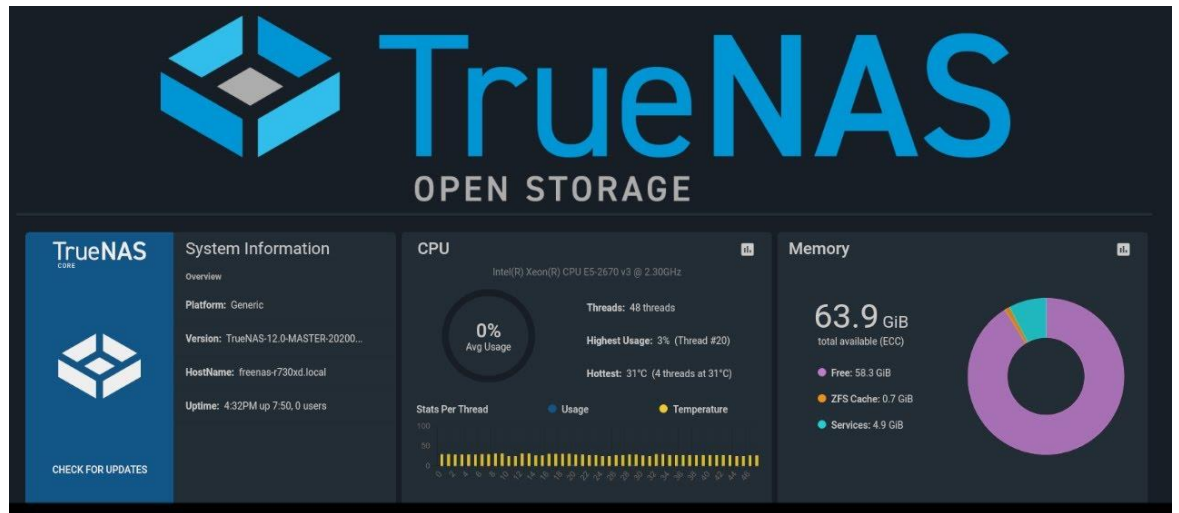


TRUENAS 13

Installer et configurer Truenas



SOMMAIRE

1. QU'EST-CE QUE TRUENAS ?
2. INSTALLER TRUENAS CORE (version 13)
3. CONFIGURER UN DATASET, UN PARTAGE, UN UTILISATEUR
4. CONFIGURER UN ACCES VPN VIA OPEN VPN SUR TRUENAS
5. MISE EN PLACE DE SNAPSHOTS ET PLANIFICATION

© tutos-info.fr - 07/2022



DIFFICULTE



UTILISATION COMMERCIALE INTERDITE

1 – QU'EST-CE QUE TRUENAS ?



TRUENAS est un système d'exploitation sous licence libre, basé sur FreeBSD (Linux). Truenas est destiné aux serveurs de stockage en réseau et supporte de nombreux Il supporte de nombreux protocoles. Truenas dispose d'une interface web moderne qui permet d'effectuer la configuration du système.

Plus qu'un NAS, Truenas offre une multitude de plugins permettant de le transformer en un véritable serveur (gestion du RAID « Z », gestion d'une connexion sécurisée VPN (OpenVPN), gestion des sauvegardes sur un cloud externalisé, gestion des utilisateurs d'un domaine, remontée LDAP, etc...

Ici, nous allons présenter l'installation de Truenas en version « core » (basée sur FreeBSD) mais il existe également une version dite Truenas « scale » basée sur Debian 11.

Ce guide présente l'installation, la configuration du système et la gestion d'une connexion sécurisée au NAS via OpenVPN.

2 - INSTALLER TRUENAS « CORE »

Pour installer Truenas « Core » (version 13) vous devez disposer d'un ordinateur avec les caractéristiques suivantes :

- Processeur Pentium ou supérieur (Core i3 ou plus selon utilisation qui sera faite du NAS)
- Mémoire vive minimum = 8 Go (16 Go si mise en place d'un RAID de type « Z » ou « Z2 »)
- Disque dur système = 10 Go
- Au minimum 2 disques durs pour le stockage (il est recommandé d'avoir plutôt 4 disques au minimum)

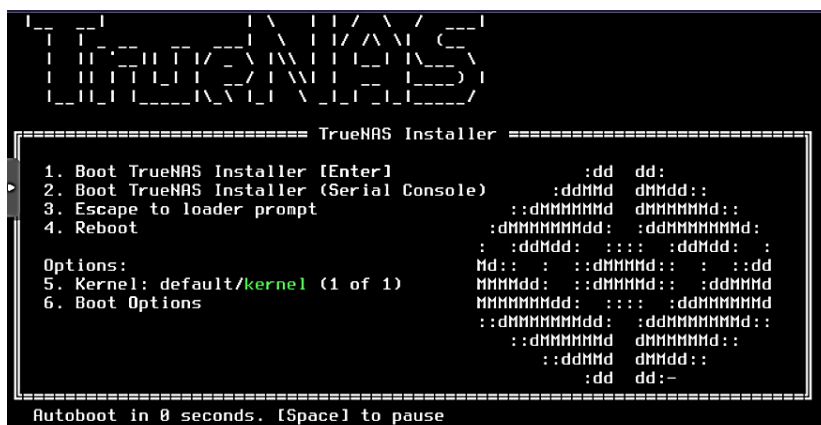
Dans ce guide, nous allons installer Truenas « core » sur une machine virtuelle créée avec © Proxmox. Le disque dur système occupe un espace de 10 Go et nous avons ajouté 4 disques de stockage de 15 Go chacun.

TELECHARGEMENT DU FICHER « ISO »

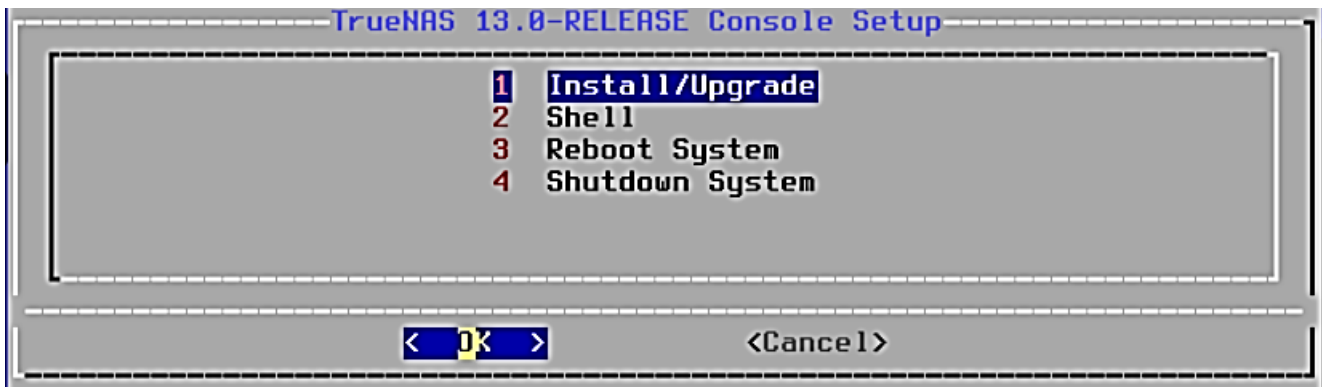
- Ouvrez un navigateur et téléchargez le fichier ISO directement depuis le site officiel de Truenas : <https://www.truenas.com/download-truenas-core/>
- Une fois le fichier téléchargé, vous pouvez le graver sur une clé USB pour en faire une « clé bootable » (vous pouvez utiliser un logiciel comme © Rufus pour créer votre clé).

INSTALLATION DU PROGRAMME

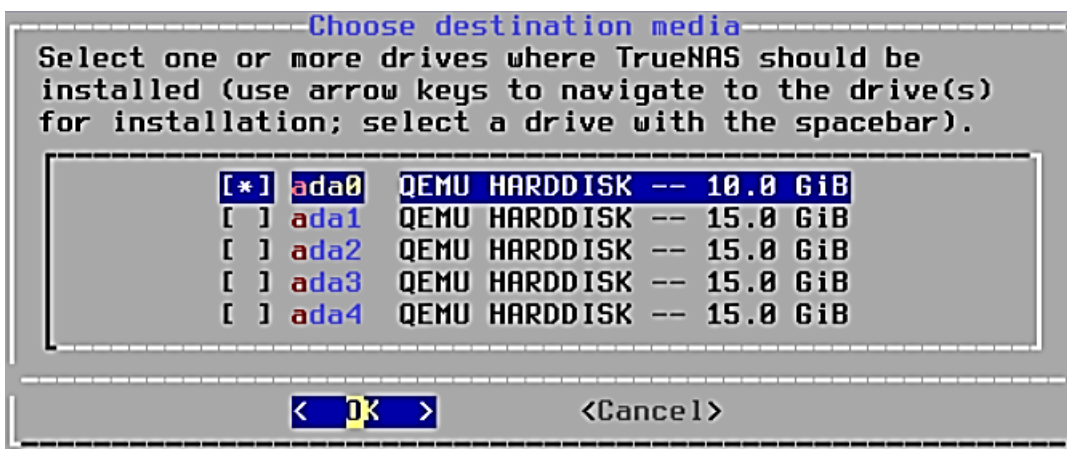
- Connectez la machine à une interface réseau (distribuant du DHCP) et faites démarrer votre machine de manière à ce qu'elle boote sur la clé USB contenant le fichier ISO. Un écran d'installation s'affiche. Vous pouvez appuyer sur la touche « Entrée » :



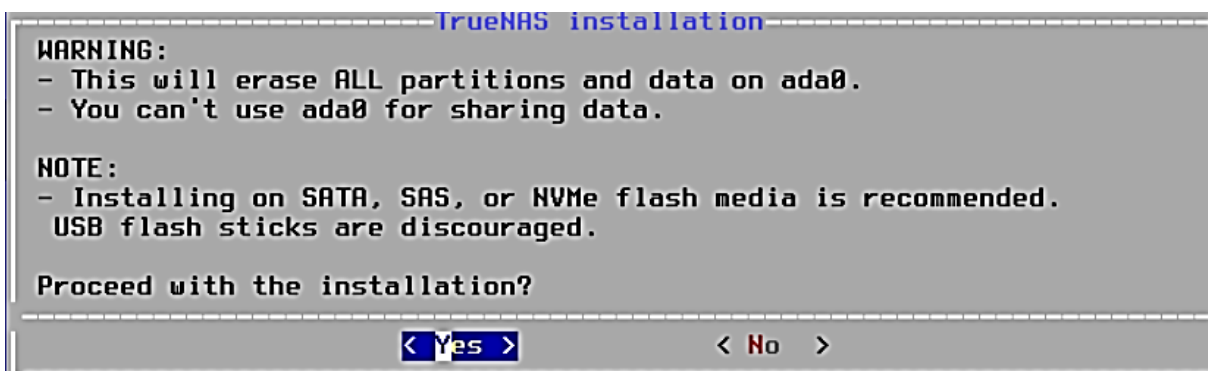
- Vérifiez que l'option « 1 – Install/upgrade » est sélectionnée et appuyez sur la touche « Entrée » :



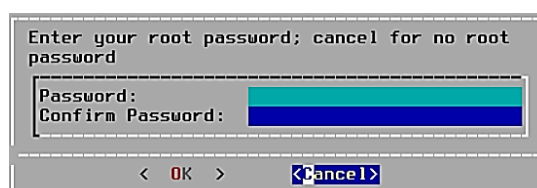
- Appuyez sur la barre d'espace pour sélectionner le disque d'installation du système et appuyez sur la touche « Entrée ». Ici nous avons un disque de 10 Go qui accueillera le système et les 4 autres disques de 15 Go chacun serviront au stockage des données :



