Livrable : Mise en place d'une solution de sauvegarde centralisée

EcoSolar Solutions — Scénario 2 (BTS SIO SISR 2025)

Client : EcoSolar Solutions

Prestataire : WildCorp (Pôle Infrastructure & Cybersécurité)

Consultant en charge : Roques-Bedos Joris

1. Contexte du projet

Dans le cadre de sa croissance et de la sécurisation de son savoir-faire technologique, l'entreprise **EcoSolar Solutions**, leader toulousain des panneaux solaires à haut rendement, a mandaté **WildCorp** pour moderniser son infrastructure informatique.

Avec un effectif en expansion et une production basée sur une technologie brevetée, la disponibilité et l'intégrité des données sont critiques. Une perte de données (plans de fabrication, données de R&D, gestion de la production) pourrait paralyser l'atelier de haute technologie et nuire gravement à l'économie locale soutenue par l'entreprise.

2. Objectifs de la mission

Ma mission au sein de l'équipe infrastructure consiste à concevoir et mettre en place une **solution de sauvegarde centralisée et automatisée**. L'objectif est de garantir que l'ensemble de l'écosystème virtualisé (serveurs de gestion, outils de production, bases de données) soit protégé contre toute défaillance matérielle ou attaque informatique.

Les axes prioritaires de cette solution sont :

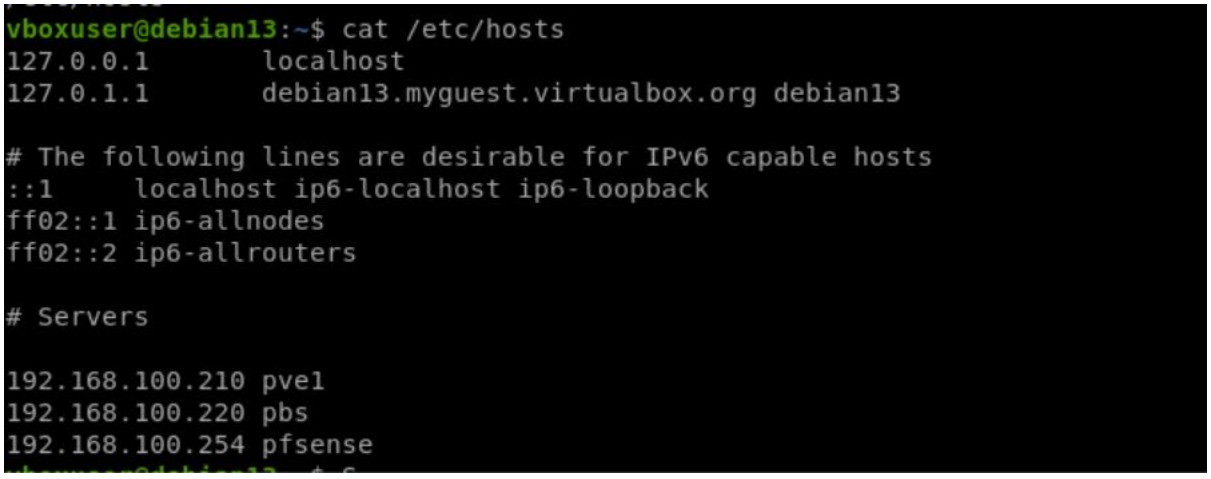
- **La centralisation :** Un point de contrôle unique pour toutes les sauvegardes des machines virtuelles (VM).
- **L'automatisation :** Éliminer l'erreur humaine par des routines de sauvegarde régulières.
- **La résilience :** Mise en place d'une stratégie de rotation efficace et de tests de restauration pour valider la "restaurabilité" réelle des données.

I. Début du projet

Objectif : Mettre en place une solution de sauvegarde automatisée pour l'infrastructure virtualisée (Proxmox VE) et formaliser un Plan de Reprise d'Activité (PRA) local.

Solution retenue : **Proxmox Backup Server (PBS)**, choisi pour sa compatibilité native avec Proxmox VE, sa déduplication intégrée, et ses fonctionnalités avancées de rétention, chiffrement et vérification de l'intégrité.

Composant	IP	Rôle
PBS	192.168.100.220	Solution de sauvegarde centralisée
PVE (Proxmox VE)	192.168.100.210	Hyperviseur hébergeant les VMs
Gateway	192.168.100.254	Firewall / Passerelle
VMs	192.168.100.x	AD, GLPI, Dolibarr, XiVO, Poste.io, etc.
Debian Test	192.168.100.10	Machine de test pour la restauration de fichiers et l'administration



[La PJ au-dessus contient la configuration de fichier hosts faites sur la machine Debian, permettant d'accéder aux interfaces graphiques de pbs, pve1, pfsense plus facilement sans avoir à entrer l'ip de chaque serveur (ex : https://pve1:8006/)]

II. Périmètre & Objectifs Techniques

2.1 Démarche d'analyse du besoin

J'ai utilisé la méthode **APTE (Application aux Techniques d'Entreprise)** pour structurer l'analyse du besoin. Cette approche permet :

- D'identifier le **véritable besoin** et le contexte d'utilisation.
- De formaliser les **fonctions utiles** et les **contraintes** du système.
- De préparer un Cahier des Charges Fonctionnel (**CdCF**) cohérent.

2.2 Bête à cornes (APTE)

- **À qui le système rend-il service ?** À EcoSolar Solutions, à son service informatique, et à l'ensemble des utilisateurs dépendant des services internes (AD, GLPI, fichiers, etc.).
- **Sur quoi agit-il ?** Sur les **machines virtuelles** de Proxmox, les **données critiques** des services, et la **continuité d'activité** en cas de panne.
- **Dans quel but existe-t-il ?** Pour garantir la **protection, la disponibilité, la restauration rapide** et la **pérennité** du système d'information.

2.3 Reformulation du besoin

Problème actuel	Besoin principal	Besoins secondaires
L'entreprise ne dispose **d'aucun système de sauvegarde fiable** ni de procédure officielle de reprise (PRA). L'ensemble des services pourrait être perdu en cas d'incident majeur.	Mettre en place une solution de sauvegarde centralisée et automatisée pour toutes les VMs Proxmox, associée à un **PRA permettant une restauration contrôlée et rapide.**	Automatiser les sauvegardes quotidiennes. **Sécuriser** le stockage des sauvegardes (chiffrement, rétention). Pouvoir restaurer **rapidement** un service critique (AD, GLPI…). Mettre en place des objectifs mesurables : **RPO 4h, RTO 2–4h.** Documenter l'ensemble du processus.

