Mission 8 : SERVEUR DNS

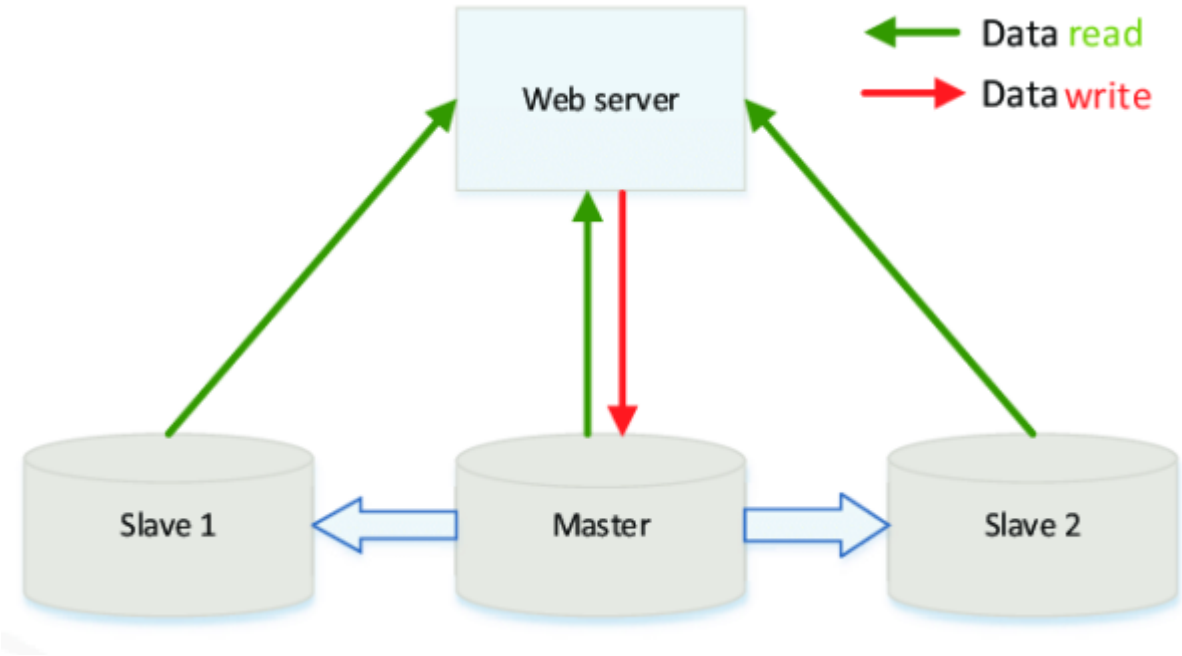
Pré-requis

Afin de pouvoir réaliser cette mission il faut :

- Un serveur sous Debian 13
- Un routeur sous Debian 13
- La configuration IP des deux machines conforme au cahier des charges,
- La configuration DNS des deux machines conforme au cahier des charges,

Introduction

Nous allons installer deux serveur DNS, un dit Master qui est le principal et le Slave qui lui sert a prendre la place du master si le master venait a crash ou avoir des problèmes histoire d'avoir un service fonctionnelle quoi qu'il arrive



Avantage de la réplication Master/Slave :

* Si le serveur DNS master tombe en panne, le slave continue de répondre aux requêtes.
* Les utilisateurs peuvent toujours contacter le domaine.
* Les clients peuvent interroger le slave autant que le master → ça répartit le trafic.
* Un DNS slave sert à garantir que ton domaine reste disponible, rapide et fiable, même si ton master tombe ou est trop sollicité.

