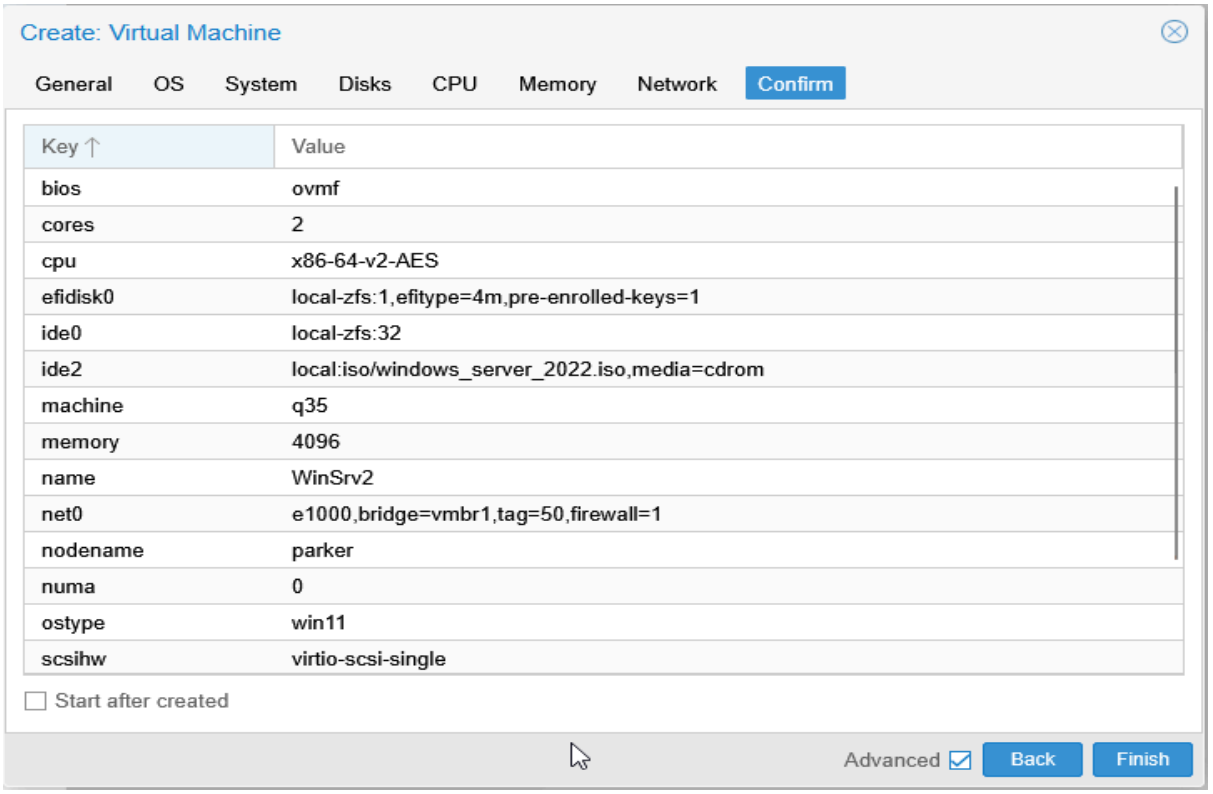
SOMMAIRE

I. Haute Disponibilité et Services Windows

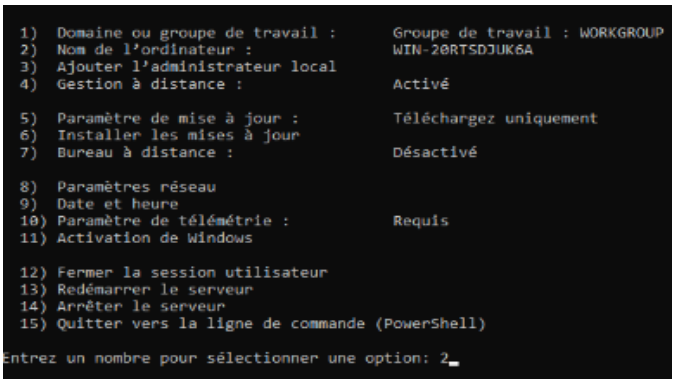
- Configuration d'un second serveur AD/DNS/DHCP pour la redondance

Redondance Windows Server ADDS/DNS/DHCP

Création de la VM :



Pour l’installation voir l’installation du serveur main
Changement du nom :



```
Nom de l'ordinateur actuel : WIN-20RTSDJUK6A

Entrer un nouveau nom d'ordinateur (Vide = annuler): WinSrv2
```

Paramètres réseau :

```
---------------------------------------------------------------------------
            Bienvenue dans Windows Server 2022 Standard Evaluation
---------------------------------------------------------------------------

  1)  Domaine ou groupe de travail :      Groupe de travail : WORKGROUP
  2)  Nom de l'ordinateur :               WINSRV2
  3)  Ajouter l'administrateur local
  4)  Gestion à distance :                Activé

  5)  Paramètre de mise à jour :          Téléchargez uniquement
  6)  Installer les mises à jour
  7)  Bureau à distance :                 Désactivé

  8)  Paramètres réseau
  9)  Date et heure
  10) Paramètre de télémétrie :           Requis
  11) Activation de Windows

  12) Fermer la session utilisateur
  13) Redémarrer le serveur
  14) Arrêter le serveur
  15) Quitter vers la ligne de commande (PowerShell)

Entrez un nombre pour sélectionner une option: 8
```

```
Cartes réseau disponibles :

Index numéro | Adresse IP      | Description
1            | 192.168.50.2    | Intel(R) PRO/1000 MT Network Connection

Sélectionnez le numéro d'index de la carte réseau (Vide = annuler): 1
```

```
Index NIC :             1
Description :           Intel(R) PRO/1000 MT Network Connection
Adresse IP :            192.168.50.2,
                        fe80::e978:3402:b9de:6068
Masque de sous-réseau : 255.255.255.224
DHCP activé :           True

Passerelle par défaut :  192.168.50.1
Serveur DNS préféré :
Serveur DNS auxiliaire :

  1) Définir l'adresse de la carte réseau
  2) Définir les serveurs DNS
  3) Effacer les paramètres du serveur DNS

Entrez la sélection (Vide = annuler): 1
```

```
Entrez la sélection (Vide = annuler): 1
Sélectionnez le protocole (D)HCP ou l'adresse IP (S)tatique (Vide = annuler): S
Entrer une adresse IP statique : (Vide = annuler): 192.168.50.11
Entrer un masque de sous-réseau (Vide=255.255.255.0): 255.255.255.224
Entrez la passerelle par défaut (Vide = annuler): 192.168.50.1
```

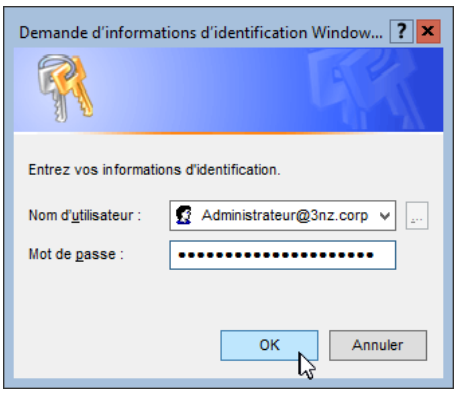
Assignation des serveurs DNS :

```
Passerelle par défaut :  192.168.50.1
Serveur DNS préféré :
Serveur DNS auxiliaire :

  1) Définir l'adresse de la carte réseau
  2) Définir les serveurs DNS
  3) Effacer les paramètres du serveur DNS

Entrez la sélection (Vide = annuler): 2
```

```
Entrez la sélection (Vide = annuler): 2
Entrer un nouveau serveur DNS préféré (Vide = annuler): 192.168.50.10
Entrer un autre serveur DNS (vide=aucun): 192.168.50.11
Le ou les serveurs DNS ont été assignés.
```

Mise en redondance :
Installer les outils de gestion AD :
Install-WindowsFeature -Name AD-Domain-Services

Promouvoir le serveur en tant que contrôleur secondaire :
Install-ADDSDomainController -DomainName "3nz.corp" -InstallDns -Credential (Get-Credential) -SafeModeAdministratorPassword (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -Force)

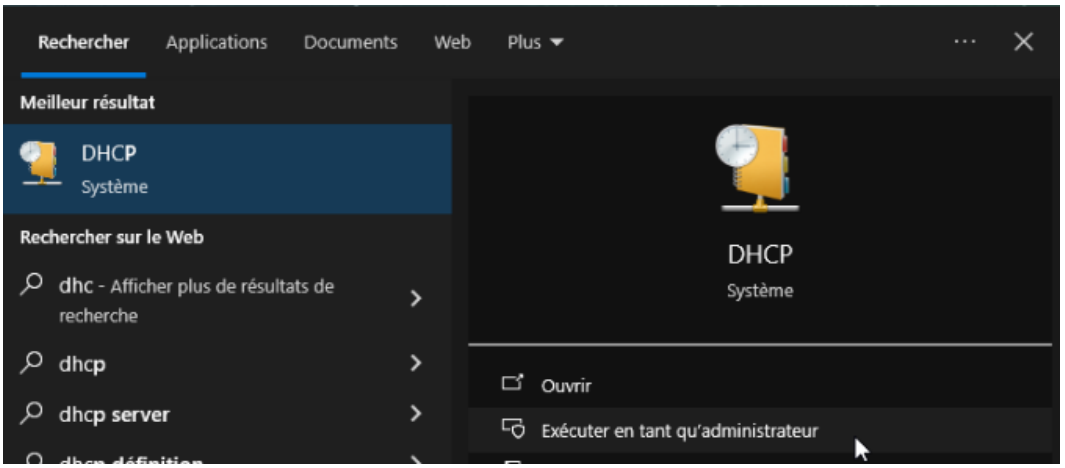


- Mise en place du DHCP Failover pour la haute disponibilité

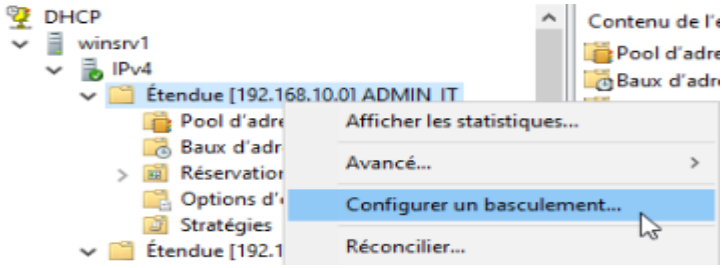
Redondance DHCP (DHCP Failover) :
Installation de l'outil RSAT DHCP sur une machine cliente avec droit Administrateur :

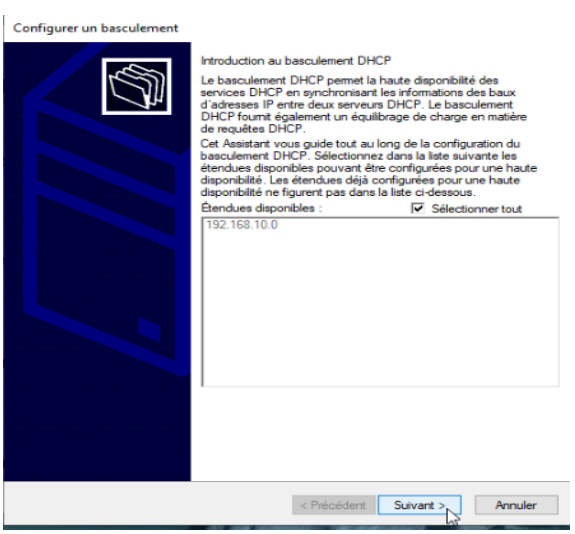
```
PS C:\Windows\system32> Add-WindowsCapability -Online -Name Rsat.DHCP.Tools~~~~0.0.1.0
```

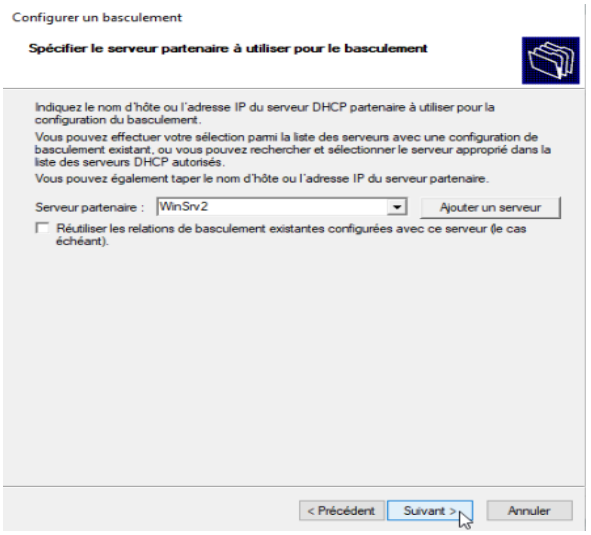
Tapez DHCP dans la barre de recherche, ouvrir en tant qu'Administrateur :

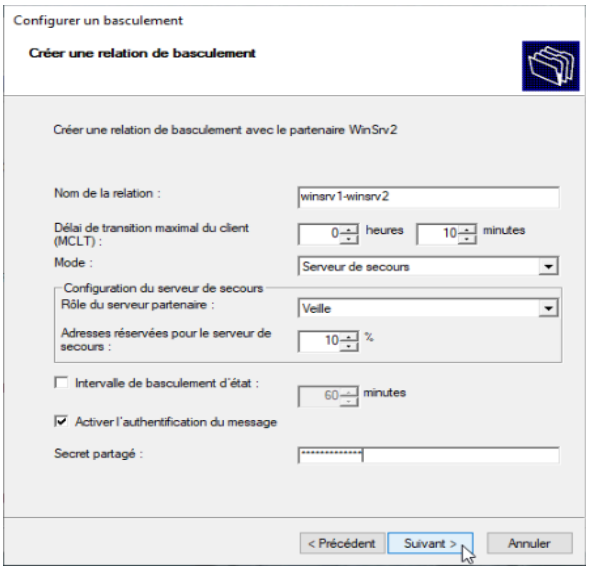


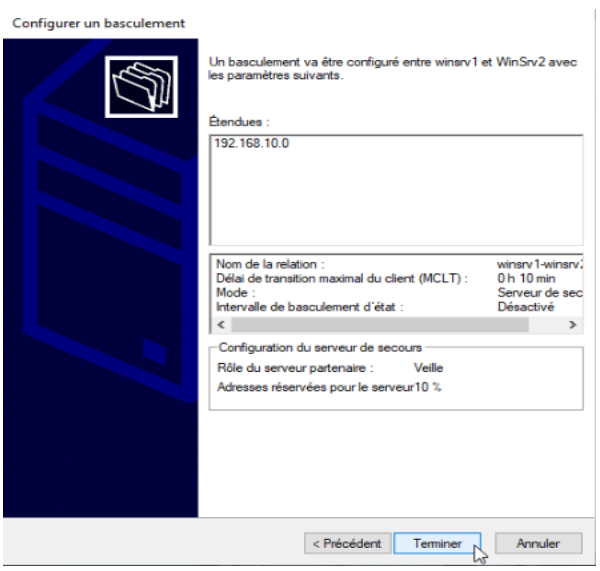
On se rend sur le premier serveur (WinSrv1), on clique droit sur les étendues souhaitées puis Configurer un basculement :



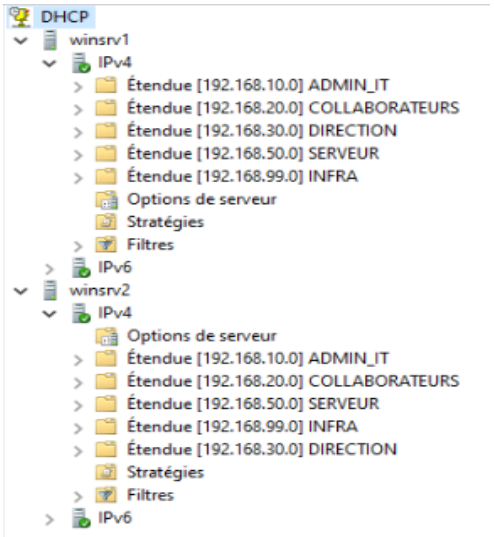








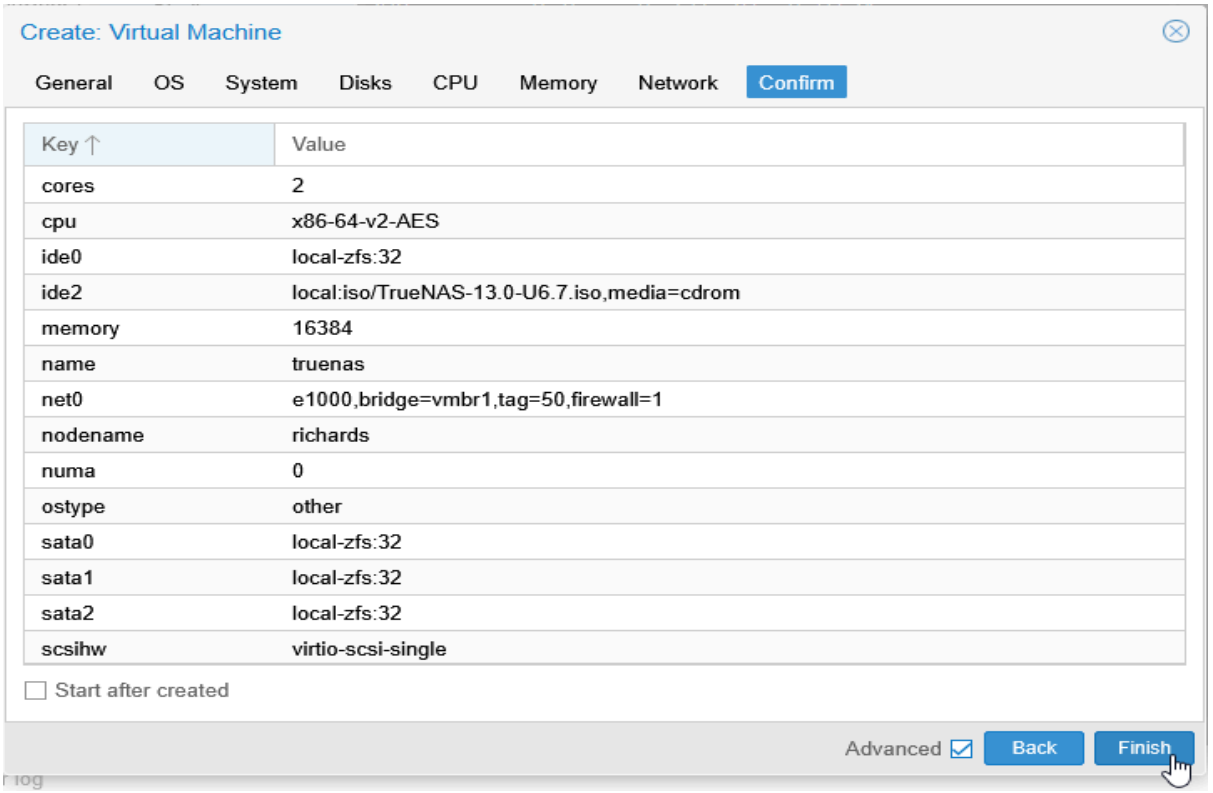
Refaire les mêmes actions pour les différentes étendues.



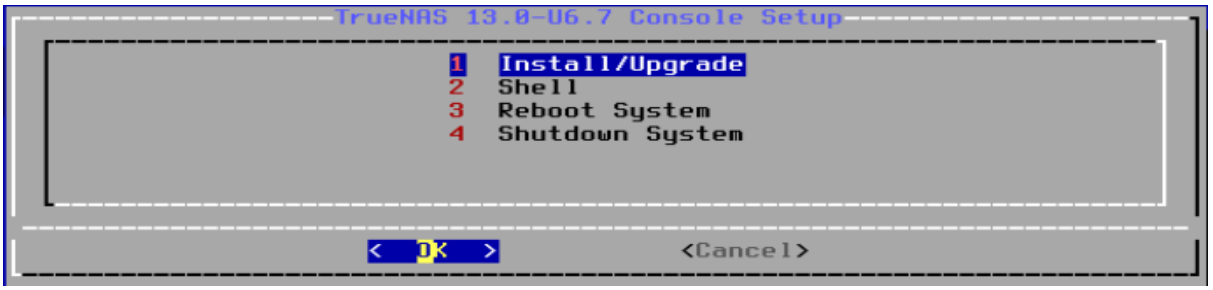
II. Stockage et PCA

- Installation et configuration de TrueNAS pour le stockage

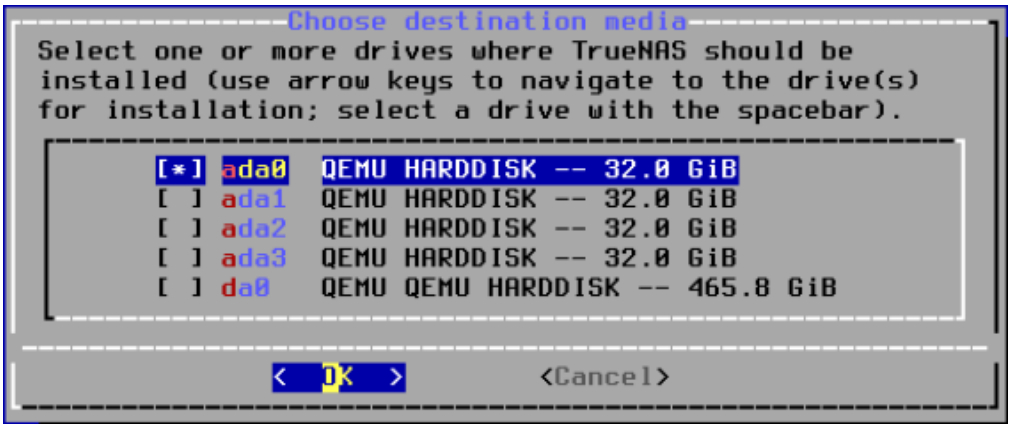
Création de la VM TrueNAS :



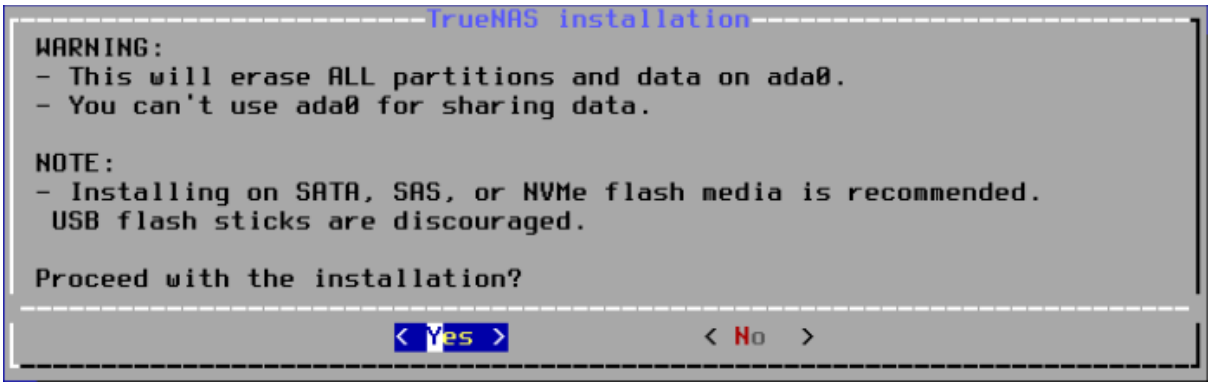
Installation de TrueNAS :
Sélectionnez install/upgrade :



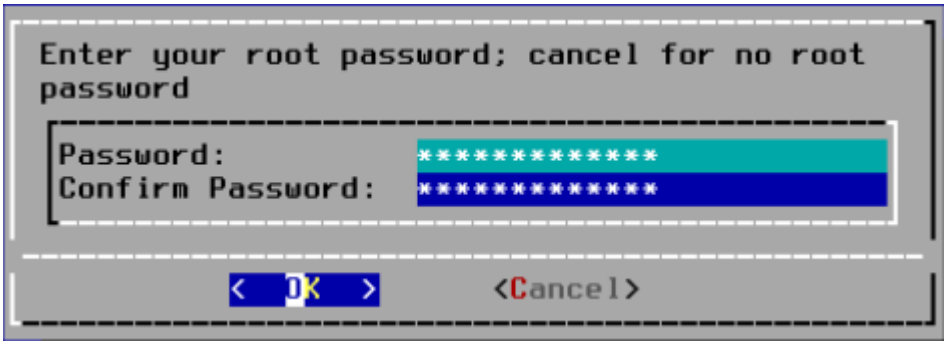
Choisir le disque d'installation :



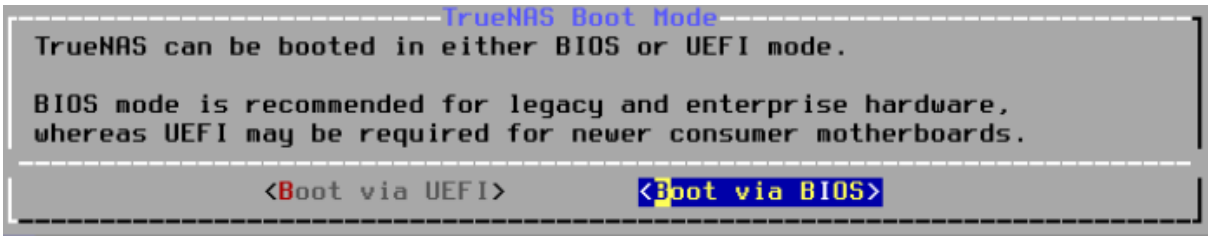
Je sélectionne : YES



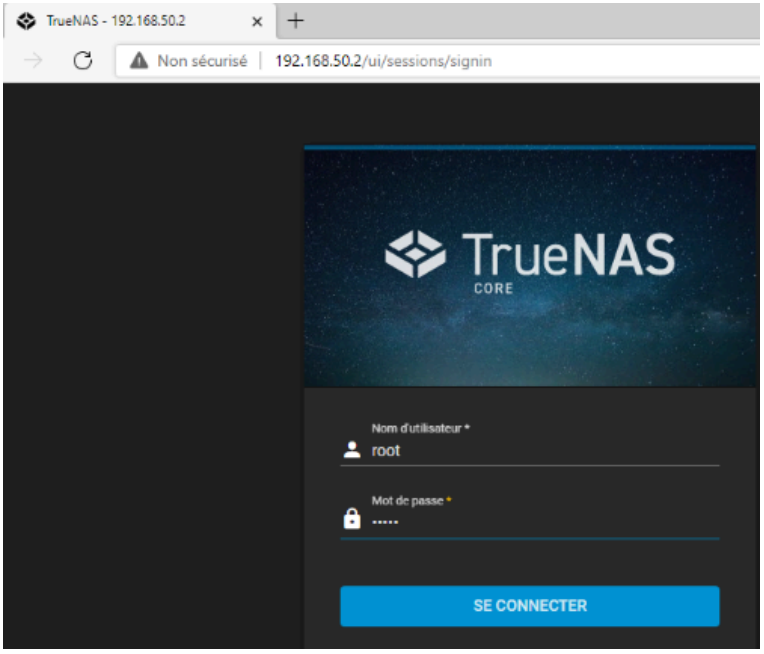
Configuration du mot de passe puis OK



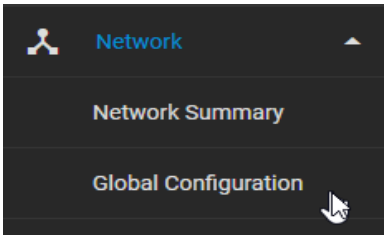
BOOT via BIOS :



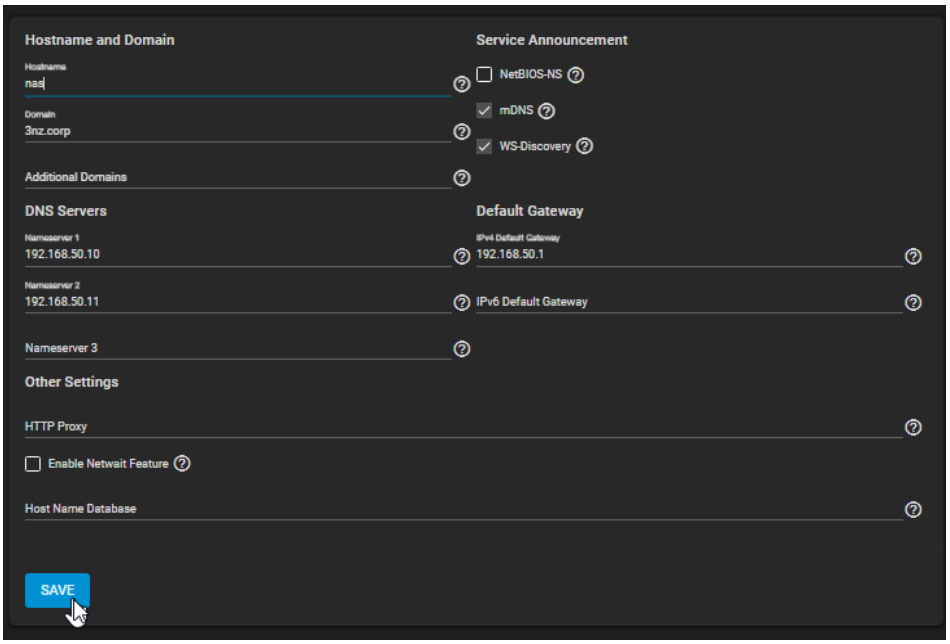
Maintenant se connecter à l'interface WEB de TRUENAS :



Network -> Global Configuration

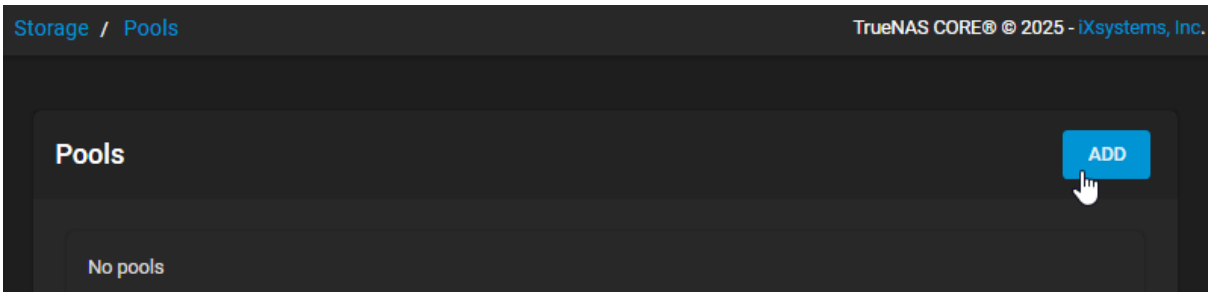


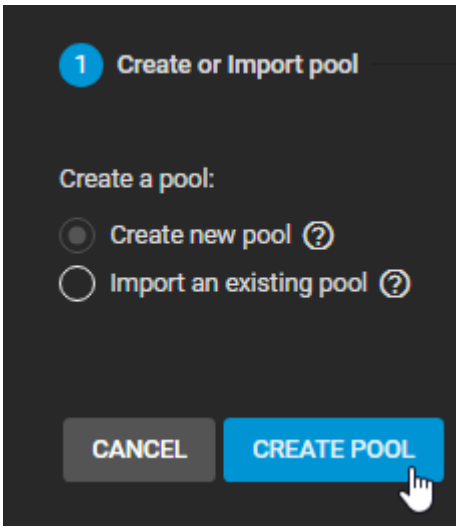
Changer le hostname, domain, DNS servers et la gateway



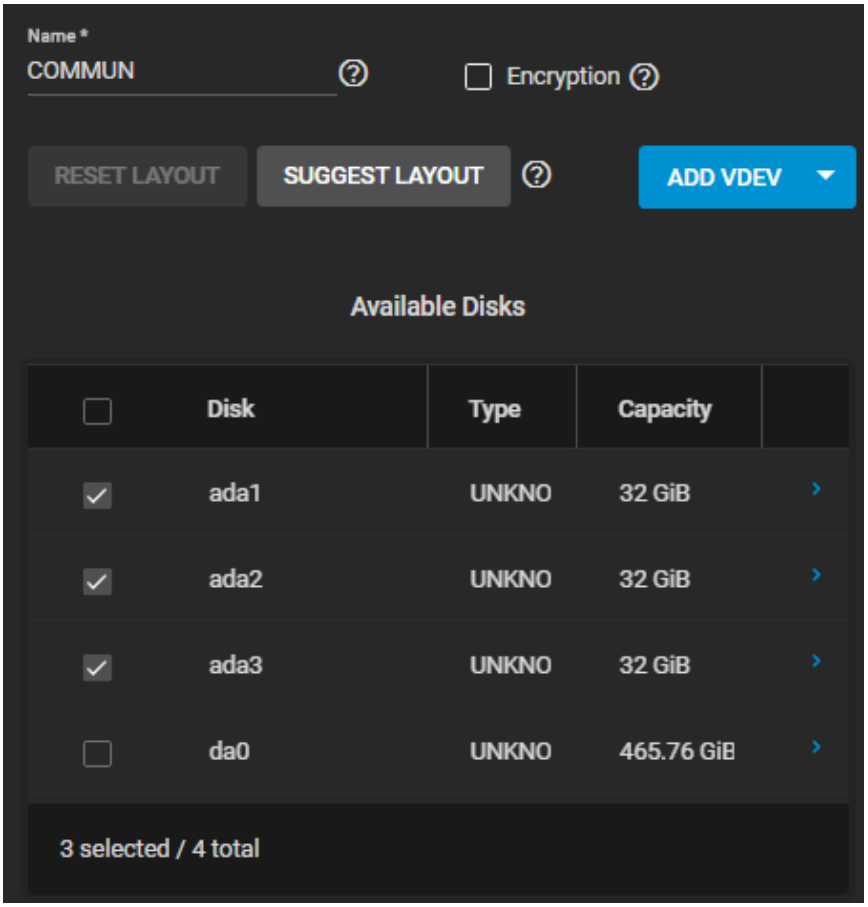
- Création de pools, datasets et partages SMB avec ACLs

Création d’un pool Stockage -> Pools

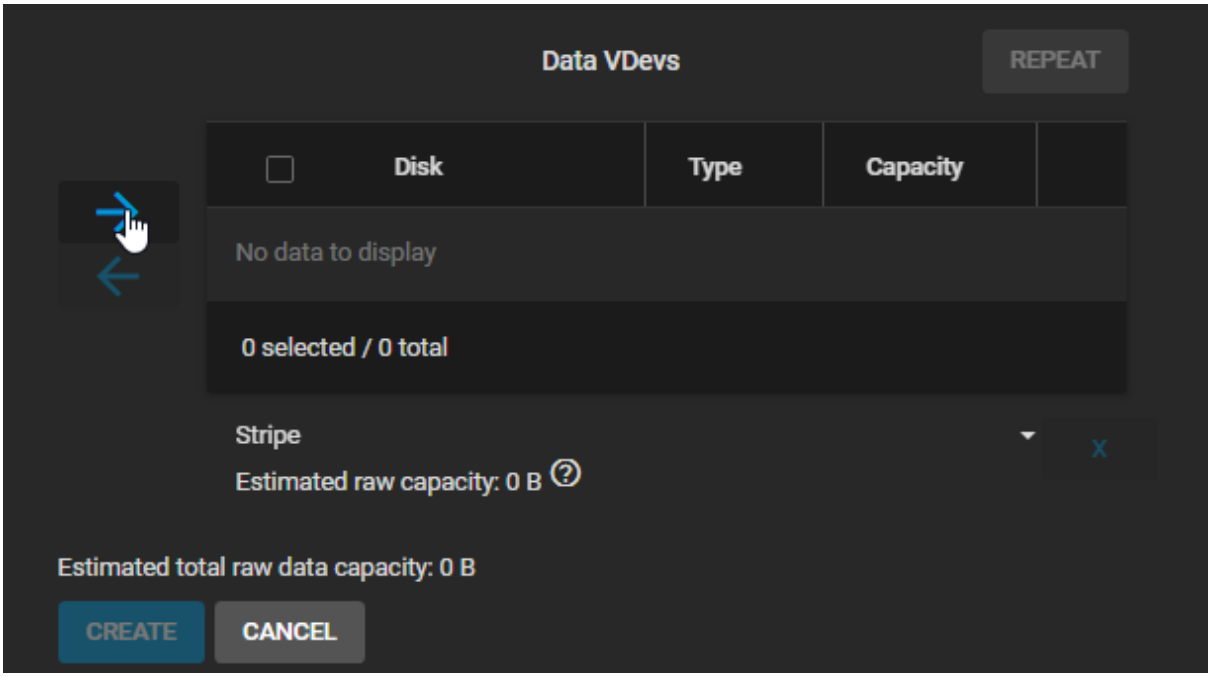




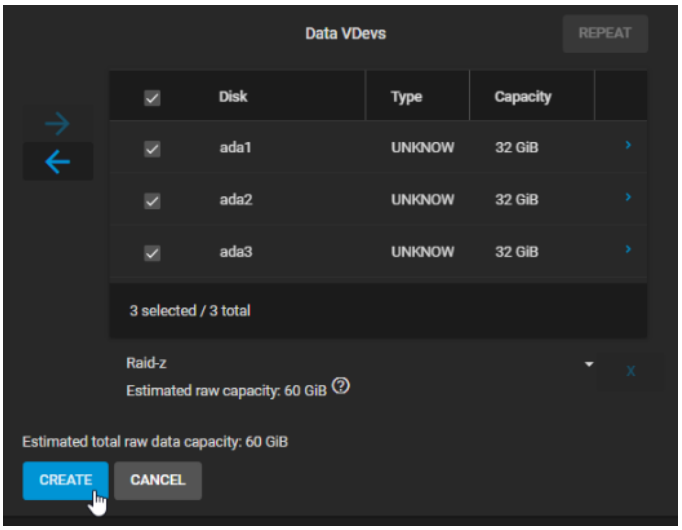
Choisir le nom et les disques

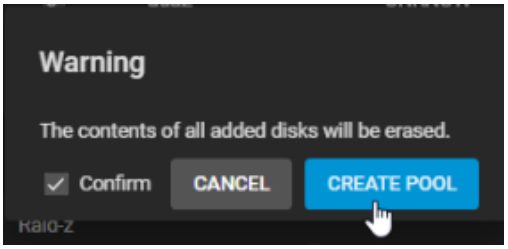


Cliquez sur la flèche en surbrillance bleue pour assigner les disques sélectionnés

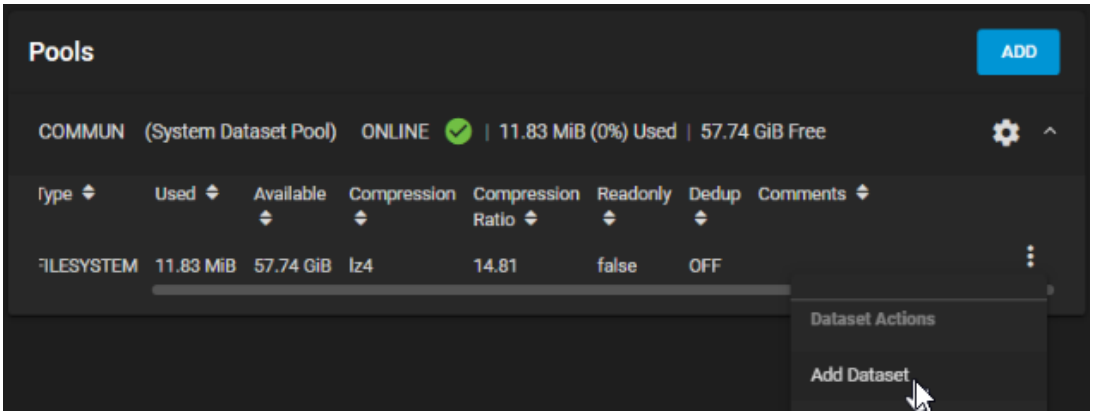


Re-sélectionnez les disques, choisissez votre type de raid, en l'occurrence raid-z puis créez :

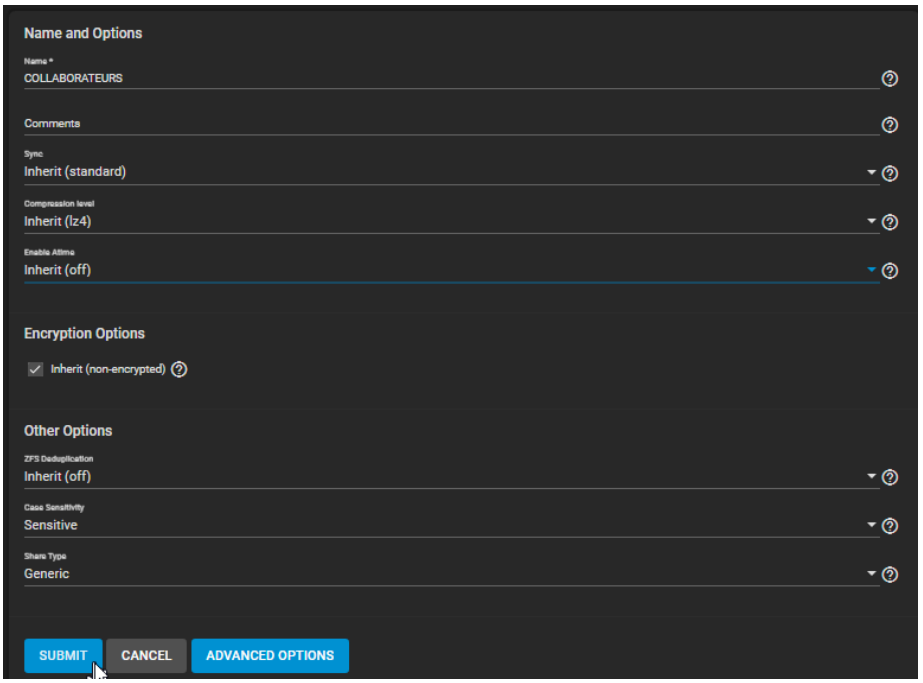




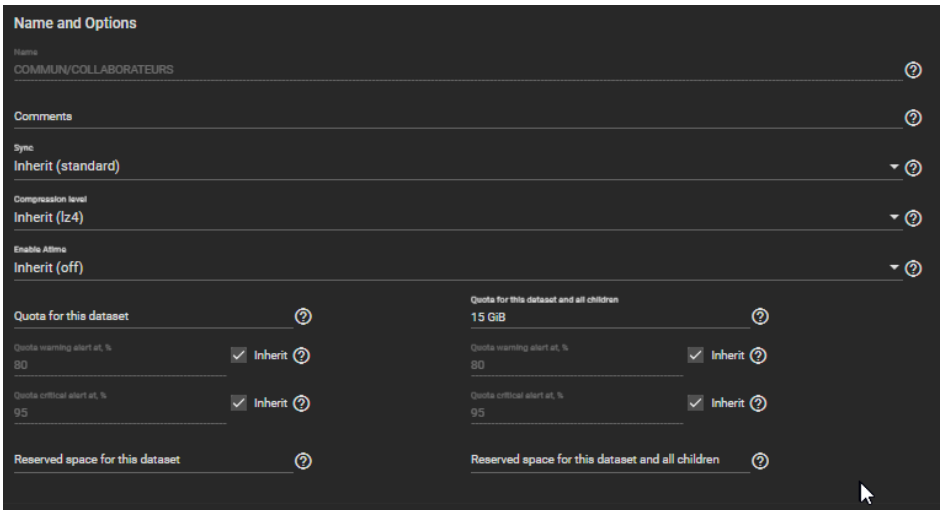
Dans stockage > Pools > votre pool, appuyez sur les trois petits points et ajoutez un dataset



Création du dataset :



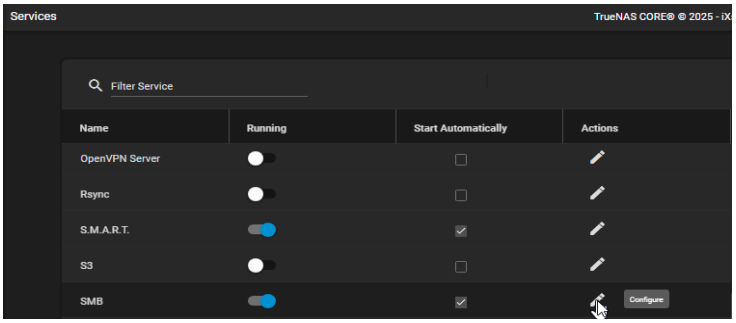
Dans Advanced Options je choisi de lui attribuer 15 GiB de quota pour lui et ses enfants :



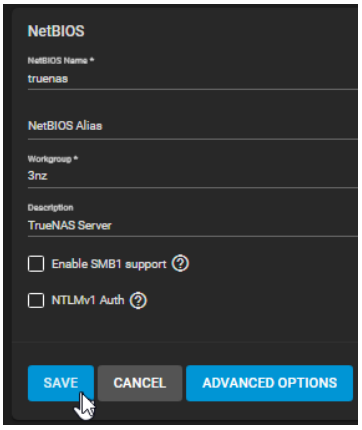
J’en créer 2 autres, DIRECTION et DSI

COMMUN	FILESYSTEM	12.68 MiB	57.74 GiB	lz4	14.25	false	OFF
COLLABORATEURS	FILESYSTEM	127.88 KiB	15 GiB	Inherits (lz4)	1.00	false	OFF
DIRECTION	FILESYSTEM	127.88 KiB	15 GiB	Inherits (lz4)	1.00	false	OFF
DSI	FILESYSTEM	127.88 KiB	20 GiB	Inherits (lz4)	1.00	false	OFF

Ensuite, configuration du partage SMB : Services > SMB, on active la case Start AUTOMATICALLY puis configure :

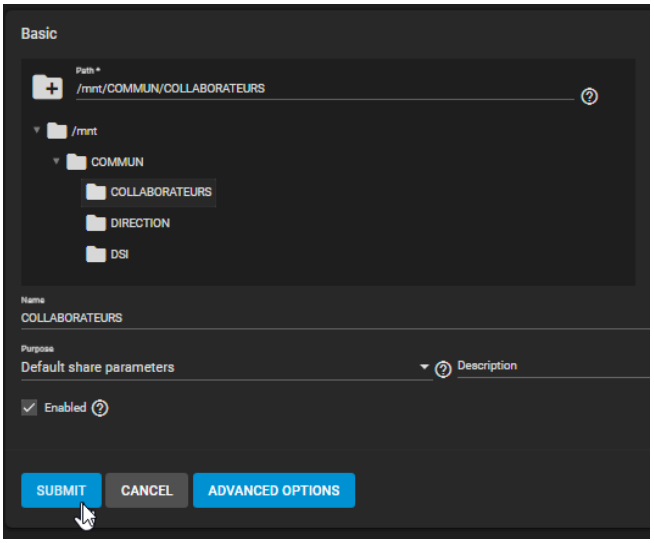


Changez le workgroup puis sauvegardez :

