

## **BTS SERVICES INFORMATIQUES AUX ORGANISATIONS SESSION 2025**

### **Épreuve E5 - Administration des systèmes et des réseaux (Option SISR)**

#### **Projet 2 : Mise en place d'une infrastructure réseau avancée**

##### **Contexte :**

Nous souhaitons renforcer la sécurité et la résilience de l'infrastructure réseau de l'étude Moreau & Associés en intégrant une solution de redondance Active Directory et DNS, un VPN pour les accès distants, un système de détection/prévention d'intrusions (IDS/IPS), un serveur de messagerie ainsi que des stratégies de groupe avancées pour la protection des postes clients.

##### **Objectifs du projet :**

- Assurer la haute disponibilité des services grâce à un contrôleur de domaine secondaire en cas de panne du principal.
- Proposer une solution VPN sécurisée pour permettre aux employés d'accéder aux ressources à distance.
- Surveiller les intrusions via un système IPS avec Snort et une analyse Complémentaire avec Wireshark.
- Mettre en place un serveur de sauvegarde performant
- Proposer un mail dédié a l'étude notarial

---

#### **L'infrastructure ainsi que les outils déployés**

##### **Redondance Active Directory et DNS**

- Mise en place d'un contrôleur de domaine principal sous Windows Server 2019.
- Déploiement d'un serveur secondaire assurant la redondance d'Active Directory et du DNS.
- Réplication automatique des objets Active Directory et des enregistrements DNS pour garantir une continuité de service en cas de panne.

##### **VPN sécurisé avec OpenVPN**

- Mise en place de OpenVPN pour sécuriser les connexions distantes des collaborateurs.
- Authentification via les comptes Active Directory pour garantir un accès sécurisé aux ressources internes.
- Chiffrement des communications pour empêcher toute interception des données.

## Surveillance réseau avec Snort, et Wireshark

- **Snort** : Déploiement d'un système de détection d'intrusion (IDS) et de prévention (IPS) pour analyser le trafic réseau et bloquer les menaces en temps réel.
- **Wireshark** : Utilisé pour l'analyse détaillée du trafic et le diagnostic des incidents réseau.

## Stockage et partage de fichiers avec un NAS

- Mise en place d'un serveur de stockage NAS pour centraliser les données.
- Configuration des droits d'accès basés sur les groupes Active Directory.
- Sauvegarde automatique des fichiers critiques avec une solution de réplication en réseau.

## Messagerie d'entreprise avec Zimbra

- Mise en place de **Zimbra** comme solution de messagerie collaborative.
- Création d'un **webmail interne accessible via un navigateur**, adapté aux besoins des collaborateurs.
- Configuration des certificats et du chiffrement SSL/TLS pour garantir la confidentialité des échanges.

---

## ***Table des matières***

### 1. Infrastructure réseau

#### 1.1. Redondance Active Directory et DNS

- 1.1.1. Serveur principal sous Windows Server 2019
- 1.1.2. Serveur de secours pour la continuité de service

#### 1.2. VPN sécurisé avec OpenVPN

- 1.3.1. Authentification et gestion des accès distants
- 1.3.2. Chiffrement et sécurité des connexions

### 2. Surveillance et sécurité du réseau

#### 2.1. Système de détection d'intrusion (IDS/IPS)

- 2.1.1. Déploiement de Snort pour l'analyse du trafic

#### 2.2. Analyse du trafic avec Wireshark

- 2.2.1. Surveillance des échanges réseau
- 2.2.2. Détection et diagnostic des anomalies

### 3. Stockage et partage des données

#### 3.1. Infrastructure NAS

- 3.1.1 Configuration nas via TrueNAS

- 3.1.2. Sauvegarde automatique et réplication des fichiers via bucket AWS

#### 4. Messagerie d'entreprise

- 4.1. Déploiement d'un webmail interne avec Zimbra
- 4.2. Intégration aux comptes Active Directory
- 4.3. Sécurisation des échanges et accès externes

### **Conclusion**

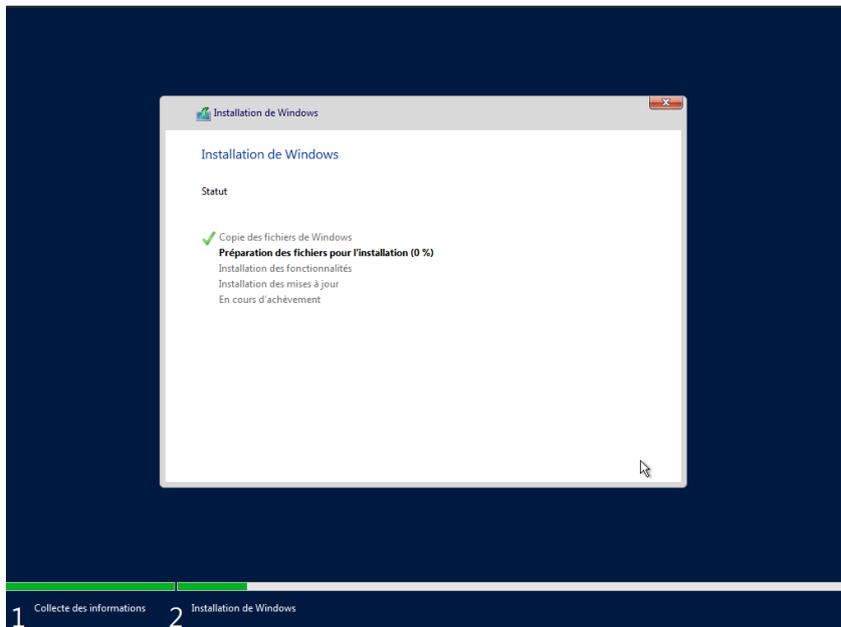
Cette infrastructure offre une solution robuste et sécurisée pour TechNovalis. La redondance de l'Active Directory assure une continuité de service en cas de panne d'un serveur. Le VPN permet un accès distant sécurisé pour les employés, tandis que l'IPS et l'analyse réseau renforcent la détection des menaces. Enfin, la messagerie interne Zimbra et l'application des GPO garantissent une gestion optimisée des postes utilisateurs.

Avec ces solutions, TechNovalis dispose d'une infrastructure résiliente et adaptée aux besoins actuels en matière de sécurité et de connectivité.

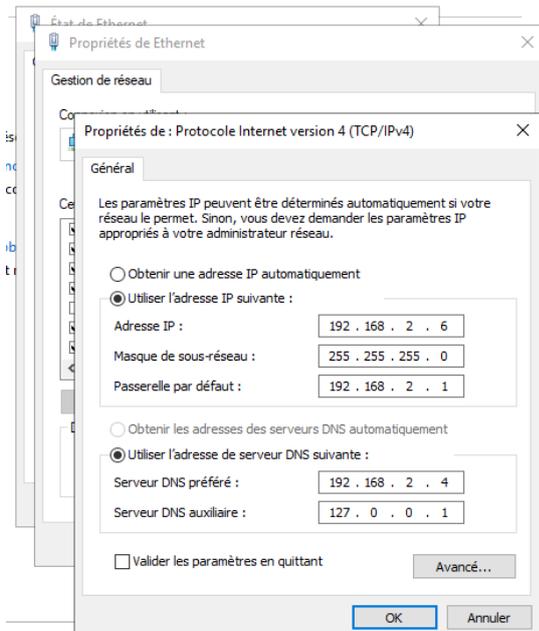
## 1.1. Redondance Active Directory et DNS

Pour mettre en place la redondance, nous commençons par déployer une seconde machine virtuelle sous Windows Server afin d'assurer la continuité de service.

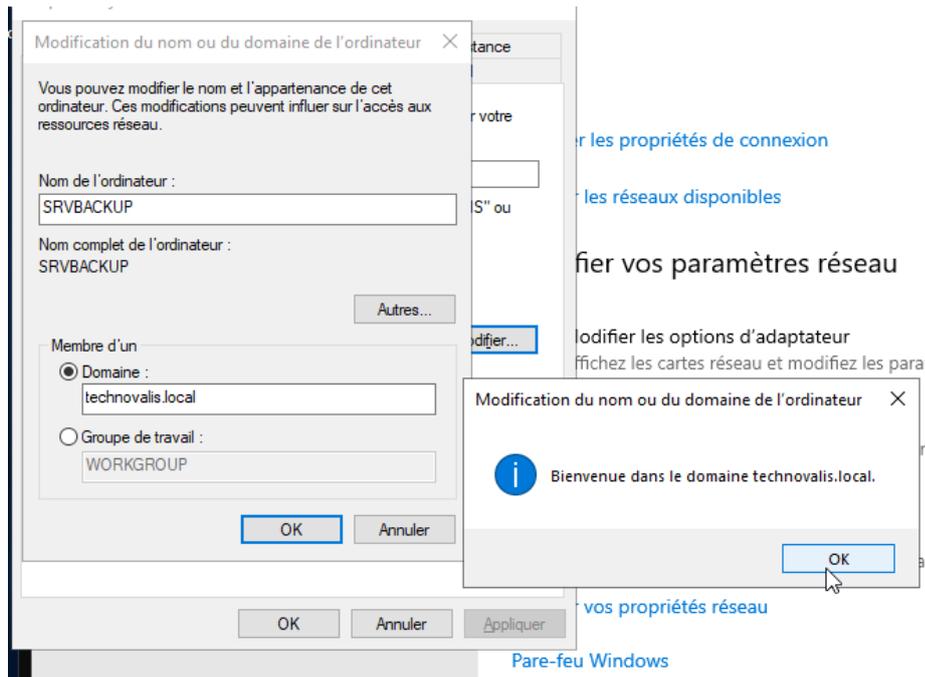
Nous installons Windows Server sur une nouvelle machine virtuelle afin d'assurer la redondance de notre infrastructure. Cette étape consiste à copier les fichiers nécessaires et préparer l'installation avant d'ajouter les rôles et fonctionnalités requis pour l'intégration du serveur dans notre domaine existant.



Nous configurons l'adresse IP statique de notre serveur de secours afin d'assurer sa disponibilité sur le réseau. L'adresse 192.168.2.6 est attribuée à la machine, avec comme DNS principal le contrôleur de domaine principal (192.168.2.4).



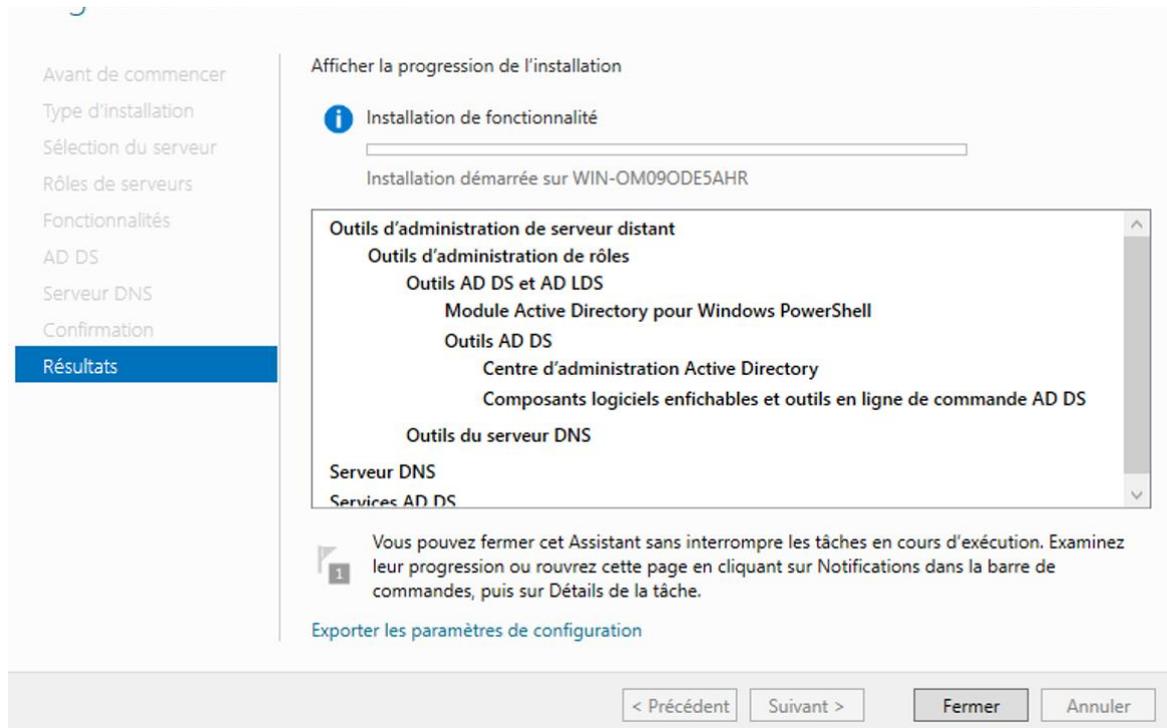
Nous intégrons le serveur de secours **SRVBACKUP** au domaine **technovalis.local**.



On redémarre la VM

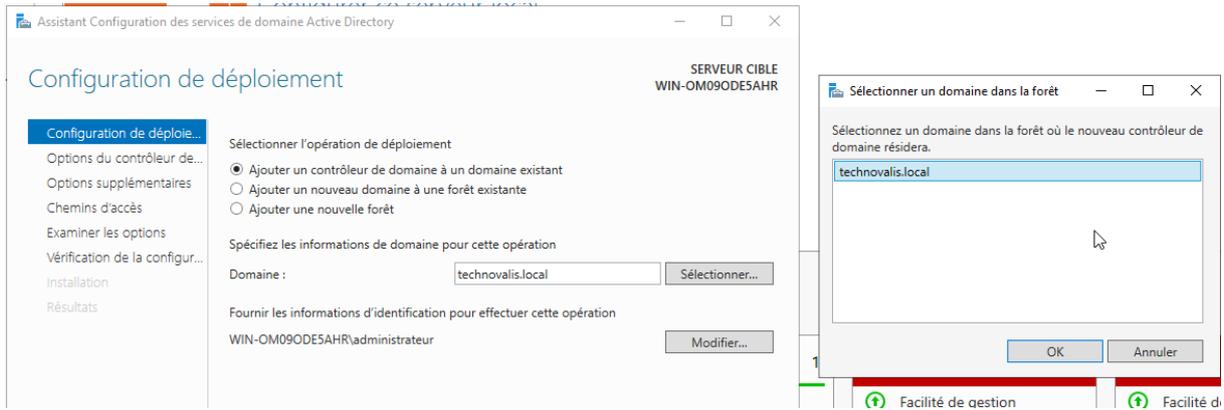


Nous installons les rôles AD DS et DNS sur le serveur backup pour assurer la redondance du domaine.