Cahier des charges

8.3 Cahier des charges

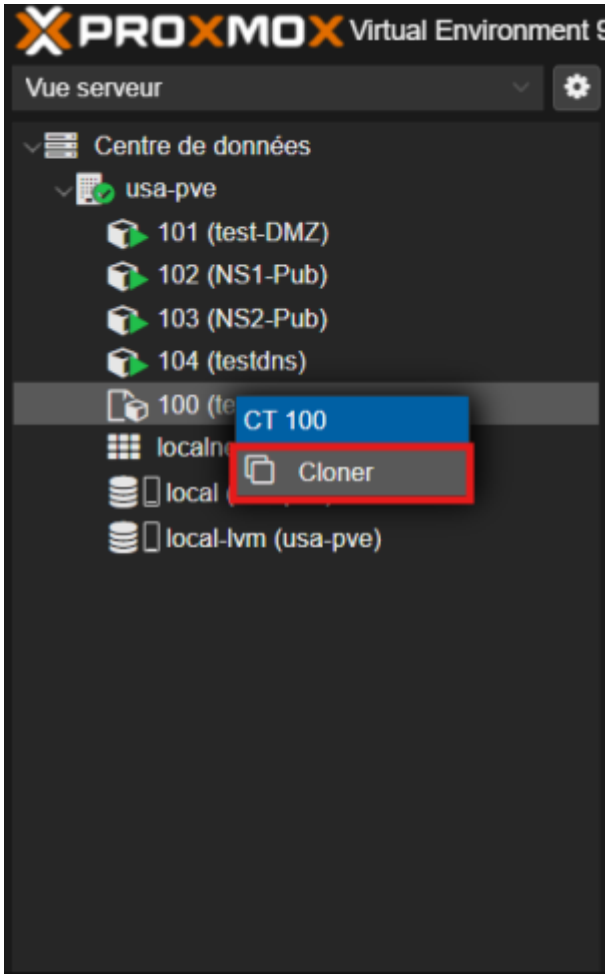
- Le serveur DNS primaire sera installé sur le réseau public
- Le serveur DNS secondaire sera installé sur le réseau public
- Le serveur DNS primaire aura pour nom d'hôte : ns1-pub
- Le serveur DNS secondaire aura pour nom d'hôte : ns2-pub
- Le serveur DNS primaire aura pour adresse IP (réservée) : 10.31.X.53
- Le serveur DNS secondaire aura pour adresse IP (réservée) : 10.31.X.54
- Les zones gérées seront gsb.org et ***zone***.gsb.org (**zone** = usa|afrique|asie|europe|oceanie)
- Les requêtes vers les autres zones devront être transférées aux DNS des autres zones
- Tous les services déjà installés devront avoir un enregistrement A dans la configuration du DNS
- Un enregistrement MX devra être présent pour chaque zone
- Les logs devront être étudiés afin de vérifier le chargement des zones ainsi que les transferts de base entre le serveur primaire et le serveur secondaire.

NS1

création et paramétrage du conteneur NS 1

Création conteneur NS1

Pour commencer nous avons cloné le conteneur Template créé au préalable sur Proxmox pour l'appeler NS1-Pub



Après avoir cloné notre Template il fallait modifier les paramètres IP pour qu'il soit conforme au cahier des charges.
Le cahier des charges nous demande de mettre nos DNS dans la DMZ(Zone démilitarisé) qui dans notre cas et le 3eme sous reseau et donc en 10.31.248.53/54
Je suis donc aller dans le répertoire etc/network pour remplir le fichier interfaces et ainsi mettre ma nouvelle adresse IP

```
nano /etc/network/interfaces
```


```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
        address 10.31.248.53/22
        gateway 10.31.251.254
```

Pour finir la configuration réseau je suis retourner dans le répertoire etc mais cette fois-ci dans le dossier rc.local pour y implanter tout les paramètre réseau nécessaire au bon fonctionnement du centenaire


```
#!/bin/sh -e
ifconfig eth0 10.31.248.53/22 up
route add default gw 172.31.0.1

echo "nameserver 8.8.8.8" > /etc/resolv.conf

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING -j MASQUERADE
```

Important:

Faire un systemctl restart networking a fin de redémarrer le service pour que la machine prennent les nouvelle configuration réseau

Une fois la configuration fini il faut installer tout les services qui vont nous servir pour la mise en place du DNS.

