



CHECKLIST IMPRIMABLE

# Votre plan de sauvegarde 3-2-1 prêt à vérifier

Transformez la règle 3-2-1 en dispositif réellement restaurable. Utilisez cette checklist pour répartir vos copies, protéger vos accès et valider votre procédure de reprise.

## Au sommaire

- 1 Le repère 3-2-1 en une minute
- 2 1. Inventorier ce qui doit pouvoir être restauré
- 3 2. Construire des copies qui ne tombent pas ensemble
- 4 3. Choisir l'outil selon l'emplacement du dépôt
- 5 4. Sécuriser le dépôt et les accès
- 6 5. Tester une restauration, pas seulement une sauvegarde

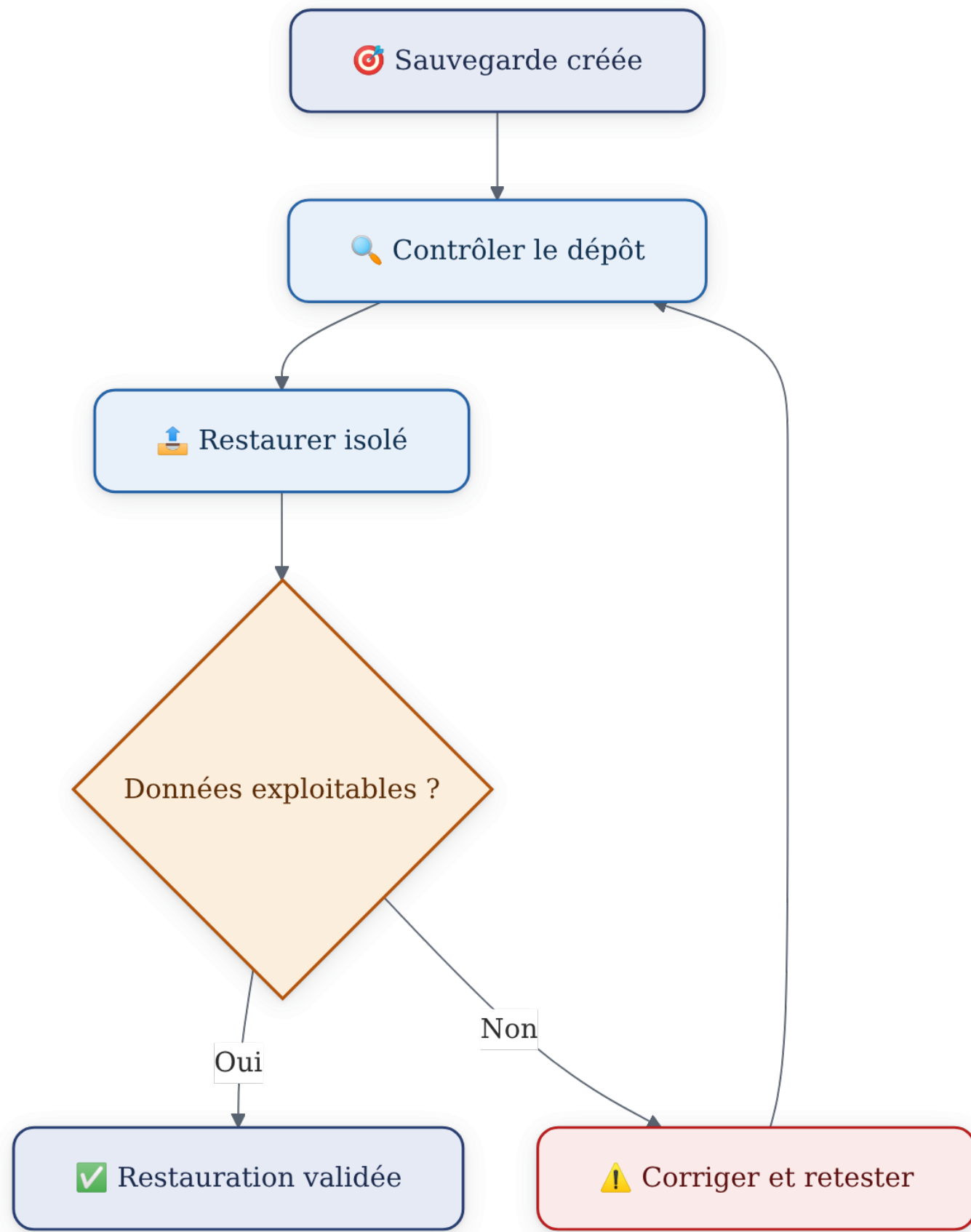
## Le repère 3-2-1 en une minute

**3 copies** : les données de production comptent comme une copie, auxquelles s'ajoutent au moins deux copies de secours.

