

DOCUMENTATION APACHE ET DNS

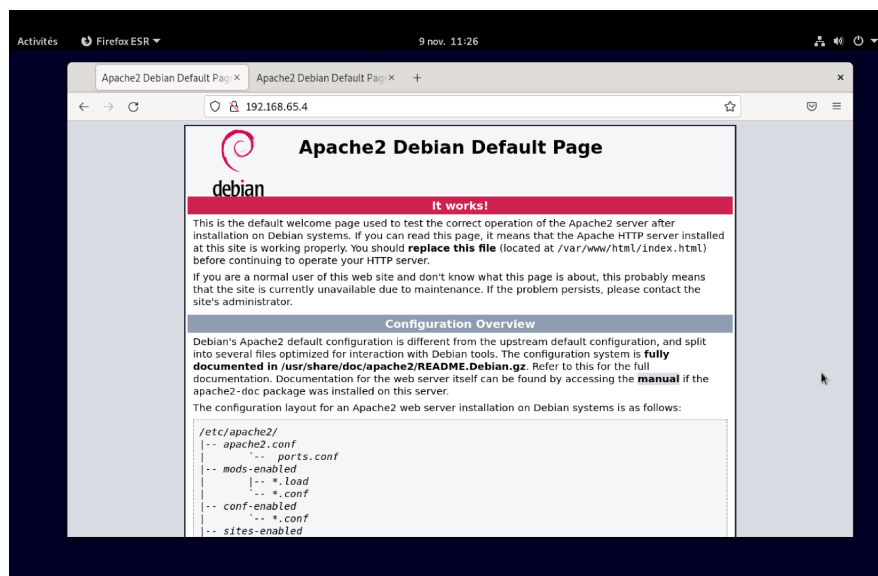
JOB 2:

installer apache

```
sudo apt-get install apache2
```

accéder a la page

local ou ip de la machine ex: 192.168.65.4



JOB 3:

Quels sont les différents serveurs web ?

Apache HTTP Server

Le serveur HTTP Apache souvent appelé httpd, ou simplement Apache a été lancé en 1995 et a célébré son 20^{ème} anniversaire en Février 2015. 52% des sites web sont hébergés sur un serveur qui utilise Apache.

Alors que Apache httpd est plus souvent utilisé sur Linux, vous pouvez également le déployer sur OS X et Windows. Apache est, sans surprise, sous licence Apache 2. Le serveur Web lui-même utilise une architecture modulaire, dans lequel les modules supplémentaires peuvent être chargés d'étendre ses fonctionnalités. Par exemple, le chargement du mod_proxy permettra un proxy / passerelle sur votre serveur, et mod_proxy_balancer permettra l'équilibrage de charge pour tous les protocoles pris en charge. Depuis la version 2.4, Apache prend également en charge HTTP / 2 grâce à un nouveau module, mod_http2.

NGINX

Igor Sysoev a commencé à développer NGINX en 2002, avec sa première version publique en 2004. NGINX a été développé comme une réponse à la soi-disant le problème C10K, qui est un raccourci pour «comment concevez un serveur web qui peut gérer 10 000 connexions simultanées ? » Nginx est deuxième sur une liste de serveurs web open source par l'usage, utilisé sur un peu plus de 30% des serveur. NGINX repose sur une architecture événementielle asynchrone pour aider à alimenter son objectif de gérer des sessions simultanées massives. Il est devenu un serveur web très populaire en raison de son utilisation des ressources de sa rapidité et de sa capacité à évoluer facilement.

Nginx est publié sous une licence BAD-vie, il peut être déployé non seulement en tant que serveur Web, mais aussi en tant que serveur proxy ou équilibreur de charge.

Apache Tomcat

Apache Tomcat Java est un conteneur de servlets open source qui fonctionne comme un serveur Web. Une servlet Java est un programme Java qui étend les capacités d'un serveur. Bien que les servlets peuvent répondre à tous les types de demandes, ils mettent en œuvre le plus souvent des applications hébergées sur des serveurs Web. Ces servlets Web sont la contrepartie Java à d'autres technologies de contenu web dynamique tels que PHP et ASP.NET. la base du code de Tomcat a été donné par Sun Microsystems à l'Apache Software Foundation en 1999, et est devenu un projet Apache haut niveau en 2005. Il est utilisé actuellement un peu moins de 1% de tous les sites.

Apache Tomcat, publié sous la version Apache License 2, est généralement utilisé pour exécuter des applications Java. Il peut, cependant, être étendue avec Coyote, pour effectuer également le rôle d'un serveur web normal qui sert des fichiers locaux en tant que documents HTTP. Plus d'informations peuvent être trouvées sur le site web du projet.

Node.js

Node.js est un environnement JavaScript côté serveur pour les applications de réseau tels que les serveurs Web. Avec une part de marché plus petite, Node.js est utilisé sur 0,2% des sites. Il a été écrit en 2009 par Ryan Dahl. Le projet Node.js, régie par la Fondation Node.js, est facilitée par le programme des projets de collaboration de la Fondation Linux.

La différence entre Node.js et autres serveurs web populaires est qu'il est avant tout un environnement d'exécution multi-plateforme. Node.js applique une architecture événementielle capable de asynchrones I / O. Ces choix de conception d'optimiser le débit et l'évolutivité des applications Web permettant d'exécuter la communication et navigateur jeux en temps réel. Node.js met également en évidence la différence dans les piles de développement web, où Node.js fait clairement partie de l'HTML, CSS et JavaScript pile, par opposition à Apache ou Nginx qui font partie de nombreuses piles de logiciels différents.

