BERRADA Ilyes

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

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.

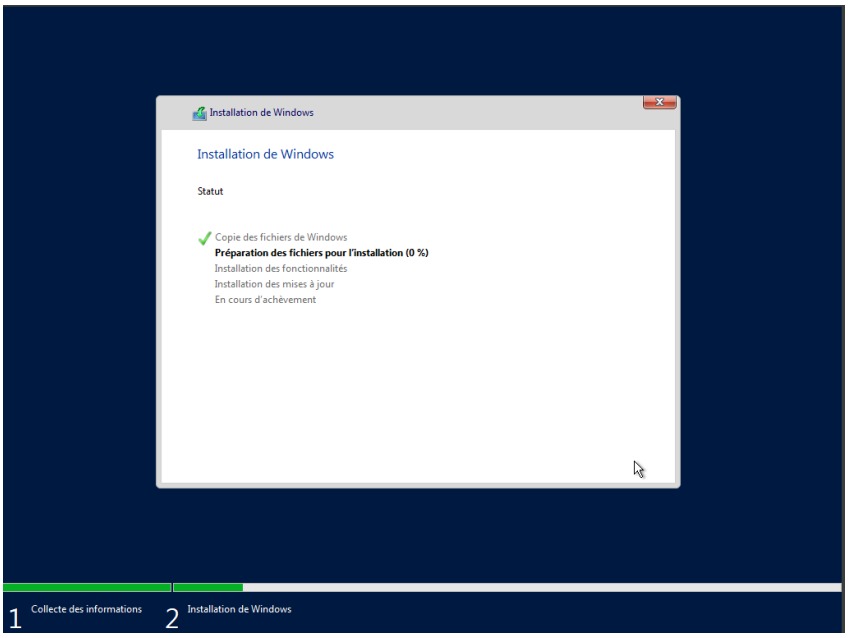
Avec ces solutions, TechNovalis dispose d'une infrastructure résiliente et adaptée aux besoins actuels en matière de sécurité et de connectivité.

1. ***Infrastructure réseau***

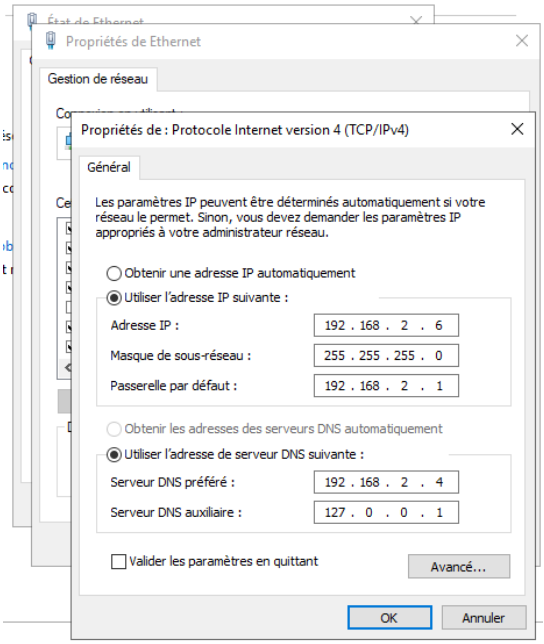
1.1. Redondance Active Directory et DNS

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

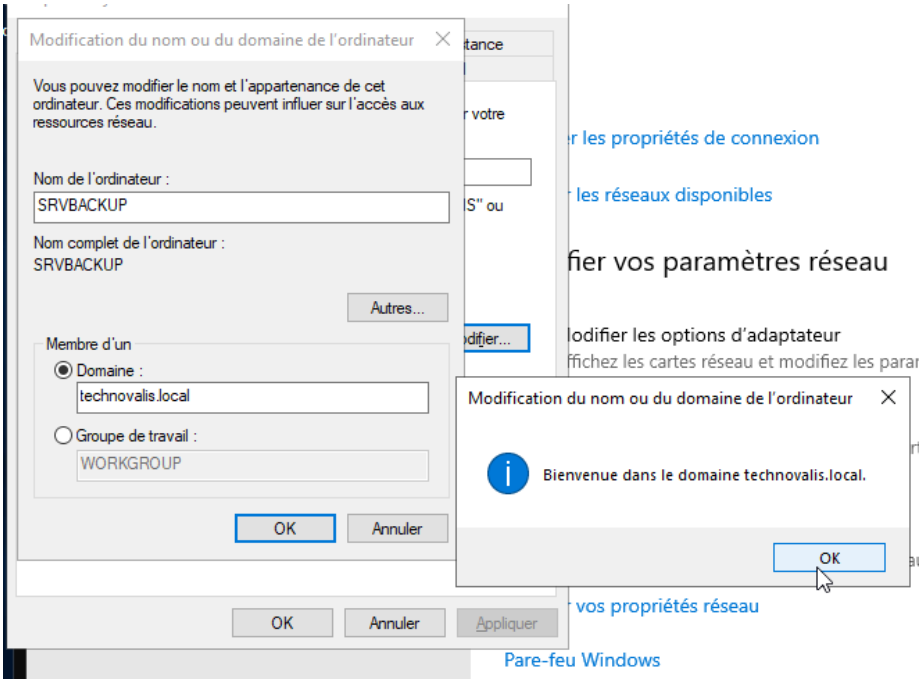
Nous installons Windows Server sur une nouvelle machine virtuelle afin d'assurer la redondance de notre infrastructure. Cette étape consiste à copier les fichiers nécessaires et préparer l'installation avant d'ajouter les rôles et fonctionnalités requis pour l'intégration du serveur dans notre domaine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

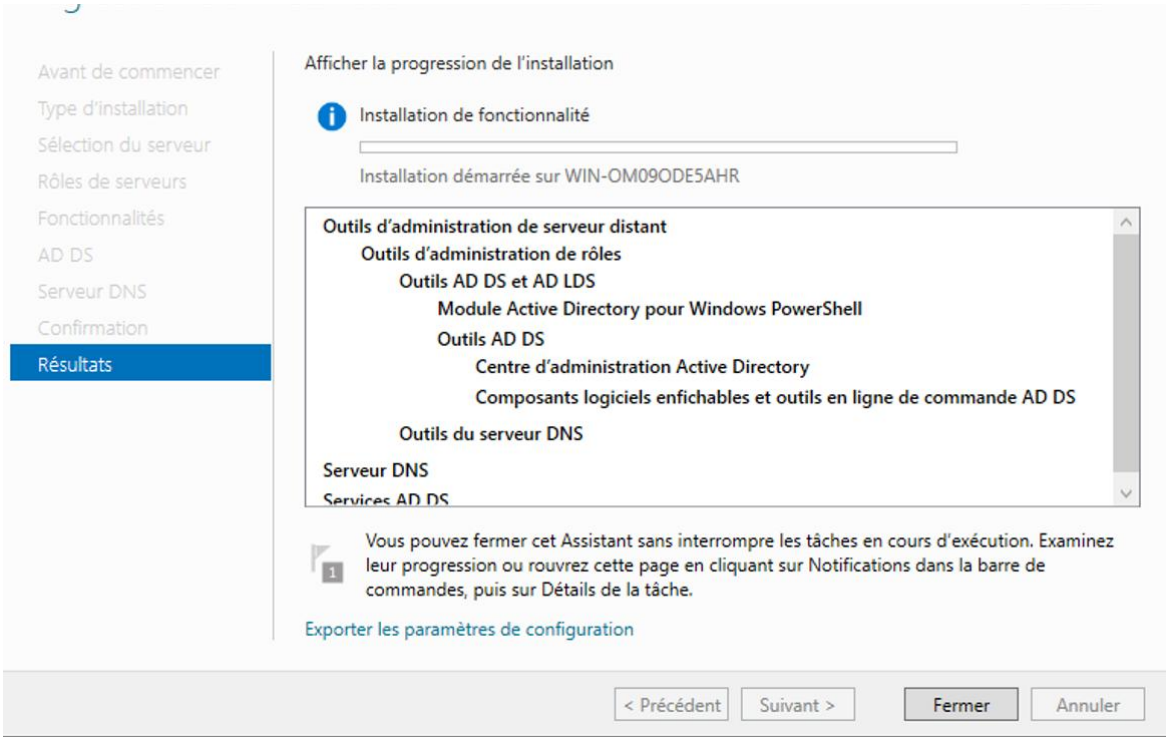


Nous intégrons le serveur de secours **SRVBACKUP** au domaine **technovalis.local**.



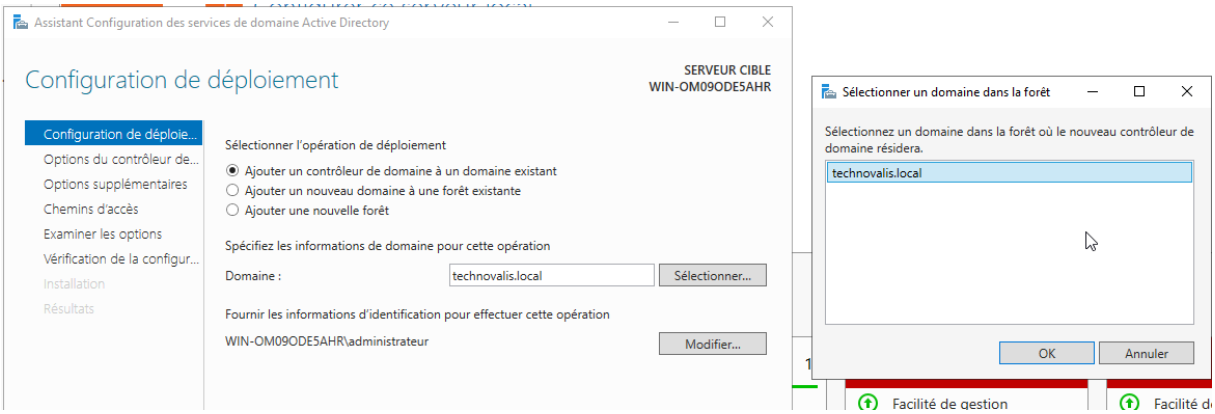
On redémarre la VM

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

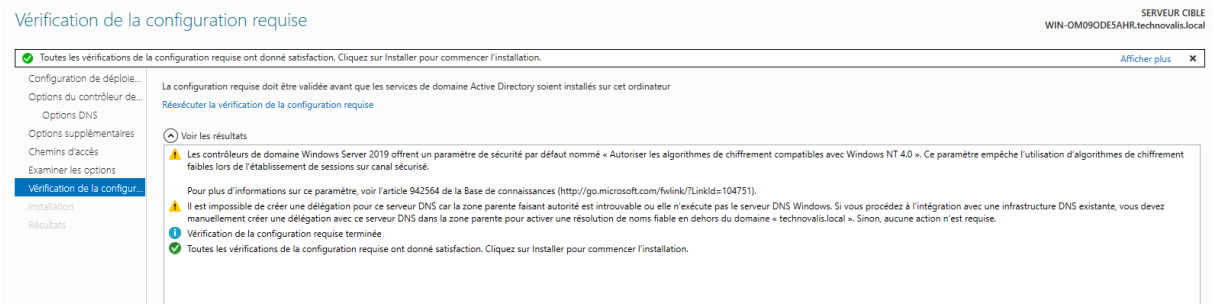


Nous configurons notre nouveau serveur en tant que contrôleur de domaine supplémentaire dans la forêt existante du domaine principal technovalis.local. Cette étape permet d'assurer la redondance d'Active

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

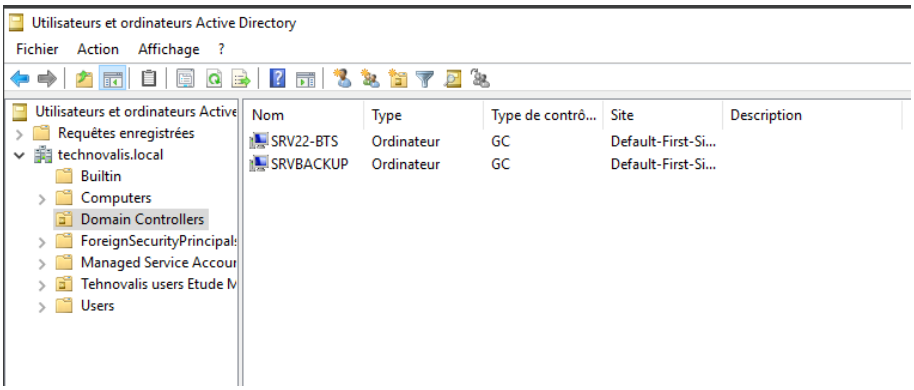


Nous avons effectué la vérification de la configuration requise avant l'installation d'Active Directory sur notre serveur secondaire. Toutes les vérifications ont été validées avec succès, nous pouvons maintenant lancer l'installation sans problème.

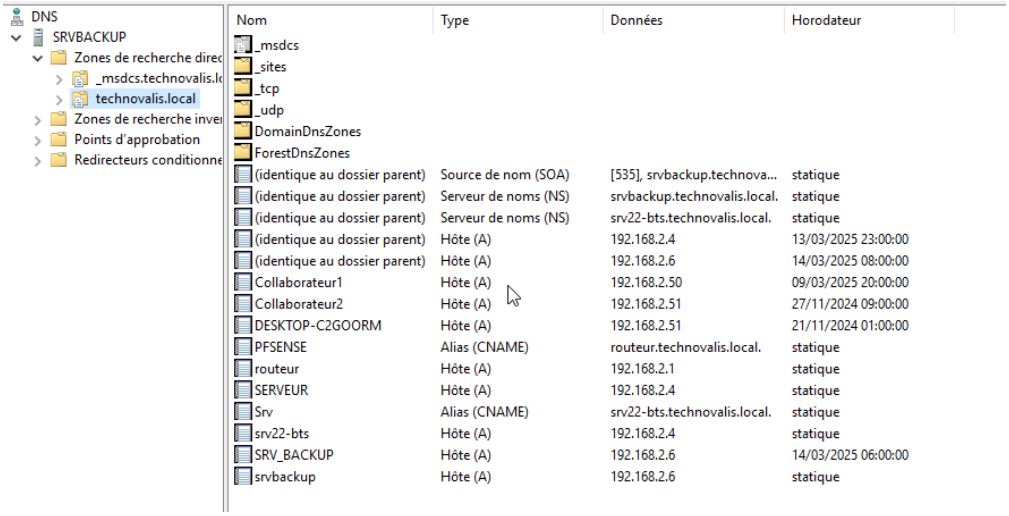


Nous pouvons à présent redémarrer le second serveur.

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.



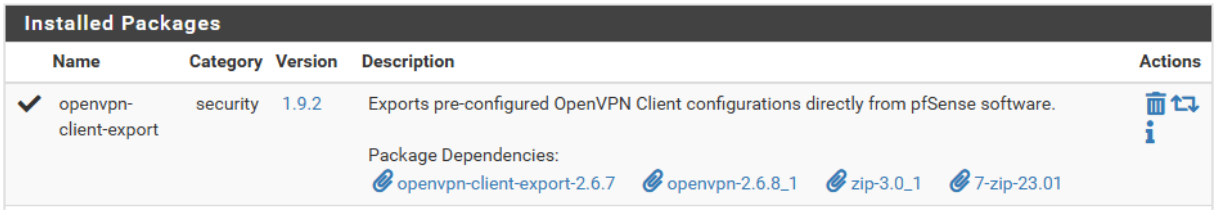
Nous avons effectué une résolution de nom avec NSLOOKUP en interrogeant SRVBACKUP (192.168.2.6). Celui-ci renvoie bien les adresses IP des deux contrôleurs de domaine (SRV22-BTS et SRVBACKUP), confirmant ainsi que la redondance DNS est opérationnelle.

