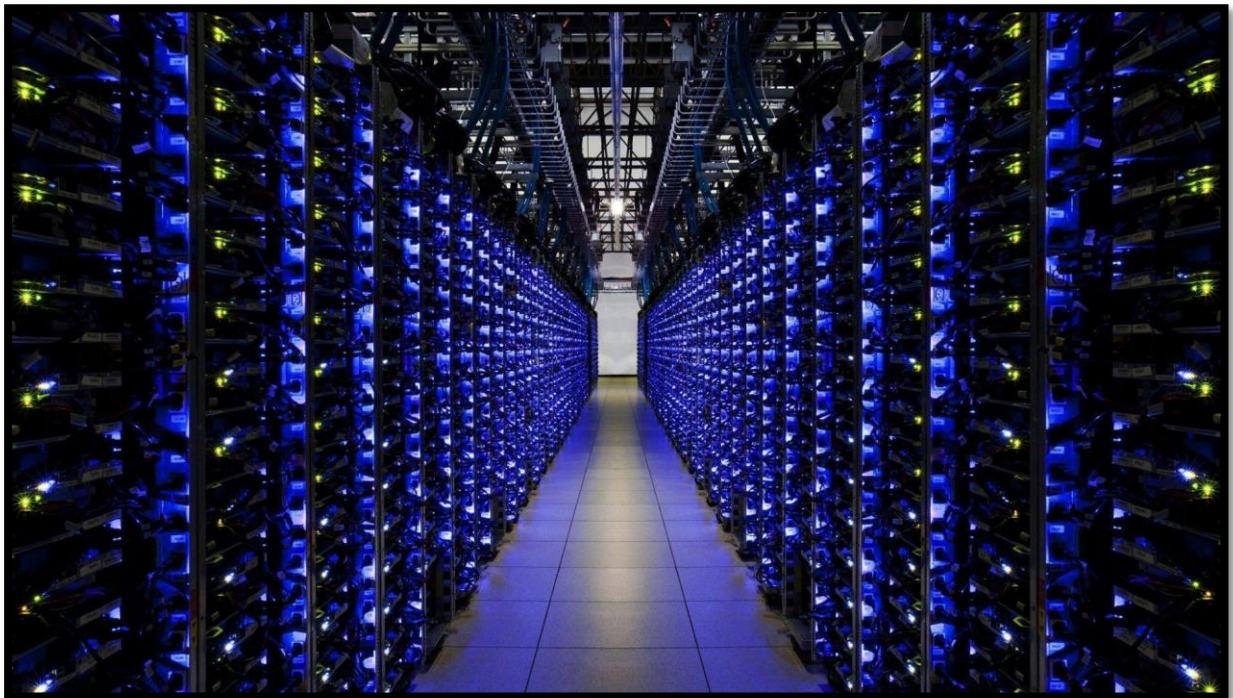


EPSIC – 2018

Module ICT 143

Rapport du groupe 3 – Winston, Quentin, Pablo, Dylan



1 Table des matières

1	TABLE DES MATIÈRES	2
2	PARTIE 1	6
2.1	Casino de Montreux	6
2.1.1	Introduction	6
2.1.2	Traitement de données.....	6
2.1.3	RGPD - Actions et mesures prises.....	6
2.1.4	Techniques de protections des données.....	6
2.1.5	Technologies utilisées	6
2.1.6	PRA et PCA.....	6
2.1.7	Suite Google	7
2.2	La Loterie Romande	9
2.2.1	Introduction	9
2.2.2	Les données au sein de la Loterie Romande	9
2.2.3	Actions et mesures	9
2.2.3.1	Protections logiques	9
2.2.3.2	Protections techniques	9
2.2.4	Stratégies de sauvegardes	10
2.2.4.1	Infrastructures	10
2.2.4.2	Stratégie de conservation des sauvegardes	10
2.3	VTX.....	13
2.3.1	Introduction	13
2.3.2	Les techniques utilisées	13
2.4	Université de Lausanne	15
2.4.1	Présentation entreprise	15
2.4.2	Présentation du système	15
2.4.3	Problématique.....	15
2.4.3.1	Hardware	15
2.4.3.2	Humaine	16
2.4.3.3	Évènement majeur.....	16
2.4.3.4	Archivage.....	17
2.4.4	Les stratégies de sauvegardes.....	17
2.4.4.1	Cohesity.....	17
2.4.4.2	Networker	17
2.4.4.3	Avamar	18
2.4.5	Les stratégies en cas de récupération	18
3	PARTIE 2.....	18
3.1	Lois sur les protections des données	18
3.1.1	LPD.....	18
3.1.2	RGPD	18
3.1.2.1	Première chose à se demander : Qu'est qu'une donnée personnelle ?	18
3.1.2.2	En vrai, à quoi servent ces deux lois ?	19
3.1.2.3	Qui est concerné ?	19
3.1.3	Mise en conformité	19
3.1.4	Organisation et actions :	19

3.1.5	Mesures techniques adéquates.....	20
3.2	Les disques durs et le systèmes RAIDs	20
3.2.1	Raid Logiciel et matériel	21
3.2.1.1	Raid matériel.....	21
3.2.1.2	Raid Logiciel	21
3.2.2	Le JBOD (Just A Bunch Of Disks):.....	21
3.2.3	RAID 0 (entrelacement) :	22
3.2.4	RAID 1 (écriture miroir) :	22
3.2.5	RAID 1E (écriture miroir entrelacée) :	22
3.2.6	RAID 5 (entrelacement avec parité) :	23
3.2.7	RAID 5EE (Hot Space)	23
3.2.8	RAID 6 (entrelacement avec double parité) :	23
3.2.9	RAID 10 (ensembles RAID 1 entrelacés) :	24
3.2.10	RAID 50 (ensembles RAID 5 entrelacés) :	24
3.2.11	RAID 60 (ensembles RAID 6 entrelacés) :	24
3.2.12	Raid DP	24
3.3	Les différents systèmes de stockages.....	25
3.3.1	Première génération – supports physiques	25
3.3.1.1	Le ruban perforé	25
3.3.1.2	La carte perforée	25
3.3.2	Deuxième génération – supports magnétiques.....	25
3.3.2.1	La bande magnétique	25
3.3.2.2	La cassette audio.....	26
3.3.2.3	La cassette vidéo.....	26
3.3.2.4	Le disque dur	26
3.3.2.5	La disquette	27
3.3.3	Troisième génération – supports optiques	27
3.3.3.1	Le disque compact	27
3.3.3.2	Le DVD	27
3.3.3.3	Le Blu-ray	28
3.3.4	Quatrième génération – supports numériques	28
3.3.4.1	La clé USB.....	28
3.4	La connectique des systèmes de stockage.....	28
3.4.1	USB	28
3.4.2	ATA.....	29
3.4.3	SATA	29
3.4.4	Le PCI Express.....	30
3.4.5	mSATA	30
3.5	Les types de sauvegardes.....	31
3.5.1	Sauvegarde complète.....	31
3.5.1.1	Point positif :	31
3.5.1.2	Point Négatif :	31
3.5.2	Sauvegarde incrémentale.....	31
3.5.2.1	Point positif :	31
3.5.2.2	Point Négatif :	31
3.5.3	Sauvegarde différentielle	31
3.5.4	Sauvegarde décrémentationale	32
3.6	Onduleurs – UPS	32
3.6.1	Types d'UPS.....	32
3.6.1.1	Off-line (Passive Standby).....	32
3.6.1.2	In-line (Line-Interactive):.....	33

3.6.1.3	On-line (Double conversion)	34
3.6.2	Comment choisir son Onduleur	35
3.7	DRP – Plan de reprise d’activité	36
3.7.1	RTO	36
3.7.2	RPO	36
3.7.3	Schématisation d’un incident.....	36
3.8	iSCSI	37
3.8.1	Utilité	37
4	PARTIE 3.....	38
4.1	Mise en conformité LPD/RGPD	38
4.2	Infrastructure Informatique	38
4.3	Backup.....	40
4.3.1	SERVEUR SQL	40
4.3.2	SERVEUR DE MESSAGERIE	40
4.3.3	SERVEUR DE FICHIERS	40
4.3.4	SERVEUR WEB	41
4.3.5	SERVEUR AD	41
4.3.6	CLOUD	41
4.4	Reprise d’activité.....	41
4.4.1	RTO	41
4.4.2	RPO	41
5	SOURCES	42

Casino de Montreux



2 Partie 1

2.1 Casino de Montreux

2.1.1 Introduction

Le casino de Montreux est le premier casino de Suisse en termes de résultat brut des jeux, il appartient au Groupe Barrière, groupe français de divertissement (hôtels, casinos, spas...). Le groupe possède deux autres casinos en Suisse : Fribourg (Granges-Paccot) et Courrendlin (Jura).

2.1.2 Traitement de données.

Le Casino de Montreux traite un nombre considérable de données, principalement en raison du Club Barrière (programme de fidélité du casino) et aussi pour des raisons juridiques, une fois que toutes les entrées sont sauvegardées par le but de prestation de comptes à la CFMJ.

2.1.3 RGPD - Actions et mesures prises.

Le casino a formé deux DPO et nommé des responsables de traitement par secteur (exemple RH, Marketing, etc.) ainsi comme des suppléants aussi formés pour le traitement de données.

Le rôle des responsables de traitement de donnée est de tenir un registre à jour de tous les fichiers contenant des données personnelles (selon procédure mise en place par le DPO). Ensuite tout est validé par le DPO. Le DPO met en place des nouvelles mesures de traitement et sécurité, il doit aussi former les utilisateurs selon les principes juridiques et mesures de sécurité.

2.1.4 Techniques de protections des données.

La sécurité des données est déjà en place avec des backups journaliers, clustering, firewall, portes sécurisées, utilisateurs avec mots de passe, entre autres.

2.1.5 Technologies utilisées

On utilise aussi les **Raids 1 et 1+0**, cette technique assure la protection des données de la baie de disques (**SAN**) avec une redondance permanente.

Une **réplication des données** hors site est en place sur un deuxième SAN sur un des casinos distants.

L'armoire serveurs est protégé contre les coupure électrique par moyen d'un **UPS** de type On-line.

Une documentation est en place afin de garantir la reprise d'activité.

2.1.6 PRA et PCA

Afin d'apporter une totale redondance des services et des données nous utilisons un système PRA-PCA. Le PCA, visant à assurer la continuité, est composé d'un Cluster HP physique qui héberge un cluster de serveurs SQL virtuels.

Le PRA est composé d'une documentation complète afin d'assurer la reprise d'activité de l'entreprise.

2.1.7 Suite Google

En 2018 le groupe Barrière a passé à utiliser la suite Google d'application et services. Cette suite comprend la messagerie (Gmail), les outils bureautique (Sheets, Docs, Slide, etc), espace de stockage Cloud (Drive), entre autres.

Le projet de migration est long et lent, car les utilisateurs doivent suivre des formations, et les responsables de la DSI doivent suivre les bonnes pratiques, afin de faire la migration d'une manière propre.

Ce nouveau projet impliquera un changement d'infrastructure informatique, vu que les NAS et SAN ne seront plus utilisés pour le stockage des fichiers partagés.

La Loterie Romande



2.2 La Loterie Romande

2.2.1 Introduction

Le but de la Loterie Romande est d'organiser et exploiter, avec les autorisations prescrites par la loi, des loteries et paris comportant des lots en espèces ou en nature et d'en destiner le bénéfice net à des institutions d'utilité publique – sociale, culturelle, de recherche ou sportive – profitant aux cantons romands.

2.2.2 Les données au sein de la Loterie Romande

La Loterie Romande traite un grand nombre de données, majoritairement en raison des jeux d'argent et des données clients que cela importe d'avoir. La société doit se plier à LPD et au RGPD car des clients Suisses ou étrangers à la Suisse peuvent aussi jouer aux jeux d'argent de la société. Toutes ces données doivent donc être gérées très sérieusement car cela représente beaucoup de données sensibles.

Nos normes standards concernant ces lois au point de vue sécurité sont toutes issues de l'ISO 27001.

