RÉPUBLIQUE DU BÉNIN
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ D'ABOMEY-CALAVI

INSTITUT DE FORMATION ET DE RECHERCHE EN INFORMATIQUE

BP 526 Cotonou Tel : +229 21 14 19 88
http://www.ifri-uac.net Courriel : contact@ifri.uac.bj

MÉMOIRE

pour l'obtention du

Diplôme de Licence en Informatique

Option : Sécurité Informatique

Présenté par :
Déborah Priscillia Océane **GRIMAUD**

Mise en place d'un Système de Sauvegarde des Données à la Caisse Autonome de Gestion de la Dette

Sous la supervision :
M. Hervé **AKAKPO**

Membres du jury :

SANYA Max Fréjus Owolabi	Docteur	IFRI	Président
GOHOUE Rose	Ingénieur	IFRI	Examinatrice
AKAKPO Hervé	Ingénieur	IFRI	Rapporteur

Année Académique : **2023-2024**

Sommaire

Dédicace ii

Remerciements iii

Résumé iv

Abstract v

Table des figures vi

Liste des tableaux viii

Liste des acronymes ix

Glossaire 1

Introduction 2

1 Revue de littérature 4

2 Choix et présentation de la solution de sauvegarde 11

3 Déploiement de la solution de sauvegarde et test de fonctionnalités 20

Perspectives 42

Conclusion 43

Bibliographie 44

Webographie 45

Annexe 47

Table des matières 67

Dédicace

Je dédie ce mémoire à :

- Mon père Mathieu GRIMAUD ;
- Ma mère Léa ZOCLI ;
- Mon frère et ma sœur ;
- A toute ma famille et mes amis.

Remerciements

Je tiens à remercier tout d'abord le Seigneur pour sa protection, et pour m'avoir donné l'inspiration, la force ainsi que la volonté nécessaire pour la réalisation du mémoire. Je remercie aussi toutes les personnes qui ont contribué à rendre meilleur notre travail, notamment :

- Le professeur Eugène C. EZIN, Directeur de l'Institut de Formation et de Recherche en Informatique (IFRI) ;
- M. Hervé AKAKPO mon maître mémoire, enseignant à l'Institut de Formation et de Recherche en Informatique (IFRI) ;
- M. Jospy K. GOUDALO, informaticien à la Caisse Autonome de Gestion de la Dette, pour ses conseils et son assistance ;
- M. Yéssoufou LADJOHOUNLOU Chef du Service Infrastructures et Systèmes, mon maître de stage, pour ses divers apports ;
- Tout le corps professoral de l'IFRI, pour le savoir qu'ils nous ont transmis ;
- À toutes les personnes, de près ou de loin, qui m'ont permis de réaliser ce projet.

Résumé

Dans un contexte où la protection des données devient essentielle pour assurer la continuité des activités des entreprises, ce mémoire se concentre sur la mise en place d'un système de sauvegarde efficace et sécurisé. Le projet propose une solution Open-source Duplicati permettant à chaque utilisateur de gérer ses propres sauvegardes tout en garantissant la confidentialité et l'intégrité des données grâce à des mécanismes de chiffrement robustes. L'étude explore l'installation, la configuration et l'utilisation de Duplicati. Pour évaluer la résilience du système, une simulation de panne matérielle à été réalisée, entraînant une perte des données. Les résultats montrent que Duplicati, lorsqu'il est bien configuré, offre une solution fiable pour protéger les données contre les pertes accidentelles ou les cyberattaques. Ce mémoire met également en avant des recommandations pour améliorer la gestion et le suivi des sauvegardes dans un environnement professionnel.

Mots clés : système de sauvegarde, protection des données, cyberattaque

Abstract

In a context where data protection is becoming essential to ensure business continuity, this thesis focuses on the implementation of an efficient and secure backup system. The project offers an open-source Duplicati solution allowing each user to manage their own backups while guaranteeing the confidentiality and integrity of the data thanks to robust encryption mechanisms. The study explores the installation, configuration, and use of Duplicati. To assess the resilience of the system, a hardware failure simulation operation has been carried out, resulting in loss of data. The results show that Duplicati, when configured correctly, offers a reliable solution to protect data from accidental loss or cyberattacks. This thesis also highlights recommendations to improve the management and monitoring of backups in a professional environment.

Key words: backup system, data protection, cyberattacks

Table des figures

1.1 Sauvegardes complètes, différentielles et incrémentielles [6] 7

2.1 Script pour la planification des sauvegardes 12
2.2 Script pour l'éxécution des sauvegardes 12
2.3 Quelques backends de Duplicati 17
2.4 Système d'authentification à 2 facteurs [19] 18
2.5 Ancien logo 19
2.6 Nouveau logo 19

3.1 Téléchargement de Duplicati 20
3.2 Lancement de l'installation (1) 21
3.3 Lancement de l'installation (2) 21
3.4 Première connexion à l'interface 22
3.5 Dashboard de Duplicati 22
3.6 Sous-menu "ajouter une nouvelle sauvegarde" 23
3.7 Sous-menu "restaurer" 23
3.8 Sous-menu "paramètres" 24
3.9 Sous-menu "à propos" 24
3.10 Authentification par Google (1) 25
3.11 Authentification par Google (2) 25
3.12 Authentification par Google (3) 26
3.13 QR Code 26
3.14 Accès à duplicati 27
3.15 Configuration d'une nouvelle sauvegarde 27
3.16 Paramètres généraux de la nouvelle sauvegarde 28
3.17 Choix de la destination 29
3.18 Connexion au backend réussie 29
3.19 Choix des données sources 30
3.20 Planification de la sauvegarde 31
3.21 Options générales de sauvegarde 32
3.22 Nouvelle sauvegarde configurée 32
3.23 Jeu de sauvegarde de "Sauvegarde" 33
3.24 Choix de démarrage de la sauvegarde (1) 33
3.25 Choix de démarrage de la sauvegarde (2) 34
3.26 Sauvegarde réussie (1) 34
3.27 Sauvegarde réussie (2) 35
3.28 Sauvegardes effectuées au départ 35

3.29 Choix de la restauration 36
3.30 Emplacement de la sauvegarde 37
3.31 Connexion fonctionnelle 37
3.32 Chiffrement 38
3.33 Sélection des fichiers à restaurer 39
3.34 Options de restauration 39
3.35 Réussite de la restauration 40
3.36 Emplacement de la sauvegarde (Google Drive) 40
3.37 Données restaurées avec succès 41

Liste des tableaux

1.1 Tableau comparatif de quelques solutions de sauvegarde de données 9

Liste des acronymes

2FA :

2 Facteurs 5, 67

EFS :

Encrypted File System 12

FTP :

File Transfer Protocol 7

NAS :

Network Attached Storage 7

SFTP :

SSH File Transfer Protocol 7

SSD :

Solid State Drive 7

SSH :

Secure Shell 35

TCP :

Transmission Control Protocol 14

USB :

Universal Serial Bus 7

VPS :

Virtual Private Server 7

Glossaire

AuthID : Identifiant utilisé pour autoriser l'accès aux services de stockage cloud dans Duplicati. 40

Backend : Service ou emplacement où sont stockées les sauvegardes. 16, 68

Cryptage AES-256 : Le cryptage AES-256 est un algorithme symétrique qui utilise une clé de 256 bits pour convertir des données lisibles en un texte chiffré hautement sécurisé et quasi-indéchiffrable sans la clé appropriée. 14

Open-source : Logiciel dont le code source est accessible à tous, permettant ainsi à quiconque de le modifier, de l'améliorer ou de l'utiliser gratuitement. iv

Processus : Programme en cours d'exécution. 15

Introduction Générale

Les données sont le moteur de toute entreprise. Perdre ces données, que ce soit à cause d'une panne, d'une cyberattaque ou d'une erreur humaine, peut gravement affecter les activités de l'entreprise. Pour éviter des conséquences désastrueuses, il est indispensable de mettre en place un système de sauvegarde fiable.

Contexte et justification

Les organisations et les entreprises sont confrontées depuis toujours à diverses menaces telles que les cyberattaques, les pannes matérielles, les catastrophes naturelles et les erreurs humaines qui affectent principalement leurs données au cœur de toutes les opérations, provoquant plusieurs dégâts irrémédiables si elles n'ont pas été bien préparées pour réagir face à ces incidents. Nombreuses sont celles qui se retrouvent en difficulté ou font même faillite dans les deux années suivant le sinistre. On assiste par exemple à des cas d'entreprises qui, après une attaque par ransomware, ont dû payer des millions afin de récupérer leurs données, sans oublier l'arrêt des activités entraînant une baisse de productivité, la perte des revenus, l'atteinte à la réputation etc. Ainsi, selon une étude de Comparitech (un site web qui aide ses lecteurs du monde entier à améliorer leur cybersécurité et protéger leur vie privée en ligne), plus de 5 400 attaques par ransomware ont eu lieu sur l'année 2024 et plus de 195,4 millions de données ont été compromises avec le montant des rançons payés qui s'est élevé à 133,5M$ pour un montant moyen de 3,5M$ [1]. C'est dans ce contexte que des mesures comme les solutions de sauvegarde de données efficaces doivent être mises en place au préalable pour assurer la reprise après sinistre et garantir ainsi la continuité des activités.

Problématique

La Caisse Autonome de Gestion de la Dette (CAGD) dispose d'un système de sauvegarde de données déployé sur les postes de chaque utilisateur. Ce système repose sur un script qui planifie et exécute les sauvegardes des différents postes de l'entreprise. Cependant, avec l'augmentation des cyberattaques par exemple, son efficacité et sa capacité à répondre aux exigences actuelles en matière de protection des données sont remises en question. On s'interroge alors sur les stratégies et solutions de sauvegarde modernes et efficaces à mettre en place pour minimiser les risques de perte de données critiques et assurer la continuité des opérations de l'entreprise sans engager de dépenses.

Objectifs

L'objectif général de ce projet est de mettre en place un système de sauvegarde de données gratuit, efficace, sécurisé et automatisé pour garantir la protection et la récupération rapide des données critiques d'une entreprise en cas de sinistre. Les objectifs spécifiques consistent à :

- Mettre en place un système de sauvegarde sécurisé et automatisé
- Assurer la sécurité des données par le biais de mécanismes de chiffrement.
- Définir une politique de sauvegarde en fonction des exigences de l'entreprise
- Tester la solution pour s'assurer de son efficacité et de sa capacité à restaurer des données en cas de perte.

Structuration du mémoire

Le document est organisé en trois chapitres. Le premier chapitre est consacré à la revue de littérature. Puis, nous présentons dans le deuxième chapitre le choix de l'outil de sauvegarde ainsi qu'une étude détaillée de celui-ci. Enfin, le chapitre trois aborde le déploiement de l'outil et les tests effectués.

Chapitre 1

Revue de littérature

Introduction

La sauvegarde des données joue un rôle fondamental dans la gestion des systèmes d'information. Ainsi, face aux menaces croissantes telles que les cyberattaques principalement les attaques par ransomware, les erreurs humaines ou les pannes matérielles, il est essentiel de disposer de mécanismes robustes pour assurer la sécurité et la disponibilité des informations critiques. Ce chapitre explore les concepts clés de la sauvegarde des données ainsi que les solutions existantes, afin d'établir une base théorique pour la mise en œuvre d'un système adéquat.

1.1 Définitions

1.1.1 Système d'Information

Un Système d'Information (SI) est un ensemble organisé de ressources (matérielles, logicielles, humaines, données et procédures) permettant de collecter, traiter, stocker et diffuser des informations au sein d'une organisation. Il a pour objectif de soutenir les activités de l'entreprise, d'améliorer la prise de décision et de garantir une communication efficace.

1.1.2 Protection des données

La protection des données désigne un ensemble de pratiques, de technologies et de mesures mises en place pour assurer la confidentialité, l'intégrité et la disponibilité des données, qu'elles soient stockées, transmises ou utilisées. Cette protection est essentielle pour éviter la perte, la corruption, l'accès non autorisé ou l'exploitation abusive des informations. Elle concerne tous types de données : personnelles, professionnelles, sensibles, etc.

1.1.3 La restauration des données

La récupération des données (ou restauration des données) est une opération informatique qui consiste à retrouver les données perdues à la suite d'une erreur humaine, une défaillance matérielle, une défaillance logicielle d'un programme ou d'un système d'exploitation, un accident ou au moment op-

portun d'un test de récupération de données définie dans une procédure de stratégie de sauvegarde et d'archive (également appelé plan de sauvegarde) [2].

1.1.4 L'automatisation des sauvegardes

L'automatisation des sauvegardes désigne l'utilisation de logiciels ou de systèmes pour planifier et exécuter les sauvegardes sans intervention manuelle. Cela permet de garantir que les données sont sauvegardées régulièrement, selon un calendrier prédéfini, et réduit le risque d'oubli ou d'erreur humaine.

1.1.5 L'authentification 2FA

L'authentification à 2 facteurs (2FA) est une méthode de sécurité basée sur la gestion des identités et accès qui impose deux formes d'identification pour accéder aux ressources et données. Elle permet aux entreprises de surveiller et protéger leurs informations et réseaux les plus vulnérables. Modules de sécurité matériels, vérification par sms, notification push, authentification vocale [3].

1.2 Les cyberattaques

1.2.1 Définition

Une cyberattaque désigne des actions coordonnées par voie numérique qui visent les systèmes d'information ou les données qui y sont hébergées. Son objectif est de porter atteinte à la disponibilité des services ou des informations, à leur intégrité ou leur confidentialité.

1.2.2 Types de cyberattaques

Il existe beaucoup de cyberattaques notamment les plus courantes en entreprise telle que :[4]

- Un malware est un logiciel malveillant. Il est développé dans le but de nuire aux utilisateurs du matériel informatique. Il peut être utilisé pour voler des données personnelles ou sensibles, les chiffrer ou les supprimer, ou bien pour espionner l'activité de l'entreprise.
- L'hameçonnage, ou phishing consiste à se faire passer auprès d'un employé de l'entreprise comme un tiers de confiance.
- Le ransomware, ou rançongiciel en français, est un type de malware ou logiciel informatique malveillant, prenant en otage les données. Le ransomware chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange de la clé permettant de les déchiffrer.
- Les attaques par déni de service distribué ou DDoS rendent inaccessibles les serveurs. Ce type de cyberattaque consiste en l'envoi de multiples requêtes pour saturer le service.
- L'anarque au président ou l'arnaque aux faux ordres de virement repose sur un appel ou un courriel dans lequel un tiers se fait passer pour le président d'un groupe ou d'une société mère. Ce dernier exige alors un virement international.
- L'attaque par force brute a pour but de trouver un mot de passe en testant des milliards de combinaisons en quelques secondes.

- Le cryptojacking est une forme particulière de malware. Son rôle est de détourner la puissance des processeurs de vos appareils informatiques pour procéder au minage de crypto-monnaies.
- etc.

1.3 La sauvegarde des données

1.3.1 Définition

Une sauvegarde de données est une copie des données de votre système, de votre configuration ou de votre application, stockée séparément des données d'origine.
La sauvegarde des données est une fonction de protection des données essentielles pour réduire le risque de perte totale ou partielle des données en cas d'événements imprévus tels que des catastrophes naturelles, des erreurs humaines, des événements de sécurité ou des défaillances de systèmes. Elle offre aux organisations la possibilité de restaurer les systèmes et les applications dans un état antérieur souhaité [5].

- Une donnée peut être des fichiers, des bases de données, des documents, ou tout autre type d'information utilisée dans des applications diverses.

1.3.2 Principaux types de sauvegarde

Complète : Ce processus consiste à transférer toutes les données stockées sur un système de production dans un système de sauvegarde pour les conserver en toute sécurité. Les sauvegardes complètes protègent chaque octet de données de tout serveur, toute base de données, machine virtuelle (VM) ou source de données connectés au réseau. Ces sauvegardes peuvent prendre plusieurs heures, voire plusieurs jours, en fonction de la quantité de données à sauvegarder. Plus une solution de gestion des données est moderne, moins les sauvegardes complètes sont nombreuses, et lorsque cela s'avère nécessaire, plus elle est rapide.

Incrémentielle : Une sauvegarde incrémentielle capture uniquement les nouvelles données depuis la dernière sauvegarde incrémentielle complète. Cependant, une sauvegarde complète est nécessaire avant qu'une solution de sauvegarde puisse effectuer sa première sauvegarde incrémentielle. Par la suite, la sauvegarde peut être automatisée sur la base du dernier incrément.

Différentielle : Comme les sauvegardes incrémentielles, la quantité de données sauvegardées est évaluée à partir de la dernière sauvegarde complète et non de la dernière sauvegarde incrémentielle. Considérez cette sauvegarde comme ce qui est différent depuis la dernière fois que vous avez effectué une sauvegarde. Là encore, cela ne peut se produire que si une sauvegarde complète a été effectuée au préalable. En général, les organisations définissent des stratégies quant à la quantité de données à sauvegarder et le moment où les sauvegardes incrémentielles ou différentielles doivent être effectuées.

La Figure 1.1 illustre clairement les principaux types de sauvegarde tels que décrits plus haut.

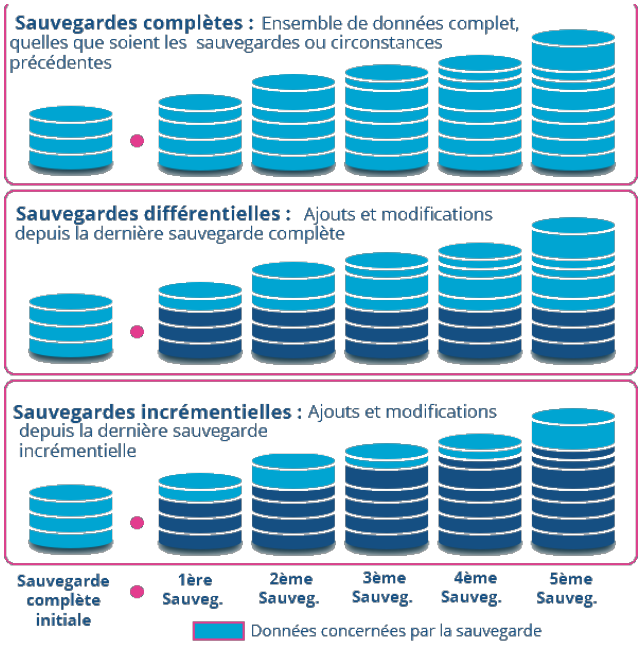


FIGURE 1.1 : Sauvegardes complètes, différentielles et incrémentielles [6]

1.3.3 Modes de stockage des sauvegardes

Les sauvegardes peuvent être stockées sur différents types de supports :

1.3.3.1 Stockage local

Le stockage local consiste à sauvegarder les données sur des supports physiques situés à proximité de vos systèmes principaux, tels que des disques durs externes, des clés USB ou des SSD. Il offre une solution rapide et économique pour accéder aux données sauvegardées sans dépendre d'Internet. Cependant, il présente des risques en cas de sinistre local, comme un incendie ou un vol, qui pourraient entraîner la perte de toutes les copies. Ce mode est idéal pour des sauvegardes fréquentes ou de petite taille, mais nécessite une gestion prudente pour éviter les risques liés à un stockage unique.

Stockage sur le serveur local (NAS ou réseau partagé) : Le stockage sur serveur local, tel qu'un NAS ou un partage réseau, consiste à centraliser les sauvegardes sur un serveur ou un dispositif dédié, accessible via un réseau local. Ce mode permet de stocker les données de plusieurs appareils en un seul endroit, facilitant ainsi la gestion et l'automatisation des sauvegardes. Accessible à tous les utilisateurs du réseau, cette solution est idéale pour les entreprises ou les foyers avec plusieurs appareils à sauvegarder. Toutefois, elle reste vulnérable aux sinistres locaux et nécessite des précautions supplémentaires, comme des sauvegardes hors site pour garantir une protection maximale.

1.3.3.2 Stockage distant

Le stockage distant implique de transférer les données vers un serveur situé dans un autre emplacement géographique, souvent via Internet. Cela peut inclure des solutions comme un serveur VPS, un NAS distant ou un serveur configuré pour recevoir des sauvegardes via SFTP ou FTP. Ce mode protège vos données contre les catastrophes locales, car elles sont stockées hors site. Bien qu'il améliore la sécurité, il peut être limité par la bande passante disponible et engendrer des coûts récurrents pour l'hébergement ou le transfert des données. Ce mode est recommandé pour des sauvegardes critiques ou pour assurer une redondance maximale.

1.3.3.3 Stockage hybride

Le stockage hybride combine les avantages du stockage local et distant pour une protection optimale. Les données sont d'abord sauvegardées localement pour un accès rapide et des restaurations fréquentes, puis copiées sur un serveur distant ou dans le cloud pour se prémunir contre les sinistres locaux. Cette approche assure une redondance maximale et s'adapte à différents scénarios. Cependant, elle peut être plus complexe à configurer et nécessite une planification pour gérer les sauvegardes sur deux environnements. Le stockage hybride est particulièrement adapté aux entreprises ou aux utilisateurs qui souhaitent une solution complète et fiable.

1.4 Différence entre stockage de données et sauvegarde de données

Le stockage est utilisé pour un accès régulier et rapide aux données nécessaires aux opérations quotidiennes, tandis que la sauvegarde est destinée à protéger les données en cas de perte ou de corruption. Les données stockées doivent être accessibles fréquemment et rapidement. En revanche, les sauvegardes ne sont généralement consultées qu'en cas de besoin de restauration, donc moins fréquemment [7].

1.5 Solutions de sauvegarde existantes

1.5.1 Quelques solutions de sauvegarde

- **Veeam Agent Free** est un logiciel de sauvegarde et de récupération de données pour Windows, Linux et macOS qui permet de sauvegarder des fichiers, des disques ou des systèmes complets et de récupérer des données en cas de sinistre [8].
- **EaseUS Todo Backup Free** est une solution de sauvegarde de données de haute volée, assurant la protection des données optimale pour chaque besoin [9].
- **Duplicati** est un logiciel de sauvegarde qui dispose de plusieurs fonctionnalités qui en font une solution de sauvegarde attrayante, notamment sa capacité à chiffrer les sauvegardes et son support pour les sauvegardes incrémentielles.
- **FBackup** propose à ses utilisateurs professionnels et non professionnels de mettre en place la sauvegarde automatique de leurs données [12].
- **Iperius Backup** est un logiciel de sauvegarde et de restauration de données. Dans sa version gratuite, l'outil est destiné au grand public et propose de nombreuses fonctionnalités qui vous permettront de réaliser vos sauvegardes rapidement et efficacement.

1.5.2 Comparaisons

Nous avons présenté dans le Tableau 1.1 une comparaison entre 5 solutions de sauvegarde gratuites et les plus utilisées.

TABLE 1.1 : Tableau comparatif de quelques solutions de sauvegarde de données

Solutions	Fonctionnalités	Limites
Veeam Agent Free [17]	• Sauvegarde fiable pour postes de travail et serveurs physiques/virtuels • Restauration granulaire rapide • Planification automatique • Sauvegardes complète et incrémentielle	• Fonctionnalités avancées réservées à la version payante (configuration d'une seule tâche pour la version gratuite) • Compatibilité cloud limitée
EaseUS Todo Backup Free [14]	• Clonage de disque et migration système • Sauvegarde complète, incrémentielle et différentielle • Planification automatique • Interface utilisateur intuitive	• Certaines fonctions réservées à la version payante • Compatibilité cloud absente dans la version gratuite
Duplicati [11]	• Compatibilité cloud étendue : Google Drive, Dropbox, OneDrive, Amazon S3, Backblaze B2, FTP, WebDAV, etc. • Chiffrement AES-256 intégré • Open Source et totalement gratuit • Sauvegarde incrémentielle et complète + déduplication • Planification avancée • Interface web intuitive • Multiplateforme : Windows, Linux, macOS • Conservation intelligente des sauvegardes • Restauration flexible (partielle ou complète)	• Interface limitée • Configuration avancée : peut être complexe pour les novices
FBackup [15]	• Sauvegarde locale, réseau et cloud (Google Drive, Dropbox) • Planification automatique basique • Interface simple • Compression ZIP • Sauvegrde complète et miroir	• Compatibilité cloud limitée (Google drive et Dropbox uniquement)
Iperius Backup Free [13]	• Sauvegarde sur plusieurs supports : USB, NAS, FTP, réseau • Planification automatique • Sauvegarde complète, incrémentielle et différentielle • Notifications par e-mail	• Pas de support technique • Fonctionnalités cloud limitées pour cette version • Aucune gestion avancée des restaurations

Conclusion

Ce chapitre nous a permis de présenter les généralités sur la sauvegarde des données ainsi que des mécanismes qui l'entourent et de faire une comparaison de quelques solutions de sauvegarde existantes. Dans le chapitre suivant, nous avons fait le choix de la solution de sauvegarde qui répond le mieux à nos besoins puis nous l'avons présenté.