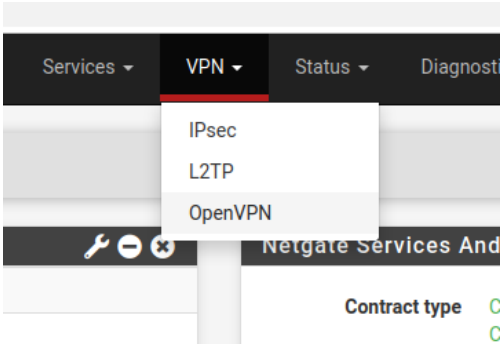
```
C:\Users\Administrateur.TECHNOVALIS>nslookup technovalis.local 192.168.2.6
Serveur :   SRVBACKUP.technovalis.local
Address:  192.168.2.6

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

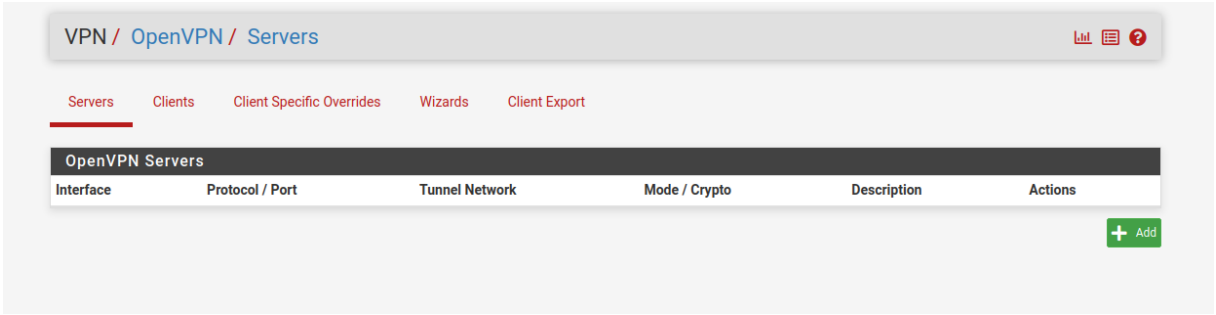
1.2. VPN sécurisé avec OpenVPN

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

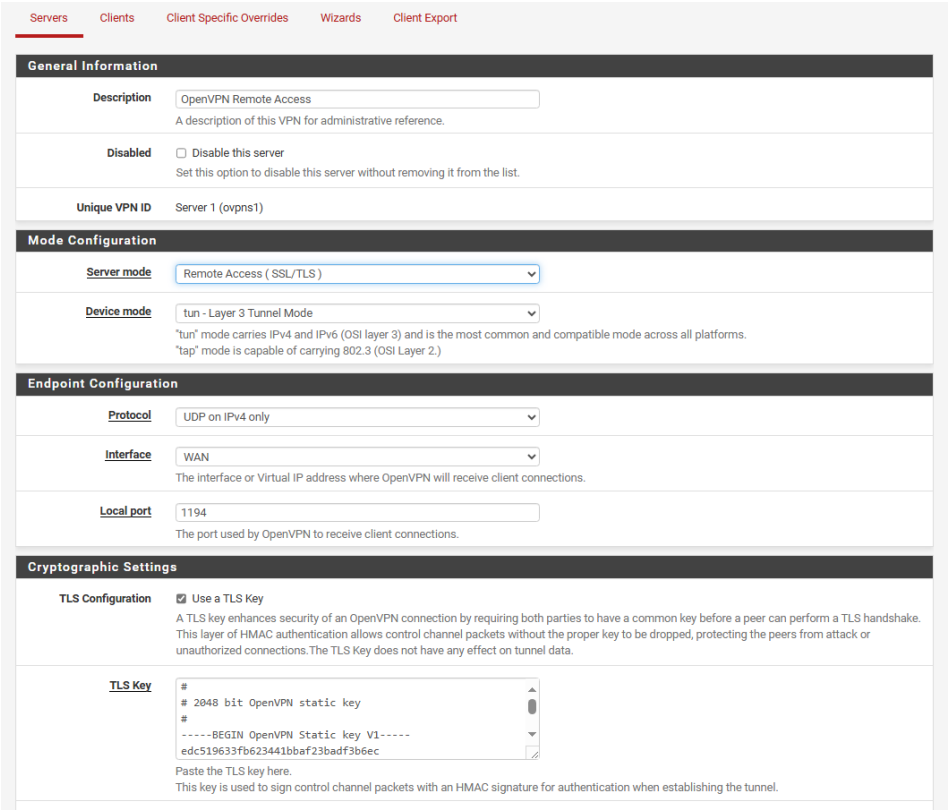




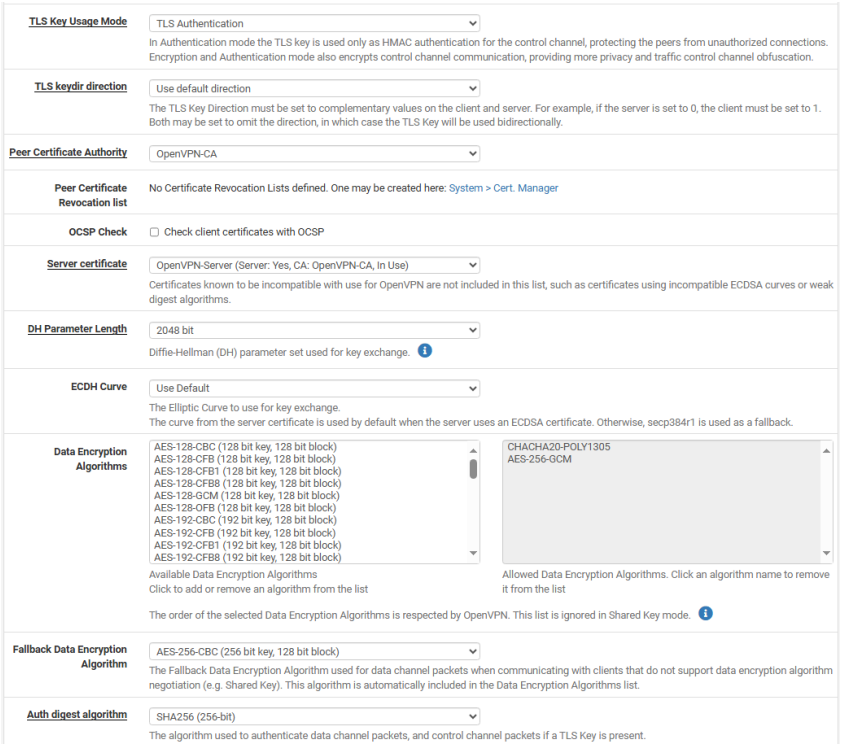
Nous accédons à l'interface de configuration d'OpenVPN sur pfSense via **VPN > OpenVPN > Servers**. À cette étape, aucun serveur VPN n'est encore configuré.



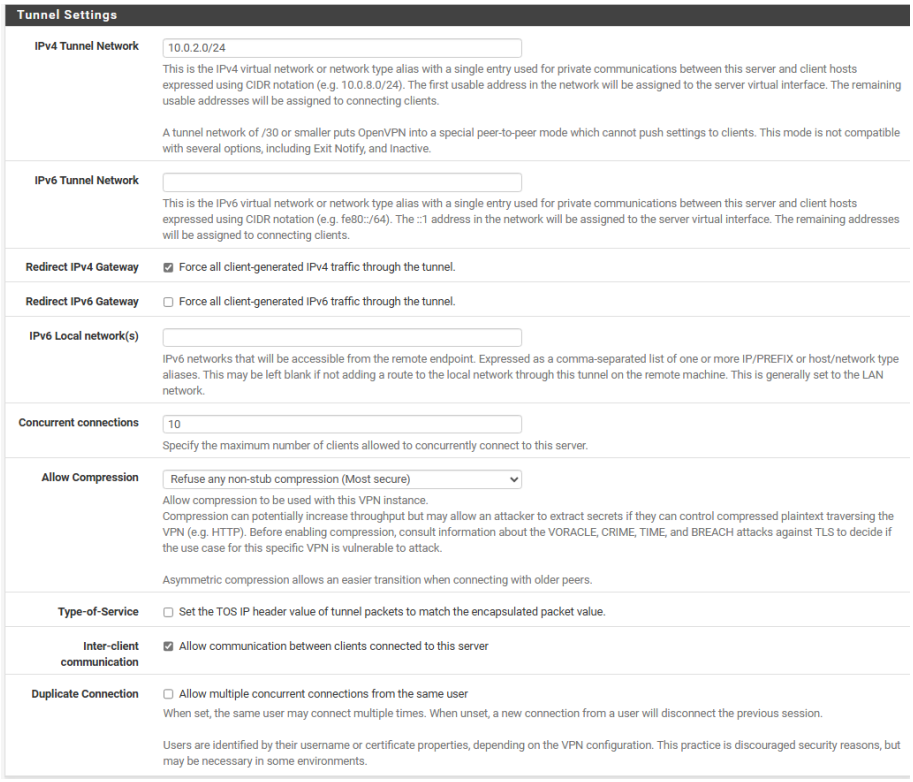
Nous configurons le serveur OpenVPN en mode Remote Access (SSL/TLS), permettant aux clients de se connecter de manière sécurisée. Nous définissons l'interface d'écoute sur WAN et utilisons le port standard 1194/UDP. Une clé TLS est activée pour renforcer la sécurité du tunnel VPN



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.

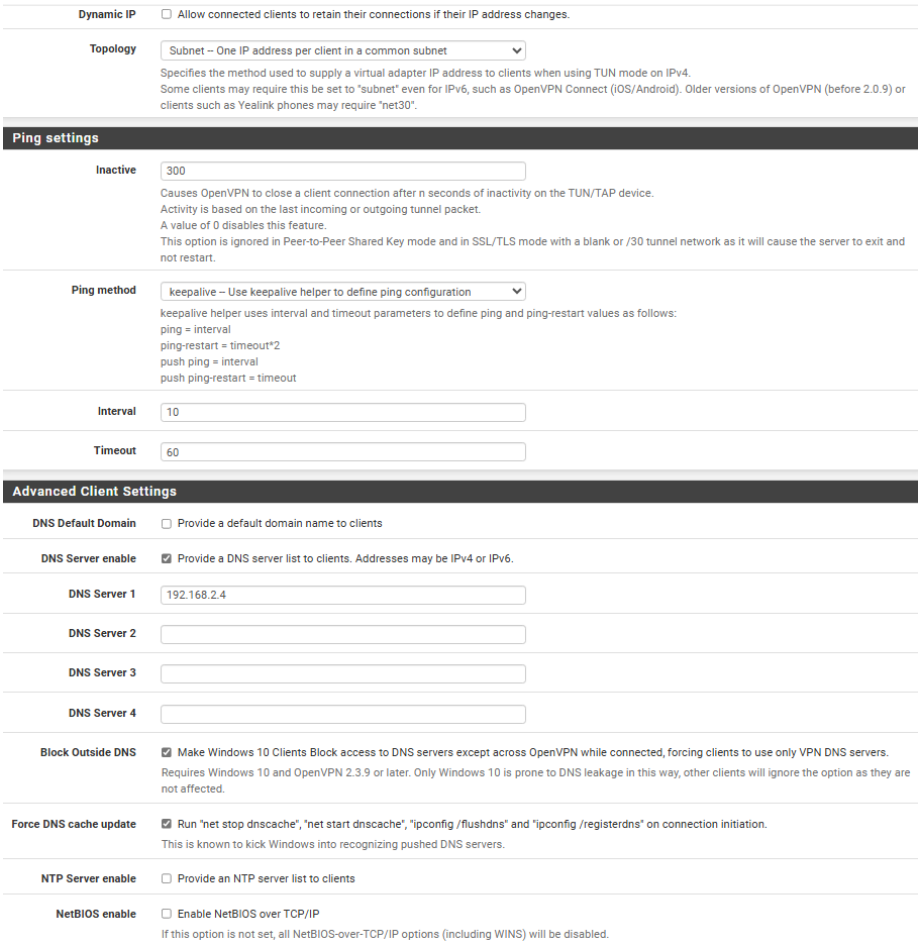


Nous configurons le réseau du tunnel VPN en attribuant une plage d'adresses IP privée 10.0.2.0/24 pour la communication entre le serveur et les clients OpenVPN. Nous activons également l'option de redirection de la passerelle IPv4, afin que tout le trafic des clients passe par le tunnel sécurisé. Le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

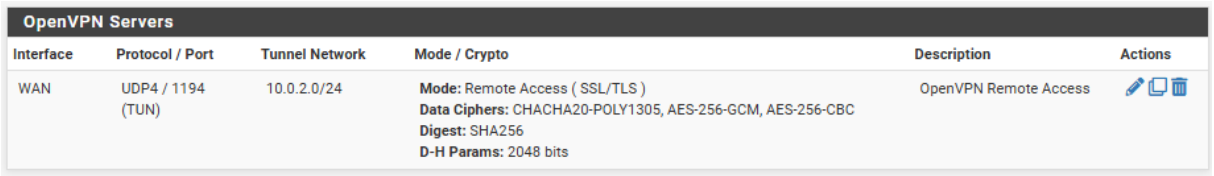


Nous configurons les paramètres avancés des clients OpenVPN pour assurer une connectivité fluide et sécurisée. Nous définissons la topologie du VPN en mode subnet, attribuant une adresse IP distincte à chaque client connecté. Pour améliorer la stabilité, nous utilisons le mode de ping keepalive avec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

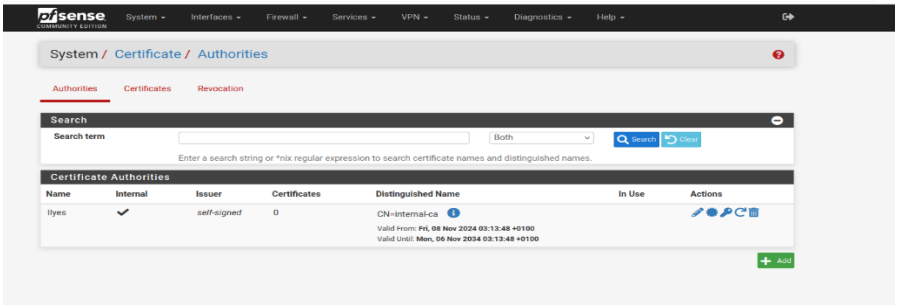
Nous configurons également le serveur DNS interne (192.168.2.4) pour que les clients du VPN puissent résoudre les noms internes du domaine.

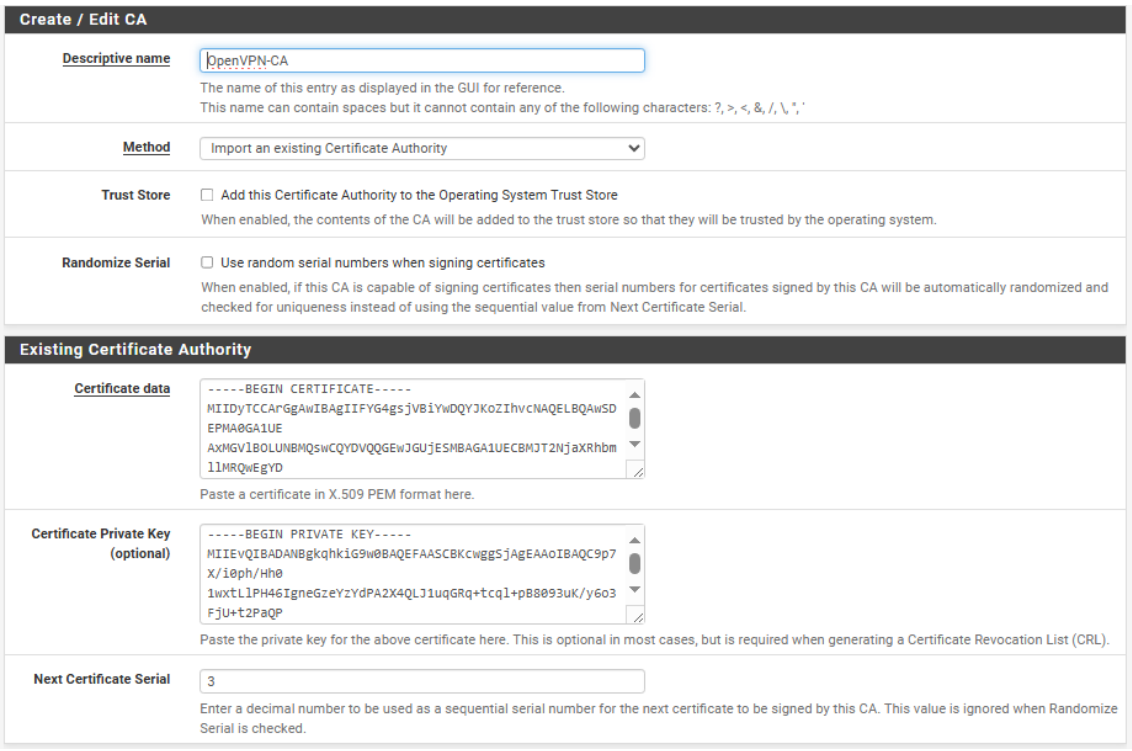


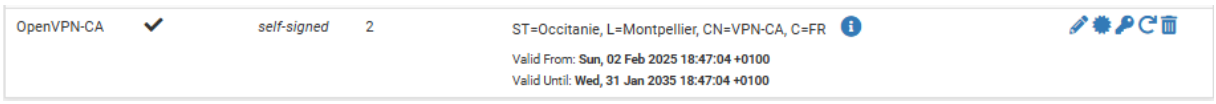
