2. Mise à jour des systèmes Vérifiez et appliquez les mises à jour nécessaires sur les deux machines.

commande: **apt update & apt upgrade**.

```
E: Le dépôt http://deb.debian.org/debian bookworm-updates InRelease n'est plu
N: Les mises à jour depuis un tel dépôt ne peuvent s'effectuer de manière séc
sactivées par défaut.
N: Voir les pages de manuel d'apt-secure(8) pour la création des dépôts et le
ion d'un utilisateur.
root@debian:/home/laplateforme# apt upgrate
E: L'opération upgrate n'est pas valable
root@debian:/home/laplateforme# apt upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian:/home/laplateforme#
```

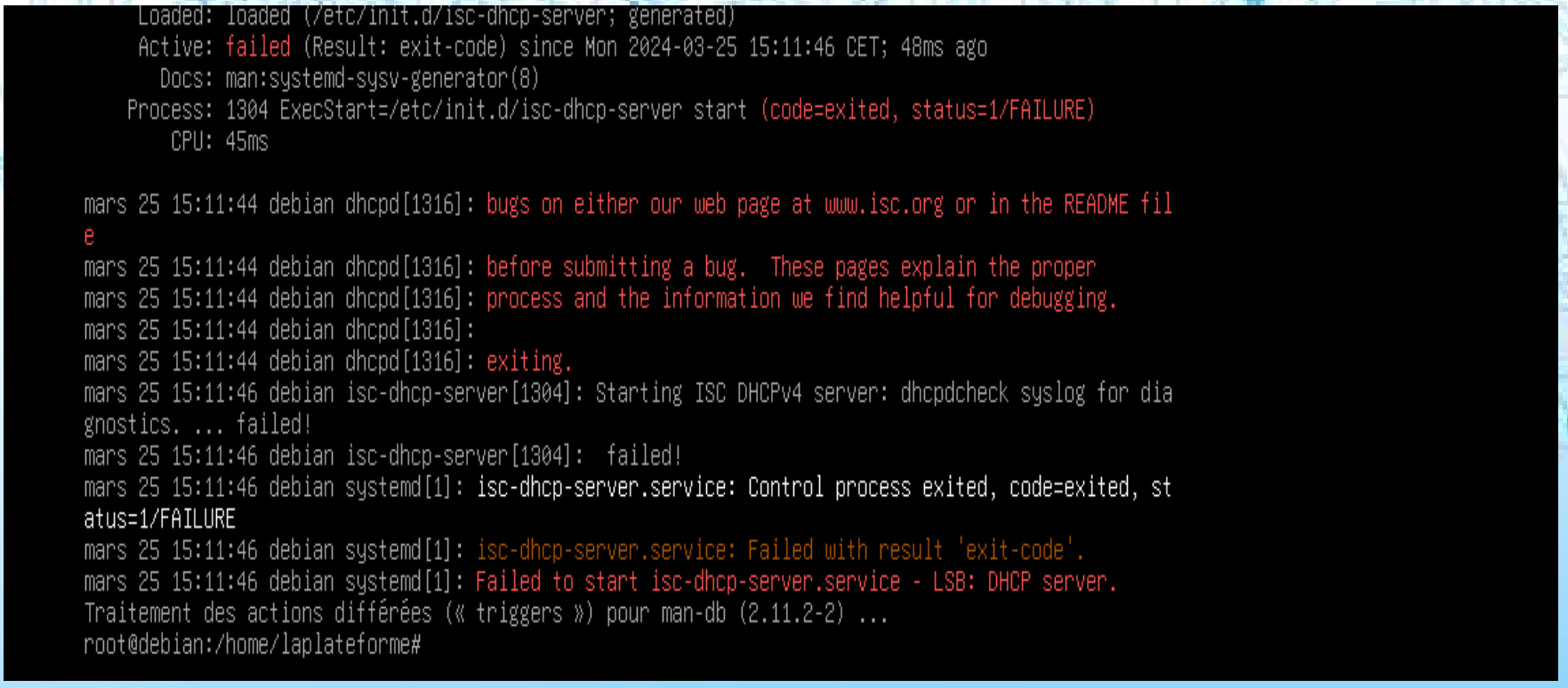
3. Configuration du serveur DHCP :

- Installez un serveur DHCP sur la première machine.

