

Sécurité - La sauvegarde



Difficulté : Novice

Notions : Sauvegardes, stratégies de sauvegarde, gestion du risque.

I. Introduction

1.1 Principe de la sauvegarde

Le but d'une sauvegarde est de garder une copie de la donnée à un instant T.

Combiné à une stratégie de sauvegarde, cela permet de garder un historique de la donnée ou d'un système à des fins de restauration ultérieure en cas de perte ou d'altération.

Cela peut se produire dans plusieurs situations :

- Perte de donnée (suite à une fausse manipulation, défaillance ou cyberattaque)
- Corruption de donnée
- Désastre (de cause naturelle ou anthropique)

1.2 Types de sauvegarde

Là où la sauvegarde diffère de la simple copie, c'est dans sa régularité et dans le fait d'en garder des copies à des dates antérieures.

En effet, bien qu'une copie seule permettrait de se prémunir contre une défaillance matérielle, si l'on en a un seul exemplaire et que la donnée d'origine est corrompue ou altérée, cette corruption ou altération sera également copiée.

Plusieurs types de sauvegardes existent.

1.2.1 Full backup

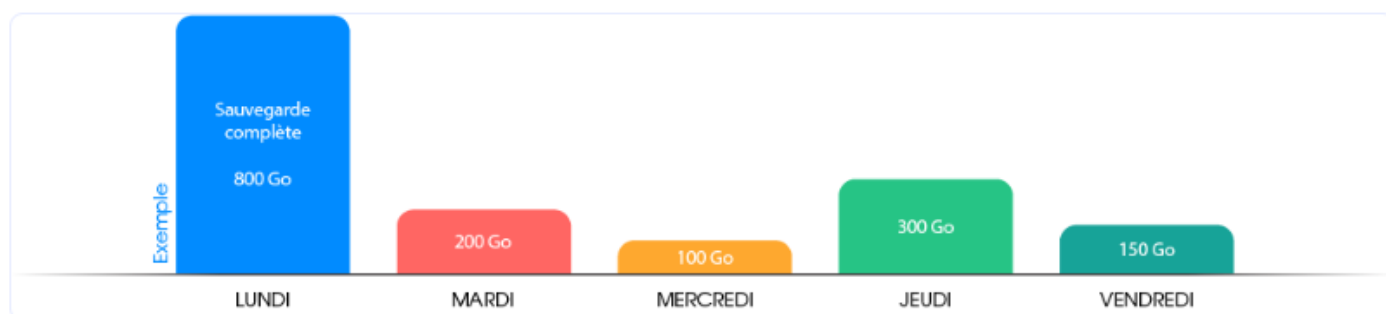
Sauvegarde complète du système, de la machine virtuelle ou du jeu de donnée.

AVANTAGES	INCONVENIENTS
• Copie complète. • Ne nécessite pas de rassembler plusieurs jeu de sauvegardes. • Restauration simple en l'état.	• Peut être très (trop) longue. • Nécessite beaucoup d'espace.

1.2.2 Incrémental

Une première sauvegarde complète est faite en début de cycle.

Puis chaque jour, une sauvegarde uniquement des données modifiées ou ajoutées depuis la dernière sauvegarde qui peut être une sauvegarde complète ou une sauvegarde incrémentielle..



