

1^{er} cours : 8 fevrier 2018

- serveur web
- serveur DNS

1) serveur web

Comment config un serveur web (Malaise a choisi apache) ?

- par default, apres l'installation il est déjà configuré vers une page par default

Probleme de SE linux, pas moyen de changer le dossier par default.

Car SE linux va empecher... donc comment le modifier ?

Active Directory (Windows Server)

Quelle est la 1ere chose à faire lorsque l'on met un dns en place ?

- mettre une ip fixe (qui soit dans le range de l'ecole car besoin d'une connexion internet)
- changer le nom de la machine (lors de la creation de zone)

Pour changer l'ip, et mettre une ip fixe : utiliser *ifconfig*

- recuperer l'ip sur lequel on est connecté
- recuperer la passerelle par default (malaise c'est le .2)

1) Configuration de l'interface reseau

vi /etc/sysconfig/network-scripts/ifcfg-eth0

- mettre :

bootproto= « dhcp » → « static »

- ajouter

ipaddr=192.168.188.33

netmask=255.255.255.0

gateway=192.168.188.1

- ajouter un dns

- redemarrer l'interface reseau

systemctl restart network.service

2) Installer le serveur web (apache)

yum install httpd

3) Configuration du serveur web

systemctl start httpd

systemctl status httpd (verification qu'il soit bien démarré)

systemctl enable httpd (démarrage automatique)

Le serveur apache doit etre ok

4) Fichier de config d'apache

```
cd /etc/httpd/conf
```

→ serveurRoot : /etc/httpd

c'est là où il va chercher les fichiers par default d'apache
(rien à changer)

Listen 80

(port d'ecoute)

Etant donné que c est un deamon, il a besoin d'un user pour etre lancé :

user apache

group apache

ServerAdmin :root@localhost

A qui faut il envoyer un mail si le serveur plante ?

serverName : donner un nom au serveur

Directory : quand on veut partager un dossier avec un serveur web

Exemple pour : /

Require all denied (on refuse l'accès à la racine) → c est logique

→ faut le laisser

DocumentRoot : /var/www/html

C'est là où se trouve la racine du site web

Par default, il y en a donc qu'un seul

Quand on cree un doc root : il faut partager le dossier

Le dossier c est : /var/www/html

option indexes followSymLinks

indexes signifie : ?

→ fa parle, jcomprends pas

allow override None

→ fa arrete pas de parler, c'est quoi ?

Require all granted

→ on en a pas vraiment besoin, mais c'est quoi ?

</directory> fermeture de la balise

Option pour les modules

options pour les modules (pas besoin pr le prof)

Lynx est un browser en terminal

yum install lynx

Test avec une page web

cd /var/www/html

vi index.html

hello world

lynx localhost

→ ça marche

Autorisation du trafic http et https dans le firewall

→ sudo firewall-cmd --add-service=http --permanent && sudo firewall-cmd --add-service=https --permanent

→ sudo systemctl restart firewalld

Si on change DocumentRoot de place

ça va pas marcher à cause de SELinux

→ ça se passe aussi dans httpd.conf

pour modifier l'emplacement du documentRoot

ça marchera pas (pas expliqué)

→ il était dans : /etc/httpd/conf/httpd.conf

Maintenant on a qu'un seul site web

Mais pour le projet il va en falloir plusieurs sur le même serveur WEB

Dossier où se trouve cette config :

cd /etc/httpd/conf.d

vi welcome.conf

(c'est pas le bon fichier pr faire ça)

Il va créer des virtual host
cd /etc/httpd/conf.d
vi vhost.conf

Il y a 3 types de serveur virtuel sur apache :

- port
- nom
- par carte reseau

Initialement, la configuration du serveur Apache s'effectuait dans un seul fichier /etc/httpd/conf/httpd.conf. Avec le temps, ce fichier est devenu de plus en plus volumineux et de moins en moins lisible.

Les distributions modernes ont donc tendance à répartir la configuration d'Apache sur une série de fichiers *.conf répartis dans les répertoires /etc/httpd/conf.d et /etc/httpd/conf.modules.d, rattachés au fichier principal /etc/httpd/conf/httpd.conf par la directive Include.

lien utile pour la config : <https://blog.microlinux.fr/apache-centos/#configuration>

Test de creation, de virtual host avec apache

```
cd /etc/httpd/conf.d  
vi vhost.conf
```

```
namevirtualhost 192.168.188.34
```

```
<VirtualHost 192.168.188.34:80>  
ServerAdmin florian.giarrusso@std.heh.be  
DocumentRoot "/var/www/html/toto.com/"  
ServerName toto.com  
ServerAlias www.toto.com  
ErrorLog "/var/log/httpd/toto.com-error_log"  
CustomLog "/var/log/httpd/toto.com-access_log" combined  
</VirtualHost>
```

```
<VirtualHost 192.168.188.34:80>  
ServerAdmin florian.giarrusso@std.heh.be  
DocumentRoot "/var/www/html/tata.com/"  
ServerName tata.com  
ServerAlias www.tata.com  
ErrorLog "/var/log/httpd/tata.com-error_log"  
CustomLog "/var/log/httpd/tata.com-access_log" combined  
</VirtualHost>
```

```
<Directory "/var/www/html/toto.com/">  
DirectoryIndex index.html index.php  
Options Indexes FollowSymLinks Multiviews  
order allow,deny  
Allow from all  
</Directory>
```

```
<Directory "/var/www/html/tata.com/">  
DirectoryIndex index.html index.php  
Options Indexes FollowSymLinks Multiviews  
allow from all  
order allow,deny  
</Directory>
```

