

Table des matières

Table des matières	1
Prérequis	1
Déploiement du NAS.....	2
1) Installation de TrueNAS	2
2) Configuration de la carte réseau	4
3) Configuration de TrueNAS	7
4) Configuration d'un volume avec RAID.....	9
5) Ajout du NAS au domaine Active Directory	12
6) Création des datasets	14
7) Modification des ACL pour les 3 datasets.....	18
a) Dossier public (Commun)	18
b) Dossier Groupe de sécurité	19
c) Dossier nominatif.....	21
8) Création de Partages.....	24
9) Configuration des lecteurs réseaux	27

Prérequis

- L'ISO TrueNAS <https://www.truenas.com/download-truenas-core/> - Une machine virtuelle avec au moins 3 disques en SATA et 8Go de RAM (Minimum recommandé pour du RAID 5/6).

Déploiement du NAS

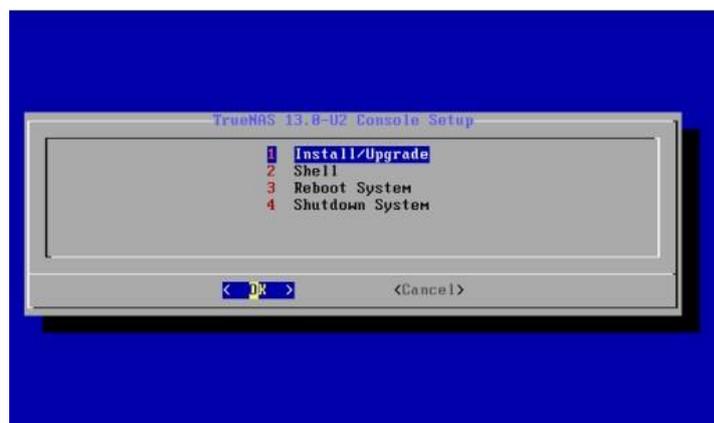


1) Installation de TrueNAS

- Une fois la machine virtuelle lancée, choisir l'option 1 « Boot TrueNAS Installer » en appuyant sur « Entrée ».



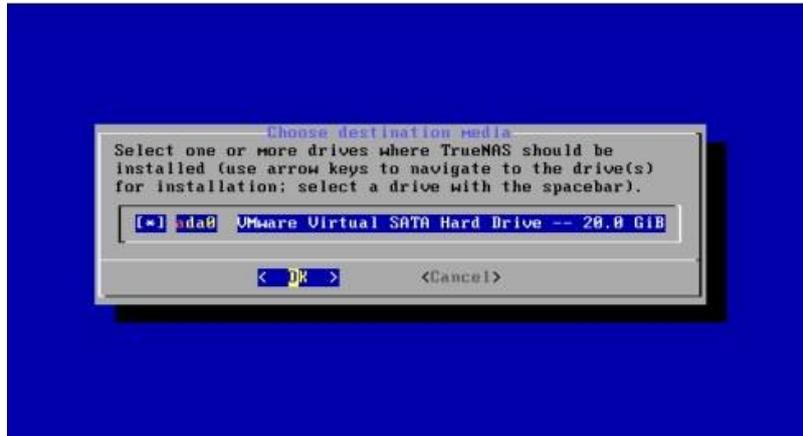
- Choisir l'option 1 « Install/Upgrade » pour démarrer l'installation.



- Le NAS peut fonctionner avec moins de 8Go de RAM mais ce n'est pas recommandé. Choisir « Yes » pour continuer l'installation.



- Sélectionner le disque cible sur lequel TrueNAS sera installé (Ici, le disque principal de la machine) en appuyant sur « Espace ». Puis sélectionner « OK ».



- Choisir « Yes » pour formater le disque.



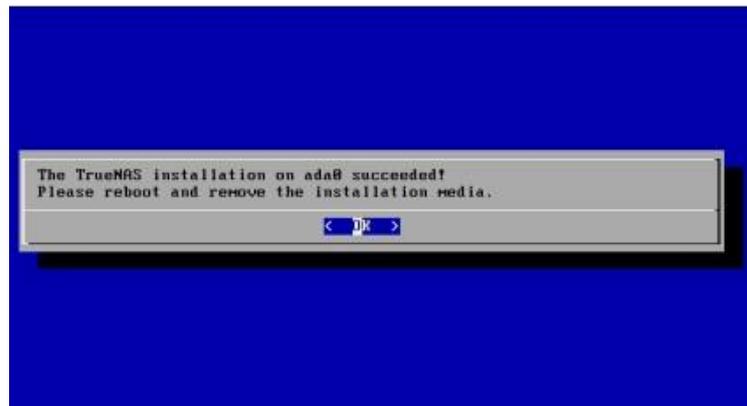
- Renseigner le mot de passe root qui servira à accéder à la console de TrueNAS (ATTENTION, le clavier est en QWERTY).



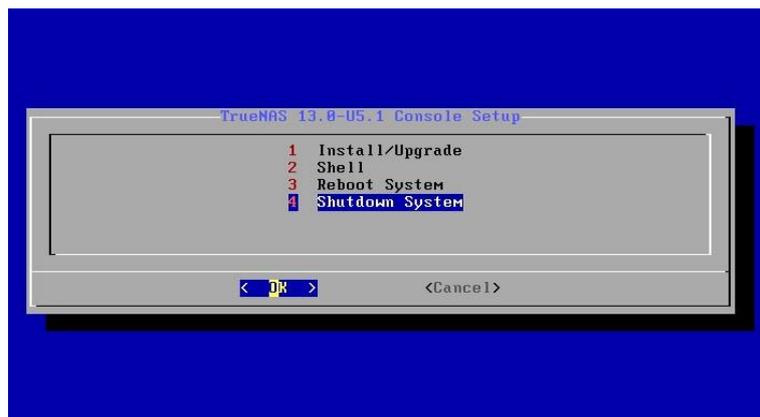
- Choisir « BOOT via BIOS ». Celui-ci est plus stable que le BOOT UEFI.



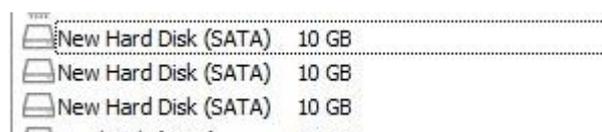
- Cliquer sur « OK » après la fin de l'installation de TrueNAS. La machine va redémarrer.



- Cliquer sur « Shutdown System ».



- Ajouter les disques SATA qui serviront d'unité de stockage pour le NAS.



2) Configuration de la carte réseau

Nous allons maintenant configurer la carte réseau de TrueNAS pour pouvoir y accéder via son interface WEB.

- Après redémarrage, écrire « 1 » pour accéder aux paramètres de l'interface réseau. (Attention clavier en QWERTY).



```
FreeBSD/amd64 (truenas.local) (ttyv0)
```

```
Console setup
```

```
1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset Root Password
8) Reset Configuration to Defaults
9) Shell
10) Reboot
11) Shut Down
```

```
The web user interface is at:
```

```
http://0.0.0.0
https://0.0.0.0
```

```
Enter an option from 1-11: █
```

- Choisir l'interface em0 avec l'option « 1 ».

```
Enter an option from 1-11: 1
```

```
1) em0
```

```
Select an interface (q to quit): 1 █
```

- Si demandé, écrire « n » pour ne pas supprimer l'interface.

```
Delete interface? (y/n) n █
```

- Taper « n » pour ne pas supprimer les paramètres par défaut de l'interface.

```
Remove the current settings of this interface? (This causes a momentary disconnection of the network.) (y/n) n █
```

- Ecrire « n » pour ne pas configurer l'interface en DHCP. Nous le faisons manuellement ici avec une adresse IP statique.

```
Configure interface for DHCP? (y/n) n █
```

Nous allons maintenant configurer l'adresse IP.

