Politique de sauvegarde et de récupération

Modèle

Contenu

[Autorité et révision 3](#_Toc157756670)

[Contrôle et révision des documents 3](#_Toc157756671)

[Gestion des versions 3](#_Toc157756672)

[Intro 4](#_Toc157756673)

[Responsabilités 4](#_Toc157756674)

[Procédure de sauvegarde et de récupération 4](#_Toc157756675)

[RPO et RTO 5](#_Toc157756676)

[Accès à la sauvegarde et au cryptage 5](#_Toc157756677)

[Sauvegarde hors site 5](#_Toc157756678)

[Surveillance de secours 5](#_Toc157756679)

[Test de récupération 6](#_Toc157756680)

[ANNEXES 7](#_Toc157756681)

[Intro 7](#_Toc157756682)

[ANNEXE 1 : Calendrier de sauvegarde du GFS 8](#_Toc157756683)

[Qu'est-ce que la sauvegarde Grand-père-Père-Fils ? 8](#_Toc157756684)

[Le principe de la rotation des sauvegardes GFS 8](#_Toc157756685)

[Exemple de schéma G-F-S 8](#_Toc157756686)

[Représentation schématique G-F-S 8](#_Toc157756687)

[Types de techniques de sauvegarde des données 9](#_Toc157756688)

[Sauvegarde complète des données 9](#_Toc157756689)

[Sauvegarde incrémentale des données 9](#_Toc157756690)

[Sauvegarde différentielle des données 9](#_Toc157756691)

[Sauvegarde de données mixtes 9](#_Toc157756692)

[ANNEXE 2 : Stratégie de sauvegarde 3-2-1 10](#_Toc157756693)

[Règle de sauvegarde 3-2-1 10](#_Toc157756694)

[L'importance de la règle 3-2-1 10](#_Toc157756695)

[3-2-1 gestion des sauvegardes 11](#_Toc157756696)

[3-2-1 RÉSUMÉ 12](#_Toc157756697)

# Autorité et révision

## Contrôle et révision des documents

|  |  |
| --- | --- |
| **Vérification des documents** |  |
| Auteur |  |
| Propriétaire |  |
| Date de création |  |
| Dernière révision par |  |
| Date de la dernière révision |  |

.

## Gestion des versions

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date d'approbation** | **Approuvé par** | **Description du changement** |
| 1.0 |  |  |  |

# Intro

Les informations et les systèmes d'information critiques doivent être protégés contre la perte et l'endommagement des données. Les procédures de sauvegarde et de récupération nous permettent de restaurer les informations en cas de scénarios catastrophes tels que la défaillance d'un système, un incendie, une suppression accidentelle ou l'apparition de logiciels malveillants.

La sauvegarde n'est pas nécessaire lorsque la perte de données est acceptable ou lorsque d'autres mesures de contrôle sont utilisées pour surmonter les situations de catastrophe. Un exemple courant est celui d'un système PLC qui contient une configuration statique pouvant être facilement redéployée ou remplacée en cas de sinistre.

Le présent document d'orientation fait partie d'un ensemble de documents d'orientation destinés à aider **[l'organisation]** à mettre en place une stratégie solide en matière de cybersécurité.

# Responsabilités

Le propriétaire des données est responsable d'un processus de sauvegarde et de restauration efficace qui répond aux besoins de l'entreprise. Les tâches opérationnelles peuvent être déléguées à des administrateurs système ou à des fournisseurs.

# Procédure de sauvegarde et de récupération

Une procédure de sauvegarde et de récupération doit être mise en place pour tous les systèmes critiques. La procédure de sauvegarde doit définir les points suivants :

* Quelles informations sauvegardez-vous (systèmes ET données) ?

