

RAPPORT

THEME 3 LES DNS

Réalisé par :

Quentin GAVILAN
201093677

Monsieur Petit

2022-2023

SOMMAIRE

PROBLEMATIQUE	3
CONCEPTION	4
PARTIE 1 : DNS Maitre	4
PARTIE 2 : Serveur Esclave.....	7

PROBLEMATIQUE

On nous met à dispositions 3 machines virtuelles sous le système d'exploitation Debian 11, nommé respectivement serv1, serv2 et serv3 ayant comme spécificité qu'ils sont connectés en NAT au réseau 172.16.5.0, qu'ils ont respectivement les adresses IP suivante 172.16.5.11/24, 172.16.5.12/24, 172.16.5.13/24 et que leur Gateway est 172.16.5.2.

L'objectif est d'arriver à installer un serveur DNS faisant autorité sur serv1, puis un serveur DNS secondaire sur serv2 et enfin récursif sur serv3 dans la zone ibgbi.shayol.org.

Pour nous permettre d'atteindre cet objectif nous installeront et configureront différents paquets et logiciel sur nos serveurs.

Pour ce projet nous utiliseront :

- ✓ bind9, bind9-doc, bind9utils
- ✓ resolvconf, ufw
- ✓ libirs161

CONCEPTION

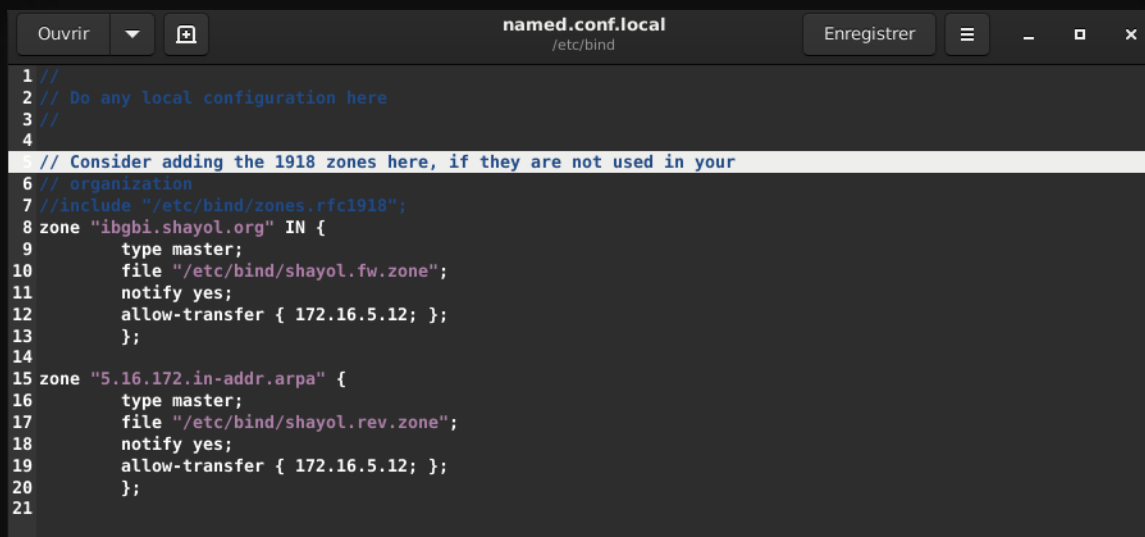
PARTIE 1 : DNS Maitre

Nous commencerons par installer le serveur DNS primaire de la zone ibgbi.shayol.org, pour ce faire nous devons installer les différents paquets listés précédemment en utilisant la commande apt install.

Une fois installé on rappelle ce qu'est un serveur DNS primaire (maitre), soit un serveur faisant autorité sur une zone DNS, chaque changement effectué sur ce serveur sera envoyé aux autres serveurs secondaires (esclave) de la zone grâce au mécanisme de [réplication](#) mise en place.

A présent nous nous rendons dans les fichiers conf de l'outil bind9 se trouvant dans le dossier/etc/bind, pour mettre en place notre serveur on utilisera l'éditeur de texte Gedit afin de modifier ses fichiers.