- Mettre « y » pour configurer l'IPv4.

```
Configure IPv4? (y/n) y █
```

- Ajouter un nom à l'interface (ici « NAS »).

```
Interface name [hh1]:Nas █
```



- Configurer l'adresse IP en fonction du plan d'adressage d'Assurmer (172.16.0.15/24).

```
Several input formats are supported
Example 1 CIDR Notation:
  192.168.1.1/24
Example 2 IP and Netmask separate:
  IP: 192.168.1.1
  Netmask: 255.255.255.0 /24 or 24
IPv4 Address:172.16.0.15/24
Saving interface configuration: Ok
```

- Ne pas configurer l'IPv6. Mettre « n ».

```
Configure IPv6? (y/n) n
```

Nous allons maintenant déclarer le serveur DNS.

- Taper 6 pour configurer le DNS.

6) Configure DNS

```
Enter an option from 1-11: 6
```

- Renseigner le domaine « assurmer.fr », et les serveurs DNS (172.16.0.1 et 172.16.0.9).

```
Enter an option from 1-11: 6
DNS Domain [local]:assurmer.fr
Enter nameserver IPs, an empty value ends input
DNS Nameserver 1:172.16.0.1
DNS Nameserver 2:172.16.0.9
```

- Valider en appuyant sur « Entrée ».
- Appuyer ensuite sur « 4 » pour configurer la passerelle par défaut.

4) Configure Default Route

- Ecrire « y » pour ajouter la passerelle.

```
Configure IPv4 Default Route? (y/n)y
```

```
IPv4 Default Route:172.16.0.254
```

- Ne pas configurer l'IPv6. Mettre « n ».

```
Configure IPv6 Default Route? (y/n)n
```

La configuration de la carte réseau est terminée.



A partir d'un poste client, se connecter à l'interface web du NAS en renseignant l'adresse IP du NAS pour commencer sa configuration.

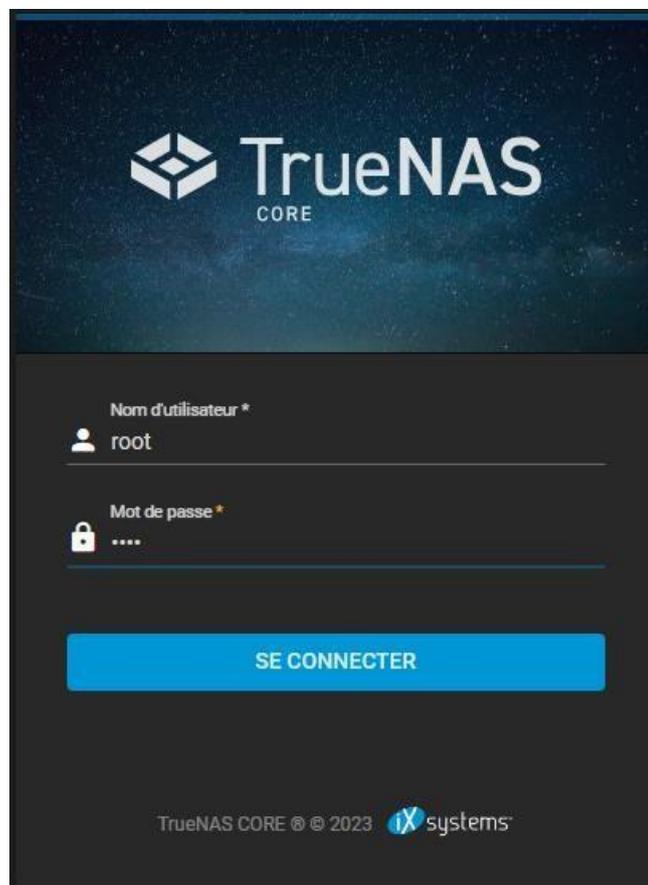
The web user interface is at:

http://172.16.0.15

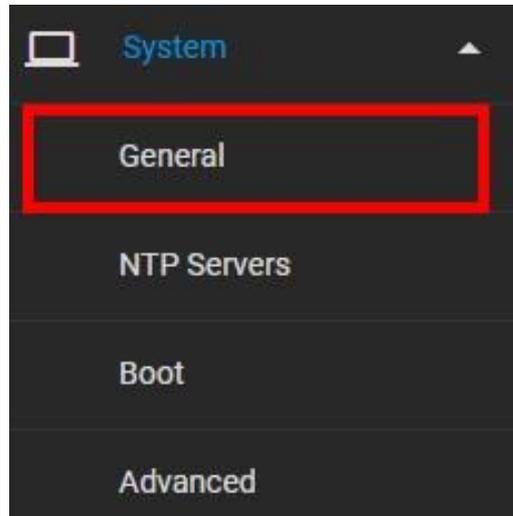
https://172.16.0.15

3) Configuration de TrueNAS

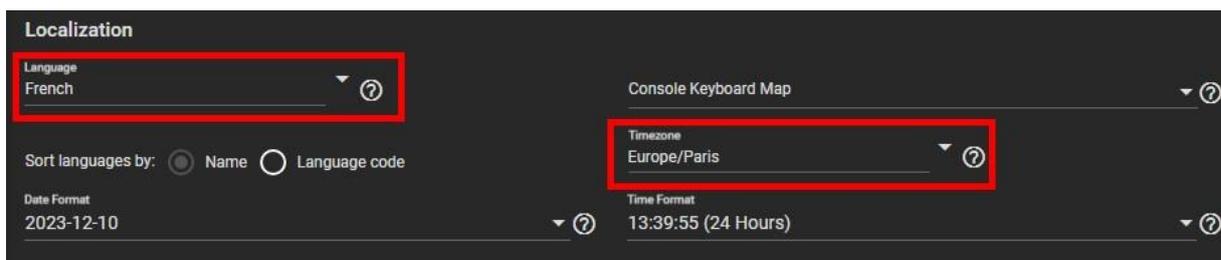
- Sur un poste client, se connecter au NAS avec l'adresse <http://172.16.0.15/>
- Se connecter avec les identifiants créés précédemment : root/motdepasse



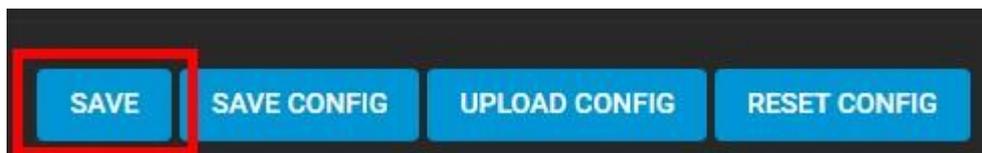
- Changer la langue en cliquant sur « System » puis « General ».



- Cliquer ensuite sur « Language » et « Timezone » puis mettre « French » et « Europe/Paris ».

