Installation d'un serveur DNS Bind 9 sur Debian

But de ce document

Ce document me sert de **mémo pour installer un serveur Bind 9 sur une Debian.** Ce document a été testé sur Debian Etch et Debian Sarge. Je le diffuse en espérant qu'il puisse servir à d'autres personnes.

Pré-requis

Avoir installé une Debian de Base :

- cf mon autre document sur ce sujet :

http://www.coagul.org/article.php3 ?id_article=158

Présentation rapide d'un système DNS

L'architecture de réseau TCP/IP sur lequel est basé Internet et la plupart des réseaux locaux actuels, utilisent des adresses IP numériques du type 192.168.0.1. Mais pour faciliter la lecture de ces adresses par l'homme, un système permet de transformer ces adresses en adresses plus lisibles comme www.coagul.org

Pour effectuer cette opération, il est nécessaire d'utiliser des serveurs DNS. Un serveur DNS fera donc la correspondance entre les adresses IP et les noms des domaines.

Un serveur DNS s'occupe en général d'un domaine limité et s'occupe de transmettre les questions à d'autres serveurs s'il ne connaît pas la réponse.

Principe de fonctionnement de la recherche de noms

Lorsque qu'une demande de résolution de nom est demandée, Linux commence par regarder le fichier « **/etc/hosts.conf** :

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

La première ligne de ce fichier indique qu'il faut commencer la recherche en regardant la table hosts locale et ensuite il faut interroger le serveur DNS.

La table hosts locale est enregistrée dans le fichier « **/etc/hosts** » elle contient une table de correspondance entre des adresses IP et des noms, elle ressemble à :

```
127.0.0.1       localhost.localdomain   localhost
192.168.0.6     debian1.mondomaine.com     debian1
```

La première ligne est obligatoire pour que le système fonctionne même quand le réseau est désactivé. L'adresse IP 127.0.0.1 est toujours associée au nom localhost.

Les lignes suivantes peuvent être ajoutées manuellement pour faire la correspondance entre des adresses IP et des noms. C'est ce qui est fait en l'absence de serveur DNS.

Si le résultat n'est pas trouvé dans la table hosts,le système recherche le serveur DNS indiqué dans le fichier « **/etc/resolv.conf** » :

```
search mondomaine.com
nameserver 192.168.0.1
.....
```

La première ligne indique quel domaine il faut ajouter au noms si celui-ci n'est pas indiqué lors d'une demande de résolution de nom. Exemple :

- ping monserveur.mondomaine.com -> Aucun domaine ne sera ajouté lors de la résolution du nom, car le domaine est fourni.
- ping monserveur -> Le domaine mondomaine.com, sera ajouté avant d'effectuer la demande de résolution du nom (La recherche du nom, portera donc sur monserveur.mondomaine.com)

La deuxième ligne indique le serveur DNS principal.

Et c'est donc le serveur DNS qui sera chargé de donner le résultat s'il connaît la réponse ou de transmettre la question à un autre serveur DNS.

Si le serveur principal n'est pas disponible, le serveur DNS indiqué sur la ligne suivante sera utilisé.

Pourquoi installer un serveur DNS

Pour au moins deux raisons :

- Éviter de tenir à jour la table hosts de chaque poste client d'un réseau.
- Avoir un cache DNS qui accélère la recherche des noms.
- Sur un réseau locale, un serveur DNS permet d'accélérer le trafic sur le réseau car de nombreux services ont besoins d'un serveur DNS bien configuré pour fonctionner correctement (WEB, POP, SMTP,..)

Installation de Bind 9

Sous Debian, il faut installer le paquet suivant :

```
# aptitude install bind9
```

Fichier de Configuration Principal (/etc/bind/named.conf)

Le fichier de Configuration principal « **/etc/bind/named.conf** » contient la liste des zones (ou domaines) que le serveur DNS doit prendre en charge.

Voici un exemple de description de zone :

```
zone "mondomaine.com" {
      type master;
      file "/etc/bind/db.mondomaine.com";
      forwarders{};
};
```

mondomaine.com : Nom du domaine à prendre en charge

type master : Cette ligne indique que le serveur est le serveur principal de ce domaine.

file "/etc/bind/db.mondomaine.com" ; :Cette ligne donne le chemin du fichier qui contiendra la correspondance entre les noms et les adresses IP pour ce domaine.

