Dernière mise-à-jour : 2020/01/30 03:27

# 207.1 - Basic DNS server configuration

**Weight: 3**

Description: Candidates should be able to configure BIND to function as a caching-only DNS server. This objective includes the ability to managing a running server and configuring logging.

**Key Knowledge Areas:**

- BIND 9.x configuration files, terms and utilities
- Defining the location of the BIND zone files in BIND configuration files
- Reloading modified configuration and zone files
- Awareness of dnsmasq, djbdns and PowerDNS as alternate name servers

**The following is a partial list of the used files, terms and utilities:**

- /etc/named.conf
- /var/named/
- /usr/sbin/rndc
- kill
- host
- dig

## Le serveur DNS

Le principe du DNS est basé sur l'équivalence entre un **FQDN** ( Fully Qualified Domain Name ) et une adresse IP. Les humains retiennent plus facilement des noms tels www.linuxelearning.com, tandis que les ordinateurs utilisent des chiffres.

Le **DNS** ( Domain Name Service ) est né peut après l'introduction des FQDN en 1981.

Lorque un ordinateur souhaite communiquer avec un autre par le biais de son nom, par exemple avec www.fenestros.com, il envoie une requête à un server DNS. Si le serveur DNS a connaissance de la correspondance entre le nom demandé et le numéro IP, il répond directement. Si ce n'est pas le cas, il démarre un processus de **Recursive Lookup**.

Ce processus tente d'identifier le serveur de domaine responsable pour le **SLD** ( Second Level Domain ) afin de lui passer la reqûete. Dans notre exemple, il tenterait d'identifier le serveur de domaine responsable de **linuxelearning.com**.

Si cette tentative échoue, le serveur DNS cherche le serveur de domaine pour le **TLD** ( Top Level Domain ) dans son cache afin de lui demander l'adresse du serveur responsable du SLD. Dans notre cas il tenterait trouver l'enregistrement pour le serveur de domaine responsable de **.com**

Si cette recherche échoue, le serveur s'adresse à un **Root Name Server** dont il y en a peu. Si le Root Name Server ne peut pas répondre, le serveur DNS renvoie une erreur à la machine ayant formulé la demande.

Le serveur DNS sert à faire la résolution de noms. Autrement dit de traduire une adresse Internet telle **www.fenestros.com** en **numéro IP**.

# Préparation à l'Installation

Le serveur DNS nécessite à ce que la machine sur laquelle il est installé possède un nom FQDN et une adresse IP fixe. Il est également important à noter que le service de bind ne démarrera **pas** dans le cas où le fichier **/etc/hosts** comporte une anomalie. Trois étapes préparatoires sont donc nécessaires :

- Modification de l'adresse IP de la machine en adresse IP fixe
- Définition d'un nom FQDN (Fully Qualified Domain Name)
- Vérification du fichier /etc/hosts

Afin d'étudier ce dernier cas, nous prenons en tant qu'exemple la machine suivante :

- **FQDN** - centos.fenestros.loc
- **Adresse IP** - 10.0.2.15

Vérifiez que votre fichier /etc/hosts prend la forme suivante :

hosts

```
10.0.2.15   centos.fenestros.loc
127.0.0.1   localhost.localdomain    localhost
::1    centos    localhost6.localdomain6    localhost6
```

Il est important de noter que la configuration du serveur DNS dépend du nom de votre machine. Dans le cas où vous changeriez ce nom, vous devez re-configurer votre serveur DNS en éditant les fichiers de configuration directement.

