



I. Politique de sauvegarde et de restauration d'un Système d'Information (SI)

I.1 Définition

La mise en place d'une politique de sauvegarde et de restauration pour un Système d'Information (SI) est cruciale pour assurer la protection des données, la continuité des activités, et la résilience face aux incidents. Quelle que soit la taille ou la nature du SI, cette politique doit être bien structurée pour couvrir les aspects essentiels de la sauvegarde des données et de la récupération en cas de sinistre.

Voici un cadre général pour mettre en place cette politique

I.2 Analyse des besoins et identification des données critiques

La première étape consiste à identifier les données et les systèmes critiques qui doivent être sauvegardés. Il peut s'agir de :

- **Bases de données** : Données transactionnelles, informations des clients, documents financiers.
- **Applications métiers** : ERP, CRM, logiciels spécifiques à l'entreprise.
- **Fichiers et configurations** : Systèmes de fichiers, configurations des serveurs, documents internes.
- **Journaux systèmes** : Logs importants pour le diagnostic et la sécurité.

Il est essentiel de bien comprendre la criticité des données pour prioriser la fréquence des sauvegardes et définir le niveau de protection requis.

I.3 Objectifs de récupération : RPO et RTO

La politique de sauvegarde doit définir deux indicateurs clés :

- **RPO (Recovery Point Objective)** : Indique la quantité maximale de données que l'organisation peut se permettre de perdre. Par exemple, un RPO de 1 heure signifie que les données doivent être sauvegardées au moins toutes les heures.
- **RTO (Recovery Time Objective)** : Désigne le temps maximal acceptable pour restaurer les systèmes après un sinistre. Un RTO de 4 heures signifie que l'organisation doit être capable de remettre le système en service dans ce délai.

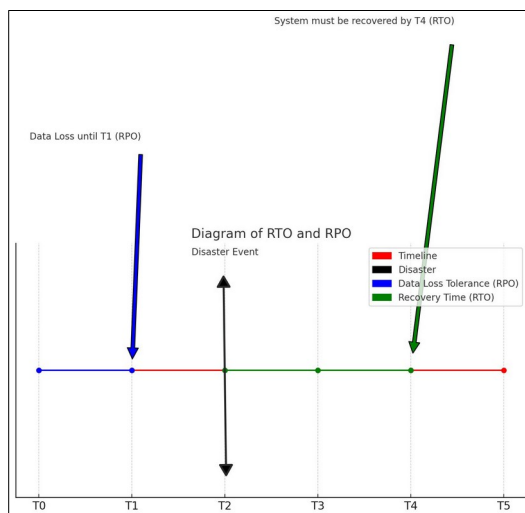


Figure 1 Figure 1 - RPO et RTO

Ces indicateurs varient en fonction des activités de l'entreprise et des contraintes métiers. Les systèmes critiques peuvent nécessiter un RPO et un RTO très bas, tandis que les systèmes moins critiques peuvent tolérer des temps de récupération plus longs.

I.4 Choix des types de sauvegardes

Les types de sauvegardes les plus couramment utilisés sont :

- **Sauvegarde complète** : Copie intégrale de toutes les données. Ce choix de sauvegarde est simple à restaurer mais consomme beaucoup d'espace de stockage.
- **Sauvegarde incrémentielle** : Sauvegarde uniquement les données modifiées depuis la dernière sauvegarde (complète ou incrémentielle). Ce choix de sauvegarde est moins gourmand en espace, mais plus complexe à restaurer car nécessite de restaurer la dernière sauvegarde complète et toutes les sauvegardes incrémentielles suivantes.
- **Sauvegarde différentielle** : Sauvegarde des données modifiées depuis la dernière sauvegarde complète. Ce choix de sauvegarde nécessite moins d'espace que la sauvegarde complète, mais plus que l'incrémentielle.

Le choix du type de sauvegarde dépend des besoins en termes de rapidité de restauration et des contraintes de stockage.

I.5 Stratégie de sauvegarde

Une bonne stratégie de sauvegarde prend en compte :

- **Fréquence des sauvegardes** : Elle peut être quotidienne, hebdomadaire, ou plus fréquente selon l'importance des données.