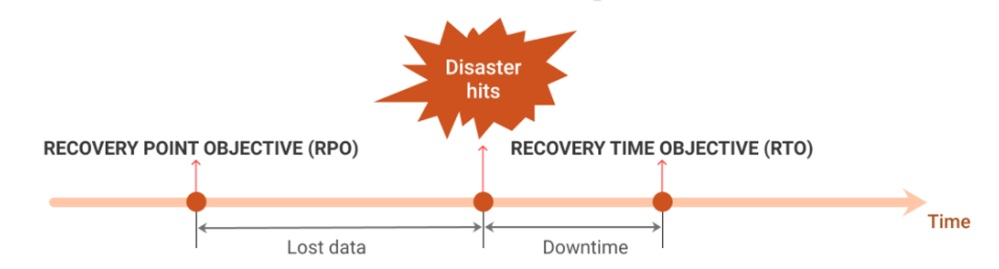
-Faire une sauvegarde

-Surveillance des sauvegardes

* Quand et à quelle fréquence faut-il faire des sauvegardes ?
* Combien de temps faut-il conserver la sauvegarde ?
* Comment et où stocker la sauvegarde ?
* Comment les données de sauvegarde sont-elles transférées ?

## RPO et RTO

La procédure de sauvegarde doit répondre aux besoins de l'entreprise en matière de RPO (recovery point objective) et de RTO (recovery time objective), par exemple sur la base de l'évaluation des risques et de la classification des informations.



Le RPO définit la période maximale pendant laquelle des données peuvent être perdues à la suite d'un incident majeur. Par exemple, si une copie statique est effectuée chaque nuit à 2 heures du matin, la perte maximale de données est de 24 heures.

Le RTO (Recovery Time Objective) est le temps nécessaire pour récupérer les données.

Pour ce faire, utilisez le schéma GFS, par exemple. (**Voir ANNEXE 1 : Programme de sauvegarde GFS).**

## Accès à la sauvegarde et au cryptage

L'accès aux sauvegardes doit bénéficier d'un niveau de protection au moins égal à celui des données originales. Lorsque des données de sauvegarde confidentielles sont stockées ou transportées physiquement ou logiquement de manière à être accessibles à des personnes non autorisées, elles doivent être cryptées.

En voici quelques exemples :

* Trafic réseau pour la sauvegarde.
* Les supports de sauvegarde stockés ou transférés par des personnes qui ne devraient pas avoir accès aux données originales.
* Fichiers de sauvegarde sur des supports stockés dans un endroit qui peut être accessible à des personnes qui ne devraient pas avoir accès aux données originales.
* La clé de chiffrement de sauvegarde nécessaire pour décrypter le support hors site ne doit pas seulement être stockée sur place.

## Sauvegarde hors site

Pour éviter la perte à la fois de l'information et de la sauvegarde, les données de sauvegarde doivent, dans la mesure du possible, être stockées dans un lieu physique différent de celui où se trouvent les données elles-mêmes. Une vue d'ensemble des supports hors site doit être disponible. Pour ce faire, utilisez la stratégie de sauvegarde 3-2-1, par exemple. (**Voir ANNEXE 2 : Stratégie de sauvegarde 3-2-1**)

## Surveillance de secours

Le processus de sauvegarde doit être surveillé afin de garantir son bon fonctionnement et de corriger les erreurs. Le bon fonctionnement doit pouvoir être démontré par des journaux, des rapports ou un système automatisé.

## Test de récupération

Pour toutes les méthodes de sauvegarde utilisées pour les systèmes critiques, des tests de restauration doivent être effectués au moins une fois par an. Une restauration opérationnelle (non planifiée) en dehors d'une restauration de test périodique programmée peut être considérée comme un test de récupération.

# ANNEXES

## Intro

Les deux diagrammes présentés dans les annexes suivantes peuvent être déployés séparément.

Le plan de sauvegarde **Grand-père-Père-Fils** (GFS) est utilisé dans les environnements contenant des quantités relativement importantes de données ou de systèmes, lorsque l'on ne dispose pas de suffisamment de temps pour effectuer des sauvegardes entre deux heures et/ou lorsqu'il est important de pouvoir remonter dans le temps de manière détaillée. ce plan ne tient pas compte du support de sauvegarde ou de l'emplacement des sauvegardes.

