Introduction au service DNS

Philippe Latu
philippe.latu(at)inetdoc.net

http://www.inetdoc.net

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. Meta-information

Ce document est écrit avec DocBook[1] XML sur un système Debian GNU/Linux[2]. Il est disponible en version imprimable au format PDF : `sysadm-net.dns.qa.pdf`[3].

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.

[1] http://www.docbook.org
[2] http://www.debian.org
[3] http://www.inetdoc.net/pdf/sysadm-net.dns.qa.pdf

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

2. Architecture type de travaux pratiques

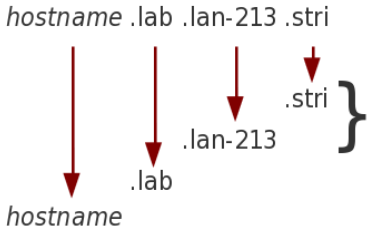
Comme indiqué dans le support Architecture réseau des travaux pratiques[4], on part d'une configuration type avec deux de postes de travail qui partagent le même domaine de diffusion. Le schéma d'une maquette utilisant deux instances de machines virtuelles et un système hôte est le suivant :

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 corresopondant aux affectations données ci-dessus ?

À partir des information du document Architecture réseau des travaux pratiques[5], compléter la chaîne des serveurs DNS permettant la résolution des noms de domaines jusqu'à la racine.



Serveur primaire	Serveur secondaire
casper	cooper
casper	cooper
primary-srvr	secondary-srvr

Dans la suite de ce document, on utilise le nom de domaine `lab.lan-213.stri` auquel correspond le réseau `198.51.100.0/24`.

Les affectations d'adresses IP sont :

- `primary-srvr.lab.lan-213.stri` : `198.51.100.2`
- `secondary-srvr.lab.lan-213.stri` : `198.51.100.3`

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).

[4] http://www.inetdoc.net/travaux_pratiques/infra.tp/
[5] http://www.inetdoc.net/travaux_pratiques/infra.tp/

On oriente la recherche dans la base de données des paquets de la distribution vers la chaîne de caractères qui débute par `bind`.

```
# aptitude search ^bind
p   bind9      - Serveur de noms de domaines internet
p   bind9-doc  - documentation de BIND
i   bind9-host - Version de « host » intégrée avec BIND 9.X
p   bind9utils - Utilitaires pour BIND
p   bindfs     - mirrors or overlays a local directory with altered permissions
p   bindgraph  - DNS statistics RRDtool frontend for BIND9
```

Les paquets à installer à partir de la liste ci-dessus sont : `bind9` et `bind9-doc`. Une fois l'opération **`# aptitude install bind9 bind9-doc`** effectuée, on vérifie le résultat.

```
# aptitude search ~ibind9
i   bind9       - Serveur de noms de domaines internet
i   bind9-doc   - documentation de BIND
i   bind9-host  - Version de « host » intégrée avec BIND 9.X
i A bind9utils  - Utilitaires pour BIND
i A libbind9-80 - Bibliothèque partagée BIND9 utilisée par BIND
```

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.

La «singularité» du service DNS provient du nom du processus exécuté : `named`.

Liste des processus actifs

```
# ps aux | grep na[m]ed
bind      2863  0.0  1.2 170168 13224 ?        Ssl  21:05   0:00 /usr/sbin/named -u bind
```

Ports réseau ouverts

En utilisant la commande **lsof**, on obtient la liste ports ouverts en fonction du processus.

```
# lsof -i | grep na[m]ed
named   2863        bind   20u  IPv6   6733      0t0  TCP *:domain (LISTEN)
named   2863        bind   21u  IPv4   6738      0t0  TCP localhost:domain (LISTEN)
named   2863        bind   22u  IPv4   6740      0t0  TCP 198.51.100.2:domain (LISTEN)
named   2863        bind   23u  IPv4   6743      0t0  TCP localhost:953 (LISTEN)
named   2863        bind   24u  IPv6   6744      0t0  TCP localhost:953 (LISTEN)
named   2863        bind  512u  IPv6   6732      0t0  UDP *:domain
named   2863        bind  513u  IPv4   6737      0t0  UDP localhost:domain
named   2863        bind  514u  IPv4   6739      0t0  UDP 198.51.100.2:domain
```

En utilisant la commande **netstat**, on obtient les mêmes informations en partant des ports réseau ouverts.

```
# netstat -autp | grep na[m]ed
tcp   0      0 198.51.100.2:domain     *:*         LISTEN      2863/named
tcp   0      0 localhost:domain        *:*         LISTEN      2863/named
tcp   0      0 localhost:953           *:*         LISTEN      2863/named
tcp6  0      0 [::]:domain             [::]:*      LISTEN      2863/named
tcp6  0      0 localhost:953           [::]:*      LISTEN      2863/named
udp   0      0 198.51.100.2:domain     *:*                     2863/named
udp   0      0 localhost:domain        *:*                     2863/named
udp6  0      0 [::]:domain             [::]:*                  2863/named
```