On ouvre en premier le fichier named.conf.local et on y ajoute ces lignes :



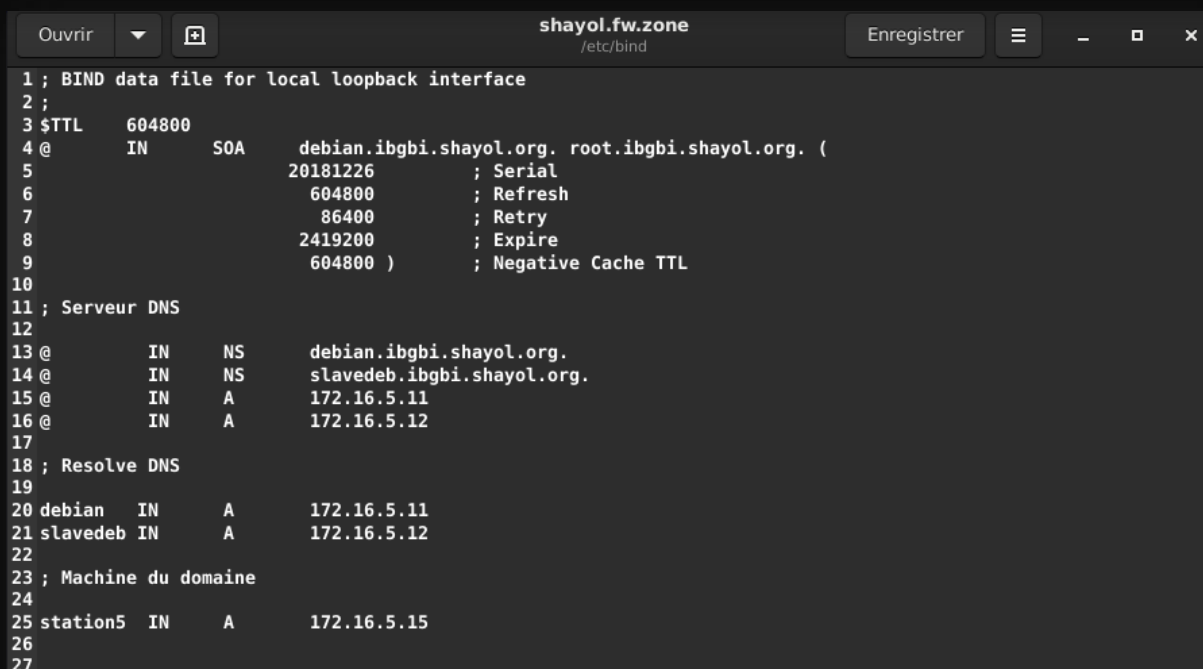
```
1 //
2 // Do any local configuration here
3 //
4
5 // Consider adding the 1918 zones here, if they are not used in your
6 // organization
7 //include "/etc/bind/zones.rfc1918";
8 zone "ibgbi.shayol.org" IN {
9     type master;
10    file "/etc/bind/shayol.fw.zone";
11    notify yes;
12    allow-transfer { 172.16.5.12; };
13 };
14
15 zone "5.16.172.in-addr.arpa" {
16    type master;
17    file "/etc/bind/shayol.rev.zone";
18    notify yes;
19    allow-transfer { 172.16.5.12; };
20 };
21
```

Nous avons donc 2 blocs de code :

- ✓ De la ligne 8 à 14 définissant la zone ibgbi.shayol.org contenant le type (master qui signifie DNS primaire), le chemin vers la configuration de cette zone et 2 autres options que nous expliquerons dans la [Partie 2](#)
- ✓ De la ligne 15 à 20 définissant la zone inverse du domaine ibgbi.shayol.org contenant donc les mêmes options que précédemment mais avec un chemin différent pour la configuration de la zone inverse.

Une fois modifié nous devons créer les fichiers conf des différents chemins vus précédemment shayol.fw.zone et shayol.rev.zone.

Nous ouvrons /etc/bind/shayol.fw.zone et nous y ajoutons ces lignes :



```
1 ; BIND data file for local loopback interface
2 ;
3 $TTL      604800
4 @         IN      SOA      debian.ibgbi.shayol.org. root.ibgbi.shayol.org. (
5             20181226      ; Serial
6             604800        ; Refresh
7             86400         ; Retry
8             2419200       ; Expire
9             604800 )      ; Negative Cache TTL
10
11 ; Serveur DNS
12
13 @         IN      NS       debian.ibgbi.shayol.org.
14 @         IN      NS       slavedeb.ibgbi.shayol.org.
15 @         IN      A        172.16.5.11
16 @         IN      A        172.16.5.12
17
18 ; Resolve DNS
19
20 debian    IN      A        172.16.5.11
21 slavedeb  IN      A        172.16.5.12
22
23 ; Machine du domaine
24
25 station5  IN      A        172.16.5.15
26
27
```

Nous retrouvons dans ce document :

- ✓ de la ligne 4 à 9 l'enregistrement SOA (Start of Authority) qui stocke les informations importantes d'une zone ou domaine, on a donc ici le MNAME debian.ibgbi.shayol.org le RNAME root.ibgbi.shayol.org ainsi que les numéros de serial, refresh, retry, expire et le TTL (Time To Live)
- ✓ de la ligne 11 à 26 les enregistrements A et NS des différents serveurs et machines de la zone, on retrouve le serveur maitre ayant comme nom debian.ibgbi.shayol.org et son IP 172.16.5.11 et un serveur esclave ayant comme nom slavedeb.ibgbi.shayol.org et son IP 172.16.5.12 que nous développerons dans la [partie 2](#).

