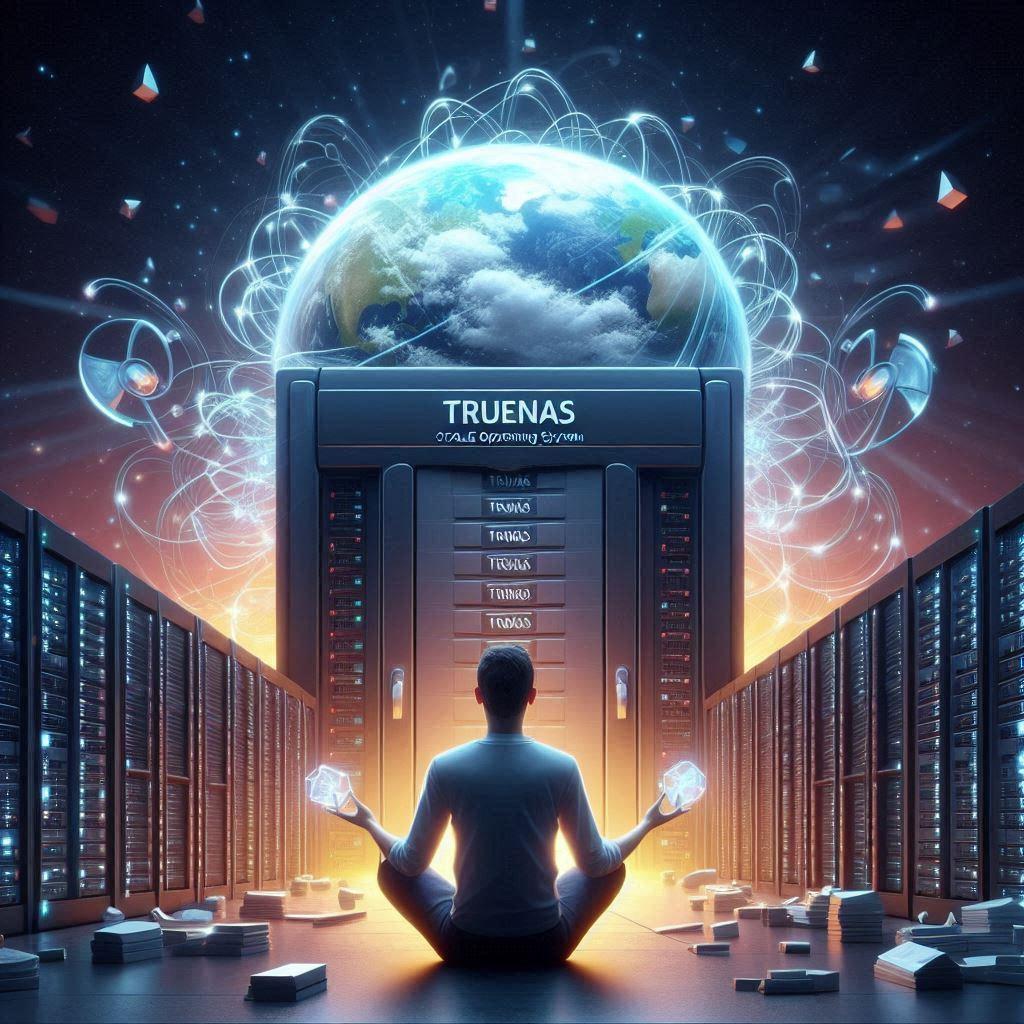
*PROJET TrueNas Scale*

**

*fait par* [Rija RASOANAIVO](mailto:rija.rasoanaivo@laplateforme.io) *et Manon RITTLING*

*AVANT PROJET :TrueNas Scale*

*Créer un serveur TrueNas Scale*

1. Installez deux machines virtuelles (VM) et un serveur TrueNAS Scale sur l'une d'entre elles. Vous pouvez télécharger le serveur depuis [ce lien](https://www.truenas.com/download-truenas-scale/).

2. Pour la première VM, installez Debian avec une interface graphique selon les critères suivants :

- Processeur : 2 cœurs

- Mémoire vive (RAM) : 2 Go

- Disque dur (DD) : 1 de 8 Go

3. Les spécifications de la VM hébergeant le serveur TrueNAS doivent respecter les critères suivants :

- Processeur : 2 cœurs

- Mémoire vive (RAM) : 4 Go

- Disques durs (DD) : 2 de 16 Go

- Disques durs supplémentaires : 5 de 2 To, que vous convertirez en un espace de stockage de 2 Go en utilisant un RAID 6 logiciel.

Première étape :

1. Après avoir accompli l'installation, créez un RAID 6 logiciel en utilisant les 5 disques de 2 To que vous avez préalablement configurés.

2. Allez dans l'onglet « Stockage » et créez un nouveau volume que vous nommerez « Stockage ».

Connexions et configurations :

1. Établissez des connexions à votre serveur via SSH, HTTPS et SFTP à partir de votre deuxième machine virtuelle.

2. Connectez-vous en HTTPS pour accéder au portail administrateur de votre serveur une fois l'installation terminée.

3. Vérifiez les mises à jour de votre installation et redémarrez le système si nécessaire.

4. Activez les services FTP et SSH de votre serveur.

5. Configurez le serveur SFTP en créant plusieurs sessions avec des dossiers dédiés et un dossier public. Assurez-vous de modifier le port de connexion par défaut.

Test et vérification :

1. Connectez-vous à votre serveur SFTP en utilisant la session de votre choix depuis la deuxième machine virtuelle. Assurez-vous de mettre à jour le port lors de la connexion.

2. Utilisez le logiciel de votre préférence pour vérifier le bon fonctionnement de l'ensemble.

Extensions possibles :

1. Pour aller plus loin, installez des applications qui peuvent améliorer votre serveur NAS. Ajoutez le catalogue TRUECHARTS avec l'URL fournie.

2. Pour une extension encore plus poussée, créez une VM sur TrueNAS Scale avec les identifiants fournis.

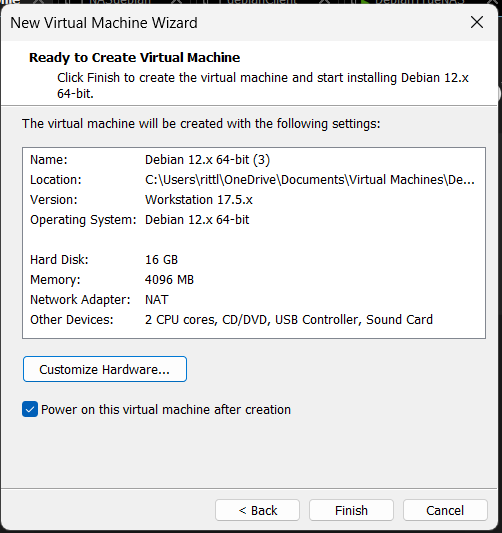
**PROJET**

1. **Configuration d’un raid et partitions de disques avec BIOS Debian**

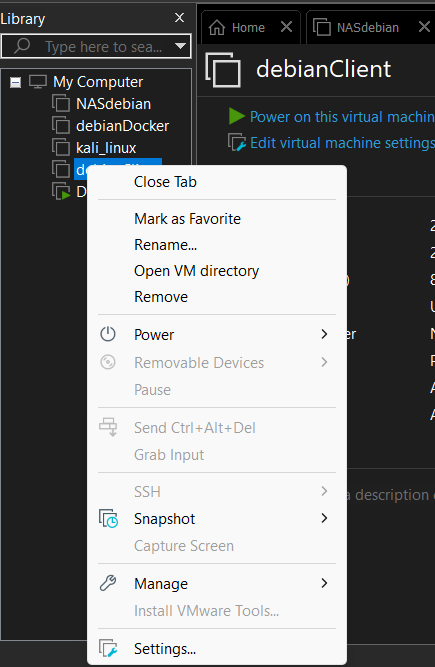
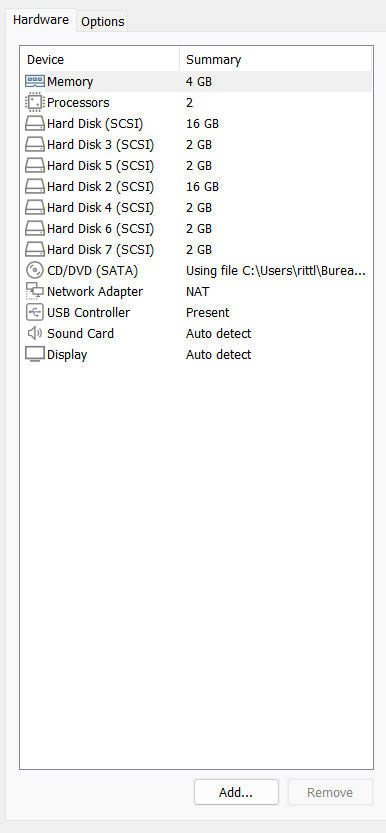
Pour commencer on crée notre vm debian pour ***TrueNAS*** avec un ***RAID 6*** dessus

Nous allons faire le partitionnement et configurer notre **RAID 6** via le ***BIOS*** directement.

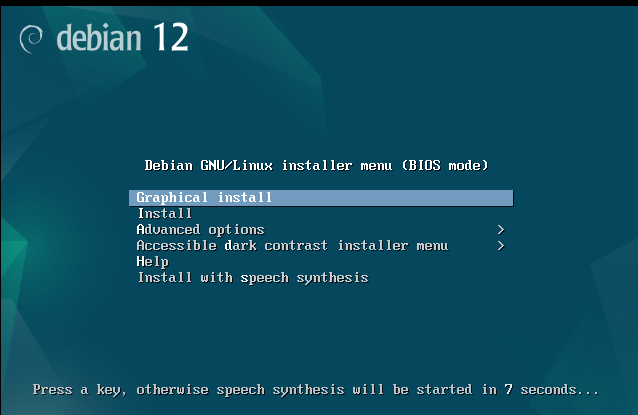
* Alors pour ce faire nous commençons par créer une nouvelle VM sur Vmware, on va sur ***CUSTOMIZE HARDWARE*** pour augmenter la ***ram a 4*** et on vérifie que ***le disque principal est bien a 16 giga.***



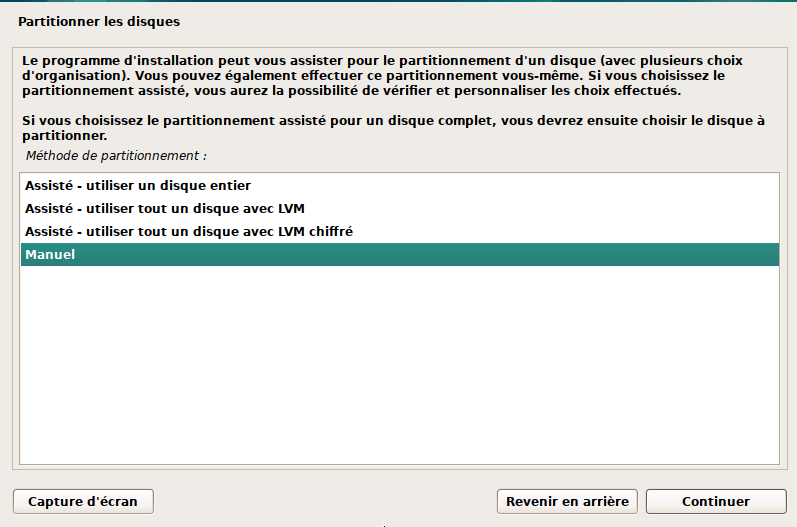
* Après clic droit sur la vm fraichement créer puis **“*setting”*** pour accéder à la configuration  
  de notre vm, nous allons ***ajouter*** notre ***second disque de 16g*** ainsi que ***nos 4 disques de 2g pour notre RAID 6.***

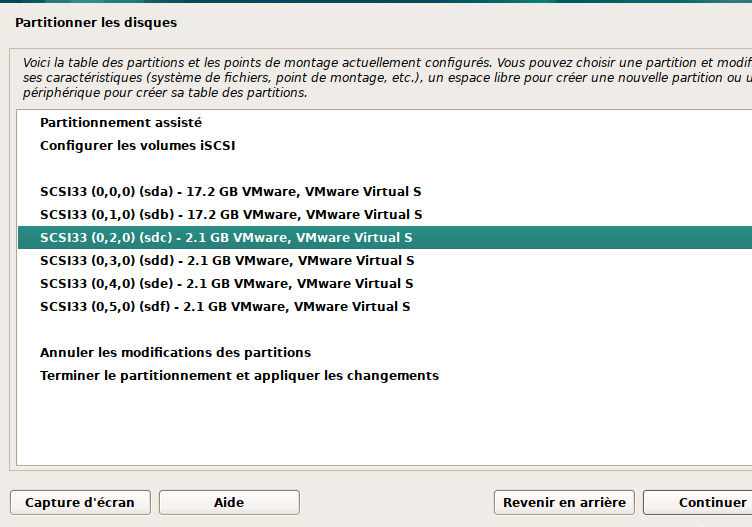
* L’ étape suivante, nous allons ***installer notre système d’exploitation debian 12*** et nous allons ***configurer notre RAID*** ainsi que faire ***les partitions de nos disques***.



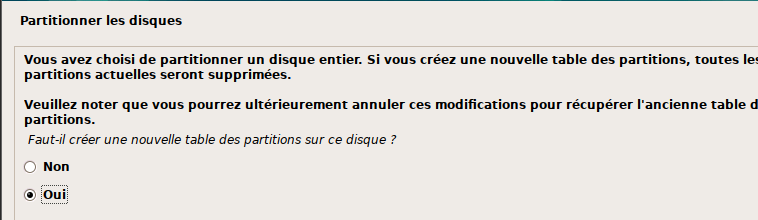
* On arrive à la page ***“PARTITIONNER LES DISQUES”***, on sélectionne ***“Manuel”.***



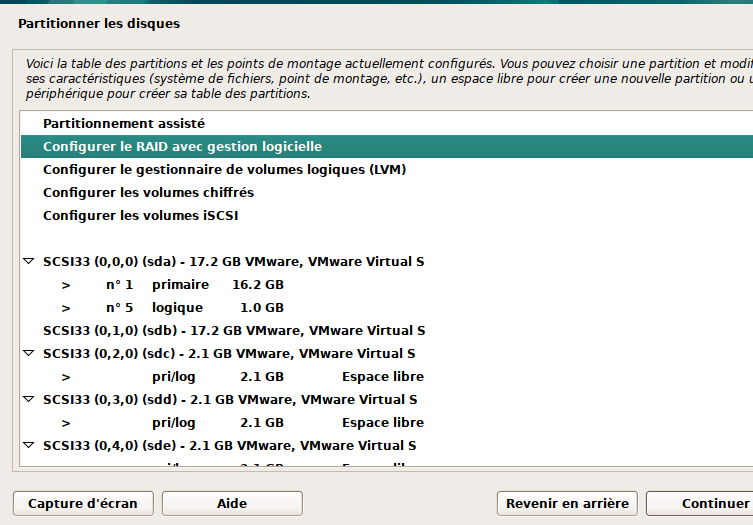
* On sélectionne un des disques que l’on souhaite partitionner



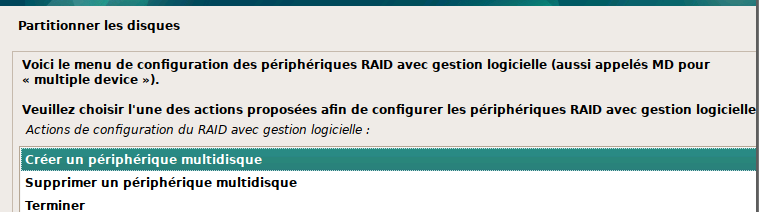
* On coche ***“oui”*** pour créer une nouvelle partition sur ce disque



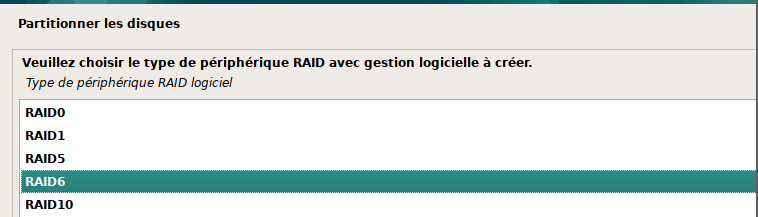
* Une fois les partitions faites sur nos 4 disques destinés pour notre RAID, on sélectionne ***“Configurer le RAID avec gestion logicielle”***

******

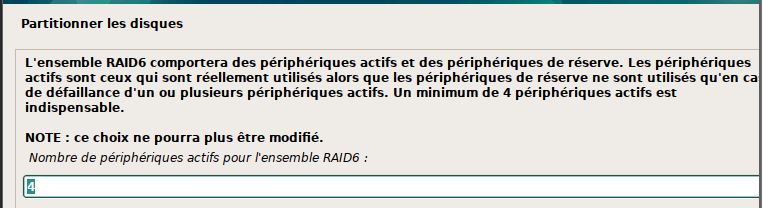
* On sélectionne ***“ Créer un périphérique multidisque”***

******

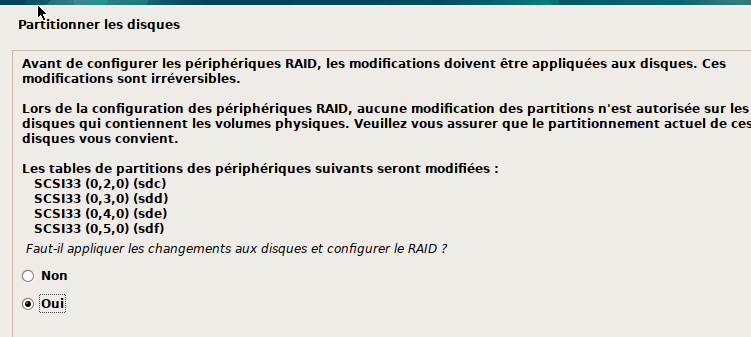
* Puis on choisi le raid que l’on souhaite mettre en place, pour nous il s’agit du ***“RAID 6”***

