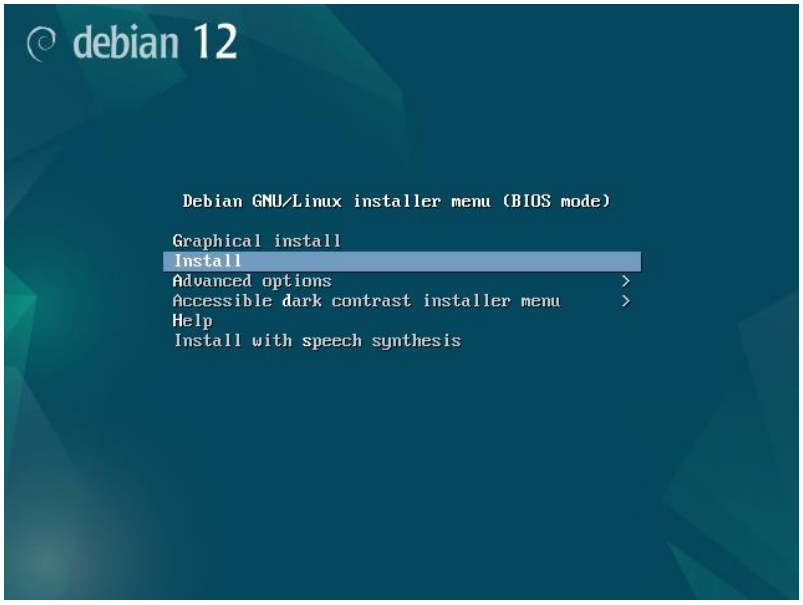
Serveur de transfère de fichier (FTP) avec Proftpd

Installation de Debian 12 :

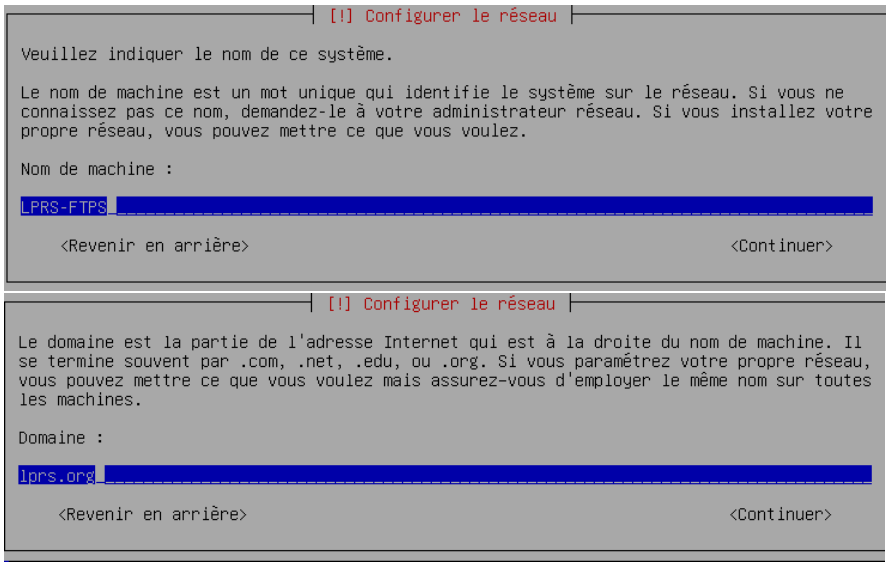
J'ai commencé par installer un système d'exploitation Linux Debian 12 sur lequel nous installerons les packages Apache2 et Proftpd.

Nous utilisons principalement Linux Debian en ligne de commande et donc avons fait une **installation sans interface graphique**.

