Bind9

Table des matières

1 Introduction

Tester `host -a narval.tk` et `host -t mx narval.tk`.

- `A` : adresse IP de la machine
- `MX` : serveur MAIL du domaine
- `TXT` : serveur XMPP ou autre

2 dot-tk

Je cherche à ajouter un champ `MX` aux DNS afin que mon serveur soit en mesure de recevoir des mail depuis l'extérieur.

Créer un nom de domaine chez dot.tk.

```
$ host narval.tk
narval.tk has address 94.103.151.195
narval.tk has address 217.119.57.22
narval.tk has address 209.172.59.196
narval.tk has address 193.33.61.2
narval.tk mail is handled by 20 MX-HOST.DOT.tk.
```

Teste d'un mail à "nroche@narval.tk" en ayant choisi le "forwarding DNS" depuis l'interface WEB de DOT-TK :

```
This is the mail system at host smtp4-g21.free.fr.
I'm sorry to have to inform you that your message could not
be delivered:

<nroche@narval.tk>: host MX-HOST.DOT.tk[71.6.218.116] said: 554 5.1.2
    <nroche@narval.tk>: Recipient address rejected: Bad destination system
    address (in reply to RCPT TO command)
```

Rq : je n'ai pas réussi à ajouter un champ `MX` en utilisant le "use dot-tk free DNS service". Reste l'option "Use custom DNS service" nécessitant d'héberger son propore serveur DNS.

3 Installation

```
                             # tail -f/var/syslog
# apt-get install bind9
# host google.fr localhost
# /etc/init.d/bind9 stop
```

4 Configuration

4.1 Fichier */etc/bind/name.conf.options*

```
options {
directory "/var/cache/bind";
query-source address *;

        // your ISP IP addresses for stable nameservers
forwarders {
212.27.53.252;
  212.27.54.252;
};

auth-nxdomain no;    # conform to RFC1035
listen-on-v6 { any; };
        allow-query { any; }; // pour limiter l'accès au forwarders ci-dessus (je crois)
};
```

4.2 Fichier */etc/bind/name.conf.local*

```
 //
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
include "/etc/bind/zones.rfc1918";

zone "narval.tk" {
type master;
file "/etc/bind/db.narval.tk";
};

zone "148.5.242.82.in-addr.arpa" {
```

```
        type master;
        file "/etc/bind/db.82.242.5.148";
};
```

4.3 DNS secondaire

Même fichier en donnant l'adresse du serveur "master" afin d'y télécharger (automatiquement) le dit fichier :

```
zone "narval.tk" {
        type slave;
        file "/etc/bind/db.narval.tk";
        masters {
                5.135.154.197;
        };
};

zone "5.135.154.197.in-addr.arpa" {
        type slave;
        file "/etc/bind/db.197.154.135.5";
        masters {
                5.135.154.197;
        };
};

zone "79.143.250.133.in-addr.arpa" {
        type master;
        file "/etc/bind/db.133.250.143.79";
};
```

4.4 Fichier */etc/bind/db.narval.tk*

```
$TTL    604800
@ IN SOA ns.narval.tk. root.ns.narval.tk.  (
        2012032801 ; Serial  -> N° de série à incrémenter à chaque modif
                   ;            de ce fichier. Ce N° est utilisé par les
                   ;            serveurs esclaves pour lui indiquer qu'il
                   ;            doit mettre à jour sa base. Par commodité
                   ;            ce n° est une date à l'envers.
        604800     ;Refresh ->  A l'expiration du délai Refresh exprimé en
                   ;            secondes, le serveur excalve va entrer en
                   ;            communication avec le maitre et si il ne
                   ;            le trouve pas, il fera une nouvelle
                   ;            tentative au bout du délai Retry et si au
                   ;            bout du délai Expire il considerera que le
                   ;            serveur n'est plus disponible.
        86400      ; Retry
        2419200    ; Expire
        604800 )   ; Minimum -> Durée de vie minimum du cache en secondes


;** Les 2 lignes suivantes permettent au serveur de se retrouver lui même
@       IN      NS      maximus.narval.tk.
@       IN      MX   10 maximus.narval.tk.
```

```
maximus IN A       82.242.5.148
maximus         HINFO   "cowsay" "yé" ;Info complémentaire

max IN CNAME   maximus.narval.tk.
ns IN CNAME   maximus.narval.tk.
mail IN CNAME   maximus.narval.tk.
www IN CNAME   maximus.narval.tk.
```

4.5 Fichier */etc/bind/db.82.242.5.148*

```
$TTL    604800
@       IN      SOA     max.narval.tk. root.narval.tk.      (
                    2010062000
                        604800
                         86400
                       2419200
                        604800 )

@       IN      NS      ns.narval.tk.

        IN      PTR     narval.tk.
```

5 Test

5.1 Fichier */etc/resolv.conf*

```
search narval.tk
nameserver 127.0.0.1
#nameserver 212.27.53.252
#nameserver 212.27.54.252
```

5.2 Fichier */etc/hostname*

```
maximus
```

5.3 Victoire !

```
$ host -a narval.tk maximus

narval.tk. 604800 IN SOA ns.narval.tk. ...
narval.tk. 604800 IN NS ns.narval.tk.
narval.tk. 604800 IN MX 10 mail.narval.tk.
narval.tk. 604800 IN A 82.242.5.148
```

Rq : Pensez à ouvrir le ports UDP 53 (domain) en entrée et en sortie.

```
$ host -a narval.tk ROOT-F.TALOHA.tk.

narval.tk. 602525 IN A 82.242.5.148
narval.tk. 300 IN NS NS.narval.tk.
narval.tk. 82918 IN MX 20 MX-HOST.DOT.tk.
```

5.4 Remarques

- Bien que le serveur de mail ne soit pas répertorié par le DNS de `tk.`, l'information est bien relayée aux autres DNS.

  ```
  $ host -t mx narval.tk ROOT-F.TALOHA.tk.
  narval.tk has no MX record
  ```

- Les DNS de `google.com` et du CC à Lyon ne répertorient pas du tout le domaine `narval.tk`. C'est normal car il ne servent que les noms de domaines quils hébergent.

  ```
  $ host -a narval.tk  ns2.google.com.
  Host narval.tk not found: 5(REFUSED)

  $ host -a mx narval.tk cri.ens-lyon.fr.
  Host narval.tk not found: 5(REFUSED)
  ```

- Etre très patient car la propagation des informations peut prendre du temps.

6 Exemple configuration maître/esclave

- Commun : *named.conf.options* pointent sur le DNS de FDN ?!
- Server chey OVH
  - *db.narval.tk*
  - *db.197.154.135.5*
  - *named.conf.local* :

    ```
    zone "narval.tk" {
            type master;
            file "/etc/bind/db.narval.tk";
    };

    zone "5.135.154.197.in-addr.arpa" {
           type master;
           file "/etc/bind/db.197.154.135.5";
    };

    zone "79.143.250.133.in-addr.arpa" {
           type slave;
           file "/var/lib/bind/db.133.250.143.79";
    };
    ```

- Server chey MOI
  - *db.133.250.143.79*
  - *named.conf.local* :

    ```
    zone "narval.tk" {
            type slave;
            file "/var/lib/bind/db.narval.tk";
            masters {5.135.154.197;};
    };
    ```

```
zone "5.135.154.197.in-addr.arpa" {
       type slave;
       file "/var/lib/bind/db.197.154.135.5";
        masters {5.135.154.197;};
};

zone "79.143.250.133.in-addr.arpa" {
       type master;
       file "/etc/bind/db.133.250.143.79";
};
```

Attention, penser à garder à l'heure le serveur !
diagramme