windows ! Vous apprendrez par la suite à le sécuriser un peu plus et à créer la zone inverse qui est utilisée pour faire la résolution de l’adresse IP vers le nom de domaine.

# Paramétrer le serveur DNS sur les machines clientes

Pour faire cela, sur la **machine cliente** **Linux** qui va utiliser le serveur DNS, pensez à :

* Modifier le fichier ‘resolv.conf’
  + nameserver 192.168.15.150
  + search pxvp.lan

Pour tester que le DNS fonctionne, vous pouvez utiliser aussi la commande dig, mais il faudra au préalable installer le paquet dnsutils.

Sur la **machine Windows**, vous avez simplement besoin d’ajouter l’adresse IP du serveur en tant que DNS dans la configuration de votre carte réseau, et pour tester vous faites un ping vers le nom qui vous intéresse.

Sur le **serveur DNS**, pensez à :

* Rajouter à la fin du fichier de zone directe db.pxvp.lan une ligne par machine cliente qui utilisera le serveur DNS, avec la syntaxe suivante :

[nom\_machine\_cliente] IN A [@\_IP\_machine\_cliente]

N’oubliez pas de redémarrer le service BIND après y avoir apporté ces modifications.

Et pensez à réaliser à nouveau les différents tests entre vos deux machines clientes afin de savoir si elles arrivent à résoudre leurs noms respectifs.

# Explication complémentaire

Un serveur DNS a la possibilité d’avoir de nombreux enregistrements.

**Seuls les 4 enregistrements ci-dessous sont obligatoires,** que ce soit sur Windows ou sur Linux. C’est juste que sur Linux vous voyez le fichier en entier, et vous le manipulez vous-même. Alors que sur Windows c’est plus « caché ». Mais les deux serveurs DNS fonctionnent exactement de la même façon sur la configuration des zones.

