TP Service sur Réseaux N°3 - MMI 2

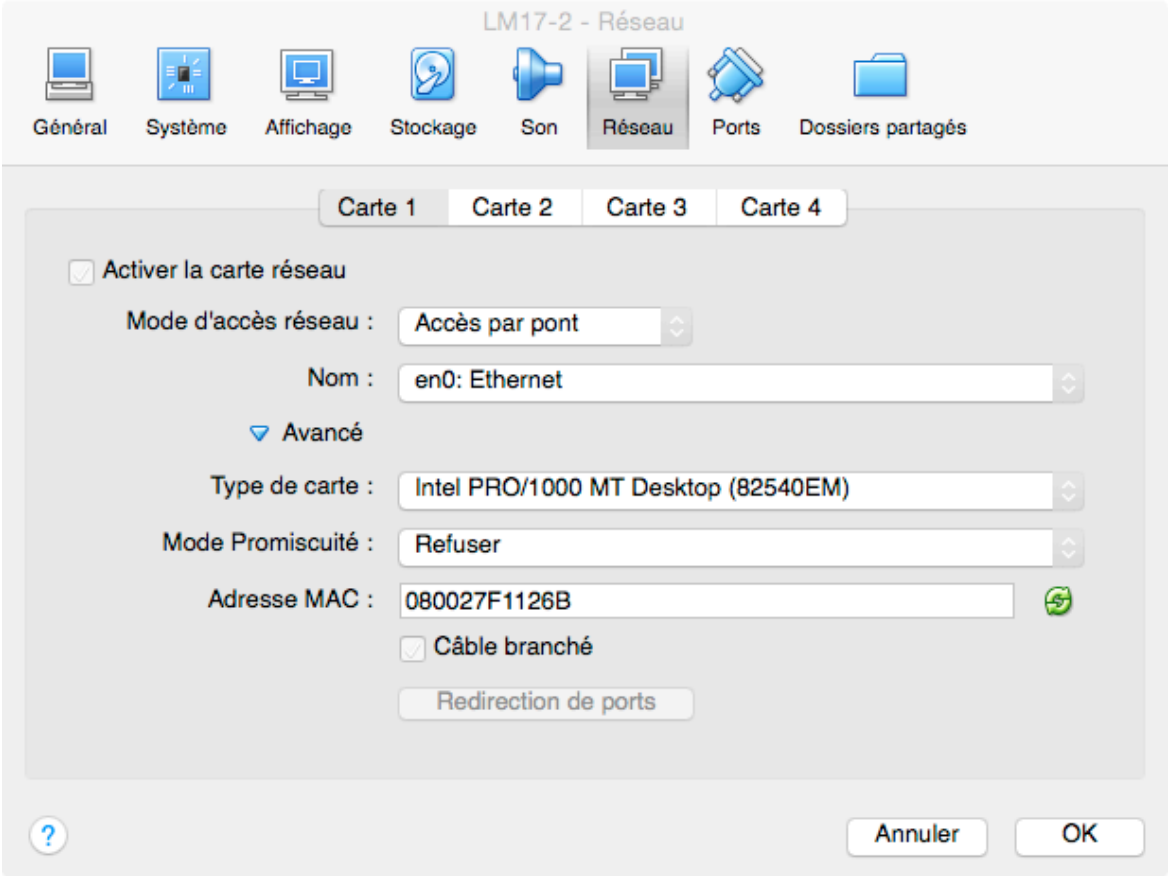
Ce TP permet d'installer un DNS (`bind`) sur un système Linux, à savoir Linux Mint. Ce dernier étant dérivé d'Ubuntu, qui lui même est dérivé de Debian, la configuration vue ici sera valable sur toutes ces distributions. Pour les systèmes dérivé de Red Hat (Fedora, CentOS...), seuls la localisation des fichiers de configuration et le nom des paquets changent, la logique propre à `bind` reste néanmoins la même.

Introduction

Virtualbox

Ouvrez VirtualBox.

Modifiez les paramètres réseaux de la VM, sélectionnez un accès par pont.



et assurez vous que vous allez démarrer la machine LM17 à partir du snapshot 'Fresh Install'.

Une fois la VM démarrée, ouvrez le menu et lancez Konsole.

Installation de bind

Exécutez la commande suivante afin d'installer `bind`, ainsi que divers utilitaires :

```
sudo apt-get install bind9 dnsutils
```

Resolv.conf

Afin de pouvoir travailler de manière autonome, il est nécessaire de changer la configuration de vos postes. Nous allons indiquer à votre machine de désormais, le serveur DNS c'est votre propre machine.

