

## ODE Loïck

mercredi 6 juin 2018 16:43

### ■ Le DNS pour les nuls.

#TODO : mettre un réplica à 1 quand on le déploiera avec docker swarm.

#TODO : Automatisation de la procédure d'ajout d'adresse.

Utilisation de docker-compose pour créer le container.

```
1 #Le volumes n'étant pas sur un NAS il faut qu'il soit présent sur l'hôte.
2 version: '2'
3 services:
4   bind:
5     container_name: dns_server
6     restart: always
7     image: sameersbn/bind:9.9.5-20161106
8     ports:
9       - "53:53/udp"
10      - "53:53/tcp"
11      - "10000:10000/tcp"
12     volumes:
13       - dns-data:/data
14     environment:
15       - ROOT_PASSWORD=I9o8I7c6k5
16     networks:
17
18 volumes:
19   dns_data:
```

Vérification que le container tourne correctement.

Container ID	Name	Image	Command	Created	Status	Ports
913af6bdc9	bind	sameersbn/bind:9.9.5-20161106	"/usr/sbin/inetd -s"	About an hour ago	Up about an hour	0.0.0.0:2222->22/tcp, 0.0.0.0:9999->99/tcp
913af6bdc9	bind	sameersbn/bind:9.9.5-20161106	"/usr/sbin/inetd -s"	2 hours ago	Up 2 hours	0.0.0.0:53->53/tcp, 0.0.0.0:53->53/udp, 0.0.0.0:10000->10000/tcp, 0.0.0.0:10000->10000/udp

On se connecte à l'interface web pour configurer le DHCP, pour cela on se connecte à l'adresse suivante

<https://localhost:10000/> ou <https://<address ip container>:10000/>

Login to Webmin

You must enter a username and password to login to the Webmin server on 172.28.0.2.

Username

Password

☐ Remember login permanently?

Username : root

Password : I9o8I7c6k5

#Si tu aimes pas mon pwd, modifie le dans le docker-compose

#Création du reverse DNS :

Module Config

LOGIN: root

Webmin

System

Servers

Bind DNS Server

Read User Mail

Others

Networking

Hardware

Cluster

Un-used Modules

Search:

View Module's Logs

System Information

Refresh Modules

Logout

Module Config

Global Server Options

Other DNS Servers

Logging and Errors

Access Control Lists

Files and Directories

Forwarding and Transfers

Addresses and Topology

Miscellaneous Options

Control Interface Options

DNS Keys

Zone Defaults

Cluster Slave Servers

Setup RNDNC

DNSSEC Verification

DNSSEC Key Re-Signing

Check BIND Config

Edit Config File

Existing DNS Zones

Select all | Invert selection | Create master zone | Create slave zone | Create stub zone | Create forward zone | Create delegation zone | Create zones from batch file.

☐ Root zone

☐ 0

☐ 127

☐ 172.20.0.2

☐ 255

☐ example.com

☐ localhost

Select all | Invert selection | Create master zone | Create slave zone | Create stub zone | Create forward zone | Create delegation zone | Create zones from batch file.

New master zone options

Zone type ☐ Forward (Names to Addresses) ☒ Reverse (Addresses to Names)

Domain name / Network

Records file ☐ Automatic

Master server  ☒ Add NS record for master server?

Email address

Use zone template? ☐ Yes ☒ No

IP address for template records

Add reverses for template addresses? ☒ Yes ☐ No

Refresh time  seconds

Expiry time  seconds

Transfer retry time  seconds

Negative cache time  seconds

#Création DNS

**Zone type** ☒ Forward (Names to Addresses) ☐ Reverse (Addresses to Names)

Domain name / Network

Records file ☒ Automatic ☐

Master server  ☒ Add NS record for master server?

Email address

Use zone template? ☐ Yes ☒ No

IP address for template records

Add reverses for template addresses? ☒ Yes ☐ No

Refresh time  seconds

Transfer retry time  seconds

Expiry time  seconds

Negative cache time  seconds

On sélectionne la zone que l'on vient de créer qui est "example.com".



