

2024

PROJET INFRASTRUCTURE SÉCURISÉE

Présenté par :

Zouaoui Mehdi

SISR

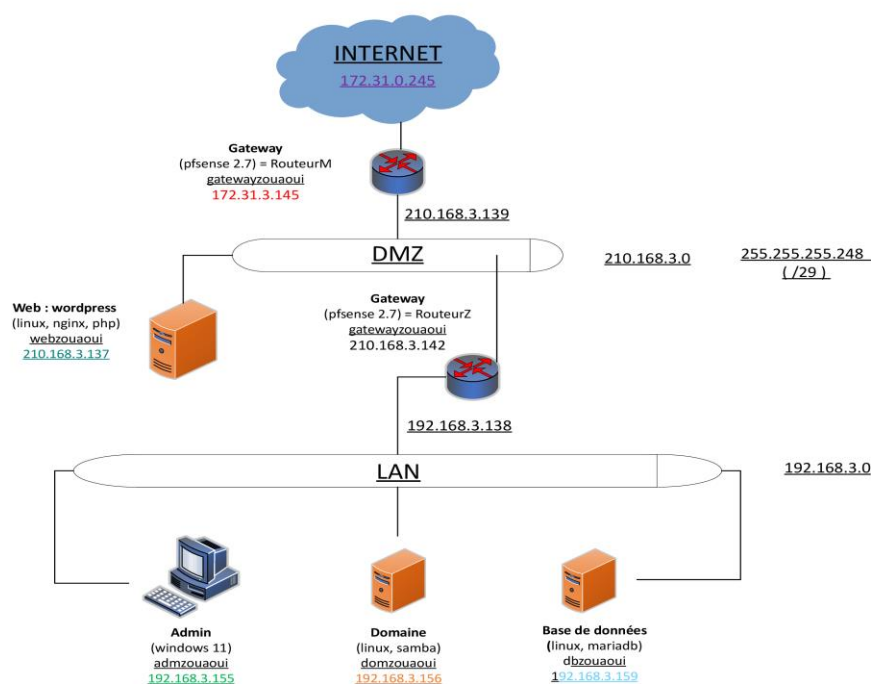
SOMMAIRE

Organisation	3-4
Configuration des machines	4-5
Machine Linux	4-5
Machine Windows 11	5
Machine WEB	5-7
Machine Base de données	7-8
Machine WORDPRESS	8
Partie Routeurs	8-11
Machine de Domaine	12-18

L'organisation :

Pour l'organisation concernant le PROJET D'INFRASTRUCTURE ainsi que les tâches à accomplir qui sont accompagnées nous avons procédé étape par étape.

Dans un premier temps, nous avons construit notre propre schéma réseaux avec l'ensemble des machines/serveurs/routeurs présents pour le projet.



Le projet contiendra 2 routeurs (nommés«gatewayzouaoui») puis, un serveur Web WORDPRESS sous Linux, nginx, Php (nommé«webzouaoui») qui sera dans la DMZ (DemilitarizedZone).

Concernant le LAN, un ensemble de 3 serveurs qui sont le serveur Admin sous Windows11 (nommés«admzouaoui»), un serveur de Domaine sous Linux et Samba (nommés«domzouaoui») puis le serveur Base de données sous linux et mariadb (nommé « dbzouaoui »).

Suite à la création du schéma réseau, nous avons aussi fait une table de routage du schéma / projet :

Machine	Nom	Adresse IP	Masque	Passerelle	DNS
Réseau 1	Réseau 1	172.31.0.0/21	255.255.248.0		
Routeur 1	RouteurZ	172.31.3.145	255.255.248.0	172.31.0.245	
Réseau DMZ	Réseau DMZ	210.168.3.136/29	255.255.255.248		
Routeur 1	RouteurZ	210.168.3.138	255.255.255.248	172.31.0.245	
Routeur 2	RouteurM	210.168.3.139	255.255.255.248	210.168.3.141	
Serveur Web	webzouaoui	210.168.3.137	255.255.255.248	210.168.3.141	
Réseau LAN	Réseau LAN	192.168.3.0/24	255.255.255.0		
Routeur 1	RouteurZ	192.168.3.140	255.255.255.0	210.168.3.141	
Admin	adminzouaoui	192.168.3.155	255.255.255.0	192.168.3.140	
Base de données	dbzouaoui	192.168.3.159	255.255.255.0	192.168.3.140	
Domaine	domzouaoui	192.168.3.156	255.255.255.0	192.168.3.140	

Suite à la création du schéma réseau et de la table de routage ci-dessus nous avons donc procédé à la création / configuration / installation des différentes machines / serveurs.

Configuration des machines :

Machines Linux :

Linux ou GNU/Linux est une famille de systèmes d'exploitation open source de type Unix fondés sur le noyau Linux créé en 1991 par Linus Torvalds. De nombreuses distributions Linux ont depuis vu le jour et constituent un important vecteur de popularisation du mouvement du logiciel libre.

Concernant la configuration pour l'ensemble des machines Linux il suffit tout simplement d'utiliser ces 3 commandes qui sont essentiels pour configurer une machine / serveur en Linux.

Les commandes :

nano /etc/hostname = Permet de renommer le nom de la machine.

nano /network/interfaces = Permet de config la catégorie réseau (IP..).

apt update&upgrade = Permet de mettre à jour et de les télécharger.

Machine Windows 11 :

Windows 11 est une version majeure du système d'exploitation Windows développé par Microsoft, exploitant le noyau Windows NT en version 10. Windows 11 a été annoncé lors du Microsoft Event le 24 juin 2021.

Concernant la configuration Windows 11, il suffit tout simplement d'aller dans :

Paramètres -> Réseau et Internet : puis de configurer en mettant les bonnes informations comme un exemple l'adresse IP.

Pour changer le nom de la machine Windows 11 il suffit d'aller dans :

Paramètres -> Système -> À propos de. -> Renommer ce PC

Installation de la machine WEB à l'aide de NGINX :

NGINX Open Source ou NGINX est un logiciel libre de serveur Web ainsi qu'un proxy inverse écrit par Igor Sysoev, dont le développement a débuté en 2002 pour les besoins d'un site russe à très fort trafic. La documentation est disponible dans plusieurs langues.

Concernant l'installation de la machine WEB à l'aide de NGINX il faut dans un premier **désinstallait apache**.

La commande : **`apt remove apache2`**

Ensuite, nous pouvons installer plusieurs outils / services qui va nous permettre d'avancer dans l'installation et la configuration.

