

Configuration de DNS

Hasna Daoui

January 2025

Introduction au DNS dans DHCP

Le **DNS** (Domain Name System) et le **DHCP** (Dynamic Host Configuration Protocol) sont deux protocoles essentiels dans les réseaux informatiques, souvent utilisés ensemble pour faciliter la gestion des adresses IP et des noms de domaine.

Rôle du DNS dans DHCP

Le DNS permet de résoudre les noms de domaine en adresses IP, offrant ainsi une méthode conviviale pour accéder aux ressources réseau. Par exemple, il est plus simple pour un utilisateur de se connecter à **example.com** qu'à une adresse IP comme **192.168.1.1**.

Le DHCP, quant à lui, attribue dynamiquement des adresses IP et d'autres paramètres réseau aux appareils clients. En intégrant le DNS dans la configuration DHCP, un serveur DHCP peut automatiquement fournir aux clients les informations nécessaires pour utiliser un serveur DNS. Cela permet aux clients de résoudre les noms de domaine dès qu'ils obtiennent une adresse IP.

Avantages de l'Intégration DNS-DHCP

- **Simplification de la gestion réseau** : Les clients reçoivent automatiquement les informations DNS nécessaires, réduisant ainsi le besoin de configuration manuelle.
- **Mise à jour automatique du DNS** : Certains serveurs DHCP peuvent mettre à jour dynamiquement les enregistrements DNS pour refléter les nouvelles adresses IP des clients.
- **Optimisation de la connectivité** : En assurant que tous les appareils du réseau ont un accès correct au serveur DNS, la résolution de noms de domaine devient fiable et rapide.

Objectif de la Configuration DNS dans DHCP

Le but de cette configuration est de permettre au serveur DHCP de transmettre les adresses des serveurs DNS aux clients, ainsi que d'intégrer des fonctionnalités avancées telles que les mises à jour dynamiques du DNS. Cela garantit un réseau efficace, avec une résolution rapide des noms de domaine et une gestion centralisée des adresses IP et DNS.

Dans les sections suivantes, les étapes détaillées pour configurer le DNS dans un serveur DHCP seront abordées.

Objectifs du TP :

- Installer et configurer un serveur DNS avec BIND.
- Configurer un domaine personnalisé : EIDIA.UEMF.
- Créer des zones DNS (zone principale, reverse lookup).
- Tester la configuration.

Étape 1 : Installation de BIND

0.1 Mettre à jour les paquets sur votre machine :

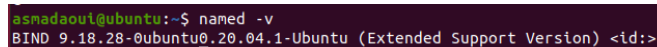
```
sudo apt update  
sudo apt upgrade
```

0.2 Installer BIND et les outils associés :

```
sudo apt install bind9 bind9utils bind9-doc dnsutils
```

0.3 Vérifiez si BIND est correctement installé en vérifiant la version :

```
named -v
```



```
asnadaoui@ubuntu:~$ named -v  
BIND 9.18.28-0ubuntu0.20.04.1-Ubuntu (Extended Support Version) <id:>
```

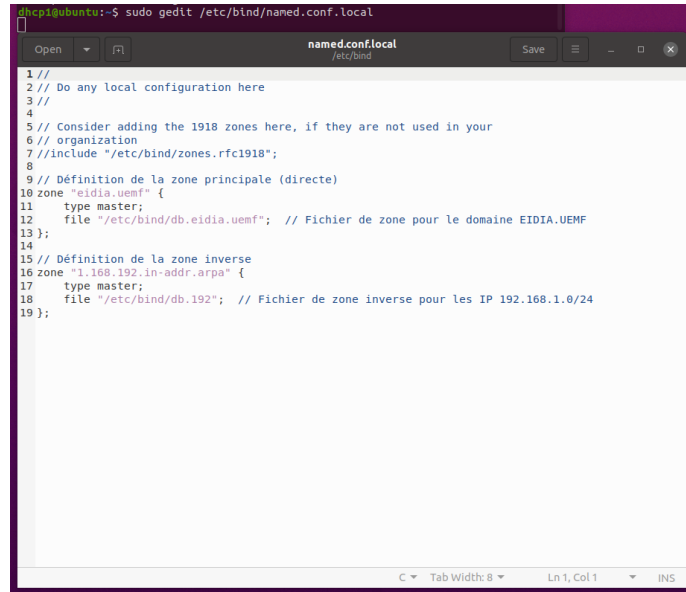
Étape 2 : Configuration des zones DNS

0.4 Configurer le fichier de configuration principal (named.conf)

Les fichiers de configuration de BIND sont stockés dans `/etc/bind/`. Le fichier principal de configuration est `/etc/bind/named.conf`. Modifier le fichier `named.conf.local` pour définir les zones :

