Teo BASOL
BTS SIO 2

Migration Chiffrée avec Rclone

I. Contexte

Ce document détaille la mise en œuvre de l'outil Rclone pour réaliser une migration de données sécurisée par chiffrement depuis un serveur NAS vers un espace Google Drive partagé. Cette démarche répond au besoin de transférer des données vers le cloud tout en garantissant leur confidentialité grâce au chiffrement, et d'automatiser ce processus pour assurer des sauvegardes régulières.

II. Prérequis

- Installation de l'outil Rclone sur le poste réalisant la migration.
- Accès réseau au serveur NAS source.
- Un compte Google avec accès au Drive partagé cible.
- Connexion Internet pour la configuration et la synchronisation.

III. Démarche et Structure de la Mise en Place

A. Installation et Configuration Initiale

- Téléchargement de la version appropriée de Rclone depuis le site officiel.
- Extraction et placement des fichiers Rclone dans un dossier système (ex: C:\rclone).
- Lancement de la configuration interactive via la commande rclone config.

B. Création des "Remotes"

- Remote Google Drive Non-Chiffré :
    - Création d'un nouveau "remote".
    - Sélection du type "Google Drive".
    - Configuration de l'ID client et du secret.

    - Choix de la portée d'accès (scope), typiquement "Full access".
    - Authentification via navigateur web pour lier le compte Google.
    - Configuration spécifique pour utiliser un Drive Partagé.
- Remote Chiffré (Crypt) :
    - Création d'un nouveau remote.
    - Sélection du type "Encrypt/Decrypt a remote".
    - Indication du remote Google Drive précédemment créé comme base à chiffrer.
    - Choix du mode de chiffrement pour les noms de fichiers et de dossiers.
    - Définition de mots de passe forts pour le chiffrement.

C. Commandes de Base et Synchronisation

- Création de dossiers : rclone mkdir nom_remote:chemin/dossier.
- Synchronisation : rclone sync source:chemin destination:chemin.
    - Utilisation de flags utiles : -P (progression), -v (verbose/détails), --backup-dir remote:chemin_backup (sauvegarde des fichiers écrasés/supprimés), --log-file chemin/log.txt (fichier log), --log-level LEVEL (niveau de log).
- Liste de fichiers/dossiers : rclone lsf remote:chemin (fichiers) ou rclone lsd remote:chemin (dossiers).

D. Automatisation (Script Batch)

- Création d'un script Windows Batch pour automatiser la synchronisation.
- Utilisation de commandes for pour récupérer la date et l'heure actuelles.
- Intégration de ces variables dans le chemin du --backup-dir pour créer des sauvegardes datées.
- Exécution de la commande rclone sync avec les chemins source/destination (utilisant le remote chiffré) et les options de log/backup.
- Planification de l'exécution du script via le Planificateur de tâches Windows.

E. Interface Graphique Web (Optionnel)

- Lancement d'une interface web locale pour gérer Rclone via la commande rclone rcd --rc-web-gui.

- Permet de visualiser les remotes, la bande passante, de créer/gérer les configurations et d'explorer les remotes.

IV. Remarques Techniques

- Sécurité : La gestion des mots de passe du remote chiffré est cruciale. Ils doivent être stockés en lieu sûr. Le chiffrement s'applique aux données sur le cloud ; elles sont déchiffrées lors de l'accès via le remote "crypt".
- Gestion des Comptes : Prévoir une procédure en cas de perte d'accès au compte Google associé au remote (recréation de la configuration Rclone, relier le nouveau compte, etc.).
- Chemins et Flags : Bien vérifier les chemins source et destination. Utiliser les flags (-P, -v, --backup-dir, etc.) pour contrôler et surveiller les opérations.
- Tests : Il est essentiel d'effectuer des tests réguliers de synchronisation et surtout de récupération des données depuis le Drive pour s'assurer du bon fonctionnement du chiffrement et du processus de sauvegarde.
- Comptes de Service : Pour éviter l'authentification interactive liée à un utilisateur spécifique, Rclone supporte l'utilisation de Comptes de Service Google Cloud, ce qui est recommandé pour les automatisations serveur.

Retour d'expérience : Rclone s'avère très pratique pour synchroniser des données qui évoluent peu (type archives). Pour des données modifiées très fréquemment, les limites intrinsèques de Google Drive (notamment le nombre maximal d'items dans un Drive partagé et les limitations d'API lors de modifications massives et rapides) peuvent rendre son utilisation moins adaptée que pour des archives statiques.

V. Évolutions Possibles

- Mise en place de monitoring plus avancé des tâches de synchronisation.
- Utilisation de Comptes de Service pour une meilleure intégration serveur.
- Explorer d'autres commandes Rclone (ex: check, copy, move, mount).
- Intégration avec d'autres systèmes de scripting ou d'orchestration.

VI. Bilan

La mise en place de Rclone a permis une migration réussie et sécurisée des données du NAS vers Google Drive Partagé. L'outil offre une grande flexibilité

pour la synchronisation et le chiffrement, et le processus automatisé assure des sauvegardes régulières. Cependant, il est crucial de prendre en compte les limitations inhérentes aux Drives Partagés Google (nombre d'objets, quotas API) qui peuvent affecter les performances ou la faisabilité pour des jeux de données très volumineux ou extrêmement dynamiques, comme souligné dans les remarques techniques. Un suivi et des tests périodiques restent recommandés pour garantir la pérennité de la solution. Les capacités de stockage utilisées montrent l'ampleur des données gérées.