Guide d'utilisation du service de location de stockage (NAS virtuel)

MÉSOCENTRE DE LILLE

Cyrille TOULET
hpc@univ-lille.fr

4 avril 2023

Avant-propos

Merci d'avoir choisi notre service de stockage de données scientifiques.

Notre service de stockage de données scientifiques à la location est basé sur la distribution open source OpenMediaVault, hébergée sur notre plate-forme cloud Openstack et son cluster de stockage CEPH.

Cette documentation détaille l'utilisation du service de location de stockage (NAS virtuel) scientifique du Mésocentre Régional, opérée par l'Université de Lille. Elle résume la documentation officielle d'OMV (OpenMediaVault) à laquelle vous pouvez également vous référer.

Si vous remarquez une erreur, un manque d'information ou une explication perfectible, n'hésitez pas à nous faire parvenir vos remarques à l'adresse suivante : hpc@univ-lille.fr.

Cette documentation pouvant fréquemment évoluer, faites un geste pour l'environnement en évitant de l'imprimer.

Enfin, si nos services vous plaisent, sachez que vous pouvez remercier vos administrateurs préférés à tout moment de l'année, par exemple lors du SysAdmin Day.

Table des matières

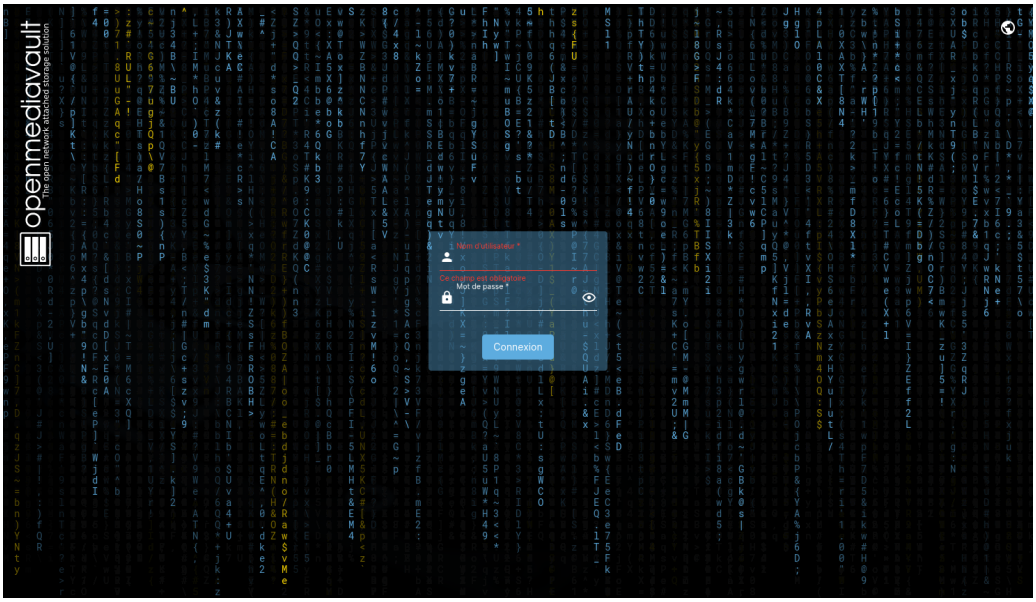
Chapitre 1

Administration

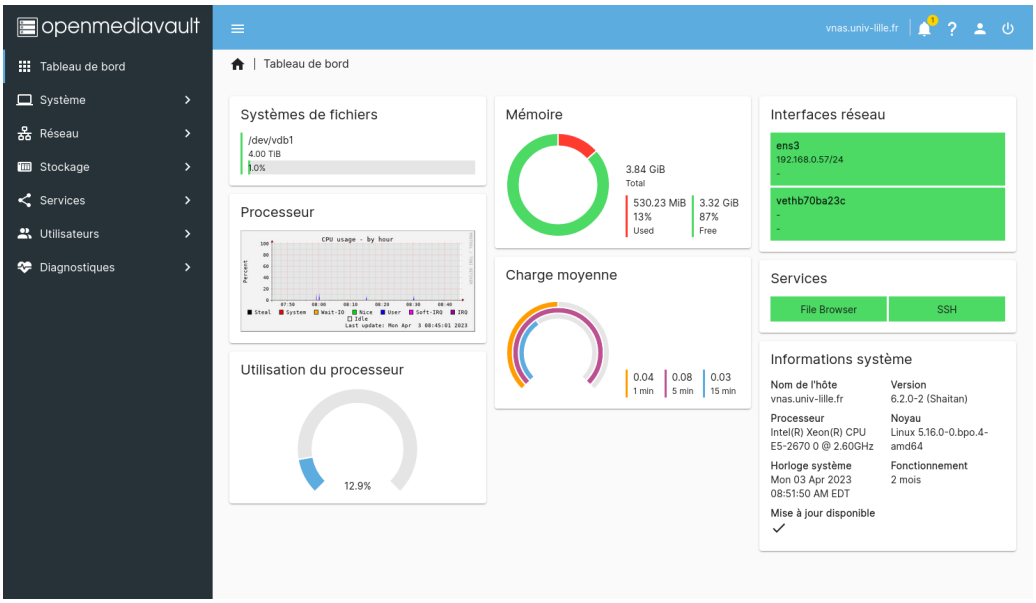
1.1 Connexion

L'interface d'administration du NAS (Network Attached Storage) virtuel est une interface web directement accessible depuis votre navigateur Internet. Elle ne nécessite aucun logiciel spécifique.

Pour vous y connecter, rendez-vous depuis votre navigateur Internet à l'adresse du serveur qui vous a été communiquée par le mésocentre.



Une fois l'authentification réussie, vous vous retrouverez sur la vue d'information du serveur.



1.2 Support utilisateur

Pour toute demande de support concernant ce service (aide, incident, filtrage réseau, etc.), merci de nous contacter uniquement par mail à l'adresse hpc@univ-lille.fr.

Le mot de passe "admin" ne doit en aucun cas être modifié ou divulgué sans l'accord explicite du mésocentre. De la même manière, l'utilisateur "omv" ne doit en aucun cas être modifié ou utilisé. Ces comptes utilisateurs techniques sont l'unique moyen pour le Mésocentre de vous assister en cas de problème.

Enfin, seules les adresses IP des personnels de l'Université et du service VPN associé sont autorisées par défaut. Veuillez nous contacter en cas de blocage réseau.

1.3 Responsabilités

L'administration et la sécurisation du service OpenMediaVault sont à la seule responsabilité du laboratoire qui administre le service.

Chaque utilisateur du service est responsable des données stockées sur cette infrastructure et de l'usage qu'il fait des moyens mis à sa disposition par le Mésocentre.

L'administrateur du service et les utilisateurs finaux prendront soin de sécuriser leurs ressources, par exemple en restreignant les droits d'accès aux fichiers (ACL, droits POSIX), en restreignant l'accès aux services réseaux aux seules adresses IP concernées et en mettant régulièrement le système à jour.

Le Mésocentre ne pourra pas être tenu responsable en cas de perte accidentelle de données due à une fausse manipulation où à un manque de sécurisation du service.

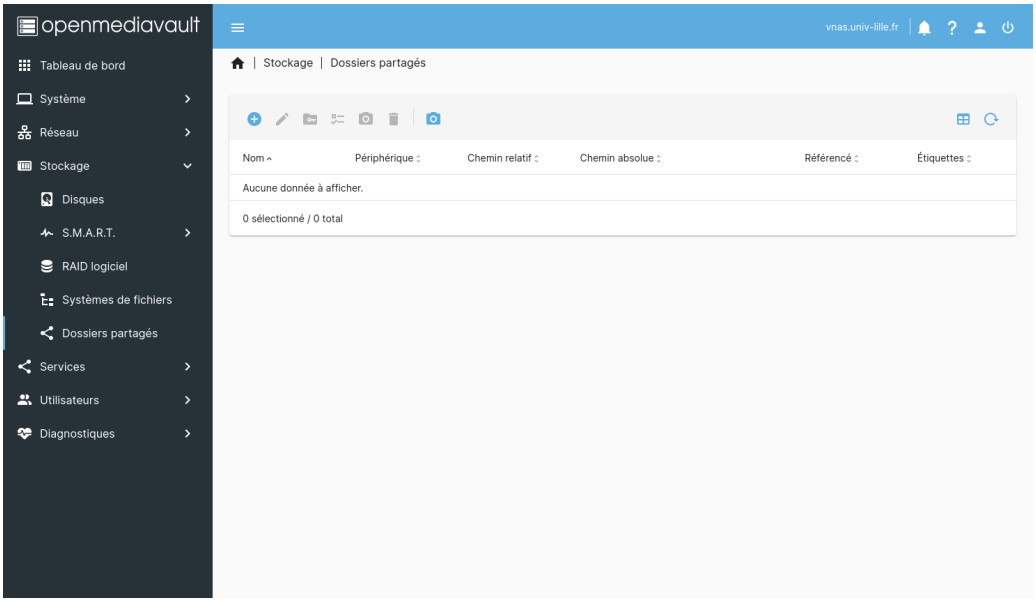
Seuls les services et paramétrages décrits dans la présente documentation sont officiellement supportés par le Mésocentre. L'usage de plugins supplémentaires ou de configurations alternatives et la modification du serveur en ligne de commande sont strictement interdit et rendraient nulles toute demande d'assistance.

Chapitre 2

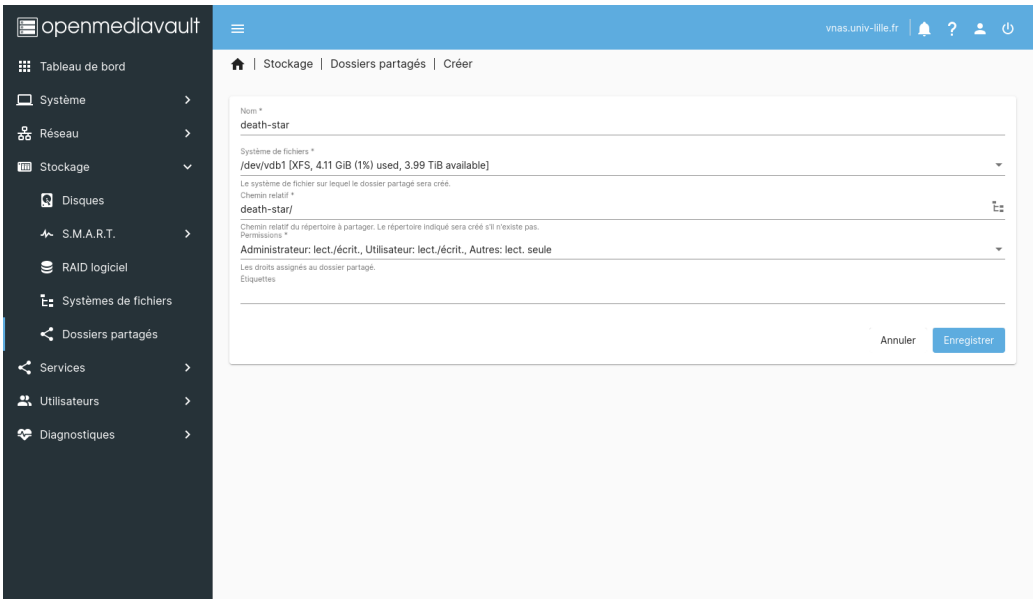
Gestion des ressources

2.1 Création d'un répertoire principal

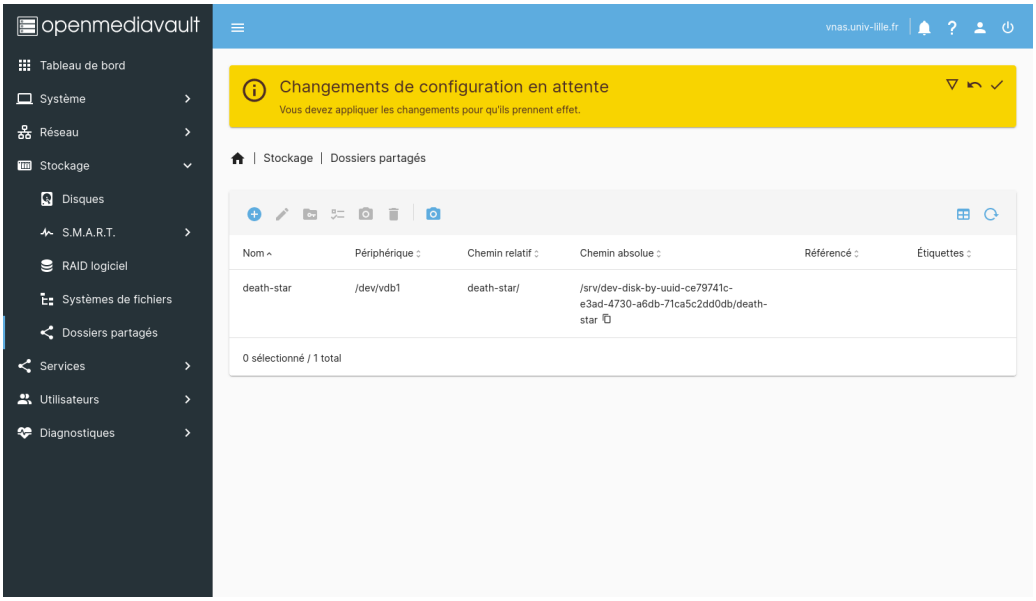
Pour créer un répertoire principal (ou répertoire racine), rendez-vous dans le menu **Stockage / Dossiers partagés**, puis cliquez sur le bouton **+ (Ajouter)** :



