Reprise et Adaptation d'une Stratégie de Sauvegarde et de Restauration

Table des matières

[**1.** **Analyse de la stratégie d'application** 3](#_Toc175822727)

[**a)** **Éléments à sauvegarder** 3](#_Toc175822728)

[**b)** **Solutions de sauvegarde actuelles** 3](#_Toc175822729)

[**c)** **Procédures existantes** 3](#_Toc175822730)

[**2.** **Identification des différences entre les projets** 3](#_Toc175822731)

[**a)** **Comparaison** 3](#_Toc175822732)

[**b)** **Impact sur la stratégie** 3](#_Toc175822733)

[**3.** **Nouveau plan de sauvegarde** 4](#_Toc175822734)

[**a)** **Ajustements proposés** 4](#_Toc175822735)

[**b)** **Nouvelles procédures** 4](#_Toc175822736)

[**4.** **Mise en œuvre** 4](#_Toc175822737)

[**a)** **Configuration des outils** 4](#_Toc175822738)

[**b)** **Exécution des premières sauvegardes** 4](#_Toc175822739)

[**c)** **Tests de restauration** 4](#_Toc175822740)

[**5.** **Documentation de la stratégie** 5](#_Toc175822741)

[**a)** **Manuel utilisateur** 5](#_Toc175822742)

[**b)** **Procédures opérationnelles** 5](#_Toc175822743)

[**6.** **Éco-responsabilité** 5](#_Toc175822744)

[**a)** **Optimisation du stockage** 5](#_Toc175822745)

[**b)** **Réduction de la consommation énergétique** 5](#_Toc175822746)

[**7.** **Livrables** 5](#_Toc175822747)

[**8.** **Plan de Continuité d'Activité (PCA)** 5](#_Toc175822748)

[**a)** **Analyse des Risques** 5](#_Toc175822749)

[**b)** **Objectifs de Continuité** 6](#_Toc175822750)

[**Stratégies de Continuité** 6](#_Toc175822751)

[**a)** **Redondance des Systèmes** 6](#_Toc175822752)

[**b)** **Solutions de Secours** 6](#_Toc175822753)

[**Organisation et Responsabilités** 6](#_Toc175822754)

[**a)** **Équipe de Gestion de Crise** 6](#_Toc175822755)

[**b)** **Procédure d'Alerte** 6](#_Toc175822756)

[**Procédures de Continuité** 6](#_Toc175822757)

[**a)** **En cas de Panne du Système Principal** 6](#_Toc175822758)

[**b)** **En cas de Cyberattaque** 7](#_Toc175822759)

[**Tests et Exercices** 7](#_Toc175822760)

[**Formation** 7](#_Toc175822761)

[**Documentation** 7](#_Toc175822762)

[**Aspects Éco-responsables** 7](#_Toc175822763)

[**Mise à Jour et Amélioration Continue** 7](#_Toc175822764)

# **Analyse de la stratégie d'application**

## Éléments à sauvegarder

* Fichiers critiques : documents de projet, rapports financiers
* Bases de données : MySQL, PostgreSQL
* Systèmes : serveurs Windows et Linux
* Machines virtuelles : environnements de test et de développement

## Solutions de sauvegarde actuelles

* Logiciel : Veeam Backup & Replication
* Matériel : NAS Synology pour stockage local
* Cloud : Azure Backup pour stockage hors site

## Procédures existantes

* Sauvegardes incrémentales quotidiennes
* Sauvegardes complètes hebdomadaires
* Tests de restauration mensuels

# **Identification des différences entre les projets**

## Comparaison

| **Aspect** | **Projet existant** | **Nouveau projet** |
| --- | --- | --- |
| Volume de données | 5 TB | 10 TB |
| Types d'applications | Principalement bureautique | Incluant des applications métier critiques |
| Contraintes de temps | RPO 24h, RTO 48h | RPO 4h, RTO 8h |

## Impact sur la stratégie

* Nécessité d'augmenter la fréquence des sauvegardes
* Besoin de solutions de sauvegarde plus rapides
* Renforcement des mesures de sécurité pour les applications critiques

# **Nouveau plan de sauvegarde**

## Ajustements proposés

* Mise en place de sauvegardes incrémentales toutes les 4 heures
* Utilisation de la déduplication pour optimiser le stockage
* Implémentation d'une solution de sauvegarde continue pour les applications critiques

## Nouvelles procédures

* Sauvegarde continue pour les bases de données critiques
* Snapshots toutes les heures pour les machines virtuelles importantes
* Tests de restauration hebdomadaires pour les systèmes critiques