On sauvegarde, et le serveur vpn est configuré.



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





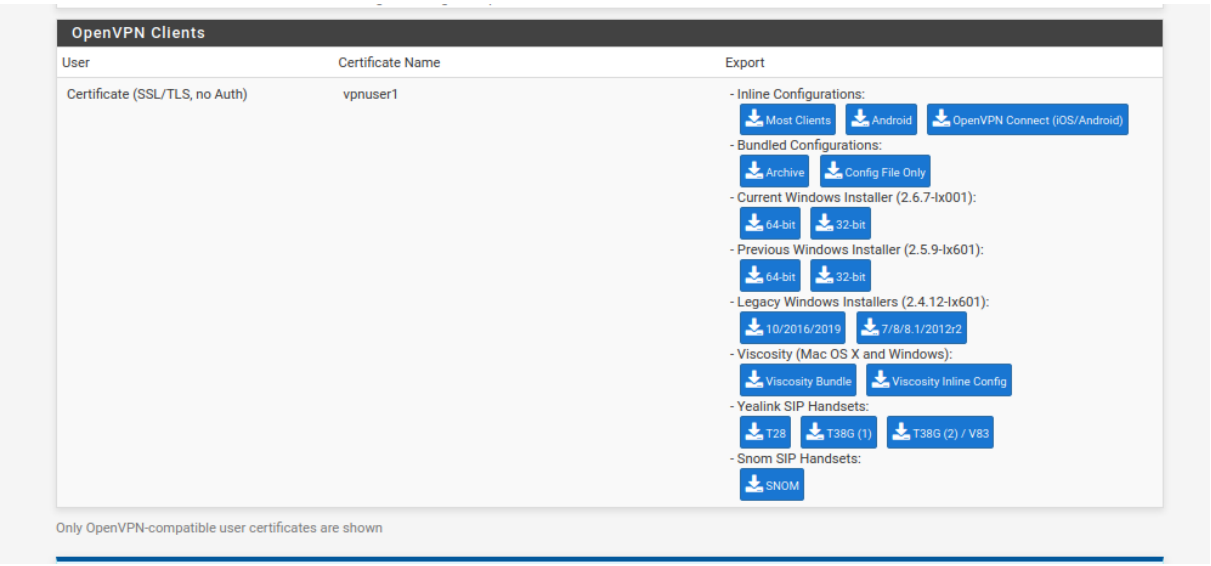


Notre Autorité de Certification OpenVPN a été générée et auto-signée. Elle est valide jusqu'en 2035 et servira à authentifier les connexions VPN en signant les certificats des serveurs et des clients

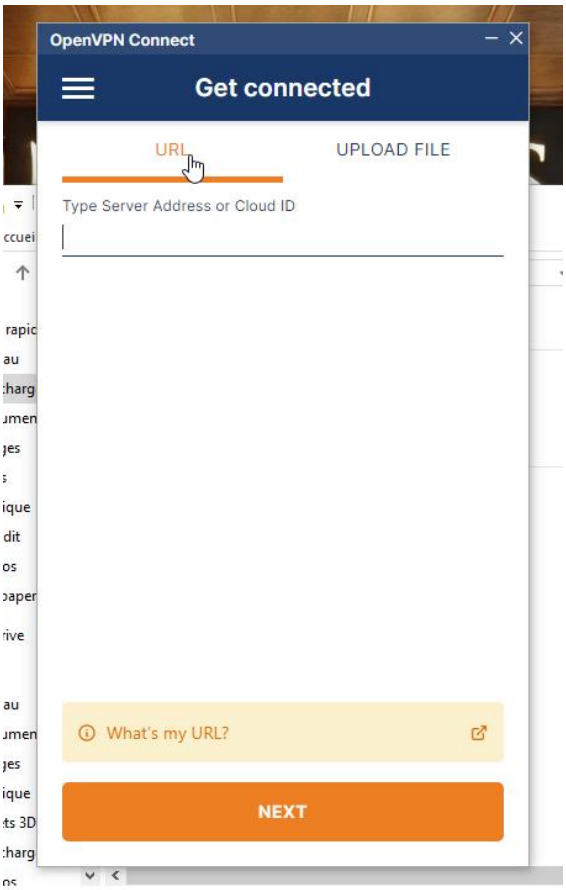
Nous avons généré un certificat serveur OpenVPN, signé par notre Autorité de Certification.

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

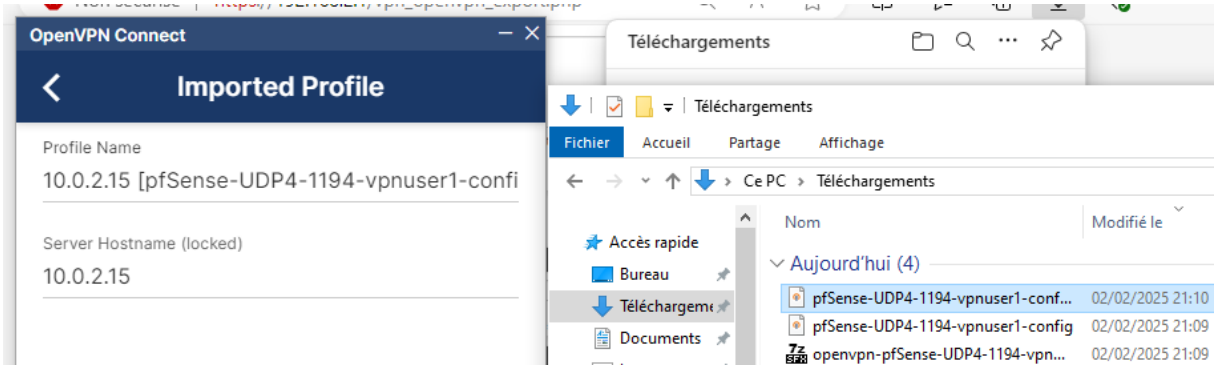
Nous allons exporter le fichier de configuration OpenVPN (.ovpn) pour l'utilisateur vpnuser1. Ce fichier contient toutes les informations nécessaires pour établir une connexion sécurisée au serveur VPN.

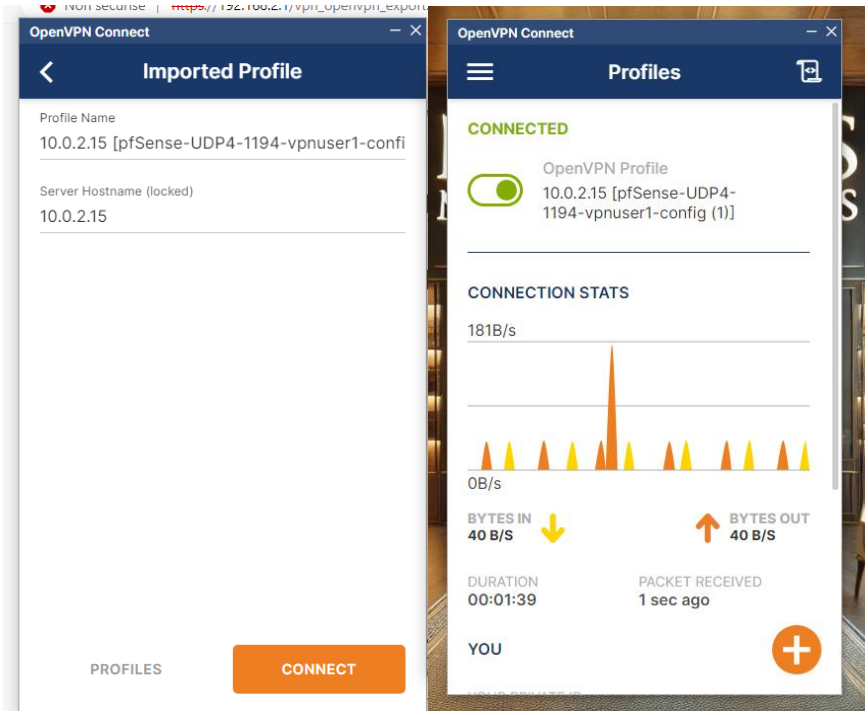


On installe ensuite openVPN sur un poste client pour y intégrer le fichier de configuration précédemment téléchargé.



On importe le profile vpnuser1





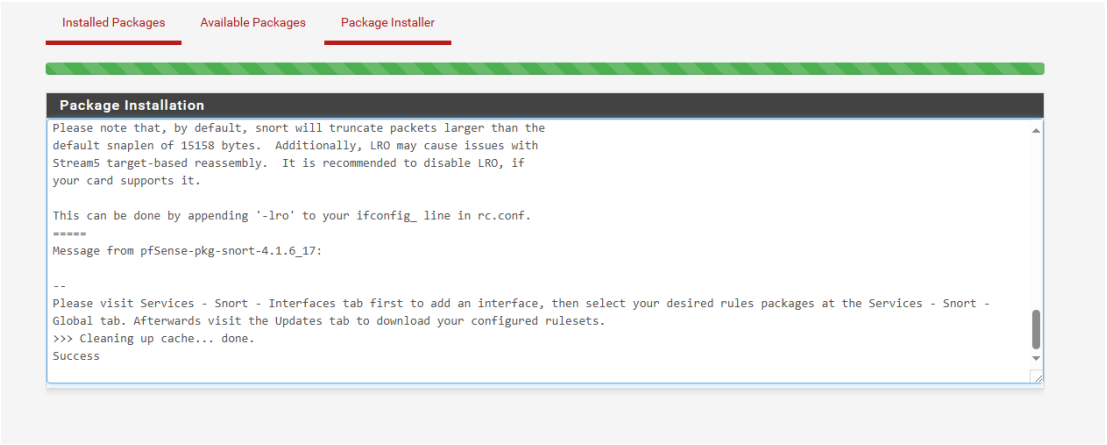
Nous avons importé le fichier de configuration OpenVPN sur le client. Une fois le profil vpnuser1 chargé dans OpenVPN Connect, nous avons initié la connexion au serveur VPN. L'état CONNECTED ainsi que les statistiques de trafic confirment que l'utilisateur est bien connecté et que la communication chiffrée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

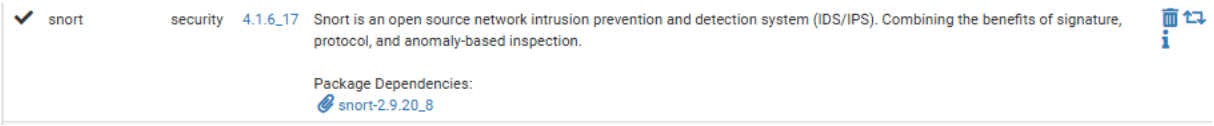
2. Surveillance et sécurité du réseau

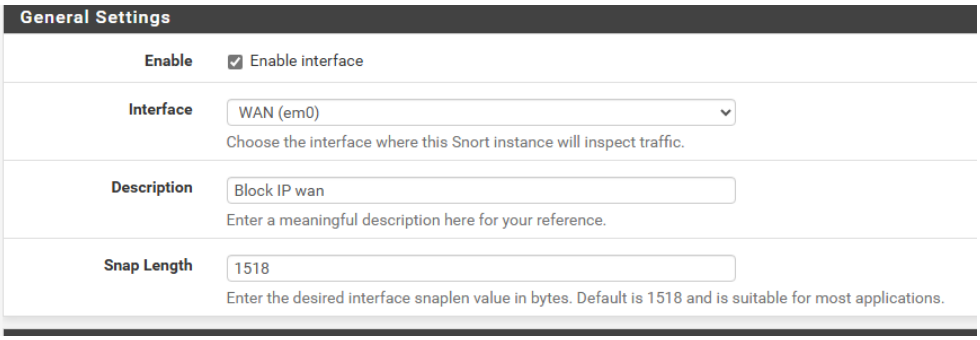
2.1. Système de détection d'intrusion (IDS/IPS)

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

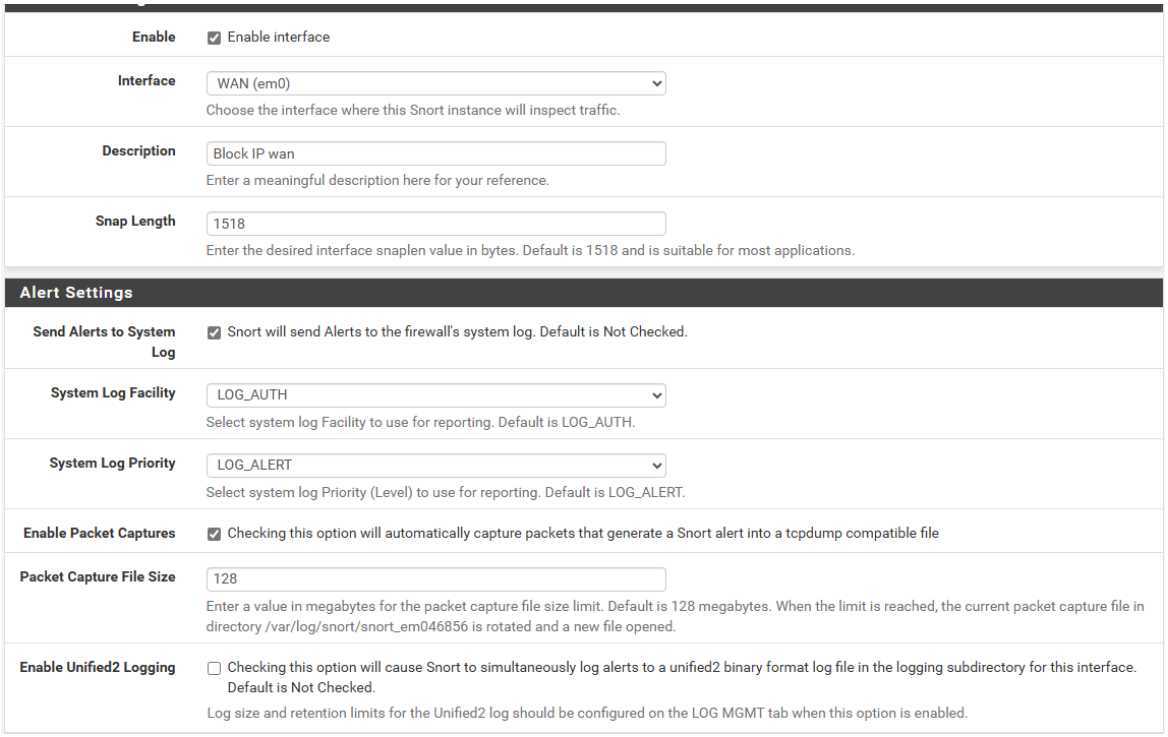
Nous avons installé Snort sur pfSense avec succès. Cette installation nous permet de mettre en place un système de détection et de prévention d'intrusion (IDS/IPS) afin d'analyser le trafic réseau et de détecter d'éventuelles menaces.



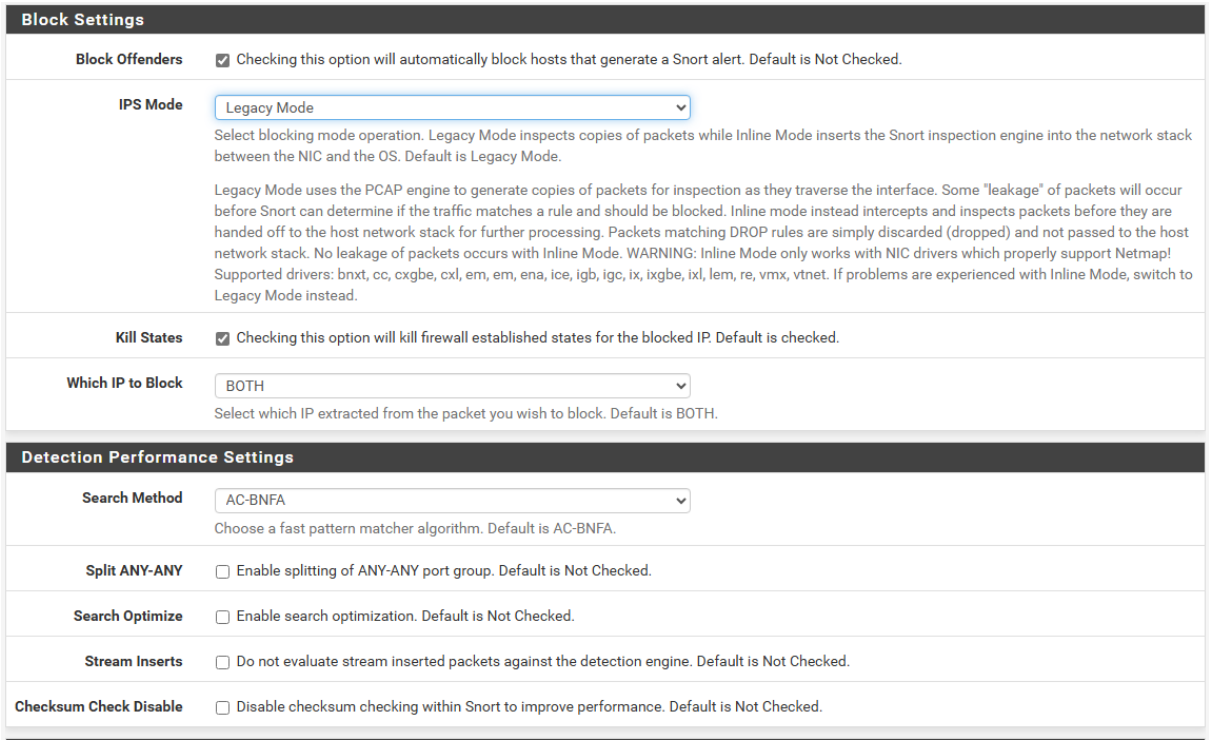




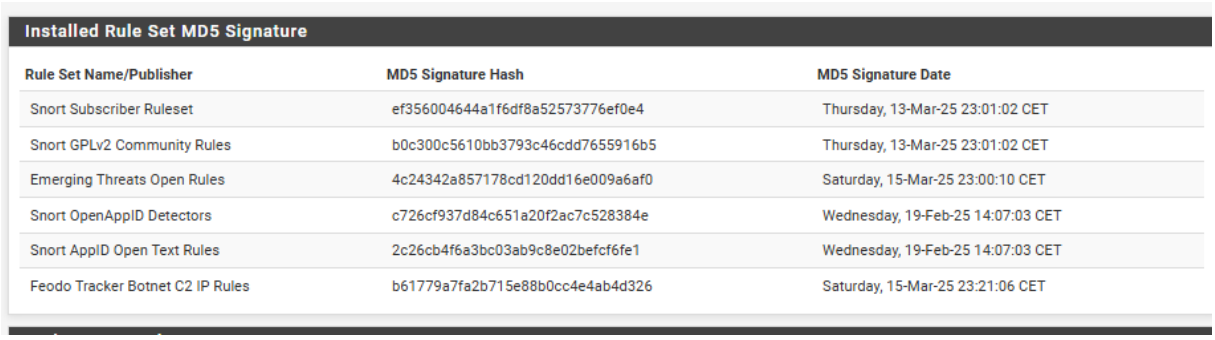
