SOMMAIRE

I. Socle de virtualisation

- Installation de Proxmox VE sur deux serveurs (parker et richards)
- Configuration VLAN sur l'hyperviseur pour la segmentation réseau

Après avoir installer l'os proxmox ve sur mes deux machines, je procèdes aux configurations réseaux :

```
auto lo
iface lo inet loopback

iface enx9cebe8fd9b9b inet manual

auto vmbr0
iface vmbr0 inet static
        address 192.168.1.77/24
        gateway 192.168.1.1
        bridge-ports enx9cebe8fd9b9b
        bridge-stp off
        bridge-fd 0
        bridge-vlan-aware yes
        bridge-vids 2-4094

iface enp4s0 inet manual

iface wlp3s0 inet manual


source /etc/network/interfaces.d/*
```

Modification du fichier de configuration des interfaces de mon hyperviseur "parker", en ajoutant les lignes : bridge-vlan-aware et bridge-vids 2-4094.
Comme je n'ai pas de switch "intelligent" j'utiliserais du VLAN Trunking simulé au niveau hyperviseur.
vlan aware sert à activer les VLANs

```
auto lo
iface lo inet loopback

iface enp2s0f0 inet manual

auto vmbr0
iface vmbr0 inet static
        address 192.168.1.88/24
        gateway 192.168.1.1
        bridge-ports enp2s0f0
        bridge-stp off
        bridge-fd 0
        bridge-vlan-aware yes
        bridge-vids 2-4092

iface enp2s0f1 inet manual


source /etc/network/interfaces.d/*
```

suivi de la commande :

```
systemctl restart networking.service
```

- ## Mise en place d'un cluster Proxmox

Je pars sur le cluster de mes deux serveurs proxmox avant de déployer les windows server, donc, je commence par ajouter le hostname du serveur parker (.77) sur le serveur richards (.88) :
vim /etc/hosts :

```
127.0.0.1 localhost.localdomain localhost
192.168.1.88 richards.3nz richards
192.168.1.77 parker.3nz parker
```

puis maintenant l'inverse :
vim /etc/hosts :

```
127.0.0.1 localhost.localdomain localhost
192.168.1.77 parker.3nz parker
192.168.1.88 richards.3nz richards
```

- ## Configuration SSH sécurisée entre les nœuds

Maintenant, sur parker je vais demander l'accès SSH à richards, une fois validé, je n'aurais plus jamais besoin de retaper le mot de passe :

```
root@parker:~# ssh-copy-id root@192.168.1.88
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/root/.ssh/id_rsa.pub"
The authenticity of host '192.168.1.88 (192.168.1.88)' can't be established.
ED25519 key fingerprint is SHA256:mGOEVANzaAp5yvlQKgzuxmDJ48VifH0SrixiLEwUy38.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
root@192.168.1.88's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.1.88'"
and check to make sure that only the key(s) you wanted were added.
```

```
root@parker:~# ssh root@192.168.1.88
Linux richards 6.8.12-9-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-9 (2025-03-16T19:18Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 11 14:04:48 2025
root@richards:~#
```

- Sauvegarde et restauration des VMs/LXCs

Avant de faire le cluster, je vais sauvegarder mes vms sur une clé usb, pour éviter qu'elles se fassent écraser lors de la clusterisation :

Je liste mes disques :

```
root@richards:~# lsblk
NAME      MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
sda         8:0    0 931.4G  0 disk
├─sda1      8:1    0  1007K  0 part
├─sda2      8:2    0     1G  0 part
└─sda3      8:3    0   464G  0 part
sdb         8:16   0   1.8T  0 disk
├─sdb1      8:17   0  1007K  0 part
├─sdb2      8:18   0     1G  0 part
└─sdb3      8:19   0   464G  0 part
sdc         8:32   0 465.8G  0 disk
├─sdc1      8:33   0  1007K  0 part
├─sdc2      8:34   0     1G  0 part
└─sdc3      8:35   0   464G  0 part
sdd         8:48   1   233G  0 disk
└─sdd1      8:49   1   233G  0 part
zd0       230:0    0    30G  0 disk
├─zd0p1   230:1    0    50M  0 part
├─zd0p2   230:2    0  29.4G  0 part
└─zd0p3   230:3    0   560M  0 part
zd16      230:16   0     8G  0 disk
├─zd16p1  230:17   0     8G  0 part
├─zd16p5  230:21   0   7.6G  0 part
└─zd16p6  230:22   0   410M  0 part
```

sdd est ma clé, je créer un point de montage est j'y associe la partition de ma clé :

```
root@richards:~# mkdir -p /mnt/usb
root@richards:~# mount /dev/sdd1 /mnt/usb
```

Création du fichier de backup :

```
root@richards:~# mkdir -p /mnt/usb/richards_backup
```

Je sauvegardes les VMs :

```
root@richards:~# for id in $(qm list | awk 'NR>1 {print $1}'); do vzdump $id --dumpdir /mnt/usb/richards_backup --compress zstd; done
```

Puis, les LXC :

```
root@richards:~# for id in $(pct list | awk 'NR>1 {print $1}'); do vzdump $id --dumpdir /mnt/usb/richards_backup --compress zstd; done
```

Je vérifie si les backups on été faites :

```
root@richards:~# ls -lh /mnt/usb/richards_backup
total 6.1G
-rwxr-xr-x 1 root root  619 May 11 14:54 vzdump-lxc-102-2025_05_11-14_53_37.log
-rwxr-xr-x 1 root root 336M May 11 14:54 vzdump-lxc-102-2025_05_11-14_53_37.tar.zst
-rwxr-xr-x 1 root root 2.0K May 11 14:48 vzdump-qemu-100-2025_05_11-14_47_57.log
-rwxr-xr-x 1 root root 449M May 11 14:48 vzdump-qemu-100-2025_05_11-14_47_57.vma.zst
-rwxr-xr-x 1 root root 5.2K May 11 14:52 vzdump-qemu-101-2025_05_11-14_48_34.log
-rwxr-xr-x 1 root root 5.3G May 11 14:52 vzdump-qemu-101-2025_05_11-14_48_34.vma.zst
```

Je retire la clé en évitant les risques de corruption :

```
root@richards:~# umount /mnt/usb
```

umount assure que les buffers disques sont bien vidés.

Le cluster ne fonctionnait pas car le nœud richards contenait déjà des VM ou LXC, Proxmox refusait donc de l'ajouter au cluster pour éviter les corruptions.

Donc, je liste mes VMs et LXC :

```
root@richards:~# qm list
      VMID NAME                 STATUS     MEM(MB)    BOOTDISK(GB) PID
       100 pfSense              stopped    2048              8.00 0
       101 Windows10            stopped    2048             30.00 0
root@richards:~# pct list
VMID       Status     Lock         Name
102        stopped                 WireGuardLAN
```

Suppression des VMs et LXC :

```
root@richards:~# qm destroy 100
root@richards:~# qm destroy 101
root@richards:~# pct destroy 102
```

Elle sont bien supprimés :

```
root@richards:~# qm list
root@richards:~# pct list
root@richards:~#
```

Création du cluster à partir de parker (maître) :

```
root@parker:~# pvecm create web-hub
Corosync Cluster Engine Authentication key generator.
Gathering 2048 bits for key from /dev/urandom.
Writing corosync key to /etc/corosync/authkey.
Writing corosync config to /etc/pve/corosync.conf
Restart corosync and cluster filesystem
```

maintenant, sur richards (noeud secondaire) :

```
pvecm add 192.168.1.77
```

Vérification du cluster :

```
root@richards:~# pvecm status
Cluster information
-------------------
Name:             web-hub
Config Version:   2
Transport:        knet
Secure auth:      on

Quorum information
------------------
Date:             Sun May 11 15:09:19 2025
Quorum provider:  corosync_votequorum
Nodes:            2
Node ID:          0x00000002
Ring ID:          1.9
Quorate:          Yes

Votequorum information
----------------------
Expected votes:   2
Highest expected: 2
Total votes:      2
Quorum:           2
Flags:            Quorate

Membership information
----------------------
    Nodeid      Votes Name
0x00000001          1 192.168.1.77
0x00000002          1 192.168.1.88 (local)
```

Maintenant, restauration des VMs sur le noeud “richards”

```
root@richards:~# mkdir -p /mnt/usb
root@richards:~# mount /dev/sdd1 /mnt/usb
```

exemple restauration d’une vm :

```
root@richards:~# qmrestore /mnt/usb/richards_backup/vzdump-qemu-101-2025_05_11-14_48_34.vma.zst 101 --
storage local-zfs
```

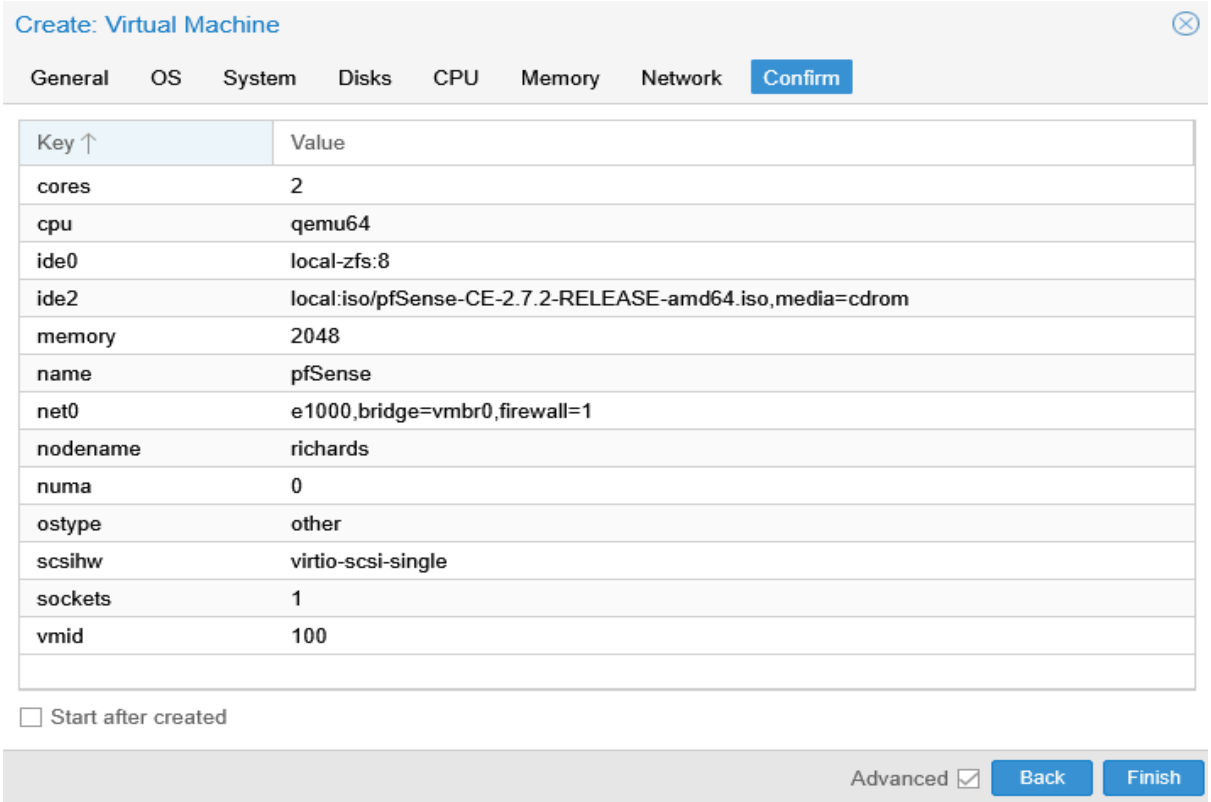
restauration d’un CT :

```
root@richards:~# pct restore 102 /mnt/usb/richards_backup/vzdump-lxc-102-2025_05_11-14_53_37.tar.zst -
-storage local-zfs
```

II. Connectivité et Sécurité Périmétrique

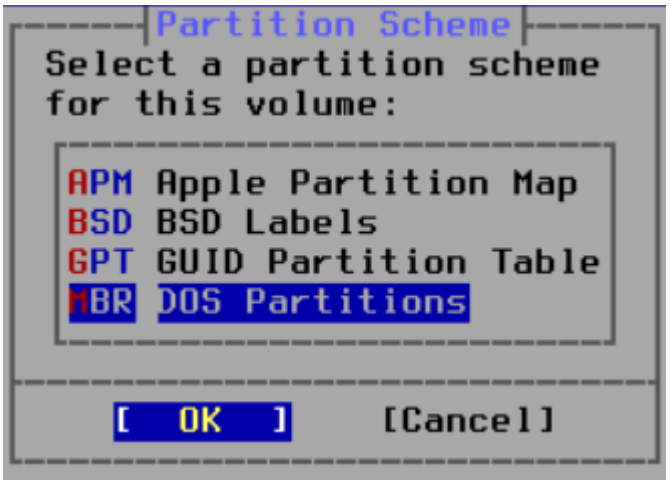
- Déploiement pfSense avec configuration WAN/LAN

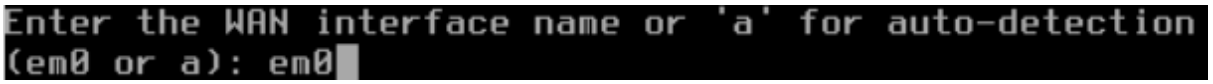
Création de la vm pfSense :

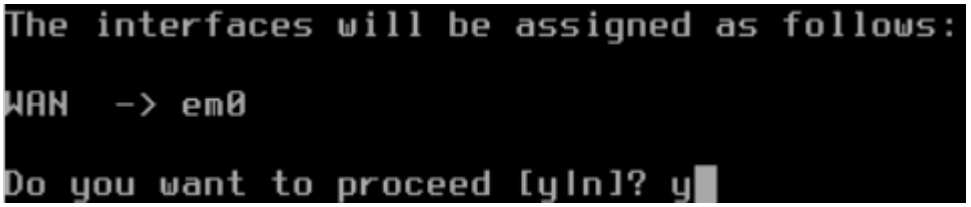


Pas de vlan sur l’interface net0 (vmbr0) car c’est celle qui aura accès au wan.

Installation de l’os pfsense sur la machine :







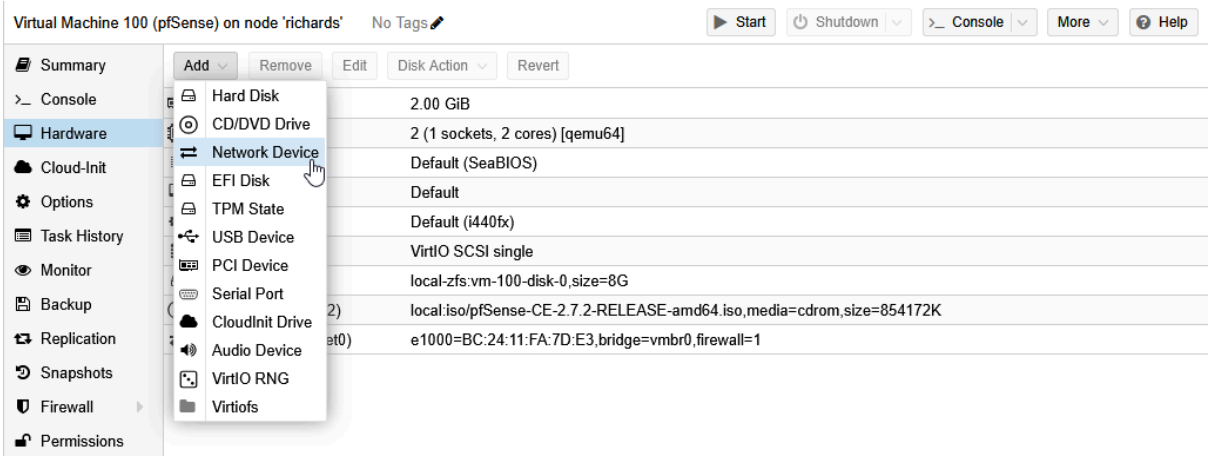
Création d’un nouvelle interface virtuel sur mon node :

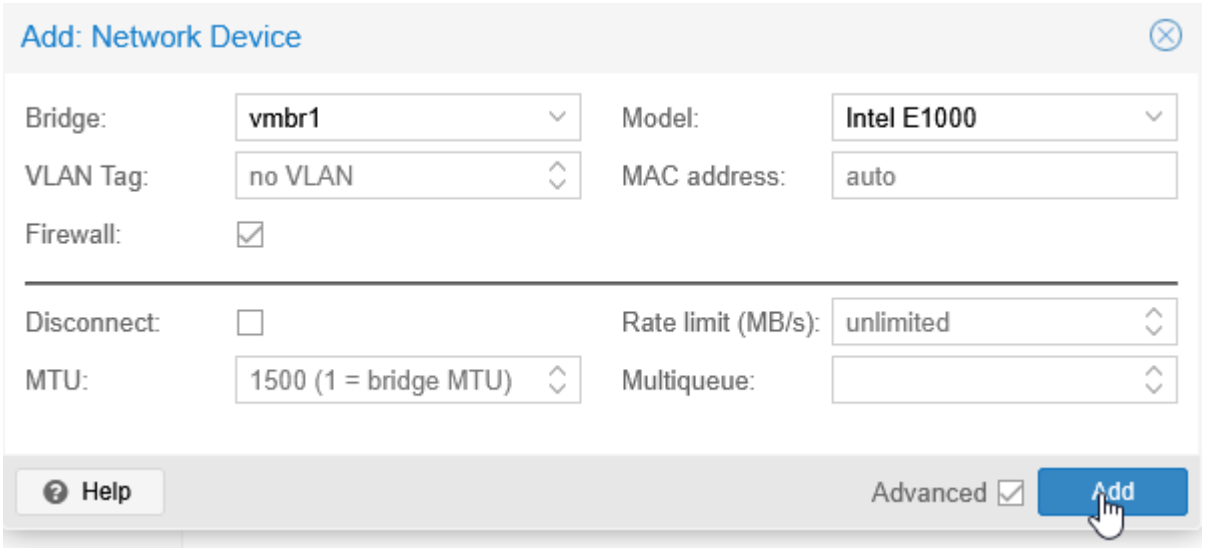
```
systemctl stop networking.service
```

```
auto lo
iface lo inet loopback

iface enp2s0f0 inet manual

auto vmbr0
iface vmbr0 inet static
        address 192.168.1.88/24
        gateway 192.168.1.1
        bridge-ports enp2s0f0
        bridge-stp off
        bridge-fd 0
        bridge-vlan-aware yes
        bridge-vids 2-4092

auto vmbr1
iface vmbr1 inet manual
        bridge-ports none
        bridge-stp off
        bridge-fd 0
        bridge-vlan-aware yes
        bridge-vids 10 20 30 50 99

iface enp2s0f1 inet manual

source /etc/network/interfaces.d/*
```

```
systemctl start networking.service
```

Ajout de l'interface virtuelle sur la vm pfsense pour l'assigner en temps que LAN :
(L'interface vmbr1 servira uniquement a se connecter les autres VMs à pfSense, comme un switch)





Configuration de l'adresse WAN en static

```
Enter an option: 2

Configure IPv4 address WAN interface via DHCP? (y/n) n
```

```
Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 192.168.1.50

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24
```

```
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1

Should this gateway be set as the default gateway? (y/n) y
```

```
Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on WAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

J'assigne la nouvelle interface LAN (em1), je décide de ne pas configurer les vlans maintenant mais plutôt avec l'interface WEB.