-Configurez le serveur DHCP pour attribuer des adresses de classe B aux machines connectées au réseau.

-Assurez-vous que la machine hébergeant le serveur DHCP possède une adresse IP fixe.

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



Configuration du serveur DHCP :

Une fois le serveur DHCP installé, on doit le configurer pour attribuer des adresses de classe B. On peut le faire en modifiant le fichier de configuration du serveur DHCP, généralement situé dans `/etc/dhcp/dhcpd.conf` sur les systèmes Linux.

commande: nano /etc/dhcp/dhcpd.conf

```
# You can declare a class of clients and then do address allocation
# based on that.   The example below shows a case where all clients
# in a certain class get addresses on the 10.17.224/24 subnet, and all
# other clients get addresses on the 10.0.29/24 subnet.

#class "foo" {
#  match if substring (option vendor-class-identifier, 0, 4) = "SUNW";
#}

#shared-network 224-29 {
#  subnet 10.17.224.0 netmask 255.255.255.0 {
#    option routers rtr-224.example.org;
#  }
#  subnet 10.0.29.0 netmask 255.255.255.0 {
#    option routers rtr-29.example.org;
#  }
#  pool {
#    allow members of "foo";
#    range 10.17.224.10 10.17.224.250;
#  }
#  pool {
#    deny members of "foo";
#    range 10.0.29.10 10.0.29.230;
#  }
#}
subnet 172.16.0.0 netmask 255.255.0.0 {
        range 172.16.0.10 172.16.255.254;
        option subnet-mask 255.255.0.0;
        option routers 172.016.0.1;
        option broadcast-address 172.16.255.255;
}
```

Configuration du serveur DHCP pour attribuer des adresses de la plage 172.16.0.10 à 172.16.255.254, avec un masque de sous-réseau de 255.255.0.0.

Redémarrez le service DHCP :

commande: sudo systemctl restart isc-dhcp-server

4. Installation du Serveur FTP et SSH :

-Sur la deuxième machine, installez un serveur FTP (proFTPd) et SSH.

- Configurez le serveur FTP avec une seule session de connexion possible. - Utilisez les identifiants suivants pour le FTP :

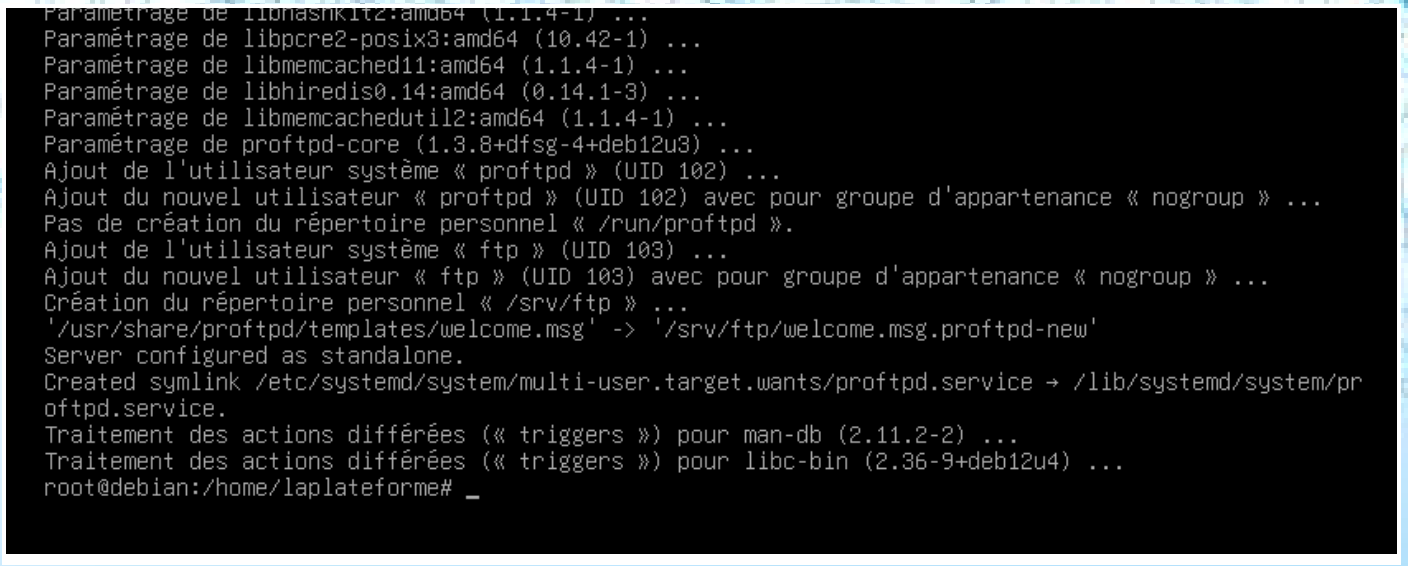
- Identifiant : laplateforme - Mot de passe : Marseille13!