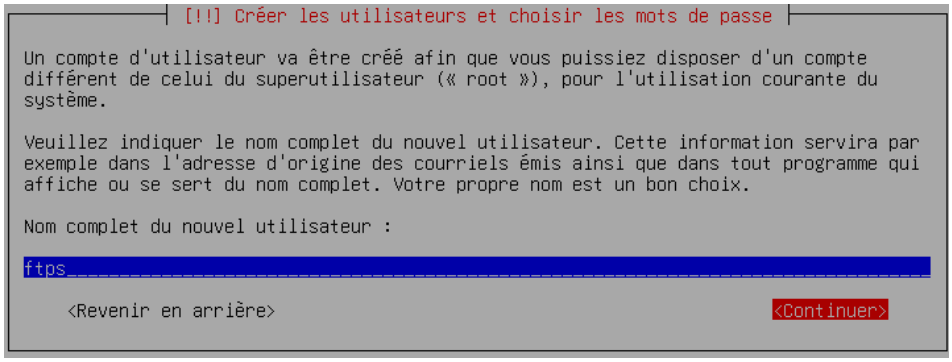


Pour le choix de la langue, de la situation géographique pour le fuseau horaire ou encore le choix de configuration du clavier, nous avons choisi **"français"**.

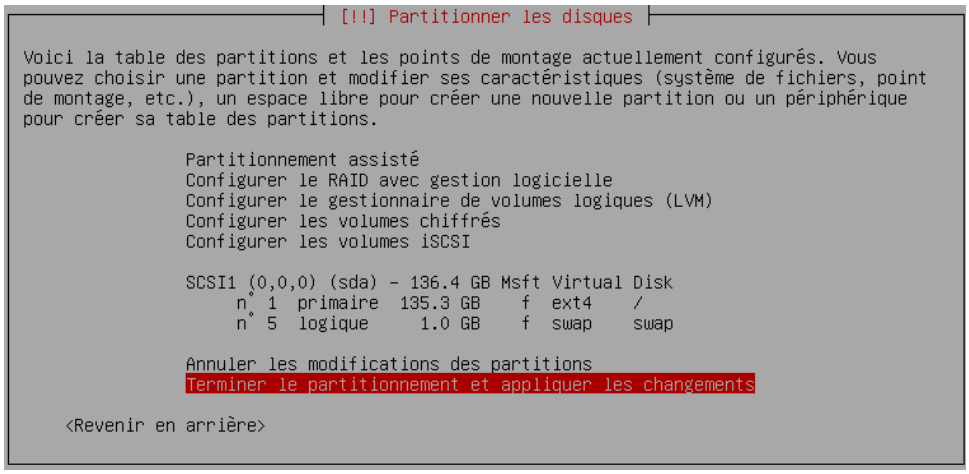
Nous avons ensuite choisi le nom de machine, dans notre cas **"LPRS-FTPS"** et le nom du domaine **"lprs.org"**.



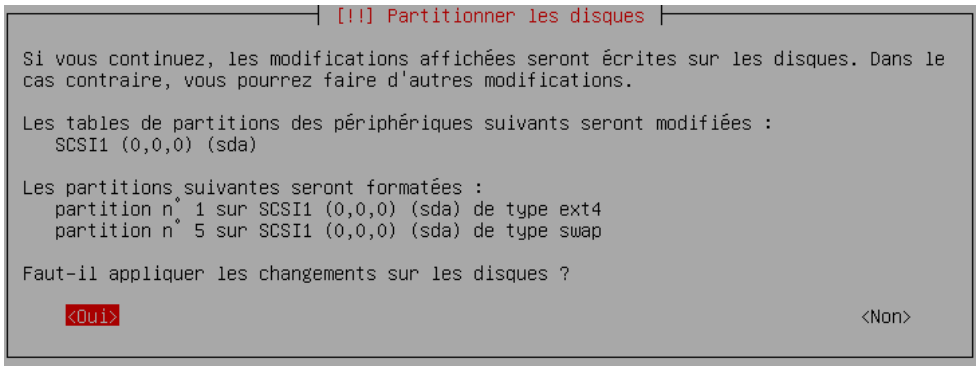
Au moment de crée les utilisateurs et de choisir les mots de passe, nous avons mis un mot de passe pour le compte de base **"root"**, nous avons ensuite crée un utilisateur nommé **"ftps"** sur lequel nous avons également attribuer un mot de passe.



