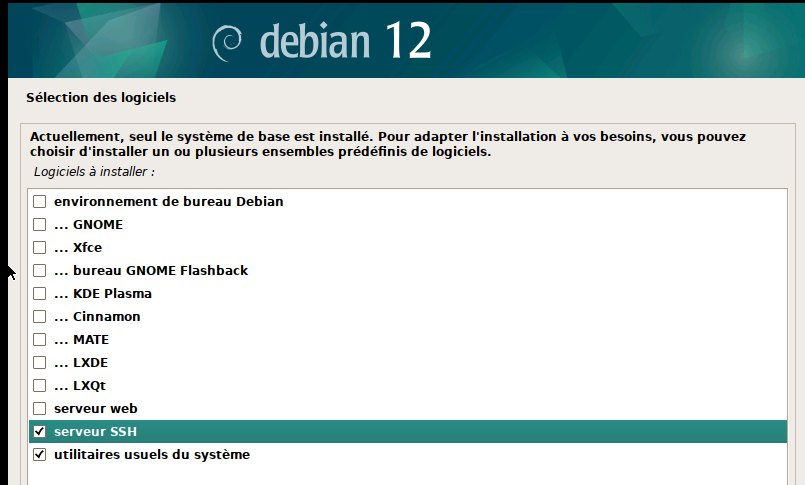
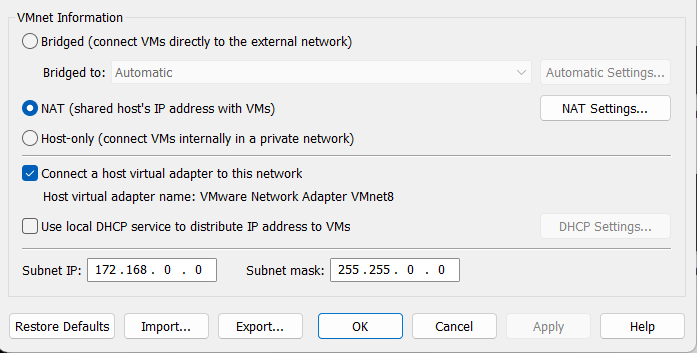
Nous avons commencé par installer les deux machines debian sans interface, sur l’une nous avons activer le SSH durant l’installation car il nous l’a été demandé.



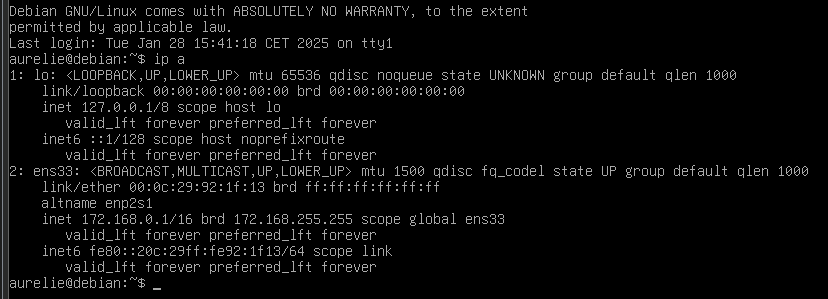
Ensuite nous avons mis à jour nos machines avec à l’aide des commandes **apt update** et **apt upgrade**.

Pour la configuration du serveur DHCP, nous avons commencé par l’installer à l’aide de la commande **apt install isc-dhcp-server**. Un problème a été rencontré celui de la commande **sudo**, nous avons dû l’installer en mode root (su -) : **apt install sudo**.

Une fois tout cela fait, nous avons configuré le serveur DHCP pour lui attribuer des adresses de classe B aux machines :



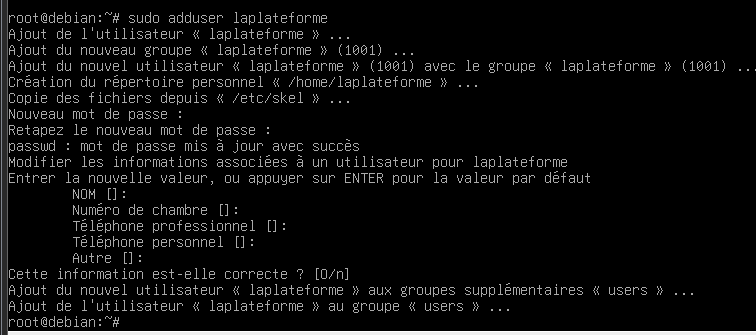
Il a fallu décocher la partie “Use local DHCP…”, pour ensuite pouvoir attribuer l’adresse de classe B.



**ip a** nous a permis de voir que notre adresse est bien celle que nous avons inscrite juste avant. Pour nous assurer que la machine hébergeant le serveur DHCP possède bien une adresse IP fixe ….

