CONFIGURATION D'UN SERVEUR DNS

Le serveur **DNS BIND** repose sur un exécutable **named** et sur un fichier de configuration **named.conf**.

CONFIGURATION DE BASE

STRUCTURE DU FICHIER « named.conf » ET PRINCIPAUX ÉLÉMENTS DE CONFIGURATION

Ci-dessous un exemple générique de fichier named.conf. Selon les cas, on le trouvera sous une forme entière et monolithique, mais il est fréquent de le trouver éclaté en plusieurs morceaux pour des raisons de lisibilité.

Les sous-fichiers sont alors appelés par la directive **include**. Le rôle principal du fichier est de déclarer les zones qui seront gérées par ce serveur, mais également de préciser tout élément de configuration.

Format simplifié de named.conf

```
include "/chemin/fichier";
options {
        directory "/chemin/repertoiredetravail";
        forwarders { A.B.C.D };
        };
zone "NOMDEZONE1" {
        type type;
        file "/CHEMIN/NOMFICHIER1";
        };
zone "NOMDEZONE2" {
        type type;
        file "/CHEMIN/NOMFICHIER2";
        };
```

Fichier « named.conf » : principales directives utilisées	
include	Indique le nom d'un "sous-fichier" de configuration. Évite d'avoir un fichier named.conf trop grand pour être administré confortablement.
options	Conteneur pour certains mots-clés, notamment directory et forwarders.
directory	Dans une directive option. Indique le répertoire utilisé pour le stockage sur disque des données de cache du serveur.
forwarders	Placé dans une directive option pour les configurations simples (redirection inconditionnelle). Si le serveur ne dispose pas dans ses fichiers de la résolution demandée, renvoyer la demande vers le serveur dont l'adresse IP est donnée en référence.
zone	Conteneur pour le nom d'une zone DNS gérée par le serveur.
type	Dans une directive zone. Indique le type de zone stockée. Les principales valeurs sont hint (serveurs racine), master (serveur maître d'une zone), et slave (réplique depuis un master).
file	Dans une directive zone. Indique le fichier contenant les informations de zone.

LES FICHIERS DE DÉFINITION DE ZONE PRÉ-INSTALLÉS

Selon les implémentations, un certain nombre de zones sont présentes par défaut à l'installation du serveur pour assurer un fonctionnement standard et permettre les résolutions courantes. Par exemple, la zone localhost qui permet de résoudre le nom localhost en 127.0.0.1, y compris au sein du service DNS et pas seulement dans le fichier hosts.

Ces fichiers de zones sont créés à l'installation, et correctement référencés dans le fichier named.conf.

Exemple de fichier named.conf sur une distribution Debian

Notez la déclaration des zones par défaut, ainsi que l'appel de deux sous-fichiers de configuration appelés par la directive include.

```
include "/etc/bind/named.conf.options";

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";
};

include "/etc/bind/named.conf.local";
```

Notez les directives include, qui renvoient vers deux fichiers vides à l'installation (ils ne contiennent que des commentaires). Le reste de la configuration se résume à la déclaration de zones, dont la seule indispensable à la résolution de noms publique est la zone « . » évoquée plus haut.

SERVEUR DE CACHE

Un serveur DNS de cache assure une résolution de noms, mais n'héberge aucune donnée de résolution locale et s'appuie sur une infrastructure déjà existante. Il se contente de relayer les demandes vers d'autres serveurs. Ce faisant, ce serveur mettra en cache pour une durée déterminée toutes les résolutions enregistrées.

Par définition, un serveur de cache ne dispose pas localement de zones DNS personnalisées. C'est-à-dire qu'il n'assurera pas lui-même de résolution de type « Quelle est l'adresse IP correspondant au nom "www.sitegenial.com ?" : Il n'héberge tout simplement pas ce type d'information, et devra pour répondre aux requêtes s'en remettre à d'autres serveurs mieux renseignés.

CONFIGURATION DU SERVEUR DE CACHE

C'est la bonne nouvelle : un serveur BIND fraîchement installé est naturellement un serveur de cache. Il n'y a donc pas de configuration particulière à réaliser, il s'agit simplement d'installer un serveur fonctionnel sans information de zone locale.

