**Documentation projet pré-TPI**

**Serveur Linux :**

Connexion à internet avec un jeton jetable pour l’authentification.

J’ai créé sur VMware une machine avec 8Gb de RAM, 60 Gb de mémoire et 1 processeur avec 2 cœurs. J’ai ensuite ajouté une image ISO d’un serveur Linux Ubuntu 18.04. J’ai ensuite démarré le serveur et fait une installation normale.

Puis j’ai entré ces commandes :

* sudo apt-get update
* sudo apt-get upgrade
* sudo apt-get install tasksel –y (permet d’installer Ubuntu desktop et d’autres paquets)[[1]](#footnote-1)
* sudo tasksel

A partir d’ici, une image s’ouvre et on peut sélectionner Ubuntu desktop pour un avoir un GUI avec le serveur. L’installation se fait automatiquement et il suffira de rebooter pour que le serveur se lance via le desktop d’Ubuntu.

**Assistant NAS :** <https://www.pcastuces.com/pratique/astuces/5014.htm>

J’ai été télécharger l’assistant NAS pour pouvoir accéder au NAS (il va scanner le réseau). Le fichier se trouve sous : <https://www.synology.com/fr-fr/support/download/DS413j#utilities>

Il faut prendre le fichier pour Ubuntu et ensuite lancer le téléchargement.

**Modification carte eth0 :**

* sudo ifconfig enp0s31f6 172.17.215 netmask 255.255.255.0 up

<https://waytolearnx.com/2019/05/configurer-une-adresse-ip-en-ligne-de-commande-sous-linux.html>

<https://askubuntu.com/questions/704361/why-is-my-network-interface-named-enp0s25-instead-of-eth0>

**Se connecter au NAS + Nettoyage :**

Il faut aller soit sur une page internet et entrer l’IP, soit double cliquer sur le NAS détecter avec l’assistant et une page s’ouvre.

NAS .237 : Admin/Pa$$w0rd 🡪 4x1Tb

NAS .218 : SynoCPNV/Pa$$w0rd 🡪 4x500Gb

Une fois connecté, je vais dans le storage manager et je supprimer tous les volumes dans le but de faire de la place et de créer mes volumes.

Planifier des tâches (redondance) :

<https://www.synology.com/fr-fr/knowledgebase/DSM/help/DSM/AdminCenter/system_taskscheduler>

**Choix architecture réseau :**

*Concernant le NAS :*

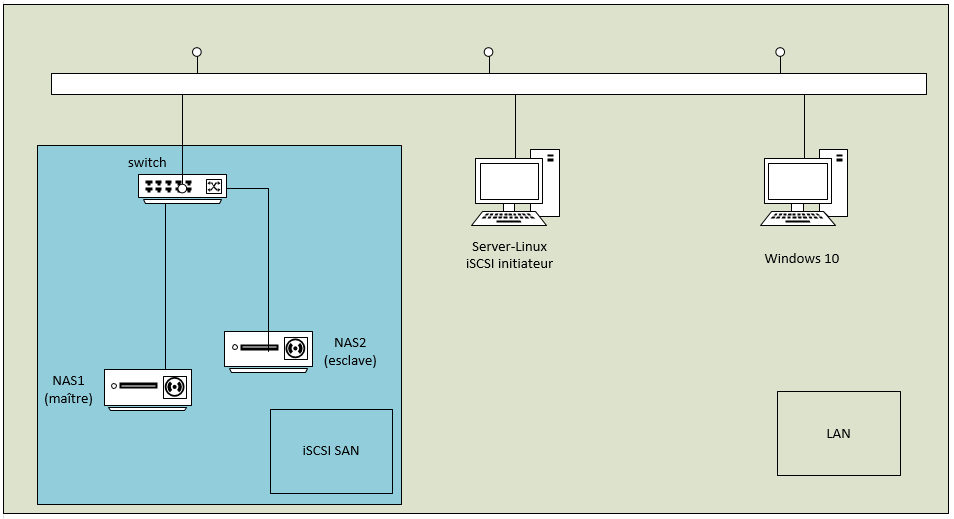
Il y aura un premier NAS, dit maître. C’est-à-dire qu’il va enregistrer la totalité des données sur ces disques durs et il aura à sa charge de dire à l’autre NAS, dit esclave, de faire des backups afin de garantir une redondance pour la sécurité des données.