Pour l’installation du serveur FTP (proFTPd) nous avons utilisé la commande **apt-get install proftpd**. Nous devions configurer le serveur FTP de sorte qu’une seule session de connexion soit possible, nous avons dû éditer le fichier **proftpd.conf**. Pour se faire nous avons utilisé la commande **nano /etc/proftpd/proftpd.conf**, une fois à l'intérieur il nous a suffit d’ajouter **MaxClientsPerUser 1, MaxConnectionsPerHost 1** et de changer le **MaxInstances 30** à **1**. Redémarrage du service avec **sudo systemctl restart proftpd**.



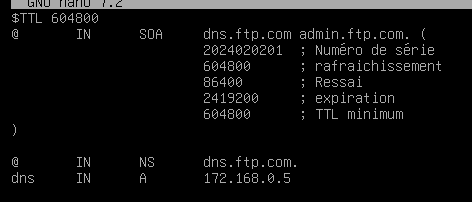


Nous a été demandé de créer un utilisateur **laplateforme** avec un mot de passe, pour cela nous avons utilisé la commande **sudo adduser laplateforme**, le mot de passe nous a donc été automatiquement demandé.

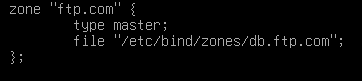


voir avec léonce comment expliquer ça

Pour l’installation du serveur DNS nous avons exécuté la commande : **sudo apt install bind9**. La configuration a été assez complexe à faire, pour commencer on a dû configurer un fichier de zone avec la commande **sudo mkdir -p /etc/bind/zones**, puis créer et éditer le fichier de zone pour ftp.com, nous utilisons la commande **nano /etc/bind/zones/db.ftp.com**, nous ajoutons ensuite le contenu suivant :



L’adresse IP que nous entrons est celle reliée à la machine qui héberge le serveur FTP. Pour que cela fonctionne nous avons dû configurer BIND9 en ouvrant le fichier de configuration local avec la commande **nano /etc/bind/named.conf.local**. Une fois à l’intérieur on ajoute la déclaration de la zone :



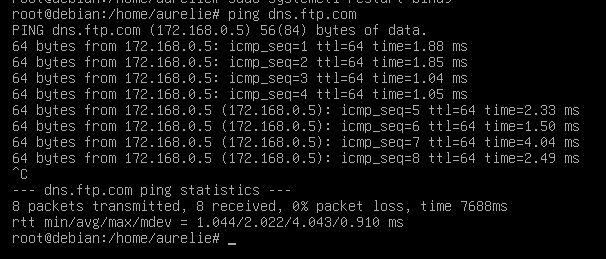
Redémarrage du serveur DNS **sudo systemctl restart bind9**. Pour vérifier qu’il n’y pas d'erreurs, on utilise les commandes **sudo named-checkzone ftp.com /etc/bind/zones/db.ftp.com** et **sudo named-checkconf**.

On teste ensuite la résolution DNS avec **nslookup dns.ftp.com 127.0.0.1**.



Nous avons rencontré une erreur… Pour la corriger nous avons dû vérifier que notre serveur DNS était bien utilisé par notre machine, la commande pour le vérifier est **cat /etc/resolv.conf**. Celle-ci ne renvoyait pas la bonne, on a donc dû l’éditer avec la commande **nano /etc/resolv.conf** et ajouter à nameserver **127.0.0.1**.

Nous avons ping **dns.ftp.com** :

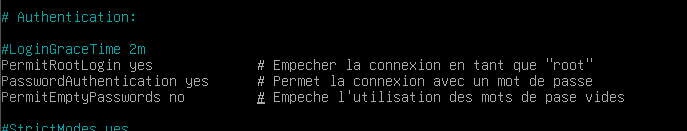


Nous voyons bien que le ping vers le serveur FTP a fonctionné. Et là nous allons tester sa connexion en se connectant avec l’utilisateur laplateforme et son mot de passe.



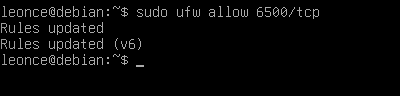
Afin de renforcer la sécurité du serveur, Dans le fichier **/etc/ssh/sshd\_config**, activer le port 6500 en ajoutant la ligne **Port 6500** car à la base le serveur SSH est sur le port 22 et ajouter les lignes:

* AllowUsers laplateforme: Pour permettre à l’utilisateur laplateforme de pouvoir se connecter au réseau
* PermitRootLogin yes
* PasswordAuthentication yes
* PermitEmptyPasswords no



Ensuite, pour plus de sécurité on a installé le pare-feu **UFW** (Uncomplicated Firewall) qui est un pare-feu simplifié pour Linux servant à faciliter les règles sans avoir à écrire des commandes complexes. Pour l’installer on tape la commande **sudo apt install ufw**. Puis, pour autoriser le port 6500, on tape la commande **sudo ufw allow 6500/tcp.**

Pourquoi on précise /tcp? Pour avoir des connexions fiables.



Pour vérifier, voici la connexion avec l’utilisateur laplateforme et celui du root. Dans ce cas, nous observons bien que le root ne se connecte pas.