## Installation

Pour installer le serveur DNS, utilisez la commande **yum**:

```
[root@centos6 ~]# yum install bind
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirrors.ircam.fr
 * extras: mirrors.ircam.fr
 * updates: mirrors.ircam.fr
Setting up Install Process

Resolving Dependencies
--> Running transaction check
---> Package bind.i686 32:9.7.3-8.P3.el6_2.2 set to be updated
--> Processing Dependency: bind-libs = 32:9.7.3-8.P3.el6_2.2 for package: 32:bind-9.7.3-8.P3.el6_2.2.i686
--> Processing Dependency: libdns.so.69 for package: 32:bind-9.7.3-8.P3.el6_2.2.i686
--> Processing Dependency: libisccfg.so.62 for package: 32:bind-9.7.3-8.P3.el6_2.2.i686
--> Processing Dependency: libisc.so.62 for package: 32:bind-9.7.3-8.P3.el6_2.2.i686
--> Running transaction check
--> Processing Dependency: libdns.so.64 for package: 32:bind-utils-9.7.0-5.P2.el6_0.1.i686
```

```
--> Processing Dependency: libisc.so.60 for package: 32:bind-utils-9.7.0-5.P2.el6_0.1.i686
--> Processing Dependency: libisccfg.so.60 for package: 32:bind-utils-9.7.0-5.P2.el6_0.1.i686
---> Package bind-libs.i686 32:9.7.3-8.P3.el6_2.2 set to be updated
--> Running transaction check
---> Package bind-utils.i686 32:9.7.3-8.P3.el6_2.2 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package          Arch       Version                          Repository     Size
================================================================================
Installing:
 bind             i686       32:9.7.3-8.P3.el6_2.2            updates       3.9 M
Updating for dependencies:
 bind-libs        i686       32:9.7.3-8.P3.el6_2.2            updates       850 k
 bind-utils       i686       32:9.7.3-8.P3.el6_2.2            updates       177 k

Transaction Summary
================================================================================
Install       1 Package(s)
Upgrade       2 Package(s)

Total download size: 4.9 M
Is this ok [y/N]: y
Downloading Packages:
(1/3): bind-9.7.3-8.P3.el6_2.2.i686.rpm                  | 3.9 MB     00:03
(2/3): bind-libs-9.7.3-8.P3.el6_2.2.i686.rpm             | 850 kB     00:00
(3/3): bind-utils-9.7.3-8.P3.el6_2.2.i686.rpm            | 177 kB     00:00
--------------------------------------------------------------------------------
Total                                           1.2 MB/s | 4.9 MB     00:04
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
```

```
Running Transaction
  Updating       : 32:bind-libs-9.7.3-8.P3.el6_2.2.i686                    1/5
  Updating       : 32:bind-utils-9.7.3-8.P3.el6_2.2.i686                   2/5
  Installing     : 32:bind-9.7.3-8.P3.el6_2.2.i686                         3/5
  Cleanup        : 32:bind-utils-9.7.0-5.P2.el6_0.1.i686                   4/5
  Cleanup        : 32:bind-libs-9.7.0-5.P2.el6_0.1.i686                    5/5

Installed:
  bind.i686 32:9.7.3-8.P3.el6_2.2

Dependency Updated:
  bind-libs.i686 32:9.7.3-8.P3.el6_2.2   bind-utils.i686 32:9.7.3-8.P3.el6_2.2

Complete!
```

Configurez le service **named** du paquet **bind** pour que celui-ci soit activé correctement pour les niveaux d'exécution 3, 4 et 5 :

```
[root@centos6 ~]# chkconfig --level 345 named on
[root@centos6 ~]# chkconfig --list | grep named
named           0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche6:arrêt
```

**Options de la commande named**

Les options de cette commande sont :

```
[root@centos6 ~]# named --help
usage: named [-4|-6] [-c conffile] [-d debuglevel] [-E engine] [-f|-g]
             [-n number_of_cpus] [-p port] [-s] [-t chrootdir] [-u username]
             [-m {usage|trace|record|size|mctx}]
named: unknown option '--'
```

# Les fichiers de configuration

- /var/named/named.ca
- /etc/named.conf
- /var/named/named.loopback
- /var/named/named.localhost
- /var/named/data/db.2.0.10.hosts
- /var/named/data/db.fenestros.loc.hosts

## named.ca

Ce fichier doit se trouver dans /var/named.

