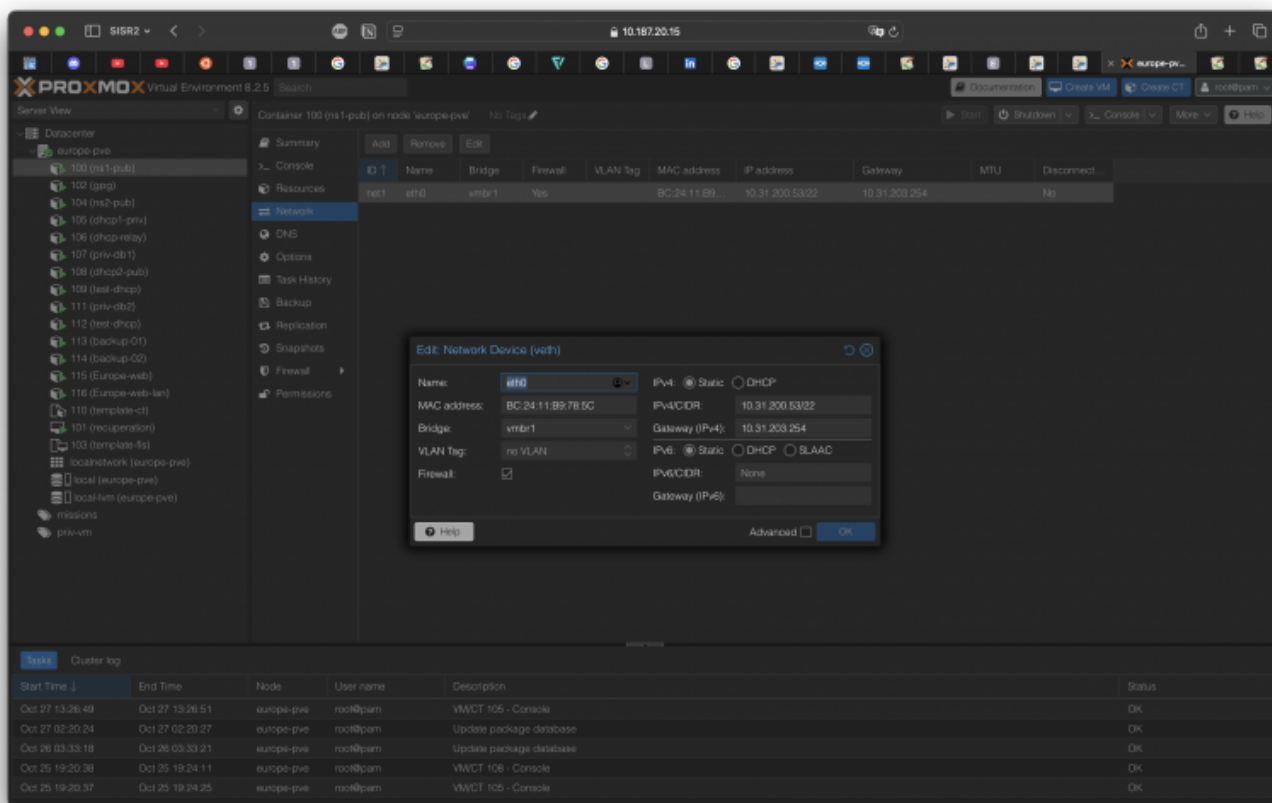


Installation des services et création de la zone

Configuration Interface réseau du DNS publique *ns1-pub*

Sur proxmox on crée a dupliqué a partir du *template* et qu'on a renommé *ns1-pub* On a configuré les interfaces du serveur DNS directement sur l'hyperviseur Proxmox



- **Bridge** : vmbr1 (celle de la DMZ)
- **IPv4** : 10.31.200.53/22
- **Gateway** : 10.31.203.254

Installation du paquetage BIND

Et enfin, on a installé le paquetage **bind9 bind9utils dnsutils** et **rsyslog** avec les commandes suivantes :

```
apt update
apt install bind9
apt install bind9utils
apt install dnsutils
apt install rsyslog
```

Explication

bind9 :