******

* Choix du nombre de disque que l’on souhaite pour notre RAID 6 ( on choisi le minimum requis soit 4)

******

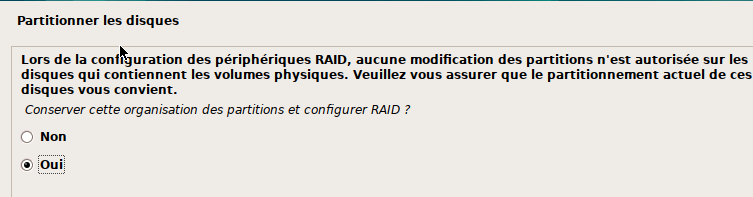
* Appliquer les changements aux disques que l’on vient de partitionner

******

* On termine la configuration du RAID

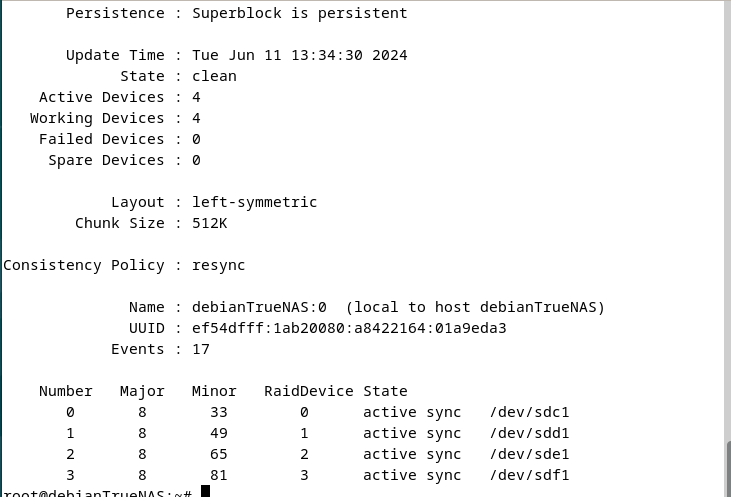
******

* ***On confirme la configuration faites***

******

* Pour obtenir les informations détaillés du RAID, il suffit de faire la commande suivante

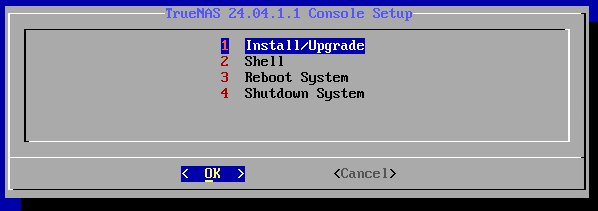
******



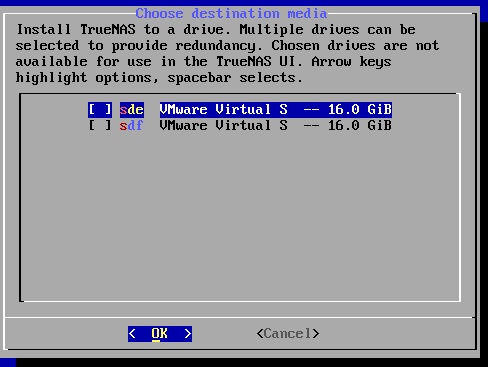
1. ***INSTALLATION ET CONFIG DE TrueNAS SCALE***

On se rend sur le site <https://www.truenas.com/download-truenas-scale/> pour ***télécharger l’image ISO*** de la version de ***TrueNas Scale.***

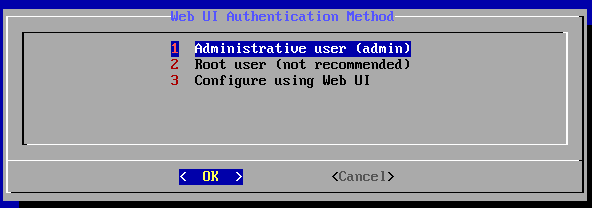
Une fois une nouvelle VM créée pour accueillir notre ***système d’exploitation*** TrueNas Scale.



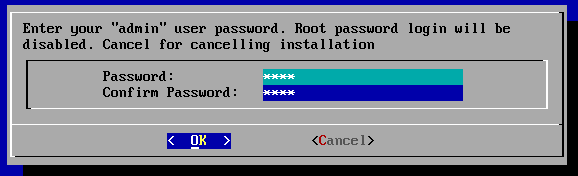
On choisi le disque avec lequel on souhaite installer notre OS



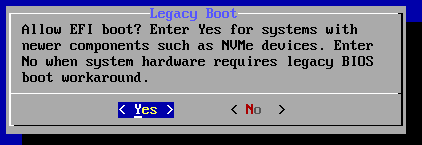
On choisi les autorisations que l’on souhaite pour notre ***USER => Admin pour avoir un maximum de droits***

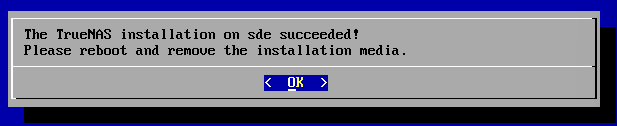


Puis on defini le mot de passe

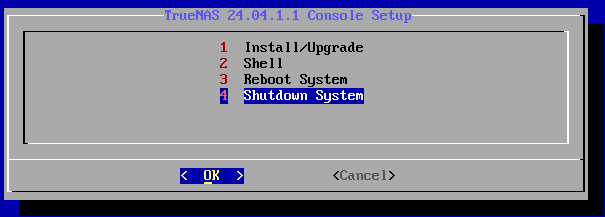


On valide la configuration

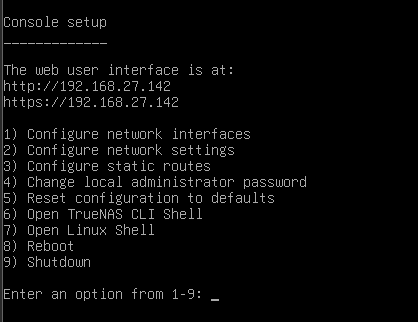




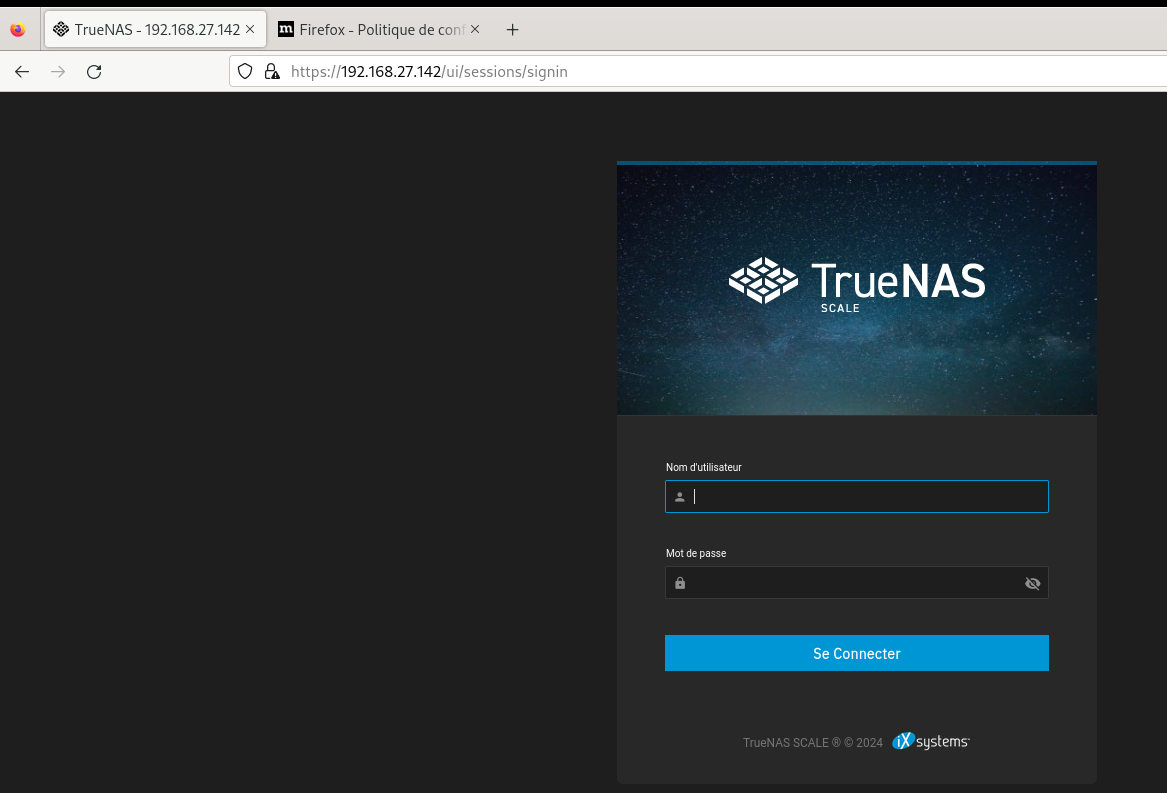
Puis on éteint le système



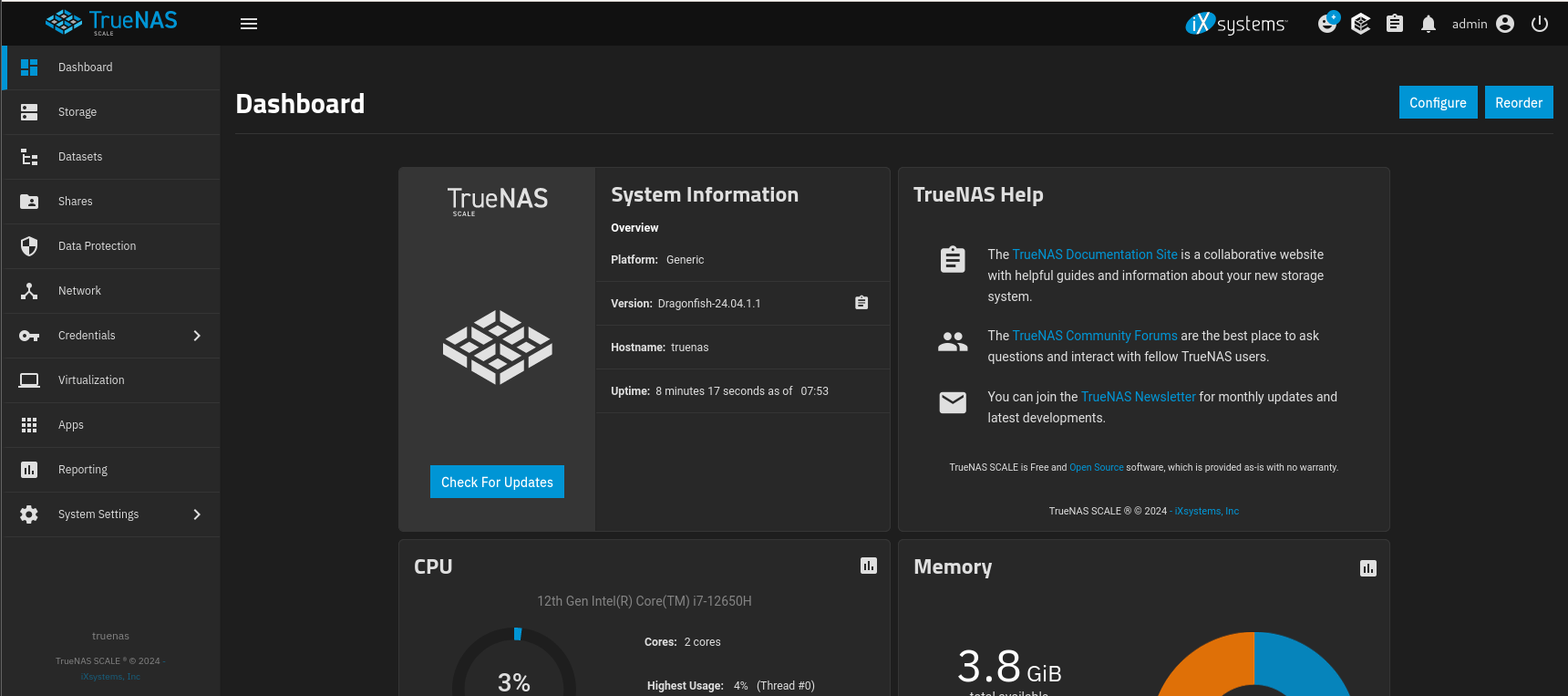
Résultat de la console TrueNas Scale



On ouvre la VM client que l’on a crée sous debian 12 puis on va sur le navigateur pour se connecter au serveur :

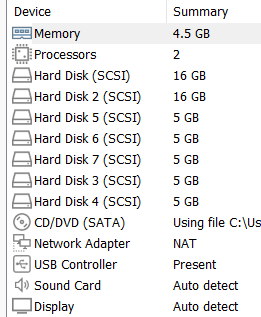


Et nous voila connecter a notre serveur

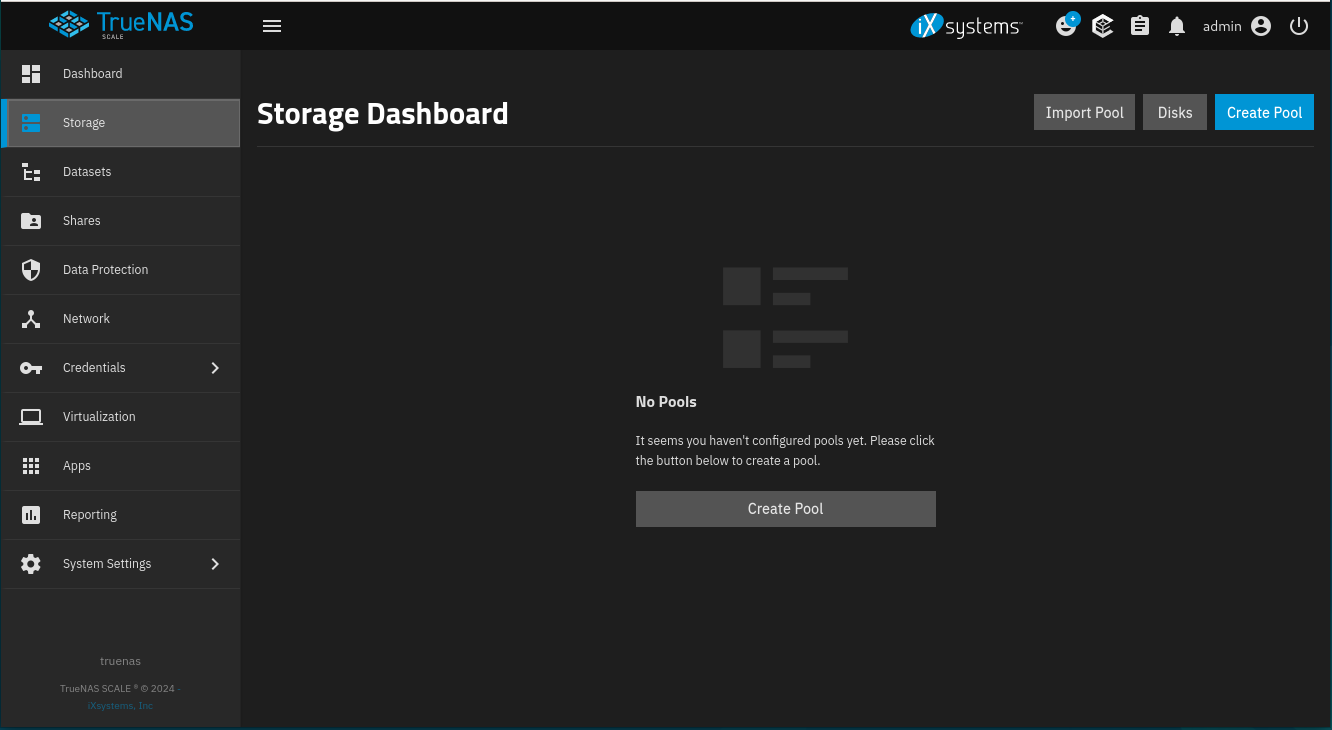


**Première étape :**

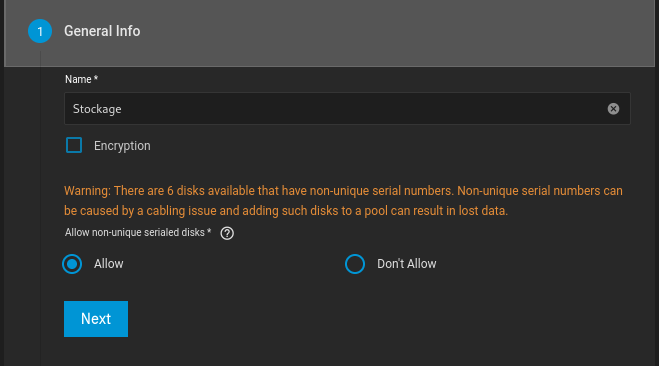
***1***. ***Après avoir accompli l'installation, créez un RAID 6 logiciel en utilisant les 5 disques de 2 To (convertit en 5go) que vous avez préalablement configuré***

TrueNAS ne peut pas configurer un RaidZ2 avec 5 disques durs de 2Go. Nous avons donc augmenté la capacité de nos disques durs afin d’avoir 5 disques durs de 5Go.  
Voici la configuration matériel de notre VM:  


