TUTORIEL

L'informatique par l'exemple





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

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 II 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, <u>nous allons présenter l'installation de Truenas en version « core »</u> (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 FICHIER « ISO »

- Ouvrez un navigateur et téléchargez le fichier ISO directement depuis le site officiel de Truenas : <u>https://www.truenas.com/download-truenas-core/</u>
- 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 quelle 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 » :

TrueNAS	13.0-RELEASE	Console Se	etup
	1 Install/	Upgrade	
	3 Reboot Su	ystem Sveter	
	4 SNULDOWN	aystem	
L			J
	2	(Capacil)	

 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 :

Choose destination media Select one or more drives where TrueNAS should be installed (use arrow keys to navigate to the drive(s) for installation; select a drive with the spacebar).								
[*] ada0 QEMU HARDDISK 10.0 GiB [] ada1 QEMU HARDDISK 15.0 GiB [] ada2 QEMU HARDDISK 15.0 GiB [] ada3 QEMU HARDDISK 15.0 GiB [] ada3 QEMU HARDDISK 15.0 GiB [] ada4 QEMU HARDDISK 15.0 GiB								
<pre>Cancel></pre>								

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

WARNING: - This will erase ALL partitions and data on ada0. - You can't use ada0 for sharing data.
NOTE: - Installing on SATA, SAS, or NVMe flash media is recommended. USB flash sticks are discouraged.
Proceed with the installation?
<pre>< Yes > < No ></pre>

 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 » :

Enter you password	ır r	oot	pas	sword; cancel for no root
Password Confirm	l: Pa⊆	suor	d:	
	<	OK	>	K <mark>B</mark> ancel>

 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 :

TrueNAS can be booted in either BIOS or UEFI mode. BIOS mode is recommended for legacy and enterprise hardware, whereas UEFI may be required for newer consumer motherboards. <Boot via UEFI> Boot Node

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 » :

1 Install/Upgrade 2 Shell 3 Reboot System 4 Shutdown System
<pre>Cancel></pre>

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) :

	🛠 TrueNAS		≡ <				₫ systems	¢	8		: U
	Areat		Dashboard					TrueNAS	Coreø © 20	22 - iXs	ystems, In
	truenas.local										
8	Dashboard			System Information	СРО	ili,	Memory				<u>.</u>
*	Accounts	•		Platform: Generic	Т	Threads: 1 threads	70				
	System	•		Version: TrueNAS-13.0-RELEASE	1% Avg Usage	Highest Usage: 1% (Thread #0)	/ . O GiB total available (ECC)	(
	Tasks	•		HostName: truenas.local		Hottest: Data not provided	Free: 6.1 GiB				
*	Network	•		Uptime: 9 minutes as of 06:58	Stats Per Thread	Usage	ZFS Cache: 0.2 GiB	$\langle \langle \rangle$			
	Storage	•			100 80 60 40		Services: 1.5 GiB				
⊕	Directory Services	•	CHECK FOR UPDATES								
	Sharing	•									
	Services		Interface	¢ 🛛	TrueNAS Help						
۲	Plugins	I		Overview	The TrueNAS Docu	mentation Site is a collaborative website					
IÖI	Jails		em0	Media Type: Ethernet	system.	and information about your new storage					
11	Reporting		LINK STATE UP 🥥	Media Subtype: 1000baseT	The TrueNAS Comm questions and inter	nunity Forums are the best place to ask act with fellow TrueNAS users.					
	Virtual Machines		In: 0.03 KiB/s Out: 0.09 KiB/s	IP Addresses: 192.168.1.29/24	You can join the Tru	NAS Newsletter for monthly updates and					
4	Display System Proces	ses			atest development						
>_	Shell				TrueNAS CORE is Free and Ope	en Source software, which is provided as-is with no warranty.					

