

# SOMMAIRE

## **I. Haute Disponibilité et Services Windows**

- Configuration d'un second serveur AD/DNS/DHCP pour la redondance
- Disponibilité réseau (Configuration du DHCP Failover)

## **II. Stockage et Plan de Continuité d'Activité (PCA)**

- Installation et configuration de TrueNAS pour le stockage
- Création de pools, datasets et partages SMB avec ACLs
- Déploiement Veeam Backup sur serveur dédié
- Création de référentiel de sauvegarde et automatisation

## **III. Durcissement de la Sécurité (GPO & Postes de travail)**

- Politique de mots de passe
- Restriction des outils d'administration
- Sécurité Physique
- Gestion des privilèges

## **IV. Zone Démilitarisée (DMZ) et Publication Web**

- Création du VLAN 40 (DMZ) et règles de filtrage strictes sur pfSense
- Reverse Proxy Nginx (Point d'entrée unique, certificats SSL Let's Encrypt)
- Sécurisation applicative avec Fail2Ban
- Configuration DNS et Redirection de Ports
- Activation SSL avec Let's Encrypt
- Déploiement du site web 3nz Corp
- Implémentation de Fail2Ban

## **V. Supervision Proactive (Zabbix)**

- Installation du serveur Zabbix
- Installation des agents Zabbix

# 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 :

Key ↑	Value
bios	ovmf
cores	2
cpu	x86-64-v2-AES
efidisk0	local-zfs:1,efitype=4m,pre-enrolled-keys=1
ide0	local-zfs:32
ide2	local:iso/windows_server_2022.iso,media=cdrom
machine	q35
memory	4096
name	WinSrv2
net0	e1000,bridge=vibr1,tag=50,firewall=1
nodename	parker
numa	0
ostype	win11
scsihw	virtio-scsi-single

Start after created

Advanced  Back Finish

\*Pour l'installation voir l'installation du serveur main\*

Changement du nom :

```
1) Domaine ou groupe de travail : Groupe de travail : WORKGROUP
2) Nom de l'ordinateur : WIN-20RTSDJUK6A
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: 2_
```

```
Nom de l'ordinateur actuel : WTN-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 : 255.255.255.0
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
```

## Assignment 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.
```

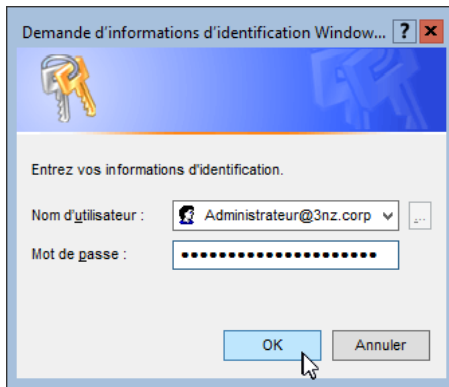
## Mise en redondance :

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)
```



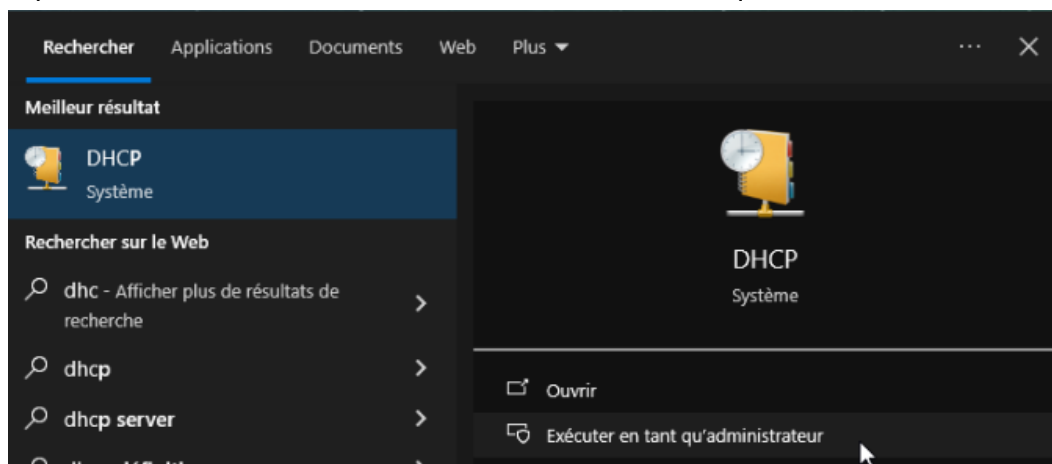
- Mise en place du DHCP Failover pour la haute disponibilité

Redondance DHCP (DHCP Failover) :

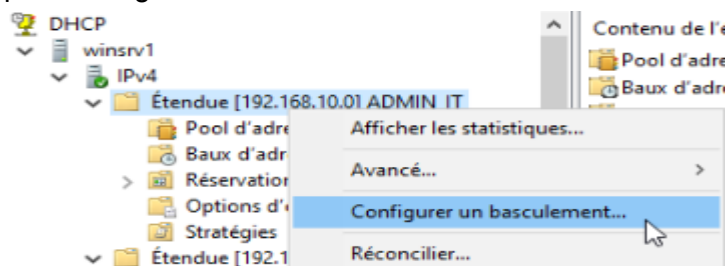
Installation de l'outil RSAT DHCP sur une machine cliente avec droit Administrateur :

```
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 :



**Configurer un basculement**

**Introduction au basculement DHCP**

Le basculement DHCP permet la haute disponibilité des services DHCP en synchronisant les informations des baux d'adresses IP entre deux serveurs DHCP. Le basculement DHCP fournit également un équilibrage de charge en matière de requêtes DHCP.

Cet Assistant vous guide tout au long de la configuration du basculement DHCP. Sélectionnez dans la liste suivante les étendues disponibles pouvant être configurées pour une haute disponibilité. Les étendues déjà configurées pour une haute disponibilité ne figurent pas dans la liste ci-dessous.

Étendues disponibles :  Sélectionner tout

192.168.10.0

< Précédent   **Suivant >**   Annuler

**Configurer un basculement**

**Spécifier le serveur partenaire à utiliser pour le basculement**

Indiquez le nom d'hôte ou l'adresse IP du serveur DHCP partenaire à utiliser pour la configuration du basculement.

Vous pouvez effectuer votre sélection parmi la liste des serveurs avec une configuration de basculement existant, ou vous pouvez rechercher et sélectionner le serveur approprié dans la liste des serveurs DHCP autorisés.

Vous pouvez également taper le nom d'hôte ou l'adresse IP du serveur partenaire.

Serveur partenaire : WinSrv2  

Réutiliser les relations de basculement existantes configurées avec ce serveur (le cas échéant).

< Précédent   **Suivant >**   Annuler

**Configurer un basculement**

**Créer une relation de basculement**

Créer une relation de basculement avec le partenaire WinSrv2

Nom de la relation : winsrv1-winsrv2

Délai de transition maximal du client (MCLT) : 0 heures 10 minutes

Mode : Serveur de secours

Configuration du serveur de secours

Rôle du serveur partenaire : Veille

Adresses réservées pour le serveur de secours : 10 %

Intervalle de basculement d'état : 60 minutes

Activer l'authentification du message

Secret partagé : .....

< Précédent   **Suivant >**   Annuler

**Configurer un basculement**

Un basculement va être configuré entre winsrv1 et WinSrv2 avec les paramètres suivants.

Étendues : 192.168.10.0

Nom de la relation : winsrv1-winsrv2  
Délai de transition maximal du client (MCLT) : 0 h 10 min  
Mode : Serveur de sec  
Intervalle de basculement d'état : Désactivé

Configuration du serveur de secours

Rôle du serveur partenaire : Veille  
Adresses réservées pour le serveur 10 %

< Précédent   **Terminer**   Annuler

Refaire les mêmes actions pour les différentes étendues.

**DHCP**

- winsrv1
  - IPv4
    - Étendue [192.168.10.0] ADMIN\_IT
    - Étendue [192.168.20.0] COLLABORATEURS
    - Étendue [192.168.30.0] DIRECTION
    - Étendue [192.168.50.0] SERVEUR
    - Étendue [192.168.99.0] INFRA
    - Options de serveur
    - Stratégies
    - Filtres
  - IPv6
- winsrv2
  - IPv4
    - Options de serveur
    - Étendue [192.168.10.0] ADMIN\_IT
    - Étendue [192.168.20.0] COLLABORATEURS
    - Étendue [192.168.50.0] SERVEUR
    - Étendue [192.168.99.0] INFRA
    - Étendue [192.168.30.0] DIRECTION
    - Stratégies
    - Filtres
  - IPv6

## II. Stockage et PCA

- Installation et configuration de TrueNAS pour le stockage

Création de la VM TrueNAS :

Create: Virtual Machine ⊗

General OS System Disks CPU Memory Network **Confirm**

Key ↑	Value
cores	2
cpu	x86-64-v2-AES
ide0	local-zfs:32
ide2	local:iso/TrueNAS-13.0-U6.7.iso,media=cdrom
memory	16384
name	truenas
net0	e1000,bridge=vibr1,tag=50,firewall=1
nodename	richards
numa	0
ostype	other
sata0	local-zfs:32
sata1	local-zfs:32
sata2	local-zfs:32
scsihw	virtio-scsi-single

Start after created

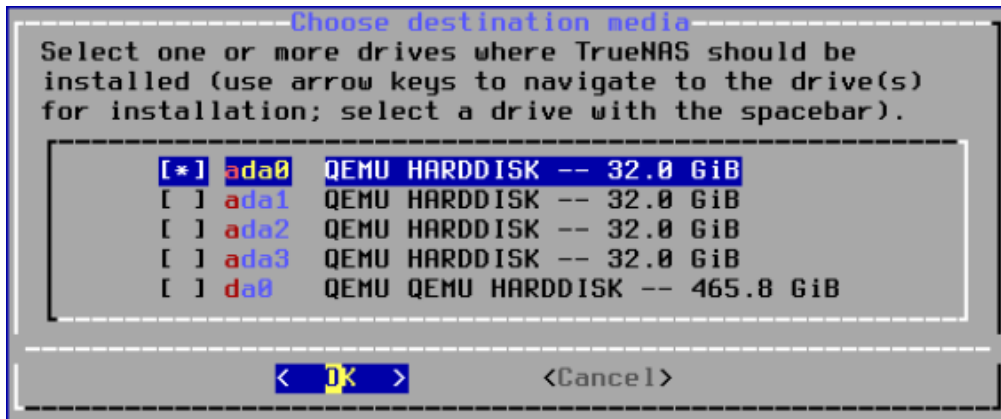
Advanced  **Back** **Finish**

Installation de TrueNAS :

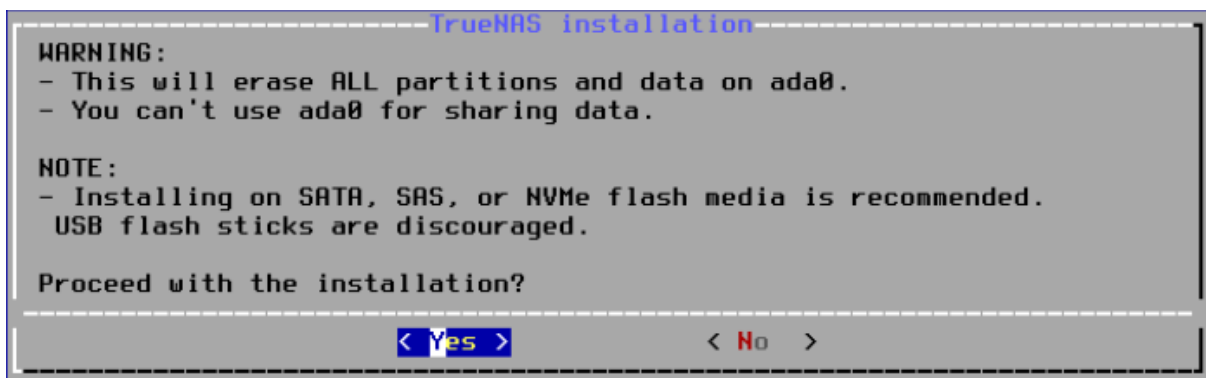
Sélectionnez install/upgrade :

```
----- TrueNAS 13.0-U6.7 Console Setup -----
|
|          1 Install/Upgrade
|          2 Shell
|          3 Reboot System
|          4 Shutdown System
|
|-----|
|          < OK >          <Cancel>
|-----|
```

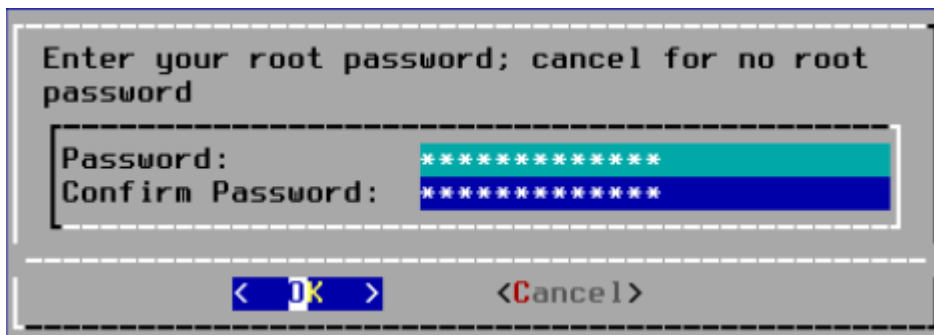
Choisir le disque d'installation :



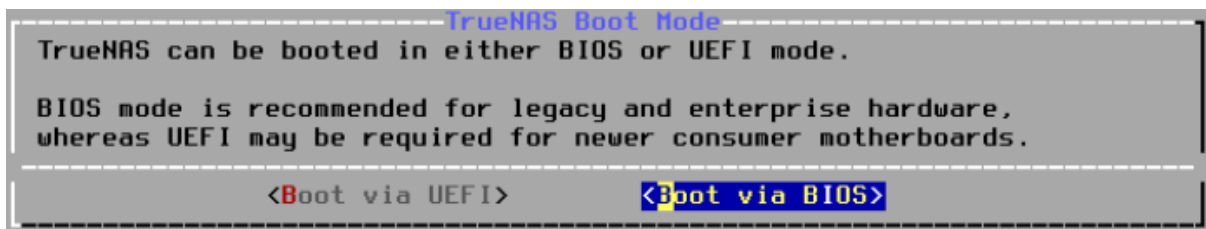
Je sélectionne : YES



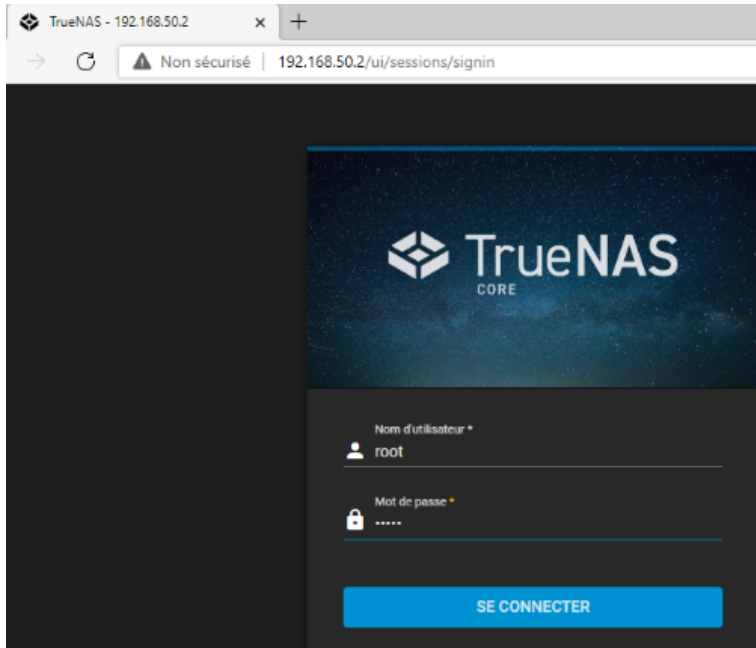
Configuration du mot de passe puis OK



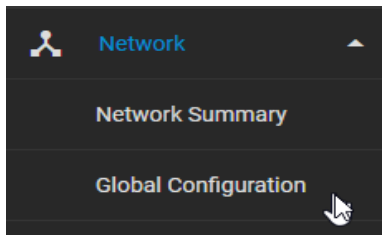
BOOT via BIOS :



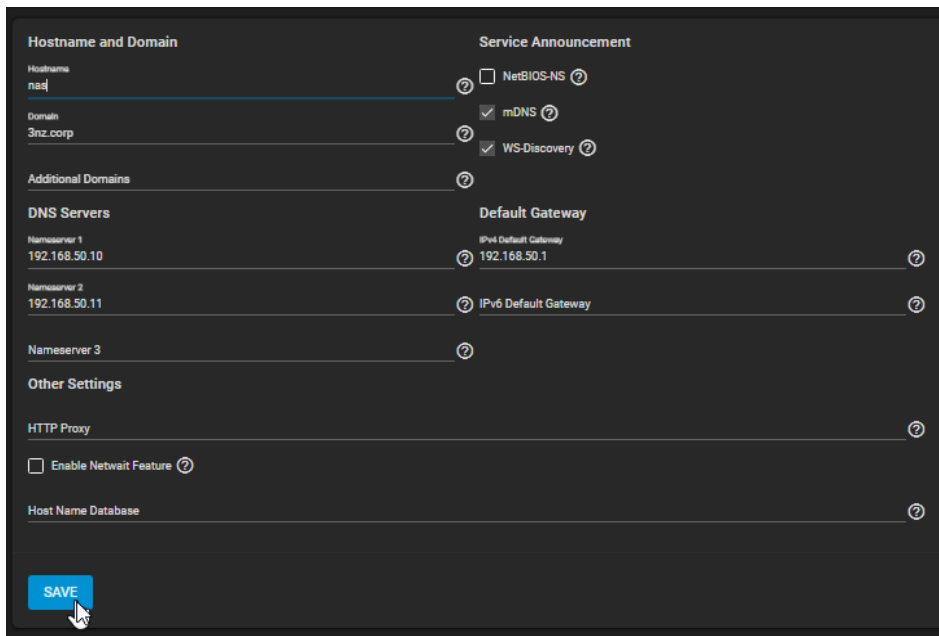
Maintenant se connecter à l'interface WEB de TRUENAS :



Network -> Global Configuration

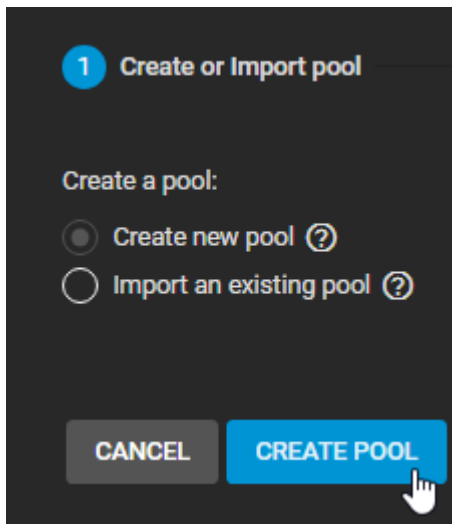
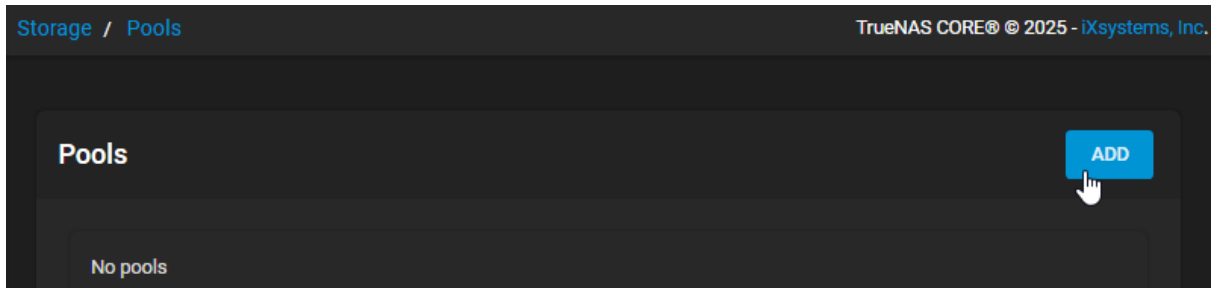


Changer le hostname, domain, DNS servers et la gateway



- Création de pools, datasets et partages SMB avec ACLs

Création d'un pool Stockage -> Pools



Choisir le nom et les disques

Name \*  
COMMUN  Encryption

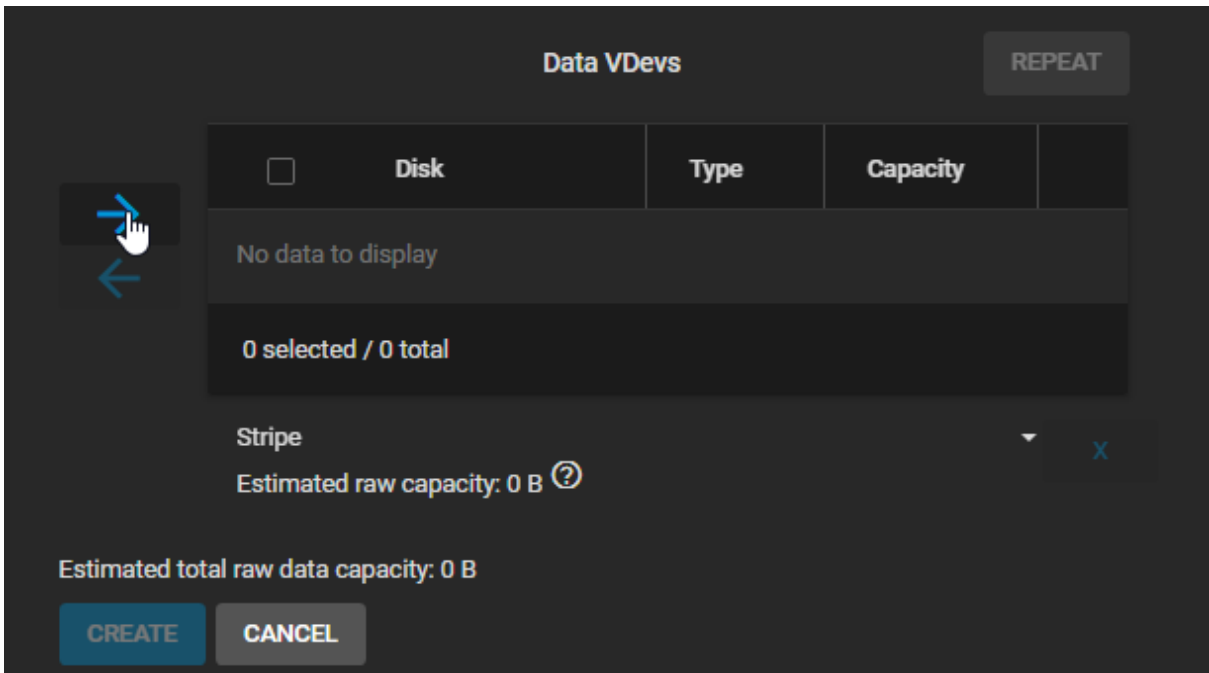
RESET LAYOUT SUGGEST LAYOUT  ADD VDEV ▾

Available Disks

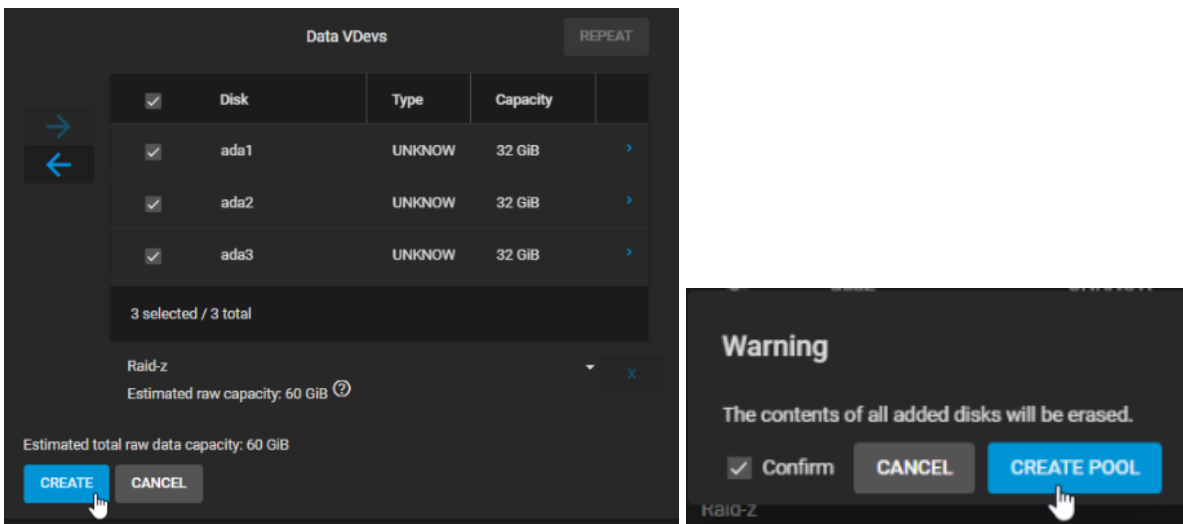
<input type="checkbox"/>	Disk	Type	Capacity	
<input checked="" type="checkbox"/>	ada1	UNKNO	32 GiB	>
<input checked="" type="checkbox"/>	ada2	UNKNO	32 GiB	>
<input checked="" type="checkbox"/>	ada3	UNKNO	32 GiB	>
<input type="checkbox"/>	da0	UNKNO	465.76 GiB	>

3 selected / 4 total

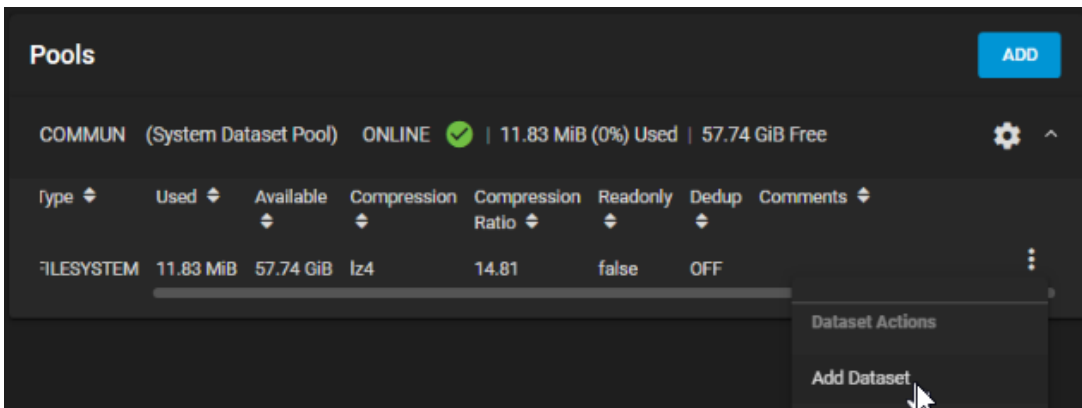
Cliquez sur la flèche en surbrillance bleue pour assigner les disques sélectionnés



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 :

The screenshot shows the configuration interface for a dataset named 'COLLABORATEURS'. It includes sections for 'Name and Options', 'Encryption Options', and 'Other Options'. The 'Name and Options' section contains fields for Name, Comments, Sync, Compression level, and Enable Attime. The 'Encryption Options' section has a checked checkbox for 'Inherit (non-encrypted)'. The 'Other Options' section includes ZFS Deduplication, Case Sensitivity, and Share Type. At the bottom, there are buttons for 'SUBMIT', 'CANCEL', and 'ADVANCED OPTIONS'.

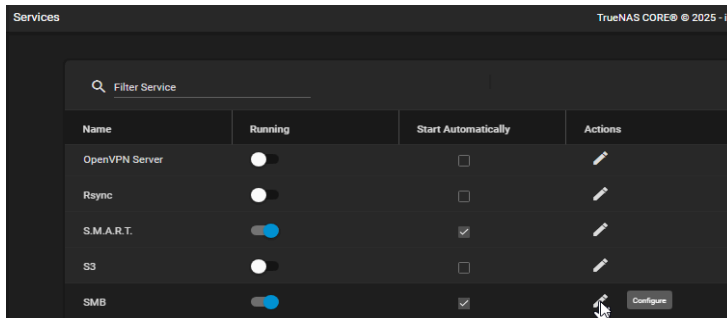
Dans Advanced Options je choisi de lui attribuer 15 GiB de quota pour lui et ses enfants :

This screenshot shows the 'Advanced Options' section of the configuration interface. It features fields for 'Quota for this dataset' (set to 15 GiB) and 'Quota for this dataset and all children' (set to 15 GiB). There are also checkboxes for 'Quota warning alert at, %' and 'Quota critical alert at, %', all of which are set to 'Inherit'. The 'Reserved space for this dataset' and 'Reserved space for this dataset and all children' fields are also visible.

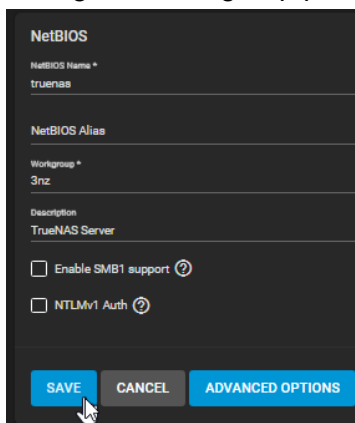
J'en créer 2 autres, DIRECTION et DSI

▼ 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

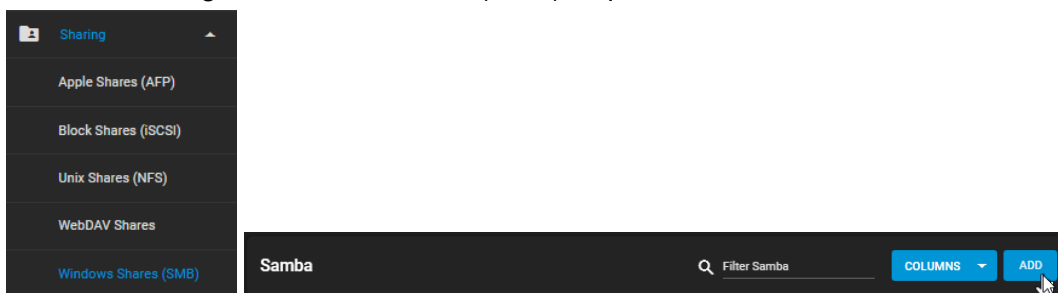
Ensuite, configuration du partage SMB : Services > SMB, on active la case Start AUTOMATICALLY puis configure :



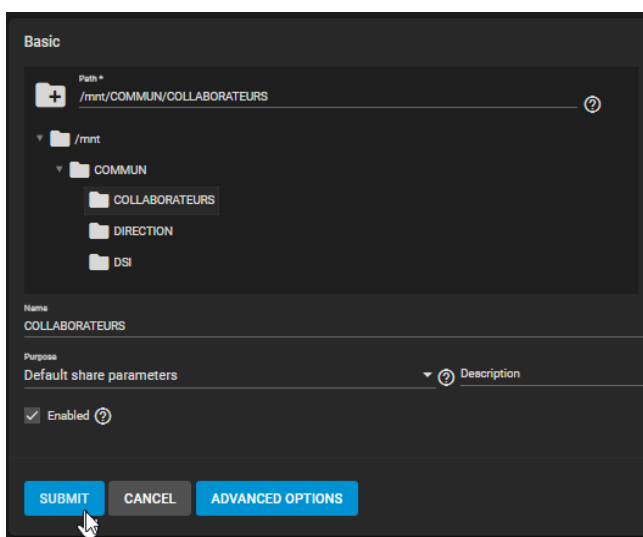
Changez le workgroup puis sauvegardez :



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 :

Localization

Language: English ⓘ

Console Keyboard Map: French (fr) ⓘ

Sort languages by:  Name  Language code

Timezone: Europe/Paris ⓘ

Date Format: 2025-05-29 ⓘ

Time Format: 00:50:41 (24 Hours) ⓘ

Other Options

Crash reporting ⓘ

Usage collection ⓘ

**SAVE** **SAVE CONFIG** **UPLOAD CONFIG** **RESET CONFIG**

Ajout des serveurs NTP :

NTP Server Settings

Address: 192.168.50.10 ⓘ

Burst ⓘ

IBurst ⓘ

Prefer ⓘ

Min Poll: 6 ⓘ

Max Poll: 10 ⓘ

Force ⓘ

**SUBMIT** **CANCEL**

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 :