- Utilisez le serveur SSH pour les connexions au FTP en SFTP, renforçant ainsi la sécurité.

Installation de proFTPd et SSH :

Utilisez le gestionnaire de paquets de votre système d'exploitation pour installer proFTPd et SSH.

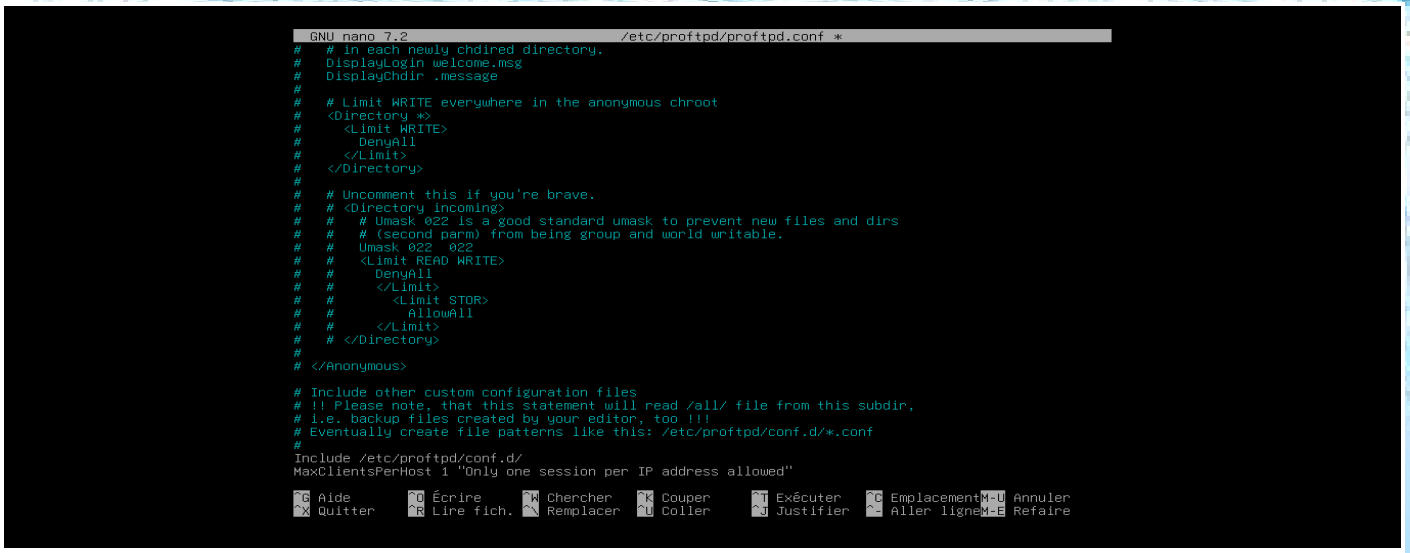
Commande : sudo apt-get install proftpd ssh



Configuration de proFTPd :

Une fois proFTPd installé, on peut le configurer pour permettre une seule session de connexion. Il faut modifier le fichier de configuration de proFTPd, généralement situé dans `/etc/proftpd/proftpd.conf`.

Commande: nano /etc/proftpd/proftpd.conf



Après avoir modifié la configuration, on doit redémarrer le service proFTPd pour appliquer les modifications.

commande: sudo systemctl restart proftpd

Une fois cela fait, proFTPd limitera le nombre de sessions FTP autorisées par adresse IP à une seule à la fois, comme spécifié dans la directive `MaxClientsPerHost`.