**1 copie hors site** : placez une sauvegarde dans un autre lieu physique ou chez un prestataire distant.

**2 supports distincts** : évitez de concentrer toutes les copies sur le même disque, la même machine ou le même type de stockage.

**La version renforcée 3-2-1-1-0** ajoute une copie hors ligne ou immuable et des restaurations testées sans erreur.



**INFOGRAPHIE** Schéma de test de restauration pour une sauvegarde 3-2-1 avec Borg ou Restic

# ARCHITECTURE DE SAUVEGARDE 3-2-1

## LA RÈGLE D'OR POUR PROTÉGER VOS DONNÉES

La stratégie 3-2-1 garantit la résilience de vos données face aux pannes, aux sinistres, aux erreurs humaines et aux cyberattaques (ransomware).



### OBJECTIF

Avoir plusieurs copies de vos données, stockées de différentes manières et à différents endroits, pour pouvoir toujours récupérer vos données critiques.

### LA RÈGLE 3-2-1

3

#### 3 COPIES DE VOS DONNÉES

Conservez au moins 3 copies de vos données : l'originale et 2 sauvegardes.



1 DONNÉE ORIGINALE

Données actives

2

#### 2 SUPPORTS DIFFÉRENTS

Stockez vos copies sur 2 types de supports différents pour éviter qu'un même incident n'affecte toutes vos sauvegardes.



COPIE LOCALE

Sauvegarde locale chiffrée sur disque externe



COPIE DISTANTE

Sauvegarde distante chiffrée séparée

1

#### 1 COPIE HORS LIGNE

Conservez au moins 1 copie hors ligne (air-gapped) : déconnectée du réseau après la sauvegarde.



COPIE HORS LIGNE

Support déconnecté après exécution

### POURQUOI C'EST ESSENTIEL ?



#### RÉSILIENCE MAXIMALE

Protège contre les pannes matérielles, erreurs humaines, incendies, inondations, vols et cyberattaques.



#### RÉCUPÉRATION GARANTIE

Augmente vos chances de restaurer vos données, même en cas d'incident majeur.



#### CONTINUITÉ D'ACTIVITÉ

Réduit les temps d'arrêt et l'impact financier sur votre organisation.



#### CONFORMITÉ

Répond aux bonnes pratiques et exigences réglementaires (ISO 27001, RGPD, etc.).



#### INVESTISSEMENT INTELLIGENT

Une stratégie simple et efficace pour éviter des pertes de données coûteuses.



#### BONNES PRATIQUES

Testez régulièrement vos sauvegardes et vos restaurations.

Automatisez vos sauvegardes et surveillez leur succès.

Chiffrez vos sauvegardes (au repos et en transit).

Conservez vos sauvegardes distantes dans une localisation géographique différente.

Documentez votre plan de sauvegarde et de reprise.

3-2-1 : TROIS COPIES, DEUX SUPPORTS DIFFÉRENTS, UNE HORS LIGNE = VOS DONNÉES TOUJOURS PROTÉGÉES.

**SCHEMA** Architecture minimale : données actives, copie locale chiffrée et copie distante séparée.

## 1. Inventorier ce qui doit pouvoir être restauré

### Lister les données irremplaçables

Documents administratifs, photos, dépôts de code, données métier et bases de données.

### Ajouter les éléments nécessaires au redémarrage

Configurations de services, clés, secrets de récupération et médias d'installation.

### Distinguer les données recréables ou téléchargeables

Ne leur attribuez pas la même priorité que les données uniques.

### Définir l'ordre de restauration

Identifiez ce qui doit revenir en premier après un incident.

### Adapter la fréquence au rythme des modifications

Une base modifiée fréquemment et des archives mensuelles n'ont pas les mêmes besoins.