Editez le fichier `/etc/resolvconf/resolv.conf.d/head` et ajoutez votre adresse IP. Exemple :

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by
resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.40.1.xxx
```

Redémarrez le service de résolution par la commande suivante :

```
sudo service resolvconf restart
```

Note	Pour lancer un éditeur en ligne tapez : `sudo nano /etc/resolvconf/resolv.conf.d/head` Les sportifs peuvent utiliser vi au lieu de nano....

Installation d'un serveur DNS standalone

Déclaration des zones

Les fichiers de configurations du DNS se trouvent dans `/etc/bind`. Le fichier de configuration principal est `named.conf`.

Contenu de named.conf :

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in
/etc/bind/named.conf.local


include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

Il ne contient que des inclusions de fichiers. La bonne pratique constiste donc à ne jamais modifier named.conf, mais l'un des 3 fichiers inclus.

Nous allons ajouter notre zone privée dans le fichier `named.conf.local`. La syntaxe est la suivante :

```
zone "labo.fr" {
        type master;
        file "/etc/bind/db.labo.fr";
        };
```

Explications :

- La zone s'appelle 'labo.fr'.
- Le serveur DNS est master pour cette zone (c'est à dire qu'il est DNS primaire)
- La liste des hosts se trouve dans le fichier /etc/bind/db.labo.fr

Nous allons créer ce fichier. Exécutez la commande suivante afin de lancer un éditeur de fichier :

```
sudo nano /etc/bind/db.labo.fr
```

Copier ceci à l'intérieur :

```
labo.fr.      IN      SOA     ns1.labo.fr. admin.labo.fr. (
                              2014120701 ; serial
                              28800      ; refresh (4 hours)
                              3600       ; retry  (1 hour)
                              3600000    ; expire (5 weeks 6 days 16 hours)
                              14400      ; minimum (4 hours)
 )

labo.fr.          IN      NS      ns1.labo.fr.
ns1               IN      A       10.40.1.xxx
prof              IN      A       10.40.1.201
```

Explications :

La première ligne (après SOA) indique le nom du serveur primaire de la zone (ici ns1.labo.fr) et l'adresse mail de la personne à contacter: admin@labo.fr. Vous noterez que l'arobase est remplacé par un point.

• Les informations qui suivent le SOA (entre parenthèses) indiquent respectivement :

- ◦ Serial : Numéro de version : (aammjjVV)
- ◦ Refresh : Pour les serveurs secondaires, période de rafraîchissement (entre deux interrogations), en seconde.
- ◦ Retry : Pour les serveurs secondaires, en cas d 'échec après un transfert de zone, durée minimale avant l'interrogation suivante
- ◦ Expire : durée de vie maximale dans un serveur secondaire si un contrôle de serial number n'a pu être fait (au-delà non garantie)

◦ minimum : durée de conservation d'un enregistrement dans un cache name server

• NS indique les serveurs de nom de la zone. Ici la zone n'est desservie que par un seul serveur : le vôtre.

• A indique pour un nom l'adresse correspondante. Par exemple la machine 'prof' a comme adresse : 10.40.1.201.

Relancez le service bind afin que les modifications soient prises en compte :

```
sudo service bind9 restart
```

Tests et captures

Ouvrez wireshark et observez les échanges lors des opérations suivantes :

```
ping prof.labo.fr
host -t a www.google.com
```

Testez cette dernière commande 2 fois de suite, pourquoi la seconde requête est beaucoup plus courte ?

–

Forwarding

Configurez votre serveur DNS pour qu'il renvoie ses requêtes à un autre serveur DNS. En l'occurrence, celui de l'IUT : 10.40.1.254.

Pour ce faire, ouvrez le fichier `named.conf.options` et renseignez le champ 'forwarders' avec l'IP du DNS de l'IUT.

Redémarrez le service `bind` grâce à la commande vue précédemment.

Lancez une capture réseau avec wireshark, filtrez sur le port 53.

Tapez la commande suivante

```
host -t a www.google.fr
```

Qu'observez-vous ?

–

Zone inverse

Nous venons de mettre en place une résolution dans le sens Nom -> Adresse IP. Pour que le serveur puisse également répondre aux requêtes inverses, il faut ajouter une nouvelle zone dans le fichier named.conf.local.

Editer `/etc/bind/named.conf.local` et ajouter les lignes suivantes :

```
zone "1.40.10.in-addr.arpa" {
        type master;
        file "/etc/bind/db.10.40.1.rev";
};
```

Nous allons créer le fichier 'reverse'. Exécutez la commande suivante afin de lancer un éditeur de fichier :

```
sudo nano /etc/bind/db.10.40.1.rev
```

Copiez ceci à l'intérieur :

```
1.40.10.in-addr.arpa. IN SOA ns1.labo.fr. admin.labo.fr. (
                        2014120701;
                        28800;
                        604800;
                        604800;
                        86400
)

1.40.10.in-addr.arpa.                   IN    NS     ns1.labo.fr.
xxx                                     IN    PTR   ns1.labo.fr.
201                                     IN    PTR   prof.labo.fr.
```

Explications :

Les champs utilisés sont les mêmes que pour la zone `labo.fr`. La seule différence concerne l'enregistrement de type pointeur à la fin du fichier.

Test de la résolution inverse

```
dig 1.40.10.in-addr.arpa. AXFR
```

Tester la zone

```
named-checkzone labo.fr /etc/bind/db.labo.fr
```

Résultat attendu :

```
/etc/bind/db.labo.fr:1: no TTL specified; using SOA MINTTL instead
zone labo.fr/IN: loaded serial 1014120701
OK
```

Tester la syntaxe

Vous pouvez utiliser la commande suivante afin de vérifier la syntaxe de vos fichiers de configuration avant de relancer le démon.

