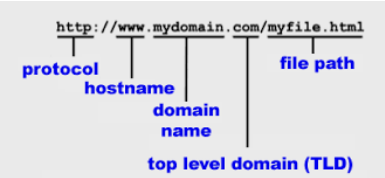
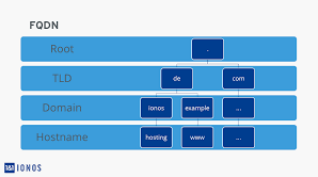



# Mise en place d'un serveur DNS



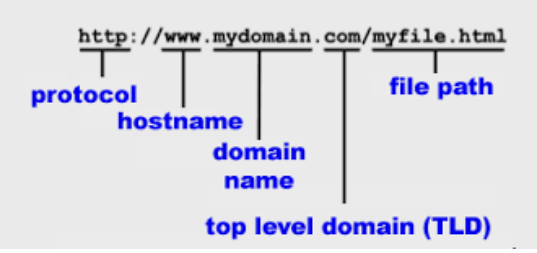

## Table des matières

# Intdoduction :

Tout dabor nous allons parlez du bind qui est un service, il permet de métre en place un serveur de DNS. Domaine Name Server (DNS) ceci nous permettra de faire de la correspondance de nom à une IP. Par exemple si nous avons un serveur lap en 192.168.200.253, sa corespondance IP / nom ce sera lap. Dans un réseau local, par convention, il faut un nom de domaine (Généralement lier à lactiviter de l'entreprise) dans le contexte j'ai choisi un nom de domaine pmmonnier.hyp

Pour mieux comprendre :

Il nous faut un protocole soit http où https, le nom de domaine (pmmonnier) et TLD (.hyp), donc il nous manque le hostname qui luis va nous indiquer le nom d'hote a joindre, comme par exemple le serveur Web nomer LAP, ce qui nous donnera http où https si vous voulez un protocole sécuriser ou pas, hostname (LAP) suivie du nom de domaine (pmmonnier) et du TLD (.hyp)
https://LAP.pmmonnier.hyp




## Contexte :

Dans le cadre pédagogique, nous avons à notre disposition un serveur de virtualisation (PVE), sur ce serveur de virtualisation, il s'y trouve :

- Un réseau locle adresser (192.168.200.0/24)
- Une passerelle
- Un serveur Web
- Un client

À la fin nous aurons dans le réseau local un serveur DNS, qui nous permettera de faire de la corespondance nom IP en local.

# Installation du paquet bind9

Pour installer bind9, il vous suffit d'utiliser cette commande, **apt install bind9**.

Si le DNS ne sait pas répondre à une requette demander, il faut luis renseigner un autre DNS à contacter, ces pourquoi il faut renserigner le Forwarders avec un autre DNS par exemple celuis de google (8.8.8.8). Fichier de configuration se trouve dans **/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.

         forwarders {
                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 auto;

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

## Déclaration des zones :

Pour cette partie nous allons choisir un nom de domaine, cette configuration s'effectue dans le fichier **/etc/bind/named.conf.local**

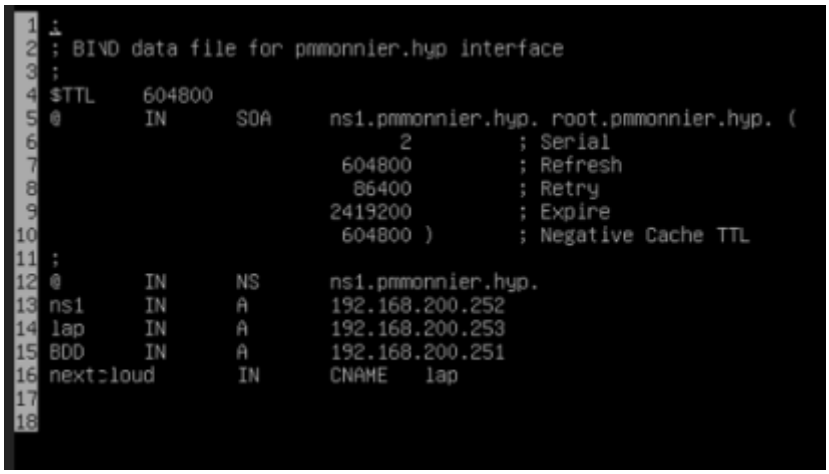
```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
include "/etc/bind/zones.rfc1918";

zone "pmmonnier.hyp" {
        type master;
        file "/etc/bind/db.pmmonnier.hyp";
};

zone "200.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/rev.pmmonnier.hyp";
};
```

