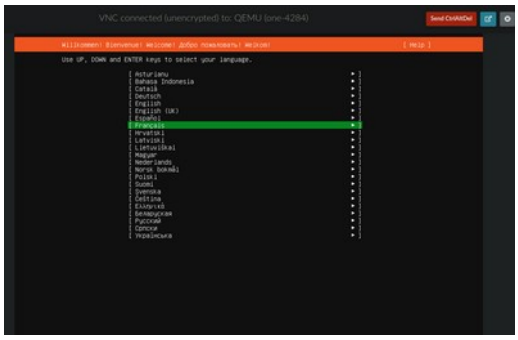
TD n° 6 : Sécurité, installation d'un pare-feu

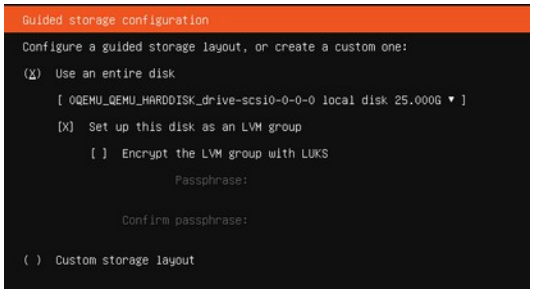
Rappel : ce TD doit faire l'objet d'un Compte Rendu électronique à déposer sur GitLab avant le début de séance suivante, à l'attention de l'enseignant responsable de votre groupe.

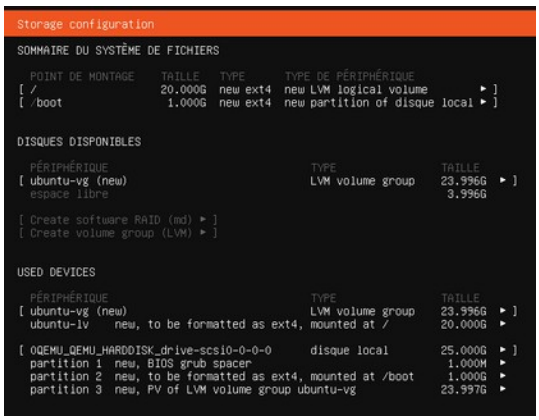
Ce TD se déroulera sous Windows, pour permettre l'utilisation de Wireshark et l'étude des échanges sur le réseau.

Partie 1 : Installation d'une machine virtuelle OpenNebula

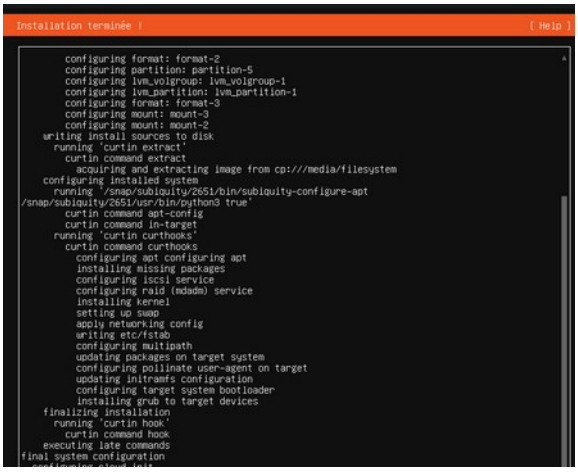
1. Créer une machine virtuelle Ubuntu Server à partir du modèle **`Ubuntu-Server`** présent sur OpenNebula.
   Créer un utilisateur **`user`** avec le mot de passe **`iutinfo`** (et un clavier français)



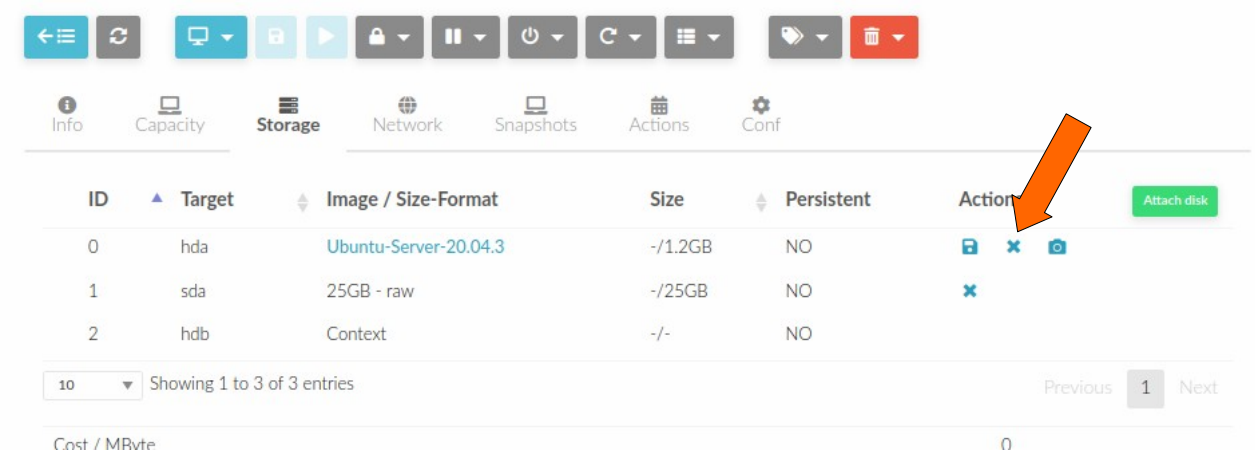




Ne rien cocher dans les derniers écrans (installation OpenSSH, Featured Server Snaps) et laisser la mise à jour se terminer ...