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

Ajouter les lignes suivantes pour définir la zone directe et la zone inverse :



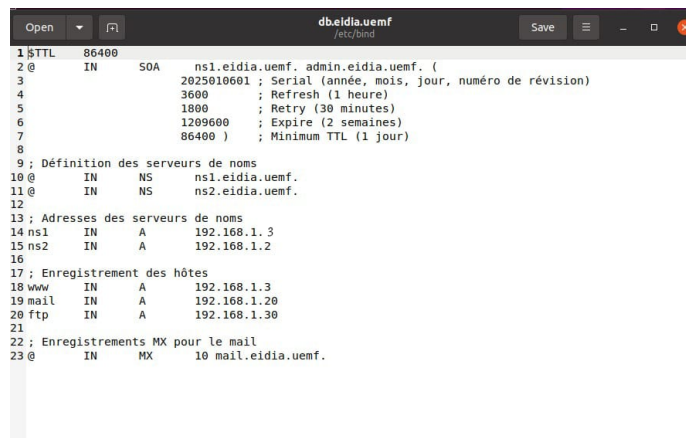
```
1 //
2 // Do any local configuration here
3 //
4
5 // Consider adding the 1918 zones here, if they are not used in your
6 // organization
7 //include "/etc/bind/zones.rfc1918";
8
9 // Définition de la zone principale (directe)
10 zone "eidia.uemf" {
11     type master;
12     file "/etc/bind/db.eidia.uemf"; // Fichier de zone pour le domaine EIDIA.UEMF
13 };
14
15 // Définition de la zone inverse
16 zone "1.168.192.in-addr.arpa" {
17     type master;
18     file "/etc/bind/db.192"; // Fichier de zone inverse pour les IP 192.168.1.0/24
19 };
```

0.5 Configurer la zone directe

Créez un fichier de zone pour EIDIA.UEMF.

`sudo nano /etc/bind/db.eidia.uemf`

Ajoutez le contenu suivant dans le fichier de zone :



```
1 $TTL 86400
2 @ IN SOA ns1.eidia.uemf. admin.eidia.uemf. (
3     2025010601 ; Serial (année, mois, jour, numéro de révision)
4     3600      ; Refresh (1 heure)
5     1800      ; Retry (30 minutes)
6     1209600   ; Expire (2 semaines)
7     86400     ; Minimum TTL (1 jour)
8
9 ; Définition des serveurs de noms
10 @ IN NS ns1.eidia.uemf.
11 @ IN NS ns2.eidia.uemf.
12
13 ; Adresses des serveurs de noms
14 ns1 IN A 192.168.1.3
15 ns2 IN A 192.168.1.2
16
17 ; Enregistrement des hôtes
18 www IN A 192.168.1.3
19 mail IN A 192.168.1.20
20 ftp IN A 192.168.1.30
21
22 ; Enregistrements MX pour le mail
23 @ IN MX 10 mail.eidia.uemf.
```

Explications :

- SOA définit le start of authority, la première ligne d'une zone.
- NS définit les serveurs de noms pour ce domaine.
- A définit les adresses IP pour des sous-domaines (par exemple, `\href{http://www.eidia.uemf/}{www.ei`
- MX définit les serveurs de messagerie.

