Dernière mise-à-jour : 2020/01/30 03:28

Gestion des Serveurs DNS, NTP, FTP et DHCP

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

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

Le Serveur d'Horloge

Introduction

Dans le cas d'un serveur de réseau, il est souvent important de maintenir l'heure de la machine à l'heure exacte pour des raisons de simplification de synchronisation avec des portables ou bien des systèmes de fichiers externes. Pour accomplir cette tâche, nous utilisons les services de serveurs de temps publics disponibles sur Internet sur lesquels nous synchronisons l'horloge de notre serveur. De même, les machines de notre réseau peuvent se synchroniser ensuite avec l'heure de notre serveur.

Le protocole utilisé s'appelle **NTP** (**Network Time Protocol**) qui utilise le port **123**. Celui-ci, permet la synchronisation avec plusieurs serveurs publics. Les serveurs de temps de racine s'appellent des serveurs de **Strate 1**. En dessous se trouvent des serveurs de Strate 2, Strate 3 etc..

Linux utilise le fuseau d'horaire **UTC** (*Coordinated Universal Time*) en interne. Linux doit donc être capable de traduire entre l'UTC et l'heure locale et vice versa. Linux utilise le fichier **/etc/localtime** pour connaître l'heure locale :

```
[root@centos6 ~]# ls -l /etc/localtime
-rw-r--r--. 1 root root 2945 23 mai    2012 /etc/localtime
```

Ce fichier peut être un fichier ordinaire ou bien un lien symbolique pointant vers un de sfichiers dans le répertoire **/usr/share/zoneinfo** :

```
[root@centos6 ~]# ls /usr/share/zoneinfo/
Africa      Chile    GB         Indian       Mideast   posixrules  US
America     CST6CDT  GB-Eire    Iran         MST       PRC         UTC
Antarctica  Cuba     GMT        iso3166.tab  MST7MDT   PST8PDT     WET
Arctic      EET      GMT0       Israel       Navajo    right       W-SU
Asia        Egypt    GMT-0      Jamaica      NZ        ROC         zone.tab
Atlantic    Eire     GMT+0      Japan        NZ-CHAT   ROK         Zulu
Australia   EST      Greenwich  Kwajalein    Pacific   Singapore
Brazil      EST5EDT  Hongkong   Libya        Poland    Turkey
Canada      Etc      HST        MET          Portugal  UCT
CET         Europe   Iceland    Mexico       posix     Universal
```

Pour connaître le fuseau d'horaire local, utilisez la commande **date** :

```
[root@centos6 ~]# date
jeu. sept. 25 14:07:21 CEST 2014
```

Vous pouvez consulter la liste des codes des zones à l'adresse **http://www.timeanddate.com/library/abbreviations/timezones/**.

Le fuseau d'horaire est aussi contenu en clair dans le fichier **/etc/sysconfig/clock**. Sous Red Hat :

```
[root@centos6 ~]# cat /etc/sysconfig/clock
# The time zone of the system is defined by the contents of /etc/localtime.
# This file is only for evaluation by system-config-date, do not rely on its
# contents elsewhere.
ZONE="Europe/Paris"
```

Sous Debian et ses dérivés, le fichier /etc/sysconfig/clock n'existe pas. Debian utilise le fichier **/etc/timezone** :

```
root@debian:~# cat /etc/timezone
Europe/Paris
```

Vous pouvez modifier le fuseau d'horaire à l'aide de la commande **tzselect**. Sous Red Hat :

```
[root@centos6 ~]# tzselect
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
```

```
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#?
```

Sous Debian :

```
root@debian:~# tzselect
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#?
```

Vous pouvez aussi modifier le fuseau d'horaire directement ainsi :

```
[root@centos6 ~]# rm /etc/localtime
rm : supprimer fichier « /etc/localtime » ? o
[root@centos6 ~]# ln -s /usr/share/zoneinfo/Europe/Paris /etc/localtime
[root@centos6 ~]# ls -l /etc/localtime
lrwxrwxrwx. 1 root root 32 25 sept. 14:32 /etc/localtime -> /usr/share/zoneinfo/Europe/Paris
```

Dernièrement il est possible de modifier le fuseau d'horaire uniquement pour la session en cours et dans le shell courant :

```
[root@centos6 ~]# date
jeu. sept. 25 14:33:44 CEST 2014
[root@centos6 ~]# export TZ=:/usr/share/zoneinfo/Europe/London
[root@centos6 ~]# date
jeu. sept. 25 13:34:09 BST 2014
```

