

BIND-9. | Installation d'un serveur DNS

Table des Matières

<u>Installation d'un DNS, BIND 9</u>	1
<u>1. Introduction</u>	1
<u>2. Bind version 9</u>	1
<u>3. Commentaires</u>	1
<u>4. Conclusion</u>	1
<u>Introduction</u>	2
<u>Avant propos</u>	2
<u>Convention</u>	2
<u>BIND version 9</u>	3
<u>Nouveautés dans bind-9.x:</u>	3
<u>Configuration de bind-9</u>	4
<u>Test de bind et de votre config DNS</u>	6
<u>Utilisation de la commande dig</u>	6
<u>NOTE</u>	7
<u>Commentaires</u>	8
<u>Syntaxe des fichiers de Zone</u>	8
<u>Conclusion</u>	10

Installation d'un DNS, BIND 9

Version 0.2.1-2 du 15-03-2002

© 1996-2002 copyleft Michel Luc

cern91@tuxfamily.org

Permission vous est accordée de distribuer des copies exactes ou modifiées de ces articles tant que ces lignes de permission et le copyright apparaissent dans vos copies et tant que ces copies restent sous licence FDL.

1. [Introduction](#)

- [Avant propos](#)
- [Convention](#)

2. [Bind version 9](#)

- [Nouveautés dans bind-9.x](#)
- [Configuration de bind-9](#)
 - ◆ [Test de bind](#)
 - ◆ [Commande dig](#)
- [Note](#)

3. [Commentaires](#)

- [Syntaxe des fichiers de Zone](#)

4. [Conclusion](#)

[Page suivante](#) [Page précédente](#) [Table des matières](#)

Introduction

Avant propos

Vous trouverez sur le site cern91 [cern91.cern91.tuxfamily.org](http://cern91.tuxfamily.org), un document plus détaillé sur l'installation et la configuration d'un serveur DNS.

Ici je vais simplement commenter la configuration de Bind-9. pour une comparaison avec les versions 8 de Bind.

Convention

Je reprend l'exemple déjà utilisé dans la page configuration d'un DNS sur cern91, donc:

le serveur DNS, la machine **orion** sur un réseau Ethernet **192.168.154.0**, reliée à l'internet par modem et utilisant Worldnet (par exemple) comme FAI :

Cette machine **orion** sera le serveur (primaire) de nom de domaine avec l'adresse IP **192.168.154.1**

Le nom de domaine de ce réseau est **linuxpc.fr**, les autres machines reliées au réseau, sont :

droopy : 192.168.154.2, **cern** : 192.168.154.3, **lmsoft** : 192.168.154.4

Adapter, évidemment, le nom des machines, le nom du domaine et les adresses IP à votre réseau !

orion.linuxpc.fr 192.168.154.1

droopy.linuxpc.fr 192.168.154.2

cern.linuxpc.fr 192.168.154.3

lmsoft.linuxpc.fr 192.168.154.4

Configuration et fichiers de zone:

Le principal fichier de configuration est `/etc/named.conf`, ensuite vous avez besoin de trois autres fichiers qui sont les fichiers de zone à placer dans le répertoire `/var/named/`.

Les noms de ces fichiers de zone ont peu d'importance, l'essentiel est qu'ils soient déclarés dans `/etc/named.conf`, j'ai conservé les noms des fichiers mis en place par l'installation de bind, mais vous faites à votre goût :

named.local : Cette zone contient un seul enregistrement qui permet de résoudre "**127.0.0.1**" en **localhost**

Vous pouvez très bien utiliser un nom comme `localhost.zone`, `127.0.0`, `db0.0.127...` etc.

linuxpc.fr : Cette zone décrit le domaine, c'est à dire la liste des adresses IP des machines sur ce domaine (ici `linuxpc.fr`).

db.192.168.154 : Cette zone va permettre la résolution inverse des noms de machines sur le domaine, c'est à dire renvoyer le nom de machine à partir de l'adresse IP, elle doit donc contenir également les noms des machines sur le domaine et leurs adresses IP correspondantes.

A propos du nom de domaine et plus particulièrement du **TLD** (Top Level Domain), si vous utilisez un TLD déjà attribué sur internet comme, `.fr`, `.com`, `.org`, `.net...` etc. il est indispensable d'ajouter "**notify no;**" dans la définition de zone dans votre fichier `named.conf`, ceci pour éviter tout conflit avec l'internet pendant que vous surfer sur le web ;-)

Le plus indiqué étant de ne pas utiliser un TLD existant mais un autre comme `.home`, `.tux`, `.pc....` etc.

