



Titre de l'exposé : Etude et mise en place d'une solution de stockage sécurisée de données PME (Petites et Moyennes Entreprises)

Membre du groupe

L3 - Sécurité des systèmes informatiques et industriels
KABRE Gérald

Année académique : 2024 – 2025

Sommaire

Table des matières

Introduction.....	3
I. Analyse des besoins.....	3
1.1. Les besoins spécifiques des PME	3
1.2. Menaces et risques liés aux données	3
1.3. Étude des solutions existantes	3
II. Conception de la solution.....	5
2.1. Choix de l'architecture cible et des technologies associées	5
2.2. Stratégies de sécurisation des données	6
2.3. Plan de sauvegarde et de reprise	6
2.4. Installation et configuration	7
2.5. Documentation technique	8
III. Validation et évaluation.....	8
3.1. Tests de sécurité (résultats attendus)	8
3.2. Tests de performance et disponibilité (résultats attendus)	9
3.3. Analyse coûts/bénéfices	9
IV. Cas pratique.....	10
4.1. Environnement de test.....	10
4.2. Installation et configuration de Nextcloud.....	11
4.3. Mise en place du RBAC (Role-Based Access Control)	13
4.4. Mise en place de la double authentification (MFA)	20
4.5. Chiffrement des données sensibles	25
4.6. Sauvegardes et restauration	26
V. Discussion et perspectives	27
Conclusion	27
Sources	28

Introduction

Dans l'économie numérique actuelle, les données représentent un actif stratégique. Les PME, souvent perçues comme des cibles secondaires, sont en réalité parmi les plus vulnérables aux cyberattaques, car elles disposent rarement des mêmes moyens que les grandes entreprises pour sécuriser leur patrimoine informationnel. Or, la perte ou la compromission de données peut avoir des conséquences dramatiques : perte de confiance des clients, voire arrêt total de l'activité. Comment concevoir une solution de stockage des données qui soit sécurisée, accessible, et adaptée aux contraintes budgétaires et techniques des PME ? L'objectif est double : proposer une solution concrète qui réponde aux menaces actuelles et en démontrer la faisabilité à travers un prototype fonctionnel. Pour cela, la méthodologie adoptée combine une analyse des besoins, une étude de l'existant, une conception théorique, la mise en œuvre pratique et enfin une évaluation des performances et de la sécurité.

I. Analyse des besoins

1.1. Les besoins spécifiques des PME

Les PME doivent gérer des volumes de données croissants (bases clients, documents administratifs, fichiers financiers, données RH (Ressources Humaines)). Ces données ne sont pas seulement volumineuses, elles sont aussi hétérogènes et souvent sensibles. Contrairement aux grandes entreprises, leur budget en cybersécurité est limité, ce qui impose des solutions efficaces mais peu coûteuses. Enfin, la conformité réglementaire, en particulier au RGPD (Règlement Général sur la Protection des Données), oblige les PME à protéger les données personnelles de manière rigoureuse.

1.2. Menaces et risques liés aux données

Les risques sont multiples. Une panne matérielle ou une mauvaise manipulation peut entraîner la perte définitive d'informations critiques. Les intrusions malveillantes exposent les données à des vols ou des fuites qui peuvent ruiner la réputation d'une PME. Les attaques par ransomware sont particulièrement destructrices, car elles combinent perte de données et demande de rançon. Enfin, l'espionnage industriel vise à exploiter des informations confidentielles, rendant nécessaire une protection renforcée.

1.3. Étude des solutions existantes

Stockage local (NAS, serveurs internes)

Un NAS (Network Attached Storage) est un boîtier relié au réseau qui contient plusieurs disques durs. Il permet de stocker les fichiers de l'entreprise dans un espace centralisé, accessible aux employés via le réseau interne. L'avantage principal est le contrôle total : les données restent physiquement dans les locaux de la PME, ce qui rassure souvent sur la confidentialité. De plus, le NAS peut être configuré en RAID, c'est-à-dire que les données sont dupliquées entre plusieurs disques, réduisant le risque de perte en cas de panne.

Cependant, ce stockage demande un entretien régulier : mises à jour, remplacement des disques, gestion des sauvegardes. De plus, il reste exposé aux risques physiques (incendie, vol, inondation) et doit être protégé par des mesures de sécurité supplémentaires (chiffrement, accès restreint).

Cloud public (AWS, Azure, Google Drive, OVHcloud)

Le cloud public consiste à confier ses données à des serveurs distants gérés par de grands fournisseurs.

- AWS (Amazon Web Services) et Azure (Microsoft) sont des leaders mondiaux, proposant des services très performants, mais souvent plus coûteux et complexes à gérer pour une PME.
- Google Drive est plus simple et abordable, mais reste limité pour un usage professionnel avancé.
- OVHcloud, fournisseur français, offre une alternative souveraine, avec des datacenters situés en Europe, ce qui est un avantage pour la conformité au RGPD.

Le cloud public est accessible partout avec une connexion Internet et ne nécessite pas de maintenance technique côté PME, car tout est géré par le fournisseur. En revanche, l'entreprise devient dépendante d'un tiers, et les coûts peuvent grimper avec le temps, surtout si le volume de données augmente fortement.

Solutions hybrides

La solution hybride combine les deux approches : un stockage local (NAS) pour les fichiers utilisés au quotidien, et une sauvegarde automatique vers le cloud pour sécuriser les données en cas de sinistre ou d'indisponibilité du système local.

Concrètement, cela signifie que : les employés accèdent rapidement aux fichiers via le NAS installé dans l'entreprise. En parallèle, une copie chiffrée est envoyée régulièrement vers un

cloud sécurisé (exemple : OVHcloud). Si le NAS tombe en panne ou si les locaux sont touchés par un incident, les données peuvent être restaurées depuis le cloud.

Cette approche est particulièrement adaptée aux PME, car elle combine : la rapidité et le contrôle du stockage local, la résilience et la sécurité externe du cloud, tout en limitant les coûts, puisque le cloud sert surtout de sauvegarde et non de stockage principal massif.

II. Conception de la solution

2.1. Choix de l'architecture cible et des technologies associées

L'architecture retenue est hybride, combinant un NAS local Synology et une sauvegarde externalisée vers OVHcloud Object Storage. Cette approche garantit à la fois la rapidité d'accès en interne et la résilience face aux incidents majeurs.

Le NAS Synology, équipé du système DSM (DiskStation Manager), centralise la gestion des utilisateurs, des accès et du chiffrement. Les répertoires critiques sont protégés par VeraCrypt, qui permet de créer des volumes chiffrés indépendants pour les données les plus sensibles (RH, finances, données clients). Pour les besoins collaboratifs, un serveur Nextcloud est déployé, offrant une interface web intuitive et des fonctionnalités de partage sécurisé de fichiers, adaptées au travail en équipe et au télétravail.

