BTS SIO — Option SISR

PROJET

Mise en œuvre d'une stratégie de sauvegarde 3-2-1

avec Duplicati, Google Drive, Mega et Rclone

Sasiraj GUNARATNARAJAH

Étudiant BTS SIO SISR — 2e année

CNED / F2I — Saint-Gobain Digital & IT

Session 2026

Sommaire

1. Contexte et objectifs du projet

1.1 Contexte

Dans le cadre de la préparation de l'épreuve E5 du BTS SIO option SISR, j'ai mis en place une stratégie de sauvegarde complète destinée à protéger un ensemble de données personnelles critiques : documents de cours, fiches de révision, dossiers des projets E6 (Projet 1 — Active Directory / pfSense / DFS, Projet 2 — GLPI sur Debian) et captures d'écran du portfolio.

La perte de ces données, à quelques semaines des examens finaux, constituerait un préjudice majeur : retard de révisions, perte de travail de plusieurs mois pour les projets professionnels, impossibilité de présenter les dossiers à l'oral. Il est donc indispensable de disposer d'une solution de sauvegarde fiable, automatisée, chiffrée et testée.

1.2 Objectifs

- Protéger les données contre les pannes matérielles (défaillance du SSD, panne du PC).
- Protéger les données contre les erreurs humaines (suppression accidentelle, écrasement involontaire).
- Protéger les données contre les sinistres locaux (incendie, vol, inondation) via une copie hors site.
- Protéger les données contre les ransomwares via le chiffrement et la diversification des supports.
- Automatiser entièrement le processus pour garantir une exécution régulière sans intervention manuelle.
- Valider la procédure par des tests de restauration documentés.

1.3 Indicateurs de performance cibles

Indicateur	Valeur cible
RPO (Recovery Point Objective)	24 heures — une sauvegarde quotidienne est suffisante
RTO (Recovery Time Objective)	Inférieur à 1 heure pour restaurer l'intégralité des données
Rétention	GFS (Grandfather-Father-Son) : 7 jours / 4 semaines / 12 mois
Intégrité	Test de restauration obligatoire et documenté pour chaque outil

2. Principe de la stratégie 3-2-1

La stratégie de sauvegarde 3-2-1 est une méthode éprouvée et reconnue comme standard dans l'industrie. Elle se décompose en trois règles simples :

- **3 copies** des données (l'original + deux sauvegardes distinctes)
- **2 supports** de stockage de types différents
- **1 copie hors site** (externalisée géographiquement du site principal)

Cette règle garantit qu'en cas de défaillance d'un support ou d'un sinistre local, il reste toujours au minimum une copie exploitable des données. C'est le socle de toute politique de protection des données en entreprise.

> **À RETENIR — Principe clé**
>
> Une seule copie = aucune sauvegarde. Deux copies sur le même support = risque élevé. Trois copies dont une hors site = sécurité maximale. Ce principe doit s'accompagner d'une politique de chiffrement et de tests de restauration réguliers pour être pleinement efficace.

3. Architecture retenue

Pour ce projet, j'ai mis en œuvre l'architecture suivante :

Copie	Emplacement	Rôle
Copie 1 (original)	SSD local — C:\Donnees_BTS\	Données de travail quotidiennes, accès rapide
Copie 2 (sauvegarde)	Google Drive via Duplicati	Sauvegarde chiffrée AES-256 avec historique de versions
Copie 3 (miroir hors site)	Mega.nz via Rclone	Synchronisation miroir brute, redondance fournisseur

3.1 Conformité à la règle 3-2-1

- **3 copies :** original + Google Drive + Mega ✓
- **2 supports différents :** SSD local + stockage cloud ✓
- **1 copie hors site :** les deux clouds sont externalisés ✓

> **À RETENIR — Choix assumé — Diversification des fournisseurs cloud**
>
> J'ai choisi d'utiliser deux fournisseurs cloud distincts (Google et Mega) plutôt qu'un seul cloud associé à un support physique. Cette décision apporte une redondance géographique et juridique : si un fournisseur subit une panne, ferme mon compte ou est victime d'une attaque, l'autre prend le relais. En environnement professionnel, j'ajouterais une bande magnétique LTO ou un disque externe déconnecté pour garantir un véritable air gap contre les ransomwares.

4. Choix technologiques

4.1 Duplicati

Duplicati est un logiciel open-source de sauvegarde multiplateforme. Il a été retenu pour les raisons suivantes :

- Sauvegarde incrémentielle : seules les modifications sont transférées après la première exécution.
- Chiffrement AES-256 côté client : les fichiers sont chiffrés sur le poste avant d'être envoyés au cloud.
- Déduplication : les blocs identiques ne sont pas stockés plusieurs fois, ce qui économise de l'espace.
- Interface web intuitive : la configuration se fait via le navigateur, simple à prendre en main.
- Gratuit, open-source et maintenu activement par la communauté.

4.2 Rclone

Rclone est un outil en ligne de commande compatible avec plus de 70 fournisseurs cloud. Il a été retenu pour :

- Support natif de nombreux services (Google Drive, Mega, Dropbox, S3, Backblaze, WebDAV, etc.).
- Synchronisation miroir rapide et fiable (commande rclone sync).
- Scripting simple : intégration facile dans des fichiers .bat Windows ou des scripts shell.
- Gestion avancée des logs pour la traçabilité.
- Gratuit, open-source et maintenu activement.

4.3 Complémentarité des deux outils

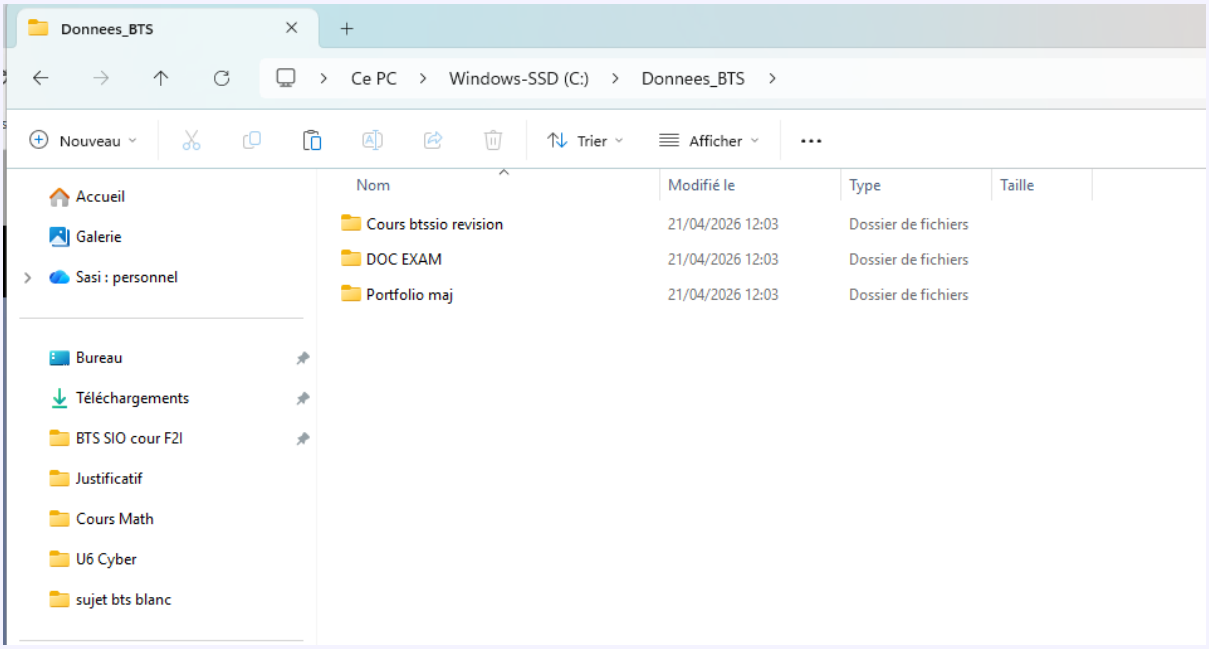
Duplicati et Rclone n'ont pas exactement la même fonction : Duplicati est un outil de sauvegarde (chiffrement, déduplication, historique), tandis que Rclone est un outil de synchronisation (miroir brut, rapide). Les combiner dans la stratégie 3-2-1 permet de profiter des avantages de chacun.

Critère	Duplicati	Rclone
Type	Sauvegarde	Synchronisation
Chiffrement	AES-256 côté client	Aucun (serveur selon cloud)
Historique	Oui (versions multiples)	Non (miroir écrasé)
Déduplication	Oui	Non
Interface	Web (GUI)	Ligne de commande
Visibilité fichiers	Fichiers chiffrés illisibles (.aes)	Fichiers en clair
Usage cible	Archivage à long terme	Miroir temps réel

5. Mise en œuvre — Partie 1 : Duplicati vers Google Drive

5.1 Préparation des données

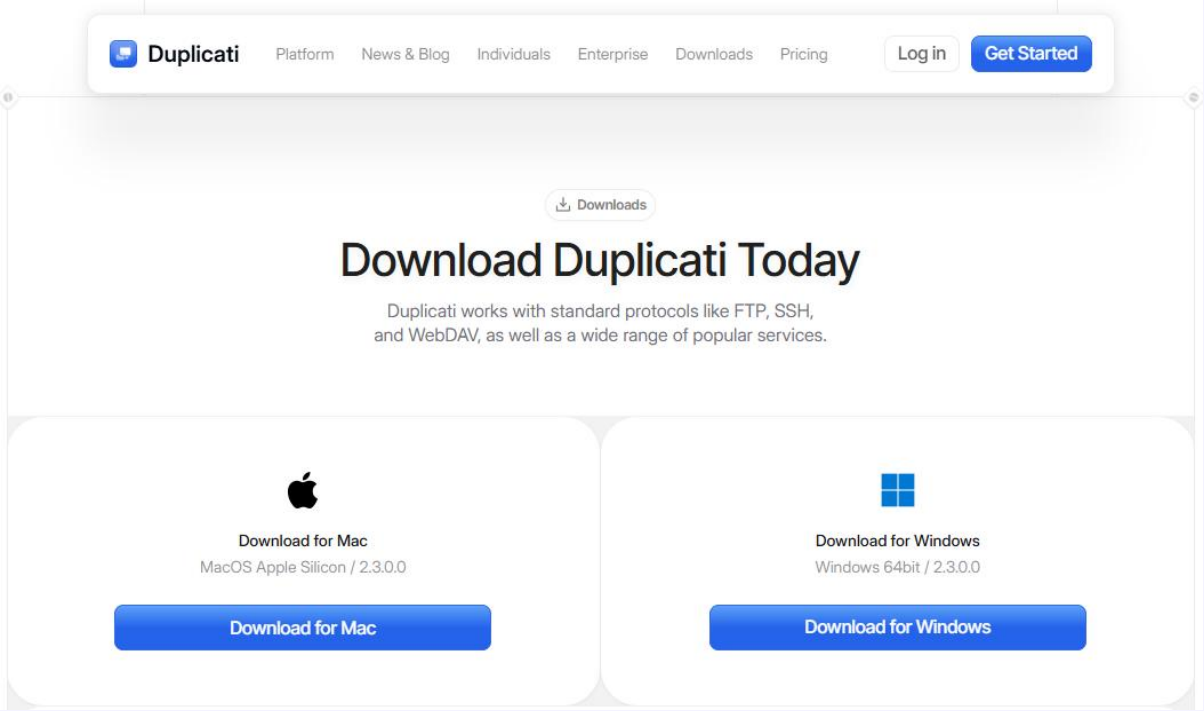
J'ai créé un dossier C:\Donnees_BTS\ contenant mes documents réels de BTS : cours, révisions, dossiers des projets E6 et sauvegardes du portfolio. La taille totale atteint environ 70 Mo répartis dans trois sous-dossiers : Cours btssio revision, DOC EXAM et Portfolio maj.



Contenu du dossier C:\Donnees_BTS\ avec ses trois sous-dossiers dans l'explorateur Windows

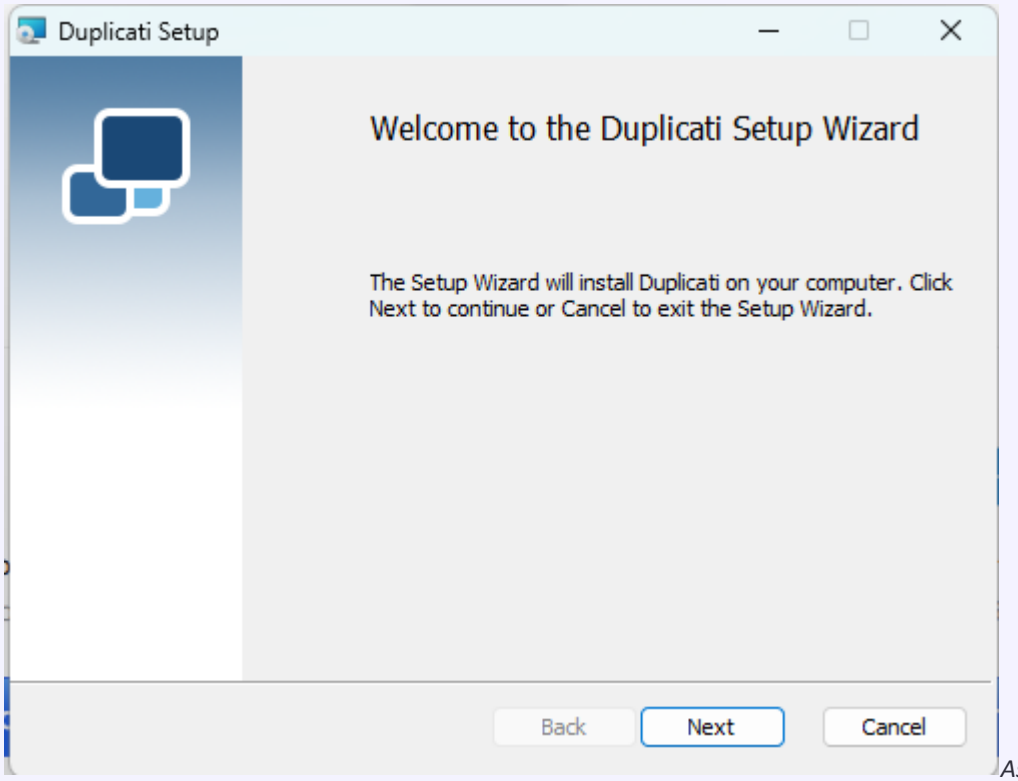
5.2 Installation de Duplicati

Duplicati a été téléchargé depuis le site officiel duplicati.com/download en version stable Windows 64-bit.



