Aller au contenu

Introduction

Installation :

Il faut installer le paquet **bind9** pour le service DNS
Il faut installer à minima le paquet dnsutils pour les tests sur les clients

Configuration du serveur DNS Principal
Fichiers de configuration principaux :
- **/etc/bind/named.conf.local**
- **/etc/bind/named.conf.options**
- **/etc/bind/db.zone.ext** (un fichier par zone gérée)

DNS

Pour commencer il faut installer les outils bind9 pour le service DNS et dnsutils pour les tests sur les clients . On a aussi installé bind9utils.

```
apt-get install bind9 bind9utils dnsutils
```

Configuration du serveur DNS Principal

Dans le fichier de configuration **/etc/bind/named.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";


// Déclaration d'une zone gérée par le DNS
zone "gsb.org" IN {
        type master;
        file "/etc/bind/db.gsb.org";
};




// Déclaration d'une seconde zone gérée par le DNS
zone "afrique.gsb.org" IN {
        type master;
        file "/etc/bind/db.afrique.gsb.org";
};


```

```
28
29  // Délégation de zone
30  // Toutes les requêtes DNS portant sur le sous domaine ssdom2.example.com seront
31  // transférées à la machine 10.31.232.53
32  zone "europe.gsb.org" IN {
33          type forward;
34          forwarders {10.31.232.53;};
35  };
36
37  zone "usa.gsb.org" IN {
38          type forward;
39          forwarders {10.31.216.53;};
40  };
41
42
43
44  zone "asie.gsb.org" IN {
45          type forward;
46          forwarders {10.31.208.53;};
47  };
```

La partie “Délégation de zone” correspond aux DNS des autres groupent de la classe, lesquels vont recevoir la demande à leur DNS si le notre est interroger demandant un des leurs.

Fichier **named.conf.options**

```
1   options {
2           directory "/var/cache/bind";
3
4           // If there is a firewall between you and nameservers you want
5           // to talk to, you may need to fix the firewall to allow multiple
6           // ports to talk.  See http://www.kb.cert.org/vuls/id/800113
7
8           // If your ISP provided one or more IP addresses for stable
9           // nameservers, you probably want to use them as forwarders.
10          // Uncomment the following block, and insert the addresses replacing
11          // the all-0's placeholder.
12
13          //========================================================================
14          // If BIND logs error messages about the root key being expired,
15          // you will need to update your keys.  See https://www.isc.org/bind-keys
16          //========================================================================
17          dnssec-validation no;
18
19          //listen-on-v6 { any; };
20
21          allow-query { any; };
22          recursion yes;
23          forwarders { 8.8.8.8; 8.8.4.4; };
24          //forwarders { 10.31.248.1; 10.31.248.126; };
25          forward only;
26
27  };
```

La ligne “**dnssec-validation no;**” doit être décommenter car sinon le “**dig ns europe.gsb.org @10.31.248.53**” (par exemple ne fonctionnerai pas).

Fichier **db.gsb.org**

```
$TTL 604800 ;TTL durée de vie du cache
$ORIGIN gsb.org.

@ IN SOA ns1.gsb.org. root.gsb.org. (
202100401 ;serial number (pour les secondaires)
3600 ;refresh - temps de mise à jour du slave
600 ;retry – délai d'attente avant 2ème demande si le master est down
2419200 ;expire – temps durant lequel le slave tentera de contacter le master
604800 ) ;min - validité du cache

@ IN A 10.31.248.53
@ IN NS ns1
@ IN NS ns2
ns1 IN A 10.31.248.53
ns2 IN A 10.31.248.54


www IN A 10.31.248.53
smtp IN A 10.31.248.1


web IN CNAME www




;Seconde zone (même DNS)
$ORIGIN afrique.gsb.org.
@ 86400 IN NS ns1.afrique.gsb.org.
ns1.afrique.gsb.org. IN A 10.31.248.53


;Délégation de zone (autre DNS)
$ORIGIN europe.gsb.org.
@ 86400 IN NS ns1.europe.gsb.org.
ns1.europe.gsb.org. IN A 10.31.232.53 ;Zone gérée par un autre serveur DNS


;Délégation de zone (autre DNS)
$ORIGIN usa.gsb.org.
@ 86400 IN NS ns1.usa.gsb.org.
ns1.usa.gsb.org. IN A 10.31.216.53 ;Zone gérée par un autre serveur DNS


;Délégation de zone (autre DNS)
$ORIGIN asie.gsb.org.
@ 86400 IN NS ns1.asie.gsb.org.
ns1.asie.gsb.org. IN A 10.31.208.53 ;Zone gérée par un autre serveur DNS
```

Fichier **db.afrique.gsb.org**

```
@ IN SOA ns1.afrique.gsb.org. root.afrique.gsb.org. (
2020091401
604800
86400
2419200
604800 ) ;