Création d'un utilisateur FTP :

On doit créer un utilisateur pour permettre la connexion FTP.

Commande: sudo adduser laplateforme

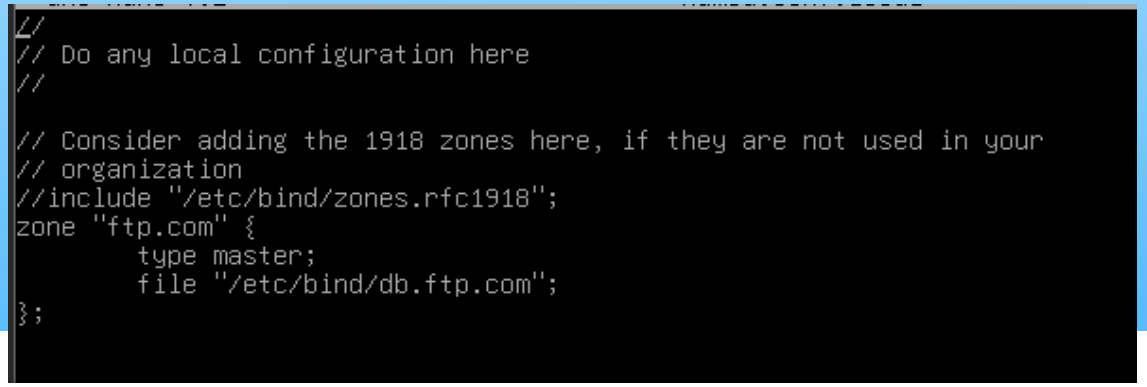
Installer le serveur DNS :

Utilisez le gestionnaire de packages de votre système d'exploitation pour installer un serveur DNS. installer le serveur BIND (Berkeley Internet Name Domain) avec la commande : sudo apt-get install bind9

configurer pour qu'il réponde aux requêtes DNS et qu'il gère les enregistrements de zone. Le fichier de configuration principal pour BIND sur la plupart des distributions Linux est /etc/bind/named.conf.

Dans le fichier /etc/bind/named.conf.local, on peut ajouter une zone pour `dns.ftp.com` :

```
zone “ftp.com” {
        type master;
        file “/etc/bind/db.ftp.com.”;
};
```



Ensuite, créez un fichier de zone pour `dns.ftp.com` à l'emplacement spécifié (`/etc/bind/zones/dns.ftp.com.zone`):

```
$TTL 86400
@ IN SOA      ftp.com admin.    ftp.com. (
              2024032801
              86400
              7200
              20240050101
              86400
              )
@             IN  NS     ftp.com.
                         172.16.0.5
                         172.16.0.11
```

Restreindre l'accès aux seuls identifiants fournis :

Vous devez configurer votre serveur SFTP pour qu'il n'accepte que les identifiants spécifiques autorisés. Pour cela, vous pouvez utiliser des comptes d'utilisateurs système existants ou créer de nouveaux comptes d'utilisateurs

dédiés pour les utilisateurs autorisés. Assurez-vous que seuls ces comptes ont des autorisations d'accès au serveur SFTP.

Configuration du serveur pour fonctionner sur le port 6500 :

Vous devez modifier la configuration du serveur SFTP pour qu'il écoute sur le port 6500 au lieu du port par défaut (généralement 22). Selon le serveur SFTP que vous utilisez, la manière de faire cela peut varier. Voici un exemple avec OpenSSH :

- Ouvrez le fichier de configuration SSH, généralement situé à `/etc/ssh/sshd_config`.
- Recherchez la ligne `Port` et changez-la pour `Port 6500`.
- Pour éviter les connexions anonymes ou invitées, vous pouvez désactiver l'accès à l'utilisateur invité dans la configuration du serveur SFTP.
- Assurez-vous que l'option `PermitEmptyPasswords` est définie sur `no` pour empêcher les connexions sans mot de passe.
- Enregistrez les modifications et redémarrez le service SSH pour appliquer les changements :
- Sudo systemctl restart sshd