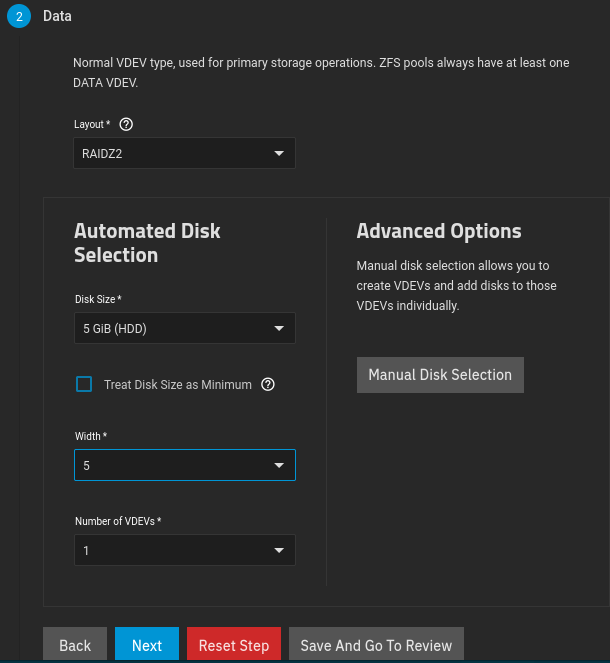
1. On clique ensuite sur “Storage” et “Create Pool”



1. On donne le nom “Stockage” à notre pool et cliquer sur “Allow” pour que le système détecte les disques durs. Puis cliquer sur “Next”

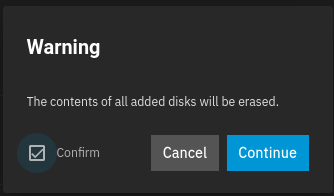
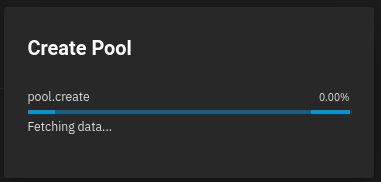


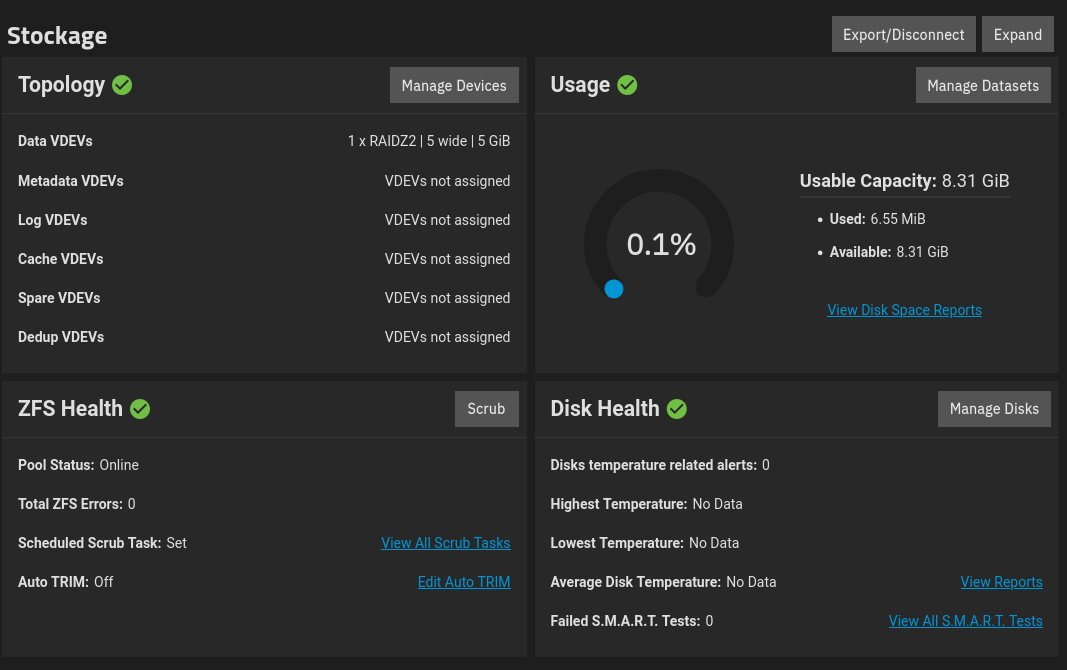
1. On choisit “RAIDZ2” équivalent à un RAID6. On sélectionne la taille “5GIB” correspondant à la taille des disques que l’on souhaite monter, puis le nombre de disques.  
   Enfin, on va directement à la fin de l’étape en cliquant sur “Save And Go To Review”

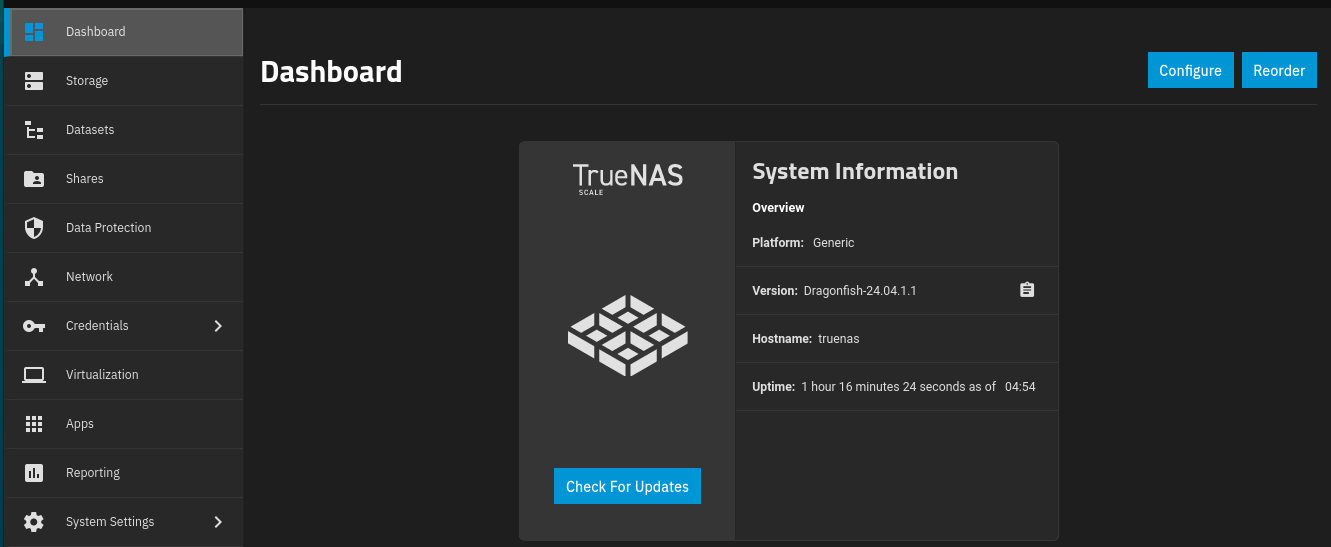


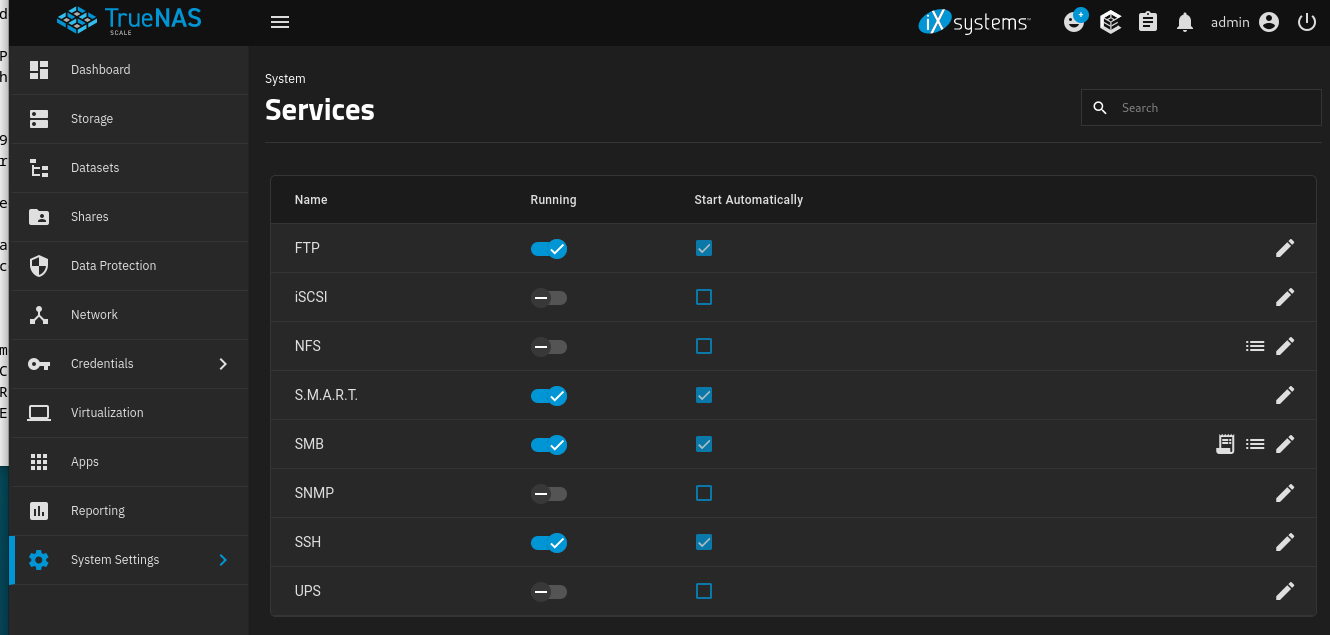
1. On clique ensuite sur “Create Pool”.  
   Une fenêtre “Warning” va apparaître, on check “Confirme” et on clique sur “Continue”



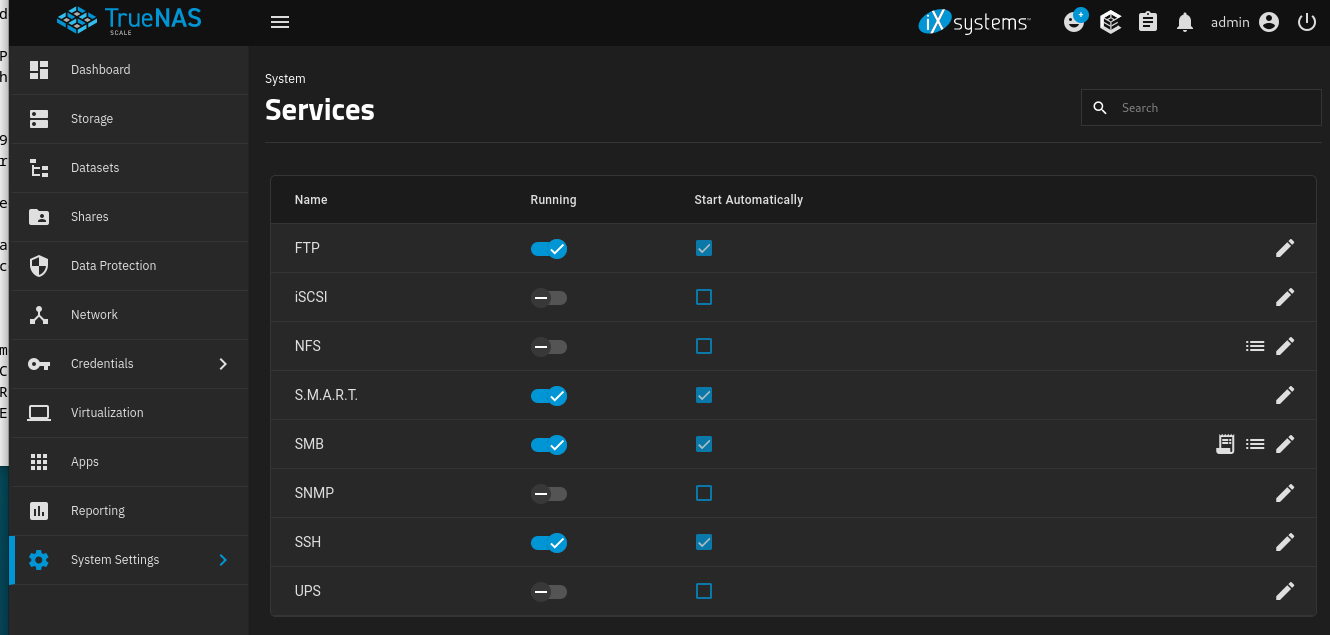
Voici notre interface une fois le RAIDZ2 monté :  


Pour vérifier les MàJ. Dans l’onglet “Dashboard”, on clique sur “Check For Updates”  


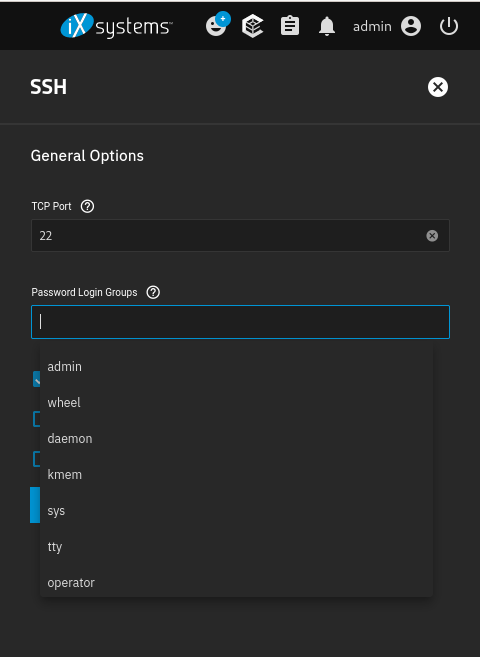
***Activer le service FTP et SSH:***Pour activer le service “FTP” et “SSH” on va sur l’onglet “System Settings” et on active les services que l’on souhaite  


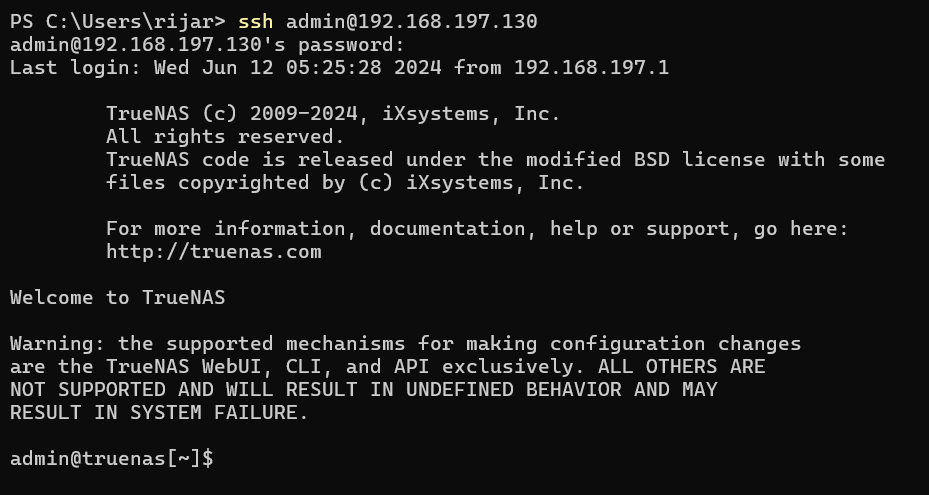
***Connection en SSH***

* Pour configurer nos services, il suffit de se rendre dans le menu de configuration du service, on clique sur le stylo