Journaux systèmes

```
# grep na[m]ed /var/log/syslog
named[2863]: starting BIND 9.8.1-P1 -u bind
named[2863]: built with '--prefix=/usr' '--mandir=/usr/share/man'
'--infodir=/usr/share/info' '--sysconfdir=/etc/bind' '--localstatedir=/var'
'--enable-threads' '--enable-largefile' '--with-libtool' '--enable-shared'
'--enable-static' '--with-openssl=/usr' '--with-gssapi=/usr' '--with-gnu-ld'
'--with-geoip=/usr' '--enable-ipv6' 'CFLAGS=-fno-strict-aliasing -DDIG_SIGCHASE
-O2'
named[2863]: adjusted limit on open files from 4096 to 1048576
named[2863]: found 2 CPUs, using 2 worker threads
named[2863]: using up to 4096 sockets
named[2863]: loading configuration from '/etc/bind/named.conf'
named[2863]: reading built-in trusted keys from file '/etc/bind/bind.keys'
named[2863]: using default UDP/IPv4 port range: [1024, 65535]
named[2863]: using default UDP/IPv6 port range: [1024, 65535]
named[2863]: listening on IPv6 interfaces, port 53
named[2863]: listening on IPv4 interface lo, 127.0.0.1#53
named[2863]: listening on IPv4 interface eth0, 198.51.100.2#53
named[2863]: generating session key for dynamic DNS
named[2863]: sizing zone task pool based on 5 zones
named[2863]: using built-in root key for view _default
named[2863]: set up managed keys zone for view _default, file 'managed-keys.bind'
named[2863]: Warning: 'empty-zones-enable/disable-empty-zone' not set: disabling RFC 1918 empt
named[2863]: automatic empty zone: 254.169.IN-ADDR.ARPA
named[2863]: automatic empty zone: 2.0.192.IN-ADDR.ARPA
named[2863]: automatic empty zone: 100.51.198.IN-ADDR.ARPA
named[2863]: automatic empty zone: 113.0.203.IN-ADDR.ARPA
named[2863]: automatic empty zone: 255.255.255.255.IN-ADDR.ARPA
named[2863]: automatic empty zone: 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
named[2863]: automatic empty zone: 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0
named[2863]: automatic empty zone: D.F.IP6.ARPA
named[2863]: automatic empty zone: 8.E.F.IP6.ARPA
named[2863]: automatic empty zone: 9.E.F.IP6.ARPA
named[2863]: automatic empty zone: A.E.F.IP6.ARPA
named[2863]: automatic empty zone: B.E.F.IP6.ARPA
named[2863]: automatic empty zone: 8.B.D.0.1.0.0.2.IP6.ARPA
named[2863]: command channel listening on 127.0.0.1#953
named[2863]: command channel listening on ::1#953
named[2863]: zone 0.in-addr.arpa/IN: loaded serial 1
named[2863]: zone 127.in-addr.arpa/IN: loaded serial 1
named[2863]: zone 255.in-addr.arpa/IN: loaded serial 1
named[2863]: zone localhost/IN: loaded serial 2
named[2863]: managed-keys-zone ./IN: loading from master file managed-keys.bind failed: file n
named[2863]: managed-keys-zone ./IN: loaded serial 0
named[2863]: running
```

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.

Comme pour tout service implanté sur un système GNU/Linux, les fichiers de configuration sont placés dans le répertoire `/etc/`.

```
# dpkg -L bind9 |grep etc
/etc
/etc/bind
/etc/bind/named.conf.default-zones
/etc/bind/named.conf
/etc/bind/db.empty
/etc/bind/db.255
/etc/bind/db.127
/etc/bind/db.local
/etc/bind/db.root
/etc/bind/db.0
/etc/bind/named.conf.local
/etc/bind/zones.rfc1918
/etc/bind/bind.keys
/etc/init.d
/etc/init.d/bind9
/etc/ppp
/etc/ppp/ip-down.d
/etc/ppp/ip-down.d/bind9
/etc/ppp/ip-up.d
/etc/ppp/ip-up.d/bind9
/etc/apparmor.d
/etc/apparmor.d/force-complain
/etc/apparmor.d/usr.sbin.named
/etc/apparmor.d/local
/etc/apparmor.d/local/usr.sbin.named
/etc/network
/etc/network/if-down.d
/etc/network/if-down.d/bind9
/etc/network/if-up.d
/etc/network/if-up.d/bind9
/etc/ufw
/etc/ufw/applications.d
/etc/ufw/applications.d/bind9
```

De la même façon, les données du service doivent être placées dans le répertoire `/var/`.

```
# dpkg -L bind9 |grep var
/var
/var/cache
/var/cache/bind
/var/run
```

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[6].

