



Table des matières

1) DNS.....	1
2) Mail.....	5
3) Antispam.....	6

1) DNS

Je commence par me placer dans le répertoire /etc/bind

Maintenant je définie mes zones dans le fichier named.conf.local

```
//  
// Do any local configuration here  
//  
zone "laforge-samuel.local" {  
    type master;  
    file "/etc/bind/db.laforge-samuel.local";  
};  
  
zone "12.205.10.in-addr.arpa" {  
    type master;  
    notify no;  
    file "/etc/bind/db.10.205.12";  
};  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";
```

Maintenant on s'occupe de modifier les fichiers db.laforge-samuel.local et db.10.205.12

Fichier db.laforge-samuel.local :

```
$TTL 604800;  
@      IN      SOA      server.laforge-samuel.local. root.laforge-samuel.local. (  
                                2                          ; Serial
```

```
        604800      ; Refresh
        86400       ; Retry
        2419200     ; Expire
        604800 )    ; Negative Cache TTL
;
@      IN      NS      server.laforge-samuel.local.
server IN      A       10.205.12.1
smtp   IN      A       10.205.12.12
pop     IN      A       10.205.12.13
imap    IN      A       10.205.12.14
```

Fichier db.10.205.12 ci-dessous :

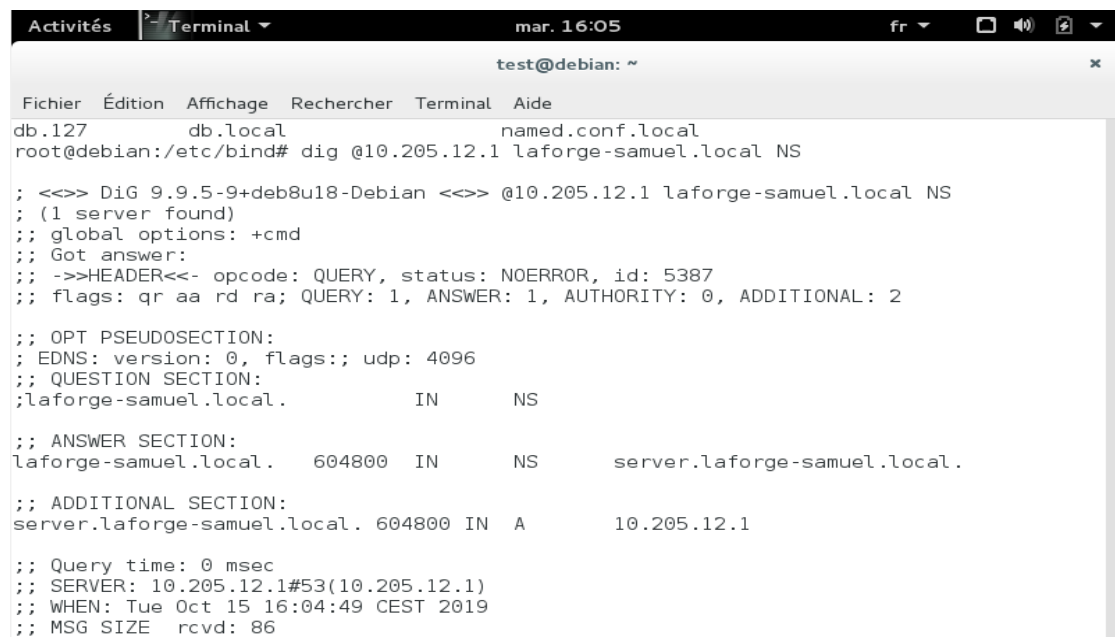
```
$TTL 604800
@      IN      SOA      server.laforge-samuel.local. root.laforge-samuel.local. (
        1          ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )    ; Negative Cache TTL
;
@      IN      NS      server.laforge-samuel.local.
1      IN      PTR     server.laforge-samuel.local.
12     IN      PTR     smtp.laforge-samuel.local
13     IN      PTR     pop.laforge-samuel.local
14     IN      PTR     imap.laforge-samuel.local
```

Je modifie aussi le fichier named.conf.options et j'y ajoute une option de forward pour que si on ne trouve pas mon dns les paquets puissent être envoyés à l'adresse DNS du prof :

```
options {
    directory «/var/cache/bind»;
    forwarders {
        10.205.2.64;
    };
    dnssec-validation auto;
    auth-nxdomain no;
    listen-on-v6 { any; };
};
```