Les commandes :

`apt install nginx` = Permet d'installer NGINX

`apt install php-fpm` = Permet d'installer PHP FPM

`apt install php-server` = Permet d'installer PHP SERVER

Une fois ces étapes faites, nous allons se concentrer sur le site WEB. Pour configurer le site WEB nous devons enlever le " # " sur certaines lignes. (décommenter les lignes du fichier)

La commande : **`nano etc/nginx/sites-avaible/default`**

Puis, nous devons mettre du contenu dans notre site internet à l'aide de MobaXterm ou directement en ligne de commande.

La commande (le fichier) : **`/var/www/html/index.html`**

Ensuite, concernant PHPMyAdmin il faudra l'installer depuis Internet en format ZIP.

Nous allons pour cette étape utiliser MobaXterm, il suffira de glisser / transférer le fichier ZIP de PHPMyAdmin.

Une fois le ZIP transféré, nous devons utiliser les commandes ci-dessous pour la suite :

apt install unzip = Permet d'installer pour dézipper les fichiers ZIP.

mv 'le nom du fichier' 'nouveau nom' = Permet de renommer le fichier.

var/www/html/phpMyAdmin = Permet à cet emplacement de rentrer les informations.

Installation de la machine Base de Données à l'aide de MARIADB

:

MariaDB est un système de gestion de base de données édité sous licence GPL. Il s'agit d'un embranchement communautaire de MySQL : la gouvernance du projet est assurée par la fondation MariaDB, et sa maintenance par la société Monty Program AB, créateur du projet

Pour la machine / serveur Base de données nous devons installer MARIADB et PHPMySQLI.

Les commandes :

apt install mariadb-server = Permet d'installer Mariadb Server.

apt install php-mysqli = Permet d'installer PHPMySQLI.

Ensuite, on le configure à l'aide de cette commande ou l'on va modifier le BIND.

La commande : **nano /etc/mysql/mariadb.conf.d/50-server.cnf**

Concernant PHP voici les commandes suivantes à rentrer :

`mysql -u root -p` = Permet de se connecter à la base de donnée SQL.

Puis de créer un user avec les permissions / privilèges :

```
CREATE USER 'root'@'%' IDENTIFIED BY 'sio';  
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'sio';  
FLUSH PRIVILEGES ;  
ALTER USER 'root'@'ip' IDENTIFIED BY 'sio' ;
```

Configuration et Installer de WORDPRESS :

WordPress est un système de gestion de contenu gratuit, libre et open-source. Ce logiciel écrit en PHP repose sur une base de données MySQL et est distribué par la fondation WordPress.org

Pour WORDPRESS, nous allons l'installer sur internet en ZIP puis le transférer sur MobaXterm puis ensuite le dézipper. (Même étape que pour PHP)

Nous devons mettra le permission, pour cela :

```
chown -R www-data /var/www/html
```

Catégorie Routeurs :

Concernant les routeurs (gateway), nous avons importé à l'aide de l'application VirtualBox un serveur Windows (OVA) et une ISO pour le routeur.

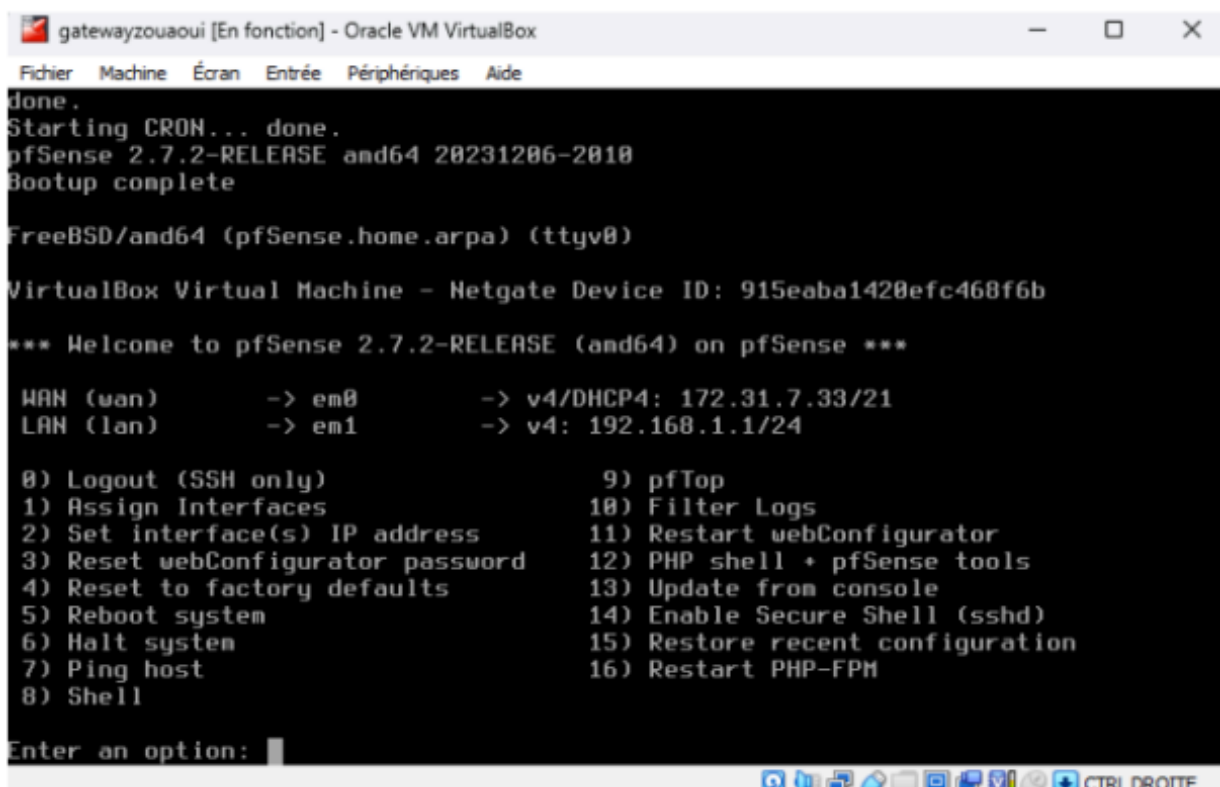
Mettre l'OVA et l'ISO sur le Disque D :

On importe l'OVA avec le bon nom (admzouaoui) puis l'ISO avec le bon nom (gatewayzouaoui) + vérifier la configuration réseau et ajouter une 2 ème carte réseau.

Ensuite, aller sur nouvelle / insérer l'ISO / type BSD / 64 bits Free / RAM 1 go / Stockage disque 16 go / accès par pont.

Puis, lancer sur (MONTER) l'ISO en appuyant et laisser tout par défaut.