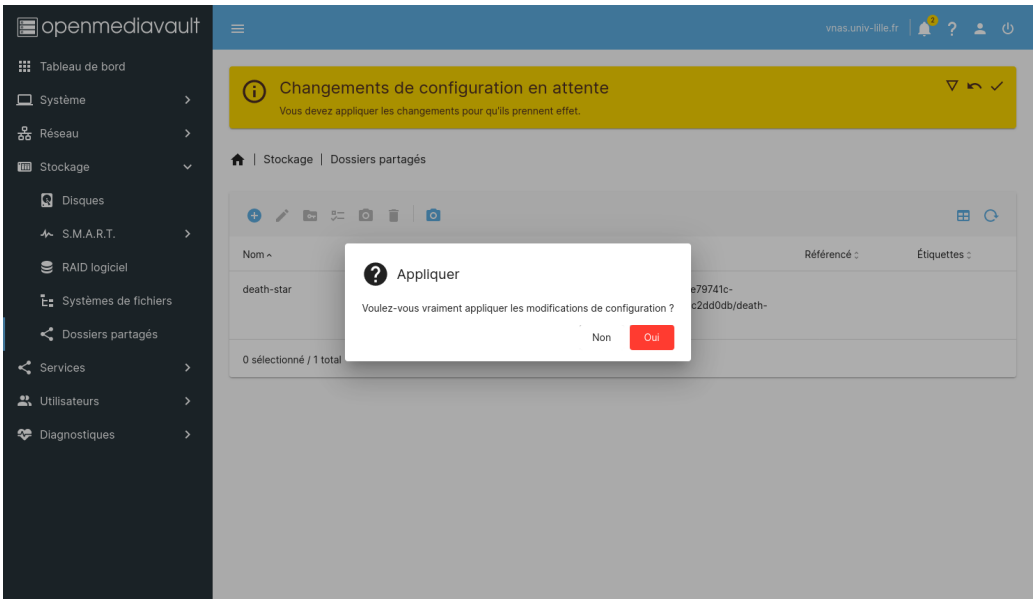
Renseignez à minima le nom du répertoire et le périphérique (disque de destination) dans le formulaire puis cliquez sur **Enregistrer** :



Une barre d'information sur fond jaune apparaîtra en haut de la fenêtre pour vous indiquer que la configuration a changé. Cliquez sur **la coche (Appliquer)** :



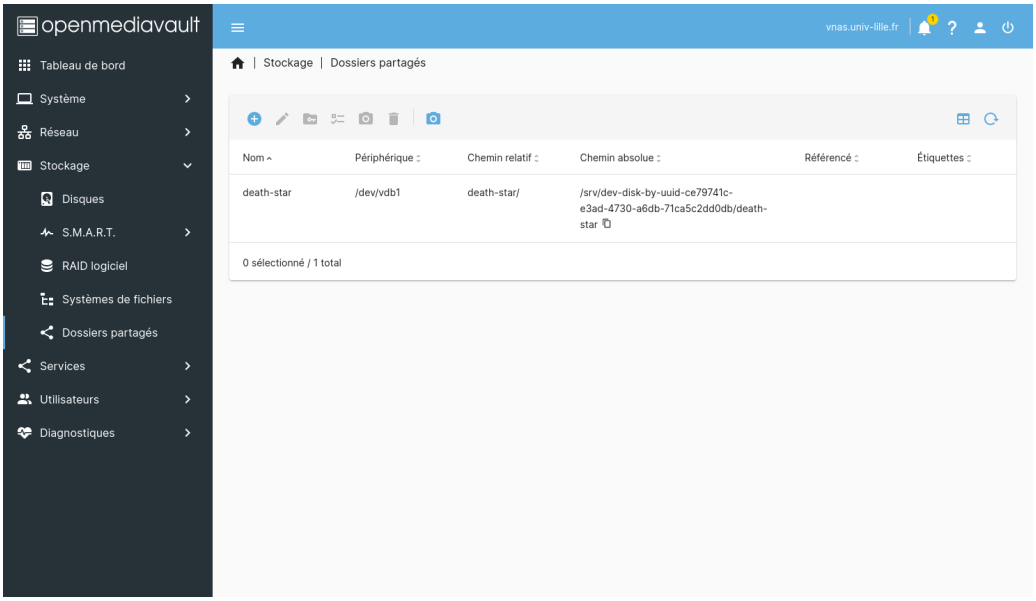
Puis validez les changements en cliquant sur le bouton **Oui** :



Note importante : Cette fenêtre de confirmation apparaîtra à chaque modification de la configuration. Les changements ne seront effectifs qu'une fois appliqués.

Cette étape de validation sera omise dans la suite de la documentation, mais reste valable pour chaque modification de configuration.

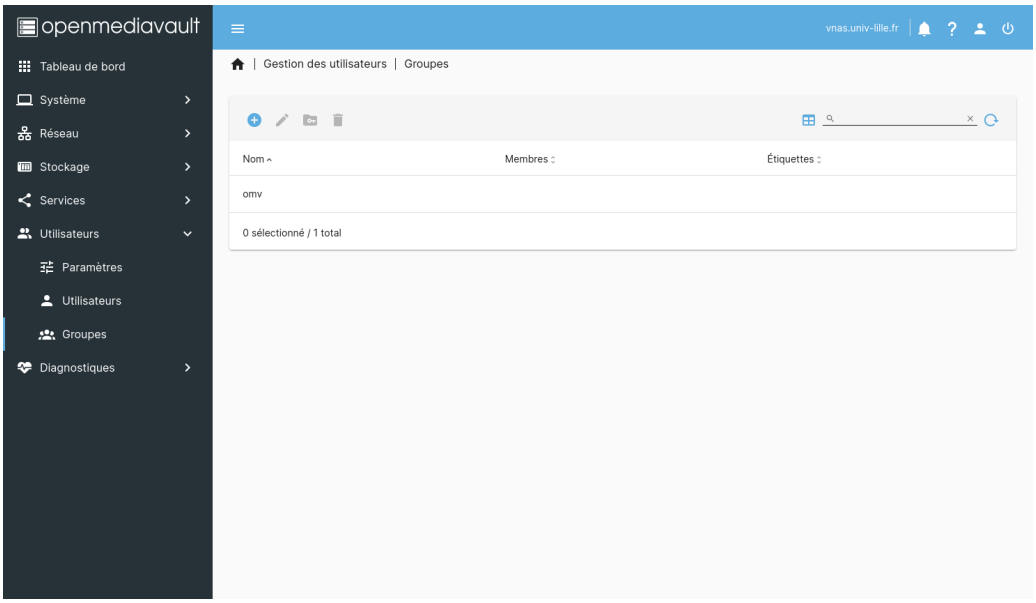
Le nouveau répertoire devrait apparaître dans la liste :



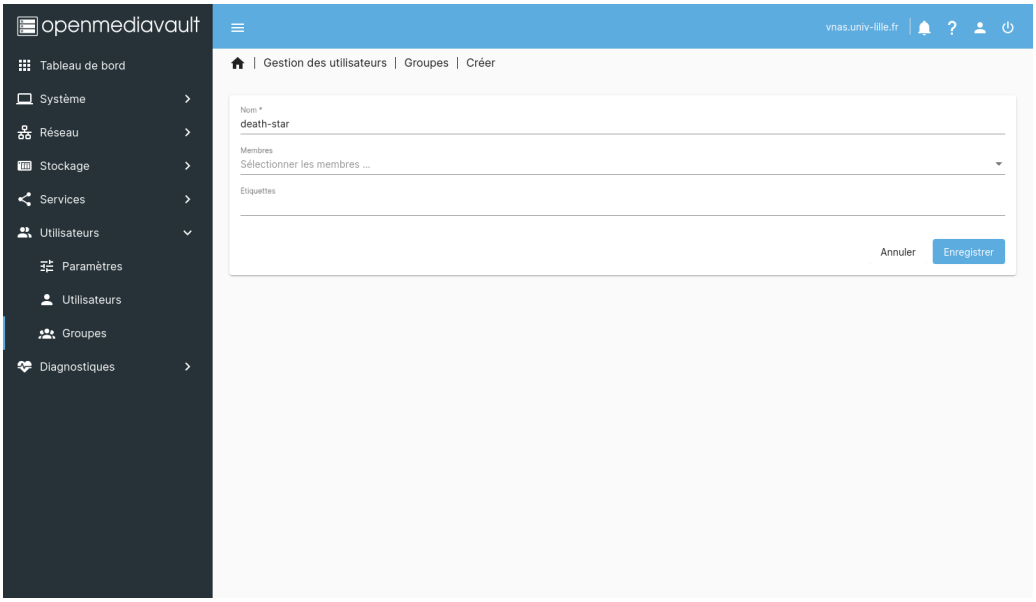
2.2 Création d'un groupe d'utilisateurs

Les groupes utilisateurs ne sont pas obligatoires, mais vous permettront de gérer plus facilement les droits d'accès à certains répertoires (voir chapitre *Séparation des privilèges*).

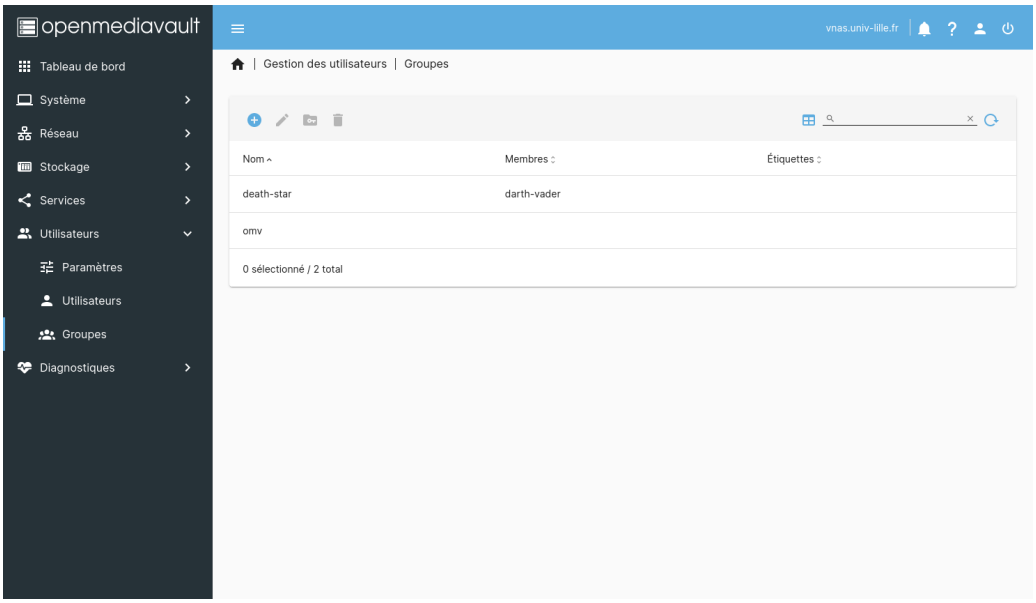
Pour créer un groupe d'utilisateurs, allez dans le menu **Utilisateurs** / **Groupes**, puis cliquez sur le bouton + **(Créer)** :



Remplissez le formulaire puis cliquez sur **Enregistrer** :

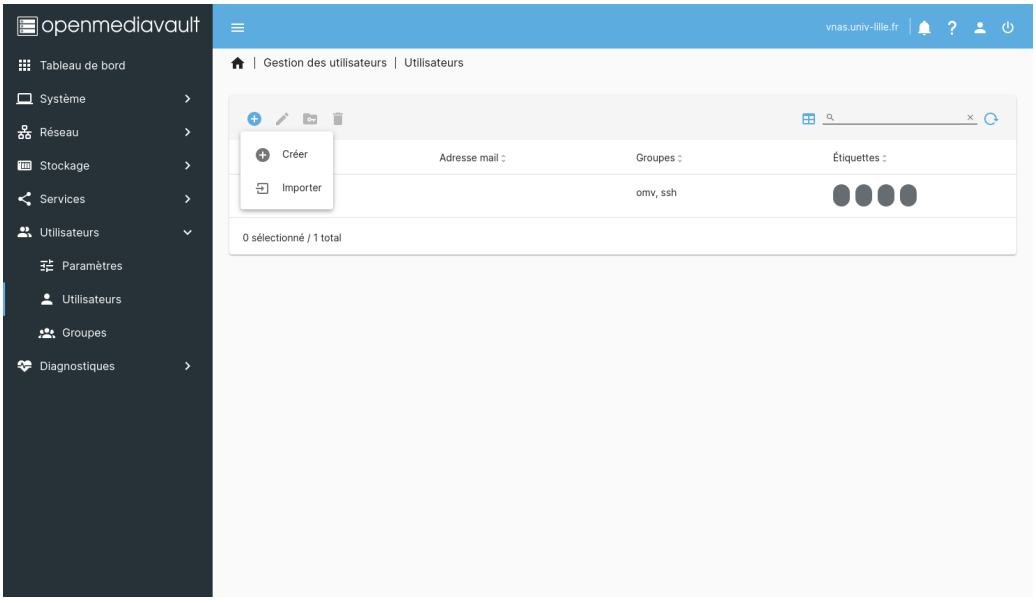


Le nouveau groupe devrait apparaître dans la liste :

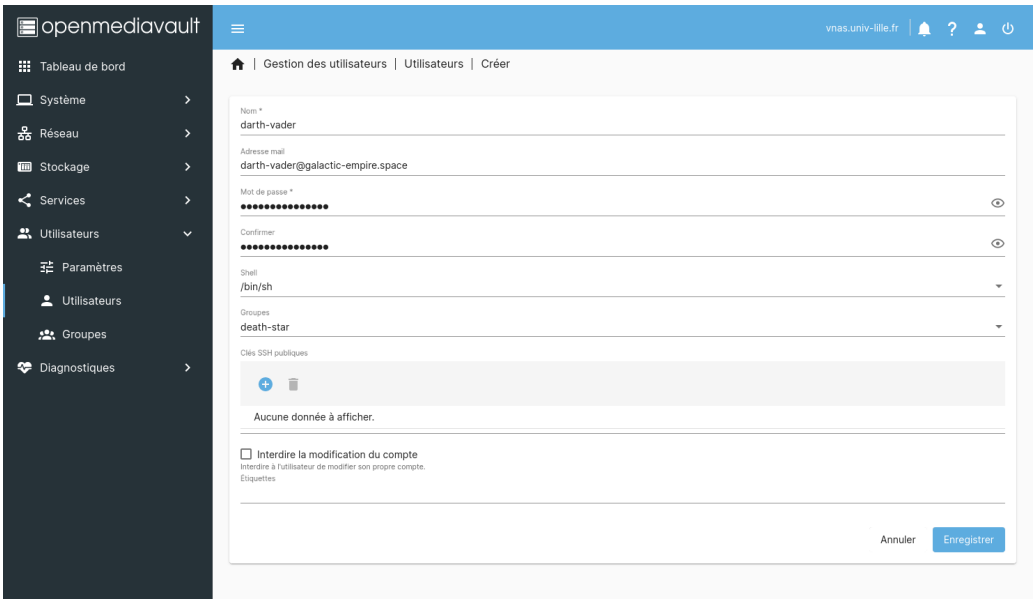


2.3 Création d'un utilisateur

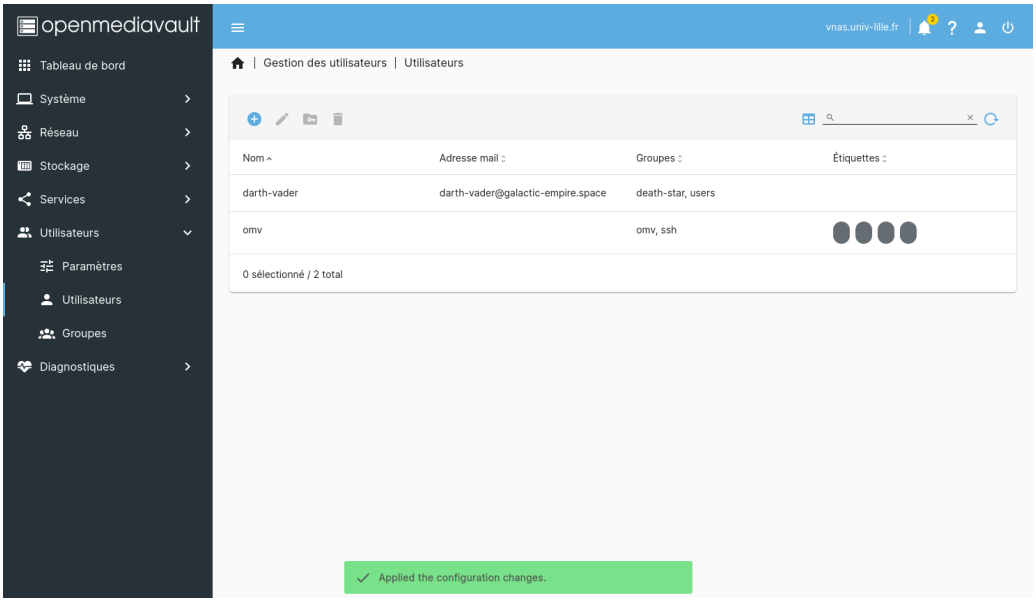
Pour créer un utilisateur, allez dans le menu **Utilisateurs** / **Utilisateurs**, puis cliquez sur le bouton + **(Créer)**.



