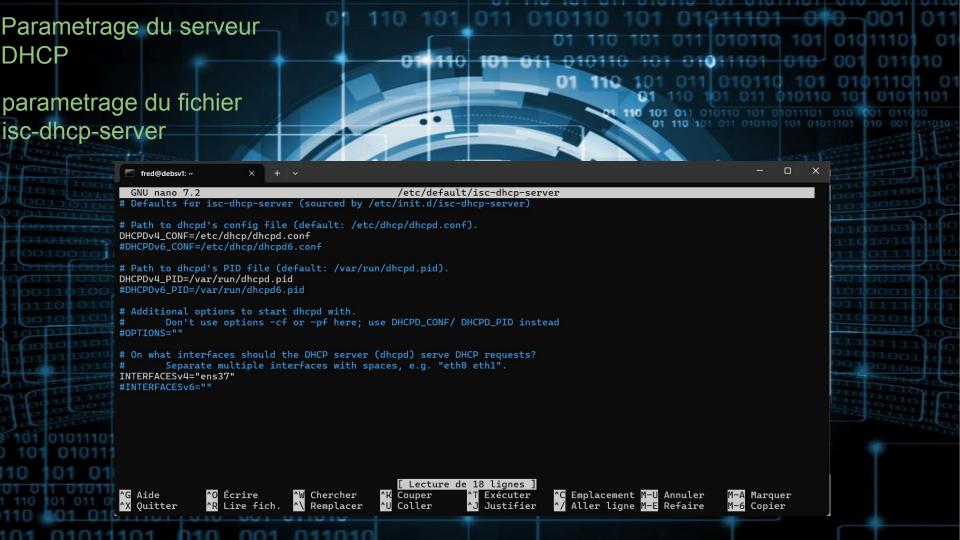






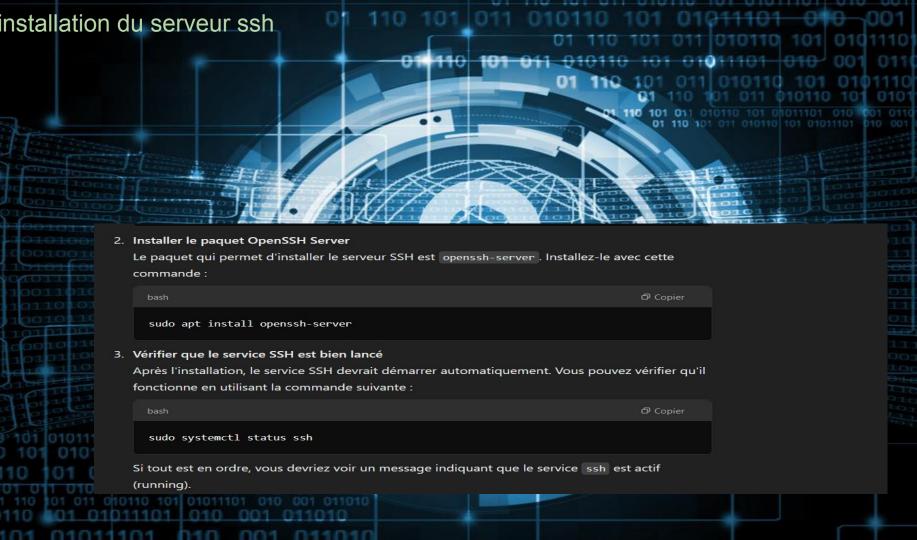
## Configuration du serveur DHCP lines 1-17/17 (END) root@debsv1:~# systemctl restart isc-dhcp-server root@debsv1:~# systemctl status isc-dhcp-server isc-dhcp-server.service - LSB: DHCP server Loaded: loaded (/etc/init.d/isc-dhcp-server; generated) Active: active (running) since Wed 2025-01-29 13:39:35 CET; 3s ago Docs: man:systemd-sysv-generator(8) Process: 917 ExecStart=/etc/init.d/isc-dhcp-server start (code=exited, status=0/SUCCESS) Tasks: 1 (limit: 2273) Memory: 4.7M CPU: 251ms CGroup: /system.slice/isc-dhcp-server.service └926 /usr/sbin/dhcpd -4 -q -cf /etc/dhcp/dhcpd.conf ens37 janv. 29 13:39:32 debsv1 systemd[1]: Starting isc-dhcp-server.service - LSB: DHCP server... janv. 29 13:39:32 debsv1 isc-dhcp-server[917]: Launching IPv4 server only. ianv. 29 13:39:32 debsv1 dhcpd[926]: Wrote 0 leases to leases file. janv. 29 13:39:32 debsv1 dhcpd[926]: Server starting service. janv. 29 13:39:35 debsv1 isc-dhcp-server[917]: Starting ISC DHCPv4 server: dhcpd. janv. 29 13:39:35 debsv1 systemd[1]: Started isc-dhcp-server.service - LSB: DHCP server. root@debsv1:~#



