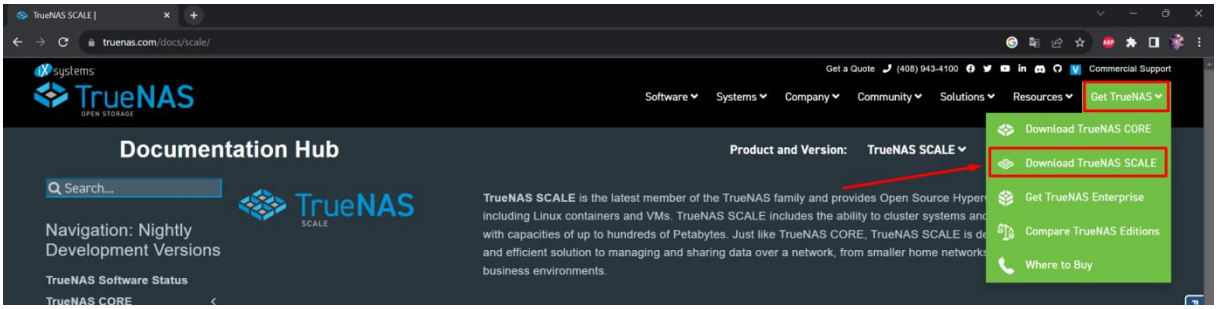
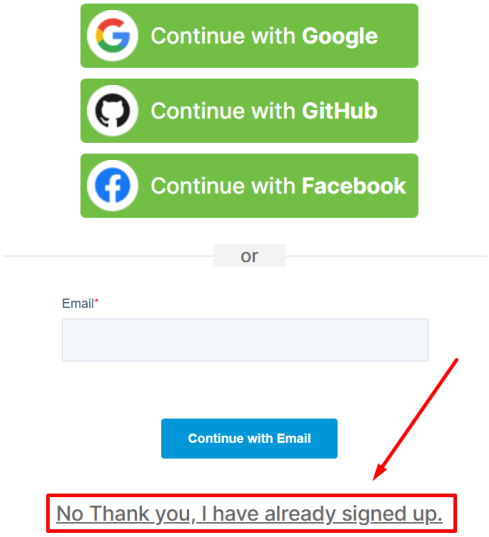
I. Installation et configuration de TrueNAS

A. Installation de TrueNAS

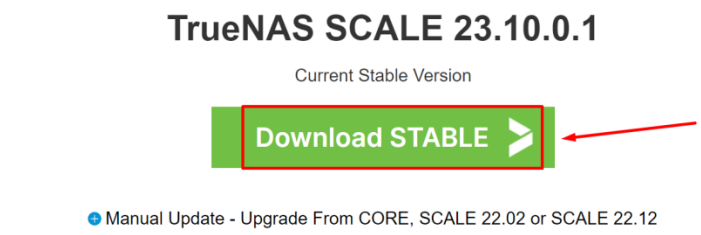
Etape 1 : Tout d'abord, on va aller sur le site officiel de True NAS, puis en haut à droite, on clique sur « Get TrueNAS » puis dans le menu déroulant, on clique sur « Download TrueNAS SCALE ».



Une nouvelle page va s'ouvrir pour vous demander de vous créer un compte. On clique sur « No Thank you… ». Cela nous ramènera sur la page d'installation.



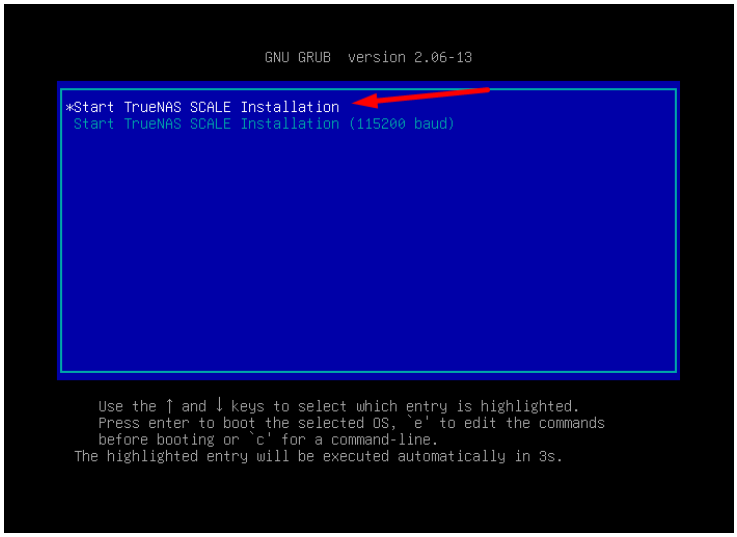
Etape 2 : Nous cliquons enfin sur « Download STABLE »



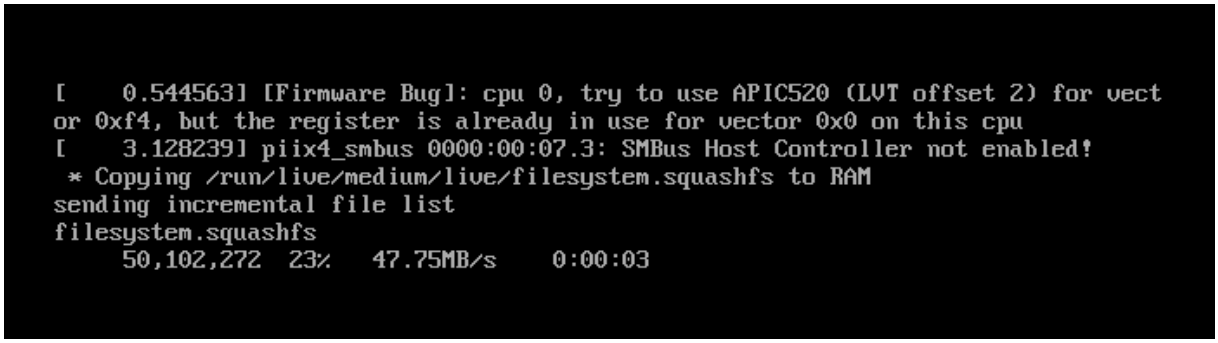
Une fois l'ISO installé. Nous pouvons créer notre vm et booter dessus.

Attention, il est recommandé d'avoir au moins 8Go de RAM sur la vm pour le bon fonctionnement de celui-ci.

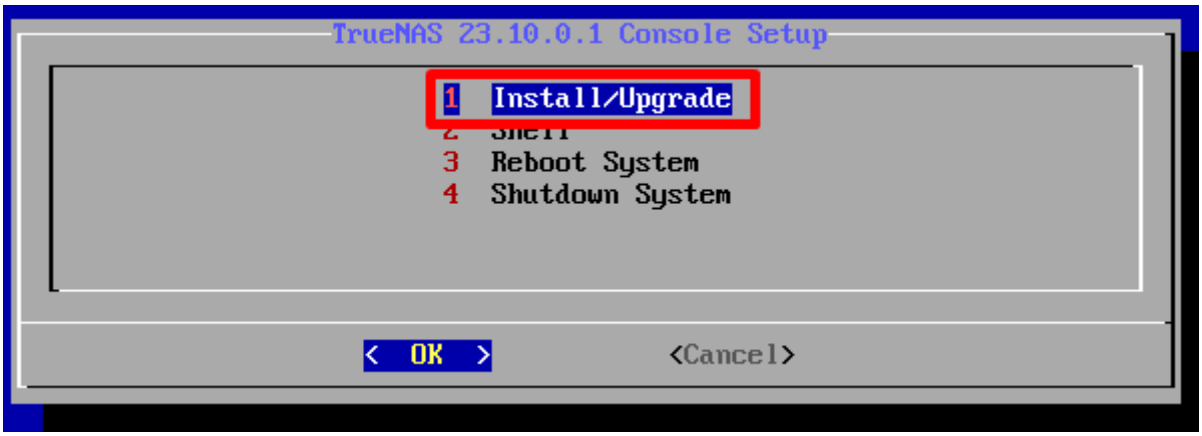
Etape 3 : L'installeur Grub se lance, on clique sur Enter



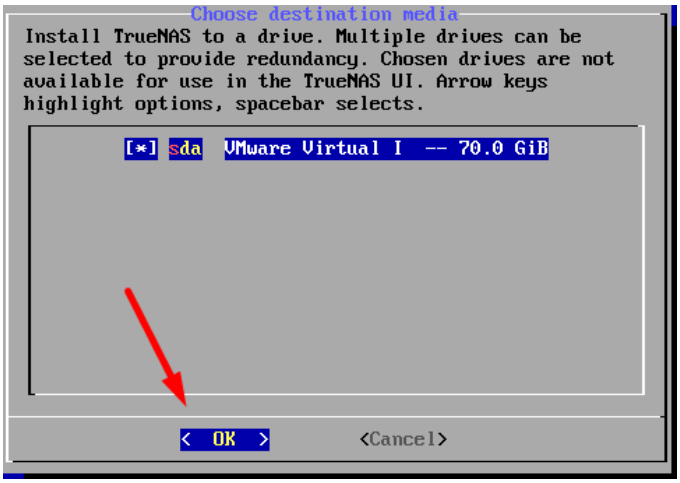
Une fois fait, l'installation devrait commencer comme ci-dessous. Cela prend environ 10 minutes.



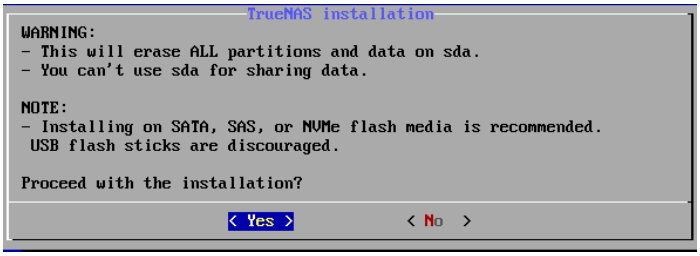
Etape 4 : Ensuite, une nouvelle fenêtre devrait apparaitre. On doit choisir la première option pour installer TrueNas .



