

## Résumé

Ce support de travaux pratiques sur le service Domain Name System s'appuie sur le logiciel BIND. Côté client ou resolver, il illustre les différents tests de fonctionnement du service à l'aide de la **dig**. Côté serveur, il présente l'utilisation du service suivant 3 modes : cache seulement (cache-only), maître (primary|master) et esclave (secondary|slave).

## Table des matières

1. Copyright et Licence .....	1
1.1. Meta-information .....	1
1.2. Conventions typographiques .....	1
2. Architecture type de travaux pratiques .....	3
3. Installation du service DNS cache-only .....	3
4. Requêtes DNS sur les différents types d'enregistrements (Resource Records) .....	4
5. Validation ou dépannage d'une configuration .....	4
6. Serveur primaire de la zone zone(i).lan-213.stri .....	8
7. Configuration du serveur secondaire de la zone zone(i).lan-213.stri .....	10
8. Délégation de la zone lab depuis le niveau lan-213.stri .....	10
8.1. Échange du niveau supérieur vers le niveau inférieur .....	10
8.2. Échange du niveau inférieur vers le niveau supérieur .....	11
9. Sécurisation de premier niveau .....	12
10. Documents de référence .....	13

## 1. Copyright et Licence

Copyright (c) 2000,2015 Philippe Latu.  
Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2015 Philippe Latu.  
Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.3 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture, et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est incluse dans la section intitulée « Licence de Documentation Libre GNU ».

### 1.1. Meta-information

Ce document est écrit avec **DocBook**<sup>1</sup> XML sur un système **Debian GNU/Linux**<sup>2</sup>. Il est disponible en version imprimable au format PDF : [sysadm-net.dns.q.pdf](http://www.inetdoc.net/pdf/sysadm-net.dns.q.pdf)<sup>3</sup>.

### 1.2. Conventions typographiques

Tous les exemples d'exécution des commandes sont précédés d'une invite utilisateur ou prompt spécifique au niveau des droits utilisateurs nécessaires sur le système.

- Toute commande précédée de l'invite \$ ne nécessite aucun privilège particulier et peut être utilisée au niveau utilisateur simple.

<sup>1</sup> <http://www.docbook.org>

<sup>2</sup> <http://www.debian.org>

<sup>3</sup> <http://www.inetdoc.net/pdf/sysadm-net.dns.q.pdf>

- Toute commande précédée de l'invite # nécessite les privilèges du super-utilisateur.

## 2. Architecture type de travaux pratiques

Comme indiqué dans le support [Architecture réseau des travaux pratiques](#)<sup>4</sup>, on part d'une configuration type avec deux de postes de travail qui partagent le même domaine de diffusion. Le schéma d'une maquette utilisant deux instances de machines virtuelles et un système hôte est le suivant :

**Tableau 1. Adressage IP des postes et attribution des zones DNS**

Poste 1 : serveur primaire	Adresse IP	Poste 2 : serveur secondaire	Passerelle par défaut	zone DNS
Alderaan	192.168.126.66/28	Bespin	192.168.126.65/28	zone1.lan-213.stri
Centares	172.19.115.194/26	Coruscant	172.19.115.193/26	zone2.lan-213.stri
Dagobah	192.168.109.2/25	Endor	192.168.109.1/25	zone3.lan-213.stri
Felucia	10.7.10.2/23	Geonosis	10.7.10.1/23	zone4.lan-213.stri
Hoth	10.5.6.2/23	Mustafar	10.5.6.1/23	zone5.lan-213.stri
Naboo	172.19.114.130/26	Tatooine	172.19.114.129/26	zone6.lan-213.stri

**Q1.** Quelle est la représentation graphique de l'arborescence DNS correspondant aux affectations données ci-dessus ?

À partir des informations du document [Architecture réseau des travaux pratiques](#)<sup>5</sup>, compléter la chaîne des serveurs DNS permettant la résolution des noms de domaines jusqu'à la racine.

## 3. Installation du service DNS cache-only

Avant d'aborder la configuration du service DNS, il faut passer par l'étape rituelle de sélection et d'installation des paquets contenant les outils logiciels de ce service.

**Q2.** Quels sont les paquets Debian correspondant au service DNS ?

Reprendre les différentes possibilités d'interrogation de la base de données des paquets vues lors des travaux pratiques précédents. On ne retient que les paquets relatifs à la version 9.x du logiciel BIND (Berkeley Internet Name Domain).