```
root@nas[~]# ntpdate -u 192.168.50.10
```

Pour forcer la synchronisation ntp.

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

**Domain Credentials**

Domain Name \*  
3nz.corp

Domain Account Name \*  
Administrateur

Domain Account Password  
\*\*\*\*\*

Enable (requires password or Kerberos principal)

Verbose logging  Allow DNS updates

Allow Trusted Domains  Disable TrueNAS Cache

Use Default Domain  Restrict PAM

Site Name DNS Timeout  
Kerberos Realm Winbind NSS Info  
Kerberos Principal Netbios Name \*  
Computer Account OU NetBIOS alias  
AD Timeout

60

**SAVE** **BASIC OPTIONS** **EDIT IDMAP** **REBUILD DIRECTORY SERVICE CACHE**

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

**Access Control List**

Who \*  
Group

Group \*  
collaborateurs

ACL Type \*  
Allow

Permissions Type \*  
Basic

Permissions \*  
Modify

Flags Type \*  
Basic

Flags \*  
Inherit

Who \*  
Group

Group \*  
dsi

ACL Type \*  
Allow

Permissions Type \*  
Advanced

Permissions \*  
Read Data, Write Data, Append Data, Read Named Attributes, Writ...

Flags Type \*  
Basic

Flags \*  
Inherit

**Advanced**

Apply permissions recursively

Apply permissions to child datasets

**SAVE** **CANCEL** **USE PERMISSIONS EDITOR**

Pour le dataset DIRECTION :

Access Control List

Who \*  
Group

Group \*  
direction

ACL Type \*  
Allow

Permissions Type \*  
Basic

Permissions \*  
Modify

Flags Type \*  
Basic

Flags \*  
Inherit

Who \*  
Group

Group \*  
dsi

ACL Type \*  
Allow

Permissions Type \*  
Advanced

Permissions \*  
Read Data, Write Data, Append Data, Read Named Attributes, Writ...

Flags Type \*  
Basic

Flags \*  
Inherit

Advanced

Apply permissions recursively

Apply permissions to child datasets

SAVE CANCEL USE PERMISSIONS EDITOR

Pour le dataset DSI :

Access Control List

Who \*  
Group

Group \*  
dsi

ACL Type \*  
Allow

Permissions Type \*  
Advanced

Permissions \*  
Read Data, Write Data, Append Data, Read Named Attributes, Writ...

Flags Type \*  
Basic

Flags \*  
Inherit

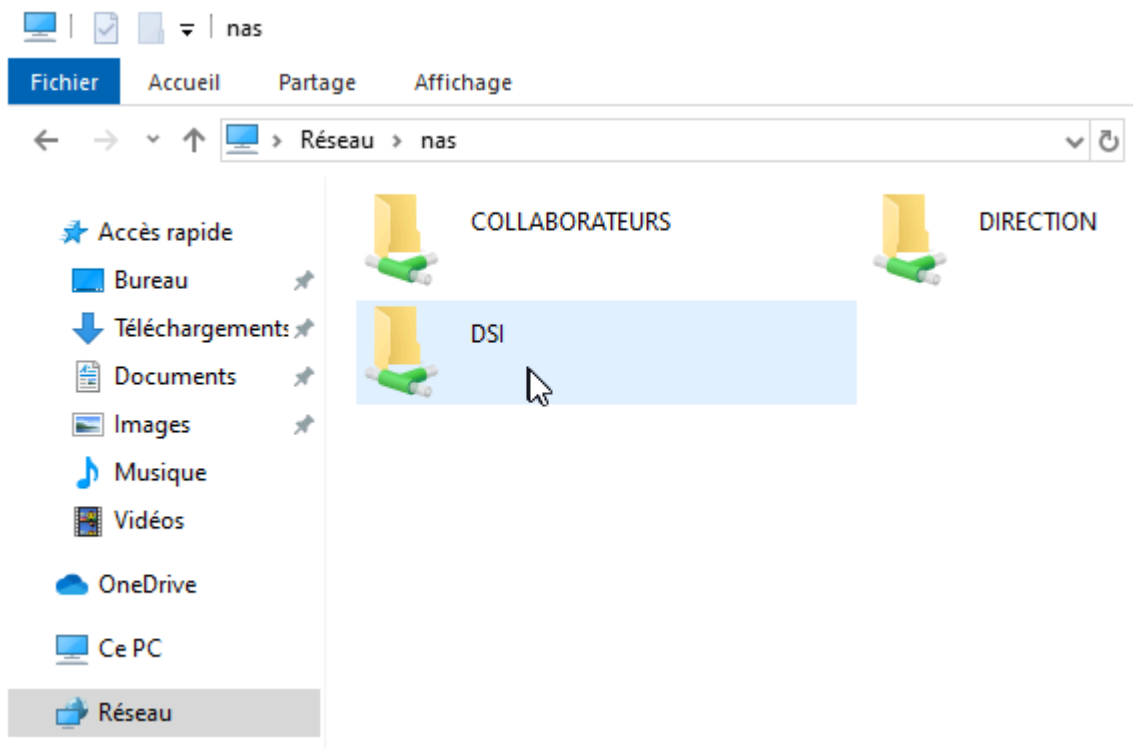
Advanced

Apply permissions recursively

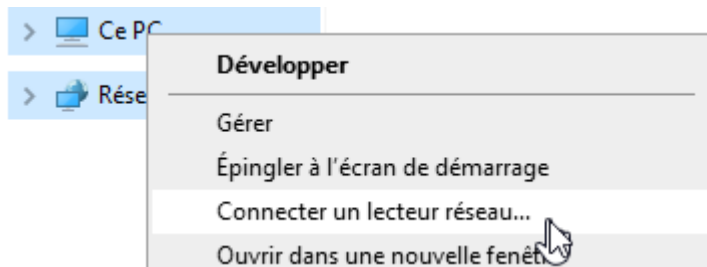
Apply permissions to child datasets


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 :



←  Connecter un lecteur réseau

## À quel dossier réseau voulez-vous vous connecter ?

Spécifiez la lettre désignant le lecteur et le dossier auxquels vous souhaitez vous connecter :

Lecteur :

Dossier :

Exemple : \\serveur\partage

Se reconnecter lors de la connexion




Se connecter à l'aide d'informations d'identification différentes

[Se connecter à un site Web permettant de stocker des documents et des images.](#)

Terminer

Annuler

### ▼ Emplacements réseau (3)

 <b>dsi (\\nas) (E:)</b> 19,9 Go libres sur 20,0 Go	 <b>direction (\\nas) (Y:)</b> 14,9 Go libres sur 15,0 Go
 <b>collaborateurs (\\nas) (Z:)</b> 14,9 Go libres sur 15,0 Go	

- 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 :

Dataset	Schedule
Dataset * COMMUN	Snapshot Lifetime * 1 WEEK
<input checked="" type="checkbox"/> Recursive ?	Naming Schema auto-%d-%m-%Y_%H-%M
Exclude	Schedule * Daily (0 0 * * *) at 00:00 (12:00 AM)
	<input checked="" type="checkbox"/> Allow Taking Empty Snapshots ?
	<input checked="" type="checkbox"/> Enabled ?

---

- 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 :

Create: Virtual Machine

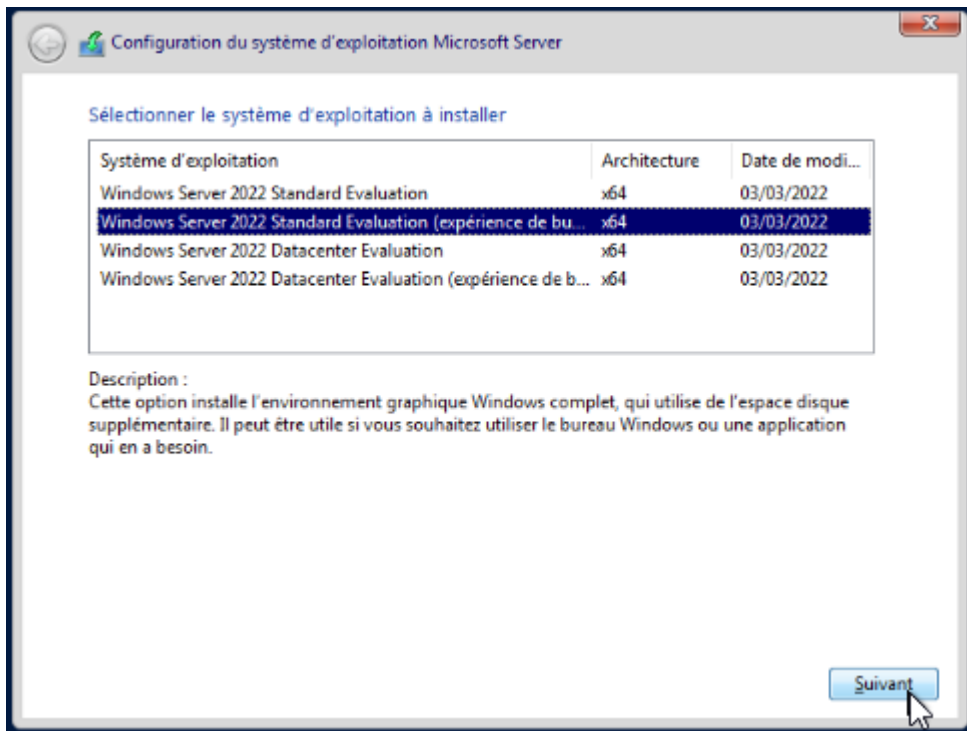
General OS System Disks CPU Memory Network **Confirm**

Key ↑	Value
bios	ovmf
cores	2
cpu	x86-64-v2-AES
efidisk0	local-zfs:1,efitype=4m,pre-enrolled-keys=1
ide0	local-zfs:100
ide2	local:iso/windows_server_2022.iso,media=cdrom
machine	q35
memory	6144
name	veeam
net0	e1000,bridge=vibr1,tag=50,firewall=1
nodename	parker
numa	0
ostype	win11
scsihw	virtio-scsi-single

Start after created

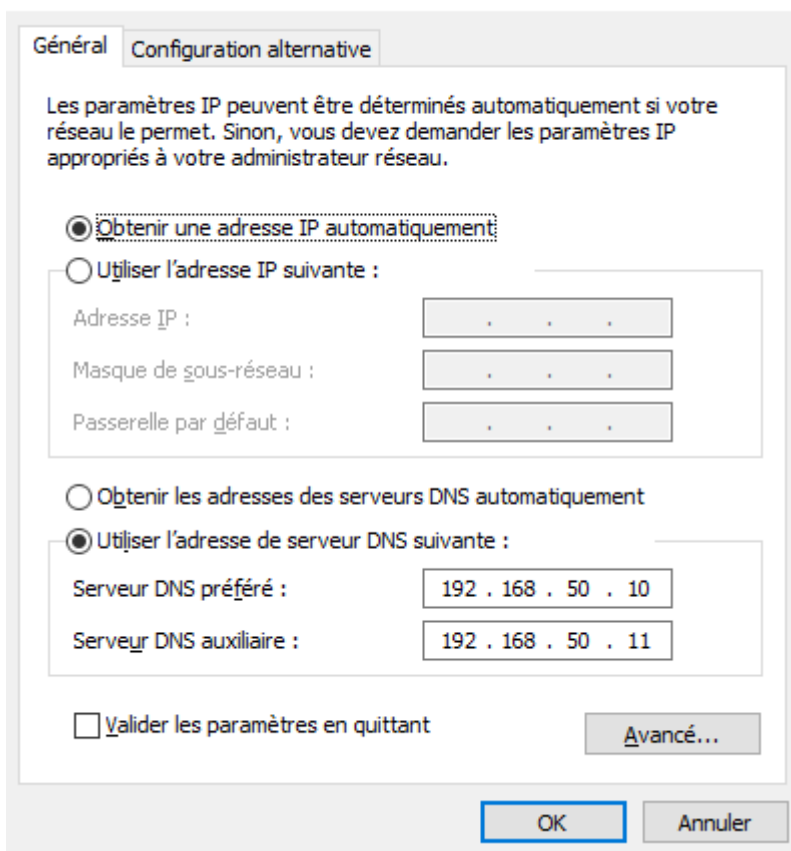
Advanced  **Back** **Finish**

Exactement les mêmes 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 :

Propriétés de : Protocole Internet version 4 (TCP/IPv4)



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

Modification du nom ou du domaine de l'ordinateur ✕

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur :

Nom complet de l'ordinateur :  
veeam.3nz.corp

Autres...

Membre d'un

Domaine :

Groupe de travail :

OK Annuler

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

▼ Datacenter (web-hub)

- ▼ parker
  - 200 (qdevice)
  - 201 (glpi-web)
  - 202 (glpi-db)
  - 104 (WinUse2)
  - 105 (WinSrv2)
  - 107 (veeam)

Summary

- Console
- Hardware
- Cloud-Init
- Options
- Task History

Add Remove

- Hard Disk
- CD/DVD Drive
- Network Device
- EFI Disk
- TPM State
- USB Device

Je sélectionne l'iso et j'ajoute :

Add: CD/DVD Drive ✕

Bus/Device: IDE 1

Use CD/DVD disc image file (iso)

Storage: local

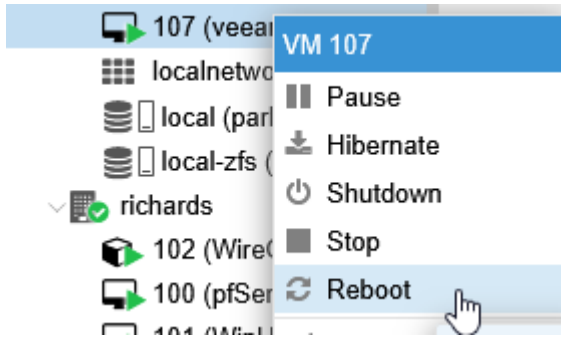
ISO image: VeeamDataPlatform\_v12.:

Use physical CD/DVD Drive

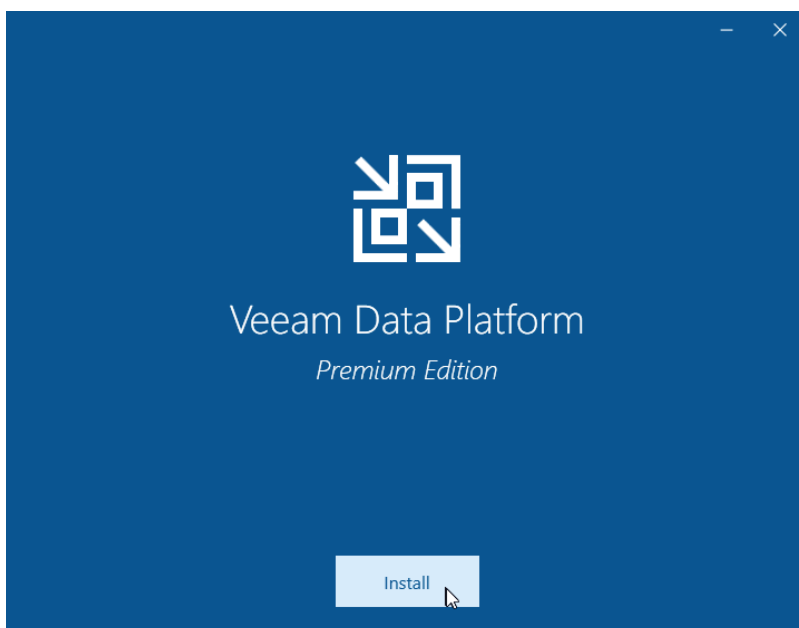
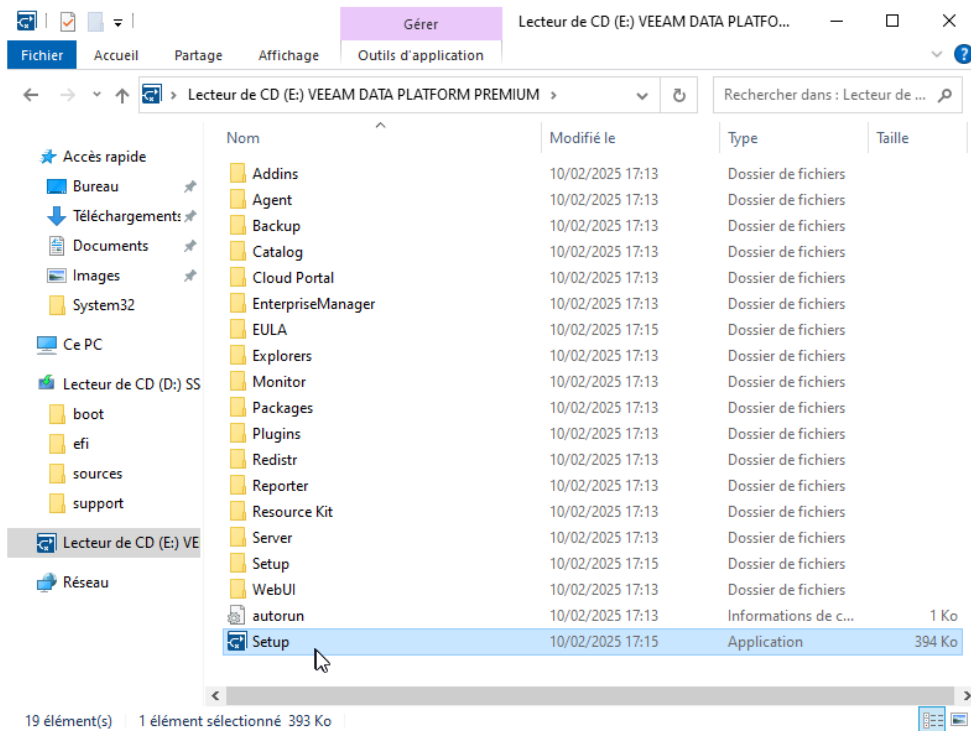
Do not use any media

Add


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

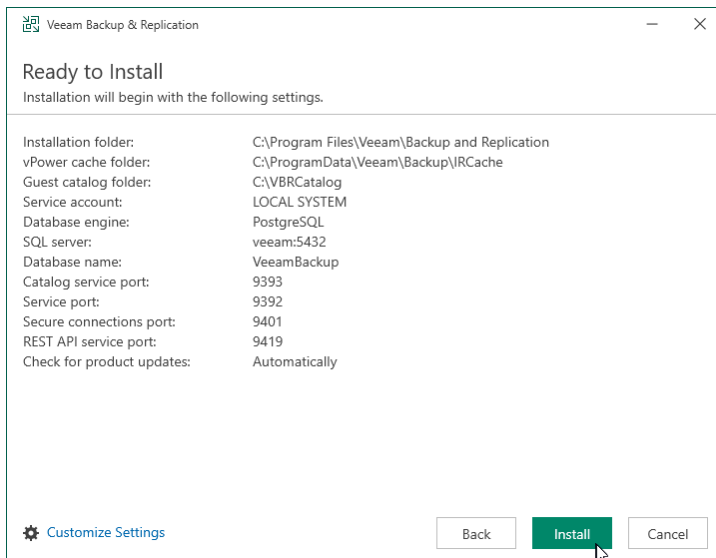
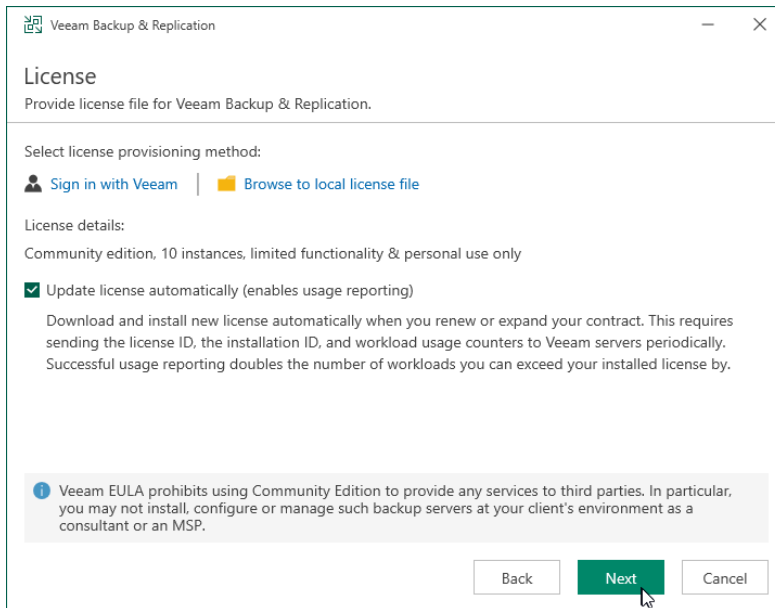
### License Agreement

Read the license agreements and accept them to proceed.

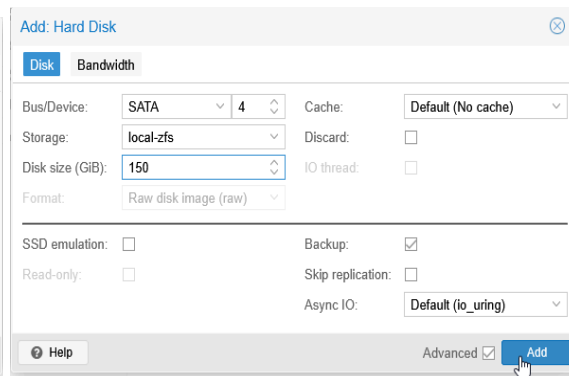
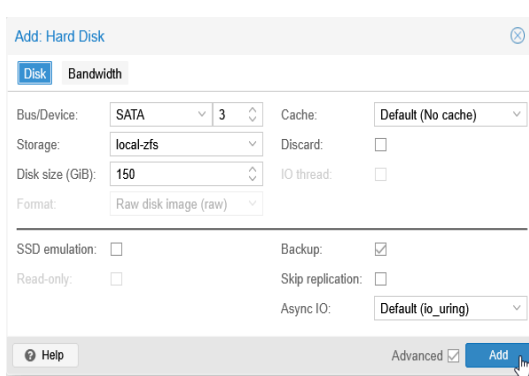
Please view, print or save the documents linked below.

By clicking "I Accept" button, I hereby accept the following:

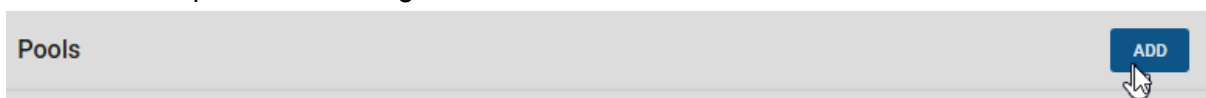
- Agree and consent to the terms of [Veeam License Agreement](#) and [licensing policy](#)
- Agree and consent to each of the license agreements of [3rd party components used](#)
- Agree and consent to each of the license agreements of [required software](#)



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



1 Create or Import pool

Create a pool:

Create new pool ?

Import an existing pool ?

**CANCEL** **CREATE POOL**

### Pool Manager

Name \*  ?  Encryption ?

**RESET LAYOUT** **SUGGEST LAYOUT** ? **ADD VDEV** ▾

Available Disks

<input type="checkbox"/>	Disk	Type	Capacity
No data to display			
0 selected / 0 total			

Filter disks by name  Filter disks by capacity

Data VDevs **REPEAT**

<input checked="" type="checkbox"/>	Disk	Type	Capacity	
<input checked="" type="checkbox"/>	ada4	UNKNOW	150 GiB	>
<input checked="" type="checkbox"/>	ada5	UNKNOW	150 GiB	>
2 selected / 2 total				

Mirror  
Estimated raw capacity: 148 GiB ?

Estimated total raw data capacity: 148 GiB

**CREATE** **CANCEL**

### Warning

The contents of all added disks will be erased.

Confirm **CANCEL** **CREATE POOL**

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

Accounts / Users TrueNAS CORE® © 2025 - iXsystems, Inc.

**Users**  **COLUMNS** ▾ **ADD** ⚙️

Username	UID	Builtin	Full Name	
root	0	yes	root	>

1 - 1 of 1

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

**Identification**

Full Name \*  
Veeam

Username \*  
veeam

Email

Password \*  
.....

Confirm Password \*  
.....

**User ID and Groups**

User ID \*  
1000

New Primary Group

Primary Group

Auxiliary Groups

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

Storage / Pools TrueNAS CORE® © 2025 - iXsystems, Inc.

**Pools** ADD

COMMUN (System Dataset Pool) ONLINE ✔ | 26.13 MiB (0%) Used | 57.73 GiB Free

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
COMMUN	FILESYSTEM	26.13 MiB	57.73 GiB	lz4	8.05	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	
> iocage	FILESYSTEM	9.17 MiB	57.73 GiB	lz4	1.06	false	OFF	

VeeamBackup ONLINE ✔ | 660 KiB (0%) Used | 142.44 GiB Free

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
VeeamBackup	FILESYSTEM	660 KiB	142.44 GiB	lz4	1.00	false	OFF	

**Dataset Actions**

- Add Dataset
- Add Zvol
- Edit Options
- Edit Permissions
- User Quotas
- Group Quotas
- Create Snapshot

**Name and Options**

Name

Comments

Sync **Inherit (standard)**

Compression level **Inherit (lz4)**

Enable Atime **Inherit (off)**

---

**Encryption Options**

Inherit (non-encrypted)

---

**Other Options**

ZFS Deduplication **Inherit (off)**

Case Sensitivity **Sensitive**

Share Type **Generic**

**SUBMIT** **CANCEL** **ADVANCED OPTIONS**

Maintenant je vais mettre le droit full control de notre utilisateur sur notre pool :

Storage > Pools > Veeam Backup > Plus d'options

Storage / Pools TrueNAS CORE® © 2025 - iXsystems, Inc

**Pools** **ADD**

**COMMUN** (System Dataset Pool) ONLINE ✔ | 26.13 MiB (0%) Used | 57.73 GiB Free ⚙️ ^

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
▼ COMMUN	FILESYSTEM	26.13 MiB	57.73 GiB	lz4	8.05	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	
> iocage	FILESYSTEM	9.17 MiB	57.73 GiB	lz4	1.06	false	OFF	

---

**VeeamBackup** ONLINE ✔ | 660 KiB (0%) Used | 142.44 GiB Free ⚙️ ^

Name	Type	Used	Available	Compression	Compression Ratio	Readonly	Dedup	Comments
▼ VeeamBackup	FILESYSTEM	660 KiB	142.44 GiB	lz4	1.00	false	OFF	
saves	FILESYSTEM	96 KiB	142.44 GiB	Inherits (lz4)	1.00	false	OFF	

Dataset Actions

Add Dataset

Add Zvol

Edit Options

**Edit Permissions**

User Quotas

Group Quotas

Delete Dataset

Create Snapshot

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

**Dataset Path**  
Path  
/mnt/VeeamBackup/saves

**Owner**  
User  
veeam  
 Apply User  
Group  
wheel  
 Apply Group

**Access**  
Access Mode  
Read Write Execute  
User     
Group     
Other

**Advanced**  
 Apply Permissions Recursively  
 Traverse

**SAVE** **CANCEL** **USE ACL MANAGER**

**Create an ACL**

Select a preset ACL  
 Create a custom ACL

**CONTINUE**

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

**File Information**  
Path  
/mnt/VeeamBackup/saves  
User  
veeam  
 Apply User  
Group  
wheel  
 Apply Group

**Access Control List**  
Who \*  
User  
User \*  
veeam  
ACL Type \*  
Allow  
Permissions Type \*  
Basic  
Permissions \*  
Full Control  
Flags Type \*  
Basic  
Flags \*  
Inherit

**SELECT AN ACL PRESET** **ADD ACL ITEM** **DELETE**

**Advanced**  
 Apply permissions recursively  
 Apply permissions to child datasets

