

TSSR - Compte rendu TP9 : Serveur Cockpit Sous Debian

Jean-Paul MELISSE

13 Février 2025

1 Introduction

L'objectif de ce TP est de nous familiariser un peu plus avec la distribution Linux. Pour ce faire, on va créer un serveur Cockpit sous Debian. Cockpit fournit une interface graphique intuitive via un navigateur web, permettant aux administrateurs de gérer plusieurs aspects du serveur sans avoir à utiliser uniquement la ligne de commande. On utilisera l'hyperviseur VirtualBox pour créer plusieurs machines virtuelles. Ce petit document va nous décrire les étapes à suivre.

2 Créer un dossier de travail

On choisit un emplacement de travail où on va garder tous les fichiers installés et la configuration des machines virtuelles. On décide de sauvegarder dans le chemin : "C:\Users\Jean-Paul\Desktop\tp9\", comme montre la Figure 1.

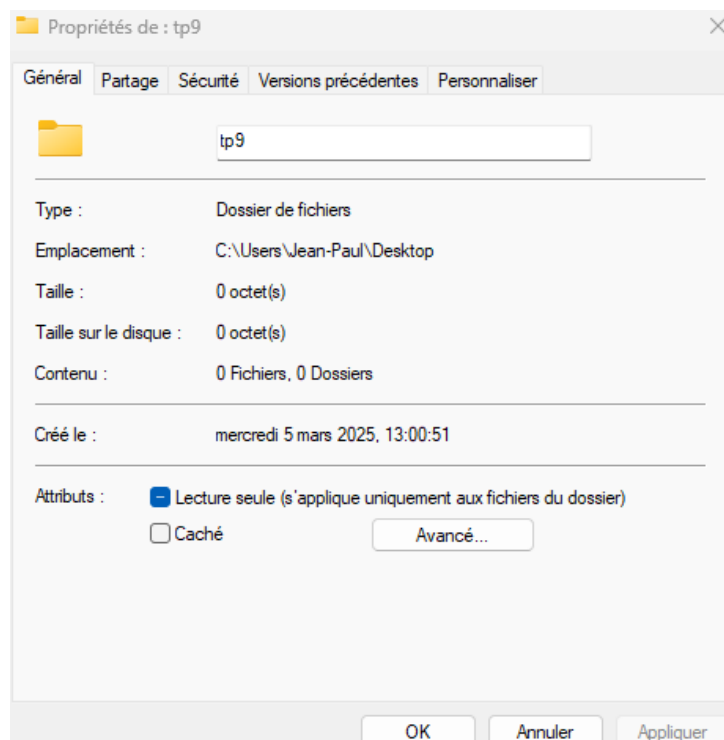


Figure 1

3 Télécharger Debian

La suite est de télécharger le système d'exploitation Debian. On y accède via le lien <https://www.debian.org/>. On clique sur "Téléchargement". On le sauvegarde dans le dossier tp9 sous le format .iso (Voir la Figure 2).

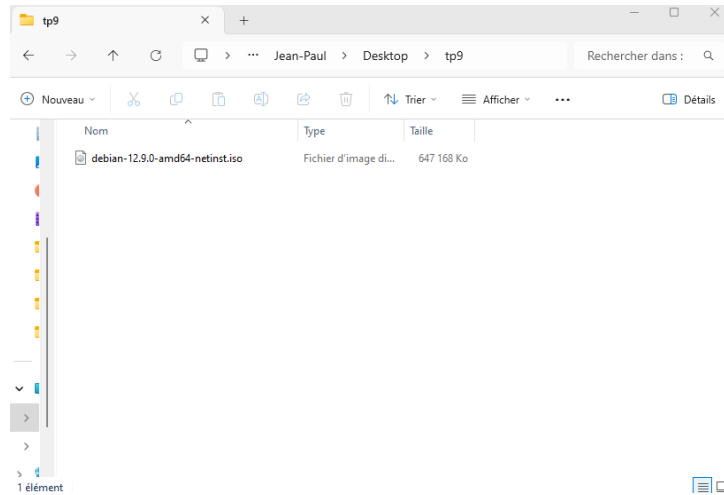


Figure 2

4 Créer la machine virtuelle tp9-router

On ouvre VirtualBox. On clique sur "Nouveau" pour créer une nouvelle machine virtuelle. On met "tp9-router" comme nom de la machine virtuelle. On choisit son emplacement de sauvegarde et on importe le CD contenant le système d'exploitation de Debian. En détectant le CD, le type "Linux", le subtype "Debian" et la version "Debian (64 bits)" sont automatiquement mis. On coche la case "Skip Unattended Installation" et on clique sur "Suivant". On lui donne une mémoire vive (RAM) de 2048 Mo et un processeur, et on clique sur "Suivant". On lui donne un disque dur de 20 Go et on clique sur "Suivant". On regarde bien le récapitulatif et on clique sur "Finish" (Voir la Figure 3).

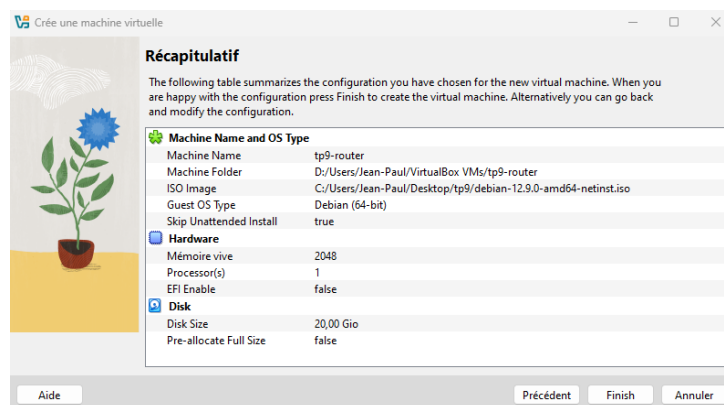


Figure 3

Maintenant que la nouvelle machine est créée, il faut la configurer. On clique sur "Configurations". On clique sur "Réseau" et sur l'interface "Adapter 1". On change le mode d'accès réseau à "Accès par pont", puis on clique sur "OK". Le mode "Accès par pont" va permettre à la machine virtuelle de récupérer une

adresse IP directement depuis un serveur DHCP (par exemple : notre box). Cela permet de connecter la machine virtuelle à l'Internet. On clique sur "Adapteur 2" et on coche la case "Activer l'interface réseau". Pour cette interface, on change le mode d'accès réseau à "Réseau interne". Maintenant qu'on a configuré la machine virtuelle, on clique sur "Démarrer" pour l'allumer.

5 Installer Debian sur tp9-router

Après avoir démarré la machine virtuelle, on choisit l'option "Graphical Install". On choisit la langue "English" et on clique sur "Continue". Le fait qu'on ait choisi l'anglais comme langue, Debian va nous proposer des pays anglophones par défaut pour la géolocalisation. On choisit donc "other" et on clique sur "Continue". Il nous propose donc dans un premier temps, des zones continentales. On choisit "Europe" pour la localisation car on se trouve en Europe et on clique sur "Continue". Enfin, on choisit "France" pour la localisation et on clique sur "Continue". Debian comprend qu'il y a une incohérence entre la langue choisie et le pays. Il nous propose différentes versions de la langue anglaise en fonction des pays. On choisit "United States - en_US.UTF-8" et on clique sur "Continue". Pour la configuration du clavier, on choisit "French" et on clique sur "Continue". Debian a détecté plusieurs interfaces réseau. On choisit l'interface "enp0s3" comme l'interface primaire et on clique sur "Continue". Après avoir reçu par le service DHCP une adresse IP, on renomme le nom de l'hôte (Hostname) en "tp9-router" et on clique sur "Continue" (Figure 4).



Figure 4

On lui donne un nom de domaine (Domain Name), qui sera "afpa" ici et on clique sur "Continue". On donne un mot de passe à l'administrateur root (dans ce cas ici, le mot de passe est "root" et on le met deux fois) et on clique sur "Continue". On crée un nouvel utilisateur qu'on nomme "user" et on clique sur "Continue" deux fois. Comme pour l'administrateur root, on donne un mot de passe à l'utilisateur user (dans ce cas ici, le mot de passe est "user" et on le met deux fois) et on clique sur "Continue".

On choisit l'option "Guide - use entire disk" pour la partition du disque et on clique sur "Continue" deux fois. Pour la partition, on choisit "All files in one partition" et on clique sur "Continue" deux fois. On

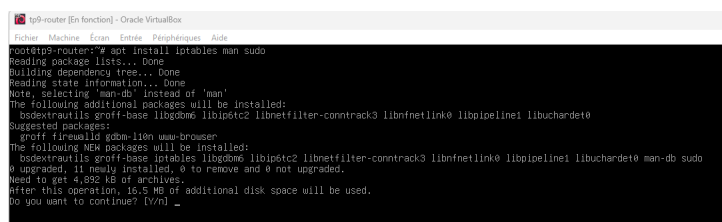
coche la case "Yes" pour appliquer les changements sur la partition du disque et on clique sur "Continue". Comme on a mis un seul disque dur pour cette machine virtuelle, on n'a pas besoin de scanner d'autres disques. On coche la case "No" et on clique sur "Continue".

La prochaine étape concerne le gestionnaire de paquets "Advanced Packaging Tool" (APT). Ce gestionnaire contient tous les programmes et applications utilisés pour les machines Debian et Ubuntu. Il gère aussi les mises à jour de ces applications. On choisit le pays "France" et on clique sur "Continue". On choisit le miroir pour le gestionnaire de paquets : "deb.debian.org" et on clique sur "Continue" deux fois. Ce qui signifie que quand on va utiliser le gestionnaire APT, il va se connecter à ce miroir pour vérifier ou installer les paquets. On coche la case "No" car on ne veut pas participer aux études statistiques et on clique sur "Continue".