Installation

Sous CentOS, le serveur **ntpd** est normalement installé par défaut :

```
[root@centos6 ~]# rpm -qa | grep ntp
ntpdate-4.2.4p8-2.el6.i686
fontpackages-filesystem-1.41-1.1.el6.noarch
ntp-4.2.4p8-2.el6.i686
```

Par contre le service ntpd n'est pas démarré par défaut :

```
[root@centos6 ~]# chkconfig --list | grep ntpd
ntpd            0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
ntpdate         0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
```

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

```
[root@centos6 ~]# chkconfig --level 345 ntpd on
[root@centos6 ~]# chkconfig --list | grep ntpd
ntpd            0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
ntpdate         0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
```

> La commande **ntpdate**, utilisée pour synchroniser l'horloge **sans** utiliser le démon **ntpd** est maintenant remplacée par l'option **-q** de la commande **ntp**. Lors de l'utilisation de **ntpdate**, le démon **ntpd** doit être arrêté. Si ntpdate constatait que l'erreur de l'horloge local était supérieur à 0,5 secondes, celle-ci appelait la routine **settimeofday()** tandis que si l'erreur était inférieur à 0,5 secondes, elle appelait la

routine **adjtime()**.

Le fichier ntp.conf

Le service **ntpd** est configuré par le fichier **/etc/ntp.conf** :

ntp.conf

```
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

# Permit all access over the loopback interface.  This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict -6 ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
```

```
server 2.rhel.pool.ntp.org

#broadcast 192.168.1.255 autokey    # broadcast server
#broadcastclient            # broadcast client
#broadcast 224.0.1.1 autokey        # multicast server
#multicastclient 224.0.1.1      # multicast client
#manycastserver 239.255.254.254     # manycast server
#manycastclient 239.255.254.254 autokey # manycast client

# Undisciplined Local Clock. This is a fake driver intended for backup
# and when no outside source of synchronized time is available.
#server 127.127.1.0    # local clock
#fudge  127.127.1.0 stratum 10

# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
```

```
#statistics clockstats cryptostats loopstats peerstats
```

Les directives actives de ce fichier sont :

ntp.conf.bare

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
driftfile /var/lib/ntp/drift
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org
includefile /etc/ntp/crypto/pw
keys /etc/ntp/keys
```

Afin de mieux comprendre les détails de ce fichier, nous passons en revue ces directives.

Les directives suivantes permettent la synchronisation avec notre source ntp mais interdisent à cette source de faire de requêtes à notre serveur ou de modifier le service sur notre système :

```
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
```

Les directives suivantes permettent l'accès au serveur via l'interface loopback :

```
restrict 127.0.0.1
restrict -6 ::1
```

Les directives suivantes stipulent quel serveur est utilisé pour la synchronisation. La liste peut aussi comporter des numéros IP:

```
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org
```

Les directives ci-dessus sont souvent suivies par deux options : **server 0.rhel.pool.ntp.org iburst dynamic**. L'option **iburst** implique qu'en cas de non-disponibilité du serveur concerné, votre serveur enverra des lots de 8 paquets au lieu d'un seul. L'option **dynamic** permet la configuration de votre serveur même dans le cas où le serveur NTP distant n'est pas disponible car l'utilisation de cette option présume que le serveur distant deviendra disponible à un moment donné.

Les directives suivantes stipulent que votre serveur doit se synchroniser sur l'horloge locale, une horloge fictive, utilisée lors de l'inaccessibilité des serveurs sur Internet :

```
server 127.127.1.0                # local clock
fudge 127.127.1.0 stratum 10
```

Ces deux lignes étant en commentaire, il convient d'ôter les caractères **#** pour activer cette fonctionalité.

La directive suivante identifie le fichier contenant la déviation moyenne:

```
driftfile /var/lib/ntp/drift
```

La directive suivante indique le répertoire qui stocke les clefs symétriques lors d'accès sécurisés éventuels :

```
keys /etc/ntp/keys
```

La directive suivante génère des statistiques dans le répertoire **/var/log/ntpstats** :

```
statistics clockstats cryptostats loopstats peerstats
```

Etant en commentaire, il convient d'ôter le caractère **#** pour activer les statistiques.

Pour créer un fichier d'historique, il convient d'ajouter la directive suivante :

