



**OFPPT**

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle  
et de la Promotion du Travail

Complexe de Formation dans les Métiers des Nouvelles Technologies de l'Information, de  
l'Offshoring et de l'Electronique -Oujda

**Module : Administration d'un Réseau sous Linux**

## **Installation et configuration du serveur DNS sous Centos**

**Formatrice : ZITI Iham**

## Sommaire

1.	Introduction.....	3
2.	Installation du serveur DNS.....	3
2.1	Vérification de l'installation.....	3
2.2	Lancement du serveur DNS.....	3
2.3	Vérification le démarrage de serveur DNS .....	3
2.4	Activer le lancement au démarrage .....	3
3.	Configuration.....	4
3.1	Configuration de base.....	4
3.2	Configuration d'un serveur DNS primaire (maître) .....	4
a.	Zone directe.....	4
b.	Zone inverse .....	5
3.3	Configuration de la zone DNS.....	6
3.4	Vérification de la configuration.....	9
4.	Tests de configuration.....	9
4.1	nslookup.....	10
4.2	dig .....	11
4.3	host.....	11
5.	Configuration serveur secondaire.....	11
5.1	Configuration du serveur primaire.....	12
5.2	Configuration du serveur secondaire .....	12
5.3	Test.....	12
6.	Déléguer une zone d'un sous domaine .....	13
7.	Configuration de la journalisation.....	13
8.	Référence :.....	14

## 1. Introduction

Voir le cour **Mise en place du serveur DNS sous Windows Server 2012r2**

## 2. Installation du serveur DNS

Le paquetage qui régit l'installation du serveur DNS sous Linux s'appelle **bind**.  
Installons Bind grâce à la commande yum, dnf ou rpm

```
# yum -y install bind
```

```
#dnf -y install bind bind-utils
```

```
#rpm -ivh bindxxxxxxx.rpm
```

### 2.1 Vérification de l'installation

Pour vérifier l'installation du serveur DNS on utilise la commande suivante

```
# rpm -aq bind
```

### 2.2 Lancement du serveur DNS

La commande suivante permet de démarrer le serveur DNS

```
#systemctl start named.service
```

Ou via la commande

```
# rndc start
```

*NB:* Remplacer **start** par **stop** pour arrêter le serveur

### 2.3 Vérification le démarrage de serveur DNS

```
[root@localhost ofppt]# ps -aux |grep named
named    2779  0.1  2.2 68180 37920 ?        Ssl  17:51   0:00 /usr/sbin/named -u named
root     3260  0.0  0.1  5120  2296 pts/0    S+   17:52   0:00 grep --color=auto named
[root@localhost ofppt]#
```

### 2.4 Activer le lancement au démarrage

Pour activer le lancement au démarrage du serveur DNS lancer la commande

```
#systemctl enable named.service
```

```
[root@localhost ofppt]# systemctl enable named.service
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to /usr/lib/systemd/system/named.service.
[root@localhost ofppt]#
```

### 3. Configuration

#### 3.1 Configuration de base

Le fichier principal de configuration du serveur DNS est `named.conf`. Il se situe dans le répertoire `/etc/`. Il faut commencer par le sauvegarder, en cas de mauvaise manipulation on pourra le remettre en place :

```
# cp /etc/named.conf /etc/named.conf.save
```

Ouvrir le fichier `/etc/named.conf` et modifier la ligne comme suit :

```
listen-on port 53 { localhost; };
```

L'option permet d'autoriser les requêtes récursives que depuis lui-même

L'option "**forwarders**" permet de rediriger les requêtes qui ne sont pas résolues par notre serveur vers un serveur DNS distant

Cela permet d'utiliser le cache d'un serveur déjà existant et donc d'obtenir des temps d'accès plus rapides. Si la requête DNS n'est pas résolue par le serveur DNS "*distant*" alors la requête sera envoyée aux serveurs DNS racine.

```
forwarders { 212.27.40.240; 212.27.40.241; };
```

