14/02/2020

SOVILLA Flavio

SI –CA2a CPNV

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

Table des matières

[1. Introduction 3](#_Toc33688188)

[1.1 Cadre du projet 3](#_Toc33688189)

[1.2 Description du projet 3](#_Toc33688190)

[1.3 Matériel à disposition 3](#_Toc33688191)

[1.4 Planning 4](#_Toc33688192)

[2. SAN et NAS 4](#_Toc33688193)

[3. Protocole iSCSI 6](#_Toc33688194)

[3.1 Comment fonctionne-t-il 6](#_Toc33688195)

[3.2 L’encapsulation 6](#_Toc33688196)

[3.3 Les couches 7](#_Toc33688197)

[3.4 La sécurité 8](#_Toc33688198)

[4. Architecture réseau 9](#_Toc33688199)

[4.1 Réseau en BUS 9](#_Toc33688200)

[4.2 Réseau Hybride 9](#_Toc33688201)

[5. Redondance NAS 10](#_Toc33688202)

[5.1 Le principe 10](#_Toc33688203)

[5.2 Les RAID 11](#_Toc33688204)

[5.2.1 RAID 0 11](#_Toc33688205)

[5.2.2 RAID 1 12](#_Toc33688206)

[5.2.3 RAID 5 13](#_Toc33688207)

[5.3 Les types de backups 13](#_Toc33688208)

[5.3.1 Complet 14](#_Toc33688209)

[5.3.2 Différentiel 14](#_Toc33688210)

[5.3.3 Incrémentiel 14](#_Toc33688211)

[5.4 Le choix pour le réseau 14](#_Toc33688212)

[6. Montage de la redondance 15](#_Toc33688213)

[7. Montage du service iSCSI 15](#_Toc33688214)

[8. Problèmes rencontrés 15](#_Toc33688215)

[9. Conclusions 15](#_Toc33688216)

[10. Sources 15](#_Toc33688217)

[11.1 SAN et NAS 15](#_Toc33688218)

[11.2 Protocole iSCSI 15](#_Toc33688219)

[11.3 Architecture réseau 16](#_Toc33688220)

[11.4 Redondance NAS 16](#_Toc33688221)

[11.5 Montage de l’infrastructure 16](#_Toc33688222)

[11.6 Montage de la redondance 16](#_Toc33688223)

[11.7 Montage du service iSCSI 16](#_Toc33688224)

# Introduction

## 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 vérifier 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.

## 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 avions déjà entendu parlé mais nous n’avons jamais vu de quoi il s’agissait. Enfin, il faudra créer une infrastructure sécurisée pour l’environnement du SAN.