Le fichier **named.ca** a besoin d'être mis à jour en utilisant la commande **dig** :

```
[root@centos6 ~]# dig +tcp @A.ROOT-SERVERS.NET > /var/named/named.ca
```

named.ca

```
; <<>> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.2 <<>> @A.ROOT-SERVERS.NET
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32525
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;.              IN    NS

;; ANSWER SECTION:
.           518400    IN    NS    f.root-servers.net.
```

```
.           518400    IN    NS    a.root-servers.net.
.           518400    IN    NS    j.root-servers.net.
.           518400    IN    NS    d.root-servers.net.
.           518400    IN    NS    m.root-servers.net.
.           518400    IN    NS    i.root-servers.net.
.           518400    IN    NS    g.root-servers.net.
.           518400    IN    NS    e.root-servers.net.
.           518400    IN    NS    l.root-servers.net.
.           518400    IN    NS    c.root-servers.net.
.           518400    IN    NS    b.root-servers.net.
.           518400    IN    NS    k.root-servers.net.
.           518400    IN    NS    h.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net. 3600000    IN    A    198.41.0.4
a.root-servers.net. 3600000    IN    AAAA    2001:503:ba3e::2:30
b.root-servers.net. 3600000    IN    A    192.228.79.201
c.root-servers.net. 3600000    IN    A    192.33.4.12
d.root-servers.net. 3600000    IN    A    128.8.10.90
d.root-servers.net. 3600000    IN    AAAA    2001:500:2d::d
e.root-servers.net. 3600000    IN    A    192.203.230.10
f.root-servers.net. 3600000    IN    A    192.5.5.241
f.root-servers.net. 3600000    IN    AAAA    2001:500:2f::f
g.root-servers.net. 3600000    IN    A    192.112.36.4
h.root-servers.net. 3600000    IN    A    128.63.2.53
h.root-servers.net. 3600000    IN    AAAA    2001:500:1::803f:235
i.root-servers.net. 3600000    IN    A    192.36.148.17
i.root-servers.net. 3600000    IN    AAAA    2001:7fe::53

;; Query time: 149 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Wed May 30 13:28:45 2012
;; MSG SIZE  rcvd: 512
```

Le fichier named.ca doit appartenir à l'utilisateur **root** du groupe **root** et avoir les permissions en 0644.

```
[root@centos6 ~]# ls -l /var/named/named.ca
-rw-r--r--. 1 root root 1666 30 mai   13:28 /var/named/named.ca
```

## named.conf

Le fichier de configuration principal du serveur DNS Bind est **/etc/named.conf** :

named.conf

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
    listen-on port 53 { 127.0.0.1; };
    listen-on-v6 port 53 { ::1; };
    directory     "/var/named";
    dump-file     "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { localhost; };
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;
```

```
    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
    type hint;
    file "named.ca";
};

include "/etc/named.rfc1912.zones";
```

Dans ce fichier on trouve des sections ayant la forme suivante :

```
section {
   variable1  valeur1;
   variable2  valeur2;
};
```

Il existe différentes sections dont une des plus importantes est **options**. C'est dans cette section que nous définissons les options globales:

```
...
options {
    listen-on port 53 { 127.0.0.1; };
    listen-on-v6 port 53 { ::1; };
    directory     "/var/named";
```

```
    dump-file     "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { localhost; };
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";
};
...
```

Notons certaines directives. D'abord nous définissons le chemin des fichiers des **zones**:

```
directory "/var/named";
```

Afin de limiter les machines qui peuvent et qui ne peuvent pas utiliser notre DNS, nous utilisons la valeur “allow-query”. Dans notre cas les requêtes sont permises en provenance uniquement du localhost :

```
allow-query { localhost; };
```

Modifiez donc la section **options** de votre fichier **/etc/named.conf** ainsi :

```
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query {
```

```
                localhost;
                10.0.2.0/24;
        };
        recursion yes;
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";
};
...
```

Dans l'exemple ci-dessus nous autorisons toutes les machines de notre réseau, ainsi que la machine locale à utiliser le DNS.

## Les Sections de Zone

Dans le fichier **/etc/named.conf** vous pouvez constater la présence d'une directive **include**.

Le fichier concerné par cette directive est **/etc/named.rfc1912.zones** :

named.rfc1912.zones

```
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and http://www.ietf.org/internet-drafts/draft-ietf-dnsop-default-local-zones-02.txt
```

