Stratégie de sauvegarde 3-2-1

Documentation rédigée par : GADONNAUD Ewen

Formation : BTS SIO 1ère année - Option SISR

Établissement : Lycée Paul-Louis Courier, Tours

Date : Mars 2026

1. Présentation de la règle 3-2-1

La règle **3-2-1** est une stratégie de sauvegarde largement adoptée dans le domaine de la sécurité informatique. Elle constitue un standard minimal recommandé par l'ANSSI pour garantir la disponibilité et l'intégrité des données en cas d'incident.

Principe clé : Aucune sauvegarde n'est fiable si elle repose sur un support unique ou un emplacement unique. La règle 3-2-1 impose une diversification systématique des copies et des supports.

Chiffre	Signification
3	Conserver **3 copies** des données (l'original + 2 sauvegardes)
2	Stocker ces copies sur **2 supports différents** (ex : disque local + NAS)
1	Conserver **1 copie déconnectée** (cloud, site distant, support physique externalisé)

2. Pourquoi cette règle ?

Sans stratégie structurée, les risques suivants menacent l'intégrité des données :

- **Défaillance matérielle** — panne disque, corruption de fichiers système
- **Ransomware** — chiffrement malveillant des données locales et des sauvegardes accessibles en réseau
- **Sinistre physique** — incendie, inondation, vol de matériel
- **Erreur humaine** — suppression accidentelle, écrasement de fichier

La copie hors site est le dernier rempart face aux sinistres physiques et aux attaques qui compromettent l'ensemble d'un site.

3. Mise en œuvre concrète

Exemple d'architecture 3-2-1

Copie	Support	Emplacement	Rôle
Copie 1 (originale)	Disque interne du serveur	On-premise	Données en production
Copie 2 (sauvegarde locale)	NAS / disque externe	On-premise (réseau local)	Restauration rapide
Copie 3 (sauvegarde distante)	VPS / stockage cloud	Hors site	Reprise après sinistre majeur

Outils courants

- **Rsync** — synchronisation incrémentale de fichiers entre machines Linux
- **Restic** — sauvegarde chiffrée et dédupliquée, compatible cloud (S3, Backblaze B2, SFTP…)
- **BorgBackup** — sauvegarde dédupliquée et compressée, orientée serveurs
- **Duplicati** — interface graphique, compatible nombreux backends cloud
- **Cron** — planification automatique des sauvegardes sur systèmes Unix

4. Types de sauvegardes

Le choix du type de sauvegarde influe directement sur l'espace de stockage consommé, la durée d'exécution et la complexité de la restauration.

Sauvegarde complète

Copie **intégrale** de l'ensemble des données à un instant T, sans distinction par rapport aux sauvegardes précédentes.

- **Avantage** — restauration simple et autonome, aucune dépendance à d'autres sauvegardes
- **Inconvénient** — consomme beaucoup d'espace et de temps à chaque exécution
- **Usage typique** — sauvegarde hebdomadaire de référence, point de départ d'un cycle

Sauvegarde incrémentale

Ne sauvegarde que les données **modifiées depuis la dernière sauvegarde** (complète ou incrémentale précédente).

- **Avantage** — très rapide, faible consommation d'espace
- **Inconvénient** — restauration complexe : nécessite la sauvegarde complète + **toutes** les incrémentales dans l'ordre
- **Usage typique** — sauvegardes quotidiennes entre deux sauvegardes complètes

Sauvegarde différentielle

Sauvegarde les données modifiées **depuis la dernière sauvegarde complète** uniquement (contrairement à l'incrémentale qui repart de la dernière sauvegarde quelle qu'elle soit).

- **Avantage** — restauration simple : sauvegarde complète + **une seule** différentielle suffisent
- **Inconvénient** — grossit progressivement au fil du temps jusqu'à la prochaine sauvegarde complète
- **Usage typique** — compromis entre incrémentale et complète

Sauvegarde immuable

Sauvegarde écrite en mode **WORM** (Write Once, Read Many) : une fois créée, elle ne peut être ni modifiée ni supprimée avant l'expiration d'une période de rétention définie.

- **Avantage** — protection maximale contre les ransomwares et les suppressions accidentelles ou malveillantes
- **Inconvénient** — nécessite un stockage compatible (ex : Object Lock S3, Backblaze B2, bandes magnétiques)
- **Usage typique** — copie hors site dans une architecture 3-2-1, conformité réglementaire

Comparatif

Type	Espace consommé	Vitesse de sauvegarde	Complexité de restauration	Résistance ransomware
Complète	Élevé	Lente	Simple	Faible (si accessible)
Incrémentale	Faible	Rapide	Complexe	Faible (si accessible)
Différentielle	Moyen	Moyenne	Moyenne	Faible (si accessible)
Immuable	Variable	Variable	Simple	**Élevée**

5. Bonnes pratiques

Planification

- Définir une **fréquence de sauvegarde** adaptée à la criticité des données (quotidienne, hebdomadaire...)
- Mettre en place une **politique de rétention** (ex : 7 sauvegardes quotidiennes, 4 hebdomadaires, 12 mensuelles)
- Automatiser via cron pour éviter les oublis

Intégrité et chiffrement

- Vérifier régulièrement l'**intégrité des sauvegardes** (checksums, tests de restauration)
- Chiffrer les sauvegardes hors site pour protéger les données en transit et au repos
- Ne jamais considérer une sauvegarde comme fiable sans l'avoir **testée en restauration**

Isolation

- La copie hors site ne doit **pas être montée en permanence** sur le réseau local (risque ransomware)
- Appliquer le principe du **moindre privilège** sur les accès aux dépôts de sauvegarde

6. Test de restauration

Une sauvegarde non testée est une sauvegarde dont on ne peut pas garantir l'efficacité. Il est indispensable de planifier des **tests de restauration réguliers** :

- Restaurer un fichier isolé pour vérifier l'intégrité des données
- Simuler une restauration complète sur un environnement de test
- Documenter les procédures de restauration (temps de reprise, ordre des opérations)

Indicateur	**Description**
RPO (Recovery Point Objective)	Perte de données maximale acceptable — détermine la fréquence des sauvegardes
RTO (Recovery Time Objective)	Durée maximale acceptable pour restaurer le service

7. Références

- ANSSI — Recommandations pour les sauvegardes
- CNIL — Sécurité des données personnelles

8. RAID, instantanés et continuité d’administration

Le RAID améliore la disponibilité selon le niveau choisi ; il ne protège pas contre toutes les suppressions logiques ni contre la perte du stockage. Un instantané reste lui aussi dépendant de son support.

Une restauration de bastion doit tenir compte de la configuration, de la base des comptes, des enregistrements et des accès nécessaires pour rétablir le service. La présence de WAC ne constitue pas à elle seule un plan de secours complet.

Voir RAID, Virtualisation et Guacamole.

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=reseau:divers:sauvegardes

Last update: **2026/10/18 01:23**