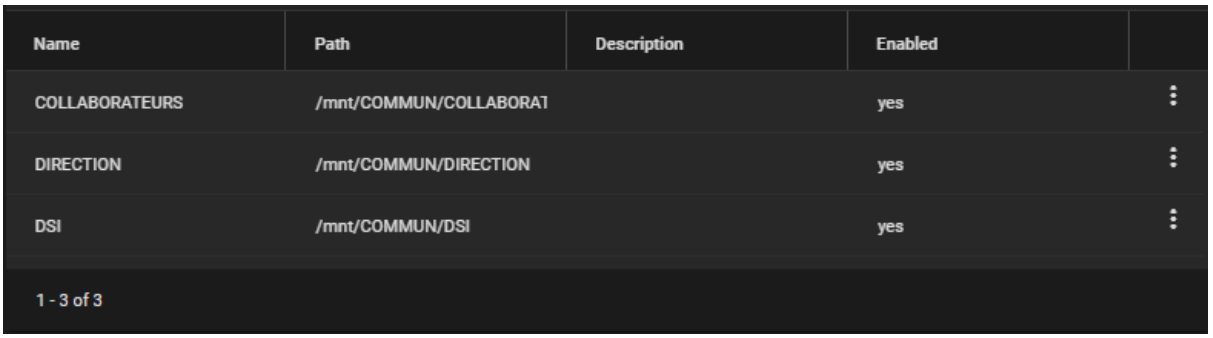


Ensuite, Sharing > Windows Shares (SMB) cliquez sur ADD :

Je sélectionne le dataset à partager, puis je valide la création du partage, dans mon cas /COMMUN/COLLABORATEURS :



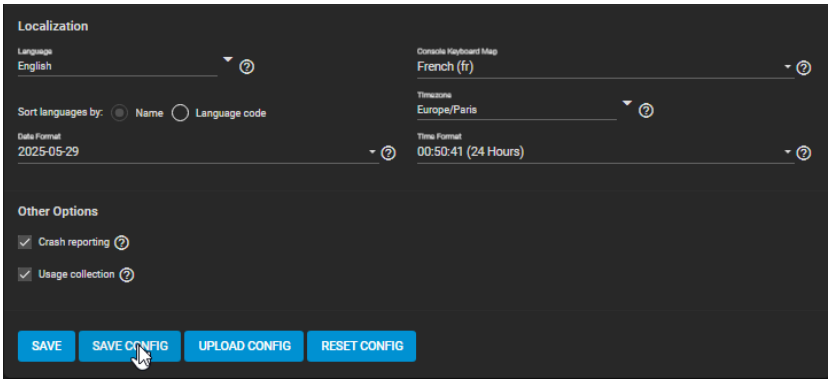
Je fais la même chose pour DIRECTION et DSI :



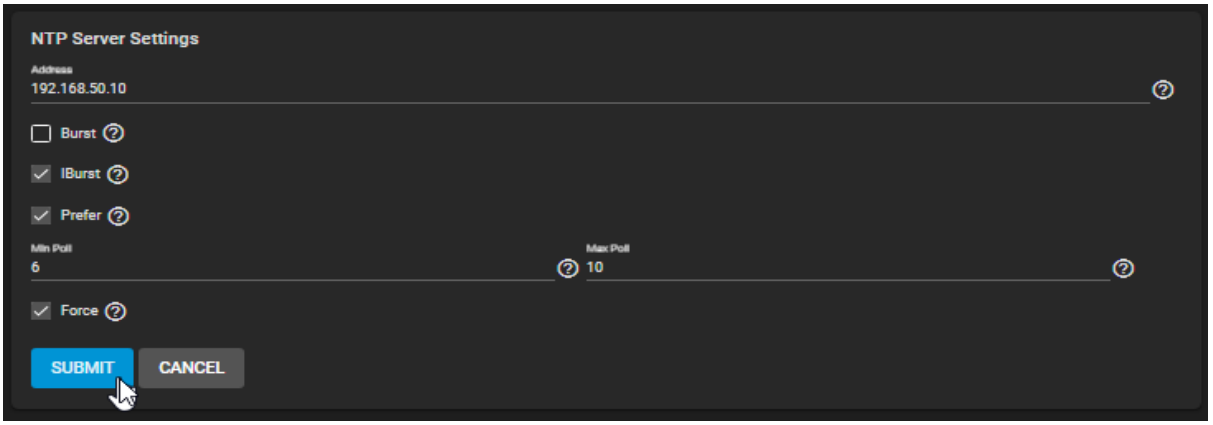
Name	Path	Description	Enabled
COLLABORATEURS	/mnt/COMMUN/COLLABORAT		yes
DIRECTION	/mnt/COMMUN/DIRECTION		yes
DSI	/mnt/COMMUN/DSI		yes

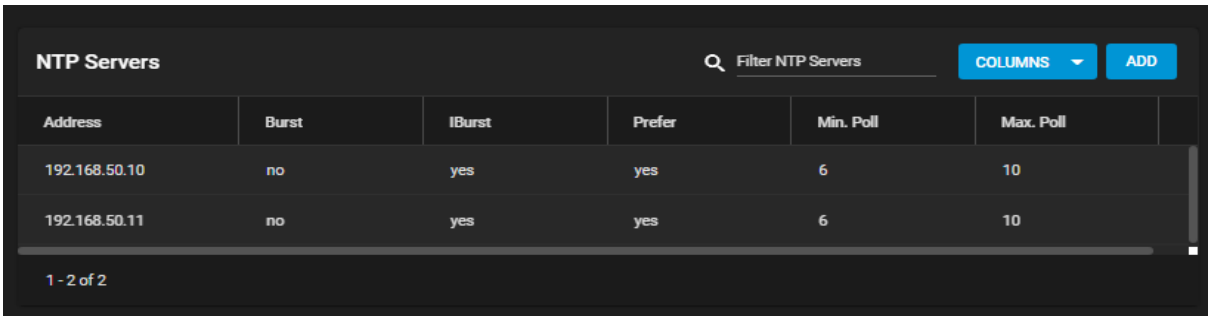
1 - 3 of 3

Changez la localisation de TrueNAS :



Ajout des serveurs NTP :



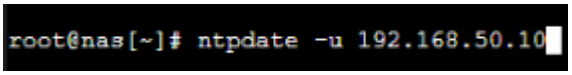


NTP Servers — Filter NTP Servers — COLUMNS — ADD

Address	Burst	IBurst	Prefer	Min. Poll	Max. Poll
192.168.50.10	no	yes	yes	6	10
192.168.50.11	no	yes	yes	6	10

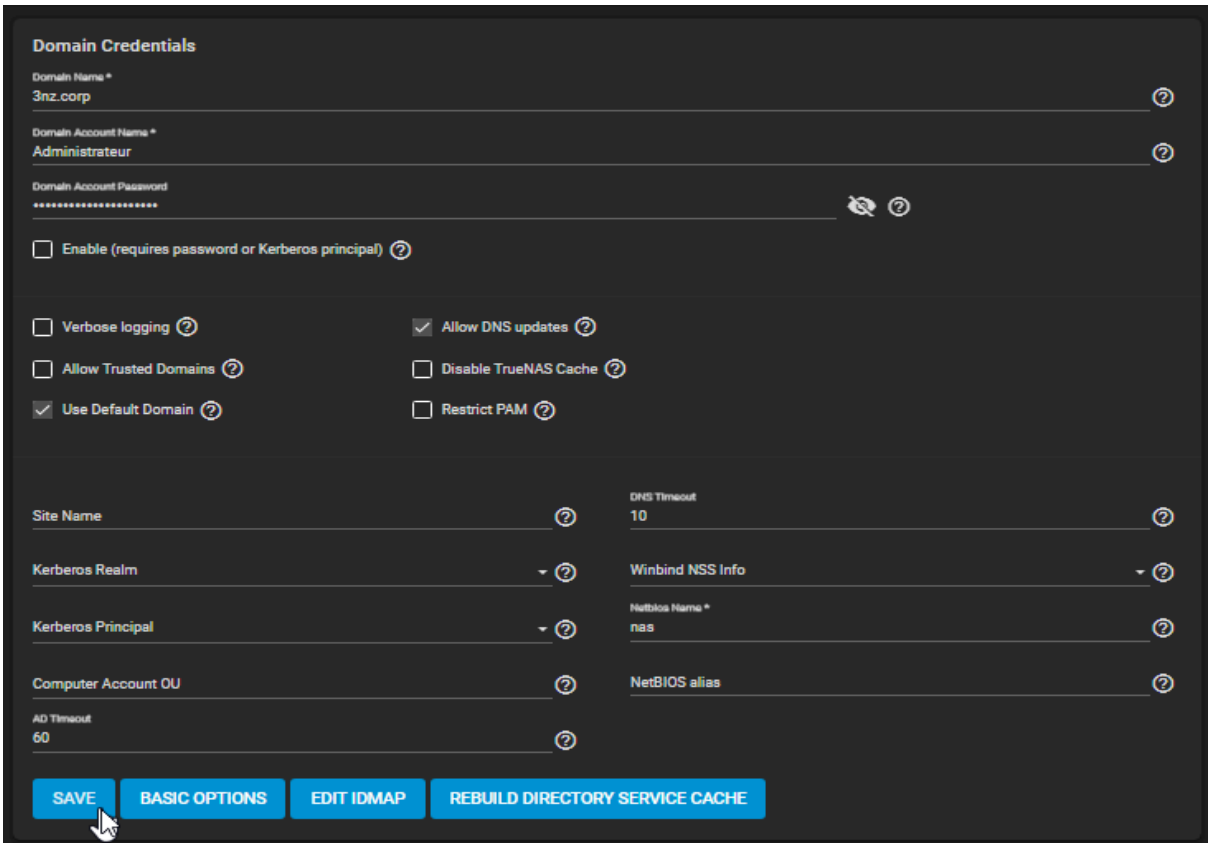
1 - 2 of 2

Puis dans l'onglet Shell de TrueNas je tape :

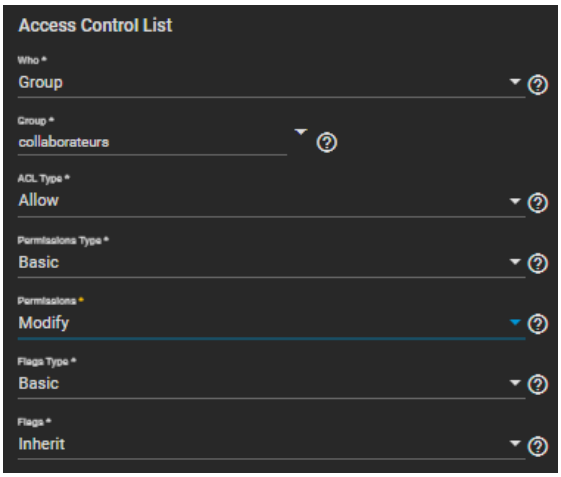


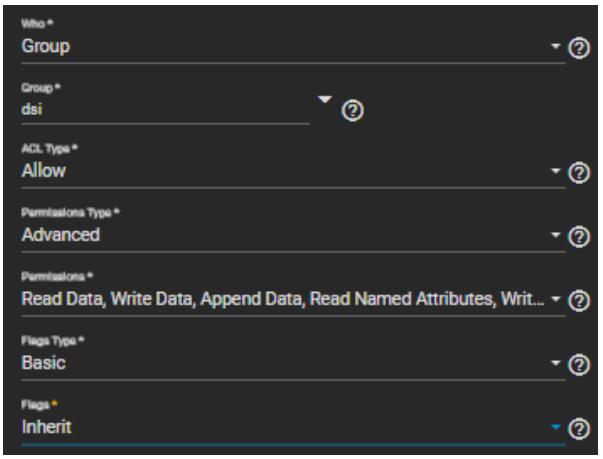
Pour forcer la synchronisation ntp.

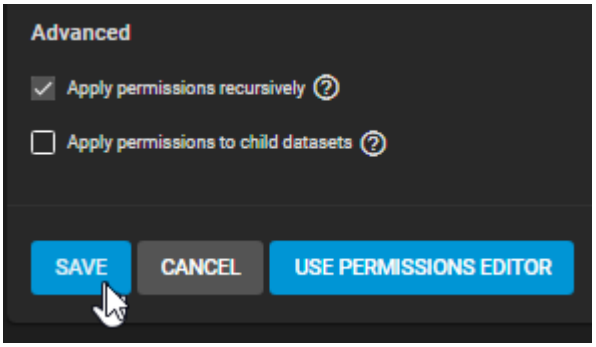
Puis je me rends dans Directory Services > Active Directory (s'il n'était pas déjà configuré)



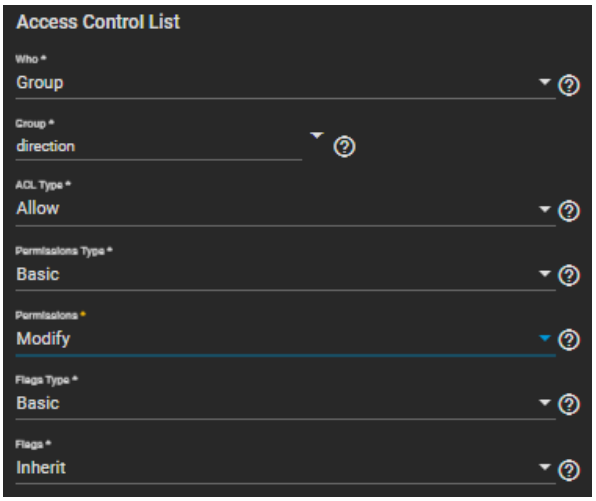
Ensuite de retour dans Storage > Pools > Edit ACL
Pour le dataset COLLABORATEURS :

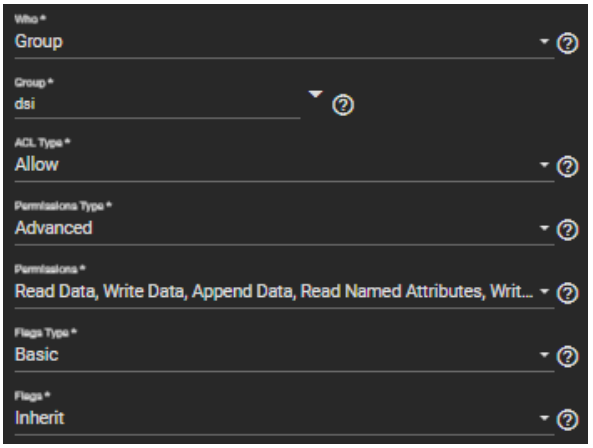


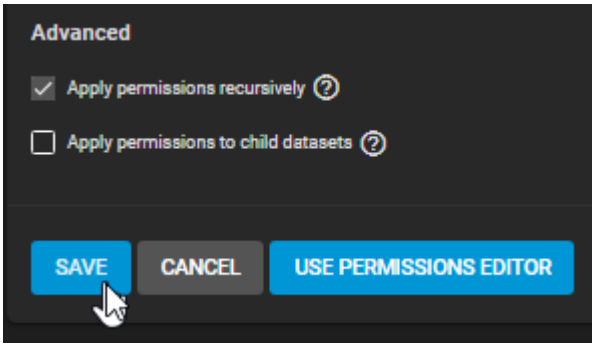




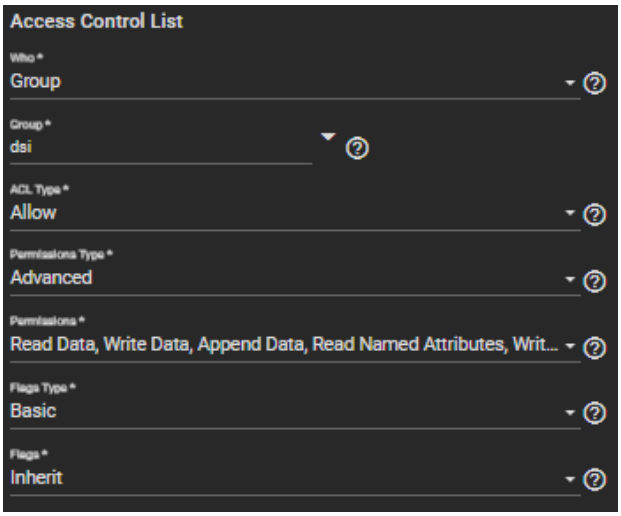
Pour le dataset DIRECTION :

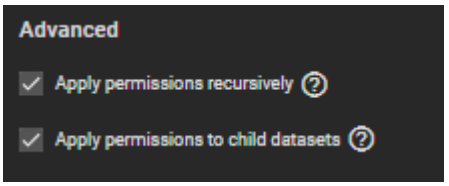






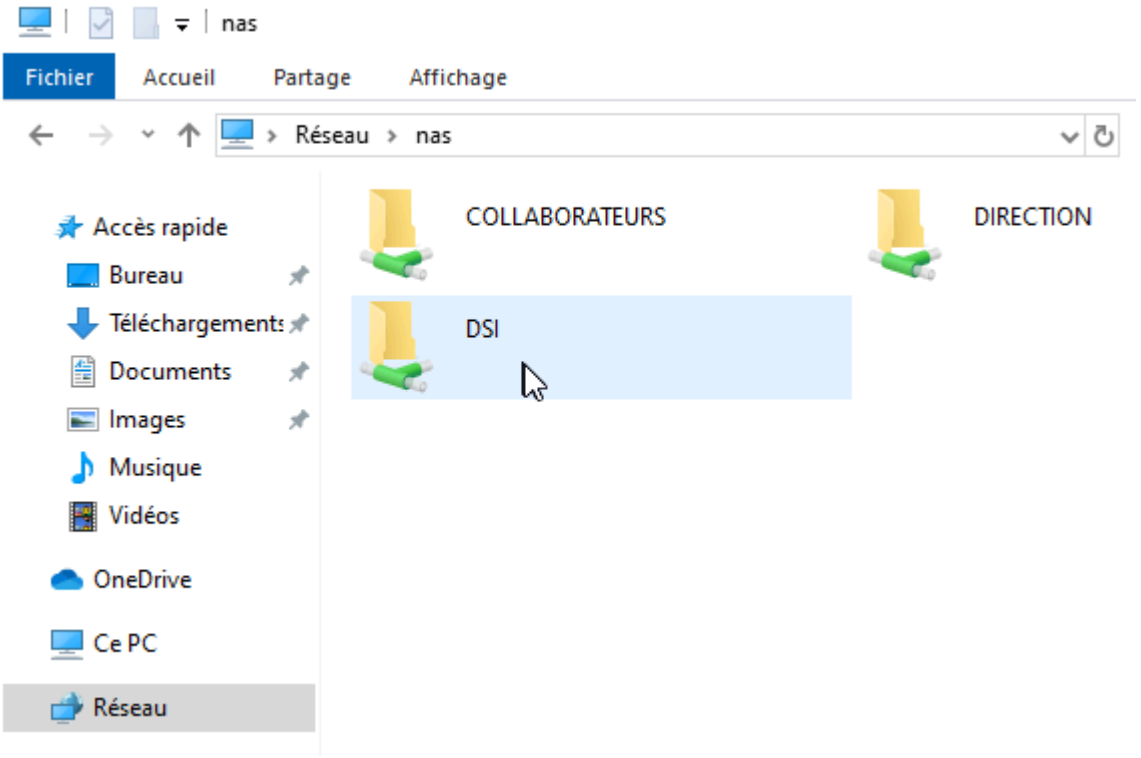
Pour le dataset DSI :



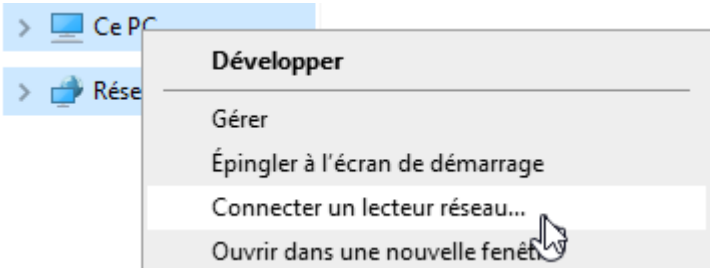


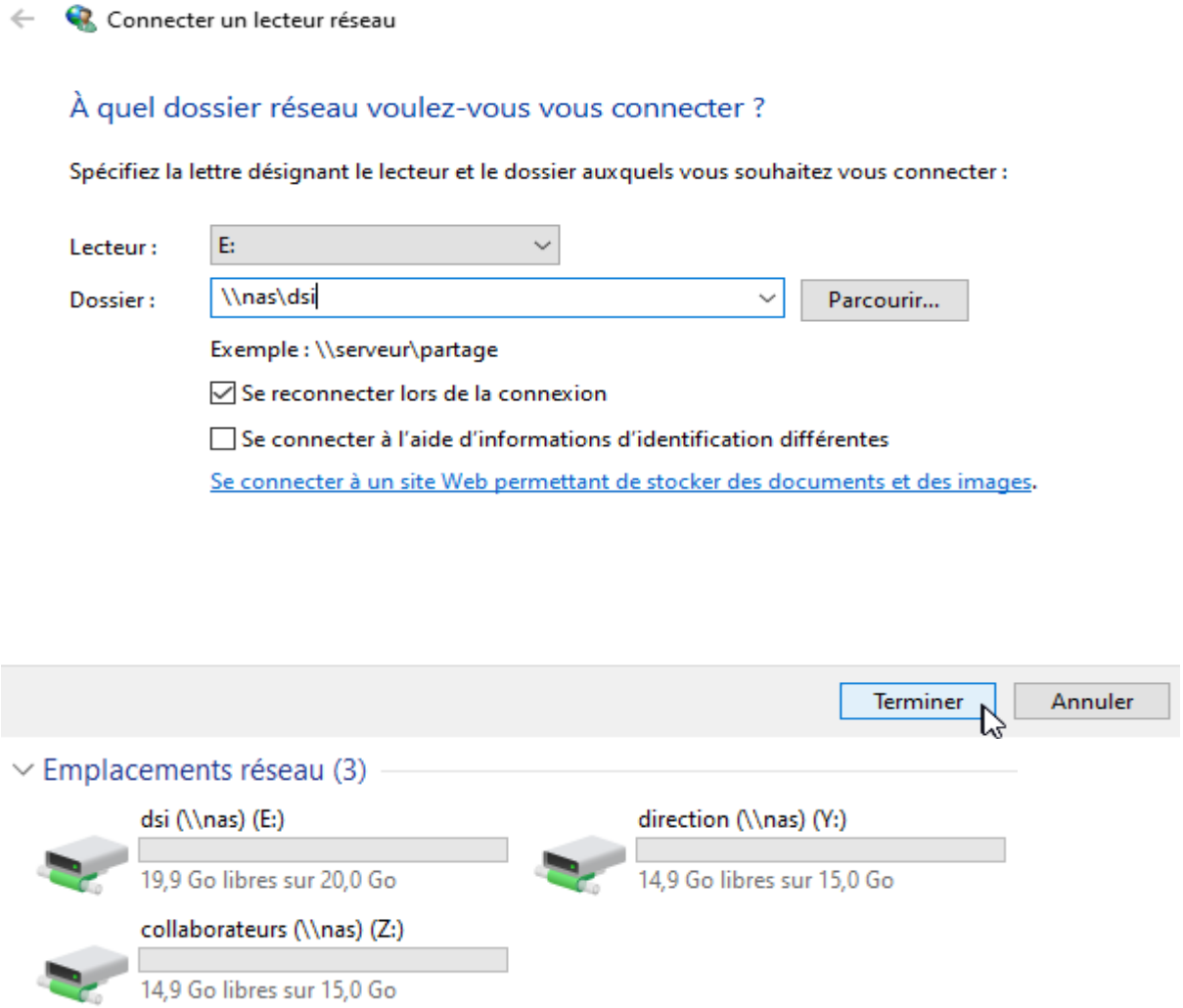
Accès aux partages depuis la vm windows, exemple sur un poste du groupe DSI :

Activer la découverte réseau et ouvrir l'explorateur de fichiers et tapez l'adresse ip du serveur nas ou simplement son nom dns : \\nas



Pour monter le partage de façon permanente : clic droit sur ce pc > Connecter un lecteur réseau :

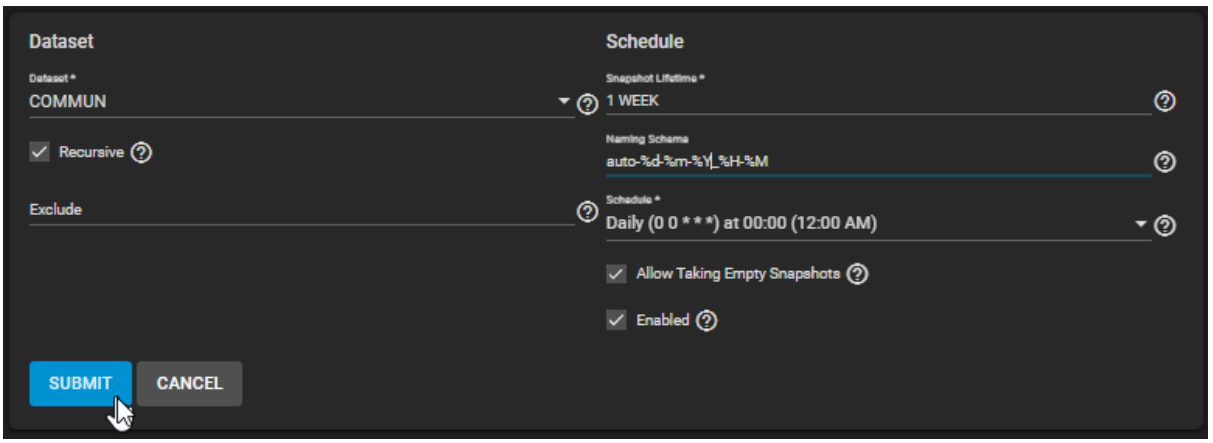




- Configuration des snapshots automatiques sur TrueNAS

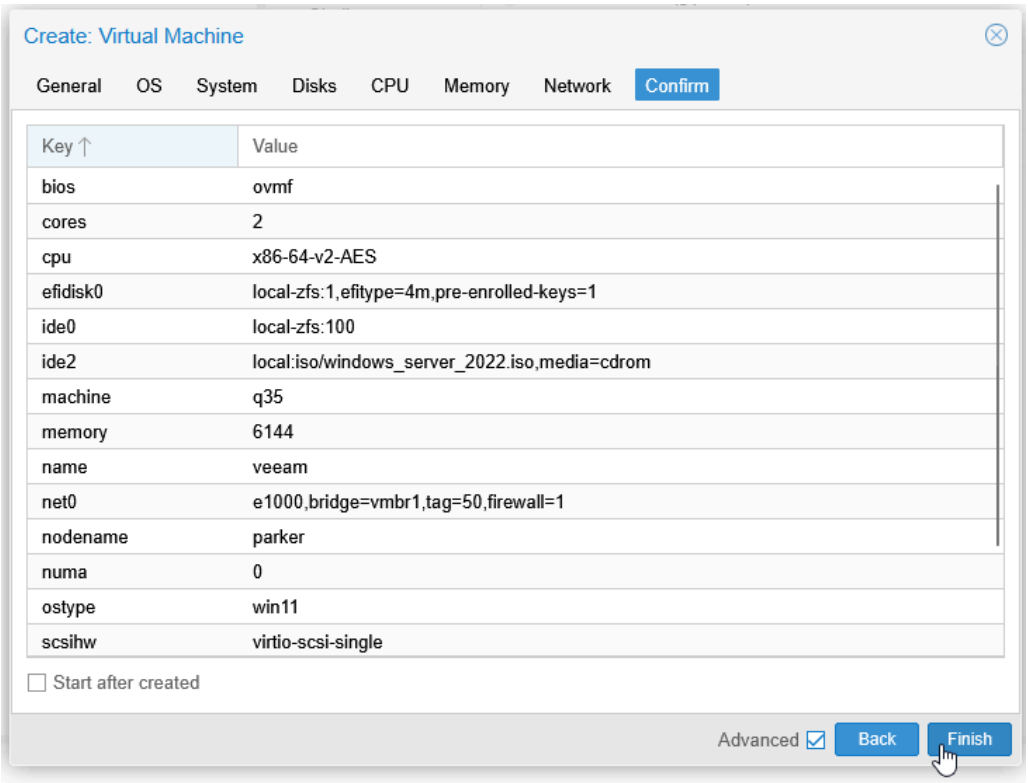
Configuration des snapshots :
Tasks > Periodic Snapshot Tasks

Je crée une snapshot périodique, sa durée de vie est d'une semaine et elle est faites tous les jours à minuit :

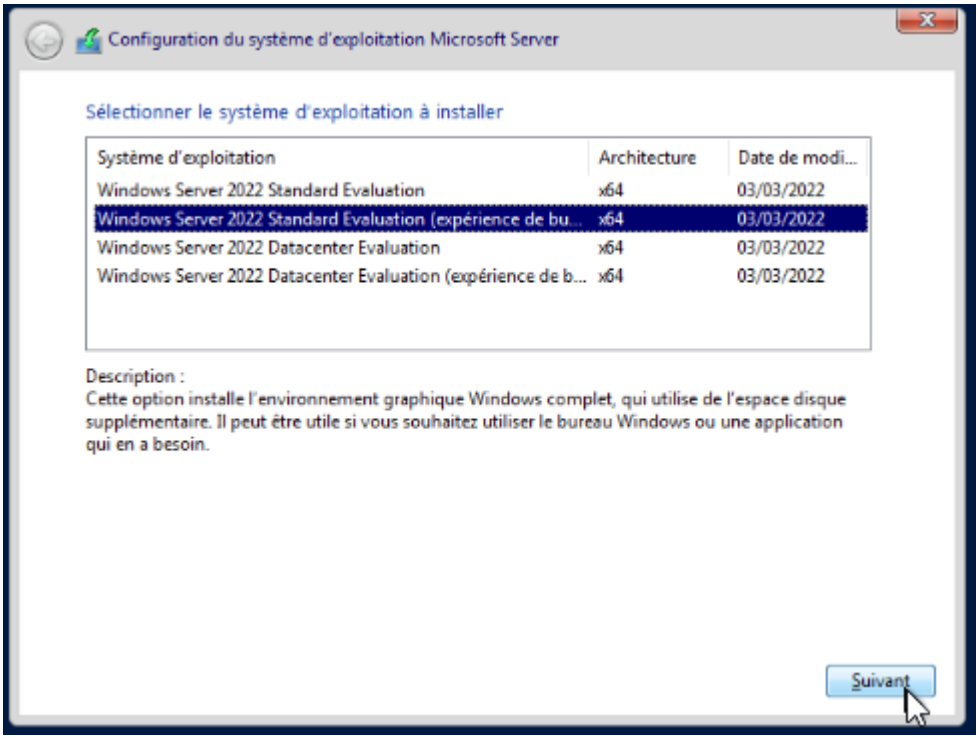


- Déploiement Veeam Backup sur serveur dédié

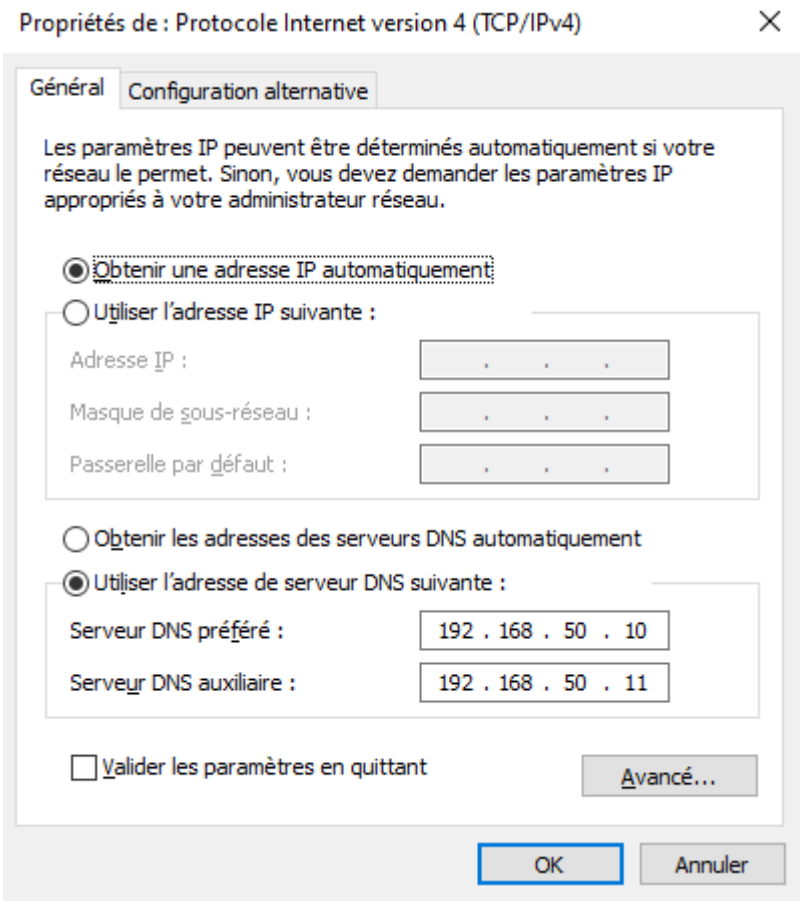
Maintenant,on passe à la configuration d'une sauvegarde Veeam Backup vers TrueNAS :
Création de la VM Windows Server, sur lequel nous allons installer Veeam Backup :



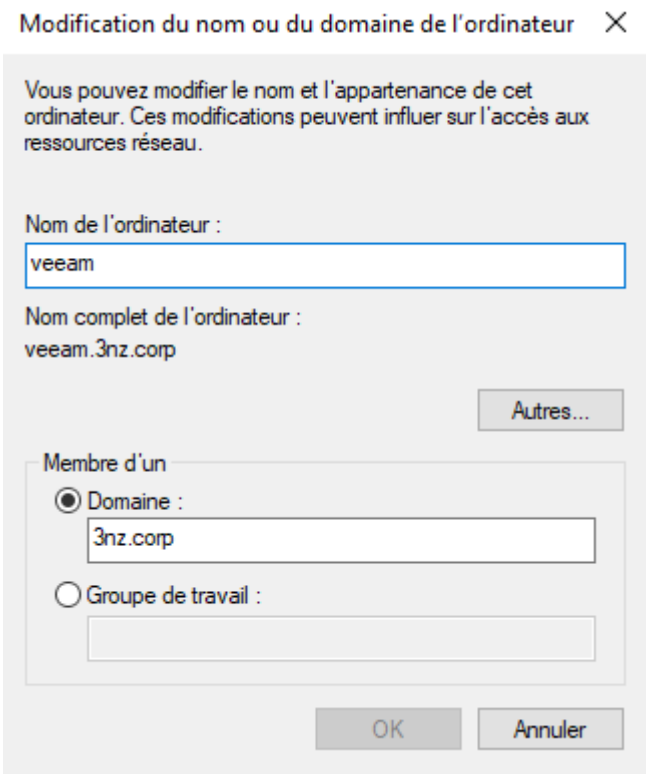
Exactement les même manips que lors du premier windows server, sauf que celui-ci je le mets en expérience de bureau :



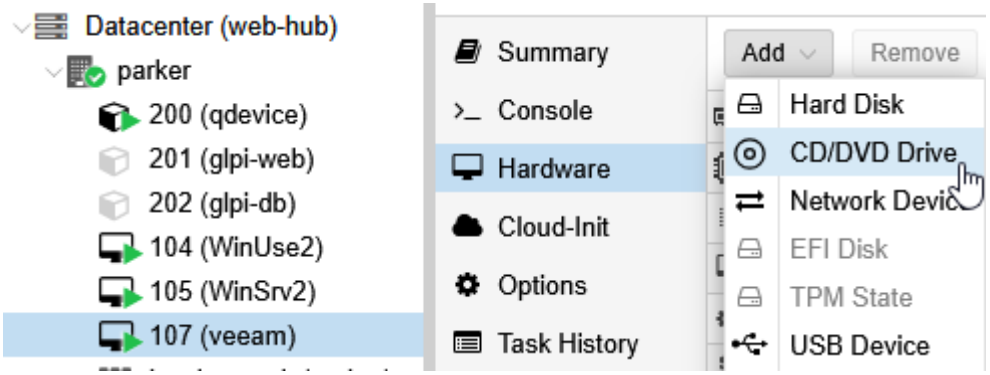
Une fois l'os installé, je modifie l'adresse des serveurs DNS :



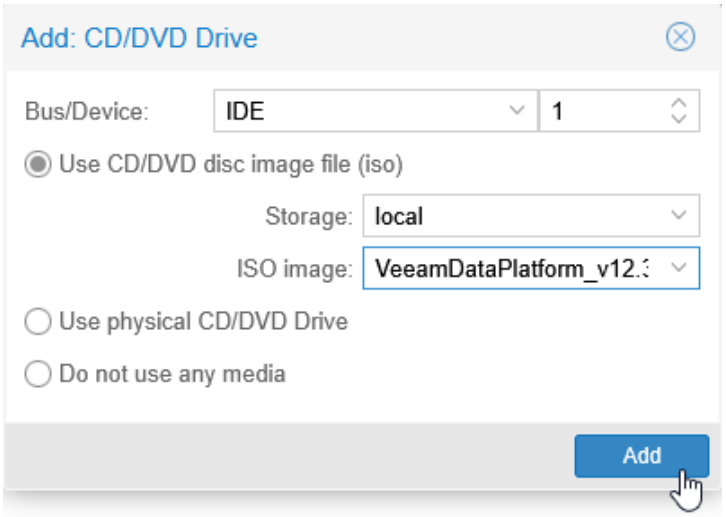
Modification du nom de la machine et du nom de domaine :



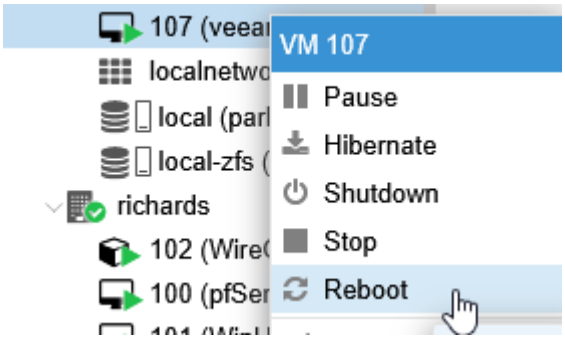
Maintenant je me rends sur l'interface GUi de proxmox et je vais sur ma vm veeam > Hardware > Add > CD/DVD Drive



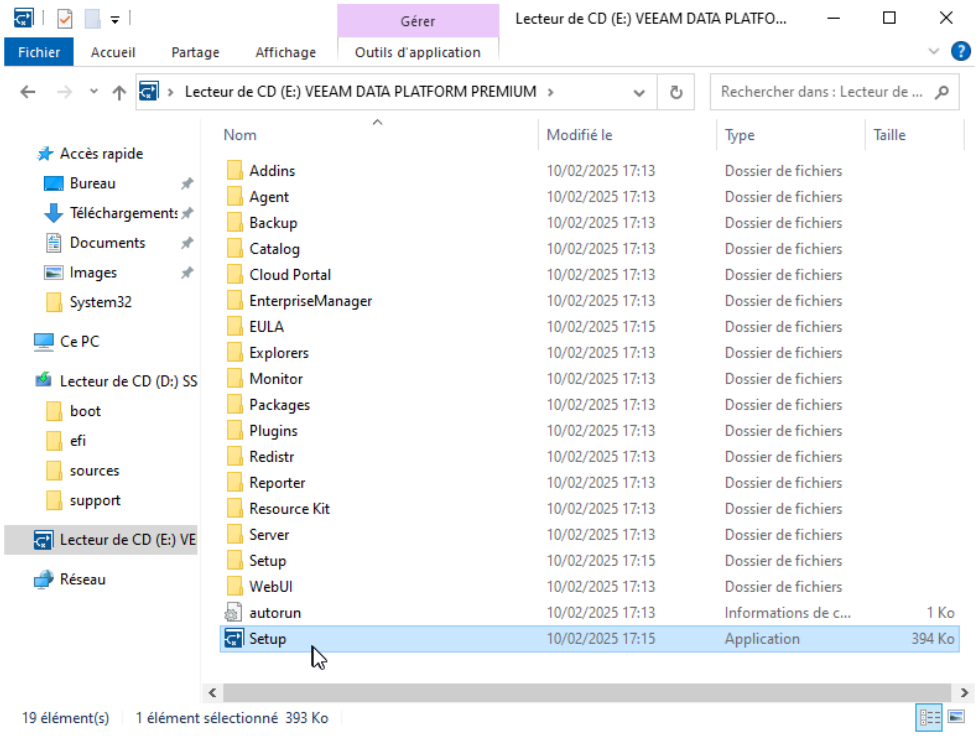
Je sélectionne l'iso et j'ajoute :

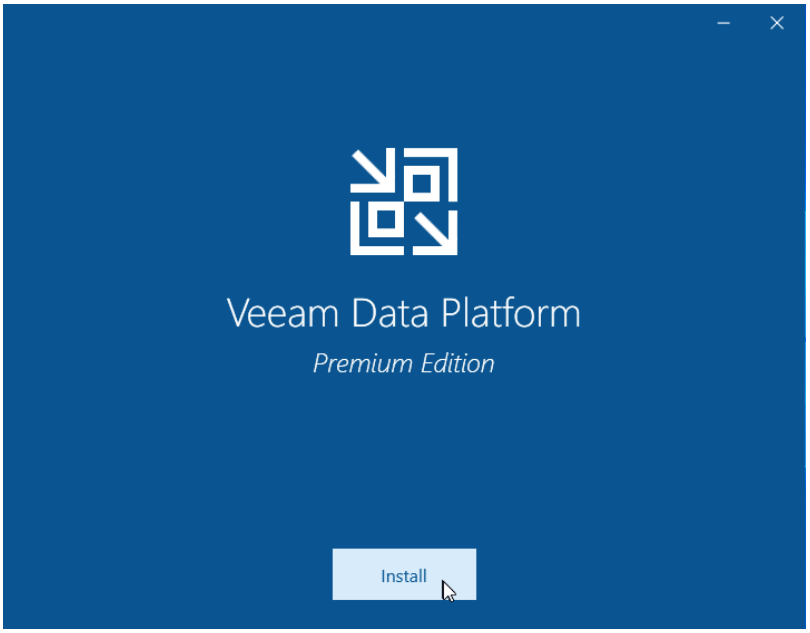


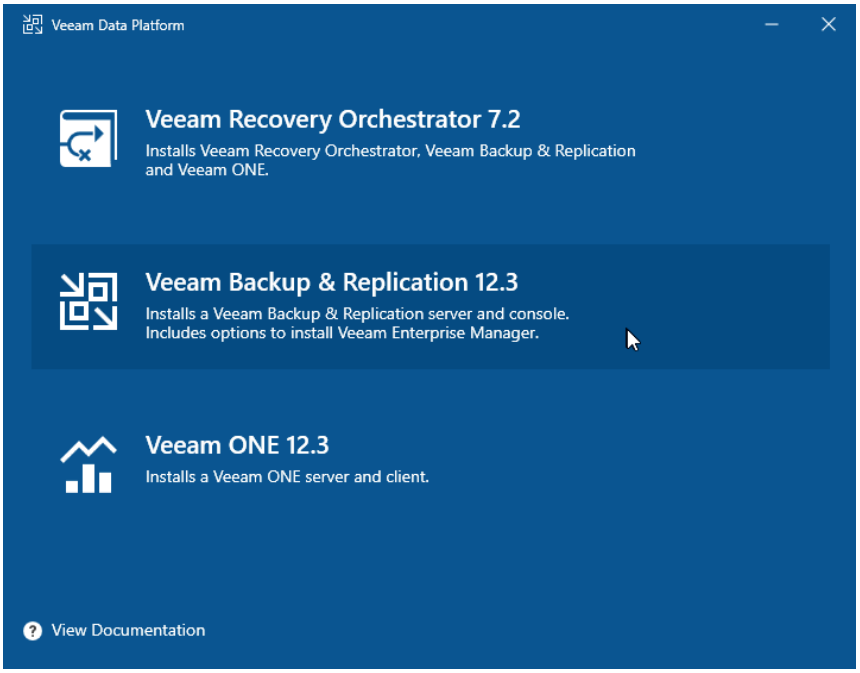
Puis reboot la VM :

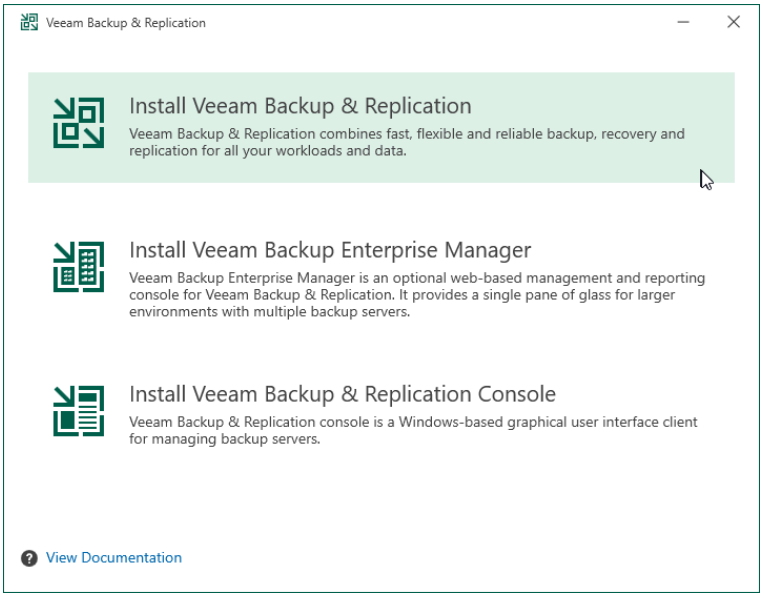


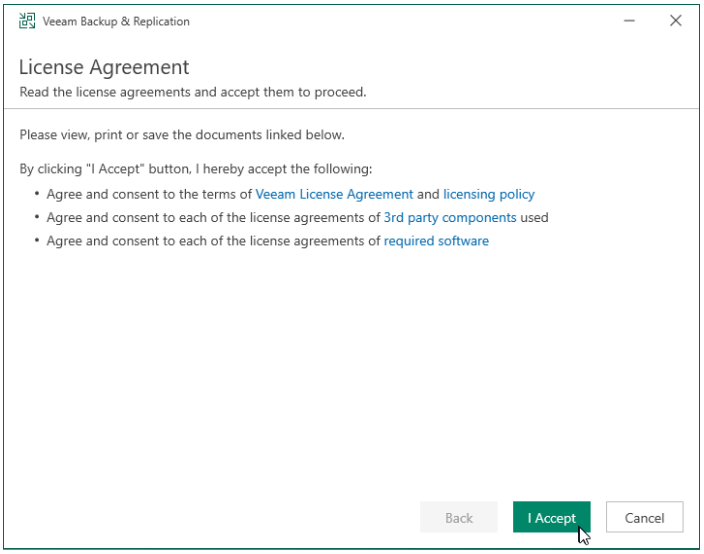
De retour sur le serveur, on lance le setup :