Remplissez le formulaire et si nécessaire, choisissez les groupes utilisateurs dans lesquels ajouter le futur utilisateur, puis cliquez sur **Enregistrer** :



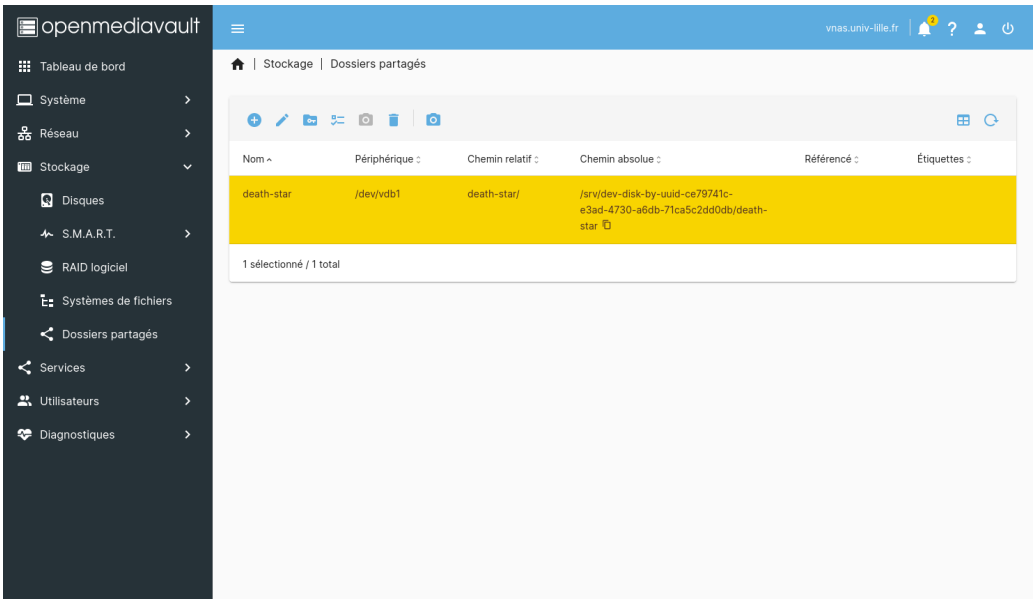
Le nouvel utilisateur devrait apparaître dans la liste :



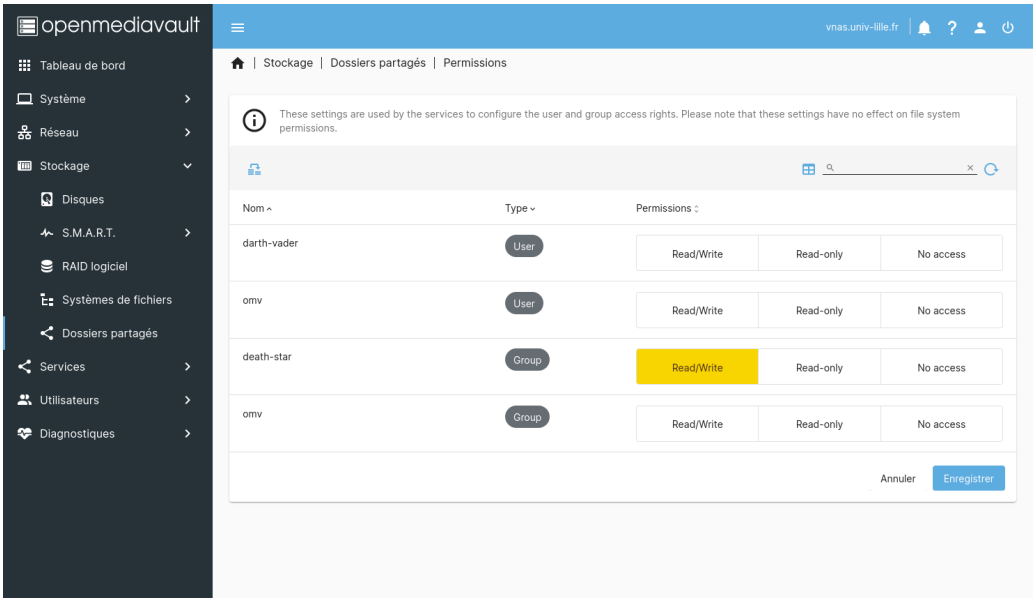
2.4 Gestion des privilèges (ACL)

Par défaut, les utilisateurs n'ont aucun privilège sur les répertoires principaux. Les privilèges permettent de gérer qui a accès aux données ou non, en lecture comme en écriture. On parle alors de gestion de privilèges ou d'ACL (Access Control List).

Pour configurer les privilèges d'un répertoire, rendez-vous dans le menu **Stockage** / **Dossiers partagés**, sélectionnez le répertoire concerné, puis cliquez sur le troisième icone de **dossier (Premissions)** :



Enfin, dans le formulaire, choisissez quels utilisateurs ou groupes d'utilisateurs ont accès à ce répertoire, en cochant les cases correspondantes :



Pour terminer, cliquez sur le bouton **Enregistrer** et validez les changements.

Chapitre 3

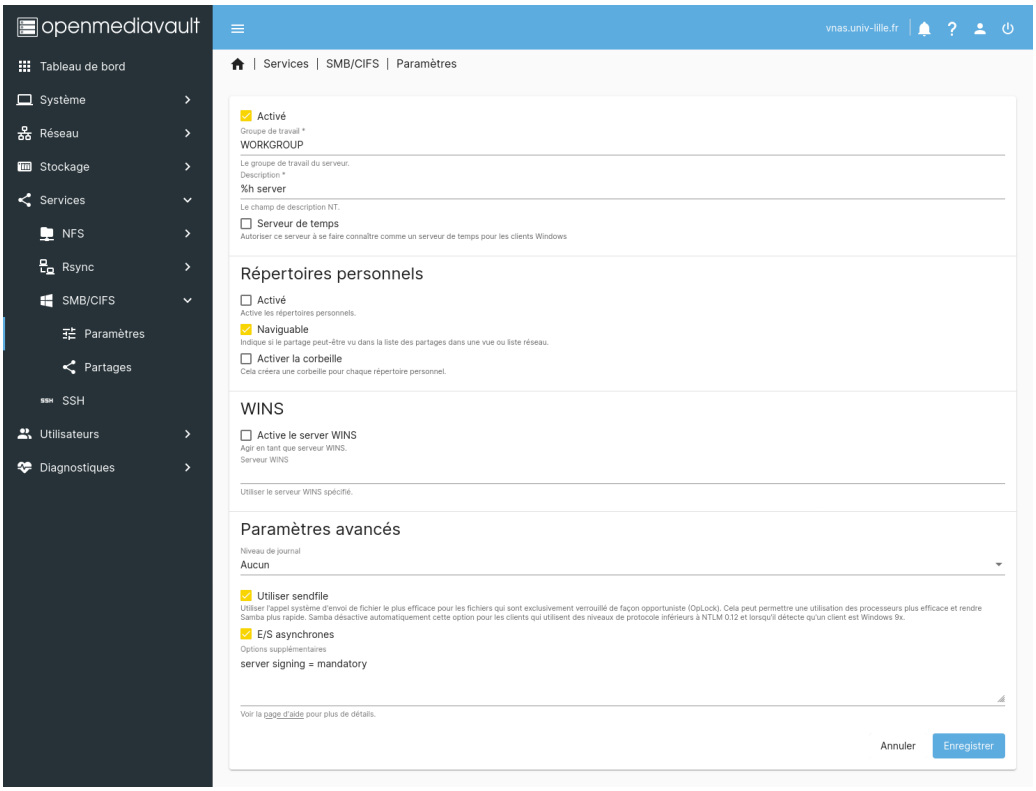
Gestion des services

Maintenant que vous avez créé vos partages et utilisateurs, il reste à les rendre disponibles aux postes clients sur le réseau.

3.1 Partages SMB/CIFS (Windows/Linux/MacOS)

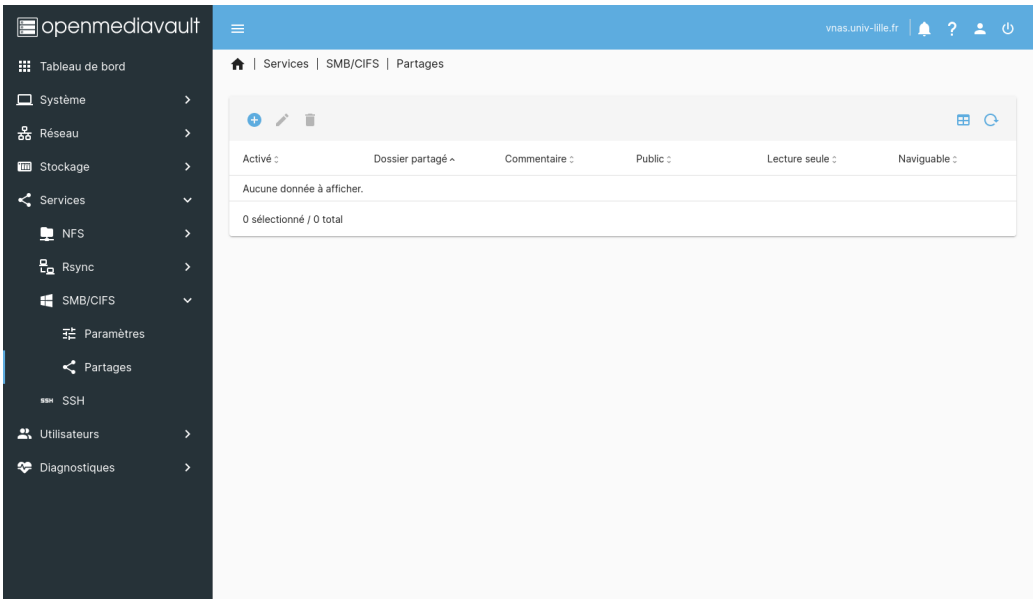
Pour activer le partage SMB/CIFS, rendez-vous dans le menu **Services** / **SMB/CIFS** / **Paramètres**.

Cochez l'option **Activé**, puis plus bas dans la zone **Paramètres avancés**, ajoutez l'option *server signing = mandatory* dans le champ **Options supplémentaires** avant de cliquer sur **Enregistrer** :

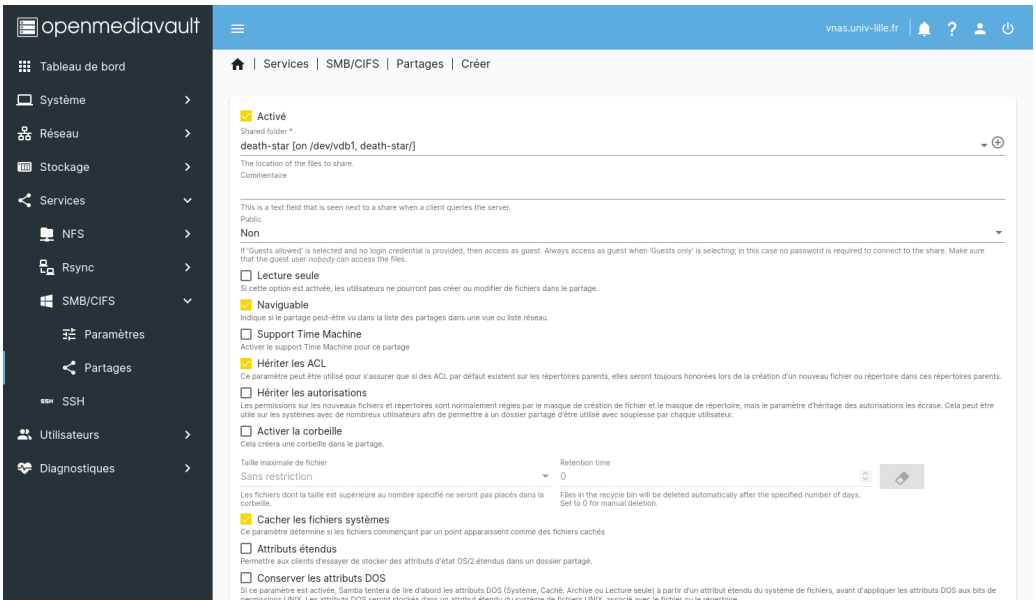


Vous pouvez maintenant partager des répertoires principaux (voir chapitre *Création d'un répertoire principal*) sur le réseau via le protocole SMB/CIFS.