#### 3.2 Configuration d'un serveur DNS primaire (maître)

Éditer le fichier `/etc/named.conf` en ajoutant les lignes suivantes

##### a. Zone directe

###### Syntaxe :

```
zone "votredomaine.com" IN {
    type master;
    file "votredomaine.com.zone";
    allow-update { none; };
};
```

###### Exemple :

```
zone "ntic.local" IN {
    type master;
    file "ntic.local.host";
    allow-update {none;};
};
```

## b. Zone inverse

### Syntaxe :

#### Cas IPV4

```
zone "Adresse réseau inverse.in-addr.arpa" IN {  
  type master;  
  file "votredomaine.com.inverse";  
  allow-update { none; };  
};
```

#### Cas IPV6

```
zone "Adresse réseau inverse.ip6.arpa" IN {  
  type master;  
  file "votredomaine.com.inverse";  
  allow-update { none; };  
};
```

- L'option **type** permet d'indiquer le type du serveur DNS primaire ou secondaire
- L'option **file** permet de définir les fichiers de zone que nous allons utiliser, nous allons les créer juste après, l'emplacement par défaut de tous les fichiers de zones est le repertoire /var/named
- L'instruction **allow-update { none; }** n'autorise pas de mise à jour dynamique du DNS.

### Exemple :

#### Cas IPV4

- Réseau 10.0.0.0/8

```
zone "10.in-addr.arpa" IN {  
  type master;  
  file "10.inv";  
  allow-update {none;};  
};
```

- Réseau 192.168.2.0/24

```
zone "2.168.192.in-addr.arpa" IN {  
  type master;  
  file "192.168.2.inv";  
  allow-update {none;};  
};
```

#### Cas IPV6

- Réseau 2001:660:3006::/48
- 

```
zone "6.0.0.3.0.6.6.0.1.0.0.2.ip6.arpa" IN {
    type master;
    file "2001.0660.3006.inv";
    allow-update {none;};
};
```

### **Remarque:**

Il faut ajouter l'option suivante dans la zone primaire pour autoriser le transfert de zone vers le serveur DNS secondaire (esclave)

```
allow-transfer { adresse ip du secondaire1; adresse ip du secondaire2; };
};
```

Les options de notification peuvent aussi être utilisées:

**notify:** Paramètre d'activation de la notification. On le met à oui ou non (yes/no)

**allow-notify :** On y inscrit les adresses IP des serveurs secondaires à notifier en cas de modification

### **3.3 Configuration de la zone DNS**

Chaque zones doit correspondre à un fichier dans /var/named/nomdomaine.com.zone  
Voici la structure de la configuration de la zone directe

```
$ttl 86400
@ IN SOA ns.votredomaine.com. dnsmaster.votredomaine.com. (
2006110801
10800
3600
604800
38400 )

@ IN NS ns.votredomaine.com.
@ IN NS ns2.votredomaine.com.

@ IN MX 10 mail.votredomaine.com.
@ IN MX 20 mail2.votredomaine.com.
_ldap_tcp.ntic.ma 86400 IN SRV 20 100 389 AD.ntic.ma.

ns IN A votreip
ns2 IN A votreip

mail IN A votreip
mail2 IN A votreip
www IN A votreip
ftp IN AAAA votreipV6
* IN CNAME www
```

**\$TTL 86400** : indique une durée de vie (Time To Live) par défaut de 86400 secondes (une journée) pour les enregistrements où cela n'est pas précisé.

**@** : est un raccourci pour le nom de la zone indiquée dans le fichier named.conf suivi d'un point.

**SOA** : Permet de définir les informations relatives à la zone. En l'occurrence le nom du serveur DNS primaire (**ns.votredomaine.com**) et l'adresse mail du contact technique (dnsmaster.votredomaine.com. le @ est remplacé par un point). Il est composé de plusieurs champs :

- **Serial** : C'est le numéro de série à incrémenter à chaque modification du fichier. Il permet au serveur secondaire de recharger les informations qu'ils ont. L'usage général vient à le formater de cette manière YYYYMMDDXX.
- **Refresh** : définit la période de rafraîchissement des données.
- **Retry** : si une erreur survient au cours du dernier rafraîchissement, celle-ci sera répétée au bout du délai Retry.
- **Expire** : le serveur sera considéré comme non disponible au bout du délai Expire.
- **Negative cache TTL** : Durée de vie est la durée de validité des données communiquée par le serveur pour toute requête .