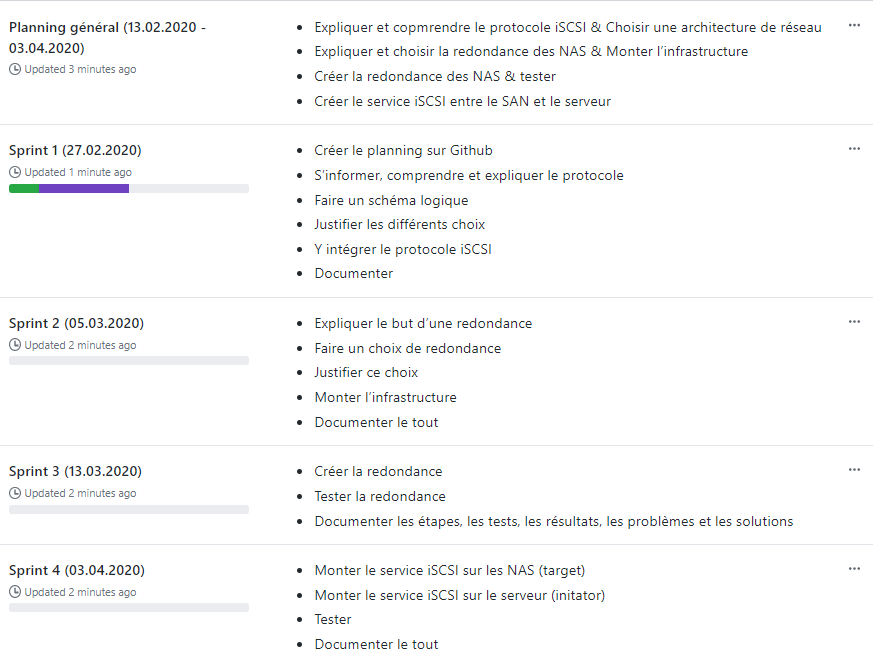
## Matériel à disposition

Pour pouvoir mener à bien ce projet, nous allons avoir à disposition le 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
* 2x Switch Netgear GS105 v4 de 5 ports 10/100Mbits (avec prises d’alimentation)
* 3x câble RJ-45 pour les connexions
* 1x Ordinateur tour avec un serveur virtuel Ubuntu

## Planning

Voici le planning initial généré sur Github :



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.

# SAN et NAS

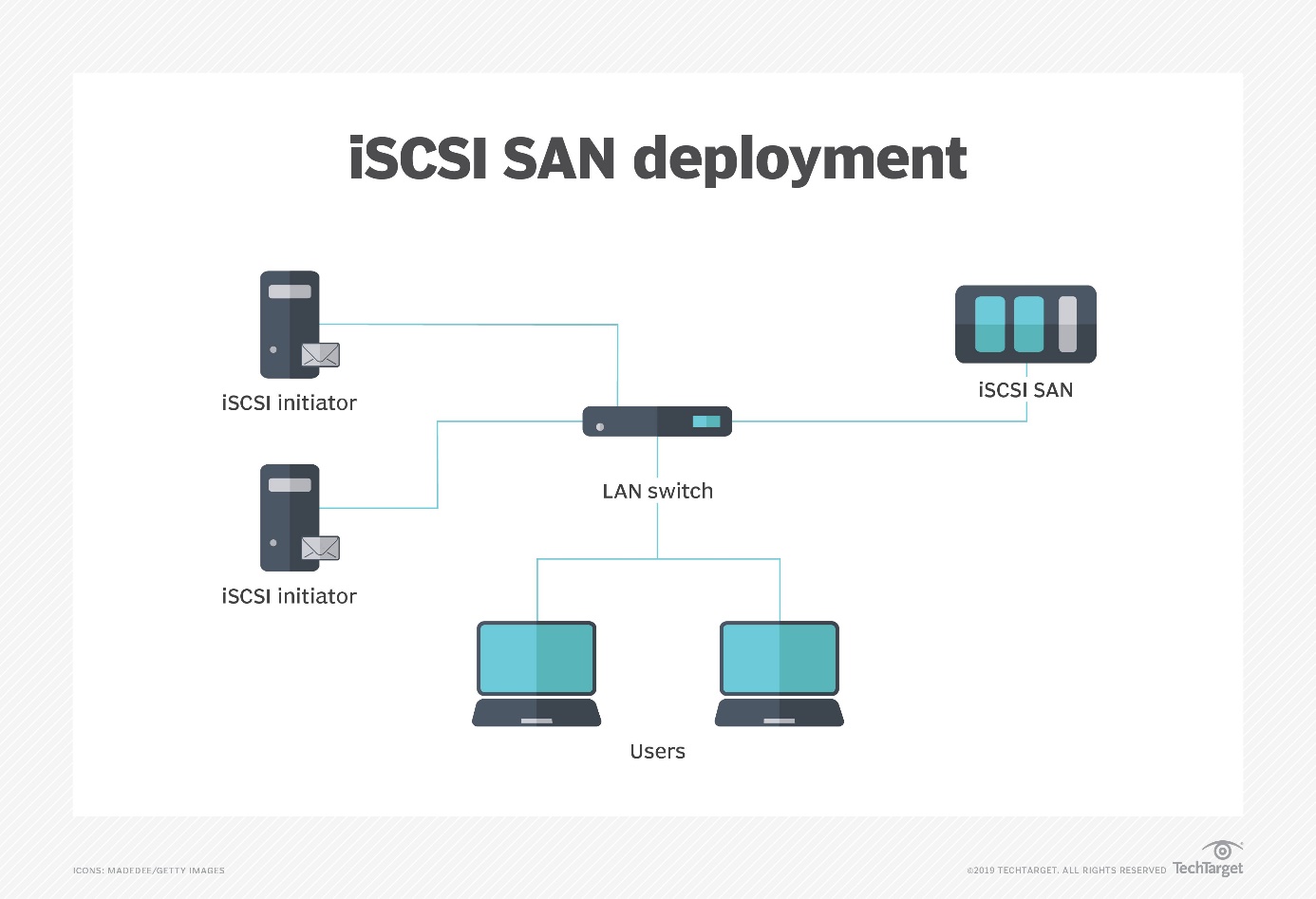
Tout d’abord, avant de se lancer sur ce qu’est le protocole iSCSI, il va falloir comprendre dans quel but nous allons l’utiliser.