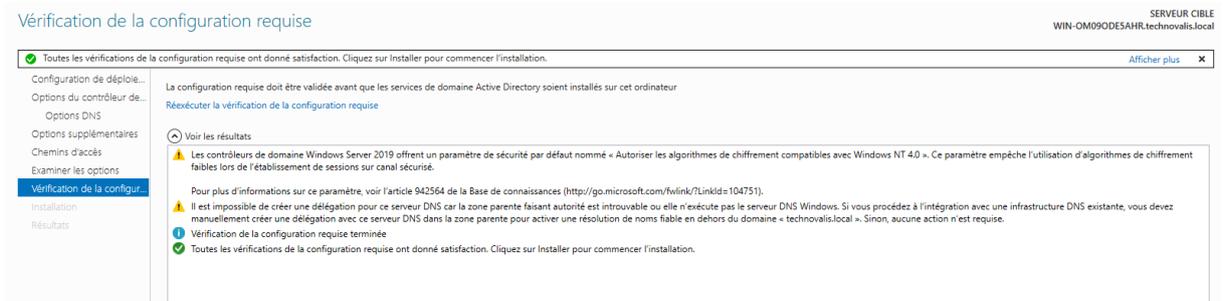


Nous configurons notre nouveau serveur en tant que contrôleur de domaine supplémentaire dans la forêt existante du domaine principal technovalis.local. Cette étape permet d'assurer la redondance d'Active

Directory et du DNS, garantissant ainsi une continuité de service en cas de défaillance du serveur principal.



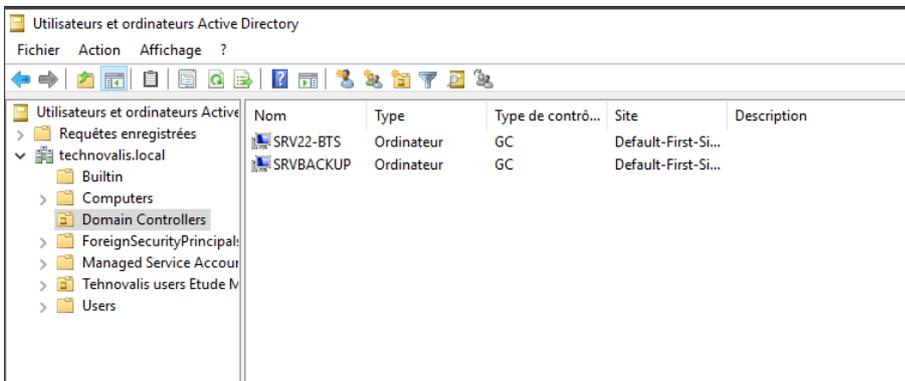
Nous avons effectué la vérification de la configuration requise avant l'installation d'Active Directory sur notre serveur secondaire. Toutes les vérifications ont été validées avec succès, nous pouvons maintenant lancer l'installation sans problème.



Nous pouvons à présent redémarrer le second serveur.



Le serveur SRVBACKUP a été intégré en tant que contrôleur de domaine secondaire dans Active Directory, assurant la redondance et la continuité des services d'authentification en cas de défaillance du contrôleur principal SRV22-BTS.



Nous avons configuré le serveur DNS sur SRVBACKUP, où nous retrouvons les enregistrements des hôtes et des services du domaine technovalis.local. Les enregistrements SOA (Start of Authority) et NS (Name Server) confirment que ce serveur est bien un serveur DNS secondaire, assurant la redondance avec SRV22-BTS.

	Nom	Type	Données	Horodateur
	_msdcs			
	_sites			
	_tcp			
	_udp			
	DomainDnsZones			
	ForestDnsZones			
	(identique au dossier parent)	Source de nom (SOA)	[535], srvbackup.technova...	statique
	(identique au dossier parent)	Serveur de noms (NS)	srvbackup.technovalis.local.	statique
	(identique au dossier parent)	Serveur de noms (NS)	srv22-bts.technovalis.local.	statique
	(identique au dossier parent)	Hôte (A)	192.168.2.4	13/03/2025 23:00:00
	(identique au dossier parent)	Hôte (A)	192.168.2.6	14/03/2025 08:00:00
	Collaborateur1	Hôte (A)	192.168.2.50	09/03/2025 20:00:00
	Collaborateur2	Hôte (A)	192.168.2.51	27/11/2024 09:00:00
	DESKTOP-C2GOORM	Hôte (A)	192.168.2.51	21/11/2024 01:00:00
	PFSENSE	Alias (CNAME)	routeur.technovalis.local.	statique
	routeur	Hôte (A)	192.168.2.1	statique
	SERVEUR	Hôte (A)	192.168.2.4	statique
	Srv	Alias (CNAME)	srv22-bts.technovalis.local.	statique
	srv22-bts	Hôte (A)	192.168.2.4	statique
	SRV_BACKUP	Hôte (A)	192.168.2.6	14/03/2025 06:00:00
	srvbackup	Hôte (A)	192.168.2.6	statique

Nous avons effectué une résolution de nom avec NSLOOKUP en interrogeant SRVBACKUP (192.168.2.6). Celui-ci renvoie bien les adresses IP des deux contrôleurs de domaine (SRV22-BTS et SRVBACKUP), confirmant ainsi que la redondance DNS est opérationnelle.

```
C:\Users\Administrateur.TECHNOVALIS>nslookup technovalis.local 192.168.2.6
Serveur : SRVBACKUP.technovalis.local
Address: 192.168.2.6

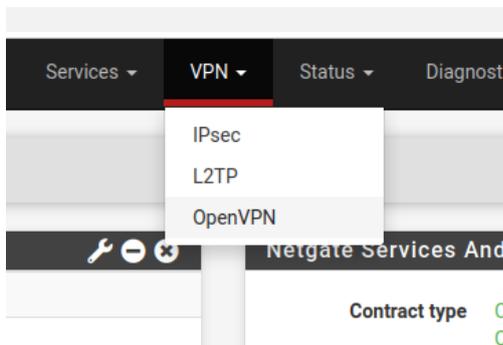
Nom : technovalis.local
Addresses: 192.168.2.4
          192.168.2.6
```

Nous allons ensuite passer à la configuration d'openVPN pour les clients de l'étude

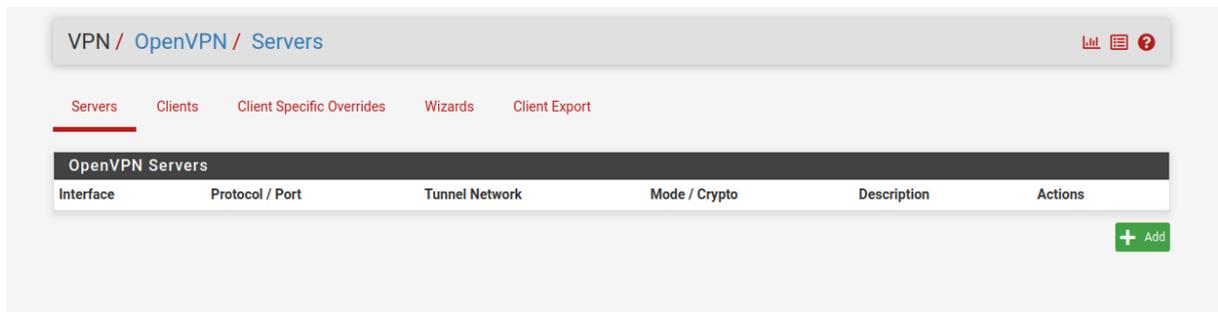
## 1.2. VPN sécurisé avec OpenVPN

Nous avons installé le package `openvpn-client-export` sur pfSense. Ce package nous permet d'exporter facilement des configurations OpenVPN préconfigurées pour les clients.

Installed Packages				
Name	Category	Version	Description	Actions
✓ openvpn-client-export	security	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.	  
Package Dependencies:				
<a href="#">openvpn-client-export-2.6.7</a> <a href="#">openvpn-2.6.8_1</a> <a href="#">zip-3.0_1</a> <a href="#">7-zip-23.01</a>				



Nous accédons à l'interface de configuration d'OpenVPN sur pfSense via **VPN > OpenVPN > Servers**. À cette étape, aucun serveur VPN n'est encore configuré.



Nous configurons le serveur OpenVPN en mode Remote Access (SSL/TLS), permettant aux clients de se connecter de manière sécurisée. Nous définissons l'interface d'écoute sur WAN et utilisons le port standard 1194/UDP. Une clé TLS est activée pour renforcer la sécurité du tunnel VPN

Servers	Clients	Client Specific Overrides	Wizards	Client Export
<b>General Information</b>				
<b>Description</b>		OpenVPN Remote Access A description of this VPN for administrative reference.		
<b>Disabled</b>		<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.		
<b>Unique VPN ID</b>		Server 1 (ovpn1)		
<b>Mode Configuration</b>				
<b>Server mode</b>		Remote Access (SSL/TLS)		
<b>Device mode</b>		tun - Layer 3 Tunnel Mode <small>*tun* mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. *tap* mode is capable of carrying 802.3 (OSI Layer 2).</small>		
<b>Endpoint Configuration</b>				
<b>Protocol</b>		UDP on IPv4 only		
<b>Interface</b>		WAN <small>The interface or Virtual IP address where OpenVPN will receive client connections.</small>		
<b>Local port</b>		1194 <small>The port used by OpenVPN to receive client connections.</small>		
<b>Cryptographic Settings</b>				
<b>TLS Configuration</b>		<input checked="" type="checkbox"/> Use a TLS Key <small>A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.</small>		
<b>TLS Key</b>		<pre># # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- edc519633fb623441bbaf23badf3b6ec</pre> <p>Paste the TLS key here. This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.</p>		

Nous mettons en place les paramètres de sécurisation du tunnel OpenVPN en activant l'authentification TLS et en utilisant un certificat serveur OpenVPN-CA. L'algorithme de chiffrement choisi est AES-256-GCM, et nous appliquons un échange de clés Diffie-Hellman en 2048 bits pour garantir un niveau de sécurité optimal.

<b>TLS Key Usage Mode</b>	TLS Authentication	<small>In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.</small>
<b>TLS keydir direction</b>	Use default direction	<small>The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.</small>
<b>Peer Certificate Authority</b>	OpenVPN-CA	
<b>Peer Certificate Revocation list</b>	No Certificate Revocation Lists defined. One may be created here: <a href="#">System &gt; Cert. Manager</a>	
<b>OCSP Check</b>	<input type="checkbox"/> Check client certificates with OCSP	
<b>Server certificate</b>	OpenVPN-Server (Server: Yes, CA: OpenVPN-CA, In Use)	<small>Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.</small>
<b>DH Parameter Length</b>	2048 bit	<small>Diffie-Hellman (DH) parameter set used for key exchange.</small>
<b>ECDH Curve</b>	Use Default	<small>The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.</small>
<b>Data Encryption Algorithms</b>	<ul style="list-style-type: none"> <li>AES-128-CBC (128 bit key, 128 bit block)</li> <li>AES-128-CFB (128 bit key, 128 bit block)</li> <li>AES-128-CFB1 (128 bit key, 128 bit block)</li> <li>AES-128-CFB8 (128 bit key, 128 bit block)</li> <li>AES-128-GCM (128 bit key, 128 bit block)</li> <li>AES-128-OFB (128 bit key, 128 bit block)</li> <li>AES-192-CBC (192 bit key, 128 bit block)</li> <li>AES-192-CFB (192 bit key, 128 bit block)</li> <li>AES-192-CFB1 (192 bit key, 128 bit block)</li> <li>AES-192-CFB8 (192 bit key, 128 bit block)</li> </ul>	<ul style="list-style-type: none"> <li>CHACHA20-POLY1305</li> <li>AES-256-GCM</li> </ul>
<b>Fallback Data Encryption Algorithm</b>	AES-256-CBC (256 bit key, 128 bit block)	<small>The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.</small>
<b>Auth digest algorithm</b>	SHA256 (256-bit)	<small>The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.</small>

Nous configurons le réseau du tunnel VPN en attribuant une plage d'adresses IP privée 10.0.2.0/24 pour la communication entre le serveur et les clients OpenVPN. Nous activons également l'option de redirection de la passerelle IPv4, afin que tout le trafic des clients passe par le tunnel sécurisé. Le nombre maximal de connexions simultanées est défini à 10.

Tunnel Settings	
<b>IPv4 Tunnel Network</b>	<input type="text" value="10.0.2.0/24"/> This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.  A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.
<b>IPv6 Tunnel Network</b>	<input type="text"/> This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
<b>Redirect IPv4 Gateway</b>	<input checked="" type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
<b>Redirect IPv6 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
<b>IPv6 Local network(s)</b>	<input type="text"/> IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
<b>Concurrent connections</b>	<input type="text" value="10"/> Specify the maximum number of clients allowed to concurrently connect to this server.
<b>Allow Compression</b>	<input type="text" value="Refuse any non-stub compression (Most secure)"/> Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.  Asymmetric compression allows an easier transition when connecting with older peers.
<b>Type-of-Service</b>	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
<b>Inter-client communication</b>	<input checked="" type="checkbox"/> Allow communication between clients connected to this server
<b>Duplicate Connection</b>	<input type="checkbox"/> Allow multiple concurrent connections from the same user When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.  Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Nous configurons les paramètres avancés des clients OpenVPN pour assurer une connectivité fluide et sécurisée. Nous définissons la topologie du VPN en mode subnet, attribuant une adresse IP distincte à chaque client connecté. Pour améliorer la stabilité, nous utilisons le mode de ping keepalive avec un intervalle de 10 secondes et un timeout de 60 secondes afin de détecter les connexions inactives.

Nous configurons également le serveur DNS interne (192.168.2.4) pour que les clients du VPN puissent résoudre les noms internes du domaine.

**Dynamic IP**  Allow connected clients to retain their connections if their IP address changes.

**Topology**    
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

---

**Ping settings**

**Inactive**    
Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

**Ping method**    
keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:  
ping = interval  
ping-restart = timeout\*2  
push ping = interval  
push ping-restart = timeout

**Interval**

**Timeout**

---

**Advanced Client Settings**

**DNS Default Domain**  Provide a default domain name to clients

**DNS Server enable**  Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

**DNS Server 1**

**DNS Server 2**

**DNS Server 3**

**DNS Server 4**

**Block Outside DNS**  Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers.   
Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

**Force DNS cache update**  Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation.   
This is known to kick Windows into recognizing pushed DNS servers.