**SAVE** **CANCEL** **STRIP ACLS**

## Création du partage : Sharing > SMB

Samba

Filter Samba

COLUMNS ADD

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

1 - 4 of 4

- Edit
- Edit Share ACL
- Edit Filesystem ACL
- Delete

Basic

Path +  
/mnt/VeeamBackup/saves

/mnt  
COMMUN  
VeeamBackup  
saves ACL

Name  
saves

Purpose  
Default share parameters Description

Enabled

SAVE CANCEL ADVANCED OPTIONS

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

Veeam Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

localhost 9392

VEEAM\Administrateur

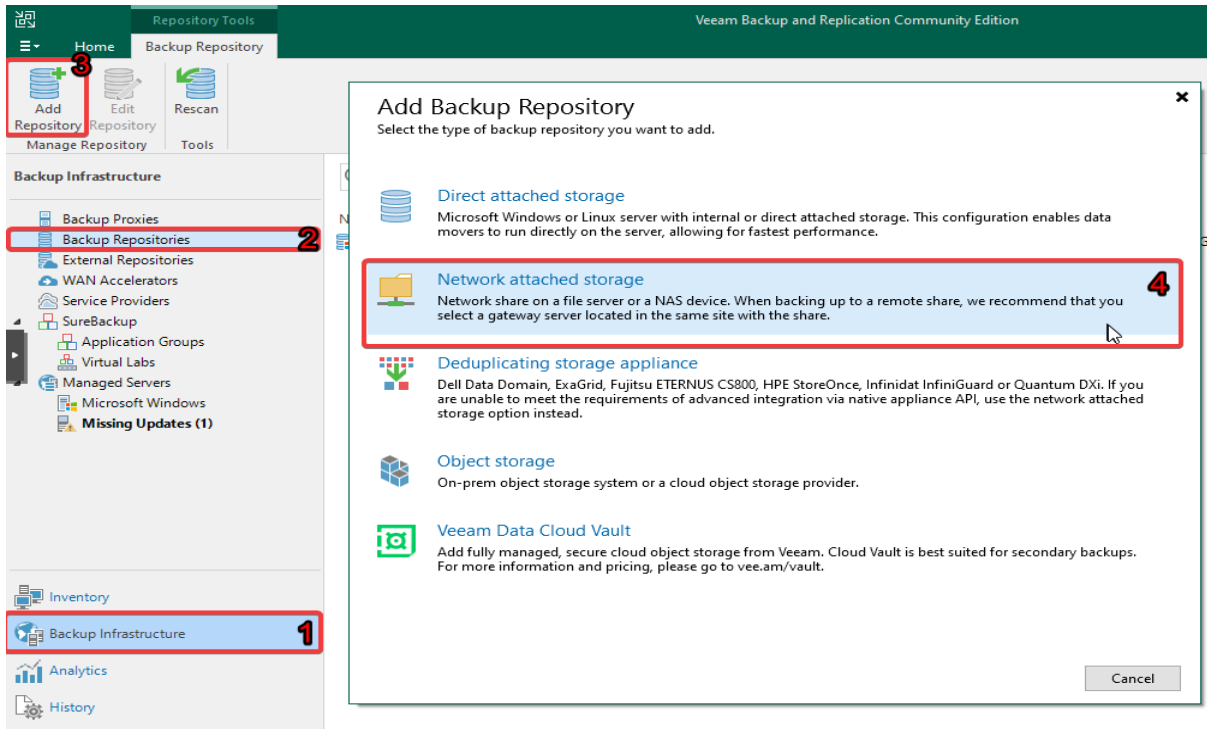
Password

Use Windows session authentication

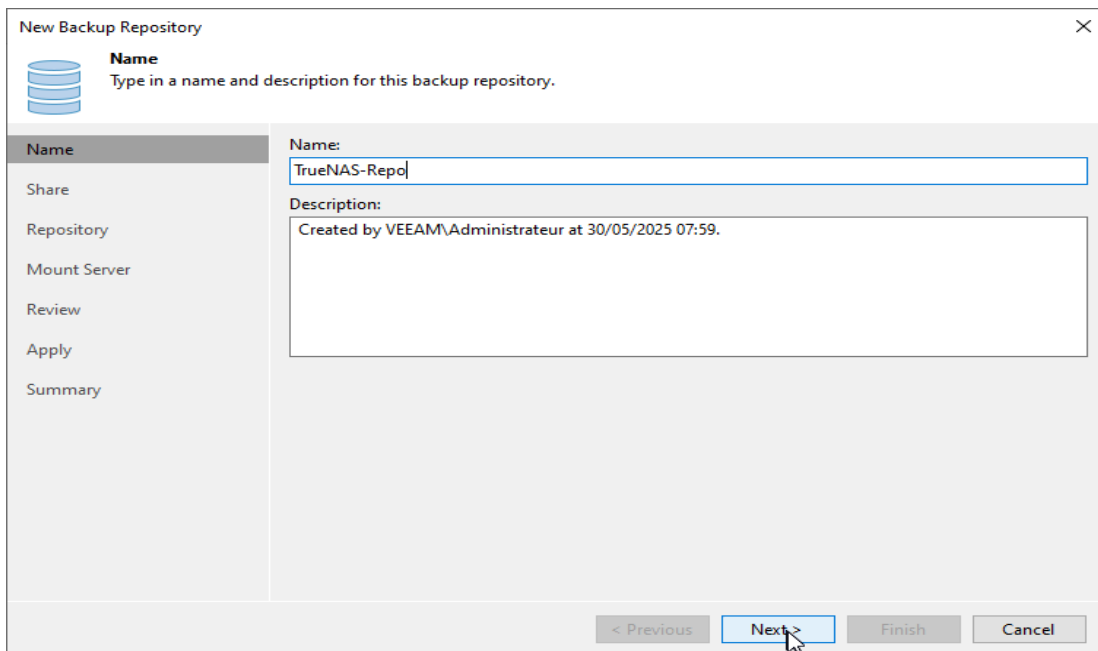
Save shortcut Connect Close

- 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** Shared folder:  
 [Browse...](#)

**Share** Use \\server\folder format

**Repository**  This share requires access credentials:

**Mount Server**  [Add...](#)  
[Manage accounts](#)

**Review** **Gateway server:**  
 [Choose...](#)

**Apply**

**Summary**

< 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:**  [Populate](#)

**Capacity:** 142,4 GB  
**Free space:** 142,4 GB

**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:

Limit read and write data rate to:  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:

**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	Mount server: veeam.3nz.corp (Backup server) <span style="float: right;">Add New...</span>
Share	
Repository	Instant recovery write cache folder: C:\ProgramData\Veeam\Backup\IRCache\ <span style="float: right;">Browse...</span>
<b>Mount Server</b>	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.
Review	<input checked="" type="checkbox"/> Enable vPower NFS service on the mount server (recommended) <span style="float: right;">Ports...</span>
Apply	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.
Summary	

< Previous Next > Finish Cancel

New Backup Repository ✕


 **Review**  
Please review the settings, and click Apply to continue.

Name	The following components will be processed on server veeam.3nz.corp:	
Share	Component name	Status
Repository	vPower NFS	already exists
Mount Server	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	Message	Duration
Share	✔ Starting infrastructure item update process	0:00:06
Repository	✔ Discovering installed packages	
Mount Server	✔ Registering client veeam for package vPower NFS	
Review	✔ Registering client veeam for package Mount Server	
<b>Apply</b>	✔ Registering client veeam for package VMware VDDK	
Summary	✔ 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	

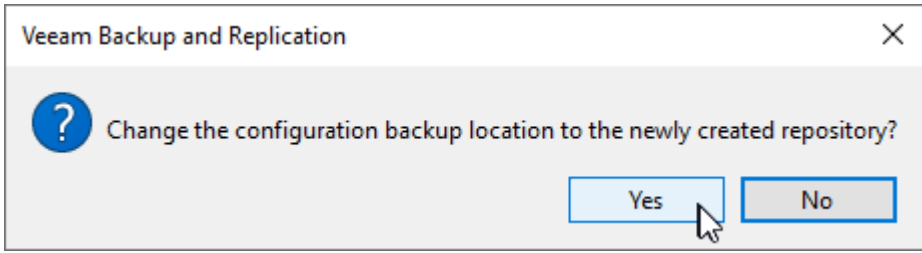
< Previous
Next >
Finish
Cancel

New Backup Repository ✕

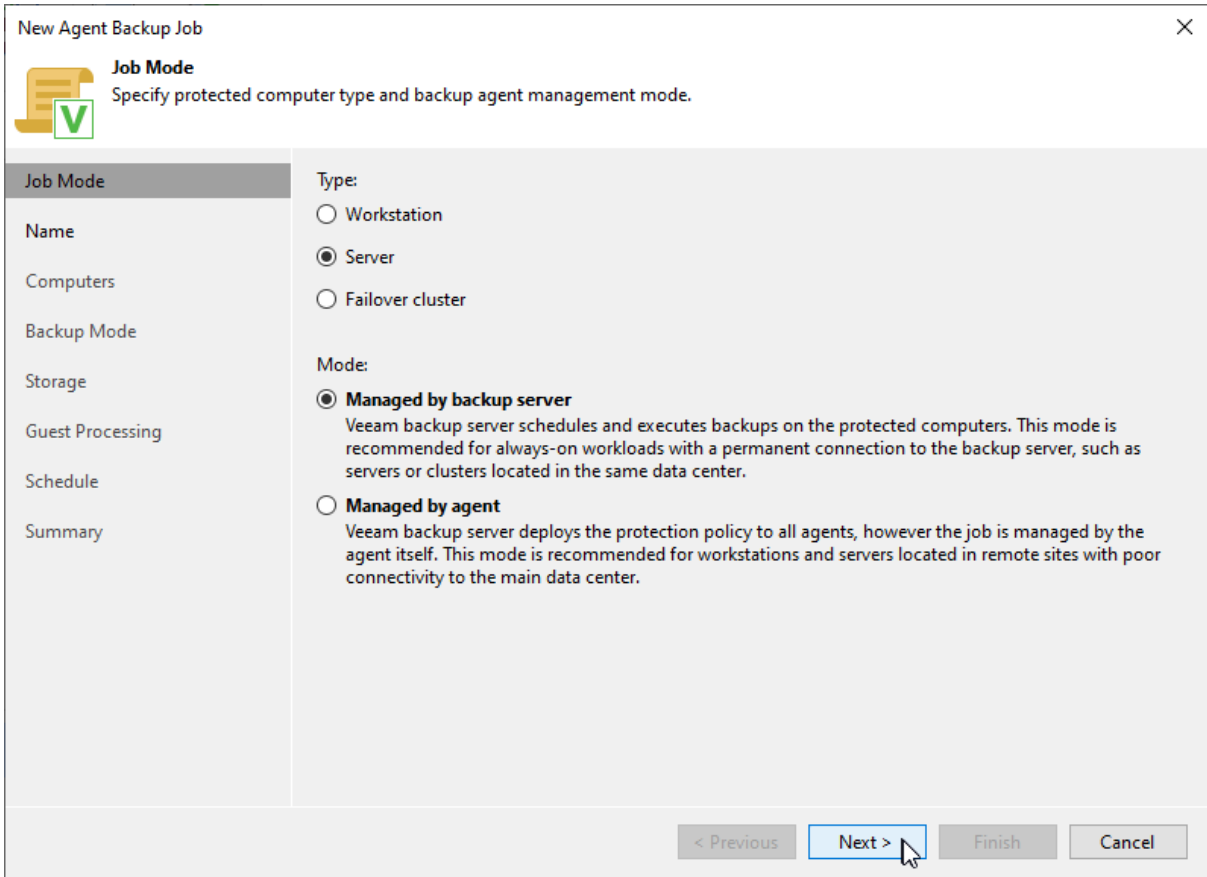
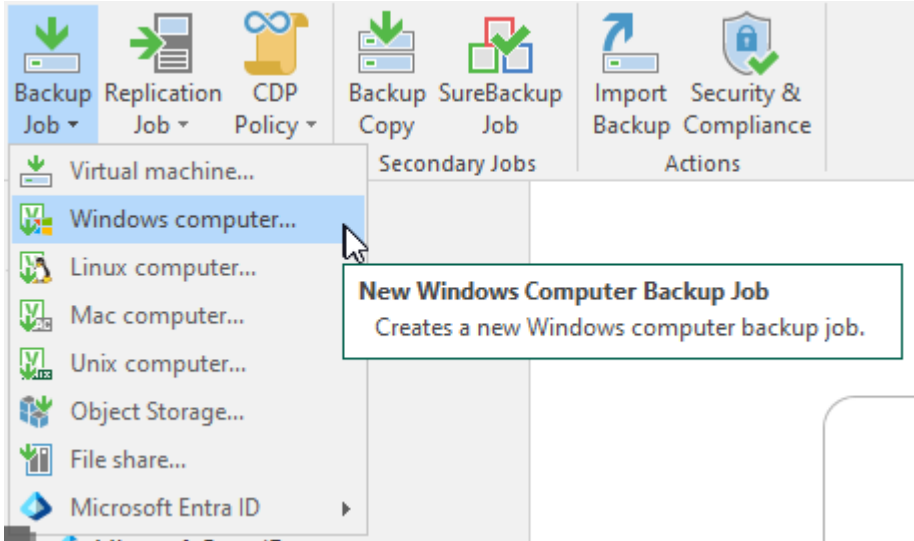
 **Summary**  
You can copy the configuration information below for future reference.

Name	Summary:
Share	SMB backup repository 'TrueNAS-Repo' was successfully saved.
Repository	Mount host: veeam.3nz.corp
Mount Server	Account: nas\veeam
Review	Backup folder: \\nas\saves
<b>Apply</b>	Write throughput: unlimited
Summary	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**

**Description:**

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.

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**

**Protected computers:**

Name	Type


**Add Computer** ✕

Host name or IP address:

Credentials:

[Manage accounts](#)


New Agent Backup Job ✕

 **Backup Mode**  
Choose what data you want to back up from selected computers.

Job Mode	<input checked="" type="radio"/> <b>Entire computer</b> 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. <input type="checkbox"/> Include external USB drives
Name	
Computers	
<b>Backup Mode</b>	<input type="radio"/> <b>Volume level backup</b> 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.
Storage	
Guest Processing	
Schedule	
Summary	<input type="radio"/> <b>File level backup (slower)</b> 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	Backup repository: TrueNAS-Repo (Created by VEEAM\Administrateur at 30/05/2025 11:14.) 142,4 GB free of 142,4 GB <a href="#">Map backup</a>
Name	
Computers	
Backup Mode	Retention policy: 7 days
<b>Storage</b>	<input type="checkbox"/> Keep certain full backups longer for archival purposes <a href="#">Configure...</a> GFS retention policy is not configured
Guest Processing	<input type="checkbox"/> 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.
Schedule	
Summary	Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings. <a href="#">Advanced...</a>

< Previous   **Next >**   Finish   Cancel


New Agent Backup Job ✕

 **Guest Processing**  
Choose application processing options.

Job Mode	<input checked="" type="checkbox"/> <b>Enable application-aware processing</b> 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 <span style="float: right;">Applications...</span>
Name	
Computers	
Backup Mode	<input type="checkbox"/> <b>Enable guest file system indexing and malware detection</b> 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 <span style="float: right;">Indexing...</span>
Storage	
<b>Guest Processing</b>	
Schedule	
Summary	

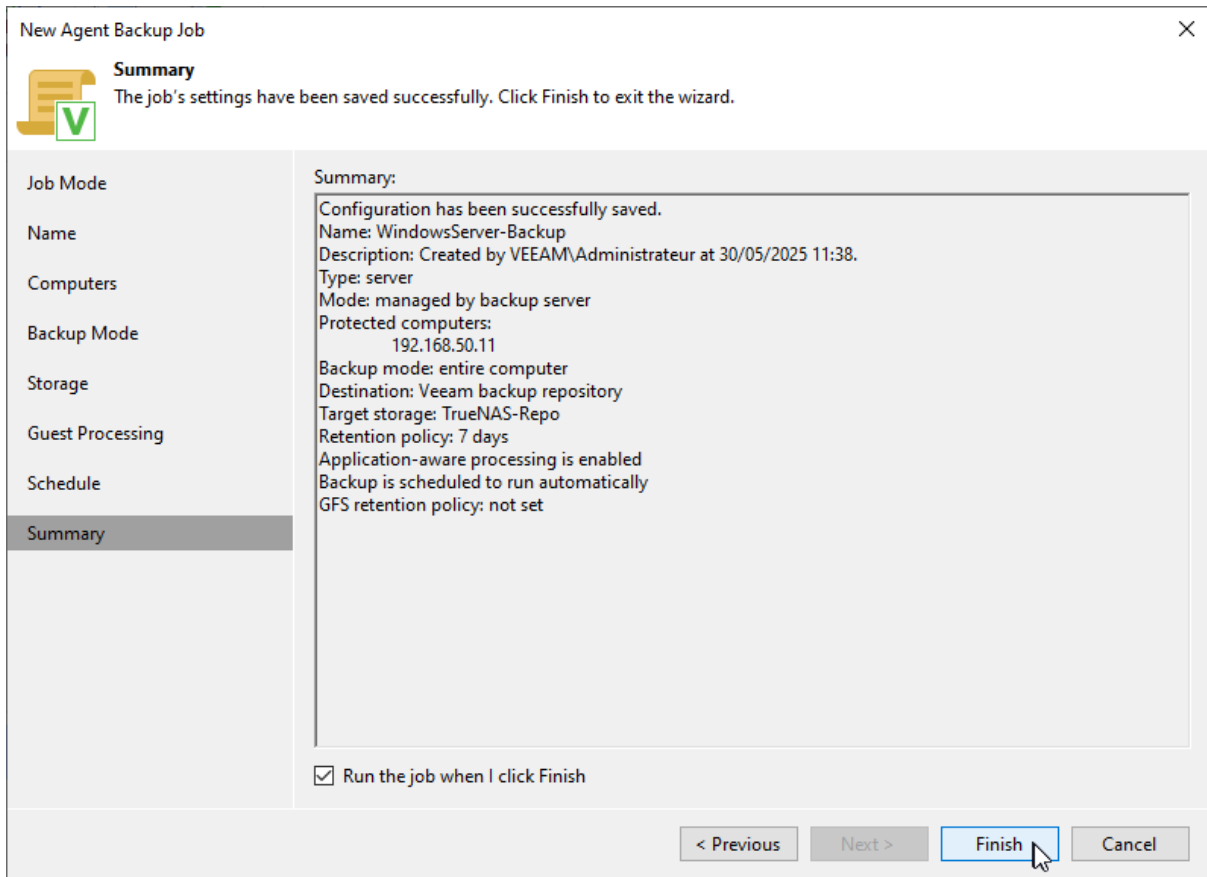
< Previous Next > Finish Cancel

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	<input checked="" type="checkbox"/> <b>Run the job automatically</b>
Name	<input checked="" type="radio"/> <b>Daily at this time:</b> <input type="text" value="22:00"/> <input type="text" value="Everyday"/> <span style="float: right;">Days...</span>
Computers	<input type="radio"/> <b>Monthly at this time:</b> <input type="text" value="22:00"/> <input type="text" value="Fourth"/> <input type="text" value="samedi"/> <span style="float: right;">Months...</span>
Backup Mode	<input type="radio"/> <b>Periodically every:</b> <input type="text" value="1"/> <input type="text" value="Hours"/> <span style="float: right;">Schedule...</span>
Storage	<input type="radio"/> <b>After this job:</b> <input type="text"/>
Guest Processing	<b>Automatic retry</b>
<b>Schedule</b>	<input checked="" type="checkbox"/> <b>Retry failed items processing:</b> <input type="text" value="3"/> times Wait before each retry attempt for: <input type="text" value="10"/> minutes
Summary	<b>Backup window</b>
	<input type="checkbox"/> <b>Terminate job outside of the backup window</b> <span style="float: right;">Window...</span> 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 :

Job Name	Session Type	Status	Start Time ↓	End Time
Rescan of WindowsServer-Backup	Rescan	Success	30/05/2025 11:46	30/05/2025 11:49

La backup a bien été créé :

← → ↕ ↑ 📁 > Réseau > nas > saves > WindowsServer-Backup > 192.168.50.11

Nom	Modifié le	Type	Taille
WindowsServer-Backup - 192.168.50.11	30/05/2025 11:56	Veeam backup ch...	32 Ko
WindowsServer-Backup - 192.168.50.11D...	30/05/2025 11:55	Veeam full backup...	5 379 880 Ko

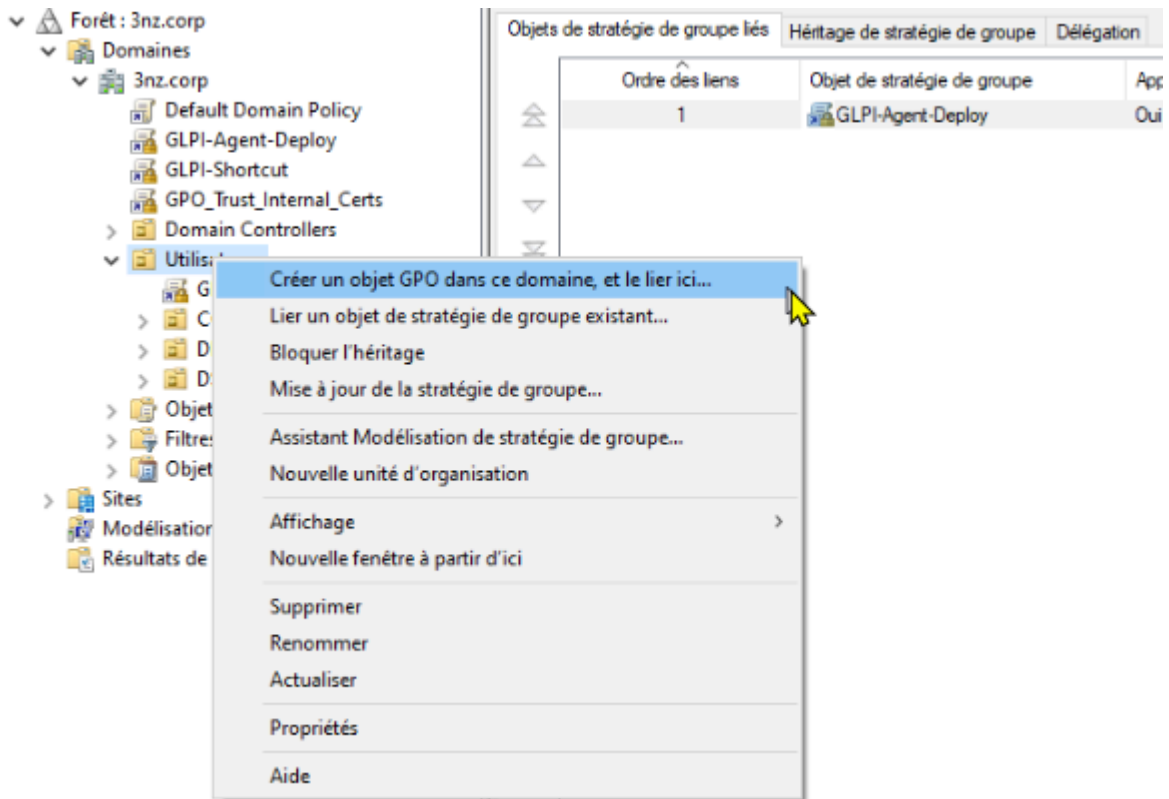
### III. Durcissement de la Sécurité

Plan de mes GPO :

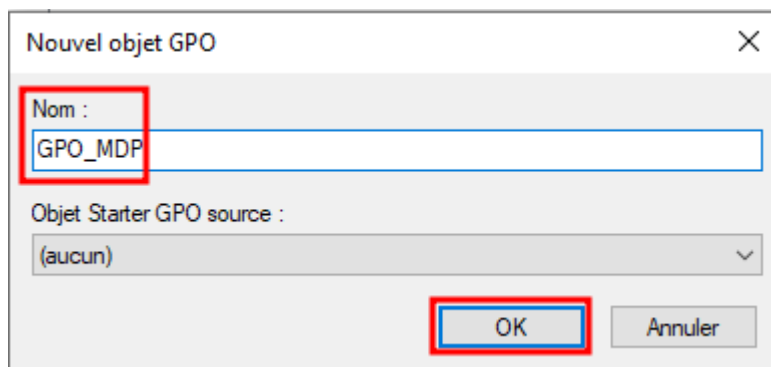
Domaine	Paramètre (Chemin GPO)	Réglage Préconisé	Justification Professionnelle (BTS)
Mots de passe	Longueur minimale du mot de passe	<b>12 caractères</b>	Protection contre le <i>Brute Force</i> . Augmente la complexité entropique nécessaire au décryptage.
Mots de passe	Durée de vie maximale du mdp	<b>365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

- Politique de mots de passe

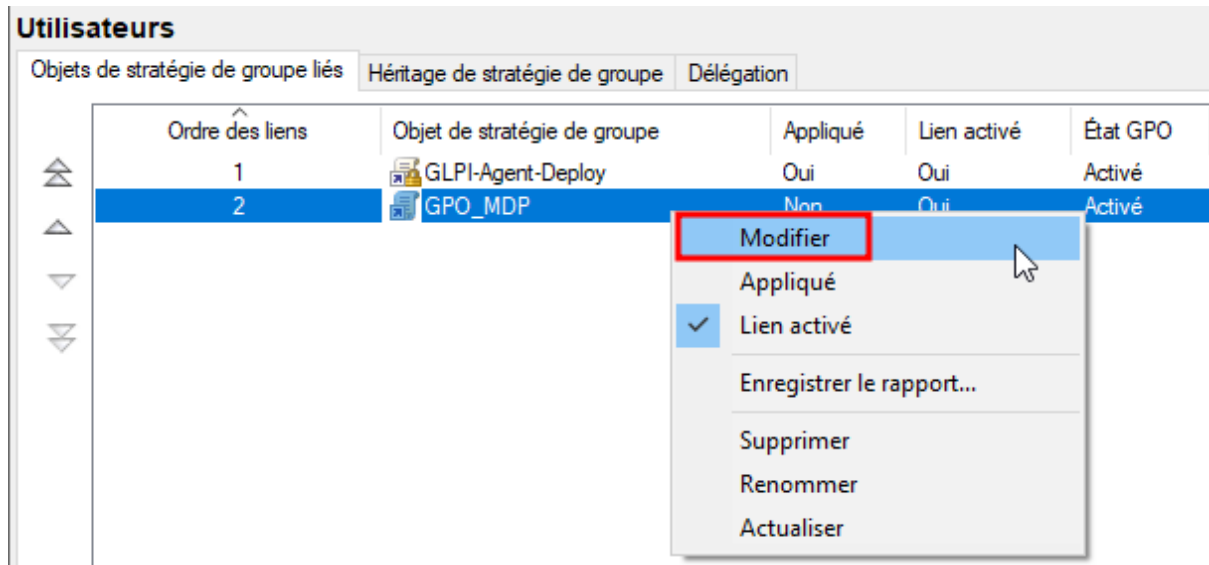
Création de la GPO pour la politique des mots de passe :



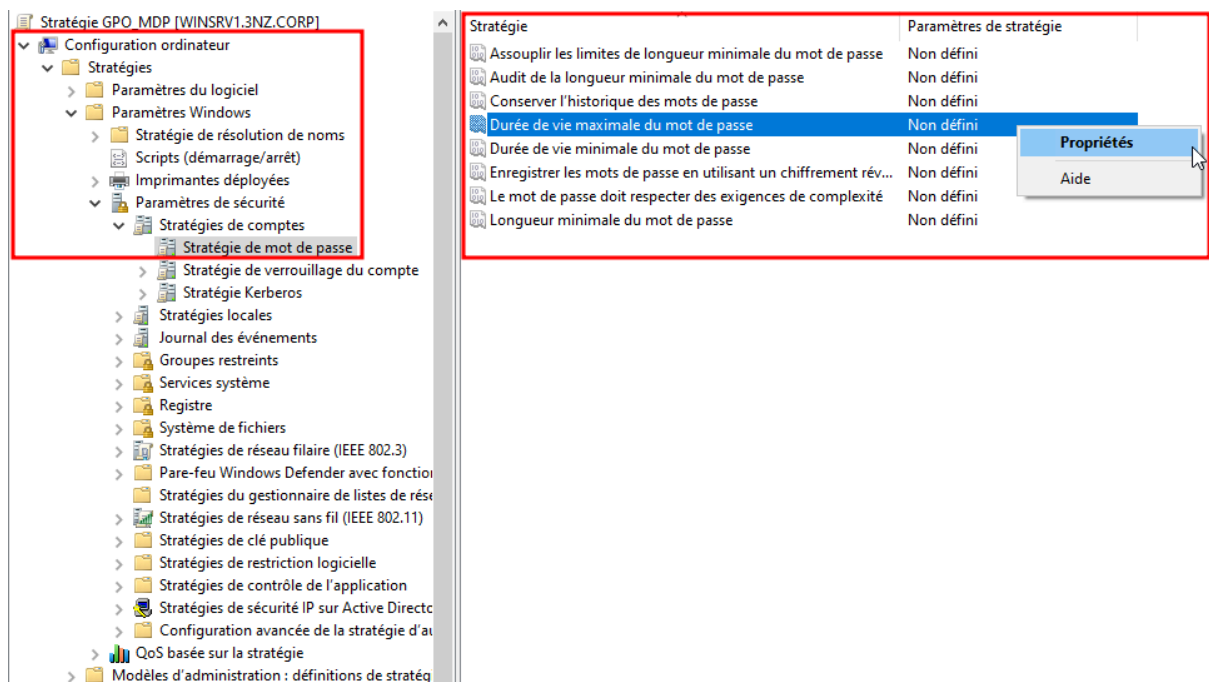
Je la nomme :



Une fois créée, clic droit, modifier :



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



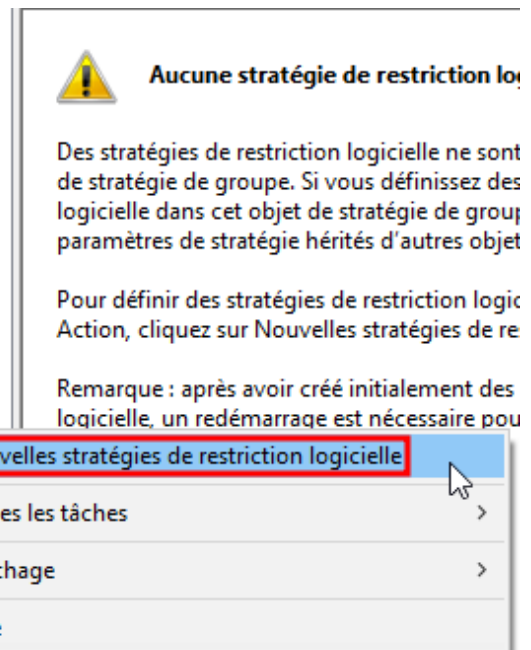
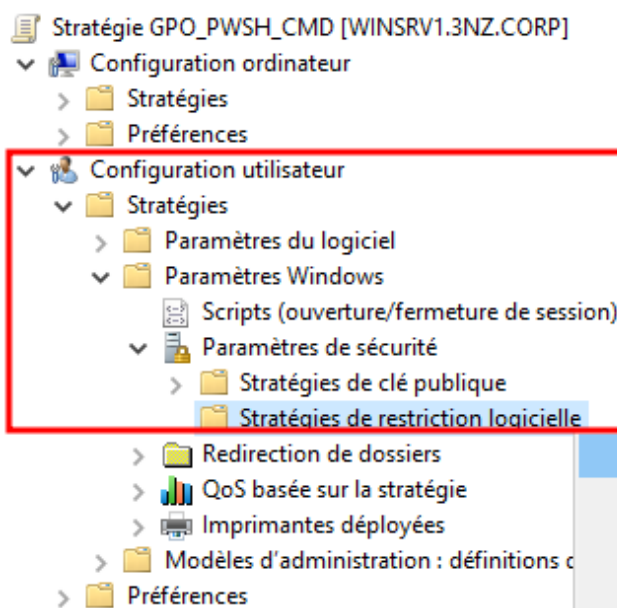
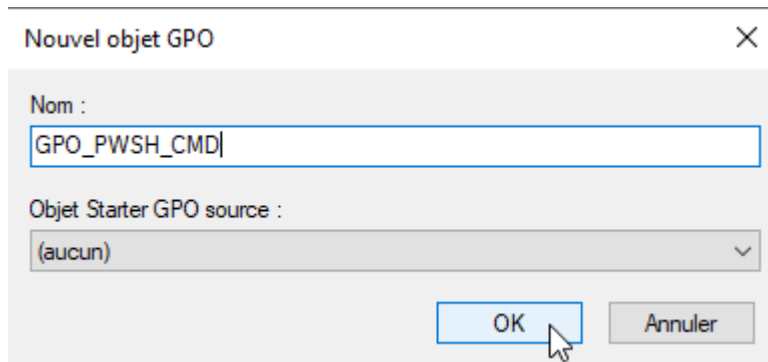
Voici donc, ma stratégie pour les mots de passe :

Stratégie	Paramètres de stratégie
Assouplir les limites de longueur minimale du mot de passe	Non défini
Audit de la longueur minimale du mot de passe	Non défini
Conserver l'historique des mots de passe	10 mots de passe mémorisés
Durée de vie maximale du mot de passe	365 jours
Durée de vie minimale du mot de passe	30 jours
Enregistrer les mots de passe en utilisant un chiffrement rév...	Non défini
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	12 caractère(s)

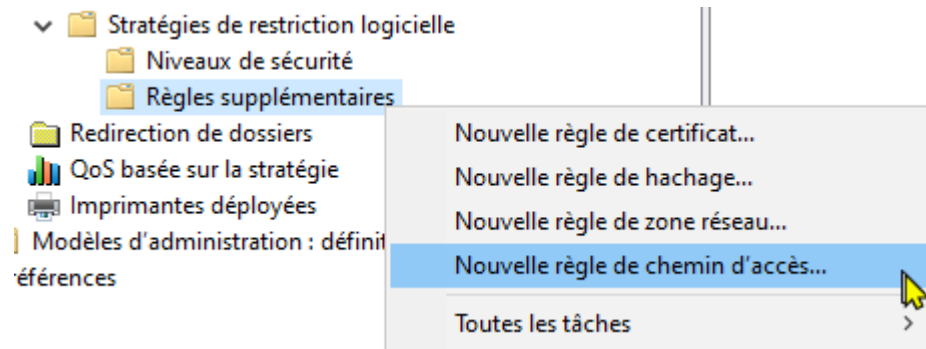
- Restriction des outils d'administration

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

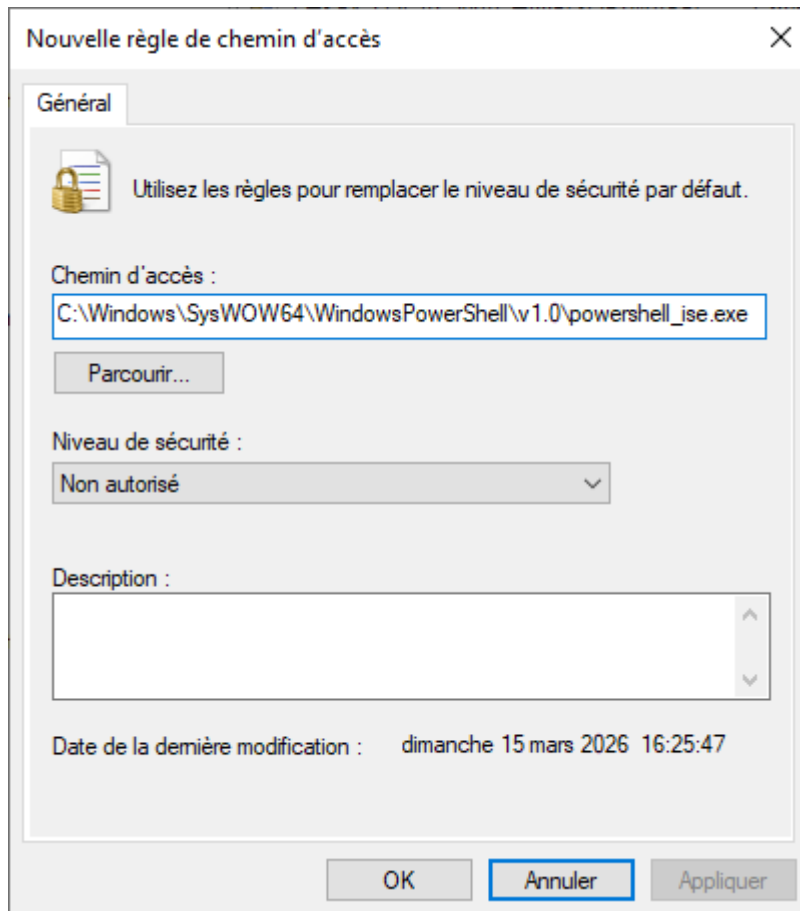
Création d'un GPO nommé GPO\_PWSH\_CMD puis modifier :







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



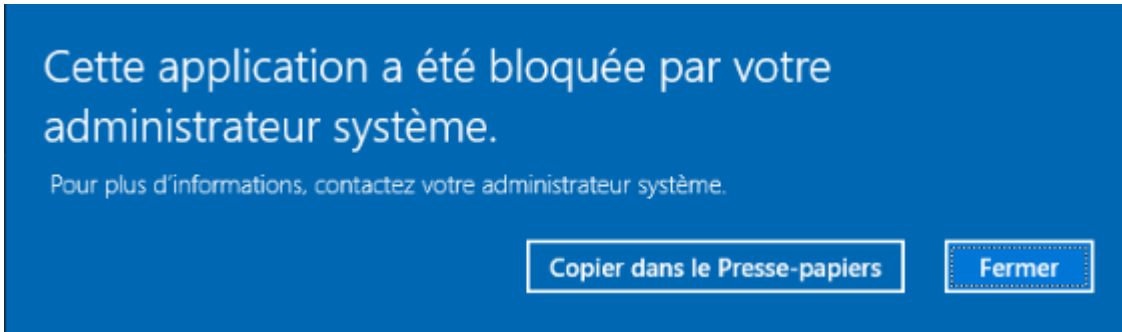
Parcourir jusqu'au chemin où se trouve les .exe de powershell :



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 :

Éditeur de gestion des stratégies de groupe

Stratégie GPO\_PWSH\_CMD [WINSRV1.3NZ.CORP]

- Configuration ordinateur
  - Stratégies
  - Préférences
  - Configuration utilisateur
    - Stratégies
      - Paramètres du logiciel
      - Paramètres Windows
      - Modèles d'administration : définitions de stratégies
        - Bureau
        - Composants Windows
        - Dossiers partagés
        - Menu Démarrer et barre des tâches
        - Panneau de configuration
        - Réseau
        - Système**
          - Accès au stockage amovible
          - Affichage
          - Gestion de l'alimentation
          - Gestion de la communication Internet
          - Installation de pilotes
          - Options Ctrl+Alt+Suppr
          - Options d'atténuation
          - Ouverture de session
          - Profils utilisateur
          - Redirection de dossiers
          - Scripts
          - Services Paramètres régionaux
          - Stratégie de groupe
          - Tous les paramètres
        - Préférences

**Système**

**Désactiver l'accès à l'invite de commandes**

Modifier le paramètre de stratégie

Configuration requise :  
Au minimum Windows 2000

Description :  
