

## 1. Introduction.

Bind, le service se cachant en général derrière DNS est passé de la version 4 à la version 8. Si vous désirez passer à la version 8, il faut oublier les anciens fichiers de configurations et démarrer de zéro. Le tableau suivant reprend les différences essentielles entre les deux versions.

Version 4	Version 8
Le fichier comprenant les paramètres d'initialisation se nomme /etc/named.boot	Le fichier se nomme /etc/named.conf. La syntaxe à utiliser pour configurer ce fichier est complètement différente
/etc/resolv.conf est optionnel.	/etc/resolv.conf est nécessaire. Vous ne pouvez envoyer un ping vers une URL prédéfinie sans ce fichier. La syntaxe à utiliser pour configurer ce fichier est complètement différente
Avait certains trous de sécurité.	La sécurité a été amélioré.

## 2. Le fichier named.conf

### 2.1. Exemple de configuration.

```
// Si vous désirez n'utiliser votre serveur DNS que comme serveur de
// cache, seule la définition de zone suivante est nécessaire.
//
options {
    directory "/var/named";
};

zone "." {
    type hint;
    file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
    type master;
    file "named.local";
};

zone "helho.be" {
    notify no;
    type master;
    file "helho.be.dns";
};

zone "131.191.193.in-addr.arpa" {
    notify no;
    type master;
    file "named.131.191.193";
};
```

## 2.2. Définition des zones.

Dans l'exemple précédent, on retrouve clairement la définition de l'ensemble des zones. Cette définition correspond à la syntaxe suivante:

```
zone domain_name [ ( in | hs | hesiod | chaos ) ] {
    type master;
    file path_name;
    [ check-names ( warn | fail | ignore ); ]
    [ allow-update { address_match_list }; ]
    [ allow-query { address_match_list }; ]
    [ allow-transfer { address_match_list }; ]
    [ dialup yes_or_no; ]
    [ notify yes_or_no; ]
    [ also-notify { ip_addr; [ ip_addr; ... ] }; ]
    [ pubkey number number number string; ]
};

zone domain_name [ ( in | hs | hesiod | chaos ) ] {
    type ( slave | stub );
    [ file path_name; ]
    masters [ port ip_port ] { ip_addr; [ ip_addr; ... ] };
    [ check-names ( warn | fail | ignore ); ]
    [ allow-update { address_match_list }; ]
    [ allow-query { address_match_list }; ]
    [ allow-transfer { address_match_list }; ]
    [ transfer-source ip_addr; ]
    [ max-transfer-time-in number; ]
    [ notify yes_or_no; ]
    [ also-notify { ip_addr; [ ip_addr; ... ] }; ]
    [ pubkey number number number string; ]
};

zone domain_name [ ( in | hs | hesiod | chaos ) ] {
    type forward;
    [ forward ( only | first ); ]
    [ forwarders { [ ip_addr ; [ ip_addr ; ... ] ] }; ]
    [ check-names ( warn | fail | ignore ); ]
};

zone "." [ ( in | hs | hesiod | chaos ) ] {
    type hint;
    file path_name;
    [ check-names ( warn | fail | ignore ); ]
};
```

### 2.2.1. Les types de zones

Nous allons retrouver cinq types de zones différentes:

master	Le serveur a une copie maître des données pour la zone et a autorité pour cette zone.
slave	Une zone esclave est une réplique d'une zone maître. La liste maître contient une ou plusieurs adresses IP que l'esclave peut contacter pour effectuer une mise à jour de la copie de sa zone. Si un nom de fichier est spécifié, alors la réplique y sera placée. L'utilisation d'une telle clause est recommandée.
stub	Une zone "stub" est semblable à une zone esclave excepté que la réplique ne contient que les enregistrements NS de la zone maître

forward	<p>au lieu de la zone entière.</p> <p>Une zone "forward" est utilisée pour rediriger toutes les demandes vers un autre serveur. Cette information peut figurer dans la définition des options mais une telle spécification dans une zone vient cacher toute déclaration similaire dans les options.</p> <p>Si aucune clause "forwarders" n'est présente dans la zone ou qu'une liste vide est renseignée, alors aucun transfert ne sera effectué pour les demandes vers un autre serveur.</p>
hint	La zone "hint" comprend l'ensemble des serveurs de noms racine.