Chapitre 2

Choix et présentation de la solution de sauvegarde

Introduction

La sauvegarde des données est essentielle pour garantir leur sécurité et leur disponibilité. Ce chapitre a pour objectif de présenter tout d'abord la Caisse Autonome de Gestion de la Dette (CAGD) et son système de sauvegarde, puis la raison du choix de notre solution, ses fonctionnalités ainsi que ses caractéristiques.

2.1 Présentation de la Caisse Autonome de Gestion de la Dette (CAGD) et de son système de sauvegarde de données

2.1.1 Présentation de la Caisse Autonome de Gestion de la Dette (CAGD)

La Caisse Autonome d'Amortissement (CAA) a été instituée par l'ordonnance N° 28/PR/MFAE du 03 août 1966 portant création de la Taxe Spéciale d'Amortissement (TSA). Depuis lors, les textes ré gissant l'institution, ses objectifs et attributions ont évolué avec le développement socio-économique du Bénin ainsi que l'évolution du contexte financier international. Par ailleurs, pour que son nom reflète mieux ses activités et son importance dans le système des finances publiques béninois, d'une part et pour d'avantage promouvoir le Bénin comme un modèle de gestion transparente, innovante, proactive et diversifiée de la dette publique, la CAA a changé de dénomination le 12 juillet 2023 et est devenue la Caisse Autonome de Gestion de la Dette (CAGD) du Bénin. Placée sous la tutelle du Mi nistère de l'Économie et des Finances (MEF), la CAGD est l'organisme chargé de la mobilisation des ressources de financement et de la bonne gestion de la dette publique et de la politique économique de l'État béninois [18].

2.1.2 Présentation du système de sauvegarde de données de la CAGD

Le système de sauvegarde de données existant à la CAGD repose sur 2 scripts dont l'un relatif à la planification des sauvegardes et le second à l'execution des sauvegardes. Ces scripts sont déployés

sur les postes de chaque utilisateur. Le premier script illustré par la Figure 2.1, planifie les sauvegardes tous les mardis et vendredis à 17 heures. Le second script illustré par la Figure 2.2, copie des données spécifiques de chaque poste vers leurs destinations respectives. En effet, ce script utilise la commande `xcopy` pour copier les fichiers récents ou récemment modifiés tout en poursuivant la copie même en cas d'erreur. De plus, si les fichiers sont chiffrés avec EFS, ils sont déchiffrés avant d'être sauvegardés sur le serveur distant, au cas où celui-ci ne serait pas compatible avec le chiffrement EFS. Les fichiers concernés sont ceux ayant des extensions spécifiques telles que `.doc`, `.docx`, `.xls`, `.xlsx`, `.pdf`, `.ppt`, `.pptx`. Ces fichiers sont sauvegardés respectivement dans des emplacements dédiés à chaque utilisateur et dans des répertoires spécifiques.

```
# Pour remplacer tous fichiers de sauvegardes existants par le fichier sauvegarde-fichier.bat
sur le poste de l'utilisateur
set currentpath=%~dp0
IF EXIST %systemdrive%\sauvegarde-fichier.bat GOTO fichier_existe
:fichier_existe
attrib -H %systemdrive%\sauvegarde-fichier.bat
del %systemdrive%\sauvegarde-fichier.bat

xcopy "%currentpath%sauvegarde-fichier.bat" "%systemdrive%\sauvegarde-fichier.bat"
attrib +H %systemdrive%\sauvegarde-fichier.bat
pause

# Pour supprimer toutes tâches de sauvegardes existantes puis créer une nouvelle pour le
fichier sauvegarde-fichier.bat sur le poste de l'utilisateur
SCHTASKS /delete /TN sauvegarde /f
SCHTASKS /Create /SC WEEKLY /D MAR,VEN /TN sauvegarde /TR "%systemdrive%\sauvegarde-
fichier.bat" /ST 17:00

# Démarrer la sauvegarde
schtasks /run /tn sauvegarde
pause
```

FIGURE 2.1 : Script pour la planification des sauvegardes

```
@echo off

# Pour copier les fichiers spécifiés depuis le répertoire "Desktop" de l'utilisateur vers son
répertoire spécifique sur le serveur de sauvegarde
SET destination="\\172.16.0.13\F\%Username%\Bureau\"

CD %UserProfile%\Desktop
xcopy *.doc %destination% /c /D /Y/g /s /J
xcopy *.docx %destination% /c /D /Y/g /s /J
xcopy *.xls %destination% /c /D /Y/g /s /J
xcopy *.xlsx %destination% /c /D /Y/g /s /J
xcopy *.pdf %destination% /c /D /Y/g /s /J
xcopy *.ppt %destination% /c /D /Y/g /s /J
xcopy *.pptx %destination% /c /D /Y/g /s /J

# Pour copier les fichiers spécifiés depuis le répertoire "Mes documents" de l'utilisateur
vers son répertoire spécifique sur le serveur de sauvegarde
CD %UserProfile%\Documents
SET destination="\\172.16.0.13\F\%Username%\Mes documents\"
xcopy *.doc %destination% /c /D /Y/g /s /J
xcopy *.docx %destination% /c /D /Y/g /s /J
xcopy *.xls %destination% /c /D /Y/g /s /J
xcopy *.xlsx %destination% /c /D /Y/g /s /J
xcopy *.pdf %destination% /c /D /Y/g /s /J
xcopy *.ppt %destination% /c /D /Y/g /s /J
xcopy *.pptx %destination% /c /D /Y/g /s /J
```

FIGURE 2.2 : Script pour l'éxécution des sauvegardes

• **Avantages**

Ce système présente plusieurs avantages, notamment la sauvegarde des fichiers importants afin d'optimiser l'espace de stockage, la planification automatique des sauvegardes, ainsi que la gestion des fichiers volumineux grâce à l'option `/J`, qui permet de copier des fichiers sans utiliser de mémoire tampon, ce qui est idéal pour les fichiers très lourds.

• **Inconvénients**

Cependant, il convient de noter certains inconvénients, tels que l'absence de gestion des erreurs lors d'une sauvegarde, la non vérification de l'intégrité des données après la sauvegarde, l'absence de chiffrement des sauvegardes, une gestion du stockage pas assez optimale avec les fichiers qui sont sauvegardés tels quels, la non redondance des sauvegardes.

Bien que ce système offre de nombreux avantages, il présente également beaucoup d'inconvénients cités ci-dessus qui nous incitent à privilégier des solutions plus modernes et qui répondent mieux à nos besoins.

2.2 Choix de la solution

La CAGD dispose d'un système de sauvegarde basé sur des scripts, qui pose des limites en termes de sécurité, de gestion et de flexibilité. Son objectif est donc de mettre en place un système plus moderne sans engager de dépenses, en s'appuyant sur des solutions de sauvegarde gratuites alternatives aux options commerciales coûteuses, et offrant des fonctionnalités garantissant la reprise après sinistre et la continuité des activités. D'après le tableau comparatif 1.1, Duplicati apparaît comme une solution adaptée aux exigences de la CAGD, en étant gratuite et open-source et grâce à ses fonctionnalités avancées : interface web intuitive facilitant son utilisation, compatibilité avec plusieurs destinations de sauvegarde, chiffrement AES pour la sécurisation des sauvegardes, planification et automatisation des sauvegardes, ainsi que la compression des sauvegardes afin d'optimiser l'espace de stockage.

2.3 Présentation de Duplicati

2.3.1 Généralité

Duplicati est un logiciel de sauvegarde qui planifie et stocke une copie complète ou incrémentielle des fichiers à conserver. La copie de sauvegarde peut être compressée, chiffrée et stockée localement, en ligne, depuis des services de cloud computing ou vers des serveurs de fichiers distants. Duplicati supporte les différents services de sauvegarde en ligne comme OneDrive, Amazon S3, Rackspace, Cloud Files, Tahoe LAFS et Google Drive, mais aussi tous les serveurs qui prennent en charge SFTP, WebDAV ou FTP.

2.3.2 Composant de Duplicati

Le serveur : Lorsque le serveur Duplicati est démarré, Duplicati peut effectuer des tâches en arrière-plan, comme effectuer des sauvegardes, effectuer des opérations de restauration et effectuer

des tâches de maintenance.
La partie serveur dispose d'un planificateur intégré pour démarrer automatiquement les tâches de sauvegarde à intervalles réguliers.
Pour configurer de nouvelles tâches de sauvegarde (ou modifier des tâches existantes), modifier les paramètres et surveiller les sauvegardes en cours, un serveur Web est inclus dans le composant serveur.
Si le composant serveur démarre, le webservice écoute sur l'interface de bouclage, ce qui le rend accessible uniquement à partir de l'hôte local. Le serveur tente de démarrer l'écoute sur le port TCP 8200. Si ce port n'est pas disponible (en raison d'une autre instance de serveur Duplicati en cours d'exécution ou d'un autre processus qui utilise le port 8200), le port 8300 sera essayé, augmentant jusqu'à ce qu'un port inutilisé soit trouvé. Le port et l'interface peuvent être personnalisés en spécifiant certains paramètres de ligne de commande [10].

Les outils de ligne de commande : Duplicati peut effectuer des sauvegardes sans charger le composant serveur, en utilisant les outils de ligne de commande. Pour planifier des sauvegardes sans utiliser le composant serveur, presque tous les planificateurs de tâches peuvent être utilisés, par exemple le planificateur de tâches Windows (Windows) ou Cron (Linux).
D'autres outils en ligne de commande peuvent aider aux opérations de restauration, à la récupération de fichiers à partir de sauvegardes corrompues, à l'installation du composant serveur en tant que serveur, à l'analyse de la communication avec les backends ou à la mise à jour du logiciel [10].

L'icône de la barre d'état : Lorsqu'il est démarré, l'outil Icône de la barre d'état des doublons crée une petite icône dans la barre d'état système pour faciliter l'accès à l'interface Web des doublons. Le composant serveur est inclus dans l'outil Icône de la barre d'état. Après une installation par défaut, l'outil Icône de la barre d'état sera automatiquement démarré après la connexion d'un utilisateur, ce qui rend inutile la configuration du composant serveur dans un cas d'utilisation quotidien [10].

Le service : Fondamentalement, il s'agit du même composant que le serveur Duplicati, mais il s'exécute en tant que service Windows. Si Duplicati est enregistré en tant que service Windows, un petit agent démarre le composant serveur et envoie une requête ping au serveur pour vérifier qu'il est en cours d'exécution. Si le composant serveur est inaccessible, l'agent le redémarre [10].

2.3.3 Fonctionnalités

Duplicati possède de nombreuses fonctionnalités avancées telles que : [11]

- Utilise un Cryptage AES-256 fort pour protéger les sauvegardes. Il est conçu selon le principe TNO (Trust No One) : Ne faites confiance à personne. Par exemple, toutes les données sont cryptées localement avant d'être transférées vers le système de stockage distant ;
- Effectue initialement une sauvegarde complète. Ensuite, Duplicati met à jour la sauvegarde initiale en ajoutant uniquement les données modifiées : sauvegarde incrémentielle. Cela permet d'économiser du temps et de l'espace, et la taille de la sauvegarde augmente généralement lentement ;

- Compression : Toutes les données de sauvegarde sont compressées avant d'être chiffrées et téléchargées. Duplicati prend en charge la compression Zip/Deflate ou 7z/LZMA2. Pour des raisons de performances, Duplicati détecte les fichiers déjà compressés et les ajoute tels quels aux archives Zip ou 7z. Par exemple, les fichiers multimédias tels que les fichiers mp3, jpeg ou mkv contiennent déjà des données très bien compressées ;

- Déduplication : Analyse le contenu des fichiers et stocke les blocs de données. Pour cette raison, Duplicati trouvera les fichiers en double et le contenu similaire et ne les stockera qu'une seule fois dans la sauvegarde. Comme Duplicati analyse le contenu des fichiers, il peut très bien gérer les situations si les fichiers et les dossiers sont déplacés ou renommés. Comme le contenu ne change pas, la prochaine sauvegarde sera minuscule ;

- Conçu pour gérer différents types de problèmes : problèmes de réseau, sauvegardes interrompues, systèmes de stockage indisponibles ou corrompus. Même si une exécution de sauvegarde a été interrompue, elle peut être poursuivie ultérieurement. Duplicati sauvegardera alors tout ce qui a été manqué lors de la dernière sauvegarde. Et même si les fichiers distants sont corrompus, Duplicati peut essayer de les réparer si les données locales sont toujours présentes ou restaurer autant que possible ;

- Interface web : Duplicati est livré avec une interface web. Il peut être utilisé pour configurer et exécuter des sauvegardes sur la machine locale. Mais il permet également de configurer et d'exécuter des sauvegardes à distance sur des machines sans tête comme un NAS ;

- Duplicati offre toutes les fonctions et caractéristiques via Duplicati.Commandline.exe. Cela permet d'ajouter des fonctionnalités de sauvegarde aux scripts ou d'exécuter des sauvegardes dans une fenêtre de terminal ;

- Duplicati stocke également les métadonnées des fichiers dans la sauvegarde. Lorsque les fichiers de sauvegarde sont restaurés, les horodatages (dernière modification, création) seront également restaurés ainsi que les autorisations d'accès au système. Pour éviter les fichiers inaccessibles, par exemple lorsque l'utilisateur du système a changé, la restauration des autorisations d'accès est facultative ;

- Le planificateur intégré exécute automatiquement les sauvegardes aux heures et aux intervalles définies. Une sauvegarde tous les jours, le week-end, toutes les heures ou même 15h tous les 3èmes lundis est possible. Et même si une date n'est pas respectée, Duplicati exécutera le travail dans les plus brefs délais ;

- Mise à jour automatique : Duplicati est livré avec un programme de mise à jour intégré qui télécharge et installe la dernière version disponible . De cette façon, on peut facilement garder Duplicati à jour ;

- Lorsqu'un fichier est utilisé par un Processus ou une application, il ne peut généralement pas être lu par un autre processus, ce qui rend impossible la sauvegarde de ce fichier. Les services VSS (Volume Shadow Copy services) sur les systèmes Windows et LVM (Logical Volume Manager) sur les systèmes Linux sont utilisés par Duplicati pour effectuer une sauvegarde fiable de ces fichiers ouverts.

Duplicati est une solution de sauvegarde basée sur des blocs. Les fichiers sont divisés en petits blocs de données , qui sont éventuellement chiffrés et compressés avant d'être envoyés à l'emplacement de sauvegarde. Dans l'emplacement de sauvegarde, Duplicati télécharge non pas les fichiers originaux, mais les fichiers contenant des blocs de fichiers originaux et d'autres données nécessaires qui permettent à Duplicati de restaurer les fichiers stockés dans leur forme d'origine par le processus de restauration. Ce système de sauvegarde basé sur des blocs permet des fonctionnalités telles que la gestion des versions de fichiers et la déduplication.

2.3.4 Destinations de sauvegarde ou Backend

Duplicati peut effectuer des sauvegardes vers un grand nombre de cibles. Pour les sauvegardes locales, tous les périphériques connectés localement ou à l'aide d'un chemin UNC (Universal Naming Convention) peuvent être utilisés, tels que :

- Disque dur externe
- Clé USB
- Dossier partagé sur un autre ordinateur du même réseau
- Stockage en réseau (NAS)

Les sauvegardes vers ces cibles à l'aide des protocoles réseau standard suivants sont prises en charge :

- FTP
- FTP (Alternative)
- Stockage d'objets OpenStack / Swift
- S3 Compatible
- SFTP (SSH)
- WebDAV

Les fournisseurs de stockage cloud suivants sont pris en charge nativement par Duplicati :

- Amazon S3
- Blob Azure
- Stockage dans le cloud B2
- Box.com
- Dropbox
- Stockage Google Cloud
- Google Drive
- Jottacloud
- Mega.nz

- Groupes Microsoft Office 365
- Microsoft OneDrive pour les entreprises
- Microsoft OneDrive
- Microsoft SharePoint
- Stockage simple OpenStack
- Rackspace CloudFiles
- Rclone
- Cloud décentralisé Sia
- Storj (ex Tardigrade) Stockage cloud décentralisé
- Tencent COS

Autres cibles prises en charge :

- Tahoe-LAFS

Ainsi, la Figure 2.3 met en évidence quelques backends de Duplicati :

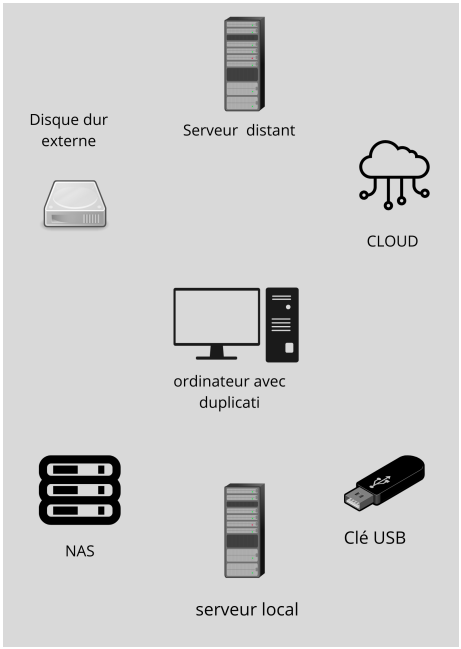


FIGURE 2.3 : Quelques backends de Duplicati

2.4 Mécanismes de sécurité et de surveillance pour Duplicati

Afin d'assurer une surveillance et une sécurité renforcée des sauvegardes, nous avons mis en place plusieurs mécanismes telles que l'authentification à double facteurs pour accéder à l'interface de duplicati, un vpn pour le transfert sécurisé des sauvegardes et Duplicati monitoring qui permet de surveiller les sauvegardes.

2.4.1 Système d'authentification à 2 facteurs

Nous avons mis en place un système d'authentification (illustré par la Figure 2.4) basé sur OAuth2 et OpenID Connect (OIDC), avec Auth0 comme fournisseur d'identité et Google Authenticator pour la validation en deux étapes (2FA). Plus précisément :

– **OAuth2 :** Un protocole d'autorisation qui permet à un utilisateur de donner accès à une application à certaines ressources sans partager son mot de passe. Il repose sur des tokens d'accès pour garantir la sécurité.

– **OpenID Connect (OIDC) :** Un protocole d'identification qui fonctionne sur OAuth2, ajoutant une couche d'identification d'utilisateur. Il permet de vérifier l'identité de l'utilisateur et de récupérer des informations sur lui via un ID token.

– **Auth0 :** Un fournisseur d'identité qui gère l'authentification des utilisateurs, la gestion des rôles et l'intégration de la 2FA via Google Authenticator. Auth0 offre une interface pour configurer les utilisateurs et gérer les paramètres de sécurité.

– **Google Authenticator :** Application mobile utilisé pour la 2FA, il génère des codes temporaires (généralement tous les 30 secondes) que l'utilisateur doit entrer après avoir saisi son mot de passe.

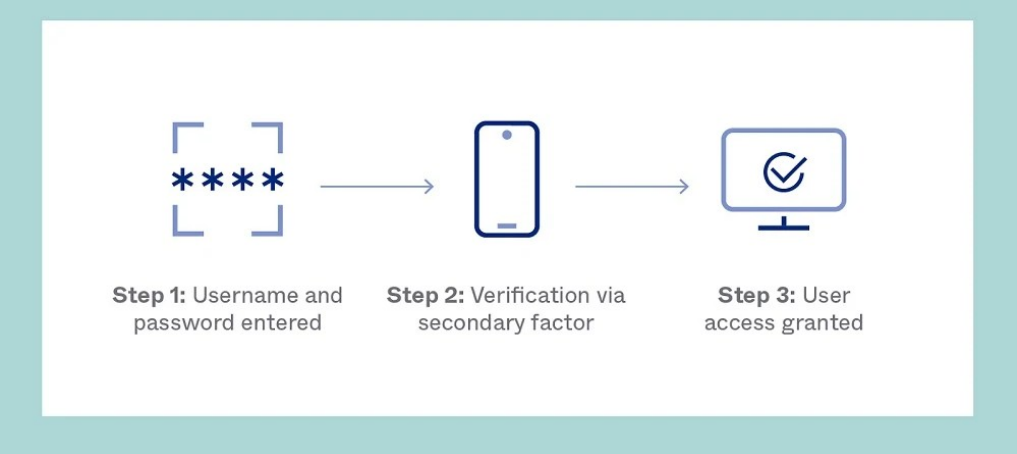


FIGURE 2.4 : Système d'authentification à 2 facteurs [19]

2.4.2 VPN pour le transfert sécurisé des sauvegardes

Nous avons utilisé Zérotier qui est un logiciel de réseau virtuel privé (VPN) qui permet aux utilisateurs de créer et de rejoindre des réseaux virtuels décentralisés. Il fonctionne en utilisant un système de "nœuds" pour connecter des ordinateurs ou serveurs distants entre eux. Nous l'avons utilisé pour assurer le transfère sécurisé des sauvegardes vers le serveur backup distant et nous avons restreint l'accès au serveur uniquement pour les adresses IP du VPN pour plus de sécurité.

2.4.3 La surveillance des sauvegardes

Nous avons utilisé Duplicati monitoring qui est une application web qui permet de surveiller l'état et le fonctionnement des sauvegardes effectuées avec Duplicati. Elle fournit une interface pour visualiser les rapports, alertes, et logs des tâches de sauvegarde, facilitant ainsi la gestion et la surveillance

des sauvegardes. Pour visualiser les sauvegardes de duplicati, il faut créer un compte sur duplicati monitoring puis créer des jeux de sauvegardes relatifs à chaque tâche de sauvegarde dans duplicati sans oublier de mettre le lien de duplicati dans le champs réservé pendant la création. Ensuite lorsque le jeu de sauvegarde est créé, il faut copier l'url de rapport http puis éditer la sauvegarde dans duplicati et coller l'url dans l'option avancée "send-http-url" au niveau de l'étape "Options générales". Ainsi lors du démarrage d'une sauvegarde, nous pouvons visualiser dans Duplicati Monitoring les informations des tâches de sauvegarde comme le statut des sauvegardes (réussie, échouée, en cours), le nombre de fichiers sauvegardés et l'espace utilisé, les rapports détaillés et les logs des sauvegardes etc.

2.5 Personnalisation du logo de Duplicati

Nous avons poussé notre travail un peu plus loin en apportant une légère modification au logo d'origine de Duplicati, représenté sur la Figure 2.5. Cette modification nous a permis d'obtenir un nouveau logo que nous pouvons voir sur la Figure 2.6 :



FIGURE 2.5 : Ancien logo



FIGURE 2.6 : Nouveau logo

Conclusion

Ce chapitre nous a permis tout d'abord de présenter les raisons du choix de Duplicati et d'établir une étude détaillée à travers ses fonctionnalités et ses caractéristiques. Passons maintenant au déploiement de Duplicati et au test effectué.

Chapitre 3

Déploiement de la solution de sauvegarde et test de fonctionnalités

Introduction

Ce chapitre est consacré à la mise en place proprement dite de notre solution. Nous effectuons l'installation et les configurations nécessaires pour son fonctionnement ainsi que les tests réalisés pour illustrer comment elle répond aux besoins spécifiques sans oublier d'exposer quelques limites de notre solution.

3.1 Installation de Duplicati

Notre solution Duplicati sera installé sur une machine virtuelle Windows 10.

