Serveur DNS
forward global
et DNS maître (sur une zone)

Le système de noms de domaine (DNS)

Un DNS (domain name system) est nécessaire pour résoudre les noms de domaine et les noms d'hôte en adresses IP.

Remarque : **Chaque élève doit utiliser les plages d'adresses ainsi que le suffixe de domaine qui lui ont été assignés.**

1 Terminologie DNS

Zone

L'espace de noms de domaine est divisé en régions appelées zones. Par exemple, si vous avez opensuse.org, vous avez la section ou la zone opensuse, du domaine org.

Serveur DNS

Le serveur DNS est un serveur qui gère les informations de nom et IP d'un domaine.
Vous pouvez avoir un serveur DNS primaire pour la zone maître, un serveur secondaire pour la zone esclave, ou un serveur DNS sans aucune zone pour la mise en cache.

Serveur DNS de la zone maître

La zone maître inclut tous les hôtes de votre réseau. Une zone maître du serveur DNS stocke les enregistrements à jour pour tous les hôtes de votre domaine dans un fichier local sur le serveur..

Serveur DNS de la zone esclave

Une zone esclave représente une copie de la zone maître. Le serveur DNS de la zone esclave obtient ses données de zone avec des opérations de transfert de zone à partir du serveur maître. Le serveur DNS de la zone esclave répond de façon autoritaire pour la zone tant qu'il a des données de zone valides (qui n'ont pas expirés). Si l'esclave ne peut obtenir de nouvelle copie des données de la zone, il cesse de répondre pour la zone.

Redirecteur (forwarder)

Les redirecteurs sont des serveurs DNS auxquels votre serveur DNS doit envoyer des requêtes auxquelles il ne peut pas répondre. Les serveurs DNS redirecteurs cherchent la réponse à la requête puis répondent à votre serveur DNS.

Enregistrement

L'enregistrement est une information concernant le nom et l'adresse IP. Les enregistrements pris en charge et leur syntaxe sont décrits dans la documentation de BIND. En voici quelques exemples :

Enregistrement NS

Un enregistrement NS indique aux serveurs de noms quelles machines sont chargées d'une zone de domaine donnée.

Enregistrement MX

Les enregistrements MX (mail exchange) décrivent les machines à contacter pour diriger les messages électroniques.

Enregistrement SOA

L'enregistrement SOA (Start of Authority) est le premier enregistrement d'un fichier de zone. L'enregistrement SOA est utilisé pour synchroniser des données entre le DNS primaire (master) et les DNS esclaves.

Installer et préparer le DNS Bind sous Fedora/CentOS Linux

Étape 1 : Introduction

- Installer le service : **sudo yum/dnf install bind**

- Fichiers et dossier du DNS :
  - Fichier de configuration : **/etc/named.conf**
  - Dossier des fichiers de zone : **/var/named/**
  - fichier binaire du service : **/usr/sbin/named**
  - Démarrer le service DNS : **systemctl start named**
  - Arrêter le service DNS : **systemctl stop named**
  - Commande pour le test : **dig, host et nslookup**

Étape 2 : configuration initiale

- Modifier le fichier : /etc/named.conf :
  - Pour écouter sur toutes les interfaces : (remplacer 127.0.0.1 par any)

    listen-on port 53 { any; };
  - Pour accepter les requêtes de résolution de toutes les adresses IP (clientes):

    allow-query { any; };
  - Désactiver les paramètres de sécurité:

    dnssec-enable no;

- Redémarrer le service : **sudo systemctl restart named**
- **Vérifier le démarrage du service : netstat -nulp (le port 53/UDP)**

Étape 3 : Configuration du serveur

- Configuration de la transmission globale des requêtes vers le DNS du collège 10.20.10.20 et/ou 10.20.10.23 ou tout autre DNS publique sur Internet comme 8.8.8.8 ou 1.1.1.1

