

# **SRV-DNS**

Bind 9 sous Debian 11 & Bind 9 sous PFsense.

Noah MAILLET Projet-SANDBOX



### Table of contents

1	Preface						
1.1	Present	ation Bind9	3				
1.2	Configu	ration minimale	3				
2	Créatio	n du conteneur	4				
3	Installa	tion Bind9	8				
4	Configu	ration Bind9	9				
4.1	Configu	10					
	4.1.1	Limitation du reseau	10				
	4.1.2	Forwarders	10				
	4.1.3	Sécurité du DNS	11				
4.2	Ajout d	une nouvelle zone DNS dans BIND9	12				
	4.2.1	Configuration recherche directe	12				
	4.2.1.1	Ajout Zone directe	12				
	4.2.1.2	Déclaration db.sandbox.local	13				
	4.2.2	Configuration Recherche inverse	14				
	4.2.2.1	Ajout de la Zone inversée	14				
	4.2.2.2	Déclaration « db.inverse.sandbox.local »	15				
4.3	Configuration des log						
	4.3.1	Création du fichier de log	16				
	4.3.2	Modification du fichier de configuration ajout du fichier de log	16				
4.4	Vérifica	tion des configurations et test	18				
	4.4.1	Verification des configurations	18				
	4.4.2	Allumage DNS et Configuration client	19				
	4.4.3	Test recherche directe	20				
	4.4.3.1	Test internet	20				
	4.4.3.2	Test reseau local	21				
	4.4.4	Test DNS (Recherche inverse)	22				
	4.4.4.1	Internet	22				
	4.4.4.2	Réseau Local	23				
5	DNS sur	PFSENSE	24				
5.1	Configu	ration DNS Resolver	24				
5.2	Test co	nfiguration DNS	28				
6	BliblioV	Veb :					
6.1	IT-Conn	ect					
6.2	Docume	entation ubuntu					
6.3	Malekal						

# 1 Preface

### 1.1 Presentation Bind9

#### Nom du Service : BIND9 (Berkeley Internet Name Domain)

Description : BIND9 est le serveur DNS (Domain Name System) le plus utilisé sur Internet. Il fonctionne comme un logiciel open-source qui fournit les services de résolution de noms de domaine. En d'autres termes, il traduit les noms de domaine en adresses IP et vice versa, facilitant ainsi la navigation sur le Web.

Fonctionnalités principales :

- Résolution DNS : BIND9 résout les noms de domaine en adresses IP et vice versa. Cela permet aux utilisateurs d'accéder à des sites Web en utilisant des noms conviviaux plutôt que de se souvenir d'adresses IP numériques.
- Hébergement de Zones DNS : Il permet aux administrateurs système de gérer leurs propres zones DNS. Les zones peuvent inclure des enregistrements pour des hôtes individuels, des sous-domaines, des serveurs de messagerie, etc.
- 3. Support DNSSEC : BIND9 prend en charge DNSSEC (Domain Name System Security Extensions), une suite de protocoles de sécurité qui protègent les données DNS contre les attaques telles que la falsification de réponse DNS.
- 4. Scalabilité : Il est hautement configurable et peut être utilisé pour répondre aux besoins d'infrastructures de réseau de petite à grande échelle.
- 5. Redondance et Réplication : BIND9 supporte la redondance et la réplication pour assurer la disponibilité et la tolérance aux pannes des services DNS.

Utilisations courantes :

- 1. Hébergement Web : Les fournisseurs d'hébergement web utilisent BIND9 pour gérer les enregistrements DNS de leurs clients et permettre l'accès à leurs sites web.
- 2. Réseau d'Entreprise : Les grandes entreprises utilisent BIND9 pour gérer leurs propres infrastructures DNS internes, facilitant ainsi l'accès aux ressources internes et externes.
- 3. Fournisseurs de Services Internet (ISP): Les ISP utilisent BIND9 pour gérer les serveurs DNS qui permettent à leurs clients d'accéder à Internet.
- 4. Universités et Institutions Éducatives : Les institutions éducatives utilisent BIND9 pour gérer leurs propres infrastructures DNS, offrant ainsi des services de noms de domaine à leurs étudiants et personnels.

#### Conclusion :

BIND9 est un outil essentiel pour la gestion des services DNS sur Internet et dans les réseaux locaux. Avec ses fonctionnalités avancées, sa fiabilité et sa sécurité, il reste le choix privilégié pour les administrateurs système et les organisations qui dépendent d'une résolution DNS rapide et précise.

### 1.2 Configuration minimale

#### DNS (<u>https://urlz.fr/pyaF</u>) :

- Processeur: 1 cœur
- RAM:512Mo
- Espace disque : 10Go



# 2 Création du conteneur

Dans le cadre du projet sandbox, l'outil de virtualisation qui a été retenue est Proxmox.

Vous pouvez installer Bind9 dans tout autre environnement de virtualisation tant que vous respectez la configuration minimale.

- 1. Je me connecte à ma ferme de serveur ProxMox.
- 2. Créer un conteneur.



3. Je renseigne le numéro du conteneur, le nom de l'hôte « SRV-DNS », le pool de ressource « SANDBOX-TRAINING », configuration du mot de passe. → Suivant.