Node.js est publié sous un mélange de licences; plus d'informations sont disponibles sur le site web du projet.

Lighttpd

Lighttpd est apparu en Mars 2003. Il est actuellement utilisé sur environ 0,1% des sites Web et distribué sous licence BSD.

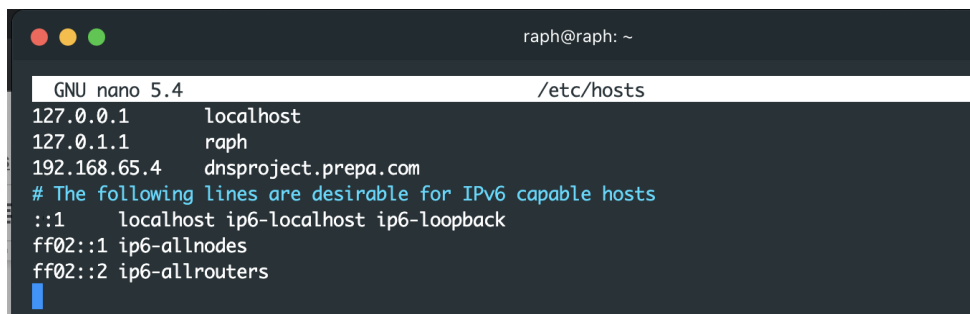
Lighttpd se distingue par sa faible utilisation mémoire, faible charge CPU, et des optimisations de vitesse. Il utilise une architecture événementielle, il est optimisé pour un grand nombre de connexions parallèles, et il prend en charge FastCGI, SCGI, Auth, Output-compression, URL-réécriture et de nombreuses autres fonctionnalités. Lighttpd est un serveur Web populaire pour Catalyst et Ruby on Rails framework web.

JOB 4:

pour accéder à la page grace a un nom de domaine dnsproject.prepa.com

aller modifier le fichier hosts dans

```
sudo nano /etc/hosts
```



```
raph@raph: ~  
GNU nano 5.4 /etc/hosts  
127.0.0.1    localhost  
127.0.1.1    raph  
192.168.65.4  dnsproject.prepa.com  
# The following lines are desirable for IPv6 capable hosts  
::1          localhost ip6-localhost ip6-loopback  
ff02::1      ip6-allnodes  
ff02::2      ip6-allrouters
```

JOB 5:

Comment obtenir un nom de domaine :

Pour déposer un nom de domaine, il faut s'adresser à l'un des nombreux prestataires agréés. Il est fréquent qu'ils proposent en complément des services comme de l'hébergement, des solutions de création de site, un service de messagerie.

Exemples : **Amen, Gandi, Mail Club, Ovh, Ikoula, Ionos, etc.**

Pour un .fr, le site de l'Association française pour le nommage internet en coopération - **Afnic** - l'organisme qui gère les noms de domaine en suffixe .fr - propose une liste de prestataires ayant adhéré à sa charte. La plupart d'entre eux permet, en ligne, de vérifier la disponibilité du nom souhaité.

Les différents types d'extension accessibles aux entreprises. Les plus courants sont:

- .fr : peut être attribué à toute entité ou personne ayant une existence légale en France, sans autre condition. Le choix d'un suffixe .fr peut être rassurant pour les contacts commerciaux de l'entreprise.
Il atteste d'une proximité de l'entreprise vis-à-vis du marché français ainsi que de sa réelle existence juridique.
Les personnes physiques qui résident sur le territoire de l'un des Etats membres de l'Union européenne et les personnes morales qui y ont leur siège social ou leur établissement principal, peuvent demander l'enregistrement d'un nom de domaine en .fr.
- .com : plus "global" que le .fr. (à l'origine il était destiné aux entreprises commerciales), mais aussi moins "fiable" car aucune condition particulière n'est exigée pour son dépôt.
Attention, cependant, à ne pas enregistrer, même involontairement, un nom correspondant à une marque appartenant à un tiers.
- .net : à l'origine destiné aux structures liées à Internet. Fonctionnant comme le .com, il peut aujourd'hui être déposé par toute personne.
- .org : à l'origine destiné aux structures à but non commercial. Il est aujourd'hui aussi "ouvert" que le .com.
- Et aussi : .biz, .info, .tv, .eu, .asia, .pro, etc.
Hors de l'Europe, si, par exemple, votre entreprise travaille avec la Chine ou l'Inde, il est également recommandé de réserver le .cn ou le .in.

Le choix entre .fr, .com, .eu, .mobi : Ce choix relève de la stratégie de l'entreprise. Pour une entreprise française, le .fr s'impose. Si le .com est disponible, il ne faut pas hésiter à le réserver également. Le .eu quant à lui est très peu utilisé.