2.4 Diagramme pieuvre (APTE)

Acteurs / Contraintes autour du système de sauvegarde :

Élément externe	Interaction / Fonction
Proxmox VE	Envoie les VMs au serveur PBS (via TCP 8007)
Administrateurs	Gèrent les sauvegardes et les tests de restauration
Réseau LAN	Doit supporter le transfert des sauvegardes (impact sur la bande passante)
Sécurité	Exige chiffrement (AES-256) et accès restreint (Authentification)
Stockage	Capacité limitée -> impose une politique de rétention stricte

Fonctions obligatoires du système :

- Sauvegarder automatiquement les VMs et les fichiers critiques.
- Conserver l'historique selon la politique de rétention (**Pruning**).
- Restaurer une VM partielle ou complète (**Granularité**).
- Chiffrer les sauvegardes (**Confidentialité**).
- Valider l'intégrité des données après sauvegarde (**Verify**).
- Assurer un PRA rapide et documenté (**Disponibilité**).

2. Objectifs du projet

Objectif	Principe de Sécurité Associé	Mesurable / Justification
1. Centraliser la sauvegarde (PBS)	Intégrité, Confidentialité	Stockage unique, gestion des permissions, vérification.
2. Automatiser toutes les VMs	Disponibilité, Intégrité	Planification quotidienne. **RPO cible : 4 heures** (perte max acceptable).
3. Définir objectifs RPO/RTO	Disponibilité, Continuité	**RTO cible : 2 à 4 heures** (temps max pour redémarrer un service critique).

4. Déployer et documenter un PRA	Disponibilité, Traçabilité	Procédure claire et testée pour la reprise d'activité.
5. Sécuriser l'environnement	Confidentialité, Intégrité	Chiffrement AES-256, firewall strict, authentification par **token API**.

- **Objectifs mesurables** : Sauvegarde automatisée quotidienne + incrémentales horaires pour services critiques.

3. Choix techniques et justification

- **Proxmox Backup Server (PBS)** : Solution **Open Source** et **nativement optimisée** pour Proxmox VE. Offre la **déduplication** (réduction de l'espace), la **compression ZSTD** (rapidité et bon ratio), et une gestion fine de la rétention (**Prune/GC**).
- **Modes de sauvegarde** : Utilisation du mode **Snapshot** (*hot backup*) pour minimiser l'interruption des VMs.
- **Sécurité réseau** : Limitation du flux (PVE -> PBS) au seul port **TCP 8007** (protocole Proxmox Backup).
- **Authentification** : Utilisation d'un **token API dédié** (ex: `pve-backup@pbs!pve-token`) plutôt que du mot de passe `root` pour limiter la surface d'attaque en cas de compromission. (Finalement nous sommes passés par root dans notre cas car l'authentification par token api ne fonctionnait pas)

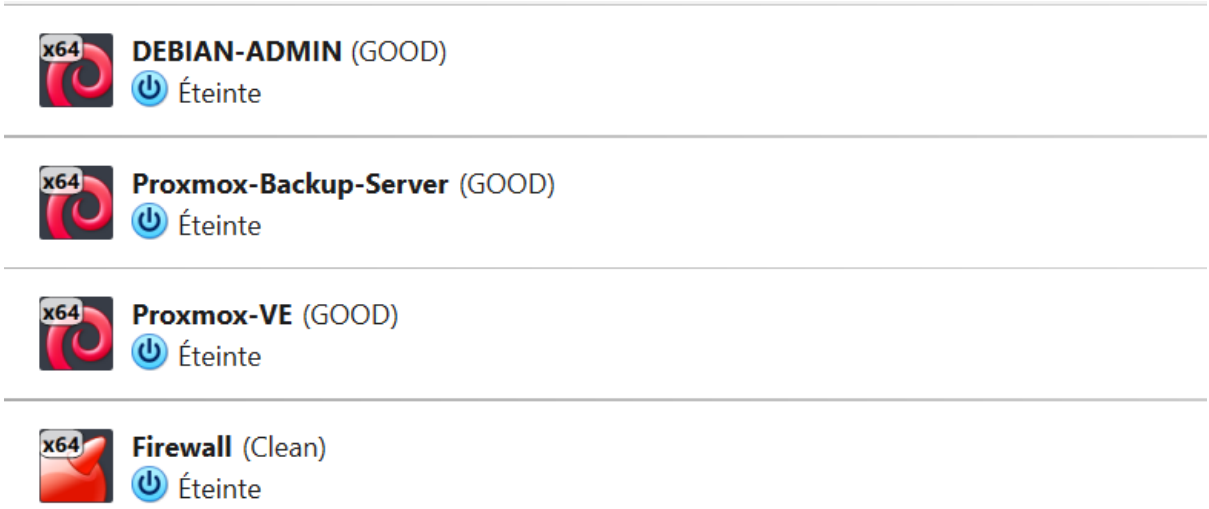
4. Prérequis matériels & logiciels

Composant	Configuration
PBS	IP 192.168.100.220, package `proxmox-backup-server`, stockage `/mnt/datastore/proxmox-data`.
Proxmox VE	192.168.100.210, accès root.
Flux réseau	Le firewall doit autoriser **TCP 8007** (PVE > PBS) pour la sauvegarde.

5. Étapes détaillées — Installation & Configuration

Remarque : exécute ces commandes en `root` sur les machines concernées.

Ici nous mettons en place 4 VMS différentes sur virtual box :



Debian-Admin : accès aux interface graphique de PBS, de PVE, et du firewall (pfsense)