Nous avons activé Snort sur l'interface WAN (em0) et configuré l'envoi d'alertes dans le journal système du pare-feu. Les paquets générant une alerte seront automatiquement capturés et stockés dans un fichier pour analyse.



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.



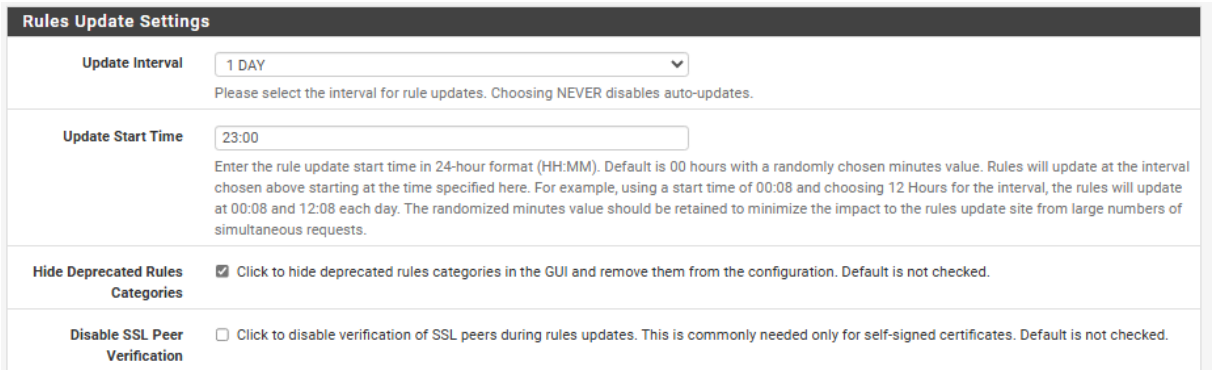
Nous avons mis à jour les règles de détection de Snort, incluant des signatures provenant de plusieurs sources telles que Snort Subscriber Ruleset, Emerging Threats Open Rules et Feodo Tracker Botnet C2 IP Rules. Ces mises à jour permettent d'améliorer la détection des menaces en temps réel et d'optimiser 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 — 1 DAY

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

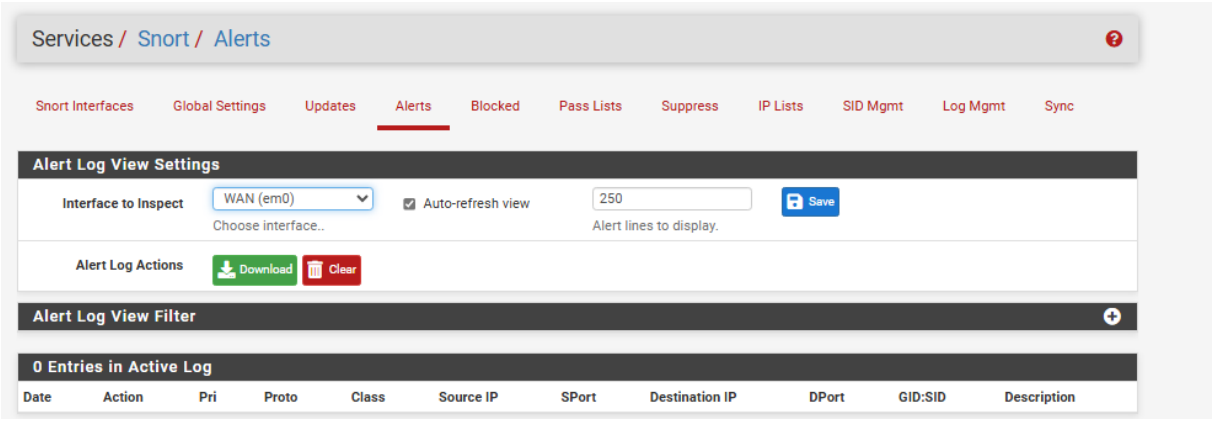
Update Start Time — 23:00

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 — WAN (em0) — Choose interface.. — Auto-refresh view — 250 — Alert lines to display. — Save

Alert Log Actions — Download — Clear

Alert Log View Filter

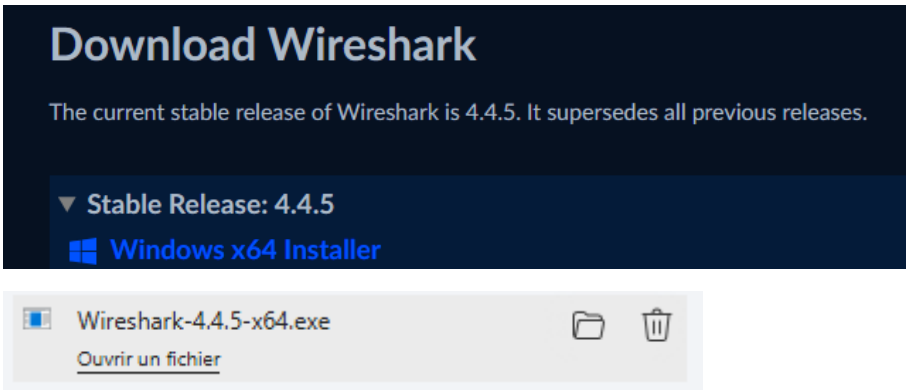
0 Entries in Active Log

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

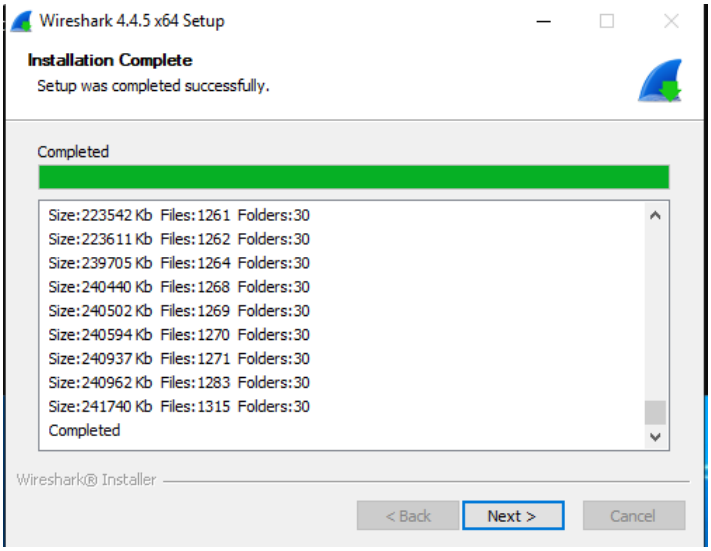
Snort est maintenant configuré avec toutes les règles nécessaires à la surveillance.

2.2. Analyse du trafic avec Wireshark

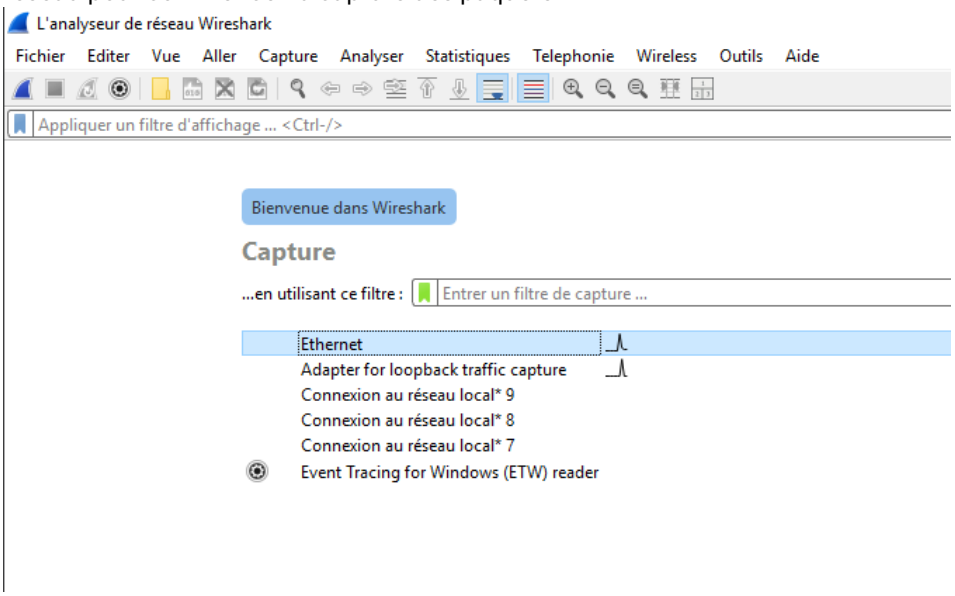
Nous téléchargeons la dernière version stable de Wireshark (4.4.5) pour l'installer sur notre machine d'analyse réseau.



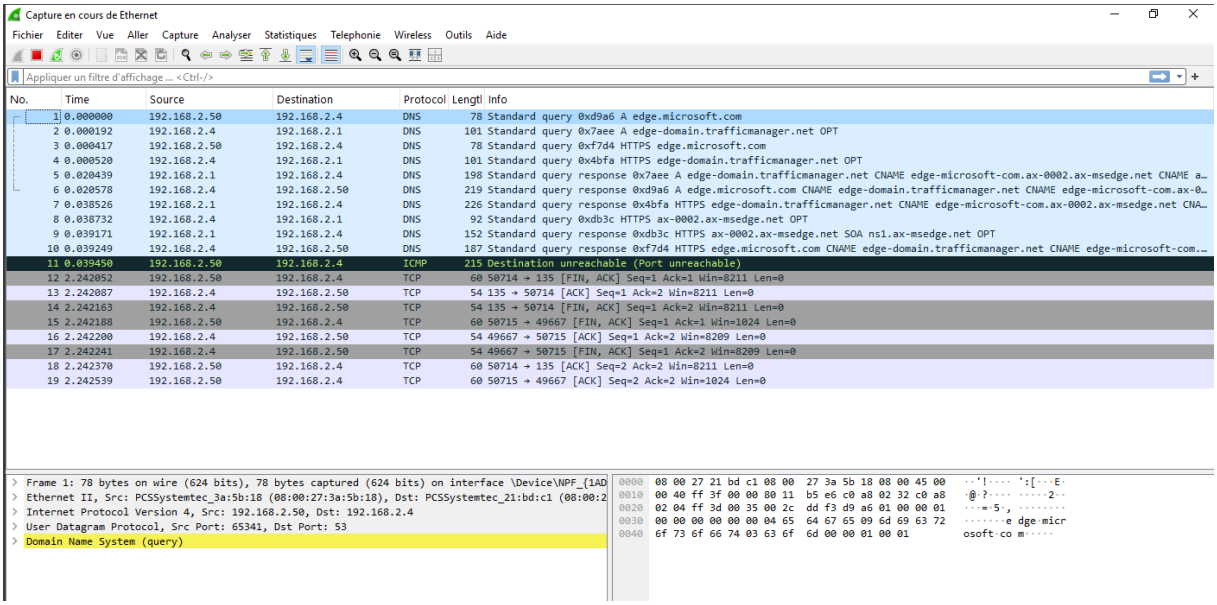
Nous avons installé avec succès Wireshark 4.4.5 sur notre machine, prêt à capturer et analyser le trafic réseau.



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

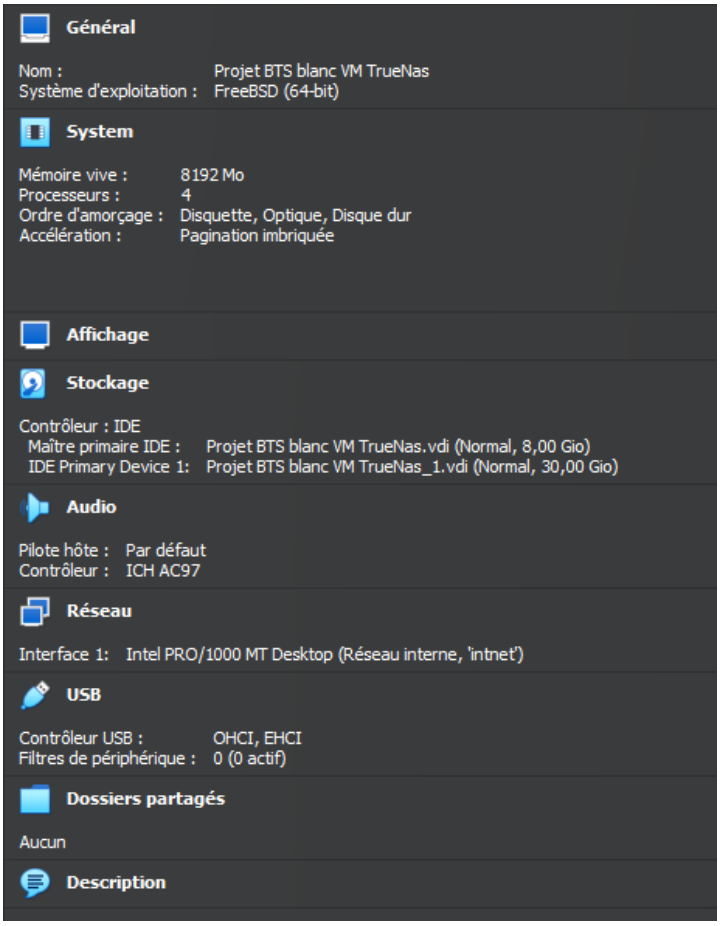


Nous avons capturé et analysé le trafic réseau en temps réel avec Wireshark, cet outil permet d'identifier d'éventuels problèmes de communication et d'analyser les flux réseau en détail.

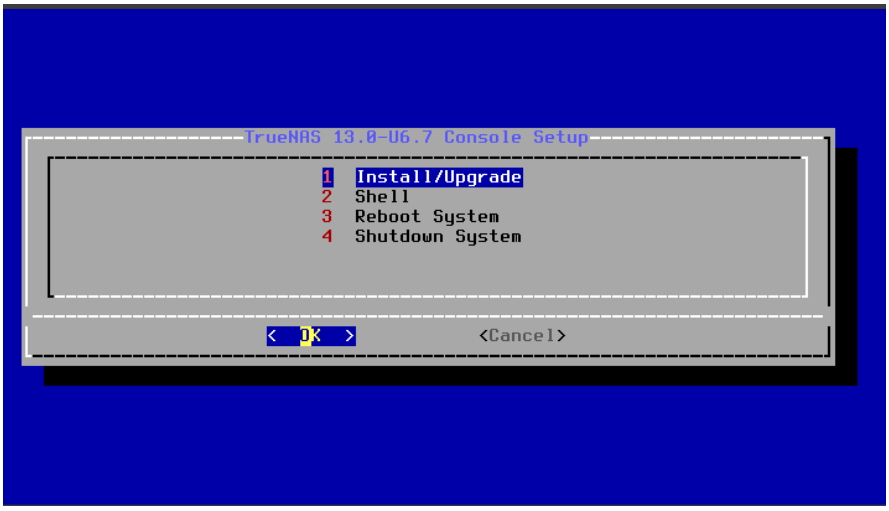
3.1. Infrastructure NAS

- 4.1.1 Configuration nas via TrueNAS

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

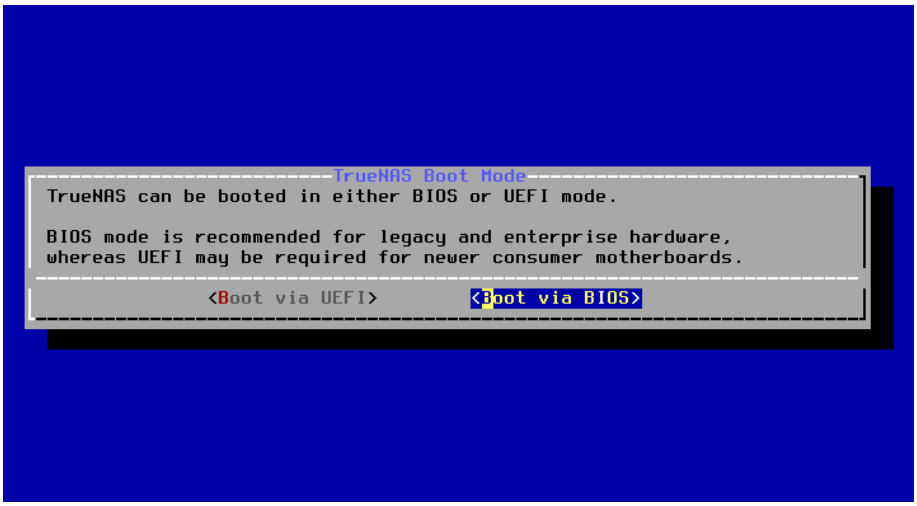


