

BIND9

Le service DNS (Domain Name System) est un service TCP ()/IP permettant la correspondance entre un nom de domaine qualifié (FQDN : Fully Qualified Domain Name) et une adresse IP, par exemple www.ubuntu-fr.org (<http://www.ubuntu-fr.org>) = 193.55.221.76. Ainsi, grâce à DNS (), il n'est pas nécessaire de se souvenir des adresses IP.

Un serveur qui héberge le service DNS () est appelé "serveur de noms". Ubuntu est livré par défaut avec BIND (Berkeley Internet Naming Daemon), le serveur DNS () le plus utilisé sur Internet.

Ce guide est destiné aux personnes désireuses d'apprendre comment configurer et maintenir un serveur DNS () BIND9.

1. Pré-requis

- Disposer des droits d'administration sur le serveur.
- Disposer d'un réseau local.
- Connaître les bases de TCP ()/IP.
- Éventuellement disposer d'une connexion à Internet configurée et activée, pour faire les tests.

2. Installation

BIND9 est disponible dans le dépôt principal. Aucun dépôt supplémentaire n'est nécessaire ;

Pour installer le serveur BIND9, il suffit d'installer le paquet **bind9** (<apt://bind9>).

Le paquet **dnsutils** (<apt://dnsutils>) (`sudo apt-get install dnsutils`) fournit des outils très pratiques pour tester et débugger le service DNS (). La documentation BIND9 peut également être trouvée dans le paquet **bind9-doc** (<apt://bind9-doc>) (`sudo apt-get install bind9-doc`).

3. Scénarios de configuration

BIND9 peut être utilisé de différentes façons, les plus fréquentes sont :

3.1 Serveur cache

Dans cette configuration, BIND9 va effectuer les requêtes DNS () et se rappeler de la réponse pour la prochaine requête. Cette méthode peut être utile pour une connexion internet lente. En mettant les réponses DNS () en cache, on diminue l'utilisation de la bande passante et (encore plus important) on réduit également le temps de latence.

3.2 Serveur primaire

Utilisé pour contenir les enregistrements DNS () d'un nom de domaine enregistré. Un ensemble d'enregistrements DNS () pour un nom de domaine est appelé une "zone". (Le nom de domaine peut être imaginaire si on est dans le cas d'un réseau local fermé)

3.3 Serveur secondaire

Un serveur secondaire est utilisé en complément à un serveur primaire, en servant de copie à la ou les zones configurées sur le serveur primaire. Les serveurs secondaires sont recommandés sur des gros réseaux. Ceux-ci assurent la disponibilité de la zone DNS (), même si le serveur primaire est hors ligne.

3.4 Serveurs hybrides

Un serveur BIND9 peut être configuré à la fois comme serveur cache et comme serveur primaire, comme serveur cache et serveur secondaire, ou même serveur cache, serveur primaire et secondaire. Il suffit de combiner les différentes configurations présentées dans les exemples.

3.5 Serveurs furtifs

Il existe deux autres configurations fréquentes pour un serveur DNS () : serveur furtif maître et serveur furtif esclave. Ils sont identiques aux serveurs maître et esclave, mais avec une organisation légèrement différente : ils ne sont visibles qu'à l'intérieur du domaine.

Par exemple, vous disposez de 3 serveurs DNS () : A, B et C.

A est un serveur maître, B et C sont des esclaves.

Si votre domaine est configuré pour utiliser A et B comme serveurs de noms, alors C est un serveur furtif esclave. Il fait toujours office de serveur esclave, mais il ne sera pas interrogé depuis Internet.

Si votre domaine est configuré pour utiliser B et C comme serveurs de noms, alors A est un serveur furtif maître. Tout édition de la zone ou ajout est fait sur A, mais les ordinateurs depuis Internet interrogeront seulement B et C.

Dans les deux cas, le serveur passif n'est pas interrogé depuis Internet. Il peut ainsi être réservé pour une utilisation locale.

3.6 Serveurs Récursifs / Non récursifs

Les serveurs BIND9 peuvent être récursifs, c'est-à-dire interroger tour à tour les serveurs DNS () nécessaires jusqu'à obtenir la réponse, et la transmettre à leur client.

Dans le cas contraire (par défaut), le serveur DNS () délègue la résolution du nom de domaine à un autre serveur DNS ().

