MARS 2025

Mise en place d'une solution de type NAS

Auteurs : COMBETTES Elise, Gana Stéphane

Validateurs : DEGEN Loïc, EDOUARD Claire

ASSURMER

SOMMAIRE

Étude des fonctionnalités d'un serveur NAS

Dans le cadre de la création du serveur pour Assurmer, il est important de permettre aux utilisateurs d'accéder facilement et de manière sécurisée à des données stockées, un serveur NAS est un choix plus que judicieux.

Un serveur NAS (Network Attached Storage) est une solution de stockage réseau permettant de centraliser, partager et sécuriser des données. Il facilite l'accès aux fichiers pour plusieurs utilisateurs tout en assurant une gestion collaborative et sécurisée.

Les NAS utilisent des protocoles comme SMB, NFS ou FTP, compatibles avec différents systèmes d'exploitation et couramment adoptés pour leur fiabilité et la gestion des droits d'accès. La sécurité est renforcée par le chiffrement des données, qui les rend inaccessibles sans clé, même en cas de vol des disques.

Les snapshots permettent de conserver des copies instantanées des fichiers à différents moments. Contrairement aux sauvegardes traditionnelles, ils enregistrent uniquement les modifications, offrant une récupération rapide tout en consommant moins d'espace.

Les NAS prennent en charge des configurations RAID, assurant la tolérance aux pannes en répartissant les données sur plusieurs disques. Certains modèles proposent aussi la réplication entre serveurs pour une redondance géographique.

L'intégration avec Active Directory simplifie la gestion des utilisateurs. Par exemple, un NAS peut attribuer automatiquement des droits d'accès en fonction des groupes définis dans l'annuaire. La synchronisation avec des services cloud permet de combiner stockage local et sauvegarde distante.

En résumé, le NAS constitue une solution fiable et évolutive pour centraliser, sécuriser et partager des données dans un cadre professionnel.

Analyse des solutions de type RAID

Les solutions RAID (Redundant Array of Independent Disks) permettent d'assurer la sécurité des données et d'améliorer les performances des systèmes de stockage. Voici une comparaison des principales configurations RAID adaptées aux NAS :

- RAID 0 (Striping) : Répartit les données sur plusieurs disques pour améliorer les performances. Il n'offre aucune tolérance aux pannes : la perte d'un disque entraîne la perte totale des données.
- RAID 1 (Mirroring) : Duplique les données sur deux disques. Il garantit la sécurité en cas de panne d'un disque, mais réduit la capacité de stockage disponible de moitié.
- RAID 5 : Nécessite au moins trois disques. Il répartit les données et les informations de parité, offrant tolérance aux pannes avec une capacité utile égale au nombre de disques moins un. Cependant, les performances peuvent être réduites lors de la reconstruction après une panne.
- RAID 6 : Similaire au RAID 5 mais avec deux blocs de parité, il supporte la panne de deux disques simultanément. Il offre une meilleure sécurité mais nécessite au moins quatre disques et consomme plus d'espace.
- RAID 10 (1+0) : Combine RAID 1 et RAID 0. Il offre à la fois des performances élevées et une bonne tolérance aux pannes, mais utilise seulement 50 % de la capacité totale pour le stockage.

Le choix d'une configuration RAID dépend des besoins spécifiques en matière de sécurité, de performances et de capacité. Pour une entreprise comme Assurmer, qui nécessite une sécurité accrue, le RAID 1 ou le RAID 5 est souvent recommandé, car ils offrent un bon équilibre entre protection des données et utilisation de l'espace de stockage.

Proposition de politique de sécurité pour l'intégrité et la sauvegarde des données d'Assurmer

La sécurité des données est essentielle pour assurer la continuité des activités d'Assurmer. Voici les principes fondamentaux d'une politique de sécurité visant à garantir l'intégrité et la sauvegarde des données professionnelles.

- Sécurisation des accès : L'accès aux données doit être limité aux utilisateurs autorisés uniquement. L'utilisation de mots de passe complexes, combinée à une authentification à deux facteurs, est obligatoire. Un contrôle d'accès basé sur les rôles (RBAC) permettra de restreindre l'accès en fonction des responsabilités de chaque utilisateur.
- Sauvegarde des données : Il est impératif d'effectuer des sauvegardes régulières des données critiques. La solution NAS, configurée avec un système RAID, offrira une redondance pour assurer une disponibilité constante des données. Les sauvegardes doivent être automatiques et incrémentielles, avec une révision périodique de la politique de sauvegarde.
- Cryptage des données : Pour protéger les données sensibles, un cryptage des fichiers doit être activé, tant pour les données stockées que pour les transferts. Cela garantit que même en cas de vol physique des supports de stockage, les données restent inaccessibles sans la clé de décryptage.
- Surveillance et journalisation : La surveillance continue des accès et des opérations sur les données est essentielle. Les logs d'accès seront enregistrés et analysés pour détecter toute activité suspecte. En cas d'anomalie, des alertes en temps réel permettront de réagir rapidement.
- Gestion des vulnérabilités : Le NAS et les systèmes associés doivent être maintenus à jour pour se prémunir contre les failles de sécurité. Un processus de veille technologique sera mis en place pour suivre l'apparition de nouvelles vulnérabilités et assurer une gestion proactive des risques.
- Plan de reprise d'activité (PRA) : En cas de panne ou d'incident majeur, un plan de reprise d'activité permettra de restaurer rapidement les données et les services. Des tests réguliers garantiront l'efficacité de ce plan pour limiter les impacts sur l'activité.

Cette politique vise à garantir la confidentialité, l'intégrité et la disponibilité des données d'Assurmer, tout en mettant en place des processus de protection et de récupération adaptés aux risques identifiés.

Comparatif de deux solutions NAS

Puisque les solutions NAS logicielles jouent un rôle clé dans la gestion des données des entreprises, le choix de la solution logicielle est crucial.

Parmi les solutions les plus populaires, TrueNAS et OpenMediaVault se démarquent par leurs fonctionnalités et leur fiabilité.

TrueNAS, développé par iXsystems, est une solution open source basée sur FreeBSD, connue pour sa robustesse, sa sécurité avancée et son système de fichiers ZFS. Il est souvent privilégié dans les environnements professionnels pour sa capacité à assurer l'intégrité des données et sa compatibilité avec les environnements Active Directory.

OpenMediaVault, quant à lui, repose sur Debian Linux. Il est apprécié pour sa simplicité d'installation et d'utilisation, ce qui en fait une solution intéressante pour les petites entreprises ou les particuliers. OpenMediaVault propose une interface web conviviale et une large gamme de plugins permettant d'ajouter des fonctionnalités supplémentaires.

Voici un tableau comparatif des deux solutions :

Critères	TrueNAS	OpenMediaVault
Système d'exploitation	FreeBSD	Debian
Système de fichiers	ZFS	EXT4, XFS, Btrfs
Sécurité	Chiffrement natif, snapshots	Chiffrement via plugins
Gestion AD	Intégration native	Via plugins
Interface	Interface web avancée	Interface web simple
Performances	Optimisé pour les environnements professionnels	Adapté pour les petites infrastructures
Support de la communauté	Large communauté professionnelle	Communauté orientée particuliers

>Le choix de TrueNAS s'impose pour Assurmer en raison de sa stabilité, de son intégration native avec Active Directory et de la sécurité qu'offre ZFS.