Lien : <https://www.rosehosting.com/blog/apache-virtual-hosts-on-centos/>

Il faudra automatiser ce bordel

Il faudra config le dns pr faire les enregistrement

Ça va pas marcher

Il faut faire les balises directory sinon on aura pas acces au repertoire

Il a mis ça aussi dans le fichier : vhost.conf à la suite de la creation des virtual host

system restart httpd

teste :

www.toto.com

www.tata.com

Etant donné qu'il n y a pas de dns de config

Il faut dire à /etc/hosts

De pointer vers le serveur lui-même

donc dans /etc/hosts :

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1      localhost localhost.localdomain localhost6 localhost6.localdomain6
```

```
192.168.188.34 www.toto.com www.tata.com
```

This command will assign **apache:apache** to every file and directory/subdirectory inside **/var/www/html/your_domain/**.

→ `chown apache:apache -R /var/www/html/toto.com`

→ `chown apache:apache -R /var/www/html/tata.com`

Ça fonctionne : j'ai pas du modifier le fichier resolve.conf (mettre order host blabla)

Le DNS

lien : <https://www.unixmen.com/setting-dns-server-centos-7/>

Prérequis

Dans le pare-feu, ouvrir le port 53 en TCP et en UDP. Les gourous de la sécurité ont longtemps conseillé d'ouvrir le port 53 en UDP seulement pour les requêtes DNS. Or, ces dernières peuvent également utiliser le port 53 en TCP si l'UDP n'est pas accepté.

```
yum install bind bind-utils
```

Outre le serveur bind à proprement parler, on installera le paquet bind-utils, qui fournit une collection d'outils comme dig, host et nslookup.

Basculer SELinux en mode permissif.

→ **setenforce 0**

(j'ai pas utilisé)

Ne plus utiliser le dns de google et utiliser son propre DNS

→ utilisation de *nmtui* pour config le reseau

vim /etc/sysconfig/network-scripts/ifcfg-eth0

Contenu :

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME=eth0
UUID=686db863-a8f2-48c9-ac4d-59c540972255
DEVICE=eth0
ONBOOT=yes
```

```
IPADDR=192.168.188.34
PREFIX=32
GATEWAY=192.168.188.1
DNS1=192.168.188.34
```

redemarer interface :

→ `systemctl restart network`

Serveur cache DNS

vim /etc/named.conf

commande pour tester dns :

→ `nslookup`

→ `dig`

3 modes de fonctionnement d'un DNS

- cache
- reverse
-

Configuration de named.conf

vim /etc/named.conf

listen-on : ajouter ip du serveur

allow query : ajouter le reseau (netID) à autoriser

Recursivité sur les adresses jusqu'au moment où il trouve
mettre sur yes pour continuer de chercher si rien en cache

Ne pas oublier de mettre en place l'authentification auprès du dns

nslookup

dig

fonctionnel sur dns externe (non enregistré dans le cache)

changement de l'hostname

vim /etc/hostname

→ server.linux.lan

Configuration des zones dans named.conf

Vim /etc/named.conf

zone maitre
FORWARD
→linux.lan
→type master
→fichier : forward.linux
→autoriser update

REVERSE
→188.168.192.in-addr.arpa
→type master
→fichier : reverse.linux
→autoriser update

```
zone "linux.lan" IN {  
type master;  
file "forward.linux";  
allow-update { none; };  
};
```

```
zone "188.168.192.in-addr.arpa" IN {  
type master;  
file "reverse.linux";  
allow-update { none; };  
};
```

Creation des fichiers de zones

cd /var/named/

→forward.linux

\$TTL 86400

```
@ IN SOA  server.linux.lan. root.linux.lan. (
    2011071001 ;Serial
    3600      ;Refresh
    1800      ;Retry
    604800    ;Expire
    86400     ;Minimum TTL
)
@ IN NS  server.linux.lan.
@ IN A   192.168.188.34
@ IN A   192.168.188.26
server IN A   192.168.188.34
client IN A   192.168.188.26
```

→reverse.linux

\$TTL 86400

```
@ IN SOA  server.linux.lan. root.linux.lan. (
    2011071001 ;Serial
    3600      ;Refresh
    1800      ;Retry
    604800    ;Expire
    86400     ;Minimum TTL
)
@ IN NS   server.linux.lan.
@ IN PTR  linux.lan.
server IN A   192.168.188.34
client IN A   192.168.188.26
34 IN PTR  server.linux.lan.
26 IN PTR  client.linux.lan.
```

Activation du service DNS

Systemctl enable named

systemctl start named

Firewall configuration

We must allow the DNS service default port 53 through firewall.

```
firewall-cmd --permanent --add-port=53/tcp  
firewall-cmd --permanent --add-port=53/udp
```

Restart Firewall

```
firewall-cmd --reload
```

Configuration Permission, Proprietaire et SELinux

```
chgrp named -R /var/named  
chown -v root:named /etc/named.conf  
restorecon -rv /var/named  
restorecon /etc/named.conf
```

Test DNS config et fichier de zone (erreur de syntaxe)

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

(si aucun retour, pas d'erreur de syntaxe)

Check Forward Zone

```
named-checkzone linux.local /var/named/forward.linux
```

Check Reverse Zone

```
named-checkzone linux.local /var/named/reverse.linux
```

Ajouter le serveur DNS dans les parametres d'interface

```
vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DNS1="192.168.188.34"
```

Editer le fichier /etc/resolv.conf

```
vim /etc/resolv.conf
```

```
nameserver 192.168.188.34
```

Redemarrer interface reseau

```
systemctl restart network
```

Test DNS Server

```
dig server.linux.lan  
nslookup linux.lan
```

ça marche

Tester SE linux voir ce qu'il pense d'un fichier log

Yum install setroubleshoot-server
sealert -a /var/log/audit/audit.log