

KHOULKHALI MONTASIR  
[www.linkedin.com/in/montasir-k/](https://www.linkedin.com/in/montasir-k/)

## **ArchLinux - Installation de Bind9**

# 2025

Procédure d'installation et  
configuration du service **DNS / DoT**



04/03/2025

# 1 INTRODUCTION

Cette documentation décrit la procédure complète d'installation et de configuration d'un serveur DNS sous Arch Linux en utilisant Bind9, conformément aux bonnes pratiques en matière d'administration système.

Le Domain Name System (DNS) est un élément fondamental des infrastructures réseau, permettant la résolution des noms de domaine en adresses IP et la gestion des zones DNS.

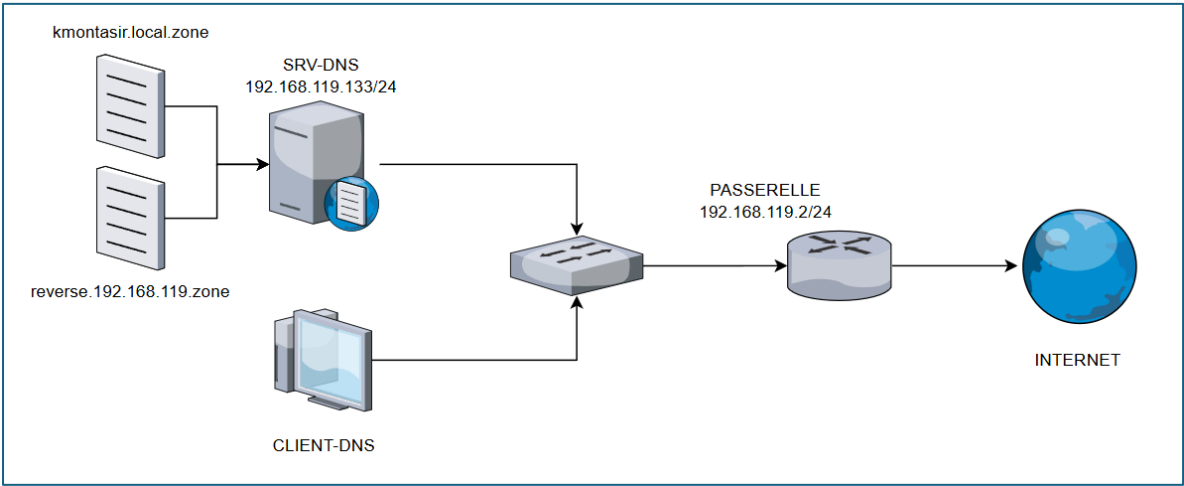
Ce guide détaille chaque étape nécessaire à la mise en place d'un serveur DNS fonctionnel et sécurisé, incluant l'installation, la configuration des zones directes et inverses, ainsi que les tests de bon fonctionnement.

Nous aborderons également la désactivation optionnelle de l'IPv6, la gestion des conflits potentiels avec systemd-resolved, et les vérifications à effectuer pour garantir la fiabilité du service.

Cette procédure s'adresse aux administrateurs système et aux professionnels souhaitant déployer un serveur DNS optimisé sous Arch Linux.

## 2 SCHEMA DE REFERENCE

Le schéma ci-dessous sera utilisé comme référence pour cette procédure :



## 3 TABLE DES MATIERES

1	Introduction.....	2
2	Schéma de référence .....	2
4	Prérequis.....	3
5	Désactivation complète d'IPv6 sur le système (facultatif) .....	3
6	Installation de Bind9 .....	4
7	Problèmes possibles avec systemd-resolved.....	4
8	Configuration de Bind9 .....	5
9	Vérification des permissions et redémarrage de Bind .....	7
10	Tests de la résolution DNS .....	7
11	Configurer un serveur DNS sécurisé (DoT) avec Bind9 et Stunnel.....	8

## 4 PREREQUIS

- **Arch Linux est installé** avec un **compte sudo disponible** sur le serveur cible.
  - **Lien GitHub vers la procédure d'installation d'Arch Linux :**
    - <https://github.com/KMontasir/Procedures/blob/main/ArchLinux/01-ArchLinux-Install.pdf>
- **Une connexion réseau est active** sur le serveur.
- **(Facultatif) : Un accès SSH** sur le serveur cible :
  - **Lien GitHub vers la procédure d'installation du service SSH (OpenSSH) sous Arch Linux :**
    - <https://github.com/KMontasir/Procedures/blob/main/ArchLinux/02-ArchLinux-SSH.pdf>

## 5 DESACTIVATION COMPLETE D'IPv6 SUR LE SYSTEME (FACULTATIF)

Si les besoins nécessitent de **désactiver IPv6 complètement** sur Arch Linux, suivre les étapes ci-dessous.

