

Mise en place d'un Serveur DNS (Bind9)

Marouane Belmahfoud

 LinkedIn

9 novembre 2025

Table des matières

1	Introduction	2
1.1	Objectif	2
1.2	Prérequis	2
1.3	Architecture Réseau Cible	3
2	Étapes de Configuration	4
2.1	Étape 1 : Démarrer la passerelle DHCP	4
2.2	Étape 2 : Mettre à jour les paquets	5
2.3	Étape 3 : Installer Bind9	6
2.4	Étape 4 : Confirmer l'installation	7
2.5	Étape 5 : Éditer la configuration de Bind9	8
2.6	Étape 6 : Redémarrer le service Bind9	11
2.7	Étape 7 : Tester le serveur DNS	13
2.8	Étape 8 : Éditer la configuration DHCP	15
2.9	Étape 9 : Configurer le DNS dans DHCP	16
2.10	Étape 10 : Redémarrer le service DHCP	18
3	Conclusion	20
3.1	Récapitulatif des Actions Réalisées	20
3.2	Points Clés à Retenir	20
3.3	Fonctionnement Final	20
3.4	Vérifications Finales	20
3.5	Cas d'Usage	21

1 Introduction

Contexte du Tutoriel

Ce tutoriel vous guide pas à pas dans l'installation et la configuration d'un serveur DNS (Bind9) sur une passerelle Debian/Linux déjà configurée avec un serveur DHCP. L'objectif est de permettre aux clients du réseau interne de résoudre automatiquement les noms de domaine via le DNS local, sans configuration manuelle.

1.1 Objectif

L'objectif principal est de mettre en place un serveur DNS (Bind9) sur la passerelle Debian utilisée précédemment comme serveur DHCP.

Cette configuration permet de :

- Résoudre les noms de domaine pour tous les clients du réseau interne
- Distribuer automatiquement l'adresse du DNS via DHCP
- Améliorer la performance de résolution DNS avec un cache local
- Centraliser la gestion DNS du réseau

1.2 Prérequis

- Une passerelle Debian avec serveur DHCP déjà configuré
- VirtualBox installé et fonctionnel
- Accès administrateur (sudo) sur la machine virtuelle
- Connaissances de base en réseau et DNS

Précautions Importantes

Avant de commencer :

- Assurez-vous que le serveur DHCP fonctionne correctement
- Notez l'adresse IP actuelle de votre passerelle
- Testez la connectivité Internet de la passerelle
- Sauvegardez la configuration DHCP existante