Par la suite on crée l'autre fichier shayol.rev.zone avec ces modifications :

```
shayol.rev.zone
/etc/bind

1 ;
2 ; BIND reverse data file for local loopback interface
3 ;
4 $TTL      604800
5 @        IN      SOA      debian.ibgbi.shayol.org. root.ibgbi.shayol.org. (
6          1          ; Serial
7          604800     ; Refresh
8          86400      ; Retry
9          2419200    ; Expire
10         604800 )    ; Negative Cache TTL
11 ;
12 @        IN      NS       debian.ibgbi.shayol.org.
13 @        IN      NS       slavedeb.ibgbi.shayol.org.
14 @        IN      PTR      ibgbi.shayol.org.
15
16 debian   IN      A         172.16.5.11
17 slavedeb IN      A         172.16.5.12
18
19 ; Machine du domaine
20
21 11        IN      PTR      debian.ibgbi.shayol.org.
22 12        IN      PTR      slavedeb.ibgbi.shayol.org.
23 15        IN      PTR      station5.ibgbi.shayol.org.
```

On remarque :

- ✓ La ligne 5 à 10 on retrouve l'enregistrement SOA
- ✓ La ligne 11 à 23 on retrouve les enregistrements NS, A et PTR servant aux bonnes fonctions de la zone inverse.

Par la suite on vérifie l'intégrations du domaine et du DNS dans les configurations réseau de la machine pour cela on y ajoute dans le fichier /etc/resolv.conf les lignes nameserver 172.16.5.11 et search ibgbi.shayol.org ainsi que dans le fichier /etc/network/interfaces les lignes dns-domain ibgbi.shayol.org et dns-nameservers 172.16.5.11 Après avoir écrit les fichiers conf de la zone DNS on vérifie son fonctionnement avec les commandes :

- ✓ named-checkconf
- ✓ named-checkzone ibgbi.shayol.org /etc/bind/shayol.fw.zone
- ✓ named-checkzone ibgbi.shayol.org /etc/bind/shayol.fw.zone

```
Terminal - user1@debian: ~/Bureau
Fichier  Édition  Affichage  Terminal  Onglets  Aide
user1@debian:~/Bureau$ nslookup 172.16.5.11
11.5.16.172.in-addr.arpa      name = debian.ibgbi.shayol.org.

user1@debian:~/Bureau$ nslookup ibgbi.shayol.org
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   ibgbi.shayol.org
Address: 172.16.5.11
Name:   ibgbi.shayol.org
Address: 172.16.5.12

user1@debian:~/Bureau$ nslookup 172.16.5.12
12.5.16.172.in-addr.arpa      name = slavedeb.ibgbi.shayol.org.
```

PARTIE 2 : Serveur Esclave

Maintenant que nous avons configuré le serveur maître, nous allons configurer un serveur esclave pour assurer une disponibilité du service en cas de panne du serveur maître.

Pour mettre en place ce serveur on va modifier et autoriser les transferts de zone en ajoutant les lignes notify yes ; et allow-transfer { 172.16.5.12 ; } au fichier [named.conf.local](#)

On rappelle l'utilisation et le fonctionnement d'un transfert de zone :

La fonction DNS notify (RFC 1996) soit notification de changement de zone est utilisé par les serveurs DNS dans le but de mettre à jour les bases de données des serveurs esclaves.

Son fonctionnement réside dans l'enregistrement SOA possédant les champs retry, refresh et serial servant à la demande et à l'obtention de nouveau fichier de zone modifier par le serveur maître. Le numéro de série s'incrémente à chaque modification effectuée cela permet aux différents serveurs de comparer le numéro de série qu'ils possèdent avec celui du maître, s'ils diffèrent la mise à jour se poursuit. Le temps de retry et de refresh est le temps d'attente avant une nouvelle demande de vérification de fichier de zone au serveur maître après avoir eu un échec et sans avoir eu d'échec.

La particularité de Notify est que même si le temps de rafraîchissement n'est pas fini le serveur maître peut envoyer une notification de changement de zone s'il détecte une modification du numéro de série.

