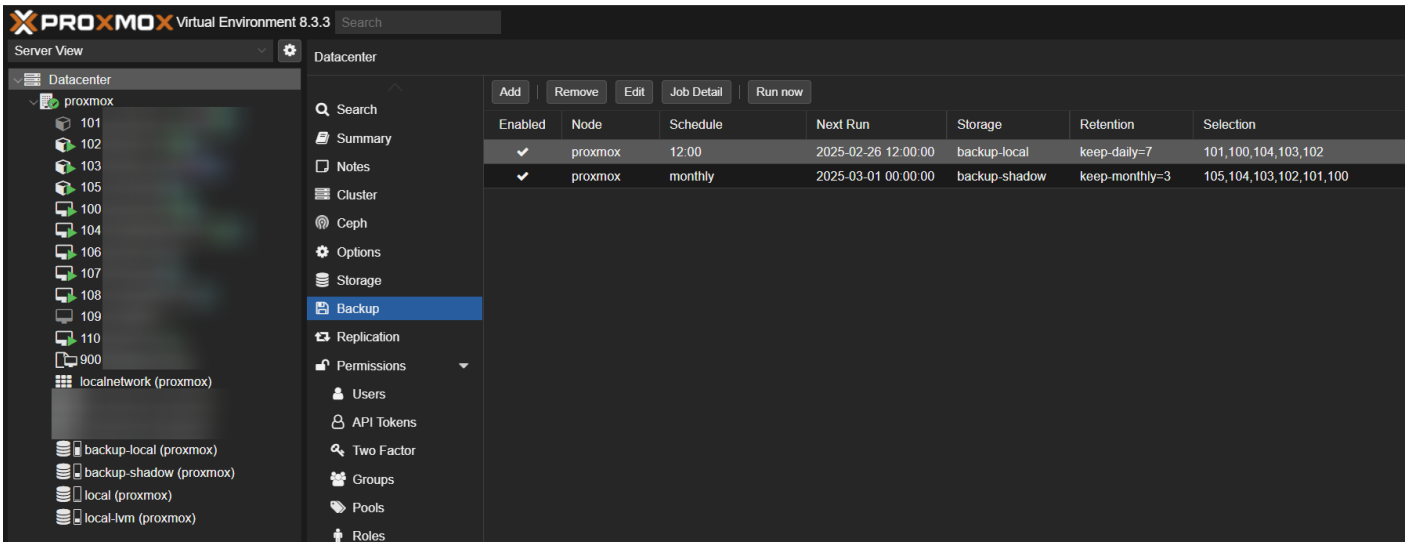
Méthode de sauvegarde

Méthode 3-2-1

La méthode de sauvegarde que j'utilise est basée sur le principe 3-2-1, qui est considéré comme une bonne pratique en matière de sauvegarde des données. J'ai 3 copies de mes données, stockées sur 2 types de supports différents, avec 1 copie hors site.

Ma méthode de sauvegarde :

1. **Sauvegardes quotidiennes :**
   - Les sauvegardes des serveurs, VM/VPS et configurations sont effectuées quotidiennement par l'utilisateur root.
   - Ces sauvegardes sont conservées pendant 7 jours.
   - Elles sont transférées sur le NAS et stockées à la fois sur la machine source et le NAS, puis synchronisées sur Scaleway.
2. **Sauvegardes mensuelles :**
   - Les sauvegardes des serveurs et VM/VPS sont effectuées le premier jour de chaque mois.
   - Ces sauvegardes sont conservées pendant 3 mois.
   - Elles sont directement stockées sur le NAS ou transférées après leur création, puis synchronisées sur Scaleway.
3. **Sauvegardes manuelles :**
   - Deux copies des sauvegardes des serveurs, des dossiers personnels (photos/vidéos) et des VM/VPS sont effectuées manuellement tous les trois ou six mois.
   - Ces sauvegardes sont stockées sur un ou deux disques durs externes, qui sont connectés uniquement pour le transfert.
4. **Sauvegarde Proxmox :**
   - Sur Proxmox, j'utilise l'interface graphique pour effectuer des sauvegardes quotidiennes des VMs et des conteneurs. Ces sauvegardes sont conservées pendant 7 jours sur le stockage local de Proxmox.
   - Les sauvegardes mensuelles sont ensuite transférées directement sur le NAS avec le point de montage NFS.