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 :

Gestionn	Gestionnaire de volume									
Nom* datas RÉINITIAI I	Nom* datas ⑦ □ Chiffrement ⑦ RÉINITIALISER LA MISE EN PAGE SUGGÉRER UNE MISE EN PAGE Ø AJOUTER VDEV -									
	Disques d	lisponibles					Données V	/Devs		RÉPÉTER
	Disque	Туре	Capacity				Disque	Туре	Capacity	
	ada1	UNKNO	15 GiB		→ ←	No data to	display			
\checkmark	ada2	UNKNO	15 GiB			0 selected	l / O total			
\checkmark	ada3	UNKNO	15 GiB			Stripe	0			▼ x
~	ada4	UNKNO	15 GiB			Capacité brut	te estimée: O B O			

 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 :

Données VDevs									
	Disque	Туре	Capacity						
	ada1	UNKNOW	15 GiB						
	ada2	UNKNOW	15 GiB						
\checkmark	ada3	UNKNOW	15 GiB						
Stripe									
Miroir									
Raid-z									
Raid-z2	Raid-z2								
Capacite brute	estimee: 26 GiB 🔍								

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 :

Raid-z Capacité brute estimée: 39 GiB 🕐 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 (Syst	tem Dataset Pool)		ON	ILINE 🥑 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



• 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	tz4	14.24	false	OFF		8
public	FILESYSTEM	139.5 KiB	36.25 GiB	Hérite (lz4)	1.00	false	OFF	espace de partage commun	8

:

• 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 »

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 :



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 :

- 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 » :



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 »

Partages / SMB / Ajouter	
Basique	
Chamin * /mnt/datas/utilisateurs	
v 🖿 /mnt	partage.
▶ ■ public ACL	
► in usertest ► in utilisateurs ACL	
Nom utilisateurs	En sélectionnant le type de partage « Multi-
oesacer Multi-protocol (AFP/SMB) shares	Protocol (AFP/SMB) shares » on permet aux ordinateurs © Apple d'accéder également à
🗸 Activé 🕥	l'espace de partage public.
ENVOYER ANNULER OPTIONS AVANCÉES	

- Cliquez le bouton « Options avancées »
- <u>Cliquez la case « Utiliser comme partage d'accueil</u> (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 <u>\\192.168.1.29</u> qui correspond à l'adresse IP de notre Truenas) ; une fenêtre d'authentification s'affiche :



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



En créant un nouvel utilisateur, on constate que son dossier personnel est automatiquement créé (/mnt/datas/utilisateurs/usertest) dans le dataset « utililsateurs ». 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		- @	Longueur de la clé *	
		<u>•</u> س	2048	Ces paramètres sont à adapter en fonction du
Profile Openyon Root CA	Sélectionnez « Openvpn	-0	Algorithme Digest *	niveau de sécurité
openipiritoor ori	de l'autorité de certification.	·@	SHA250	souhaité (attention plus
			Durée de vie *	l'algorithme est
			820	important plus le
Objet du certificat				temps en fonction de
Paya*		Et	at *	votre matériel).
France		• ⊘ ⊻	IANCHE	
Localité *		0	rganisation *	
AVRANCHES		0	ABOPROF	
Unité organisationnelle		C	ourriel *	
LABOPROF		0 ×	x@xx.fr	
Nom commun		N	oms alternatifs de sujet *	
truenas.local		0	truenas.local 🛞	
		2		
Contraintes de base			Identificateur d	e clé d'autorité
Activé				
Longueur du chemin		ଉ	Configuration de la clé d'a Authority Cert Is	suconté
		°		
Configuration des contraintes de base CA, Critical Extension		- 0)	
		°		~
Utilisation étendue des	clés		Utilisation des	clés
🗸 Activé 🕜			🗸 Activé 🕜	
Usages *			Configuration de l'utilisati	ion des clés
CLIENT_AUTH, SERVER_	AUTH	<u> </u>	Key Cert Sign, Cl	RL Sign, Critical Extension
	Cliquez le bouton «	« Envoyer »		
	une fois les paramè	etres saisis.		
ANNO				