Voici les fichiers de configuration utilisés, il vous reste à modifier le nom des machines et du domaine pour les adapter à votre système.

[Page suivante](#) [Page précédente](#) [Table des matières](#)

BIND version 9

Nouveautés dans bind-9.x:

Une meilleure sécurité, entre autre, avec BIND version 9 mais aussi une syntaxe un peu différente, **DiG 9.1.** a remplacé "DiG 8.2.", il est conseillé d'utiliser **host** en remplacement de "nslookup", "ndc" est remplacé par **rndc**.

Commencez par vérifier que, dans le répertoire /etc, vous avez bien un fichier **rndc.conf** et certainement aussi un fichier **rndc.key**.

rndc.key contient la clé md5, également présente à la fin du fichier **rndc.conf** sous la forme :

```
key "key" {
    algorithm      hmac-md5;
    secret "QOnXmEIGx0RWeQ0NZ0GtLcQmSDBympnctTaCwPxTjvYYoTUcsXbQAHrZBMtt ";
};
```

Il vous faut ajouter cette clé au début de votre fichier /etc/**named.conf**, 2 cas sont possibles :

_1) /etc/**rndc.key** existe, alors :

```
// /etc/named.conf

include "/etc/rndc.key";

controls {
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
```

_2) vous avez seulement /etc/**rndc.conf**, alors :

```
// /etc/named.conf

key "key" {
    algorithm      hmac-md5;
    secret "QOnXmEIGx0RWeQ0NZ0GtLcQmSDBympnctTaCwPxTjvYYoTUcsXbQAHrZBMtt ";
};

controls {
    inet 127.0.0.1 allow { localhost; } keys { "key"; };
};
```

Si vous avez ajouté les DNS de votre FAI, donc pour une connexion internet, remplacez "localhost;" par "any;".

En plus de la syntaxe à modifier dans vos fichiers de zone, vous devrez certainement ajouter dans chaque fichier de zone, comme première ligne du fichier : **\$TTL 3h** ou **\$TTL 86400**.

Par défaut les fichiers **named.conf** et **rndc.conf** sont lisibles par tous, il faut corriger cela en donnant les droits sur ces fichiers à root ou named et au groupe named, par exemple:

chown root.named named.conf

ou

chown named.named named.conf

et ensuite :

chmod 640 named.conf

Vous faites la même chose sur tous les fichiers qui contiennent la clé md5.

Configuration de bind-9.

Le principe reste identique à ce que j'ai décrit dans la page Installer un DNS sur [cern91](#), donc je vous donne ici simplement le contenu, sans commentaire, des différents fichiers de zone et du fichier de configuration /etc/named.conf.

...**ATTENTION !** J'ai effectué les tests en installant des archives Tarball et non des RPMs, j'ignore donc si les packages RPMs fonctionnent correctement !?

Version 9.1.

Fichier de configuration:

named.conf :

```
/* /etc/named.conf
 * generated by named-bootconf.pl
 */

include "/etc/rndc.key";

options {
    directory "/var/named";
    /*
     * If there is a firewall between you and nameservers you want
     * to talk to, you might need to uncomment the query-source
     * directive below. Previous versions of BIND always asked
     * questions using port 53, but BIND 8.1 uses an unprivileged
     * port by default.
     */
    // query-source address * port 53;
    // ISP IP Address, Worldnet Provider DNS :
    forward first;
    forwarders {
        195.3.4.1;
        195.3.4.2;
    };
};

//
// a caching only nameserver config
//
controls {
    inet 127.0.0.1 allow { any; } keys { rndckey; };
};

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

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

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.local";
    allow-update { none; };
};

zone "linuxpc.fr" IN {
    type master;
    file "linuxpc.fr";
};
```

```
zone "154.168.192.in-addr.arpa" IN {
    type master;
    file "db.192.168.154";
};
```