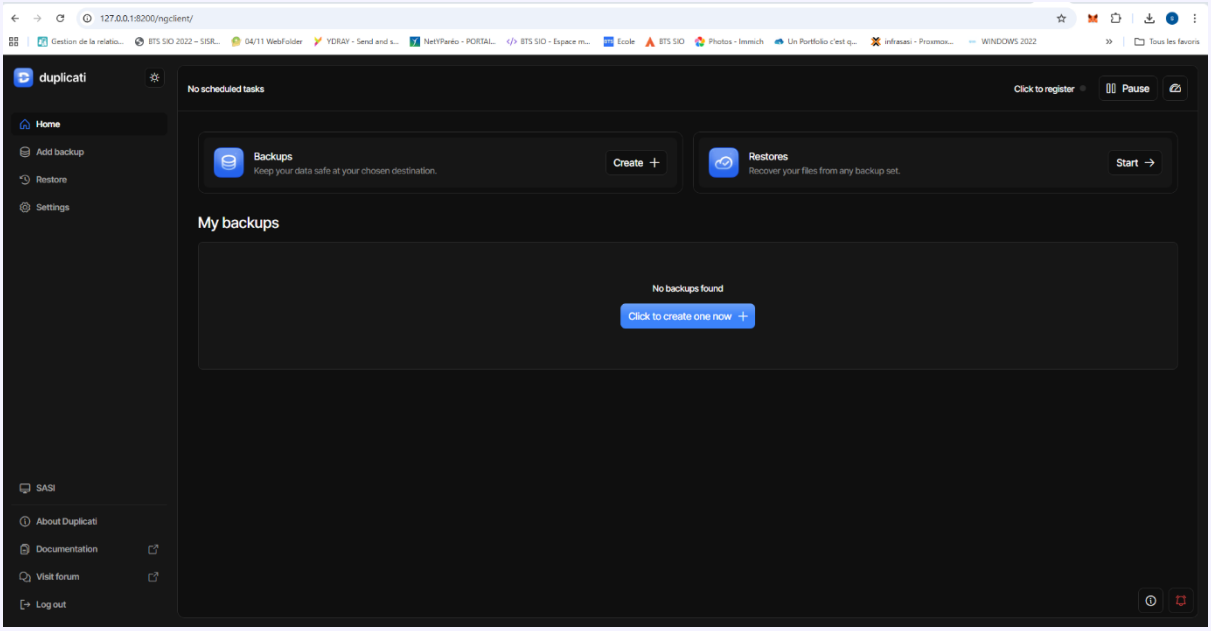
Page de téléchargement officielle de Duplicati

L'installation s'effectue via l'assistant MSI standard en laissant les paramètres par défaut.



Assistant d'installation Duplicati — écran final

Après installation, Duplicati tourne en tâche de fond et expose une interface web accessible à l'adresse http://localhost:8200.

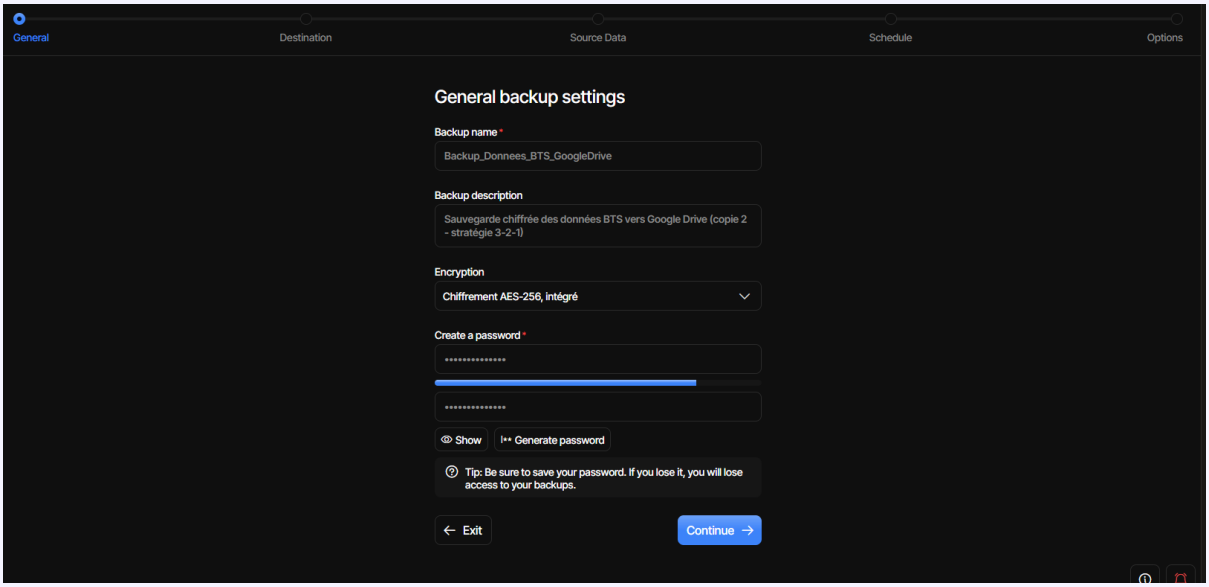


Interface web Duplicati à la première ouverture

5.3 Configuration du job de sauvegarde

Étape 1 — Paramètres généraux

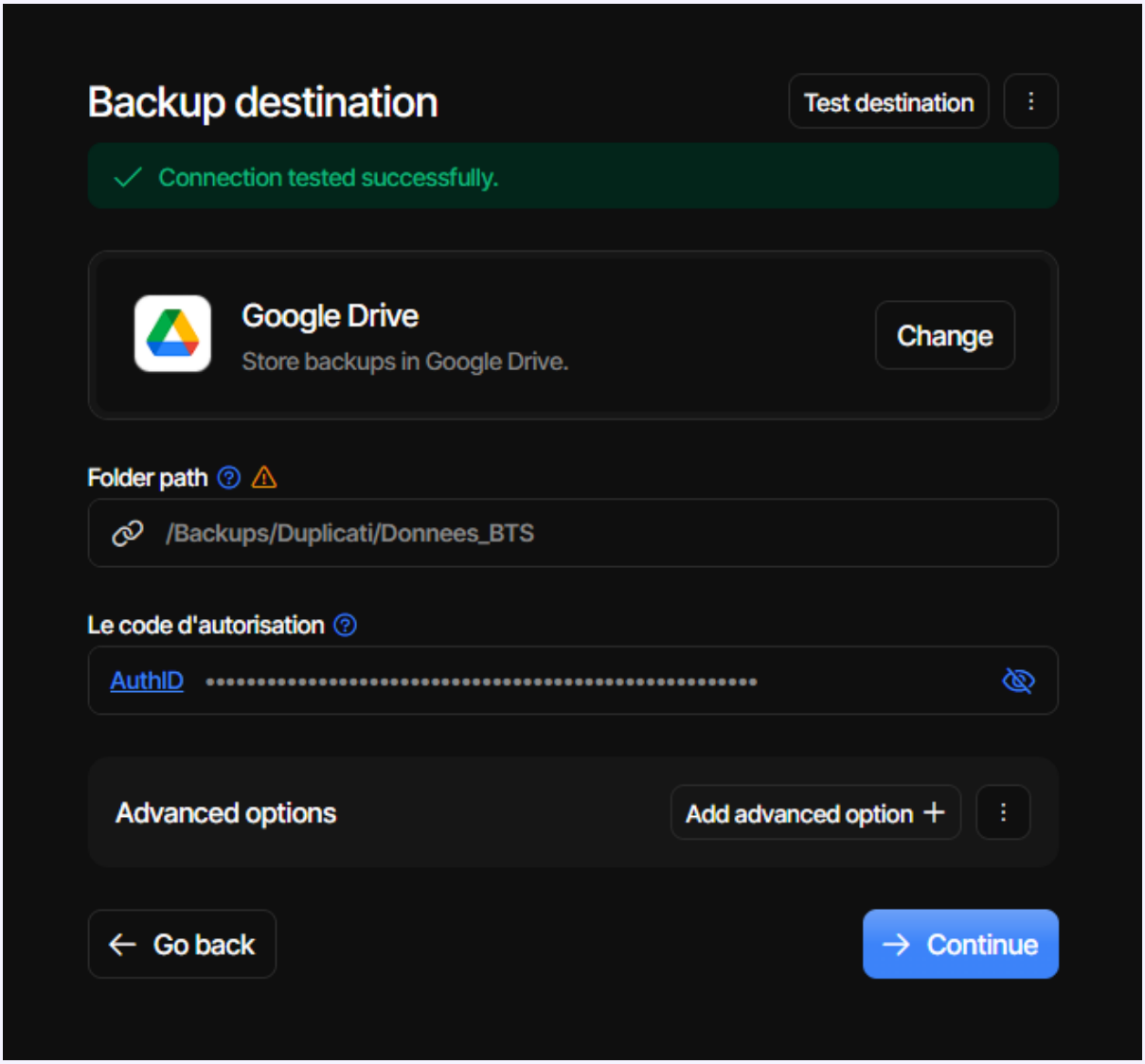
Création d'un nouveau job nommé Backup_Donnees_BTS_GoogleDrive. Activation du chiffrement AES-256 natif avec une passphrase robuste qui doit être conservée dans un gestionnaire de mots de passe sécurisé. Sans cette passphrase, la restauration est impossible : même l'administrateur de Duplicati ou Google ne peut pas déchiffrer les données.



Écran General settings — nom du backup et chiffrement AES-256 activé

Étape 2 — Destination Google Drive

Sélection de Google Drive comme destination. L'autorisation s'effectue via un token OAuth 2.0 généré par le service AuthID de Duplicati. Après authentification Google, le test de connexion confirme que la communication est établie.

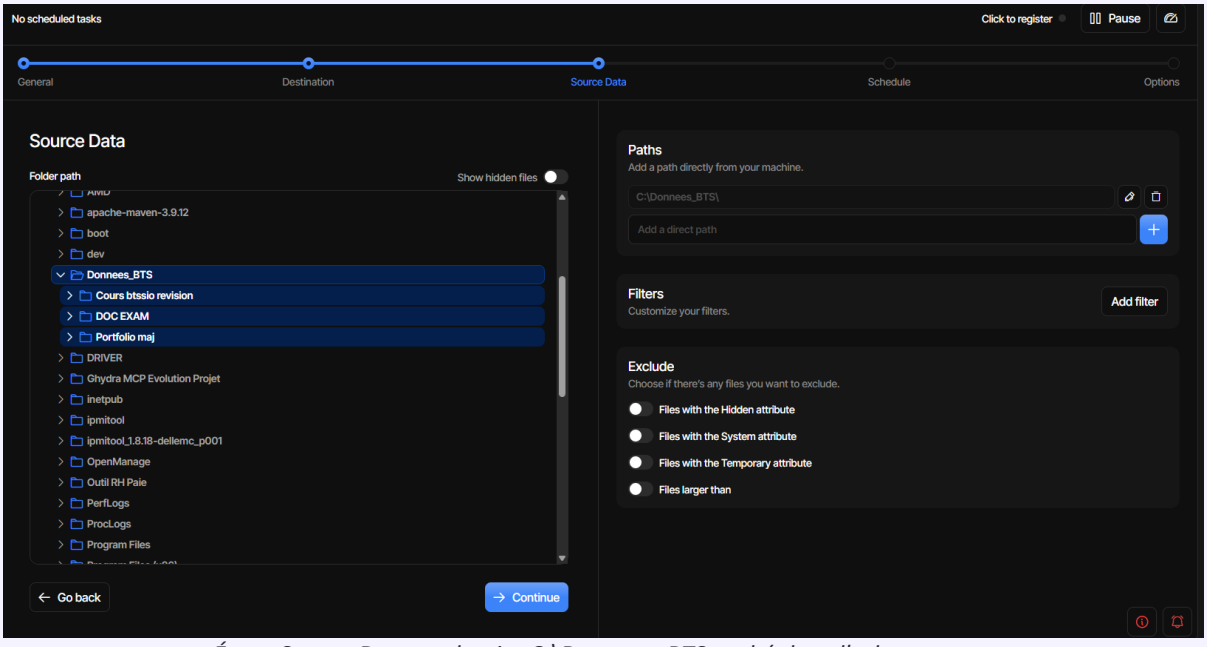


Écran Backup destination — Google Drive avec le message Connection tested successfully

> **À RETENIR — Principe du moindre privilège — OAuth**
>
> Duplicati utilise un scope OAuth restreint à son application : il n'a accès qu'aux fichiers qu'il crée lui-même, pas au reste de mon Google Drive. Cela applique le principe du moindre privilège : si Duplicati était compromis, un attaquant ne pourrait pas accéder à mes autres documents.