Pour activer la récursivité, modifier **/etc/bind/named.conf.options**

```
allow-recursion { any; };
```

4. Enregistrements DNS

Il existe de nombreux types d'enregistrements DNS (), mais certains sont plus communs :

4.1 Enregistrement de type A (Address)

C'est le type le plus courant. Cet enregistrement fait correspondre une adresse IP à un nom de machine. Bien vu

```
www      IN      A      1.2.3.4
```

4.2 Enregistrement de type CNAME (Alias)

Utilisé pour créer un alias depuis un enregistrement de type A. Il est possible de créer un enregistrement de type CNAME qui pointe vers un autre enregistrement CNAME, mais cela double le nombre de requêtes qui seront faites au serveur de noms. Cette méthode est donc déconseillée.

```
mail      IN      CNAME  www
www      IN      A      1.2.3.4
```

4.3 Enregistrement MX (Mail Exchange)

Utilisé pour définir vers quel serveur de la zone un email à destination du domaine doit être envoyé, et avec quelle priorité. Cet enregistrement doit pointer vers un enregistrement de type A, et non un alias CNAME. Il peut y avoir plusieurs enregistrements MX s'il existe plusieurs serveurs de messagerie sur le domaine. Le plus petit nombre a la plus grande priorité.

```
;** ENREGISTREMENTS "MX"
@      IN      MX    10  mikvdw.ddns.net.
@      IN      MX    20  audevdw.ddns.net.
```

4.4 Enregistrement NS (Name Server)

Utilisé pour définir quels serveurs répondent pour cette zone. Cet enregistrement doit pointer vers un enregistrement de type A, non pas vers un enregistrement de type CNAME.

C'est ici que le serveur maître et les esclaves sont définis. Les serveurs furtifs sont intentionnellement omis.

```
      IN      NS      ns.ubuntu-fr.lan.
      [...]
ns      IN      A      1.2.3.4
```

5. Configuration

Les fichiers de configuration de BIND9 sont stockés sous :

```
/etc/bind/
```

La configuration principale de BIND9 est effectuée dans les fichiers suivants :

```
/etc/bind/named.conf
/etc/bind/named.conf.options
/etc/bind/named.conf.local
```

5.1 Configuration pour un seul ordinateur (PC Domestique)

Dans ce cas, BIND est configuré pour ne répondre qu'aux requêtes du PC sur lequel il est installé. Il se charge lui-même de la résolution de noms, sans passer par les serveurs DNS () de votre FAI ().



Cette configuration implique que vous chargez directement la résolution des noms de domaine. Vous ne profitez plus du cache DNS () de votre fournisseur d'accès, et vous sollicitez du coup plus les serveurs racines, mais vous ne serez pas soumis au filtrage (ou parfois au DNS () menteur) de votre

fournisseur d'accès.

- Afin de rendre BIND inaccessible depuis l'extérieur, éditer le fichier **"/etc/bind/named.conf.options"**, positionner les options "listen-on" sur **127.0.0.1** et "listen-on-v6" sur **::1** comme ceci :

```
listen-on { 127.0.0.1; };
listen-on-v6 { ::1; };
```

- Puis toujours dans ce même fichier, **commenter** l'option **"forwarders"**. Il suffit de mettre un **#** devant chaque ligne :

```
#/ forwarders {
#// 0.0.0.0;
#// };
```

- Pour que toutes les requêtes passent par BIND :

Si votre carte réseau est configurée pour utiliser **DHCP** (), décommenter la ligne 20 du fichier **"/etc/dhcp3/dhclient.conf"** :

```
prepend domain-name-servers 127.0.0.1;
```

Si, au contraire, elle est configurée avec une adresse IP statique, modifier le fichier **"/etc/resolv.conf"** afin que toutes les requêtes passent par BIND. Ce fichier doit donc contenir :

```
nameserver 127.0.0.1
```

Redémarrer bind :

```
sudo service bind9 restart
```

5.2 Configuration pour un serveur cache

Le serveur BIND9 est configuré par défaut en tant que serveur cache.

Il suffit simplement d'ajouter les serveurs DNS () de votre prestataire Internet.

Décommentez et éditez les lignes suivantes dans **/etc/bind/named.conf.options** :

```
[...]
forwarders {
    1.2.3.4;
    5.6.7.8;
};

[...]
```

(ou 1.2.3.4 et 5.6.7.8 sont les adresses IP des serveurs DNS () de votre prestataire Internet.