Fichiers de zone :

named.local:

```
$TTL      86400
@         IN      SOA      localhost. root.localhost. (
                                1997022700 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum ttl
                                IN      NS      localhost.
1         IN      PTR      localhost.
```

localhost.zone :

```
$TTL      86400
$ORIGIN   localhost.
@         1D IN SOA      @ root (
                                42        ; serial (d. adams)
                                3H        ; refresh
                                15M       ; retry
                                1W        ; expiry
                                1D )      ; minimum
                                1D IN NS   @
                                1D IN A    127.0.0.1
```

linuxpc.fr :

```
$TTL 86400
@         IN      SOA      orion.linuxpc.fr. postmaster.orion.linuxpc.fr. (
                                2002031200 ; serial
                                28800 ; refresh
                                7200 ; retry
                                604800 ; expire
                                86400 ; ttl
                                )
@         IN      NS      orion.linuxpc.fr.
@         IN      MX      10 mail.linuxpc.fr.
@         IN      MX      20 orion.linuxpc.fr.
@         IN      TXT     "linuxpc.fr domaine Linux FR sur PC "

; serveurs de noms
localhost      IN      A      127.0.0.1
orion          IN      A      192.168.154.1
mail           IN      A      192.168.154.1

; adresses IP des machines du reseau
droopy        IN      A      192.168.154.2
cern          IN      A      192.168.154.3
lmsoft        IN      A      192.168.154.4

; aliases
www           IN      CNAME    orion
ftp           IN      CNAME    orion
```

```
news      IN      CNAME      orion
```

db.195.168.154 :

```
$TTL 86400
@          IN      SOA      orion.linuxpc.fr. postmaster.orion.linuxpc.fr. (
                                2002031200 ; serial
                                28800 ; refresh
                                7200 ; retry
                                604800 ; expire
                                86400 ; ttl
                                )

; serveurs de noms
@          IN      NS       orion.linuxpc.fr.

; adresses IP inverses
1          IN      PTR      orion.linuxpc.fr.
2          IN      PTR      droopy.linuxpc.fr.
3          IN      PTR      cern.linuxpc.fr.
4          IN      PTR      lmsoft.linuxpc.fr.
```

Test de bind et de votre config DNS

Pour tester la configuration de votre DNS en remplacement de "nslookup", bien que toujours disponible, la doc de BIND conseille l'utilisation de **host**:

```
host -a orion
host -a linuxpc.fr
host -a www.linuxpc.fr
....etc.
```

Utilisation de la commande dig

Pour récupérer le fichier de zone internet (named.ca) le script décrit, dans la page Installer un DNS sur cern91, pour "DiG 8.2" ne fonctionne pas avec la version **DiG 9.1.3** de **bind-9.1.3**.

Utilisez **@a.root-servers.net** à la place de "@rs.internic.net" :

Après vous être connecté, pour afficher le contenu de named.ca, tapez simplement:

```
dig
Pour récupérer ce fichier named.ca, tapez:
dig @a.root-servers.net > /var/named/named.ca
ou
dig > /var/named/named.root
```

et comparez le contenu de ces 2 fichiers (named.ca et named.root) qui doit être identique.

Pour vous amuser, essayez, en remplaçant orion par le nom de machine de votre serveur DNS, cette commande:

```
dig @a.root-servers.net . orion > ~/named.ca
```

et regardez le contenu du fichier **~/named.ca**,

vous comprendrez pourquoi vous ne pouvez pas utiliser le script de la version 8.2, ni même utiliser la commande :

```
dig @a.root-servers.net . orion >/var/named/named.ca.new 2>&1
```

pour mettre à jour votre fichier **named.ca**.

NOTE

Version 9.2.

Pour la version 9.2, j'ai utilisé la forme :

```
NS orion.linuxpc.fr.
```

à la place de

```
@ IN NS orion.linuxpc.fr.
```

et cela fonctionne très bien !

[Page suivante](#) [Page précédente](#) [Table des matières](#)

Commentaires

Syntaxe des fichiers de Zone

Forme et syntaxe :

Le @ (\$ORIGIN) au début d'une ligne pour définir une zone n'est pas indispensable (voir le [DNS-HOWTO](#)). La syntaxe pour **Bind 9.1** et **Bind 9.2** est différente, regardez la section suivante [Nouveautés de la version 9 de BIND](#)

SOA :(Start Of Authority ou Origine de l'Autorité) doit être suivi du nom du serveur (machine réelle et physique) et de l'adresse du responsable qui administre le domaine, ces deux noms complets de domaine doivent se terminer par un point .