Le .mobi permet d'identifier un site sur un téléphone mobile qui a été adapté à ce type de navigation mais avec l'évolution des sites qui s'adaptent automatiquement au support de consultation (responsive design), il est en voie de disparition progressive

JOB 6:

pour mettre en place le serveur dns sur notre machine

installer bind9

```
sudo apt-get install bind9
```

une fois installer se rendre dans le dossier bind and /etc/bind

```
raph@raph:/etc/bind$ ls
bind.keys  db.255  dnsproject.prepa.com.rev  named.conf.default-zones  rndc.key
db.0       db.empty dnsproject.prepa.com.zone  named.conf.local          zones.rfc1918
db.127     db.local named.conf                named.conf.options
```

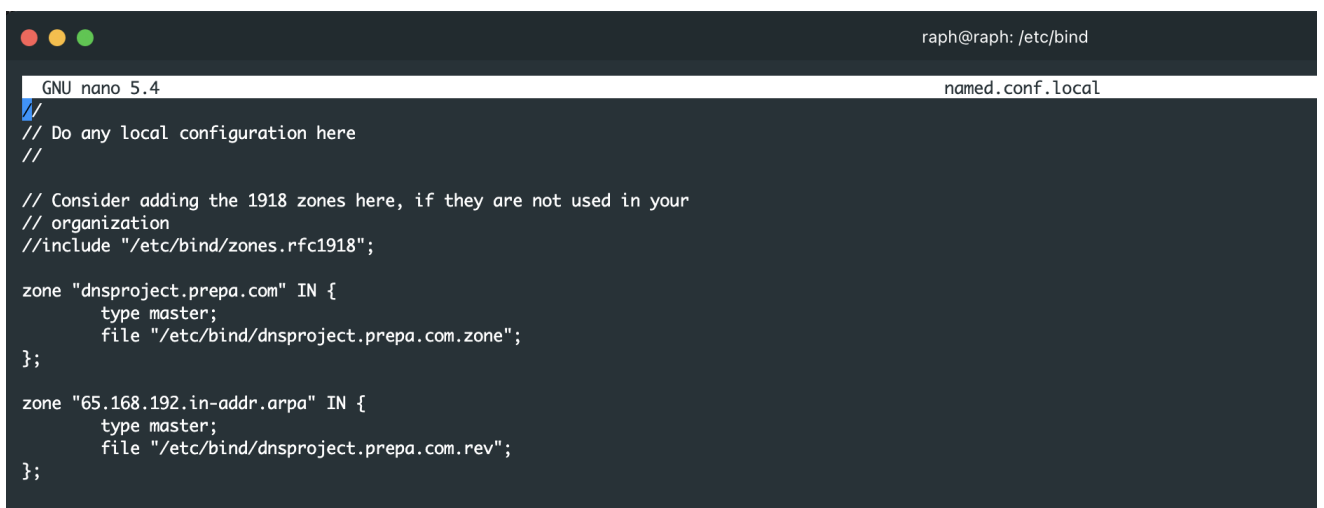
une fois dans le dossier créer deux fichiers dans notre cas

dnsproject.prepa.com.zone et

dnsproject.prepa.com.rev, ils nous serviront pour la configuration de votre dns en gardant les fichier d'origine.

editer le dossier named.conf.local

```
sudo nano named.conf.local
```



```
GNU nano 5.4 named.conf.local
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "dnsproject.prepa.com" IN {
    type master;
    file "/etc/bind/dnsproject.prepa.com.zone";
};

zone "65.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/dnsproject.prepa.com.rev";
};
```

ajouter les 2 zones ci- dessus.

une fois le dossier named.conf.local éditer nous allons éditer le fichier
dnsproject.prepa.com.zone

sudo nano dnsproject.prepa.com.zone

```
raph@raph: /etc/bind
GNU nano 5.4 dnsproject.prepa.com.zone
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA dnsproject.prepa.com. root.dnsproject.prepa.com. (
    2      ; Serial
    604800 ; Refresh
    86400  ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS dnsproject.prepa.com.
@ IN A 192.168.65.4
@ IN AAAA ::1
```

ensuite éditer le fichier dnsproject.prepa.com.rev

sudo nano dnsproject.prepa.com.rev

```
raph@raph: /etc/bind
GNU nano 5.4 dnsproject.prepa.com.rev
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA dnsproject.prepa.com. root.dnsproject.prepa.com. (
    2      ; Serial
    604800 ; Refresh
    86400  ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS dnsproject.prepa.com.
4 IN PTR dnsproject.prepa.com.
```

ensuite restart le service bind9

sudo service bind9 restart

on peut utiliser la commande nslookup ip ou nom de domaine pour voir si les info de
notre dns sont bien prise en compte

nslookup dnsproject.prepa.com

```
raph@raph:~$ nslookup dnsproject.prepa.com
Server:      192.168.65.1
Address:     192.168.65.1#53

Name:   dnsproject.prepa.com
Address: 192.168.65.4
Name:   dnsproject.prepa.com
Address: ::1

raph@raph:~$
```

nslookup 192.168.65.4

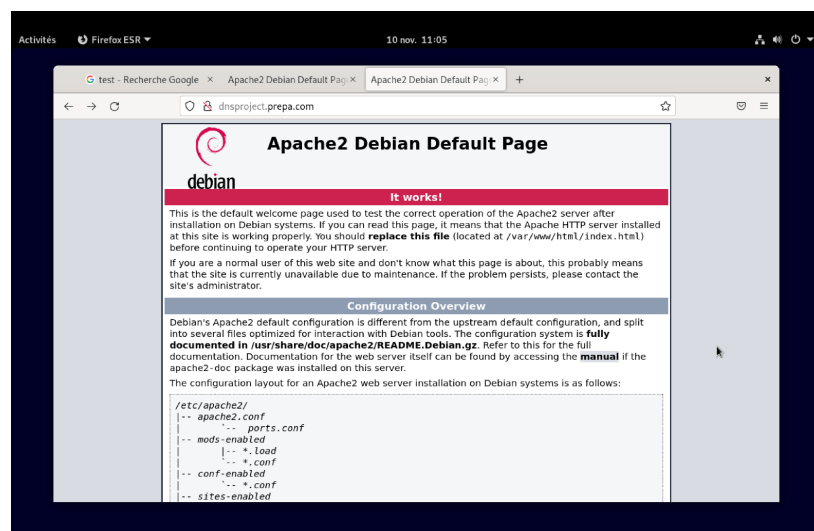
```
raph@raph:/etc/bind$ nslookup 192.168.65.4
4.65.168.192.in-addr.arpa      name = dnsproject.prepa.com.

raph@raph:/etc/bind$
```

