

# Prosit 8 : PANIQUE À BORD

# Contexte

Abstergo a eu un problème de sauvegarde le serveur a arrêter les sauvegardes il y’a 3 jours.

# Mots clés

Raid : https://www.ontrack.com/fr-fr/recuperation-donnees/raid/configurations#:~:text=De%20toutes%20ces%20configurations%20RAID,inscrit%20les%20informations%20en%20double

RAID 0-5 : Les niveaux RAID 0 à 5 font référence à différentes configurations de stockage redondant utilisées pour améliorer la performance et la résilience des systèmes de stockage. Par exemple, le RAID 0 divise les données en bandes et les répartit sur plusieurs disques, tandis que le RAID 5 utilise une parité distribuée pour la tolérance aux pannes.

ESN : ESN signifie "Entreprise de Services du Numérique". C'est un terme utilisé en France pour désigner les entreprises qui fournissent des services liés à l'informatique, aux technologies de l'information et à la transformation numérique.

RTO : RTO signifie "Recovery Time Objective", soit l'objectif de temps de récupération en français. Il définit la durée maximale acceptable pour restaurer un service après une panne ou un incident.

RPO : RPO signifie "Recovery Point Objective", soit l'objectif de point de récupération en français. Il représente la quantité maximale de données qui peut être perdue en cas de sinistre, mesurée en fonction du temps.

Modèle de sauvegarde 3-2-1 : Le modèle de sauvegarde 3-2-1 est une méthode de sauvegarde recommandée qui consiste à avoir trois copies de vos données (2 copies sur site, 1 copie hors site) pour garantir leur sécurité.

Certification ISO : La certification ISO fait référence à la conformité d'une organisation à des normes établies par l'Organisation internationale de normalisation (ISO) pour garantir la qualité, la sécurité ou d'autres aspects liés aux processus et produits.

Norme ISO : Une norme ISO est un document qui spécifie des exigences, des recommandations ou des lignes directrices pour garantir la qualité, la sécurité ou d'autres aspects liés à un produit, un service ou un processus.

Sauvegarde différentielle : Une sauvegarde différentielle consiste à sauvegarder uniquement les données qui ont changé depuis la dernière sauvegarde complète. Cela permet de réduire l'espace de stockage nécessaire pour les sauvegardes.

PCI : PCI signifie "Payment Card Industry", soit l'industrie des cartes de paiement en français. Les normes de sécurité PCI définissent les exigences de sécurité pour les entreprises qui traitent des informations de paiement par carte de crédit.

PRI : PRI peut signifier "Primary Rate Interface" en anglais, ce qui se traduit en français par "Interface d'accès primaire". Il s'agit d'une interface numérique pour la transmission de données et de voix.

PCA : PCA peut signifier "Plan de Continuité d'Activité", qui est un ensemble de procédures et de ressources permettant à une organisation de maintenir ses opérations en cas de perturbations majeures.

PRA : PRA signifie "Plan de Reprise d'Activité", ce qui est similaire au PCA. Il s'agit des mesures et des procédures mises en place pour reprendre les activités après une interruption.

Contrat de maintenance : Un contrat de maintenance est un accord entre un fournisseur de services et un client qui spécifie les services de maintenance qui seront fournis, y compris la durée, les coûts et les obligations des parties.

Business Impact Analysis : L'analyse de l'impact sur l'activité (BIA) est un processus visant à évaluer les effets potentiels des perturbations sur les activités d'une organisation et à identifier les priorités de récupération.

Stockage PC : Le stockage PC fait référence à l'espace de stockage disponible sur un ordinateur sur ses différents disques, utilisé pour stocker des fichiers, des applications et des données.

Archivage : L'archivage consiste à stocker des données, des documents ou des informations de manière organisée et à long terme pour des raisons de conformité, de conservation ou d'historique.

T.I. : T.I. signifie "Technologies de l'Information", ce qui englobe l'informatique, les réseaux, la sécurité informatique et d'autres domaines liés à la technologie.

# Problématique

**- Comment rétablir la sauvegarde ?**

**- Comment éviter que le problème (arrêt du système de sauvegarde) se répète à l’avenir ?**

# Contraintes

Sauvegarde différentielle

# Généralisation

Stratégie de gestion

Stratégie de sauvegarde

Criticité des risques

# Livrables

Rédaction du protocole de sauvegarde

Liste des risques qui pèsent sur le S.I.

Script qui envoie un mail lorsque la sauvegarde est terminée

# Pistes de solution

Utiliser le cloud Sauvegarde 3-2-1

Raid duplication de donnée d’un disque (deux disques : un principale et le second un duplicata du premier)

# Plan d’action

Mots-clefs + ressource + corbeille

Rédaction des livrables

Script

# Réalisation du plan d’action

## Rédaction du protocole de sauvegarde

Protocole de Sauvegarde pour PME

Objectif :

Mettre en place une procédure de sauvegarde fiable et efficace pour garantir la disponibilité et la protection des données critiques de l'entreprise.