Vous avez noté l'importance du point qui caractérise un nom de domaine pleinement qualifié, si le point est absent à la fin du nom de domaine alors le nom du domaine définit dans **named.conf** (dans la zone correspondante) sera automatiquement ajouter à la fin, ce qui dans notre cas pour "**NS orion.linuxpc.fr**" donnerai **orion.linuxpc.fr.linuxpc.fr** ??? mais est correcte avec "**NS orion**" et donne **orion.linuxpc.fr**

postmaster@orion.linuxpc.fr le @ est remplacé par un . : **postmaster.orion.linuxpc.fr**
postmaster.orion.linuxpc.fr , en fait "postmaster" est un alias déclaré dans /etc/aliases et vous pouvez utiliser l'alias qu vous plait, mais il doit correspondre à un compte sur la machine, par exemple si vous utilisez **domainmaster.orion.linuxpc.fr** /etc/aliases doit contenir la ligne **domainmaster : toto** , "**toto**" étant un compte ayant les droits d'administration sur la machine et cette adresse sera interprétée comme **toto@orion.linuxpc.fr** et recevra tout le courrier concernant l'administration du domaine .
ATTENTION ! Chaque fois que vous modifiez le fichier /etc/**aliases** vous devez taper la commande **newaliases** .

Le numéro de série : Il est judicieux d'augmenter ce numéro après chaque nouvelle modification des fichiers de configuration, aussi le plus parlant est d'utiliser la date suivi d'un numéro de version indiquant le nombre de modif (release), mais ce n'est pas une obligation vous pouvez simplement mettre 01, 02, 03 ...etc.
Pourquoi utiliser la forme **1999112002** pour le 20 novembre 1999 et non la forme (FR) 2011199902 :
Supposez que la prochaine modification (03) soit effectué le 2 décembre 1999 cela donne **1999120203** > 1999112002, dans le cas (FR) = **0212199903** < 2011199902 .
Ce numéro de série sert à synchroniser les serveurs maîtres et esclaves, il doit donc augmenter à chaque modification de la zone.

NS Ce champ indique le serveur de noms pour la résolution nom de machine/adresse IP.

IN C'est un mot clé (optionnel) qui indique qu'il s'agit d'une zone INternet.

MX qui indique le serveur de Mail (Xchanger) est suivi d'un nombre: c'est l'indice de priorité .
Ce nombre indique au gestionnaire de courrier à quelle machine envoyer en priorité le courrier, dans notre cas c'est orion (le plus petit nombre) qui est prioritaire sur orion.linuxpc.fr. : C'est la même machine !?
Pour un réseau plus important et/ou un courrier abondant, vous pouvez désigner plusieurs machines :

```
MX      5  orion.linuxpc.fr.  
MX      10 droopy.linuxpc.fr.  
MX      20 cern.linuxpc.fr.
```

A Ce champ va retourner l'adresse IP correspondante, par exemple définir le nom du serveur de messagerie (MX) comme "mail.linuxpc.fr" qui correspond au serveur orion **orion.linuxpc.fr** que l'on pourra donc

atteindre avec **mail.linuxpc.fr**

```
mail      IN      A      192.168.154.1
```

PTR ce champ permet la résolution inverse en indiquant par exemple que **1** (154.168.192.in-addr.arpa) correspond à 192.168.154.**1**

```
1         IN      PTR    orion.linuxpc.fr.
```

notify no : il est préférable d'utiliser ce paramètre pour éviter toute pollution de l'Internet avec vos adresses privées, et à plus fortes raisons si vous vous amusez à utiliser des adresses comme 198.32.x.x qui sont attribuées .

[Page suivante](#) [Page précédente](#) [Table des matières](#)

Conclusion

Cette courte description ne saurait en rien remplacer le [DNS-HOWTO](#).

Doc en ligne sur le Web aux formats PDF, HTML et autres:

Configurer un DNS sur Mandrake: <http://www.funix.org> rubrique Linux/DNS

Installer un DNS: <http://www.linuxenrezo.org> Ce site ferme définitivement en fin d'année 2002.

Méthode d'installation d'un DNS: <http://www.linux-france.org/article/>

Serveur DNS: <http://www.lea-linux.org> Récupérez le "LeaBook" Ça peut servir !

Page suivante [Page précédente](#) [Table des matières](#)