Nous avons démarré l'ISO de TrueNAS sur notre machine virtuelle. L'écran d'installation s'affiche et on sélectionne "Install/Upgrade".

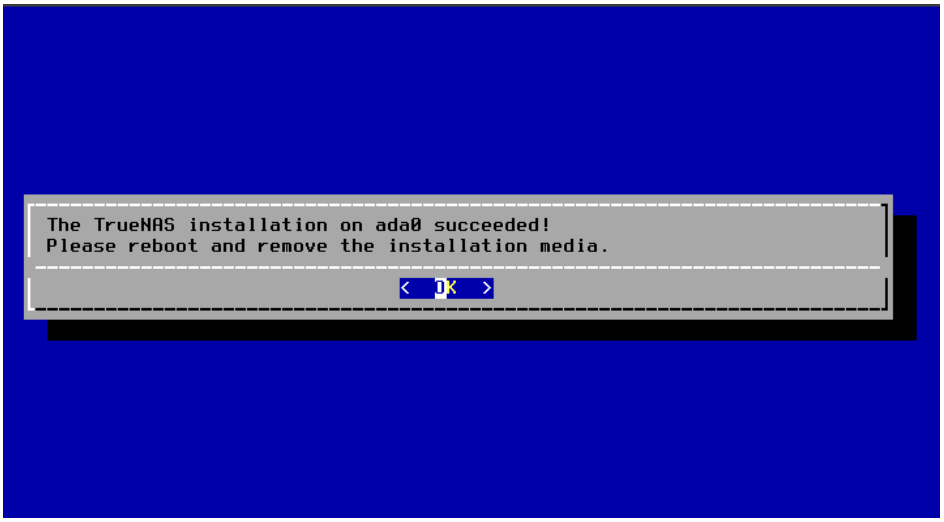


Nous sélectionnons le disque sur lequel TrueNAS sera installé. Nous avons choisi le disque ada0 (8 GiB) afin de réserver le second disque ada1 (30 GiB) pour le stockage des données.

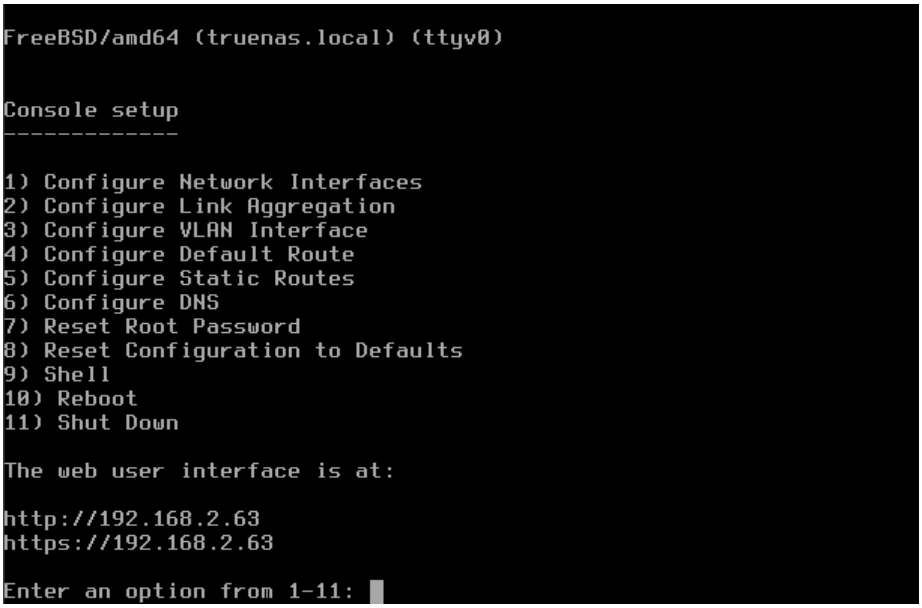
Nous avons sélectionné le mode de démarrage de TrueNAS. Nous avons choisi Boot via BIOS, ce qui est recommandé pour les infrastructures d'entreprise et les environnements legacy. L'option UEFI aurait été préférable pour un matériel plus récent.



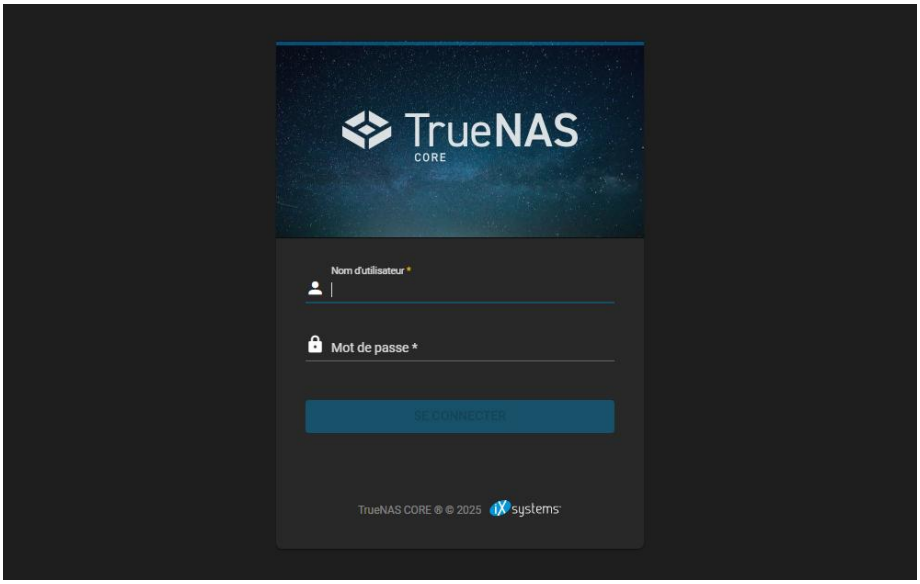
L'installation de **TrueNAS** s'est terminée avec succès. On redémarre la VM et on enlève l'ISO d'installation.



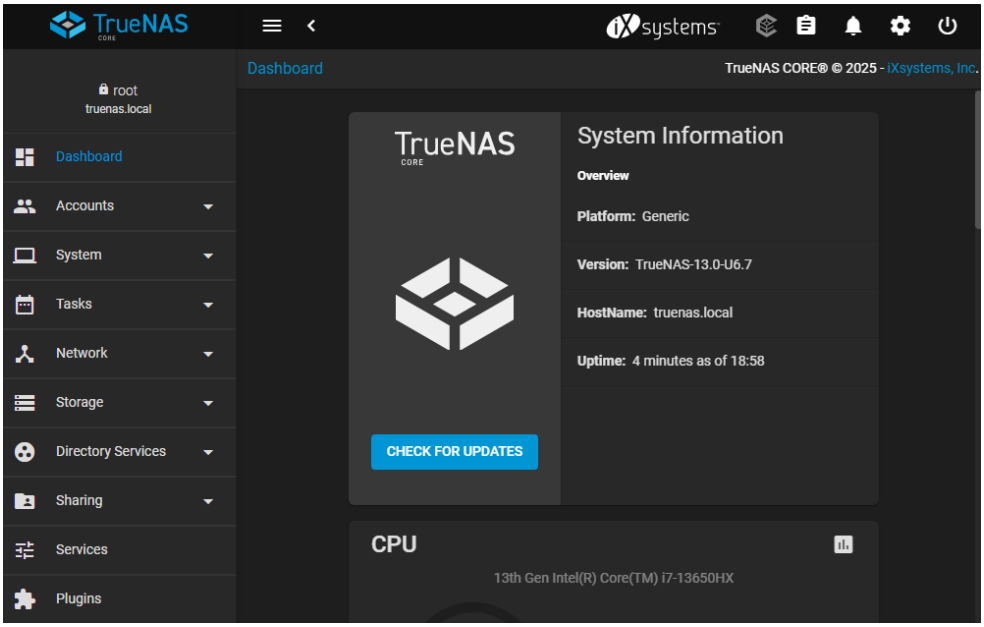
TrueNAS est bien installé et nous avons accès au menu de configuration. L'interface web est disponible à l'adresse 192.168.2.63 fournit grâce au DHCP.



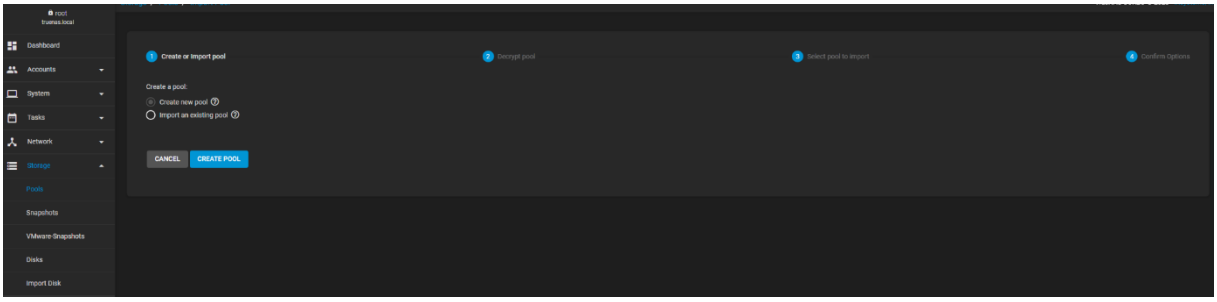
Nous arrivons sur la page de connexion de TrueNAS. Nous allons nous connecter avec l'utilisateur root et le mot de passe défini lors de l'installation.



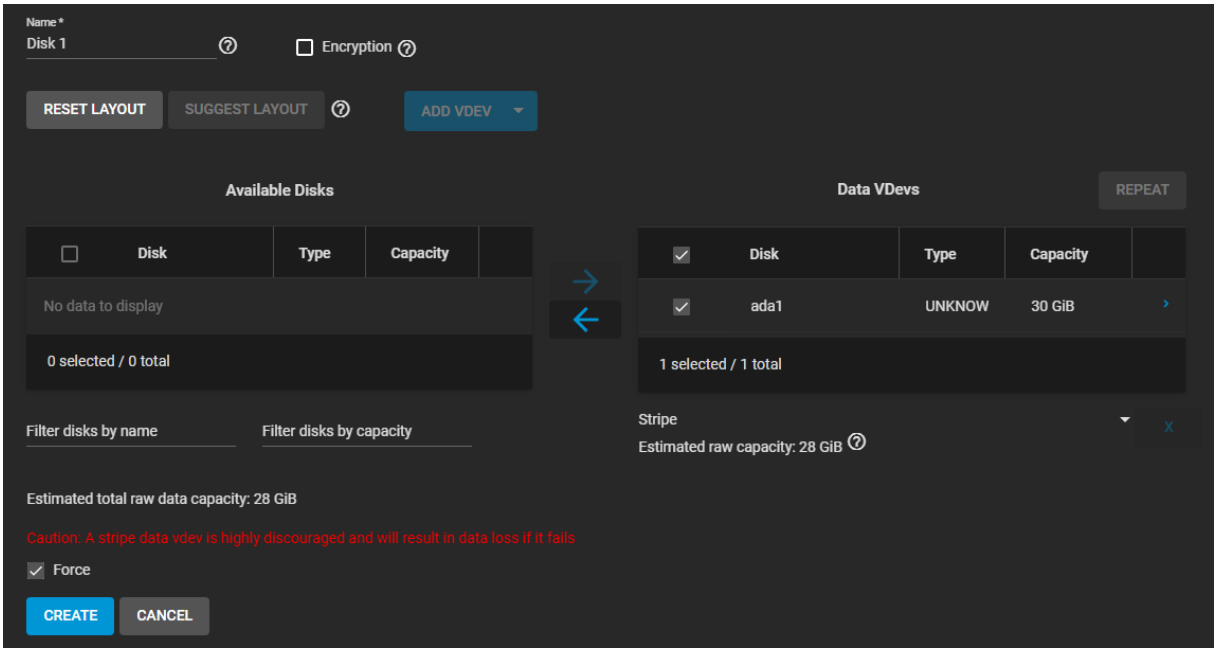
Nous sommes maintenant sur le **tableau de bord** de TrueNAS.



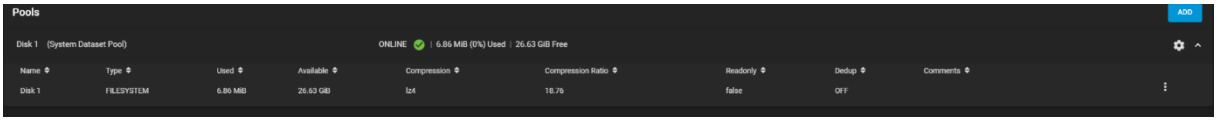
Nous sommes dans la section Pools du stockage. Nous allons créer un nouveau pool pour utiliser notre disque dur disponible.



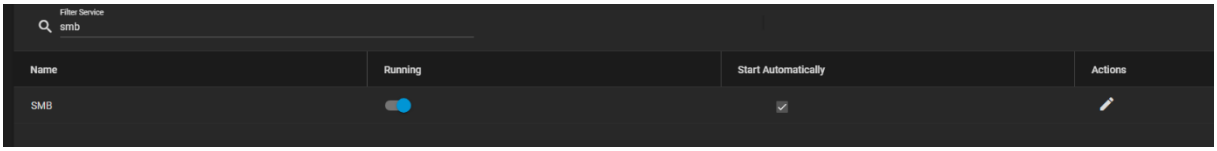
Nous avons sélectionné notre disque de 30 Go (**ada1**) pour créer un pool de stockage en mode **Stripe**.



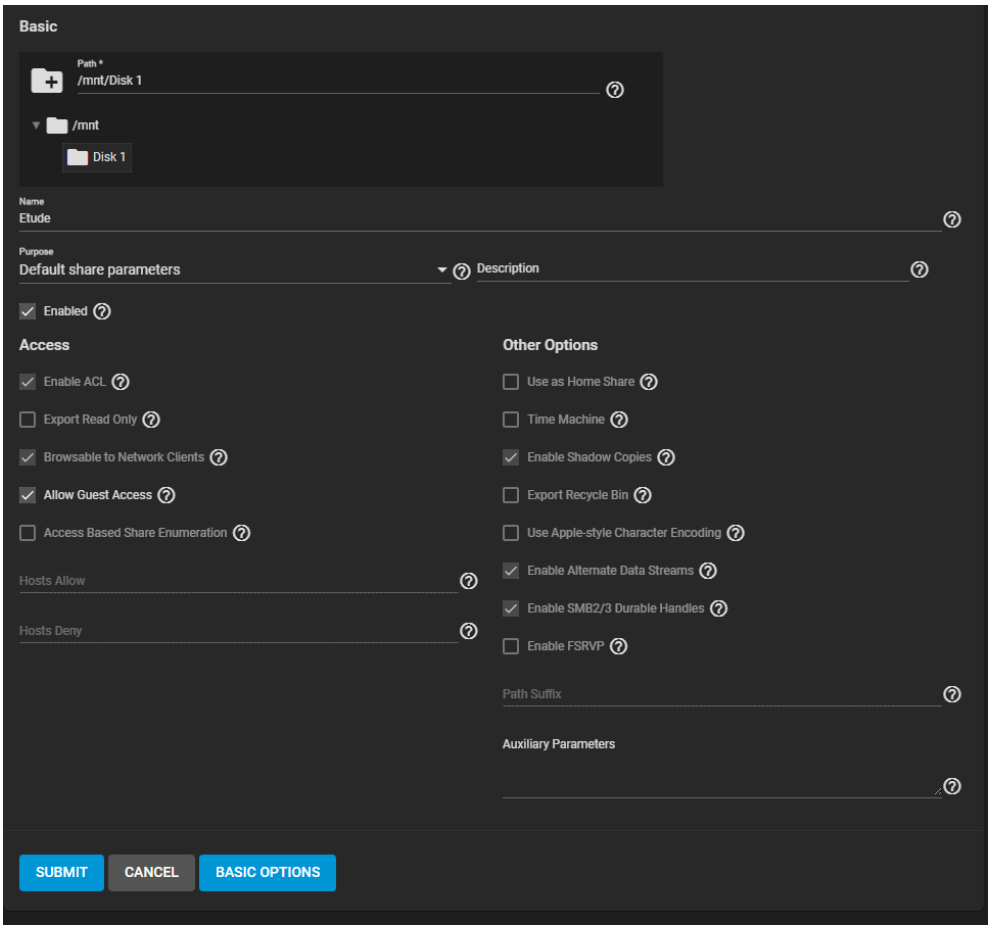
Notre pool Disk 1 est maintenant créé et opérationnel.



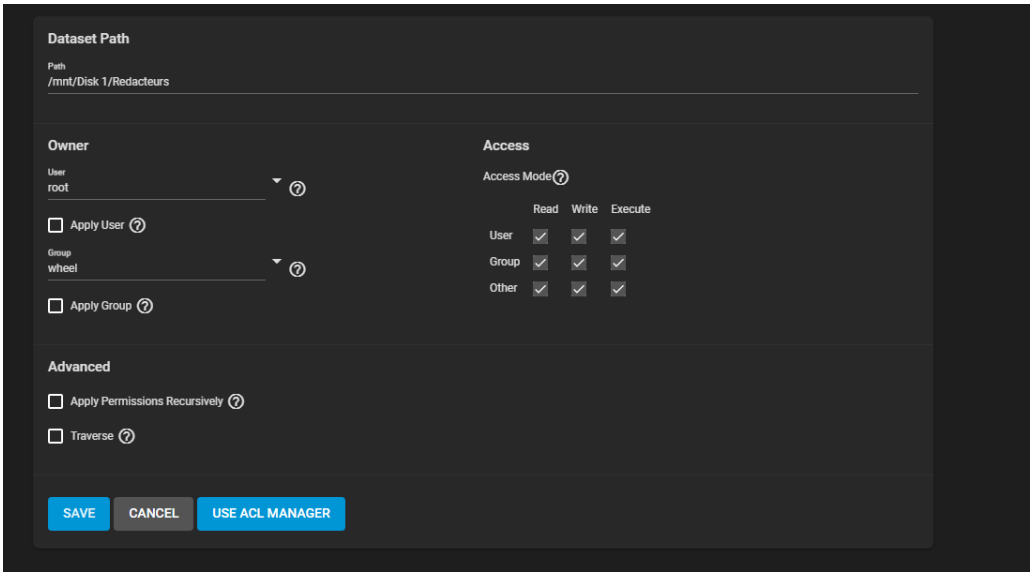
Le service SMB est maintenant activé et configuré pour démarrer automatiquement au boot. Cela nous permettra de partager des fichiers sur le réseau en utilisant le protocole Samba.



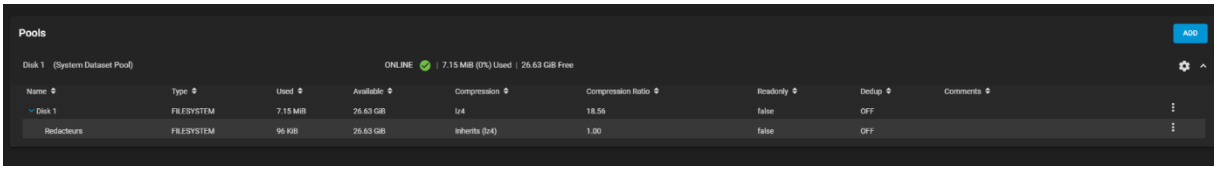
