BIND 9 : DNS sous Linux

Contribueurs

(SISR2-2017) Sébastien Mornier, Aurélien Ardillon

Bind9 est le service responsable de la gestion DNS sous Linux.

Procédure

Le logiciel serveur pour DNS se nomme *bind9* sous *Debian/Ubuntu*.

Installation du service et création de la zone sur le principal

1. Installer le paquetage *bind9*
2. **Déclarer la zone** à gérer dans *named.conf.local* avec le type ***master***
3. Configurer le fichier de la zone en y ajoutant les **enregistrements** nécessaires (*NS*, *A*, *MX*, *AAAA*, ...)
4. Vérifier la validité de la configuration du service : ***named-checkconf***
5. Vérifier la validité de la configuration de la zone : ***named-checkzone***
6. Recharger le fichier de configuration ou redémarrer le service : ***service bind9 restart|reload***
7. Paramétrer un client pour qu'il utilise ce serveur, faire un *ping* sur un *FQDN*

Installation du secondaire

1. Installer le paquetage *bind9*
2. Déclarer la zone dans *named.conf.local* avec le type ***slave***
3. Vérifier la validité de la configuration du service : ***named-checkconf***
4. Recharger le fichier de configuration ou redémarrer le service : : ***service bind9 restart|reload***
5. Paramétrer un client pour qu'il utilise ce serveur secondaire, faire un *ping* sur un *FQDN*

Mode opératoire

1 Serveur Autorité

On parlera d'un ***maître***, d'un primaire ou d'un principal. Il est définit comme **Start Of Authority**

(*SOA*). Il n'y a qu'un serveur *SOA* pour un domaine DNS. Il est autorisé à apporter des modifications dans le **fichier de zone**. Il comporte l'ensemble des informations nécessaires à faire fonctionner BIND. À savoir :

- un fichier de configuration du service et de déclaration des zones (*/etc/bind/named.conf*)
- autant de **fichiers de zones** que nécessaires, accessibles dans */etc/bind/*.

Les fichiers de configuration et la description des zones

named.conf.options

Ce fichier de référence décrit les options courantes du serveur (attention, les valeurs sont des exemples) :

```
options {
    directory "/var/cache/bind";                #repertoire de stockage des fichiers de zone
    dump-file "/var/data/cache_dump.db";        #repertoire de cache
    statistics-file "/var/bind/named_stats.txt"; #repertoire de statistiques

        allow-recursion { any; };
        allow-recursion-on { any ; };
}
```

named.conf.local

On écrira dans ce fichier la déclaration des zones directes (sens FQDN→IP) et inverses (sens IP→FQDN). On portera une attention particulière aux points-virgules.

- pour chaque zone qu'il gère (exemple pour une zone nommée *rostand.fr*)

```
zone "rostand.fr" IN {
    type master;              #serveur maître
    file "/etc/bind/base.rostand.dns";  #nom du fichier qui décrit la zone
    allow-update { any; };    #possibilité de mise à jour en réseau vers les secondaires
};
```

- chaque zone de résolution inverse (exemple pour le réseau 192.168.0.0/24)

```
zone "0.168.192.in-addr.arpa" IN { #adresse IP du réseau à l'envers suivi de in-addr.arpa
    type master;
    file "rostand.inverse";
    allow-update { none; };
};
```

Les fichiers de zone et de zone inverse

On trouvera ensuite, conformément à ce qui a été indiqué dans *named.conf.local*, autant de fichiers que de zones ou de zones inverse.

Exemple pour un fichier de zone

```
#Fichier rostand.dns décrivant la zone rostand.fr
#SOA : start of authority + nom du serveur maître de la zone + nom de l'administrateur
@ IN SOA dns.rostand.fr. root.rostand.fr. (
    42  #; numéro de série important pour les secondaires (actualisé à chaque modification)
    3H  #; temps de rafraîchissement des secondaires (3 heures)
    15M #; temps d'attente entre deux tentatives de mise à jour pour les secondaires (15 min)
    1W  #; durée de vie d'une information (1 week)
    1D ) #; temps avant la déclaration d'invalidité permanente du principal (1 day)

IN NS dns.rostand.fr. # déclaration serveurs de noms principaux et secondaires

btsinfo NS srvinfo.rostand.fr. # délégation d'autorité pour la sous-zone btsinfo.rostand.fr
                  # le serveur aura pour nom srvinfo.rostand.fr

MX 10 smtp                    # pointeur pour le serveur de messagerie avec numéro d'ordre
MX 20 mail                    # deuxième pointeur, serveur secondaire

dns A 192.168.0.152           # association pour le nom de machine dns.rostand.fr
www A 192.168.0.152           # déclaration d'association pour le nom de machine www
srvinfo A 192.168.0.153       # association pour la machine srvinfo
smtp IN A 192.168.0.253       # association pour le nom smtp
mail IN A 192.168.0.154       # association pour pour le nom mail

console CNAME srvinfo         # alias pour le nom de machine srvinfo

www6 IN AAAA ::1              #; association pour une adresse IPv6
```

Exemple pour la résolution inverse :

```
#Fichier rostand.inverse décrivant la zone 0.168.192.in-addr.arpa
#SOA : start of authority + IP du maître et nom de zone + nom de
```

```
l'administrateur
@ IN SOA 0.168.192.in-addr.arpa. root. 0.168.192.in-addr.arpa. (
42 3H 15M 1W 1D )
IN NS rostand.fr   # déclaration serveurs de noms par nom DNS

152 IN PTR www     #association le numéro 253 vers le nom de machine www
153 PTR srvinfo    # association pour le numéro 153 vers la machine srvinfo
253 PTR smtp       # association pour le numéro 253 vers le nom smtp
```