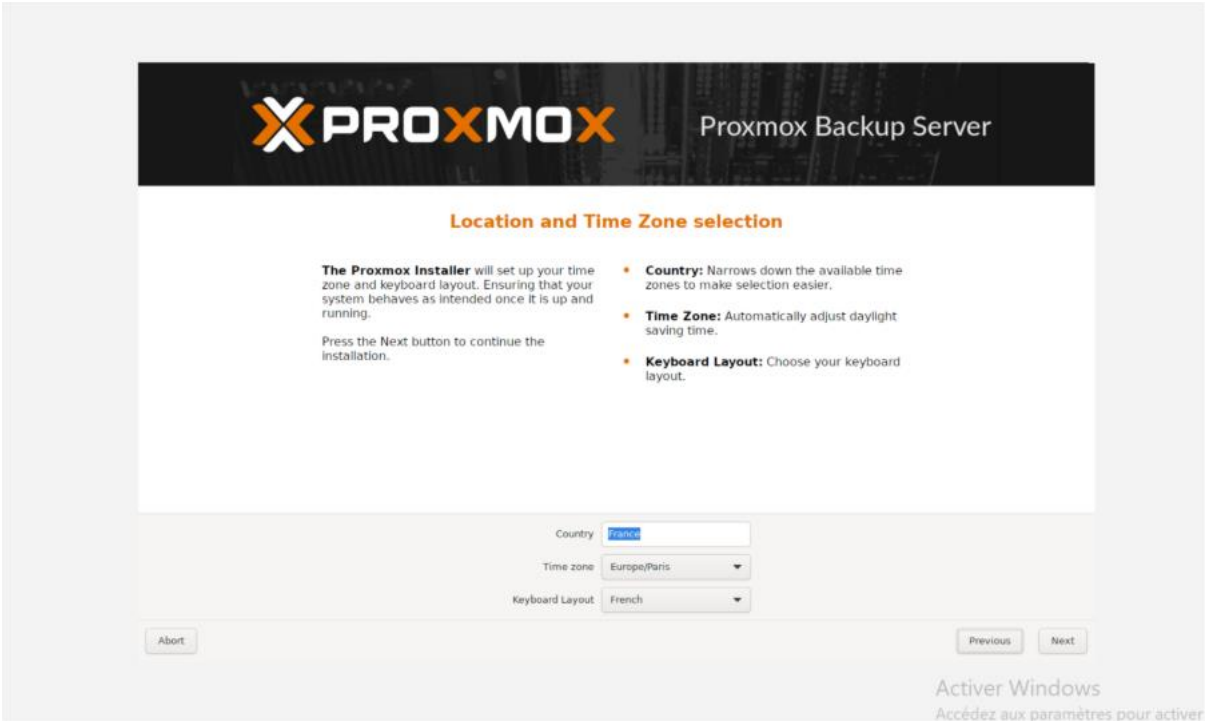
PBS : PROXMOX BACKUP SERVER

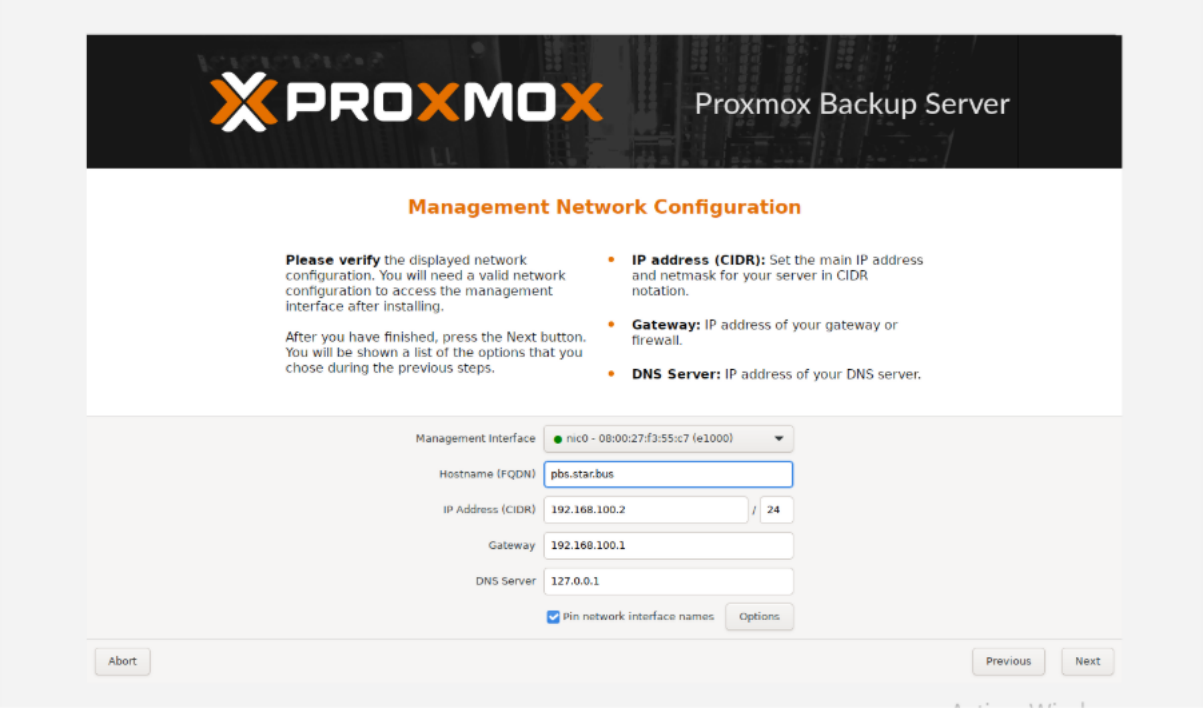
Proxmox VE : server proxmox

Firewall :

5.1. Installer Proxmox Backup Server (PBS)

Installation standard via l'ISO officiel. Configuration réseau : IP `192.168.100.220`, Gateway `192.168.100.254`.





5.2. Sur PBS — Préparation du stockage

```
Bash
# créer le dossier réel sur le disque dur du serveur PBS qui va contenir tous les morceaux de données.
#intérêt du -p : Cela crée toute la hiérarchie de dossiers d'un coup
mkdir -p /mnt/datastore/proxmox-data
# Définir la propriété et les permissions de sécurité pour l’user root (l’admin), si un service est corrompu cela empêche que les sauvegardes soient supprimés ou modifiées
chown root:root /mnt/datastore/proxmox-data
chmod 750 /mnt/datastore/proxmox-data
```

5.3. Créer le datastore via l'interface PBS

1. Ouvrir : https://192.168.100.220:8007
2. **Datastores** > **Create**
3. Name : proxmox-data
4. Directory/Backing Path : /mnt/datastore/proxmox-data
5. Configurer le **Scheduler** (prune/verify/gc) selon les objectifs de rétention.

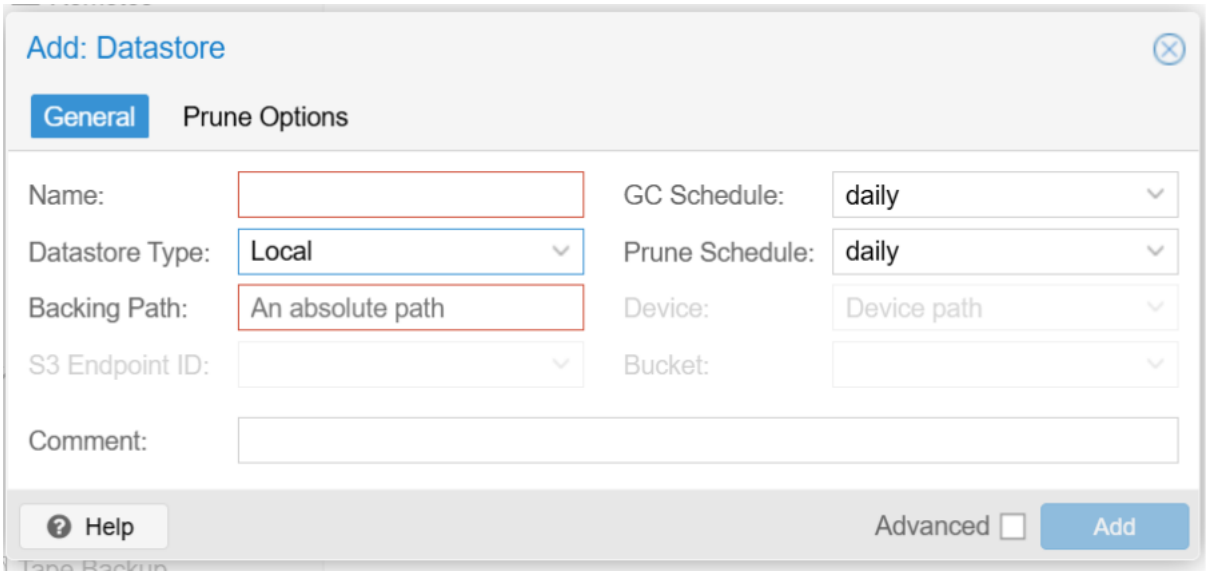
Retention :

- **Keep Last 7 / Daily 7 :** Tu gardes une image précise de chaque jour de la semaine passée. Si un bug survient le mardi, tu peux revenir au lundi.