Nous avons créé un partage réseau SMB nommé Étude, pointant vers le disque Disk 1. Ce partage est activé et utilisera les paramètres par défaut.



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



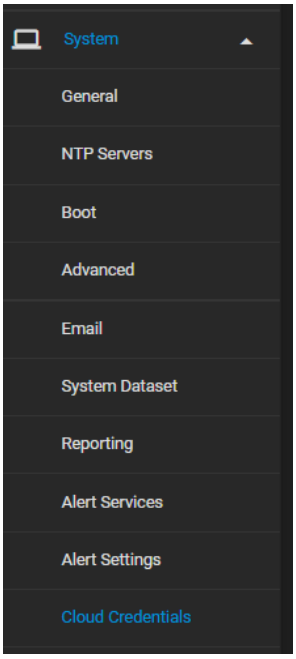
Nous avons ajouté le dataset Rédacteurs au pool Disk 1, permettant d'organiser le stockage en sous-volumes distincts. Ce dataset hérite de la compression lz4 et est opérationnel.



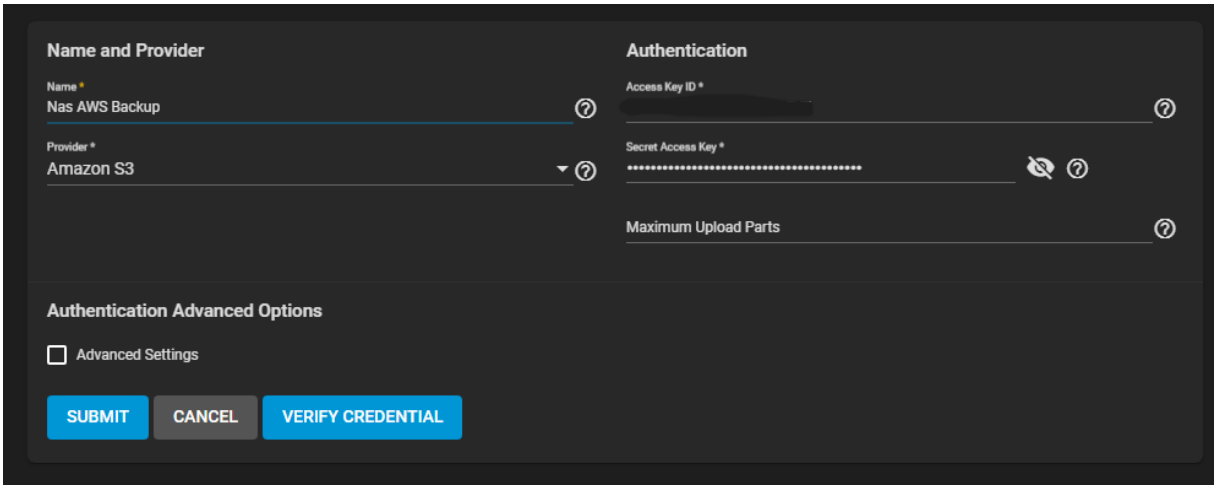
Maintenant que tout est en place, les collaborateurs pourront accéder au stockage via l'explorateur de fichier en tapant \\192.168.2.63

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

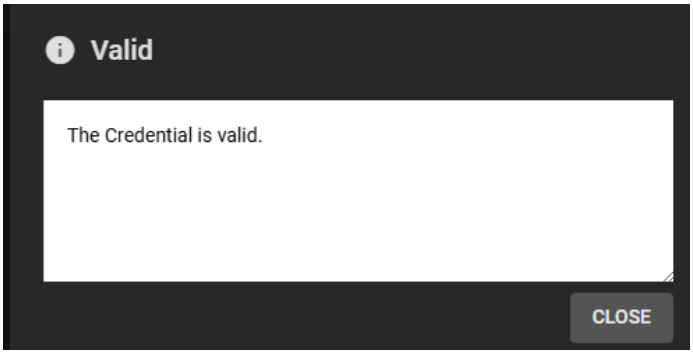
Maintenant nous accédons à Cloud Credentials pour configurer notre sauvegarde sur AWS



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

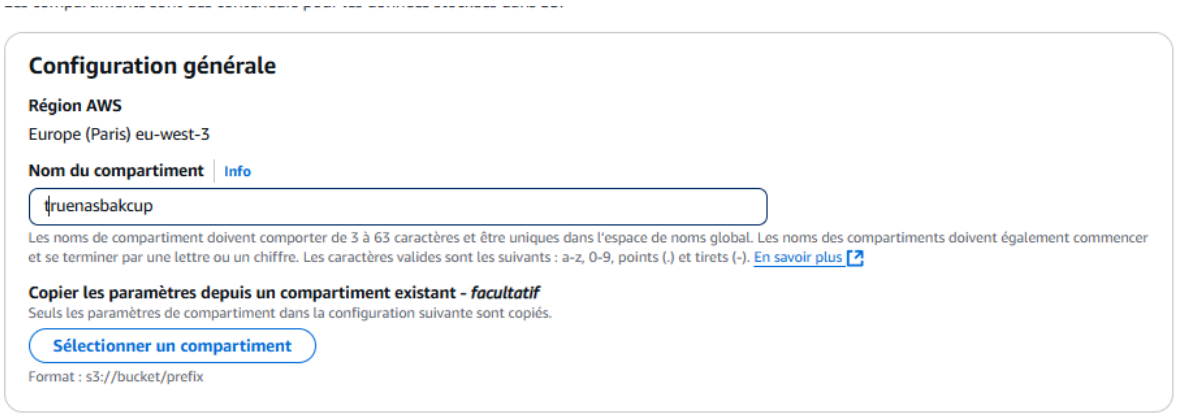


Nos identifiants AWS ont été validés avec succès. Nous pouvons maintenant configurer la sauvegarde automatique de notre NAS vers Amazon S3.

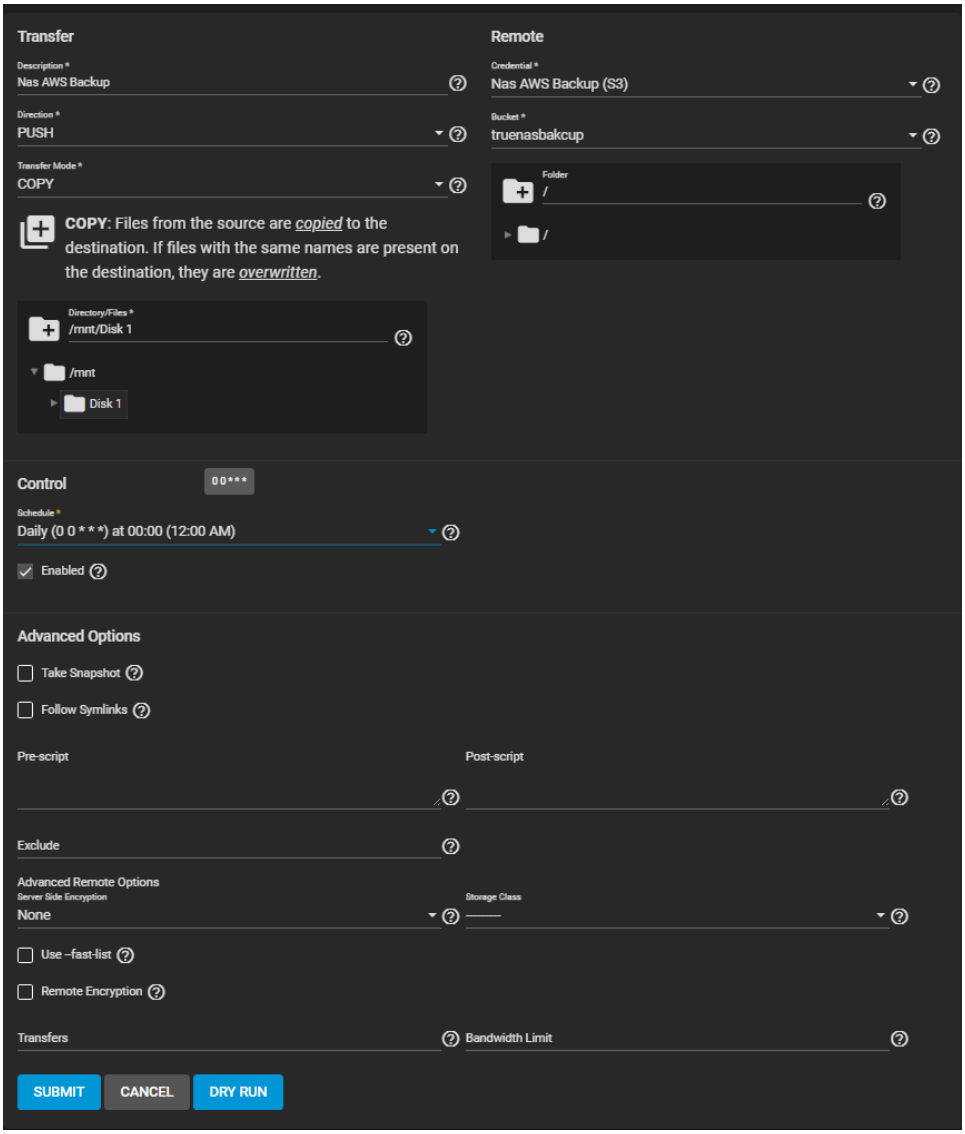


Tout d'abord nous allons nous rendre sur la console administrateur AWS et créer un **compartiment S3** nommé **"truenasbackup".**

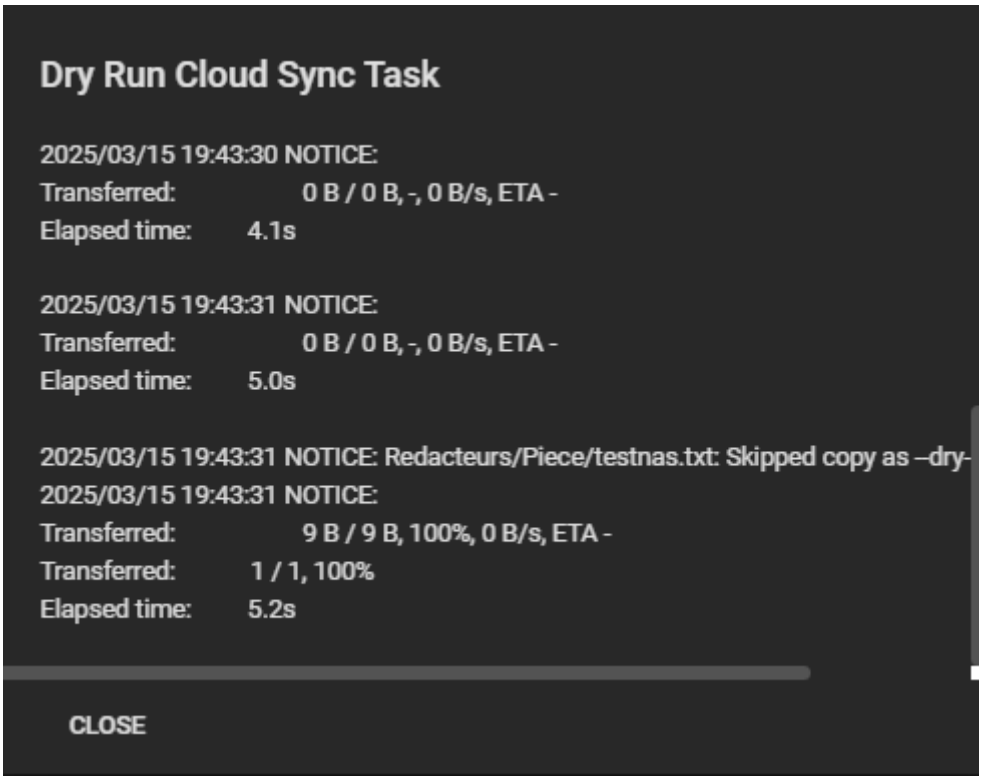
Ce compartiment servira à stocker les sauvegardes de notre TrueNAS.



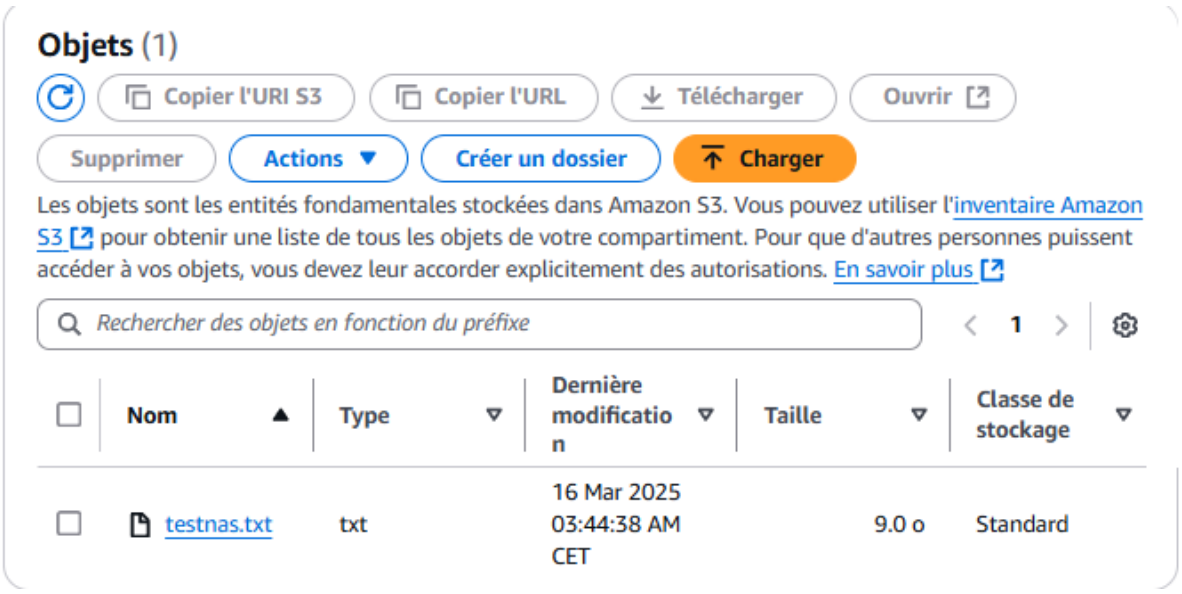
Nous avons configuré une tâche de synchronisation Cloud Sync pour envoyer (PUSH) les fichiers de /mnt/Disk 1 vers notre compartiment S3 "truenasbackup". La synchronisation se fera quotidiennement à minuit en mode COPY, ce qui garantit que les fichiers du NAS seront copiés sur AWS sans suppression des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

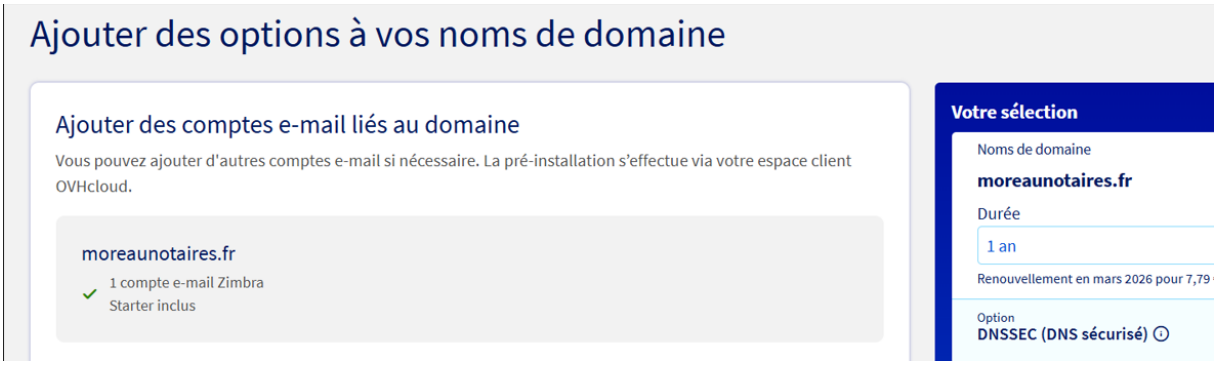


Le fichier **testnas.txt** est bien présent dans le compartiment configuré, confirmant que la synchronisation entre **TrueNAS et AWS** fonctionne correctement.



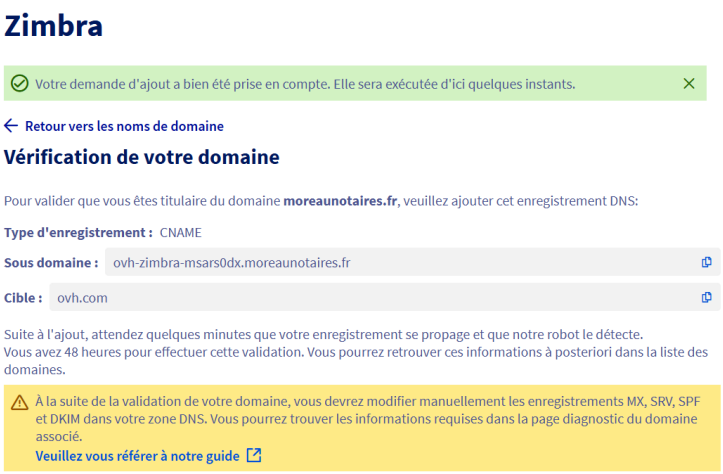
5/ Messagerie d’entreprise avec Zimbra

Je possède le nom de domaine moreaunotaires.fr

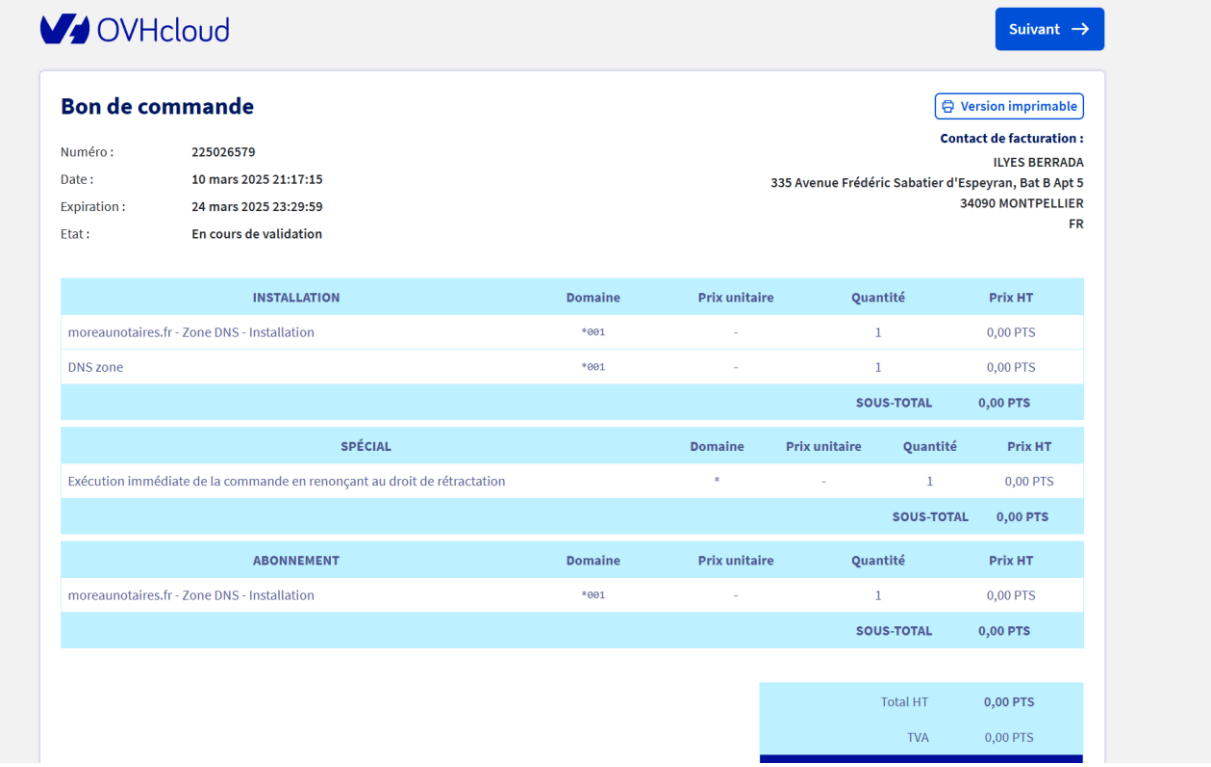


