

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=19o8i7c6k5
16     networks:
17
18 volumes:
19   dns-data:
```

Vérification que le container tourne correctement.

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
951399a3c89	wordpress:latest	"/usr/lib/systemd/sy..."	About an hour ago	Up About an hour	0.0.0.0:2222->22/tcp, 0.0.0.0:8081->80/tcp
ead09393b1c	mysql	"mysqld"	About an hour ago	Up About an hour	0.0.0.0:3306->3306/tcp, 0.0.0.0:3306->3306/tcp
1702d...	dns_server	"bind -t /data -c /etc/n..."	2 hours ago	Up 2 hours	0.0.0.0:53->53/udp, 0.0.0.0:53->53/tcp, 0.0.0.0:10000->10000/tcp, 0.0.0.0:53->53/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 172.20.0.2.

Username

Password

☐ Remember login permanently?

Login

Clear

Username : root
Password : 19o8i7c6k5

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

#Création du reverse DNS :

Login: root

Webmin

System

Servers

Other

Networking

Hardware

Cluster

Un-used Modules

Search:

View Module's Logs

System Information

Refresh Modules

Logout

Module Config

BIND DNS Server

BIND version 9.9.5

Apply Configuration

Stop BIND

Search Docs...

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

172.20.0.2

Records file

Automatic

...

Master server: ns.example.com ☒ Add NS record for master server?

Email address: admin@example.com

Use zone template? ☐ Yes ☒ No

Add reverses for template addresses? ☒ Yes ☐ No

Refresh time: 10800 seconds

Expiry time: 604800 seconds

IP address for template records:

Transfer retry time: 3600 seconds

Negative cache time: 38400 seconds

#Création DNS

New master zone options

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

Domain name / Network: example.com

Records file: ☒ Automatic ☐

Master server: ns.example.com ☒ Add NS record for master server?

Email address: admin@example.com

Use zone template? ☐ Yes ☒ No

Add reverses for template addresses? ☒ Yes ☐ No

Refresh time: 10800 seconds

Expiry time: 604800 seconds

IP address for template records:

Transfer retry time: 3600 seconds

Negative cache time: 38400 seconds

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

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 ☐ 205

☐ example.com ☐ localhost

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

Add Address Record

Name: ns Time-To-Live: ☒ Default ☐ seconds

Address: 172.20.0.2

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: ynov.example.com. Time-To-Live: ☒ Default ☐ seconds

Address: 172.17.0.2

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: www Time-To-Live: ☒ Default ☐ seconds

Real Name: ynov (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 créé.

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.      IN      A
;; ANSWER SECTION:
ynov.example.com.      38400   IN      A      172.17.0.2
;; AUTHORITY SECTION:
example.com.           38400   IN      NS      ns.example.com.
;; ADDITIONAL SECTION:
ns.example.com.        38400   IN      A      172.20.0.2
;; 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