Une fois l'installation faite, supprimer le disque sur VirtualBox afin de ne pas faire en boucle l'installation.



```
gatewayzouaoui [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/and64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 915eaba1428efc468f6b

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.31.7.33/21
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Ensuite, il faudra bien configurer avec les bonnes adresses IP en sélectionnant le 2 (Set interface(s) IP address).

Ainsi l'option 7 est disponible pour tester la connexion (ping).

Une fois bien configurés avec les bonnes adresses IP nous allons sur la machine WINDOWS (admzouaoui).

Sur la machine WINDOWS, vérifier la connexion en allant sur le CMD (Windows+R -> CMD).

Tester la connexion avec les commandes suivantes sur le cmd :

ping google.fr

ping 8.8.8.8

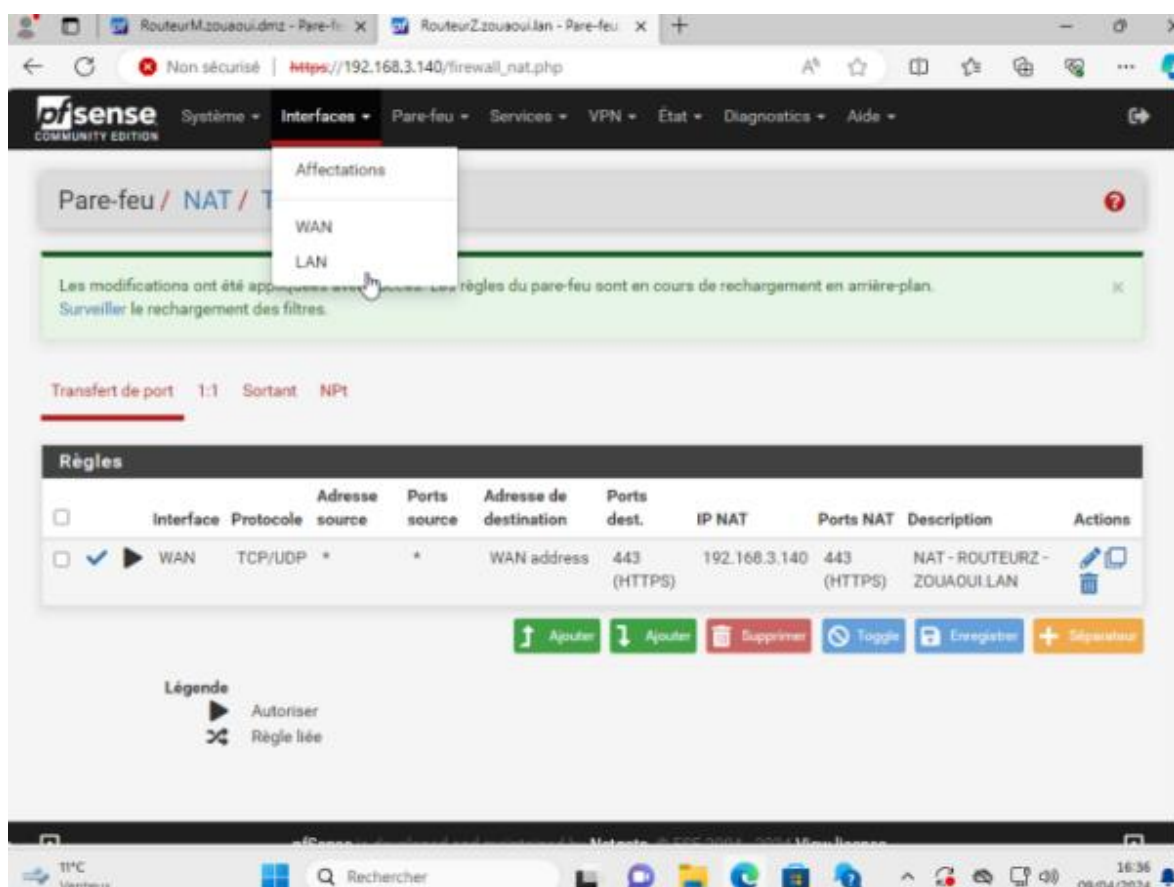
Une fois les tests effectués, aller sur internet depuis la machine WINDOWS en rentrant l'adresse IP du LAN du routeur.

Ensuite, nous allons arrivé sur Pfsense.

User : admin | Mot de passe : sio (modifier le mot de passe !)

Ping protocole Icmp

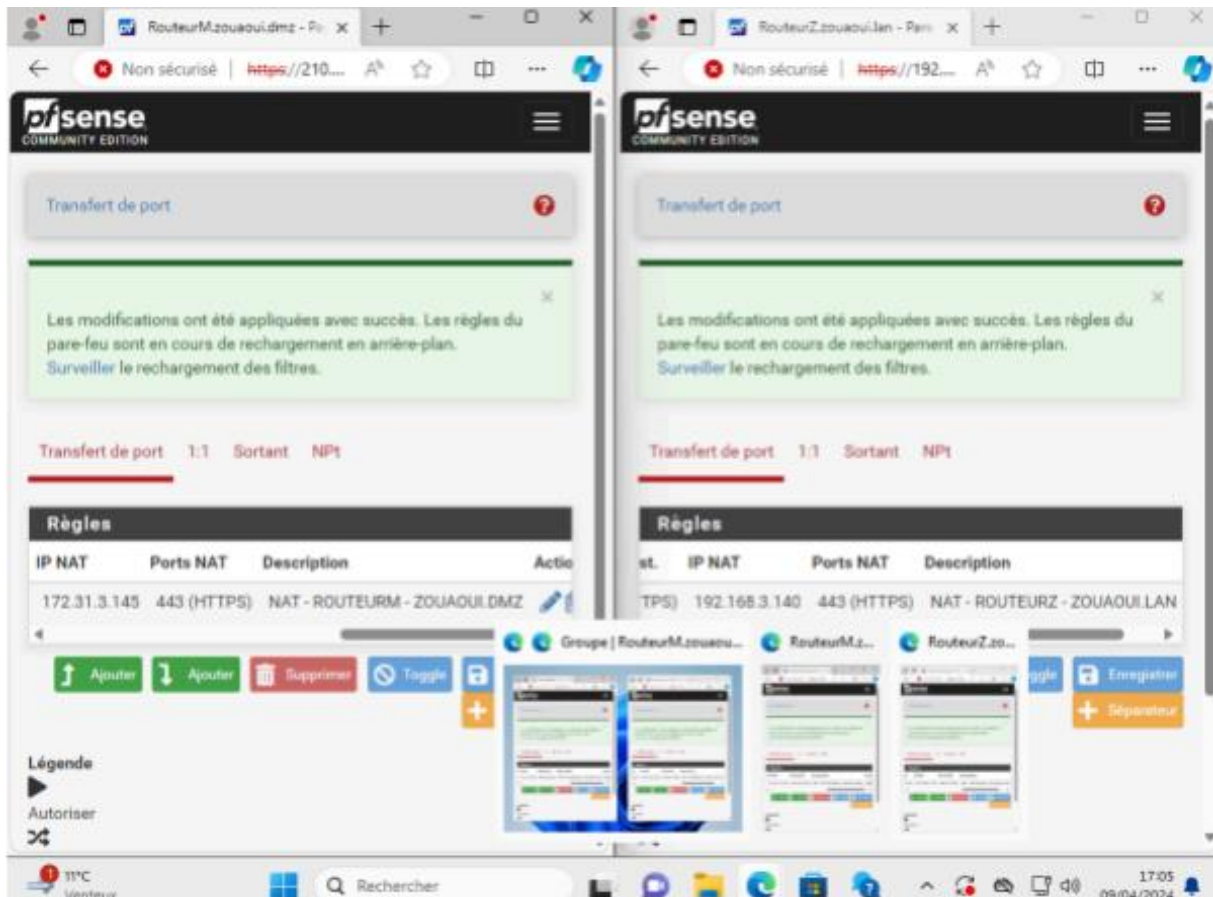
Une fois connecté sur Pfsense il faudra modifier et configurer le WAN et le LAN dans l'interface.



RAPPEL : S'il n'y a plus de connexion alors sélectionnez bien dans le WAN la passerelle IPV4 en AMONT puis aller dans Pare-feu puis dans NAT.

Une fois que le routeur est bien configuré et que les tests ont bien été effectués, suivez les mêmes étapes pour le 2ème routeur.

Après avoir configuré le 2ème routeur nous irons dans Pare-feu / NAT / Transfert de Port.



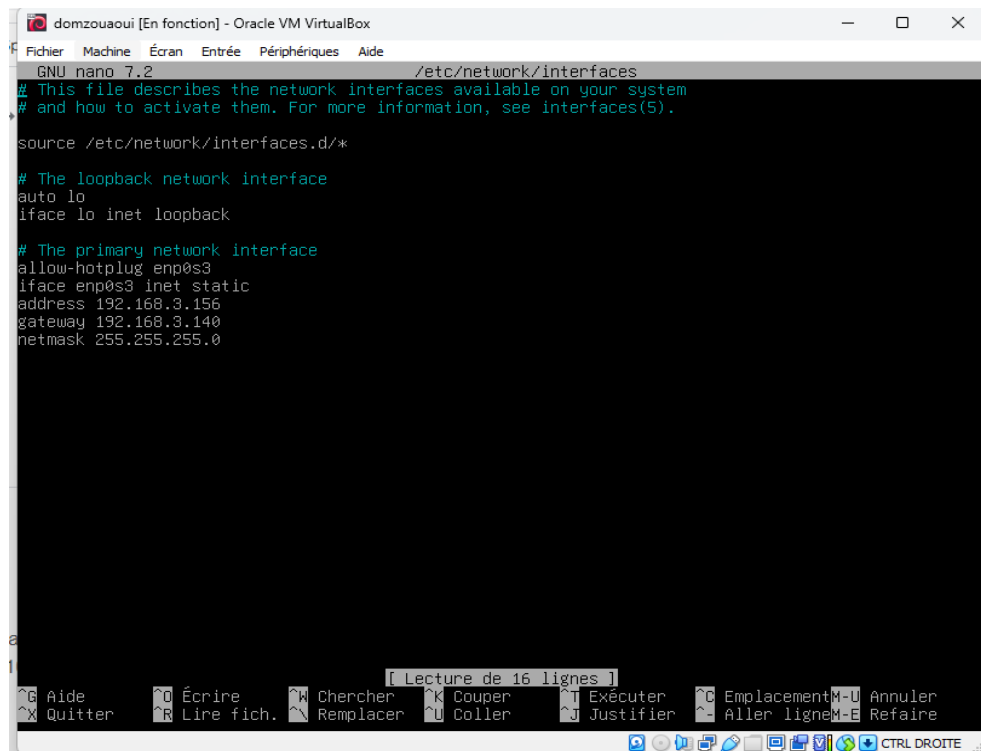
Une fois que les règles NAT des 2 routeurs sont finis, nous avons modifier à nouveau l'adresse IP du serveur WEB et le serveur de Base de données.

Serveur de Domaine (SAMBA)

Pour le serveur de domaine, nous avons importé une OVA en version Debian 64 bits de type Linux avec les paramètres par défaut en réseau interne.

Une fois l'OVA importée et lancée, nous allons configurer la machine avec les commandes suivantes :

`nano /etc/network/interfaces` = Dossier de configuration