AVANTAGES	INCONVENIENTS
-----------	---------------

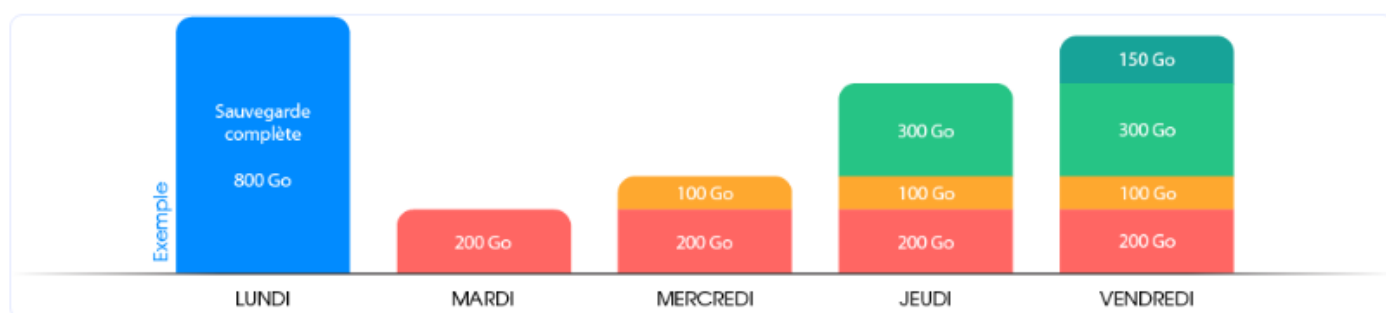
- Sauvegarde rapide
- Nécessite beaucoup moins d'espace

- Nécessite d'avoir l'ensemble du jeu de sauvegarde

1.2.3 Différentiel

Une première sauvegarde complète est faite en début de cycle.

Puis, chaque jour, une sauvegarde des données modifiées ou nouvellement ajoutées sur la base de la dernière sauvegarde complète.



Pour cette méthode, les avantages et inconvénients sont un compromis sur les deux méthodes précédentes.

- La sauvegarde est plus rapide qu'une complète, mais moins qu'une incrémentale.
- Nécessite moins d'espace qu'une complète journalière, mais plus qu'une incrémentale.
- Ne nécessite que la complète et la dernière différentielle pour la restauration au lieu du jeu complet.

En résumé, c'est un bon compromis entre les deux méthodes.

Mais l'important est avant tout d'avoir la méthode la plus adaptée aux contraintes de productions et aux budgets.

1.3 Supports de sauvegardes

Les supports de sauvegardes sont multiples et se divisent en 3 catégories majeures :

1. Le stockage local (HDD, SSD, NAS, SAN, ...).
2. Le stockage **Offsite** ou externalisé (Bande, disque externe).
3. Le stockage Cloud.

Comme il sera vu plus tard, il est nécessaire de mixer au moins deux types de sauvegardes afin de pérenniser la solution et anticiper le plus de risques possible.

II. Définir un plan de sauvegarde

2.1 Composantes de la stratégie

Pour créer une stratégie de sauvegarde pertinente, il est avant tout nécessaire de se poser certaines question :

- **Scope** : Quelles données je sauvegarde ? Machine virtuelle, répertoires, fichiers, ...
- **Fréquence** : A quelle fréquence je sauvegarde ? Les données changent elles souvent ?
- **Responsabilité** : Qui en prends la responsabilité ? Qui en suit l'exécution ?
- **Stockage** : Où sont-elles stockées, sur quel support ?
- **Sécurité** : Comment sont-elles protégées ?

Conseil : Répondre à ces questions est essentiel et il faudra le faire dans cet ordre car les réponses aux premières conditionneront les réponses aux suivantes.

Exemple

Scope : je dois sauvegarder un serveur de fichiers contenant des données de production tels que des bons de commande et de la facturation d'une volumétrie d'environ 400Go (+ ou - 500Mo par jours)

Fréquence : les données sont vitales dans l'activité de l'entreprise et changent tous les jours. Il faudra donc à minima une sauvegarde journalière. Au vu du volume et des temps de sauvegarde, on pourra opter pour une complète hebdomadaire dans la nuit de samedi à dimanche et des incrémentales ou des différentielles quotidiennes

Responsabilité : le service informatique en assurera le fonctionnement et la restauration éventuelle. Le suivi se fera par le service informatique également et des mails d'alerte et de rapports seront envoyés au service informatique et au responsable de production pour suivi.

Stockage : le volume étant important, un disque est à exclure, il faudra donc opter pour un NAS en local avec suffisamment d'espace. D'autant que pour des raisons juridiques, il faudra garder un historique long. Le plan de sauvegarde pourrait ainsi s'accompagner d'un plan d'archivage sur un cold Storage (stockage à froid) pour les sauvegardes les plus anciennes.

