



TrueNAS
CORE



FileZilla

Document d'exploitation

Table des matières

- 1. Définition**
- 2. Prérequis**
- 3. Installation et configuration**
- 4. FileZilla**
- 5. Fonctionnement**

1. Définition

FTP signifie File Transfer Protocol. Il s'agit d'un protocole qui permet de transférer des fichiers d'un ordinateur à un serveur et vice versa. Vos fichiers trop lourds pour être envoyés par mail peuvent être envoyés par FTP par exemple.

Par défaut, FTP n'est pas sécurisé. Hors, nous avons besoin de sécuriser les transferts de fichiers pour qu'ils ne soient pas interceptés par des personnes malveillantes.

Il y a plusieurs manières de sécuriser FTP. Nous pouvons l'allier à SSH qui est un protocole de communication sécurisé, nous obtiendrons alors un SFTP pour SSH File Transfer Protocol. Nous pouvons également utiliser TLS pour Transport Layer Security qui est le successeur du protocole SSL - Secure Socket Layer. Il s'agit également d'un protocole de communication chiffrée. Le protocole alors obtenu est FTPS - File Transfer Protocol Secure. Il s'agit de la forme implicite. Pour la forme explicite nous avons FTPES - File Transfer Protocol Explicit Protocol.

Dans le cadre du projet pour l'entreprise M2L, nous avons décidé d'utiliser FTPES qui est plus simple à mettre en place que FTPS qui nécessite des configurations sur le pare-feu du poste client mais également sur le routeur fourni par le FAI.

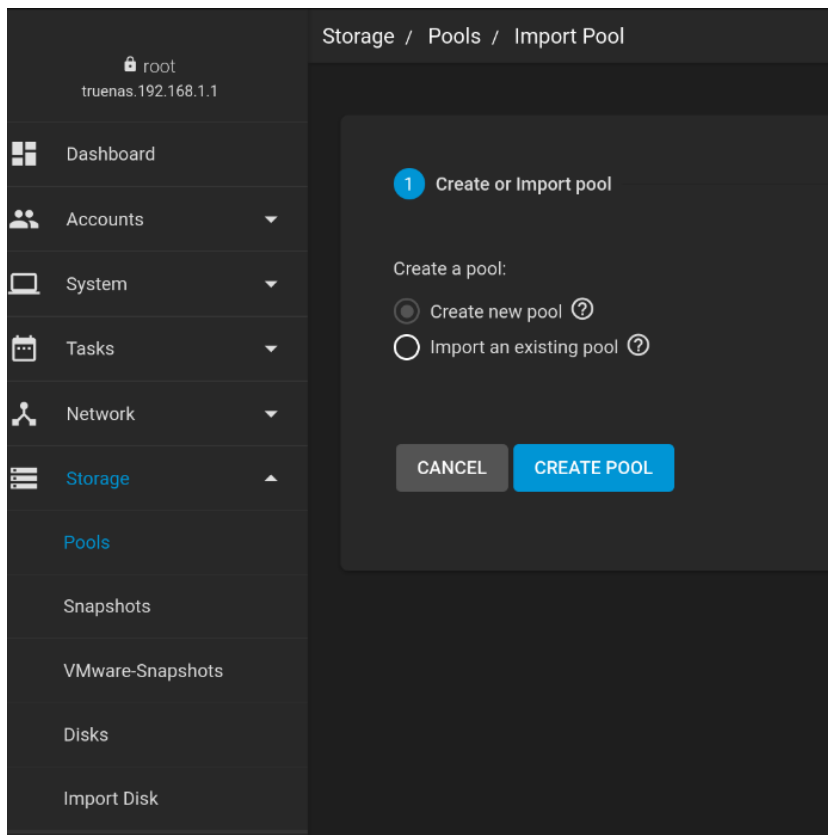


2. Prérequis

- TrueNAS ou FreeNas d'installé.
- Un Filezilla pour vos tests, ou toutes autres applications vous permettant de tester votre serveur FTPES
- Un disque de stockage supplémentaire