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 à accès.

# Protocole iSCSI

* 1. 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).

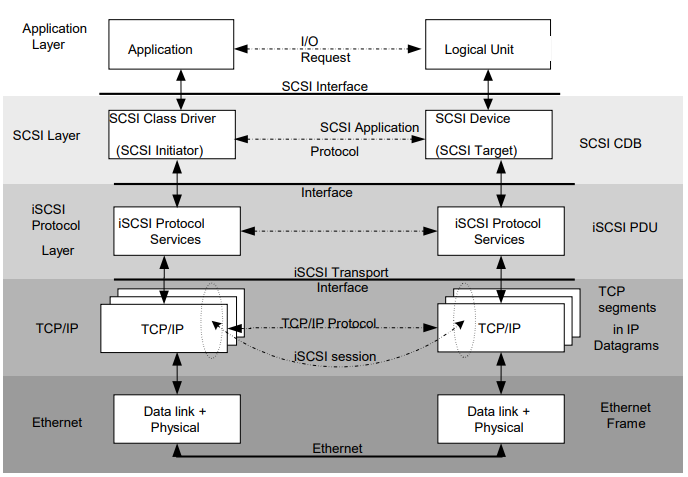
Dans l’ordre d’encapsulation, nous avons :

* 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

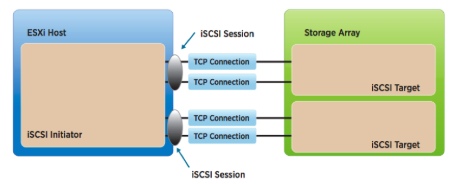
Voici une image montrant les différentes couches d’iSCSI :



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 précèdent.

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 gérer si nous souhaitons 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.

## 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 authentification :** (Challenge-Handshake Authentification 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 un 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) :

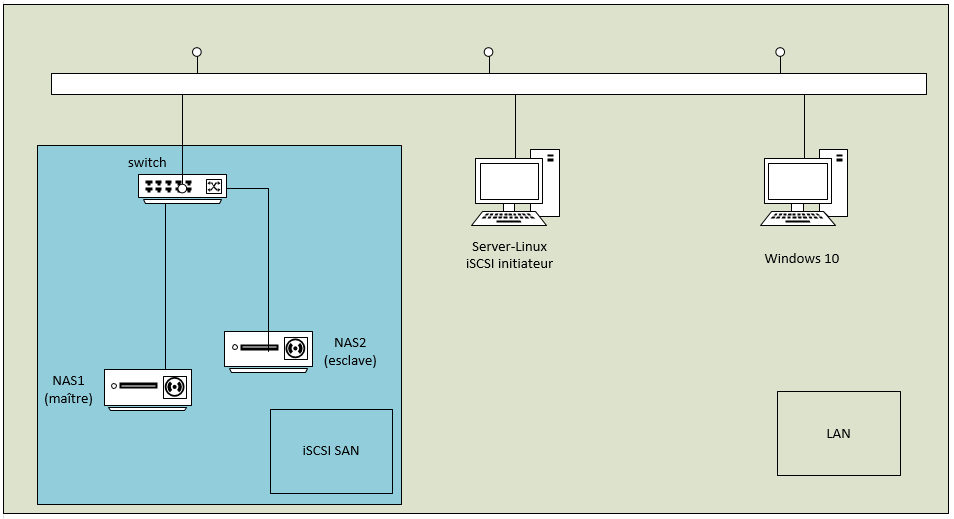
* **RADIUS Authentification :** (Remote Authentification Dial-In user Service) Permet un accès à un serveur pour garantir l’authentification.
* **IPSec Authentification :** Comme le CHAP authentification n’est pas assez sécurisé, ce protocole offre une couche de sécurité supplémentaire sur le paquet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

