



Auteur : Christophe Pierrès	Maison en place V2	
Révision 1 - 25/08/2025 16:06	Plan de sauvegarde des données	
Référence : p12_3_donnees_202508.docx		Page 1 / 5



Plan de sauvegarde des données

Diffusion : OpenClassrooms – Mentor : Cesare de Padua - Evalueur : Théo Lemoine


Version	Date	Auteur	Motif
1	22/08/2025	Christophe Pierrès	Création du document
2			

Auteur : Christophe Pierrès	Maison en place V2	
Révision 1 - 25/08/2025 16:06	Plan de sauvegarde des données	
Référence : p12_3_donnees_202508.docx		Page 2 / 5

Contenu

Page

1. Plan de Sauvegarde des Données	3
1.1. Méthodologie appliquée	3
1.2. Définition des besoins	3
1.3. Solution sélectionnée	3
2. Plan de restauration des données.....	5

Auteur : Christophe Pierrès	Maison en place V2	
Révision 1 - 25/08/2025 16:06	Plan de sauvegarde des données	
Référence : p12_3_donnees_202508.docx		Page 3 / 5

1. Plan de Sauvegarde des Données

1.1. Méthodologie appliquée

Continuity Management : Mise en place de sauvegardes automatisées et de plans de reprise d'activité pour assurer la continuité de service en cas d'incident majeur.

1.2. Définition des besoins

L'application MaisonEnPlace nécessite une solution de sauvegarde robuste pour garantir la continuité de service et protéger les données critiques.

Les besoins identifiés sont :

- Haute disponibilité** : L'application doit être disponible 24/7 avec un objectif de temps de récupération (RTO) inférieur à 4 heures et un objectif de point de récupération (RPO) inférieur à 1 heure.
- Intégrité des données** : Les données des utilisateurs, du catalogue produit et des transactions doivent être protégées contre la corruption ou la perte.
- Évolutivité** : La solution doit pouvoir s'adapter à la croissance de l'entreprise et au volume croissant de données.
- Sécurité** : Les sauvegardes doivent être chiffrées et protégées contre les accès non autorisés.
- Géo-redondance** : Les données doivent être répliquées dans plusieurs zones géographiques pour se prémunir contre les catastrophes locales.
- Automatisation** : Le processus de sauvegarde doit être automatisé pour minimiser les erreurs humaines.
- Vérification** : Des tests réguliers de restauration doivent être effectués pour valider l'intégrité des sauvegardes.

1.3. Solution sélectionnée


Après analyse des besoins, nous recommandons une solution cloud combinant :

1. Infrastructure principale :

- Mise en place d'une architecture multi-AZ (Availability Zones) sur OVH Cloud
- Utilisation de bases de données gérées avec réplication automatique (OVH Cloud Databases)
- Stockage des fichiers dans un service de stockage d'objets avec versioning (OVH Object Storage Swift)

2. Stratégie de sauvegarde :

- Sauvegardes incrémentielles toutes les heures
- Sauvegardes complètes quotidiennes
- Conservation des sauvegardes selon une politique de rétention :
 - Horaires : 24 heures
 - Quotidiennes : 7 jours
 - Hebdomadaires : 4 semaines
 - Mensuelles : 12 mois
 - Annuelles : 7 ans


Auteur : Christophe Pierrès	Maison en place V2	
Révision 1 - 25/08/2025 16:06	Plan de sauvegarde des données	
Référence : p12_3_donnees_202508.docx		Page 4 / 5

3. Outils recommandés :

- OVH Veeam Backup & Replication pour la gestion centralisée des sauvegardes
- Snapshots automatiques des bases de données
- Réplication cross-region pour la géo-redondance
- Système de surveillance et d'alerte (OVH Monitoring)

4. Chiffrement et sécurité :

- Chiffrement des sauvegardes au repos (AES-256)
- Chiffrement en transit (TLS)
- Contrôle d'accès basé sur les rôles (RBAC)
- Journalisation et audit des accès aux sauvegardes

Auteur : Christophe Pierrès	Maison en place V2	
Révision 1 - 25/08/2025 16:06	Plan de sauvegarde des données	
Référence : p12_3_donnees_202508.docx		Page 5 / 5

2. **Plan de restauration des données**

En cas d'incident majeur nécessitant une restauration des données, voici les étapes à suivre :

1. **Évaluation de l'incident :**

- Identifier la nature et l'étendue de l'incident
- Déterminer les données affectées
- Constituer une équipe de gestion de crise

2. **Sélection de la sauvegarde :**

- Identifier la dernière sauvegarde valide avant l'incident
- Vérifier l'intégrité de la sauvegarde

3. **Préparation de l'environnement de restauration :**

- Si nécessaire, provisionner de nouvelles ressources d'infrastructure
- Configurer les paramètres réseau et de sécurité

4. **Processus de restauration :**

- Restaurer d'abord les bases de données
- Restaurer ensuite les fichiers statiques et les configurations (facilité par dockerisation)
- Vérifier les dépendances entre les composants

5. **Validation :**

- Exécuter des tests fonctionnels pour vérifier l'intégrité des données
- Vérifier les performances du système

6. **Basculement :**

- Rediriger le trafic vers l'environnement restauré
- Surveiller les métriques système pendant la transition

7. **Documentation et amélioration :**

- Documenter l'incident et le processus de restauration
- Identifier les points d'amélioration pour le futur