

Proxmox VE Backup & Restore — Stratégies Avancées 2026

Catégorie : Virtualisation | Lecture : 18 min | Publié le : 12/04/2026 | Auteur : Ayi NEDJIMI

Guide expert PBS Proxmox : sauvegardes incrémentales, déduplication, réplication off-site, restauration granulaire et scénarios DR. Retours d'expérience production.

La protection des données dans un environnement Proxmox VE ne se limite pas à planifier un job de sauvegarde hebdomadaire et espérer que tout fonctionne le jour où l'on en a besoin. Les architectures de virtualisation modernes hébergent des charges critiques — contrôleurs de domaine, bases de données transactionnelles, serveurs applicatifs métier — dont la perte entraîne des conséquences financières et opérationnelles mesurables en heures d'interruption et en données irrécupérables. Proxmox Backup Server (PBS) change la donne en apportant une solution native de sauvegarde incrémentale avec déduplication au niveau bloc, conçue spécifiquement pour l'écosystème Proxmox. Ce guide détaille les stratégies avancées de backup et de restauration que nous déployons en production chez nos clients, des architectures PBS multi-sites aux procédures de Disaster Recovery testées trimestriellement, en passant par l'intégration avec les solutions de sauvegarde entreprise comme Veeam et Nakivo. Chaque recommandation s'appuie sur des retours d'expérience concrets issus d'environnements de 10 à 500 machines virtuelles.

Architecture Proxmox Backup Server (PBS)

PBS fonctionne comme un serveur de stockage dédié qui reçoit les flux de sauvegarde depuis les nœuds Proxmox VE via une API REST authentifiée par certificat. Le protocole de transfert utilise un mécanisme de chunking qui découpe chaque flux en blocs de taille variable (64 Ko à 4 Mo), identifiés par leur empreinte SHA-256. Cette approche permet une déduplication globale : un bloc identique présent dans 50 VMs différentes n'est stocké qu'une seule fois sur le datastore PBS.

Dimensionnement matériel du serveur PBS

Le dimensionnement du serveur PBS dépend directement du volume de données à protéger et de la fenêtre de rétention souhaitée. Pour un parc de 100 VMs totalisant 10 To de données brutes, le ratio de déduplication typique se situe entre 3:1 et 8:1 selon l'homogénéité des systèmes d'exploitation. Consultez [notre calculateur de sizing Proxmox](#) pour estimer vos besoins.

Composant	Petit env. (≤30 VMs)	Moyen env. (30-150 VMs)	Grand env. (150+ VMs)
CPU	4 cores	8 cores	16+ cores
RAM	8 Go	32 Go	64+ Go
Stockage OS	2x SSD 256 Go RAID1	2x SSD 512 Go RAID1	2x NVMe 1 To RAID1
Datastore	4x HDD 4 To RAIDZ1	8x HDD 8 To RAIDZ2	12x HDD 16 To RAIDZ2 + SSD cache
Réseau	1 Gbps dédié	10 Gbps	2x 10 Gbps LACP
Ratio dédup. attendu	3:1 à 5:1	4:1 à 6:1	5:1 à 8:1

Installation et configuration initiale

```
# Installation PBS sur Debian 12
echo "deb http://download.proxmox.com/debian/pbs bookworm pbs-no-subscription" > /etc/apt/sources.list.d/pbs.list
wget https://enterprise.proxmox.com/debian/proxmox-release-bookworm.gpg -O /etc/apt/trusted.gpg.d/proxmox-release-bookworm.gpg
apt update && apt install proxmox-backup-server -y

# Création du datastore ZFS
zpool create -o ashift=12 pbspool raidz2 /dev/sd{b,c,d,e,f,g}
proxmox-backup-manager datastore create backups /pbspool/backups

# Configuration de la rétention par défaut
proxmox-backup-manager datastore update backups \
  --keep-daily 7 \
  --keep-weekly 4 \
  --keep-monthly 6 \
  --keep-yearly 2

# Ajout du PBS dans Proxmox VE (côté PVE)
pvesm add pbs pbs-main \
  --server 10.0.1.50 \
  --datastore backups \
  --username backup@pbs \
  --fingerprint $(proxmox-backup-manager cert info --output-format json | jq
-r .fingerprint)
```

Modes de sauvegarde : Stop, Suspend, Snapshot

Le choix du mode de sauvegarde impacte directement la cohérence des données capturées et le temps d'indisponibilité de la VM pendant l'opération. Ce choix n'est pas anodin et doit être adapté à chaque charge de travail. Les environnements que nous auditions chez **nos clients migrant de VMware vers Proxmox** révèlent souvent un mauvais choix de mode de backup, source de corruptions silencieuses.