On décoche toutes les cases des logiciels et on clique sur "Continue". On coche la case "Yes" pour installer le boot GRUB et on clique sur "Continue". On choisit l'option "/dev/sda" pour installer GRUB dans cet emplacement et on clique sur "Continue". On clique sur "Continue" pour finaliser l'installation de Debian et redémarrer la machine. Note : Après le redémarrage de Debian, on peut faire un clone de notre machine virtuelle.

6 Installer les paquets nécessaires sur tp9-router

Le but ici est d'installer les paquets nécessaires pour le bon fonctionnement de notre routeur. Après le redémarrage de notre machine virtuelle, on se connecte avec les identifiants de l'utilisateur root. On tape la commande : "apt install iptables iptables-save man sudo" pour installer le paquet manuel, la commande sudo, les paquets bind9, iptables et iptables-save qui sont essentiels pour configurer le pare-feu. [Attention : l'installation de iptables include iptables-save. Donc pas besoin de le mettre dans la commande] (Voir la Figure 5).



```
tp9-router [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
root@tp9-router:~# apt install iptables iptables-save man sudo
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'man-db' instead of 'man'
The following additional packages will be installed:
  libgdbm libp6tc2 libnetfilter-conntrack3 libnfnetlink0 libpipeline1 libuchardet0
Suggested packages:
  groff-base libgdbm-dev nano-browser
The following NEW packages will be installed:
  libgdbm libp6tc2 libnetfilter-conntrack3 libnfnetlink0 libpipeline1 libuchardet0 man-db sudo
0 upgraded, 11 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,692 kB of archives.
After this operation, 16.5 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure 5

7 Configurer sudo sur tp9-router

Le suite maintenant est de configurer la commande sudo afin qu'on puisse l'utiliser avec l'utilisateur user. Après avoir installé sudo, on va modifier le fichier sudoers pour ajouter l'utilisateur user dans les droits de permissions. On fait une copie du fichier sudoers en tapant la commande "cp /etc/sudoers /etc/sudoers.ori" pour éviter d'écraser le fichier original. Pour modifier ce fichier, on tape la commande : "nano /etc/sudoers". Dans ce fichier, on ajoute après la ligne du root la commande : "user ALL=(ALL:ALL) ALL". On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée" pour sauvegarder avec le même nom. On peut visualiser cette étape sur la Figure 6.

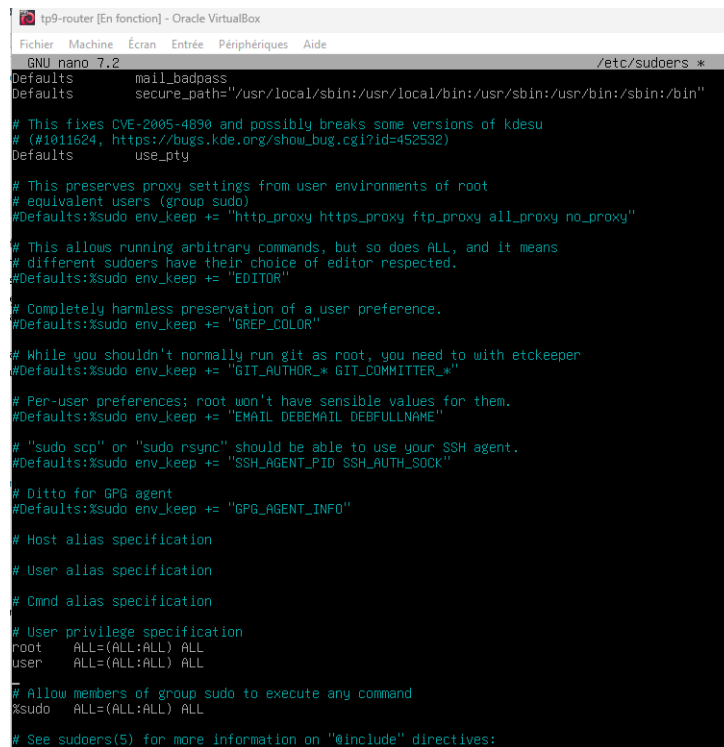
A screenshot of a terminal window titled "tp9-router [En fonction] - Oracle VirtualBox". The terminal shows the GNU nano 7.2 editor editing the file /etc/sudoers. The file content includes various defaults, host, user, and command specifications for the sudo command. Key lines include: Defaults: mail_badpass; Defaults: secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"; # This fixes CVE-2005-4890...; Defaults: use_pty; # This preserves proxy settings...; # This allows running arbitrary commands...; # Completely harmless preservation of a user preference...; # While you shouldn't normally run git as root...; # Per-user preferences...; # "sudo scp" or "sudo rsync" should be able to use your SSH agent...; # Ditto for GPG agent...; # Host alias specification; # User alias specification; # Cmnd alias specification; # User privilege specification; root ALL=(ALL:ALL) ALL; user ALL=(ALL:ALL) ALL; # Allow members of group sudo to execute any command; %sudo ALL=(ALL:ALL) ALL; # See sudoers(5) for more information on "@include" directives.

Figure 6

On a fini de configurer le fichier sudo. On peut se déconnecter du compte en utilisant la commande "logout".

8 Configurer le réseau sur tp9-router

On retourne sur la machine "tp9-router" et on se connecte en tant qu'utilisateur user. On crée une copie du fichier "interfaces" qui se trouve dans le chemin "/etc/network" avec la commande : "sudo cp /etc/network/interfaces /etc/network/interfaces.ori" pour ne pas écraser le fichier original. Par la suite, on va travailler sur le fichier "interfaces" pour configurer le réseau de notre Debian. On modifie le fichier en tapant la commande : "sudo nano /etc/network/interfaces". Dans ce fichier, on laisse l'interface enp0s3 en dhcp IPV4 et on donne une IP fixe à notre serveur et on ajoute une passerelle sur l'interface enp0s8 (Voir la Figure 7)

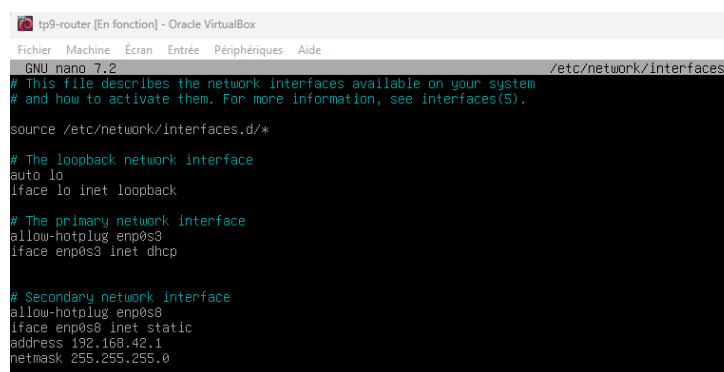
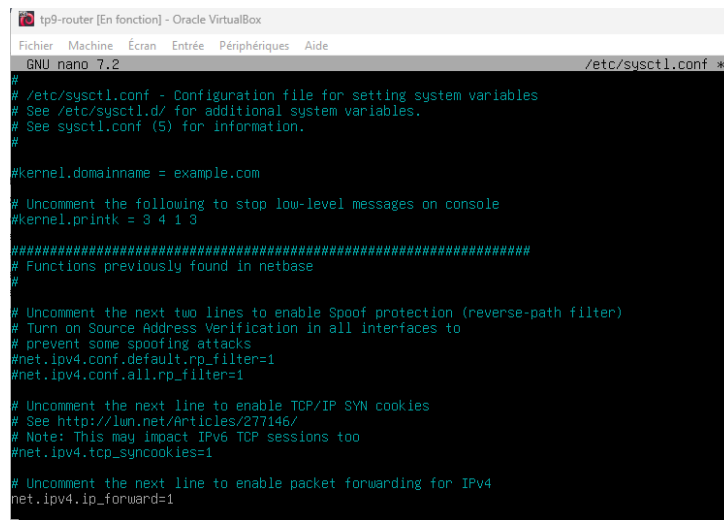
A screenshot of a terminal window titled "tp9-router [En fonction] - Oracle VirtualBox". The terminal shows the GNU nano 7.2 editor editing the file /etc/network/interfaces. The file content includes comments about network interfaces and configurations for loopback, primary, and secondary network interfaces. Key lines include: # 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 dhcp; # Secondary network interface; allow-hotplug enp0s8; iface enp0s8 inet static; address 192.168.42.1; netmask 255.255.255.0;

Figure 7

On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée". On redémarre

la configuration réseau de la machine en utilisant la commande "sudo systemctl restart networking". On vérifie si le service de configuration réseau marche correctement en tapant la commande "sudo systemctl status networking" et c'est bien le cas. On vérifie aussi avec la commande "sudo sysctl net.ipv4.ip_forward" que l'IP forwarding est désactivé et c'est bien le cas. On décide de l'activer en modifiant le fichier "sysctl.conf" qui se trouve dans le chemin "/etc/". On le copie d'abord avec la commande : "sudo cp /etc/sysctl.conf /etc/sysctl.conf.ori" pour éviter d'écraser le fichier original. On tape donc : "sudo nano /etc/sysctl.conf". On enlève le caractère "#" devant la ligne "net.ipv4.ip_foward=1" pour activer l'IP forwarding (Voir la Figure 8).