2.2.3 Actions et mesures

2.2.3.1 Protections logiques

Toutes les données de la Loterie Romande sont stockées en interne dans des Datacenter. Ces données ont une rétention de 10 ans sur l'archivage. L'archivage se fait dans les serveurs de la Loterie, aucun archivage papier n'est présent.

Chaque collaborateur de la Loterie Romande doit suivre une journée d'information concernant la sécurité physique et logique lors de sa première journée de travail dans l'entreprise. Cette formation sert à instruire les collaborateurs des risques potentiels qu'ils pourraient faire et ce qu'il faut éviter.

Afin de vérifier si notre système de sécurité est fiable, nous procédons à un audit technique. Chaque mois un scan complet de nos systèmes est effectué.

2.2.3.2 Protections techniques

L'accès à nos sites, nos serveurs, nos Datacenter, nos armoires de câbles se font soit par l'intermédiaire de l'Active Directory soit par un système de badge et de code.

Les serveurs de productions sont répliqués de manière synchronisée sur deux Datacenter.

Pour gérer nos logs, nous possédons une grosse base de données dans laquelle tous nos logs sont répertoriés. Ces logs sont contrôlés par une autre entreprise.

Dans l'entreprise nous chiffons tous les flux ssl et https ainsi que nos cassettes de sauvegarde.

Afin de prévenir les virus, nous avons tous un antivirus sur nos postes, un système qui vérifie tous les mails entrants et un contrôle des flux http et https.

2.2.4 Stratégies de sauvegardes

2.2.4.1 Infrastructures

Au sein de la Loterie Romande nous utilisons la Logiciel « Net Backup » pour tout ce qui concerne la récupération des données sur les serveurs. Chaque service est dupliqué sur deux sites différents en prévision d'un problème.

Master/EMM

Nous avons deux serveurs « Net backup Master » qui vont principalement servir d'ordonnanceur. Ces deux serveurs sont tous deux reliés par un SAN qui va non-stop les répliqués au cas où il y aurait un problème.

Media

Nous avons deux serveurs « Media » qui serviront d'intermédiaire entre les masters et les datas domains.

Stockage online

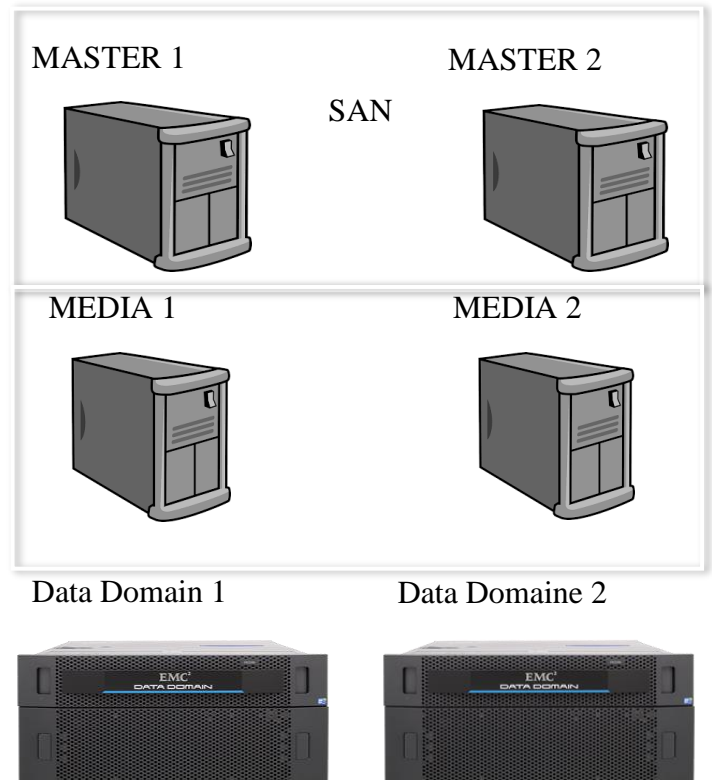
Nous avons deux serveurs Data Domaine qui sont dupliqués qui reçoivent des ordres de l'ordonnanceur par l'intermédiaire des « Media ».

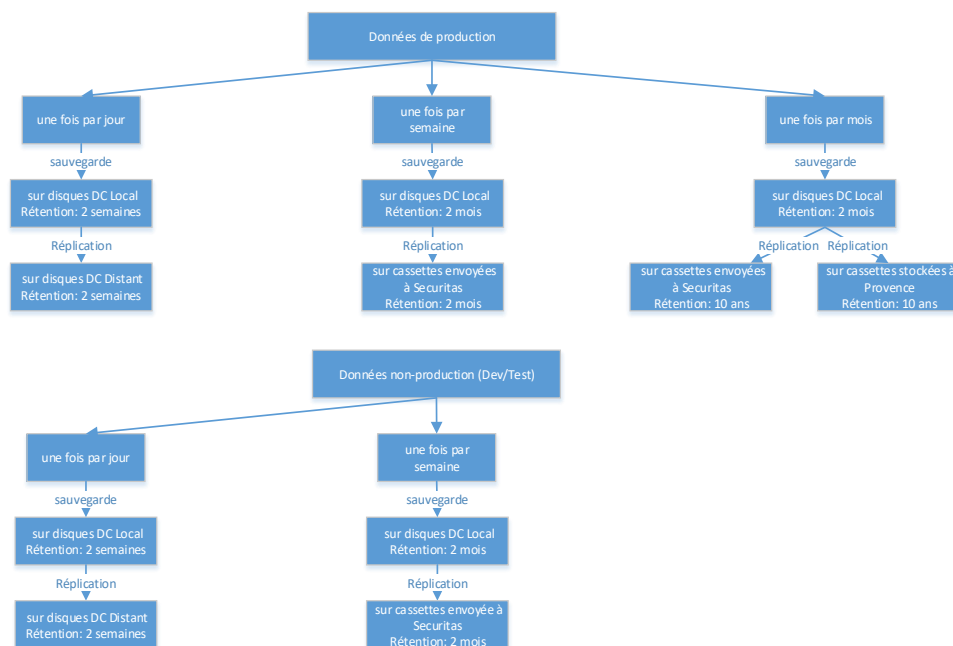
Stockage externalisé

Nous faisons des sauvegardes sur des cassettes que nous conserverons 10 ans chaque sauvegarde et répliquée, une est envoyée à Securitas et nous concevront la deuxième.

2.2.4.2 Stratégie de conservation des sauvegardes

Le diagramme ci-dessous reflète la stratégie :





Les données de production et de non production sont identifiées par serveur. En cas de doute sur le type de données stockés sur certains serveurs, ils seront traités comme étant des serveurs de production. De même que pour les serveurs d'infrastructure nécessaire à la restauration et l'exploitation des données de production (exemple : Microsoft Active Directory, environnement DNS...).

VTX



2.3 VTX

2.3.1 Introduction

VTX est une entreprise qui occupe la télécommunication. La société a été fondée en 1989 et son nom signifie Videotex. Le siège est à Pully et nous avons d'autre succursale à Genève, Sion et Bâle.

Nous fournissons :

- Internet
- Téléphonie
- Nom de domaine
- Hébergement
- Mail
- Sécurité de réseau informatique
- Télévision
- Cloud

2.3.2 Les techniques utilisées

Pour conserver nos données nous utilisons comme technologie Bacula / Veam et notre hardware est du NetApp. Le tout est conservé en VHD.

Nous enregistrons toutes les 3 semaines en bande magnétique en cas d'attaque grave via un ransomware.

Nos données sont sécurisées physiquement par un lieu inconnu et ne sont accessibles que par l'équipe qui s'occupe des backups.

Les sauvegardes se font toutes les 8 heures et sont sauvegardées sur plusieurs de nos Datacenter.

En cas de récupération de nos données, nous envoyons des mails à tous nos clients via un système automatique en 48 heures. Si nous avons leurs portables dans la base de données le programme leur envoie aussi un SMS.

Ensuite VTX au niveau de la LPD et le RGPD se situe dans les entreprises où cette protection doit s'appliquer de la façon la plus rigoureuse, dû au fait qu'elle détient l'intégralité des données personnelles des clients.

Nous avons par exemple des mesures où le renouvellement de mot de passe n'est même plus visible pour les employés concernés aux bords de 24 heures.

Université de Lausanne



UNIL | Université de Lausanne

2.4 Université de Lausanne

2.4.1 Présentation entreprise

L'Université de Lausanne, bâtiment dédié aux étudiants, professeurs et chercheurs universitaires, est un bâtiment qui regroupe pas moins de 15'000 étudiants et 5'000 employés situés sur les bords du Lac Léman, et il est composé de 7 facultés : médecine-biologie / sciences sociales / lettre / théologie / géosciences / droit / commerciales (HEC). Ce bâtiment a eu ses débuts en 1537 et l'une des plus vieilles sociétés de Suisse. Nous respectons la LPD et la GDPR, car nous avons des employés qui habitent sur le territoire européen (hors suisse).

2.4.2 Présentation du système

Les systèmes sont distribués sur trois centres de calculs répartis sur le campus de l'Université de Lausanne. On peut distinguer trois familles d'équipement :

Serveur virtuel & SAN : Il existe 650 serveurs virtuels hébergé sur 14 hosts vxrail connecté à un SAN ceci dupliqué sur deux sites. Cela représente 180TB de données pour les SAN et 112Tb de données pour les serveurs.

NAS : Deux NAS fournissent un stockage de 1.26Pb aux utilisateurs.

Postes individuels : Il y a environ 5'000 postes de travail à travers le campus.

2.4.3 Problématique

Afin de préserver les données de manière sécurisée, nous avons plusieurs problématiques à résoudre comme la défaillance d'un disque, des événements catastrophiques majeurs, la suppression de données intentionnelles ou encore la mise en panne d'un nœud.

Pour cela, L'UNIL applique la règle 3-2-1 qui consiste à garder trois copies des données, l'original et 2 jeux de données qui sont stockées sur 2 médias différents avec une copie qui se trouve en dehors de l'entreprise. Voici les solutions mises en place pour se prémunir des problèmes cités plus haut :

2.4.3.1 Hardware

- **Serveur**

Les deux serveurs SAN sont montés en mode raid 51. C'est-à-dire que sur deux sites, les SAN sont en RAID5 et la réplication entre eux est un RAID1 (miroir) sur le SAN qui se trouve sur le site2. De cette façon, nous avons une protection accrue des données, car nous pouvons perdre un SAN complet, mais les données seront toujours préservées sur l'autre site.

- **NAS**

Les deux NAS sont construits en cluster¹, c'est-à-dire qu'un NAS dispose de plusieurs nœuds² qui forment un seul système de fichiers. Les utilisateurs n'ont pas la perception des espaces de stockage et ne peuvent pas déterminer sur quel disque dur sont disposés leurs documents. Lorsqu'on introduit un fichier dans le NAS, il est découpé en bloc et est répliqué plusieurs fois entre les différents nœuds. Grâce à cette méthode, les fichiers restent accessibles en haute-disponibilité et cela évite une surcharge des serveurs et augmente les performances, car les nœuds se répartissent le travail. Un calcul de signature est fait pour arranger les différents blocs afin de retrouver les données. La donnée est alors répliquée en forme de bloc et elle est redondante. Si un nœud vient à tomber en panne, la donnée se retrouvera dans un autre nœud et sera retrouvée grâce à la parité.

De plus, Le cluster primaire est répliqué de manière asynchrone toutes les 4 heures sur le cluster secondaire disponible dans un autre lieu sur le campus. Le second cluster est accessible qu'en read-only afin que les fichiers ne soient pas modifiables. Si le cluster primaire venait à tomber en panne, nous pourrions basculer les utilisateurs sur le cluster secondaire. Par la suite, il faudra reconstruire le cluster primaire et le resynchroniser avec les données du cluster secondaire.