REDIRECTION

Nous savons qu'un serveur de cache n'héberge pas localement d'enregistrements de ressources. S'il doit faire une résolution, il va s'adresser aux seuls serveurs qu'il connaisse, à savoir les serveurs racine. Cette méthode de résolution n'est pas forcément la plus rapide, et on pourrait souhaiter tirer parti du cache de serveurs déjà en fonctionnement, comme ceux d'un hébergeur ou d'un fournisseur d'accès. Il faut pour cela indiquer à notre serveur l'adresse d'autres serveurs vers lesquels il pourra rediriger ses requêtes. Ce type de redirection est appelé inconditionnelle car toutes les résolutions non lourdes sont redirigées.

Configuration de la redirection dans named.conf

```
options {
    forwarders {
      A.B.C.D;
      };
};
```

Fichier « named.conf » : directives utilisées pour la redirection	
options	Annonce la section options dans le fichier named.conf. Les redirections inconditionnelles sont annoncées dans une section options.
forwarders	Dans une directive options. Annonce la ou les adresses IP du ou des redirecteurs.

COMMANDE DE PILOTAGE « rndc »

Comme tous les services Linux, BIND est lancé ou arrêté par un script dans /etc/init.d. Pour une gestion précise du service, on dispose d'une commande de pilotage : rndc. Cette commande associée à quelques mots-clés permet de transmettre au serveur diverses instructions.

Il n'est pas obligatoire d'utiliser rndc dans le cadre d'une administration courante. Mais alors toute modification d'un fichier de configuration quel qu'il soit imposerait le redémarrage complet du service, et donc son interruption temporaire. rndc devrait donc être utilisé systématiquement, surtout si le serveur gère un grand nombre de zones, comme c'est le cas pour un hébergeur par exemple.

Syntaxe

```
rndc action [paramètre]
```

Commande rndc : actions possibles	
reload	Recharge les fichiers de configuration et les informations de zone.
reload zone zone	Recharge les fichiers d'une zone unique.
reconfig	Charge les fichiers de configuration pour les nouvelles zones uniquement.
flush	Efface le cache du serveur.
flush zone	Efface le cache du serveur pour la zone spécifiée.
status	Affiche l'état du serveur

GESTION DE ZONES DNS

GESTION DE ZONES LOCALES

CRÉATION D'UN FICHIER DE ZONE DIRECTE

Les informations nécessaires à la résolution devront se trouver dans un fichier de déclaration de zone.

L'emplacement de ce fichier est libre, puisqu'il est défini dans une section zone de named.conf. Toutefois, un usage établi veut que ce fichier soit placé dans le répertoire /var/named. Notez que selon les distributions, il peut aussi se trouver dans le répertoire /etc ou dans /etc/bind.

Ce fichier aura le format très strict indiqué ci-dessous. Dans la plupart des cas, un refus de démarrer est dû à un fichier de zone mal formé. Il est composé des déclarations de durée de vie en cache des informations, du serveur ayant autorité sur la zone, des serveurs de noms desservant cette zone, et de l'ensemble des enregistrements de ressources (RR) de cette zone.

Format type du fichier de zone directe

```
$TTL      ttl
nomzone  IN  SOA  serveur mailadmin (
         serial
         refresh
         retry
         expire
         negative )
nomzone  IN  NS  serveur
```