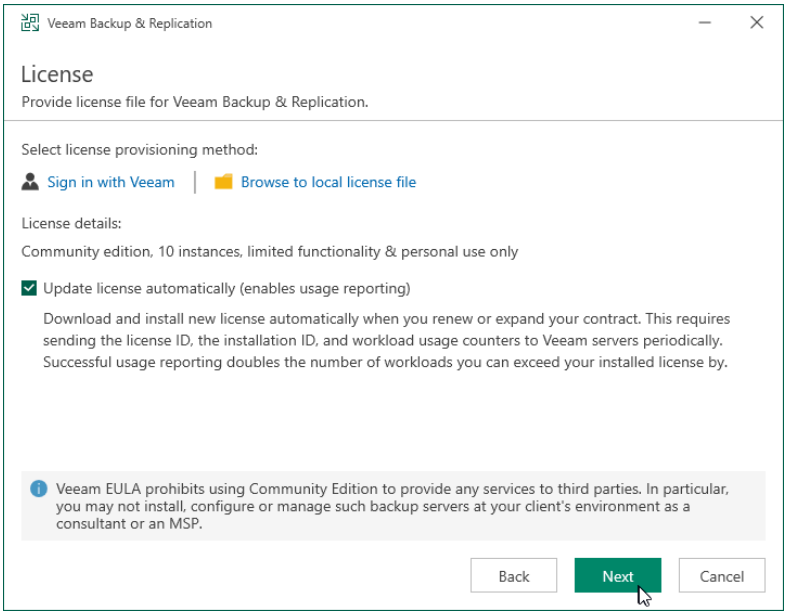


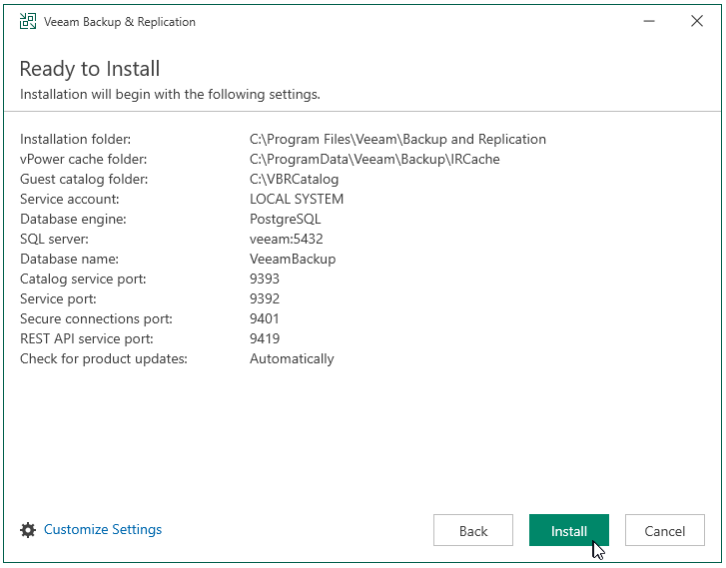



Veeam Data Platform
Veeam Recovery Orchestrator 7.2
Installs Veeam Recovery Orchestrator, Veeam Backup & Replication and Veeam ONE.
Veeam Backup & Replication 12.3
Installs a Veeam Backup & Replication server and console. Includes options to install Veeam Enterprise Manager.
Veeam ONE 12.3
Installs a Veeam ONE server and client.
View Documentation

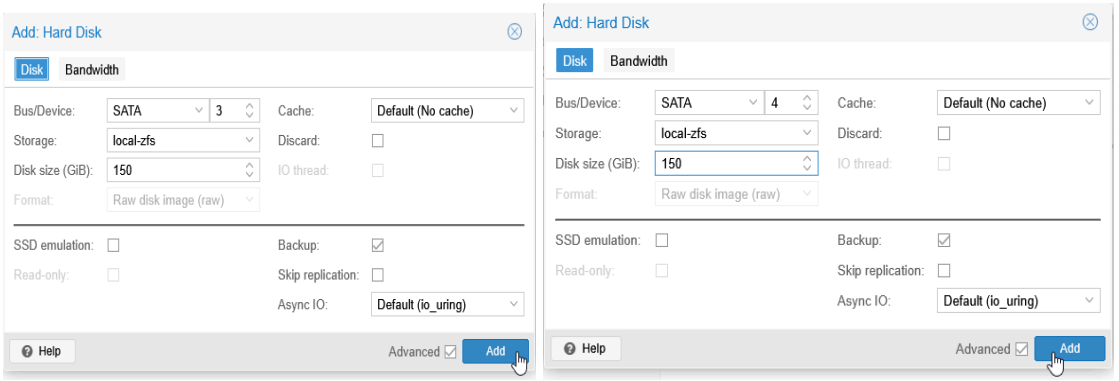

Veeam Backup & Replication
Install Veeam Backup & Replication
Veeam Backup & Replication combines fast, flexible and reliable backup, recovery and replication for all your workloads and data.
Install Veeam Backup Enterprise Manager
Veeam Backup Enterprise Manager is an optional web-based management and reporting console for Veeam Backup & Replication. It provides a single pane of glass for larger environments with multiple backup servers.
Install Veeam Backup & Replication Console
Veeam Backup & Replication console is a Windows-based graphical user interface client for managing backup servers.
View Documentation


Veeam Backup & Replication
License Agreement
Read the license agreements and accept them to proceed.
Please view, print or save the documents linked below.
By clicking "I Accept" button, I hereby accept the following:
• Agree and consent to the terms of Veeam License Agreement and licensing policy
• Agree and consent to each of the license agreements of 3rd party components used
• Agree and consent to each of the license agreements of required software
Back
I Accept
Cancel

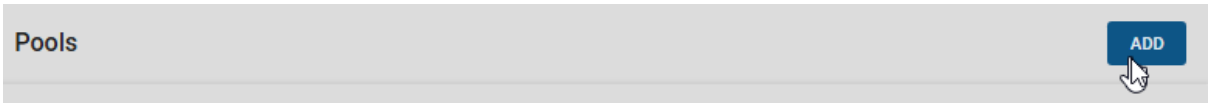


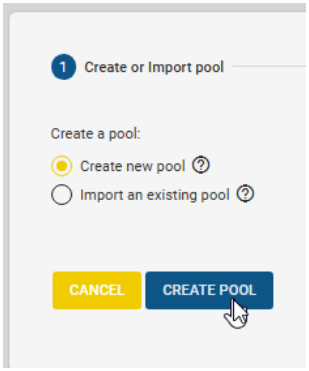


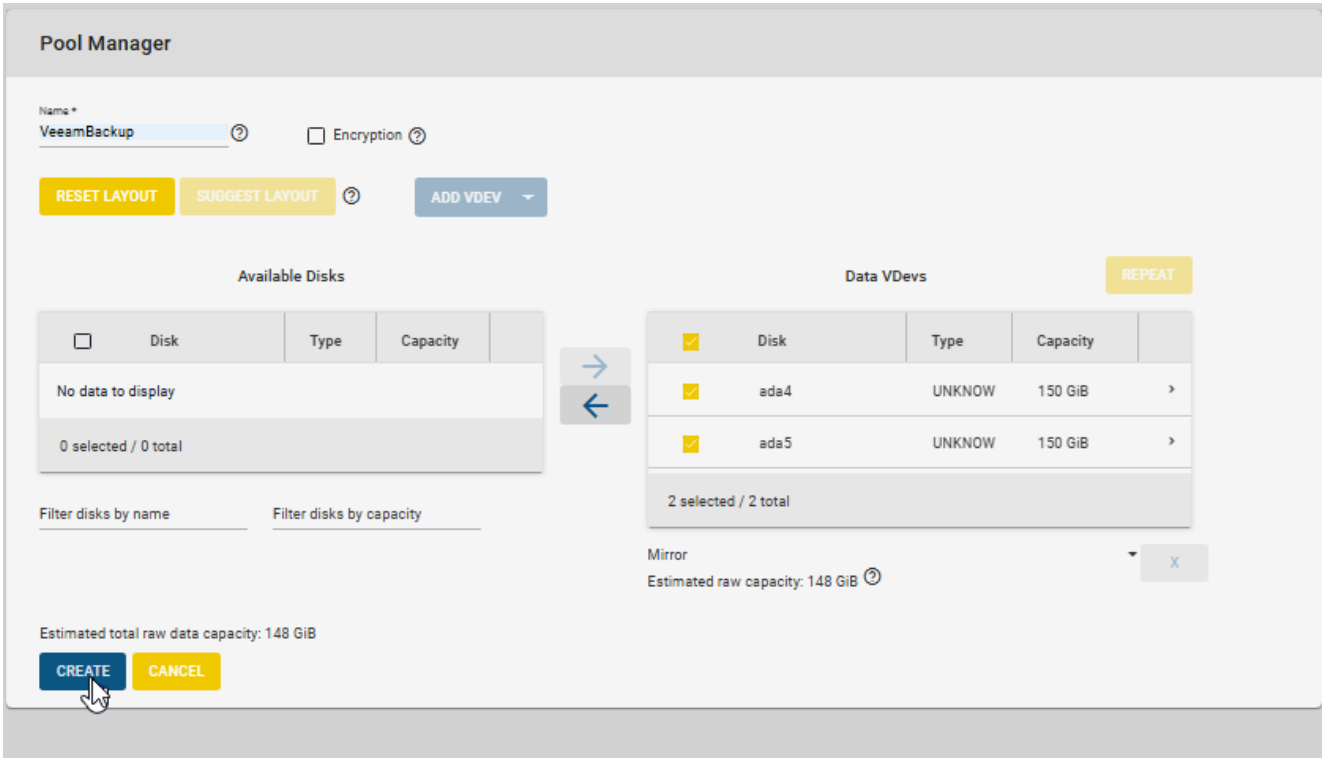
Durant l'installation, je créer une nouvelle pool pour partager les sauvegardes via SMB sur TrueNAS :
Je rajoute 2 disques virtuel de 150G

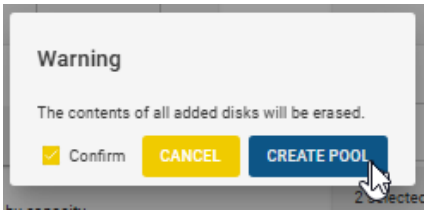


Création de la pool dans Storage > Pools > Add

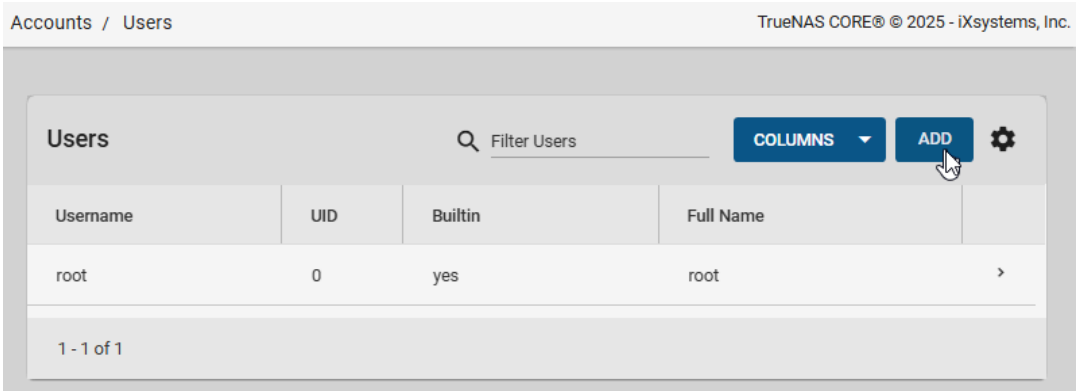




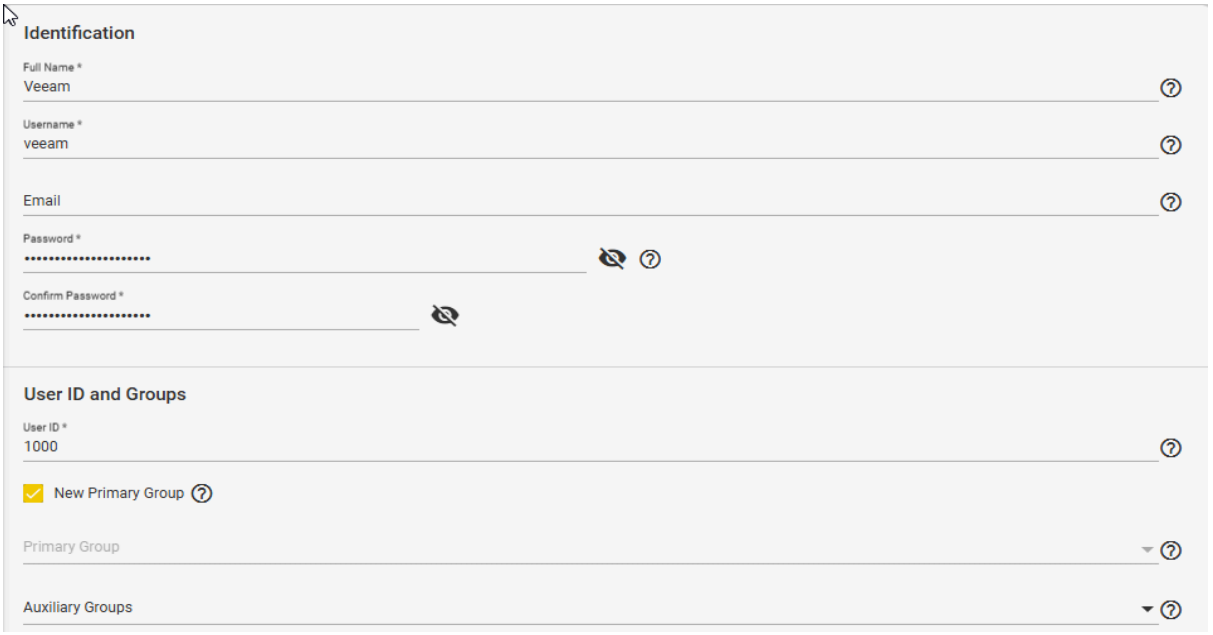




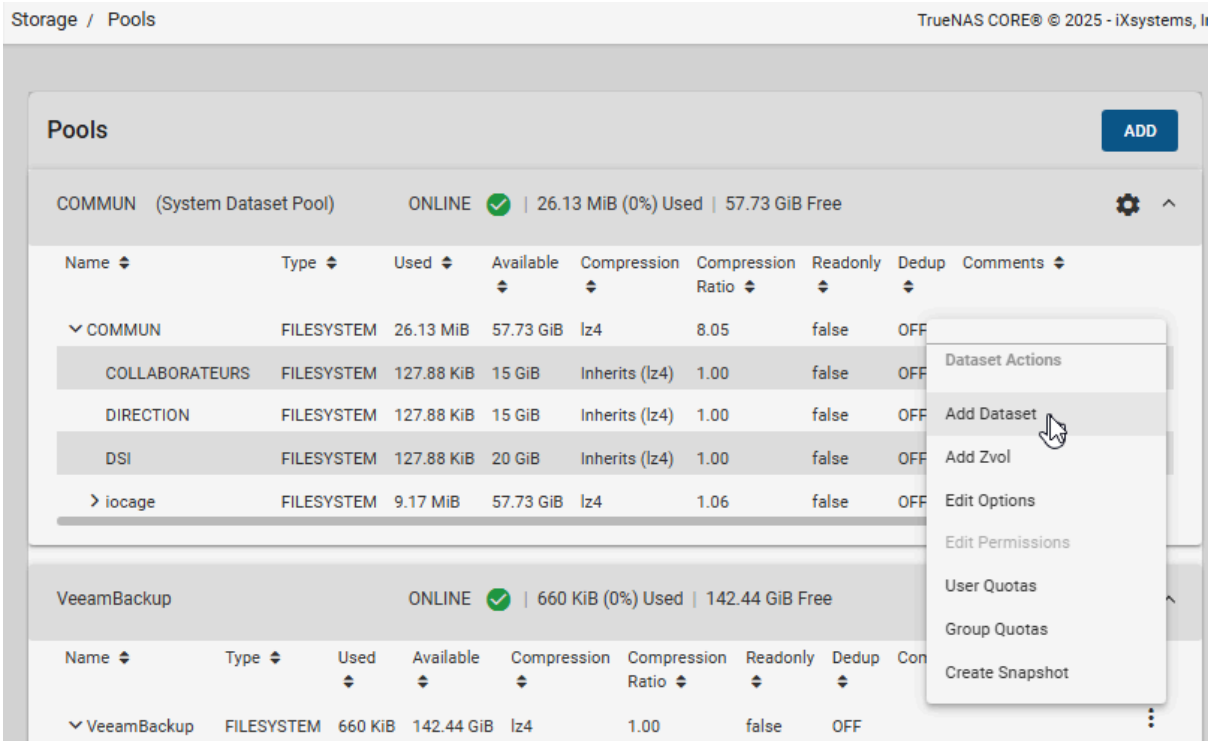
Pour des raisons de sécurité, je configure un utilisateur qui pourra avoir accès au dossier :
Accounts > Users

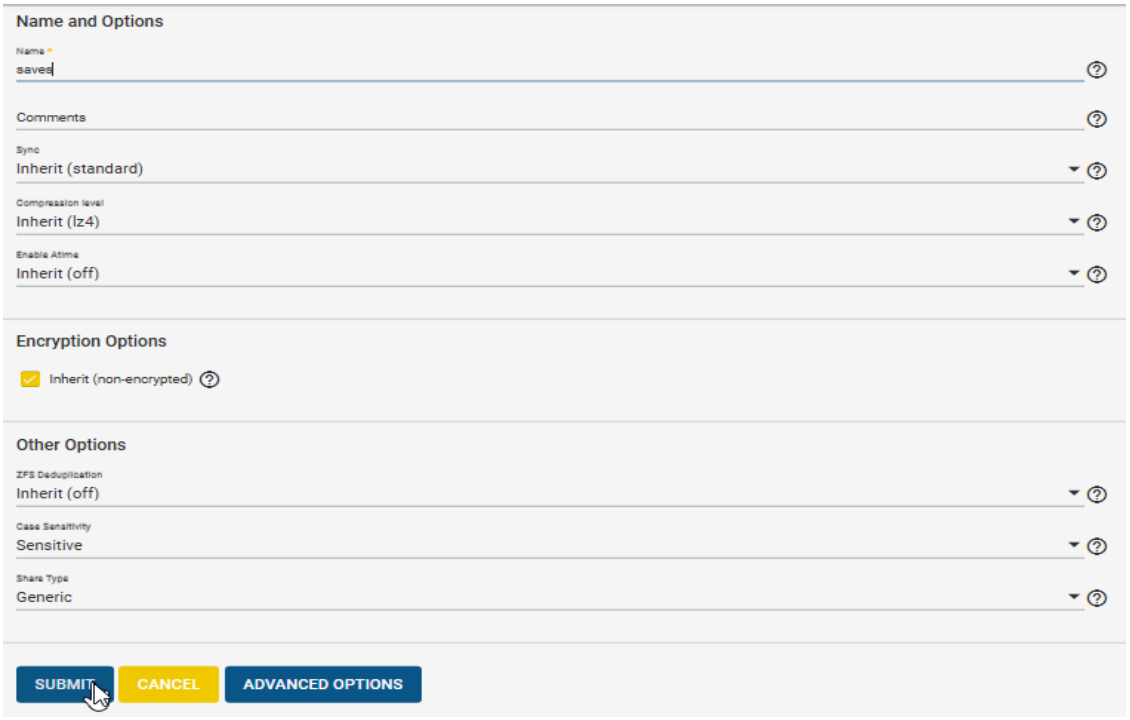


Je met un mot de passe sécurisé avec les recommandation de la ANSSI et je submit :

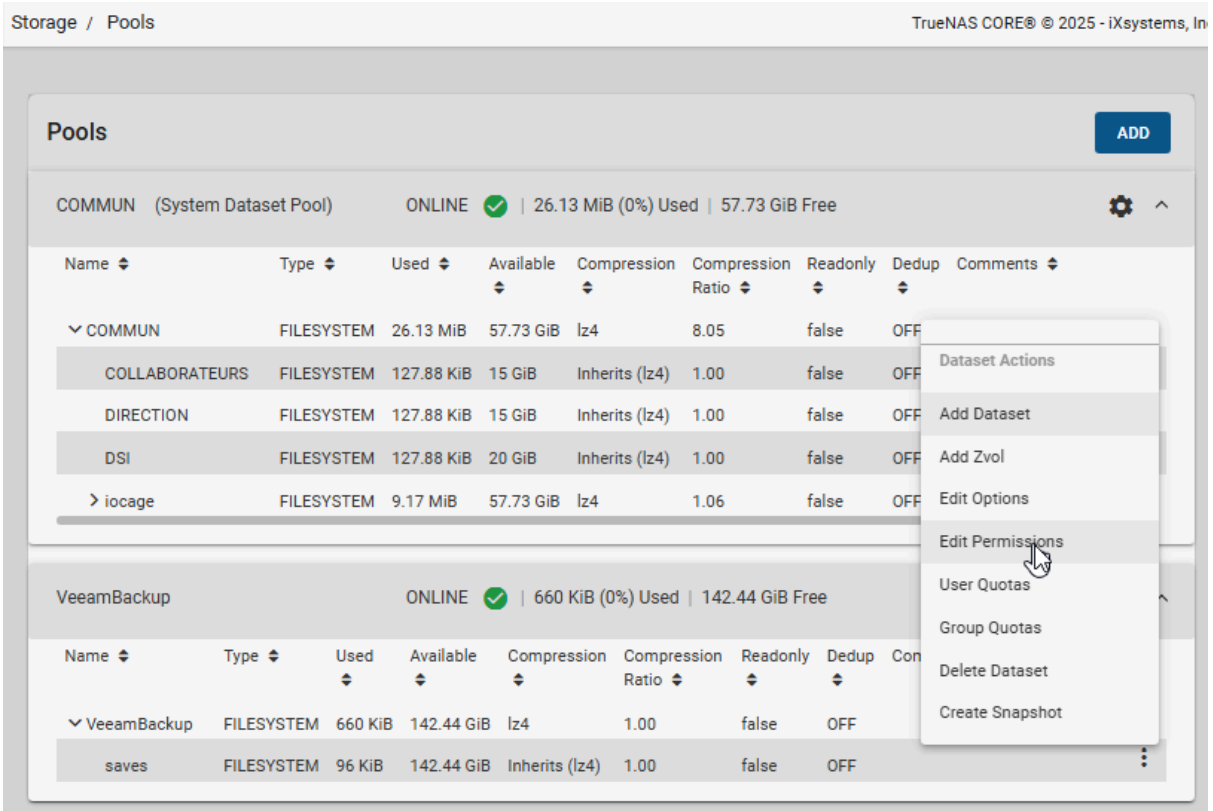


Maintenant je créer un dataset dans cette pool car nous ne pouvons pas changer les permissions d'une pool :
Storage > Pools > Plus d'options

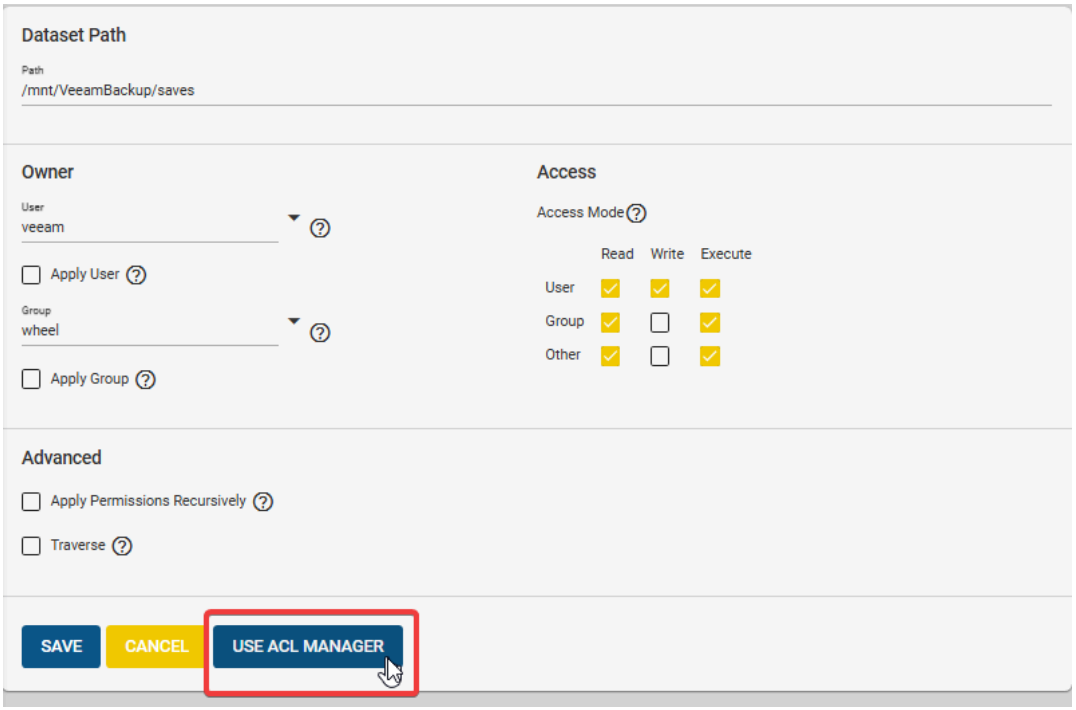


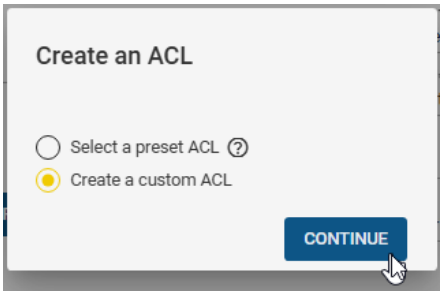


Maintenant je vais mettre le droit full control de notre utilisateur sur notre pool :
Storage > Pools > Veeam Backup > Plus d'options

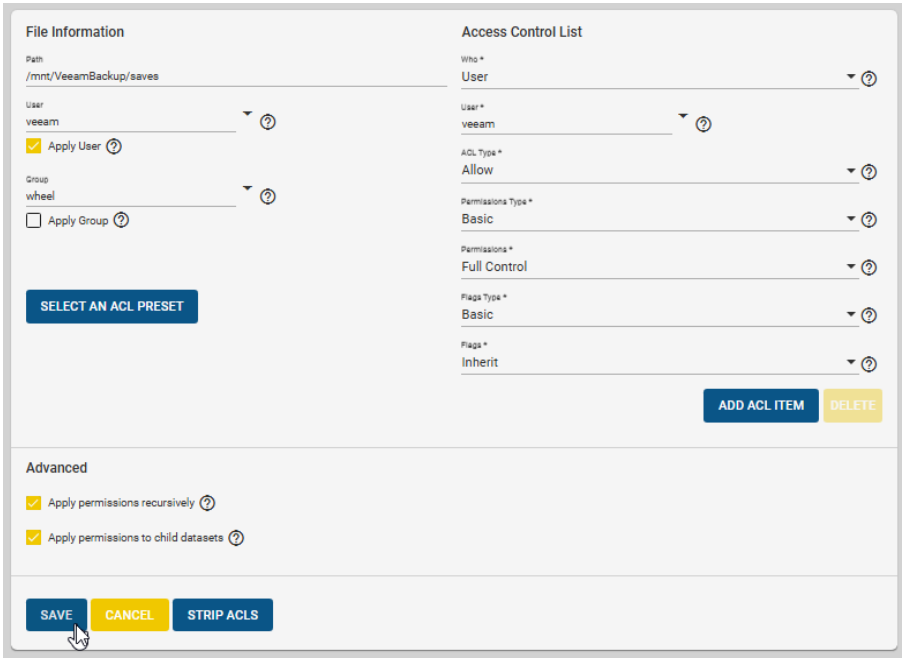


On ajoute l'utilisateur et on coche la case Apply User, puis on clique sur USE ACL MANAGER

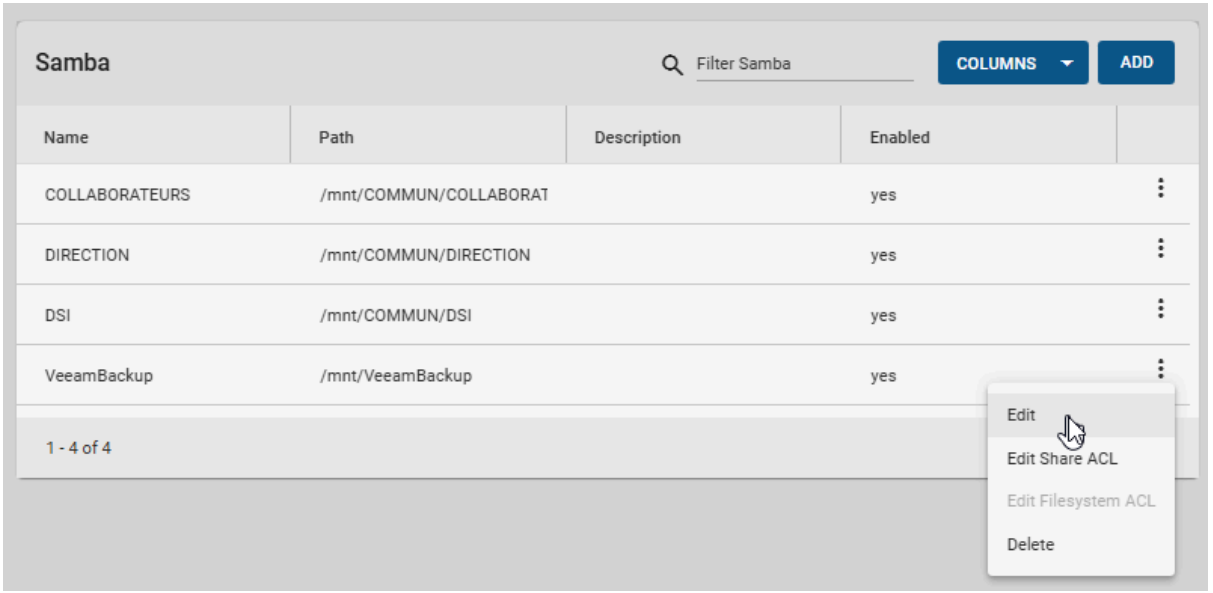


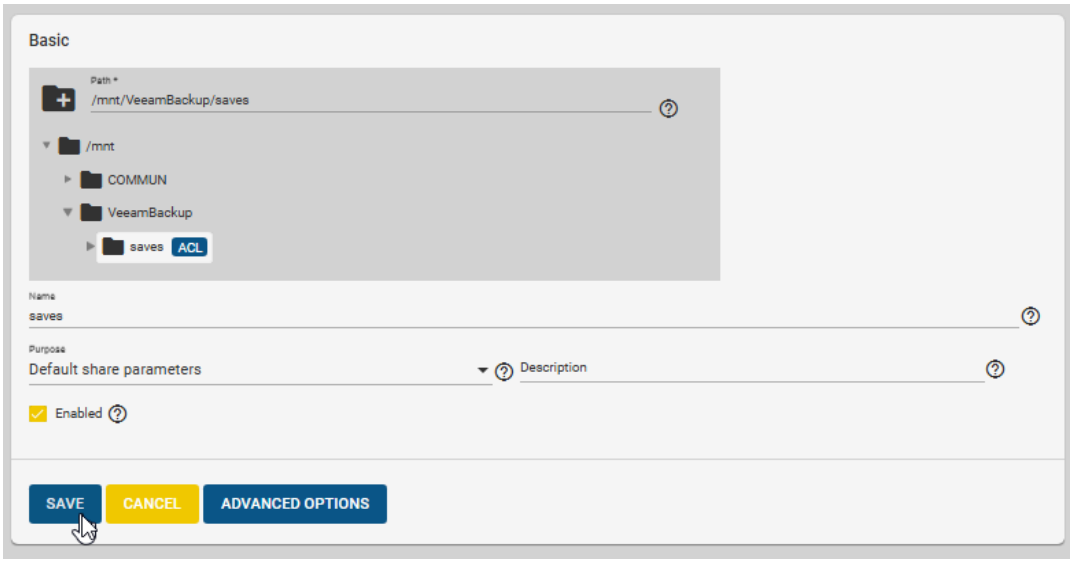


Puis dans les ACL on laisse que veeam en full control, flags Inherit, on coche la case Apply Permissions recursively et on save

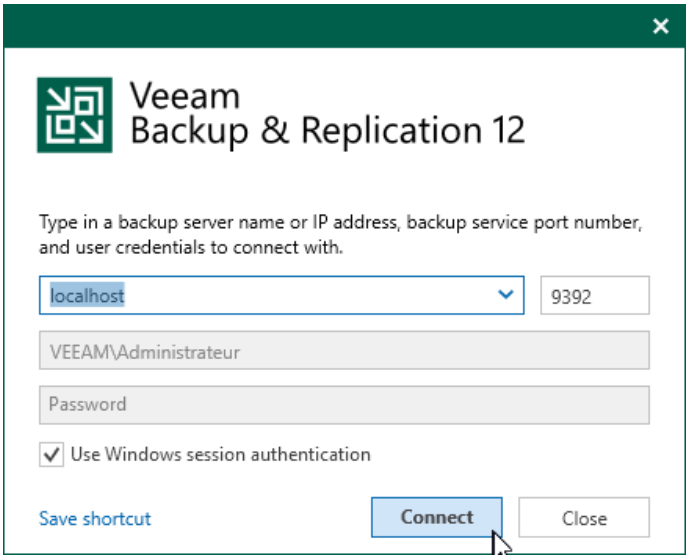


Création du partage : Sharing > SMB



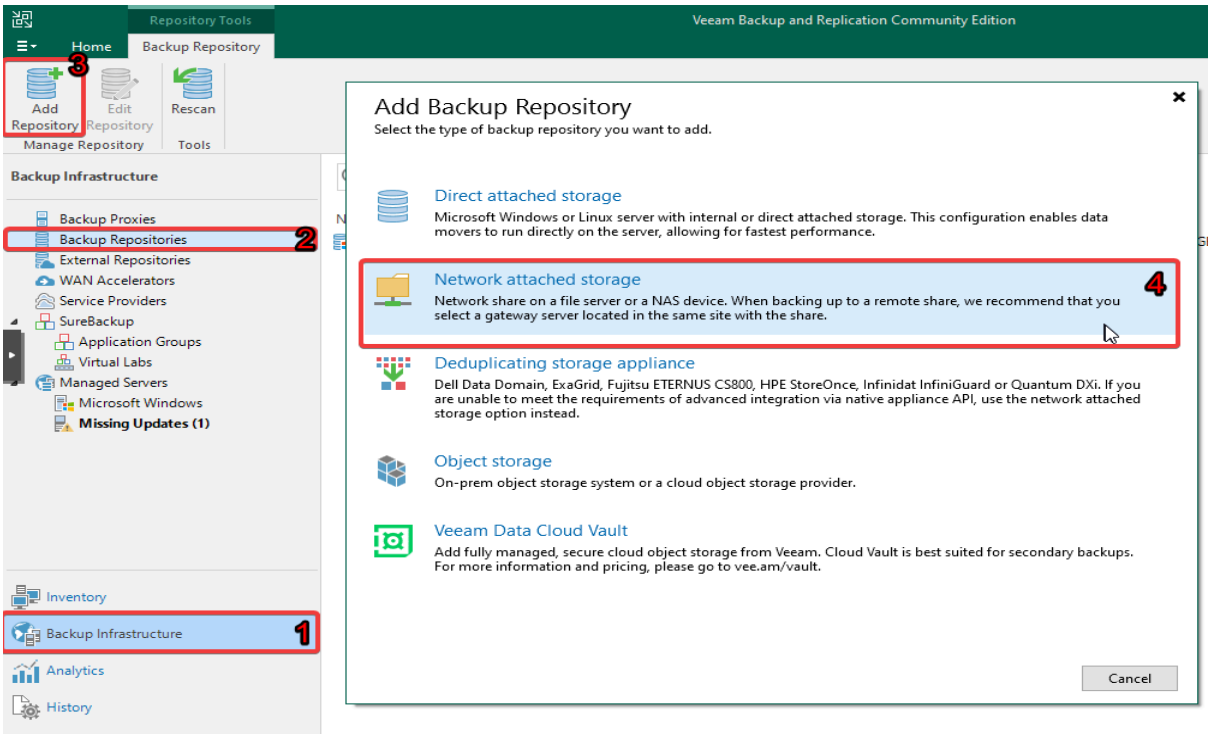


Après l'install, je lance la console Veeam, puis je me connecte :

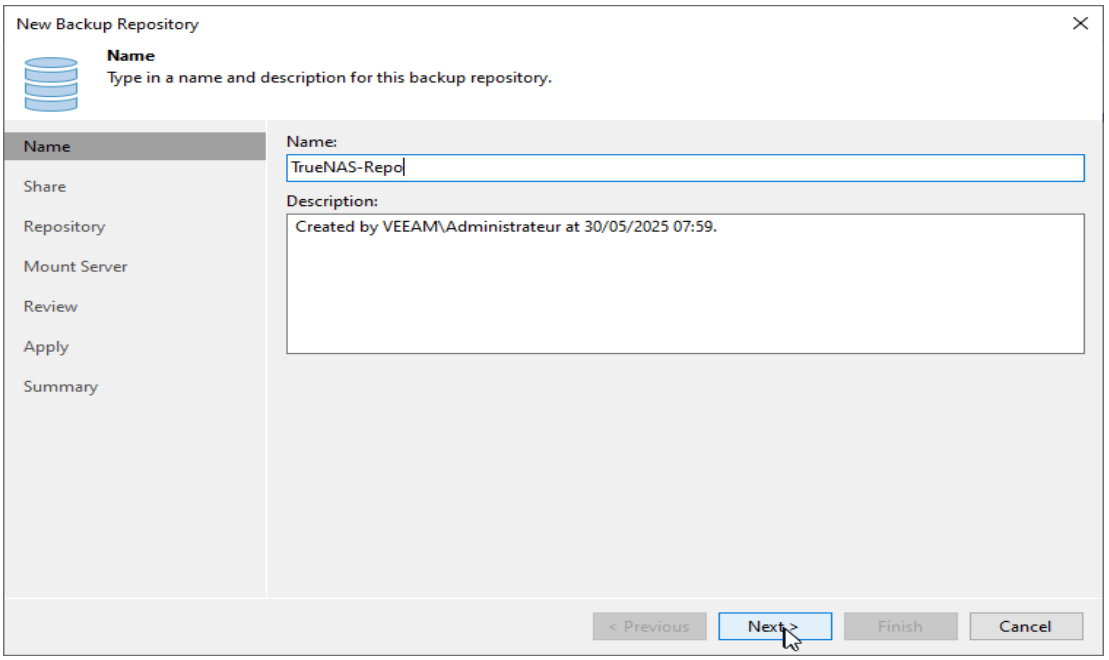


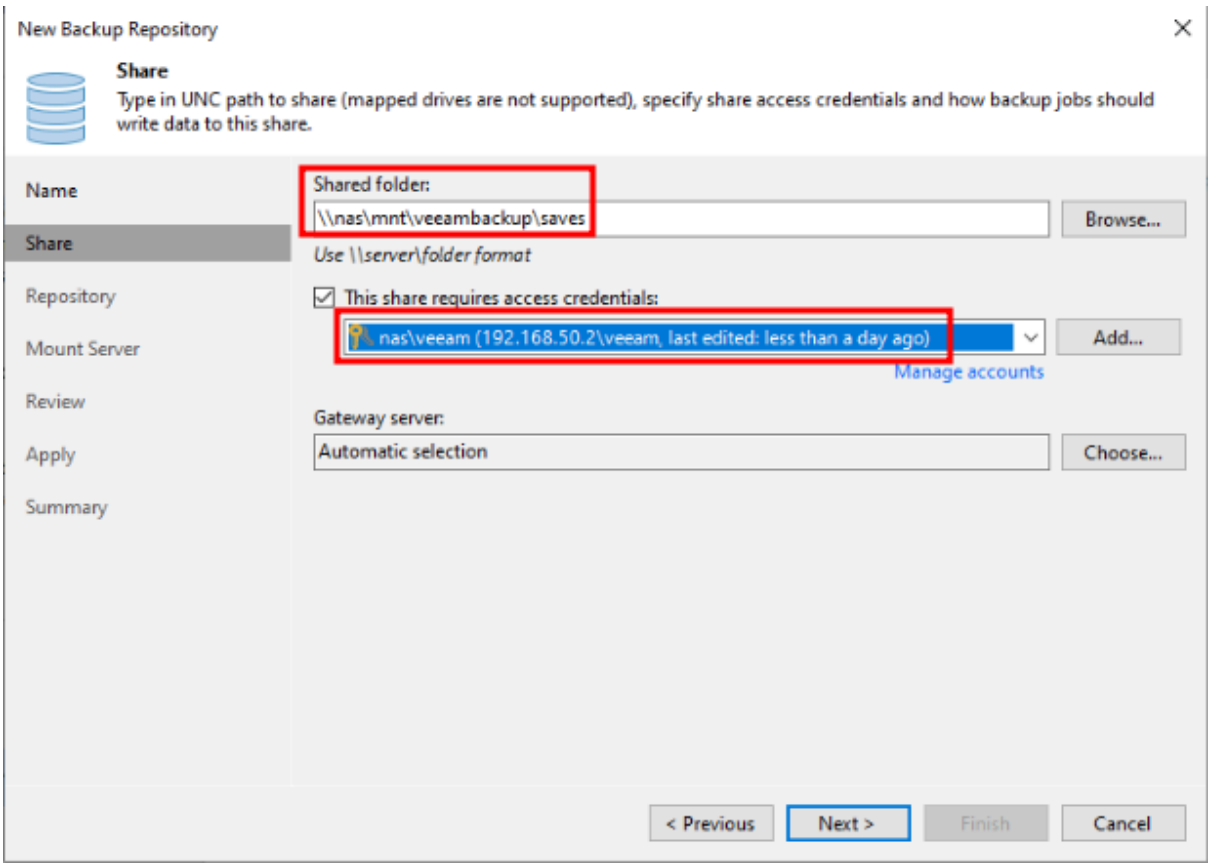
- Création de référentiel de sauvegarde et automatisation

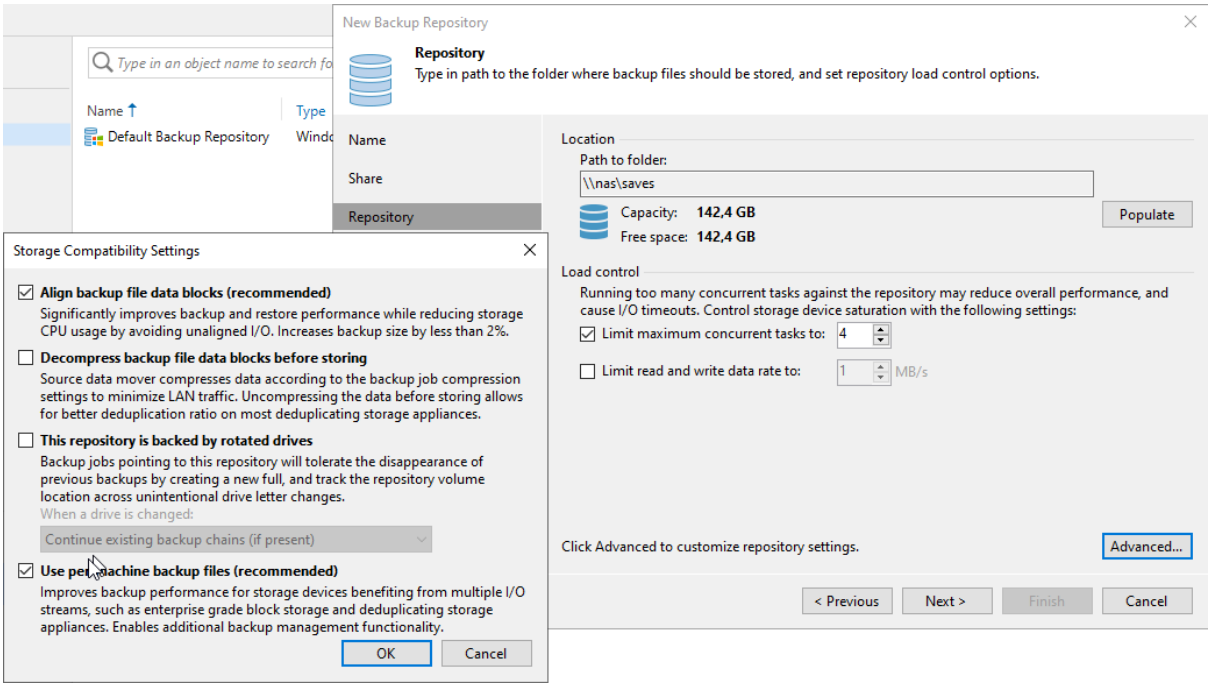
Une fois dans la console, nous allons ajouter un référentiel de sauvegarde, pour se faire, allez dans Backup Infrastructure > Backup repositories, cliquer sur Add repository et enfin Network attached storage.

