POLYTECHNIQUE MONTRÉAL

INF8480 - Systèmes répartis et infonuagique

TP4 - Services de nom et de temps

Chargés de laboratoire :
Sébastien Darche
Mathias Coulais
Redacteur :
Pierre-Frederick Denys

Automne 2024 - V7.0

1 Introduction

1.1 Prérequis

— **Service de répertoire de noms :** Modèle et Mécanismes. Exemple du DNS
— **Services de temps et de coordination :** Synchronisation d'horloges physiques. Synchronisation par des horloges logiques. Coordination dans un système réparti.

1.2 Buts du TP

— Déploiement de services dans des containers docker
— Compréhension du fonctionnement du service de nom DNS et des enjeux de sécurité
— Compréhension du fonctionnement des services de temps, et de leur importance dans les systèmes distribués

2 Introduction

Le but du TP est de découvrir le fonctionnement des services de nom et de temps. Le déploiement va s'effectuer sur une machine virtuelle comme cela se fait dans l'industrie. La machine virtuelle est en local sur vos machines, mais vous ne pouvez y accéder que par SSH.

2.1 Mise en place de la VM

Suivre les instructions du TP2 pour déployer la VM sur virtualbox et vous y connecter en SSH. **Vous pouvez utiliser encore une fois la même VM déployée lors des TP 2 et 3**. Assurez-vous que le service docker est "up and running" avec `docker ps`, et arrêtez et supprimez les containers du TP précédent si ils tournent encore.

3 Partie 1 : Services de noms

3.1 Introduction

Le but de cette première partie est de mettre en place un service de résolution de noms.

3.2 Mise en place

3.2.1 Introduction

Vous allez lancer dans cette partie plusieurs containers afin de mettre en place l'architecture suivante :
— 1 serveur DNS maitre bind9 pour le domaine `polymtl.ca` : `ns1.polymtl.ca`
— 1 serveur DNS esclave bind9 pour le domaine `polymtl.ca` : `ns2.polymtl.ca`

— 1 serveur web `web.polymtl.ca`
— 1 serveur web `dossieretudiant.polymtl.ca`
— 1 client
— Toutes ces machines sont situées sur le même sous-réseau interne à Docker.

3.2.2 Deux serveurs web

Attention

En règle générale, recopier les commandes à la main vous aide à les comprendre. Cependant, vérifiez que des espaces supplémentaires ne se soient pas ajoutés si vous copiez-coller des commandes depuis le PDF.

Mise en place du serveur de deux serveurs web :

1. Ajouter un réseau docker isolé :

```
docker network create --subnet=172.20.0.0/16 tp4net
```

2. Transférer les fichiers présents dans l'archive disponible sur Moodle TP sur la machine virtuelle avec scp
3. Compiler une image docker "`tp4-web`" avec le dockerfile situé dans l'archive :

```
docker build -t tp4-web .
```

4. Lancer deux containers serveurs web :

```
docker run -dit --net tp4net --ip 172.20.0.4 --name web --hostname web
   -p 8085:80 tp4-web
docker run -dit --net tp4net --ip 172.20.0.5 --name dossieretudiant --
   hostname dossieretudiant -p 8086:80 tp4-web
```

3.2.3 1 seul serveur DNS

Mise en place du serveur de résolution de noms :

1. Lancer un container sur la machine virtuelle avec la commande suivante :

```
docker run --net tp4net --ip 172.20.0.2 -t -d --privileged=true --name
   ns1 --hostname ns1 -p 53 ubuntu
```

2. Se connecter au container `ns1` et et y installer `bind9`
3. Le fichier `/etc/bind/named.conf.local` permet de configurer les domaines que le serveur doit gérer

```
zone "polymtl.ca" {
                type master;
                file "/etc/bind/db.polymtl.ca";
                allow-transfer { 172.20.0.3; };
        };
```