Ajouter ces lignes dans `/etc/sysctl.d/99-sysctl.conf` :

```
sudo nano /etc/sysctl.d/99-sysctl.conf
```

Ajouter :

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

Puis appliquer les changements :

```
sudo sysctl --system
```

Ajouter `ipv6.disable=1` dans GRUB :

```
sudo nano /etc/default/grub
```

Trouver la ligne :

```
GRUB_CMDLINE_LINUX_DEFAULT="loglevel=3 quiet"
```

Ajouter `ipv6.disable=1` :

```
GRUB_CMDLINE_LINUX_DEFAULT="loglevel=3 quiet ipv6.disable=1"
```

Appliquer les changements :

```
sudo grub-mkconfig -o /boot/grub/grub.cfg
```

Redémarrer le système :

```
sudo reboot
```

## 6 INSTALLATION DE BIND9

S'assurer que le système est à jour, puis installer **Bind9** :

```
sudo pacman -Syu
sudo pacman -S bind
```

## 7 PROBLEMES POSSIBLES AVEC SYSTEMD-RESOLVED

- `systemd-resolved` écoute parfois sur **127.0.0.53:53**, ce qui peut empêcher Bind9 de fonctionner.
- `systemd-resolved` peut forcer l'utilisation de ses propres DNS au lieu de Bind9.
- Si une requête est en cache dans `systemd-resolved`, Bind9 ne la verra pas.

Vérifier si `systemd-resolved` est actif :

```
systemctl is-active systemd-resolved
```

Si la réponse est `active`, alors `systemd-resolved` est en cours d'exécution et pourrait interférer avec Bind9.

Il est possible de voir sur quel port il écoute avec :

```
ss -tulpn | grep 53
```

**127.0.0.53:53**, cela signifie que `systemd-resolved` prend le contrôle du DNS.

Si `systemd-resolved` est actif, le désactiver pour éviter les conflits :

```
sudo systemctl disable --now systemd-resolved
```

Cela va :

- **Arrêter immédiatement** `systemd-resolved`
- **Empêcher son démarrage** au prochain boot

Après avoir désactivé `systemd-resolved`, vérifier que `/etc/resolv.conf` pointe bien vers le serveur Bind9.

Supprimer le lien symbolique (si présent) :

```
sudo rm -f /etc/resolv.conf
```

Créer un fichier `/etc/resolv.conf` propre :

```
sudo nano /etc/resolv.conf
```

Ajouter :

```
nameserver 127.0.0.1
nameserver 192.168.119.133
```

Empêcher `systemd` de le modifier à l'avenir :

```
sudo chattr +i /etc/resolv.conf
```

Activer et démarrer le service `named` :

```
sudo systemctl enable named
sudo systemctl start named
```

Vérifier si le service a démarré correctement :

```
sudo systemctl status named
```

## 8 CONFIGURATION DE BIND9

Le fichier de configuration principal de Bind9 sur Arch Linux est `/etc/named.conf`.

Ouvrir le fichier avec un éditeur de texte :

```
sudo nano /etc/named.conf
```

Le fichier doit être configuré avec les paramètres suivants (le reste peut être supprimé) :

```
options {
    directory "/var/named";
    pid-file "/run/named/named.pid";

    listen-on { 192.168.119.133; 127.0.0.1; };
    listen-on-v6 { none; };

    allow-recursion { 127.0.0.1; 192.168.119.0/24; };
    allow-transfer { none; };
    allow-update { none; };

    version none;
    hostname none;
    server-id none;

    // Ajout du forwarder
    forwarders {
        8.8.8.8;
    };

    // Autoriser les requêtes DNS internes
    allow-query { any; };
};

zone "kmontasir.local" {
    type master;
    file "/var/named/kmontasir.local.zone";
};

zone "119.168.192.in-addr.arpa" {
    type master;
    file "/var/named/reverse.192.168.119.zone";
};

zone "localhost" IN {
    type master;
    file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "127.0.0.zone";
};
```