```
logfile /var/log/xntpd
```

Votre fichier /etc/ntp.conf deviendra donc :

ntp.conf

```
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

# Permit all access over the loopback interface.  This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict -6 ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 0.rhel.pool.ntp.org
server 1.rhel.pool.ntp.org
server 2.rhel.pool.ntp.org

#broadcast 192.168.1.255 autokey    # broadcast server
```

```
#broadcastclient            # broadcast client
#broadcast 224.0.1.1 autokey        # multicast server
#multicastclient 224.0.1.1      # multicast client
#manycastserver 239.255.254.254     # manycast server
#manycastclient 239.255.254.254 autokey # manycast client

# Undisciplined Local Clock. This is a fake driver intended for backup
# and when no outside source of synchronized time is available.
server  127.127.1.0    # local clock
fudge   127.127.1.0 stratum 10

# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8

# Enable writing of statistics records.
statistics clockstats cryptostats loopstats peerstats

logfile /var/log/xntpd
```

Options de la commande

Les options de la commande ntpd sont :

```
[root@centos6 ~]# ntpd --help
ntpd - NTP daemon program - Ver. 4.2.4p8
USAGE:  ntpd [ -<flag> [<val>] | --<name>[{=| }<val>] ]...
  Flg Arg Option-Name    Description
   -4 no  ipv4           Force IPv4 DNS name resolution
   -6 no  ipv6           Force IPv6 DNS name resolution
                - an alternate for ipv4
   -a no  authreq        Require crypto authentication
                - prohibits these options:
                authnoreq
   -A no  authnoreq      Do not require crypto authentication
                - prohibits these options:
                authreq
   -b no  bcastsync      Allow us to sync to broadcast servers
   -c Str configfile     configuration file name
   -d no  debug-level    Increase output debug message level
                - may appear multiple times
   -D Str set-debug-level Set the output debug message level
                - may appear multiple times
   -f Str driftfile      frequency drift file name
   -g no  panicgate      Allow the first adjustment to be Big
   -i Str jaildir        Jail directory
   -I Str interface      Listen on interface
                - may appear multiple times
   -k Str keyfile        path to symmetric keys
   -l Str logfile        path to the log file
   -L no  novirtualips   Do not listen to virtual IPs
   -n no  nofork         Do not fork
   -N no  nice           Run at high priority
```

```
   -p Str pidfile        path to the PID file
   -P Num priority       Process priority
   -q no  quit           Set the time and quit
   -r Str propagationdelay Broadcast/propagation delay
   -U Num updateinterval interval in seconds between scans for new or dropped interfaces
   -s Str statsdir       Statistics file location
   -t Str trustedkey     Trusted key number
                - may appear multiple times
   -u Str user           Run as userid (or userid:groupid)
   -v Str var            make ARG an ntp variable (RW)
                - may appear multiple times
   -V Str dvar           make ARG an ntp variable (RW|DEF)
                - may appear multiple times
   -x no  slew           Slew up to 600 seconds
   -m no  mlock          Lock memory
   -v opt version        Output version information and exit
   -? no  help           Display usage information and exit
   -! no  more-help      Extended usage information passed thru pager

Options are specified by doubled hyphens and their name
or by a single hyphen and the flag character.

The following option preset mechanisms are supported:
 - examining environment variables named NTPD_*



please send bug reports to:  http://bugs.ntp.org, bugs@ntp.org
```

Créez maintenant le fichier de journalisation :

```
[root@centos6 ~]# touch /var/log/xntpd
```

Ensuite modifiez le groupe associé à ce fichier :

```
[root@centos6 ~]# chgrp ntp /var/log/xntpd
```

Dernièrement modifiez les permissions sur le fichier de journalisation :

```
[root@centos6 ~]# chmod 664 /var/log/xntpd
```

LAB #2

> Modifiez votre fichier ntp.conf afin de dé-commenter les directives nécessaires et ajouter celle du fichier de journalisation. Démarrez le serveur ntp afin de tester celui-ci. Contrôlez la présence des statistiques et le contenu du fichier /var/log/xntpd.

Le Serveur FTP

Installation

Le paquet **vsftpd** *Very Secure FTP daemon* se trouve dans les dépôts CentOS.