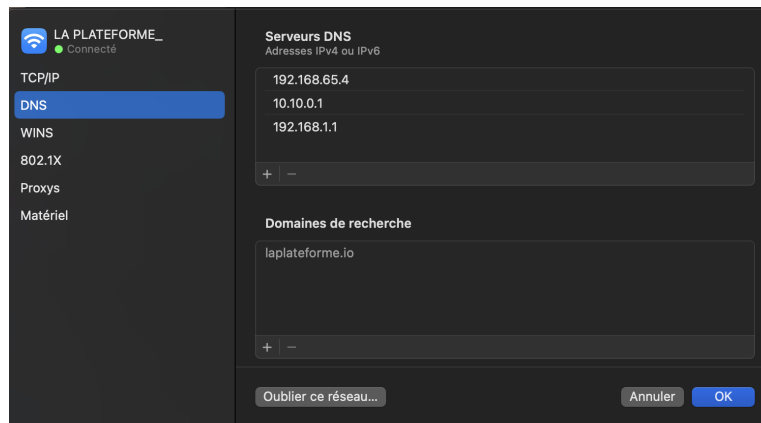
on peut maintenant enlever la ligne ajouter précédemment dans /etc/hosts et taper dns

```
GNU nano 5.4 /etc/hosts
127.0.0.1    localhost
127.0.1.1    raph
#192.168.65.4 dnsproject.prepa.com
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
```

project dans le moteur de recherche de notre vm



ajouter l'adresse du serveur dnsproject.prepa.com dans les serveurs dns sur le réseau de l'hôte



pour vérifier que cela fonctionne taper dnsproject.prepa.com dans un navigateur sur la machine hôte.



on peut aussi ping dnsproject.prepa.com depuis notre hôte :

ping dnsproject.prepa.com

```
raphaelmalet@MacBook-Air-de-Raphael: /Users/raphaelmalet
→ ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.65.4): 56 data bytes
64 bytes from 192.168.65.4: icmp_seq=0 ttl=64 time=1.028 ms
64 bytes from 192.168.65.4: icmp_seq=1 ttl=64 time=1.707 ms
64 bytes from 192.168.65.4: icmp_seq=2 ttl=64 time=1.128 ms
64 bytes from 192.168.65.4: icmp_seq=3 ttl=64 time=1.183 ms
64 bytes from 192.168.65.4: icmp_seq=4 ttl=64 time=1.089 ms
64 bytes from 192.168.65.4: icmp_seq=5 ttl=64 time=1.331 ms
64 bytes from 192.168.65.4: icmp_seq=6 ttl=64 time=1.126 ms
^C
--- dnsproject.prepa.com ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.028/1.227/1.707/0.214 ms
raphaelmalet@MacBook-Air-de-Raphael: /Users/raphaelmalet
→
```

JOB 7-8:

Installer le paquet isc-dhcp-server

sudo apt-get install isc-dhcp-server

pendant l'installation du paquet une interface va apparaître pour nous demander sur quel réseau on souhaite effectuer un dhcp, dans notre cas 192.168.65.0 et sur quelle interface réseau on souhaite écouter ici enp0s1

aller dans le dossier dhcp /etc/dhcp

cd /etc/dhcp

```
raph@raph:/etc/dhcp$ ls
debug dhclient.conf dhclient-enter-hooks.d dhclient-exit-hooks.d dhcpd6.conf dhcpd.conf
raph@raph:/etc/dhcp$
```

Une fois dans le dossier dhcp nous allons éditer le fichier dhcpd.conf pour modifier les paramètres de notre serveur dhcp.

sudo nano dhcpd.conf

```
raph@raph:/etc/dhcp
GNU nano 5.4 dhcpd.conf *
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# option definitions common to all supported networks...
option domain-name "dhcpproject";
option domain-name-servers 192.168.65.4;

default-lease-time 3600;
max-lease-time 7200;

# The ddns-update-style parameter controls whether or not the server will
# attempt to do a DNS update when a lease is confirmed. We default to the
# behavior of the version 2 packages ('none', since DHCP v2 didn't
# have support for DDNS.)
# have support for DDNS.)
ddns-update-style none;
```

```
raph@raph: /etc/dhcp
GNU nano 5.4 dhcpd.conf *
# option routers rtr-239-0-1.example.org, rtr-239-0-2.example.org;
#}

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

#subnet 10.254.239.32 netmask 255.255.255.224 {
#  range dynamic-bootp 10.254.239.40 10.254.239.60;
#  option broadcast-address 10.254.239.31;
#  option routers rtr-239-32-1.example.org;
#}

# A slightly different configuration for an internal subnet.
subnet 192.168.65.0 netmask 255.255.255.224 {
  range 10.5.5.20 10.5.5.30;
  option domain-name-servers 192.168.65.4;
  option domain-name "dhcproject";
  option routers 192.168.5.1;
  option broadcast-address 192.168.65.255;
  default-lease-time 3600;
  max-lease-time 7200;
}
```

Première ligne donne les paramètres de notre dhcp, sur qu'elle réseau il va être actif et sur quelle masque de sous réseau.

range donne la plage d'ip sur lesquelles les ip vont être distribué.