@ IN A 10.31.248.53
@ IN NS ns1
ns1 IN A 10.31.248.53
ns2 IN A 10.31.248.54

www IN A 10.31.248.53 ; association pour le nom de machine www
```

```
smtp IN A 10.31.248.53 ; association pour le nom de machine smtp

web IN CNAME www ; alias pour la machine www
```

Configuration serveur DNS Secondaire

Fichier conf dans **/etc/bind/gsb.org** :

```
@ IN SOA ns1.gsb.org. root.gsb.org. (
2021012201      ; numéro de série important pour les secondaires
43200           ; temps de rafraîchissement des secondaires
3600            ; temps d'attente entre deux tentatives de mise à jour pour les secondair
3600000         ; Temps après lequel le serveur secondaire ne répond plus aux requêtes lc
172800 )        ; ttl de mise en cache



@ IN A 10.31.248.53         ;
@ IN NS ns1.gsb.org.       ; déclaration serveurs de noms principaux et secondaires
@ IN NS ns2                ; serveur dns secondaire

ns1 IN A 10.31.248.53        ; association pour le nom de machine ns1.m2l.org
ns2 IN A 10.31.248.54      ; serveur secondaire
smtp IN A 10.31.248.53       ; association pour le nom smtp
ftp IN A 10.31.248.53        ; association pour le serveur ftp

console IN CNAME www        ; alias pour le nom de machine www
```

Fichier **named.conf.local**

```
zone "gsb.org" {
        type slave;
        file "/var/lib/bind/db.gsb.org";
        masters { 10.31.248.53; };
};


// Déclaration dune seconde zone gérée par le DNS
zone "afrique.gsb.org" IN {
       type slave;
       file "/var/lib/bind/db.afrique.gsb.org";
        masters { 10.31.248.53; };
};

zone "248.31.10.in-addr.arpa"  {
        type slave;
        file "/var/lib/bind/db.248.31.10.in-addr.arpa";
        masters { 10.31.248.53; };
};

zone "240.31.10.in-addr.arpa"  {
        type slave;
```

```
        file "/var/lib/bind/db.240.31.10.in-addr.arpa";
        masters { 10.31.248.53; };
};
```

Fichier **named.conf.options**

```
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.
         allow-query { any; };
         forwarders { 8.8.8.8; 8.8.4.4; };
         forward only;

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
```

Mise en place de la résolution inverse

Qu'est ce qu'un **Reverse DNS** ?

La résolution DNS inverse comme son nom l'indique consiste à réaliser l'opération inverse de la résolution d'adresse. Il s'agit de retrouver un FQDN à partir d'une adresse IP.

La résolution inverse est très utile voire indispensable dans certains cas. La majorité des serveurs mails refuseront tout courrier provenant d'une adresse IP pour laquelle la résolution inverse n'est pas possible.

Donc si vous souhaitez installer un serveur de messagerie pour votre domaine, vous devez configurer le DNS inverse.

Modification du fichier **named.conf.local** :

```
zone "248.31.10.in-addr.arpa" {
        type master;
```

```
        file "/etc/bind/db.248.31.10.in-addr.arpa";
};
```

Pour le nommage du fichier il suffit de taper notre ip à l'envers sans taper le "**.53**" (on le rajoutera dans le fichier conf juste après).

Ensuite on créer le fichier "**db.248.31.10.in-addr.arpa**" dans lequel se trouve :

```
$TTL 3D
@ IN SOA 248.31.10. root.248.31.10. (
 199609206 ; Serial
 28800 ; Refresh
 7200 ; Retry
 604800 ; Expire
 86400) ; Minimum TTL

;Les serveurs de noms
        NS      gsb.org.

;
; Servers

53 PTR gsb.org.
```

Sur la ligne "**;Les serveurs de noms**", il doit y avoir une tabulation avant et après le "**NS**". NE PAS OUBLIER LES " **.** ".

Même chose pour le sous-réseau **X.X.240.53**. → Modification du **named.conf.local**

```
zone "240.31.10.in-addr.arpa" {
        type slave;
        file "/etc/bind/db.240.31.10.in-addr.arpa";
        masters {10.31.248.53; };
};
```

Ensuite on créer un autre fichier "**db.240.31.10.in-addr.arpa**" :

```
$TTL 3D
```

```
@ IN SOA 240.31.10. root.240.31.10. (
 199609206 ; Serial
 28800 ; Refresh
 7200 ; Retry
 604800 ; Expire
 86400) ; Minimum TTL

;Les serveurs de noms
        NS      gsb.org.

