

Mise en place de stockage SAN en iSCSI dans un environnement Linux



*Sovilla Flavio
Ch. De Brit 15
1462 Yvonand
Flavio.sovilla@cpnv.ch*

SI-CA2a

*vendredi 3 avril
2020*

Table des matières

1	Analyse préliminaire	4
1.1	Introduction	4
1.1.1	Cadre du projet	4
1.1.2	Description du projet	4
1.2	Objectifs	5
1.3	Planification initiale	5
1.4	Structure du dossier	6
2	Analyse	6
2.1	Analyse comparative des solutions envisageables	6
2.1.1	SAN et NAS	6
2.1.2	Protocole iSCSI	7
2.1.3	Architecture réseau	11
2.1.4	Redondance NAS	13
2.1.5	Les RAID	13
2.1.6	Les types de backups	16
2.1.7	Contraintes techniques	17
2.1.8	Justification de la solution retenue	18
2.2	Planification	20
2.3	Stratégie de test	22
3	Conception	23
3.1	Plans topologiques	23
3.1.1	Topologie physique	23
3.1.2	Topologie logique	24
3.1.3	Structures logiques et arborescences	24
3.2	Implémentation matérielle	25
3.2.1	Caractéristiques techniques détaillées	25
3.2.2	Configurations spécifiques	25
3.3	Implémentation logicielle	25
3.3.1	Types de logiciels et de licences	25
3.4	Mise en place de la Sécurité	25
3.4.1	Sécurité appliquée aux utilisateurs	25
3.4.2	Sécurisation de la liaison	25
4	Réalisation et mise en service	26
4.1	Description des tâches effectuées	26
4.1.1	Montage	26
4.1.2	Connexion au service graphique NAS	26
4.1.3	Suppression des anciens éléments	27
4.1.4	Création du RAID5	27
4.1.5	Création des volumes	30
4.1.6	Création d'une LUN iSCSI	35
4.1.7	Connexion Linux – iSCSI LUN	40
4.1.8	Création des dossiers partagés	44

4.1.9	Création des utilisateurs et droits.....	45
4.1.10	Backup des données	49
4.1.11	Haute disponibilité	51
4.2	Modifications apportées par rapport à la conception	59
4.3	Description des tests effectués	60
4.3.1	Matériel.....	60
4.3.2	Réseau	60
4.3.3	iSCSI	61
4.3.4	Droits	61
4.3.5	Backups.....	62
4.3.6	Synchronisation	62
4.4	Problèmes rencontrés et solutions.....	62
4.4.1	Problèmes RAID 5	62
4.4.2	Problèmes mount.....	62
4.4.3	Problèmes compréhensions de LUN	63
4.4.4	Problèmes sécurité CHAP	64
4.4.5	Problèmes de droits.....	64
4.4.6	Problèmes confinement	64
4.4.7	Problème backups	65
4.4.8	Problèmes Synchronisation	65
5	Conclusions	66
6	Annexes.....	67
6.1	Sources – Bibliographie.....	67
6.1.1	iSCSI	67
6.1.2	Sauvegardes.....	67
6.1.3	Utilisateurs, groupes et droits	68
6.1.4	Backups.....	68
6.1.5	Synchronisation	68
6.2	Supports d'archivage du projet	69

1 Analyse préliminaire

1.1 Introduction

1.1.1 Cadre du projet

Le projet sera effectué au CPNV de Ste-Croix dans le cadre d'une préparation au projet TPI (Travail Professionnel Individuel) de fin d'année, qui durera environ 90h. Cette préparation se doit d'être assez proche, c'est pourquoi nous avons à disposition 12 périodes par semaine, ce qui fera un total d'environ 72h sur tout le trimestre. Nous devons notamment rédiger et signer un cahier des charges qui sera vérifié par notre chef de projet. Ce dernier nous suivra pour la totalité du projet et nous guidera si nous nous éloignons trop du chemin prévu pour le projet. Nous devons aussi rendre des comptes rendus à la fin des différents sprints ainsi qu'une documentation complète. Comme vous pouvez le lire, ce projet se rapproche de notre TPI de fin d'année à l'exception des experts et de quelques heures en moins.

1.1.2 Description du projet

Afin de ne pas empiéter sur le projet de fin d'année, j'ai demandé à mon chef de projet de me donner un sujet différent mais qui est en rapport avec le choix que j'avais fait. Dès lors, je me suis vu attribué la tâche de :
« Mettre en place un stockage SAN en iSCSI dans un environnement Linux ».

Cette dernière a pour but d'approfondir mon savoir avec un environnement Linux, tout en gardant un côté réseau et sécurité. En effet, le but sera de créer un réseau SAN avec deux NAS et d'en assurer la sécurité des données avec un système de redondance. De plus, je devrais utiliser un nouveau protocole encore jamais vu, le protocole iSCSI. Nous en avons déjà entendu parler mais nous n'avons jamais vu de quoi il s'agissait. Enfin, il faudra créer une infrastructure sécurisée pour l'environnement du SAN.

La méthode AGILE sera utilisée dans le cadre de ce projet. Des sprints seront créés avec une date butoir. A chaque fin de sprint une entrevue avec le chef de projet se doit d'être faite pour évaluer la situation et apporté en temps réel des modifications sur le projet. Ainsi selon les problèmes ou solutions rencontrés, le planning avec les sprints sera modifié au fur et à mesure de la progression.

1.2 Objectifs

Voici la liste des objectifs à suivre pour la mise en place de la structure du réseau avec iSCSI :

- Analyse du projet et pertinence de la solution choisie
- La solution est fonctionnelle et facile à mettre en œuvre
- Topologie physique et logique du réseau et description du fonctionnement
- Redondance et pertinence de la solution de sauvegarde
- Stratégie de sécurité matérielle, réseau, autorisations des utilisateurs, etc.
- Description et qualité des tests effectués
- Haute disponibilité et explication du mécanisme de synchronisation entre les serveurs

1.3 Planification initiale

Voici le planning initial généré sur Github :

Planning général (13.02.2020 - 03.04.2020) <small>Updated 3 minutes ago</small>	<ul style="list-style-type: none"> • Expliquer et comprendre le protocole iSCSI & Choisir une architecture de réseau • Expliquer et choisir la redondance des NAS & Monter l'infrastructure • Créer la redondance des NAS & tester • Créer le service iSCSI entre le SAN et le serveur 	***
Sprint 1 (27.02.2020) <small>Updated 1 minute ago</small>	<ul style="list-style-type: none"> • Créer le planning sur Github • S'informer, comprendre et expliquer le protocole • Faire un schéma logique • Justifier les différents choix • Y intégrer le protocole iSCSI • Documenter 	***
Sprint 2 (05.03.2020) <small>Updated 2 minutes ago</small>	<ul style="list-style-type: none"> • Expliquer le but d'une redondance • Faire un choix de redondance • Justifier ce choix • Monter l'infrastructure • Documenter le tout 	***
Sprint 3 (13.03.2020) <small>Updated 2 minutes ago</small>	<ul style="list-style-type: none"> • Créer la redondance • Tester la redondance • Documenter les étapes, les tests, les résultats, les problèmes et les solutions 	***
Sprint 4 (03.04.2020) <small>Updated 2 minutes ago</small>	<ul style="list-style-type: none"> • Monter le service iSCSI sur les NAS (target) • Monter le service iSCSI sur le serveur (initiator) • Tester • Documenter le tout 	***

Il est fort probable que ce planning subisse des modifications. En effet, nous ne pouvons savoir à l'avance si certaines tâches sont assez précises concernant le temps consacré. Certaines pourront être faites plus rapidement et d'autres prendront peut-être plus de temps. Ce planning subira donc des modifications au fur et à mesure de l'avancement du projet. Les problèmes rencontrés, les solutions pour y remédier ainsi que la modification du planning seront expliqués plus bas lorsque cela sera nécessaire.

1.4 Structure du dossier

Cette partie peut présenter la façon dont est organisé le document. En quelques lignes, on décrit le contenu des différents chapitres, ce qui permet d'avoir une vue d'ensemble.

Nous allons commencer par une analyse des différents points à aborder qui me semblent important pour la compréhension de la généralité du projet. Nous partirons ensuite sur la conception du projet afin d'expliquer au mieux possible l'idée souhaitée. Après cela, nous partirons sur la construction du projet et pour finir une conclusion pour parler des différents problèmes, solutions et de certains points du projet.

2 Analyse

2.1 Analyse comparative des solutions envisageables

2.1.1 SAN et NAS

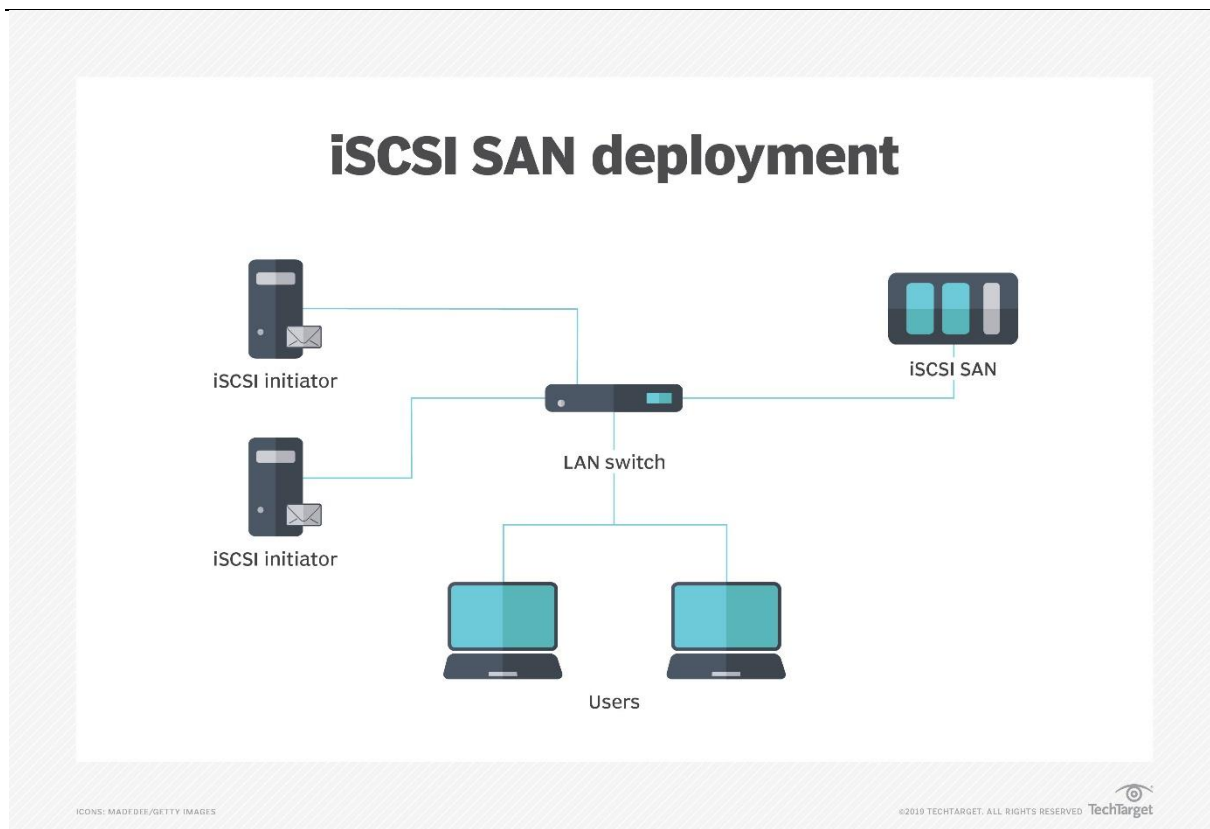
Tout d'abord, avant de se lancer sur ce qu'est le protocole iSCSI, il va falloir comprendre dans quel but nous allons l'utiliser.

Dans notre petit réseau, nous voulons créer ce qui s'appelle un SAN ou Storage Area Network. Ce SAN, sera créé avec l'aide de deux NAS ou Network Attached Storage. Ce sont deux solutions de stockage en réseau, cependant elles diffèrent quant à l'utilisation. En effet, alors que le NAS va offrir un stockage sur de simples fichiers le SAN, lui, va offrir un stockage sur un bloc de disque. Les protocoles sont notamment différents, le SAN va utiliser SCSI, Fibre Channel ou SATA alors que le NAS va utiliser un Serveur de fichiers, NFS ou CIFS. A noter qu'une infrastructure SAN sera plus coûteuse et plus complexe à installer contrairement à son homologue, un NAS, dont l'infrastructure sera moins coûteuse et complexe.

Nous n'allons pas plus nous étendre sur la technologie NAS. Par contre, comme nous allons utiliser la technologie SAN, voici de plus amples explications.

Comme vous avez pu le lire, SAN utilise SCSI. Ce protocole a été amélioré pour donner deux protocoles plus puissants : Fibre Channel et iSCSI (que nous expliquerons plus tard). Ces derniers permettent des débits plus puissants et sur de plus longues distances. Nous pourrons alors connecter plus d'appareils sur le SAN et ils auront tous accès aux différents disques.

Voici un schéma plus explicatif :



Comme vous pouvez le voir, nous retrouvons notre SAN relié à un switch, lui-même relié à des utilisateurs et des iSCSI initiateurs. Ici, notre SAN n'est pas protégé, mais il sert d'espace disque de stockage où tout le monde a accès.

2.1.2 Protocole iSCSI

Comment fonctionne-t-il

Le protocole iSCSI ou internet Small Computer System Interface est un protocole initié en 1990 et lancé sur le marché en 1998. Il a pour but de relier des installations de stockage de données. Il va faciliter le transport des données sur un LAN ou un WAN en utilisant les réseaux IP sur de courtes ou longues distances.

Le fonctionnement est très simple, le client (appelé initiateur), va envoyer une commande SCSI sur des périphériques de stockage utilisant iSCSI (appelés cibles) qui peuvent se trouver en local ou sur des serveurs distants (appelés SAN), qui rassemblent les ressources de stockages en un point unique et offre un disque atteignable pour les clients contenant des fichiers. Une fois que la commande a atteint la cible, cette dernière va la récupérer, la lire, récupérer les informations et pour finir envoyer une réponse à l'initiateur.

Dans le cadre de notre projet, nous allons créer un SAN sur un LAN. Il ne sera atteignable que sur le réseau et non pas l'extérieur (cf. WAN). Un schéma logique du réseau sera présenté plus tard.

L'encapsulation

Voici une image montrant une encapsulation d'un fragment iSCSI :



On constate donc que c'est comme une encapsulation commune du modèle TCP/IP, à l'exception d'iSCSI qui vient se loger avant le segment TCP de la couche protocole (ici, la couche application avec les données est omise).

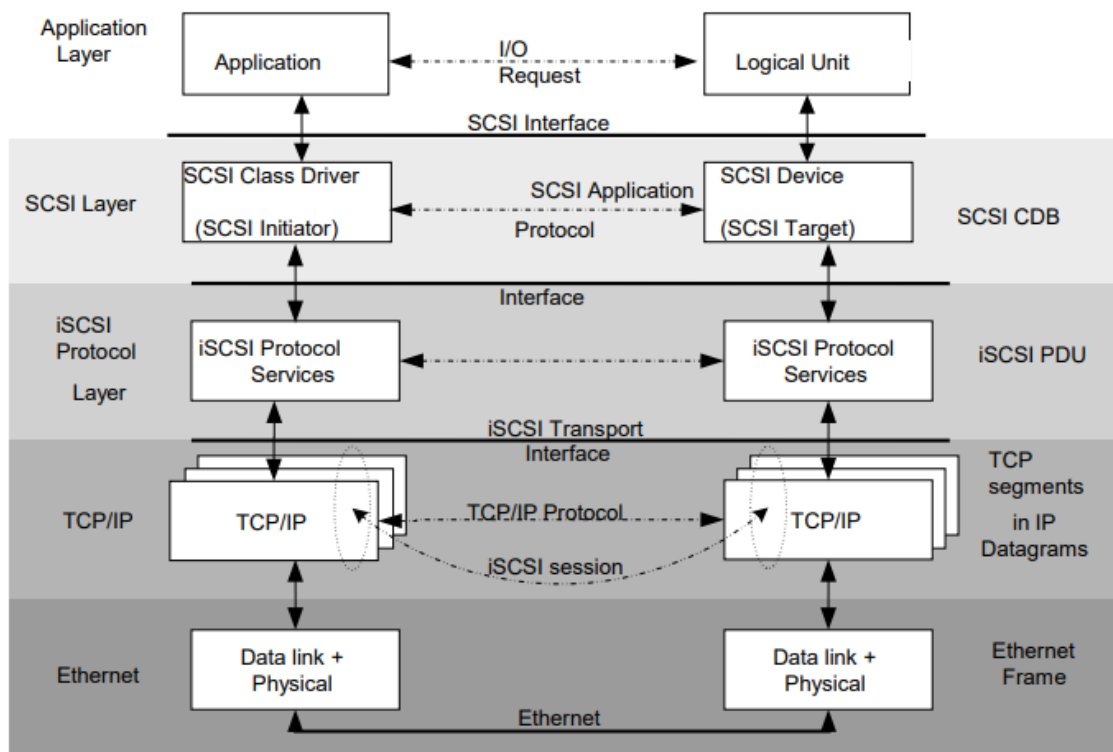
Dans l'ordre d'encapsulation, nous avons :

- iSCSI qui va fournir les instructions d'ordre et de control avec les commandes SCSI et si besoin est, des données supplémentaires.
- iSCSI mis dans un segment avec le protocole TCP (Transmission Control Protocol) qui va permettre un envoi sûr du segment grâce à son protocole de vérification.
- Le segment est ensuite englobé dans un paquet IP, qui va permettre les échanges à distance avec d'autres protocoles à l'intérieur, notamment la possibilité d'une fragmentation du paquet si le flux doit être restreint ou encore le Time to Live pour que le paquet n'encombre pas le réseau.
- Et pour finir le tout s'encapsule dans une trame Ethernet, qui elle, contiendra les adresses MAC pour l'échange de données sur un LAN. A noter que cette trame contient un en-tête avec les informations habituelles comme le préambule, le SFD (Start of Frame Delimiter), ... et une queue de bande (ou FCS, Frame Check Sequence) qui permet la vérification de la trame.

Une fois tout cela encapsulé, la trame est prête à être envoyée en bit sur le réseau physique.