- **Keep Weekly 4 :** Tu gardes un "cliché" de chaque fin de semaine sur le dernier mois.
- **Keep Monthly 3 :** Tu gardes une trace par mois sur un trimestre.
    - o
- **Encryption : activée (AES-256)**

Justification technique :

- Politique 7/7/4/3 = norme PME pour PRA de 30 jours glissants.
- Chiffrement AES256 → recommandation ANSSI.
- Datastore séparé du système pour isoler les risques.



5.4. Récupérer le Fingerprint TLS du PBS

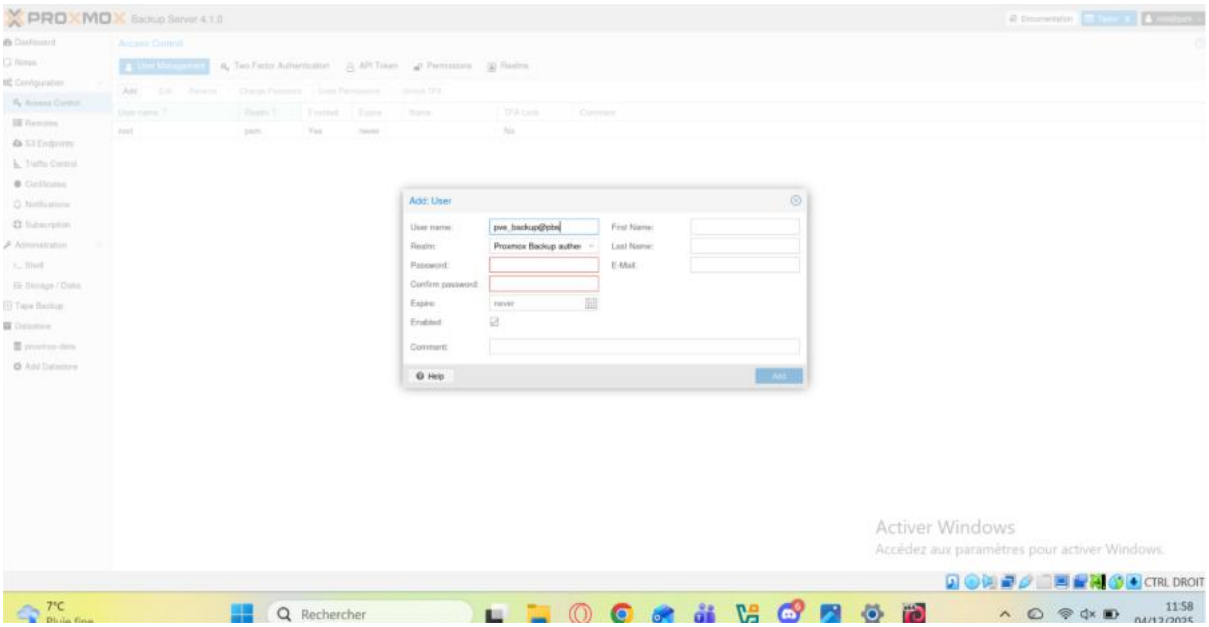
Sur le serveur PBS (CLI) :

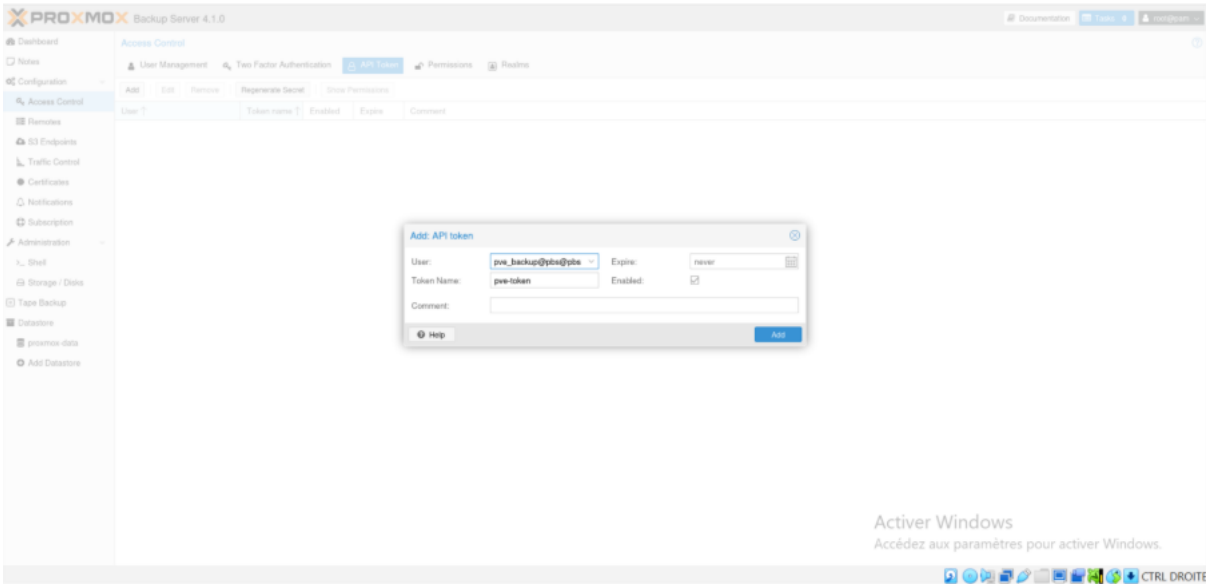
```
Bash
proxmox-backup-manager cert info
```

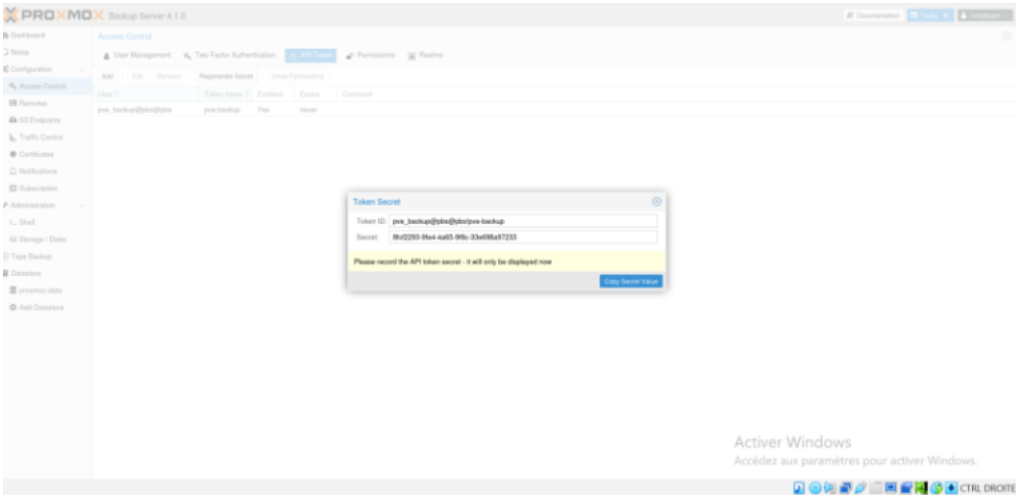
Copier la ligne **Fingerprint (SHA256)**.