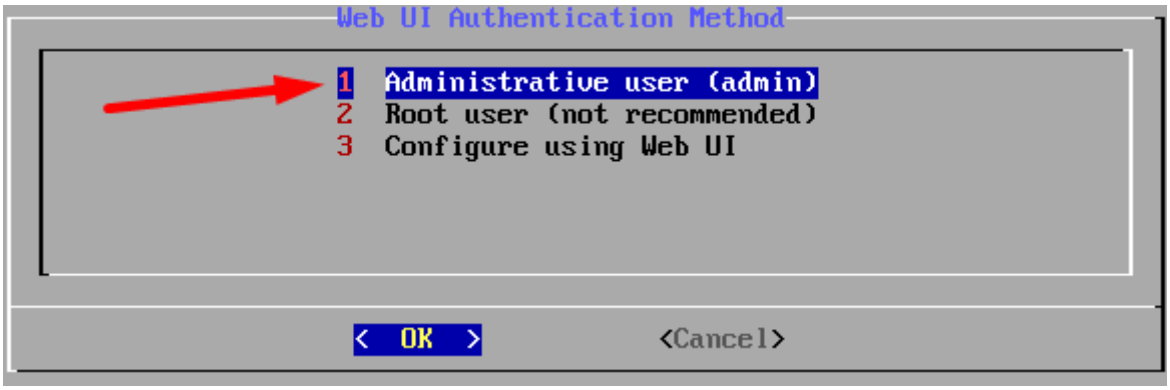
Etape 5 : Une nouvelle fenêtre devrait s'afficher nous demandant de choisir sur quel disque installer l'OS. Pour l'instant nous allons choisir notre seul disque par défaut. Pour cela, on appuis sur Espace puis sur Entré.



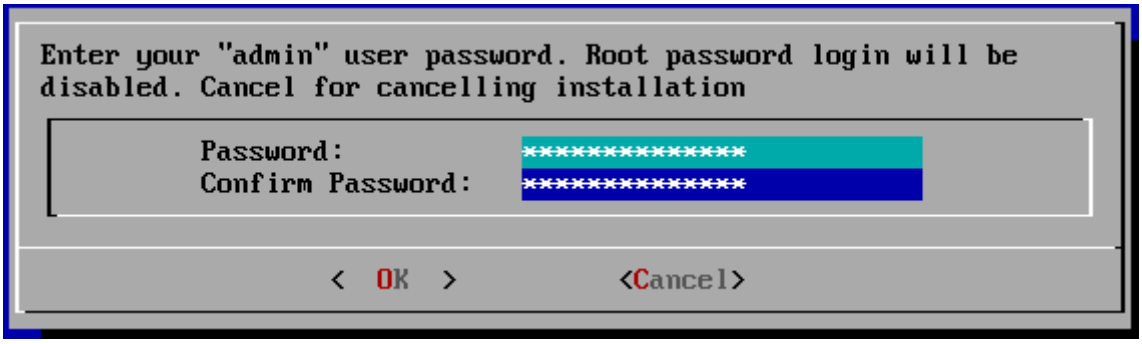
Nous allons confirmer en cliquant sur « Yes » pour effacer le disque et poursuivre l'installation de TrueNAS. Cela signifie que le disque ne sera pas utilisable pour le partage de données ultérieurement.



Etape 6 : Il faudra ensuite choisir le moyen d'identification sur le web. Nous allons choisir le mode administrateur pour une question de sécurité. (Surtout pas root car si mdp découvert, la personne a le contrôle total sur la vm).

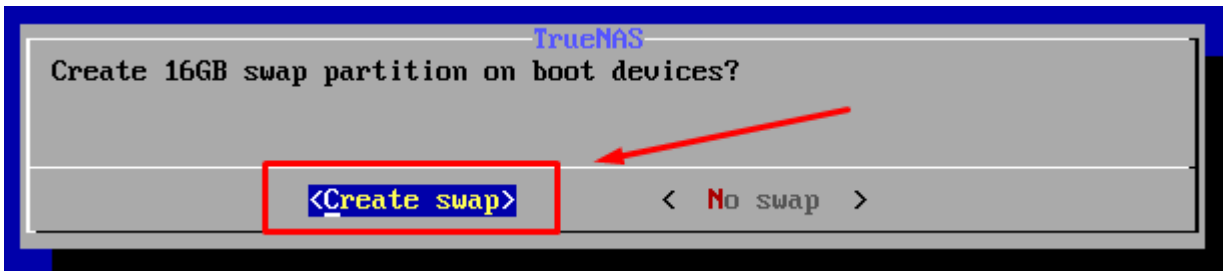


Etape 7 : Nous devons par la suite renseigner notre mot de passe Administrateur pour l'accès au TrueNAS

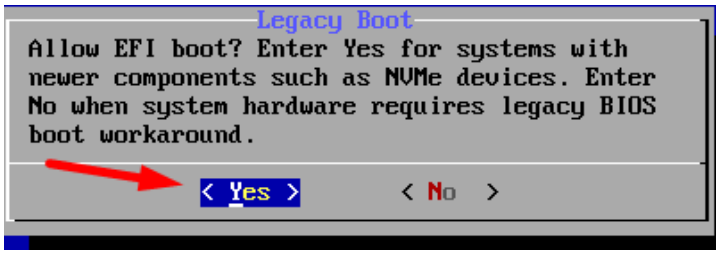


Étape 8 : Nous allons créer une partition d'échange (swap) de 16GB en cliquant sur « Create swap ».

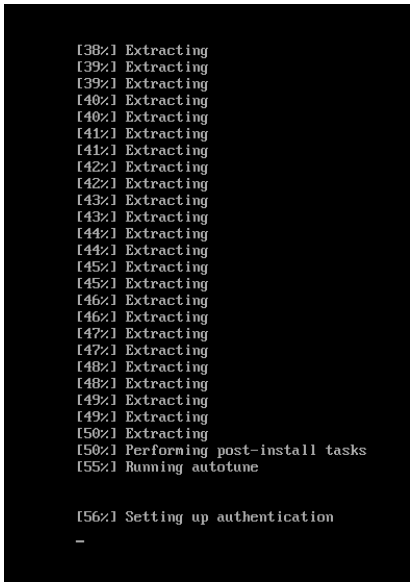
Cette partition est utilisée par TrueNAS comme mémoire virtuelle lorsque la RAM est pleine, ce qui peut améliorer les performances dans certains scénarios de charge élevée.



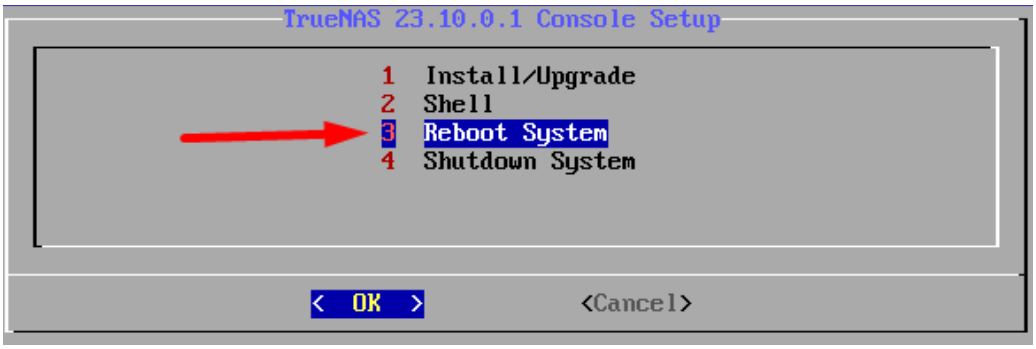
Étape 9 : Nous allons autoriser le démarrage EFI en sélectionnant « Yes », ce qui est adapté pour des systèmes avec des composants plus récents.



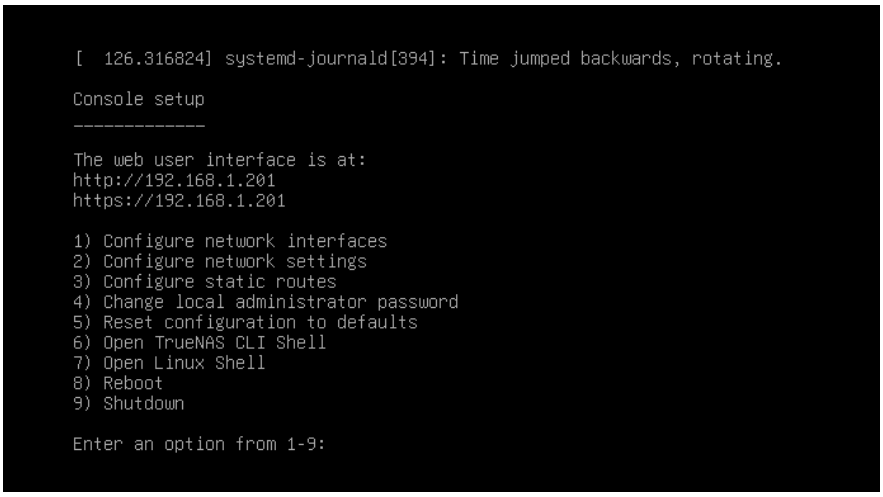
L'installation s'effectue avec succès



Quand tout est bon, une fenêtre s'affiche. Nous allons redémarrer notre serveur.