Ce paramètre de stratégie empêche les utilisateurs d'exécuter l'invite de commandes interactive, Cmd.exe. Ce paramètre de stratégie indique également s'il est permis d'exécuter ou non les fichiers de commandes (.cmd et .bat) sur l'ordinateur.

Si vous activez ce paramètre de stratégie et que l'utilisateur essaie d'ouvrir une fenêtre de commande, le système affiche un message signalant qu'un paramètre bloque l'action.

Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter normalement Cmd.exe et des fichiers de commandes.

Remarque : n'empêche pas l'exécution des fichiers de commandes sur l'ordinateur si celui-ci utilise des scripts de fichiers de commandes pour la connexion, la déconnexion, le démarrage ou l'arrêt, ou pour les utilisateurs ayant recours aux services Bureau à distance.

Paramètre	État
Accès au stockage amovible	
Affichage	
Gestion de l'alimentation	
Gestion de la communication Internet	
Installation de pilotes	
Options Ctrl+Alt+Suppr	
Options d'atténuation	
Ouverture de session	
Profils utilisateur	
Redirection de dossiers	
Scripts	
Services Paramètres régionaux	
Stratégie de groupe	
Télécharger les composants manquants	Non configuré
Interprétation du siècle pour l'an 2000	Non configuré
Restreindre l'exécution de ces programmes à partir de l'aide	Non configuré
Ne pas afficher l'écran de démarrage Mise en route à l'ouver...	Non configuré
Interface utilisateur personnalisée	Non configuré
<b>Désactiver l'accès à l'invite de commandes</b>	<b>Non configuré</b>
Empêche l'accès aux outils de modifications du Registre	Non configuré
Ne pas exécuter les applications Windows spécifiées	Non configuré
Exécuter uniquement les applications Windows spécifiées	Non configuré
Mises à jour automatiques Windows	Non configuré

Étendu / Standard

10 paramètre(s)

Double-cliquez puis configurez :

Désactiver l'accès à l'invite de commandes

Paramètre précédent Paramètre suivant

Non configuré    Commentaire :

**Activé**

Désactivé    Pris en charge sur :

Options :    Aide :

Désactiver également le traitement des scripts d'invite de commande ?

Ce paramètre de stratégie empêche les utilisateurs d'exécuter l'invite de commandes interactive, Cmd.exe. Ce paramètre de stratégie indique également s'il est permis d'exécuter ou non les fichiers de commandes (.cmd et .bat) sur l'ordinateur.

Si vous activez ce paramètre de stratégie et que l'utilisateur essaie d'ouvrir une fenêtre de commande, le système affiche un message signalant qu'un paramètre bloque l'action.

Si vous désactivez ou ne configurez pas ce paramètre de stratégie, les utilisateurs peuvent exécuter normalement Cmd.exe et des fichiers de commandes.

Remarque : n'empêchez pas l'exécution des fichiers de commandes sur l'ordinateur si celui-ci utilise des scripts de fichiers de commandes pour la connexion, la déconnexion, le démarrage ou l'arrêt, ou pour les utilisateurs ayant recours aux services Bureau à distance.

   Annuler    Appliquer

## ● 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 :

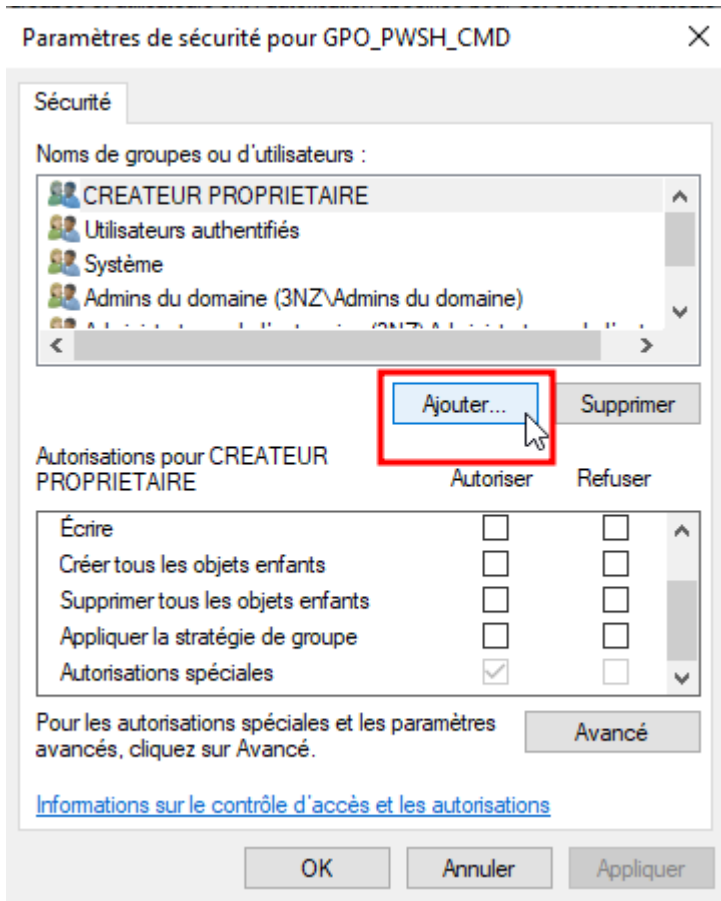
The screenshot shows the Group Policy Management console for the domain '3nz.corp'. The left pane shows the tree structure with 'GPO\_PWSH\_CMD' selected under 'Utilisateurs'. The right pane shows the 'Délégation' tab for this GPO, listing groups and users with their permissions.

**1** points to the selected GPO in the left pane.

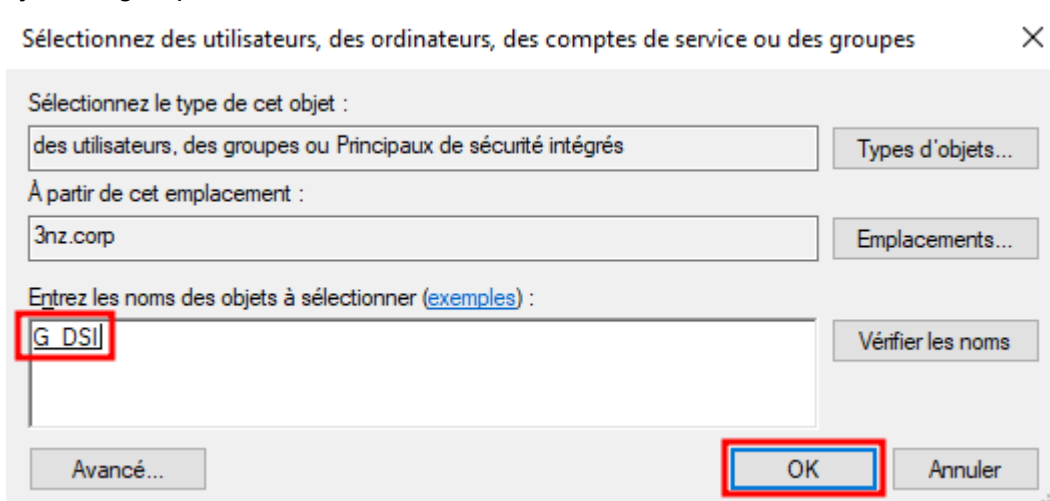
**2** points to the 'Délégation' tab in the right pane.

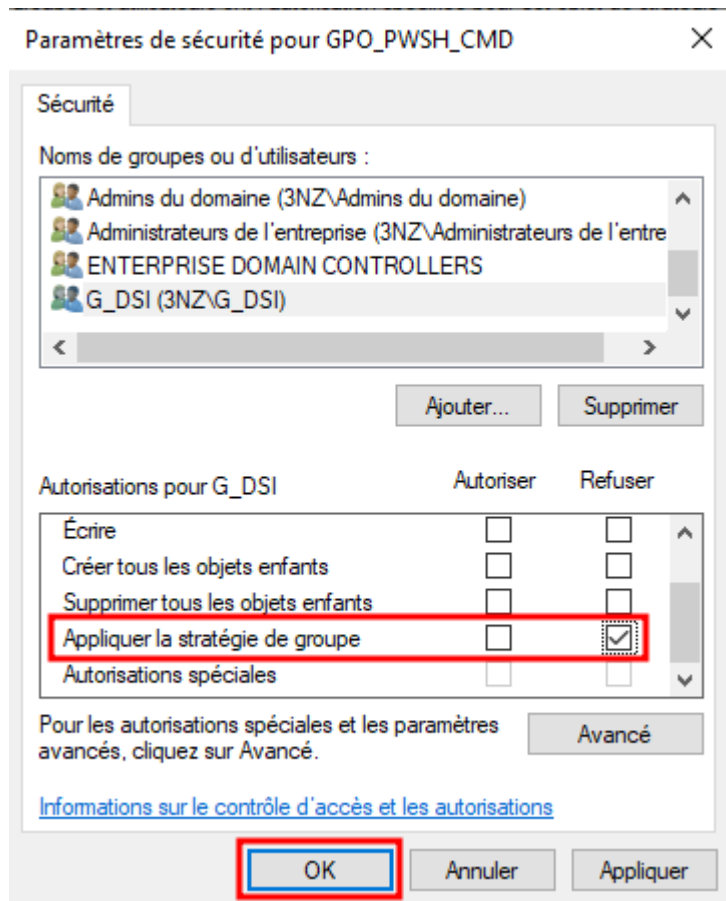
**3** points to the 'Avancé...' button at the bottom right of the right pane.

Nom	Autorisations acceptées	Hérité
Administrateurs de l'entreprise (3NZ\Administrateurs de l'entreprise)	Modifier les paramètres, supprimer, modifier...	Non
Admins du domaine (3NZ\Admins du domaine)	Modifier les paramètres, supprimer, modifier...	Non
ENTERPRISE DOMAIN CONTROLLERS	Lecture	Non
Système	Modifier les paramètres, supprimer, modifier...	Non
Utilisateurs authentifiés	Lecture (à partir du filtrage de sécurité)	Non



Ajout du groupe dsi :

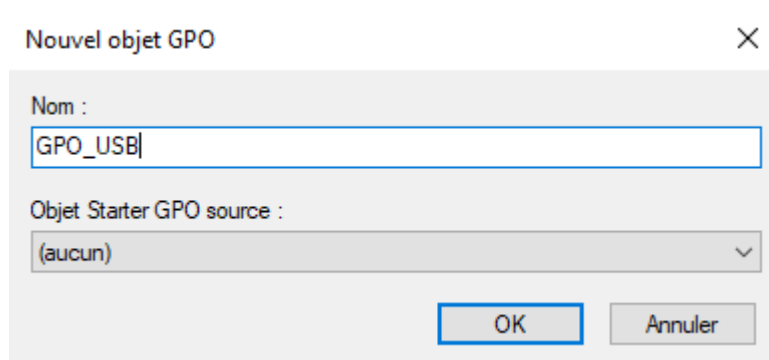




Voilà, maintenant tous les utilisateurs authentifiés sur le réseau sauf la DSI n'ont pas accès à PowerShell ni à l'invite de commande.

## ● Sécurité Physique

Création d'une GPO nommée GPO\_USB :



ensuite, on la modifie :

Stratégie GPO\_USB [WINSRV1.3NZ.CORP]

- Configuration ordinateur
  - Stratégies
    - Paramètres du logiciel
    - Paramètres Windows
    - Modèles d'administration : définitions de str
      - Composants Windows
      - Imprimantes
      - Menu Démarrer et barre des tâches
      - Panneau de configuration
      - Réseau
      - Serveur
      - Système
        - Accès au stockage amovible**
        - Accès au stockage étendu
        - Affichage
        - App-V
        - Appel de procédure distante
        - Assistance à distance
        - Assistance en cas d'accès refusé
        - Assistant de stockage
        - Audit de création de processus
        - Cache NV de disque
        - Complexité du code confidentiel
        - DCOM
        - Délégation d'informations d'identific
        - Dépannage et diagnostics
        - Device Guard
        - Fermeture
        - Fournisseur de clichés instantanés du
        - Gestion de l'alimentation
        - Gestion de la communication Internet
        - Gestionnaire de serveur

Accès au stockage amovible

Sélectionnez un élément pour obtenir une description.

Paramètre	État
Définir le délai (en secondes) avant de forcer le redémarrage	Non configuré
CD et DVD : refuser l'accès en exécution	Non configuré
CD et DVD : refuser l'accès en lecture	Non configuré
CD et DVD : refuser l'accès en écriture	Non configuré
Classes personnalisées : refuser l'accès en lecture	Non configuré
Classes personnalisées : refuser l'accès en écriture	Non configuré
Lecteurs de disquettes : refuser l'accès en exécution	Non configuré
Lecteurs de disquettes : refuser l'accès en lecture	Non configuré
Lecteurs de disquettes : refuser l'accès en écriture	Non configuré
Disques amovibles : refuser l'accès en exécution	Non configuré
Disques amovibles : refuser l'accès en lecture	Non configuré
Disques amovibles : refuser l'accès en écriture	Non configuré
Toutes les classes de stockage amovible : refuser tous les acc...	Non configuré
Tout stockage amovible : permet l'accès direct pendant des ...	Non configuré
Lecteurs de bandes : refuser l'accès en exécution	Non configuré
Lecteurs de bandes : refuser l'accès en lecture	Non configuré
Lecteurs de bandes : refuser l'accès en écriture	Non configuré
Périphériques WPD : refuser l'accès en lecture	Non configuré
Périphériques WPD : refuser l'accès en écriture	Non configuré

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.

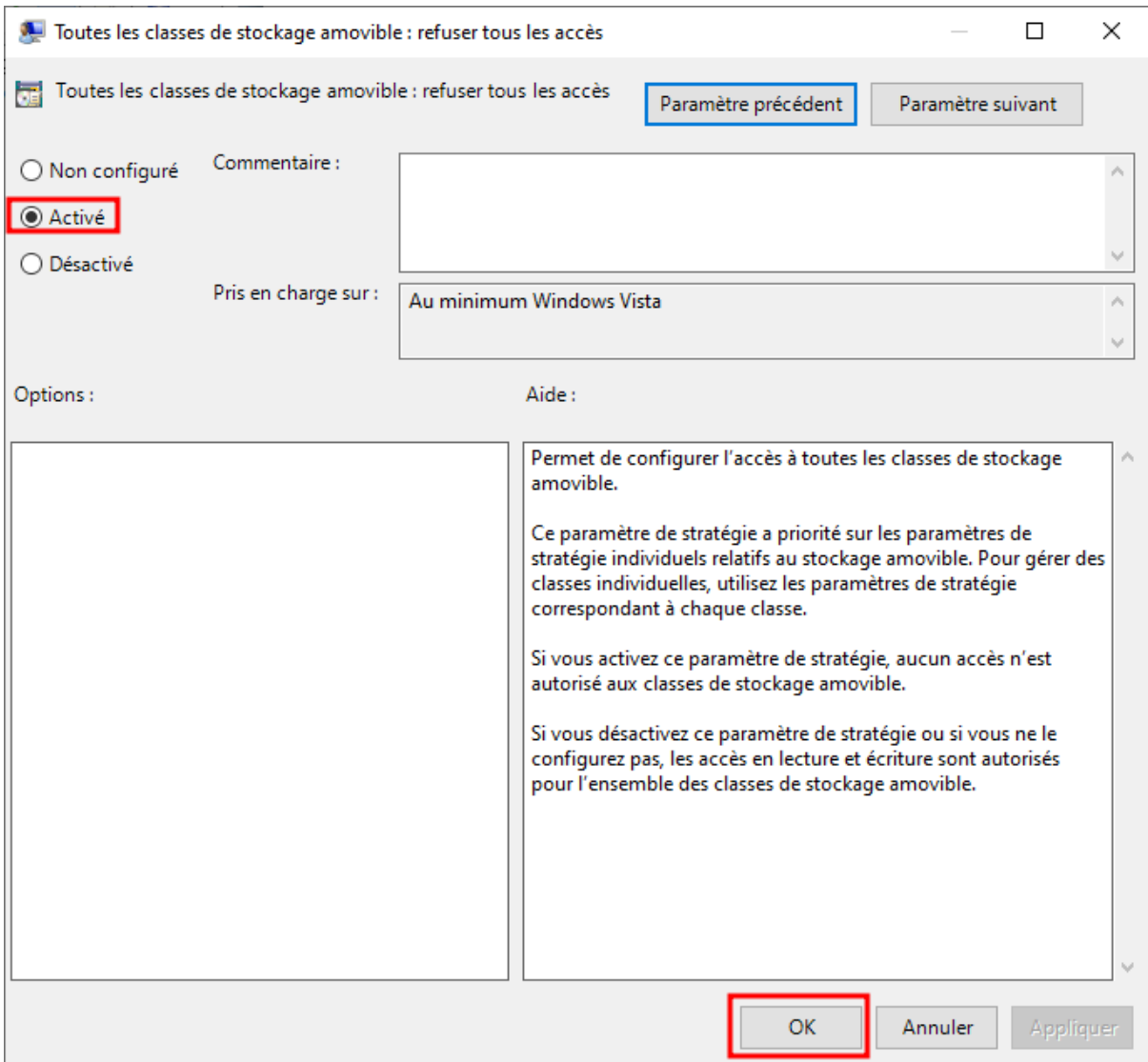
Si vous activez ce paramètre de stratégie, aucun accès n'est autorisé aux classes de stockage amovible.

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.

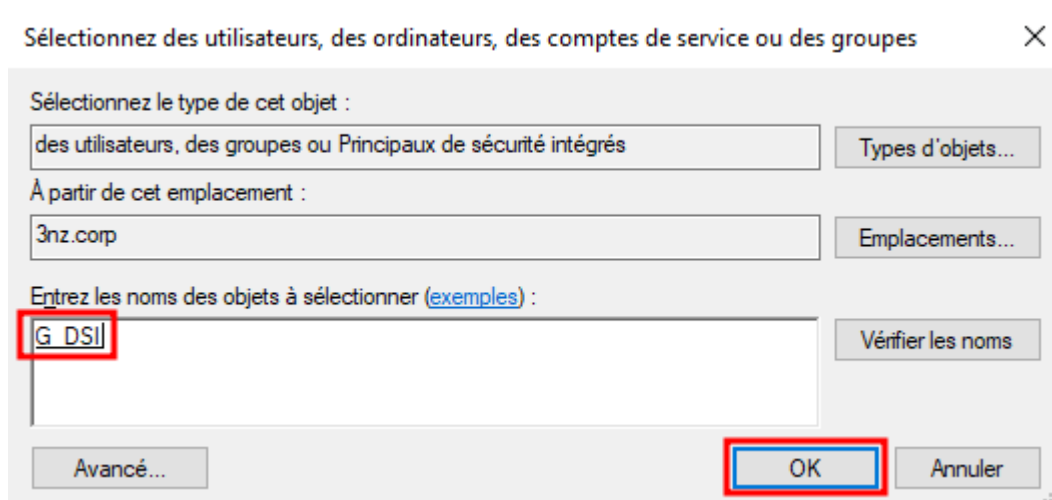
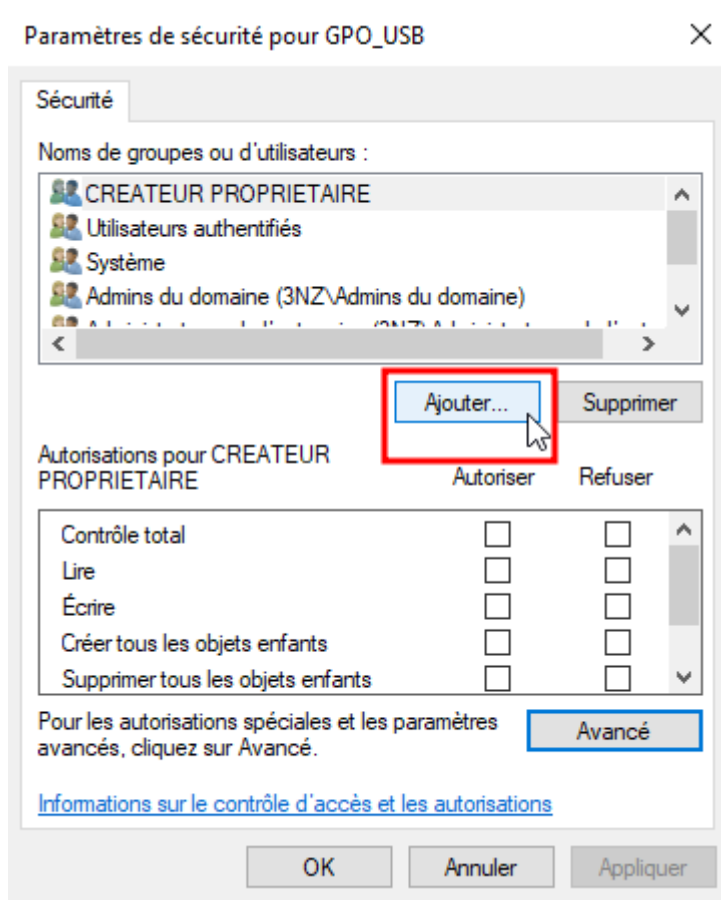
Paramètre	État
Définir le délai (en secondes) avant de forcer le redémarrage	Non config
CD et DVD : refuser l'accès en exécution	Non config
CD et DVD : refuser l'accès en lecture	Non config
CD et DVD : refuser l'accès en écriture	Non config
Classes personnalisées : refuser l'accès en lecture	Non config
Classes personnalisées : refuser l'accès en écriture	Non config
Lecteurs de disquettes : refuser l'accès en exécution	Non config
Lecteurs de disquettes : refuser l'accès en lecture	Non config
Lecteurs de disquettes : refuser l'accès en écriture	Non config
Disques amovibles : refuser l'accès en exécution	Non config
Disques amovibles : refuser l'accès en lecture	Non config
Disques amovibles : refuser l'accès en écriture	Non config
<b>Toutes les classes de stockage amovible : refuser tous les accès</b>	<b>Non config</b>
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	

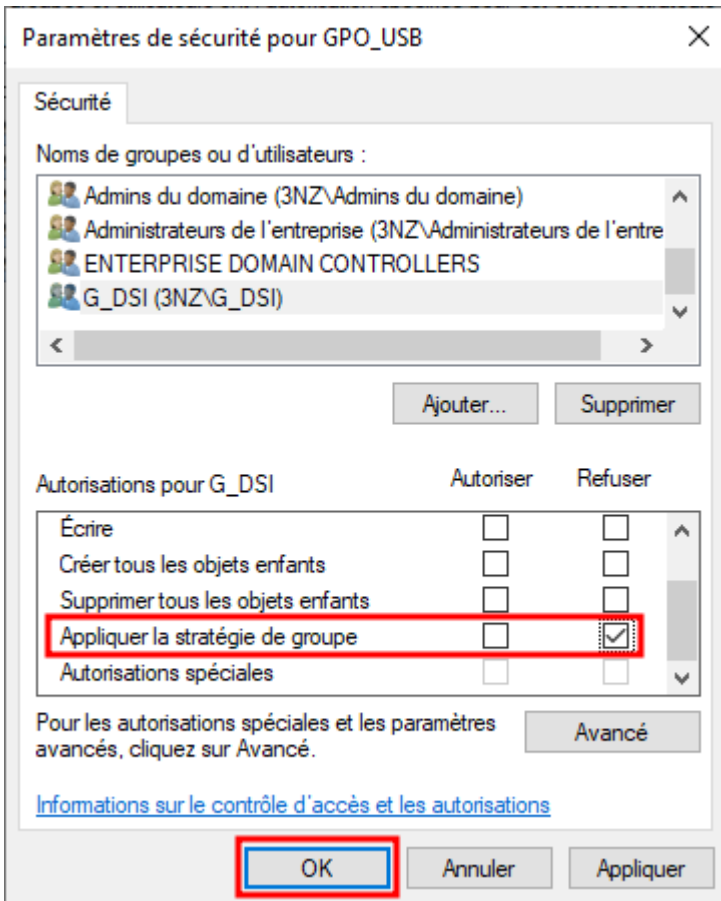
Context menu for the selected parameter:

- Modifier
- Filtre activé
- Options des filtres...
- Réappliquer le filtre
- Toutes les tâches >
- Aide

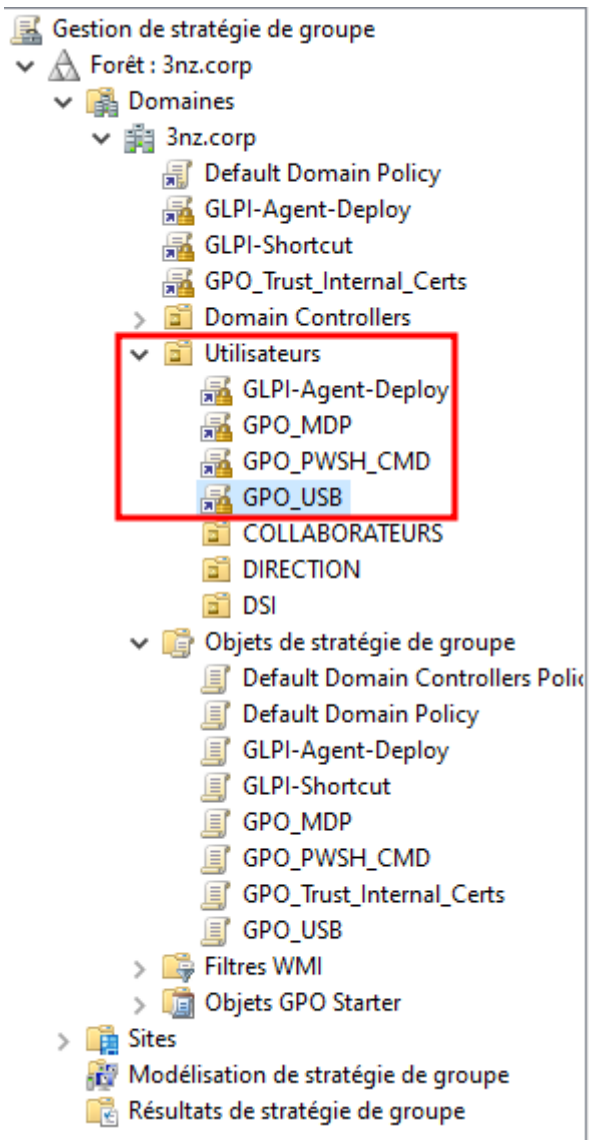


Je décide de faire une délégation pour le groupe DSI :





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



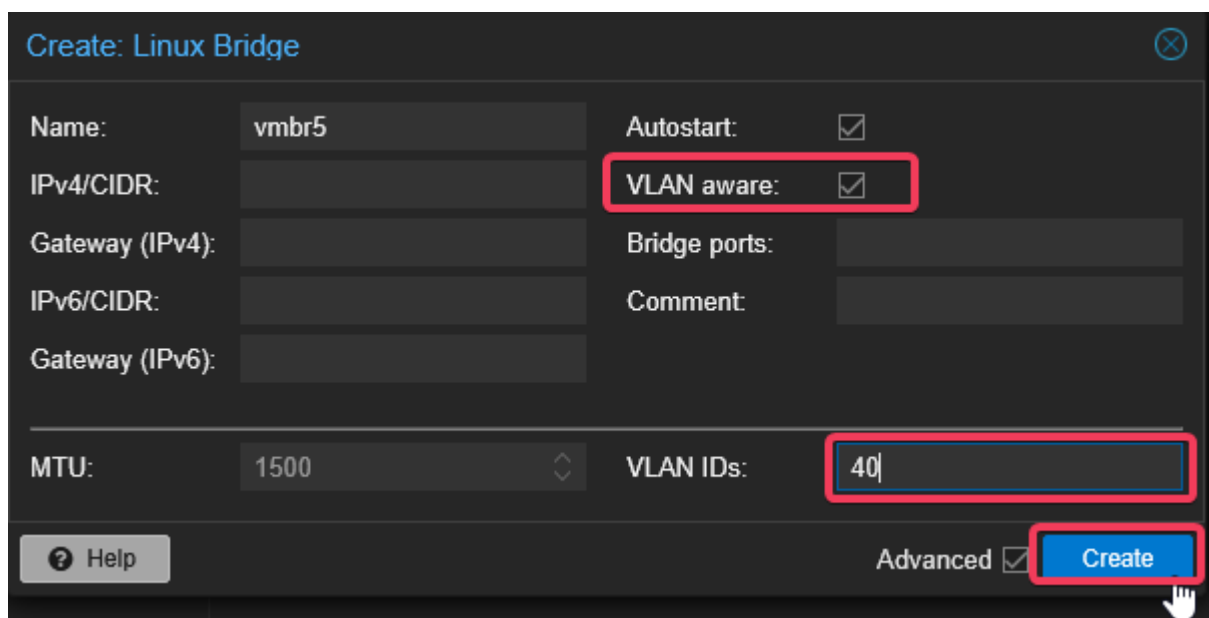
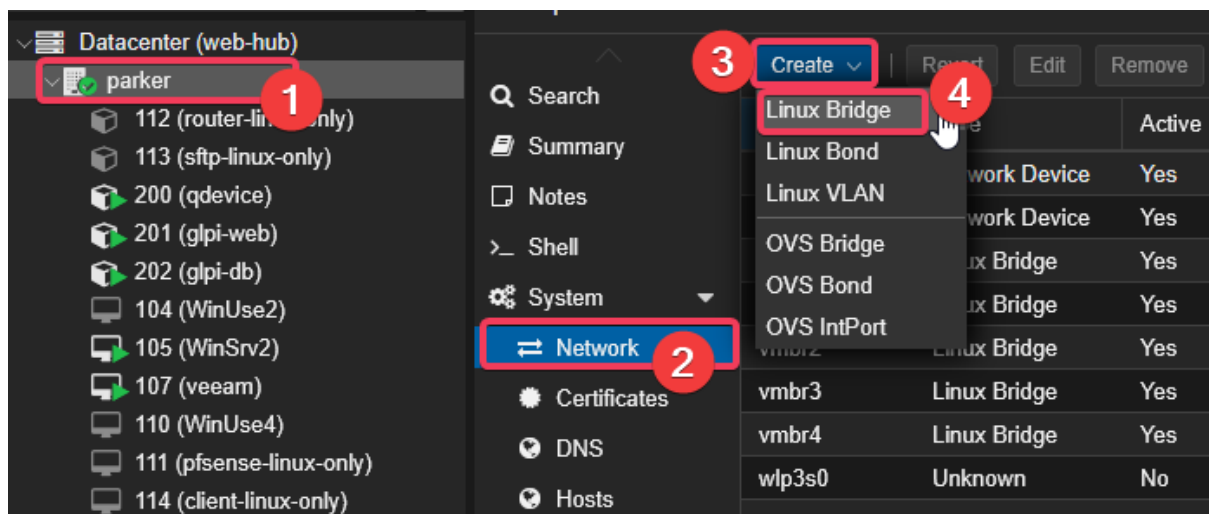
## V. DMZ et Publication Web

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

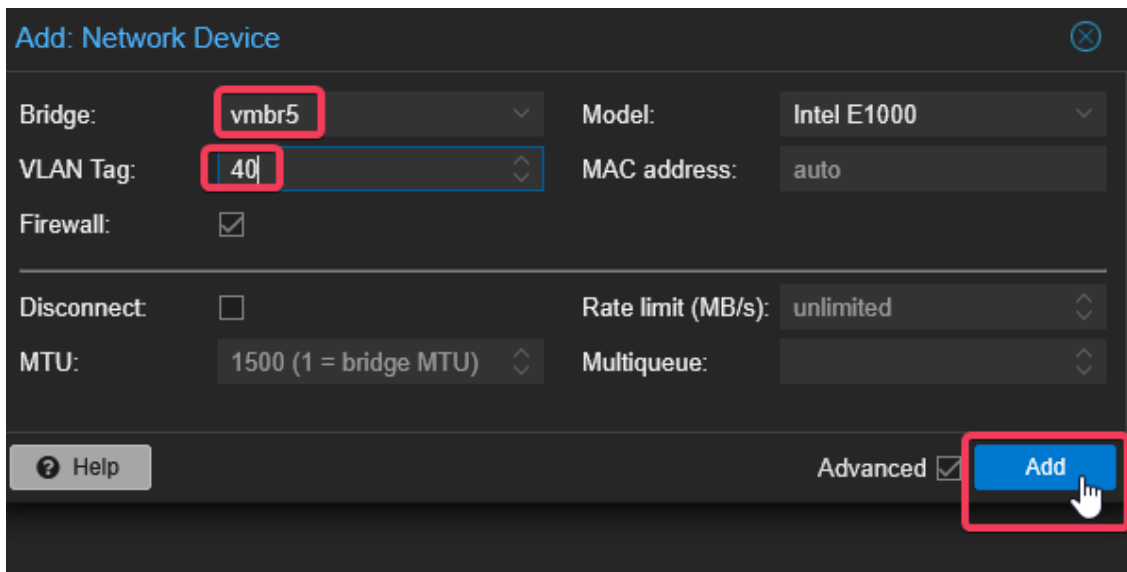
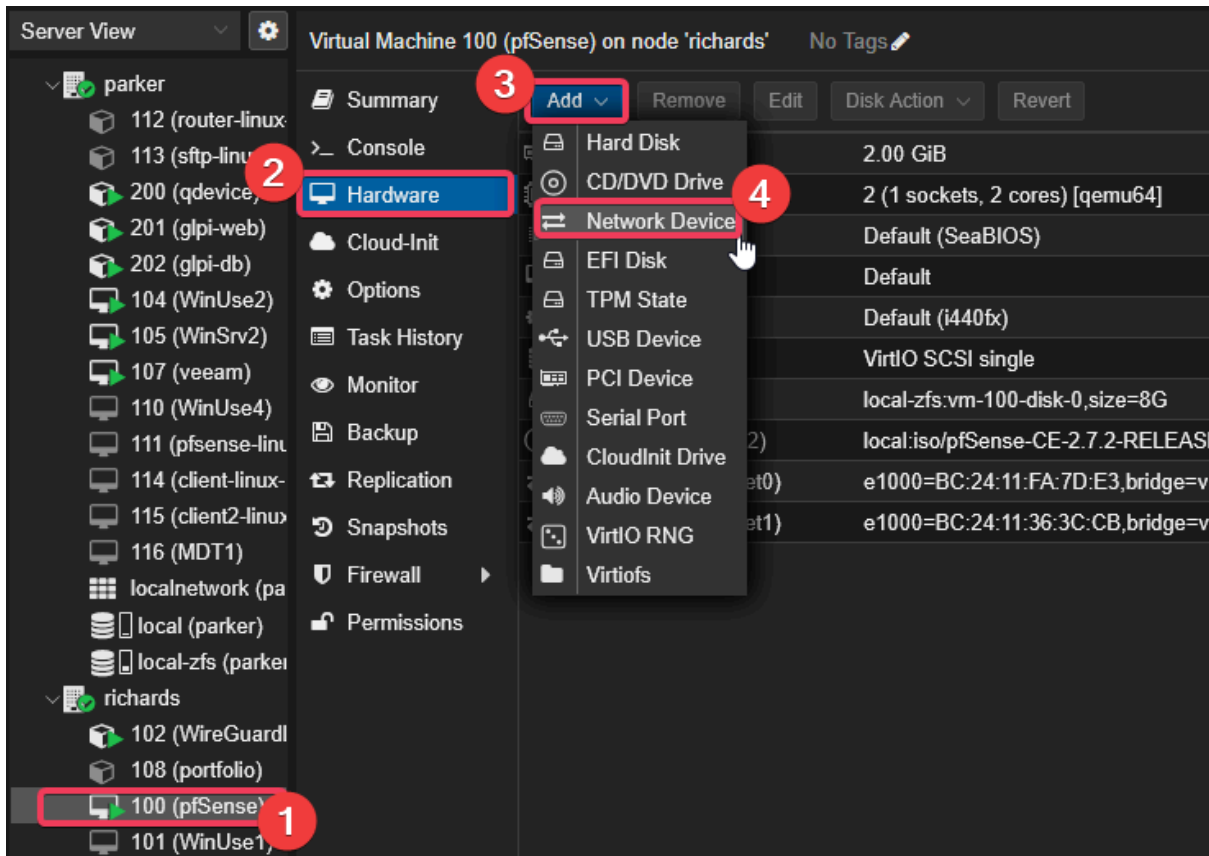
L'entreprise voulant créer un site vitrine, la nécessité de créer une DMZ est crucial. Je créer donc un nouveau VLAN qui portera le numéro 40 (192.168.40.0/27).

1ère étape :

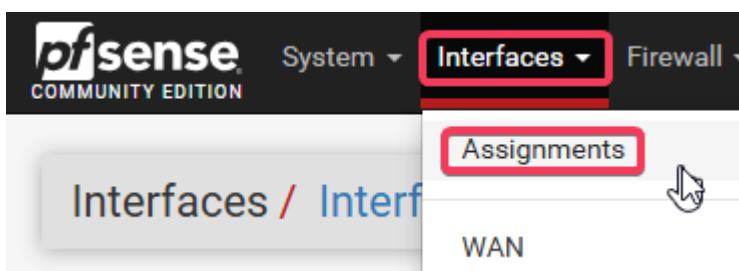
Créer la nouvelle interface pour ce VLAN et l'assigner sur pfSense :



Ajouter l'interface vmbr5 sur le pfsense :



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



Interfaces / Interface Assignments [?] [list icon]

Interface Assignments **Interface Groups** Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port	
WAN	em0 (bc:24:11:fa:7d:e3)	
LAN	em1 (bc:24:11:36:3c:cb)	Delete
ADMIN_IT	VLAN 10 on em1 - lan (IT_ADMINISTRATION)	Delete
COLLABORATEURS	VLAN 20 on em1 - lan (COLLABORATEURS)	Delete
DIRECTION	VLAN 30 on em1 - lan (DIRECTION)	Delete
SERVEURS	VLAN 50 on em1 - lan (SERVEURS)	Delete
Available network ports:	em2 (bc:24:11:7b:3f:37) <b>1</b>	+ Add <b>2</b>

**3** Save

Puis sélectionner votre interface :

**OPT5** em2 (bc:24:11:7b:3f:37) Delete

Save

**General Configuration**

Enable  Enable interface

Description **VLAN 40**  
Enter a description (name) for the interface here.

IPv4 Configuration Type **Static IPv4**

IPv6 Configuration Type None

MAC Address xxxxxxxxxxxx  
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

MTU  
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS  
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)  
Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

**IPv4 Address** 192.168.40.1 / 27

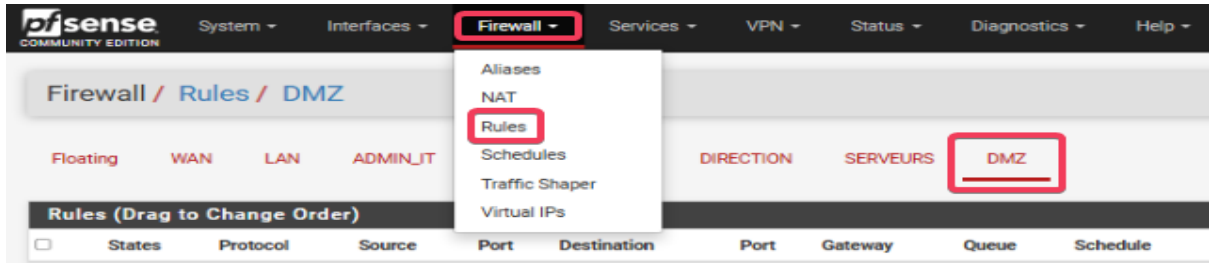