3. Installation

Dans un premier temps, nous allons créer une pool de stockage :



A cette étape de création de la pool, nous allons ajouter le disque de stockage ainsi créer notre pool :

The screenshot shows the 'Pool Manager' interface. At the top, there's a 'Name' field with 'storage' entered and an 'Encryption' checkbox. Below are buttons for 'RESET LAYOUT', 'SUGGEST LAYOUT', and 'ADD VDEV'. The 'Available Disks' section contains a table with one row: 'da2' (Type: UNKNO, Capacity: 32 GiB). The 'Data VDevs' section is empty, showing 'No data to display'. At the bottom, there are filters for disks by name or capacity, an estimated total raw data capacity, and 'CREATE' and 'CANCEL' buttons.

Available Disks	Data VDevs												
<table><tr><th>Disk</th><th>Type</th><th>Capacity</th></tr><tr><td>da2</td><td>UNKNO</td><td>32 GiB</td></tr></table>	Disk	Type	Capacity	da2	UNKNO	32 GiB	<table><tr><th>Disk</th><th>Type</th><th>Capacity</th></tr><tr><td colspan="3">No data to display</td></tr></table>	Disk	Type	Capacity	No data to display		
Disk	Type	Capacity											
da2	UNKNO	32 GiB											
Disk	Type	Capacity											
No data to display													

Une fois cette étape effectuée, nous allons ajouter un dataset (ensemble de données en français) :

The screenshot shows the ZFS dataset 'storage' with properties: ONLINE, 420 KiB (0%) Used, 28.58 GiB Free. A dropdown menu is open, showing actions like 'Add Dataset', 'Add Zvol', 'Edit Options', 'Edit Permissions', 'User Quotas', 'Group Quotas', and 'Create Snapshot'.

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
storage	FILESYSTEM	420 KiB	28.58 GiB	lz4	1.00	false	OFF	

Voici la configuration, ici nous l'avons nommé FTPS :

Name and Options

Name *

FTPS

?

Comments

?

Sync

Inherit (standard)

▼

?

Compression level

Inherit (lz4)

▼

?

Enable Atime

Inherit (on)

▼

?

Encryption Options

☒ Inherit (non-encrypted) ?

Other Options

ZFS Deduplication

Inherit (off)

▼

?

Case Sensitivity

Sensitive

▼

?

Share Type

Generic

▼

?

SUBMIT

CANCEL

ADVANCED OPTIONS

Par la suite nous allons configurer dans le Certificate Authorities, qui gère les autorisations de certificat, un nouveau certificat nécessaire pour créer un certificat auto signé pour notre serveur FTPS :

The screenshot shows the TrueNAS web interface for adding a new Certificate Authority. The left sidebar contains a navigation menu with options like Accounts, System, General, NTP Servers, Boot, Advanced, Email, System Dataset, Reporting, Alert Services, Alert Settings, Cloud Credentials, SSH Connections, SSH Keypairs, Tunables, Update, and CAs. The main content area is titled 'System / Certificate Authorities / Add' and contains a form with the following sections:

- Identifier and Type**: Name (certFTPS), Type (Internal CA), Profiles (SHA512).
- Certificate Options**: Key Type (RSA), Key Length (4096), Digest Algorithm (SHA512), Lifetime (3650).
- Certificate Subject**: Country (France), State (France), Locality (Every), Organization (M2L), Email (M2L@pro.fr), Common Name (M2L).
- Basic Constraints**: Enabled checkbox.
- Extended Key Usage**: Enabled checkbox.
- Authority Key Identifier**: Enabled checkbox.
- Key Usage**: Enabled checkbox.