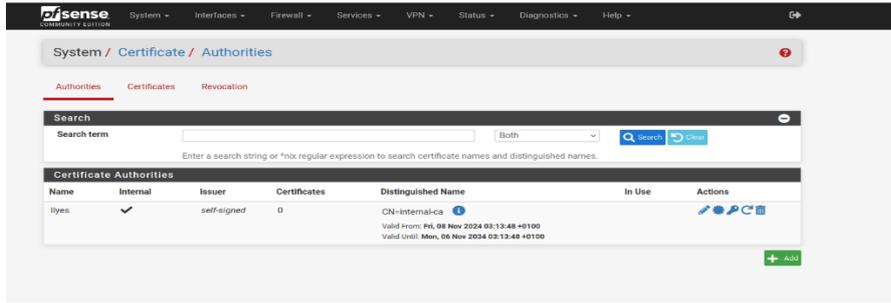
**NTP Server enable**  Provide an NTP server list to clients

**NetBIOS enable**  Enable NetBIOS over TCP/IP   
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

On sauvegarde, et le serveur vpn est configuré.

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.0.2.0/24	<b>Mode:</b> Remote Access ( SSL/TLS ) <b>Data Ciphers:</b> CHACHA20-POLY1305, AES-256-GCM, AES-256-CBC <b>Digest:</b> SHA256 <b>D-H Params:</b> 2048 bits	OpenVPN Remote Access	  

Nous créons une Autorité de Certification OpenVPN qui servira à signer les certificats nécessaires à l'authentification des clients et du serveur.



**Create / Edit CA**

**Descriptive name**: OpenVPN-CA  
The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, '.

**Method**: Import an existing Certificate Authority

**Trust Store**:  Add this Certificate Authority to the Operating System Trust Store  
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

**Randomize Serial**:  Use random serial numbers when signing certificates  
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

**Existing Certificate Authority**

**Certificate data**:  

```
-----BEGIN CERTIFICATE-----
MIIDYTCCARggAwIBAgIIFYG4gsjVB1YwDQYJKoZIhvcNAQELBQAwSD
EPMA0GA1UE
AxMhGVI1BOLUNBMQswCQYDVQQGEwJGUjESMBAGA1UECBM3T2NjaXRhbm
11MRQwEgYD

```

Paste a certificate in X.509 PEM format here.

**Certificate Private Key (optional)**:  

```
-----BEGIN PRIVATE KEY-----
MIIEVQIBADANBgkqhkiG9w0BAQEFAASCCKCngGSjAgEAAoIBAQC9p7
X/i0ph/Hh0
1wxTL1PH46IgneGzeYzYdPA2X4QLJ1uqGRq+tcq1+pB8093uK/y603
FjU+t2PaQP

```

Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

**Next Certificate Serial**: 3  
Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is ignored when Randomize Serial is checked.

OpenVPN-CA	✓	self-signed	2	ST=Occitanie, L=Montpellier, CN=VPN-CA, C=FR		
				Valid From: Sun, 02 Feb 2025 18:47:04 +0100		
				Valid Until: Wed, 31 Jan 2035 18:47:04 +0100		

Notre Autorité de Certification OpenVPN a été générée et auto-signée. Elle est valide jusqu'en 2035 et servira à authentifier les connexions VPN en signant les certificats des serveurs et des clients

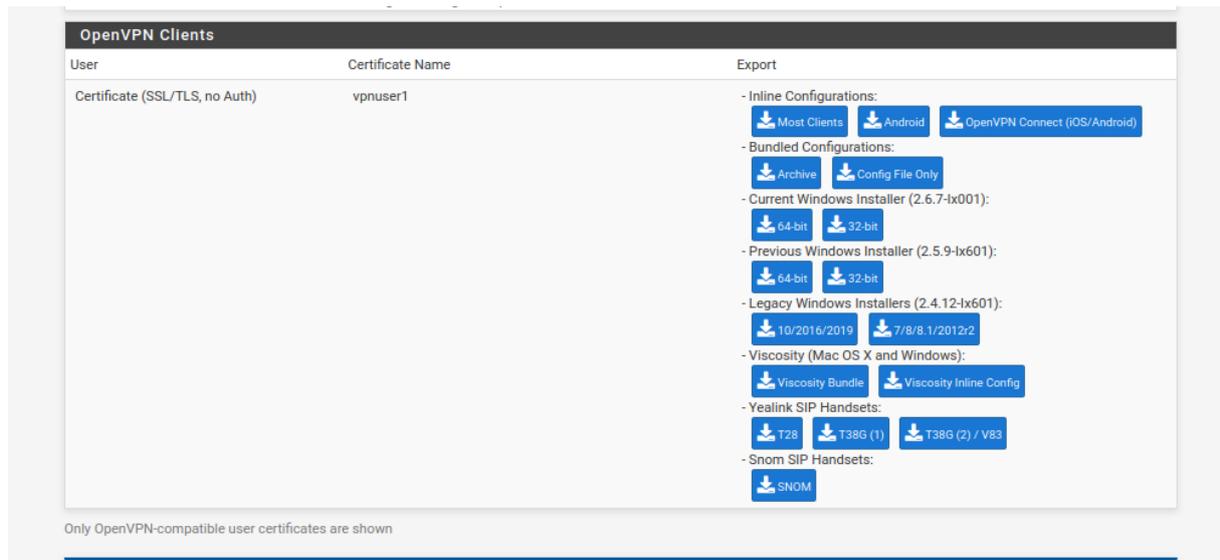
Nous avons généré un certificat serveur OpenVPN, signé par notre Autorité de Certification.



Nous avons généré un certificat utilisateur pour vpnuser1, signé par notre Autorité de Certification



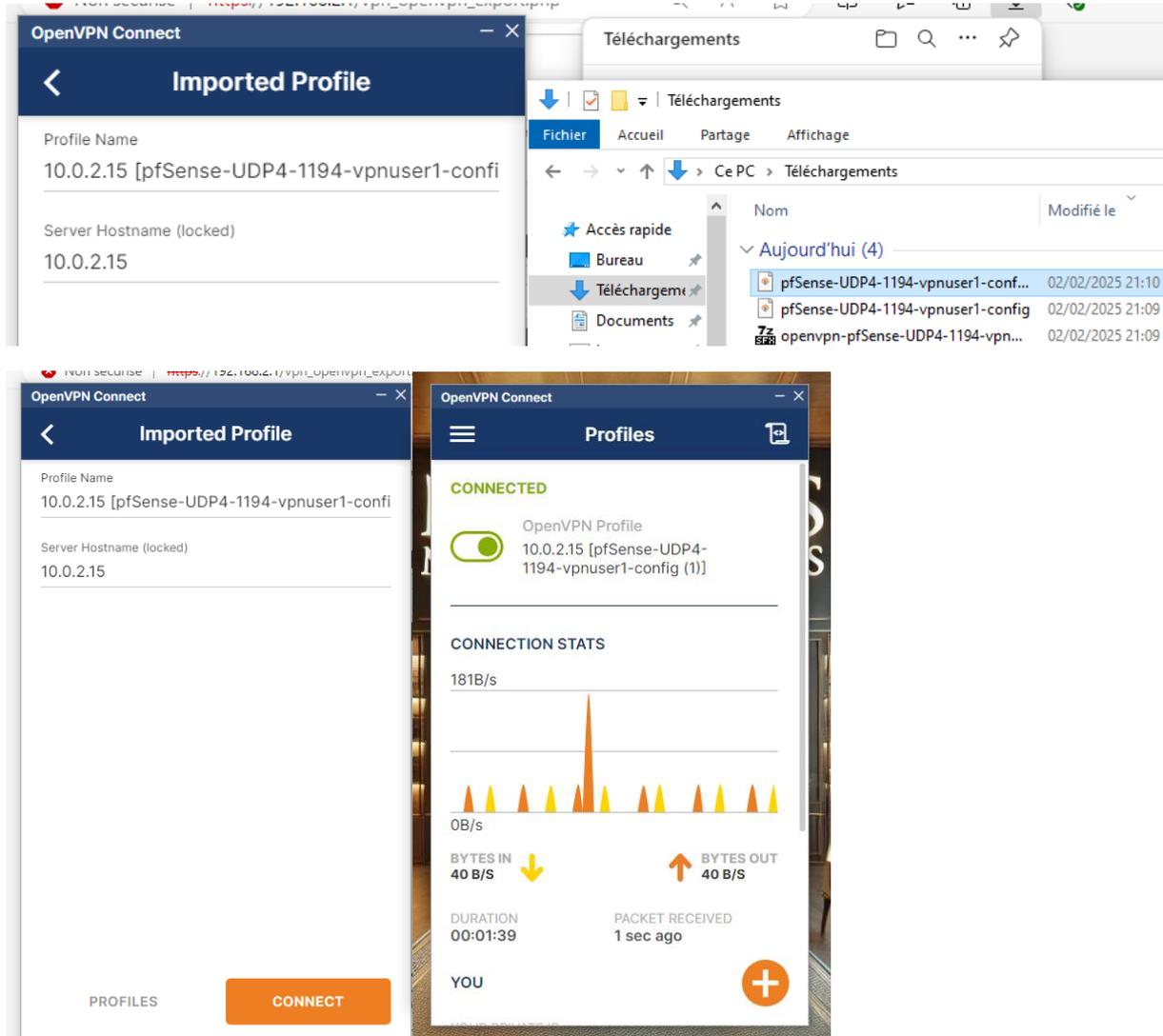
Nous allons exporter le fichier de configuration OpenVPN (.ovpn) pour l'utilisateur vpnuser1. Ce fichier contient toutes les informations nécessaires pour établir une connexion sécurisée au serveur VPN.



On installe ensuite openVPN sur un poste client pour y intégrer le fichier de configuration précédemment téléchargé.



### On importe le profile vpnuser1



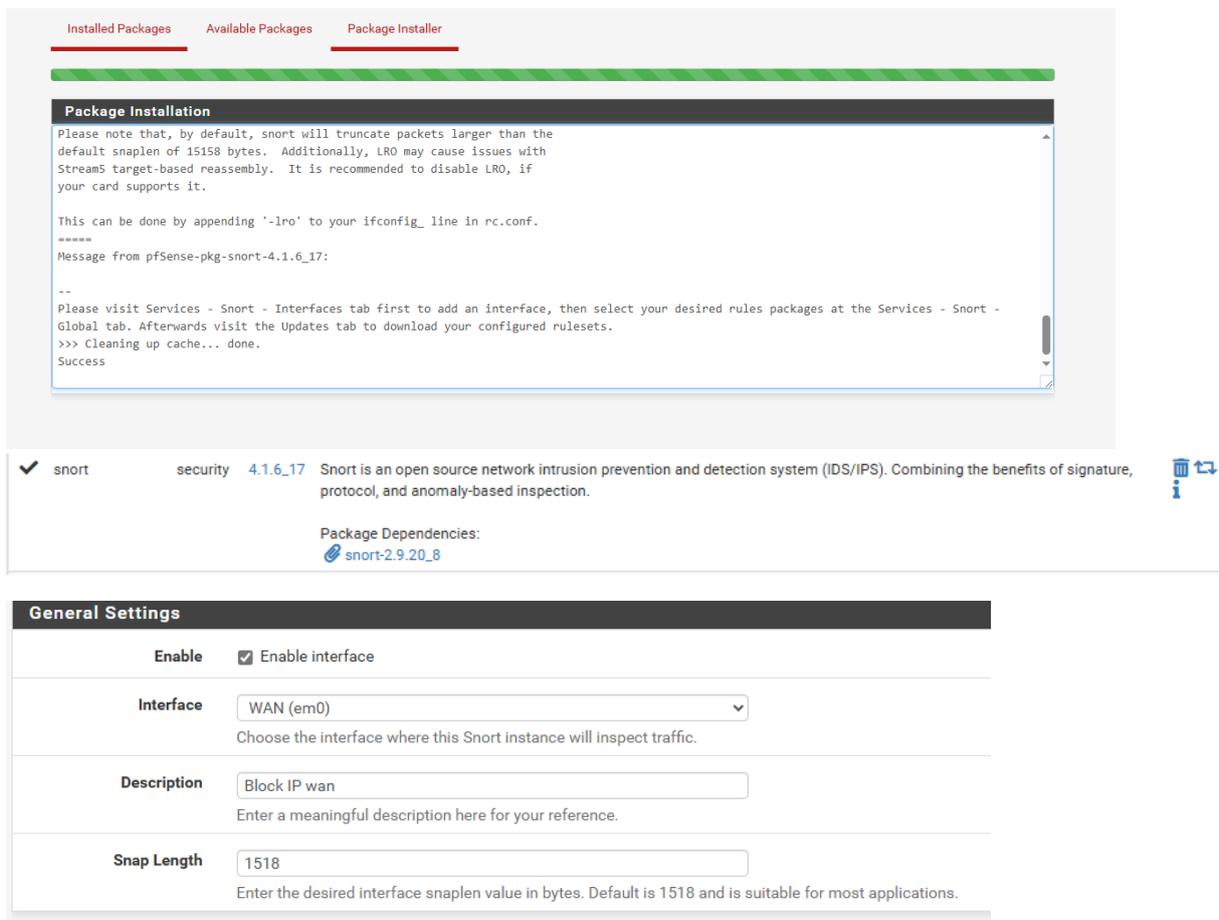
Nous avons importé le fichier de configuration OpenVPN sur le client. Une fois le profil vpnuser1 chargé dans OpenVPN Connect, nous avons initié la connexion au serveur VPN. L'état CONNECTED ainsi que les statistiques de trafic confirment que l'utilisateur est bien connecté et que la communication chiffrée est active.

## 2. Surveillance et sécurité du réseau

### 2.1. Système de détection d'intrusion (IDS/IPS)

#### - 2.1.1. Déploiement de Snort pour l'analyse du trafic

Nous avons installé Snort sur pfSense avec succès. Cette installation nous permet de mettre en place un système de détection et de prévention d'intrusion (IDS/IPS) afin d'analyser le trafic réseau et de détecter d'éventuelles menaces.



The screenshot displays the pfSense Package Installer interface. At the top, there are tabs for 'Installed Packages', 'Available Packages', and 'Package Installer'. The 'Package Installer' tab is active, showing a 'Package Installation' window with a terminal output. The terminal text reads:

```

Please note that, by default, snort will truncate packets larger than the
default snaplen of 15158 bytes.  Additionally, LRO may cause issues with
Stream5 target-based reassembly.  It is recommended to disable LRO, if
your card supports it.

This can be done by appending '-lro' to your ifconfig_ line in rc.conf.
*****
Message from pfSense-pkg-snort-4.1.6.17:

--
Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort -
Global tab. Afterwards visit the Updates tab to download your configured rulesets.
>>> Cleaning up cache... done.
Success
  
```

Below the terminal output, the package details for 'snort' are shown:

- ✓ snort security 4.1.6.17 Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
- Package Dependencies: snort-2.9.20\_8

The 'General Settings' section is also visible, showing the following configuration:

- Enable:**  Enable interface
- Interface:** WAN (em0) (Choose the interface where this Snort instance will inspect traffic.)
- Description:** Block IP wan (Enter a meaningful description here for your reference.)
- Snap Length:** 1518 (Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.)