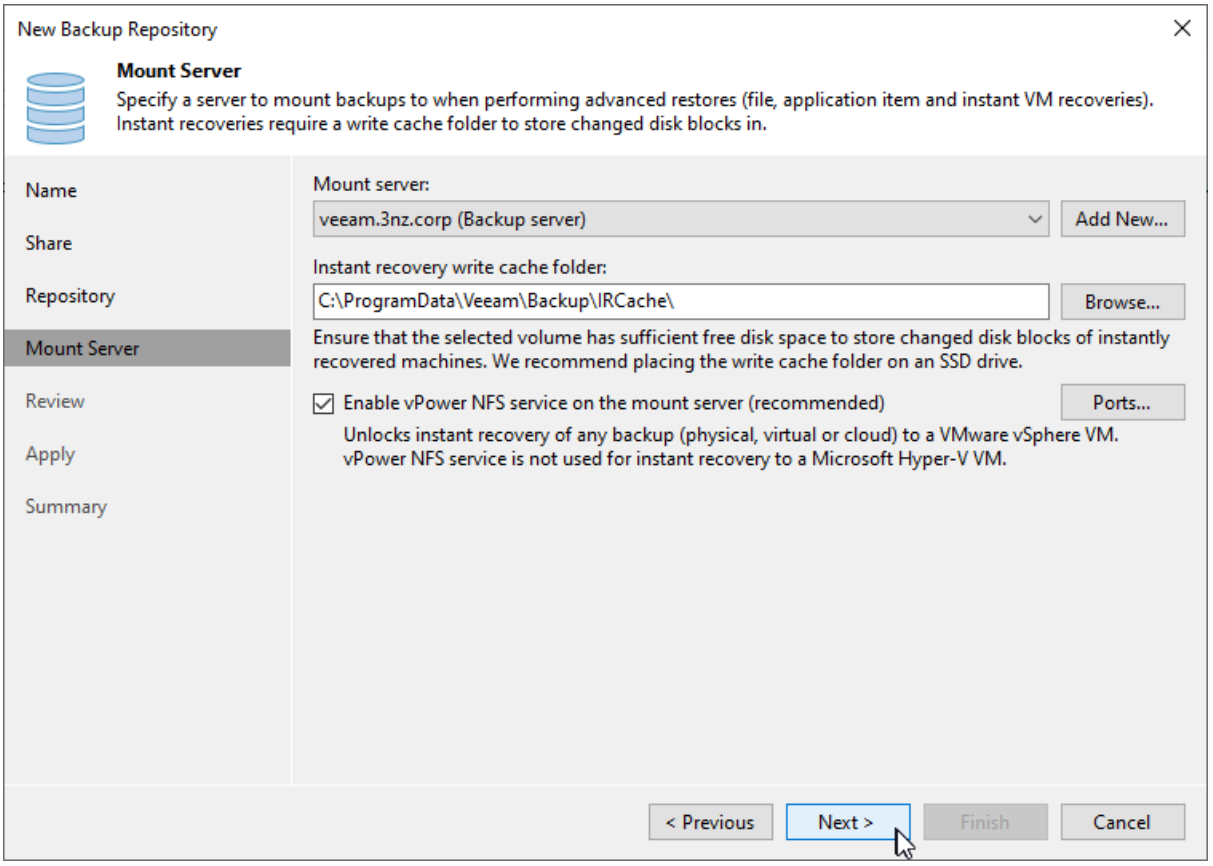


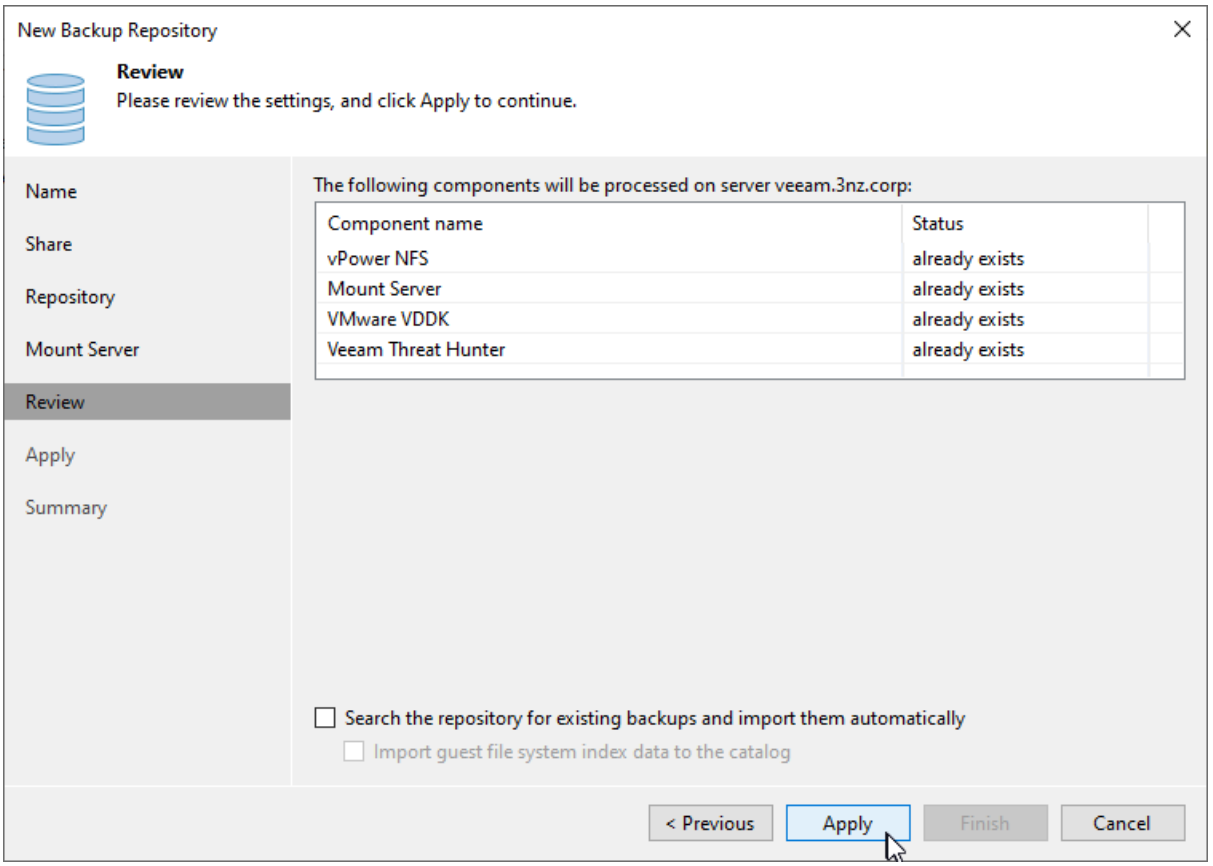
Modification du nom

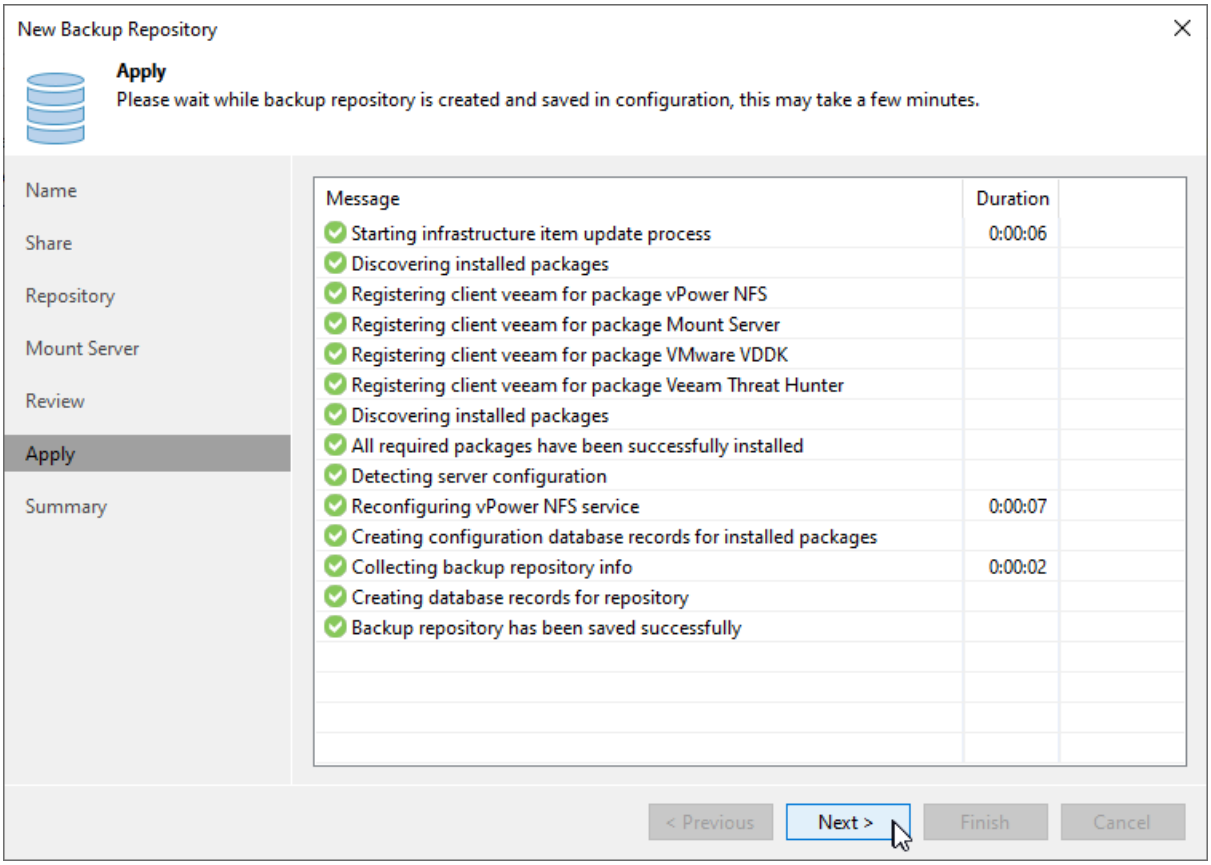


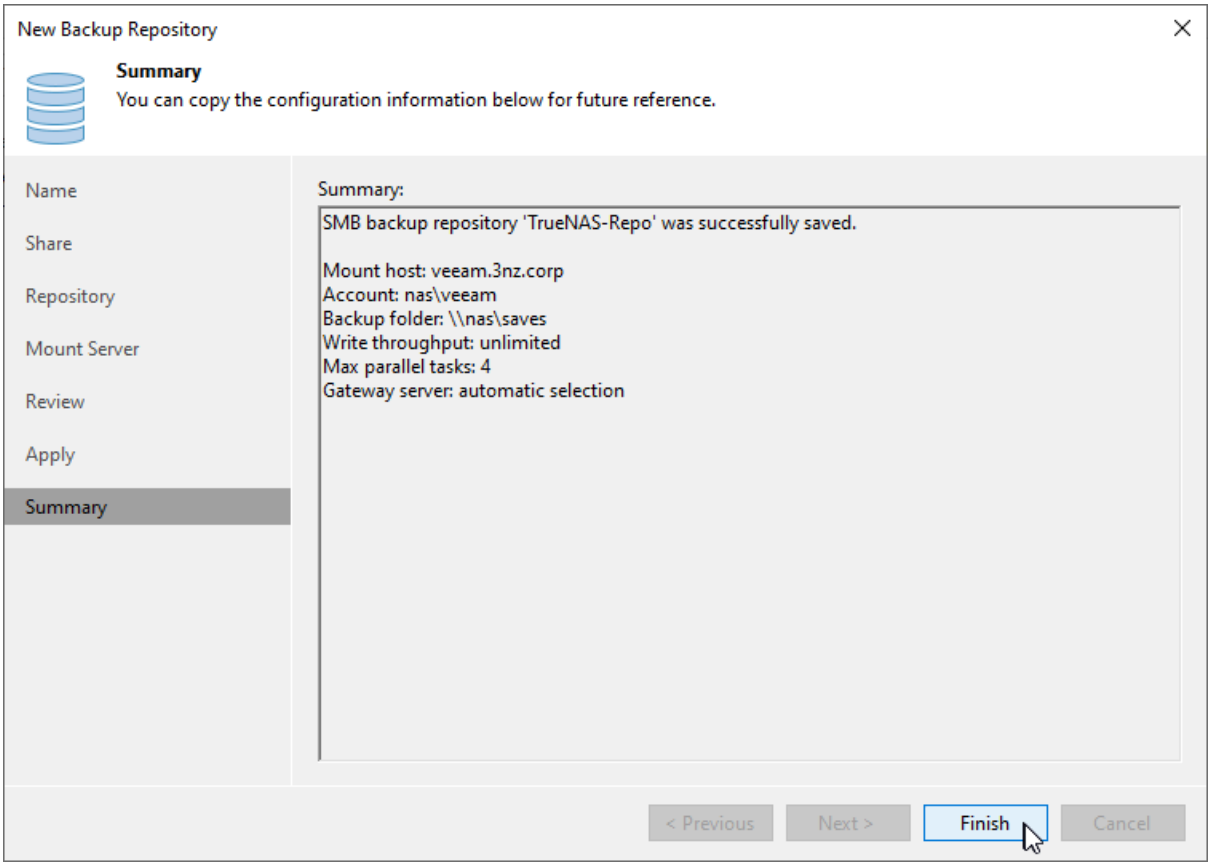

New Backup Repository
Share
Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Shared folder:
\\nas\mnt\veeambackup\saves
Browse...
Use \\server\folder format
This share requires access credentials:
nas\veeam (192.168.50.2\veeam, last edited: less than a day ago)
Add...
Manage accounts
Gateway server:
Automatic selection
Choose...
< Previous
Next >
Finish
Cancel

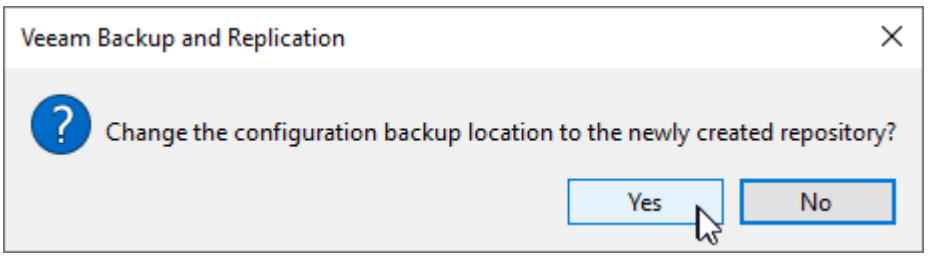

New Backup Repository
Repository
Type in path to the folder where backup files should be stored, and set repository load control options.
Name
Share
Repository
Location
Path to folder:
\\nas\saves
Capacity: 142,4 GB
Free space: 142,4 GB
Populate
Load control
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:
Limit maximum concurrent tasks to: 4
Limit read and write data rate to: 1 MB/s
Click Advanced to customize repository settings.
Advanced...
< Previous
Next >
Finish
Cancel
Storage Compatibility Settings
Align backup file data blocks (recommended)
Significantly improves backup and restore performance while reducing storage CPU usage by avoiding unaligned I/O. Increases backup size by less than 2%.
Decompress backup file data blocks before storing
Source data mover compresses data according to the backup job compression settings to minimize LAN traffic. Uncompressing the data before storing allows for better deduplication ratio on most deduplicating storage appliances.
This repository is backed by rotated drives
Backup jobs pointing to this repository will tolerate the disappearance of previous backups by creating a new full, and track the repository volume location across unintentional drive letter changes.
When a drive is changed:
Continue existing backup chains (if present)
Use per-machine backup files (recommended)
Improves backup performance for storage devices benefiting from multiple I/O streams, such as enterprise grade block storage and deduplicating storage appliances. Enables additional backup management functionality.
OK
Cancel


New Backup Repository
Mount Server
Specify a server to mount backups to when performing advanced restores (file, application item and instant VM recoveries). Instant recoveries require a write cache folder to store changed disk blocks in.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Mount server:
veeam.3nz.corp (Backup server)
Add New...
Instant recovery write cache folder:
C:\ProgramData\Veeam\Backup\IRCache\
Browse...
Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered machines. We recommend placing the write cache folder on an SSD drive.
Enable vPower NFS service on the mount server (recommended)
Ports...
Unlocks instant recovery of any backup (physical, virtual or cloud) to a VMware vSphere VM. vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.
< Previous
Next >
Finish
Cancel

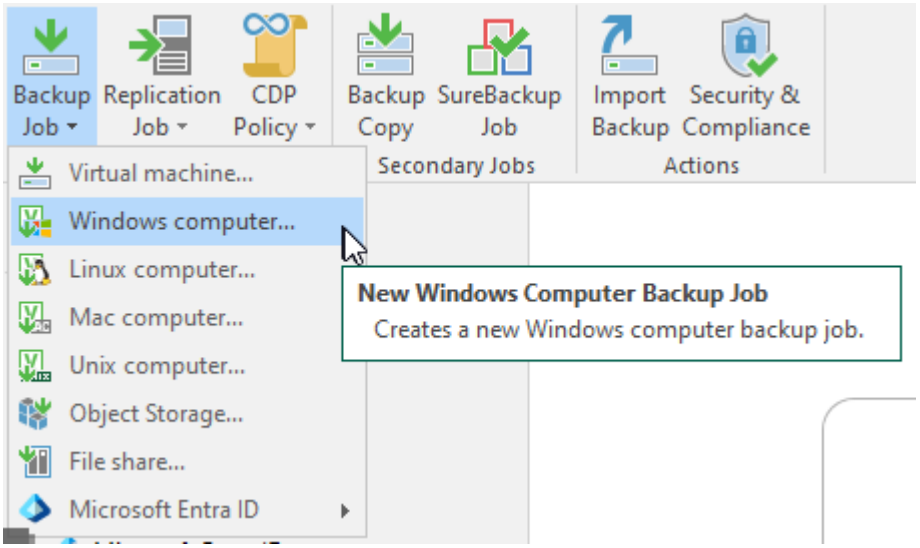

New Backup Repository
Review
Please review the settings, and click Apply to continue.
Name
Share
Repository
Mount Server
Review
Apply
Summary
The following components will be processed on server veeam.3nz.corp:
Component name
Status
vPower NFS
already exists
Mount Server
already exists
VMware VDDK
already exists
Veeam Threat Hunter
already exists
Search the repository for existing backups and import them automatically
Import guest file system index data to the catalog
< Previous
Apply
Finish
Cancel

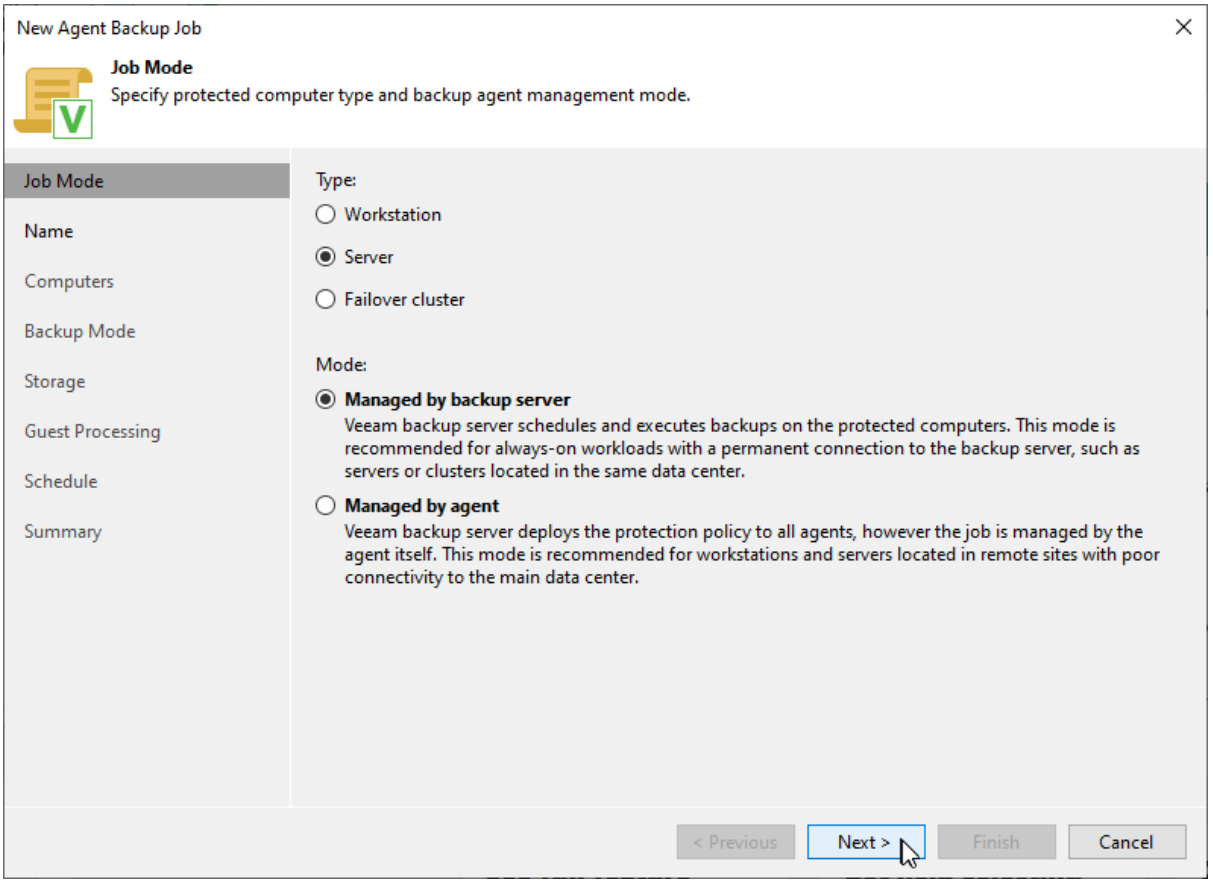

New Backup Repository
Apply
Please wait while backup repository is created and saved in configuration, this may take a few minutes.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Message
Duration
Starting infrastructure item update process
0:00:06
Discovering installed packages
Registering client veeam for package vPower NFS
Registering client veeam for package Mount Server
Registering client veeam for package VMware VDDK
Registering client veeam for package Veeam Threat Hunter
Discovering installed packages
All required packages have been successfully installed
Detecting server configuration
Reconfiguring vPower NFS service
0:00:07
Creating configuration database records for installed packages
Collecting backup repository info
0:00:02
Creating database records for repository
Backup repository has been saved successfully
< Previous
Next >
Finish
Cancel

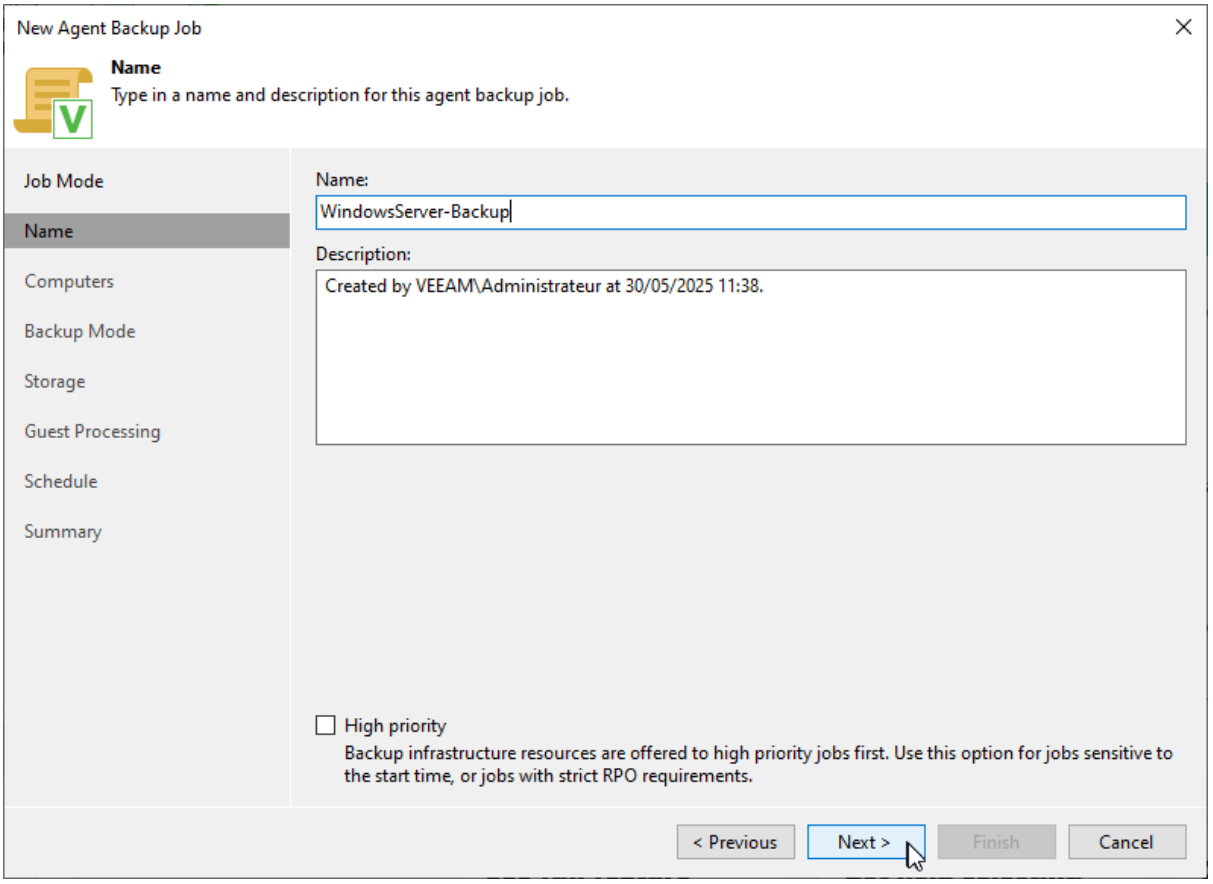

New Backup Repository
Summary
You can copy the configuration information below for future reference.
Name
Share
Repository
Mount Server
Review
Apply
Summary
Summary:
SMB backup repository 'TrueNAS-Repo' was successfully saved.
Mount host: veeam.3nz.corp
Account: nas\veeam
Backup folder: \\nas\saves
Write throughput: unlimited
Max parallel tasks: 4
Gateway server: automatic selection
< Previous
Next >
Finish
Cancel

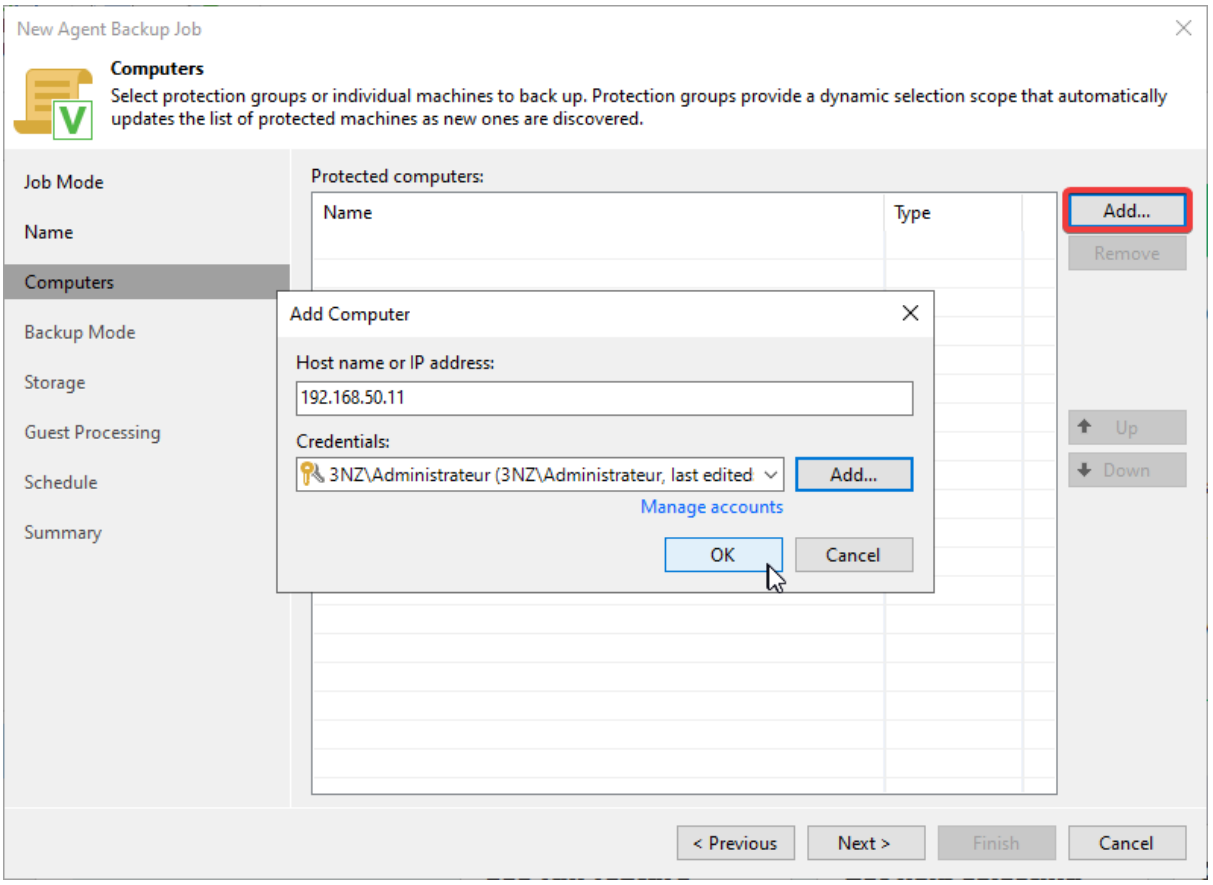


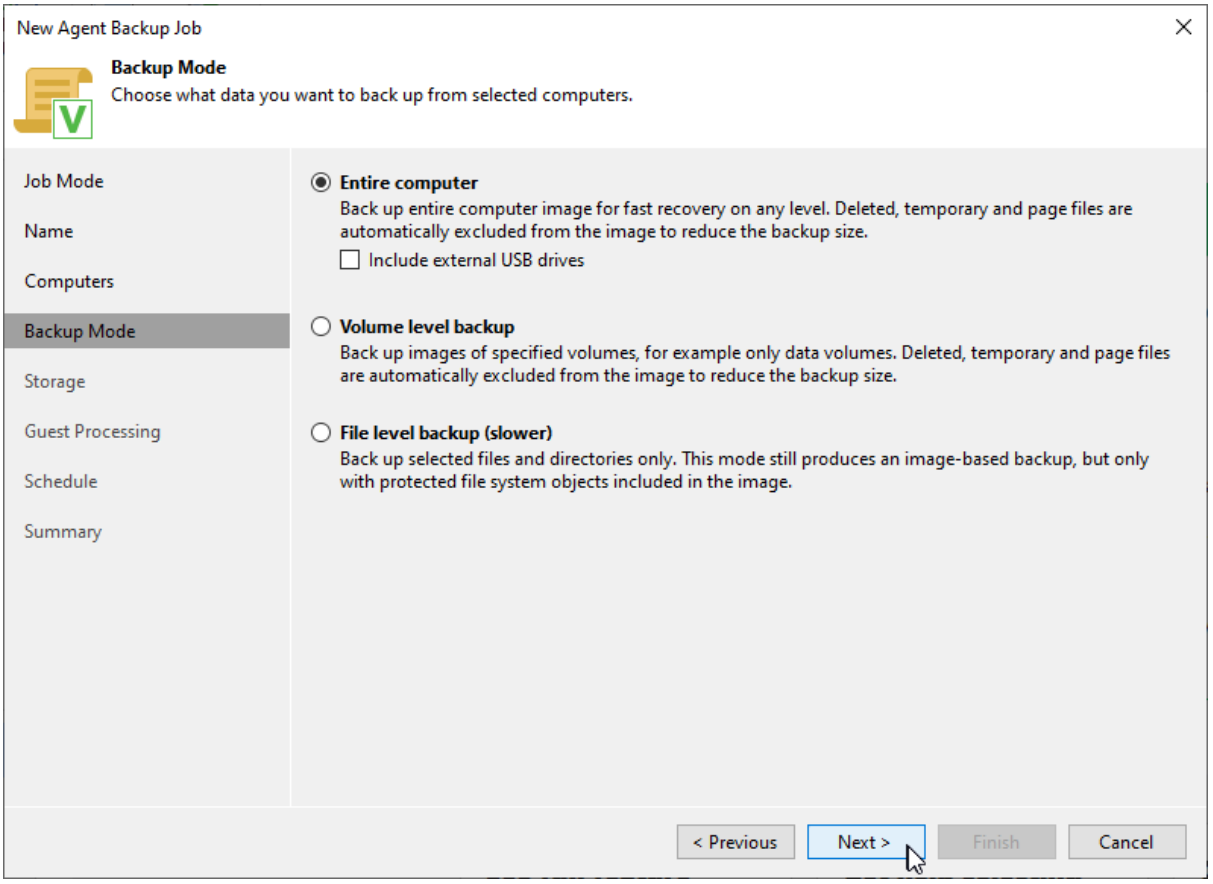
Configuration de la tâche de sauvegarde :
Dans la console Veeam > Backup Job > Windows Computer

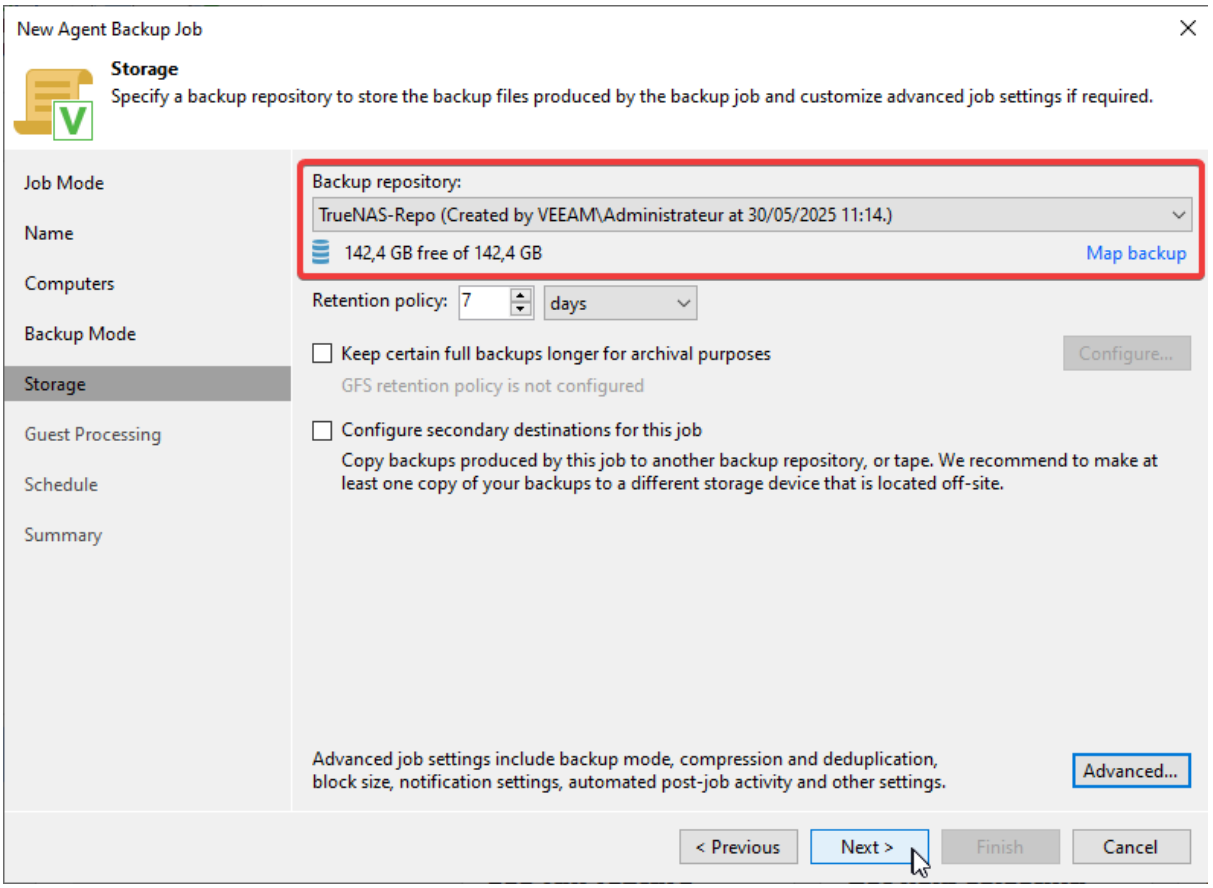


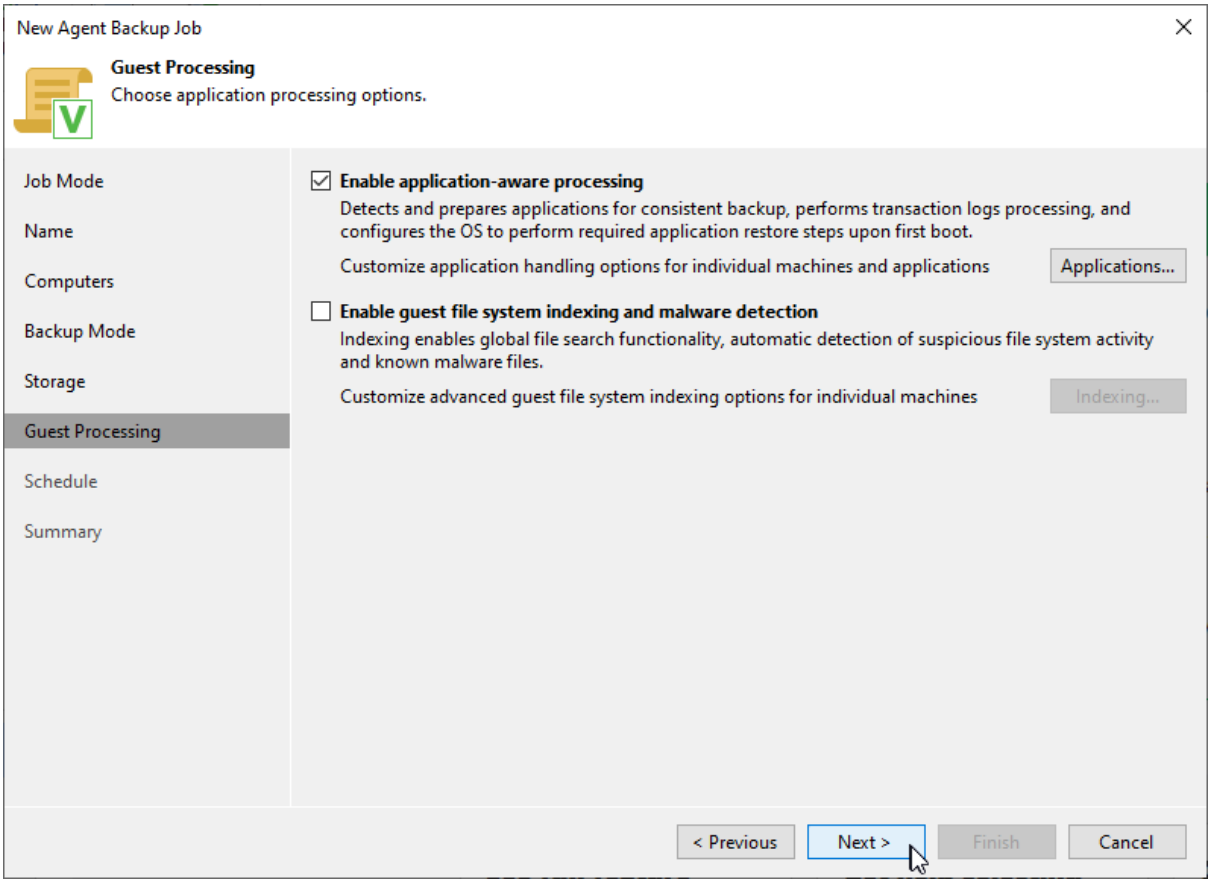


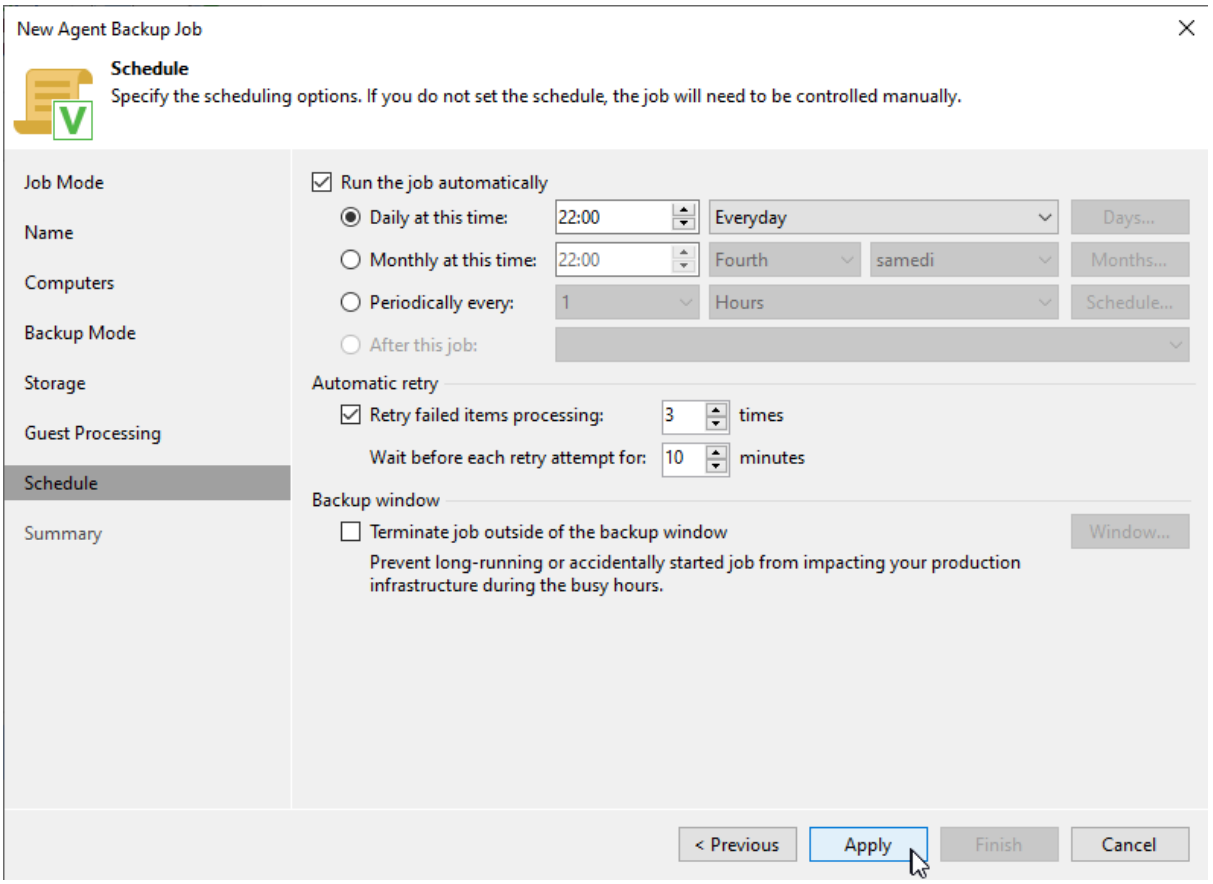

New Agent Backup Job
Name
Type in a name and description for this agent backup job.
Job Mode
Name
Computers
Backup Mode
Storage
Guest Processing
Schedule
Summary
Name:
WindowsServer-Backup
Description:
Created by VEEAM\Administrateur at 30/05/2025 11:38.
High priority
Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.
< Previous
Next >
Finish
Cancel

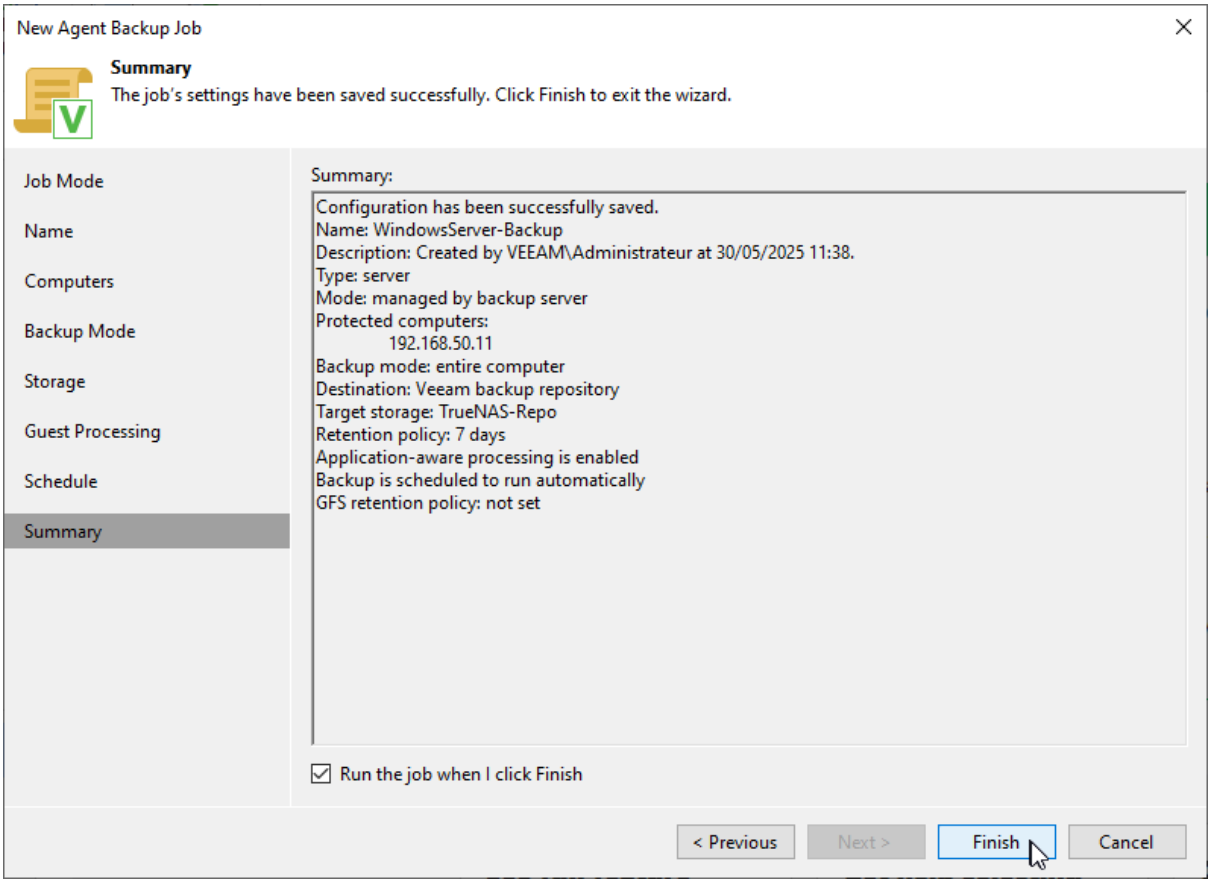

New Agent Backup Job
Computers
Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.
Job Mode
Name
Computers
Backup Mode
Storage
Guest Processing
Schedule
Summary
Protected computers:
Name
Type
Add...
Remove
Up
Down
Add Computer
Host name or IP address:
192.168.50.11
Credentials:
3NZ\Administrateur (3NZ\Administrateur, last edited
Add...
Manage accounts
OK
Cancel
< Previous
Next >
Finish
Cancel


New Agent Backup Job
Backup Mode
Choose what data you want to back up from selected computers.
Job Mode
Name
Computers
Backup Mode
Storage
Guest Processing
Schedule
Summary
Entire computer
Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
Include external USB drives
Volume level backup
Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
File level backup (slower)
Back up selected files and directories only. This mode still produces an image-based backup, but only with protected file system objects included in the image.
< Previous
Next >
Finish
Cancel