Vous pouvez trouver plus d'informations sur la [sauvegarde Proxmox dans la documentation officielle](#).

Synchronisation des fichiers personnels

Mes photos, vidéos, clés SSH, sauvegardes de jeux, documents personnels et gestionnaire de mots de passe sont synchronisés sur mon ordinateur portable, mon téléphone et mon PC fixe. Cela signifie que j'ai à tout moment ces fichiers synchronisés avec **Syncthing**. Sur Proxmox, j'ai un serveur Syncthing qui est lui-même sauvegardé selon les méthodes 1, 2 et 3 mentionnées précédemment.

Transfert des sauvegardes avec rclone

Pour le transfert des sauvegardes, j'utilise l'outil en ligne de commande **rclone**. Rclone est compatible avec de nombreux services de stockage tels que SFTP, Google Drive, Dropbox, Amazon S3, Scaleway, Proton Drive et bien d'autres. Cela me permet de gérer facilement les différents stockages et de synchroniser les données de manière efficace.

Chiffrement des sauvegardes avec rclone

Rclone offre une fonctionnalité de chiffrement intégrée appelée "crypt", qui me permet de chiffrer les fichiers uniquement sur le stockage distant (Scaleway, dans notre cas), sans avoir à les chiffrer localement. Ainsi, mes données sont sécurisées sur le service de stockage, mais restent lisibles sur mon système local. Lorsque je souhaite accéder à ces sauvegardes, je les déchiffre et les

télécharge en utilisant rclone avec ce fichier de configuration.

Tester les sauvegardes

Il est essentiel de tester régulièrement la restauration de vos sauvegardes pour vous assurer qu'elles sont fonctionnelles et que vous pouvez bien récupérer vos données en cas de besoin. Cela vous permettra d'identifier d'éventuels problèmes et de prendre les mesures correctives nécessaires.

Je recommande de tester la restauration de vos sauvegardes au moins une fois par trimestre. Choisissez des fichiers ou des données représentatifs, restaurez-les et vérifiez qu'ils sont bien récupérés et utilisables. Cette étape est cruciale pour garantir la fiabilité de votre système de sauvegarde.

Sécurité des transferts

Pour sécuriser les transferts de sauvegardes vers le NAS, il est important d'ouvrir les ports nécessaires sur le pare-feu et de mettre en place une liste blanche des adresses IP autorisées à se connecter. De plus, il est recommandé de créer un utilisateur dédié pour chaque machine qui a les droits d'accès spécifiques à son dossier de sauvegarde sur le NAS.

Cela permet de limiter les risques d'accès non autorisés et de garantir la confidentialité des données sauvegardées. Il est également important de s'assurer que les communications entre les machines et le NAS soient chiffrées (SSH, SFTP, etc.).

Stockage externe

Kdrive ou Swiss Backup

Il existe également la solution Kdrive ou Swiss Backup que vous pouvez utiliser. Il est possible de monter le disque sur votre ordinateur via le protocole WebDAV ou avec Rclone. Il faut découper les fichiers en blocs de moins de 50 gigaoctets avec Rclone, puis ces blocs seront automatiquement reconstitués lors du téléchargement.

Scaleway Cold Storage

Pour le stockage externe à long terme, j'utilise le service de stockage froid (Cold Storage) de Scaleway. Mes données sont stockées dans un abri sous-terrain sécurisé à un coût très abordable

de 0,002 € par gigaoctet et par mois. Cela me permet de conserver des copies de mes sauvegardes les plus importantes à un faible coût tout en bénéficiant d'un stockage sécurisé et durable.