Les couches

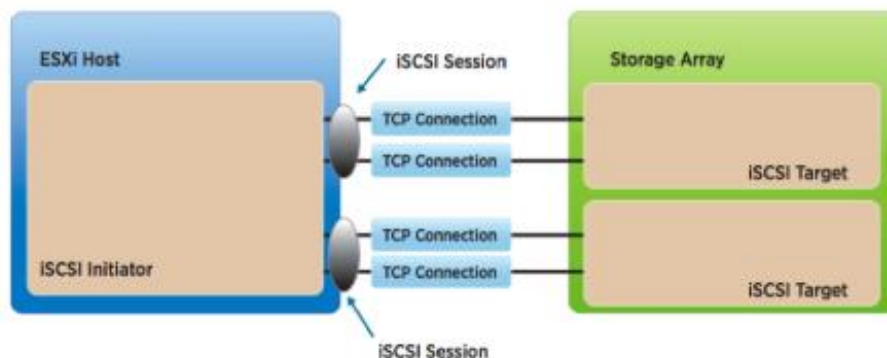
Voici une image montrant les différentes couches d'iSCSI :



Comme vous pouvez le voir, ici nous retrouvons notre encapsulation pas à pas, mais cette fois, avec une vue des différentes couches du protocole TCP/IP. Il y a notamment la couche application qui a été omise lors de l'explication du sous chapitre précédent.

Le petit plus à noter est le SCSI Layer avec le SCSI CDB (Commande description Block) qui se joint entre le protocole iSCSI (qui va encapsuler la commande) et la couche application qui va permettre de donner l'ordre à la couche SCSI. En effet, une fois que nous avons souhaité faire une demande aux disques de notre SAN, SCSI Layer va transformer cette demande afin de garantir l'interopérabilité entre les disques des différents fournisseurs et ainsi garantir un accès quel que soit le support (les commandes SCSI ont été normalisée dans ce but, pour de plus amples informations vous pouvez rechercher la norme ANSI INCITS 408-2005).

Il existe notamment une session iSCSI sur la couche TCP/IP, cette dernière sert à garantir l'échange entre l'initiateur et la cible. Comme mentionné plus haut, iSCSI utilise le protocole TCP pour initier cette session avec un SYN/ACK et va utiliser une iSCSI session ID (ISID) pour l'identification. Il est possible d'avoir de multiples sessions ouvertes entre l'initiateur et la cible comme présenté dans l'image suivante :



Il existe notamment une Connection ID (CID) qui sert à identifier à l'aide d'un ID de connexion (tout est dans le nom) et un Target Session Identifying Handle (TSIH) qui permet de cibler une cible spécifique pour une session avec un nom d'initiateur.

De notre côté, pour présenter les disques aux clients, nous allons utiliser ce qui s'appelle une LUN (Logical Unit Number), qui va nous permettre de mettre un numéro d'identification à notre unité de stockage. Une fois ce numéro attribué, nous avons la possibilité de masquer ou non l'espace de stockage à un serveur en particulier (cela s'appelle le LUN Masking). Mais comme nous ne possédons qu'un serveur et dans le but de simplifier l'infrastructure, nous allons lui attribuer une connexion avec notre numéro de LUN afin qu'il puisse communiquer avec.

Cette LUN va être représentée sur notre serveur comme un disque dur. Nous pourrons faire ce que nous souhaitons dessus et le tout sera sauvegardé sur les NAS. Cependant, il n'est possible de lire les données de la LUN que depuis notre serveur et non sur notre NAS.

La sécurité

Il existe plusieurs méthodes pour sécuriser l'échange d'informations et d'en garantir la sécurité. Nous n'utiliserons bien entendu pas toutes les méthodes car certaines se révèlent être complexes et hors de portée, mais en utilisant les principales, nous serons capables d'offrir des connexions sécurisées à notre SAN.

Voici les méthodes que nous utiliserons :

- **CHAP authentication** : (Challenge-Handshake Authentication Protocol) Permet une authentification pour se connecter à la cible. Il existe aussi le Mutual CHAP qui va exiger une authentification des deux côtés et qui est plus sécurisé.
- **Autorisation** : Une gestion des autorisations en fonction des personnes authentifiées. Ce qu'elles peuvent lire, modifier ou exécuter.
- **Encryptions** : Ajouter une clé d'encryptions (AES-256) sur les dossiers partagés pour en protéger le contenu (attention les clés doivent être gardées).

Quelques autres méthodes qui permettent une sécurité plus performante mais qui demande un travail plus fourni (je n'explique que la fonction principale) :

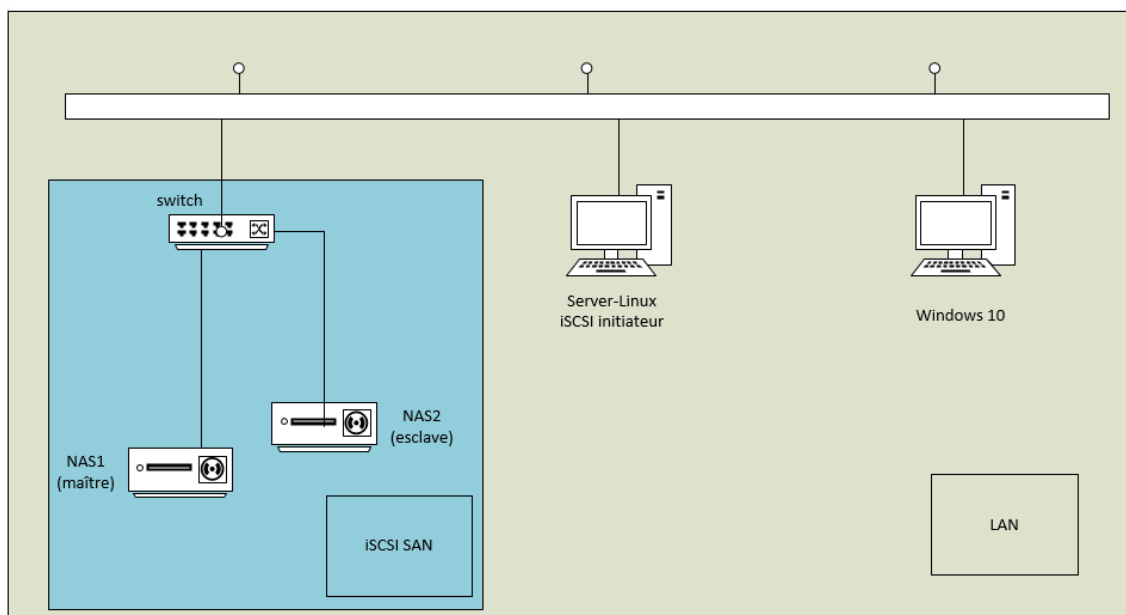
- **RADIUS Authentication** : (Remote Authentication Dial-In user Service) Permet un accès à un serveur pour garantir l'authentification.
- **IPSec Authentication** : Comme le CHAP authentication n'est pas assez sécurisé, ce protocole offre une couche de sécurité supplémentaire sur le paquet de la couche IP.
- **IPSec Encryption** : Pour fortifier l'encryptions des données.

2.1.3 Architecture réseau

Il est possible de créer différentes architectures du réseau. Cependant, nous ne verrons que deux architectures et nous choisirons la plus efficace et complète.

Réseau en BUS

Une possibilité est de monter un réseau en BUS comme ci-dessous.

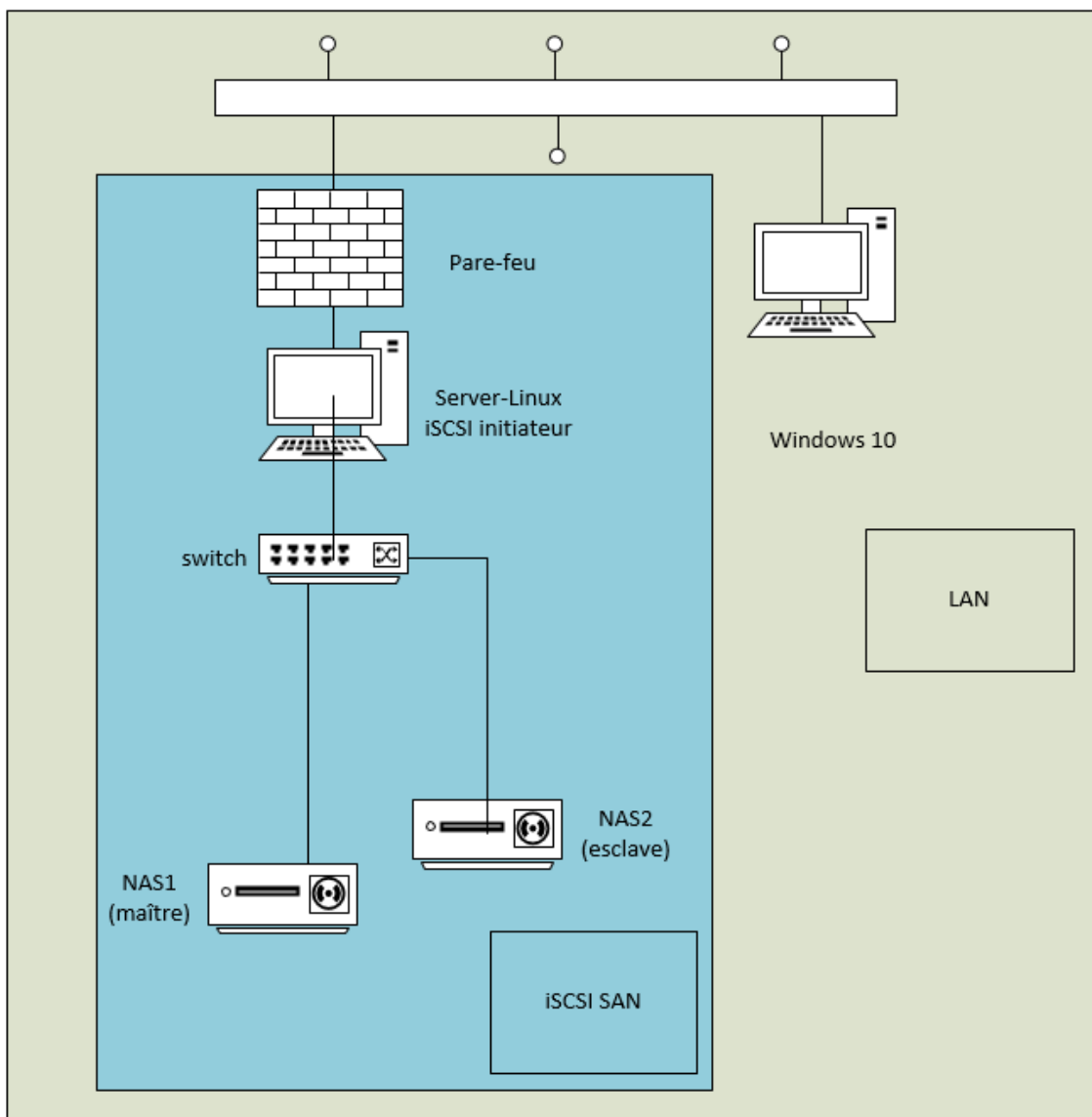


Nous constatons qu'il existe un LAN avec un SAN sur le même réseau. Le SAN est donc ouvert et à portée de tous les utilisateurs sur le réseau. Ce n'est donc pas une bonne idée. En effet, il se peut qu'une personne mal intentionnée ou ne faisant pas exprès perturbe le fonctionnement du SAN et de ce fait le rende inatteignable. La disponibilité et l'intégrité des données du NAS sont donc en « danger ». C'est pourquoi cette disposition n'est pas préconisée.

Réseau Hybride

Contrairement à un simple réseau en BUS, nous allons créer un réseau hybride. Ce dernier sera composé d'une partie en BUS et d'une autre en étoile.

Voici ce que à quoi va ressembler le réseau :



Nous retrouvons ici notre topologie en bus pour le LAN, mais, avec cette fois, une topologie en étoile pour le SAN. Cette disposition, va permettre une plus grande sécurité des données du SAN. Comme vous pouvez le voir, le SAN sera protégé par un pare-feu qui sera capable de gérer les entrées et les sorties avec des règles et ainsi en garantir une plus ample protection.

2.1.4 Redondance NAS

Le principe

Comme vous avez pu le constater, j'ai exprès omis de vous parler des deux NAS dans l'infrastructure du SAN. C'était voulu. En effet, bien qu'à eux deux ils composent le réseau SAN, ils vont servir à notamment créer la redondance. Mais qu'est-ce qu'une redondance ? Le Larousse nous offre une définition plus ou moins exhaustive de ce terme : « En informatique et dans les télécommunications, duplication d'informations afin de garantir leur sécurité en cas d'incident ». Cela paraît presque complet, mais pas tout à fait. Voici une explication plus exhaustive : différents problèmes peuvent survenir sur une machine, une surtension qui provoque un court-circuit, un disque dur usé, une mauvaise manipulation qui efface des dossiers importants, etc... C'est pourquoi en informatique, nous effectuons ce qui s'appelle un backup des informations afin de garantir la sécurité des informations qui sont sur les disques durs. Ce backup se doit d'être redondant afin de perdre le moins de données possibles. C'est-à-dire qu'il faut faire des backups sur des intervalles de temps courts. Grâce à cela, s'il faut récupérer une donnée, il est possible de le faire presque en l'état.

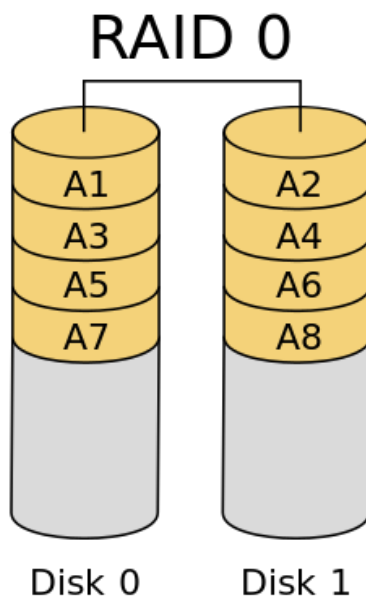
Nous allons donc créer une redondance avec les deux NAS. L'un, dit maître, sera celui sur lequel les informations sont directement stockées. L'autre, dit esclave, servira à enregistrer les backups du maître et en garantir la sécurité avec une redondance. Ainsi si un problème survient sur le maître, nous possédons une réplique de toutes les informations nécessaires sur l'esclave. Et l'inverse est vrai aussi, si l'esclave a un problème, nous pouvons tout retransférer sur ce dernier depuis le maître.

2.1.5 Les RAID

La dernière phrase du paragraphe précédent n'est pas totalement juste. En effet, il faudrait préconiser les problèmes sur l'esclave car il contient tous les backups. Il est donc important de protéger les données sur ses disques (nous utiliserons aussi cette technique sur les disques du maître pour en accroître la sécurité). Pour cela, nous allons faire appel à ce qui s'appelle du RAID. Il en existe différents types : RAID 0, 1, 5, 6 et 10 sont les plus connus. Je vais ici m'attarder que sur le RAID 0, 1 et 5. C'est ce qui nous intéresse le plus. Voici donc une petite explication de ces derniers.

RAID 0

Aussi appelé « volume agrégé par bandes », sa fonctionnalité consiste à augmenter les performances de la grappe (comme plusieurs disques sont utilisés, nous parlons de grappe) car on va utiliser plusieurs disques simultanément. Voici un exemple en image :

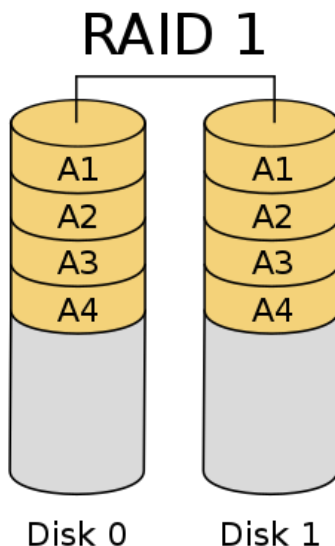


Comme on peut le voir, les informations se divisent sur deux différents disques, formant une grappe, et si nous souhaitons écrire ou lire des informations, ces actions seront faites deux fois plus rapidement. Le gros problème avec cette disposition est qu'il suffit qu'un seul des disques rencontre un problème et ne peut plus être utilisé et c'est la totalité des données qui est perdue. Il est notamment possible d'utiliser plus que deux disques pour créer cette grappe, cependant un minimum de deux est requis.

Concernant l'espace de stockage, celui-ci est donc 'agrandi'. En effet, si nous avons deux disques de 1To, nous aurons 2To d'espace libre pour stocker nos données.

RAID 1

Aussi appelé « miroir », sa fonctionnalité consiste à dupliquer toutes les données. Celles-ci seront alors sécurisées sur deux disques différents. Voici un exemple en image :

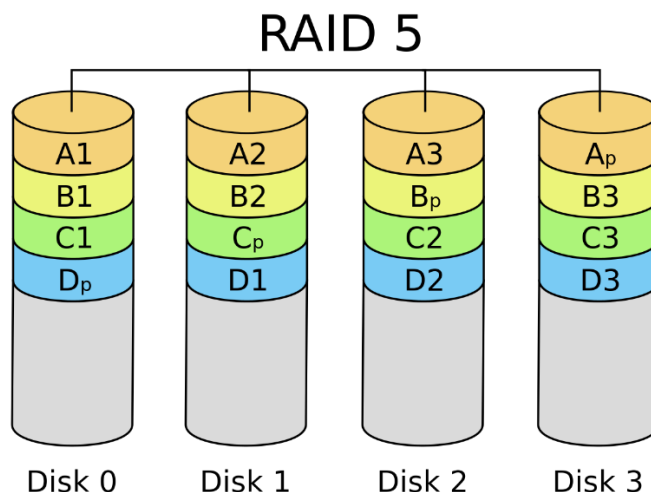


Comme on peut le constater, les informations sont dupliquées et donc, contrairement au RAID 0, elles sont sécurisées en cas de perte d'un des deux disques. Ici, un minimum de deux disques se doit d'être utilisé.

Ici, les données seront 'divisées' comme nous utilisons un disque pour copier le tout. Si nous avons par exemple deux disques de 1To, alors nous n'aurons que 1To d'espace de stockage de données.