Redémarrez le démon BIND9 :

```
sudo service bind9 restart
```

5.2.1 Tests

Si le package **dnsutils** a été installé, il est possible de tester la nouvelle configuration en utilisant **dig** :

```
dig -x 127.0.0.1
```

Si tout fonctionne bien, vous devriez voir apparaître une sortie similaire à :

```
; <>> DiG 9.4.1-P1 <>> -x 127.0.0.1
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13427
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
[...]
;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Nov 26 23:22:53 2007
;; MSG SIZE  rcvd: 93
```

La commande **dig** peut aussi être utilisée pour interroger d'autres domaines, comme par exemple :

```
dig ubuntu-fr.org
```

Si vous "digitez" un même domaine plusieurs fois, vous devriez voir apparaître une énorme diminution du temps mis par la requête (Query time), entre la première et la deuxième requête. Ceci est possible parce que le serveur a déjà mis en cache la réponse de la requête.

5.3 Configuration Serveur Maître

BIND9 va être configuré comme serveur maître pour le domaine ubuntu-fr.lan. Remplacez simplement ubuntu-fr.lan par votre propre nom de domaine.

5.3.1 Fichier de zone

Pour ajouter une zone, et faire de BIND9 un serveur maître :

- Editer le fichier named.conf.local :

```
[...]
zone "ubuntu-fr.lan" IN {
    type master;
    file "/etc/bind/db/ubuntu-fr.lan";
};

[...]
```

- Utiliser le fichier d'une zone existante comme modèle :

```
sudo cp /etc/bind/db.local /etc/bind/db/ubuntu-fr.lan
```

- Editer le nouveau fichier pour la zone (/etc/bind/db/ubuntu-fr.lan),
- Changer localhost par le FQDN de votre serveur, en laissant le point "." supplémentaire à la fin.
- Changer 127.0.0.1 par l'adresse IP du serveur de nom et root.localhost par une adresse email valide, mais avec un point "." à la place de l'arobase "@". Laisser également le point à la fin.
- Créer un enregistrement de type hôte A pour le serveur de nom ns/ubuntu-fr.lan :

```
;
; BIND data file for local loopback interface
;

$TTL    604800
@       IN      SOA     ns.ubuntu-fr.lan admin.ubuntu-fr.lan (
                        1           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )     ; Negative Cache TTL
;
@       IN      NS      ns.ubuntu-fr.lan.
NS      IN      A       10.10.10.10
box    IN      A       192.168.1.10
```

Le numéro de série doit être incrémenté à chaque changement dans le fichier de zone. En cas de multiples changements, une seule incrémentation suffit.

 Il est fréquent d'utiliser la date d'édition de la zone comme numéro de série, au format américain. Exemple : 2010122710 = incrémentation 10 du 27 décembre 2010.

Il est maintenant possible d'ajouter des enregistrements DNS () à la suite de la zone .

Une fois les changements dans le fichier de zone effectués, il faut redémarrer BIND9 pour qu'ils prennent effet :

```
sudo service bind9 restart
```

5.3.2 Zone de recherche inversée

Maintenant que notre fichier de zone est configuré et que les adresses IP sont résolues, une zone de recherche inversée est requise. Une zone de recherche inversée permet DNS () de convertir une adresse en nom.

- Editer /etc/bind/named.conf.local et ajouter les lignes suivantes :

```
zone "1.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind/db.192";
};
```

 Remplacer 1.168.192 par les trois premiers octets (si vous êtes en classe C) de votre réseau dans l'ordre inversé. Remplacer également le nom du fichier de zone db.192 par le nom approprié.

- Créer maintenant le fichier db.192 depuis un fichier existant :

```
sudo cp /etc/bind/db.127 /etc/bind/db.192
```

- Editer le fichier /etc/bind/db.192 et changer comme nous l'avons fait précédemment le nom de domaine et l'adresse email :

```

;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.ubuntu-fr.lan admin.ubuntu-fr.lan (
                        2           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800      ; Negative Cache TTL
;
@       IN      NS      ns.ubuntu-fr.lan.
10      IN      PTR     ns.ubuntu-fr.lan.

```

Le numéro de série de la zone de recherche inversée nécessite d'être incrémenté à chaque changement. Pour chaque enregistrement A ajouté dans /etc/bind/db.ubuntu-fr.l il faut créer un enregistrement PTR dans /etc/bind/db.192.