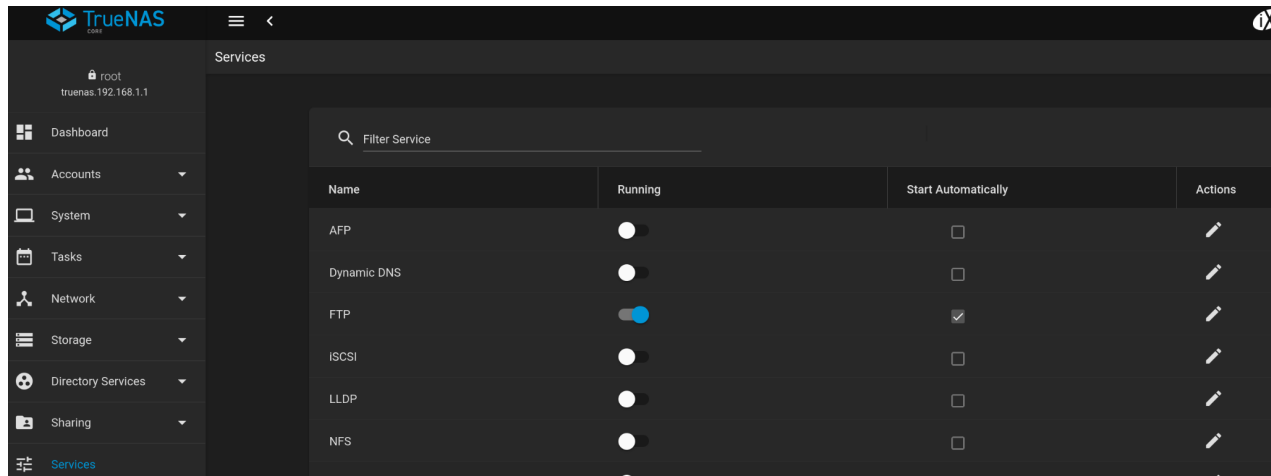
At the bottom of the form are 'SUBMIT' and 'CANCEL' buttons.

Puis nous devons créer un certificat en utilisant le CA précédemment créé :

System / Certificates / Add

Identifier and Type		Certificate Options	
Name *	<input type="text" value="certm2l"/>	Signing Certificate Authority *	<input type="text" value="certm2l"/>
Type	<input type="text" value="Internal Certificate"/>	Key Type *	<input type="text" value="RSA"/>
Profiles	<input type="text" value=""/>	Key Length *	<input type="text" value="4096"/>
		Digest Algorithm *	<input type="text" value="SHA512"/>
		Lifetime *	<input type="text" value="3650"/>
Certificate Subject			
Country *	<input type="text" value="United States"/>	State *	<input type="text" value=""/>
Locality *	<input type="text" value=""/>	Organization *	<input type="text" value=""/>
Organizational Unit	<input type="text" value=""/>	Email *	<input type="text" value=""/>
Common Name	<input type="text" value=""/>	Subject Alternate Names *	<input type="text" value=""/>
Basic Constraints		Authority Key Identifier	
<input type="checkbox"/> Enabled		<input type="checkbox"/> Enabled	
Extended Key Usage		Key Usage	
<input type="checkbox"/> Enabled		<input type="checkbox"/> Enabled	
<input type="button" value="SUBMIT"/> <input type="button" value="CANCEL"/>			

Une fois le service FTP en le cochant simplement dans les Services, nous allons le configurer :



Nous avons choisi d'utiliser le port 21, puis activé le TLS et choisi le certificat que l'on a créé, enfin nous validons notre configuration :

The screenshot displays the ProFTPD configuration interface with the following settings:

- General Options**
 - Port *: 21
 - Clients *: 5
 - Connections *: 0
 - Login Attempts *: 2
 - Timeout *: 600
 - Certificate: certftps
- Access**
 - ☒ Always Chroot
 - ☒ Allow Root Login
 - ☐ Allow Anonymous Login
 - ☒ Allow Local User Login
 - ☐ Require IDENT Authentication
- File Permissions**

	Read	Write	Execute
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
- Directory Permissions**