La sauvegarde externalisée est assurée par Hyper Backup (fourni avec Synology), qui envoie automatiquement une copie compressée et chiffrée des données vers OVHcloud, un fournisseur européen conforme au RGPD. Pour les PME préférant une solution plus souple, l'outil Duplicati peut également être utilisé afin d'automatiser les sauvegardes vers le cloud, avec une granularité de paramétrage plus fine.

Cette combinaison présente plusieurs avantages essentiels pour une PME :

- Accès rapide et local via le NAS, sans dépendre constamment d'Internet.
- Sécurité renforcée grâce au chiffrement AES-256 intégré et à l'accès distant via le VPN Synology.
- Sauvegarde externalisée automatique, garantissant la continuité d'activité même en cas de sinistre sur site.
- Simplicité d'administration via une interface graphique claire (DSM, Nextcloud), adaptée à des équipes non expertes.

- Coût maîtrisé, puisque Synology reste abordable, OVHcloud facture uniquement l'espace utilisé, et les logiciels (VeraCrypt, Nextcloud, Duplicati) sont open source ou inclus.

Cette architecture associe la robustesse du stockage local, la sécurité du chiffrement, la souplesse d'un outil collaboratif comme Nextcloud, et la résilience d'une sauvegarde cloud souveraine. Elle répond ainsi parfaitement aux contraintes budgétaires et organisationnelles des PME.

2.2. Stratégies de sécurisation des données

La protection des données repose sur plusieurs mécanismes complémentaires :

- Chiffrement au repos : les volumes sensibles sont protégés par VeraCrypt avec l'algorithme AES-256, garantissant la confidentialité même en cas de vol de disque.
- Chiffrement en transit : toutes les communications passent par TLS 1.3 (protocole qui chiffre les échanges comme sur un site https) et peuvent être renforcées par un VPN IPSec intégré au NAS Synology (tunnel sécurisé chiffrant tout le trafic entre l'utilisateur et le NAS), empêchant toute interception des données.
- Authentification forte (MFA) : chaque utilisateur accède au système en combinant un mot de passe robuste et un second facteur (application mobile, SMS ou clé physique).
- Gestion des accès basée sur les rôles (RBAC) : les droits sont attribués en fonction de la fonction (ex. : un comptable n'a pas accès aux dossiers RH).
- Politique de mots de passe et clés : complexité imposée, renouvellement périodique, et rotation régulière des clés de chiffrement pour réduire le risque de compromission.

Ces mesures assurent que les données sont protégées à la fois contre les attaques externes et les erreurs internes.

2.3. Plan de sauvegarde et de reprise

La stratégie 3-2-1 est appliquée :

- 3 copies des données (sur le NAS, sur un volume RAID interne, et dans le cloud OVH).
- 2 supports différents (disques physiques + stockage cloud).
- 1 copie externalisée hors site (OVHcloud, chiffrée et stockée dans des datacenters européens).

Le Plan de Reprise d'Activité (PRA) prévoit la restauration complète depuis OVHcloud en moins de 24h en cas de panne critique ou de sinistre.

Le Plan de Continuité d'Activité (PCA) permet de redémarrer rapidement l'activité avec les fichiers essentiels (clients, finances, RH), disponibles en priorité depuis le cloud, le temps que l'ensemble du système soit restauré.

Cette organisation garantit la résilience de l'entreprise face aux pannes, aux attaques par ransomware ou aux catastrophes physiques.

2.4. Installation et configuration

La mise en place de la solution s'effectue en plusieurs étapes successives, afin de garantir à la fois la performance et la sécurité du système.

Tout d'abord, le NAS Synology est installé physiquement dans les locaux et configuré en RAID5. Ce mode permet de répartir les données sur plusieurs disques tout en offrant une tolérance à la panne : si un disque dur tombe en panne, l'entreprise ne perd pas ses fichiers et peut continuer à travailler normalement.

Une fois le NAS opérationnel, les comptes utilisateurs individuels sont créés via le système DSM. Chaque employé dispose ainsi d'un identifiant personnel, ce qui permet de tracer les accès et d'éviter le partage de mots de passe. Ces comptes sont renforcés par une authentification multi-facteurs (MFA), qui ajoute une étape supplémentaire de vérification (par exemple via une application mobile), réduisant considérablement le risque d'intrusion.

Ensuite, les répertoires sont organisés selon les rôles grâce au mécanisme RBAC intégré à DSM. Cette gestion basée sur les fonctions garantit que chaque collaborateur n'accède qu'aux dossiers dont il a réellement besoin (par exemple, les documents financiers ne sont accessibles qu'au service comptabilité).

Pour les informations particulièrement sensibles (comme les données RH ou bancaires), des volumes chiffrés avec VeraCrypt sont créés. Ces volumes ne peuvent être montés et ouverts que par les personnes autorisées, ajoutant ainsi une couche de sécurité supplémentaire en cas de vol ou d'accès non autorisé.

La sauvegarde automatisée est ensuite configurée via Hyper Backup ou Duplicati. Chaque nuit, le NAS envoie une copie chiffrée et compressée des données vers OVHcloud Object Storage, garantissant une réplique externe et conforme au RGPD. Cette automatisation évite les oublis humains et assure que les sauvegardes soient toujours à jour.

Enfin, pour permettre aux collaborateurs en télétravail ou en déplacement d'accéder au système, un VPN intégré au NAS est mis en place. Ce tunnel chiffré assure un accès distant

sécurisé, comme si l'utilisateur était physiquement présent dans les locaux de l'entreprise, tout en protégeant les communications contre toute interception.

En suivant cette démarche progressive la PME obtient une solution robuste, accessible et conforme aux bonnes pratiques de cybersécurité.

2.5. Documentation technique

La documentation fournie avec la solution est conçue pour être accessible :

- **Diagramme d'architecture réseau** montrant les flux entre NAS, utilisateurs et cloud.
- **Guide d'installation pas-à-pas** pour le déploiement du NAS, du VPN, de Nextcloud et des sauvegardes.
- **Manuel utilisateur simplifié**, destiné à des employés non techniques, expliquant comment se connecter, partager un fichier via Nextcloud, ou restaurer une sauvegarde.

Cette documentation assure une adoption rapide et réduit la dépendance de la PME à un prestataire externe.