```
domzouaoui [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

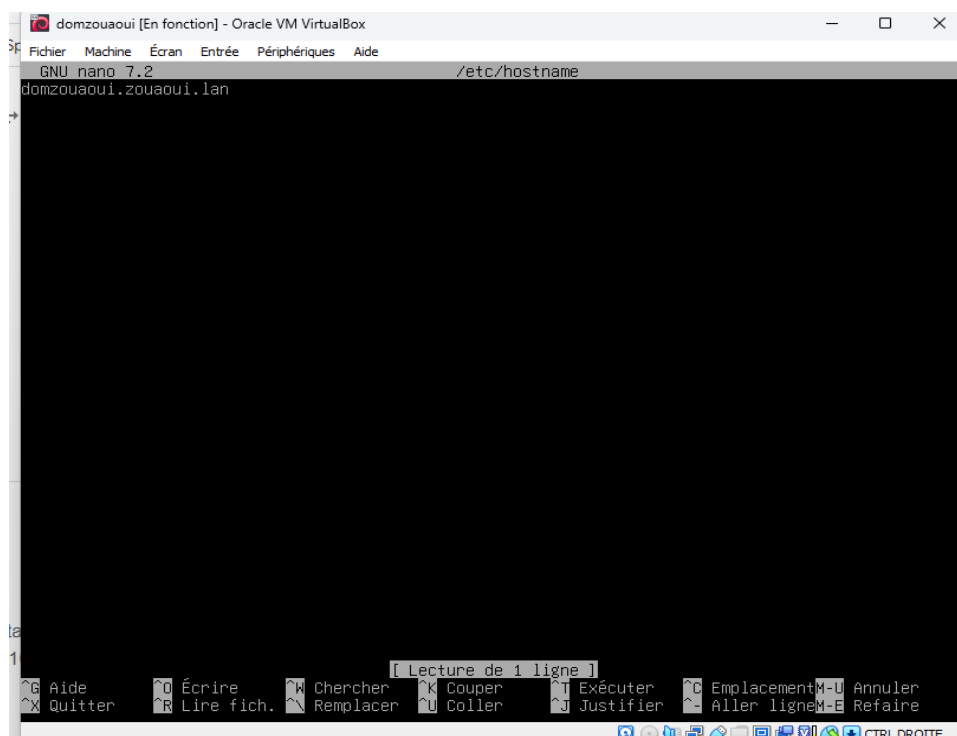
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.3.156
gateway 192.168.3.140
netmask 255.255.255.0