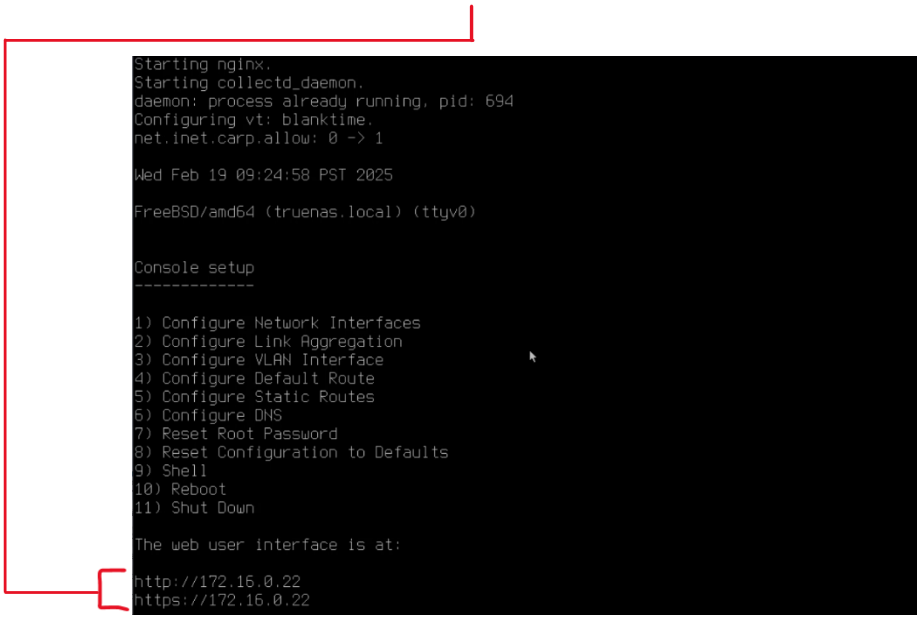
De plus, sa capacité à gérer des snapshots et des sauvegardes automatiques permet d'assurer l'intégrité des données, un enjeu majeur pour une entreprise. Bien que plus complexe à prendre en main, TrueNAS représente une solution pérenne pour une infrastructure professionnelle.

Installation de la solution choisie

Tout d'abord, téléchargez et installez sur une machine virtuelle la dernière solution de TrueNAS-Core disponible via ce lien :

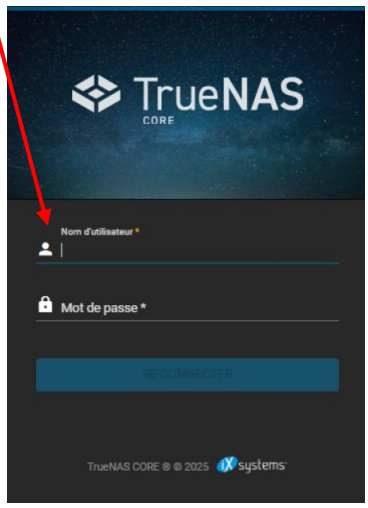
https://download-core.sys.truenas.net/13.0/STABLE/U6.7/x64/TrueNAS-13.0-U6.7.iso

Une fois installé, au redémarrage, vous aurez une adresse IP renseignée par défaut, tenant compte de votre réseau.
Dans notre cas, nous avons eu l'adresse 172.16.0.22.

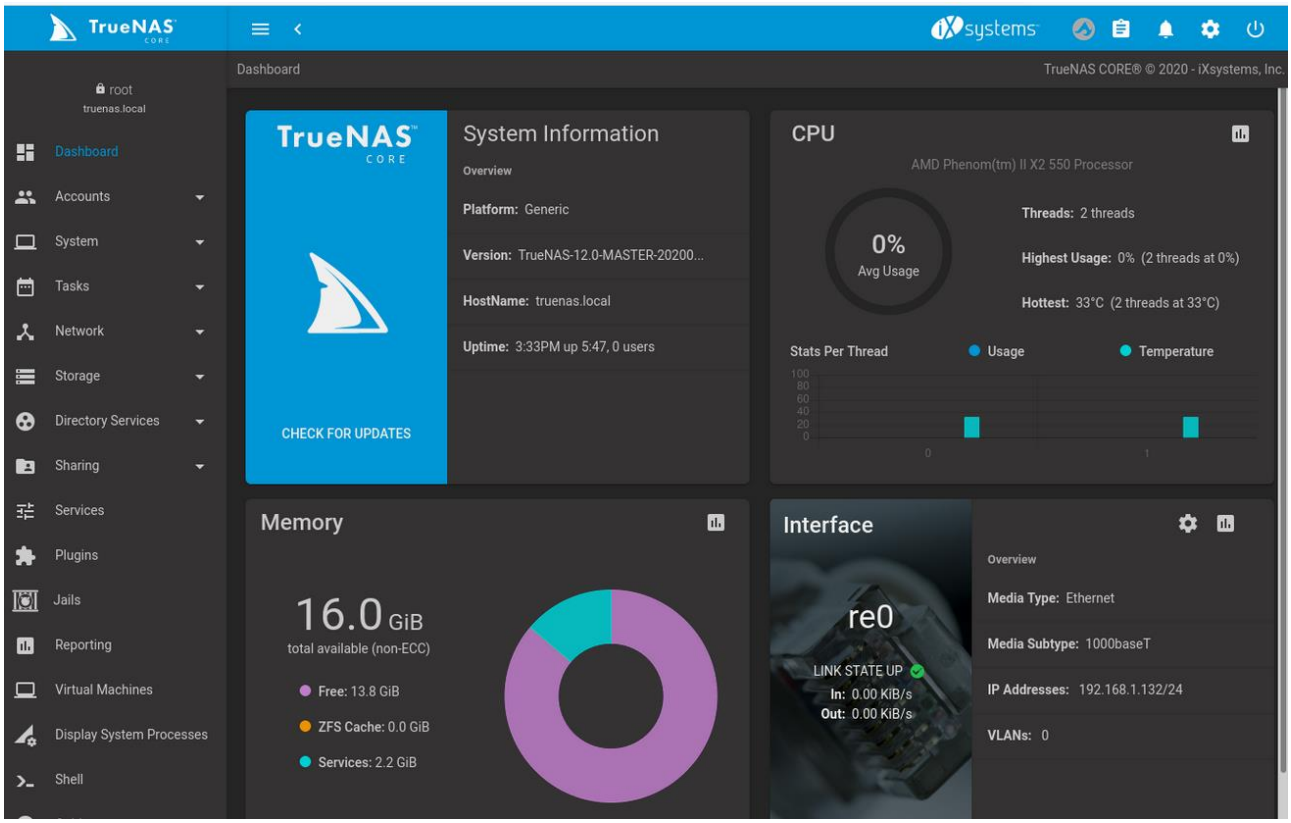


En la tapant dans la barre d'adresse de votre navigateur internet, vous tomberez alors sur la page de connexion de votre interface TrueNAS.