1. Pour installer Duplicati, nous nous sommes rendus sur son site officiel **duplicati.com** comme illustré sur la Figure 3.1

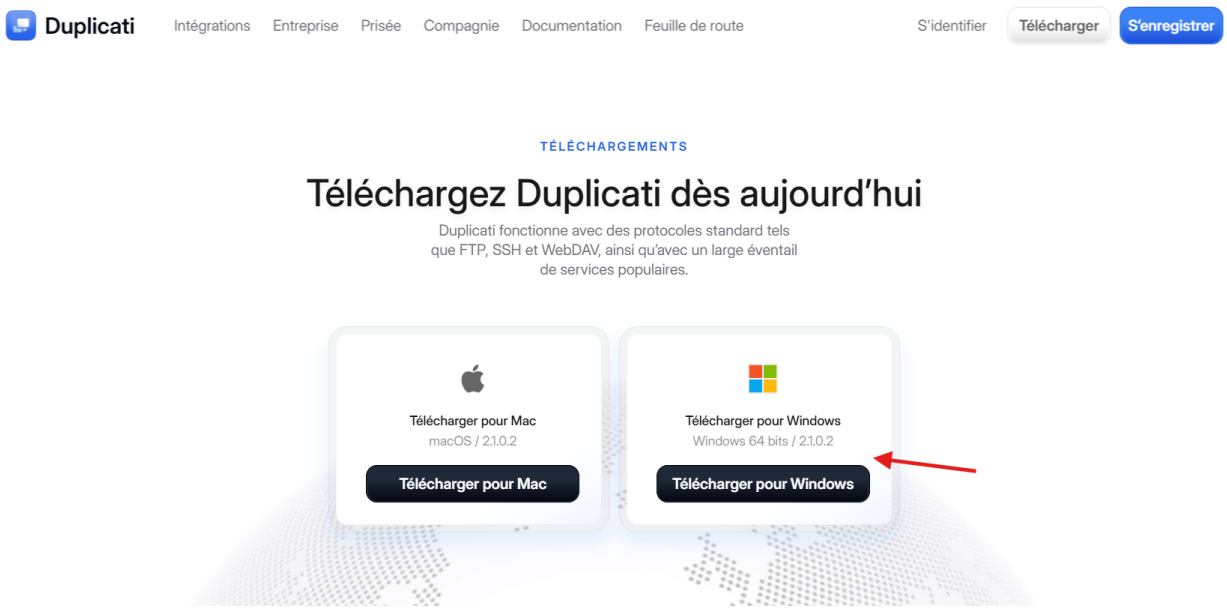


FIGURE 3.1 : Téléchargement de Duplicati

2. Ensuite il faut lancer l'installation du package d'installation téléchargé sur le site et cliquer sur le bouton Next comme sur la Figure 3.2

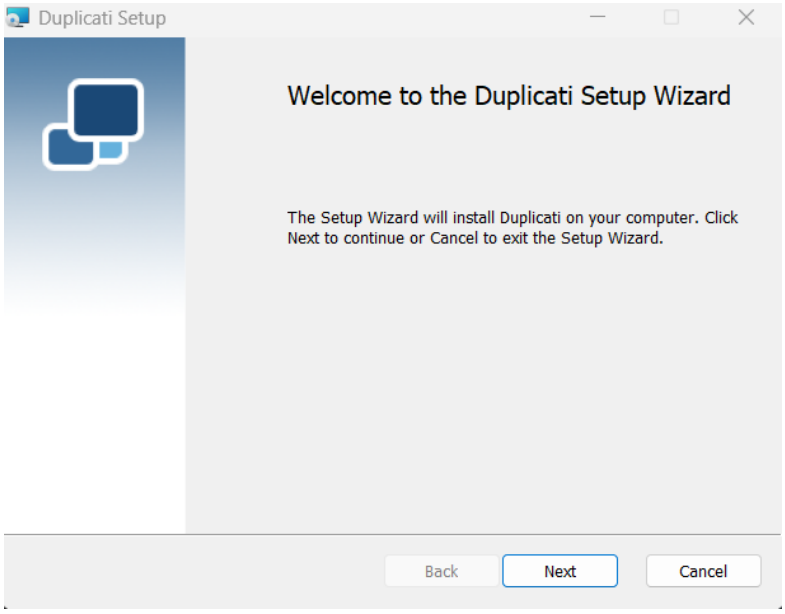


FIGURE 3.2 : Lancement de l'installation (1)

3. Approuver le contrat de licence et suivre les instructions pour poursuivre l'installation (Figure 3.3)

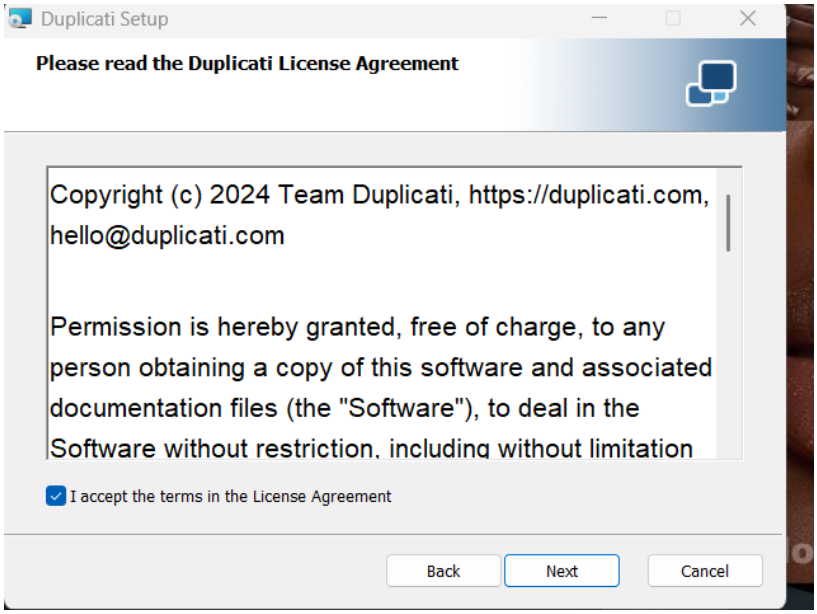


FIGURE 3.3 : Lancement de l'installation (2)

4. Une fois l'installation terminée, nous pouvons accéder à l'interface de Duplicati en entrant dans la barre de recherche de notre navigateur `localhost:8200`
   La première fois que vous démarrez l'interface Web de Duplicati, ce message s'affiche : "Ici, toute personne ayant accès à votre ordinateur (ou même à un autre ordinateur de votre réseau) pourrait potentiellement avoir accès à vos fichiers personnels en utilisant l'interface Web Duplicati" comme nous montre la Figure 3.4. Ainsi, il est recommandé de configurer un mot de passe pour accéder à l'interface.

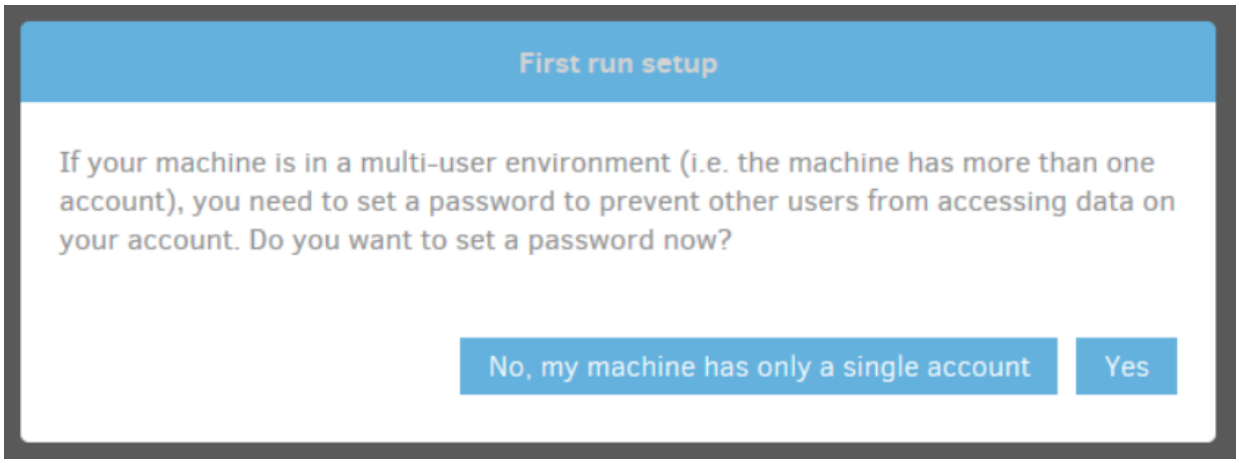


FIGURE 3.4 : Première connexion à l'interface

5. Nous pouvons enfin voir sur la Figure 3.5 le dashboard de Duplicati

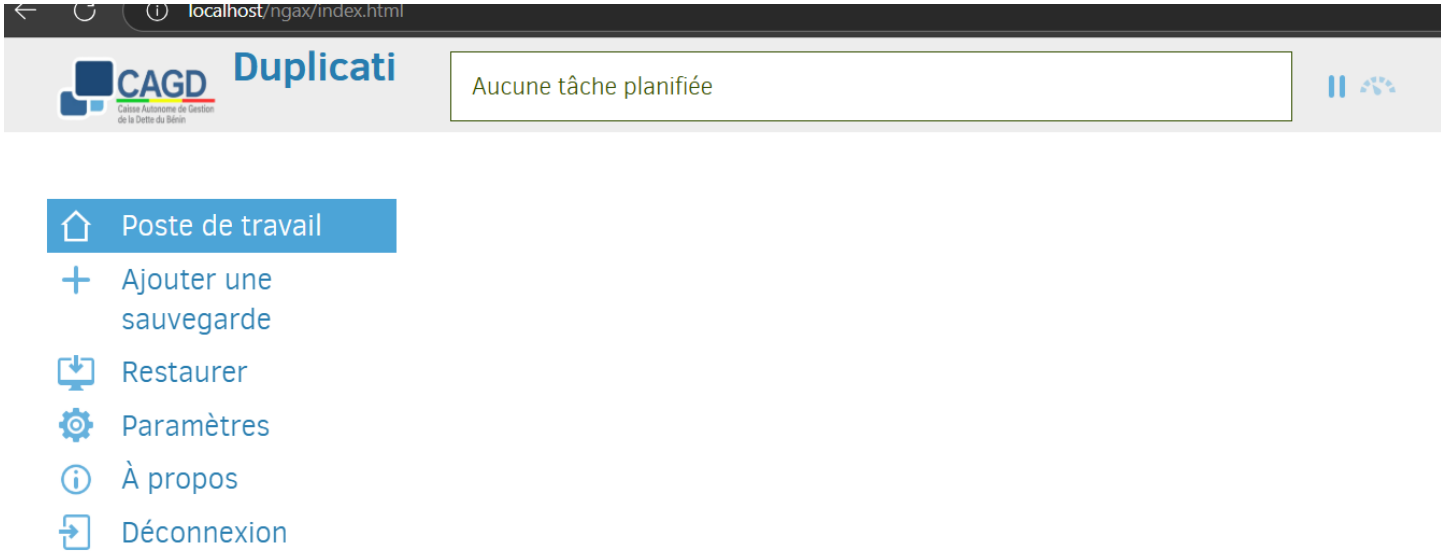


FIGURE 3.5 : Dashboard de Duplicati

3.2 Brève description des éléments du menu

- Nous avons le sous-menu "home" ou "poste de travail" qui est là par défaut qui permet de quitter un sous-menu pour revenir à l'écran d'accueil ou d'afficher les sauvegardes configurées
- Le sous-menu "ajouter une sauvegarde" qui permet d'ajouter une nouvelle sauvegarde (voir Figure 3.6)

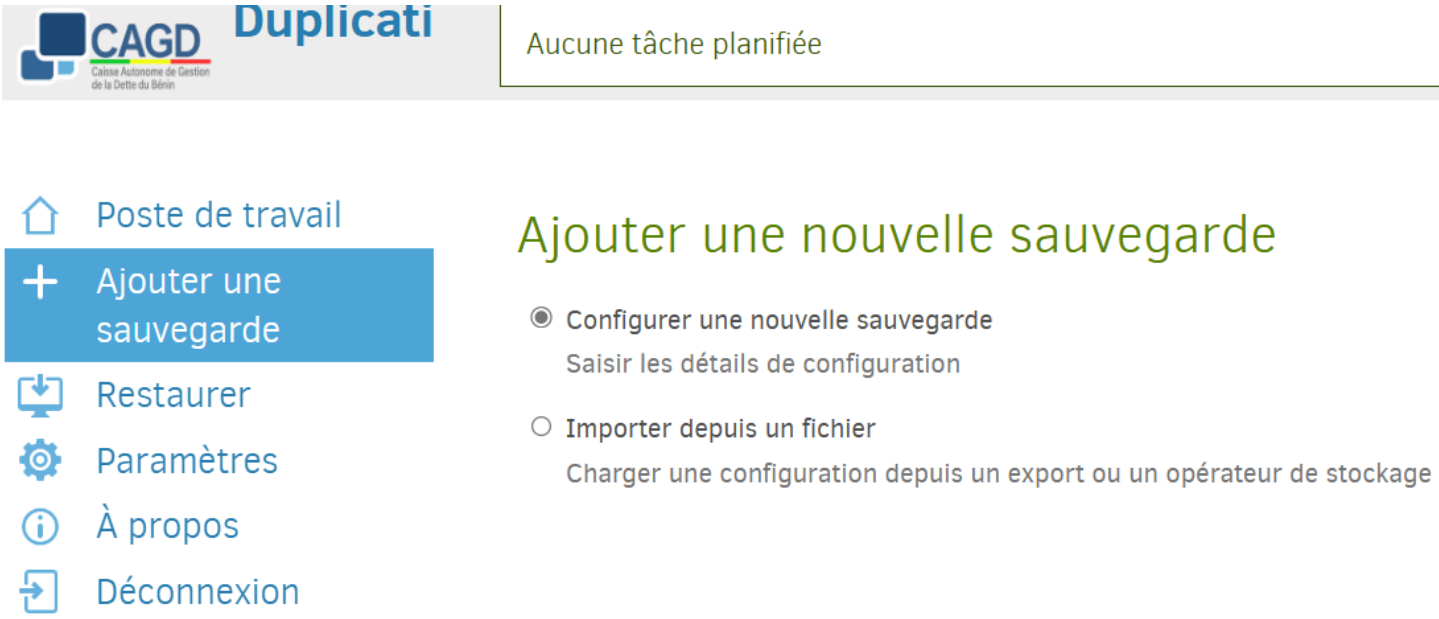


FIGURE 3.6 : Sous-menu “ajouter une nouvelle sauvegarde”

- Le sous-menu “restaurer” pour restaurer des fichiers à partir d’une tâche de sauvegarde déjà configurée ou directement à partir du backend ou d’un fichier de configuration importé (voir Figure 3.7)



FIGURE 3.7 : Sous-menu “restaurer”

- Le sous-menu “paramètres” pour modifier les paramètres généraux du programme et définir les paramètres par défaut pour toutes les tâches de sauvegarde (voir Figure 3.8)

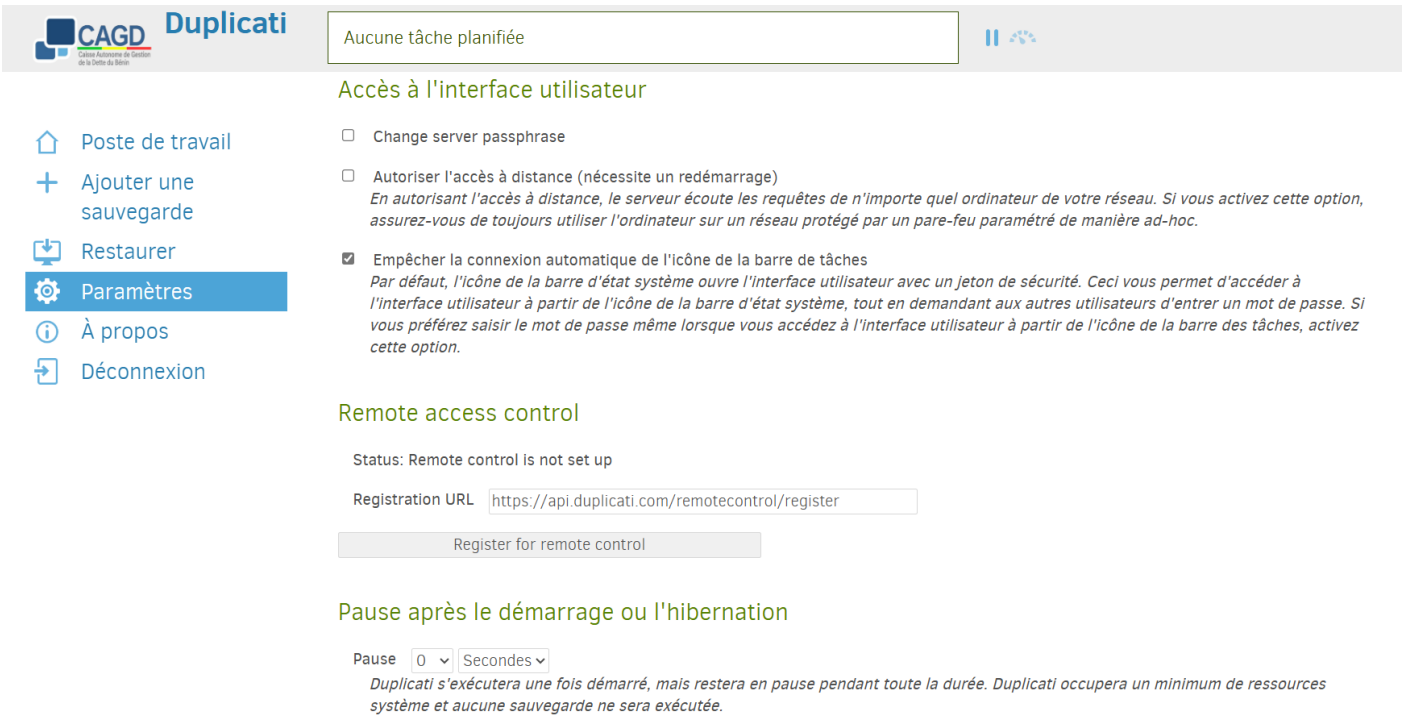


FIGURE 3.8 : Sous-menu “paramètres”

- Le sous-menu “à propos” pour afficher les informations sur la version actuelle de Duplicati et des informations systèmes (voir Figure 3.9)



FIGURE 3.9 : Sous-menu “à propos”

3.3 Configuration d'une nouvelle sauvegarde

Connectons nous d'abord en passant par l'authentification 2FA et en choisissant Google pour valider mon identité comme sur les Figures 3.10, 3.11 et 3.12 :

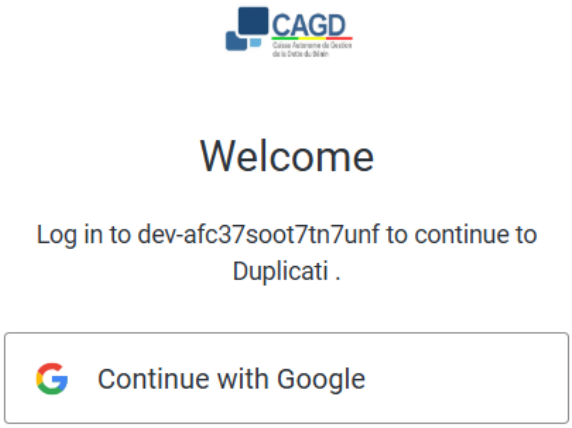


FIGURE 3.10 : Authentification par Google (1)

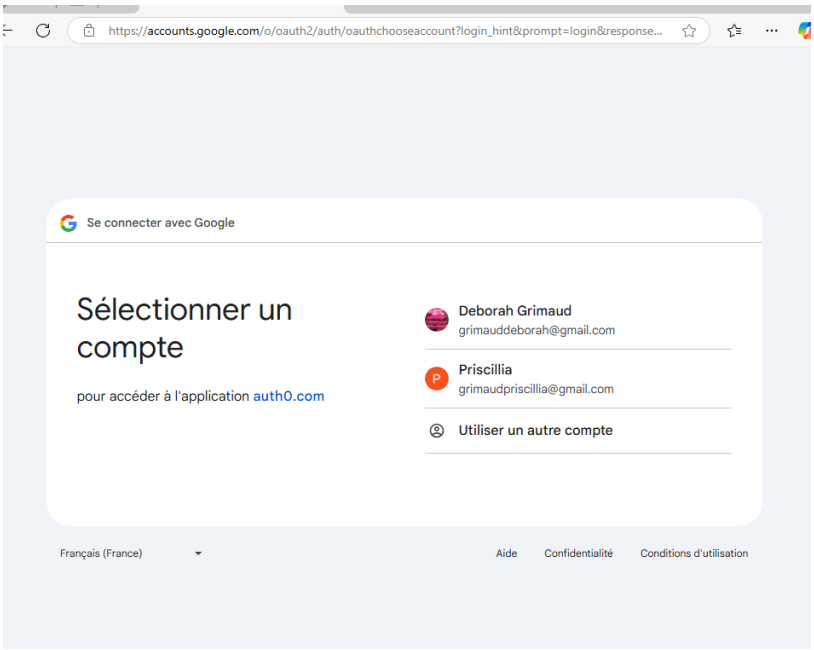


FIGURE 3.11 : Authentification par Google (2)

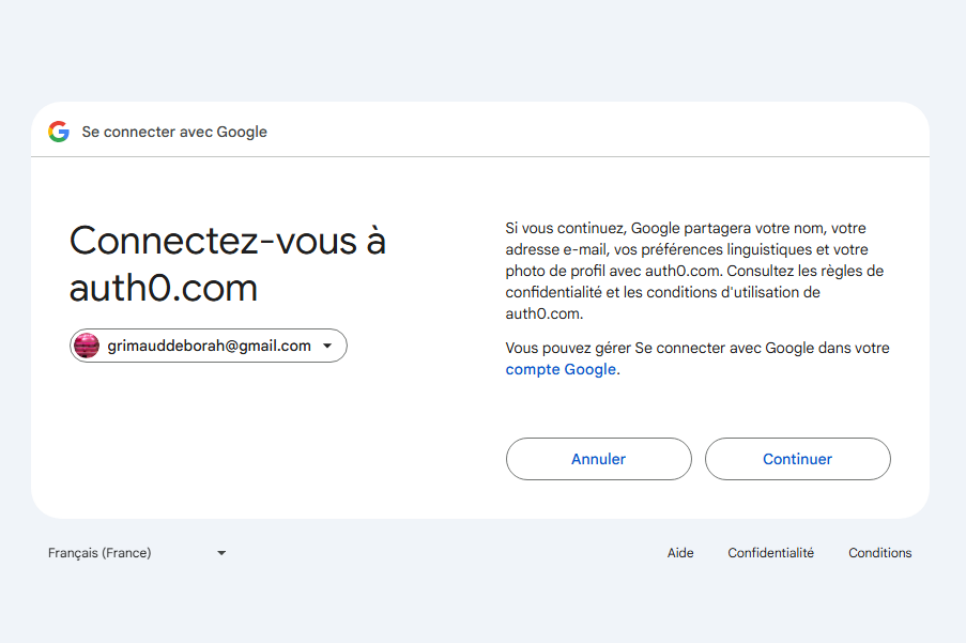


FIGURE 3.12 : Authentification par Google (3)

Ensuite avec Google authenticator nous avons scanné le QR code pour recevoir le code à entrer (voir Figure 3.13)

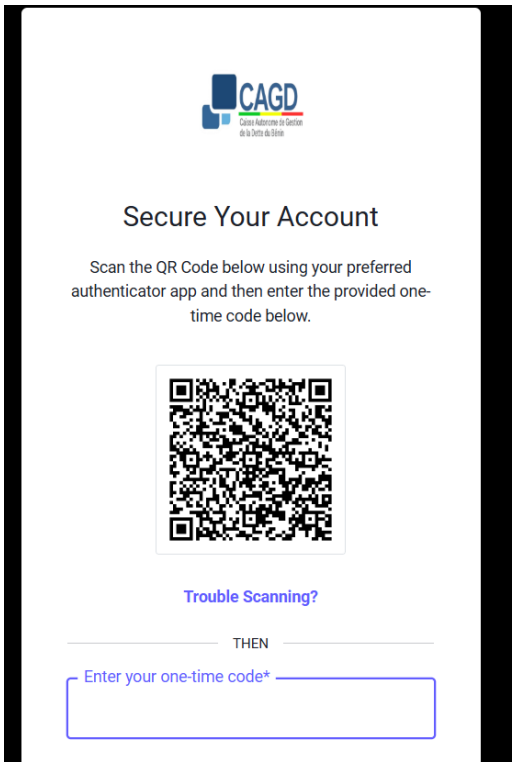


FIGURE 3.13 : QR Code

Dans l'écran montré par la Figure 3.14, nous pouvons maintenant accéder à duplicati et entrer le mot de passe de duplicati