C'est dans le répertoire `/var/cache/bind/` que l'on place les fichiers contenant les enregistrements ou Resource Records (RRs). Ces enregistrements correspondent aux zones sur lesquelles le serveur a autorité. Ce choix de répertoire fait partie des options du service. Voir l'option `directory` dans le fichier `/etc/bind/named.conf.options`.

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

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

Consulter la section relative au service de type cache-only dans le document BIND 9 Administrator Reference Manual[7].

- La configuration livrée avec le paquet ne contient aucune déclaration de zone spécifique. Le fichier `/etc/bind/named.conf.local` ne contient que des commentaires.
- Le répertoire `/var/cache/bind/` est vide.

[6] http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.html
[7] http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.html

- Le service peut contacter les serveurs racine. La liste de ces serveurs est donnée dans le fichier `db.root`.
- Le service étant actif, il peut prendre en charge les requêtes et mémoriser dans son cache les résultats.

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.

C'est le fichier `/etc/resolv.conf` qui sert à configurer la partie cliente du service de résolution des noms de domaines ; le resolver. Dans le cas des postes de travaux pratiques, la configuration initiale du resolver est prise en charge par le service DHCP.

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`.

Il est possible de créer un nouveau fichier simplement en désignant l'interface de boucle locale.

```
# echo nameserver 127.0.0.1 >/etc/resolv.conf
```

Vu du système sur lequel le service est exécuté, on optimise le traitement des requêtes en alimentant puis en utilisant le cache mémoire. Vu de l'Internet, on sollicite directement les serveurs racines à chaque nouvelle requête.

Q9. À quel paquet appartient la commande **dig** ? Quelle est sa fonction ?

Utiliser le gestionnaire de paquets local **dpkg**.

La commande **dig** est le «couteau suisse» qui va permettre d'effectuer tous les tests de requêtes DNS. On obtient le nom du paquet auquel elle appartient à partir d'une recherche du type :

```
# dpkg -S `which dig`
dnsutils: /usr/bin/dig
```

Le paquet `dsnutils` fait partie de l'installation de base. Il est donc présent sur tous les systèmes.

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.

L'utilisation du cache du serveur DNS est identifiable à partir du temps de traitement d'une requête. Ce temps de traitement apparaît dans le champ `Query time` des résultats affichés à la suite d'un appel à la commande **dig**.

Dans les deux exemples ci-dessous, le serveur interrogé est bien le service local avec l'adresse IP `127.0.0.1`. La première requête a un temps de traitement de 1301ms tandis que la seconde a un temps de traitement de 0ms. Cette seconde réponse est fournie par le cache du serveur DNS.

```
# dig www.iana.org

; <<>> DiG 9.8.1-P1 <<>> www.iana.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61419
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 4

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

;; ANSWER SECTION:
www.iana.org.           600     IN      CNAME   ianawww.vip.icann.org.
ianawww.vip.icann.org.  30      IN      A       192.0.32.8

;; AUTHORITY SECTION:
vip.icann.org.          3600    IN      NS      gtm1.lax.icann.org.
vip.icann.org.          3600    IN      NS      gtm1.dc.icann.org.

;; ADDITIONAL SECTION:
gtm1.dc.icann.org.      21600   IN      A       192.0.47.252
gtm1.dc.icann.org.      21600   IN      AAAA    2620:0:2830:296::252
gtm1.lax.icann.org.     21600   IN      A       192.0.32.252
gtm1.lax.icann.org.     21600   IN      AAAA    2620:0:2d0:296::252

;; Query time: 1301 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Oct  8 00:28:32 2012
;; MSG SIZE  rcvd: 211
```

```
# dig www.iana.org

; <<>> DiG 9.8.1-P1 <<>> www.iana.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61419
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 4

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

;; ANSWER SECTION:
www.iana.org.           600     IN      CNAME   ianawww.vip.icann.org.
ianawww.vip.icann.org.  30      IN      A       192.0.32.8

;; AUTHORITY SECTION:
vip.icann.org.          3600    IN      NS      gtm1.lax.icann.org.
vip.icann.org.          3600    IN      NS      gtm1.dc.icann.org.

;; ADDITIONAL SECTION:
gtm1.dc.icann.org.      21600   IN      A       192.0.47.252
gtm1.dc.icann.org.      21600   IN      AAAA    2620:0:2830:296::252
gtm1.lax.icann.org.     21600   IN      A       192.0.32.252
gtm1.lax.icann.org.     21600   IN      AAAA    2620:0:2d0:296::252

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Oct  8 00:28:40 2012
;; MSG SIZE  rcvd: 211
```

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.