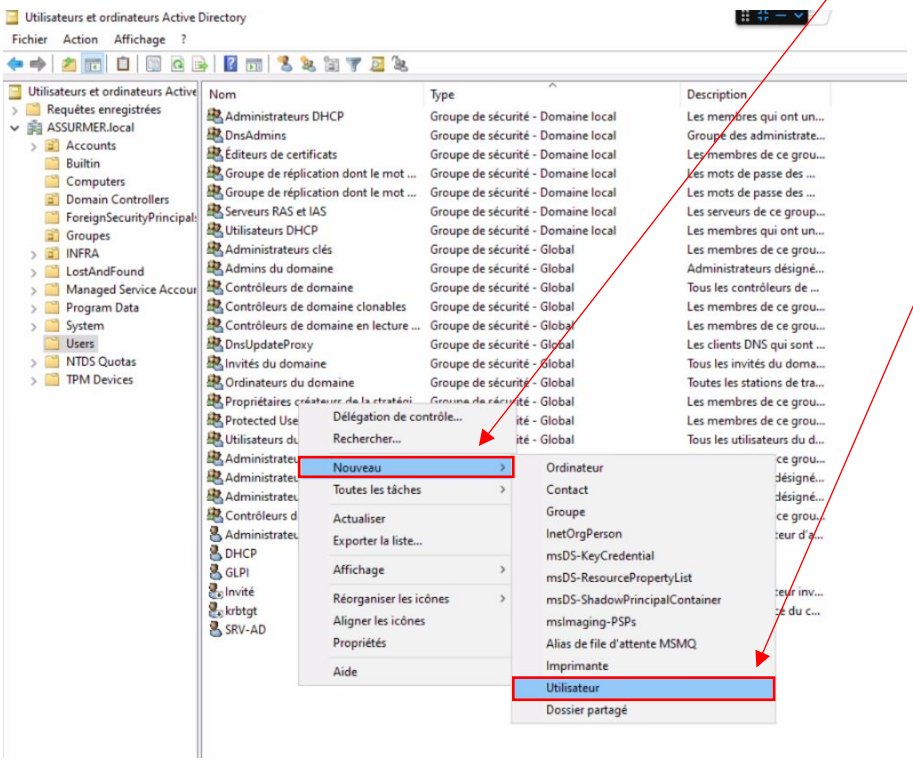
L'identifiant par défaut est « root » et le mot de passe est celui qui vous a été demandé lors de l'installation.



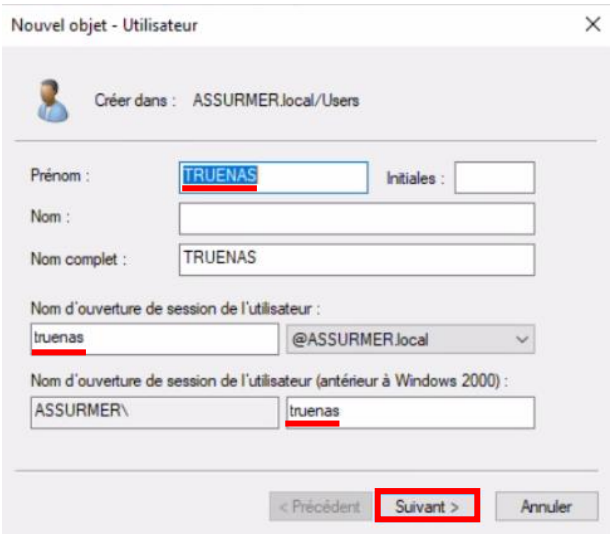
Vous voici alors sur la page d'accueil de TrueNAS.

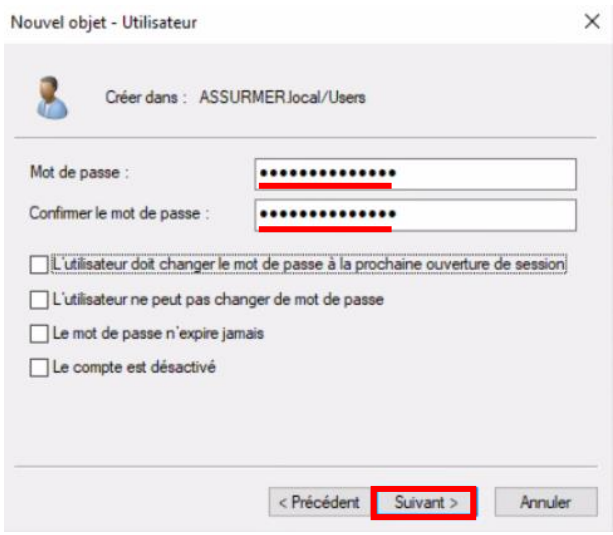


La prochaine étape sera, tout d'abord de créer un utilisateur dans notre Active Directory.
Rendez-vous dans votre AD et créez un utilisateur.
Cliquez droit dans une zone vide de votre fenêtre d'AD, puis « Nouveau » / « Utilisateur ».



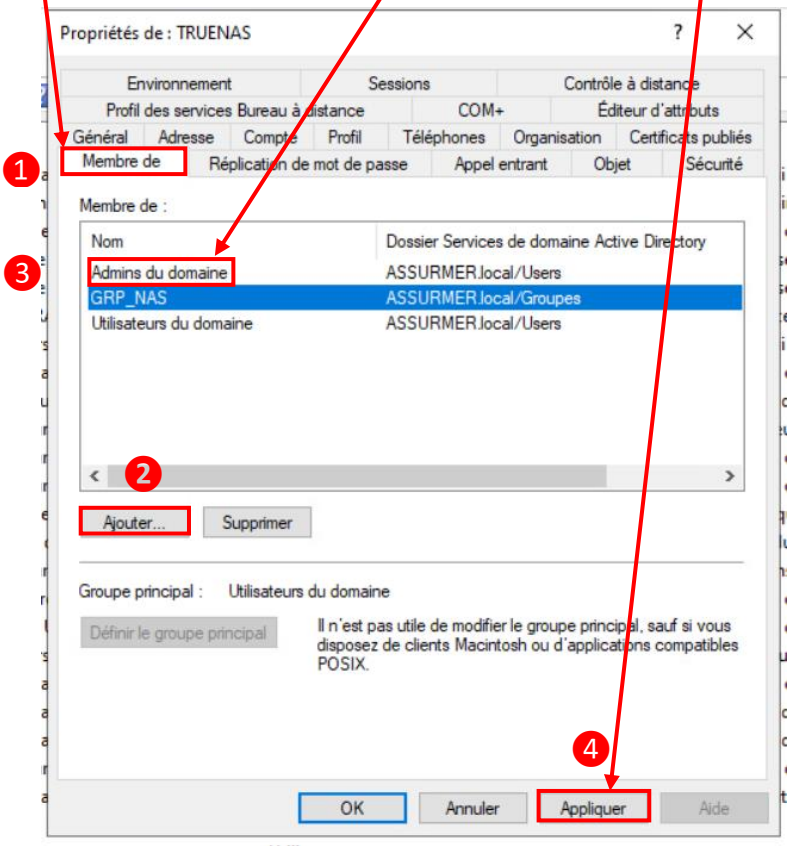
Ensuite, nous allons nommer notre nouvel utilisateur pour Truenas avec son propre nom d'utilisateur ainsi que son mot de passe.





Ensuite, nous allons ajouter notre utilisateur dans les groupes qui nous intéressent.