1.3 Architecture Réseau Cible

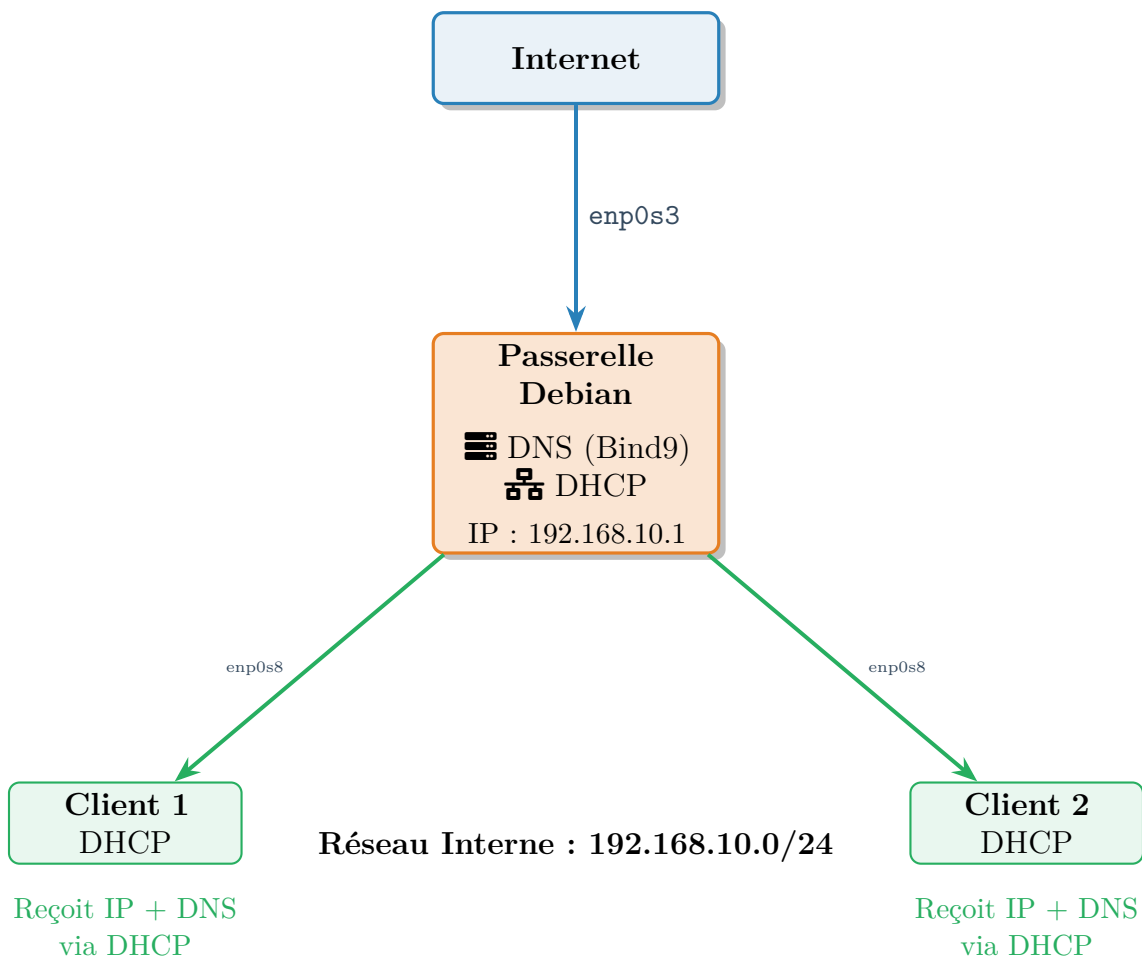


FIGURE 1 – Architecture réseau avec serveur DNS Bind9 et DHCP

i Fonctionnement

Le serveur DNS (Bind9) installé sur la passerelle intercepte les requêtes DNS des clients et les transmet aux DNS publics (1.1.1.1, 8.8.8.8). Le serveur DHCP distribue automatiquement l'adresse du DNS local (192.168.10.1) aux clients du réseau.

2 Étapes de Configuration

2.1 Étape 1 : Démarrer la passerelle DHCP

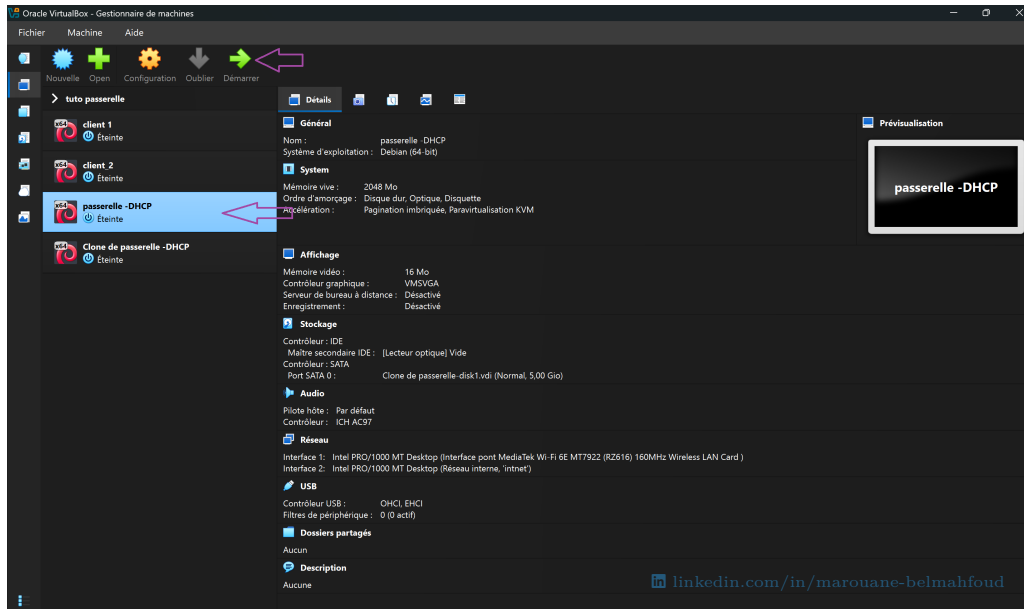


FIGURE 2 – Démarrage de la VM Passerelle DHCP dans VirtualBox

Dans VirtualBox, sélectionnez la machine virtuelle **Passerelle DHCP** puis cliquez sur le bouton **Démarrer**.