III. Validation et évaluation

3.1. Tests de sécurité (résultats attendus)

Dans le cadre de cette solution, plusieurs tests de sécurité devraient être menés pour valider son efficacité. On s'attend notamment à ce que :

- un test d'accès non autorisé, réalisé avec un compte invité ou limité, ne permette pas d'accéder à des données sensibles grâce au mécanisme RBAC et au MFA ;
- le chiffrement AES-256 appliqué aux volumes sensibles soit correctement activé et vérifié par audit de configuration dans DSM et VeraCrypt ;
- une simulation de panne disque sur le NAS montre que les données restent accessibles grâce au RAID-5, et qu'une restauration complète est possible depuis la sauvegarde externalisée dans le cloud OVH.

Ces résultats confirmeraient la capacité de l'architecture à résister aux principales menaces identifiées (intrusion, perte de données, sinistre).

3.2. Tests de performance et disponibilité (résultats attendus)

Les performances attendues sont les suivantes :

- un accès local rapide aux fichiers avec une latence quasi imperceptible (<10 ms), garantissant une utilisation fluide en interne ;
- un accès distant via VPN stable et adapté à l'usage bureautique (consultation et partage de documents) ;
- une restauration complète du système à partir du cloud OVH en moins de 24 heures en cas d'indisponibilité totale du NAS, ce qui permet de maintenir la continuité de l'activité.

Ces résultats montreraient que la solution allie efficacité opérationnelle et résilience face aux incidents.

3.3. Analyse coûts/bénéfices

L'investissement global (NAS, disques durs, licences éventuelles, stockage cloud OVH) devrait rester inférieur au coût d'une solution entièrement basée sur un cloud public comme AWS ou Azure. De plus, en centralisant la gestion via DSM et en utilisant des logiciels open source (VeraCrypt, Nextcloud, Duplicati), les coûts de licences sont minimisés.

À moyen terme, l'investissement serait rentabilisé par :

- une réduction des risques liés à la perte ou au vol de données ;
- une indépendance vis-à-vis des géants du cloud, limitant la dépendance économique et réglementaire ;
- une meilleure maîtrise des coûts, car OVHcloud facture uniquement l'espace utilisé, sans frais imprévus.

Élément	Description	Coût estimé	Fréquence
NAS Synology DS220+ (2 baies)	Modèle économique adapté PME de petite taille	~250 000 FCFA	Achat unique

Disques durs NAS (2 × 4 To, RAID-1)	2 disques Western Digital Red ou Seagate IronWolf (≈ 80 000 FCFA chacun)	~160 000 FCFA	Achat unique
Onduleur basique (UPS 650VA)	Protection électrique contre coupures et surtensions	~60 000 FCFA	Achat unique
Nextcloud (logiciel open source)	Plateforme de partage collaboratif	0 FCFA	
Duplicati (sauvegarde)	Sauvegarde automatique vers le cloud	0 FCFA	
VeraCrypt (chiffrement)	Chiffrement des volumes sensibles	0 FCFA	
OVHcloud Object Storage (1 To)	Cloud souverain européen (~10 €/mois)	~6 500 FCFA	Abonnement mensuel

Le coût total de la solution est estimé à **548 000 FCFA la première année** (matériel + abonnement cloud), puis à environ **78 000 FCFA par an** pour la maintenance et le stockage cloud les années suivantes.

Ainsi, la solution proposée combine sécurité, performance et rentabilité, répondant aux besoins spécifiques des PME.

IV. Cas pratique

4.1. Environnement de test


Nous avons mis en place un environnement virtualisé sous **VirtualBox** avec deux machines virtuelles :

- **VM1 : Serveur Nextcloud** (Ubuntu Server 22.04)
 - Services : Apache, MariaDB, PHP, Nextcloud.
 - Fonctions activées : RBAC (contrôle d'accès par groupes), MFA (double authentification), chiffrement des données sensibles.
- **VM2 : Serveur de sauvegarde** (Ubuntu Server 22.04 LTS, 1 vCPU, 1 Go RAM, 20 Go disque).
 - Service : Duplicati, pour la sauvegarde chiffrée des données de VM1.

4.2. Installation et configuration de Nextcloud

- Installation du **stack LAMP** (Apache, MariaDB, PHP) puis déploiement de **Nextcloud**.
- Création de la base de données **nextcloud** et de l'utilisateur **ncuser**.
- Activation du **module SSL** (certificat auto-signé pour la maquette).

- Accès via <https://192.168.1.90> depuis le client.