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			Options de certificat	Sélectionnez
Nom* certificat serveur		0	Autorité de certification signataire *	ici l'autorité de
Tree				précédemmen
Internal Certificate		<u>•</u> 0	RSA	t créée.
Profile Openvpn Server Certificate		<u>-</u> 0	Longueur de la clé * 2048	
Sélection « Openv	nnez ici le profil pn Server Certificate ».		Algorithme Digest * SHA256	
			Durée de vie * 825	
Objet du certificat				
Paga* France	,	• @ M	et* ANCHE	
Localité * AVRANCHES		_@u	parisation* ABOPROF	
Unité organisationnelle LABOPROF			und * @xx.fr	
Nan commun truenas.local		_0	ans alternatifs de sujet * truenas.local 😒	
Contraintes de base		_	Identificateur de clé d'autorité	
🖌 Activé 🕜			🔽 Activé 🕜	
Longueur du chemin		0	Configuration de la clé d'autorité Authority Cert Issuer	
Configuration des contraintes de base Critical Extension		<u>-</u> 0)	
Utilisation étendue des clés			Utilisation des clés	
🗸 Activé 🕜			🗸 Activé 🕜	
Usages* SERVER_AUTH		-0	Configuration de l'utilisation des clés Digital Signature, Key Encipherme	ent, Critical Extension
Extension critique (2)	Cliquez le bouton « Envoy une fois les paramètres sai	er » sis.		

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			Options de certificat	Célectionnez isi	
Non*		0	Autorité de certification signataire *	l'autorité de	
			ADTORITE_TROENAS	certification	
Internal Certificate		•0	Type de dé * RSA	précédemment créée	
Profils			Longueur de la clé *		
Openvpn Client Certificate		<u>•</u> 0	2048		
Sé « (lectionnez ici le profil Openvpn Client Certificate ».		Algorithme Digest * SHA256		
			Durfe de vic * 825		
Objet du certificat					
Pays*		- @ #			
		<u>•</u> ⊘≞			
Localité* AVRANCHES		ົ່ງມີ	parisation * ABOPROF		
Unité organisationnelle LABOPROF		`@`¤	unid * @xx.fr		
Nom commun truenas.local		_@	truenas.local		
				-	
Contraintes de base			Identificateur de clé d'autorit	e	
🗸 Activé 🕜			🗸 Activé 🕜		
Longueur du chemin		0	Configuration de la clé d'autorité Authority Cert Issuer		
Configuration des contraintes de base Critical Extension		<u>-</u> 0)		
Utilisation étendue des cl	és		Utilisation des clés		
🗸 Activé 🕜			🗸 Activé 🕜		
Usages * CLIENT_AUTH		•0	Configuration de l'utilisation des clés Digital Signature, Key Agreemen	nt, Critical Extension	
Extension critique 🕥	Cliquez le bouton « Envi	oyer »			
	une fois les paramètres	saisis.			
ENVOYER ANNULER					

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_cliet	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	•	• 1
OpenVPN Server	•	ľ

• Complétez la fenêtre ainsi :

Certificat du client certificat_cliet		-0	Type de périphérique TAP
Root CA AUTORITE_TRUENAS Distant * 192.168.1.29	ATTENTION, ici nous travaillons en local c'est pour cette raison que nous indiquons l'adresse IP de notre serveur Truenas, <u>sinon il faut</u> <u>indiquer un nom de domaine valide</u> afin que l'on puisse accéder depuis l'extérieur au serveur Truenas.	•0 _0 _0	Nobind ⑦ TLS Crypt Auth Activé ⑦ Paramètres supplémentaires
Algorithme d'authentification SHA256 (256 bit digest size)	<u>-</u> 0	
Cipher		<u>-</u> 0	TLS Crypt Auth
Compression		<u>-</u> 0	
Protocole UDP UDP Cliquez le l une fois les	pouton « Enregistrer » s paramètres saisis.	<u>-</u> 0	
ENREGISTRER ANN	ULER		