```
 1) Assign Interfaces
 2) Set interface(s) IP address
 3) Reset webConfigurator password
 4) Reset to factory defaults
 5) Reboot system
 6) Halt system
 7) Ping host
 8) Shell

Enter an option: 1


Valid interfaces are:

em0     bc:24:11:fa:7d:e3   (up) In
em1     bc:24:11:36:3c:cb (down) In

Do VLANs need to be set up first?
If VLANs will not be used, or only
say no here and use the webConfigur

Should VLANs be set up now [y|n]? n
```

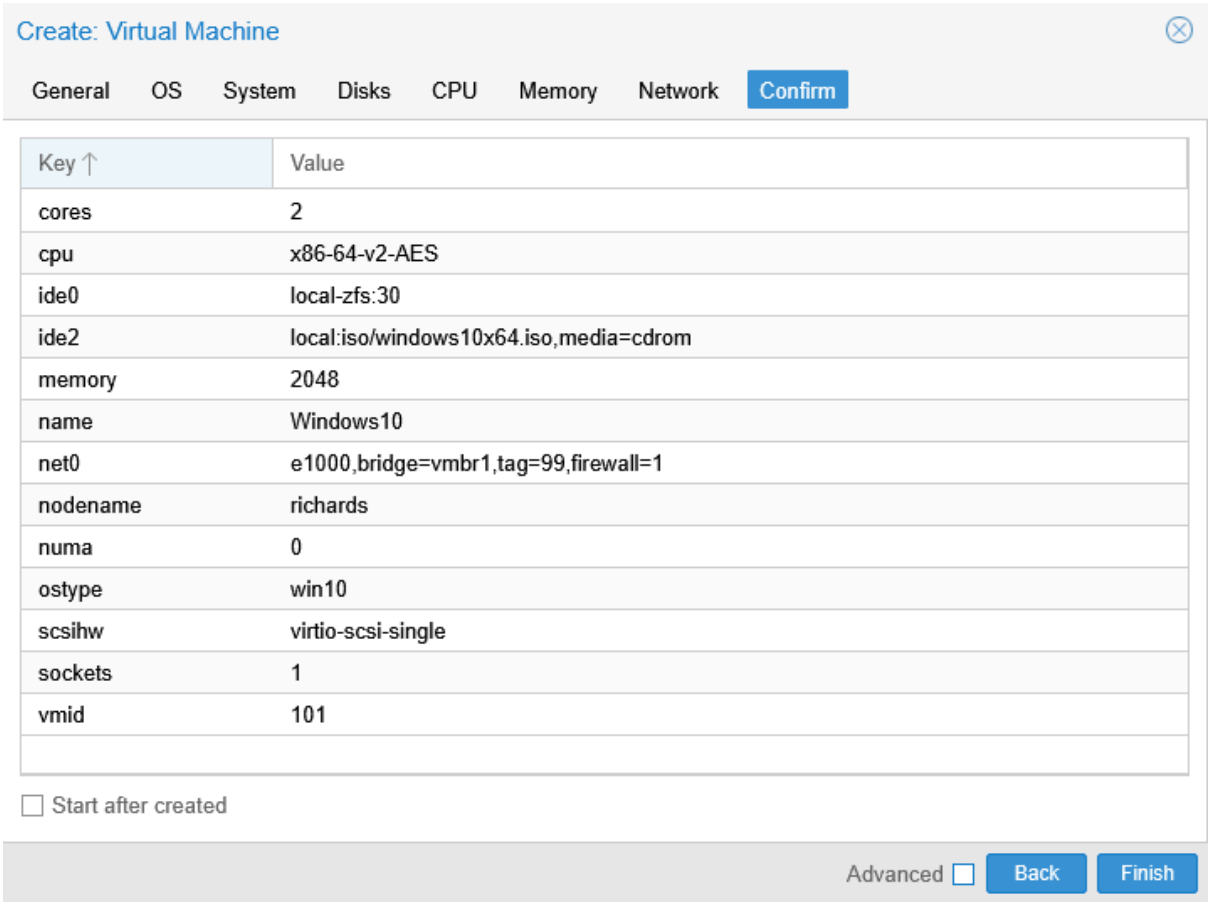
```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1
```

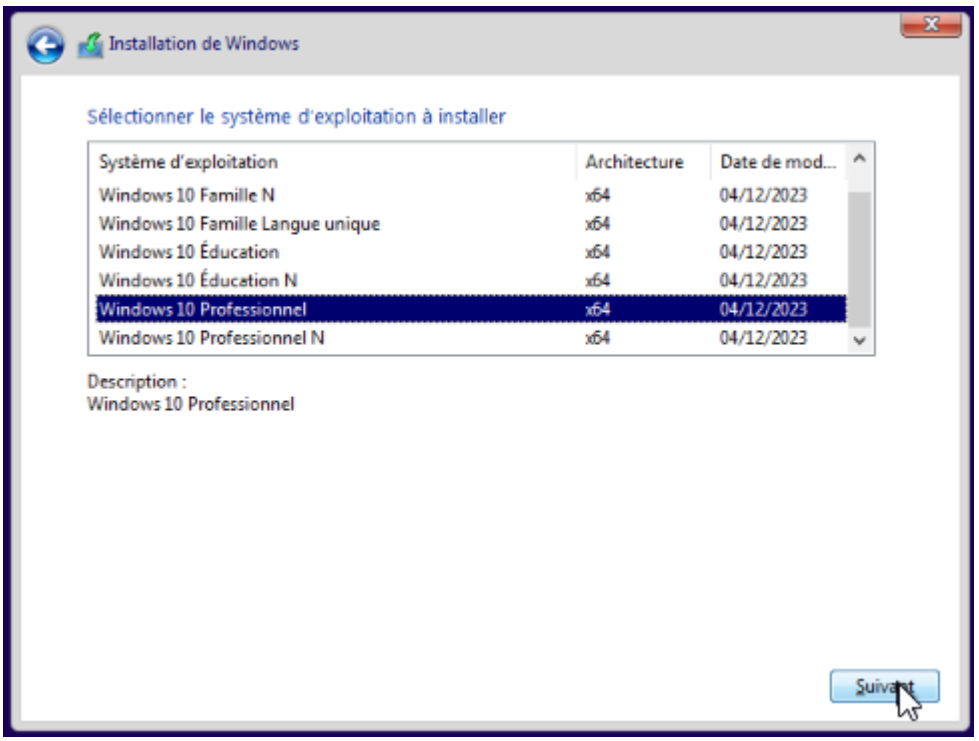
```
The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed [y|n]? y
```

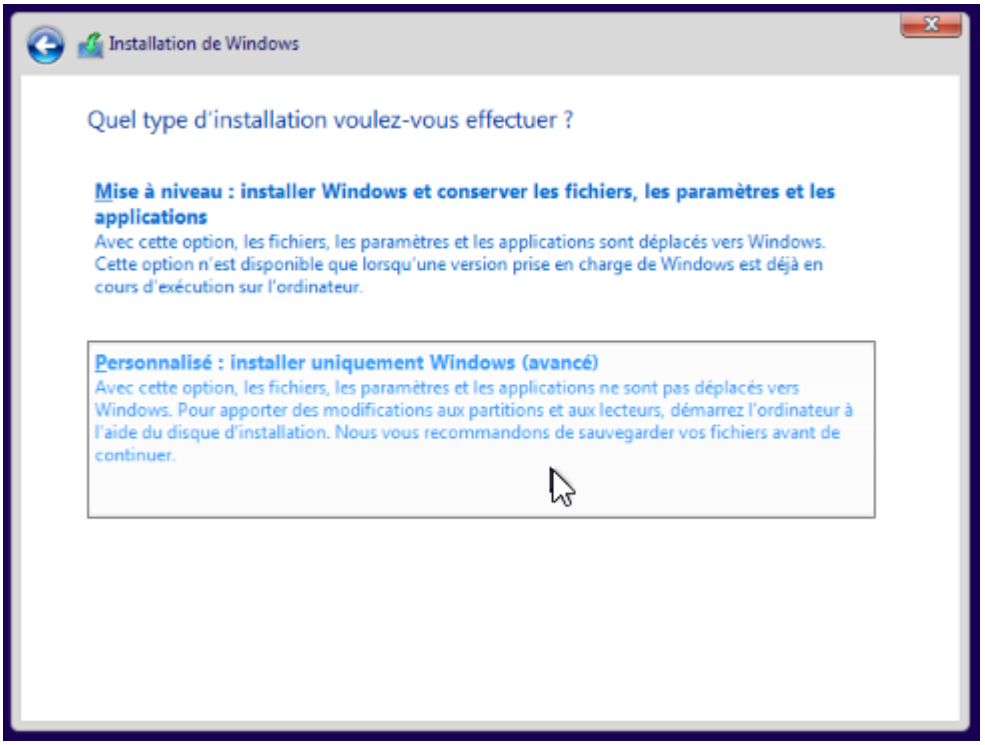
```
Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.99.30

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 27

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

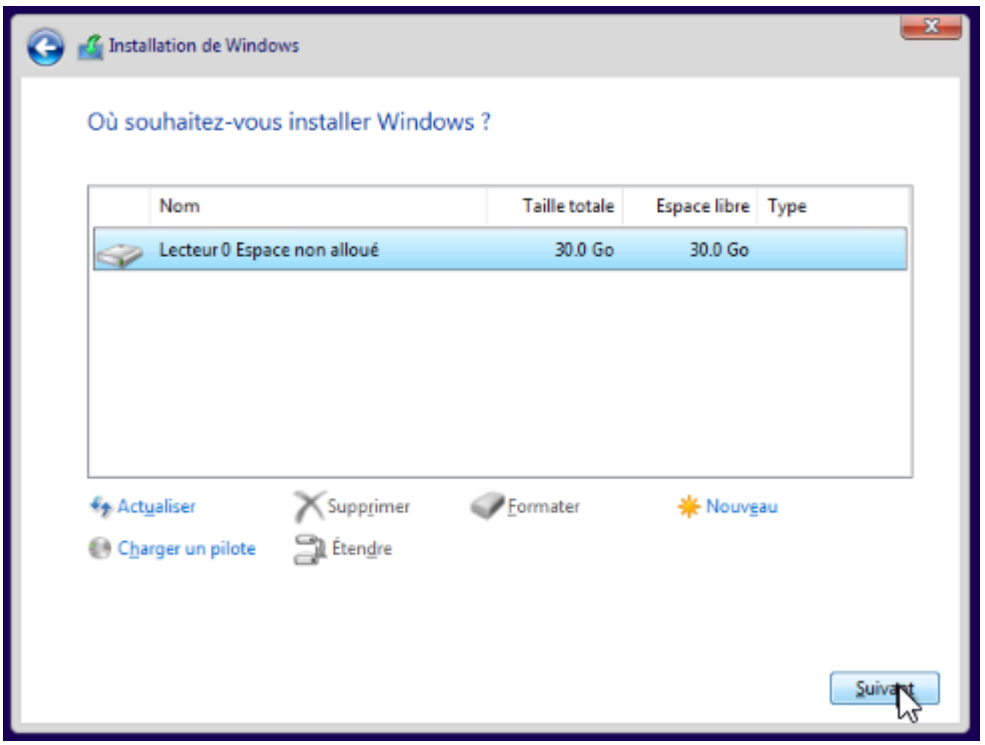
Je ne configure pas encore le DHCP car, dans mon cas, pfSense fera le relais avec mon windows server.

J'en profite pour créer une nouvelle VM Windows 10 pour avoir accès à l'interface WEB de pfSense :

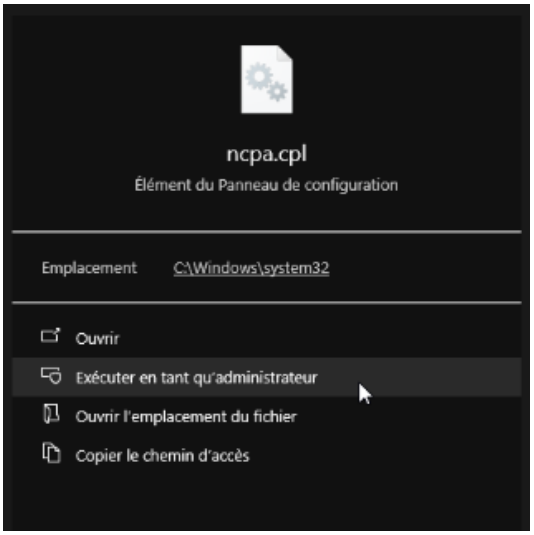


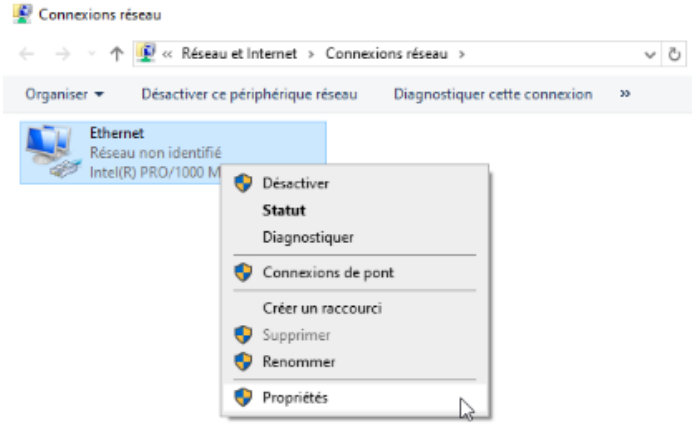

Installation de Windows
Sélectionner le système d'exploitation à installer
Système d'exploitation
Architecture
Date de mod...
Windows 10 Famille N
x64
04/12/2023
Windows 10 Famille Langue unique
x64
04/12/2023
Windows 10 Éducation
x64
04/12/2023
Windows 10 Éducation N
x64
04/12/2023
Windows 10 Professionnel
x64
04/12/2023
Windows 10 Professionnel N
x64
04/12/2023
Description :
Windows 10 Professionnel
Suivant

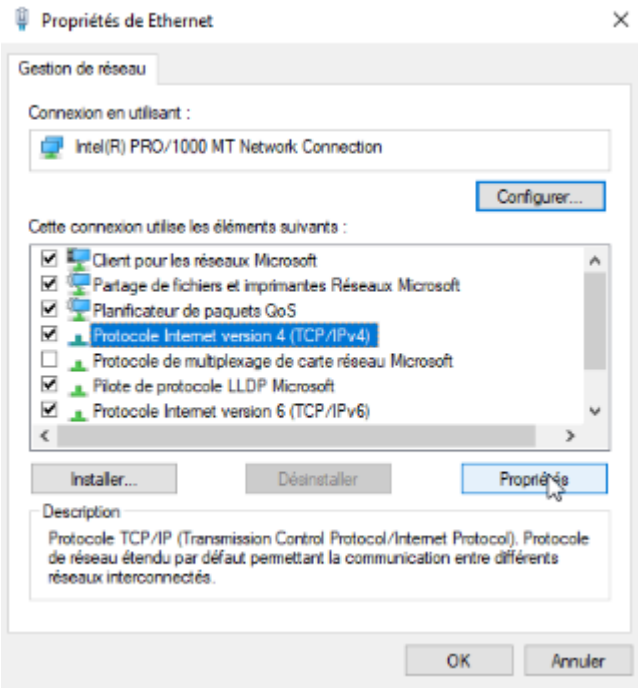

Installation de Windows
Quel type d'installation voulez-vous effectuer ?
Mise à niveau : installer Windows et conserver les fichiers, les paramètres et les applications
Avec cette option, les fichiers, les paramètres et les applications sont déplacés vers Windows. Cette option n'est disponible que lorsqu'une version prise en charge de Windows est déjà en cours d'exécution sur l'ordinateur.
Personnalisé : installer uniquement Windows (avancé)
Avec cette option, les fichiers, les paramètres et les applications ne sont pas déplacés vers Windows. Pour apporter des modifications aux partitions et aux lecteurs, démarrez l'ordinateur à l'aide du disque d'installation. Nous vous recommandons de sauvegarder vos fichiers avant de continuer.