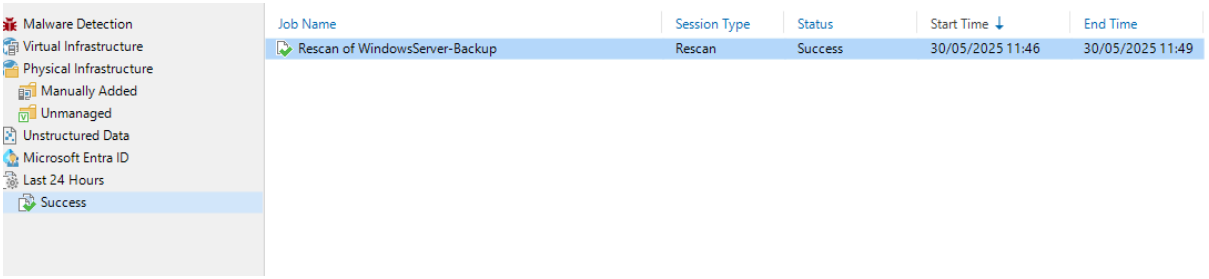

New Agent Backup Job
Storage
Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.
Job Mode
Name
Computers
Backup Mode
Storage
Guest Processing
Schedule
Summary
Backup repository:
TrueNAS-Repo (Created by VEEAM\Administrateur at 30/05/2025 11:14.)
142,4 GB free of 142,4 GB
Map backup
Retention policy: 7 days
Keep certain full backups longer for archival purposes
Configure...
GFS retention policy is not configured
Configure secondary destinations for this job
Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.
Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.
Advanced...
< Previous
Next >
Finish
Cancel


New Agent Backup Job
Guest Processing
Choose application processing options.
Job Mode
Name
Computers
Backup Mode
Storage
Guest Processing
Schedule
Summary
Enable application-aware processing
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.
Customize application handling options for individual machines and applications
Applications...
Enable guest file system indexing and malware detection
Indexing enables global file search functionality, automatic detection of suspicious file system activity and known malware files.
Customize advanced guest file system indexing options for individual machines
Indexing...
< Previous
Next >
Finish
Cancel

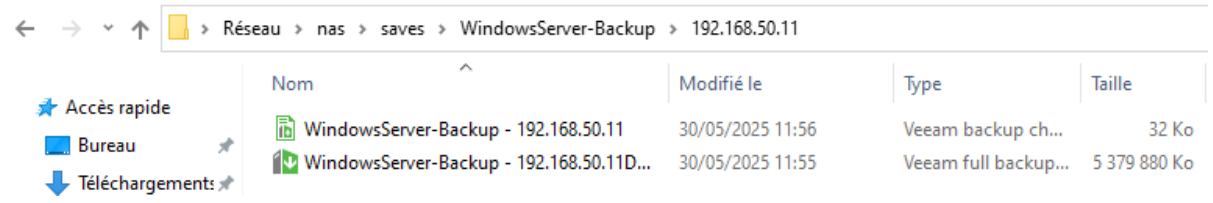

New Agent Backup Job
Schedule
Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.
Job Mode
Name
Computers
Backup Mode
Storage
Guest Processing
Schedule
Summary
Run the job automatically
Daily at this time:
22:00
Everyday
Days...
Monthly at this time:
22:00
Fourth
samedi
Months...
Periodically every:
1
Hours
Schedule...
After this job:
Automatic retry
Retry failed items processing:
3
times
Wait before each retry attempt for:
10
minutes
Backup window
Terminate job outside of the backup window
Window...
Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours.
< Previous
Apply
Finish
Cancel



La tâche c'est terminé :



La backup a bien été créé :



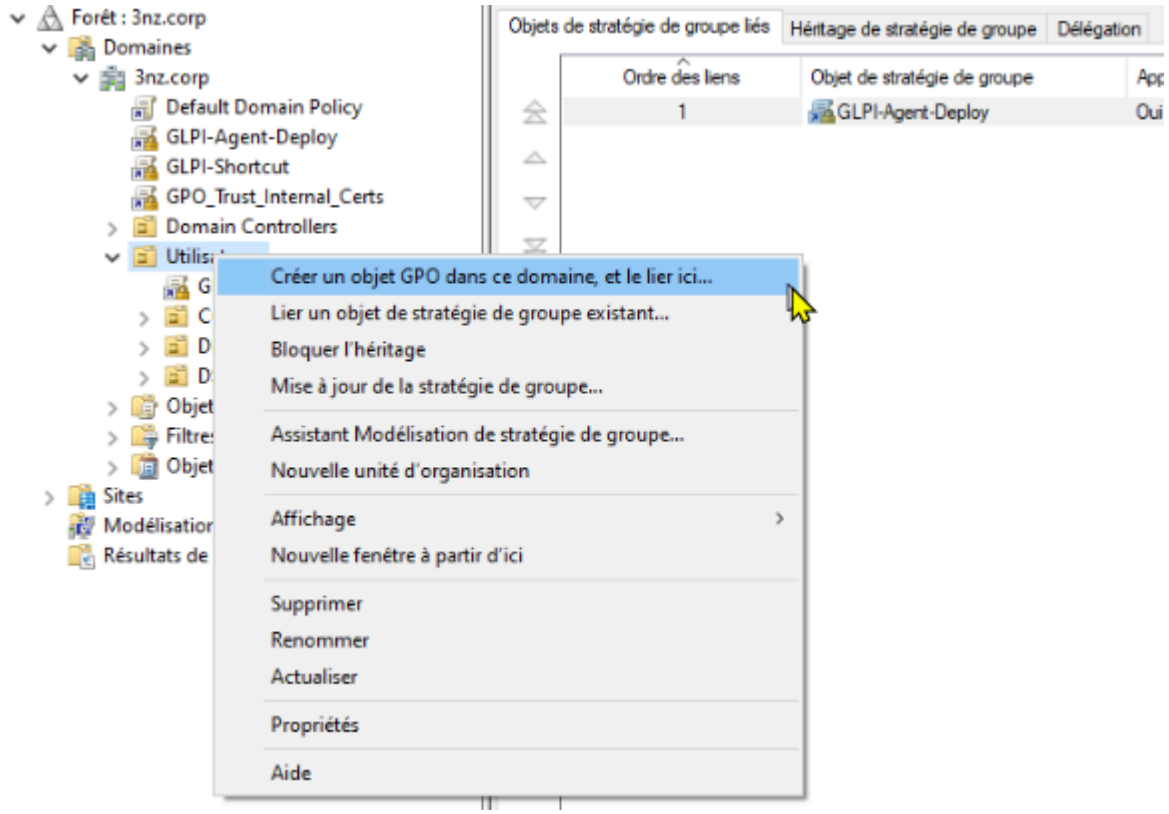
III. Durcissement de la Sécurité

Plan de mes GPO :

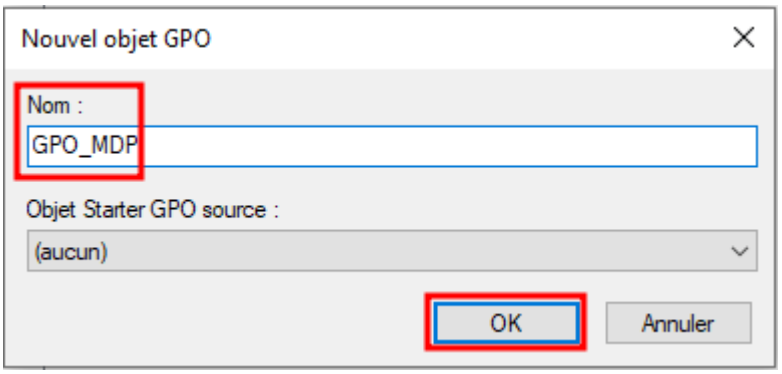
Domaine	**Paramètre (Chemin GPO)**	**Réglage Préconisé**	**Justification Professionnelle (BTS)**
Mots de passe	Longueur minimale du mot de passe	**12 caractères**	Protection contre le *Brute Force*. Augmente la complexité entropique nécessaire au décryptage.
Mots de passe	Durée de vie maximale du mdp	**365 jours**	Compromis entre sécurité et ergonomie. Limite l'usage d'un mot de passe potentiellement fuité.
Mots de passe	Historique des mots de passe	**10 derniers**	Empêche la rotation cyclique entre deux mots de passe identiques par l'utilisateur.
Accès CMD	Empêcher l'accès à l'invite de commande	**Désactivé**	Réduction de la surface d'attaque. Interdiction des outils de reconnaissance réseau.
Accès PowerShell	N'exécutez pas les applications spécifiées	**powershell.exe**	Bloque l'accès à l'interpréteur de scripts évolué, limitant l'exécution de malwares "fileless".
USB / Stockage	Disques amovibles : refus d'accès	**Activé**	Prévention de l'exfiltration de données (DLP) et protection contre les infections par périphériques (USB Killer, Virus).

- Politique de mots de passe

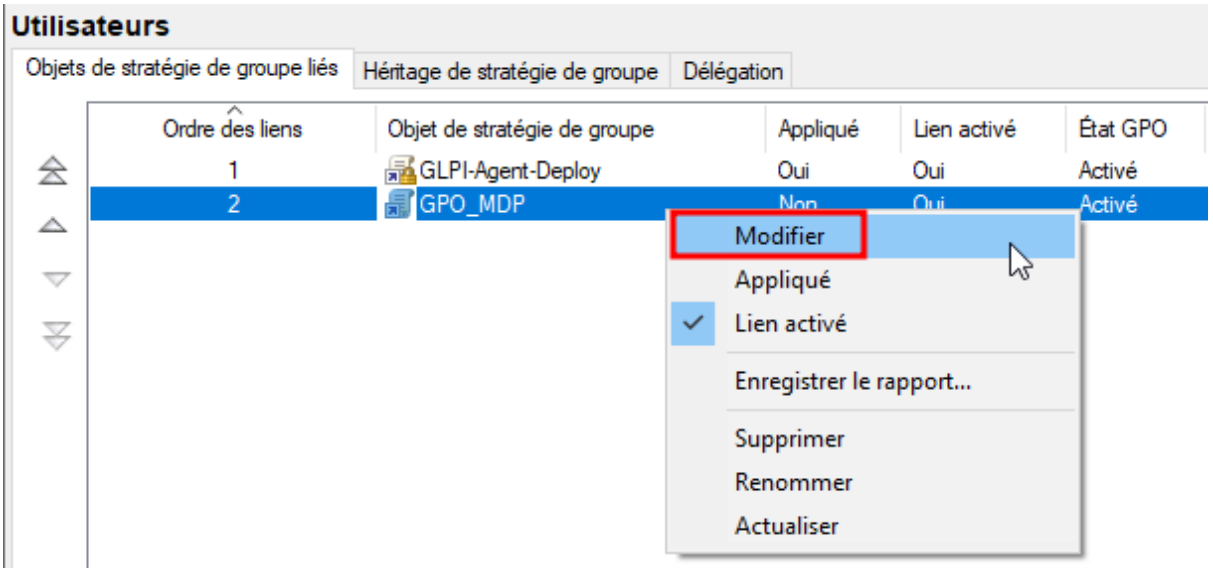
Création de la GPO pour la politique des mots de passe :



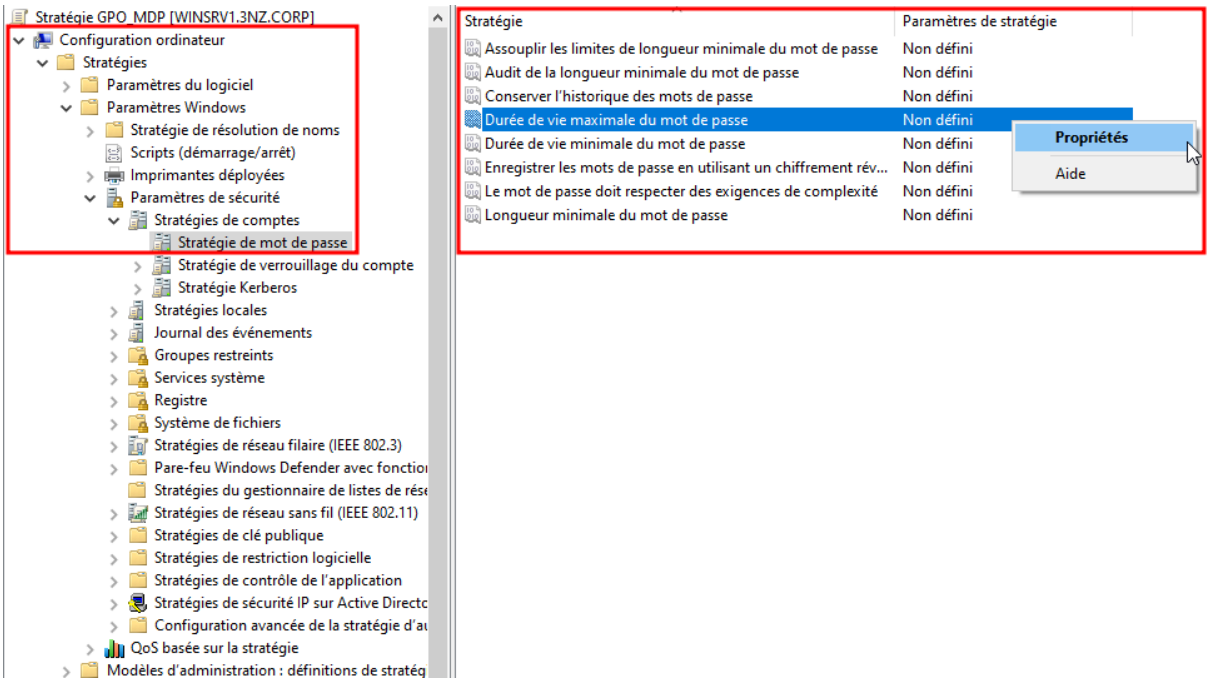
Je la nomme :



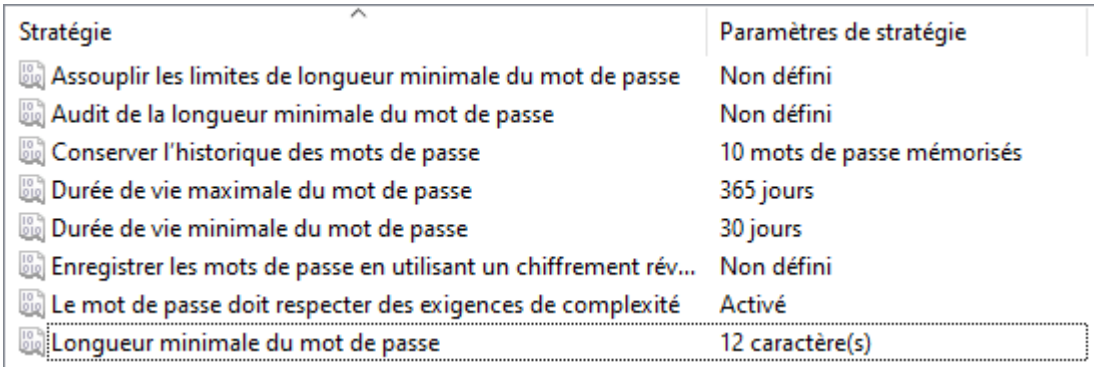
Une fois créée, clic droit, modifier :



Allez dans : `Configuration ordinateur` > `Paramètres Windows` > `Paramètres de sécurité` > `Stratégies de comptes` > `Stratégie de mots de passe`



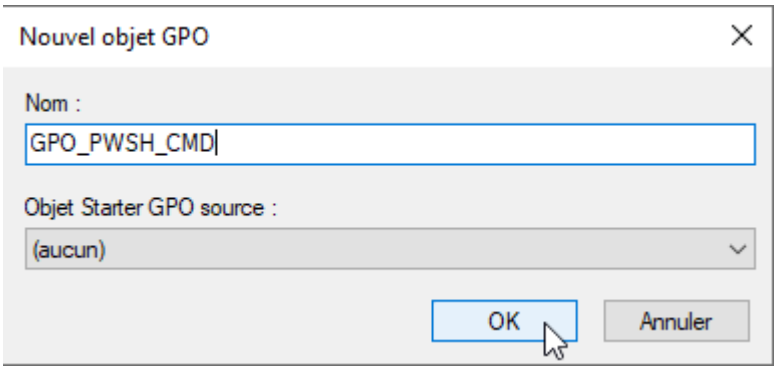
Voici donc, ma stratégie pour les mots de passe :

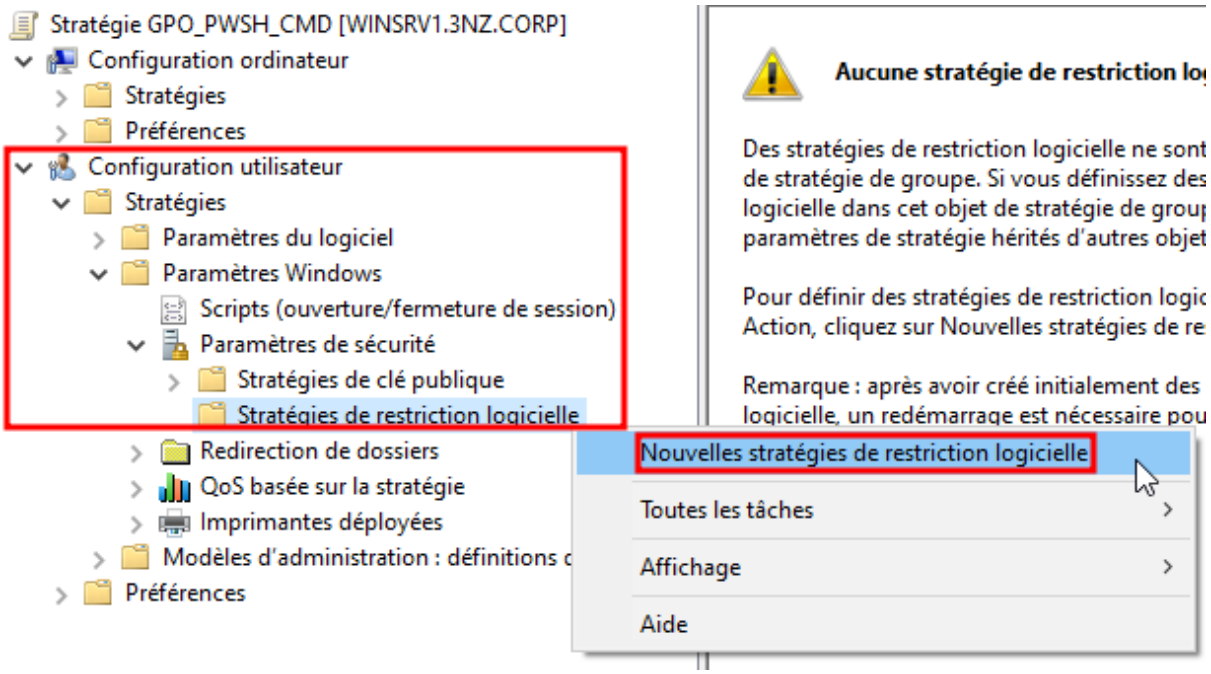


- Restriction des outils d’administration

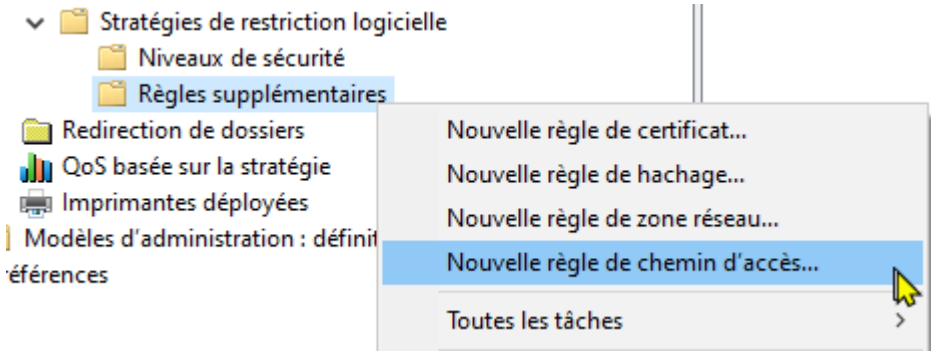
Blocage de PowerShell et de l’invite de commande CMD :

Création d’un GPO nommé GPO_PWSH_CMD puis modifier :

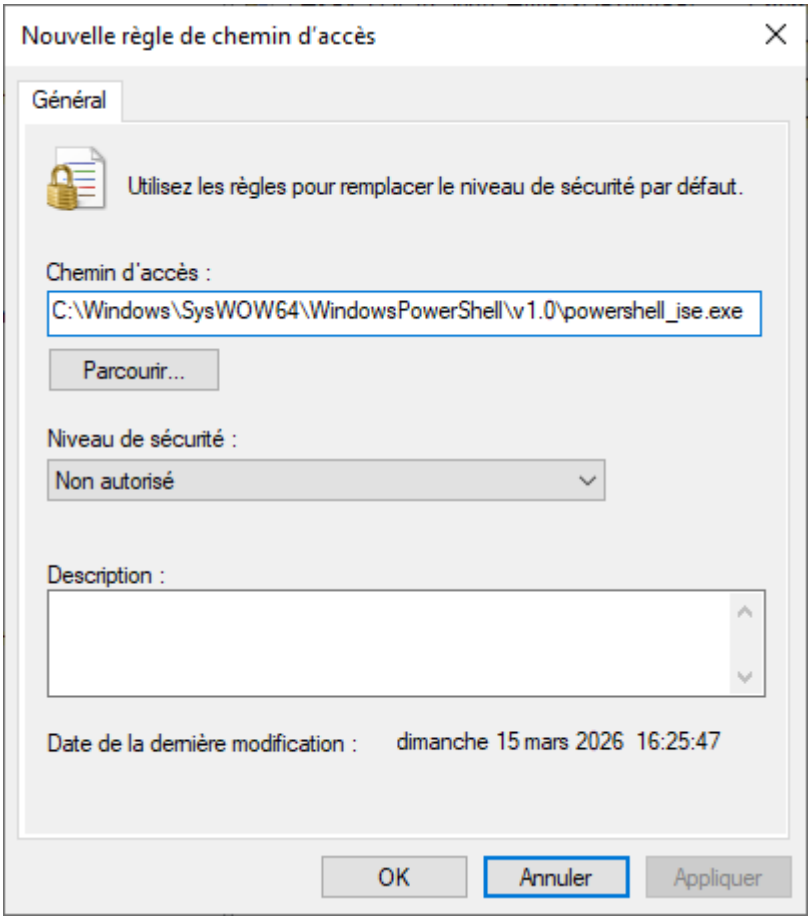




Ensuite, déployer Stratégies de restriction logicielle, puis clic droit sur Règles supplémentaires et cliquer sur Nouvelle règle de chemin d'accès… :



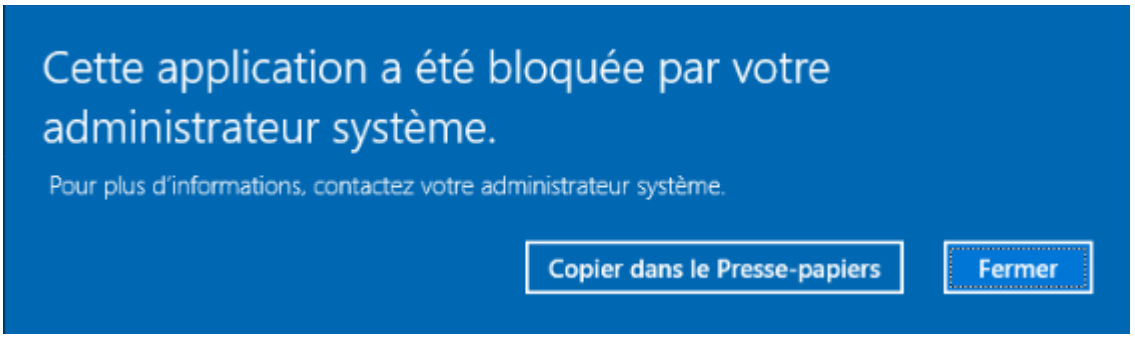
Parcourir jusqu'au chemin ou se trouve les .exe de powershell :



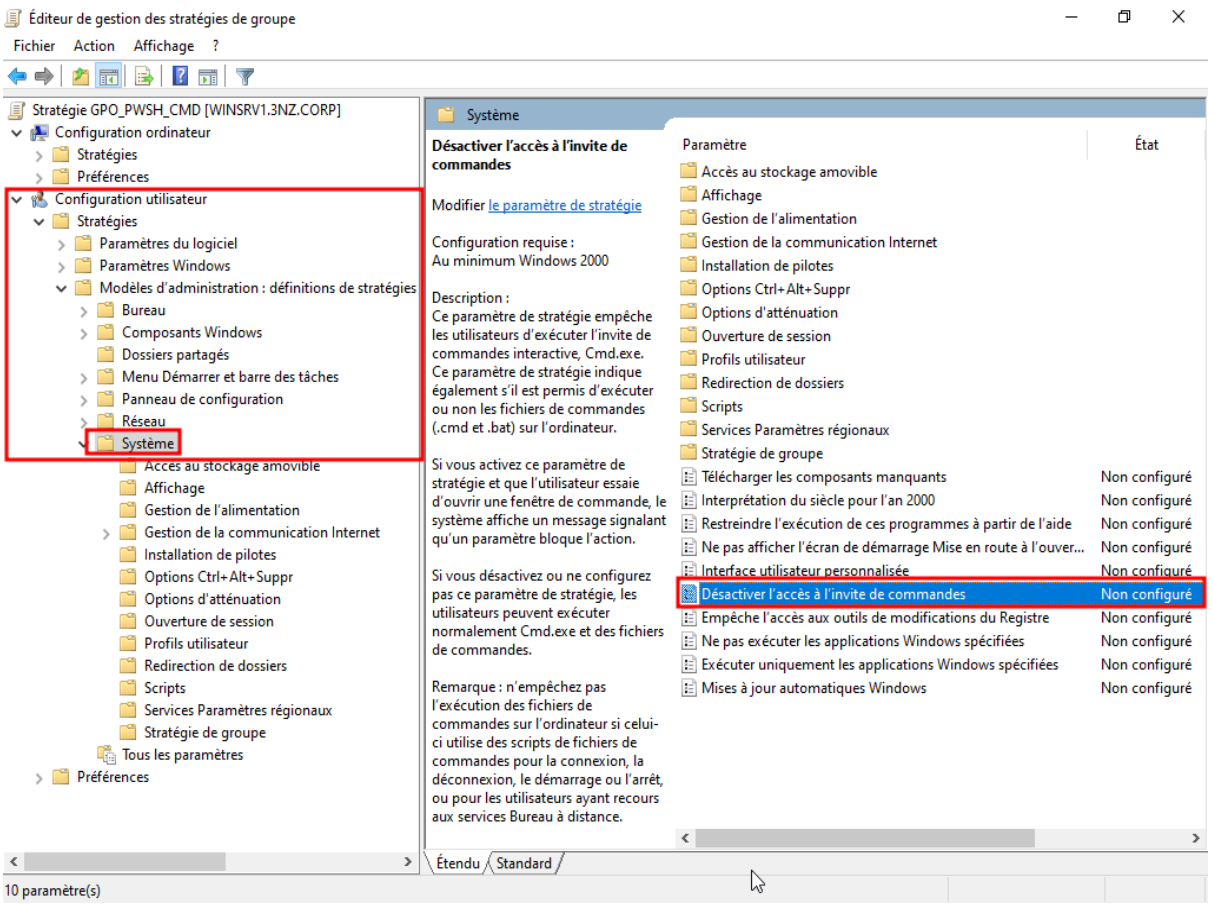
Il y a 4 emplacements :

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe

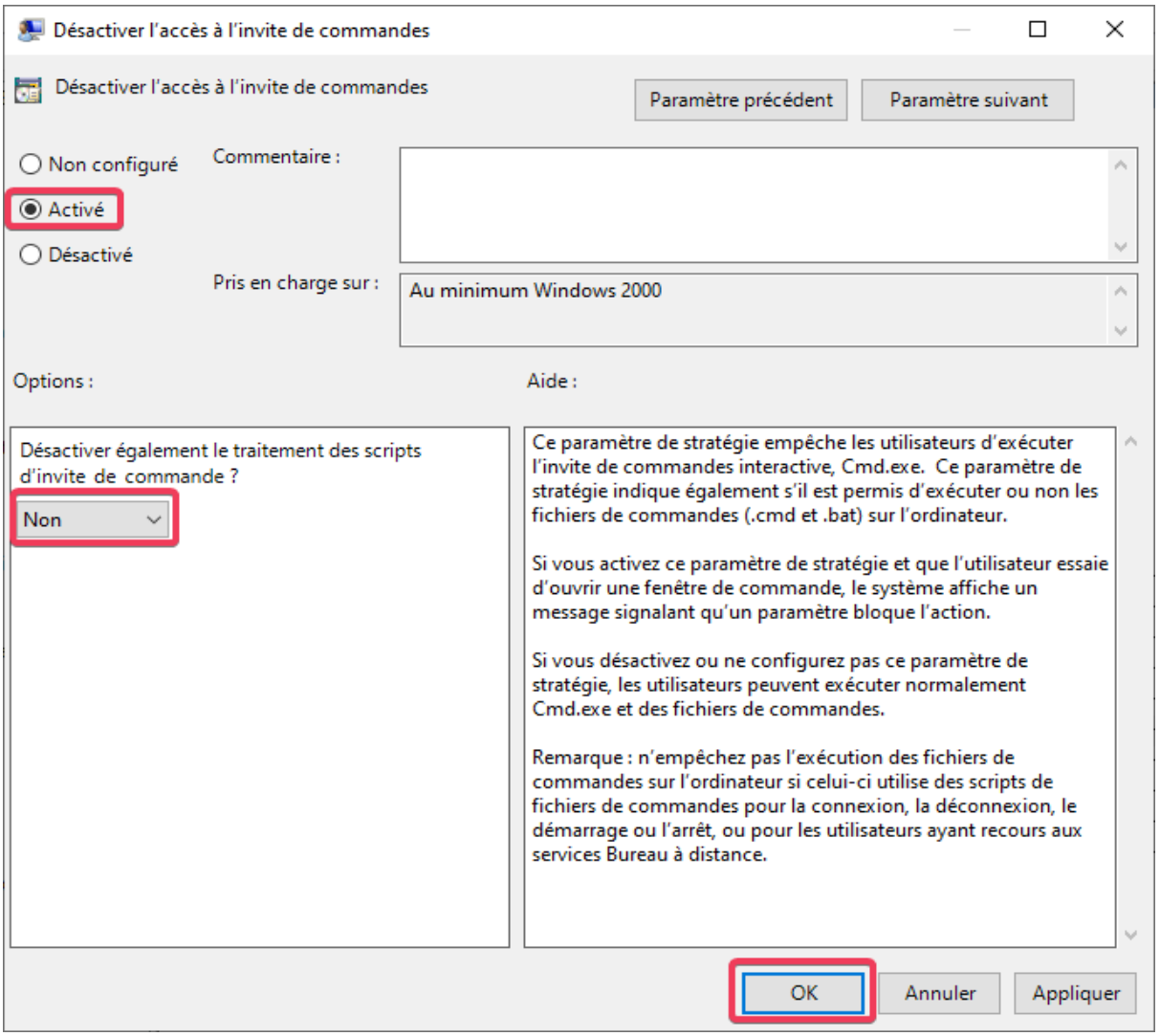
Une fois la GPO appliqué, tous les utilisateurs du domaines n'ont plus accès à PowerShell :



Bloquer l'invite de commande CMD :

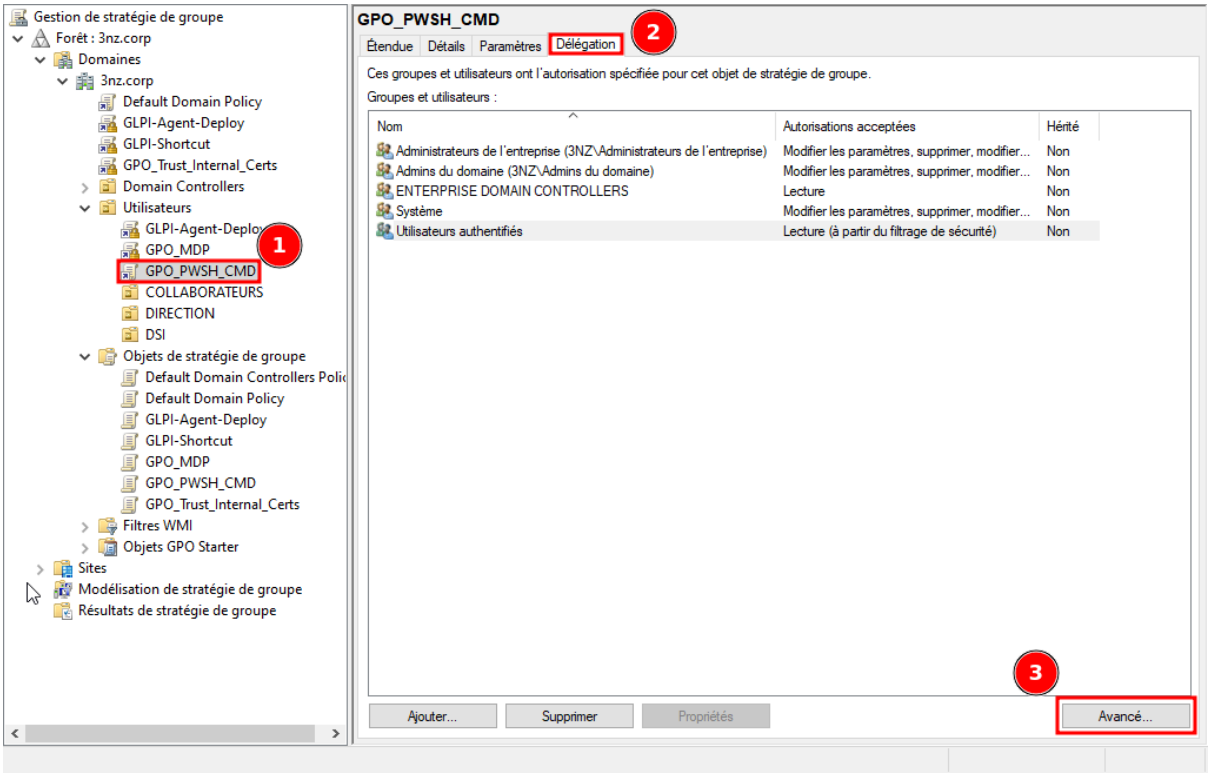


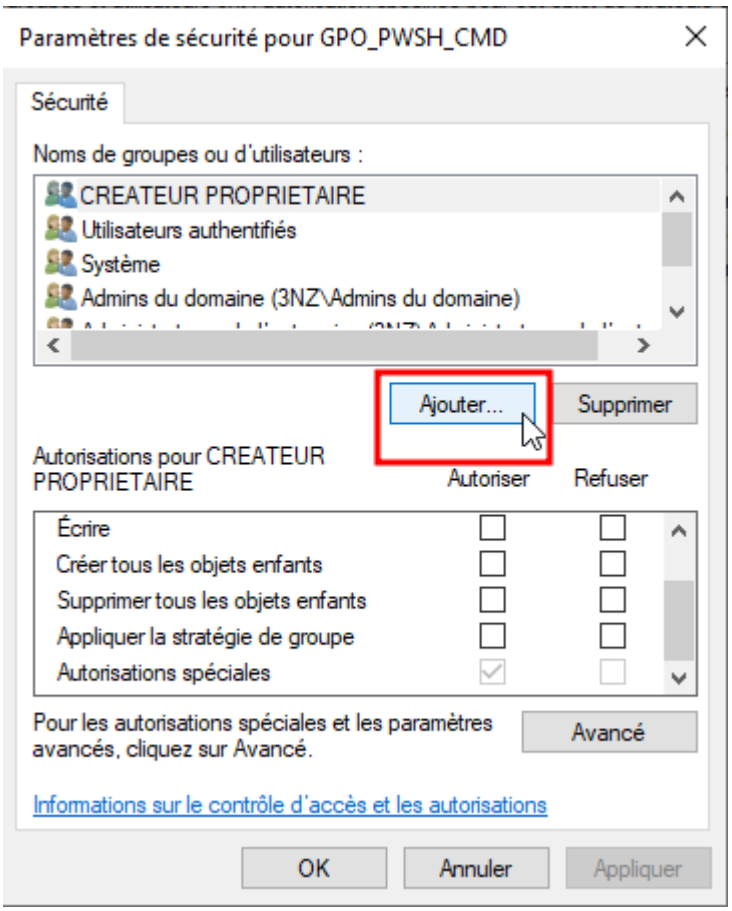
Double-cliquez puis configurez :



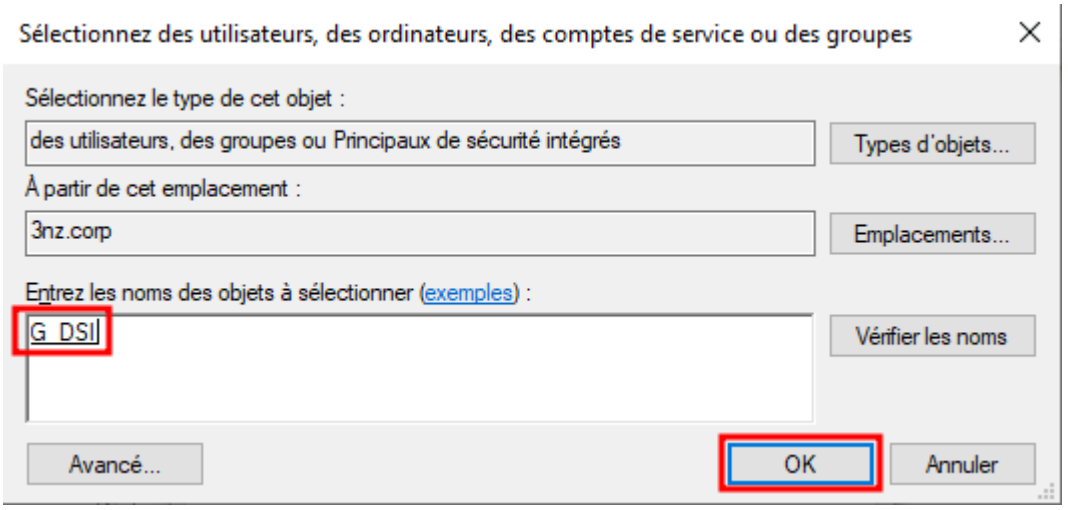
- Gestion des privilèges

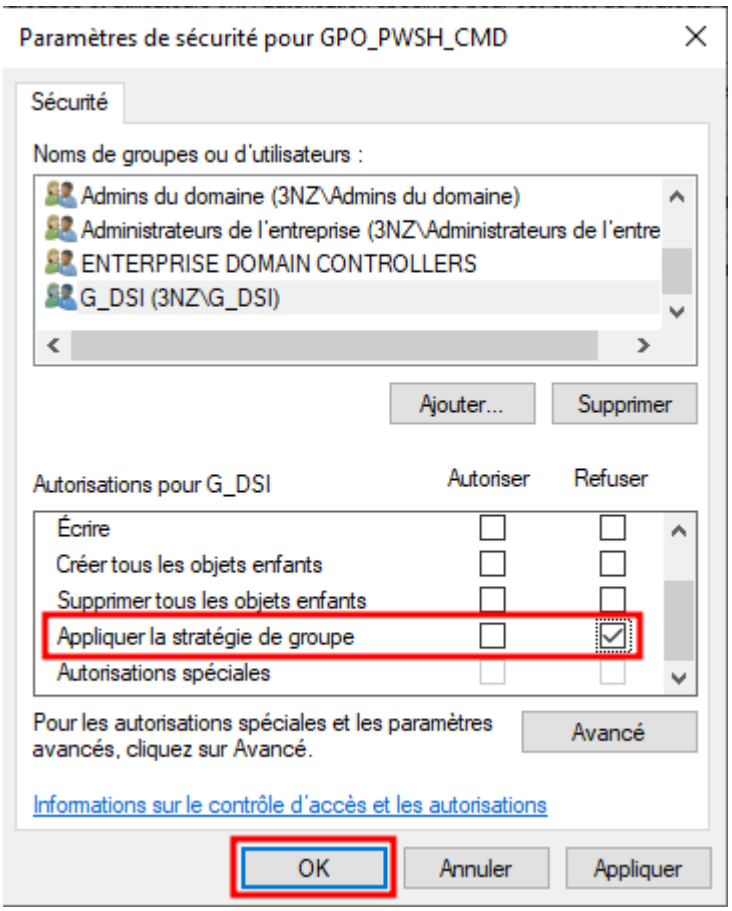
Etant donné que la DSI aura forcément besoin d'utiliser CMD ou PowerShell pour dépanner les utilisateurs, je décide de créer un délégation sur la GPO :





Ajout du groupe dsi :

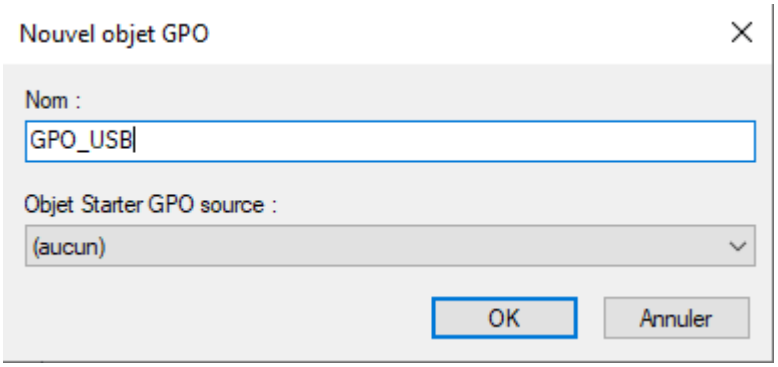




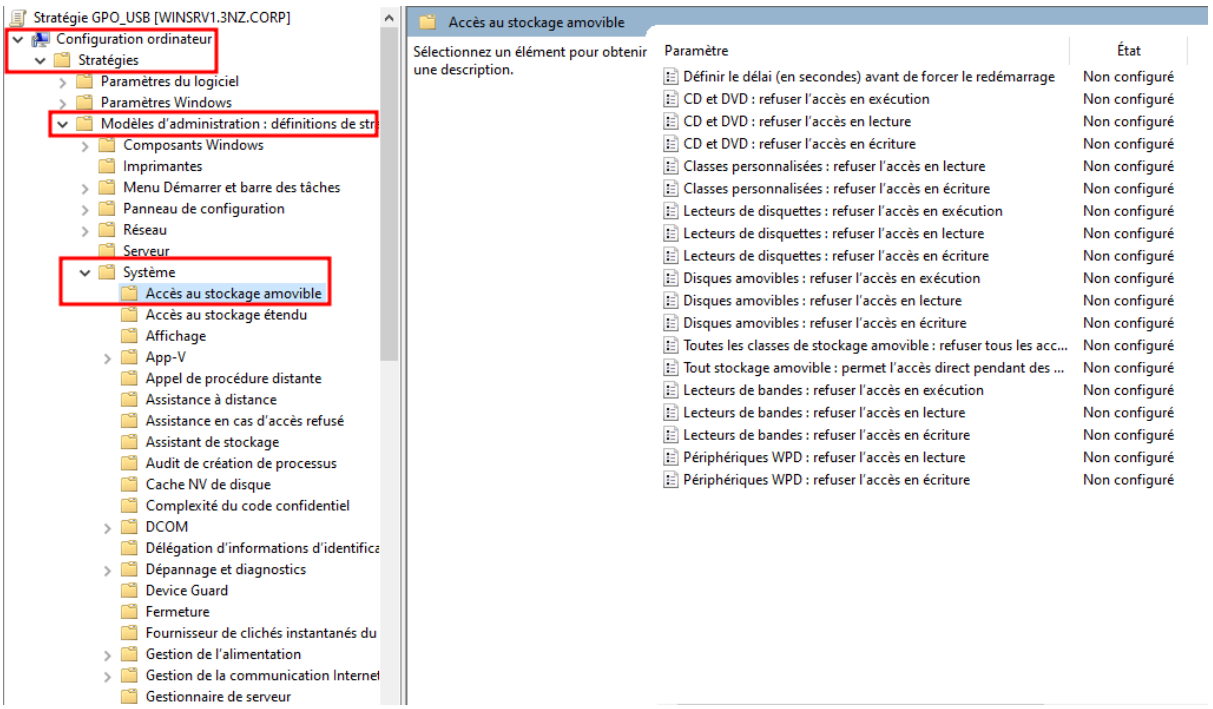
Voilà, maintenant tous les utilisateurs authentifiés sur le réseau sauf la DSI n'ont pas accès à PowerShell ni à l'invite de commande.