```
// (c)2007 R W Franks
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

zone "localhost.localdomain" IN {
    type master;
    file "named.localhost";
    allow-update { none; };
};

zone "localhost" IN {
    type master;
    file "named.localhost";
    allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
    type master;
    file "named.loopback";
    allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
    type master;
    file "named.loopback";
    allow-update { none; };
};

zone "0.in-addr.arpa" IN {
    type master;
    file "named.empty";
    allow-update { none; };
```

```
};
```

### La Valeur Type

Maintenant, étudions les sections de zones. La valeur “type” peut prendre plusieurs valeurs:

- **master**
  - Ce type définit le serveur DNS comme serveur maître ayant **autorité** sur la zone concernée.
- **slave**
  - Ce type définit le serveur DNS comme serveur esclave pour la zone concernée. Ceci implique que la zone est une réplication d'une zone maître. Un type de zone esclave contiendra aussi une directive **masters** indiquant les adresses IP des serveurs DNS maîtres.
- **stub**
  - Ce type définit le serveur DNS comme serveur esclave pour la zone concernée mais uniquement pour les **enregistrements** de type **NS**.
- **forward**
  - Ce type définit le serveur DNS comme serveur de transit pour la zone concernée. Ceci implique que toute requête est re-transmise vers un autre serveur.
- **hint**
  - Ce type définit la zone concernée comme une zone racine. Ceci implique que lors du démarrage du serveur, cette zone est utilisée pour récupérer les adresses des serveurs DNS racine.

La valeur “notify” est utilisée pour indiquer si non ( no ) ou oui ( yes ) les autres serveurs DNS sont informés de changements dans la zone.

### La Valeur File

La deuxième directive dans une section de zone comporte la valeur **file**. Il indique l'emplacement du fichier de zone.

### Exemples de Sections de Zone

Chaque section de zone, à l'exception de la zone “.” est associée avec une section de zone inversée.

La zone “.” est configurée dans le fichier **/etc/named.conf** :

```
...
zone "." IN {
    type hint;
    file "named.ca";
};
...
```

La section de zone fait corréspondre un nom avec une adresse IP tandis que la section de zone inversée fait l'inverse. La section inversée a un nom d'un syntaxe spécifique :

```
adresse_réseau_inversée.in-addr.arpa.
```

Par exemple dans le fichier ci-dessus nous trouvons les trois sections suivantes :

```
...
zone "localhost" IN {
    type master;
    file "named.localhost";
    allow-update { none; };
};
...
zone "1.0.0.127.in-addr.arpa" IN {
    type master;
    file "named.loopback";
    allow-update { none; };
};

zone "0.in-addr.arpa" IN {
    type master;
    file "named.empty";
    allow-update { none; };
};
```

Notez la présence de deux sections inversées, respectivement pour IPv4 et IPv6. Dans la suite de cette leçon, nous allons nous concentrer sur IPv4.

### Sections de Zones de votre Machine

Afin de configurer notre serveur correctement donc, il est necéssaire d'ajouter à ce fichier deux sections supplémentaires :

- La zone correspondant à notre domaine, ici appelée “fenestros.loc”. Celle-ci fait correspondre le nom de la machine avec son adresse IP:

```
...
zone "fenestros.loc" {
    type master;
    file "data/db.fenestros.loc.hosts";
    forwarders { };
};
...
```

- La zone à notre domaine mais dans le sens inverse. A savoir le fichier **db.2.0.10.hosts** qui fait correspondre notre adresse IP avec le nom de la machine.

```
...
zone "2.0.10.in-addr.arpa" {
    type master;
    file "data/db.2.0.10.hosts";
    forwarders { };
};
...
```

Ajoutez donc ces deux sections au fichier **/etc/named.rfc1912.zones** :

named.rfc1912.zones

```
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and http://www.ietf.org/internet-drafts/draft-ietf-dnsop-default-local-zones-02.txt
// (c)2007 R W Franks
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

zone "localhost.localdomain" IN {
    type master;
    file "named.localhost";
    allow-update { none; };
};

zone "localhost" IN {
    type master;
    file "named.localhost";
    allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
    type master;
    file "named.loopback";
    allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
    type master;
```