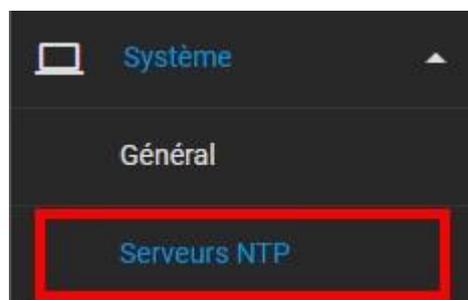


- Cliquer sur « Save » pour appliquer les paramètres.



Nous allons maintenant supprimer les serveurs NTP (Network Time Protocol) par défaut car ils peuvent être à l'origine de certains problèmes pour la liaison Active Directory.

- Cliquer sur « Système » puis « Serveurs NTP ».



- Supprimer les 3 serveurs présents par défaut.



se	Burst	IBurst	Prefer	Poll Min	Poll Max	
bsd.pool.ntp.org	non	oui	non	6	10	...
bsd.pool.ntp.org	non	oui	non	6	10	...
bsd.pool.ntp.org				6	10	...

Supprimer

Delete NTP Server 0.freebsd.pool.ntp.org?

Confirmer

- Cliquer sur « Ajouter ».

Adresse	Burst	IBurst	Prefer	Poll Min	Poll Max
No data to display					

- Paramétrer un nouveau serveur NTP avec notre contrôleur de domaine ASFRDC01.

Paramètres du Serveur NTP

Adresse: ASFRDC01.assumerer.fr

Burst ?

IBurst ?

Prefer ?

Poll Min: 6 Poll Max: 10

Forcer ?

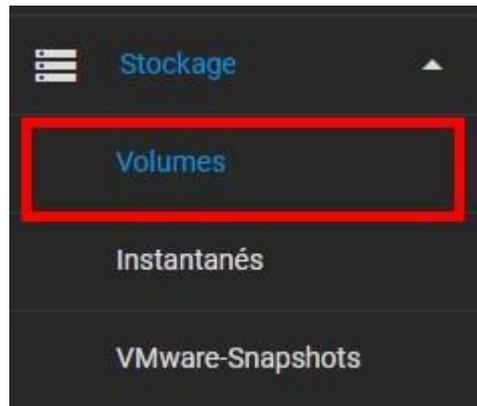
Notre NAS est désormais synchronisé avec notre contrôleur de domaine.

4) Configuration d'un volume avec RAID

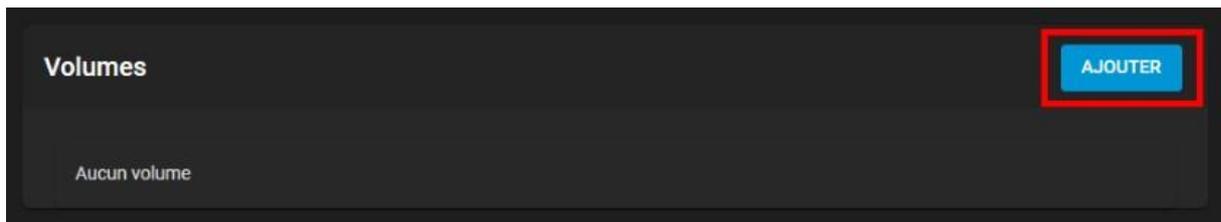
Nous allons maintenant créer notre premier volume de stockage/pool (regroupement de plusieurs disques physiques en une seule unité logique).



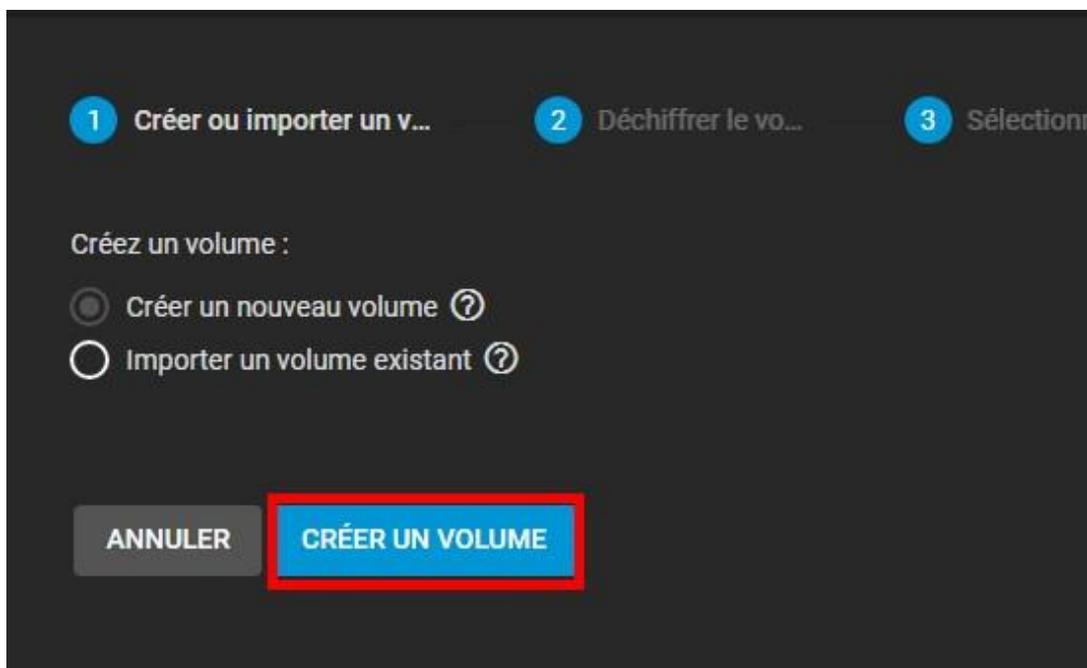
- Cliquer sur « Stockage » puis « Volumes ».



- Cliquer sur « Ajouter ».



- Sélectionner « Créer un volume ».



- Donner un nom au volume et sélectionner les 3 HDD de la machine.



Gestionnaire de volume

Nom*
Volume1 ? Chiffrement ?

RÉINITIALISER LA MISE EN PAGE SUGGÉRER UNE MISE EN PAGE ? AJOUTER VDEV ▼

Disques disponibles

<input checked="" type="checkbox"/>	Disque	Type	Capacity	
<input checked="" type="checkbox"/>	ada0	SSD	10 GiB	>
<input checked="" type="checkbox"/>	ada1	SSD	10 GiB	>
<input checked="" type="checkbox"/>	ada2	SSD	10 GiB	>

3 selected / 3 total

Filter les disques par nom Filter les disques par capacité

- Placer les disques dans « VDevs » en cliquant sur la flèche. Cela signifie « Virtual Devices ».

Données VDevs

RÉPÉTER

<input type="checkbox"/>	Disque	Type	Capacity	
<input type="checkbox"/>	ada0	SSD	10 GiB	>
<input type="checkbox"/>	ada1	SSD	10 GiB	>
<input type="checkbox"/>	ada2	SSD	10 GiB	>

0 selected / 3 total

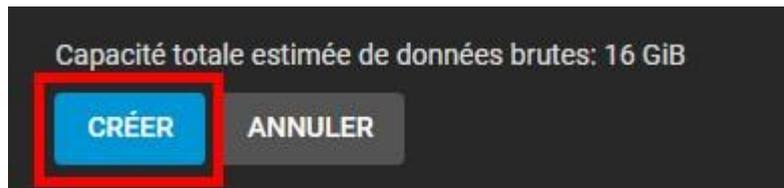


Choisir le mode de « RAID ». Ici, nous avons choisi le RAID-z qui correspond au RAID 5.

