Situation 2 : Mise en place sauvegarde automatique sur serveur de fichier

Rapport d'incident

Description			
Date :	Lundi 26 janvier 2026	**Heure :**	11h44
Equipement :	Serveur de fichier vm-files01		
Personnes impactées :	Service financier et administratif		
Symptômes :	Un fichier Excel important a été supprimé accidentellement. La restauration récente est impossible car la dernière sauvegarde date du 16 janvier au lieu du 23 janvier (oubli humain). Cela a entraîné une perte de travail significative du 19 au 23 janvier.		
Gravité :	☐Mineur	☒Majeur	☐Critique
Analyse			
La cause racine est une erreur humaine (sauvegarde manuelle oubliée). L'incident a été aggravé par l'absence d'automatisation, de vérification systématique et d'alertes en cas d'échec. Le processus manuel non vérifié a créé un point de défaillance silencieux.			
Action corrective			
Immédiate	**À prévoir**		
Une sauvegarde manuelle a été lancée le lundi à 12h42 et une vérification de l'intégrité a été effectuée.	Mise en place d'une sauvegarde automatique planifiée, incluant des tests de restauration.		
Conclusion			
L'incident a révélé la fragilité du processus manuel. Le passage à une solution technique durable et automatisée est nécessaire pour garantir la traçabilité et éviter la perte de données future.			

Analyse du besoin :

Limite actuelle :

La société a récemment fait face à une suppression accidentelle de fichiers sur le serveur de fichiers vm-files01. Les données d'une semaine d'un fichier ont été perdues, car la dernière sauvegarde remontait à deux semaines, en raison d'un oubli humain. Afin d'éviter toute perte future, l'entreprise souhaite mettre en place un système de sauvegarde automatique quotidienne, permettant de combler les erreurs humaines.

L'objectif principal est la mise en place d'un système de sauvegarde automatisé (pour les fichiers vm-files01) :

- Une **exécution planifiée chaque nuit** des sauvegardes ;
- Un **stockage sécurisé sur un disque dédié** ;
- Le maintien d'une **sauvegarde manuelle complémentaire chaque vendredi**, copiée sur un disque externe et **déplacé dans un autre bâtiment** (bâtiment B) pour réduire les risques physiques ;
- Une **alerte** en cas d'échec ;
- Une possibilité de **restauration simple et rapide**.

Les besoins fonctionnels sont les suivants :

- **Automatiser les sauvegardes** : planification de la sauvegarde complète sans intervention humaine ;
- **Gérer la rétention** : conserver plusieurs versions (par exemple les 10 dernières sauvegardes) ;
- **Prévoir une double sauvegarde** :
    - Automatique quotidienne vers un disque dédié monté sur le serveur Proxmox ;
    - Manuelle hebdomadaire vers un disque dur externe stocké physiquement dans un autre bâtiment (B) pour garantir une protection contre les sinistres (incendie, vol…) ;
- **Tester les restaurations** : prévoir une procédure de test régulière pour valider les points de sauvegarde.

Juridique :

Cette solution doit respecter plusieurs exigences juridiques :

- **Protection des données (RGPD)** : les fichiers sauvegardés peuvent contenir des données personnelles. Leur conservation, leur accès et leur restauration doivent être sécurisés et documentés.
- **Traçabilité** : chaque action de sauvegarde doit pouvoir être tracée (log).

Contexte d'utilisation, processus et acteurs concernés :

La solution est utilisée **au sein de l'infrastructure existante** : un serveurs Windows Server (ad01), un serveur Proxmox (hébergeant GLPI, fichier, ad02…) et une vingtaine de postes utilisateurs.
Les sauvegardes concernent principalement **les fichiers partagés sur la machine virtuelle vm-files01**, utilisés quotidiennement par les différents services.

Processus métier impactés :

- Accès et travail sur les **fichiers collaboratifs** ;
- Gestion de crise en cas de **perte** ou de **corruption** ;
- Plan de continuité d'activité.

Acteurs concernés :

- **Utilisateurs finaux**, qui dépendent de la disponibilité des fichiers ;
- **Techniciens du service informatique**, chargés de la supervision, de la sauvegarde manuelle et de la restauration.