```

tp9-router [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 7.2 /etc/sysctl.conf *
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

```

Figure 8

On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée". On tape la commande "sudo sysctl -p" afin de prendre en compte les changements. On retape la commande "sudo sysctl net.ipv4.ip_forward" pour vérifier que maintenant l'IP forwarding est activé et c'est bien le cas. On va créer un fichier où on va stocker des règles de pare-feu pour notre serveur Cockpit. On tape la commande : "sudo nano iptables.sh" pour créer le fichier iptables.sh. Dans ce fichier, on ajoute les règles suivantes :

- 1 # delete rules and chains in the tables
- 2 iptables -F
- 3 iptables -X
- 4 iptables -t nat -F
- 5 iptables -t nat -X
- 6
- 7 # set the policy for the chains to the target
- 8 iptables -P INPUT DROP
- 9 iptables -P OUTPUT ACCEPT

```

10 iptables -P FORWARD ACCEPT
11
12 # add rules to the end of the chain
13 iptables -A INPUT -i lo -j ACCEPT
14 iptables -A INPUT -i enp0s8 -j ACCEPT
15 iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
16 iptables -t nat -A POSTROUTING -s 192.168.42.0/24 -j MASQUERADE

```

On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée". On applique les changements en tapant la commande : "sudo bash iptables.sh" [Attention : Si on redémarre le serveur tp9-router, il faut relancer cette commande]. On peut vérifier les règles et les chaînes du pare-feu dans la table "filter" en tapant la commande : "sudo iptables -L -v". On vérifie aussi la table "nat" en tapant la commande : "sudo iptables -t nat -L -v". On voit qu'il y a bien une entrée "POSTROUTING" venant des sources 192.168.42.0/24.

On va rendre les règles de pare-feu persistantes en tapant la commande : "sudo iptables-save | sudo tee /etc/iptables/rules.v4" [Attention : le dossier iptables doit être créé d'abord avec la commande : "sudo mkdir /etc/iptables"]. On redémarre la machine avec la commande "sudo reboot". Après le redémarrage de la machine, on se connecte avec les identifiants de l'utilisateur "user". On vérifie que les règles de pare-feu sont conservées en tapant les commandes : "sudo iptables -L -v" ou "sudo iptables -t nat -L -v" [Si ce n'est pas le cas, on recharge les règles avec la commande : "sudo iptables-restore -n < /etc/iptables/rules.v4"].

9 Créer la machine virtuelle tp9-server

On retourne sur VirtualBox. On clique sur "Nouveau" pour créer une nouvelle machine virtuelle. On met "tp9-server" comme nom de la machine virtuelle. On choisit son emplacement de sauvegarde et on importe le CD contenant le système d'exploitation de Debian. En détectant le CD, le type "Linux", le subtype "Debian" et la version "Debian (64 bits)" sont automatiquement mis. On coche la case "Skip Unattended Installation" et on clique sur "Suivant". On lui donne une mémoire vive (RAM) de 2048 Mo et un processeur, et on clique sur "Suivant". On lui donne un disque dur de 20 Go et on clique sur "Suivant". On regarde bien le récapitulatif et on clique sur "Finish" (Voir la Figure 9).

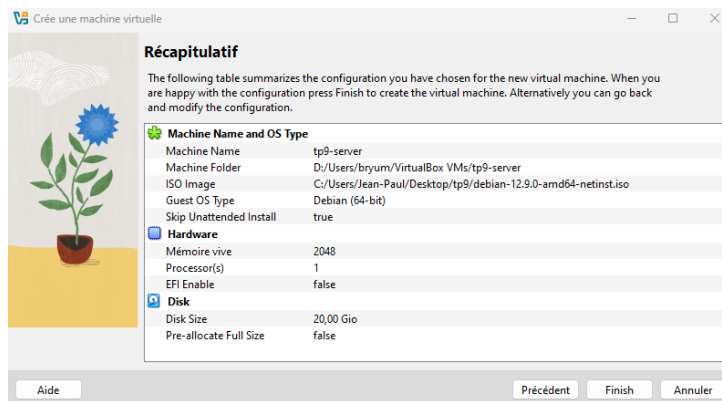


Figure 9

Maintenant que la nouvelle machine est créée, il faut la configurer. On clique sur "Configurations". On clique sur "Réseau" et sur l'interface "Adapter 1". On change le mode d'accès réseau à "Réseau interne". Maintenant qu'on a configuré la machine virtuelle, on clique sur "Démarrer" pour l'allumer.

10 Installer Debian sur tp9-server

Après avoir démarré la machine virtuelle, on choisit l'option "Graphical Install". On choisit la langue "English" et on clique sur "Continue". Le fait qu'on ait choisi l'anglais comme langue, Debian va nous proposer des pays anglophones par défaut pour la géolocalisation. On choisit donc "other" et on clique sur "Continue". Il nous propose donc dans un premier temps, des zones continentales. On choisit "Europe" pour la localisation car on se trouve en Europe et on clique sur "Continue". Enfin, on choisit "France" pour la localisation et on clique sur "Continue". Debian comprend qu'il y a une incohérence entre la langue choisie et le pays. Il nous propose différentes versions de la langue anglaise en fonction des pays. On choisit "United States - en_US.UTF-8" et on clique sur "Continue". Pour la configuration du clavier, on choisit "French" et on clique sur "Continue". Debian va essayer de se connecter via un serveur DHCP, mais n'arrive pas parce qu'il y a pas de serveur DHCP. On clique donc sur "Continue". On choisit l'option "Configure network manually" pour configurer manuellement le réseau, puis on clique sur "Continue". On met l'adresse IP "192.168.42.2/24" pour notre serveur et on clique sur "Continue". Pour la passerelle, on met l'adresse de notre routeur : "192.168.42.1" et on clique sur "Continue". Pour le serveur DNS, on met l'adresse IP du serveur DNS de Google, soit : "8.8.8.8" et on clique sur "Continue". On renomme le nom de l'hôte (Hostname) en "tp9-server" et on clique sur "Continue" (Figure 10).

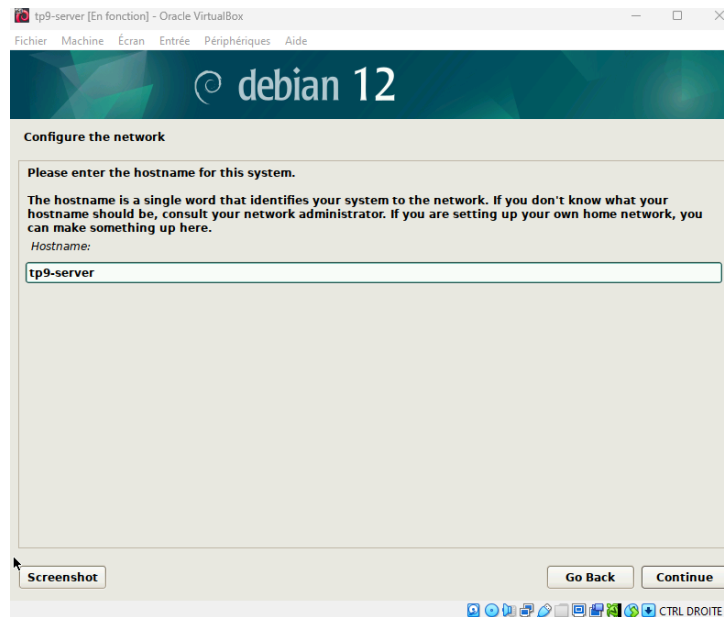


Figure 10

On lui donne un nom de domaine (Domain Name), qui sera "afpa" ici et on clique sur "Continue". On donne un mot de passe à l'administrateur root (dans ce cas ici, le mot de passe est "root" et on le met deux fois) et on clique sur "Continue". On crée un nouvel utilisateur qu'on nomme "user" et on clique sur "Continue" deux fois. Comme pour l'administrateur root, on donne un mot de passe à l'utilisateur user (dans ce cas ici, le mot de passe est "user" et on le met deux fois) et on clique sur "Continue".

On choisit l'option "Guide - use entire disk" pour la partition du disque et on clique sur "Continue" deux fois. Pour la partition, on choisit "All files in one partition" et on clique sur "Continue" deux fois. On coche la case "Yes" pour appliquer les changements sur la partition du disque et on clique sur "Continue". Comme on a mis un seul disque dur pour cette machine virtuelle, on n'a pas besoin de scanner d'autres disques. On coche la case "No" et on clique sur "Continue".

La prochaine étape concerne le gestionnaire de paquets "Advanced Packaging Tool" (APT). Ce gestionnaire contient tous les programmes et applications utilisés pour les machines Debian et Ubuntu. Il gère aussi les mises à jour de ces applications. On choisit le pays "France" et on clique sur "Continue". On choisit le miroir pour le gestionnaire de paquets : "deb.debian.org" et on clique sur "Continue" deux fois. Ce qui signifie que quand on va utiliser le gestionnaire APT, il va se connecter à ce miroir pour vérifier ou installer les paquets. On coche la case "No" car on ne veut pas participer aux études statistiques et on clique sur "Continue".

On décoche toutes les cases des logiciels et on clique sur "Continue". On coche la case "Yes" pour installer le boot GRUB et on clique sur "Continue". On choisit l'option "/dev/sda" pour installer GRUB dans cet emplacement et on clique sur "Continue". On clique sur "Continue" pour finaliser l'installation de Debian et redémarrer la machine. Note : Après le redémarrage de Debian, on peut faire un clone de notre machine virtuelle.

11 Installer les paquets nécessaires sur tp9-server

Le but ici est d'installer les paquets nécessaires pour le bon fonctionnement de notre serveur. Après le redémarrage de notre machine virtuelle, on se connecte avec les identifiants de l'utilisateur root. On tape la commande "apt install apache2 bind9 cockpit isc-dhcp-server man sudo" pour installer le paquet manuel, la commande sudo, le paquet apache2 qui est essentiel pour faire du serveur web, et les paquets bind9 et isc-dhcp-server pour les services DHCP et DNS. (Voir la Figure 11).

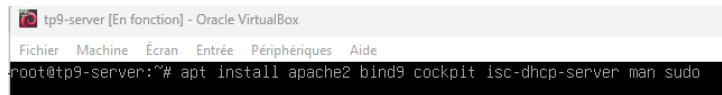


Figure 11

12 Configurer sudo sur tp9-server

La suite maintenant est de configurer la commande sudo afin qu'on puisse l'utiliser avec l'utilisateur user. Après avoir installé sudo, on va modifier le fichier sudoers pour ajouter l'utilisateur user dans les droits de permissions. On fait une copie du fichier sudoers en tapant la commande "cp /etc/sudoers /etc/sudoers.ori" pour éviter d'écraser le fichier original. Pour modifier ce fichier, on tape la commande : "nano /etc/sudoers". Dans ce fichier, on ajoute après la ligne du root la commande : "user ALL=(ALL:ALL) ALL". On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée" pour sauvegarder avec le même nom. On peut visualiser cette étape sur la Figure 12.

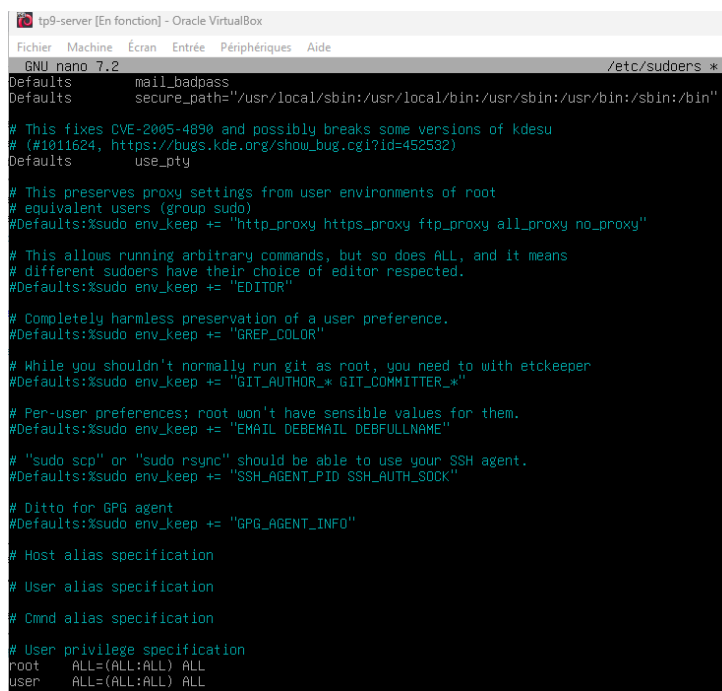
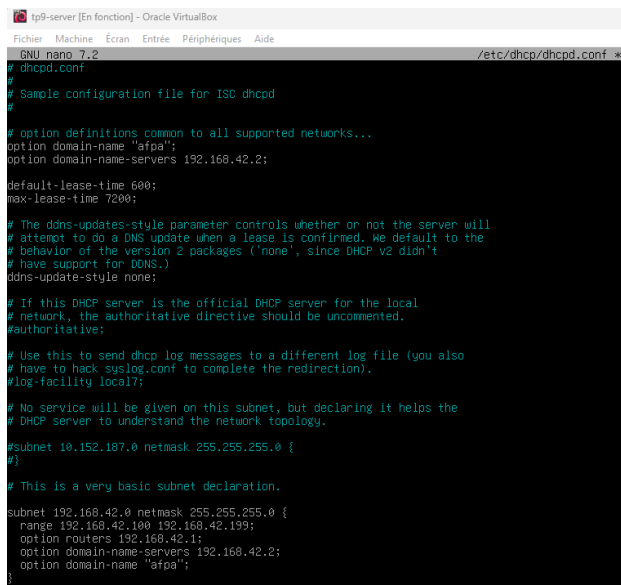


Figure 12

On a fini de configurer le fichier sudo. On peut se déconnecter du compte en utilisant la commande "logout".

13 Configurer les serveurs sur tp9-server

On retourne sur la machine "tp9-server" et on se connecte en tant qu'utilisateur user. Le but ici est de configurer le serveur DHCP. On copie le fichier dhcpd.conf afin de pouvoir modifier une copie pour ne pas écraser le fichier original en faisant la commande : "sudo cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.ori". On édite le fichier dhcpd.conf avec la commande : "sudo nano /etc/dhcp/dhcpd.conf". Dans ce fichier, on va ajouter le réseau 192.168.42.0, une nouvelle plage d'adresses (192.168.42.100 - 192.168.42.199) qui sera accessible pour les machines. On rajoute aussi une passerelle par défaut qui sera 192.168.42.1. On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée". Puis on va modifier le fichier isc-dhcp-server. On tape la commande : "sudo nano /etc/default/isc-dhcp-server." Dans ce fichier, on va spécifier notre interface réseau (ici c'est "enp0s3"). On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée". On peut voir les étapes précédentes sur les Figures 13 et 14.