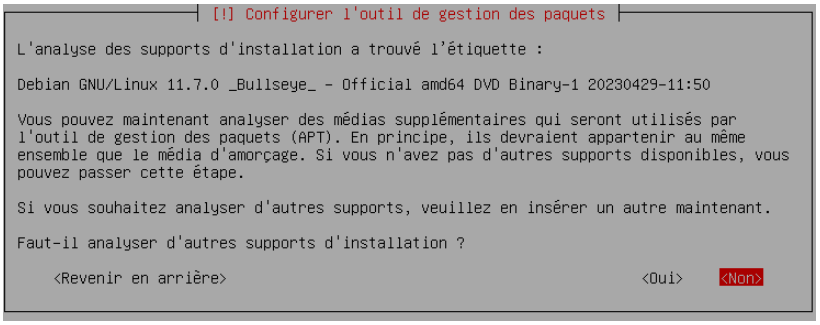
Pour la méthode de partitionnement, nous avons laissé par défaut **"Assisté – utiliser un disque entier"** puis avons choisi le seul disque disponible avec un schéma de partitionnement **"Tout dans une seule partition"**. Enfin nous avons appliqué les changements de partitionnement.



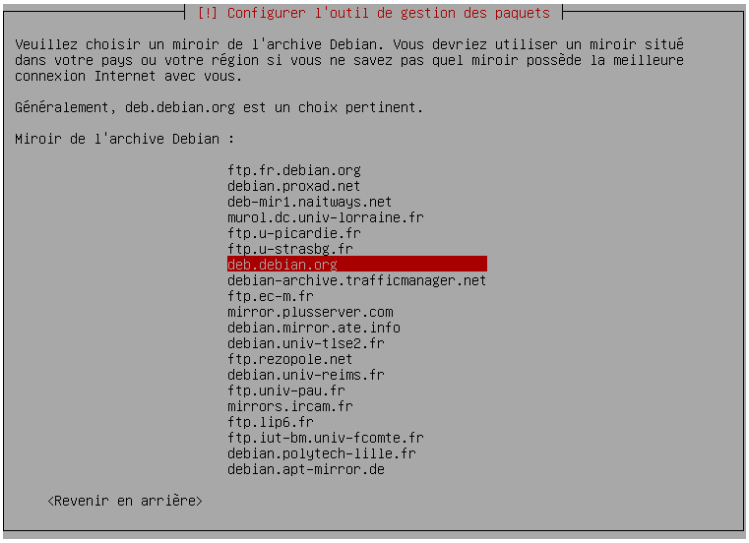
Faut-il appliquer les changements sur les disques ? on met **"oui"** pour effectuer les modifications.



Faut-il analyser d'autres supports d'installation ? on met **"non"** car on en possède pas d'autre.

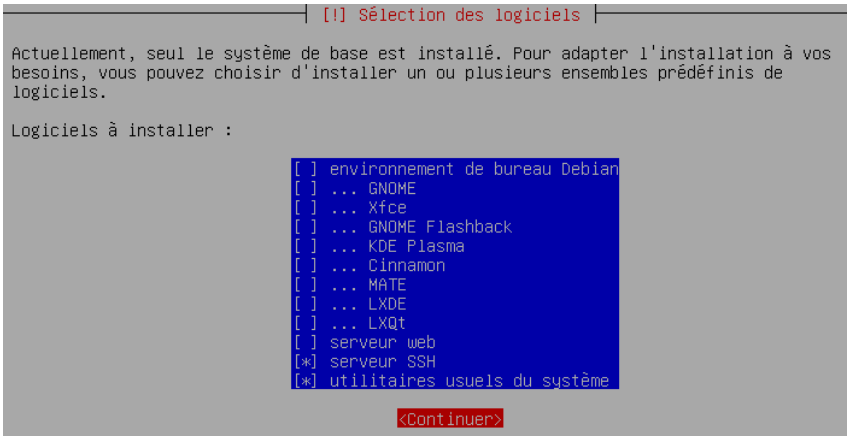


Faut-il utiliser un miroir sur le réseau ? on met **"oui"** pour configurer l'outil de gestion des paquets. On choisit comme pays du miroir de l'archive Debian **"France"** puis **"deb.debian.org"**.