3 choix pour la solution possible :

- **Rsync** : outil de synchronisation de fichiers sous Linux. Il permet de copier efficacement les données d'un répertoire vers une autre destination, avec prise en charge des mises à jour incrémentales.
- **BorgBackup** : logiciel de sauvegarde moderne orienté serveur. Adapté aux environnements professionnels où la sécurité et l'efficacité du stockage sont importantes.
- **BackupPC :** système de sauvegarde centralisé et versionné, basé sur disque, destiné à sauvegarder un parc de postes (Linux/Unix, Windows, Mac). Il propose une interface web pour l'administration et la restauration.

Solution	Rsync	BorgBackup	BackupPC
Principe	Copie/synchro de fichiers	Déduplication, compression et chiffrement des archives (repo borg).	Serveur central de sauvegarde fichier-level : collecte les clients, conserve des versions et économise l'espace via pooling
Avantages	Simple, rapide, standard, facile à restaurer fichier par fichier.	Sauvegardes chiffrées, déduplication, historiques faciles, fiable pour sauvegarder les serveurs.	Interface Web pour gérer, Déduplication intelligente, support plusieur os
Défauts	Pas de chiffrement / déduplication natif (sauf en ajoutant outils) ; historique moins élégant.	Nécessite installation et apprentissage borg ; repo spécifique.	Pas de chiffrement, paramétrage des transferts plus techniques
Automatisation	Facile	Facile : borg a des outils pour prune/verify.	Facile : BackupPC est conçu pour une utilisation automatisée
Restauration	Directe (copie de fichiers).	Très bonne (restauration suivant les versions, fichier unique ou snapshot).	Restauration au niveau fichier via l'interface web, restauration granulaire
Coût	Logiciel Open Source, aucun coût de licence.	Logiciel Open Source, aucun coût de licence.	Logiciel Open Source, aucun coût de licence.
Adapté au contexte	OK si besoin simple mais pas un vrai outil de sauvegarde, juste de la copie/coller	Recommandé (sécurisé + historique + faible stockage grâce à la déduplication).	Plus orienté pour la centraliser/sauvegarde de beaucoup de clients et moins pour un seul serveur.

Choix de la solution retenue

Plusieurs points nous laissent tendre sur **BorgBackup** :

- Répond aux **sauvegardes automatiques fiable** (besoin initiale)
- **Chiffrement** important pour la **sécurité des données**
- **Déduplication** permet l'économie de **l'espace disque**

C'est le meilleur compromis **sécurité** / **conservation** / **simplicité** d'exploitation.

La solution repose sur la mise en place d'un **disque interne dédié** sur le serveur de l'hyperviseur (srv-prox01) permettant la **réception des sauvegardes quotidiennes** de vm-files01 ainsi que la bonne configuration sur vm-files01.

Spécifications techniques

Élément	Détail
Système d'exploitation	Ubuntu Server (vm-files01)
Outils	BorgBackup
Repo	/mnt/backup/borgRepo
Planification	Sauvegarde quotidienne dans la nuit

Notification	Enregistrement de logs + message en cas d'erreur

Justification en termes de coût, de délai et de qualité

Critère	Justification
Coût	Matériel minimal requis : **1 disque dédié** pour les sauvegardes locales (monté sur Proxmox) + **1 disque externe** (déjà dans l'entreprise pour la sauvegarde hebdo). Logiciel : **Borg** (open source) → pas de coûts de licence. Coût maîtrisé (achat de(s) disque(s)).
Délai	**Installation** et **configuration** de Borg, **tests** : **1 à 2 jours ouvrés**. Mise en place du **disque dédié Proxmox** : quelques heures selon disponibilité matériel.
Qualité	Sauvegardes **chiffrées** et **dédupliquées** → bonne efficacité stockage et sécurité. Restauration possible vers un état précis (**historique**). Automatisation **quotidienne** + copie hebdo hors-site → bon niveau de résilience pour l'entreprise.

Limites de responsabilité du prestataire

Le prestataire est responsable :

- De **l'installation** et **configuration conforme** de **Borg** et des jobs de sauvegarde.
- De la **formation minimale** (procédure d'attachement du disque externe, vérification des logs, procédures de restauration basique).