- **Planification des sauvegardes** : Les sauvegardes doivent être planifiées pour ne pas interférer avec les opérations courantes (par exemple, la nuit ou en dehors des heures de pointe).
- **Emplacements de sauvegarde** : Les données peuvent être sauvegardées localement (sur des serveurs ou des disques locaux), mais il est recommandé d'utiliser des solutions externes comme des **sites distants** ou le **cloud** pour la résilience.

I.6 Sécurité des sauvegardes

Les données sauvegardées doivent être protégées contre les accès non autorisés :

- **Chiffrement des sauvegardes** : Les données doivent être chiffrées à la fois en transit (lors de la transmission des sauvegardes) et au repos (lorsqu'elles sont stockées).
- **Contrôle d'accès** : Seules les personnes et les systèmes autorisés doivent avoir accès aux sauvegardes. Il est important d'appliquer une gestion stricte des permissions et d'utiliser des systèmes d'authentification sécurisés.
- **Conservation des sauvegardes** : Une politique de rétention doit être définie pour conserver un certain nombre de copies de sauvegarde (exemple – garder les sauvegardes hebdomadaires pendant 6 mois, les sauvegardes mensuelles pendant 1 an).

I.7 Test de restauration

Une politique de sauvegarde n'est utile que si les restaurations fonctionnent correctement. Il est donc essentiel de :

- **Tester régulièrement les procédures de restauration** pour s'assurer que les données sauvegardées peuvent être récupérées en cas de besoin.
- **Simuler des scénarios de sinistre** pour vérifier si les délais de récupération (RTO) sont respectés.
- **Documenter les procédures de restauration** de manière à ce qu'elles puissent être suivies facilement par le personnel technique.

I.8 Automatisation des sauvegardes

Automatiser les sauvegardes est essentiel pour garantir leur régularité et minimiser les erreurs humaines. Cela peut inclure :

- **Solutions de sauvegarde automatisée** : Utilisation de logiciels de sauvegarde qui permettent de planifier et d'exécuter automatiquement des tâches de sauvegarde (tar + cron, Percona XtraBackup, Veeam, Acronis, Bacula, etc.).



- **Surveillance des sauvegardes** : Mise en place de systèmes de surveillance et d'alerte pour détecter les échecs de sauvegarde et les anomalies.

I.9 Externalisation et redondance

Il est recommandé d'externaliser les sauvegardes dans des environnements distants pour se prémunir contre des sinistres majeurs (incendie, inondation, etc.). Les options incluent :

- **Solutions de cloud** : Utilisation de services cloud (Amazon S3, Azure, Google Cloud) pour stocker des copies des sauvegardes.
- **Sites distants** : Réplication des sauvegardes vers des centres de données situés dans d'autres régions géographiques.

I.10 Politique de rétention des sauvegardes

Une politique de rétention définit combien de temps chaque sauvegarde est conservée. Elle doit équilibrer le besoin de stocker des sauvegardes anciennes avec les coûts de stockage. Un plan typique peut inclure :

- **Sauvegardes journalières** : Conserver les sauvegardes quotidiennes pendant 7 jours.
- **Sauvegardes hebdomadaires** : Conserver les sauvegardes hebdomadaires pendant un mois.
- **Sauvegardes mensuelles** : Conserver les sauvegardes mensuelles pendant un an.

I.11 Documentation et formation

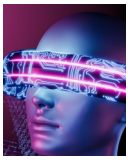
La politique de sauvegarde et de restauration doit être documentée en détail, avec :

- **Les procédures de sauvegarde** : Quand, comment, et où sont effectuées les sauvegardes.
- **Les procédures de restauration** : Étapes détaillées pour restaurer les systèmes et les données.
- **Les contacts clés** : Les personnes responsables de la gestion des sauvegardes et de la restauration.

De plus, le personnel doit être formé pour savoir comment exécuter les processus de restauration en cas de besoin.

I.11.1 Conclusion

La mise en place d'une politique de sauvegarde et de restauration d'un SI repose sur une approche méthodique qui inclut l'identification des besoins, le choix des solutions



BTS CIEL_IR



SI

Politique de sauvegarde et restauration

techniques, la sécurisation des données, et l'automatisation des processus. Une bonne politique garantit non seulement la protection des données critiques, mais aussi une capacité à récupérer rapidement après un sinistre, assurant ainsi la continuité des activités.