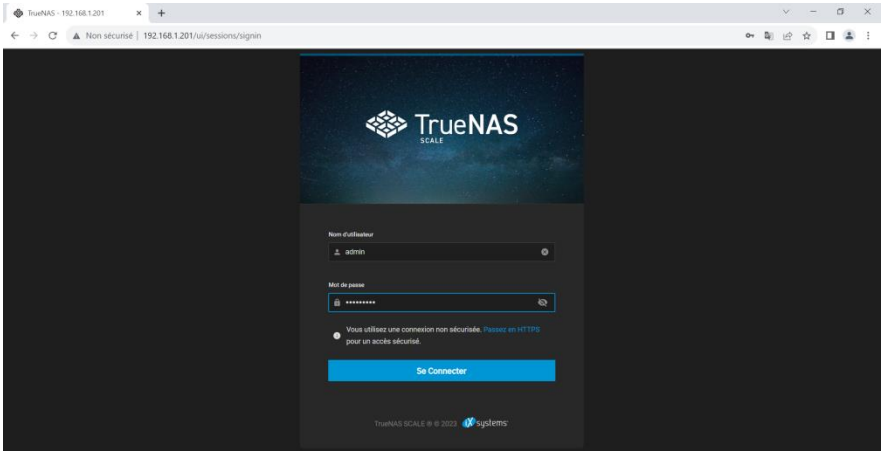
Une fois l'installation terminer, nous avons désormais accès à TrueNAS. Nous pouvons voir que nous avons récupérer une adresse IP



Etape 10 : Pour continuer nos configurations plus simplement sur le serveur NAS, nous devons nous rendre sur son interface web du serveur. Pour cela, nous entrons son adresse IP sur le navigateur d'une machine de notre réseau interne

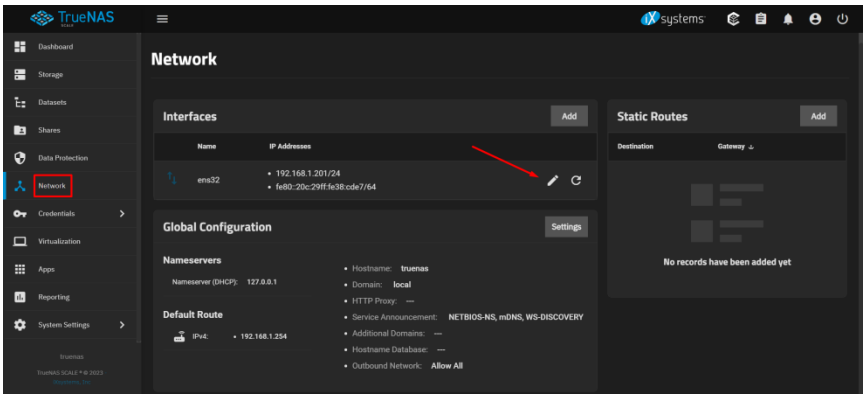
Une fois sur l'interface web, on renseigne nos informations pour se connecter.

(Attention le clavier est en qwerty par défaut)

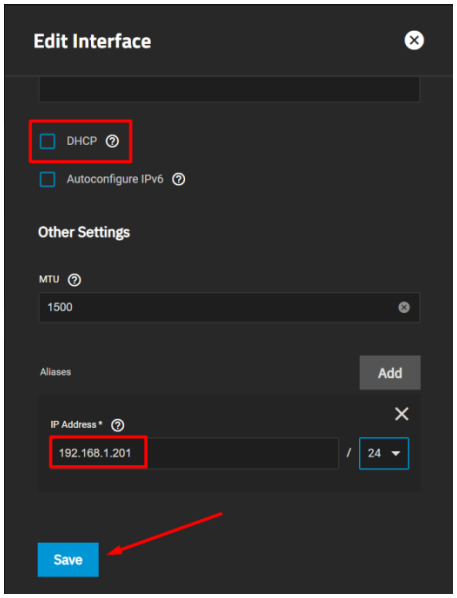


B. Configuration

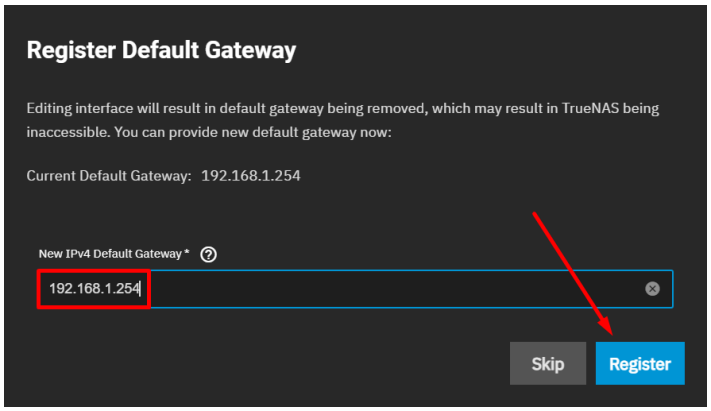
Etape 1: Nous allons dès à présent configurer une adresse ip statique. Pour ce faire, on va dans l'onglet « Network » pour cliquer sur le stylo.



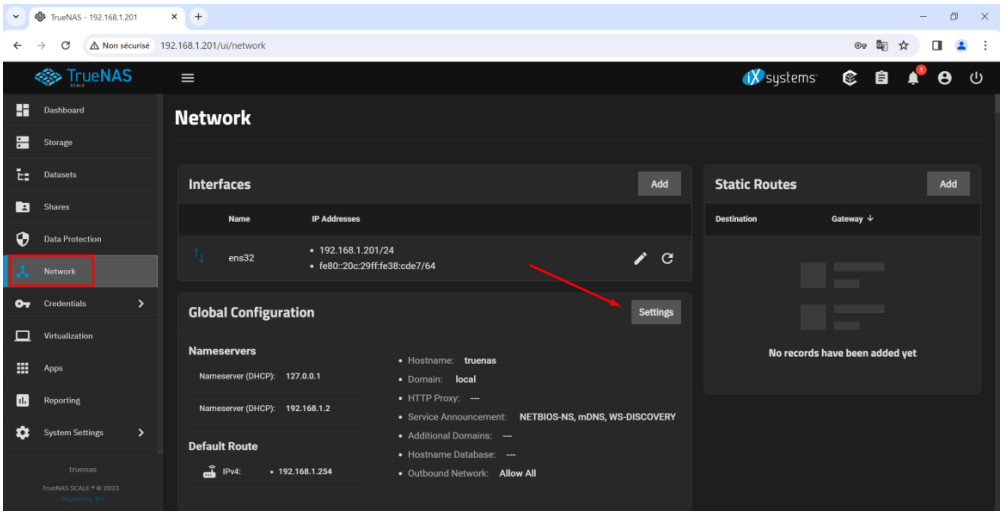
A partir de ce moment, une fenêtre latérale va s'ouvrir, on désactive le mode DHCP et attribuer notre adresse IP statique. Il faudra redémarrer le serveur NAS pour que cela soit actif



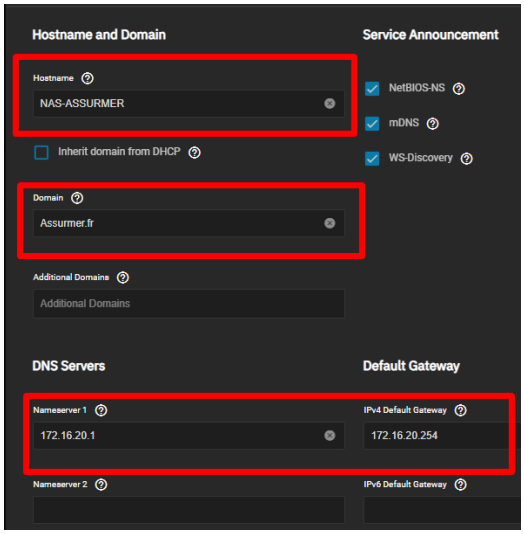
Après cela, il nous demandera de renseigner la passerelle par défaut et on clique sur « Register ».



Etape 2 : Nous allons dès à présent intégrer le NAS dans notre domaine Assurmer . Pour se faire, rendez-vous dans l'onglet « Network » puis on clique sur « Settings ».



Etape 3 : A partir de là, sur la nouvelle fenêtre, on remplit les informations et on clique sur « Save ».

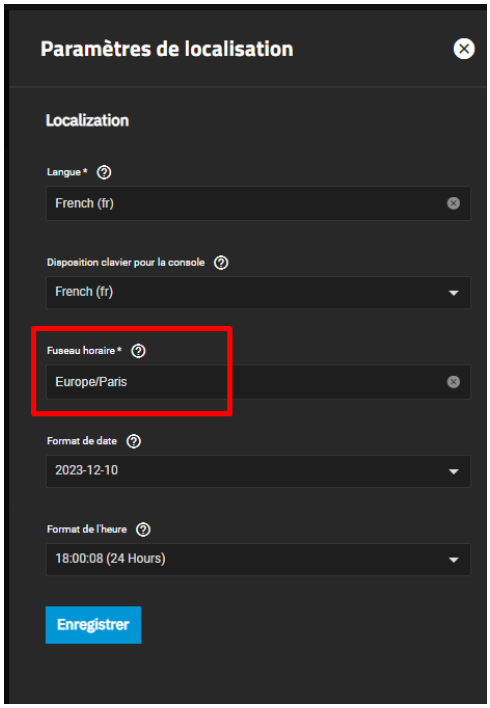


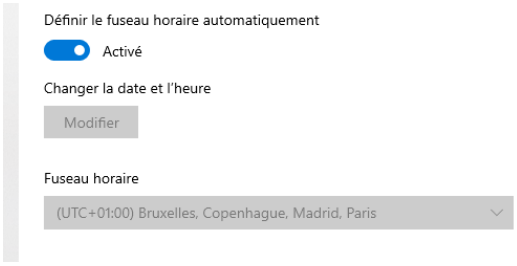
Hostname : On va nommer notre serveur

Domain : On va mentionner notre domaine

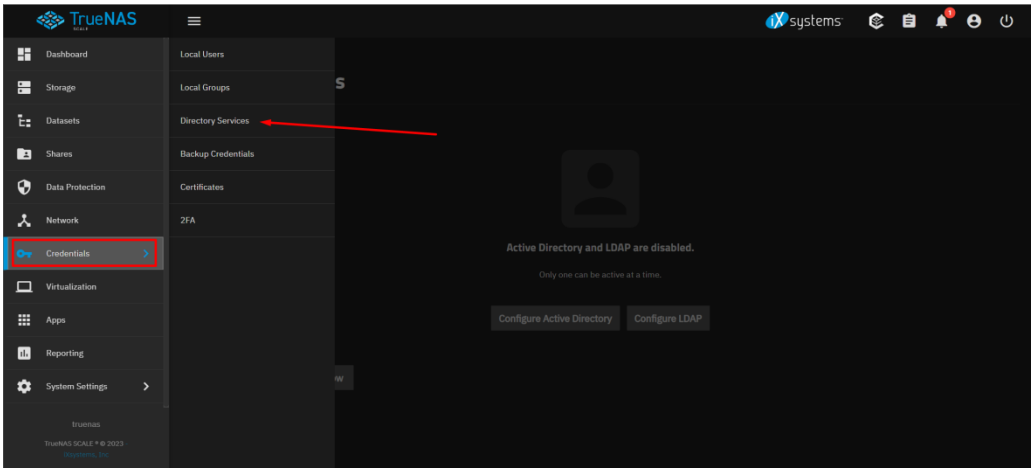
DNS Server et Default Gateway : On indique les adresses ip de notre DNS et passerelle par défaut