Les modes « Raid-z » et « Raid-z2 » offrent les meilleures performances mais sont plus gourmands au niveau des ressources matérielles (processeur et RAM).



- Cliquer sur « Créer » pour créer le volume.



La capacité de stockage disponible par rapport à nos 3 disques de 10 GiB est de 16GiB avec le Raid-z.

- Le volume apparaît ensuite.

Volumes							
NAS							
		ONLINE 408 KiB (0%) Utilisé 7.27 GiB Libre					
Nom	Type	Utilisé	Available	Compression	Compression Ratio	Readonly	Dedup
NAS	FILESYSTEM	408 KiB	7.27 GiB	lz4	1.00	false	OFF

5) Ajout du NAS au domaine Active Directory

Nous allons désormais ajouter notre NAS à notre domaine pour pouvoir récupérer nos utilisateurs

- Cliquer sur « Services d'annuaire » puis « Active Directory ».



- Renseigner le nom de domaine et les credentials d'un compte administrateur du domaine.



Identifiants du Domaine

Nom de domaine *
assurmer.fr

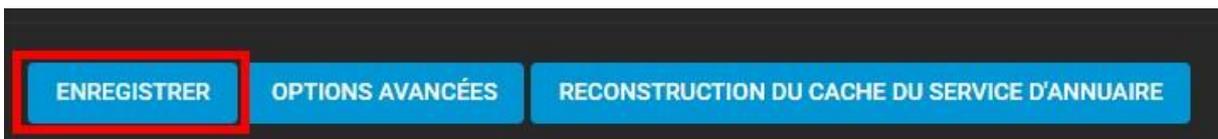
Nom de compte de domaine *
administrateur

Mot de passe du compte de domaine *

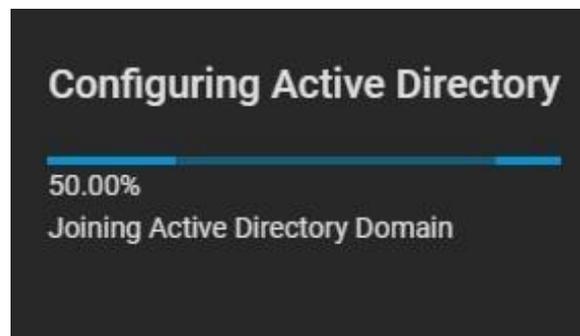
Activer (requiert le mot de passe ou le principal Kerberos)

ENREGISTRER OPTIONS AVANCÉES RECONSTRUCTION DU CACHE DU SERVICE D'ANNUAIRE

- Cliquer ensuite sur « Enregistrer ».



- Un pop-up va apparaître pour indiquer l'état d'avancement de la jointure. Une fois la jointure terminée, elle disparaît.



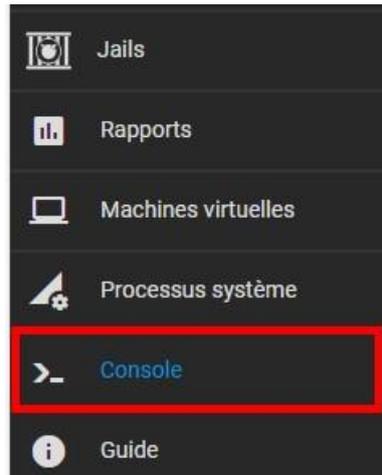
Sur notre Active Directory, notre NAS apparaît bien.

	Nom	Type	Description
Utilisateurs et ordinateurs Active Directory			
> Requetes enregistrees			
v assurmer.fr			
ASCOMPUTERS	ASFRFILE	Ordinateur	
Builtin	ASFRGW	Ordinateur	
Computers	TRUENAS	Ordinateur	
Domain Controllers			
ForeignSecurityPrincipal:			
HQ			
Managed Service Accour			
RDS			
Users			

Nous allons vérifier que nous pouvons bien récupérer la liste de nos utilisateurs.



- Cliquer sur l'onglet « Console » en bas du menu déroulant.



- Ecrire les commandes « wbinfo -g » et « wbinfo -u ».

Si la jointure a bien fonctionné, les commandes affichent les groupes de sécurité et les utilisateurs du domaine

```
root@truenas[~]# wbinfo -g
ASSURMER\ordinateurs du domaine
ASSURMER\contrôleurs de domaine
ASSURMER\administrateurs du schéma
ASSURMER\administrateurs de l'entreprise
ASSURMER\éditeurs de certificats
ASSURMER\admins du domaine
ASSURMER\utilisateurs du domaine
ASSURMER\invités du domaine
```

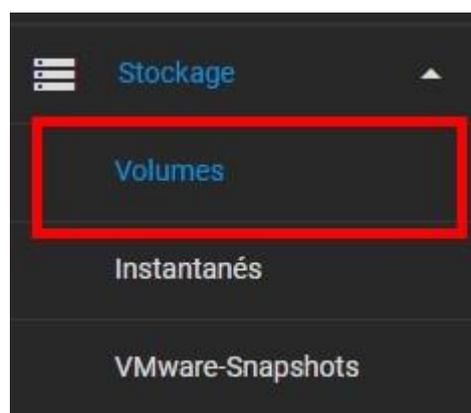
```
root@truenas[~]# wbinfo -u
ASSURMER\administrateur
ASSURMER\invité
ASSURMER\krbtgt
ASSURMER\chaudyl
ASSURMER\baugeax
root@truenas[~]#
```

6) Création des datasets

Les partages ou dossier réseau sur TrueNAS portent le nom de « dataset ».

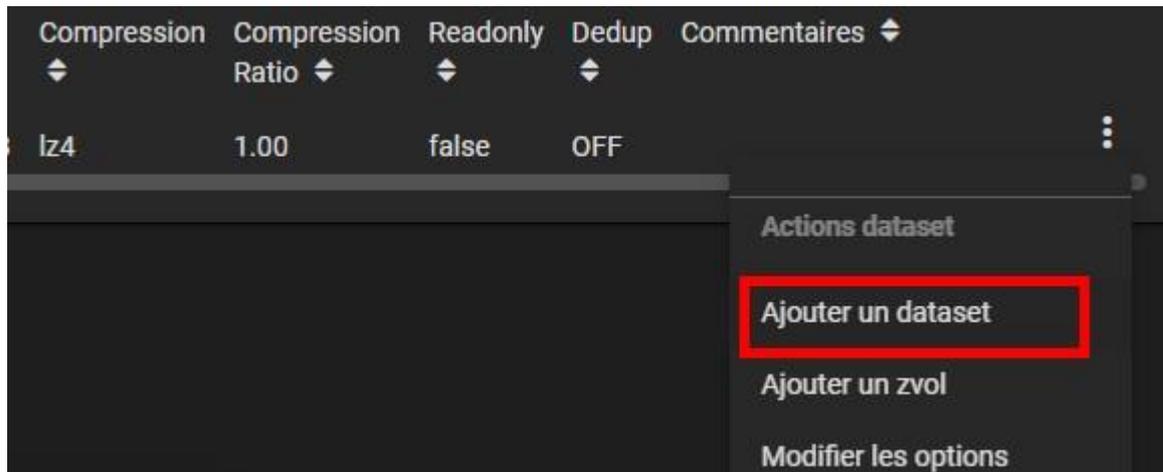
Nous allons donc créer notre premier dataset commun aux utilisateurs du domaine qui sera un partage public en lecture seule.