```
[root@centos6 ~]# yum install vsftpd
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package vsftpd.i686 0:2.2.2-6.el6_2.1 set to be updated
```

```
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================
 Package                                Arch                                Version
Repository                               Size
================================================================================================================
================================================
Installing:
 vsftpd                                 i686                                2.2.2-6.el6_2.1
updates                                155 k

Transaction Summary
================================================================================================================
================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 155 k
Installed size: 343 k
Is this ok [y/N]: y
Downloading Packages:
vsftpd-2.2.2-6.el6_2.1.i686.rpm
| 155 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : vsftpd-2.2.2-6.el6_2.1.i686
1/1

Installed:
```

```
  vsftpd.i686 0:2.2.2-6.el6_2.1

Complete!
```

Par contre le service vsftpd n'est pas démarré par défaut :

```
[root@centos6 ~]# chkconfig --list vsftpd
vsftpd          0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
```

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

```
[root@centos6 ~]# chkconfig --level 345 vsftpd on
[root@centos6 ~]# chkconfig --list vsftpd
vsftpd          0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
```

Avant de poursuivre, modifiez le mode de **SELinux** de **enforced** à **permissive** pour la session en cours :

```
[root@centos6 ~]# setenforce permissive
[root@centos6 ~]# getenforce
Permissive
```

Ensuite éditez le fichier **/etc/selinux/config** ainsi :

config.selinux

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
```

```
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Configuration de base

Le fichier de configuration de vsftpd est **/etc/vsftpd/vsftpd.conf** :

vsftpd.conf

```
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
```

```
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
```

```
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
```

```
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=YES
#
# This directive enables listening on IPv6 sockets. To listen on IPv4 and IPv6
# sockets, you must run two copies of vsftpd with two configuration files.
# Make sure, that one of the listen options is commented !!
#listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

Les directives actives de ce fichier sont :

vsftpd.conf.bare

```
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

Ces directives sont détaillées ci-après :

Directive	**Valeur par Défaut**	**Description**
anonymous_enable	YES	Si oui, autorise les connexions anonymes
local_enable	YES	Si oui, autorise des connexions par des utilisateurs ayant un compte valide sur le système
write_enable	YES	Si oui, permet l'écriture
local_umask	022	Spécifie la valeur de l'umask lors de la création de fichiers et de répertoires
dirmessage_enable	NO	Si oui, permet d'afficher le contenu du fichier .message quand un utilisateur rentre dans le répertoire
xferlog_enable	NO	Si oui, permet d'activer la journalisation dans le fichier **/var/log/vsftpd.log**
connect_from_port_20	NO	Permet les connexions de ftp-data
listen	NO	Si oui, vfsftpd fonctionne en mode Standalone et non en tant que sous-service de xinetd
pam_service_name	S/O	Indique le nom du service PAM utilisé par vsftpd
userlist_enable	NO	Si oui, vsftpd charge une liste d'utilisateurs spécifiés dans le fichier identifié par la directive **userlist_file**. Si un utilisateur spécifié dans la liste essaie de se connecter, la connexion sera réfusée avant la demande d'un mot de passe
tcp_wrappers	NO	Si oui, vsftpd utilise TCP WRAPPERS

/etc/ftpusers

Votre serveur FTP est maintenant configuré pour les connexions en provenance des utilisateurs ayant un compte sur votre système.

Dans le cas où vous souhaiteriez **interdire** la connexion vers le serveur de certaines personnes mais pas de toutes les personnes ayant un compte système, éditez le fichier **/etc/ftpusers**.

Voici la liste des utilisateurs système qu'il convient d'ajouter à ce fichier:

ftpusers

```
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
uucp
operator
gopher
nobody
dbus
vcsa
rpc
nscd
tcpdump
haldaemon
apache
nslcd
postfix
avahi
```

```
ntp
rpcuser
sshd
gdm
vboxadd
named
```

Il est ensuite nécessaire d'inclure une directive supplémentaire dans le fichier /etc/vsftpd/vsftpd.conf :

```
...
userlist_file=/etc/ftpusers
...
```

et de démarrer le serveur :

```
[root@centos6 ~]# service vsftpd start
Démarrage de vsftpd pour vsftpd :                          [  OK  ]
```

Testez maintenant le serveur :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): trainee
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/trainee"
ftp>
```

Bien que trainee puisse se connecter, ce n'est pas le cas pour **root** :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): root
530 Permission denied.
Login failed.
```

Pour **chrooter** l'utilisateur dans son répertoire personnel, il convient d'ajouter la directive suivante au fichier /etc/vsftpd/vsftpd.conf :