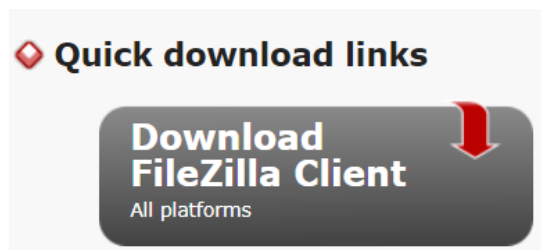
	Read	Write	Execute
User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Other	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- TLS**
 - ☒ Enable TLS
 - TLS Policy: On
 - ☐ TLS Allow Client Renegotiations
 - ☒ TLS Allow Dot Login
 - ☐ TLS Allow Per User
 - ☐ TLS Common Name Required
 - ☒ TLS Enable Diagnostics
 - ☐ TLS Export Certificate Data
 - ☐ TLS No Certificate Request
 - ☐ TLS No Empty Fragments
 - ☒ TLS No Session Reuse Required
 - ☐ TLS Export Standard Vars
 - ☐ TLS DNS Name Required
 - ☐ TLS IP Address Required

Notre serveur FTPS est fonctionnel. Il ne reste alors qu'à créer les user dont nous avons besoin, ainsi que de leur donner un dossier dans lequel ils auront accès.

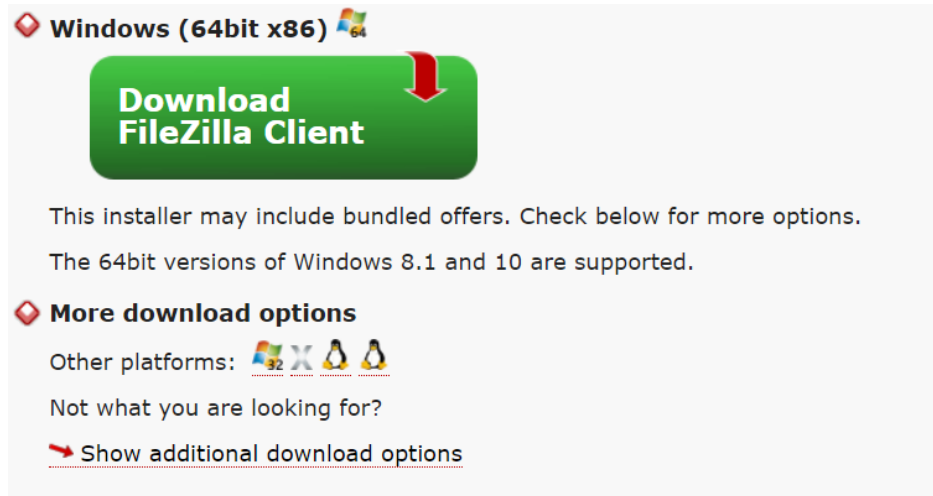
4. FileZilla

FileZilla est un client FTP. Ce logiciel permet de se connecter à un serveur distant et de télécharger des fichiers à partir et sur ce serveur. Celui-ci est gratuit.

Nous nous sommes rendus sur le site <https://filezilla-project.org/>. Deux choix s'offraient à nous, FileZilla Client et FileZilla Serveur. Nous avons sélectionnés FileZilla Client :



Puis avons choisi la version qui correspondait à notre système d'exploitation, c'est-à-dire celle étant compatible avec Windows 10.



Maintenant que FileZilla est installé, lançons le puis configurons le pour pouvoir se connecter au serveur.



5. Fonctionnement

Dans Hôte, indiquons l'adresse ip du serveur précédé de l'indicatif "ftpes".

Puis nous entrons le nom du compte local autorisé à se connecter au serveur, son mot de passe et le numéro de port.

Par défaut, FTP se connecte sur le port 20, FTPS utilise les ports 989 et 990, FTPES lui, le port 21 et SFTP utilise le port 22.