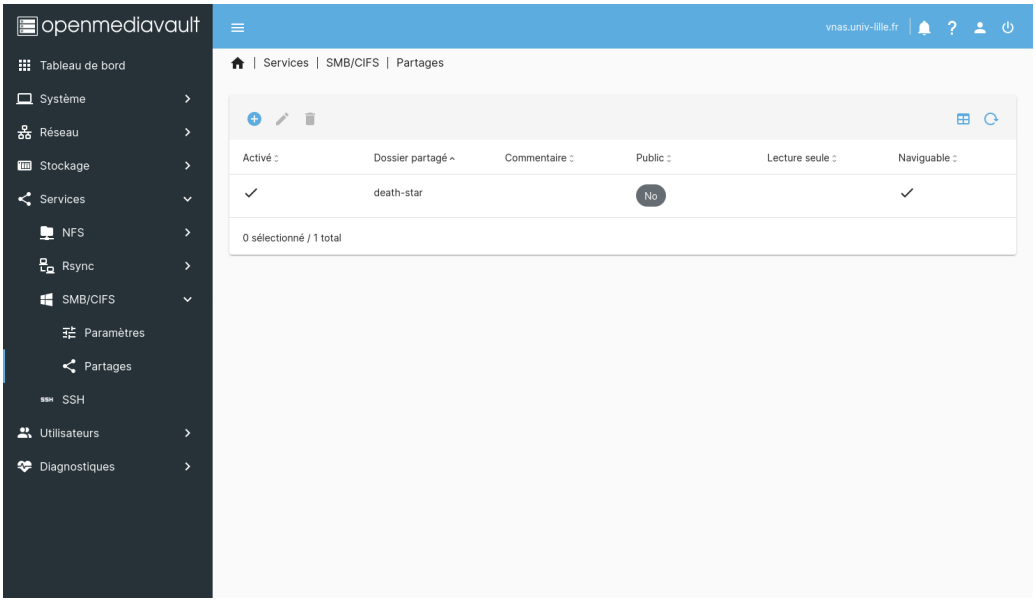
Dans le menu **Services** / **SMB/CIFS** / **Partages**, cliquez sur le bouton **+ (Créer)** :



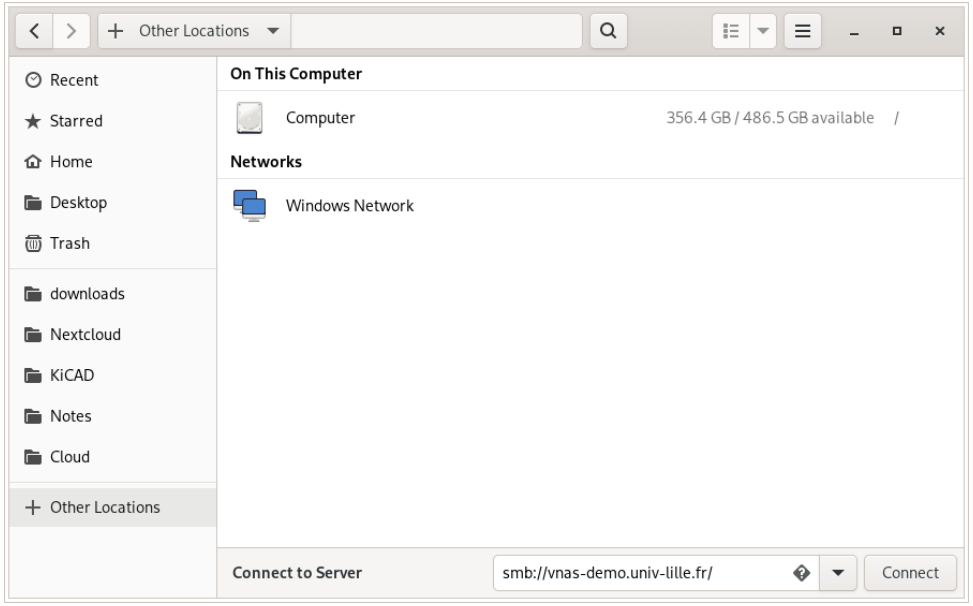
Dans le formulaire, renseignez le nom du répertoire (dossier partagé), cochez en plus des cases par défaut la case **Héritez les ACL** puis cliquez sur **Enregistrer** en bas du formulaire :

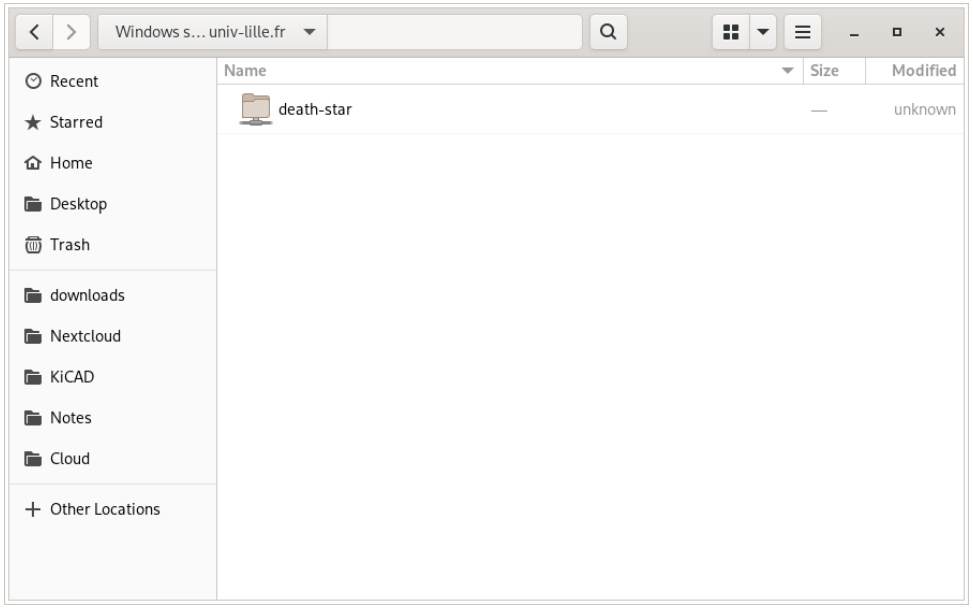


Le nouveau partage devrait apparaître dans la liste :

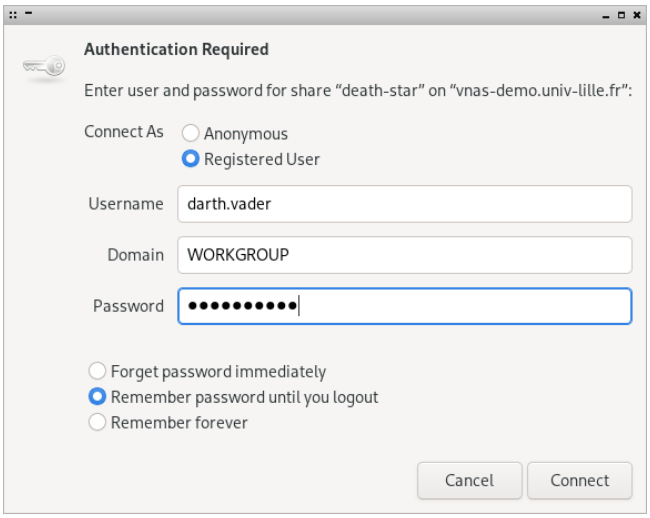


Vous pouvez désormais monter le stockage depuis un client en utilisant l'adresse du serveur qui vous a été communiquée par le mésocentre (dans cet exemple, *vnas-demo.univ-lille.fr*) :

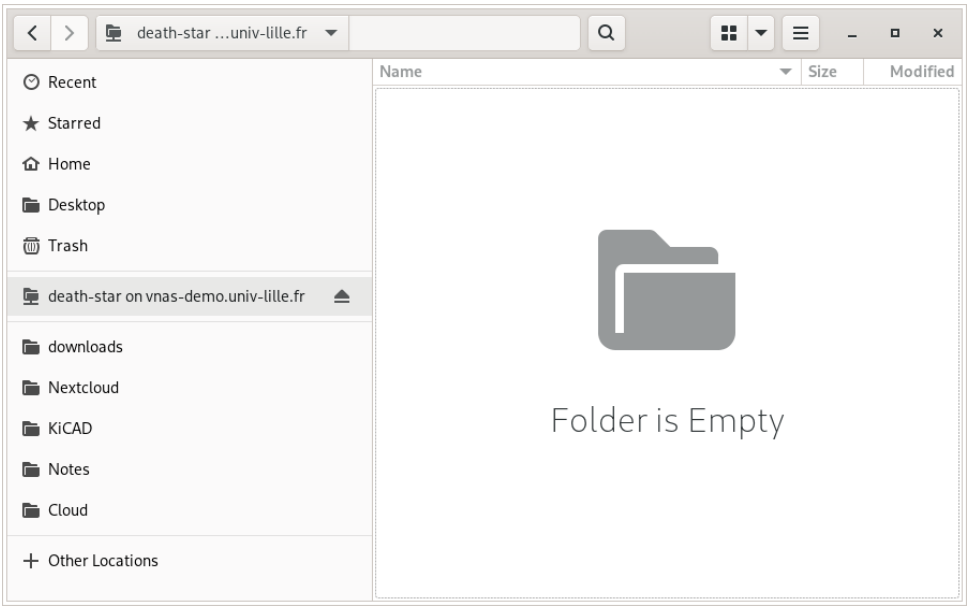




On utilise un utilisateur ayant les droits d'accès au répertoire (voir chapitre *Gestion des privilèges (ACL)*) pour s'authentifier :



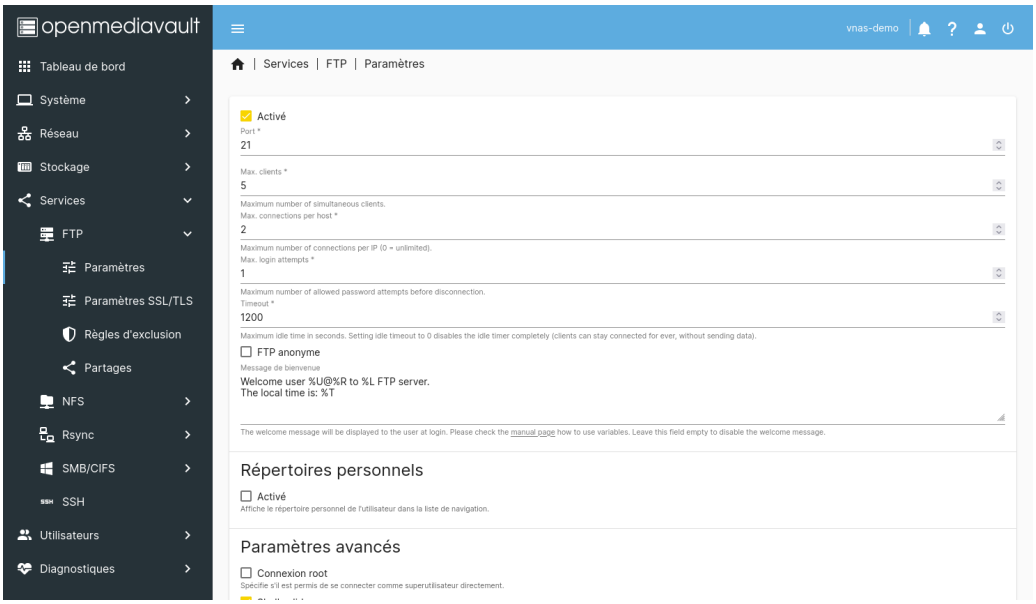
Puis le répertoire principal devrait être monté :



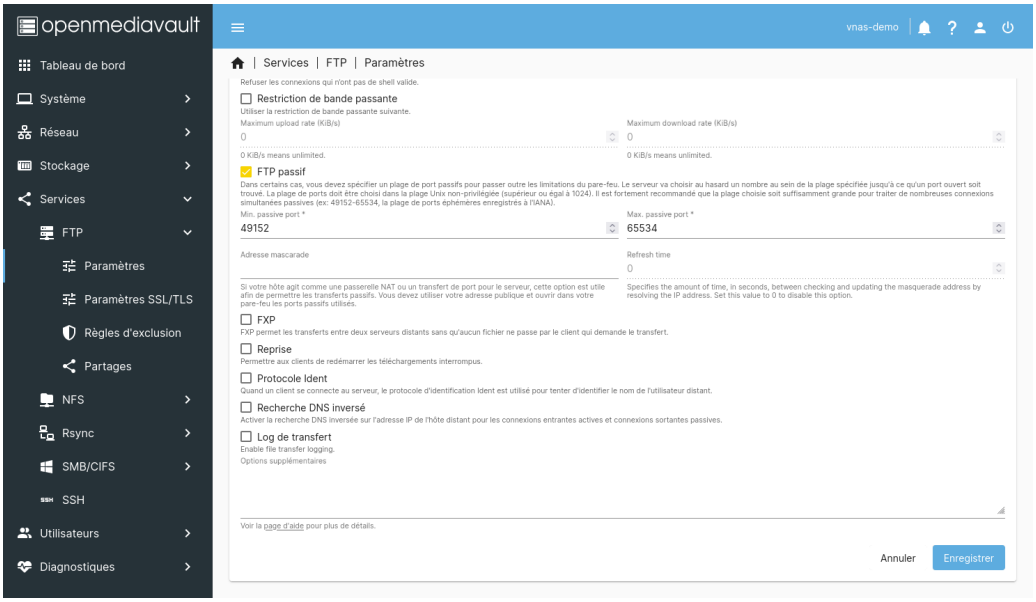
3.2 Partages FTP (Windows/Linux/MacOS)

Pour activer le service FTPs (FTP sécurisé par SSL/TLS à travers SSH), rendez-vous dans le menu **Services** / **FTP** / **Paramètres**.