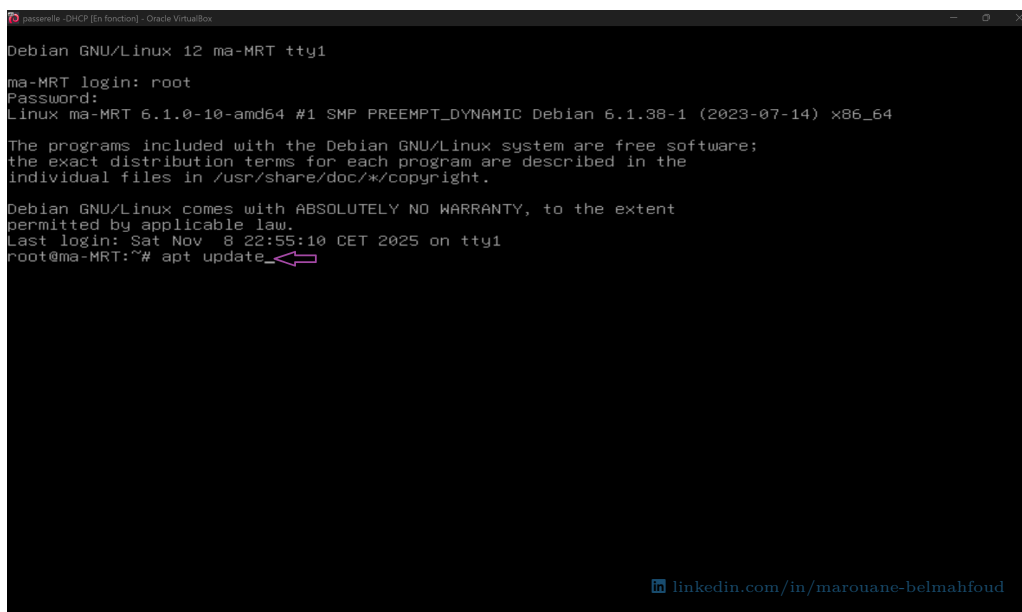
Cette machine servira à héberger le serveur DNS Bind9 en plus du serveur DHCP déjà configuré.

i Machine Virtuelle

La passerelle doit être correctement configurée avec deux interfaces réseau :

- `enp0s3` : Accès pont (Internet)
- `enp0s8` : Réseau interne (192.168.10.0/24)

2.2 Étape 2 : Mettre à jour les paquets



```
Debian GNU/Linux 12 ma-MRT tty1
ma-MRT login: root
Password:
Linux ma-MRT 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov  8 22:55:10 CET 2025 on tty1
root@ma-MRT:~# apt update
```

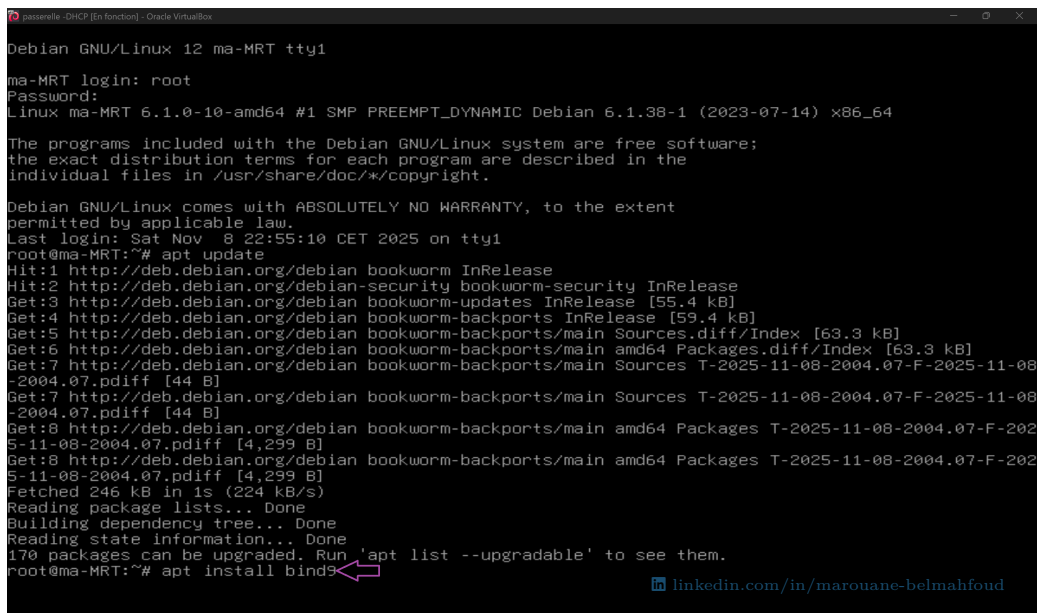
FIGURE 3 – Mise à jour de la liste des paquets

Une fois connecté sur la passerelle, mettez à jour la liste des paquets disponibles :

```
>_ Mise à jour des paquets
1          sudo apt update
```

Cette commande synchronise la liste des paquets avec les dépôts Debian et vérifie les mises à jour disponibles.