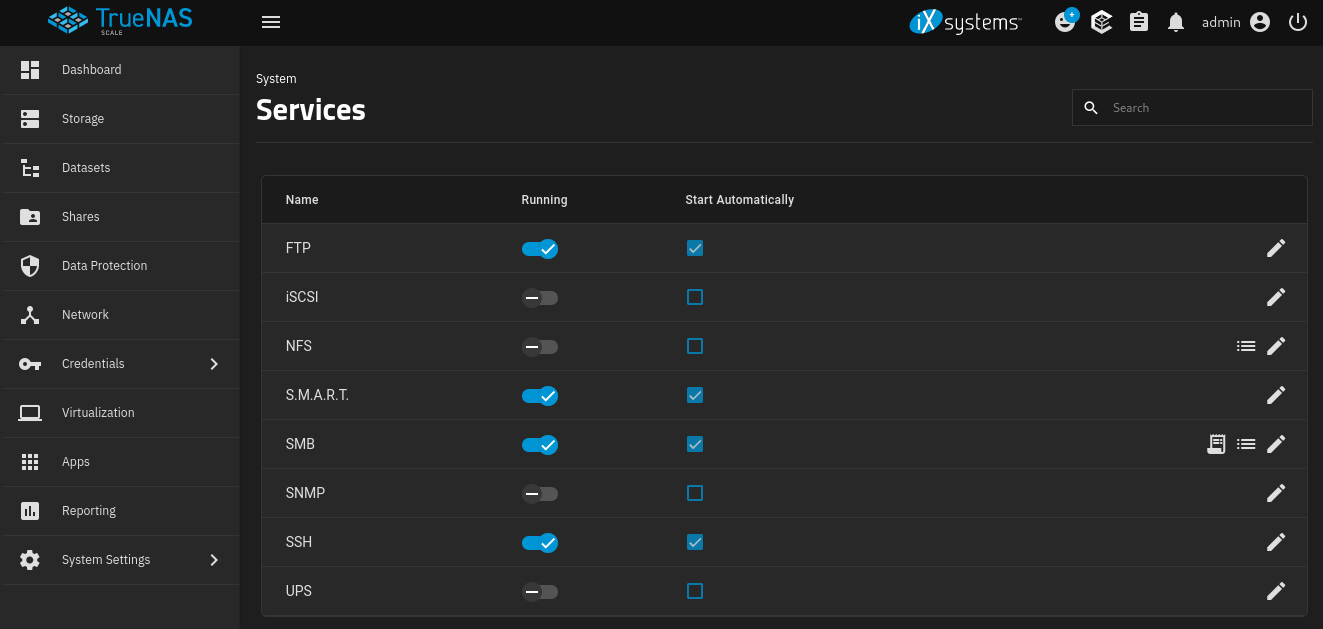
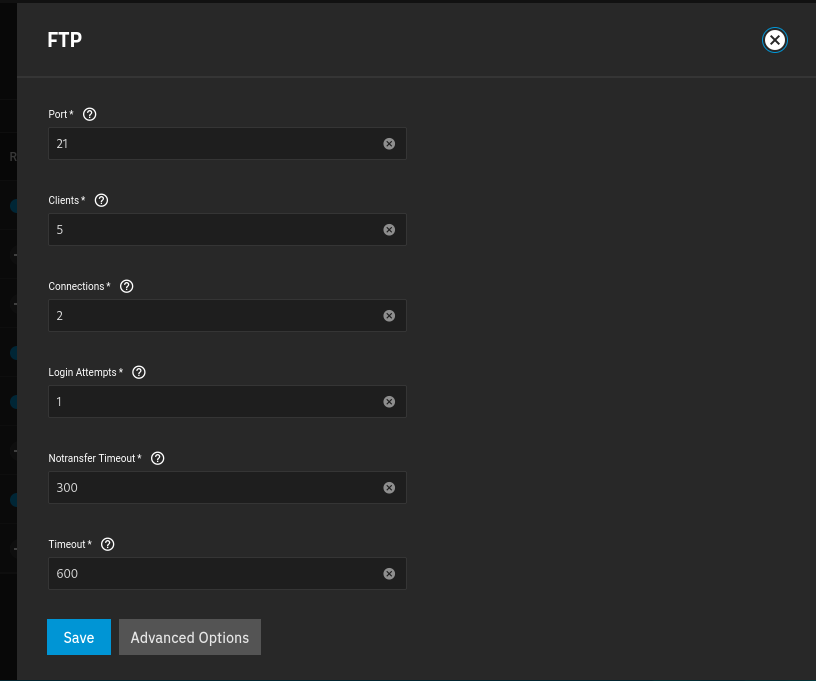
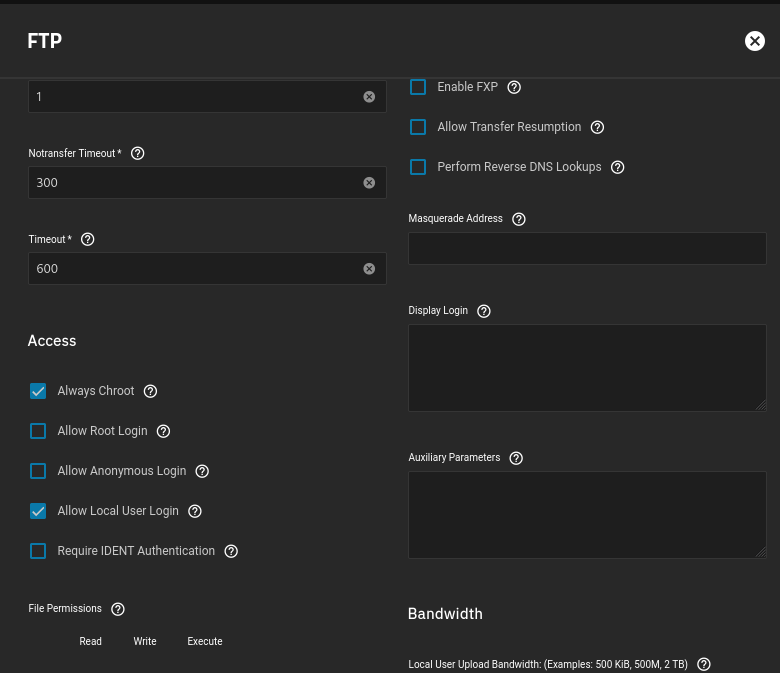
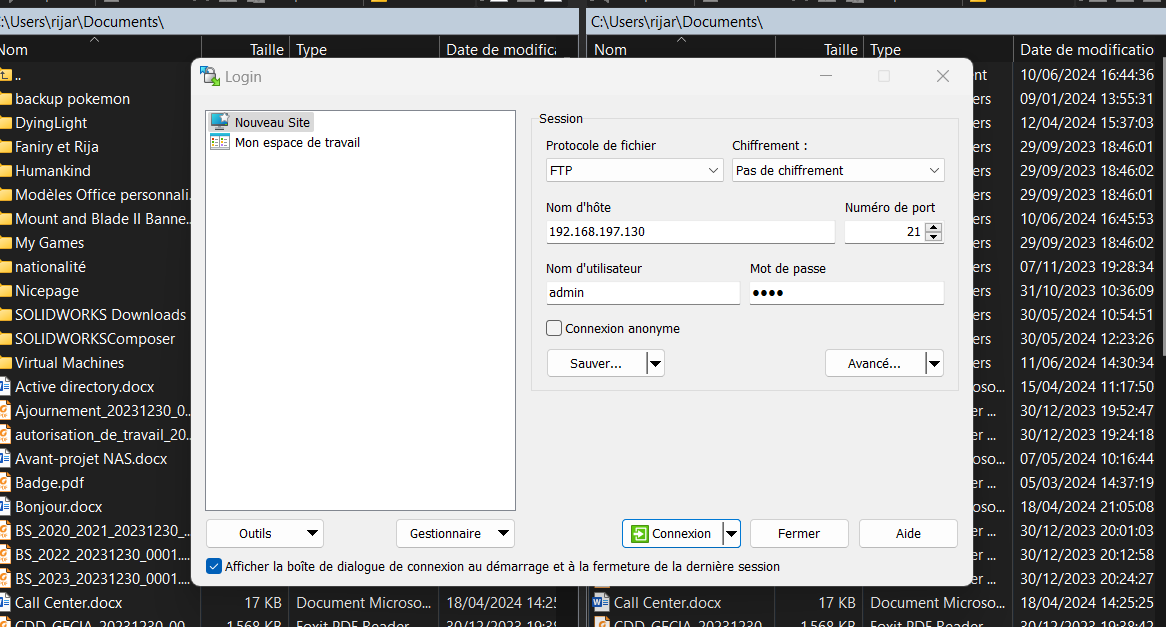
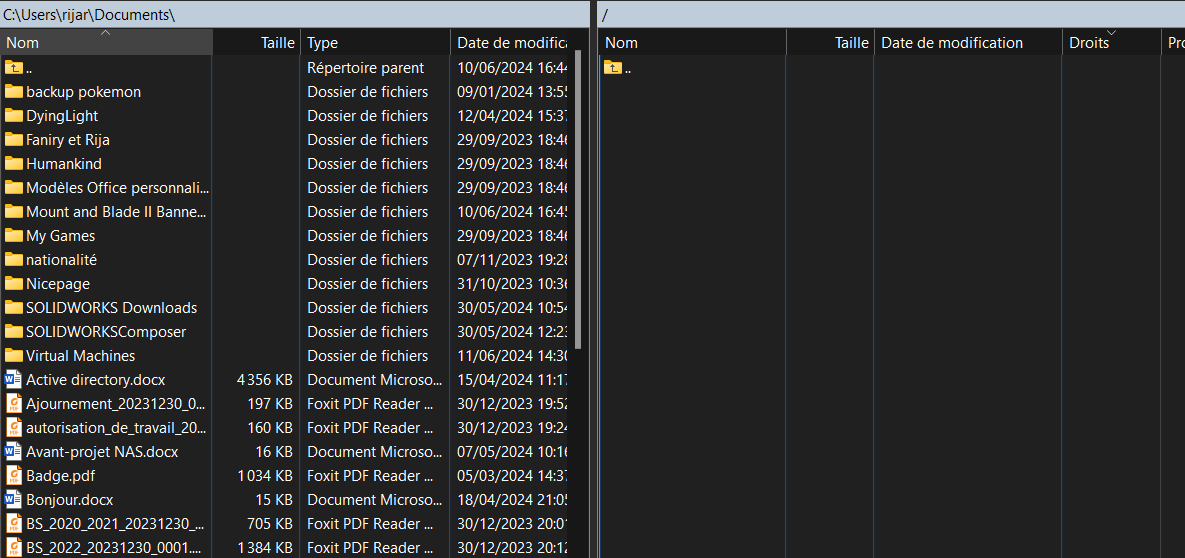


* On ajoute admin pour pouvoir se connecter au serveur en toute sécurité



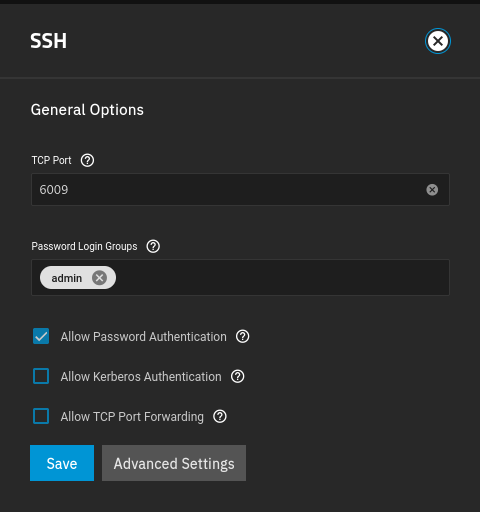
* Sur un terminal Windows, pour se connecter en SSH tape la commande ci-dessous et on rentre ensuite notre mot de passe:  
  

***Connexion en FTP***

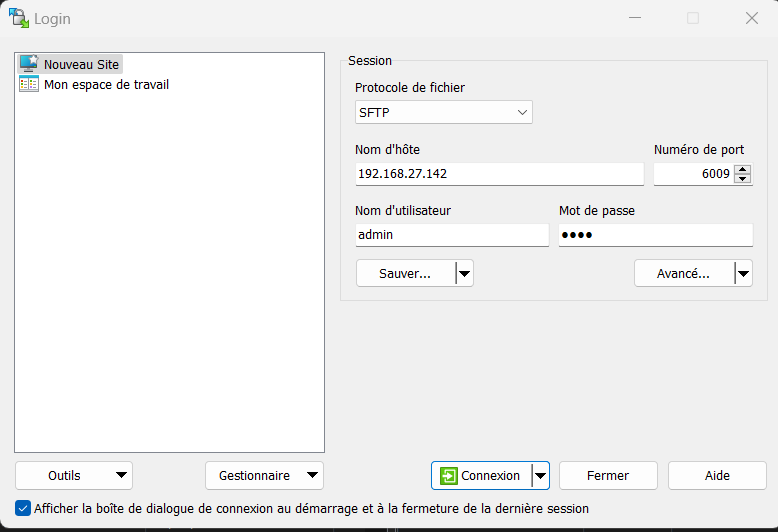
* Pour nous connecter en FTP, nous devons d’abord le configurer FTP en acceptant les utilisateurs local:  
  
* Une fenêtre s’ouvre, on clique sur “Advanced Options”:  
  
* On active ensuite “Allow Local User Login”  
  
* Pour tester la connexion en FTP, je me connecte via WinSCP:  
  
* Nous avons maintenant un FTP fonctionnel (a gauche le PC Windows et à droite TrueNAS):  
  

***Connexion en SFTP:***

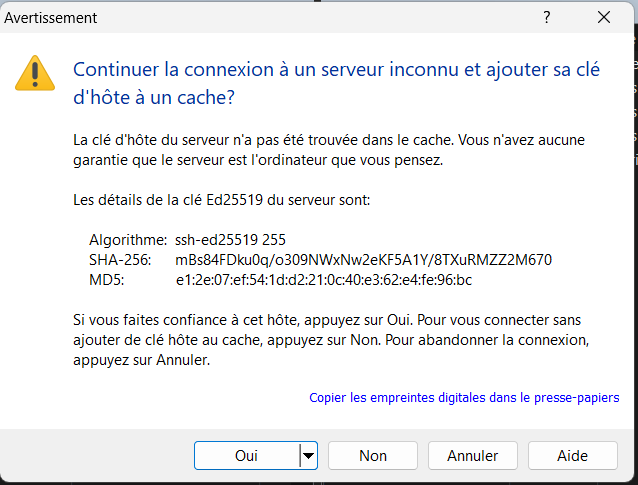
* Pour nous connecter en SFTP, il suffit de se rendre sur le service ssh pour changer le port 22 pour un autre port. On passe au port 22 qui est le port de base tcp sur un port dispo.



* On retourne sur WINSCP pour se connecter en “SFTP” on change le port 22 avec le port que l’on a choisi

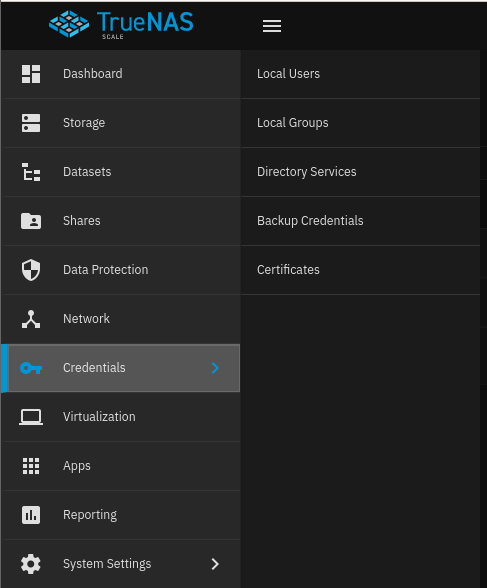


* Une fois la demande de connexion effectuée, le serveur crée un certificat d'authentification qui va nous permettre de nous connecter avec une connexion sécurisée.

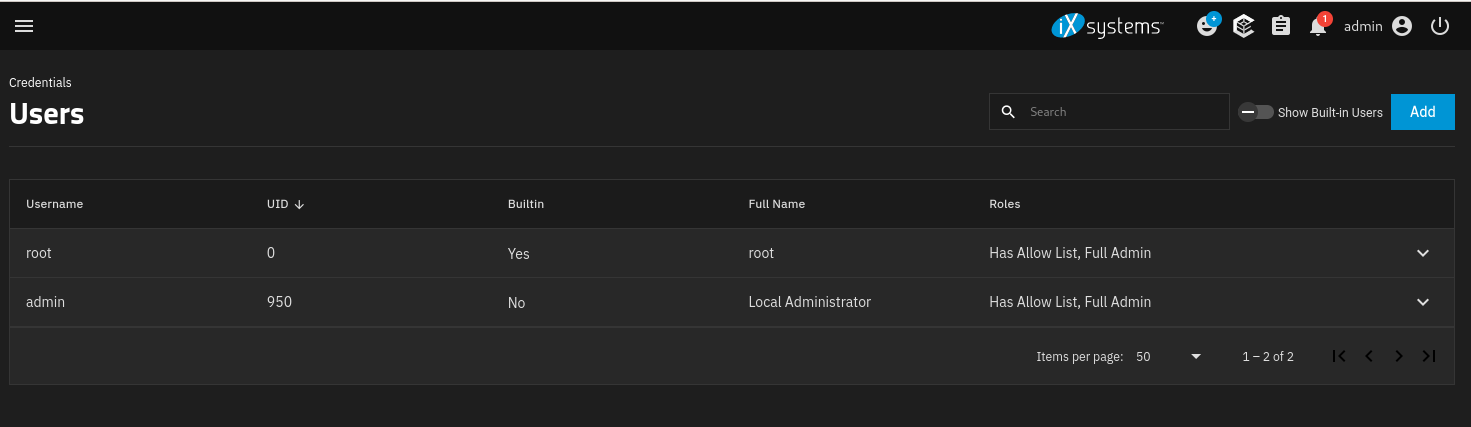


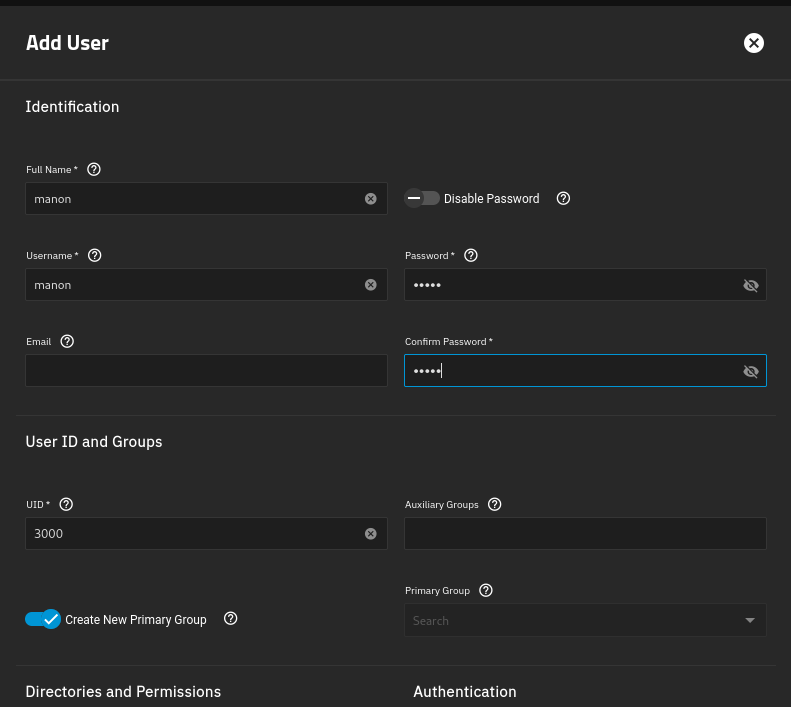


***Créer un utilisateur et une session sur TrueNas Scale***

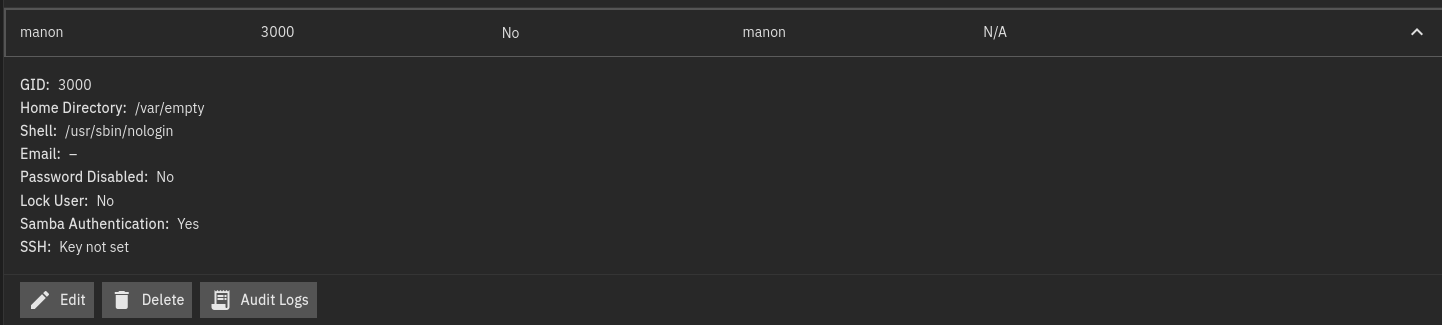
Pour ce faire, on se rend sur ***“CREDENTIALS”, “LOCAL USERS”*** 