RAID 5

Aussi appelé « volume agrégé par bandes à parité répartie ». Cette grappe va utiliser la méthode du RAID 0 et y ajoutée une parité. Voici une image explicative :



Comme on peut le voir sur la première tranche, nous retrouvons la même disposition que le RAID 0, cependant, une parité est ajoutée. Cette dernière va nous servir à reconstruire le tout si un disque est perdu. Ainsi si nous perdons un disque il est possible de tout reconstruire. Cependant, nous ne pouvons perdre qu'un unique disque. En effet, perdre deux disques signifierais la perte de toutes les données. Ici, nous avons une image avec 4 disques mais un minimum de 3 disques est requis pour effectuer ce type de grappe. Pour la vitesse d'écriture, celle-ci est un peu accrue comme pour le RAID 0 mais elle va perdre un peu de sa vitesse à cause de la parité. La vitesse de lecture dépendra de la répartition sur les disques mais elle sera accrue.

Supposons que nous possédons le minimum requis de 3 disques de 1To chacun, alors nous ne posséderons qu'un espace de 2To de données. La parité prendra sera répartie sur les disques mais prendra un tiers des données.

2.1.6 Les types de backups

Il existe trois types de backups. Ils sont tous des fonctionnalités différentes et peuvent être utilisés selon divers besoins.

Complet

Comme son nom l'indique, c'est une sauvegarde complète des données. Elle est donc à utiliser le moins possible. En effet, selon la quantité de données à importer elle peut s'avérer longue. Elle est donc à effectuer lorsque personne ne manipule les données et à ne pas faire tous les jours. Il est conseillé d'en faire une toutes les semaines à un moment où personne ne travaille (durant la nuit du weekend par exemple).

Différentiel

C'est un type de sauvegarde un peu plus complexe. Mais elle va nous permettre de gagner du temps et de l'espace de stockage. Cette technique consiste à ne sauvegarder que les derniers fichiers modifiés depuis le dernier backup complet. On utilisera ensuite ce dernier ainsi que la sauvegarde différentielle pour recréer une sauvegarde complète du jour J avec tous les fichiers modifiés. Nous allons donc à chaque fois faire un backup des nouvelles données en fonction de la sauvegarde complète. Il en adviendra que les données seront de plus en plus 'lourdes' au fil des jours. Cependant il ne faudra qu'une sauvegarde différentielle et la complète pour retrouver toutes les données.

Incrémentiel

Ici, nous avons la technique la plus légère. Cette technique va aussi demander une sauvegarde complète et à partir de celle-ci, faire des backups réguliers. Elle ne prendra en compte que les fichiers modifiés, mais au lieu de prendre référence sur la complète, elle va regarder son ancienne sauvegarde incrémentale. Ainsi elle n'augmentera pas au fil des jours. Le désavantage est qu'il faudra récupérer toutes les données incrémentielles précédentes pour faire une restauration complète. Cependant comme elle prend moins de données en compte, elle nous permettra de n'utiliser que peu de flux pour la sauvegarde et ainsi permettre un backup sur un court instant pour permettre de retrouver les données perdues sur un temps court.

2.1.7 Contraintes techniques

Les premiers risques techniques viennent d'une part du manque de compétences. En effet, n'ayant jamais rien fait avec Linux à part des lignes de commandes pour créer des dossiers ou gérer des droits, il est flagrant qu'une absence de connaissances dans cet OS peut être problématique. À ajouter que c'est la première fois que je rencontre le protocole iSCSI et que je n'en avais jamais entendu parler auparavant.

Mes seules connaissances sont celles de la redondance des sauvegardes pour la sécurité que nous avons déjà un peu travaillée au préalable.

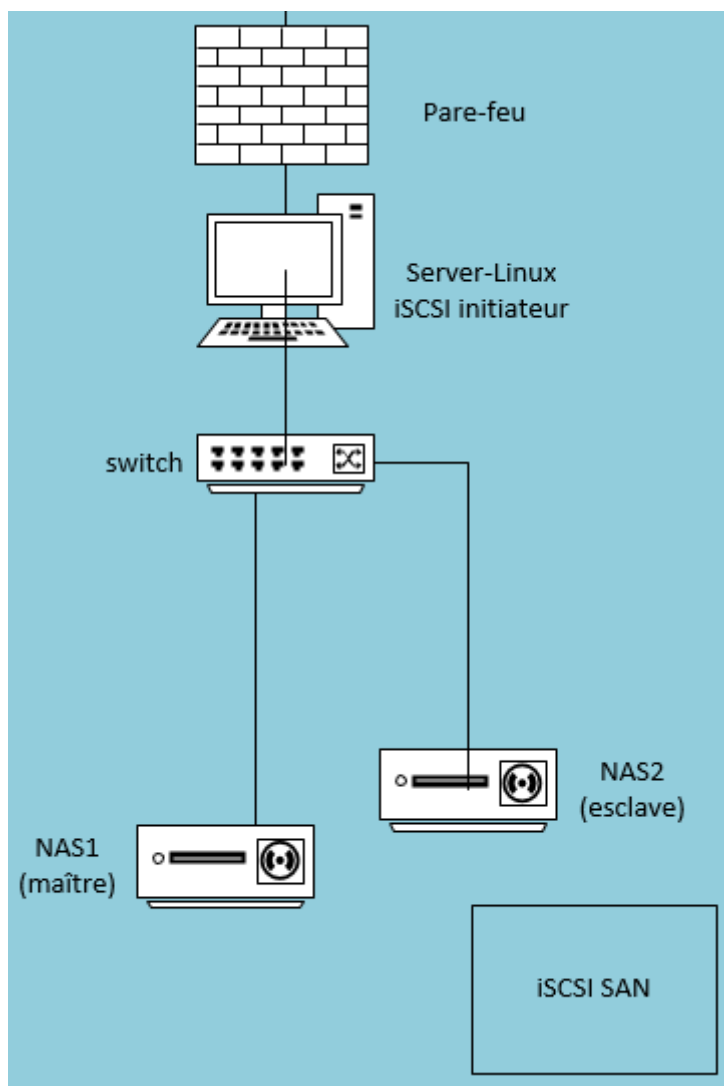
Aucunes actions n'ont été entreprises pour combler ces lacunes. Le but étant de se lancer dans un nouvel environnement et d'essayer de prouver mon indépendance face à une problématique inconnue. Ainsi cela me permettra d'améliorer mes capacités en tant qu'informaticien et développer mes compétences en autodidacte.

2.1.8 Justification de la solution retenue

Le réseau

Pour la construction de notre réseau, nous allons choisir le réseau hybride afin de garantir un minimum de sécurité pour le NAS. Cette topologie est certes un peu plus compliquée à mettre en place que le réseau en BUS mais elle nous permettra d'étendre nos connaissances sur le déploiement d'un réseau plus sécurisé ainsi que nous améliorer dans le domaine du système.

Voici ce à quoi va ressembler le réseau :



Nous aurons toujours la possibilité de l'agrandir, ajouter des ressources et logiciels ainsi que de tester le tout si nous parvenons à tout finir en avance.

Les backups et la redondance

Comme nous possédons quatre disques sur chaque NAS et qu'il est très peu probable que 2 disques cassent en même temps, il serait bien d'opter pour le RAID 5 afin de garantir tout de même une sécurité pour les données mais aussi augmenter la vitesse de lecture et d'écriture sur ceux-ci.

Supposons maintenant que nous n'avons vraiment pas de chance et que deux disques deviennent soudainement défectueux, nous pouvons compter sur notre NAS esclave qui garde nos données bien au chaud. Pour cela une sauvegarde complète (supposons un dimanche soir lorsqu'il y a le plus de chance de personne de travail) suivi d'incrémentielles toutes les 30 secondes pour garantir une récupération immédiate durant la journée et une différentielle le soir ainsi que toutes les heures pendant la nuit (car peu de personnes travaillent de nuit dans une PME).

Voici un petit tableau qui résumerait les sauvegardes :

	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi	Dimanche
00:00	D	D	D	D	D	D	D
01:00	D	D	D	D	D	D	D
02:00	D	D	D	D	D	D	D
03:00	D	D	D	D	D	D	D
04:00	D	D	D	D	D	D	D
05:00	D	D	D	D	D	D	D
06:00	D	D	D	D	D	D	D
07:00	D	D	D	D	D	D	D
Journée	I	I	I	I	I	I	I
20:00	D	D	D	D	D	D	D
21:00	D	D	D	D	D	D	D
22:00	D	D	D	D	D	D	D
23:00	D	D	D	D	D	D	C

C = complète D = différentielle I = Incrémentielle (toutes les 30 sec)

La sécurité

Comme expliqué plus haut, nous n'allons utiliser que les bases de la sécurité pour ce projet. Elles consisteront au CHAP Authentication et à l'autorisation des utilisateurs. Il sera possible d'en modifier et d'en ajouter au fur et à mesure du projet, mais elles resteront les principales sécurités.

Concernant la sécurité d'accès, il est possible de mettre un pare-feu sur le serveur pour augmenter la sécurité, cependant il est fort probable que le temps ne le permette pas, mais tout dépendra de l'avancement du projet.

2.2 Planification

Voici une modification du planning. Les recherches ayant pris moins de temps que prévu, j'ai avancé les dates des premiers sprints (dates auxquelles j'ai fini) et j'ai laissé les autres dates afin de laisser une plus grande marge, mais peut-être que se sera terminé avant.

Planning général (13.02.2020 - 03.04.2020)

🕒 Updated 15 days ago

- Expliquer et comprendre le protocole iSCSI & Choisir une architecture de réseau
- Expliquer et choisir la redondance des NAS & Monter l'infrastructure
- Créer la redondance des NAS & tester
- Créer le service iSCSI entre le SAN et le serveur

Sprint 1 (21.02.2020)

🕒 Updated yesterday



- Créer le planning sur Github
- S'informer, comprendre et expliquer le protocole
- Faire un schéma logique
- Justifier les différents choix
- Y intégrer le protocole iSCSI
- Documenter

Sprint 2 (28.02.2020)

🕒 Updated 11 seconds ago



- Expliquer le but d'une redondance
- Faire un choix de redondance
- Justifier ce choix
- Monter l'infrastructure
- Documenter le tout

Sprint 3 (13.03.2020)

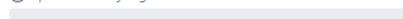
🕒 Updated yesterday



- Créer la redondance
- Tester la redondance
- Documenter les étapes, les tests, les résultats, les problèmes et les solutions

Sprint 4 (03.04.2020)

🕒 Updated 15 days ago



- Monter le service iSCSI sur les NAS (target)
- Monter le service iSCSI sur le serveur (initiator)
- Tester
- Documenter le tout

Après avoir remarqué que la redondance n'était pas possible sans avoir créé les LUN iSCSI, j'ai changé une dernière fois le plan :

Planning général (13.02.2020 - 03.04.2020)

🕒 Updated on 13 Feb

- Expliquer et comprendre le protocole iSCSI & Choisir une architecture de réseau
- Expliquer et choisir la redondance des NAS & Monter l'infrastructure
- Créer la redondance des NAS & tester
- Créer le service iSCSI entre le SAN et le serveur

Sprint 1 (21.02.2020)

🕒 Updated on 27 Feb



- Créer le planning sur Github
- S'informer, comprendre et expliquer le protocole
- Faire un schéma logique
- Justifier les différents choix
- Y intégrer le protocole iSCSI
- Documenter

Sprint 2 (28.02.2020)

🕒 Updated on 28 Feb



- Expliquer le but d'une redondance
- Faire un choix de redondance
- Justifier ce choix
- Monter l'infrastructure
- Documenter le tout

Sprint 3 (13.03.2020)

🕒 Updated 1 minute ago



- Monter le service iSCSI sur les NAS (target)
- Monter le service iSCSI sur le serveur (initiator)
- Tester
- Documenter les différents points

Sprint 4 (03.04.2020)

🕒 Updated now



- Gérer les fichiers et droits
- Créer la redondance
- Tester la redondance
- Documenter les étapes, les tests, les résultats, les problèmes et les solutions

2.3 Stratégie de test

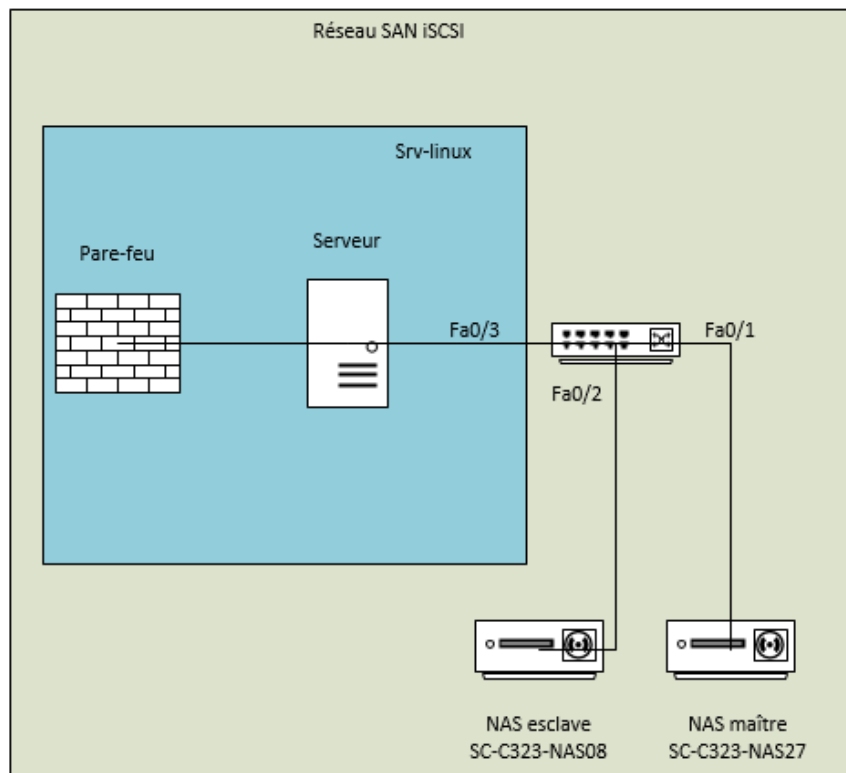
Voici une liste non exhaustive des différents tests à effectuer dans cet ordre :

- Test physique du matériel
 - o Branchement des câbles
 - o Allumage / démarrage fonctionnel
- Test du réseau
 - o Ping entre les diverses machines
- Test iSCSI
 - o Communication entre NAS et Linux
 - o Création de dossiers
- Test de droits
 - o Bons droits sur les dossiers
 - o Accès avec utilisateur
 - o Création fichier ou dossier
- Test de backups
 - o Fichiers sauvegardés
 - o Suppression de fichiers
 - o Restauration

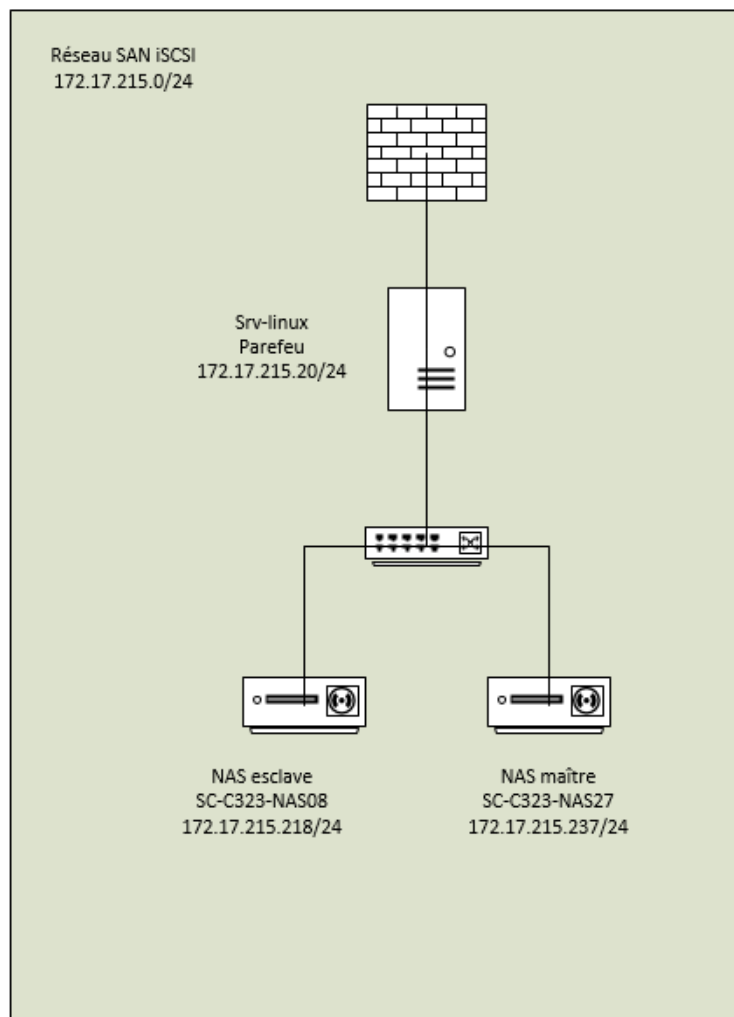
3 Conception

3.1 Plans topologiques

3.1.1 Topologie physique



3.1.2 Topologie logique



3.1.3 Structures logiques et arborescences

Nous créerons un dossier de Partage accessible à tout le monde et qui permettra la gestion des sous-dossiers de chaque branche. Les branches seront : Directeurs, RH, Comptabilité, Ventes et Achats. Il y aura 1 utilisateur par groupe et il aura les droits à son dossier et uniquement son dossier.

3.2 Implémentation matérielle

3.2.1 Caractéristiques techniques détaillées

Pour pouvoir mener à bien ce projet, nous allons avoir besoin du matériel suivant :

- 1x Synology NAS DS413j possédant 4 disques HDD de 1Tbits (4Tbits au total)
- 1x Synology NAS DS413j possédant 4 disques HDD de 500Mbits (2Tbits au total)
- 2x Prises pour alimenter les NAS DS413j
- 1x Switch Netgear GS105 v4 de 5 ports 10/100Mbits (avec alimentation)
- 3x câble RJ-45 pour les connexions
- 1x Ordinateur tour avec un serveur Ubuntu 18.04

3.2.2 Configurations spécifiques

Aucunes configurations spécifiques ne sont requises.

3.3 Implémentation logicielle

3.3.1 Types de logiciels et de licences

- Serveur Ubuntu 18.04 x64
- Synology NAS DS413j avec DSM
- Aucunes licences ne sont requises

3.4 Mise en place de la Sécurité

3.4.1 Sécurité appliquée aux utilisateurs

Les utilisateurs n'auront accès qu'au dossier qui leur est défini en fonction de leur groupe et lorsqu'ils créent un dossier ou fichier, les autres pourront le(s) manipuler à souhait.