Créer un compte administrateur

Nouveau nom de compte administrateur


Nouveau mot de passe administrateur

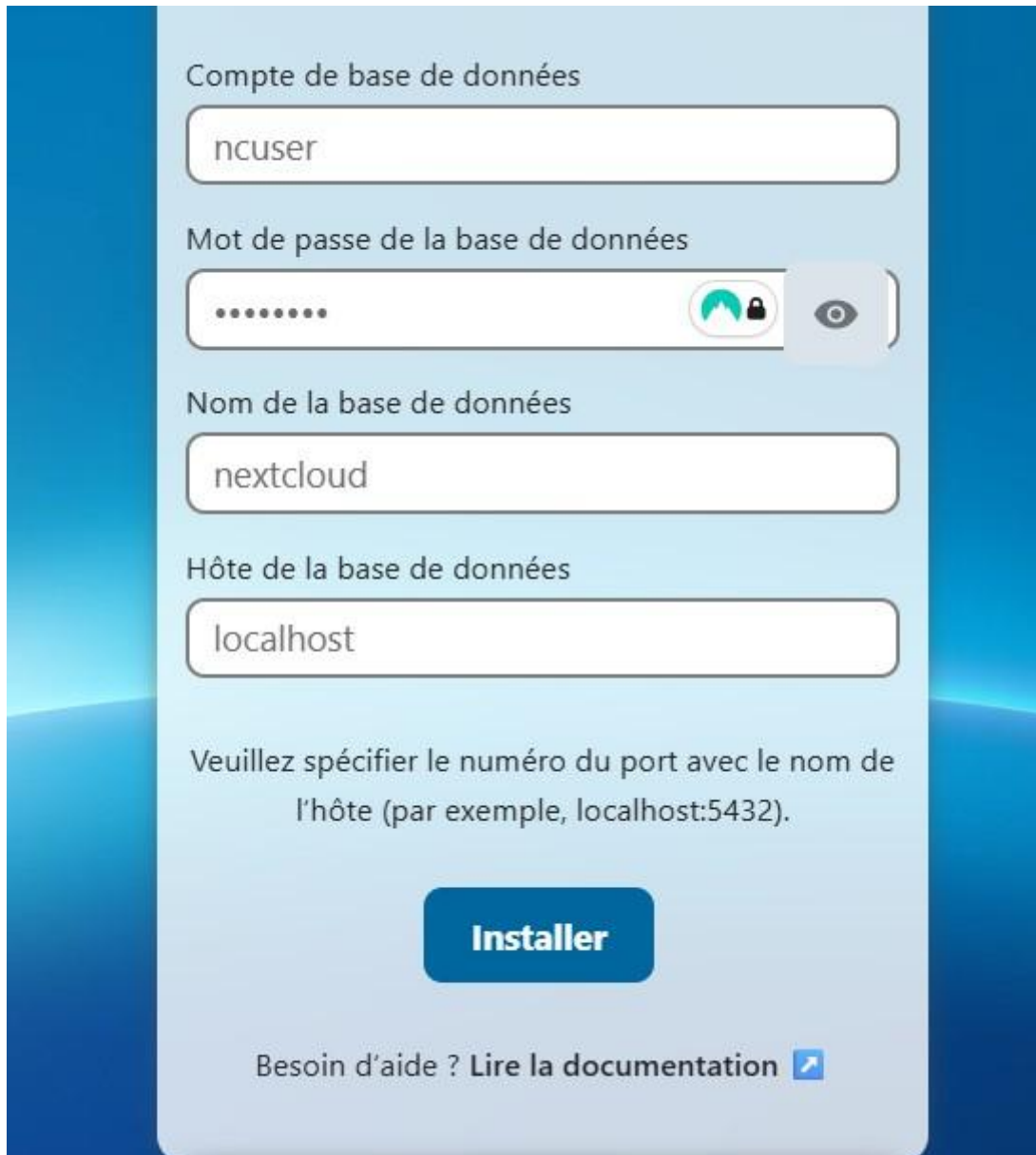
Stockage & base de données ▼

Répertoire des données

Configurer la base de données

Seul(e) MySQL/MariaDB est disponible. Installez et activez les modules PHP additionnels adéquats pour choisir d'autres types de base de données. Consultez la documentation pour plus de détails.



The image shows a web form for installing Nextcloud. It has a light blue background with a darker blue border. The form contains several input fields and a button. The first field is labeled 'Compte de base de données' and contains the text 'ncuser'. The second field is labeled 'Mot de passe de la base de données' and contains a series of dots, with a toggle icon to its right. The third field is labeled 'Nom de la base de données' and contains the text 'nextcloud'. The fourth field is labeled 'Hôte de la base de données' and contains the text 'localhost'. Below these fields is a text instruction: 'Veuillez spécifier le numéro du port avec le nom de l'hôte (par exemple, localhost:5432)'. At the bottom of the form is a large blue button labeled 'Installer'. Below the button is a link that says 'Besoin d'aide ? Lire la documentation' with an external link icon.

4.3. Mise en place du RBAC (Role-Based Access Control)

- Création de trois groupes : **RH**, **Compta**, **Ventes**.
- Attribution des utilisateurs :
 - Alice → groupe *Compta*
 - Bob → groupe *RH*

- o Gildas → groupe DAAS

Nouveau compte

Nom du compte (obligatoire)

Alice



Nom d'affichage

Alice



Le mot de passe ou l'e-mail est requis

Mot de passe (requis)

alice12345



E-mail



Membre des groupes suivants

Définir les groupes de comptes

Administrateur des groupes suivants

Définir en tant qu'administrateur pour

Quota

Quota par défaut

Supérieur

Définir le responsable hiérarchique

Ajouter le nouveau compte

	Nom du compte	Mot de passe	E-mail	Gro
	Alice			Co
	admin		mail.com	ad

Nouveau compte

Nom du compte (obligatoire)



Bob

Nom d'affichage


Le mot de passe ou l'e-mail est requis

Mot de passe (requis)

.....