```
...
chroot_local_user=YES
...
```

et de redémarrer le serveur :

```
[root@centos6 ~]# service vsftpd restart
Arrêt de vsftpd :                                          [  OK  ]
Démarrage de vsftpd pour vsftpd :                          [  OK  ]
```

Lors de sa prochaine connexion, l'utilisateur voit son répertoire personnel comme la racine du système de fichiers :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): trainee
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
```

```
ftp>
```

Serveur vsftpd Anonyme

Configuration

Le serveur anonyme étant déjà configuré par la présence de la directive **anonymous_enable=YES**, il convient de tester celui-ci :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> ls
227 Entering Passive Mode (127,0,0,1,143,6).
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jan 03 01:21 pub
226 Directory send OK.
ftp> quit
221 Goodbye.
```

Le répertoire pour les connexions anonymes est **/var/ftp** :

```
[root@centos6 ~]# ls -l /var | grep ftp
drwxr-xr-x.  3 root root  4096 31 mai   15:12 ftp
```

Par défaut il contient un répertoire **pub** :

```
[root@centos6 ~]# ls -l /var/ftp
total 4
drwxr-xr-x. 2 root root 4096  3 janv. 02:21 pub
```

Pour permettre aux utilisateurs anonymes de transférer des fichiers vers le serveur, il faut d'abord créer un répertoire **upload** dans **/var/ftp/pub** et de l'affecter à ftp:ftp :

```
[root@centos6 ~]# mkdir /var/ftp/pub/upload
[root@centos6 ~]# chown ftp:ftp /var/ftp/pub/upload
```

Ensuite il faut ajouter la directive suivante au fichier **/etc/vsftpd/vsftpd.conf** :

```
...
anon_upload_enable=YES
...
```

Votre fichier de configuration ressemblera donc à :

vsftpd.conf.anon

```
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

```
userlist_file=/etc/ftpusers
anon_upload_enable=YES
chroot_local_user=YES
```

Testez ensuite votre configuration :

```
[root@centos6 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (127,0,0,1,70,196).
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 May 31 14:03 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> cd upload
250 Directory successfully changed.
ftp> put rndc.key
local: rndc.key remote: rndc.key
227 Entering Passive Mode (127,0,0,1,238,121).
150 Ok to send data.
226 Transfer complete.
77 bytes sent in 0,0349 secs (2,21 Kbytes/sec)
ftp> ls
227 Entering Passive Mode (127,0,0,1,230,251).
150 Here comes the directory listing.
```

```
-rw-------    1 14       50              77 May 31 14:09 rndc.key
226 Directory send OK.
```

Serveur vsftpd et Utilisateurs Virtuels

Introduction

Le serveur vsftpd utilise le système PAM pour gérer les authentifications. Le module concerné est **pam_userdb**. Ce module consulte une base de données au format Berkeley pour obtenir les coordonnées de connexion des utilisateurs.

Configuration

Pour configurer des utilisateurs virtuels, il convient de créer un fichier de configuration à part, **/root/vftpusers** , dans lequel on inscrit le nom et le mot de passe des utilisateurs virtuels :

vftpusers

```
alexandre
123456789
```

Ce fichier doit ensuite être converti au format Berkeley :

```
[root@centos6 ~]# db_load -T -t hash -f /root/vftpusers /etc/vsftpd/vftpusers.db
```

Modifiez ensuite les permissions sur le fichier **/etc/vsftpd/vftpusers.db** et supprimez le fichier **/root/vftpusers** :

```
[root@centos6 ~]# chmod 600 /etc/vsftpd/vftpusers.db
[root@centos6 ~]# rm -f /root/vftpusers
```

Créez ensuite un fichier PAM **/etc/pam.d/vftpusers** :

vftpusers

```
#%PAM-1.0
auth    required    pam_userdb.so    db=/etc/vsftpd/vftpusers
account required    pam_userdb.so    db=/etc/vsftpd/vftpusers
session required    pam_loginuid.so
```

Notez que **pam_userdb.so** ajoute automatiquement l'extension **.db** aux noms des fichiers de base de données.