Nous devons régler d'abord le fuseau horaire de TrueNAS sur 'Europe/Paris' pour correspondre à celui de notre domaine contrôleur. Le serveur TrueNAS devra avoir accès à Internet

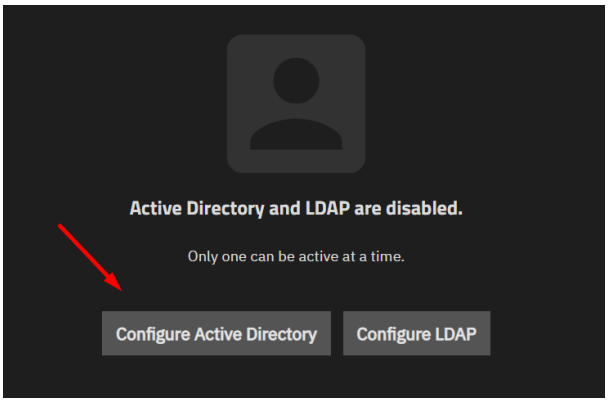




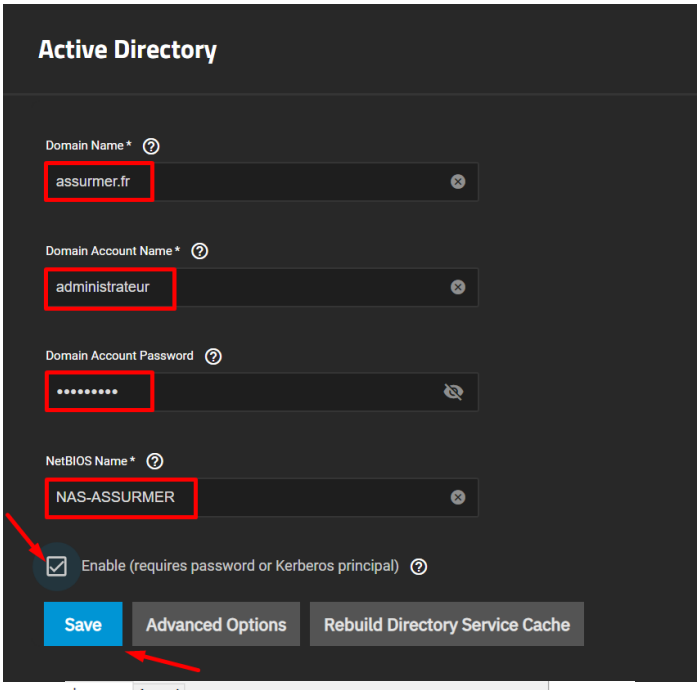
Etape 4 : On va ensuite dans l'onglet « Credentials » puis dans « Directory Services ».

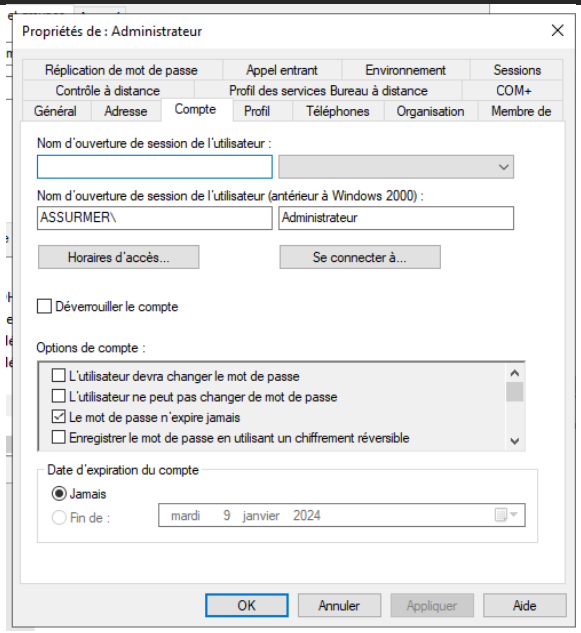


Etape 5 : A partir de là, on clique sur « Configure Active Directory ».



On remplit ensuite nos informations pour le rentrer dans le domaine.

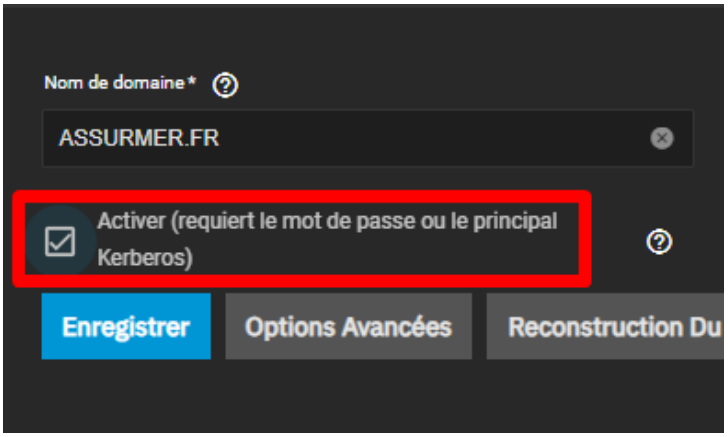




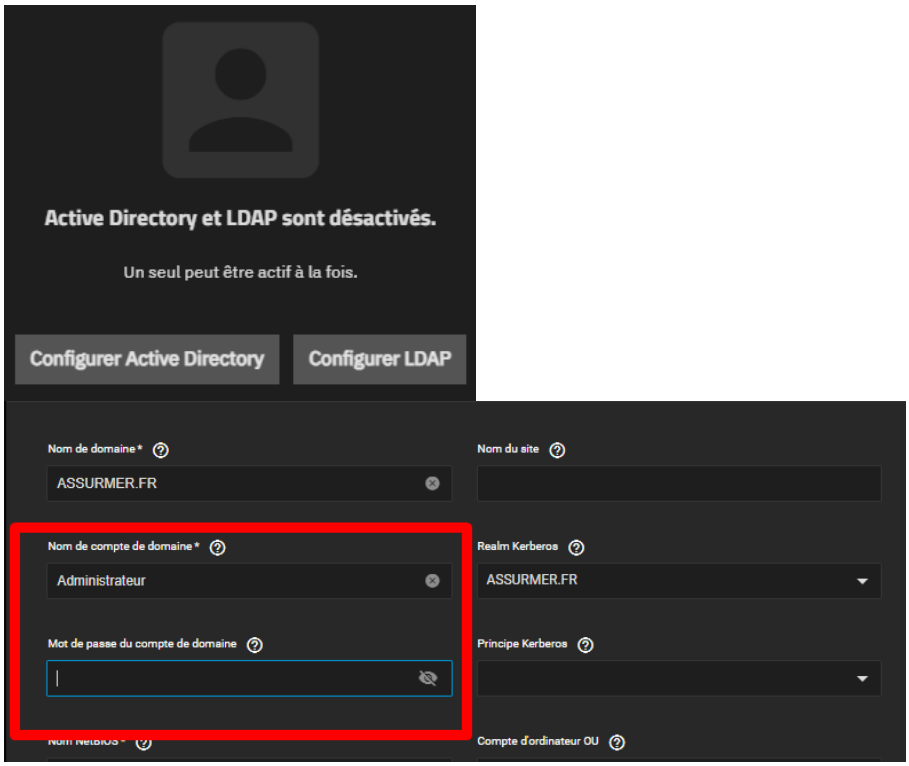
Dans le champ « **Domain Account Name** » nous devons spécifier les coordonnées du compte « Administrateur » de notre Active directory car celui-ci aura des droites spécifiques permettant à TrueNas de parcourir tout l'annuaire AD

En cas de problème de jointure de domaine

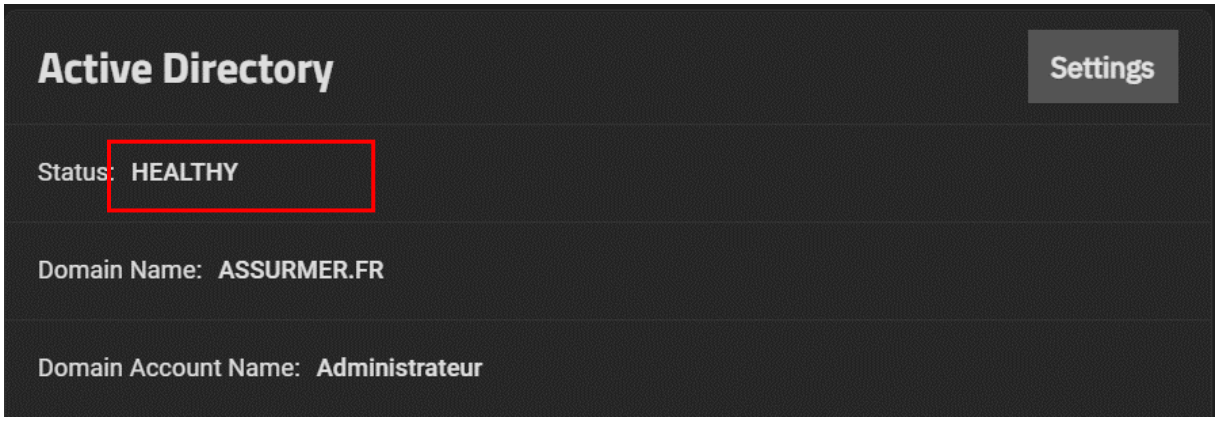
Désactiver la jointure du domaine. Il faudra ensuite peut-être réinitialiser le mot de passe du compte administrateur du domaine