D'écommenter les zones rfc1918, ceci sert a interroger les serveurs racine du DNS.

Puis nous déclarons les zones, le nom de domaine sera pmmonnier.hyp, le serveur DNS sera maître, il fera autorité, l'indication ou sont enregistrer les fichiers DNS. En suite nous déclarons le sou réseau qui s'écrit à l'envers, ceci servira à faire une recherche inversée du DNS.

# Configuration des fichiers d'enregistrement.

Pour configuré le fichier il faut copier le fichier **db.local**, comme ceci : **cp db.local db.pmmonnier.hyp** puis vous le renommer par convention avec le nom de votre domaine.



```
;
; BIND data file for pmmonnier.hyp interface
;
$TTL    604800
@       IN      SOA     ns1.pmmonnier.hyp. root.pmmonnier.hyp. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns1.pmmonnier.hyp.
ns1     IN      A       192.168.200.252
lap     IN      A       192.168.200.253
BDD     IN      A       192.168.200.251
nextcloud       IN      CNAME   lap
```

Sur la 2ème ligne vous renseigner le nom du fichier pour ne pas se tromper entre le fichier db | rev
La 5ème ligne nous déclarons le serveur DNS (ns1) Hostname suivie du nom de domaine et son TLD, la 6ème ligne à la 10ème ce sont les paramètres du fichier, ceci veut dire :

| | |
|---|---|
| Serial | Le numéro de série à incrémentation à chaque modification de ce fichier. Par convention ceci et écrit : année-mois-jour-numéro_à_2_chiffres. Ce qui comporte 10 chiffres. |
| Refresh | Ceci est l'expiration du délai de Refresh en secondes, le serveur esclave va renter en communication avec le maître, s'il ne le trouve pas, il fera une nouvelle tentative au bout du délai Retry si se délai expire il considérera que le serveur n'est plus disponible. |
| Retry | Le Nombre de seconds avant d'effectuer une nouvelle demande au serveur maître en cas de non-réponse. |
| Expire | Temps en secondes d'expiration su serveur principal en cas de non-réponse |
| Négative cahe TLL | Durée de vie du cache en secondes |

De la ligne 12 à 16, c'est ici que nous renseignons les informations DNS a déclaré. :

| | | |
|---|---|---|
| @ = Qui fait référence à luis même | IN = Internet | NS = Nom de serveur |
| NS1 = le nom (hostname) | IN | A = l'adresse IPv4 de la machine. |
| Nextcloud = son nom (hostname) | IN | CNAME = c'est un alias qui renvoie sur le serveur LAP, car nextcloud est hébergé sur le serveur Web. |

## Création du fichier inverse :

Copie du ficher d'enregistrement (db.pmmonnier.hyp) en le renommant **rev.votre nom**, ceci permettra de créer le fichier inverse, **cp db.pmmonnier.hyp rev.pmmonnier.hyp**

```
1  ;
2  ; BIND data file for rev.pmmonnier.hyp interface
3  ;
4  $TTL    604800
5  @       IN      SOA     ns1.pmmonnier.hyp. root.pmmonnier.hyp. (
6                                2         ; Serial
7                           604800         ; Refresh
8                            86400         ; Retry
9                          2419200         ; Expire
10                          604800 )       ; Negative Cache TTL
11 ;
12 @       IN      NS      ns1.pmmonnier.hyp.
13 252     IN      PTR     ns1
14 253     IN      PTR     lap
15 251     IN      PTR     BDD
16
```