Puis on clique ***“ADD”*** pour ajouter un utilisateur

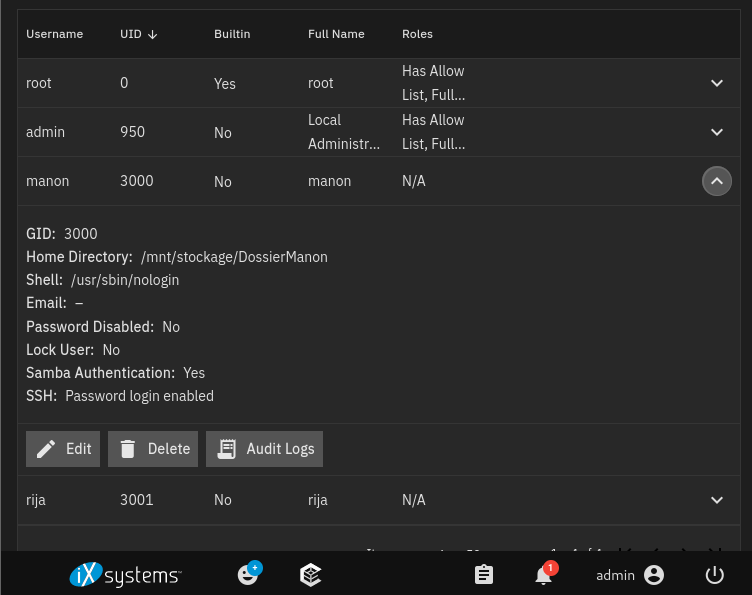




Voici l’utilisateur créer

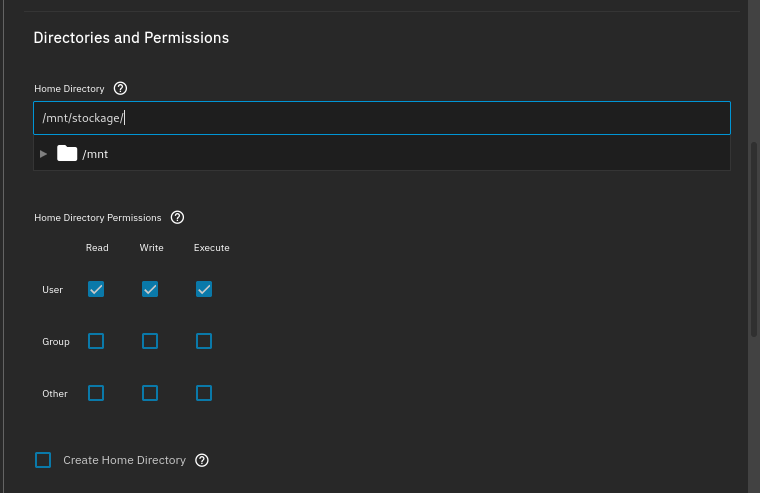


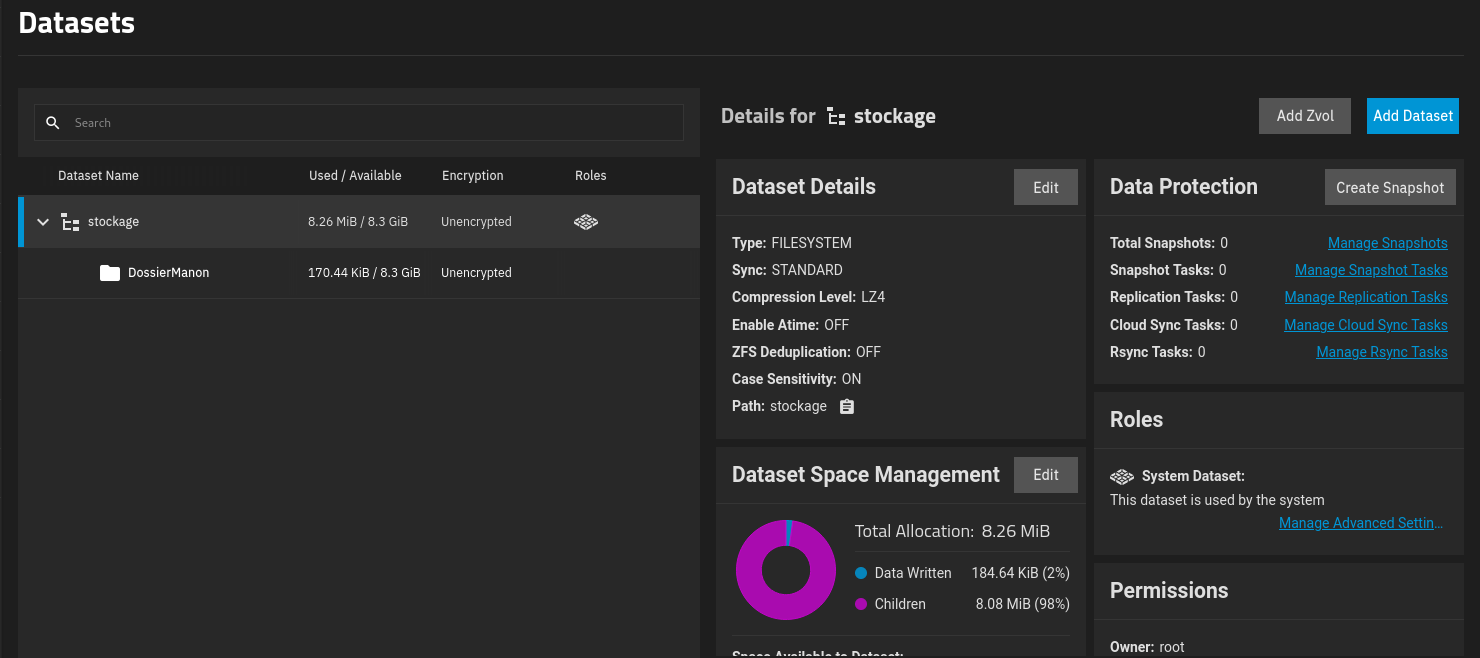
Créer un dossier privée et public avec les autorisations nécessaires pour chacun

on se rend dans ***“CREDENTIALS”, “LOCAL USERS”*** pour afficher nos utilisateurs puis nous rentrons dans **“*EDIT”*** de l’utilisateur choisi

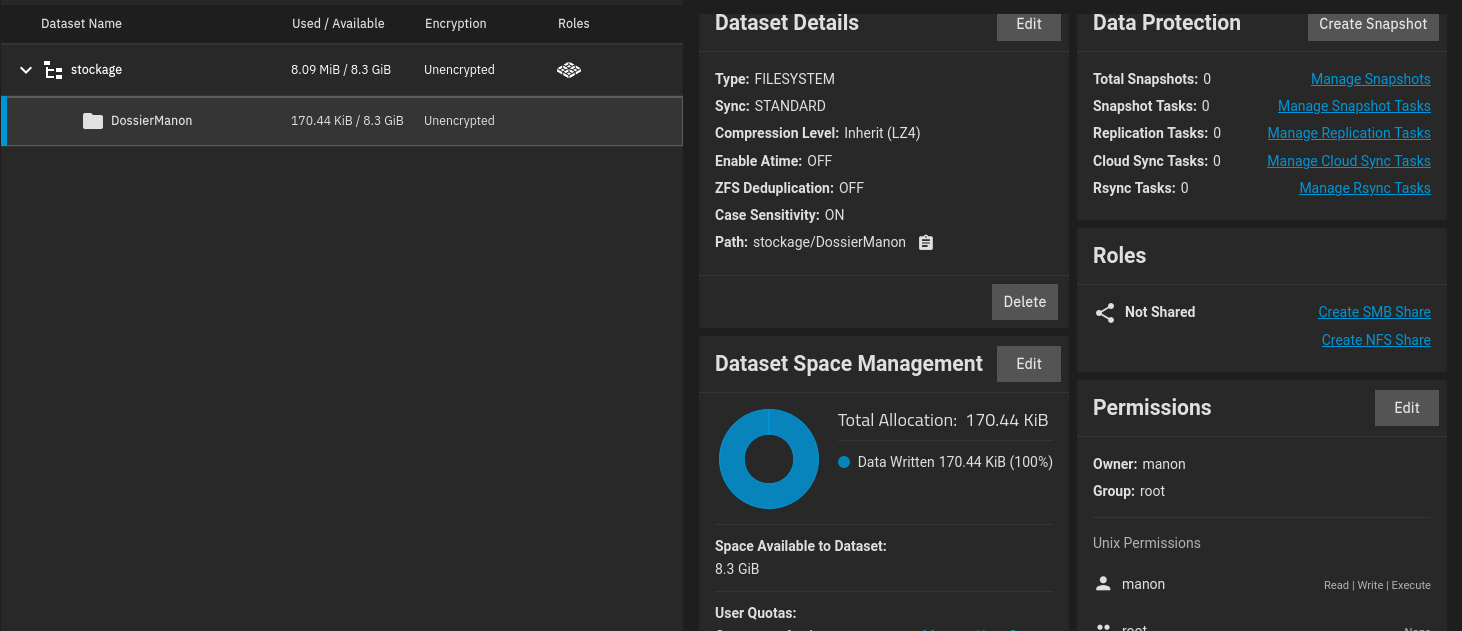


Une fois dans le profil de l’utilisateur, on va dans “DIRECTORIES” AND PERMISSIONS” pour mettre le bon chemin du répertoire ou se trouvera le dossier de Manon .



Maintenant on se rend sur ***“DATASETS”*** puis on va sur ***“ADD DATASET”*** pour ***créer le dossier privé*** de Manon.

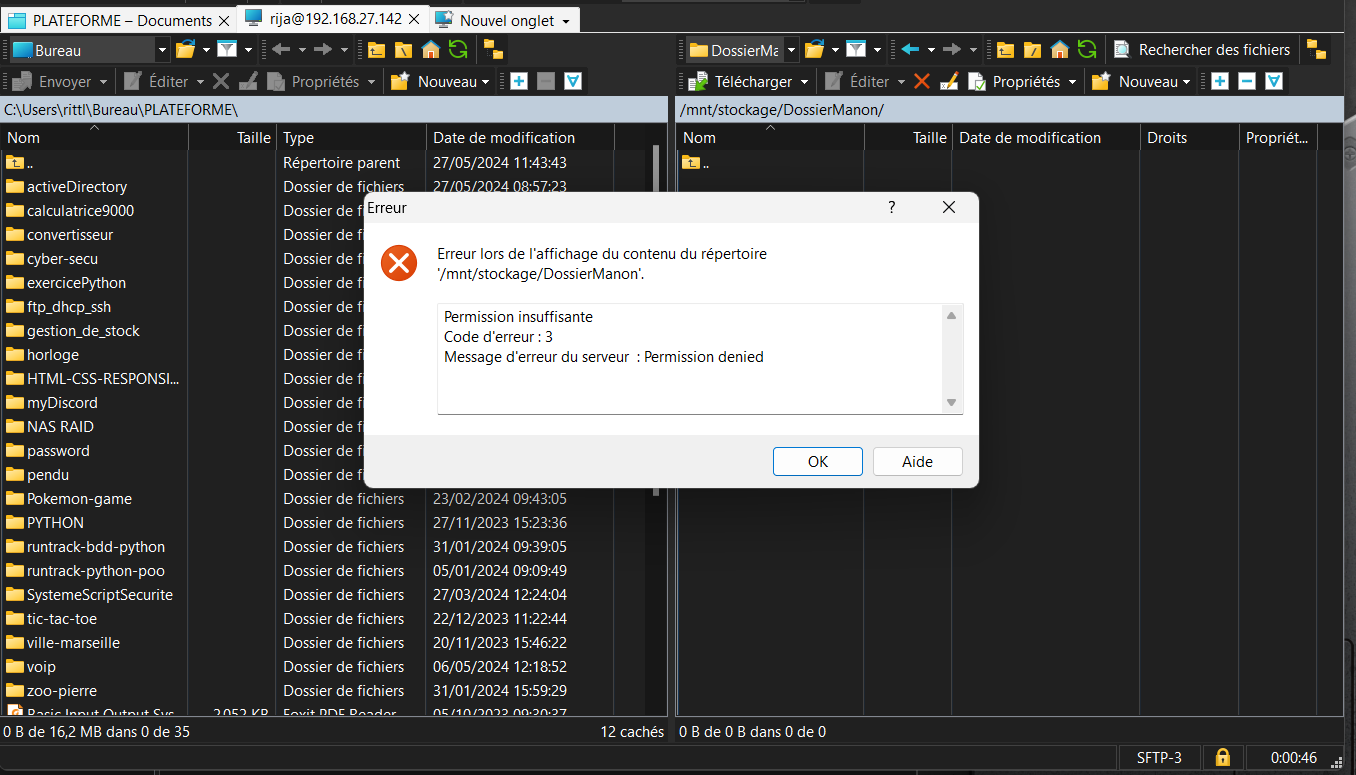
On vérifie le chemin et ajoute le nom du nouveau dossier

On se rend sur le Dossier fraichement créé, puis on va dans “EDIT” des permissions du dossier pour spécifier que seulement l’utilisateur “Manon” a droit d’avoir accès à ce dossier.

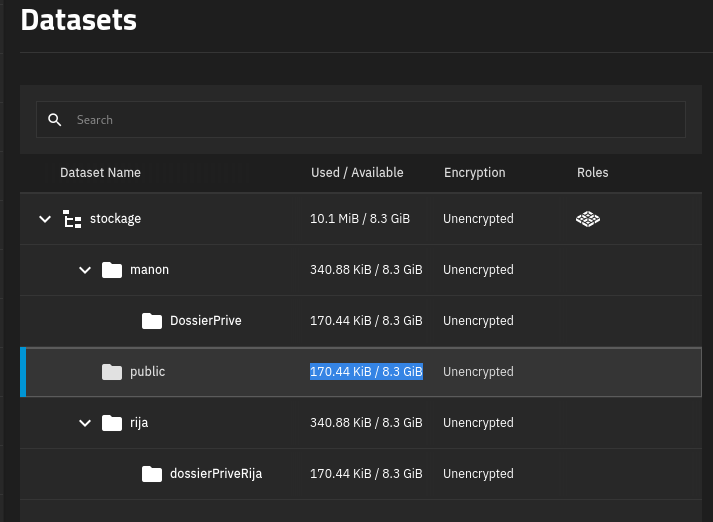


On peut voir que l’utilisateur “RIJA” ne peut pas se connecter au “dossierManon” qui est

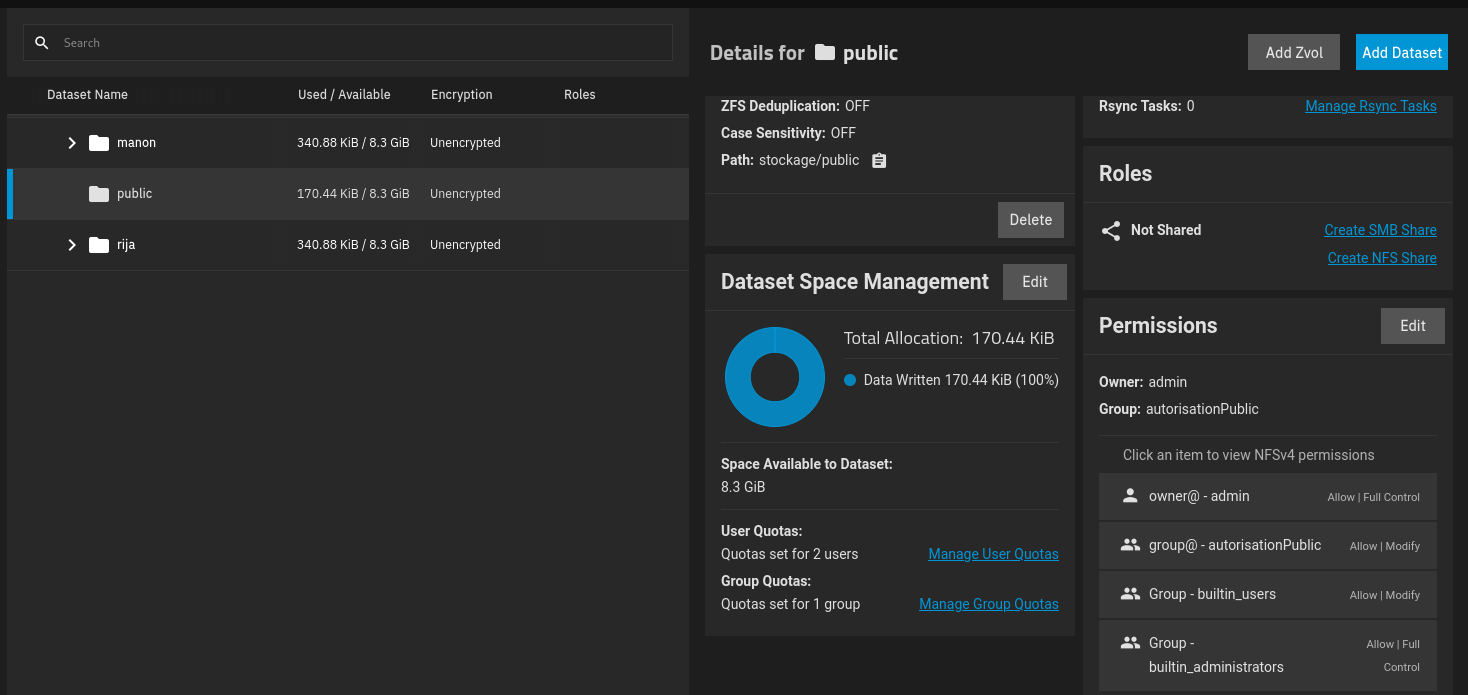
privé. Il est accessible seulement pour “MANON”