Activation d’un compte Zimbra lié au domaine moreaunotaires.fr via OVH.

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



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



OVHcloud

Suivant →

Bon de commande

Version imprimable

Numéro : 225026579
Date : 10 mars 2025 21:17:15
Expiration : 24 mars 2025 23:29:59
Etat : En cours de validation

Contact de facturation :
ILYES BERRADA
335 Avenue Frédéric Sabatier d'Espeyran, Bat B Apt 5
34090 MONTPELLIER
FR

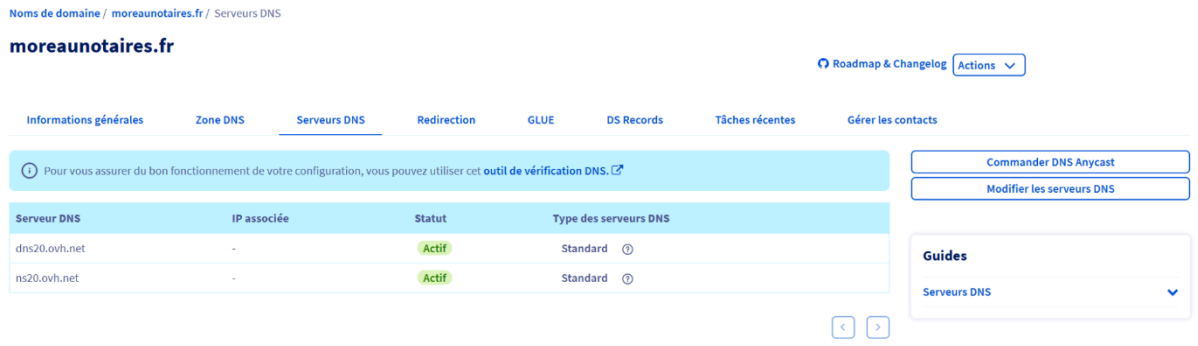
INSTALLATION	Domaine	Prix unitaire	Quantité	Prix HT
moreaunotaires.fr - Zone DNS - Installation	*001	-	1	0,00 PTS
DNS zone	*001	-	1	0,00 PTS
			SOUS-TOTAL	0,00 PTS

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

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

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.

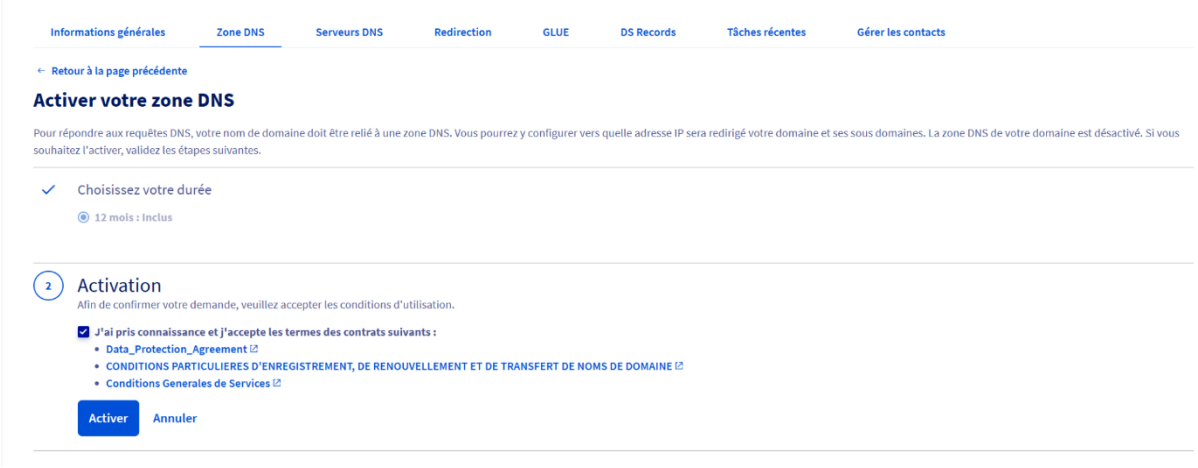
Commander DNS Anycast
Modifier les serveurs DNS

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

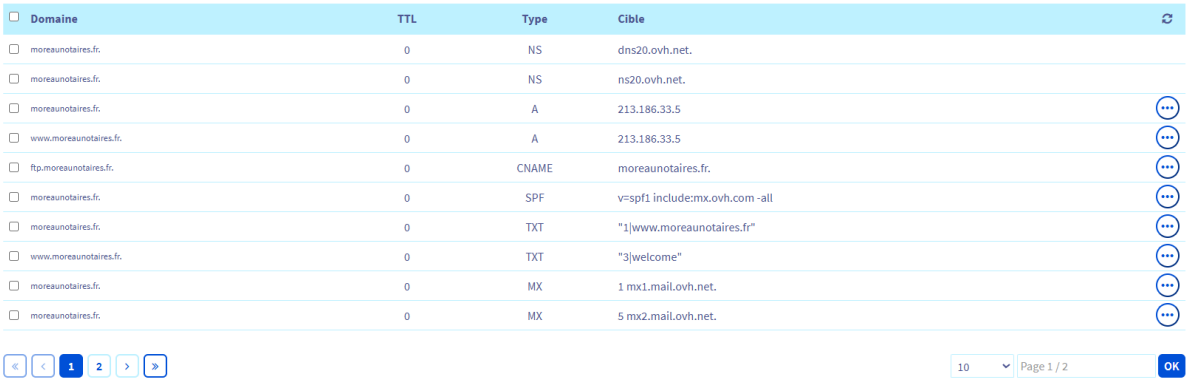
Guides

Serveurs DNS

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

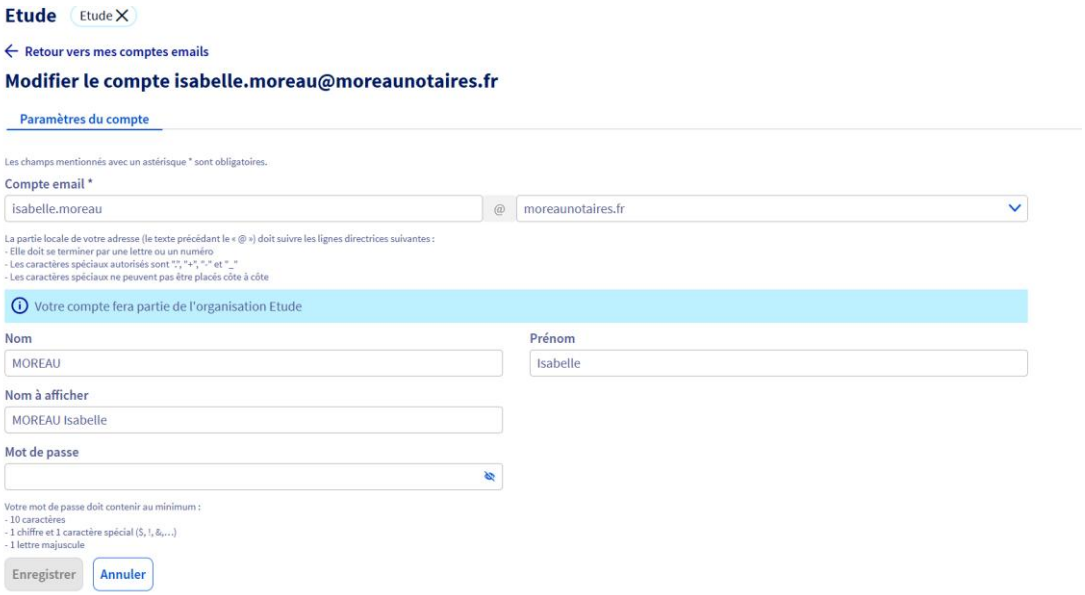


Nous avons configuré les enregistrements DNS nécessaires (A, MX, SPF, TXT, CNAME) pour assurer le bon fonctionnement du domaine moreaunotaires.fr avec la messagerie et le site.

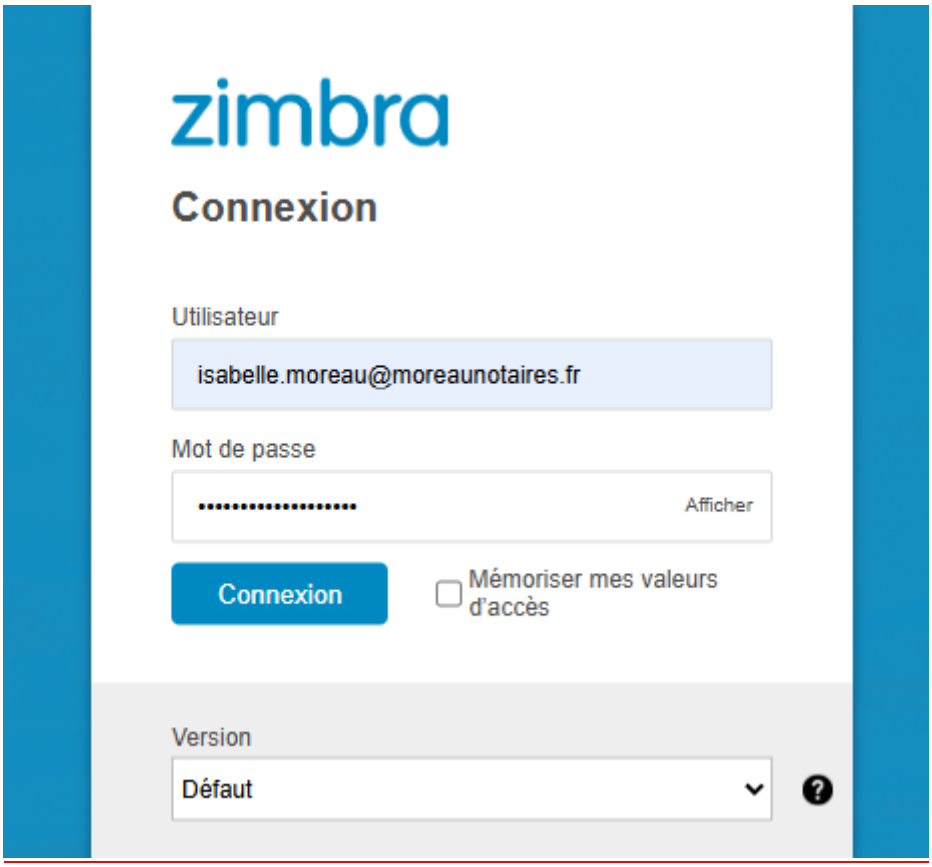


Nous avons associé le domaine moreaunotaires.fr à l'organisation "Étude" et confirmé que le statut du service Zimbra est "READY".

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



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



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 procèderons 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

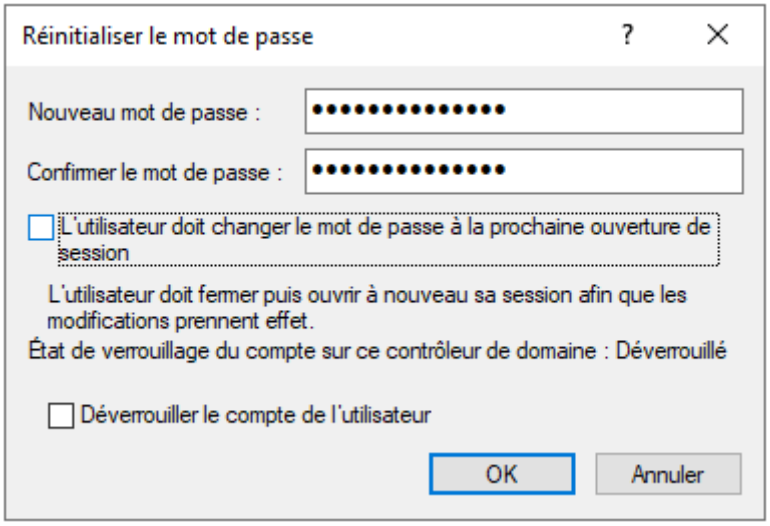
4.1. Infrastructure NAS avec TrueNAS

1. Redondance Active Directory et DNS

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

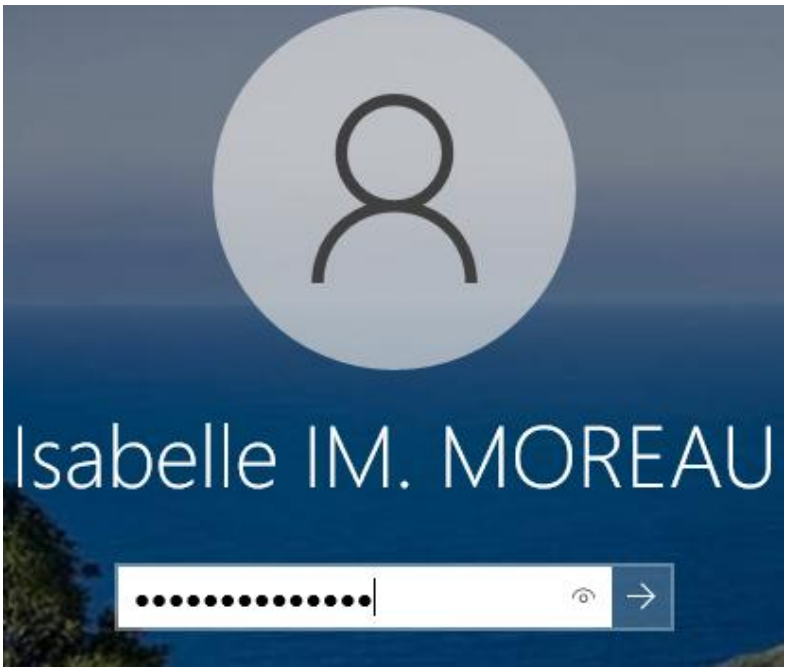
```
C:\Users\i.moreau>nslookup technovalis.local 192.168.2.6
Serveur :   SRVBACKUP.technovalis.local
Address:  192.168.2.6