Après avoir créé le fichier de la zone de recherche inversée, redémarrez BIND9 :

```
sudo service bind9 restart
```

5.3.3 Tests

Il doit maintenant être possible de faire un ping sur ubuntu-fr.lan et la requête doit être résolue :

```
ping ns.ubuntu-fr.lan
```

L'utilitaire named-checkzone (inclus dans le package BIND9) peut également être utilisé :

```
named-checkzone ubuntu-fr.lan /etc/bind/db.ubuntu-fr.lan
```

et

```
named-checkzone 1.168.192.in-addr.arpa /etc/bind/db.192
```

Utiliser cet utilitaire est un bon moyen de s'assurer de l'absence d'erreurs avant le redémarrage de bind.

Pour tester la recherche inversée, l'utilitaire dig peut être utilisé :

```
dig -x 192.168.1.10
```

Vous devriez voir en sortie console la résolution de 1.168.192.in-addr.arpa. par votre serveur de nom.

5.4 Configuration en serveur esclave

Maintenant qu'un serveur maître a été configuré, un serveur esclave peut être configuré pour assurer une disponibilité du domaine en cas de panne du serveur maître.

Dans un premier temps, le serveur maître doit être configuré pour permettre le transfert de zone. Ajoutez l'option *allow-transfer* dans les définitions des zones principales et inversées du fichier /etc/bind/named.conf.local :

```

[...]
zone "ubuntu-fr.lan" {
    type master;
    file "/etc/bind/db.ubuntu-fr.lan";
    allow-transfer { @ip_esclave; };
};

[...]
zone "1.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind/db.192";
    allow-transfer { @ip_esclave; };
};

[...]

```

 Remplacez @ip_esclave par l'adresse IP du serveur esclave.

Ensuite, sur le serveur esclave, installez le package BIND9, de la même manière que pour le serveur maître. Editez le fichier /etc/bind/named.conf.local, et ajoutez les lignes suivantes pour la zone principale et inversée :

```
[...]
zone "ubuntu-fr.lan" {
    type slave;
    file "/var/cache/bind/db/ubuntu-fr.lan";
    masters { @ip_maitre; };
};

[...]
zone "1.168.192.in-addr.arpa" {
    type slave;
    file "/var/cache/bind/db.192";
    masters { @ip_maitre; };
};

[...]
```

 Remplacez @ip_maitre par l'adresse IP du serveur maître. Le fichier de zone doit être dans /var/cache/bind/, car par défaut, AppArmor ne permet l'accès en écriture que dans ce répertoire (voir la configuration de AppArmor dans /etc/apparmor.d/usr.sbin.named).

Redémarrez le serveur, et dans /var/log/syslog, vous devriez voir apparaître des informations similaires :

```
syslog.5.gz:Dec 27 23:33:53 ubuntu named[5064]: zone ubuntu-fr.lan/IN: transferred serial 2010122701
syslog.5.gz:Dec 27 23:33:53 ubuntu named[5064]: transfer of 'ubuntu-fr.lan/IN' from 10.0.0.202#53: end of transfer
syslog.5.gz:Dec 27 23:33:53 ubuntu named[5064]: slave zone "1.168.192.in-addr.arpa" (IN) loaded (serial 2010122701)
```

 Une zone n'est transférée que si son numéro de série sur le serveur maître est supérieur à celui du serveur esclave

5.4.1 Tests

Vous pouvez tester le serveur esclave de la même façon que pour le serveur maître. Il est possible d'arrêter BIND9 sur le serveur maître et essayer de faire un ping sur ubuntu-fr.lan. depuis un poste configuré pour utiliser le serveur esclave comme le serveur maître pour sa résolution de nom. Si tout ce passe bien, le serveur esclave devrait résoudre ubuntu-fr.lan.

6. Chrooter BIND9

Configurer BIND9 pour être chrooté est une sécurité recommandée si AppArmor n'est pas installé. Dans un environnement chrooté, BIND9 n'a accès qu'aux fichiers et matériels dont il a besoin, et est incapable d'accéder à autre chose. AppArmor est installé par défaut dans les versions récentes d'Ubuntu. A moins d'avoir désactivé explicitement AppArmor, chrooter BIND9 n'est pas nécessaire. Si malgré tout, vous désirez continuer en désactivant AppArmor et en chrootant BIND9, vous trouverez les informations nécessaires sur cette page (EN) : Ubuntu Bind9 Howto (<https://help.ubuntu.com/community/BIND9ServerHowto#Chrooting%20BIND9>)

7. Logging

BIND9 dispose d'une large variété de configurations possibles pour le logging. Il existe deux options principales, l'option Channel configure où vont les logs, et l'option Category détermine ce qui doit être loggé.