Cochez l’option **Activé** en haut du formulaire :

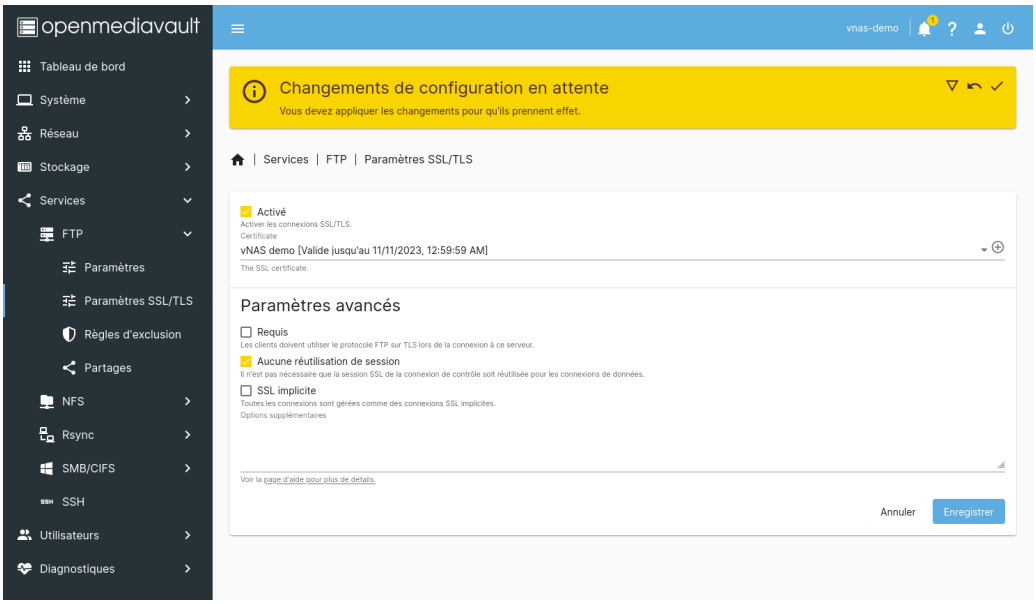


Plus bas, dans l'encart **Paramètres avancés**, cochez l'option **FTP passif** :



Cliquez sur **Enregistrer**.

Dans le menu **Services** / **FTP** / **Paramètres SSL/TLS**, cochez l'option **Activé** et choisissez le certificat dans l'encart **Paramètres généraux**, puis cochez l'option **Aucune réutilisation de session** de l'encart **Paramètres avancés** :

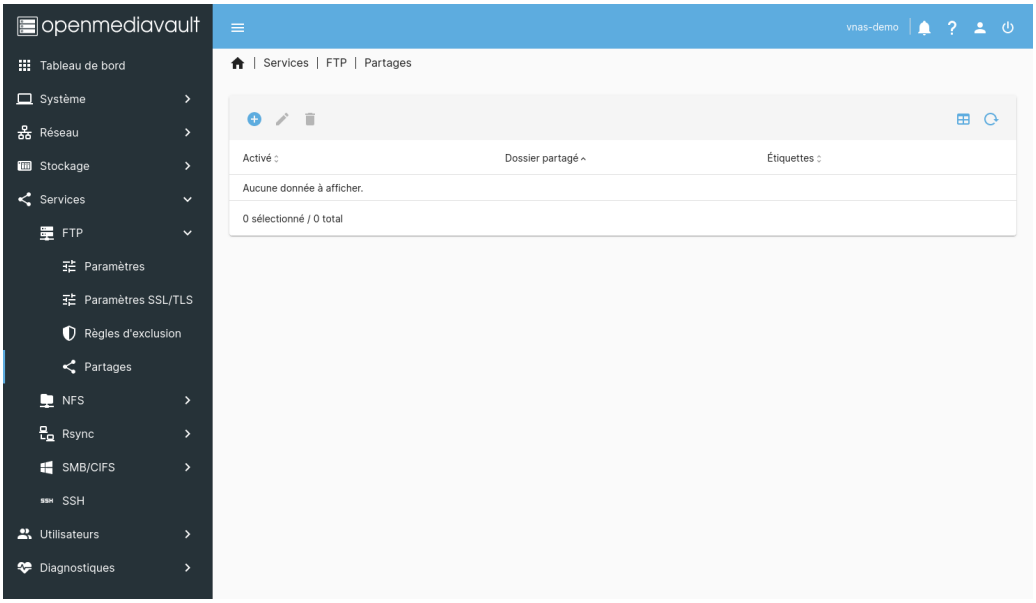


Important : Le protocole FTP étant de base très peu sécurisé, ces options doivent obligatoirement rester activées pour des raisons de sécurité !

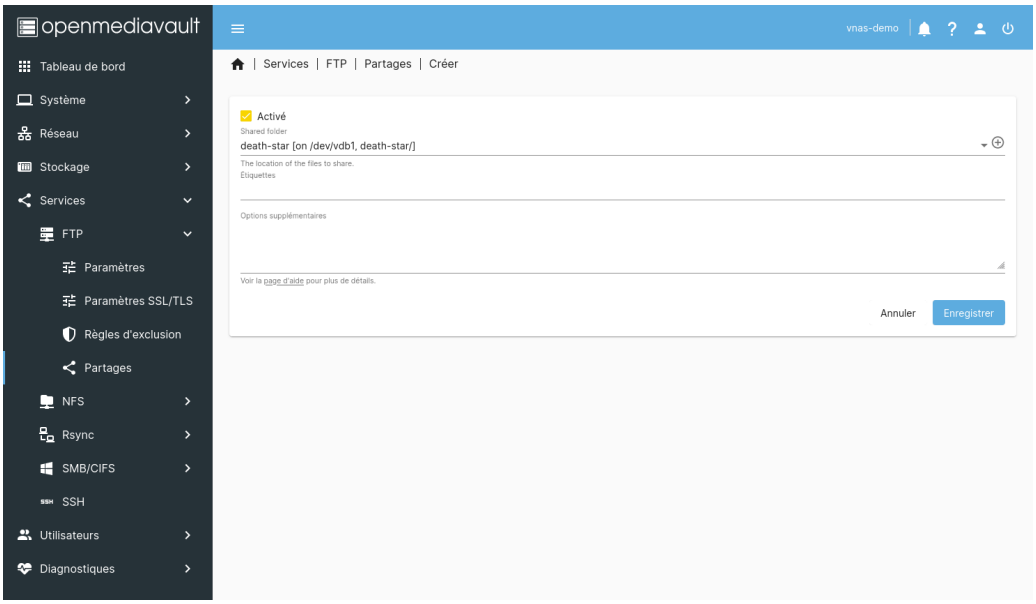
Cliquez sur **Enregistrer** et validez les changements.

Nous pouvons maintenant partager des répertoires principaux (voir chapitre *Création d'un répertoire principal*) sur le réseau via le protocole FTP.

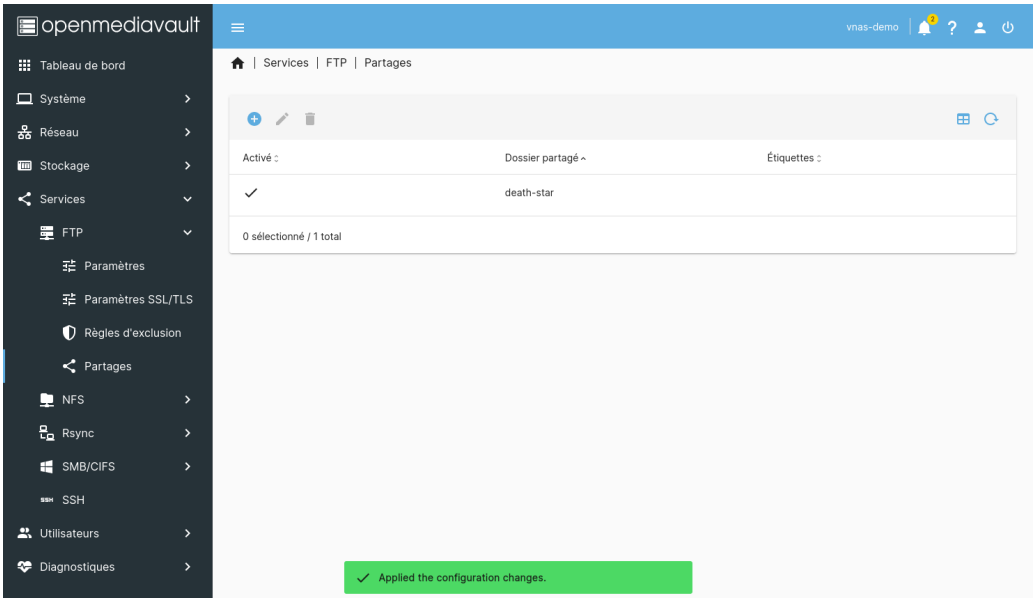
Dans le menu **Services** / **FTP** / **Partages**, cliquez sur le bouton **+ (Créer)** :



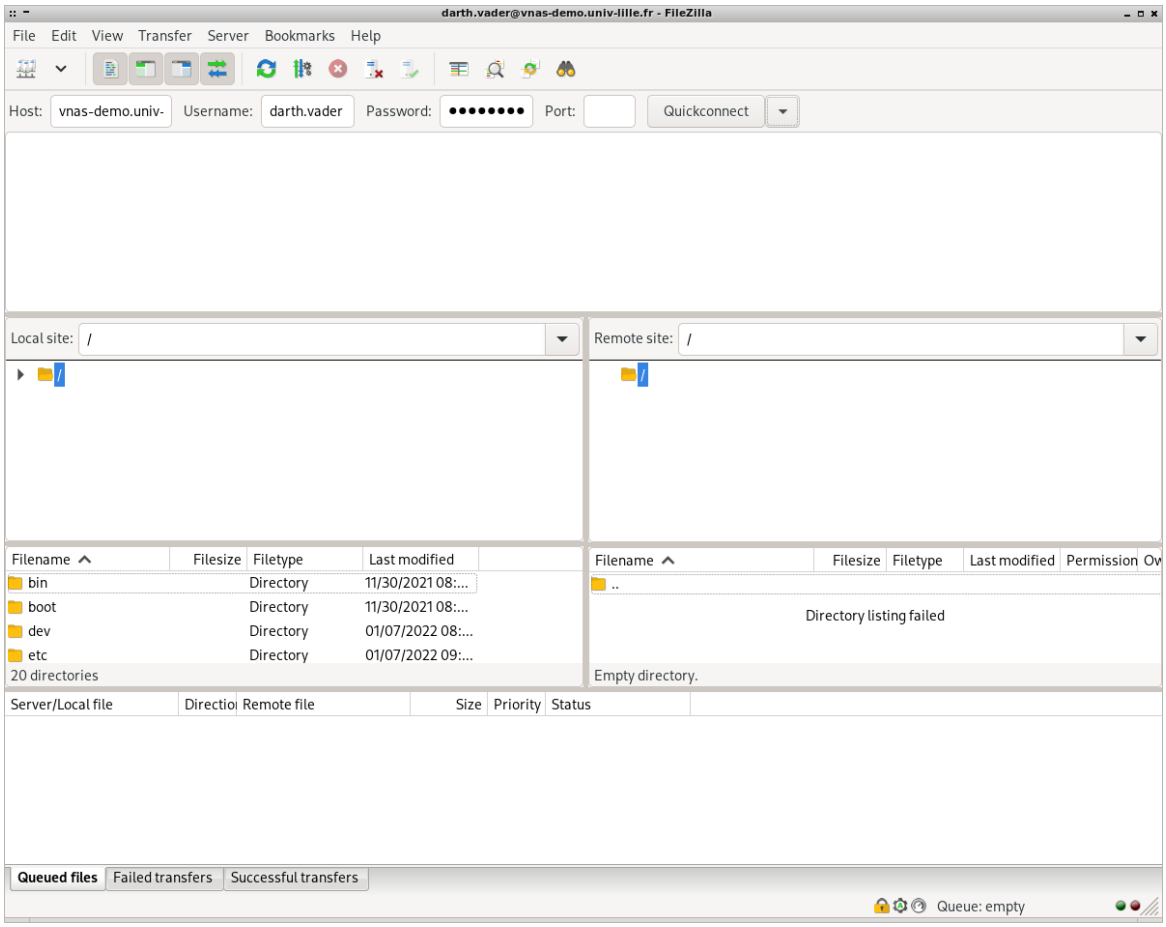
Dans le formulaire, sélectionnez le nom du répertoire (dossier partagé) puis cliquez sur **Enregistrer** :



Le nouveau partage devrait apparaître dans la liste :

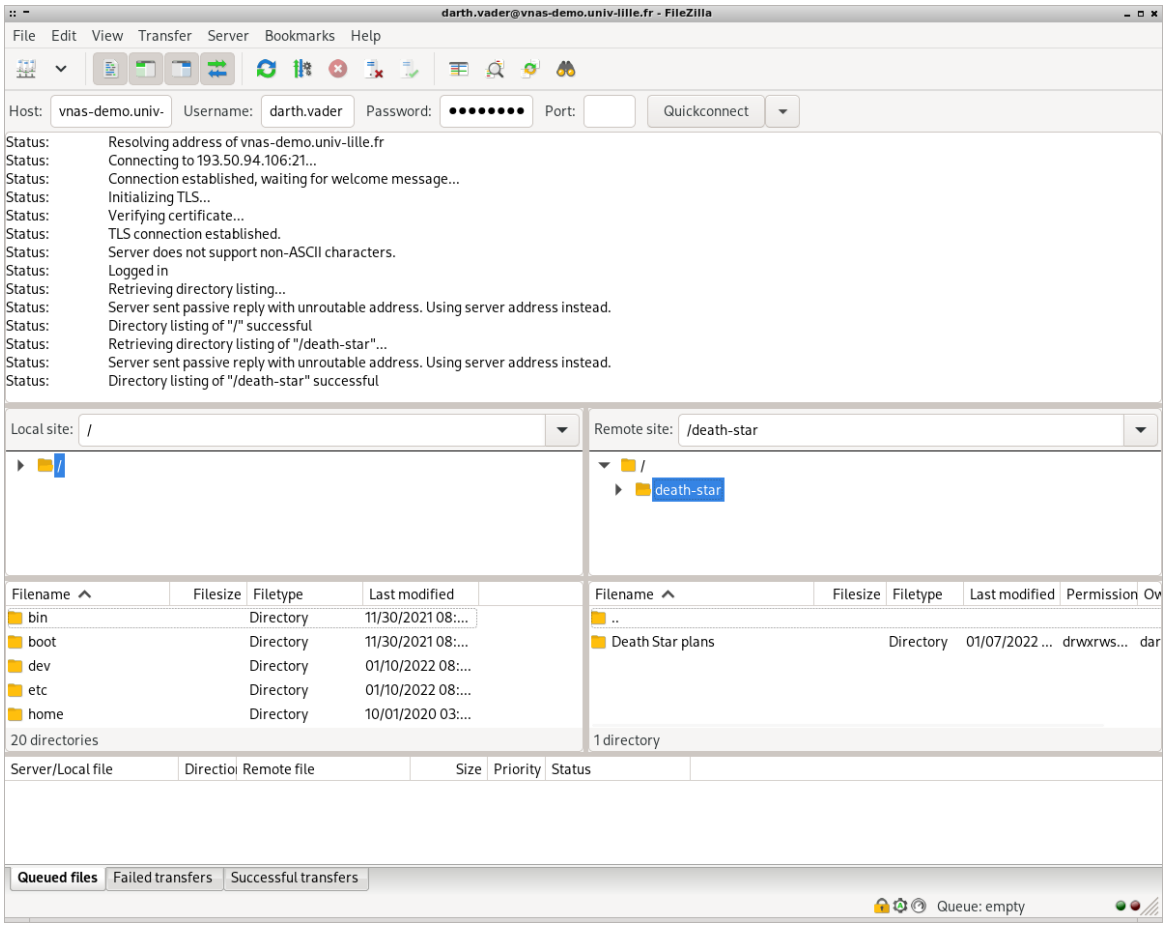


Il est maintenant possible de monter le stockage depuis un client FTP en utilisant l'adresse du serveur qui vous a été communiquée par le mésocentre (dans cet exemple, *vnas-demo.univ-lille.fr*) et un utilisateur ayant les droits d'accès au répertoire (voir chapitre *Gestion des privilèges (ACL)*) :