Modifiez maintenant le fichier /etc/vsftpd/vsftpd.conf :

```
...
pam_service_name=vftpusers
guest_enable=YES
guest_username=ftp
virtual_use_local_privs=YES
...
```

Votre fichier de configuration ressemblera à :

vsftpd.conf

```
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
```

```
connect_from_port_20=YES
xferlog_std_format=YES
listen=YES
pam_service_name=vftpusers
guest_enable=YES
guest_username=ftp
virtual_use_local_privs=YES
userlist_enable=YES
tcp_wrappers=YES
userlist_file=/etc/ftpusers
anon_upload_enable=YES
chroot_local_user=YES
```

Redémarrez le service vsftpd :

```
[root@centos6 ~]# service vsftpd restart
Arrêt de vsftpd :                                          [  OK  ]
Démarrage de vsftpd pour vsftpd :                          [  OK  ]
```

Testez ensuite la configuration :

```
[root@centos6 log]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:trainee): alexandre
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> ls
```

```
227 Entering Passive Mode (127,0,0,1,214,118).
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 May 31 14:03 pub
226 Directory send OK.
```

Notez que les utilisateurs virtuels atterrissent dans le répertoire personnel du compte indiqué par la directive **guest_username** du fichier **/etc/vsftpd/vsftpd.conf**.

LAB #3

Configurez votre serveur ftp anonyme et un utilisateur virtuel.

Le Serveur DHCP

Introduction

Un serveur DHCP (**Dynamic Host Configuration Protocol**) est un ordinateur exécutant un logiciel serveur DHCP. L'avantage de la présence d'un serveur DHCP sur le réseau local est que celui-ci permet de spécifier à un niveau central les paramètres TCP/IP.

Installation

Pour installer le serveur DHCP, il convient d'utiliser **yum**.

D'abord déinstallez le paquet du client dhcp :

```
[root@centos6 ~]# yum remove dhclient
...
```

Ensuite installez le serveur dhcp :

```
[root@centos6 ~]# yum install dhcp
...
```

Vérifiez ensuite que le service dhcpd est activé au démarrage du serveur:

```
[root@centos6 ~]# chkconfig --list dhcpd
dhcpd           0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
```

Activez donc le serveur dhcpd dans les niveaux d'exécution 3, 4 et 5 :

```
[root@centos6 ~]# chkconfig --level 345 dhcpd on
[root@centos6 ~]# chkconfig --list dhcpd
dhcpd           0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
```

Configuration de base

Le fichier dhcpd.conf

Lors de l'installation du paquetage, un fichier **dhcpd.conf.sample** est installé dans /usr/share/doc/dhcp-4.1.1/. Ce fichier est un exemple du fichier de configuration du serveur DHCP, **dhcpd.conf** :

```
[root@centos6 ~]# cat /usr/share/doc/dhcp-4.1.1/dhcpd.conf.sample
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
```

```
# option definitions common to all supported networks...
option domain-name "example.org";
option domain-name-servers ns1.example.org, ns2.example.org;

default-lease-time 600;
max-lease-time 7200;

# Use this to enble / disable dynamic dns updates globally.
#ddns-update-style none;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.

subnet 10.152.187.0 netmask 255.255.255.0 {
}

# This is a very basic subnet declaration.

subnet 10.254.239.0 netmask 255.255.255.224 {
  range 10.254.239.10 10.254.239.20;
  option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.
```

```
subnet 10.254.239.32 netmask 255.255.255.224 {
  range dynamic-bootp 10.254.239.40 10.254.239.60;
  option broadcast-address 10.254.239.31;
  option routers rtr-239-32-1.example.org;
}

# A slightly different configuration for an internal subnet.
subnet 10.5.5.0 netmask 255.255.255.224 {
  range 10.5.5.26 10.5.5.30;
  option domain-name-servers ns1.internal.example.org;
  option domain-name "internal.example.org";
  option routers 10.5.5.1;
  option broadcast-address 10.5.5.31;
  default-lease-time 600;
  max-lease-time 7200;
}

# Hosts which require special configuration options can be listed in
# host statements.   If no address is specified, the address will be
# allocated dynamically (if possible), but the host-specific information
# will still come from the host declaration.

host passacaglia {
  hardware ethernet 0:0:c0:5d:bd:95;
  filename "vmunix.passacaglia";
  server-name "toccata.fugue.com";
}

# Fixed IP addresses can also be specified for hosts.   These addresses
# should not also be listed as being available for dynamic assignment.
# Hosts for which fixed IP addresses have been specified can boot using
# BOOTP or DHCP.   Hosts for which no fixed address is specified can only
# be booted with DHCP, unless there is an address range on the subnet
# to which a BOOTP client is connected which has the dynamic-bootp flag
```

```
# set.
host fantasia {
  hardware ethernet 08:00:07:26:c0:a5;
  fixed-address fantasia.fugue.com;
}

# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

class "foo" {
  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
}

shared-network 224-29 {
  subnet 10.17.224.0 netmask 255.255.255.0 {
    option routers rtr-224.example.org;
  }
  subnet 10.0.29.0 netmask 255.255.255.0 {
    option routers rtr-29.example.org;
  }
  pool {
    allow members of "foo";
    range 10.17.224.10 10.17.224.250;
  }
  pool {
    deny members of "foo";
    range 10.0.29.10 10.0.29.230;
  }
}
```