# **Mise en œuvre**

## Configuration des outils

* Mise à jour de Veeam Backup & Replication vers la dernière version
* Configuration de la réplication en temps réel vers Azure
* Mise en place d'agents de sauvegarde sur tous les serveurs critiques

## Exécution des premières sauvegardes

* Planification d'une sauvegarde complète initiale pendant un week-end
* Vérification de l'intégrité des données après la première sauvegarde complète
* Démarrage des sauvegardes incrémentales selon le nouveau planning

## Tests de restauration

* Restauration complète d'un serveur critique dans un environnement isolé
* Test de récupération de fichiers individuels à partir de différents points de sauvegarde
* Simulation d'une panne majeure et exécution du plan de reprise d'activité

# **Documentation de la stratégie**

## Manuel utilisateur

* Guide étape par étape pour initier une restauration
* Procédures de vérification des sauvegardes
* Instructions pour demander une restauration de données

## Procédures opérationnelles

* Checklist quotidienne pour la vérification des sauvegardes
* Processus de gestion des incidents de sauvegarde
* Protocole de mise à jour des systèmes de sauvegarde

# **Éco-responsabilité**

## Optimisation du stockage

* Utilisation de la déduplication pour réduire l'espace de stockage nécessaire
* Mise en place d'une politique de rétention des données plus stricte

## Réduction de la consommation énergétique

* Utilisation de matériel de sauvegarde à faible consommation
* Planification des sauvegardes intensives pendant les heures creuses

# **Livrables**

* **Schéma** : détaillé de l'infrastructure de sauvegarde.
* **Rapports** : des tests de restauration.
* **Documentation complète** : de la nouvelle stratégie de sauvegarde.
* **Plan de formation** : pour l'équipe technique.

# **Plan de Continuité d'Activité (PCA)**

## Analyse des Risques

* **Pannes matérielles** : Risque de défaillance des serveurs de sauvegarde.
* **Corruption des données** : Risque de perte ou d'endommagement des fichiers.
* **Cyberattaques** : Risque d'attaques par ransomware ou autres malwares.
* **Erreurs humaines** : Risque d'erreurs lors des opérations de sauvegarde.
* **Pannes électriques** : Risque de coupures prolongées d'électricité.

## Objectifs de Continuité

* **Temps Maximal d'Interruption Admissible (TMIA)** : 2 heures
* **Objectif de Point de Reprise (RPO)** : 30 minutes

# **Stratégies de Continuité**

## Redondance des Systèmes

* Mise en place d'un système de sauvegarde secondaire sur site.
* Réplication des données vers un stockage cloud sécurisé.

## Solutions de Secours

* Serveurs virtuels préconfigurés prêts à être déployés.
* Contrat avec un fournisseur de matériel pour remplacement rapide

# **Organisation et Responsabilités**

## Équipe de Gestion de Crise

* **Chef de projet TSSR** : Coordination générale.
* **Technicien systèmes** : Gestion technique.
* **Formateur TSSR** : Supervision et conseil.
* **Responsable de la formation** : Prise de décision finale.

## Procédure d'Alerte

* Détection du problème.
* Notification au chef de projet TSSR.
* Évaluation de la situation.
* Activation du PCA si nécessaire.
* Information à l'équipe pédagogique.

# **Procédures de Continuité**

## En cas de Panne du Système Principal

* Basculer sur le système de sauvegarde secondaire.
* Vérifier l'intégrité des données.
* Lancer les procédures de restauration si nécessaire.
* Informer les utilisateurs de l'interruption temporaire.

## En cas de Cyberattaque

* Isoler les systèmes affectés.
* Activer les sauvegardes hors-ligne.
* Restaurer depuis la dernière sauvegarde saine.
* Renforcer les mesures de sécurité.

# **Tests et Exercices**

* Simulation mensuelle de panne du système principal.
* Exercice trimestriel de restauration complète.
* Révision du PCA après chaque exercice.

# **Formation**

* Formation initiale de l'équipe TSSR aux procédures du PCA.
* Mise à jour des connaissances lors des exercices.

# **Documentation**

* Manuel du PCA accessible sur un portail sécurisé.
* Procédures détaillées pour chaque scénario de crise.

# **Aspects Éco-responsables**

* Optimisation de l'utilisation des ressources de stockage.
* Choix de solutions de sauvegarde économes en énergie.
* Recyclage du matériel obsolète.

# **Mise à Jour et Amélioration Continue**

* Révision trimestrielle du PCA.
* Intégration des retours d'expérience après chaque incident.
* Veille technologique sur les nouvelles solutions de sauvegarde.