Créer: Contene	eur LXC		$\otimes$
Général Moo	dèle Disques Processeur Mér	moire Réseau Di	NS Confirmation
Nœud:	pve	Pool de ressources:	SANDBOX-TRAINING × ~
CTID: Nom d'hôte:	102 SRV.DNS	Mot de passe:	•••••
Nom d'hôte: Conteneur non		Confirmer le mot de passe:	•••••
Imbriqué:		Clef(s) SSH publique(s):	
		Charger le fichier	de clef SSH

4. Je sélectionne le modèle de mon conteneur → suivant.

Créer: Conteneur LXC									$\otimes$
Général	Mod	lèle	Disques	Processeur	Mémoire	Réseau	DNS	Confirmation	
Stockage:		stor	rage		$\sim$				
Modèle:		deb	oian-11-stand	ard_11.7-1_am	d64 🗸				



#### 5. J'alloue 10Go de stockage. → Suivant.

Créer: Co	nteneur L	хс						$\otimes$
Général	Modèle	Disques Proc	cesseur	Mémoire	Réseau	DNS	Confirmation	
rootfs	Û	Stockage:	local-lv	m	$\sim$			
		Taille du disque	10		0			
		(GIO):						

6. J'alloue 1 cœur de processeur → Suivant.

er	Créer: Co	nteneur L)	хс						$\otimes$
	Général	Modèle	Disques	Processeur	Mémoire	Réseau	DNS	Confirmation	e
	Cœurs:	1			$\bigcirc$				

### 7. Je laisse la configuration par défaut → suivant.

Créer: Conteneur LXC							
Général Modèle	Disques	Processeur	Mémoire	Réseau	DNS	Confirmation	e
Mémoire (MiB):	512		$\bigcirc$				L.
Espace d'échange (swap) (MiB) <sup>:</sup>	512		$\bigcirc$				C

8. Je renseigne le VLAN et les @IP, je décoche l'option pare-feu → Suivant.

Créer: Contene	eur LXC		$\otimes$
Général Mo	dèle Disques Processeur Mémo	ire Réseau DN	NS Confirmation
Nom:	eth0	IPv4: 💿 Statique	e ODHCP
Adresse MAC:	auto	IPv4/CIDR:	10.16.1.2/28
Pont (bridge):	vmbr0 ~	Passerelle (IPv4):	10.16.1.14
Etiquette de VLAN:	1	IPv6:   Statique	e ODHCP OSLAAC
Pare-feu:		IPv6/CIDR:	Aucun
		Passerelle (IPv6):	



#### 9. Je rentre le nom de domaine et le DNS. → Suivant.

Créer: Conteneur LXC								
Général Mo	dèle Disques	Processeur	Mémoire	Réseau	DNS	Confirmation		
Domaine DNS:	sandbox.local							
Serveurs DNS:	8.8.8.8						c	

#### 10. Je vérifie que toutes les informations sont correctes $\rightarrow$ terminer.

Général	Modèle	Disques	Processeur	Mémoire	Réseau	DNS	Confirmation	
Key ↑		Value						
cores		1						
eatures		nesting	=1					
nostname		SRV-D	NS					
nemory		512						
nameserve	r	8.8.8						
net0		name=	eth0,bridge=vm	br0,tag=1,ip=	10.16.1.2/28	8, <b>gw=1</b> 0.	16.1.14	
nodename		pve						
ostemplate		storage	vztmpl/debian-	11-standard	_11.7-1_amd	64.tar.zs	ıt	
lood		SANDE	30X-TRAINING					
ootfs		local-lv	m:10					
searchdom	ain	sandbo	x.local					
ssh-public-l	keys							
swap		512						
unprivilegeo	d	1						
Démarrer	après cré	ation						
							Avancé 🗌 Retour	Termi
ot@pam		VM 103 -	Cloner					



### 11. Le conteneur a été créé.

Task viewer: CT 103 - Créer	$\otimes$
Sortie Statut	
Stopper	📥 Télécharger
WARNING: You have not turned on protection against thin pools running out of space. WARNING: Set activation/thin_pool_autoextend_threshold below 100 to trigger automatic extension of thin pools before they get full. Logical volume "vm-103-disk-0" created. WARNING: Sum of all thin volume sizes (390.00 GiB) exceeds the size of thin pool pve/data and the size of whole volume group (<222.57 Creating filesystem with 2621440 4k blocks and 655360 inodes Filesystem UUID: 19e31d29-8e89-4285-8340-500b5a674594 Superblock backups stored on blocks: 32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632 extracting archive '/mnt/pve/storage/template/cache/debian-11-standard_11.7-1_amd64.tar.zst' Total bytes read: 490127360 (468MiB, 268MiB/s) Detected container architecture: amd64 Creating SSH host key 'ssh_host_ecdsa_key' - this may take some time done: SHA256:UdgBSkQQq3Wevv6Vq2e1r6mlDcsR9tNH3kxOm8kK73b8 root@SRV-DNS Creating SSH host key 'ssh_host_ed25519_key' - this may take some time done: SHA256:WdpQMp2wOHgRp5rJKt2mI7uZ3ZQOtbnZkfPkKV+g87M root@SRV-DNS Creating SSH host key 'ssh_host_rsa_key' - this may take some time done: SHA256:WJDHJNeALOkD+TF4VtruC1j7GqrafOIsoput1cesyw root@SRV-DNS Creating SSH host key 'ssh_host_rsa_key' - this may take some time done: SHA256:HoJBNeALOkD+TF4VtruC1j7GqrafOIsoput1cesyw root@SRV-DNS Creating SSH host key 'ssh_host_dsa_key' - this may take some time done: SHA256:HTPmsKJG7Db4Qo7rbpPGb/0DZZrgX/6sxGaNgS0j/cU root@SRV-DNS TASK OK	GIB).

