

MISSION 8: SERVEUR DNS

0.PREREQUIS

Cette année nous allons installer un serveur DNS , avec 2 zones différentes mais aussi **Une résolution inverse** Je vous laisse découvrir notre production .

Nous allons l'installer sur le réseau public (DMZ) , nous aurons besoin d'un DNS primaire (ns1-pub) et un DNS secondaire (ns2-pub) sur le réseau public .

I.Configuration du serveur DNS principal (Master)

1.1 CLONE ET MODIFICATION DU CONTENEUR TEMPLATE

Nous utilisons proxmox , et c'est là où se déroulera toutes nos actions . On a clone le Template puis on a modifié son adresse IP dans **Réseau**

Contenu du /etc/network/interfaces de ns1-pub

ID ↑	Name	Bridge	Firewall	VLAN Tag	MAC address	IP address	Gateway	MTU
net0	eth0	virtbr1	Yes		BC:24:11:CE...	10.31.216.53/22	10.31.219.254	

1.2 Procédure d'installation du paquetage bind9

```
apt update
apt install bind9 dnsutils
```

```
root@DNS:~# apt install bind9 dnsutils
Note, selecting 'bind9-dnsutils' instead of 'dnsutils'
bind9-dnsutils is already the newest version (1:9.20.11-4).
Installing:
  bind9

Installing dependencies:
  bind9-utils dns-root-data

Suggested packages:
  bind9-doc resolvconf ufw

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 0
  Download size: 442 kB
```

1.3 Déclarer les zones à gérer dans named.conf.local avec le type « master »

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

zone "gsb.org" IN {
    type master;
    file "/etc/bind/db.gsb.org";
```

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

1.3 La récursion dans named.conf.options

```
options {
    directory "/var/cache/bind";
    allow-query{ any; };
    recursion yes;
    forwarders { 8.8.8.8 ; 8.8.4.4; };
    forward only ;
    dnssec-validation no;
} ;
```

1.4 Configuration du fichier db.oceanie.gsb.org

```
$TTL 604800;
@ IN SOA ns1-pub.oceanie.gsb.org. root.oceanie.gsb.org. (
    2020122601;
    43200;
    3600;
    3600000;
    172800 ) ;
@ IN A 10.31.216.80 ;
@ IN NS ns1-pub.oceanie.gsb.org. ;
@ IN NS ns2-pub.oceanie.gsb.org. ;

ns1-pub IN A 10.31.216.53 ;
ns2-pub IN A 10.31.216.54 ;
www IN A 10.31.216.80 ;
console IN CNAME www
```

1.5 Configuration du fichier db.gsb.org

```
$TTL 604800;
@ IN SOA ns1-pub.gsb.org. root.gsb.org. (
    2020122601;
    43200;
    3600;
    3600000;
    172800 ) ;
@ IN A 10.31.216.80 ;
@ IN NS ns1-pub.gsb.org. ;
@ IN NS ns2-pub.gsb.org. ;

ns1-pub IN A 10.31.216.53 ;
ns2-pub IN A 10.31.216.54 ;
www IN A 10.31.216.80 ;
console IN CNAME www
```

```
$ORIGIN europe.gsb.org.
@ 86400 IN NS ns1.europe.gsb.org.
ns1.europe.gsb.org IN A 10.31.200.53 ;

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

$ORIGIN usa.gsb.org.
@ 86400 IN NS ns1.usa.gsb.org.
ns1.usa.gsb.org IN A 10.31.248.53 ;

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

1.6 Téléchargement DU PACKAGE RSYSLOG

```
apt install rsyslog
```

1.7 Les Forwarders

Un forwarder est un DNS relais :

Si le serveur DNS ne connaît pas une réponse (pas dans ses zones, ni en cache), il redirige la requête vers un autre serveur DNS pour qu'il fasse la résolution à sa place. Exemple : Google DNS (8.8.8.8, 8.8.4.4) ou le DNS d'un autre groupe. Pourquoi ?

Gain de performance : Le DNS local n'a pas besoin de parcourir tout l'Internet (résolution récursive complète), il délègue ainsi on peut renvoyer certaines requêtes vers d'autres serveurs spécifiques (exemple : Europe, Afrique, USA, etc.).

Comment ça marche ?

Dans le fichier de conf, on ajoutes ce bloc

```
nano /etc/bind/named.conf.local
```

```
zone "gsb.org" {
    type master;
    file "/etc/bind/db.gsb.org";
    allow-transfer { 10.31.216.64; }; // autorise le secondaire
};

zone "oceanie.gsb.org" {
    type master;
    file "/etc/bind/db.oceanie.gsb.org";
    allow-transfer { 10.31.216.64; }; // secondaire
};

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

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

zone "asie.gsb.org" {
    type forward;
    forwarders { 10.31.184.53; };
};

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

Ainsi si notre DNS receoit une requete qui ne lui est pas destiné, mais plutot destiné a une un autre DNS il le lui enverra.

1.8 Test de Nos Serveurs DNS

II.Configuration du serveur DNS secondaire (slave)

Le DNS Secondaire (Slave)

Principe Le slave est une copie de secours du master.

Nous allons cloner le template DMZ et y attribué une adresse ip valide ici 10.31.216.53 Il ne possède pas directement la configuration des zones (pas de fichiers de zone complets écrits à la main).

Il récupère automatiquement la zone depuis le serveur maître (master) grâce à un mécanisme appelé zone transfer .

Pourquoi ?

Redondance : si le master tombe en panne, le slave peut continuer à répondre aux requêtes. Répartition de charge : plusieurs serveurs DNS répondent aux clients, ça évite de saturer un seul \\\server. Disponibilité : dans un réseau distribué, certains clients peuvent interroger plus rapidement le slave que le master.

Comment ça marche ? Le slave a une configuration qui n'a besoin que de deux fichier(mais avant cela on installe d'abord bind 9 :

```
apt install bind9 dnsutils
```

On commence par configiurer le premier fichier

CONFIGURATION NAMED.CONF.OPTIONS

```
nano /etc/bind/named.conf.options
```

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

```
dnssec-validation no;
allow-query { any; };
recursion yes ;
forwarders { 8.8.8.8 ; 8.8.4.4; };
forward only;
};
```

CONFIGURATION NAMED.CONF.LOCAL

Ensuite on modifie le

```
nano /etc/bind/named.conf.local
```

```
zone "gsb.org" IN {
    type slave;
    file "/var/lib/bind/db.gsb.org";
    masters { 10.31.208.63; };
};

zone "oceanie.gsb.org" IN {
    type slave;
    file "/var/lib/bind/db.oceanie.gsb.org";
    masters { 10.31.208.63; };
};
```

Ici :

masters = adresse du master (ns3-pub).

file = où sera stockée la copie locale de la zone (générée automatiquement).

Quand le slave voit que le serial number de la zone a changé sur le master → il refait une copie.

Téléchargement DU PACKAGE RSYSLOG

```
apt install rsyslog
```

From:

<https://sisr2.beaupeyrat.com/> - Documentations SIO2 option SISR

Permanent link:

https://sisr2.beaupeyrat.com/doku.php?id=sisr2-oceanie:installation_serveur_dns



Last update: **2025/11/05 08:50**