Les réponses aux requêtes suivantes apparaissent après la mention `ANSWER SECTION:`.

Requête sur un serveur de noms, NS

```
$ dig ns iana.org

; <<>> DiG 9.8.1-P1 <<>> ns iana.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25044
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;iana.org.                      IN      NS

;; ANSWER SECTION:
iana.org.               86400   IN      NS      d.iana-servers.net.
iana.org.               86400   IN      NS      ns.icann.org.
iana.org.               86400   IN      NS      c.iana-servers.net.
iana.org.               86400   IN      NS      a.iana-servers.net.
iana.org.               86400   IN      NS      b.iana-servers.net.

;; Query time: 313 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Oct  7 22:41:52 2012
;; MSG SIZE  rcvd: 129
```

Requête sur un nom d'hôte, A

```
$ dig a iana.org

; <<>> DiG 9.8.1-P1 <<>> a iana.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56033
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0

;; QUESTION SECTION:
;iana.org.                      IN      A

;; ANSWER SECTION:
iana.org.               600     IN      A       192.0.43.8

;; AUTHORITY SECTION:
iana.org.               86293   IN      NS      a.iana-servers.net.
iana.org.               86293   IN      NS      ns.icann.org.
iana.org.               86293   IN      NS      c.iana-servers.net.
iana.org.               86293   IN      NS      b.iana-servers.net.
iana.org.               86293   IN      NS      d.iana-servers.net.

;; Query time: 190 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Oct  7 22:43:39 2012
;; MSG SIZE  rcvd: 145
```

Requête sur une adresse IP, PTR

```
$ dig -x 192.0.32.9

; <<>> DiG 9.8.1-P1 <<>> -x 192.0.32.9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16786
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0

;; QUESTION SECTION:
;9.32.0.192.in-addr.arpa.       IN      PTR

;; ANSWER SECTION:
9.32.0.192.in-addr.arpa. 21600  IN      PTR     www.internic.net.

;; AUTHORITY SECTION:
32.0.192.in-addr.arpa.  86400   IN      NS      b.iana-servers.net.
32.0.192.in-addr.arpa.  86400   IN      NS      a.iana-servers.net.
32.0.192.in-addr.arpa.  86400   IN      NS      c.iana-servers.net.
32.0.192.in-addr.arpa.  86400   IN      NS      ns.icann.org.
32.0.192.in-addr.arpa.  86400   IN      NS      d.iana-servers.net.

;; Query time: 426 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Oct  7 22:46:44 2012
;; MSG SIZE  rcvd: 174
```

Requête sur un agent de transfert de courrier électronique, MX

```
$ dig mx internic.net

; <<>> DiG 9.8.1-P1 <<>> mx internic.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45729
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;internic.net.                  IN      MX

;; ANSWER SECTION:
internic.net.           600     IN      MX      10 pechorax.dc.icann.org.
internic.net.           600     IN      MX      10 pechorax.lax.icann.org.

;; Query time: 112 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sun Oct  7 22:48:27 2012
;; MSG SIZE  rcvd: 96
```

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.

Pour émettre une requête itérative (ou non récursive), il faut utiliser l'option `+trace`.

```
$ dig +trace ns iana.org

; <<>> DiG 9.8.1-P1 <<>> +trace ns iana.org
;; global options: +cmd
.                       511837  IN      NS      i.root-servers.net.
.                       511837  IN      NS      j.root-servers.net.
.                       511837  IN      NS      c.root-servers.net.
.                       511837  IN      NS      h.root-servers.net.
.                       511837  IN      NS      a.root-servers.net.
.                       511837  IN      NS      l.root-servers.net.
.                       511837  IN      NS      d.root-servers.net.
.                       511837  IN      NS      e.root-servers.net.
.                       511837  IN      NS      g.root-servers.net.
.                       511837  IN      NS      m.root-servers.net.
.                       511837  IN      NS      f.root-servers.net.
.                       511837  IN      NS      b.root-servers.net.
.                       511837  IN      NS      k.root-servers.net.
;; Received 512 bytes from 127.0.0.1#53(127.0.0.1) in 8 ms

org.                    172800  IN      NS      a0.org.afilias-nst.info.
org.                    172800  IN      NS      c0.org.afilias-nst.info.
org.                    172800  IN      NS      d0.org.afilias-nst.org.
org.                    172800  IN      NS      b2.org.afilias-nst.org.
org.                    172800  IN      NS      b0.org.afilias-nst.org.
org.                    172800  IN      NS      a2.org.afilias-nst.info.
;; Received 428 bytes from 128.8.10.90#53(128.8.10.90) in 1705 ms

iana.org.               86400   IN      NS      a.iana-servers.net.
iana.org.               86400   IN      NS      b.iana-servers.net.
iana.org.               86400   IN      NS      c.iana-servers.net.
iana.org.               86400   IN      NS      d.iana-servers.net.
iana.org.               86400   IN      NS      ns.icann.org.
;; Received 173 bytes from 2001:500:48::1#53(2001:500:48::1) in 1101 ms

iana.org.               86400   IN      NS      c.iana-servers.net.
iana.org.               86400   IN      NS      a.iana-servers.net.
iana.org.               86400   IN      NS      d.iana-servers.net.
iana.org.               86400   IN      NS      b.iana-servers.net.
iana.org.               86400   IN      NS      ns.icann.org.
;; Received 129 bytes from 199.43.132.53#53(199.43.132.53) in 18 ms
```

