AYI NEDJIMI Consultants

Proxmox Backup Server : Stratégie de Sauvegarde et

Catégorie : Virtualisation Lecture : 8 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet Proxmox Backup Server : architecture, déduplication, chiffrement côté client, snapshots incrémentaux, restauration granulaire.

Avertissement : Les techniques présentées dans cet article sont destinées exclusivement à des fins éducatives et de tests autorisés. Toute utilisation malveillante est illégale et contraire à l'éthique professionnelle.

2.1 Composants principaux

PBS repose sur une architecture client-serveur efficace, développée en **Rust** pour des performances maximales et une sécurité mémoire garantie par le compilateur. Les composants principaux sont :

- **proxmox-backup-server** : le démon principal qui expose l'API REST sur le port 8007 en HTTPS. Il gère l'authentification, les datastores, les tâches de vérification et la garbage collection
- **proxmox-backup-client** : l'outil en ligne de commande installé sur les nœuds Proxmox VE (ou tout serveur Linux). Il gère le chunking, la déduplication côté client, le chiffrement et le transfert des données
- **proxmox-backup-manager** : l'outil d'administration pour la configuration des datastores, la gestion des utilisateurs, les tâches planifiées et le monitoring
- **Web UI** : interface web complète basée sur ExtJS, accessible sur `https://<pbs-host>:8007`, offrant une vue d'ensemble des tâches, datastores et statistiques

2.2 Communication et protocole

Toute communication entre le client et le serveur se fait via **HTTPS (TLS 1.3)** sur le port 8007. Le protocole HTTP/2 est utilisé pour le multiplexage des flux, ce qui permet de transférer simultanément plusieurs chunks sans overhead de connexion TCP. L'authentification est gérée par des **API tokens** (recommandé pour l'automatisation) ou des comptes utilisateur PAM/PBS avec support TOTP pour le MFA.

Le flux de sauvegarde suit ce processus optimisé :

1. **Snapshot** : Proxmox VE crée un snapshot QEMU (pour les VMs) ou un snapshot ZFS/LVM (pour les conteneurs LXC)
2. **Chunking** : le client découpe les données en chunks de taille variable (64 KiB à 4 MiB) via l'algorithme de *content-defined chunking* (CDC)

3. **Déduplication** : chaque chunk est identifié par son hash SHA-256. Seuls les chunks nouveaux (non déjà présents sur le serveur) sont transférés
4. **Chiffrement (optionnel)** : si activé, chaque chunk est chiffré côté client avec AES-256-GCM avant le transfert
5. **Transfert** : les chunks sont envoyés via HTTPS/HTTP2 et écrits dans le datastore
6. **Manifest** : un fichier manifest signé répertorie tous les chunks composant cette sauvegarde, permettant une vérification d'intégrité

2.3 Prérequis matériels et dimensionnement

Le dimensionnement d'un serveur PBS dépend du volume de données à sauvegarder, du taux de changement quotidien (change rate) et de la profondeur de rétention souhaitée. Voici les recommandations basées sur notre expérience en production :

Composant	Minimum	Recommandé (prod)	Notes
CPU	4 cores	8-16 cores	SHA-NI accélère le hashing, AES-NI le chiffrement
RAM	4 GiB	16-32 GiB	~1 GiB par To de données dédupliquées pour le cache d'index
Stockage OS	32 GiB SSD	64 GiB SSD	ZFS mirror pour l'OS, RAID-1 minimum
Stockage Datastore	1 To HDD	RAID-Z2 / RAID-10	ZFS fortement recommandé pour l'intégrité (checksums)
Réseau	1 Gbps	10 Gbps	Réseau dédié backup recommandé

Attention au choix du filesystem
PBS est optimisé pour **ZFS** ou **ext4**. N'utilisez jamais XFS ou Btrfs comme filesystem pour un datastore PBS. ZFS est le choix idéal car il offre des checksums au niveau des blocs (protection contre le bit rot), la compression transparente (lz4/zstd), et les snapshots atomiques. Si vous utilisez ext4, vous perdez la protection contre la corruption silencieuse des données.

Notre avis d'expert
La microsegmentation réseau dans les environnements virtualisés offre un niveau de protection que les architectures physiques traditionnelles ne peuvent égaler. Encore faut-il la configurer correctement — ce qui, dans notre expérience, reste l'exception plutôt que la norme.