IPv4 Upstream gateway None **+ Add a new gateway**  
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by [clicking here](#).

Comme cette interface ne sera pas g er par le DHCP de mon serveur Windows  tant donn  que c'est une DMZ.

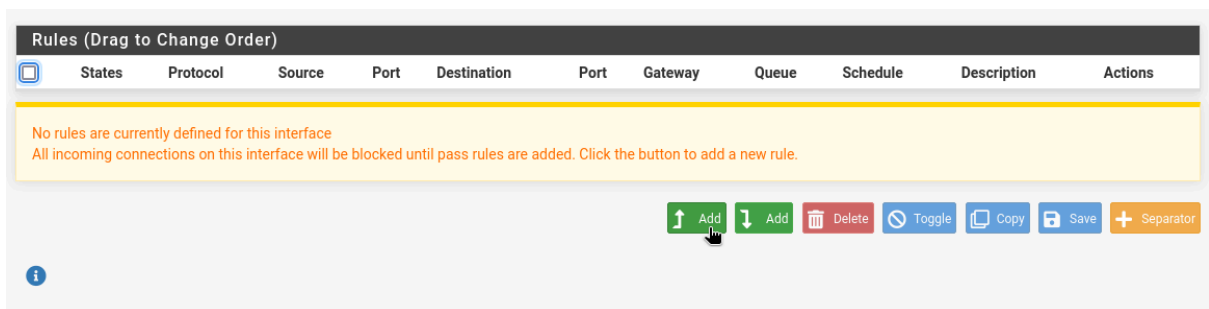
Mes serveurs expos s seront tous en statique.

- 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 :

**Edit Firewall Rule**

**Action**    
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**    
Choose the interface from which packets must come to match this rule.

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

**Protocol**    
Choose which IP protocol this rule should match.

---

**Source**

**Source**  Invert match     
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

---

**Destination**

**Destination**  Invert match     
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

**Destination Port Range**       
From Custom To Custom

---

**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**    
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**

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

The firewall rule configuration has been changed. The changes must be applied for them to take effect.

Floating WAN LAN ADMIN\_IT COLLABORATEURS DIRECTION SERVEURS **DMZ**

**Rules (Drag to Change Order)**

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	192.168.40.10	*	*	443 (HTTPS)	*	none		Autorisation du trafic entre le reverse proxy et internet.	<input type="button" value="Save"/>

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

**Rules (Drag to Change Order)**

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	192.168.40.10	*	*	443 (HTTPS)	*	none		Autorisation du trafic entre le reverse proxy et internet.	<input type="button" value="Save"/>

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

<input type="checkbox"/>	<span style="color: green;">✓</span>	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** Blocage du trafic 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

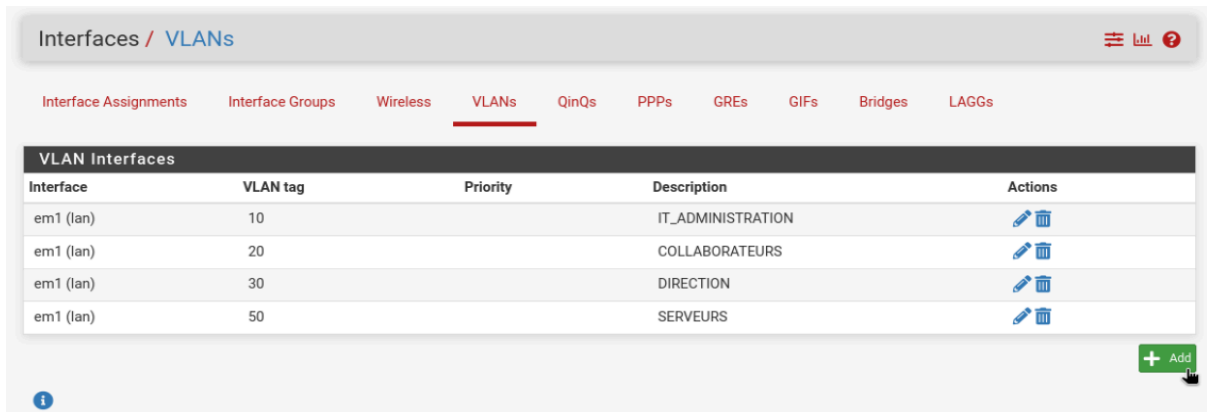
Enfin, voici toutes les règles de pare-feu de ma DMZ.

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<span style="color: red;">✗</span>	0/0 B	IPv4 *	ADMIN_IT subnets	*	DMZ subnets	*	*	none	Blocage du trafic entre les réseaux internes et la DMZ.	
<input type="checkbox"/>	<span style="color: red;">✗</span>	0/0 B	IPv4 *	COLLAB subnets	*	DMZ subnets	*	*	none	Blocage du trafic entre les réseaux internes et la DMZ.	
<input type="checkbox"/>	<span style="color: red;">✗</span>	0/0 B	IPv4 *	DIRECTION subnets	*	DMZ subnets	*	*	none	Blocage du trafic entre les réseaux internes et la DMZ.	
<input type="checkbox"/>	<span style="color: red;">✗</span>	0/0 B	IPv4 *	SERVEURS subnets	*	DMZ subnets	*	*	none	Blocage du trafic entre les réseaux internes et la DMZ.	
<input type="checkbox"/>	<span style="color: red;">✗</span>	0/0 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none	Blocage du trafic entre les réseaux internes et la DMZ.	
<input type="checkbox"/>	<span style="color: green;">✓</span>	0/0 B	IPv4	DMZ subnets	*	1.1.1.1	53 (DNS)	*	none	Autorisation du trafic entre la DMZ et internet	
<input type="checkbox"/>	<span style="color: green;">✓</span>	0/0 B	IPv4	DMZ subnets	*	*	80 (HTTP)	*	none	Autorisation du trafic entre la DMZ et internet	
<input type="checkbox"/>	<span style="color: green;">✓</span>	0/0 B	IPv4	DMZ subnets	*	*	443 (HTTPS)	*	none	Autorisation du trafic entre la DMZ et internet	
<input type="checkbox"/>	<span style="color: green;">✓</span>	0/504 B	IPv4 *	DMZ subnets	*	DMZ subnets	*	*	none		
<input type="checkbox"/>	<span style="color: red;">✗</span>	0/4 KiB	IPv4 *	DMZ subnets	*	*	*	*	none	Règle de blocage par défaut de la DMZ	

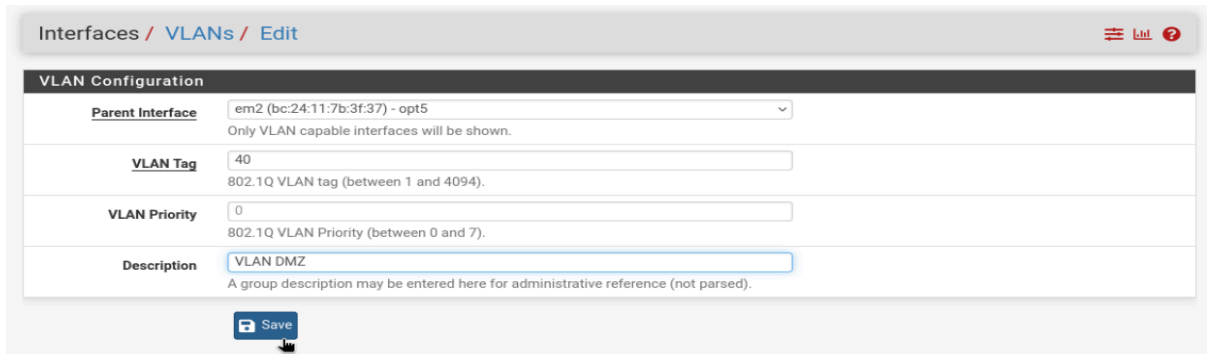
Maintenant on déclare le VLAN sur pfSense, sinon il ne reconnaîtra pas les paquets tagués

Interfaces -> VLANs

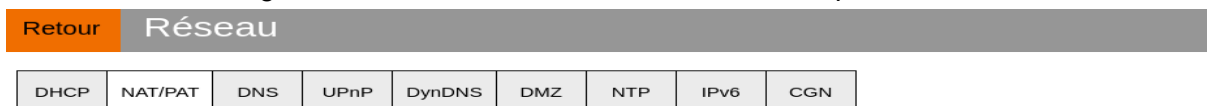
Cliquez sur Add



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:



### Vos règles personnalisées

Choisissez des ports qui ne sont pas bloqués par le pare-feu.  
 Nous vous déconseillons la création d'une règle sur le port 53 (service DNS).  
 Les équipements doivent être configurés avec une adresse IP statique pour être disponibles.

IP externes autorisées

Activer	Application/Service	Port interne	Port externe	Protocole	Équipement	IP externe	
<input checked="" type="checkbox"/>	VPN	47777	47777	UDP	Device-20	Toutes	
<input checked="" type="checkbox"/>	Web Server (HTTP)	80	80	TCP	Device-2506	Toutes	
<input checked="" type="checkbox"/>	Secure Web Server (HTTPS)	443	443	TCP	Device-2506	Toutes	

- 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 :

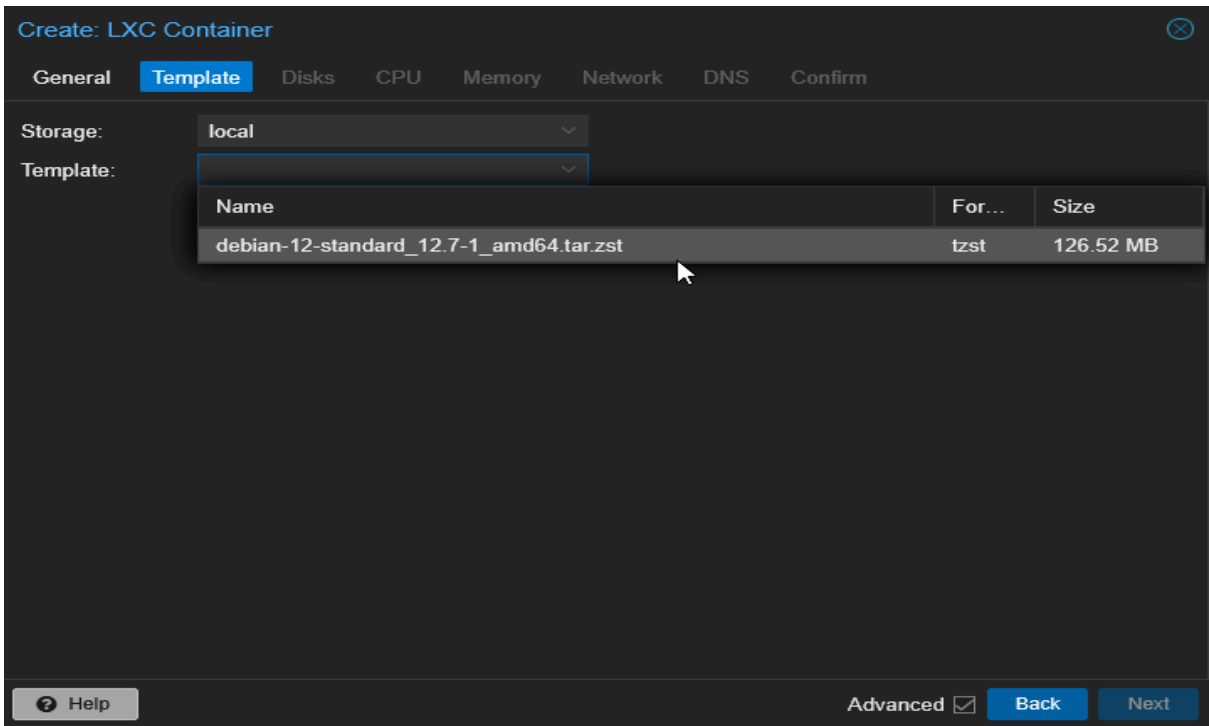
The screenshot shows a configuration window titled "Create: LXC Container" with a close button in the top right corner. The window has several tabs: "General" (selected), "Template", "Disks", "CPU", "Memory", "Network", "DNS", and "Confirm".

Under the "General" tab, the following fields are visible:

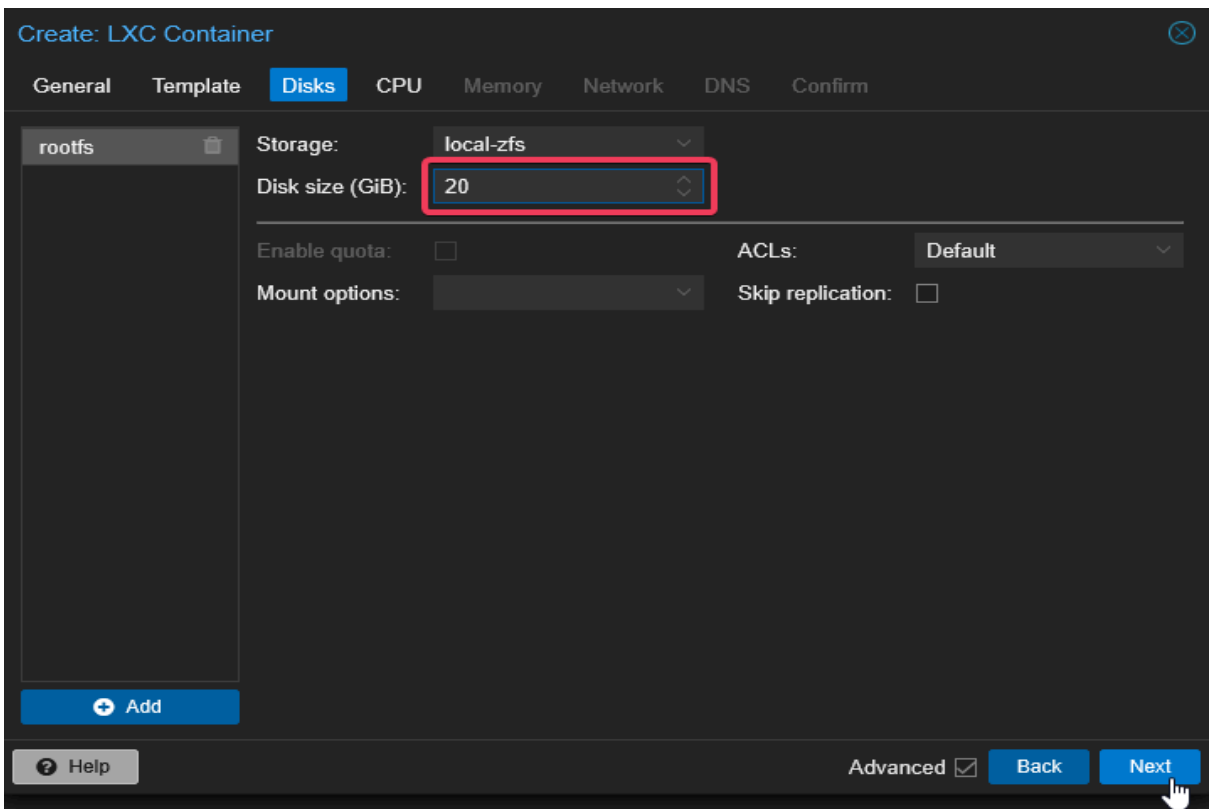
- Node:** A dropdown menu with "richards" selected.
- CT ID:** A dropdown menu with "119" selected.
- Hostname:** A text input field containing "ReverseProxy".
- Resource Pool:** A dropdown menu with "infra" selected.
- Unprivileged container:** A checkbox that is checked.
- Nesting:** A checkbox that is checked.
- Password:** A password input field with masked characters.
- Confirm password:** A password input field with masked characters.
- SSH public key(s):** A text area for entering SSH keys.

Below these fields is a blue button labeled "Load SSH Key File".

At the bottom of the window, there is a "Tags" section with the text "No Tags" and a plus sign button. In the bottom right corner, there are three buttons: "Help" (with an information icon), "Advanced" (with a checked checkbox), and "Next" (with a mouse cursor hovering over it).



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



1 Cores est largement suffisant :

Create: LXC Container ⓧ

General Template Disks **CPU** Memory Network DNS Confirm

Cores:

CPU limit:  CPU units:

Advanced

1 Go de RAM :

Create: LXC Container ⓧ

General Template Disks CPU **Memory** Network DNS Confirm

Memory (MiB):

Swap (MiB):

Advanced

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

Create: LXC Container

General Template Disks CPU Memory Network DNS Confirm

Name: eth0  
MAC address: auto  
Bridge: vibr5  
VLAN Tag: 40  
Firewall:

IPv4:  Static  DHCP  
IPv4/CIDR: 192.168.40.10/27  
Gateway (IPv4): 192.168.40.1

IPv6:  Static  DHCP  SLAAC  
IPv6/CIDR: None  
Gateway (IPv6):

Disconnect:   
MTU: Same as bridge

Rate limit (MB/s): unlimited

Help Advanced  Back Next

Pour les DNS je choisi celui de CloudFlare :

Create: LXC Container

General Template Disks CPU Memory Network DNS Confirm

DNS domain: use host settings  
DNS servers: 1.1.1.1

Advanced  Back Next

Voilà la création du container est fini :

Create: LXC Container

General Template Disks CPU Memory Network DNS Confirm

Key ↑	Value
cores	1
features	nesting=1
hostname	ReverseProxy
memory	1024
nameserver	1.0.0.1
net0	name=eth0,bridge=vibr5,tag=40,firewall=1,ip=192.168.40.10/27,gw=192.168.40.1
nodename	richards
ostemplate	local:vztmpl/debian-12-standard_12.7-1_amd64.tar.zst
pool	infra
rootfs	local-zfs:20
searchdomain	1.1.1.1
ssh-public-keys	
swap	1024
unprivileged	1

Start after created

Advanced  Back Finish

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

Edit: Network Device (veth)

Name: eth0 IPv4:  Static  DHCP

MAC address: BC:24:11:B6:9B:E5 IPv4/CIDR: 192.168.40.20/24

Bridge: vibr5 Gateway (IPv4): 192.168.40.1

VLAN Tag: no VLAN IPv6:  Static  DHCP  SLAAC

Firewall:  IPv6/CIDR: None

Gateway (IPv6):

Disconnect:  Rate limit (MB/s): unlimited

MTU: Same as bridge

Help Advanced  OK

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

The top screenshot shows the 'Firewall / NAT / Port Forward' configuration page. The 'Rules' table is empty. A tooltip is visible over the 'Add' button, stating 'Add rule to the top of the list'.

The bottom screenshot shows the same page after two rules have been added. A green message at the top indicates: 'The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.'

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/> WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.40.10	80 (HTTP)	Redirection du trafic vers le reverse proxy	
<input type="checkbox"/> WAN	TCP	*	*	WAN address	443 (HTTPS)	192.168.40.10	443 (HTTPS)	Redirection du trafic vers le reverse proxy	

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

### 3nz.fr

Renouvellement automatique prévu en **avr. 2028**

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

[Informations générales](#) [Zone DNS](#) [Serveurs DNS](#) [Redirection](#) [DynHost](#) [GLUE](#)

**Vous pouvez voir ici la configuration des diverses entrées de votre domaine.**

Vous avez également la possibilité de configurer ces entrées pour relier votre domaine à vos différents services (bouton « ajouter une entrée »).

Tous Recherche domaine...

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

1 2 > >>

10 Page 1 / 2 OK

- Ajouter une entrée
- Modifier en mode textuel
- Modifier le TTL par défaut
- Voir l'historique de ma zone DNS
- Réinitialiser ma zone DNS

#### Guides

Zone DNS

Je choisis A en champs de pointage :

✕

### Ajouter une entrée à la zone DNS

*Étape 1 sur 3*

Sélectionnez un type de champ DNS :

Champs de pointage

**A**   **AAAA**   **NS**   **CNAME**   **DNAME**

Champs étendus

**CAA**   **TXT**   **NAPTR**   **SRV**   **LOC**   **SSHFP**   **TLSA**

Champs mails

**MX**   **SPF**   **DKIM**   **DMARC**

Annuler   Suivant

✕

### Ajouter une entrée à la zone DNS

*Étape 2 sur 3*

\* Les champs suivis d'un astérisque sont obligatoires.

**Sous-domaine**

Attention: une cible est déjà configurée pour ce domaine.

**TTL**

**Cible \***

**Le champ A actuellement généré est le suivant :**