3.4.2 Sécurisation de la liaison

Comme le schéma le montre, le serveur « confine » le SAN et ses deux NAS et est capable de gérer tout le trafic entrant et sortant. Il serait donc bien pour la sécurité d'ajouter un pare-feu avec des règles pour que les clients ne puissent pas faire n'importe quoi et surtout n'attaquent pas le SAN. Bien entendu, cela sera rajouté si le temps le permet à la fin de projet.

4 Réalisation et mise en service

4.1 Description des tâches effectuées

4.1.1 Montage

Il faut commencer par monter la petite infrastructure en fonction du model physique. Ici rien de compliquer. Ensuite, on met le tout sur le même réseau. Pour cela, on attribue une adresse IP au serveur Linux pour qu'il soit sous le même réseau que les deux NAS et créer ainsi le réseau SAN iSCSI.

J'ai notamment ajouté au serveur Ubuntu « tasksel ». Ce dernier permet de télécharger un bureau afin de gérer le tout comme sur une machine Windows. Cela va nous permettre de nous connecter au NAS avec une page internet. En effet, il est difficile de tout gérer sur le NAS en ligne de commande (c'est du BSD et ce n'est pas tout à fait les mêmes commandes que sous Ubuntu ou Debian).

Voici comment l'installer :

- `sudo apt-get update`
- `sudo apt-get upgrade`
- `sudo apt-get install tasksel -y` (permet d'installer Ubuntu desktop et d'autres paquets)
- `sudo tasksel`

Une fois tasksel lancé, il nous suffit de sélectionner un desktop avec la barre espace et le tout se charger. Il ne reste plus qu'à attendre.

4.1.2 Connexion au service graphique NAS

Une fois tout cela fait, il faut se connecter aux NAS. Pour se connecter je recommande vivement de télécharger l'assistant NAS¹ qui va nous permettre de trouver tous les NAS sur le réseau. Après il nous suffit de cliquer sur le NAS qu'il a trouvé ou on peut entrer l'adresse IP de chaque NAS dans une barre de recherche internet et on accède à l'interface de connexion. Voici les noms et les mots de passe pour se connecter :

Nom	SC-C323-NAS08	SC-C323-NAS27
IP	172.17.215.218	172.17.215.237
User	Admin	Admin
Mot de passe	Pa\$\$w0rd	Pa\$\$w0rd

Pour simplifier la mise en service, j'ai laissé ces noms, IPs, users et mots de passe. Il est tout à fait possible de changer le tout mais dans notre cas, cela n'est pas très utile.

¹ <https://www.synology.com/fr-fr/support/download/DS413j#utilities>

Attention ! Suite à la reconfiguration des NAS à cause du COVID-19, la configuration des NAS a changé et ils ont dorénavant ces caractéristiques :

Nom	NAS_Master	NAS_Slave	srv-tpi
IP	192.168.1.200	192.168.1.201	192.168.1.199
User	flavio	flavio	flavio
Mot de passe	Pa\$\$w0rd	Pa\$\$w0rd	Pa\$\$w0rd

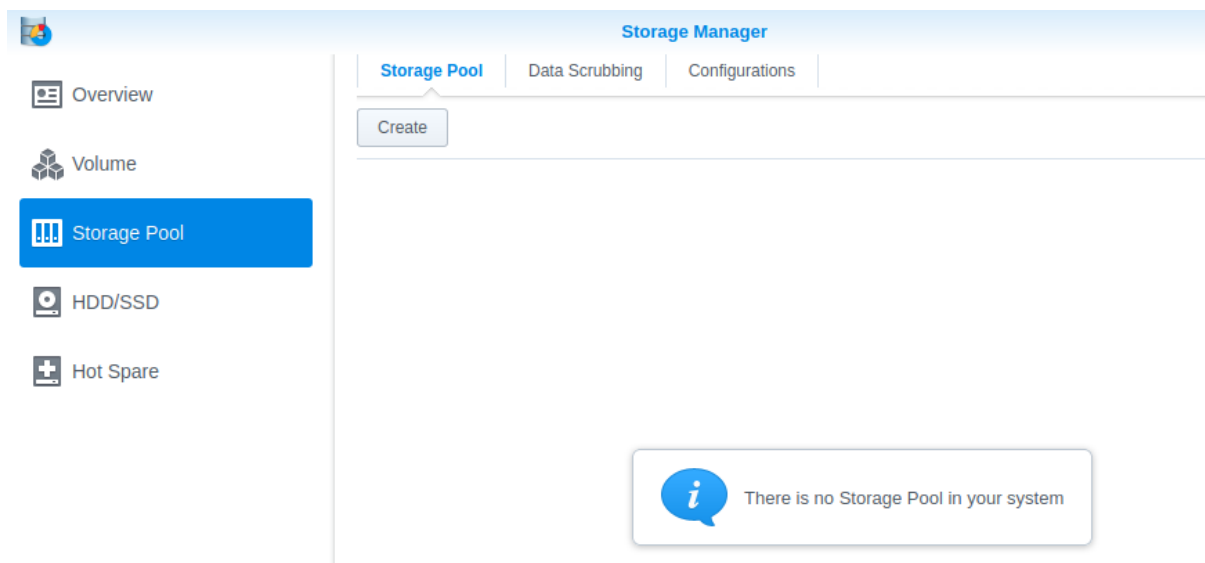
4.1.3 Suppression des anciens éléments

Une fois connecté au NAS, on ouvre le « storage manager » et on va simplement supprimer les volumes existant ainsi que le storage pool pour tout recréer selon nos besoins. S'il n'existe aucun volume de base, cette étape n'est pas nécessaire.

4.1.4 Création du RAID5

Il faut maintenant créer un RAID5 avec les différentes baies disponibles. Voici les étapes à suivre pour faire cela :

Il faut se rendre sur le Storage Manager et créer un pool :



Comme on va sélectionner plusieurs disques on prend cette option :

Storage Pool Creation Wizard

Select storage pool type

Please select the type of storage pool you want to create. You can create a RAID on either type.

☐ Better performance

This type of storage pool supports only a single volume but provides better performance.

Note: The maximum volume capacity of this model is 16 TB. The drive space may not be fully used because this type of storage pool only supports single volume.

☒ Higher flexibility

This type of storage pool supports multiple volumes, allowing higher flexibility in space allocation.

Note: Supports Synology Hybrid RAID.

Next Cancel

Sélectionner tous les disques :

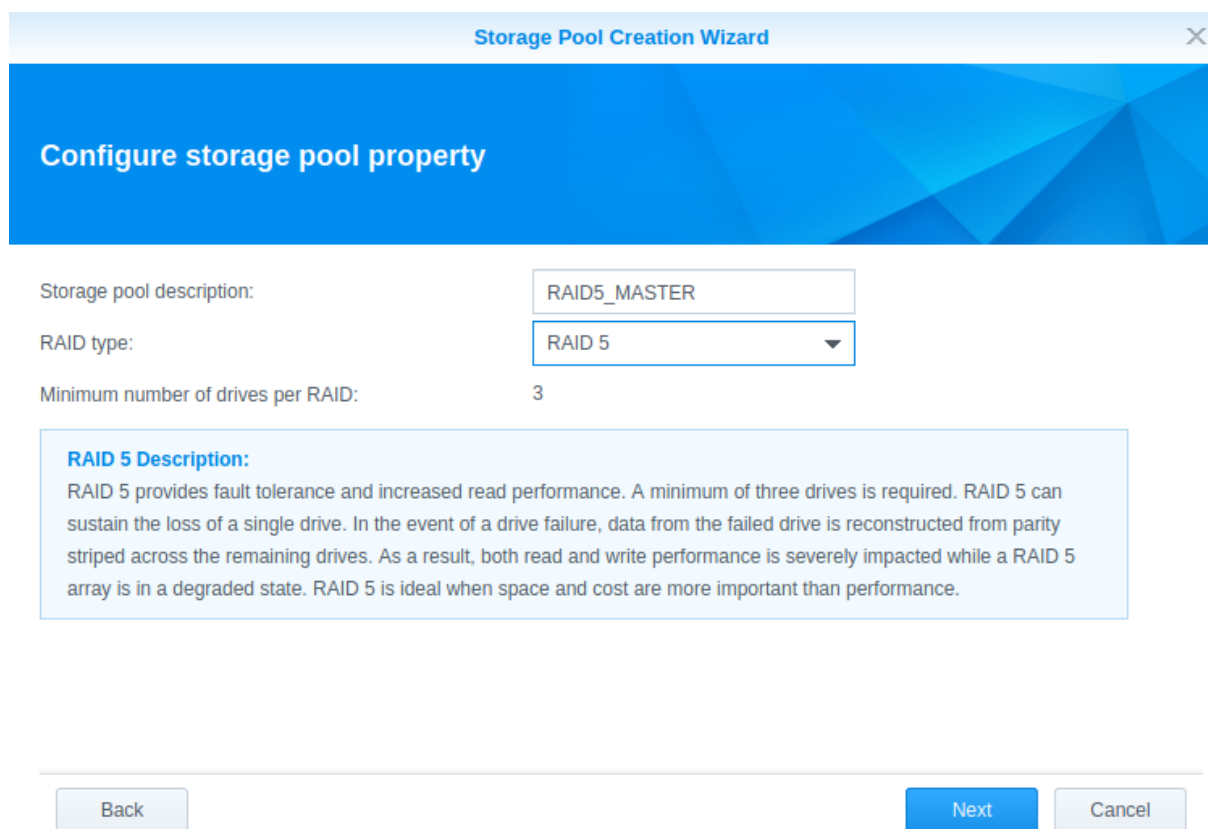
Storage Pool Creation Wizard

Choose drives

<input checked="" type="checkbox"/>	Number	Model	Drive Type	4K ...	Drive Size
<input checked="" type="checkbox"/>	Drive 1	WD10EZEX-75ZF5A0	HDD	No	931.51 GB
<input checked="" type="checkbox"/>	Drive 2	WD10EZEX-75ZF5A0	HDD	No	931.51 GB
<input checked="" type="checkbox"/>	Drive 3	WD10EZEX-75ZF5A0	HDD	No	931.51 GB
<input checked="" type="checkbox"/>	Drive 4	WD10EZEX-75ZF5A0	HDD	No	931.51 GB

Back Next Cancel

On choisit ensuite de faire un RAID5 qu'on nomme RAID5_MASTER :



The screenshot shows a window titled "Storage Pool Creation Wizard" with a close button (X) in the top right corner. The main heading is "Configure storage pool property". Below this, there are three configuration fields:

- "Storage pool description:" with a text input field containing "RAID5_MASTER".
- "RAID type:" with a dropdown menu showing "RAID 5".
- "Minimum number of drives per RAID:" with a numeric input field containing "3".

Below these fields is a light blue box titled "RAID 5 Description:" containing the following text:

RAID 5 provides fault tolerance and increased read performance. A minimum of three drives is required. RAID 5 can sustain the loss of a single drive. In the event of a drive failure, data from the failed drive is reconstructed from parity striped across the remaining drives. As a result, both read and write performance is severely impacted while a RAID 5 array is in a degraded state. RAID 5 is ideal when space and cost are more important than performance.

At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel". The "Next" button is highlighted in blue.

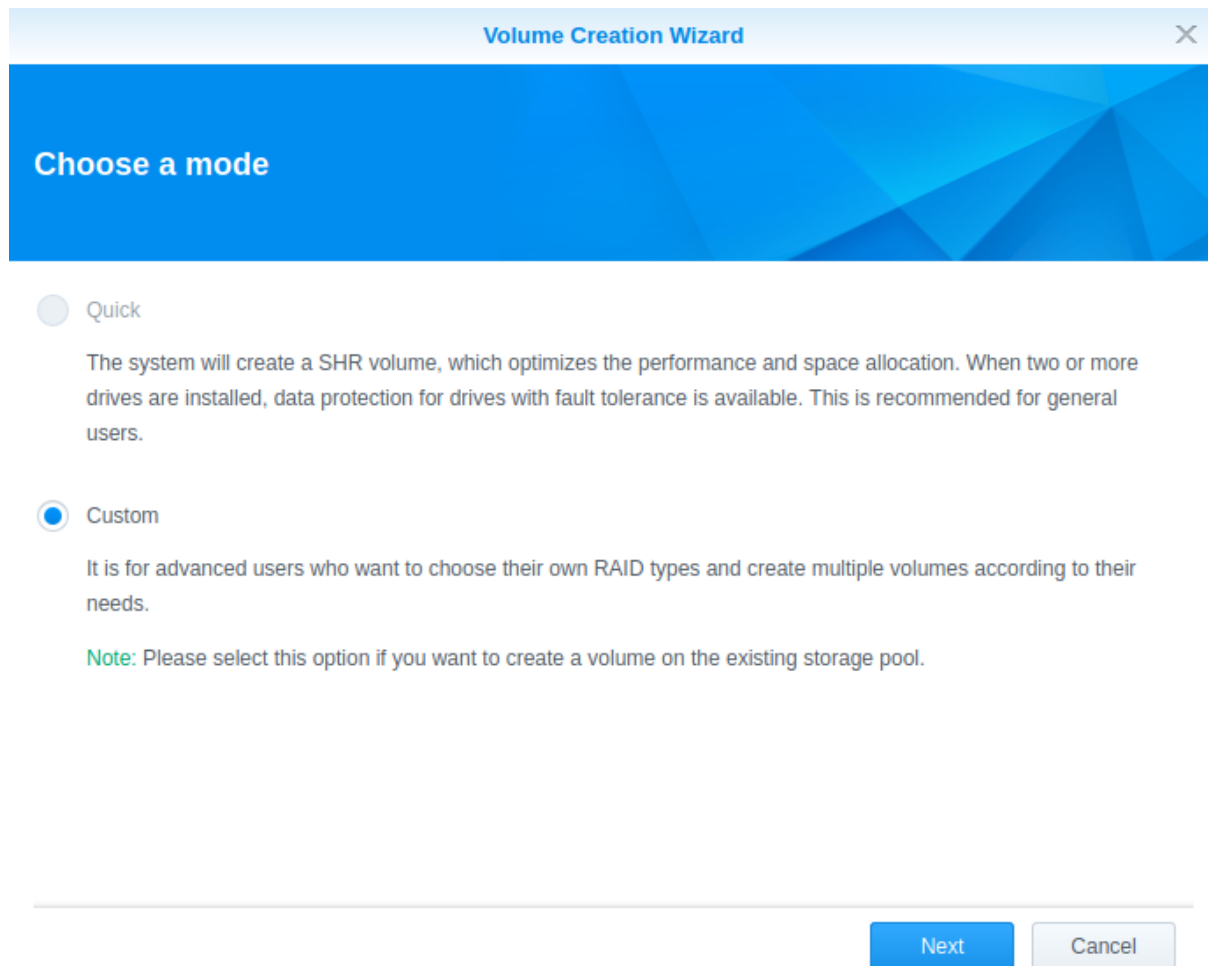
On clique ensuite sur « Next » et on applique. Rien de plus simple ! Il faudra notamment refaire cette opération avec le second NAS qu'on nommera cette fois-ci RAID5_ESCALVE.

Pour que les RAID5 se mettent en place, le NAS va vérifier les bits de parité et cela peut prendre quelques minutes.

4.1.5 Création des volumes

On peut maintenant créer le volume qui nous servira à stocker les différents dossiers/fichiers.

On choisit custom pour créer un volume avec notre RAID5 :



The image shows a 'Volume Creation Wizard' window. The title bar says 'Volume Creation Wizard' with a close button. The main area has a blue header with the text 'Choose a mode'. Below this, there are two radio button options. The first is 'Quick', which is unselected. The second is 'Custom', which is selected. Below the 'Custom' option, there is a note: 'Note: Please select this option if you want to create a volume on the existing storage pool.' At the bottom right, there are two buttons: 'Next' and 'Cancel'.

Volume Creation Wizard

Choose a mode

☐ Quick

The system will create a SHR volume, which optimizes the performance and space allocation. When two or more drives are installed, data protection for drives with fault tolerance is available. This is recommended for general users.

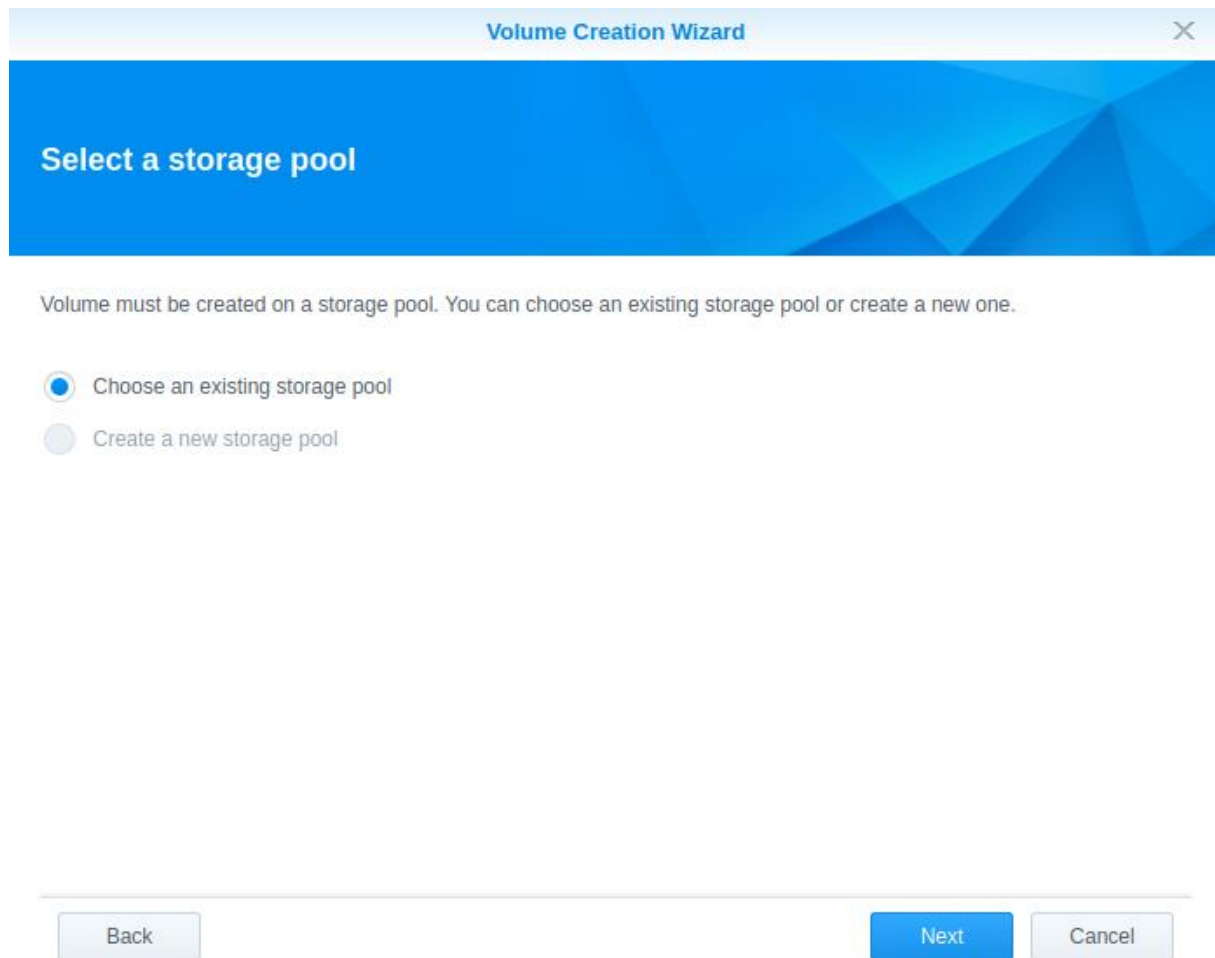
☒ Custom

It is for advanced users who want to choose their own RAID types and create multiple volumes according to their needs.

