

# **TP : La mise en place d'un serveur DNS (bind9) sous Debian**

# Configuration SSH

## 1. La génération d'une paire de clés SSH sur le client

```
john@debian:~$ ssh-keygen

john@debian:~$ ls -l .ssh/

total 12
-rw----- 1 john john 2590  7 mars  23:15 id_rsa
-rw-r--r-- 1 john john  565  7 mars  23:15 id_rsa.pub
-rw-r--r-- 1 john john  222  5 mars  15:54 known_hosts
```

## 2. L'exportation de la clé SSH publique du client sur le serveur

```
john@debian:~$ ssh-copy-id bob@192.168.100.5

bob@192.168.100.5's password:

Number of key(s) added: 1
```

### 3. Connexion SSH sur le serveur

```
john@debian:~$ ssh bob@192.168.100.5  
bob@server:~$
```

### 4. Sécurisation de la configuration SSH

- Éditer le fichier `"/etc/ssh/sshd_config"`.

```
bob@server:~$ sudo nano /etc/ssh/sshd_config
```

```
#Configuration SSH
```

```
Port 2222
```

```
PermitRootLogin no
```

```
PubkeyAuthentication yes
```

```
PasswordAuthentication no
```

```
PermitEmptyPasswords no
```

```
ClientAliveInterval 360
```

```
ClientAliveCountMax 0
```

- Redémarre le service SSH.

```
bob@server:~$ sudo systemctl restart ssh
```

# Configuration IP du serveur

**Attention :** Le serveur doit avoir une configuration IP statique.

- Éditer le fichier **"`/etc/network/interfaces`"**.

```
bob@server:~$ sudo nano /etc/network/interfaces
```

```
# The primary network interface
allow-hotplug enp0s3
auto enp0s3
iface enp0s3 inet static
    address 192.168.100.5/24
    gateway 192.168.100.1
```

- Redémarre le service networking.

```
bob@server:~$ sudo systemctl restart networking.service
```

- Vérifier la configuration IP du serveur.

```
bob@server:~$ hostname -I  
  
192.168.100.5
```

## Mise en place d'un pare-feu sur le serveur

### 1. Installation "ufw"

```
bob@server:~$ sudo apt install ufw
```

## 2. Configuration "ufw"

- Ajouter les règles firewall pour les services **SSH** et **DNS**.

```
bob@server:~$ sudo ufw allow 2222
```

```
bob@server:~$ sudo ufw allow dns
```

**ou**

```
bob@server:~$ sudo ufw allow 53/tcp  
bob@server:~$ sudo ufw allow 53/udp
```



### 3. Activation "ufw"

```
bob@server:~$ sudo ufw status
```

```
Status: inactive
```

```
bob@server:~$ sudo ufw enable
```

```
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y  
Firewall is active and enabled on system startup
```

```
bob@server:~$ sudo ufw status
```

To	Action	From
--	-----	----
2222	ALLOW	Anywhere
DNS	ALLOW	Anywhere
2222 (v6)	ALLOW	Anywhere (v6)
DNS (v6)	ALLOW	Anywhere (v6)

## 4. Vérification de l'accessibilité SSH au serveur via le port 2222

```
john@debian:~$ ssh bob@192.168.100.5 -p 2222  
bob@server:~$
```

## Installation et Configuration de "bind9"

### 1. Installation "bind9"

```
bob@server:~$ sudo apt install bind9
```

## 2. Configuration "bind9"

- Changement du hostname du serveur.

```
bob@server:~$ sudo hostnamectl set-hostname ns1  
  
bob@ns1:~$ hostname  
  
ns1
```

- Éditer le fichier **"/etc/hosts"**.

```
bob@ns1:~$ sudo nano /etc/hosts  
  
127.0.0.1      localhost  
127.0.1.1      ns1
```

- Création des fichiers de configuration pour les **"Zone directe"** et **"Zone inversée"**.

```
bob@ns1:~$ cd /etc/bind/
```

```
bob@ns1:/etc/bind$ sudo touch db.direct-zone db.reverse-zone
```

```
bob@ns1:/etc/bind$ ls
```

bind.keys	db.255	db.local	named.conf.default-zones	rndc.key
db.0	db.direct-zone	db.reverse.zone	named.conf.local	zones.rfc1918
db.127	db.empty	named.conf	named.conf.options	

- Configuration du fichier **"/etc/bind/named.conf"**.

```
bob@ns1:/etc/bind$ sudo nano named.conf
```

- Utiliser le modèle de configuration stocké dans le fichier `"/etc/bind/named.conf.default-zones"` afin de configurer le fichier `"/etc/bind/named.conf"`.