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

Une fois les paquets installé, un répertoire du nom de Bind est apparu dans le répertoire etc. C'est donc dans ce répertoire que tous nos fichier de conf seront

```
cd /etc/bind
```

Dans ce répertoire nous allons créer 3 fichier de configuration

FICHIER DE CONFIGURATION

EXPLIQUATION FICHIER DE CONF

named.conf.local : c'est dans se fichier que nous allons definir nos zones DNS
named.conf.options : Va plus servir a paramétrer notre DNS, vers quelle serveur il envoie les requêtes, quelle adresse il écoute etc
db.gsb.conf : Est le fichier de Zone DNS, c'est la ou on entre toute les zone avec leur SOA

named.conf.local

```
zone "gsb.org" IN {
        type master;
        file "/etc/bind/db.gsb.org";
        allow-transfer { localhost; 10.31.248.54; };
        notify yes;

};
zone "usa.gsb.org" IN {
        type master;
        file "/etc/bind/db.usa.gsb.org";
        allow-transfer { localhost; 10.31.248.54; };
        notify yes;
```

Dans ce fichier est présent 2 zones, la zone gsb.org et la zone usa.gsb.org qui sont 2 zones différentes dont usa.gsb.org qui est le sous domaine de gsb.org

Dans se fichier on peut voir que la Zone est en type Master et qu'elle autorise les transferts avec l'adresse 10.31.248.54 qui est l'adresse du serveur DNS Slave. C'est le même principe avec la zone usa.gsb.org

named.conf.options

```
options {
        directory "/var/cache/bind";
        allow-query{any;};
        recursion yes;
        forwarders { 8.8.8.8; 8.8.4.4; };
        forward only;
};
```

Dans ce fichier on peut voir que le file et le même que dans le fichier named.conf.local car c'est dans ce fichier que bind va travailler et communiquer avec le Slave
Dans la ligne d'en dessous on peut voir allow-query{any;};. Cette ligne veut dire qu'on autorise tout le monde a contacter notre DNS
La troisième ligne va autoriser la récursivité ce qui va permettre a nôtres DNS de pouvoir interrogé d'autre DNS lorsqu'il ne connaitra pas la requêtes
Comme dans le premier fichier la ligne forwarders sert a pouvoir communiquer avec les adresse qui sont mentionné dans notre cas se sont les 2 DNS de google qui vont servir a pouvoir les interroger si notre DNS ne connait pas le requêtes
Et forward only va obliger le DNS a utilisé les ligne forwarders pour communiquer des requêtes externes

db.gsb.conf

Ce fichier est vraiment le noyaux de notre DNS, c'est grace a lui qu'ont va définir tous les enregistrement DNS d'un domaine

```
$TTL 86400
@ IN SOA ns1.gsb.org. root.gsb.org. (
        2005111201;
        43200;
        3600;
        3600000;
        172800 );

@ IN A  10.31.248.80;
@ IN NS ns1.gsb.org. ;
ns1 IN A 10.31.248.53;

www IN A 10.31.248.80;

@ IN NS ns2.gsb.org.
ns2 IN A 10.31.248.54

@ IN MX 10 mail.gsb.org.
mail IN A 10.31.248.81
```