2.3 Étape 3 : Installer Bind9



```
Debian GNU/Linux 12 ma-MRT tty1
ma-MRT login: root
Password:
Linux ma-MRT 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Nov  8 22:55:10 CET 2025 on tty1
root@ma-MRT:~# apt update
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://deb.debian.org/debian-security bookworm-security InRelease
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Get:4 http://deb.debian.org/debian bookworm-backports InRelease [59.4 kB]
Get:5 http://deb.debian.org/debian bookworm-backports/main Sources.diff/Index [63.3 kB]
Get:6 http://deb.debian.org/debian bookworm-backports/main amd64 Packages.diff/Index [63.3 kB]
Get:7 http://deb.debian.org/debian bookworm-backports/main Sources T-2025-11-08-2004.07-F-2025-11-08-2004.07.pdiff [44 B]
Get:7 http://deb.debian.org/debian bookworm-backports/main Sources T-2025-11-08-2004.07-F-2025-11-08-2004.07.pdiff [44 B]
Get:8 http://deb.debian.org/debian bookworm-backports/main amd64 Packages T-2025-11-08-2004.07-F-2025-11-08-2004.07.pdiff [4,299 B]
Get:8 http://deb.debian.org/debian bookworm-backports/main amd64 Packages T-2025-11-08-2004.07-F-2025-11-08-2004.07.pdiff [4,299 B]
Fetched 246 kB in 1s (224 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
170 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ma-MRT:~# apt install bind9
```

FIGURE 4 – Installation du serveur DNS Bind9

Installez le serveur DNS Bind9 avec la commande suivante :

>_ Installation de Bind9

```
1 sudo apt install bind9
```

Bind9 est le serveur DNS le plus utilisé sous Linux. Il permet de résoudre les noms de domaine et de gérer un cache DNS local.

2.4 Étape 4 : Confirmer l'installation

```
root@ma-MRT:~# apt update
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://deb.debian.org/debian-security bookworm-security InRelease
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Get:4 http://deb.debian.org/debian bookworm-backports InRelease [59.4 kB]
Get:5 http://deb.debian.org/debian bookworm-backports/main Sources.diff/Index [63.3 kB]
Get:6 http://deb.debian.org/debian bookworm-backports/main amd64 Packages.diff/Index [63.3 kB]
Get:7 http://deb.debian.org/debian bookworm-backports/main Sources T-2025-11-08-2004.07-F-2025-11-08-2004.07.pdiff [44 B]
Get:7 http://deb.debian.org/debian bookworm-backports/main Sources T-2025-11-08-2004.07-F-2025-11-08-2004.07.pdiff [44 B]
Get:8 http://deb.debian.org/debian bookworm-backports/main amd64 Packages T-2025-11-08-2004.07-F-2025-11-08-2004.07.pdiff [4,299 B]
Get:8 http://deb.debian.org/debian bookworm-backports/main amd64 Packages T-2025-11-08-2004.07-F-2025-11-08-2004.07.pdiff [4,299 B]
Fetched 246 kB in 1s (224 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
170 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@ma-MRT:~# apt install bind9
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  bind9-dnswutils bind9-host bind9-libs bind9-utils dns-root-data
Suggested packages:
  bind-doc resolvconf ufw
The following NEW packages will be installed:
  bind9 bind9-utils dns-root-data
The following packages will be upgraded:
  bind9-dnswutils bind9-host bind9-libs
3 upgraded, 3 newly installed, 0 to remove and 167 not upgraded.
Need to get 1,806 kB of archives.
After this operation, 4,311 kB disk space will be freed.
Do you want to continue? [Y/n] Y
```

FIGURE 5 – Confirmation de l'installation

Le système demande une confirmation avant de télécharger et d'installer les paquets. Tapez **Y** (pour Yes) puis appuyez sur **Entrée** pour continuer l'installation. L'installation télécharge Bind9 et toutes ses dépendances nécessaires.

2.5 Étape 5 : Éditer la configuration de Bind9

Capture manquante

La capture d'écran du lancement de l'éditeur nano est manquante, mais cette étape est essentielle.

