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

Table des matières

1. Analyse de la stratégie d'application 3

a) Éléments à sauvegarder 3

b) Solutions de sauvegarde actuelles 3

c) Procédures existantes 3

2. Identification des différences entre les projets 3

a) Comparaison 3

b) Impact sur la stratégie 3

3. Nouveau plan de sauvegarde 4

a) Ajustements proposés 4

b) Nouvelles procédures 4

4. Mise en œuvre 4

a) Configuration des outils 4

b) Exécution des premières sauvegardes 4

c) Tests de restauration 4

5. Documentation de la stratégie 5

a) Manuel utilisateur 5

b) Procédures opérationnelles 5

6. Éco-responsabilité 5

a) Optimisation du stockage 5

b) Réduction de la consommation énergétique 5

7. Livrables 5

8. Plan de Continuité d'Activité (PCA) 5

a) Analyse des Risques 5

b) Objectifs de Continuité 6

Stratégies de Continuité 6

a) Redondance des Systèmes 6

b) Solutions de Secours 6

Organisation et Responsabilités 6

a) Équipe de Gestion de Crise 6

b) Procédure d'Alerte 6

Procédures de Continuité 6
a) En cas de Panne du Système Principal 6
b) En cas de Cyberattaque 7
Tests et Exercices 7
Formation 7
Documentation 7
Aspects Éco-responsables 7
Mise à Jour et Amélioration Continue 7

1. Analyse de la stratégie d'application

a) 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

b) Solutions de sauvegarde actuelles

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

c) Procédures existantes

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

2. Identification des différences entre les projets

a) Comparaison

Aspect	Projet existant	Nouveau projet
Volume de données	5 TB	15 TB
Types d'applications	Principalement bureautique	Incluant des applications métier critiques
Contraintes de temps	RPO 24h, RTO 48h	RPO 4h, RTO 8h

b) 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

3.Nouveau plan de sauvegarde

a) 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

b) 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

4.Mise en œuvre

a) 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

b) 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

c) 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

5.Documentation de la stratégie

a) Manuel utilisateur

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

b) 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

6.Éco-responsabilité

a) 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

b) Réduction de la consommation énergétique

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

7.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.

8.Plan de Continuité d'Activité (PCA)

a) 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.

b) Objectifs de Continuité

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

Stratégies de Continuité

a) Redondance des Systèmes

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

b) Solutions de Secours

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

Organisation et Responsabilités

a) 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.

b) 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

a) 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.

b) 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.