Étape 3 — Source Data

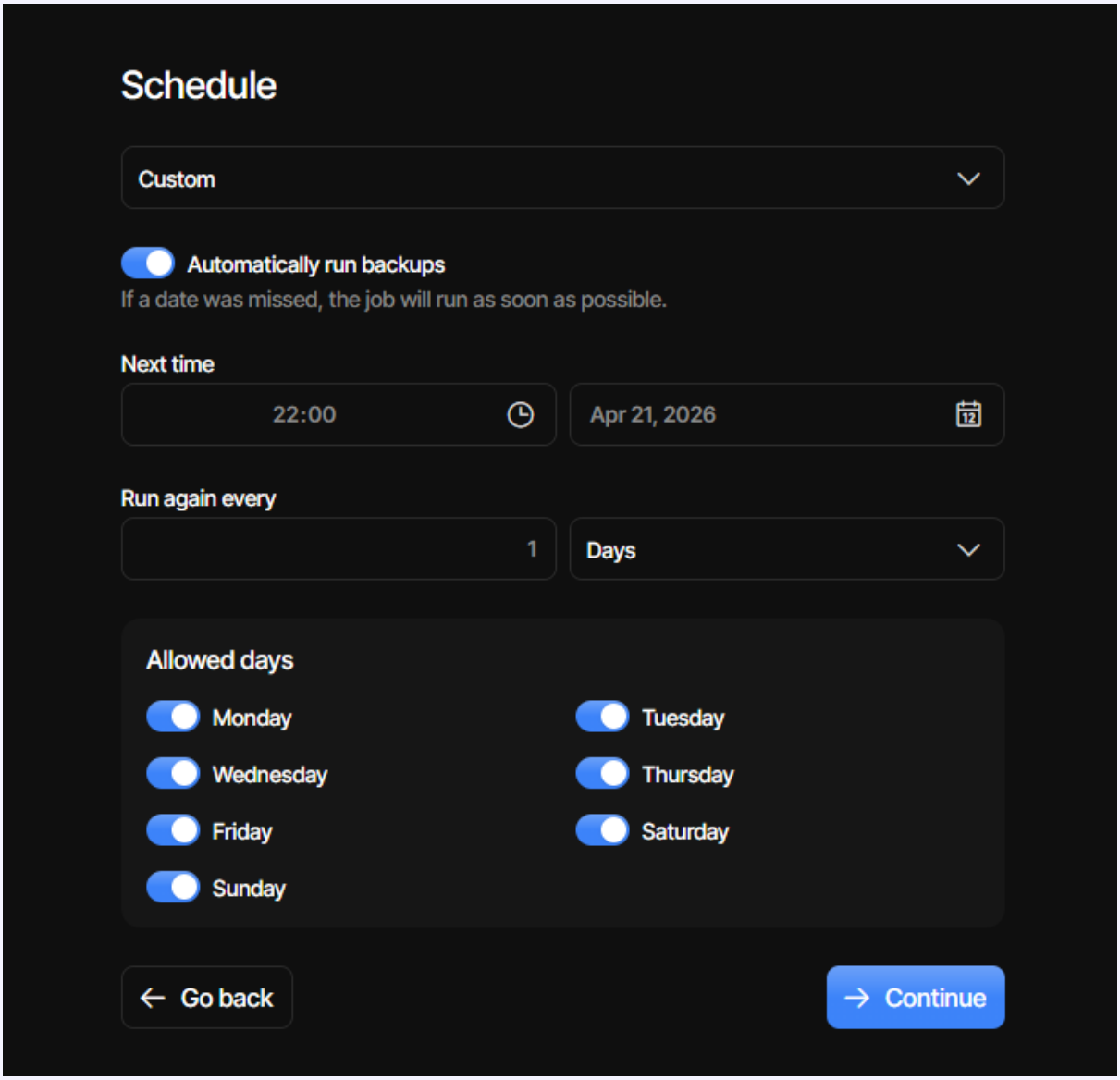
Sélection du dossier C:\Donnees_BTS\ dans l'arborescence. Aucun filtre d'exclusion n'est appliqué puisque l'ensemble du dossier doit être protégé.



Écran Source Data — dossier C:\Donnees_BTS coché dans l'arborescence

Étape 4 — Planification

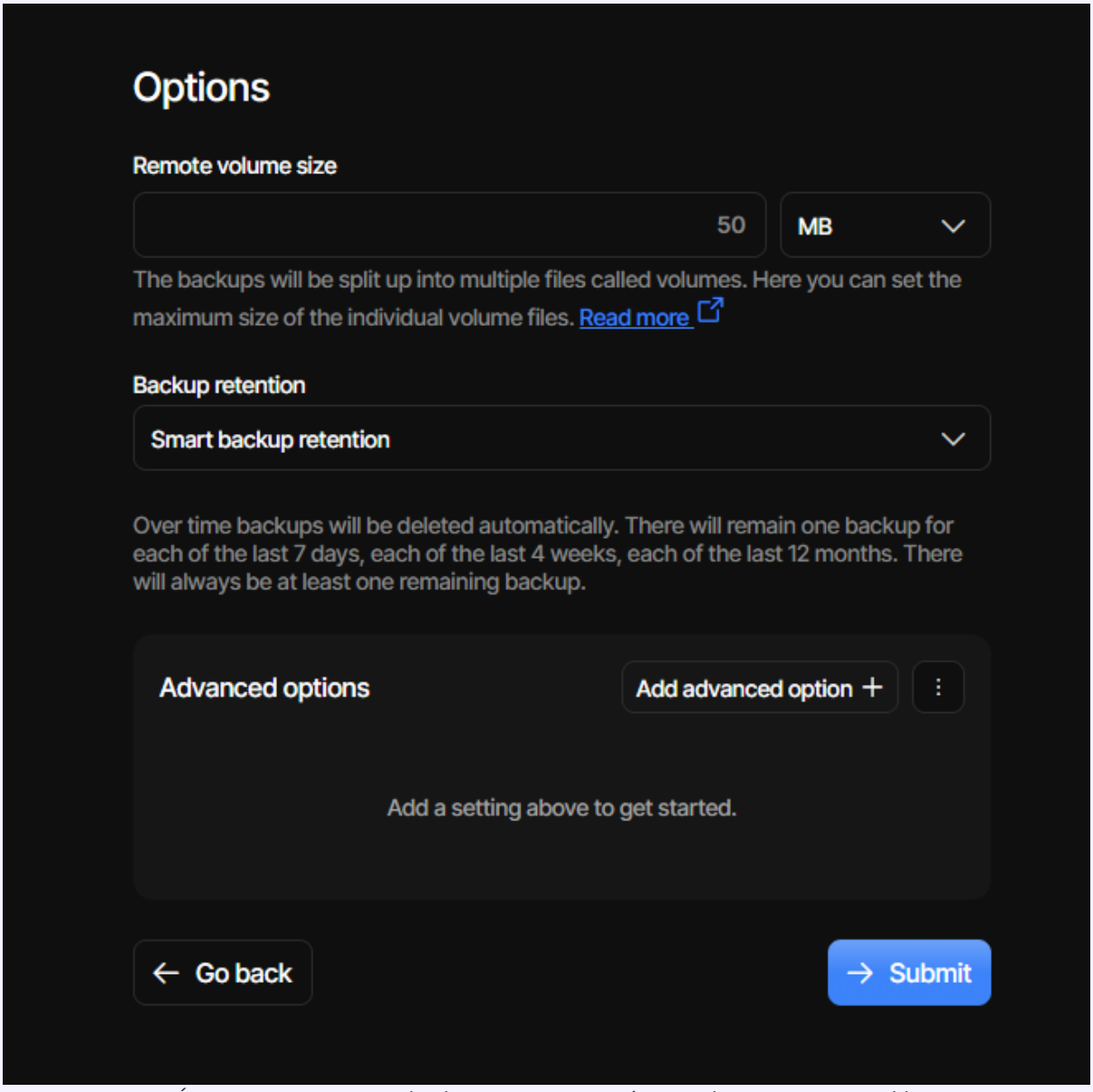
La sauvegarde est configurée pour s'exécuter quotidiennement à 22h00. Cet horaire correspond à une période de faible activité, hors heures d'utilisation du poste, et garantit un RPO de 24 heures.



Écran Schedule — planification quotidienne à 22h00 sur les 7 jours de la semaine

Étape 5 — Options et rétention

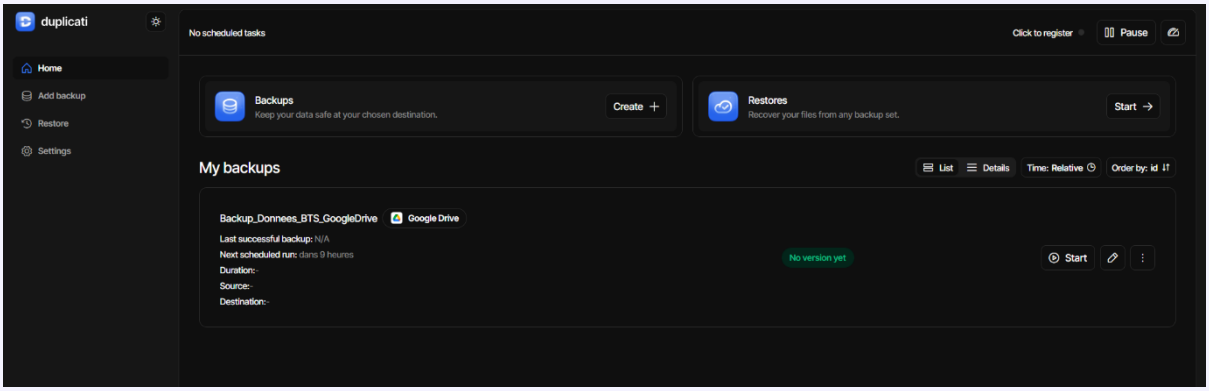
La rétention Smart backup retention (GFS) est activée : Duplicati conserve automatiquement une sauvegarde par jour pendant 7 jours, une par semaine pendant 4 semaines, et une par mois pendant 12 mois. Ce mécanisme évite la saturation du cloud tout en conservant un historique long.



Écran Options — Smart backup retention activée avec description GFS visible

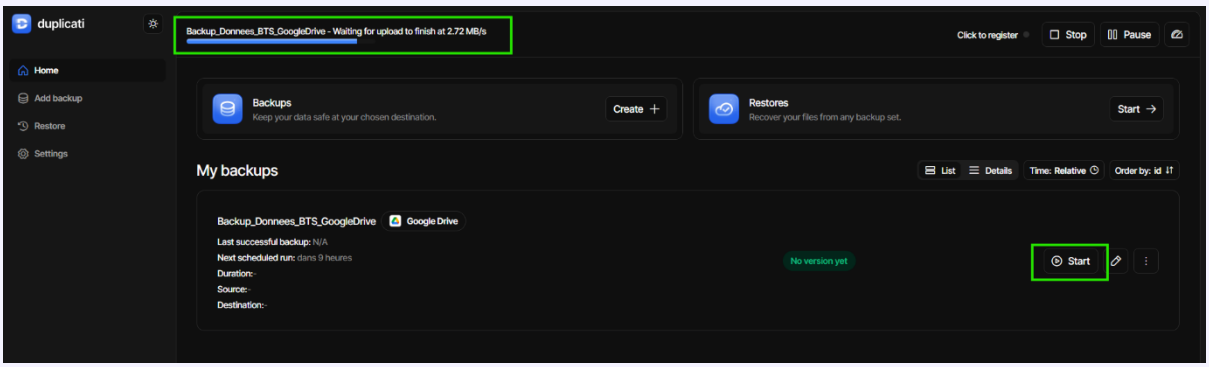
5.4 Première exécution et vérification

Une fois le job créé, il apparaît dans la liste des backups avec son prochain déclenchement planifié.



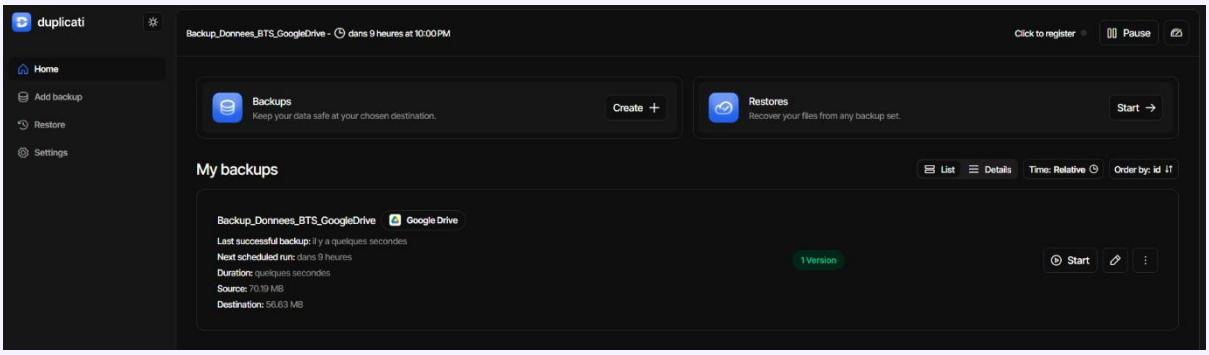
Page d'accueil Duplicati — job Backup_Donnees_BTS_GoogleDrive créé avec Next scheduled run dans 9 heures

Le lancement manuel via le bouton Start initie la première sauvegarde. Duplicati scanne les fichiers, les compresse, les chiffre en AES-256 puis les transmet vers Google Drive par blocs successifs.



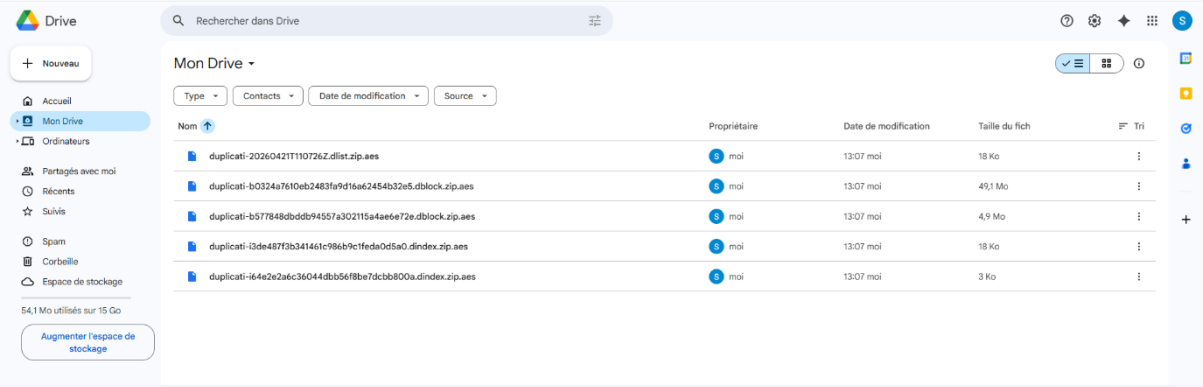
Job en cours d'exécution — barre de progression avec vitesse de transfert 2,72 Mo/s

À l'issue de la sauvegarde, Duplicati affiche un récapitulatif complet : 70,19 Mo de données source ont été compressés en 56,63 Mo sur le cloud, soit environ 20 % de gain d'espace grâce à la compression. Une version est désormais enregistrée.



Job terminé — Source 70,19 Mo / Destination 56,63 Mo / 1 Version

La vérification côté Google Drive confirme la présence des fichiers de sauvegarde au format .aes (Advanced Encryption Standard). Aucun fichier n'est lisible en clair : les noms sont des empreintes SHA-256 et le contenu est chiffré.



