DNS

Un DNS (Domain Name Server) est un serveur par lequel une adresse IP (Internet Protocol) est convertie sur un ordinateur ou un autre dispositif connecté en un nom de domaine lisible par l'homme.

DNS Master

Le principe de master (maître) est de contrôler la zone, il possède le fichier “original”.

Création du conteneur

On crée un nouveau conteneur, sur les serveurs DHCP dans les fichier */etc/dhcp/dhcpd.conf* on rajoute ceci sous *use-host-decl-names true;* de la partie DMZ :

```
host ns1-pub {
                        hardware ethernet bc:24:11:fe:8d:06;
                        fixed-address 10.31.216.53;
                }
```

Sur le DNS, on met la machine en mode **dhcp** dans le fichier */etc/network/interfaces*.

```
systemctl restart networking
```

On nomme notre machine **ns1-pub**.

```
hostnamectl set-hostname ns1-pub
```

Installation du service DNS

Nous utiliserons le service d'ISC, bind9.

```
apt update
apt install bind9
```

Configuration du DNS

Dans le fichier */etc/bind/named.conf.local* on écrit ceci :

```
# Declaration de nos zones
zone "gsb.org" IN {
        type master;
        file "/etc/bind/db.gsb.org";
```

```
        allow-transfer { 10.31.216.54; };
        notify yes;
};

zone "oceanie.gsb.org" IN {
        type master;
        file "/etc/bind/db.oceanie.gsb.org";
        allow-transfer { 10.31.216.54; };
        notify yes;
};

#Declaration des autres zones
zone "asie.gsb.org" IN {
        type forward;
        forwarders {10.31.184.53;};
};

zone "europe.gsb.org" IN {
        type forward;
        forwarders {10.31.200.53;};
};

zone "afrique.gsb.org" IN {
        type forward;
        forwarders {10.31.232.53;};
};

zone "usa.gsb.org" IN {
        type forward;
        forwarders {10.31.248.53;};
};
```

Dans le fichier */etc/bind/named.conf.options* on écrit ceci :

```
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.

        // forwarders {
        //      0.0.0.0;
        // };

//========================================================================
```

```
        // 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 no;
        allow-query { any; };
        recursion yes;
        forwarders { 8.8.8.8; 8.8.4.4; };
        forward only;
        listen-on-v6 { any; };
};
```

Nous allons maintenant décrire notre zone **gsb.org** en créant ce fichier :

```
nano /etc/bind/db.gsb.org
```

Nous allons écrire :

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

@ IN SOA gsb.org. root.gsb.org. (
; serial number (pour les secondaires)
2024100101
; refresh - temps de mise a jour du slave
3600
; retry delai d attente avant 2eme demande si le master est down
600
; expire - temps durant lequel le slave tentera de contacter le master
2419200
; min - validite du cache
604800 )

@ IN NS ns1.gsb.org.
@ IN NS ns2.gsb.org.
ns1 IN A 10.31.216.53
ns2 IN A 10.31.216.54

; Associations
@ IN A 10.31.216.80
www IN A 10.31.216.80

; Seconde zone (meme DNS)
$ORIGIN oceanie.gsb.org.
@ 86400 IN NS ns1.oceanie.gsb.org.
@ 86400 IN NS ns2.oceanie.gsb.org.
ns1.oceanie.gsb.org. IN A 10.31.216.53
ns2.oceanie.gsb.org. IN A 10.31.216.54

; Delegations
```

```
$ORIGIN afrique.gsb.org.
@ 86400 IN NS ns1.afrique.gsb.org.
@ 86400 IN NS ns2.afrique.gsb.org.
ns1.afrique.gsb.org. IN A 10.31.232.53
ns2.afrique.gsb.org. IN A 10.31.232.54

$ORIGIN asie.gsb.org.
@ 86400 IN NS ns1.asie.gsb.org.
@ 86400 IN NS ns2.asie.gsb.org.
ns1.asie.gsb.org. IN A 10.31.184.53
ns2.asie.gsb.org. IN A 10.31.184.54

$ORIGIN europe.gsb.org.
@ 86400 IN NS ns1.europe.gsb.org.
@ 86400 IN NS ns2.europe.gsb.org.
ns1.europe.gsb.org. IN A 10.31.200.53
ns2.europe.gsb.org. IN A 10.31.200.54