**NS** : renseigne le nom des serveurs de noms pour le domaine.

**MX** : renseigne sur le serveur de messagerie. Plusieurs peuvent être définis. Ainsi, il est possible de leur donner une priorité en leur affectant un numéro. Plus bas est le numéro, plus haute est la priorité.

**A** : associe un nom d'hôte à une adresse ipv4 (32 bits)

**AAAA** : associe un nom d'hôte à une adresse ipv6 (128 bits)

**CNAME** : identifie le nom canonique d'un alias, un nom pointant sur un autre nom

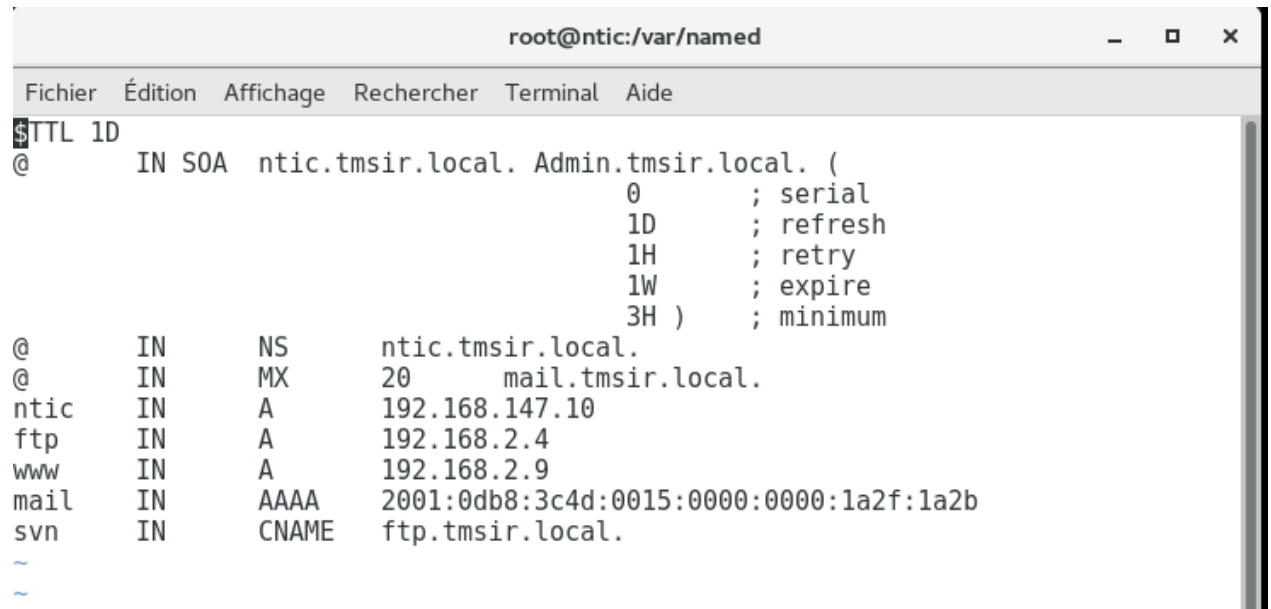
**SRV** : renseigne sur le serveur LDAP (Ex : Active directory), il contient les informations suivantes :

- **Service**: le nom symbolique commençant généralement par un symbole de soulignement du service concerné (par exemple \_ldap).
- **Protocole** : généralement, c'est soit "\_tcp" pour TCP, soit "\_udp" pour UDP.
- **Nom de domaine**: le domaine de validité de l'enregistrement pleinement qualifié au format FQDN.
- **TTL** : champ standard DNS indiquant la durée de validité (Time-To-Live, durée de vie) de la réponse en secondes.
- **Classe** : champ standard DNS indiquant la classe d'adressage, c'est toujours IN pour Internet.
- **Type** : l'identifiant du type d'enregistrement DNS, ici c'est SRV
- **Priorité** : la priorité du serveur cible valeur entière non négative, plus elle est faible, plus ce serveur sera utilisé s'il est disponible.
- **Poids** : poids relatif pour les enregistrements de même priorité valeur entière

de 0 à 65535.

