

Configuration de base du serveur

1. Fonctionnement du serveur BIND

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

a. 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/repertoirede travail";
    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.

b. 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 nom publique est la zone « . » évoquée plus haut.

2. Serveur de cache

Un serveur DNS de cache assure une résolution de nom, 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.

a. 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.

b. 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 adresse(s) IP du ou des redirecteur(s).

3. Commande de pilotage rndc

Comme tous les services Unix ou 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