**DDWS**

**JOB 1:**

-Télécharger une image Debian en .iso.

-Lancer une nouvelle VM depuis VMware.

-Choisir l’installation graphique lors du lancement de la machine.

-Installer SSH: sudo apt-get install ssh

**JOB 2:**

sudo apt-get install apache2

Aller sur la page d'accueil d’Apache2 pour vérifier l’installation: aller à l’adresse de la VM depuis l’hôte sur un navigateur.

**JOB 3:**

2 principaux serveurs Web:

* Apache :

Est:

* + Open-source, et par extension gratuit
  + Régulièrement mis à jour
  + Simple à configurer
  + Compatible avec les systèmes Unix et Windows
  + Communauté active et support disponible

Mais:

* + Peut rencontrer des problèmes de performance sur les sites Web avec un trafic élevé
  + Ses options de configuration peuvent mener à la vulnérabilité de la sécurité.

[source](https://www.hostinger.fr/tutoriels/quest-ce-quapache-serveur-web-apache#Les_avantages_et_inconvenients_dApache)

* Nginx:
  + A une architecture modulaire (configurations)
  + Est régulièrement mis à jour et de manière optimisée
  + Est plus adapté pour les sites Web avec un trafic élevé
  + Est conçu sur mesure pour accélérer le fonctionnement des serveurs privés virtuels (VPS).

Mais:

* + Ne prend pas en charge .htaccess (fichiers de config propres à un répertoire)
  + Est moins compatible avec les technologies tierces
  + Communauté et support plus réduite qu’ Apache

[source](https://www.opportunites-digitales.com/guide-complet-du-serveur-nginx/)

**JOB 4:**

ajouter l’IP et le nom de domaine dans le fichier **/etc/hosts**:

192.168.19.135 dnsproject.prepa.com

**JOB 5:**

Pour obtenir un nom de domaine, il faut s’adresser à un agent d’enregistrement « registrar »,

c’est une société privée qui se charge des démarches administratives et techniques d'enregistrement d'un nom de domaine auprès des registres concernés. Il joue le rôle d'intermédiaire entre le “Registrant” et le “Registre“

Certaines extensions sont utilisées à vocation commerciale: .com, .net, .org, etc…

Tandis que d’autres sont à vocation nationale ou géographique: .fr (France), .eu (Union européenne), .tv (Tuvalu), .it (Italie).

**JOB 6:**

Ce job a été réalisé en étant connecté au réseau WIFI en bridge. (10.10.29.58)

Dans **/etc/apache2/sites-enabled/000-default.conf**, ajouter la ligne:

*ServerName = dnsproject.prepa.com*

Ajouter l’adresse du serveur dans **/etc/resolv.conf** :

* Désactiver la réinitialisation automatique de **resolv.conf** :

Ajouter un fichier de configuration dans **/etc/NetworkManager/conf.d/** en **.conf** qui contiendra:

*[main]*

*dns=none*

* Dans **/etc/resolv.conf**, ajouter les lignes:

*search dnsproject.prepa.com*

*nameserver 10.10.29.58*

Dans **/etc/bind/named.conf.local**, ajouter les lignes:

*zone "prepa.com" IN {*

*type master;*

*file "/etc/bind/prepa.forward.zone";*

*};*

*zone "29.10.10.in-addr.arpa" IN {*

*type master;*

*file "/etc/bind/prepa.reverse.zone";*

*};*

Créer les fichiers “**prepa.forward.zone**” et “**prepa.reverse.zone**” dans **/etc/bind**

Dans **prepa.forward.zone** :

*$TTL 604800*

*@ IN SOA prepa.com. root.dnsproject.prepa.com. (*

*2 ; Serial*

*604800 ; Refresh*

*86400 ; Retry*

*2419200 ; Expire*

*604800 ) ; Negative Cache TTL*

*;*

*@ IN NS dnsproject.prepa.com.*

*dnsproject IN A 10.10.29.58*

*www IN CNAME dnsproject.prepa.com.*

Dans **prepa.reverse.zone** :

*$TTL 604800*

*@ IN SOA prepa.com. root.dnsproject.prepa.com. (*

*2 ; Serial*

*604800 ; Refresh*

*86400 ; Retry*

*2419200 ; Expire*

*604800 ) ; Negative Cache TTL*

*;*

*@ IN NS dnsproject.prepa.com.*

*dnsproject IN A 10.10.29.58*

*58 IN PTR dnsproject.prepa.com.*

**prepa.forward.zone** va permettre au DNS de trouver l’ip du site web en fonction du nom de domaine, tandis que **prepa.reverse.zone** permet l’opération inverse.

Dans la configuration hôte, il faut modifier les paramètres DNS en ajoutant l’ip de la machine virtuelle comme DNS.

Comme le DNS de la VM n’est configuré que pour trouver un seul nom de domaine, il faut spécifier un forwarder sur l’hôte (sous Windows, entrer **8.8.8.8** ou **8.8.4.4** comme forwarder dans le champ “Autre DNS” ou “DNS Secondaire”, cela va permettre d’utiliser le serveur DNS public fourni par Google).

**JOB 8 :**

Ce job a été réalisé en étant connecté en NAT.