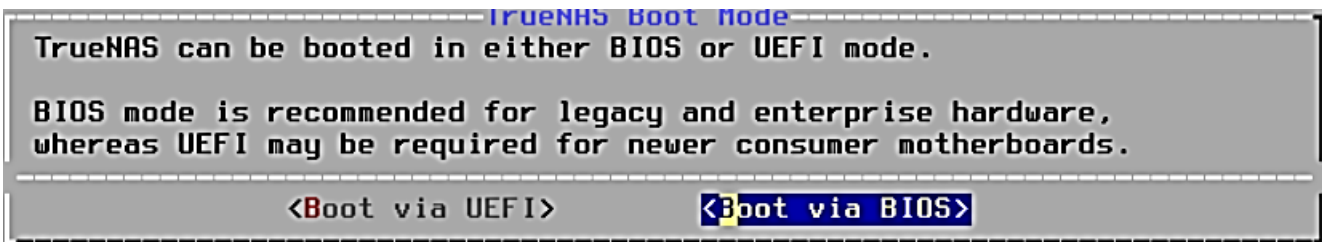
- Le message suivant indique que toutes les données du disque, sur lequel l'installation se fera, seront supprimées. Normalement l'option « Yes » est sélectionnée ; appuyez sur la touche « Entrée » pour lancer l'installation sur ce disque :



- Ici nous ne saisissons pas de mot de passe (nous le saisirons plus tard, lors de la première connexion à l'interface Truenas). Déplacez le curseur, à l'aide des flèches directionnelles, sur l'option « Cancel » et appuyez sur la touche « Entrée » :



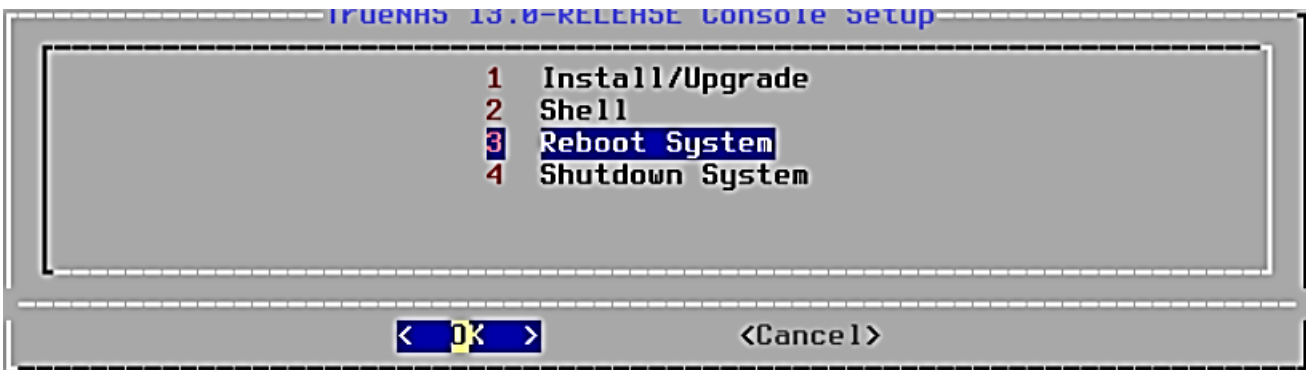
- Sélectionnez le type d'installation souhaitée : mode « UEFI » ou mode « BIOS ». Ici, nous avons laissé sur le mode « Boot via Bios » ; Appuyez sur la touche « Entrée » pour valider votre choix :



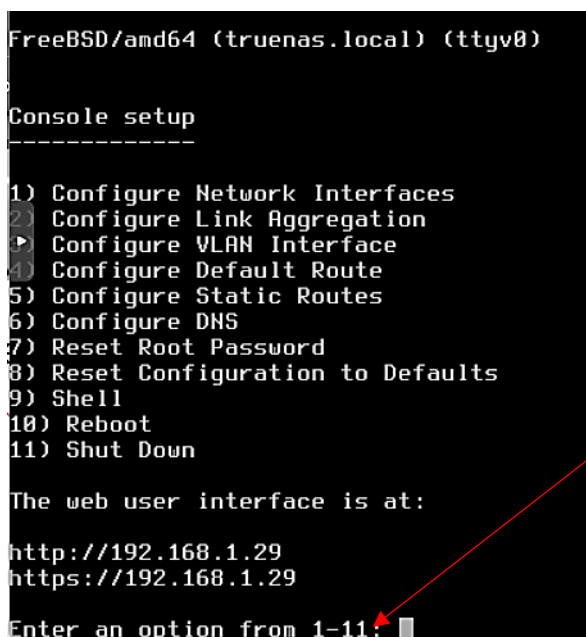
L'installation est lancée ; patientez pendant l'initialisation des processus (assez long selon la configuration de l'ordinateur sur lequel vous installez Truenas). Une fois l'installation terminée, un message s'affiche : appuyez sur la touche « Entrée » :



- Sélectionnez l'option « Reboot system » et appuyez sur la touche « Entrée » :



La machine redémarre et, une fois l'ensemble des processus initialisés, l'écran affiche l'adresse IP qui permettra d'administrer Truenas via une interface web :



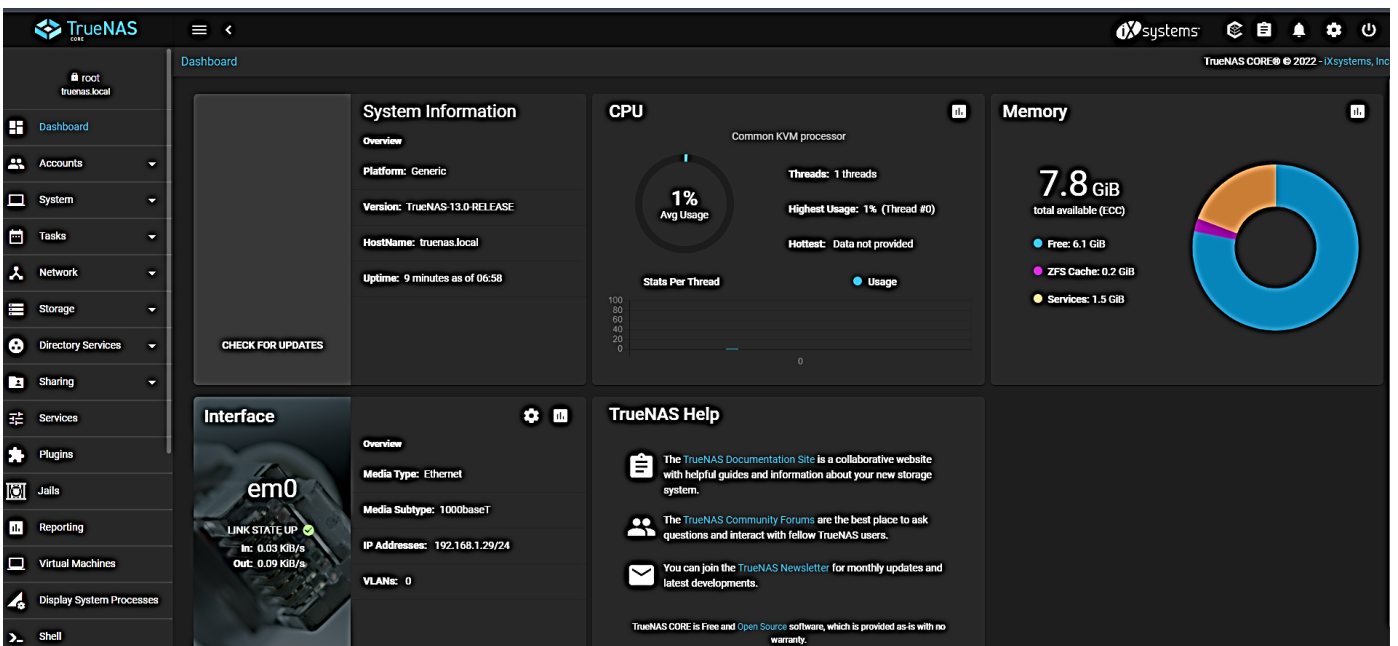
Une fois l'installation terminée, nous obtenons l'adresse IP qui a été attribuée automatiquement par notre box à notre serveur Truenas. Cette adresse permettra d'administrer le serveur via une interface web.

- Ouvrez un navigateur et saisissez l'adresse IP fournie à la fin de l'installation ; un écran d'accueil s'ouvre :



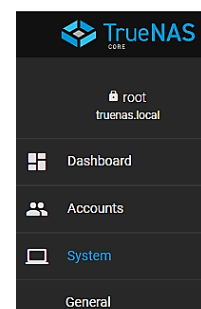
Etant donné que nous n'avons pas saisi de mot de passe lors de l'installation du système, Truenas nous demande, lors de la 1^{ère} connexion, de définir un mot de passe pour le compte « root ». Saisissez-le et cliquez le bouton « Connexion » pour ouvrir l'interface d'administration de Truenas.

L'écran d'accueil de Truenas Core (version 13) :



MISE EN FRANÇAIS DE L'INTERFACE D'ADMINISTRATION

- En haut à droite, cliquez sur la roue crantée et cliquez sur « Préférences »
- Dans le volet de gauche, cliquez sur « System » et « Général »
- Dans « Localization », sélectionnez « French » et cliquez « Save »



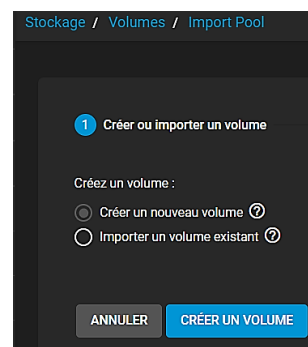
3 – CONFIGURER UN DATASET, CREER UN PARTAGE ET UN UTILISATEUR

Une fois l'installation de Truenas réalisée, nous allons commencer par créer un **volume de stockage** avec les disques disponibles dans notre machine (ici nous avons 4 disques de 15 Go chacun).