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.

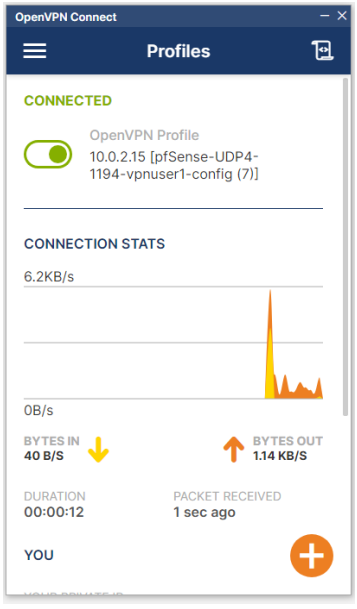


2. VPN Sécurisé avec OpenVPN

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.

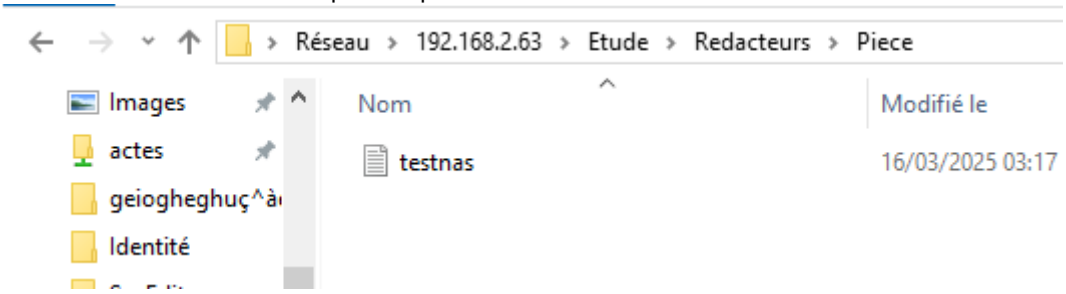
La trame icmp du ping remonte bien.

```
└  68 8.190140    192.168.2.50    192.168.2.4    ICMP    101 Destination unreachable (Port unreachable)
```

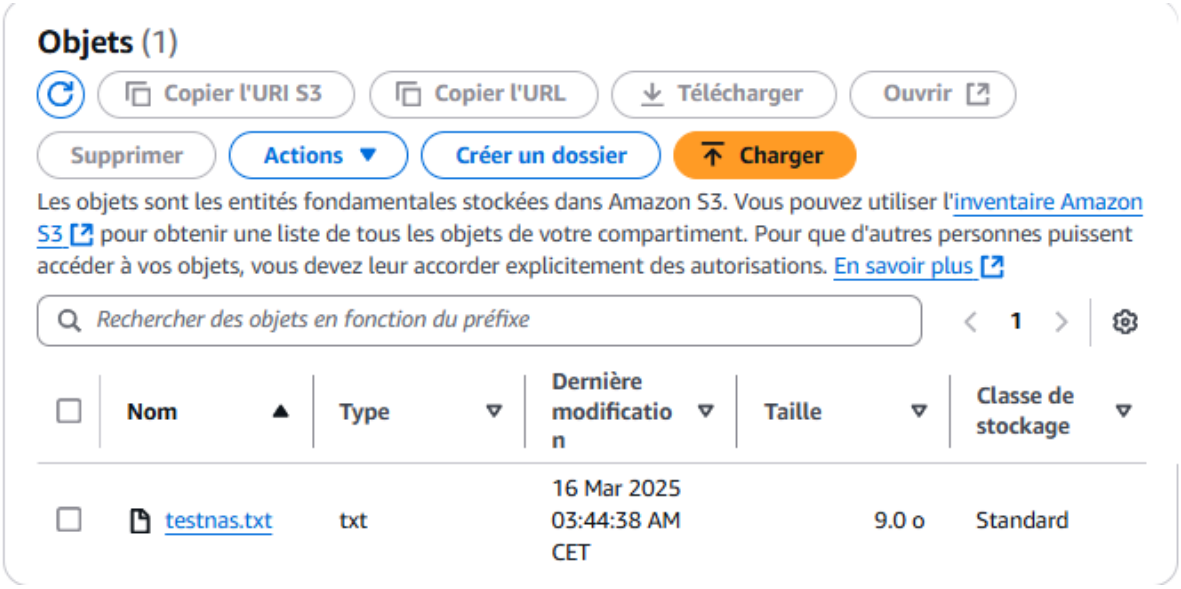
3. Infrastructure NAS avec TrueNAS

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

On a bien accès au server 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.