```
named-checkconf
```

Tester le serveur

```
dig @10.40.1.xxx -t SOA labo.fr
```

Si dans les flags vous voyez 'aa', c'est que vous avez reçu une réponse faisant autorité. Votre serveur est donc bien configuré.

Serveur secondaire

Vous allez créer un couple primaire/secondaire en vous mettant par groupe de 2 personnes. Choisissez entre vous et votre voisin qui va être serveur primaire (ns1, adresse IP= 10.40.1.xxx), et qui sera serveur secondaire (ns2, adresse IP= 10.40.1.yyy).

Pour définir un serveur secondaire ns2, nous allons procéder en 3 étapes.

1/ ns1 doit être configuré pour permettre les transferts de zone vers ns2

2/ ns1 doit être configuré pour définir comment les transferts doivent s'effectuer. (ici NOTIFY)

3/ ns2 doit être configuré comme esclave de ns1.

Sur ns1

Tout d'abord, Il faut autoriser le transfert de zone grâce à la directive « allow transfert »

```
zone "labo.fr" {
        type master;
        notify yes;
        also-notify { 10.40.1.yyy ; };
        allow-transfer { 10.40.1.yyy ; };
        file "/etc/bind/db.labo.fr";
        };

zone "1.40.10.in-addr.arpa" {
        type master;
        notify yes;
        also-notify { 10.40.1.yyy ; };
        allow-transfer { 10.40.1.yyy; };
        file "/etc/bind/db.10.40.1.rev";
};
```

Et ajouter le serveur secondaire comme étant un NS de la zone :

```
labo.fr.        IN      NS      ns1.labo.fr.
labo.fr.        IN      NS      ns2.labo.fr.
ns1       IN       A        10.40.1.xxx
ns2       IN       A        10.40.1.yyy
```

Redémarrez le service bind afin de prendre en compte les changements

```
sudo service bind9 restart
```

Sur ns2

Sur le serveur secondaire, précisez le type slave dans le fichier de configuration de la zone, et l'adresse IP du serveur master.

Exemple :

```
zone "labo.fr" {
        type slave;
        file "/var/lib/bind/db.labo.fr";
        masters { 10.40.1.xxx; };
 };
zone "1.40.10.in-addr.arpa" {
        type slave;
        file "/var/lib/bind/db.10.40.1.rev";
        masters { 10.40.1.xxx; };
};
```

Redémarrez le service bind

```
sudo service bind9 restart
```

Consultez le contenu du répertoire /var/lib/bind, il doit désormais contenir les fichiers `db*`.

Editez le fichier `/etc/resolvconf/resolv.conf.d/head` pour chaque serveur (primaire et secondaire) et ajoutez l'adresse IP du serveur secondaire. Exemple :

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by
resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 10.40.1.xxx
nameserver 10.40.1.yyy
```

Redémarrez le service de résolution par la commande suivante :

```
sudo service resolvconf restart
```

Tester le transfert

Créer un nouvel enregistrement dans votre DNS. Relancez le démon et regarder ensuite si votre serveur secondaire a récupéré cet enregistrement.

Vous pouvez utiliser `dig @10.40.1.yyy nom` pour explicitement interroger le DNS 10.40.1.yyy.

Tester la redondance

Fermez le démon `bind` sur ns1 grâce à la commande suivante :

```
sudo service bind9 stop
```

Essayer à présent de lancer un ping sur `prof.labo.fr`

Autres champs

Nous avons vu les enregistrements A et PTR. Il en existent d'autres. Voici les principaux :

CNAME

Il s'agit d'un alias. Attention, il renvoie vers un nom pas une IP.

Exemple pour notre domaine labo.fr :

Enregistrement	Type	
www	A	10.40.1.201
auth	A	10.40.1.122
*	CNAME	www
signon	CNAME	auth

MX

Mail Exchange. Permet d'indiquer aux client de messagerie l'adresse IP du serveur de courrier.

Enregistrement	Type	Priority	
mail	MX	10	10.40.1.2
mail	MX	20	10.40.1.3

TXT

Champ texte. Souvent utilisé pour prouver que vous être bien le propriétaire du domaine.

Enregistrement	Type	
manifest	TXT	Vive les MMI

En vous aidant de la doc, créez tous ces champs sur ns1.