Note

Après tous ces exemples de requêtes, on voit clairement que le fonctionnement par défaut du logiciel BIND est récursif. Cette prise en charge «ouverte» des requêtes peut poser quelques soucis de sécurité. Si il est légitime de prendre complètement en charge les interrogations DNS émises par les hôtes du réseau administré de façon à alimenter le cache et optimiser le fonctionnement du service, il n'en va pas de même pour les hôtes du réseau public. Il est donc important de configurer le service en conséquence. Les contrôles d'accès qui permettent de ne satisfaire que les requêtes émises par les hôtes appartenant aux «réseaux de confiance» sont présentées dans la Section 9, « Sécurisation de premier niveau ».

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.

Tous les exemples de requêtes donnés ci-avant utilisent la classe Internet (IN) de façon implicite. Pour interroger un type de la classe CHAOS, il est nécessaire d'indiquer cette classe dans la commande d'interrogation du service DNS. Voici deux exemples de requêtes sur les deux types les plus souvent recherchés : la version du logiciel et la liste de ses auteurs.

```
$ dig @localhost. version.bind txt chaos +novc

; <<>> DiG 9.8.1-P1 <<>> @localhost. version.bind txt chaos +novc
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39711
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.8.1-P1"

;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Sun Oct  7 23:01:44 2012
;; MSG SIZE  rcvd: 65
```

```
$ dig @localhost. authors.bind txt chaos +novc

; <<>> DiG 9.8.1-P1 <<>> @localhost. authors.bind txt chaos +novc
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36899
;; flags: qr aa rd; QUERY: 1, ANSWER: 15, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;authors.bind.                  CH      TXT

;; ANSWER SECTION:
authors.bind.           0       CH      TXT     "Matt Nelson"
authors.bind.           0       CH      TXT     "Jeremy C. Reed"
authors.bind.           0       CH      TXT     "Michael Sawyer"
authors.bind.           0       CH      TXT     "Brian Wellington"
authors.bind.           0       CH      TXT     "Mark Andrews"
authors.bind.           0       CH      TXT     "James Brister"
authors.bind.           0       CH      TXT     "Ben Cottrell"
authors.bind.           0       CH      TXT     "Michael Graff"
authors.bind.           0       CH      TXT     "Andreas Gustafsson"
authors.bind.           0       CH      TXT     "Bob Halley"
authors.bind.           0       CH      TXT     "Evan Hunt"
authors.bind.           0       CH      TXT     "JINMEI Tatuya"
authors.bind.           0       CH      TXT     "David Lawrence"
authors.bind.           0       CH      TXT     "Danny Mayer"
authors.bind.           0       CH      TXT     "Damien Neil"

;; AUTHORITY SECTION:
authors.bind.           0       CH      NS      authors.bind.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Sun Oct  7 23:03:43 2012
;; MSG SIZE  rcvd: 430
```

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.

- 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, « Sécurisation 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[8]. 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.

[8] 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.

Le fichier `/etc/bind/named.conf.local` du nouveau serveur DNS doit être édité de façon à faire apparaître les zones directes et inverses sur lesquelles il a autorité. Une fois l'opération effectuée, on recharge la configuration du serveur et on consulte les journaux système. Voici une copie du fichier correspondant à la zone `lab.lan-213.stri`.

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

zone "lab.lan-213.stri" {
        type master;
        file "lab.lan-213.stri";
        };

zone "100.51.198.in-addr.arpa" {
        type master;
        file "100.51.198";
        };

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

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.

- C'est le fichier `named.conf.options` qui désigne le répertoire de travail du service de noms de domaines : `/var/cache/bind/`.

- On retrouve la même information au niveau des paramètres du compte utilisateur système dédié au service.

  ```
  $ grep bind /etc/passwd
  bind:x:105:107::/var/cache/bind:/bin/false
  ```

- Le masque de permissions donne les droits d'écriture aux membres du groupe système `bind`.

  ```
  $ ll /var/cache/ | grep bind
  drwxrwxr-x  2 root bind 4,0K oct.   7 21:05 bind
  ```

Q16. À l'aide de l'exemple donné dans le document DNS HOWTO : A real domain example[9], 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.