Mode Stop

Le mode stop arrête proprement la VM (via ACPI shutdown ou qemu-guest-agent), prend une image complète du disque, puis redémarre la VM. C'est le mode le plus fiable en termes de cohérence car il garantit que le système de fichiers est proprement démonté.

```
# Configuration dans /etc/pve/vzdump.cron ou via GUI
# Mode stop pour les VMs de base de données critiques
vzdump 100 --mode stop --storage pbs-main --compress zstd --notes-template "{{guestname}}
- backup stop mode"
```

Mode Suspend

Le mode suspend gèle l'état de la VM en mémoire (QEMU savevm), copie les disques, puis reprend l'exécution. Le temps de pause est plus court qu'un stop complet mais la RAM est aussi sauvegardée, ce qui augmente la taille du backup.

Mode Snapshot (recommandé)

Le mode snapshot utilise la fonctionnalité dirty bitmap de QEMU pour capturer un instantané cohérent des disques sans interrompre la VM. Avec le qemu-guest-agent installé, un appel `fsfreeze` est effectué juste avant le snapshot pour garantir la cohérence du système de fichiers.

```
# Vérifier que le guest-agent est installé et fonctionnel
qm agent 100 ping

# Backup snapshot avec guest-agent freeze
vzdump 100 --mode snapshot --storage pbs-main --compress zstd

# Pour les VMs Windows, installer le QEMU Guest Agent MSI
# et activer le VSS provider pour la cohérence applicative
```

Recommandation terrain

Utilisez le mode **snapshot** par défaut pour toutes les VMs avec le guest-agent installé. Réservez le mode **stop** uniquement aux VMs de bases de données critiques (PostgreSQL, MySQL) qui n'ont pas de mécanisme de journalisation WAL/binlog activé, ou aux contrôleurs de domaine Active Directory où la cohérence NTDS.dit est impérative. Le mode **suspend** est rarement justifié en 2026 compte tenu des performances du mode snapshot avec dirty bitmaps.

Sauvegardes incrémentales avec déduplication

PBS implémente une approche incrémentale au niveau bloc qui réduit drastiquement les temps de sauvegarde et l'espace de stockage consommé. Après un premier backup complet (full), chaque sauvegarde suivante ne transfère que les blocs modifiés depuis la dernière exécution. La déduplication opère ensuite au niveau du datastore global.

Fonctionnement du dirty bitmap

Proxmox VE 8.x+ utilise les dirty bitmaps QEMU pour suivre les blocs modifiés entre deux sauvegardes. Ce mécanisme, similaire au Changed Block Tracking (CBT) de VMware, permet de ne lire et transférer que les blocs réellement modifiés. Pour un serveur de fichiers de 2 To avec un taux de changement quotidien de 3%, le backup incrémental ne transfère que ~60 Go au lieu de 2 To.

```
# Vérifier les bitmaps actifs sur une VM
qm monitor 100 -c "info block"

# Statistiques de déduplication du datastore
proxmox-backup-manager datastore list --output-format json | jq '[][.stats]'

# Rapport d'espace économisé
proxmox-backup-client catalog dump --repository backup@pbs:backups
```

Garbage Collection et maintenance

```
# Planifier le GC (libérer les chunks orphelins)
proxmox-backup-manager datastore update backups --gc-schedule "sat 02:00"

# Vérification d'intégrité des chunks
proxmox-backup-manager datastore verify backups --ignore-verified --outdated-after 30

# Monitoring de l'utilisation du datastore
proxmox-backup-client status --repository backup@pbs:backups
```

Réplication off-site via PBS Remote Sync

Une sauvegarde qui réside sur le même site que l'infrastructure qu'elle protège n'est pas un plan de reprise d'activité. PBS intègre nativement un mécanisme de synchronisation entre datastores, local ou distant, permettant de répliquer les sauvegardes vers un site secondaire. Cette réplication est elle-même incrémentale et dédupliquée, minimisant la bande passante nécessaire. Pour les architectures réseau avancées, consultez [notre guide cluster Proxmox 3 nœuds](#).

```
# Sur le PBS distant, créer un sync job
proxmox-backup-manager sync-job create offsite-sync \
  --store backups \
  --remote pbs-site-a \
  --remote-store backups \
  --schedule "daily 04:00" \
  --remove-vanished true

# Monitoring de la bande passante utilisée
proxmox-backup-manager sync-job status offsite-sync
```