Exemple de script Bash pour sauvegarder des dossiers

Voici un exemple de script Bash qui permet de sauvegarder des dossiers de manière automatique. Vous pouvez commenter avec `#` ce qui ne vous convient pas :

```
#!/bin/bash

# Description
# Ce script effectue une sauvegarde quotidienne des dossiers spécifiés.
# Les sauvegardes sont conservées pendant 7 jours et transférées sur le NAS.
# Le script est exécuté via une tâche cron tous les jours à 2h du matin.

# Dossiers à sauvegarder
BACKUP_DIRS=("/home/user/documents" "/home/user/photos" "/etc/config")

# Destination des sauvegardes
BACKUP_DEST="/mnt/nas/backups"

# Nombre de jours de conservation
RETENTION_DAYS=7

# Exécution de la sauvegarde
for dir in "${BACKUP_DIRS[@]}"; do
    filename="$(basename "$dir")_$(date +%Y-%m-%d).tar.gz"
    tar -czf "$BACKUP_DEST/$filename" "$dir"

    # Création du fichier de checksum SHA-256
    sha256sum "$BACKUP_DEST/$filename" > "$BACKUP_DEST/$filename.sha256"
done

# Suppression des sauvegardes obsolètes
find "$BACKUP_DEST" -type f -mtime +$RETENTION_DAYS -delete
```

```
# Synchronisation des sauvegardes sur Scaleway
rclone sync "$BACKUP_DEST" remote:backups

# Fin du script
echo "Sauvegarde terminée."

# Pour vérifier le checksum d'un fichier de sauvegarde, utilisez la commande suivante :
# sha256sum -c "$BACKUP_DEST/nom_du_fichier.tar.gz.sha256"
# Remplacez "nom_du_fichier" par le nom de votre fichier de sauvegarde.
```

Sans compression/suppression/syncronisation :

```
#!/bin/bash

# Description
# Ce script effectue une sauvegarde des dossiers spécifiés.

# Dossiers à sauvegarder
BACKUP_DIRS=("/home/user/documents" "/home/user/photos" "/etc/config")

# Destination des sauvegardes
BACKUP_DEST="/mnt/nas/backups"

# Exécution de la sauvegarde
for dir in "${BACKUP_DIRS[@]}"; do
    filename="$(basename "$dir")_$(date +%Y-%m-%d).tar"
    tar -cf "$BACKUP_DEST/$filename" "$dir"

    # Création du fichier de checksum SHA-256
    sha256sum "$BACKUP_DEST/$filename" > "$BACKUP_DEST/$filename.sha256"
done

# Fin du script
echo "Sauvegarde terminée."

# Pour vérifier le checksum d'un fichier de sauvegarde, utilisez la commande suivante :
# sha256sum -c "$BACKUP_DEST/nom_du_fichier.tar.sha256"
# Remplacez "nom_du_fichier" par le nom de votre fichier de sauvegarde.
```

Utilisation avec Crontab : Pour exécuter ce script automatiquement tous les jours à 2h du matin, ajoutez la ligne suivante à votre fichier Crontab (crontab -e) :

```
0 2 * * * /chemin/vers/votre/script.sh
```

Cela permettra d'effectuer les sauvegardes quotidiennes de manière régulière.

Exemple de crontab avec Rclone

Voici un exemple de script crontab qui permet de transférer les sauvegardes vers Scaleway de mes sauvegardes Proxmox :

```
0 2 * * * rclone sync /mnt/backupHDD/dump crypt_scaleway_sauvegarde_proxmox:/1semaines --verbose --log-file=/mnt/backupHDD/rclone_sauvegarde_proxmox.txt
0 3 1 * * rclone sync /mnt/pve/backup-shadow/dump crypt_scaleway_sauvegarde_proxmox:/3mois --verbose --log-file=/mnt/pve/backup-shadow//rclone_sauvegarde_proxmox.txt
```

Fichier de configuration rclone

Rclone offre une fonctionnalité de chiffrement intégrée appelée "crypt", qui me permet de chiffrer les fichiers uniquement sur le stockage distant (Scaleway, dans notre cas), sans avoir à les chiffrer localement. Ainsi, mes données sont sécurisées sur le service de stockage, mais restent lisibles sur mon système local. Lorsque je souhaite accéder à ces sauvegardes, je les déchiffre et les télécharge en utilisant rclone avec ce fichier de configuration.

Rclone se charge de générer les mots de passe nécessaires au chiffrement et au déchiffrement des données lors de la configuration du remote "crypt". Vous pouvez alors sauvegarder ce fichier de configuration rclone.conf et le transférer sur d'autres machines si nécessaire, afin d'accéder à vos sauvegardes chiffrées depuis différents endroits.