0.6 Configurer la zone inverse

Créez le fichier de zone inverse :

```
sudo nano /etc/bind/db.192
```

```
GNU nano 4.8
$TTL      86400
@          IN      SOA      ns1.eidia.uemf. admin.eidia.uemf. (
                                2025010601 ; Serial
                                3600       ; Refresh
                                1800       ; Retry
                                1209600    ; Expire
                                86400      ; Minimum TTL

; Définition des serveurs de noms
@          IN      NS       ns1.eidia.uemf.
@          IN      NS       ns2.eidia.uemf.

; Enregistrements PTR (pour la résolution inverse)
3         IN      PTR       ns1.eidia.uemf.
2         IN      PTR       ns2.eidia.uemf.
10        IN      PTR       www.eidia.uemf.
20        IN      PTR       mail.eidia.uemf.
30        IN      PTR       ftp.eidia.uemf.
```

0.6.1 Explications :

Les enregistrements PTR permettent de résoudre les adresses IP en noms de domaine.

Chaque octet de l'adresse IP inverse est écrit à l'envers, par exemple pour l'IP **192.168.1.1**, le nom inverse est **1.1.168.192.in-addr.arpa**.

Étape 3 : Vérification de la configuration

0.6.2 Vérifiez la configuration de BIND pour s'assurer qu'il n'y a pas d'erreurs de syntaxe :

```
sudo named-checkconf
```

0.6.3 Vérifiez les fichiers de zone :

```
sudo named-checkzone eidia.uemf /etc/bind/db.eidia.uemf
sudo named-checkzone 0.168.192.in-addr.arpa /etc/bind/db.192
```

```
server@ubuntu:~$ sudo named-checkconf
server@ubuntu:~$ sudo named-checkzone eidia.uemf /etc/bind/db.eidia.uemf
zone eidia.uemf/IN: loaded serial 2025010601
OK
server@ubuntu:~$ sudo named-checkzone 0.168.192.in-addr.arpa /etc/bind/db.192
zone 0.168.192.in-addr.arpa/IN: loaded serial 2025010601
OK
server@ubuntu:~$ sudo systemctl restart bind9
server@ubuntu:~$ sudo systemctl enable bind9
Failed to enable unit: Refusing to operate on alias name or linked unit file: bind9.service
```

0.6.4 Redémarrez le service BIND pour appliquer la configuration :

```
sudo systemctl restart bind9
```

0.6.5 Activez BIND au démarrage :

```
sudo systemctl enable bind9
```

```
dhcp1@ubuntu:~$ sudo named-checkconf
dhcp1@ubuntu:~$ sudo named-checkzone eidia.uemf /etc/bind/db.eidia.uemf
zone eidia.uemf/IN: loaded serial 2025010601
OK
dhcp1@ubuntu:~$ sudo named-checkzone 0.168.192.in-addr.arpa /etc/bind/db.192
zone 0.168.192.in-addr.arpa/IN: loaded serial 2025010601
OK
dhcp1@ubuntu:~$ sudo systemctl restart bind9
dhcp1@ubuntu:~$ sudo systemctl enable bind9
```

1 Étape 4 : Tester la configuration

1.1 Tester la résolution de noms (forward lookup) :

Utilisez **dig** ou **nslookup** pour vérifier si le serveur DNS répond correctement aux requêtes :

```
dig @localhost www.eidia.uemf
dig @localhost mail.eidia.uemf
Tester la résolution inverse (reverse lookup) :
dig @localhost -x 192.168.0.10
dig @localhost -x 192.168.0.20
```

```

dhcp1@ubuntu:~$ dig @localhost mail.eidia.uenf

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> @localhost mail.eidia.uenf
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29445
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 87f8cacb1648ed3701000000678144863212cd95695ae3a2 (good)
;; QUESTION SECTION:
;mail.eidia.uenf.                IN      A

;; ANSWER SECTION:
mail.eidia.uenf.                86400   IN      A      192.168.1.20

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Fri Jan 10 08:02:14 PST 2025
;; MSG SIZE rcvd: 88

dhcp1@ubuntu:~$ dig @localhost www.eidia.uenf

; <<>> DiG 9.18.28-0ubuntu0.20.04.1-Ubuntu <<>> @localhost www.eidia.uenf
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47266
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 19139f87f69358fa01000000678144aed43786788be6aef4 (good)
;; QUESTION SECTION:
;www.eidia.uenf.                IN      A

;; ANSWER SECTION:
www.eidia.uenf.                86400   IN      A      192.168.1.3

;; Query time: 4 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Fri Jan 10 08:02:54 PST 2025
;; MSG SIZE rcvd: 87