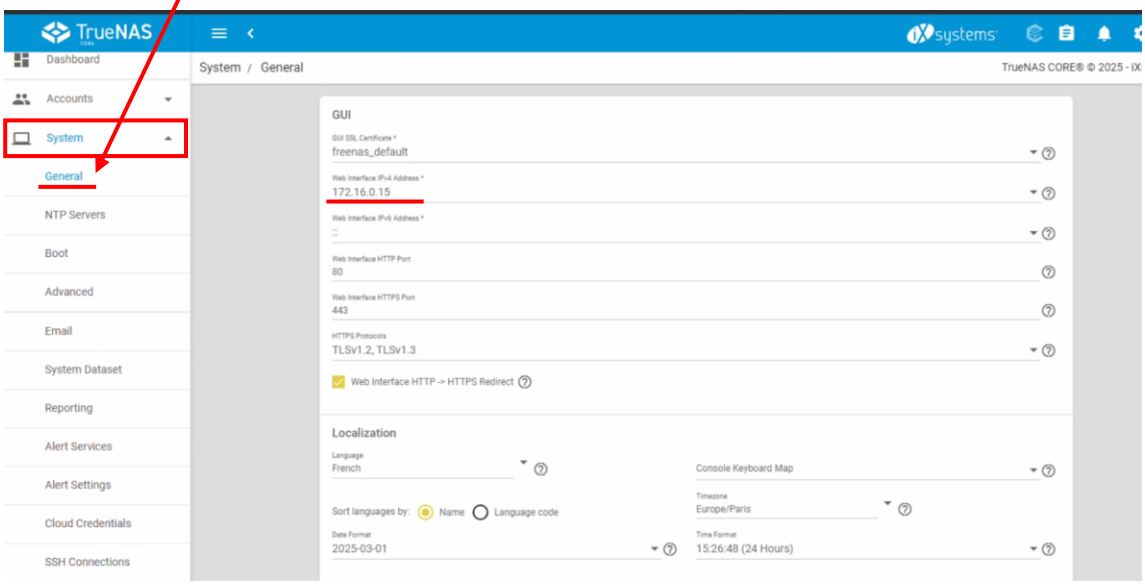
Ouvrez les propriétés de votre utilisateur.
Dans l'onglet « Membre de », ajoutez l'utilisateur dans les groupes nécessaires.
Dans notre cas, nous choisirons surtout « Admins du domaine ». Puis validez.



Nous avons besoin d'avoir un utilisateur Admin afin que TrueNAS puisse accéder à notre AD afin de mieux gérer les groupes et utilisateur pour les partages.

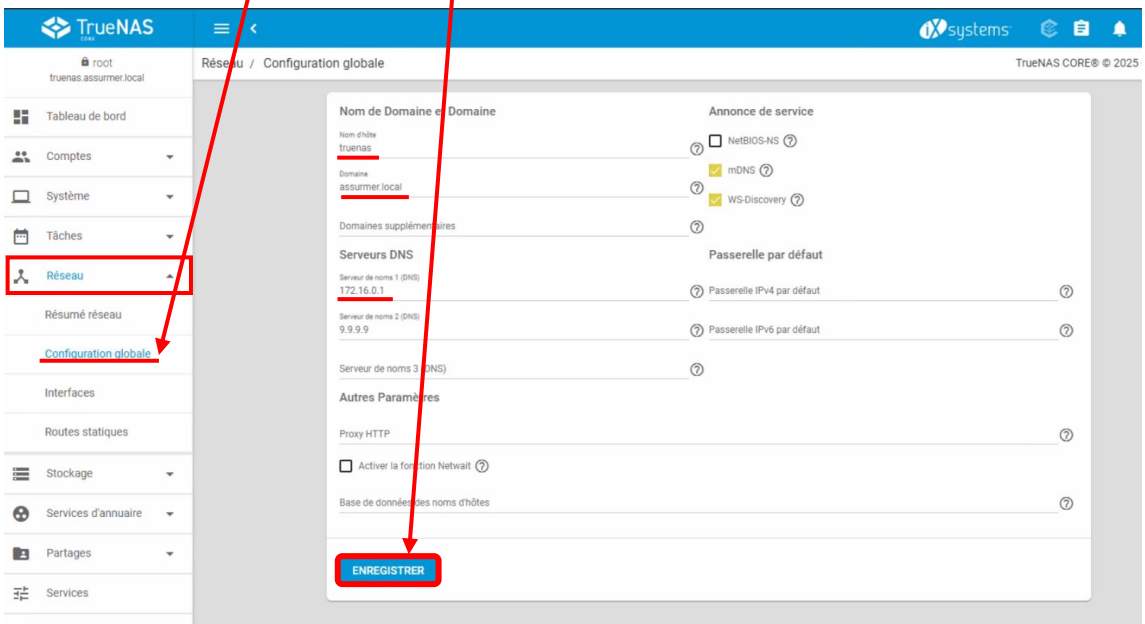
Retournez sur votre interface TrueNAS.
Modifiez l'adresse IPV4 afin d'attribuer une IP fixe à notre serveur NAS
Vous pouvez également en profiter pour modifier la langue, l'interface, l'heure de votre NAS.

Allez dans Système / Général :



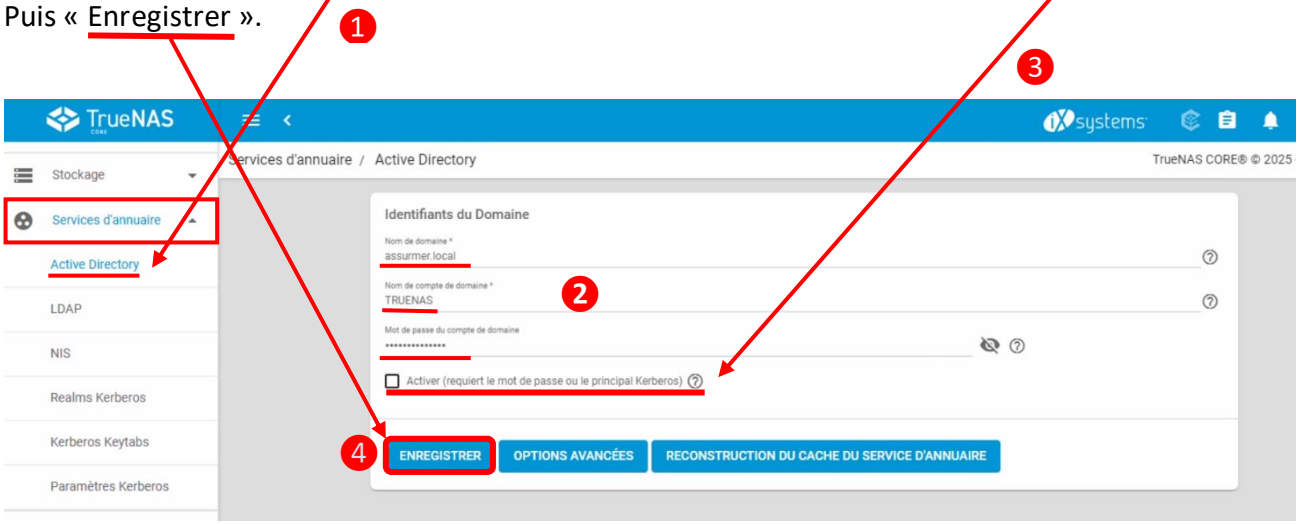
Ensuite, rendez-vous dans Réseau/Configuration globale. Rentrez-y le nom de votre serveur TrueNAS, le nom de votre domaine ainsi que le serveur DNS associé.

Ensuite, validez en cliquant sur « Enregistrer ».