L'option domain-name server donne l'ip du serveur sur lequel il est actif.

L'option domain-name donne le nom du réseau.

Options routers, on informe l'ip du routeur de notre réseau pour avoir accès à internet.

L'option broadcast donne l'ip broadcast du réseau.

Default-lease-time donne le temps minimum ou l'ip est actif sur le réseau.

La dernière ligne donne le temps maximum ou l'ip sera actif.

JOB 9:

installer le paquet ufw

```
sudo apt-get install ufw
```

commande ufw status pour connaître le statut du pare feu

```
sudo ufw status
```

```
raph@raph:/etc/bind$ sudo ufw status
Status: inactive
```

de base quand on installe le paquet ufw le statut sera toujours désactiver

une fois installer ouvrir les port 80 pour avoir accès à notre site qui émet sur le port 80

```
sudo ufw allow 80/tcp
```

```
sudo ufw allow 80/udp
```

```
raph@raph:/etc/bind$ sudo ufw allow 80/tcp
Rules updated
Rules updated (v6)
raph@raph:/etc/bind$ sudo ufw allow 80/udp
Rules updated
Rules updated (v6)
raph@raph:/etc/bind$
```

pour avoir accès au serveur mais ne pas pouvoir le ping il faut aller dans /etc/ufw éditer le fichier before.rules

```
sudo nano before.rules
```

```
# ok icmp codes for INPUT
-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp code for FORWARD
-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT
```

mettre en commentaire les lignes ci-dessus

```
# ok icmp codes for INPUT
#-A ufw-before-input -p icmp --icmp-type destination-unreachable -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type time-exceeded -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type parameter-problem -j ACCEPT
#-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT

# ok icmp code for FORWARD
#-A ufw-before-forward -p icmp --icmp-type destination-unreachable -j ACCEPT
#-A ufw-before-forward -p icmp --icmp-type time-exceeded -j ACCEPT
#-A ufw-before-forward -p icmp --icmp-type parameter-problem -j ACCEPT
#-A ufw-before-forward -p icmp --icmp-type echo-request -j ACCEPT
```

activer le service ufw

```
sudo ufw enable
```

```
raph@raph:/etc/ufw$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y/n)? y
Firewall is active and enabled on system startup
raph@raph:/etc/ufw$
```

avant de mettre le pare-feu

```
raphaelmalet@MacBook-Air-de-Raphael: /Users/raphaelmalet
[→ ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.65.4): 56 data bytes
64 bytes from 192.168.65.4: icmp_seq=0 ttl=64 time=0.749 ms
64 bytes from 192.168.65.4: icmp_seq=1 ttl=64 time=1.087 ms
64 bytes from 192.168.65.4: icmp_seq=2 ttl=64 time=1.391 ms
^C
--- dnsproject.prepa.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.749/1.076/1.391/0.262 ms
raphaelmalet@MacBook-Air-de-Raphael: /Users/raphaelmalet
```

après que le pare-feu soit activé avec les réglages effectués ci-dessus:

```
you have new mail.
raphaelmalet@MacBook-Air-de-Raphael: /Users/raphaelmalet
[→ ping dnsproject.prepa.com
PING dnsproject.prepa.com (192.168.65.4): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
^C
--- dnsproject.prepa.com ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
raphaelmalet@MacBook-Air-de-Raphael: /Users/raphaelmalet
→
```

mais la page du serveur est toujours disponible

JOB 10:

Installer le paquet samba.

sudo apt-get install samba

une fois téléchargé aller à /etc/samba

```
raph@raph:/etc/apache2/sites-available$ cd /etc/samba
raph@raph:/etc/samba$ ls
gdbcommands  smb.conf  tls
```