```

2 Étape 5 : Configurer un client pour tester

2.1 Configurez un client pour utiliser votre serveur DNS, en ajoutant l'adresse IP de votre serveur DNS dans `/etc/resolv.conf` :

`nameserver 192.168.1.3` (adresse ip de server dhcp)

2.2 testez la résolution des noms à partir du client en utilisant `dig` ou `nslookup` :

```

nslookup www.eidia.uenf
nslookup mail.eidia.uenf

```

3 Configuration de DNS dans DHCP server

on change le dns dans le fichier `.conf` le parametre de *options domaine-name-servers* pour avoir ip de serveur dhcp. car dns est dans meme machine.

```
dhcpi@ubuntu:~$ sudo gedit /etc/resolv.conf
resolv.conf
1# This file is managed by man:systemd-resolved(8). Do not edit.
2#
3# This is a dynamic resolv.conf file for connecting local clients to the
4# internal DNS stub resolver of systemd-resolved. This file lists all
5# configured search domains.
6#
7# Run "resolvectl status" to see details about the uplink DNS servers
8# currently in use.
9#
10# Third party programs must not access this file directly, but only through the
11# symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a different way,
12# replace this symlink by a static file or a different symlink.
13#
14# See man:systemd-resolved.service(8) for details about the supported modes of
15# operation for /etc/resolv.conf.
16
17nameserver 192.168.1.3
18options edns0 trust-ad
```

```
dhcpi@ubuntu:~$ sudo nano /etc/bind/db.eldia.uenf
dhcpi@ubuntu:~$ sudo systemctl restart bind9
dhcpi@ubuntu:~$ nslookup www.eldia.uenf
Server:      192.168.1.3
Address:     192.168.1.3#53

Name:   www.eldia.uenf
Address: 192.168.1.10
```

et en change dans ip adresse de serveur dhcp dans dns pour avoir meme address

Cancel
Wired
Apply

Details
Identity
IPv4
IPv6
Security

Link speed1000 Mb/s

IPv4 Address192.168.1.3

IPv6 Addressfe80::90fa:576d:4362:43a9

Hardware Address00:0C:29:90:A9:3C

Default Route192.168.1.254

DNS192.168.1.3

☒ Connect automatically

☒ Make available to other users

☐ Metered connection: has data limits or can incur charges
Software updates and other large downloads will not be started automatically.

Remove Connection Profile

Open
dhcpd.conf
Save

```

95
96 #shared-network 224-29 {
97 #   subnet 10.17.224.0 netmask 255.255.255.0 {
98 #       option routers rtr-224.example.org;
99 #   }
100 #   subnet 10.0.29.0 netmask 255.255.255.0 {
101 #       option routers rtr-29.example.org;
102 #   }
103 #   pool {
104 #       allow members of "foo";
105 #       range 10.17.224.10 10.17.224.250;
106 #   }
107 #   pool {
108 #       deny members of "foo";
109 #       range 10.0.29.10 10.0.29.230;
110 #   }
111 #}Profile 1
112
113
114
115
116 subnet 192.168.1.0 netmask 255.255.255.0 {
117     range 192.168.1.1 192.168.1.253;
118     option routers 192.168.1.254;
119     option domain-name-servers 192.168.1.3;
120 }
121
122 }
123
124
125 subnet 192.168.2.0 netmask 255.255.255.0 {
126     range 192.168.2.1 192.168.2.253;
127     option routers 192.168.2.254;
128     option domain-name-servers 192.168.2.3;
129 }
130
131
132

```

Plain Text
Tab Width: 8
Ln 1, Col 1
INS

4 Conclusion

Le serveur DNS est essentiel pour la résolution des noms de domaine en adresses IP, facilitant ainsi la navigation et la communication entre les équipements du réseau. Dans ce rapport, nous avons mis en place un serveur DNS capable de gérer les zones de recherche directe et inverse, assurant une résolution rapide et précise des noms tout en renforçant la sécurité du système.