2.4.3.1.1 Individuel

Les postes de travail individuel peuvent être, selon les choix du collaborateur, sauvegardés chaque jour avec le logiciel Crash Plan. Sur les 5'000 machines que possède l'UNIL, seulement 200 machines utilisent cette solution. Le faible nombre de postes de travail qui sauvegarde leur machine s'explique, car les utilisateurs enregistrent leurs données sur les serveurs. La rétention des documents avec ce logiciel est de 3 mois. De cette façon, nous nous préservons de la défaillance d'un disque dur d'un poste de travail.

2.4.3.2 Humaine

2.4.3.2.1 Protection contre la malveillance

Afin d'éviter qu'un employé supprime l'ensemble des sauvegardes faites par l'UNIL, l'accès de ses données est restreint à 2 personnes. L'un détient la clé pour accéder aux sauvegardes des machines virtualisées et la seconde personne ne détient que les sauvegardes des fichiers. De cette façon, une seule et même personne ne pourrait pas détruire l'ensemble des données stockées de l'UNIL. L'accès des centres de calculs est protégé par un système de badge.

2.4.3.2.2 Erreurs humaines

Une sauvegarde des fichiers est effectuée 2 fois par jour, à midi et le soir. Le fichier antécédent est alors disponible via l'historique des fichiers Windows. La rétention des copies est de trois mois.

2.4.3.3 Évènement majeur

Il se peut qu'une catastrophe naturelle ou un incendie se produise sur le campus, les données sont alors sauvegardées sur des disques et exportées sur un lieu externe de manière

¹ Le Cluster est une grappe de serveurs qui regroupe plusieurs ordinateurs sous forme de nœuds. https://fr.wikipedia.org/wiki/Grappe_de_serveurs

² Un Nœuds est un ensemble disposant d'un CPU est d'un système de stockage, il est généralement de plusieurs disques durs. [https://fr.wikipedia.org/wiki/N%C5%93ud_\(r%C3%A9seau\)](https://fr.wikipedia.org/wiki/N%C5%93ud_(r%C3%A9seau))

physique. Cette sauvegarde est aussi offline, elle n'est pas accessible via le réseau pour éviter tout accès par l'extérieur. La sauvegarde est une « incremental-forever backup¹ », elle est effectuée chaque mois et est stockée sur un serveur Linux en dehors du campus. La sauvegarde est alors conservée pour toujours et elle est utilisée en dernier recours.

2.4.3.4 Archivage

La quantité de données de l'UNIL à sauvegarder étant conséquente, nous utilisons la déduplication pour compresser les données. Ce système est assez pratique et permet de gagner énormément d'espace, le gain d'espace est tel que les données sont de 50x à 70x fois plus légères. Il permet de mettre ensemble les blocs qui se répètent, et un index est créé pour indiquer où se trouve-le ou les bloc/s compressé/s.

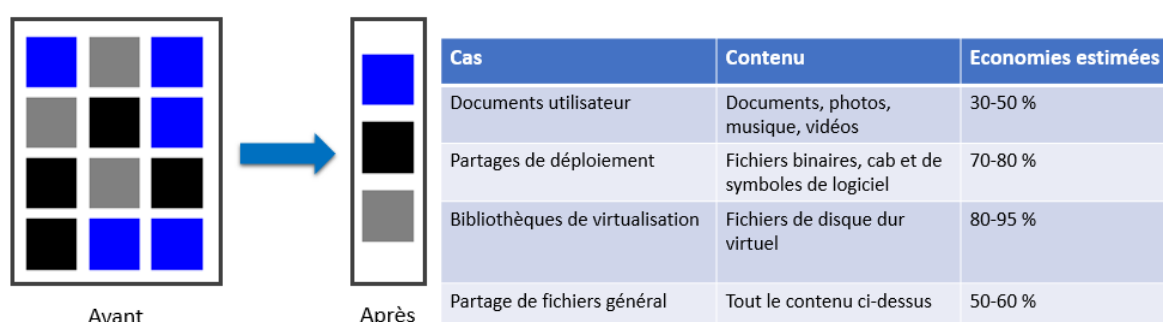


Figure 1 et 2 : <https://all-it-network.com/deduplication/>

2.4.4 Les stratégies de sauvegardes

L'UNIL utilise deux logiciels pour effectuer les sauvegardes des différents serveurs (serveur, serveur virtualisé, serveur de fichier).

2.4.4.1 Cohesity

Le logiciel Cohesity est utilisé pour les sauvegardes ponctuelles des 650 machines et machines virtualisées. Il effectue une image de chaque VMs de manière quotidienne en incrémental, sauf le samedi où il effectue une sauvegarde complète. Les sauvegardes incrémentales se font par un système CBT(Change Block Tracking), où les données sont enregistrées sous forme de blocs, seuls les blocs qui ont changé sont sauvegardés. Les sauvegardes effectuées par Cohesity passent par une connexion dédiée uniquement aux sauvegardes afin d'avoir une sécurité contre une attaque extérieure.

La rétention des sauvegardes est de 90 jours et le RPO maximum est de 24 heures.

2.4.4.2 Networker

Networker permet la sauvegarde de certaines bases de données au fil de l'eau et aussi de proposer une conservation jusqu'à trois mois des documents pour les serveurs.

¹ L'incremental-forever backup est une sauvegarde où on effectue une seule fois au début une sauvegarde full et on effectue en continue une sauvegarde incrémentale.

Network effectue une sauvegarde quotidienne incrémentale chaque nuit sauf le samedi, car il effectue une sauvegarde full chaque vendredi. La rétention des fichiers est de 3 mois selon les directives de la SLA (Service Level agreement).

Il est également utilisé pour sauvegarder les données du serveur Microsoft exchange de manière particulière.

Un Recover Point Objective (RPO) d'un maximum de 24 heures pour les fichiers et un RPO maximum de 8h pour les bases de données.

2.4.4.3 Avamar

Les sauvegardes des images de machine virtuelle dans un site distant s'effectuent à l'aide d'Avamar. Il effectue les sauvegardes en « incrémental forever-backup ».

2.4.5 Les stratégies en cas de récupération

La restauration des données est faite selon le point de sauvegarde le plus récent ou la demande de la date précisée par le collaborateur. La restauration ne demande aucun spécialiste IT s'il utilise le point de restauration Windows, les utilisateurs sont capables de le faire eux-mêmes sur le serveur. Concernant les postes individuelles, à condition que les collaborateurs aient souscrit à une sauvegarde avec le logiciel Crash Plan. Il peut également restaurer ses données de lui-même.

En cas d'un problème d'un serveur virtualisé, le logiciel Cohesity est utilisé pour restaurer la machine ou un fichier.

3 Partie 2

3.1 Lois sur les protections des données

Avec la mise en place de la RGPD au niveau européen, et la révision de la LPD au niveau suisse, une réflexion sur l'état actuel de la situation a été menée, qui amène plusieurs entreprises à se mettre à niveau en parlant de traitement des données.

3.1.1 LPD

La loi fédérale sur la protection des données a entrée en vigueur le 1 juillet 1993, cette dernière vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données (LPD art1).

3.1.2 RGPD

L'Union Européenne représentée par son parlement a voté une Loi afin d'assurer le bon traitement des données personnelles ses citoyens, la **RGPD** (règlement général sur la protection des données). Cette dernière, entrée en vigueur le 25 mai 2018, vise à donner aux citoyens plus de contrôle sur leurs données personnelles, à responsabiliser davantage les entreprises et à renforcer le rôle des autorités de protection des données.

3.1.2.1 Première chose à se demander : Qu'est qu'une donnée personnelle ?

Toutes les informations qui se rapportent à une personne identifiée ou identifiable (art3 LPD). Par exemple : Nom et prénom, numéro de passeport, etc.

3.1.2.2 En vrai, à quoi servent ces deux lois ?

La LPD et RGPD ont été mises en place afin d'éviter la mauvaise utilisation des données de la personne, comme par exemple le profilage, vu dernièrement dans le scandale Facebook et Cambridge Analytica.

3.1.2.3 Qui est concerné ?

Toutes les entreprises, organes fédéraux ou personnes privées traitant des données personnelles d'un tiers, avec quelques exceptions, comme par exemple : LPD art2 al2a « elle ne s'applique pas aux données personnelles qu'une personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers ; ».

3.1.3 Mise en conformité

Principes Juridiques (liste pas exhaustive) :

Licéité, bonne foi, proportionnalité, finalité, reconnaissabilité et exactitude.

- Principe de la **bonne foi** : la collecte doit se faire dans la loyauté, de manière transparente
- Principe de la **proportionnalité** : les données doivent être aptes, objectivement nécessaires pour atteindre le but poursuivi ;
- Principe de **reconnaissabilité** : la collecte et la finalité du traitement doivent être reconnaissables pour la personne concernée ;
- Principe de **finalité** : la collecte, le traitement des données doivent se faire dans un but préalablement défini. Quid du big data ?
- Principe **d'exactitude** des données (droit de rectification)
- Principe de **sécurité** : des mesures techniques et opérationnelles doivent être prises pour protéger les données et éviter tout traitement non autorisé

3.1.4 Organisation et actions :

- Nommer Un DPO (Digital protection Officer), responsable par but principalement permettre à un organisme effectuant des traitements de données personnelles de s'assurer qu'il respecte bien la réglementation applicable à leur protection.
- Mentions d'informations : Les personnes concernées doivent être informées de qui est derrière la collecte, de combien de temps seront conservés les fichiers, la finalité des données collectées et les informer sur comment elles peuvent exercer leurs droits.
- Être en mesure de répondre aux sollicitations d'une personne à accéder à ses données, aussi les modifier et supprimer selon sa volonté. Par exemple la mise en place d'un formulaire de contact.
- Demander l'accord aux personnes et leur donner la possibilité de retirer cet accord.
- Mettre en place des mesures de sécurité adaptées à la sensibilité de la donnée sauvegardée. Données sensibles, exemple : ethnie ou race, religion, options sexuelles, etc.
- Analyser les fichiers et tenir un registre de traitements des données.

3.1.5 Mesures techniques adéquates

RGPD oblige le responsable du traitement à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Elle assure aussi l'obligation de notifier à l'autorité de contrôle les violations 72h au plus tard.

Voici une liste de mesures de sécurité à prendre :

- Sensibiliser les utilisateurs ;
- Authentifier les utilisateurs ;
- Tracer les accès et gérer les incidents ;
- Sécuriser les postes de travail ;
- Sécuriser l'informatique mobile ;
- Protéger le réseau informatique interne ;
- Sécuriser les serveurs ;
- Sécuriser les sites web ;
- Sauvegarder et prévoir la continuité d'activité ;
- Archiver de manière sécurisée ;
- Encadrer la maintenance et la destruction des données ;
- Sécuriser les échanges avec d'autres organismes ;
- Protéger les locaux ;
- Encadrer les développements informatiques ;
- Chiffrer, garantir l'intégrité ou signer.

3.2 Les disques durs et les systèmes RAIDs

La technologie RAID qui veut dire Redundant Array of Independent Disks a été créée pour joindre plusieurs disques et ainsi diminuer le prix de stockage. Ce fut créée en 1987 pour remplacer les disques plutôt chers de 6.5 et 9.5 pouces par des ensembles formés de disques de 3.5 pouces. Nous l'avons ensuite amélioré et développé pour accélérer et sécuriser notre stockage.

Les RAID sont utilisables partout et par n'importe qui mais leurs utilisations sont vraiment importantes en entreprise. Un particulier n'aura pas forcément besoin de 4 disques durs travaillant en redondances pour sauvegarder de simples photos, vidéos etc...

Les systèmes RAIDs sont compatibles avec tout type d'utilisation sur ordinateur comme les travaux de virtualisation (VMware, Microsoft Hyper-V, etc...), bases de données (Microsoft SQL et Oracle), les systèmes de courrier électronique comme Microsoft Exchange etc.