Note: Please select this option if you want to create a volume on the existing storage pool.

Next Cancel

On choisit un storage pool existant :



The image shows a 'Volume Creation Wizard' dialog box. The title bar is light blue with the text 'Volume Creation Wizard' and a close button (X). The main content area has a blue header with the text 'Select a storage pool'. Below this, a message states: 'Volume must be created on a storage pool. You can choose an existing storage pool or create a new one.' There are two radio button options: 'Choose an existing storage pool' (which is selected) and 'Create a new storage pool'. At the bottom, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

Volume Creation Wizard

Select a storage pool

Volume must be created on a storage pool. You can choose an existing storage pool or create a new one.

☒ Choose an existing storage pool

☐ Create a new storage pool

Back Next Cancel

On sélectionne le RAID5 que nous avons créé :

Volume Creation Wizard

X

Select a storage pool

Storage pool:

Storage Pool 1 (RAID 5) ▼

RAID type:

RAID 5 (With data protection)

Multiple volume support:

Yes

Total capacity:

2.72 TB

Available capacity:

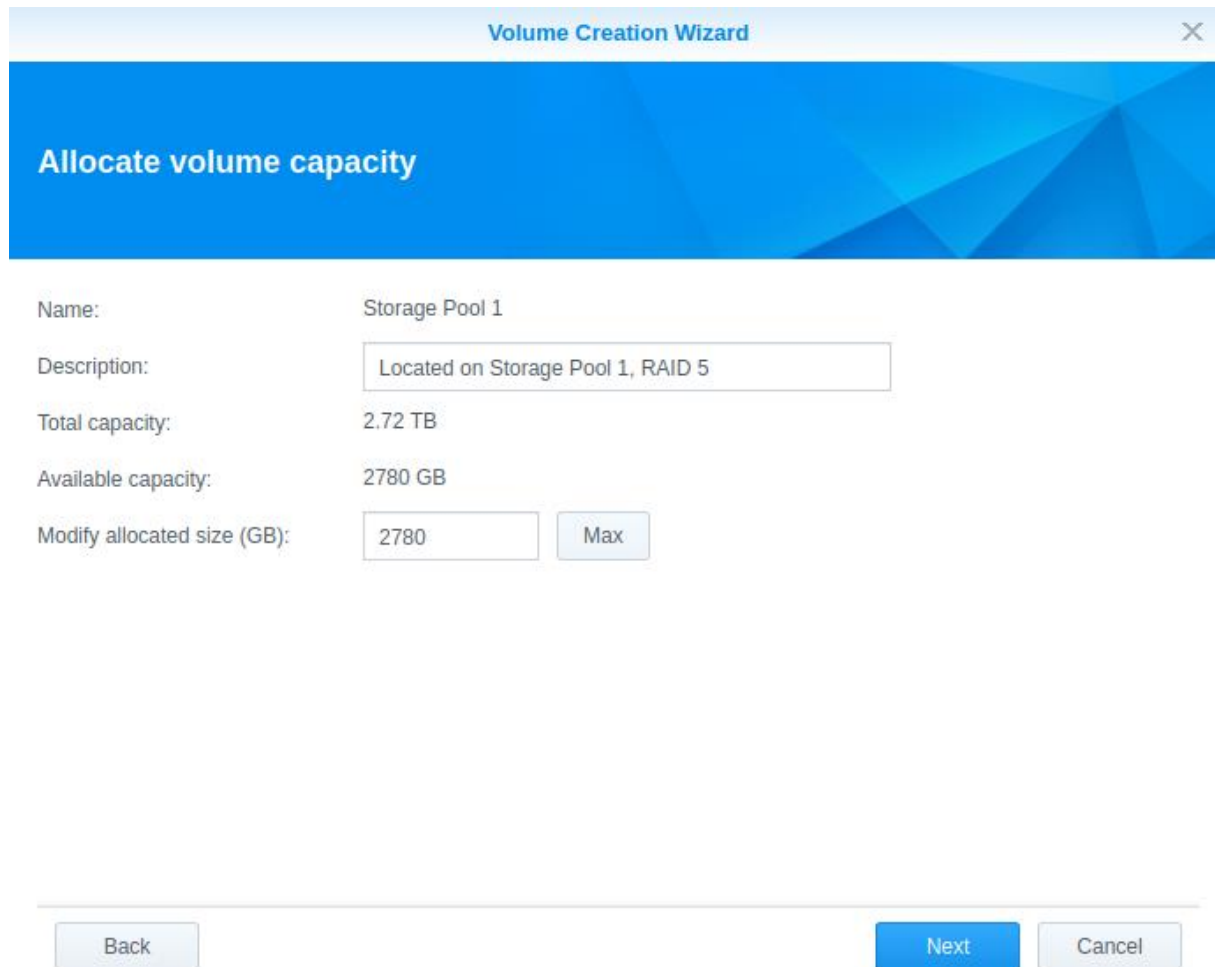
2.72 TB

Back

Next

Cancel

On choisit sa description et modifie son allocation si l'on souhaite faire d'autres volumes :



The image shows a 'Volume Creation Wizard' window with a blue header and a light blue body. The title bar says 'Volume Creation Wizard' with a close button. The main heading is 'Allocate volume capacity'. Below this, there are several fields and buttons:

- Name:** Storage Pool 1
- Description:** Located on Storage Pool 1, RAID 5
- Total capacity:** 2.72 TB
- Available capacity:** 2780 GB
- Modify allocated size (GB):** 2780 (with a 'Max' button next to it)

At the bottom, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

Ensuite on applique le tout et le volume se crée tout seul :

Volume Creation Wizard

Confirm settings

The wizard will apply the following settings. The process will take a few seconds.

Item	Value
Usage	Volume
Storage pool	Storage Pool 1
Allocated capacity	2780 GB
Volume description	Located on Storage Pool 1, RAID 5

Back

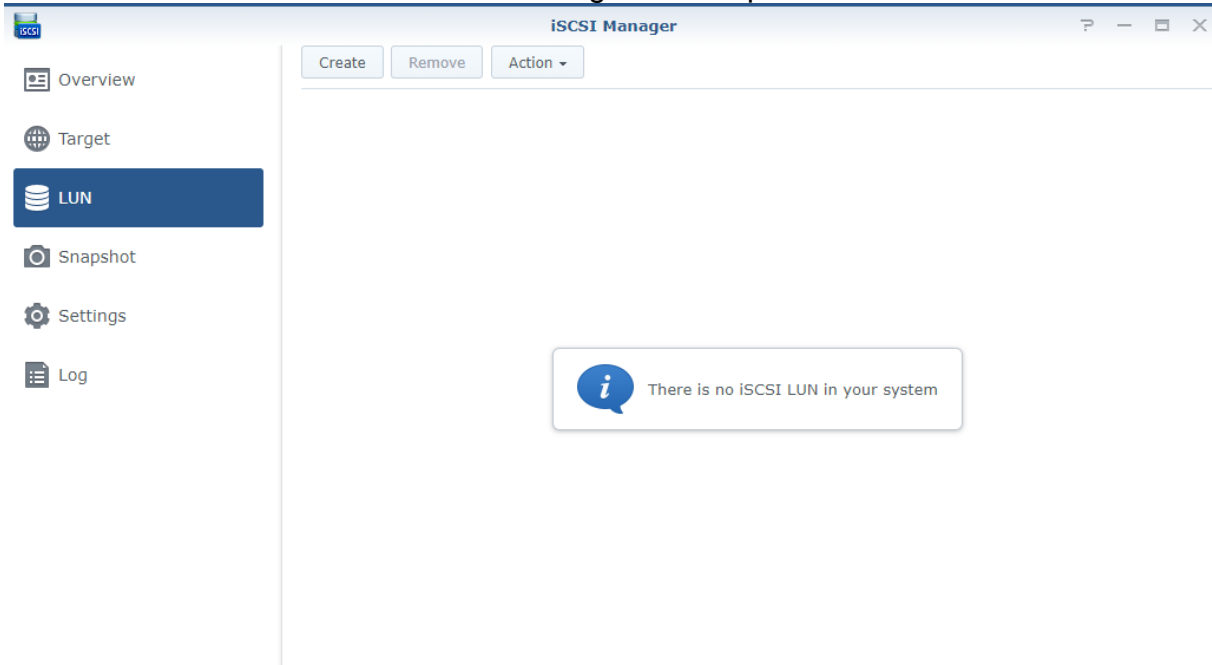
Apply

Cancel

4.1.6 Création d'une LUN iSCSI

Nous allons maintenant créer une LUN iSCSI qui va nous permettre d'avoir un disque virtuel dans le serveur qui sera relié au NAS.

Premièrement allez dans l' « iSCSI Manager » et cliquer sur create :



Ensuite, il faut paramétrer sa LUN :

The screenshot shows the 'iSCSI LUN Creation Wizard' window. On the left is a sidebar with navigation links: Overview, Target, LUN (selected), Snapshot, Settings, and Log. The main area is titled 'Set up iSCSI LUN Properties' and contains the following fields:

- Name: LUN-Master
- Location: Volume 1 (Available: 187 GB) - btrfs
- Capacity (GB): 50
- Thin Provisioning: No
- Advanced LUN features: No

Below these fields is a light blue box with the title 'What are Advanced LUN features?'. It contains the text: 'Advanced LUN features include the support for LUN snapshot and replication, VMware VAAI, and Windows ODX. Please note that enabling this option may affect I/O performance.' Below this is a green note: 'Note: ext4 volumes support only legacy Advanced LUN features. LUNs on Btrfs volumes with Advanced LUN features are recommended due to their instant snapshots and faster cloning capabilities.' At the bottom right of the wizard are 'Next' and 'Cancel' buttons.

On choisit le volume créé et la capacité (max 250 GB avec notre serveur).

On crée ensuite une cible iSCSI (elle permettra la connexion avec notre serveur) :

The screenshot shows the 'iSCSI LUN Creation Wizard' window. On the left is a sidebar with navigation links: Overview, Target, LUN (selected), Snapshot, Settings, and Log. The main panel has a blue header 'Set up iSCSI LUN Mapping'. Below the header, it says 'You can choose to map a target to the LUN now or after the creation of the LUN.' There are three radio button options: 'Create a new iSCSI target' (selected), 'Map existing iSCSI targets', and 'Map later.'. Under 'Map existing iSCSI targets', there is a text box and a dropdown arrow, with the note 'Mapped targets will not be shown in the list.' At the bottom are 'Back', 'Next', and 'Cancel' buttons.

iSCSI LUN Creation Wizard

Set up iSCSI LUN Mapping

You can choose to map a target to the LUN now or after the creation of the LUN.

- ☒ Create a new iSCSI target
Create a new target and map it to this LUN.
- ☐ Map existing iSCSI targets
Mapped targets will not be shown in the list.
 ▼
- ☐ Map later.

[Back](#) [Next](#) [Cancel](#)

On rentre un nom et on modifie l'IQN :

iSCSI LUN Creation Wizard

Create a new iSCSI target

Name: Target-Master

IQN: iqn.2000-01.com.synology:Master.1

☐ Enable CHAP

Name:

Password:

Confirm password:

☐ Enable Mutual CHAP

Name:

Password:

Confirm password:

Back **Next** **Cancel**

On laisse le début (iqn.2000-01.com.synology:) et on ne change que la fin pour mettre « Master.1 ».

On applique le tout et notre LUN iSCSI sera créée :

iSCSI LUN Creation Wizard

Confirm Settings
The wizard will apply the following settings. The process will take a few seconds.

Item	Value
Name	LUN-Master
Location	Volume 1 (Available: 187 GB) - btrfs
Capacity	50 (GB)
Thin Provisioning	No
Advanced LUN fe...	No
Name	Target-Master
IQN	iqn.2000-01.com.synology:Master.1
Authentication	None

Back Apply Cancel

On refait la même procédure avec le second synology. Pour le nom j'ai mis « LUN-Slave » et pour l'IQN j'ai mis la fin en « Slave.1 ».

4.1.7 Connexion Linux – iSCSI LUN

Il faut entrer les commandes suivantes sur le serveur Linux :

- sudo apt-get install open-iscsi (pour installer iscsi)
- sudo ln -s /etc/{iscsid.conf,initiatorname.iscsi} /etc/iscsi/ (pour lier 2 fichiers)
- sudo nano /etc/iscsi/iscsid.conf

```
flavio@srv-tpi:~$ sudo apt-get install open-iscsi
[sudo] password for flavio:
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
open-iscsi est déjà la version la plus récente (2.0.874-5ubuntu2.7).
open-iscsi passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
flavio@srv-tpi:~$ ln -s /etc/{iscsid.conf,initiatorname.iscsi} /etc/iscsi/
ln: failed to create symbolic link '/etc/iscsi/iscsid.conf': File exists
ln: failed to create symbolic link '/etc/iscsi/initiatorname.iscsi': File exists
```

Dans ce dossier il faudra mettre le node.startup en automatique :

```
GNU nano 2.9.3 /etc/iscsi/iscsid.conf Modified

# Startup settings
#*****

# To request that the iscsi initd scripts startup a session set to "automatic".
node.startup = automatic
#
# To manually startup the session set to "manual". The default is manual.
# node.startup = manual

# For "automatic" startup nodes, setting this to "Yes" will try logins on each
# available iface until one succeeds, and then stop. The default "No" will try
# logins on all available ifaces simultaneously.
node.leading_login = No

# *****
# CHAP Settings
# *****

# To enable CHAP authentication set node.session.auth.authmethod
# to CHAP. The default is None.
#node.session.auth.authmethod = CHAP

# To set a CHAP username and password for initiator

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File  ^\ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line

> flavio : sudo
```


Et mettre aussi le `node.session.nr_sessions` à 2.

```
# For multipath configurations, you may want more than one session to be
# created on each iface record. If node.session.nr_sessions is greater
# than 1, performing a 'login' for that node will ensure that the
# appropriate number of sessions is created.
node.session.nr_sessions = 2
```

- `sudo /etc/init.d/open-iscsi restart` (on restart iscsi)
- `sudo iscsiadm -m discovery -t sendtargets -p 192.168.1.200` (pour découvrir la LUN du NAS_Master créée auparavant)

```
flavio@srv-tpi:~$ sudo /etc/init.d/open-iscsi restart
[ ok ] Restarting open-iscsi (via systemctl): open-iscsi.service.
flavio@srv-tpi:~$ sudo iscsiadm -m discovery -t sendtargets -p 192.168.1.200
192.168.1.200:3260,1 iqn.2000-01.com.synology:Master.1
[2a02:1205:503c:5990:211:32ff:fe2c:a700]:3260,1 iqn.2000-01.com.synology:Master.1
[fe80::211:32ff:fe2c:a700]:3260,1 iqn.2000-01.com.synology:Master.1
```

On voit qu'elle a bien été trouvée et on retrouve notre IQN avec la fin en Master.1.

- `sudo iscsiadm --mode node --targetname iqn.2000-01.com.synology:Master.1 --portal 192.168.1.200:3260 --login` (pour se connecter à la LUN)

```
flavio@srv-tpi:~$ sudo iscsiadm -m node --targetname iqn.2000-01.com.synology:Master.1 -
p 192.168.1.200:3260 --login
Logging in to [iface: default, target: iqn.2000-01.com.synology:Master.1, portal: 192.16
8.1.200,3260] (multiple)
Login to [iface: default, target: iqn.2000-01.com.synology:Master.1, portal: 192.168.1.2
00,3260] successful.
flavio@srv-tpi:~$
```

On est dorénavant connecté à notre LUN du NAS et on peut la retrouver sur un disque.

- `sudo fdisk -l` (pour retrouver notre disque monter avec la LUN)

```
Disk /dev/sdb: 50 GiB, 53687091200 bytes, 104857600 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
flavio@srv-tpi:~$
```

On retrouve notre disque de 50 Gb, mais il n'est pas encore monté et donc inutilisable.

- `sudo fdisk /dev/sdb` (pour aller sur le lien du disque de la LUN)

```
flavio@srv-tpi:~$ sudo fdisk /dev/sdb

Welcome to fdisk (util-linux 2.31.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xa93c2f6e.

Command (m for help):
```

Ici, à l'aide de lettres dans la commande on peut créer et partitionner un disque.

- n (pour créer une partition GPT et on laisse tout par défaut)

```
flavio@srv-tpi:~$ sudo fdisk /dev/sdb

Welcome to fdisk (util-linux 2.31.1).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0xa93c2f6e.

Command (m for help): n
Partition type
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
Select (default p):
```

Et on laisse le reste par défaut.

```
Command (m for help): n
Partition type
  p   primary (0 primary, 0 extended, 4 free)
  e   extended (container for logical partitions)
Select (default p):

Using default response p.
Partition number (1-4, default 1):
First sector (2048-104857599, default 2048):
Last sector, +sectors or +size{K,M,G,T,P} (2048-104857599, default 104857599):

Created a new partition 1 of type 'Linux' and of size 50 GiB.

Command (m for help):
```

- w (pour enregistrer)

```
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

flavio@srv-tpi:~$
```

Voilà, notre partition est créée !

- sudo fdisk -l (on retrouve notre partition)

```
Disk /dev/sdb: 50 GiB, 53687091200 bytes, 104857600 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xa93c2f6e

Device      Boot Start      End  Sectors  Size Id Type
/dev/sdb1                2048 104857599 104855552  50G 83 Linux

flavio@srv-tpi:~$
```

On la retrouve sous /dev/sdb1.