Interface Google Drive — fichiers duplicati-.dblock.zip.aes, *.dindex.zip.aes et *.dlist.zip.aes visibles*

À RETENIR — Architecture Duplicati — Trois types de fichiers

Duplicati structure chaque sauvegarde en trois types de fichiers chiffrés : les dblock (blocs de données), les dindex (index pour accélérer les recherches) et les dlist (manifeste listant l'état de la sauvegarde). Cette architecture rend possible la déduplication et la restauration rapide.

6. Mise en œuvre — Partie 2 : Rclone vers Mega

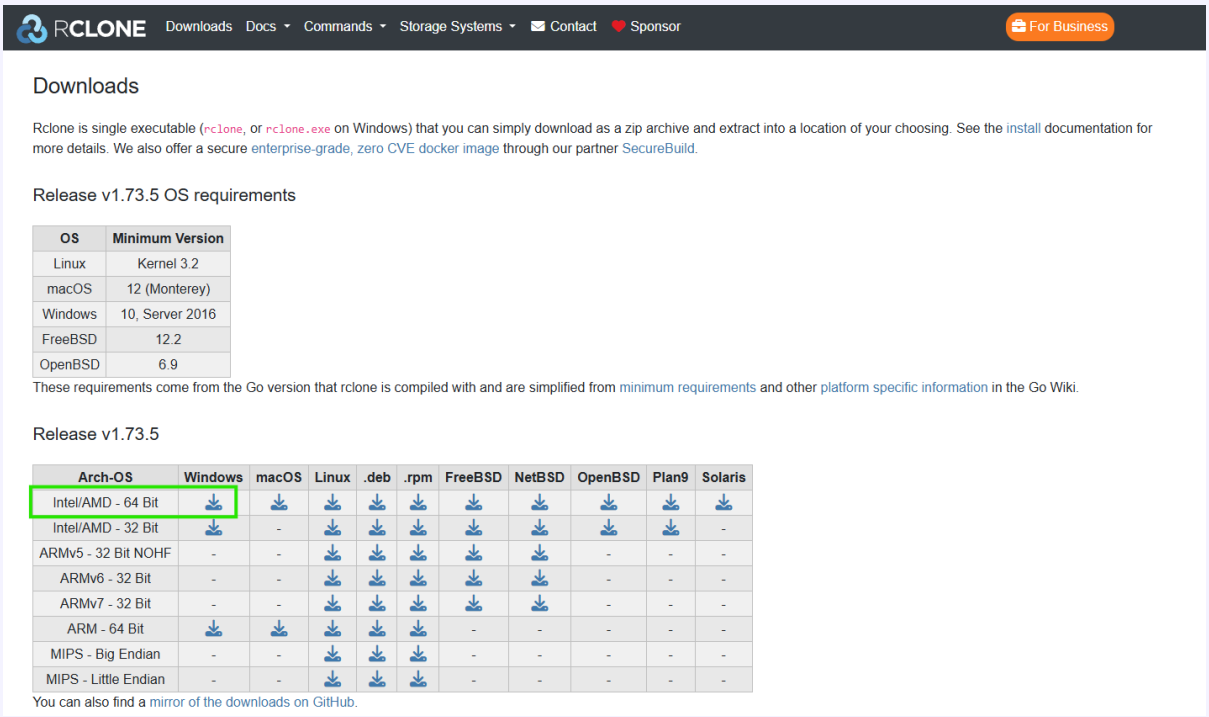
6.1 Choix du fournisseur cloud

Initialement, le projet prévoyait d'utiliser k-Drive d'Infomaniak. Après vérification, le support WebDAV de k-Drive nécessite une offre payante (kSuite Pro ou kDrive Solo) et n'est pas disponible sur le plan gratuit myKSuite. J'ai donc opté pour Mega.nz, qui présente plusieurs avantages :

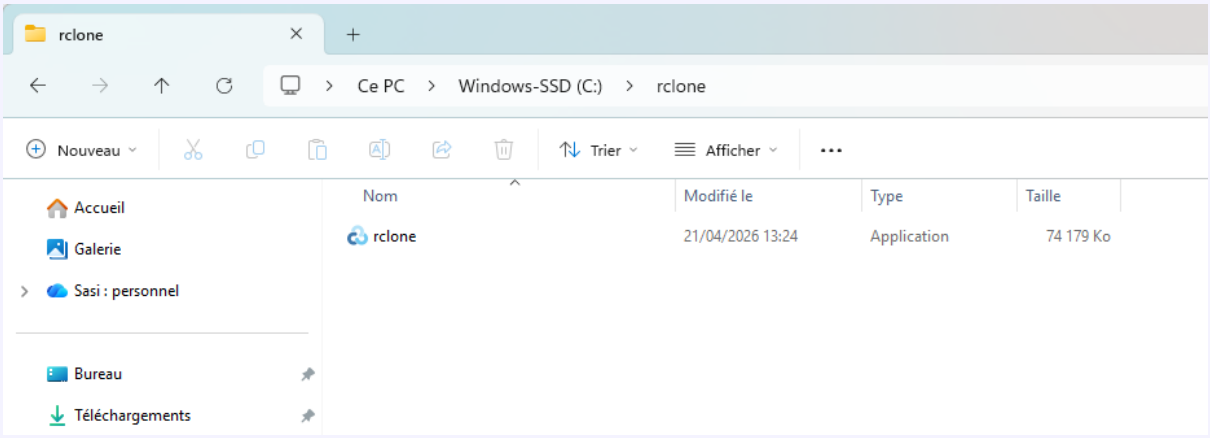
- 20 Go d'espace gratuit (contre 15 Go chez Google Drive).
- Support natif dans Rclone via le backend dédié mega (pas besoin de WebDAV).
- Chiffrement zero-knowledge côté serveur (Mega n'a pas accès au contenu des fichiers).
- Fournisseur indépendant de Google, ce qui garantit la redondance géographique et juridique.

6.2 Installation de Rclone

Rclone est un exécutable unique qui ne nécessite pas d'installeur. Téléchargement depuis rclone.org/downloads en version Windows AMD64, extraction de l'archive ZIP puis placement du fichier rclone.exe dans le dossier C:\rclone\.



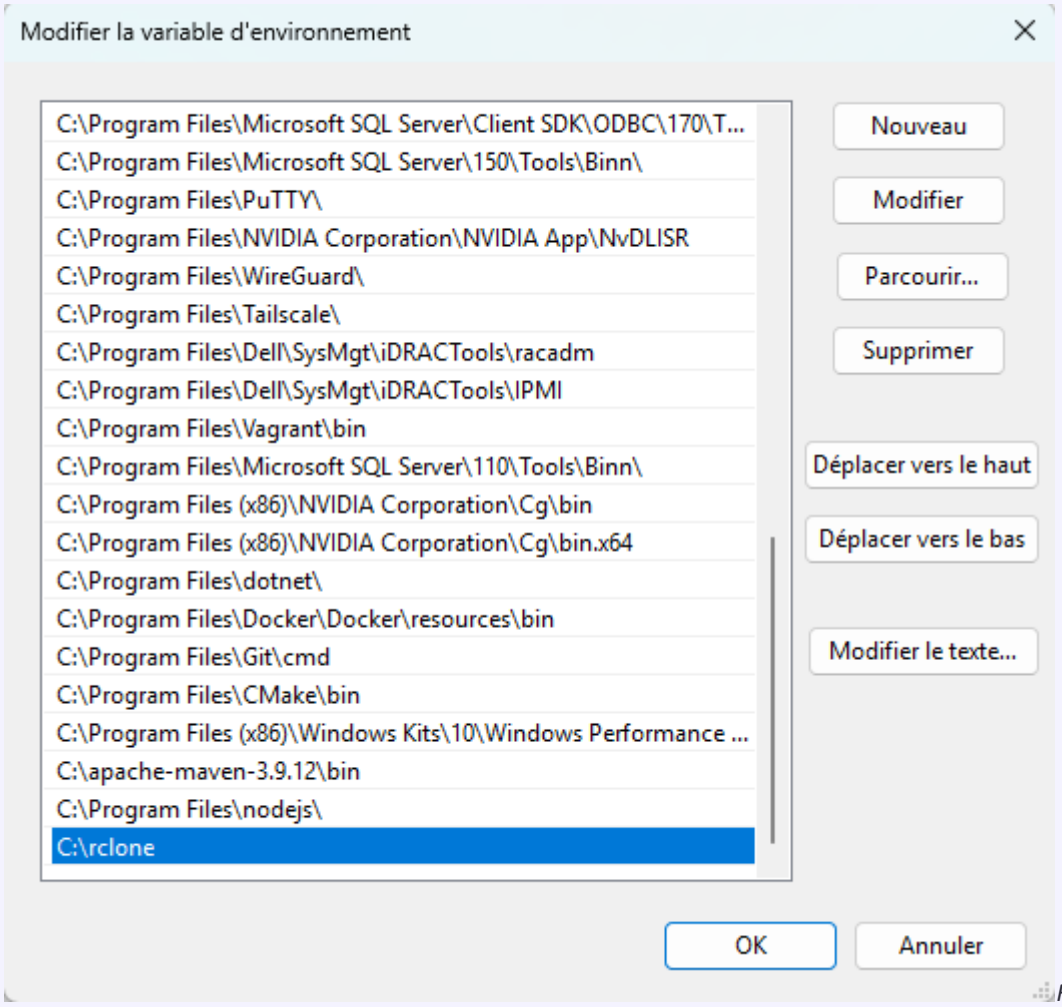
Page de téléchargement officielle de Rclone



Dossier C:\rclone\ contenant le fichier rclone.exe

Ajout au PATH système

Pour permettre l'appel de rclone depuis n'importe quel terminal sans spécifier le chemin complet, j'ai ajouté C:\rclone à la variable d'environnement PATH (Variables système > Path > Modifier > Nouveau).

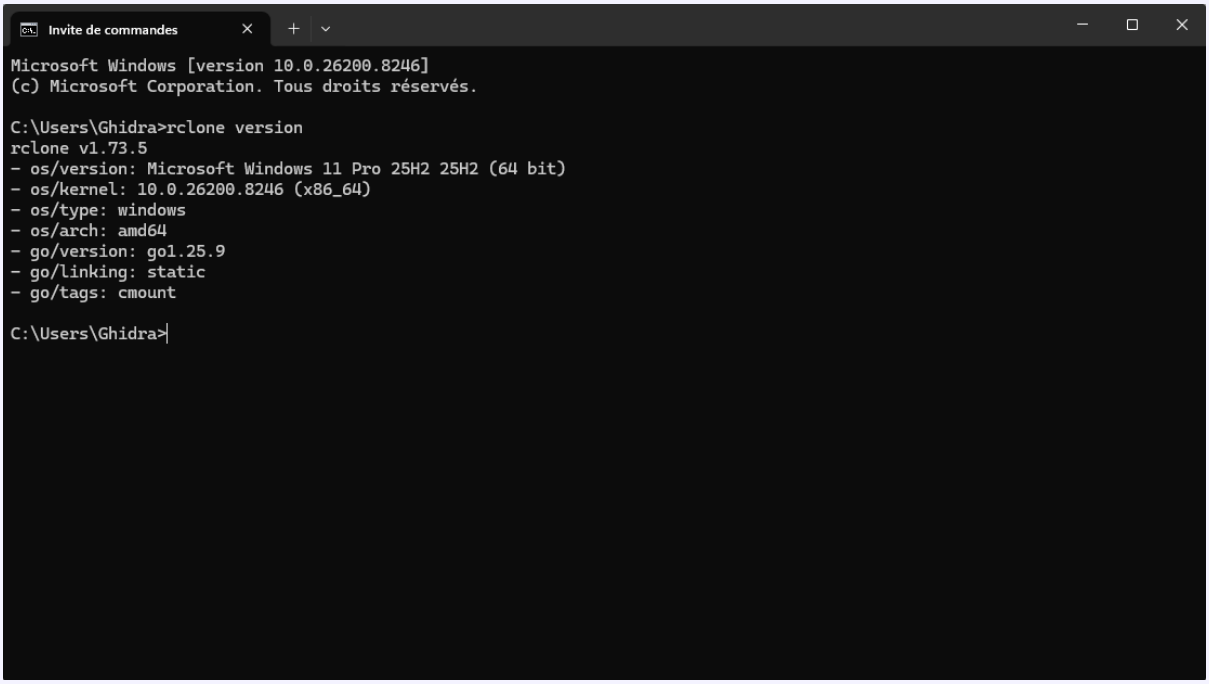


Fenêtre de modification de la variable PATH avec C:\rclone ajouté

Vérification

L'installation est validée en tapant rclone version dans une nouvelle fenêtre d'invite de commande :

```
C:\Users\Ghidra> rclone version
rclone v1.73.5
- os/version: Microsoft Windows 11 Pro 25H2 (64 bit)
- os/kernel: 10.0.26200.8246 (x86_64)
- os/type: windows
- os/arch: amd64
```



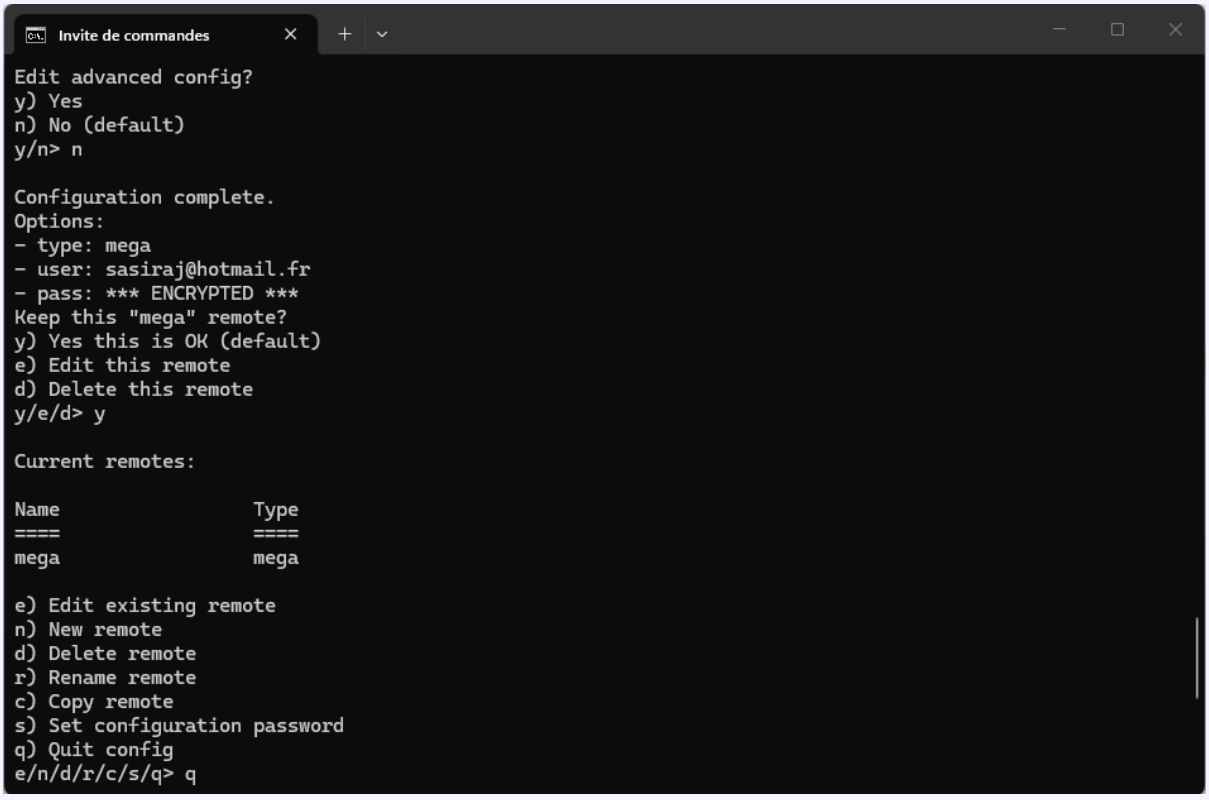
Terminal CMD affichant le résultat de la commande rclone version

6.3 Configuration du remote Mega

La configuration de Rclone s'effectue via la commande interactive rclone config. Elle crée un fichier de configuration (rclone.conf) dans le profil utilisateur, dans lequel le mot de passe est stocké sous forme chiffrée.

