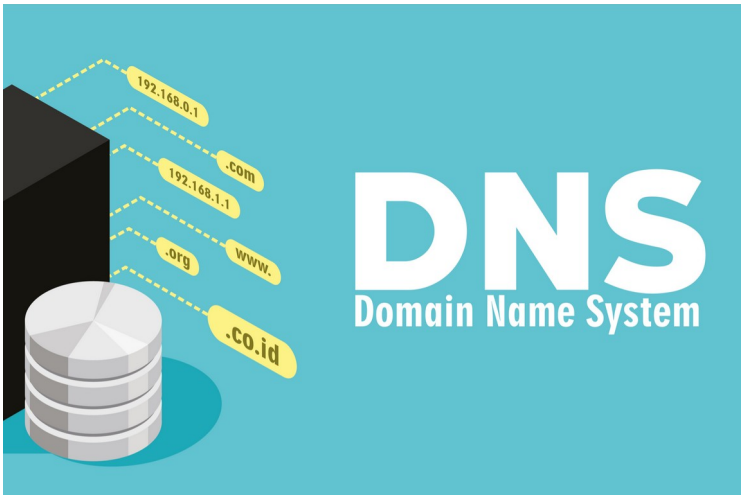
MODULE 9

Serveur DNS



Objectifs de ce module :

- ✓ ***Installation de bind***
- ✓ ***Configuration des fichiers reliés au serveur***
- ✓ ***Activer le serveur***
- ✓ ***Tester le serveur***

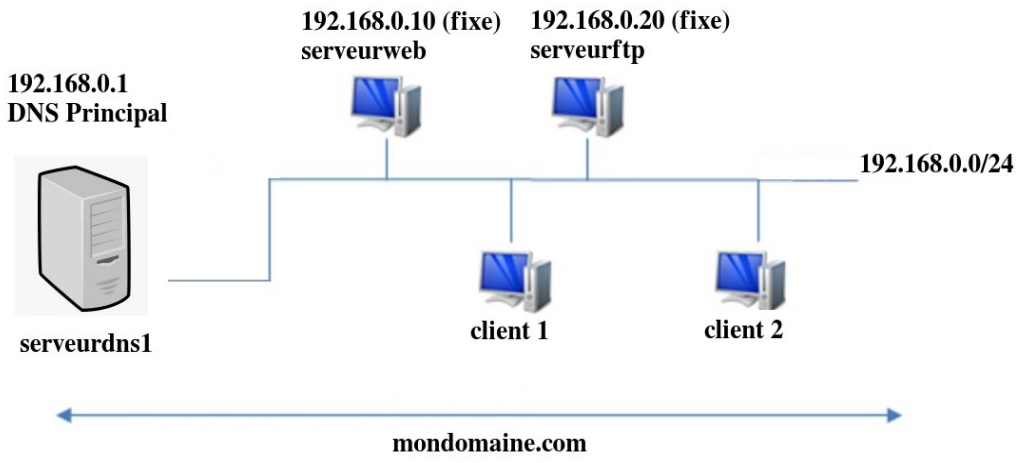
Table des matières

Introduction

Nous allons apprendre à mettre en place et configurer un service DNS sous Linux avec le paquet Bind. Pour ce faire, nous allons prendre le cas simple de la configuration d'un nom de domaine fictif pour un petit réseau(voir le schéma ci-dessous). Nous mettrons en place un nom de domaine qui pointera vers différents services tel qu'un serveur HTTP, un serveur Mail, ... etc. Il n'est pas nécessaire que ces services existent réellement.

Un serveur DNS (Domain Name System) est un serveur de noms qui gère les correspondances entre les noms de domaine et les adresses IP. Dans le cas d'un réseau local, si vous souhaitez faire de la résolution de noms, c'est à dire que les hôtes du LAN puissent communiquer entre eux grâce à leur nom de domaine, le serveur DNS permet de donner un nom de domaine complet à une machine. Ainsi, il y aura une correspondance entre l'adresse IP de l'hôte et le nom que vous lui donnez grâce au DNS.

Petit réseau pour lequel nous installerons un service de DNS



Un serveur principal pour le DNS local. Il pourrait y en avoir un autre qui sert de secondaire mais on ne l'installera pas ici. De plus, il pourrait, comme montré sur le schéma, y avoir d'autres ordinateur qui offrent des services spécifiques comme un serveur Web ou un serveur ftp qui pourraient obtenir des adresses IP fixes par exemple.