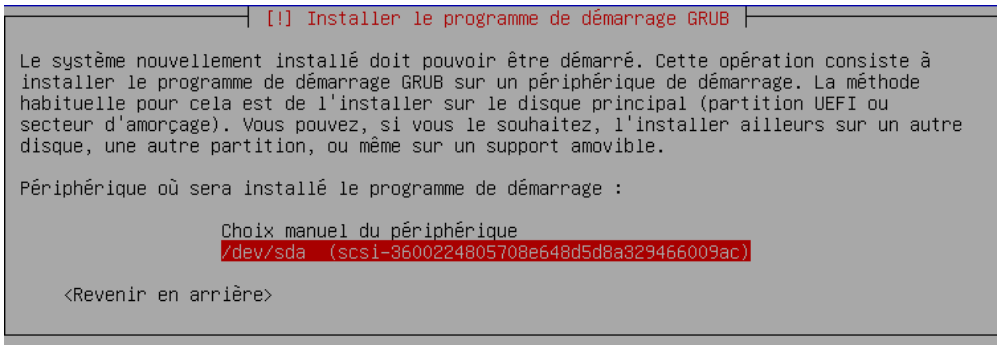


Ensuite on ne met pas de mandataire HTTP, puis on passe la question sur l'étude statistique sur l'utilisation des paquets.

Pour les logiciels à installer, on décoche **"environnement de bureau Debian"** et **"GNOME"** et on coche **"serveur SSH"** et **"utilitaires usuels du système"** et on continue.



Installer le programme de démarrage GRUB sur le disque principal ? on met **"oui"** et ont choisi le périphérique ou sera installé le programme de démarrage c'est à dire **"/dev/sda"** puis on finit l'installation de l'OS.



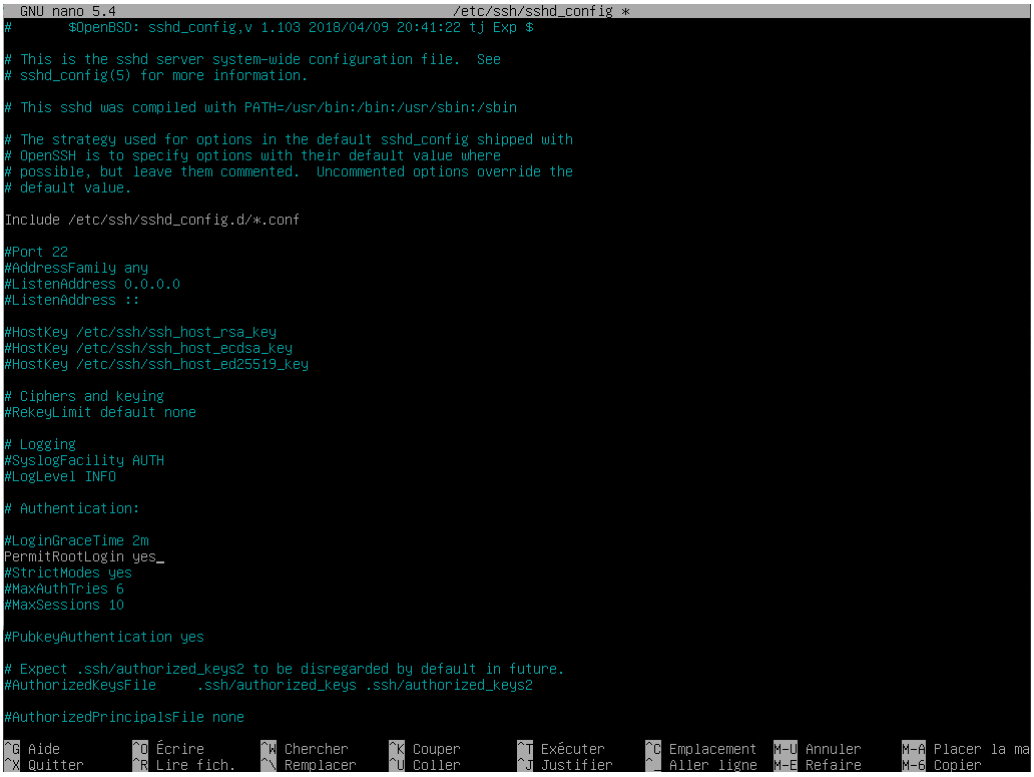
Configuration ssh :

Une fois le système d'exploitation installé, j'ai dans un premier temps configuré le service ssh afin d'avoir accès au terminal sur le logiciel MobaXterm d'une machine sur le même réseau pour une configuration plus simple.