  Ajoutez les options forward et **forwarders** dans le section **options** du fichier /etc/named.conf

```
options {
        forward only;
        forwarders { 10.20.10.20; 10.20.10.23; };

    listen-on port 53 { any; };
    listen-on-v6 port 53 { ::1; };
    directory       "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { any; };
*/
    recursion yes;

    dnssec-validation no;

    /* Path to ISC DLV key */
    /* In case you want to use ISC DLV, please uncomment the following line. */
    //bindkeys-file "/etc/named.iscdlv.key";

    managed-keys-directory "/var/named/dynamic";
        …

};
```

Étape 4 : Configurer les machine virtuelles A, B et C comme client DNS de votre DNS (A)

- Quel DNS utilise votre machine A : resolvectl -4 dns

```
[miloud@fed38Cin LINUX]$
[miloud@fed38Cin LINUX]$ resolvectl -4 dns
Global:
Link 2 (ens33): 192.168.2.1 207.164.234.193
[miloud@fed38Cin LINUX]$
```

  Quelles adresses IP de DNS utilise la machine virtuelle ?

  ……

- La machine A : qui a une interface bridge : reçoit les adresses IP du DNS par le protocole DHCP (du collège) : soit **10.20.10.20 et 10.20.10.23**

- Les machines B et C : ont des adresses IP statiques (vous devez vous-même) configurer l'adresse(s) IP du DNS.

- Comment modifier l'adresse IP du DNS (sur A) que doit utiliser cette machine virtuelle :
  - Méthode temporaire :
    resolvectl -4 dns ens33 192.168.1.1

    ens33 : spécirifer l'interface bridge
    192.168.1.1 : IP vmnet2 de votre machine A

    Faire un test de résolution de nom : (avec l'une des commandes suivantes)

    dig www.google.ca

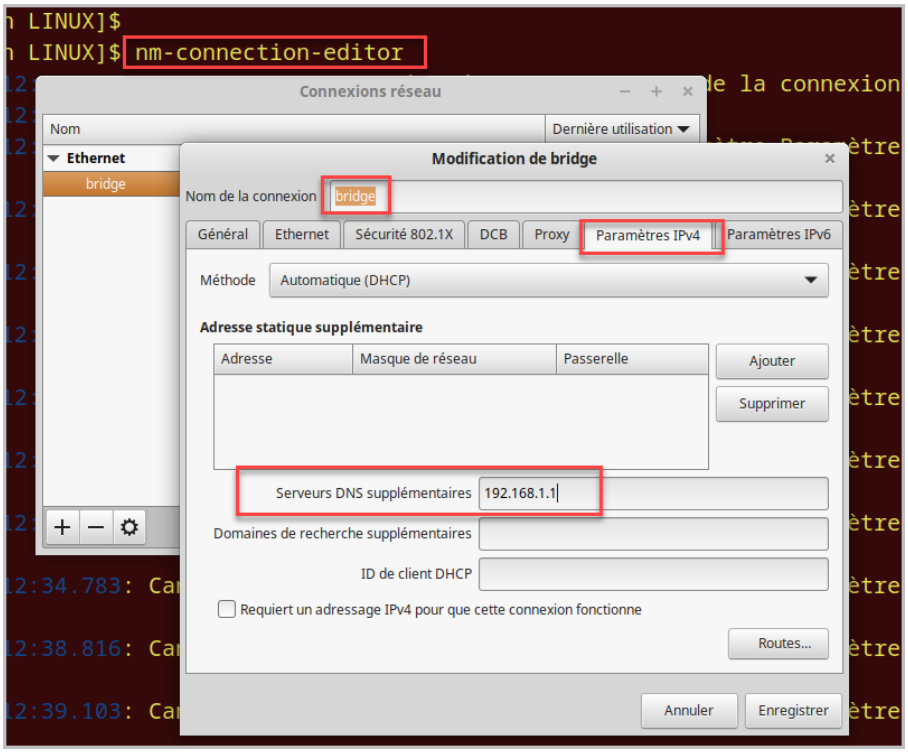
    nslookup www.google.ca

    host www.google.ca

    resolvectl query www.google.ca

    Remarque : Si vous redémarrez le service nmcli : nmcli networking off/on
    La configuration avec resolvectl est supprimée et remplacée par celle fournie par le DHCP sur l'interface ens33.