Aller dans **/etc/network/interfaces** et ajouter les lignes:

*#carte connectée à internet*

*auto ens33*

*iface ens33 inet static*

*address 192.168.0.1*

*network 192.168.0.0*

*netmask 255.255.255.0*

*gateway 192.168.0.254*

#permet de charger la configuration à chaque redémarrage

*post-up iptables-restore < /etc/iptables.save*

*#carte vers le LAN*

*auto ens34*

*iface ens34 inet static*

*address 192.168.1.1*

*network 192.168.1.0*

*netmask 255.255.255.0*

Pour appliquer les modifications, il faut relancer le service “networking”:

*systemctl restart networking*

Décommenter la ligne dans **/etc/sysctl.conf**:

*net.ipv4.ip\_forward=1*

Mettre à jour les modifications : *sudo sysctl -p*

Mise en place de la passerelle sur ens33 pour le protocole NAT

*iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE*

Écraser le fichier de configuration avec le nouveau :

*iptables-save > /etc/iptables.save*

Redémarrer le système, puis vérifier la passerelle mise en place:

iptables -L -t nat

Sur les VM reliées à notre serveur, il suffit d’ajouter en passerelle l’ip 192.168.1.1

**JOB 7 :**

Configuration avec ISC DHCP:

*sudo apt-get install isc-dhcp-server*

Dans le fichier de config **/etc/dhcp/dhcpd.conf**, ajouter les lignes:

*subnet 192.168.1.0 netmask 255.255.255.0 {*

*range 192.168.1.2 192.168.1.50;*

*option domain-name-servers 192.168.1.1;*

*option domain-name "dnsproject.prepa.com";*

*option netbios-name-servers 192.168.1.1;*

*option routers 192.168.1.1;*

*option subnet-mask 255.255.255.0;*

*option broadcast-address 192.168.1.255;*

*default-lease-time 86400;*

*max-lease-time 676800;*

*}*

Pour appliquer les changements, redémarrer le service:

*systemctl restart isc-dhcp-server*

**Job 9 :**

Installation de UFW:

*sudo apt-get install ufw*

Activation du service :

*ufw enable*

Pour interdire le ping, commenter la ligne suivante dans le fichier **/etc/ufw/before.rules** :

*-A ufw-before-input -p icmp --icmp-type echo-request -j ACCEPT*

Cela va bloquer les requêtes icmp en echo-request, les requêtes qu’envoient la commande ping.

Pour appliquer les changements :

*ufw disable*

*ufw enable*

**Job 10 :**

Installation de Samba :

*apt-get install samba*

Éditer fichier de configuration Samba **/etc/samba/smb.conf** :

*[partage]*

*comment = Partage de données*

*path = /srv/partage*

*guest ok = no*

*read only = no*

*browseable = yes*

*valid users = @partage*

Redémarrage de samba pour appliquer les changements:

*systemctl restart smbd\**

"partage" est un groupe d'utilisateurs qui n'existe pas. On créer le groupe:

*groupadd partage*

Ne pas oublier de créer le dossier “**/srv/partage”**, c’est là que seront stocké les fichiers:

*mkdir /srv/partage*

*chgrp -R partage /srv/partage/*

*chmod -R g+rw /srv/partage/*

Les utilisateurs étant dans le groupe “partage” seront les seuls à avoir accès au dossier partagé.

Pour ajouter des utilisateurs:

*adduser [username]*

Ensuite, lui attribuer un mot de passe pour samba:

*smbpasswd -a =[username]*

Enfin, ajouter les utilisateurs au groupe:

*gpasswd -a [username] partage*

**Pour aller plus loin :**

Activer le support TLS pour le serveur Web:

*sudo a2enmod ssl*

*sudo a2ensite default-ssl*

Recharger la configuration:

*systemctl reload apache2*

Installer Certbot :

*sudo apt install certbot*

Certbot permet d’utiliser des certificats Let’s Encrypt pour des sites Webs administrés manuellement, et permet d’activer le HTTPS pour un site Web.

Pour générer le certificat:

*sudo certbot certonly --webroot -w /var/www/html/index.html -d prepa.com -d dnsproject.prepa.com*

Dans le fichier **/etc/apache2/sites-available/000-default.conf**, ajouter les lignes:

*<Directory /srv/web/prepa.com/www>*

*Options -Indexes +FollowSymLinks +MultiViews*

*AllowOverride none*

*Require all granted*

*</Directory>*

*SSLEngine on*

*SSLCertificateFile /etc/letsencrypt/live/prepa.com/fullchain.pem #pointe vers le certificat généré*

*SSLCertificateKeyFile /etc/letsencrypt/live/prepa.com/privkey.pem #pointe vers la clé générée*

*Header always set Strict-Transport-Security "max-age=15768000"*

Et changer le port utilisé de 80 à 443:

<VirtualHost \*:80> → <VirtualHost \*:443>

Appliquer les changements des configurations:

*systemctl reload apache2*

**Questions:**

Quelle est la différence entre les certificats SSL donnés par des organismes extérieurs et le vôtre auto-signé ?

La différence est qu’un certificat auto-signé n’est pas approuvé par une autorité de certification (CA). Celui-ci a donc moins de “valeur” qu’un certificat approuvé par une autorité de certification, car l’autorité de certification permet d’établir avec certitude l’identité de l’entreprise et du serveur web.

Pourquoi votre certificat apparaît-il comme non sécurisé dans votre navigateur ?

Le certificat est auto-signé, il n’est donc approuvé par aucune autorité de certification, et n’est donc pas approuvé par une autorité compétente (il est donc basé sur la confiance).