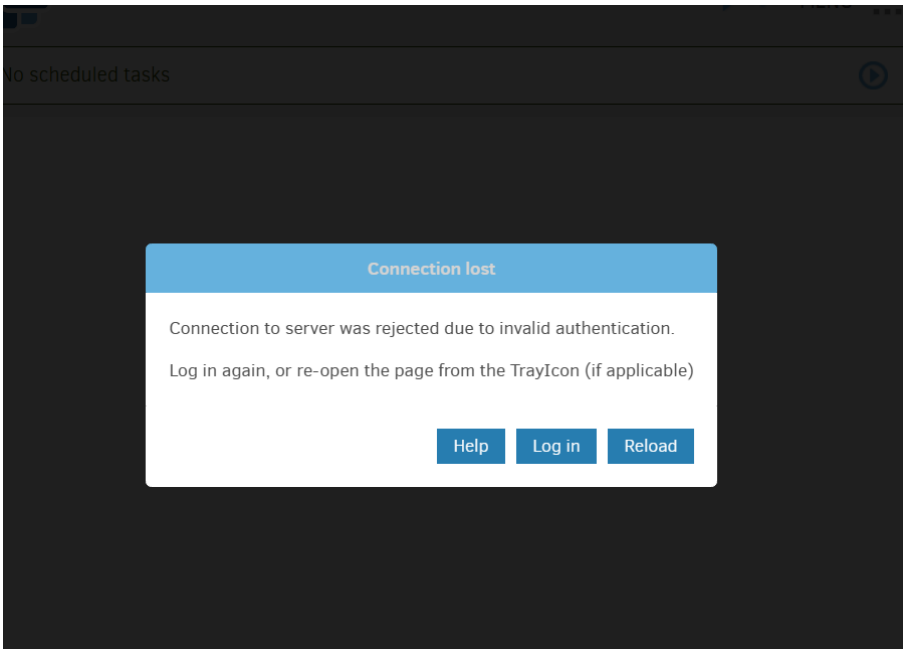


FIGURE 3.14 : Accès à duplicati

Nous avons ensuite cliqué sur le sous-menu "ajouter une nouvelle sauvegarde" et coché "configurer une nouvelle sauvegarde" puis sur le bouton suivant (voir Figure 3.15)

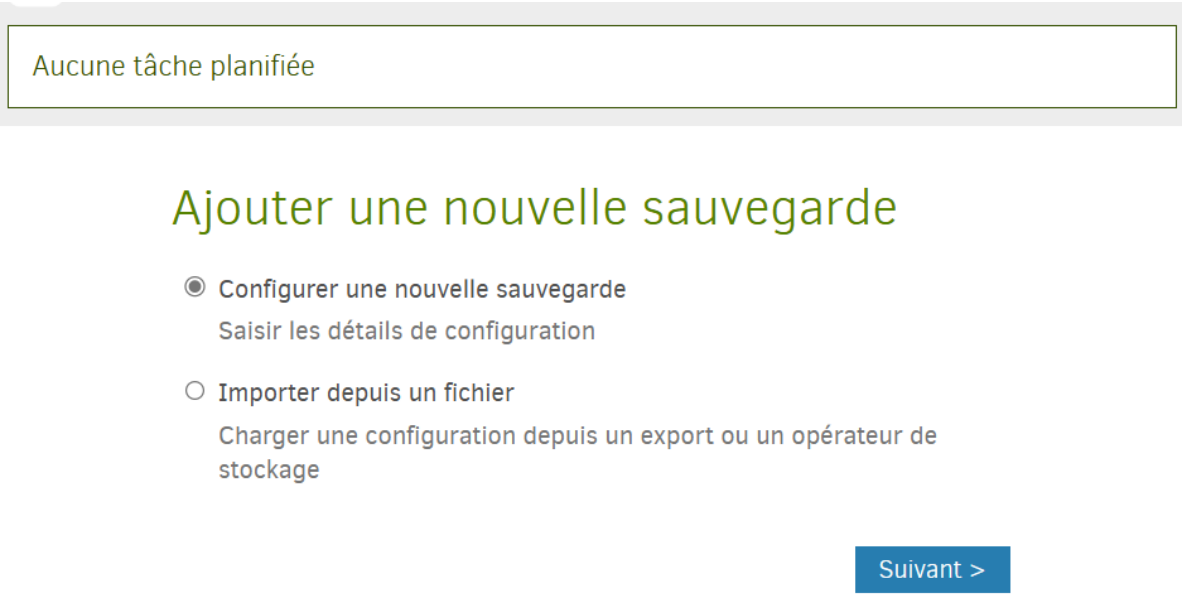


FIGURE 3.15 : Configuration d'une nouvelle sauvegarde

La configuration d'une nouvelle sauvegarde se fait en 5 étapes :

Étape 1 : Général

A ce niveau comme illustré sur la Figure 3.16, il faut entrer un nom descriptif, ajouter une description (facultative), sélectionner le type de chiffrement et spécifier une clé de chiffrement forte. En option, Duplicati peut générer une clé de cryptage forte.
Nous avons choisi comme nom "doc(local)" sans chiffrer.



FIGURE 3.16 : Paramètres généraux de la nouvelle sauvegarde

Étape 2 : Destination

À l'étape 2 illustrée par la Figure 3.17, il faut spécifier le type de stockage souhaité pour les sauvegardes et les informations d'identification. Dans cet exemple, nous avons fait une sauvegarde en local sur le pc de l'utilisateur et testé la connexion (voir Figure 3.18). Duplicati essaiera de se connecter au backend en utilisant les informations fournies. Si Duplicati peut se connecter au backend, mais que le dossier spécifié n'existe pas, Duplicati le crée. Cependant si le dossier spécifié existe déjà, Duplicati enverra une notification de succès.
Nous avons créé un dossier backup sur le bureau pour recevoir les sauvegardes puis testé la connexion au backend

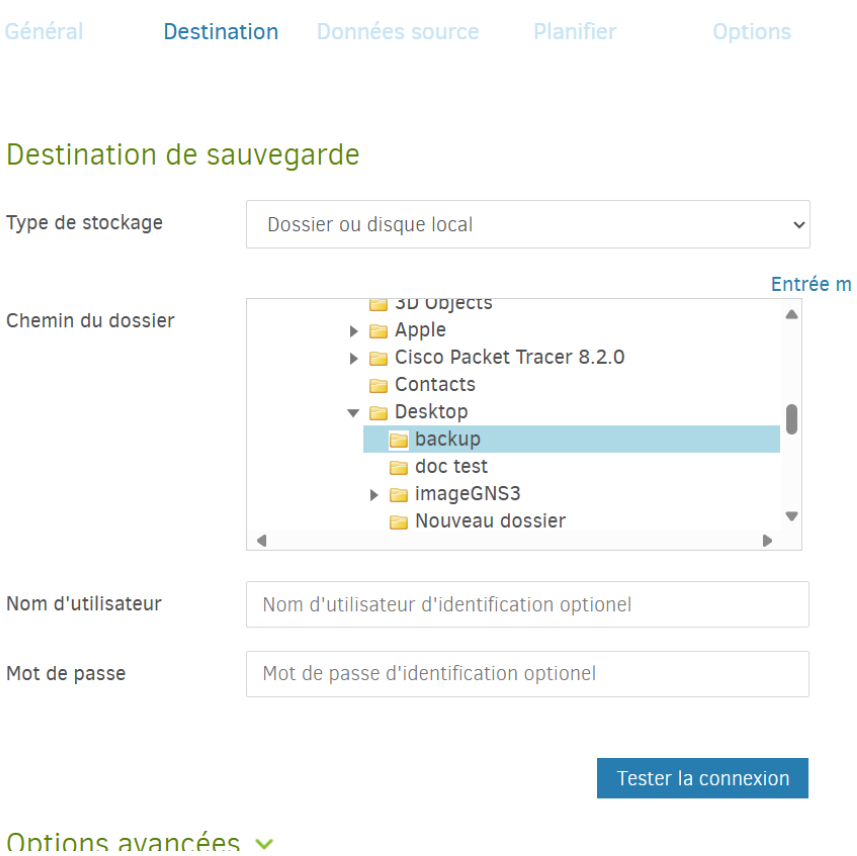


FIGURE 3.17 : Choix de la destination

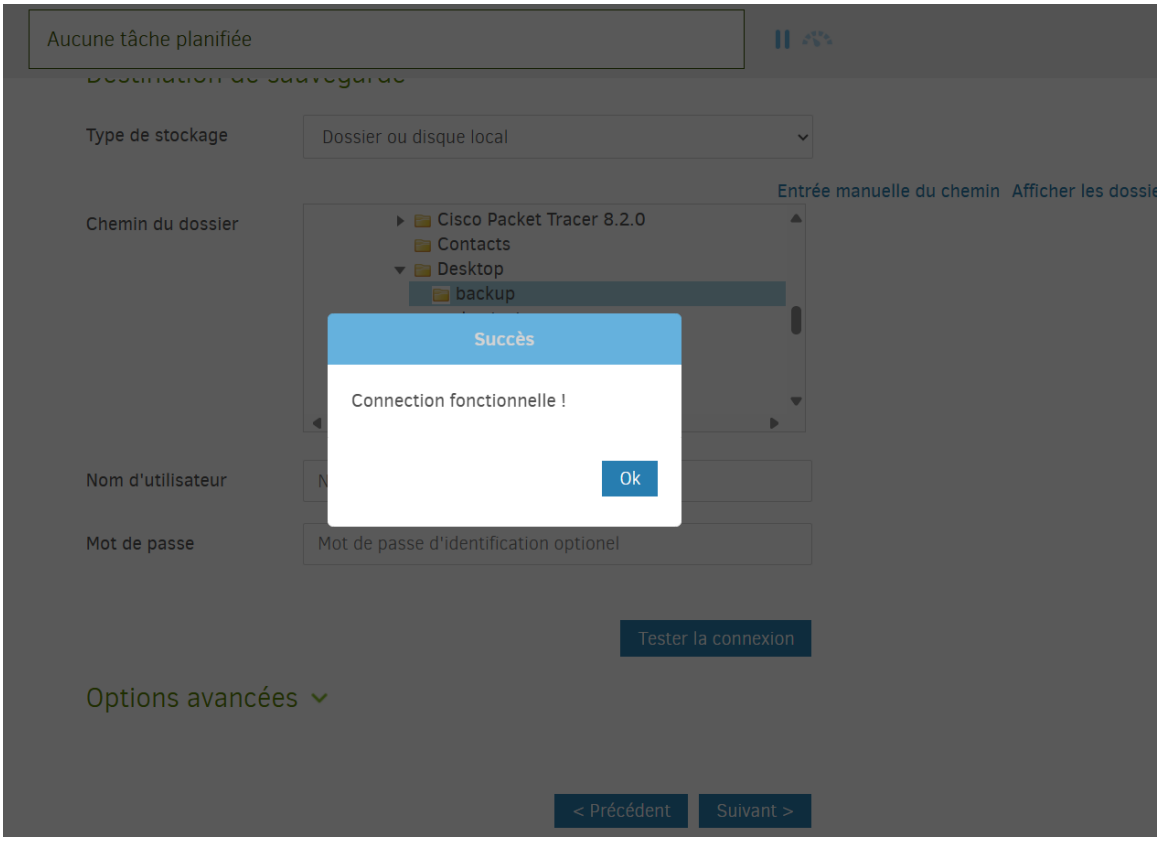


FIGURE 3.18 : Connexion au backend réussie

Étape 3 : Sélection des données sources

À l'étape 3, il s'agit de sélectionner les fichiers et dossiers qui sont à inclure dans la sauvegarde. Cela peut être fait en sélectionnant des fichiers et des dossiers dans le sélecteur de fichiers. Seuls les fichiers et dossiers locaux peuvent être sélectionnés à l'aide du sélecteur de fichiers. Mais on peut également inclure des dossiers partagés dans le réseau local, en spécifiant le chemin d'accès dans la zone de texte située sous le sélecteur de fichiers.
Nous avons créé un dossier doc test sur le bureau pour notre démonstration de sauvegarde (voir figure 3.19)

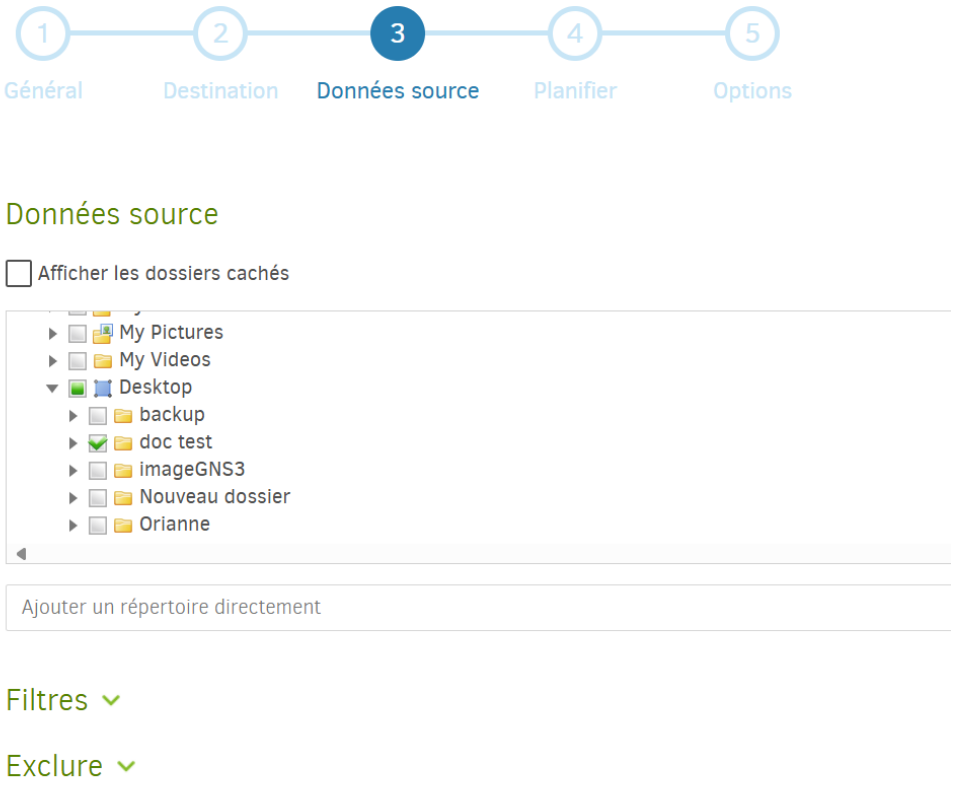


FIGURE 3.19 : Choix des données sources

Étape 4 : Planification

À l'étape 4, il s'agit de planifier les sauvegardes. La sélection de l'option "Automatically run backups" désactive la planification de cette tâche de sauvegarde. Une fois désactivé, on peut démarrer la tâche de sauvegarde manuellement à n'importe quel moment. Si cette option est activée, on spécifie alors la fréquence et l'heure de démarrage de la sauvegarde. On peut également exclure un ou plusieurs jours de la semaine. Si une tâche de sauvegarde ne respecte pas la planification définie, par exemple si l'ordinateur est hors tension, la tâche de sauvegarde commencera dès que possible après l'heure spécifiée.
Nous avons planifié la sauvegarde tous les jours à 16h00 (voir Figure 3.20)

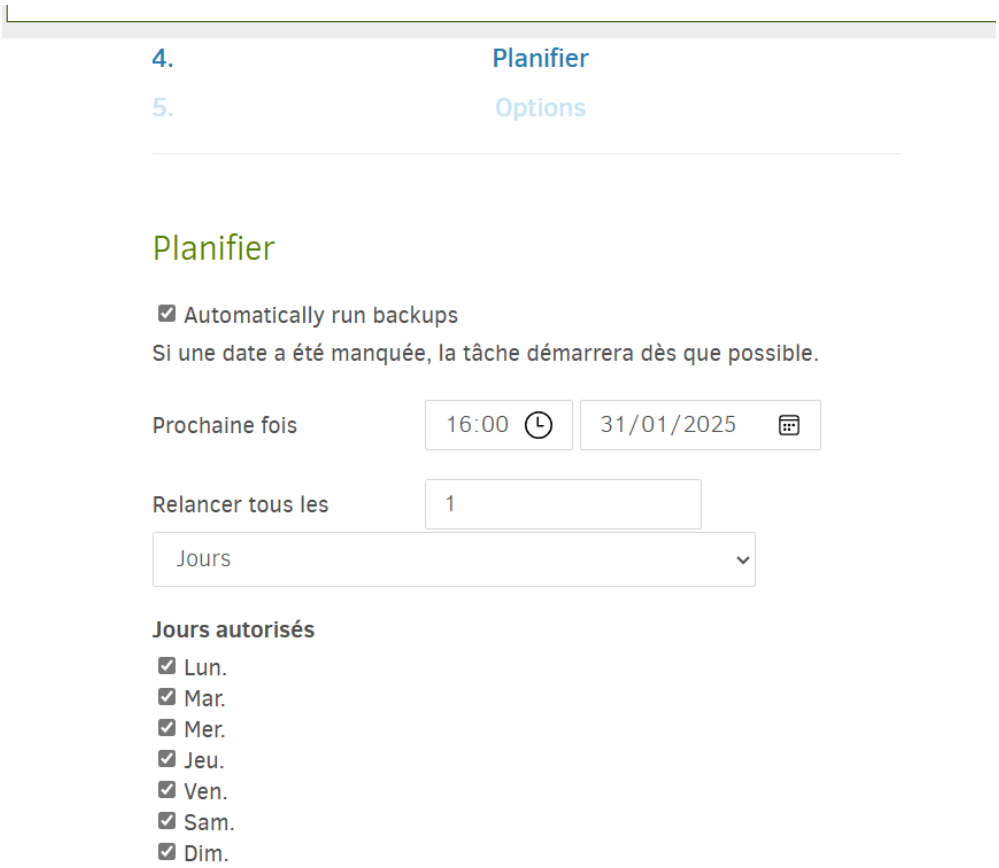


FIGURE 3.20 : Planification de la sauvegarde

Étape 5 : Options

À l'étape 5, vous pouvez définir la taille du volume de téléchargement et le nombre de sauvegardes disponibles pour les opérations de restauration. Le volume de téléchargement est un fichier compressé chiffré qui contient une partie de la sauvegarde. Pour les opérations de sauvegarde normales, on peut conserver cette valeur inchangée, mais dans certains scénarios, par exemple les sauvegardes très volumineuses, on peut augmenter la taille pour réduire le nombre de fichiers à l'emplacement de stockage distant. La taille par défaut d'un volume de téléchargement est de 50 Mo. Augmenter cette valeur si nécessaire.
La rétention peut être paramétrée de 5 façons :

- **Conserver toutes les sauvegardes :** les sauvegardes ne seront jamais supprimées. Il s'agit de l'option la plus sûre, mais la capacité de stockage à distance ne cessera d'augmenter.
- **Supprimer les sauvegardes antérieures à :** les sauvegardes antérieures à un certain nombre de jours, de semaines, de mois ou d'années seront supprimées.
- **Conserver un nombre spécifique de sauvegardes :** le nombre spécifié de versions de sauvegarde sera conservé, toutes les sauvegardes plus anciennes seront supprimées
- **Conservation des sauvegardes personnalisées :** entrer ses propres paramètres dans la zone de texte qui s'affiche.

- **Conservation intelligente des sauvegardes :** conserve une sauvegarde pour chacun des 7 derniers jours, chacune des 4 dernières semaines et chacun des 12 derniers mois.

Dans notre exemple, nous avons utilisé la rétention de sauvegarde intelligente (voir Figure 3.21)

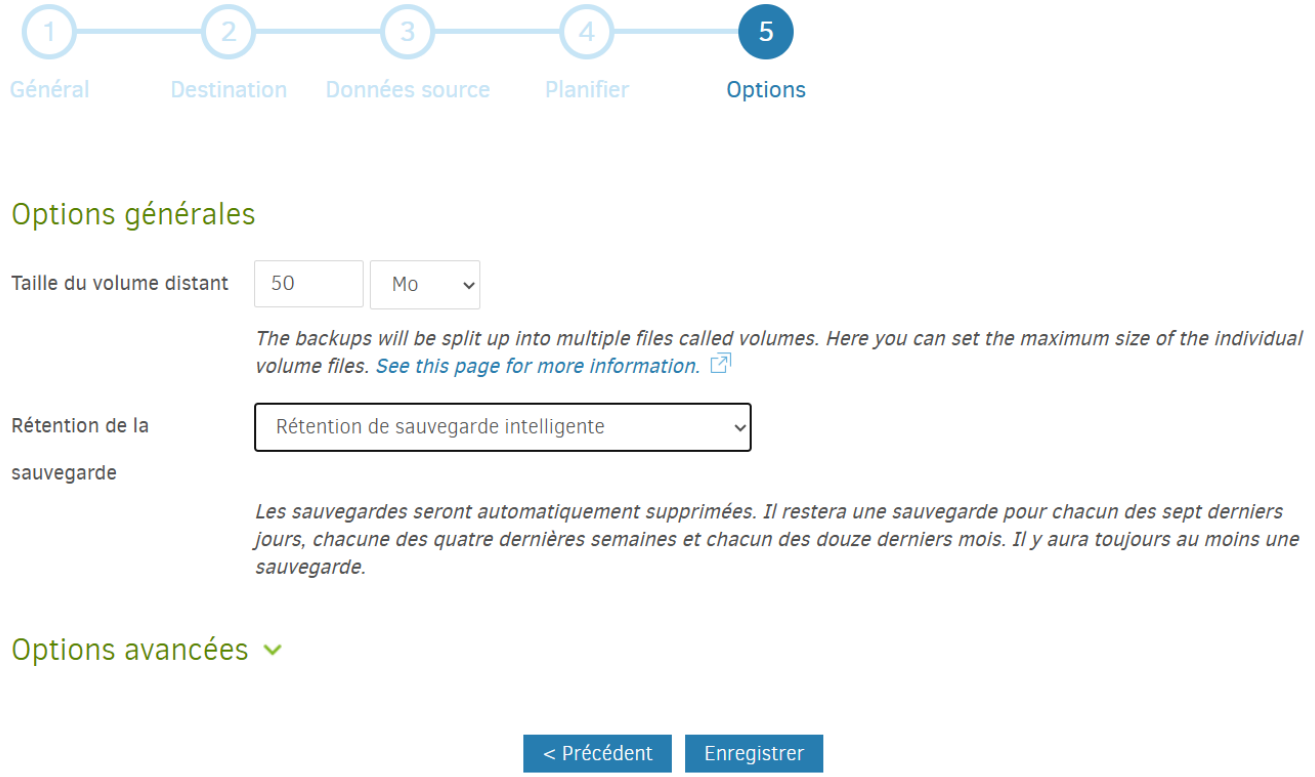


FIGURE 3.21 : Options générales de sauvegarde

Après nous avons cliqué sur le bouton "Enregistrer" pour enregistrer notre nouvelle sauvegarde et l'apercevoir dans le sous-menu "Postes de travail" comme sur la Figure 3.22



FIGURE 3.22 : Nouvelle sauvegarde configurée

Nous avons également créé le jeu de sauvegarde relatif à celle-ci dans le dashboard de duplicati

monitoring puis nous l'avons relié à duplicati (voir Figure 3.23)

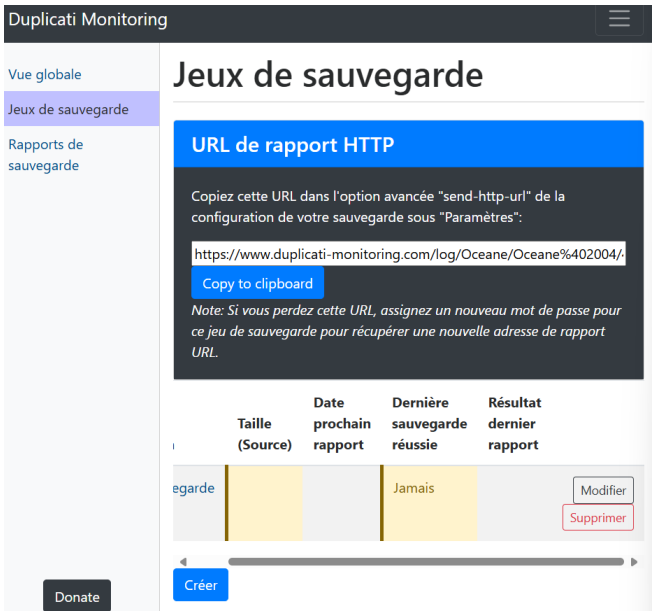


FIGURE 3.23 : Jeu de sauvegarde de "Sauvegarde"

Ainsi, nous pouvons apercevoir notre nouvelle sauvegarde et dont la prochaine exécution est programmée pour le lendemain à 16h. Cependant, nous pouvons la démarrer en cliquant sur le bouton "Démarrer maintenant".
En effet, il existe 3 façons de démarrer une sauvegarde à l'aide de l'interface utilisateur graphique :

- S'il s'agit d'une sauvegarde programmée, attendre simplement la prochaine heure programmée. La sauvegarde démarrera automatiquement.
- Cliquer sur Démarrer maintenant, juste sous le nom de la sauvegarde comme sur la Figure 3.24.