En respectant les options de configuration du paquet Debian, on créé le fichier `lab.lan-213.stri` dans le répertoire `/var/cache/bind/`.

```
# cat /var/cache/bind/lab.lan-213.stri
$TTL 60
@       IN      SOA     lab.lan-213.stri. postmaster.lab.lan-213.stri. (
                        2012100801      ; serial, yearmonthdayserial#
                        20              ; refresh, seconds
                        5               ; retry, seconds
                        420             ; expire, seconds
                        60 )            ; minimum, seconds
                        NS      primary-srvr.lab.lan-213.stri.
                        NS      secondary-srvr.lab.lan-213.stri.
                        MX      10 smtp.lab.lan-213.stri.  ; Primary Mail Exchanger
                        TXT     "DNS training Lab"

rtr             A       198.51.100.1
primary-srvr    A       198.51.100.2
ns1             CNAME   primary-srvr.lab.lan-213.stri.
secondary-srvr  A       198.51.100.3
ns2             CNAME   secondary.lab.lan-213.stri.
file-srvr       A       198.51.100.5
nfs             CNAME   file-srvr.lab.lan-213.stri.
ldap            CNAME   file-srvr.lab.lan-213.stri.
smtp            A       198.51.100.10
```

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

Les enregistrements (RRs) utilisés pour la résolution inverse des adresses IP doivent correspondre exactement aux décarations de la zone directe.

[9] http://www.tldp.org/HOWTO/DNS-HOWTO-7.html
[10] http://www.tldp.org/HOWTO/DNS-HOWTO-7.html

```
# cat /var/cache/bind/100.51.198
$TTL 60
@       IN      SOA     lab.lan-213.stri. postmaster.lab.lan-213.stri. (
                        2012100801      ; serial, yearmonthdayserial#
                        20              ; refresh, seconds
                        5               ; retry, seconds
                        420             ; expire, seconds
                        60 )            ; minimum, seconds
                        NS      primary-srvr.lab.lan-213.stri.
                        NS      secondary-srvr.lab.lan-213.stri.

1               PTR     rtr.lab.lan-213.stri.
2               PTR     primary-srvr.lab.lan-213.stri.
3               PTR     secondary-srvr.lab.lan-213.stri.
;
5               PTR     file-srvr.lab.lan-213.stri.
10              PTR     smtp.lab.lan-213.stri.
```

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.

Le paquet `bind9utils` fournit plusieurs outils dont le programme named-checkzone qui permet de valider la syntaxe des fichiers de déclaration de zone.

Dans le cas des deux exemples ci-dessus, on obtient les résultats suivants.

```
# named-checkzone lab.lan-213.stri. /var/cache/bind/lab.lan-213.stri
zone lab.lan-213.stri/IN: loaded serial 2012100801
OK
```

```
# named-checkzone  100.51.198.in-addr.arpa. /var/cache/bind/100.51.198
zone 100.51.198.in-addr.arpa/IN: loaded serial 2012100801
OK
```

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

Le rechargement de la configuration du service ne se distingue pas des autres services Internet.

```
# service bind9 reload
[ ok ] Reloading domain name service...: bind9.
```

Voici un extrait de journal système.

```
# tail -100 /var/log/syslog
named[2863]: received control channel command 'reload'
named[2863]: loading configuration from '/etc/bind/named.conf'
named[2863]: reading built-in trusted keys from file '/etc/bind/bind.keys'
named[2863]: using default UDP/IPv4 port range: [1024, 65535]
named[2863]: using default UDP/IPv6 port range: [1024, 65535]
named[2863]: sizing zone task pool based on 7 zones
named[2863]: using built-in root key for view _default
named[2863]: Warning: 'empty-zones-enable/disable-empty-zone' not set: disabling RFC 1918 empty z
named[2863]: reloading configuration succeeded
named[2863]: reloading zones succeeded
named[2863]: zone 100.51.198.in-addr.arpa/IN: zone serial (2012100801) unchanged. zone may fail t
named[2863]: zone 100.51.198.in-addr.arpa/IN: loaded serial 2012100801
named[2863]: zone 100.51.198.in-addr.arpa/IN: sending notifies (serial 2012100801)
named[2863]: zone lab.lan-213.stri/IN: zone serial (2012100801) unchanged. zone may fail to trans
named[2863]: zone lab.lan-213.stri/IN: loaded serial 2012100801
named[2863]: zone lab.lan-213.stri/IN: sending notifies (serial 2012100801)
```

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

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.

Le fichier `/etc/bind/named.conf.local` du serveur DNS secondaire doit être édité. Bien sûr, les noms de zone doivent correspondre à ceux du serveur primaire. Voici une copie de la configuration globale du service.