Les clients (client 1 et client 2, il pourrait y en avoir plus) sont des ordinateurs de bureau ou des portables. Pour notre exemple, cela importe peu car ces ordinateurs vont recevoir les informations de notre serveur DHCP et n'ont aucune autre configuration à faire.

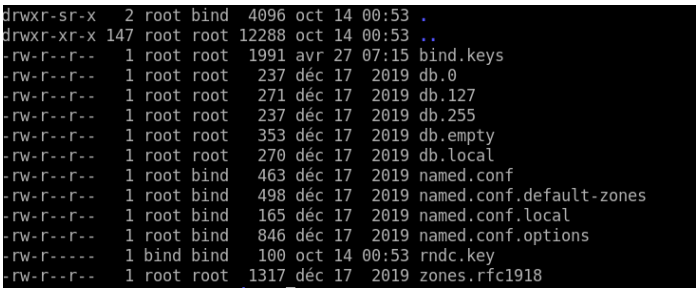
Installation du serveur Bind

La première étape à effectuer est évidemment d'installer le serveur DNS au moyen du paquet logiciel « bind9 » avec la ligne de commande suivante. (dnsutils ici permet d'installer également quelques outils supplémentaires comme nslookup et dig)

```
sudo  apt  install  bind9
```

Les fichiers de configuration du serveur se trouvent dans le répertoire **/etc/bind.**

Voici le contenu:



Les fichiers "**db**." correspondent aux fichiers de zones inclus par défaut dans **Bind**. Ils vont nous servir de modèle pour la création de nos fichiers de zones.

Le fichier "**named.conf**" est le fichier de configuration de Bind9, dans lequel on trouve un lien vers 3 autres fichiers :

- **named.conf.options** contient les options de configuration de Bind;
- **named.conf.local** sert à déclarer des zones et
- **named.conf.default-zones** contient la définition des zones incluses par défaut avec Bind.

Fichier de configuration de Bind

Le fichier se nomme named.conf.options et son contenu ressemble à ceci :

```
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;

	listen-on-v6 { any; };
};
```

- **directory** : il s'agit du chemin vers le répertoire qui contient les fichiers de zone. C'est-à-dire que lorsqu'on indique un nom de fichier de zone comme « **mondomaine.com** », Bind sait que le fichier se trouve dans « **/etc/bind** ».
- **dnssec-validation auto** : la valeur par défaut est auto, le **DNSSEC** est un système qui permet de sécuriser les échanges **DNS**.
- **listen-on-v6** : Active le fait de résoudre les requêtes sur des adresses **IPv6**.

Pour la plupart des configurations, ce fichier de base est suffisant et nous pouvons laisser la configuration telle quelle.

Les options intéressantes qui pourraient être ajoutées sont les suivantes :

- listen-on-port numero_du_port {nom_machine; adresse_reseau; };

ex. : Pour écouter sur le port 5353
listen-on-port 5353 {192.168.0.0/24;};

- allow-query {nom_machine; adresse_reseau; };
  Ex. : Pour permettre les requêtes provenant d'un sous-réseau particulier ou d'une machine particulière
  allow-query {serveurweb; 192.168.0.0/24;};

- forwarders {adresse_IP d'un autre DNS par défaut};
  Ex. : Pour faire en sorte que les requêtes non servies par notre serveur DNS soient redirigées vers un autre serveur DNS.
  fowarders { 8.8.8.8; 192.168.0.2;};

Les différentes zones

Il y a principalement 2 type de zones qui peuvent être résolues par un DNS. Il s'agit des zones directes et des zones inverses.

Les zones **directes** permettent de retrouver l'adresse IP à partir du nom tandis que les zones **inverses** permettent de retrouver le nom à partir de l'adresse IP, c'est à dire de faire l'inverse des zones directes. Ce qui permet une résolution dans les deux sens.

Étapes de configuration

Étape 1 : Configuration du fichier « named.conf.local » qui indique les deux zones majeures

Ici je vais créer mes zones, celles-ci seront « mondomaine.com » (mais vous pouvez modifier cette zone avec votre nom) et « 1.168.192.in-addr.arpa » (vous pouvez également adapter à votre situation en fonction de vos adresses réseaux).

Dans l'option file, vous devez indiquer les fichiers de zone que vous allez utiliser. Nous les utiliserons juste après. Le nom du fichier est libre à vous. Dans mon cas, j'utiliserai db.mondomaine.local et rev.mondomaine.local.

