TP Mise en oeuvre de bind sous Linux Debian

Objectifs

- installer un serveur DNS **bind9** sur une machine *Debian Stretch*
- mettre en évidence le fonctionnement du serveur DNS maître au moyen d'outils de test (*host*, *nslookup*) dans les situations suivantes :
  - ✓ nom courts/FQDN
  - ✓ résolution directe/inverse
  - ✓ depuis un client local/distant
  - ✓ test des différents types d'enregistrements (A, CNAME, PTR)
  - ✓ résolution hors zone d'autorité (redirection DNS)
- installer un serveur esclave
- mettre en évidence le transfert de zone du maître vers l'esclave
- autres pistes
  - ✓ délégation de zones
  - ✓ utilisation d'ACL (Access Control List)
  - ✓ scripting pour automatiser la gestion des fichiers de zone

Concepts

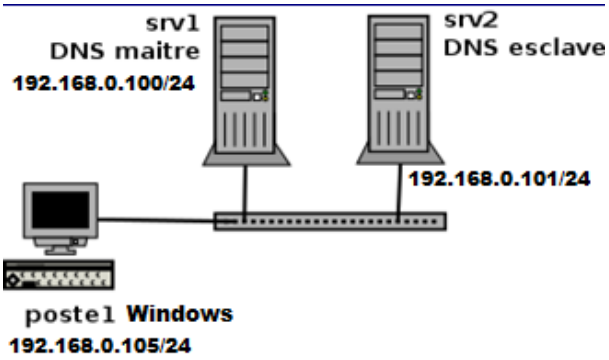
- domaine, sous-domaine
- zone d'autorité, zone directe/inverse
- enregistrements SOA, NS, A, CNAME, MX, PTR
- TTL
- résolution directe/inverse
- requête itérative/récursive
- serveurs maître/esclave/cache
- transfert de zone
- délégation de zone
- roots serveurs
- clients (résolvers)
- outils de test
- tolérance de panne
- sécurité

Prérequis

Remarque : adapter au réseau 192.168.0.0 la répartition du **dernier octet** entre les membres d'un même plot. Plages : 100-109, 110-119, 120-129 par ex. pour 3 utilisateurs (10 adresses chacun). Il faudra bien sûr « fixer » les adresses (fichier /etc/network/interfaces).

- le réseau est en **192.168.0.0/24**
- le domaine concerné s'appelle **domaine.lan**
- le serveur maître *Debian Stretch* **srv1** (192.168.0.**100**)
- le serveur esclave *Debian Stretch* **srv2** (192.168.0.**101**)
- le poste *Windows* **poste1** (192.168.0.**105**)

Schéma



Créer ce réseau avec la configuration des interfaces et le nommage des postes :

```
root@stretch64:~# sed -i 's/stretch64/srv1/g' /etc/host{s,name}
```

1. Installation du serveur maître

- **Paquetages à installer**

bind9, bind9-doc, dnsutils

Les fichiers de configuration sont situés dans */etc/bind*

- **le fichier /etc/bind/named.conf**

Il contient des *includes* vers les autres fichiers de configuration.

- **le fichier /etc/bind/named.conf.local**

Il doit comprendre les *déclarations de zone* : ici la *zone maitre directe* **domaine.lan** et la *zone inverse arpa* **0.168.192-in-addr.arpa**.

```
// zone directe
zone "domaine.lan" {
     type master;
     file "/etc/bind/db.domaine.lan";
};

// zone inverse
zone "0.168.192.in-addr.arpa" {
     type master;
     notify no;
     file "/etc/bind/db.domaine.lan.rev";
};
```

- **le fichier de zone directe db.domaine.lan**

On pourra se servir du fichier *db.local* comme base de travail en le copiant. Il devra comporter au minimum un enregistrement SOA, un NS et un A correspondant au NS.

On créera également d'autres enregistrements A et des alias (CNAME).

- **le fichier de zone inverse db.domaine.lan.rev**

On pourra se servir du fichier *db.local* comme base. Il devra comporter au minimum :

- ✓ un enregistrement **SOA** (Start Of Authority),
- ✓ un **NS** (Name Server)
- ✓ et un **PTR** correspondant au **NS**.

On créera également d'autres enregistrements PTR.