4. La commande suivante vous permet de vérifier si votre fichier de configuration est correct.

```
named-checkconf /etc/bind/named.conf.local
```

5. Configurer ensuite la zone du serveur DNS maître en créant le fichier de la zone (`/etc/bind/db.polymtl.ca`) :

```
$TTL 604800 ; 1 semaine
$ORIGIN polymtl.ca.
@ IN SOA ns1.polymtl.ca. admin.polymtl.ca. (
                              2020102501 ; serial
                              3600 ; refresh (1 hour)
                              3000 ; retry (50 minutes)
                              4619200 ; expire (7 weeks)
                              604800 ; minimum (1 week)
                              )

@ IN NS ns1.polymtl.ca.
@ IN NS ns2
@ IN MX 10 mx1
@ IN MX 20 mx2
ns1 IN A 172.20.0.2
ns2 IN A 172.20.0.3
web IN A 172.20.0.4
```

6. Pour vérifier la syntaxe de ce fichier, lancer la commande suivante :

```
named-checkzone polymtl.ca /etc/bind/db.polymtl.ca
```

7. Nettoyer le cache du serveur (si besoin), et redémarrer le service :

```
rm /var/cache/bind/managed-keys.bind
/sbin/service named restart
```

8. Créer un client, qui va utiliser le serveur DNS :

```
docker run --ip 172.20.0.11 --net tp4net -t -d --privileged=true --name
    client --hostname client ubuntu
```

9. Se connecter sur le container `client`

```
apt-get update && apt-get install dnsutils
```

10. Toujours sur le client **Remplacer** le contenu du fichier `/etc/resolv.conf` par :

```
nameserver 172.20.0.2
```

11. Tester la résolution de nom avec la commande suivante (paquet à installer) (le container `client` utilise maintenant le DNS que l'on vient de mettre en place :

```
nslookup web.polymtl.ca
```

3.2.4 Ajout du second DNS

Nous allons maintenant ajouter un second DNS (esclave) pour faire face aux pannes du DNS maître.

1. Lancer un container sur la machine virtuelle avec la commande suivante et y installer le paquet du serveur DNS :

```
docker run --net tp4net --ip 172.20.0.3 -t -d --privileged=true --name
   ns2 --hostname ns2 -p 53 ubuntu
```

2. Le fichier `/etc/bind/named.conf.local` permet de configurer les domaines que le serveur doit gérer. Le paramètre `masters` permet de dire quel serveur interroger pour reçevoir les mises à jour de zone.

```
zone "polymtl.ca" {
                type slave;
                file "/etc/bind/db.polymtl.ca";
                masters { 172.20.0.2;};
        };
```

3. Sur le client **Remplacer** le contenu du fichier `/etc/resolv.conf` par :

```
nameserver 172.20.0.2
nameserver 172.20.0.3
```

4. Sur le serveur ns1 (container `ns1`), éditer le fichier `db.polymtl.ca`, pour y ajouter l'entrée correspondante à `dossieretudiant.polymtl.ca`. Ne pas oublier de changer le `serial` (voir la doc de bind). Exécutez la commande permettant de vérifier le fichier de zone. Puis relancer le service bind.

On va maintenant tester la répartition de charge entre les deux serveurs DNS depuis le container `client`. Pour cela, un script `test.sh` disponible dans l'archive lance des requêtes de résolution de nom. Transférer ce fichier de la VM vers le client, Installer `curl` dans le client, et exécuter ce script.

```
apt-get install curl
sh test.sh
```

Toutes les commandes du script **doivent réussir** et résoudre correctement les noms de domaines de chacun des containers. Sinon, vérifier vos configurations de zone.