Voici une liste non exhaustive des systèmes RAIDs :

- Le JBOD (Just A Bunch Of Disks)
- RAID 0 (entrelacement)
- RAID 1 (écriture miroir)
- RAID 1E (écriture miroir entrelacée)
- RAID 5 (entrelacement avec parité)
- RAID 5EE (Hot Space)
- RAID 6 (entrelacement avec double parité)

- RAID 10 (ensembles RAID 1 entrelacés)
- RAID 50 (ensembles RAID 5 entrelacés)
- RAID 60 (ensembles RAID 6 entrelacés)

3.2.1 Raid Logiciel et matériel

Un système Raid peut être créé de deux formes : Logiciel et matériel.

3.2.1.1 Raid matériel

Le Raid matériel est un système indépendant qui gère le flux de données par moyen d'un périphérique connecté sur un hôte (pc, serveur, etc.), ses performances sont indépendantes de celles de l'hôte, ce qui fait que ses traitements de données soient beaucoup plus rapides que sur un raid logiciel.

Le Raid matériel est un contrôleur, il peut donc recevoir plusieurs disques, en revanche l'hôte sur lequel il est connecté en voit qu'un seul.

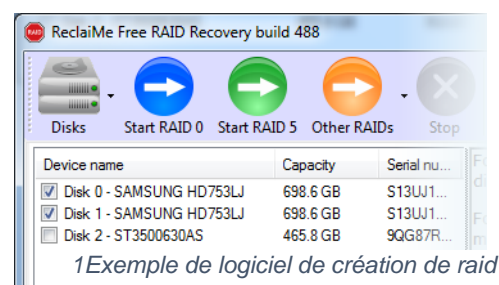


	RAID logiciel	Raid matériel
Recopie de disque de secours	Non	Oui
Disque de secours dédié	Non	Oui
Code basé sur le micrologiciel pour isoler la protection RAID des plantages du système d'exploitation	Non, basé sur le pilote	Oui
Récupération des données à la suite de plantages système de l'OS, de paniques et d'écrans bleus	Non	Oui
Reprise automatique après une coupure de courant	Reconstitution, CC, BGI	RLM, OCE, Reconstitution, CC, BGI
Protection de la mémoire cache intégrée avec batterie de secours	Non	Oui
Services de cryptage pour les disques durs SED	Non	Oui
Protection de la mémoire cache intégrée	Non	Oui

Figure 1 Fonctions de protection des données généralement disponibles dans les solutions de RAID matériel et non incluses dans le RAID logiciel

3.2.1.2 Raid Logiciel

Différemment du raid matériel les système raid logiciel n'ont pas besoin d'une carte dédié pour fonctionner, ce dernier utilise le noyau de l'hôte sur lequel il est configuré. Ce système est plus accessible car c'est l'hôte qui va gérer le traitement de données, c'est une solution moins couteuse mais aussi moins performante.



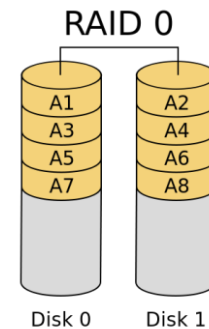
3.2.2 Le JBOD (Just A Bunch Of Disks):

Ce RAID permet de rassembler tous nos disques en seul virtuel. Si vous avez des disques de 12, 33 et 44 Go sa vous fera un disque de 89 Go

3.2.3 RAID 0 (entrelacement) :

Le RAID 0 permet comme le JBOD de lier plusieurs disque dur ensemble en un seul. La différence est qu'il améliore les performances en vitesse mais les disques doivent être identiques car sinon il se calque sur le disque le plus petit.

L'amélioration en vitesse vient du fait que par exemple s'il a envie d'enregistrer un fichier de 1 giga il va enregistrer à chaque fois 200 méga en même temps sur chaque disque pour alléger la tâche et l'accélérer. Si l'un des disques casse nous perdons toutes les données.



Nbs de disques au minimum : **2**

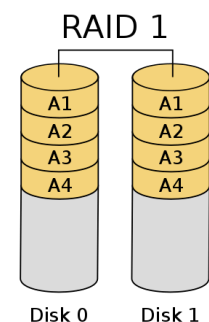
Avantage(s) : **grande vitesse**

Perte de disques max : **1**

Calcul volume : $\text{nbDisk} * \text{singleDiskSize} = \text{capacity}$ (ex : deux disques de 1TB = $2 * 1 = 2$ TB)

3.2.4 RAID 1 (écriture miroir) :

Le RAID 1 lui fait une copie sur l'autre disque et crée ainsi un miroir identique. Grâce à cela nous pouvons perdre un des disques et le remplacer par un autre sans perte. Le problème est que ce RAID ne marche qu'à 50% des capacités des disques. 2 disques de 100 Go ne feront que 100 Go.



Nbs de disques au minimum : **2**

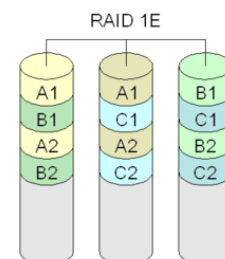
Avantage(s) : bonne protection de données

Perte de disques max : **n-1** (nbDisk - 1)

Calcul volume : 50% du volume total

3.2.5 RAID 1E (écriture miroir entrelacée) :

Le RAID 1E mélange le RAID 0 et 1. Il est utilisable à partir de 3 disques et est utile sur un nombre impair de disques (*"En cas d'utilisation d'un nombre pair de disques, il est toujours préférable d'utiliser RAID 10"*). Il permet d'avoir le bonus de vitesse du RAID 0 et la sécurité du RAID 1. Il utilise lui aussi 50% de l'intégralité des disques durs.



Nbs de disques au minimum : **3**

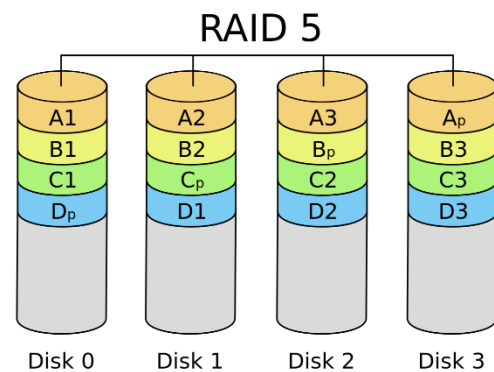
Avantage(s) : grande vitesse et bonne fiabilité

Perte de disques max : **1**

Calcul volume : 50% du volume total

3.2.6 RAID 5 (entrelacement avec parité) :

Le RAID 5 Utilise l'entrelacement des données dans une technique de stockage conçue pour assurer au cas de la perte d'un disque, mais ne nécessite pas la duplication des données comme RAID 1 et RAID 1E. Les données sont entrelacées sur tous les disques de la pile, chaque disque a ces informations de parité. Les performances en lecture sont donc très bonnes, mais les écritures sont pénalisées en ce que les données de parité doivent être recalculées et enregistrées en même temps que les nouvelles données. La capacité est de de [disque fois (x-1) EX : $60 \times (4-2) = 120 \text{ Go}$]



Nbs de disques au minimum : **3**

Avantage(s) : conçu pour assurer la perte d'un disque

Perte de disques max : **1**

Calcul volume: $(nbDisk - 1) * singleDiskSize = capacity$

3.2.7 RAID 5EE (Hot Space)

Au niveau de la protection, le RAID 5EE est équivalent au RAID 5. La différence est que le nombre d'écriture par seconde est plus grande grâce à l'utilisation d'un disque supplémentaire.

L'inconvénient du RAID 5EE est que le disque de secours ne peut être commun à plusieurs piles physiques, comme pourrait le faire le RAID 5.

Nbs de disques au minimum : **4 à 16**

Avantage(s) : conçu pour assurer la perte d'un disque

Perte de disques max : **1**

Calcul volume: $(nbDisk - 1) * singleDiskSize = capacity$

3.2.8 RAID 6 (entrelacement avec double parité) :

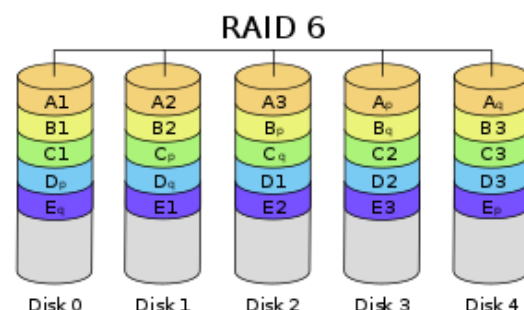
Le RAID 6 fonctionne comme le RAID 5 à part qu'il a une double parité. La vitesse d'écriture est moins bonne et il a besoin de 2 disques de secours mais il permet une perte de 2 disques. Le calcul de capacité est de de [disque fois (x-2) EX : $60 \times (4-2) = 120 \text{ Go}$]

Nbs de disques au minimum : **4**

Avantage(s) : plus grande sécurité

Perte de disques max : **2**

Calcul volume: $(nbDisk - 2) * singleDiskSize = capacity$



3.2.9 RAID 10 (ensembles RAID 1 entrelacés) :

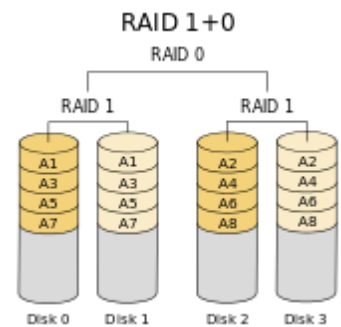
Le RAID 10 permet aussi comme le RAID 1^E d'avoir une vitesse de d'écriture accélérer tout en ayant du mirroring. La différence est qu'il marche avec des disques en nombre pair. L'architecture est 2 disques forme un disque en RAID 0 et un deuxième pair fait la même chose. Ensuite nous unissons les 2 disque que forment les paires pour faire un raid 1. Cela permet la perte de 1 disque et d'avoir une vitesse accélérer. Ça reste malgré tout un mode ou seulement 50% des capacité total des disques est utilisable.

Nbs de disques au minimum : 4

Avantage(s) : redondance des données et bonne vitesse d'écriture

Perte de disques max : 2

Calcul volume : 50% du volume total



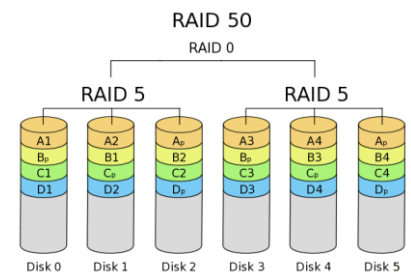
3.2.10 RAID 50 (ensembles RAID 5 entrelacés) :

Nbs de disques au minimum : 6

Avantage(s) : **volume agrégé**

Perte de disques max : 1

Calcul volume : trop teck à calculer



3.2.11 RAID 60 (ensembles RAID 6 entrelacés) :

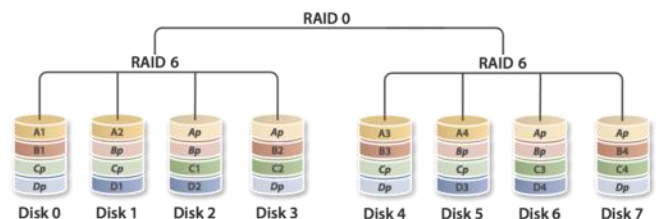
Le RAID 60 permet d'avoir 2 piles de disques en RAID 6 entrelacer en RAID 0. Chaque pile en RAID 6 a donc sa capacité à perde 2 disque et l'entrelacement entre chacune des piles accélère le traitement.

Nbs de disques au minimum : 8

Avantage(s) : beaucoup de disques avec redondance plus grande (la performance est nul)

Perte de disques max : 2

Calcul volume :



3.2.12 Raid DP

Le RAID DP est une technologie utilisée par les systèmes NAS. Le principe du raid dp et de reprendre en grande partie le système du raid 6 mais avec des disques à double parités fixes. C'est le seul système raid qui peut subir une perte de 2 disques dans un même groupe raid. Cette technologie est principalement utilisée par la société *NetApp*.

