Documentation dind9 sur linux

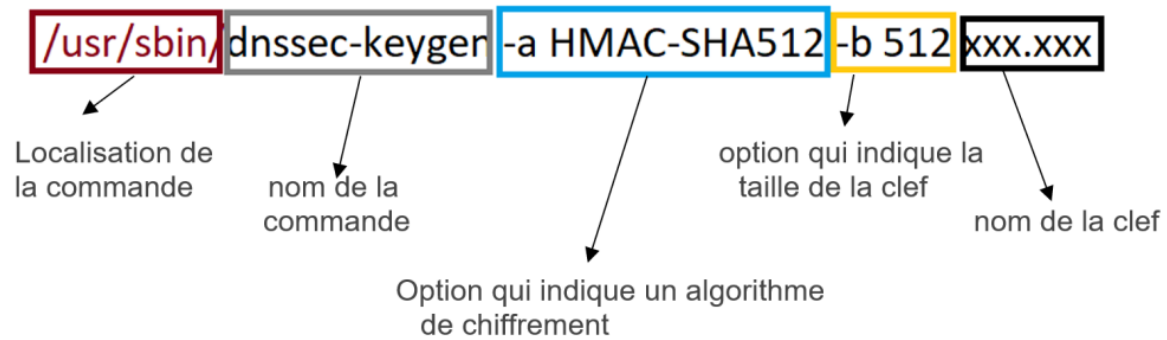
apt-get install bind9 dnsutils

Sur les deux serveurs, ensuite nous allons enchainer avec les configurations de bases de BIND9, dans le fichier /etc/bind/named.conf.options, on y retrouvera les différentes options à adapter selon le besoin :

```
directory "/var/cache/bind";
dnssec-enable yes;
dnssec-validation yes;
dnssec-lookaside auto;
empty-zones-enable no;
auth-nxdomain no;
# conform to RFC1035
listen-on-v6 { any; };
# adresse ip publique du serveur :
listen-on {; };
version "SECRET";
edns-udp-size 4096; #
notify-source 188.165.162.39;
#       notify-source-v6 2001:41d0:1:d6e::110;
#       allow-transfer { key key-ns2; key key-ns3; key key-ns4; };
#       allow-notify {;};
allow-notify {;};
allow-transfer {"none";};
recursion no;
allow-query-cache {none;};
additional-from-cache no;
additional-from-auth no ;
zone-statistics yes;
rate-limit { responses-per-second 3;
slip 2;
# adresses IP des serveurs DNS authoritaires à exclure des limitations de
requêtes :
exempt-clients {;};
};
};
```

Pour finaliser, un aspect fort important et non négligeable, la sécurité. En effet, le flux DNS de ces serveurs de doit pas être traçable et être crypté, pour cela nous allons voir comment sécuriser les flux DNS :

Nous allons créer les clefs avec la commande dnssec-keygen :



Cette commande créera deux fichiers contenant l'un une clef publique et l'autre la clef privée. La clef publique sera donnée aux autres serveurs pour s'identifier et la clef privée restera sur le serveur initial.

Dans le fichier named.conf, ajouter les lignes suivantes :

```
// * TSIG *
key test-test {
algorithm hmac-sha512;
secret "La clef se situe dans le fichier qui fini par .private"
} ;
```

Pour finir sur le maître, ajouter la ligne suivante dans /etc/bind/named.conf.options :

Maintenant passons au secondaire, commençons par modifier le fichier named.conf et ajouter :

```
Key dns-dns. {
algorithm hmac-sha512;
secret " La clef se situe dans le fichier qui fini par . private ";
};
Ip primaire {
keys {
xxx-xxx.;
};
```

C'est bon, votre service BIND9 est installé avec succès. Je vais maintenant vous expliquer comment l'utiliser. On va ici prendre un cas d'école : on veut ajouter un enregistrement DNS exemple.com

On va commencer par aller dans le fichier /etc/bind/named.conf.local et on va ajouter ces lignes :