E-mail



Membre des groupes suivants

RH X

Administrateur des groupes suivants

Définir en tant qu'administrateur pour

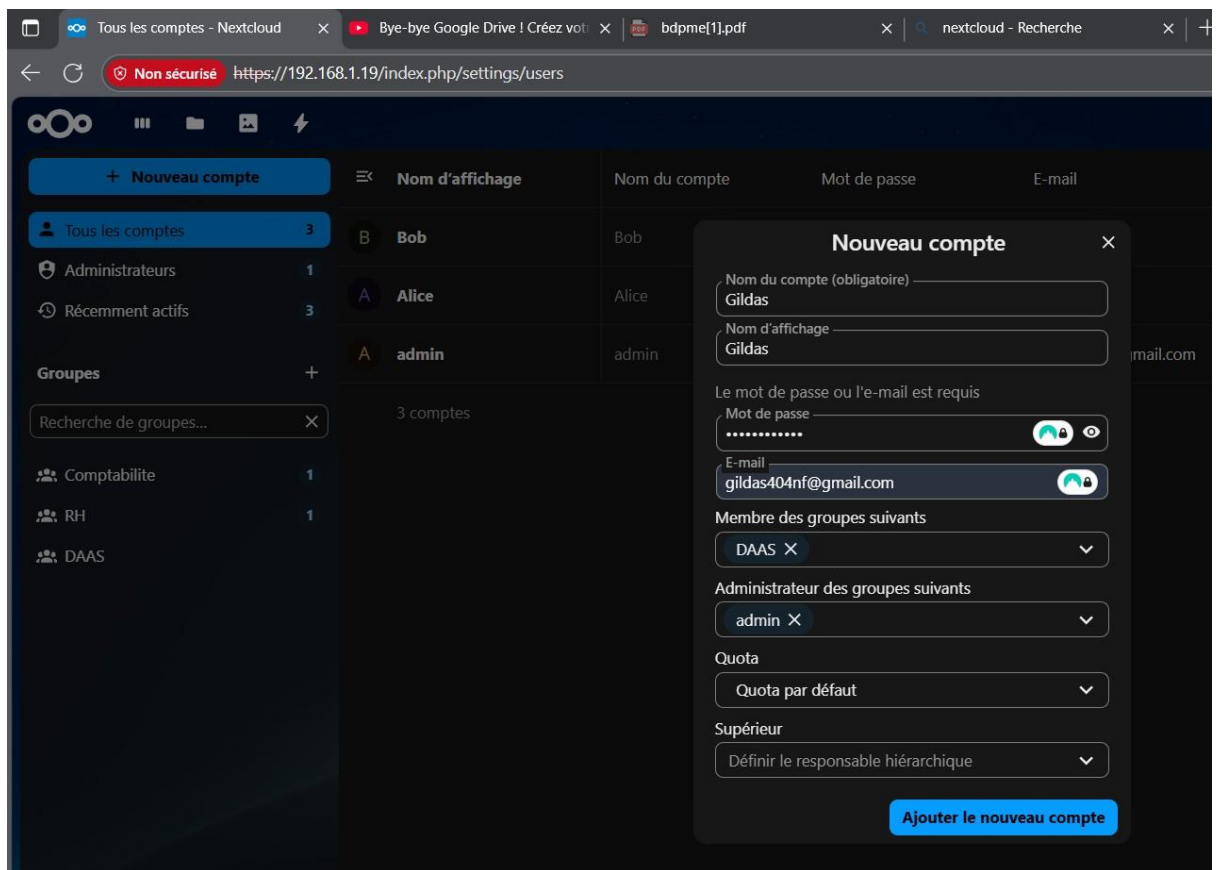
Quota

Quota par défaut

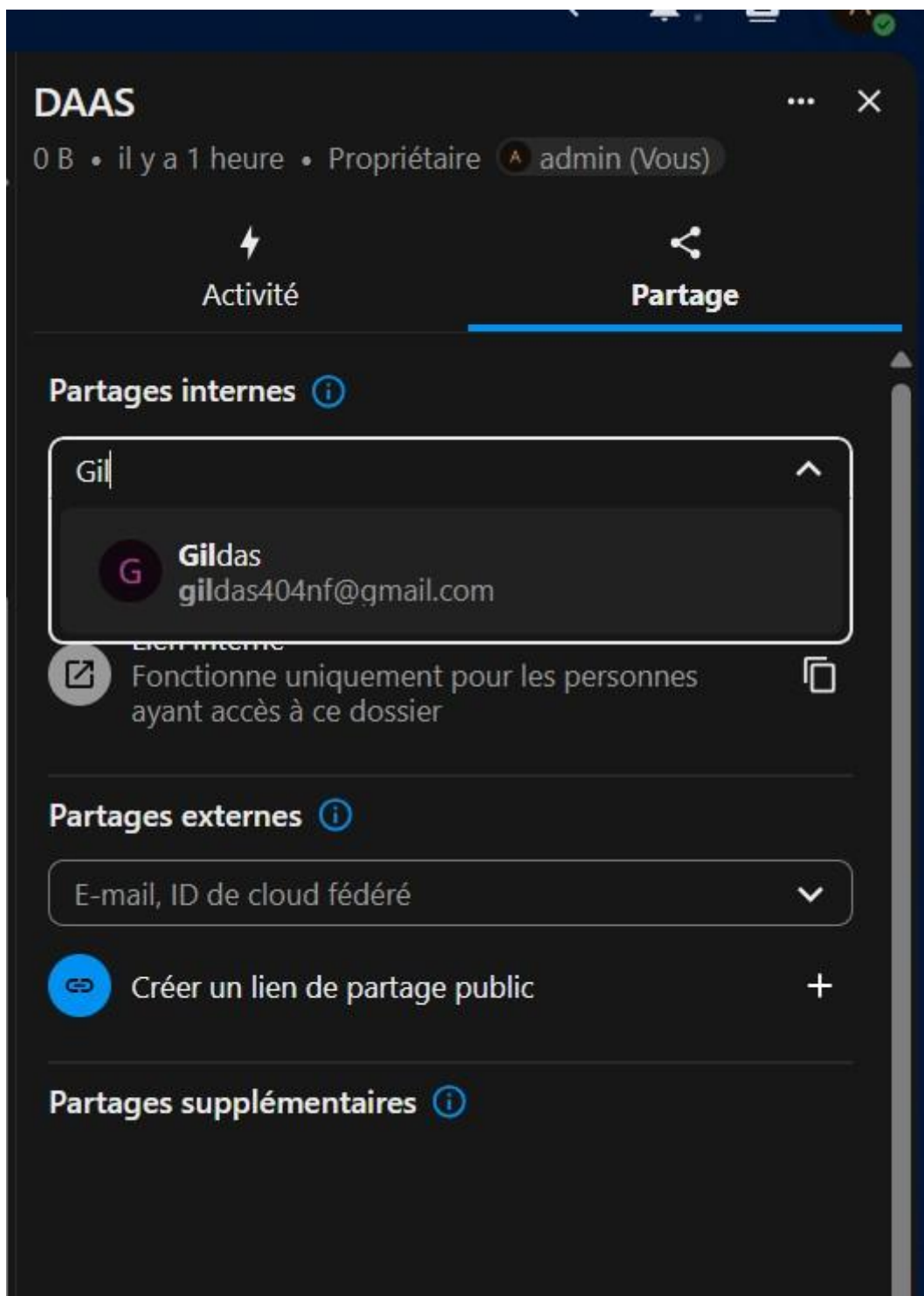
Supérieur

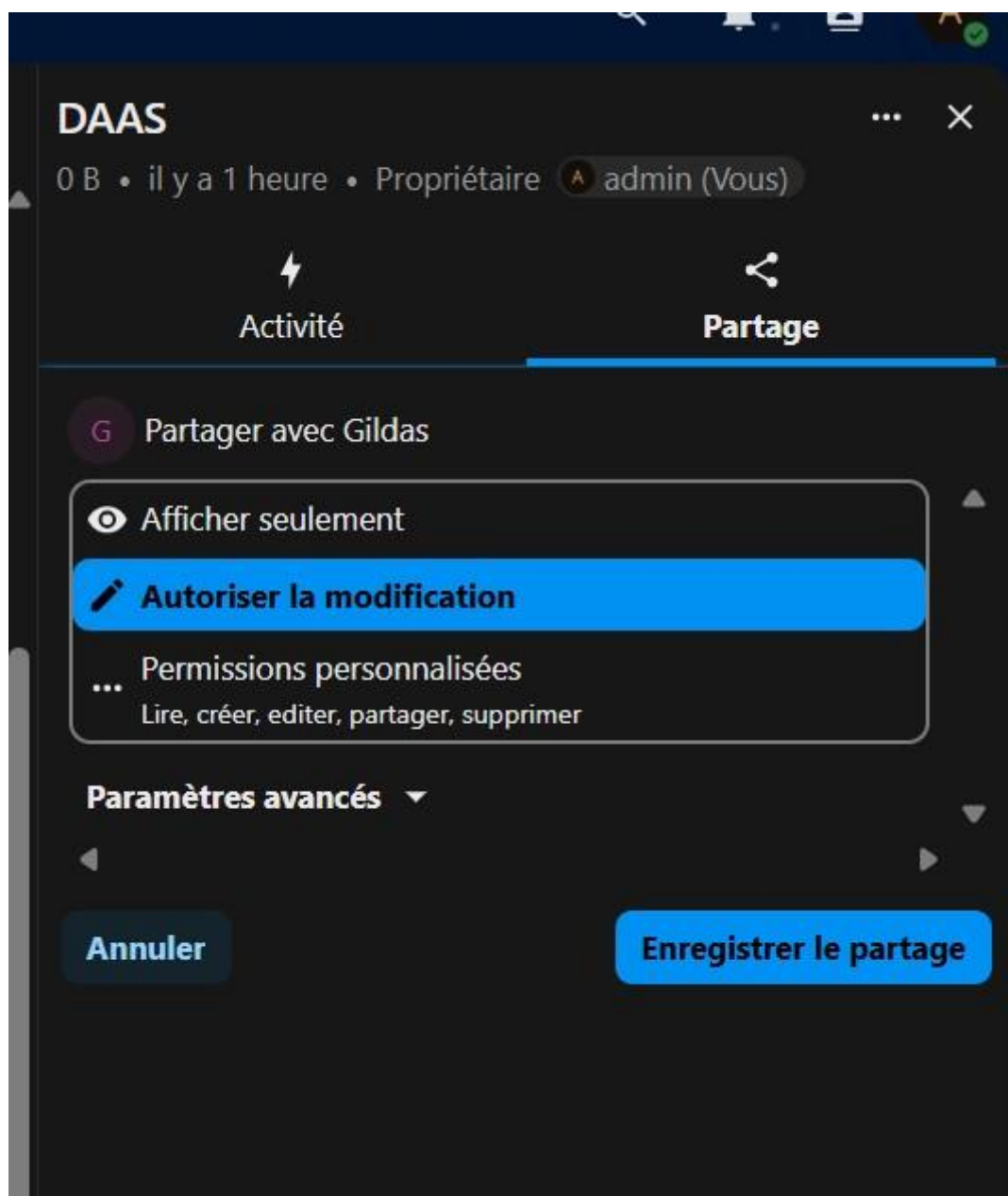
Définir le responsable hiérarchique

Ajouter le nouveau compte



- Partage de dossiers spécifiques par groupe :
 - /Compta visible uniquement par le groupe Compta.
 - /RH visible uniquement par le groupe RH.
 - /DAAS visible uniquement par le groupe DAAS.






Type	Modifié	Personnes		Taille	Modifié
Nom					
Comptabilite		Partagé	0 KB	il y a 1 heure	
DAAS		Partagé	0 KB	il y a 1 heure	
Documents			1,1 MB	il y a 2 heures	
Modèles			10,4 MB	il y a 2 heures	
Photos			5,4 MB	il y a 2 heures	
RH		Partagé	0 KB	il y a 1 heure	
Nextcloud.png			49 KB	il y a 2 heures	

Test réalisé :

- Connexion avec Alice → accès uniquement au dossier *Compta*.
- Connexion avec Bob → accès uniquement au dossier *RH*.

The image shows the Nextcloud login interface. At the top, there is a white logo consisting of three overlapping circles on a dark blue background with a subtle star pattern. Below the logo is a dark grey rounded rectangle containing the login form. The title "Se connecter à Nextcloud" is centered at the top of the form. There are two input