J'ai donc taper la commande pour modifier le fichier de configuration ssh :

```
nano /etc/ssh/sshd_config
```

J'ai ensuite sur le fichier changer la ligne **"PermitRootLogin prohibit-password"** en **"PermitRootLogin yes"** sans oublier de retirer le commentaire **"#"**. Ceci permet d'accéder au logiciel MobaXterm avec le compte **"root"**.



Enfin on redémarre le service ssh avec la commande suivante :

```
/etc/init.d/ssh restart
```

Sur MobaXterm, je mets l'IP de mon serveur que je peux trouver avec la commande **"ip –c a"** et je me connecte avec les identifiant du compte **"root"**.

Mise à jour et installation des paquets nécessaires :

Dans un premier temps je mets à jour la liste des packages disponibles dans les dépôts de logiciels configurés sur le système et les packages déjà installés sur le système vers les versions les plus récentes disponibles.

```
apt-get update && upgrade
```

Ensuite j'installe le package Apache2 :

```
apt-get install apache2
```

Et le package Proftpd :

```
apt-get install proftpd
```

Une fois les installations terminer, je peux maintenant modifier le fichier de configuration.

Modification des fichiers de configuration Asterisk :

Dans un premier temps on commence par modifier le fichier **"proftpd.conf"**. Il définit les paramètres de fonctionnement du serveur ProFTPD, tels que les ports à écouter, les autorisations d'accès aux fichiers et répertoires, les options de sécurité, les paramètres de journalisation, les configurations de virtual hosts, et bien d'autres.

```
nano /etc/proftpd/proftpd.conf
```

Sur le fichier on supprime le commentaire **"#"** de la ligne **"DefaultRoot"** puis on rajoute **"/var/www"** derrière ce qui permet de définir le répertoire racine par défaut pour les utilisateurs lorsqu'ils se connectent au serveur FTP avec leurs identifiants. On ajoute également une ligne juste en dessous avec **"RootLogin OFF"** ce qui permet de désactiver la possibilité pour l'utilisateur **"root"** de se connecter au serveur FTP pour renforcer la sécurité car l'utilisateur root possède des privilèges étendus sur le système, et autoriser sa connexion via FTP peut présenter un risque de sécurité accru. Enfin on change le port FTP standard de **"21"** à un autre port tel que **"21987"** pour notre cas. Cela améliore la sécurité du serveur en rendant plus difficile pour les attaquants de scanner et de trouver le serveur FTP.

```
DefaultRoot /var/www
RootLogin OFF
Port 21987
```

Une fois le fichier de configuration modifier on l'enregistre et on passe au droit.

Gestion des droits utilisateurs et groupes aux dossiers :

On ajoute maintenant les permissions appropriées à un utilisateur pour qu'il puissent accéder et modifier les fichiers dans le répertoire /var/www, tout en maintenant un niveau de sécurité adéquat pour ce répertoire.

```
usermod -a -G  www-data ftps
```

- **"usermod"** est une commande utilisée pour modifier les paramètres d'un utilisateur.
- L'option **" -a "** ajoute l'utilisateur spécifié au groupe mentionné.
- L'option **"-G www-data"** spécifie le groupe **"www-data"** auquel l'utilisateur sera ajouté.
- **"ftps"** est le nom de l'utilisateur auquel nous ajoutons le groupe **"www-data".**

Cette commande ajoute l'utilisateur **"ftps"** au groupe **"www-data"**. Ceci est fait pour permettre à l'utilisateur **"ftps"** d'accéder aux fichiers du répertoire **"/var/www"**.

Ensuite on met la commande suivante :

```
chown www-data:www-data /var/www
```

- **"chown"** est une commande utilisée pour changer le propriétaire et/ou le groupe d'un fichier ou d'un répertoire.
- **"www-data:www-data"** spécifie que le propriétaire et le groupe du répertoire seront tous deux **"www-data"**.
- **"/var/www"** est le chemin du répertoire sur lequel nous appliquons les changements.

Cette commande modifie le propriétaire et le groupe du répertoire /var/www en **"www-data"**. Cela garantit que le serveur FTP (et l'utilisateur associé, s'il est dans le groupe **"www-data"**) aura les permissions nécessaires pour accéder et manipuler les fichiers dans ce répertoire.