Il ne peut être tenu responsable :

- De **l'oubli de branchement du disque externe** si le processus dépend d'une action manuelle.
- Des **pertes dues** à une **absence de tests de restauration par l'entreprise** si ceux-ci ne sont pas planifiés.
- Des **pannes matérielles simultanées** rendant indisponibles la production et les backups si **aucune copie** hors-site/indépendante **n'est conservée**.

Considérations éthiques et environnementales

- Respect du RGPD : **chiffrement** des données sauvegardées, **contrôle d'accès** et **conservation limitée** selon nécessité.

Évolution envisagée :

L'évolution consiste à **mettre en place un système de sauvegarde automatique** sur la machine virtuel vm-files01 (serveur de fichiers) et la **modification de la procédure actuelle pour sauvegarder la VM complète**, elle doit :

- **Automatiser** la sauvegarde,
- **Envoyer des alertes** en cas d'échec,
- **Conserver plusieurs versions** de sauvegarde (rétention),
- Permettre une restauration **simple et fiable**.

Composants impactés de l'architecture technique :

Les principaux composants touchés par cette évolution sont :

- **vm-files01 :** Installation d'un logiciel ou script de sauvegarde automatique. Création d'une tâche planifiée.
- **Serveur Proxmox :** Utilisé comme destination de la sauvegarde automatique quotidienne : montage d'un disque dédié en local.
- **Sécurité :** Gestion des droits d'accès aux sauvegardes, chiffrement éventuel des fichiers et protection contre la suppression non autorisée.

- **Service informatique :** Modification des procédures internes : vérification automatique plutôt que manuelle, supervision, contrôle périodique des restaurations.

Risques liés à une mauvaise utilisation ou à un dysfonctionnement

Mauvaise utilisation :

- **Planification mal configurée** : si les politiques ne sont pas bien configurées, des mots de passe faibles peuvent mettre en danger le domaine. Permettant à des personnes non autorisées à accéder à des données sensibles de l'entreprise
- **Pas de contrôle de validité** : sans test de restauration régulier, les sauvegardes peuvent être inutilisables le jour où elles sont nécessaires.
- **Suppression involontaire du support** : si le disque de sauvegarde est effacé, déconnecté ou mal protégé, les données peuvent être perdues définitivement.

Dysfonctionnement technique :

- **Permission bloquante :** une mauvaise configuration peut empêcher l'accès à la sauvegarde lors de la restauration.
- **Mauvais montage ou permissions sur le disque** : si le disque dédié est mal monté, plein ou mal protégé, la sauvegarde automatique échouera ou sera vulnérable.
- **Centralisation des sauvegardes sur le même serveur** : si le disque de sauvegarde est directement lié au Proxmox et que la machine subit une panne matérielle majeure ou un ransomware, production et sauvegarde peuvent être perdues en même temps.

Éléments à sauvegarder et à journaliser

a. Éléments à sauvegarder :

Pour garantir la continuité du service de fichiers et pouvoir restaurer rapidement en cas d'incident, les sauvegardes doivent couvrir :

- **Les données utilisateurs** stockés dans **vm-files01** (tous les partages).
- **Les images/snapshot** de la VM.
- **L'état des points de montage** (montage du disque dédié sur Proxmox et du disque externe) pour détecter erreurs de montage.
- **Une copie hebdomadaire hors-site** complète du repo (disque externe) conservée physiquement dans le bâtiment B.

b. Journalisation :

Les éléments de journalisation à conserver pour **la traçabilité et le diagnostic :**

- **Logs des tâches Borg** (création, prune, check) : réussite / échec / durée / taille.
- **Événements de montage/démontage** du disque de sauvegarde (mount/umount).
- **Alertes d'espace disque** (seuils configurés).