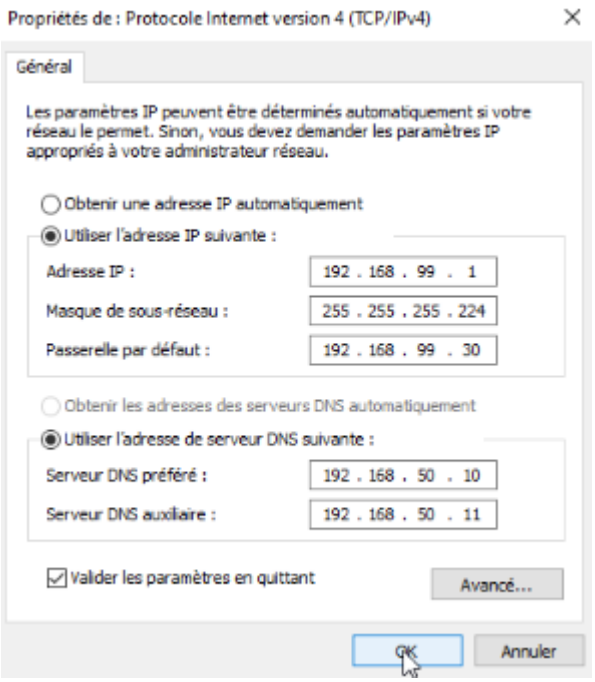


Création d'un compte local, puis Assignation d'une ip statique :

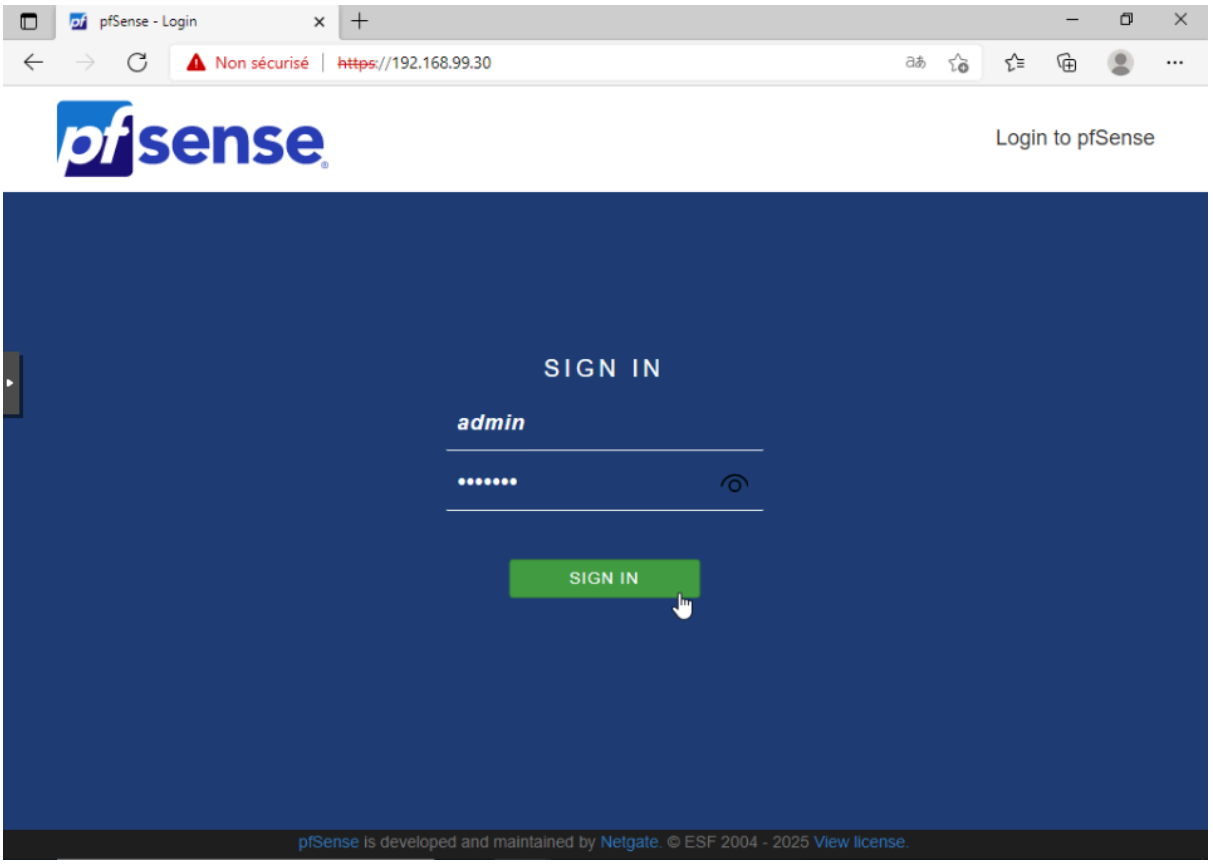


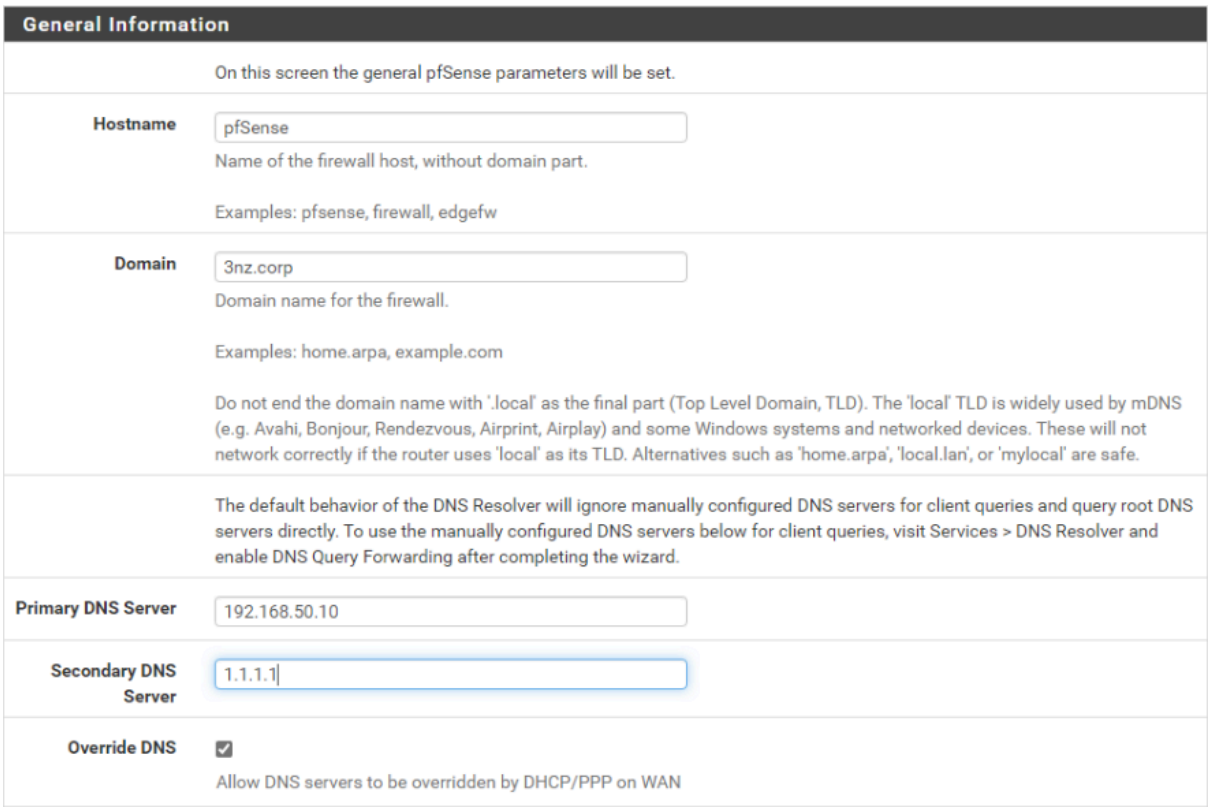


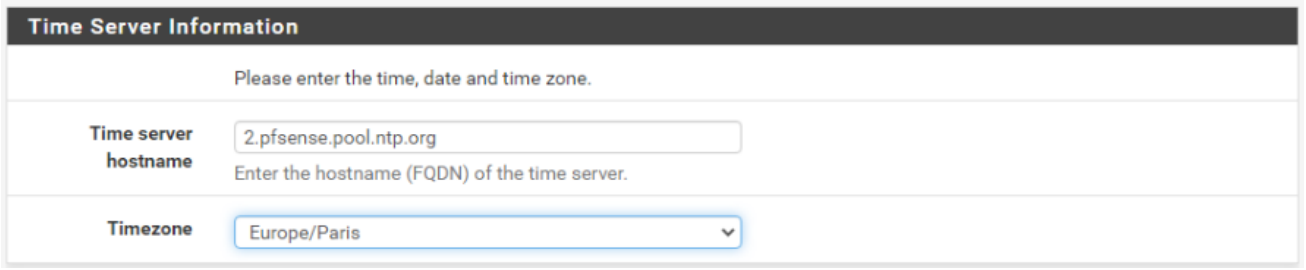

Propriétés de Ethernet
Gestion de réseau
Connexion en utilisant :
Intel(R) PRO/1000 MT Network Connection
Configurer...
Cette connexion utilise les éléments suivants :
Client pour les réseaux Microsoft
Partage de fichiers et imprimantes Réseaux Microsoft
Planificateur de paquets QoS
Protocole Internet version 4 (TCP/IPv4)
Protocole de multiplexage de carte réseau Microsoft
Pilote de protocole LLDP Microsoft
Protocole Internet version 6 (TCP/IPv6)
Installer...
Désinstaller
Propriétés
Description
Protocole TCP/IP (Transmission Control Protocol/Internet Protocol). Protocole de réseau étendu par défaut permettant la communication entre différents réseaux interconnectés.
OK
Annuler


Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général
Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
Obtenir une adresse IP automatiquement
Utiliser l'adresse IP suivante :
Adresse IP : 192 . 168 . 99 . 1
Masque de sous-réseau : 255 . 255 . 255 . 224
Passerelle par défaut : 192 . 168 . 99 . 30
Obtenir les adresses des serveurs DNS automatiquement
Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré : 192 . 168 . 50 . 10
Serveur DNS auxiliaire : 192 . 168 . 50 . 11
Valider les paramètres en quittant
Avancé...
OK
Annuler

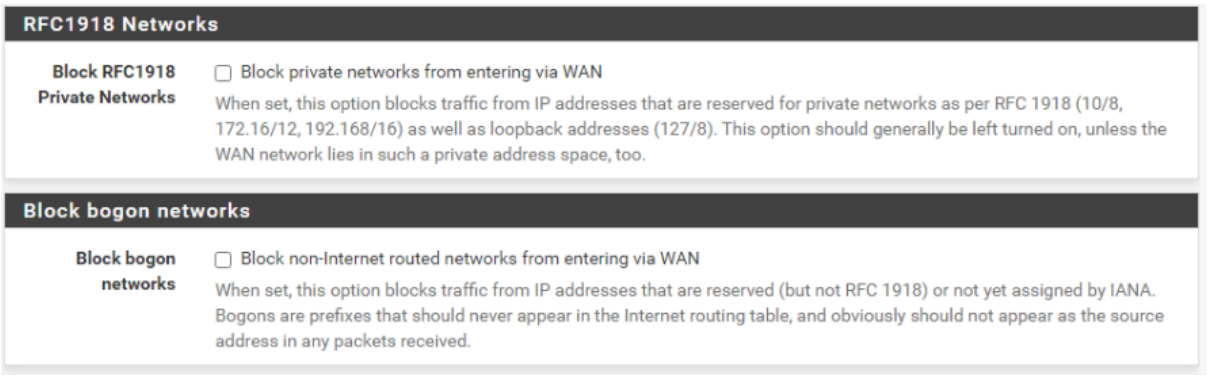
Accès à l'interface web de pfsense via le login par défaut :
admin - pfsense

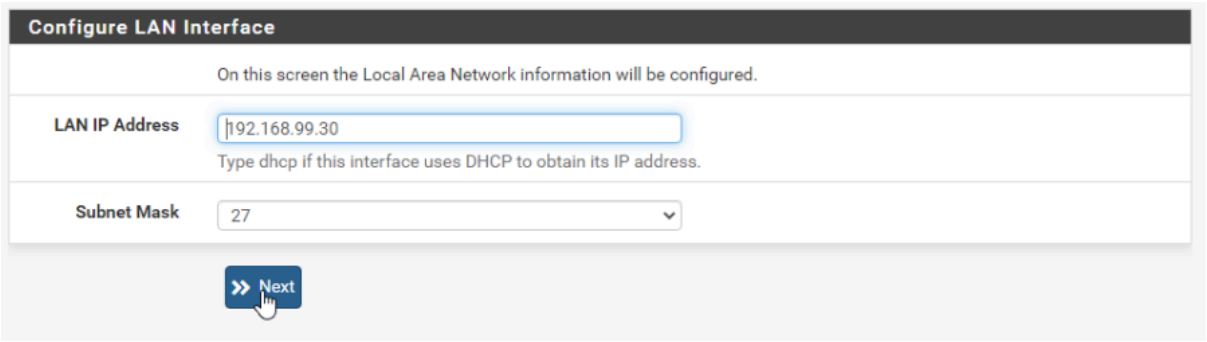




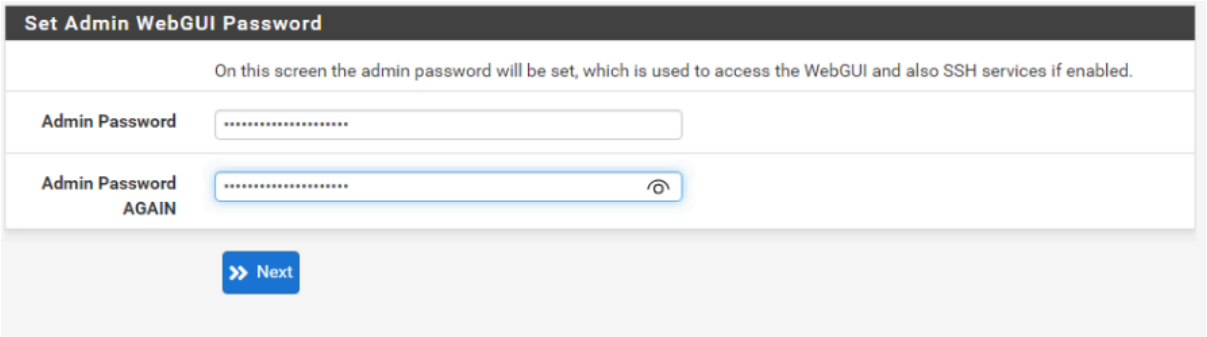


Etant donné que nous avons déjà configuré l'interface WAN je n'ai pas besoin de modifier les paramètres suivants, si ce n'est décocher ces deux règles de pare-feu, qui interdisent toutes ip de classes privés à communiquer avec mon routeur. Etant donné que je suis en lab, les cocher pourrais me bloquer lors de la configuration, je choisi donc, pour le moment d'enlever ces règles de pare-feu



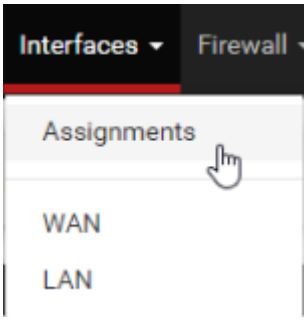


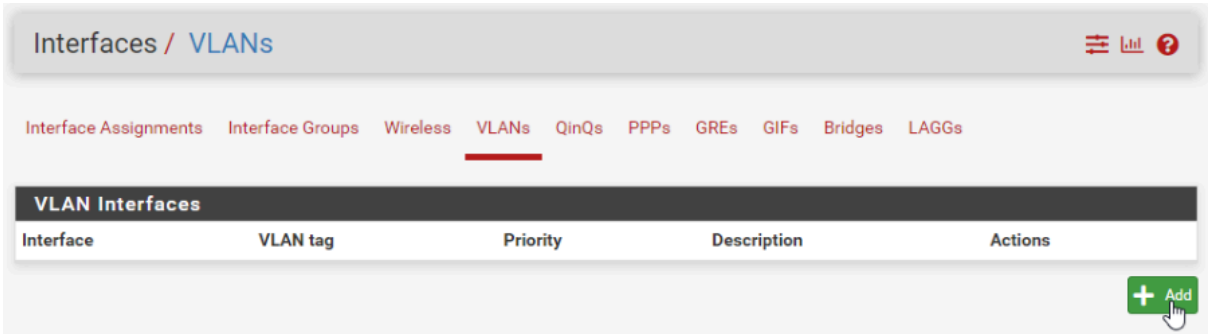
Modification du mot de passe avec les recommandations de l'ANSSI, au moins 12 caractères, inclure un mélange de lettres minuscules, majuscules, chiffres et symboles ou caractères spéciaux.