Lors de la première connexion, vous devrez probablement autoriser le certificat en tant que certificat de confiance :

Puis les répertoires auxquels l'utilisateur a accès apparaîtront dans la liste :

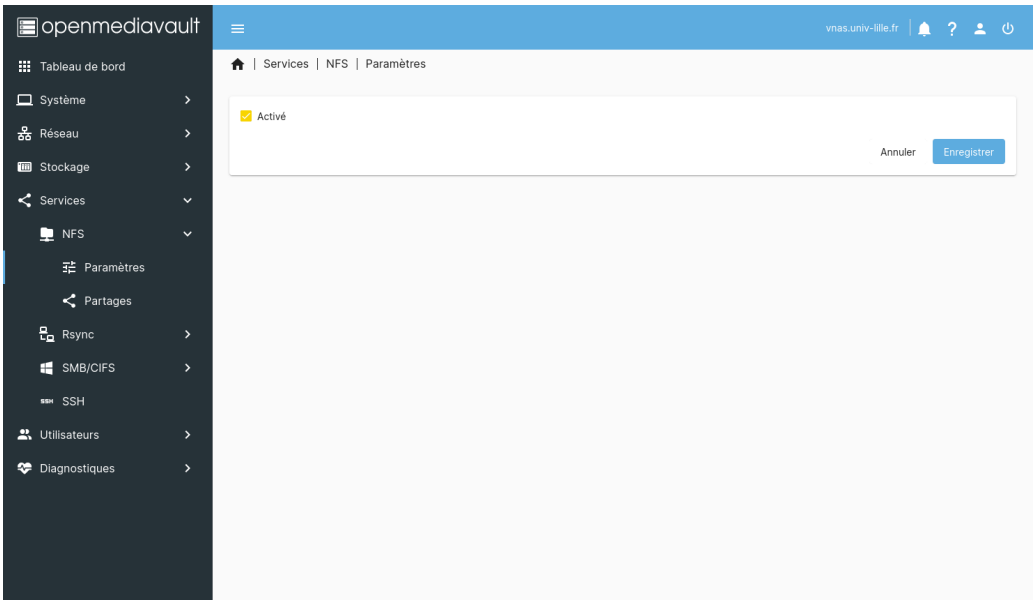


3.3 Partages NFS (Linux/MacOS)

Attention : Le NFS permet une gestion moins fine des privilèges en comparaison des protocoles précédents.

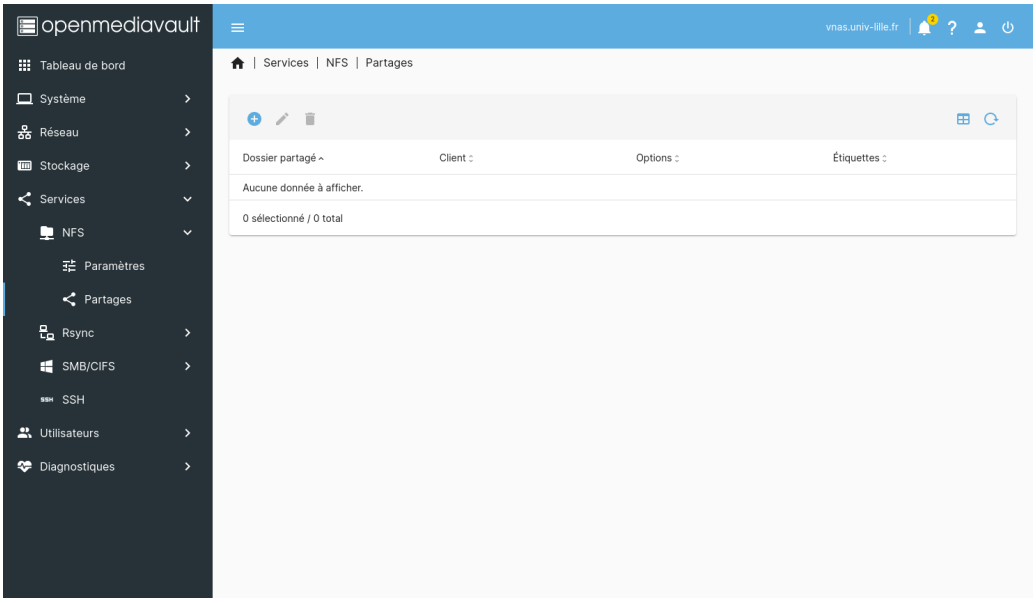
Pour activer le partage NFS, rendez-vous dans le menu **Services** / **NFS** / **Paramètres**.

Cochez l'option **Activer** puis cliquez sur **Enregistrer** :

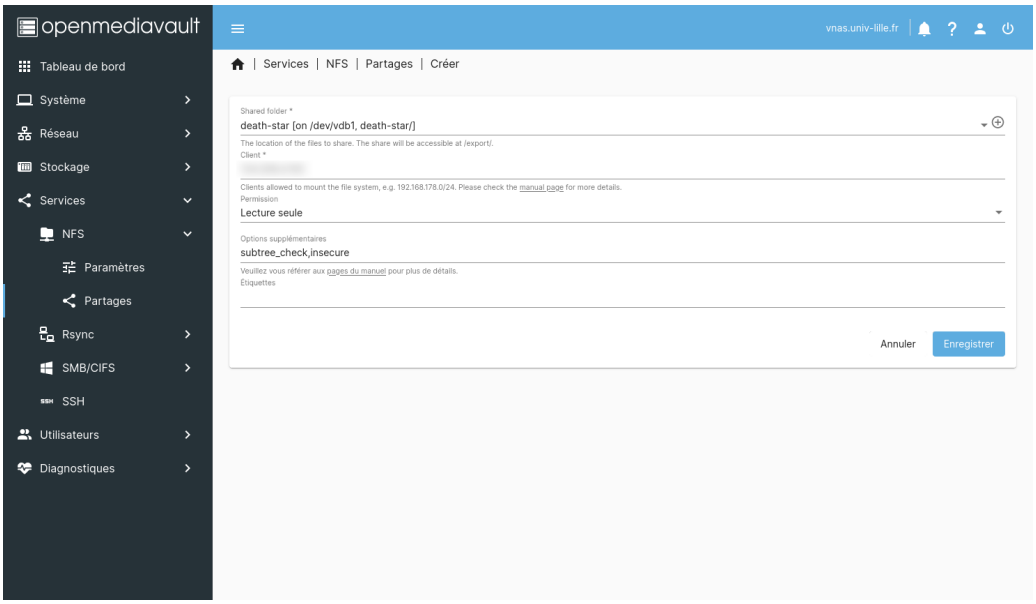


Vous pouvez maintenant partager des répertoires principaux (voir chapitre *Création d'un répertoire principal*) sur le réseau via le protocole NFS.

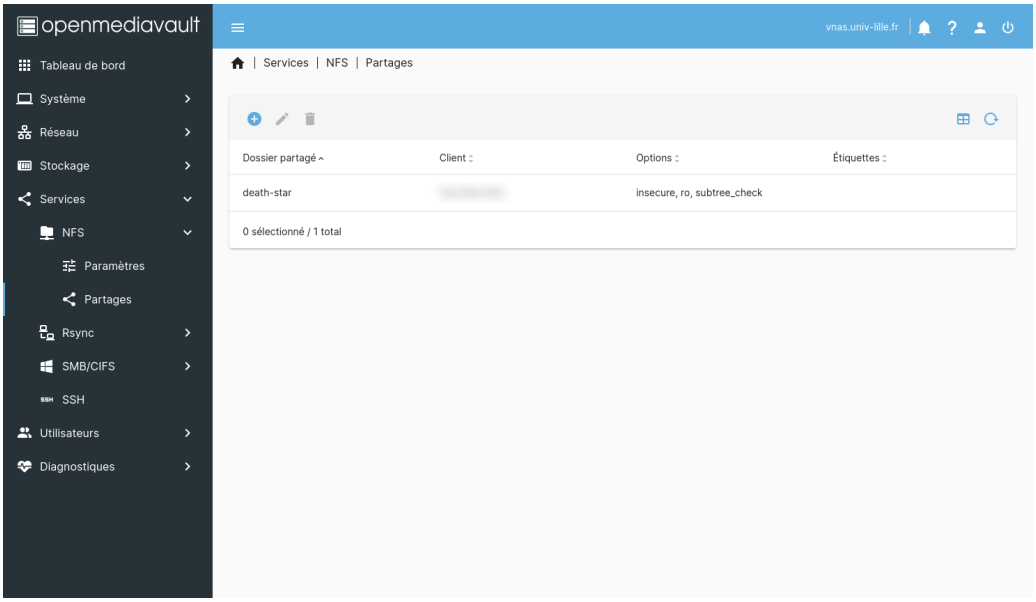
Dans le menu **Services** / **NFS** / **Partages**, cliquez sur le bouton + **(Créer)** :



Dans le formulaire, renseignez le nom du répertoire (dossier partagé) ainsi que l'adresse IP du client, choisissez le niveau de permissions puis cliquez sur **Enregistrer** :



Le nouveau partage devrait apparaître dans la liste :



Vous pouvez maintenant monter le stockage depuis un client NFS en utilisant l'adresse du serveur qui vous a été communiquée par le mésocentre (dans cet exemple, *vnas-demo.univ-lille.fr*) et le nom du répertoire principal :

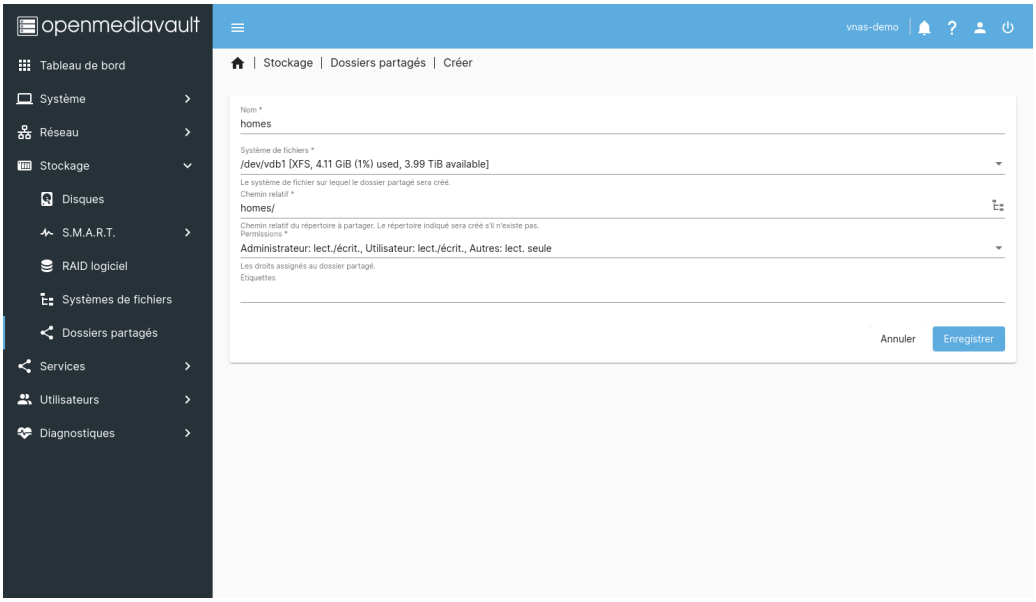
```
[vader@starship ~]$ sudo mount -t nfs vnas-demo.univ-lille.fr:death-star/ /mnt/
[vader@starship ~]$ ls /mnt/
'Death Star plans'
```

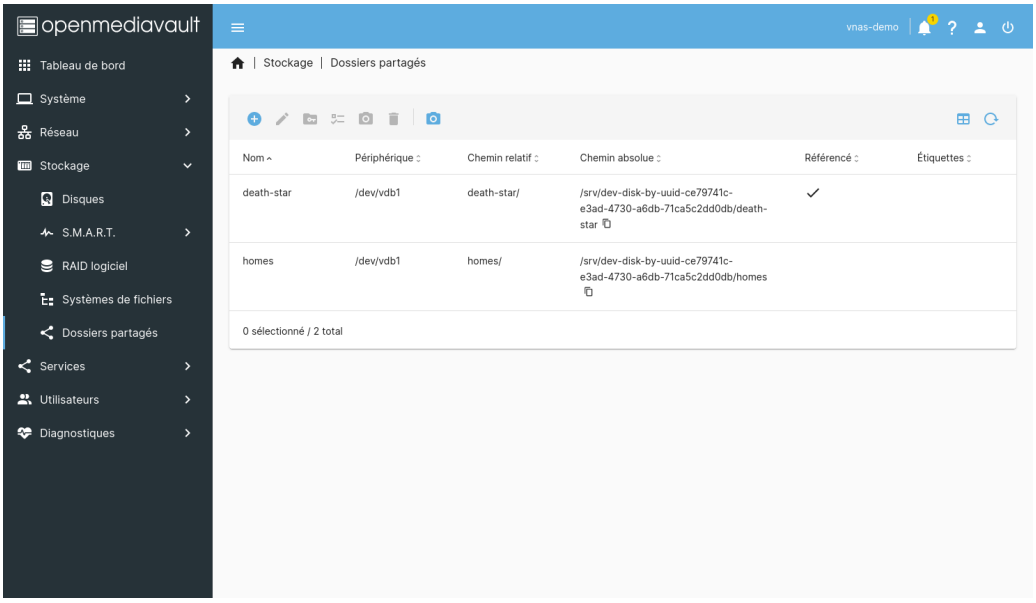
3.4 Répertoires utilisateurs

Il est possible d'activer les répertoires utilisateurs pour le service SMB/CIFS uniquement.