# **3 Installation Bind9**

- 1. Je me connecte à la ferme de serveur proxmox.
- 2. Je démarre le conteneur et je me connecte.
- 3. Je teste l'accès à internet.

```
root@SRV-DNS:~# ping www.google.fr
PING www.google.fr (142.250.179.99) 56(84) bytes of data.
64 bytes from par21s20-in-f3.1e100.net (142.250.179.99): icmp_seq=1 ttl=115 time=12.7 ms
64 bytes from par21s20-in-f3.1e100.net (142.250.179.99): icmp_seq=2 ttl=115 time=12.6 ms
64 bytes from par21s20-in-f3.1e100.net (142.250.179.99): icmp_seq=3 ttl=115 time=12.7 ms
64 bytes from par21s20-in-f3.1e100.net (142.250.179.99): icmp_seq=3 ttl=115 time=12.7 ms
64 bytes from par21s20-in-f3.1e100.net (142.250.179.99): icmp_seq=4 ttl=115 time=12.9 ms
^C
--- www.google.fr ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 12.596/12.696/12.863/0.100 ms
root@SRV-DNS:~# []
```

4. Je mets à jour la liste des dépôts et les paquets.

#### Commande :

apt update && apt upgrade



5. J'installe bind9 et ces dépendances.

### Commande :

apt install bind9 bind9utils bind9-doc dnsutils

root@SRV-DNS:~# apt install bind9 bind9utils bind9-doc dnsutils
Reading package lists Done
Building dependency tree Done
Reading state information Done
The following additional packages will be installed:
bind9-utils dns-root-data python3-ply
Suggested packages:
bind-doc resolvconf ufw python-ply-doc
The following NEW packages will be installed:
bind9 bind9-doc bind9-utils bind9utils dns-root-data dnsutils python3-ply
0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.
Need to get 6699 kB of archives.
After this operation, 12.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y



# 4 Configuration Bind9

- 1. Je me connecte au serveur Bind9.
- 2. Je fais une copie du fichier de configuration :

```
Commande :
```

cp /etc/bind/named.conf.options /etc/bind/named.conf.options-old

```
root@SRV-DNS:/etc/bind# cp named.conf.options named.conf.options-OLD
root@SRV-DNS:/etc/bind# ls -lh
total 52K
-rw-r--r-- 1 root root 2.0K Feb 12 16:25 bind.keys
-rw-r--r-- 1 root root 237 Feb 12 16:25 db.0
-rw-r--r-- 1 root root 271 Feb 12 16:25 db.127
 rw-r--r-- 1 root root 237 Feb 12 16:25 db.255
 rw-r--r-- 1 root root 353 Feb 12 16:25 db.empty
-rw-r--r-- 1 root root 270 Feb 12 16:25 db.local
 rw-r--r-- 1 root bind 463 Feb 12 16:25 named.conf
 rw-r--r-- 1 root bind 498 Feb 12 16:25 named.conf.default-zones
 rw-r--r-- 1 root bind 165 Feb 12 16:25 named.conf.local
 rw-r--r-- 1 root bind 846 Feb 12 16:25 named.conf.options
 rw-r--r-- 1 root bind 846 Mar 7 16:36 named.conf.options-OLD
 rw-r---- 1 bind bind 100 Mar 7 16:00 rndc.key
-rw-r--r-- 1 root root 1.3K Feb 12 16:25 zones.rfc1918
root@SRV-DNS:/etc/bind# |
```

3. Je modifie le fichier : /etc/bind/named.conf.options

### Commande :

nano /etc/bind/named.conf.options



# 4.1 Configurer les options de Bind9

### 4.1.1 Limitation du reseau.

Ce paramètre permet de définir le réseau pour limiter à son seul réseau.





### 4.1.2 Forwarders.

Activer les forward permet de transférer les requetes de bind9 qui ne sont pas dans une zone DNS.

<u>Configuration :</u> forwarders { 192.168.1.254; 8.8.8.8; 1.1.1.1;

};





### 4.1.3 Sécurité du DNS

Les options suivantes sont facultatives, mais permette d'améliorer la sécurité.

*Listen-on port* permet de définir le port d'écoute ainsi que les @IP du serveur DNS.

#### **Configuration :**

Listen-on port 53 {localhost; 10.16.1.2; };

Dnssec-validation activation de la validation DNSSEC.

### **Configuration :**

Dnssec-validation auto;

*Allow-recursion* Ce paramètre indique quels sont les hôtes sont autorisés à effectuer des requêtes récursives via ce serveur. (Le paramètre « Any », permet de faire en sorte que le serveur DNS interroge tous les serveurs DNS qu'il connaît pour avoir une réponse).

#### **Configuration :**

Allow-recursion {any; };

*auth-nxdomain no* : Le *NXDOMAIN* est le message qui signifie que le nom de domaine n'existe pas (Non eXistent Domain).

#### **Configuration:**

Auth-nxdomain no; #conform to RFC1035.