Fichier de zone directe : format type de l'en-tête	
ttl	Time To Live (durée de vie) : indique la durée de conservation en secondes des données en mémoire cache. Cette valeur est précédée par la directive $TTL.
nomzone	FQDN de la zone gérée par ce fichier. Souvent remplacé par un arobase (@) pour alléger le fichier. Attention, puisqu'il s'agit d'un FQDN, le nom de la zone doit se terminer par un point.
IN	Obsolète mais courant : classe Internet (aucune autre classe n'est plus utilisée).
SOA	Start Of Authority. Enregistrement obligatoire pour indiquer que ce serveur est légitime sur cette zone.
serveur	FQDN du serveur ayant autorité sur la zone.
mailadmin	Adresse e-mail de l'administrateur du serveur. L'arobase étant un caractère réservé dans les fichiers de zone, il est conventionnellement remplacé par un point. admin@saintmarcelin.fr devient donc admin.saintmarcelin.fr.
serial	Valeur numérique. Numéro de série du fichier. Utile quand la zone est répliquée sur d'autres serveurs pour savoir si les données ont changé et si la réplication doit être faite.
refresh	Valeur numérique. Utilisé quand la zone est répliquée. Indique au serveur esclave à quel intervalle tester la validité de sa zone.
-retry	Valeur numérique. Utilisé quand la zone est répliquée. S'il est impossible pour l'esclave de contacter le serveur maître, indique au bout de combien de temps réessayer.
expire	Valeur numérique. Utilisé quand la zone est répliquée. S'il est impossible pour l'esclave de contacter le serveur maître, indique au bout de combien de temps les enregistrements non rafraîchis perdent leur validité et ne doivent plus être utilisés.
negative	Valeur numérique. Indique combien de temps le serveur doit conserver en cache une réponse négative.
NS	Enregistrement indiquant quel est le serveur de noms pour cette zone.

CRÉATION D'UN FICHIER DE ZONE INVERSE

Le fichier de zone inverse aura la même structure qu'un fichier de zone directe. Comme indiqué plus haut, le nom normalisé de la zone est formé par les octets de la partie réseau de l'adresse IP ordonnés en sens inverse, suivi de la chaîne de caractères « .in-addr.arpa ».

Par exemple, la zone inverse pour le réseau 192.168.99.0 sera : 99.168.192.in-addr.arpa, et c'est ce nom qui devra être employé dans le fichier de zone et dans le fichier named.conf.

Format type du fichier de zone inverse

```
$TTL    ttl
nomzoneinv  IN  SOA  serveur mailadmin (
         serial
         refresh
         retry
         expire
         negative )

nomzoneinv  IN  NS  serveur
```

Fichier de zone inverse : format type de l'en-tête	
nomzoneinv	Nom normalisé de la zone inverse : subnet-inversé.in-addr.arpa. Où subnet-inversé représente les octets du subnet en ordre inversé. Attention, le nom de la zone inverse est un FQDN, il doit donc se terminer par un point.
SOA	Start Of Authority. Enregistrement obligatoire pour indiquer que ce serveur est légitime sur cette zone.
serveur	FQDN du serveur ayant autorité sur la zone.
NS	Enregistrement indiquant quel est le serveur de noms pour cette zone.

Constatez que c'est rigoureusement la même chose que pour la zone directe. C'est le format des enregistrements qui fait l'essentiel de la différence.

CRÉATION D'ENREGISTREMENTS DANS LES FICHIERS DE ZONE

Une fois les fichiers de zone créés, il suffit d'ajouter autant d'enregistrement de ressource que l'on souhaite, à raison d'un par ligne.

Format d'un enregistrement de ressource dans un fichier de zone directe

```
nom IN typeRR valeur_résolue
```

Format d'un enregistrement de ressource dans un fichier de zone inverse

```
adresse_hôte IN PTR nom
```

Fichier de zone directe : format des enregistrements	
nom	Nom simple ou FQDN auquel il faut faire correspondre une adresse IP.
IN	Obsolète mais nécessaire : classe Internet.
typeRR	Type d'enregistrement. Souvent de type A : fait correspondre une adresse IP à un nom. Valeurs courantes : A, CNAME, MX.
valeur*résolue*|*Ce à quoi on fait correspondre le nom. Dans le cas d'un enregistrement de type A, une adresse IP.*| |*adresse*hôte	L'octet ou les octets qui associés à l'adresse du réseau de la zone inverse formeront l'adresse IP à résoudre.
PTR	Type pointeur : fait correspondre un nom à une adresse IP. Hors enregistrements SOA et NS, c'est le seul type qu'on rencontre dans les zones inverses.

L'ajout d'un grand nombre d'enregistrements est évidemment fastidieux, et gagnera à être réalisé sous forme de script.

