/etcLe système DNS (Domain Name System)

Mise en place d'un serveur bind9 sur Debian

Objectif	Configuration du service DNS (bind9) sur un système Linux Debian.
Outils	Serveur Linux debian Clients linux, Windows ou autre système.
Mots-clés	DNS, nom de domaine, serveur primaire, serveur secondaire, serveurs racines, zone primaire, zone secondaire, zone reverse, délégation, requête récursive, requête itérative

Contexte matériel :

- Une VM Debian pour le serveur DNS ;
- La VM Linux « Serveur Apache » ;
- Une VM Linux client pour les tests.

Ressources :

- Documents annexes ;
- Internet.

Important : Avant de commencer le TP, consulter les documents fournis en annexe.

a. Rappeler le rôle du service DNS.

Le DNS permet de traduire des noms de domaine en adresse IP.

Expliquer le rôle des serveurs racines DNS. Qui gère ces serveurs racines ?

Les serveurs racines DNS interviennent quand un serveur DNS local n'a pas l'adresse IP en cache. Ils redirigent les requêtes vers les serveurs DNS responsable des domaines de premiers niveaux. Géré par ICANN et autres entreprises.
Il y a 13 serveurs racines

b. Donner des exemples de domaines de 1er niveau (TLD) :

.com .fr .net .org etc …

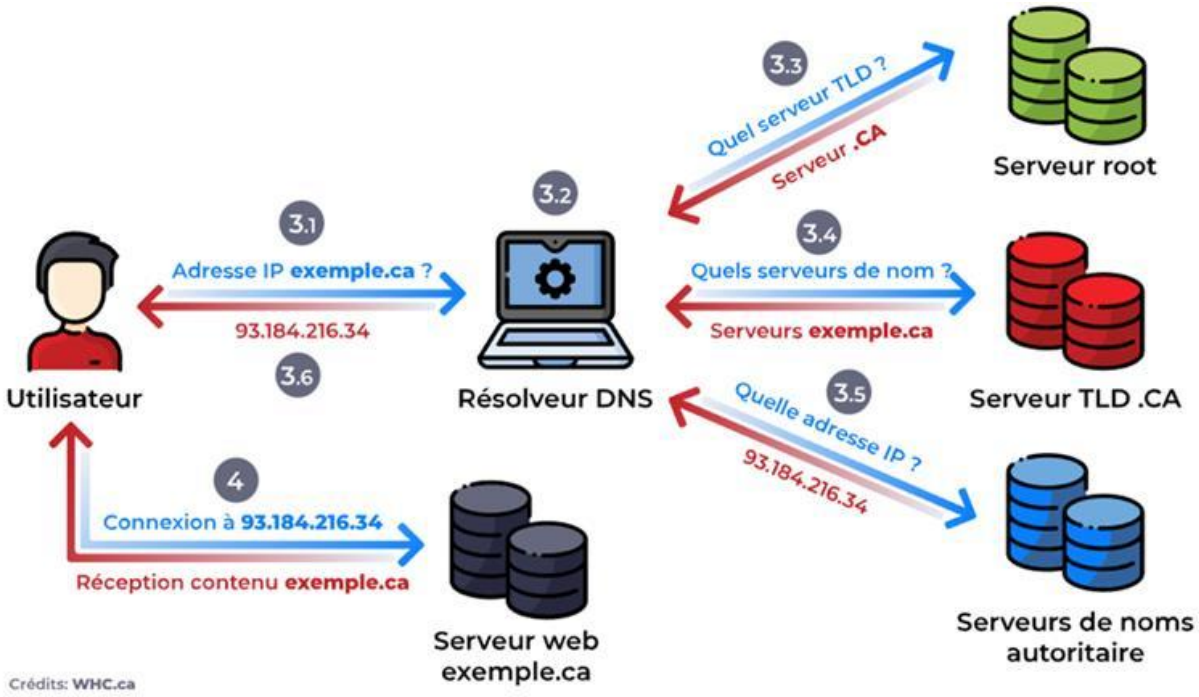
c. Quel est le rôle d'un serveur DNS résolveur ou récursif ?

Un serveur DNS résolveur est un serveur qui va lancer une série de requêtes vers d'autres serveurs DNS pour obtenir l'information s'il ne le pas en cache. Il interroge d'abord les serveurs racines, puis les serveurs de domaines de premier niveau (TLD), et enfin les serveurs de noms faisant autorité pour le domaine concerné. Il met l'info en cache pour une durée déterminé pour optimiser les requêtes futures.

d. Qu'est-ce qu'un serveur DNS autoritaire d'une zone ?