- `sudo mkfs.ext4 /dev/sdb1` (pour formater et mettre au bon format, ici ext4)

```
flavio@srv-tpi:~$ sudo mkfs.ext4 /dev/sdb1
mke2fs 1.44.1 (24-Mar-2018)
Creating filesystem with 13106944 4k blocks and 3276800 inodes
Filesystem UUID: f28d631e-6e38-49a6-9d9b-f3bb16b1984e
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424

Allocating group tables: done
Writing inode tables: done
Creating journal (65536 blocks): done
Writing superblocks and filesystem accounting information: done
```

La connexion iSCSI se refait automatiquement au démarrage, cependant le NAS doit être atteignable et cela peut prendre quelques minutes (environ 2 min. pour ma part).

Maintenant que nous avons notre partition, il la monter sur un fichier.

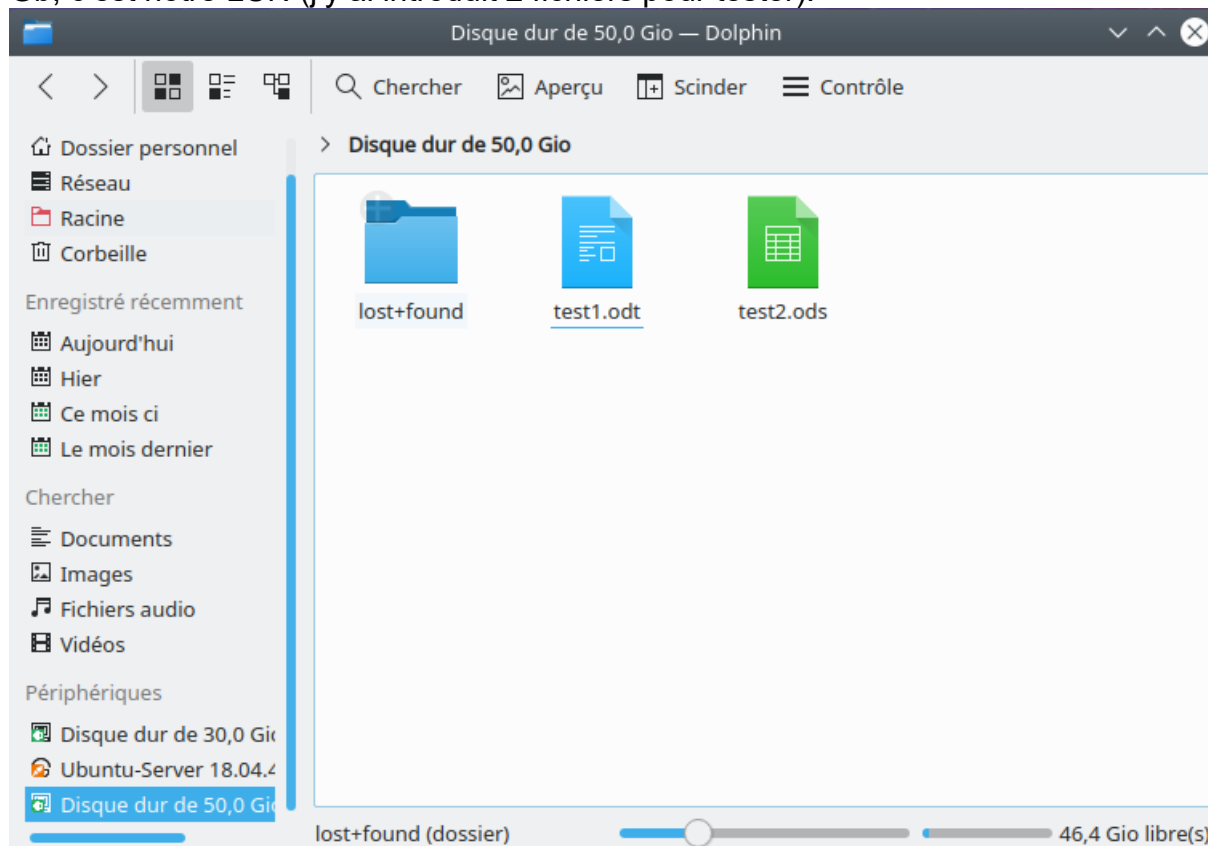
- `sudo mkdir /home/flavio/iSCSI` (On crée un dossier pour la liaison)
- `sudo mount /dev/sdb1 /home/flavio/iSCSI` (on monte la LUN et le dossier)

```
flavio@srv-tpi:~$ sudo mount /dev/sdb1 /home/flavio/iSCSI/
flavio@srv-tpi:~$
```

- `sudo chown -R flavio :flavio /home/flavio` (pour redonner les droits sur iSCSI et ne plus avoir que du root)

```
flavio@srv-tpi:~$ sudo chown -R flavio:flavio /home/flavio/
flavio@srv-tpi:~$
```

Nous pouvons maintenant constater que notre serveur possède bien un disque de 50 Gb, c'est notre LUN (j'y ai introduit 2 fichiers pour tester).



Maintenant, il faut ajouter le second disque (pour nos backups). Il suffit de faire la même chose. Cependant, il faut créer un autre dossier pour monter le disque dessus (j'ai créé un dossier nommé backup au même endroit) et pour la connexion avec la cible, il faut changer l'IP et l'IQN. Normalement le disque va se créer en /dev/sdc et non /dev/sdb.

4.1.8 Création des dossiers partagés

Concernant les dossiers, nous allons en créer sous le NAS maître et il y sera fait des backups régulièrement sous le NAS esclave. Il y aura un dossier source Partage et il contiendra les dossiers suivants : Directeurs, RH, Comptabilite, Achats et Ventes. Pour créer les dossiers c'est simple, il suffit de faire :

- Sudo mkdir /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage
- Sudo mkdir /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/Directeurs
- Sudo mkdir /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH
- Sudo mkdir /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/Comptabilite
- Sudo mkdir /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/Achats
-

- Sudo mkdir /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/Ventes

```
flavio@srv-tpi:~$ sudo ls /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/
[sudo] password for flavio:
Achats Comptabilite Directeurs RH Ventes
```

Et on peut voir tous nos dossiers.

Ici, « 0d5d2a0a-919d-45a7-8786-7ae92f103a06 » représente mon ID de disque qui a été généré lorsque je l'ai créé. On peut retrouver la liste des disques avec « sudo lsblk ». Ceci affichera la liste des disques et leur point de montage.

4.1.9 Création des utilisateurs et droits

Maintenant que les dossiers ont été créés, il nous faut ajouter les utilisateurs et y mettre leurs droits dans le dossier correspondant. Nous allons, pour cela, créer un utilisateur pour chaque dossier, l'ajouter dans un groupe correspondant au dossier et mettre le bon groupe dans le bon dossier. Ainsi l'utilisateur qui sera dans le groupe du dossier, pourra y accéder et commencer à créer, utiliser ou supprimer des dossiers ou fichiers.

Voici les commandes à entrer pour créer les groupes :

- Sudo groupadd partage (pour donner les droits des dossiers racines)
- Sudo groupadd RH
- Sudo groupadd Directeurs
- Sudo groupadd Comptabilite
- Sudo groupadd Ventes
- Sudo groupadd Achats

Maintenant nous pouvons créer les utilisateurs et les mettre dans les groupes :

- Sudo useradd monique (pour les RH)
- Sudo useradd pascal (directeurs)
- Sudo useradd charlotte (Comptabilite)
- Sudo useradd gilles (Achats)
- Sudo useradd christian (Ventes)

```
flavio@srv-tpi:~$ sudo adduser monique
Adding user 'monique' ...
Adding new group 'monique' (1006) ...
Adding new user 'monique' (1001) with group 'monique' ...
Creating home directory '/home/monique' ...
Copying files from '/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for monique
Enter the new value, or press ENTER for the default
  Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
```

Nous pouvons maintenant ajouter les utilisateurs dans les groupes :

- Sudo /etc/group
- Et on ajoute les noms des utilisateurs à côté des groupes

```
GNU nano 2.9.3 /etc/group

rtkit:x:115:
avahi-autoipd:x:116:
bluetooth:x:117:
whoopsie:x:118:
avahi:x:119:
lpadmin:x:120:
scanner:x:121:saned
saned:x:122:
sddm:x:123:
colord:x:124:
pulse:x:125:
pulse-access:x:126:
geoclue:x:127:
RH:x:1001:monique
Directeurs:x:1002:pascal
Comptabilite:x:1003:charlotte
Ventes:x:1004:gilles
Achats:x:1005:christian
partage:x:1006:flavio,monique,pascal,charlotte,gilles,christian
monique:x:1007:
pascal:x:1008:
charlotte:x:1009:
gilles:x:1010:
christian:x:1011:
```

Ensuite nous pouvons changer les utilisateurs et groupes des dossiers pour que chaque utilisateur puisse y accéder à partir de son groupe. Pour le dossier Directeurs nous allons y mettre le groupe Directeurs et laisser l'utilisateur flavio (qui fait office d'admin).

- Sudo chown flavio:RH /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH (Et on fait de même pour tous les autres)

```
flavio@srv-tpi:~$ sudo chown flavio:Directeurs /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/Directeurs/
```

On fait cela pour chaque dossier.

On ajoute maintenant le groupe partage pour que les utilisateurs accèdent aux dossiers :

```
flavio@srv-tpi:~$ sudo chown flavio:partage /media
flavio@srv-tpi:~$ sudo chown flavio:partage /media/flavio/
flavio@srv-tpi:~$ sudo chown flavio:partage /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/
flavio@srv-tpi:~$ sudo chown flavio:partage /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/
```


On remarque que les droits sont là mais ils ne sont pas bons. En effet, je ne souhaite pas qu'une personne autre que mes utilisateurs puisse lire, écrire ou exécuter quelque chose dans un autre dossier.

```
flavio@srv-tpi:~$ sudo ls -l /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/
total 20
drwxrwxr-x 2 flavio Achats      4096 mars  31 11:04 Achats
drwxrwxr-x 2 flavio Comptabilite 4096 mars  31 11:04 Comptabilite
drwxrwxr-x 2 flavio Directeurs  4096 mars  31 11:04 Directeurs
drwxrwxr-x 2 flavio RH          4096 mars  31 11:04 RH
drwxrwxr-x 2 flavio Ventes      4096 mars  31 11:04 Ventes
```

On voit que les utilisateurs « autres » peuvent avoir accès aux dossiers et on n'aime pas ça !

Pour cela nous allons restreindre les droits avec chmod :

- Sudo chmod 770 /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH

```
flavio@srv-tpi:~$ sudo ls -l /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/
total 20
drwxrwxr-x 2 flavio Achats      4096 mars  31 11:04 Achats
drwxrwxr-x 2 flavio Comptabilite 4096 mars  31 11:04 Comptabilite
drwxrwxr-x 2 flavio Directeurs  4096 mars  31 11:04 Directeurs
drwxrwx--- 2 flavio RH          4096 mars  31 11:04 RH
drwxrwxr-x 2 flavio Ventes      4096 mars  31 11:04 Ventes
flavio@srv-tpi:~$
```

On voit maintenant que seules les personnes du groupe RH peuvent aller dans les dossiers ainsi que l'admin flavio. On fait pareil pour tous les autres et voici ce que cela donne :

```
flavio@srv-tpi:~$ sudo ls -l /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/
total 20
drwxrwx---+ 2 flavio Achats      4096 mars  31 11:04 Achats
drwxrwx---+ 2 flavio Comptabilite 4096 mars  31 11:04 Comptabilite
drwxrwx---+ 2 flavio Directeurs  4096 mars  31 11:04 Directeurs
drwxrwx---+ 2 flavio RH          4096 avril  1 21:56 RH
drwxrwx---+ 2 flavio Ventes      4096 mars  31 11:04 Ventes
flavio@srv-tpi:~$
```

Les petits plus sont quelques chose que j'ai rajouté après ces commandes. Nous verrons cela dans quelques lignes.

On va maintenant mettre les droits pour que les utilisateurs puissent naviguer jusqu'à leur dossier. Sinon ils seront bloqués à la racine et cela serait embêtant. Pour cela on change le groupe (on va utiliser partage) et on change les droits d'accès :

- Sudo chown flavio:partage /media/flavio
- Sudo chown flavio:partage /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06
- Sudo chown flavio:partage /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage

```
flavio@srv-tpi:~$ sudo chown flavio:partage /media
flavio@srv-tpi:~$ sudo chown flavio:partage /media/flavio/
flavio@srv-tpi:~$ sudo chown flavio:partage /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/
flavio@srv-tpi:~$ sudo chown flavio:partage /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/
```

- Sudo chmod 750 /media/flavio
- Sudo chmod 750 /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06

- Sudo chmod 750 /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage

```
flavio@srv-tpi:~$ sudo chmod 750 /media/
flavio@srv-tpi:~$ sudo chmod 750 /media/flavio/
flavio@srv-tpi:~$ sudo chmod 750 /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/
flavio@srv-tpi:~$ sudo chmod 750 /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/
```

- Sudo ls -l -R /media (pour voir si tout a bien changé)

Une fois cela fait, il reste un petit problème à résoudre. Lorsqu'un utilisateur va créer un petit dossier ou un fichier, il sera le seul à y avoir accès. C'est plutôt embêtant si quelqu'un d'autre de son département souhaite entrer dans ce dossier ou lire le fichier. Pour cela on va utiliser « setfacl » pour créer un access list par défaut (comme un umask). Cette dernière va faire en sorte que lorsqu'un utilisateur crée un fichier ou un dossier, il aura les droits qu'on aura accordé par défaut.

Voici la commande à entrer :

- Sudo setfacl -m default:o::rwx /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH

```
flavio@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ sudo getfacl /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH/
getfacl: Removing leading '/' from absolute path names
# file: media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH/
# owner: flavio
# group: RH
user::rwx
group::rwx
other::---

flavio@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ sudo setfacl -m default:o::rwx /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH/
flavio@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ sudo getfacl /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH/
getfacl: Removing leading '/' from absolute path names
# file: media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH/
# owner: flavio
# group: RH
user::rwx
group::rwx
other::---
default:user::rwx
default:group::rwx
default:other::rwx
```

On voit ici que cela a fonctionné. Je me permets de donner tous les droits car seuls les RH ont accès au dossier et non les autres. Ils peuvent donc gérer leurs propres fichiers et dossiers (c'est à ce moment qu'apparaît le + dont je parlais avant, en effet, il y a plus que les simples groupes et donc il signifie que qu'il y a d'autres groupes qui ne sont pas montrés avec un simple « ls »).

On voit que monique des RH a accès au dossier et peut créer des fichiers et dossiers avec tous les droits pour les autres, mais lorsque pascal tente d'entrer dans le dossier, il ne peut pas ! En effet, il n'a pas les droits requis.

```
flavio@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ su monique
Password:
monique@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ ls
Test Test2 test2.txt test.txt
monique@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ mkdir Test3
monique@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ touch test3.txt
monique@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ ls -l
total 12
drwxrwxr-x  2 monique monique 4096 avril  1 21:07 Test
drwxrwx---+ 2 monique monique 4096 avril  1 21:44 Test2
-rw-rw----+ 1 monique monique  0 avril  1 21:44 test2.txt
drwxrwxrwx+ 2 monique monique 4096 avril  1 21:52 Test3
-rw-rw-rw-  1 monique monique  0 avril  1 21:52 test3.txt
-rw-rw-r--  1 monique monique  0 avril  1 21:07 test.txt
monique@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$
monique@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ su pascal
Password:
pascal@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$ ls
ls: cannot open directory '.': Permission denied
pascal@srv-tpi:/media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage/RH$
```

4.1.10 Backup des données

Nous allons utiliser « rsync » pour faire les backups des différents dossiers partagés. Nous allons donc transporter les dossiers du NAS maître dans les dossiers du NAS esclave. Nous avons donc déjà créés les disques qui ont été montés sur le serveur Linux et qui se trouvent sous /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage pour le NAS maître et sous /media/flavio/6fc13f7a-8905-463f-bb2f-cc019de82014 pour le NAS esclave.

Pour cela nous allons faire la commande suivante :

- Créer un fichier test

```
flavio@srv-tpi:~$ sudo touch /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Test.txt
flavio@srv-tpi:~$ sudo nano /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Test.txt
```

Fichier	Édition	Affichage	Signets	Configuration	Aide
GNU nano 2.9.3		/media/flavio/0d5d2a0a			
Test					
1					
2					
3					
4					
5					
6					
Test fin					

- Maintenant nous pouvons faire un backup du tout
- Rsync -avzX /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/ /media/flavio/6fc13f7a-8905-463f-bb2f-cc019de82014/backup.complet

```
flavio@srv-tpi:~$ sudo rsync -avzX /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/ /media/flavio/6fc13f7a-8905-463f-bb2f-cc019de82014/backup.complet
sending incremental file list
created directory /media/flavio/6fc13f7a-8905-463f-bb2f-cc019de82014/backup.complet
./
Test.txt
.Trash-1000/
.Trash-1000/files/
.Trash-1000/info/
Partage/
Partage/Achats/
Partage/Comptabilite/
Partage/Directeurs/
Partage/RH/
Partage/Ventes/
lost+found/

sent 583 bytes  received 170 bytes  1,506.00 bytes/sec
total size is 26  speedup is 0.03
flavio@srv-tpi:~$
```

On voit que le tout a été enregistré et nous avons pu transférer tous les fichiers (il y a la possibilité d'ajouter -delete afin de supprimer les vieux fichiers onéreux qui seraient restés dans le backup complet).

On crée les dossiers de backups :

```
flavio@srv-tpi:/media/flavio/6fc13f7a-8905-463f-bb2f-cc019de82014$ ls
backup.1 backup.2 backup.3 backup.complet
```

Maintenant pour faire des backups complets, il va falloir suivre les commandes suivantes :

- Rm -rf backup.3
- Mv backup.2 backup.3
- Mv backup.1 backup.2
- Cp -al backup.complet backup.1
- Rsync -avzX *source* backup.complet

(J'ai omis le nom complet des fichiers afin de faciliter la lecture des commandes).