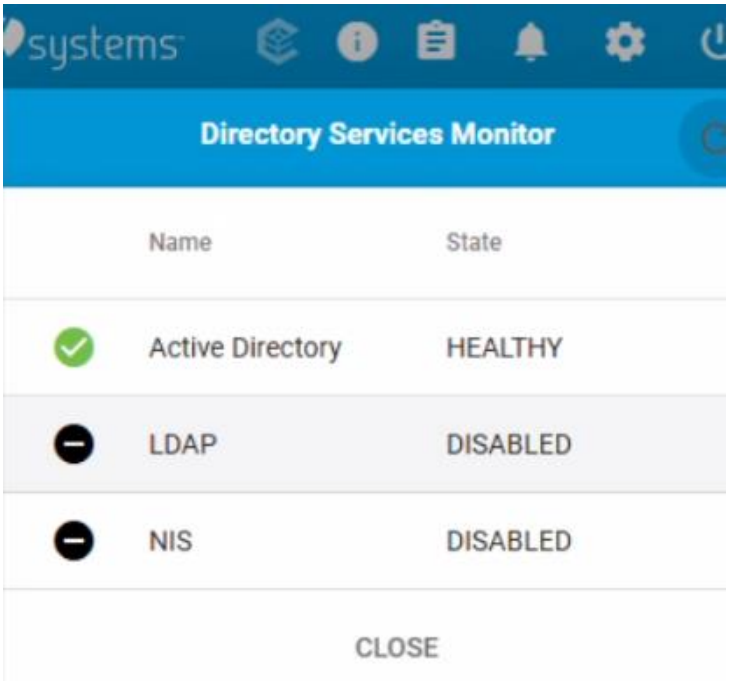


Désormais, nous allons joindre le serveur au domaine.

Dans la rubrique Service d'annuaire / Active Directory, rentrez le nom de domaine, le nom d'utilisateur créé pour l'occasion dans l'AD et son mot de passe. Cliquez sur « Activer » Puis « Enregistrer ».

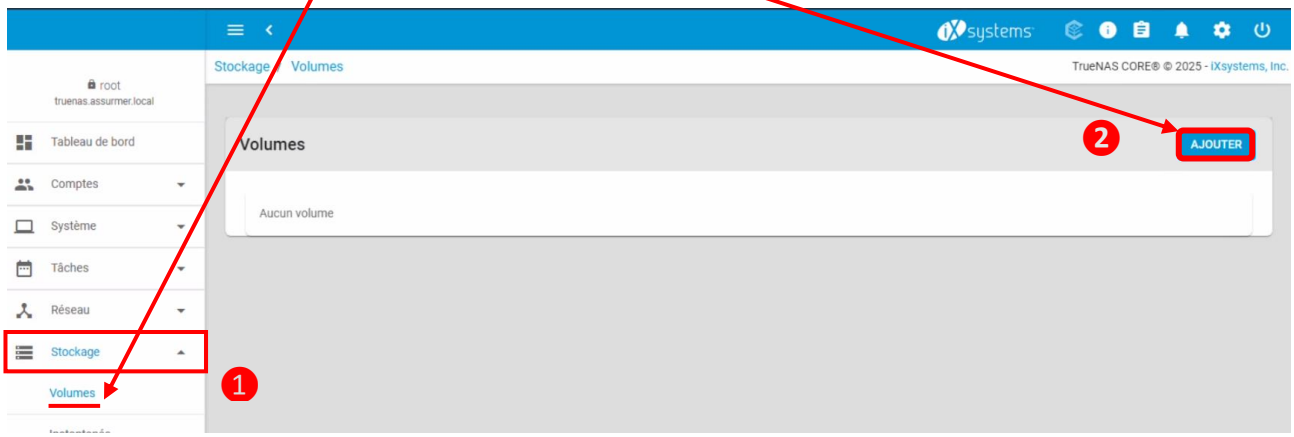


Vous aurez, en haut à droite de votre interface, une fenêtre qui vous permettra de voir l'état de la connexion à votre AD.



Désormais notre NAS est bien relié à notre Active Directory.

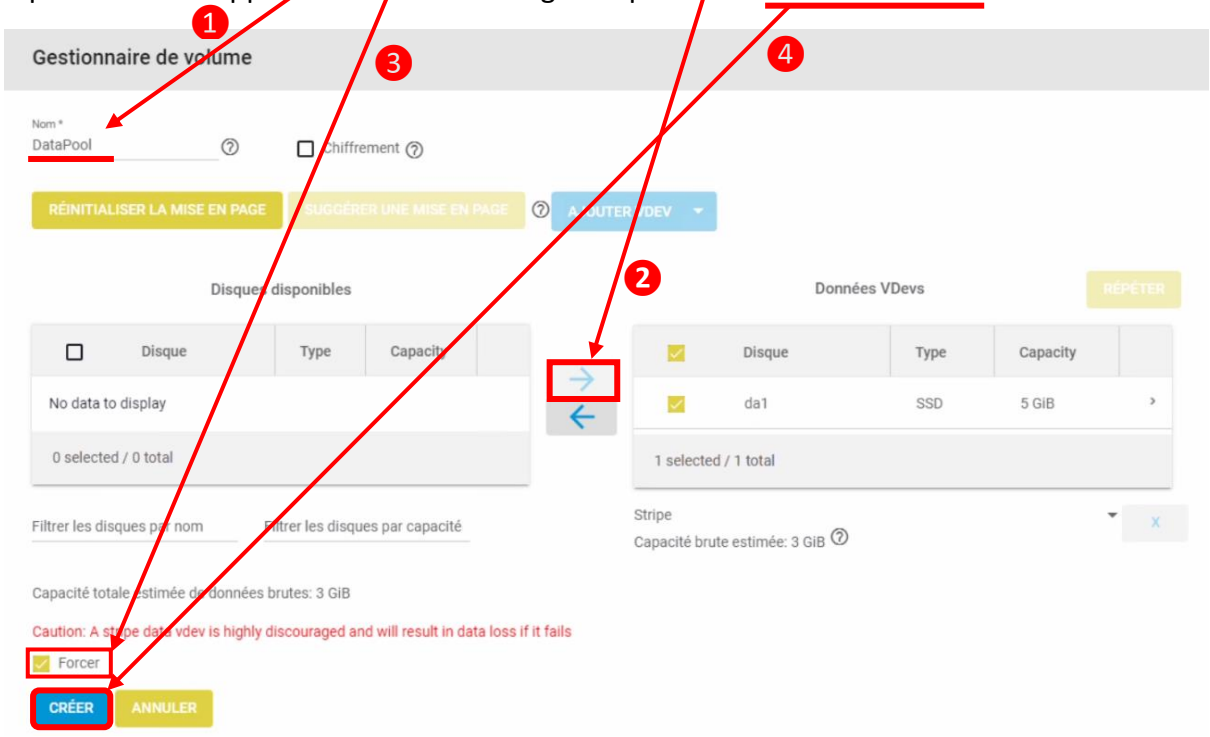
Désormais nous allons créer un Volume de donnée, ou « Pool »
Allez dans Stockage/Volumes et cliquez sur « Ajouter »