Enfin pour finir :

```
chmod 775 /var/www
```

- **"chmod"** est une commande pour changer les permissions d'accès sur des fichiers ou des répertoires.
- **"775"** est un ensemble de permissions octales qui spécifie les droits pour l'utilisateur, le groupe et les autres.
- **"/var/www"** est le répertoire sur lequel nous appliquons ces changements de permissions.

Cette commande accorde des permissions de lecture, d'écriture et d'exécution à l'utilisateur et au groupe **"www-data"** dans notre cas sur le répertoire **"/var/www"**. Les autres utilisateurs auront seulement la permission de lire et d'exécuter les fichiers dans ce répertoire.

- Utilisateur propriétaire : permissions de lecture (4), écriture (2) et exécution (1) = (7).
- Membres du groupe : permissions de lecture (4), écriture (2) et exécution (1) = (7).
- Les autres utilisateurs ont la permission de lecture (4) et d'exécution (1) = (5).

Sécurisation du serveur avec Secure Sockets Layer (SSL) :

Pour un serveur FTP, l'utilisation de SSL/TLS (Secure Sockets Layer/Transport Layer Security) assure une connexion sécurisée entre le client FTP et le serveur FTP. Cela crypte les données qui transitent entre les deux, empêchant ainsi les interceptions et les manipulations malveillantes des données. C'est particulièrement important lors de l'envoi de données sensibles, telles que des identifiants de connexion ou des fichiers confidentiels, sur un réseau public comme Internet.

On installe donc dans un premier temps le package Openssl :

```
apt-get install openssl
```

Ensuite on génère des clés et des certificats SSL/TLS.

```
openssl genrsa –des3 –out private.key 2048
```

Cette commande génère une paire de clés RSA (clé privée et clé publique) avec une longueur de **"2048"** bits. La clé privée est stockée dans le fichier **"private.key"**. L'option **"-des3"** demande à OpenSSL de chiffrer la clé privée avec un chiffrement Triple DES.

```
openssl req -new -key private.key -out ftp.csr
```

Cette commande crée une demande de signature de certificat (Certificate Signing Request, CSR) à partir de la clé privée précédemment générée. La CSR contient des informations sur l'entité qui demande le certificat, telles que le nom de domaine du serveur.

```
openssl rsa -in private.key -out public.key
```

Cette commande extrait la clé publique à partir de la clé privée générée précédemment. La clé publique est stockée dans le fichier **"public.key"**.

```
openssl x509 -req -days 365 -in ftp.csr -signkey private.key -out certif.crt
```

Cette commande crée un certificat auto-signé à partir de la CSR générée précédemment. Le certificat est signé avec la clé privée pour créer une autorité de certification auto-signée. Le certificat est valable pendant 365 jours **"-days 365"** et est enregistré dans le fichier **"certif.crt"**.

Pour finir, il faut configurer le fichier tls.conf :

```
/etc/proftpd/tls.conf
```

On supprime le commentaire des lignes suivantes et on les modifie en fonction des chemins ou sont stocker les clés et les certificats.

```
TLSEngine                   on
TLSLog                      /var/log/proftpd/tls.log
TLSProtocol                 SSLv23
TLSRSACertificateFile       /etc/ssl/certs/certif.crt
TLSRSACertificateKeyFile    /etc/ssl/private/private.key
TLSOptions                  NoCertRequest AllowClientRenegotiations
TLSVerifyClient             off
TLSRequired                 on
```

Configuration des Paramètres Réseau :

Pour finir, j'ai paramétrer la carte réseau en statique, j'ai donc commencer par me rendre sur le fichier de configuration réseau :

```
nano /etc/network/interfaces
```

J'ai paramétrer la carte réseau eth0 comme ceci :

```
# Interface Static
auto eth0
iface eth0 inet static
    address 172.30.0.13
    netmask 255.255.240.0
    gateway 172.30.0.1
    dns-nameservers 172.30.0.5
```

On peut maintenant redémarrer tous les services afin de prendre en compte les modifications :

```
/etc/init.d/networking restart
```

```
/etc/init.d/apache2 restart
```

```
/etc/init.d/proftpd restart
```