Fiche de procédure

Sauvegarder un NAS Synology vers OVHcloud S3 avec Hyper Backup

Document de synthèse pour Wiki.js / PROCYB — basé sur la configuration mise en place dans le homelab.

Objectif	Mettre en place une sauvegarde distante chiffrée du NAS Synology vers OVHcloud Object Storage S3.
Source	NAS Synology principal
Destination	Bucket S3 OVHcloud **backup-synology-home** — région Gravelines (GRA)
Outil	Hyper Backup

1. Paramètres OVHcloud

Projet	Projet 2026-11-02
Bucket	backup-synology-home
Service	Object Storage compatible S3
Région	Gravelines (GRA)
Endpoint	s3.gra.io.cloud.ovh.net
Déploiement	1-AZ
Versioning S3	Désactivé
Object Lock	Désactivé
Chiffrement serveur	SSE-OMK activé
Compte technique	PROCYBNAS

2. Configuration Hyper Backup

Nom de la tâche	OVHcloud-Synology
Serveur S3	URL de serveur personnalisé
Adresse du serveur	s3.gra.io.cloud.ovh.net
Signature	v4
Type de requête	Hébergement virtuel
Région S3	gra
Bucket	backup-synology-home
Répertoire	HyperBackup
Dossiers	CLOUD FAMILLE, PROJET PROCYB, homes, photo
Compression	Activée
Planification	Quotidienne à 22h00
Vérification d'intégrité	Hebdomadaire (samedi 17h30, à confirmer)
Rotation	Smart Recycle
Versions	30 versions recommandées / à confirmer

3. Étapes de la procédure

1. Créer un projet Public Cloud dans OVHcloud.
2. Créer un bucket Object Storage compatible S3 en 1-AZ dans la région Gravelines (GRA).
3. Créer un utilisateur S3 dédié et enregistrer l'Access Key et la Secret Key dans un gestionnaire de mots de passe.
4. Dans Hyper Backup, créer une nouvelle tâche de sauvegarde de type S3 Storage.
5. Saisir le serveur personnalisé, l'endpoint, la signature v4, la région gra et le bucket backup-synology-home.
6. Sélectionner les dossiers à sauvegarder : CLOUD FAMILLE, PROJET PROCYB, homes et photo.
7. Activer la compression, la planification, la vérification d'intégrité et le chiffrement côté client.
8. Choisir une politique de rotation Smart Recycle et une limite de 30 versions.
9. Lancer la première sauvegarde complète.
10. Contrôler le succès de la tâche, puis effectuer un test de restauration.

4. Sécurité et bonnes pratiques

- Conserver la clé privée Hyper Backup (.pem) et le mot de passe de chiffrement dans un emplacement sûr, distinct du NAS.
- Ne jamais publier les clés S3 ou les mots de passe dans Wiki.js ou sur le site public.
- Conserver Synology C2 tant que la première sauvegarde OVHcloud et le test de restauration ne sont pas validés.
- Ne pas configurer de règle Lifecycle OVHcloud qui supprimerait automatiquement les objets du dépôt Hyper Backup.
- Surveiller l'espace réellement consommé dans OVHcloud pour estimer le coût mensuel réel.

5. Contrôles après déploiement

Élément à vérifier	Statut
Première sauvegarde complète	À confirmer
Limite de 30 versions	À confirmer
Vérification d'intégrité	À confirmer
Test de restauration	À effectuer
Volume stocké OVHcloud	À relever
Coût mensuel observé	À estimer
Décision sur Synology C2	Après validation

Références : documentation Synology Hyper Backup, documentation OVHcloud Object Storage S3.