- **Port** : le numéro de port
- **Cible** : le nom du serveur qui fournit le service concerné, il doit être résolu en adresse IPv4 ou IPv6 par d'autres requêtes DNS sur les enregistrements A ou AAAA du nom de service cible.

### Exemple :



```
root@ntic:/var/named
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
$TTL 1D
@      IN SOA  ntic.tmsir.local. Admin.tmsir.local. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

@      IN    NS     ntic.tmsir.local.
@      IN    MX     20     mail.tmsir.local.
ntic   IN    A      192.168.147.10
ftp    IN    A      192.168.2.4
www    IN    A      192.168.2.9
mail   IN    AAAA   2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b
svn    IN    CNAME  ftp.tmsir.local.
~
~
```

Voici la structure de la configuration de la zone inverse

```
$ttl 86400
@ IN SOA ns.votredomaine.com. dnsmaster.votredomaine.com. (
2006110801
10800
3600
604800
38400 )

@ IN NS ns.votredomaine.com.
Votreip IN PTR ns
Votreip IN PTR mail
Votreip IN PTR ns2
```

### Exemple IPV4



```
@ IN SOA dns.ofpptoujda.ma. admin.ofpptoujda.ma. (
                                1          ; serial
                                1D        ; refresh
                                1H        ; retry
                                1W        ; expire
                                3H )     ; minimum

@      IN      NS      dns.ofpptoujda.ma.
@      IN      MX      10      mail.ofpptoujda.ma.
190    IN      PTR     dns
191    IN      PTR     mail
193    IN      PTR     test
```

**Exemple IPV6**

```
$TTL 1D
@      IN SOA  ntic.tmsir.local. Admin.tmsir.local. (
                                0          ; serial
                                1D        ; refresh
                                1H        ; retry
                                1W        ; expire
                                3H )     ; minimum

@      IN      NS      ntic.tmsir.local.
0.2.0.0.4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0      IN      PTR     ftp.tmsir.local.
```

Modifier les droits des fichiers de configuration des zones

```
#chown root.named votredomaine.com.zone
#chown root.named votredomaine.com.inverse
```

Mettre l'adresse du serveur dans la liste du resolver DNS en ajoutant la ligne suivante au fichier /etc/resolv.conf :

```
nameserver Adresse du serveur DNS
```

**3.4 Vérification de la configuration**

Pour vérifier le fichier de configuration lancer la commande suivante

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

Pour vérifier les fichiers zone lancer la commande suivante

```
named-checkzone -d nomdomaine.com /var/named/nomdomaine.zone
named-checkzone -d adresse inverse réseau.in-addr.arpa
/var/named/nomdomaine.inverse
```

**4. Tests de configuration**

Avant de tester la configuration du serveur il faut redémarrer le service DNS pour la prise ne charge des modifications

```
#systemctl restart named.service
```

Il faut ajouter l'adresse IP du serveur DNS dans le fichier **/etc/resolv.conf**

Pour tester le fonctionnement du serveur. Il existe deux principaux utilitaires qui le permettent : **nslookup** , **dig** et **host** .

#### 4.1 nslookup

**Nslookup** permet de retrouver l'adresse IP d'une machine à part de son nom DNS, et l'inverse. Il faut préciser que cela est propre à un réseau bien donné. Le premier serveur DNS interrogé est celui-ci spécifié dans l'inscription. Sous UNIX, nslookup est de plus en plus obsolète, mais il reste encore d'actualité sous Windows.

```
[root@localhost ~]# nslookup dns.ntic.ma
Server:          192.168.247.149
Address:         192.168.247.149#53

Name:   dns.ntic.ma
Address: 192.168.247.128
```