- Sécurité Physique

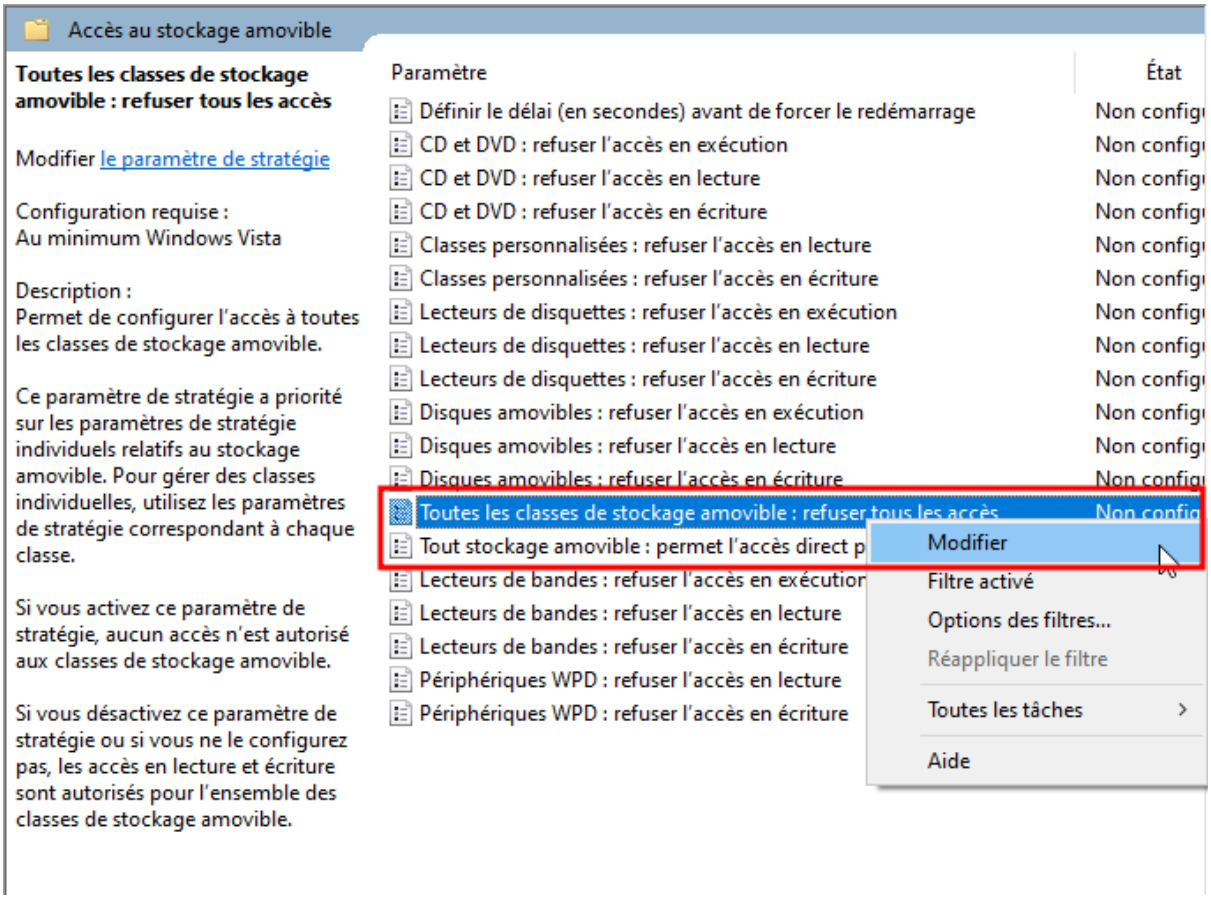
Création d'une GPO nommée GPO_USB :

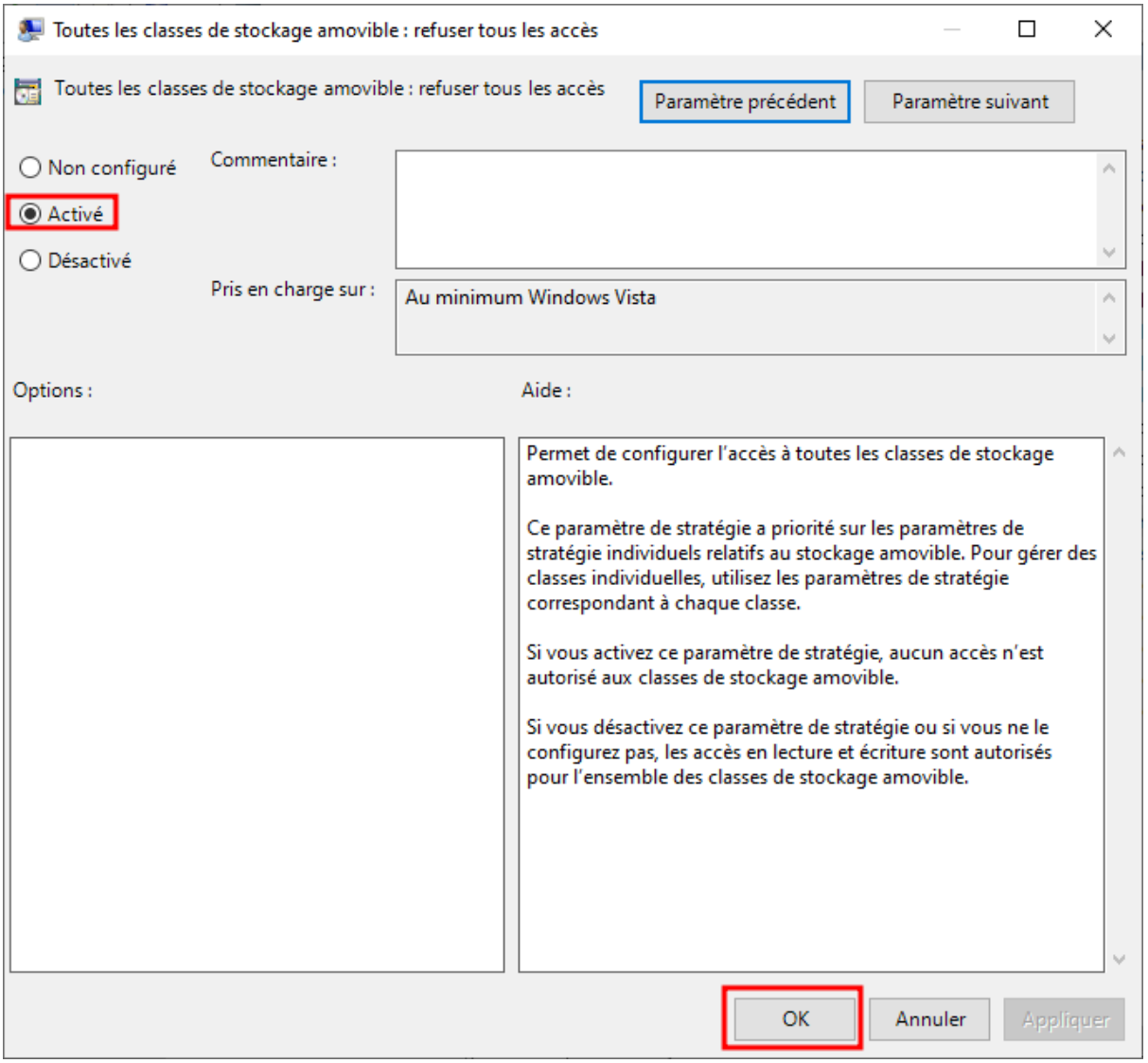


ensuite, on la modifie :

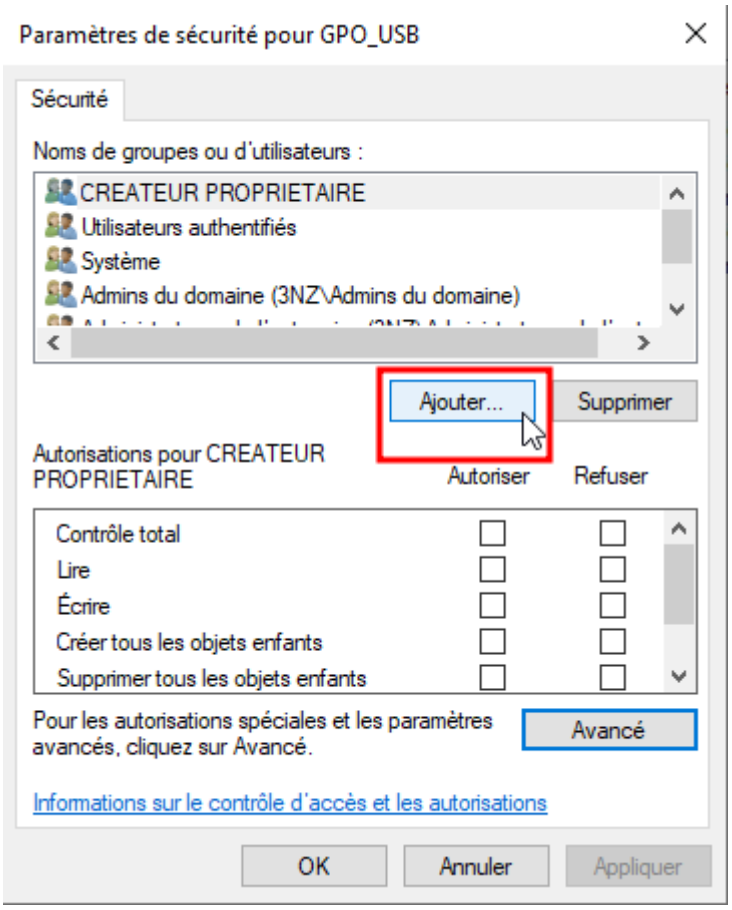


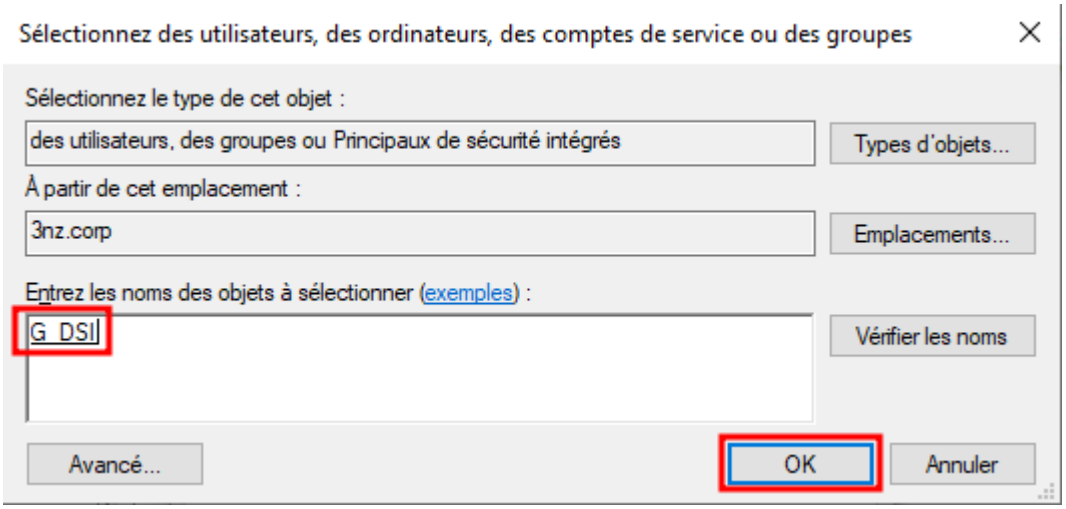
Il y a un paramètre radical qui se nomme **"Toutes les classes de stockage amovible : refuser tous les accès"** (*All Removable Storage Classes: Deny All Access*) et qui permet tout simplement de **bloquer tous les périphériques de stockage : CD, DVD, disquette, clé USB, carte mémoire, disque externe**, etc.

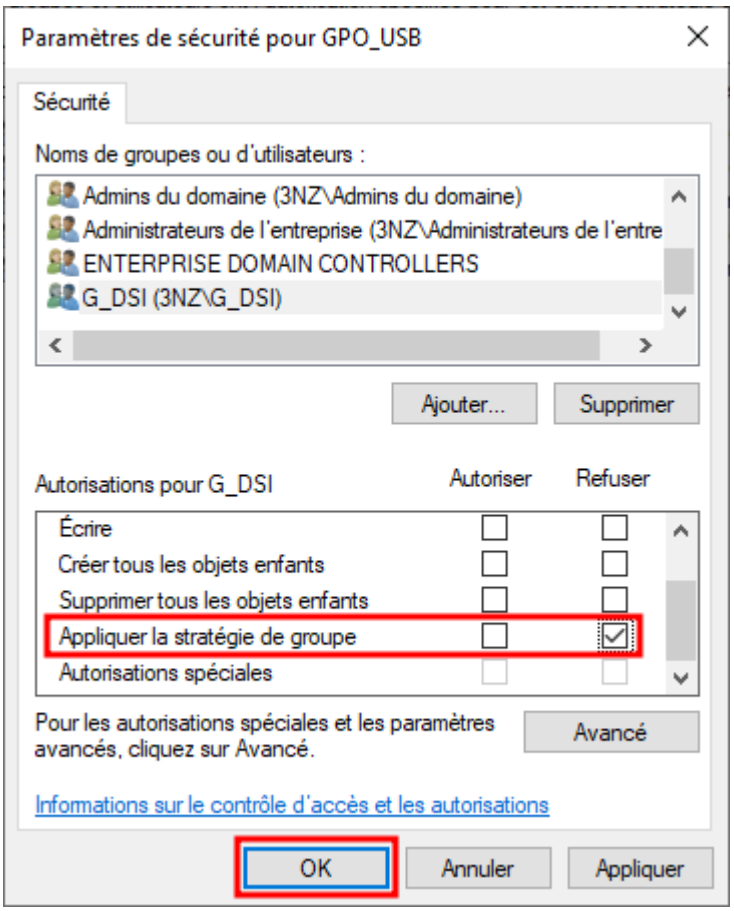

Accès au stockage amovible
Toutes les classes de stockage amovible : refuser tous les accès
Modifier le paramètre de stratégie
Configuration requise :
Au minimum Windows Vista
Description :
Permet de configurer l'accès à toutes les classes de stockage amovible.
Ce paramètre de stratégie a priorité sur les paramètres de stratégie individuels relatifs au stockage amovible. Pour gérer des classes individuelles, utilisez les paramètres de stratégie correspondant à chaque classe.
Si vous activez ce paramètre de stratégie, aucun accès n'est autorisé aux classes de stockage amovible.
Si vous désactivez ce paramètre de stratégie ou si vous ne le configurez pas, les accès en lecture et écriture sont autorisés pour l'ensemble des classes de stockage amovible.
Paramètre
État
Définir le délai (en secondes) avant de forcer le redémarrage
CD et DVD : refuser l'accès en exécution
CD et DVD : refuser l'accès en lecture
CD et DVD : refuser l'accès en écriture
Classes personnalisées : refuser l'accès en lecture
Classes personnalisées : refuser l'accès en écriture
Lecteurs de disquettes : refuser l'accès en exécution
Lecteurs de disquettes : refuser l'accès en lecture
Lecteurs de disquettes : refuser l'accès en écriture
Disques amovibles : refuser l'accès en exécution
Disques amovibles : refuser l'accès en lecture
Disques amovibles : refuser l'accès en écriture
Toutes les classes de stockage amovible : refuser tous les accès
Tout stockage amovible : permet l'accès direct p
Lecteurs de bandes : refuser l'accès en exécution
Lecteurs de bandes : refuser l'accès en lecture
Lecteurs de bandes : refuser l'accès en écriture
Périphériques WPD : refuser l'accès en lecture
Périphériques WPD : refuser l'accès en écriture
Non config
Modifier
Filtre activé
Options des filtres...
Réappliquer le filtre
Toutes les tâches
Aide


Toutes les classes de stockage amovible : refuser tous les accès
Toutes les classes de stockage amovible : refuser tous les accès
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Au minimum Windows Vista
Options :
Aide :
Permet de configurer l'accès à toutes les classes de stockage amovible.
Ce paramètre de stratégie a priorité sur les paramètres de stratégie individuels relatifs au stockage amovible. Pour gérer des classes individuelles, utilisez les paramètres de stratégie correspondant à chaque classe.
Si vous activez ce paramètre de stratégie, aucun accès n'est autorisé aux classes de stockage amovible.
Si vous désactivez ce paramètre de stratégie ou si vous ne le configurez pas, les accès en lecture et écriture sont autorisés pour l'ensemble des classes de stockage amovible.
OK
Annuler
Appliquer

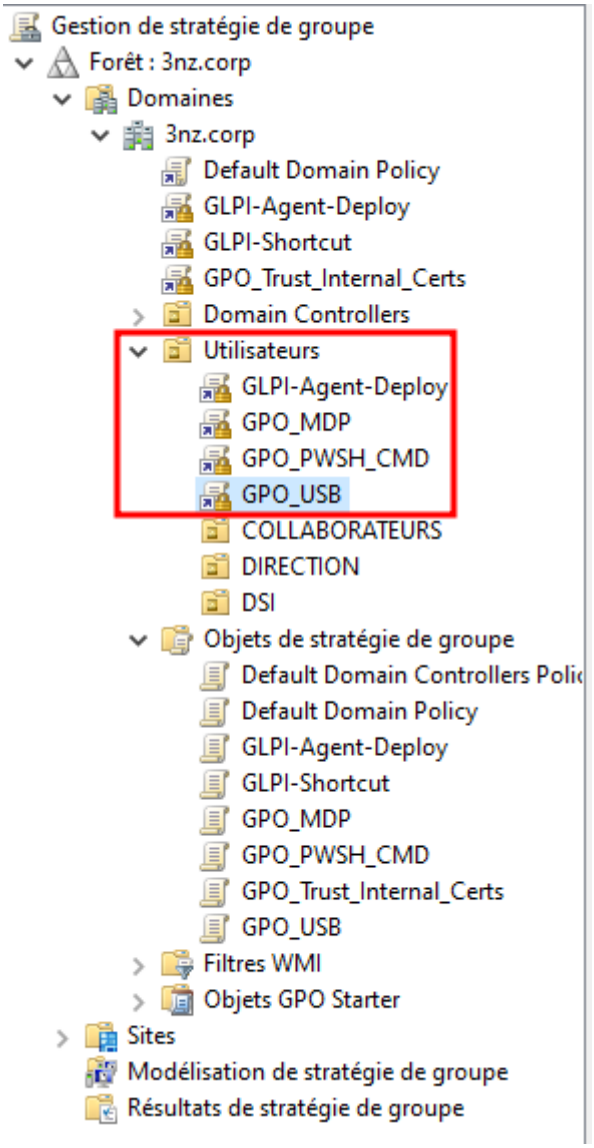
Je décide de faire une délégation pour le groupe DSI :






Paramètres de sécurité pour GPO_USB
Sécurité
Noms de groupes ou d'utilisateurs :
Admins du domaine (3NZ\Admins du domaine)
Administrateurs de l'entreprise (3NZ\Administrateurs de l'entre
ENTERPRISE DOMAIN CONTROLLERS
G_DSI (3NZ\G_DSI)
Ajouter...
Supprimer
Autorisations pour G_DSI
Autoriser
Refuser
Écrire
Créer tous les objets enfants
Supprimer tous les objets enfants
Appliquer la stratégie de groupe
Autorisations spéciales
Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé.
Avancé
Informations sur le contrôle d'accès et les autorisations
OK
Annuler
Appliquer

L’ensemble de ces règles sont positionnées dans l’OU Utilisateurs afin qu’elles s’appliquent sur ces derniers :

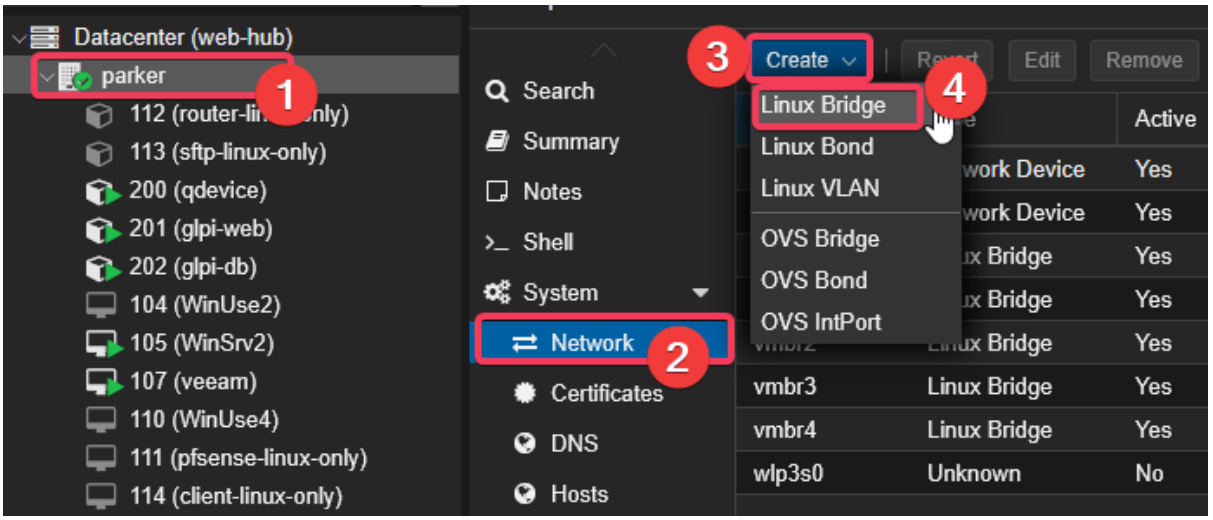


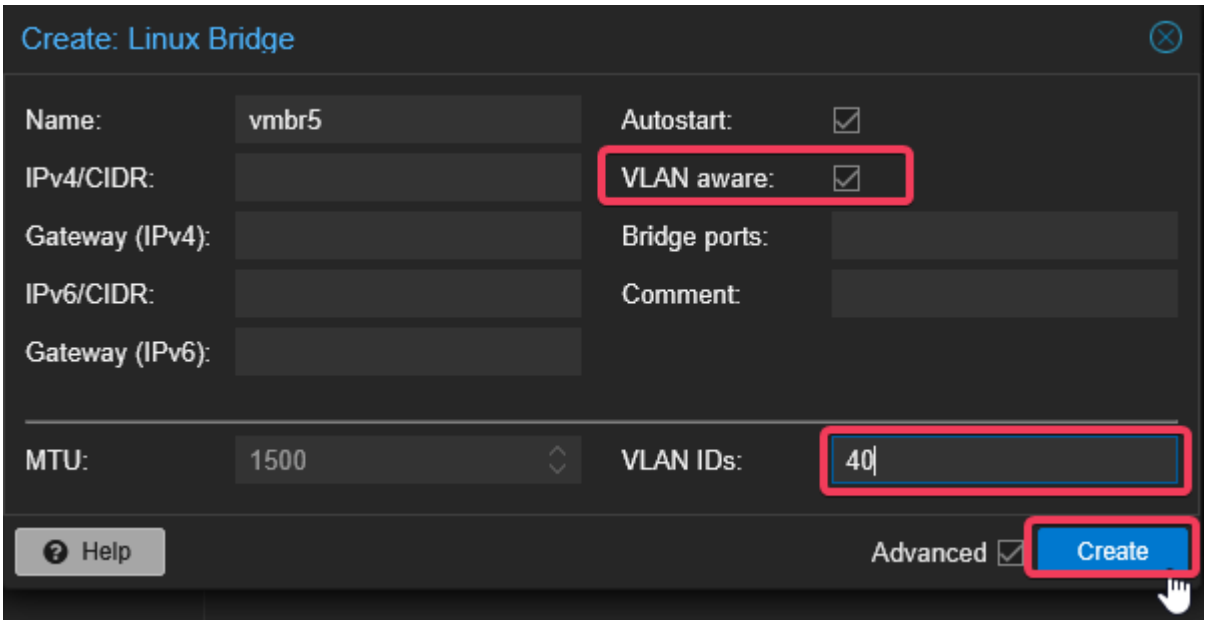
V. DMZ et Publication Web

- Création du VLAN 40 (DMZ) et Configuration sur pfSense

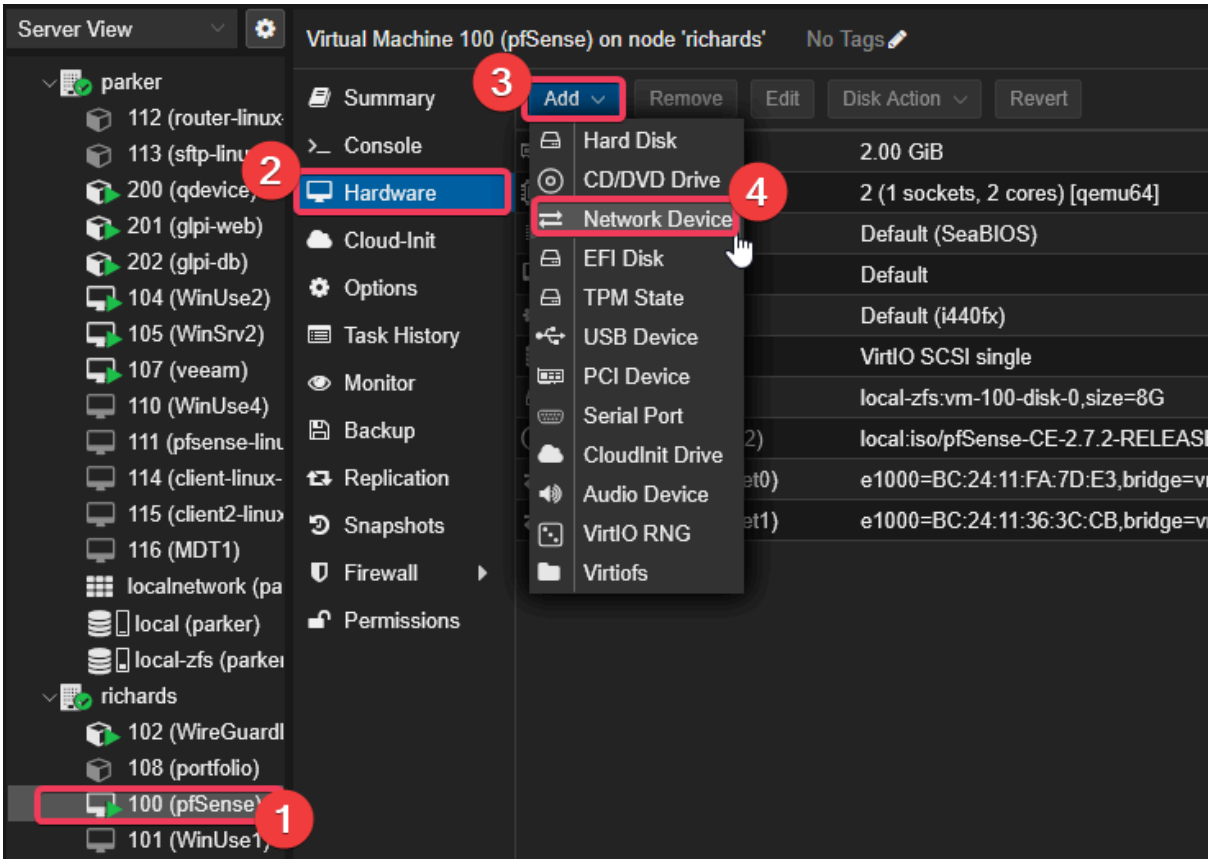
L'entreprise voulant créer un site vitrine, la nécessité de créer une DMZ est crucial.
Je créer donc un nouveau VLAN qui portera le numéro 40 (192.168.40.0/27).

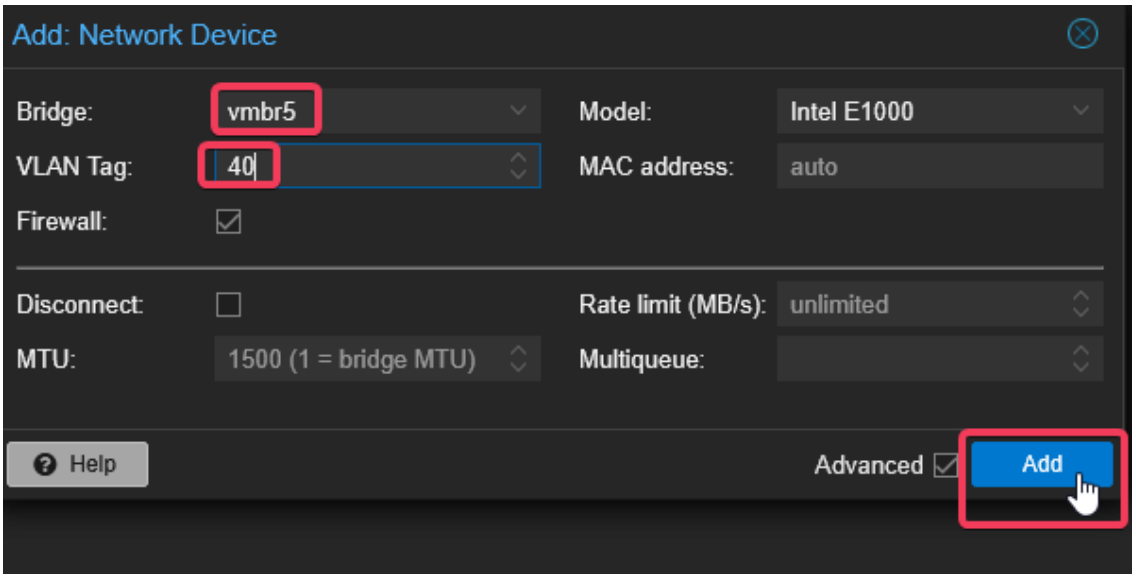
1ère étape :
Créer la nouvelle interface pour ce VLAN et l'assigner sur pfSense :



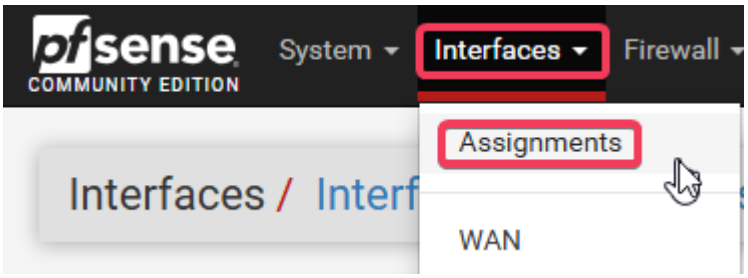


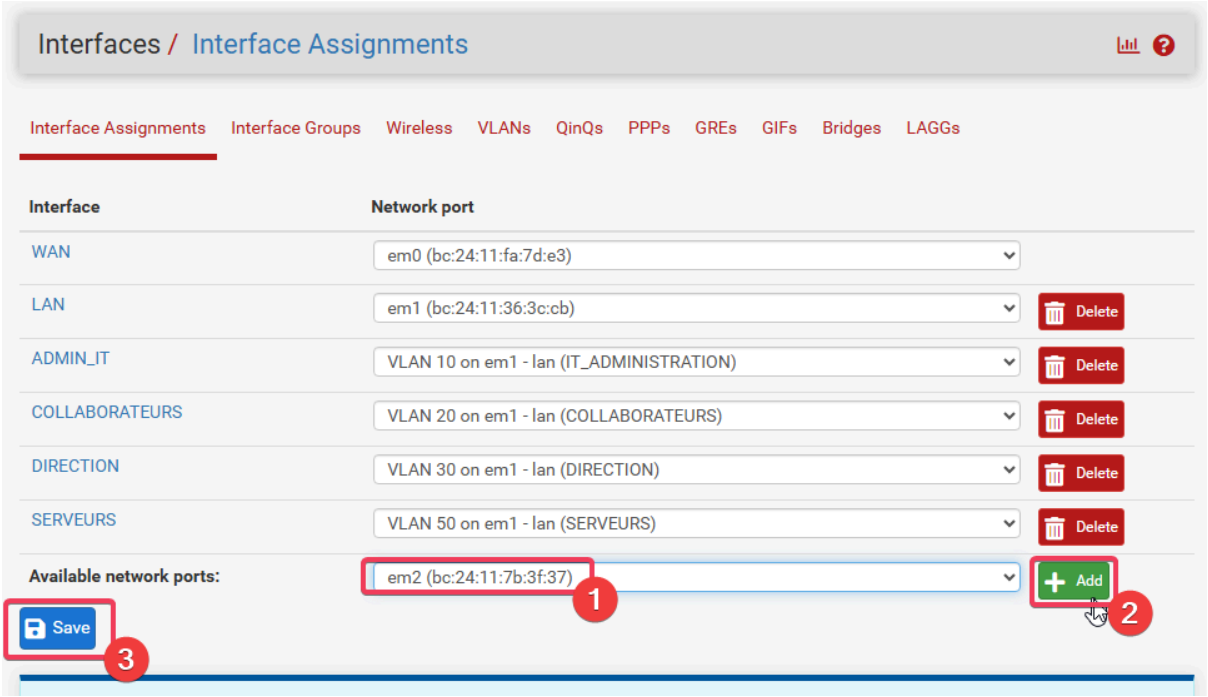
Ajouter l'interface vmbr5 sur le pfsense :



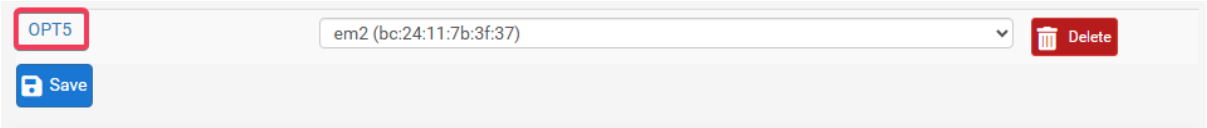


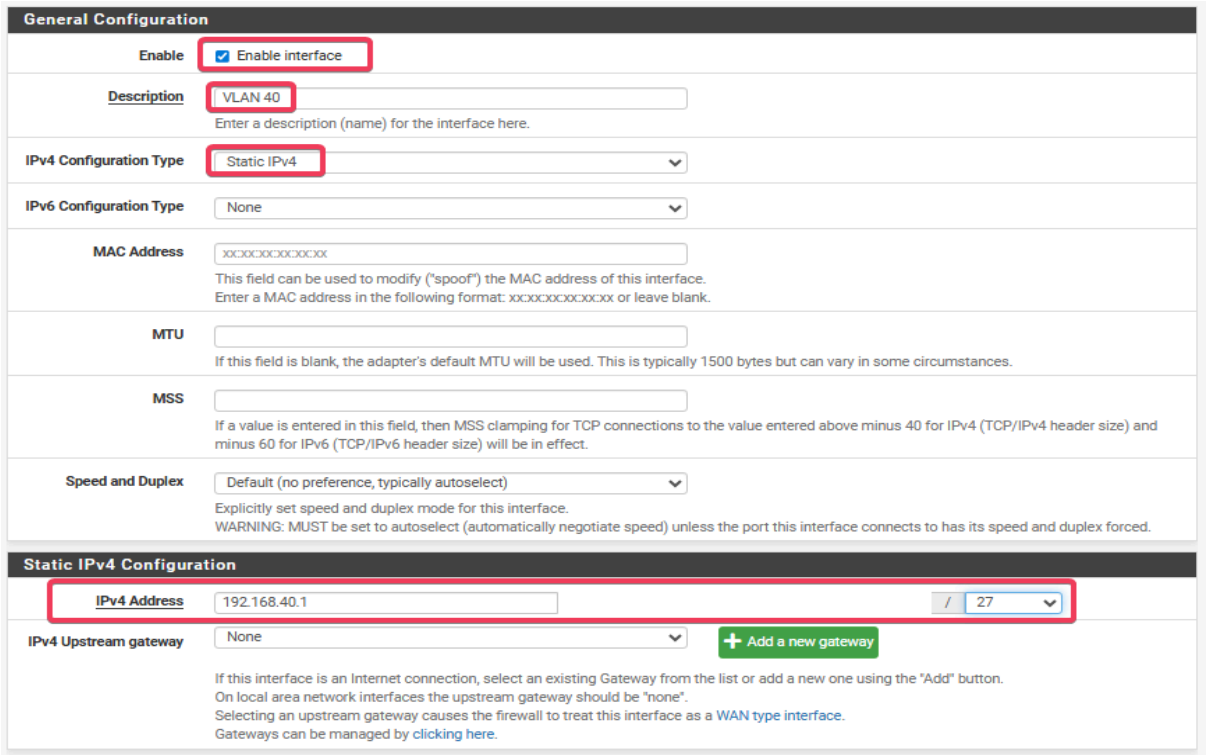
Démarrer une machine cliente, se rendre sur l'adresse du pfSense pour le configurer :





Puis sélectionner votre interface :

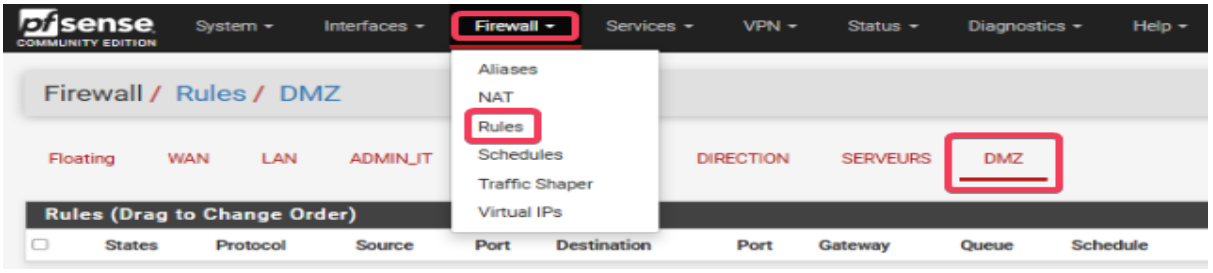




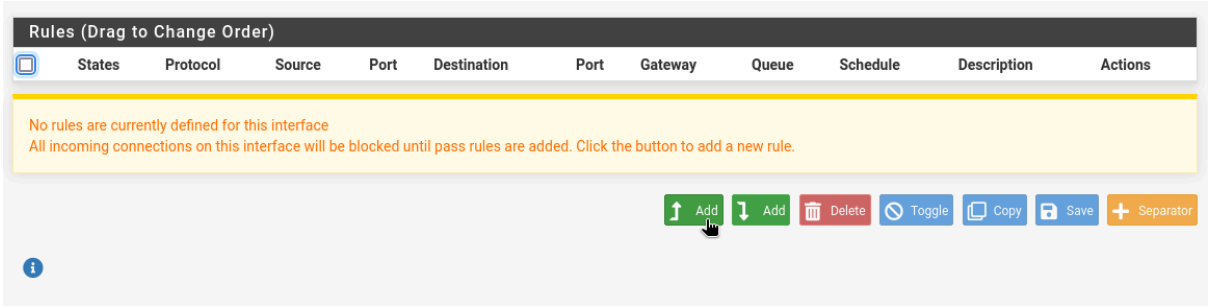
Comme cette interface ne sera pas gérer par le DHCP de mon serveur Windows étant donné que c'est une DMZ.
Mes serveurs exposés seront tous en statique.

- Mise en place des Règles de Pare-feu de la DMZ

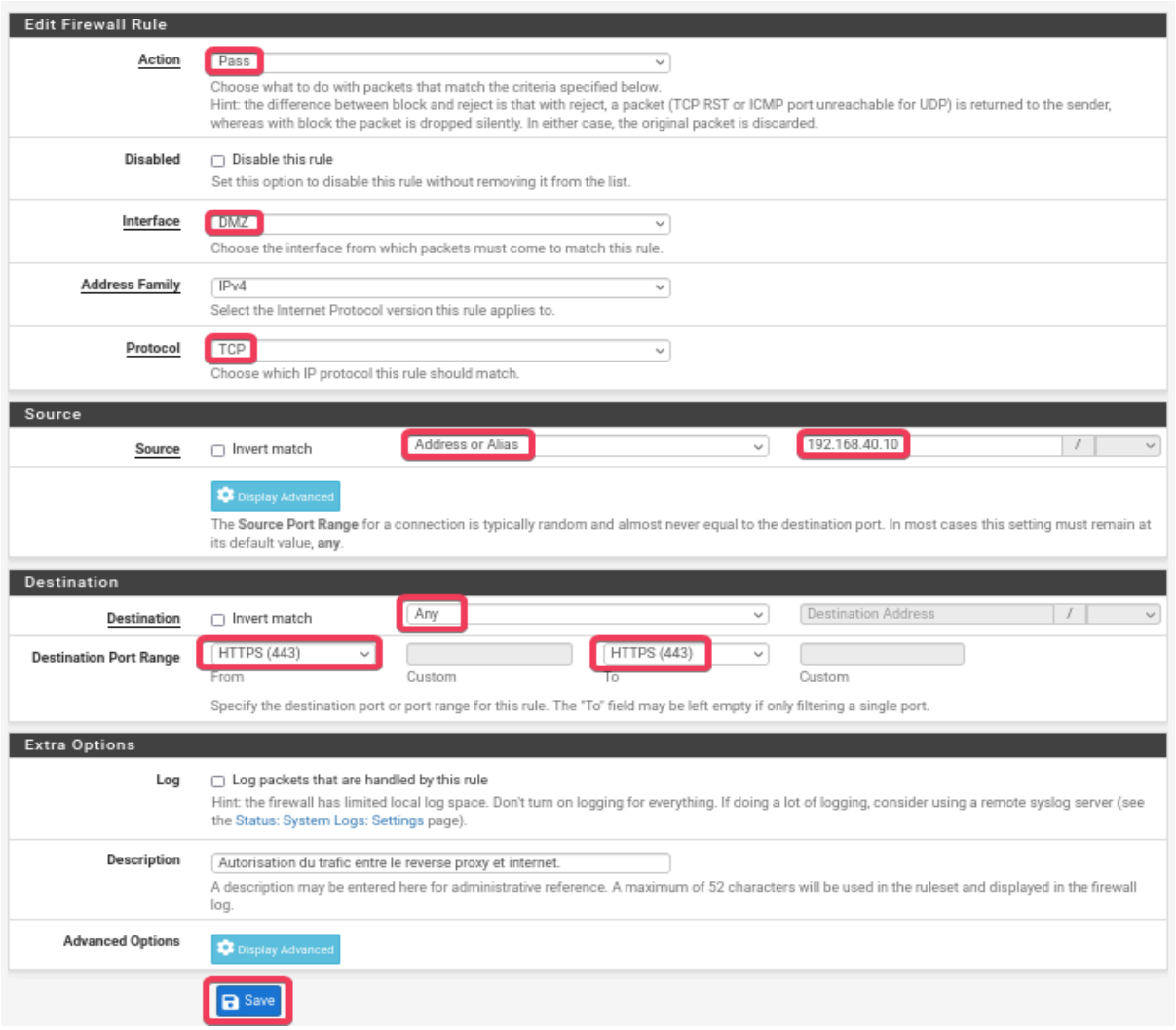
Création des règles de pare-feu pour l'interface DMZ :



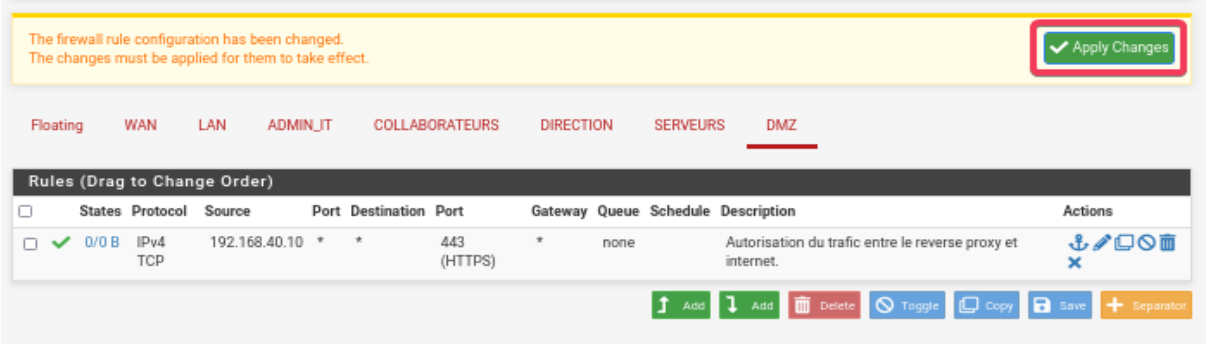
Cliquez simplement sur Add l'ordre n'importe pas pour le moment :



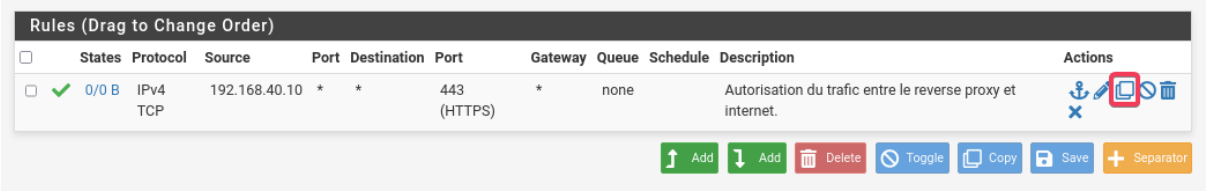
Voici la règle que j'ai mise en place pour le trafic entre le reverse proxy et internet :



Cliquez sur Save, puis n'oubliez pas d'appliquer les changements :



Puis, je copie la règle qui autorise le 443 pour en créer une avec le ports 80



Je change juste le protocole 443 par 80 et je l'ajoute :

☐	✓	0/0 B	IPv4 TCP	192.168.40.10	*	*	80 (HTTP)	*	none	Autorisation du trafic entre le reverse proxy et internet.

Maintenant, je bloque tout le trafic de mes réseaux internes vers mes réseaux internes :

Edit Firewall Rule

Action : Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled : ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface : DMZ
Choose the interface from which packets must come to match this rule.

Address Family : IPv4
Select the Internet Protocol version this rule applies to.

Protocol : Any
Choose which IP protocol this rule should match.

Source

Source : ☐ Invert match — ADMIN_IT subnets — Source Address /

Destination

Destination : ☐ Invert match — DMZ subnets — Destination Address /

Extra Options

Log : ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description : Blockage du traffic entre les réseaux internes et la DMZ.
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options : Display Advanced

Save

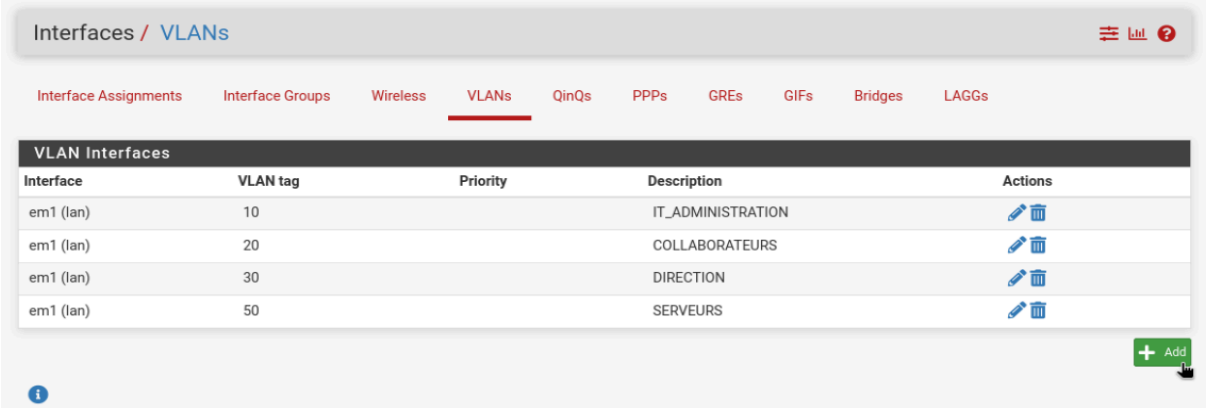
Enfin, voici toutes les règles de pare-feu de ma DMZ.