Le schéma **3-2-1** est souvent utilisé comme base. Cela signifie que vous disposez d'au moins trois copies complètes sur deux supports différents. Il est important que l'un des supports se trouve à un autre endroit. Cependant, la règle du 3-2-1 ne parle pas du RPO-RPO de la sauvegarde.

Comme nous l'avons expliqué précédemment, les deux systèmes peuvent être utilisés séparément. Toutefois, la combinaison des deux apporte une valeur ajoutée. Le schéma GFS se concentre sur le RPO-RTO des données, tandis que la stratégie 3-2-1 se concentre sur le stockage des sauvegardes effectuées.

L'exemple suivant clarifie l'utilisation des deux principes :

Toutes les données se trouvent sur un NAS (Network Attached Storage) dont les disques sont en RAID 10\*. Via un serveur de sauvegarde, ce NAS est sauvegardé chaque nuit sur un autre NAS. Ce NAS est relié au serveur de sauvegarde par un réseau séparé. Une sauvegarde complète des données prend actuellement plus de 12 heures. Pour continuer à sauvegarder les données changeantes, le calendrier GFS est choisi. Les sauvegardes hebdomadaires et mensuelles sont en outre copiées dans un environnement cloud sécurisé. Nous avons ainsi combiné la stratégie 3-2-1 avec le calendrier de sauvegarde GFS. [\*https://en.wikipedia.org/wiki/Nested\_RAID\_levels](*https:/en.wikipedia.org/wiki/Nested_RAID_levels)

La figure suivante donne une représentation schématique de ce qui précède.



## ANNEXE 1 : Calendrier de sauvegarde du GFS

### Qu'est-ce que la sauvegarde Grand-père-Père-Fils ?

La technique de rotation de la sauvegarde GFS est une méthode populaire de **sauvegarde des données** qui permet de combiner des copies complètes et partielles sur différents supports afin de réduire le temps de sauvegarde et d'améliorer la sécurité du stockage. De nombreux articles sont consacrés à la stratégie de sauvegarde "grand-père-père-fils".

### Le principe de la rotation des sauvegardes GFS

Dans la technique de sauvegarde grand-père-père-fils, les trois étapes prévues créent des sauvegardes :

* Le **"grand-père (G)"** - sauvegarde complète d'un site particulier, d'un site externe ou de plusieurs sites ;
* Le **"père (F)"** - une autre sauvegarde complète, plus régulière, sur un support plus rapide ;
* Le **"fils (S)"** - sauvegarde incrémentale (ou différentielle) sur le même espace de stockage que le "père".

### Exemple de schéma G-F-S

Le programme GFS commence par les **sauvegardes quotidiennes**. En général, il y a quatre supports de sauvegarde étiquetés en fonction du jour de la semaine où ils sont sauvegardés, par exemple du lundi au jeudi. Chaque bande est appelée pour être utilisée le jour indiqué. Si l'historique des versions des fichiers n'est conservé que pendant une semaine, chaque bande est écrasée chaque semaine. Pour conserver un historique des versions des fichiers sur trois semaines (recommandé), il faut davantage de bandes. Par exemple, la bande du lundi de cette semaine ne sera pas écrasée avant 3 semaines.

**Les sauvegardes hebdomadaires** suivent un scénario similaire. Un ensemble de cinq supports de sauvegarde hebdomadaires est étiqueté "Semaine 1", "Semaine 2", etc. Les sauvegardes complètes sont enregistrées chaque semaine le jour où un support "Son" n'est pas utilisé. Dans l'exemple ci-dessus, il s'agirait des bandes "Vendredi". Ce support "Père" est réutilisé tous les mois. Cinq bandes hebdomadaires sont nécessaires pour conserver un historique de fichiers d'un mois, car certains mois comptent 5 semaines