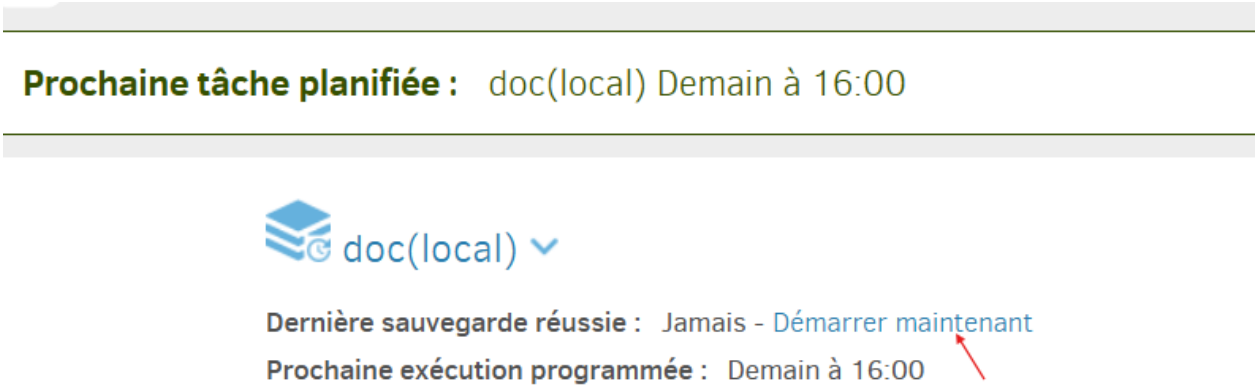


FIGURE 3.24 : Choix de démarrage de la sauvegarde (1)

- Cliquer sur le nom de la sauvegarde. Cliquer ensuite sur "Démarrer maintenant" sous Opérations comme sur la Figure 3.25.



FIGURE 3.25 : Choix de démarrage de la sauvegarde (2)

Ici, nous avons démarré notre sauvegarde en cliquant sur le bouton "démarrer maintenant" juste sous le nom de la sauvegarde et elle a été un succès comme le montre la Figure 3.26.

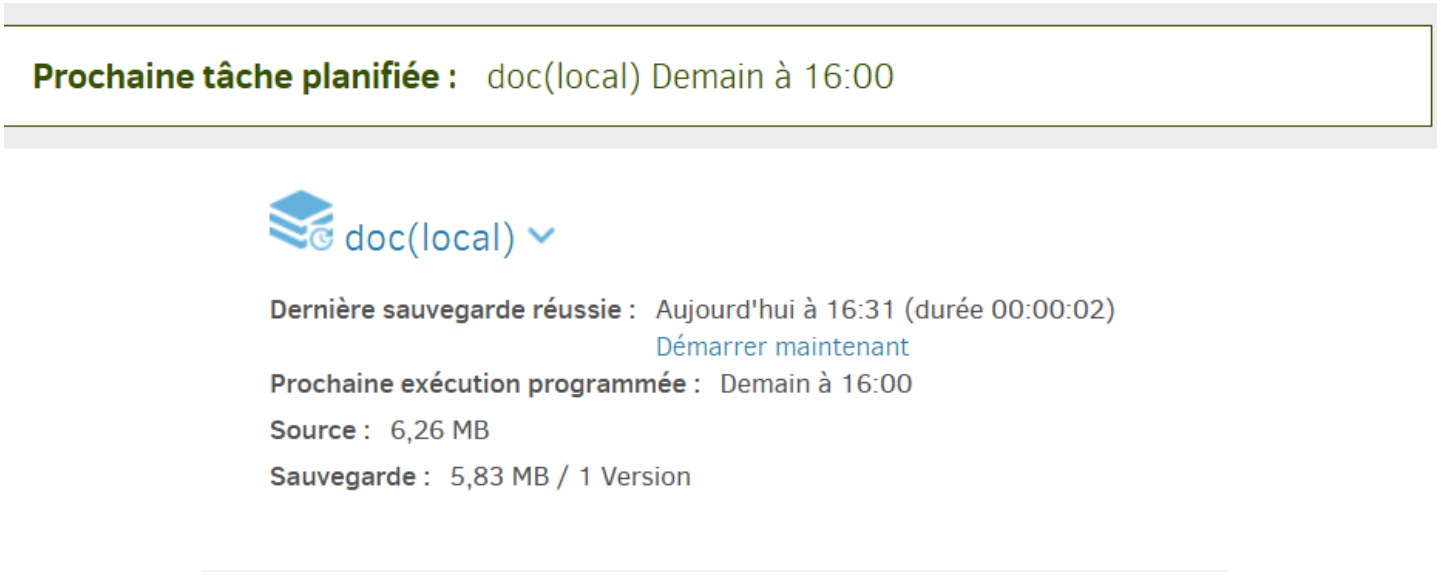


FIGURE 3.26 : Sauvegarde réussie (1)

Ainsi, nous pouvons voir que la sauvegarde a réussi à 16h31 et que la prochaine sauvegarde est programmée pour le lendemain à 16h00 comme indiqué lors de notre configuration. Aussi, la taille des données à la source qui était de 6.26 MB est revenu à 5.83 MB après la sauvegarde grâce à la fonctionnalité de compression des sauvegardes que propose Duplicati.
Nous pouvons voir aussi dans le dashboard de duplicati monitoring que la sauvegarde a réussi (voir Figure 3.27)



FIGURE 3.27 : Sauvegarde réussie (2)

3.4 Test de fonctionnalités

3.4.1 Scenario de test

Nous avons simulé un utilisateur qui a perdu ses données suite à une panne de son disque dur. Il faut noter que des sauvegardes de ses données ont été configurées avec Duplicati : une sur le cloud (Google Drive) et une sur le serveur backup distant de l'entreprise accessible par SSH à l'adresse 192.168.191.249 (voir Figure 3.28).

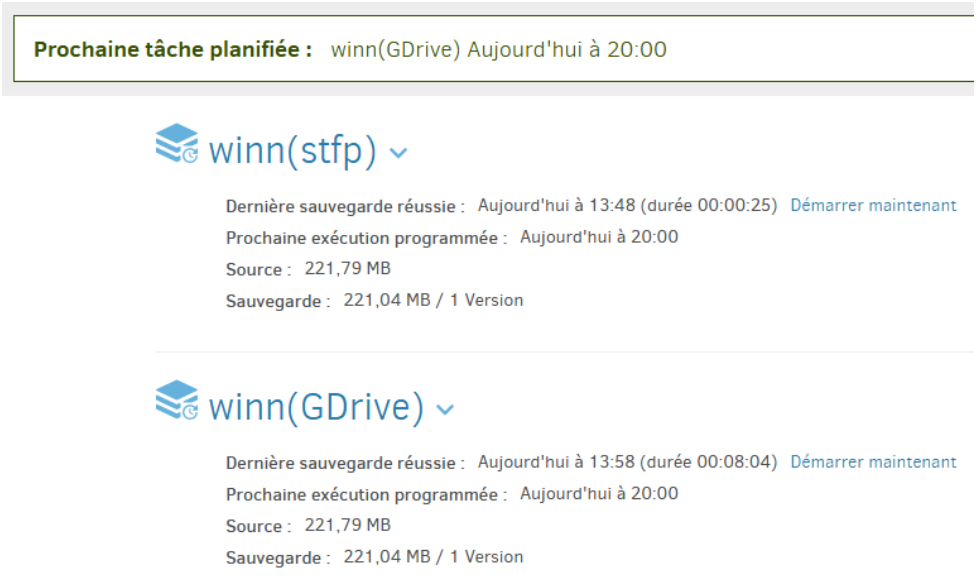


FIGURE 3.28 : Sauvegardes effectuées au départ

Ainsi, pour restituer les données perdues sur le nouveau disque dur, nous avons procédé à la restauration dans Duplicati.

3.4.2 Restauration

Nous avons restauré les données perdues à partir des 2 destinations choisies auparavant.

- **Restauration à partir du serveur backup de l'entreprise**

A ce niveau comme l'indique la Figure 3.29, nous avons choisi la restauration à partir de l'emplacement des fichiers de sauvegarde dans le sous-menu restaurer

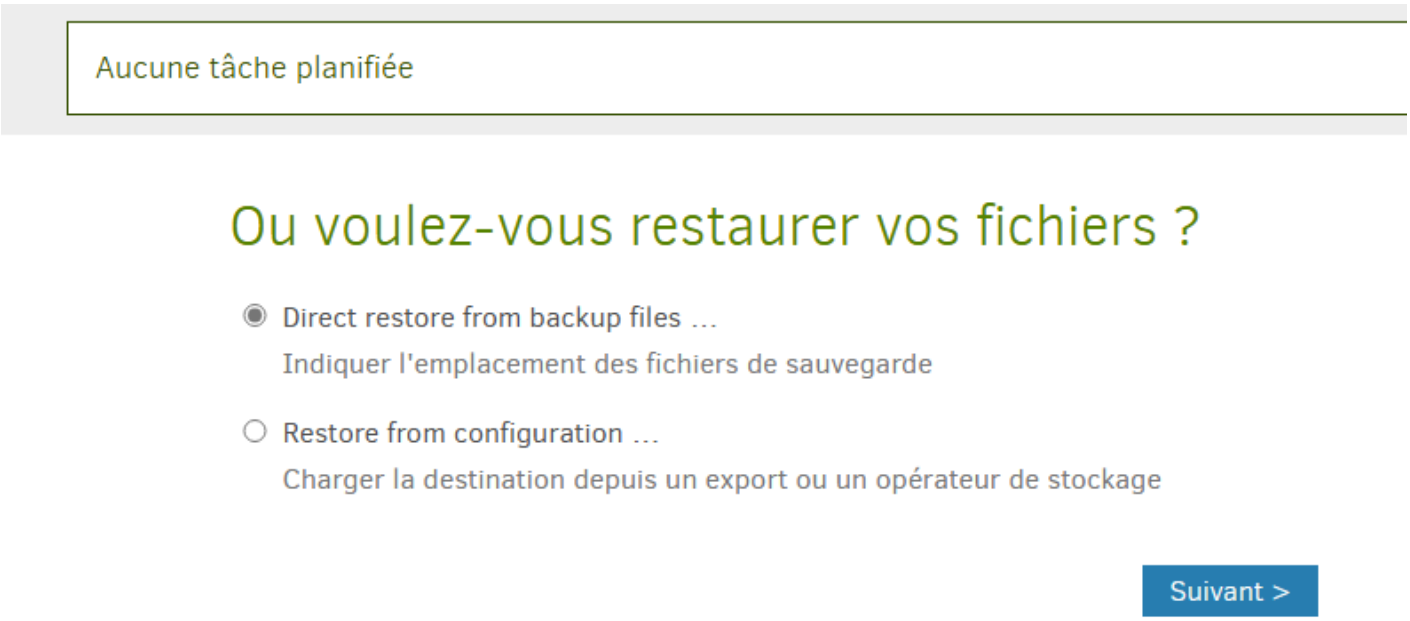


FIGURE 3.29 : Choix de la restauration

En effet la restauration se fait en 4 étapes :

Étape 1 : Emplacement de la sauvegarde

À l'étape 1, nous avons fourni toutes les informations nécessaires. Il faudrait connaître au préalable l'emplacement du backend et de la sauvegarde, les informations d'identification et les renseigner dans les champs respectifs (voir Figure 3.30) puis tester la connexion au backend pour voir si elle est fonctionnelle (voir Figure 3.31).

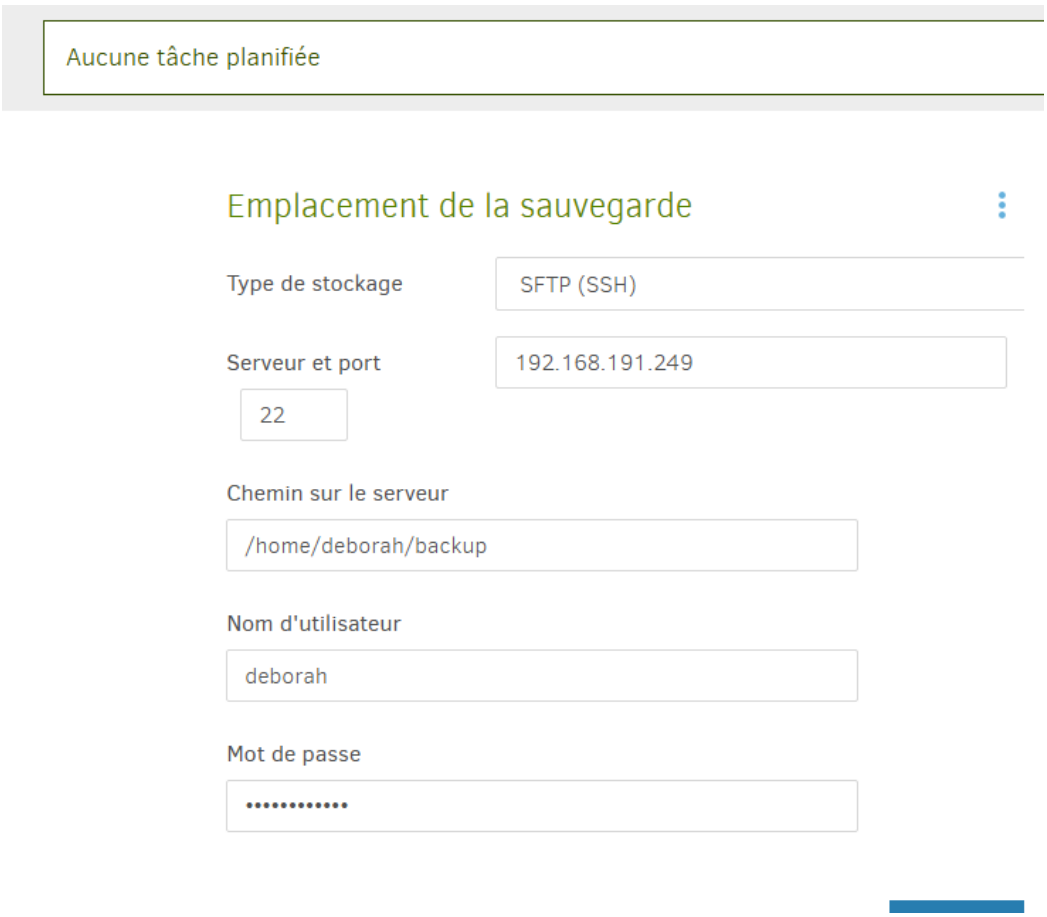


FIGURE 3.30 : Emplacement de la sauvegarde

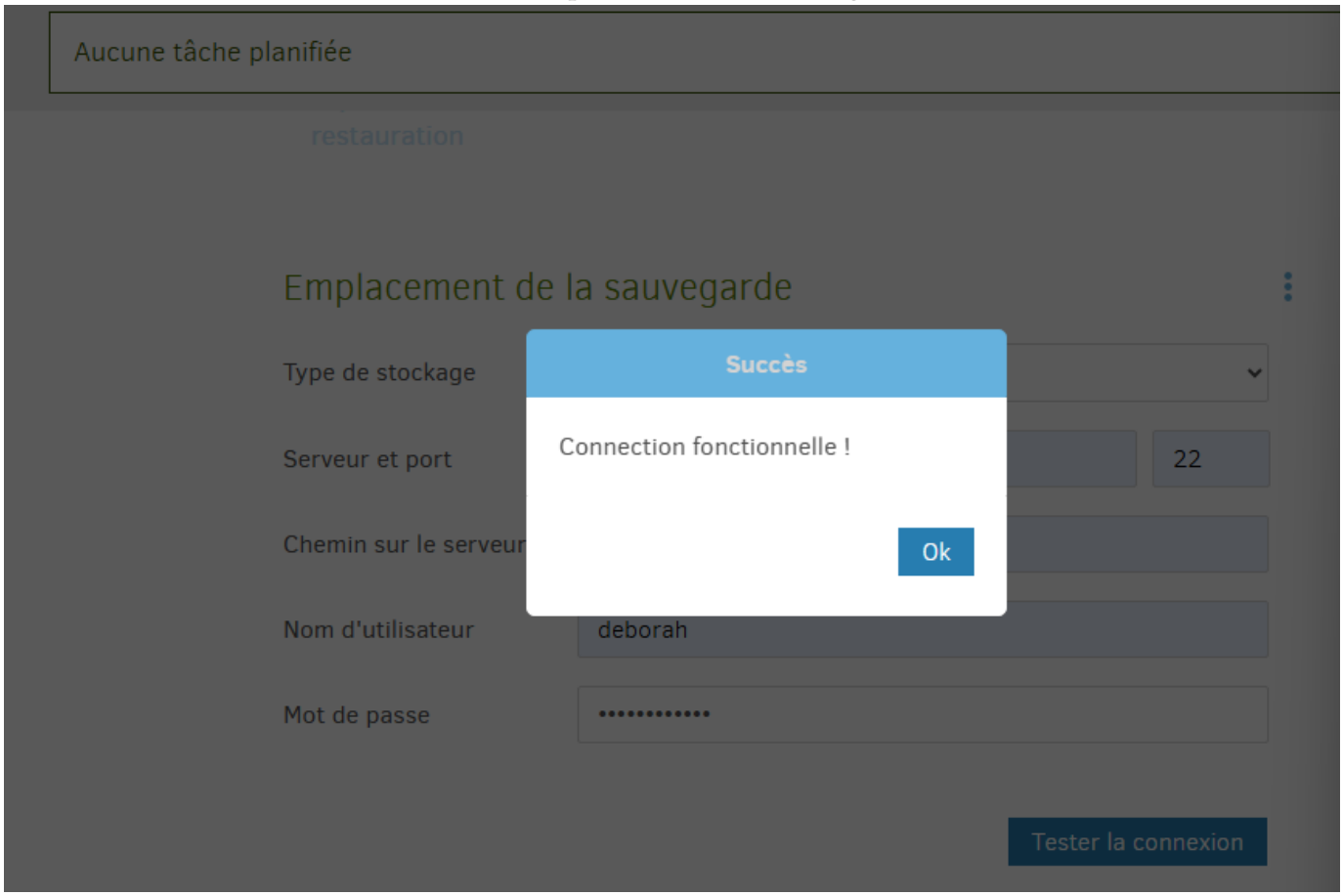


FIGURE 3.31 : Connexion fonctionnelle

Étape 2 : Chiffrement

A l'étape 2, nous avons spécifié la phrase secrète utilisée pour chiffrer la sauvegarde lors de sa configuration comme sur la Figure 3.32

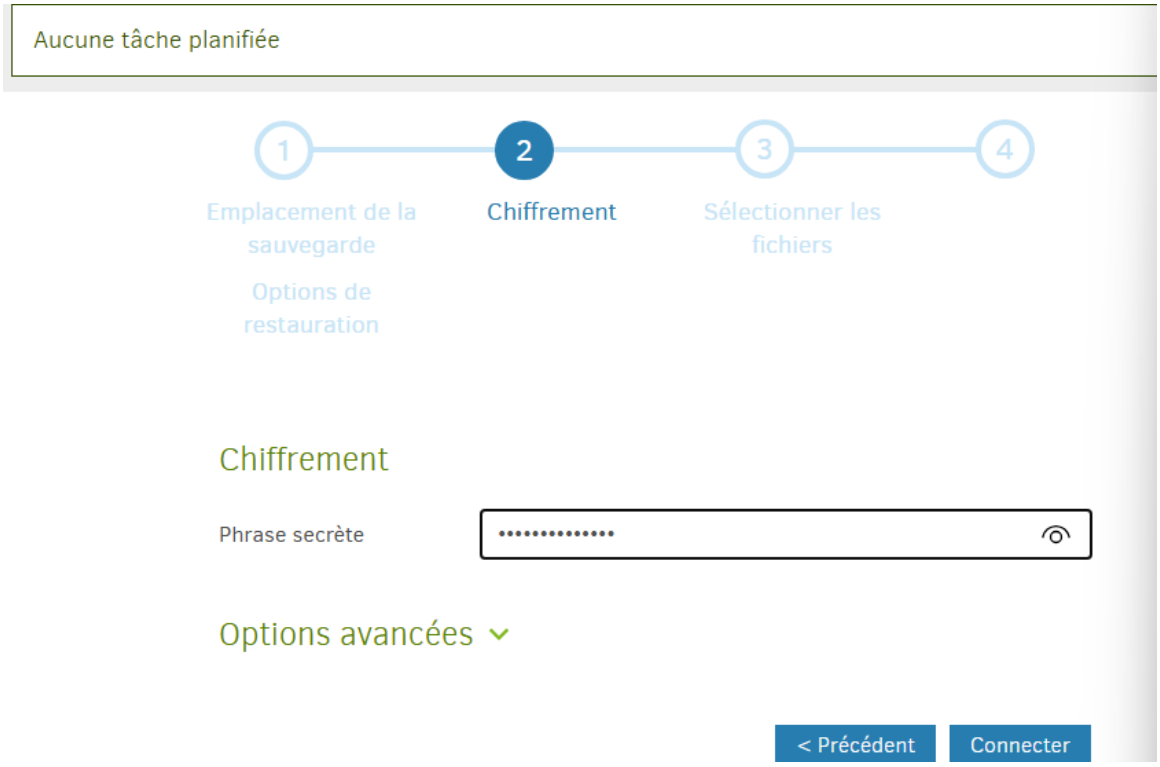


FIGURE 3.32 : Chiffrement

Ensuite en cliquant sur connecter, Duplicati se connecte au backend et récupère une liste des sauvegardes disponibles.

Étape 3 : Sélectionner les fichiers

A l'étape 3, nous avons sélectionné les fichiers à restaurer ainsi que la version souhaitée comme le montre la Figure 3.33



FIGURE 3.33 : Sélection des fichiers à restaurer

Étape 4 : Options de restauration

Ici, nous avons choisi de placer les données à restaurer dans le dossier restauration sur le bureau en écrasant les fichiers existants dans le dossier et en restaurant les permissions (voir Figure 3.34).



FIGURE 3.34 : Options de restauration

Nous avons enfin lancé la restauration qui a été une réussite (voir Figure 3.35)

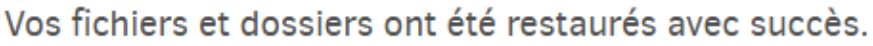


FIGURE 3.35 : Réussite de la restauration

- **Restauration à partir du cloud (Google Drive)**

Nous avons répété les étapes précédentes en modifiant juste l'étape 1 qui est l'emplacement de la sauvegarde. Nous avons spécifié à cette étape le type de stockage, le chemin sur le serveur ainsi que l'AuthID (voir Figure 3.36) :



FIGURE 3.36 : Emplacement de la sauvegarde (Google Drive)

Il est à noter que nous devons disposer d'un compte Google Drive pour y effectuer les sauvegardes.