Fichier de configuration secondaire

Pour chaque domaine à gérer, il faut créer le fichier indiqué dans « **named.conf** ». Dans l'exemple précédent, il faudra créer le fichier « **/etc/bind/db.mondomaine.com** »

Voici le contenu de ce fichier :

```
$TTL    604800
@ IN SOA pgdebian.mondomaine.com. root.mondomaine.com.  (
      20041122   ; Serial  -> N° de série à incrémenter à chaque modif
                 ;          de ce fichier. Ce N° est utilisé par les
                 ;          serveurs esclaves pour lui indiquer qu'il
                 ;          doit mettre à jour sa base. Par commodité
                 ;          ce n° est une date à l'envers.
      604800     ;Refresh ->  A l'expiration du délai Refresh exprimé en
                 ;          secondes, le serveur excalve va entrer en
                 ;          communication avec le maitre et si il ne
                 ;          le trouve pas, il fera une nouvelle
                 ;          tentative au bout du délai Retry et si au
                 ;          bout du délai Expire il considerera que le
```

```
                ;       serveur n'est plus disponible.
        86400     ; Retry
        2419200   ; Expire
        604800 )  ; Minimum -> Durée de vie minimum du cache en secondes
;** Les  lignes suivantes permettent au serveur de se retrouver lui même
                NS      pgdebian.mondomaine.com.        ;Nom du serveur
pgdebian        A       192.168.0.3                     ;Adresse IP du
                                                        ;serveur de noms
pgdebian        HINFO   "PII 233 :-)" "Debian Testing"  ;Info
complèmentaire
;** Les lignes suivantes définissent la table entre les noms et les IP
pglinux         A       192.168.0.1
pg-cao          A       192.168.0.2
plgmao          A       192.168.0.9
cpi             A       192.168.0.10
prod            A       192.168.0.100
pgcie           A       10.2.2.1
;** Les lignes suivantes sont des alias entre des noms et des autres noms
pop             CNAME   pglinux
smtp            CNAME   pglinux
www             CNAME   pglinux
ldap            CNAME   pgdebian
```

La première partie est utilisée pour la gestion maître-esclave des serveurs DNS.

La deuxième partie permet au serveur DNS de se retrouver lui-même.

La troisième partie contient la table de correspondance entre les noms et les adresses IP.

La dernière partie donne les alias possibles pour un même nom de serveur.

Résolution inverse

De nombreux services réseaux utilisent la résolution inverse (Trouver l'adresse IP à partir du nom) pour vérifier que le nom est valide.

Il est donc nécessaire de configurer le serveur pour qu'il prenne également en charge la résolution inverse.

Le principe est quasiment le même que pour la résolution classique. il faut déjà définir le domaine inverse dans le fichier « **named.conf** » comme dans l'exemple suivant :

```
zone "0.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.mondomaine.com.inv";
        forwarders{};
};
```

L'adresse IP doit être indiquée à l'envers et il faut ajouter .in-addr.arpa.

Il faut également définir un nouveau fichier qui ressemblera à ceci :

```
$TTL    604800
@       IN      SOA     pgdebian.mondomaine.com.
root.mondomaine.com.  (
                20041122
                604800
                86400
                2419200
                604800 )
        NS      pgdebian.mondomaine.com.
1               PTR     pglinux.mondomaine.com.
2               PTR     pg-cao.mondomaine.com.
3               PTR     pgdebian.mondomaine.com.
9               PTR     plgmao.mondomaine.com.
```

La première partie est utilisée pour la gestion maître-esclave des serveurs DNS.

La deuxième partie donne le nom du serveur DNS (NS = Name Server).

La troisième partie contient la correspondance entre la fin de l'adresse IP et le nom du serveur.

Pour finir, il est conseillé (mais pas obligatoire) d'indiquer les adresses IP des serveurs DNS de son fournisseur d'accès à Internet. Pour cela, il faut décommenter et renseigner la section suivante du fichier « **/etc/bind/named.conf.options** » :

```
forwarders {
        194.2.0.50;
        194.2.0.20;
};
```

Démarrer le démon

Après chaque modification des fichiers de configuration, il faut redémarrer le démon :

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

ATTENTION : Il est vivement conseillé de regarder les logs pour vérifier que le démarrage du démon s'est correctement effectué :

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

Tester la résolution des noms

Il existe plusieurs outils pour tester le bon fonctionnement de la résolution des noms :

ping

La commande « **ping** » est la plus simple (mais la plus limité). Elle permet de tester la résolution du nom, mais pas la résolution inverse :

```
$ ping NomDuServeur
```

host

La commande « **host** », permet de tester la résolution du nom et la résolution inverse :

```
$ host NomDuServeur
```

ou :

```
$ host AdresseIPduServeur
```

nslookup

La commande « **nslookup** » du paquet « **dnsutils** », permet également de tester la résolution du nom et la résolution inverse :

```
$ nslookup NomDuServeur
```

ou :

```
$ nslookup AdresseIPduServeur
```