[ Lecture de 16 lignes ]
^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement M-U Annuler
^X Quitter   ^R Lire fich. ^N Remplacer ^U Coller    ^J Justifier ^_ Aller ligne M-E Refaire
CTRL DROITE
```

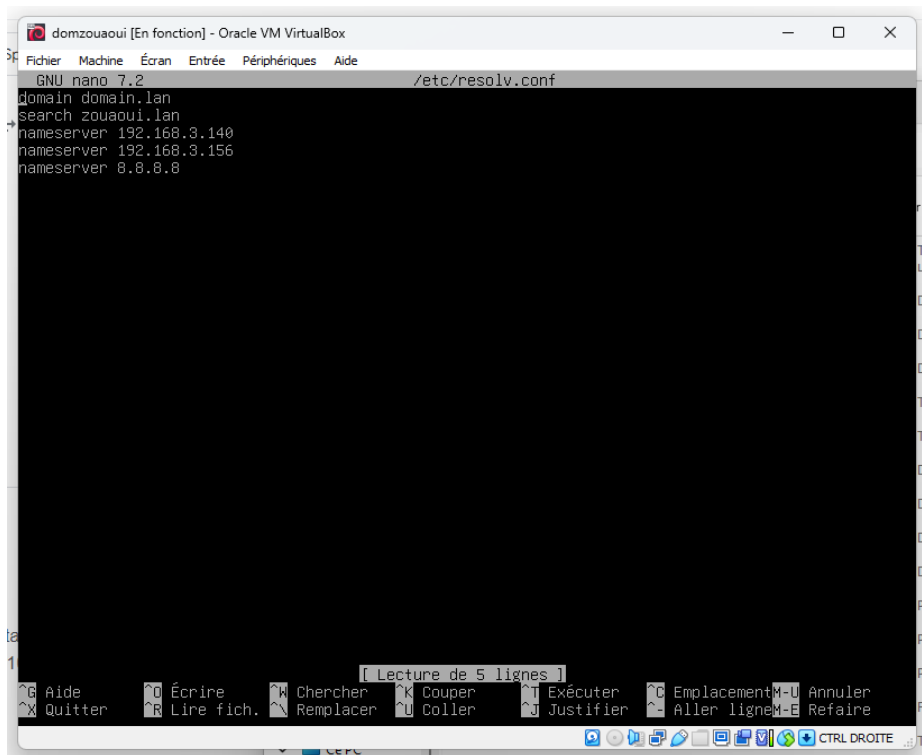
`nano etc/hostname` = Renommer le nom de la machine



```
domzouaoui [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
GNU nano 7.2 /etc/hostname
domzouaoui.zouaoui.lan

[ Lecture de 1 ligne ]
^G Aide      ^O Écrire   ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement M-U Annuler
^X Quitter   ^R Lire fich. ^N Remplacer ^U Coller    ^J Justifier ^_ Aller ligne M-E Refaire
CTRL DROITE
```

nano etc/resolv.conf

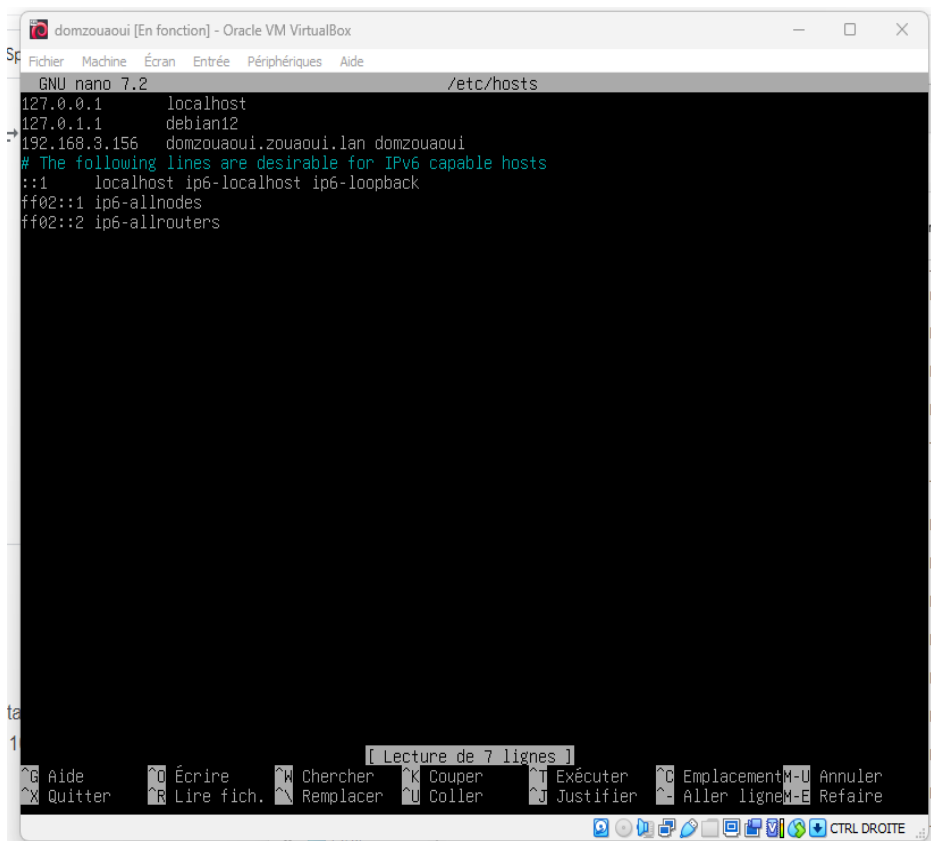


The screenshot shows a nano editor window titled 'domzouaoui [En fonction] - Oracle VM VirtualBox'. The editor is editing the file '/etc/resolv.conf'. The content of the file is as follows:

```
domain domain.lan
search zouaoui.lan
nameserver 192.168.3.140
nameserver 192.168.3.156
nameserver 8.8.8.8
```

The nano editor's status bar at the bottom indicates '[Lecture de 5 lignes]' (Reading 5 lines). The bottom of the window shows the standard nano editor keyboard shortcuts.

nano etc/hosts



The screenshot shows a nano editor window titled 'domzouaoui [En fonction] - Oracle VM VirtualBox'. The editor is editing the file '/etc/hosts'. The content of the file is as follows:

```
127.0.0.1 localhost
127.0.1.1 debian12
192.168.3.156 domzouaoui.zouaoui.lan domzouaoui
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

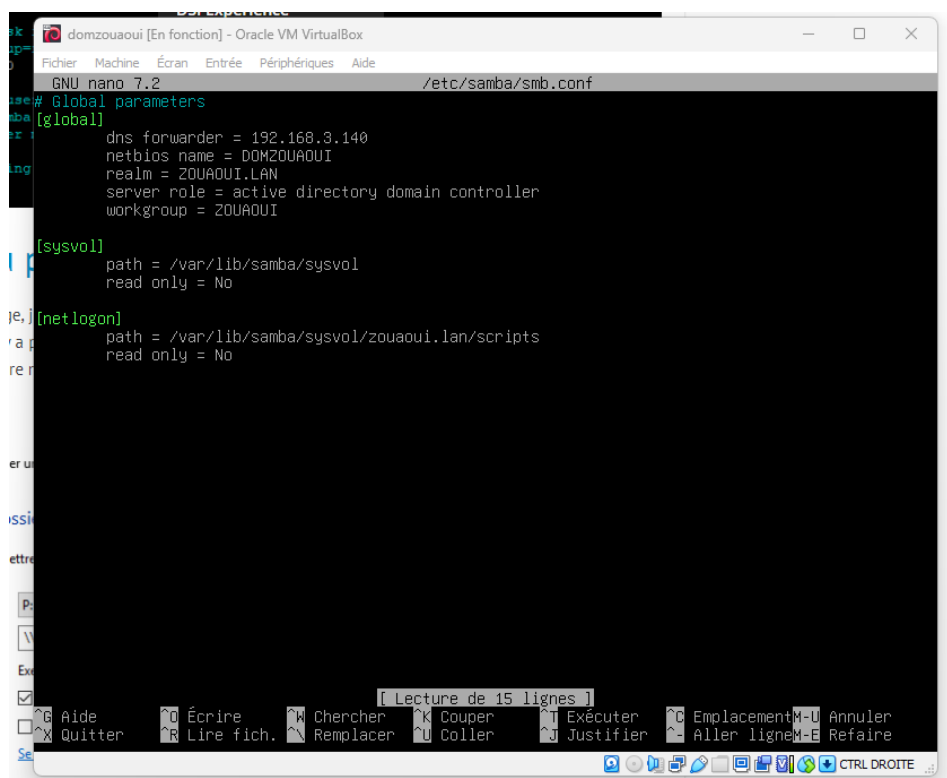
The nano editor's status bar at the bottom indicates '[Lecture de 7 lignes]' (Reading 7 lines). The bottom of the window shows the standard nano editor keyboard shortcuts.

Après avoir configuré la machine, nous allons installer SAMBA AD à l'aide de la commande ci-dessous :

```
apt-get install samba winbind libnss-winbind krb5-user smbclient ldb-tools python3-cryptography
```

Une fois SAMBA AD installé nous allons faire la commande suivante pour configurer SAMBA AD :

```
nano etc/samba/smb.conf
```



The screenshot shows a terminal window titled "domzouaoui [En fonction] - Oracle VM VirtualBox". Inside, the nano 7.2 text editor is open to the file /etc/samba/smb.conf. The editor displays the following configuration:

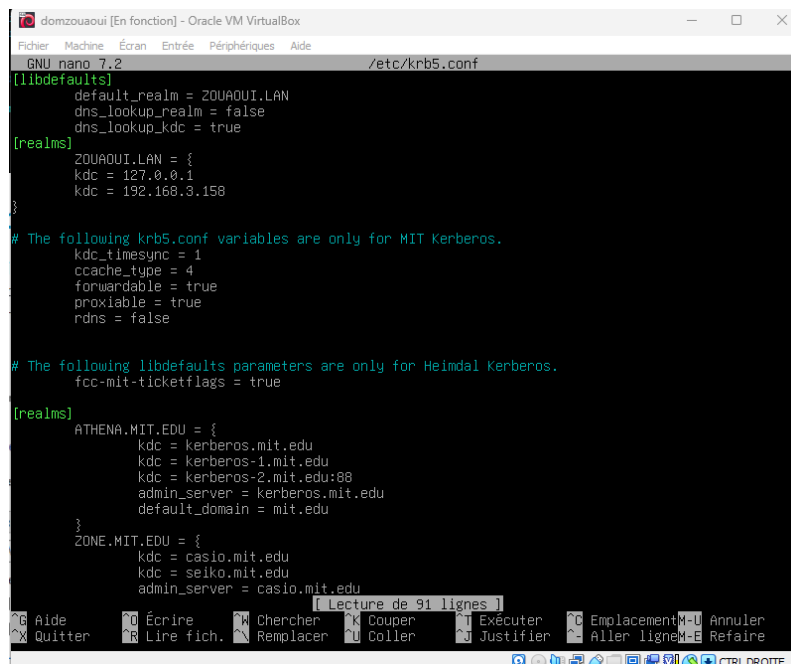
```
GNU nano 7.2 /etc/samba/smb.conf
# Global parameters
[global]
    dns forwarder = 192.168.0.140
    netbios name = DOMZOUAQUI
    realm = ZOUAQUI.LAN
    server role = active directory domain controller
    workgroup = ZOUAQUI

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/zouaoui.lan/scripts
    read only = No
```

At the bottom of the terminal, a status bar shows "[Lecture de 15 lignes]" and a list of keyboard shortcuts: Aide, Écrire, Chercher, Couper, Exécuter, Emplacement, Annuler, Quitter, Lire fich., Remplacer, Coller, Justifier, Aller ligne, Refaire. The bottom of the window shows the Ubuntu desktop taskbar with various application icons and the text "CTRL DROITE".