Les options par défauts de logging sont :

```
logging {
    category default { default_syslog; default_debug; };
    category unmatched { null; };
};
```

Nous allons configurer BIND9 pour envoyer les messages de débogage relatifs aux requêtes DNS () dans un fichier séparé.

Apparmor est, au moins depuis lucid, installé par défaut. Ce logiciel de sécurité ne permettra pas à bind d'écrire son fichier de log où bon lui semble. On peut voir dans le fichier de configuration d' apparmor pour bind: **/etc/apparmor.d/usr.sbin.named** que bind a par défaut les droits d'écriture dans le répertoire **/var/log/named/**. Il peut donc être judicieux de l'utiliser.

7.1 Option Channel

Dans un premier temps, nous devons configurer un channel pour spécifier dans quel fichier les messages seront enregistrés. Editez le fichier /etc/bind/named.conf.local et ajoutez les lignes suivantes :

```
logging {
    channel query.log {
        file "/var/log/named/query.log";
        // Set the severity to dynamic to see all the debug messages.
        severity dynamic;
    };
};
```

7.2 Option Category

Nous configurons ensuite une catégorie pour envoyer toutes les requêtes DNS () dans le fichier de requêtes

```
logging {
    channel query.log {
        file "/var/log/named/query.log";
        // Set the severity to dynamic to see all the debug messages.
        severity debug 3;
    };
    category queries { query.log; };
};
```

 L'option debug peut être un niveau allant de 1 à 3. Si aucun niveau n'est spécifié, le niveau 1 est utilisé par défaut.

Depuis que le daemon tourne en tant qu'utilisateur bind, le fichier **/var/log/named/query.log** doit être créé et le propriétaire changé :

```
sudo mkdir /var/log/named/
sudo touch /var/log/named/query.log
sudo chown -R bind /var/log/named/
```

Redémarrez BIND9 pour que les changements prennent effet :

```
sudo service bind9 restart
```

Vous devriez voir le fichier **/var/log/named/query.log** se remplir avec les logs de BIND9. Ceci n'est qu'un simple exemple des options possibles de logging. Allez voir le manuel sur le site bind9.net (<http://bind9.net>) pour plus d'informations.

8. Enregistrement dynamique des clients

Voir la page Serveur DHCP : [dhcp3-server](#)

9. Autres possibilités

Il est possible de moniturer l'utilisation du serveur en installant le package bindgraph, depuis le dépôt Universe, et suivre les détails de configurations dans le README de bindgraph. Tutoriel (<http://opentodo.net/2012/09/09/monitoring-dns-queries-with-bindgraph/>) disponible sur le site opentodo.net (<http://opentodo.net/>).

10. Désinstallation

Pour supprimer cette application, il suffit de supprimer son paquet. Selon la méthode choisie, la configuration globale de l'application est conservée ou supprimée.

11. Voir aussi

- [\(http://www.commentcamarche.net/contents/internet/dns.php3\)](http://www.commentcamarche.net/contents/internet/dns.php3)
- [\(http://www.linux-france.org/prj/edu/archinet/systeme/ch30.html\)](http://www.linux-france.org/prj/edu/archinet/systeme/ch30.html)
- [\(http://www.afnic.fr/ext/dns/index.html\)](http://www.afnic.fr/ext/dns/index.html)
- [\(http://www.it-connect.fr/dns-avec-bind-9%ef%bb%bf/\)](http://www.it-connect.fr/dns-avec-bind-9%ef%bb%bf/) sur IT-Connect
- [\(http://www.it-connect.fr/securiser-dns-bind9-serveur-unique%ef%bb%bf/\)](http://www.it-connect.fr/securiser-dns-bind9-serveur-unique%ef%bb%bf/) sur IT-Connect
- [\(http://actual-it.info/2013/bind9-serveur-dns/\)](http://actual-it.info/2013/bind9-serveur-dns/) - Actual-IT.info

Contributeurs principaux : lmrv.

Basé sur «BIND9ServerHowto» (<https://help.ubuntu.com/community/BIND9ServerHowto>) par Auteur Original.