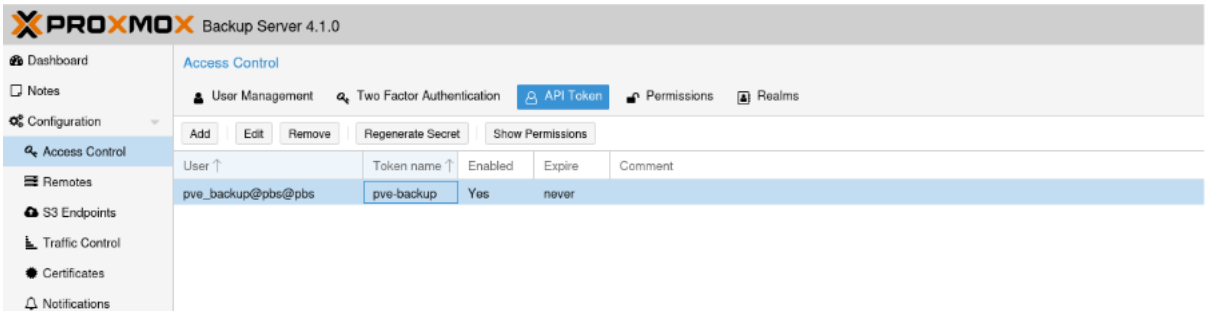
5.5. Créer un utilisateur/token PBS pour Proxmox

1. Interface PBS -> **Access Control** -> **Users** -> Créer l'utilisateur (ex: `pve-backup@pbs`).
2. **API Tokens** -> Créer un **token** (ex: `pve-token`). **Noter le Secret** (mot de passe du token).

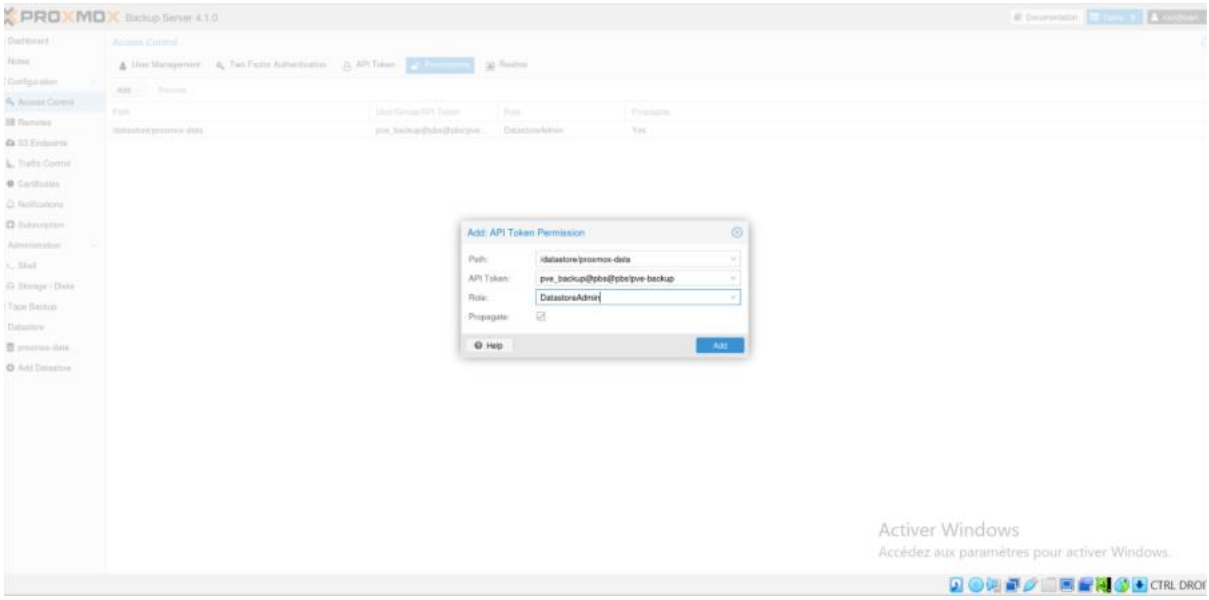
3. 
PROXMOX Backup Server 4.1.0
Add: User
Activer Windows
Accédez aux paramètres pour activer Windows.
Rechercher

4. 
PROXMOX Backup Server 4.1.0
Add: API token
Activer Windows
Accédez aux paramètres pour activer Windows.

5. 
PROXMOX Backup Server 4.1.0
Token Secret
Activer Windows
Accédez aux paramètres pour activer Windows.

6. 

Permissions : Attribuer les droits minimaux requis (ex : **Datastore Admin** sur `/proxmox-data`) au Token ou à l'utilisateur --> **Ajout des permissions = Access Control → Permissions → Add → API Token Permission :**



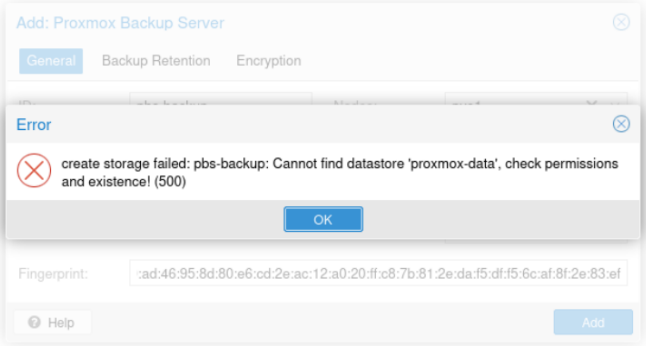
Proxmox VE utilisera donc l'user/TOKEN pour :

- Créer des sauvegardes
- Lire les sauvegardes
- Supprimer les anciennes (rotation)
- Vérifier l'espace disponible
- Gérer l'historique

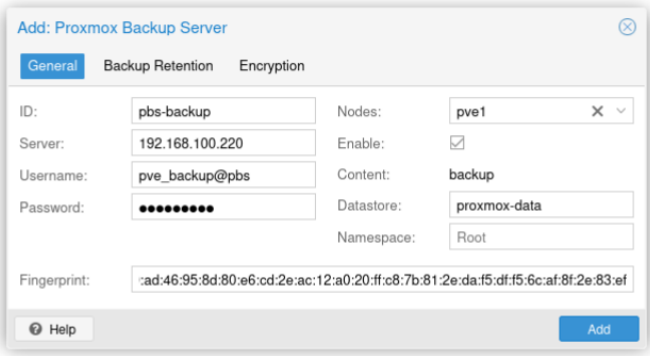
Mais **il ne doit PAS avoir accès à toute l'administration de PBS**, pour des raisons de sécurité. C'est pour cela que l'on n'utilise pas root@pam

5.6. Ajouter le PBS comme storage dans Proxmox VE (relier PVE à PBS)

Via PVE, cela permet de lui indiquer comment communiquer avec le PBS, via le token que nous venons



de créer.