Créez un fichier **dhcpd.conf** dans le répertoire **/etc/dhcp**.

Editez-le ainsi :

dhcpd.conf

```
#
# Section Globale
#
ddns-update-style none;
DHCPD_INTERFACE = "eth0";
#
# Section sous-réseau
#
subnet 10.0.2.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option routers 10.0.2.2;
  option domain-name-servers 10.0.2.15;
  option domain-name-servers 10.0.2.3;
  option ntp-servers 10.0.2.15;
  option domain-name "fenestros.loc";
  default-lease-time 28800;
  max-lease-time 86400;
  not authoritative;

  pool {
       range 10.0.2.100 10.0.2.150;
       }
}
```

Ce fichier doit commencer avec une section globale. Notez que chaque directive se termine par ;.

Cette ligne définit l'interface réseau pour le serveur DHCP

```
DHCPD_INTERFACE = "eth0";
```

Cette ligne définit le réseau pour lequel ce serveur est un serveur dhcp et déclare l'ouverture de la section de directives concernant ce réseau

```
subnet 10.0.2.0 netmask 255.255.255.0 {
```

Cette ligne définit le masque de sous-réseau

```
option subnet-mask 255.255.255.0;
```

Cette ligne définit la passerelle par défaut

```
option routers 10.0.2.2;
```

Cette ligne définit le serveur DNS de notre réseau :

```
option domain-name-servers 10.0.2.15;
```

Cette ligne définit le serveur DNS *upstream* :

```
option domain-name-servers 10.0.2.3;
```

Cette ligne définit le serveur d'horloge :

```
option ntp-servers              10.0.2.15;
```

Cette ligne nomme notre domaine :

```
option domain-name "fenestros.loc";
```

Cette ligne définit la valeur des baux par défaut :

```
default-lease-time 28800;
```

Cette ligne définit les valeur maximum des baux par défaut :

```
max-lease-time 86400;
```

Cette ligne stipule que le serveur ne tiendra pas compte d'une demande d'un client sur un segment de réseau autre que le sien :

```
not authoritative;
```

Cette ligne déclare la fermeture de la section spécifique au réseau 10.0.2.0 :

```
  }
```

Cette ligne définit l'ouverture de la section de directives concernant la plage d'adresses disponibles pour les clients

```
  pool {
```

Cette ligne définit la plage des adresses disponibles pour les clients

```
range 10.0.2.100 10.0.2.150;
```

Selon ce fichier de configuration, lorsque un client demande une adresse IP au serveur DHCP, le client reçois les informations suivantes :

- La première adresse IP disponible dans la plage,
- Le nom du domaine, à savoir « fenestros.loc »,
- L'adresse IP du serveur DNS primaire, à savoir notre serveur DNS - la 10.0.2.15,
- L'adresse IP du serveur DNS secondaire, à savoir la 10.0.2.3,
- L'adresse IP du passerelle, à savoir la 10.0.2.2,
- L'adresse IP du serveur d'horloge, à savoir la 10.0.2.15,
- La durée du bail, à savoir 28800 secondes soit 8 heures,
- La durée maximal du bail, à savoir 86400 secondes, soit 24 heures.

Afin de suivre l'état des baux accordés, le serveur DHCP les inscrit dans le fichier **/etc/dhcp.leases**. Dans ce fichier, il faut noter que les heures indiquées sont en **UTC** (GMT).

<note tip> Pour plus d'information concernant les autres options du fichier dhcpd.conf, consultez la traduction en français du manuel de DHCPD qui se trouve à **cette adresse**. </note>