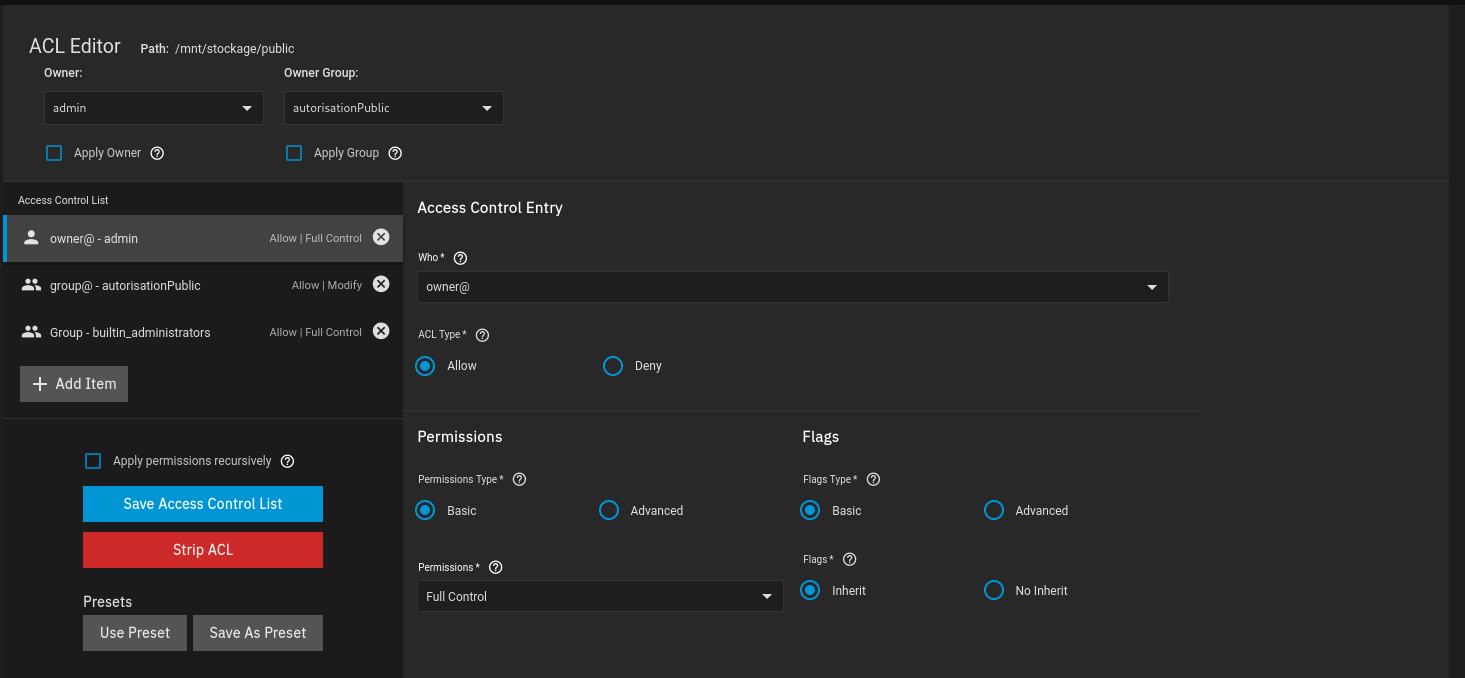
Configuration de la datasets, nous avons choisi de créer 2 dossier pour servant de home directory pour rija et manon dans lequel nous avons crée pour chacun leur dossier privé

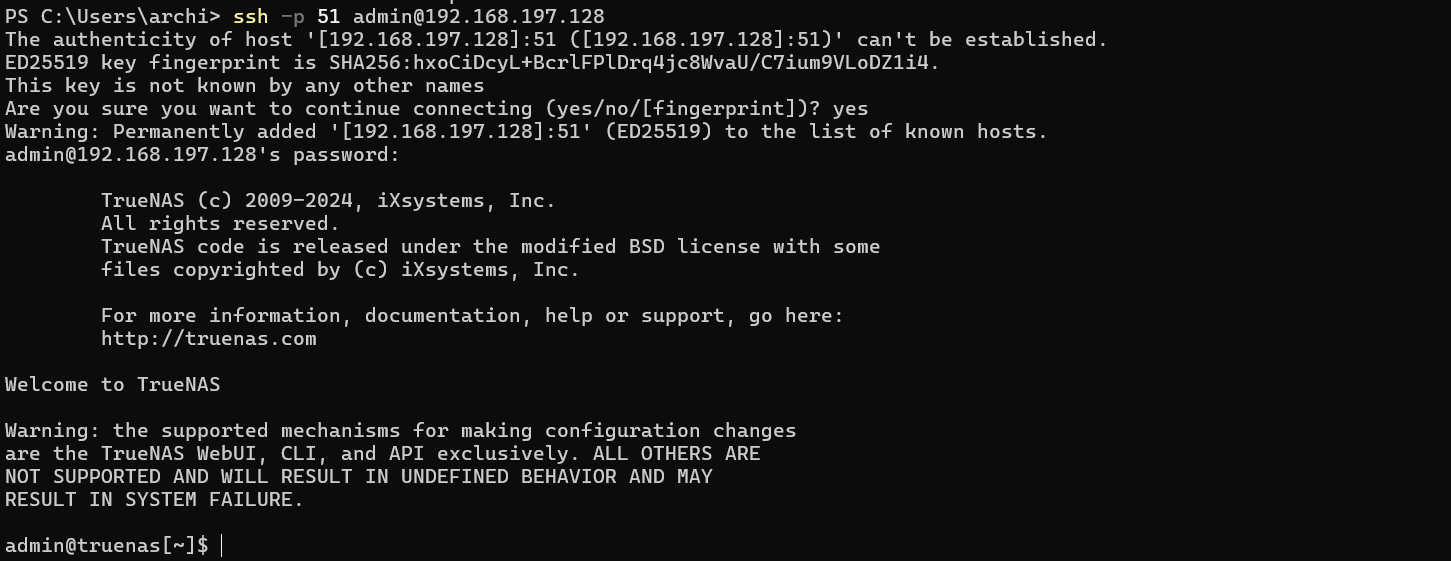


Pour ***le dossier PUBLIC*** on le crée puis on autorise le groupe ou se trouve rija et manon pour qu’il puisse y accéder, pour le faire on se rend dans “PERMISSIONS” de “public”



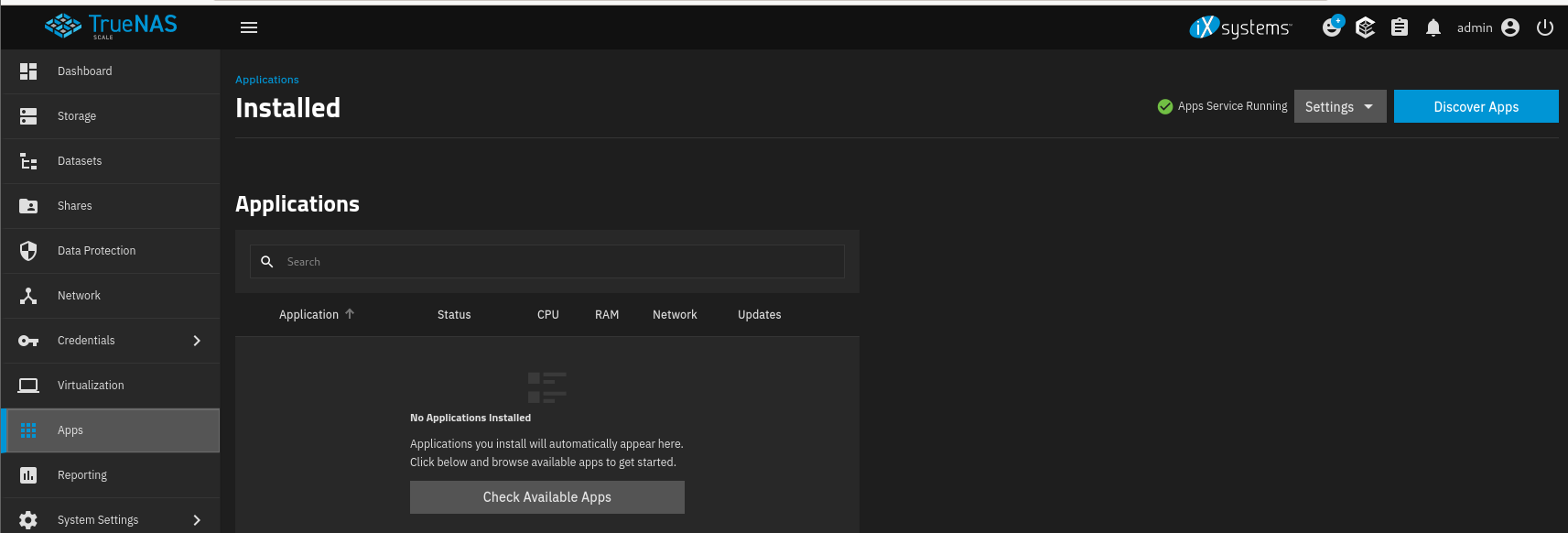
Une fois dans ACL editor pour gérer les autorisations, on autorise seulement **l’ admin et le groupe** dans lequel on mettra **tous les utilisateurs qui ont besoin d’avoir accès au dossier** ***“public”***



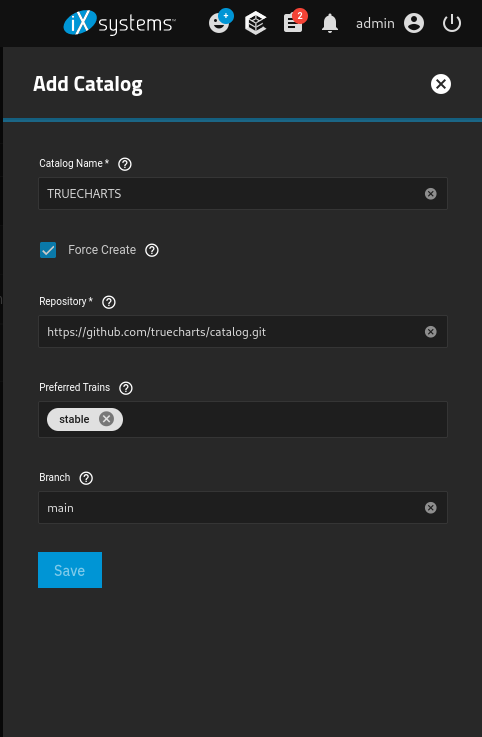
******

***Pour aller plus loin, installez des applications qui peuvent améliorer votre serveur NAS. Ajoutez le catalogue TRUECHARTS .***

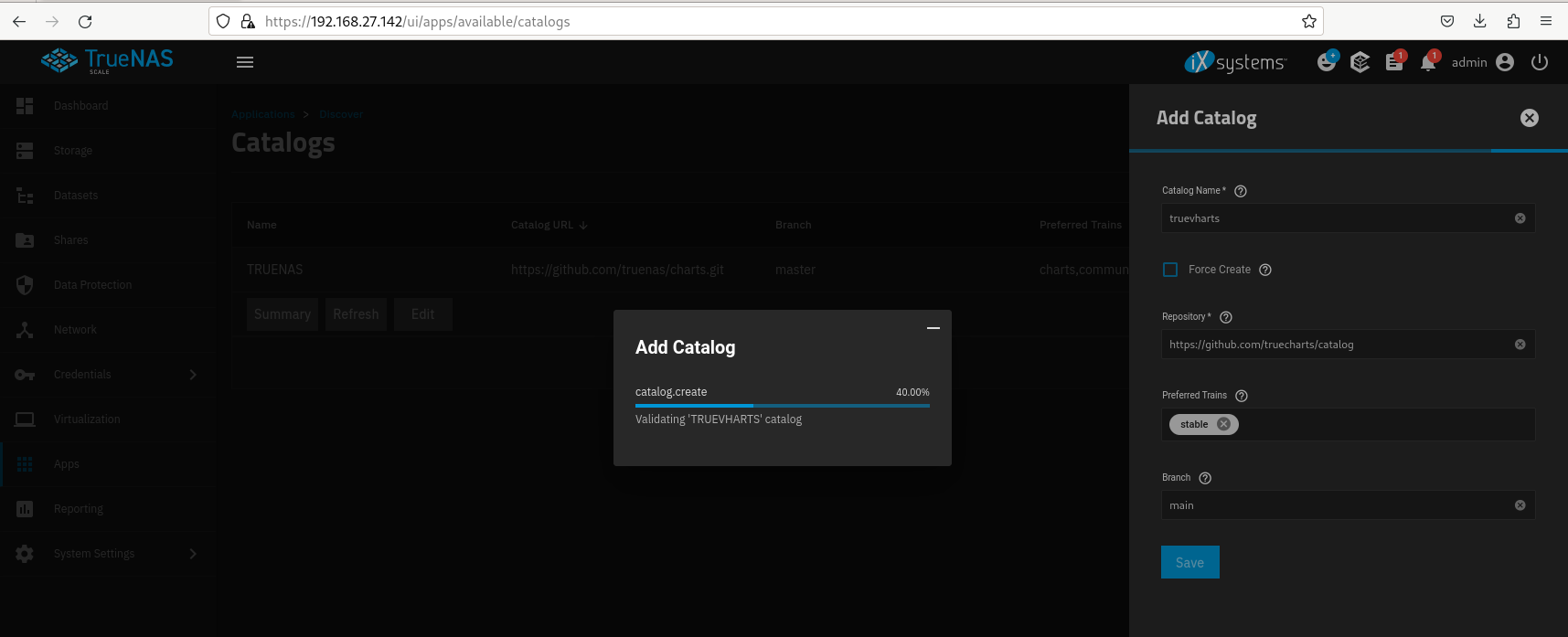
Pour ajouter le catalogue TRUECHARTS avec “<https://github.com/truecharts/catalog>” a TrueNas Scale.