PBS implémente un modèle de contrôle d'accès basé sur les rôles (RBAC) avec des ACL hiérarchiques. Ce modèle est essentiel pour la sécurité, car il permet de respecter le **principe du moindre privilège** -- un concept fondamental aussi en sécurité Active Directory. Les rôles prédéfinis sont :

Rôle	Permissions	Usage recommandé
Admin	Toutes les permissions	Administrateurs PBS uniquement (limiter au strict minimum)
DatastoreAdmin	Gérer un datastore spécifique	Responsables de la sauvegarde par périmètre
DatastoreBackup	Créer des sauvegardes et lire les siennes	Comptes de service Proxmox VE (proxmox-backup-client)
DatastoreReader	Lecture seule sur les sauvegardes	Monitoring, audit, restauration par un tiers
DatastoreAudit	Voir les logs et statistiques	Équipe de supervision (SOC)

```
# Créer un utilisateur de service pour chaque nœud PVE
proxmox-backup-manager user create pve-node1@pbs \
    --comment "Service account for PVE Node 1"

# Assigner le rôle DatastoreBackup uniquement sur le datastore production
proxmox-backup-manager acl update /datastore/production \
    --auth-id pve-node1@pbs \
    --role DatastoreBackup

# Créer un API token pour l'automatisation (évite de stocker le mot de passe)
proxmox-backup-manager user generate-token pve-node1@pbs backup-token
```

Séparation des privilèges anti-ransomware
Le compte utilisé par les nœuds Proxmox VE pour envoyer les sauvegardes (**DatastoreBackup**) ne doit **jamais** avoir le droit de supprimer des sauvegardes existantes. Ainsi, même si un nœud PVE est compromis par un ransomware, l'attaquant ne peut pas purger les sauvegardes sur PBS. Seul le rôle **DatastoreAdmin** ou **Admin** peut supprimer des snapshots, et ces comptes ne doivent jamais être configurés sur les nœuds PVE.

Cas concret
L'attaque par évasion de VM VENOM (CVE-2015-3456) exploitant le contrôleur de disquette virtuel de QEMU a marqué un tournant dans la sécurité des hyperviseurs. Bien que corrigée, elle a prouvé que l'isolation entre machines virtuelles n'est jamais absolue et que les composants legacy de virtualisation sont des cibles potentielles.

En complément de la déduplication, PBS applique une **compression zstd (Zstandard)** à chaque chunk individuellement. Développé par Facebook/Meta, zstd offre un excellent compromis entre ratio de compression et performance. PBS supporte également lzo et aucun compression, mais zstd est le choix par défaut et recommandé.

```
# Backup avec compression zstd (niveau 1, rapide)
proxmox-backup-client backup \
    root.pxar:/ \
    --repository pbs.example.com:production \
    --compress zstd

# Vérification de l'espace utilisé par le datastore
proxmox-backup-manager datastore status production

# Exemple de sortie :
# Datastore: production
# Total: 10.0 TiB
# Used: 4.2 TiB (42%)
# Deduplication Factor: 5.83x
# Chunk Count: 14,235,892
# Compression Ratio: 1.65x
```

4.4 Garbage Collection

Lorsque des snapshots sont supprimés (via la politique de rétention), les chunks qui ne sont plus référencés par aucun snapshot deviennent orphelins. La **Garbage Collection (GC)** est le processus qui identifie et supprime ces chunks orphelins pour récupérer l'espace disque.

La GC fonctionne en deux phases :

1. **Phase 1 -- Mark** : parcourt tous les index de tous les snapshots et marque chaque chunk référencé comme "actif". Cette phase est read-only et safe
2. **Phase 2 -- Sweep** : supprime tous les chunks non marqués. Un chunk n'est supprimé que s'il est orphelin depuis au moins 24 heures (safety delay) pour éviter les race conditions avec des sauvegardes en cours

```
# Lancer la GC manuellement
proxmox-backup-manager garbage-collection start production

# Planifier la GC (recommandé : quotidien à 3h du matin)
proxmox-backup-manager garbage-collection scheduling update production \
    --schedule "daily 03:00"
```

Une question fréquente : le chiffrement côté client détruit-il les bénéfices de la déduplication ? La réponse courte est : **partiellement, mais c'est maîtrisé**.

PBS utilise une approche ingénieuse : la déduplication est basée sur le hash SHA-256 du contenu en clair (avant chiffrement), et le chiffrement est déterministe pour une même clé. Cela signifie que deux chunks identiques chiffrés avec la même clé produiront le même résultat, et la déduplication fonctionnera normalement **au sein d'un même utilisateur/clé**. En revanche, la déduplication cross-utilisateur est perdue si les utilisateurs utilisent des clés différentes -- ce qui est le comportement attendu en termes de sécurité.