**Q3.** Quelles sont les manipulations à effectuer pour valider le fonctionnement du service DNS ?

Contrôler la liste des processus actifs sur le système, la liste des ports réseau ouverts ainsi que les journaux système.

**Q4.** Quels sont les répertoires contenant les fichiers de configuration du service DNS ?

Identifier les répertoires à partir de la liste des fichiers du paquet bind9.

**Q5.** Qu'est ce qui distingue le répertoire général de configuration du répertoire de stockage des fichiers de zone ?

Consulter la documentation [BIND 9 Administrator Reference Manual](#)<sup>6</sup>.

**Q6.** Pourquoi l'installation du paquet bind9 correspond à un service DNS de type cache-only ?

Identifier la ou les zones sur lesquelles le service a autorité à partir des informations contenues dans les journaux système et les fichiers de configuration `named.conf.*`.

<sup>4</sup> [http://www.inetdoc.net/travaux\\_pratiques/infra.tp/](http://www.inetdoc.net/travaux_pratiques/infra.tp/)

<sup>5</sup> [http://www.inetdoc.net/travaux\\_pratiques/infra.tp/](http://www.inetdoc.net/travaux_pratiques/infra.tp/)

<sup>6</sup> <http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.html>

Consulter la section relative au service de type cache-only dans le document [BIND 9 Administrator Reference Manual](#)<sup>7</sup>.

- Q7.** Comment appelle-t-on le logiciel client chargé d'interroger le service de noms de domaines ? Rechercher le mot clé `resolver` dans les pages de manuels.
- Q8.** Quelle est l'opération à effectuer pour le service DNS installé plus tôt soit effectivement utilisé ? Rechercher la syntaxe à utiliser pour éditer le fichier `/etc/resolv.conf`.
- Q9.** À quel paquet appartient la commande **dig** ? Quelle est sa fonction ? Utiliser le gestionnaire de paquets local **dpkg**.

#### 4. Requêtes DNS sur les différents types d'enregistrements (*Resource Records*)

Avant d'aborder la déclaration de nouvelles zones, il faut installer et valider le fonctionnement du service. La phase de validation passe par une batterie de tests d'interrogation des différents champs du service DNS.

Cette section est basée sur la commande **dig**. Les pages de manuels de cette commande doivent servir de base de réponse aux questions suivantes.



##### Pourquoi abandonner **nslookup** ?

La commande **nslookup** est la commande historique liée aux requêtes du service DNS. Le principal reproche fait à cette commande vient de ses réponses inadéquates en cas d'erreurs. Malheureusement, ce comportement non conforme a été utilisé dans de très nombreux développements de shell scripts. Pour ne pas entraîner des problèmes en cascade, les développeurs ont décidé d'initier un nouveau développement avec les versions 8.x puis 9.x de BIND : la commande **dig**. Comme ces travaux pratiques utilisent une version 9.x de BIND, il est logique de s'appuyer sur cette nouvelle commande **dig**.

- Q10.** Comment reconnaître le serveur DNS utilisé lors d'une requête avec la commande **dig** ? Comment peut-on visualiser l'utilisation du cache du service DNS ? Lire attentivement les résultats d'une exécution de la commande **dig** sur un nom de domaine quelconque.
- Q11.** Quelles sont les options de la commande **dig** à utiliser pour émettre des requêtes des types suivants : NS, A, PTR, et MX ? Donner un exemple de chaque type. Les différents enregistrements ou Resource Records d'une zone sont accessibles à partir de requêtes individuelles. Les options de la commande **dig**, documentées dans les pages de manuels (`man dig`), permettent d'indiquer le type d'enregistrement demandé (RR) après le nom de domaine.
- Q12.** Quelle est l'option de la commande **dig** à utiliser pour émettre des requêtes itératives ? Donner un exemple. Consulter les pages de manuels de la commande **dig** à la recherche du traçage des étapes d'une requête.
- Q13.** Quelle est la syntaxe de la commande **dig** à utiliser pour interroger la classe CHAOS ? Donner deux exemples de requêtes sur les champs `version.bind` et `authors.bind`. Consulter les pages de manuels de la commande **dig** à la recherche des définitions de classes.

#### 5. Validation ou dépannage d'une configuration

Les sections précédentes sur les types de requêtes fournissent déjà quelques éléments sur la validation ou le dépannage du service DNS.

<sup>7</sup> <http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.html>

- Le temps de réponse à une requête (Query time:) renseigne sur l'utilisation ou non du cache mémoire.
- En cas de panne, une **requête itérative** permet d'identifier le point de rupture dans la chaîne de résolution des noms.

