UNIVERSITE ASSANE SECK DE ZIGUINCHOR
♦◊♦♦◊♦♦◊♦◊♦
UFR Sciences et Technologies
♦◊♦♦◊♦
Département d'informatique

TP1 : Configuration d'un serveur de nom

Objectifs du TP

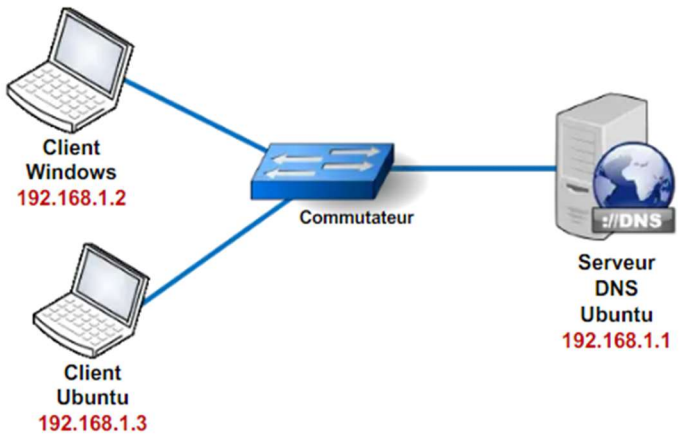
- Installer et configurer un serveur maitre dans un LAN
- Faire des résolutions de noms et inverses

Environnement du TP

Pour ce TP, nous allons avoir besoin d'au moins :

- Une machine Linux (Ubuntu ou Debian) où sera hébergé le serveur
- Un client Windows
- Un client Linux

1. Plan de configuration



Nom de domaine : l2i.sn

Noms	Adresse IP
Serveur.l2i.sn	192.168.1.1
Machine1.l2i.sn	192.168.1.2
Machine2.l2i.sn	192.168.1.3

2. Installation du serveur Bind9

BIND (Barkeley Internet Name Domain) est un logiciel open source permettant de publier le système de noms de domaine associé à un LAN et de résoudre les requêtes DNS pour ses utilisateurs. C'est le logiciel DNS le plus utilisé sur Internet spécialement sur les systèmes de type UNIX. Il existe des alternatives à BIND comme **DJBdns** ou **MaraDNS**, qui sont souvent réputés plus sécurisés mais ils sont beaucoup moins utilisés.

- Pour installer BIND, tapez la commande

apt-get install bindo dnsutils bind9-doc

Cette commande installe BIND(bind9), le client permettant de le tester(dnsutils) et des documentations sur BIND(bind9-doc).

- Pour vérifier que Bind est bien installé, tapez

apt-cache show bind9

3. Creation de la zone principale

La zone principale permet de faire pointer un FQDN sur une adresse IP. Un FQDN a la forme **hote.domaine.extension** :

- **hôte** correspond au nom d'hôte d'une machine faisant partie du domaine
- **domaine** correspond au nom du domaine
- **extension** correspond à l'extension (.sn par exemple)

Dans notre cas, nous avons :

- Le nom du domaine : **l2i**
- Extension : **.sn**
- Le FQDN du serveur DNS : **serveur.l2i.sn**
- Le FQDN de la machine Windows : machine1.l2i.sn
- Le FQDN de la machine Linux : machine2.l2i.sn

La création d'une zone se fait dans le fichier de configuration locale BIND : **/etc/bind/named.conf.local.**

C'est dans ce fichier que nous déclarons les zones associées au domaine (directes ou inverse). Chaque zone crée, doit être associée à un fichier de description.

- Placez-vous sous **/etc/bind**
- Editez le fichier **named.conf.local**
- Saisissez le bout suivant (respectez la syntaxe)

```
        zone    "l2i.sn"        IN {
    type master;
    file    "/etc/bind/db.l2i.sn"
};
```

L'option type a la valeur master pour indiquer que le serveur sur lequel nous travaillons est le maitre de la zone l2i.sn et l'option file indique le chemin vers le fichier de configuration de la zone, que nous allons créer. Le fichier db.léi.sn contiendra les détails des machines du domaine.