- Fonction principale : BIND (Berkeley Internet Name Domain) est un serveur DNS open-source. Il est utilisé pour résoudre les noms de domaine en adresses IP et vice versa.
- Rôle : BIND est essentiellement le serveur DNS, **responsable de la résolution des requêtes DNS**, du **stockage des enregistrements DNS** et de **la gestion des zones**.

bind9utils :

- Fonction principale : Ce paquet contient divers utilitaires et outils associés au serveur BIND.
- Rôle : Il fournit des **outils de gestion**, de **maintenance** et de **configuration pour le serveur BIND**. Certains outils peuvent être utilisés pour la gestion des zones, la configuration du serveur et la vérification de son état.

dnsutils :

- Fonction principale : Le paquet dnsutils comprend plusieurs outils liés à la résolution de noms de domaine et au diagnostic du DNS.
- Rôle : Il inclut des utilitaires tels que **dig** (domain information groper) et **nslookup** qui permettent d'interroger des serveurs DNS, de récupérer des informations sur les enregistrements DNS, et de diagnostiquer des problèmes liés au DNS.

rsyslog :

- Fonction principale : rsyslog est un démon de journalisation du système.
- Rôle : Il est utilisé pour la gestion et la centralisation des journaux système. rsyslog collecte les messages de journal générés par divers composants du système d'exploitation et les enregistre ou les transmet vers des destinations spécifiées. Il facilite la **surveillance** et le **dépannage** des systèmes en stockant les journaux de manière centralisée.

En résumé, bind9 est le serveur DNS, bind9utils fournit des outils liés à la gestion du serveur BIND, dnsutils offre des utilitaires pour la résolution de noms de domaine et le diagnostic DNS, et rsyslog est utilisé pour la gestion des journaux système. Ces outils sont souvent utilisés en combinaison pour configurer, gérer et surveiller efficacement les services DNS sur un système.

Configurer le bind

Nous avons installé le paquetage **Bind(Berkeley Internet Name Domain)** il faut maintenant le configurer les fichiers suivants:

1. [/etc/bind/named.conf.options](#)
2. [/etc/bind/named.conf.local](#)
3. [/etc/bind/db.m2l.org](#) ← le fichier de zone

Le fichier /etc/bind/named.conf.options:

Nous avons configuré ce fichier comme ceci :

```
root@ns1-pub:~# cat /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
    allow-query { any; };
    recursion yes;
    forwarders { 8.8.8.8; 8.8.4.4; };
    forward only;
};
```

Explications

Ce fichier, **/etc/bind/named.conf.options**, contient les options de configuration globales pour le serveur BIND (Berkeley Internet Name Domain) sur un système Debian. Voici une explication ligne par ligne :

options { : C'est le début de la section où vous spécifiez diverses options de configuration pour le serveur BIND.

directory "/var/cache/bind"; : Cette ligne spécifie le **répertoire dans lequel BIND stockera ses données temporaires**. Dans ce cas, les données temporaires seront stockées dans le répertoire `/var/cache/bind`.

dnssec-validation no; : Cette option désactive la validation DNSSEC (Domain Name System Security Extensions). DNSSEC est un ensemble de extensions de sécurité pour le DNS. Dans ce cas, la validation DNSSEC est désactivée (no).

allow-query { any; }; : Cette option autorise les requêtes DNS à être traitées par ce serveur BIND depuis n'importe quelle adresse IP (any). Cela signifie que le serveur BIND acceptera les requêtes de n'importe quelle source.

recursion yes; : Cette option active la récursivité sur le serveur BIND. Cela signifie que le serveur BIND est autorisé à effectuer des requêtes récursives pour les clients.

forwarders { 8.8.8.8; 8.8.4.4; }; : Cette ligne spécifie les serveurs DNS vers lesquels le serveur BIND va transmettre les requêtes DNS qui ne peuvent pas être résolues localement. Dans cet exemple, les serveurs DNS de Google (8.8.8.8 et 8.8.4.4) sont utilisés comme serveurs de redirection.

forward only; : Cette option indique que le serveur BIND doit agir uniquement en tant que serveur de transfert de requêtes vers les serveurs spécifiés dans forwarders.

}; : Marque la **fin** de la section des options de configuration BIND.