3.2.5 Ouverture

Le contenu du fichier `resolv.conf` est dans la plupart des cas fourni par le routeur d'un réseau. Vous pouvez donc en déduire les vulnérabilités des services de résolution de nom. Si une personne arrive a accéder à l'interface d'administration d'un routeur (trop souvent faiblement protégée, et accessible avec un mot de passe par défaut) elle peut forcer les clients à utiliser un serveur DNS pirate, et rediriger par exemple https ://google.com vers https ://google.com **Avez-vous vu la différence entre les deux URL précédentes ? non ? sûr ? Il y en a pourtant une !**

3.3 Remise

Lancer le script de correction et remettez le résultat sur moodle Exécuter **SUR LA VM** le script de correction (que vous pouvez copier à l'aide de la commande scp) avec le code header obtenu dans la question 1 du quiz. Si le fonctionnement de votre serveur de fichier est correct, le hash obtenu permet de valider la seconde question du quiz.

```
./correct.sh.x code_header_moodle
```

4 Partie 2 : Services de temps

4.1 Introduction

NTP est un protocole qui permet de synchroniser, via un réseau informatique, l'horloge locale d'ordinateurs sur une référence d'heure. Lors de la synchronisation, le client A envoie une requête au serveur B, à la date T_1, B reçoit le message à la date T_2, et envoie une réponse à A à la date T_3. Finalement, A reçoit la réponse à la date T_4. On trouve dans la documentation les deux définitions suivantes :

— **Time offset :** the difference in absolute time between the two clocks
— **round-trip delay :** the length of time it takes for a signal to be sent plus the length of time it takes for an acknowledgement of that signal to be received. This time delay includes the propagation times for the paths between the two communication endpoints.

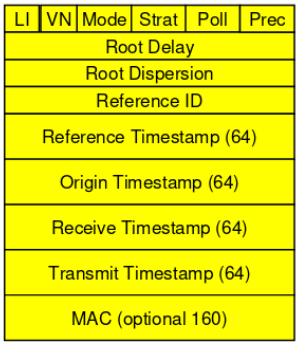
Name	Formula	Description
leap	*leap*	leap indicator (LI)
version	*version*	version number (VN)
mode	*mode*	mode
stratum	*stratum*	stratum
poll	τ	poll interval ($\log_2$ s)
precision	ρ	precision ($\log_2$ s)
rootdelay	Δ	root delay
rootdisp	E	root dispersion
refid	*refid*	reference ID
reftime	*reftime*	reference timestamp
org	T_1	origin timestamp
rec	T_2	receive timestamp
xmt	T_3	transmit timestamp
dst*	T_4	destination timestamp*

Packet Variables

* Strictly speaking, *dst* is not a packet variable; it is the value of the system clock upon arrival.

Name	Formula	Description
keyid		key ID
mac		message digest

Message Authentication Code (MAC)



Voir `https://www.eecis.udel.edu/~mills/database/brief/flow/flow.pdf`

Lors de la synchronisation, le serveur répond par :
— la date à laquelle la requête a été transmise selon le client
— la date à laquelle la requête a été reçue selon le serveur
— la date à laquelle la réponse a été transmise selon le serveur
— la date à laquelle l'horloge du serveur a été réglée pour la dernière fois

4.2 Application pratique

Installer le paquet `ntp` sur votre machine virtuelle, et lancer le daemon ntp. Vous pouvez voir la liste des serveurs sur lesquels le daemon ntp va se connecter pour synchroniser l'horloge de votre VM.

```
sudo service ntp start
ntpq -pn
```

4.3 Analyse

Vous devez utiliser le logiciel Wireshark `https://www.wireshark.org/#download` pour analyser le fichier `trace.pcap` fourni et calculer pour la synchronisation avec le serveur 54.39.23.64 et le serveur 216.232.132.77 le décalage (*offset*, θ) et le délai observé (*delay* δ). Sur quelle serveur l'horloge du client va être synchronisée ?

Conseil

Attention, le temps T_4 (destination timestamp) n'est pas dans les données du paquet NTP, mais c'est le champ `arrival time`.

4.4 Remise

Déposez sur moodle les résultats du calcul de l'offset et du delai.

♢