Le dernier ensemble de trois supports sera étiqueté "**Month1**", "Month2" et ainsi de suite, en fonction du mois du trimestre où ils seront utilisés. Ce support "Grandfather" enregistre les sauvegardes complètes le dernier jour ouvrable de chaque mois. Si votre plan de sauvegarde suit un calendrier fiscal, votre bande mensuelle remplacera la bande hebdomadaire/grand-père de la semaine 4 ou de la semaine 5, selon le mois. Si votre plan de sauvegarde suit les mois calendaires, votre sauvegarde mensuelle variera tout au long de l'année, remplaçant une bande quotidienne ou hebdomadaire. En général, les bandes mensuelles sont écrasées tous les trimestres ou tous les ans (recommandé), en fonction des exigences de l'historique des versions.

### Représentation schématique G-F-S

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lundi** | **Mardi** | **Mercredi** | **Jeudi** | **Semaine 1** |
| **Lundi** | **Mardi** | **Mercredi** | **Jeudi** | **Semaine 2** |
| **Lundi** | **Mardi** | **Mercredi** | **Jeudi** | **Semaine 3** |
| **Lundi** | **Mardi** | **Mercredi** | **Jeudi** | **Mois1** |

### Types de techniques de sauvegarde des données

Tous les logiciels de sauvegarde de fichiers proposent au moins une méthode de sauvegarde des données, la sauvegarde complète, qui permet de copier l'ensemble des données sur un bit final. Toutefois, il existe d'autres types de sauvegarde de données, souvent pour gagner du temps et de l'espace lors des sauvegardes régulières. Ces types de sauvegarde sont les suivants :

* **Sauvegarde complète** - copie complète des données comme décrit précédemment ;
* **Sauvegarde partielle** - copie uniquement les données modifiées après la dernière sauvegarde :
  + **Sauvegarde incrémentale** - copie uniquement les données modifiées après la dernière sauvegarde incrémentale
  + **Sauvegarde différentielle** - copie uniquement les données modifiées après la dernière sauvegarde complète
* **Sauvegarde mixte** - une séquence de sauvegardes complètes et de quelques sauvegardes partielles, avec des rotations répétées :
  + Sauvegarde incrémentielle mixte - une chaîne de sauvegardes incrémentielles complètes et simples ;
  + Sauvegarde différentielle mixte - un ensemble de sauvegardes différentielles complètes et simples.

La sauvegarde complète est la base de toute sauvegarde différentielle ou incrémentale, ainsi que des sauvegardes mixtes.

### Sauvegarde complète des données

Une sauvegarde complète suppose que chaque fois que vous exécutez la tâche, l'ensemble des données est copié à l'emplacement choisi. Une sauvegarde complète prend beaucoup d'espace, de temps et de ressources PC et effectue souvent de nombreuses copies de données inutiles, car la plupart des données de l'ensemble ne subissent aucune modification entre les sauvegardes.

### Sauvegarde incrémentale des données

La sauvegarde incrémentielle ne traite que les fichiers apparus ou modifiés depuis la précédente sauvegarde incrémentielle. Après une sauvegarde initiale complète, chaque sauvegarde ultérieure sera incrémentale, ne stockant que la différence entre l'ensemble de données actuel et une copie incrémentale précédente.

### Sauvegarde différentielle des données

La sauvegarde différentielle est très similaire à la sauvegarde incrémentielle, mais elle utilise différents types de stratégies de sauvegarde des données. Après une sauvegarde initiale complète, chaque sauvegarde ultérieure sera incrémentale, ne stockant qu'une différence entre l'ensemble de données actuel et une copie incrémentale précédente.

### Sauvegarde de données mixtes

Cette approche est une combinaison de deux types différents de sauvegardes : les sauvegardes complètes et les sauvegardes partielles (incrémentielles ou différentielles). Elle s'apparente également à une technique de sauvegarde versionnée. Dans cette méthode, une sauvegarde complète est effectuée, suivie d'un nombre fixe de sauvegardes partielles.