Dans le cas des adresse **IPV6** il faut ajouter l'option **-type=aaaa**

```
[root@ntic named]# nslookup -type=aaaa mail.tmsir.local
Server:          192.168.147.10
Address:         192.168.147.10#53

mail.tmsir.local      has AAAA address 2001:db8:3c4d:15::1a2f:1a2b
```

```
[root@ntic named]# nslookup 2001:0660:3006:2::4:0020
Server:          192.168.147.10
Address:         192.168.147.10#53

0.2.0.0.4.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.6.0.0.3.0.6.0.1.0.0.2.ip6.arpa
ame = ftp.tmsir.local.
```

Il est possible de modifier le mode d'interrogation de la commande nslookup grâce à l'option **type** :

- **type=mx** permet de recueillir les informations concernant le ou les serveurs de messagerie d'un domaine.
- **type=ns** permet de recueillir les informations concernant le serveur de noms associé au domaine
- **type=a** permet de recueillir les informations concernant un hôte du réseau. Il s'agit du mode d'interrogation par défaut.
- **type=soa** permet d'afficher les informations du champ SOA (Start Of Authority).
- **type=cname** permet d'afficher les informations concernant les alias.

```
[root@ntic named]# nslookup -type=mx tmsir.local
Server:          192.168.147.10
Address:         192.168.147.10#53

tmsir.local      mail exchanger = 20 mail.tmsir.local.

[root@ntic named]# nslookup -type=soa tmsir.local
Server:          192.168.147.10
Address:         192.168.147.10#53

tmsir.local
  origin = ntic.tmsir.local
  mail addr = Admin.tmsir.local
  serial = 0
  refresh = 86400
  retry = 3600
  expire = 604800
  minimum = 10800

[root@ntic named]#
```

### 4.2 dig

**dig** : analogue à nslookup, il permet de spécifier le type de serveurs ou de machines qu'on veut contacter.

```
[root@localhost ~]# dig dns.ntic.ma
;; <<> DiG 9.10.4-P4-RedHat-9.10.4-2.P4.fc23 <<> dns.ntic.ma
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 23705
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;dns.ntic.ma.                IN      A
;; ANSWER SECTION:
dns.ntic.ma.                86400   IN      A      192.168.247.128
;; AUTHORITY SECTION:
ntic.ma.                    86400   IN      NS     dns.ntic.ma.

;; Query time: 19 msec
;; SERVER: 192.168.247.128#53(192.168.247.128)
;; WHEN: mar. sept. 19 17:25:32 WEST 2017
```

### 4.3 host

```
[root@ntic named]# host 2001:0660:3006:2::4:0020 localhost
*Using domain server:
Name: localhost
Address: ::1#53
Aliases:

0.2.0.0.4.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.6.0.0.3.0.6.6.0.1.0.0.2.ip6.arpa domain
name pointer ftp.tmsir.local.
```

## 5. Configuration serveur secondaire

Dans vos fichiers (primaire et secondaire) /etc/bind/named.conf vérifier que les paramètres suivants :

```
listen-on port 53 { localhost; };
allow-query { any; }; //Tout le monde peut interroger le serveur (nécessaire pour
serveur publique)
```

## 5.1 Configuration du serveur primaire

Fichier `/etc/bind/named.conf` ajouter les paramètres suivants à la zone

```
zone "ntic.ma" {
type master;
file "ntic.ma.direct";
allow-transfer{ 10.20.30.40;};
notify yes;
};
```

- ◆ `type master;` : déclare que ce serveur est le maître de la zone (serveur primaire)
- ◆ `file « /etc/bind/db.benjaminperrin.fr »;` spécifie où se trouvent les fichiers de la zone
- ◆ `allow-transfer{ 10.20.30.40;};` autorise le serveur primaire à transférer la zone vers le serveur secondaire
- ◆ `notify yes;` notifie le serveur secondaire lorsqu'il y a des modifications

## 5.2 Configuration du serveur secondaire

Fichier `/etc/bind/named.conf` ajouter le paramètre suivants aux options :

```
zone "ntic.ma" {
type slave;
file "ntic.ma.directe"
masters { 10.20.30.41;};

allow-notify { 10.20.30.41; };

};
```