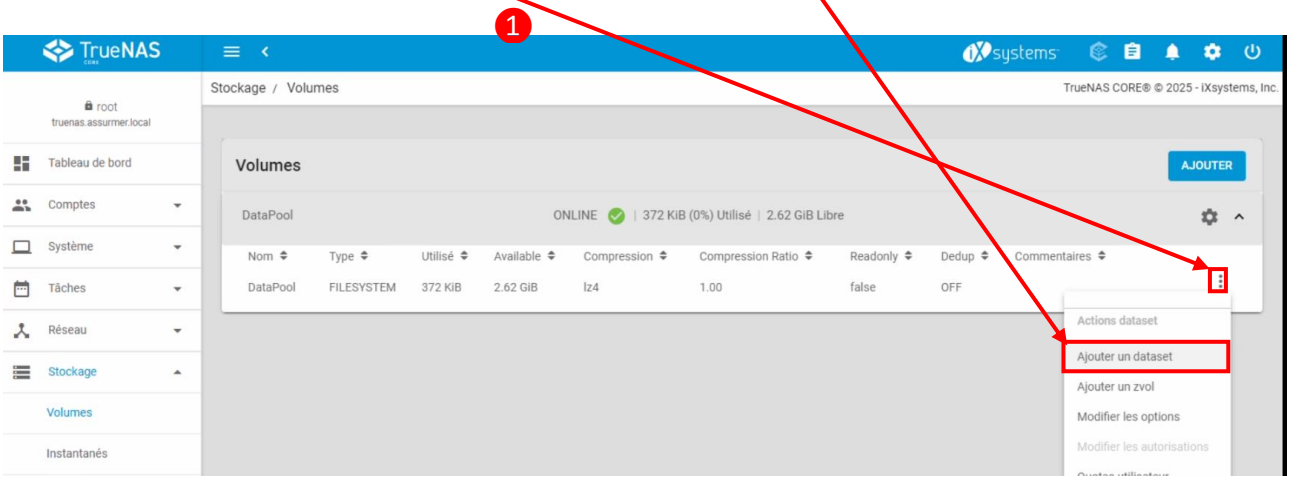
Pour le bien de la démonstration, nous avons un disque virtuel de 5Go.

Tout d'abord, nommez-le (par ex : DataPool). Déplacez-le sur la droite grâce aux flèches.

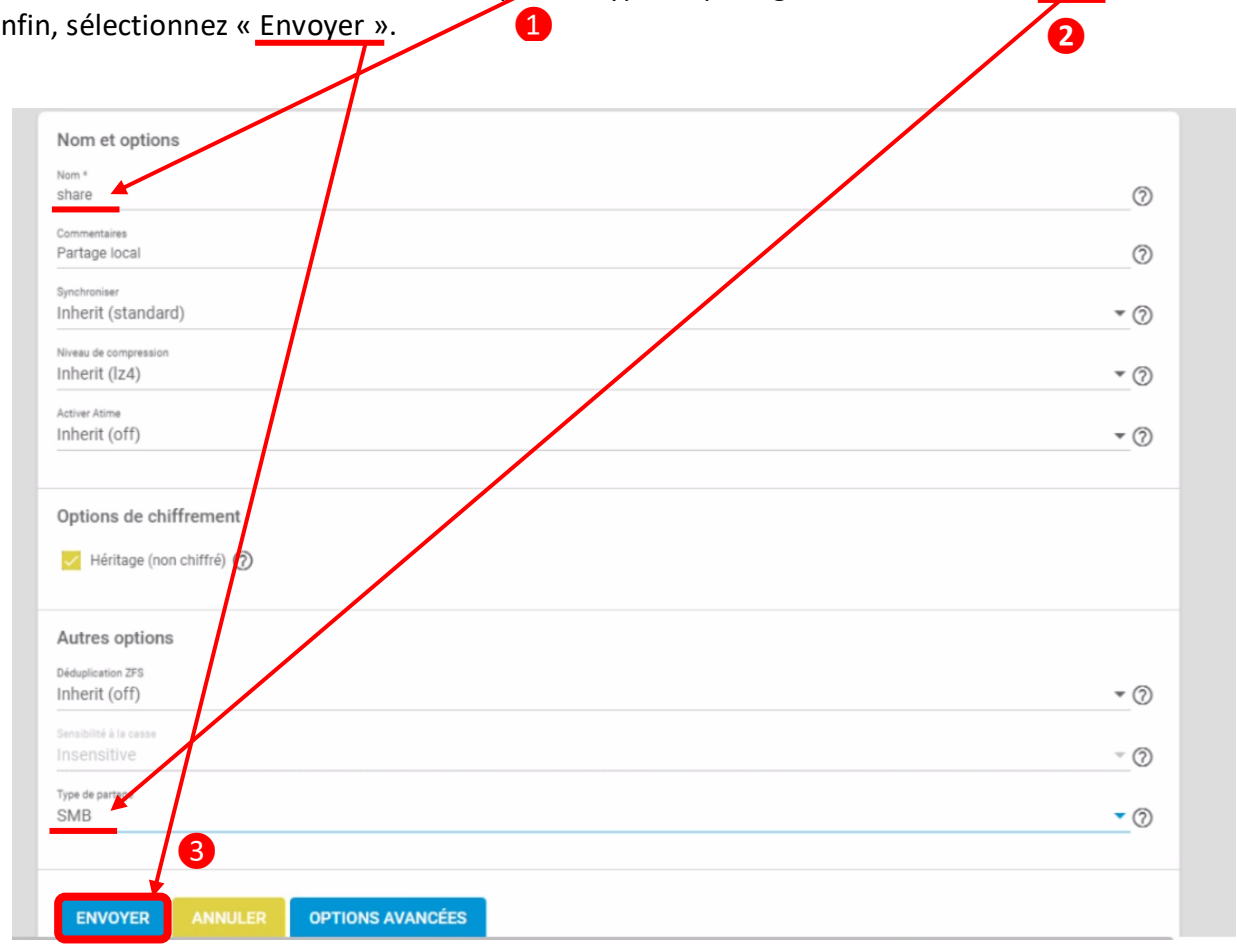
Dans notre cas, nous avons à « forcer » la création et confirmer que nous prenons en compte le fait que tout sera supprimé sur notre stockage. Cliquez sur « Créer un volume ».



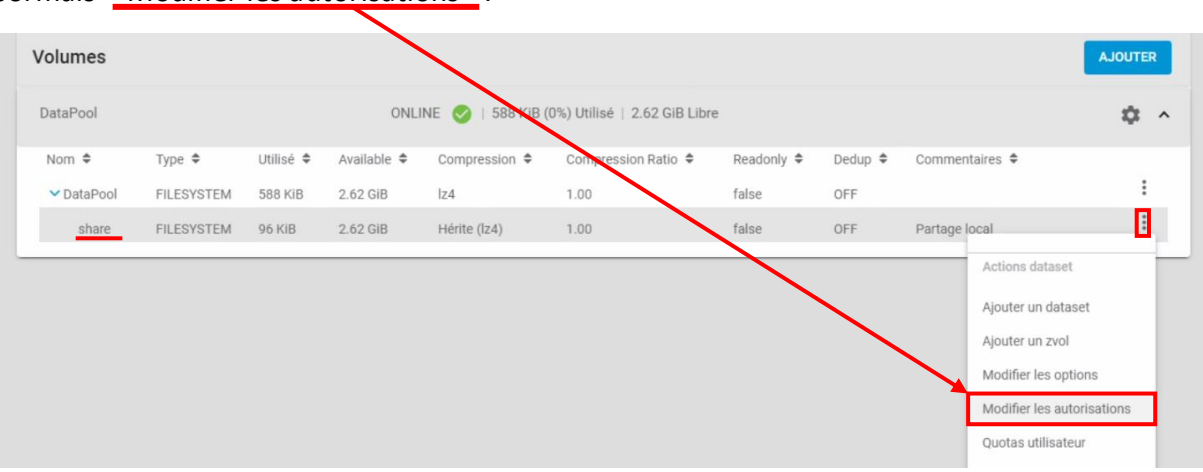
Ensuite, nous allons ajouter un « dataset », soit l'équivalent d'un dossier, que nous pourrons partager, ou non. Cliquez sur les 3 points à droite puis « Ajouter un dataset ».