Puis, **nano etc/krb5.conf**



```
GNU nano 7.2 /etc/krb5.conf
[libdefaults]
    default_realm = ZOUAQUI.LAN
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
    ZOUAQUI.LAN = {
        kdc = 127.0.0.1
        kdc = 192.168.3.158
    }

# The following krb5.conf variables are only for MIT Kerberos.
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true
rdns = false

# The following libdefaults parameters are only for Heimdal Kerberos.
fcc-mit-ticketflags = true

[realms]
    ATHENA.MIT.EDU = {
        kdc = kerberos.mit.edu
        kdc = kerberos-1.mit.edu
        kdc = kerberos-2.mit.edu:88
        admin_server = kerberos.mit.edu
        default_domain = mit.edu
    }
    ZONE.MIT.EDU = {
        kdc = casio.mit.edu
        kdc = seiko.mit.edu
        admin_server = casio.mit.edu
    }
```

Une fois toutes les configurations effectués ci-dessus, nous allons retirer le fichier de configuration de SAMBA à l'aide de la commande suivante :

rm -f /etc/samba/smb.conf

Suite à cela, nous allons mettre écrire cette commande afin de créer un nouveau :

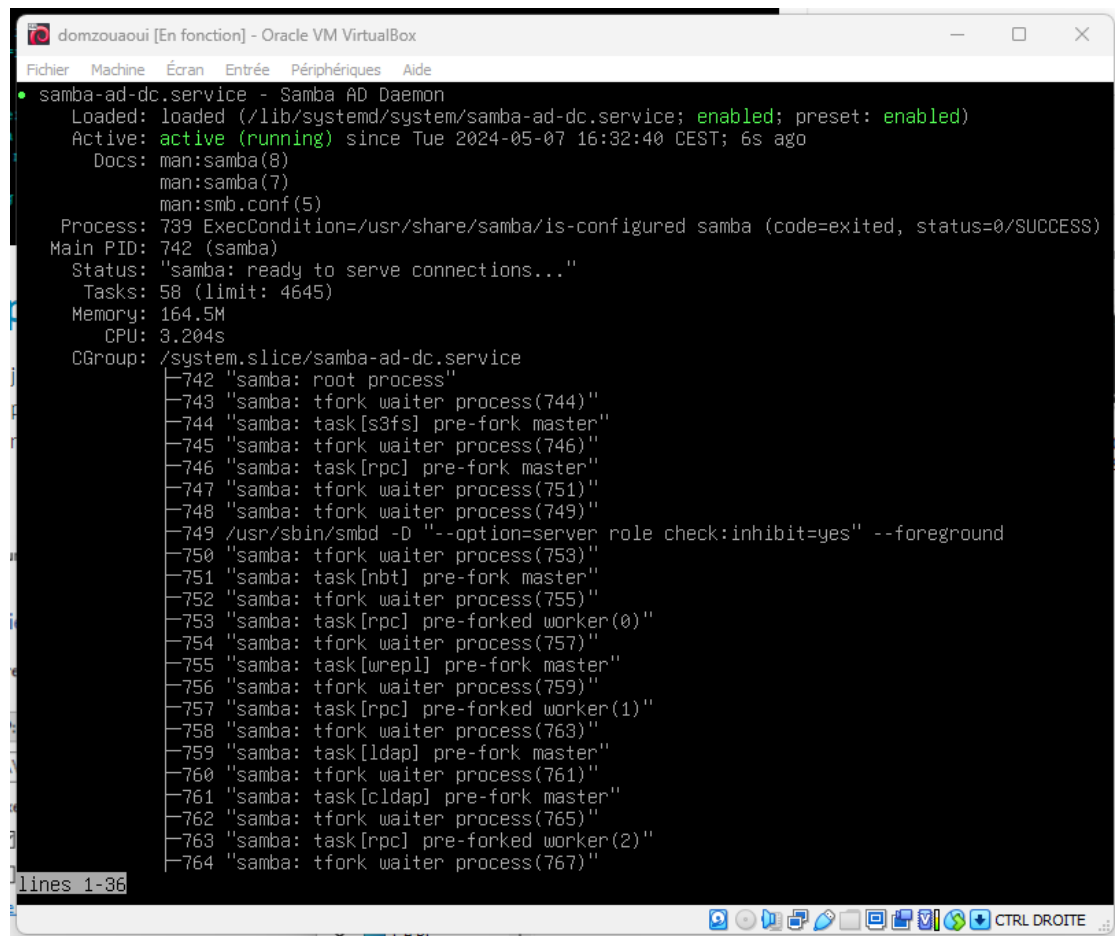
samba-tool domain provision --realm=MYDOMAIN.LAN --domain MYDOMAIN --server-role=dc

Ainsi, nous pouvons reboot la machine ou redémarrer le système à l'aide de la commande suivante :

systemctl restart samba-ad-dc = Redémarrer le système

Puis

systemctl status samba-ad-dc = Voir la status du système



```
domzouaoui [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
• samba-ad-dc.service - Samba AD Daemon
  Loaded: loaded (/lib/systemd/system/samba-ad-dc.service; enabled; preset: enabled)
  Active: active (running) since Tue 2024-05-07 16:32:40 CEST; 6s ago
    Docs: man:samba(8)
          man:samba(7)
          man:smb.conf(5)
  Process: 739 ExecCondition=/usr/share/samba/is-configured samba (code=exited, status=0/SUCCESS)
 Main PID: 742 (samba)
  Status: "samba: ready to serve connections..."
    Tasks: 58 (limit: 4645)
  Memory: 164.5M
    CPU: 3.204s
  CGroup: /system.slice/samba-ad-dc.service
          └─742 "samba: root process"
              └─743 "samba: tfork waiter process(744)"
                  └─744 "samba: task[s3fs] pre-fork master"
                      └─745 "samba: tfork waiter process(746)"
                          └─746 "samba: task[rpc] pre-fork master"
                              └─747 "samba: tfork waiter process(751)"
                                  └─748 "samba: tfork waiter process(749)"
                                      └─749 /usr/sbin/smbd -D "--option=server role check:inhibit=yes" --foreground
                                          └─750 "samba: tfork waiter process(753)"
                                              └─751 "samba: task[nbt] pre-fork master"
                                                  └─752 "samba: tfork waiter process(755)"
                                                      └─753 "samba: task[rpc] pre-forked worker(0)"
                                                          └─754 "samba: tfork waiter process(757)"
                                                              └─755 "samba: task[wrepl] pre-fork master"
                                                                  └─756 "samba: tfork waiter process(759)"
                                                                      └─757 "samba: task[rpc] pre-forked worker(1)"
                                                                          └─758 "samba: tfork waiter process(763)"
                                                                              └─759 "samba: task[ldap] pre-fork master"
                                                                                  └─760 "samba: tfork waiter process(761)"
                                                                                      └─761 "samba: task[cldap] pre-fork master"
                                                                                          └─762 "samba: tfork waiter process(765)"
                                                                                              └─763 "samba: task[rpc] pre-forked worker(2)"
                                                                                                  └─764 "samba: tfork waiter process(767)"
lines 1-36
```