Une fois mes fichiers modifiés je n'ai plus qu'à lancer la commande dig sur l'adresse de mon serveur et je recherche le nom de mon DNS via ma zone :

```
root@debian:/etc/bind# dig @10.205.12.1 laforge-samuel.local NS
```



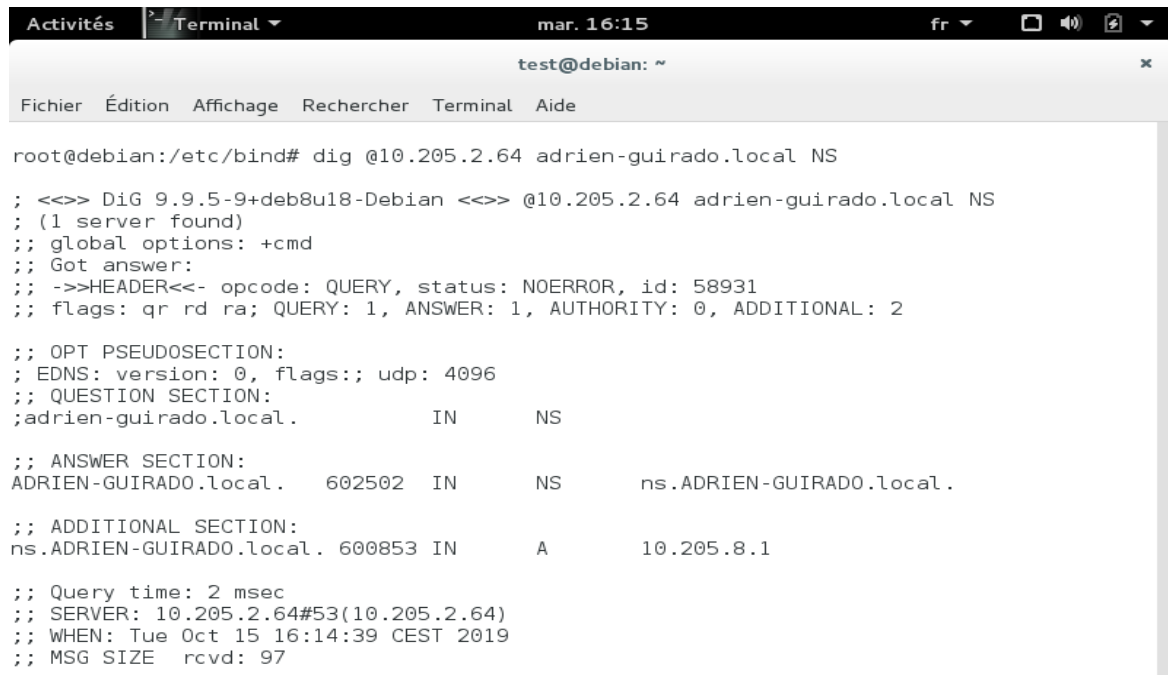
```
test@debian: ~  
Fichier Édition Affichage Rechercher Terminal Aide  
db.127 db.local named.conf.local  
root@debian:/etc/bind# dig @10.205.12.1 laforge-samuel.local NS  
  
; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @10.205.12.1 laforge-samuel.local NS  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 5387  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2  
  
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags:; udp: 4096  
;; QUESTION SECTION:  
;laforge-samuel.local. IN NS  
  
;; ANSWER SECTION:  
laforge-samuel.local. 604800 IN NS server.laforge-samuel.local.  
  
;; ADDITIONAL SECTION:  
server.laforge-samuel.local. 604800 IN A 10.205.12.1  
  
;; Query time: 0 msec  
;; SERVER: 10.205.12.1#53(10.205.12.1)  
;; WHEN: Tue Oct 15 16:04:49 CEST 2019  
;; MSG SIZE rcvd: 86
```

Je vois que je retrouve bien le nom de mon domaine qui est server.laforge-samuel.local.

Maintenant si le prof utilise la même commande sur son ordinateur il doit retrouver la même chose.

Une fois fait le prof entre notre zone et notre adresse dans son fichier pour que nous puissions communiquer avec les autres personnes de la classe.