Ensuite nous allons créer ce fichier db.exemple.com à l'emplacement indiqué ci-dessus pour y indiquer des informations telles que les IP :

```
>_ nano /etc/bind/db.exemple.com

$ttl 1H
exemple.com.          IN      SOA     ksxxxxx.kimsufi.com. email@example.com. (
                                        2011041902 ; Serial
                                        1H ; Refresh
                                        15M ; Retry
                                        2W ; Expire
                                        3M ; Minimum TTL
                                        )
exemple.com.  IN      NS              ksxxxxx.kimsufi.com.
exemple.com.  IN      NS              ns.kimsufi.com.
exemple.com.  IN      A               111.222.111.222
```

Pour analyser ce fichier on va le couper en deux parties

```
>_ nano /etc/bind/db.exemple.com

$ttl 1H
exemple.com.          IN      SOA     ksxxxxx.kimsufi.com. email@example.com. (
                                        2011041902 ; Serial
                                        1H ; Refresh
                                        15M ; Retry
                                        2W ; Expire
                                        3M ; Minimum TTL
                                        )
```

Dans cette partie on va retrouver les informations relatives à l'administration et à la validité des informations

On y retrouve notamment :

exemple.com.		C'est votre nom de domaine, attention : ne pas oublier le point.
IN		Signifie internet, c'est à dire que la zone après le IN Est destinée à internet
SOA		Star Of Authority indiquant le serveur de nom faisant autorité c'est à dire votre DNS principal.
ksxxxx.kimsufi.com.		DNS principal de votre domaine
email@example.com		Adresse email (valide de préférence) il faut remplacer le @ par un point et on termine par un point également.
1H	$TTL	TTL (Time to Live) pour cette zone. Temps pendant lesquels les informations de la zone peuvent être considérées comme valides et être mises en cache

2011041902	Serial	N° de série à incrémenter à chaque modification de ce fichier. Par convention, on écrit : année-mois-jour-numéro_à_2_chiffres.
1H	Refresh	A l'expiration du délai Refresh, le serveur esclave va entrer en communication avec le maitre, s'il ne le trouve pas, il fera une nouvelle tentative au bout du délai Retry, si au bout du délai Expire il considérera que le serveur n'est plus disponible.
15M	Retry	Nombre de secondes avant d'effectuer une nouvelle demande au serveur maître en cas de non-réponse.
2W	Expire	Temps (en secondes) d'expiration du serveur principal en cas de non-réponse.
3M	Minimum TTL	Durée de vie minimum du cache en secondes

Passons maintenant à la deuxième partie :

```
exemple.com.  IN    NS      ksxxxxx.kimsufi.com.
exemple.com.  IN    NS      ns.kimsufi.com.
exemple.com.  IN    A       111.222.111.222
```

- Cette partie définit où sera redirigé la requête, ici ce sera vers l'IP 111.222.111.222 mais en réalité, il existe des dizaines de types de types d'enregistrement :
- A : il s'agit des enregistrements d'adresses faisant correspondre un nom d'hôte à une adresse IPv4 de 32bits. En IPv6, on utilise des enregistrements AAAA codés sur 128bits.
- CNAME : il s'agit d'enregistrements canoniques créant un alias d'un domaine vers un autre. L'alias hérite de tous les sous-domaines de l'original.
- MX : définit les serveurs de messagerie pour le domaine.
- PTR : associe une adresse IP à un enregistrement de nom de domaine (on parle de reverse puisqu'il s'agit du contraire de l'enregistrement A).
- NS : définit les serveurs DNS du domaine (primaire et secondaire).
- SOA : fournit les informations générales de la zone : serveur principal, contact, délai d'expiration, n° de série de la zone.
- SRV : généralise la notion d'enregistrement MX en proposant des fonctions avancées : taux de répartition de charge (décrit dans la RFC2782).
- NAPTR : donne accès aux règles de réécriture de l'information permettant de lier le nom de domaine et une ressource (RFC3403).
- TXT : permet à l'administrateur d'insérer un texte quelconque pour un enregistrement DNS.