## ANNEXE 2 : Stratégie de sauvegarde 3-2-1

La **sauvegarde 3-2-1** est une méthode éprouvée de protection et de récupération des données qui permet de s'assurer que les données sont protégées de manière adéquate et que des copies de sauvegarde à jour des données sont disponibles en cas de besoin. Le concept de base de la stratégie de sauvegarde 3-2-1 consiste à effectuer trois sauvegardes des données à protéger, à stocker les sauvegardes sur deux types de supports de stockage différents et à envoyer une sauvegarde des données à un autre endroit.

Dans le scénario classique de la sauvegarde 3-2-1, un logiciel de sauvegarde est utilisé pour sauvegarder des données critiques, la sauvegarde des données étant stockée sur un autre dispositif de stockage de données sur site. Au cours de ce processus, ou immédiatement après, deux autres sauvegardes des données sont stockées sur deux autres périphériques ; traditionnellement, au moins l'un de ces périphériques était une bibliothèque de bandes. La bande était un élément standard du processus car il était facile de créer une sauvegarde portable des données sous la forme d'une cartouche de bande qui pouvait être facilement expédiée hors du site. Dans de nombreux environnements, cependant, la bande a été remplacée par un système de stockage sur disque dur.

Bien que l'approche de sauvegarde 3-2-1 soit la pierre angulaire de la protection des données dans les grands et petits centres de données depuis des décennies, c'est un concept encore adopté par la plupart des fournisseurs de logiciels et de matériel de sauvegarde comme "meilleure pratique" pour l'utilisation efficace de leurs produits. Les fournisseurs reconnaissent que le concept général est toujours valable, quel que soit le mode ou le lieu de stockage des données d'une entreprise, même si les nouvelles exigences et le big data ont rendu l'équation 3-2-1 un peu plus compliquée.

### Règle de sauvegarde 3-2-1

La stratégie de sauvegarde 3-2-1 se compose de trois règles :

* **Trois copies des données**. Trois copies de sauvegarde de toutes les données critiques doivent être effectuées régulièrement - quotidiennement ou plus souvent - comprenant les données d'origine et au moins deux copies de sauvegarde.
* **Deux types de stockage.** Deux types de stockage différents doivent être utilisés pour stocker les données. Les deux copies des données de sauvegarde doivent être stockées sur deux types de stockage différents afin de minimiser le risque de défaillance. Les types de dispositifs de stockage peuvent inclure un disque dur interne, un disque dur externe, un lecteur de stockage amovible, une bibliothèque de bandes, une matrice de stockage secondaire ou un environnement de sauvegarde en nuage.
* **Un emplacement hors site**. Une copie des données de sauvegarde doit être envoyée à un centre de stockage hors site. Au moins une copie des données doit être stockée dans un lieu hors site afin de garantir que les catastrophes naturelles ou géographiques ne puissent pas affecter toutes les copies de données. Cette copie peut être livrée physiquement à l'emplacement hors site, comme dans le cas des sauvegardes sur bande, ou peut être répliquée vers l'emplacement secondaire par le biais d'installations de télécommunication.

### L'importance de la règle 3-2-1

La stratégie de sauvegarde 3-2-1 est reconnue comme une "meilleure pratique" par les professionnels de la sécurité de l'information et de la protection des données. Bien que ce processus ne garantisse pas que toutes les données ne seront jamais compromises de quelque manière que ce soit, la stratégie élimine certains des risques associés aux procédures de sauvegarde. La méthodologie 3-2-1 est importante pour garantir qu'il n'y a pas de point de défaillance unique pour les données. Une organisation est couverte non seulement si une copie est corrompue ou si une technologie tombe en panne, mais aussi en cas de catastrophe naturelle ou de vol qui détruit les types de stockage physique.