Un fichier de zone comporte les éléments suivants :

Enregistrement	Rôle
SOA	Définit les indications du Start Of Authority : nom du domaine (ou de la zone) nom de la machine qui est SOA dans ce domaine nom de l'administrateur du domaine numéro de version de fichier délais pour la synchronisation
NS	Déclare les noms des machines qui sont serveur de noms (principal ou secondaires) pour la zone *Remarque* : Ces noms devront en plus être associés à une adresse par un enregistrement A.
A	Déclare les associations entre FQDN et adresse IP. On parle d'un hôte Remarques : un nom non terminé par un point est complété par la zone décrite dans le SOA un nom terminé par un point est un FQDN
MX	Déclare le nom de la ou des machines assurant la fonction de serveur de messagerie pour le domaine. Remarque : Ces noms devront en plus être associés à une adresse par un enregistrement A.
RT	Déclare le nom de la ou des machines assurant le rôle de routeur dans le domaine. Utilisé pour les systèmes avec auto-configuration. Remarque : Ces noms devront en plus être associés à une adresse par un enregistrement A.
PTR	Enregistrement inverse qui associe le nom FQDN à une adresse IP de machine dans le réseau IP déclaré dans le SOA. Utilisé pour les systèmes de cartographie de réseau ou pour l'administration distante

2 Serveur secondaire ou esclave

Un serveur ***secondaire*** est un serveur BIND qui a déclaré dans son fichier *named.conf.local* qu'il était ***esclave*** pour une zone déterminée (la terminologie Windows est ***secondaire***).

```
zone "rostand.fr" IN {
    type slave;             #serveur esclave
    masters {192.168.0.152 ;}     #adresse des serveurs maîtres
    file "double.rostand.dns";      #nom du fichier si on veut en conserver
une copie en local
    allow-update { none; };     #impossibilité de mise à jour en réseau vers
                        # d'autres secondaires
};
```

Dès lors, il recevra à intervalle régulier les mises à jour.

Attention : Il est important de changer le numéro de version à chaque modification du fichier principal de sorte que les secondaires se mettent correctement à jour.

3 Serveur de zone délégué

Un serveur de zone délégué est un serveur DNS qui a l'autorité sur un sous ensemble d'une zone principale. Par exemple, la zone *.gouv.fr.* a délégué la responsabilité de nombreuses sous-zones : *education.gouv.fr*, *impots.gouv.fr*, etc. Pour chaque sous-zone, une inscription a été faite dans le fichier de zone principale, et chaque délégation renvoie vers un nouveau serveur *SOA* pour la sous zone. Cet enregistrement au niveau supérieur est indispensable pour éviter tout ajout non désiré (on ne peut pas décider librement de créer une sous-zone, il faut qu'on nous ait donné une délégation).

Exemple, dans le fichier de la zone gouv.fr, on trouvera :

```
education IN NS nom_dns_du_serveur_délégué_education
impots IN NS nom_dns_du_serveur_délégué_impots
```

puis

```
nom_dns_du_serveur_délégué_education IN A adresse_ip_education
nom_dns_du_serveur_délégué_impots IN A adresse_ip_impots
```

Pour le serveur délégué, il s'agit ni plus ni moins qu'un maître pour la zone *education.gouv.fr* ou *impots.gouv.fr.*

4 Test des configurations

Avant de lancer un serveur suite à une modification, on peut prendre la précaution de tester les configurations des fichiers.

Commande	Rôle
named-checkconf	teste la validité des déclarations de zone (fichier *named.conf* et fichier de déclaration *named.conf.local*, *named.conf.default-zones*, etc).
named-checkzone	Teste la validité d'une zone à partir de son fichier de configuration *named-checkzone <nomZone> <cheminFichierZone>*

CLIENT ET TEST

Un client DNS est une machine qui dispose du service DNS client activé et qui a une adresse IP d’un serveur DNS indiqué dans son paramétrage réseau. On paramètrera les clients pour qu'ils aillent s'informer auprès de leur serveur DNS (qui peut être le secondaire ou le principal).

Sous Windows

Dans les propriétés de la carte, indiquer le serveur DNS principal ou préféré.

Sous Linux

Dans l'environnement graphique, utiliser « Adresses Automatiques uniquement » pour donner une valeur manuelle à la partie DNS (ici, copie d'écran sous ubuntu 10.10).

Test

On teste le bon fonctionnement du serveur DNS en tapant :

- *ping nomFQDN* : prouve que la résolution fonctionne
- *ping -a adresseIP* : si la résolution DNS inverse fonctionne, donne le nom FQDN de la machine possédant l'adresse interrogée
- *nslookup nomFQDN* : interroge le serveur DNS pour connaître l'adresse IP correspondant au nom FQDN
- *nslookup adresseIP* : interroge le serveur DNS pour savoir si un enregistrement inverse est associé à l'adresse IP et récupère alors le FQDN correspondant
- *nslookup -type=champ nomDomaine* : interroge le champs particulier (NS, MX, RT, etc) pour le domaine spécifié
- *dig @adresseServeur nomzone champ* (sous Linux) : permet d'interroger le contenu d'une zone en demandant les informations associées à un champ particulier (NS, MX, RT, etc)

Source

• http://www.zytrax.com/books/dns : site complet en anglais sur DNS et Bind9