Après avoir sélectionné la DNS zones, il faudra ajouter des adresses. Pour cela on clique sur "Address".

**Add Address Record**

Name  Time-To-Live ☒ Default ☐  seconds

Address

Update reverse? ☒ Yes ☐ Yes (and replace existing) ☐ No

#Ajouter des adresses IP pour le DNS.

De la même manière que précédemment on sélectionne notre zone DNS, ici "example.com" puis on rajoute des adresses.

L'adresse IP correspond à l'IP du container du service web. Dans notre exemple, celui-ci est sur un apache.

**Edit Address Record**

Name  Time-To-Live ☒ Default ☐  seconds

Address

Update reverse? ☒ Yes ☐ No

#Création d'un CNAME

De la même manière que précédemment on sélectionne notre zone DNS, ici "example.com" puis on rajoute "Name Alias"

**Add Name Alias Record**

Name  Time-To-Live ☒ Default ☐  seconds

Real Name  (Absolute names must end with a .)

#Vérification du fonctionnement

On retrouve bien l'adresse IP de notre DNS.

```
root@Linux:~# host ynov.example.com 172.20.0.2
Using domain server:
Name: 172.20.0.2
Address: 172.20.0.2#53
Aliases:
ynov.example.com has address 172.17.0.2
```

Actuellement je suis sûr d'autre DNS

```
# Generated by NetworkManager
nameserver 8.8.8.8
nameserver 213.244.0.2
nameserver 172.20.0.2
/etc/resolv.conf (END)
```

Il serait peut-être intéressant de créer une VM et de remplacer les DNS par celui créer.

Pour se faire il faudrait modifier le fichier "/etc/resolv.conf" et créer la "nameserver 172.20.0.2" et supprimer les autres.

```
root@Linux:~# dig @172.20.0.2 ynov.example.com
; <<>> DiG 9.11.3-1-Debian <<>> @172.20.0.2 ynov.example.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 42845
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
```

```
;; QUESTION SECTION:
ynov.example.com.      NIDERPRIM Michael      IN      A
                        ODE Loïck
;; ANSWER SECTION:
ynov.example.com.      38400      IN      A      172.17.0.2
                        PRAT Florian
;; AUTHORITY SECTION:
example.com.           38400      IN      NS      ns.example.com.
;; ADDITIONAL SECTION:
ns.example.com.        THOLLY Robin
                        38400      IN      A      172.20.0.2
                        TRINKLER Maxime
;; Query time: 0 msec
;; SERVER: 172.20.0.2#53(172.20.0.2)
;; WHEN: Thu Jun 07 09:24:16 CEST 2018
;; MSG SIZE rcvd: 94
```

- Ubuntu accès SSH avec un /home exporté sur un NAS + définir un utilisateur pour chaque étudiant

#Création du Dockerfile

```
FROM ubuntu

WORKDIR ubuntu

#Mettre a jour l'image.
RUN apt-get -y update &&\
    apt-get -y upgrade

# Don't start any optional services except for the few we need.
RUN find /etc/systemd/system \
    /lib/systemd/system \
    -path '*.wants/*' \
    -not -name '*journald*' \
    -not -name '*systemd-tmpfiles*' \
    -not -name '*systemd-user-sessions*' \
    -exec rm \{\} \;

#Installation du serveur SSH
RUN apt-get update && \
    apt-get install -y \
    dbus && \
    apt-get install -y openssh-server && \
    apt-get clean && \
    rm -rf /var/lib/apt/lists/*

RUN systemctl set-default multi-user.target

RUN sed -i 's/\(PermitRootLogin\) prohibit-password/\1 yes/' /etc/ssh/sshd_config

VOLUME [ "/sys/fs/cgroup" ]

EXPOSE 22

CMD ["/lib/systemd/systemd" , "--system"]
```