C'est le serveur qui stocke la base de données (fichiers) dans laquelle se trouvent les enregistrements noms de domaines et adresses IP

e. A l'aide d'un schéma, expliquer comment fonctionne la résolution de nom sur un serveur résolveur :



1. Installation des paquets et vérifications

f. *Installer les paquets suivants :*

```
apt update
apt install bind9 bind9-doc bind9utils dnsutils
```

Un nouveau groupe ainsi qu'un utilisateur système "**bind**" sont créés.

g. *Vérifier à l'aide des commandes :*

```
cat /etc/passwd | grep bind
cat /etc/group | grep bind
```

h. *Vérifier si le service est en écoute :*

```
ps -ef | grep named
```

i. *Vérifier l'état du service bind9 :* `systemctl…`

j. *Exécuter la commande suivante et commenter le résultat :*

```
ss -natu | grep 53
```

Marche pas

2. Utilisation des outils de diagnostic DNS

Le paquet **dnsutils** fournit quelques outils de diagnostic comme `nslookup`, `host` **et** `dig` permettent de vérifier les données relatives à chaque zone.

a. *Exécuter les commandes « dig » suivantes et commenter leur résultat :*

```
dig @8.8.8.8 google.com
```

```
dig gmail.com MX
```

```
dig google.com SOA
```

```
dig google.com NS
```

```
dig +trace www.google.com
```

b. *Exécuter les commandes « nslookup » suivantes et commenter leur résultat :*

```
nslookup www.google.com
```

```
nslookup www.google.com 8.8.8.8
```

c. Exécuter les commandes « host » suivantes et commenter leur résultat :

```
host google.com
```

```
host 8.8.8.8
```

```
host 9.9.9.9
```

3. Fichiers de configuration de bind9

Les fichiers principaux nécessaires à la configuration du DNS sont créés par défaut dans le dossier **`/etc/bind/`**.

a. Avant de commencer les modifications, effectuer une sauvegarde du dossier /etc/bind : *`cp -r …`*

b. Lister le contenu du dossier /etc/bind :

c. Afficher le contenu du fichier de configuration globale *`named.conf`* ***. Que contient-il ?***

Contient les zones DNS que le serveur est autorisé à gérer.

d. Afficher le contenu du fichier *`named.conf.options`* ***. Que contient-il ?***

Option général du serveur qui s'applique à l'ensemble.

e. Afficher le contenu du fichier *`named.conf.default-zones`* ***. Que contient-il ?***

Les zones DNS par défaut

f. Afficher le contenu du fichier *`named.conf.local`* ***. Que contient-il ?***

l'endroit où vous définissez les zones DNS que votre serveur gère localement. Il sépare les configurations spécifiques aux zones des options globales, ce qui rend la configuration plus organisée et plus facile à gérer.

Les serveurs racines : `voir annexes`

Le fichier des serveurs racine `/usr/share/dns/root.hints` contient la liste de tous les serveurs racine (root) avec leur nom et leur adresse IP.

g. Afficher le contenu du fichier *`/usr/share/dns/root.hints`* ***. Combien y a-t-il de serveur racine ?***

13 serveurs

Les fichiers d'enregistrements de zone :

Il faut un fichier par zone pour toutes les zones pour lesquelles le serveur a autorité, il contient les **enregistrements propres à chaque zone** ; le fichier créé par défaut est `db.local` et correspond à la zone "localhost".

a. Afficher le contenu du fichier `db.local` :

```
  GNU nano 7.2
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

Les fichiers de zone « reverse » : `voir annexes`

Ces fichiers permettent la résolution inverse AdresseIP → nom-domaine.

Par défaut, ils sont au nombre de 3 par défaut : db.127 (zone reverse pour localhost), db.255 (zone locale de broadcast), db.0 (zone locale de broadcast).

b. Afficher le contenu du fichier `db.127.`

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     localhost. root.localhost. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      localhost.
1.0.0   IN      PTR     localhost.
```

Des exemples de fichiers de zone sont détaillés en *`annexe 2.`*

Si ces fichiers sont modifiés, il est nécessaire de les "relire" ou de redémarrer le service *bind9* (`systemctl restart bind9 ou systemctl reload bind9`).

4. Création de la zone « sio1.local » : `voir annexes`

a. ***Editer le fichier named.conf.local et y ajouter la zone*** « `sio1.local` »***. Nommer le fichier de zone*** `db.sio1.local`. ***Ecrire le code ci-dessous :***

b. ***Créer et compléter le fichier d'enregistrements de la zone*** `sio1.local` ***en le nommant*** `db.sio1.local`.(Voir exemple page 9).

c. ***Redémarrer le service bind9.***

d. ***Vérifier la configuration en exécutant la commande :***

```
named-checkconf -z
```

e. ***Vérifier la configuration de la zone*** « **`sio1.local`** » ***et son fichier*** « **`db.sio1.local`** » ***:***

```
named-checkzone nomZone fichier-zone
```

f. ***Vérifier l'état du service bind9.***

```
systemctl …
```

g. ***Tester le service à l'aide de la commande :***

```
dig @IP-serveurDNS nom-serveur.sio1.local
```

```
ping nom-serveur.sio1.local
```

5. Création de la zone reverse « `1.168.192.in-addr.arpa` » (voir annexes)

h. ***Rappeler le rôle d'une zone inverse ou reverse :***

i. ***Editer le fichier*** ***`named.conf.local`*** ***et y ajouter la zone reverse « `1.168.192.in-addr.arpa` ».*** *(Voir annexe).*

j. ***Créer et compléter le fichier d'enregistrements de la zone reverse en le nommant*** `db.192.168.1.rev`. (Voir annexe).

k. ***Redémarrer le service bind9.***

l. ***Vérifier la configuration en exécutant la commande :***

```
named-checkconf -z
```

Résultat :

m. ***Tester la résolution inverse à l'aide de la commande :***

```
dig -x adesse-ip
```

6. Capture et analyse des trames DNS sur Wireshark