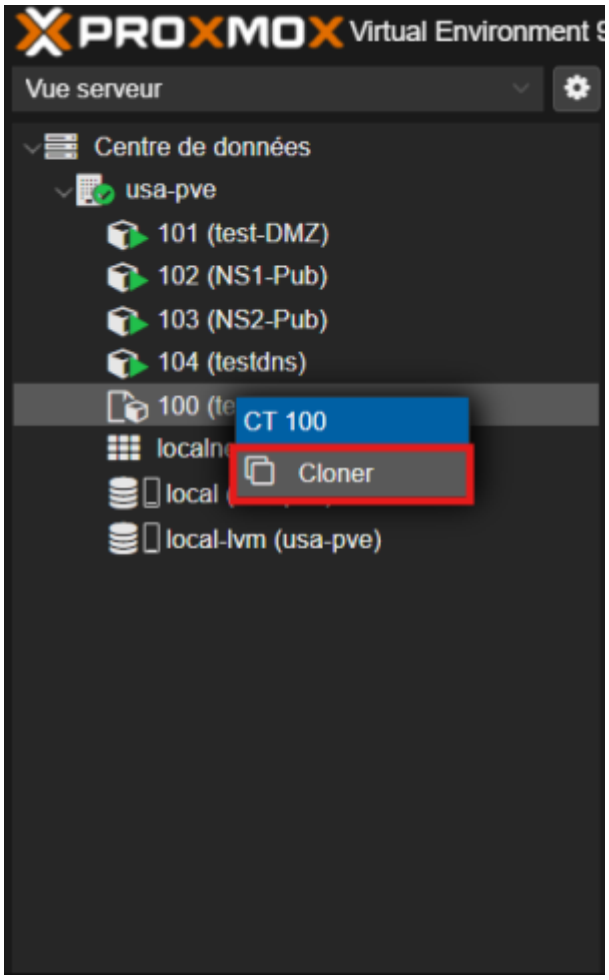
la premiere ligne est un TTL (Time to leave) on peut voir qu'il est réglé sur 86400 qui signifie que le resolveur DNS conserver les reponse dans le cache pendant 24heures
La deuxieme ligne indique le serveur Maitre (ns1.gsb.org) et le compte admin (root@gsb.org)
les ligne de 3 a 7 sont des ligne de paramètre de synchronisation pour les serveurs secondaire
Les lignes commencent pas IN NS indique les serveurs DNS pour la zone donc la NS1 qui est le Master et ns2 qui est le Slave
Les lignes contenant IN A enregistre les adresse IP et a quoi elle correspondent
La ligne avec MX (Mail eXanger) sert a mettre en place un serveur de messagerie

NS2

création et paramétrage du conteneur NS 2

Création conteneur NS2

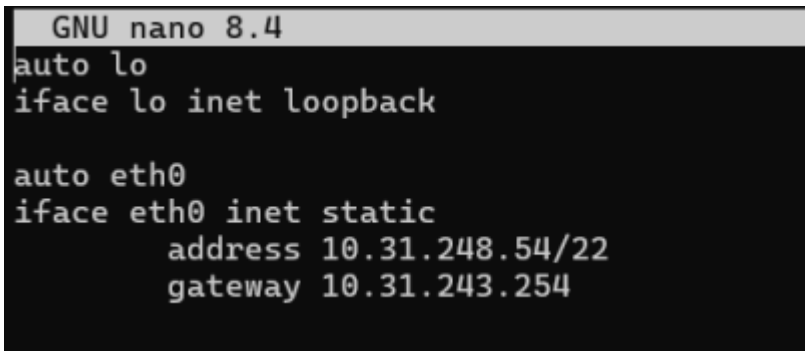
Pour créer le conteneur, même principe que pour NS1 donc clonage du conteneur Template puis paramétrage IP



Après avoir cloné notre Template il fallait modifier les paramètres IP pour qu'il soit conforme au cahier des charges.
Le cahier des charges nous demande de mettre nos DNS dans la DMZ(Zone démilitarisé) qui dans

notre cas et le 3eme sous reseau et donc en 10.31.248.53/54
Je suis donc aller dans le répertoire etc/network pour remplir le fichier interfaces et ainsi mettre ma nouvelle adresse IP

```
nano /etc/network/interfaces
```

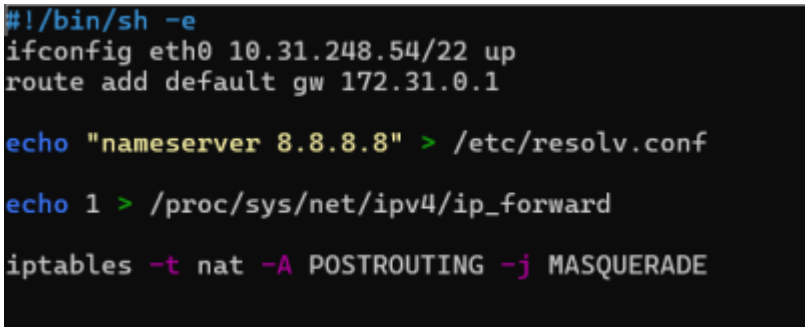


auto lo iface lo inet loopback

auto eth0 iface eth0 inet static

```
      address 10.31.248.53/22
      gateway 10.31.243.254
```