Vous devez exécuter la commande suivante pour éditer le fichier de configuration de Bind9 :

Édition de la configuration

```
1          sudo nano /etc/bind/named.conf.options
```

```

GNU nano 7.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.
    recursion yes;
    allow-recursion { 192.168.10.0/24; };
    listen-on { 192.168.10.1; };
    allow-query { any; };

    forwarders {
        1.1.1.1;
        8.8.8.8;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation no;

    listen-on-v6 { any; };
};

[ Read 29 lines ]
Help Write Out Where Is Cut Execute Location M-U Undo
Exit Read File Replace Paste Justify Go To Line M-E Redo

```

FIGURE 6 – Configuration des forwarders et options DNS

Dans le fichier `/etc/bind/named.conf.options`, ajoutez ou modifiez la configuration suivante :

```

>_ Configuration Bind9

1         forwarders {
2             1.1.1.1;
3             8.8.8.8;
4         };
5
6         allow-query { any; };
7         listen-on { any; };

```

Explication de la configuration

- `forwarders` : DNS publics utilisés pour résoudre les requêtes (Cloudflare et Google)
- `allow-query { any; }` : Autorise toutes les machines à interroger le DNS
- `listen-on { any; }` : Le serveur écoute sur toutes les interfaces réseau

Adaptation au réseau

Si votre réseau interne utilise un autre sous-réseau que 192.168.10.0/24, adaptez la configuration en conséquence.

Enregistrez les modifications : **Ctrl + O**, puis **Entrée**

Quittez l'éditeur : **Ctrl + X**

2.6 Étape 6 : Redémarrer le service Bind9



```
passerelle -DHCP [En fonction] - Oracle VirtualBox
GNU nano 7.2 /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.
    recursion yes;
    allow-recursion { 192.168.10.0/24; };
    listen-on { 192.168.10.1; };
    allow-query { any; };

    forwarders {
        1.1.1.1;
        8.8.8.8;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation no;

    listen-on-v6 { any; };
};

root@ma-MRT:~# systemctl restart bind9
```

FIGURE 7 – Redémarrage du service DNS

Après avoir modifié la configuration, redémarrez le service Bind9 pour appliquer les changements :

>_ Redémarrage de Bind9

```
1 sudo systemctl restart bind9
```

Si aucune erreur n'apparaît, le service DNS a été redémarré avec succès.

i Vérification du service

Vous pouvez vérifier l'état du service avec :

```
1 sudo systemctl status bind9
```

Le service doit afficher `active (running)`.

2.7 Étape 7 : Tester le serveur DNS

```
passerelle -DHCP [En fonction] - Oracle VirtualBox
// you will need to update your keys. See https://www.isc.org/bind-keys
//=====
dnssec-validation no;

listen-on-v6 { any; };
};

root@ma-MRT:~# systemctl restart bind9
root@ma-MRT:~# dig @192.168.10.1 google.com ←

; <<>> DiG 9.18.41-1~deb12u1-Debian <<>> @192.168.10.1 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3828
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 1232
; COOKIE: 9cc29054d5f97f9a01000000690fd1a90a30a7871557b753 (good) ✓
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                117     IN      A      216.58.214.174

;; Query time: 12 msec
;; SERVER: 192.168.10.1#53(192.168.10.1) (UDP)
;; WHEN: Sun Nov 09 00:26:33 CET 2025
;; MSG SIZE rcvd: 83

root@ma-MRT:~# _
```

FIGURE 8 – Test de résolution DNS avec dig

Testez le bon fonctionnement du serveur DNS en effectuant une requête :

>_ Test DNS

```
1 dig @192.168.10.1 google.com
```

✔ DNS Fonctionnel

Si la configuration est correcte, vous verrez une réponse complète contenant :

- L'adresse IP de google.com dans la section ANSWER
- Le temps de réponse
- Les serveurs DNS utilisés

Cela signifie que le serveur DNS local fonctionne et relaie correctement les requêtes vers les DNS publics configurés.