Le fichier de configuration rclone.conf est généralement placé dans l'un des emplacements suivants :

- Sur Linux/Unix : `~/.config/rclone/rclone.conf` (répertoire personnel de l'utilisateur)
- Sur Windows : `%USERPROFILE%\.config\rclone\rclone.conf` (répertoire personnel de l'utilisateur)
- Sur macOS : `~/Library/Application Support/rclone/rclone.conf` (répertoire personnel de l'utilisateur)

Vous pouvez également le placer à un emplacement de votre choix, mais vous devrez alors spécifier le chemin complet lors de l'utilisation de rclone.

Les principaux paramètres à configurer sont :

- `access_key_id` et `secret_access_key` : à remplacer par vos propres identifiants Scaleway.

- `region = fr-par` : région de stockage en France.
- `storage_class = GLACIER` : utilisation du stockage froid Glacier.
- `password` et `password2` : à remplacer par vos propres mots de passe forts pour le chiffrement.

Lorsque je souhaite accéder à ces sauvegardes, je les déchiffre et les télécharge en utilisant rclone avec ce fichier de configuration.

Exemple de commande pour télécharger les sauvegardes chiffrées

```
rclone ls crypt_scaleway:backups
rclone cat crypt_scaleway:backups/filename.tar.gz | tar xzf -
```

Explications :

1. `rclone ls crypt_scaleway:backups` : Cette commande liste le contenu du dossier "backups" sur le remote "crypt_scaleway". Cela vous permet de voir quels fichiers sont présents.
2. `rclone cat crypt_scaleway:backups/filename.tar.gz | tar xzf -` : Cette commande télécharge le fichier "filename.tar.gz" depuis le dossier "backups" du remote "crypt_scaleway", le déchiffre automatiquement, puis l'extrait dans le répertoire courant.

Le remote "crypt_scaleway" fait référence à la section `[crypt]` de votre fichier de configuration rclone. Il permet d'accéder aux fichiers chiffrés sur le stockage Scaleway.

Assurez-vous d'avoir correctement configuré les paramètres de chiffrement (mot de passe, etc.) dans votre fichier de configuration rclone.conf avant d'exécuter ces commandes.

Passage de la classe de stockage Glacier vers Standard

Lorsque vous avez des fichiers stockés dans la classe de stockage Glacier de Scaleway, vous pouvez changer leur classe de stockage individuellement via la console Scaleway. Cependant, si vous avez de nombreux fichiers à restaurer, cette méthode peut s'avérer fastidieuse.

Les scripts ci-dessous vous permettent de gérer de manière automatisée le passage de la classe Glacier vers la classe Standard pour l'ensemble des fichiers dans un ou plusieurs dossiers. Avant d'utiliser ces scripts, vous devez configurer l'AWS CLI pour accéder à votre compte Scaleway, en suivant la documentation officielle.

Vous pouvez télécharger les scripts ci-joint.

Liste des objets stockés en Glacier

Le script `list-glacier-objects.sh` vous permet de lister tous les objets stockés dans la classe Glacier d'un bucket Scaleway spécifique, avec la possibilité de filtrer par répertoire.

```
./list-glacier-objects.sh my-bucket my-directory
```

Cela générera un fichier texte contenant la liste des objets à restaurer.

Restauration des objets Glacier

Le script `update_class_standard.sh` lit la liste des objets générée précédemment et initie la restauration de ces objets depuis Glacier vers la classe de stockage Standard. Il vérifie au préalable que l'objet est bien encore en Glacier et qu'aucune restauration n'est en cours.

```
./update_class_standard.sh my-bucket object-list.txt 3
```

Cela restaurera les objets pendant 3 jours dans la classe Standard.

Liste des fichiers restaurés

Enfin, le script `list-file-bucket.sh` vous permet de lister tous les objets d'un bucket Scaleway, y compris ceux qui ont été restaurés depuis Glacier.

```
./list-file-bucket.sh my-bucket my-directory
```

Cela vous permet de vérifier que la restauration s'est bien déroulée.

Pour réaliser les scripts, je me suis basé sur la documentation officielle de Scaleway.

Révision #4
Créé 2025-04-21 22:44:21 CEST par Philippe Favre
Mis à jour 2025-04-22 01:43:41 CEST par Philippe Favre