;
; Servers

53 PTR gsb.org.
```

Ensuite on test

Tests

Vérification des configurations

Avant de lancer un serveur suite à une modification, on peut prendre la précaution de tester les configurations des fichiers.

Commande	Rôle
named-checkconf	teste la validité des déclarations de zone (fichier named.conf et fichier de déclaration named.conf.local, named.conf.default-zones, etc).
named-checkzone	Teste la validité d'une zone à partir de son fichier de configuration named-checkzone nomZone cheminFichierZone

Test DNS primaire avec **Dig ns gsb.org @localhost**

```
root@dns-prim:/etc/bind# dig ns1 gsb.org @10.31.248.53

; <<>> DiG 9.16.15-Debian <<>> ns1 gsb.org @10.31.248.53
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 59771
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;ns1.                           IN      A

;; AUTHORITY SECTION:
.                       86399   IN      SOA     a.root-servers.net. nstld.verisign-grs.com. 2021100401 1800 900 604800 86400

;; Query time: 24 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: mar. oct. 05 11:17:01 CEST 2021
;; MSG SIZE  rcvd: 107

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59692
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 78db1570104eb5ad01000000615c180dedc75c581ca6bf5d (good)
;; QUESTION SECTION:
;gsb.org.                       IN      A

;; ANSWER SECTION:
gsb.org.                604800  IN      A       10.31.248.53

;; Query time: 0 msec
;; SERVER: 10.31.248.53#53(10.31.248.53)
;; WHEN: mar. oct. 05 11:17:01 CEST 2021
;; MSG SIZE  rcvd: 80
```

```
named-checkconf -z named.conf.local
```

```
root@dns-prim:/etc/bind# named-checkconf -z named.conf.local
zone gsb.org/IN: loaded serial 202100401
/etc/bind/db.afrique.gsb.org:1: no TTL specified; using SOA MINTTL instead
zone afrique.gsb.org/IN: loaded serial 2020091401
```

```
named-checkzone gsb.org db.gsb.org
```

```
root@dns-prim:/etc/bind# named-checkzone gsb.org db.gsb.org
zone gsb.org/IN: afrique.gsb.org/NS 'ns1.afrique.gsb.org' (out of zone) has no addresses records (A or AAAA)
zone gsb.org/IN: asie.gsb.org/NS 'ns1.asie.gsb.org' (out of zone) has no addresses records (A or AAAA)
zone gsb.org/IN: europe.gsb.org/NS 'ns1.europe.gsb.org' (out of zone) has no addresses records (A or AAAA)
zone gsb.org/IN: usa.gsb.org/NS 'ns1.usa.gsb.org' (out of zone) has no addresses records (A or AAAA)
zone gsb.org/IN: loaded serial 202100401
OK
```

Test de résolution **dns inverse (côté primaire)**:

```
root@dns-prim:/etc/bind# dig -x 10.31.248.53 @localhost

; <<>> DiG 9.16.15-Debian <<>> -x 10.31.248.53 @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34679
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 124d735e015a8e2f01000000615c67eda720a3e2339f389a (good)
;; QUESTION SECTION:
;53.248.31.10.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
53.248.31.10.in-addr.arpa. 259200 IN    PTR     gsb.org.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: mar. oct. 05 16:57:49 CEST 2021
;; MSG SIZE  rcvd: 103

root@dns-prim:/etc/bind# dig -x 10.31.240.53 @localhost

; <<>> DiG 9.16.15-Debian <<>> -x 10.31.240.53 @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52121
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 15c5c383c66618fd01000000615c67fb393aa00e0c584682 (good)
;; QUESTION SECTION:
;53.240.31.10.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
53.240.31.10.in-addr.arpa. 259200 IN    PTR     gsb.org.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: mar. oct. 05 16:58:03 CEST 2021
;; MSG SIZE  rcvd: 103

root@dns-prim:/etc/bind#
```

Test de résolution **dns inverse (côté secondaire)**:

```
root@dns-sec:/etc/bind# dig -x 10.31.248.53 @localhost

; <<>> DiG 9.16.15-Debian <<>> -x 10.31.248.53 @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27218
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 23a28a6f388b2f0301000000615c68af76f3e5edaa422e1d (good)
;; QUESTION SECTION:
;53.248.31.10.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
53.248.31.10.in-addr.arpa. 259200 IN    PTR     gsb.org.

;; Query time: 4 msec
;; SERVER: ::1#53(::1)
;; WHEN: mar. oct. 05 17:01:03 CEST 2021
;; MSG SIZE  rcvd: 103

root@dns-sec:/etc/bind# dig -x 10.31.240.53 @localhost

; <<>> DiG 9.16.15-Debian <<>> -x 10.31.240.53 @localhost
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56671
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 752cd9d7868287360100000615c68b4d3eee470941e118b (good)
;; QUESTION SECTION:
;53.240.31.10.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
53.240.31.10.in-addr.arpa. 259200 IN    PTR     gsb.org.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: mar. oct. 05 17:01:08 CEST 2021
;; MSG SIZE  rcvd: 103
```

Pour éviter d'avoir à taper "@localhost" il suffit de changer dans **/etc/resolv.conf**, le "**nameserver 8.8.8.8**" en "**nameserver 10.31.248.53**"

Grille de tests

Afin de vérifier le bon fonctionnement des services il faut :
Vérifier les configurations :

```
named-checkconf
named-checkzone
dig ns afrique.gsb.org
dig a www.afrique.gsb.org
dig mx afrique.gsb.org
```

Productions attendues

- Configuration du serveur DNS principal (Master)
- Configuration du serveur DNS secondaire (Slave)
- Mise en place de la résolution inverse
- Grille de test de validation du service.