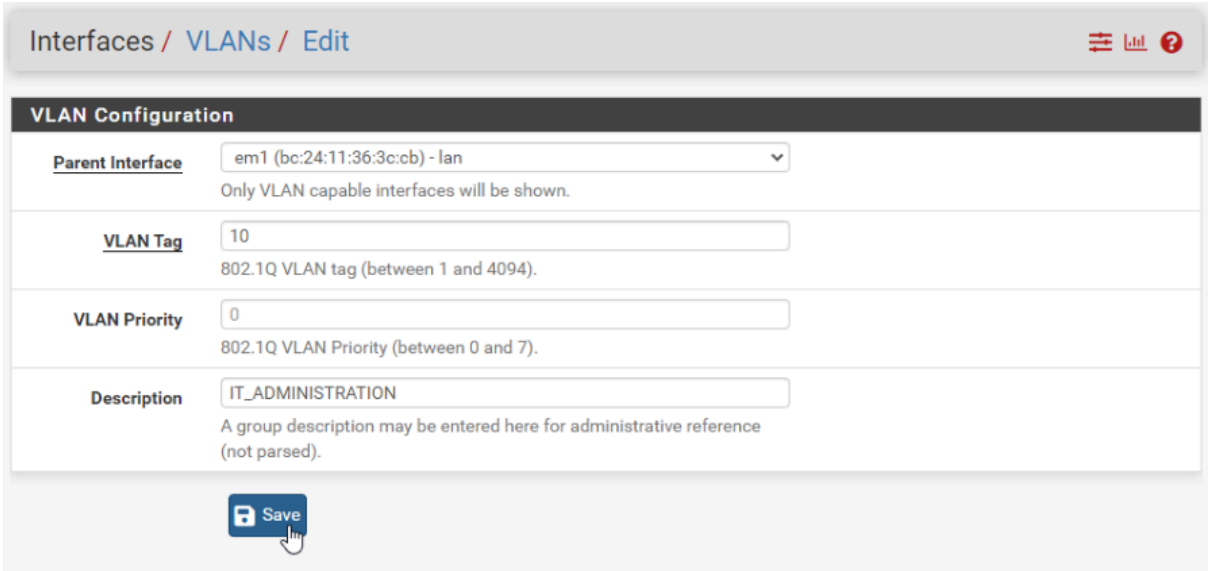


- Segmentation réseau (Création des 4 premiers VLANs)

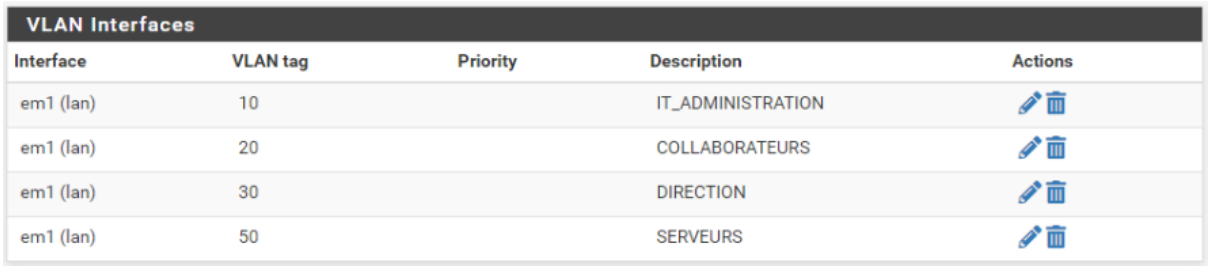
Ajout des vlans sur l'interface physique vmbr1, qui est maintenant le "LAN trunk virtuel"



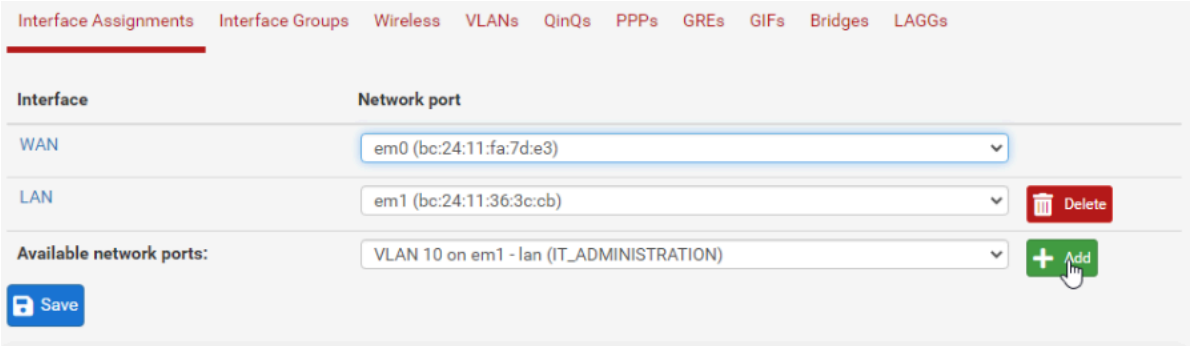


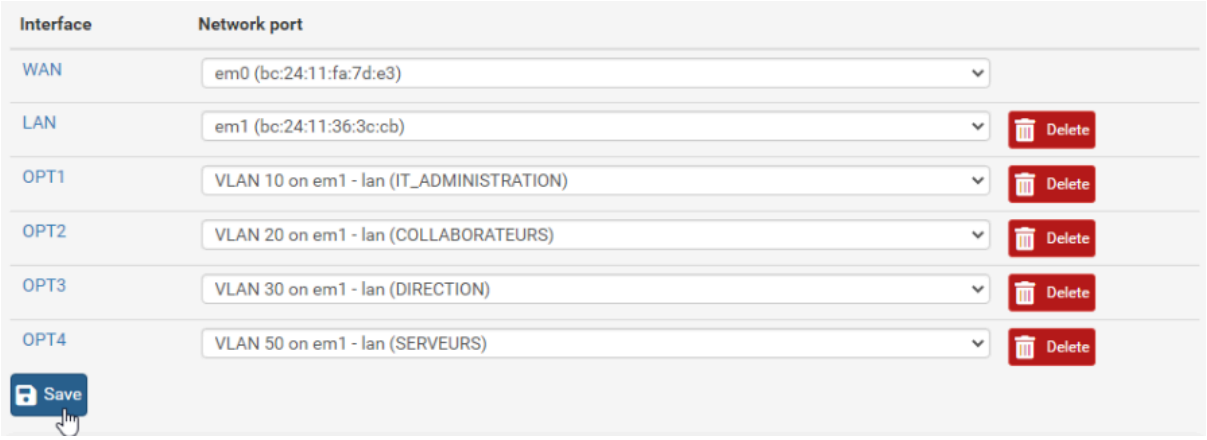


Je réitère pour les VLANs, 20,30 et 50.

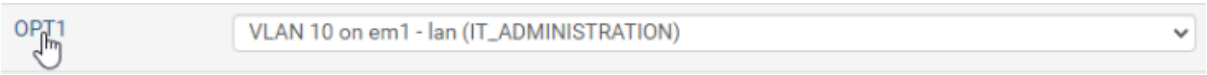


Maintenant on retourne dans l'onglet interface assignments et on ajoute les interfaces créé :



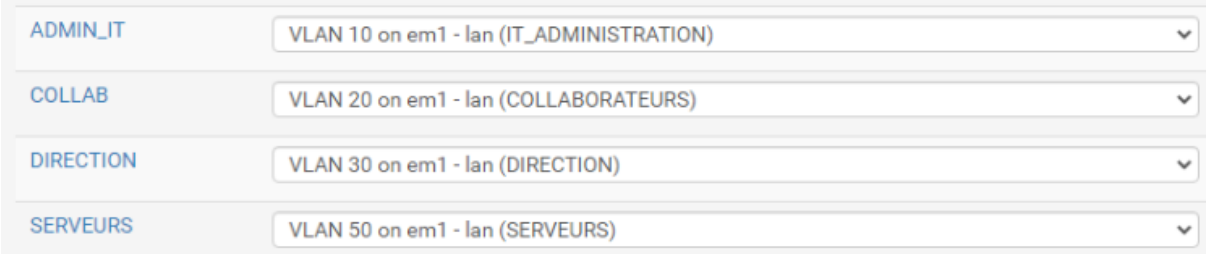


Ensuite, on va paramétrer ces interfaces et leur ajouter une ip qui sera alors, la passerelle des VLANs.



Activation de l'interface, description, IPv4 en statique et je renseigne l'adresse de l'interface.

Je réitère pour les autres VLANs.



- Configuration des règles de pare-feu et aliases par VLAN

Maintenant, nous allons paramétrer les règles pare-feu, mais avant ça, je créer des aliases pour simplifier la configuration :

Les IP Aliases :

Firewall Aliases IP

Name	Type	Values	Description	Actions
ALIAS_ALL_INTERNAL_NETWORKS	Network(s)	192.168.10.0/29, 192.168.20.0/28, 192.168.30.0/29, 192.168.50.0/27		
ALIAS_DOMAIN_CONTROLLERS	Network(s)	192.168.50.10/27, 192.168.50.11/27		
HOST_AD_PRIMARY	Network(s)	192.168.50.10/27		
HOST_AD_SECONDARY	Network(s)	192.168.50.11		
HOST_GLPI_DB	Network(s)	192.168.50.30/27		
HOST_GLPI_WEB	Network(s)	192.168.50.3/27		
HOST_TRUENAS	Network(s)	192.168.50.2/27		
HOST_VEEAM	Network(s)	192.168.50.7/27		
LAN_PHYSIQUE	Network(s)	192.168.1.0/24		
NET_VLAN_COLLABORATEURS	Network(s)	192.168.20.0/28		
NET_VLAN_DIRECTION	Network(s)	192.168.30.0/29		
NET_VLAN_DSI	Network(s)	192.168.10.0/29		

Les ports aliases :

Firewall Aliases Ports

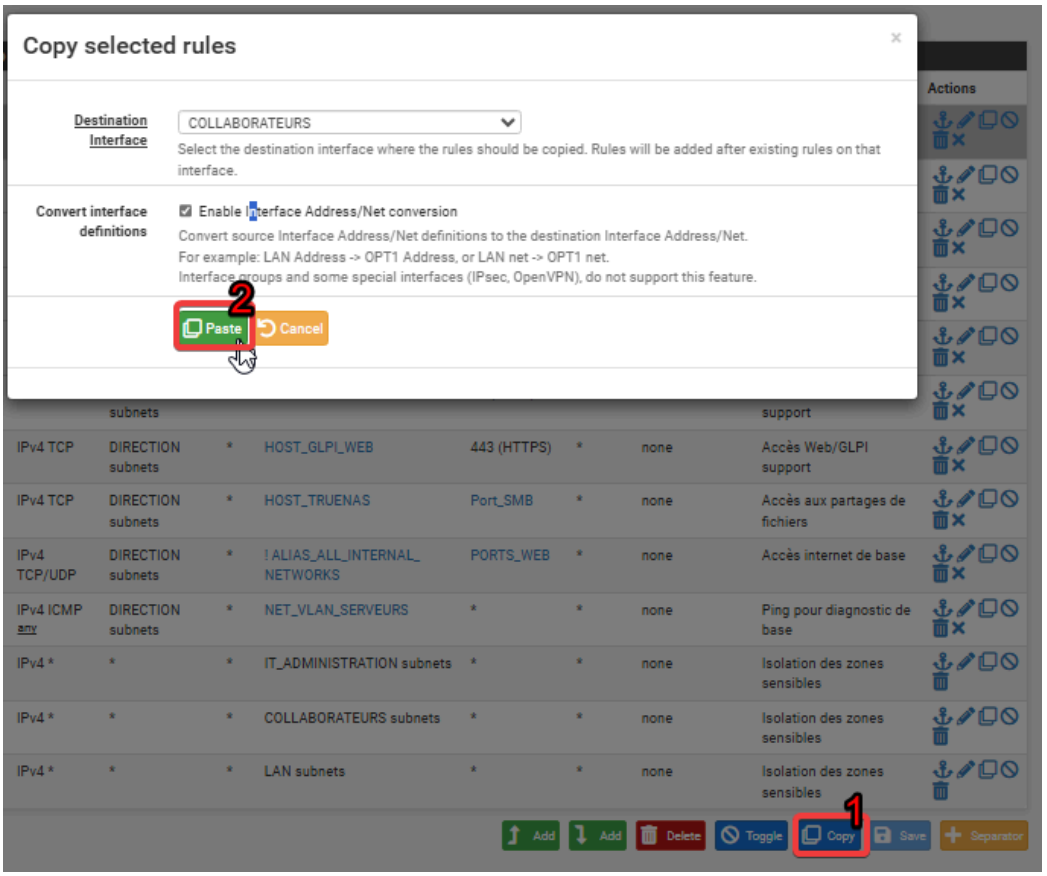
Name	Type	Values	Description	Actions
AD_GC_DFS	Port(s)	135, 389, 445, 3268:3269, 5722	Replication_AD_ GC_DFS	
PORTS_GLPI_DB	Port(s)	3306		
PORTS_GLPI_WEB	Port(s)	443		
PORTS_WEB	Port(s)	80, 443		
PORT_AD_CLIENT	Port(s)	53, 389, 636, 88, 445, 464, 3268, 3269, 135		
PORT_DHCP	Port(s)	67, 68		
PORT_DNS	Port(s)	53		
PORT_NTP	Port(s)	123		
Port_RDP	Port(s)	3389	Connexion Bureau à distance	
Port_SMB	Port(s)	445, 139, 137, 138	Partage réseau, DFS (AD/NAS)	
PORT_SSH	Port(s)	22		

Les règles firewall par VLANs
DIRECTION :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓ 0/0 B	IPv4 UDP	DIRECTION subnets	*	ALIAS_DOMAIN_CONTROLLERS	PORT_DHCP	*	none		DHCP relay vers AD	
☐	✓ 0/36 KiB	IPv4 TCP/UDP	DIRECTION subnets	*	ALIAS_DOMAIN_CONTROLLERS	PORT_DNS	*	none		DNS (résolution domaine)	
☐	✓ 0/42 KiB	IPv4 TCP/UDP	DIRECTION subnets	*	ALIAS_DOMAIN_CONTROLLERS	PORT_AD_CLIENT	*	none		Communication AD (auth, gpo)	
☐	✓ 0/0 B	IPv4 TCP	DIRECTION subnets	*	ALIAS_DOMAIN_CONTROLLERS	636 (LDAP/S)	*	none		LDAPS pour auth GPO etc.	
☐	✓ 0/296 B	IPv4 UDP	DIRECTION subnets	*	ALIAS_DOMAIN_CONTROLLERS	123 (NTP)	*	none		NTP	
☐	✓ 0/0 B	IPv4 TCP	DIRECTION subnets	*	HOST_GLPI_WEB	80 (HTTP)	*	none		Accès Web/GLPI support	
☐	✓ 0/59 KiB	IPv4 TCP	DIRECTION subnets	*	HOST_GLPI_WEB	443 (HTTPS)	*	none		Accès Web/GLPI support	
☐	✓ 0/0 B	IPv4 TCP	DIRECTION subnets	*	HOST_TRUENAS	Port_SMB	*	none		Accès aux partages de fichiers	
☐	✓ 0/2.85 MiB	IPv4 TCP/UDP	DIRECTION subnets	*	! ALIAS_ALL_INTERNAL_NETWORKS	PORTS_WEB	*	none		Accès internet de base	
☐	✓ 0/0 B	IPv4 ICMP any	DIRECTION subnets	*	NET_VLAN_SERVEURS	*	*	none		Ping pour diagnostic de base	
☐	✗ 0/0 B	IPv4 *	*	*	IT_ADMINISTRATION subnets	*	*	none		Isolation des zones sensibles	
☐	✗ 0/0 B	IPv4 *	*	*	COLLABORATEURS subnets	*	*	none		Isolation des zones sensibles	
☐	✗ 0/0 B	IPv4 *	*	*	LAN subnets	*	*	none		Isolation des zones sensibles	

COLLAB :
Je sélectionne les règles en communs, je clique sur Copy (1) puis je colle en cochant la conversion des interfaces :