Allez dans le dossier **/etc/bind** et éditez le fichier **named.conf.local** et ajoutez-y l'information pour les 2 zones :

```
//La zone directe
zone "mondomaine.com"  {
  type master;
  file "db.mondomaine.local"; #Vous pouvez nommer ce fichier comme vous voulez.
  allow-update {none;};
};

//La zone inverse
zone « 0.168.192.in-addr.arpa"  {
  type master;
  file "rev.mondomaine.local";  #Vous pouvez nommer ce fichier comme vous voulez.
  allow-update {none;};
};
```

- **zone "mondomaine.com"**: On définit le nom de la zone. Cela correspond habituellement au nom du domaine.
- **type master** : On indique que ce serveur fait autorité principale sur la zone.
- **file "/var/cache/bind/db.mondomaine.local"** : On indique le lien vers le fichier contenant la base d'enregistrements pour la zone.
- **allow-update { none ;}** : On n'autorise pas les mises à jour du fichier d'enregistrements par un tiers, ce qui permet d'augmenter la sécurité et être sur qu'il n'y ait que le serveur DNS qui s'occupe de la zone.

Remarque : Il est important d'indiquer un point virgule à chaque fin de ligne pour la définition des options, sinon le fichier de configuration sera incorrecte pour Bind.

Étape 2 : Configuration du fichier de zone directe

Nous allons maintenant créer le fichier qui indique les informations pour la zone directe.

Vous devez éditer le fichier que vous avez inscrit dans la directive file associée à la zone directe. Dans notre exemple, ce fichier se nomme « db.mondomaine.local ».

Dossier des fichiers de zone

À des fins de maintenance, le service DNS s'attend par défaut à trouver les fichiers de zone dans le dossier « /var/cache/bind ». Nous allons laisser le défaut mais ça pourrait se changer assez facilement.

Nous allons copier un fichier qui se nomme « db.local » pour pouvoir partir avec un exemple que nous allons ajuster pour nos besoins.

```
cp  db.local    /var/cache/bind/db.mondomaine.local
```

Déplacez-vous dans le dossier **/var/cache/bind**
puis créez le fichier **db.mondomaine.local** qui est le fichier indiquant les informations pour la zone directe.

Entrez les lignes suivantes :

```
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.
;
$TTL    1d
@       IN      SOA     serveurdns1.mondomaine.com.  root.mondomaine.com. (
        2022000001              ; Serial
        1w                      ; Refresh
        1d                      ; Retry
        4w                      ; Expire
        1w )                    ; Negative Cache TTL

@       IN      NS      serveurdns1.mondomaine.com.
; les autres enregistrement de type A ici
; nom_ordinateur IN  A  Adresse_IP
serveurdns1             IN          A           192.168.0.1
serveurweb              IN          A           192.168.0.10
serveurftp              IN          A           192.168.0.20
; et ainsi de suite
; si on veut définir un enregistrement qui servira d'alias pour indiquer le serveur web, je peux utiliser CNAME
www                     IN          CNAME  serveurweb
```

- "**$TTL 86400**" correspond à la durée de vie des informations fournies et donc la durée pendant laquelle elles sont gardées en cache par les autres serveurs **DNS**. Par défaut, ce temps est définit sur 24 heures (86400 secondes). On peut également y indiquer l'information en nombre de jour (1d signifie donc 1 jour).

- "**SOA**" signifie **Start Of Authority**, ceci indique le serveur qui a autorité sur la zone, puis l'adresse mail du contact technique dont le caractère « **@** » est remplacé par un «.».

- **Serial** : C'est la version du fichier de configuration. Le **serial** est surtout utile quand plusieurs serveurs **DNS** agissent sur une même zone. Le **serial** est incrémenté lorsque des modifications sont effectuées sur la zone, ce qui permet aux autres serveurs **DNS** de voir que des modifications ont été effectuées. Pour les besoins de la démo, 2022 correspond à l'année et 000001 correspond à l'heure à laquelle le fichier a été édité (000001 correspond donc à minuit et 1 secondes. Ce qui ne correspond pas à la réalité. Vous pouvez effectivement mettre n'importe quel valeur ici.

- **Refresh "604800"** : C'est le délai de rafraîchissement pour la synchronisation des configurations entre plusieurs serveurs **DNS**.