Le fichier /etc/bind/named.conf.local

Nous avons configuré ce fichier comme ceci :

```
root@ns1-pub:~# cat /etc/bind/named.conf.local
zone "europe.gsb.org" {
    type master;
```

```
    file "/etc/bind/db.europe.gsb.org";
    allow-transfer { 10.31.200.53; 10.31.200.54; };
    notify yes;
};

zone "gsb.org" {
    type master;
    file "/etc/bind/db.gsb.org";
    allow-transfer { 10.31.200.53; 10.31.200.54; };
    notify yes;
};

zone "asie.gsb.org" IN {
    type forward;
    forwarders { 10.31.184.53; 10.31.184.54; };
};

zone "oceanie.gsb.org" IN {
    type forward;
    forwarders { 10.31.216.53; 10.31.216.54; };
};

zone "afrique.gsb.org" IN {
    type forward;
    forwarders { 10.31.232.53; 10.31.232.54; };
};

zone "usa.gsb.org" IN {
    type forward;
    forwarders { 10.31.248.53; 10.31.248.54; };
};
```

Explications

Ce fichier, `/etc/bind/named.conf.local`, contient des déclarations de zone pour les domaine "gsb.org" dans le serveur DNS BIND sur un système Debian. Voici une explication ligne par ligne :

`zone "europe.gsb.org"` : Déclare une zone pour le domaine "m2l.org". Les configurations spécifiques pour cette zone seront incluses entre les accolades ouvrantes et fermantes.

`type master` : Spécifie que ce serveur BIND est le serveur principal (**master**) pour la zone "m2l.org". Cela signifie qu'il est autorisé à mettre à jour les enregistrements de cette zone et à répondre aux requêtes pour cette zone.

`file "/etc/bind/db.europe.gsb.org"` : Indique le chemin du fichier de zone associé à "m2l.org". Dans ce cas, le fichier de zone est situé à `/etc/bind/db.m2l.org`. Ce fichier contient **les enregistrements DNS spécifiques pour la zone "m2l.org"**.

`allow-transfer { 10.31.200.53; 10.31.200.54; }` : Spécifie les adresses IP autorisées

à effectuer un transfert de zone (zone transfer). Dans cet exemple, le serveur permet le transfert de zone depuis localhost (lui-même) et depuis l'adresse IP 10.31.112.64. Cela permet à d'autres serveurs autorisés de copier la zone.

notify yes; Active la notification de modification de zone. Lorsque des modifications sont apportées à la zone "m2l.org" sur ce serveur, des notifications seront envoyées aux serveurs listés dans la configuration pour les informer des changements.

}; C'est la fin de la déclaration de zone pour "europe.gsb.org".

En résumé, ce fichier indique que le **serveur BIND** sur le système Debian est configuré en tant que serveur principal (master) pour la zone "europe.gsb.org". Il spécifie le fichier de zone, les adresses IP autorisées pour le transfert de zone, et active la notification des modifications de zone.

Le fichier de zone /etc/bind/db.europe.gsb.org

Nous avons configuré ce fichier comme ceci:

```
root@ns1-pub:~# cat /etc/bind/db.europe.gsb.org
$TTL 604800
@ IN SOA europe.gsb.org. root.europe.gsb.org. (
    2024020201 ; serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL

@      IN      A      10.31.200.53
@      IN      NS      ns1.europe.gsb.org.
@      IN      NS      ns2.europe.gsb.org.
@      IN      NS      intranet.europe.gsb.org.
@      IN      NS      docs.europe.gsb.org.

ns1    IN      A      10.31.200.53 ;
ns2    IN      A      10.31.200.54 ;

www    IN      A      10.31.200.80 ;
ftp    IN      A      10.31.200.81 ;
intranet      IN      A      10.31.192.80 ;
docs        IN      A      10.31.192.80 ;
nextcloud   IN      A      10.31.192.80 ;
```

Explications

Ce fragment de code représente une zone de configuration du fichier de zone pour le service DNS BIND. Il définit les **enregistrements pour le domaine "europe.gsb.org"**. Voici une explication ligne par ligne :

\$TTL 604800: Définit la durée de vie par défaut des enregistrements dans cette zone en secondes (604800 secondes ou 7 jours).