Si j'utilise la commande suivante je retrouve bien le nom de serveur d'Adrien GUIRADO via le domaine du prof :



```
Activités Terminal mar. 16:15 test@debian: ~
Fichier Édition Affichage Rechercher Terminal Aide

root@debian:/etc/bind# dig @10.205.2.64 adrien-guirado.local NS

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @10.205.2.64 adrien-guirado.local NS
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 58931
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;adrien-guirado.local.      IN      NS

;; ANSWER SECTION:
ADRIEN-GUIRADO.local.  602502 IN      NS      ns.ADRIEN-GUIRADO.local.

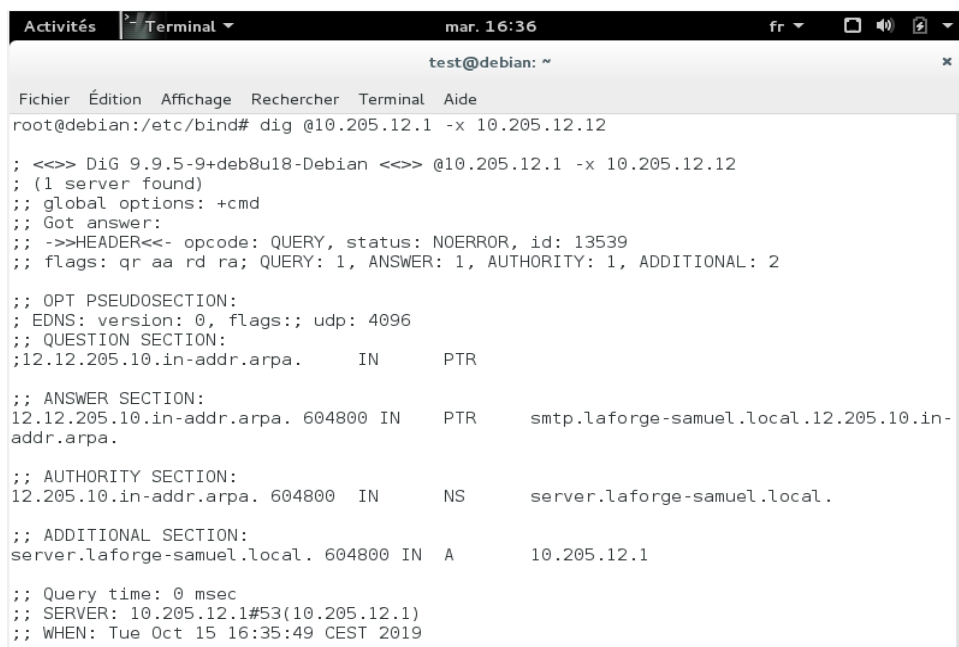
;; ADDITIONAL SECTION:
ns.ADRIEN-GUIRADO.local. 600853 IN      A      10.205.8.1

;; Query time: 2 msec
;; SERVER: 10.205.2.64#53(10.205.2.64)
;; WHEN: Tue Oct 15 16:14:39 CEST 2019
;; MSG SIZE rcvd: 97
```

Mon serveur DNS est maintenant bien configuré.

Question c) Pour que mon serveur DNS renvoi bien les adresses des serveurs nommés smtp, pop et imap j'utilise les commandes suivantes :

```
root@debian:/etc/bind# dig @10.205.12.1 -x 10.205.12.12
```



```
Activités Terminal mar. 16:36 test@debian: ~
Fichier Édition Affichage Rechercher Terminal Aide

root@debian:/etc/bind# dig @10.205.12.1 -x 10.205.12.12

; <<>> DiG 9.9.5-9+deb8u18-Debian <<>> @10.205.12.1 -x 10.205.12.12
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 13539
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;12.12.205.10.in-addr.arpa. IN      PTR

;; ANSWER SECTION:
12.12.205.10.in-addr.arpa. 604800 IN      PTR      smtp.laforge-samuel.local.12.205.10.in-addr.arpa.

;; AUTHORITY SECTION:
12.205.10.in-addr.arpa. 604800 IN      NS      server.laforge-samuel.local.

;; ADDITIONAL SECTION:
server.laforge-samuel.local. 604800 IN      A      10.205.12.1

;; Query time: 0 msec
;; SERVER: 10.205.12.1#53(10.205.12.1)
;; WHEN: Tue Oct 15 16:35:49 CEST 2019
```

2) Mail

Je met la configuration avec un site

Le site est: samuel-laforge.local

Je configure le serveur avec 2 réseaux: 127.0.0.0/8 et 10.1.0.0/16

a. Je crée des users sur le serveur mail:

```
adduser samuel  
adduser post  
adduser test
```

b) On va devoir Installer Dovecot, MUTT et changer la configuration de certains dossiers

1. Pour changer le format des mails en Maildir, il faut faire:

```
postconf -e «home_mailbox = Maildir/»
```

Et il faut aussi changer la variable MAIL de l'utilisateur

```
MAIL=/home/samuel/Maildir
```

2. Pour que le serveur gère notre domaine, on peut le changer lorsqu'on installe postfix ou alors aller dans le fichier /etc/postfix/main.cf

```
mydomain = smtp.samuel-laforge.local
```