Nous avons activé Snort sur l'interface WAN (em0) et configuré l'envoi d'alertes dans le journal système du pare-feu. Les paquets générant une alerte seront automatiquement capturés et stockés dans un fichier pour analyse.

<b>Enable</b>	<input checked="" type="checkbox"/> Enable interface
<b>Interface</b>	<input type="text" value="WAN (em0)"/> <small>Choose the interface where this Snort instance will inspect traffic.</small>
<b>Description</b>	<input type="text" value="Block IP wan"/> <small>Enter a meaningful description here for your reference.</small>
<b>Snap Length</b>	<input type="text" value="1518"/> <small>Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.</small>
<b>Alert Settings</b>	
<b>Send Alerts to System Log</b>	<input checked="" type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
<b>System Log Facility</b>	<input type="text" value="LOG_AUTH"/> <small>Select system log Facility to use for reporting. Default is LOG_AUTH.</small>
<b>System Log Priority</b>	<input type="text" value="LOG_ALERT"/> <small>Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.</small>
<b>Enable Packet Captures</b>	<input checked="" type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
<b>Packet Capture File Size</b>	<input type="text" value="128"/> <small>Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em046856 is rotated and a new file opened.</small>
<b>Enable Unified2 Logging</b>	<input type="checkbox"/> Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. <small>Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.</small>

Nous avons activé le mode **IPS en "Legacy Mode"**, permettant à **Snort** d'inspecter les paquets et de bloquer automatiquement les adresses IP malveillantes. Nous avons également activé la suppression des sessions associées aux IP bloquées pour une meilleure réactivité.

<b>Block Settings</b>	
<b>Block Offenders</b>	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
<b>IPS Mode</b>	<input type="text" value="Legacy Mode"/> <small>Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.</small> <small>Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.</small>
<b>Kill States</b>	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
<b>Which IP to Block</b>	<input type="text" value="BOTH"/> <small>Select which IP extracted from the packet you wish to block. Default is BOTH.</small>
<b>Detection Performance Settings</b>	
<b>Search Method</b>	<input type="text" value="AC-BNFA"/> <small>Choose a fast pattern matcher algorithm. Default is AC-BNFA.</small>
<b>Split ANY-ANY</b>	<input type="checkbox"/> Enable splitting of ANY-ANY port group. Default is Not Checked.
<b>Search Optimize</b>	<input type="checkbox"/> Enable search optimization. Default is Not Checked.
<b>Stream Inserts</b>	<input type="checkbox"/> Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.
<b>Checksum Check Disable</b>	<input type="checkbox"/> Disable checksum checking within Snort to improve performance. Default is Not Checked.

Nous avons mis à jour les règles de détection de Snort, incluant des signatures provenant de plusieurs sources telles que Snort Subscriber Ruleset, Emerging Threats Open Rules et Feodo Tracker Botnet C2 IP Rules. Ces mises à jour permettent d'améliorer la détection des menaces en temps réel et d'optimiser la protection du réseau.

Installed Rule Set MD5 Signature		
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	ef356004644a1f6df8a52573776ef0e4	Thursday, 13-Mar-25 23:01:02 CET
Snort GPLv2 Community Rules	b0c300c5610bb3793c46cdd7655916b5	Thursday, 13-Mar-25 23:01:02 CET
Emerging Threats Open Rules	4c24342a857178cd120dd16e009a6af0	Saturday, 15-Mar-25 23:00:10 CET
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Wednesday, 19-Feb-25 14:07:03 CET
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Wednesday, 19-Feb-25 14:07:03 CET
Feodo Tracker Botnet C2 IP Rules	b61779a7fa2b715e88b0cc4e4ab4d326	Saturday, 15-Mar-25 23:21:06 CET

Nous configurons la mise à jour automatique des règles de Snort afin de garantir une protection continue contre les menaces. L'intervalle est fixé à 24 heures avec une mise à jour programmée à 23h00.

**Rules Update Settings**

**Update Interval**    
Please select the interval for rule updates. Choosing NEVER disables auto-updates.

**Update Start Time**    
Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

**Hide Deprecated Rules Categories**  Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

**Disable SSL Peer Verification**  Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

Nous accédons à l'onglet des alertes de Snort pour surveiller les événements détectés sur l'interface WAN (em0). Nous activons l'actualisation automatique pour afficher en temps réel les alertes générées. Cette interface nous permettra de télécharger ou de purger les journaux d'alerte selon les besoins.

Services / Snort / Alerts ?

Snort Interfaces   Global Settings   Updates   **Alerts**   Blocked   Pass Lists   Suppress   IP Lists   SID Mgmt   Log Mgmt   Sync

---

**Alert Log View Settings**

**Interface to Inspect**   Auto-refresh view     
Choose interface.. Alert lines to display.

**Alert Log Actions**

---

**Alert Log View Filter** +

---

**0 Entries in Active Log**

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
------	--------	-----	-------	-------	-----------	-------	----------------	-------	---------	-------------

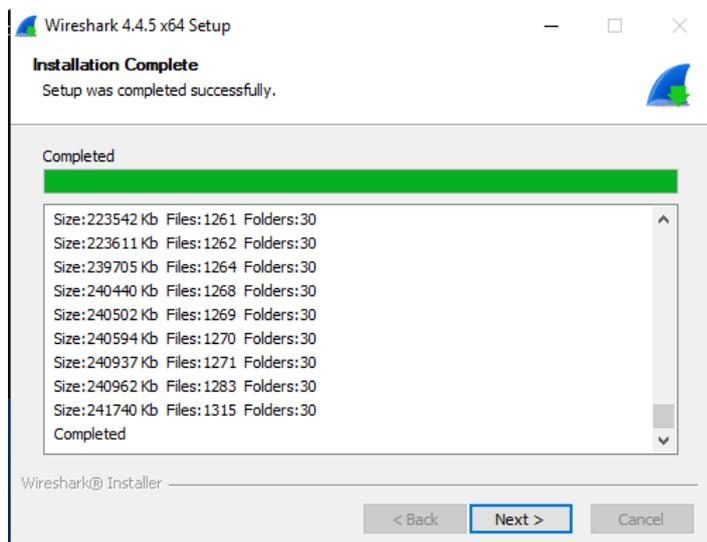
Snort est maintenant configuré avec toutes les règles nécessaires à la surveillance.

## 2.2. Analyse du trafic avec Wireshark

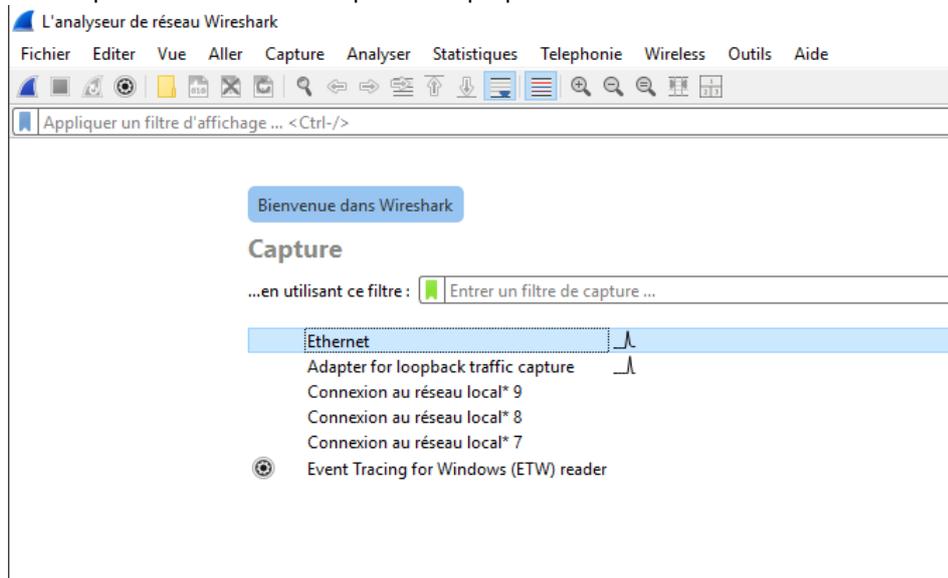
Nous téléchargeons la dernière version stable de Wireshark (4.4.5) pour l'installer sur notre machine d'analyse réseau.



Nous avons installé avec succès Wireshark 4.4.5 sur notre machine, prêt à capturer et analyser le trafic réseau.



Nous lançons Wireshark et accédons à l'interface principale, où nous pouvons sélectionner une interface réseau pour commencer la capture des paquets.



Nous lançons une capture de trafic sur l'interface Ethernet avec Wireshark. Nous observons les paquets échangés, incluant des requêtes DNS, des connexions TCP, ainsi qu'un message ICMP

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.50	192.168.2.4	DNS	78	Standard query 0xd9a6 A edge.microsoft.com
2	0.000192	192.168.2.4	192.168.2.1	DNS	101	Standard query 0x7aee A edge-domain.trafficmanager.net OPT
3	0.000417	192.168.2.50	192.168.2.4	DNS	78	Standard query 0x7d4 HTTPS edge.microsoft.com
4	0.000520	192.168.2.4	192.168.2.1	DNS	101	Standard query 0x4bfa HTTPS edge-domain.trafficmanager.net OPT
5	0.020439	192.168.2.1	192.168.2.4	DNS	198	Standard query response 0x7aee A edge-domain.trafficmanager.net CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNAME a...
6	0.020578	192.168.2.4	192.168.2.50	DNS	219	Standard query response 0xd9a6 A edge.microsoft.com CNAME edge-domain.trafficmanager.net CNAME edge-microsoft-com.ax-0...
7	0.038526	192.168.2.1	192.168.2.4	DNS	226	Standard query response 0x4bfa HTTPS edge-domain.trafficmanager.net CNAME edge-microsoft-com.ax-0002.ax-msedge.net CNA...
8	0.038732	192.168.2.4	192.168.2.1	DNS	92	Standard query 0xdb3c HTTPS ax-0002.ax-msedge.net OPT
9	0.039171	192.168.2.1	192.168.2.4	DNS	152	Standard query response 0xdb3c HTTPS ax-0002.ax-msedge.net SOA ns1.ax-msedge.net OPT
10	0.039249	192.168.2.4	192.168.2.50	DNS	187	Standard query response 0xf7d4 HTTPS edge.microsoft.com CNAME edge-domain.trafficmanager.net CNAME edge-microsoft-com...
11	0.039450	192.168.2.50	192.168.2.4	ICMP	215	Destination unreachable (Port unreachable)
12	2.242052	192.168.2.50	192.168.2.4	TCP	60	50714 → 135 [FIN, ACK] Seq=1 Ack=1 Win=8211 Len=0
13	2.242087	192.168.2.4	192.168.2.50	TCP	54	135 → 50714 [ACK] Seq=1 Ack=2 Win=8211 Len=0
14	2.242163	192.168.2.4	192.168.2.50	TCP	54	135 → 50714 [FIN, ACK] Seq=1 Ack=2 Win=8211 Len=0
15	2.242188	192.168.2.50	192.168.2.4	TCP	60	50715 → 49667 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
16	2.242200	192.168.2.4	192.168.2.50	TCP	54	49667 → 50715 [ACK] Seq=1 Ack=2 Win=8209 Len=0
17	2.242241	192.168.2.4	192.168.2.50	TCP	54	49667 → 50715 [FIN, ACK] Seq=1 Ack=2 Win=8209 Len=0
18	2.242370	192.168.2.50	192.168.2.4	TCP	60	50714 → 135 [ACK] Seq=2 Ack=2 Win=8211 Len=0
19	2.242539	192.168.2.50	192.168.2.4	TCP	60	50715 → 49667 [ACK] Seq=2 Ack=2 Win=1024 Len=0

```

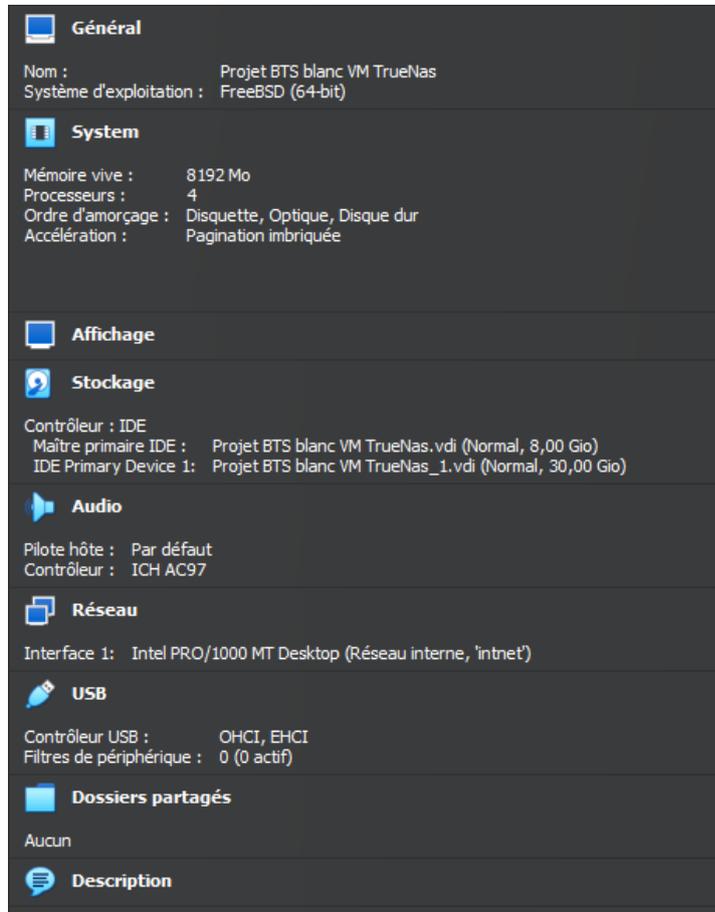
> Frame 11: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{1AD...}
> Ethernet II, Src: PCSysntec_3a:5b:18 (08:00:27:3a:5b:18), Dst: PCSysntec_21:bd:c1 (08:00:2...
> Internet Protocol Version 4, Src: 192.168.2.50, Dst: 192.168.2.4
> User Datagram Protocol, Src Port: 65341, Dst Port: 53
> Domain Name System (query)
    
```

Nous avons capturé et analysé le trafic réseau en temps réel avec Wireshark, cet outil permet d'identifier d'éventuels problèmes de communication et d'analyser les flux réseau en détail.