Si vous avez suivie la configuration ci-dessus vous devriez avoir le résultat suivant :

```
options {
    directory "/var/cache/bind";
    version "Bind Server";
    forwarders {
        192.168.1.254;
        8.8.8;
        1.1.1.1;
    };
    listen-on port 53 {localhost; 10.16.1.2; };
    dnssec-validation auto;
    allow-recursion{any; };
    auth-nxdomain no; # Conform to RFC1035
};
```



## 4.2 Ajout d'une nouvelle zone DNS dans BIND9

Dans un premier temps je fais une copie du fichier de zone « /etc/bind/named.conf.local »

### Commande :

cp /etc/bind/named.conf.local /etc/bind/named.conf.local-old

Puis je modifie le fichier de configuration /etc/bind/named.conf.local

### Commandes :

nano /etc/bind/named.conf.local

### 4.2.1 Configuration recherche directe.

### 4.2.1.1 Ajout Zone directe.

Voici les paramètres de configuration à modifier :

- Zone « sandbox.local » → Définit le nom de la zone.
- *Type Master* → Inidique que ce serveur fait autorité sur la zone.
- *file « /etc/bind/db.sandbox.local* » → On indique le lien vers le fichier contenant la base d'enregistrements pour la zone.
- Allow-update {none ;} → N'autorise pas la mise à jour du fichier d'enregistrement par un tiers ce qui permet d'augmenter la sécurité et être sur qu'il n'y ait que le serveur DNS qui s'occupe de la zone.

### **Configuration :**

```
// Zone Directe « sandbox.local » :
zone "sandbox.local" {
type master;
file "/etc/bind/db.sandbox.local";
notify no;
allow-update {none; };
};
```

Voici la configuration du fichier named.conf.local que vous devriez avoir.





### 4.2.1.2 Déclaration db.sandbox.local

Dans un premier temps je vais faire la copie du fichier de configuration db.empty vers db.sandbox.local. puis je modifie le propriétaire du fichier.

#### Commande: cp db.empty db.sandbox.local shown shown bind db.sandbox.local Puis je modifie le fichier db.sandbox.local Commande : nano db.sandbox.local Voici les informations que vous devrez renseigner dans le fichier. \$TTL 86400 IN sandbox.local root.sandbox.local ( @ SOA ; Serial 1 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 86400) ; Negative Cache TTL ; @ IN NS srv-dns.sandbox.local. Pfsense IN Α 10.16.1.14 srv-lldap IN А 10.16.1.1

Voici la configuration que vous devriez avoir :

А

А

Α

Α

Α

10.16.1.2

10.16.1.3

10.16.1.4

10.16.1.5

10.16.1.10

IN

IN

IN

srv-dns

srv-auto

W10-Admin

srv-guacamole IN

srv-supervision IN

<b>ŞTTL</b>	86400							
0	IN	SOA	sandbox	local r	00	t.sandbox.	local	(
			1		;	Serial		
			604800		;	Refresh		
			86400		;	Retry		
			2419200		;	Expire		
			86400	)	;	Negative	Cache	$\mathbf{TTL}$
;								
6	IN	NS	srv-dns.	.sandbox	.10	ocal.		
pfsense		IN	A	10.16.1	.14	4		
srv-llda	ар	IN	A	10.16.1	.1			
srv-dns		IN	A	10.16.1	•2			
srv-guad	camole	IN	A	10.16.1	.3			
srv-supe	ervision	IN	A	10.16.1	• 4			
srv-auto	)	IN	A	10.16.1	.5			
W10-Admi	in	IN	A	10.16.1	.10	0		



### 4.2.2 Configuration Recherche inverse

### 4.2.2.1 Ajout de la Zone inversée.

Je me rends dans /etc/bind/ et je modifie named.conf.local.

Commande :
cd /etc/bind
nano Named.conf.local
Voici la configuration que vous devez renseigner :
// Déclaration Zone Inverse « Sandbox.local » :
zone « 1.16.10.in-addr.arpa » {
type master;
file « /etc/bind/db.inverse.sandbox.local »;
allow-update (none;);
};

Voici la configuration que vous devriez avoir :

```
// Zone Indirecte "sandbox.local":
zone "1.16.10.in-addr.arpa" {
type master;
file "/etc/bind/db.inverse.sandbox.local";
allow-update {none; };
};
```



### 4.2.2.2 Déclaration « db.inverse.sandbox.local »

Je me rends dans /etc/bind, je fais une copie du fichier «db.empty» et je nomme la copie «db.inverse.sandbox.local » puis je change le propriétaire du fichier.

Commande :					
Cd /etc/bin	Cd /etc/bind				
Cp db.empt	y db.invers	se.sandb	ox.local		
shown show	n bind db	.sandbo	<.local		
Nano db.inv	erse.sandl	oox.loca	l		
Voici les inf	ormations	que vou	s devrez renseigner dans le fichier.		
\$TTL 8640	0				
@ IN	SOA	srv-dn	s.sandbox.local. root.sandbox.local. (		
1		;Serial			
604	800	; Refre	esh		
864	00	; Retry	/		
241	9200	; Ехріг	e		
864	00)	; Nega	itive Cache TTL		
;					
@ IN	NS	srv-dn	s.sandbox.local.		
@ IN	PTR	sandb	ox.local.		
Pfsense	IN	А	10.16.1.14		
srv-lldap	IN	А	10.16.1.1		
srv-dns	IN	А	10.16.1.2		
srv-guacam	ole IN	А	10.16.1.3		
srv-supervis	ion IN	А	10.16.1.4		
srv-auto	IN	А	10.16.1.5		
Host-Admir	IN	А	10.16.1.10		
14 IN	PTR	pfsens	se.sandbox. local.		
1 IN	PTR	srv-lld	ap.sandbox.local.		
2 IN	PTR	srv-dn	s.sandbox.local.		
3 IN	PTR	srv-gu	acamole.sandbox.local.		
4 IN	PTR	รгง-รน	pervision.sandbox.local.		
5 IN	PTR	srv-au	to sandbox local.		

host-admin.sandbox.local.