Exemple de script simple d'alimentation d'un fichier de zone :

Les hébergeurs et autres DNS gérant de gros volumes d'enregistrement utilisent naturellement des scripts beaucoup plus élaborés.

```
#!/bin/bash
echo "Nom à ajouter à la zone ?"
read nom
echo "Adresse IP correspondant ?"
read ip
echo "$nom  IN  A  $ip" >> /var/named/saintmarcelin.fr
```

DÉCLARATION DE ZONE PRINCIPALE DANS LE FICHIER « named.conf »

Une fois que l'on dispose d'un fichier de zone, il faut faire savoir au serveur qu'il doit le charger au démarrage. Ceci se fera avec une déclaration de zone normalisée dans le fichier named.conf.

Format type de la déclaration de zone dans named.conf

```
zone "nomzone" {
```

```
    type master;
    file "fichier";
};
```

Fichier named.conf : directives et syntaxe de la déclaration de zone	
nomzone	Le FQDN de la zone gérée par le serveur.
type master	Précise qu'il s'agit d'une zone maîtresse à synchroniser éventuellement vers des serveurs esclaves.
fichier	Chemin absolu du fichier à lire pour prendre connaissance des éléments propres à la zone (configuration, RR, etc.).

PRISE EN COMPTE DE LA NOUVELLE CONFIGURATION

Il faut ensuite faire en sorte que le serveur DNS recharge ses fichiers de configuration afin de prendre en compte les nouveautés. Deux solutions pour cela : le redémarrage du service ou le chargement de la nouvelle zone par commande de pilotage rndc.

Rechargement du service

```
/etc/init.d/bind9 restart
Chargement de la nouvelle zone par rndc
rndc reload saintmarcelin.fr
```

GESTION DE ZONES SECONDAIRES

Une zone DNS ne devrait pas dépendre d'un serveur unique et il est courant de créer sur un deuxième serveur des zones secondaires, strictement identiques aux zones primaires, et synchronisées à intervalles réguliers.

DÉCLARATION DE LA ZONE SECONDAIRE DANS « named.conf »

Il n'est évidemment pas nécessaire de créer les fichiers de zones, puisqu'ils seront synchronisés depuis le serveur autoritaire. On parle couramment de serveur maître et de serveurs esclaves.

Le chargement de la zone esclave se fait avec une déclaration de zone normalisée dans le fichier named.conf.

Format type de la déclaration de zone secondaire dans named.conf

```
zone "nomzone" {
    type slave;
    masters { adresse_maître ; } ;
    file "fichier";
};
```

Fichier named.conf : directives et syntaxe de la déclaration de zone	
nomzone	Le FQDN de la zone gérée par le serveur.
type slave	Précise qu'il s'agit d'une zone esclave à synchroniser depuis un serveur maître.
adresse_maître	Adresse IP du serveur autoritaire.
fichier	Chemin absolu du fichier dans lequel stocker les éléments synchronisés. Le compte de service doit avoir les droits d'écriture sur le répertoire de travail.

PRISE EN COMPTE DE LA NOUVELLE CONFIGURATION

Il faut ensuite faire en sorte que le serveur DNS recharge ses fichiers de configuration afin de prendre en compte les nouveautés. Deux solutions pour cela :

- le redémarrage du service
    - ou le chargement de la nouvelle zone par commande de pilotage rndc.

Rechargement du service

```
/etc/init.d/bind9 restart
```

Chargement de la nouvelle zone par rndc

```
rndc reload saintmarcelin.fr
```

DELEGATION DE ZONES

Une délégation de zone consiste à faire gérer par un serveur tiers une zone enfant d'une zone hébergée par un serveur parent. C'est le principe de la délégation qui permet de distribuer l'ensemble de l'espace de noms DNS sur des milliers de serveurs. La délégation se configurera sur le serveur parent.

On ajoutera dans le fichier de zone du parent deux Resource Records : l'un de type NS pour indiquer qu'il existe un serveur de noms pour la zone enfant, et l'autre de type A pour connaître l'adresse IP de ce serveur de noms. L'enregistrement NS assurant la délégation est appelé glue record (enregistrement colle).