Nbs de disques au minimum : 4

Avantage(s) : peut supporter une perte de 2 disques sur un même groupe raid

Perte de disques max : 3

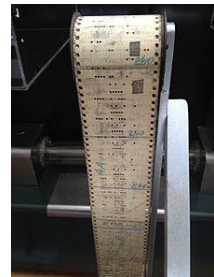
Calcul volume : (Nombre de disque – 2) * singleDiskSize = capacity

3.3 Les différents systèmes de stockages

3.3.1 Première génération – supports physiques

3.3.1.1 Le ruban perforé

Le premier ruban perforé est apparu en 1725. Son inventeur Basile Bouchon l'utilisa dans son métier à tisser. Cette technologie est très vite devenue obsolète dû à l'arrivée de la « carte perforée ».



3.3.1.2 La carte perforée

La carte perforée est l'un des premiers systèmes de mémoires de masse. Elles seront utilisées dans les débuts de l'informatique. La carte perforée est un perfectionnement du ruban perforé apparu dans les années 1884 pour donner des instructions à des machines analytiques.



Dans les années 1950, la spécification Hollerith/IBM apparait pour les cartes 8 colonnes. Sa longueur doit être de 187.32mm et sa largeur de 82.55mm avec une marge de 2 dixièmes. Il doit être propre (sans poussière) lors de son utilisation, afin de ne pas abimer la machine.

Les cartes perforées étaient généralement utilisées pour faire les traitements automatiques des bulletins de salaires, faire des calculs et des statistiques, écrire des codes sources.

3.3.2 Deuxième génération – supports magnétiques

3.3.2.1 La bande magnétique

La bande magnétique, développée en Allemagne en 1928, est utilisée pour enregistrer et écouter des informations analogiques ou numériques. Le magnétophone servira alors à écouter les signaux audios et le magnétoscope pour les signaux vidéo.

L'utilisation d'une bande magnétique se caractérisera à l'aide de la largeur de la bande et à son nombre de pistes.

Les bandes magnétiques sont très vite devenues le système de mémoire de masse par excellence.



Différentes générations de LTO :

- LTO-1 : Produit en 2000, taille native de 100 Go, compression 2 :1, débit 20 Mo/s.
- LTO-2 : Produit en 2002, taille native de 200 Go, compression 2 :1, débit 40 Mo/s.
- LTO-3 : Produit en 2004, taille native de 400 Go, compression 2 :1, débit 80 Mo/s.
- LTO-4 : Produit en 2007, taille native de 800 Go, compression 2 :1, débit 120 Mo/s.
- LTO-5 : Produit en 2010, taille native de 1.5 To, compression 2 :1, débit 140 Mo/s.
- LTO-6 : Produit en 2012, taille native de 2.5 To, compression 2.5 :1, débit 160 Mo/s.
- LTO-7 : Produit en 2015, taille native de 6.4 To, compression 2.5 :1, débit 300 Mo/s.

- LTO-8 : Produit en 2018, taille native de 12 To, compression 2.5 :1, débit 360 Mo/s.

Caractéristiques LTO :

Les différentes générations de LTO sont rétro-compatibles, elles sont capables d'écrire jusqu'à une génération en dessous (n-1) et de lire jusqu'à deux génération en dessous (n-2).

La dimensions d'une bande : 102 mm x 106.4 mm x 21.mm

Poids d'une cartouche : 200 g

3.3.2.2 La cassette audio

La cassette audio / minicassette / musicassette a été introduite par Philips. Une cassette contient deux bobines où est enroulée une bande magnétique.

Elle s'utilise pour écouter ou enregistrer des sons et s'utilise à l'aide d'un magnétophone. Plus tard, elles furent intégrées à des appareils plus complexes comme un autoradio ou un radiocassette.

Une cassette est composée de quatre canaux qui sont écrits en parallèle sur la bande, deux par côté. C'est pour cela qu'il faut retourner la cassette, chaque face comporte deux bandes.

Il existe différents types de cassettes, ces types se différencient par leurs matériaux de constructions et leurs performances :

- Type 1 – normale : de 30Hz à 15kHz
- Type 2 – chrome : de 30Hz à 16kHz
- Type 3 – ferrichrome : de 30Hz à 16kHz
- Type 4 – métal : de 30Hz à 18kHz

La durée d'une cassette peut varier en fonction de la longueur de la bande et de la vitesse de défilement.

3.3.2.3 La cassette vidéo

La cassette vidéo fonctionne de la même manière qu'une cassette audio : elle comprend une bobine de magnétique capable de défiler afin de pouvoir lire ou enregistrer des signaux audios ou vidéos.

Il existe différents formats de cassettes vidéo comme la VHS, le VCR, le U-matic, etc... La différence entre ces formats se caractérise par une différente largeur de bande pour la luminance et une différente largeur de bande pour la chrominance.

3.3.2.4 Le disque dur

Le disque dur aussi appelé Hard Disk Drive (HDD) est un support magnétique permettant de stocker des données sur de la mémoire morte. Apparue en 1980, il est à présent le système de stockage qui possède les plus importantes capacités de stockages du marché. La plus grosse capacité de stockage d'un seul disque dur est de 24 To mais en général la norme est plutôt entre 2 et 4 To.



Un disque dur possède en général un à huit plateaux tournant à plusieurs milliers de tours par minutes. Il possède aussi une tête de lecture qui se situe à la surface des plateaux. Les disques durs s'alimentent en général soit par connecteur Molex soit par Serial ATA ou SATA.



Caractéristiques :

Taille pour serveur et ordinateur fixe : 3.5 pouces

Taille pour ordinateur portable : 2.5 pouces

Le temps d'accès d'un disque dur (durée de déplacement de la tête de lecture d'un bloc de donnée à l'autre) dépend des caractéristiques du moteur et du nombre de plateau.

La vitesse de rotation est liée à la vitesse du moteur, plus le moteur sera efficace plus le taux de transfert sera élevé. De nos jours la majorité des disques ont une vitesse de rotation de 7200 tpm (tour par minute). Pour les disques serveurs la vitesse peut monter jusqu'à 10'000 ou 15'000 tpm.

3.3.2.5 La disquette

Après plusieurs années de tests, la disquette fut lancée par IBM en 1967. Les disquettes sont des supports de stockages de donnée amovible, elles sont aussi appelées disque souple (floppy disk).



Une disquette est composée de plusieurs pistes qui forment une sorte de cercles. La disquette est souvent divisée en 2 faces car les lecteurs sont équipés de deux têtes (Lecture / Ecriture). La capacité d'une disquette est en général aux alentours de 3Mo.

3.3.3 Troisième génération – supports optiques

3.3.3.1 Le disque compact

Le disque compact ou « Compact Disc » est un support de stockage optique. Il est lu par un faisceau laser infrarouge qui vient frapper le disque en rotation. En 1979, Philips et Sony Corporation ont collaboré pour inventer le disque compact.

Un CD-ROM possède en général ~700Mo de données et peut tourner à une vitesse linéaire de 500 tr/min pour permettre une lecture optimale.

Un CD audio a une longévité qui se situe entre 50 et 200 ans.

3.3.3.2 Le DVD

Créé en 1995, le DVD est un système de stockage optique qui stocke la donnée sous forme numérique. Le DVD fonctionne selon les mêmes principes que le disque compact mais avec des caractéristiques nettement supérieures.

Selon la catégorie un DVD peut stocker jusqu'à 18 Go. Le DVD possède différents formats qui se sont développés durant des années.



3.3.3.3 Le Blu-ray

Apparut en 2006, le Blu-ray est le successeur du CD et du DVD. Il fonctionne comme un DVD à la différence que le lecteur doit être doté d'un laser violet pour le lire. Le Blu-Ray est utilisé pour graver des vidéos en haute définition.

Un Blu-Ray peut contenir jusqu'à 27 Go ou 240 min de vidéo HD.



3.3.4 Quatrième génération – supports numériques

3.3.4.1 La clé USB

La clé USB est un support de stockage amovible, il se branche sur un port « Universal Serial Bus ». Une clé USB permet de stocker facilement des données et permet de transférer rapidement des informations d'un ordinateur à un autre.

Un avantage de la clé USB, c'est qu'elle ne peut pas se rayer et n'est pas sensible à la poussière. Elle est donc plus fiable.

La durée de vie de la donnée est estimée à 10 ans ou plus, mais cela va dépendre du modèle acheté.

Les vitesses de transferts diffèrent en fonction de la catégorie de la clé :

- USB 1.1 : 12Mbit/s
- USB 2.0 : 480Mbits/s
- USB 3.0 : 640Mbits/s



Ces valeurs sont bien évidemment théoriques et ne relate pas la vérité la vitesse de lecture sera toujours supérieure à la vitesse d'écriture.

3.4 La connectique des systèmes de stockage

La connectique utilisée dans les différents types de système de stockage change par rapport au volume de données voulant être traitées. Voici les types les plus courants :

3.4.1 USB

Type A : Ordinateurs, clés USBs, c'est le port de référence. Il offre une vitesse maximale théorique de 12 Mbit/s.



Type A (USB 3.0) :

Identique au port ci-dessus, la différence réside que ce port comporte 5 fils supplémentaires au qui permettent de faire transiter plus d'informations. Il est rétro-compatible avec le port standard. Il est reconnaissable par sa petite barre en bas qui est bleue. Il offre une vitesse maximale théorique de 5.0 Gbit/s



Micro B C'est le port que possèdent la majorité des téléphones actuels.

Micro B (USB 3.0) :

nouvelle version de la Micro B, qui contient en fait tous les fils du Micro B, plus une petite rangée de fils en plus comme pour le Type A, et qui est rétro-compatible mais seulement dans un sens (vous pouvez brancher une Micro B mâle sur une Micro B 3.0 femelle, mais pas l'inverse). Il offre une vitesse maximale théorique de 5.0 Gbit/s



Type C (USB 3.1) :

Ce nouveau connecteur, défini dans le standard USB 3.1, est totalement réversible (on peut le brancher à l'envers ou à l'endroit), est censé remplacer tous les connecteurs USB, et même les autres car il peut servir de connecteur vidéo (DisplayPort). Il offre une vitesse maximale théorique de 10 Gb/s (Gigabits, donc 1,25 Gigaoctets/s)



3.4.2 ATA

La connectique ATA (aussi appelé IDE pour *Integrated Drive Electronics*) conçue par Western Digital, utilise un câble avec 40 à 80 fils parallèles et des connecteurs identiques pour le contrôleur et pour les périphériques.

Les ATA sont utilisés uniquement internement et ne propose pas une connexion é chaud.



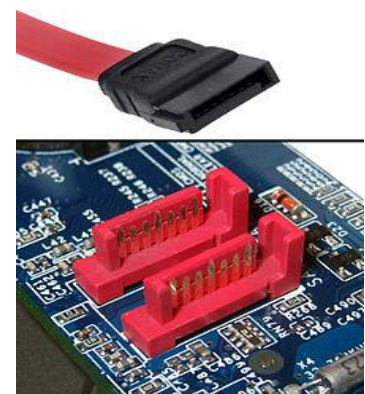
Vitesse de Débit: 16 MB/s puis 33, 66, 100 et 133 MB/s dans le plus recents.

3.4.3 SATA

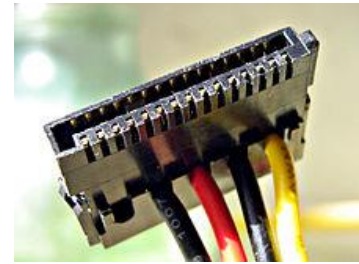
Le SATA, ou Serial ATA est un connecteur pour lecteur interne créé en 2003.

Vitesse de débit :

Le SATA a eu un débit maximal de 1.5 Gbit/s, soit 192 Mo/s, mais a connu plusieurs versions qui changèrent ceci : le SATA II a doublé la vitesse avec 3 Gbit/s (384 Mo/s) puis le SATA III avec 6 Gbit/s (768 Mo/s).



