

Les caractéristiques essentielles d'un bon backup

Quand tu travailles comme technicien informatique, tu es responsable d'assurer la **préservation**, l'**intégrité** et la **disponibilité** des données. Pour y arriver, il ne suffit pas « d'en faire une copie » : il faut mettre en place des sauvegardes efficaces, régulières et conformes aux bonnes pratiques du métier.

Exploration

Dans ce cours, tu vas découvrir les **caractéristiques principales d'une sauvegarde professionnelle** : ce qui définit un bon backup, les différents types de sauvegarde, leur fréquence, et les options modernes comme l'immutabilité.

Objectifs du cours

À la fin de cette leçon, tu dois être capable de :

- identifier les principales caractéristiques d'une sauvegarde fiable ;
- faire la différence entre sauvegarde complète, incrémentale et différentielle ;
- expliquer l'importance de la périodicité ;
- comprendre l'intérêt du chiffrement et de l'immutabilité (WORM) ;
- reconnaître les bonnes pratiques utilisées dans les entreprises.

Les 5 critères essentiels d'un backup

Voici les caractéristiques qu'un technicien doit évaluer lorsqu'il choisit ou configure une solution de sauvegarde.

Périodicité : la fréquence des sauvegardes

La périodicité définit à **quel intervalle** les données sont sauvegardées.

Pourquoi c'est important ?

- Plus un système change souvent, plus les sauvegardes doivent être fréquentes.
- Un intervalle trop long augmente le **RPO** (Recovery Point Objective) → la quantité de données perdues en cas de problème.

Exemples :

- PC d'un utilisateur : sauvegarde quotidienne.
- Serveur de fichiers : toutes les 4 heures.
- Base de données : toutes les heures.
- Serveur critique (finances, hôpital) : toutes les 5 minutes.

👉 Une bonne périodicité dépend de la criticité des données, pas d'un chiffre magique.

Type de sauvegarde : complète, incrémentale et différentielle

TYPES OF BACKUP: FULL, DIFFERENTIAL, AND INCREMENTAL

Full Backups: Entire data set, regardless of any previous backups or circumstances.



Differential Backups: Additions and alterations since the most recent full backup.



Incremental Backups: Additions and alterations since the most recent incremental backup.



Initial Full Backup



1st Backup

2nd Backup

3rd Backup

4th Backup

5th Backup



Data subject to backup

Sauvegarde complète

On sauvegarde **toutes** les données à chaque fois. ✓ Simple ✗ Long ✗ Utilise beaucoup d'espace ✗ Rend les restaurations plus lentes si tu en fais souvent

À utiliser : pour les petites quantités de données ou comme point de départ.

Sauvegarde incrémentale

On sauvegarde **uniquement** ce qui a changé depuis la dernière sauvegarde (qu'elle soit complète ou incrémentale).

✓ Très rapide ✓ Occupe peu d'espace ✓ Standard en entreprise ✗ Restauration parfois plus lente (il faut assembler plusieurs incréments)

Utilisation typique : sauvegardes quotidiennes ou horaires.

Sauvegarde différentielle

On sauvegarde **tout ce qui a changé depuis la dernière sauvegarde complète.**

✓ Restauration plus simple qu'avec un incrémental ✗ Plus lourde qu'un incrémental ✗ L'espace utilisé augmente avec le temps

Bonne solution intermédiaire quand on veut un compromis.

Rétention : combien de versions tu gardes

Une vraie stratégie de backup ne garde pas juste « la dernière » version.

Pourquoi ?

- Une corruption peut passer inaperçue pendant plusieurs jours.
- Un ransomware peut chiffrer tes fichiers avant que tu n'aies le temps d'agir.

Exemples de politiques de rétention :

- 30 jours glissants
- 12 versions mensuelles
- 7 versions quotidiennes + 4 versions hebdomadaires + 6 versions mensuelles

👉 Plus tu gardes d'historique, plus tu peux revenir loin en arrière.

Chiffrement (Encryption)

Le chiffrement protège les données en cas :

- de vol de disque externe ;
- d'interception d'un flux réseau (ex : backup vers un cloud) ;
- d'accès non autorisé à un NAS.

Bonne pratique :

- chiffrer les données en **transit** (TLS)
- chiffrer les données **au repos** (AES-256)
- stocker la clé **séparément** du système de sauvegarde !

💡 Sans clé → données irrécupérables. 💡 Avec clé stockée au même endroit → chiffrement inutile.

Immutabilité (WORM)

Une sauvegarde immuable est **impossible à modifier ou supprimer** pendant une période définie.

WORM = *Write Once, Read Many* → Écrire une fois, lire autant de fois que nécessaire.

Intérêt majeur :

- protège contre les ransomware ;
- empêche les erreurs humaines ;
- garantit l'intégrité dans les systèmes légaux (archivage, finance).

Exemples de sources immuables :

- snapshots verrouillés (ZFS, NetApp, Synology) ;
- stockage cloud avec immutabilité (AWS S3 Object Lock, Azure Immutable Storage) ;
- bandes LTO en mode WORM.

Vérification et tests de restauration

Une sauvegarde non testée n'existe pas. Tu dois vérifier régulièrement :

- l'intégrité (checksums, hashing) ;
- la restaurabilité (faire une restauration réelle dans un environnement de test) ;
- la cohérence (fichiers lisibles, bases de données fonctionnelles).

👉 C'est la règle du **0 erreur** dans la méthode 3-2-1-1-0.

Vitesse de sauvegarde et de restauration

Deux paramètres essentiels :

- **vitesse d'écriture** → le temps nécessaire pour faire un backup ;
- **vitesse de lecture** → le temps pour restaurer.

En entreprise, une restauration trop lente peut coûter très cher (serveur indisponible = pertes financières). C'est le RTO (Recovery Time Objective) → combien de temps peut prendre la restauration avant que ce soit critique ?

Emplacement : local, distant, cloud

La solution doit tenir compte des risques :

- local : rapide mais vulnérable au vol/incendie
- NAS : pratique mais vulnérable aux ransomware (sauf immutabilité)
- cloud : excellent off-site, mais dépend du réseau
- bandes : très bonnes pour l'archivage long terme
- hybride : le plus courant (NAS + cloud)

Synthèse (à retenir absolument)

- Une bonne sauvegarde est **régulière, multiple et testée**.
- Le type de backup (complet/incrémental/différentiel) influence la vitesse et la taille.
- La périodicité dépend de la criticité de la donnée.
- Le chiffrement protège la confidentialité.
- L'immutabilité protège contre les ransomware et les erreurs humaines.
- Sans test de restauration, aucun backup n'est fiable.