```
    file "named.loopback";
    allow-update { none; };
};

zone "0.in-addr.arpa" IN {
    type master;
    file "named.empty";
    allow-update { none; };
};

zone "fenestros.loc" {
    type master;
    file "data/db.fenestros.loc.hosts";
    forwarders { };
};

zone "2.0.10.in-addr.arpa" {
    type master;
    file "data/db.2.0.10.hosts";
    forwarders { };
};
```

### Les fichiers de zone

La fichiers de zone sont composées de lignes d'une forme:

| nom | TTL | classe | type | donnée |
|---|---|---|---|---|

où

- **nom**
  - Le nom DNS.

- **TTL**
  - La durée de vie en cache de cet enregistrement.
- **classe**
  - Le réseau de transport utilisé. Dans notre cas, le réseau est du TCP. La valeur est donc IN.
- **type**
  - Le type d'enregistrement:
    - SOA - Start of Authority - se trouve au début du fichier et contient des informations générales
    - NS - Name Server - le nom du serveur de nom
    - A - Address - indique une résolution de nom vers une adresse IP. Ne se trouve que dans les fichiers **.hosts**
    - PTR - PoinTeR - indique une résolution d'une adresse IP vers un nom. Ne se trouve que dans les fichiers inversés.
    - MX - Mail eXchange - le nom d'un serveur de mail.
    - CNAME - Canonical Name - un alias d'une machine.
    - HINFO - Hardware Info - fournit des informations sur le matériel de la machine
- **donnée**
  - La donnée de la ressource:
    - Une adresse IP pour un enregistrement de type A
    - Un nom de machine pour un eregistrement de type PTR

#### db.fenestros.loc.hosts

Ce fichier se trouve dans /var/named/data. Il est le fichier qui définit la correspondance du nom de la machine **centos.fenestros.loc** avec son numéro IP, à savoir le **10.0.2.15**. On définit dans ce fichier les machines qui doivent être appelées par leur nom :

db.fenestros.loc.hosts

```
$TTL 3D
@       IN     SOA     centos.fenestros.loc. root.centos.fenestros.loc. (
               2012120301       ; Serial
               8H   ; Refresh
               2H   ; Retry
               4W  ; Expire
               1D)  ; Minimum TTL
               IN      NS      centos.fenestros.loc.
```

```
localhost                   A               127.0.0.1
dnsmaster                   IN      CNAME   centos.fenestros.loc.
centos.fenestros.loc.       IN      A       10.0.2.15

ftp IN CNAME centos.fenestros.loc.
www IN CNAME centos.fenestros.loc.
mail IN CNAME centos.fenestros.loc.
news IN CNAME centos.fenestros.loc.
```

La première ligne de ce fichier commence par une ligne semblable à celle-ci:

```
$TTL 3D
```

Cette ligne indique aux autres serveurs DNS pendant combien de temps ils doivent garder en cache les enregistrements de cette zone. La durée peut s'exprimer en jours (**D**), en heures (**H**) ou en secondes (**S**).

La deuxième ligne définit une **classe IN**ternet, un **SOA** (Start Of Authority), le nom du serveur primaire et l'adresse de l'administrateur de mail :

```
@       IN     SOA     centos.fenestros.loc. root.centos.fenestros.loc. (
```

Le caractère **@** corréspond au nom de la zone et est une abréviation pour le nom de la zone décrit par le fichier de la zone, soit dans ce cas db.**fenestros.loc**.hosts, et présent dans le fichier /etc/named.conf :

<box 95% blue | **Extrait de la section de zone du fichier named.rfc1912.zones**>

```
zone "fenestros.loc" {
      type master;
      file "data/db.fenestros.loc.hosts";
      forwarders { };
};
```

</box>

Notez le point à la fin de chaque nom de domaine. Notez bien le remplacement du caractère @ dans l'adresse email de l'administrateur de mail par le caractère “.”

**Le numéro de série** doit être modifié chaque fois que le fichier soit changé. Il faut noter que dans le cas de plusieurs changements dans la même journée il est necessaire d'incrémenter les deux derniers chiffres du numéro de série. Par exemple, dans le cas de deux changements en date du 03/12/20012, le premier fichier comportera une ligne Serial avec la valeur 2012120301 tandis que le deuxième changement comportera le numéro de série 2012120302 :