@ IN SOA europe.gsb.org. root.europe.gsb.org. (...): Définit l'enregistrement d'autorité de la zone (SOA). Il spécifie des informations sur la gestion de la zone.

europe.gsb.org.: Le nom du domaine principal.

root.europe.gsb.org.: L'adresse email de l'administrateur de la zone (terminée par un point).

(...): Contient des informations supplémentaires, notamment *le numéro de série, le temps de rafraîchissement, le temps de réessai, le délai d'expiration et le TTL négatif*.

@ IN NS ns1.europe.gsb.org.;: Définit le serveur de noms (Name Server) principal pour la zone. Le symbole "@" représente le nom du domaine principal.

ns1 IN A 10.31.200.53 ;: Associe l'adresse IP 10.31.200.53 au nom "**ns1.europe.gsb.org**".

@ IN NS ns2.europe.gsb.org. ;: Définit le deuxième serveur de noms pour la zone.

ns2 IN A 10.31.200.54 ;: Associe l'adresse IP 10.31.112.64 au nom "**ns2.europe.gsb.org**".

www IN A 10.31.200.80 ;: Associe l'adresse IP 10.31.200.80 au sous-domaine "**www.europe.gsb.org**".

ftp IN A 10.31.200.81 ;: Associe également l'adresse IP 10.31.200.81 au sous-domaine "**ftp.europe.gsb.org**".

En résumé, ce code configure une zone DNS pour le domaine "**europe.gsb.org**" avec deux serveurs de noms (**ns1 et ns2**), une entrée pour le sous-domaine "**www**" et une entrée pour le sous-domaine "**ftp**", tous ayant des adresses IP associées.

Le fichier de zone /etc/bind/db.gsb.org

```
$TTL 604800
$ORIGIN gsb.org.
@ IN SOA gsb.org. root.gsb.org. (
    2024020201 ; serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL

@      IN      A      10.31.200.53
@      IN      NS      ns1.gsb.org.
@      IN      NS      ns2.gsb.org.

ns1    IN      A      10.31.200.53 ;
ns2    IN      A      10.31.200.54 ;

www    IN      A      10.31.200.80 ;
ftp    IN      A      10.31.200.81 ;
```

Configurer le slave

Dans le répertoire `/etc/network/interfaces` on configure les adresses pour commencer.

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 10.31.200.54/22
    gateway 10.31.203.254
```

Ensuite on installe Bind9 dans le conteneur slave.

```
apt get install bind9
```

Configuration du fichier **named.conf.local** dans le répertoire **/etc/bind**

```
zone "europe.gsb.org" IN {
    type slave;
    file "/var/lib/bind/db.europe.gsb.com";
    masters { 10.31.200.53; };
};

zone "gsb.org" IN {
    type slave;
    file "/var/lib/bind/db.gsb.org";
    masters { 10.31.200.53; };
};
```

Explications des éléments du fichier de zone

Enregistrements	Rôle
SOA	Définit les indications du Start Of Authority : nom du domaine (ou de la zone) nom de la machine qui est SOA dans ce domaine nom de l'administrateur du domaine numéro de version de fichier, délais pour la synchronisation
NS	Déclare les noms des machines qui sont serveur de noms (principal ou secondaires) pour la zone. Remarque : Ces noms devront en plus être associés à une adresse par un enregistrement A.
A	Déclare les associations entre FQDN et adresse IP. On parle d'un hôte Remarques : un nom non terminé par un point est complété par la zone décrite dans le SOA un nom terminé par un point est un FQDN

MX	Déclare le nom de la ou des machines assurant la fonction de serveur de messagerie pour le domaine. Remarque : Ces noms devront en plus être associés à une adresse par un enregistrement A
CNAME	Canonical Name, permet de déclarer des alias

Vérifications

Configurer bind :

- `/etc/bind/named.conf.local` → déplacer la zone `ml2.org`
- `/etc/bind/named.conf.options` → options de bind
- `/etc/bind/db.2l.org` → base de donnée de la zone d'enregistrement DNS

From:

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

Permanent link:

<https://sisr2.beaupeyrat.com/doku.php?id=sisr2-europe:dns>

Last update: **2024/11/07 10:35**