Dans la version 4 de BIND, on retrouvait dans le fichier d'initialisation les termes primary pour la zone master, secondary pour la zone slave et cache pour la zone hint..

### 2.2.2. Les classes.

Un nom de zone est suivi d'une classe qui est optionnelle. Si une classe n'est pas spécifiée, la classe in (pour internet ) est prise par défaut. Ce sera celle correspondant à la majorité des cas.

### 2.2.3. Les options.

check-names	Voir la description de la même section dans la définition des options.
allow-query	Voir la description de la même section dans la définition des options.
allow-update	Spécifie quels sont les hôtes autorisés à demander des mises à jours dynamiques vers le serveur. La valeur par défaut est d'interdire les mises à jours à partir d'autres hôtes.
allow-transfert	Voir la description de la même section dans la définition des options.
transfert-source	transfer-source détermine l'adresse locale utilisée pour lier la connexion TCP lors de la réception de cette zone.
max-transfert-time-in	Voir la description de la même section dans la définition des options.
dialup	Voir la description de la même section dans la définition des options.
notify	Voir la description de la même section dans la définition des options.
also-notify	
forward	Forward est seulement utile si la zone possède une liste "forwarders". La valeur "only" aura comme conséquence l'échec de la recherche si après avoir essayé tous les "forwarders" aucune réponse n'a pu être obtenue. Si la valeur "first" est utilisée, une recherche normale peut être exécutée si aucune réponse des "forwarders" n'a été obtenue.
forwarders	Cette option est utilisée dans une zone pour surcharger la liste globale des "forwarders" utilisée dans la définition des options.
pubkey	

## 2.3. Définition des options.

```
options {
  [ version version_string; ]
  [ directory path_name; ]
  [ named-xfer path_name; ]
  [ dump-file path_name; ]
  [ memstatistics-file path_name; ]
  [ pid-file path_name; ]
  [ statistics-file path_name; ]
  [ auth-nxdomain yes_or_no; ]
  [ deallocate-on-exit yes_or_no; ]
  [ dialup yes_or_no; ]
  [ fake-iquery yes_or_no; ]
  [ fetch-glue yes_or_no; ]
  [ has-old-clients yes_or_no; ]
  [ host-statistics yes_or_no; ]
  [ multiple-cnames yes_or_no; ]
  [ notify yes_or_no; ]
  [ recursion yes_or_no; ]
  [ rfc2308-type1 yes_or_no; ]
  [ use-id-pool yes_or_no; ]
  [ treat-cr-as-space yes_or_no; ]
  [ also-notify yes_or_no; ]

  [ forward ( only | first ); ]
  [ forwarders { [ in_addr ; [ in_addr ; ... ] ] }; ]

  [ check-names ( master | slave | response )( warn | fail | ignore);]

  [ allow-query { address_match_list }; ]
  [ allow-recursion { address_match_list }; ]
  [ allow-transfer { address_match_list }; ]
  [ blackhole { address_match_list }; ]

  [ listen-on [ port ip_port ] { address_match_list }; ]
  [ query-source [ address ( ip_addr | * ) ]
    [ port ( ip_port | * ) ] ; ]
  [ lame-ttl number; ]

  [ max-transfer-time-in number; ]

  [ max-ncache-ttl number; ]
  [ min-roots number; ]

  [ transfer-format ( one-answer | many-answers ); ]
  [ transfers-in number; ]
  [ transfers-out number; ]
  [ transfers-per-ns number; ]
  [ transfer-source ip_addr; ]
  [ maintain-ixfr-base yes_or_no; ]
  [ max-ixfr-log-size number; ]
  [ coresize size_spec ; ]
  [ datasize size_spec ; ]
  [ files size_spec ; ]
  [ stacksize size_spec ; ]
  [ cleaning-interval number; ]
  [ heartbeat-interval number; ]
  [ interface-interval number; ]
```

```
[ statistics-interval number; ]
[ topology { address_match_list }; ]
[ sortlist { address_match_list }; ]
[ rrset-order { order_spec ; [ order_spec ; ... ] }; ]
};
```