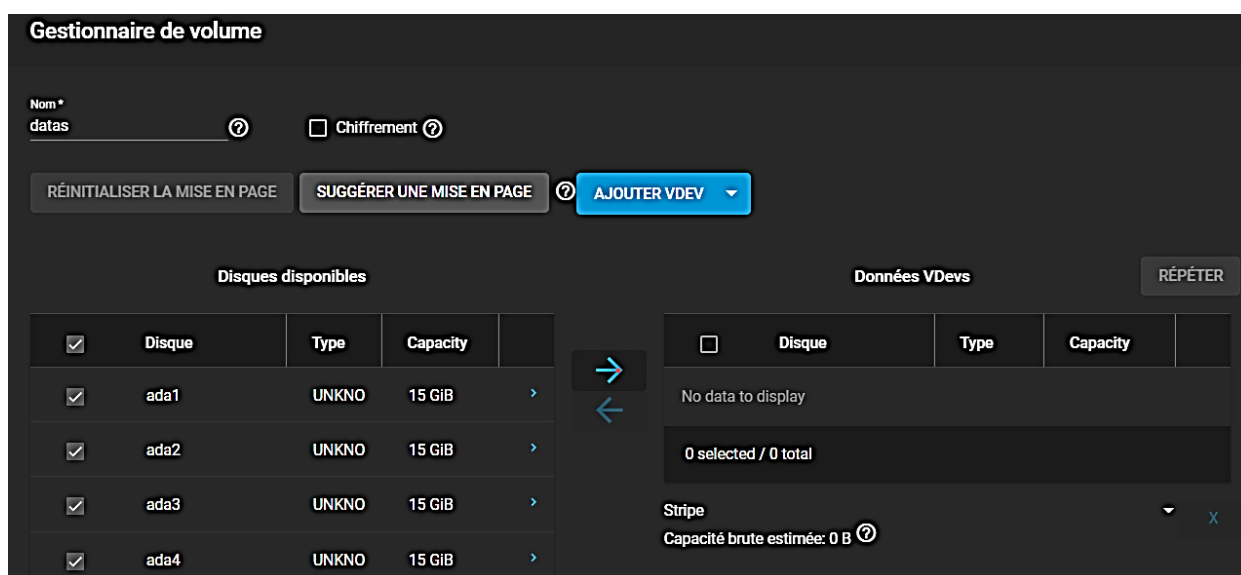
CREATION D'UN POOL DE STOCKAGE

- Dans le volet de gauche, cliquez sur « Stockage » et « Volumes »
- Cliquez le bouton « Ajouter » (sur la droite)
- Cliquez le bouton « Créer un volume »

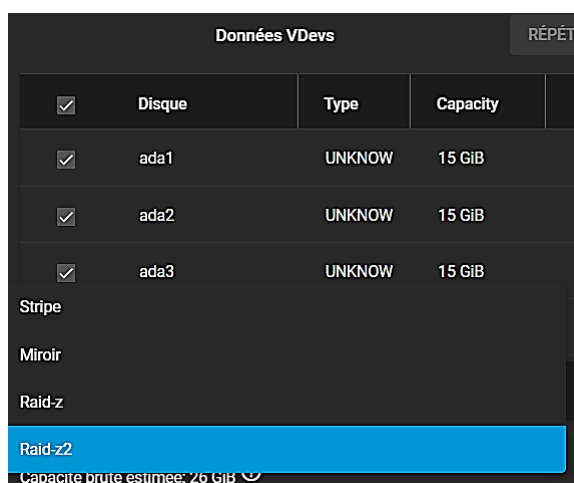
Une nouvelle fenêtre s'affiche et présente l'ensemble des disques durs disponibles pour la création du volume de stockage.



- Saisissez un nom pour votre volume de stockage (« datas » dans cet exemple) et sélectionnez l'ensemble des disques durs et cliquez la flèche bleue pour basculer les disques sélectionnés sur la droite :

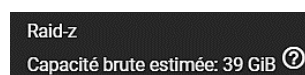


- Sélectionnez l'architecture désirée (RAID stripping, mirroring, Raid-z ou Raid-z2). Attention, le RAID stripping ne permet pas la sécurisation des données ! Le Raid-z2 est le plus fiable en terme de redondance mais ce type de configuration est gourmand en ressources mémoire et en capacité de stockage :




Une fois les disques sélectionnés, il faut choisir un système de redondance (sauf le « stripe »). Les modes « Raid-z » et « Raid-z2 » offrent les meilleures performances mais sont plus gourmands au niveau des ressources matérielles (processeur et RAM).

Ici, nous avons sélectionné le « RAID-z » et la capacité de stockage allouée est de 39 Go :



Cliquez le bouton « Créer » pour valider la création de votre volume de stockage.

Une fois le volume de stockage créé, nous obtenons un résumé :

Volumes					
datas (System Dataset Pool)		ONLINE  10.34 MiB (0%) Utilisé 36.25 GiB Libre			
Nom ↕	Type ↕	Utilisé ↕	Available ↕	Compression ↕	Compression Ratio ↕
datas	FILESYSTEM	10.34 MiB	36.25 GiB	lz4	19.08

CREATION D'UN DATASET « PUBLIC »

Ce dataset « public » sera l'équivalent d'un dossier réseau « échange » dans lequel des données pourront être enregistrées et partagées entre les membres du NAS.

- Dans le volet de gauche, cliquez sur « Stockage » et « Volumes »
- Cliquez, à droite du nom de votre volume précédemment créé, sur les 3 points verticaux
- Cliquez « Ajouter un dataset »
- Complétez la fenêtre de paramétrage du dataset



Stockage / Volumes / Ajouter un dataset

Nom et options

Nom *

public

Commentaires

espace de partage commun

Synchroniser

Inherit (standard)

Niveau de compression

Inherit (lz4)

Activer Adms

Inherit (off)

Options de chiffrement

☒ Héritage (non chiffré) ?

Autres options

Désactivation 2FS

Inherit (off)

Sensibilité à la casse

Insensitive

Type de partage

SMB

ENVOYER ANNULER OPTIONS AVANCÉES

On indique ici le nom du dataset

On peut donner une indication sur le dataset créé.

On indique, ici, que le partage sera de type « SMB » (partage Windows).

- Une fois les paramètres du dataset saisis, cliquez le bouton « Envoyer ».

MODIFICATION DES AUTORISATIONS SUR LE DATASET PUBLIC

Une fois le dataset créé, il faut allouer des autorisations au dataset. Pour cela :

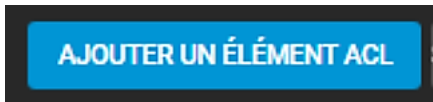
- Cliquez les 3 points verticaux (à droite du nom du dataset) :

▼ datas	FILESYSTEM	15.06 MiB	36.25 GiB	lz4	14.24	false	OFF	⋮
public	FILESYSTEM	139.5 KiB	36.25 GiB	Hérite (lz4)	1.00	false	OFF	espace de partage commun ⋮

- Cliquez « Modifier les autorisations »

La fenêtre des autorisations du dataset s'affiche :

- Cliquez, en bas et dans la partie droite de la fenêtre, sur « Ajouter un élément ACL »



- Configurez l'élément ACL ainsi et cliquez « Enregistrer » :

Ici on autorise « tout le monde » à accéder à ce dataset « public » (qui sert d'espace d'échange) et l'on accorde des droits de modification dans l'espace.

CREATION D'UN DATASET UTILISATEUR

Ici, nous allons créer un dataset destiné à un utilisateur authentifié (espace personnel sur le NAS). Pour cela :

- Dans le volet de gauche, cliquez sur « Stockage » et « Volumes »
- Cliquez, à droite du nom de votre volume précédemment créé, sur les 3 points verticaux
- Cliquez « Ajouter un dataset »
- Complétez la fenêtre de paramétrage du dataset « utilisateurs » comme suit :

On indique ici le nom du dataset et un commentaire

On indique que le type de partage du dataset est « SMB » et on clique « Envoyer » pour créer le dataset.

MODIFICATION DES AUTORISATIONS SUR LE DATASET UTILISATEURS

Une fois le dataset créé, il faut allouer des autorisations au dataset. Pour cela :

- Cliquez les 3 points verticaux (à droite du nom du dataset) :



- Cliquez « Modifier les autorisations »

La fenêtre des autorisations du dataset s'affiche :

SELECT AN ACL PRESET

- Cliquez le bouton bleu « Select an ACL PRESET »
- Sélectionnez « HOME » et continuer : les autorisations de base pour un utilisateur sont renseignées
- Cliquez le bouton « Enregistrer »

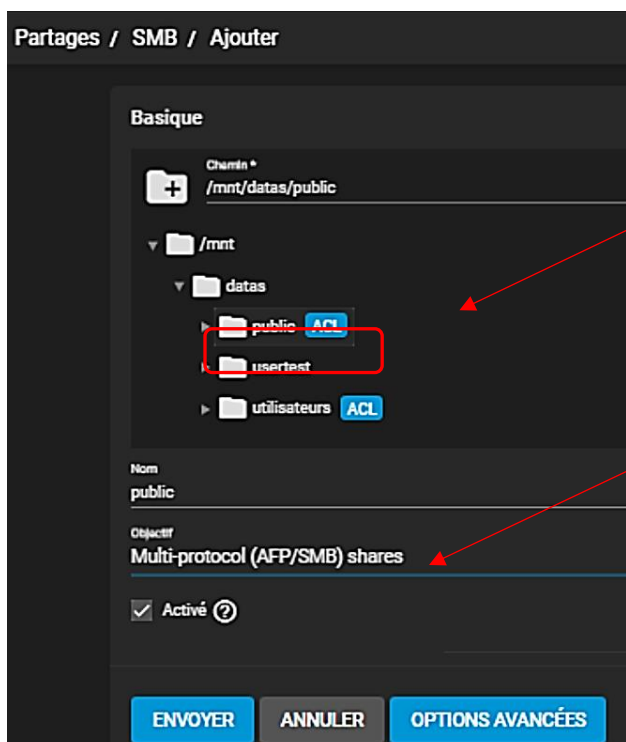
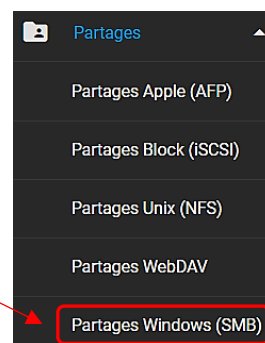
Une fois les dataset nécessaires créés, il faut maintenant lancer les partages « SMB » afin que les espaces de stockage du volume de stockage du NAS soient accessibles depuis Windows.

CREATION DES PARTAGES WINDOWS (SMB)

Afin de pouvoir utiliser l'espace de stockage depuis un ordinateur Windows, il est nécessaire de créer un partage Windows de type « SMB ».

Création du partage SMB pour le dataset « public » :

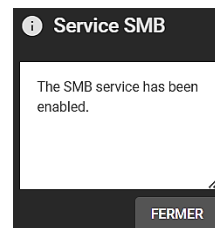
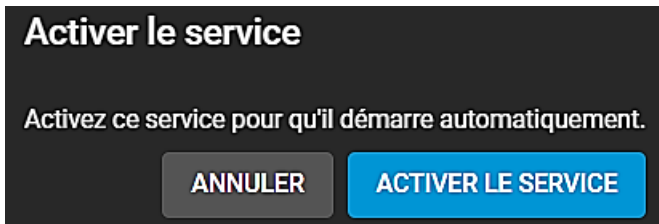
- Dans le volet de gauche, cliquez sur « Partages » et sur « Partages Windows (SMB) »
- Cliquez, sur la droite de l'écran, le bouton « Ajouter » : une fenêtre s'affiche
- Cliquez sur le dataset « public »
- Sélectionnez le « Multi-Protocol (AFP/SMB) shares »
- Cliquez le bouton « Envoyer » :



Sélectionnez le dataset qui fera partie du partage.

En sélectionnant le type de partage « Multi-Protocol (AFP/SMB) shares » on permet aux ordinateurs © Apple d'accéder également à l'espace de partage public.

- Activez le service en cliquant le bouton « ACTIVER LE SERVICE » :

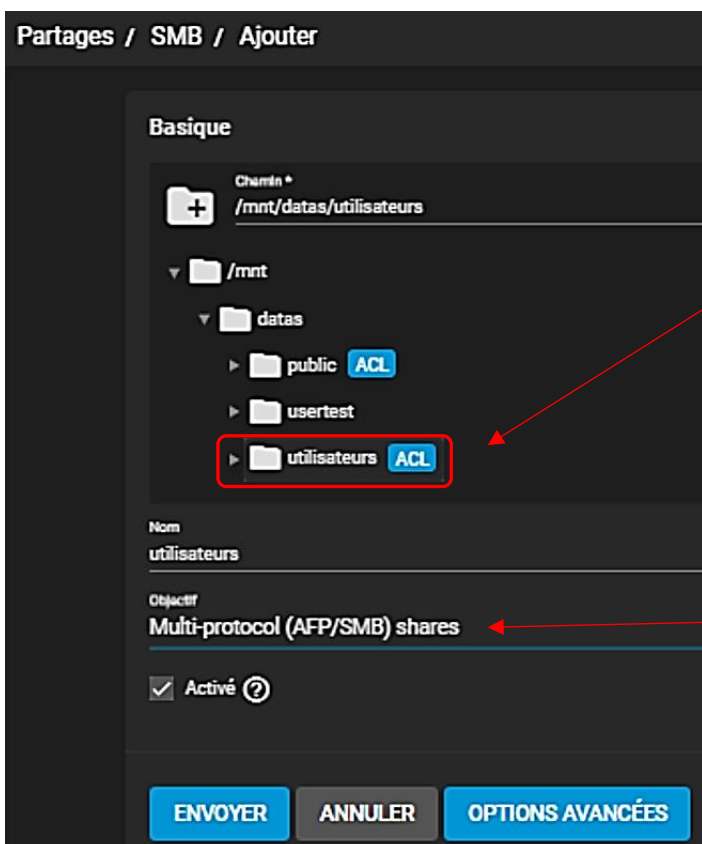


Activez le service de partage SMB et vérifiez que l'initialisation a réussi (un message s'affiche pour vous informer du lancement du service).