# 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.

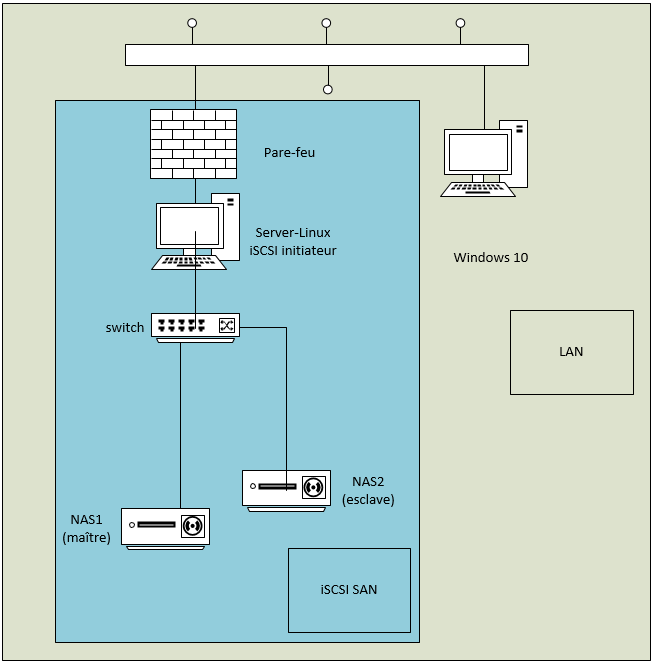


Nous constatons qu’il existe un LAN avec un SAN sur le même réseau. Le SAN est donc ouvert et à portée de tous les utilisateurs sur le réseau. Ce n’est donc pas une bonne idée. En effet, il se peut qu’une personne mal intentionnée ou ne faisant pas exprès perturbe le fonctionnement du SAN et de ce fait 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.

Pour la construction de notre réseau, nous allons donc 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.

# 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 »[[1]](#footnote-1). 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.

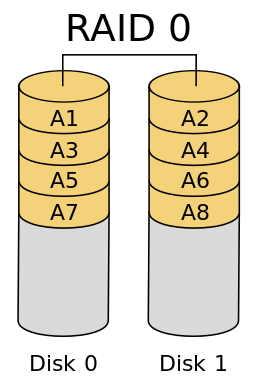
Nous allons donc créer une redondance avec les deux NAS. L’un, dit maître, sera celui sur lequel les informations sont directement stockées. L’autre, dit esclave, servira à enregistrer les backups du maître et en garantir la sécurité avec une redondance. Ainsi si un problème survient sur le maître, nous 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.

## Les RAID

La dernière phrase du paragraphe précèdent 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 le 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 :

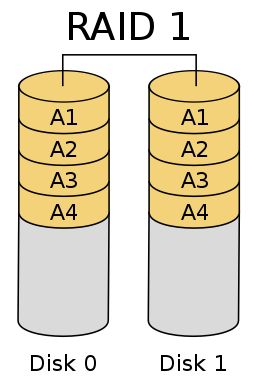


Comme on peut le voir, les informations se divisent sur deux différents disques, formant une grappe, et si nous souhaitons écrire ou lire des informations, ces actions seront faites deux fois plus rapidement. Le gros problème avec cette disposition est qu’il suffit qu’un seul des disques rencontre un problème et ne peut plus être utilisé et c’est la totalité des données qui est perdu. 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 ‘agrandit’. 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 :