Sur la ligne 2 modifier le nom du fichier, la ligne 12 à 15 vous remplacer les noms par leur fin d'adresse IP, remplacer A par le PTR (PTR sert aux recherches inverses), puis vous remplacer les IPs par leur nom (hostname). Effectuer un redémarrage de Bind9 **systemctl restart bind9**

## Renseignement du serveur de nom au DHCP.

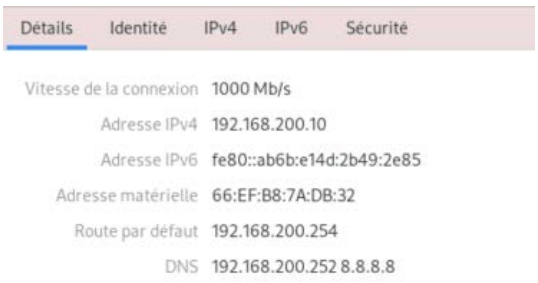
Dans notre contexte nous avons un serveur DHCP, il faut renseigner le serveur DNS dans les fichiers de configuration. Ceci ce déclare dans le fichier **/etc/dhcp/dhcpd.com** sur la ligne 7 vous déclarer votre nom de domaine, sur la ligne 8 vous renseigner votre serveur DNS avec sont adresse IP.

```
1 # dhcpd.conf
2 #
3 # Sample configuration file for ISC dhcpd
4 #
5
6 # option definitions common to all supported ne
7 option domain-name "pmmonnier.hyp";
8 option domain-name-servers 192.168.200.252;
```

## Phase de test :

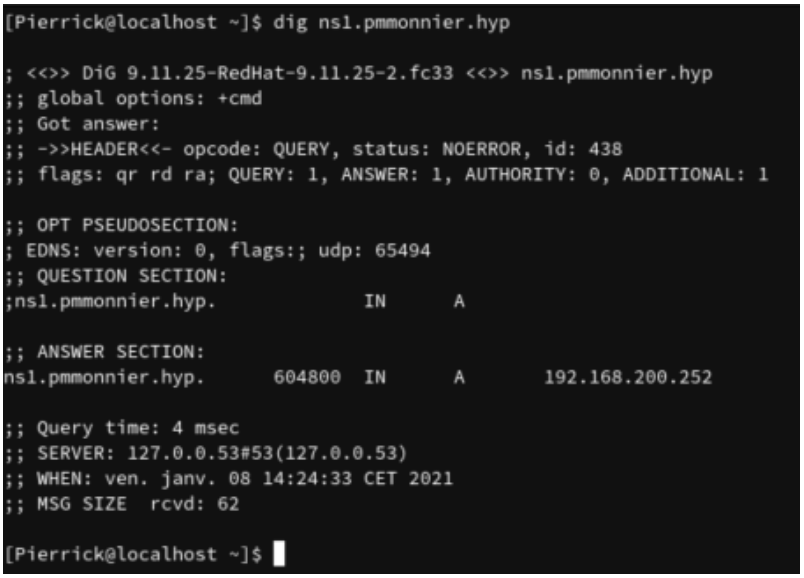
### Test client

Sur notre client, il faut actualiser les paramètres de connexion, ceci nous permettra de récupérer les nouvelles informations du serveur DHCP que nous avons rajouté précédemment.