On peut par exemple envisager une sauvegarde NAS pour un cycle d'une semaine, puis basculer les sauvegardes les plus anciennes sur des bandes externalisées pour plus de sécurité.

Sécurité : Le NAS qui contiendra les sauvegardes des cycles les plus récents devra être isolé du réseau autant que faire se peut pour limiter les risques de cyber attaque.

Les volumes seront montés si pas de traces d'activité suspectes en début de travail (job) et seront démontés à la fin après validation.

Les bandes devront être stockées dans un local adapté en dehors du site de production principal pour palier au risque d'incendie.

L'ensemble des locaux contenant les données seront munies de portes coupe-feu, situé à un étage pour éviter les dommages en cas d'inondation et équipés de serrures à codes et d'alarmes pour limiter les risques d'intrusion.

2.2 Bonnes pratiques

- **Utiliser la règle des 3-2-1** : 3 copies sur au moins 2 médias différents et une copie hors site.
 - Automatiser les jobs de backup pour réduire le risque d'erreur humaine.
 - Chiffrer les supports de sauvegardes, plus particulièrement ceux en transit et en stockage hors site.
 - Effectuer des tests de restauration réguliers pour s'assurer du bon fonctionnement des sauvegardes.
 - Documenter **Clairement** et **précisément** les processus de sauvegardes et de restauration.
-

II. Rétention et conformité

2.1 Stratégies de rétention

En plus des stratégies de rétention interne, des politiques règlementaires et normatives peuvent s'appliquer.

Voire dans certains cas, des contraintes d'ordre juridique (données liées au douanes, rétention à vie des bulletin de paye).

Il faudra donc adapter les politiques de sauvegarde et moyens de rétention de la donnée afin d'adresser ces problématique.

On distinguera ainsi deux types de stratégies de rétention :

- Court terme (jours, semaines, mois)
- Long terme (années, décennies, à vie)

On distinguera également deux types de stockage :

- **Hot storage** (stockage à chaud).
 - disponible rapidement
 - pouvant être sollicité facilement et souvent si nécessaire
 - à un coût modéré à élevé selon la quantité et les performances
- **Cold storage** (stockage à froid).
 - souvent sur des supports de grande capacité
 - non immédiatement accessible voire hors ligne
 - assez peu coûteux en prix au GigaOctet.



Stockage sur bande LTO

LTO formats	Raw Capacity (TB)	Compressed Capacity (TB) 2.5:1
LTO-4	0.8	1.6
LTO-5	1.6	3.2
LTO-6	2.5	6.25
LTO-7	6.0	15
LTO-8	12.0	30
LTO-9	24.0	60
LTO-10	48.0	120
LTO-11	96TB	240TB
LTO-12	192TB	480TB
LTO-13	384TB	960TB
LTO-14	768TB	1,920TB

Evolution de la capacité de stockage des bandes LTO

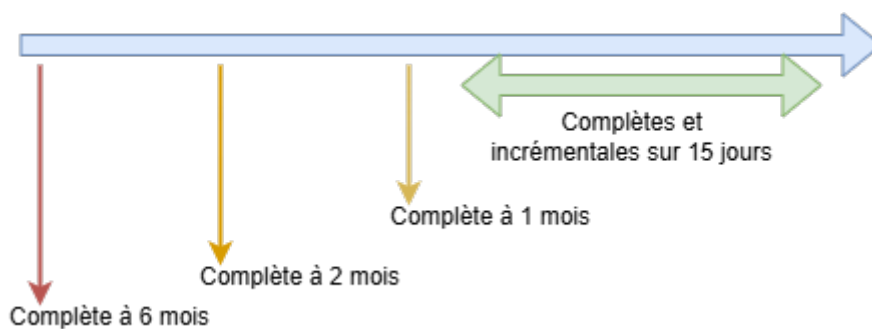
Basés sur ces deux éléments, le principe d'une bonne politique de rétention est d'obtenir le meilleurs compromis possible entre la durée de rétention, et l'optimisation des coûts de celle-ci.