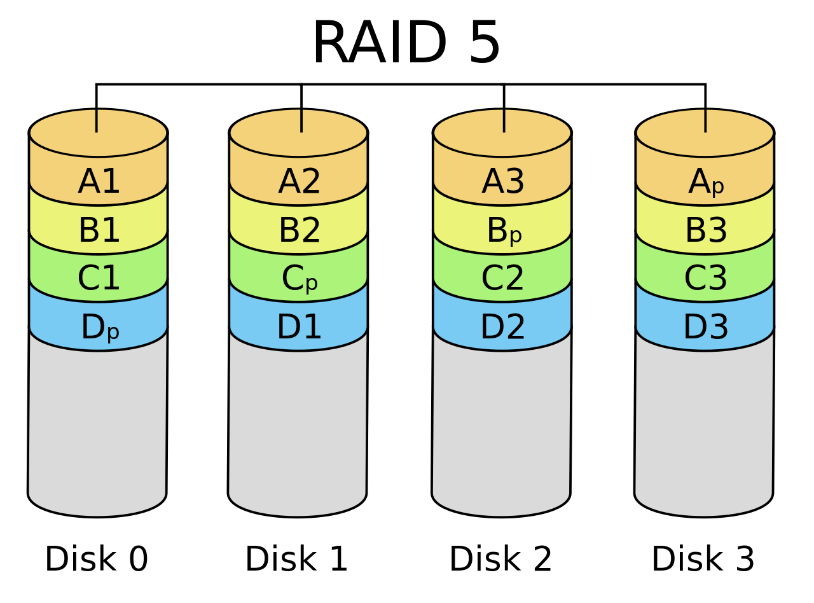


Comme on peut le constater, les informations sont dupliquées et donc, contrairement au RAID 0, elles sont sécurisées en cas de perte d’un des deux disques. Ici, un minimum de deux disques se doit d’être utilisé.

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 ajouté 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 disque 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.

## Les types de backups

Il existe trois types de backups, les voici :

### 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 recrée 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

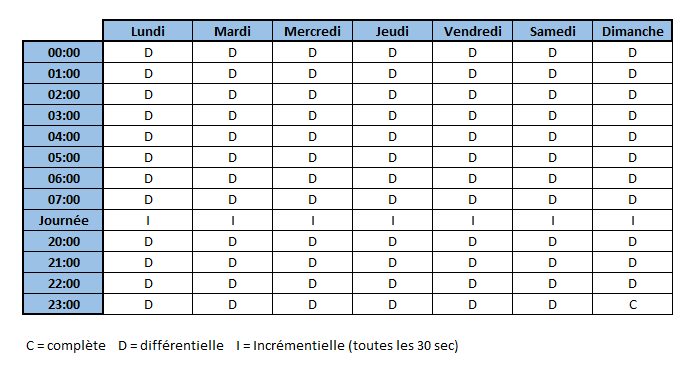
Ici, nous avons la technique la plus légère. Cette technique va aussi demander une sauvegarde complète et à partir de celle-ci, faire des backups réguliers. Elle ne prendra en compte que les fichiers modifiés, mais au lieu de prendre référence sur la complète, elle va regarder son ancienne sauvegarde 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.

## Le choix pour le réseau

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 :



# Montage de la redondance

# Montage du service iSCSI

# Problèmes rencontrés

# Modification du planning

Ayant fini le premier sprint et le second sprint avec beaucoup d’avance, j’ai modifié les dates, ce qui va me laisser plus de temps pour la mise en place de la redondance des NAS et l’iSCSI.



# Conclusions

# Sources

## 11.1 SAN et NAS

<https://en.wikipedia.org/wiki/Storage_area_network>

<https://waytolearnx.com/2018/07/difference-entre-san-et-nas.html>

<https://www.laurentbloch.net/MySpip3/NFS-SANs-et-NAS>

## 11.2 Protocole iSCSI

<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>

## 11.3 [Architecture réseau](#_Toc32504790)

## 11.4 [Redondance NAS](#_Toc32504791)

<https://fr.wikipedia.org/wiki/RAID_(informatique)>

<https://fr.wikipedia.org/wiki/Sauvegarde_(informatique)>

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

## 11.5 [Montage de l’infrastructure](#_Toc32504792)

## 11.6 [Montage de la redondance](#_Toc32504793)

## 11.7 [Montage du service iSCSI](#_Toc32504794)

1. *https://www.larousse.fr/dictionnaires/francais/redondance/67331* [↑](#footnote-ref-1)