Un message affiche que le service SMB est maintenant actif sur le réseau

Création du partage SMB pour le dataset « utilisateurs » :

- Dans le volet de gauche, cliquez sur « Partages » et sur « Partages Windows (SMB) »
- Cliquez, sur la droite de l'écran, le bouton « Ajouter » : une fenêtre s'affiche
- Cliquez sur le dataset « utilisateurs »
- Sélectionnez le « Multi-Protocol (AFP/SMB) shares »



Sélectionnez le dataset qui fera partie du partage.

En sélectionnant le type de partage « Multi-Protocol (AFP/SMB) shares » on permet aux ordinateurs © Apple d'accéder également à l'espace de partage public.

- Cliquez le bouton « Options avancées »
- **Cliquez la case « Utiliser comme partage d'accueil (home) ».** En cochant cette case cela signifie que si vous créez un nouvel utilisateur, il aura directement un répertoire créé à son nom avec un accès autorisé.
- Cliquez le bouton « Enregistrer » (pas de modification dans la fenêtre ACL)

On peut maintenant effectuer différents tests d'accès au NAS. Pour cela, ouvrez l'explorateur et saisissez l'adresse IP de votre serveur NAS (ici nous avons saisi [\\192.168.1.29](http://192.168.1.29) qui correspond à l'adresse IP de notre Truenas) ; une fenêtre d'authentification s'affiche :

Sécurité Windows

Entrer les informations d'identification réseau

Entrez vos informations d'identification pour vous connecter à :
192.168.1.29

Nom d'utilisateur

Mot de passe

☐ Mémoriser mes informations d'identification

Le nom d'utilisateur ou le mot de passe est incorrect.

OK Annuler

En saisissant, dans votre explorateur, l'adresse IP de votre NAS, vous obtiendrez cette fenêtre demandant une authentification. Cette demande est normale puisque, par défaut, les accès « invité » sont désactivés.

Dans la partie suivante, nous allons voir comment autoriser un utilisateur à accéder à son espace de partage sur le NAS.

CREATION D'UN UTILISATEUR SUR LE NAS ET AUTORISATION D'ACCES

Création d'un compte « utilisateur test » :

- Dans le volet de gauche, cliquez sur « Comptes » et « Utilisateurs »
- En haut à droite de l'écran, cliquez sur « Ajouter »
- Complétez les rubriques (celles comportant un « * » sont obligatoires)

Comptes / Utilisateurs / Ajouter

Nom d'utilisateur*
usertest

Courriel

Mot de passe*
xxxx

Confirmer le mot de passe*
xxxx

ID utilisateur et groupes

ID de l'utilisateur*
1000

☒ Nouveau groupe primaire ⓘ

Groupe primaire

Groupes auxiliaires

Répertoires et Permissions

Répertoire utilisateur
+ /mnt/datas/utilisateurs/usertest

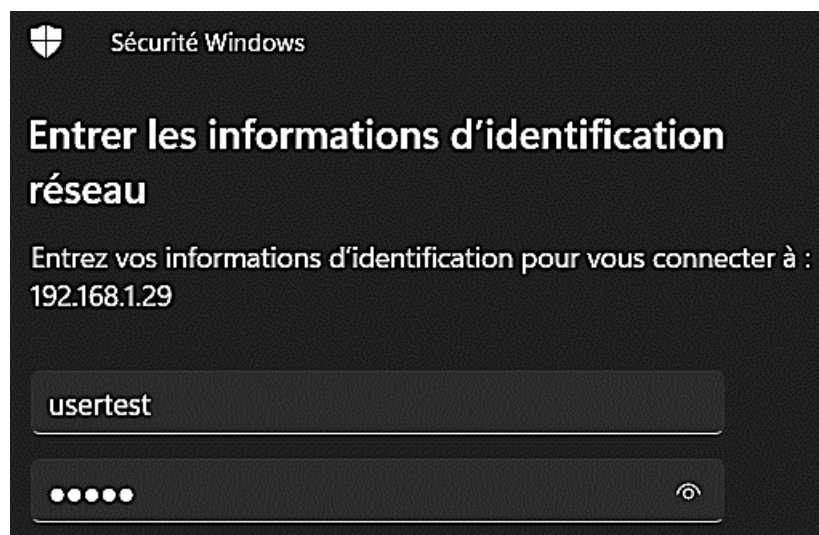
> /mnt

Autorisations du répertoire personnel ⓘ

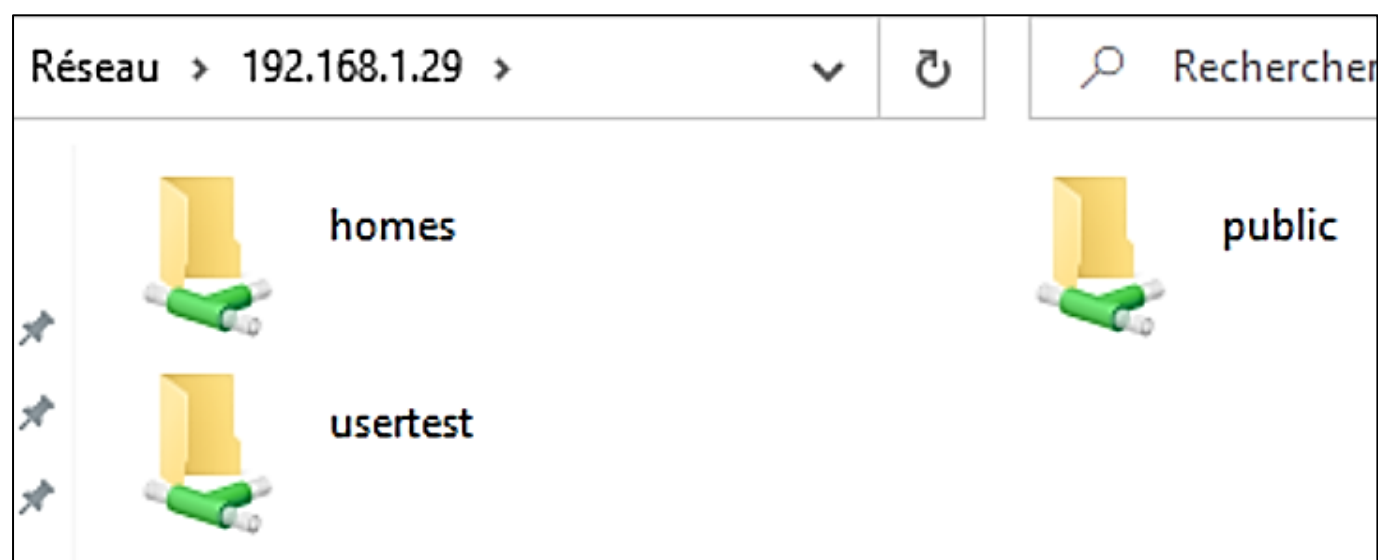
	Lire	Écrire	Exécuter
Utilisateur	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Groupe	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Autre	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

En créant un nouvel utilisateur, on constate que son dossier personnel est automatiquement créé (/mnt/datas/utilisateurs/usertest) dans le dataset « utilisateurs ». Vérifiez et adaptez les permissions si nécessaires et cliquez le bouton « Envoyer »

Testez l'accès à votre espace de partage sur le NAS depuis un explorateur en saisissant l'adresse IP du NAS et en vous authentifiant avec l'utilisateur « usertest » précédemment créé :



L'explorateur affiche la fenêtre suivante :



On retrouve le dossier personnel de l'utilisateur (ici « usertest ») et l'espace de partage « public » dans lequel il pourra déposer des fichiers accessibles à tous (seul son espace « usertest » lui est réservé et inaccessible aux autres utilisateurs non autorisés).

Note :

Il est possible de créer une multitude d'utilisateurs, de groupes et d'attribuer diverses permissions. Il n'est pas possible, ici, de présenter ces possibilités qui sont à adapter à la politique de stockage et d'accès aux données de l'entreprise.

4 – CONFIGURER UN ACCES VPN VIA LE PROTOCOLE OPENVPN DE TRUENAS

Truenas offre la possibilité de se connecter de manière sécurisée via le protocole OpenVPN. Pour utiliser OpenVPN, la procédure à suivre est la suivante (respecter l'ordre des tâches !) :

1^{ère} étape - CREATION DE L'AUTORITE DE CERTIFICATION

- Dans le volet de gauche, cliquez sur « Système »
- Cliquez sur « CAs »
- Cliquez, en haut à droite de l'écran, sur le bouton « Ajouter » et complétez la fenêtre
- Cliquez le bouton « Envoyer » une fois les paramètres saisis :

Type
Internal CA

Longueur de la clé *
2048

Profil
Openvpn Root CA

Sélectionnez « Openvpn Root CA » au niveau du profil de l'autorité de certification.

Algorithme Digest *
SHA256

Objet du certificat

Durée de vie *
825

Pays *
France

Etat *
MANCHE

Localité *
AVRANCHES

Organisation *
LABOPROF

Unité organisationnelle
LABOPROF

Courriel *
xx@xx.fr

Nom commun
truenas.local

Noms alternatifs de sujet *
truenas.local

Contraintes de base

Identificateur de clé d'autorité

☒ Activé

☒ Activé

Longueur du chemin

Configuration de la clé d'autorité
Authority Cert Issuer

Configuration des contraintes de base
CA, Critical Extension

Utilisation des clés

Utilisation étendue des clés

Configuration de l'utilisation des clés
Key Cert Sign, CRL Sign, Critical Extension

☒ Activé

☒ Activé

Usages *
CLIENT_AUTH, SERVER_AUTH

Extension critique

Envoyer

Annuler

Cliquez le bouton « Envoyer » une fois les paramètres saisis.

Ces paramètres sont à adapter en fonction du niveau de sécurité souhaité (attention plus l'algorithme est important plus le traitement prendra du temps en fonction de votre matériel).