10

IN

PTR



# 4.3 Configuration des log

### 4.3.1 Création du fichier de log

Dans un premier temps ont créer le fichier bind dans « /var/log » puis dans un deuxième temps on change le propriétaire du fichier de log.

<u>Commandes :</u>	
cd /var/log	
mkdir bind	
shown bind:bind bind/	

root@SRV-DNS:~# cd /var/log
root@SRV-DNS:/var/log# mkdir bind
root@SRV-DNS:/var/log# chown bind:bind bind/

# 4.3.2 Modification du fichier de configuration ajout du fichier de log

Dans un premier temps on ce rends dans « /etc/bind/ » puis on modifie le fichier « /etc/bind/named.conf.options ».

### <u>Commandes :</u>

cd /etc/bind/

nano named.conf.options

J'ajoute la configuration si dessous à la fin du fichier.

```
Configuration:
logging {
    channel transfers {
        file "/var/log/bind/transfers" versions 3 size 10M;
        print-time yes;
        severity info;
    };
    channel notify {
        file "/var/log/bind/notify" versions 3 size 10M;
        print-time yes;
        severity info;
    };
    channel dnssec {
        file "/var/log/bind/dnssec" versions 3 size 10M;
        print-time yes;
```



severity info;

```
};
```

```
channel query {
```

file "/var/log/bind/query" versions 5 size 10M;

```
print-time yes;
```

severity info;

### };

channel general {

file "/var/log/bind/general" versions 3 size 10M;

print-time yes;

severity info;

### };

channel slog {

syslog security;

severity info;

### };

```
category xfer-out { transfers; slog; };
category xfer-in { transfers; slog; };
category notify { notify; };
```

```
category lame-servers { general; };
category config { general; };
category default { general; };
category security { general; slog; };
category dnssec { dnssec; };
```

// category queries { query; };

Après avoir rentré les informations suivantes :

Je test la bonne configuration du fichier de configuration :

### Commandes :

}

named-checkconf /etc/bind/named.conf.options

```
root@SRV-DNS:/etc/bind# named-checkconf /etc/bind/named.conf.options
root@SRV-DNS:/etc/bind#
```

Sur la capture ci-dessus on peut voir que la configuration ne contient aucune erreur.



# 4.4 Vérification des configurations et test

### 4.4.1 Verification des configurations

Vérification des fichiers de configurations :

### Commandes :

Named-checkconf

Vérification des fichiers de configuration des zones :

Commandes:

named-checkzone sandbox.local /etc/bind/db.sandbox.local

named-checkzone 1.16.10.in-addr.arpa /etc/bind/db.inverse.sandbox.local

Voici les resultat que vous devriez avoir :

root@SRV-DNS:/etc/bind# named-checkconf root@SRV-DNS:/etc/bind# named-checkzone sandbox.local /etc/bind/db.sandbox.local zone sandbox.local/IN: loaded serial 1 OK root@SRV-DNS:/etc/bind# named-checkzone 1.16.10.in-addr.arpa /etc/bind/db.inverse.sandbox.local zone 1.16.10.in-addr.arpa/IN: loaded serial 1 OK



### 4.4.2 Allumage DNS et Configuration client

1. Allumage du service DNS.

### Commandes :

Systemctl start bind9

root@SRV-DNS:/etc/bind# systemctl start bind9
root@SRV-DNS:/etc/bind#

2. Vérification du bon fonctionnement de bind9

#### Commandes :

```
Systemctl status bind9
```

```
named.service - BIND Domain Name Server
     Loaded: loaded (/lib/system/system/named.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2024-03-11 14:57:00 UTC; 9min ago
       Docs: man:named(8)
   Main PID: 1593 (named)
     Tasks: 6 (limit: 18983)
     Memory: 38.8M
        CPU: 93ms
     CGroup: /system.slice/named.service
              -1593 /usr/sbin/named -f -u bind
Mar 11 14:57:00 SRV-DNS named[1593]: automatic empty zone: 9.E.F.IP6.ARPA
Mar 11 14:57:00 SRV-DNS named[1593]: automatic empty zone: A.E.F.IP6.ARPA
Mar 11 14:57:00 SRV-DNS named[1593]: automatic empty zone: B.E.F.IP6.ARPA
Mar 11 14:57:00 SRV-DNS named[1593]: automatic empty zone: 8.B.D.0.1.0.0.2.IP6.ARPA
Mar 11 14:57:00 SRV-DNS named[1593]: automatic empty zone: EMPTY.AS112.ARPA
Mar 11 14:57:00 SRV-DNS named[1593]: automatic empty zone: HOME.ARPA
Mar 11 14:57:00 SRV-DNS named[1593]: configuring command channel from '/etc/bind/rndc.key'
Mar 11 14:57:00 SRV-DNS named[1593]: command channel listening on 127.0.0.1#953
Mar 11 14:57:00 SRV-DNS named[1593]: configuring command channel from '/etc/bind/rndc.key'
Mar 11 14:57:00 SRV-DNS named[1593]: command channel listening on ::1#953
```

3. Je modifie ma configuration DNS :

#### Commandes :

nano /etc/resolv.conf

### **Configuration :**

nameserver 127.0.0.1

nameserver 10.16.1.2

search sandbox.local	
#DNS LOCAL	
nameserver 127.0.0.1	
nameserver 10.16.1.2	2
#DNS SECONDAIRE	
nameserver 8.8.8.8	

Dans le cas suivant je commente la ligne « nameserver 8.8.8.8 » pour voir le bon fonctionnement du DNS.