Configuration de la délégation dans le fichier de la zone parente

```
zone_enfant IN NS dns_enfant
dns_enfant IN A A.B.C.D
```

Éléments	
zone*enfant*|*Nom simple de la zone enfant.*| |*IN*|*Obsolète mais obligatoire : classe Internet.*| |*NS*|*Cet enregistrement est de type Name Server (serveur de noms).*| |*dns*enfant	Nom du serveur DNS qui gère la zone enfant.
A	C'est un enregistrement de type A.
A.B.C.D	Adresse IP du serveur de noms pour la zone enfant.

OUTILS DE TESTS ET DIAGNOSTICS

ping

Même si ça n'est pas sa fonction première, ping peut tout à fait servir de test rudimentaire pour la résolution de noms. On sera alors limité à tester la réponse des serveurs par défaut, renseignés dans /etc/resolv.conf.

Utilisation de ping pour tester une résolution de noms

Quand on utilise ping pour tester une résolution de noms, c'est la traduction de l'adresse qui importe et non la réponse ICMP de la machine distante.

```
donald:/etc/bind# ping donald.formation.fr
PING donald.formation.fr (192.168.1.1) 56(84) bytes
64 bytes from donald.formation.fr (192.168.1.1): icmp
64 bytes from donald.formation.fr (192.168.1.1): icmp
64 bytes from donald.formation.fr (192.168.1.1): icmp
```

nslookup

nslookup est l'outil le plus populaire pour l'interrogation des serveurs DNS. Il est présent sur la grande majorité des plates-formes Unix et Windows.

nslookup est utilisé la plupart du temps en mode interactif. C'est-à-dire qu'après avoir tapé nslookup, on se trouve dans son interface où on tapera des commandes spécifiques. Les serveurs de noms interrogés par défaut sont ceux référencés dans /etc/resolv.conf. Ceci pourra éventuellement être modifié par la suite.

Utilisation de nslookup pour une résolution de noms

Par défaut, nslookup adresse aux serveurs DNS des requêtes de type A.

```
donald:/etc/bind# nslookup
> server
Default server: 192.168.1.1
Address: 192.168.1.1#53
> coincoin.formation.fr
Server:         192.168.1.1
Address:        192.168.1.1#53
coincoin.formation.fr   canonical name = donald.formation.fr.
Name:   donald.formation.fr
Address: 192.168.1.1
>
```

Requêtes et paramètres dans l'interface interactive nslookup	
nom	Taper un nom DNS directement dans l'interface nslookup revient à en demander la résolution. nslookup indiquera alors quel serveur DNS il a interrogé, et la réponse qui lui a été faite. Il peut s'agir d'un nom complet (FQDN) ou d'un nom simple si on s'appuie sur un suffixe de recherche défini dans /etc/resolv.conf.
server A.B.C.D	La commande server suivie de l'adresse IP d'un serveur à interroger indique à nslookup que toutes les interrogations futures devront être adressées à ce serveur.
set type=TYPE	Par défaut, nslookup fait des requêtes de type A (résolution ordinaire de nom en adresse IPv4). La commande set type permet d'adresser des requêtes d'un autre type. On s'en sert couramment pour connaître par exemple les serveurs de noms ou de messagerie associés à une zone.

Utilisation de nslookup pour trouver l'adresse d'un serveur de messagerie

On peut utiliser nslookup pour tous les types d'enregistrements courants (ici MX).

```
donald:/etc/bind# nslookup
> set type=MX
> elysee.org
Server:         192.168.1.1
Address:        192.168.1.1#53


Réponse ne faisant pas autorité :
elysee.org      MX preference = 10, mail exchanger = mail.elysee.org

mail.elysee.org internet address = 64.182.1.213
>
```

dig

dig est le nouvel outil proposé par l'ISC pour l'interrogation et le diagnostic des serveurs DNS. Passant pour être le plus précis et abouti des outils de test, il devrait éventuellement finir par s'imposer comme solution de référence. Toutefois, les habitudes prises par les administrateurs DNS laissent présager encore de beaux jours pour nslookup.

dig est utilisé en mode non interactif, c'est-à-dire que chaque utilisation de dig devra donner l'ensemble des paramètres nécessaires à la résolution.