- ◆ `type slave;` : déclare que ce serveur est un esclave (serveur secondaire)
- ◆ `file « /etc/bind/db.benjaminperrin.fr »;` spécifie où se trouvent les fichiers de la zone
- ◆ `masters { 1.2.3.4;};` Spécifie l'adresse du serveur primaire
- ◆ `allow-notify { 10.20.30.41; };` Autorise les notifications du serveur primaire

## 5.3 Test

Depuis le serveur slave tester la résolution d'un enregistrement A

```
[root@localhost ~]# nslookup ftp.ntic.ma
Server:      192.168.247.128
Address:     192.168.247.128#53

Name:   ftp.ntic.ma
Address: 45.25.26.23

[root@localhost ~]#
```

## 6. Déléguer une zone d'un sous domaine

Pour des grands domaines, il peut être utile de mettre en place plusieurs serveurs serveurs DNS, chacun gérant sa zone correspondant à son sous-domaine.

Si le domaine **ntic.ma** veut déléguer la gestion des sous-domaines **tri.ntic.ma**, **tmsir.ntic.ma** au serveur de nom **ns.tri.ntic.ma** (*192.168.1.1*) et **ns.tmsir.ntic.ma** (*192.168.2.1*), il faut que dans le fichier de zone de **ntic.ma** figure les lignes suivantes :

```
tri.ntic.ma.    IN  NS  ns.tri.ntic.ma.
tmsir.ntic.ma. IN  NS  ns.dtmsir.ntic.ma.

ns.tri.ntic.ma. IN  A   192.168.1.1
ns.tmsir.ntic.ma. IN  A   192.168.2.1
```

Pour la résolution inverse, il faut compléter le fichier de résolution comme suit :

```
1.168.192.in-addr.arpa. IN  NS  ns.tri.ntic.ma.
2.168.192.in-addr.arpa. IN  NS  ns.tmsir.ntic.ma.
```

## 7. Configuration de la journalisation

Dans notre configuration actuelle, les logs inondent **/var/log/messages**. Pour éviter ça, on va configurer une journalisation propre à BIND en ajoutant la stance correspondante à **/etc/named.conf**.

```
options {
    directory "/var/named";
};
logging {
    channel single_log {
        file "/var/log/named/named.log" versions 3 size 2m;
        severity info;
        print-time yes;
        print-severity yes;
        print-category yes;
    };
    category default {
        single_log;
    };
};
```

BIND ne peut pas créer ce fichier à la volée. On va donc le faire à sa place, en attribuant les permissions correctes.

```
# mkdir /var/log/named
# touch /var/log/named/named.log
# chown -R named:named /var/log/named/
```

```
# chmod 0770 /var/log/named
```

Recharger la configuration de BIND

```
# systemctl reload named
```

## 8. Dynamic DNS (DDNS)

Le DNS dynamique (DDNS ou DynDNS) est un mécanisme par lequel le serveur de noms du système de noms de domaine (DNS) est automatiquement mis à jour avec le nom de domaine personnalisé et les adresses IP en constante évolution. La méthode DNS est utile dans le cas d'adresses IP dynamiques, où l'adresse IP est mappée sur un domaine personnalisé qui change fréquemment. Toutefois, dans le cas d'une adresse IP statique mappée sur un domaine personnalisé, le DDNS n'est pas requis.

### 8.1 Configuration :

#### a. Serveur DHCP

Au niveau du fichier de configuration du serveur DHCP `dhcpd.conf` ajouter les lignes suivantes :

```
ddns-updates on;
ddns-update-style interim;
deny client-updates;
ddns-domainname "tri.local";
ddns-rev-domainname "2.168.192.in-addr.arpa";
authoritative;

zone tri.local. {
    primary 192.168.2.1;
}
zone 2.168.192.in-addr.arpa. {
    primary 192.168.2.1;
}
```

Les directives utilisées dans ce fichier sont les suivantes :

- ◆ **authoritative** permet de préciser au serveur DHCP qu'il est le serveur DHCP prioritaire sur le réseau local.
- ◆ **ddns-updates** permet ici d'autoriser les mises à jour des zones DNS associées en fonction des adresses IPv4 distribuées.
- ◆ **ddns-update-style** permet de définir quel type de mise à jour sera utilisé pour DDNS. Ici, le paramètre `interim` précise qu'il s'agit d'une mise à jour vers un serveur DNS local.
- ◆ **ignore client-updates** permet d'empêcher les clients de s'enregistrer eux-mêmes auprès du serveur DNS.