Étapes suivies pas à pas :

1. Choix de n (new remote) pour créer un nouveau remote.
2. Nom du remote : mega.
3. Type de stockage : mega (backend natif Rclone).
4. Identifiant : adresse e-mail du compte Mega.
5. Mot de passe : saisi manuellement, stocké chiffré dans rclone.conf.
6. 2FA : laissé vide (non activé sur ce compte).
7. Configuration avancée : non (valeurs par défaut).
8. Validation : y (conserver la configuration).



*Terminal CMD — récapitulatif de la configuration Mega avec pass: *** ENCRYPTED ****

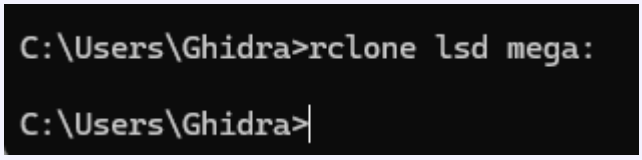
> **À RETENIR — Sécurité du fichier de configuration**
>
> Le mot de passe Mega n'est pas stocké en clair dans rclone.conf mais de manière chiffrée (mention *** ENCRYPTED *** dans le récapitulatif). C'est une bonne pratique de sécurité : si le fichier de configuration est consulté par un tiers, le mot de passe ne peut pas être extrait directement.

6.4 Test de la connexion

Avant toute synchronisation, j'ai validé la connexion avec la commande rclone lsd mega: (list directories).

```
C:\Users\Ghidra> rclone lsd mega:
C:\Users\Ghidra>
```

L'absence d'erreur et le retour immédiat au prompt confirment que l'authentification a réussi et que le compte Mega est accessible (l'absence de sortie est normale : le compte vient d'être créé et ne contient aucun dossier).



Terminal CMD — commande rclone lsd mega: exécutée sans erreur

6.5 Première synchronisation

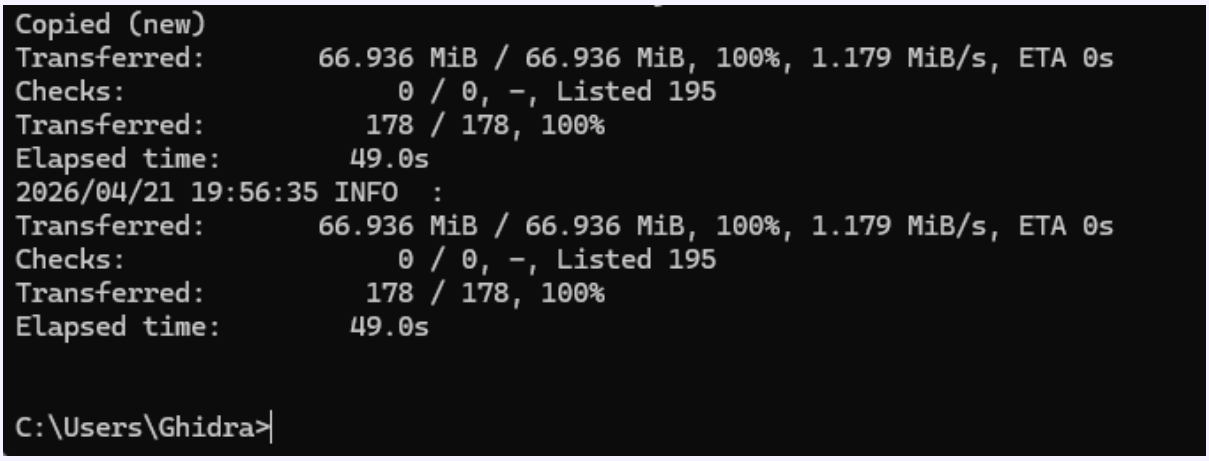
La synchronisation vers Mega est réalisée avec la commande suivante :

```
rclone sync C:\Donnees_BTS mega:/Backups/Donnees_BTS -v --progress
```

Explication des paramètres :

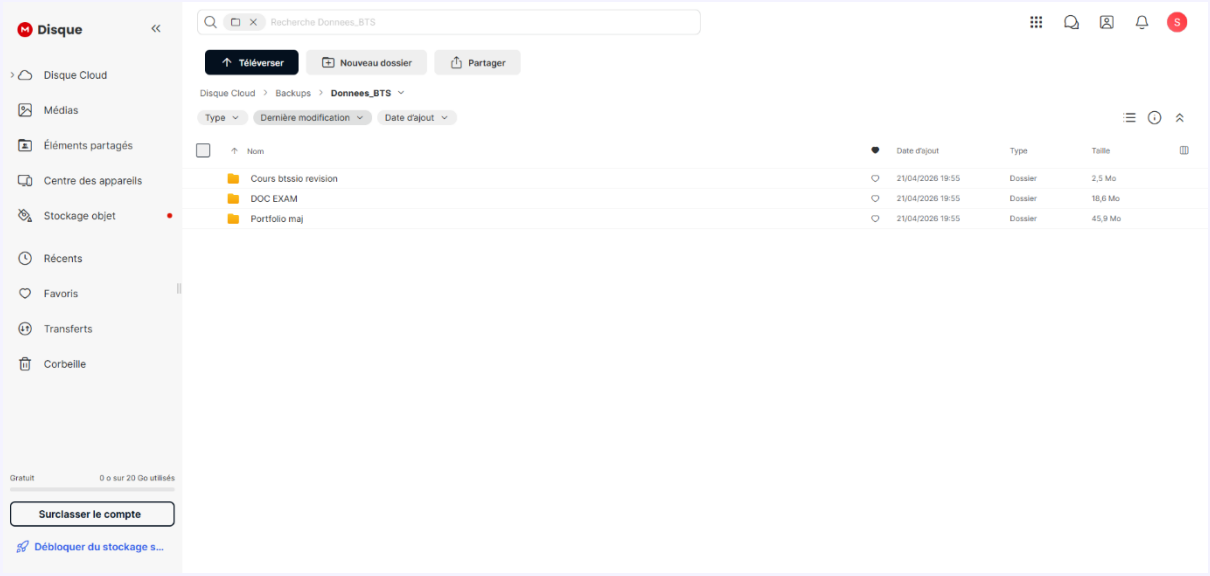
- sync : mode miroir — la destination devient le reflet exact de la source.
- C:\Donnees_BTS : répertoire source sur le PC.
- mega:/Backups/Donnees_BTS : destination sur Mega (le dossier est créé automatiquement).
- -v : mode verbose, affichage détaillé des opérations.
- --progress : affichage en temps réel de la progression.

Résultat obtenu : 178 fichiers transférés pour un total de 66,936 Mo en 49 secondes, soit une vitesse moyenne d'environ 1,18 Mo/s.



Terminal CMD — récapitulatif final de rclone sync : Transferred 100 %, Elapsed time 49 s

La vérification sur l'interface web de Mega confirme la présence de l'arborescence complète dans le chemin Disque Cloud > Backups > Donnees_BTS. Les trois sous-dossiers sont visibles avec leurs fichiers en clair : Rclone n'applique pas de chiffrement côté client, contrairement à Duplicati.



Interface web Mega — arborescence Disque Cloud > Backups > Donnees_BTS visible

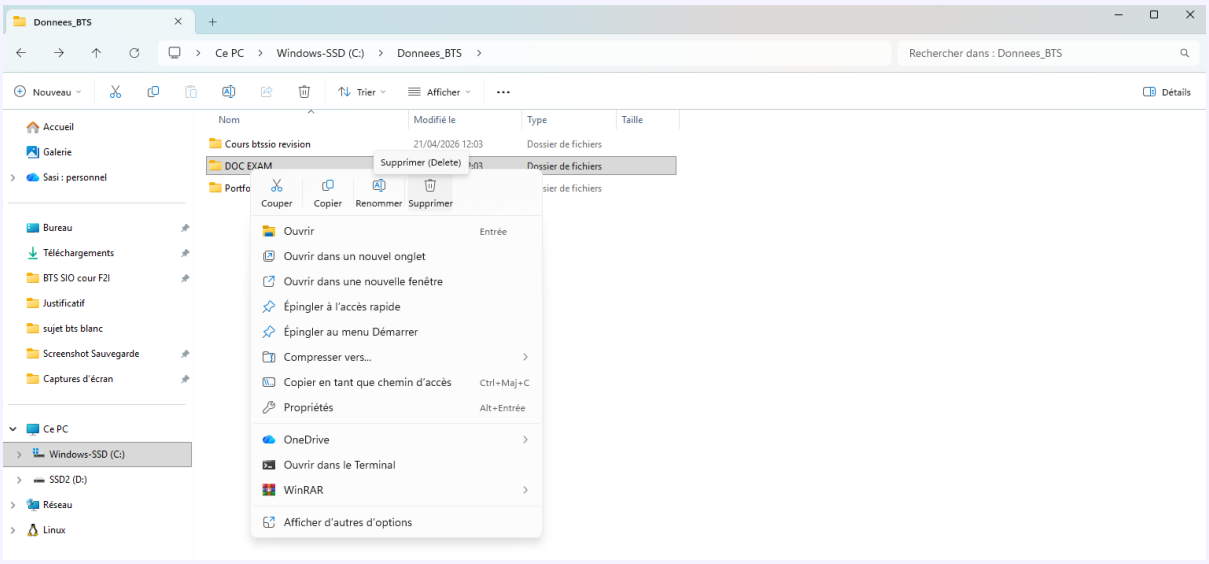
7. Tests de restauration

Une sauvegarde qui n'a jamais été testée n'est pas une sauvegarde. Cette règle fondamentale de l'administration système impose de valider régulièrement la procédure de restauration pour s'assurer que les données sont effectivement récupérables en cas de sinistre.

7.1 Test 1 — Restauration Duplicati depuis Google Drive

Scénario

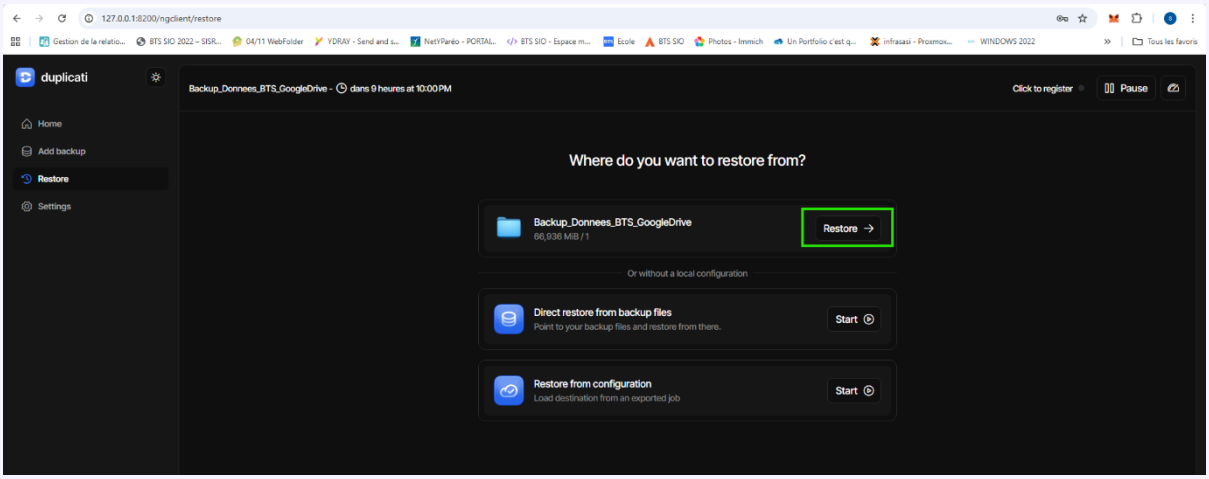
Simulation d'une perte accidentelle : suppression volontaire du dossier DOC EXAM (contenant mes documents d'examen, 46 fichiers et 19,49 Mo) dans C:\Donnees_BTS\, puis vidage de la corbeille pour simuler une perte définitive.



