Installer un server DNS en local bind9

- Objet : Installer un server DNS maître en local
- Niveau requis :
  avisé
- Suivi :
  tester
  - Création par Hypathie le 01/09/2014
  - Testé par ... le ...
- Commentaires sur le forum : Lien vers le forum concernant ce tuto [1)]

Source : http://archil.fr/Doc_install_BIND.html

Introduction au DNS

Quelques bases sur les servers DNS

DNS permet une correspondance entre nom d'hôte (FQDN) et adresse IP.
Principe de hiérarchie :

- serveur racine (serveur DNS de plus haut niveau (.)
- serveur TLD : Top Level Domaine (com org net fr ...)
- Domaine (toto.fr)
- hôte (www)
  Par exemple www.toto.com.
  il peut y avoir des sous-domaines comme par exemple, www.domaine1.toto.com..

Le point après com est sous-entendu pour l'utilisation du côté client, mais pas dans la configuration du DNS.

Tout cela compose le **FQDN** (fool domaine name).

- Exemple :

Un client souhaite savoir à quel adresse IP correspond **www.toto.com**.

Dans l'ordi de ce client on a configuré un ou plusieurs DNS dans le fichier **/etc/resolv.conf** dans lequel est indiqué l'adresse IP de serveur local Bind comme server de référence.

Cette ordi a donc l'adresse IP d'un DNS est lui pose la question “donne moi l'IP de **www.toto.com**.

Si le server sait répondre il lui donne l'IP, s'il ne sait pas il va interroger les serveurs DNS au dessus de lui, TLD, Racine...
Quand il a l'adresse, il répond au client qui peut joindre l'ordi de toto.com

Vocabulaire

- Zone : Ensemble des directives correspondantes à un Domaine. À chaque zone correspond un fichier. (Une zone n'est pas forcément un domaine).
- DNS récursif : DNS capable d'interroger d'autres servers DNS, lorsqu'il ne parvient à trouver un serveur faisant autorité sur le nom de domaine recherché.
- Serveur “primaire” ou “maître” (d'une zone), en anglais serveur “authoritive”) : serveur qui a la configuration de sa zone grâce à un fichier. C'est le serveur principal d'une domaine.
- Serveur secondaire : serveur qui des informations sur une zone à partir d'un serveur primaire et non grâce à sa configuration.
- Faire autorité sur un domaine : C'est le fait pour un serveur DNS de répondre directement aux requêtes un domaine, sans passer par un autre serveur ou un cache. Le cache c'est le fichier dans lequel le serveur DNS récursif conserve l'information qu'il a obtenu d'un autre serveur à la suite d'une requête qui lui a été faite par un client.

Donc les serveur qui font autorité sur un domaine sont, soit des serveurs primaires, soit des serveurs secondaires s'ils ont une copie de ces informations.

Composants de bind 9

bind : Berkeley Internet Name Daemon

Version 9 : stable, sécurisée est celle dont il s'agit .

(Version 10 depuis 2013 intègre le DHCP.)

/usr/sbin/named

Le programme qui lance le serveur.

/etc/init.d/bind9

Permet de gérer bind.

- En **root** :
  - **`/etc/init.d/bind9 stop`** : pour arrêter
  - **`/etc/init.d/bind9 start`** : pour rédémarrer
  - **`/etc/init.d/bind9 restart`** : pour redémarrer (si il était démarrer, avec restart, il est éteint, puis redémarrer avec un nouveau processus
  - **`/etc/init.d/bind9 reload`** : pour recharger la configuration (ne stoppe pas avant de recharger

On peut aussi utiliser **`service`** avec chacune des commandes décrites pour init.d par exemple :

```
service bind9 restart
```

L'utilitaire rndc

/usr/sbin/rndc est le fichier binaire de l'utilitaire de contrôle rndc.
Il permet de gérer Bind9

```
rndc [b source-adress] [-c config-file] [k key-file] [-s serveur]
 [-p port] [-V] [-y key-id] {commande}
```

- Après l'installation de bind9, on peut utiliser les commandes rndc suivantes :
  - **`reload`** : pour recharger
  - **`stop`** : arrêter le serveur
  - **`flush`** : vider le cache
  - **`status`** : afficher l'état du serveur
  - **aucune** : liste des commandes utilisables

/etc/bind/named.conf

C'est le fichier de configuration centrale de bind.
Il peut se trouver dans différents dossiers (sécurité, chroot) par exemple dans /etc/named.conf ou /etc/

On peut externaliser certaines points de configuration de ce fichier central dans des fichiers;
/etc/bind/named.conf.local
/etc/bind/named.conf.options

/etc/init.d/bind

Ils 'agit d'un init script qui permet de redémarrer bind :

```
/etc/init.d/bind9 restart
```

/var/named/

Il s'agit d'un répertoire de travail.