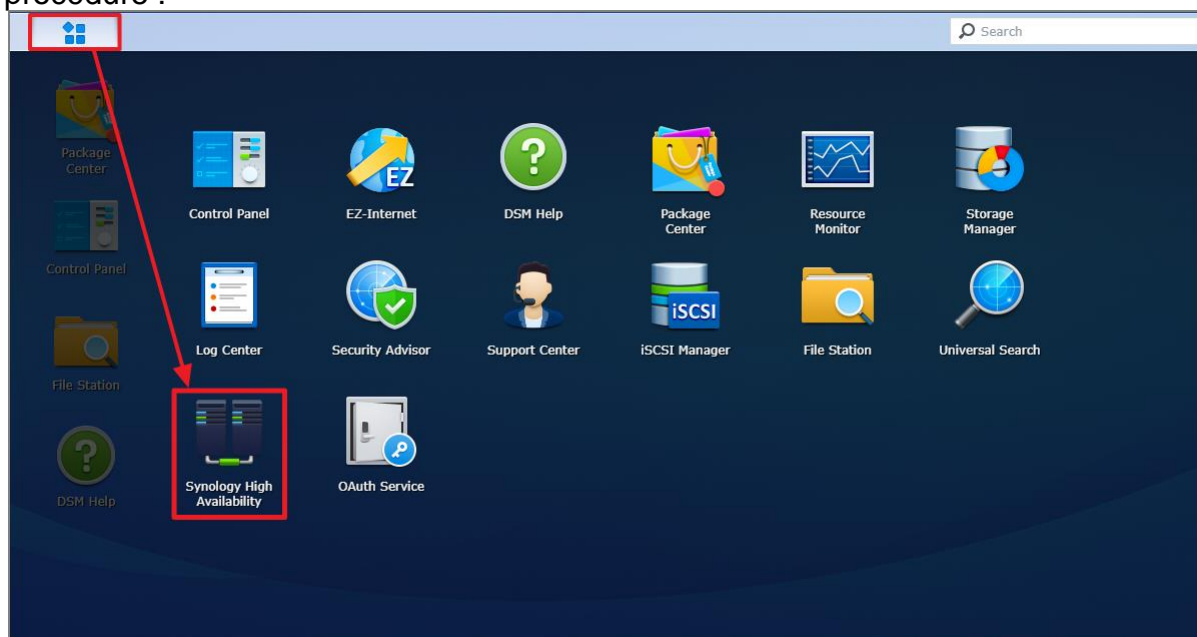
Avec cela, nous aurons jusqu'à 4 backups complets allant de la plus vieille (backup.3) à la plus récente (backup.complet).

Il faudrait mettre notamment ces commandes dans le cron afin qu'elles s'exécutent aux moments souhaités. De plus, il faudrait ajouter les backups incrémentiels (toutes les minutes 7h-20h) et différentiels (toutes les heures 20h-7h) pour avoir une sauvegarde parfaite des données des utilisateurs.

4.1.11 Haute disponibilité

La première chose importante à savoir est qu'il faut que les NAS soient exactement les mêmes. Le modèle, le DSM utilisé, la version du « High availability », le nombre de disques ainsi que l'emplacement des disques.

Premièrement, il faut installer « Synology High Availability » sur le NAS maître. Ensuite il faudra mettre une liaison par câble entre les 2 NAS. Ceci servira pour leur propre échange de données qui ne « polluera » la liaison NAS – Serveur. Nous pouvons dorénavant appuyer sur le logiciel nouvellement installé et commencer la procédure :



On crée notre cluster :

Synology High Availability

High-availability Cluster

Synology High Availability is designed to maximize the service continuity of your Synology NAS.

The high-availability cluster consists of two hosts and two network connections:

- The **active server** is responsible for running all services.
- The **passive server** is placed on standby, only receiving data from the active server in real time. It is not available for user login until it takes over the services once the active server malfunctions.
- The **cluster network connection** is responsible for the primary access to the cluster.
- The **Heartbeat network connection** syncs data between the two hosts.

Create high-availability cluster

Il nous rappelle comme annoncé précédemment que tout doit être identique :

Synology High Availability

Before you start

Synology High Availability requires two [compatible Synology NAS](#) and identical system configurations.

1. Make sure the following configurations are identical on both hosts:

Storage

- The number, capacity and inserted slots of drives i

Network

- The total number of network interfaces i
- The network settings

DSM version

2. Make sure both hosts are assigned with at least one set of static IP address as the cluster connection.

3. Make sure the hostnames of both hosts are different i

4. Refer to the [video tutorial](#) on how to set up a high-availability cluster

Note: We recommend setting up a UPS to protect the high-availability cluster from a power outage. Please refer to [this tutorial](#) for further instructions.

Next
Back
Cancel

On choisit le cluster (le lien avec le serveur) et le Heartbeat (le lien avec l'autre NAS) selon nos branchements :

? X

Synology High Availability

Set up network interfaces

Both cluster and Heartbeat interfaces are crucial in the high-availability cluster. [Link Aggregation](#) is highly recommended for a better performance.

Cluster interface is the network interface used for accessing the cluster. ⓘ

Select a cluster interface ▼

Heartbeat interface is the network interface used for syncing data between the hosts. ⓘ

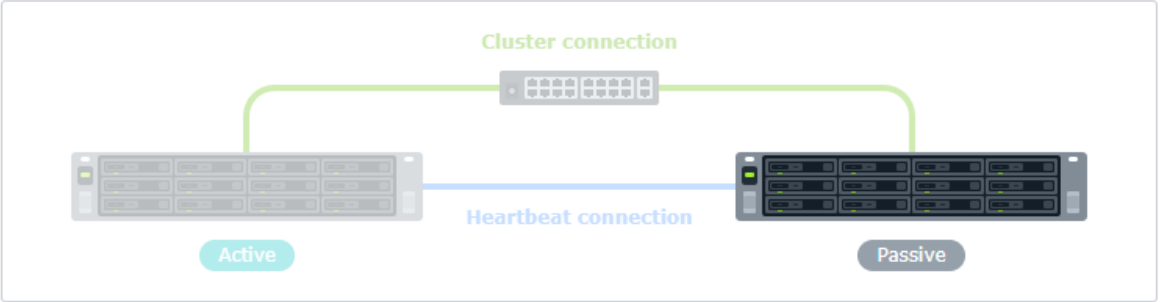
Select a Heartbeat interface ▼

Back
Next
Cancel

On met le user et le mot de passe d'un admin de l'autre NAS (ici flavio et Pa\$\$w0rd) :

Synology High Availability

Enter passive server information



Cluster connection

Heartbeat connection

Active

Passive

Enter the administrator's credential of the passive server to continue.

Passive Server:

Username: admin

Password:

Back

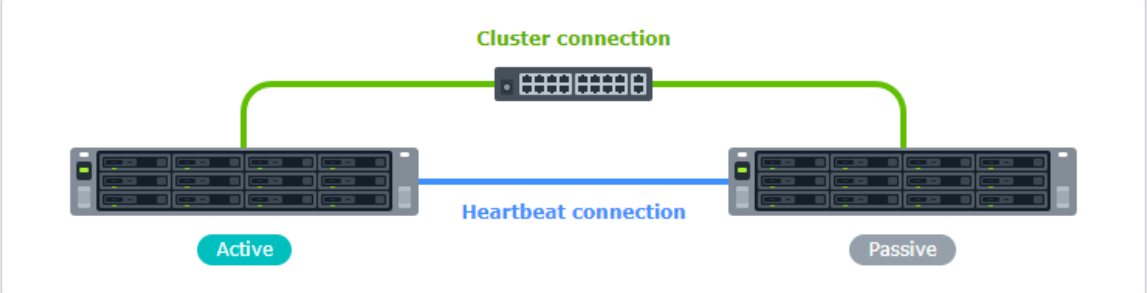
Next

Cancel

On met le nom du second cluster et son IP (ici NAS-Slave et 192.168.1.201) :

Synology High Availability

Set up High Availability Cluster



Set up the hostname and IP address of the high-availability cluster. You can access the cluster with this IP address.

Cluster hostname:

i

Cluster IP:

i

Back
Next
Cancel

Le système vérifie que tout soit bon :

Synology High Availability ? X

Verify the requirements

Name	Status
System Information	✓
Volume	✓
Network Service	✓
Network Setup	✓
Heartbeat Interface	✓

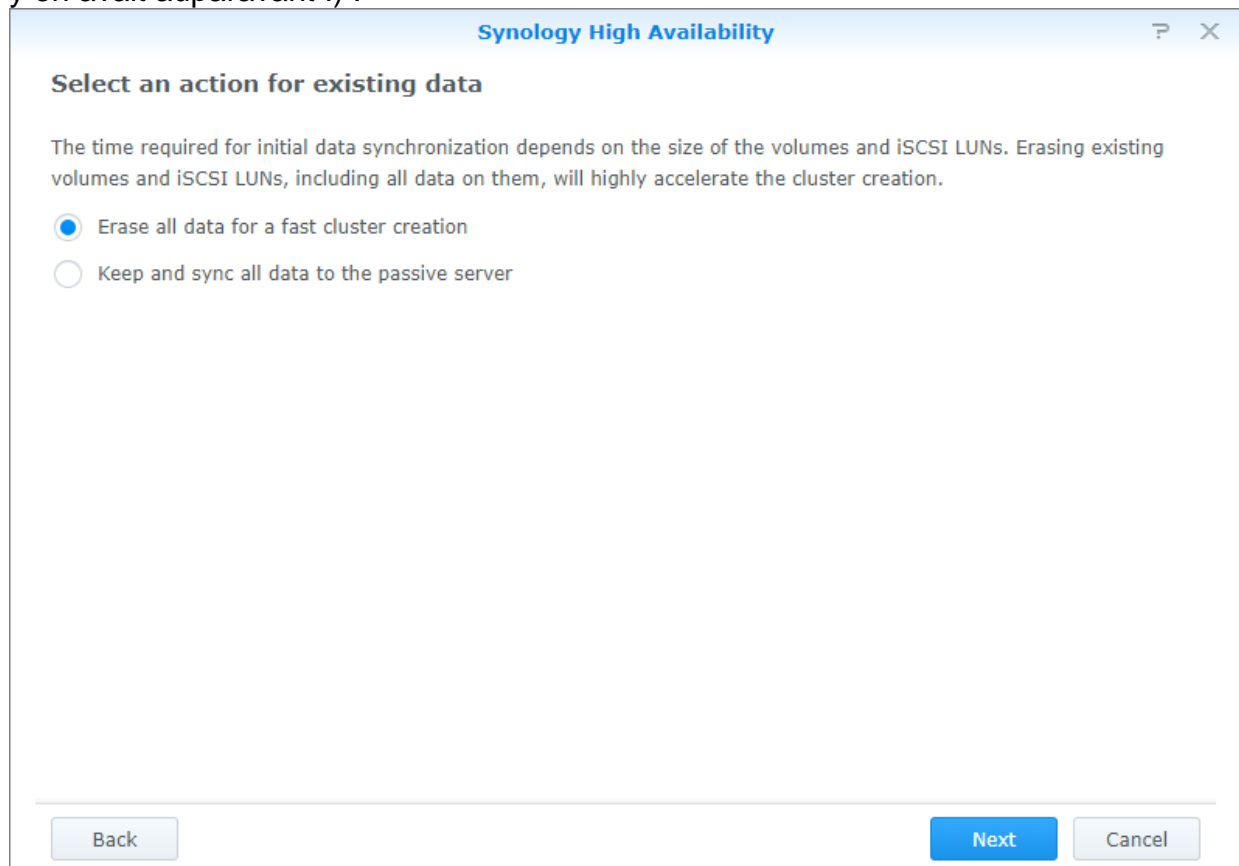
Your system meets all the requirements for creating a high-availability cluster.

Back

Next

Cancel

On supprimer le tout sur le NAS esclave (attention à faire un backup des données s'il y en avait auparavant !) :



The image shows a screenshot of a 'Synology High Availability' configuration window. The title bar is light blue with the text 'Synology High Availability' and standard window controls. The main content area has a light blue header 'Select an action for existing data'. Below this, a paragraph explains that the time for initial data synchronization depends on the size of the volumes and iSCSI LUNs, and that erasing existing data will accelerate cluster creation. There are two radio button options: 'Erase all data for a fast cluster creation' (which is selected) and 'Keep and sync all data to the passive server'. At the bottom, there are three buttons: 'Back', 'Next' (highlighted in blue), and 'Cancel'.

Synology High Availability

Select an action for existing data

The time required for initial data synchronization depends on the size of the volumes and iSCSI LUNs. Erasing existing volumes and iSCSI LUNs, including all data on them, will highly accelerate the cluster creation.

☒ Erase all data for a fast cluster creation

☐ Keep and sync all data to the passive server

Back Next Cancel

On applique le tout :

Synology High Availability

Confirm settings

Item	Value
Heartbeat interface	LAN 2 (1 Gbps)
Passive Server	<input type="checkbox"/>
Cluster hostname	Cluster_SHA
Cluster interface	LAN 1 (1 Gbps)
Cluster IP	<input type="text"/>

Back

Apply

Cancel

On accepte et c'est pourquoi il faut faire un backup au préalable :

The screenshot shows the 'Synology High Availability' settings window. A modal dialog titled 'Create high-availability cluster' is displayed in the center. The dialog contains the following text:

The system will start creating the high-availability cluster. Before you perform this action, please note the following:

- All services will be stopped and then resume after the operation is completed.
- All the data stored on the passive server will be removed.

Are you sure you want to continue?

Below the text, there is a checkbox with a blue checkmark and the text: 'I understand all the data stored on the passive server will be permanently removed and cannot be recovered.' This checkbox and its text are highlighted with a red rectangular border.

At the bottom right of the dialog are two buttons: 'Yes' (red) and 'No' (grey).

In the background, the 'Confirm settings' window is visible, showing a table with the following items and values:

Item	Value
Heartbeat interface	LAN 2 (1 Gbps)
Passive Server	
Cluster hostname	
Cluster interface	
Cluster IP	

At the bottom of the settings window are three buttons: 'Back', 'Apply', and 'Cancel'.

Après cette étape l'état du cluster des NAS s'affiche et nous pouvons tout gérer à partir de là. Rien de bien compliqué, tout ce fait automatiquement.

4.2 Modifications apportées par rapport à la conception

Les seules modifications apportées à la conception est que suite au confinement du COVID-19 il a fallu tout réinstaller à la maison. Cependant, ne pouvant transporter les 2 NAS ainsi que la tour qui faisait office de serveur, j'ai créé des machines virtuelles pour simuler le réseau et les machines. Le tout étant hébergé sur ma machine Windows.

4.3 Description des tests effectués

4.3.1 Matériel

Il faut tester que tout fonctionne. Il suffit donc d'allumer l'ordinateur, le switch et les Synology. Tout était fonctionnel et je n'ai remarqué aucun problème.

4.3.2 Réseau

Une fois que le tout est prêt et opérationnel, on peut tester s'ils se voient sur le réseau. Pour ma part, j'ai installé l'assistant NAS qui permet de scanner le réseau et de trouver les différents NAS reliés. J'ai fait cela avec ma machine sous Windows pour voir s'il n'y avait pas de problèmes. Ensuite j'ai fait le test avec ma machine virtuelle Linux mais cela n'a donné aucun résultat. J'ai donc commencé par mettre la VM (Virtual Machine) en mode bridge et non NAT (Network Address Translation) afin qu'elles se partagent la même carte réseau et donc l'IP. A nouveau je ne pouvais pas atteindre les NAS depuis la VM mais depuis Windows oui. J'avais déjà eu un problème de ce genre lors d'un précédent projet où je devais installer Pfsense pour gérer les authentifications sur un réseau et malgré l'aide de Mr. Jaggi, un mois durant, nous ne sommes pas arrivés à faire passer ne serait-ce qu'un simple ping de la VM en dehors de la machine physique. Nous avons conclu à un problème avec VMware. Afin de ne pas perdre trop de temps avec ce problème, j'ai donc demandé une tour pour installer Linux directement dessus. Une fois cela fait, j'ai mis une adresse IP au serveur. Voici comment j'ai procédé : enp0s3

```
GNU nano 2.9.3 /etc/network/interfaces
# ifupdown has been replaced by netplan(5) on this system. See
# /etc/netplan for current configuration.
# To re-enable ifupdown on this system, you can run:
#   sudo apt install ifupdown
auto enp0s31f6
iface enp0s31f6 inet static
    address 172.17.215.20
    netmask 255.255.255.0
```

On met l'adresse en statique sous /etc/network/interfaces comme ci-dessus. Il faut ensuite redémarrer le network :

```
flavio@linux:~$ sudo /etc/init.d/networking restart
[ ok ] Restarting networking (via systemctl): networking.service.
```

Et on peut voir que l'IP est la bonne :

```
flavio@linux:~$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.215.20 netmask 255.255.255.0 broadcast 172.17.215.255
    inet6 fe80::4a4d:7eff:fee8:1f3d prefixlen 64 scopeid 0x20<link>
    ether 48:4d:7e:e8:1f:3d txqueuelen 1000 (Ethernet)
    RX packets 1327 bytes 164026 (164.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 76 bytes 12961 (12.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 memory 0xf7100000-f7120000
```

J'ai ensuite fait un ping sur les deux NAS. Tout était fonctionnel, voici les résultats obtenus en image :

```
flavio@linux:~$ ping 172.17.215.218
PING 172.17.215.218 (172.17.215.218) 56(84) bytes of data.
64 bytes from 172.17.215.218: icmp_seq=1 ttl=64 time=0.390 ms
64 bytes from 172.17.215.218: icmp_seq=2 ttl=64 time=0.196 ms
^C
--- 172.17.215.218 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1031ms
rtt min/avg/max/mdev = 0.196/0.293/0.390/0.097 ms
```

```
flavio@linux:~$ ping 172.17.215.237
PING 172.17.215.237 (172.17.215.237) 56(84) bytes of data.
64 bytes from 172.17.215.237: icmp_seq=1 ttl=64 time=0.393 ms
64 bytes from 172.17.215.237: icmp_seq=2 ttl=64 time=0.186 ms
^C
--- 172.17.215.237 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.186/0.289/0.393/0.104 ms
```

On voit donc bien que les machines communiquent entre-elles sur le réseau.

4.3.3 iSCSI

Ici, le test a simplement consisté à voir si on pouvait créer un dossier ou un fichier sur le disque qui a été monté et notamment éteindre et rallumer le serveur pour voir si les disques avec les dossiers et fichiers étaient toujours présents. Cela a fonctionné sans aucuns soucis.

4.3.4 Droits

Voici les différents tests effectués pour vérifier la qualité et l'exactitude des droits administrer sur les dossiers partagés pour les utilisateurs :

- Vérification des de l'attribution des droits
- Authentification avec utilisateur et tentative d'accès au dossier
- Création d'un dossier et d'un fichier
- Connexion sur un autre compte (flavio) et modification des fichiers et dossiers pour tester les droits après création

- Connexion avec un compte qui n'a pas accès au dossier et tentative de s'y introduire

Tous les tests ont été réussis avec succès et les droits ont été parfaitement administrés comme souhaité.