Prérequis : le service SMB/CIFS doit être activé en suivant les étapes du chapitre *Partages SMB/CIFS (Windows/Linux/MacOS)*.

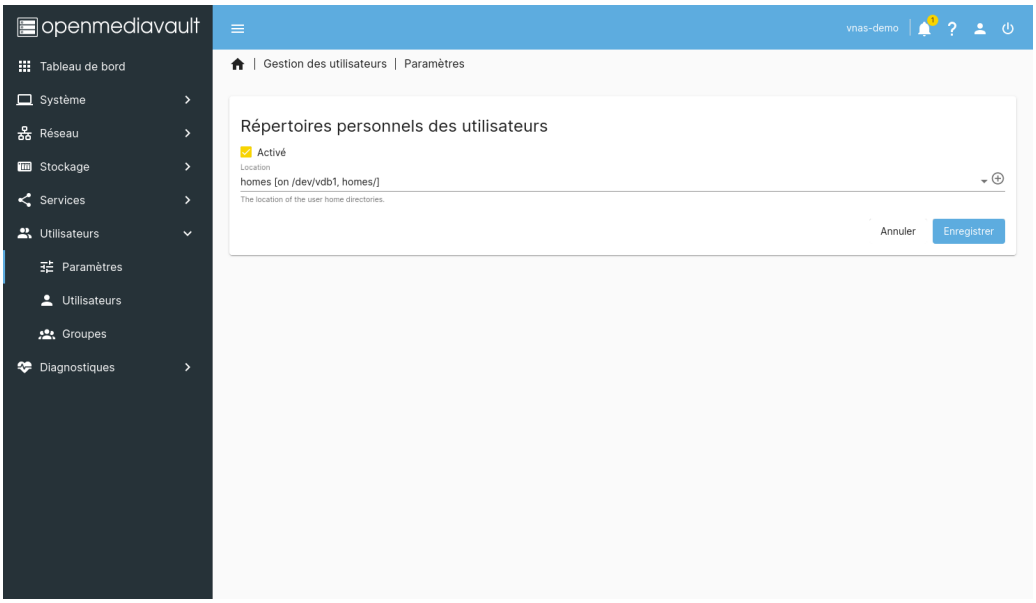
La première étape est de créer un répertoire partagé (nommé **homes** dans cet exemple) qui contiendra les répertoires utilisateurs (voir chapitre *Création d'un répertoire principal*) :



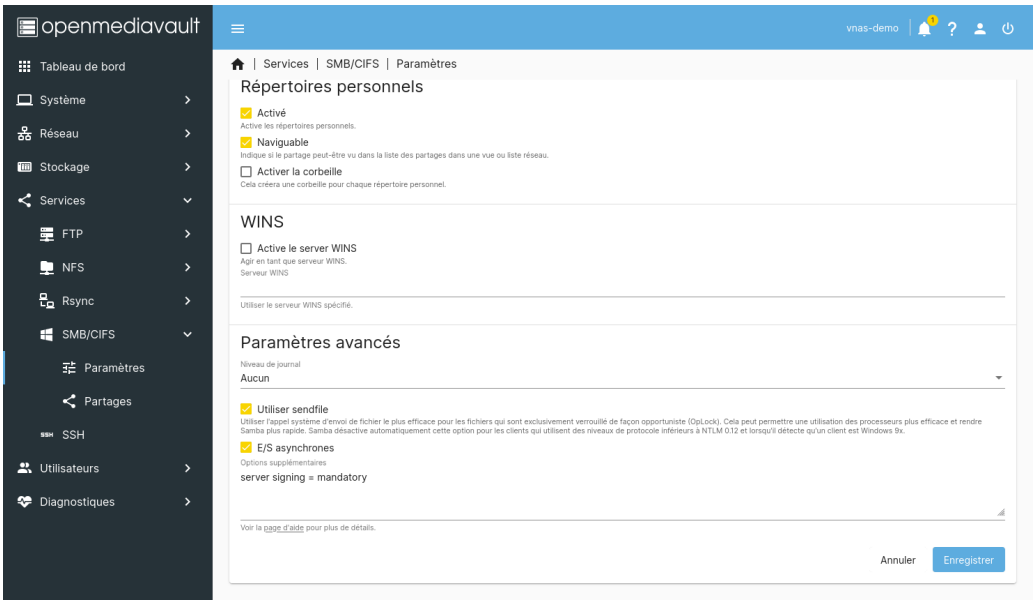


Une fois ce répertoire principal créé, rendez-vous dans le menu **Utilisateurs** / **Paramètres**.

Cochez l'option **Activé**, sélectionnez le répertoire principal que vous venez de créer, puis cliquez sur **Enregistrer** :



Enfin, rendez-vous dans le menu **Services** / **SMB/CIFS** / **Paramètres** et cochez l'option **Activé** dans l'encart **Répertoires personnels** avant de cliquer sur **Enregistrer** :



L'utilisateur aura maintenant accès à son répertoire personnel dans les montages réseau SMB/CIFS sous le nom du répertoire partagé que vous aurez choisi (ici **homes**).

Chapitre 4

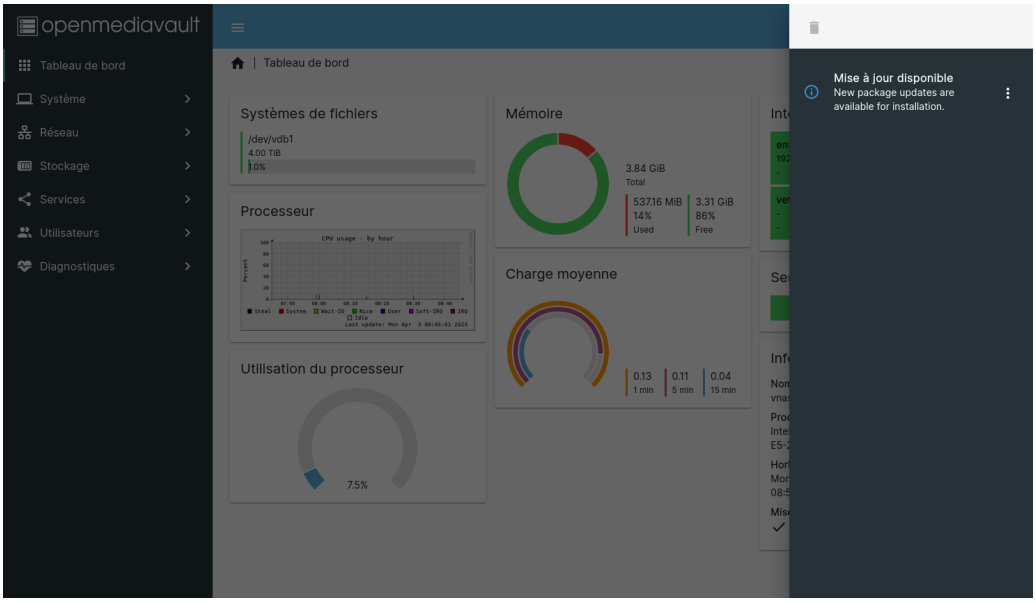
Bonnes pratiques et sécurité

4.1 Mises à jour

Vous serez régulièrement amené à effectuer des mises à jour pour garder votre service de stockage sécurisé.

Les notifications en haut à droite du tableau de bord sont là pour vous le rappeler :

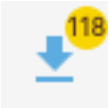
Vous pouvez cliquer sur la cloche pour voir le détail des notifications :



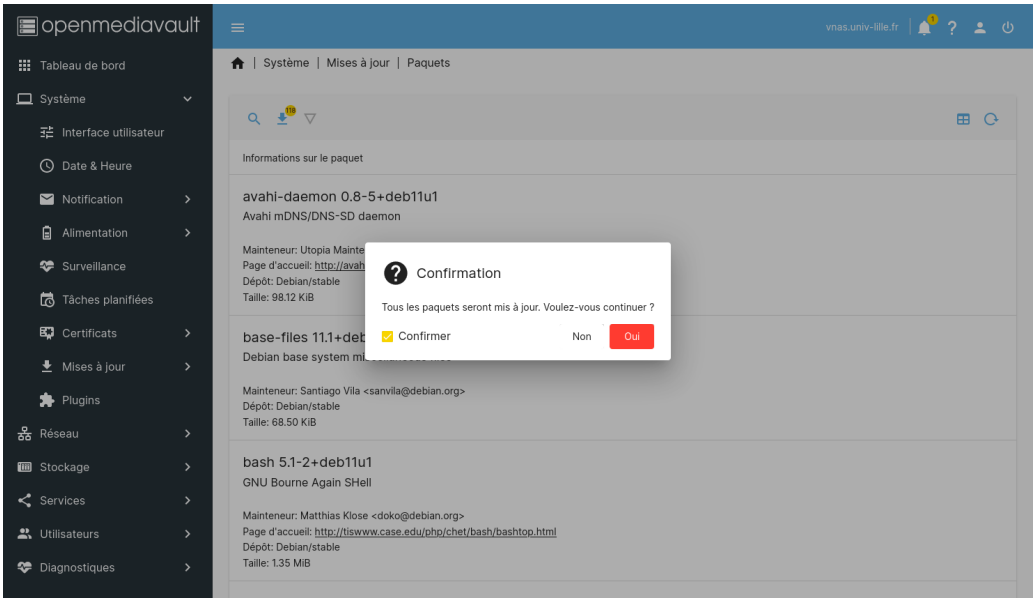
Pour voir les mises à jour disponibles, cliquez sur la notification ou allez dans le menu

Système / Mises à jour / Paquets.

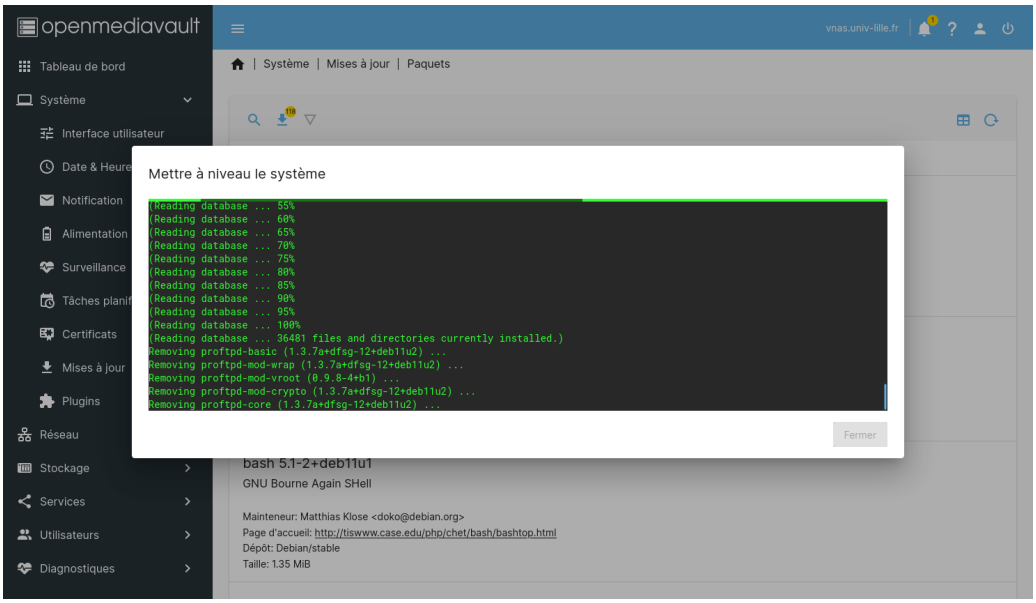
La flèche vers le bas vous permettant d'installer les mises à jour s'illumine en bleu avec le nombre de mises à jour disponibles en étiquette :



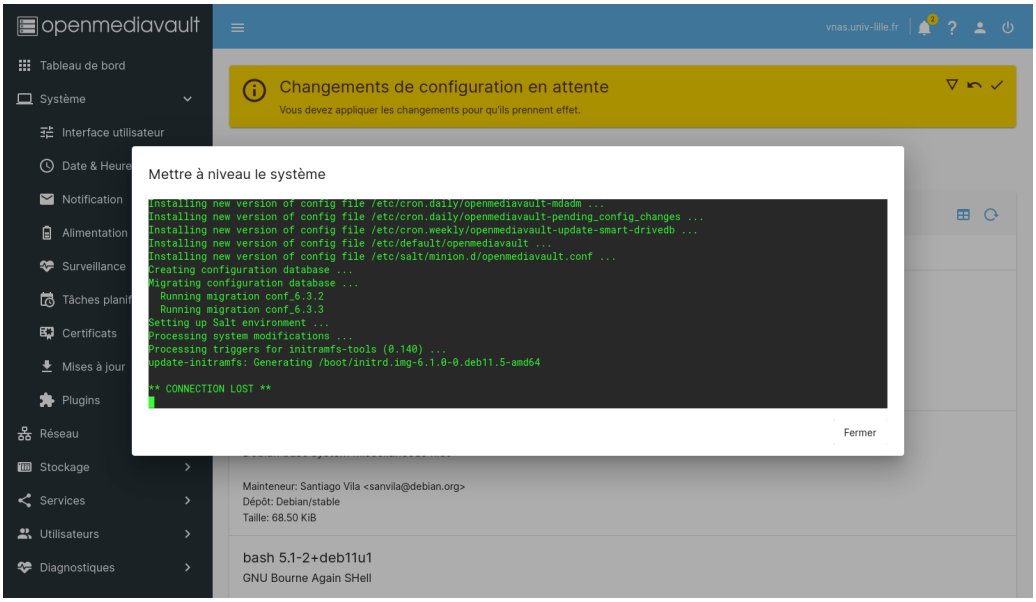
Cliquez dessus, puis confirmez votre souhait d'installer les mises à jour :