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✗	0/0 B	IPv4 *	ADMIN_IT subnets	*	DMZ subnets	*	*	none		Blocage du trafic entre les réseaux internes et la DMZ.	
☐	✗	0/0 B	IPv4 *	COLLAB subnets	*	DMZ subnets	*	*	none		Blocage du trafic entre les réseaux internes et la DMZ.	
☐	✗	0/0 B	IPv4 *	DIRECTION subnets	*	DMZ subnets	*	*	none		Blocage du trafic entre les réseaux internes et la DMZ.	
☐	✗	0/0 B	IPv4 *	SERVEURS subnets	*	DMZ subnets	*	*	none		Blocage du trafic entre les réseaux internes et la DMZ.	
☐	✗	0/0 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none		Blocage du trafic entre les réseaux internes et la DMZ.	
☐	✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	1.1.1.1	53 (DNS)	*	none		Autorisation du trafic entre la DMZ et internet	
☐	✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	*	80 (HTTP)	*	none		Autorisation du trafic entre la DMZ et internet	
☐	✓	0/0 B	IPv4 TCP/UDP	DMZ subnets	*	*	443 (HTTPS)	*	none		Autorisation du trafic entre la DMZ et internet	
☐	✓	0/504 B	IPv4 *	DMZ subnets	*	DMZ subnets	*	*	none			
☐	✗	0/4 KiB	IPv4 *	DMZ subnets	*	*	*	*	none		Règle de blocage par défaut de la DMZ	

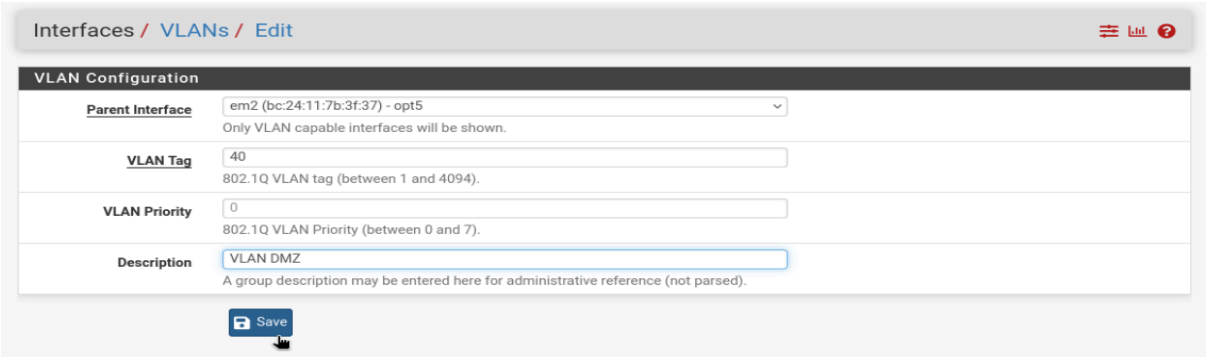
Maintenant on déclare le VLAN sur pfSense, sinon il ne reconnaîtra pas les paquets tagués

Interfaces -> VLANs

Cliquez sur Add



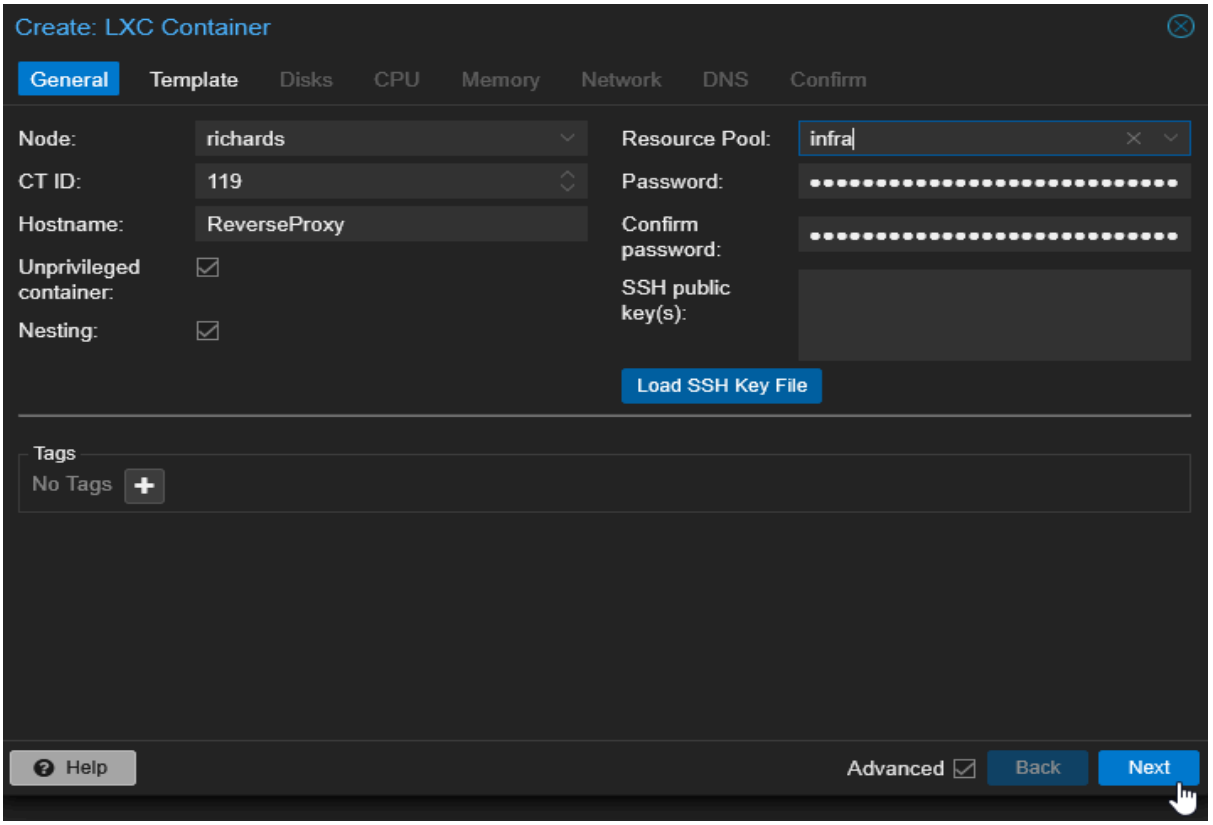
Choisissez votre interface, votre VLAN tag et une description si vous le souhaitez.

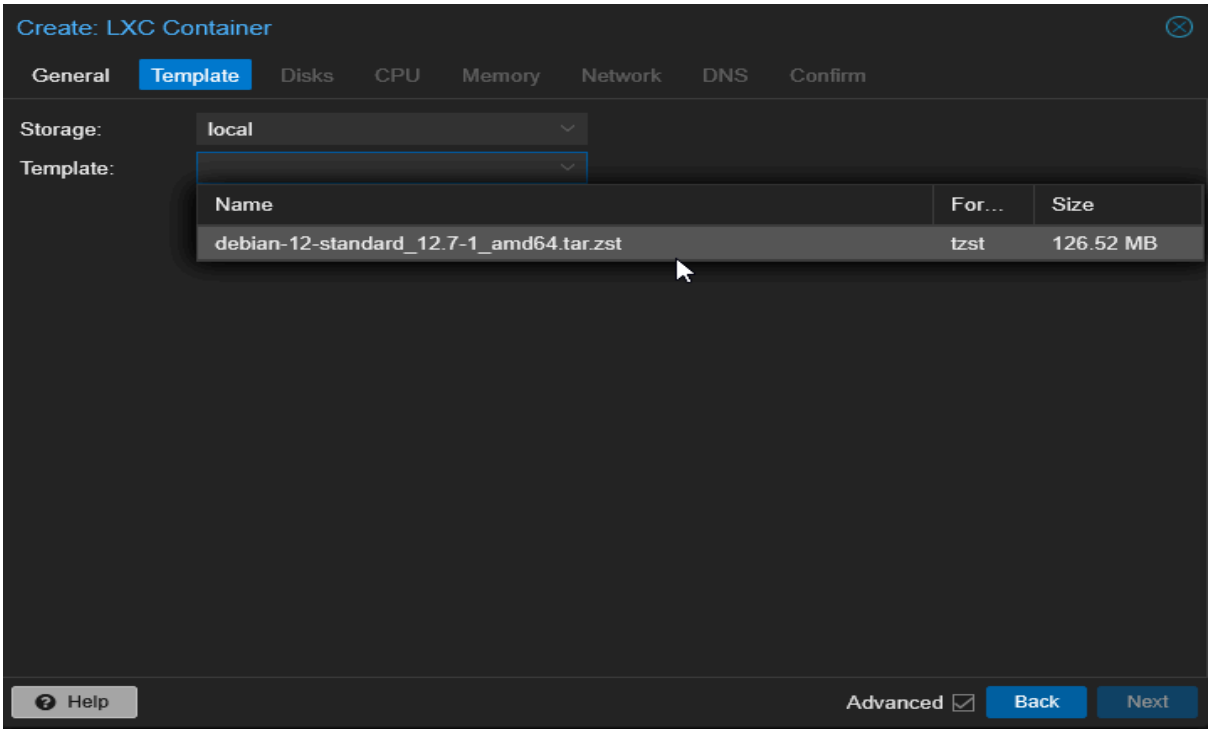


Création de deux règles de redirection de ma Livebox vers mon pfSense:

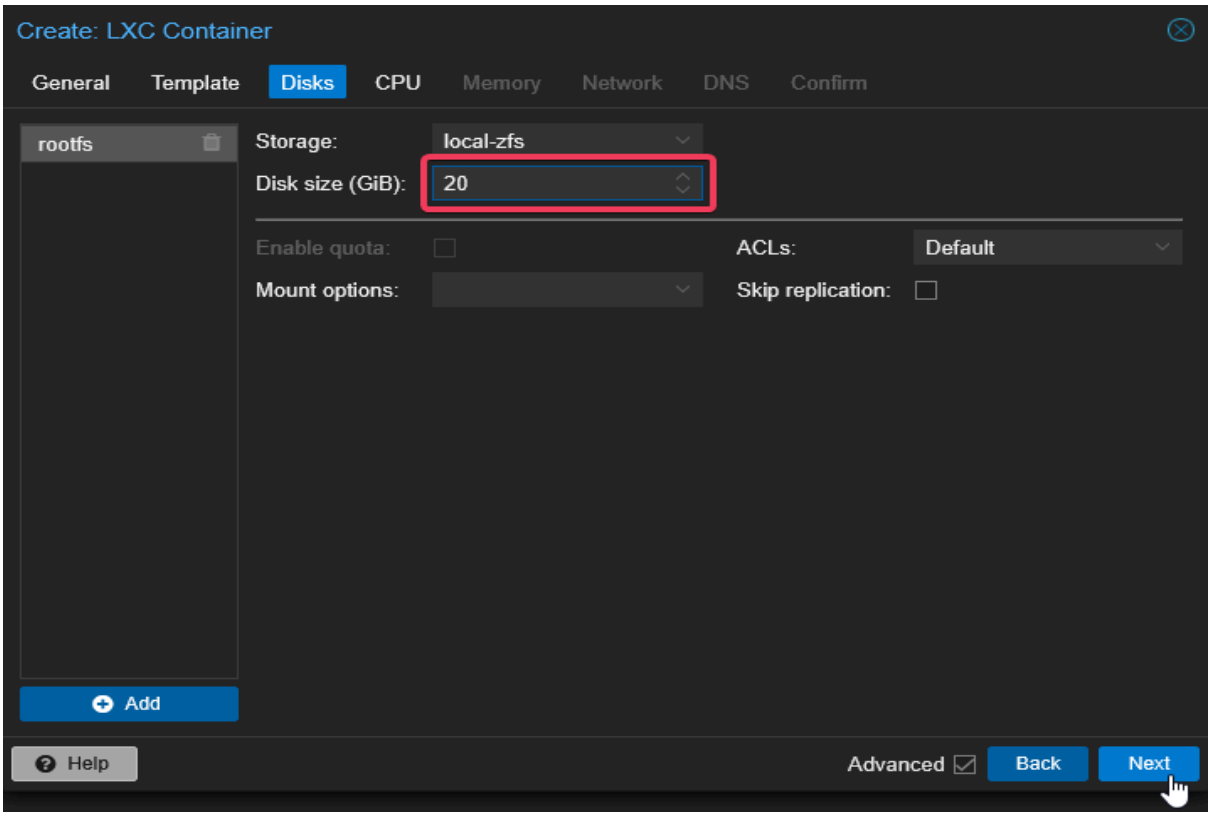
- Mise en place des Règles de Pare-feu de la DMZ

Une fois les règles paramétré, on peut passer à la création de la VM ou du LXC Container :
Pour des raisons de praticité et gestion de ressources, je choisi le container :

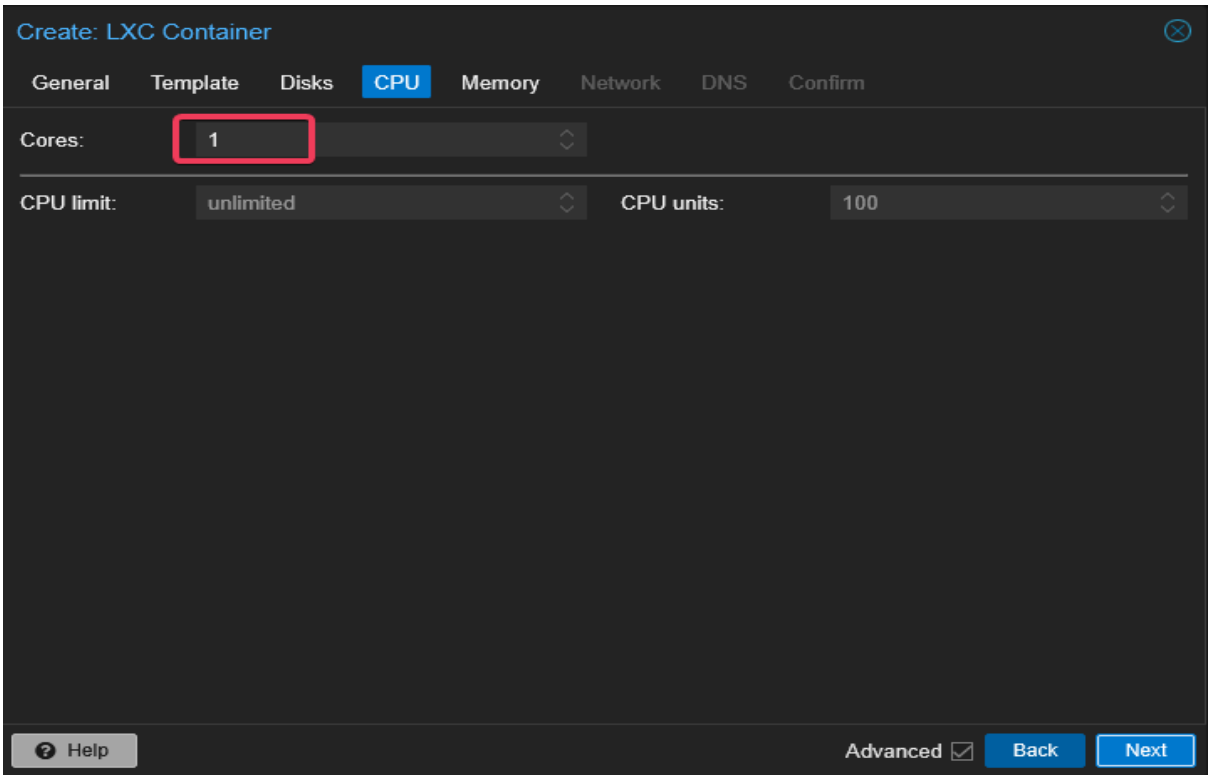




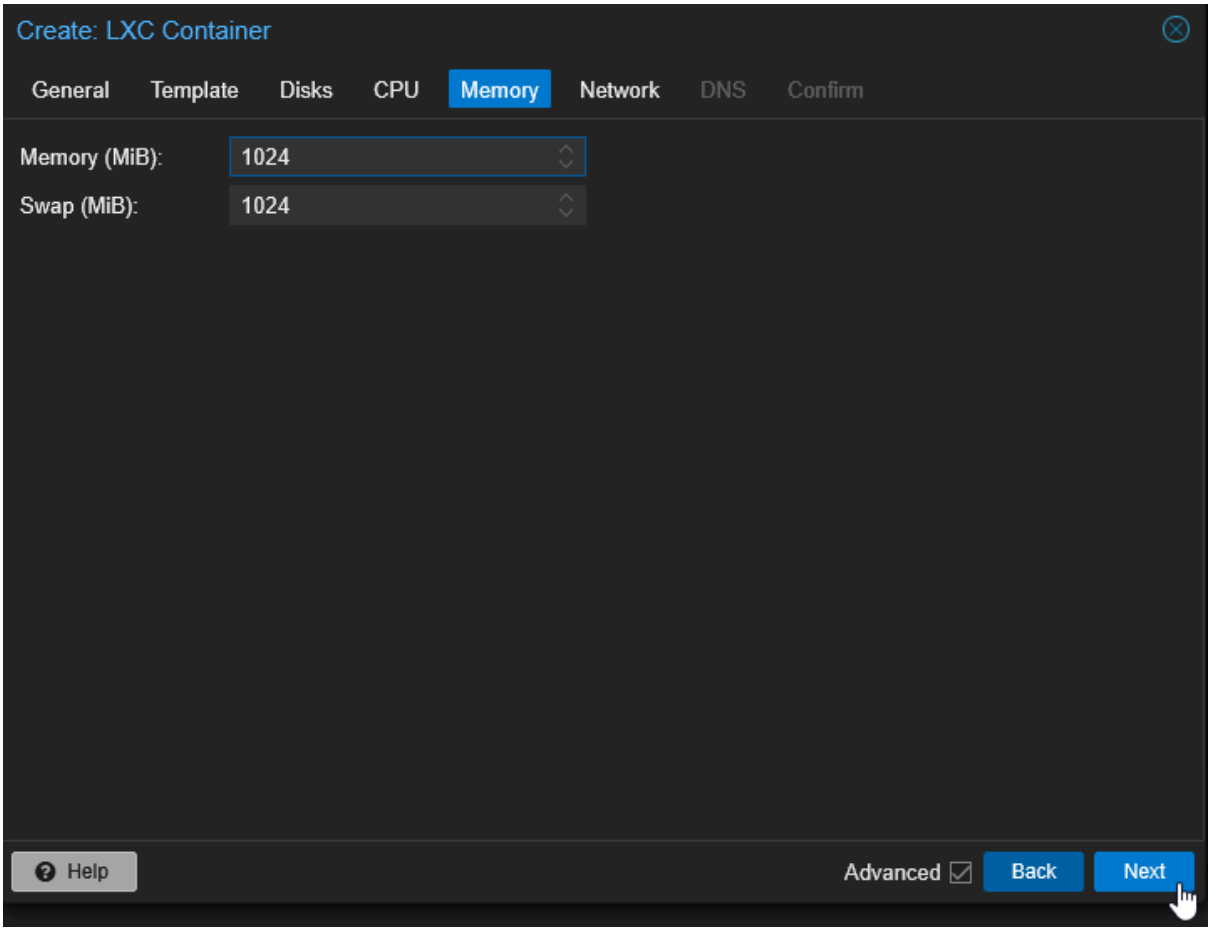
Je décide d'allouer 20 GiB au LXC Container car les conteneurs Docker peuvent prendre de la place.



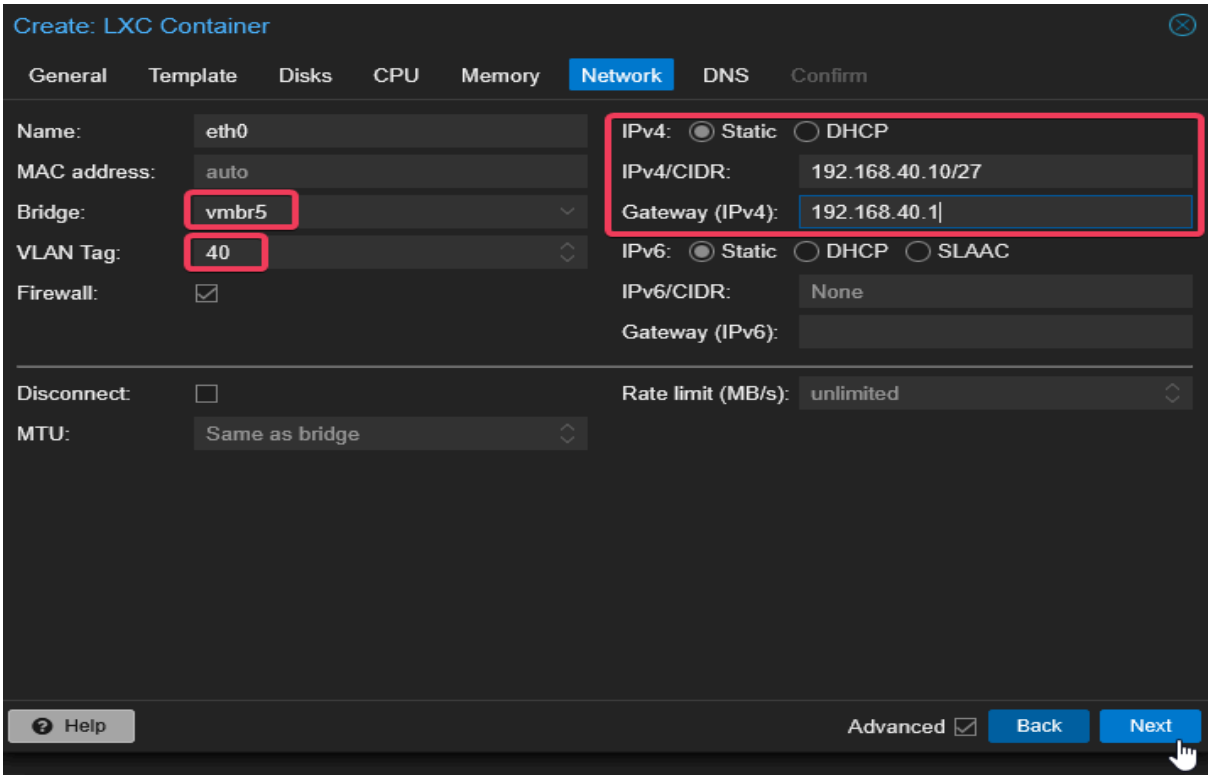
1 Cores est largement suffisant :



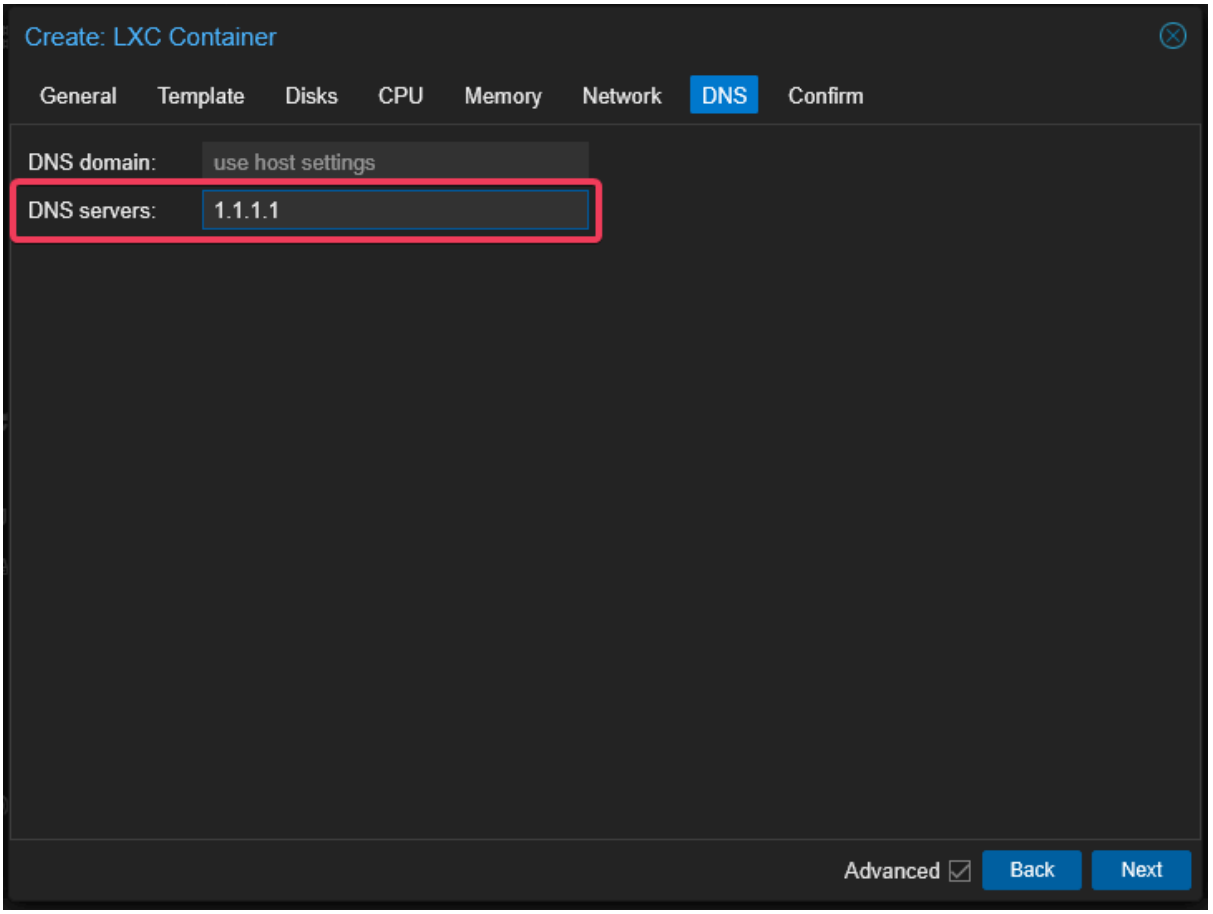
1 Go de RAM :



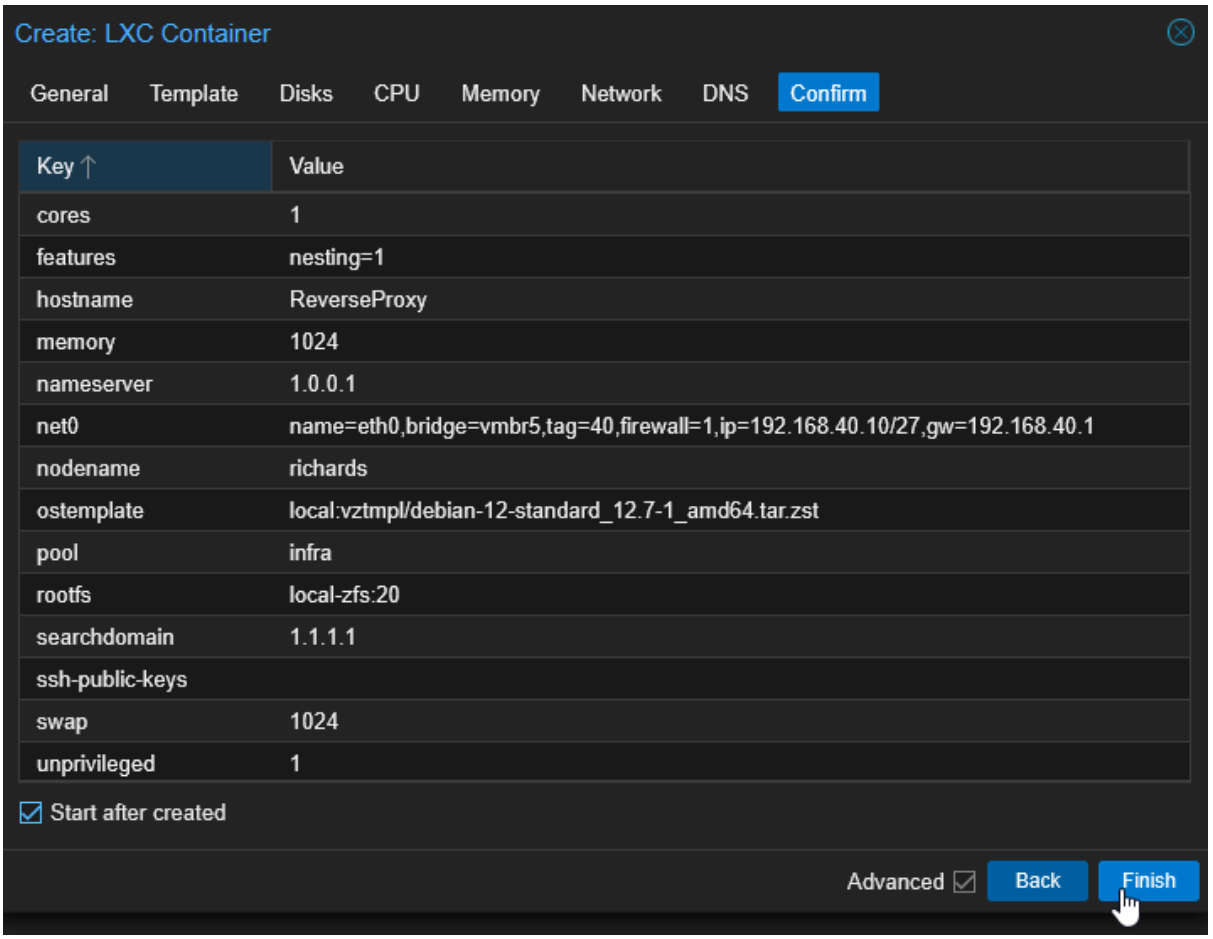
On choisit, le bon bridge, le bon VLAN Tag, ainsi que les bonnes adresses IP (gateway ainsi que celle de la machine).



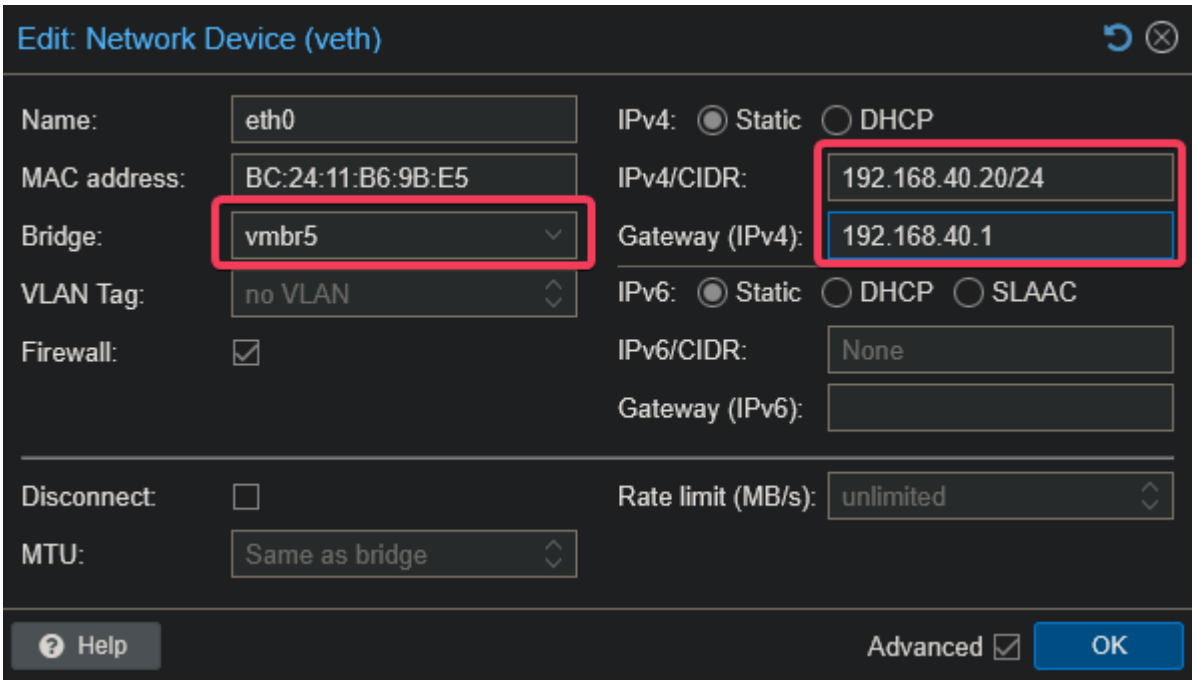
Pour les DNS je choisi celui de CloudFlare :



Voilà la création du container est fini :



Modification de la configuration réseau du container LXC (Portfolio) :



0

Sur le conteneur Nginx, mise à jour des paquets puis installation de Nginx :

```
root@ReverseProxy:~# apt update && apt upgrade -y
```

```
root@ReverseProxy:~# apt install nginx
```

Une fois installé déplacez vous dans le dossier etc/nginx/sites-available/

Puis, utilisez un éditeur de texte pour créer un fichier de configuration

```
root@ReverseProxy:/etc/nginx/sites-available# vim corp
```

Modifier votre fichier de conf :

```
server {
    server_name corp.3nz.fr;

    location / {
        proxy_pass http://192.168.40.20;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }
```

Puis toujours dans le dossier sites-available, supprimer le fichier de conf par défaut :

```
/etc/nginx/sites-available# rm default
```

Liaison du nouveau fichier de configuration

```
/etc/nginx/sites-available# ln -s /etc/nginx/sites-available/corp /etc/nginx/sites-enabled/
```

Maintenant, ajoutons SSL avec Let's Encrypt :

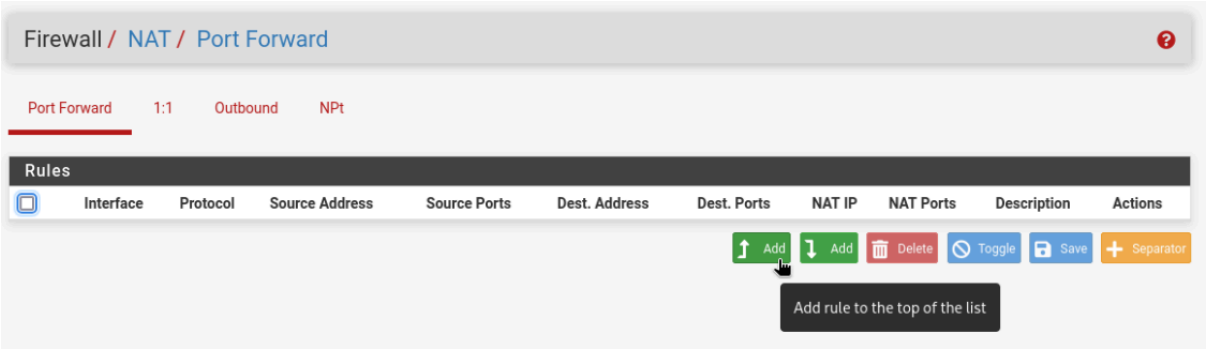
```
apt install certbot python3-certbot-nginx -y
```

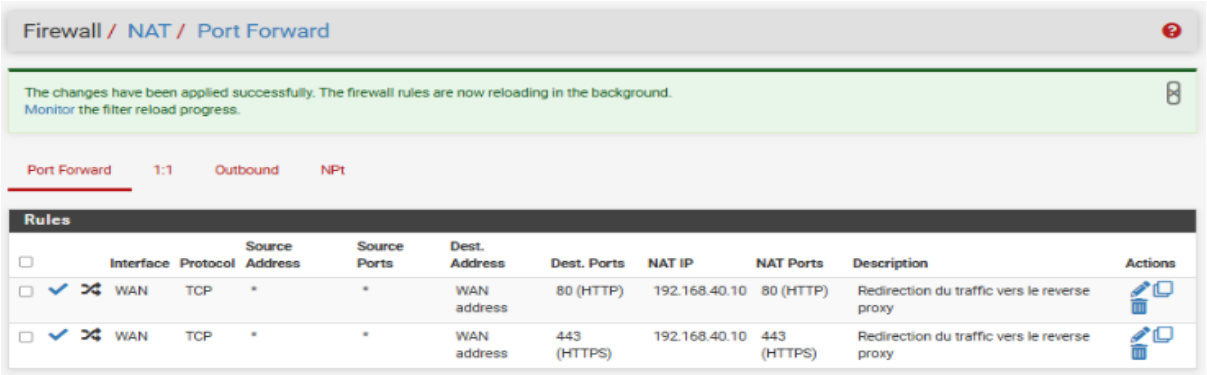
```
certbot --nginx -d 3nz.fr
```

```
root@ReverseProxy:/etc/nginx/sites-enabled# certbot --nginx -d portfolio.3nz.fr -d yacreader.3nz.fr
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Requesting a certificate for portfolio.3nz.fr and yacreader.3nz.fr

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/portfolio.3nz.fr/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/portfolio.3nz.fr/privkey.pem
This certificate expires on 2026-01-20.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for portfolio.3nz.fr to /etc/nginx/sites-enabled/reverse-proxy
Successfully deployed certificate for yacreader.3nz.fr to /etc/nginx/sites-enabled/reverse-proxy
Congratulations! You have successfully enabled HTTPS on https://portfolio.3nz.fr and https://yacreader.3nz.fr

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
If you like Certbot, please consider supporting our work by:
 * Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
 * Donating to EFF:                    https://eff.org/donate-le
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

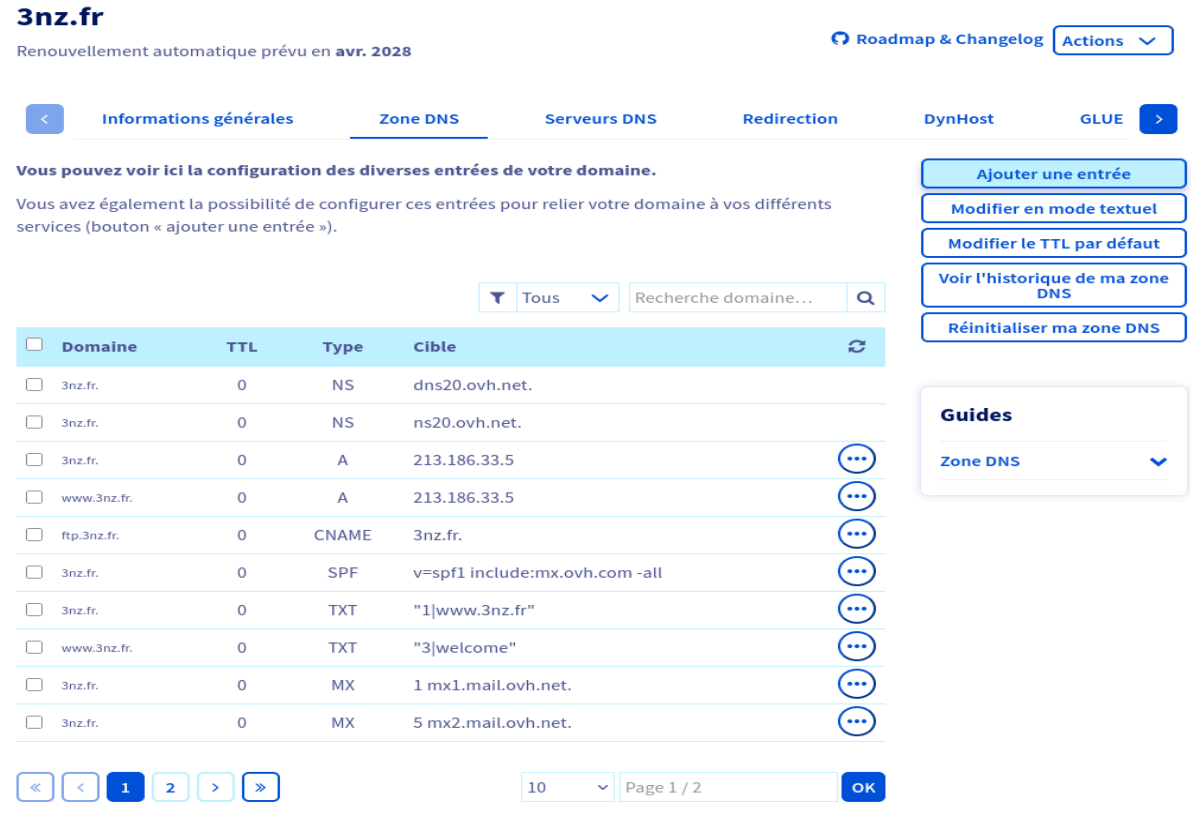
- Configuration DNS et Redirection de Ports

Créer une règle de redirection de port sur votre routeur, en l'occurrence pfSense:
Firewall -> NAT -> Port Forward

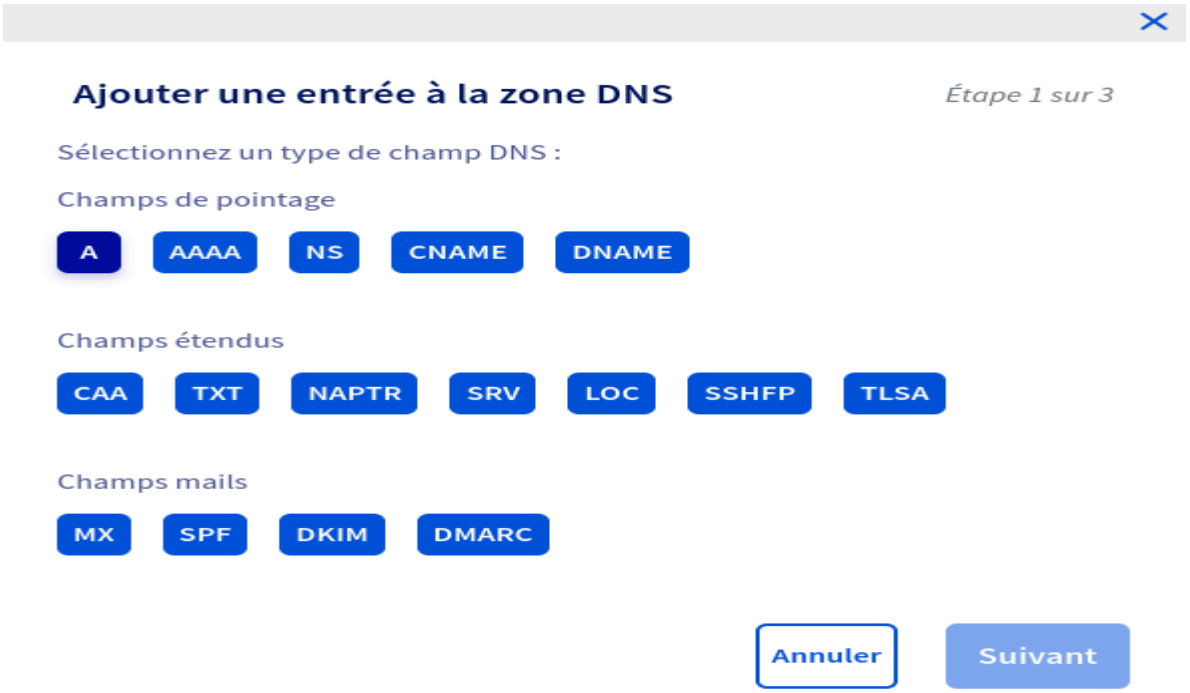


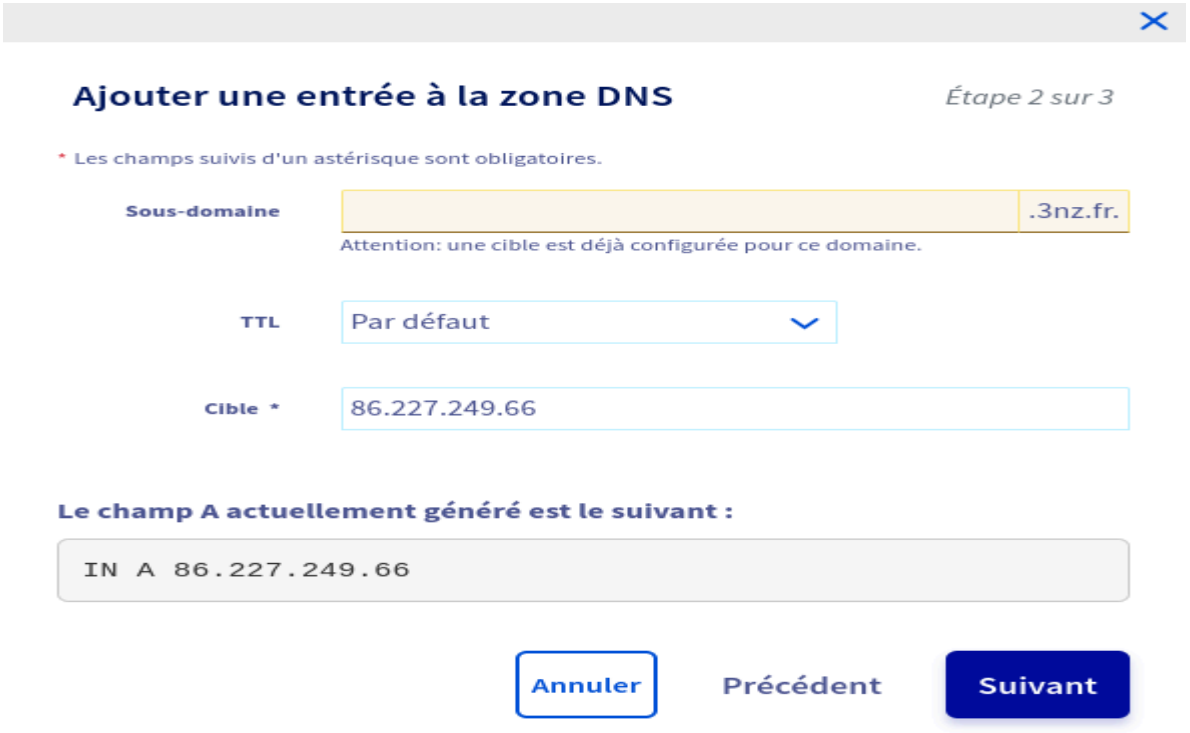


Maintenant, sur mon espace OVH, je vais ajouter des entrées dans ma zone DNS.



Je choisi A en champs de pointage :





- Déploiement du site web 3nz Corp

Une fois cela fait, mon site web portfolio est bien accessible sur internet, en exposant, uniquement l'adresse publique de mon reverse proxy nginx.

Maintenant, création du site web de l'entreprise 3nz Corp :

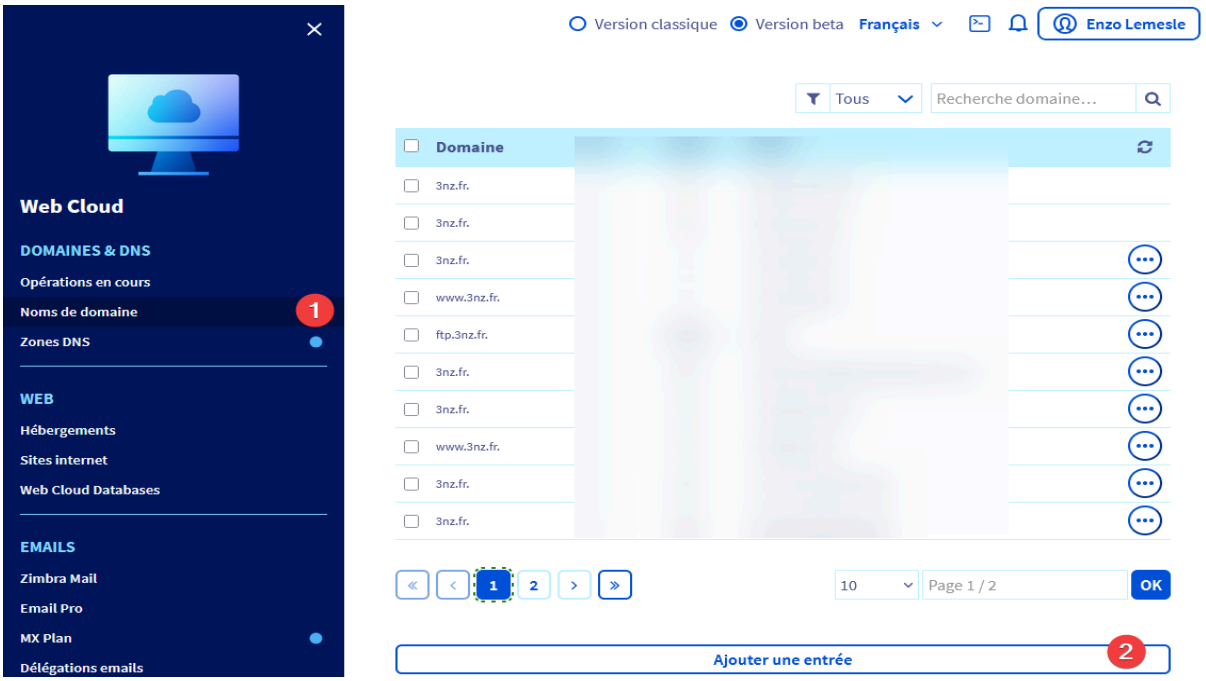
Etape 1 : Création du Site (CT Debian 12 - 192.168.40.20)

vim /etc/nginx/sites-available/

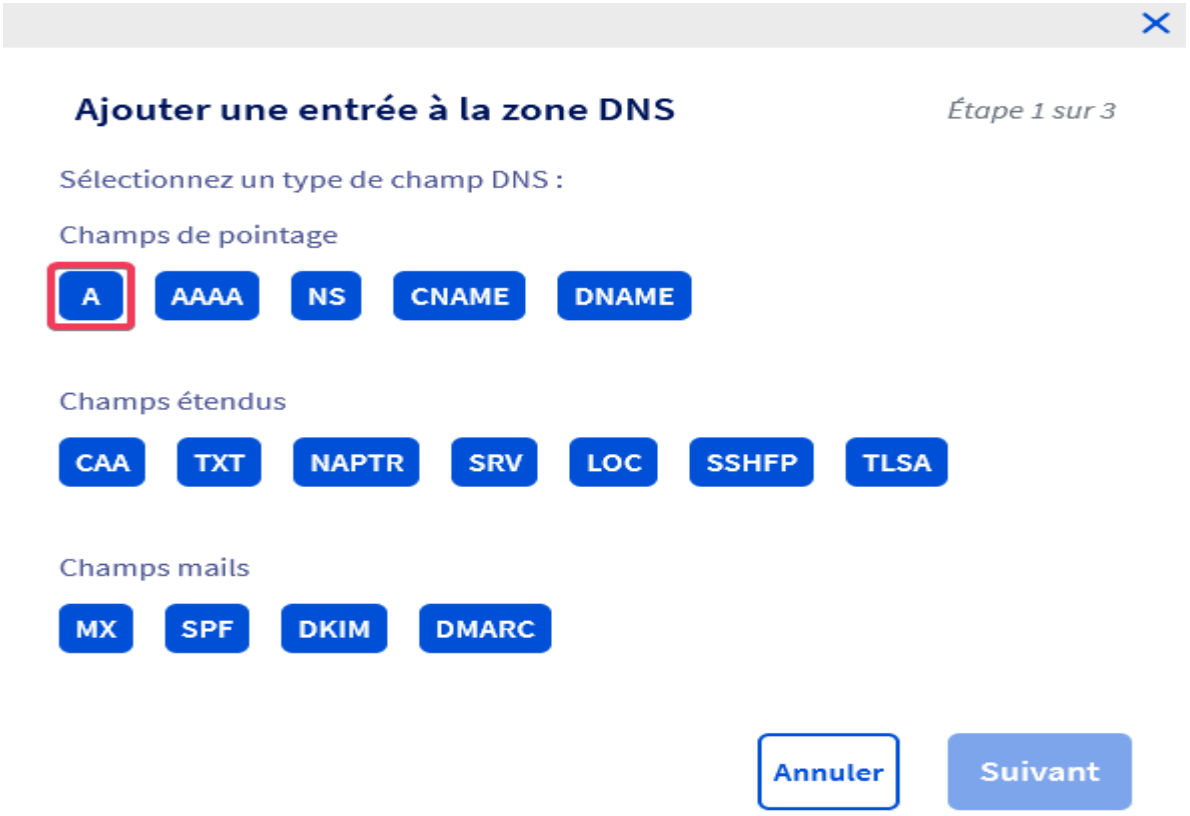
Je déplace les fichiers .html et .css dans le dossier /var/www/html

Etape 2 : Configuration DNS (OVH)

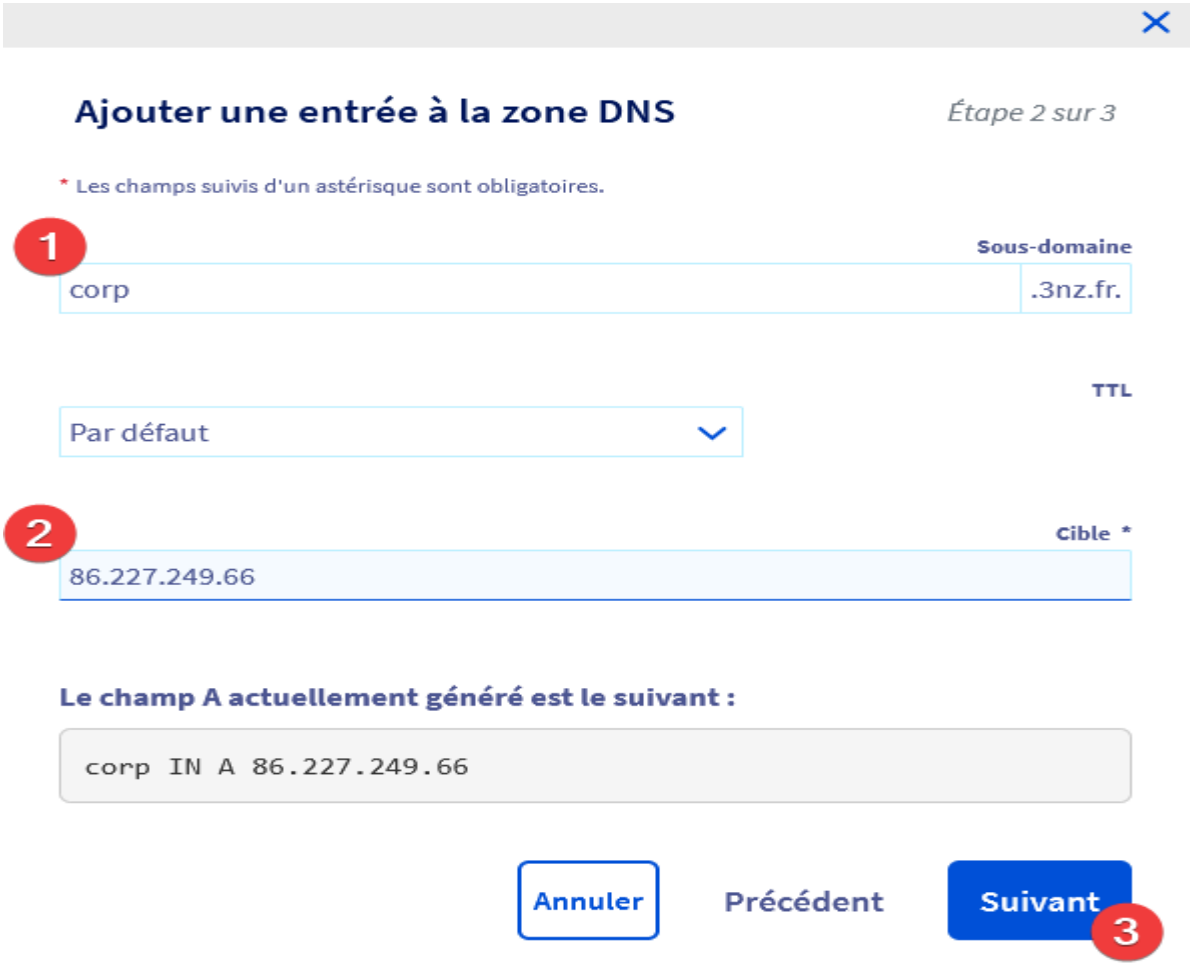
Maintenant, sur l'interface noms de domaine de mon hébergeur de domaine, en l'occurrence OVH, j'ajoute une entré DNS :



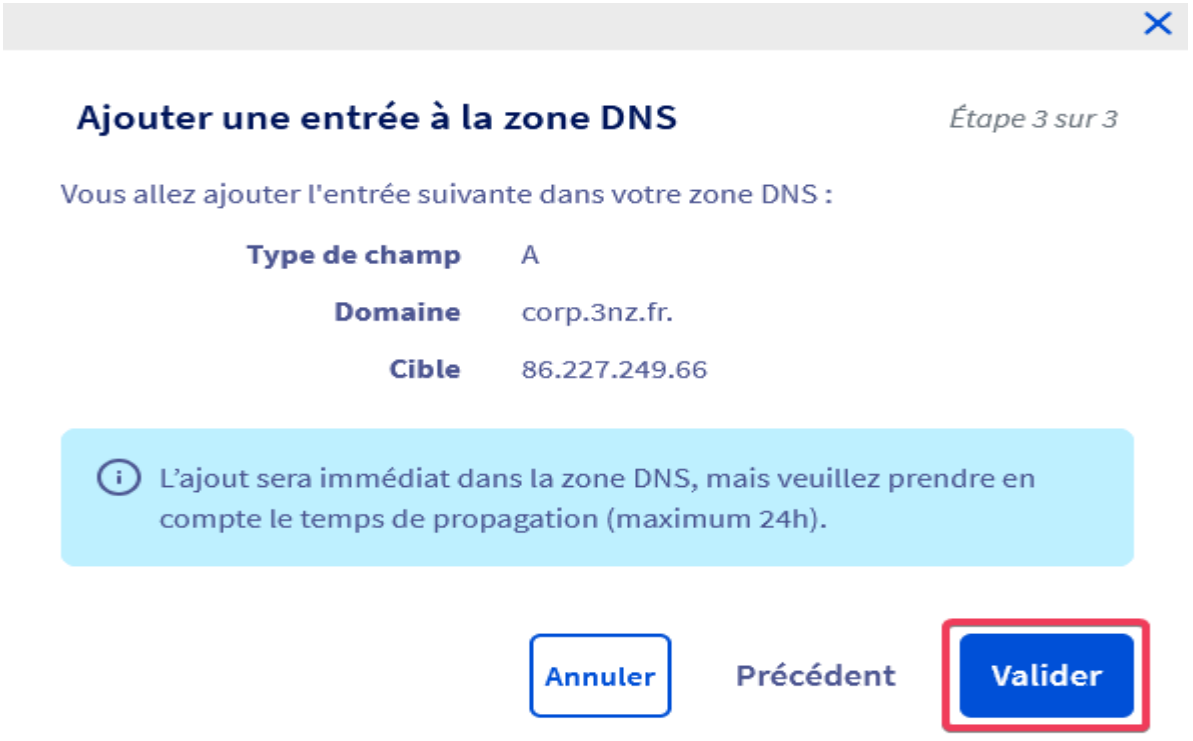
J’ajoute une entrée A :



Appuyer sur suivant et remplissez le nom de votre sous-domaine, ainsi que la cible (mon ip publique) :



Pour la troisième étape, valider :



Etape 3 : Configuration du Reverse Proxy

Création du fichier de configuration :

