DNS : Bind9

- Objet : installer un server DNS en local bind9
- Niveau requis :
  débutant, avisé
- Commentaires : *Contexte d'utilisation du sujet du tuto.*

Introduction au DNS

Quelques bases au 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/resolve.conf** dans lequel est indiqué l'adresse IP de serveur local Bind comme server de référence.

Cet ordi a donc l'adresse IP d'un DNS, et 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 d'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 server.

/usr/sbin/rndc

rndc est un utilitaire de contrôle.

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

→ commandes :

`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”;

Options	significations	exemples

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

Configurer un server DNS Maître en local sous wheezy

Il s'agit d'un serveur qui ne fera autorité que sur le réseau local et non sur aucune autre zone.
Il va s'occuper d'aller chercher les infos sur des forwarders ou des serveurs racine ... et de les stoker dans son cache.

- 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

Pré-requis

IP statique

- Configurer une IP statique pour le serveur sur lequel on installe bind9.

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

Compléter /etc/hostname

```
vim /etc/hostname
```

```
debian-serveur.mondomaine.hyp
```

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

Compléter /etc/host.conf

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

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

Compléter /etc/hosts

```
vim /etc/hosts
```

```
127.0.0.1   localhost.localdomain localhost

192.168.0.14    serveur-debian.mondomaine.hyp serveur-debian
192.168.0.22    debian.mondomaine.hyp debian

192.168.0.1     gateway.mondomaine.hyp gateway


# 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

Il faut déclarer un nom de domaine dans /etc/resolv.conf.
Au passage on peut indiquer d'autres DNS extérieurs que ceux du FAI.
On va créer un script pour que la nouvelle configuration du fichier /etc/resolv.conf ne soit par effacer lors d'un redémarrage, par **NetworkManager**.

- Voir : 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 network-manager
```

On peut soit éditer le fichier **/etc/resolv.conf**, mais comme le script suivant est nécessaire pour ne pas être embêté par NetworkManager, on va modifier le fichier avec le script.

Création du script pour networkmanager

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

- Création d'un fichier de démarrage :

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

> **Adapter le contenu son nom de domaine et à son de choix de forwarder**

```
#!/bin/sh
echo "domain mondomaine.hyp" > /etc/resolv.conf
echo "search mondomaine.hyp" >> /etc/resolv.conf
echo "nameserver 127.0.0.1" >> /etc/resolv.conf
echo "nameserver 8.8.8.8" >> /etc/resolv.conf
echo "nameserver 8.8.4.4" >> /etc/resolv.conf
```

> On met après l'instruction `domain` le nom de son domaine : il n'est pas nécessaire pour une utilisation locale que ce soit un nom de domaine acheté ou loué auprès un registre de noms de domaine.
> Puis l'instruction `search` et son nom de domaine ;
> Puis l'intruction `nameserver` suivi de l'IP d'un serveur de nom qui soit interrogeable.
> Ici ce sont ceux de Google, mais il est peut-être préférable de laisser ceux de son FAI.
> On peut aussi ajouter en dessous de la ligne comportant l'instruction `search` :
> `echo nameserver ip-fixe-du-serveur-bind`.

- On donne les droits d'exécution

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

- On exécution le script :

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

- On peut vérifier :

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

```
domain mondomaine.hyp
search mondomaine.hyp
nameserver 127.0.0.1
nameserver 8.8.8.8
nameserver 8.8.4.4
```

- Redémarrer le réseau :

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

Installer et configurer bind

installation du paquetage

```
apt-get update
```

```
apt-get install bind9
```

Configuration de bind pour un serveur DNS maître en 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 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
```

- 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";
};
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 {
                192.168.0.1;
                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 "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.
```

Vérifier le DNS

Pour avoir le nom complet :

```
hostname
```

```
debian-serveur.mondomaine.hyp
```

- Avec nslookup :

```
nslookup
```

```
> 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 :

```
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
```

Interroger le DNS local sur un client du réseau

Configuration

```
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
```

Et pour la réserve inverse :

```
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
```

Vérification

```
nslookup
```

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

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

22.0.168.192.in-addr.arpa   name = debian-client1.
> exit
```

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
```

- Ajouter la nouvelle clé 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 `option {` :

```
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.
```

Côté client

Se débarrasser de networkmanager avant tout.

- Il n'y a qu'un fichier à éditer “/etc/resolv.conf”:

```
vim /etc/resolv.conf
```

```
domaine mondomaine.hyp
search mondomaine.hyp
nameserver 192.168.0.14
```

- Puis recharger la configuration réseau :

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