1. Interface PVE -> **Datacenter** -> **Storage** -> **Add** -> **Proxmox Backup Server**.
2. `ID` : `pbs-backup`
3. `Server` : `192.168.100.220`
4. `Datastore` : `proxmox-data`
5. `Username` : `pve-backup@pbs!pve-token` (ou `root@pam` si nécessaire pour le TP)
6. `Password` : Le **Secret** du token API.
7. `Fingerprint` : Coller le fingerprint obtenu à l'étape 5.4.

Vérification : la connexion doit réussir et `pbs-backup` doit apparaître dans les stockages disponibles.

Création OK via id : root@pam

Un utilisateur dédié aurait été préférable, mais un problème de compatibilité dans l'interface a nécessité l'usage temporaire de root@pam afin de valider les tests de sauvegarde, par la suite.

5.6. Autoriser l'accès réseau (firewall)

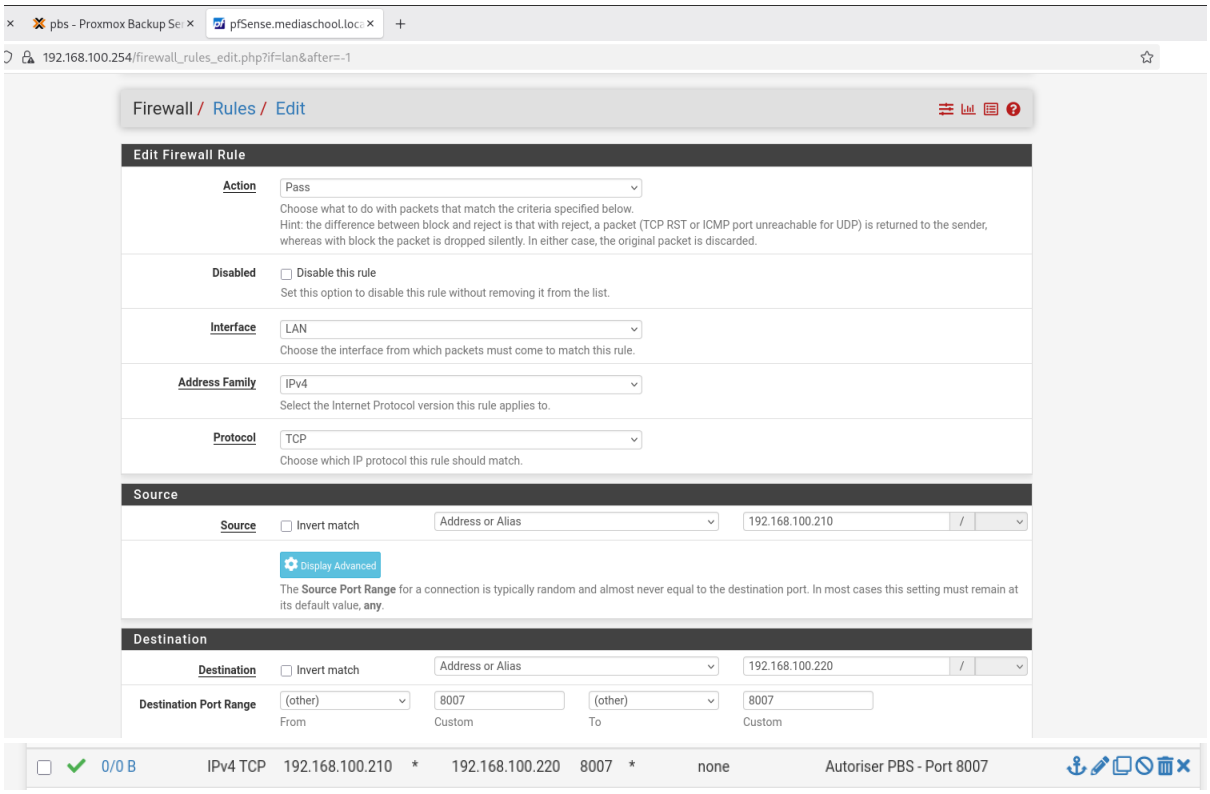
Sur la Gateway / pfSense / VirtualBox réseau : autoriser depuis **Proxmox VE (192.168.100.210)** vers **PBS (192.168.100.220)** :

- TCP **8007** (proxmox-backup)

Sur PBS, restreins les règles iptables / firewalld pour n'autoriser que l'IP du PVE.

Dans pfsense :

Firewall > Rules > LAN > ADD > Configuration de la règle :



Le fait de ne pas mettre la source en “any” sans spécifier l’adresse du PVE permet de limiter l’accès au serveur PVE sur le port 8007 et donc de faire en sorte que les autres machines sur le port 8007 ne puisse pas y accéder non plus.

5.7. Créer un Backup Job dans Proxmox VE

1. PVE -> **Datacenter** -> **Backup** -> **Add**.
2. `Storage` : `pbs-backup`
3. `Schedule` : **`0 */4 * * *`** (toutes les 4 heures pour les services critiques) ou `21:00 daily`.
4. `Mode` : **Snapshot**.
5. **Sélection** : `Include selected VMs` (AD, GLPI, etc.).

Enregistrer. Le job s’exécutera automatiquement selon le planning.

5.8. Tester une sauvegarde manuelle

1. PVE -> Sélectionner la VM (ex : VM 101).
2. **Backup** -> **Backup now** -> Choisir `pbs-backup`.

6. Procédure de Restauration (Pas-à-Pas)

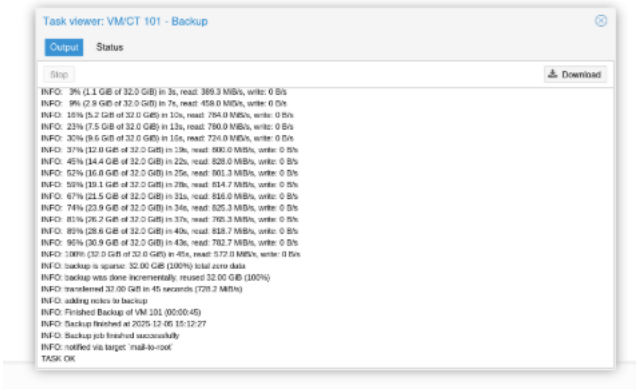
6.1. Restauration complète d'une VM (PRA)