### 4.4.3 Test recherche directe

### 4.4.3.1 Test internet

1. Je ping <u>www.google.fr</u>

#### Commandes :

Ping <u>www.google.fr</u>

```
root@SRV-LLDAP:~# ping www.google.fr
PING www.google.fr (216.58.214.163) 56(84) bytes of data.
64 bytes from parl0s42-in-f3.le100.net (216.58.214.163): icmp_seq=1 ttl=115 time=12.1 ms
64 bytes from mad01s26-in-f163.le100.net (216.58.214.163): icmp_seq=2 ttl=115 time=12.5 ms
64 bytes from mad01s26-in-f163.le100.net (216.58.214.163): icmp_seq=3 ttl=115 time=12.7 ms
64 bytes from mad01s26-in-f3.le100.net (216.58.214.163): icmp_seq=4 ttl=115 time=12.8 ms
64 bytes from mad01s26-in-f163.le100.net (216.58.214.163): icmp_seq=5 ttl=115 time=12.8 ms
64 bytes from mad01s26-in-f163.le100.net (216.58.214.163): icmp_seq=5 ttl=115 time=12.2 ms
64 bytes from mad01s26-in-f163.le100.net (216.58.214.163): icmp_seq=5 ttl=115 time=12.2 ms
7C
---- www.google.fr ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 12.149/12.483/12.829/0.263 ms
```

2. Je mets à jour les paque debian.

#### Commandes :

Apt update && apt upgrade

```
root@SRV-LLDAP:~# apt update && apt upgrade
Hit:1 http://deb.debian.org/debian bullseye InRelease
Hit:2 http://security.debian.org bullseye-security InRelease
Get:3 http://download.opensuse.org/repositories/home:/Masgalor:/LLDAP/Debian 11 InRelease [1556 B]
Hit:4 http://deb.debian.org/debian bullseye-updates InRelease
Fetched 1556 B in 0s (3321 B/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@SRV-LLDAP:~#
```

3. Relevé d'info domaine : « pk33prod.ovh »

### Commandes :

Nslookup pk33prod.ovh

root@SRV	-LLDAP:~# nslookup	pk33prod.ovh
Server:	10.16.1.2	
Address:	10.16.1.2#	53
Non-auth	oritative answer:	
Name:	pk33prod.ovh	
Address:	51.91.236.255	
Name:	pk33prod.ovh	
Address:	2001:41d0:301::29	



### 4.4.3.2 Test reseau local

1. Ping srv-lldap.sandbox.local

#### Commandes :

Ping srv-lldap.sandbox.local

```
root@SRV-DNS:~# ping srv-dns.sandbox.local
PING SRV-DNS.sandbox.local (10.16.1.2) 56(84) bytes of data.
64 bytes from SRV-DNS.sandbox.local (10.16.1.2): icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from SRV-DNS.sandbox.local (10.16.1.2): icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from SRV-DNS.sandbox.local (10.16.1.2): icmp_seq=3 ttl=64 time=0.019 ms
^C
--- SRV-DNS.sandbox.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 0.019/0.022/0.028/0.004 ms
```

2. Ping srv-dns.sandbox.local

#### Commandes :

Ping srv-dns.sandbox.local

```
root@SRV-DNS:~# ping srv-lldap.sandbox.local
PING srv-lldap.sandbox.local (10.16.1.1) 56(84) bytes of data.
64 bytes from srv-lldap.sandbox.local (10.16.1.1): icmp_seq=1 ttl=64 time=0.113 ms
64 bytes from srv-lldap.sandbox.local (10.16.1.1): icmp_seq=2 ttl=64 time=0.036 ms
64 bytes from srv-lldap.sandbox.local (10.16.1.1): icmp_seq=3 ttl=64 time=0.036 ms
^C
--- srv-lldap.sandbox.local ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2039ms
rtt min/avg/max/mdev = 0.036/0.061/0.113/0.036 ms
```



### 4.4.4 Test DNS (Recherche inverse)

### 4.4.4.1 Internet

1. Nslookup 8.8.8.8 (DNS Google).



2. Dig 1.1.1.1 (DNS Cloud Flare).



#### 3. Recherche sur internet.

🗖 🔍 apache guac	amole - Search x +	-	o ×
$\leftarrow \rightarrow $ G	https://www.bing.com/search?q=apache+guacamole&cvid=5d21b53e2e2b46fc8474cfb1db098 🏠	£≞ @	•
🥌 Apache Guacamole	🗾 Pfsense 🕒 LLDAP		
			A
Microsoft Bing	Q apache guacamole		Sign i
	Q SEARCH 🙋 COPILOT VIDEOS IMAGES MAPS NEWS SHOPPING : MORE	ABOUT SEAF	RCH RESULTS
	About 96 200 results		
	Apache Guacamole		See more
	Apache Guacamole <sup>TM</sup> (Web) Apache Guacamole is a web-based clientless remote desktop gateway that supports VNC, RDP, and SSH protocols. It is free, open source, and commercially supported by a		ß



### 4.4.4.2 Réseau Local

1. Nslookup 10.16.1.1 (srv-lldap)

SRV DNS :

SRV LLDAP:

2. Nslookup 10.16.1.2 (srv-dns)

SRVL DNS:

SRV LLDAP :

root@SRV-LLDAP:~# nslookup 10.16.1.2
2.1.16.10.in-addr.arpa name = srv-dns.sandbox.local.