2^{ème} étape - CREATION DU CERTIFICAT OPENVPN SERVEUR

- Dans le volet de gauche, cliquez sur « Système »
- Cliquez sur « Certificats »
- Cliquez, en haut à droite de l'écran, sur le bouton « Ajouter » et complétez la fenêtre
- Cliquez le bouton « Envoyer » une fois les paramètres saisis :

Identifiant et type

Nom *
certificat_serveur

Type
Internal Certificate

Profil
Openvpn Server Certificate

Options de certificat

Autorité de certification signataire *
AUTORITE_TRUENAS

Type de clé *
RSA

Longueur de la clé *
2048

Algorithme Digest *
SHA256

Durée de vie *
825

Objet du certificat

Pays *
France

Localité *
AVRANCHES

Unité organisationnelle
LABOPROF

Nom commun
truenas.local

Etat *
MANCHE

Organisation *
LABOPROF

Courriel *
xxx@xxx.fr

Noms alternatifs de sujet *
truenas.local

Contraintes de base

☒ Activé

Longueur du chemin

Configuration des contraintes de base
Critical Extension

Utilisation étendue des clés

☒ Activé

Usages *
SERVER_AUTH

☒ Extension critique

Identificateur de clé d'autorité

☒ Activé

Configuration de la clé d'autorité
Authority Cert Issuer

Utilisation des clés

☒ Activé

Configuration de l'utilisation des clés
Digital Signature, Key Encipherment, Critical Extension

ENVOYER

ANNULER

Sélectionnez ici l'autorité de certification précédemment créée.

Sélectionnez ici le profil « Openvpn Server Certificate ».

Cliquez le bouton « Envoyer » une fois les paramètres saisis.

3^{ème} étape - CREATION DU CERTIFICAT OPENVPN CLIENT

- Dans le volet de gauche, cliquez sur « Système »
- Cliquez sur « Certificats »
- Cliquez, en haut à droite de l'écran, sur le bouton « Ajouter » et complétez la fenêtre
- Cliquez le bouton « Envoyer » une fois les paramètres saisis :

Identifiant et type

Nom *
certificat_client

Type
Internal Certificate

Profil
Openvpn Client Certificate

Options de certificat

Autorité de certification signataire *
AUTORITE_TRUENAS

Type de clé *
RSA

Longueur de la clé *
2048

Algorithme Digest *
SHA256

Durée de vie *
825

Objet du certificat

Pays *
France

Localité *
AVRANCHES

Unité organisationnelle
LABOPROF

Nom commun
truenas.local

Etat *
MANCHE

Organisation *
LABOPROF

Courriel *
xxx@xxx.fr

Noms alternatifs de sujet *
truenas.local

Contraintes de base

☒ Activé

Longueur du chemin

Configuration des contraintes de base
Critical Extension

Utilisation étendue des clés

☒ Activé

Usages *
CLIENT_AUTH

☒ Extension critique

Identificateur de clé d'autorité

☒ Activé

Configuration de la clé d'autorité
Authority Cert Issuer

Utilisation des clés

☒ Activé

Configuration de l'utilisation des clés
Digital Signature, Key Agreement, Critical Extension

ENVOYER

ANNULER

Sélectionnez ici l'autorité de certification précédemment créée.

Sélectionnez ici le profil « Openvpn Client Certificate ».



Cliquez le bouton « Envoyer » une fois les paramètres saisis.

Une fois les certificats créés, une fenêtre affiche l'ensemble des certificats présents sur le serveur (le certificat « freenas_default » est le certificat de base qui ne sera pas utilisé ici) :

Certificats			
Nom	Émetteur	Nom distinctif	De
certificat_client	AUTORITE_TRUENAS	/CN=truenas.local/C=FR/ST=MANCHE/L=AVRANCHES/	2022-05-14 08:28:48
certificat_serveur	AUTORITE_TRUENAS	/CN=truenas.local/C=FR/ST=MANCHE/L=AVRANCHES/	2022-05-14 08:24:21
freenas_default	external	/C=US/O=IXsystems/CN=localhost/emailAddress=info@	2022-05-14 06:49:40

4^{ème} étape – ACTIVATION DES SERVICES OPENVPN

- Dans le volet de gauche, cliquez sur « Services »
- Cliquez sur le petit crayon à droite de « OpenVPN client »

OpenVPN Client	<input type="checkbox"/>	<input type="checkbox"/>	
OpenVPN Server	<input type="checkbox"/>	<input type="checkbox"/>	

- Complétez la fenêtre ainsi :

Certificat du client
certificat_client

Root CA
AUTORITE_TRUENAS

Distant *
192.168.1.29

Port
1194

Algorithme d'authentification
SHA256 (256 bit digest size)

Cipher

Compression

Protocole
UDP

ENREGISTRER

ANNULER

ATTENTION, ici nous travaillons en local c'est pour cette raison que nous indiquons l'adresse IP de notre serveur Truenas, sinon il faut indiquer un nom de domaine valide afin que l'on puisse accéder depuis l'extérieur au serveur Truenas.

Cliquez le bouton « Enregistrer » une fois les paramètres saisis.

Type de périphérique
TAP

☒ Nobind

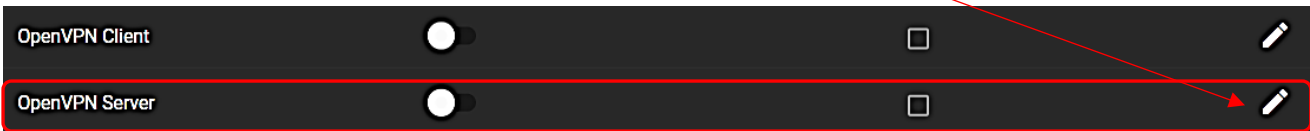
☐ TLS Crypt Auth Activé

Paramètres supplémentaires

TLS Crypt Auth

Il est nécessaire, ensuite, de configurer le service pour le certificat serveur (voir page suivante).

- Cliquez sur le petit crayon à droite de « OpenVPN Server »

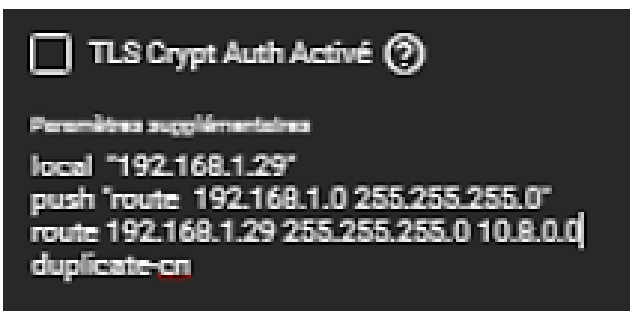


- Complétez la fenêtre ainsi :



Important (paramètres supplémentaires) :

Il est très important de saisir, dans les « Paramètres supplémentaires » les lignes permettant de configurer la route statique une fois le tunnel VPN connecté :



local « 192.168.1.29 »
push « route 192.168.1.0 255.255.255.0 »
route « 192.168.1.29 255.255.255.0 10.8.0.0 »
duplicate-cn

local pour indiquer l'adresse du serveur truenas
push pour créer la route
route pour indiquer les paramètres de la route statique
duplicate-cn pour avoir plusieurs connexions VPN

Une fois les paramètres saisis pour le service OpenVPN serveur, cliquez le bouton « Enregistrer ».

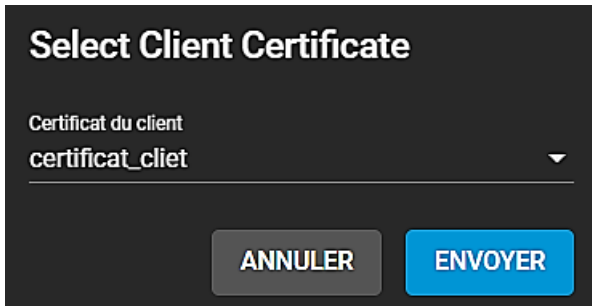
Cliquez à nouveau sur le petit crayon à droite de « Openvpn Server »



Il est nécessaire ensuite de télécharger les fichiers de configuration « client » qui seront nécessaires au futur client VPN.

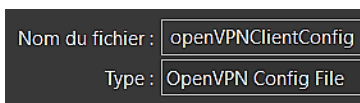
Pour cela, cliquez le bouton « Télécharger la configuration du client ». Une fenêtre s'affiche :

- Sélectionnez le certificat client précédemment créé et cliquez le bouton « Envoyer » :



The dialog box is titled "Select Client Certificate". It features a dropdown menu labeled "Certificat du client" with the value "certificat_cliet" selected. At the bottom, there are two buttons: "ANNULER" (grey) and "ENVOYER" (blue).

Téléchargez, sur votre ordinateur, le fichier proposé « openVPNClientConfig » puis fermez la fenêtre :



A small form showing file details: "Nom du fichier : openVPNClientConfig" and "Type : OpenVPN Config File".

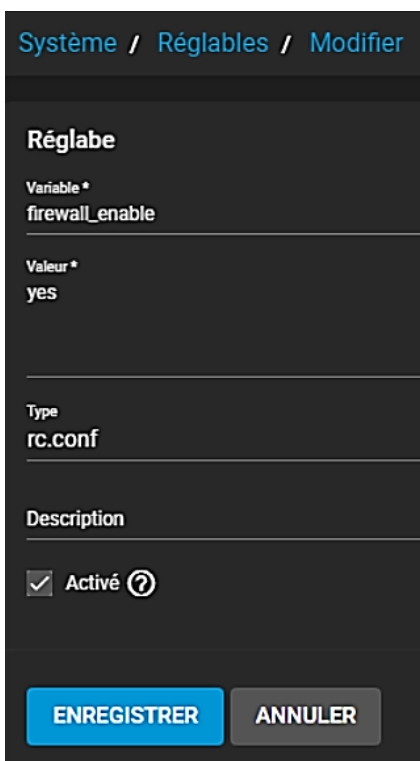
- Démarrez le service « OpenVPN Server » en déplaçant le bouton sur la droite et cochez la case « Démarrage automatique » :



A dark bar representing the OpenVPN Server service. It contains a toggle switch (currently on the left) and a checkbox (checked). Red arrows point from the text above to these two controls.

- Cliquez ensuite sur « Système » et « Réglables »
- Cliquez le bouton « Ajouter » (en haut à droite de l'écran)
- **Ajoutez impérativement les variables suivantes :**

ACTIVATION DU PARE-FEU



The screenshot shows the "Système / Réglables / Modifier" page. Under the "Réglable" section, the variable "firewall_enable" is set to the value "yes". The type is "rc.conf". At the bottom, there is a checkbox labeled "Activé" which is checked, and two buttons: "ENREGISTRER" (blue) and "ANNULER" (grey).

VARIABLE : firewall_enable
VALEUR : yes

AUTORISATION DES CONNEXIONS VPN DANS LE PARE-FEU

Système / Réglables / Modifier

Réglable

Variable *
firewall_type

Valeur *
open

Type
rc.conf

Description

☒ Activé ?

ENREGISTRER ANNULER

VARIABLE : firewall_type
VALEUR : open

ACTIVATION DE LA REDIRECTION

Système / Réglables / Modifier

Réglable

Variable *
gateway_enable

Valeur *
yes

Type
rc.conf

Description

☒ Activé ?

ENREGISTRER ANNULER

VARIABLE : gateway_enable
VALEUR : yes

ACTIVATION DE LA TRANSLATION D'ADRESSE (NAT)

Système / Réglables / Modifier

Réglable

Variable*
natd_enable

Valeur*
yes

Type
rc.conf

Description

☒ Activé ?

ENREGISTRER ANNULER

VARIABLE : natd_enable
VALEUR : yes

Système / Réglables / Modifier

Réglable

Variable*
net.inet.ip.forwarding

Valeur*
1

Type
sysctl

Description

☒ Activé ?

ENREGISTRER ANNULER

VARIABLE : net.inet.ip.forwarding
VALEUR : 1

Système / Réglables / Modifier

Réglable

Variable *
natd_interface

Valeur *
em0

Type
rc.conf

Description

☒ Activé ?

ENREGISTRER ANNULER

Indiquez, ici, le nom de votre interface réseau. Cette valeur est stipulée dans « Réseau – Résumé réseau ».