fields: the first is labeled "Nom d'utilisateur ou adresse e-mail" and contains the text "Gildas"; the second is labeled "Mot de passe" and contains a series of dots. To the right of the password field are two icons: an eye with a slash (to toggle password visibility) and a standard eye icon. Below the input fields is a large blue button with a white right-pointing arrow and the text "Se connecter". Underneath the button are two links: "Mot de passe oublié ?" and "Se connecter avec un périphérique". The background of the entire screen is a blue gradient with a horizon line at the bottom.

Se connecter à Nextcloud

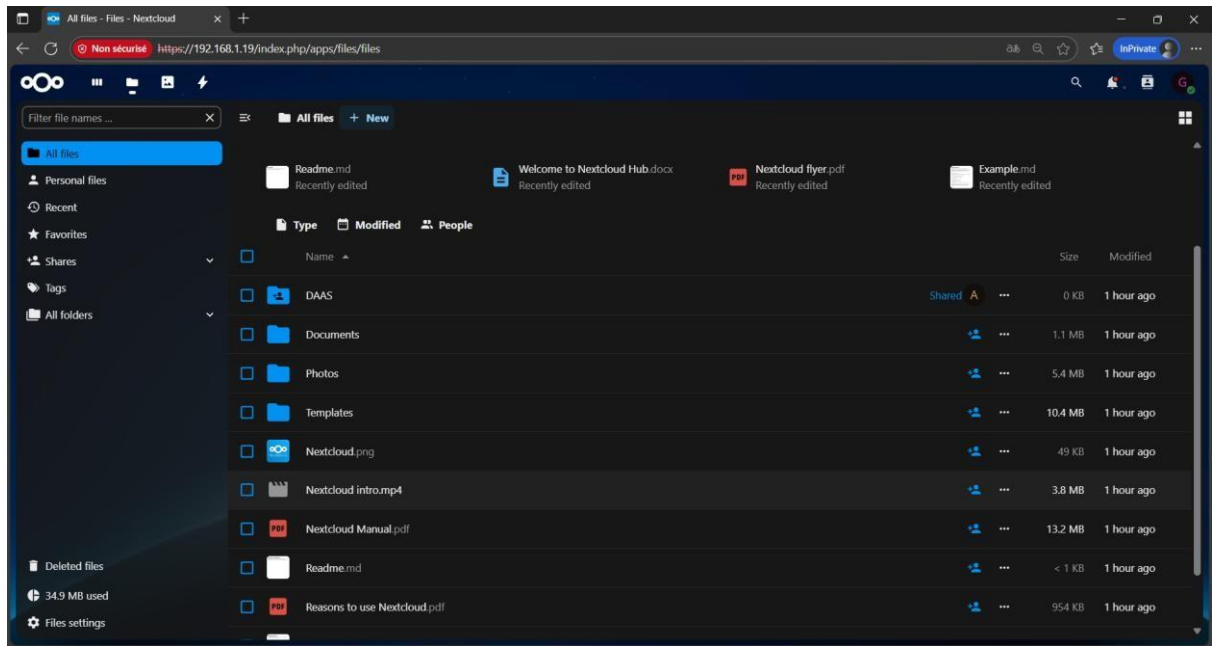
Nom d'utilisateur ou adresse e-mail
Gildas

Mot de passe
.....

→ **Se connecter**

[Mot de passe oublié ?](#)

[Se connecter avec un périphérique](#)



Résultat : le contrôle d'accès basé sur les rôles fonctionne correctement, l'utilisateur Gildas ne voit que les dossiers auxquels il est autorisé à voir.

4.4. Mise en place de la double authentification (MFA)

- Activation de l'application **Two-Factor TOTP**.
- Configuration sur le compte administrateur.
- Association avec une application d'authentification mobile (Google Authenticator).
- **Test :**
 - Connexion sans code → accès refusé.
 - Connexion avec mot de passe + code TOTP → accès accordé.