# Utilisation de la commande DIG

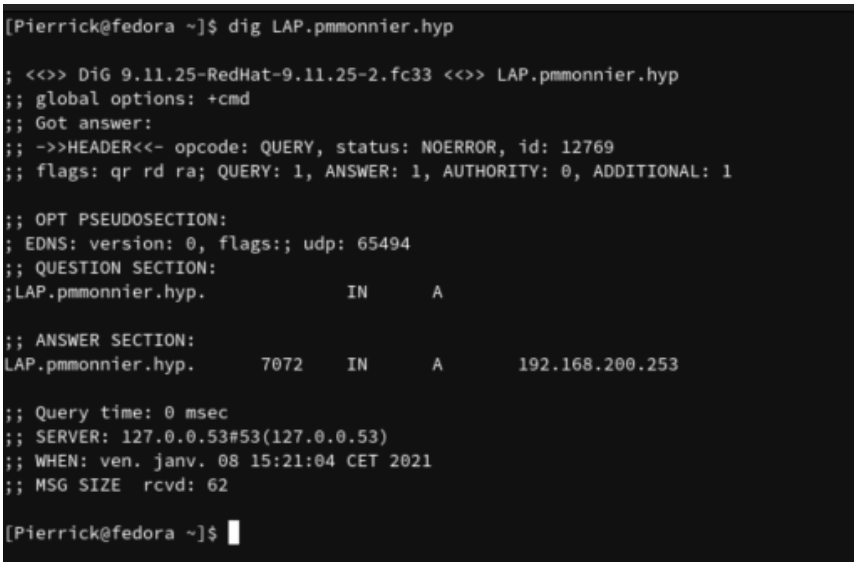
Sur notre client nous alons test la résolution de nom / IP avec la commande dig, cette commande nous permettra de faire des requêtes DNS. Avec cette commande **dig ns1.pmmonnier.hyp** nous voulons savoir qui est ns1.pmmonnier.hyp




| | |
|---|---|
| Ligne 4 ->>HEADER<<- | Cette ligne nous indique si la commande a fonctionner ou pas, ici il nous indique qu'il n'y a pas d'erreur. |
| Ligne 8 QUESTION SECTION | La requete soumise. |
| ligne 10 ANSWER SECTION | La réponse à la question posée. |

## Résultat de la commande DIG

Les résulta que notre client à obetenu et que la résolution DNS, de notre nom de domaine fonctionne, car nous retrouvons notre IP du serveur DNS. Second test, avec comme requete **dig LAP.pmmonnier.hyp**



## Test de la commande DIG inverse.

Depuis notre client nous teston la résolution inverse conclusion, ceci se fait de cette manière **dig -x 192.168.200.253** -x c'est l'option qu'il faut ajouter pour effectuer la redirection inverse.

```
[Pierrick@fedora ~]$ dig -x 192.168.200.253

; <<>> DiG 9.11.25-RedHat-9.11.25-2.fc33 <<>> -x 192.168.200.253
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49487
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;253.200.168.192.in-addr.arpa.  IN      PTR

;; ANSWER SECTION:
253.200.168.192.in-addr.arpa. 604800 IN PTR     lap.200.168.192.in-addr.arpa.

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: ven. janv. 08 15:24:48 CET 2021
;; MSG SIZE  rcvd: 75
```