2.8 Étape 8 : Éditer la configuration DHCP



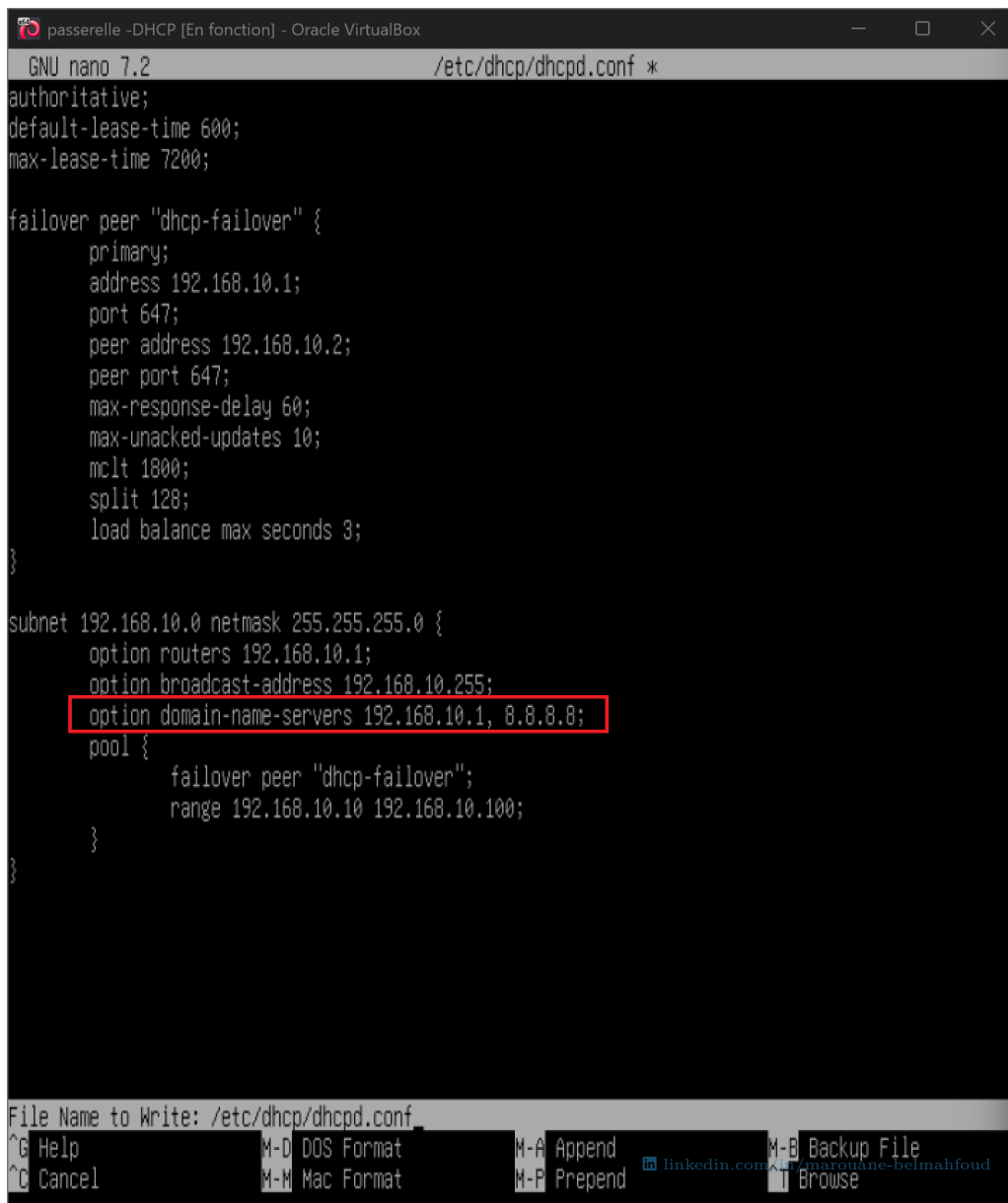
FIGURE 9 – Ouverture du fichier de configuration DHCP

Maintenant que le DNS fonctionne, configurez le serveur DHCP pour distribuer automatiquement l'adresse du DNS aux clients :

>_ Édition de la configuration DHCP

```
1          sudo nano /etc/dhcp/dhcpd.conf
```

2.9 Étape 9 : Configurer le DNS dans DHCP



```
passerelle -DHCP [En fonction] - Oracle VirtualBox
GNU nano 7.2 /etc/dhcp/dhcpd.conf *
authoritative;
default-lease-time 600;
max-lease-time 7200;

failover peer "dhcp-failover" {
    primary;
    address 192.168.10.1;
    port 647;
    peer address 192.168.10.2;
    peer port 647;
    max-response-delay 60;
    max-unacked-updates 10;
    mclt 1800;
    split 128;
    load balance max seconds 3;
}

subnet 192.168.10.0 netmask 255.255.255.0 {
    option routers 192.168.10.1;
    option broadcast-address 192.168.10.255;
    option domain-name-servers 192.168.10.1, 8.8.8.8;
    pool {
        failover peer "dhcp-failover";
        range 192.168.10.10 192.168.10.100;
    }
}

File Name to Write: /etc/dhcp/dhcpd.conf
^G Help      M-D DOS Format  M-A Append     M-B Backup File
^C Cancel    M-M Mac Format  M-P Prepend    M-T Browse
linkedin.com marouane-belmahfoud
```