- Cliquer sur « Stockage » puis « Volumes ».





- Sur le volume précédemment créé, cliquer sur les 3 points à droite puis « Ajouter un dataset ».



Ajouter un nom et un commentaire. Mettre le type de partage en « SMB » et régler en « off » l'option « Activer Atime ».



Nom et options

Nom *
Public

Commentaires
Partage public

Synchroniser
Inherit (standard)

Niveau de compression
Inherit (lz4)

Activer Atime
off

Options de chiffrement

Héritage (non chiffré) ?

Autres options

Déduplication ZFS
Inherit (off)

Sensibilité à la casse
Insensitive

Type de partage
SMB

ENVOYER **ANNULER** **OPTIONS AVANCÉES**

- Cliquer ensuite sur « Envoyer ».
- Le dataset apparaît en dessous du volume directement.

Volume1		ONLINE ✔ 927.09 KiB (0%) Utilisé 15.16 GiB Libre						
Nom	Type	Utilisé	Available	Compression	Compression Ratio	Readonly	Dedup	Commentaires
Volume1	FILESYSTEM	927.09 KiB	15.16 GiB	lz4	1.00	false	OFF	
Public	FILESYSTEM	127.88 KiB	15.16 GiB	Hérite (lz4)	1.00	false	OFF	Partage public

Nous allons maintenant un dataset destiné à un utilisateur authentifié (un dossier nominatif) et un dataset lié à un groupe de sécurité (Un service par exemple).



- Créer le dataset « Utilisateurs » et « Service » en suivant le modèle cidessous.

Nom et options	Nom et options
Nom * Service	Nom * Utilisateurs
Commentaires Espace Service	Commentaires Espace Utilisateurs
Synchroniser Inherit (standard)	Synchroniser Inherit (standard)
Niveau de compression Inherit (lz4)	Niveau de compression Inherit (lz4)
Activer Atime off	Activer Atime off
Options de chiffrement <input checked="" type="checkbox"/> Héritage (non chiffré) ?	Options de chiffrement <input checked="" type="checkbox"/> Héritage (non chiffré) ?
Autres options Déduplication ZFS Inherit (off)	Autres options Déduplication ZFS Inherit (off)
Sensibilité à la casse Insensitive	Sensibilité à la casse Insensitive
Type de partage SMB	Type de partage SMB
ENVOYER ANNULER OPTIONS AVANCÉES	ENVOYER ANNULER OPTIONS AVANCÉES

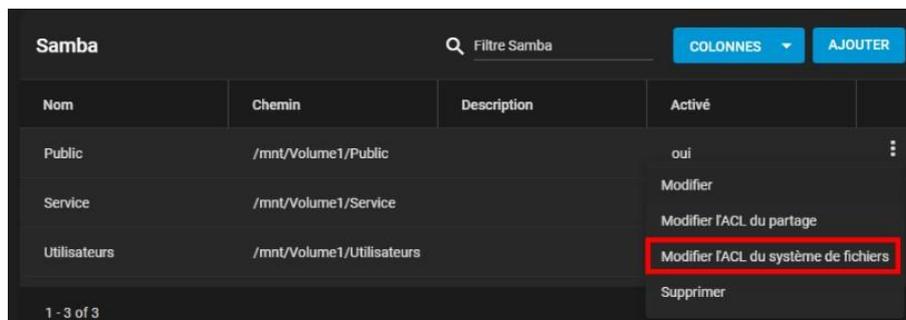


7) Modification des ACL pour les 3 datasets

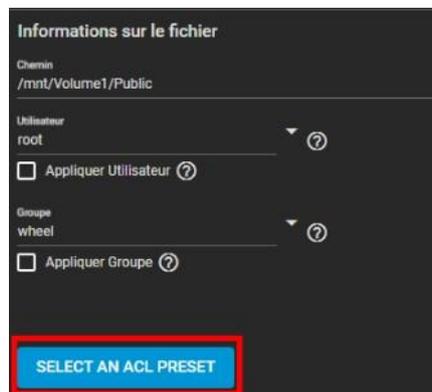
Nous allons maintenant modifier les autorisations d'accès aux datasets. TrueNAS propose des presets mais il est également possible de faire ses propres configurations.

a) Dossier public (Commun)

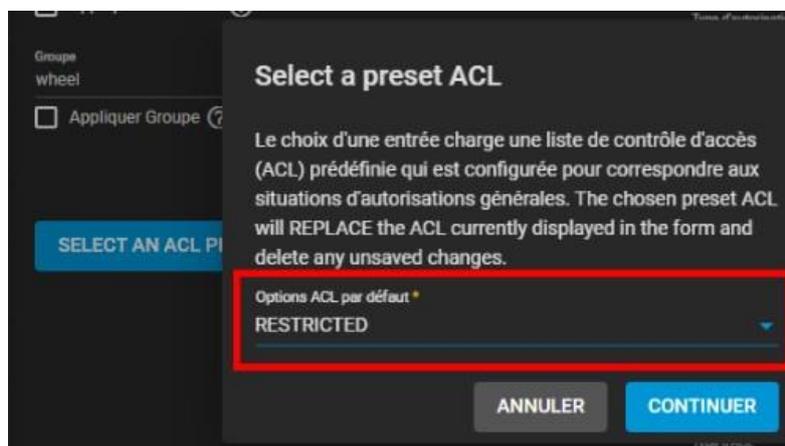
- Sur le dataset « Public », cliquer sur les 3 points puis sur « Modifier l'ACL du système de fichiers ».



- Cliquer « SELECT AN ACL PRESET ».

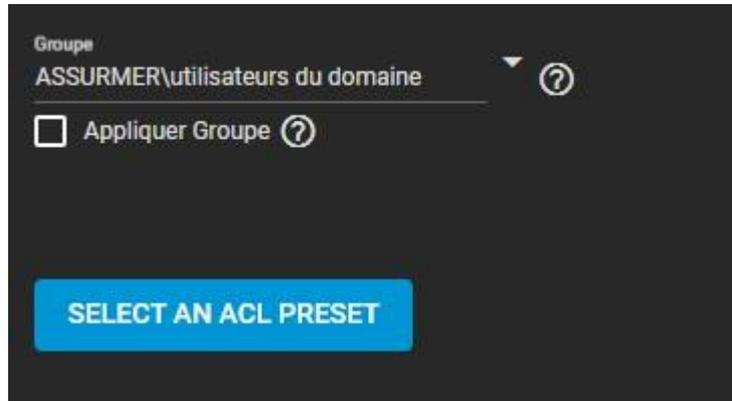


- Mettre l'option « RESTRICTED ».

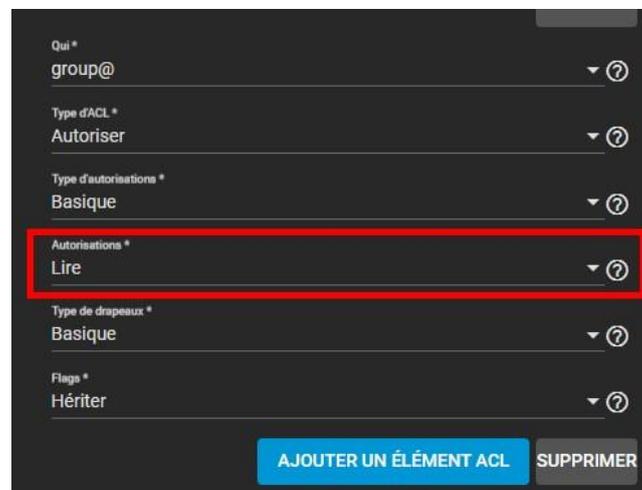




Choisir le groupe « Utilisateurs du domaine » et cocher la case « Appliquer Groupe ». **Si les groupes ASSURMER n'apparaissent pas, il faut relancer la reconstruction du cache dans l'onglet Active Directory.**



- Dans « Liste de contrôle d'accès », changer le paramètre « Autorisations » pour « Group@ » en « Lire ». Cliquer sur « Enregistrer ».