```
GNU nano 7.2 /etc/dhcp/dhcpd.conf
# dhcpd.conf
# Sample configuration file for ISC dhcpd
#

# option definitions common to all supported networks...
option domain-name "afpa";
option domain-name-servers 192.168.42.2;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-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.)
ddns-update-style none;

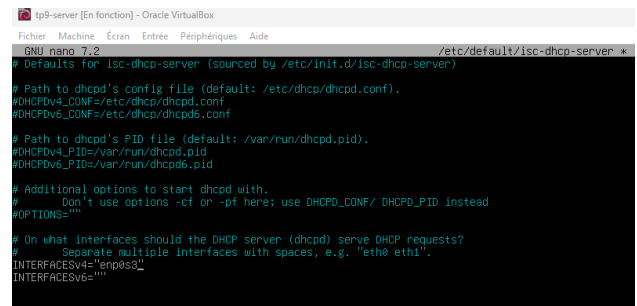
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
#authoritative;

# Use this to send dhcp log messages to a different log file (you also
# have to hack syslog.conf to complete the redirection).
#log-facility local7;

# No service will be given on this subnet, but declaring it helps the
# DHCP server to understand the network topology.
#subnet 10.152.187.0 netmask 255.255.255.0 {
#}

# This is a very basic subnet declaration.
subnet 192.168.42.0 netmask 255.255.255.0 {
    range 192.168.42.100 192.168.42.199;
    option routers 192.168.42.1;
    option domain-name-servers 192.168.42.2;
    option domain-name "afpa";
}
```

Figure 13



```
GNU nano 7.2 /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
DHCPD_CONF=/etc/dhcp/dhcpd.conf
DHCPD_OVS_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
DHCPD_PID=/var/run/dhcpd.pid
DHCPD_OVS_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
# Separate multiple interfaces with spaces, e.g. 'eth0 eth1'.
INTERFACESv6="enp0s3"
INTERFACES=""
```

Figure 14

Maintenant on va modifier le fichier configuration du paquet bind afin d'ajouter le serveur DNS de Google. On modifie le fichier en tapant la commande : "sudo nano /etc/bind/named.conf.options". Dans ce fichier, on ajoute "8.8.8.8" dans la partie "forwarder" afin d'ajouter le serveur DNS de Google comme "forwarder". On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée". On peut voir l'étape précédente sur la Figure 15.

```

tp9-server [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
GNU nano 7.2 /etc/bind/named.conf.options *
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        8.8.8.8;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    listen-on-v6 { any; };
};

```

Figure 15

Après avoir modifié le fichier de configuration du bind, il faut redémarrer le service DNS. Pour cela on tape : "sudo systemctl restart named". Puis, on va ajouter une nouvelle zone DNS dans notre serveur DNS. On tape la commande : "sudo nano /etc/bind/named.conf.local" pour éditer ce fichier. Dans ce fichier, on ajoute les commandes "zone" pour définir la zone qu'on veut créer. On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée". Ensuite, on va créer la base de données pour la zone "afpa". On tape la commande : "sudo nano /etc/bind/db.afpa" pour créer le fichier de configuration. Dans ce fichier, on ajoute les commandes pour configurer la zone "afpa" et créer les enregistrements du serveur principal de noms (ns1), du tp9-router et du tp9-server. On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée". On peut voir les étapes précédentes sur les Figures 16 et 17.

```

tp9-server [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
GNU nano 7.2 /etc/bind/named.conf.local *
//
// Do any local configuration here
//
zone "afpa" {
    type master;
    file "/etc/bind/db.afpa";
};

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

```

Figure 16

```

tp9-server [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
GNU nano 7.2 /etc/bind/db.afpa
; zone file for afpa
$TTL 86400
@ IN SOA ns1.afpa. hostmaster.afpa. (
    15 ; serial
    3600 ; refresh
    3600 ; retry
    604800 ; expire
    3600 ) ; minimum

@ In NS ns1.afpa.

ns1.afpa. IN A 192.168.42.2
tp9-router.afpa. IN A 192.168.42.1
tp9-server.afpa. IN A 192.168.42.2

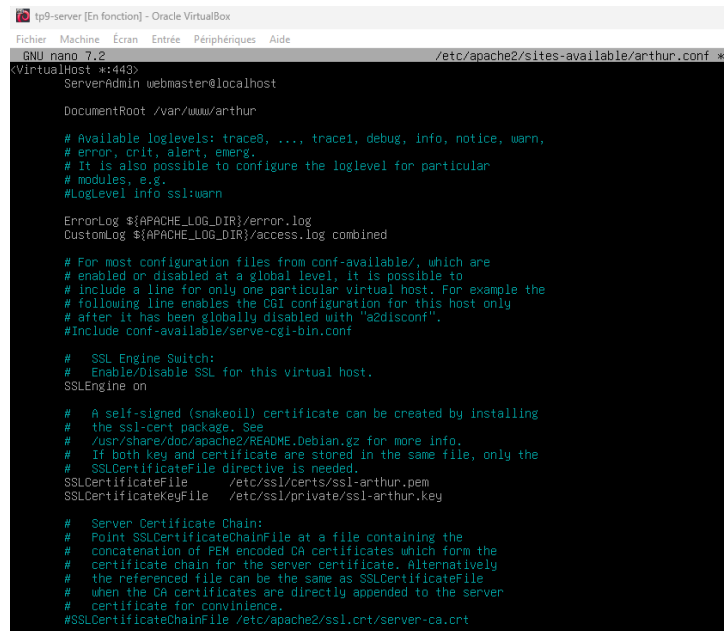
```

Figure 17

On peut vérifier si le fichier de configuration est bon en tapant la commande : "sudo named-checkconf" et "sudo named-checkzone afpa /etc/bind/db.afpa". Si tout est OK, on redémarre le service bind en tapant : "sudo service bind9 restart". On redémarre la configuration réseau de la machine en utilisant la commande "sudo systemctl restart networking". On vérifie si le service de configuration réseau marche correctement en tapant la commande "sudo systemctl status networking" et c'est bien le cas.

La prochaine étape est de créer une page web pour un utilisateur (ici Arthur) en HTTPs. Pour cela, on va utiliser les certificats SSL qui vont permettre de sécuriser la connexion vers le serveur. Sur la machine tp9-server, on va générer un certificat SSL et sa clé. Pour cela, on tape la commande "sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/ssl-arthur.key -out /etc/ssl/certs/ssl-arthur.pem". On va appuyer sur "Entrée" jusqu'à la fin du processus. On va ensuite copier le fichier default-ssl.conf qui se trouve dans le chemin "/etc/apache2/sites-available/" afin de pouvoir configurer le SSL sans écraser le fichier original. On tape "sudo cp /etc/apache2/sites-available/default-ssl.conf

/etc/apache2/sites-available/arthur.conf". On modifie le fichier arthur.conf en tapant la commande "sudo nano /etc/apache2/sites-available/arthur.conf". Dans ce fichier, on remplace la racine /var/www/html par /var/www/arthur et on indique le chemin vers le certificat SSL ainsi que sa clé. On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée" pour sauvegarder (Voir la Figure 18).