Il reste deux options particulièrement utiles à la mise au point d'une configuration correcte.

Il est possible de désigner explicitement le serveur DNS qui doit prendre en charge la requête à l'aide de son adresse IP. Cette opération est très utile pour vérifier qu'un serveur primaire répond correctement aux demandes sur les enregistrements qu'il détient. Dans le contexte de la sécurisation du service, cette même opération sert à contrôler qu'un serveur ne répond qu'au requêtes qu'il est sensé traiter. Voici deux exemples utilisant respectivement la désignation du serveur interrogé par son adresse IP et la requête directe de transfert de zone.

Pour vérifier que le service DNS de la zone `nic.fr` fournit l'adresse du serveur Web ayant le nom `www.nic.fr`, on peut procéder comme suit.

- On identifie un serveur de nom pour la zone.

```
$ dig ns nic.fr

; <<>> DiG 9.8.1-P1 <<>> ns nic.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23937
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 11

;; QUESTION SECTION:
;nic.fr.                                IN      NS

;; ANSWER SECTION:
nic.fr.      176789  IN      NS      ns1.ext.nic.fr.
nic.fr.      176789  IN      NS      ns3.nic.fr.
nic.fr.      176789  IN      NS      ns1.nic.fr.
nic.fr.      176789  IN      NS      ns4.ext.nic.fr.
nic.fr.      176789  IN      NS      ns2.nic.fr.
nic.fr.      176789  IN      NS      ns6.ext.nic.fr.

;; ADDITIONAL SECTION:
ns1.ext.nic.fr. 176789  IN      A       193.51.208.13
ns1.nic.fr.     176789  IN      A       192.134.4.1
ns1.nic.fr.     176789  IN      AAAA    2001:660:3003:2::4:1
ns2.nic.fr.     176789  IN      A       192.93.0.4
ns2.nic.fr.     176789  IN      AAAA    2001:660:3005:1::1:2
ns3.nic.fr.     176789  IN      A       192.134.0.49
ns3.nic.fr.     176789  IN      AAAA    2001:660:3006:1::1:1
ns4.ext.nic.fr. 176789  IN      A       193.0.9.4
ns4.ext.nic.fr. 176789  IN      AAAA    2001:67c:e0::4
ns6.ext.nic.fr. 176789  IN      A       130.59.138.49
ns6.ext.nic.fr. 176789  IN      AAAA    2001:620:0:1b:5054:ff:fe74:8780

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Oct 7 23:09:40 2012
;; MSG SIZE rcvd: 372
```

- On interroge directement le serveur primaire de la zone.

```

$ dig @ns1.nic.fr www.nic.fr

; <<>> DiG 9.8.1-P1 <<>> @ns1.nic.fr www.nic.fr
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33946
;; flags: qr aa rd; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 11
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.nic.fr.                IN      A

;; ANSWER SECTION:
www.nic.fr.                172800  IN      CNAME   web.nic.fr.
web.nic.fr.                172800  IN      A       192.134.4.20

;; AUTHORITY SECTION:
nic.fr.                    172800  IN      NS      ns3.nic.fr.
nic.fr.                    172800  IN      NS      ns6.ext.nic.fr.
nic.fr.                    172800  IN      NS      ns4.ext.nic.fr.
nic.fr.                    172800  IN      NS      ns1.nic.fr.
nic.fr.                    172800  IN      NS      ns1.ext.nic.fr.
nic.fr.                    172800  IN      NS      ns2.nic.fr.

;; ADDITIONAL SECTION:
ns1.ext.nic.fr.           172800  IN      A       193.51.208.13
ns1.nic.fr.               172800  IN      A       192.134.4.1
ns1.nic.fr.               172800  IN      AAAA    2001:660:3003:2::4:1
ns2.nic.fr.               172800  IN      A       192.93.0.4
ns2.nic.fr.               172800  IN      AAAA    2001:660:3005:1::1:2
ns3.nic.fr.               172800  IN      A       192.134.0.49
ns3.nic.fr.               172800  IN      AAAA    2001:660:3006:1::1:1
ns4.ext.nic.fr.           172800  IN      A       193.0.9.4
ns4.ext.nic.fr.           172800  IN      AAAA    2001:67c:e0::4
ns6.ext.nic.fr.           172800  IN      A       130.59.138.49
ns6.ext.nic.fr.           172800  IN      AAAA    2001:620:0:1b:5054:ff:fe74:8780

;; Query time: 40 msec
;; SERVER: 2001:660:3003:2::4:1#53(2001:660:3003:2::4:1)
;; WHEN: Sun Oct 7 23:11:33 2012
;; MSG SIZE rcvd: 410

```

On voit apparaître une indication selon laquelle le serveur interrogé ne prendra pas en charge les requêtes récursives pour le client utilisé. C'est tout à fait normal dans la mesure où ces tests de requêtes ne sont pas effectués depuis un poste client appartenant au domaine `nic.fr`.