COLLABORATEURS :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 UDP	COLLABORATEURS subnets	*	ALIAS_DOMAIN_ CONTROLLERS	PORT_DHCP	*	none		DHCP relay vers AD	
☐	✓	0/21 KiB	IPv4 TCP/UDP	COLLABORATEURS subnets	*	ALIAS_DOMAIN_ CONTROLLERS	PORT_DNS	*	none		DNS (résolution domaine)	
☐	✓	0/38 KiB	IPv4 TCP/UDP	COLLABORATEURS subnets	*	ALIAS_DOMAIN_ CONTROLLERS	PORT_AD_ CLIENT	*	none		Communication AD (auth, gpo)	
☐	✓	0/0 B	IPv4 TCP	COLLABORATEURS subnets	*	ALIAS_DOMAIN_ CONTROLLERS	636 (LDAP/S)	*	none		LDAPS pour auth GPO etc.	
☐	✓	0/296 B	IPv4 UDP	COLLABORATEURS subnets	*	ALIAS_DOMAIN_ CONTROLLERS	123 (NTP)	*	none		NTP	
☐	✓	0/0 B	IPv4 TCP	COLLABORATEURS subnets	*	HOST_GLPI_WEB	80 (HTTP)	*	none		Accès Web/GLPI support	
☐	✓	4/371 KiB	IPv4 TCP	COLLABORATEURS subnets	*	HOST_GLPI_WEB	443 (HTTPS)	*	none		Accès Web/GLPI support	
☐	✓	0/0 B	IPv4 TCP	COLLABORATEURS subnets	*	HOST_TRUENAS	Port_SMB	*	none		Accès aux partages de fichiers	
☐	✓	1/1.29 MiB	IPv4 TCP/UDP	COLLABORATEURS subnets	*	! ALIAS_ALL_INTERNAL_ NETWORKS	PORTS_WEB	*	none		Accès internet de base	
☐	✓	0/0 B	IPv4 ICMP any	COLLABORATEURS subnets	*	NET_VLAN_SERVEURS	*	*	none		Ping pour diagnostic de base	
☐	✗	0/0 B	IPv4 *	*	*	IT_ADMINISTRATION subnets	*	*	none		Isolation des zones sensibles	
☐	✗	0/0 B	IPv4 *	*	*	COLLABORATEURS subnets	*	*	none		Isolation des zones sensibles	
☐	✗	0/0 B	IPv4 *	*	*	LAN subnets	*	*	none		Isolation des zones sensibles	

SERVEURS :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 ICMP any	NET_VLAN_DSI	*	NET_VLAN_SERVEURS	*	*	none		Ping depuis DSI vers Serveurs	
☐	✓	0/0 B	IPv4 TCP	NET_VLAN_DSI	*	NET_VLAN_SERVEURS	PORT_SSH	*	none		Accès management DSI aux serveurs	
☐	✓	0/229 B	IPv4 *	ALIAS_DOMAIN_ CONTROLLERS	*	ALIAS_DOMAIN_ CONTROLLERS	*	*	none		Communication et réplication AD	
☐	✓	0/0 B	IPv4 TCP	HOST_GLPI_WEB	*	HOST_GLPI_DB	PORTS_ GLPI_DB	*	none		GLPI WEB vers GLPI DB	
☐	✓	0/0 B	IPv4 TCP	HOST_GLPI_WEB	*	ALIAS_DOMAIN_ CONTROLLERS	389 (LDAP)	*	none		GLPI VERS AD pour LDAP	
☐	✓	0/0 B	IPv4 TCP	HOST_GLPI_WEB	*	ALIAS_DOMAIN_ CONTROLLERS	636 (LDAP/S)	*	none		GLPI VERS AD pour LDAP	
☐	✓	0/0 B	IPv4 TCP/UDP	HOST_VEEAM	*	ALIAS_DOMAIN_ CONTROLLERS	*	*	none		Veeam vers serveurs pour backup	
☐	✓	0/0 B	IPv4 TCP	HOST_VEEAM	*	HOST_TRUENAS	Port_SMB	*	none		Veeam vers TrueNAS pour stockage backups	
☐	✓	0/0 B	IPv4 TCP/UDP	NET_VLAN_SERVEURS	*	ALIAS_DOMAIN_ CONTROLLERS	PORT_DNS	*	none		Serveurs vers DNS internes	
☐	✓	0/0 B	IPv4 UDP	NET_VLAN_SERVEURS	*	ALIAS_DOMAIN_ CONTROLLERS	123 (NTP)	*	none		Synchronisation NTP des serveurs	
☐	✓	0/0 B	IPv4 TCP/UDP	NET_VLAN_SERVEURS	*	*	PORTS_WEB	*	none		Accès web pour maj	

ADMIN_IT :

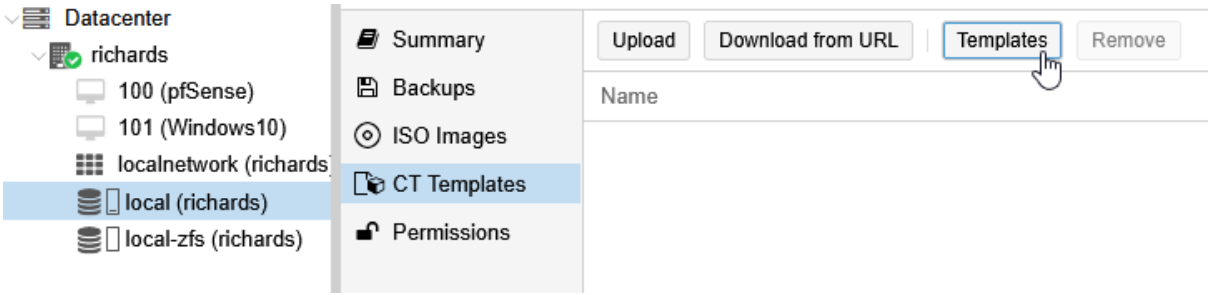
Rules (Drag to Change Order)

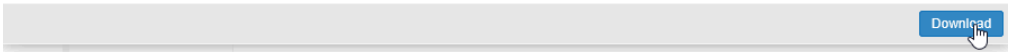
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	0/0 B	IPv4 UDP	ADMIN_IT subnets	*	ALIAS_DOMAIN_ CONTROLLERS	PORT_DHCP	*	none		DHCP relay vers AD	
☐	✓	0/1 KiB	IPv4 TCP/UDP	ADMIN_IT subnets	*	ALIAS_DOMAIN_ CONTROLLERS	PORT_DNS	*	none		DNS (résolution domaine)	
☐	✓	0/22 KiB	IPv4 TCP/UDP	ADMIN_IT subnets	*	ALIAS_DOMAIN_ CONTROLLERS	PORT_AD_ CLIENT	*	none		Communication AD (auth, gpo)	
☐	✓	0/0 B	IPv4 TCP	ADMIN_IT subnets	*	ALIAS_DOMAIN_ CONTROLLERS	636 (LDAP/S)	*	none		LDAPS pour auth GPO etc.	
☐	✓	0/6 KiB	IPv4 *	NET_VLAN_ DSI	*	ALIAS_ALL_INTERNAL_ NETWORKS	*	*	none		Accès complet de la DSI aux autres VLANs	
☐	✓	0/0 B	IPv4 TCP	NET_VLAN_ DSI	*	! ALIAS_ALL_INTERNAL_ NETWORKS	*	*	none		Accès internet non restreint pour la dsi	

- Accès distant sécurisé (Tunnel WireGuard et DynDNS OVH)

Création d’un tunnel VPN via WireGuard, indépendant de l’infra 3nz.corp :

Téléchargement de la container template debian 12 :





Création du CT :

Key	Value
cores	1
features	nesting=1
hostname	WireGuardLAN
memory	512
nameserver	1.1.1.1
net0	name=eth0,bridge=vmbr0,firewall=1,ip=192.168.1.99/24,gw=192.168.1.1
nodename	richards
ostemplate	local:vztmpl/debian-12-standard_12.7-1_amd64.tar.zst
pool	
rootfs	local-zfs:8
searchdomain	192.168.1.1
ssh-public-keys	
swap	512
unprivileged	1

MàJ des paquets disponible, téléchargements et installation des màj des paquets présents dans le système :

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

Installation de wireguard :

```
apt install wireguard
```

Génération des clés publique et privés :

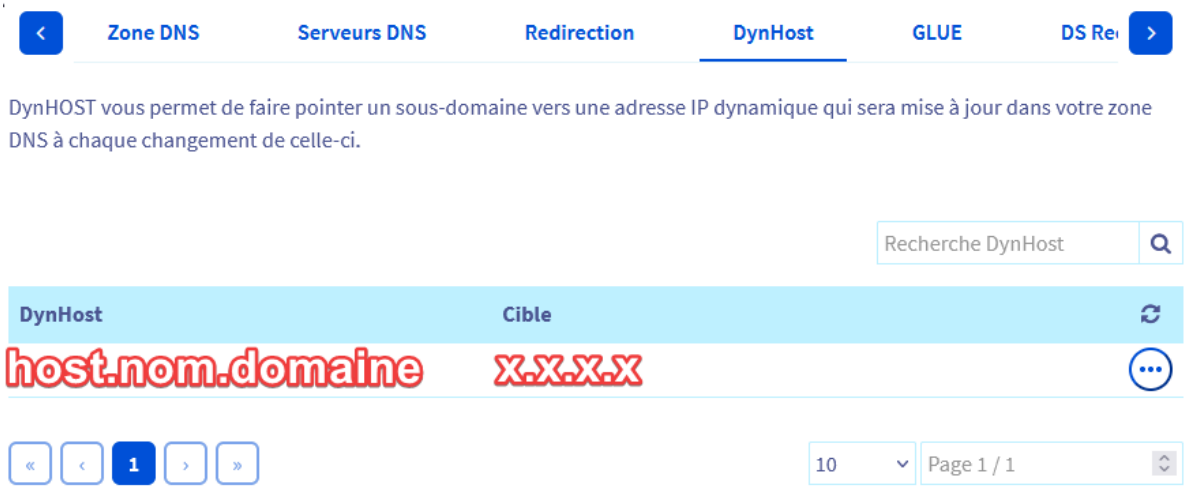
```
root@WireGuardLAN:~# wg genkey | tee /etc/wireguard/privatekey | wg pubkey > /etc/wireguard
/publickey
```

- Configuration DynDNS avec domaine OVHCloud (3nz.fr)

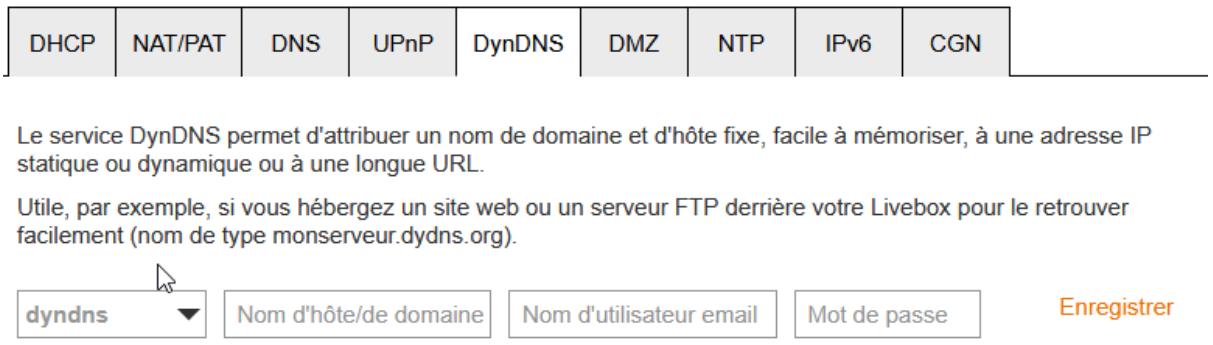
Pré-requis pour le tunnel :

IP Fixe ou DynDNS

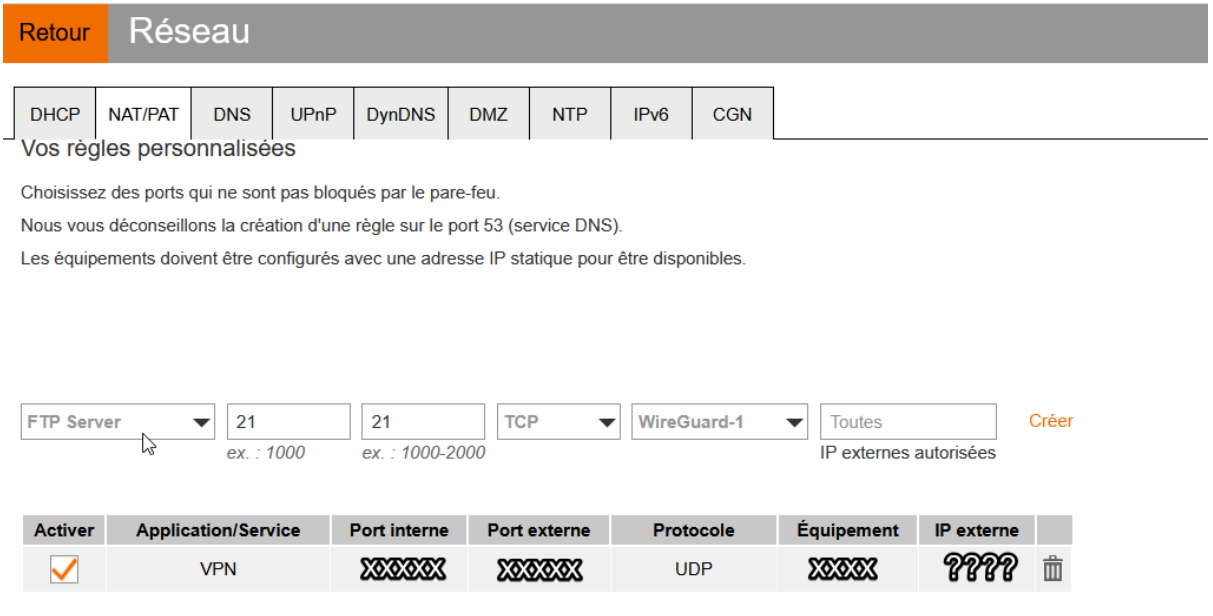
J'ai donc décidé de prendre un domaine chez OVHCloud, 3nz.fr.



Depuis mon routeur FAI, je renseigne dans la partie paramètre réseau, l'accès à un DynDNS :



et sur l'interface firewall de mon FAI, je fait la redirection de port sur l'équipement qui héberge le serveur wireguard :



modification des fichiers de conf :
SERVEUR :

```
[Interface]
Address = 10.0.0.1/24
MTU = 1380
SaveConfig = true
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -A FORWARD -o %i -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -D FORWARD -o %i -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
ListenPort =
PrivateKey =

[Peer]
PublicKey =
AllowedIPs = 10.0.0.2/32
Endpoint =
```

UTILISATEUR :

```
[Interface]
Address = 10.0.0.2/24
DNS = 1.1.1.1
PrivateKey =
MTU = 1380

[Peer]
PublicKey =
AllowedIPs = 0.0.0.0/0
Endpoint =
PersistentKeepalive = 25
```

iptables n'étant pas installé sur le serveur, je l'installe :

```
root@WireGuardLAN:/etc/wireguard# apt install iptables
```

Je peux ping le serveur en 10.0.0.1/24 mais pas le réseau local, solution : activer le forwarding de paquet sur le serveur :

```
vim /etc/sysctl.conf
```

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Maintenant, j'ai donc accès à mon infra depuis l'extérieur.
Je décide de rajouter une sécurité en plus :

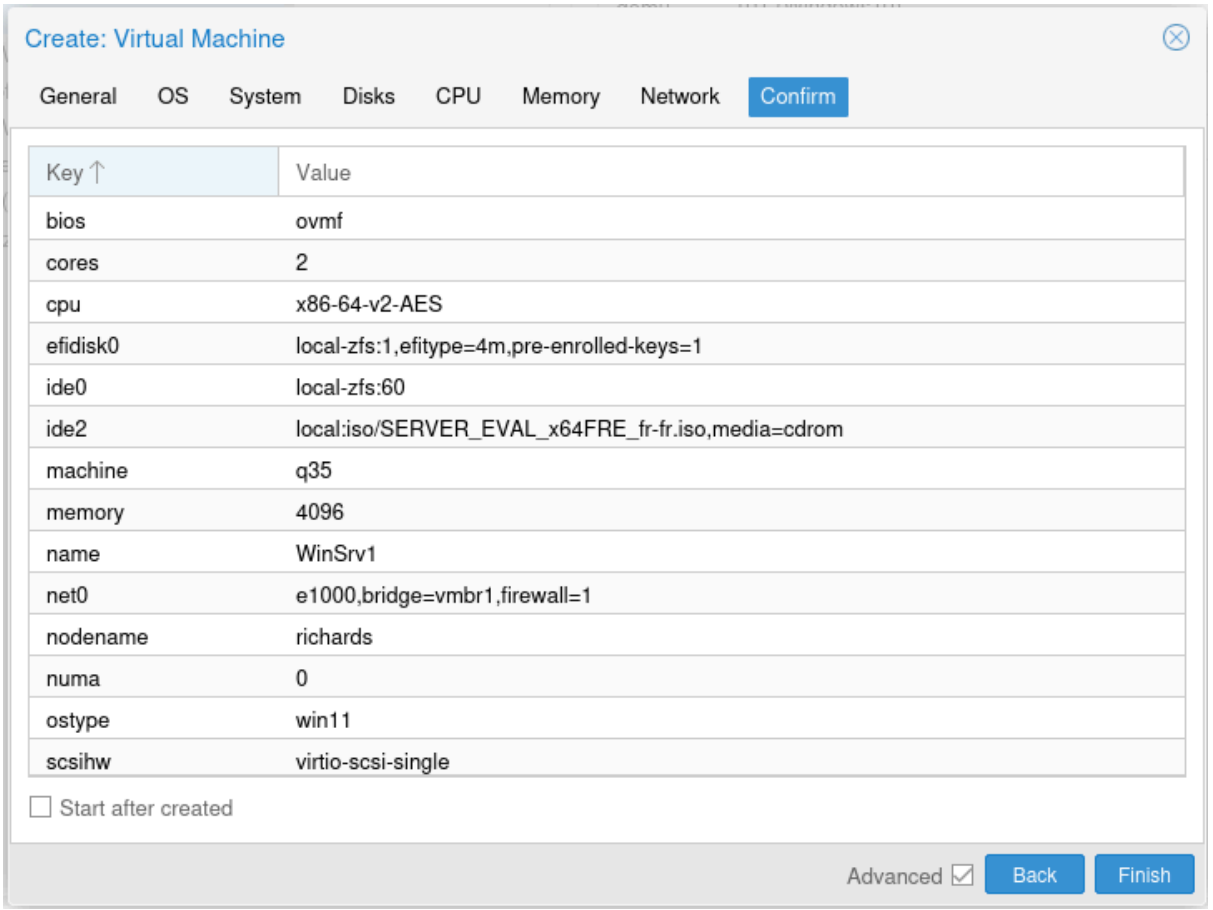
```
root@richards:/etc/pve/firewall# vim cluster.fw
```