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

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

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

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

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.

- C'est le fichier `named.conf.options` qui désigne le répertoire de travail du service de noms de domaines : `/var/cache/bind/`.

- On retrouve la même information au niveau des paramètres du compte utilisateur système dédié au service.

```
$ grep bind /etc/passwd
bind:x:105:107::/var/cache/bind:/bin/false
```

- Le masque de permissions donne les droits d'écriture aux membres du groupe système `bind`.

```
$ ll /var/cache/ | grep bind
drwxrwxr-x  2 root bind 4,0K oct.   7 21:05 bind
```

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.

Le paquet `bind9utils` fournit plusieurs outils dont le programme named-checkconf qui permet de valider la syntaxe des fichiers de configuration.

Dans le cas de notre exemple, on obtient les résultats suivants.

```
# named-checkconf -p /etc/bind/named.conf
options {
        directory "/var/cache/bind";
        listen-on-v6 {
                "any";
        };
        auth-nxdomain no;
        dnssec-validation auto;
};
zone "lab.lan-213.stri." {
        type slave;
        file "backup.lab.lan-213.stri";
        masters {
                198.51.100.2 ;
        };
};
zone "100.51.198.in-addr.arpa" {
        type slave;
        file "backup.100.51.198";
        masters {
                198.51.100.2 ;
        };
};
zone "." {
        type hint;
        file "/etc/bind/db.root";
};
zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

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**.

Les enregistrements d'un serveur secondaire sont obtenus par transfert réseau.

Le type d'une requête de transfert de zone est : AXFR. Voici deux exemples de résultats.

```
# dig axfr @198.51.100.2 lab.lan-213.stri

; <<>> DiG 9.8.1-P1 <<>> axfr @198.51.100.2 lab.lan-213.stri
; (1 server found)
;; global options: +cmd
lab.lan-213.stri.       60      IN      SOA     lab.lan-213.stri. postmaster.lab.lan-213.stri. 20
lab.lan-213.stri.       60      IN      NS      primary-srvr.lab.lan-213.stri.
lab.lan-213.stri.       60      IN      NS      secondary-srvr.lab.lan-213.stri.
lab.lan-213.stri.       60      IN      MX      10 smtp.lab.lan-213.stri.
lab.lan-213.stri.       60      IN      TXT     "DNS training Lab"
file-srvr.lab.lan-213.stri. 60  IN      A       198.51.100.5
ldap.lab.lan-213.stri.  60      IN      CNAME   file-srvr.lab.lan-213.stri.
nfs.lab.lan-213.stri.   60      IN      CNAME   file-srvr.lab.lan-213.stri.
ns1.lab.lan-213.stri.   60      IN      CNAME   primary-srvr.lab.lan-213.stri.
ns2.lab.lan-213.stri.   60      IN      CNAME   secondary.lab.lan-213.stri.
primary-srvr.lab.lan-213.stri. 60 IN    A       198.51.100.2
rtr.lab.lan-213.stri.   60      IN      A       198.51.100.1
secondary-srvr.lab.lan-213.stri. 60 IN  A       198.51.100.3
smtp.lab.lan-213.stri.  60      IN      A       198.51.100.10
lab.lan-213.stri.       60      IN      SOA     lab.lan-213.stri. postmaster.lab.lan-213.stri. 20
;; Query time: 1 msec
;; SERVER: 198.51.100.2#53(198.51.100.2)
;; WHEN: Mon Oct  8 17:20:52 2012
;; XFR size: 15 records (messages 1, bytes 400)
```

```
# dig axfr @198.51.100.2 100.51.198.in-addr.arpa.

; <<>> DiG 9.8.1-P1 <<>> axfr @198.51.100.2 100.51.198.in-addr.arpa.
; (1 server found)
;; global options: +cmd
100.51.198.in-addr.arpa. 60     IN      SOA     lab.lan-213.stri. postmaster.lab.lan-213.stri. 20
100.51.198.in-addr.arpa. 60     IN      NS      primary-srvr.lab.lan-213.stri.
100.51.198.in-addr.arpa. 60     IN      NS      secondary-srvr.lab.lan-213.stri.
1.100.51.198.in-addr.arpa. 60   IN      PTR     rtr.lab.lan-213.stri.
10.100.51.198.in-addr.arpa. 60  IN      PTR     smtp.lab.lan-213.stri.
2.100.51.198.in-addr.arpa. 60   IN      PTR     primary-srvr.lab.lan-213.stri.
3.100.51.198.in-addr.arpa. 60   IN      PTR     secondary-srvr.lab.lan-213.stri.
5.100.51.198.in-addr.arpa. 60   IN      PTR     file-srvr.lab.lan-213.stri.
100.51.198.in-addr.arpa. 60     IN      SOA     lab.lan-213.stri. postmaster.lab.lan-213.stri. 20
;; Query time: 1 msec
;; SERVER: 198.51.100.2#53(198.51.100.2)
;; WHEN: Mon Oct  8 17:22:34 2012
;; XFR size: 9 records (messages 1, bytes 296)
```

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

Le rechargement de la configuration du service ne se distingue pas des autres services Internet.