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 » _____

OpenVPN Client	•		1
OpenVPN Server	•		

• Complétez la fenêtre ainsi :

Services / OpenVPN Server			
Certificat de server * certificat_serve	ur	-0	TAP
Rest CA- AUTORITE_TRU	Indiquez, ici, l'a	dresse du tunnel	Topologie
Server* 10.8.0.0	VPN souhaité. /	Attention, ne pas	TLS Crypt Auth Active 🕜
Put 1194	votre réseau !	e auressage que	Perambites applifmentates 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
Nacrime Sudwate SHA256 (256 b	nton it digest size)	-0	duplicate-on
Cipher	Cliquez le bouton « Enregistrer » une	-@	TLS Crypt Auth
Compression	fois les paramètres	-0	
Protocole UDP	saisis.	-0	
ENREGISTRE	R ANNULER RENOUVEL	ER LA CLÉ STATIQUE TÉI	LÉCHARGER LA CONFIGURATION DU CLIENT

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 :

TLS Crypt Auth Activé (2) Peramitres supplémentates 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-on	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 » :

Select Client Certificate			
Certificat du client certificat_cliet			
ANNULER	ENVOYER		

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



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

OpenVPN Server

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

ACTIVATION DU PARE-FEU

Système / Réglables / Modifier
Réglabe Variable * firewall_enable
Valeur * yes
Type rc.conf
Description
✓ Activé ⑦
ENREGISTRER ANNULER

VARIABLE : firewall_enable VALEUR : yes

AUTORISATION DES CONNEXIONS VPN DANS LE PARE-FEU

Système / Réglables / Modifier
Réglabe Variable * firewall_type
Valeur* open
_{Туре} rc.conf
Description
ENREGISTRER ANNULER
ACTIVATION DE LA REDIRECTION
Système / Réglables / Modifier
Réglabe
Variable * gateway_enable
Valeur * yes

VARIABLE : firewall_type VALEUR : open

VARIABLE : gateway_enable VALEUR : yes

© TUTOS-INFO.FR – INSTALLER ET CONFIGURER TRUENAS 13

ANNULER

Type rc.conf

Description

🗸 Activé 🕜

ENREGISTRER

ACTIVATION DE LA TRANSLATION D'ADRESSE (NAT)

Système / Réglables / Modifier	
Réglabe ^{Variable *} natd_enable ^{Valeur *} yes	VARIABLE : natd_enable VALEUR : yes
^{Туре} rc.conf	
Description Activé ⑦	
ENREGISTRER ANNULER Système / Réglables / Modifier	
Réglabe Variable * net.inet.ip.forwarding	VARIABLE : net.inet.ip.forwarding
Valeur* 1	VALEUR : 1
Type sysctl	
Description	
Activé (?)	

Système / Réglables / Modifier		
Réglabe Variable * natd_interface	VARIABLE : natd_interface VALEUR : em0	
em0 Indiquez, ici, le nom d votre interface réseau Cette valeur est stipulé dans « Réseau – Résum	e J. e é Réseau / Résumé réseau	
Type reseau ».		
Description	Résumé réseau	
Activé 🕜	Interfaces	
	Nom	Adresse IPv4
ENREGISTRER ANNULER	em0	192.168.1.29/24
Système / Réglables / Modifier Réglabe Variable * natd_flags Valeur * -dynamic -m	VARIABLE : natd_flags VALEUR : -dynamic -m	
Type rc.conf Description		
ENREGISTRER ANNULER		

• 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 :



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 :

Redirection de port		×	
IP Destination :	192.168.1.29	On indique ici l'adresse de destination, c'est-à-dire notre serveur Truenas	
Redirection active :			
IP source :	Toutes ┥	protocole UDP auront le droit d'accéder a	u serveur.
Protocole :	UDP ┥	On indique ici le protocole autorisé	
Port de début :	1194		
Port de fin :	1194	On indique ici le port utilisé par le VPN	
Port de destination :	1194	\$	
Commentaire :	Accès VPN Truenas		
	••••		
	XA	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.