Nous allons nommer notre Dataset (par ex : share), vous pouvez ajouter un commentaire pour décrire brièvement son utilité. Ensuite, pour le type de partage, nous voulons du SMB.
Enfin, sélectionnez « Envoyer ».

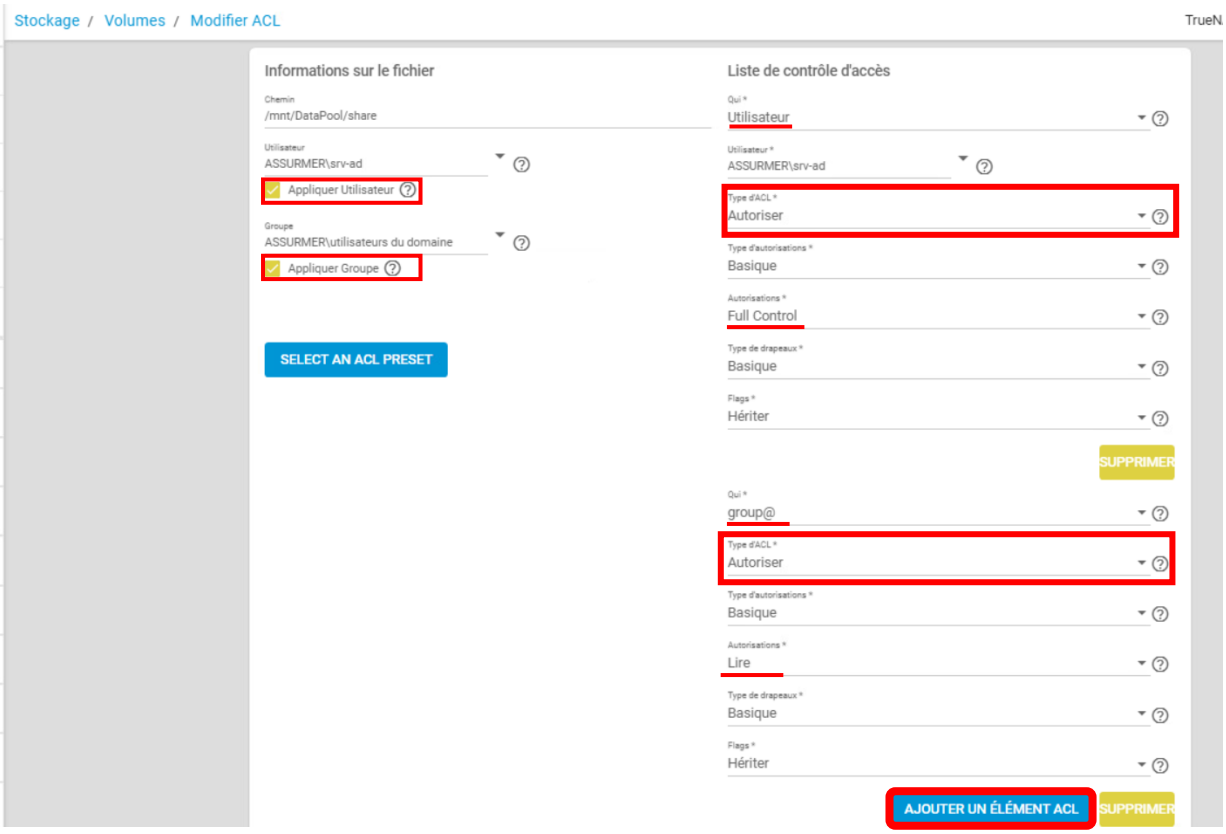


Une fois de retour dans notre page de volumes, nous avons bien notre « share » et allons désormais « Modifier les autorisations ».



Cette étape est très importante, nous allons déterminer les autorisations, via les ACL.

L'utilisateur est celui (utilisateur ou groupe) considéré comme propriétaire du dossier.
Groupe, est le groupe de sécurité autorisé à accéder/interagir avec le dossier.



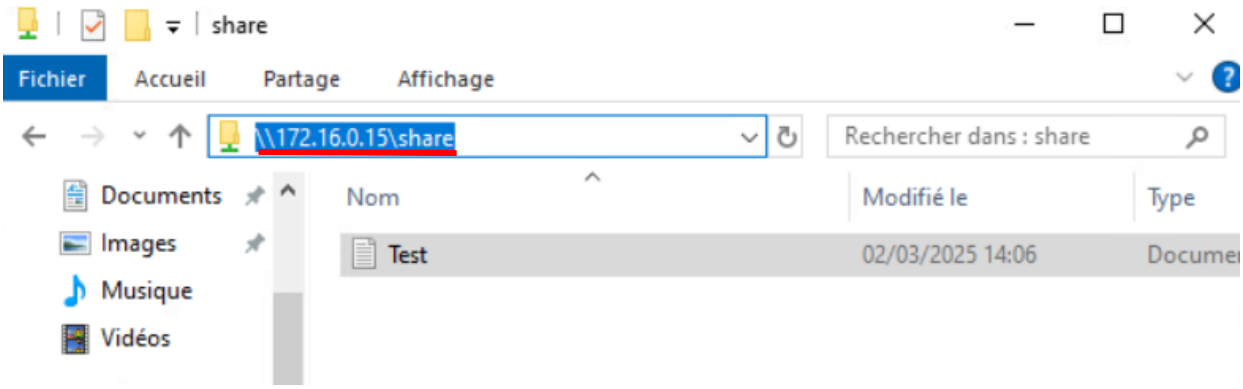
Ensuite, pour nos tests, sur la partie gauche, comme à droite, nous avons deux éléments d'ACL, d'abord, l'utilisateur, que nous avons désigné comme étant propriétaire du dossier avec comme autorisation « Full Control ».
Pour le groupe, nous avons choisi « Utilisateurs du domaine » avec les mêmes réglages (à gauche) mais seulement la capacité de « lire ».

Une fois validé, vous aurez donc un partage disponible sur l'adresse suivante, en SMB soit *ip_du_nas*\share.