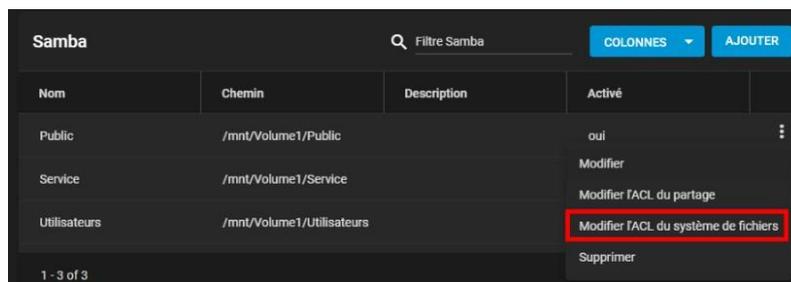
Les utilisateurs du domaine ont désormais par défaut accès en lecture au dossier « Public ».

b) Dossier Groupe de sécurité

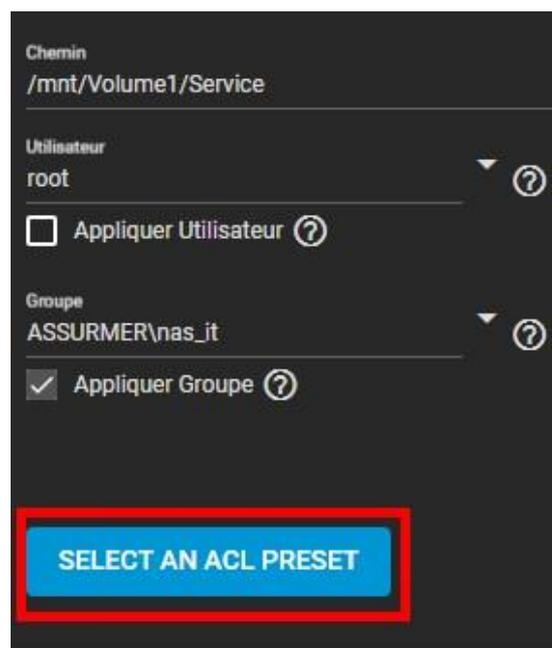
- Sur l'Active Directory, créer un groupe de sécurité qui correspondra au service de l'utilisateur par exemple.



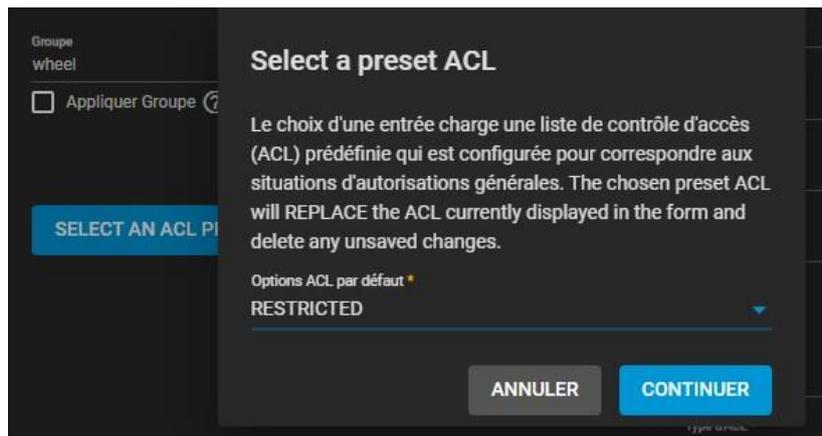
- Sur le dataset « Service », cliquer sur les 3 points puis sur « Modifier l'ACL du système de fichiers ».



- Cliquer « SELECT AN ACL PRESET ».



Mettre « RESTRICTED ».



- Choisir le groupe « nas_it » et cocher la case « Appliquer Groupe ». Il s'agit du groupe de sécurité correspondant au service IT d'Assurmer.



- Dans « Liste de contrôle d'accès », changer le paramètre « Autorisations » pour « Group@ » en « Modify ». Cliquer sur « Enregistrer ».



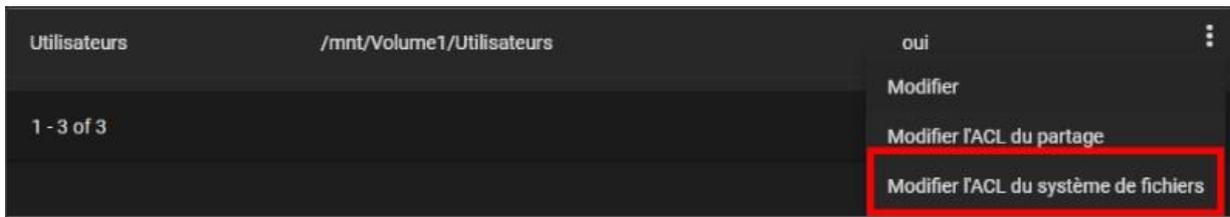
Les utilisateurs du domaine ayant le groupe de sécurité et faisant partie du service IT peuvent désormais lire et modifier le dossier « Service ». Il est possible de créer d'autres partages correspondant aux autres services d'Assurmer.

c) Dossier nominatif

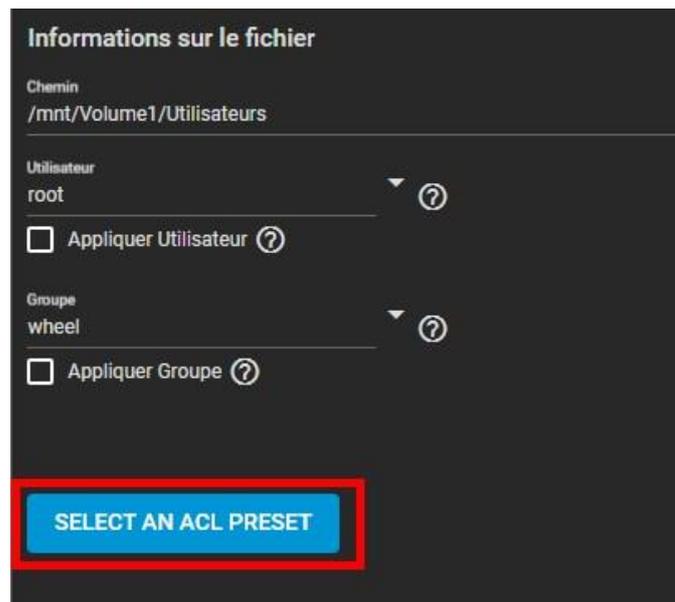
TrueNAS propose une option « Home Shares » permettant de fournir automatiquement un répertoire personnel pour chaque utilisateur.