```
vim /etc/nginx/sites-available/corp.conf
```

```
server {
    server_name corp.3nz.fr;

    location / {
        proxy_pass http://192.168.40.20;
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    }

    listen 443 ssl; # managed by Certbot
    ssl_certificate /etc/letsencrypt/live/corp.3nz.fr/fullchain.pem; # managed by Certbot
    ssl_certificate_key /etc/letsencrypt/live/corp.3nz.fr/privkey.pem; # managed by Certbot
    include /etc/letsencrypt/options-ssl-nginx.conf; # managed by Certbot
    ssl_dhparam /etc/letsencrypt/ssl-dhparams.pem; # managed by Certbot

}
server {
    if ($host = corp.3nz.fr) {
        return 301 https://$host$request_uri;
    } # managed by Certbot


    listen 80;
    server_name corp.3nz.fr;
    return 404; # managed by Certbot


}
```

L'activation SSL a été faites via Certbot avec cette commande :

```
certbot --nginx -d corp.3nz.fr
```

Le site est maintenant sur le WEB !

Mise en place de Fail2Ban sur le Reverse Proxy :

On commence par mettre à jour les paquets :

```
apt update && apt upgrade
```

Installation du paquet Fail2Ban :

```
apt install fail2ban -y
```

Etape 2 : Configuration de la "Prison" (Jail)

Fail2Ban ne doit jamais être configuré dans le fichier jail.conf (car il est écrasé lors des mises à jour). Je vais créer un fichier jail.local.

```
vim /etc/fail2ban/jail.local
```

Voici le contenu de mon fichier :

```
[DEFAULT]
# backend systemd pour eviter les erreurs sur LXC
backend = systemd
bantime = 1h
findtime = 10m
maxretry = 5
ignoreip = 127.0.0.1/8 192.168.0.0/16

# Desactiver SSH pour eviter l'erreur de log manquant
[sshd]
enabled = false

# --- Prisons Nginx ---
# On force le backend sur 'auto' pour lire les fichiers logs nginx

[nginx-botsearch]
enabled = true
backend = auto
port    = http,https
logpath = /var/log/nginx/access.log
maxretry = 2

[nginx-http-auth]
enabled = true
backend = auto
port    = http,https
logpath = /var/log/nginx/error.log

[nginx-limit-req]
enabled = true
backend = auto
port    = http,https
logpath = /var/log/nginx/error.log
```

Etape 3 : Test de fail2ban

Après avoir fait une requête avec mon téléphone en 5G suspicieuse du genre : corp.3nz.fr/phpmyadmin

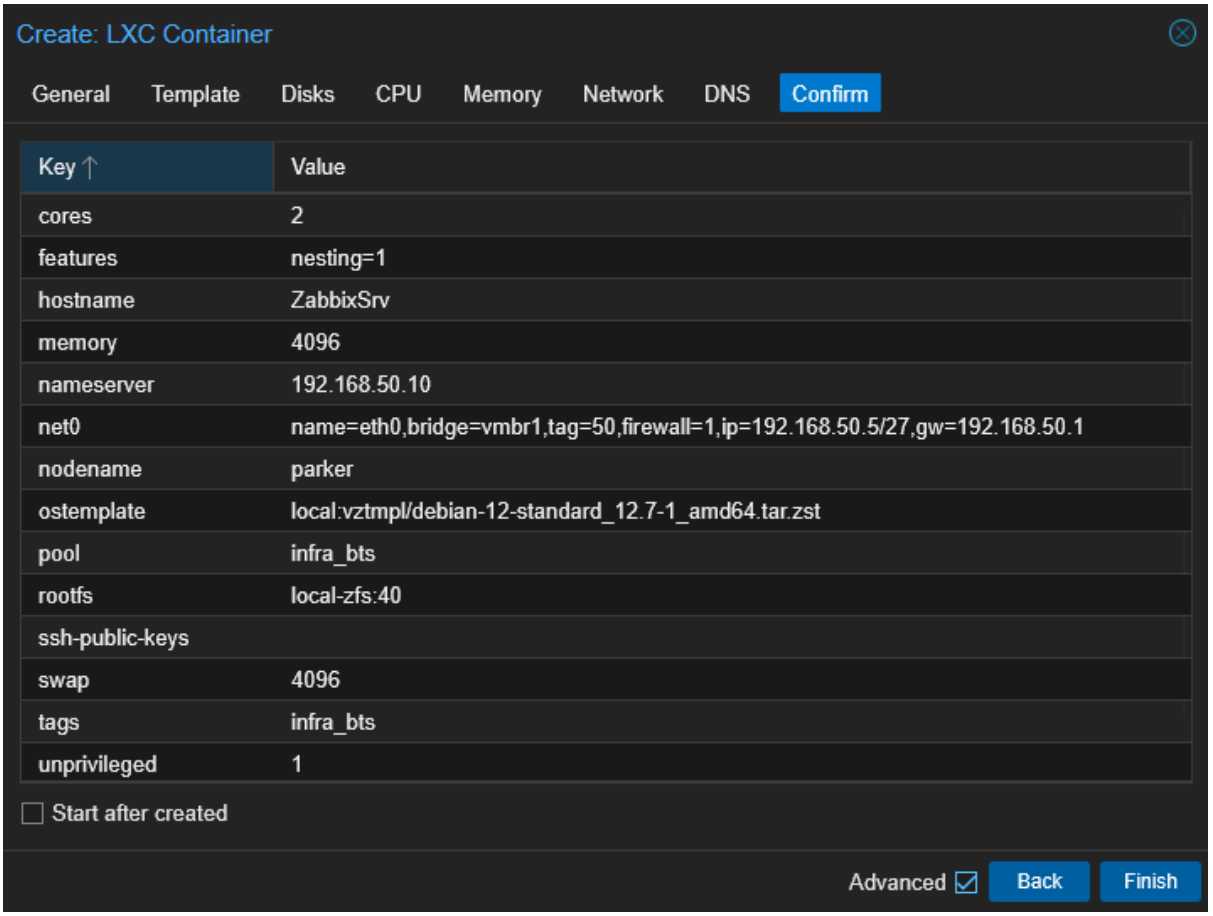
```
root@ReverseProxy:/# fail2ban-client status nginx-botsearch
Status for the jail: nginx-botsearch
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     8
|  `- File list:        /var/log/nginx/access.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   37.167.12.241
```

Je suis bien banni !

VI. Supervision Proactive

- Installation Zabbix

Création du LXC Debian 12 qui héberge le serveur Zabbix :



Une fois le LXC crée :

```
apt -y update && apt upgrade && apt full-upgrade && apt autoclean && apt clean
```

```
apt install mariadb-server mariadb-client -y
```

```
systemctl start mariadb
systemctl enable mariadb
```

```
mysql_secure_installation
```

Ajout du dépôt Zabbix :

```
root@ZabbixSrv:~# wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_latest+debian12_all.deb
```

```
dpkg -i zabbix-release_latest+debian12_all.deb
```

```
apt update
```

Installation de Zabbix et de ses dépendances :
```
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent -y
```

Connection à la DB :
```
mysql -u root -p
```
Préparation de la DB :
```
root@ZabbixSrv:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 42
Server version: 10.11.14-MariaDB-0+deb12u2 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> CREATE USER 'zabbix'@'localhost' IDENTIFIED BY '[redacted]';
Query OK, 0 rows affected (0.012 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
Query OK, 0 rows affected (0.012 sec)

MariaDB [(none)]> SET GLOBAL log_bin_trust_function_creators = 1;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> EXIT;
Bye
```

Importation du **schéma initial** de Zabbix en utilisant le mot de passe de votre utilisateur **"zabbix"** :
```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix
```

Désactivation de l'option log_bin_trust_function_creators :
```
mysql -u root -p -e "SET GLOBAL log_bin_trust_function_creators = 0;"
```

Configurer Zabbix Server :

```
nano /etc/zabbix/zabbix_server.conf
```

Trouvez et modifiez les lignes suivantes :

```
DBPassword=VotreMotDePasseZabbix
EnableGlobalScripts=1
```

Configurer Apache et PHP

```
nano /etc/zabbix/apache.conf
```

Ajouter cette ligne dans la section “mod_php7.c” :

```
php_value date.timezone Europe/Paris
```

Puis redémarrer apache pour appliquer les modifications :

```
sudo a2enmod php8.2
sudo systemctl restart apache2
sudo systemctl enable apache2
```

Configuration du pare-feu sur le serveur zabbix :

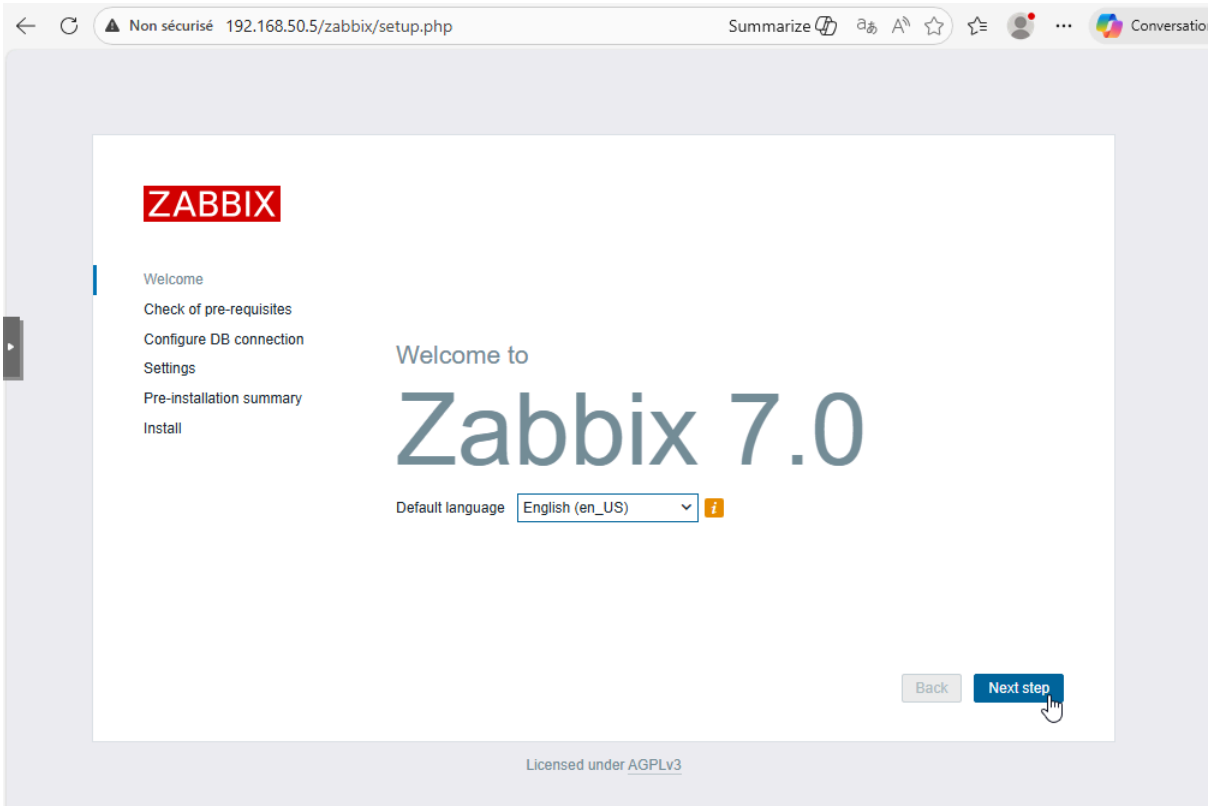
```
sudo apt install -y iptables
sudo iptables -A INPUT -p tcp --dport 10051 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 10050 -j ACCEPT
sudo mkdir -p /etc/iptables
sudo sh -c "iptables-save > /etc/iptables/rules.v4"
sudo iptables-restore < /etc/iptables/rules.v4
```

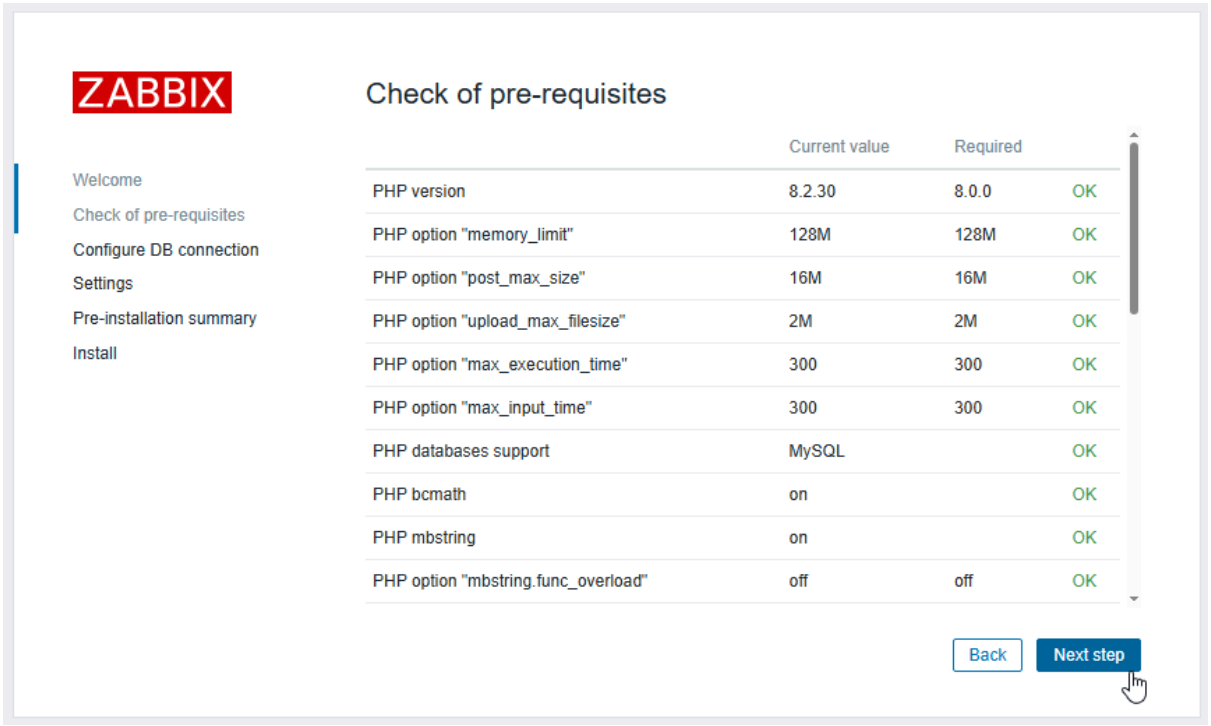
Démarrer les services Zabbix :

```
sudo systemctl restart zabbix-server zabbix-agent apache2
sudo systemctl enable zabbix-server zabbix-agent apache2
```

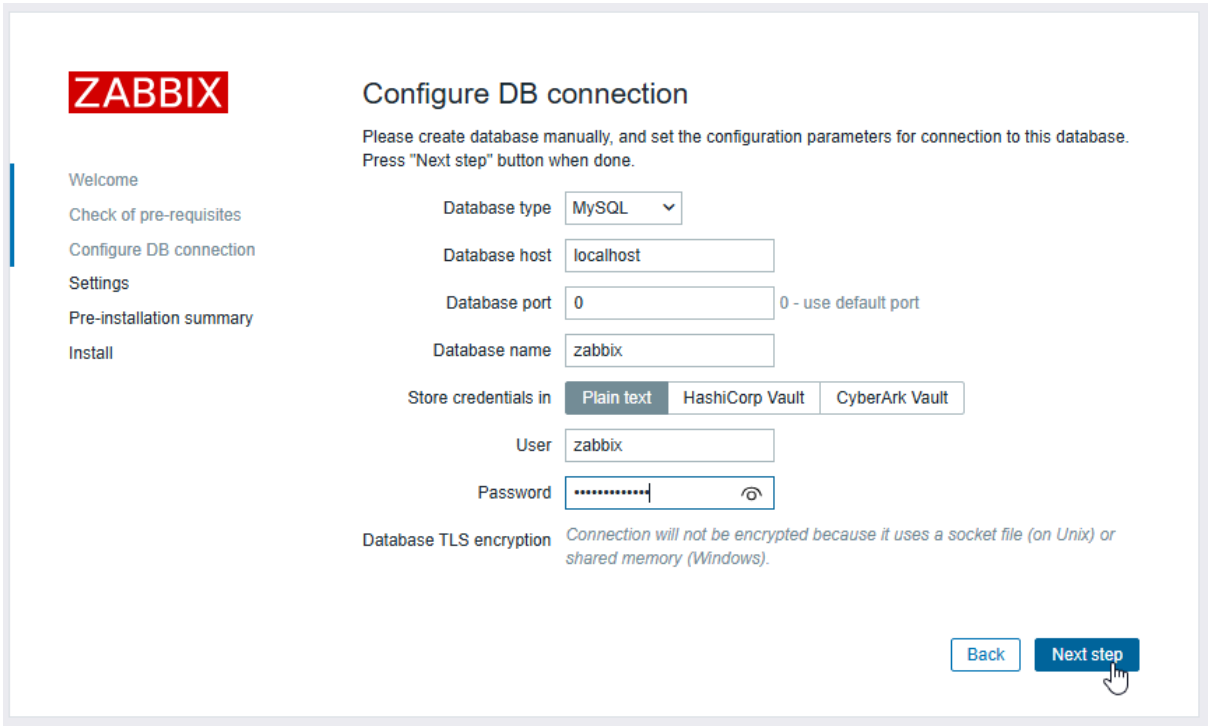
Accès à l'interface WEB de Zabbix :

http://<adresse_ip_serveur>/zabbix

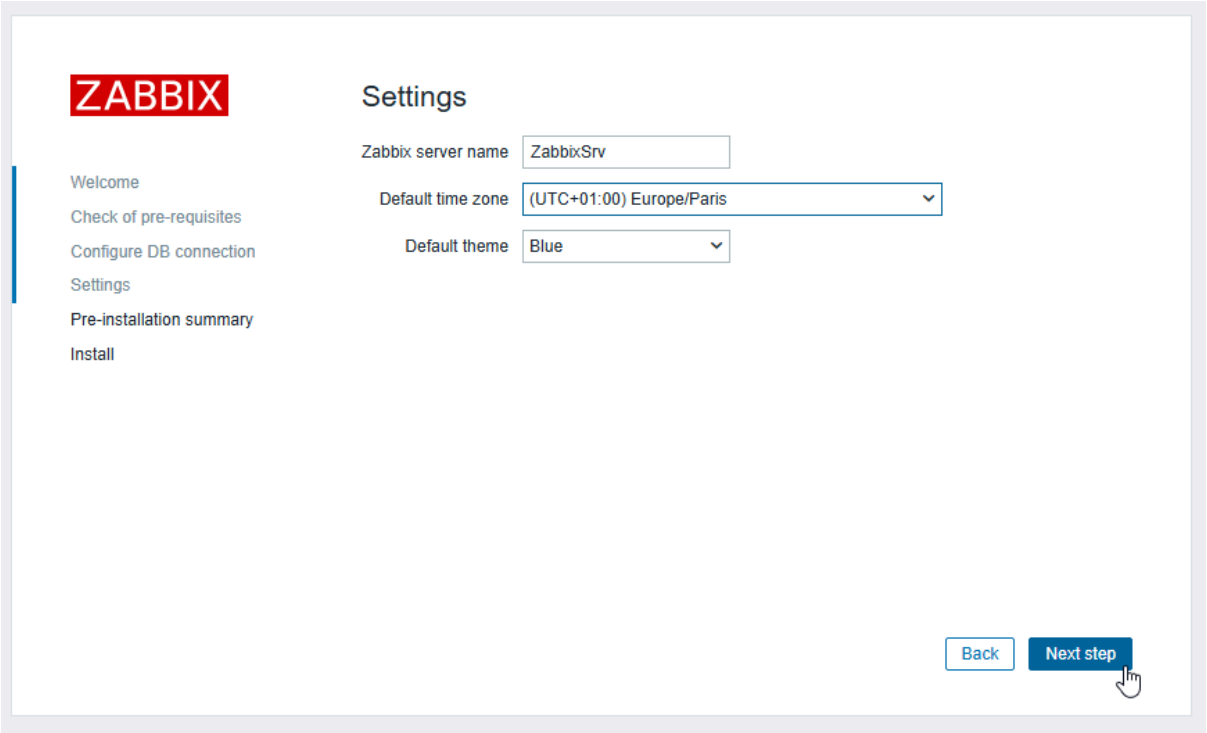




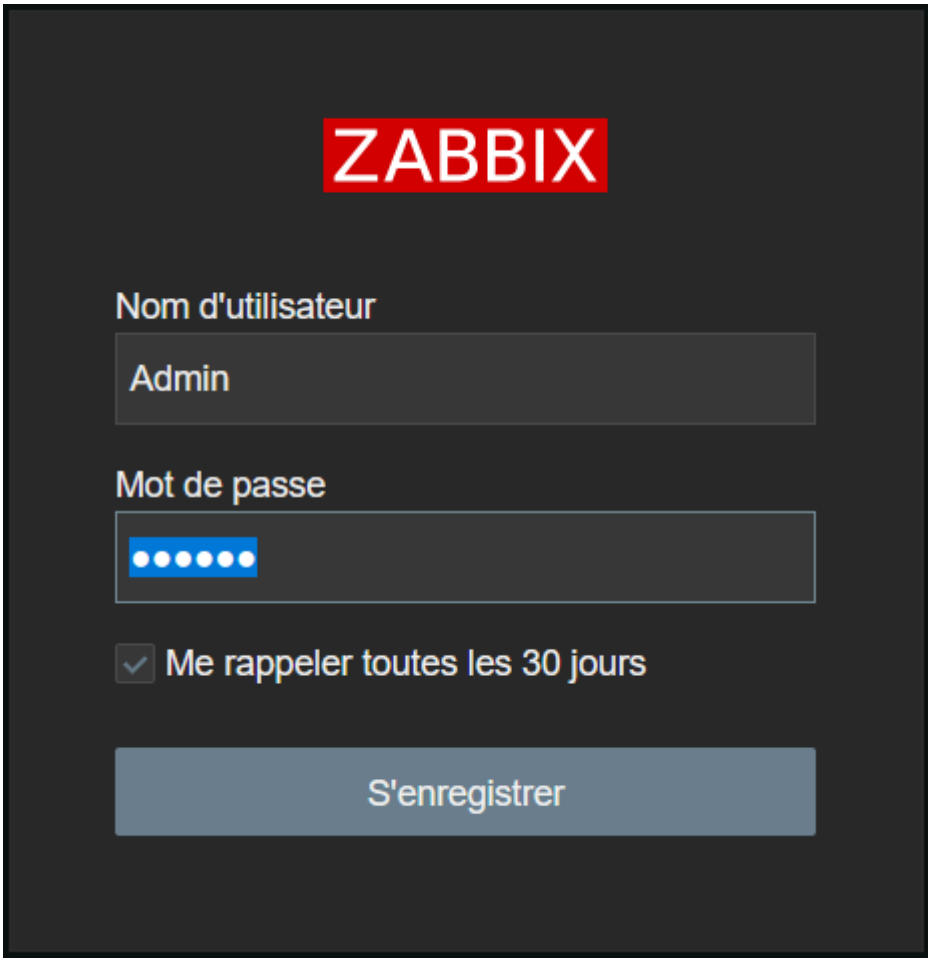
Renseigner le user ainsi que le mot de passe :



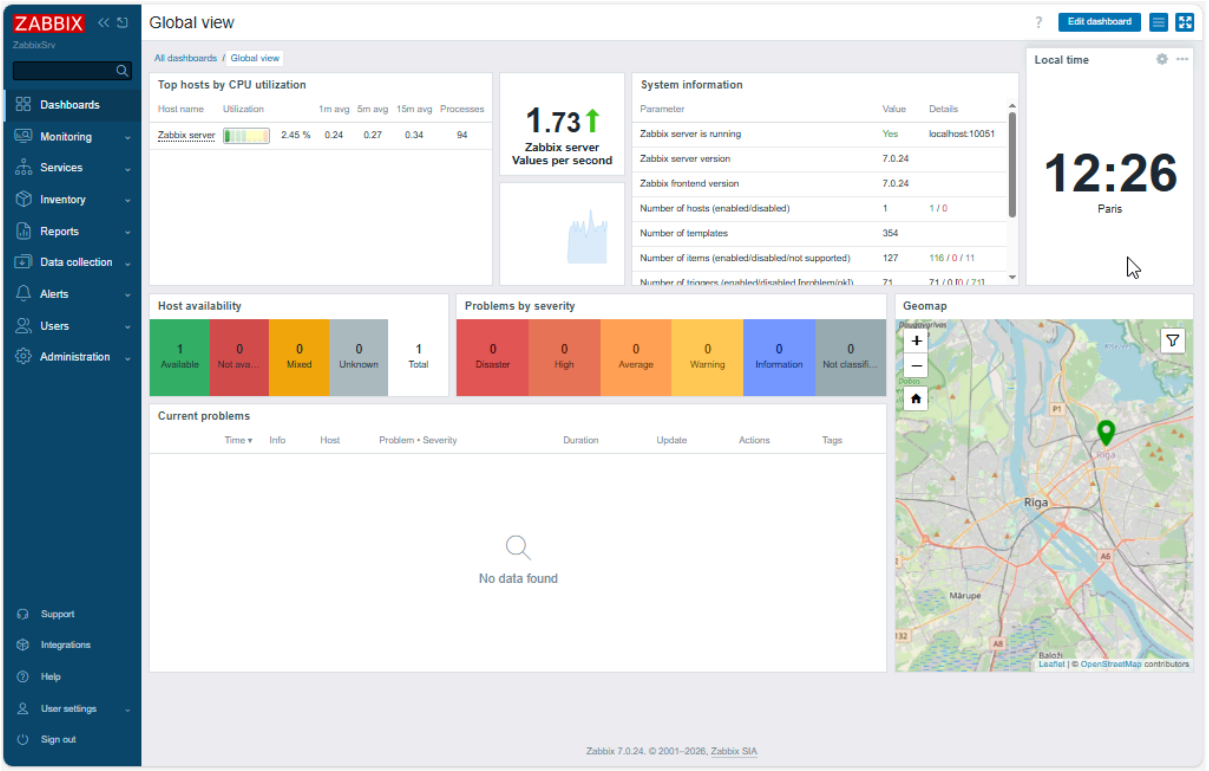
Renseigner votre fuseau horaire :



Dès que l'installation est fini il faut se connecter avec Admin et mdp zabbix



Voilà, j'ai accès à l'interface web de zabbix :



- Installation des agents Zabbix

Pour superviser un appareil, installez l'agent Zabbix sur celui-ci.

Exemple pour des postes sur debian 12 :
`apt install zabbix-agent -y`

Modifiez le **fichier de configuration de l'agent** pour indiquer l'adresse de votre serveur Zabbix :
`nano /etc/zabbix/zabbix_agentd.conf`

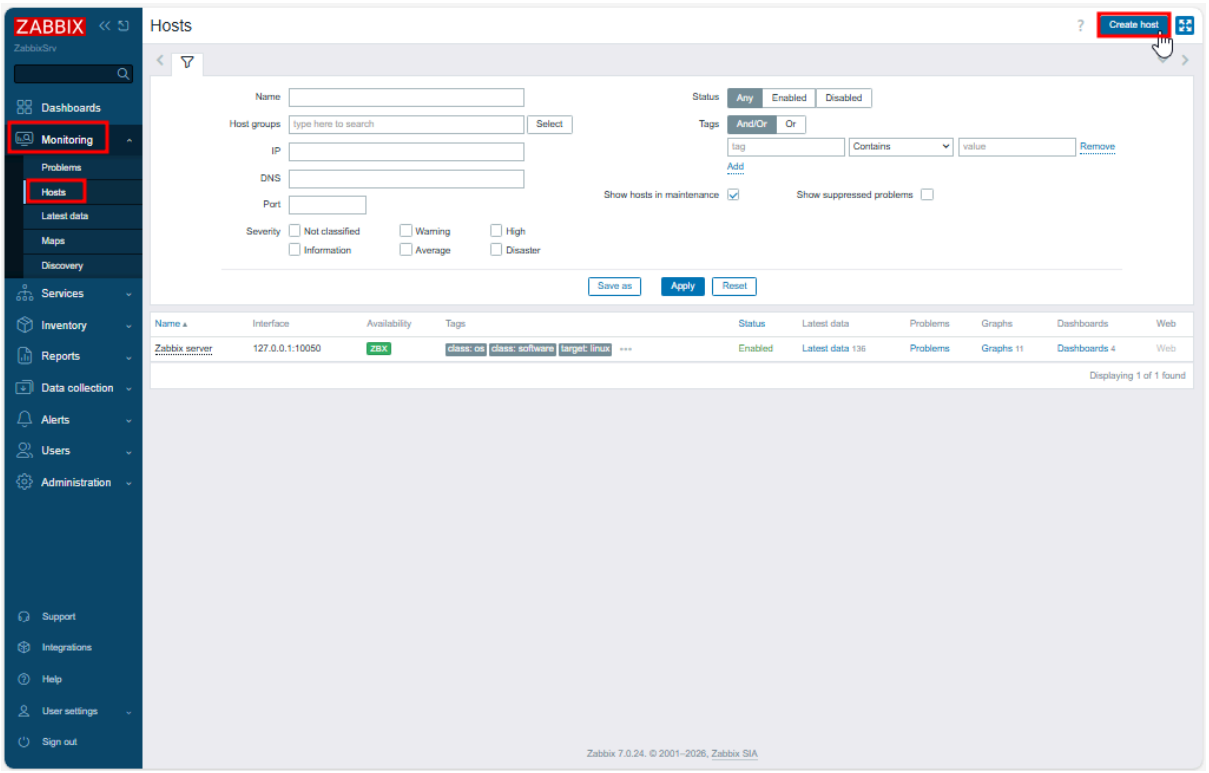
Modifier ces lignes :
`Server=<ip_de_votre_serveur_zabbix>`
`ServerActive=<ip_de_votre_serveur_zabbix>`
`Hostname=<nom_de_votre_serveur_a_ajouter>`

Appliquer les modifications :
`systemctl restart zabbix-agent`
`systemctl enable zabbix-agent`

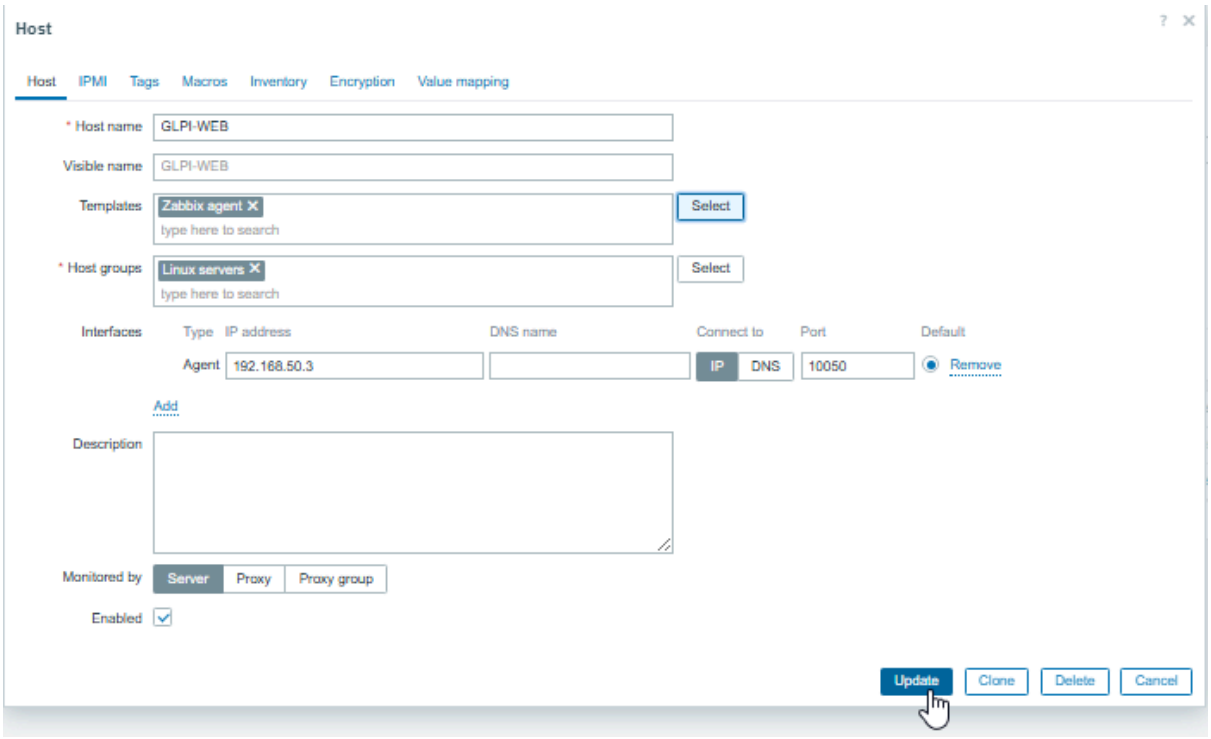
Afin que l’agent Zabbix remonte bien, j’autorise le flux :

☐	✔	0/0 B	IPv4 TCP	192.168.50.5	*	SERVEURS subnets	10050	*	none	Remonter glpi agent
☐	✔	0/0 B	IPv4 TCP	192.168.50.5	*	DMZ subnets	10050	*	none	Remonter glpi agent

Accédez au menu **"Surveillance"**, puis cliquez sur **"Hôtes"** et enfin sur **"Créer un hôte".**

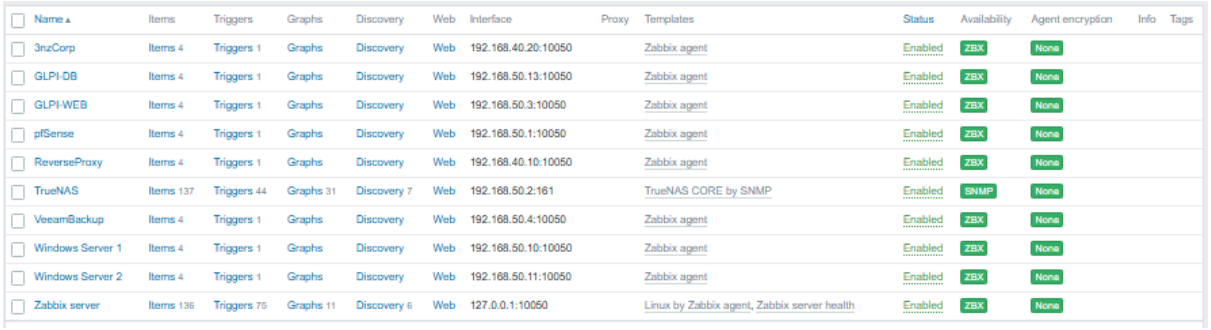


Remplir les champs :



Mon serveur GLPI-WEB est bien remonté et disponible :

Après avoir installé tous les agents zabbix sur les machines que je souhaitais monitorer mes hosts ressemble à ça :



Enfin, de retour au dashboard, vous pouvez voir si vos hosts sont disponibles (1) et s'il y a des problèmes (2) :