```
        2012120301       ; Serial
```

La ligne suivante indique le temps de rafraîchissement, soit 8 heures. Ce temps correspond à la durée entre les mises à jour d'un autre serveur :

```
        8H ; Refresh
```

La ligne suivante indique le temps entre de nouveaux essaies de mise à jour d'un autre serveur dans le cas où la durée du Refresh a été dépassée :

```
        2H ; Retry
```

La ligne suivante indique le temps d'expiration, c'est-à-dire la durée d'autorité de l'enregistrement. Cette directive est utilisée seulement par un serveur esclave :

```
        4W ; Expire
```

La ligne suivante indique le temps minimum pour la valeur TTL, soit un jour:

```
        1D) ; Minimum TTL
```

Cette ligne identifie notre serveur de noms :

```
IN NS centos.fenestros.loc.
```

Dans le cas où notre serveur était également un serveur mail. Nous trouverions aussi une entrée du type SMTP (MX) :

```
IN MX 10 mail.fenestros.loc.
```

Ci-dessous on définit avec une entrée du type A, les machines que l'on souhaite appeler par leur nom, à savoir **centos.fenestros.loc** et **localhost** :

```
localhost                   A               127.0.0.1
centos.fenestros.loc.       IN      A       10.0.2.15
```

Ci-dessous on définit des **Alias** avec des entrées du type CNAME. Les alias servent à identifier une machine.

```
dnsmaster                   IN      CNAME   centos.fenestros.loc.
```

Nous pourrions aussi trouver ici des entrées telles:

```
ftp IN CNAME centos.fenestros.loc.
www IN CNAME centos.fenestros.loc.
mail IN CNAME centos.fenestros.loc.
news IN CNAME centos.fenestros.loc.
```

#### db.2.0.10.hosts

Ce fichier se trouve dans /var/named/data. Il est le fichier qui définit la correspondance de l'adresse IP de la machine, à savoir le **10.0.2.15** avec le nom **centos.fenestros.loc**. Le chiffre **15** dans la dernière ligne correspond au 10.0.2.**15**:

db.2.0.10.hosts

```
$TTL 3D
@       IN      SOA     centos.fenestros.loc.        centos.fenestros.loc. (
                2008120301 ; Serial
                10800   ; Refresh
                3600    ; Retry
```

```
                604800  ; Expire
                86400) ; Minimum TTL
                NS      centos.fenestros.loc.
15      IN       PTR     centos.fenestros.loc.
```

Modifiez maintenant les permissions sur les fichiers de configuration :

```
[root@centos6 named]# chmod g+w /var/named/data/*
[root@centos6 named]# ls -l /var/named/data/*
-rw-rw-r--. 1 root root 350 30 mai   15:52 /var/named/data/db.2.0.10.hosts
-rw-rw-r--. 1 root root 610 30 mai   15:51 /var/named/data/db.fenestros.loc.hosts
```

Modifiez maintenant le fichier **/etc/resolv.conf** afin d'utiliser votre propre serveur DNS :

resolv.conf

```
search fenestros.loc
nameserver 127.0.0.1
```

Dernièrement, démarrez le service named :

```
[root@centos6 named]# service named start
Démarrage de named :                                       [  OK  ]
```

Testez maintenant votre serveur :

```
[root@centos6 ~]# dig www.linuxelearning.com

; <<>> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.2 <<>> www.linuxelearning.com
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44024
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 13, ADDITIONAL: 0

;; QUESTION SECTION:
;www.linuxelearning.com.        IN    A

;; ANSWER SECTION:
www.linuxelearning.com. 39795    IN    CNAME    linuxelearning.com.
linuxelearning.com. 60    IN    A    212.198.31.61

;; AUTHORITY SECTION:
com.            172599    IN    NS    k.gtld-servers.net.
com.            172599    IN    NS    m.gtld-servers.net.
com.            172599    IN    NS    l.gtld-servers.net.
com.            172599    IN    NS    b.gtld-servers.net.
com.            172599    IN    NS    d.gtld-servers.net.
com.            172599    IN    NS    a.gtld-servers.net.
com.            172599    IN    NS    f.gtld-servers.net.
com.            172599    IN    NS    i.gtld-servers.net.
com.            172599    IN    NS    e.gtld-servers.net.
com.            172599    IN    NS    c.gtld-servers.net.
com.            172599    IN    NS    j.gtld-servers.net.
com.            172599    IN    NS    h.gtld-servers.net.
com.            172599    IN    NS    g.gtld-servers.net.