Responsabilités :

L'administrateur informatique est responsable de la gestion du processus de sauvegarde.

Les employés sont tenus de suivre les directives de sauvegarde et de signaler tout problème ou perte de données.

Fréquence de sauvegarde :

Les sauvegardes complètes seront effectuées chaque semaine, le vendredi soir.

Des sauvegardes différentielles seront effectuées chaque jour ouvrable, du lundi au jeudi.

Support de stockage :

Les données sauvegardées seront stockées sur des disques durs externes dédiés et chiffrés pour des raisons de sécurité.

Des copies de sauvegarde seront stockées hors site dans un coffre-fort sécurisé ou via une solution de stockage cloud sécurisée.

Procédure de sauvegarde :

L'administrateur informatique configurera un logiciel de sauvegarde automatisé sur le serveur ou sur un dispositif de stockage dédié.

Les données importantes seront stockées dans des répertoires désignés pour la sauvegarde. Les employés seront informés de ces emplacements.

Chaque vendredi soir, une sauvegarde complète de tous les fichiers sera effectuée sur le disque dur externe.

Du lundi au jeudi, des sauvegardes différentielles seront effectuées pour capturer toutes les modifications apportées aux fichiers depuis la dernière sauvegarde complète.

Les fichiers de sauvegarde seront stockés dans des dossiers clairement étiquetés et datés sur le disque dur externe.

Les disques durs externes seront stockés dans un endroit sécurisé hors site, de préférence dans un coffre-fort ou via une solution de stockage cloud sécurisée.

Test de restauration :

L'administrateur informatique effectuera régulièrement des tests de restauration pour vérifier que les sauvegardes sont valides et que les données peuvent être restaurées en cas de besoin.

Mise à jour du protocole :

Ce protocole sera révisé régulièrement pour s'adapter aux besoins changeants de l'entreprise, aux évolutions technologiques et aux nouvelles menaces.

Sensibilisation des employés :

Les employés seront sensibilisés à l'importance de la sauvegarde des données, à la manière de stocker les fichiers dans les répertoires dédiés et à la procédure à suivre en cas de perte de données.

## Liste des risques qui pèsent sur le S.I.

Les systèmes d'information (S.I.) sont confrontés à de nombreux risques potentiels qui peuvent affecter leur fonctionnement, leur sécurité et leur disponibilité. Voici une liste des risques courants qui pèsent sur les Systèmes d'Information :

Cyberattaques : Les attaques informatiques, telles que les virus, les logiciels malveillants, les attaques par déni de service (DDoS), les ransomwares, peuvent compromettre la sécurité des données et des systèmes.

Pertes de données : Les pannes matérielles, les erreurs humaines, les cyberattaques et d'autres incidents peuvent entraîner la perte de données critiques.

Pannes matérielles : La défaillance de composants matériels, comme les disques durs, les serveurs ou les routeurs, peut entraîner des temps d'arrêt inattendus.

Pannes logicielles : Les bogues, les erreurs de programmation et les mises à jour logicielles défaillantes peuvent causer des problèmes de fonctionnement des applications.

Incompatibilité logicielle : L'utilisation de logiciels incompatibles peut entraîner des conflits et des problèmes de compatibilité.

Perturbations réseau : Les interruptions de réseau, qu'elles soient causées par des pannes matérielles, des attaques ou des erreurs de configuration, peuvent affecter la connectivité et la disponibilité des services.

Problèmes de sécurité : Les vulnérabilités de sécurité, les fuites de données et les accès non autorisés sont des risques majeurs pour la sécurité des S.I.

Conformité réglementaire : Les S.I. doivent se conformer aux lois et réglementations en vigueur, ce qui peut entraîner des sanctions en cas de non-conformité.

Risques humains : Les erreurs humaines, la négligence, les utilisateurs malveillants et les attaques sociales peuvent compromettre la sécurité des S.I.

Obsolescence technologique : Les systèmes et logiciels obsolètes peuvent devenir moins sécurisés et moins fonctionnels avec le temps.

Problèmes de gestion de projet : Les retards, les dépassements de budget et les problèmes de gestion de projet peuvent affecter la mise en place de nouveaux systèmes d'information.

Évolutions technologiques : Les avancées rapides de la technologie peuvent rendre obsolètes les systèmes actuels, nécessitant des mises à jour coûteuses.

## Script qui envoie un mail lorsque la sauvegarde est terminée

J’ai ensuite réalisé ce script avec la corbeille, malheureusement les sécurités renforcés de google ne permettent pas de se connecter a ma boite mail de test.

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

# 