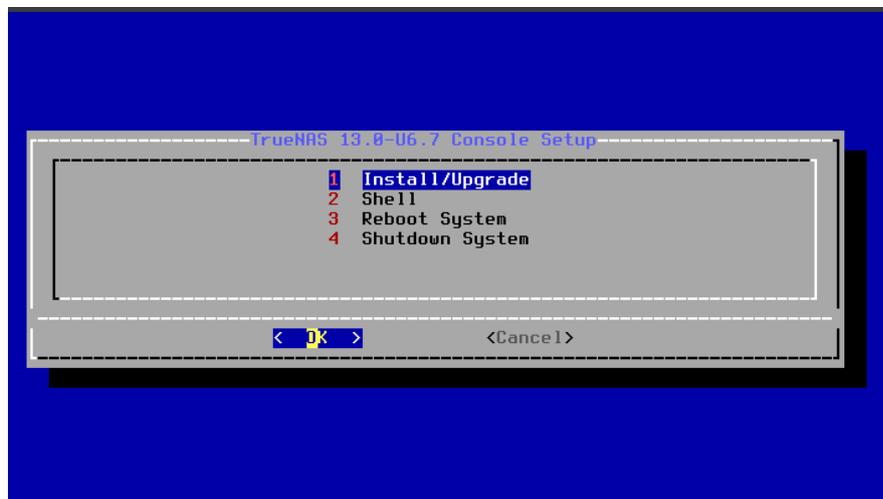
### 3.1. Infrastructure NAS

#### - 4.1.1 Configuration nas via TrueNAS

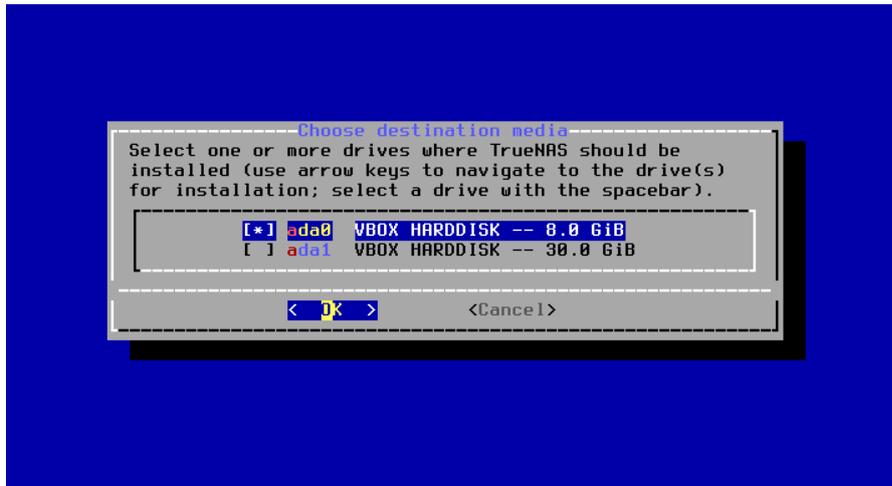
Nous commençons tout d'abord par monter une vm NAS en utilisant pour ce faire TrueNAS



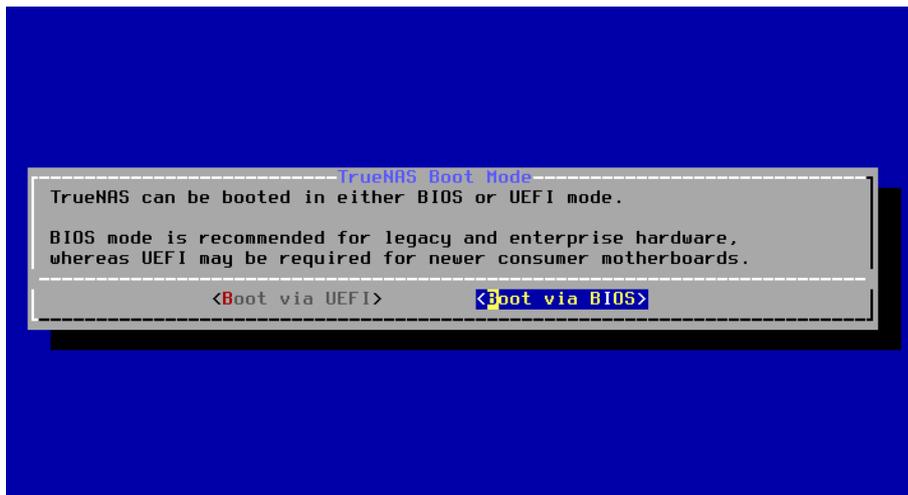
Nous avons démarré l'ISO de TrueNAS sur notre machine virtuelle. L'écran d'installation s'affiche et on sélectionne "Install/Upgrade".



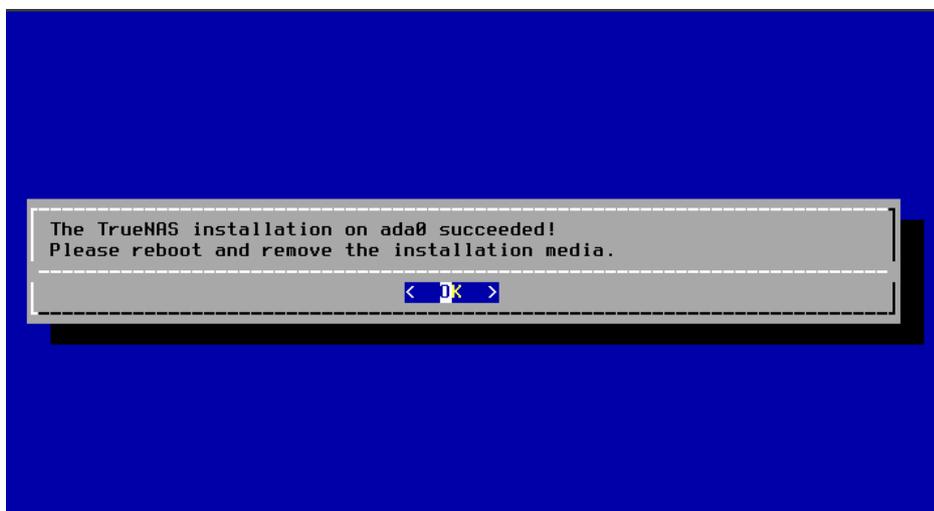
Nous sélectionnons le disque sur lequel TrueNAS sera installé. Nous avons choisi le disque ada0 (8 GiB) afin de réserver le second disque ada1 (30 GiB) pour le stockage des données.



Nous avons sélectionné le mode de démarrage de TrueNAS. Nous avons choisi Boot via BIOS, ce qui est recommandé pour les infrastructures d'entreprise et les environnements legacy. L'option UEFI aurait été préférable pour un matériel plus récent.



L'installation de **TrueNAS** s'est terminée avec succès. On redémarre la VM et on enlève l'ISO d'installation.



TrueNAS est bien installé et nous avons accès au menu de configuration. L'interface web est disponible à l'adresse 192.168.2.63 fournit grâce au DHCP.

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

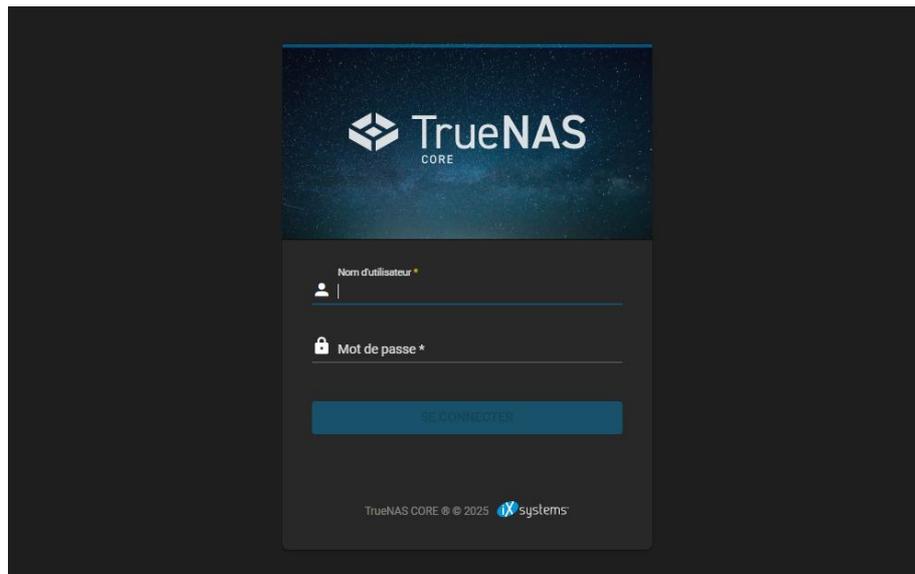
Console setup
-----

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

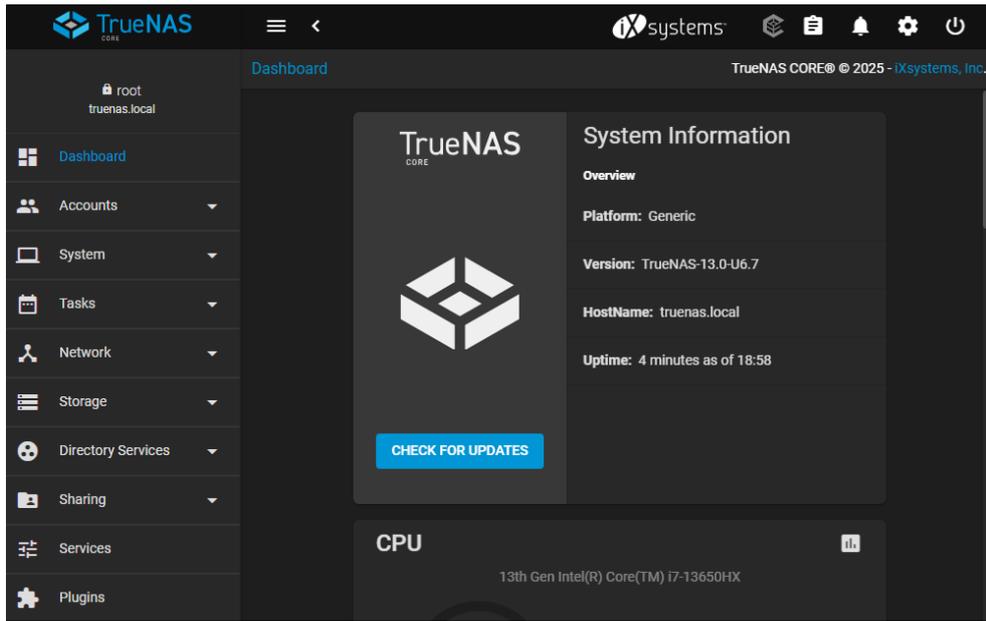
The web user interface is at:
http://192.168.2.63
https://192.168.2.63