```
IN A 86.227.249.66
```

Annuler   Précédent   Suivant




## Ajouter une entrée à la zone DNS

Étape 3 sur 3

Vous allez ajouter l'entrée suivante dans votre zone DNS :

Type de champ	A
Domaine	3nz.fr.
Cible	86.227.249.66

 L'ajout sera immédiat dans la zone DNS, mais veuillez prendre en compte le temps de propagation (maximum 24h).

Annuler

Précédent

Valider

### ● 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 :

Étape 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

Étape 2 : Configuration DNS (OVH)

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

Version classique Version beta Français Enzo Lemesle

Tous Recherche domaine...

Domaine

- 3nz.fr
- 3nz.fr
- 3nz.fr
- www.3nz.fr
- ftp.3nz.fr
- 3nz.fr
- 3nz.fr
- www.3nz.fr
- 3nz.fr
- 3nz.fr

10 Page 1 / 2 OK

Ajouter une entrée 2

J'ajoute une entrée A :

Ajouter une entrée à la zone DNS Étape 1 sur 3

Sélectionnez un type de champ DNS :

Champs de pointage

A AAAA NS CNAME DNAME

Champs étendus

CAA TXT NAPTR SRV LOC SSHFP TLSA

Champs mails

MX SPF DKIM DMARC

Annuler Suivant

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



## Ajouter une entrée à la zone DNS

Étape 2 sur 3

\* Les champs suivis d'un astérisque sont obligatoires.

1

Sous-domaine  
corp .3nz.fr.

Par défaut

TTL

2

Cible \*  
86.227.249.66

Le champ A actuellement généré est le suivant :