- **Retry "86400"** : C'est le délai au bout duquel un serveur **DNS** secondaire devra retenter une synchronisation si celle qu'il a fait au bout du temps "**refresh**" a échouée.

- **Expire "2419200"** : Si toutes les tentatives de synchronisation échouent, un serveur **DNS** secondaire considérera qu'il ne peut plus répondre aux requêtes concernant cette zone une fois que le temps est écoulé. Par défaut le temps est de "**2419200**" secondes, soit 28 jours.

- **Negative Cache TTL "86400"** : Durée de conservation dans le cache de l'information "**NXDOMAIN**" lorsqu'un incident se produit.

- Le symbole "**@**" : Ce symbole permet de représenter le nom de domaine de la zone. Par exemple, dans notre cas lorsqu'on met "@" c'est comme si on utilisait "mondomaine.com".

Les types d'enregistrement

Il y a plusieurs types d'enregistrements qui ont chacun un rôle différent :

- **NS (Name Server)** : Sert à définir le ou les serveurs **DNS** qui répondent à cette zone.

- **A** : Enregistrement d'un hôte ayant une adresse IPv4 (32 bits).

- **AAAA** : Enregistrement d'un hôte ayant une adresse IPv6 (128 bits).

- **CNAME (Canonical Name)** : Enregistrement qui sert d'alias à un enregistrement "A" déclaré auparavant.

- **MX** : Sert à définir le ou les serveurs **SMTP** à utiliser pour l'envoi du courriel selon un ordre de priorité définit dans l'enregistrement.

- Dans notre cas, nous avons besoin de créer des enregistrements de type "**A**" et "**CNAME**", l'enregistrement de type "**NS**" étant déjà définit par défaut.

Étape 3 : Configuration du fichier de zone inverse

Maintenant que notre première zone fonctionne, nous allons créer la zone inverse à celle-ci c'est-à-dire celle qui permettre de retrouver le nom « **serveurdns1.mondomaine.com**» à partir de l'adresse IP « **192.168.0.1** ».

Encore une fois, nous allons partir d'un fichier déjà fait :

```
cp  db.local  /var/cache/bind/rev.mondomaine.local
```

On édite le fichier pour s'assurer que les informations correspondent à notre domaine :

```
$TTL    86400
@       IN      SOA     serveurdns1.mondomaine.com.  root.mondomaine.com. (
        2022000002              ; Serial
        1w                      ; Refresh
        1d                      ; Retry
        4w                      ; Expire
        1w )                    ; Negative Cache TTL

@       IN      NS      serveurdns1.mondomaine.com.
@       IN  PTR         mondomaine.com.
; Les enregistrements de type PTR ici
1       IN  PTR         serveurdns1.mondomaine.com.
10      IN  PTR         serveurweb.mondomaine.com.
; d'autres ordinateurs spécifiques au besoin ici
```

Étape 4 (optionnelle) : Vérification de la configuration

Avant de lancer le service et de commencer à utiliser notre serveur DNS, il convient de s'assurer que l'on n'a rien oublié et que le paramétrage ne contient aucune erreur.

Vérifier le fichier de configuration principal

On peut vérifier la configuration avec la commande « named-checkconf fichier_de_config »

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

Évidemment, remplacez le fichier named.conf.local par le nom que vous aurez choisi.

Si tout se passe bien, on ne devrait pas avoir de message d'erreur. Sinon, il faut scruter les journaux de logs et voir ce qui ne va pas.

Vérification de la configuration des fichiers de zone

Ensuite, on peut passer à la vérification de la configuration, zone par zone. On peut donc vérifier la zone directe ainsi que la zone inverse. La commande se nomme « named-checkzone nom_zone fichier_de_la_zone ».

Pour vérifier le fichier de la zone directe dans l'exemple que nous avons fait :

```
sudo named-checkzone mondomaine.com /var/named/bind/db.mondomaine.local
```

Si tout va bien, vous obtiendrez quelque chose de similaire à :

zone mondomaine.com/IN: loaded serial 2022000001
OK

Et pour vérifier la zone inverse :

```
sudo named-checkzone 0.168.192.in-addr.arpa /etc/named/bind/rev.mondomaine.local
```

Encore là, vous obtiendrez le message que tout est OK si il n'y a pas d'erreur.

Lorsqu'il y a une erreur, généralement les messages sont suffisamment claires pour que vous puissiez corriger le problème et relancer le service.