éditer le fichier samba.conf

sudo nano smb.conf

```
# The specific set of interfaces / networks to bind to
# This can be either the interface name or an IP address/netmask;
# interface names are normally preferred
; interfaces = 192.168.65.4/14 eth0
```

```

GNU nano 5.4
usershare allow guests = yes

#===== Share Definitions =====

[homes]
    comment = Home Directories
    browseable = yes

# By default, the home directories are exported read-only. Change the
# next parameter to 'no' if you want to be able to write to them.
    read only = no

# File creation mask is set to 0700 for security reasons. If you want to
# create files with group=rw permissions, set next parameter to 0775.
    create mask = 0700

# Directory creation mask is set to 0700 for security reasons. If you want to
# create dirs. with group=rw permissions, set next parameter to 0775.
    directory mask = 0700

# By default, \\server\username shares can be connected to by anyone
# with access to the samba server.
# The following parameter makes sure that only "username" can connect
# to \\server\username
# This might need tweaking when using external authentication schemes
    valid users = %S

# Un-comment the following and create the netlogon directory for Domain Logons
# (you need to configure Samba to act as a domain controller too.)
;[netlogon]
;    comment = Network Logon Service
;    path = /home/samba/netlogon
;    guest ok = yes
;    read only = yes

# Un-comment the following and create the profiles directory to store
# users profiles (see the "logon path" option above)
# (you need to configure Samba to act as a domain controller too.)
# The path below should be writable by all users so that their
# profile directory may be created the first time they log on
;[profiles]
;    comment = Users profiles
;    path = /home/samba/profiles
;    guest ok = yes
;    browseable = no
;    create mask = 0600
;    directory mask = 0700

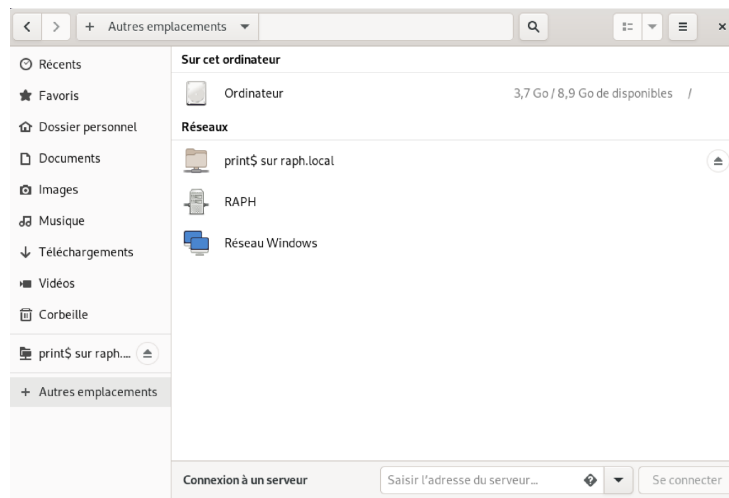
[printers]
    comment = All Printers
    browseable = no
    path = /var/spool/samba
    printable = yes
    guest ok = yes
    read only = yes
    create mask = 0700

# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
    comment = Printer Drivers
    path = /var/lib/samba/printers
    browseable = yes
    read only = yes
    guest ok = yes
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions

```

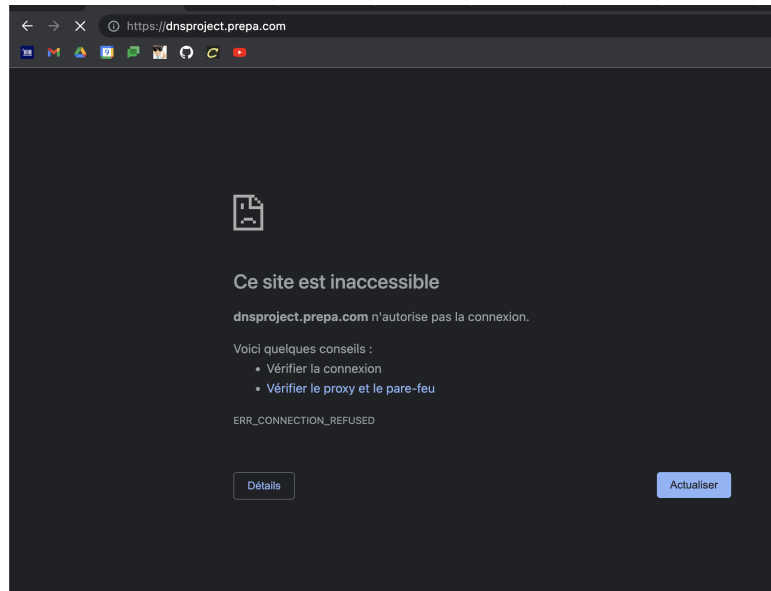
editer le fichier pour mettre l'adresse du réseau

une fois le fichier le dossier est disponible dans autre emplacement dans les fichier



JOB Bonus:

dans on chercher <https://dnsproject.prepa.com> on tombe sur



pour activer le HTTPS on doit se rendre dans le dossier apache

cd /etc/apache2

```
raph@raph:/etc/ufw$ cd /etc/apache2
raph@raph:/etc/apache2$ ls
apache2.conf  conf-enabled  magic          mods-enabled  sites-available
conf-available  envvars      mods-available  ports.conf    sites-enabled
raph@raph:/etc/apache2$
```

Créer un dossier ssl pour stocker les clé openssl qu'on va créer

sudo mkdir ssl

```
raph@raph:/etc/apache2$ sudo mkdir ssl
[sudo] Mot de passe de raph :
raph@raph:/etc/apache2$ ls
apache2.conf  conf-enabled  magic          mods-enabled  sites-available  ssl
conf-available  envvars      mods-available  ports.conf    sites-enabled
raph@raph:/etc/apache2$
```

une fois le dossier créé on crée la clé ssl

on génère la clé ssl

```
sudo openssl req -new -x509 -nodes -out /etc/apache2/ssl/server.crt  
-keyout /etc/apache2/ssl/server.key
```

```
raph@raph:/etc/apache2$ sudo openssl req -new -x509 -nodes -out /etc/apache2/ssl/server.crt -keyout  
/etc/apache2/ssl/server.key  
Generating a RSA private key  
.....+++++  
.....+++++  
writing new private key to '/etc/apache2/ssl/server.key'  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [AU]:FR  
State or Province Name (full name) [Some-State]:France  
Locality Name (eg, city) []:Marseille  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:dnsproject.prepa  
Organizational Unit Name (eg, section) []:laplateforme  
Common Name (e.g. server FQDN or YOUR name) []:dnsproject.prepa.com  
Email Address []:  
raph@raph:/etc/apache2$
```

on vérifie que les clés sont bien dans le dossier ssl

```
raph@raph:/etc/apache2$ cd ssl  
raph@raph:/etc/apache2/ssl$ ls  
server.crt  server.key  
raph@raph:/etc/apache2/ssl$
```

une fois les créer on peut se rendre dans /etc/apache2/sites-available

```
raph@raph:/etc/apache2$ cd sites-available/  
raph@raph:/etc/apache2/sites-available$ ls  
000-default.conf  default-ssl.conf  
raph@raph:/etc/apache2/sites-available$
```