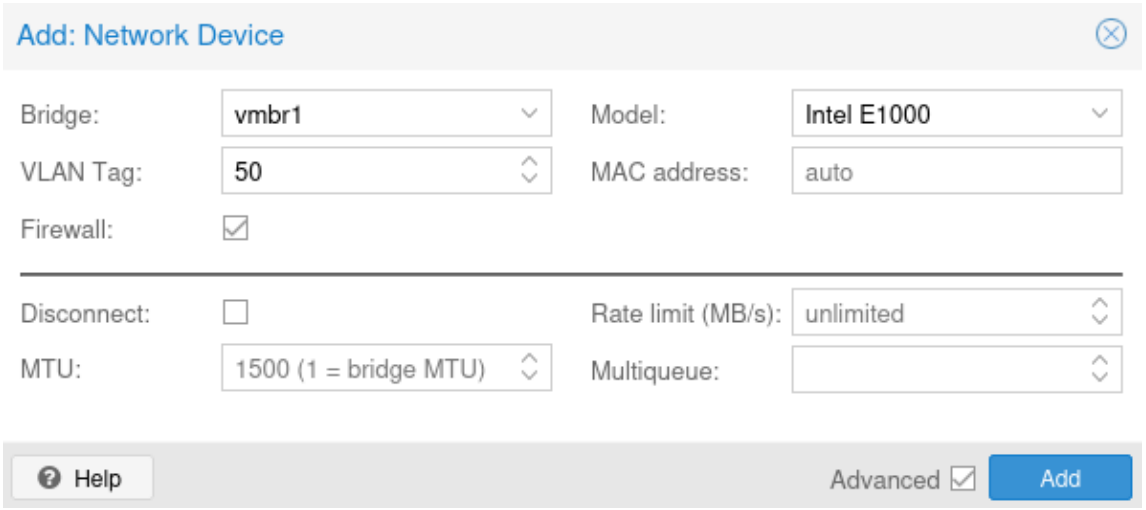
```
[OPTIONS]
enable: 1

[RULES]
IN ACCEPT -source 10.0.0.0/24 -dest_port 8006 -proto tcp
IN ACCEPT -source 192.168.1.0/24 -dest_port 8006 -proto tcp
IN DROP -dest_port 8006 -proto tcp
```

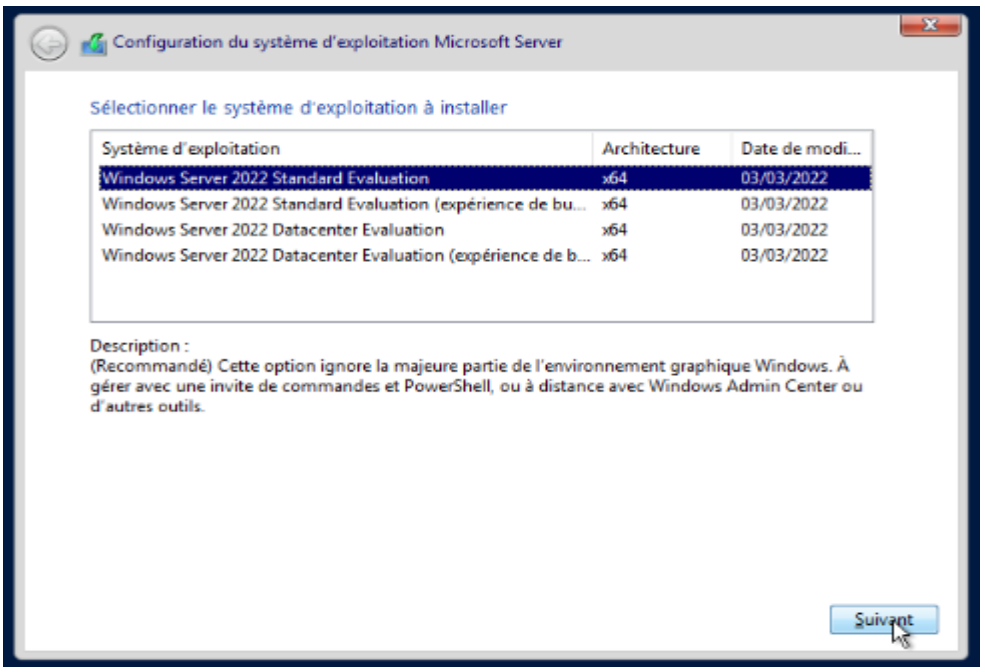
III. Services d'Annuaire et Réseau Windows

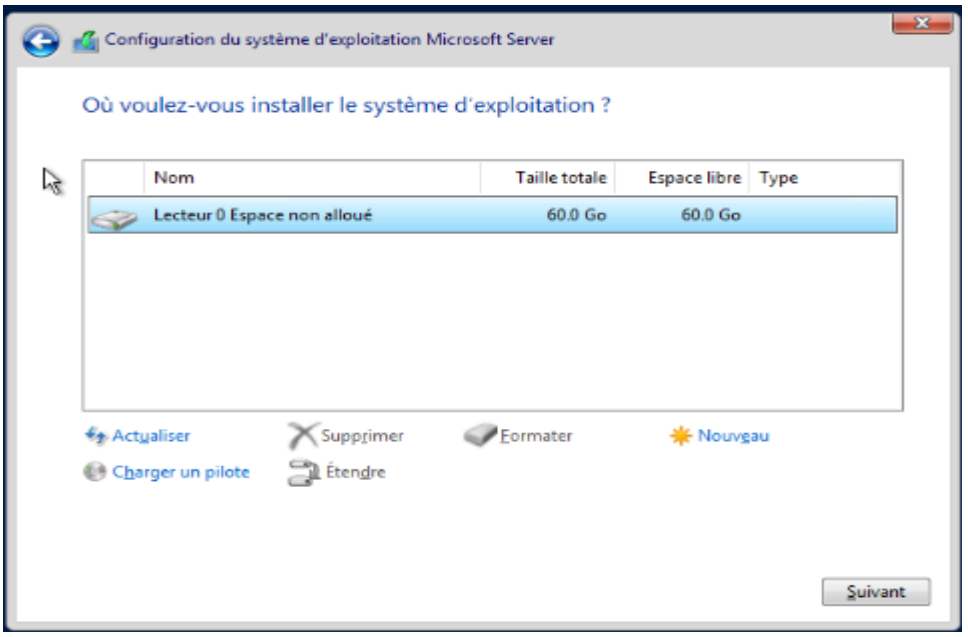
- Installation du contrôleur de domaine (AD DS 3nz.corp)

On passe maintenant à l'installation de la VM Windows Server AD DS :

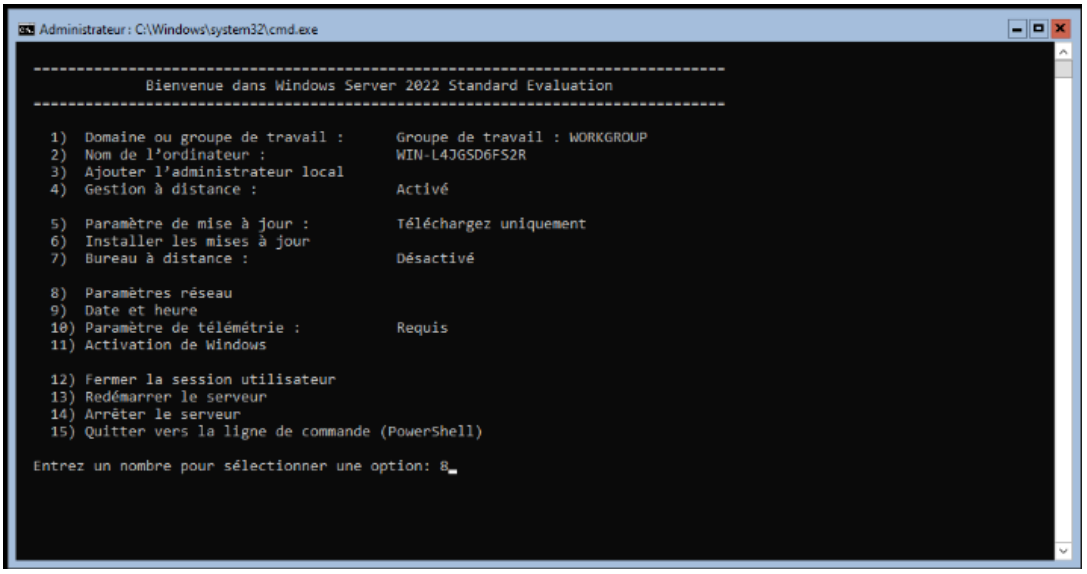


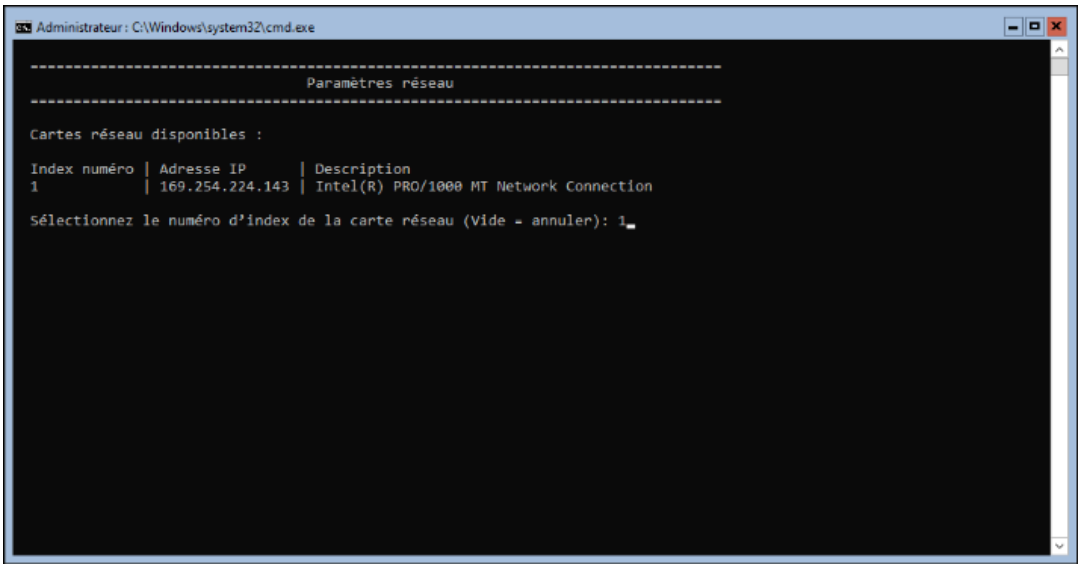


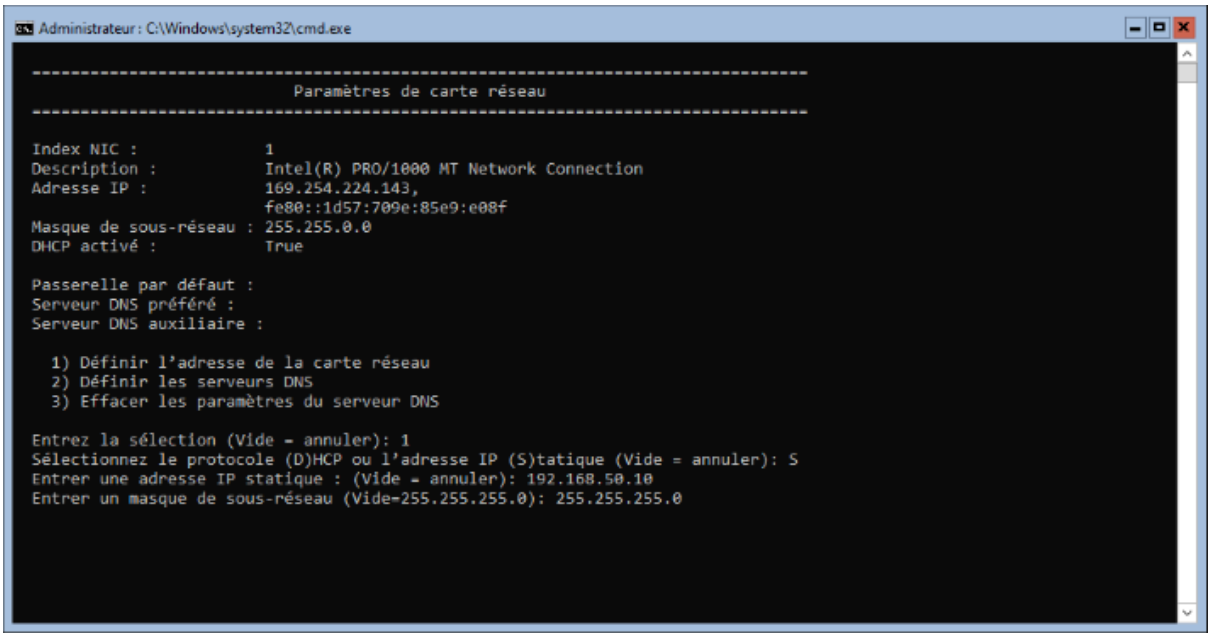




Je commence par paramétrer l'interface réseau :







Entrez la passerelle par défaut (Vide = annuler): 192.168.50.1

```
Affectation en cours de l'adresse IP statique à la carte réseau... Merci de patienter.
Le bail DHCP a été libéré avec succès.
L'adressage statique a été correctement activé. DHCP n'est pas activé pour cette carte réseau.
La passerelle a été correctement définie.
Définition de l'adresse de la carte réseau effectuée avec succès.
```

Attribution du dns :

```
   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_
```

```
Entrer un nouveau serveur DNS préféré (Vide = annuler): 127.0.0.1
```

- ## Création du domaine Active Directory (3nz.corp)

Maintenant dans SConfig, je tape la commande 15 -> PowerShell
Installation des features Windows : ADDS et DNS

```
AVERTISSEMENT : Pour lancer de nouveau l'outil de configuration du serveur, exécutez « SConfig »
PS C:\Users\Administrateur> Install-WindowsFeature -Name AD-Domain-Services, DNS -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Services AD DS, Serveur DNS, Gestion de s...
```

Avec la commande ADDSForest :

```
applet de commande Install-ADDSForest à la position 1 du pipeline de la commande
Fournissez des valeurs pour les paramètres suivants :
DomainName: 3nz.corp
SafeModeAdministratorPassword: *********************
Confirmer SafeModeAdministratorPassword: *********************

Le serveur cible sera configuré en tant que contrôleur de domaine et redémarré à la fin de cette opération.
Voulez-vous continuer en procédant à cette opération ?
[O] Oui  [T] Oui pour tout  [N] Non  [U] Non pour tout  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : O
```

```
Install-ADDSForest

  Validation d'environnement et d'entrée utilisateur
     Tous les tests ont réussi
     [ooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo]
  Installation d'une nouvelle forêt
     Démarrage
```

Vérification de l'installation de ADDomain

```
PS C:\Users\Administrateur> Get-ADDOMAIn


AllowedDNSSuffixes                 : {}
ChildDomains                       : {}
ComputersContainer                 : CN=Computers,DC=3nz,DC=corp
DeletedObjectsContainer            : CN=Deleted Objects,DC=3nz,DC=corp
DistinguishedName                  : DC=3nz,DC=corp
DNSRoot                            : 3nz.corp
DomainControllersContainer         : OU=Domain Controllers,DC=3nz,DC=corp
DomainMode                         : Windows2016Domain
DomainSID                          : S-1-5-21-4259766835-2419328018-3478043482
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=3nz,DC=corp
Forest                             : 3nz.corp
InfrastructureMaster               : WIN-L4JGSD6FS2R.3nz.corp
LastLogonReplicationInterval       :
LinkedGroupPolicyObjects           : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=3nz,DC=corp}
LostAndFoundContainer              : CN=LostAndFound,DC=3nz,DC=corp
ManagedBy                          :
Name                               : 3nz
NetBIOSName                        : 3NZ
ObjectClass                        : domainDNS
ObjectGUID                         : 89dfcd70-ac11-4417-ba17-3bb74b3a2fa5
ParentDomain                       :
PDCEmulator                        : WIN-L4JGSD6FS2R.3nz.corp
PublicKeyRequiredPasswordRolling   : True
QuotasContainer                    : CN=NTDS Quotas,DC=3nz,DC=corp
ReadOnlyReplicaDirectoryServers    : {}
ReplicaDirectoryServers            : {WIN-L4JGSD6FS2R.3nz.corp}
RIDMaster                          : WIN-L4JGSD6FS2R.3nz.corp
SubordinateReferences              : {DC=ForestDnsZones,DC=3nz,DC=corp, DC=DomainDnsZones,DC=3nz,DC=corp,
                                     CN=Configuration,DC=3nz,DC=corp}
SystemsContainer                   : CN=System,DC=3nz,DC=corp
UsersContainer                     : CN=Users,DC=3nz,DC=corp
```