L'ensemble des différentes rubriques que l'on retrouve dans le bloc d'options peuvent être regroupées en fonction de l'utilité qu'elles ont.

### 2.3.1. Contrôle d'accès.

L'accès à un serveur peut être restrictif et basé sur l'adresse IP du système demandeur ou au moyen de clefs secrètes partagées.

allow-query	Spécifie quels sont les hôtes autorisés à effectuer des demandes ordinaires.
allow-recursion	Spécifie quels sont les hôtes pouvant effectuer des demandes récursives. Par défaut, tous les hôtes peuvent effectuer des requêtes récursives.
allow-transfer	Spécifie quels sont les hôtes qui sont autorisés à recevoir des transferts de zone à partir du serveur. Par défaut, les transferts de zone sont autorisés à partir de tous les hôtes.
blackhole	Spécifie une liste d'adresses pour lesquelles le serveur ne peut pas accepter la moindre requête de demande de résolution de noms.

### 2.3.2. Transfert des requêtes (forwarding).

forward	Cette option est seulement utile si une liste de "forwarders" a été définie. La valeur "first" qui est celle par défaut aura comme conséquence que la demande sera en premier transférée vers les "forwarders". Si aucun des forwarders ne peut fournir la réponse, le serveur effectuera la demande lui même. Si la valeur "only" est spécifiée, le serveur effectuera seulement le transfert de la requête.
Forwarders	Spécifie les adresses IP qui doivent être utilisées pour le transfert des demandes.

### 2.3.3. Interfaces.

Permet de spécifier les interfaces réseaux et les ports pour lesquels le serveur doit fournir une réponse aux demandes reçues. Si un port n'est pas renseigné, ce sera le port 53 qui sera utilisé.

Exemple:

```
listen-on { 5.6.7.8; };
listen-on port 1234 { !1.2.3.4; 1.2/16; };
```

### 2.3.4. Adresses de demande.

Si le serveur ne connaît pas la réponse à une question, il pourra interroger d'autres serveurs de noms. Query-source permet de spécifier les adresses et les ports à utiliser pour de telles demandes.