On se rend dans l’onglet ***“APPS”*** si le service est en route on clique sur ***“discover apps”  
***

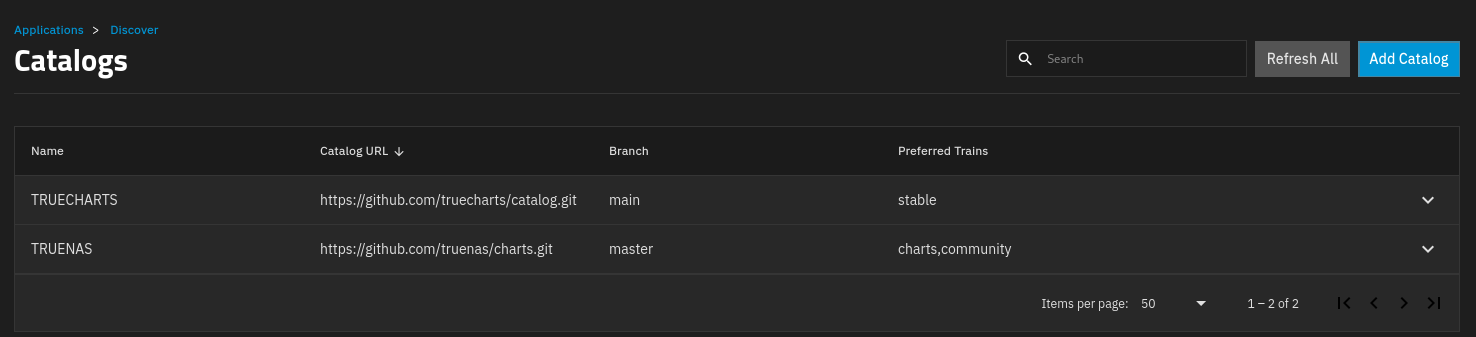
on copie l’url sans oublier le “.git” a la fin et coche la case “FORCE CREATE”



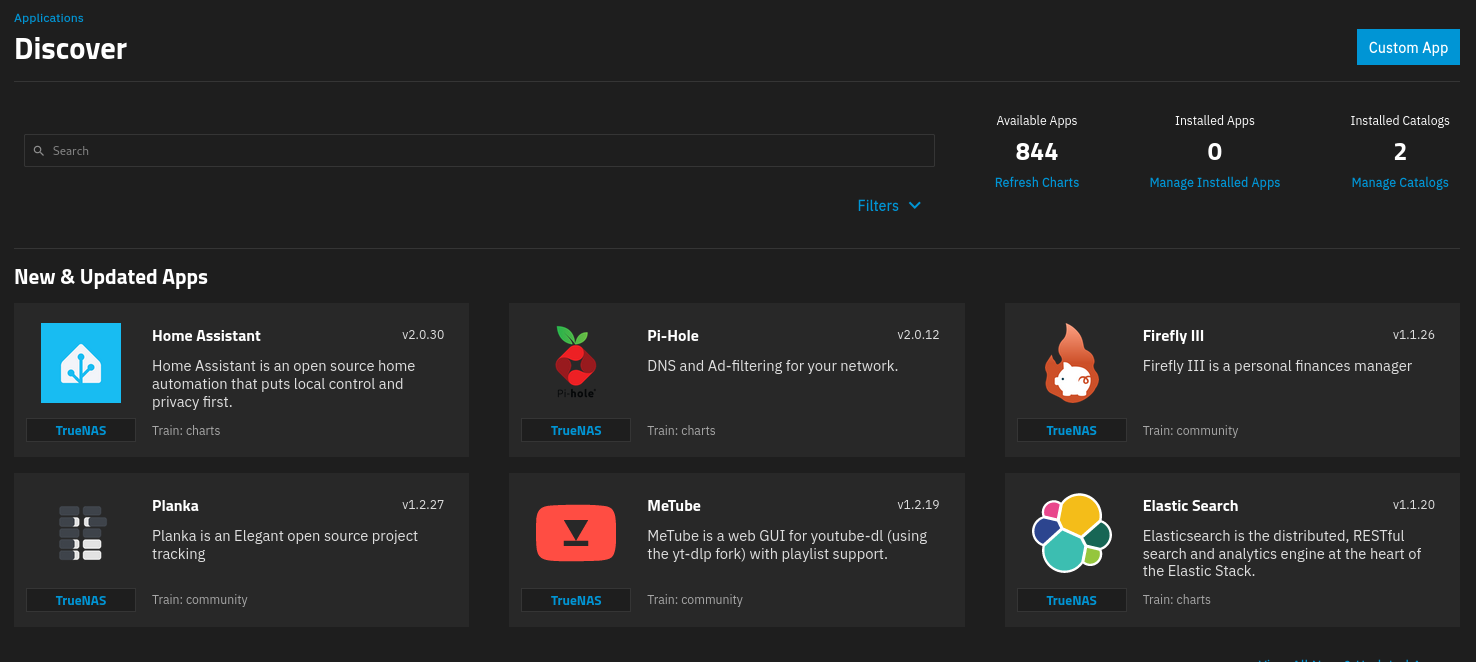
on copie l’url sans oublier le “.git” a la fin



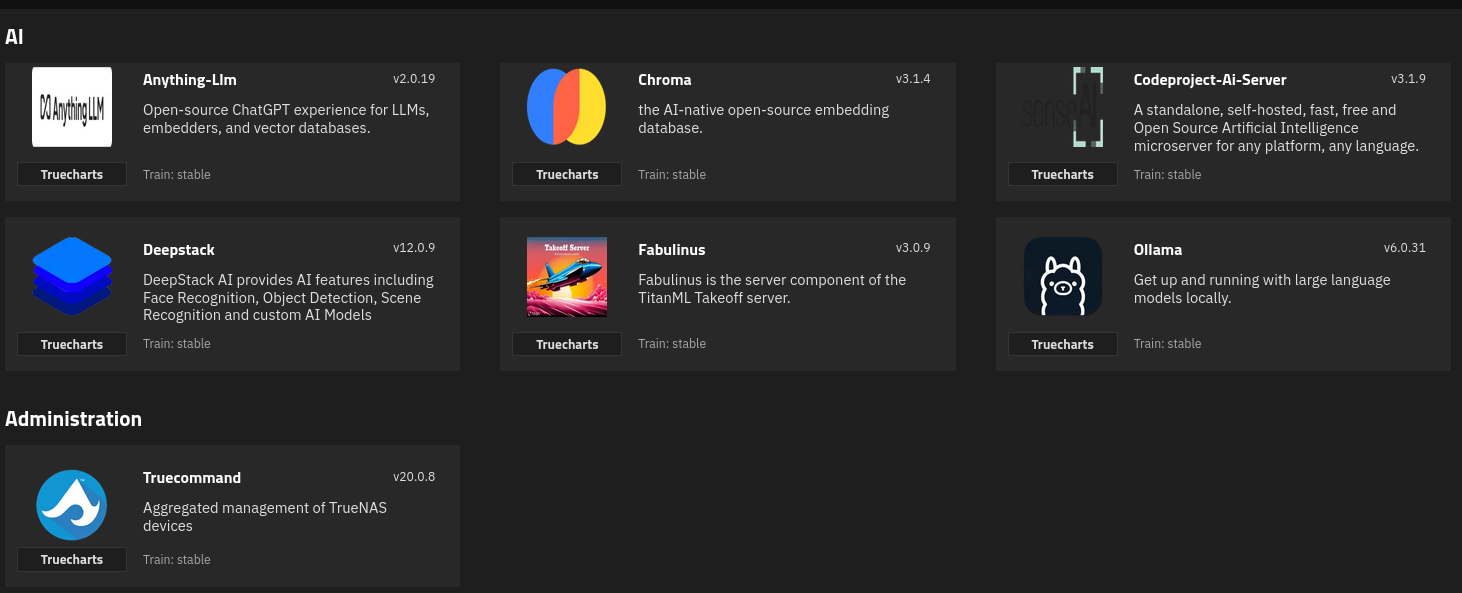
le catalogs est bien ajouté à notre TrueNas Scale



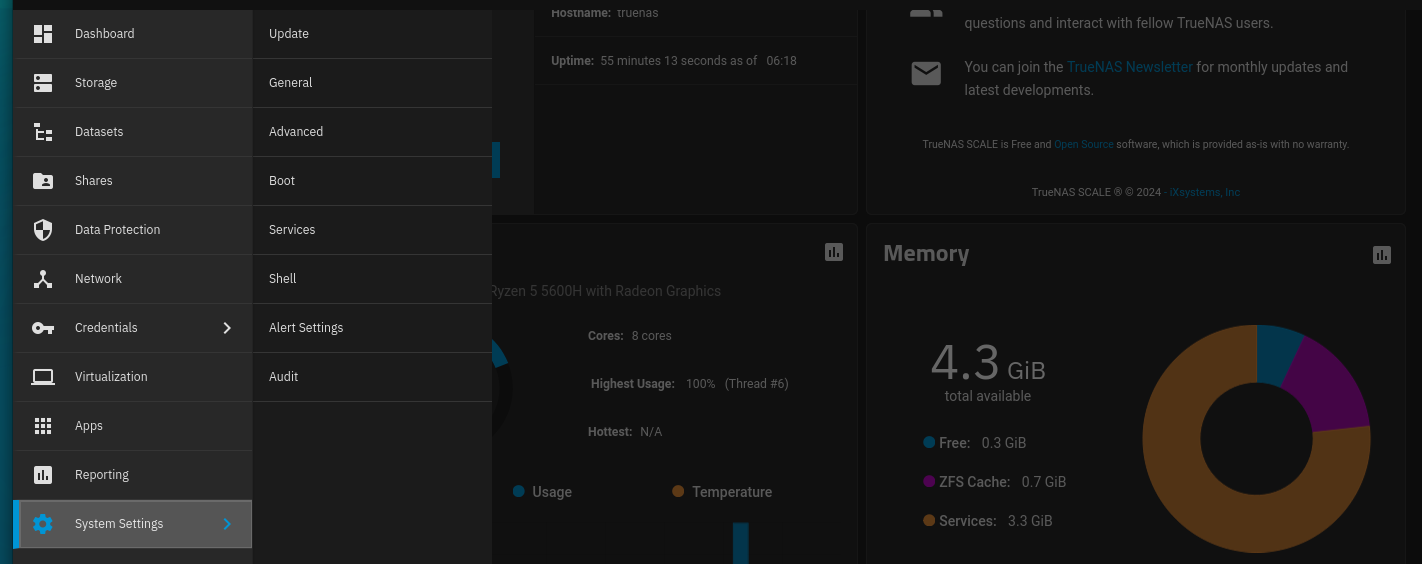
Quand on retourne sur “DIscover APPS” on peut clic sur refresh charts pour mettre le catalog a jour et on voir bien que le catalog “TRUECHARTS” est bien pris en compte

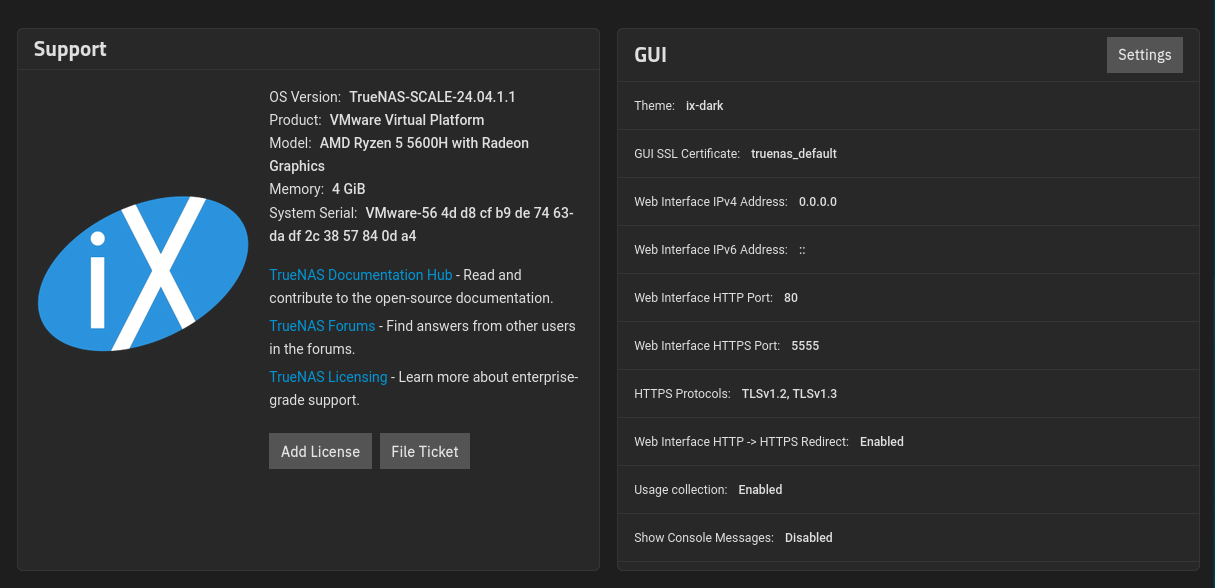


Voici quelques **applications “truecharts”** que nous pouvons télécharger maintenant

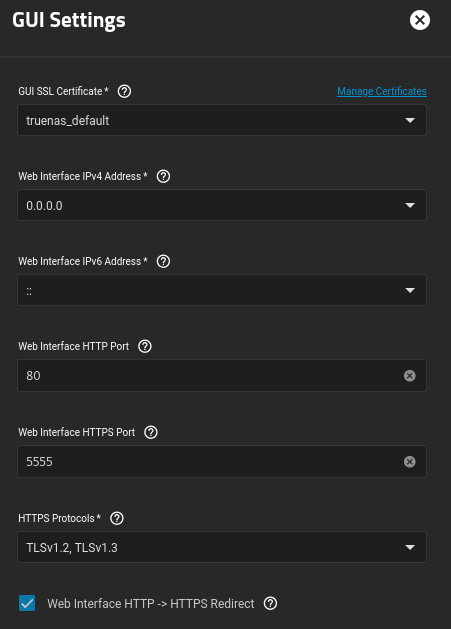
  
  
***Redirection automatique de ‘http’ vers ‘https’ et changement du port initial 443 en port 5555.***

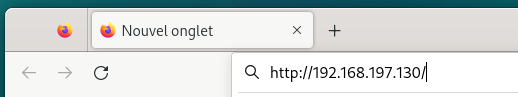
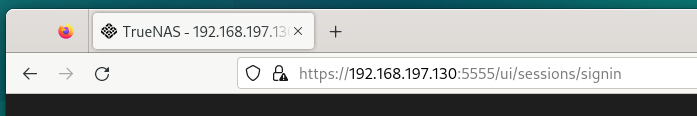
Aller dans l’onglet **System Settings -> General**



Dans la fenêtre “GUI”, cliquer sur **Settings**  


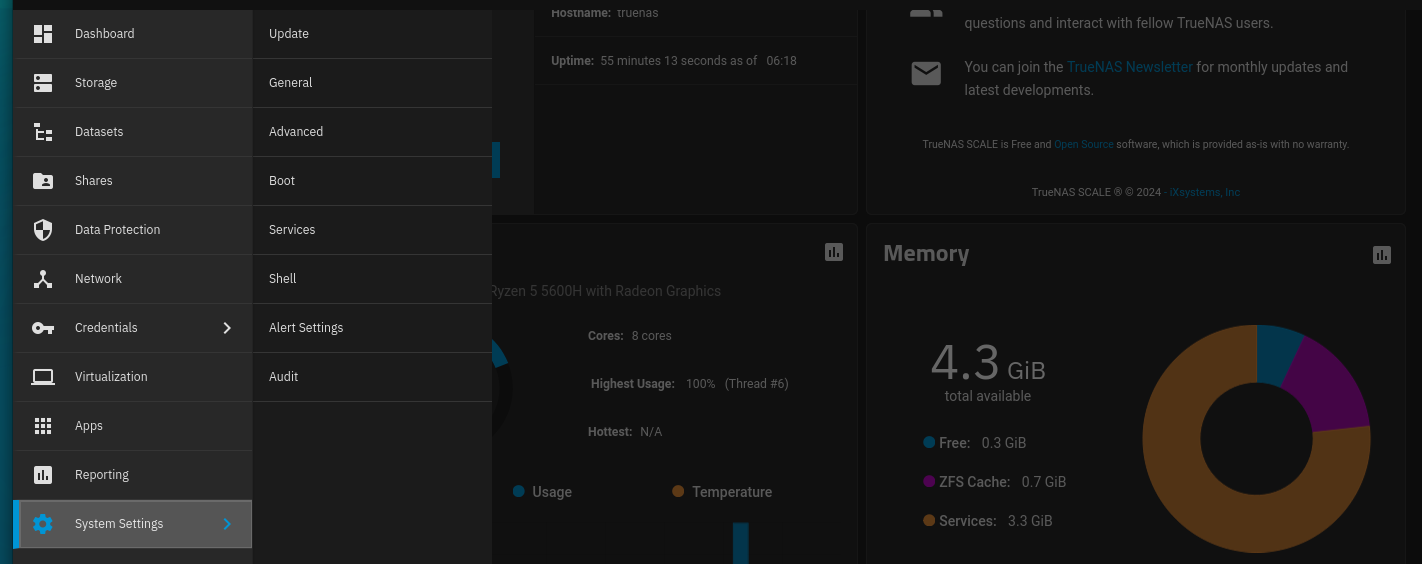
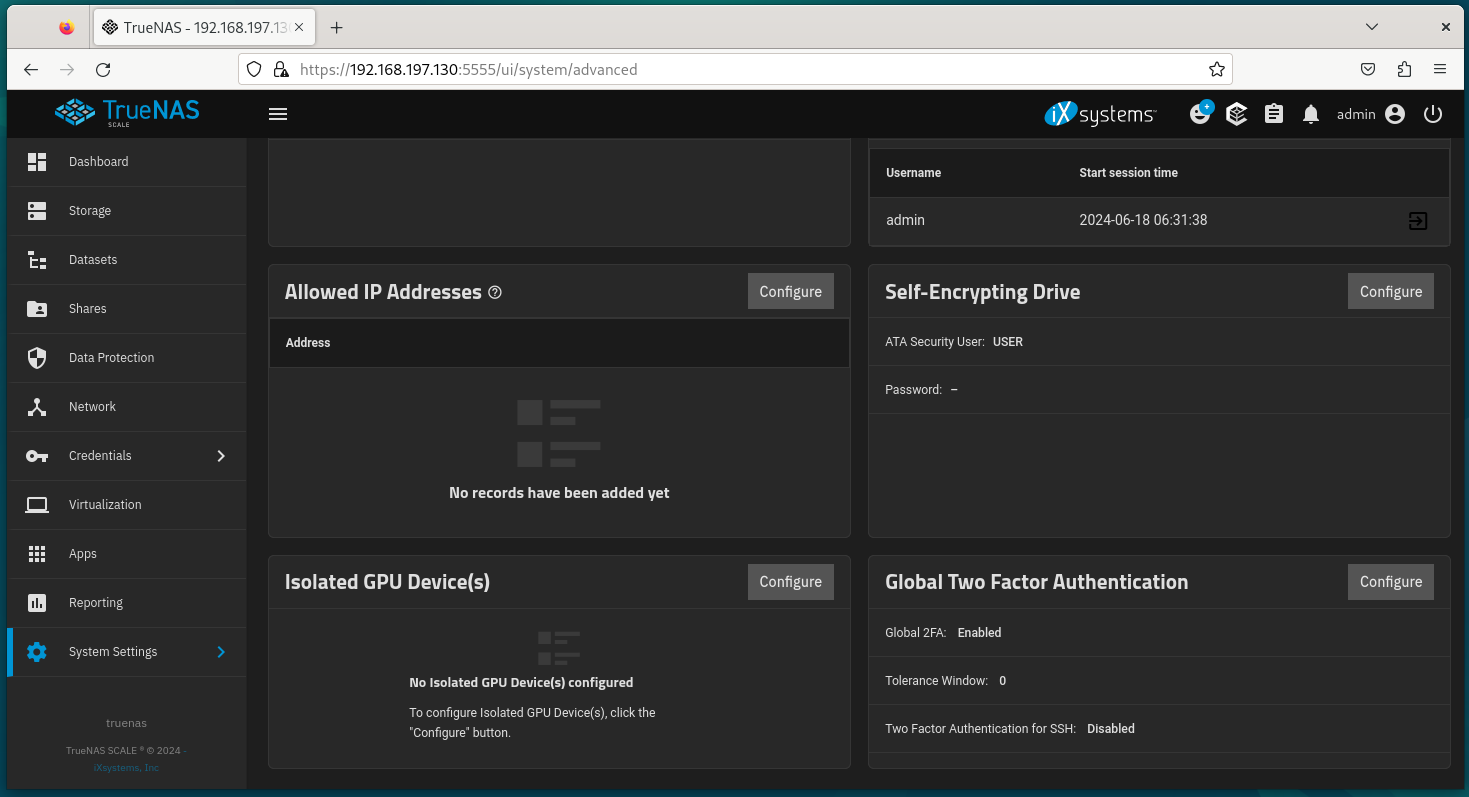
Modifiez le **“Web Interface HTTPS Port”** et mettez le port que vous voulez. Attention à ne pas mettre un port déjà utilisé par un autre service.  
Cochez ensuite **“Web Interface HTTP -> HTTPS Redirect”** qui va ensuite permettre la redirection automatique