Syntaxe simplifiée de dig

```
dig nom
```

```
dig A.B.C.D nom TYPE
```

Éléments	
nom	Le nom complet (FQDN) dont on veut assurer la résolution.
A.B.C.D	L'adresse IP du serveur DNS à interroger. En cas d'omission, les serveurs de noms interrogés sont ceux référencés dans /etc/resolv.conf.
TYPE	Par défaut, dig fait des requêtes de type A (résolution ordinaire de nom en adresse IPv4). Le paramètre type s'il est précisé permet d'adresser des requêtes d'un autre type. On s'en sert couramment pour connaître par exemple les serveurs de noms ou de messagerie associés à une zone.

Exemple d'utilisation de dig :

De loin la plus précise des commandes de diagnostic DNS.

```
donald:/etc/bind# dig @127.0.0.1 coincoin.formation.fr

; <<>> DiG 9.2.4 <<>> @127.0.0.1 coincoin.formation.fr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18067
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;coincoin.formation.fr.         IN      A

;; ANSWER SECTION:
coincoin.formation.fr.  86400   IN      CNAME   donald.formation.fr.
```

```
donald.formation.fr.    86400   IN      A       192.168.1.1

;; AUTHORITY SECTION:
formation.fr.           86400   IN      NS      donald.formation.fr.

;; Query time: 9 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jun 15 19:49:45 2006
;; MSG SIZE  rcvd: 90
```

host

host est un outil simple pour faire une requête DNS en mode non interactif.

Syntaxe simplifiée pour la commande host

```
host nom
```

```
host nom -t type A.B.C.D
```

Éléments	
nom	Le nom DNS dont il faut assurer la résolution. Il peut s'agir d'un FQDN ou du nom simple qui sera complété par le suffixe de recherche s'il est défini dans /etc/resolv.conf.
-t type	Facultatif : le type de requête qui est adressée. Par défaut le type est sélectionné automatiquement parmi les types A, AAAA et MX.
A.B.C.D	Facultatif : l'adresse IP du serveur DNS à interroger. Si cet élément n'est pas renseigné, ce sont les serveurs présents dans /etc/resolv.conf qui sont utilisés.

Utilisation de host pour tester une résolution de noms

host présente un résultat concis.

```
donald:/etc/bind# host coincoin.formation.fr
coincoin.formation.fr is an alias for donald.formation.fr.
donald.formation.fr has address 192.168.1.1

donald:/etc/bind#
```

Utilisation de host pour récupérer les enregistrements NS

```
donald:/etc/bind# host -t NS formation.fr
formation.fr name server donald.formation.fr.

donald:/etc/bind#
```

Mesure des performances (commande « time »)

La commande time qui mesure le temps consommé par une application permet de mesurer la performance d'une résolution DNS. Elle indique le temps total consommé par la commande, et le temps consommé par les processus dans les espaces d'exécution système et utilisateur.

Observation du temps pris par une résolution DNS

Les temps mesurés dépendent de la bande passante disponible, de la disponibilité du serveur, et de la rapidité de la machine cliente.

```
hannibal@box:~$ time host www.laposte.net
www.laposte.net is an alias for www.lpn.fr.
www.lpn.fr is an alias for lb-lp.lpn.fr.
lb-lp.lpn.fr has address 130.193.27.21

real    0m0.288s
user    0m0.000s
sys 0m0.008s
hannibal@box:~$
```

SECURISATION DU SERVEUR DNS : LIMITATION DES CLIENTS

Il est possible de limiter les requêtes autorisées. La directive **allow-query** dans le fichier de configuration permet de définir les hôtes ou réseaux auxquels un serveur acceptera de répondre. Limitation des clients autorisés dans le fichier « named.conf »

```
allow-query { réseaux-autorisés; };
```

Où « réseaux-autorisés » représente la ou les adresses de réseaux ou d'hôte qui pourront s'adresser au serveur.