2.2 Sauvegarde vs archivage

La rétention de sauvegarde peut être mise en place en vue de pouvoir restaurer à des dates antérieures en cas de compromission silencieuse.

Info : Il est arrivé par exemple qu'un serveur soit 'cryptolocké' par un virus, mais que celui-ci ai en fait compromis le serveur 1 mois avant et soit resté en dormance.

Un exemple de stratégie de rétention :



L'archivage quand à lui est prévu à plus ou moins long terme et consistera à garder la donnée en vue d'une utilité ou consultation ultérieure, sans forcément attendre un sinistre. C'est le cas des documents où la loi exige de garder un historique, pour le fournir à l'administration sur demande.

2.2 Politique de suppression et d'audit

Dans les deux cas, il faudra prévoir une politique de suppression, sans quoi le besoin en stockage ne fera que croître indéfiniment.

Dans le cas des sauvegardes, cela pourra être géré automatiquement par la solution de sauvegarde qui supprimera automatiquement les points de restauration les plus anciens.

Info : Il faudra également prendre en compte le point à partir duquel on considèrera qu'une sauvegarde est trop vieille et qu'une récupération de celle-ci sera de toute façon inutile tant ses données seront obsolètes.

Dans le cas de l'archivage, cela se fera en fonction des contraintes légales. Il s'agira alors de purger les **n** plus vieux fichiers ou les fichiers plus vieux que **n** jours, mois, années.

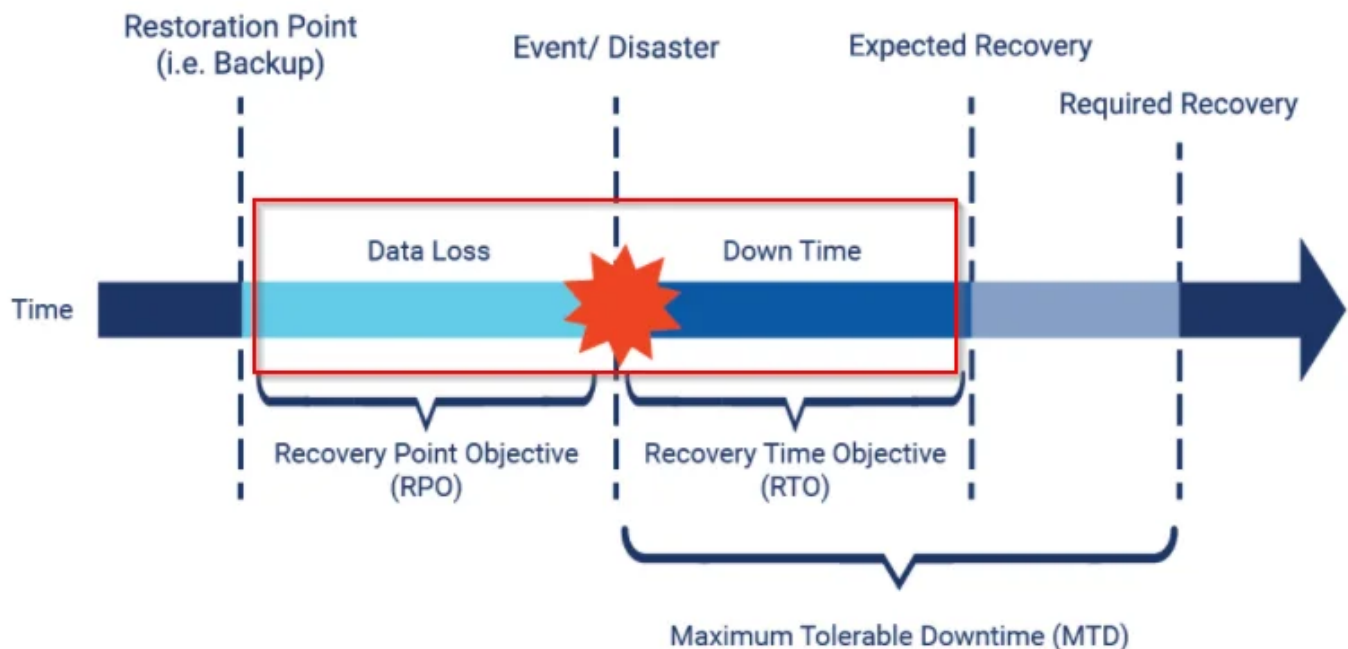
Info : Tout comme il sera parfois nécessaire juridiquement de garder des fichiers sur une certaine période de temps, il pourra être obligatoire de les supprimer après une certaine période. Par exemple les données à caractère personnel dans le cadre de la **RGPD**.