3. On désactive le relai via le fichier main.cf

On regarde la ligne smtpd_relay_restrictions. On laisse juste nos réseaux et on enlève le reste

```
smtpd_relay_restrictions = permit_mynetworks
```

4. Pour envoyer à l'extérieur, rien ne fonctionne. Je me fais éjecter de google ou outlook par telnet

```
530 5.7.57 SMTP; Client was not authenticated to send anonymous mail during  
MAIL FROM [MRXP264CA0007.FRAPH264.PROD.OUTLOOK.COM] Connection  
closed by foreign host.
```

Mais mon serveur trouve bien les serveurs concernés.

EDIT: C'est sûrement un problème dû à l'encryption que je n'ai pas réussi à régler

Pour pouvoir lire les mails, il faut un paquet pour gérer IMAP/POP3

Ici, on va utiliser Dovecot

On l'installe avec:

```
root@debian:~# apt install dovecot-common dovecot-imapd dovecot-pop3d
```

J'installe aussi un client pour lire le IMAP/POP3

Ici je prend MUTT.

Si je lance MUTT, il trouve les mails que j'ai envoyé auparavant

Ici le 1er:

```
Date: Thu, 24 Oct 2019 12:40:06 +0200 (CEST)
```

```
From: root@localhost
```

```
rrrrrr
```

d. Pour paramétrer la taille de la boîte mail des users, il faut aller dans le fichier main.cf

On regarde la ligne:

```
mailbox_size_limitmailbox_size_limit = 100000000
```

La taille est en octets, ici on a alors mis 100 Million d'octets soit 100 Mo

e. Pour paramétrer la taille maximale des mails, il faut aller dans le fichier main.cf

```
message_size_limit = 2000000
```

Et rajouter/Modifier la ligne message_size_limit et mettre 2Mo comme demandé

Comme avant, la taille est en octets

Test du serveur:

```
Dans le fichier /var/log/mail.log, je vois que le daemon s'est bien lancé  
Oct 24 11:12:53 debian postfix/master[2360]: daemon started -- version 3.4.5,  
configuration /etc/postfix
```

Je fais un telnet localhost sur le port 25

Je fais:

```
ehlo localhostmail  
from: root@localhostrcpt  
to: samuel@localhost  
data  
Test  
.  
quit
```

Je fais un bonjour au serveur (ici localhost car je suis dessus)

Mail de root vers adrian avec un mail contenant dans sa data Test

Je finis le message avec . et je quitte

Je regarde si tout s'est bien passé dans le fichier de log

```
Oct 24 11:16:25 debian postfix/qmgr[2363]: 06F4E434AC:  
from=<root@localhost>, size=300, nrcpt=1 (queue active)
```

```
Oct 24 11:16:25 debian postfix/local[2669]: 06F4E434AC:  
to=<samuel@localhost>, relay=local, delay=21, delays=21/0.01/0/0,  
dsn=2.0.0, status=sent (delivered to mailbox)
```

Il y a bien un message de root qui est mis dans le queue et qui a été ensuite envoyé à samuel

Je lance mutt sur le compte samuel

Je vois bien les messages que j'ai envoyé. Si je clique dessus, j'ai bien la data que j'avais rentrée auparavant.

3) Antispam

On installe le paquet spamassassin.

On ajoute l'utilisateur spamassassin. Son groupe se crée automatiquement

On modifie les paramètres de spamassassin depuis le fichier /etc/default/spamassassin

On change:

```
OPTIONS="--username spamassassin --nouser-config --max-children 2 --helper-home-dir ${SAHOME} --socketowner=spamassassin --socketgroup=spamassassin -socketmode=0660"
```

On donne comme nom d'utilisateur à spamassassin «spamassassin»

On donne 2 daemon maximum à créer

On donne comme owner du socket et le group du socket spamassassin

On met aussi CRON=1 et on touche plus le fichier

Il faut maintenant ajouter spamassassin dans postfix

On va dans le fichier /etc/postfix/master.cf

On rajoute les lignes:

```
smtp      inet  n       -       -       -       smtpd
          -o content_filter=spamassassin
```

et ces 2 lignes à la fin du fichier

```
spamassassin unix - n n - - pipe
```

```
user=spamassassin argv=/usr/bin/spamc -f -e /usr/sbin/sendmail -oi
-f ${sender} ${recipient}
```

Je teste le spamassassin avec un message considéré comme SPAM:

En data:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-
EMAIL*C.34X
```