Syntaxe des fichiers de configuration

(named.conf, named.conf.local, named.conf.options, etc.)

- Toujours un point virgule pour finir une instruction.
- Instruction entre accolades :

On donne une “intruction” (statements)

```
mot-clé {
            ...
};
```

- Instruction simples entre guillemets doubles :

Par exemple dans /etc/bind/named.conf :

```
include "/etc/bind/name.conf.options";
include "/etc/bind/name.conf.local";
include "/etc/bind/name.conf.default-zones";
include "/etc/bind/name.conf.example-zones";
```

Options de configuration du DNS

Souvent dans le fichier “named.conf.options.

Dans l'instruction “option” du fichier named.conf.options, on peut donner les instructions suivantes:

Options	**significations**	**exemples**
directory	répertoire de travail	directory ”/var/named”;

forwarders	serveurs de référence (aucun par défaut)	forwarders {
		adresses.IP.de.serveurs.de.référence;
		}
		(sinon il interroge récursivement les autres serveurs DNS)

forward	comportement avec les forwarders (first : en prorité only : uniquement)	forward only ;
version	version du serveur à afficher quand le serveur est interrogé	version none ;

L'instruction zones

Permet de définir les paramètres généraux d'une zone.

```
zone "nom-de-notre-zone" {
    type master;
    file "/etc/bind/db.xxx";
}
```

- Nom de la zone dans l'entête ;
- type (**master** pour primaire ou **slave** pour secondaire ou **int** pour Le programme qui lance le server : /usr/sbin/nracine) ;
- fichier chemin du fichier de configuration de zone
- éventuellement des options

Pré-requis à la l'installation d'un DNS Maître du réseau local

Il va s'agir de configurer un serveur DNS qui servira de serveur cache pour le système sur lequel Bind va être installé, et qui sera de serveur DNS maître pour les systèmes clients du réseau local.

- Soit un server sous Debian Wheezy nommé : “debian-serveur”
- Adresse IP pour “eth0 ” du serveur “debian-serveur” : 192.168.0.14
- Soit un nom de domaine : “mondomaine.hyp”
- Soit un ordi client sur le réseau local : “debian-client” avec l'IP 192.168.0.22
- Soit un autre ordi sur le réseau local : “debian-hp” avec l'IP 192.168.0.23

Les IP des ordinateurs clients et du système sur lequel il va être installé Bind sont fixées par le serveur DHCP par exemple celui du modem fourni par son FAI[2)], ou encore par un serveur DHCP installé entre le routeur et les clients du réseau local.

Connaître le nom du système sur lequel on installera Bind

```
hostname
```

```
debian-serveur
```

- Si on veut le changer pour lui donner un nom plus significatif de sa fonction de server :

```
vim /etc/hostname
```

- Puis ré-initialiser :

```
/etc/init.d/hostname.sh start
```

Compléter /etc/host.conf

Il s'agit là de la partie cliente du système sur lequel va être installé Bind. Un même système peut être à la fois client et serveur, c'est-à-dire, serveur DNS “pour lui-même”.

```
vim /etc/host.conf
```

```
order hosts, bind
multi on
```