Dans le dossier on va modifier le fichier default-ssl.conf ce dossier va nous permettre d'activer le protocole https


```
sudo nano default-ssl.conf
```

```
SSLCertificateFile      /etc/apache2/ssl/server.crt
SSLCertificateKeyFile   /etc/apache2/ssl/server.key
```

modifier ces deux ligne pour qu'elles face référence au clés qu'on vient de créer

si ufw est toujours actif penser à ouvrir le port 443 car c'est sur ce port que le serveur https sera émis

```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/html
```

ouvrir le port 443

```
sudo ufw allow 443/tcp
```

```
sudo ufw allow 443/udp
```

```
raph@raph:/etc/apache2/sites-available$ sudo ufw allow 443/tcp
Rules updated
Rules updated (v6)
raph@raph:/etc/apache2/sites-available$ sudo ufw allow 443/udp
Rules updated
Rules updated (v6)
```

sudo ufw reload pour prendre en compte les changements

```
raph@raph:/etc/apache2/sites-available$ sudo ufw reload
Firewall reloaded
raph@raph:/etc/apache2/sites-available$
```

une fois les ports ouvert on peut prendre en compte les changements effectués on utilise les commandes

```
sudo a2enmod ssl
```

```
sudo a2ensite default-ssl.conf
```

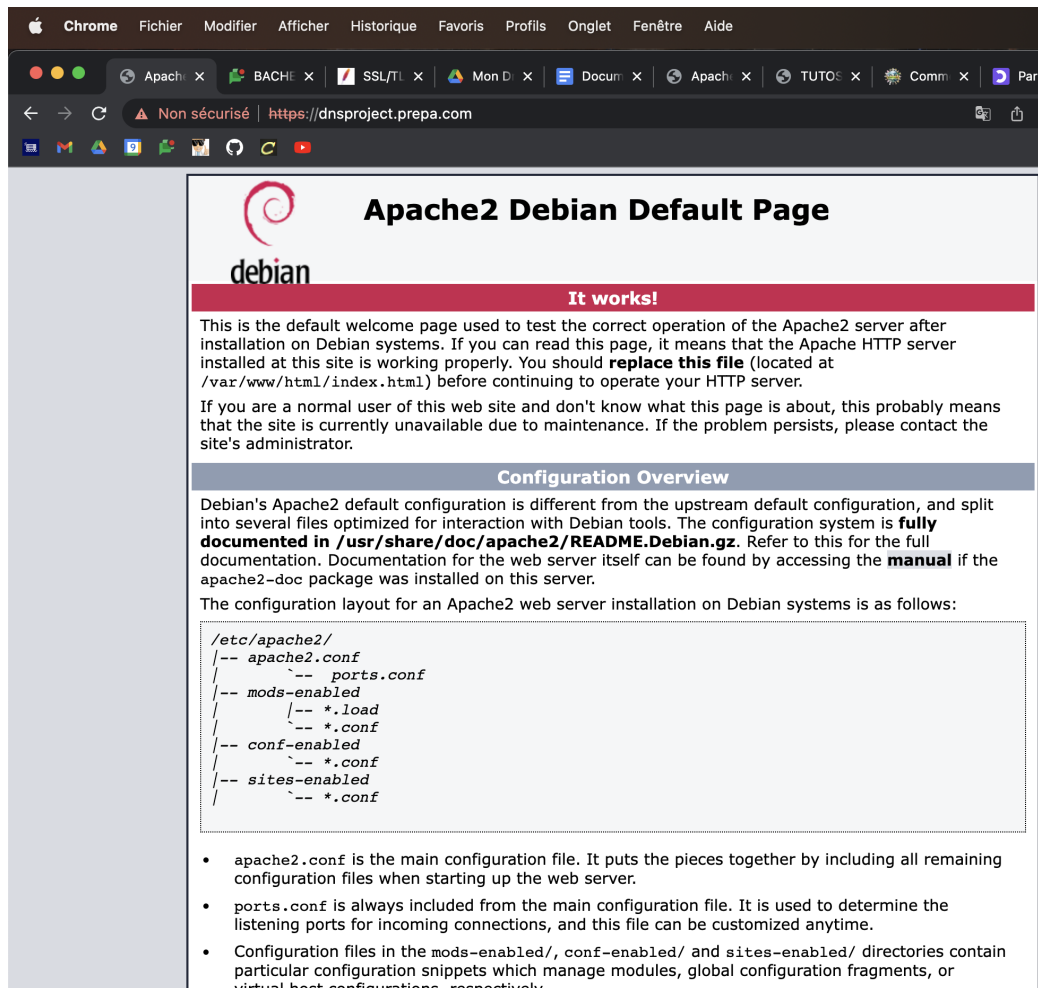
```
raph@raph:/etc/apache2/sites-available$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
raph@raph:/etc/apache2/sites-available$ sudo a2ensite default-ssl.conf
Enabling site default-ssl.
To activate the new configuration, you need to run:
  systemctl reload apache2
raph@raph:/etc/apache2/sites-available$
```

enfin on redémarre apache

```
sudo service apache2 restart
```

```
raph@raph:/etc/apache2/sites-available$ sudo service apache2 restart
raph@raph:/etc/apache2/sites-available$
```

on peut maintenant accéder au site via https



on peut voir que le site n'est pas sécurisé car c'est une clé auto-signé

les différent type de contrat SSL :

Il existe trois types de certificats SSL : les certificats à validation de domaine (DV), les certificats à validation d'organisation (OV) et les certificats à validation étendue (EV). Les niveaux de chiffrement sont les mêmes pour chaque type de certificat. Ce qui diffère, ce sont les processus d'audit et de vérification nécessaires pour obtenir le certificat.