```

tp9-server [En fonction] - Oracle VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
GNU nano 7.2 /etc/apache2/sites-available/arthur.conf
<VirtualHost *:443>
ServerAdmin webmaster@localhost

DocumentRoot /var/www/arthur

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/ssl/certs/ssl-arthur.pem
SSLCertificateKeyFile /etc/ssl/private/ssl-arthur.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate. Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convenience.
#SSLCertificateChainFile /etc/apache2/ssl.crt/server-ca.crt
  
```

Figure 18

On va créer le dossier arthur dans le chemin /var/www avec la commande "sudo mkdir /var/www/arthur". On va ensuite créer le fichier index.html à l'intérieur de ce dossier. On tape la commande "sudo nano /var/www/arthur/index.html". Dans ce fichier, on écrit les commandes suivantes :

```

1 <!DOCTYPE html>

2 <html lang="en">

3     <head>

4         <title>Arthur's page</title>

5     </head>

6     <body>

7         <h1>Arthur</h1>

8         <p>Hello I am Arthur!</p>

9     </body>

10 </html>
  
```

On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée" pour sauvegarder. On tape la commande "sudo a2enmod ssl" pour activer le module ssl. Notre serveur est désormais prêt à être utilisé. Puis, on tape la commande "sudo a2ensite arthur" pour activer le site arthur.conf et on redémarre le serveur HTTP en tapant la commande : "sudo systemctl restart apache2".

14 Créer la machine virtuelle tp9-client

On retourne sur VirtualBox. On clique sur "Nouveau" pour créer une nouvelle machine virtuelle. On met "tp9-client" comme nom de la machine virtuelle. On choisit son emplacement de sauvegarde et on importe le CD contenant le système d'exploitation de Debian. En détectant le CD, le type "Linux", le subtype "Debian" et la version "Debian (64 bits)" sont automatiquement mis. On coche la case "Skip Unattended Installation" et on clique sur "Suivant". On lui donne une mémoire vive (RAM) de 2048 Mo et un processeur, et on clique sur "Suivant". On lui donne un disque dur de 20 Go et on clique sur "Suivant". On regarde bien le récapitulatif et on clique sur "Finish" (Voir la Figure 19).

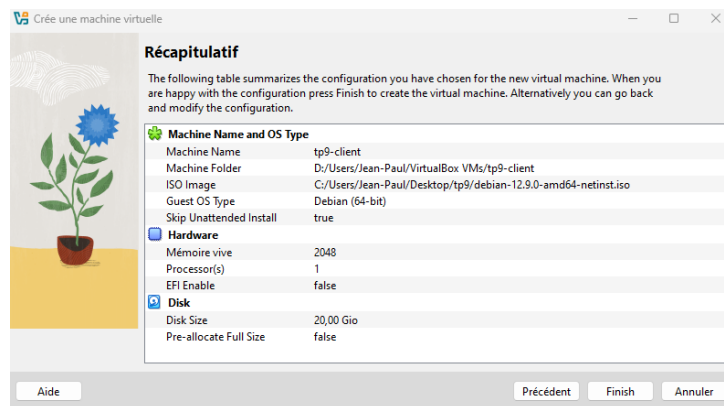


Figure 19

Maintenant que la nouvelle machine est créée, il faut la configurer. On clique sur "Configurations". On clique sur "Réseau" et sur l'interface "Adapter 1". On change le mode d'accès réseau à "Réseau interne". Maintenant qu'on a configuré la machine virtuelle, on clique sur "Démarrer" pour l'allumer.

15 Installer Debian sur tp9-client

Après avoir démarré la machine virtuelle, on choisit l'option "Graphical Install". On choisit la langue "English" et on clique sur "Continue". Le fait qu'on ait choisi l'anglais comme langue, Debian va nous proposer des pays anglophones par défaut pour la géolocalisation. On choisit donc "other" et on clique sur "Continue". Il nous propose donc dans un premier temps, des zones continentales. On choisit "Europe" pour la localisation car on se trouve en Europe et on clique sur "Continue". Enfin, on choisit "France" pour la localisation et on clique sur "Continue". Debian comprend qu'il y a une incohérence entre la langue choisie et le pays. Il nous propose différentes versions de la langue anglaise en fonction des pays. On choisit "United States - en_US.UTF-8" et on clique sur "Continue". Pour la configuration du clavier, on choisit "French" et on clique sur "Continue". Après avoir reçu par le service DHCP une adresse IP, on renomme le nom de l'hôte (Hostname) en "tp9-client" et on clique sur "Continue" (Figure 20).

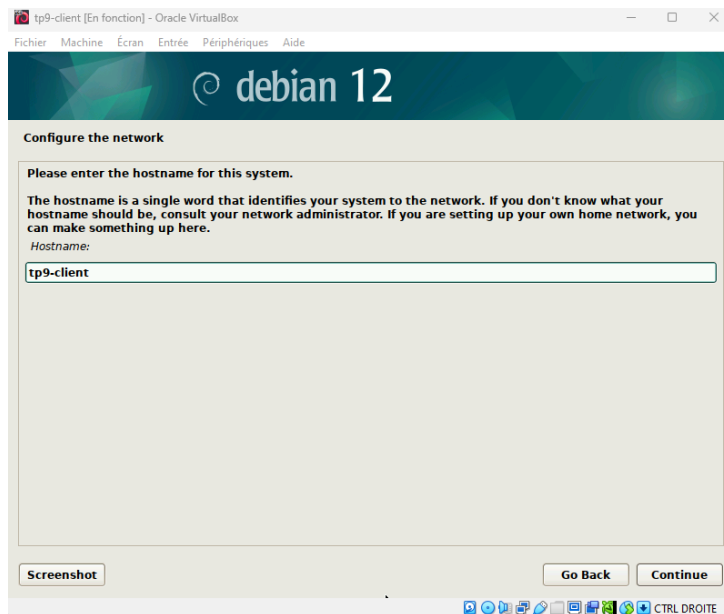


Figure 20

On lui donne un nom de domaine (Domain Name), qui sera "afpa" ici et on clique sur "Continue". On donne un mot de passe à l'administrateur root (dans ce cas ici, le mot de passe est "root" et on le met deux fois) et on clique sur "Continue". On crée un nouvel utilisateur qu'on nomme "user" et on clique sur "Continue" deux fois. Comme pour l'administrateur root, on donne un mot de passe à l'utilisateur user (dans ce cas ici, le mot de passe est "user" et on le met deux fois) et on clique sur "Continue".

On choisit l'option "Guide - use entire disk" pour la partition du disque et on clique sur "Continue" deux fois. Pour la partition, on choisit "All files in one partition" et on clique sur "Continue" deux fois. On coche la case "Yes" pour appliquer les changements sur la partition du disque et on clique sur "Continue". Comme on a mis un seul disque dur pour cette machine virtuelle, on n'a pas besoin de scanner d'autres disques. On coche la case "No" et on clique sur "Continue".

La prochaine étape concerne le gestionnaire de paquets "Advanced Packaging Tool" (APT). Ce gestionnaire contient tous les programmes et applications utilisés pour les machines Debian et Ubuntu. Il gère aussi les mises à jour de ces applications. On choisit le pays "France" et on clique sur "Continue". On choisit le miroir pour le gestionnaire de paquets : "deb.debian.org" et on clique sur "Continue" deux fois. Ce qui signifie que quand on va utiliser le gestionnaire APT, il va se connecter à ce miroir pour vérifier ou installer les paquets. On coche la case "No" car on ne veut pas participer aux études statistiques et on clique sur "Continue".

On coche les logiciels "Debian desktop environment, ... GNOME et standard system utilities" et on clique sur "Continue". On coche la case "Yes" pour installer le boot GRUB et on clique sur "Continue". On choisit l'option "/dev/sda" pour installer GRUB dans cet emplacement et on clique sur "Continue". On clique sur "Continue" pour finaliser l'installation de Debian et redémarrer la machine. Note : Après le redémarrage de Debian, on peut faire un clone de notre machine virtuelle.

16 Tester le serveur DHCP

Après le redémarrage de notre machine "tp9-client", on se connecte avec les identifiants de l'utilisateur "user". On choisit "English" pour la langue et "French" pour le clavier. On décoche la case "Location Services" et on clique sur "Next", puis "Skip". Enfin, on clique sur "Start Using Debian GNU/Linux". On ouvre un terminal : On clique sur "Activities" et on tape "Terminal" sur la barre de recherche. On tape la commande : "ip a" pour vérifier si on a bien eu une adresse IP venant de notre serveur DHCP, et c'est bien le cas (Voir la Figure 21). On tape ensuite la commande : "ip r" pour voir l'adresse IP de la passerelle par défaut et on voit, comme dans la Figure 22, qu'on a bien récupéré la bonne adresse IP de notre router "tp9-router" comme passerelle.

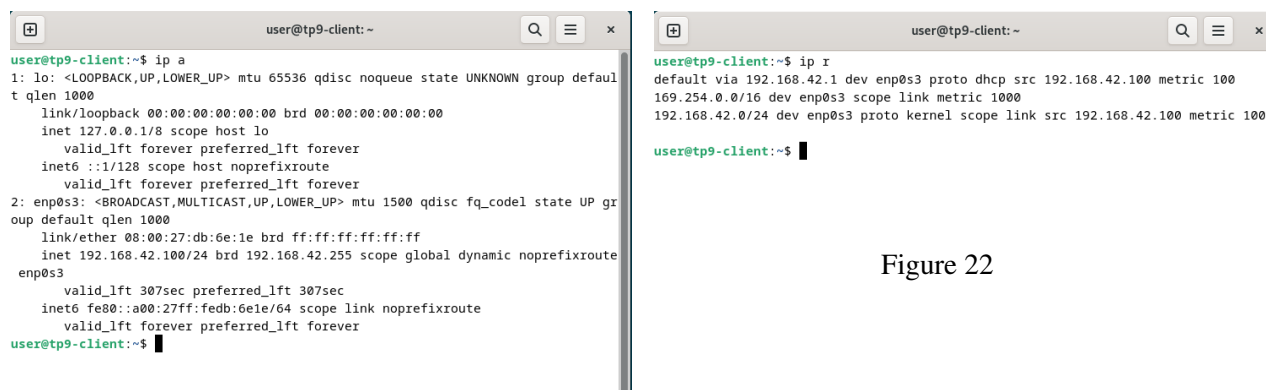


Figure 21

La suite est de vérifier si on a récupéré la bonne adresse IP du serveur DNS via le serveur DHCP. Pour cela, on tape la commande : "cat /etc/resolv.conf" et on constate que c'est bien le cas (cf : Figure 23).

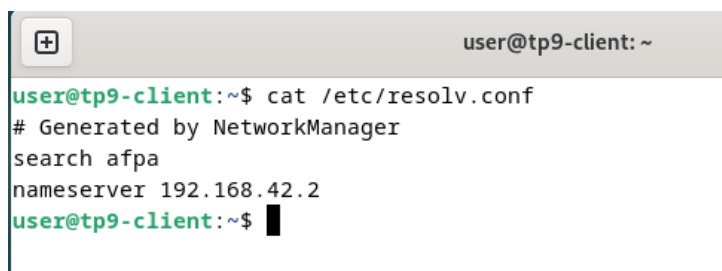
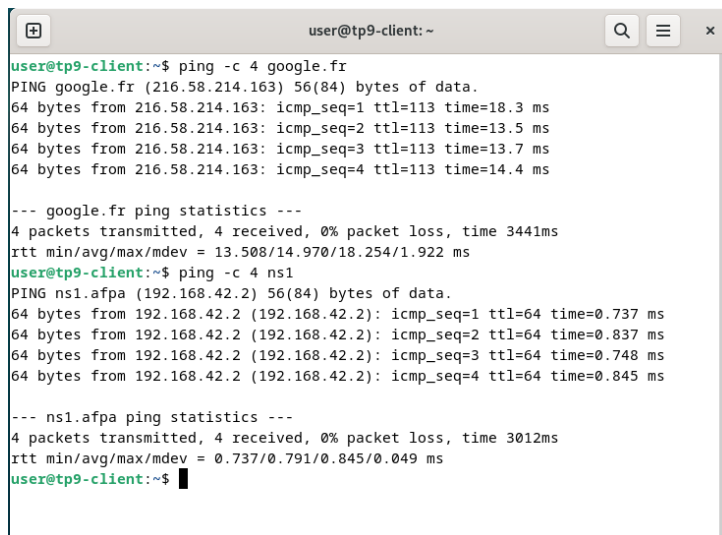


Figure 23

17 Tester le serveur DNS

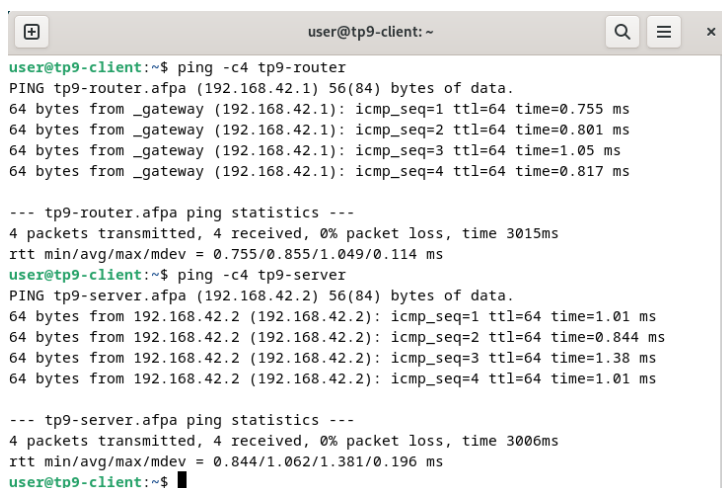
La prochaine étape est de vérifier si le serveur DNS fonctionne. Sur le terminal de la machine "tp9-client", on tape la commande : "ping google.fr". On voit bien que le forwarder DNS fonctionne correctement. On fait de même avec l'enregistrement en tapant la commande : "ping ns1" et on constate que ça marche aussi. On peut voir les étapes précédentes sur la Figure 24.