Dossier C:\Donnees_BTS\ après suppression de DOC EXAM : il ne reste que Cours btssio revision et Portfolio maj

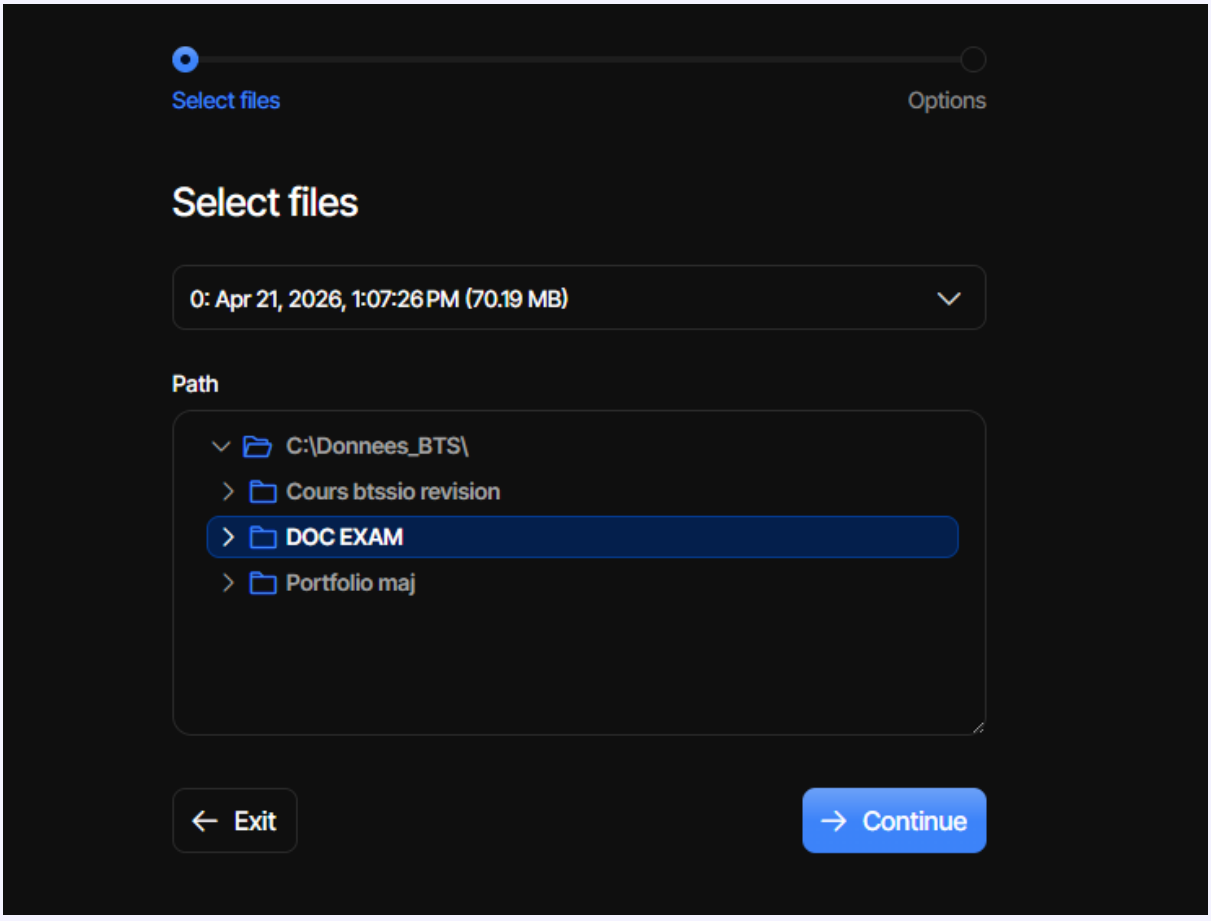
Restauration via Duplicati

Depuis l'interface web Duplicati, accès à la fonction Restore. Sélection de la sauvegarde Backup_Donnees_BTS_GoogleDrive et de la dernière version disponible.



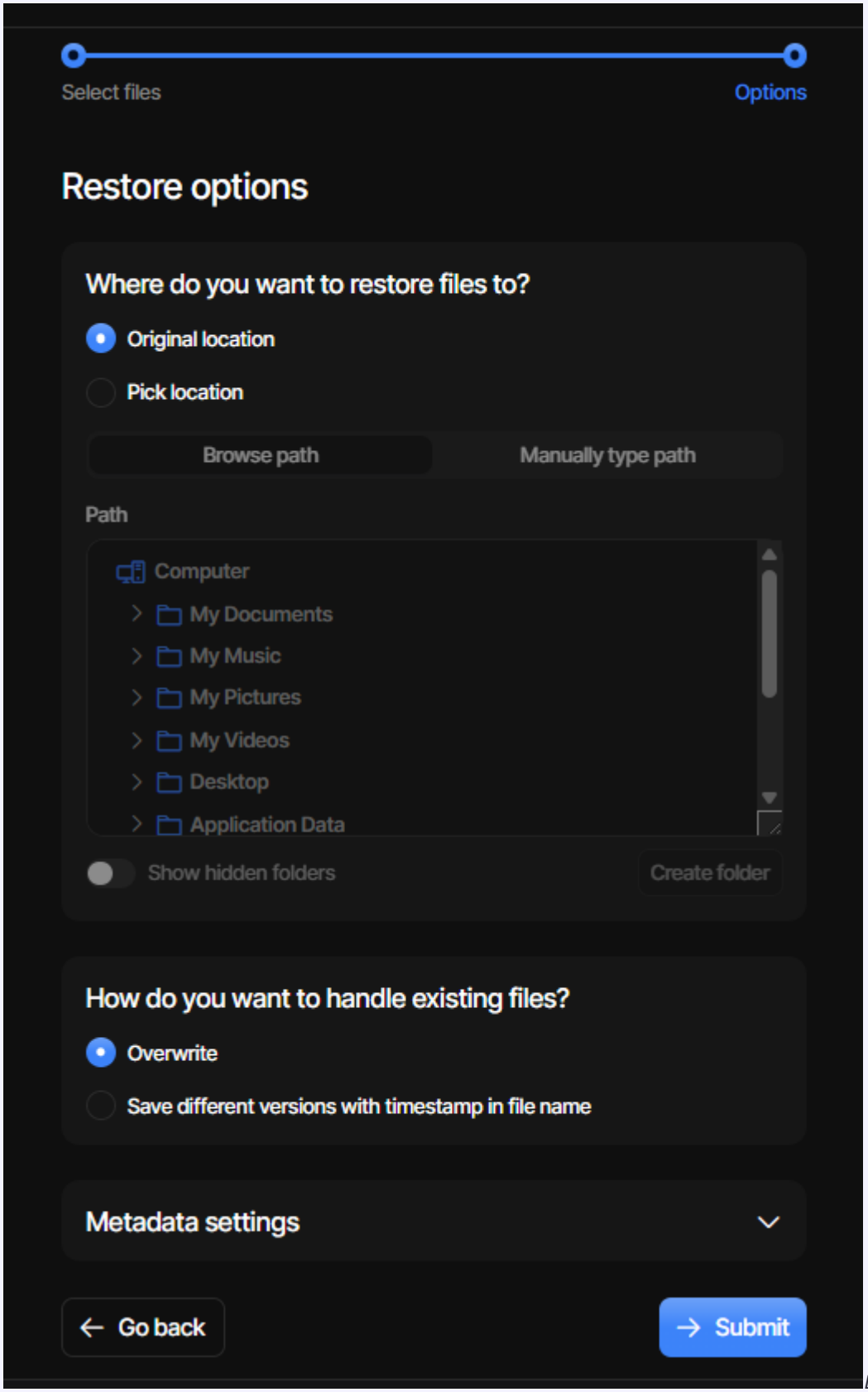
Écran de sélection de la sauvegarde et de la version à restaurer dans Duplicati

Dans l'arborescence des fichiers sauvegardés, sélection uniquement du dossier DOC EXAM à restaurer.



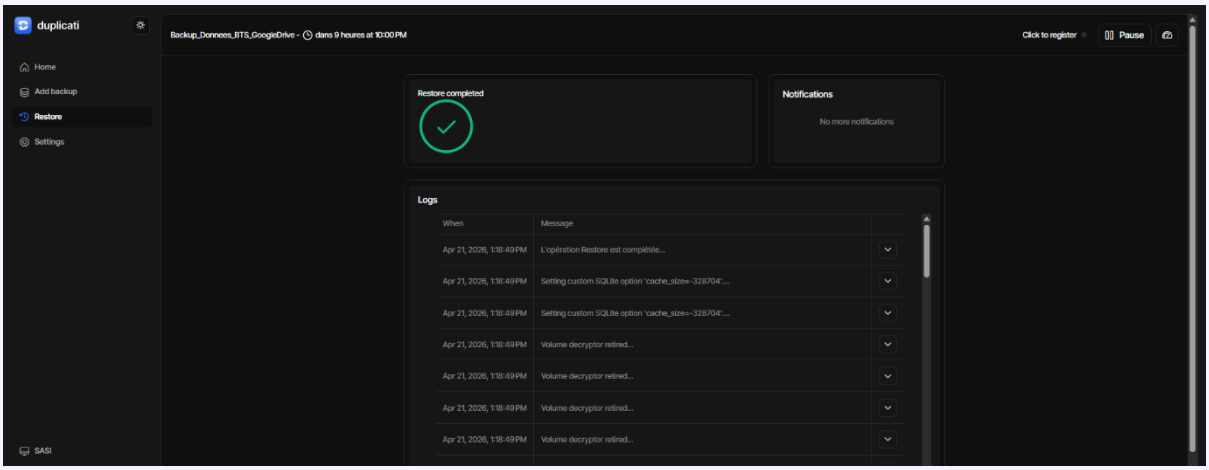
Arborescence des fichiers sauvegardés dans Duplicati — DOC EXAM coché

Choix de l'option Original location : restauration vers l'emplacement d'origine (C:\Donnees_BTS\DOC EXAM).



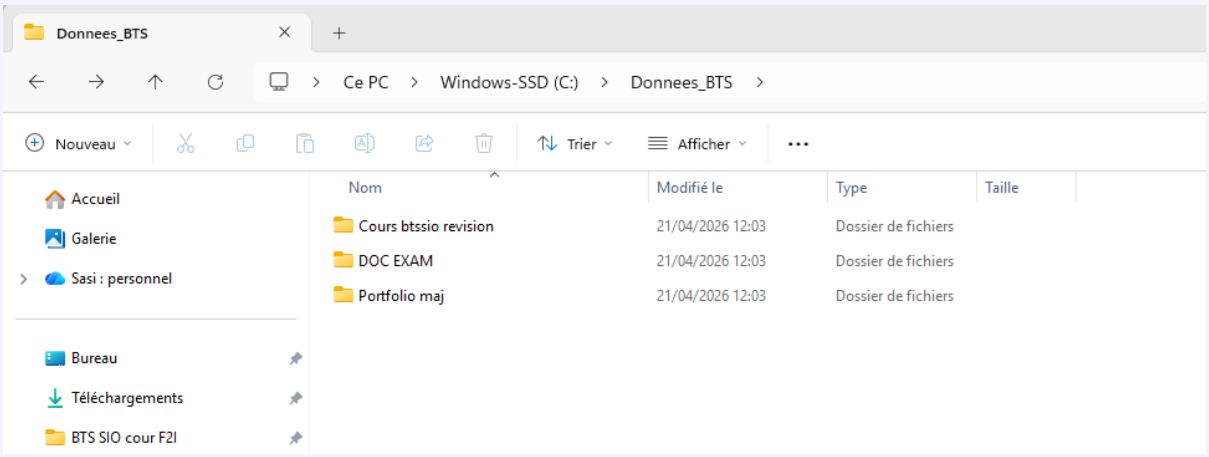
Écran d'options de restauration — Original location sélectionné

Lancement de la restauration : Duplicati télécharge les blocs chiffrés depuis Google Drive, les déchiffre avec la passphrase AES-256 et reconstruit l'arborescence complète.



Restauration en cours — barre de progression et logs détaillés de Duplicati

Vérification dans l'Explorateur Windows : le dossier DOC EXAM est bien de retour dans C:\Donnees_BTS\, avec son contenu intact.



Dossier C:\Donnees_BTS\ après restauration — les trois dossiers sont de nouveau présents

À RETENIR — Résultat du Test 1

Restauration de 46 fichiers / 19,49 Mo depuis Google Drive vers l'emplacement d'origine. Durée mesurée : moins d'une minute. RTO respecté largement. Test validé.

7.2 Test 2 — Restauration Rclone depuis Mega

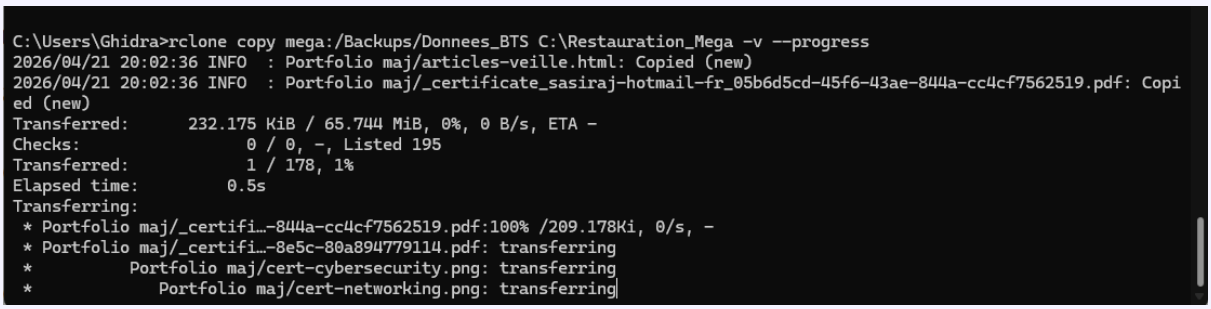
Scénario

Pour valider également la restauration du miroir Mega, j'ai effectué une restauration complète vers un emplacement séparé afin de ne pas écraser l'original.