FIGURE 10 – Modification de l'option domain-name-servers

Dans le fichier `/etc/dhcp/dhcpd.conf`, modifiez la ligne `option domain-name-servers` pour pointer vers votre DNS local :

>_ Configuration DNS via DHCP

```
1          option domain-name-servers 192.168.10.1;
```

 **Adaptation de l'adresse**

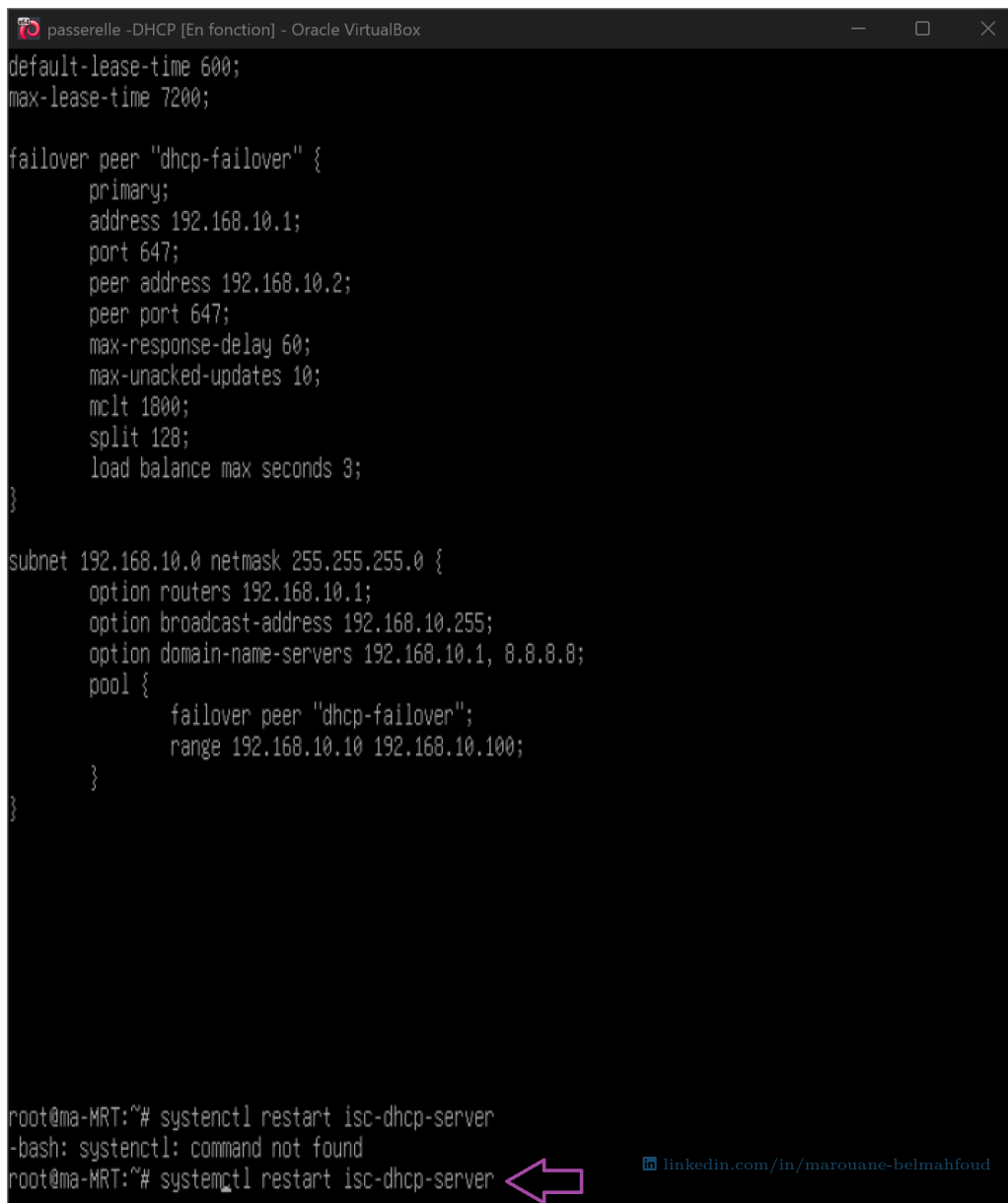
Si votre passerelle possède une adresse IP différente de 192.168.10.1, remplacez-la par l'adresse correcte.

Cette adresse doit correspondre à l'IP de l'interface interne (enp0s8) de votre passerelle.