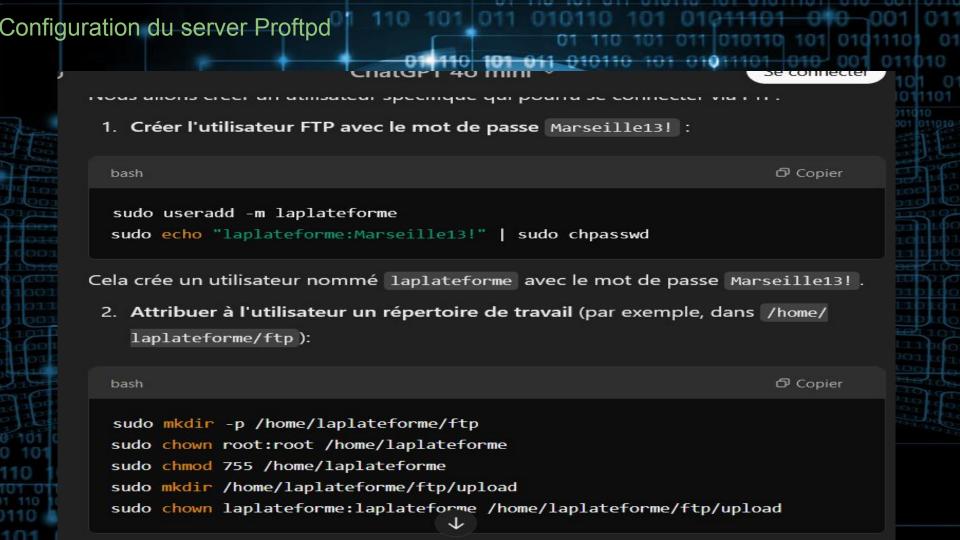
etc/dhcp/dhcpd.conf Exemple de configuration pour un réseau de classe B Spécifiez le domaine ption domain-name "example.com"; Spécifiez les serveurs DNS ption domain-name-servers 8.8.8.8, 8.8.4.4; Spécifiez le serveur de passerelle ption routers 172.16.0.1; Spécifiez l'adresse de broadcast ption broadcast-address 172.16.255.255; Définir la plage d'adresses IP à attribuer (réseau 172.16.0.0/16) ubnet 172.16.0.0 netmask 255.255.0.0 { range 172.16.10.100 172.16.10.200; # Plage d'adresses IP dynamiques option routers 172.16.0.1; # Routeur par défaut option broadcast-address 172.16.255.255; # Durée de la location par défaut (en secondes) default-lease-time 600; max-lease-time 7200; # Durée de la location maximale G Aide ^0 Écrire ^T Exécuter ^W\_Chercher Couper Emplacement Coller Remplacer ^J Justifier Aller ligne X Ouitter Lire fich.