Les données restaurées avec succès apparaissent dans le dossier **restauration**, comme le montre la Figure 3.37

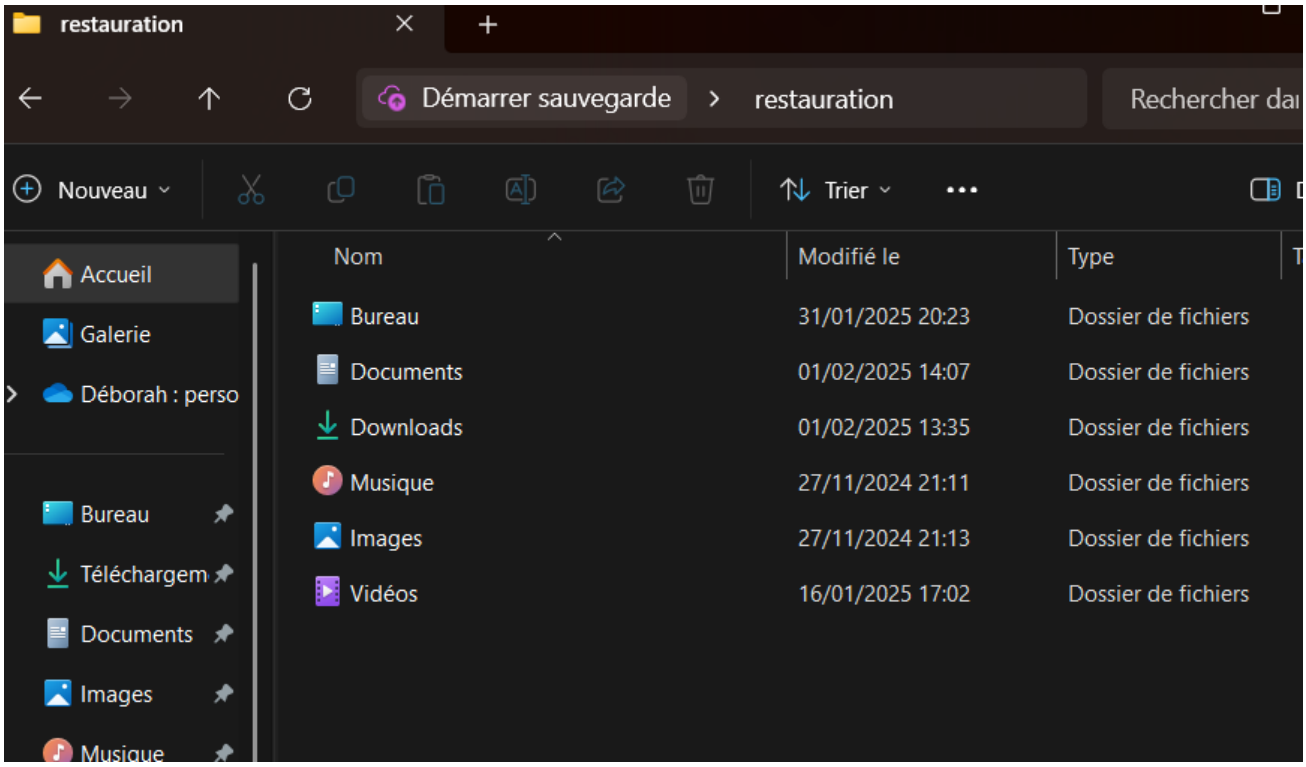


FIGURE 3.37 : Données restaurées avec succès

3.5 Discussion

L'implémentation de Duplicati comme solution de sauvegarde a permis d'automatiser et de sécuriser la sauvegarde des données. Grâce à son chiffrement intégré et sa compatibilité avec divers stockages, il offre une flexibilité appréciable pour les entreprises comme pour les particuliers. Cependant, Duplicati ne permet pas un suivi en temps réel des sauvegardes en cours et ne fournit pas d'indications précises sur l'espace de stockage disponible, ce qui pourrait compliquer la gestion des capacités de sauvegarde. Mais malgré ces points, Duplicati reste une solution fiable pour la protection des données.

Conclusion

Dans ce chapitre, nous avons montré l'installation de Duplicati puis expliqué les étapes d'une sauvegarde. Ensuite, nous avons effectué la simulation d'une panne matérielle afin de tester la restauration de Duplicati. Nous avons pu constater que Duplicati a restauré les fichiers avec succès. Cela permettra aux utilisateurs d'effectuer leurs sauvegardes en toute sécurité et de s'assurer d'une restauration efficace en cas d'attaques ou de catastrophes naturelles.

Perspectives

Conscient que notre travail est perfectible, quelques améliorations peuvent encore être envisagées :

- Amélioration de la surveillance et des alertes : Intégrer des outils comme ELK Stack ou Prometheus pour améliorer la collecte et l'analyse des logs et des métriques, permettant de mieux détecter les anomalies et d'optimiser les alertes ;
- Intégration avec des HIDS : Ajouter des systèmes de détection d'intrusion sur hôtes (HIDS) pour surveiller les modifications et accéder à des alertes en temps réel sur toute activité suspecte ;
- Renforcement de l'accès à Duplicati : Restreindre l'accès aux ressources critiques de Duplicati en appliquant des règles d'IP et en utilisant des contrôles d'accès basés sur des rôles (RBAC).

Ces améliorations permettront d'optimiser encore plus la fiabilité et la sécurité des sauvegardes.

Conclusion Générale

La mise en place d'un système de sauvegarde efficace est essentielle pour assurer la protection des données en entreprise. Ce mémoire a démontré que Duplicati est une solution open-source fiable et flexible, permettant d'automatiser les sauvegardes tout en garantissant la sécurité des fichiers grâce au chiffrement. À travers ce projet, nous avons exploré le déploiement, la configuration et les tests de restauration, tout en simulant une panne matérielle pour évaluer la résilience du système. Les résultats obtenus montrent que Duplicati est une solution adaptée aux besoins des entreprises, offrant un bon équilibre entre simplicité, efficacité et sécurité. En conclusion, l'adoption de Duplicati permet aux organisations de renforcer leur politique de sauvegarde et de récupération des données, réduisant ainsi les risques liés aux pertes accidentelles ou aux cyberattaques. Il reste toutefois important de surveiller régulièrement les sauvegardes pour s'assurer de leur bon fonctionnement.

Bibliographie

[1] Chen L., Zhao M. *"A Review on Cloud-Based Backup Solutions for Enterprise Data Protection." International Journal of Cloud Computing and Services Science*, 10(3), 45-60, 2021

[2] Simmons J., Daniel, R. *Data Backup and Recovery : Best Practices for Protecting Critical Information.* O'Reilly Media, 2020

[3] Von Solms R., Van Niekerk, J. *"From Information Security to Cyber Security." Computers & Security,* . 38, 97-102, 2013

Webographie

[1] Plus de 195 millions de données compromises en 2024.https://www.lemondeinformatique.fr/actualites/lire-plus-de-195-millions-de-donnees-compromises-en-2024-95729.html Consulté en Janvier 2025

[2] Récupération de données.https://fr.wikipedia.org/wiki/R%C3%A9cup%C3%A9ration_de_donn%C3%A9es Consulté en Janvier 2025

[3] Qu'est ce que l'authentification à 2 facteurs ?https://www.microsoft.com/fr-fr/security/business/security-101/what-is-two-factor-authentication-2fa Consulté en Mars 2025

[4] Quelles sont les 10 cyberattaques les plus courantes en entreprises.https://bigmedia.bpifrance.fr/nos-dossiers/quelles-sont-les-10-cyberattaques-les-plus-courantes-en-entreprise#top-10-des-cyberattaques-les-plus-courantes-en-e. Consulté en Janvier 2025

[5] Qu'est ce que la sauvegarde des données ?.https://aws.amazon.com/fr/what-is/data-backup/#:~:text=La%20sauvegarde%20des%20donn%C3%A9es%20est%20une%20fonction%20de%20protection%20des,dans%20un%20%C3%A9tat%20ant%C3%A9rieur%20souhait%C3%A9. Consulté en Janvier 2025

[6] Logiciel de sauvegarde : sauvegarde incrémentielle ou différentielle avec Iperius. https://www.iperiusbackup.net/fr/logiciel-de-sauvegarde-sauvegarde-incrementielle-ou-differentielle-avec-iperius/. Consulté en Février 2025

[7] Stockage ou sauvegarde de données, quelle est la différence.https://www.trinaps.com/2024/07/09/stockage-ou-sauvegarde-de-donnees-quelle-est-la-difference/#:~:text=Le%20stockage%20est%20utilis%C3%A9%20pour,de%20perte%20ou%20de%20corruption. Consulté en Janvier 2025

[8] Télécharger Veam Agent.https://www.clubic.com/telecharger-fiche437076-veeam-agent-pour-windows.html Consulté en Janvier 2025

[9] EaseUs Todo Backup : Avis, Prix et Alternatives.https://www.appvizer.fr/services-informatiques/sauvegarde/easeus-backup Consulté en Janvier 2025

[10] Installation-Manuel d'utilisation de Duplicati 2.https://prev-docs.duplicati.com/en/latest/02-installation/ Consulté en Janvier 2025

[11] Introduction-Manuel d'utilisation de Duplicati 2.https://prev-docs.duplicati.com/en/latest/01-introduction/ Consulté en Janvier 2025

[12] FBackup : Avis, Prix et Alternatives.https://www.appvizer.fr/services-informatiques/sauvegarde/fbackup Consulté en Janvier 2025

[13] Iperius Backup. https://www.iperiusbackup.fr/backup-software-windows.aspx#compare. Consulté en Décembre 2024

[14] Todo Backup Free - Logiciel de sauvegarde gratuit - EaseUS.https://www.easeus.fr/logiciel-de-sauvegarde/todo-backup-free.html. Consulté en Décembre 2024

[15] A propos d'FBackup.https://fr.fbackup.com/fbackup.html#section-features. Consulté en Décembre 2024

[16] Duplicati. https://duplicati.com/ Consulté en Janvier 2025

[17] Veam-agent-feature-comparison-ds.pdf. https://www.veeam.com/veeam_agents_feature_comparison_ds.pdf Consulté en Février 2025

[18] Missions et attributions-CAGD-Bénin Debt info. https://www.cagd.bj/missions-attributions/ Consulté en Février 2025

[19] Auth0 vs Okta. https://www.joinsecret.com/fr/compare/auth0-vs-okta Consulté en Mars 2025

Annexe

POLITIQUE DE SAUVEGARDE ET DE GESTION DES DONNEES

1. Objectifs et portée

Cette politique vise à garantir la protection, la disponibilité et l'intégrité des données critiques de l'entreprise. Elle s'applique à toutes les données numériques stockées sur les serveurs, postes de travail, bases de données et services cloud.

2. Responsabilités

Le Département des Systèmes d'Information (DSI) ou le Responsable de la Sécurité des Systèmes d'Information (RSSI) est chargé de définir et de superviser l'application de cette politique. Les administrateurs systèmes sont responsables de l'implémentation et du suivi des sauvegardes. Ils doivent s'assurer que les procédures sont bien respectées et que les sauvegardes sont effectuées conformément aux standards définis. Les employés doivent suivre les bonnes pratiques établies et signaler tout incident susceptible d'affecter l'intégrité des données.

3. Déterminer les données à sauvegarder et leur criticité

Les données critiques, telles que les bases de données clients, les informations financières ou les données RH, doivent faire l'objet d'une protection renforcée avec des sauvegardes fréquentes et sécurisées. Les données importantes, comme les documents internes et les fichiers de projet, doivent être sauvegardées régulièrement, mais ne nécessitent pas forcément une récupération immédiate en cas de sinistre. Enfin, les données non essentielles, telles que les fichiers temporaires et les logs système, peuvent être exclues des sauvegardes ou archivées selon les besoins. Cette classification permet d'optimiser l'utilisation des ressources et d'adapter la stratégie de sauvegarde en fonction des priorités de l'organisation.

4. Gestion des accès et des permissions

L'accès aux sauvegardes doit être strictement contrôlé afin d'éviter toute modification ou suppression accidentelle ou malveillante. Seuls les administrateurs et les utilisateurs autorisés peuvent accéder aux fichiers de sauvegarde. Le principe du moindre privilège est appliqué : chaque utilisateur ne peut accéder qu'aux données nécessaires à l'exercice de ses fonctions.

5. Stratégie de sauvegarde

La stratégie adoptée repose sur le principe du 3-2-1, garantissant une redondance optimale des données. Ce principe stipule que :

- Trois copies des données doivent être conservées : l'originale et deux copies de sauvegarde.
- Deux supports de stockage différents doivent être utilisés pour minimiser les risques de défaillance.
- Une copie hors site doit être stockée dans un emplacement distant ou dans le cloud pour protéger contre les catastrophes locales.

6. Type et fréquence de sauvegarde

Les sauvegardes doivent se faire comme suit : sauvegarde incrémentielle chaque jour, sauvegarde complète chaque semaine. Il faut également faire des sauvegardes mensuelles et annuelles et aussi des sauvegardes des postes des utilisateurs avant chaque congés et missions.

7. Rétention des sauvegardes

Type de sauvegarde	Fréquence	Rétention
Sauvegarde incrémentielle	Quotidienne	30 jours
Sauvegarde complète	Hebdomadaire	3 mois
Sauvegarde mensuelle	Mensuelle	1 an
Sauvegarde annuelle	Annuelle	5 ans

8. Stockage et sécurisation des sauvegardes

Les sauvegardes doivent se faire sur un serveur en local et hors site dans le cloud ou au niveau du centre de données national. Aussi, les sauvegardes de données en papier doivent être stockées dans des armoires ignifuges ainsi que tout document confidentiel et important et les disques amovibles pour les protéger contre les risques d'incendie. Les sauvegardes doivent êtres chiffrés avant d'être envoyées sur les différents supports de stockage.

9. Gestion du chiffrement et de l'intégrité des sauvegardes

La sécurité des sauvegardes repose sur l'utilisation d'un chiffrement robuste afin de protéger les données contre tout accès non autorisé. Toutes les sauvegardes doivent être chiffrées avant leur stockage, en utilisant des algorithmes éprouvés tels que AES-256. L'intégrité des sauvegardes est également une priorité. Chaque fichier doit être vérifié via des hashs cryptographiques (SHA-256) afin de détecter toute altération ou corruption. Des tests de restauration doivent être effectués régulièrement pour s'assurer que les fichiers sauvegardés restent exploitables et conformes à leur version originale.

10. Automatisation et surveillance des sauvegardes

Pour garantir une exécution fiable et efficace des sauvegardes, un système d'automatisation est mis en place. Des outils comme Duplicati, Veeam ou autres sont utilisés pour planifier et exécuter les

sauvegardes sans intervention manuelle. Un tableau de bord de supervision permet aux administrateurs de suivre l'état des sauvegardes en temps réel. En cas de problème, un système d'alerte envoie des notifications aux responsables pour une intervention rapide. Des rapports hebdomadaires sont générés afin de documenter l'état des sauvegardes et d'identifier d'éventuelles anomalies.

11. Formation des employés et bonnes pratiques

Les employés doivent être sensibilisés à l'importance des sauvegardes et formés aux bonnes pratiques de gestion des données. Des sessions de formation sont organisées annuellement pour rappeler les règles de sécurité et les procédures à suivre.
Les bonnes pratiques incluent :

- Ne jamais stocker les sauvegardes sur le même disque que les fichiers d'origine.
- Vérifier régulièrement les sauvegardes et tester leur restauration.
- Utiliser des supports de stockage sécurisés et chiffrés.
- Éviter les sauvegardes sur des supports non protégés (ex : clés USB sans chiffrement).
- Respecter les règles d'accès et signaler toute anomalie ou tentative d'intrusion.

12. Gestion des restaurations et continuité d'activité

La politique de sauvegarde doit inclure des objectifs de reprise d'activité définis par le RPO (Recovery Point Objective) et le RTO (Recovery Time Objective).

- Le RPO détermine la quantité maximale de données pouvant être perdues en cas d'incident. Il est fixé à 24 heures.
- Le RTO définit le temps maximal nécessaire pour restaurer les données et reprendre les activités, fixé à 4 heures.

Un plan de restauration détaillé est mis en place pour garantir une récupération efficace des fichiers critiques en cas de sinistre. Chaque restauration doit être testée pour vérifier son bon fonctionnement et éviter toute perte de données.

13. Plan de reprise après sinistre

- Dès qu'un incident est détecté, sa nature ainsi que sa portée doivent être identifiées.
- Une analyse des données et systèmes impactés doit être effectuée.
- L'équipe chargée de la communication doit informer les parties concernées.
- Les données critiques à restaurer en priorité doivent être identifiées, en fonction de l'impact sur les opérations.
- Les données critiques doivent être restaurées sous 4 heures, les données opérationnelles en moins de 24 heures, et les données archivées selon les besoins.
- La dernière sauvegarde valide doit être restaurée sur un serveur de test afin de vérifier son intégrité avant son déploiement en production.

- La sauvegarde doit être validée par un spécialiste de la sécurité avant la remise en service du système.
- En cas d'indisponibilité du site principal, un site de secours doit être activé pour garantir la continuité des opérations, en utilisant la dernière sauvegarde disponible.
- Il faut s'assurer que les services critiques sont bien remis en production.
- Des tests réguliers doivent être exécutés pour s'assurer de l'efficacité du plan et celui ci doit être mis à jour au minimum une fois par an.

14. Conformité et mise à jour

Cette politique est révisée annuellement pour s'adapter aux évolutions technologiques et aux nouvelles menaces en matière de cybersécurité. Elle doit également respecter les réglementations en vigueur.

MANUEL D'UTILISATION DE DUPLICATI

1. Présentation

Duplicati est un logiciel de sauvegarde gratuit qui permet d'automatiser la sauvegarde de vos fichiers vers différents types de destinations, locales ou distantes, tout en les chiffrant et en les compressant.

Fonctionnalités de Duplicati

- Chiffrement sécurisé : Duplicati protège vos données avec un chiffrement très fort (AES-256). Cela signifie que vos fichiers sont illisibles sans le mot de passe. Le chiffrement se fait avant que les fichiers quittent votre ordinateur.

- Sauvegarde intelligente : La première sauvegarde copie tout. Ensuite, seules les modifications sont sauvegardées. Cela économise du temps et de l'espace, même pour de gros fichiers.

- Compression automatique : Avant d'envoyer les fichiers, Duplicati les compresse pour gagner de la place. Il détecte les fichiers déjà compressés (comme les vidéos ou les images) et ne les recompresse pas.

- Vérification automatique : Duplicati vérifie régulièrement que vos fichiers de sauvegarde ne sont pas endommagés.

Détection des doublons : Duplicati repère les fichiers identiques ou similaires et ne les sauvegarde qu'une seule fois. Même si vous déplacez ou renommez un fichier, il reconnaît que le contenu est le même.

- Résistance aux erreurs : Duplicati gère les coupures de réseau ou les interruptions. Si une sauvegarde est interrompue, elle reprend là où elle s'était arrêtée. Si un fichier distant est cassé, il essaie de le réparer avec la copie locale.

- Interface Web : Vous utilisez Duplicati directement depuis votre navigateur, comme une page web. Cela fonctionne aussi sur des machines sans écran (comme les NAS). Il suffit d'y accéder à distance.

- Ligne de commande pour les professionnels : Pour les administrateurs système, tout peut aussi être géré avec des commandes dans un terminal ou dans des scripts automatiques.

- Métadonnées conservées : Quand vous restaurez un fichier, Duplicati remet aussi les dates de création/modification et les autorisations. Mais vous pouvez choisir de ne pas restaurer les autorisations si nécessaire.

- Planification automatique : Duplicati peut faire des sauvegardes automatiquement : chaque jour, chaque semaine, ou même à des moments précis (par exemple : tous les lundis à 15h).

- Mises à jour automatiques : Duplicati peut se mettre à jour tout seul avec la dernière version disponible.

- Sauvegarde de fichiers ouverts : Certains fichiers en cours d'utilisation ne peuvent pas être copiés. Duplicati utilise des outils spéciaux (VSS sur Windows, LVM sur Linux) pour créer un instantané et sauvegarder ces fichiers sans erreur.

Backends pris en charge

Duplicati peut effectuer des sauvegardes vers un grand nombre de cibles. Pour les sauvegardes locales, tous les périphériques connectés localement ou à l'aide d'un chemin UNC (Universal Naming Convention) peuvent être utilisés, tels que :

- Disque dur USB externe
- Clé USB
- Dossier partagé sur un autre ordinateur du même réseau
- Stockage en réseau (NAS)

Les sauvegardes vers ces cibles à l'aide des protocoles réseau standard suivants sont prises en charge :

- FTP
- FTP (Alternative)
- Stockage d'objets OpenStack / Swift
- S3 Compatible
- SFTP (SSH)
- WebDAV

Les fournisseurs de stockage cloud suivants sont pris en charge nativement par Duplicati :

- Amazon S3
- Blob Azure
- Stockage dans le cloud B2
- Box.com
- Dropbox
- Stockage Google Cloud
- Google Drive
- Jottacloud
- Mega.nz
- Groupes Microsoft Office 365
- Microsoft OneDrive pour les entreprises
- Microsoft OneDrive
- Microsoft SharePoint
- Stockage simple OpenStack

- Rackspace CloudFiles
- Rclone
- Cloud décentralisé Sia
- Storj (ex Tardigrade) Stockage cloud décentralisé
- Tencent COS

Autres cibles prises en charge :

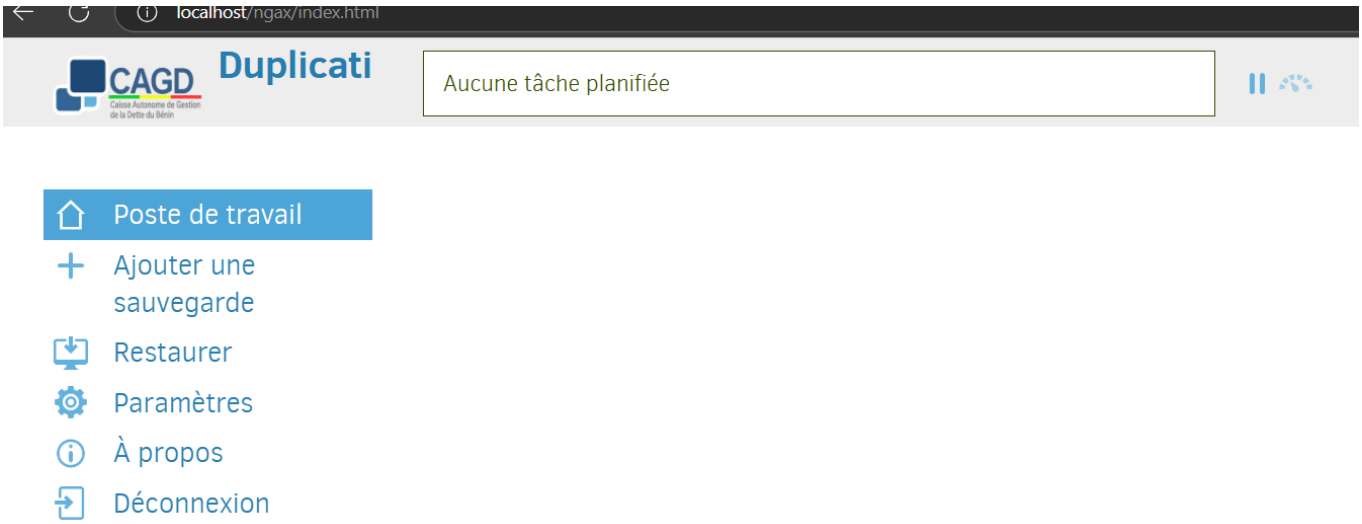
- Tahoe-LAFS

2. Lancer Duplicati

Une fois installé, cliquez sur l'icône Duplicati (dans la barre des tâches ou dans le menu Démarrer). L'interface s'ouvre automatiquement dans votre navigateur web avec un menu à gauche.