Commande utilisée

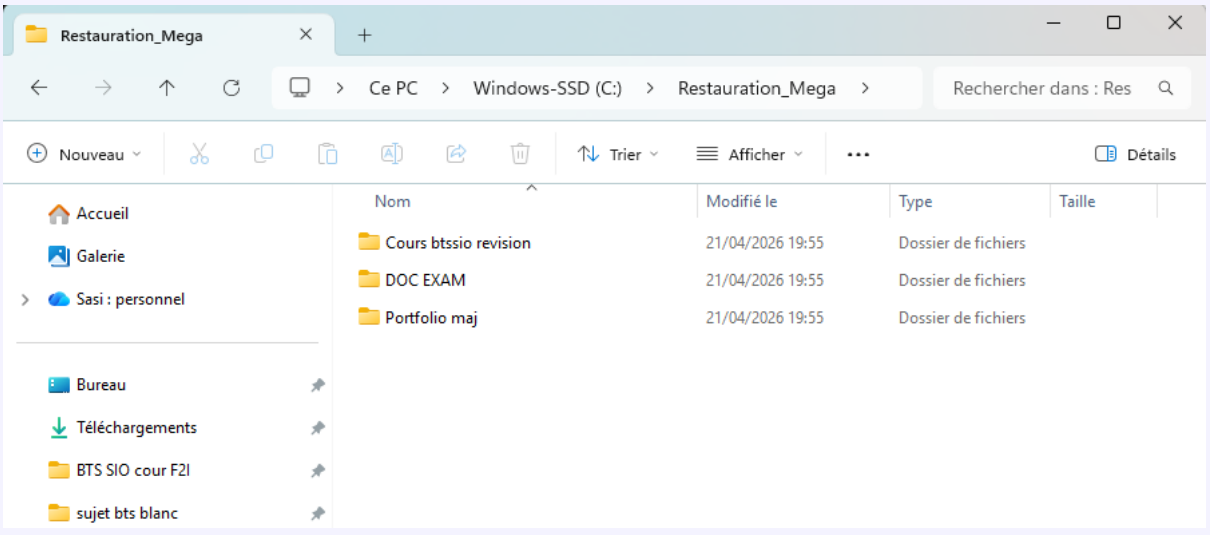
```
rclone copy mega:/Backups/Donnees_BTS C:\Restauration_Mega -v --progress
```

J'ai volontairement utilisé la commande copy (et non sync) car elle effectue une copie pure sans supprimer de fichiers, ce qui convient mieux à une opération de restauration où l'on souhaite récupérer les données sans risque.



Terminal CMD — commande rclone copy en cours ou terminée avec Transferred 100 %

Vérification dans l'Explorateur Windows : le dossier C:\Restauration_Mega\ est créé et contient les trois sous-dossiers restaurés.



Dossier C:\Restauration_Mega\ avec les trois sous-dossiers restaurés depuis Mega

À RETENIR — Résultat du Test 2

Restauration complète de l'ensemble des 178 fichiers (66,9 Mo) depuis Mega vers un dossier de test. Intégrité vérifiée visuellement. Test validé.

8. Automatisation

8.1 Duplicati — Automatisation native

Duplicati intègre nativement un planificateur interne. La tâche configurée à l'étape 5.3.4 s'exécute automatiquement chaque jour à 22h00 sans aucune intervention supplémentaire. Le service Duplicati tourne en arrière-plan au démarrage de Windows et prend en charge les éventuels échecs avec un système de retry intégré.

8.2 Rclone — Script batch et planificateur Windows

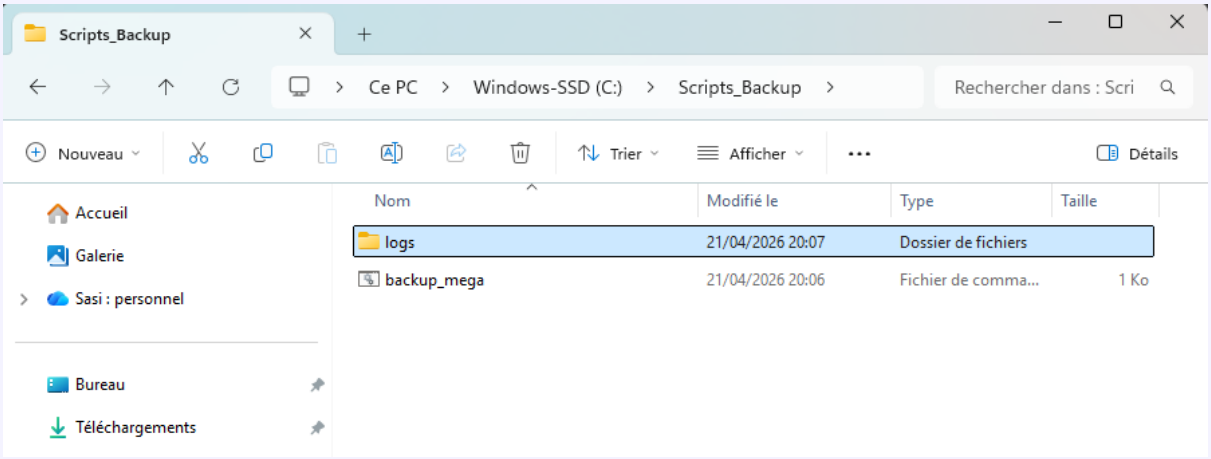
Rclone fonctionnant en ligne de commande, il nécessite un script d'automatisation pour être exécuté régulièrement. J'ai créé le fichier C:\Scripts_Backup\backup_mega.bat contenant les instructions suivantes :

```
@echo off
REM ============================================================
REM Script de sauvegarde Rclone vers Mega
REM Auteur : Sasiraj Gunaratnarajah
REM Date   : Avril 2026
REM Projet : Strategie de sauvegarde 3-2-1 (BTS SIO SISR - E5)
REM ============================================================

echo.
echo ========================================
echo   Sauvegarde Donnees_BTS vers Mega
echo ========================================
echo.
echo Date : %DATE% %TIME%
echo.

REM Execution de la synchronisation Rclone
rclone sync C:\Donnees_BTS mega:/Backups/Donnees_BTS -v --progress \
  --log-file=C:\Scripts_Backup\logs\backup_mega_%DATE:~-4%-%DATE:~3,2%-%DATE:~0,2%.log

REM Verification du code de retour
if %ERRORLEVEL% EQU 0 (
    echo [SUCCES] Sauvegarde terminee avec succes !
) else (
    echo [ERREUR] La sauvegarde a echoue - Code : %ERRORLEVEL%
)

echo Fin : %DATE% %TIME%
```

Bonnes pratiques appliquées dans le script :

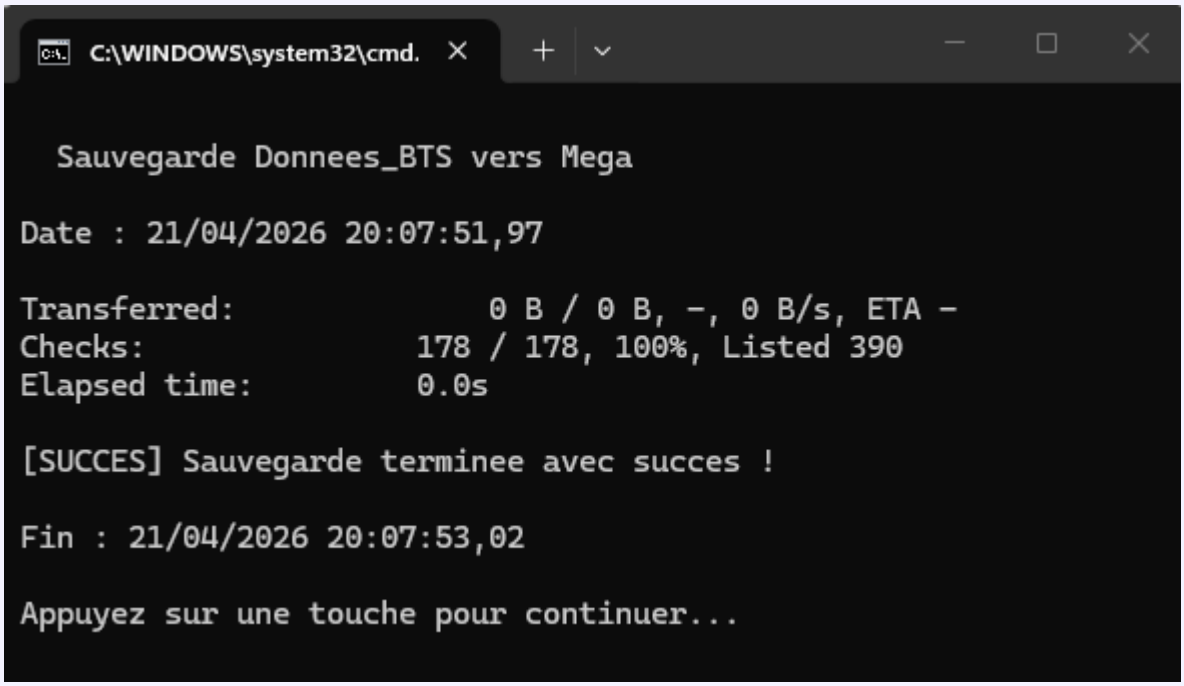
- En-tête documenté (auteur, date, projet) pour la traçabilité.
- Journalisation horodatée dans un dossier logs dédié : chaque exécution produit un fichier log nommé backup_mega_AAAA-MM-JJ.log.
- Gestion du code de retour (ERRORLEVEL) pour distinguer un succès d'un échec.

- Horodatage des messages dans la console pour faciliter le débogage.



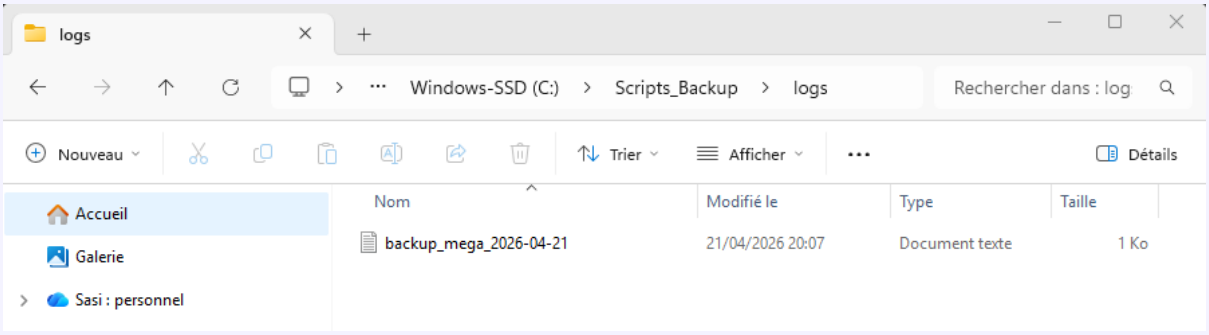
Dossier C:\Scripts_Backup\ avec le fichier backup_mega.bat et le sous-dossier logs

Un test manuel du script est effectué par double-clic. Le script se déroule normalement et affiche le message [SUCCES] en fin d'exécution.



Exécution manuelle du script — fenêtre CMD affichant [SUCCES] Sauvegarde terminee avec succes !

Le fichier de log est bien créé à chaque exécution et contient le détail des opérations Rclone (fichiers transférés, vitesse, erreurs éventuelles).

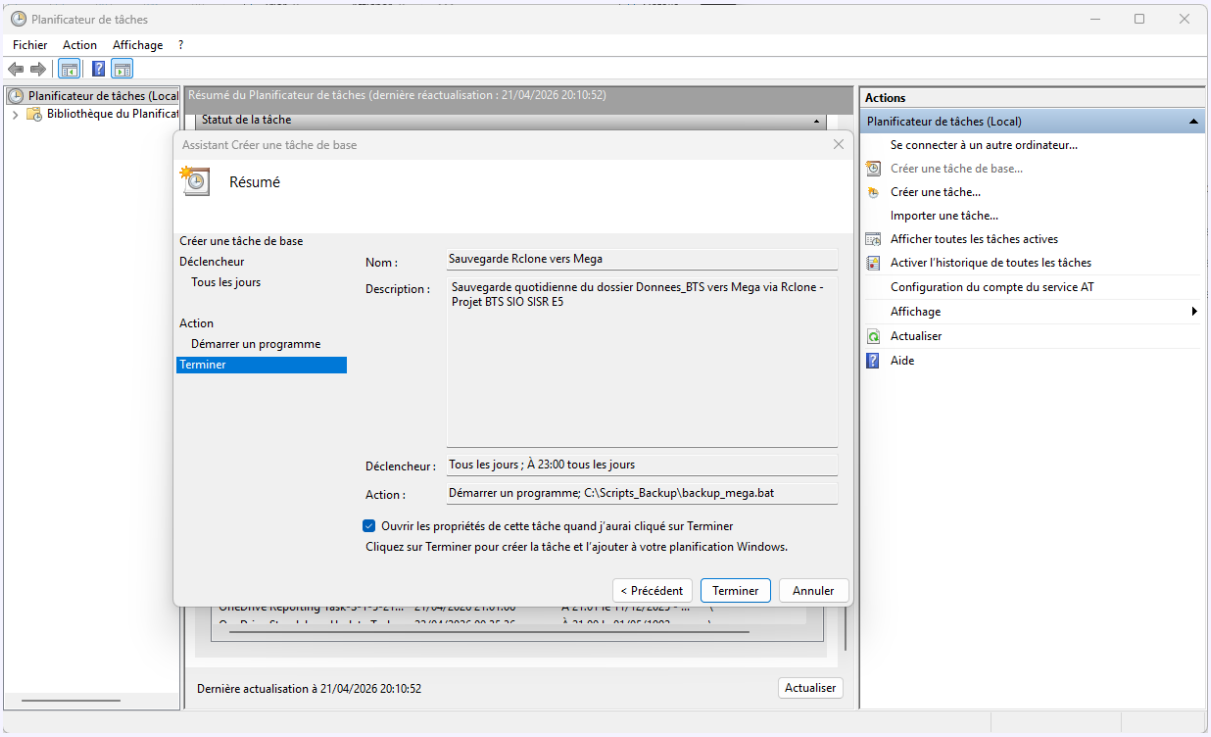


Dossier C:\Scripts_Backup\logs\ avec le fichier backup_mega_2026-04-21.log

8.3 Planification via le Planificateur de tâches Windows

L'exécution automatique du script est déléguée au Planificateur de tâches Windows (taskschd.msc) : création d'une tâche nommée Sauvegarde Rclone vers Mega, déclenchée quotidiennement à 23h00.

Le décalage d'une heure avec Duplicati (22h00) est volontaire : il évite de saturer la connexion Internet en lançant deux gros transferts simultanément et réduit la charge CPU sur le poste.