```
user@tp9-client: ~  
user@tp9-client:~$ ping -c 4 google.fr  
PING google.fr (216.58.214.163) 56(84) bytes of data.  
64 bytes from 216.58.214.163: icmp_seq=1 ttl=113 time=18.3 ms  
64 bytes from 216.58.214.163: icmp_seq=2 ttl=113 time=13.5 ms  
64 bytes from 216.58.214.163: icmp_seq=3 ttl=113 time=13.7 ms  
64 bytes from 216.58.214.163: icmp_seq=4 ttl=113 time=14.4 ms  
  
--- google.fr ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3441ms  
rtt min/avg/max/mdev = 13.508/14.970/18.254/1.922 ms  
user@tp9-client:~$ ping -c 4 ns1  
PING ns1.afpa (192.168.42.2) 56(84) bytes of data.  
64 bytes from 192.168.42.2 (192.168.42.2): icmp_seq=1 ttl=64 time=0.737 ms  
64 bytes from 192.168.42.2 (192.168.42.2): icmp_seq=2 ttl=64 time=0.837 ms  
64 bytes from 192.168.42.2 (192.168.42.2): icmp_seq=3 ttl=64 time=0.748 ms  
64 bytes from 192.168.42.2 (192.168.42.2): icmp_seq=4 ttl=64 time=0.845 ms  
  
--- ns1.afpa ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3012ms  
rtt min/avg/max/mdev = 0.737/0.791/0.845/0.049 ms  
user@tp9-client:~$
```

Figure 24

On va vérifier maintenant les enregistrements des adresses IP du serveur et du routeur par le serveur DNS. On tape la commande : "ping tp9-router" pour voir si on peut interagir avec la machine "tp9-router" et c'est bien le cas. On fait de même avec la machine "tp9-server" en tapant la commande : "ping tp9-server" et on constate la même chose. On peut voir les étapes précédentes sur la Figure 25.



```
user@tp9-client: ~  
user@tp9-client:~$ ping -c 4 tp9-router  
PING tp9-router.afpa (192.168.42.1) 56(84) bytes of data.  
64 bytes from _gateway (192.168.42.1): icmp_seq=1 ttl=64 time=0.755 ms  
64 bytes from _gateway (192.168.42.1): icmp_seq=2 ttl=64 time=0.801 ms  
64 bytes from _gateway (192.168.42.1): icmp_seq=3 ttl=64 time=1.05 ms  
64 bytes from _gateway (192.168.42.1): icmp_seq=4 ttl=64 time=0.817 ms  
  
--- tp9-router.afpa ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3015ms  
rtt min/avg/max/mdev = 0.755/0.855/1.049/0.114 ms  
user@tp9-client:~$ ping -c 4 tp9-server  
PING tp9-server.afpa (192.168.42.2) 56(84) bytes of data.  
64 bytes from 192.168.42.2 (192.168.42.2): icmp_seq=1 ttl=64 time=1.01 ms  
64 bytes from 192.168.42.2 (192.168.42.2): icmp_seq=2 ttl=64 time=0.844 ms  
64 bytes from 192.168.42.2 (192.168.42.2): icmp_seq=3 ttl=64 time=1.38 ms  
64 bytes from 192.168.42.2 (192.168.42.2): icmp_seq=4 ttl=64 time=1.01 ms  
  