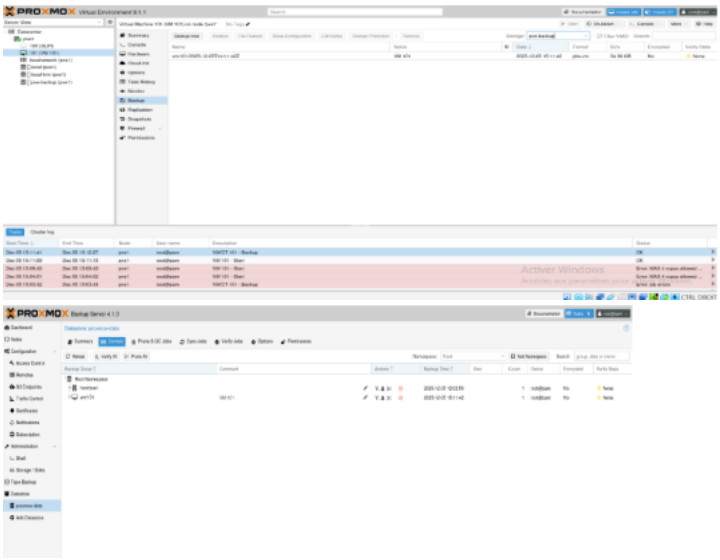
La restauration se fait depuis l'interface PVE.

- **Cas 1 : Écraser (Remplacer) l'original** : Lancer la restauration depuis l'onglet **"SAUVEGARDE”** de la VM en question
  `ID` reste le même .
  Ceci permet d’écraser la vm et de faire une sauvegarde la nouvelle.
- **Cas 2 : Créer une nouvelle VM (Test/PRA)** : Lancer la restauration depuis **Datacenter -> Storage -> pve-backup -> Backups**.
  - Sélectionner la sauvegarde -> **Restore**.
  - **Changer le VM ID** (ex: **999**).
  - **Vérifier les ressources** (RAM/vCPUs) pour éviter les erreurs de limite (`MAX 4 vcpus allowed`).

TEST et étapes :

Sur la VM --> Backup --> Sélectionne





Ici, le backup de la vm s'est réalisé même si une erreur (non importante) s'est présentée concernant le nombre de cpu de la machine qui en avait trop, j'ai juste modifié ce paramètre pour que la VM soit lancé et pour effectuer le backup.

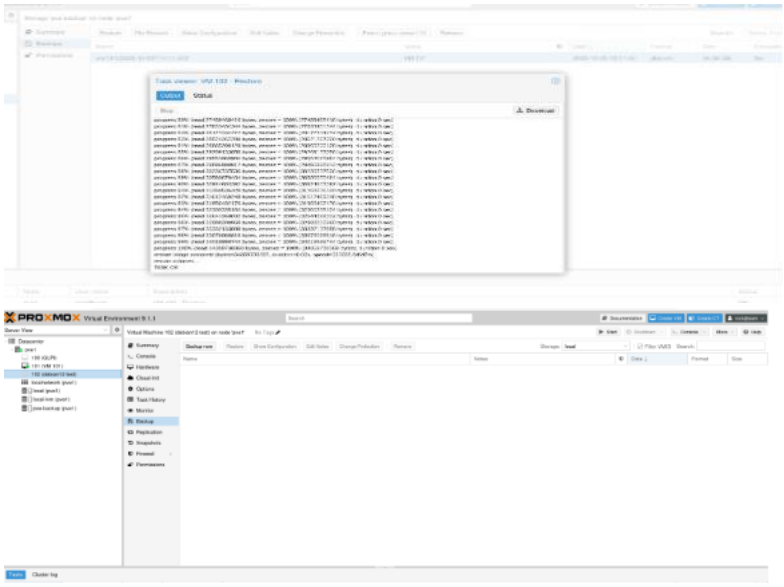
Le backup est bien présent sur PVE, et apparait dans le PBS dans "proxmox-data".

Test de restauration ensuite, ici deux solutions :

- Dans le cas 1 où nous souhaitons écraser (remplacer) la vm en question par le backup, nous lançons la restauration par = VM101 --> Sauvegarde

- Dans le cas où nous voulons avoir les deux à dispositions, et donc créer une nouvelle VM à partir du backup, nous passons par le stockage PBS dans le PVE

Ex pour la deuxième option :



6.2. Restauration d’un fichier individuel

```
root@pve1:~# ping 192.168.100.220
PING 192.168.100.220 (192.168.100.220) 56(84) bytes of data.
64 bytes from 192.168.100.220: icmp_seq=1 ttl=64 time=2.11 ms
64 bytes from 192.168.100.220: icmp_seq=2 ttl=64 time=0.853 ms
64 bytes from 192.168.100.220: icmp_seq=3 ttl=64 time=2.13 ms
^C
--- 192.168.100.220 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2061ms
rtt min/avg/max/mdev = 0.853/1.695/2.125/0.595 ms
root@pve1:~# proxmox-backup-client list --repository "root@pam@192.168.100.220:proxmox-data"
Password for "root@pam": *********
root@pve1:~# mkdir /root/backup-test
root@pve1:~# echo "Bonjour depuis PVE" > /root/backup-test/fichier1.txt
root@pve1:~# echo "Backup PBS réussi ?" > /root/backup-test/fichier2.txt
root@pve1:~#
```

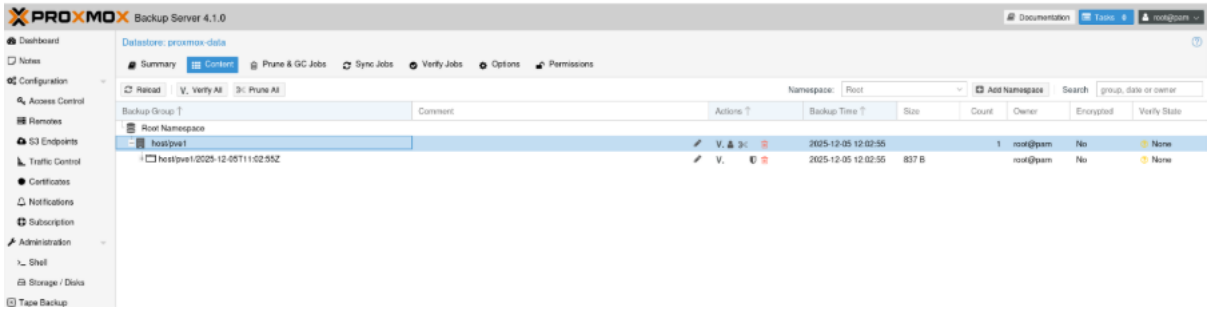
Test ping depuis PVE vers PBS OK

Création de fichier test sur le PVE

```
root@pve1:~# proxmox-backup-client backup test-pve.pxar:/root/backup-test --repository "root@pam@192.168.100.220:proxmox-data"
Starting backup: host/pve1/2025-12-05T11:02:55Z
Client name: pve1
Starting backup protocol: Fri Dec  5 12:02:55 2025
No previous manifest available.
Upload directory '/root/backup-test' to 'root@pam@192.168.100.220:8007:proxmox-data' as test-pve.pxar.didx
test-pve.pxar: had to backup 386 B of 386 B (compressed 232 B) in 0.07 s (average 5.159 KiB/s)
Uploaded backup catalog (81 B)
Duration: 0.26s
End Time: Fri Dec  5 12:02:55 2025
```