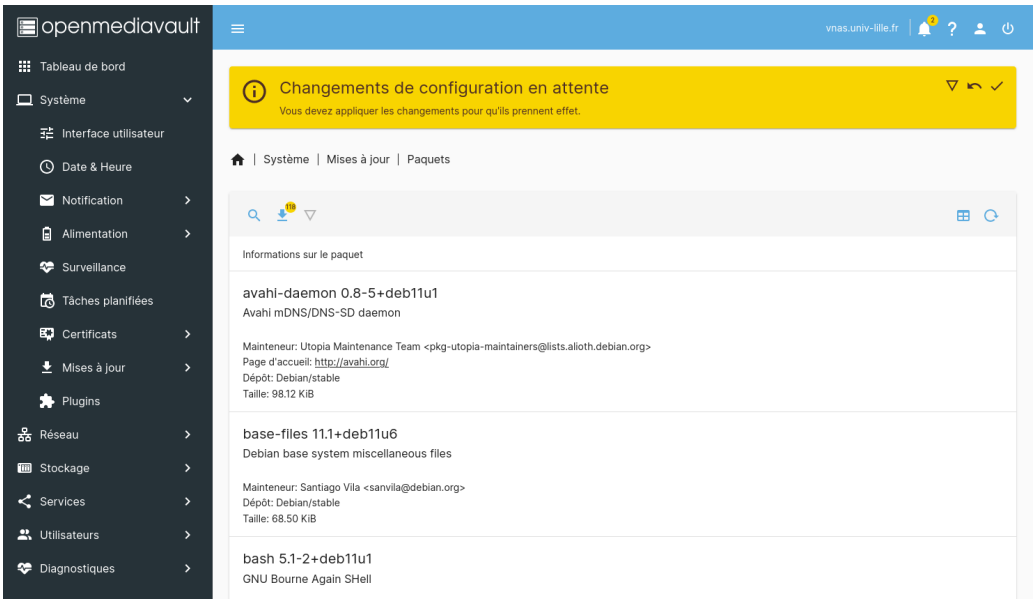
La mise à jour débute. Elle peut durer plusieurs minutes :

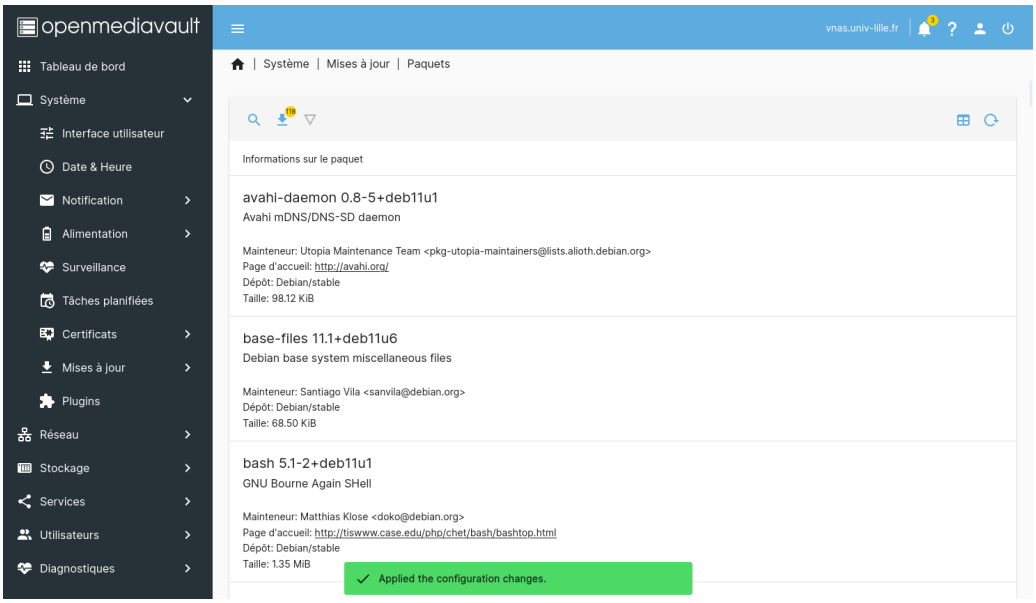


Patientez jusqu'à ce que le bouton **Fermer** en bas à droite de l'encart devienne cliquable :

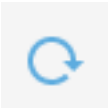


Puis validez les changements en attente :

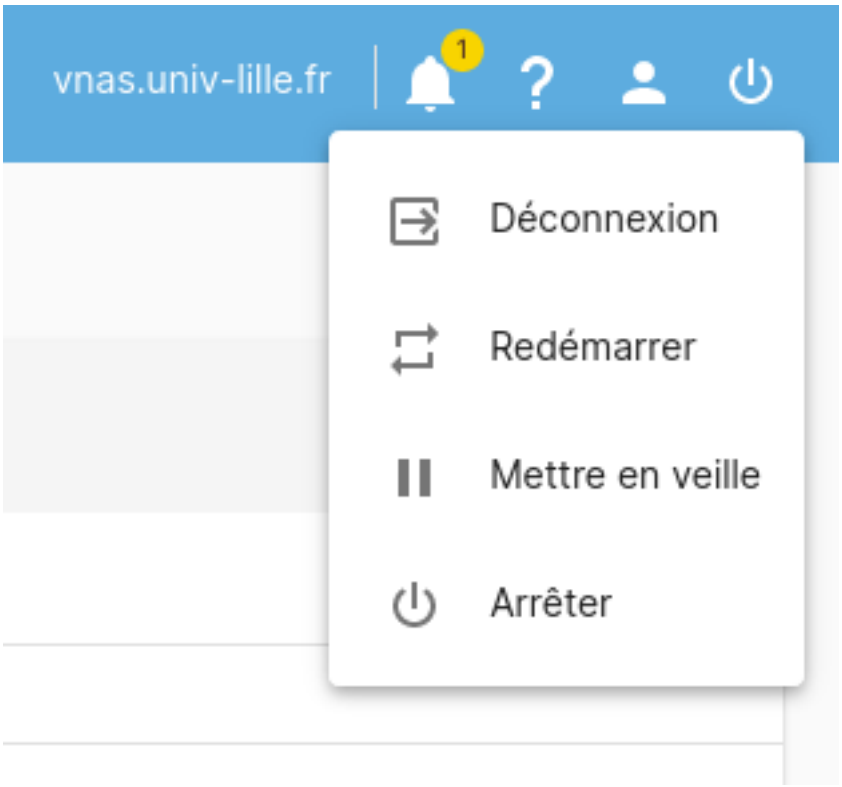




Astuce : Si le nombre de mise à jour disponibles n'a pas changé, vous pouvez réactualiser la vue en cliquant sur l'icone suivant :



Certaines mises à jour nécessitent un redémarrage qui dure quelques secondes. Pour redémarrer, cliquez sur l'icone en haut à droite puis sur **Redémarrer** :



Note importante : durant ce redémarrage, vos utilisateurs **n'auront plus accès** au stockage ! Pensez à les prévenir au préalable, ou à effectuer cette opération pendant un temps creux.

Puis la page de connexion revient automatiquement une fois le serveur redémarré.

4.2 Certificats

Votre service de stockage utilise un certificat officiel, issu d'une authorité de certification reconnue, pour garantir l'authenticité de l'interface web d'administration et des services de stockage.

Les certificats ont une durée de validité d'un an. L'équipe du Mésocentre se charge de leur renouvellement annuel et de leur installation.

Aucune action n'est requise de votre part et il est par conséquent interdit de les modifier vous-même.

4.3 Configurations immuables

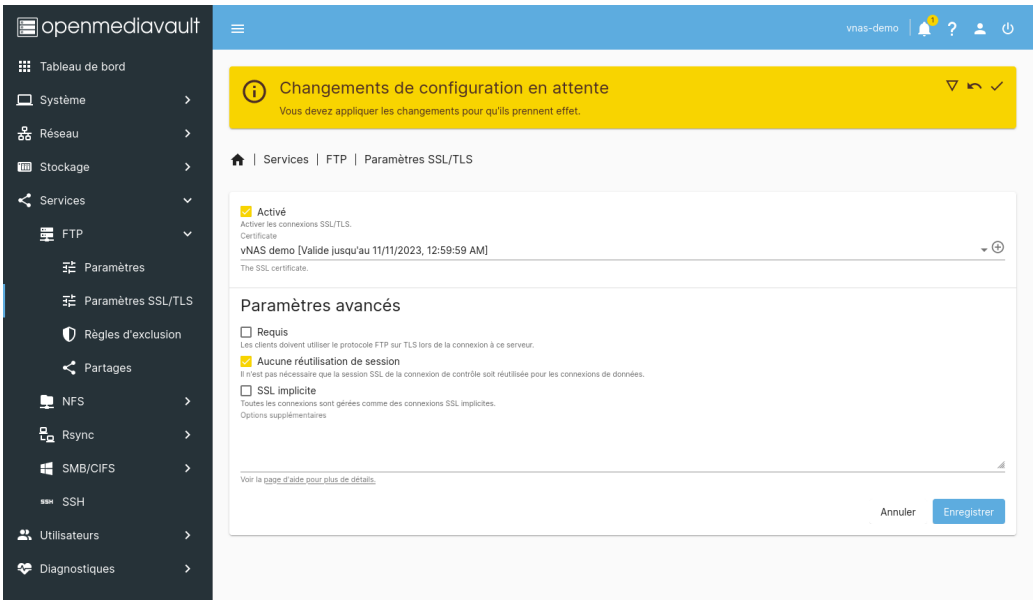
Certaines configurations ont été établies pour permettre à l'équipe du Mésocentre d'accéder au service de stockage pour les mises à jour de certificats ou pour répondre à vos demandes de support.

Il est donc interdit de modifier la configuration de l'**utilisateur omv** et le mot de passe de l'**utilisateur admin**.

Aussi, certains services de partage sont réputés peu sécurisés. C'est le cas du protocole FTP.

Sans chiffrement des communications par une connexion SSL/TLS, toutes les données et mots de passe transitent en clair sur le réseau. Il est alors aisé d'écouter les flux réseau pour voler vos informations.

Pour cette raison, il est absolument obligatoire de maintenir le paramétrage SSL/TLS du service activé tel que décrit dans le chapitre *Partages FTP (Windows/Linux/MacOS)* :



4.4 Filtrage réseau et pare-feu

Par défaut, votre service de stockage n'est accessible que depuis les bâtiments du campus Cité Scientifique de l'Université dont le réseau est géré par l'établissement (donc hors Centrale Lille, Polytech Lille, ENSCL, IMT, etc.) et via le VPN de l'Université de Lille. Si votre stockage concerne le domaine de la biologie & santé, il est également accessible depuis les bâtiments du pôle recherche du CHRU de Lille (à condition que le réseau soit géré par l'Université).

Cette restriction a été établie pour réduire les risques d'intrusion et donc de compromission de vos données.

D'autres adresses IP institutionnelles peuvent également être autorisées au cas par cas sur simple demande par mail.

Votre NAS virtuel est également protégé au sens large par un système de prévention d'intrusion (IPS) bloquant chaque jour plusieurs milliers de tentatives. Il arrive que ce pare-feu vous bloque pour une durée de 6h à cause d'un faux-positif.

En cas de blocage, merci de nous communiquer sous les 6h (et pendant les horaires de travail) votre lieu géographique et votre adresse IP à cette même adresse email.

Pour toute demande : hpc@univ-lille.fr

4.5 Nature des données

L'offre de service de stockage granulaire vNAS du Mésocentre est dédiée à l'hébergement de données de recherche :

— jeux de données ;
— données de recherche (publications, résultats, etc.) ;
— données issues d'instruments scientifiques ;
— données issues de calculs, traitements ou simulations.

Il est interdit d'utiliser ce service pour l'hébergement d'autres types de données, tels que :

— sauvegardes de poste de travail ;
— données de gestion de parc ;
— données applicatives ;
— données administratives ;
— données personnelles ;
— etc.

De plus, il est **strictement interdit** d'y déposer des données soumises à la détention d'une **habilitation HDS** (hébergement de données de santé).

4.6 Sauvegarde

L'offre de service dans sa plus simple déclinaison n'inclue pas de sauvegarde. Il est cependant possible de souscrire (initialement ou dans un second temps) à l'option de sauvegarde afin d'en bénéficier.

Cette sauvegarde est réalisée quotidiennement dans un autre datacentre (hors site) à travers un canal de communication chiffré de bout en bout.

Il ne s'agit pas d'une sauvegarde traditionnelle (fichier par fichier), mais d'une sauvegarde globale du serveur de stockage. Elle ne permet donc pas la récupération d'un fichier effacé accidentellement, mais a pour but la restauration intégrale du service suite à un incident de sécurité ou une panne matérielle majeure.

4.7 Séparation des privilèges

Selon le statut propre à chaque utilisateur du service de stockage, vous serez probablement amené à segmenter les privilèges d'accès aux fichiers par exemple pour interdire l'accès aux données par des utilisateurs étrangers à un projet de recherche.

Cette segmentation peut être globalisée et donc facilitée grâce à des groupes utilisateurs.

Prennons l'exemple d'une entité fictive nommée **l'Empire** composée de 3 chercheurs permanents (**Alice**, **Bob**, **Clémentine**) et de 2 doctorants (**Damien**, **Eléonore**).

Alice, Bob et Damien travaillent sur le projet de recherche **Destroyer Impérial**, Clémentine et Eléonore travaillent sur le projet **Chasseur TIE**, et enfin, Alice et Clémentine travaillent sur un projet un peu plus sensible nommé **Etoile de la Mort**.

Nous allons créer les groupes utilisateurs suivants :

— **empire-permanents** (membres : alice, bob, clementine)
— **empire-non-permanents** (membres : damien, eleonore)
— **destroyer-imperial** (membres : alice, bob, damien)
— **chasseur-tie** (membres : clementine, eleonore)
— **etoile-de-la-mort** (membres : alice, clementine)

Ainsi, vous pourrez donner l'accès à un répertoire principal en accordant les privilège à l'ensemble d'un groupe ou au contraire interdire l'accès à un groupe en particulier.

Par exemple :

— Répertoire **Motorisation des vaisseaux** : accessible en lecture/écriture au groupe **empire-permanents** et en lecture seule au groupe **empire-non-permanents**
— Répertoire **Systèmes de guidage** : accessible en lecture/écriture au groupe **empire-permanents** et en lecture seule au groupe **empire-non-permanents**
— Répertoire **Projet - Destroyer Impérial** : accessible en lecture/écriture au groupe **destroyer-imperial**
— Répertoire **Projet - Chasseur TIE** : accessible en lecture/écriture au groupe **chasseur-tie**
— Répertoire **Projet - Etoile de la Mort** : accessible en lecture/écriture au groupe **etoile-de-la-mort**

L'arrivée de Francis dans l'équipe de doctorants deux mois plus tard sera également plus simple à organiser.

Il suffira pour cela d'ajouter l'utilisateur **francis** aux groupes concernés, par exemple **empire-non-permanents** et **destroyer-imperial**, pour qu'il ait accès aux documents nécessaires à son projet de recherche.

Notez qu'il est possible de gérer les permissions plus finement par utilisateur en complément de la gestion par groupe (voir chapitre *Gestion des privilèges (ACL)*).