#Permet de créer une image ubuntu a jour

#Permet une connexion ssh

#Permet d'utiliser les fonction systemctl, parceque systemd à le PID 1

#On créer le container avec la commande suivante :

# Architecture de fichier :

1. Data
  - a. Loïck
  - b. Lucien
  - c. Débilou

# <user> correspond a l'élève qu'on souhaite ajouter par rapport au volume NFS

./start-compose.sh <user>

```
1 # /bin/bash
2 [ $1 == "" ] && exit 1
3 docker run --privileged -d -v /sys/fs/cgroup:/sys/fs/cgroup \
4 -v /home/loick/Bureau/Docker/Cours/Projet/UbuntuDev/data/$1:/home/$1 -P --name ubuntuunssh ubuntu:1.0
5
```

#Si tu copies se script sans le regarder tu vas avoir une erreur, alors on réfléchit et on fait pas le débile. Il y a un chemin absolu et non relatifs.

#On peut voir que le service pour se connecter en ssh fonctionne correctement.

```
root@Linux:/home/loick/Bureau/Docker/Cours/Projet/UbuntuDev# docker exec -it ubuntuunssh /bin/bash
root@1d078c660354:ubuntu# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enab
   Active: active (running) since Thu 2018-06-07 10:23:20 UTC; 30min
   Process: 35 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 40 (sshd)
   Tasks: 1 (limit: 4915)
   CGroup: /system.slice/docker.service/system.slice/ssh.service
           └─40 /usr/sbin/sshd -D

Jun 07 10:24:32 1d078c660354 sshd[49]: Failed password for loick from 172.17.0.1
port 52242 ssh2
Jun 07 10:24:41 1d078c660354 sshd[49]: Failed password for loick from 172.17.0.1
port 52242 ssh2
Jun 07 10:24:44 1d078c660354 sshd[49]: Failed password for loick from 172.17.0.1
port 52242 ssh2
Jun 07 10:24:44 1d078c660354 sshd[49]: Connection closed by authenticating user
loick 172.17.0.1 port 52242 [preauth]
Jun 07 10:24:44 1d078c660354 sshd[49]: PAM 1 more authen
tication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.17.0.1 user=lo
ick
Jun 07 10:24:51 1d078c660354 sshd[51]: pam_unix(sshd:aut
--More--
```

#Script [ createuser.sh ] pour la création de l'utilisateur par rapport au volume "/home/<user>"

#Pour les têtes en l'air "chmod +x createuser.sh"

```
1 # /bin/bash
2 #Vérifie si le repertoire exist
3 [ "$(ls /home/)" == "" ] && exit 1
4 getent passwd $(ls /home)
5 #Vérifie que l'utilisateur n'existe pas
6 [ "$(echo $?)" == "0" ] && exit 0
7
8 #Création utilisateur
9 adduser --gecos "First Last,RoomNumber,WorkPhone,HomePhone" --no-create-home --disabled-password --home /home/$(ls /home/) \
10 --uid $(ls -ln /home/ | awk '{print $3}') $(ls /home)
11
12 mypass="$(cat /home/$(ls /home)/initpasswd)"
13 echo $(ls /home):$mypass | chpasswd
14
```

#Lancer le script directement au démarrage avec systemd

#Ce script va permettre le l'exécution du script ci-dessus

```
1 [Unit]
2 Description="Create the user"
3
4 [Service]
5 type=oneshot
6 RemainAfterExit=yes
7 ExecStart=/bin/bash -c "sbin/createuser.sh"
8
```

# PROBLEME : n'apparaît pas dans le /etc/systemd/system/multi.... donc ne se lance pas au start !!

#IDEE 1 : Le mettre dans /bin/systeme..... et faire un lien symbolique

#IDEE 2 : Comprendre pourquoi le code suivant dans le dockerfile ne fonctionne pas :

COPY createuser.service /etc/systemd/system/multi-user.target.wants/

#IDEE 3 : Je te laisse deviner