  - Méthode persistante :
    En utilisant nm-connection-editor :



Fixez l'adresse IP (vmnet2) de A comme IP du DNS.

Faire les tests en redémarrant le service réseau : nmcli networking off/on

Étape 5 : Configurer un DNS primaire sur A

- Configuration de bind : serveur primaire (suffixe de domaine : teccart.tld)
  (Chaque élève doit utiliser le suffixe de domaine qui lui a été assigné).

- Dans le fichier /etc/named.conf (ajouter la déclaration de votre suffixe)

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
....
....

//=============================================================
//  Déclaration de la zone teccart.tld comme type master sur ce DNS

Zone  "teccart.tld." IN {
        type master;
        file "teccart.tld.db";
};
// ============================================================
```

Le fichier de zone teccart.tld.db (qui doit être créé)) est le fichier contenant les ressources (informations des noms à résoudre) localisé dans le dossier /var/named/ :

Dans le dossier **/var/named/** créer le fichier teccart.tld.db (il faut créer ce fichier manuellement et y ajouter les enregistrements):

sudo geany /var/named/teccart.tld.db

```
$TTL 1H
@   SOA   bridge.teccart.tld.   root.bridge.teccart.tld. (
                                                    7
                                                    3H
                                                    1H
                                                    1W
                                                    1H )
          IN       1H       MX       0        vmnet2
          NS       bridge
bridge    IN       1H       A        10.30.31.100
vmnet2    IN       1H       A        192.168.1.1
vmnet3    IN       1H       A        172.16.1.1
www       IN       1H       CNAME    vmnet2
ftp       IN       1H       CNAME    bridge
```

- Redémarrer le service avant de tester :
  sudo systemctl restart named
  dig www.teccart.tld

- Utilisez les commandes pour vérifier et dépanner : named-checkconf et la commande named-checkzone :

  named-chekconf : vérifie la syntaxe du fichier named.conf

  named-checkzone teccart.tld /var/named/teccart.tld.db : verifier le fichier de zone teccart.tld.db

  systemctl restart named

- Faire les tests pour les différents enregistrements :

  Les tests à effectuer :

  dig srv1.teccart.tld

  dig -t CNAME www.teccart.tld

  dig -t MX teccart.tld

Remarque : vérifiez toujours le fichier log en cas de problème et aussi les deux commandes named-check*:

tail -30 /var/log/messages

Complément de Lab-1

1. Editez le fichier : /etc/named.conf

   puis modifiez les options suivantes :
   - **listen-on port 53 {127.0.0.1; };** **pour** **listen-on port 53 {any; };**
   - **allow-query {localhost; };** **pour** **allow-query {any; };**

   ensuite modifiez les options de sécurité comme suit:
   - **dnssec-enable yes;** **pour** **dnssec-enable no;**
   - **dnssec-validation yes;** **pour** **dnssec-validation no;**

   Puis redémarrez le service named : **systemctl restart named**

Répondre aux questions suivantes:

2. Écrire la commande qui affiche les adresses et les ports d'écoute du service named:
   .....
   .....

3. Écrire ces adresses et ces numéros de ports:
   .....
   .....
   .....
   .....

4. Quel est le fichier et le chemin de localisation du fichier de zone de votre zone exemple quebec.tld:
   .....
   .....

5. Qui est l'utilisateur et groupe propriétaire de ce fichier:
   .....
   .....

6. Expliquez l'utilité de l'option de named suivante : listen-on port
   .....
   .....

7. Expliquez l'utilité de l'option de named suivante : allow-query
   .....
   .....

8. Éditez le fichier /etc/named.conf et écrire ci-dessous la section de déclaration de la zone DNS que vous avez configurée:
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....

9. Faire de même pour la zone inverse:
   .....
   .....
   .....
   .....

.....
.....
.....
.....

10. Éditez le fichier de zone : (de votre zone) et y ajouter un enregistrement A (srv-x) avec une adresse fictive (123.2.2.2).

11. Redémarrez le service et testez la résolution de l'enregistrement ajouté.

Travail à faire :

- Configurer une zone inverse du DNS. (Google)