Chiffrement des sauvegardes off-site

```
# Générer une clé de chiffrement
proxmox-backup-client key create /etc/pve/priv/pbs-encryption-key.json

# Backup chiffré côté client (le PBS ne voit que des données chiffrées)
vzdump 100 --mode snapshot --storage pbs-main --encrypt 1

# IMPORTANT : sauvegarder la clé de chiffrement séparément !
# Sans cette clé, les backups sont irrécupérables
proxmox-backup-client key show /etc/pve/priv/pbs-encryption-key.json
```

Procédures de restauration

Restauration complète d'une VM

```
# Restaurer la VM 100 depuis le dernier backup
qmrestore pbs-main:backup/vzdump-qemu-100-*.vma 200 --storage local-zfs

# Restaurer avec modification des paramètres réseau
qmrestore pbs-main:backup/vzdump-qemu-100-*.vma 200 \
  --storage local-zfs \
  --unique true \
  --force true
```

Restauration de fichiers individuels

PBS permet de naviguer dans les sauvegardes et d'extraire des fichiers individuels sans restaurer la VM entière. Cette fonctionnalité est précieuse pour récupérer un fichier de configuration supprimé ou une base de données corrompue.

```
# Monter le backup en lecture seule via FUSE
proxmox-backup-client mount \
  --repository backup@pbs:backups \
  --snapshot vm/100/2026-04-10T02:00:00Z \
  /mnt/restore

# Naviguer et copier les fichiers nécessaires
ls /mnt/restore/
cp /mnt/restore/etc/nginx/nginx.conf /tmp/

# Démonter proprement
umount /mnt/restore
```

Restauration cross-cluster

Pour restaurer une VM depuis un PBS vers un cluster Proxmox différent, il suffit d'ajouter le PBS comme storage sur le cluster cible. Le mécanisme d'authentification par fingerprint garantit que seuls les clusters autorisés peuvent accéder aux backups.

Politiques de rétention et automatisation

La gestion de la rétention est un équilibre entre la profondeur d'historique souhaitée et l'espace de stockage disponible. PBS utilise un système de rétention GFS (Grandfather-Father-Son) flexible. L'automatisation via **des outils d'Infrastructure as Code** permet de maintenir la cohérence des politiques sur l'ensemble du parc.

```
# Politique de rétention recommandée pour environnement de production
# keep-last: 3 (3 dernières sauvegardes, quelle que soit la date)
# keep-daily: 7 (1 par jour sur 7 jours)
# keep-weekly: 4 (1 par semaine sur 4 semaines)
# keep-monthly: 6 (1 par mois sur 6 mois)
# keep-yearly: 2 (1 par an sur 2 ans)

# Application via API
proxmox-backup-manager datastore update backups \
  --keep-last 3 --keep-daily 7 --keep-weekly 4 --keep-monthly 6 --keep-yearly 2

# Planification des jobs de backup
# VMs critiques : 2x/jour
cat >> /etc/pve/jobs.cfg << 'EOF'
vzdump: daily-critical
  schedule 0 2,14 * * *
  storage pbs-main
  mode snapshot
  pool critical-vms
  compress zstd
  notes-template {{guestname}}-{{node}}
  mailnotification failure
  mailto admin@domain.com
EOF
```

Intégration avec solutions de sauvegarde entreprise

Veeam Backup & Replication pour Proxmox

Depuis la version 12.1, Veeam supporte officiellement Proxmox VE comme hyperviseur cible. L'intégration utilise l'API Proxmox pour orchestrer les snapshots et récupérer les données. Pour les environnements ayant déjà Veeam pour protéger des workloads VMware ou Hyper-V, cette intégration unifie la gestion des sauvegardes sous une console unique.

Nakivo Backup pour Proxmox

Nakivo propose une intégration mature avec Proxmox VE, supportant les backups agentless, la granular recovery, et le site recovery orchestration. L'avantage principal de Nakivo réside dans sa simplicité de déploiement (appliance virtuelle) et son modèle de licence par socket, souvent plus économique que Veeam pour les PME.

Fonctionnalité	PBS (natif)	Veeam 12.1+	Nakivo
Coût licence	Gratuit (open source)	Élevé (par workload)	Modéré (par socket)
Déduplication	Bloc (native)	Bloc (avancée)	Bloc (standard)
Réplication off-site	Sync PBS natif	WAN accelerator	Site recovery
Restore granulaire	Fichier (FUSE mount)	Application-aware	File-level recovery
Support LXC	Natif	Non	Non
API/Automation	REST API complète	PowerShell + REST	REST API
Monitoring	Basique (intégré)	Veeam ONE	Dashboard intégré

