

## Maitre/Esclave

Installation :

Pour commencer il nous faut un server DNS fonctionnelle.

Dans ce cas-là nous allons prendre une machine virtuelle avec un nom de domaine trash.hyp.

Nous nous rendons sur le Serveur DNS Maitre.

Configuration du serveur maitre trash.hyp pour autoriser le transfert de zone vers le server esclave.

Il faut se rendre dans /etc/bind/named.conf.local ce qui nous amène dans le fichier de configuration des zones.

```
GNU nano 3.2                                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 "trash.hyp" {
    Type master;
    file "/etc/bind/db.trash.hyp";
    notify yes;
    allow-transfer { 192.168.56.249; };
};

zone "56.168.192.in-addr.arpa" {
    Type master;
    file "/etc/bind/rev.trash.hyp";
    notify yes;
    allow-transfer { 192.168.56.249; };
};
```

Pour commencer le type master c'est notre serveur DNS maitre, file sont les fichiers d'enregistrement, notify yes s'applique uniquement aux zones esclaves et il est défini par une IP ou une liste de correspondance par exemple mon serveur DNS Esclave et le seul à notifier ce serveur et à le mettre à jour implicitement la zone en plus des hôtes définis dans l'option masters pour la zone.

Donc dans allow-transfer il faut ajouter le serveur DNS Esclave.

A ne pas oublier de le renseigner dans le fichier d'enregistrement DNS le nom du serveur DNS, dans mon cas il s'appelle ns2.trash.hyp avec son IP 192.168.56.249. NS = name serveur

N'oublier pas de le renseigner aussi dans le fichier rev (revers) pour des requêtes inverser.

```
;  
; BIND data file for trash.hyp loopback interface  
;  
$TTL      604800  
@         IN      SOA     ns1.trash.hyp. root.trash.hyp. (  
                2          ; Serial  
                604800     ; Refresh  
                86400      ; Retry  
                2419200    ; Expire  
                604800 )   ; Negative Cache TTL  
;  
@         IN      NS     ns1.trash.hyp.  
@         IN      NS     ns2.trash.hyp.  
pfSense  IN      A      192.168.56.254  
ns1       IN      A      192.168.56.250  
ns2       IN      A      192.168.56.249  
lap       IN      A      192.168.56.251  
glpi      IN      CNAME   lap  
nextcloud IN      CNAME   lap  
logalyzer IN      CNAME   lap
```

Faite un redémarrage du service bind9.

Configuration du Serveur Esclave pour qu'il puisse récupérer les zones du serveur maître.

Se rendre dans le fichier /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 "trash.hyp" {  
    Type slave;  
    file "/var/cache/bind/db.trash.hyp";  
    masters { 192.168.56.250; };  
};  
  
zone "56.168.192.in-addr.arpa" {  
    Type slave;  
    file "/var/cache/bind/rev.trash.hyp";  
    masters { 192.168.56.250; };  
};
```

Comme type de serveur DNS on lui indique qu'il sera slave (esclave), file c'est l'endroit où les fichiers de configuration pourra être copier c'est l'endroit destiné pour accueillir les fichiers de zone pour configurer un serveur DNS primaire ou secondaire, il indique à quelle emplacement le serveur maitre pourra copier c'est fichier.

Redémarrer le service bind9.

Si vous avez bien configuré votre serveur DNS mais qu'il vous indique une erreur, redémarrer votre serveur DNS et faire un status de votre service bind9.

```
root@DNSs:/etc/bind# nano named.conf.local
root@DNSs:/etc/bind# systemctl restart bind9
root@DNSs:/etc/bind# nano named.conf.local
root@DNSs:/etc/bind# systemctl status bind9
* bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2020-12-02 21:10:36 CET; 10s ago
     Docs: man:named(8)
  Process: 547 ExecStart=/usr/sbin/named $OPTIONS (code=exited, status=0/SUCCESS)
 Main PID: 548 (named)
    Tasks: 4 (limit: 1150)
   Memory: 11.8M
   CGroup: /system.slice/bind9.service
           └─548 /usr/sbin/named -u bind

Dec 02 21:10:36 DNSs named[548]: running
Dec 02 21:10:36 DNSs named[548]: managed-keys-zone: Key 20326 for zone . acceptance timer complete: key now trusted
Dec 02 21:10:36 DNSs named[548]: resolver priming query complete
Dec 02 21:10:36 DNSs named[548]: zone trash.hyp/IN: Transfer started.
Dec 02 21:10:36 DNSs named[548]: zone 56.168.192.in-addr.arpa/IN: refresh: unexpected rcode (SERVFAIL) from master 19
Dec 02 21:10:36 DNSs named[548]: transfer of 'trash.hyp/IN' from 192.168.56.250#53: connected using 192.168.56.249#58
Dec 02 21:10:36 DNSs named[548]: zone trash.hyp/IN: transferred serial 2
Dec 02 21:10:36 DNSs named[548]: transfer of 'trash.hyp/IN' from 192.168.56.250#53: Transfer status: success
Dec 02 21:10:36 DNSs named[548]: transfer of 'trash.hyp/IN' from 192.168.56.250#53: Transfer completed: 1 messages, 1
Dec 02 21:10:36 DNSs named[548]: zone trash.hyp/IN: sending notifies (serial 2)
lines 1-21/21 (END)
```

Comme nous le montre cette image les fichiers se sont bien copiés.