Alerte de sécurité Windows						
Le Pare-feu Windows Defender a bloqué certaines fonctionnalités de cette application.						
Le Pare-feu Windov les réseaux publics	vs Defender a et privés.	bloqué certaines fonctionnaîtés de OpenVPN Daemon sur tous				
	Nom :	OpenVPN Daemon				
	Éditeur :	The OpenVPN Project				
	Chemin d'accès :	C: \program files \openvpn \bin \openvpn.exe				
Autoriser OpenVPN	Daemon à con	muniquer sur ces réseaux :				
🔽 Réseaux priv	vés, tels qu'un i	réseau domestique ou un réseau d'entreprise				
Réseaux publics, tels qu'un aéroport ou un cybercafé (non recommandé car ces réseaux sont rarement sécurisés)						
Si les applications sont autorisees via un pare-teu, quels sont les risques encourus ?						
SAutoriser l'accès Annuler						

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

💻 > Réseau > 192.168.1.29	~	С	م	Rechercher dan
homes public				usertest

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 » :



Le dataset est créé :

Instantanés Q Fitre Instantanés				COLONNES - A	JOUTER	•	
	Dataset	Instantané	Utilisé	Date Created	Referenced		
	datas/public	manual-2022-05-28_11-17	0.10 bytes	2022-05-28 11:25:28	139.50 KiB		8

 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 » :



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

• Supprimez le fichier précédemment créé :

📄 > Réseau >	192.168.1.29 > public		~	С
Nom	^	Modifié le	Туре	
		L	e dossier est vi	ide.

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 :

Instanta	nés		م	Filtre Instantanés	COLONNES - AJOUTER	•
	Dataset	Instantané	Utilisé	Date Created	Referenced	
	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 » :



Le fichier « test » a bien été restauré :

🚞 > Réseau > 192.168.1.29 > public		~ C	𝒫 Rechercher dar
Nom	Modifié le	Туре	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 :

Puseeu hontre Europe/Paris	• @
Format de l'Inune 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 » : _____

Tâches / Instantanés périodiques				TrueNAS CORE® @ 2022 - iX systems,
Instantanés périodiques			Q Filtre Instantanés périod	iqu COLONNES AJOUTER
Volume/Dataset	Récursif	Schéma de nommage	Activé	État

Une fenêtre s'ouvre avec différents paramètres à configurer :

Tâches / Instantanés	périodiques / Ajouter	Sélectionnez le			TrueNAS CORE® @ 2
	Dataset Cotent* datas/public Récursir ⑦ Exclure	dataset pour lequel un snapshot doit être configuré	- e	Planifier Eucle de vie des tratentends* 2 DAYS Schleine de normenge Buito-SY-Sum-Scl_SH-SSM Planifier* Dasily (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0	Indiquez (en anglais) la durée de conservation des snapshots et la fréquence de déclenchement du
				Dany (0 0 ••••) at 00:00 (12:00 AM) Autoriser la prise d'instantanés vides (2) Activé (2)	snapshot

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 :