Phase de testing

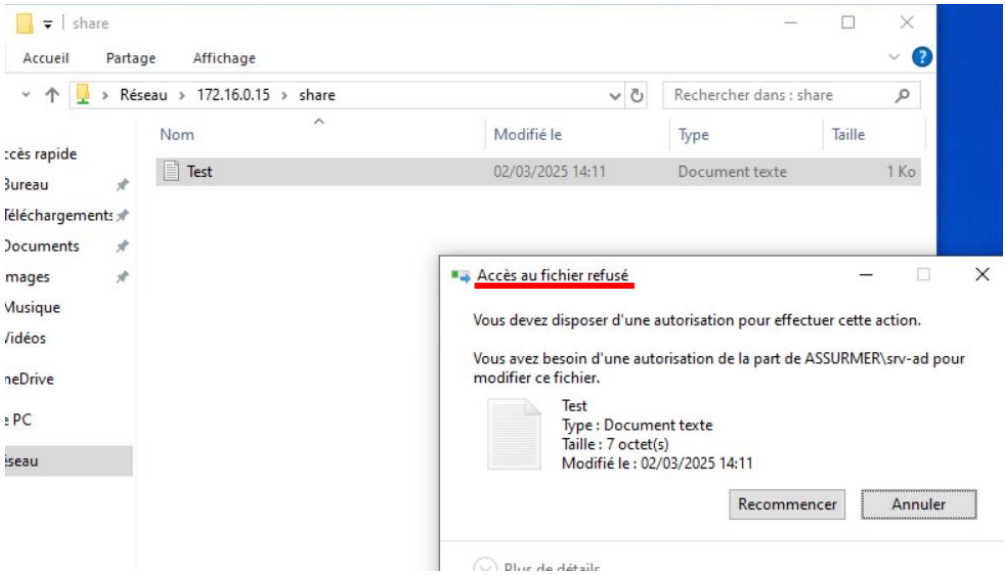
Maintenant que tout est en place, nous pouvons tester le bon fonctionnement de la restriction. Grâce au compte Admin « SRV-AD » nous avons pu ajouter un fichier de texte « Test.txt » dans ce dossier partagé.

Ensuite, dans une machine de test virtualisée, nous avons connectés une machine au domaine et connecté un utilisateur du domaine.
Ensuite nous allons sur notre partage, comme présenté ci-dessous :



Puisque nous sommes authentifiés avec un utilisateur du domaine, le dossier apparait sans avoir à retaper d'identifiants.

Désormais, le texte peut s'ouvrir, mais si nous essayons de le supprimer, soit, modifier l'intégrité et la disponibilité du fichier, nous serons alors dans l'impossibilité de supprimer le fichier.



Cela prouve que nous n'avons que le droit de lecture mais pas de modification.

Note aux utilisateurs

Chers utilisateurs,

Dans le cadre de notre engagement à vous offrir un environnement de travail toujours plus sécurisé et fiable, nous mettons en place une solution de stockage de données sur un serveur NAS (Network Attached Storage). Cette démarche a pour objectif de garantir la sécurité et la disponibilité de vos données professionnelles, tout en répondant aux normes les plus strictes en matière de protection des informations.

Pourquoi cette solution ?

Les données que vous manipulez chaque jour sont cruciales pour le bon fonctionnement de l'entreprise. Qu'il s'agisse de documents, de rapports ou de tout autre fichier professionnel, leur intégrité doit être préservée. En cas de panne de système, de perte accidentelle ou de cyberattaque, il est vital de pouvoir récupérer rapidement vos fichiers sans compromettre la sécurité.

C'est pourquoi nous avons décidé de mettre en place un NAS qui centralisera toutes les données sur un support sécurisé et de mettre en œuvre plusieurs niveaux de protection :

- ***Sauvegardes régulières** pour éviter toute perte de données.*
- ***Cryptage des informations sensibles** pour garantir leur confidentialité.*
- ***Contrôle d'accès rigoureux** pour s'assurer que seules les personnes autorisées peuvent accéder à certaines informations.*

Comment cela fonctionne-t-il ?

À partir du moment où vous stockez vos fichiers sur le NAS, plusieurs mécanismes de sécurité se déclenchent automatiquement :

- ***Accès restreint** : Vous n'aurez accès qu'aux données dont vous avez besoin pour votre travail. L'accès à des informations sensibles sera limité à certains utilisateurs en fonction de leur rôle.*
- ***Sauvegardes automatiques** : Tous les fichiers seront régulièrement sauvegardés. En cas de problème, nous pourrons restaurer vos données rapidement et facilement.*
- ***Cryptage des données** : Pour protéger vos fichiers, ceux-ci seront cryptés. Cela signifie qu'en cas de vol ou de perte du support, les données ne seront pas accessibles sans la clé de décryptage.*

Votre collaboration et votre vigilance sont essentielles pour garantir le succès de cette nouvelle solution. Nous vous encourageons à respecter les règles d'accès et de stockage des données et à signaler toute anomalie dès que vous en avez connaissance.

Nous vous remercions pour votre compréhension et votre coopération.

Bien cordialement,
L'équipe IT d'Assurmer

Mise en place d'une veille informationnelle sur TrueNAS

Mise en place d'une veille informationnelle automatisée sur TrueNAS

Afin de garantir la sécurité continue de notre serveur NAS TrueNAS, nous mettons en place une veille informationnelle automatisée. Cette solution nous permettra de suivre de manière proactive les mises à jour, les failles de sécurité (CVE) et les alertes importantes, sans nécessiter de surveillance manuelle constante.

Objectif de la veille automatisée

L'objectif principal est de :

- Suivre automatiquement les vulnérabilités et mises à jour de sécurité pour TrueNAS.
- Assurer une gestion rapide des risques sans intervention manuelle.
- Garantir une réactivité instantanée en cas de menace ou de mise à jour critique.

Outils utilisés pour la veille automatisée

Pour rendre cette veille entièrement automatisée, nous utiliserons plusieurs outils :

- **Flux RSS** : TrueNAS propose des flux RSS qui nous informeront directement des nouvelles mises à jour et alertes de sécurité. Ces informations seront envoyées automatiquement à notre système de gestion des alertes.
- **Suivi des CVE** : Grâce à des outils comme **CVE Search**, nous suivrons automatiquement les vulnérabilités affectant TrueNAS. Ces informations seront intégrées dans un tableau de bord qui nous alertera dès qu'une vulnérabilité critique est détectée.
- **Mises à jour automatiques** : Nous configurerons des mises à jour automatiques pour appliquer rapidement les patchs de sécurité dès leur disponibilité.
- **Alertes par e-mail** : Dès qu'une vulnérabilité ou mise à jour importante est identifiée, nous recevrons une alerte par e-mail, nous permettant d'agir immédiatement.

Actions après réception des alertes

Lorsque nous recevons une alerte :

1. **Évaluation automatique** : L'outil analysera la gravité de la vulnérabilité et priorisera les actions à entreprendre.
2. **Mise à jour** : Si nécessaire, une mise à jour de sécurité sera automatiquement appliquée.
3. **Vérification** : Des tests automatisés seront effectués pour s'assurer que le système est toujours fonctionnel après la mise à jour.

Cette veille automatisée nous permettra de garantir la sécurité de notre serveur NAS en toute simplicité. Grâce à ces outils, nous serons en mesure de répondre rapidement aux nouvelles vulnérabilités, tout en minimisant les interventions manuelles. Cela assurera la protection continue de nos données de manière efficace.

Planning

STATUT	NOM DE LA TÂCHE	Début de la tâche	FAIT PAR
Terminée	Planning de travail et des tâches	9 février 2025	Elise
Terminée	Fonctionnalités principales d'un NAS dont chiffrage et sécurité des données	11 février 2025	Elise
Terminée	Comparaison des différentes solutions RAID et présentation de votre solution retenue	12 février 2025	Elise / Stéphane
Terminée	Procédure d'installation et de configuration de la solution NAS choisie	19 février 2025	Stéphane
Terminée	Testing de la solution	25 février 2025	Stéphane
Terminée	Document d'accompagnement utilisateur	29 février 2024	Stéphane / Elise
Terminée	Veille (outils et résultats) concernant la solution retenue	01 mars 2025	Stéphane / Elise