Compléter /etc/hosts

Il s'agit là encore de l'aspect client du système. On renseigne tous les clients du réseau local.
On renseigne aussi le nom de domaine de ce système en tant que client.

```
vim /etc/hosts
```

```
127.0.0.1       localhost.mondomaine.hyp      localhost
192.168.0.14    debian-serveur.mondomaine.hyp debian-serveur
192.168.0.22    debian-client1
192.168.0.23    debian-hp



# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Déclarer un nom de domaine dans /etc/resolv.conf

If faut déclarer un nom de domaine dans /etc/resolv.conf.
Et retirer les DNS extérieurs, afin que Bind soit consulté.

Sur le système voué à servir de serveur DNS, s'il a été installé un environnement de bureau, lors du redémarrage du système, la nouvelle configuration du fichier **/etc/resolv.conf** sera effacée par Network Manager.

Deux solutions pour résoudre ce problème : soit on configure Network Manager, soit on se crée un script.

- **Configurer Network Manager**.

En faisant :
→ Système → Préférences → Connexions réseau
Puis il faut modifier toutes les connexions que vous avez dans tous les onglets (Filaire, Sans fil, etc…), en faisant, pour chacune d'entre-elles :

1. Cliquez sur la connexion à modifier ;
2. Bouton "Modifier" ;
3. Onglet "Paramètres IPv4" (et aussi IPv6 si vous l'utilisez) ;
4. Méthode : Adresses automatiques uniquement (DHCP) ;
5. Serveurs DNS : 127.0.0.1

Puis appliquez les modifications. Si la connexion est partagée entre tous les utilisateurs, un mot de passe administrateur vous sera demandé.

> On peut alors éditer le fichier **/etc/resolv.conf** afin qu'il ressemble à ceci :

```
domain mondomaine.hyp
search mondomaine.hyp
nameserver 127.0.0.1
```

- **Script de démarrage pour effacer les modifications de Network Manager**.

On va modifier le fichier avec le script, en même temps que résoudre le problème "Network Manager", donc inutile d'éditer /etc/resolv.conf après l'exécution du script.

- Création du script pour networkmanager :

```
cd /etc/NetworkManager/
```

```
vim /etc/NetworkManager/dispatcher.d/99-dns
```

```
#!/bin/sh
echo "domain mondomaine.hyp" > /etc/resolv.conf
echo "search mondomaine.hyp" >> /etc/resolv.conf
echo "nameserver 192.168.0.14" >> /etc/resolv.conf
echo "#nameserver 212.27.40.240" >> /etc/resolv.conf
echo "#nameserver 212.27.40.241" >> /etc/resolv.conf
```

Et c'est tout, Bind sera le server DNS du système sur lequel il est installé.
On peut simplement commenter les anciens paramètres du fichier afin d'avoir sous la main les DNS de son FAI.

```
chmod 755 /etc/NetworkManager/dispatcher.d/99-dns
```

- Exécution du script :

```
bash /etc/NetworkManager/dispatcher.d/99-dns
```

```
less /etc/resolv.conf
```

```
domain mondomaine.hyp
search mondomaine.hyp
nameserver 192.168.0.14
#nameserver 212.27.40.240
#nameserver 212.27.40.241
```

- Redémarrer le réseau :

```
/etc/init.d/networking start
```

- Au sujet de Network Manager: https://wiki.debian.org/fr/NetworkConfiguration#Configuration_de_DNS_pour_network-manager
- Attention la suppression de networkmanager déstabilise le système :

```
apt-get remove --purge network-manager-gnome netwok-manager
```

Installer et configurer un serveur DNS

Dans le cas où vous partagez votre connexion internet (modem cable, adsl, ou même simple modem) il est très utile d'utiliser un serveur DNS cache. Par contre, pour que vos stations qui utilisent cette connexion partagée se servent de ce serveur cache DNS, n'oubliez surtout pas de configurer toutes les stations pour qu'elles utilisent comme serveur DNS votre serveur et pas un autre. Pour cela, donnez comme adresse de serveur DNS l'adresse interne (côté LAN donc) de votre serveur.

Installation du paquetage

```
apt-get update
```

```
apt-get install bind9
```

Configuration de bind pour un serveur DNS maître local

Quelques commandes utiles lors de la configuration de bind9 :

- Si la configuration est difficile on peut chercher les erreurs avec les commandes suivantes :

```
named-checkzone webadonf.lan /etc/bind/db.webadonf.lan
```

```
named-checkzone webadonf.lan /etc/bind/db.webadonf.lan.inv
```

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

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

- Voir aussi les logs :

```
tail -30 /var/log/syslog
```

- Le dossier **/etc/bind/** :

```
cd /etc/bind/ && ls
```

```
bind.keys  db.127  db.empty  db.root     named.conf.default-zones
named.conf.options  zones.rfc1918
db.0       db.255  db.local  named.conf  named.conf.local       rndc.key
```

- Créer le fichier "**/etc/bind/db.mondomaine.hyp**" :

Prendre le fichier /etc/bind/db.local pour modèle.