```
# service bind9 reload
[ ok ] Reloading domain name service...: bind9.
```

Voici un extrait de journal système.

```
# tail -100 /var/log/syslog
named[3188]: received control channel command 'reload'
named[3188]: loading configuration from '/etc/bind/named.conf'
named[3188]: reading built-in trusted keys from file '/etc/bind/bind.keys'
named[3188]: using default UDP/IPv4 port range: [1024, 65535]
named[3188]: using default UDP/IPv6 port range: [1024, 65535]
named[3188]: sizing zone task pool based on 7 zones
named[3188]: using built-in root key for view _default
named[3188]: Warning: 'empty-zones-enable/disable-empty-zone' not set: disabling RFC 1918 empty z
named[3188]: zone 100.51.198.IN-ADDR.ARPA/IN: (master) removed
named[3188]: reloading configuration succeeded
named[3188]: reloading zones succeeded
named[3188]: zone 100.51.198.in-addr.arpa/IN: Transfer started.
named[3188]: transfer of '100.51.198.in-addr.arpa/IN' from 198.51.100.2#53: connected using 198.5
named[3188]: zone 100.51.198.in-addr.arpa/IN: transferred serial 2012100801
named[3188]: transfer of '100.51.198.in-addr.arpa/IN' from 198.51.100.2#53: \
  Transfer completed: 1 messages, 9 records, 296 bytes, 0.001 secs (296000 bytes/sec)
named[3188]: zone 100.51.198.in-addr.arpa/IN: sending notifies (serial 2012100801)
named[3188]: zone lab.lan-213.stri/IN: Transfer started.
named[3188]: transfer of 'lab.lan-213.stri/IN' from 198.51.100.2#53: connected using 198.51.100.3
named[3188]: zone lab.lan-213.stri/IN: transferred serial 2012100801
named[3188]: transfer of 'lab.lan-213.stri/IN' from 198.51.100.2#53: \
  Transfer completed: 1 messages, 15 records, 400 bytes, 0.001 secs (400000 bytes/sec)
named[3188]: zone lab.lan-213.stri/IN: sending notifies (serial 2012100801)
```

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 suiavnts.

```
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`.

La requête directe n'aboutit pas puisque les serveurs racines n'ont aucune connaissance de l'arborescence factice.

```
# dig cooper.lan-213.stri

; <<>> DiG 9.8.1-P1 <<>> cooper.lan-213.stri
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 61354
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;cooper.lan-213.stri.           IN      A

;; AUTHORITY SECTION:
.                       10800   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 20121

;; Query time: 184 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Oct  8 23:02:29 2012
;; MSG SIZE  rcvd: 112
```

En interrogeant directement le niveau supérieur, on obtient l'information demandée.

```
# dig @198.51.100.1 cooper.lan-213.stri

; <<>> DiG 9.8.1-P1 <<>> @198.51.100.1 cooper.lan-213.stri
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2583
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;cooper.lan-213.stri.           IN      A

;; ANSWER SECTION:
cooper.lan-213.stri.    86400   IN      A       172.16.80.1

;; AUTHORITY SECTION:
lan-213.stri.           86400   IN      NS      cooper.lan-213.stri.
lan-213.stri.           86400   IN      NS      casper.infra.stri.

;; ADDITIONAL SECTION:
casper.infra.stri.      86400   IN      A       172.16.0.2

;; Query time: 1 msec
;; SERVER: 198.51.100.1#53(198.51.100.1)
;; WHEN: Mon Oct  8 23:08:06 2012
;; MSG SIZE  rcvd: 110
```

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[11].

On édite le fichier `/etc/bind/named.conf.options` de façon à compléter la section `forwarders`.

```
forwarders {
        198.51.100.1;
};
```

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.

[11] http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.html

```
# 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 décomentée 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[12] : 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/`.

Secure BIND Template
: Secure BIND Template[13] : patrons de fichiers de configuration d'un service DNS.

root-servers.org
: root-servers.org[14] : informations sur les serveurs racines du service de noms de domaines.

[12] http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.html
[13] http://www.cymru.com/Documents/secure-bind-template.html
[14] http://root-servers.org/

Administration système en réseau : architecture réseau
: Architecture réseau des travaux pratiques[15] : présentation de l'infrastructure des travaux pratiques.

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

[15] http://www.inetdoc.net/travaux_pratiques/infra.tp/
[16] http://www.inetdoc.net/travaux_pratiques/config.interface.lan/