Procédures d'alerte associées au service

Pour permettre une **réaction rapide en cas de problème**, mettre en place des alertes simples et efficaces :

- **Surveillance des tâches de sauvegarde** :
  - Si **borg check** signale une **corruption → message d'alerte.**
- **Surveillance stockage** :
  - Alerte si **espace libre < 15 %** sur le stockage de sauvegarde.
  - Alerte si **point de montage absent** / disque non détecté.
- **Surveillance copie hebdomadaire** :
  - Si la **copie hebdo** vers disque externe ne **peut pas se lancer** (disque absent) -> message d'alerte

Solutions de fonctionnement en mode dégradé et procédures de reprise

a. Mode dégradé :

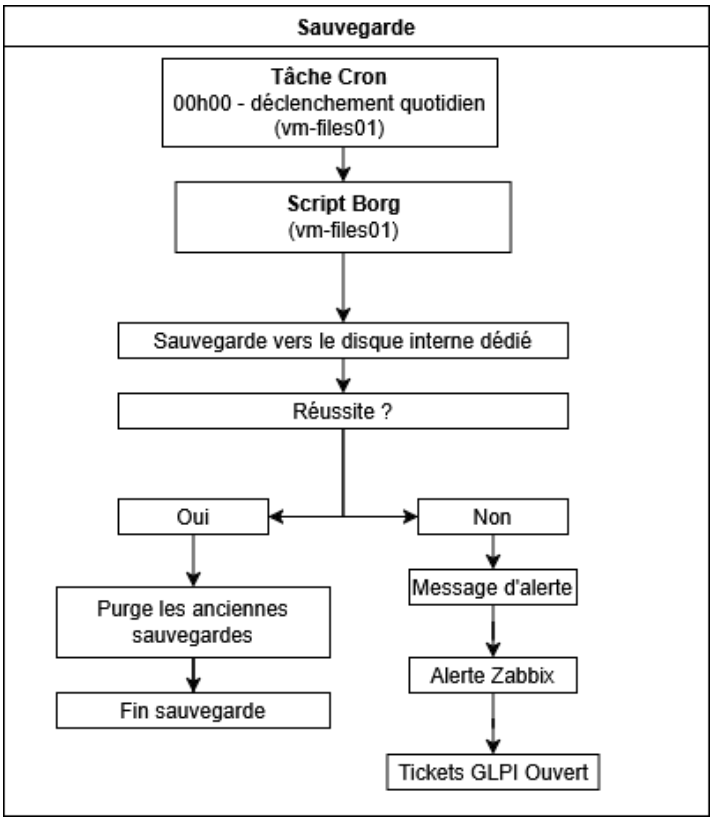
- **Accès temporaire en lecture seule** : si la VM de fichiers est indisponible mais que le repo local est intact, on peut monter le repo Borg en lecture seule sur une machine de secours (ou restaurer rapidement un répertoire critique en lecture seule) pour fournir un accès limité aux fichiers essentiels.

- **Pas de service haute disponibilité** : en cas de panne majeure, la d'une image de la vm depuis le disque externe permet de remettre le service en route.

b. Reprise du service :

1. **Identifier la cause** : Consulter les logs de sauvegarde et les messages système.
2. **Restauration rapide d'un fichier** : utiliser borg extract pour récupérer des fichiers critiques.
3. **Restauration complète** (si VM perdue) : restaurer une vm intacte via les images/snapshot sauvegardées sur le disque externe.
4. **Vérifier l'intégrité** : après restauration, vérifier permissions et effectuer un test d'accès.
5. **Rapport post-incident** : documenter l'incident, les étapes et les améliorations à apporter.

Maquette fonctionnelle :



Tests d'acceptation à réaliser

Les tests suivants permettent de valider le bon fonctionnement de la solution de sauvegarde automatique (BorgBackup) pour la VM vm-files01 :

Fonctionnement de la sauvegarde et Rétention

- Test de la création d'un snapshot borg quotidien (sauvegarde planifiée).
- Test de l'application de la politique de rétention (suppression des anciennes sauvegardes).
- Test de la création d'un snapshot hebdomadaire de vm-files01 vers le disque externe (processus hors-site).

Intégrité et Validation

- Test de l'intégrité du dépôt Borg (vérification des données).
- Test de la détection de corruption du dépôt.

Restauration des données

- Test de la restauration d'un fichier individuel.
- Test de la restauration d'un répertoire complet.

- Test de la restauration complète (simulation de reconstruction de la VM) via snapshot.

Gestion des Erreurs et Alertes

- Test du comportement si le disque externe est absent lors de la copie hebdomadaire.
- Test de la réaction du système en cas d’espace disque insuffisant sur la destination.