Il dispose de son propre câble d'alimentation :



3.4.4 Le PCI Express

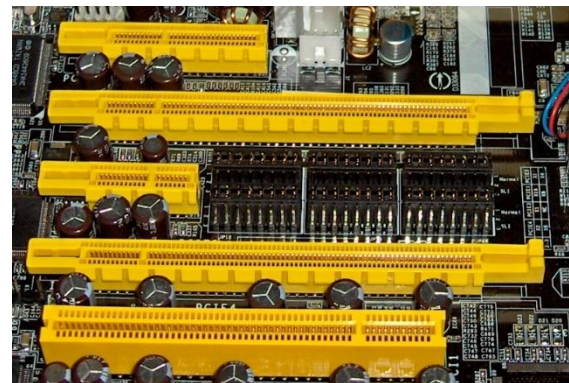
Abrégé PCI-E ou PCIe est un standard développé par Intel et introduit en 2004.

Il spécifie un bus local série (« bus PCI express ») et un connecteur qui sert à connecter des cartes d'extension sur la carte mère d'un ordinateur.

Un intérêt notable du bus PCIe est que deux cartes PCIe peuvent dialoguer entre elles sans passer par le processeur.

Tableau récapitulatif

	PCI-Express 4.x
Année d'introduction ^a	2017
Fréquence	100 MHz
Puissance max délivrée (12V+3V3)	75 watts
Bande passante	16 GT/s
Débit par ligne ^c	1969,2 Mo/s
Débit pour 16 lignes	31,508 Go/s
Compatibilité	PCIe x.x



3.4.5 mSATA

Le mSATA (m pour mini), est une version du protocole SATA utilisée dans les ordinateurs portable et aussi dans les appareils qu'utilisent des petits disques dur ou SSD. Même en étant plus petit que le SATA normal il offre les mêmes performances que ce dernier.

Vitesse de débit : 6 GBs



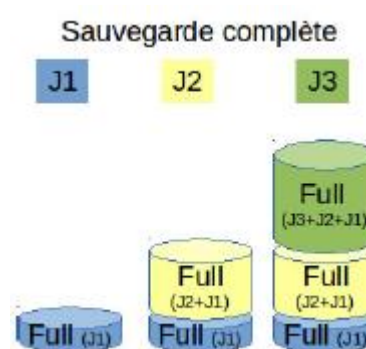
3.5 Les types de sauvegardes

3.5.1 Sauvegarde complète

La plus simple, elle sauvegarde toutes les données avec tous les répertoires et sous répertoires à chaque fois.

3.5.1.1 Point positif :

la plus fiable pour la restauration car il n'y a pas de calcul à faire ou de multiple réécriture.
la plus rapide pour la restauration de la sauvegarde car elle n'a pas de comparaison à faire ou de soustraction.



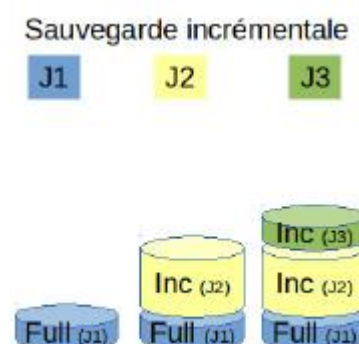
3.5.1.2 Point Négatif :

C'est la sauvegarde qui prend le plus de volumes de données. C'est aussi la plus longue à faire, car elle copie à chaque fois toutes les données alors que les autres types de sauvegarde vont en faire moins.

3.5.2 Sauvegarde incrémentale

3.5.2.1 Point positif :

Elle sauvegarde les modifications depuis la dernière sauvegarde, complète ou incrémentielle. Elle est accompagnée d'une première sauvegarde complète, qui sera le point de départ en cas de restauration, puis chaque incrémentielle sera ensuite restaurée, jusqu'à atteindre la sauvegarde voulue.



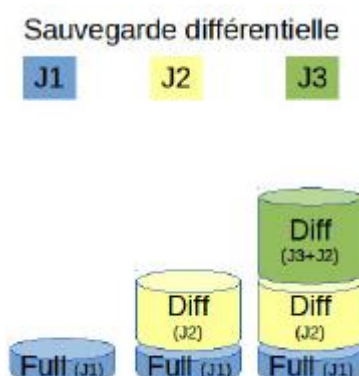
3.5.2.2 Point Négatif :

C'est la plus longue à restaurer, car TOUTES les sauvegardes depuis la dernière complète y compris doivent être restaurées une par une. C'est aussi la moins fiable, en premier lieu car elle prend plus de temps à être faite, avec de nombreuses réécriture, ce qui l'expose d'avantage à une panne qui engendrerait une corruption des données, mais aussi car les restaurations ne suppriment pas des fichiers déplacé ou dont le nom a changé

3.5.3 Sauvegarde différentielle

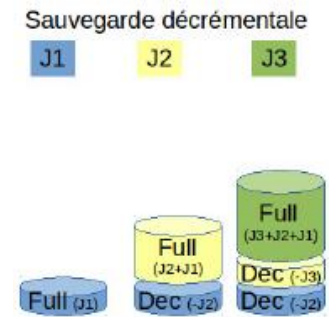
La sauvegarde différentielle effectue une première sauvegarde complète, puis chaque sauvegarde différentielle va comparer les modifications des fichiers comparé à la dernière sauvegarde complète.

C'est un compris entre la sauvegarde complète et l'incrémentale, elle équilibre les points positifs et négatif de chacun.



3.5.4 Sauvegarde décrementale

Ce type de sauvegarde n'est pas souvent utilisé car peu pratique. Elle consiste à effectuer une sauvegarde complète chaque jour et faire une sauvegarde décrementale qui va sauvegarder la différence entre le jour précédent et le jour actuel. Cette pratique nécessite d'avoir deux sauvegarde complète afin de pouvoir calculer le décrement.



3.6 Onduleurs – UPS

Un Onduleur (en anglais UPS pour Uninterruptible Power Supply) est un dispositif utilisé pour protéger des matériels électroniques contre les **pannes électriques**. Il est équipé d'une batterie de secours qui permet d'alimenter, pendant quelques minutes, ou de stabiliser les équipements branchés sur ce dernier en cas de :

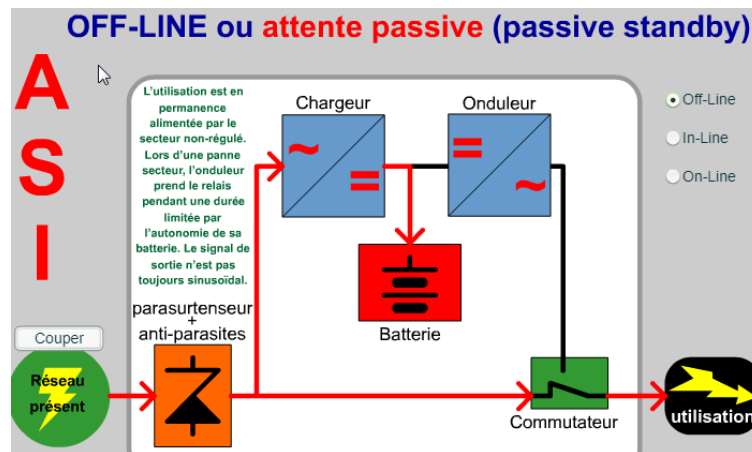
- **Coupure de courant** : Lors d'une coupure d'alimentation d'un matériel électronique l'onduleur utilise sa batterie de secours pour fournir quelques minutes de courant à ce dernier.
- **Surtension et Pics de tension** : Si la valeur de la tension qui passe dans l'onduleur est supérieure à la valeur maximale prévue pour le fonctionnement normal des appareils électriques connectés à l'onduleur.
- **Sous-tension** : C'est le contraire de la Surtension, quand la tension n'est pas suffisante pour le fonctionnement normal des composants électriques l'onduleur utilise sa batterie de secours pour stabiliser la tension.

3.6.1 Types d'UPS

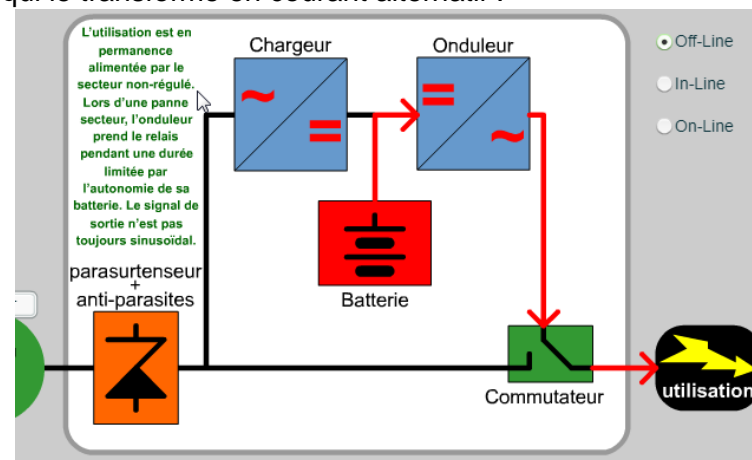
On trouve dans le marché, 3 familles d'onduleurs :

3.6.1.1 Off-line (Passive Standby)

- C'est le type le plus courant et le moins cher que l'on trouve dans le marché il est par contre celui qui fournit le moins de protection car il ne protège pas contre les microcoupures. Ce type d'UPS n'est pas conseillé si votre réseau électrique subit fréquemment des perturbations électriques
- Fonctionnement :
 - Le courant venant du secteur électrique passe par l'onduleur et alimente le matériel directement en passant juste par un **commutateur**. Un autre chemin fait le rechargement de la batterie en passant par un **redresseur** qui transforme le courant alternatif en continu :



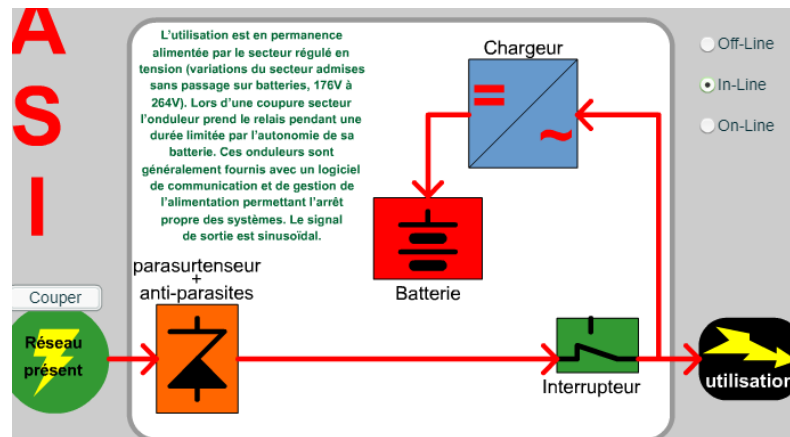
- En cas de coupure de courant le commutateur est activé et la batterie prend le relais, dans ce cas, le courant continue qui sort de la batterie passe par un onduleur qui le transforme en courant alternatif :



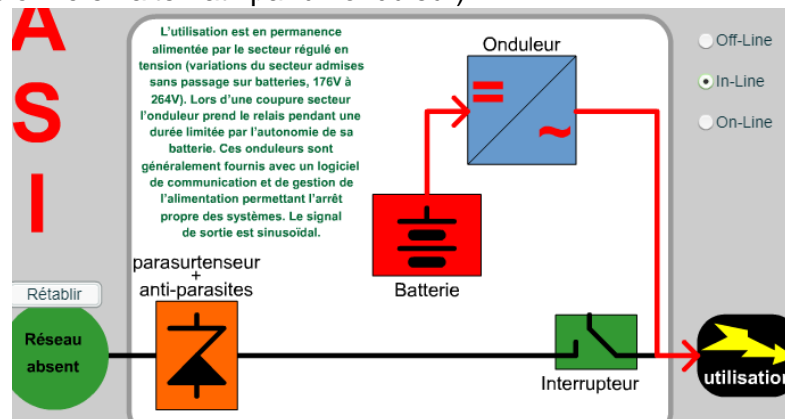
- Avantage :
 - Prix
- Désavantages :
 - Temps de bascule trop élevé.
 - En cas de sous-tension et surtension une bascule vers la batterie et aussi nécessaire.