## 2. Construire des copies qui ne tombent pas ensemble

### Conserver les données actives sur le poste ou le serveur de production

### Créer une copie locale chiffrée sur un disque externe ou un autre support maîtrisé

Elle facilite une restauration rapide après suppression ou panne simple.

### Créer une copie distante chiffrée vers un serveur ou un stockage distant

Elle protège mieux contre un sinistre au domicile, au bureau ou dans le local serveur.

- ☐ **Vérifier que la copie hors site est réellement dans un autre lieu physique**  
Un NAS dans le même bâtiment ou un disque rangé à côté de l'ordinateur ne suffit pas.
- ☐ **Prévoir une copie déconnectée après sauvegarde lorsque c'est possible**  
Un dépôt accessible en permanence peut être atteint par un logiciel malveillant.

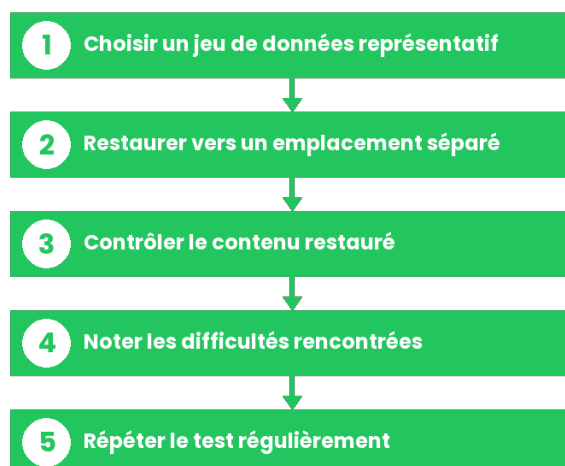
### 3. Choisir l'outil selon l'emplacement du dépôt

| Solution   | À privilégier pour                                           | Point de contrôle                                                                                  |
|------------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| BorgBackup | Disque local, volume monté, NAS ou serveur SSH contrôlé      | Vérifier la version installée avant d'automatiser : la syntaxe diffère entre les grandes versions. |
| Restic     | Postes, serveurs et stockage distant avec backend compatible | Documenter la configuration du backend distant et protéger le compte utilisé.                      |
| rsync      | Copie simple de fichiers sur un support maîtrisé             | Ne le considérer ni comme un historique chiffré ni comme une sauvegarde complète à lui seul.       |
| Syncthing  | Réplication rapide de dossiers actifs entre appareils        | Ne pas le confondre avec une sauvegarde : une suppression peut se propager.                        |

### 4. Sécuriser le dépôt et les accès

- ☐ **Initialiser un dépôt chiffré avec Borg ou Restic**
- ☐ **Conserver les clés, mots de passe et secrets de récupération dans un emplacement sûr et documenté**
- ☐ **Séparer les accès de production des accès au dépôt de sauvegarde**  
Un compte administrateur partagé peut devenir un point de compromission commun.
- ☐ **Vérifier les conditions du stockage distant**  
Coût de stockage, coût éventuel de sortie, localisation, rétention et immutabilité.
- ☐ **Documenter une procédure lisible par une personne habilitée**  
Elle doit rester utilisable même si le serveur principal est indisponible.

### 5. Tester une restauration, pas seulement une sauvegarde



**1 Choisir un jeu de données représentatif**

Incluez des fichiers importants et, si nécessaire, les éléments de configuration associés.

**2 Restaurer vers un emplacement séparé**

Évitez d'écraser les données de production pendant le test.

**3 Contrôler le contenu restauré**

Vérifiez que les fichiers attendus sont présents, lisibles et utilisables.

**4 Noter les difficultés rencontrées**

Mettez à jour les commandes, les accès, l'emplacement des clés et l'ordre de reprise.

**5 Répéter le test régulièrement**

Une sauvegarde non restaurée reste une hypothèse.

**! Les faux sentiments de sécurité à éviter**

Trois dossiers sur le même disque, une synchronisation seule, un disque externe toujours connecté ou un NAS dans le même bâtiment ne répondent pas nécessairement aux risques de panne, de suppression, de vol, d'incendie ou de rançongiciel.

Conservez cette checklist avec la documentation des dépôts, des accès et des clés de récupération. Testez la restauration avant qu'un incident ne vous y oblige.