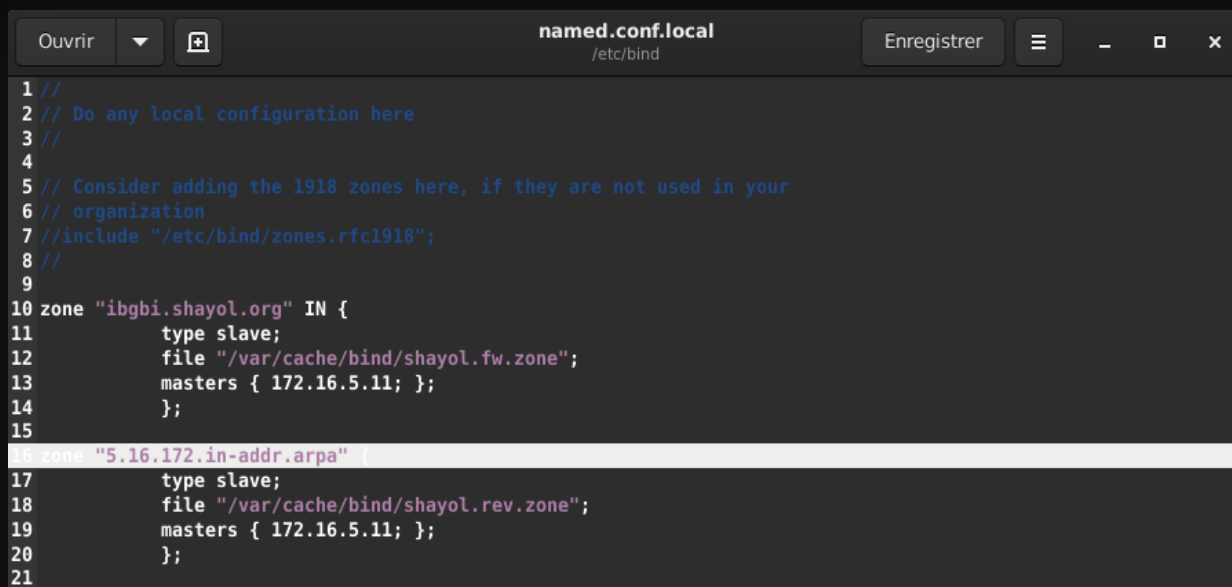
Il existe différents fonctionnements de transfert de zone dont 2 autres qui sont le transfert complet et incrémental.

Le transfert complet se fait en suivant le protocole de Notify en envoyant un QTYPE soit un query type correspondant à AXFR sur une connexion TCP au serveur maître lui répondant avec l'ensemble des ressources enregistrés de la zone commençant et finissant par le SOA

Le transfert incrémental se fait en suivant le protocole du transfert complet mais au lieu d'utiliser le QTYPE AXFR il utilisera le QTYPE IXFR comprenant la liste des modifications des ressources enregistrées de la zone dans l'ordre des numéros de série partant du dernier que possède le serveur esclave au plus récent à conserver.

Une fois ce changement effectué on modifiera les fichiers [shayol.fw.zone](#) et [shayol.rev.zone](#) pour y ajouter l'adresse IP du serveur secondaire ainsi que son hostname soit slavedeb avec l'IP 172.16.5.12 en tant qu'enregistrement NS, A et PTR.

Nous pouvons à présent modifier notre machine serv2 en ajoutant et modifiant le fichier named.conf.local ce qui nous donne :



```
1 //
2 // Do any local configuration here
3 //
4
5 // Consider adding the 1918 zones here, if they are not used in your
6 // organization
7 //include "/etc/bind/zones.rfc1918";
8 //
9
10 zone "ibgbi.shayol.org" IN {
11     type slave;
12     file "/var/cache/bind/shayol.fw.zone";
13     masters { 172.16.5.11; };
14 };
15
16 zone "5.16.172.in-addr.arpa" {
17     type slave;
18     file "/var/cache/bind/shayol.rev.zone";
19     masters { 172.16.5.11; };
20 };
21
```

On retrouve la même configuration que pour le serveur maitre avec la modification du type en tant que slave et du chemin du dossier qui est envoyé par le serveur maitre, on a aussi l'apparition de l'option masters servant à indiquer qu'elle est l'adresse du serveur primaire. Avant de faire nos tests on modifiera les fichiers interfaces et resolv.conf comme pour le serveur maitre afin d'assurer une bonne communication entre les différents serveurs.

Finalement après [vérification](#) et test de connexion on obtient bien une gestion de panne efficace avec 2 serveurs DNS sur la zone ibgbi.shayol.org soit la problématique posée par notre projet, nous n'avons malheureusement pas abordé la notion du serveur récursif aidant à la recherche indépendante des serveurs DNS dans la résolution de nom de domaine sans l'aide d'un client. Malgré cela ce projet nous aura permis de gérer un domaine existant en y installant 2 serveurs efficaces contre des pannes aléatoires.