Enter an option from 1-11: █
```

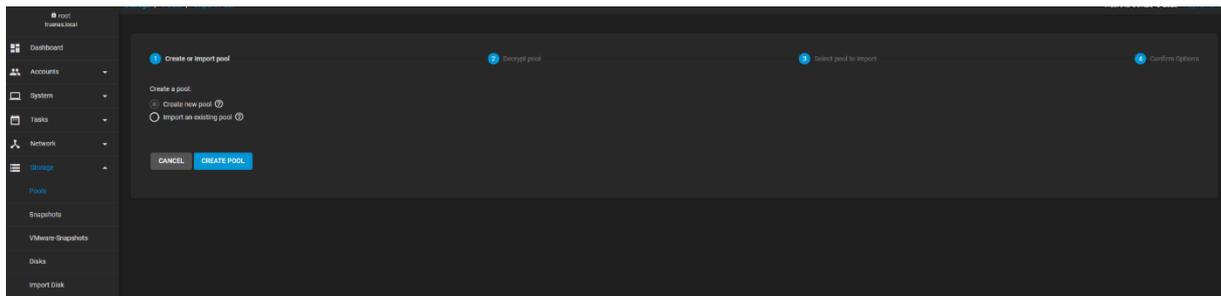
Nous arrivons sur la page de connexion de TrueNAS. Nous allons nous connecter avec l'utilisateur root et le mot de passe défini lors de l'installation.



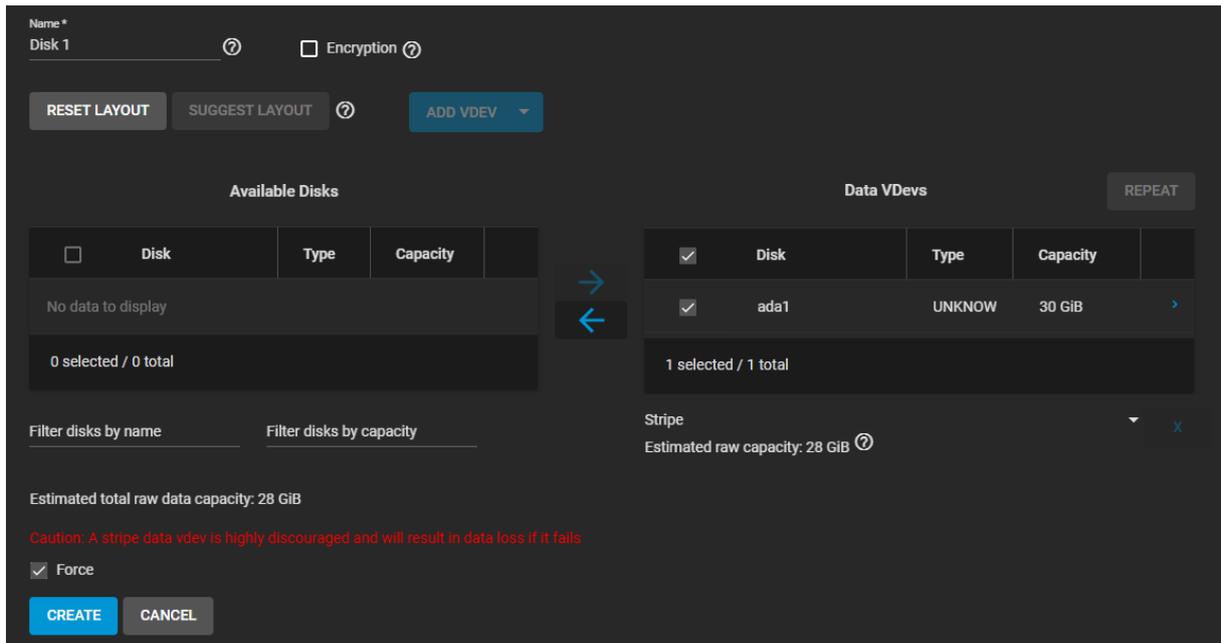
Nous sommes maintenant sur le **tableau de bord** de TrueNAS.



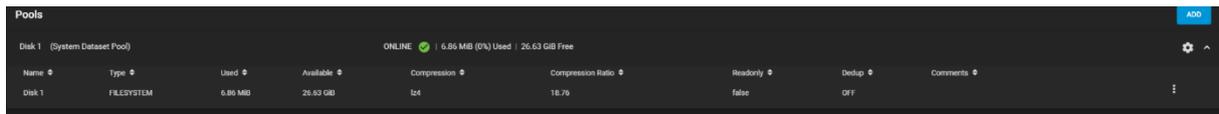
Nous sommes dans la section Pools du stockage. Nous allons créer un nouveau pool pour utiliser notre disque dur disponible.



Nous avons sélectionné notre disque de 30 Go (**ada1**) pour créer un pool de stockage en mode **Stripe**.

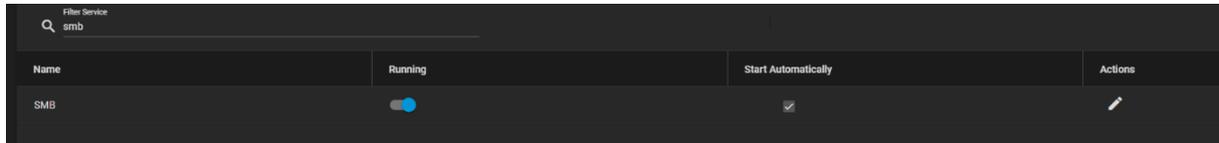


Notre pool Disk 1 est maintenant créé et opérationnel.



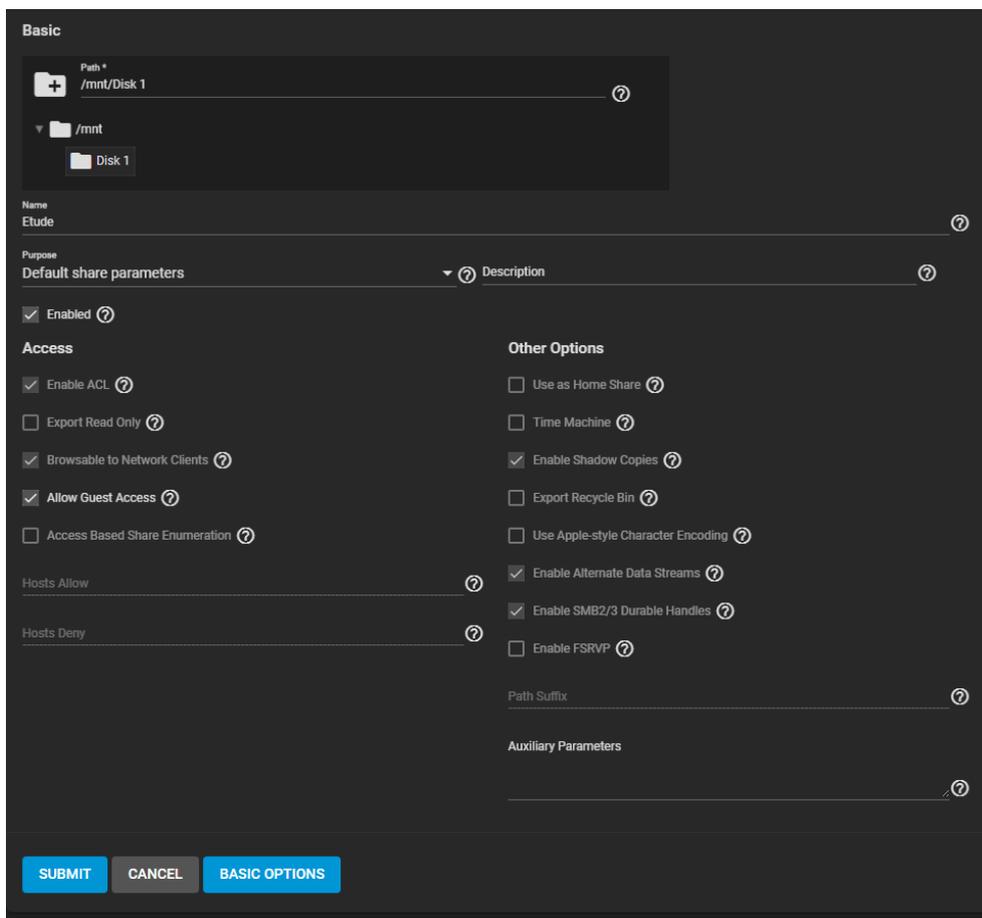
Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
Disk 1	FILESYSTEM	6.86 MB	26.63 GB	lzo	18.76	false	OFF	

Le service SMB est maintenant activé et configuré pour démarrer automatiquement au boot. Cela nous permettra de partager des fichiers sur le réseau en utilisant le protocole Samba.



Name	Running	Start Automatically	Actions
SMB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Nous avons créé un partage réseau SMB nommé Étude, pointant vers le disque Disk 1. Ce partage est activé et utilisera les paramètres par défaut.



**Basic**

Path 1  
/mnt/Disk 1

Name  
Etude

Purpose  
Default share parameters

Enabled

**Access**

Enable ACL

Export Read Only

Browsable to Network Clients

Allow Guest Access

Access Based Share Enumeration

**Other Options**

Use as Home Share

Time Machine

Enable Shadow Copies

Export Recycle Bin

Use Apple-style Character Encoding

Enable Alternate Data Streams

Enable SMB2/3 Durable Handles

Enable FSRVP

Hosts Allow

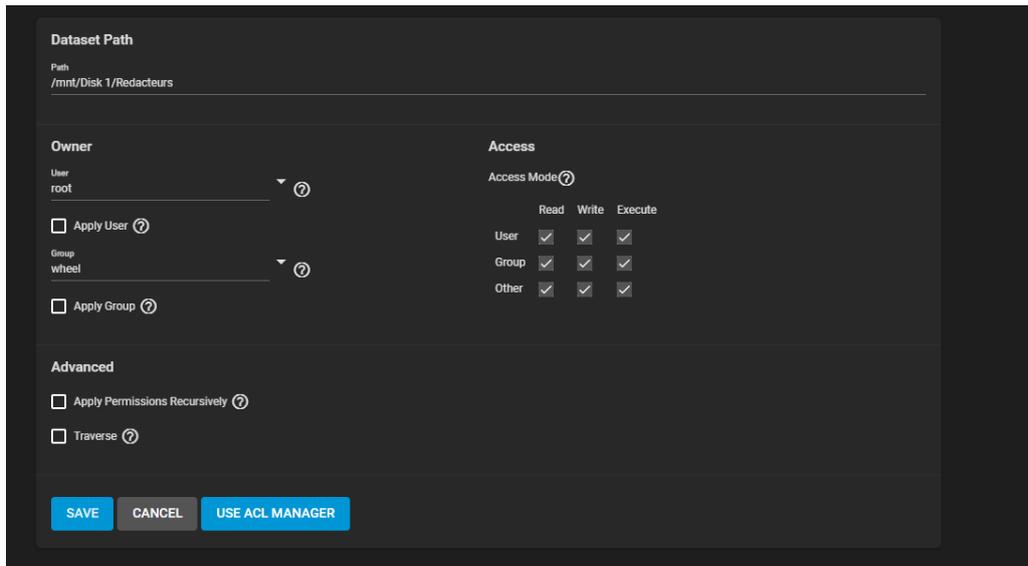
Hosts Deny

Path Suffix

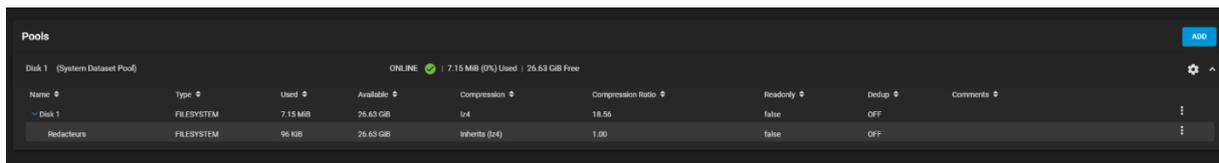
Auxiliary Parameters

**SUBMIT** **CANCEL** **BASIC OPTIONS**

Nous avons configuré les permissions du dataset **Rédacteurs**, en attribuant tous les droits (lecture, écriture, exécution) aux utilisateurs, groupes et autres.



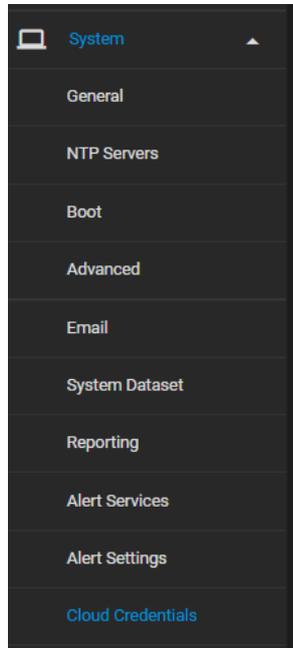
Nous avons ajouté le dataset Rédacteurs au pool Disk 1, permettant d'organiser le stockage en sous-volumes distincts. Ce dataset hérite de la compression lz4 et est opérationnel.



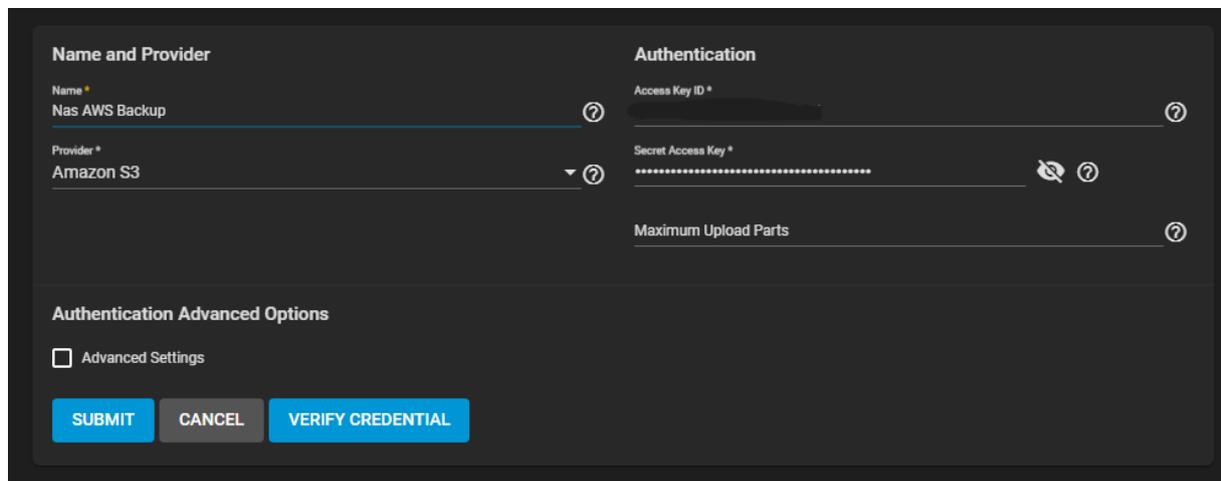
Maintenant que tout est en place, les collaborateurs pourront accéder au stockage via l'explorateur de fichier en tapant [\\192.168.2.63](http://192.168.2.63)

- 3.1.2. Sauvegarde automatique et réplication des fichiers via bucket AWS

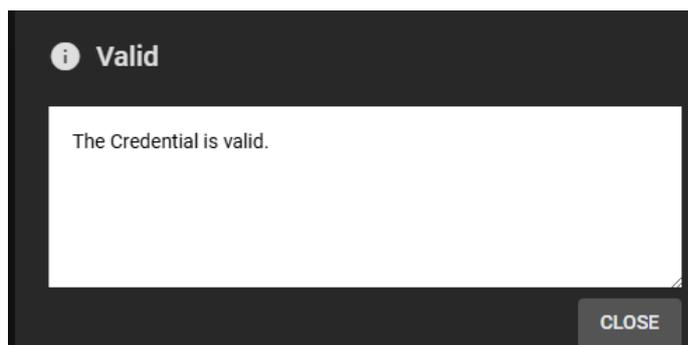
Maintenant nous accédons à Cloud Credentials pour configurer notre sauvegarde sur AWS



Nous avons ajouté nos identifiants AWS dans la section Cloud Credentials de TrueNAS. Cela nous permettra de configurer la sauvegarde vers Amazon S3.

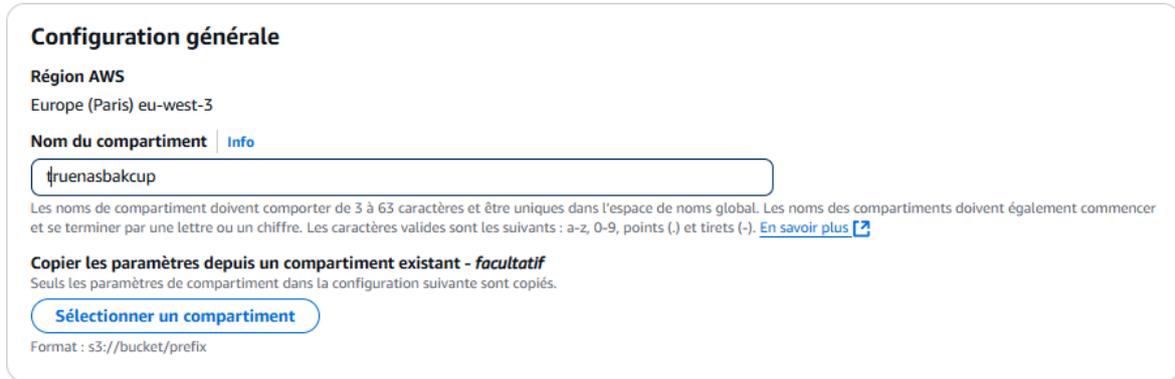


Nos identifiants AWS ont été validés avec succès. Nous pouvons maintenant configurer la sauvegarde automatique de notre NAS vers Amazon S3.

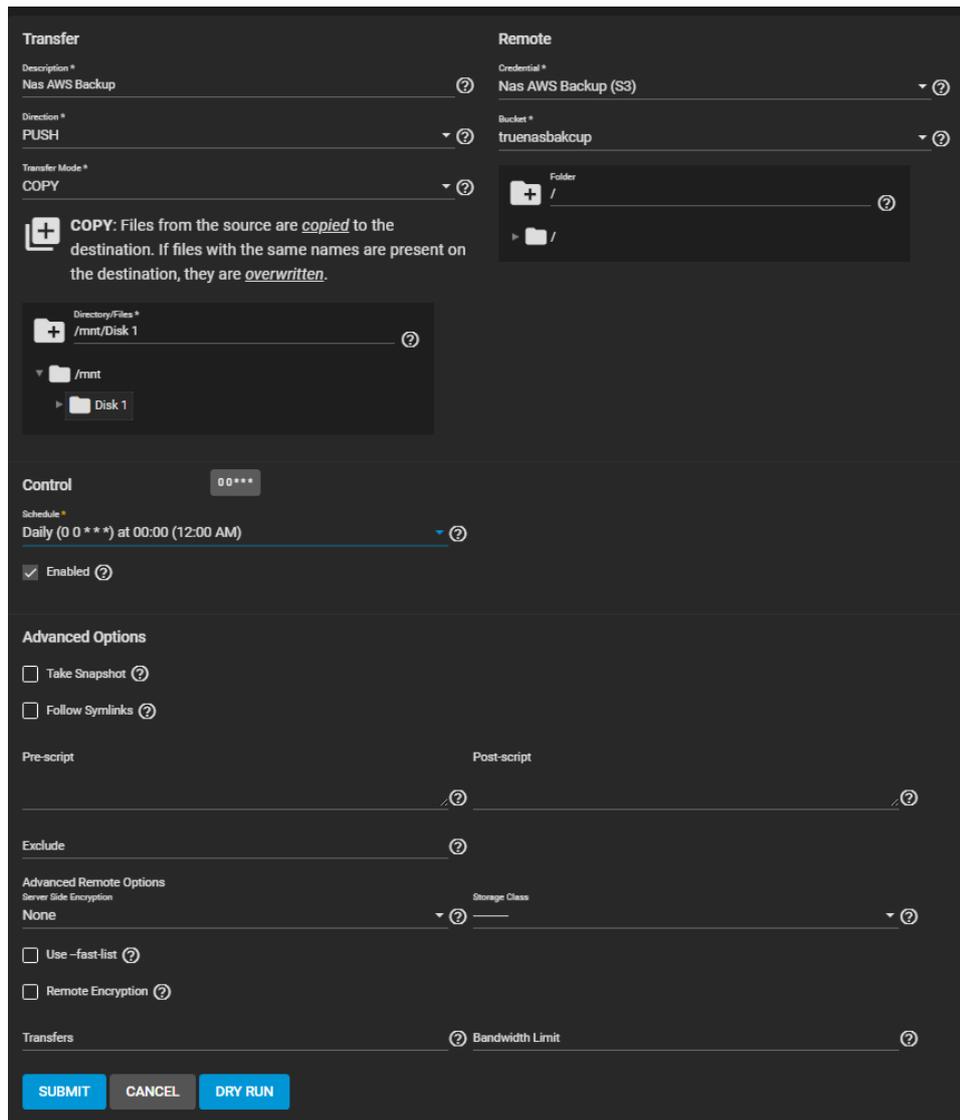


Tout d'abord nous allons nous rendre sur la console administrateur AWS et créer un **compartiment S3** nommé **"truenasbackup"**.

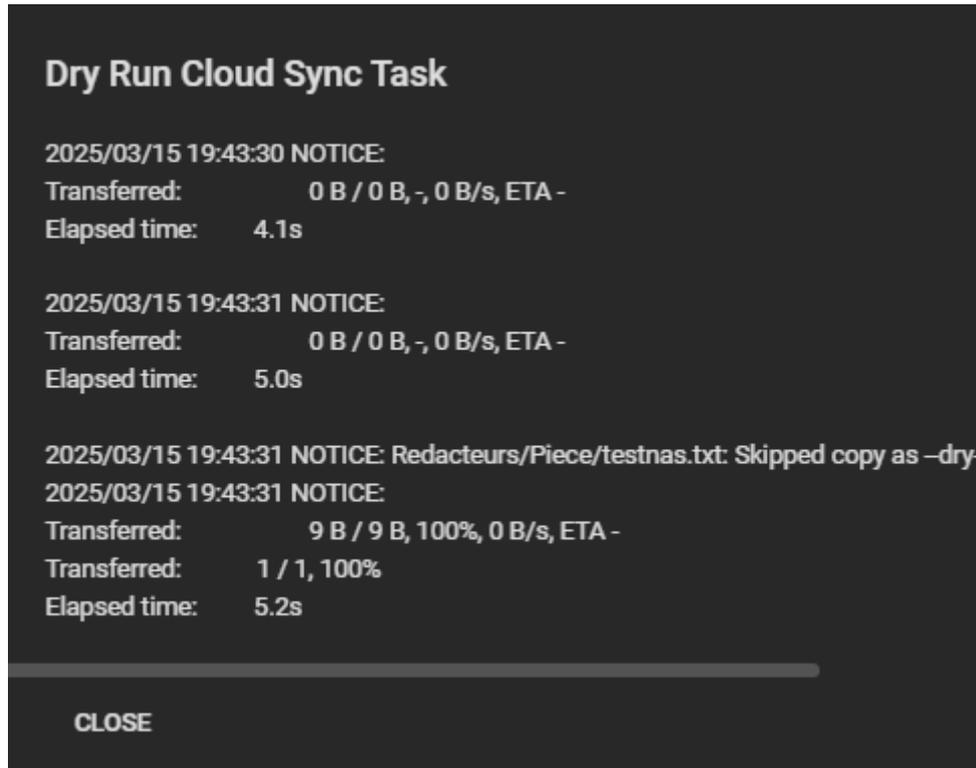
Ce compartiment servira à stocker les sauvegardes de notre TrueNAS.



Nous avons configuré une tâche de synchronisation Cloud Sync pour envoyer (PUSH) les fichiers de /mnt/Disk 1 vers notre compartiment S3 "truenasbackup". La synchronisation se fera quotidiennement à minuit en mode COPY, ce qui garantit que les fichiers du NAS seront copiés sur AWS sans suppression des données existantes. Les sauvegardes s'effectueront tous les soir à minuit.



Nous avons effectué un Dry Run pour vérifier la synchronisation des fichiers vers AWS S3. Le test montre qu'un fichier testnas.txt a bien été identifié pour transfert, confirmant que la configuration est correcte.



Le fichier **testnas.txt** est bien présent dans le compartiment configuré, confirmant que la synchronisation entre **TrueNAS** et **AWS** fonctionne correctement.

**Objets (1)**

Les objets sont les entités fondamentales stockées dans Amazon S3. Vous pouvez utiliser [l'inventaire Amazon S3](#) pour obtenir une liste de tous les objets de votre compartiment. Pour que d'autres personnes puissent accéder à vos objets, vous devez leur accorder explicitement des autorisations. [En savoir plus](#)

Rechercher des objets en fonction du préfixe < 1 >

<input type="checkbox"/>	Nom ▲	Type ▼	Dernière modification ▼	Taille ▼	Classe de stockage ▼
<input type="checkbox"/>	<a href="#">testnas.txt</a>	txt	16 Mar 2025 03:44:38 AM CET	9.0 o	Standard

## 5/ Messagerie d'entreprise avec Zimbra

Je possède le nom de domaine moreaunotaires.fr

The screenshot shows the 'Ajouter des options à vos noms de domaine' (Add options to your domain names) page. On the left, under 'Ajouter des comptes e-mail liés au domaine' (Add email accounts linked to the domain), it states 'moreaunotaires.fr' with a green checkmark and '1 compte e-mail Zimbra Starter inclus' (1 Zimbra email account included). On the right, the 'Votre sélection' (Your selection) panel shows 'Noms de domaine' (Domain names) as 'moreaunotaires.fr', 'Durée' (Duration) as '1 an' (1 year), and 'Renouvellement en mars 2026 pour 7,79€' (Renewal in March 2026 for 7.79€). An option for 'DNSSEC (DNS sécurisé)' (DNSSEC (DNS secured)) is also visible.

Activation d'un compte Zimbra lié au domaine moreaunotaires.fr via OVH.

Nous allons ajouter un enregistrement DNS CNAME pour valider le domaine moreaunotaires.fr auprès de Zimbra.