Figure 2 -- Flux de chiffrement côté client dans Proxmox Backup Server

```
# Règles iptables / nftables sur le serveur PBS
# N'autoriser que les nœuds PVE connus sur le port 8007
nft add rule inet filter input ip saddr { 10.0.1.10, 10.0.1.11, 10.0.1.12 } tcp dport 8007
accept
nft add rule inet filter input ip saddr 10.0.2.0/24 tcp dport 8007 drop
nft add rule inet filter input tcp dport 8007 drop

# Accès admin PBS uniquement depuis un bastion / jump host
nft add rule inet filter input ip saddr 10.0.100.5 tcp dport { 8007, 22 } accept
```

Stratégie 3 : Copie air-gapped

La protection ultime contre le ransomware est la copie **air-gapped** : un support physiquement déconnecté du réseau. Avec PBS, cela peut prendre plusieurs formes :

- **Disques USB rotatifs** : brancher un disque USB, déclencher une synchronisation, débrancher et stocker dans un coffre-fort. Rotation sur 5-7 jours
- **NAS hors réseau** : un NAS connecté uniquement pendant la fenêtre de synchronisation, puis éteint et déconnecté
- **Tape LTO** : exportation des sauvegardes vers des bandes LTO via `proxmox-tape-backup` (intégré depuis PBS 2.x). Les bandes sont stockées hors site

Stratégie 4 : Snapshots ZFS immutables

Si le datastore PBS est hébergé sur ZFS, les **snapshots ZFS** offrent une couche d'immutabilité au niveau du filesystem. Un snapshot ZFS est read-only par nature et ne peut être supprimé que par l'administrateur root du serveur PBS :

```
# Créer des snapshots ZFS automatiques du datastore
# Script cron sur le serveur PBS
#!/bin/bash
DATASET="zfs-pool/production"
DATE=$(date +%Y-%m-%d_%H%M)
RETENTION_DAYS=30

# Créer le snapshot
zfs snapshot ${DATASET}@backup-${DATE}

# Supprimer les snapshots de plus de 30 jours
zfs list -t snapshot -o name -H ${DATASET} | while read snap; do
    SNAP_DATE=$(echo $snap | grep -oP '\d{4}-\d{2}-\d{2}')
    if [ $(( ($(date +%s) - $(date -d "$SNAP_DATE" +%s)) / 86400 )) -gt $RETENTION_DAYS ];
then
        zfs destroy $snap
    fi
done
```