```
root@DNSs:/etc/bind# ls
bind.keys  db.127  db.empty  named.conf          named.conf.local  rndc.key
db.0      db.255  db.local  named.conf.default-zones  named.conf.options  zones.rfc1918
root@DNSs:/etc/bind# nano named.conf.local
root@DNSs:/etc/bind# cd
root@DNSs:~# cd /var/
root@DNSs:~# cd /var/
backups/  cache/  lib/      local/   lock/    log/     mail/    opt/     run/     spool/   tmp/
root@DNSs:~# cd /var/cache/bind/
root@DNSs:/var/cache/bind# ls
db.trash.hyp  managed-keys.bind  managed-keys.bind.jnl
root@DNSs:/var/cache/bind#
```

Test :

Dans ce cadre de test nous avons un serveur DHCP, nous avons renseigné le serveur DNS Esclave en DNS principale pour effectuer des questions avec la commande DIG suivie du nom d'un serveur ou l'IP, nous effectuons un DIG sur notre serveur maître (ns1.trash.hyp)

```

[client@localhost ~]$ dig ns1.trash.hyp

; <<> DiG 9.11.23-RedHat-9.11.23-1.fc32 <<> ns1.trash.hyp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54221
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 87a0e16b3f6759f32e1aa73b5fc7f7c8ab1846de861fe57a (good)
;; QUESTION SECTION:
ns1.trash.hyp.                IN      A

;; ANSWER SECTION:
ns1.trash.hyp.                604800  IN      A      192.168.56.250

;; AUTHORITY SECTION:
trash.hyp.                     604800  IN      NS     ns2.trash.hyp.
trash.hyp.                     604800  IN      NS     ns1.trash.hyp.

;; ADDITIONAL SECTION:
ns2.trash.hyp.                604800  IN      A      192.168.56.249

;; Query time: 0 msec
;; SERVER: 192.168.56.249#53(192.168.56.249)
;; WHEN: mer. déc. 02 21:23:36 CET 2020
;; MSG SIZE rcvd: 134

[client@localhost ~]$

```

Comme nous pouvons le voir, il arrive a faire la résolution du nom par son IP.

## Documentation

### 2.1 Rappels

Avant d'aborder de nouveaux concepts à propos de DNS :

— Rappelez le concept du service DNS

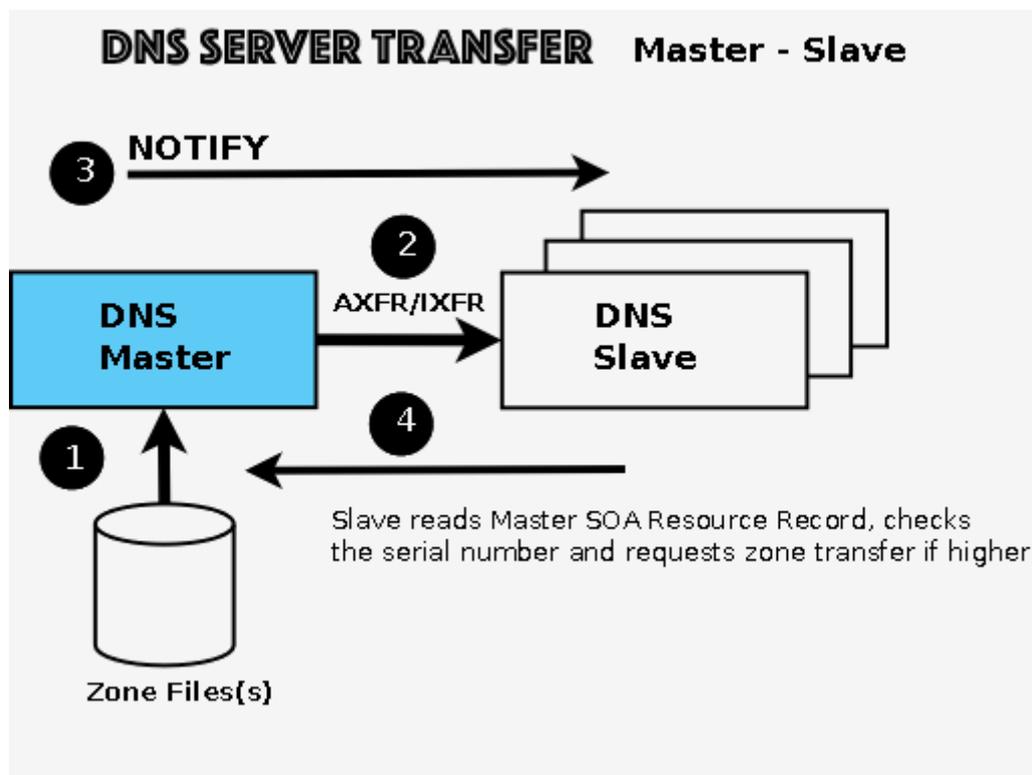
Le DNS appelé Domain Name System nous sert à traduire un nom de domaine en adresse IP. Il agit comme un annuaire, les ordinateurs qui veulent accéder par exemple à google.fr il ne vont pas taper l'adresse IP du serveur de google, l'ordinateur va interroger le Serveur DNS qui eux vont faire la correspondance avec leur IP et le nom.

— Présentez le concept de hiérarchisation du DNS

Le concept de hiérarchisation du DNS c'est se qui se passe tout en haut, appelé racine. Ce qui fait que nous pouvons créer un ou plusieurs sous-domaines.

### 2.2 Architecture Maître/esclave

Présentez en quelques mots (et en vous appuyant éventuellement sur un schéma) le principe de l'architecture maître/esclave appliqué au DNS.



Dans un premier temps il faut modifier le fichier de Zone du serveur Maître, renseigner le serveur avec l'IP du serveur notifier Esclave, puis effectuer la même opération avec le serveur Esclave mais en notifiant que c'est lui le serveur esclave, lui indiquer qui est le maître avec son IP, lui indiquer le chemin où il pourra copier les fichiers.

La délégation DNS c'est de lui donner ce fichier de configuration pour les transmettre à son tour au réseau.