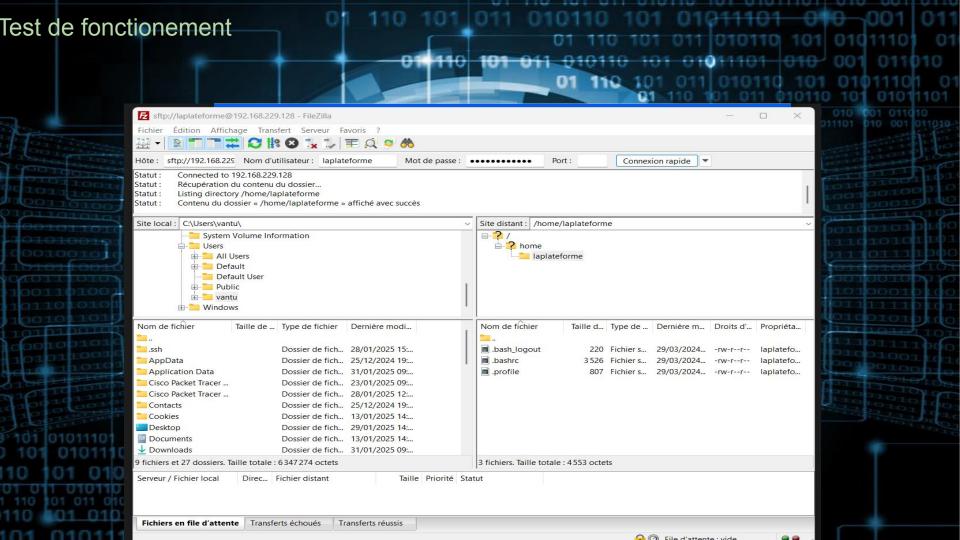
Paramétrage du fichier













#### 1. Installation de BIND9

Tout d'abord, vous devez installer BIND9 sur votre système Debian. Ouvrez un terminal et exécutez les commandes suivantes :

sudo apt update
sudo apt install bind9 bind9utils bind9-doc dnsutils

Cela installera BIND9 ainsi que quelques outils utiles pour tester et gérer le serveur DNS.

# 2. Configuration de BIND9

#### 2.1. Configurer les fichiers principaux

Les fichiers de configuration de BIND9 sont situés dans le répertoire /etc/bind . Le fichier principal est /etc/bind/named.conf .

### 2.1.1. Modifier le fichier de configuration principal

Ouvrez le fichier named.conf pour définir les  $\psi$  ions générales du serveur :

```
configuration du
serveur DNS
```

```
Ajoutez les définitions de zones. Voici un exemple pour le domaine dns.ftp.com:
```

```
zone "dns.ftp.com" IN {
    type master;
    file "/etc/bind/db.dns.ftp.com"; // Fichier de zone directe
};

zone "128.229.168.192.in-addr.arpa" IN { // Zone inverse pour 192.168.229.128
    type master;
    file "/etc/bind/db.192.168.229.128"; // Fichier de zone inverse
};
```

#### Étape 3 : Création des fichiers de zones

Créez les fichiers de zones que vous avez spécifiés dans named.conf.local.