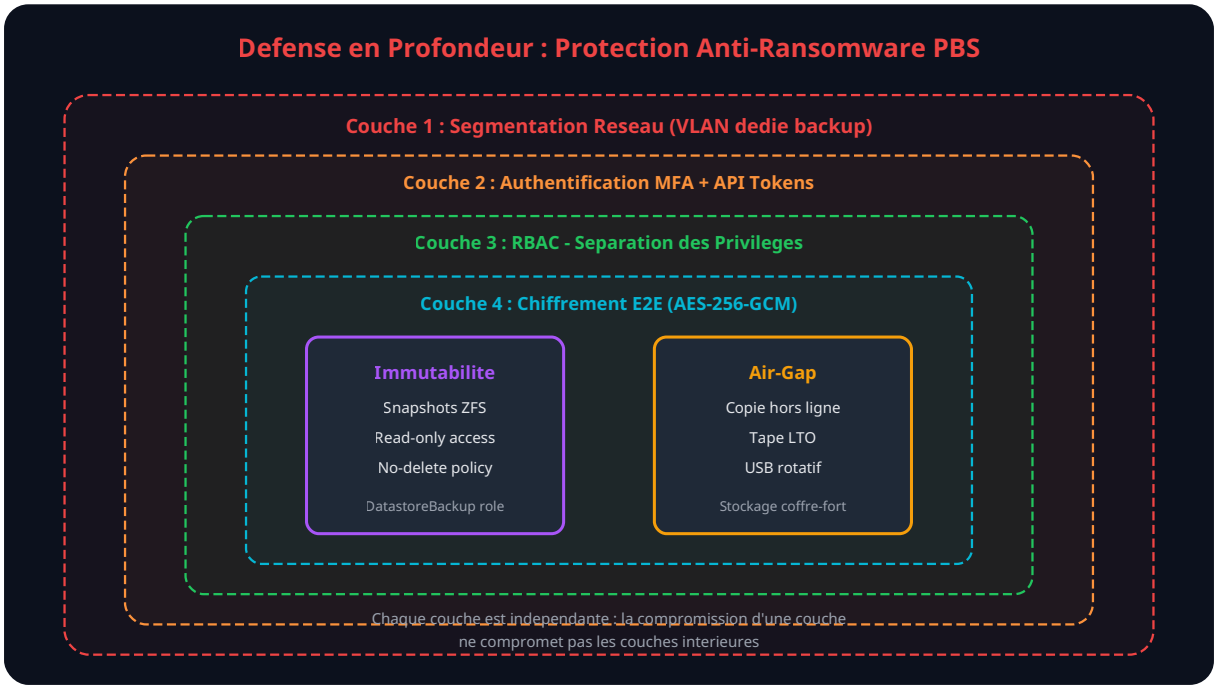

Figure 3 -- Défense en profondeur anti-ransomware pour Proxmox Backup Server

10.3 Durcissement du serveur PBS

Le serveur PBS lui-même doit être durci comme n'importe quelle infrastructure critique. Les mesures essentielles rejoignent les bonnes pratiques de durcissement des hyperviseurs :

- **Accès SSH restreint** : clés SSH uniquement, port non standard, fail2ban activé, accès uniquement depuis le bastion
- **Mises à jour automatiques de sécurité** : `unattended-upgrades` pour les patches de sécurité Debian
- **Pas de services inutiles** : PBS doit être une appliance dédiée, sans services web, sans agents tiers non nécessaires

- **Monitoring des accès** : centralisation des logs PBS vers un SIEM externe pour détecter toute activité suspecte
- **MFA sur l'interface web** : activation du TOTP (Google Authenticator / FreeOTP) pour tous les comptes administrateur

11. Monitoring et alerting

11.1 Notifications intégrées

PBS intègre un système de notification configurable qui peut alerter par email en cas d'événements importants. Les notifications sont essentielles pour détecter rapidement les problèmes avant qu'ils ne deviennent critiques :

```
# Configuration des notifications email
# /etc/proxmox-backup/notifications.cfg
sendmail: default
    mailto admin@example.com
    mailto-user root@pam
    from-address pbs@example.com
    comment "Notifications PBS"

# Types de notifications :
# - Sauvegarde échouée
# - Garbage Collection terminée (avec statistiques)
# - Vérification échouée (chunks corrompus)
# - Synchronisation remote échouée
# - Espace disque faible
```

11.2 Métriques et intégration Prometheus/Grafana

Pour un monitoring avancé, PBS expose des métriques via son API REST, ce qui permet l'intégration avec des solutions comme Prometheus + Grafana. Les métriques clés à surveiller pour un centre opérationnel de sécurité (SOC) :

- **Taux de réussite des sauvegardes** : objectif 100 %. Toute sauvegarde échouée doit générer une alerte immédiate
- **Durée des sauvegardes** : une augmentation soudaine peut indiquer un problème de performance réseau ou disque
- **Taux de déduplication** : une baisse soudaine peut indiquer un changement massif (mise à jour OS, migration, ou chiffrement par ransomware)
- **Espace disque** : alerte à 80 %, critique à 90 %. Prévoir la croissance sur 6 mois minimum
- **Intégrité des chunks** : résultats des jobs de vérification. Zéro erreur est la seule valeur acceptable
- **Statut de la synchronisation remote** : la copie offsite doit être à jour (delta < 24h)

```
# Récupérer les métriques via l'API PBS
# Status du datastore
curl -s -k -H "Authorization: PBSAPIToken=user@pbs!token:SECRET" \
    "https://pbs.example.com:8007/api2/json/admin/datastore/production/status" | jq

# Liste des tâches récentes
curl -s -k -H "Authorization: PBSAPIToken=user@pbs!token:SECRET" \
    "https://pbs.example.com:8007/api2/json/nodes/localhost/tasks?limit=50" | jq

# Métriques de déduplication
curl -s -k -H "Authorization: PBSAPIToken=user@pbs!token:SECRET" \
    "https://pbs.example.com:8007/api2/json/admin/datastore/production/status" | \
    jq '.data | {total: .total, used: .used, avail: .avail, dedup: .["dedup-factor"]}'
```

Pour approfondir ce sujet, consultez notre outil open-source container-security-scanner qui facilite l'audit de sécurité des conteneurs Docker et Kubernetes.