Enfin, il faudra s'assurer régulièrement que ces données sauvegardées ou archivées soient lisibles et exploitables en mettant en place des politiques d'audit et de tests. Au travers par exemple de tests réguliers de restauration ou de lecture, ou bien des tests de vérification d'intégrité.

III. Restauration des données

3.1 RPO, RTO et MTD

L'objectif de restauration pourra être découpé comme suit :



Le **RPO** (Objectif de récupération) est la durée maximale de perte de donnée acceptable. Elle correspond à la période entre la dernière sauvegarde et l'incident. En effet, toute donnée sur cette période est définitivement perdue.

Le **RTO** (Objectif de temps de récupération) est la durée visée pour la récupération de la donnée et le retour à un fonctionnement nominal.

Le **MTD** (Temps de rupture de service maximum toléré) est le temps total de coupure de service tolérable entre l'incident et le retour à la normale avant que les conséquences de cette absence de service deviennent critique (perte de production, pénalité financières, ...)

Il faudra ajouter aux estimations, la perte sèche de données ainsi que le temps passé à les reconstruire (si c'est possible).

Ces indicateurs, sont importants, car ils permettront de définir les stratégies de sauvegarde, cibler et prioriser les systèmes critiques et évaluer les risques financiers et opérationnels liés à l'interruption de service.

3.2 Scénarii de restauration

Dans le cadre d'une restauration, il faudra définir ce que l'on restaure :

- **File-level recovery** : Uniquement la donnée ou les fichiers perdus ou altérés.
- **System-level recovery** : Le système en entier.
- **Bare-metal restore** : Restauration de l'ensemble de la VM y compris de son enveloppe.

Le scénario de récupération dépendra principalement de plusieurs facteurs :

- le type de sinistre (système endommagé ou juste donnée perdue/altérée)
- la nature et la quantité de donnée perdue ou altérée à restaurer
- l'origine du sinistre (attaque, perte de l'installation, fichiers supprimés)

Il faudra donc faire une estimation du temps de récupération de chaque scénario afin de calculer le RTO, voir si cela rentre dans le MTD.

Ce qui amènera donc à faire des simulations et estimations afin de prévoir à l'avance le scénario le plus adapté à l'incident.

3.3 Tests et validation

Au vu de l'ensemble des éléments présentés, il est donc crucial de procéder régulièrement à des tests et auditer scrupuleusement la consistance des sauvegardes et archives.

Cela permettra de répondre à l'ensemble des questions essentielles :

- La restauration est-elle possible ?
- Quelle sera la perte pour l'entreprise ?
- Combien de temps cela prendra ?

Il faudra donc organiser ces audits avec la participation des décideurs. Ils seront à même de fournir les contraintes métiers, définir l'acceptabilité de la perte, les conséquences d'une interruption de service et sa limite.

Faire l'exercice de restauration ou consultation des archives régulièrement permet de :

- tester, valider, documenter l'ensemble des éléments vu ci-dessus.
- faire évoluer la documentation et estimations existantes.
- s'assurer que le personnel est en mesure de mener efficacement les procédures.

Revision #2

Created 2026-07-17 20:41:30 UTC by Olivier

Updated 2026-07-17 20:43:03 UTC by Olivier