3.6.1.2 In-line (Line-Interactive):

- C'est une version améliorée du Off-line.
- Fonctionnement :
 - Dans ce type d'UPS le matériel est alimenté en permanence par le secteur qui régule la tension fournie. Il fait aussi le rechargement de la batterie en passant par un transformateur de courant.



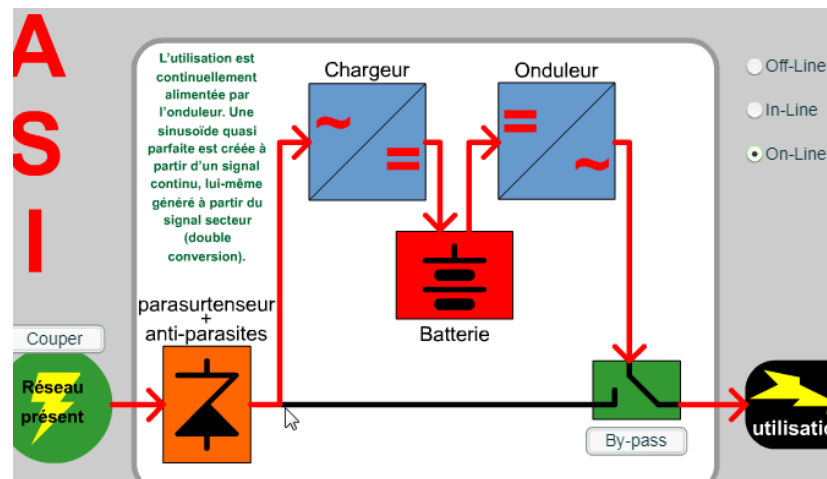
- En cas de coupure de courant la batterie de l'onduleur prend le relais pendant quelques minutes (selon puissance de l'onduleur) pour que l'utilisateur puisse sauver ses documents et arrêter l'équipement correctement (le courant continu est transformé en alternatif par un onduleur).



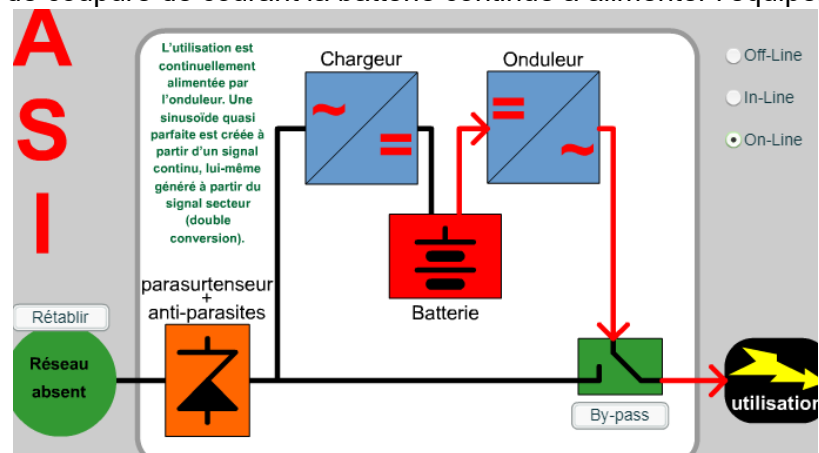
- Avantages :
 - Temps de bascule très court.
 - Logiciel fournis de gestion fourni avec, permettant de voir l'état de l'onduleur et d'arrêter automatiquement le système proprement en cas d'absence de l'utilisateur.
- Désavantages : Prix légèrement élevé.

3.6.1.3 On-line (Double conversion)

- C'est un onduleur hybride, son utilisation est conseillée même en cas de réseaux électriques très perturbés.
- Fonctionnement sans By-pass :
 - Le courant venant de la prise électrique passe par un redresseur qui transforme le courant alternatif en courant continu et ce dernier fait la recharge de la batterie.
 - Un autre courant continu sort de batterie et passe par un onduleur qui le transforme en courant alternatif permettant ainsi l'alimentation des matériaux connecté à la sortie de l'onduleur.



- En cas de coupure de courant la batterie continue à alimenter l'équipement.



- Fonctionnement avec By-pass :
 - Son fonctionnement est le même d'un onduleur Off-line.
- Avantages :
 - Temps de bascule vers la batterie égale à nul.
 - Conseillée même en cas de réseaux électriques très perturbés
 - Logiciel de gestion et d'arrêt automatique.
- Désavantages : Prix

3.6.2 Comment choisir son Onduleur

Maintenant que nous connaissons les types d'onduleur et nous sommes désormais capables d'en choisir un selon notre utilisation, nous nous rendons compte qu'il existe des différents niveaux de puissances pour chaque onduleur.

- Notion de puissance
 - La puissance d'un onduleur est donnée en V.A (volts ampères). Pour bien choisir l'onduleur le mieux adapté il faut faire la somme de la consommation de tous les équipements que nous allons lui connecter.
 - En général les équipements informatiques expriment une consommation en Watts. Dans ce cas il faut convertir les Watts en VA avec la formule suivante :
 - Nombre de VA = Nombre de Watts / 0.66
 - Exemple :
 - 1 PC 300W
 - 1 écran 90W

- Somme 390W
- $VA = 390 / 0.66$
- $VA = 590VA$

3.7 DRP – Plan de reprise d'activité

Un plan de reprise d'activité (Disaster Recovery Plan) a comme objectif de prévoir par anticipation les mécanismes d'une infrastructure informatique dans les meilleurs délais. Ceci s'applique lors d'un important sinistre ou d'incidents.

Le plan de reprise d'activité diffère du plan de continuité d'activité :

- Le plan de reprise d'activité sera la solution technique permettant la reprise suite à un sinistre informatique.
- Le plan de continuité d'activité est un document générique et surtout stratégique, planifiant et détaillant les types d'actions pour gérer une catastrophe ou un sinistre grave.

Les plans de reprise d'activité sont conçus et évoluent en fonction des besoins du business.

3.7.1 RTO

Le RTO, La Durée maximale d'interruption admissible (Return Time on Objective) détermine la durée maximale acceptable pendant lequel une ressource informatique peut être indisponible suite à un sinistre.

Cette durée d'interruption comprend :

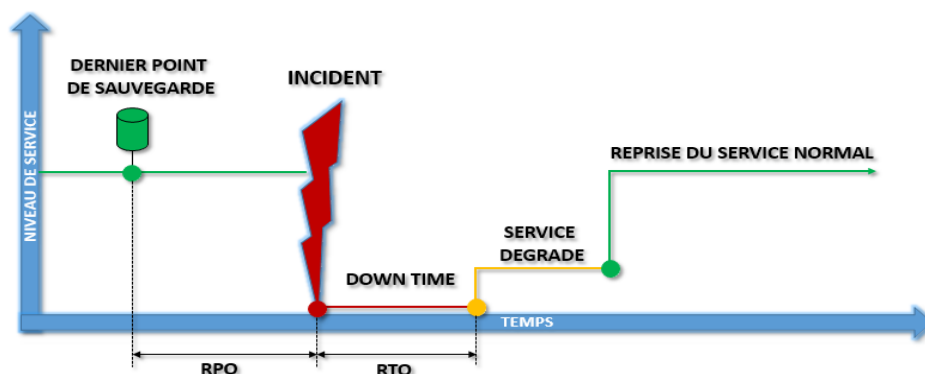
- Le délai de détection
- Le temps nécessaire à la décision pour lancer la procédure de reprise
- Le délai de mise en œuvre du plan de reprise d'activité

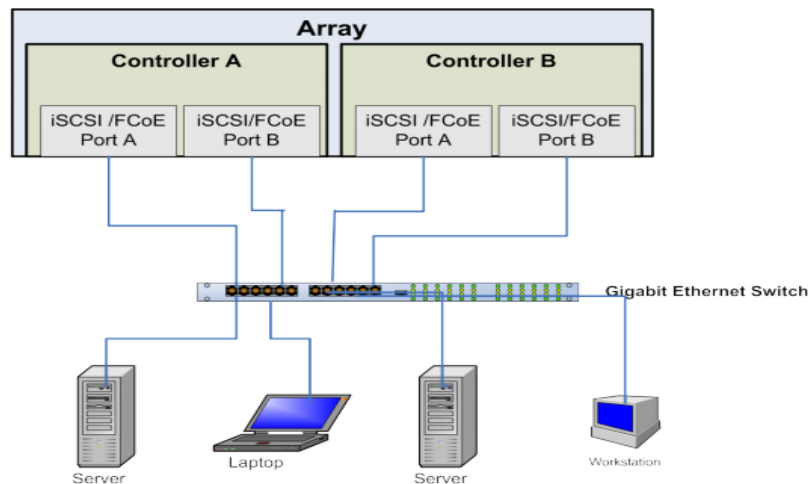
3.7.2 RPO

Le RPO, La Perte de Données Maximale Admissible (Recovery Point Objective) détermine la quantité maximale de données qui peut être perdue suite à un sinistre. Cette quantité est la différence entre la dernière sauvegarde valide et le sinistre.

3.7.3 Schématisation d'un incident

Le schéma ci-dessous représente l'évolution du niveau de service dans le temps :





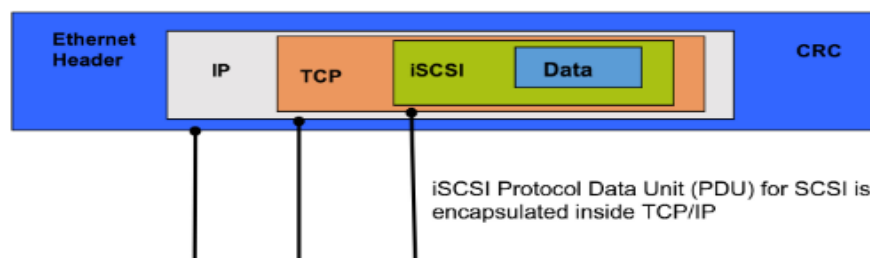
3.8 iSCSI

Le iSCSI (acronyme pour Internet Small Computer System Interface) est un standard de stockage en réseaux en utilisant le protocole internet (IP) pour relier une interface et un dispositif de stockage de données.

3.8.1 Utilité

Pendant trois ans IBM a lancé dans ses laboratoires des recherches afin de trouver un protocole intermédiaire entre l'**IP** et le **SCSI** (standard pour la connexion des dispositifs de stockage), le **iSCSI** ou **SCSI** sur **IP**.

Le protocole **iSCSI** est né afin de pouvoir interconnecter des sous-systèmes de stockage ou de sauvegarde en utilisant le réseau IP et les infrastructures de transport qui le soutiennent (Ethernet, ATM, etc).



iSCSI n'est rien d'autre qu'un traducteur qui transforme les paquets IP en blocs de données SCSI et inversement. Il est comparable au protocole de téléchargement de fichiers FTP.

Afin de simuler une connexion logique continue, iSCSI envoie plusieurs connexions TCP simultanément, elles seront considérées comme un seul canal de transmission et identifiées comme de la même session iSCSI. Les instructions et les données iSCSI sont envoyées en désordre. Le destinataire doit avoir un **contrôleur iSCSI** (un pilote logiciel ou une carte adaptatrice spécifique), ce dernier mettra les instructions et les segments de blocs de données dans leur bon ordre.

4 Partie 3

Pour cette troisième partie, nous partons du principe que l'entreprise, dont on doit planifier une stratégie de sauvegarde et de restauration en cas de problèmes, est une entreprise de taille moyenne et qui traite des données sensibles.

L'entreprise n'a pas de budget spécifié, c'est pour ça que nous avons choisi des équipements et des stratégies de haute gamme ou d'une qualité considérable.