```
corp IN A 86.227.249.66
```

Annuler

Précédent

Suivant

3

Pour la troisième étape, valider :




## Ajouter une entrée à la zone DNS

Étape 3 sur 3

Vous allez ajouter l'entrée suivante dans votre zone DNS :

Type de champ	A
Domaine	corp.3nz.fr.
Cible	86.227.249.66

 L'ajout sera immédiat dans la zone DNS, mais veuillez prendre en compte le temps de propagation (maximum 24h).

Annuler

Précédent

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 faite 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 :

Create: LXC Container ⊗

General   Template   Disks   CPU   Memory   Network   DNS   **Confirm**

Key ↑	Value
cores	2
features	nesting=1
hostname	ZabbixSrv
memory	4096
nameserver	192.168.50.10
net0	name=eth0,bridge=vibr1,tag=50,firewall=1,ip=192.168.50.5/27,gw=192.168.50.1
nodename	parker
ostemplate	local:vztmpl/debian-12-standard_12.7-1_amd64.tar.zst
pool	infra_bts
rootfs	local-zfs:40
ssh-public-keys	
swap	4096
tags	infra_bts
unprivileged	1

Start after created

Advanced  **Back** **Finish**

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
```

Connexion 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 '██████████';  
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
```

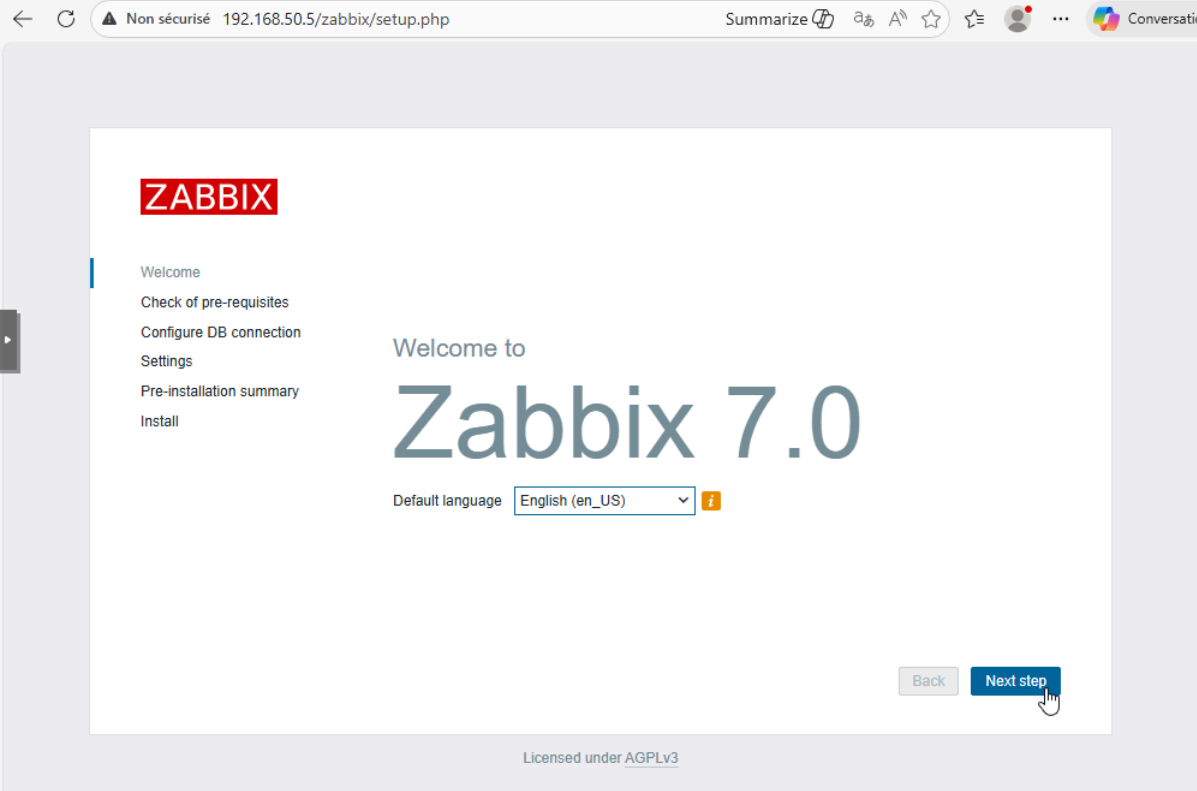
Démarrer les services Zabbix :