12. Checklist backup sécurisé

Voici la checklist complète pour une implémentation PBS sécurisée et résiliente. Utilisez-la comme référence lors de vos déploiements et audits :

Checklist Architecture & Installation

- PBS installé sur un serveur dédié (pas de colocation avec PVE)
- Système de fichiers ZFS pour les datastores (protection bit rot)
- RAID-Z2 minimum pour la tolérance aux pannes disque
- Réseau de sauvegarde dédié (VLAN séparé, 10 Gbps recommandé)
- PBS à jour avec les derniers patches de sécurité

Checklist Sécurité & Authentification

- MFA (TOTP) activé pour tous les comptes administrateur
- API tokens pour l'automatisation (pas de mots de passe en clair)
- RBAC strict : DatastoreBackup pour les nœuds PVE, pas d'Admin
- Accès SSH restreint (clés uniquement, bastion, fail2ban)
- Firewall configuré : seuls les nœuds PVE autorisés sur le port 8007
- Logs centralisés vers un SIEM externe

Checklist Chiffrement & Protection

- Chiffrement côté client activé (AES-256-GCM)
- Clé de chiffrement sauvegardée dans 3+ emplacements sécurisés
- Paper key générée et stockée dans un coffre-fort physique
- Snapshots ZFS sur le datastore pour immutabilité
- Copie air-gapped (tape LTO ou USB rotatif hors site)

Checklist Sauvegarde & Rétention

- Jobs de sauvegarde automatisés (mode snapshot + QEMU Guest Agent)
- Politiques de rétention configurées (keep-daily/weekly/monthly/yearly)
- Garbage collection planifiée quotidiennement

- Jobs de vérification d'intégrité (quotidien pour récent, hebdo pour tout)
- Synchronisation remote vers un PBS offsite fonctionnelle
- Notifications email configurées pour échecs et alertes

Checklist Tests & Documentation

- Tests de restauration de fichiers : hebdomadaires
- Tests de restauration de VM : mensuels
- Test DR complet depuis le site distant : trimestriel
- Test de validité des clés de chiffrement : semestriel
- Documentation PRA à jour avec procédures pas à pas
- Procédure de récupération de la clé de chiffrement documentée

Sources et références : Proxmox VE Wiki · ANSSI

Questions frequentes

Comment mettre en place Proxmox Backup Server dans un environnement de production ?

La mise en place de Proxmox Backup Server en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Quel hyperviseur choisir pour un environnement de production sécurisé avec Proxmox Backup Server : Stratégie de Sauvegarde ?

Le choix dépend de votre budget et de vos compétences. Proxmox VE est open source et gratuit, VMware offre un écosystème mature, Hyper-V s'intègre nativement à Windows Server.

Comment sécuriser l'accès à l'interface d'administration pour Proxmox Backup Server : Stratégie de Sauvegarde ?

Placez l'interface de gestion sur un VLAN dédié, activez le 2FA, utilisez des certificats TLS valides et limitez l'accès par IP source. Ne laissez jamais l'interface exposée sur Internet.

Articles connexes

Virtualisation
Proxmox vs VMware vs Hyper-V : Comparatif Sécurité
Analyse comparative des hyperviseurs
Virtualisation
Durcissement VMware ESXi : Guide de Sécurisation
Hardening complet des hyperviseurs ESXi
Active Directory
Sécurisation Active Directory

Guides de sécurisation et bonnes pratiques AD
Cloud Security
Sécurité Cloud
Protégez vos infrastructures cloud
Techniques Hacking
Articles Techniques de Hacking
Comprendre les techniques offensives
Conformité
Conformité et Réglementation
NIS2, ISO 27001, RGPD

Références et ressources externes

- Documentation officielle Proxmox Backup Server -- Guide complet d'administration PBS
- Proxmox Backup Server -- Site officiel -- Téléchargement et informations produit
- Forum communautaire Proxmox PBS -- Support communautaire et retours d'expérience
- ANSSI -- Recommandations relatives aux sauvegardes -- Guide ANSSI sur les bonnes pratiques de sauvegarde
- MITRE ATT&CK T1490 -- Inhibit System Recovery -- Techniques de destruction des sauvegardes par les ransomwares

> Points clés à retenir
>
> - 11. Monitoring et alerting
> - 12. Checklist backup sécurisé
> - Questions frequentes

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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