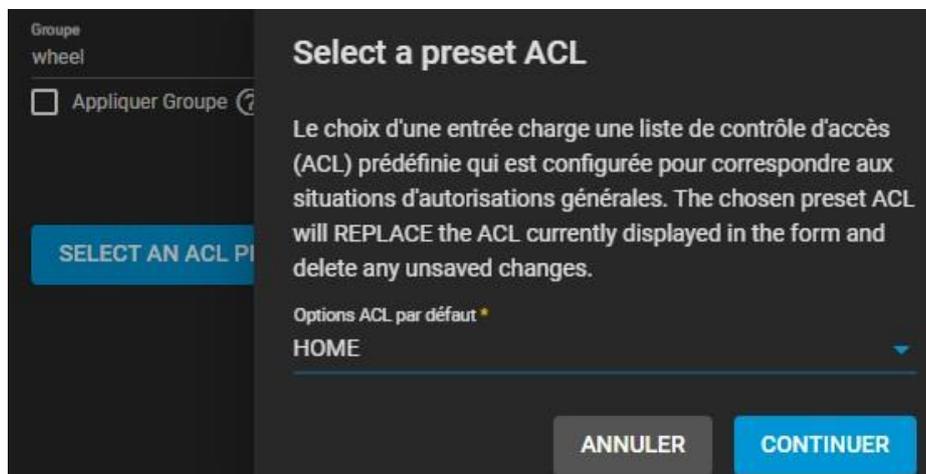
- Sur le dataset, cliquer sur les 3 points puis sur « Modifier l'ACL du système de fichiers ».



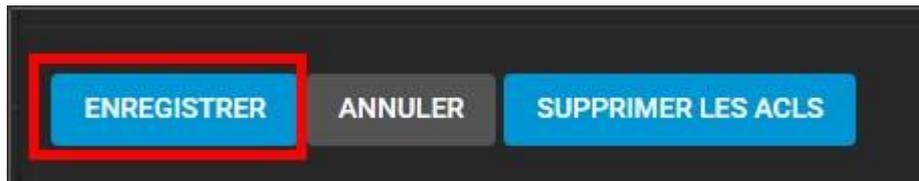
- Cliquer « SELECT AN ACL PRESET ».



- Mettre « HOME ».



Les autorisations se créent automatiquement. Cliquer sur « Enregistrer ».



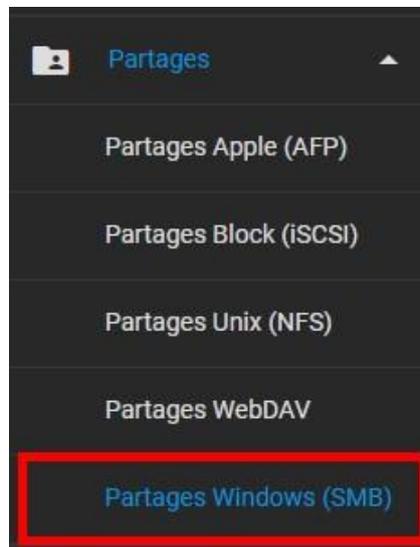
Les utilisateurs du domaine authentifiés ont désormais accès à un dossier personnel et nominatif.



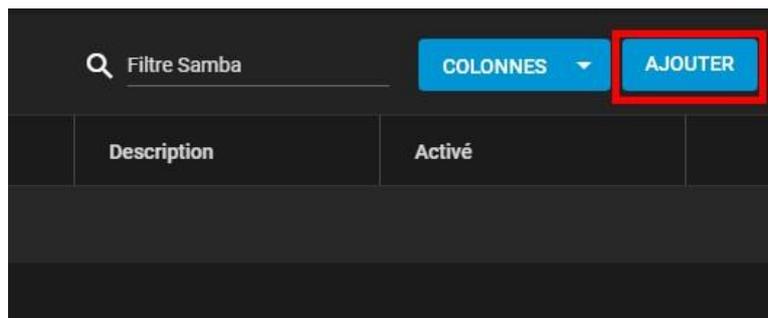
8) Création de Partages

Nous allons maintenant créer les partages Windows SMB (Server message Block) pour nos 3 datasets.

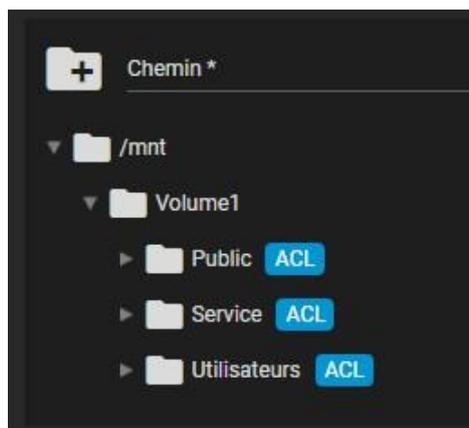
- Cliquer sur « Partages » puis « Partages Windows (SMB) ».



- Cliquer sur « Ajouter ».

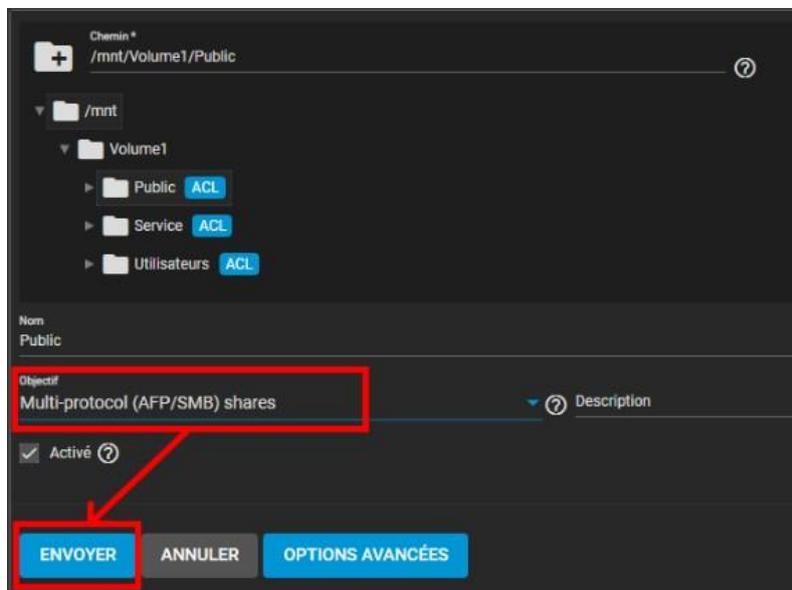


- Dérouler l'arborescence.