Monitoring et alerting des sauvegardes

Un backup qui échoue silencieusement est pire que l'absence de backup : il donne une fausse impression de sécurité. La supervision active des jobs de sauvegarde est non négociable. Pour les stratégies de monitoring avancées, consultez [notre cartographie des menaces 2026](#).

```
# Script de monitoring PBS pour Prometheus/Grafana
#!/bin/bash
# pbs_exporter.sh - À exécuter via cron toutes les 5 minutes

DATASTORE="backups"
API_TOKEN="PBSAPIToken=monitoring@pbs!monitor:xxxxxxx"

# Vérifier le dernier statut de chaque job
curl -sk "https://localhost:8007/api2/json/admin/datastore/$DATASTORE/snapshots" \
  -H "Authorization: $API_TOKEN" | jq '.data[] | {id: .["backup-id"], time: .["backup-time"], size: .size}'

# Alerter si aucun backup réussi dans les dernières 26h
LAST_BACKUP=$(curl -sk "https://localhost:8007/api2/json/status/tasks" \
  -H "Authorization: $API_TOKEN" | jq '[.data[] | select(.status == "OK")] | sort_by(.starttime) | last .starttime')

if [ "$((($(date +%s) - $LAST_BACKUP)) -gt 93600) ]; then
  echo "CRITICAL: Aucun backup réussi depuis plus de 26h" | mail -s "[PBS] Alerte backup"
  admin@domain.com
fi
```

Scénarios de Disaster Recovery

Perte d'un nœud unique dans un cluster

Lorsqu'un nœud Proxmox tombe en panne matérielle, les VMs configurées en HA sont automatiquement redémarrées sur les nœuds survivants. Les VMs non-HA doivent être restaurées manuellement depuis PBS. Le temps de reprise dépend de la taille des VMs et de la vitesse du réseau vers le PBS.

Perte totale du site primaire

Ce scénario nécessite un PBS distant (ou une réplication vers un cloud S3-compatible) et un site de reprise pré-provisionné. Le RTO typique est de 2 à 8 heures selon le volume de données et la bande passante disponible. Pour les environnements **soumis à NIS2**, ce scénario doit être testé au minimum une fois par trimestre.

```
# Procédure de DR - Restauration sur site secondaire
# 1. Vérifier l'accès au PBS distant
proxmox-backup-client list --repository backup@pbs-dr.site2.local:backups

# 2. Restaurer les VMs critiques en priorité (AD, DNS, DB)
for VMID in 100 101 102; do
    qmrestore pbs-dr:backup/vzdump-qemu-{$VMID}-latest.vma {$VMID} \
        --storage local-zfs --unique true
done

# 3. Ajuster le réseau pour le site DR
qm set 100 -net0 virtio,bridge=vibr0,tag=10
```

FAQ — Questions fréquentes

Quelle est la différence entre la déduplication PBS et la compression zstd ?

La déduplication opère au niveau des blocs identiques entre toutes les sauvegardes du datastore, éliminant les doublons avant stockage. La compression zstd réduit la taille de chaque bloc individuel après déduplication. Les deux mécanismes sont complémentaires : la déduplication réduit le nombre de blocs stockés, et zstd réduit la taille de chaque bloc unique. En pratique, la déduplication apporte un gain de 60 à 85%, et la compression un gain additionnel de 30 à 50% sur les blocs restants.

Peut-on restaurer un backup PBS si le serveur PBS est hors service ?

Non, les backups PBS sont stockés dans un format propriétaire qui nécessite le service PBS pour l'accès. C'est pourquoi la réplication vers un second PBS est indispensable. En alternative, vous pouvez exporter régulièrement les backups critiques au format VMA standard vers un stockage NFS ou S3 pour disposer d'une copie accessible sans PBS.

Comment tester la restauration sans impacter la production ?

PBS supporte la restauration vers un VMID différent avec l'option `--unique true` qui régénère les adresses MAC et les UUID. Restaurez dans un réseau isolé (VLAN dédié aux tests DR) pour valider l'intégrité des données sans risque de conflit IP ou de duplication de SID dans un domaine Active Directory. Automatisez ce test via un script cron mensuel et vérifiez le bon démarrage des services applicatifs post-restauration.

Quel est l'impact réseau d'un backup snapshot sur la VM en cours d'exécution ?

Le mode snapshot avec dirty bitmaps a un impact minimal sur la VM : une pause de 10 à 200 ms pour le freeze du système de fichiers (via guest-agent), puis un transfert réseau en arrière-plan qui consomme la bande passante configurée. Sur un réseau 10 Gbps dédié au backup, l'impact sur le réseau de production est nul. Sur un réseau partagé 1 Gbps, limitez la bande passante du job `vzdump` via le paramètre `--bwlimit` pour éviter la saturation.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr

© 2026 — Reproduction interdite sans autorisation.