Description des éléments du menu

« **Poste de travail** » : Quittez le sous-menu actuel et revenez à l'écran d'accueil.
« **Ajouter une sauvegarde** » : Ajoutez une nouvelle configuration de sauvegarde.
« **Restaurer** » : Restaurez des fichiers à partir d'une tâche de sauvegarde déjà configurée ou directement à partir du backend ou d'un fichier de configuration importé.
« **Paramètres** » : Modifiez les paramètres généraux du programme et définissez les paramètres par défaut pour toutes les tâches de sauvegarde.
« **A propos** » : Affichez des informations sur la version actuelle de Duplicati et des informations système.
« **Déconnexion** » : Se déconnecte de l'interface utilisateur graphique de Duplicati.

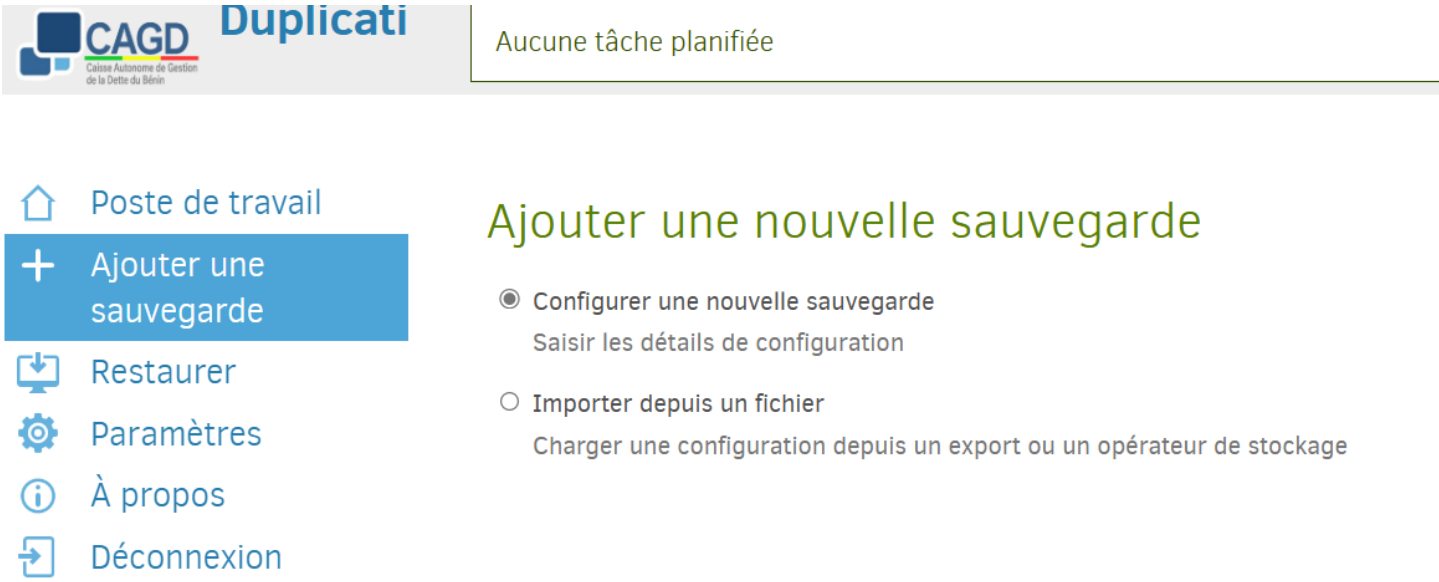


3. Créer une sauvegarde

1. Cliquez sur "Ajouter une sauvegarde"

2. Choisissez "Configurer une nouvelle sauvegarde"

3. Choisissez "Configurer une nouvelle sauvegarde"



Étape 1 : Général

Entrez un nom descriptif, une description (optionnel) puis sélectionnez le type de chiffrement et spécifiez une clé de chiffrement forte. Les doublons donnent une indication de la force de la clé que vous avez saisie. En option, Duplicati peut générer une clé de cryptage forte pour vous.
- Chiffrement :

- Aucun chiffrement : Les fichiers seront stockés en clair.
- AES-256 : Recommandé. Vos données sont protégées par un mot de passe.

Si vous choisissez cette option, saisissez un mot de passe de chiffrement. Ce mot de passe est obligatoire pour restaurer les fichiers plus tard.
Cliquez sur Suivant.

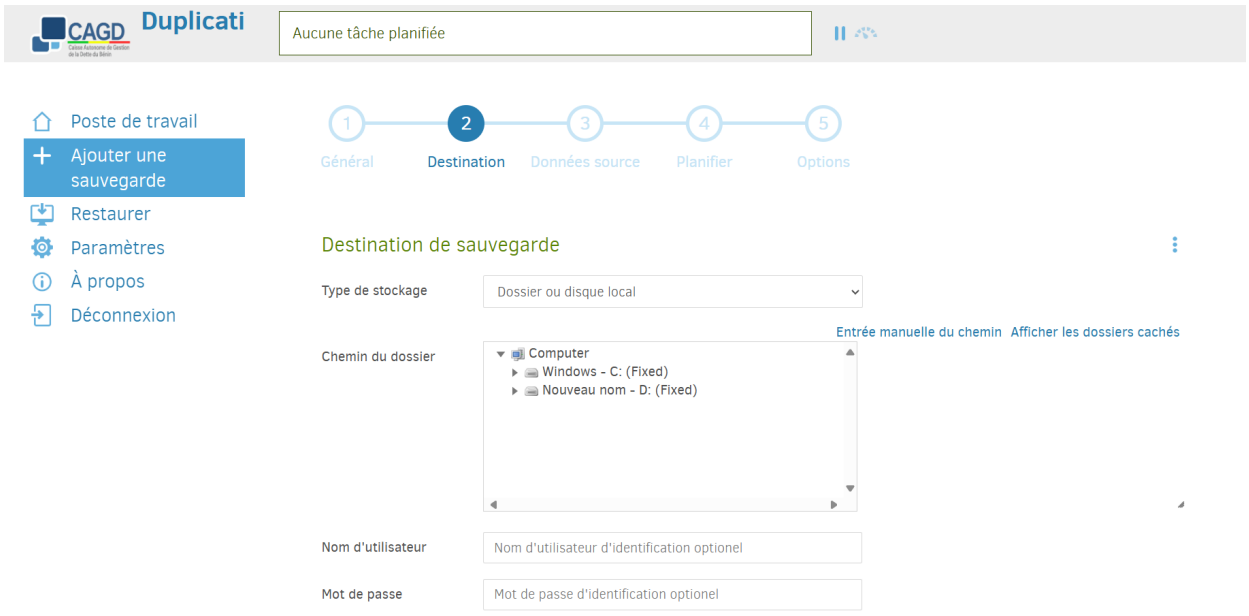


Étape 2 : Destination

A l'étape 2, vous pouvez spécifier le type de stockage que vous souhaitez utiliser pour vos sauvegardes et entrer l'URL, le chemin d'accès et les informations d'identification.
- Type de stockage (choisir dans le menu déroulant) :

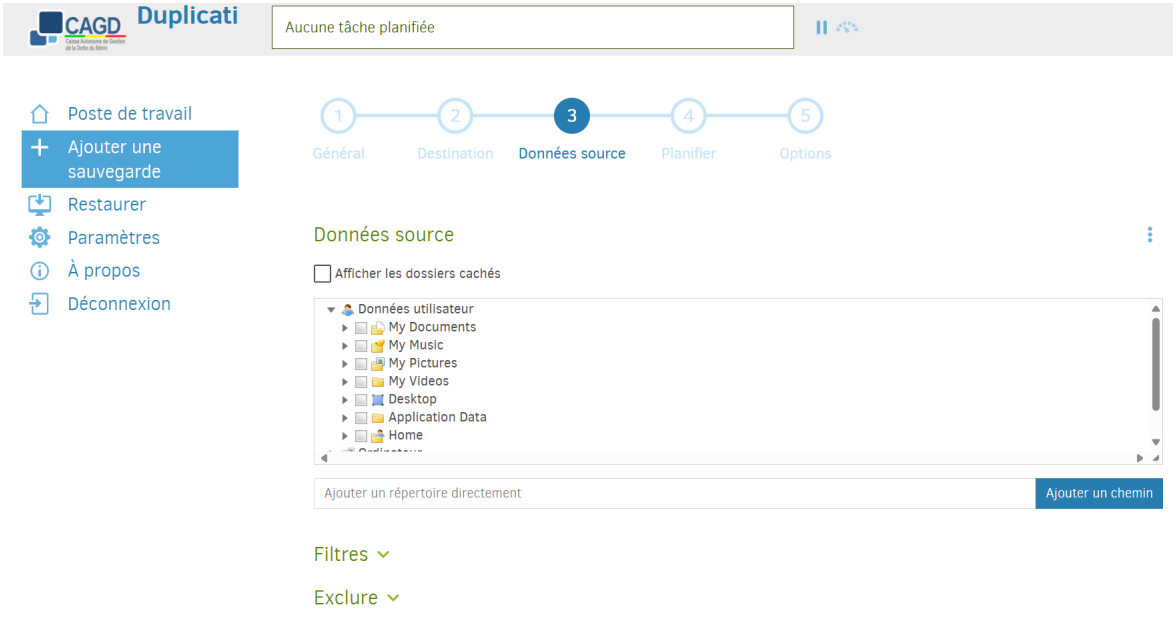
- Dossier local ou sur un lecteur réseau
- FTP / SFTP (SSH)
- WebDAV
- Stockage dans le Cloud : OneDrive, Google Drive, Dropbox, Amazon S3, etc.
- OpenStack, Microsoft Azure, etc.

- Nom d'utilisateur / mot de passe (si nécessaire)
- Test de connexion : Duplicati essaiera de se connecter au backend en utilisant les informations fournies. Si Duplicati peut se connecter au backend, mais que le dossier spécifié n'existe pas, Duplicati peut le créer pour vous.
Sous **Options avancées**, vous pouvez spécifier un certain nombre de paramètres spécifiques au type de stockage que vous avez sélectionné. Choisissez un paramètre dans la liste pour l'ajouter aux options avancées et modifiez le paramètre si nécessaire.
Cliquez sur Suivant.



Étape 3 : Dossiers sources

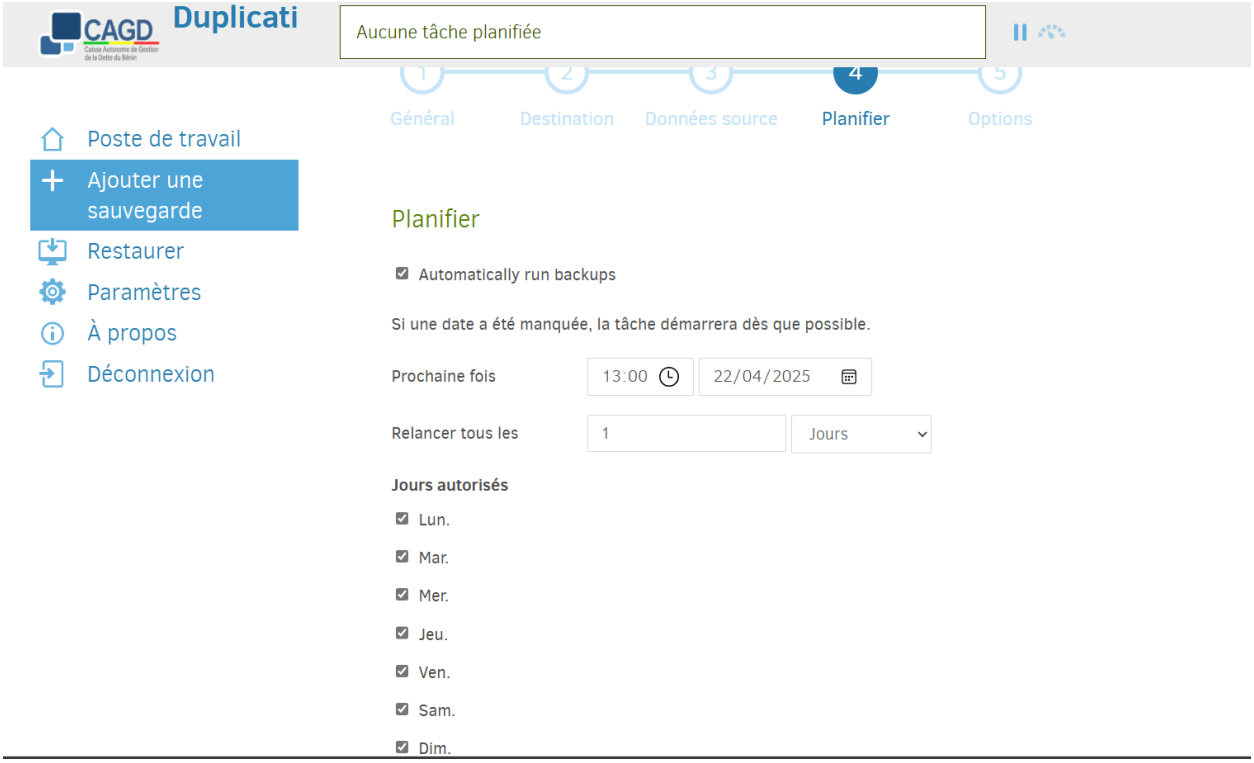
A l'étape 3, vous pouvez sélectionner les fichiers et dossiers que vous souhaitez inclure dans la sauvegarde à partir du sélecteur de fichiers. Seuls les fichiers et dossiers locaux peuvent être sélectionnés à l'aide du sélecteur de fichiers. Si vous souhaitez inclure des dossiers partagés dans votre réseau local, vous devez spécifier le chemin d'accès dans la zone de texte située sous le sélecteur de fichiers. Cliquez sur Suivant.



Étape 4 : Planification

A l'étape 4, vous pouvez planifier vos sauvegardes. La sélection de l'option **Exécuter automatiquement les sauvegardes** désactive la planification de cette tâche de sauvegarde. Une fois désactivée, vous pouvez démarrer la tâche de sauvegarde manuellement lorsque vous souhaitez qu'elle s'exécute. Si vous laissez cette option activée, vous pouvez spécifier la fréquence et l'heure de démarrage de la sauvegarde. Vous pouvez également exclure un ou plusieurs jours de la semaine.
Si une tâche de sauvegarde ne respecte pas la planification définie, par exemple si l'ordinateur est

hors tension, la tâche de sauvegarde commencera dès que possible après l'heure spécifiée.
- Fréquence : Quotidienne, hebdomadaire, mensuelle, ou personnalisée.
- Heure de début : Heure à laquelle la tâche doit s'exécuter.
Cliquez sur Suivant.



Étape 5 : Options

A l'étape 5, vous pouvez définir la taille du volume de téléchargement et le nombre de sauvegardes disponibles pour les opérations de restauration.
Un volume de téléchargement est un fichier compressé chiffré qui contient une partie de votre sauvegarde. Pour les opérations de sauvegarde normales, vous pouvez conserver cette valeur inchangée, mais dans certains scénarios, par exemple les sauvegardes très volumineuses, vous pouvez augmenter la taille pour réduire le nombre de fichiers à l'emplacement de stockage distant. La taille par défaut d'un volume de téléchargement est de 50 Mo.
- Rétention des sauvegardes : elle peut se faire de 5 façons

Conservez toutes les sauvegardes : les sauvegardes ne seront jamais supprimées. Il s'agit de l'option la plus sûre, mais la capacité de stockage à distance ne cessera d'augmenter.

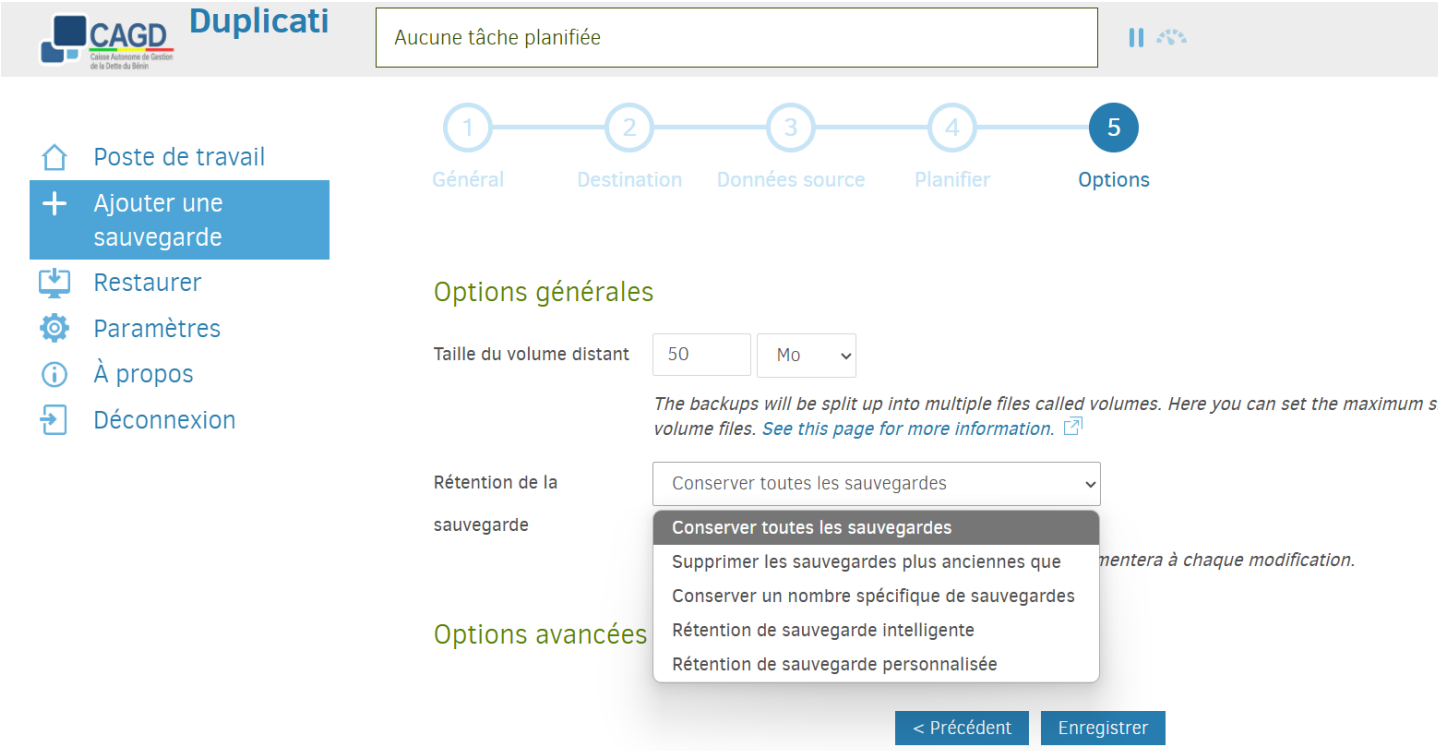
Supprimer les sauvegardes antérieures à : les sauvegardes antérieures à un certain nombre de jours, de semaines, de mois ou d'années seront supprimées.

Conservez un nombre spécifique de sauvegardes : le nombre spécifié de versions de sauvegarde sera conservé, toutes les sauvegardes plus anciennes seront supprimées.

Conservation des sauvegardes personnalisées : Entrez vos propres paramètres dans la zone de texte qui s'affiche.

Conservation intelligente des sauvegardes : conserve une sauvegarde pour chacun des 7 derniers jours, chacune des 4 dernières semaines et chacun des 12 derniers mois.

- Options avancées (pour les utilisateurs expérimentés)
Cliquez sur Enregistrer et la tâche de sauvegarde apparaitra dans le menu principal.

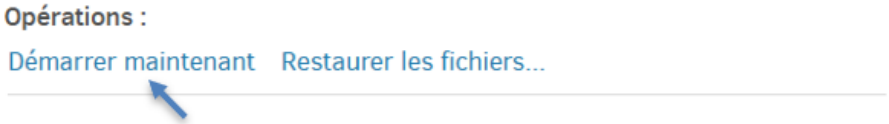


Si vous disposez d'un fichier de configuration précédemment exporté, vous pouvez l'importer en sélectionnant Importer à partir d'un fichier dans le menu Ajouter une sauvegarde. A l'étape suivante, vous pouvez accéder à l'emplacement où votre fichier de configuration est stocké, entrer une phrase de passe si le fichier de configuration est chiffré et cliquer sur Importer.

4. Lancer une sauvegarde

Il existe 3 façons de démarrer une sauvegarde à l'aide de l'interface utilisateur graphique :

- S'il s'agit d'une sauvegarde programmée, attendez simplement la prochaine heure programmée. La sauvegarde démarrera automatiquement.
- Cliquez sur **Exécuter maintenant**, juste sous le nom de la sauvegarde.
- Cliquez sur le nom de la sauvegarde. Cliquez ensuite sur **Exécuter maintenant** sous **Opérations**.

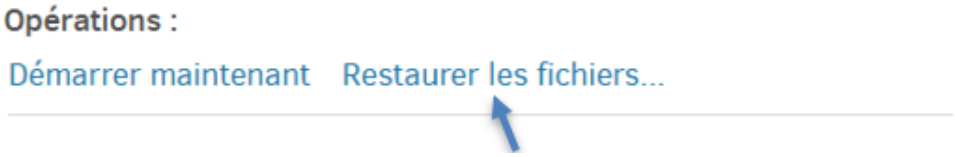


5. Restaurer une sauvegarde

A partir d'une sauvegarde

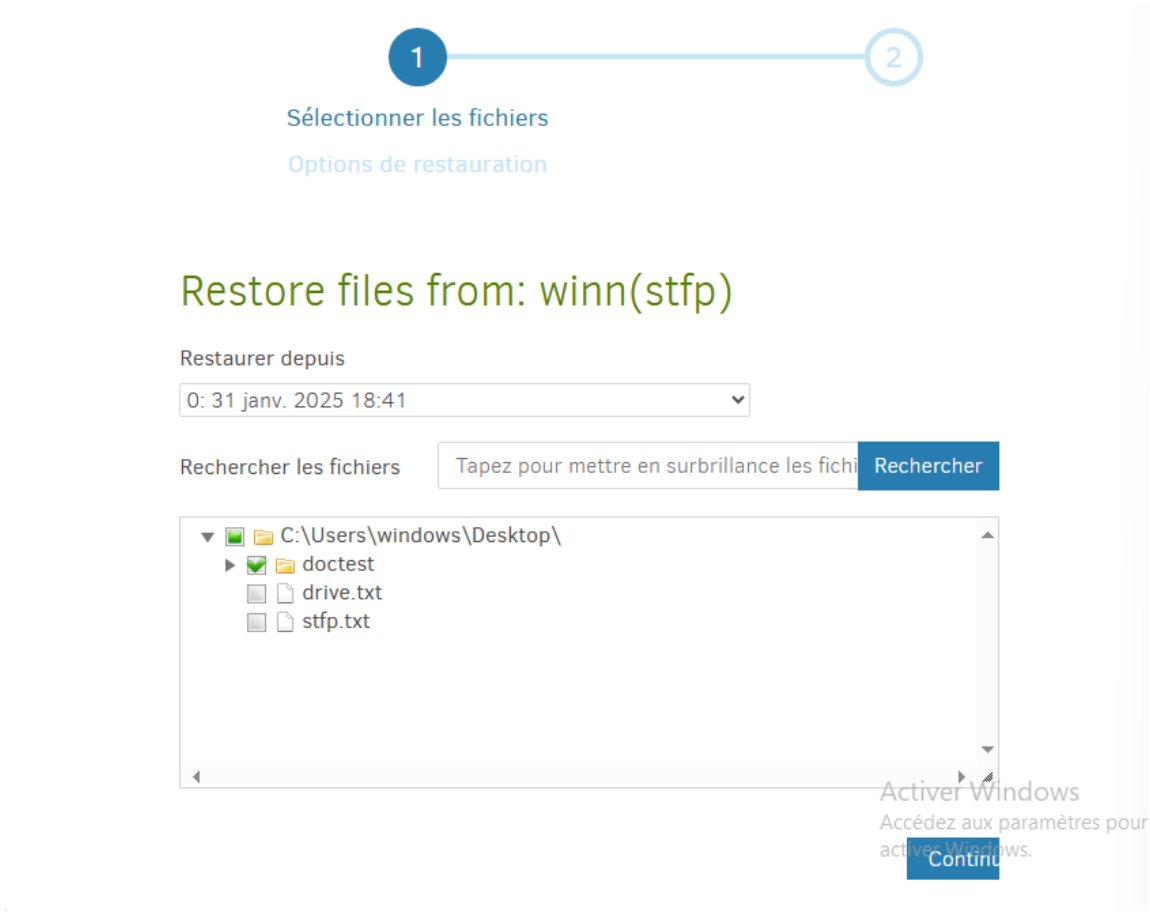
Si vous souhaitez restaurer un ou plusieurs fichiers à partir d'une sauvegarde, vous pouvez lancer l'assistant de restauration :

- En cliquant sur le nom de la sauvegarde et en cliquant sur **Restaurer** les fichiers sous **Opérations**.