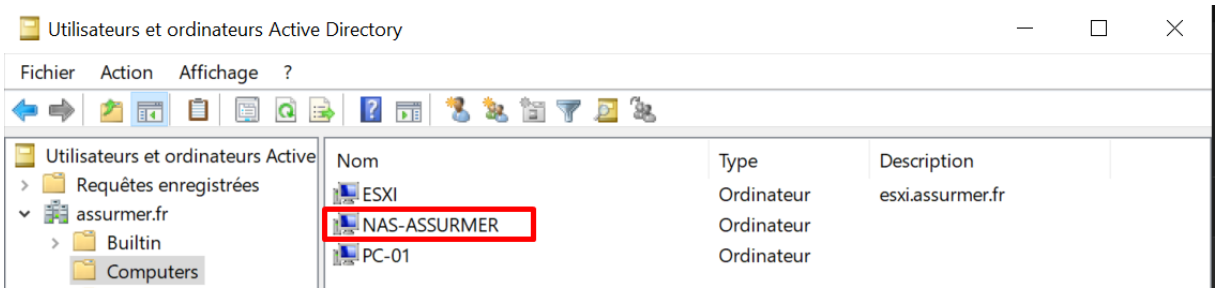
Cliquer sur Configurer Active Directory. Dans option avancé on va retirer le champs « Principe Kerberos » et renseigner les coordonnées du compte administrateur du domaine



Une fois fait, nous devrions voir comme ci-dessous.



Pour faire une seconde vérification, nous allons aller sur notre Active Directory pour voir si le serveur NAS est bien présent.



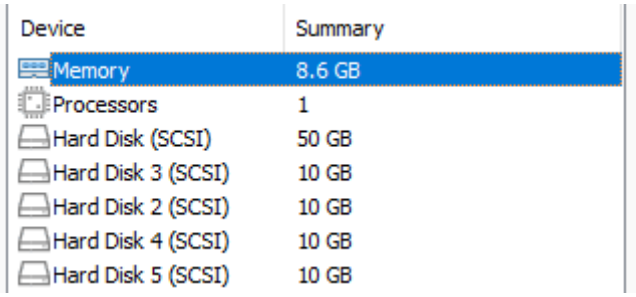
En joignant notre serveur TrueNAS à un domaine Active Directory de Windows, nous centralisons la gestion des comptes utilisateurs et des permissions sur votre réseau. Cela signifie que nous n'avons pas besoin de créer des comptes séparés pour chaque personne sur le serveur TrueNAS ; nous utilisons les mêmes identifiants que ceux pour les ordinateurs et services dans l'entreprise. Les utilisateurs peuvent ainsi accéder aux fichiers sur TrueNAS avec leur nom d'utilisateur et mot de passe habituels, ce qui rend l'accès aux ressources plus simple et plus sécurisé

II. Création d’un pool

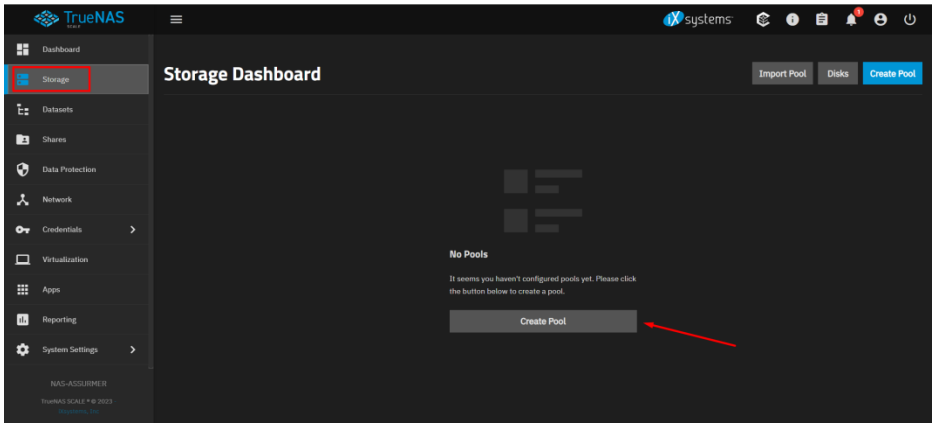
Dans le contexte de TrueNAS, un pool est un ensemble de disques durs regroupés pour stocker des fichiers. En les mettant ensemble dans un pool, nous pouvons gérer plus facilement un grand volume de données, les protéger contre les pannes en répartissant les données sur plusieurs disques, et aussi étendre l'espace de stockage en ajoutant plus de disques au fil du temps. Cela rend le stockage de nos données plus flexible et plus sûr.

Notre pool sera configuré en ZFS. Il faut savoir que ZFS est un système de fichiers qui gère le stockage des données sur notre serveur. Il est conçu pour s'assurer que nos données sont protégées contre les erreurs, facilement accessibles et peuvent être gérées de manière flexible. ZFS est connu pour ses fonctionnalités avancées comme la protection sur l’intégrité des données, la capacité à gérer de grands volumes de stockage, et la possibilité de prendre des "snapshots" de nos données à un moment donné sans utiliser beaucoup d'espace supplémentaire

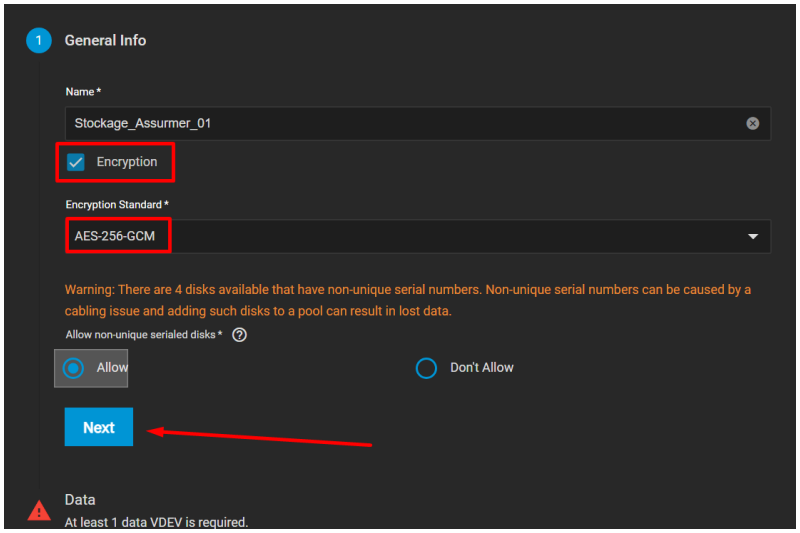
Dans notre cas, nous allons donc crée un pool ZFS avec une configuration RAIDZ6 pour une tolérance de panne de 2 disques dans lequel nous utiliserons 4 disque dur de 10 Go



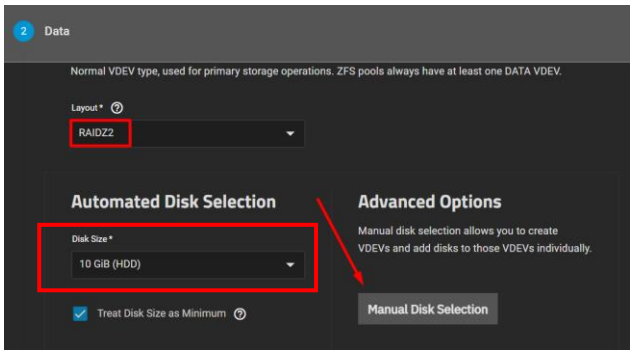
Etape 1 : Nous allons dès à présent crée notre pool ZFS sur le NAS. Pour ce faire, nous allons aller dans l’onglet « Stockage » puis dans « create pool ».



Étape 2 : On va entrer le nom souhaité dans le champ "Name". Ensuite, on coche l'option "Encryptions" pour sécuriser les données et on choisit le standard de cryptage, dans ce cas "AES-256-GCM", qui est une méthode robuste de cryptage.
Ainsi, le chiffrement se fera avec une keysize de 256 bits mais aura une keyspace de 2^256 possibilités.



Étape 3 : Dans cette configuration, nous allons faire une configuration RAIDZ2 . Ainsi, nous allons combiner à la fois du mirroring et du striping pour de la sécurité et de la vitesse.

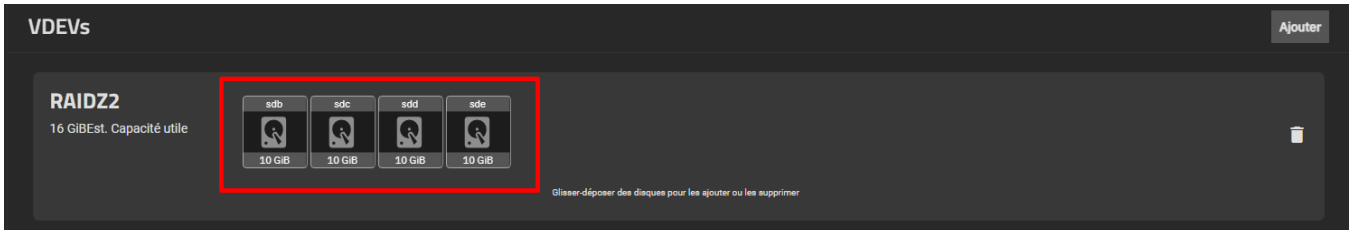


On va cocher "Treat Disk Size as Minimum » pour assurer que la taille de tous les disques dans un pool est basée sur le plus petit disque.

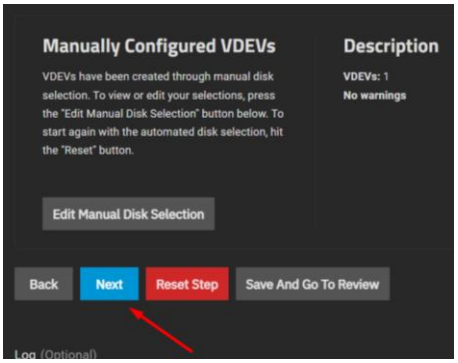
Cela uniformise la capacité de stockage, évitant les complications qui peuvent survenir avec des disques de tailles différentes

Ici, avec 10 Go par disque, cette option garantit que toute la capacité des disques sera utilisée de m anière optimale et cohérente.