Pour redémarrer le service :

```
systemctl restart bind9

Et pour le démarrer à chaque démarrage de l'ordinateur : systemctl enable bind9
```

Étape 5 : Configuration des paramètres réseaux du serveur

Vous n'aurez plus besoin de ce qu'il y avait dans le fichier /etc/hosts à partir de maintenant.

Enlever toutes les lignes du fichier /etc/hosts qui contiennent la correspondance adresse_IP et nom de machine.
Garder uniquement la ligne du localhost. Ceci dit, vous pouvez garder le fichier hosts tel quel car il s'agit simplement de spécifier dans le fichier nsswitch.conf qui est charge en priorité de la résolution de nom.

Étape 5.1 : Modifier le fichier resolv.conf

Au début, le serveur avait nécessairement un serveur DNS de déclaré pour pouvoir télécharger les paquets, maintenant qu'il est lui-même serveur DNS, nous devons le lui dire. Pour cela, on modifie le fichier « head » se situant dans le dossier « /etc/resolvconf/resolv.conf.d » :

cd /etc/resolvconf/resolv.conf.d
Éditez le fichier « head » pour y ajouter les lignes suivantes :

```
search mondomaine.com          # Domaine de recherche
domain mondomaine.com          # Domaine
nameserver 192.168.0.1         # Serveur DNS (lui-même)
```

Redémarrez le service resolvconf : systemctl restart resolvconf

Étape 5.2: Rendre permanent les modifications dans le fichier resolv.conf

Même si vous changez le contenu du fichier resolv.conf situé dans le dossier /etc, celui-ci risque d'être réécrit pas dessus par le système au démarrage de d'autres services reliés au réseau. De façon à rendre permanent les changements de l'étape précédente, réalisez les commandes suivantes :

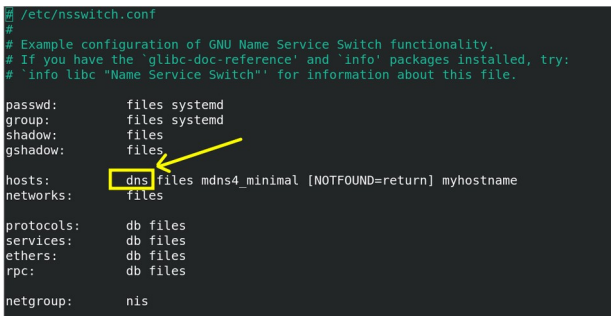
```
resolvconf --enable-updates
resolvconf -u
```

La dernière commande effectue la modification permanente.

Étape 5.3: Ne pas oublier de modifier le fichier nsswitch.conf

N'oubliez pas que le fichier nsswitch.conf, dans le dossier /etc, est responsable de la résolution de nom. Si vous ne le changez pas, toutes vos configuration aussi sophistiquées qu'elles soient n'auront aucun effet. Il faut donc vous assurer d'indiquer à nsswitch.conf que c'est maintenant votre serveur dns qui est en charge et non le fichier hosts.

Assurez-vous que l'option « dns » figure au début comme dans la ligne ci-dessous et encadrée :



Configuration des paramètres réseaux des clients

Les clients n'auront pas grand chose à faire.

Assurez-vous d'enlever les lignes du fichier /etc/hosts s'il y en avait. Ne gardez que celle qui désigne le localhost.

Clients avec adresse dynamique:

- Si les clients reçoivent l'information d'un DHCP, ils n'ont rien à faire. Les informations seront changées dans le DHCP pour refléter l'arrivée de notre serveur DNS.

Clients avec adresse statique:

On suppose ici que les clients ont activé le service networking et installé le service resolconf précédemment.

- Si les clients ont des adresses fixes, on pourra changer la ligne dns-nameserver dans les fichiers de configuration des cartes réseaux.

Par exemple, si la carte se nomme enp0s3, on va dans le fichier ifcfg-enp0s3 et on change la ligne dns-nameserver

dns-nameserver adresse_IP_de_notre_serveur_DNS

De plus, ajoutez les lignes suivantes dans le fichier « head » situé dans le dossier /etc/resolvconf/resolv.conf.d

et ajoutez-y les lignes suivantes :

```
search mondomaine.com          # Domaine de recherche
domain mondomaine.com          # Domaine
nameserver 192.168.0.1         # Serveur DNS du réseau
```

Repartez le service resolvconf : systemctl restart resolvconf

Et n'oubliez pas d'effectuer les mêmes opérations que les étapes 5.1 à 5.3.