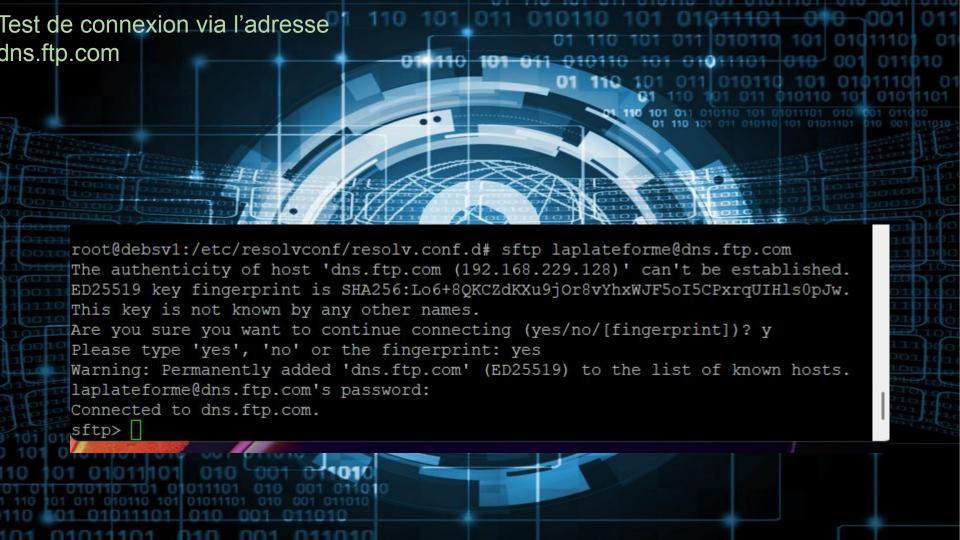
#### Fichier de zone directe ( /etc/bind/db.dns.ftp.com ):

```
$TTL 86400

@ IN SOA ns1.dns.ftp.com. admin.dns.ftp.com. (

2024042601 ; Serial

3600 ; Refresh
```



# Paramétrage sécurités supplémentaire sur le serveur sftp

lans votre fichier de configuration de ProFTPD (generalement situe a /etc/proftpd/ roftpd.conf), assurez-vous que les lignes suivantes sont présentes ou modifiées :

our changer le port d'écoute de ProFTPD, vous devez spécifier le port 6500 dans la

lans le fichier /etc/proftpd/proftpd.conf , recherchez la ligne suivante (ou ajoutez-la si elle

# Désactiver l'accès anonyme

# Désactiver l'accès invité

Anonymous off

<Limit LOGIN>

DenyA11

</Limit>

. Configurer le serveur pour fonctionner sur le port 6500 :

☼ Copier

3. Éviter toute connexion anonyme ou invité sur le serveur :

Cela restreint l'accès aux utilisateurs spécifiés dans la configuration.

spécifiques.

<Limit LOGIN>

**DenyAll** 

</Limit>

AllowUser username1

AllowUser username2

Les étapes ci-dessus désactivent déjà les connexions anonymes et invitées, mais vous pouvez

aussi configurer plus de restrictions si nécessaire. Pour empêcher tout autre type d'accès non

autorisé, vous pouvez ajouter une restriction d'accès basée sur les utilisateurs ou groupes

Voici un exemple d'ajout d'une restriction pour n'accepter que des utilisateurs authentifiés :

Port 6500

onfiguration.

'existe pas) et modifiez-la :

est du parametrage sftp par connexion anonymes oot@debsv1:~# sftp dns.ftp.com oot@dns.ftp.com's password: ermission denied, please try again. oot@dns.ftp.com's password: root@debsv1:~# sftp laplateforme@dns.ftp.com laplateforme@dns.ftp.com's password: Connected to dns.ftp.com. sftp>

pour ces jobs, la plupart des logiciel nous ont été imposé.
mise à part pour le dristou j'ai perdu du temps avec le fichier resolv conf qui ne sauvegarder pas mes paramétrage.
j'ai installé bind9, puis la suite drismasq plus facile à paramétrer.
pour résoudre mon problèmé, j'ai installer le paquet résolveconfi puis paramétrer mon serveur DNS avec le fichier base pour renseigner le DNS local rajout du dans driasquont le dns.ftp.com et redemarer dmasque puis cela à fonctionner.

installation d'outils complémentaire : net-tools pour le réseau et dinsutils pour avoir des commandes comme nalookup, dig.

l'importance dans les jobs effectuer sont la sécurité avant tout.

pour aller plus loin, une mise en place d'un serveur d'authentification à 2 facteurs seraient préconisé