$ORIGIN usa.gsb.org.
@ 86400 IN NS ns1.usa.gsb.org.
@ 86400 IN NS ns2.usa.gsb.org.
ns1.usa.gsb.org. IN A 10.31.248.53
ns2.usa.gsb.org. IN A 10.31.248.54
```

Nous allons décrire la zone oceanie.gsb.org

```
nano /etc/bind/db.oceanie.gsb.org
```

On y écrit :

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

@ IN SOA oceanie.gsb.org. root.oceanie.gsb.org. (
; serial number (pour les secondaires)
2024100101
; refresh - temps de mise a jour du slave
3600
; retry delai d attente avant 2eme demande si le master est down
600
; expire - temps durant lequel le slave tentera de contacter le master
2419200
; min - validite du cache
604800 )

@ IN A 10.31.216.80
@ IN NS ns1.oceanie.gsb.org.
@ IN NS ns2.oceanie.gsb.org.
ns1 IN A 10.31.216.53
ns2 IN A 10.31.216.54
```

```
www IN A 10.31.216.80

; Seconde zone (meme DNS)
$ORIGIN gsb.org.
@ 86400 IN NS ns1.gsb.org.
ns1.gsb.org. IN A 10.31.216.53
ns2.gsb.org. IN A 10.31.216.53
```

```
systemctl restart bind9
```

DNS Slave

Le serveur dit slave (esclave) est celui qui reçoit la zone depuis un serveur master. Ce concept de master/slave permet de redonder une zone bien plus facilement que si on le faisait manuellement.

Création du conteneur

On crée un nouveau conteneur, sur les serveurs DHCP dans les fichier */etc/dhcp/dhcpd.conf* on rajoute ceci sous *use-host-decl-names true;* de la partie DMZ :

```
host ns2-pub {
                        hardware ethernet bc:24:11:b5:50:20;
                        fixed-address 10.31.216.54;
                }
```

Sur le DNS, on met la machine en mode **dhcp** dans le fichier */etc/network/interfaces*.

```
systemctl restart networking
```

On nomme notre machine **ns2-pub**.

```
hostnamectl set-hostname ns1-pub
```

Installation du service DNS

Nous utiliserons le service d'ISC, bind9.

```
apt update
apt install bind9
```

Configuration du DNS

Dans le fichier */etc/bind/named.conf.local* on écrit :

```
# Declaration de nos zones
```

```
zone "gsb.org" IN {
        type slave;
        file "/var/lib/db.gsb.org";
        masters {10.31.216.53;};
};

zone "oceanie.gsb.org" IN {
        type slave;
        file "/var/lib/db.oceanie.gsb.org";
        masters {10.31.216.53;};
};

#Declaration des autres zones
zone "asie.gsb.org" IN {
        type forward;
        forwarders {10.31.184.53;};
};

zone "europe.gsb.org" IN {
        type forward;
        forwarders {10.31.200.53;};
};

zone "afrique.gsb.org" IN {
        type forward;
        forwarders {10.31.232.53;};
};

zone "usa.gsb.org" IN {
        type forward;
        forwarders {10.31.248.53;};
};
```

Dans le fichier */etc/bind/named.conf.options* on écrit :

```
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.

        // forwarders {
        //      0.0.0.0;
        // };
```

```
//========================================================================
        // 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 no;
        allow-query { any; };
        recursion yes;
        forwarders { 8.8.8.8; 8.8.4.4; };
        forward only;
        listen-on-v6 { any; };
};
```

```
systemctl restart bind9
```

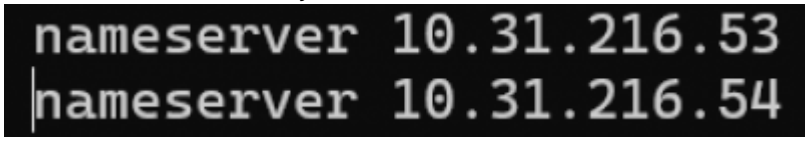
Finalisation

Revenons sur **ns1-pub**, dans le fichier */etc/bind/db.gsb.org* ajoutons 1 au **serial number**. Cela va être détecter par le **ns2-pub** et le mettre à jour.
Enfin redémarrons le service bind9 sur les 2 machines.

```
systemctl restart bind9
```

Tests

Nous allons maintenant procéder aux tests, pour ça on peut créer un nouveau conteneur.
On se rend dans le fichier */etc/resolv.conf*, on change le **nameserver 8.8.8.8** en **nameserver 10.31.216.53** et on ajoute **nameserver 10.31.216.54**.