Commande utilisée : “proxmox-backup-client backup test-pve.pxar:/root/backup-test --repository "root@pam@192.168.100.220:proxmox-data" “

Cela apparait bien dans PBS :



Créer un dossier pour récupérer les fichiers :

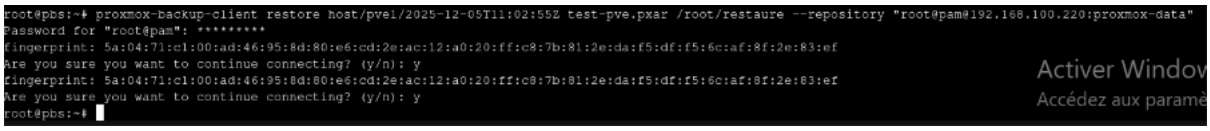
```
mkdir /root/restaure
```

Restaurer :

```
proxmox-backup-client restore test-pve.pxar /root/restaure --
repository root@pam@192.168.100.220:proxmox-data
```

```
--> Commande incomplète
```

```
Commande juste :
proxmox-backup-client restore host/pve1/2025-12-05T11:02:55Z test-
pve.pxar /root/restaure --repository
root@pam@192.168.100.220:proxmox-data
```



Je retrouve ensuite :

```
/root/restaure/fichier1.txt
/root/restaure/fichier2.txt
```

```
Ensuite je supprime le fichier1 pour tester une nouvelle
restauration :
Problème le fichier ne remonte pas :
Pour contourner ce problème j’ai donc recréé un dossier qui servira
à accueillir la restauration !
```

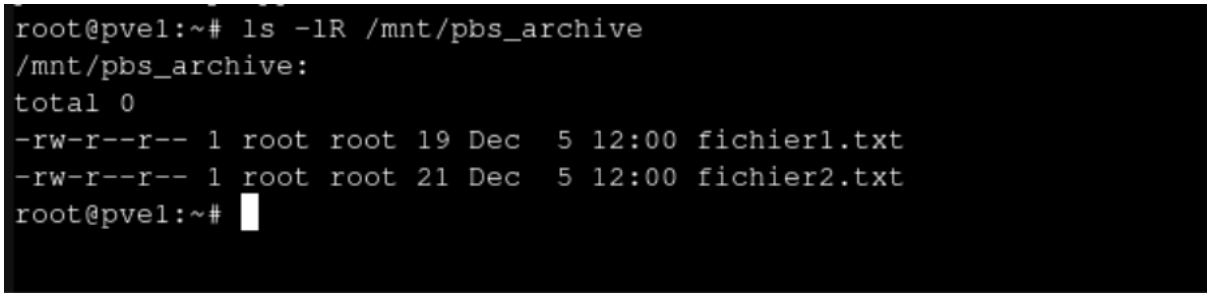
```
mkdir /mnt/pbs_archive
```

Comme la commande show et map ne fonctionne pas ici, j'utilise la commande " MOUNT" (La commande mount crée un point de montage local (comme un disque virtuel) à partir de votre archive PBS. Pour naviguer dans l'arborescence des fichiers et retrouver le fichier qui nous intéresse)

proxmox-backup-client **mount** host/pve1/2025-12-05T11:02:55Z test-pve.pxar /mnt/pbs_archive --repository root@pam@192.168.100.220:proxmox-data

Ensuite je fais : "ls -lR /mnt/pbs_archive"

Et les fichiers y sont bien présents, dont le fichier1.txt



6.2. Restauration d'un fichier individuel (Dépannage)

Procédure réelle

Contexte : Le client `proxmox-backup-client` était utilisé pour sauvegarder des fichiers dans une archive `.pxar`.

Commande de sauvegarde (ex.) :

```
Bash
proxmox-backup-client backup host/pve1/test-pve.pxar:/root/backup-test --repository "root@pam@192.168.100.220:proxmox-data"
```

Procédure de Restauration FIABLE (CLI) :

1. **Créer un répertoire de destination temporaire** :

```
Bash
mkdir /root/restaure_temp
```

2. **Lancer la restauration** (en incluant toutes les options de sécurité qui ont résolu les problèmes) :

```
Bash
proxmox-backup-client restore host/pve1/2025-12-05T11:02:55Z test-pve.pxar
/root/restaure_temp \
    --repository "root@pam@192.168.100.220:proxmox-data" \
    --ignore-ownership --ignore-permissions --allow-existing-dirs
```

3. **Copier le fichier souhaité** (ex: `fichier1.txt`) vers sa destination finale.
4. **Nettoyer** : `rm -rf /root/restaure_temp`

Outil de vérification : Pour inspecter l'archive, seule la commande **`mount`** a fonctionné sur la version de votre client :

```
Bash
proxmox-backup-client mount host/pve1/2025-12-05T11:02:55Z test-pve.pxar
/mnt/pbs_archive --repository "root@pam@192.168.100.220:proxmox-data"
# ... Inspection ...
fusermount -u /mnt/pbs_archive
```

7. Politique de sauvegarde & rétention

Type de VM	Fréquence	Rétention PBS (Ex.)
Critiques (AD, ERP)	Incrémentale toutes les 4h	`keep-hourly 24, keep-daily 7`
Non critiques (GLPI)	Daily	`keep-daily 7, keep-weekly 4`

- **Chiffrement** : Activation du chiffrement côté client (AES-256) pour les sauvegardes sensibles.
- **Tests** : Restauration partielle hebdomadaire et restauration complète trimestrielle.

8. Sécurité — Mesures et Bonnes Pratiques

- **Segmentation réseau** : Utilisation recommandée d'un **VLAN dédié** pour le flux de sauvegarde.
- **Firewall** : Autoriser uniquement **PVE -> PBS sur TCP 8007**.
- **Authentification par token** : Utilisation d'un **token API dédié** avec droits minimaux (`DatastoreAdmin`) plutôt que `root`.

- **Hardening** : Appliquer les mises à jour, désactiver les services inutiles, utiliser des clés SSH.
- **PRA Off-site** : Prévoir la réplication des sauvegardes vers un site distant pour le PRA en cas de sinistre total.

9. Plan de Reprise d'Activité (PRA) — Fiche Synthétique

- **Déclenchement** : Interruption de service ou perte matérielle majeure.
- **Priorité des services** : **AD/DNS/DHCP** (RTO 2h), File Server (RTO 3h), ERP (RTO 4h).
- **Procédure rapide** :
    - Évaluer l'incident et déclarer le PRA.
    - Préparer un hôte PVE de reprise.
    - **Restaurer AD** en priorité absolue, puis les autres services dans l'ordre de criticité.
    - Vérifier l'authentification et les services.
    - Documenter et communiquer aux utilisateurs.