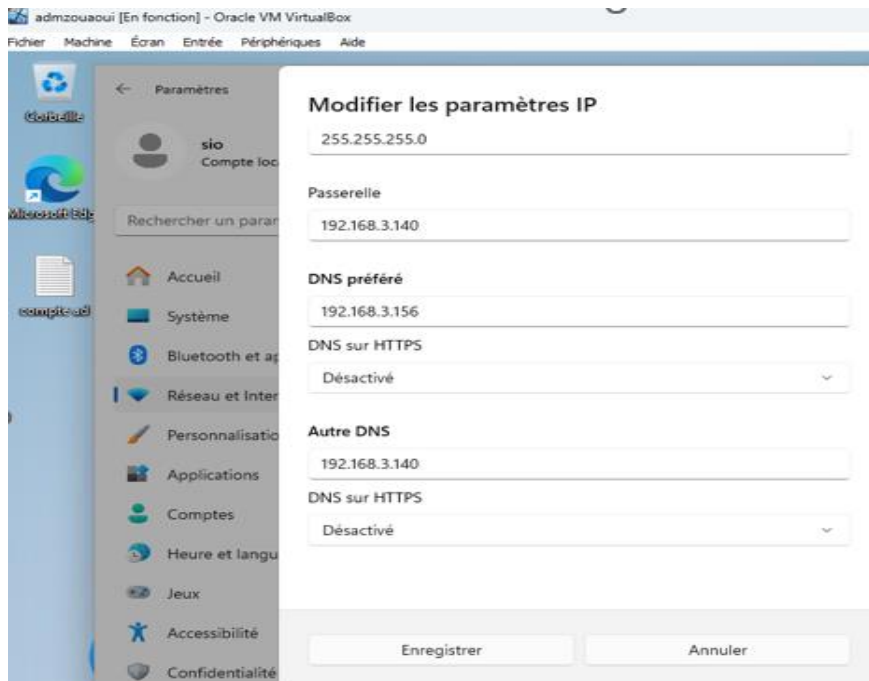
Une fois que SAMBA est bien active sans erreurs, lancez la machine WINDOWS 11 (admzouaoui) pour relié SAMBA AD.

Une fois la machine WINDOWS 11 (admzouaoui) lancée, testez la connexion avec les commandes suivantes dans le cmd :

ping 8.8.8.8

ping www.google.fr

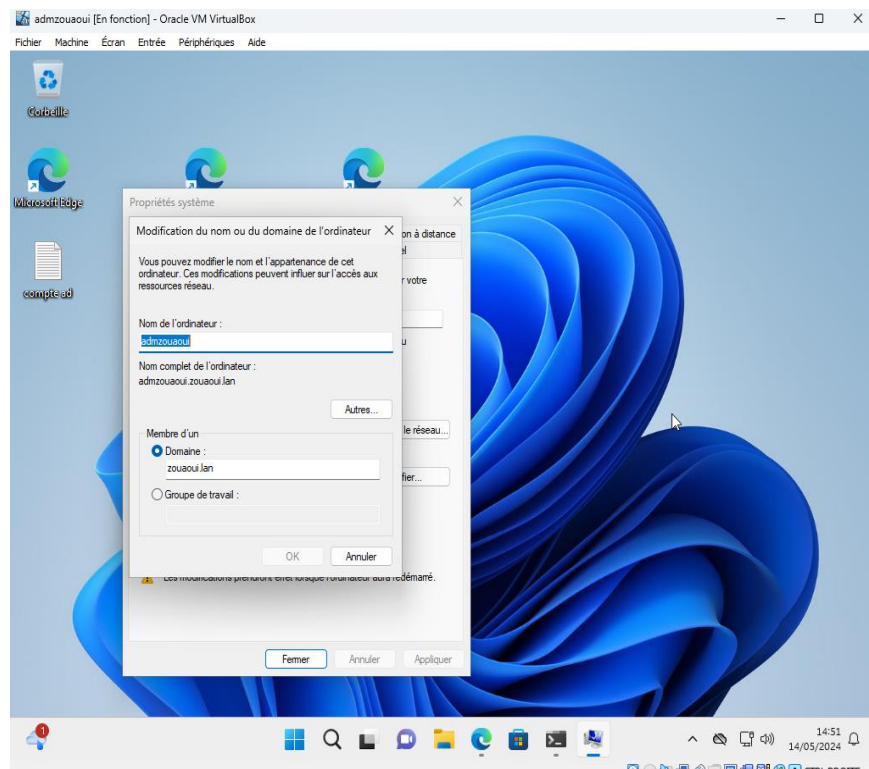
N'oubliez pas de bien configurer dans les paramètres de la machine WINDOWS 11 (DNS / IP) pour éviter des erreurs lors de la connexion du domaine.



Une fois bien configuré, nous allons dans :

Windows / Paramètres / Système / Information Système / Liens connexes / Domaine ou groupe de travail

Une fois arrivé ici, nous allons sélectionner le « Domaine » puis nous allons rentrer le nom du Domaine que nous avons mis sur la machine Debian.



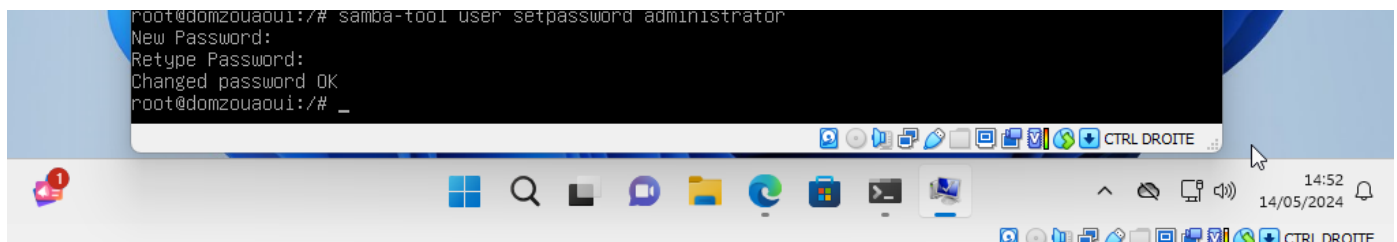
Une fois le bon nom de domaine entré, sur OK puis vous devez vous connecter avec :

Utilisateur : administrator

Mot de passe : 'mot de passe'

Pour définir votre mot de passe :

samba-tool user setpassword administrator



```
root@domzouaoui:/# samba-tool user setpassword administrator
New Password:
Retype Password:
Changed password OK
root@domzouaoui:/# _
```

The screenshot shows a terminal window with a black background and white text. The prompt is 'root@domzouaoui:/#'. The command 'samba-tool user setpassword administrator' has been entered. The output shows 'New Password:', 'Retype Password:', and 'Changed password OK'. The prompt returns to 'root@domzouaoui:/#'. Below the terminal window is a Windows taskbar with various icons and a system tray showing the time '14:52' and date '14/05/2024'.

Pour finir, nous nous connectons au domaine (Debian) depuis la machine Windows 11.