Créer le répertoire `/var/named` si ce n'est pas déjà fait :

```
sudo mkdir -p /var/named
sudo chown named:named /var/named
```

Créer et éditer le fichier de zone directe :

```
sudo nano /var/named/kmontasir.local.zone
```

Ajouter le contenu suivant :

```
$TTL 86400
@ IN SOA ns1.kmontasir.local. admin.kmontasir.local. (
    2024030301 ; Serial
    3600       ; Refresh
    1800       ; Retry
    604800     ; Expire
    86400 )    ; Minimum TTL

@ IN NS  ns1.kmontasir.local.
ns1 IN A  192.168.119.133
www IN A  192.168.119.150
mail IN A 192.168.119.151
```

Créer et éditer le fichier de zone inverse :

```
sudo nano /var/named/reverse.192.168.119.zone
```

Ajouter le contenu suivant :

```
$TTL 86400
@ IN SOA ns1.kmontasir.local. admin.kmontasir.local. (
    2024030301 ; Serial
    3600       ; Refresh
    1800       ; Retry
    604800     ; Expire
    86400 )    ; Minimum TTL

@ IN NS  ns1.kmontasir.local.
133 IN PTR ns1.kmontasir.local.
150 IN PTR www.kmontasir.local.
151 IN PTR mail.kmontasir.local.
```

Modifier le fichier `/etc/systemd/network/20-wired.network` (à adapter) pour configurer les DNS.

```
sudo nano /etc/systemd/network/20-wired.network
```

La configuration doit être semblable à ceci :

```
[Match]
Name=ens33

[Network]
Address=192.168.119.133/24
Gateway=192.168.119.1
DNS=127.0.0.1
DNS=192.168.119.133
```

Redémarrer le service réseau.

```
sudo systemctl restart systemd-networkd
```

## 9 VERIFICATION DES PERMISSIONS ET REDEMARRAGE DE BIND

Changer les permissions des fichiers de zones :

```
sudo chown named:named /var/named/kmontasir.local.zone
sudo chown named:named /var/named/reverse.192.168.119.zone
sudo chmod 640 /var/named/kmontasir.local.zone
sudo chmod 640 /var/named/reverse.192.168.119.zone
```

Redémarrer Bind pour appliquer les changements :

```
sudo systemctl restart named
```

Vérifier l'état du service :

```
sudo systemctl status named
```

```
archlinux named[750]: managed-keys-zone: loaded serial 2
archlinux named[750]: zone 0.0.127.in-addr.arpa/IN: loaded serial 42
archlinux named[750]: zone kmontasir.local/IN: loaded serial 2024030301
archlinux named[750]: zone localhost/IN: loaded serial 42
archlinux named[750]: zone 119.168.192.in-addr.arpa/IN: loaded serial 2024030301
archlinux named[750]: all zones loaded
archlinux named[750]: FIPS mode is disabled
archlinux named[750]: running
archlinux named[750]: managed-keys-zone: Key 20326 for zone . is now trusted (acceptance timer complete)
archlinux named[750]: managed-keys-zone: Key 38696 for zone . is now trusted (acceptance timer complete)
```

## 10 TESTS DE LA RESOLUTION DNS

Effectuer un test avec `dig` sur le serveur DNS :

```
dig @192.168.119.133 www.kmontasir.local
```

```
;; QUESTION SECTION:
;www.kmontasir.local.      IN      A

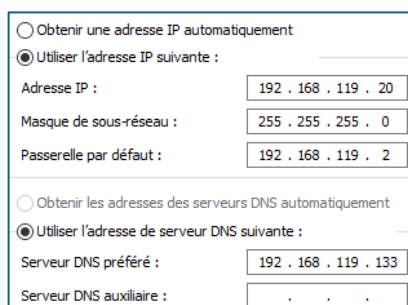
;; ANSWER SECTION:
www.kmontasir.local.      86400   IN      A      192.168.119.150
```

```
dig -x 192.168.119.150 @192.168.119.133
```

```
;; QUESTION SECTION:
;150.119.168.192.in-addr.arpa. IN      PTR

;; ANSWER SECTION:
150.119.168.192.in-addr.arpa. 86400 IN PTR      www.kmontasir.local.
```