Remarques générales à propos des tests :

- ✓ Il est très intéressant d'ouvrir une console (avec Alt-Fx) qui servira à observer les logs de *bind9* au moyen de la commande suivante : `tail -f /var/log/syslog`
- ✓ Il faudra également prendre garde aux points terminaux **obligatoires** dans les FQDN.
- ✓ le fichier **/etc/resolv.conf** contient les éléments suivants **:**

```
search domaine.lan
nameserver 127.0.0.1
```

- **Tests locaux**
  - ✓ préparer la console d'observation des logs (voir plus haut)
  - ✓ relancer le démon bind9 : `service bind9 restart`
  - ✓ vérifier le fonctionnement effectif de ce dernier en examinant les logs
  - ✓ tester

```
host srv1.domaine.lan    : résultat ?

host poste1.domaine.lan  : résultat ?

host srv1     : resultat ?

host poste1   : résultat ?

host 192.168.0.100   : resultat ?

host 192.168.0.105   : resultat ?

host -l domaine.lan

host google.com : resultat ?
```

- **Tests hors zone d'autorité**

Il est nécessaire de spécifier un ou plusieurs serveurs (**forwarder**) pour la redirection (on pourra utiliser ceux du lycée). Et mettre à *no dnssec-validation (pour une éventuelle certification).*

Le paramètre à changer est le suivant dans le fichier **/etc/bind/named.conf.options** (à adapter aux conditions locales) :

```
forwarders {
            1.2.3.4;
            5.6.7.8;
       };
```

Une fois effectué le changement, relancer le démon *bind9* puis tester à nouveau la résolution.

```
host google.com     : résultat ?
```

- **Tests depuis un client Windows**

Après avoir vérifié la configuration du client Windows (serveur DNS, nom de domaine DNS), tester la résolution de noms dans les mêmes conditions.

2. Installation du serveur esclave

- **Paquetages à installer sur srv2 (192.168.0.101)**

bind9, *bind9-doc*, *dnsutils*

- **Sur srv1**
  - ✓ Dans les fichiers de zone directe et inverse, ajouter un enregistrement **NS** correspondant au 2ème serveur DNS (**srv2**) ainsi que l'enregistrement **A** correspondant pour **db.domaine.lan** et PTR pour **db.domaine.lan.rev**
  - ✓ Relancer *bind9* pour vérifier la syntaxe des mises à jour.

- **Sur srv2**
  - ✓ L'esclave srv2 doit disposer d'un fichier **/etc/bind/named.conf.local** dans lequel on définit les zones (directe et inverse) esclaves et l'adresse du serveur maître pour récupérer les fichiers de zone. Le plus simple est de récupérer celui du serveur maître et de le transférer sur l'esclave avec la commande *scp*. On peut alors le modifier pour obtenir :

```
// zone directe
zone "domaine.lan" {
     type slave;
     file "/etc/bind/db.domaine.lan";
     masters { 192.168.0.100; };

};

// zone inverse
zone "0.168.192.in-addr.arpa" {
     type slave;
     notify no;
     file "/etc/bind/db.domaine.lan.rev";
     masters { 192.168.0.100; };

};
```

Remarque

Depuis la version 9.9 de bind, les fichiers de zone sont transférés vers les esclaves au format binaire de façon à améliorer les performances.
En conséquence, il n'est plus possible d'afficher ou d'éditer les fichiers de zone de l'esclave.
Pour revenir au comportement initial (fichiers de zone au format *texte*), on pourra ajouter la clause `masterfile-format text` dans le fichier **named.conf.local**

```
zone "domaine.lan" {
    type slave;
    file "/etc/bind/db.domaine.lan";
    masters { 192.168.0.100; };
    masterfile-format text;
};
```

- **Mise en évidence du transfert de zone sur srv2**

Depuis l'esclave srv2 :

- ✓ vérifier que le fichier **/etc/resolv.conf** contient les éléments suivants :

```
search domaine.lan
nameserver 127.0.0.1   # on résout localement
```

- ✓ relancer le démon *bind*
- ✓ vérifier dans les logs le transfert effectif des fichiers de zone ainsi que la présence des fichiers db.domaine.lan et db.domaine.lan.rev dans le répertoire */etc/bind*
- ✓ en cas de problème de transfert, vérifier les droits en écriture du démon *bind* dans le répertoire */etc/bind*. Au besoin, les adapter avec la commande *chmod*. Dans ce cas, relancer le démon *bind9* puis vérifier la présence des fichiers *db* : le transfert doit être pris en charge par les serveurs DNS hors de toute intervention humaine.
- ✓ tester la résolution de noms dans les mêmes conditions que précédemment.

- **Mise en évidence du fonctionnement du client Windows**
  - ✓ modifier le paramétrage du client pour lui indiquer l'existence de deux serveurs DNS
  - ✓ couper le serveur maître
  - ✓ tester la résolution depuis le client Windows (locale et hors zone)
  - ✓ conclure