Ensuite, on clique sur « Manual Disk Selection » pour choisir les disques qui vont servir pour le raid

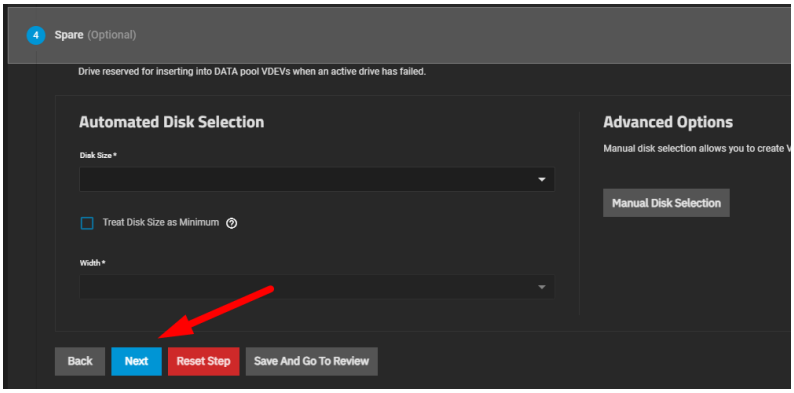


Une fois fait, on clique sur « Next ».



Ici, nous pouvons mettre en place en disque de secours en prévoyance où il y aurait une défaillance d'un disque actif. De ce fait, celui-ci est de base active.

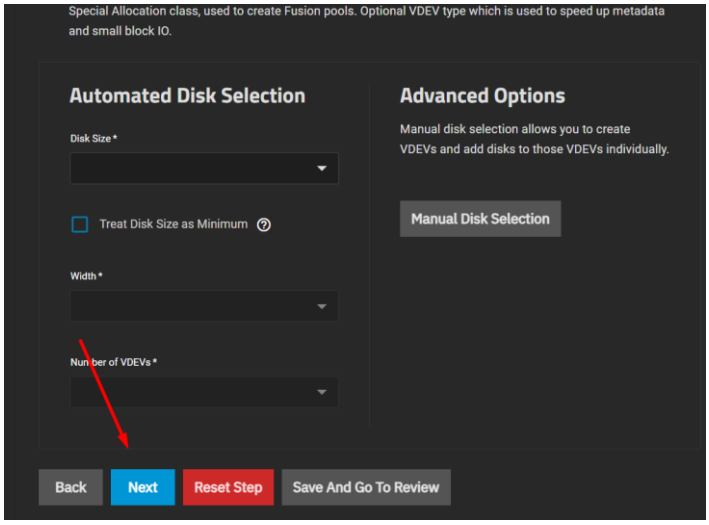
Nous n'allons pas configurer de disque de secours



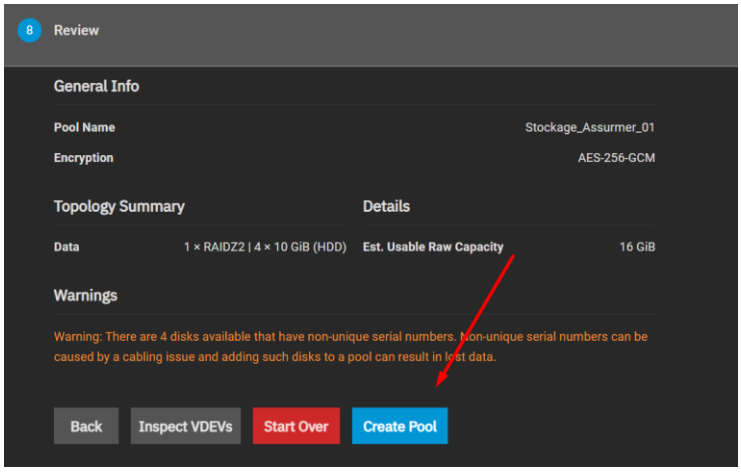
La Special Allocation Class dans ZFS permet de tirer parti des vitesses élevées des SSD pour les opérations fréquentes

Un VDEV (Virtual Device) est une unité de stockage virtuelle dans ZFS. Lorsque vous créez un Fusion Pool, vous pouvez utiliser un certain type de VDEV optionnel pour accélérer certaines opérations. De ce fait, ce type de VDEV est utilisé pour accélérer les opérations liées aux métadonnées (informations sur les données) et aux petits blocs de données.

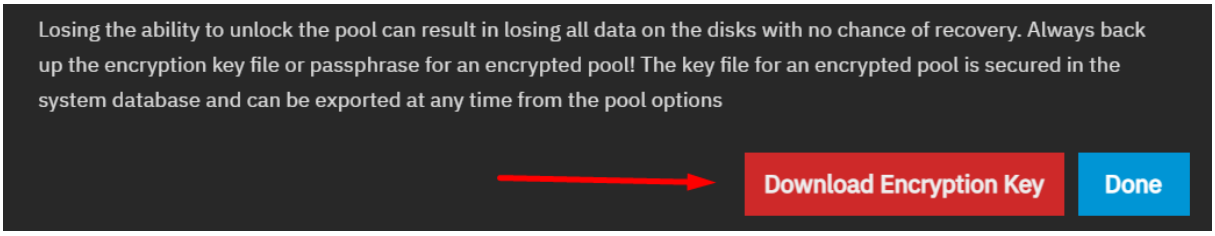
Nous allons aussi passer cette étape pour ce test



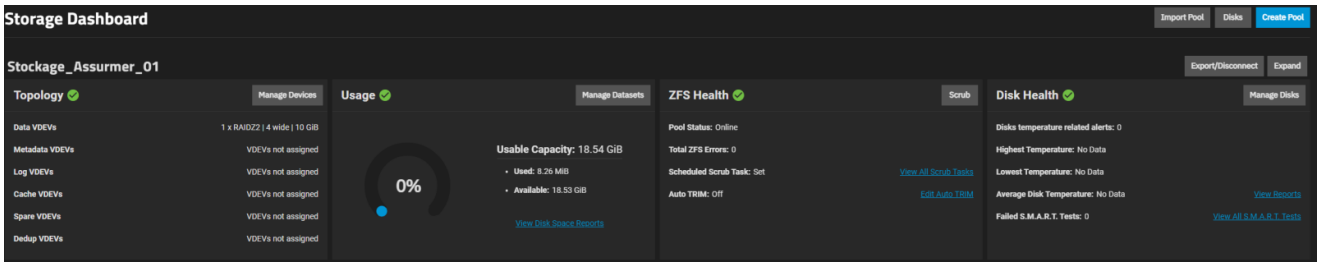
Une fenêtre récapitulative devrait s'afficher. Cliquez sur « Create Pool » puis confirmer.

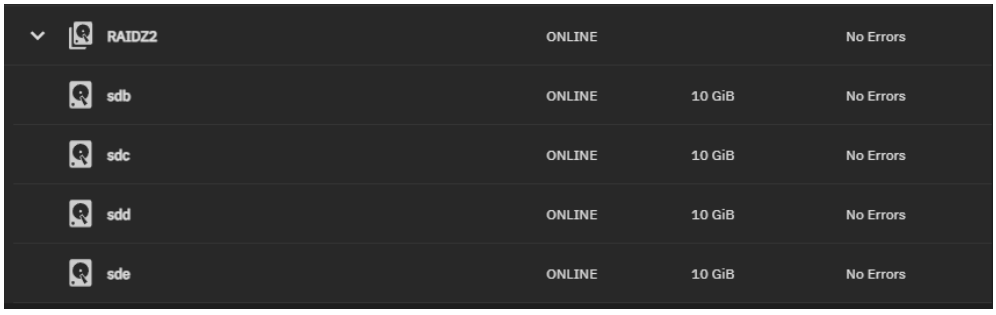


Une fenêtre d'avertissement s'affichera pour souligner l'importance de sauvegarder la clé de chiffrement de votre pool de stockage ZFS. Il est crucial de télécharger et de conserver cette clé en sécurité, car sans elle, on ne pourra pas accéder à vos données chiffrées en cas de problème. La clé est un élément essentiel pour le déchiffrement et la perte de cette clé signifie la perte de toutes les données sans possibilité de récupération. On clique alors sur « Dowload Encryption Key .



Voici, notre pool ZFS





Conclusion du pool : C’est un pool ZFS configuré avec RAIDZ2. Cela signifie que le pool utilise une forme de redondance intégrée à ZFS qui peut tolérer la défaillance de deux disques sans perte de données, similaire à ce que fait un RAID 6 avec des disques traditionnels.

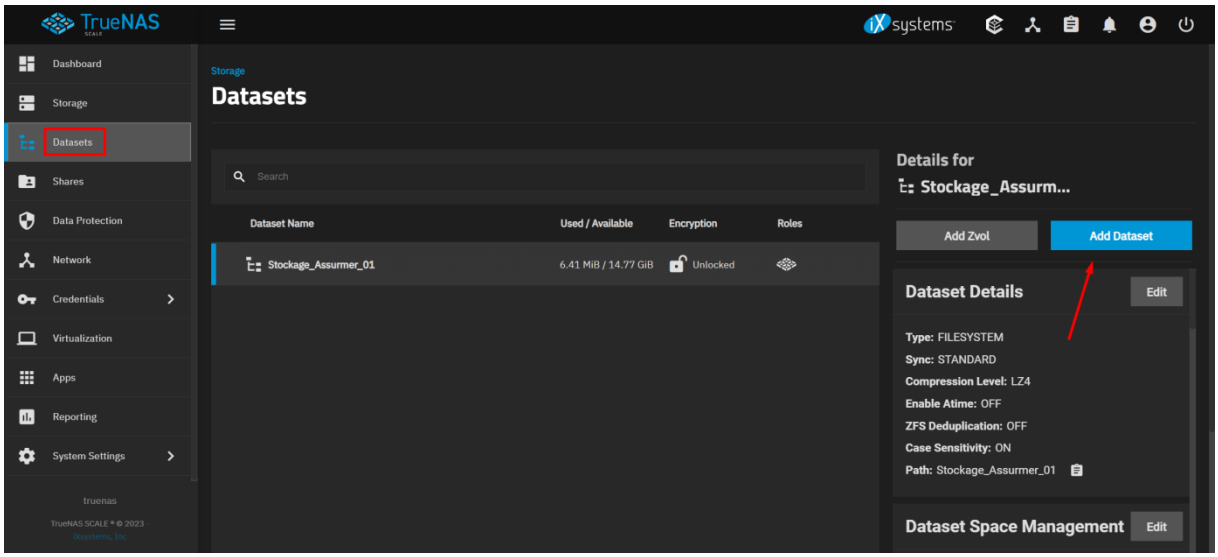
L'activation du chiffrement ajoute une couche de sécurité en s'assurant que les données stockées sont cryptées

III. Création de Dataset

Un dataset sur TrueNAS est un conteneur dans lequel nous pouvons stocker des fichiers, avec des règles spécifiques qu'on peut définir pour la sécurité et la gestion de l'espace. Chaque dataset peut avoir ses propres permissions, quotas (limites d'utilisation de l'espace disque), et snapshots (copies de sauvegarde à un instant donné).