</code> Pour finir la configuration réseau je suis retourner dans le répertoire etc mais cette fois-ci dans le dossier rc.local pour y implanter tout les paramètre réseau nécessaire au bon fonctionnement du centenaire




```
#!/bin/sh -e
ifconfig eth0 10.31.248.54/22 up
route add default gw 172.31.0.1

echo "nameserver 8.8.8.8" > /etc/resolv.conf

echo 1 > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING -j MASQUERADE
```

Une fois le réglage réseau terminer il faut installer bind9

```
apt-get installe bind9 bind9utils dnsutils
```

Une fois les paquets installé, un répertoire du nom de Bind est apparu dans le répertoire etc. C'est donc dans ce répertoire que tous nos fichier de conf seront

```
cd /etc/bind
```

Pour voir a quoi ils servent :

voir tableau fichier

Sur le Serveur Slave donc NS2 il n'y a pas besoin du fichier db.gsb.conf. Par contre il y a besoin de configurer les autres fichier

FICHIER DE CONFIGURATION

named.conf.local

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

Dans ce fichier est présent les 2 zones déjà configuré dans le DNS Master, la zone gsb.org et la zone usa.gsb.org qui sont 2 zones différentes dont usa.gsb.org qui est le sous domaine de gsb.org. Ont peut voir aussi que le file n'est pas le même et que le Slave passe par le répertoire var car il n'a pas le droit d'écriture sur le répertoire etc.

Dans se fichier on peut voir que la Zone est en type Slave et qu'elle autorise les transferts avec l'adresse 10.31.248.53 qui est l'adresse du serveur DNS Master. C'est le même principe avec la zone usa.gsb.org

named.conf.options

```
  GNU nano 8.4

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

Dans ce fichier on peut voir que le file et le même que dans le fichier named.conf.local car il n'est pas autorisé à écrire dans le répertoire etc.
Dans la ligne d'en dessous on peut voir allow-query{any;};. Cette ligne veut dire qu'on autorise tout le monde a contacter notre DNS
La troisième ligne va autoriser la récursivité ce qui va permettre a nôtres DNS de pouvoir interrogé d'autre DNS lorsqu'il ne connaitra pas la requêtes
Comme dans le premier fichier la ligne forwarders sert a pouvoir communiquer avec les adresse qui sont mentionné dans notre cas se sont les 2 DNS de google qui vont servir a pouvoir les interroger si notre DNS ne connait pas le requêtes
Et forward only va obliger le DNS a utilisé les ligne forwarders pour communiquer des requêtes externes

Sur le DNS Slave il n'y a pas besoin du fichier db.gsb.conf ou même db.usa.gsb.conf car le fichier sera copier par le Master c'est pour ca que dans le fichier de conf named.conf.local on autorise le transfert

Test

Ping NS2 vers NS1

```
root@NS2-Pub:/# ping 10.31.248.53
PING 10.31.248.53 (10.31.248.53) 56(84) bytes of data.
64 bytes from 10.31.248.53: icmp_seq=1 ttl=64 time=0.045 ms
64 bytes from 10.31.248.53: icmp_seq=2 ttl=64 time=0.013 ms
64 bytes from 10.31.248.53: icmp_seq=3 ttl=64 time=0.025 ms
64 bytes from 10.31.248.53: icmp_seq=4 ttl=64 time=0.013 ms
```

Ping NS1 vers NS2

```
PING 10.31.248.54 (10.31.248.54) 56(84) bytes of data.
64 bytes from 10.31.248.54: icmp_seq=1 ttl=64 time=0.026 ms
64 bytes from 10.31.248.54: icmp_seq=2 ttl=64 time=0.014 ms
64 bytes from 10.31.248.54: icmp_seq=3 ttl=64 time=0.013 ms
64 bytes from 10.31.248.54: icmp_seq=4 ttl=64 time=0.014 ms
```

Ping NS1 vers google.com