### Zimbra

The screenshot shows the Zimbra verification page. At the top, a green notification bar says 'Votre demande d'ajout a bien été prise en compte. Elle sera exécutée d'ici quelques instants.' (Your request for addition has been successfully received. It will be executed within a few moments). Below, there is a link 'Retour vers les noms de domaine' (Return to domain names) and the section 'Vérification de votre domaine' (Verification of your domain). The text explains: 'Pour valider que vous êtes titulaire du domaine moreaunotaires.fr, veuillez ajouter cet enregistrement DNS:' (To validate that you are the owner of the domain moreaunotaires.fr, please add this DNS record:). The 'Type d'enregistrement' (Record type) is 'CNAME'. The 'Sous domaine' (Subdomain) is 'ovh-zimbra-msars0dx.moreaunotaires.fr' and the 'Cible' (Target) is 'ovh.com'. A warning message states: 'À la suite de la validation de votre domaine, vous devrez modifier manuellement les enregistrements MX, SRV, SPF et DKIM dans votre zone DNS. Vous pourrez trouver les informations requises dans la page diagnostic du domaine associé.' (After validation of your domain, you will need to manually modify the MX, SRV, SPF, and DKIM records in your DNS zone. You will find the required information in the associated domain's diagnostic page). A link to 'notre guide' (our guide) is provided.

Nous avons validé l'installation de la zone DNS du domaine moreaunotaires.fr via OVHcloud.

**OVHcloud** Suivant →

### Bon de commande

[Version imprimable](#)

Numéro : 225026579 **Contact de facturation :**  
 Date : 10 mars 2025 21:17:15 ILYES BERRADA  
 Expiration : 24 mars 2025 23:29:59 335 Avenue Frédéric Sabatier d'Espeyran, Bat B Apt 5  
 Etat : En cours de validation 34090 MONTPELLIER  
FR

INSTALLATION	Domaine	Prix unitaire	Quantité	Prix HT
moreaunotaires.fr - Zone DNS - Installation	*001	-	1	0,00 PTS
DNS zone	*001	-	1	0,00 PTS
<b>SOUS-TOTAL</b>				<b>0,00 PTS</b>

SPÉCIAL	Domaine	Prix unitaire	Quantité	Prix HT
Exécution immédiate de la commande en renonçant au droit de rétractation	*	-	1	0,00 PTS
<b>SOUS-TOTAL</b>				<b>0,00 PTS</b>

ABONNEMENT	Domaine	Prix unitaire	Quantité	Prix HT
moreaunotaires.fr - Zone DNS - Installation	*001	-	1	0,00 PTS
<b>SOUS-TOTAL</b>				<b>0,00 PTS</b>

Total HT	0,00 PTS
TVA	0,00 PTS

Nous utilisons les serveurs DNS d'OVH (dns20.ovh.net et ns20.ovh.net) pour la gestion du domaine moreaunotaires.fr.

Noms de domaine / moreaunotaires.fr / Serveurs DNS

**moreaunotaires.fr**

[Roadmap & Changelog](#) [Actions](#) ▾

[Informations générales](#) [Zone DNS](#) [Serveurs DNS](#) [Redirection](#) [GLUE](#) [DS Records](#) [Tâches récentes](#) [Gérer les contacts](#)

⌚ Pour vous assurer du bon fonctionnement de votre configuration, vous pouvez utiliser cet [outil de vérification DNS](#).

[Commander DNS Anycast](#)

[Modifier les serveurs DNS](#)

Serveur DNS	IP associée	Statut	Type des serveurs DNS
dns20.ovh.net	-	Actif	Standard ⓘ
ns20.ovh.net	-	Actif	Standard ⓘ

⏪ ⏩

**Guides**

Serveurs DNS ▾

Nous avons activé la zone DNS du domaine pour une durée de 12 mois, avec validation des conditions d'utilisation.

Informations générales **Zone DNS** Serveurs DNS Redirection GLUE DS Records Tâches récentes Gérer les contacts

[← Retour à la page précédente](#)

### Activer votre zone DNS

Pour répondre aux requêtes DNS, votre nom de domaine doit être relié à une zone DNS. Vous pourrez y configurer vers quelle adresse IP sera redirigé votre domaine et ses sous domaines. La zone DNS de votre domaine est désactivé. Si vous souhaitez l'activer, validez les étapes suivantes.

✓ Choisissez votre durée

12 mois : Inclus

**2** Activation

Afin de confirmer votre demande, veuillez accepter les conditions d'utilisation.

J'ai pris connaissance et j'accepte les termes des contrats suivants :

- [Data\\_Protection\\_Agreement](#)
- [CONDITIONS PARTICULIERES D'ENREGISTREMENT, DE RENOUVELLEMENT ET DE TRANSFERT DE NOMS DE DOMAINE](#)
- [Conditions Generales de Services](#)

**Activer** Annuler

Nous avons configuré les enregistrements DNS nécessaires (A, MX, SPF, TXT, CNAME) pour assurer le bon fonctionnement du domaine moreaunotaires.fr avec la messagerie et le site.

Domaine	TTL	Type	Cible
moreaunotaires.fr.	0	NS	dns20.ovh.net.
moreaunotaires.fr.	0	NS	ns20.ovh.net.
moreaunotaires.fr.	0	A	213.186.33.5
www.moreaunotaires.fr.	0	A	213.186.33.5
ftp.moreaunotaires.fr.	0	CNAME	moreaunotaires.fr.
moreaunotaires.fr.	0	SPF	v=spf1 include:mx.ovh.com -all
moreaunotaires.fr.	0	TXT	"1 www.moreaunotaires.fr"
www.moreaunotaires.fr.	0	TXT	"3 welcome"
moreaunotaires.fr.	0	MX	1 mx1.mail.ovh.net.
moreaunotaires.fr.	0	MX	5 mx2.mail.ovh.net.

« 1 2 » Page 1 / 2 OK

Nous avons associé le domaine moreaunotaires.fr à l'organisation "Étude" et confirmé que le statut du service Zimbra est "READY".

Informations générales **Domaine** Compte email

[+ Ajouter un domaine](#)

Domaine	Organisation	Nombre de comptes	Statut
moreaunotaires.fr	Étude	1	READY

Nous avons créé le compte mail [isabelle.moreau@moreaunotaires.fr](mailto:isabelle.moreau@moreaunotaires.fr) pour une collaboratrice de l'étude, rattaché à l'organisation "Étude".

**Etude** Etude X

[← Retour vers mes comptes emails](#)

### Modifier le compte [isabelle.moreau@moreaunotaires.fr](mailto:isabelle.moreau@moreaunotaires.fr)

#### Paramètres du compte

Les champs mentionnés avec un astérisque \* sont obligatoires.

#### Compte email \*

@

La partie locale de votre adresse (le texte précédant le « @ ») doit suivre les lignes directrices suivantes :

- Elle doit se terminer par une lettre ou un numéro
- Les caractères spéciaux autorisés sont : ".,\_+,-" et ".\_"
- Les caractères spéciaux ne peuvent pas être placés côte à côte

Votre compte fera partie de l'organisation Etude

#### Nom

#### Prénom

#### Nom à afficher

#### Mot de passe

Votre mot de passe doit contenir au minimum :

- 10 caractères
- 1 chiffre et 1 caractère spécial (\$, !, &, ...)
- 1 lettre majuscule

Le compte de la cliente a bien été créé, en se rendant sur le webmail elle pourra travailler sans soucis de manière sécurisée

**zimbra**

## Connexion

Utilisateur

Mot de passe

Mémoriser mes valeurs d'accès

Version

Je créé aussi un raccourci sur le bureau pour que la cliente se rende sur son mail plus facilement.



## **Fiche de tests**

Nous allons maintenant vérifier si toutes les configurations faites précédemment fonctionnent. Nous procéderons comme ceci :

1. Redondance Active Directory et DNS
2. VPN Sécurisé avec OpenVPN
3. Surveillance et Sécurité du Réseau
  - 3.1. Système de Détection d’Intrusion (IDS/IPS)
  - 3.2. Analyse du Trafic avec Wireshark
4. Stockage et Partage des Données
  - 4.1. Infrastructure NAS avec TrueNAS

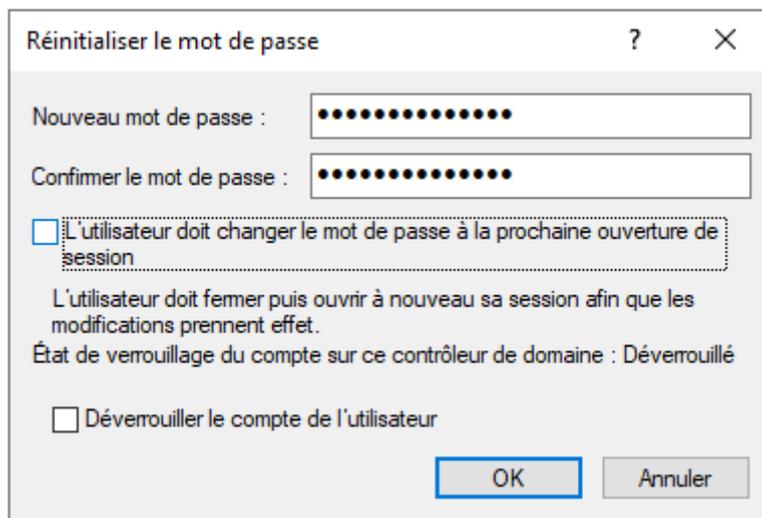
## 1. Redondance Active Directory et DNS

En premier lieu nous allons éteindre le serveur principal et voir si le serveur secondaire prend le relais.