;; Query time: 38 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed May 30 17:09:25 2012
;; MSG SIZE  rcvd: 294

[root@centos6 ~]# dig centos.fenestros.loc

; <<>> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.2 <<>> centos.fenestros.loc
;; global options: +cmd
```

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26457
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;centos.fenestros.loc.      IN    A

;; ANSWER SECTION:
centos.fenestros.loc.   259200    IN    A    10.0.2.15

;; AUTHORITY SECTION:
fenestros.loc.      259200    IN    NS    centos.fenestros.loc.

;; Query time: 3 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed May 30 17:10:05 2012
;; MSG SIZE  rcvd: 68


[root@centos6 ~]# dig -x 10.0.2.15

; <<>> DiG 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.2 <<>> -x 10.0.2.15
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59735
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;15.2.0.10.in-addr.arpa.        IN    PTR

;; ANSWER SECTION:
15.2.0.10.in-addr.arpa. 259200    IN    PTR    centos.fenestros.loc.

;; AUTHORITY SECTION:
```

```
2.0.10.in-addr.arpa.    259200    IN    NS    centos.fenestros.loc.

;; ADDITIONAL SECTION:
centos.fenestros.loc.   259200    IN    A    10.0.2.15

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed May 30 17:10:50 2012
;; MSG SIZE  rcvd: 104
```

Notez l'utilisation de l'option **-x** de la commande **dig** pour tester la zone à l'envers.

## rndc

L'utilitaire de bind **rndc** est utilisé pour contrôler **named** à partir de la ligne de commande. Pour des raisons de sécurité une clef partagée doit être référencée dans le fichier de configuration de bind, **/etc/named.conf**, ainsi que dans le fichier de configuration de **rndc**, **/etc/rndc.conf**.

### La clef rndc

Premièrement il convient de créer la clef partagée :

```
[root@centos6 ~]# rndc-confgen -a -c /root/rndc.key
wrote key file "/root/rndc.key"
```

A l'examen de la clef, vous pouvez constater que son nom est **rndc-key** et que l'algorithme est **hmac-md5** :

rndc.key

```
key "rndc-key" {
    algorithm hmac-md5;
    secret "NuPP8qFNPZ7m0rWPPahRtA==";
};
```

### Fichiers de Configuration

La clef doit être référencée dans le fichier **/etc/named.conf** :

named.conf

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
    listen-on port 53 { 127.0.0.1; };
    listen-on-v6 port 53 { ::1; };
    directory     "/var/named";
    dump-file     "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query {
        localhost;
        10.0.2.0/24;
     };
```

```
    forwarders { 10.0.2.3; };
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
    type hint;
    file "named.ca";
};

key "rndc-key" {
    algorithm hmac-md5;
    secret "NuPP8qFNPZ7m0rWPPahRtA==";
};

include "/etc/named.rfc1912.zones";
```

Afin de dire à named d'écouter sur le port par défaut 953 pour des connexions en provenance de rndc, il est necéssaire d'utiliser une clause **controls** dans le fichier /etc/named.conf :

named.conf

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
    listen-on port 53 { 127.0.0.1; };
    listen-on-v6 port 53 { ::1; };
    directory     "/var/named";
    dump-file     "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query {
        localhost;
        10.0.2.0/24;
     };
    forwarders { 10.0.2.3; };
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    /* Path to ISC DLV key */
    bindkeys-file "/etc/named.iscdlv.key";
};

logging {
```

```
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
    type hint;
    file "named.ca";
};

controls {
  inet 127.0.0.1 allow { localhost; } keys { rndc-key; };
};

key "rndc-key" {
    algorithm hmac-md5;
    secret "NuPP8qFNPZ7m0rWPPahRtA==";
};

include "/etc/named.rfc1912.zones";
```