--- tp9-server.afpa ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3006ms  
rtt min/avg/max/mdev = 0.844/1.062/1.381/0.196 ms  
user@tp9-client:~$
```

Figure 25

18 Tester le serveur HTTP

L'étape suivante est de tester le serveur HTTP. Sur la machine "tp9-client", on ouvre le navigateur Firefox: on clique sur "Activities" et on clique sur "Firefox". Sur Firefox, on entre le lien `https://tp9-server.afpa/` sur la barre de recherche et on appuie sur "Entrée". On voit qu'on arrive sur une page d'alerte de sécurité SSL. Cette alerte est due au certificat SSL qui est autosigné. On clique sur "Advanced" et sur "Accept the Risk and Continue" pour accéder au site et on tombe sur le site `arthur.conf`. On voit sur la Figure 26 qu'on a accès à la page web.

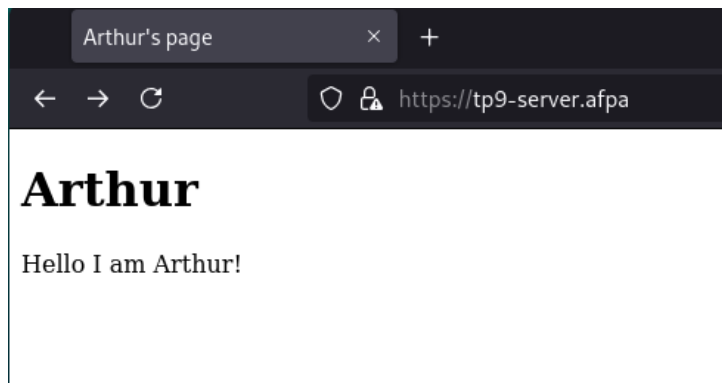


Figure 26

19 Tester le serveur Cockpit

La prochaine étape est de tester le serveur Cockpit. Sur la machine "tp9-client", on ouvre le navigateur Firefox et sur la barre de recherche on entre le lien : `https://tp9-server.afpa:9090` et on appuie sur "Entrée". On voit qu'on arrive à nouveau sur une page d'alerte de sécurité SSL. On clique sur "Advanced" et sur "Accept the Risk and Continue" pour accéder au site. On arrive sur une page de connexion comme montre la Figure 27.

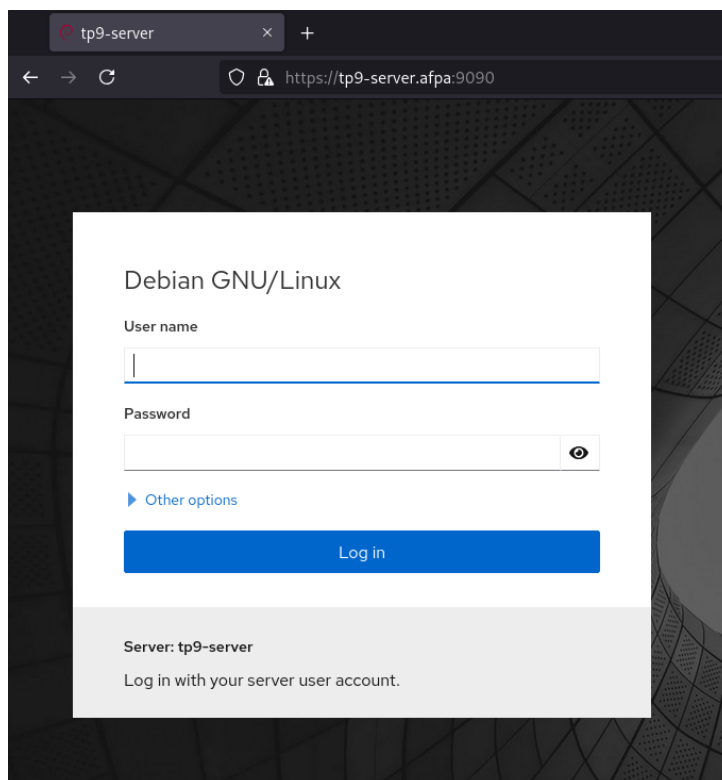


Figure 27

On met "user" comme nom d'utilisateur et mot de passe, et on clique sur "Log in". Après s'être connecté, on clique sur "Turn on administrative access" pour activer le mode administrateur sur le site.

20 Créer des utilisateurs avec Cockpit

Dans cette partie du TP, on va utiliser Cockpit sur la machine "tp9-client" pour créer et gérer des comptes sur le serveur "tp9-server". Sur le site <https://tp9-server.afpa:9090>, on clique sur l'onglet "Accounts", et on clique sur "Create new account" pour ajouter un nouvel utilisateur. On crée 3 nouveaux utilisateurs : arthur, jules et louis.

Pour Arthur : On met "Arthur" pour le nom complet, "arthur" pour le username et "arthur1234" pour le mot de passe (2x). Puis on clique sur "Create".

Pour Jules : On met "Jules" pour le nom complet, "jules" pour le username et "jules1234" pour le mot de passe (2x). Puis on clique sur "Create".

Pour Louis : "On met "Louis" pour le nom complet, "louis" pour le username et "louis1234" pour le mot de passe (2x). Puis on clique sur "Create".

On peut voir les étapes précédentes sur la Figure 28.

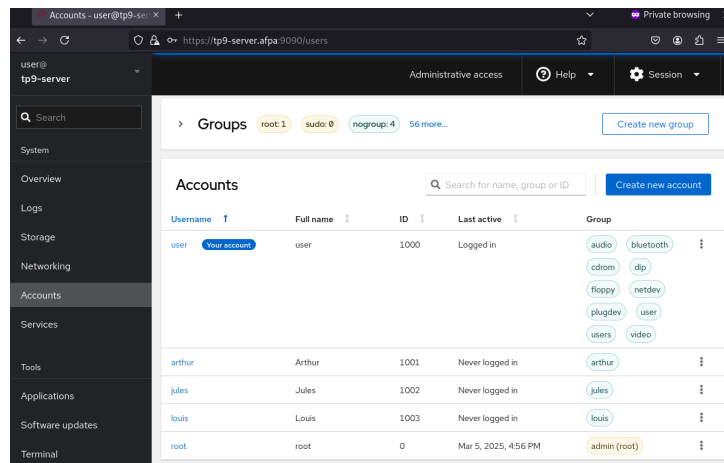


Figure 28

21 Tester les utilisateurs créés

On retourne sur la machine "tp9-server" et on va vérifier si les utilisateurs sont créés sur le serveur. Pour cela, on tape la commande : "cat /etc/passwd". On voit, comme sur la Figure 29, que les utilisateurs Arthur, Jules et Louis sont créés sur le serveur.

```

tp9-server [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide

user@tp9-server:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
messagebus:x:100:107:/:/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:108:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
user:x:1000:1000:user,,,:/home/user:/bin/bash
Debian-exim:x:102:110:/:/var/spool/exim4:/usr/sbin/nologin
bind:x:103:112:/:/var/cache/bind:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
cockpit-ws:x:104:113:/:/nonexistent:/usr/sbin/nologin
cockpit-wsinstance:x:105:114:/:/nonexistent:/usr/sbin/nologin
polkitd:x:997:997:polkit:/nonexistent:/usr/sbin/nologin
arthur:x:1001:1001:Arthur:/home/arthur:/bin/sh
jules:x:1002:1002:Jules:/home/jules:/bin/sh
louis:x:1003:1003:Louis:/home/louis:/bin/sh
user@tp9-server:~$ _

```

Figure 29

La suite est de se connecter sur les 3 comptes utilisateurs. On tape la commande : "logout" pour se déconnecter du compte "user". On se connecte avec les identifiants de l'utilisateur "arthur". Puis, on tape la commande : "pwd" pour voir qu'on est bien sur le dossier personnel d'Arthur (/home/arthur). Enfin, on tape la commande : "exit" pour se déconnecter du compte Arthur. On répète les étapes précédentes pour les utilisateurs Jules et Louis.

22 Supprimer des utilisateurs avec Cockpit

Cette fois-ci, on va supprimer des utilisateurs sur Cockpit. On retourne sur la machine "tp9-client". Sur le site <https://tp9-server.afpa:9090>, on clique sur l'onglet "Accounts", et sur le username "arthur". Sur la page "Arthur", on clique sur "Delete" pour supprimer le compte "Arthur". On coche la case "Delete files" et on clique sur "Delete" pour supprimer le compte "Arthur" ainsi que ses fichiers. On fait de même pour les comptes Jules et Louis. On voit sur la Figure 30, que les 3 utilisateurs sont bien supprimés.

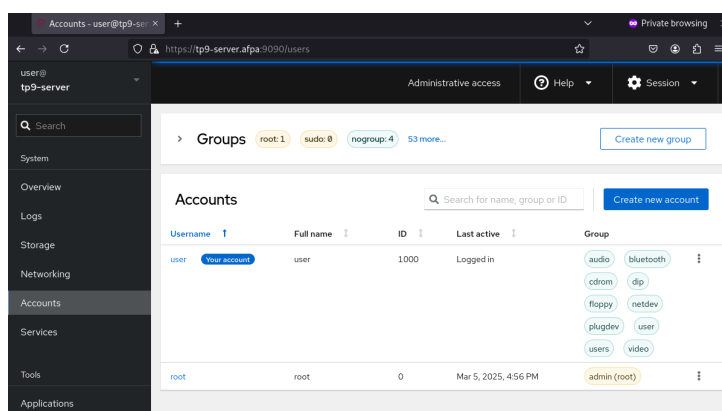
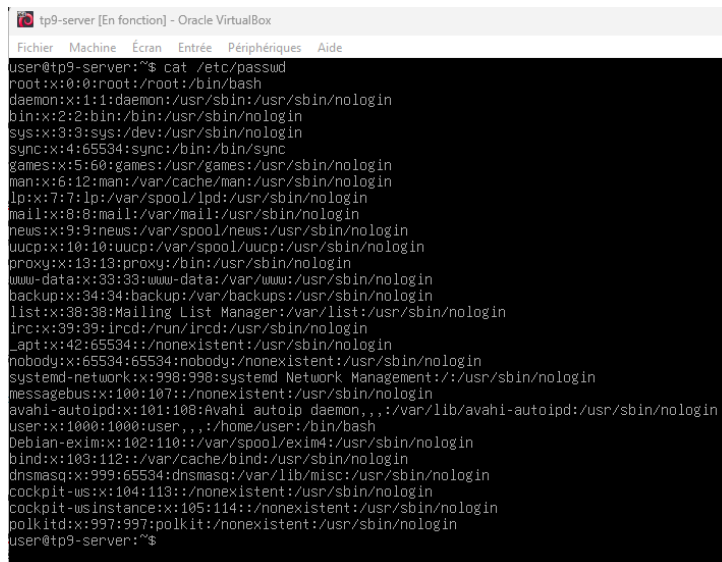


Figure 30

23 Tester les utilisateurs supprimés

On retourne sur la machine "tp9-server" et on se connecte avec les identifiants de l'utilisateur "user". On va vérifier si les utilisateurs sont supprimés sur le serveur. Pour cela, on tape la commande : "cat /etc/passwd". On voit, comme sur la Figure 31, que les utilisateurs Arthur, Jules et Louis ont été supprimés sur le serveur.