## **5 DNS sur PFSENSE**

1. Je me connecte sur le pare-feu PFSENSE.

	System ▼ Interfaces ▼ Firewall ▼ Services ▼	VPN ▼ Status ▼ Diagnostics ▼ Help ▼
Status / Da	ashboard	+ 0
System Infor	mation 🥕 🖨 🕄	Netgate Services And Support $igodot$
Name	BigFirewall.pk33prod.ovh	Contract type Community Support
User	admin@192.168.1.17 (Local Database)	Community Support Only
System	KVM Guest Netgate Device ID: d000b4b6eb74ae734a01	NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Fri Apr 26 10:05:38 CEST 2024	If you purchased your pfSense gateway firewall appliance from Netgate and elected <b>Community Support</b> at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the <b>NETGATE RESOURCE LIBRARY</b> . You also may upgrade to a Netgate Global Technical Assistance Center (TAC)
СРИ Туре	Intel(R) Core(TM) i3-6100 CPU @ 3.70GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No	Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.
Hardware crypto	Inactive	Upgrade Your Support     Community Support Resources
Kernel PTI	Enabled	Netgate Global Support FAQ     Official pfSense Training by Netgate
MDS Mitigation	Inactive	Netgate Professional Services     Visit Netgate.com

### 5.1 Configuration DNS Resolver

#### Service → DNS Resolver.

1. J'active le « DNS Resolver ».

Options générales du DNS Resolver		
Activer	Activer les résolutions DNS	

2. Je choisie l'interface « Tout ».

Interfaces réseau	Tout	<u>~</u>
	WAN LAN_SERVER_SANDBOX	
	DMZ_SANDBUX	•
	Interface IP addresses used by the DNS Resolver for responding t used. Queries to addresses not selected in this list are discarded. address.	to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are The default behavior is to respond to queries on every available IPv4 and IPv6

3. Je choisie l'interface réseau sortante « Tout ».

Interfaces réseau	Tout
sortantes	WAN LAN_SERVER_SANDBOX DMZ_SANDBOX
	Interfaces réseau utilisées par le DNS Resolver pour envoyer des requêtes aux serveurs faisant autorité et pour recevoir leurs réponses. Par défaut, toutes les interfaces sont utilisées.



- J'enregistre la configuration.
   Création de l'hote pfsense.

### **Configuration :**

#### Hôte : PFSENSE

#### Domain : sandbox.local

@IP:10.16.1.14

Options de surcharge d'hôte		
Hôte	pfsense	
	Le nom de l'hôte, sans la partie domaine . Ex: Entrer "monordinateur" si le nom complet est "monordinateur.exemple.fr"	
Domaine	sandbox.local	
	. Ex: Entrer "exemple.fr" pour "monordinateur.exemple.fr"	
Adresse IP	10.16.1.14	
	IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3	

### Enregistrer.

### 6. SRV-LLDAP.

Options de surcharge	e d'hôte
Hôte	srv-Ildap
	Le nom de l'hôte, sans la partie domaine . Ex: Entrer "monordinateur" si le nom complet est "monordinateur.exemple.fr"
Domaine	sandbox.local
	Le domaine parent de l'hôte . Ex: Entrer "exemple.fr" pour "monordinateur.exemple.fr"
Adresse IP	10.16.1.1
	IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3



### 7. SRV-GUACAMOLE

Options de surcharge	e d'hôte
Hôte	SRV-GUACAMOLE
	Le nom de l'hôte, sans la partie domaine . Ex: Entrer "monordinateur" si le nom complet est "monordinateur.exemple.fr"
Domaine	sandbox.local
	Le domaine parent de l'hôte . Ex: Entrer "exemple.fr" pour "monordinateur.exemple.fr"
Adresse IP	10.16.1.3
	IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3

#### 8. SRV-SUPERVISION

Options de surcharge d'hôte			
Hôte	srv-supervision		
	Le nom de l'hôte, sans la partie domaine . Ex: Entrer "monordinateur" si le nom complet est "monordinateur.exemple.fr"		
Domaine	sandbox.local		
	Le domaine parent de l'hôte . Ex: Entrer "exemple.fr" pour "monordinateur.exemple.fr"		
Adresse IP	10.16.1.4		
	IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3		

#### 9. SRV-AUTO.

Options de surcharge d'hôte			
Hôte	srv-auto		
	Le nom de l'hôte, sans la partie domaine . Ex: Entrer "monordinateur" si le nom complet est "monordinateur.exemple.fr"		
Domaine	sandbox.local		
	Le domaine parent de l'hôte . Ex: Entrer "exemple.fr" pour "monordinateur.exemple.fr"		
Adresse IP	10.16.1.5		
	IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3		



#### 10. HOST-ADMIN

Options de surcharge	d'hôte
Hôte	host-admin
	Le nom de l'hôte, sans la partie domaine . Ex: Entrer "monordinateur" si le nom complet est "monordinateur.exemple.fr"
Domaine	sandbox.local
	. Ex: Entrer "exemple.fr" pour "monordinateur.exemple.fr"
Adresse IP	10.16.1.10
	IPv4 or IPv6 comma-separated addresses to be returned for the host e.g.: 192.168.100.100 or fd00:abcd:: or list 192.168.1.3,192.168.4.5,fc00:123::3

