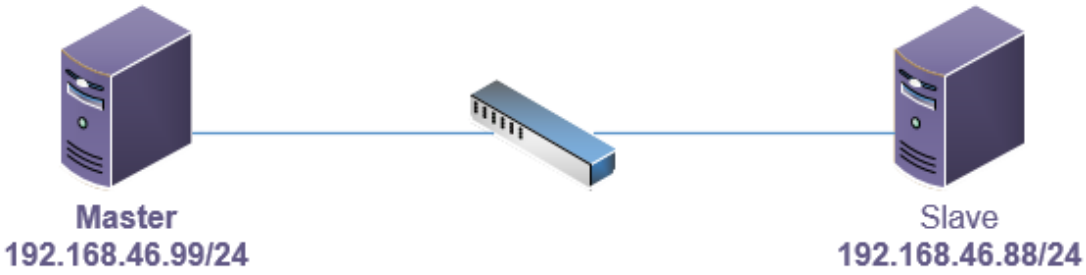
DNS Master-Slave

Serveur Linux CentOS

Table des matières

1 Introduction

Pour équilibrer les charges des DNS locaux, on peut mettre en place plusieurs DNS pour notre domaine local. Dans ce cas on met en premier un DNS primaire qui servira de "**maître**" pour le DNS secondaire.



2 Configuration du DNS primaire (master)

Sur le **DNS maître** il faut autoriser le transfert de zone en spécifiant l'adresse IP du maitre dans le paramètre *allow-transfer* :

```
options {
  listen-on port 53 { any; };
  listen-on-v6 port 53 { ::1; };
  directory  "/var/named";
  dump-file  "/var/named/data/cache_dump.db";
  statistics-file "/var/named/data/named_stats.txt";
  memstatistics-file "/var/named/data/named_mem_stats.txt";
  recursing-file  "/var/named/data/named.recursing";
  secroots-file   "/var/named/data/named.secroots";
  allow-query     { any; };
  forwarders {10.1.0.75;8.8.8.8; };
  allow-transfer {192.168.46.88; };
  recursion yes;
  dnssec-enable yes;
  dnssec-validation yes;
  bindkeys-file "/etc/named.iscdlv.key";
  managed-keys-directory "/var/named/dynamic";
  pid-file "/run/named/named.pid";
  session-keyfile "/run/named/session.key";
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
zone "." IN {
  type hint;
  file "named.ca";
};

zone "orabec.com" IN {
       type master;
       file "forward.orabec";
};

zone "46.168.192.in-addr.arpa" IN {
      type master;
      file "reverse.orabec";
};
```

On peut ajouter l'option suivante pour désactiver l'envoi de messages aux serveurs esclaves pour leur indiquer des modifications de zone :

```
notify no;
```

Fichier /var/named/forward.orabec :

```
$TTL 1D
@ IN        SOA   serveurdns hb.orabec.com. ( 0 1D 1H 1W 3H )
            NS    serveurdns
@           A     192.168.46.30
serveurdns  A     192.168.46.99
ftp         A     192.168.46.10
mail        CNAME ftp.orabec.com.
www         A     192.168.46.30
```

3 Configuration du DNS secondaire (slave)

Sur le **DNS esclave**, il faut préciser l'adresse IP du serveur "**maître**" dans le fichier **/etc/named.conf.**

On peut préciser plusieurs serveurs maîtres, séparés par un point-virgule (";").

```
options {
  listen-on port 53 { any; };
  listen-on-v6 port 53 { ::1; };
  directory  "/var/named";
  dump-file  "/var/named/data/cache_dump.db";
  statistics-file "/var/named/data/named_stats.txt";
  memstatistics-file "/var/named/data/named_mem_stats.txt";
  recursing-file  "/var/named/data/named.recursing";
  secroots-file   "/var/named/data/named.secroots";
  allow-query     { any; };
  recursion yes;
  dnssec-enable yes;
  dnssec-validation yes;
  bindkeys-file "/etc/named.iscdlv.key";
  managed-keys-directory "/var/named/dynamic";
  pid-file "/run/named/named.pid";
  session-keyfile "/run/named/session.key";
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
zone "." IN {
  type hint;
  file "named.ca";
};

zone "orabec.com" IN {
         type slave;
         file "slaves/orabec.sec";
         masters {192.168.46.99;};
};
```

La mise à jour du DNS "**esclave**" est automatique à partir du DNS "**maître**". Ainsi, insérer une nouvelle machine dans le DNS "**maître**" prend peu de temps, et tous les serveurs secondaires seront mis à jour automatiquement !

Si l'option **notify** est initialisé à **yes** alors à chaque changement de numéro de série du serveur maître, un message est envoyé aux serveurs esclaves pour leur indiquer qu'il faut mettre à jour leur configuration.

Les options figurant au début du fichier de zone (**serial**, **refresh**...) servent pour le DNS secondaire. Détaillons ces options :

serial

C'est le numéro (un nombre entier) de version du fichier d'information de zones. Ce numéro est utilisé par les DNS secondaires pour savoir si le fichier d'informations de zone du DNS primaire a été changé. Il doit être augmenté de 1 à chaque modification du fichier.

refresh

Intervalle de temps en secondes durant lequel le DNS secondaire attend avant de vérifier (et éventuellement mettre à jour) l'enregistrement **SOA** du DNS primaire. Ces enregistrements ne changent pas souvent en général, une journée (**86400** secondes) peut largement suffire.

retry

Intervalle de temps en secondes durant lequel le DNS secondaire attend avant de réessayer une requête vers le DNS primaire si celui ci n'est pas accessible. Cette valeur devrait être de quelques minutes.

expire

Intervalle de temps en secondes durant lequel le DNS secondaire attend avant de rejeter les informations de zones s'il n'a pu contacter le DNS primaire. Cette valeur devrait être de plusieurs jours (voir plusieurs mois).