Vérification de l'installation ADForest

```
PS C:\Users\Administrateur> Get-ADForest


ApplicationPartitions : {DC=ForestDnsZones,DC=3nz,DC=corp, DC=DomainDnsZones,DC=3nz,DC=corp}
CrossForestReferences : {}
DomainNamingMaster    : WIN-L4JGSD6FS2R.3nz.corp
Domains               : {3nz.corp}
ForestMode            : Windows2016Forest
GlobalCatalogs        : {WIN-L4JGSD6FS2R.3nz.corp}
Name                  : 3nz.corp
PartitionsContainer   : CN=Partitions,CN=Configuration,DC=3nz,DC=corp
RootDomain            : 3nz.corp
SchemaMaster          : WIN-L4JGSD6FS2R.3nz.corp
Sites                 : {Default-First-Site-Name}
SPNSuffixes           : {}
UPNSuffixes           : {}
```

Vérification de l'installation du DNS :

```
PS C:\Users\Administrateur> Get-DnsServerZone

ZoneName                          ZoneType        IsAutoCreated   IsDsIntegrated  IsReverseLookupZone  IsSigned
--------                          --------        -------------   --------------  -------------------  --------
_msdcs.3nz.corp                   Primary         False           True            False                False
0.in-addr.arpa                    Primary         True            False           True                 False
127.in-addr.arpa                  Primary         True            False           True                 False
255.in-addr.arpa                  Primary         True            False           True                 False
3nz.corp                          Primary         False           True            False                False


PS C:\Users\Administrateur> Resolve-DnsName localhost

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
localhost                                      AAAA   1200  Question   ::1
localhost                                      A      1200  Question   127.0.0.1
```

Ajoût du rôle DHCP :

```
PS C:\Users\Administrateur> Install-WindowsFeature -Name DHCP -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Serveur DHCP}
```

Autorisation du server dhcp dans l'ad

```
Add-DhcpServerInDC -DnsName WinSrv1.3nz.corp -IPAddress 192.168.50.10
```

- Configuration DHCP avec scopes par VLAN et DHCP Relay

Ajout des scopes DHCP :

```
Add-DhcpServerv4Scope
```

Ajout du scope pour le vlan ADMIN_IT :

```
applet de commande Add-DhcpServerv4Scope à la position 1 du pipeline de la commande
Fournissez des valeurs pour les paramètres suivants :
StartRange: 192.168.10.1
EndRange: 192.168.10.5
Name: ADMIN_IT
SubnetMask: 255.255.255.248
```

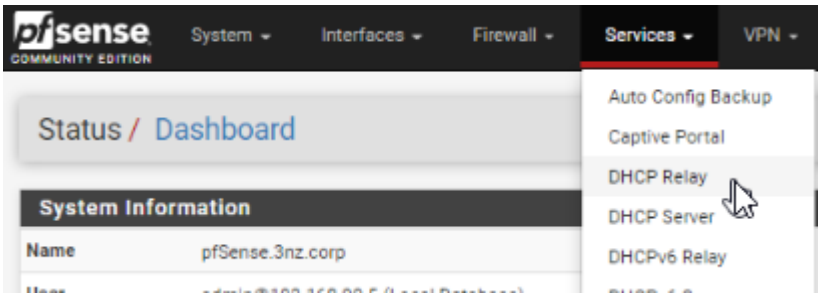
Pareil pour les autres et vérifications des scopes :

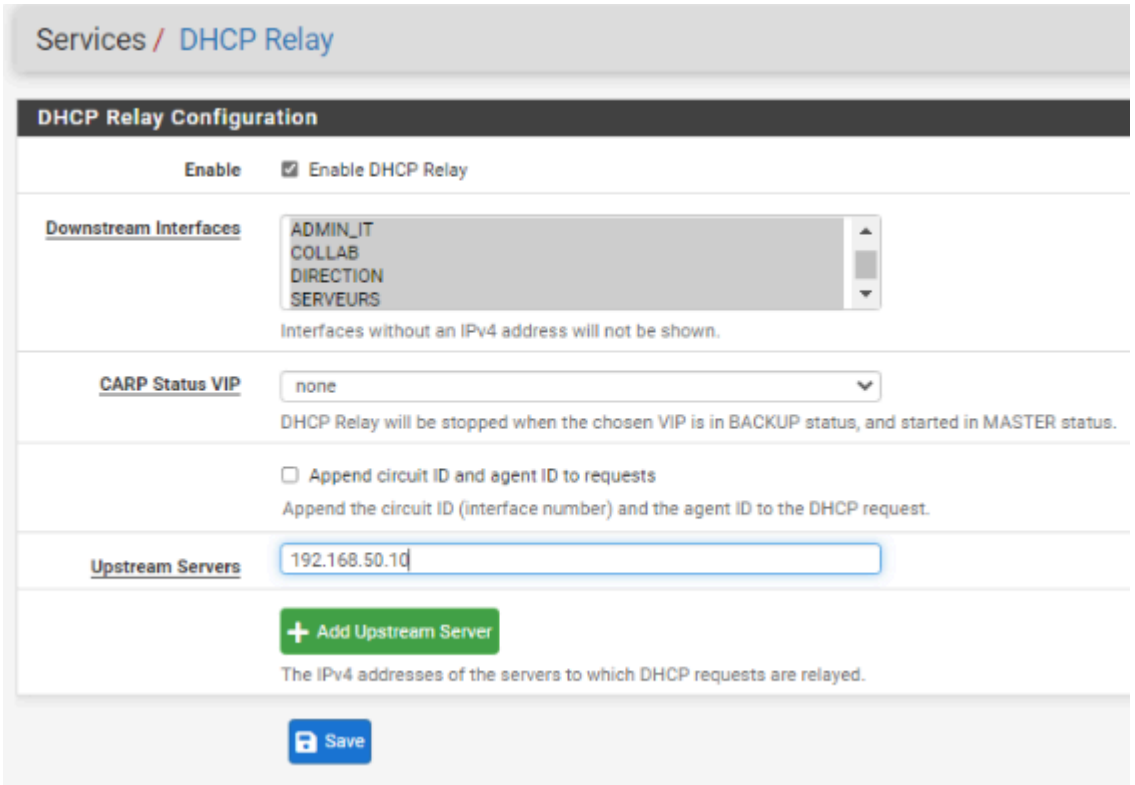
```
PS C:\Users\Administrateur> Get-DhcpServerv4Scope

ScopeId         SubnetMask      Name           State    StartRange      EndRange        LeaseDuration
-------         ----------      ----           -----    ----------      --------        -------------
192.168.10.0    255.255.255.248 ADMIN_IT       Active   192.168.10.1    192.168.10.5    8.00:00:00
192.168.20.0    255.255.255.240 COLLABORATEURS Active   192.168.20.1    192.168.20.13   8.00:00:00
192.168.30.0    255.255.255.248 DIRECTION      Active   192.168.30.1    192.168.30.5    8.00:00:00
192.168.50.0    255.255.255.224 SERVEUR        Active   192.168.50.1    192.168.50.29   8.00:00:00
192.168.99.0    255.255.255.224 INFRA          Active   192.168.99.1    192.168.99.29   8.00:00:00
```

Renseignement des passerelles pour les vlans :

```
PS C:\Users\Administrateur> Set-DhcpServerv4OptionValue -ScopeId 192.168.10.0 -OptionId 3 -Value 192.168.10.1
PS C:\Users\Administrateur> Set-DhcpServerv4OptionValue -ScopeId 192.168.20.0 -OptionId 3 -Value 192.168.20.1
PS C:\Users\Administrateur> Set-DhcpServerv4OptionValue -ScopeId 192.168.30.0 -OptionId 3 -Value 192.168.30.1
PS C:\Users\Administrateur> Set-DhcpServerv4OptionValue -ScopeId 192.168.50.0 -OptionId 3 -Value 192.168.50.1
PS C:\Users\Administrateur> Set-DhcpServerv4OptionValue -ScopeId 192.168.99.0 -OptionId 3 -Value 192.168.99.1
```

Activation DHCP Relay sur pfSense :





IV. Support et Gestion de Parc (GLPI)

- ## Déploiement de GLPI 10 (Séparation Web/DB sur LXC)

Maintenant, installation GLPI :
Avant toute chose, j'assigne une interface commune aux deux serveurs (pour qu'il puisse communiquer entre eux et donc puisse faire le routage, vlan etc).
Parker :

```
auto vmbr1
iface vmbr1 inet manual
        bridge-ports enp4s0
        bridge-stp off
        bridge-fd 0
        bridge-vlan-aware yes
        bridge-vids 10 20 30 50 99
```

Richards :

```
auto vmbr1
iface vmbr1 inet manual
        bridge-ports enp2s0f1
        bridge-stp off
        bridge-fd 0
        bridge-vlan-aware yes
        bridge-vids 10 20 30 50 99
```

Pour plus de sécurité, je décide de créer 2 containers séparé :

LXC ID	Nom	Rôle	IP	Réseau
200	glpi-web	Frontend	192.168.50.3	VLAN 50
201	glpi-db	Base MariaDB	192.168.50.13	VLAN 50

Installation de mariadb sur glpi-db (lxc) :

```
root@glpi-db:~# apt install mariadb-server -y
```

```
systemctl enable mariadb
```

```
systemctl start mariadb
```

Création de la data base :

```
MariaDB [(none)]> CREATE DATABASE glpidb CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
Query OK, 1 row affected (0.001 sec)
```

```
CREATE USER 'glpiuser'@'192.168.50.3' IDENTIFIED BY 'glpipass';
```

```
GRANT ALL PRIVILEGES ON glpidb.* TO 'glpiuser'@'192.168.50.3';
```

```
FLUSH PRIVILEGES;
```

```
EXIT;
```

Dans /etc/mysql/mariadb.conf.d/50-server.cnf :

```
bind-address            = 0.0.0.0
```

Installation GLPI sur glpi-web (lxc) :

```
root@glpi-web:~# apt install apache2 php php-mysql php-curl php-xml php-mbstring php-intl php-gd unzip -y
systemctl enable apache2
systemctl start apache2
```

Téléchargement de GLPI :

```
/var/www/html# wget https://github.com/glpi-project/glpi/releases/download/10.0.14/glpi-10.0.14.tgz
tar -xvzf glpi-10.0.14.tgz
chown -R www-data:www-data glpi
```

- Configuration de GLPI via l'interface web

Je me rends sur un pc dans le vlan 10 (ADMIN IT) et tape l'adresse du glpi-web/glpi pour avoir accès à l'interface web :


GLPI SETUP
Début de l'installation
Installation ou mise à jour de GLPI
Choisissez 'Installation' pour une nouvelle installation de GLPI.
Choisissez 'Mise à jour' pour lancer la mise à jour de votre version de GLPI à partir d'une version antérieure.
Installer
Mettre à jour

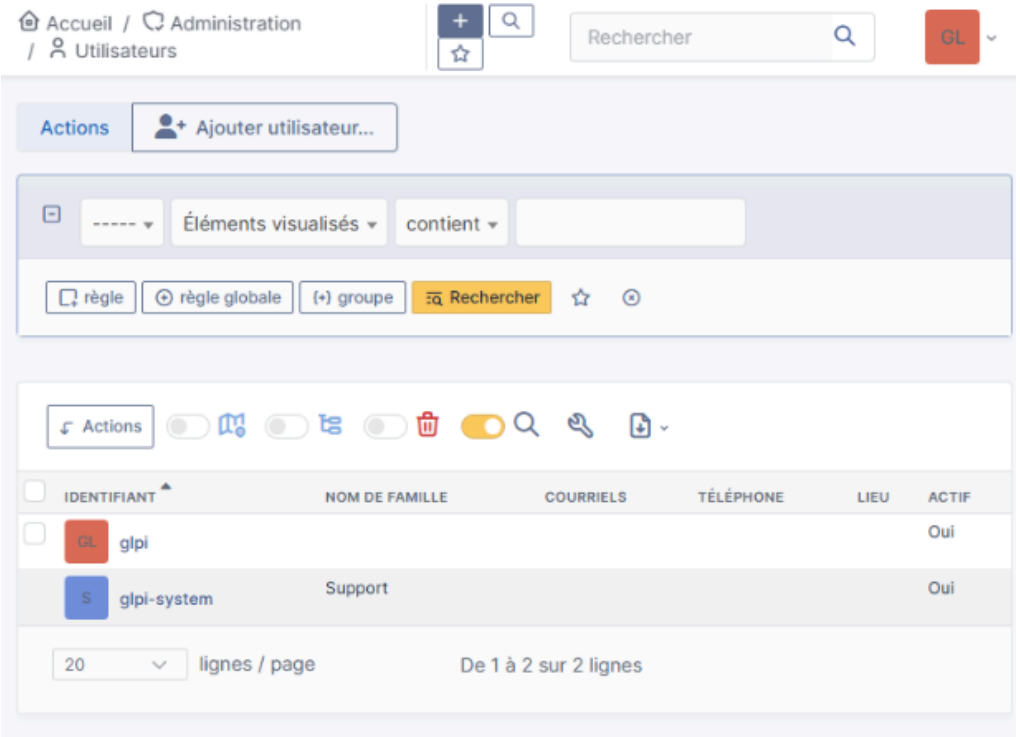

GLPI SETUP
Étape 1
Configuration de la connexion à la base de données
Serveur SQL (MariaDB ou MySQL)
192.168.50.30
Utilisateur SQL
glpiuser
Mot de passe SQL
Continuer


Veuillez sélectionner une base de données :
Créer une nouvelle base ou utiliser une base existante :
glpidb
Continuer

Suite à ces manip et par mesures de sécurité, je supprime le dossier install/ de mon glpi :

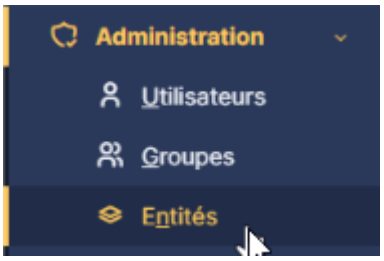
```
/var/www/html/glpi# rm -rf install/
```

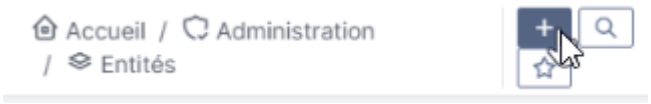
Ensuite, on se connecte avec le compte glpi et le mot de passe glpi
Ensuite, je modifie le mot de passe glpi (admin) et supprime les utilisateurs : tech, normal, post-only.

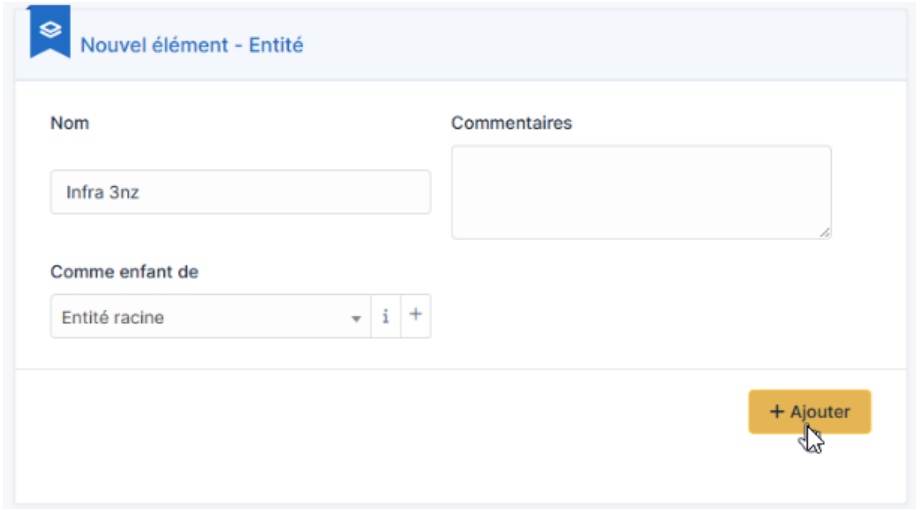


- Intégration LDAP entre GLPI et Active Directory

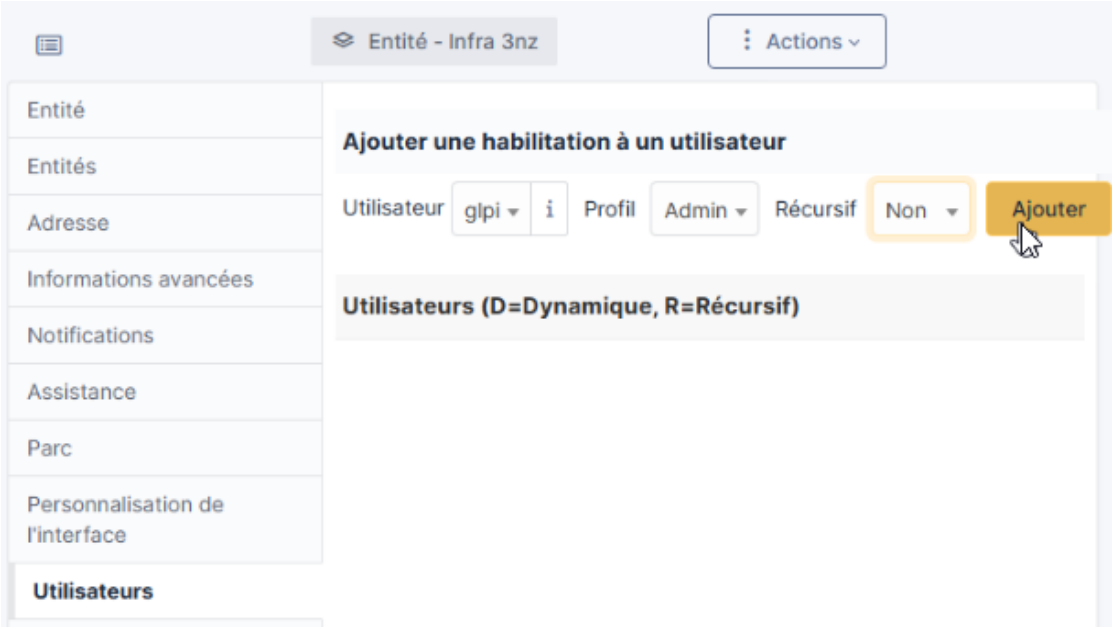
Je défini mon entitée :