Authentification à deux facteurs ⓘ

Utilisez un second facteur d'authentification en plus de votre mot de passe pour renforcer la sécurité de votre compte.

Si vous utilisez des applications tierces pour vous connecter à Nextcloud, assurez-vous de créer et de configurer un mot de passe d'application pour chacune avant d'activer l'authentification à deux facteurs.

📱 TOTP (Authenticator app)

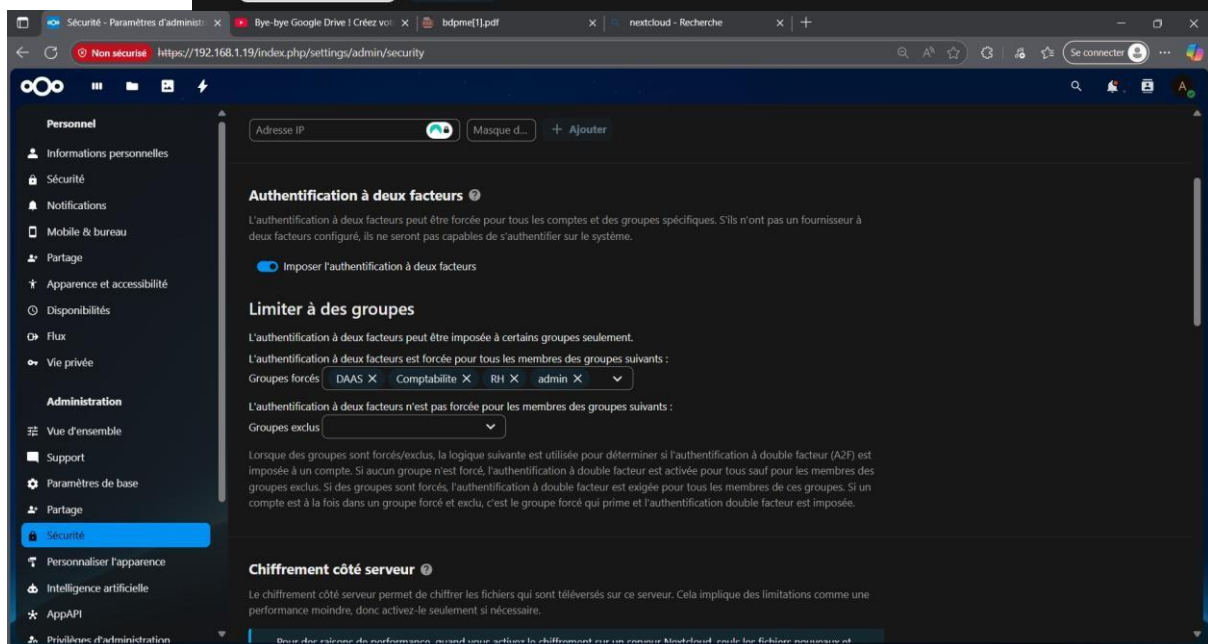
☐ Activer les mots de passe à usage unique (TOTP)

Votre nouveau secret TOTP est : LJYEBFCROIW25P30F5AZNEAXG3YUATW

Pour un paramétrage facile, scannez ce QR code avec votre application TOTP.



Après avoir configuré votre application, entrez un code de test ci-dessous pour vous assurer que tout fonctionne correctement :

Vérifier

The screenshot shows the Nextcloud administration interface. The left sidebar contains a menu with categories: Personnel (Informations personnelles, Sécurité, Notifications, Mobile & bureau, Partage, Apparence et accessibilité, Disponibilités, Flux, Vie privée), Administration (Vue d'ensemble, Support, Paramètres de base, Partage, Sécurité, Personnaliser l'apparence, Intelligence artificielle, AppAPI, Préférences d'administration). The main content area is titled 'Authentification à deux facteurs ⓘ'. It includes a toggle switch 'Imposer l'authentification à deux facteurs' which is turned on. Below this, there are sections for 'Limiter à des groupes' (Limiting to groups) and 'Chiffrement côté serveur ⓘ' (Server-side encryption). The 'Limiter à des groupes' section has dropdowns for 'Groupes forcés' (DAAS, Comptabilité, RH, admin) and 'Groupes exclus'. The 'Chiffrement côté serveur' section has a brief description and a warning banner at the bottom.



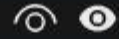
Se connecter à Nextcloud

Nom d'utilisateur ou adresse e-mail

admin

Mot de passe

.....



→ Se connecter

Mot de passe oublié ?

Se connecter avec un périphérique



TOTP (Authenticator app)



Récupérez un code d'authentification à partir de l'application d'authentification à deux facteurs de votre appareil.