Pour autant, on obtient bien la réponse à la requête posée puisque l'enregistrement demandé appartient bien à la zone sur laquelle le serveur a autorité.

- On interroge directement le même serveur avec une requête portant sur une autre zone.

```

$ dig @ns1.nic.fr www.phrack.org

; <<>> DiG 9.8.1-P1 <<>> @ns1.nic.fr www.phrack.org
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 16990
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;www.phrack.org.          IN      A

;; Query time: 39 msec
;; SERVER: 2001:660:3003:2::4:1#53(2001:660:3003:2::4:1)
;; WHEN: Sun Oct 7 23:14:58 2012
;; MSG SIZE rcvd: 32

```

Cette fois-ci la requête est refusée. Le serveur primaire ne veut pas prendre en charge la requête posée. C'est encore tout à fait normal dans la mesure le client n'appartient pas aux réseaux de la zone nic.fr.

- Certains services sont très «ouverts» et acceptent de prendre en charge les requêtes de n'importe quel client. La même requête posée à un de ces services est traitée normalement.

```

$ dig @dns1.gaoland.net www.phrack.org

; <<>> DiG 9.8.1-P1 <<>> @dns1.gaoland.net www.phrack.org
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19478
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.phrack.org.                IN      A

;; ANSWER SECTION:
www.phrack.org.                86400   IN      A      120.138.19.103

;; AUTHORITY SECTION:
phrack.org.                    86400   IN      NS     ns1.register-it.net.
phrack.org.                    86400   IN      NS     ns2.register-it.net.

;; ADDITIONAL SECTION:
ns1.register-it.net.          86395   IN      A      83.246.76.254
ns2.register-it.net.          86395   IN      A      83.246.77.10

;; Query time: 48 msec
;; SERVER: 212.94.162.1#53(212.94.162.1)
;; WHEN: Sun Oct 7 23:17:38 2012
;; MSG SIZE rcvd: 145

```

Sous toute réserve, il semble bien que le fait de répondre aux requêtes de n'importe quel client ne corresponde pas aux bonnes pratiques sur la configuration du service DNS de nos jours.

Dans le cadre de ces travaux pratiques, on veillera donc à n'autoriser les requêtes récursives qu'aux clients appartenant aux réseaux définis dans le plan d'adressage IP de l'énoncé.

La requête directe de transfert de zone permet de valider les autorisations d'échanges entre le serveur primaire et les autres serveurs ayant autorité sur la même zone.

Dans l'exemple de requête ci-dessous on interroge le serveur primaire à partir du serveur secondaire.

```

$ dig @172.16.80.1 axfr lan-213.stri

; <<>> DiG 9.8.1-P1 <<>> @172.16.80.1 axfr lan-213.stri
; (1 server found)
;; global options: +cmd
lan-213.stri.      86400   IN      SOA     casper.infra.stri. root.casper.infra.stri. 2012090701 2
lan-213.stri.      86400   IN      MX      0 mail.stri.
lan-213.stri.      86400   IN      NS      casper.infra.stri.
lan-213.stri.      86400   IN      NS      cooper.lan-213.stri.
alderaan.lan-213.stri. 86400   IN      A       172.16.80.10
amethyste.lan-213.stri. 86400   IN      A       172.16.80.5
anison.lan-213.stri. 86400   IN      A       172.16.80.23
bespin.lan-213.stri. 86400   IN      A       172.16.80.11
casper.lan-213.stri. 86400   IN      A       172.16.80.2
centares.lan-213.stri. 86400   IN      A       172.16.80.12
cooper.lan-213.stri. 86400   IN      A       172.16.80.1
coruscant.lan-213.stri. 86400   IN      A       172.16.80.13
dagobah.lan-213.stri. 86400   IN      A       172.16.80.14
endor.lan-213.stri. 86400   IN      A       172.16.80.15
felucia.lan-213.stri. 86400   IN      A       172.16.80.16
geonosis.lan-213.stri. 86400   IN      A       172.16.80.17
hoth.lan-213.stri. 86400   IN      A       172.16.80.18
kamino.lan-213.stri. 86400   IN      A       172.16.80.19
mustafar.lan-213.stri. 86400   IN      A       172.16.80.20
naboo.lan-213.stri. 86400   IN      A       172.16.80.21
perle.lan-213.stri. 86400   IN      A       172.16.80.6
tatooine.lan-213.stri. 86400   IN      A       172.16.80.22
topaze.lan-213.stri. 86400   IN      A       172.16.80.4
lan-213.stri.      86400   IN      SOA     casper.infra.stri. root.casper.infra.stri. 2012090701 2
;; Query time: 1 msec
;; SERVER: 172.16.80.1#53(172.16.80.1)
;; WHEN: Sun Oct 7 23:24:57 2012
;; XFR size: 24 records (messages 1, bytes 619)