```
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](http://<adresse_ip_serveur>/zabbix)



The screenshot shows a web browser window displaying the Zabbix 7.0 installation setup page. The browser's address bar shows the URL `192.168.50.5/zabbix/setup.php`. The page features the Zabbix logo in the top left corner. A navigation menu on the left lists the following steps: Welcome, Check of pre-requisites, Configure DB connection, Settings, Pre-installation summary, and Install. The main content area displays "Welcome to Zabbix 7.0" in large text. Below this, there is a "Default language" dropdown menu currently set to "English (en\_US)". At the bottom right of the main content area, there are two buttons: "Back" and "Next step". The "Next step" button is highlighted with a mouse cursor. At the very bottom of the page, it states "Licensed under AGPLV3".

# ZABBIX

## Check of pre-requisites

- Welcome
- Check of pre-requisites
- Configure DB connection
- Settings
- Pre-installation summary
- Install

	Current value	Required	
PHP version	8.2.30	8.0.0	OK
PHP option "memory_limit"	128M	128M	OK
PHP option "post_max_size"	16M	16M	OK
PHP option "upload_max_filesize"	2M	2M	OK
PHP option "max_execution_time"	300	300	OK
PHP option "max_input_time"	300	300	OK
PHP databases support	MySQL		OK
PHP bcmath	on		OK
PHP mbstring	on		OK
PHP option "mbstring.func_overload"	off	off	OK

[Back](#) [Next step](#)

Renseigner le user ainsi que le mot de passe :

# ZABBIX

## Configure DB connection

Please create database manually, and set the configuration parameters for connection to this database. Press "Next step" button when done.

- Welcome
- Check of pre-requisites
- Configure DB connection
- Settings
- Pre-installation summary
- Install

Database type

Database host

Database port  0 - use default port

Database name

Store credentials in  Plain text  HashiCorp Vault  CyberArk Vault

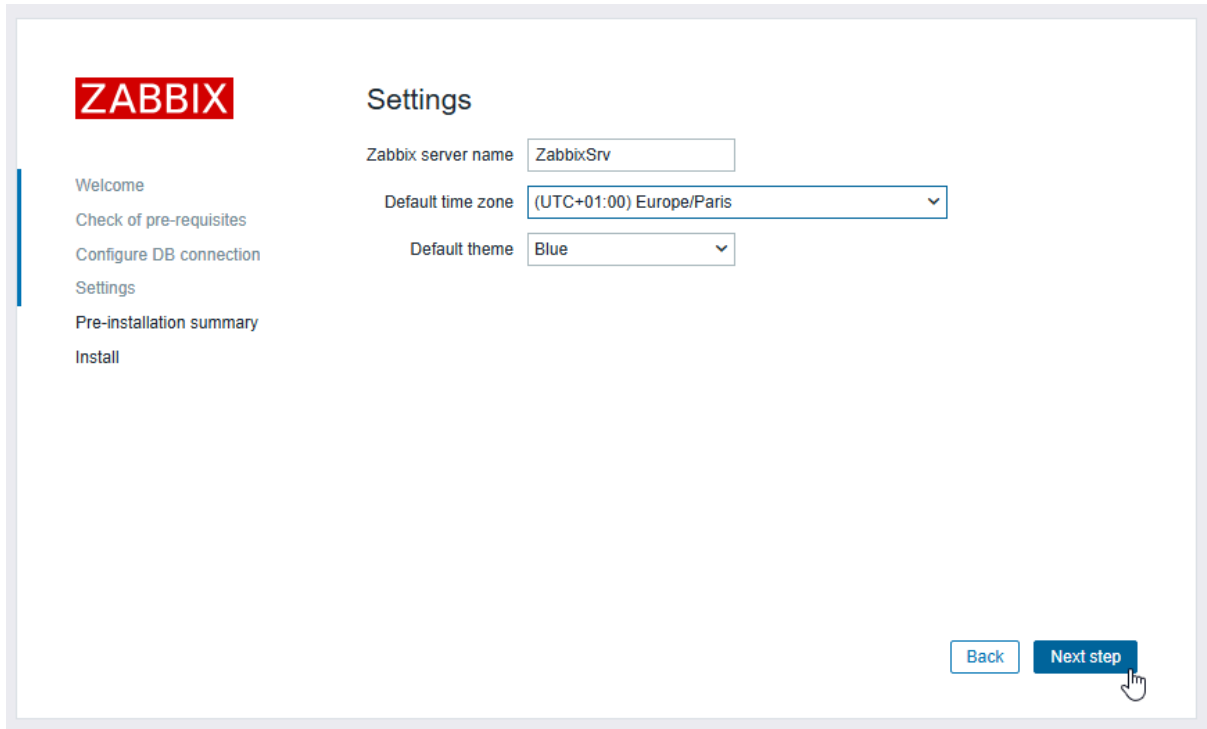
User

Password

Database TLS encryption *Connection will not be encrypted because it uses a socket file (on Unix) or shared memory (Windows).*

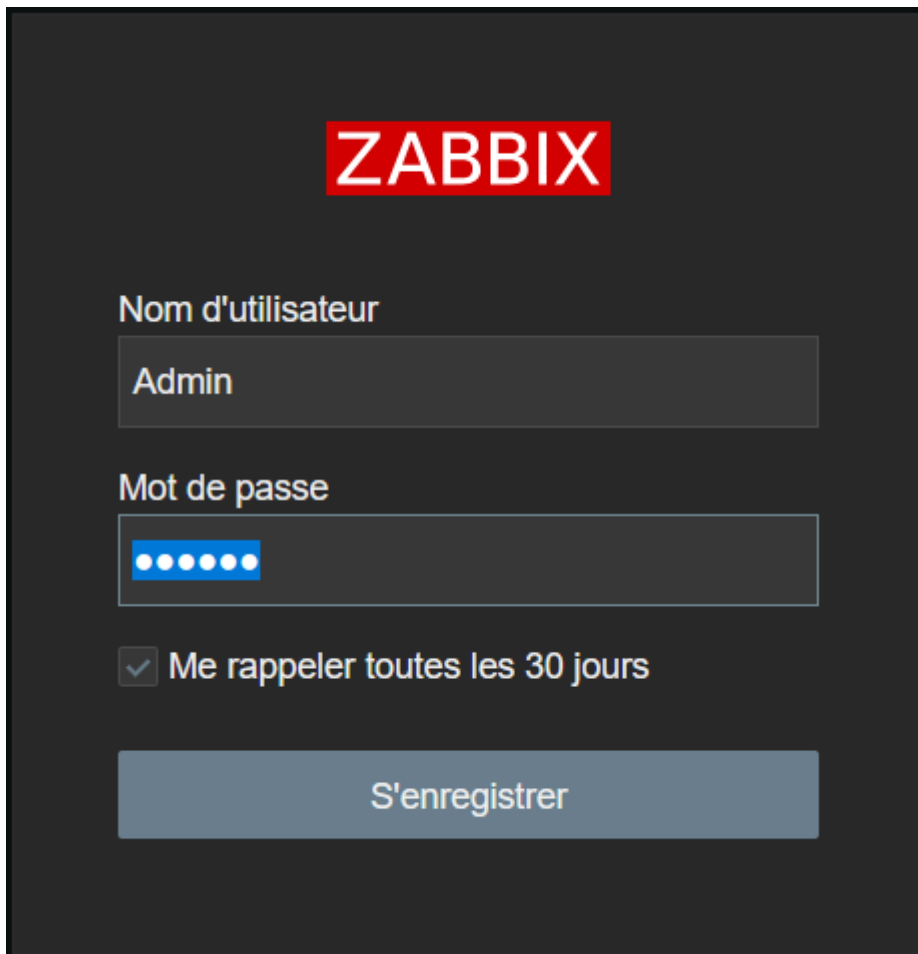
[Back](#) [Next step](#)

Renseigner votre fuseau horaire :



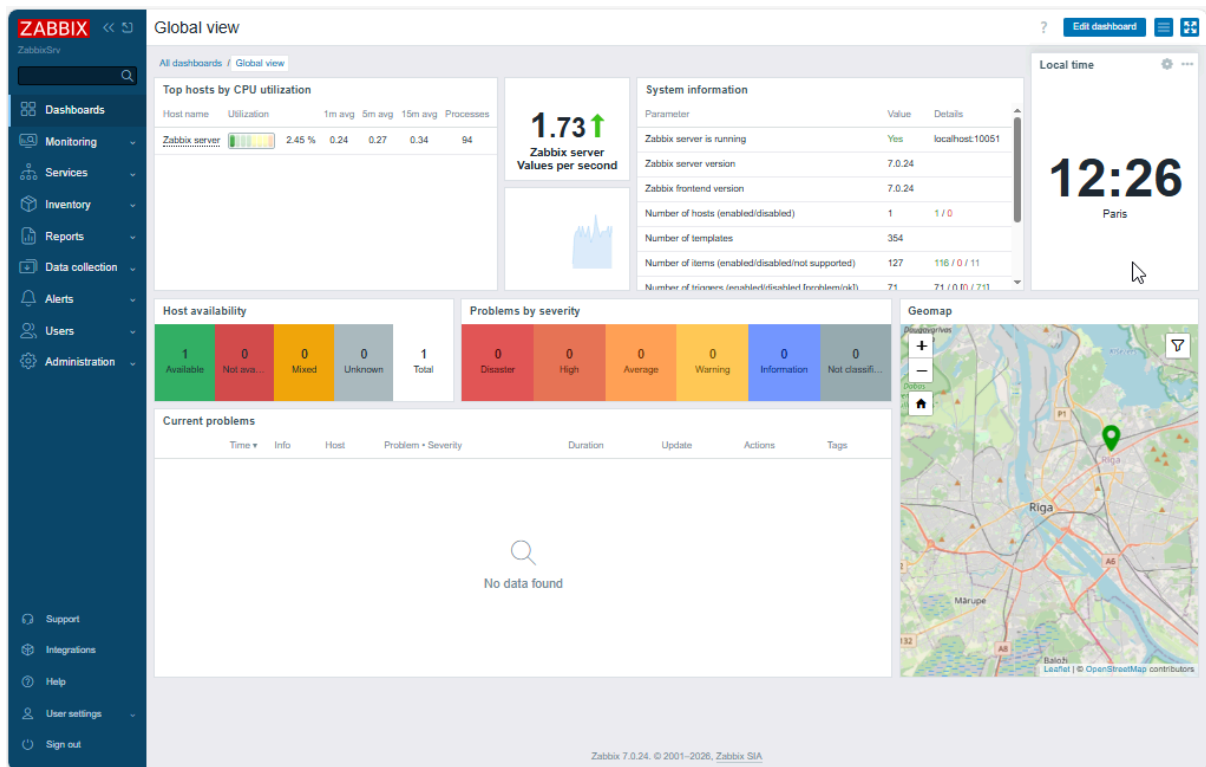
The screenshot shows the Zabbix installation settings page. On the left is a navigation menu with the ZABBIX logo at the top, followed by links for Welcome, Check of pre-requisites, Configure DB connection, Settings (which is highlighted), Pre-installation summary, and Install. The main content area is titled 'Settings' and contains three configuration fields: 'Zabbix server name' with the value 'ZabbixSrv', 'Default time zone' with a dropdown menu set to '(UTC+01:00) Europe/Paris', and 'Default theme' with a dropdown menu set to 'Blue'. At the bottom right, there are two buttons: 'Back' and 'Next step', with a mouse cursor hovering over the 'Next step' button.

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



The screenshot shows the Zabbix user registration form on a dark background. At the top is the ZABBIX logo. Below it are the following fields and options: 'Nom d'utilisateur' with a text input field containing 'Admin'; 'Mot de passe' with a password input field showing six white dots; a checkbox labeled 'Me rappeler toutes les 30 jours' which is checked; and a large 'S'enregistrer' button at the bottom.

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 :

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	192.168.50.5	*	SERVEURS subnets	10050	*	none	Remonter glpi agent	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	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"**.

The screenshot shows the Zabbix web interface. On the left sidebar, the 'Monitoring' menu is highlighted. The main content area is titled 'Hosts' and features a 'Create host' button in the top right corner. The form includes fields for Name, Host groups, IP, DNS, Port, Status (Any, Enabled, Disabled), Tags (And/Or, Or), and Severity (Not classified, Warning, High, Information, Average, Disaster). Below the form is a table with columns: Name, Interface, Availability, Tags, Status, Latest data, Problems, Graphs, Dashboards, and Web. The table contains one entry: 'Zabbix server' with interface '127.0.0.1:10050', availability 'zbx', and tags 'class: os', 'class: software', 'target: linux'. The footer indicates 'Zabbix 7.0.24. © 2001-2026, Zabbix SIA'.

Remplir les champs :

Host configuration page showing fields for Host name (GLPI-WEB), Visible name (GLPI-WEB), Templates (Zabbix agent), Host groups (Linux servers), Interfaces (Agent, 192.168.50.3, IP, DNS, 10050), Description, and Monitored by (Server). The 'Enabled' checkbox is checked. Buttons for Update, Clone, Delete, and Cancel are visible at the bottom right.

Mon serveur GLPI-WEB est bien remonté et disponible :

Name	Interface	Availability	Tags	Status	Latest data	Problems	Graphs	Dashboards	Web
GLPI-WEB	192.168.50.3:10050	ZBX	class: software target: zabbix-agent	Enabled	Latest data 4	Problems	Graphs	Dashboards 1	Web

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

Name	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags
3nzCorp	Items 4	Triggers 1	Graphs	Discovery	Web	192.168.40.20:10050		Zabbix agent	Enabled	ZBX	None		
GLPI-DB	Items 4	Triggers 1	Graphs	Discovery	Web	192.168.50.13:10050		Zabbix agent	Enabled	ZBX	None		
GLPI-WEB	Items 4	Triggers 1	Graphs	Discovery	Web	192.168.50.3:10050		Zabbix agent	Enabled	ZBX	None		
pSense	Items 4	Triggers 1	Graphs	Discovery	Web	192.168.50.1:10050		Zabbix agent	Enabled	ZBX	None		
ReverseProxy	Items 4	Triggers 1	Graphs	Discovery	Web	192.168.40.10:10050		Zabbix agent	Enabled	ZBX	None		
TrueNAS	Items 137	Triggers 44	Graphs 31	Discovery 7	Web	192.168.50.2:161		TrueNAS CORE by SNMP	Enabled	SNMP	None		
VeeamBackup	Items 4	Triggers 1	Graphs	Discovery	Web	192.168.50.4:10050		Zabbix agent	Enabled	ZBX	None		
Windows Server 1	Items 4	Triggers 1	Graphs	Discovery	Web	192.168.50.10:10050		Zabbix agent	Enabled	ZBX	None		
Windows Server 2	Items 4	Triggers 1	Graphs	Discovery	Web	192.168.50.11:10050		Zabbix agent	Enabled	ZBX	None		
Zabbix server	Items 136	Triggers 75	Graphs 11	Discovery 6	Web	127.0.0.1:10050		Linux by Zabbix agent, Zabbix server health	Enabled	ZBX	None		

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

**Global view**

All dashboards / Global view

**Top hosts by CPU utilization**

Host name	Utilization	1m avg	5m avg	15m avg	Processes
Zabbix server	2.36 %	0.24	0.37	0.79	92

**Zabbix server Values per second**

3.78 ↑

**System information**

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Zabbix server version	7.0.24	Up to date
Zabbix frontend version	7.0.24	Up to date
Number of hosts (enabled/disabled)	10	10 / 0
Number of templates	354	
Number of items (enabled/disabled/hot supported)	305	294 / 0 / 11
Number of triggers (enabled/disabled/forbidden)	127	127 / 0 / 1261

**Host availability**

Available	Not available	Mixed	Unknown	Total
9	0	0	0	9

**Problems by severity**

Disaster	High	Average	Warning	Information	Not classified
0	0	0	1	0	0

**Current problems**

Time	Info	Host	Problem • Severity	Duration	Update	Actions	Tags
03:43:55 PM		Zabbix server	Linux: Number of installed packages has been changed	28m 34s	Update	class on component on scope notice	---

**Geomap**

Riga

Mārupis

Belah

Leaflet | © OpenStreetMap contributors

Zabbix 7.0.24. © 2001–2026, Zabbix SIA