De retour dans OpenNebula, ouvrir l'onglet ***Storage*** pour détacher (supprimer) l'image du CDROM **`Ubuntu-Server-20.04.3`** avant le redémarrage.
(Un ***`PowerOff Hard`*** peut être nécessaire pour détacher le disque)



2. Télécharger le fichier **`.vv`** et ouvrez l'accès distant avec **VirtViewer** : le fichier devra être joint à votre dépôt !

3. Installer un serveur **Apache** (**`apache2`**) et **PHP** sur votre serveur.

4. Installer et démarrer les services **ftp** (**`vsftpd`**) et **telnet** (**`telnetd`**)

5. Utilisation de **Wireshark** depuis votre poste Windows pour analyser le trafic entre votre PC et le serveur virtuel et **étudier les informations des trames capturées**.

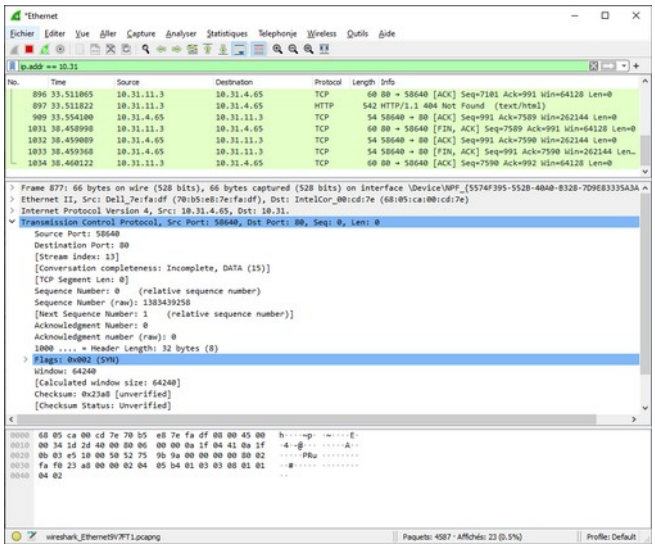
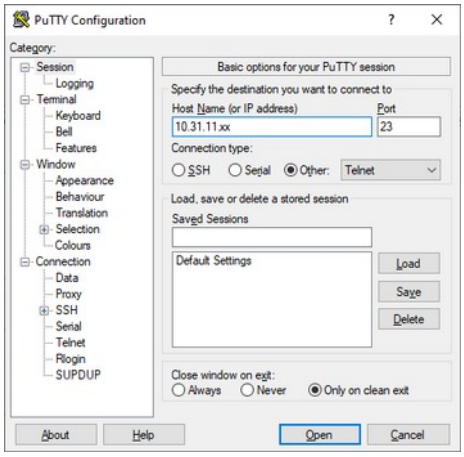


Figure 1: Capture de trames IPv4 avec Wireshark

a) **Lancer des connexions** en **`ftp, telnet`** et **`ssh`** sur votre serveur : utiliser pour cela le terminal (**`cmd`**) ou Putty …
Observer les échanges avec Wireshark.



b) Pour le protocole telnet, cherchez à retrouver les identifiants utilisés en « dépliant » les informations des paquets ("*payload*")

c) **Pour le protocole ftp, identifier les requêtes `ARP`** puis **`TCP`** (**`syn/syn ; ack/ack`**) dans la fenêtre de Wireshark.

d) Sur les transmissions du protocole **ftp**, **analyser la séquence de connexion** lors de la transmission du couple login/MdP

Que peut-on conclure sur la sécurité des protocoles testés ?
Le(s)quel(s) doit-on privilégier ? Le(s)quel(s) doit-on réserver à usage sur réseau privé ?

Partie 2 : recherche des services accessibles

Avant de commencer à installer des filtres sur les paquets IP, il est intéressant d'observer son système et de voir quels services sont accessibles (ouverts).

1. Pour cela, nous pouvons utiliser la commande **`netstat`** :

```
[root@Ubuntu-Server]# netstat –ltp
```

2. Consultez le manuel (**`man netstat`**) pour déterminer le rôle de chacune des options '**`l`**' '**`t`**' et '**`p`**'.

Quelles informations peut-on tirer du résultat de cette commande ?
Comment connaître la liste des services UDP ouverts sur la machine ?

3. Les noms, numéros et protocoles des différents services sont listés dans le fichier **`/etc/services`**

Quels sont les ports et les services ouverts sur votre serveur ?

4. De la même manière, testez les ports accessibles avec les deux commandes ci-dessous :

```
sudo lsof -i -P -n
sudo ss -tunlp
```

5. Consultez à nouveau le manuel pour déterminer le rôle de chaque option utilisée.

Partie 3 : Configuration d'un pare-feu ufw

Le pare-feu ***Uncomplicated Firewall*** est pré-installé sous Ubuntu mais il n'est pas activé par défaut : on commence par vérifier le statut actuel avec la commande :

```
sudo ufw status
```

Les commandes d'activation et de configuration sont détaillées dans le le support de cours (CM4) !

1. Première étape : blocage du trafic extérieur

1. En utilisant **`ufw`**, mettre en place le filtrage sur votre serveur avec les règles suivantes :
   - rien ne passe en provenance ou à destination PC des autres binômes (penser à rechercher l'adresse réseau des PC de votre salle) ;
   - de votre PC vers le serveur : tout passe ;
   - de votre serveur vers votre PC : rien ne passe sauf les réponses et **`ssh`** (**`tcp/22`**).
2. Vérifier le bon fonctionnement des règles, en particulier les connexions **`telnet`** (23), **`ssh`** ou **`ftp`** depuis votre PC.
3. Observer les échanges avec **Wireshark**.

2. Deuxième étape : ajout d'un trafic spécifique

1. Autoriser le trafic **`http`** depuis et vers votre serveur.
2. Vérifier le bon fonctionnement des règles.