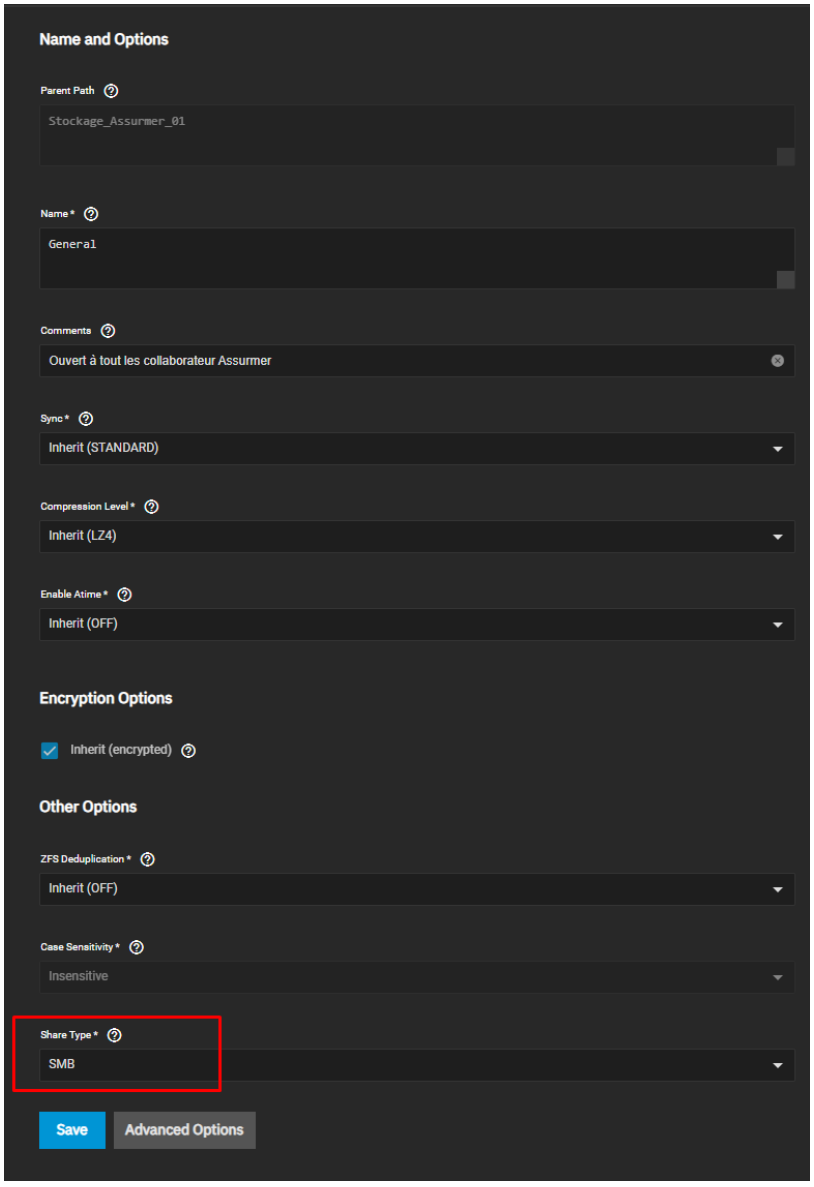
Nous allons maintenant pouvoir créer des datasets.

Etape 1 : Pour ce faire, nous allons allez dans l'onglet « Dataset » puis nous allons cliquez sur « Add Dataset » sur notre espace de stockage anciennement créer.

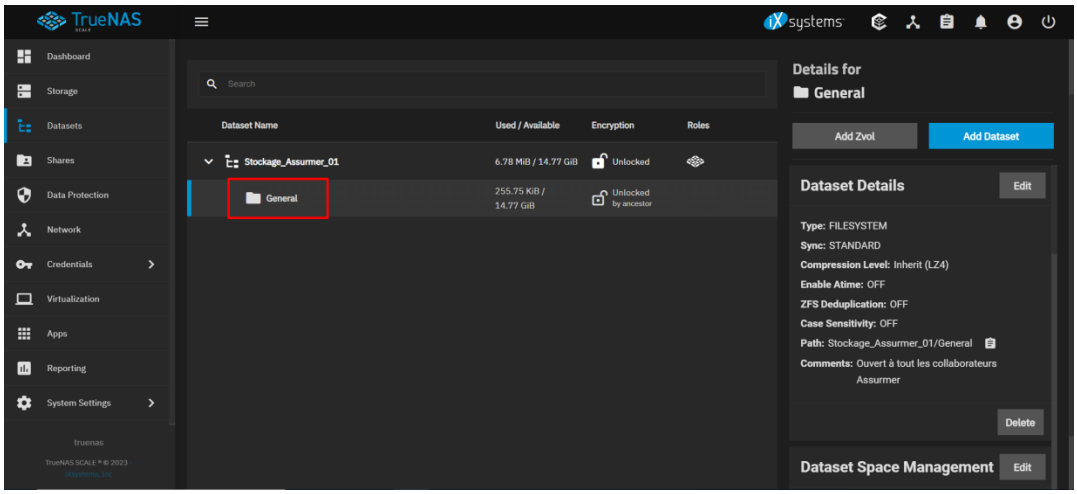


Etape 2 : Nous allons mettre ici tout par défaut. Néanmoins, comme ce partage sera accessible depuis les machines clientes Windows, nous devons activer le partage SMB

SMB, qui signifie Server Message Block, est un protocole de partage de fichiers utilisé pour permettre à des ordinateurs sur un même réseau d'accéder à des fichiers, des imprimantes, et d'autres ressources partagées sur ce réseau. C'est le protocole standard utilisé par les systèmes Windows pour le partage de fichiers, mais il est également pris en charge sur Mac et Linux

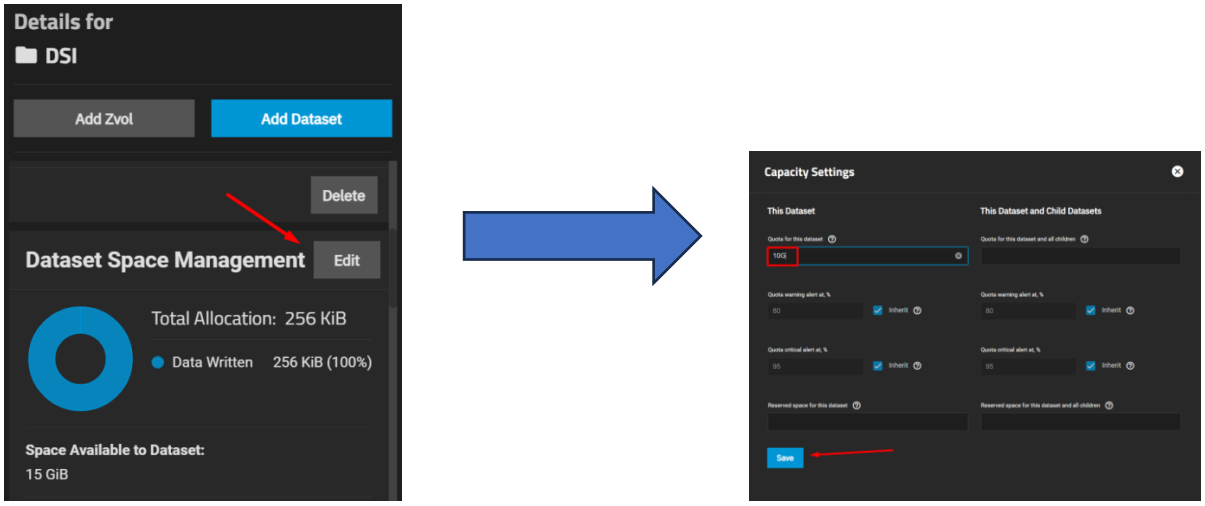


Le Dataset « Général » a été crée



Etape 3 : Nous pouvons également définir un espace de stockage maximal pour chaque dataset.

Pour ce faire, on clique tout simplement sur « Edit » dans les détails du dataset puis dans la partie gestion de l'espace du dataset.