### 2.3.5. Les transferts de zones.

max-transfer-time-in	C'est le temps maximum qu'un transfert de zones entrant peut durer. Au delà de ce temps, il sera terminé. Par défaut, la valeur est de 120 minutes.
transfer-format	Le serveur supporte deux méthodes de transfert de zones. "one-answer" utilise un message DNS par enregistrement de ressource transféré. "many-answers" est plus efficace mais est seulement utilisable avec la version 8.1 et les versions mises à jour de BIND 4.9.5. La valeur par défaut est "one-answer".
transfers-in	C'est le nombre maximum de transferts de zone entrant qui peuvent être exécutés simultanément. La valeur par défaut est 10. Augmenter ce paramètre va accélérer la mise à jour des zones esclaves mais va aussi augmenter la charge de votre système local.
transfers-out	Cette option sera utilisée dans le futur pour limiter le nombre de transferts de zones simultanés en sortie. Actuellement, cette option est ignorée.
transfers-per-ns	C'est le nombre maximum de transferts de zones entrant qui peuvent être effectués simultanément à partir d'un serveur de noms distant. La valeur par défaut est 2.
transfer-source	Ce paramètre détermine quelle est l'adresse locale qui sera liée à la connexion TCP utilisée pour rapporter toutes les zones transférées en entrée par le serveur. Par défaut, ce sera l'adresse de l'interface attachée au système distant.
notify	Si le choix est "yes" (par défaut), un message "DNS NOTIFY" sera envoyé quand une zone pour laquelle le serveur a autorité est modifiée. L'utilisation du "notify" va accélérer la convergence entre le contenu du maître et de ses esclaves. Les serveurs esclaves qui reçoivent un message "NOTIFY" et le comprennent contacteront le serveur maître pour la zone et voire si un transfert de zone est nécessaire ou pas.
also-notify	Définit une liste globale d'adresses IP qui vont également recevoir les messages "NOTIFY" toutes les fois qu'une copie récente de la zone est chargée. Cela aide à assurer que les copies des zones convergeront rapidement sur les serveurs
dialup	Si cette valeur est "yes", le serveur va alors traiter toutes les zones comme si elles allaient effectuer des transferts de zones au travers d'un réseau téléphonique à la demande, lequel pourrait voir son nombre de connexions augmenter du fait du trafic lié au serveur. Ce paramètre aura des effets différents suivant le type de zone. Cela concentre la maintenance des zones de façon à ce qu'elle se produise dans un court intervalle de temps durant le même appel.

Cela va également supprimer le trafic lié aux maintenances normales des zones. Si la zone est une zone maître, le serveur enverra un "NOTIFY" vers tous les esclaves. Cela aura pour effet de déclencher les demandes de mises à jour des zones et pour les esclaves supportant le "NOTIFY", permettre la vérification lors du même appel. Si la zone est esclave ou souche, alors le serveur supprimera les demandes régulières de mises à jour (seulement effectuées lors de l'expiration de l'intervalle "heartbeat-interval").

### 2.3.6. Pathnames

**directory** Il s'agit du répertoire de travail du serveur. N'importe quels chemins peuvent être pris comme relatif à ce répertoire pour les noms des différents fichiers dans les définitions de zones. Le répertoire spécifié doit être un chemin absolu.

### 2.3.7. Intervalles des tâches périodiques.

**cleaning-interval** Le serveur purgera la cache des enregistrements de ressource qui ont expiré toutes les "cleaning-interval" minutes. La valeur par défaut est de 60 minutes. Si 0 est choisi, aucune purge n'est effectuée.

**heartbeat-interval** Le serveur effectuera une maintenance des zones marquées avec l'option "dialup yes" quand cet intervalle vient à échéance. Par défaut, la valeur est de 60 minutes. Des valeurs raisonnables peuvent être de 1 jour (1440 minutes).

**interface-interval** Le serveur va scanner la liste des interfaces réseau toutes les "interface-interval" minutes. La valeur par défaut est de 60 minutes. Si le paramètre est 0, cette liste ne sera scannée qu'au chargement du fichier de configuration. Après le scan, une écoute sera assurée sur toutes les nouvelles interfaces s'assurant qu'elles soient reprises dans l'option listen-on.

**statistics-interval** Les statistiques du serveur de nom seront copiées dans un fichier toutes les "statistics-interval" minutes. La valeur par défaut est 60. Si le paramètre est 0, aucune copie n'est exécutée.

## 3. Les fichiers d'association directe ou inverse.

Excepté le fichier de configuration dont la syntaxe change complètement, la syntaxe des fichiers d'association directe ou inverse ne subissent aucun changement .

Exemple de fichier d'association directe:

```
@      IN      SOA      ns.helho.be. hostmaster.helho.be. (
                                5 ; Serial
                                10800 ; Refresh
                                3600 ; Retry
                                604800 ; Expire
                                86400 ) ; Minimum TTL

@      NS      ns      ; Inet Address of name server
@      MX      10 mail  ; Primary Mail Exchanger

localhost      A      127.0.0.1
ns             A      193.191.131.2
mail          A      193.191.131.2
@            A      193.191.131.2
www          CNAME  @
```