- En cliquant sur **Restaurer** dans le menu principal, sélectionnez la sauvegarde à partir de laquelle vous souhaitez restaurer et cliquez sur Suivant.

L'assistant de restauration se compose de deux étapes :
A l'étape 1, vous pouvez spécifier ce que vous souhaitez restaurer et à partir du point de restauration à partir duquel vous souhaitez restaurer ces fichiers en sélectionnant une date et une heure derrière **Restaurer à partir de**. Ensuite, sélectionnez tous les fichiers et dossiers que vous souhaitez restaurer.



Cliquez sur Continuer pour passer à l'étape 2.

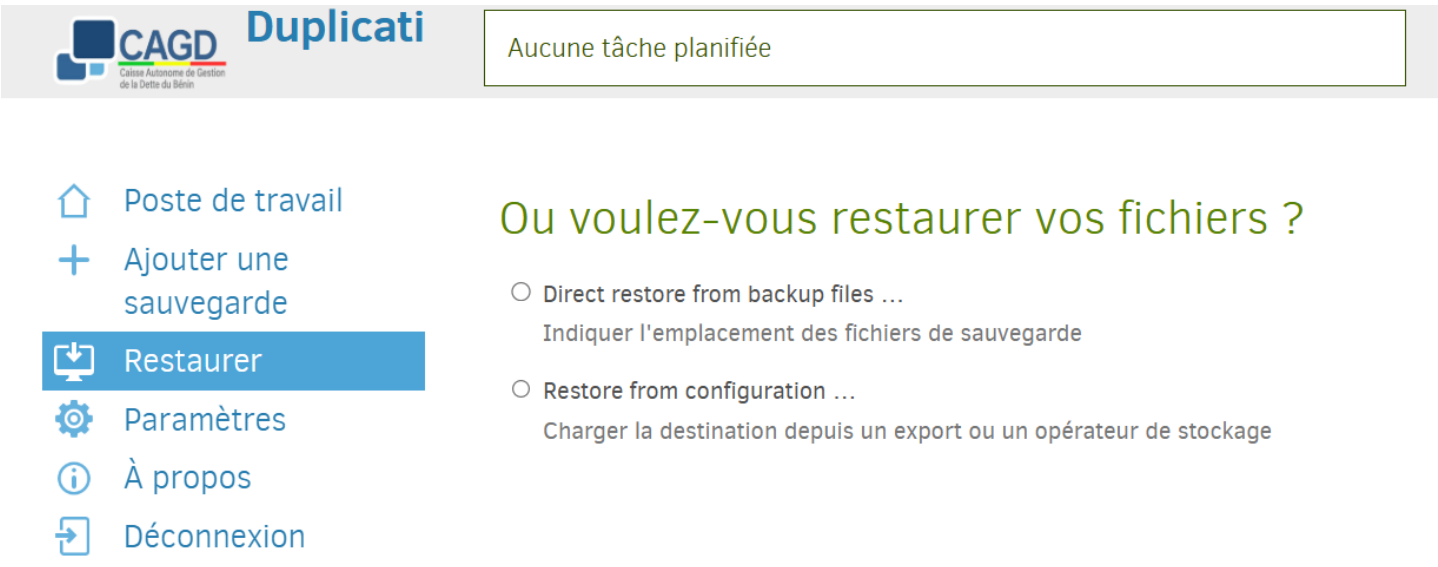
A l'étape 2, vous pouvez choisir l'emplacement auquel vous souhaitez restaurer les fichiers et fournir quelques options pour l'opération de restauration. Choisissez **Emplacement d'origine** pour restaurer les fichiers à leur emplacement d'origine. Vous pouvez aussi sélectionner un autre emplacement pour restaurer vos fichiers en tapant le chemin d'accès au dossier ou en sélectionnant le dossier racine à l'aide du bouton **Parcourir**. Ensuite vous pouvez choisir d'écraser tout ce qui se trouve à l'emplacement de restauration choisi puis également restaurer les autorisations d'accès aux fichiers.



Cliquez ensuite sur Restaurer pour lancer l'opération de restauration proprement dite.

En cas de perte de l'installation de Duplicati

Pour restaurer vos fichiers en cas de perte de Duplicati, vous devez le faire directement à partir de la destination de sauvegarde. Pour cela, téléchargez et installez d'abord Duplicati.
Pour démarrer une opération de restauration sans tâche de sauvegarde configurée, cliquez sur **Restaurer** dans le menu principal.



Vous avez 2 options de restauration :

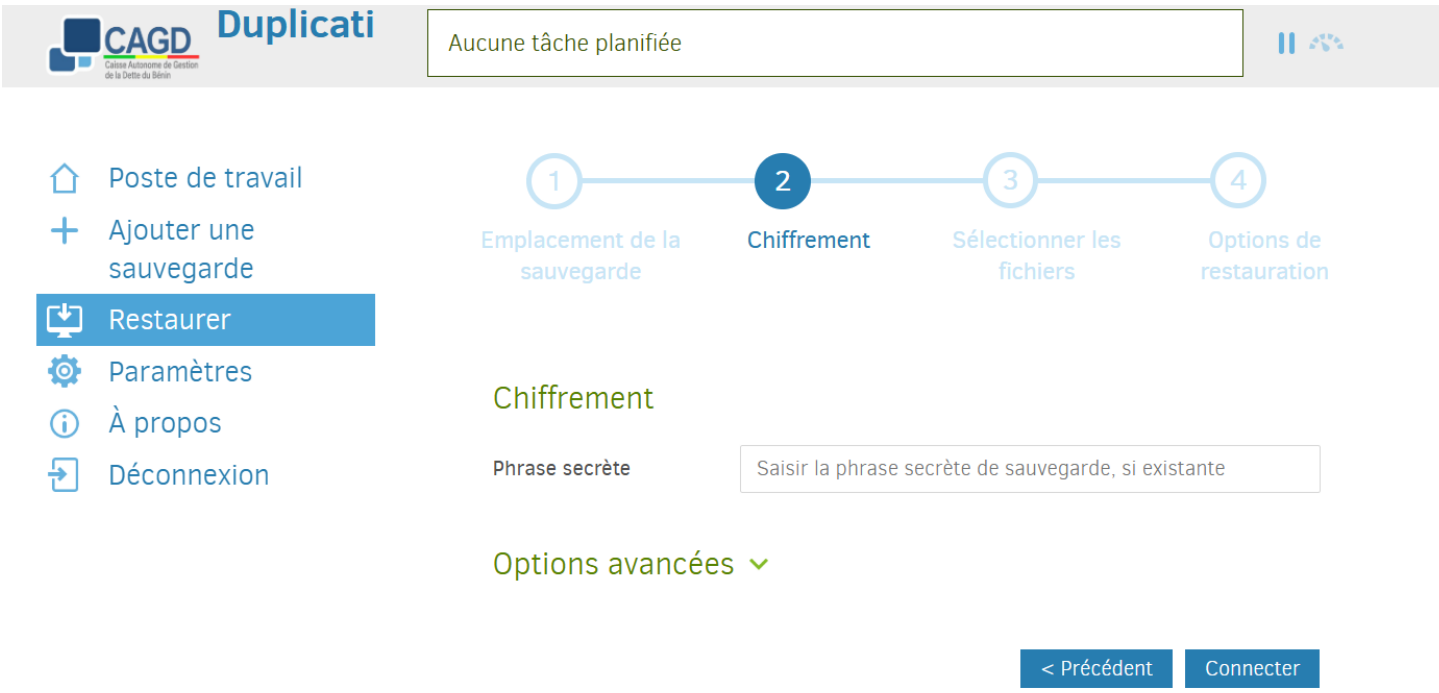
- Si vous avez une configuration exportée précédemment dans un fichier et que vous avez toujours accès à ce fichier, vous pouvez l'importer pour lancer ensuite la restauration.

- Dans le cas contraire, vous devez connaître l'URL du backend, les informations d'identification et la phrase de passe de sauvegarde. Une fois toutes les informations nécessaires saisies, vous pouvez commencer à restaurer vos fichiers.

Avec la deuxième option, la restauration se fera en 4 étapes :
A l'étape 1 (Emplacement de sauvegarde), vous devez sélectionner le type de stockage approprié et renseigner les informations requises pour vous connecter au stockage distant.



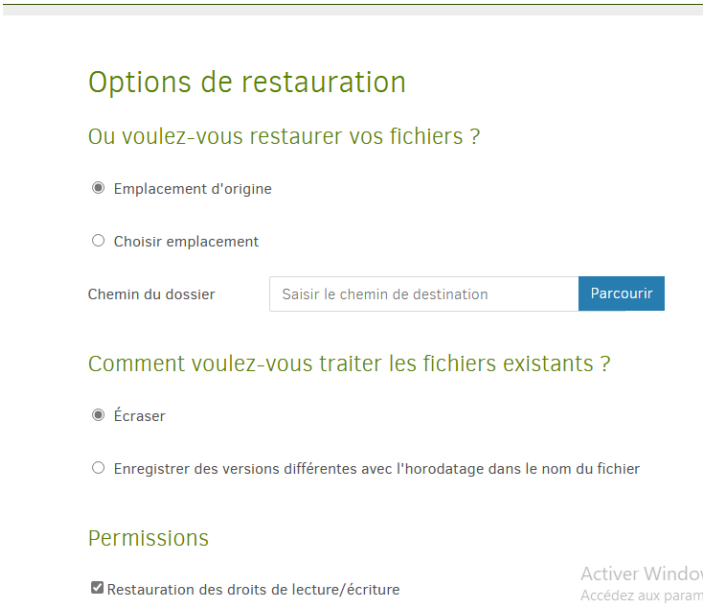
A l'étape 2 (Chiffrement), spécifiez la phrase secrète de sauvegarde et fournissez éventuellement une ou plusieurs options avancées.



A l'étape 3, vous devez sélectionner les fichiers à restaurer ainsi que la version souhaitée.



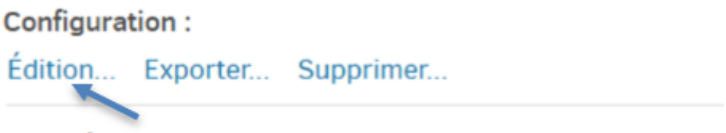
A l'étape 4 vous devez spécifier l'emplacement de restauration des fichiers et choisir d'écraser ou non tout ce qui se trouve à l'emplacement de restauration choisi puis également restaurer les autorisations d'accès aux fichiers.



6. Autres

Modifier une sauvegarde existante

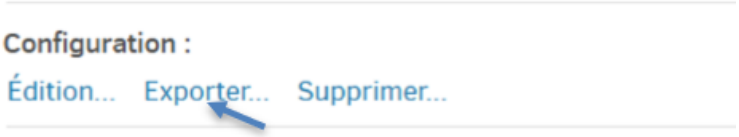
Pour modifier la configuration d'une tâche de sauvegarde, cliquez sur le nom de la tâche de sauvegarde, puis cliquez sur **Edition** sous **Configuration**. Vous revenez à l'assistant qui s'est affiché lors de l'ajout de la sauvegarde. La différence est que les 5 étapes sont déjà remplies avec les paramètres que vous avez choisis dans l'assistant d'ajout de sauvegarde. Vous pouvez parcourir l'Assistant en modifiant éventuellement certains paramètres et en cliquant sur **Suivant** jusqu'à ce que vous atteigniez la dernière étape de l'Assistant. Vous pouvez également cliquer sur le numéro de l'étape que vous souhaitez modifier dans le sélecteur en haut.



Si tous les paramètres sont corrects, cliquez sur le bouton **Enregistrer** à l'étape 5.

Exportation d'une configuration de tâche de sauvegarde

Pour exporter la configuration d'une tâche de sauvegarde, cliquez sur son nom, puis sur **Exporter** sous**Configuration**. Si vous souhaitez exporter vers un fichier, sélectionnez **A fichier** et cliquez sur le bouton **Exporter**. Si vous sélectionnez **Chiffrer le fichier**, vous pouvez entrer une phrase de passe pour brouiller votre fichier de configuration, ce qui le rend illisible pour les autres. Stockez la phrase de passe dans un endroit sûr car sans la phrase de passe, il est impossible d'extraire des informations du fichier de configuration. Lors de l'exportation vers un fichier, un fichier JSON standard contenant tous les paramètres de la configuration de la tâche de sauvegarde sélectionnée est généré. Ce fichier peut être utilisé ultérieurement pour l'importation dans une nouvelle installation de Duplicati si votre ordinateur est perdu à cause d'un sinistre.



Suppression d'une configuration de tâche de sauvegarde

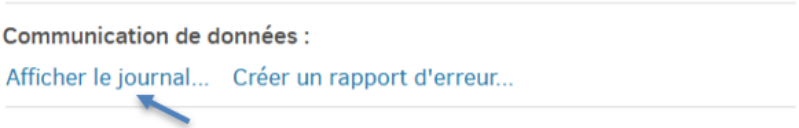
Pour supprimer une tâche de sauvegarde, cliquez sur le nom de la sauvegarde, puis sur **Supprimer** sous **Configuration**.



Si vous n'avez plus besoin des fichiers de sauvegarde eux-mêmes, Duplicati peut supprimer ces fichiers du backend, libérant ainsi de l'espace de stockage à distance. Si vous souhaitez vraiment supprimer également les fichiers de sauvegarde, sélectionnez **Supprimer les fichiers distants** et vous devez d'abord remplir un captcha pour des raisons de sécurité.

Affichage des fichiers journaux d'une tâche de sauvegarde

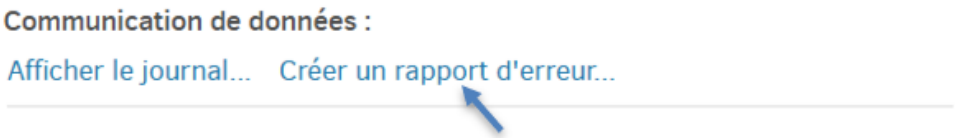
Vous pouvez afficher tous les messages et résultats liés aux opérations de tâche de sauvegarde. Pour cela, cliquez sur le nom de la sauvegarde, puis sur **Afficher le journal** sous **Communication de données** .



Les données de journal de la tâche de sauvegarde sélectionnée s'affichent. Vous pouvez choisir d'afficher les événements généraux ou les événements spécifiques aux opérations de backend, en cliquant sur le bouton **Général** ou **Distant**.

Création d'un rapport d'erreur

Un rapport de bogue contient des informations sur le système sur lequel Duplicati est installé, des informations sur l'installation de Duplicati elle-même. Pour créer un rapport de bogue, cliquez sur le nom de la sauvegarde, puis sur **Créer un rapport d'erreur** sous **Communication de données**.

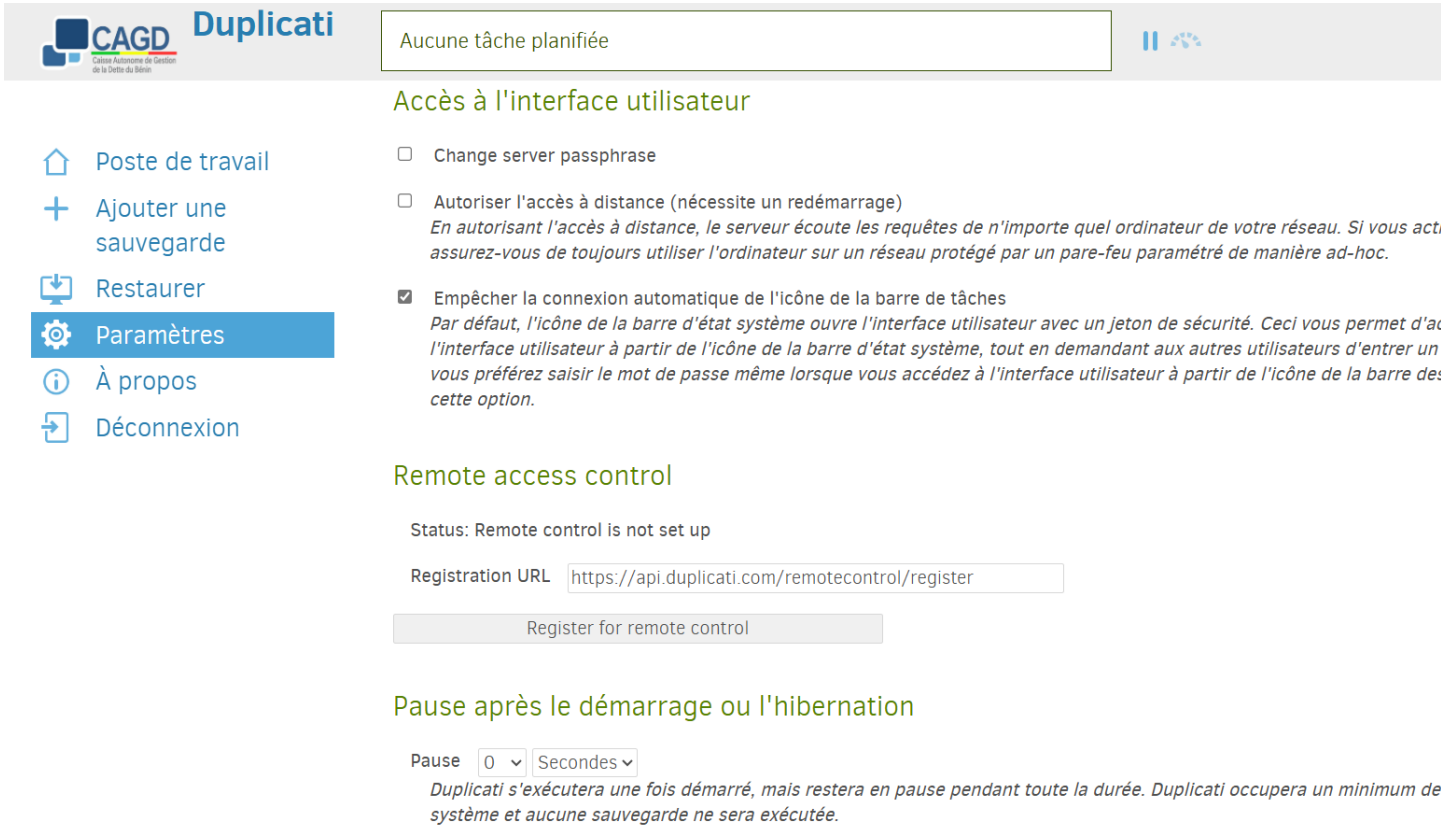


Une fois l'opération terminée, un message s'affiche et vous pouvez télécharger le rapport généré.

Paramètres dans Duplicati

Dans le menu **Paramètres**, vous pouvez spécifier différents types de paramètres :

- Modifier le mot de passe ;
- Définir un délai pour que Duplicati devienne actif après le démarrage ou la mise en veille prolongée ;
- Changer la langue de l'interface et choisir un schéma de couleurs ;
- Modifier le canal de mise à jour en sélectionnant le type de versions Duplicati que vous préférez ;
- Définir le niveau des rapports à envoyer (Information, Avertissement, Erreur ou Aucun) ;
- Générer une liste d'options avancées. Ces options seront appliquées à toutes les tâches de sauvegarde, à moins que les mêmes options avec une autre valeur ne soient spécifiées dans une configuration de tâche de sauvegarde particulière. Pour ajouter une option par défaut, ouvrez le menu déroulant en cliquant sur **Choisir une option**. Une longue liste s'affiche. Recherchez l'option que vous souhaitez définir comme option par défaut.



PROCEDURE EN CAS DE CORRUPTION DES DONNEES D'UN UTILISATEUR

1. Alerter

L'utilisateur victime alerte immédiatement l'administrateur système ou le service informatique dès qu'il constate un comportement anormal comme des fichiers inaccessibles ou renommés, des messages de rançon ou fichiers suspects…

2. Analyser l'incident et bloquer l'attaque

L'administrateur doit consulter les journaux système et les alertes des IDS pour identifier une adresse IP source ou suspecte et la bloquer puis identifier les fichiers chiffrés et l'étendue de l'attaque.

3. Supprimer les fichiers corrompus

Les fichiers corrompus identifiés sont supprimés du poste de l'utilisateur.

4. Restaurer les données via Duplicati

Les fichiers corrompus doivent être restaurer via Duplicati à partir de la sauvegarde antérieure à l'attaque dans un dossier temporaire pour vérification. Ensuite l'administrateur doit vérifier leur intégrité puis replacer les fichiers aux emplacements d'origine.

Après tout cela, la sécurité doit être renforcée en vérifiant les journaux de sauvegarde pour s'assurer que l'attaquant n'a pas altéré les sauvegardes puis éventuellement mettre à jour les règles de sécurité.

Table des matières

Dédicace ii

Remerciements iii

Résumé iv

. iv

Abstract v

. v

Table des figures vi

Liste des tableaux viii

Liste des acronymes ix

Glossaire 1

Introduction 2

1 Revue de littérature 4

Introduction 4

1.1 Définitions 4

1.1.1 Système d'Information 4

1.1.2 Protection des données 4

1.1.3 La restauration des données 4

1.1.4 L'automatisation des sauvegardes 5

1.1.5 L'authentification 2FA 5

1.2 Les cyberattaques 5

1.2.1 Définition 5

1.2.2 Types de cyberattaques 5

1.3 La sauvegarde des données 6

1.3.1 Définition 6

1.3.2 Principaux types de sauvegarde 6

1.3.3 Modes de stockage des sauvegardes 7

1.3.3.1 Stockage local 7

1.3.3.2 Stockage distant 7

1.3.3.3 Stockage hybride 8

1.4 Différence entre stockage de données et sauvegarde de données 8

1.5 Solutions de sauvegarde existantes . . . 8
1.5.1 Quelques solutions de sauvegarde . . . 8
1.5.2 Comparaisons . . . 8
Conclusion . . . 10

2 Choix et présentation de la solution de sauvegarde 11
Introduction . . . 11
2.1 Présentation de la Caisse Autonome de Gestion de la Dette (CAGD) et de son système de sauvegarde de données . . . 11
2.1.1 Présentation de la Caisse Autonome de Gestion de la Dette (CAGD) . . . 11
2.1.2 Présentation du système de sauvegarde de données de la CAGD . . . 11
2.2 Choix de la solution . . . 13
2.3 Présentation de Duplicati . . . 13
2.3.1 Généralité . . . 13
2.3.2 Composant de Duplicati . . . 13
2.3.3 Fonctionnalités . . . 14
2.3.4 Destinations de sauvegarde ou Backend . . . 16
2.4 Mécanismes de sécurité et de surveillance pour Duplicati . . . 17
2.4.1 Système d'authentification à 2 facteurs . . . 18
2.4.2 VPN pour le transfert sécurisé des sauvegardes . . . 18
2.4.3 La surveillance des sauvegardes . . . 18
2.5 Personnalisation du logo de Duplicati . . . 19
Conclusion . . . 19

3 Déploiement de la solution de sauvegarde et test de fonctionnalités 20
Introduction . . . 20
3.1 Installation de Duplicati . . . 20
3.2 Brève description des éléments du menu . . . 22
3.3 Configuration d'une nouvelle sauvegarde . . . 25
3.4 Test de fonctionnalités . . . 35
3.4.1 Scenario de test . . . 35
3.4.2 Restauration . . . 36
3.5 Discussion . . . 41
Conclusion . . . 41

Perspectives 42

Conclusion 43

Bibliographie 44

Webographie 45

Annexe 47

Table des matières 67