```

Pour éviter une «recensement trop facile» de l'identité des hôtes d'une zone, il est essentiel de n'autoriser ces requêtes de transfert qu'entre serveurs DNS. Cette configuration du contrôle d'accès est présentée dans la [Section 9, « Sécurité de premier niveau »](#).

## 6. Serveur primaire de la zone zone(i).lan-213.stri

Il s'agit ici de configurer un serveur maître pour une nouvelle branche ou zone de l'arborescence DNS de travaux pratiques. On part de l'installation du service cache-only et on complète les fichiers de configuration.

La syntaxe des fichiers de zone n'est pas facile à maîtriser au premier abord. Il est donc nécessaire de faire appel à des patrons de fichiers de configuration. Un premier jeu de ces fichiers est disponible dans la documentation [BIND 9 Administrator Reference Manual](#)<sup>8</sup>. Un second jeu, pour une configuration sécurisée, est disponible à partir du site [Secure BIND Template](#).

Le fichier `/usr/share/doc/bind9/README.Debian.gz` contient des informations importantes sur l'organisation des fichiers de configuration du service. Il faut retenir les éléments suivants :

- Les fichiers `db.*` qui contiennent les enregistrements sur les serveurs racine et l'interface de boucle locale sont fournis directement avec le paquet Debian. Ils sont donc susceptibles d'être mis à jour à chaque nouvelle version du paquet.
- Le fichier de configuration principal `named.conf` a été éclaté en trois parties.

`named.conf`

Déclarations d'autorité sur le `localhost` et la diffusion en résolution directe et inverse. Liste des fichiers `db.*`.

Ce fichier appartient au paquet `bind9` et est susceptible d'être mis à jour. Il ne faut donc pas éditer ce fichier ou y insérer des informations de définitions de zones contrôlées par le service DNS.

<sup>8</sup> <http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.html>

`named.conf.local`

Déclarations d'autorité sur les zones administrées par le serveur ; qu'il s'agisse d'un serveur primaire ou secondaire. Ce fichier n'est pas modifié lors d'une mise à jour du paquet Debian.

C'est donc le fichier qui doit être édité pour déclarer les zones sous le contrôle du serveur DNS.

`named.conf.options`

Paramétrage des options du service notamment du répertoire contenant les fichiers de déclaration des zones administrées `/var/cache/bind/`. Voir le [BIND 9 Administrator Reference Manual](#) pour obtenir la liste de ces options.

C'est le fichier qui doit être édité pour sécuriser les accès aux enregistrements des zones sous le contrôle du serveur DNS.

**Q14.** Quel est le fichier de configuration à éditer pour que le service DNS installé ait autorité sur la zone `zone(i).lan-213.stri` ?

Établir la correspondance entre l'organisation des fichiers de configuration du paquet Debian et les indications des documents de référence.

**Q15.** Quel est le fichier de configuration qui désigne le répertoire de stockage des fichiers de déclaration de zone ? Quel est ce répertoire ? Quelle est la particularité de son masque de permissions ?

Établir la correspondance entre l'organisation des fichiers de configuration du paquet Debian et les indications de la documentation de référence. Repérer le propriétaire du processus `named` et relever ses caractéristiques : `uid`, `gid`, répertoire utilisateur, etc.

**Q16.** À l'aide de l'exemple donné dans le document [DNS HOWTO : A real domain example](#)<sup>9</sup>, créer un fichier de déclaration de la zone directe `zone(i).lan-213.stri` dans le répertoire adéquat.

Le fichier de zone doit comprendre :

- Deux serveurs de noms : un primaire et un secondaire.
- Un Mail Exchanger.
- Trois hôtes avec des adresses IP différentes et quelques Canonical Names.