Depuis un client Windows : Configurer la carte réseau en renseignant le serveur DNS :



The screenshot shows the 'Internet Protocol Version 4 (TCP/IPv4) Properties' window in Windows. The 'Obtenir une adresse IP automatiquement' option is unselected, and 'Utiliser l'adresse IP suivante' is selected. The IP address is set to 192.168.119.20, the subnet mask to 255.255.255.0, and the default gateway to 192.168.119.2. Below this, the 'Obtenir les adresses des serveurs DNS automatiquement' option is unselected, and 'Utiliser l'adresse de serveur DNS suivante' is selected. The preferred DNS server is set to 192.168.119.133, and the auxiliary DNS server is left blank.

Effectuer un test d'accès vers 8.8.8.8 :

```
ping 8.8.8.8
```

```
PS C:\Users\montasir> ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=27 ms TTL=128
Réponse de 8.8.8.8 : octets=32 temps=12 ms TTL=128
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=128
Réponse de 8.8.8.8 : octets=32 temps=9 ms TTL=128
```

Effectuer ping avec un test de résolution DNS :

```
ping google.com
```

```
PS C:\Users\montasir> ping google.com

Envoi d'une requête 'ping' sur google.com [172.217.20.206] avec 32 octets de données :
Réponse de 172.217.20.206 : octets=32 temps=11 ms TTL=128
Réponse de 172.217.20.206 : octets=32 temps=12 ms TTL=128
Réponse de 172.217.20.206 : octets=32 temps=11 ms TTL=128
Réponse de 172.217.20.206 : octets=32 temps=25 ms TTL=128
```

## 11 CONFIGURER UN SERVEUR DNS SECURISE (DOT) AVEC BIND9 ET STUNNEL

Mettre à jour le système et installer **Stunnel** :

```
sudo pacman -Syu stunnel
```

Ouvrir le fichier de configuration principal de Bind9 :

```
sudo nano /etc/named.conf
```

Ajouter l'option `dnssec-validation auto;` :

```
options {
    // Les options sont ici

    forwarders {
        // Les forwarder sont ici
    };

    dnssec-validation auto;
};
```

Redémarrer Bind9 :

```
sudo systemctl restart named
```

Vérifier le statut :

```
sudo systemctl status named
```

Éditer la configuration de **Stunnel** :

```
sudo nano /etc/stunnel/stunnel.conf
```

Ajouter :

```
[dns]
accept = 0.0.0.0:853
connect = 127.0.0.1:53
cert = /etc/ssl/certs/dns-cert.pem
key = /etc/ssl/private/dns-key.pem
```



Générer un **certificat TLS auto-signé** (Pour en environnement de test) :

```
sudo openssl req -x509 -newkey rsa:4096 -keyout /etc/ssl/private/dns-key.pem -out /etc/ssl/certs/dns-cert.pem -days 365 -nodes
```

Activer et démarrer **Stunnel** :

```
sudo systemctl enable --now stunnel
```

Vérifier que **Stunnel** écoute sur le port **853** :

```
ss -tulpn | grep 853
```

Tester Bind9 en local :

```
dig @127.0.0.1 -p 53 www.google.com
dig @192.168.119.133 -p 53 www.google.com
```

Tester Stunnel avec OpenSSL :

```
openssl s_client -connect 192.168.119.133:853 -servername dns
```

```
[montasir@archlinux ~]$ openssl s_client -connect 192.168.119.133:853 -servername dns
Connecting to 192.168.119.133
CONNECTED(000000003)
depth=0 C=FR, ST=France, L=Lille, O=KMontasir, CN=archlinux.kmontasir.local
verify error:num=18:self-signed certificate
verify return:1
depth=0 C=FR, ST=France, L=Lille, O=KMontasir, CN=archlinux.kmontasir.local
verify return:1
---
Certificate chain
 0 s:C=FR, ST=France, L=Lille, O=KMontasir, CN=archlinux.kmontasir.local
  i:C=FR, ST=France, L=Lille, O=KMontasir, CN=archlinux.kmontasir.local
  a:PKEY: rsaEncryption, 4096 (bit); sigalg: RSA-SHA256
```

**Le serveur est configuré avec le DNS sécurisé (DoT).**