4.1 Mise en conformité LPD/RGPD

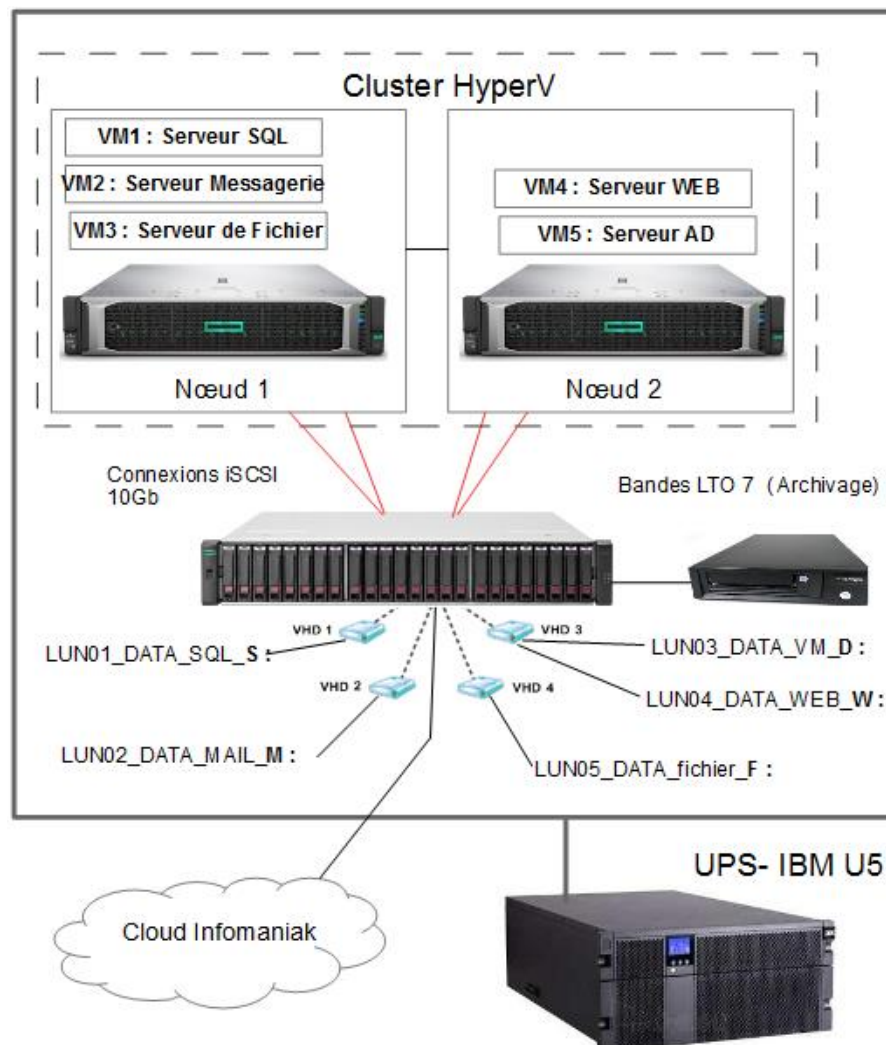
- Sensibiliser les utilisateurs :
 - Création d'une charte informatique à signer par les utilisateurs.
 - Documentation avec des consignes et conseils de comment traiter les données personnelles.
- Authentifier les utilisateurs et sécuriser les postes de travail :
 - Création d'un domaine AD
 - Création des comptes nominatifs pour tous les utilisateurs traitant des données personnelles.
 - Badges d'accès (ID unique), pour les accès aux locaux de stockage de données.
- Protéger le réseau informatique interne ;
 - Les actifs réseaux seront sécurisés par mot de passe administrateur (détenu uniquement par les administrateurs et par le directeur de l'entreprise).
- Sécuriser les serveurs ;
 - Sécurisé par mot de passe administrateur (détenu uniquement par les administrateurs et par le directeur de l'entreprise).
 - Antivirus à jour ;
- Sauvegarder et prévoir la continuité d'activité ;
 - Plan de sauvegarde et de reprise d'activité.
- Archiver de manière sécurisée ;
 - Sauvegarde interne et externe.
- Encadrer la maintenance et la destruction des données ;
 - Les données devront être détruites s'elles ne sont plus utilisées depuis leurs buts atteints.
- Protéger les locaux ;
 - Les locaux informatiques devront être sécurisé par :
 - Portes sécurisé
 - Equipement anti-incendie

4.2 Infrastructure Informatique

Afin de garantir la totale **disponibilité des données** et ressources un système de **redondance** cluster HyperV avec deux nœud physique HP et une baie de disque HP pour le stockage (**SAN**) seront mis en place avec :

- 2 Serveurs HP ProLiant 380 G10
- Baie de disque HP 2040 max 24 disques.
 - 8 disques 600Go 10k en **Raid 1**
 - 4 VHD de 600Go :
 - VHD1 : LUN01, Stockage des données SQL, mappage du disque S :.

- VDH2 : LUN02, Stockage des données du serveur de messagerie, mappage du disque M :.
- VHD3 : LUN03, Stockage de données des Machines virtuels, mappage du disque D :
LUN04, Stockage des données du serveur WEB, mappage du disque W :.
- VHD4 : LUN05, Stockage des fichiers partagés, mappage du disque F :.
- 4 connexions **iSCSI** par câble SFP 10Gb directement sur les deux contrôleurs de la baie.
- **UPS – On-line IBM U5 11000VA**
 - Serveurs HP : 4x1600
 - SAN HP MSA 2040 : 2x430



4.3 Backup

Les sauvegardes seront faites pendant la nuit entre 22h et 6h

4.3.1 SERVEUR SQL

Pour le serveur SQL, nous effectuerons des DUMPS de la base de données deux fois par jours.

Chaque DUMP sera conservé 1 semaine depuis sa création. Les DUMPS seront stockés sur « LUN01_DATA_SQL_S ».

SQL		
Jour	Disque	Heure
Lundi	Serv	6am/10pm
Mardi	Serv	6am/10pm
Mercredi	Serv	6am/10pm
Jeudi	Serv	6am/10pm
Vendredi	Serv	6am/10pm
Samedi	Serv	6am/10pm
Dimanche	Serv	6am/10pm

4.3.2 SERVEUR DE MESSAGERIE

Pour le serveur de messagerie, nous effectuerons un backup incrémental chaque soir (temps mort) sur 1 disque et chaque dimanche soir un backup complet qui sera conservé 1 mois. Les backups complets seront stockés sur « LUN02_DATA_MAIL_M ».

MAIL		
Jour	Incrémentielle	Heure
Lundi	D1	10pm
Mardi	D1'	10pm
Mercredi	D1''	10pm
Jeudi	D1'''	10pm
Vendredi	D1''''	10pm
Samedi	D1'''''	10pm
Dimanche	Complet	10pm

4.3.3 SERVEUR DE FICHIERS

Pour le serveur de fichiers, nous effectuerons 2 fois par jour des snapshots des dossiers qui contiennent l'ensemble des fichiers. Ces snapshots seront stockés dans l'espace de stockage « LUN05_DATA_fichier_F » du SAN et conservés pendant 1 mois.

Nous ferons aussi une sauvegarde différentielle chaque jour à partir d'une complète effectuée le dimanche. Nous utiliserons 1 bande par semaine et à chaque fin de mois les 4 complètes seront misent ensemble sur 1 bande et stockés dans un lieu sécurisé à l'extérieur de l'entreprise. Nous utiliserons donc 15 bandes.

	Dimanch e	Lund i	Mard i	Mercr di	Jeudi	Vendredi	Samedi	Nouvelle cassette
Différentiell e	Complèt e	L	L+M	L+M+M	L+M+M+ J	L+M+M+J+ V	L+M+M+J+V +S	Dimanche + Lundi

4.3.4 SERVEUR WEB

Pour le serveur web, nous effectuerons chaque 2 jours un snapshot de la VM sur l'espace de stockage « LUN04_DATA_WEB_W » et ces snapshots seront conservés pendant 1 semaine.

WEB		
Jour	Disque	Heure
Lundi	Serv	10pm
Mardi		
Mercredi	Serv	10pm
Jeudi		
Vendredi	Serv	10pm
Samedi		
Dimanche	Serv	10pm

4.3.5 SERVEUR AD

Pour le serveur d'Active Directory, nous effectuerons chaque 1 fois par semaine un snapshot de la VM sur l'espace de stockage « LUN03_DATA_WEB_D » et chaque snapshot sera conservé durant 1 mois.

MAIL		
Jour	Disque	Heure
Lundi		
Mardi		
Mercredi		
Jeudi		
Vendredi		
Samedi		
Dimanche	Serv	3am

4.3.6 CLOUD

Une fois par semaine, les espaces de stockage M :, D; et W :, seront stockés sur un serveur cloud de chez Infomaniak.

Une fois par jour pour les espaces de stockage S : et F :.

4.4 Reprise d'activité

Une procédure claire devra être créée et donnée au Directeur de l'entreprise, afin de donner la possibilité à n'importe quelle entreprise informatique avec les capacités requises, d'exécuter le plan de reprise d'activité.

4.4.1 RTO

En cas de sinistre grave et qu'implique une perte totale de données sauvegardées sur le local informatique, les points suivants devront être respectés :

- Le problème doit être détecté rapidement à l'aide d'un outil de supervision en ligne, qui enverra, immédiatement, des alertes lors d'un dérangement technique.
- Temps maximum de détection : 1 h
- Temps d'analyse et lancement du plan de reprise d'activité : 2h
- Mise en œuvre et restauration des données : 3h
- RTO = 6h Max

4.4.2 RPO

- Maximum une semaine de perte de données pour les serveurs Web, Mail et AD.
- Une journée pour les serveurs SQL et de fichiers.

5 Sources

N° de page	Lien de la source
5	https://www.casinosbarriere.com/fr/montreux.html
7	https://www.loro.ch
10	https://www.vtx.ch
12	http://www.unil.ch
14	https://fr.wikipedia.org/wiki/Grappe_de_serveurs https://fr.wikipedia.org/wiki/N%C5%93ud_(r%C3%A9seau)
17	https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html https://m.youtube.com/watch?v=OUMGp3HHeI4 http://urlz.fr/7Kpu
19	https://fr.wikipedia.org/wiki/RAID_(informatique) Documents fournis par l'enseignant http://www.hardware-attitude.com/fiche-885-carte-raid-sata-adaptec-2820sa---8-ports-sata-ii-pci-x.html https://stuff.mit.edu/afs/athena/project/rhel-doc/3/rhel-sag-fr-3/s1-raid-approaches.html Image Comparaison raids : file LSI_TechnologyBrief_RAID_fr.pdf
22 ->	https://fr.wikipedia.org/wiki/Stockage_d%27information
25	https://www.commentcamarche.com/contents/739-cle-usb https://fr.wikipedia.org/wiki/Cl%C3%A9_USB https://fr.wikipedia.org/wiki/Disque_dur https://community.netapp.com/t5/Tech-OnTap-Articles/Back-to-Basics-RAID-DP/ta-p/86123?REF_SOURCE=EMMt0t-1110&h http://www.materiel-informatique.be/disque-dur.php https://fr.wikipedia.org/wiki/Linear_Tape-Open
25	Les images sont tirées du polycopié de l'enseignant M. Rogeiro intitulés « Les sauvegardes ».
26	https://www.commentcamarche.com/contents/994-onduleur https://sitelec.org/cours/abati/flash/onduleur.htm https://www.ldlc.com/guides/AL00000601/guide+les+onduleurs/ http://www.europ-computer.com/dossiers/dossier_6_18.html
28-30	https://openclassrooms.com/fr/courses/1831821-la-connectique-informatique https://fr.wikipedia.org/wiki/PCI_Express https://fr.wikipedia.org/wiki/Serial_ATA https://www.samsung.com/za/memory-storage/860-evo-sata-3-msata-ssd/MZ-M6E1T0BW/
31	https://fr.wikipedia.org/wiki/Plan_de_reprise_d%27activit%C3%A9 https://www.cases.lu/drp.html
32	https://fr.wikipedia.org/wiki/Small_Computer_System_Interface https://blog.netapp.com/wp-content/uploads/2016/05/iscsi_blog_images-1.jpg https://www.snia.org/sites/default/orig/sdc_archives/2010_presentations/monday/MahmoudJibbe_ISCSI_FCoE_testing-verA.pdf https://www.01net.com/actualites/le-protocole-iscsi-152216.html