---

 **Avertissement**

Pour les besoins des travaux pratiques, les temps définis dans l'enregistrement SOA ont été considérablement réduits pour caractériser l'effet des notifications et des durées de maintien en cache mémoire. Ces temps permettent aussi de propager les modifications sur les enregistrements plus rapidement en incrémentant les numéros de version.

---

**Q17.** À l'aide de l'exemple donné dans le document [DNS HOWTO : A real domain example](#)<sup>10</sup>, créer un fichier de déclaration de la zone inverse `100.51.198` dans le répertoire adéquat.

**Q18.** Quel est l'outil à utiliser pour valider la syntaxe des déclarations d'enregistrement avant d'activer la nouvelle zone ?

Consulter la liste des outils fournis avec les paquets relatifs au logiciel `bind9`.

**Q19.** Comment activer les nouveaux enregistrements de zone ? Valider la prise en charge de ces enregistrements

Recharger la configuration du service DNS et consulter les journaux système correspondant

**Q20.** Comment valide-t-on individuellement chacun des enregistrements déclarés ?

<sup>9</sup> <http://www.tldp.org/HOWTO/DNS-HOWTO-7.html>

<sup>10</sup> <http://www.tldp.org/HOWTO/DNS-HOWTO-7.html>

Reprendre la séquence des tests donnés dans la [Section 4, « Requêtes DNS sur les différents types d'enregistrements \(Resource Records\) »](#).

## 7. Configuration du serveur secondaire de la zone `zone(i).lan-213.stri`

Il s'agit ici de configurer un serveur secondaire pour la zone de l'arborescence DNS de travaux pratiques mise en place dans la section précédente. Comme dans le cas du serveur primaire, on part de l'installation du service `cache-only` fournie par le paquet Debian et on complète les fichiers de configuration.

Pour distinguer un serveur primaire d'un serveur secondaire, il faut savoir que le serveur primaire détient effectivement les fichiers de déclaration des enregistrements. Un serveur secondaire, en revanche, obtient les copies des déclarations des enregistrements par transfert réseau.

**Q21.** Quel est le fichier de configuration à éditer pour que le service DNS installé ait autorité sur la zone `zone(i).lan-213.stri` ?

Établir la correspondance entre l'organisation des fichiers de configuration du paquet Debian et les indications des documents de référence.

**Q22.** Quel est le fichier de configuration qui désigne le répertoire de stockage des fichiers de déclaration de zone ? Quel est ce répertoire ? Quelle est la particularité de son masque de permissions ?

Établir la correspondance entre l'organisation des fichiers de configuration du paquet Debian et les indications de la documentation de référence. Repérer le propriétaire du processus `named` et relever ses caractéristiques : `uid`, `gid`, répertoire utilisateur, etc.

**Q23.** Quel est l'outil à utiliser pour valider la syntaxe des déclarations d'enregistrement avant d'activer la nouvelle zone ?

Consulter la liste des outils fournis avec les paquets relatifs au logiciel `bind9`.

**Q24.** Comment les enregistrements (Resource Records) d'un serveur DNS secondaire sont-ils obtenus ? Quel est le type de requête qui permet de valider la disponibilité des nouveaux enregistrements ?

Rechercher dans la liste des requêtes utilisables avec la commande **dig**.

**Q25.** Comment activer les nouveaux enregistrements de zone ? Valider la prise en charge de ces enregistrements

Recharger la configuration du service DNS et consulter les journaux système correspondant

Lors d'une modification de la liste des enregistrements, il est important d'incrémenter correctement le numéro de série de façon à notifier l'ensemble des serveurs ayant autorité sur une zone. Dans l'extrait du fichier `/var/log/syslog/` du serveur primaire donné ci-dessous, on voit bien apparaître ces notifications.

```
named[2863]: client 198.51.100.3#54299: transfer of 'lab.lan-213.stri/IN': AXFR started
named[2863]: client 198.51.100.3#54299: transfer of 'lab.lan-213.stri/IN': AXFR ended
named[2863]: client 198.51.100.3#57978: transfer of '100.51.198.in-addr.arpa/IN': AXFR started
named[2863]: client 198.51.100.3#57978: transfer of '100.51.198.in-addr.arpa/IN': AXFR ended
```

## 8. Délégation de la zone `lab` depuis le niveau `lan-213.stri`

### 8.1. Échange du niveau supérieur vers le niveau inférieur



#### Avertissement

Cette partie est complétée par l'enseignant sur le serveur DNS de travaux pratiques ayant autorité au niveau supérieur. Ce niveau supérieur correspond à un Top Level Domain (TLD) factice.