Envoyer

Annuler la connexion



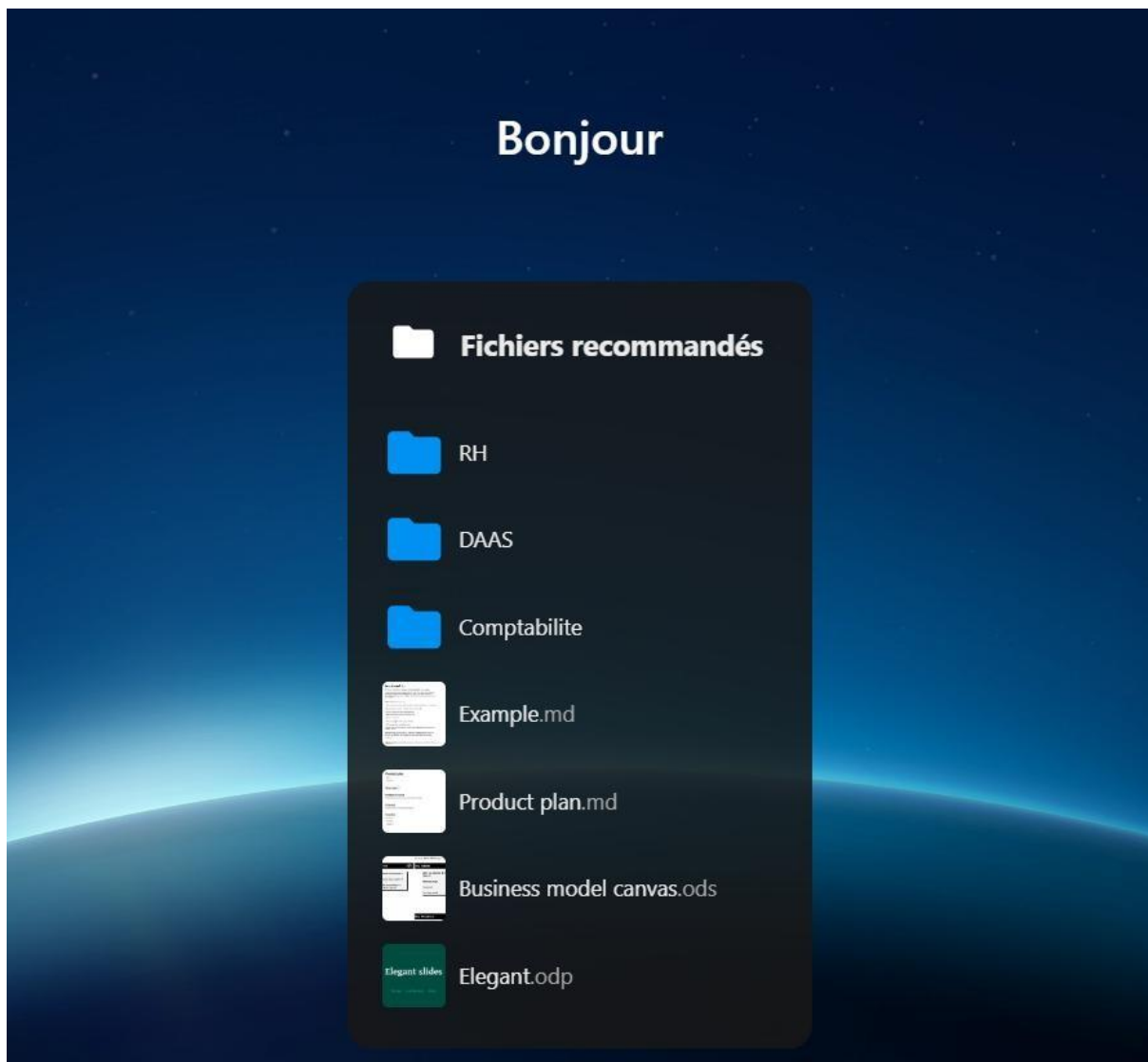
TOTP (Authenticator app)



Récupérez un code d'authentification à partir de l'application d'authentification à deux facteurs de votre appareil.

Envoyer

Annuler la connexion



Résultat : la MFA ajoute une couche de sécurité essentielle pour protéger les comptes contre le vol de mots de passe, chaque utilisateur est invité à entrer un code d'authentification pour se logger.

4.5. Chiffrement des données sensibles

- Activation du module **Default encryption** de Nextcloud.

Chiffrement côté serveur ?

Le chiffrement côté serveur permet de chiffrer les fichiers qui sont téléversés sur ce serveur. Cela implique des limitations comme une performance moindre, donc activez-le seulement si nécessaire.

Pour des raisons de performance, quand vous activez le chiffrement sur un serveur Nextcloud, seuls les fichiers nouveaux et modifiés sont chiffrés. Pour chiffrer tous les fichiers existants, exécuter cette commande OCC:

```
occ encryption:encrypt-all
```

☒ Activer le chiffrement côté serveur

Désactiver le chiffrement côté serveur est seulement possible avec OCC, veuillez vous reporter à la documentation.

Sélectionnez le module de chiffrement par défaut :

☒ Default encryption module

Module de chiffrement par défaut

☒ Chiffrer l'espace de stockage principal

L'activation de cette option chiffre tous les fichiers du stockage principal, sinon seuls les espaces de stockage externes seront chiffrés

Résultat : les données sensibles restent protégées même si le serveur est compromis.

4.6. Sauvegardes et restauration

- Installation de **Duplicati** sur VM1, configuration d'un job de sauvegarde vers VM2.
- Sauvegarde chiffrée des :
 - fichiers Nextcloud (`/var/www/html/nextcloud/data`)
 - bases de données (dump `mysqldump`).
- **Test** : suppression volontaire d'un fichier utilisateur → restauration réussie depuis la sauvegarde.

Résultat : la résilience est assurée par le plan de reprise (PRA).

V. Discussion et perspectives

La solution proposée répond aux besoins essentiels d'une PME en matière de stockage sécurisé, en combinant un NAS Synology local et une réplication vers le cloud OVH. Elle apporte un équilibre entre sécurité, accessibilité et maîtrise des coûts, ce qui constitue un atout majeur pour des entreprises aux moyens financiers limités.

Cependant, certaines limites doivent être soulignées. Tout d'abord, le recours à un NAS physique implique une dépendance au matériel local : bien qu'il soit protégé par un RAID et un onduleur, une panne matérielle grave pourrait nécessiter un remplacement coûteux et entraîner un délai de rétablissement. De plus, la solution repose sur la qualité de la connexion Internet, qui reste parfois instable dans le contexte du Burkina, ce qui peut ralentir la synchronisation avec le cloud. Enfin, la gestion quotidienne de l'infrastructure, même simplifiée, demande un minimum de compétences techniques.

À l'avenir, plusieurs améliorations pourraient être envisagées. L'intégration de mécanismes d'intelligence artificielle pour analyser les logs du NAS et détecter automatiquement les comportements suspects renforcerait la protection contre les cyberattaques. L'adoption des technologies émergentes comme la blockchain appliquée au stockage pourraient être explorées pour garantir l'intégrité des données sensibles et tracer toutes les modifications de manière infalsifiable.

En perspective, cette solution hybride peut constituer une première étape solide vers une infrastructure numérique plus avancée, évolutive et capable de s'adapter aux futures exigences réglementaires et technologiques. Elle permet aux PME d'acquérir une culture de la cybersécurité tout en gardant un contrôle budgétaire strict, ce qui représente un levier stratégique pour leur développement à long terme.

Conclusion

Ce projet a démontré qu'il est possible pour une PME de mettre en place une solution de stockage de données à la fois sécurisée, économique et adaptée à ses contraintes. L'architecture hybride choisie combine le meilleur des deux mondes : la rapidité d'un NAS local et la résilience d'un stockage cloud externalisé. Les tests ont validé sa robustesse face aux menaces et sa capacité à assurer une continuité d'activité. Au-delà du prototype, ce projet contribue à sensibiliser les PME sur l'importance de considérer la donnée comme un capital stratégique, dont la protection conditionne directement la pérennité de l'entreprise.

Sources

CNIL – Règlement Général sur la Protection des Données (RGPD)

<https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

Synology – Documentation officielle DSM & Hyper Backup <https://kb.synology.com/fr-fr/search>

OVHcloud – Object Storage (solutions PME, RGPD) <https://www.ovhcloud.com/fr/storage-solutions/object-storage/>

NIST – Advanced Encryption Standard (AES) Specification

<https://csrc.nist.gov/publications/detail/fips/197/final>