```
cp /etc/bind/db.local /etc/bind/db.mondomaine.hyp
```

Éditer "/etc/bind/db.mondomaine.hyp" :

```
vim /etc/bind/db.mondomaine.hyp
```

```
;
; BIND data file for eth0 interface
;
$TTL    604800
@       IN      SOA     debian-serveur.mondomaine.hyp. root.mondomaine.hyp.
(
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      debian-serveur.mondomaine.hyp.
debian-serveur  IN   A  192.168.0.14
```

- Créer le fichier de recherche inverse "**db.mondomaine.hyp.inv**" :

Prendre pour modèle /etc/bind/db.127

```
cp /etc/bind/db.127 /etc/bind/db.192
```

Éditer "/etc/bind/db.192" :

```
vim /etc/bind/db.192
```

```
;
; BIND reverse data file for eth0  interface
;
$TTL    604800
@       IN      SOA     debian-serveur.mondomaine.hyp. root.mondomaine.hyp.
(
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      debian-serveur.
14      IN      PTR     debian-serveur.mondomaine.hyp.
```

- Configurer le fichier "/etc/bind/named.conf.local" :

```
vim /etc/bind/named.conf.local
```

```
//
// Do any local configuration here
//
```

```
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "mondomaine.hyp" {
        type master;
        file "/etc/bind/db.mondomaine.hyp";
        allow-query { any; };
};
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
};
```

- Configurer “/etc/bind/named.conf.options” :

```
vim /etc/bind/named.conf.options
```

```
 options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

         forwarders {
                192.168.0.14;
                8.8.8.8;
                8.8.4.4;
                // 212.27.40.240;
                // 212.27.40.241;
         };

//========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See
https://www.isc.org/bind-keys
//========================================================================
        dnssec-validation auto;

        auth-nxdomain no;    # conform to RFC1035
        version none;
        forward only;
//      listen-on-v6 { any; };
};
```

On peut mettre les forwarders qu'on souhaite, par exemple ici ceux de google ou/et ceux de “boxmachin”, fournisseur adsl.

- Redémarrer bind9 :

```
service bind9 restart
```

ou

```
/etc/init.d/bind9 restart
```

```
[....] Stopping domain name service...: bind9rndc: connect failed:
127.0.0.1#953: connection refused
. ok
[ ok ] Starting domain name service...: bind9.
```

Configurer le serveur Bind au sujet des clients

Éditer le fichier /etc/bind/db.mondomaine.hyp

```
vim /etc/bind/db.mondomaine.hyp
```

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     debian-serveur.mondomaine.hyp. root.mondomaine.hyp.
(
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      debian-serveur.mondomaine.hyp.
debian-serveur  IN   A  192.168.0.14
debian-client1  IN   A  192.168.0.22
```

Éditer le fichier /etc/bind/db.192

```
vim /etc/bind/db.192
```

```
;
; BIND reverse data file for eth0  interface
;
$TTL    604800
@       IN      SOA     debian-serveur.mondomaine.hyp. root.mondomaine.hyp.
```

```
(
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      debian-serveur.
14      IN      PTR     debian-serveur.mondomaine.hyp.
22      IN      PTR     debian-client1.
```

On recharge bind :

```
/etc/init.d/bind9 restart
```

Configurer les clients du réseau

Sur chacun d'eux, il faut configurer les fichiers ci-dessous.

Éditer le fichier /etc/host.conf

Afin que le serveur bind du réseau local soit interrogé par le client.

```
vim /etc/host.conf
```

```
order hosts,bind
multi on
nospoof on
```

> **order** : indique l'ordre des requêtes : ici, d'abord le fichier hosts, puis, en cas d'échec, le serveur de noms qui sera le serveur Bind quand le fichier /etc/resolv.conf aura été modifier pour ce faire.
> **multi** mis à **on** : plusieurs adresses IP peuvent être associées à un même nom.
> **nospoof** : oblige, par sécurité, à vérifier la concordance entre adresse IP et nom lors de la résolution d'adresses inverse.

>Le client va lire le fichier **hosts.conf** et rechercher l'adresse correspondant au nom demandé d'abord dans le fichier hosts local ; si la requête échoue, il va s'adresser à Bind, le serveur DNS du réseau local, qui va lui-même demander à des forwarders s'il ne sait pas répondre. Pour qu'il trouve l'adresse de ce serveur DNS, il consulte le fichier **/etc/resolv.conf** qu'il est donc nécessaire de modifier.