Le serveur maître de la zone `lan-213.stri` doit déléguer le domaine `lab.lan-213.stri` aux postes de travaux pratiques qui détiennent les enregistrements (RRs) du sous-domaine.

Dans le contexte de la maquette utilisée pour ce document, le système hôte doit déléguer le sous-domaine aux deux instances de machines virtuelles.

Les fichiers de configuration donnés dans cette section sont surtout utiles pour les communications inter-zones lors des travaux pratiques. En effet, pour que les services internet qui s'appuient sur la résolution des noms puissent fonctionner normalement, il est essentiel que les branches de cette arborescence DNS factice soient toutes reliées les unes aux autres.

Le fichier de configuration du service sur le système hôte comprend les éléments suivants.

```
zone "lab.lan-213.stri" {
    type slave;
    file "lab.lan-213.stri.bak";
    masters { 198.51.100.2; };
};

zone "100.51.198.in-addr.arpa" {
    type slave;
    file "100.51.198.bak";
    masters { 198.51.100.2; };
};
```



### Avertissement

Le fonctionnement de la résolution inverse s'avère délicat lorsque l'on utilise des sous-réseaux. Dans le cas de ces travaux pratiques, il est essentiel que les déclarations de zones inverses soient identiques entre les différents niveaux.

Après rechargement de la configuration du service DNS sur le système hôte, les journaux système montrent que les transferts de zone se sont déroulés correctement.

```
# grep 'lab.lan-213.stri' /var/log/named/named.log
transfer of 'lab.lan-213.stri/IN/standard' from 198.51.100.2#53: \
  connected using 198.51.100.1#35001
createfetch: primary-srvr.lab.lan-213.stri A
createfetch: primary-srvr.lab.lan-213.stri AAAA
transfer of 'lab.lan-213.stri/IN/standard' from 198.51.100.2#53: \
  Transfer completed: 1 messages, 15 records, 400 bytes, 0.001 secs (400000 bytes/sec)
zone lab.lan-213.stri/IN/standard: sending notifies (serial 2012100801)

# grep '100.51.198' /var/log/named/named.log
transfer of '100.51.198.in-addr.arpa/IN/standard' from 198.51.100.2#53: \
  connected using 198.51.100.1#44547
transfer of '100.51.198.in-addr.arpa/IN/standard' from 198.51.100.2#53: \
  Transfer completed: 1 messages, 9 records, 296 bytes, 0.001 secs (296000 bytes/sec)
zone 100.51.198.in-addr.arpa/IN/standard: sending notifies (serial 2012100801)
```

On peut vérifier que les numéros de série des notifications correspondent bien aux enregistrements publiés au niveau inférieur.

## 8.2. Échange du niveau inférieur vers le niveau supérieur

Pour que les enregistrements déclarés dans les différentes zones de travaux pratiques soient visibles les uns des autres, il est nécessaire de faire appel à la notion de forwarder.

**Q26.** Est-ce que les enregistrements de l'arborescence factice sont accessibles depuis les serveurs du niveau `zone(i).lan-213.stri` ? Quelle requête faut-il utiliser pour accéder à ces enregistrements ?

Rechercher l'adresse IP correspondant au nom `cooper.lan-213.stri`.

**Q27.** Comment diriger toutes les requêtes du niveau `zone(i).lan-213.stri` vers le niveau `lan-213.stri` ?

Rechercher l'option `forwarder` dans le document [BIND 9 Administrator Reference Manual](#)<sup>11</sup>.

<sup>11</sup> <http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.html>

## 9. Sécurisation de premier niveau

L'objectif de cette section est de présenter les mécanismes de contrôle d'accès offerts par le service Berkeley Internet Name Domain à un niveau très modeste. On se contente ici de définir les adresses IP ou les réseaux qui sont autorisés à émettre des requêtes récursives sur le service DNS ainsi que les adresses IP ou les réseaux qui sont autorisés à émettre des requêtes de transfert de zone.

Les éléments de configuration présentés ci-après sont à appliquer sur tous les serveurs DNS quel que soit leur rôle.

On commence par la définition des listes de contrôle d'accès dans le fichier `/etc/bind/named.conf.options`. Ces listes permettent de définir des groupes d'adresses IP ou de réseaux. Ces groupes peuvent ensuite être réutilisés autant de fois que nécessaire au niveau global de la configuration du service ou bien dans les déclarations de zones.

Ici, on se limite à la définition de deux groupes.