Nous allons utiliser la commande **dig** pour voir si le serveur DNS répond et répond bien.
gsb - DNS master

```
dig A gsb.org @10.31.216.53
```

```
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> A gsb.org @10.31.216.53
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 153
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 822b9628a8bf7dce0100000066ff93f00c8da3c7500c6c7b (good)
;; QUESTION SECTION:
;gsb.org.                       IN      A

;; ANSWER SECTION:
gsb.org.                604800  IN      A       10.31.216.80

;; Query time: 0 msec
;; SERVER: 10.31.216.53#53(10.31.216.53) (UDP)
;; WHEN: Fri Oct 04 07:06:24 UTC 2024
;; MSG SIZE  rcvd: 80
```

gsb - DNS slave

```
dig A gsb.org @10.31.216.54
```

```
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> A gsb.org @10.31.216.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53265
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4a0f65fcb19824f90100000066ff941936a0f929dee6608c (good)
;; QUESTION SECTION:
;gsb.org.                       IN      A

;; ANSWER SECTION:
gsb.org.                604800  IN      A       10.31.216.80

;; Query time: 0 msec
;; SERVER: 10.31.216.54#53(10.31.216.54) (UDP)
;; WHEN: Fri Oct 04 07:07:05 UTC 2024
;; MSG SIZE  rcvd: 80
```

oceanie.gsb - DNS master

```
dig A oceanie.gsb.org @10.31.216.53
```

```
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> A oceanie.gsb.org @10.31.216.53
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60027
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 268975678d04e2190100000066ff943f9a353299830cddfa (good)
;; QUESTION SECTION:
;oceanie.gsb.org.               IN      A

;; ANSWER SECTION:
oceanie.gsb.org.        604800  IN      A       10.31.216.80

;; Query time: 0 msec
;; SERVER: 10.31.216.53#53(10.31.216.53) (UDP)
;; WHEN: Fri Oct 04 07:07:43 UTC 2024
;; MSG SIZE  rcvd: 88
```

oceanie.gsb - DNS slave

```
dig A oceanie.gsb.org @10.31.216.54
```

```
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> A oceanie.gsb.org @10.31.216.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30995
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d1d2185171d762d50100000066ff946b113e13623bac9297 (good)
;; QUESTION SECTION:
;oceanie.gsb.org.               IN      A

;; ANSWER SECTION:
oceanie.gsb.org.        604800  IN      A       10.31.216.80

;; Query time: 1 msec
;; SERVER: 10.31.216.54#53(10.31.216.54) (UDP)
;; WHEN: Fri Oct 04 07:08:27 UTC 2024
;; MSG SIZE  rcvd: 88
```

autre_zone.gsb - DNS master

```
dig A afrique.gsb.org @10.31.216.53
```

```
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> A afrique.gsb.org @10.31.216.53
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41459
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ba56442541251a8a0100000066ff94e5740b15134a0c61f3 (good)
;; QUESTION SECTION:
;afrique.gsb.org.               IN      A

;; ANSWER SECTION:
afrique.gsb.org.        520350  IN      A       10.31.232.80

;; Query time: 0 msec
;; SERVER: 10.31.216.53#53(10.31.216.53) (UDP)
;; WHEN: Fri Oct 04 07:10:29 UTC 2024
;; MSG SIZE  rcvd: 88
```

autre_zone.gsb - DNS slave

```
dig A afrique.gsb.org @10.31.216.54
```

```
; <<>> DiG 9.18.28-1~deb12u2-Debian <<>> A afrique.gsb.org @10.31.216.54
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26931
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: cc1d9f2d185979dd0100000066ff950672161db6aae9e907 (good)
;; QUESTION SECTION:
;afrique.gsb.org.               IN      A

;; ANSWER SECTION:
afrique.gsb.org.        604800  IN      A       10.31.232.80

;; Query time: 2 msec
;; SERVER: 10.31.216.54#53(10.31.216.54) (UDP)
;; WHEN: Fri Oct 04 07:11:02 UTC 2024
;; MSG SIZE  rcvd: 88
```