Le processus de récupération des données à l'aide de la méthode 3-2-1 se déroule comme suit :

* Les données originales (actives) ont été corrompues, endommagées ou perdues. Si la copie de production des données n'est pas disponible, la première solution consiste à restaurer les données requises à partir de la copie de sauvegarde stockée en interne sur un autre support ou un système de stockage secondaire.
* La deuxième copie des données est indisponible ou inutilisable. Si le système - bande ou disque - utilisé pour stocker la deuxième copie des données n'est pas disponible ou si la copie des données est endommagée, périmée ou inutilisable, la copie hors site doit être récupérée sur les serveurs internes.
* Redémarrer le processus 3-2-1 dès que possible. Une fois qu'une copie appropriée des données a été attachée et que le fonctionnement a été rétabli, le processus de sauvegarde doit redémarrer dès que possible afin de garantir que les données restent protégées de manière adéquate.

De nos jours, les sauvegardes ne sont plus seulement des polices d'assurance que l'on met de côté jusqu'à ce que quelque chose se passe mal. Les entreprises tirent davantage de valeur de leurs datastores de sauvegarde en utilisant ces données pour développer et tester de nouvelles applications, par exemple. Les approches contemporaines de la programmation, telles que DevOps, exigent un accès facile à des données aussi proches que possible des données d'application réelles afin de garantir que les applications sont développées de manière appropriée dans un environnement réel. Les données de sauvegarde répondent parfaitement à cette exigence, car elles sont susceptibles d'être fraîchement générées régulièrement et fréquemment.

Les applications analytiques peuvent également avoir besoin d'accéder à de grandes quantités de données actuelles. En utilisant des données de sauvegarde fraîches, les résultats du processus analytique sont susceptibles d'être plus fiables et plus précis. Des contrôles et une gestion plus stricts des sociétés de données sont nécessaires pour garantir que ces applications obtiennent les meilleures données possibles, tout en conservant les concepts fondamentaux de la sauvegarde 3-2-1. Il est à noter que si l'une des copies de sauvegarde est utilisée pour le développement ou l'analyse d'une application, elle peut être altérée ou indisponible, ce qui rendrait l'une des trois copies nécessaires inutilisable en cas de récupération.

L'intégrité des données a toujours été une préoccupation majeure dans les activités de protection des données. Il ne suffit pas de sauvegarder les données et de verrouiller les copies ; il faut s'assurer que les sauvegardes sont complètes, intactes et récupérables. Les tests de récupération y contribuent, tout comme l'utilisation de certaines des fonctions les plus avancées offertes par les applications de sauvegarde pour détecter les ransomwares et d'autres menaces. Encore une fois, ces préoccupations n'entravent pas nécessairement une approche de sauvegarde 3-2-1, mais elles peuvent ajouter certaines étapes au processus, telles que des tests de récupération régulièrement programmés.

### 3-2-1 gestion des sauvegardes

Il existe quelques principes de base pour une mise en œuvre réussie de la sauvegarde 3-2-1 :

* Toutes les copies de données sont identiques et à jour.
* Les supports sur lesquels les copies sont stockées sont des supports lisibles.
* Tous les spécimens et équipements sont testés et leur fonctionnement est confirmé.
* Les copies à distance sont stockées en toute sécurité.
* La récupération d'un ou plusieurs fichiers ou d'une sauvegarde complète est régulièrement testée.
* Les copies de données internes se trouvent sur des systèmes de stockage et des réseaux différents et ne sont pas accessibles depuis l'extérieur de l'entreprise.

Le logiciel de sauvegarde utilisé dans le processus 3-2-1 peut être très utile car il peut contrôler automatiquement la disposition des sauvegardes tout en cataloguant toutes les activités de sauvegarde. La plupart des applications de sauvegarde ont également ajouté des fonctions permettant de détecter les menaces telles que les logiciels malveillants, les logiciels rançonneurs et les virus dans les copies de sauvegarde.

### 3-2-1 RÉSUMÉ

Faire **3 copies des** données de sauvegarde.   
 (1 primaire et 2 sauvegardes

3 copies des données

**Stocker 1 de ces documents hors site** (stockage sécurisé, nuage,...)

2 supports différents

Conserver les données sur au moins **2 types de stockage**.  
 (disque local, NAS, bande,...)

1 copie hors site