- Le groupe `xfer` donne la liste des adresses IP à partir desquelles les opérations de transfert de zone sont possibles.
- Le groupe `trusted` donne la liste des réseaux de confiance qui sont habilités à utiliser le service.

Ces définitions se retrouvent au début du fichier de configuration global du service DNS.

```
# cat /etc/bind/named.conf.options
acl "xfer" {
    localhost;
    198.51.100.1;
    198.51.100.3;
    198.51.100.4;
};

acl "trusted" {
    localhost;
    198.51.100.0/27;
};

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        198.51.100.1;
    };

    auth-nxdomain no;      # conform to RFC1035
    listen-on-v6 { any; };

    allow-transfer {
        none;
    };

    allow-query {
        trusted;
    };

    allow-query-cache {
        trusted;
    };
};
```

C'est dans la section `options` que l'on trouve la première utilisation des listes de contrôle d'accès. Ce niveau est dit global puisqu'il est examiné avant les déclarations de zone qui sont effectuées dans le

fichier `/etc/bind/named.conf.local`. Dans l'exemple donné ci-dessus, les opérations de transfert sont interdites au niveau global et les requêtes récursives pour des enregistrements sur lesquels le serveur n'a pas autorité ne sont autorisées que pour les réseaux de confiance.

Il faut noter que la section `forwarders` a été décommentée et configurée avec l'adresse IP du serveur de niveau supérieur dans l'arborescence DNS. Cette configuration est nécessaire pour garantir la «continuité» de l'arborescence factice de travaux pratiques. Il faut que les communications inter zones soient effectives pour mettre en œuvre les autres services internet qui s'appuient sur la résolution des noms.

On retrouve les listes de contrôle d'accès dans le fichier de déclaration de zone.

```
# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//

zone "0.200.192.in-addr.arpa" {
    type master;
    file "198.51.100";

    allow-query {
        any;
    };

    allow-transfer {
        xfer;
    };
};

zone "stri.lab" {
    type master;
    file "stri.lab";

    allow-query {
        any;
    };

    allow-transfer {
        xfer;
    };
};

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

Les choix effectués ici reviennent à autoriser sans restriction les requêtes directes et inverses sur les enregistrements de la zone `stri.lab`. Les transferts sur les mêmes enregistrements ne sont autorisés que pour les serveurs dont les adresses IP figurent dans la liste `xfer`.

Comme dans les sections précédentes, ces options de configuration sont à valider avec la suite des tests utilisant les différents types de requêtes à l'aide de la commande **dig**. À titre d'exemple, voici ce que l'on peut lire dans les journaux système lors d'une requête de transfert de zone non autorisée.

```
named[1524]: client 198.51.100.4#58025: zone transfer 'stri.lab/AXFR/IN' denied
```

Pour être plus complète, la sécurisation de la configuration devrait utiliser la notion de vue interne et externe du service de résolution des noms. Ce niveau de configuration dépasse «quelque peu» le cadre de ces travaux pratiques d'introduction. Le contenu de cette section n'est qu'une première prise de contact avec les fonctionnalités de sécurité d'un serveur DNS.

## 10. Documents de référence

BIND 9 Administrator Reference Manual

**BIND 9 Administrator Reference Manual**<sup>12</sup> : documentation complète la plus récente sur la syntaxe de configuration du service DNS. Si le paquet `bind9-doc` est installé, ce manuel est placé dans le répertoire `/usr/share/doc/bind9-doc/arm/`.

<sup>12</sup> <http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.html>

Secure BIND Template

**Secure BIND Template**<sup>13</sup> : patrons de fichiers de configuration d'un service DNS.

root-servers.org

**root-servers.org**<sup>14</sup> : informations sur les serveurs racines du service de noms de domaines.

Administration système en réseau : architecture réseau

**Architecture réseau des travaux pratiques**<sup>15</sup> : présentation de l'infrastructure des travaux pratiques.

Configuration d'une interface de réseau local

**Configuration d'une interface de réseau local**<sup>16</sup> : tout sur la configuration des interfaces réseau ; notamment les explications sur les opérations «rituelles» de début de travaux pratiques.

---

<sup>13</sup> <http://www.cymru.com/Documents/secure-bind-template.html>

<sup>14</sup> <http://root-servers.org/>

<sup>15</sup> [http://www.inetdoc.net/travaux\\_pratiques/infra.tp/](http://www.inetdoc.net/travaux_pratiques/infra.tp/)

<sup>16</sup> [http://www.inetdoc.net/travaux\\_pratiques/config.interface.lan/](http://www.inetdoc.net/travaux_pratiques/config.interface.lan/)