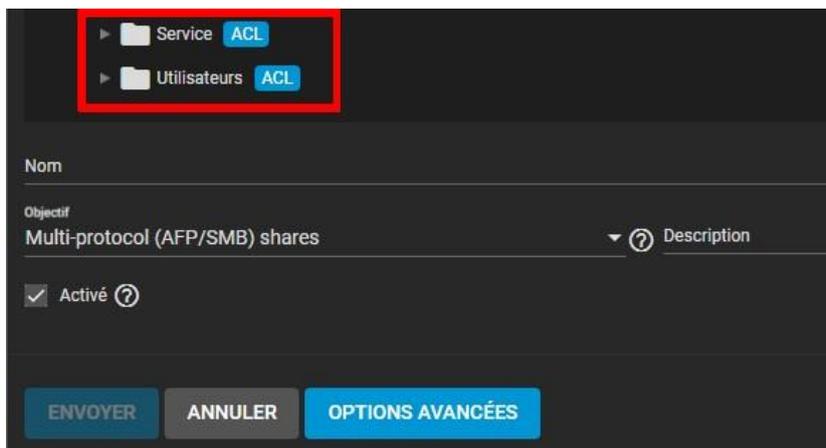




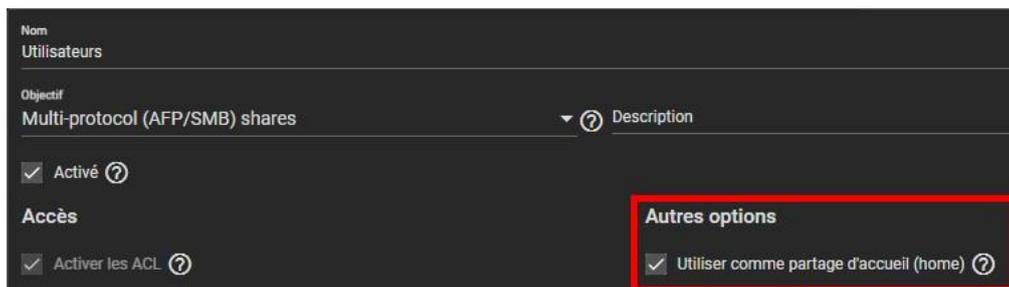
Sélectionner le partage « Public » avec dans « Objectif », le preset « Multi-protocol (AFP/SMB) shares » et cliquer sur « Envoyer ». Le preset permet aux ordinateurs Apple de se connecter au NAS avec l'AFP.



- Répéter l'opération pour le partage « Service » et « Utilisateurs »

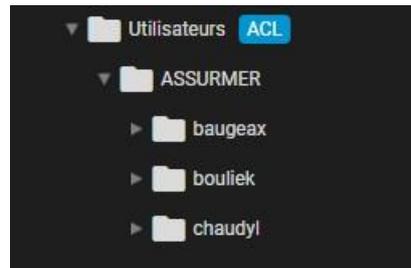


- Pour le partage « Utilisateurs », sélectionner « Options avancées » et cocher la case « Utiliser comme partage d'accueil (home) » pour créer automatiquement un répertoire nominatif.





/!\ Pour le dossier « Utilisateurs », il faudra vérifier que l'ACL ne s'applique qu'au dossier parent.



Si l'ACL s'applique aux dossiers enfants, cela peut poser des problèmes d'accès au dossier personnel.

- Dans « Services », vérifier que le SMB est bien en « Démarrage automatique ».



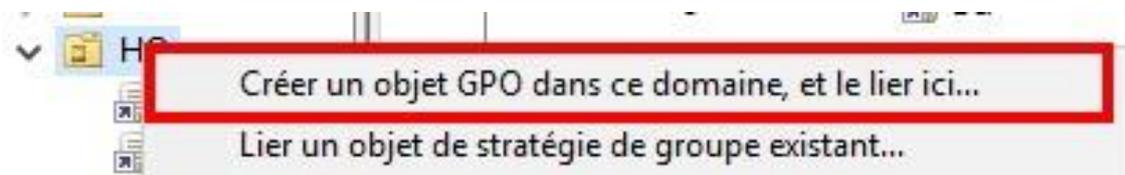


9) Configuration des lecteurs réseaux

Nous allons désormais configurer les 3 lecteurs réseaux avec une GPO. - Ouvrir la console « Gestion des stratégies de groupes ».



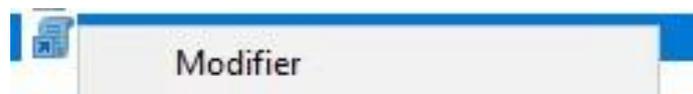
- Sur l'OU contenant les comptes des collaborateurs, faire clic droit puis « Créer un objet GPO dans ce domaine, et le lier ici ».



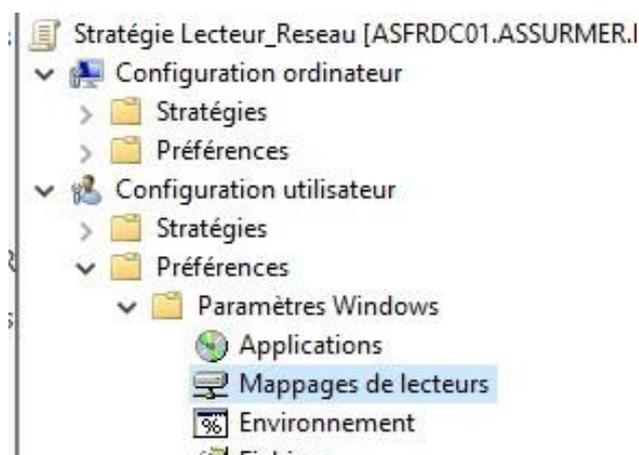
- Nommer la GPO et cliquer sur « OK ».

4	Lecteur_Reseau	Non	Oui	Activé	Aucun(e)	13/12/202...	assumer.fr
---	----------------	-----	-----	--------	----------	--------------	------------

- Faire clic droit sur la GPO puis la modifier.

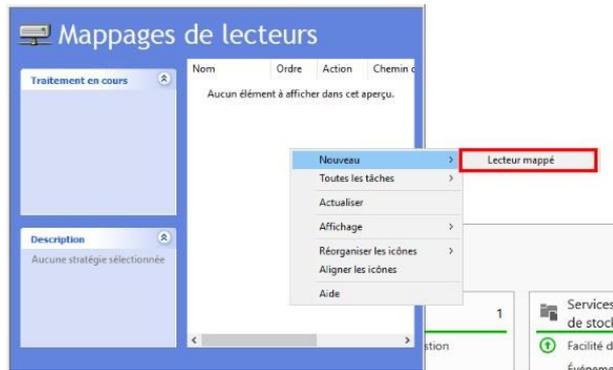


- Se rendre à l'emplacement suivant : Configuration Utilisateurs / Préférences / Paramètres Windows / Mappages de lecteur.

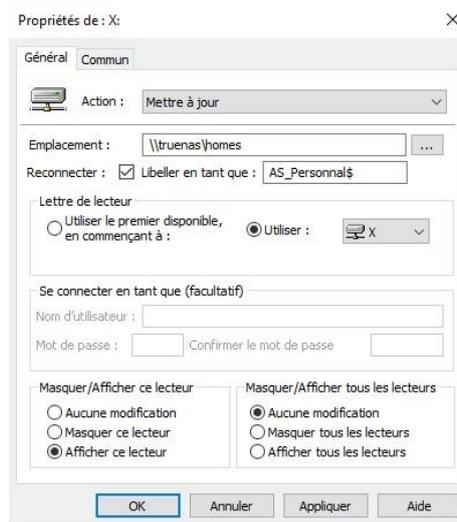




- Faire clic droit, « Nouveau » puis « Lecteur mappé ».



- Renseigner les informations du lecteur, cliquer sur « Appliquer » puis « OK ».



- Répéter l'opération pour Y:\AS_Service\$ et Z:\AS_Share\$

Nom	Ordre	Action	Chemin d'accès	Reconnecter
X:	1	Mettre ...	\\truenas\homes	Oui
Y:	2	Mettre ...	\\truenas\Service	Oui
Z:	3	Mettre ...	\\truenas\Public	Oui

Il faudra ensuite redémarrer ou faire un gpupdate /force.