VARIABLE : natd_interface
VALEUR : em0

Réseau / Résumé réseau

Résumé réseau

Interfaces

Nom	Adresse IPv4
em0	192.168.1.29/24

Système / Réglables / Modifier

Réglable

Variable *
natd_flags

Valeur *
-dynamic -m

Type
rc.conf

Description

☒ Activé ?

ENREGISTRER ANNULER

VARIABLE : natd_flags
VALEUR : -dynamic -m

- Cliquez le bouton « Enregistrer » à chaque ajout de paramètre

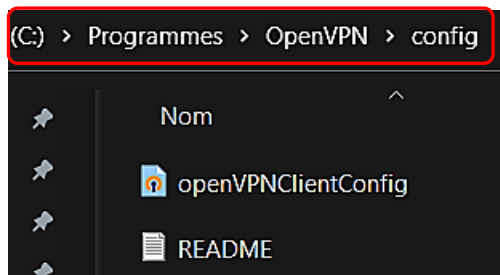
REDEMARREZ IMPERATIVEMENT TRUENAS UNE FOIS TOUS LES PARAMETRES SAISIS

5^{ème} étape – PREPARATION DE LA CONNEXION OPENVPN SUR LE POSTE CLIENT

- Téléchargez le client OpenVPN depuis le site <https://openvpn.net/community-downloads/>
- Ici, nous avons pris le client OpenVPN 2.5.6



- Installez le client OpenVPN sur le poste client (qui se connectera au NAS via le VPN)
- Copiez le fichier de configuration OpenVPNClientConfig précédemment téléchargé dans le répertoire suivant sur le poste client :



Attention, le fichier de configuration doit être copié dans le répertoire « config ».

6^{ème} et dernière étape – TEST DE CONNEXION VPN DEPUIS LE POSTE CLIENT

Avant de lancer votre connexion VPN depuis un poste client extérieur, il faut impérativement créer une redirection de ports dans votre routeur (box) afin de laisser passer les paquets UDP.

Connectez-vous à l'interface de votre box (ici nous utilisons une box Free) et créez la redirection de port vers votre serveur NAS. Ici, nous présentons la procédure pour une Freebox :

- Ouvrez les paramètres avancés de la Freebox
- Ouvrez la « Gestion des ports »
- Ajoutez une redirection de ports qui autorise l'accès à Truenas via le port UDP 1194 :

A screenshot of the 'Redirection de port' (Port Forwarding) configuration interface. The interface has a dark header with the title 'Redirection de port' and a close button. Below the header, there are several fields with labels and values, and a 'Commentaire' field at the bottom. Annotations with red arrows point to specific fields: 'IP Destination' (192.168.1.29), 'Redirection active' (checked), 'IP source' (Toutes), 'Protocole' (UDP), 'Port de début' (1194), 'Port de fin' (1194), and 'Port de destination' (1194). The 'Commentaire' field contains the text 'Accès VPN Truenas'. At the bottom, there are two buttons: 'Annuler' (Cancel) and 'Sauvegarder' (Save).

Redirection de port

IP Destination : 192.168.1.29

Redirection active : ☒

IP source : Toutes

Protocole : UDP

Port de début : 1194

Port de fin : 1194

Port de destination : 1194

Commentaire : Accès VPN Truenas

Annuler Sauvegarder

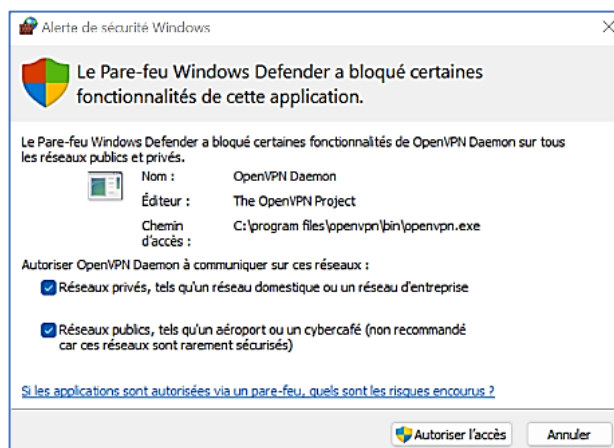
Après avoir installé OpenVPN client sur le poste client, une icône OpenVPN Client doit être accessible dans votre barre des tâches (à gauche de l'heure système).

Lancez la connexion à votre VPN de la manière suivante :

- Faites un clic droit sur l'icône : votre connexion VPN doit être affichée.
- Sélectionnez la connexion VPN relative à votre serveur Truenas (si vous en avez plusieurs) et cliquez sur « Connecter ».

La connexion VPN doit se lancer (une fenêtre s'affiche pour vous informer de l'état d'avancement).

Il est possible que vous ayez un message d'alerte de Windows vous demander d'autoriser l'accès : dans ce cas, autorisez l'accès.

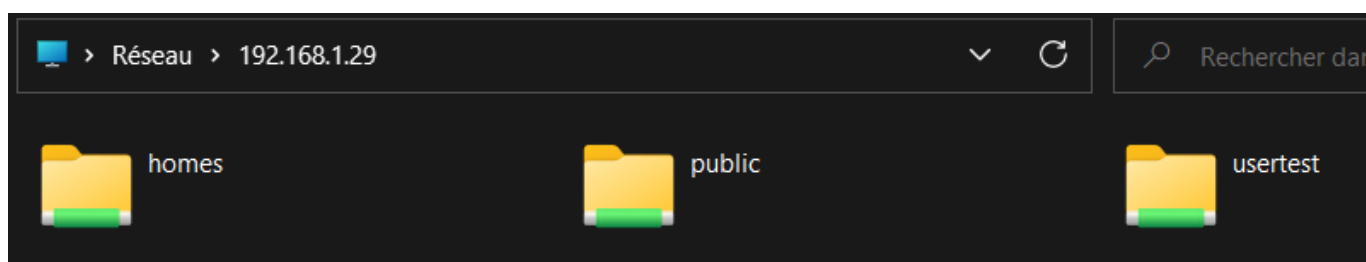


Si vous effectuez un clic droit sur l'icône OpenVPN client, vous constaterez que la connexion est bien active ; il est possible d'afficher le statut :

```
Sun May 15 08:59:19 2022 MANAGEMENT: >STATE:1652597959,CONNECTED,SUCCESS,
```

Le VPN est actif : vous pouvez maintenant vous connecter au NAS depuis l'explorateur en saisissant l'adresse IP de votre NAS. Attention, lors de la première connexion, il faudra vous authentifier selon la politique en vigueur sur votre NAS) :

[\\192.168.1.29](https://192.168.1.29)



Dans la partie suivante, nous allons étudier la mise en place de « snapshots » qui permettront la récupération de données (fichiers ou dossiers) involontairement effacées.

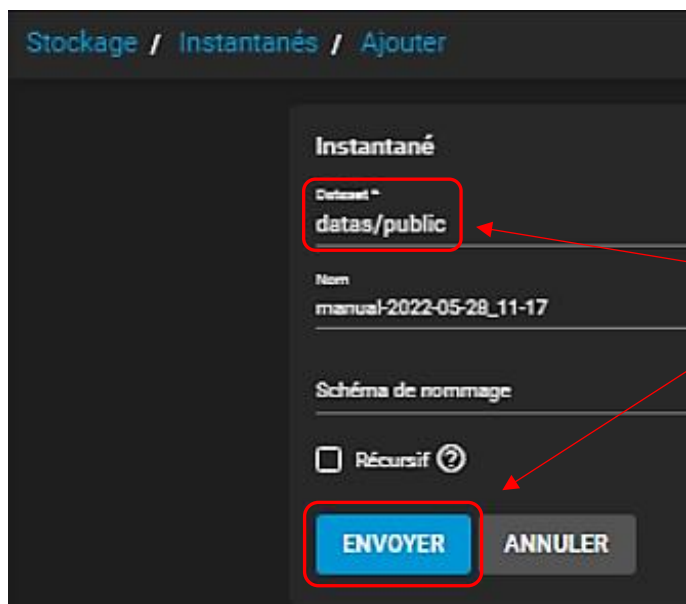
Ces snapshots peuvent être lancés de manière « manuelle » ; on parle « **d'instantanés** » ou de manière automatisée en planifiant leur exécution : on parle « **d'instantanés périodiques** ».

5 – MISE EN PLACE DES SNAPSHOTS ET PLANIFICATION

Il est possible de créer des snapshots qui permettront de restaurer des fichiers en cas de problème.

CREATION D'UN SNAPSHOT

- Cliquez, dans le volet de gauche, sur « Stockage » et « Instantanés » :

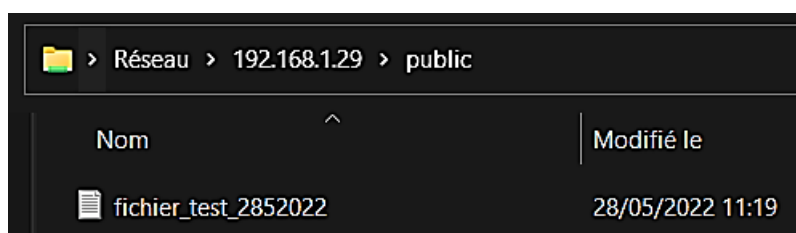


Sélectionnez le dataset pour lequel vous souhaitez effectuer un snapshot et cliquez le bouton « Envoyer ».

Le dataset est créé :

Instantanés						Rechercher	Filtre Instantanés	COLONNES	AJOUTER	Paramètres
<input type="checkbox"/>	Dataset	Instantané	Utilisé	Date Created	Referenced					
<input type="checkbox"/>	datas/public	manual-2022-05-28_11-17	0.10 bytes	2022-05-28 11:25:28	139.50 KiB					

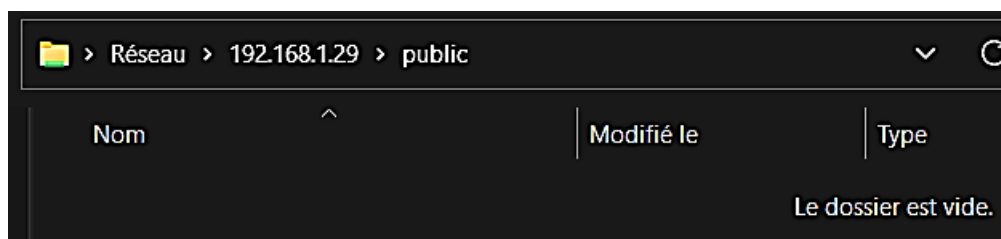
- Créez un fichier de test dans le dataset pour lequel un snapshot est configuré. Ici, nous avons créé un simple fichier texte dans le dataset « public » :



Nom	Modifié le
fichier_test_2852022	28/05/2022 11:19

Ici, nous avons créé un fichier test dans l'espace « public » de notre dataset.

- Supprimez le fichier précédemment créé :



Nom	Modifié le	Type
Le dossier est vide.		

Nous allons, maintenant, lancer une restauration du snapshot afin de restaurer le fichier supprimé.

RESTAURATION D'UN SNAPSHOT

- Cliquez, dans le volet de gauche, sur « Stockage » et « Instantanés »
- Cliquez sur les 3 petits points à droite du snapshot créé précédemment :

Instantanés					
Filtre Instantanés					
COLONNES AJOUTER					
<input type="checkbox"/>	Dataset	Instantané	Utilisé	Date Created	Referenced
<input type="checkbox"/>	datas/public	manual-2022-05-28_11-17	0.10 bytes	2022-05-28 11:25:28	139.50 KiB

- Cliquez l'option « Retour arrière »

Une fenêtre s'ouvre :

- Cliquez la case « Confirmer » et cliquez le bouton « Retour arrière » :

Dataset Rollback From Snapshot

Use snapshot *manual-2022-05-28_11-17* to roll *datas/public* back to 28/05/2022, 11:25:28?