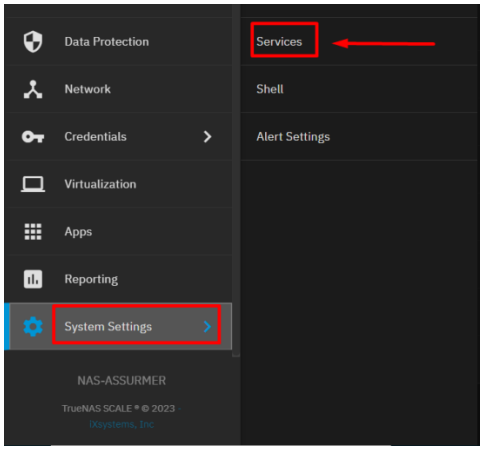


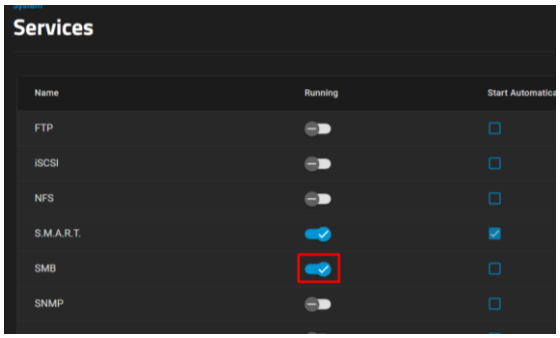
Une fois dans la nouvelle fenêtre, on définit un espace maximal pour le dataset et nous pouvons également le définir pour tous les sous répertoires.

Une fois fait, cliquez sur « Save ».

Etape 4 : Nous allons maintenant faire un partage SMB pour que ceux-ci puissent être visible sur le réseau.

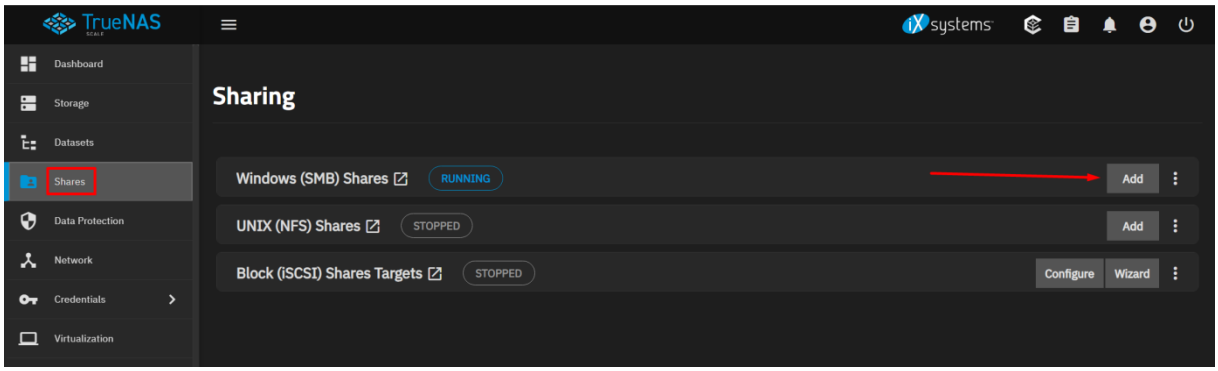
Dans un premier temps, Nous allons dans les services pour activer le protocole SMB.



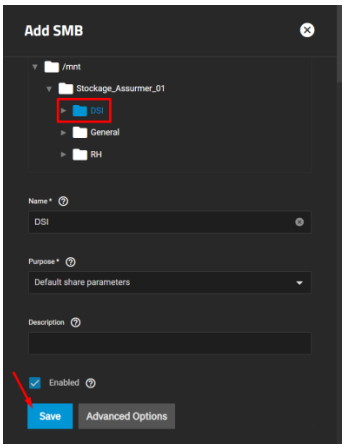


Cela permettra à Windows de voir ce qu'il y a sur le serveur TrueNas au niveau du port 139 ou 445.

Etape 5 : Nous allons aller dans « Shares », puis cliquer sur « Add »



Nous allons naviguer jusqu'à notre dataset pour partager ce dossier au sein du réseau.



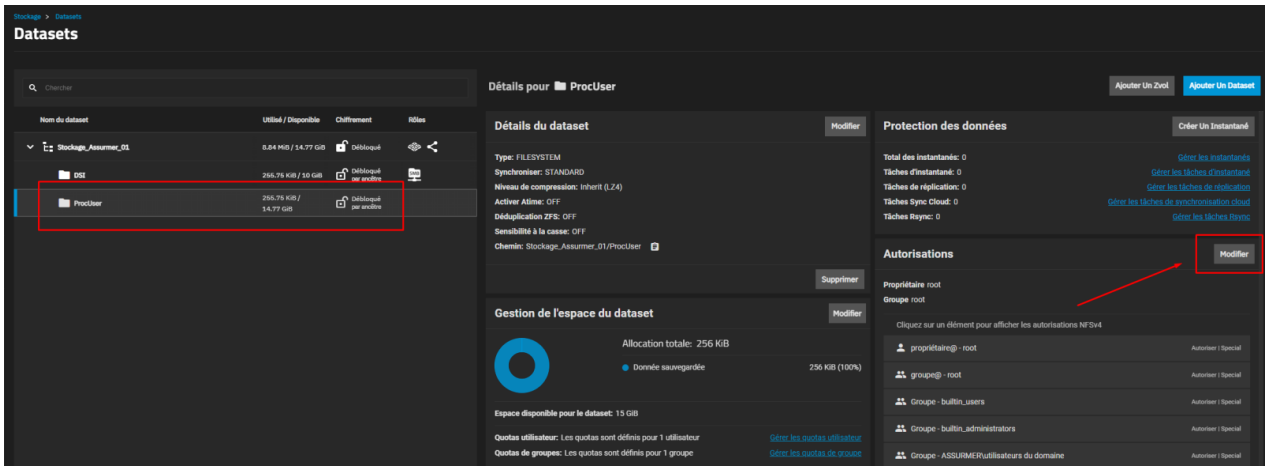
Nous allons ensuite procéder à la phase de mise en place des trois partages SMB distincts.

IV. Partage public en lecture seul

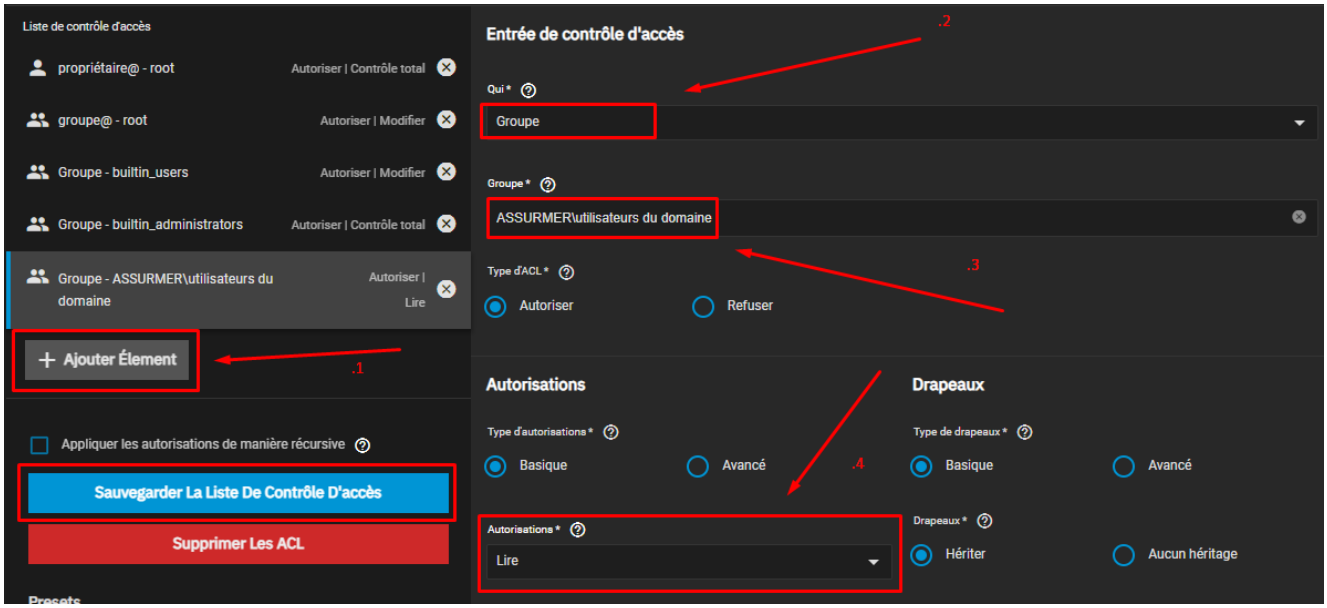
Nous allons d'abord créer un dossier de partage public qu'on appellera « ProcUsers » dans lequel on pourra mettre à disposition des procédures pour nos collaborateurs d'Assurmer. Ce dossier sera accessible par tous les utilisateurs du réseau, mais ils ne pourront que lire les fichiers, sans possibilité de les modifier ou de supprimer.

Etape 1 : Pour cela, on va configurer les droits sur les datasets via les ACL. Pour ce faire, nous allons sur le dataset qu'on souhaite configurer et cliquer sur « Edit » dans les permissions.

Sur TrueNAS, les ACL (Access Control Lists) sont des listes de permissions utilisées pour définir qui peut accéder à des fichiers ou des dossiers (datasets) et ce qu'ils peuvent faire avec.



Etape 2 : Une nouvelle fenêtre va s'afficher avec toutes les ACL que nous pouvons modifier et créer. Nous allons créer une nouvelle ACL via une configuration basique pointant sur le groupe AD « Utilisateurs du domaine » qui est le groupe par défaut de tous nos utilisateurs. De cette manière, tout le monde aura accès à ce partage



Qui : Ce champ spécifie à qui s'applique l'entrée ACL. Dans ce cas, nous avons choisi "Groupe", ce qui signifie que l'entrée ACL s'appliquera à un groupe d'utilisateurs.

Groupe : Ici, nous avons entré le nom d'un groupe de notre domaine Active Directory (AD) – "ASSURMER\utilisateurs du domaine". Cela signifie que tous les utilisateurs qui sont membres de ce groupe dans l'AD auront les permissions spécifiées par cette ACL.

Autorisations : Nous avons défini les autorisations sures "Lire". Cela accordera à tous les membres du groupe "ASSURMER\utilisateurs du domaine" le droit de lire les fichiers dans ce dossier partagé, mais ils ne pourront pas les modifier ou les supprimer.

Drapeaux : Nous avons sélectionné "Hériter", ce qui signifie que les sous-dossiers et les fichiers créés à l'intérieur de ce dossier hériteront automatiquement de cette même ACL.