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "wf3.local" {
    type master; ←
    file "/etc/bind/db.direct-zone";
};

zone "100.168.192.in-addr.arpa" {
    type master; ←
    file "/etc/bind/db.reverse-zone";
};
```

- Vérifier la bonne configuration du fichier **"/etc/bind/named.conf"** avec la commande **"named-checkconf"**.

```
bob@ns1:/etc/bind$ sudo named-checkconf
```

## Configuration Zone directe :

- Utiliser le modèle de configuration stocké dans le fichier **"/etc/bind/db.local"** afin de configurer le fichier **"db.direct-zone"** crée précédemment.

```
bob@ns1:/etc/bind$ sudo cp db.local db.direct-zone
```

```
bob@ns1:/etc/bind$ sudo nano db.direct-zone
```

```

$TTL      604800
@         IN      SOA      ns1.wf3.local. root.wf3.local. (
                                → 3          ; Serial
                                604800       ; Refresh
                                86400        ; Retry
                                2419200      ; Expire
                                604800      ) ; Negative Cache TTL
;
@         IN      NS       ns1.wf3.local.
ns1.wf3.local IN      A     192.168.100.5
~
~
~

```

## Configuration Zone inversée :

- Utiliser le fichier de configuration "**db.direct-zone**" comme modèle afin de faciliter la configuration du fichier "**db.reverse.zone**" crée précédemment.

```
bob@ns1:/etc/bind$ sudo cp db.direct-zone db.reverse.zone  
bob@ns1:/etc/bind$ sudo nano db.reverse.zone
```

```
$TTL      604800  
@         IN      SOA      ns1.wf3.local. root.wf3.local. (   
                                → 3          ; Serial  
                                604800       ; Refresh  
                                86400       ; Retry  
                                2419200    ; Expire  
                                604800 )    ; Negative Cache TTL  
;  
@         IN      NS       ns1.wf3.local.  
5         IN      PTR      ns1.wf3.local.  
~  
~
```



## Vérification des fichiers de configuration des "Zone directe" et "Zone inversée" :


- Vérification avec la commande "**named-checkzone**".

```
bob@ns1:/etc/bind$ sudo named-checkzone db.direct-zone /etc/bind/db.direct-zone  
zone db.direct-zone/IN: loaded serial 3  
OK
```

```
bob@ns1:/etc/bind$ sudo named-checkzone db.reverse.zone /etc/bind/db.reverse.zone  
zone db.reverse.zone/IN: loaded serial 3  
OK
```

- Redemarrer le service "**bind**".

```
bob@ns1:/etc/bind$ sudo systemctl restart bind9
```

```
bob@ns1:/etc/bind$ sudo systemctl status bind9 
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-03-08 01:42:51 CET; 4s ago
     Docs: man:named(8)
  Main PID: 1924 (named)
    Tasks: 6 (limit: 2340)
   Memory: 20.9M
      CPU: 65ms
   CGroup: /system.slice/named.service
           └─1924 /usr/sbin/named -f -u bind

Mar 08 01:42:51 ns1 named[1924]: network unreachable resolving './NS/IN': 2001:500:2::c#53
Mar 08 01:42:51 ns1 named[1924]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
Mar 08 01:42:51 ns1 named[1924]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Mar 08 01:42:51 ns1 named[1924]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
Mar 08 01:42:51 ns1 named[1924]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
Mar 08 01:42:51 ns1 named[1924]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Mar 08 01:42:51 ns1 named[1924]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
Mar 08 01:42:51 ns1 named[1924]: network unreachable resolving './DNSKEY/IN': 2001:500:200::b#53
Mar 08 01:42:51 ns1 named[1924]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance time>
Mar 08 01:42:51 ns1 named[1924]: resolver priming query complete
lines 1-21/21 (END)
```

**Vérifier que l'adresse IP du "nameserver" est celle du serveur.**

```
bob@ns1:~$ sudo nano /etc/resolv.conf  
  
nameserver 192.168.100.5
```

**Vérifier le bon fonctionnement du serveur DNS :**

- Utilisation de la commande **"nslookup"** sur le serveur.

```
bob@ns1:~$ nslookup 192.168.100.5  
  
5.100.168.192.in-addr.arpa      name = ns1.wf3.local.
```

- Utilisation de la commande "**nslookup**" sur le client.

```
john@debian:~$ nslookup -querytype=A ns1.wf3.local
```

```
Server:          192.168.100.5  
Address:         192.168.100.5#53
```

```
Name:   ns1.wf3.local  
Address: 192.168.100.5
```