Enregistrez les modifications : **Ctrl + O**, puis **Entrée**

Quittez l'éditeur : **Ctrl + X**

2.10 Étape 10 : Redémarrer le service DHCP



```
passerelle -DHCP [En fonction] - Oracle VirtualBox
default-lease-time 600;
max-lease-time 7200;

failover peer "dhcp-failover" {
    primary;
    address 192.168.10.1;
    port 647;
    peer address 192.168.10.2;
    peer port 647;
    max-response-delay 60;
    max-unacked-updates 10;
    mclt 1800;
    split 128;
    load balance max seconds 3;
}

subnet 192.168.10.0 netmask 255.255.255.0 {
    option routers 192.168.10.1;
    option broadcast-address 192.168.10.255;
    option domain-name-servers 192.168.10.1, 8.8.8.8;
    pool {
        failover peer "dhcp-failover";
        range 192.168.10.10 192.168.10.100;
    }
}

root@ma-MRT:~# systemctl restart isc-dhcp-server
-bash: systemctl: command not found
root@ma-MRT:~# systemctl restart isc-dhcp-server
```

linkedin.com/in/marouane-belmahfoud

FIGURE 11 – Redémarrage du serveur DHCP

Redémarrez le service DHCP pour appliquer la nouvelle configuration DNS :

>_ Redémarrage du DHCP

```
1 sudo systemctl restart isc-dhcp-server
```

✔ Configuration Terminée

Si aucune erreur n'apparaît, le serveur DHCP est correctement configuré et fonctionnel.

Le serveur DNS Bind9 est maintenant configuré via le DHCP. Les clients du réseau interne recevront automatiquement :

- Une adresse IP via DHCP
- L'adresse du serveur DNS (192.168.10.1)
- La passerelle par défaut

Les clients pourront résoudre les noms de domaine sans aucune configuration manuelle !

3 Conclusion

✓ Installation Réussie !

Félicitations! Vous avez installé et configuré avec succès un serveur DNS Bind9 sur votre passerelle Debian.

3.1 Récapitulatif des Actions Réalisées

1. **Installation de Bind9** : Serveur DNS installé sur la passerelle
2. **Configuration des forwarders** : DNS publics (1.1.1.1 et 8.8.8.8) configurés
3. **Test du DNS** : Vérification avec la commande `dig`
4. **Configuration DHCP** : Distribution automatique de l'adresse DNS aux clients
5. **Redémarrage des services** : Application et validation des configurations

3.2 Points Clés à Retenir

i Bonnes Pratiques

- Le serveur DNS doit être opérationnel avant de configurer le DHCP
- Toujours tester la résolution DNS avec `dig` ou `nslookup`
- Les clients doivent redémarrer leur interface réseau pour obtenir le nouveau DNS
- Documenter les adresses IP et configurations pour faciliter la maintenance

3.3 Fonctionnement Final

Flux de résolution DNS :

1. Un client du réseau interne reçoit son IP et l'adresse du DNS via DHCP
2. Le client effectue une requête DNS (exemple : `www.google.com`)
3. La requête est envoyée au serveur Bind9 (192.168.10.1)
4. Bind9 consulte son cache ou transmet la requête aux forwarders (1.1.1.1, 8.8.8.8)
5. La réponse est renvoyée au client
6. Le résultat est mis en cache pour les futures requêtes

3.4 Vérifications Finales

Pour s'assurer que tout fonctionne correctement :

>_ Tests de Validation

```
1          # Vérifier l'état du service Bind9
2          sudo systemctl status bind9
3
```

```
4      # Verifier l'etat du service DHCP
5      sudo systemctl status isc-dhcp-server
6
7      # Tester la resolution DNS localement
8      dig @192.168.10.1 www.debian.org
9
10     # Depuis un client, verifier le DNS recu
11     cat /etc/resolv.conf
```

3.5 Cas d'Usage

Votre infrastructure DNS est maintenant prête pour :

- **Navigation Internet** : Résolution automatique des noms de domaine
- **Performance améliorée** : Cache DNS local pour des réponses plus rapides
- **Contrôle centralisé** : Gestion du DNS pour tout le réseau interne
- **Évolution future** : Ajout de zones DNS personnalisées si nécessaire

✓ Prochaines Étapes

Vous pouvez maintenant explorer des configurations avancées comme :

- La création de zones DNS internes pour votre réseau
- La mise en place de DNS secondaire pour la redondance
- La configuration de vues DNS conditionnelles
- L'ajout de filtrage DNS pour bloquer certains domaines

✓ Configuration DNS Terminée avec Succès !

Pour toute question ou suggestion, n'hésitez pas à me contacter sur LinkedIn

 [linkedin.com/in/marouane-belmahfoud](https://www.linkedin.com/in/marouane-belmahfoud)