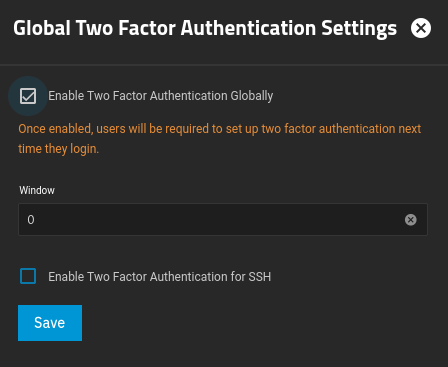
  
  
**Phase de test**

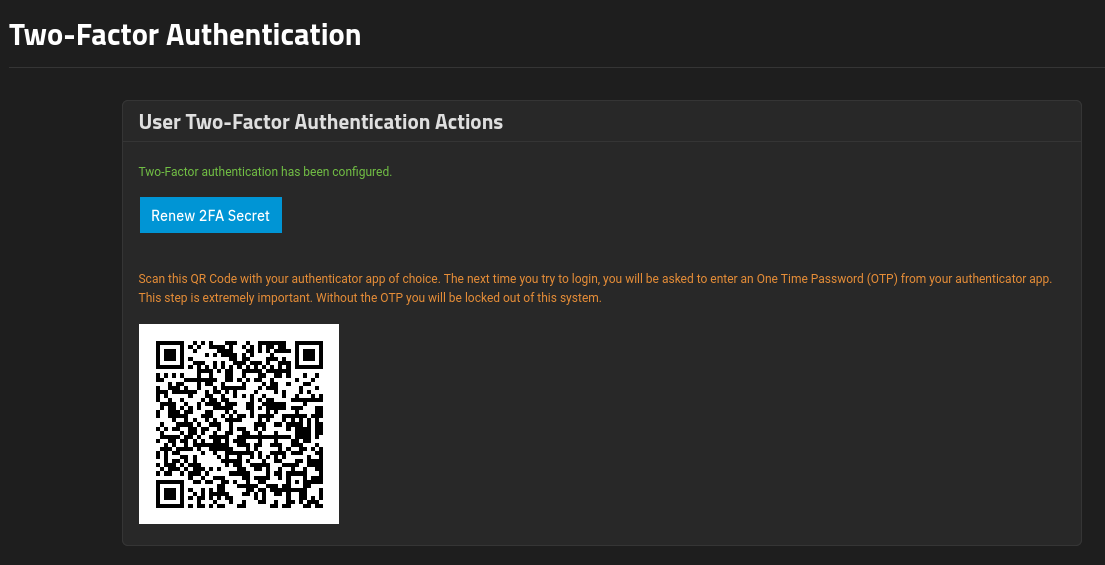
Sur le navigateur de, notre client on tape l’adresse en “http”  
  
  
On voit que TrueNAS a directement redirigé vers la connection ‘https’ sur le port 555:  


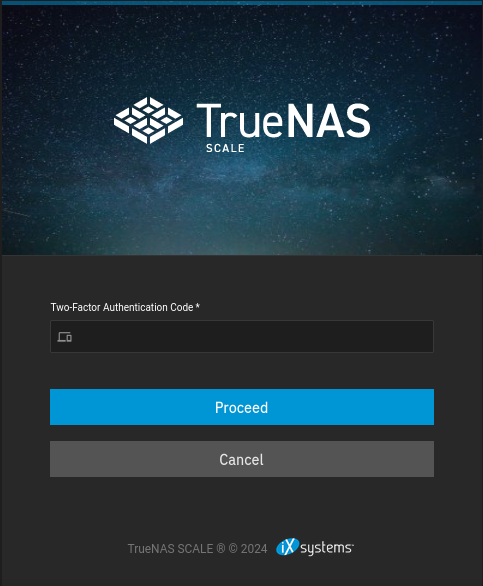
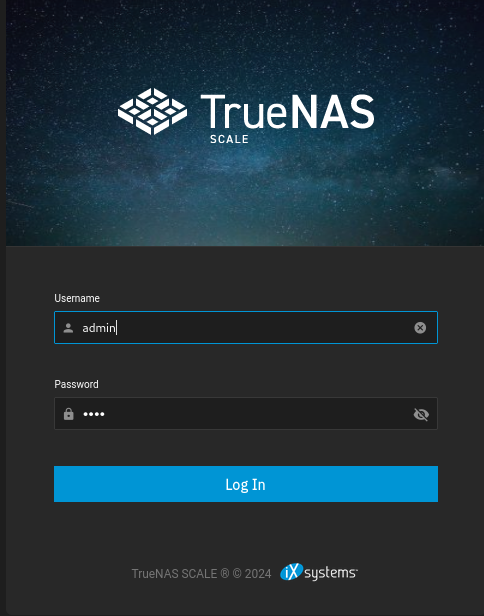
***Activation de l'authentification à deux facteurs.***

Aller dans l’onglet **System Settings -> Advanced**

  
  
Dans la fenêtre “Global Two Factor Authentication”, cliquer sur **Configure**  


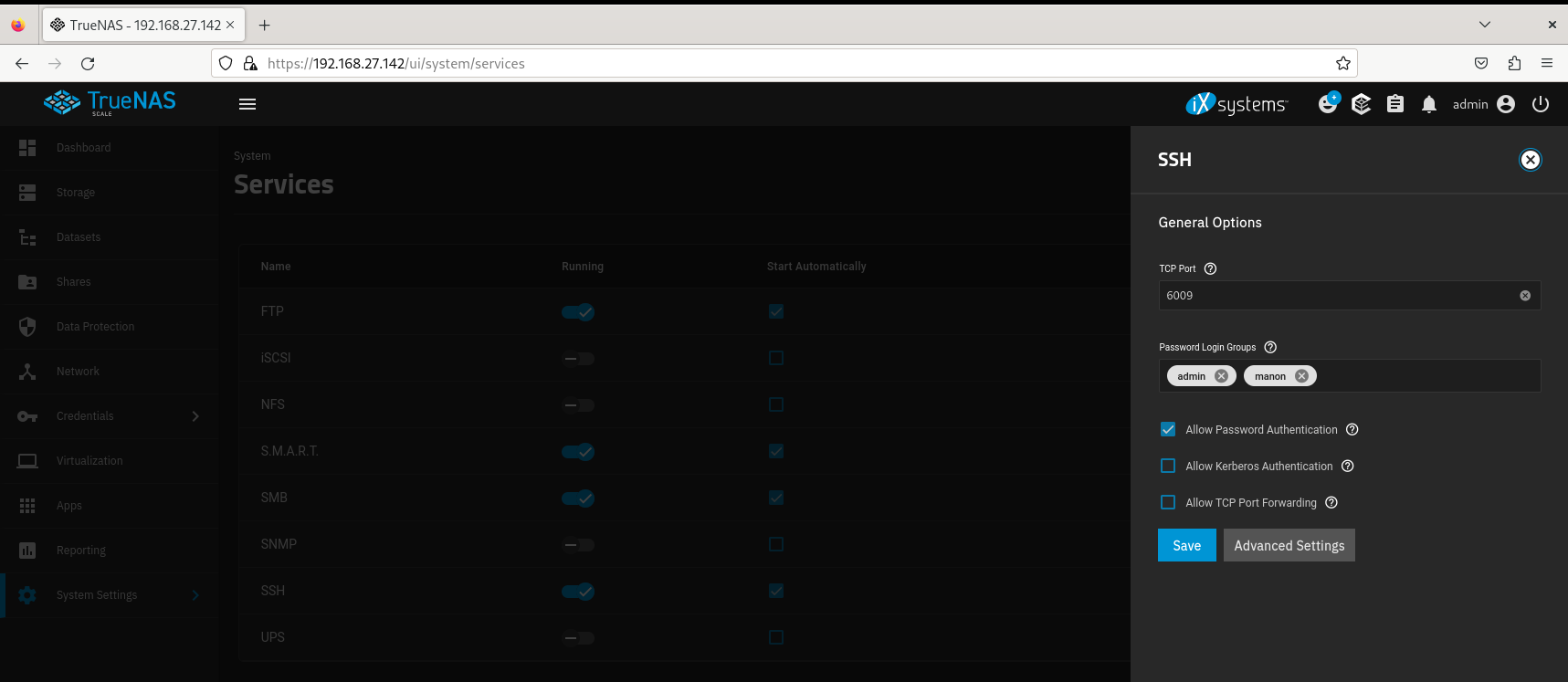
Cochez “Enable Two Factor Authentication Globally”, une fenêtre s’affiche, veuillez cliquer sur **accepter.**  


Cette fenêtre va apparaître:  
  
  
Il vous suffira de télécharger l'application **Google authenticator** et de scanner le QR code pour enregistrer l’authentification.

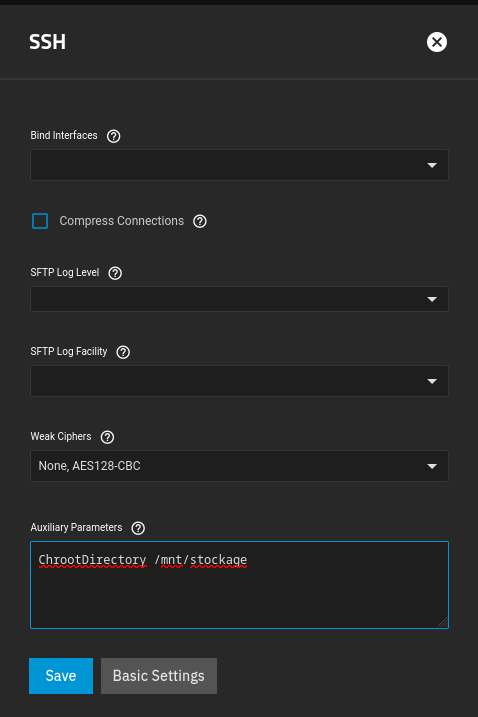
**Phase de test**On se connecte à TrueNAS. Une fenêtre va apparaître, il suffira de rentrer le code donner dans l’application Google Authenticator, puis cliquez sur ‘Proceed’:  


***DÉFINIR LA RACINE DE NOTRE NAS POUR SÉCURISER LA RACINE SYSTÈME***

Pour ce faire, on se rend dans l’onglet ***“ SYSTEME SETTING”, “SERVICE”*** puis on rentre dans le ***“EDIT”*** sur service ssh



On va sur “**ADVANCE SETTINGS**” puis on ajoute le nouveau chemin et le paramètre **ChrootDirectory**



LEXIQUE

*TrueNAS :*

C’ est un système d'exploitation sous licence libre, destiné aux serveurs de stockage en réseau (NAS). Il se décline en deux versions : TrueNAS CORE, basé sur FreeBSD, et TrueNAS SCALE, basé sur la distribution Linux Debian.

Voici ses principales caractéristiques et fonctionnalités:

* ***Support de protocoles***

*Il prend en charge plusieurs protocoles, tels que CIFS (Samba), FTP, NFS, rsync, AFP et iSCSI, et fournit également des rapports S.M.A.R.T. pour vous aider à surveiller l'état de vos disques durs.*

* ***Gestion des Utilisateurs et RAID Logiciel***

*une authentification des utilisateurs locaux et propose un RAID logiciel avec diverses options, en utilisant le système de fichiers ZFS pour assurer la redondance et la gestion efficace des données.*

* ***Interface Web***

*Utilise une interface web pour la configuration et la gestion, rendant l'administration accessible et intuitive.*

* ***Exigences et disponibilité***

*Il faut minimum 8 Go d'espace de stockage pour son installation, qui peut se faire sur un disque dur ou une clé USB. Il est disponible sous deux formats : image ISO et code source, afin de répondre aux besoins et préférences de chaque utilisateur.*

***TrueNAS SCALE:***

*C’ est une version de TrueNAS, un système d'exploitation sous licence libre conçu pour les serveurs de stockage en réseau (NAS). Il est basé sur la distribution Linux Debian. Il offre des fonctionnalités avancées de gestion de données, de virtualisation et de conteneurisation.*

*TrueNAS SCALE est une solution complète et flexible pour le stockage en réseau, offrant des fonctionnalités avancées de gestion des données et de virtualisation. Sa base Linux Debian, combinée à OpenZFS, KVM, Qemu, Kubernetes et Docker, en fait un choix puissant pour les environnements nécessitant une infrastructure de stockage robuste et évolutive.*

*Voici ses fonctionnalités spécifiques:*

* ***Gestion des VM et Conteneurs***

*Il supporte la gestion des machines virtuelles (VM) via l'interface web, en utilisant Kernel-based Virtual Machine (KVM) et Qemu. Il permet la gestion des conteneurs avec Kubernetes et Docker.*

* ***Système de Fichiers OpenZFS***

*Il utilise OpenZFS pour le support avancé de ZFS, offrant des fonctionnalités telles que la compression, les snapshots et la protection contre la corruption de données.*

***TrueNAS Core:***

*C’ est une solution complète et fiable pour le stockage en réseau, offrant des fonctionnalités avancées de gestion des données grâce à sa base FreeBSD et à l'utilisation du système de fichiers ZFS. Il est idéal pour les utilisateurs et les entreprises recherchant une solution de NAS éprouvée et robuste, avec une interface web intuitive pour une gestion facile et une prise en charge complète des protocoles de partage de fichiers.*

* ***Support de protocoles***

*Il prend en charge plusieurs protocoles, tels que CIFS (Samba), FTP, NFS, rsync, AFP et iSCSI et fournit également des rapports S.M.A.R.T. pour vous aider à surveiller l'état de vos disques durs.*

* ***Gestion des Utilisateurs et RAID Logiciel***

*Il permet l'authentification des utilisateurs locaux et utilise le RAID logiciel avec plusieurs variantes, en s'appuyant sur ZFS pour la redondance et la gestion avancée du système de fichiers.*

### **Add Dataset : Fonctionnement :**

* Comparable à un dossier dans un système de fichiers traditionnel, permet d'organiser et de gérer des fichiers et des répertoires de manière hiérarchique.

**Utilisation principale :**

* **Organisation des données :** Idéal pour structurer les données en groupes logiques comme les documents d'entreprise, les médias, etc.
* **Partages de fichiers :** Utilisé pour créer des partages de fichiers via SMB ou NFS, adapté aux besoins de collaboration.
* **Sauvegardes :** Supporte la création de snapshots pour sauvegarder et récupérer les données en cas de besoin.

**Propriétés configurables :**

* Permet de définir les **permissions d'accès**, les **quotas**, la **compression des données**, etc.

### **Add Zvol (Volume basé sur bloc) : Fonctionnement :**

* Volume de stockage basé sur blocs, similaire à un disque dur virtuel, offre un accès direct aux blocs de données.

**Utilisation principale :**

* **Stockage pour machines virtuelles (VMs) :** Utilisé pour stocker les disques des machines virtuelles, offrant des performances élevées et un accès direct aux données.
* **Bases de données :** Adapté aux applications nécessitant un accès direct et bas niveau aux blocs de données pour optimiser les performances.
* **Stockage basé sur blocs :** Idéal pour les environnements où la gestion fine des blocs de données est cruciale.

**Paramètres configurables :**

* Permet de spécifier la **taille du volume**, le **type de provisionnement** (thin ou thick), et d'autres **options avancées** de configuration du stockage.

***ACL EDITOR:***

Le **ACL (Access Control List) Editor sur TrueNAS SCALE** est **un outil graphique qui permet de gérer de manière précise les permissions d'accès aux datasets et fichiers**. Il permet d'ajouter des entrées spécifiant des permissions (lecture, écriture, exécution) pour des utilisateurs ou des groupes, et de définir des règles d'héritage pour ces permissions. Avec des options avancées, il offre un contrôle fin des autorisations, idéal pour sécuriser et organiser l'accès aux données dans un environnement NAS.

***CHROOT:***Un **"chroot"** (change root) est une opération utilisée sur les systèmes Unix et Linux pour modifier le répertoire racine apparent d'un processus et de ses enfants, créant ainsi un environnement isolé appelé "chroot jail". Voici les points clés :

* **Sécurité** : Limite les dommages potentiels en cas de compromission en confinant les processus dans un environnement restreint.
* **Test et Développement** : Permet de tester des applications dans des environnements isolés sans affecter le système principal.
* **Récupération Système** : Utilisé pour accéder et réparer un système de fichiers d'un autre système sans redémarrer la machine.