```
root@NS1-Pub:~# ping google.com
PING google.com (172.217.171.238) 56(84) bytes of data.
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=1 ttl=114 time=12.8 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=2 ttl=114 time=12.8 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=3 ttl=114 time=13.3 ms
64 bytes from mrs09s07-in-f14.1e100.net (172.217.171.238): icmp_seq=4 ttl=114 time=12.7 ms
```

Ping NS2 vers google.com

```
root@NS2-Pub:/# ping google.com
PING google.com (172.217.171.206) 56(84) bytes of data.
64 bytes from mrs09s06-in-f14.1e100.net (172.217.171.206): icmp_seq=1 ttl=113 time=12.6 ms
64 bytes from mrs09s06-in-f14.1e100.net (172.217.171.206): icmp_seq=2 ttl=113 time=12.8 ms
64 bytes from mrs09s06-in-f14.1e100.net (172.217.171.206): icmp_seq=3 ttl=113 time=12.3 ms
64 bytes from mrs09s06-in-f14.1e100.net (172.217.171.206): icmp_seq=4 ttl=113 time=12.8 ms
^C
```

Dig NS1

```
root@NS1-Pub:~# dig A ns1.gsb.org

; <<>> DiG 9.20.11-4-Debian <<>> A ns1.gsb.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1987
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8ef61b4888ae03840100000068c7f7dadc5c5aa21fdcb806 (good)
;; QUESTION SECTION:
;ns1.gsb.org.                   IN      A

;; ANSWER SECTION:
ns1.gsb.org.            86400   IN      A       10.31.248.53

;; Query time: 0 msec
;; SERVER: 10.31.248.53#53(10.31.248.53) (UDP)
;; WHEN: Mon Sep 15 11:26:18 UTC 2025
;; MSG SIZE  rcvd: 84
```

dig NS2

```
root@NS1-Pub:~# dig A ns2.gsb.org

; <<>> DiG 9.20.11-4-Debian <<>> A ns2.gsb.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 887
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d73cdc1a7687f8750100000068c7f95512de0a3131202454 (good)
;; QUESTION SECTION:
;ns2.gsb.org.                   IN      A

;; ANSWER SECTION:
ns2.gsb.org.            86400   IN      A       10.31.248.54

;; Query time: 0 msec
;; SERVER: 10.31.248.53#53(10.31.248.53) (UDP)
;; WHEN: Mon Sep 15 11:32:37 UTC 2025
;; MSG SIZE  rcvd: 84
```

dig GSB.ORG

```
root@NS1-Pub:~# dig A gsb.org

; <<>> DiG 9.20.11-4-Debian <<>> A gsb.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3215
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9ca0b20ac836f1280100000068c7f7cc26795b6398eab898 (good)
;; QUESTION SECTION:
;gsb.org.                       IN      A

;; ANSWER SECTION:
gsb.org.                86400   IN      A       10.31.248.80

;; Query time: 0 msec
;; SERVER: 10.31.248.53#53(10.31.248.53) (UDP)
;; WHEN: Mon Sep 15 11:26:04 UTC 2025
;; MSG SIZE  rcvd: 80
```

dig www.gsb.org

```
root@NS1-Pub:~# dig A www.gsb.org

; <<>> DiG 9.20.11-4-Debian <<>> A www.gsb.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29552
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f6ca59e22c5726290100000068c7f7389b9243dd7908805c (good)
;; QUESTION SECTION:
;www.gsb.org.                   IN      A

;; ANSWER SECTION:
www.gsb.org.            86400   IN      A       10.31.248.80

;; Query time: 0 msec
;; SERVER: 10.31.248.53#53(10.31.248.53) (UDP)
;; WHEN: Mon Sep 15 11:23:36 UTC 2025
;; MSG SIZE  rcvd: 84
```

From:
https://sisr2.beaupeyrat.com/ - **Documentations SIO2 option SISR**

Permanent link:
https://sisr2.beaupeyrat.com/doku.php?id=sisr2-usa:dns_master_slave

Last update: **2025/11/05 07:35**