Les options les plus courantes de la déclaration de zone comprennent :

- allow-query spécifie les clients qui sont autorisés à requérir des informations à propos de cette zone. Par défaut, toutes les requêtes d'informations sont autorisées.
- allow-transfer spécifie les serveurs esclaves qui sont autorisés à requérir un transfert des informations de la zone. Par défaut, toutes les requêtes de transfert autorisées.
- allow-update spécifie les hôtes qui sont autorisés à mettre à jour dynamiquement des informations dans leur zone. Par défaut, aucune requête de mise à jour dynamique n'est autorisée.

4. Configuration de la zone principale

Dans le dossier /etc/bind/, il existe un fichier db.local qui est un exemple de fichier de configuration.

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serie
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

Le point-virgule (;) est un commentaire.

$TTL (Time to Live)	Nombre de secondes pendant lesquels les informations de la zone peuvent être considérées comme valides et être mises en cache. A la fin du temps le fichier sera relu par BIND (vaut 7 jours dans l'exemple).
Serie	Numéro de série à changer à chaque modification du fichier si vous possédez au moins un serveur esclave, pour qu'il puisse prendre en compte les modifications sur le serveur maître. Le standard est de renseigner la date de la modification du fichier (YYYYMMDDn)
Refresh, Retry, Expire	Délais en secondes qui vont piloter le comportement des serveurs esclaves. A l'expiration du délai Refresh, l'esclave va entrer en contact avec le maître. S'il ne le trouve pas, il essaiera de nouveau à la fin du délai Retry et si, au bout du délai Expire, il n'est pas parvenu à ses fins, il considérera que le serveur maître a été retiré du service.
Negative cache TTL	Utilisé pour spécifier, en secondes, la durée de vie pendant laquelle sont conservées en cache les réponses qui correspondent à des demandes d'enregistrements inexistants.

Il faut faire une copie du fichier db.local dans db.l2i.sn pour la configuration

- **cp /etc/bind/db.local /etc/bind/db.l2i.sn**

Editer le fichier db.l2i.sn et ajouter les enregistrements relatifs à la zone.

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     serveur.l2i.sn. root.serveur.l2i.sn. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      serveur.l2i.sn.
@       IN      A       192.168.1.1
serveur IN      A       192.168.1.1
machine1 IN     A       192.168.1.2
machine IN      CNAME   machine1
serveur IN      CNAME   dns
```

Un fichier zone doit toujours commencer par la définition du SOA (Start Of Authority) :

- « @ » spécifie la zone définie dans le fichier de configuration
- « IN » précise qu'il s'agit d'une zone Internet, il s'agit presque de la valeur par défaut
- Ensuite on précise le mot clé SOA suivi du FQDN du serveur qui heberge la zone (serveur.l2i.sn.)

- Puis, sur la même ligne une adresse email de contact (email@l2i.sn)

Attention ; Les « . » à la fin de serveur.l2i.sn. et email@l2i.sn. Sont obligatoires !

Tout de suite après l'enregistrement SOA, il faut préciser le serveur DNS à consulter : la machine serveur.l2i.sn est un serveur de nom (NS=Name Server) pour la zone.

Ensuite, nous avons la définition des machines du réseau. Chaque ligne précise : le nom du pc-le type de zone-le type d'enregistrement-l 'adresse IP de la machine.

L'association du nom d'une machine à son adresse IP se fait de la manière suivante :

- **Nom_hote IN A ip_hote**

Enregistrez les modifications.

5. Vérification des fichiers de configuration

Pour voir si le fichier **named.conf.local** ne comprend pas d'erreur, on tape la commande

- **named-checkconf /etc/named.conf.local**

Si aucun message n'apparait, c'est qu'il n'y a aucune erreur.

Pour lr fichier zone, on utilise la commande :

- **named-checkzone l2i.sn /etc/bind/db.l2i.sn**

Si aucun message n'apparait, c'est qu'il n'y a aucune erreur.

Redémarrez le service bind9. Il doit etre redémarré à chaque modification, pour qu'elle prise en compte.

Testez la résolution de nom (renseignez-vous sur dig : man dig)

- **dig @192.168.1.1 l2i.sn**

Le serveur DNS doit retourner l'adresse IP de votre serveur maitre.

La section AUTHORITY SECTION indique le FDDN du serveur faisant autorité pour répondre aux requêtes concernant ce nom de domaine et la section ADDITIONAL SECTION indique l'adresse IP du serveur faisant autorité pour répondre aux requêtes concernant ce nom de domaine.

- **dig @192.168.1.1 machine1.l2i.sn**

Le serveur DNS doit retourner l'adresse IP associé à la machine machine1.

6. Création de la zone inversée

Dans une zone reverse, la résolution de nom se fait à l'envers. C'est-à-dire que l'on demande au serveur DNS de renvoyer le FQDN d'une machine à partir de son adresse IP.

Pour créer la zone inversée, vous aurez besoin de l'adresse du réseau pour lequel le serveur devra résoudre les adresses IP.

Nous considérons le réseau 192.168.1.0/24.

Editez le fichier named.conf.local et renseignez une nouvelle zone (inversée) de la manière suivante :