A ce stade, rndc ne peut pas se connecter à named :

```
[root@centos6 ~]# service named status
rndc: connection to remote host closed
This may indicate that
* the remote server is using an older version of the command protocol,
* this host is not authorized to connect,
* the clocks are not synchronized, or
* the key is invalid.
named (pid  10806) en cours d'exécution...
```

La raison est le manque du fichier **/etc/rndc.conf** qui doit prendre la forme suivante :

rndc.conf

```
key "rndc-key" {
    algorithm hmac-md5;
    secret "NuPP8qFNPZ7m0rWPPahRtA==";
};

options {
  default-server  localhost;
  default-key     "rndc-key";
};
```

Notez la présence de la section concernant la valeur de la clef et la section qui définit le serveur par défaut et la clef par défaut.Dans le cas où vous avez plusieurs serveurs à gérer à partir d'une seule instance de rndc vous pouvez inclure des clauses supplémentaires correspondantes à chaque configuration des fichiers /etc/named.conf.

Pour prendre en compte cette configuration, re-démarrez votre service named :

```
[root@centos6 ~]# service named restart
Arrêt de named : .                                         [  OK  ]
Démarrage de named :                                       [  OK  ]
```

Constatez ensuite que rndc fonctionne :

```
[root@centos6 ~]# service named status
version: 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.2
CPUs found: 1
worker threads: 1
```

```
number of zones: 21
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/0/1000
tcp clients: 0/100
server is up and running
named (pid  12105) en cours d'exécution...
```

Notez les lignes supplémentaires dans la sortie.

### Options de la commande

Les options de cette commande sont :

```
[root@centos6 ~]# rndc --help
rndc: invalid argument --
Usage: rndc [-b address] [-c config] [-s server] [-p port]
    [-k key-file ] [-y key] [-V] command

command is one of the following:

  reload    Reload configuration file and zones.
  reload zone [class [view]]
        Reload a single zone.
  refresh zone [class [view]]
        Schedule immediate maintenance for a zone.
  retransfer zone [class [view]]
```

```
      Retransfer a single zone without checking serial number.
freeze    Suspend updates to all dynamic zones.
freeze zone [class [view]]
      Suspend updates to a dynamic zone.
thaw      Enable updates to all dynamic zones and reload them.
thaw zone [class [view]]
      Enable updates to a frozen dynamic zone and reload it.
notify zone [class [view]]
      Resend NOTIFY messages for the zone.
reconfig  Reload configuration file and new zones only.
sign zone [class [view]]
      Update zone keys, and sign as needed.
loadkeys zone [class [view]]
      Update keys without signing immediately.
stats     Write server statistics to the statistics file.
querylog  Toggle query logging.
dumpdb [-all|-cache|-zones] [view ...]
      Dump cache(s) to the dump file (named_dump.db).
secroots [view ...]
      Write security roots to the secroots file.
stop      Save pending updates to master files and stop the server.
stop -p   Save pending updates to master files and stop the server
      reporting process id.
halt      Stop the server without saving pending updates.
halt -p   Stop the server without saving pending updates reporting
      process id.
trace     Increment debugging level by one.
trace level   Change the debugging level.
notrace   Set debugging level to 0.
flush     Flushes all of the server's caches.
flush [view]  Flushes the server's cache for a view.
flushname name [view]
      Flush the given name from the server's cache(s)
status    Display status of the server.
```

```
  recursing Dump the queries that are currently recursing (named.recursing)
  validation newstate [view]
        Enable / disable DNSSEC validation.
  *restart  Restart the server.
  addzone ["file"] zone [class [view]] { zone-options }
        Add zone to given view. Requires new-zone-file option.
  delzone ["file"] zone [class [view]]
        Removes zone from given view. Requires new-zone-file option.

* == not yet implemented
Version: 9.7.3-P3-RedHat-9.7.3-8.P3.el6_2.2
```

## LAB #1

**A Faire** - Créez les fichiers de configurations et modifiez votre fichier **/etc/resolv.conf**. Testez ensuite votre DNS en utilisant la commande dig.