Arrêter la restauration si un instantané existe : ?

☒ Intermédiaire, enfant et clone plus récents ?

☐ Clone plus récent ?

☐ Pas de contrôle de sécurité (ATTENTION) ?

☒ Confirmer

AVERTISSEMENT : le retour en arrière détruit les données sur dataset et peut détruire des instantanés supplémentaires qui sont liés au dataset. Cela peut entraîner une perte de données permanente ! Ne revenez pas en arrière tant que toutes les données et tous les instantanés souhaités n'ont pas été sauvegardés.

ANNULER RETOUR ARRIÈRE

Cliquez la case « Confirmer » et cliquez le bouton « Retour arrière ».

Le fichier « test » a bien été restauré :

Réseau > 192.168.1.29 > public			
Nom	Modifié le	Type	Taille
fichier_test_2852022	28/05/2022 11:19	Document texte	0 Ko

PLANIFICATION D'UN SNAPSHOT

Attention, avant de configurer une planification, assurez-vous que l'heure système de votre serveur Truenas est bien configurée. Pour cela, rendez-vous dans « Système » et « Général » et sélectionnez le fuseau horaire correspondant à votre région :

Fuseau horaire

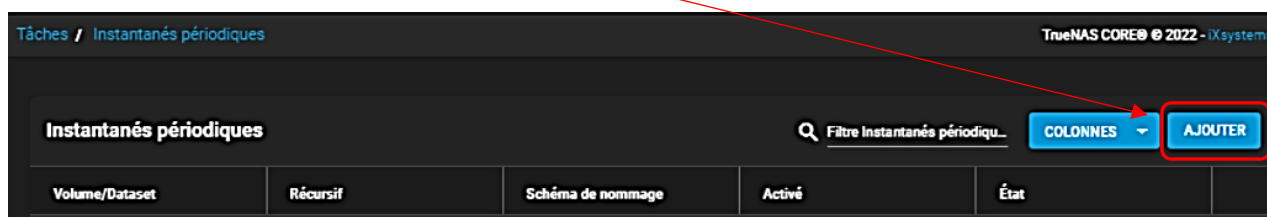
Europe/Paris

Format de l'heure

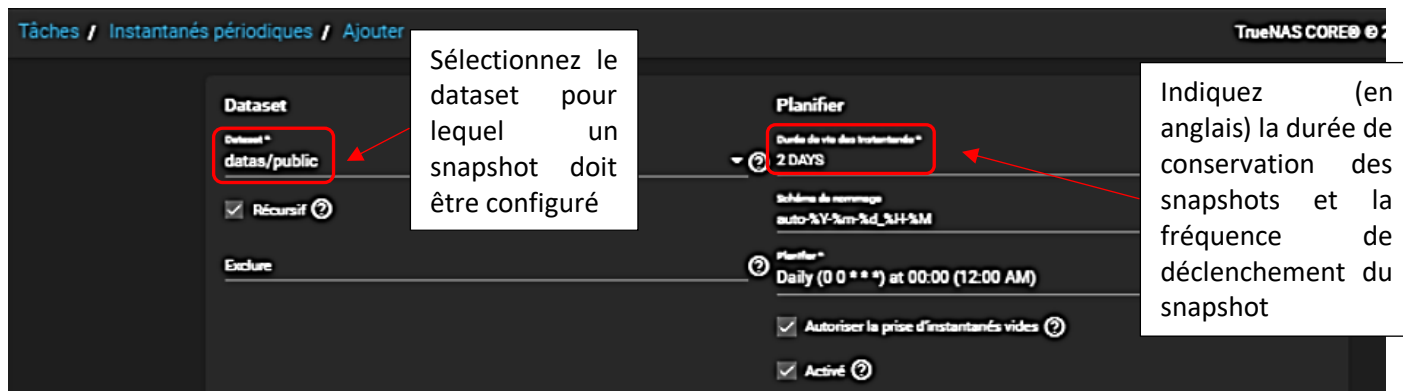
14:51:50 (24 Hours)

Dans cette partie, nous allons configurer la périodicité d'un snapshot pour le dataset « public ».

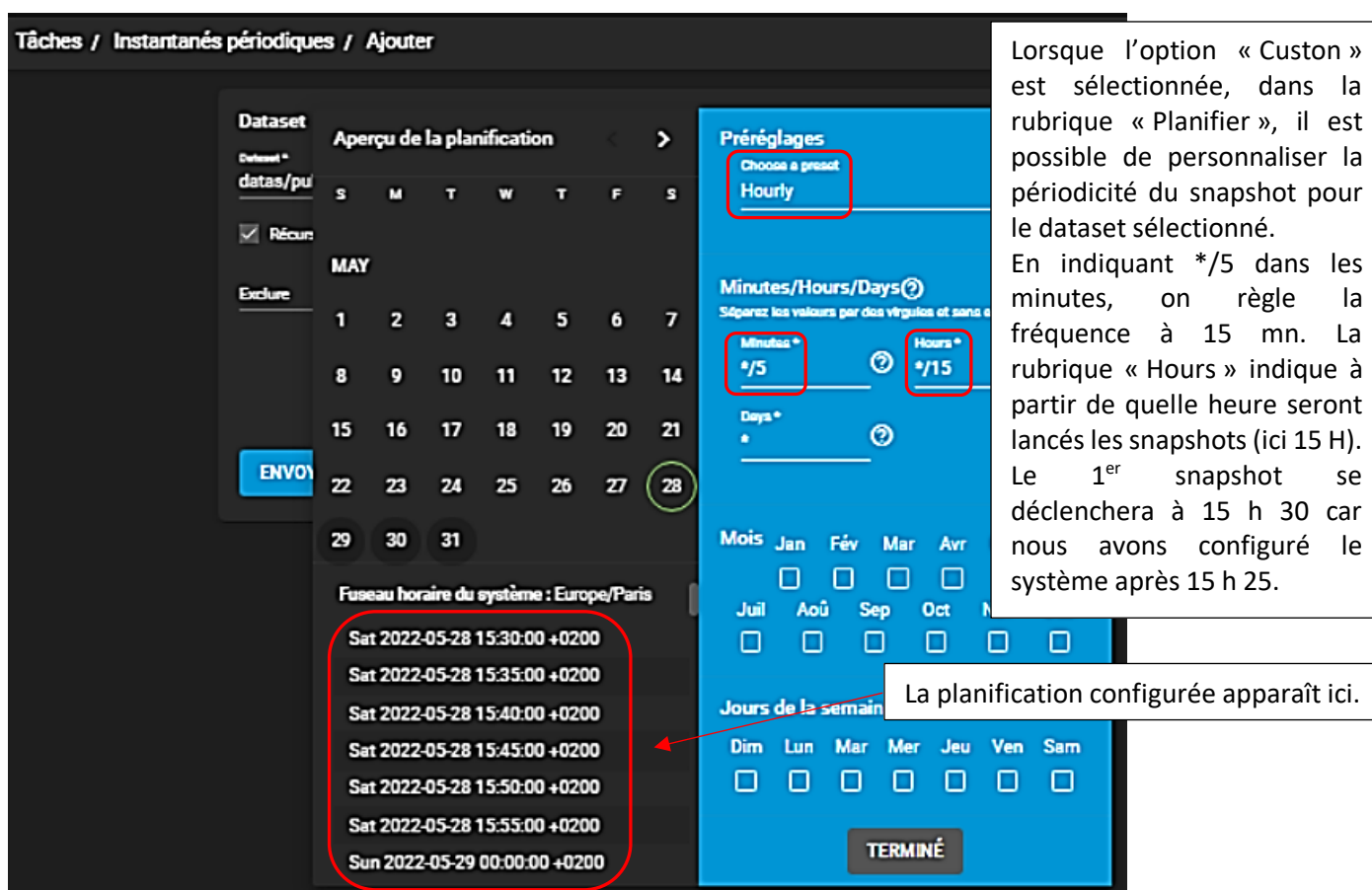
- Cliquez, dans le volet de gauche, sur « Tâches » et « Instantanés périodiques »
- Cliquez sur le bouton « Ajouter » :



Une fenêtre s'ouvre avec différents paramètres à configurer :



En cliquant, dans la rubrique « Planifier », sur « Custom » il est possible de personnaliser la périodicité des snapshots. Ici, nous allons configurer un snapshot chaque jour, toutes les 5 minutes et à partir de 15 H :



- Cliquez le bouton « Terminer » puis le bouton « Envoyer » pour valider les paramètres

La fenêtre indique que l'état des snapshots est en mode « Pending » (attente) :

Instantanés périodiques				
Volume/Dataset	Récuratif	Schéma de nommage	Activé	État
datas/public	oui	auto-%Y-%m-%d_%H-%M	<input checked="" type="checkbox"/>	PENDING

On peut vérifier le bon fonctionnement des snapshots en cliquant « Stockage » et « Instantanés » ; logiquement plusieurs snapshots se seront déclenchés selon la fréquence configurée. Ci-dessous, nous avons configuré des snapshots qui se déclenchent toutes les 5 minutes :

Instantanés				
<input type="checkbox"/>	Dataset	Instantané	Utilisé	Date Created
<input type="checkbox"/>	datas/public	auto-2022-05-28_15-30	0.10 bytes	2022-05-28 15:30:00
<input type="checkbox"/>	datas/public	auto-2022-05-28_15-35	0.10 bytes	2022-05-28 15:35:00

Dans le menu « Tâches » et « Instantanés périodiques » on constate que le snapshot a bien été lancé :

Volume/Dataset	Récuratif	Schéma de nommage	Activé	État
datas/public	oui	auto-%Y-%m-%d_%H-%M	<input checked="" type="checkbox"/>	FINISHED

TEST DU BON FONCTIONNEMENT DES SNAPSHOTS

Afin de vérifier le bon fonctionnement de nos snapshots, on a créé un fichier avant le 1^{er} snapshot de 15 h 30 et un autre après le 2^{ème} snapshot (qui était à 15 h 30) ainsi qu'un dossier :