### 11. Une fois tous les hôtes configurer j'applique la configuration.

Surcharges d'hôtes					
Hôte	Domaine parent de l'hôte	IP à renvoyer pour l'hôte	Description	Actions	
host-admin	sandbox.local	10.16.1.10		🖉 🛅	
pfsense	sandbox.local	10.16.1.14		🖉 🛅	
srv-auto	sandbox.local	10.16.1.5		A 🗇	
srv-guacamole	sandbox.local	10.16.1.3		🖉 🛅	
srv-Ildap	sandbox.local	10.16.1.1		🖉 🛅	
srv-supervision	sandbox.local	10.16.1.4		e 🖉 🗖	

Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain,' 1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.



### 5.2 Test configuration DNS

- 1. Je me connecte à ma machine host-admin.
- 2. Je me rends dans la configuration réseau.
- 3. Je modifie mon DNS « 10.16.1.14 » & « sandbox.local » puis j'enregistre ma configuration.

Modification de Wired connection 1						
Nom de la connexion Wire		Wired connection 1				
Général	Ethernet	Sécurité 802.1X	DCB Prox	y Paramètres IPv4	Paramètres IPv6	
Méthode	Manuel					
Adresses						
Adress	e	Masque de rése	Masque de réseau		Ajouter	
10.16.1.10		28	8 10.10		Supprimer	
	Serveurs D	NS 10.16.1.14, 192.16	10.16.1.14, 192.168.1.254			
Domaine	s de recherc	he sandbox.local				
ID	de client DH	СР				

- 4. Je redémarre ma connexion réseau.
- 5. Je fais un ping à tous mes hôtes.
  - a. SRV-LLADP.

```
root@host-admin:~# ping srv-lldap.sandbox.local
PING srv-lldap.sandbox.local (10.16.1.1) 56(84) bytes of data.
64 bytes from srv-lldap.sandbox.local (10.16.1.1): icmp_seq=1 ttl=64 time=0.148
ms
64 bytes from srv-lldap.sandbox.local (10.16.1.1): icmp_seq=2 ttl=64 time=0.209
ms
64 bytes from srv-lldap.sandbox.local (10.16.1.1): icmp_seq=3 ttl=64 time=0.188
ms
64 bytes from srv-lldap.sandbox.local (10.16.1.1): icmp_seq=4 ttl=64 time=0.203
ms
64 bytes from srv-lldap.sandbox.local (10.16.1.1): icmp_seq=4 ttl=64 time=0.203
ms
^C
--- srv-lldap.sandbox.local ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3043ms
rtt min/avg/max/mdev = 0.148/0.187/0.209/0.023 ms
root@host-admin:~#
```

b. SRV-GUACAMOLE

root@host-admin:~# ping srv-guacamole.sandbox.local						
PING srv-guacamole.sandbox.local (10.16.1.3) 56(84) bytes of data.						
64 bytes from srv-guacamole.sandbox.local (10.16.1.3): icmp seq=1 ttl=64 ti	.me=0.					
573 ms						
64 bytes from srv-guacamole.sandbox.local (10.16.1.3): icmp seq=2 ttl=64 ti	.me=0.					
668 ms						
64 bytes from srv-guacamole.sandbox.local (10.16.1.3): icmp_seq=3 ttl=64 ti	.me=0.					
416 ms						
64 bytes from srv-guacamole.sandbox.local (10.16.1.3): icmp seq=4 ttl=64 ti	.me=0.					
453 ms						
-^C						
srv-guacamole.sandbox.local ping statistics						
4 packets transmitted, 4 received, 0% packet loss, time 3004ms						
rtt min/avg/max/mdev = 0.416/0.527/0.668/0.099 ms						



c. SRV-SUPERVISION.

root@host-admin:~# ping srv-supervision.sandbox.local PING srv-supervision.sandbox.local (10.16.1.4) 56(84) bytes of data. 64 bytes from srv-supervision.sandbox.local (10.16.1.4): icmp\_seq=1 ttl=64 time= 0.283 ms 64 bytes from srv-supervision.sandbox.local (10.16.1.4): icmp\_seq=2 ttl=64 time= 0.392 ms 64 bytes from srv-supervision.sandbox.local (10.16.1.4): icmp\_seq=3 ttl=64 time= 0.373 ms 64 bytes from srv-supervision.sandbox.local (10.16.1.4): icmp\_seq=3 ttl=64 time= 0.315 ms ^C --- srv-supervision.sandbox.local ping statistics ---4 packets transmitted, 4 received, 0% packet loss, time 3015ms rtt min/avg/max/mdev = 0.283/0.340/0.392/0.043 ms

# 6 BliblioWeb :

# 6.1 IT-Connect

DNS avec Bind9. : <u>https://urlz.fr/pQZ2</u>

DNS installer un serveur bind sous linux : <u>https://urlz.fr/pQZe</u>

### 6.2 Documentation ubuntu

Documentation Bind9 : <u>https://urlz.fr/pQZm</u>

### 6.3 Malekal

Configurer Bind9 sur Ubuntu, Debian : <u>https://urlz.fr/nfpl</u>



### About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | <u>www.capgemini.com</u>



This document contains information that may be privileged or confidential and is the property of the Capgemini Group.

Company Confidential. Copyright © 2023 Capgemini. All rights reserved.