Editer le fichier /etc/resolv.conf

Deux solutions :

- Solution 1 : Installer un script client pour **/etc/resolv.conf**

Ce qui permet là aussi de ne plus être embêté par networkmanager, mais cette fois il va permettre de renseigner le système client DNS par l'adresse IP du serveur local bind.

```
cd /etc/NetworkManager/
```

```
vim /etc/NetworkManager/dispatcher.d/99-dns
```

```
#!/bin/sh
echo "domain mondomaine.hyp" > /etc/resolv.conf
echo "search mondomaine.hyp" >> /etc/resolv.conf
echo "nameserver 192.168.0.14" >> /etc/resolv.conf
```

- Ondonne les droits d'exécution :

```
chmod 755 /etc/NetworkManager/dispatcher.d/99-dns
```

- On exécute le script:

```
bash /etc/NetworkManager/dispatcher.d/99-dns
```

```
less /etc/resolv.conf
```

```
domain mondomaine.hyp
search mondomaine.hyp
nameserver 192.168.0.14
```

On fait cela sur tous les systèmes clients du réseau local.

- Solution 2 : **Configurer Network Manager**

En faisant :
→ Système → Préférences → Connexions réseau
Puis il faut modifier toutes les connexions que vous avez dans tous les onglets (Filaire, Sans fil, etc...), en faisant, pour chacune d'entre-elles :

1. Cliquez sur la connexion à modifier ;
2. Bouton "Modifier" ;
3. Onglet "Paramètres IPv4" (et aussi IPv6 si vous l'utilisez) ;
4. Méthode : Adresses automatiques uniquement (DHCP) ;
5. Serveurs DNS : *IP du serveur DNS local* [3)]

Puis appliquez les modifications.

> On peut alors éditer le fichier **/etc/resolv.conf** afin qu'il ressemble à ceci :

```
domain mondomaine.hyp
search mondomaine.hyp
nameserver 192.168.0.14
```

- Puis recharger la configuration réseau :

```
/etc/init.d/networking start
```

Vérifier les relations DNS/clients

Vérifier que le serveur DNS se connaisse lui-même

Pour avoir le nom complet sur système avec Bind :

```
hostname
```

```
debian-serveur
```

Avec nslookup

- Demander l'adresse associée à un nom d'hôte :

```
nslookup
```

```
> debian-serveur
Server:     127.0.0.1
Address:    127.0.0.1#53

Name:   debian-serveur.mondomaine.hyp
Address: 192.168.0.14
>debian-serveur.mondomaine.hyp
Server:     127.0.0.1
Address:    127.0.0.1#53

Name:   debian-serveur.mondomaine.hyp
Address: 192.168.0.14
> exit
```

- Idem pour la zone inverse, vérifier qu'IP correspond à un hôte:

```
nslookup
```

```
> 192.168.0.14
Server:     127.0.0.1
Address:    127.0.0.1#53

14.0.168.192.in-addr.arpa   name = debian-serveur.mondomaine.hyp.
> exit
```

Il répond aux deux, donc tout va bien !

- Avec dig :

```
dig debian-serveur
```

```
dig mondomaine.hyp
```

```
dig -x @192.168.0.14
```

Vérifier que le serveur DNS connaisse les clients

```
nslookup
```

```
> debian-client1
Server:     127.0.0.1
Address:    127.0.0.1#53

Name:   debian-client1.mondomaine.hyp
Address: 192.168.0.22
> 192.168.0.23
Server:     127.0.0.1
Address:    127.0.0.1#53

23.0.168.192.in-addr.arpa   name = debian-hp.0.168.192.in-addr.arpa.
> exit
```

> Il connaît bien les deux clients, soit à partir d'un nom d'hôte, soit à partir d'une adresse IP.

Vérifier que les clients interrogent le DNS local

Avec la commande host

```
host -a debian-serveur
```

```
Trying "debian-serveur.mondomaine.hyp"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10787
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;debian-serveur.mondomaine.hyp. IN    ANY

;; ANSWER SECTION:
debian-serveur.mondomaine.hyp. 604800 IN A  192.168.0.14

;; AUTHORITY SECTION:
mondomaine.hyp.     604800    IN    NS    debian-serveur.mondomaine.hyp.

Received 77 bytes from 192.168.0.14#53 in 0 ms
```