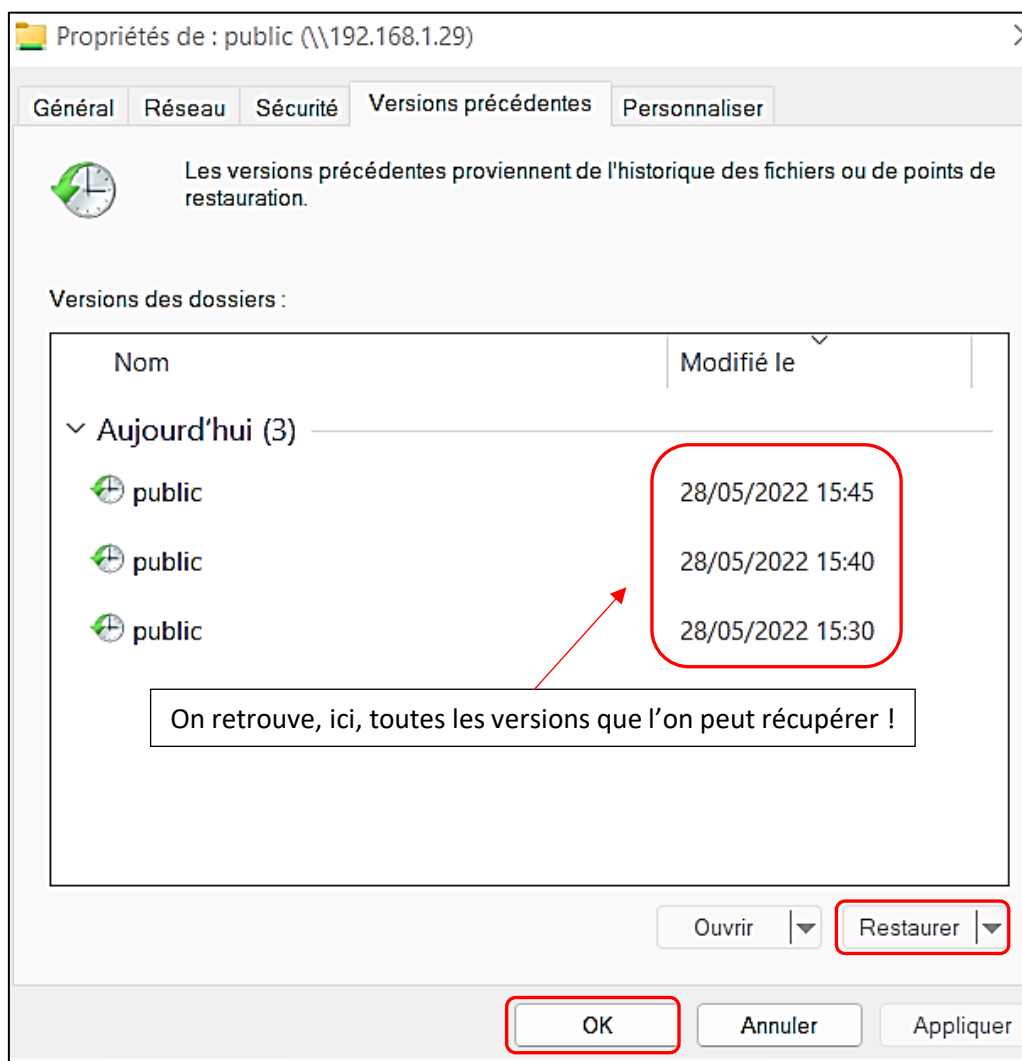
Réseau > 192.168.1.29 > public		
Nom	Modifié le	
fichier_1	28/05/2022 15:28	Fichier créé avant le lancement du 1 ^{er} snapshot (qui était à 15 h 30).
Nouveau dossier	28/05/2022 15:36	Fichier et dossier créés après le 2 ^{ème} snapshot (qui était à 15 h 35).
fichier_2	28/05/2022 15:36	

On supprime le « fichier_1 » avant l'exécution du snapshot de 15 h 45 :

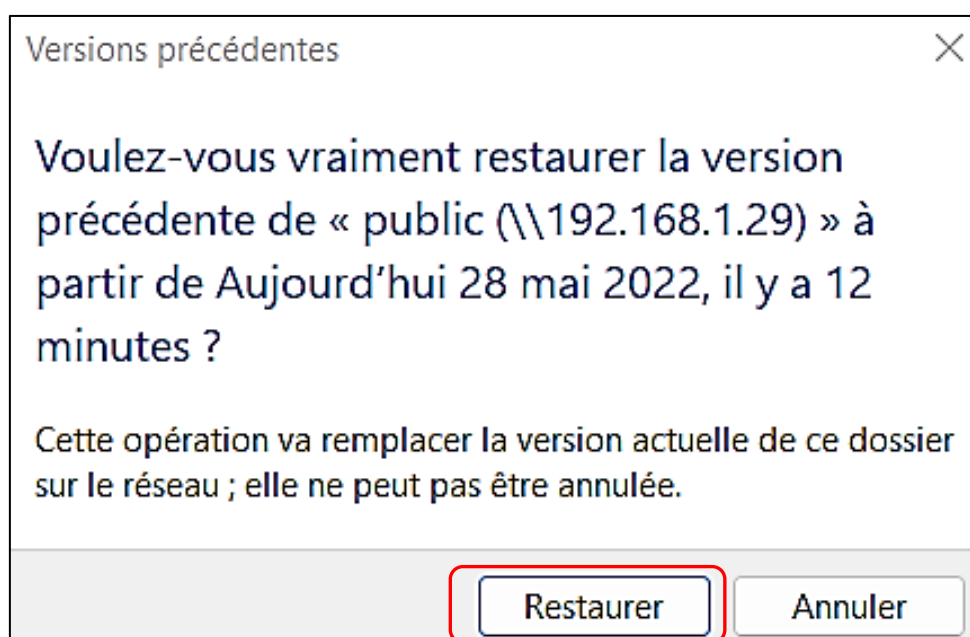
Réseau > 192.168.1.29 > public	
Nom	Modifié le
Nouveau dossier	28/05/2022 15:36
fichier_2	28/05/2022 15:36

Le fichier « fichier_1 » a été supprimé **avant** l'exécution du snapshot de 15 h 45.

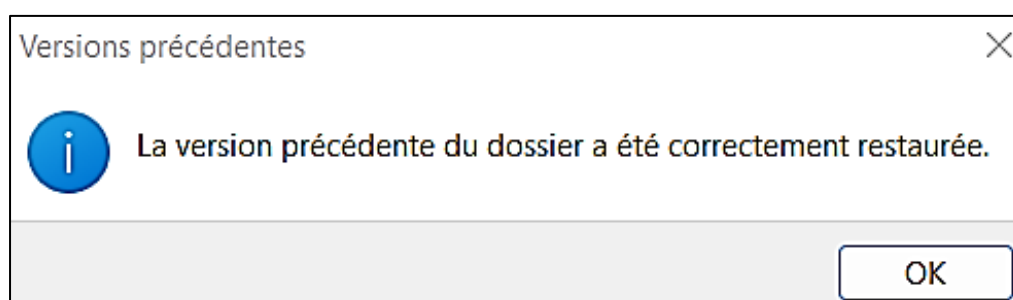
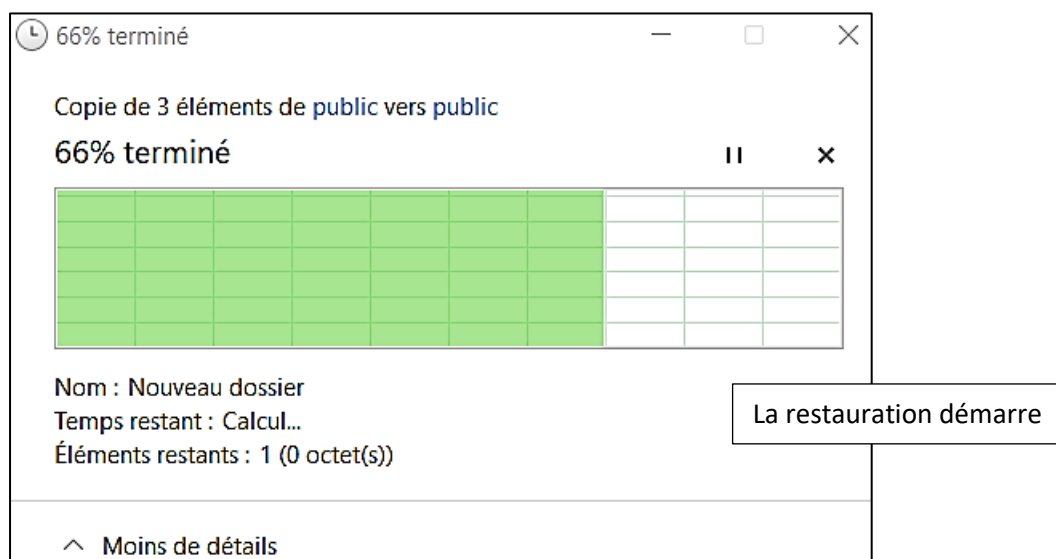
Si, dans l'explorateur Windows, l'on fait un clic droit sur le dossier « public » et que l'on clique « Propriétés » et l'onglet « Versions précédentes », on constate que différents points de restauration ont bien été créés :



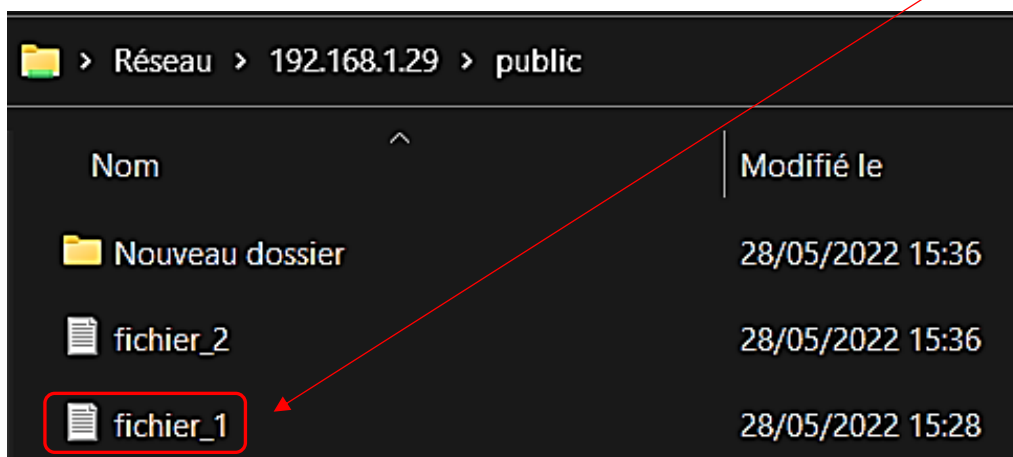
On peut effectuer, depuis l'explorateur Windows, une restauration à une date antérieure ou à un horaire antérieur ici. Pour cela, on sélectionne la version à restaurer et on clique sur « Restaurer » :



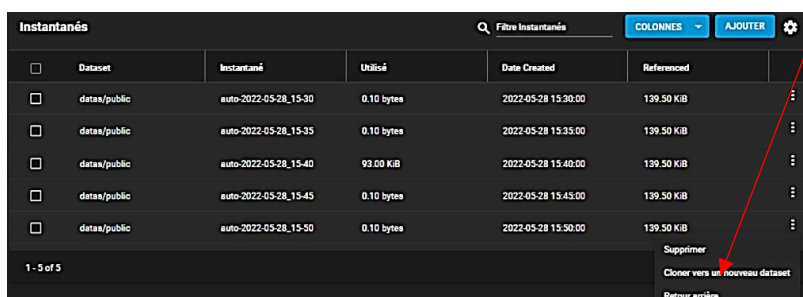
L'opération de restauration se lance :



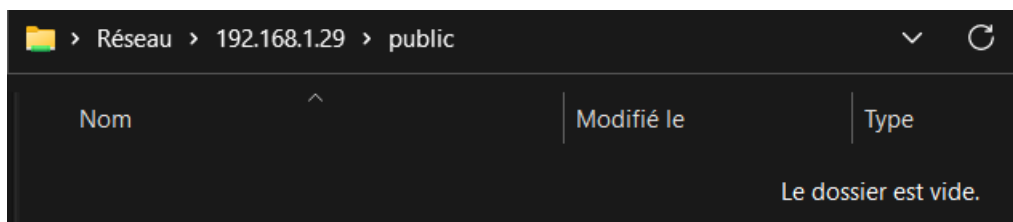
Le fichier « fichier_1 » que nous avons supprimé précédemment a été restauré :



Il est également possible de restaurer un snapshot depuis l'interface de Truenas (« Stockage » et « Instantanés ») en cliquant les 3 petits points sur la droite et en cliquant « Retour arrière » :



Par exemple, nous supprimons l'ensemble des fichiers présents dans notre dataset « public » :



Nous faisons un « Retour arrière » avec le dernier snapshot disponible. L'intégralité du dossier est revenu :