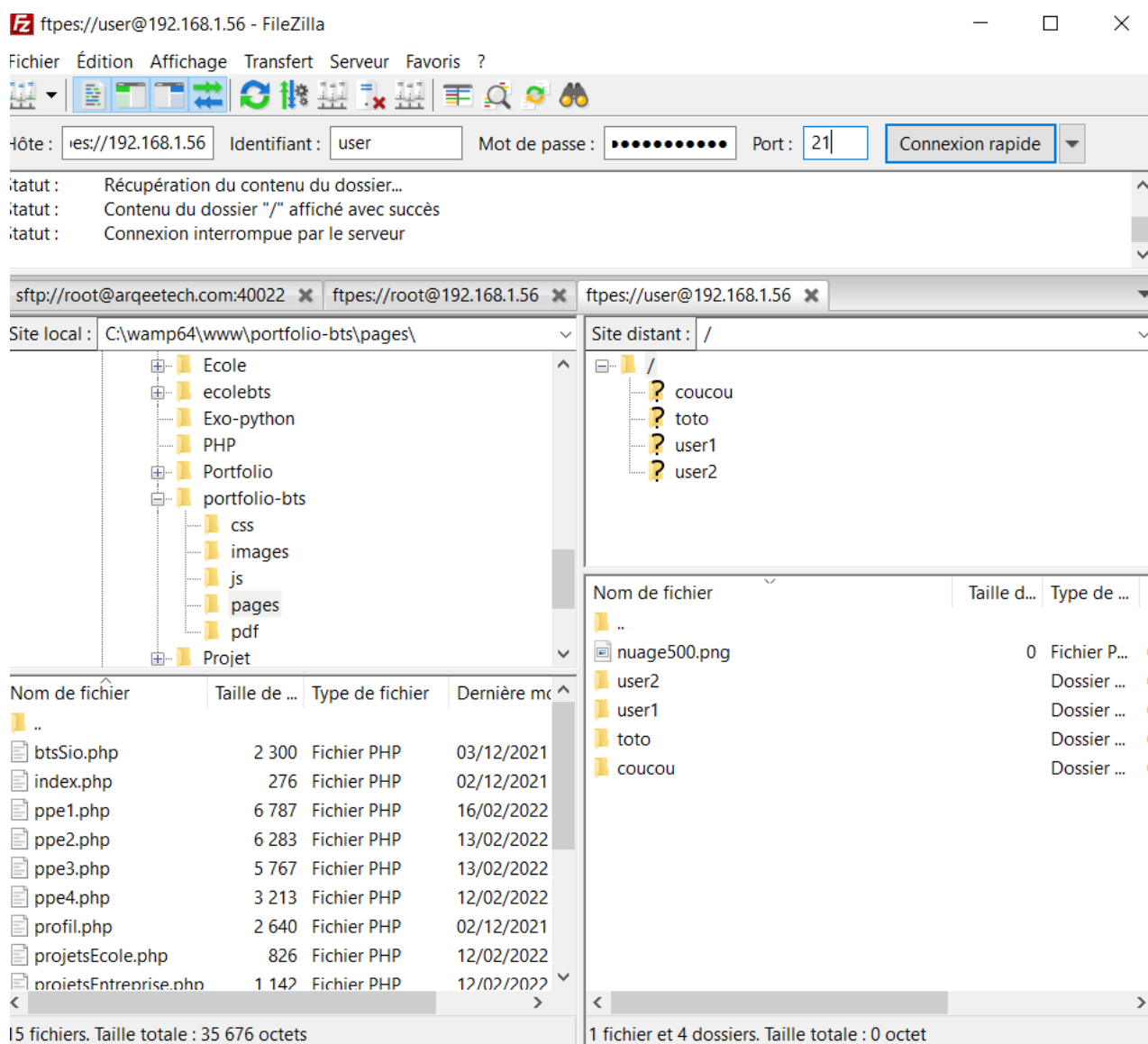
Une fois la connexion lancée, une demande de vérification du certificat apparaît :



Une fois validé, la connexion se termine, et nous pouvons créer des dossiers et importer des fichiers.

Le site local correspond à l'arborescence des documents contenus sur le disque de l'ordinateur, tandis que le site distant correspond à l'arborescence des documents du serveur FTP.

L'utilisateur étant restreint au dossier FTP, il n'en voit que le contenu. Le nom n'apparaît pas, on ne voit que le "/" qui signifie qu'il est à la racine du dossier.



Le serveur et le client FTP sont désormais en place et prêt à l'emploi.