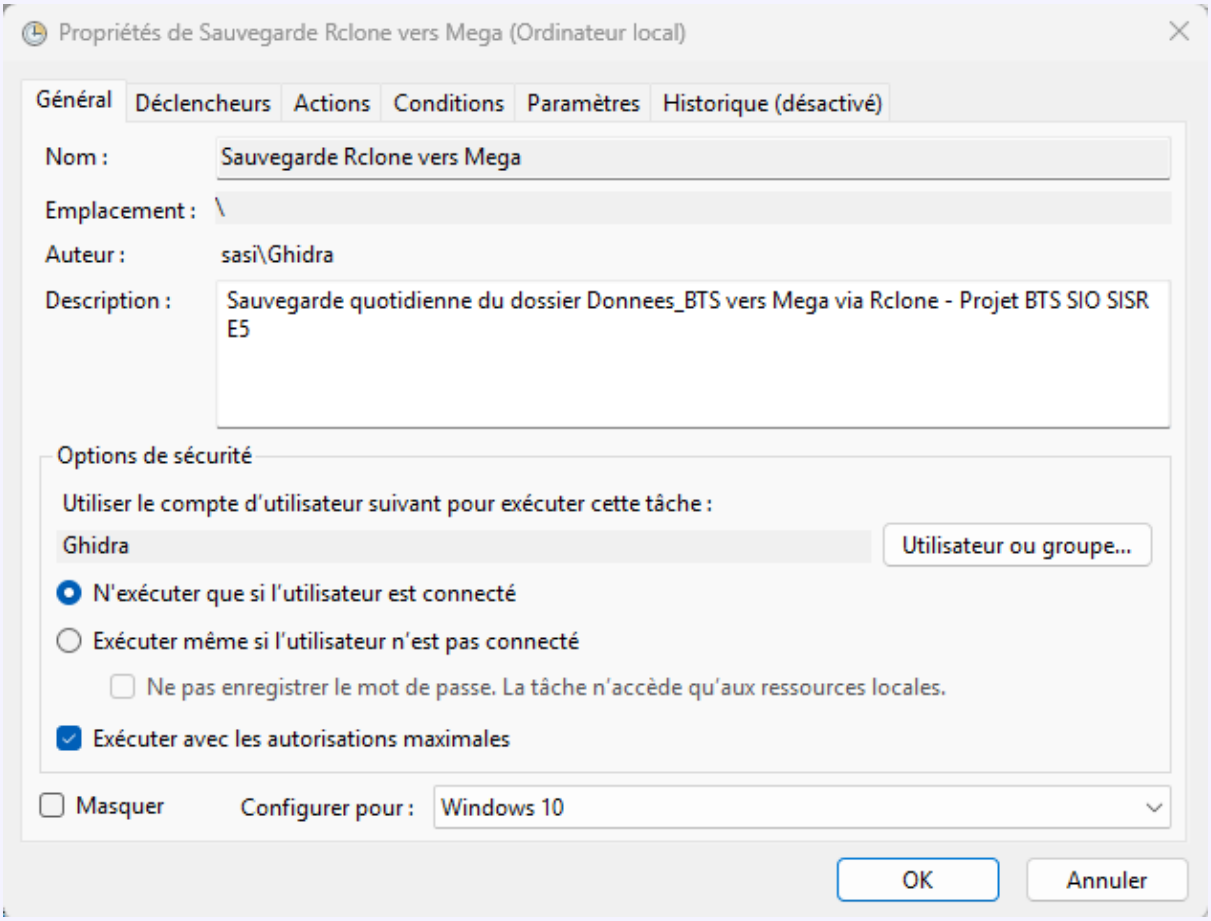


Assistant de création de tâche — résumé de la tâche Sauvegarde Rclone vers Mega

Options avancées activées dans les propriétés de la tâche :

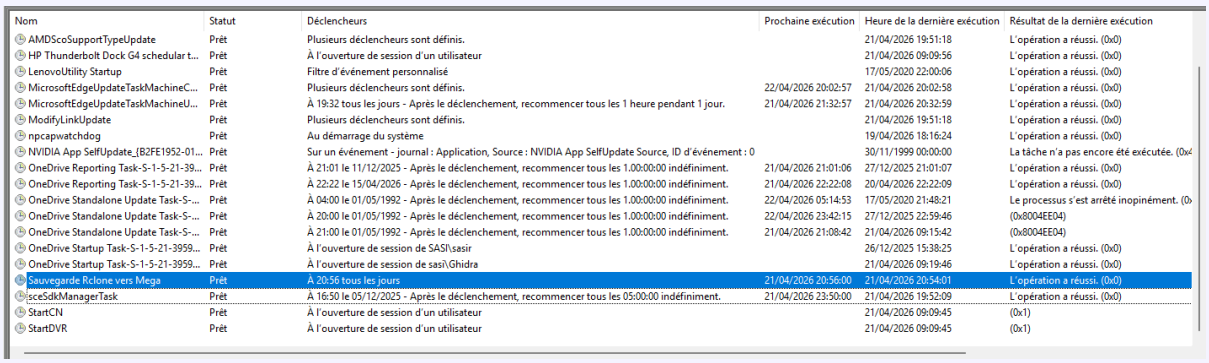
- Exécuter avec les autorisations maximales (droits administrateur).
- Réactiver l'ordinateur si celui-ci est en veille à l'heure programmée.
- Exécuter dès que possible si un démarrage planifié a été manqué (PC éteint à 23h).

- Ne pas limiter à l'alimentation secteur (la tâche doit aussi tourner sur batterie).



Propriétés de la tâche — onglet Général avec les options Exécuter avec autorisations maximales

Une exécution de test manuelle confirme que la tâche s'exécute correctement et remonte le statut L'opération a réussi (0x0) au Planificateur.



Nom	Statut	Déclencheurs	Prochaine exécution	Heure de la dernière exécution	Résultat de la dernière exécution
AMDScoSupportTypeUpdate	Prêt	Plusieurs déclencheurs sont définis.		21/04/2026 19:51:18	L'opération a réussi. (0x0)
HP Thunderbolt Dock G4 scheduler t...	Prêt	À l'ouverture de session d'un utilisateur		21/04/2026 09:09:56	L'opération a réussi. (0x0)
LenovoUtility Startup	Prêt	Filtre d'événement personnalisé		17/05/2020 22:00:06	L'opération a réussi. (0x0)
MicrosoftEdgeUpdateTaskMachineC...	Prêt	Plusieurs déclencheurs sont définis.	22/04/2026 20:02:57	21/04/2026 20:02:58	L'opération a réussi. (0x0)
MicrosoftEdgeUpdateTaskMachineU...	Prêt	À 19:32 tous les jours - Après le déclenchement, recommencer tous les 1 heure pendant 1 jour.	21/04/2026 21:32:57	21/04/2026 20:32:59	L'opération a réussi. (0x0)
ModifyLinkUpdate	Prêt	Plusieurs déclencheurs sont définis.		21/04/2026 19:51:18	L'opération a réussi. (0x0)
npcapwatchdog	Prêt	Au démarrage du système		19/04/2026 18:16:24	L'opération a réussi. (0x0)
NVIDIA App SelfUpdate_{B2FE1952-01...	Prêt	Sur un événement - journal : Application, Source : NVIDIA App SelfUpdate Source, ID d'événement : 0		30/11/1999 00:00:00	La tâche n'a pas encore été exécutée. (0x4
OneDrive Reporting Task-S-1-5-21-39...	Prêt	À 21:01 le 11/12/2025 - Après le déclenchement, recommencer tous les 1.00:00:00 indéfiniment.	21/04/2026 21:01:06	27/12/2025 21:01:07	L'opération a réussi. (0x0)
OneDrive Reporting Task-S-1-5-21-39...	Prêt	À 22:22 le 15/04/2026 - Après le déclenchement, recommencer tous les 1.00:00:00 indéfiniment.	21/04/2026 22:22:08	20/04/2026 22:22:09	L'opération a réussi. (0x0)
OneDrive Standalone Update Task-S-...	Prêt	À 04:00 le 01/05/1992 - Après le déclenchement, recommencer tous les 1.00:00:00 indéfiniment.	22/04/2026 05:14:53	17/05/2020 21:48:21	Le processus s'est arrêté inopinément. (0x
OneDrive Standalone Update Task-S-...	Prêt	À 20:00 le 01/05/1992 - Après le déclenchement, recommencer tous les 1.00:00:00 indéfiniment.	22/04/2026 23:42:15	27/12/2025 22:59:46	(0x8004EE04)
OneDrive Standalone Update Task-S-...	Prêt	À 21:00 le 01/05/1992 - Après le déclenchement, recommencer tous les 1.00:00:00 indéfiniment.	21/04/2026 21:08:42	21/04/2026 09:15:42	(0x8004EE04)
OneDrive Startup Task-S-1-5-21-3959...	Prêt	À l'ouverture de session de SASI\sasir		26/12/2025 15:38:25	L'opération a réussi. (0x0)
OneDrive Startup Task-S-1-5-21-3959...	Prêt	À l'ouverture de session de sasi\Ghidra		21/04/2026 09:19:46	L'opération a réussi. (0x0)
Sauvegarde Rclone vers Mega	Prêt	À 20:56 tous les jours	21/04/2026 20:56:00	21/04/2026 20:54:01	L'opération a réussi. (0x0)
sceSdkManagerTask	Prêt	À 16:50 le 05/12/2025 - Après le déclenchement, recommencer tous les 05:00:00 indéfiniment.	21/04/2026 23:50:00	21/04/2026 19:52:09	L'opération a réussi. (0x0)
StartCN	Prêt	À l'ouverture de session d'un utilisateur		21/04/2026 09:09:45	(0x1)
StartDVR	Prêt	À l'ouverture de session d'un utilisateur		21/04/2026 09:09:45	(0x1)

Bibliothèque du Planificateur de tâches — tâche Sauvegarde Rclone vers Mega en état Prêt avec Résultat : L'opération a réussi (0x0)

9. Bilan et compétences mobilisées

9.1 Bilan du projet

Le projet a été mené à son terme avec succès : la stratégie de sauvegarde 3-2-1 est pleinement opérationnelle et validée par deux tests de restauration. Les objectifs fixés en début de projet ont tous été atteints.

Objectif	Résultat
Protection contre les pannes matérielles	Atteint (3 copies sur 2 supports)
Protection contre les erreurs humaines	Atteint (historique GFS Duplicati)
Protection contre les sinistres locaux	Atteint (2 clouds hors site)
Protection contre les ransomwares	Partiellement atteint (chiffrement AES-256 mais pas d'air gap complet)
Automatisation complète	Atteint (Duplicati interne + Rclone via Task Scheduler)
Validation par test de restauration	Atteint (2 tests réussis, Duplicati et Rclone)

9.2 Limites et évolutions possibles

- Ajouter une 3e copie physique (disque USB chiffré ou NAS TrueNAS) pour atteindre une vraie 3-2-1 avec air gap.
- Mettre en place une alerte par e-mail en cas d'échec de sauvegarde (service SMTP externe ou sendmail).
- Chiffrer également la synchronisation Rclone avec le backend crypt pour une couche de chiffrement client supplémentaire.
- Étendre le périmètre aux VM du homelab (WINSRV-DC, SRV-GLPI, SRV-Zabbix) via Veeam Community Edition ou des scripts wbadmin et mysqldump.
- Intégrer la surveillance dans Zabbix : alerte si aucun fichier de sauvegarde récent (moins de 24 h) dans le partage Mega.

9.3 Compétences mobilisées

Ce projet a mobilisé plusieurs compétences du référentiel BTS SIO SISR :

Bloc	Compétence / sous-compétence mobilisée
Support et mise à disposition	Gérer le patrimoine informatique — Gérer les sauvegardes (C1.5)
Support et mise à disposition	Mettre à disposition des utilisateurs un service informatique — Déployer un service (C5.2)

Administration des systèmes et des réseaux	Installer et configurer un service — Installer et configurer des éléments d'infrastructure
Cybersécurité	Protéger les données — Chiffrement AES-256, principe du moindre privilège (OAuth)
Pilotage	Travailler en mode projet — Planification, jalons, livrables, tests

10. Annexes

10.1 Arborescence finale du projet

```
C:\
|-- Donnees_BTS\                <- Source des donnees
|   |-- Cours btssio revision\
|   |-- DOC EXAM\
|   `-- Portfolio maj\
|
|-- Restauration_Mega\          <- Cible de test de restauration
|   |-- Cours btssio revision\
|   |-- DOC EXAM\
|   `-- Portfolio maj\
|
|-- rclone\                     <- Binaire Rclone
|   `-- rclone.exe
|
`-- Scripts_Backup\              <- Scripts d'automatisation
    |-- backup_mega.bat
    `-- logs\
        `-- backup_mega_2026-04-21.log
```

10.2 Commandes Rclone essentielles

Commande	Rôle
rclone config	Configuration interactive d'un remote
rclone lsd mega:	Lister les dossiers à la racine du remote
rclone sync source dest	Synchronisation miroir (supprime les extras)
rclone copy source dest	Copie sans supprimer les fichiers existants
rclone check source dest	Vérifier les différences entre source et cible
rclone ls remote:path	Lister les fichiers avec leur taille

10.3 Ressources et documentation

- Documentation officielle Duplicati : duplicati.readthedocs.io
- Forum communautaire Duplicati : forum.duplicati.com
- Documentation officielle Rclone : rclone.org/docs
- Backend Rclone pour Mega : rclone.org/mega
- Site Mega.nz : mega.io

10.4 Glossaire

Terme	Définition
3-2-1	Règle de sauvegarde : 3 copies, 2 supports différents, 1 hors site
AES-256	Advanced Encryption Standard avec clé de 256 bits, norme industrielle de chiffrement symétrique
Air gap	Isolation physique d'un support de sauvegarde (déconnecté du réseau), protection contre les ransomwares
GFS	Grandfather-Father-Son : politique de rétention à trois niveaux (quotidien, hebdomadaire, mensuel)
OAuth 2.0	Protocole d'autorisation permettant à une application d'accéder à un service sans connaître le mot de passe
RPO	Recovery Point Objective : durée maximale acceptable de perte de données
RTO	Recovery Time Objective : durée maximale acceptable pour restaurer un service
WebDAV	Web-based Distributed Authoring and Versioning, extension HTTP pour la gestion de fichiers distants
Zero-knowledge	Architecture où le fournisseur du service ne peut pas lire les données stockées (chiffrement côté client)