```
user@tp9-server:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
messagebus:x:100:107:/:/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:108:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
user:x:1000:1000:user,,:/home/user:/bin/bash
Debian-exim:x:102:110:/:/var/spool/exim4:/usr/sbin/nologin
bind:x:103:112:/:/var/cache/bind:/usr/sbin/nologin
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
cockpit-ws:x:104:113:/:/nonexistent:/usr/sbin/nologin
cockpit-wsinstance:x:105:114:/:/nonexistent:/usr/sbin/nologin
polkitd:x:997:997:polkit:/nonexistent:/usr/sbin/nologin
user@tp9-server:~$
```

Figure 31

On tape la commande : "logout" pour se déconnecter du compte "user". On va essayer de se connecter sur les 3 comptes supprimés. On se connecte avec les identifiants de l'utilisateur "arthur" et on n'arrive pas (on a un "Login incorrect"). On fait de même pour les utilisateurs Jules et Louis et on constate la même erreur.

24 Stopper un service avec Cockpit

Cette fois-ci, on va arrêter un service de la machine "tp9-server" avec Cockpit. On retourne sur la machine "tp9-client" et sur le site <https://tp9-server.afpa:9090>. On clique sur l'onglet "Services" et sur "apache2". Puis on clique sur "Stop and disable" pour arrêter et désactiver le service apache2, comme montre la Figure 32.

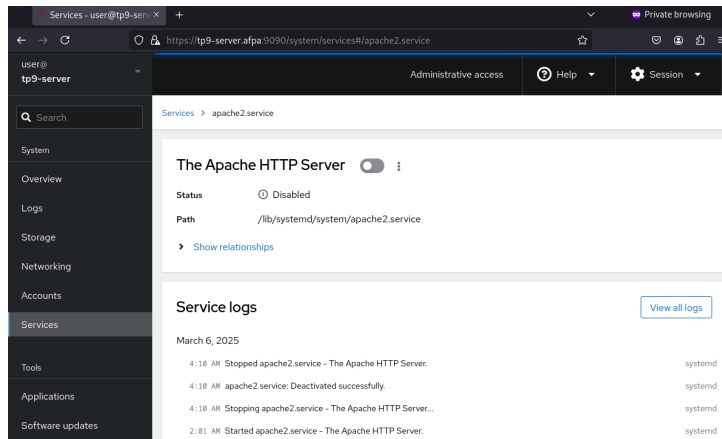


Figure 32

25 Tester le service arrêté

On ouvre le navigateur Firefox et on essaie d'accéder à la page web d'Arthur en tapant le lien `https://tp9-server.afpa/` sur la barre de recherche. On voit, comme sur la Figure 33, qu'on n'a plus accès à la page web d'Arthur.

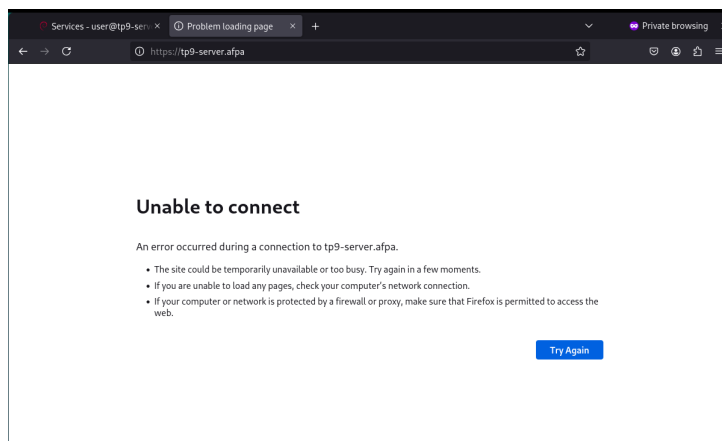


Figure 33

26 Démarrer un service avec Cockpit

Maintenant, on va redémarrer le service "apache2" avec Cockpit. On retourne sur la machine "tp9-client" et sur le site `https://tp9-server.afpa:9090`. On clique sur l'onglet "Services" et sur "apache2". Puis on clique sur "Start and enable" pour démarrer et activer le service apache2, comme montre la Figure 34.

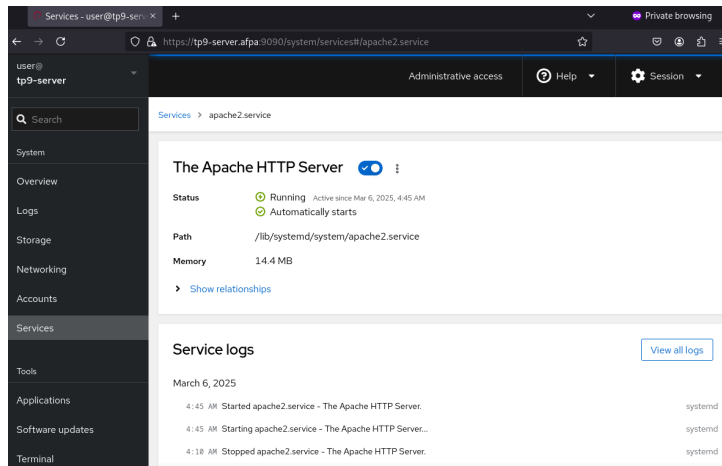


Figure 34

27 Tester le service démarré

On ouvre le navigateur Firefox et on essaie d'accéder à la page web d'Arthur en tapant le lien `https://tp9-server.afpa/` sur la barre de recherche. On voit, comme sur la Figure 35, que cette fois-ci, on a bien accès à la page web d'Arthur.

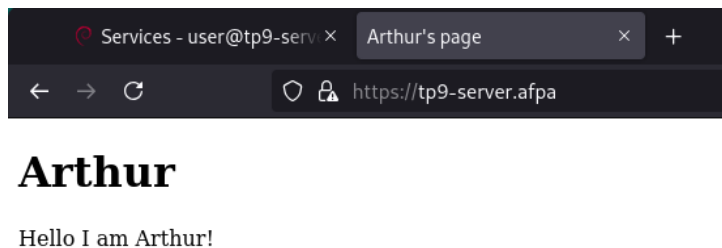
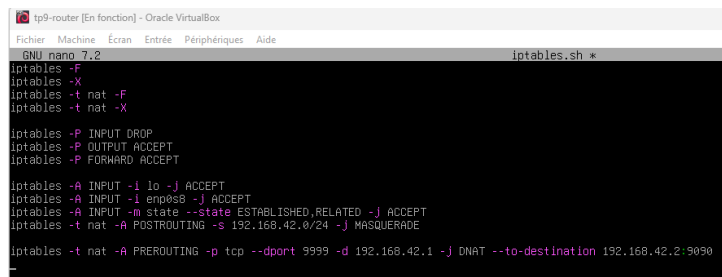


Figure 35

28 Rediriger un port

Dans cette dernière partie de ce TP, on va créer une redirection d'un port d'une adresse IP vers un autre port d'une autre adresse IP. On retourne sur la machine "tp9-router" et on modifie le fichier "iptables.sh" avec la commande : `"sudo nano iptables.sh"`. Dans ce fichier, on ajoute la ligne suivante : `"iptables -t nat -A PREROUTING -p tcp --dport 9999 -d 192.168.42.1 -j DNAT --to-destination 192.168.42.2:9090"`. On sauvegarde en utilisant "Ctrl+X" et la touche "y" pour "Yes", et la touche "Entrée" pour sauvegarder. On peut voir l'étape précédente sur la Figure 36.



```
tp9-router [En fonction] - Oracle VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
GNU nano 7.2 iptables.sh
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i enp0s8 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.42.0/24 -j MASQUERADE
iptables -t nat -A PREROUTING -p tcp --dport 9999 -d 192.168.42.1 -j DNAT --to-destination 192.168.42.2:9090
```

Figure 36

On applique les changements en tapant la commande : "sudo bash iptables.sh". On vérifie la table "nat" en tapant la commande : "sudo iptables -t nat -L -v". On voit qu'il y a bien une entrée "PREROUTING" vers la destination 192.168.42.1.

29 Tester le port redirigé

On retourne sur la machine "tp9-client" et on ouvre Firefox. Sur la barre de recherche, on tape l'adresse <https://tp9-router.afpa:9999> et on appuie sur "Entrée". On voit qu'on arrive sur une page d'alerte de sécurité SSL. On clique sur "Advanced" et sur "Accept the Risk and Continue" pour accéder au site. On voit qu'on arrive sur la page web du serveur Cockpit de la machine "tp9-server" (Voir la Figure 37).

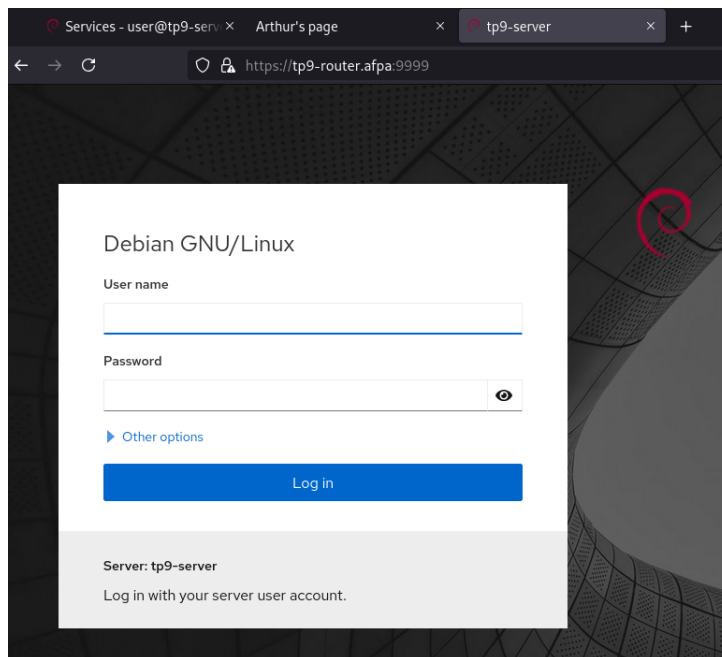


Figure 37

On voit bien que la redirection du port fonctionne correctement. Ainsi, on a vu quelques utilisations du serveur Cockpit.