Avec la commande dig

```
dig mondomaine.hyp
```

```
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> mondomaine.hyp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12579
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;mondomaine.hyp.            IN    A

;; AUTHORITY SECTION:
mondomaine.hyp.     604800    IN    SOA    debian-serveur.mondomaine.hyp.
root.mondomaine.hyp. 2 604800 86400 2419200 604800

;; Query time: 0 msec
;; SERVER: 192.168.0.14#53(192.168.0.14)
;; WHEN: Sun Sep 14 09:00:08 2014
;; MSG SIZE  rcvd: 88
```

- Avec la réserve :

```
dig -x 192.168.0.14
```

```
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> -x 192.168.0.14
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47078
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

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

;; ANSWER SECTION:
14.0.168.192.in-addr.arpa. 604800 IN    PTR    debian-
serveur.mondomaine.hyp.

;; AUTHORITY SECTION:
0.168.192.in-addr.arpa. 604800    IN    NS    debian-serveur.

;; Query time: 0 msec
;; SERVER: 192.168.0.14#53(192.168.0.14)
;; WHEN: Sun Sep 14 09:03:29 2014
;; MSG SIZE  rcvd: 114
```

Et voilà 😎

Générer une clé d'authentification avec l'utilitaire rndc

Cet utilitaire permet d'administrer notre serveur. Après l'installation de Bind, la première chose à faire est de configurer rndc, ce qui consiste à configurer une clé d'authentification relative à la configuration de son réseau local.

BIND contient un utilitaire appelé rndc qui permet d'utiliser des lignes de commande pour administrer le démon named à partir de l'hôte local ou d'un hôte distant.

Afin d'empêcher l'accès non-autorisé au démon named, BIND utilise une méthode d'authentification à clé secrète partagée pour accorder des privilèges aux hôtes. Ainsi, une clé identique doit être présente aussi bien dans /etc/named.conf que dans le fichier de configuration de rndc, à savoir /etc/rndc.conf.

Remarques sur la configuration de rndc.

Pour utiliser rmdc à distance mettre sur la machine qui génère rndc les info données en sortie par la commande rndc-confgen à mettre dans **rndc.conf** et sur le serveur distant les infos à mettre dans **named.conf**.

- Dans /etc/bind/ on voit le fichier rndc.key :

```
ls /etc/bind/
```

```
bind.keys  db.empty    named.conf.default-zones  zones.rfc1918
db.0       db.local    named.conf.local
db.127     db.root     named.conf.options
db.255     named.conf  rndc.key
```

rndc.key ne s'édite pas !

- Générer une clé :

```
rndc-confgen >/etc/bind/rndc.key
```

- Indiquer le fichier rndc.key à la fin de /etc/bind/named.conf :

```
echo 'include "/etc/bind/rndc.key";' >> /etc/bind/named.conf
```

- Éditer /etc/bind/rndc.key pour commenter toute la fin à partir de `options {` :

```
vim /etc/bind/rndc.key
```

```
# Start of rndc.conf
key "rndc-key" {
        algorithm hmac-md5;
        secret "xxxxxxxxxxxxxxxx";
```

```
};

#options {
#       default-key "rndc-key";
#       default-server 127.0.0.1;
#       default-port 953;
#};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list as needed:
# key "rndc-key" {
#       algorithm hmac-md5;
#       secret "xxxxxxxxxxxxxx";
# };
#
# controls {
#       inet 127.0.0.1 port 953
#               allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf
```

Configurer les zones qui utilise la clé

- Éditer /etc/bind/named/conf.local :

```
vim /etc/bind/named.conf.local
```

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "mondomaine.hyp" {
        type master;
        file "/etc/bind/db.mondomaine.hyp";
        allow-update {key rndc-key;};
};
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
        allow-update {key rndc-key;};
};
```

Relancer bind9

```
/etc/init.d/bind9 restart
```

```
[....] Stopping domain name service...: bind9waiting for pid 5441 to die
. ok
[ ok ] Starting domain name service...: bind9.
```

Références

Sur la commande dig : http://www.system-linux.eu/index.php?post/2009/04/23/La-commande-dig

Pour la configuration des clients Windows http://valaurea.free.fr/documents/sig11_bind9_1.html

Pour installer et configurer Bind sur une distribution linux à base de RPM
http://lea-linux.org/documentations/Reseau-name-dns1

1)

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !

2)

Se rendre sur le site de son FAI, et associer l'adresse mac du serveur à l'IP dans les BAUX/DHCP.

3)

Par exemple ici 192.168.0.14