4.3.5 Backups

Une suppression et une modification des fichiers et des dossiers ont été fait à plusieurs reprise afin tester les backups. Cela a toujours fonctionné sans problèmes. Il a été possible aussi de restaurer le tout en changeant simplement la source et la destination.

4.3.6 Synchronisation

Le test aurait été d'arrêter le NAS maître et voir si le NAS esclave prenait bien la relève. Ainsi on aurait pu vérifier la fonctionnalité du basculement pour la synchronisation des données.

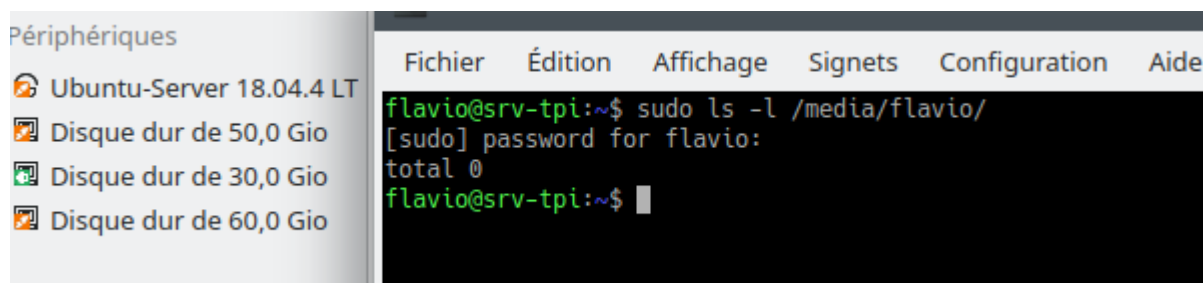
4.4 Problèmes rencontrés et solutions

4.4.1 Problèmes RAID 5

Comme expliqué dans le paragraphe précédent, il m'était impossible de monter du RAID 5 mais j'avais pu le faire en cours lors de la création des volumes avec du RAID 5. Je n'ai juste pas pu tester leur efficacité. Cependant, nous avons pu le faire lors du cours de « sauvegarde des données » avec le NAS que j'avais utilisé en cours donc je peux sans problèmes dire que le RAID 5 fonctionne sans problèmes sur ces machines.

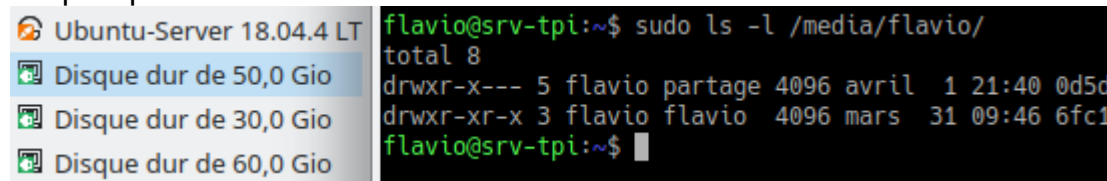
4.4.2 Problèmes mount

Ici nous avons un problème auquel je n'ai pas trouvé de solution. En effet, lorsque je redémarre le serveur (même s'il n'est pas censé être éteint mais l'on ne sait jamais) les disques ne se montent pas automatiquement.



Ils ne sont pas montés et on ne peut pas y accéder.

Dès lors il y a deux solutions, soit faire un mount à la main, soit cliquer sur les disques pour les ouvrir.

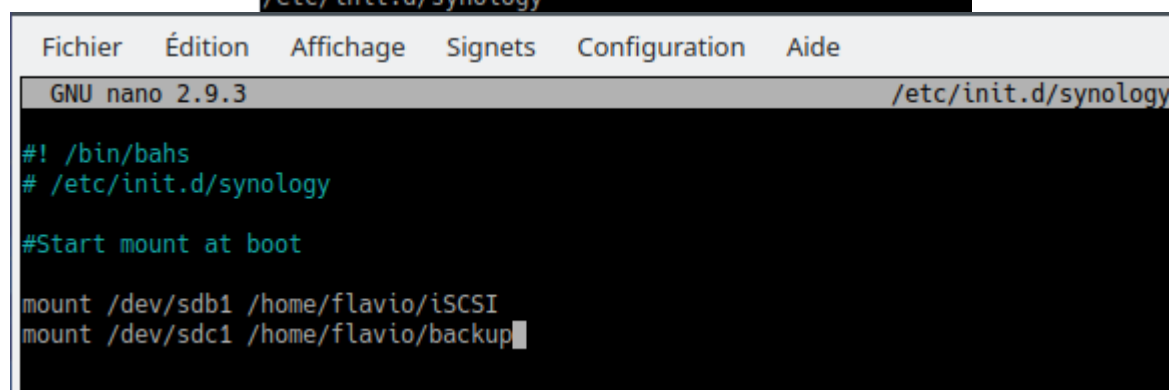


```
flavio@srv-tpi:~$ sudo ls -l /media/flavio/
total 8
drwxr-x--- 5 flavio partage 4096 avril  1 21:40 0d5d2
drwxr-xr-x 3 flavio flavio  4096 mars  31 09:46 6fc1f
flavio@srv-tpi:~$
```

On voit qu'ils sont atteignables.

J'ai tenté de faire un mount automatique au démarrage dans le fichier /etc/init.d

```
flavio@srv-tpi:~$ sudo touch /etc/init.d/synology
[sudo] password for flavio:
flavio@srv-tpi:~$ sudo ls /etc/init.d/syn*
/etc/init.d/synology
```



```
GNU nano 2.9.3 /etc/init.d/synology

#!/bin/bash
# /etc/init.d/synology

#Start mount at boot

mount /dev/sdb1 /home/flavio/iSCSI
mount /dev/sdc1 /home/flavio/backup
```

Mais ceci ne change rien ! Et de plus, lorsque je clique sur les disques, cela memet qu'ils sont déjà monté et que je ne peux le refaire une seconde fois et ils sont par la suite opérationnels.

Je pense que le problème vient du fait que dans le script, le mount se fait avant la détection des cibles iSCSI et ne se monte pas. Il faudrait mettre ce script à un autre moment mais je n'ai plus le temps de faire des recherches pour cela. Et ça ne me semble pas être un problème majeur pour que le système soit fonctionnel.

4.4.3 Problèmes compréhensions de LUN

Je me suis dès le début penché sur comment créer des dossiers partager sur le NAS et j'avais fait une synchronisation avec rsync en connexion. J'ai perdu un bon moment à chercher les dossiers à synchroniser (après les tests réussis) dans le NAS. Ce n'est que plus tard (en faisant la connexion iSCSI avec la LUN) que je me suis rendu compte qu'on montait un disque et que ce disque utilisait un espace virtuellement alloué dans le NAS et que ce dernier ne traitait pas ce volume directement. En effet, il stockait la mémoire mais ne la lisais. Pour cela il fallait se connecter depuis le serveur. J'ai tout de même réussi à rattraper ce retard en reproduisant ce que j'avais avec rsync et cela a fonctionné sans soucis.

4.4.4 Problèmes sécurité CHAP

Comme vous avez dû le constater, je n'ai pas pu mettre la connexion avec CHAP pour l'authentification car cela ne fonctionnait pas. J'ai tout tenté et j'ai cherché sur internet pour trouver des solutions mais rien n'y faisait. J'ai donc abandonné ce procédé et je suis passé à la suite.

4.4.5 Problèmes de droits

Impossible de comprendre pourquoi les utilisateurs n'avaient pas accès à leur dossier. Ils devaient passer par /media/flavio/0d5d2a0a-919d-45a7-8786-7ae92f103a06/Partage. Il m'a fallu plus de 5h pour décortiquer le problème jusqu'à sa source et comprendre sa racine. J'ai vu qu'il y avait un petit « + » après les droits du dossier media/flavio. Ayant fait plusieurs tentatives infructueuses jusqu'alors, cela me parut bien d'aller voir. Et en effet, ce fût un effort récompensé. Avec « getfacl » j'ai pu voir l'entièreté des droits et lorsque je changeais les droits du groupe (partage) cela modifiait l'« umask » des ACL (access list) et non le groupe. Après des recherches je suis tombé sur un forum et il suffisait de faire :

- Sudo setfacl -bn /media/flavio (pour supprimer les ACL et l'umask)

```
flavio@srv-tpi:~$ sudo getfacl /media/flavio/
[sudo] password for flavio:
getfacl: Removing leading '/' from absolute path names
# file: media/flavio/
# owner: flavio
# group: partage
user::rwx
group::r-x
other::---
```

On voit ici avec getfacl qu'il n'y a plus l'umask qui était mis par défaut et qui empêchait les changements dans le groupe.

Avec cela j'ai pu remettre les droits et puis un petit test utilisateur m'a confirmé que le tout fonctionnait.

4.4.6 Problèmes confinement

Comme expliqué auparavant, suite à la pandémie, je me suis retrouvé à la maison et j'ai dû refaire tout le montage. Le problème étant qu'il fût plus compliqué que prévu de monter des NAS avec une image ISO. Je vais vous passer les explications du montage mais j'ai été restreint pour le nombre de disques, je ne pouvais guère en ajouter plus que la machine préconfigurée (c'est-à-dire 1) et donc je ne pouvais pas installer comme je le souhaitais mon RAID5. D'autant plus que pour la synchronisation des NAS, il m'était impossible d'ajouter une nouvelle connexion entre les deux, et donc la synchronisation ne pouvait pas se faire.

Cette situation aura été plutôt chronophage car j'ai passé plus d'une semaine à faire des tentatives pour insérer plusieurs disques et cartes. J'aurais mieux fait de me contenter de ce que j'avais et de passer à la suite mais mon côté perfectionniste m'a fait défaut.

4.4.7 Problème backups

J'ai perdu beaucoup de temps au milieu du projet car je cherchais comment faire un backup des fichiers partagés du NAS et non des LUN. Ce n'est que plus tard (dernière semaine) que je me suis rendu compte de mon erreur. J'ai donc fait ce que j'ai pu pour rattraper ce problème. Malheureusement cela n'a pas suffi. En effet, le backup des dossiers et fichiers est plus complexe qu'il n'y paraît. Cependant après quelques recherches j'ai pu parvenir à comprendre une majeure partie en effectuant divers tests. Malheureusement je n'ai pas pu parvenir au bout de ce que j'aurais souhaité car il m'aurait fallu plus de temps.

4.4.8 Problèmes Synchronisation

Encore une fois suite au confinement, il m'était impossible de créer la synchronisation. Je me suis tout de même permis de mettre la démarche et de l'expliquer car elle n'est pas du tout compliquée, pour autant qu'on la respecte. C'est notamment un des objectifs et il était donc primordial de l'expliquer.

A noter qu'elle aurait été impossible en cours car nos NAS ne possédaient qu'une prise RJ-45 pour l'échange de données et l'abandon de la synchronisation était inévitable dans tous les cas.

5 Conclusions

Deux points ne sont pas complets, en effet je n'ai pas eu le temps de finir les backups et donc la solution n'est pas fonctionnelle dans sa totalité. Cependant le reste des points a été fait (sauf pour la synchronisation, mais ceci est un point matériel dont je n'étais pas maître).

Le point positif a été l'apprentissage avec la pratique, les tests et la recherche. En effet, je ne connaissais pas grand-chose sur Linux et le protocole iSCSI avant de commencer ce projet mais mon niveau s'est nettement amélioré grâce à ce projet. Cependant mon manque de connaissances aura aussi eu un impact négatif sur l'ensemble du projet. En effet, j'ai passé beaucoup plus de temps que prévu à faire des recherches et à installer le tout. De mon point de vue, j'avais pensé fini le projet en 50h et y ajouter des options supplémentaires mais ce ne fût pas le cas.

La difficulté particulière a été de devoir tout refaire. En effet, j'étais arrivé à environ 75% de la fin de mon projet en cours et j'ai dû tout recommencer à zéro lorsque nous avons été confinés. Cela m'a fait perdre pas mal de temps et je pense que le projet aurait pu être terminé à temps si cela n'était pas arrivé.

Il serait bien (pour ma part) de continuer à travailler sur les backups que je n'ai pas eu le temps de finir et revoir les ACL dans le but d'accroître mes connaissances avec Linux. J'aurais notamment souhaité mettre un pare-feu car nous avons vu en cours en quoi cela consistait mais nous n'avons jamais pratiqué dessus. Je trouverais cela intéressant pour mes connaissances personnelles d'autant plus que je souhaite aller à la HEIG en option sécurité et que nous allons très certainement travailler dessus.

Ce projet m'aura apporté beaucoup de connaissances que je pensais avoir mais qui n'étaient pas du tout complètes. Cela m'aura permis de voir l'étendue des commandes Linux que je connaissais déjà mais qu'en surface. Je suis notamment déçu de ne pas avoir eu le temps de finir ce projet car c'était quelque chose qui me plaisait. Cependant, rien ne m'empêche de le finir dans mon temps libre et d'y ajouter quelques modifications pour mon simple plaisir. Malgré quelques prises de têtes sur certaines recherches et fonctionnalités, j'ai éprouvé bien du plaisir à faire ce pré-TPI, j'espère que le TPI sera d'autant intéressant et me permettra de découvrir de nouvelles choses.

6 Annexes

6.1 Sources – Bibliographie

6.1.1 iSCSI

- https://en.wikipedia.org/wiki/Storage_area_network
- <https://waytolearnx.com/2018/07/difference-entre-san-et-nas.html>
- <https://www.laurentbloch.net/MySip3/NFS-SANs-et-NAS>
- <https://fr.wikipedia.org/wiki/iSCSI>
- https://fr.wikipedia.org/wiki/Commande_SCSI
- <https://www.ionos.fr/digitalguide/serveur/know-how/trame-ethernet/>
- https://fr.wikipedia.org/wiki/Internet_Protocol
- <https://storagehub.vmware.com/t/best-practices-for-running-vmware-vsphere-on-iscsi/iscsi-sessions-and-connections/>
- <https://www.sanfoundry.com/what-is-iscsi-connection-session/>
- https://fr.wikipedia.org/wiki/Logical_Unit_Number
- https://www.snia.org/sites/default/education/tutorials/2011/spring/networking/HufferdJohn-IP_Storage_Protocols-iSCSI.pdf
- <https://searchwindowsserver.techtarget.com/tip/Five-layers-of-iSCSI-storage-connection-security>
- https://www.synology.com/en-global/knowledgebase/DSM/tutorial/Virtualization/How_to_use_the_iSCSI_Target_service_on_Synology_NAS
- https://www.synology.com/en-global/knowledgebase/DSM/tutorial/File_Sharing/How_to_encrypt_and_decrypt_shared_folders_on_my_Synology_NAS
- <https://www.cyberciti.biz/faq/howto-setup-debian-ubuntu-linux-iscsi-initiator/>
- https://www.youtube.com/watch?v=W4JOsFY_K8Y
- https://www.synology.com/fr-fr/knowledgebase/DSM/tutorial/Virtualization/How_to_set_up_and_use_iSCSI_target_on_Linux
- https://www.synology.com/fr-fr/knowledgebase/DSM/tutorial/Virtualization/How_to_use_the_iSCSI_Target_service_on_Synology_NAS
- <https://www.memoinfo.fr/tutoriels-linux/configurer-client-iscsi-debian/>
- <https://doc.ubuntu-fr.org/fdisk>
- https://bugzilla.redhat.com/show_bug.cgi?id=1015563 (nb sessions)
- <https://ubuntuforums.org/showthread.php?t=2062418> (CRC)
- <https://unix.stackexchange.com/questions/20357/how-can-i-make-a-script-in-etc-init-d-start-at-boot>

6.1.2 Sauvegardes

- [https://fr.wikipedia.org/wiki/RAID_\(informatique\)](https://fr.wikipedia.org/wiki/RAID_(informatique))
- [https://fr.wikipedia.org/wiki/Sauvegarde_\(informatique\)](https://fr.wikipedia.org/wiki/Sauvegarde_(informatique))

- <https://www.appvizer.fr/magazine/services-informatiques/sauvegarde/comment-la-sauvegarde-differentielle-conserve-vos-donnees>

6.1.3 Utilisateurs, groupes et droits

- <https://www.tecmint.com/add-users-in-linux/>
- <https://www.it-connect.fr/gestion-de-lumask-sous-linux/>
- <https://doc.ubuntu-fr.org/permissions>
- <https://askubuntu.com/questions/455000/group-permissions-allow-but-still-get-permission-denied>
- <https://serverfault.com/questions/227852/what-does-a-mean-at-the-end-of-the-permissions-from-ls-l>
- <https://unix.stackexchange.com/questions/339765/how-to-remove-acl-from-a-directory-and-back-to-usual-access-control>
- https://lea-linux.org/documentations/Gestion_des_ACL
- <https://serverfault.com/questions/458550/setting-per-directory-umask-using-acls>

6.1.4 Backups

- https://www.synology.com/fr-fr/dsm/feature/snapshot_replication
- <https://synoguide.com/2018/10/05/different-backup-replication-setups-between-two-synology-nas-servers/>
- <https://codereviewvideos.com/course/everyday-linux/video/simple-backup-shell-script-linux>
- https://www.synology.com/fr-fr/knowledgebase/DSM/help/DSM/AdminCenter/file_rsync
- <https://centosfaq.org/centos/rsync-and-differential-backups/>
- <https://superuser.com/questions/730654/does-rsync-delete-files-folders-at-destination-by-default>
- <https://www.linux.com/tutorials/how-backup-files-linux-rsync-command-line/>
- <https://centosfaq.org/centos/rsync-and-differential-backups/>
- <https://superuser.com/questions/730654/does-rsync-delete-files-folders-at-destination-by-default>
- <https://www.admin-magazine.com/Articles/Using-rsync-for-Backups>
- [https://en.wikipedia.org/wiki/Ln_\(Unix\)](https://en.wikipedia.org/wiki/Ln_(Unix))

6.1.5 Synchronisation

- https://www.synology.com/en-uk/knowledgebase/DSM/tutorial/Virtualization/How_to_Use_Port_Binding_to_Configure_Multipathing_on_VMware_for_Synology_NAS
- https://www.synology.com/fr-fr/knowledgebase/DSM/tutorial/Disaster_Recovery/How_to_create_a_high_availability_configuration_with_Synology_NAS

6.2 Supports d'archivage du projet

- Ova du serveur Ubuntu
- Ova du NAS maître
- Ova du NAS esclave
- Journal de bord au format Excel