Tâches / Instantanés périodiques / Ajouter Lorsque l'option « Custon »										
	Dataset Cutomi* datas/pu	Aper s	çu de l M	la plar T	iificatio w	on T	< F	> s	Préréglages Choose a preset Hourly	est sélectionnée, dans la rubrique « Planifier », il est possible de personnaliser la périodicité du snapshot pour
	Récure Exclure ENVO	MAY 1 15 22 29	2 9 16 23 30	3 10 17 24 31	4 11 18 25	5 12 19 26	6 13 20 27	7 14 21 28	Minutes/Hours/Days@ Ségarat les valeurs par des virgules et sans e Minufisa* ⑦ Hoars* */5 ⑦ 1/15 Days* * ⑦ Mois Jan Fév Mar Avr	En indiquant */5 dans les minutes, on règle la fréquence à 15 mn. La rubrique « Hours » indique à partir de quelle heure seront lancés les snapshots (ici 15 H). Le 1 ^{er} snapshot se déclenchera à 15 h 30 car nous avons configuré le système après 15 h 25
		Fuse Sat Sat Sat Sat Sat	au hora 2022- 202- 202- 202- 2020	aire du 1 05-28 1 05-28 1 05-28 1 05-28 1 05-28 1 05-28 1 05-28 1 -05-29	eystème 15:30:00 15:35:00 15:40:00 15:45:00 15:55:00 15:55:00 00:00:00	e : Europ 0 +020 0 +020 0 +020 0 +020 0 +020 0 +020 0 +020 0 +020	pe/Pari 0 0 0 0 0 0 0 0	5	Juil Aoû Sep Oct M Jours de la semain Dim Lun Mar Mer Jeu	ification configurée apparaît ici.

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			Q Filtre Instantanés périod	liqu_ COLON
Volume/Dataset	Récursif	Schéma de nommage	Activé	État
datas/public	oui	auto-%Y-%m-%d_%H-%M	N	PENDING

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

Instantar	nés		م	Filtre Instantanés
	Dataset	Instantané	Utilisé	Date Created
	datas/public	auto-2022-05-28,15-30	0.10 bytes	2022-05-28 15:30:00
	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	Récursif	Schéma de nommage	Activé	État 🚽
datas/public	oui	auto-%Y-%m-%d_%H-%M	M	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 :



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 <u>avant</u> 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 :

📜 Propriétés de : public (\\19	2.168.1.29)	×				
Général Réseau Sécurité	Versions précédentes	Personnaliser				
Les versions précédentes proviennent de l'historique des fichiers ou de points de restauration.						
Versions des dossiers :						
Nom		Modifié le				
∼ Aujourd'hui (3) —						
🕀 public	28/05/2022 15:45					
🕀 public	28/05/2022 15:40					
🕀 public		28/05/2022 15:30				
On retrouve, ici	i, toutes les versions qu	e l'on peut récupérer !				
		Ouvrir 🛛 Restaurer				
	ОК	Annuler Appliquer				

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 :

🕒 66% terminé —	-		>	<
Copie de 3 éléments de public vers public				
66% terminé	I	I I	×	
Nom : Nouveau dossier Temps restant : Calcul Éléments restants : 1 (0 octet(s))		La	resta	uration démarre
 Moins de détails 				
Versions précédentes				×
La version précédente du dossier a été	corre	ecter	ment	restaurée.
			(ОК

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

🚞 > Réseau >	> 192.168.1.29 > public	
Nom	^	Modifié le
🛅 Nouveau	dossier	28/05/2022 15:36
fichier_2		28/05/2022 15:36
fichier_1		28/05/2022 15:28

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 » :

Instanta	nés		q	Filtre Instantanés	COLONNES - AJOUTER	•
D	Dataset	Instantané	Utilisé	Date Created	Referenced	
	datas/public	auto-2022-05-28_15-30	0.10 bytes	2022-05-28 15:30:00	139.50 KiB	4
	datas/public	auto-2022-05-28_15-35	0.10 bytes	2022-05-28 15:35:00	139.50 KiB	:
	datas/public	auto-2022-05-28_15-40	93.00 KiB	2022-05-28 15:40:00	139.50 KiB	8
	datas/public	auto-2022-05-28_15-45	0.10 bytes	2022-05-28 15:45:00	139.50 KiB	8
	datas/public	auto-2022-05-28_15-50	0.10 bytes	2022-05-28 15:50:00	139.50 KiB	8
1.545					Supprimer	
1-3013					Cioner vers un nouveau da	taset
					Retour artière	

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 :

🚞 > Réseau > 192.168.1.29 > public	
Nom	Modifié le
Nouveau dossier	28/05/2022 15:36
fichier_2	28/05/2022 15:36
fichier_1	28/05/2022 15:28