### Résultat de la commande DIG inverse

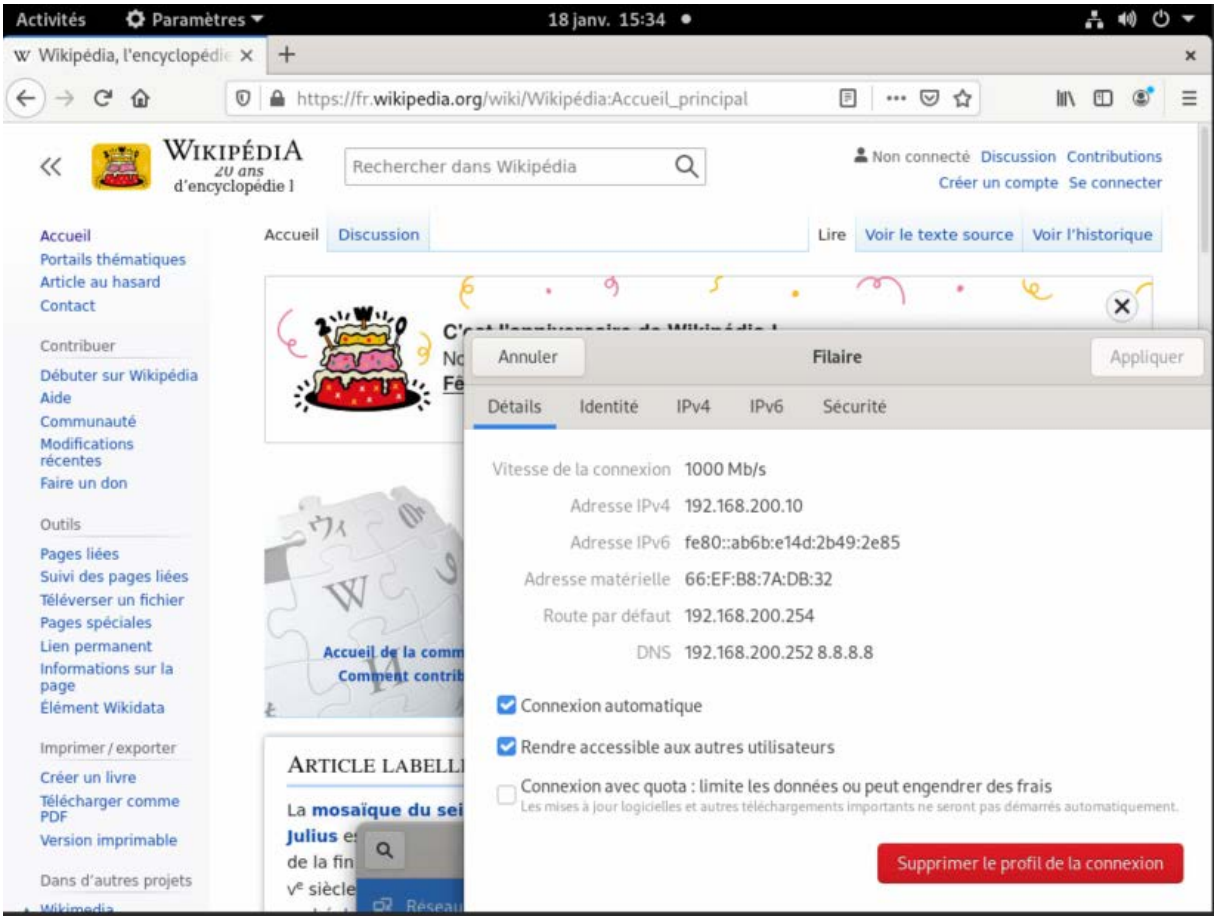
Comme nous pouvons le constater, la commande a fonctionné. Pour savoir si nous effectuons une requête inverse, dans la question, il nous est adressé l'IP à l'envers, donc dans le réseau 253 200 168 192 In-addr.arpa en interne PTR (Pointer Record) qui c'est ? Il nous répond que l'IP correspond au serveur lap.200.168.192.

## Test de résolution de NOM / IP

Test avec le client, si nous voulons afficher notre page web index.html, il suffit de taper cette l'adresse, ATENTION aucun certificat et créer, donc site non sécuriser, [http://lap.pmmonnier.hyp/index.html](http://lap.pmmonnier.hyp/index.html)

## Test de recherche externe :

Avec le client nous éfectuons une recherche sur le client Web avec comme mot clef wikipedia, il nous efectue bien la recherhe donc le Forwarder fonctionne.




## Conclusion :

Nous pouvons constater que notre serveur DNS fonctionne :

- La résolution NOM / IP ✓
- Test Client DNS ✓
- Résolution inverser ✓
- Test page Web externe ✓