```
C:\Users\i.moreau>nslookup technovalis.local 192.168.2.6
Serveur : SRVBACKUP.technovalis.local
Address: 192.168.2.6

Nom : technovalis.local
Addresses: 192.168.2.4
          192.168.2.6
```

Il prend bien le relai, maintenant nous allons tenter la modification des identifiant d'un utilisateur.



Réinitialiser le mot de passe

Nouveau mot de passe : ●●●●●●●●●●

Confirmer le mot de passe : ●●●●●●●●●●

L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

L'utilisateur doit fermer puis ouvrir à nouveau sa session afin que les modifications prennent effet.

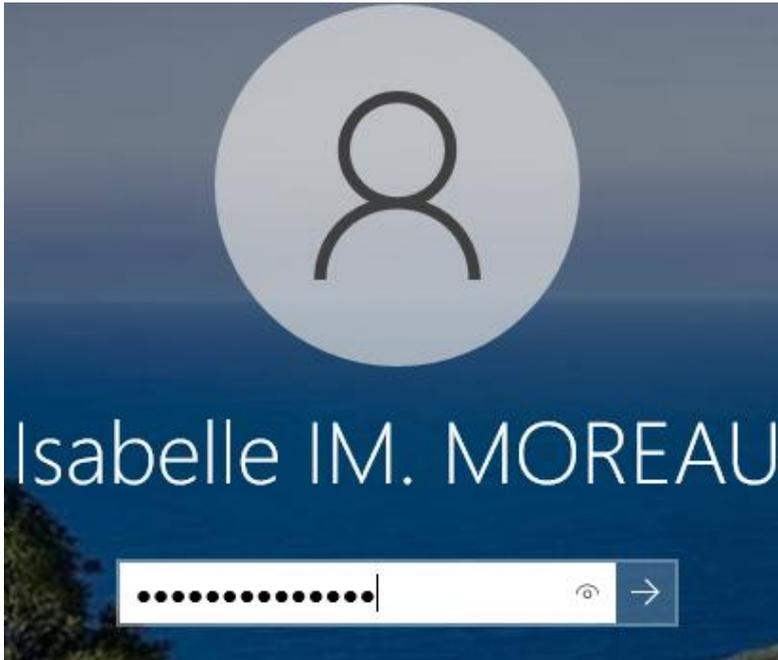
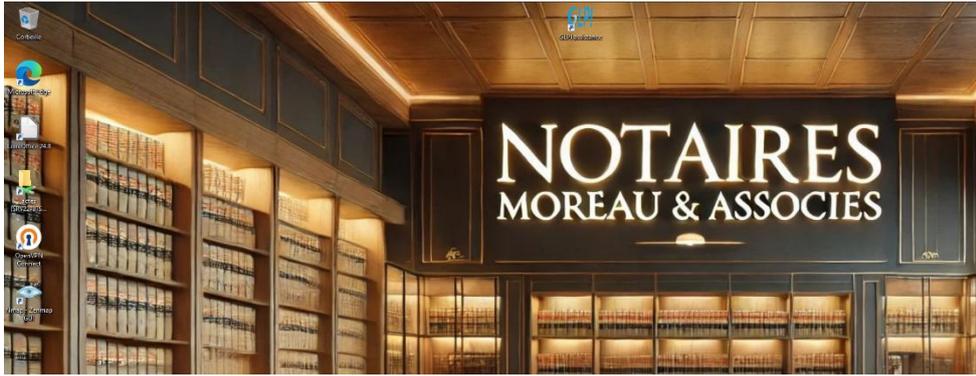
État de verrouillage du compte sur ce contrôleur de domaine : Déverrouillé

Déverrouiller le compte de l'utilisateur

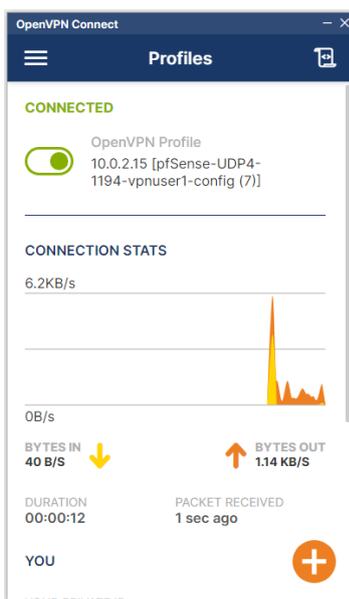
OK Annuler

## 2. VPN Sécurisé avec OpenVPN

Les identifications utilisateur ont bien été modifiés



## 2. VPN Sécurisé avec OpenVPN



On arrive bien à se connecter à notre server VPN.

### 3. Système de Détection d’Intrusion (IDS/IPS)

2017-07-22 06:15:49	2	UDP	Potentially Bad Traffic	163.172.17.76	54465		5060	140:26	(spp_sip) Method is unknown
2017-07-21 09:26:30	2	UDP	Potentially Bad Traffic	163.172.22.169	52428		5060	140:26	(spp_sip) Method is unknown
2017-07-21 01:03:28	2	UDP	Potentially Bad Traffic	163.172.17.76	46834		5060	140:26	(spp_sip) Method is unknown
2017-07-20 20:36:37	2	UDP	Potentially Bad Traffic	163.172.22.169	54788		5060	140:26	(spp_sip) Method is unknown

Notre système de détection d’intrusion fonctionne correctement, des alertes commencent à remonter

#### Analyse du Trafic avec Wireshark

Je lance wireshark sur l’interface Ethernet puis je tente de faire un ping depuis une autre machine.

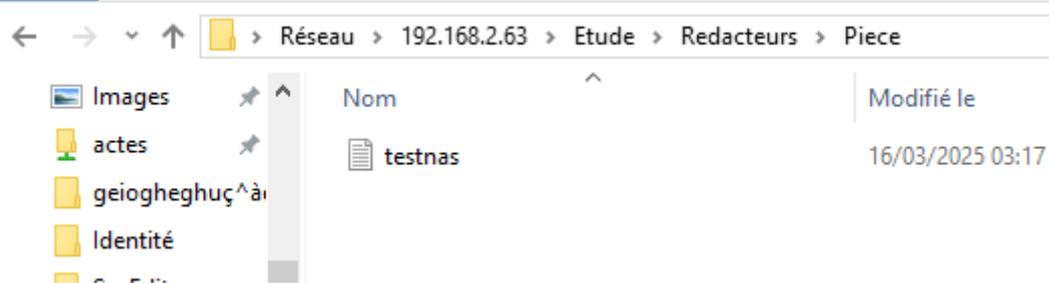
La trame icmp du ping remonte bien.



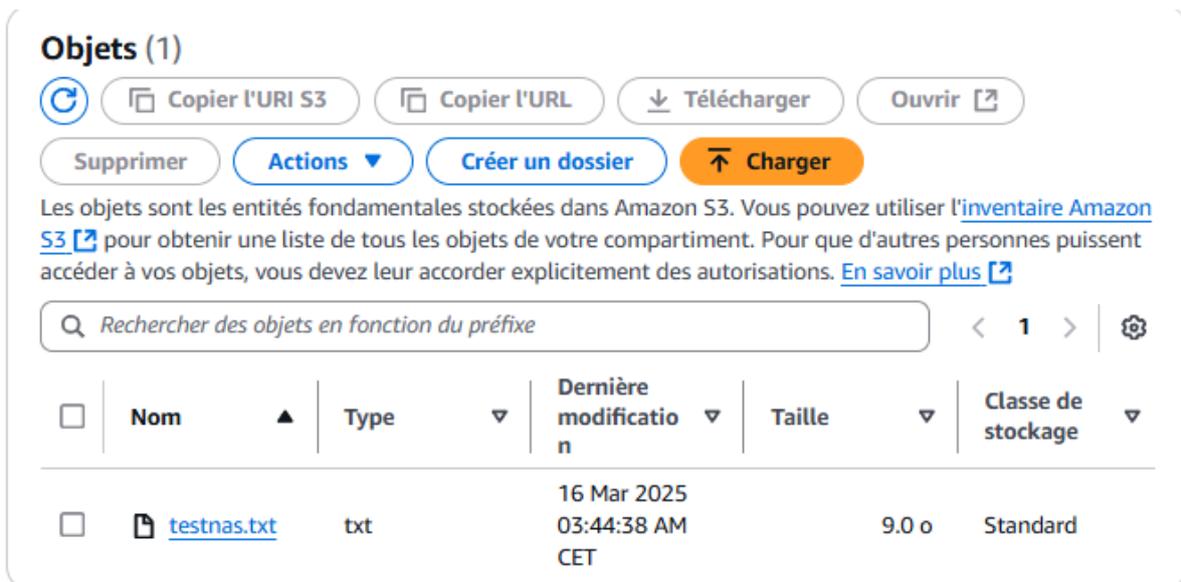
### 3. Infrastructure NAS avec TrueNAS

Je test sur un poste client l’accès au nas depuis l’explorateur de fichier

On a bien accès au serveur depuis un poste

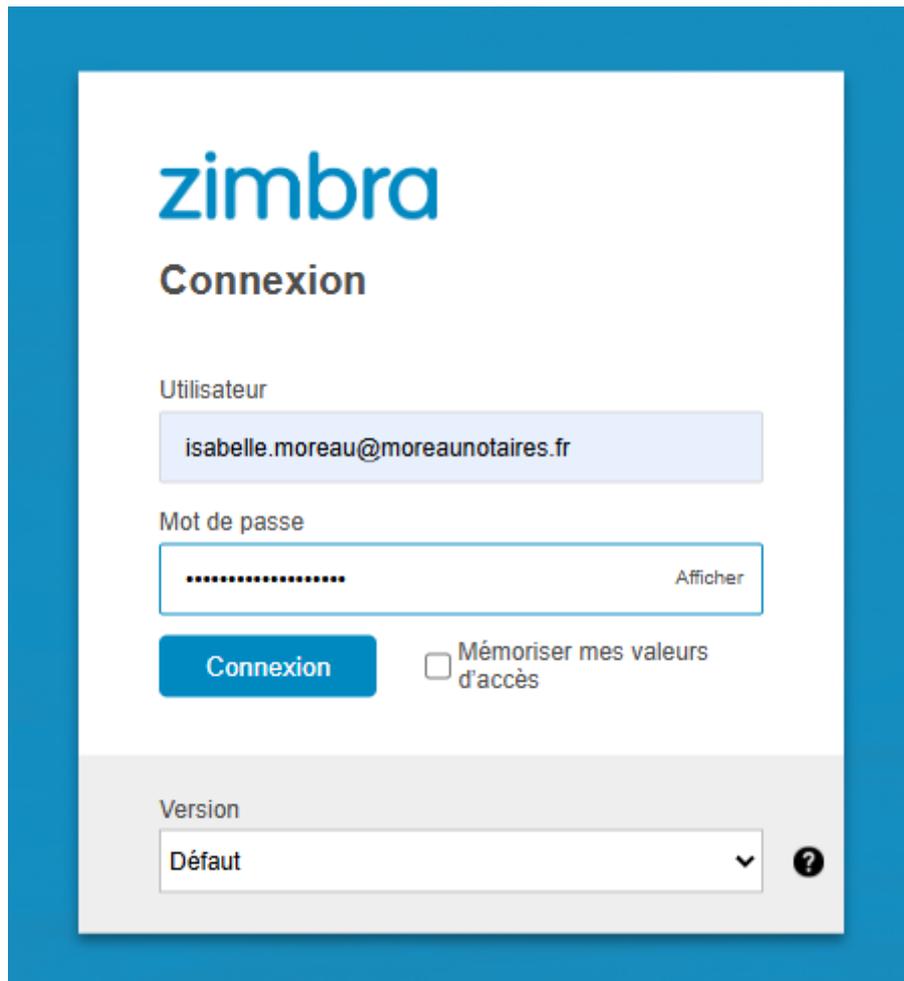


De plus la sauvegarde cloud du serveur de stockage se fait bien comme le montre la console AWS



### 4. Messagerie d’entreprise

La cliente se rendre sus zimbra pour pouvoir s’y connecter



Une fois ici on va se connecter et simplement faire un test d'envoi réception vers une adresse gmail, plus précisément la mienne



Nous pouvons voir que l'envoi de mail fonctionne bien.

## Ainsi que la réception.