Le nombre d'entreprises utilisant des certificats SSL a considérablement augmenté au cours des dernières années, et les cas d'application du SSL se sont diversifiés. Par exemple :

- vous pourriez avoir besoin du SSL pour assurer la confidentialité des communications (afin de ne pas être espionné),
- ou vous pourriez vouloir prouver que vous pouvez faire confiance à **votre interlocuteur** (identité au niveau de la communication privée).

Grâce au chiffrement, vous pouvez certes cacher les communications à un pirate informatique. Par contre, vous ne pouvez pas l'empêcher d'intercepter les communications et de se faire passer pour votre site web afin de voler les informations de vos clients. Les consommateurs se rendent de moins en moins dans les magasins traditionnels et achètent beaucoup plus en ligne. Ils doivent avoir la garantie que le propriétaire du site web du magasin sur lequel ils font leurs achats est bien celui qu'il dit être. Et cela s'avère plus difficile à prouver en ligne.

Vous pouvez prouver votre identité en faisant appel à une partie tierce (comme GlobalSign) de vérifier vos informations personnelles et celles de votre entreprise. Sur la base de cette procédure de vérification ou de contrôle, les certificats SSL peuvent être classés en trois catégories.

Certificats SSL à validation étendue (EV)

L'Autorité de Certification (AC) vérifie que l'organisation en question possède le droit exclusif d'utilisation du nom de domaine et soumet celle-ci à un **audit très approfondi**. Depuis 2007, les règles du CA/B Forum définissent les étapes strictement obligatoires que doivent suivre les Autorités de Certification afin de pouvoir émettre un certificat SSL à validation étendue. Ces étapes comprennent :

- la vérification de l'existence légale, physique et opérationnelle de l'organisation,
- la vérification de l'exactitude des informations transmises sur l'organisation (adresse, n° de téléphone) par rapport aux registres officiels,
- la vérification du droit exclusif d'utilisation du nom de domaine spécifié dans la demande de certificat EV SSL par l'organisation en question,
- la vérification de l'accord de l'organisation pour l'émission du certificat.

Les derniers, et peut-être plus importants, changements au niveau de la technologie SSL depuis sa création ont eu lieu lors de la mise en place des règles de standardisation relatives à la validation étendue. Les versions récentes des navigateurs, tels que Microsoft Internet Explorer 7+, Opera 9.5+, Firefox 3+, Google Chrome, Apple Safari 3.2+ et iPhone Safari 3.0+, qui offrent une sécurité plus élevée, identifient les certificats ExtendedSSL en tant que certificats à validation étendue. Ainsi, les symboles de renforcement de la sécurité sont activés au niveau de l'interface du navigateur. ExtendedSSL est la solution idéale pour les clients souhaitant garantir un niveau élevé d'authenticité.

Les certificats EV SSL sont disponibles pour tous types d'entreprises, que ce soit des agences gouvernementales et des entreprises enregistrées ou non constituées en société. D'autres règles appelées l'"EV Audit Guidelines", indiquent les critères obligatoires que les Autorités de Certification doivent remplir afin de pouvoir émettre des certificats SSL à validation étendue. Un audit vérifiant que ces critères sont bien remplis est conduit chaque année.

Certificats SSL à validation de l'organisation (OV)

L'AC vérifie que l'organisation en question possède le droit exclusif d'utilisation du nom de domaine pour lequel elle souhaite recevoir le certificat et soumet celle-ci à certaines vérifications. Les informations vérifiées apparaissent également dans le sceau de site sécurisé, pour une confiance accrue de la part des visiteurs. Le nom de l'organisation apparaît également dans le certificat sous le champ ON.

Certificats SSL à validation de domaine (DV)

L'AC vérifie que l'organisation en question possède le droit exclusif d'utilisation du nom de domaine pour lequel elle souhaite recevoir le certificat. L'identité de l'entreprise ne fait l'objet d'aucune vérification particulière. Aucune information n'apparaît donc dans le sceau de site sécurisé, mis à part les informations relatives au chiffrement. Vous avez la garantie que vos informations sont chiffrées, mais vous ne pouvez pas être sûr de savoir qui est réellement le destinataire de ces informations.

Le certificat DomainSSL est aussi reconnu et affiche les mêmes symboles de sécurité que le certificat OrganizationSSL au niveau du navigateur. Contrairement à ce dernier, il a l'avantage majeur de pouvoir être émis quasi immédiatement, sans avoir à soumettre de documents spécifiques relatifs à l'entreprise. Ainsi, DomainSSL est le certificat idéal pour les entreprises ayant besoin d'un certificat SSL pas cher, rapidement et sans contraintes administratives.

Certificats SSL autosigné.

Même si les certificats SSL auto-signés chiffrent tout aussi bien les connexions de clients et les identifiants d'autres comptes personnels, **ils déclenchent des alertes de sécurité sur la plupart des serveurs web car ils n'ont pas été vérifiés par une Autorité de Certification de confiance.**