*Concernant les backups sur le NAS :*

Comme cité précédemment, nous devons garantir une redondance pour la sécurité des données. Dès lors, nous devons gérer une sauvegarde du maître sur l’esclave. Pour cela nous pouvons utiliser une sauvegarde complète suivie d’incrémentielles toutes les 30 secondes. Cela est tout à fait plausible car, comme la sauvegarde est incrémentielle, elle ne va sauvegarder que ce qui a été modifié. Dès lors, comme le réseau est dit petit, il n’y aura pas beaucoup de modifications. Et donc le flux entre les NAS ne sera pas surchargé car la sauvegarde ne va enregistrer que ce qui a été modifié. Et si rien n’est touché, la sauvegarde va le voir et n’enregistrera rien. Et donc aucun flux ne sera utilisé inutilement.

Comme il existe plusieurs baies dans un NAS, une possibilité de créer un RAID est envisageable.

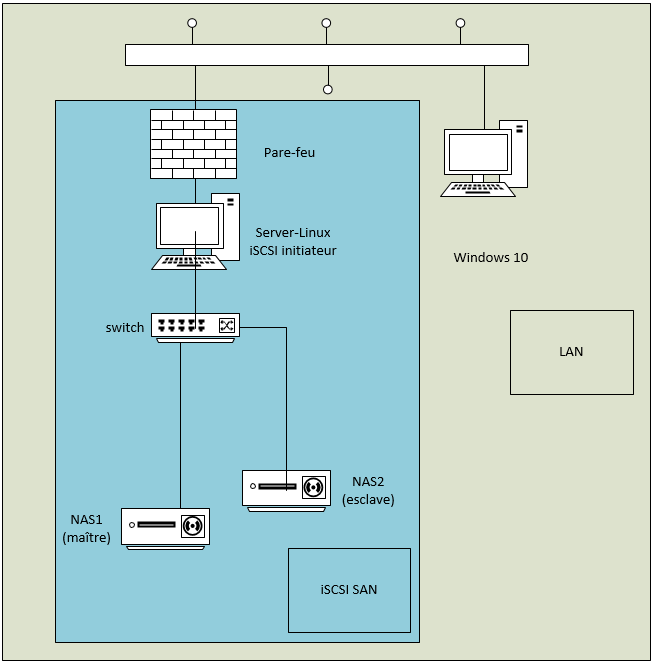
*Schéma logique avec iSCSI SAN ouvert sur le réseau :*



Le SAN pourra notamment être accessible avec un autre client (Windows 10 par exemple).

Nous pouvons voir sur cette architecture que le SAN est accessible par tout le monde. Dès lors cette infrastructure est plausible pour que les fichiers soient atteignables mais il en résulte un manque de sécurité flagrant. En effet, toutes personnes sur le réseau souhaitant faire quelque chose de malveillant, sera capable d’atteindre le SAN et d’utiliser différentes techniques (failles) pour y parvenir. C’est pourquoi il faut une architecture plus sécurisée comme celle présentée en dessous.

*Schéma logique avec iSCSI SAN protégé :*



Ici, nous pouvons constater que le SAN est bien accessible mais qu’il sera protégé par un serveur contenant un pare-feu et ce dernier limitera l’accès au SAN ainsi que les différentes demandes.

Le SAN est donc tout à fait atteignable comme sur le précèdent schéma. Cependant les règles du pare-feu ne permettront pas à la personne de l’atteindre avec des demandes autres que des transferts de fichiers. Et cela augmente donc la sécurité de notre infrastructure SAN.

**Pare-feu :**

<https://www.installerunserveur.com/installer-parefeu-iptables>

1. https://www.techrepublic.com/article/how-to-install-the-gnome-desktop-on-ubuntu-server-18-04/ [↑](#footnote-ref-1)