```
zone "1.168.192.in-addr.arpa" IN {
      type master;
      file "/etc/bind/192.168.1";
};
```

Pour le nom de la zone, vous devez renseigner les 3 premiers octets de l'adresse réseau à l'envers, suivi du nom de **.in-addr.arpa**. la zone **in-addr.arpa** permet la résolution inversée.

Enregistrez les modifications.

7. Configuration de la zone inversée

Créez le fichier de description de la zone inversée, en faisant une copie du fichier de description de la zone principale :

- **cp /etc/bind/db.l2i.sn /etc/bind/192.168.1**

Editez le fichier de description crée et l'adaptez de la manière suivante

```
;
; BIND data file for local loopback interface
;
$TTL   604800
@      IN      SOA                    serveur.l2i.sn.    email@l2i.sn.          (
                201809121      ; Serial
                  604800       ; Refresh
                   86400       ; Retry
                 2419200       ; Expire
                  604800 )     ; Negative Cache TTL
;
@      IN      NS      serveur.l2i.sn.

1      IN      PTR     serveur.l2i.sn.
2      IN      PTR     machine1.l2i.sn.
3      IN      PTR     machine2.l2i.sn.
```

L'association de l'adresse IP d'une machine à son nom se fait de la manière suivante :

- **IP IN PTR FQDNMachine**

Le nombre au début de chaque ligne correspond au dernier octet de l'adresse IP d'une machine du LAN.

PTR (Point Record) permet d'effectuer des inversement d'enregistrement A ou AAAA et de donner le nom d'hôte associé à l'adresse IP à résoudre.

Remarquez le « . » en fin du FQDN.

Enregistrez les modifications et vérifiez la syntaxe :

- **Named-checkzone 1.168.192.in-addr.arpa /etc/bind/192.168.1**

Redémarrez le service bind9

Testez la résolution d'adresse IP :

- **dig @192.168.1.1 -x IPMachine**

Exemple : IPMachine=192.168.1.2

Attention à ajouter l'option **-x** à la commande **dig** pour pouvoir demander au serveur DNS de résoudre une adresse IP.

Vérifiez le résultat sous ANSWER SECTION.

8. Tests du serveur DNS

8.1 Configuration des clients

a. Cas du client linux

Il faut d'abord indiquer à la machine l'adresse du serveur DNS à consulter. Pour cela, il suffit d'éditer le fichier **/etc/resolv.conf.**

```
search      l2i.sn
nameserver 192.168.1.1
```

La commande search indique que si un nom de domaine n'est pas trouvé, il faudra essayer en lui ajoutant .l2i.sn.

b. Cas d'un client Windows

Il suffit de spécifier l'adresse du serveur BIND (à savoir 192.168.1.1) comme serveur DNS primaire au niveau de la configuration de la carte réseau.

8.2 Test : NSLOOKUP

Deux commandes peuvent être utilisées pour la résolution de noms : dig (Linux) et nslookup(Windows/Linux).

1. Pour faire l'essai de résolution directe, il suffit d'utiliser la commande :
   - **nslookup machine2.l2i.sn**
2. Pour tester la résolution inversée, il suffit d'utiliser la commande :
   - **nslookup 192.168.1.2**