- ◆ **update-static-leases** permet de préciser si le serveur DHCP est autorisé ou non à modifier des enregistrements DNS statiques définis dans les fichiers de zone.

### b. Serveur DNS

Au niveau du fichier de configuration du serveur DNS named.conf indiquer l'adresse IP du serveur DHCP dans l'option allow-update pour permettre au serveur DHCP de mettre à jour dynamiquement les zones

```
zone "tri.local" IN {
    type master;
    file "tri.local";
    allow-update {192.168.2.1};
};
```

## 8.2 Test

Lancer une machine client puis vérifier l'ajout automatique en utilisant la commande nslookup

```
[root@ntic named]# nslookup examen-PC.tri.local
Server:          192.168.2.1
Address:         192.168.2.1#53

Name:   examen-PC.tri.local
Address: 192.168.2.20

[root@ntic named]#
```

Nous remarquons que le contenu du fichier de zone à été modifié

```
[root@ntic named]# cat tri.local
$ORIGIN .
$TTL 86400      ; 1 day
tri.local      IN SOA  dns.tri.local. admin.tri.local. (
                1          ; serial
                86400     ; refresh (1 day)
                3600      ; retry (1 hour)
                604800    ; expire (1 week)
                10800     ; minimum (3 hours)
                )
                NS      dns.tri.local.
$ORIGIN tri.local.
dns            A      192.168.2.1
$TTL 3600      ; 1 hour
examen-PC     A      192.168.2.20
              TXT    "31626c70fffd4ea3dfee1acf5dcd2334c5"

[root@ntic named]#
```

## 8.3 Configuration sécurisée

### a. Serveur DNS

Pour permettre la communication entre les serveurs DNS et DHCP, une clé devra être utilisée. La clé sera générée sur le serveur DNS à l'aide de la commande suivante :

```
# rndc-confgen -a
```

```
[root@ntic ~]# rndc-confgen -a
wrote key file "/etc/rndc.key"
[root@ntic ~]# █
```

Vérifier que le fichier rndc.key appartient au groupe named

```
[root@ntic ~]# ls -l /etc/rndc.key
-rw-r----- 1 root named 77 7 oct. 09:40 /etc/rndc.key
[root@ntic ~]#
```

Ajouter la ligne include "/etc/rndc.key" dans le fichier named.conf

```
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/rndc.key"
```

Modifier la valeur de l'option allow-query

```
recursing-file "/var/named/data/named.recursing";
secroots-file "/var/named/data/named.secroots";
allow-query { any; };

/*
```

## b. Serveur DHCP

Editer le fichier dhcpd.conf, effectuer les modifications suivantes

```
ddns-updates on;
ddns-update-style interim;
ignore client-updates
authoritative;
include "/etc/rndc.key";
zone tri.local. {
    primary 192.168.2.1;
}
zone 2.168.192.in-addr.arpa. {
    primary 192.168.2.1;
}
```

**NB :** si le serveur DHCP n'est pas sur la même machine que le serveur DNS, le serveur DHCP va donc devoir posséder une copie du fichier rndc.key créé précédemment dans /etc/dhcp .

## 9. Référence :

<https://blog.microlinux.fr/bind-centos/>  
<http://www.linux-france.org/article/memo/dns/node18.html>  
<http://blog.benjaminperrin.fr/index.php/2014/02/06/dns-bind9-ajout-dun-serveur-secondaire-a-votre-zone/>



<https://4sysops.com/archives/server-roles-in-server-core-part-3-dns-servers/>  
<https://technet.microsoft.com/library/jj649925.aspx>  
<http://www.joryck-leyes.fr/tuto/DNS.pdf>  
<https://www.techopedia.com/definition/1337/dynamic-domain-name-system-ddns>  
<https://www.supinfo.com/articles/single/1715-dynamic-dns-avec-bind9-isc-dhcp-server>