Je l'associe à mon compte admin glpi principal :



Maintenant liaison LDAP :

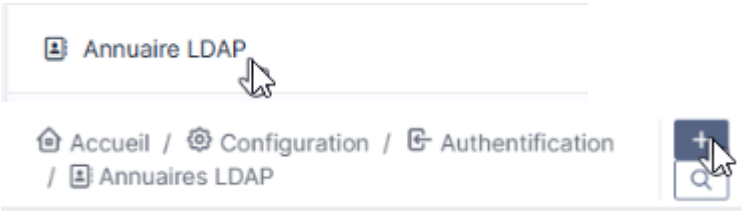
```
root@glpi-web:~# apt install php-ldap -y
```

```
root@glpi-web:~# apt install ldap-utils -y
```

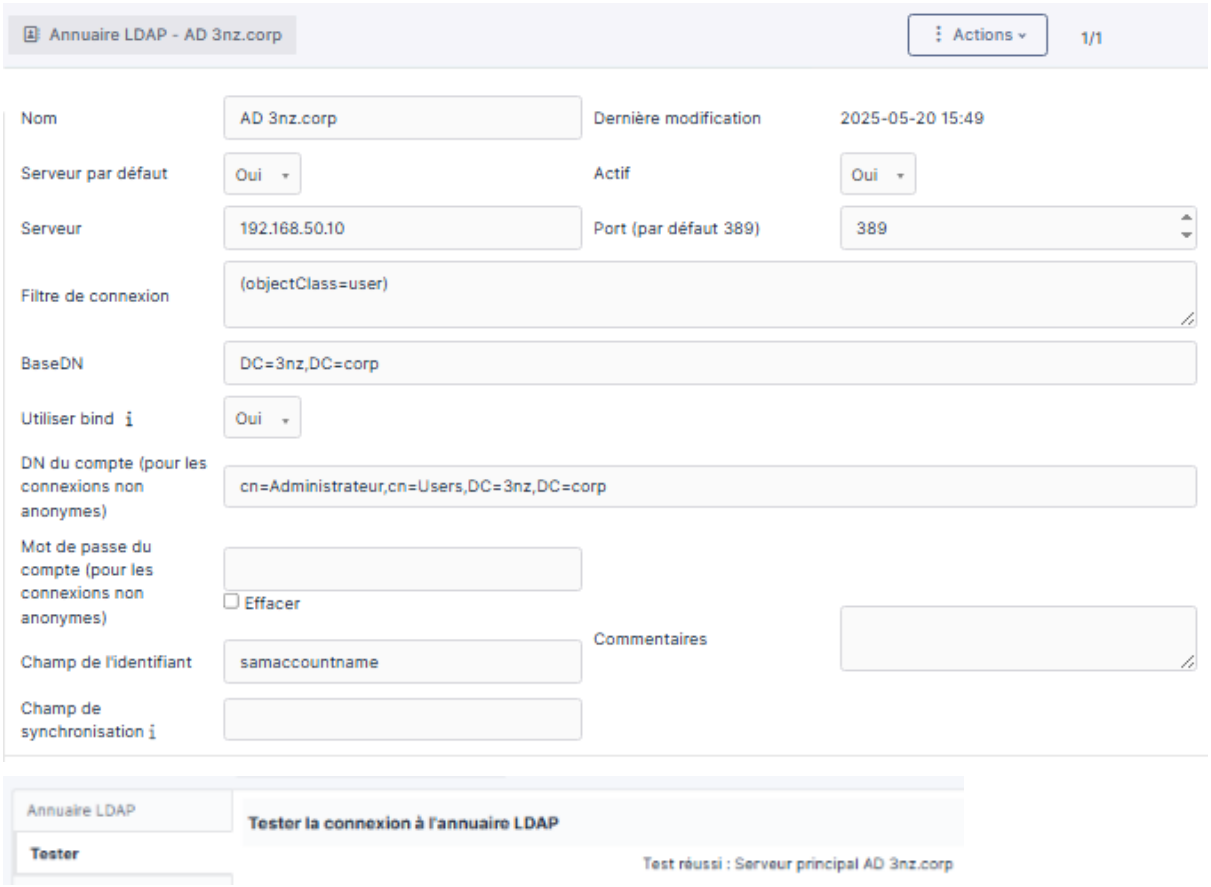
Je récupère les infos de mon AD :

```
PS C:\Users\Administrateur> hostname
>> (Get-ADDomain).DistinguishedName
WinSrv1
DC=3nz,DC=corp
```

Et je configure LDAP dans GLPI :



Renseigner (objectClass=user) pour que tous les utilisateurs de l'AD remonte



Création des groupes et des utilisateurs dans l'AD :

```
PS C:\Users\Administrateur> New-ADGroup -Name "DSI" -GroupScope Global -GroupCategory Security
PS C:\Users\Administrateur> New-ADGroup -Name "DIRECTION" -GroupScope Global -GroupCategory Security
PS C:\Users\Administrateur> New-ADGroup -Name "COLLABORATEURS" -GroupScope Global -GroupCategory Security
```

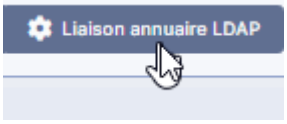
Pour les utilisateurs, création d'un script powershell :

```
notepad C:\Scripts\create-users-glpi.ps1
```

```
# Groupe DSI (3 IT)
@(
	@{Sam="vlefevre"; Name="Victor Lefevre"},
	@{Sam="slaurent"; Name="Sophie Laurent"},
	@{Sam="rpetit"; Name="Romain Petit"}
) | ForEach-Object {
	$login = $_.Sam
	$name = $_.name
	$upn = "$login@3nz.corp"
	New-ADUser -Name $name -SamAccountName $login -UserPrincipalName $upn -AccountPassword (ConvertTo-SecureString "3nzPwd!" -AsPlainText -Force) -Enabled $true -ChangePasswordAtLogon $tru
	Add-ADGroupMember -Identity "DSI" -Members $login
}

# Groupe DIRECTION (2)
@(
	@{Sam="cdubois"; Name="Claire Dubois"},
	@{Sam="jmarchand"; Name="Julien Marchand"}
) | ForEach-Object {
	$login = $_.Sam
	$name = $_.name
	$upn = "$login@3nz.corp"
	New-ADUser -Name $name -SamAccountName $login -UserPrincipalName $upn -AccountPassword (ConvertTo-SecureString "3nzPwd!" -AsPlainText -Force) -Enabled $true -ChangePasswordAtLogon $tru
	Add-ADGroupMember -Identity "DIRECTION" -Members $login
}

# Groupe COLLABORATEURS (10)
@(
	@{Sam="cmorel"; Name="Camille Morel"},
	@{Sam="ldurand"; Name="Luc Durand"},
	@{Sam="ebernard"; Name="Elisa Bernard"},
	@{Sam="nrobert"; Name="Nicolas Robert"},
	@{Sam="lmartin"; Name="Léa Martin"},
	@{Sam="aperrin"; Name="Axel Perrin"},
	@{Sam="jgirard"; Name="Julie Girard"},
	@{Sam="anoel"; Name="Arnaud Noël"},
	@{Sam="srenard"; Name="Sara Renard"},
	@{Sam="pgautier"; Name="Pierre Gautier"}
) | ForEach-Object {
	$login = $_.Sam
	$name = $_.name
	$upn = "$login@3nz.corp"
	New-ADUser -Name $name -SamAccountName $login -UserPrincipalName $upn -AccountPassword (ConvertTo-SecureString "3nzPwd!" -AsPlainText -Force) -Enabled $true -ChangePasswordAtLogon $tru
	Add-ADGroupMember -Identity "COLLABORATEURS" -Members $login
}
```

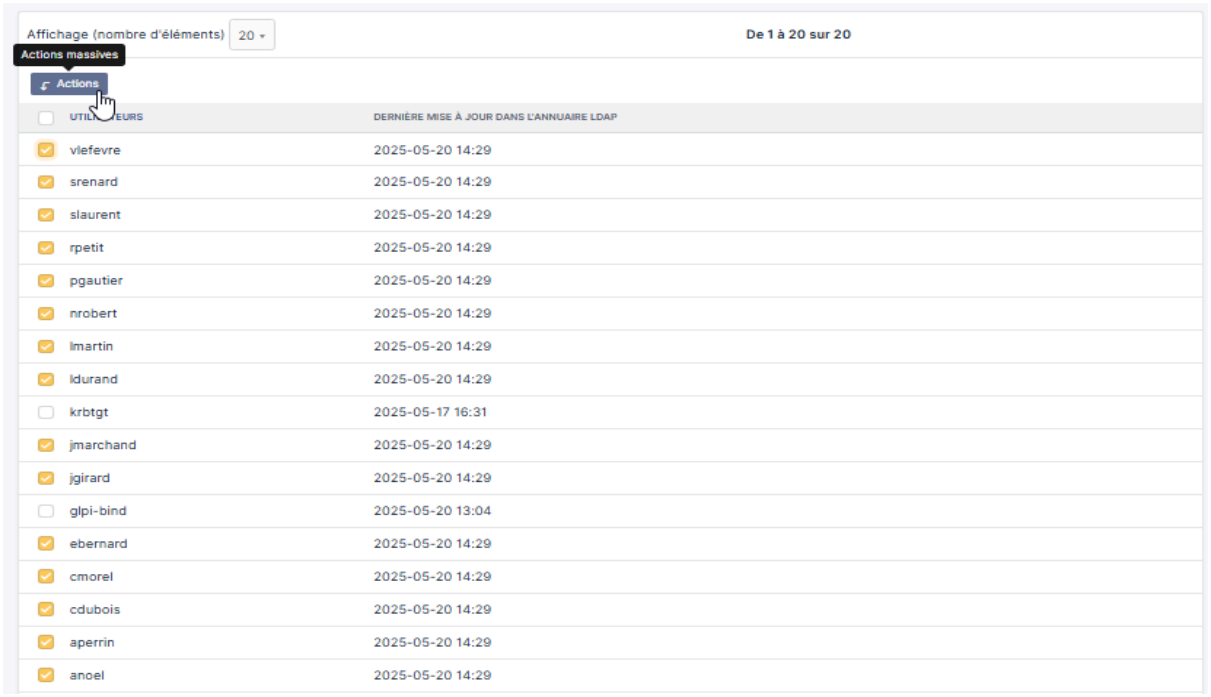
```
PS C:\Scripts> Set-ExecutionPolicy RemoteSigned -Scope Process
>> & "C:\Scripts\create-users.ps1"
```

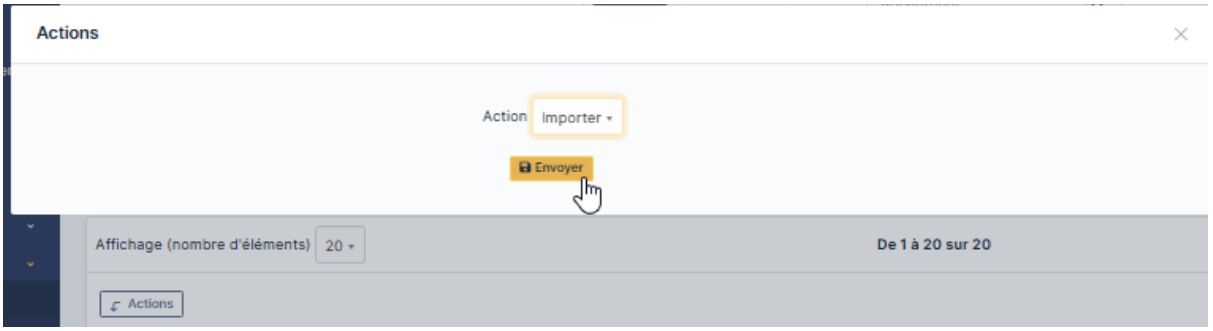
Maintenant, on importe (LDAP) les utilisateurs dans GLPI

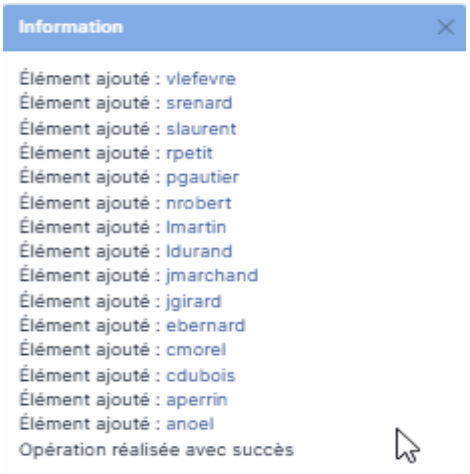


On clique sur rechercher

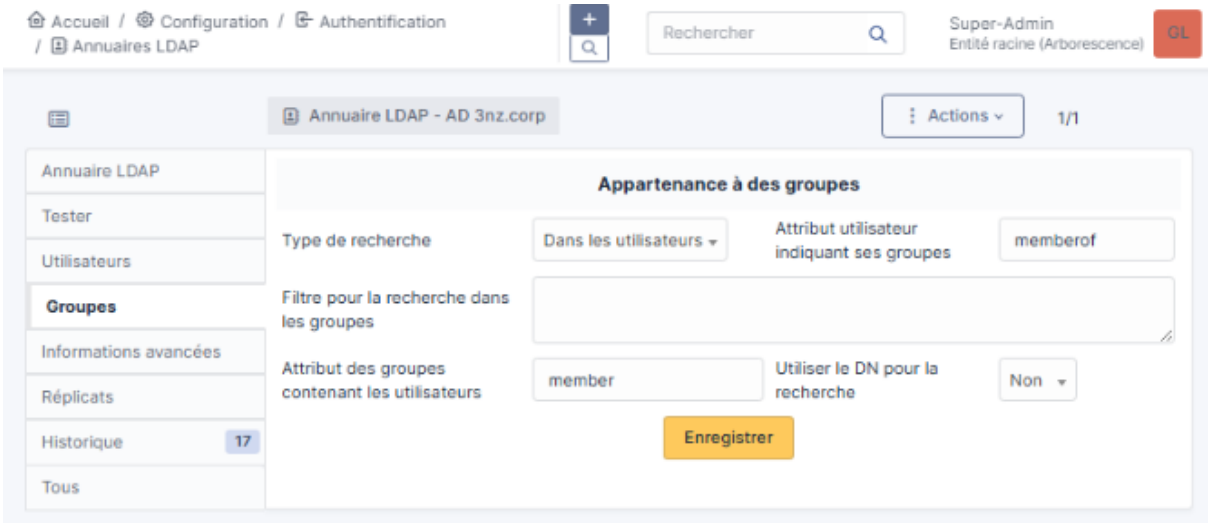
Sélection des utilisateurs souhaité





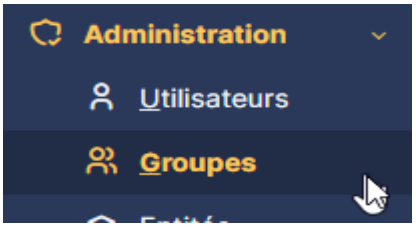


Dans Configuration > Authentification > Annuaire LDAP > Groupe

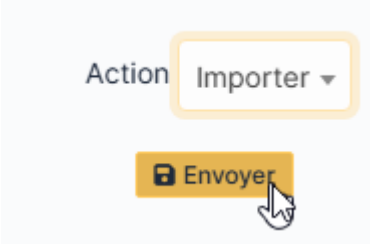


Cela permet à GLPI de comprendre la relation utilisateur-groupe à travers l'attribut memberOf

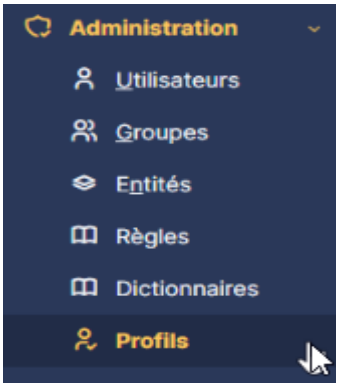
Importation des groupes LDAP :

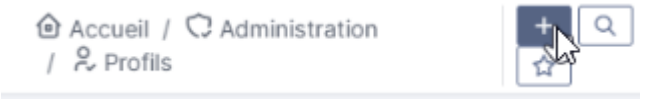


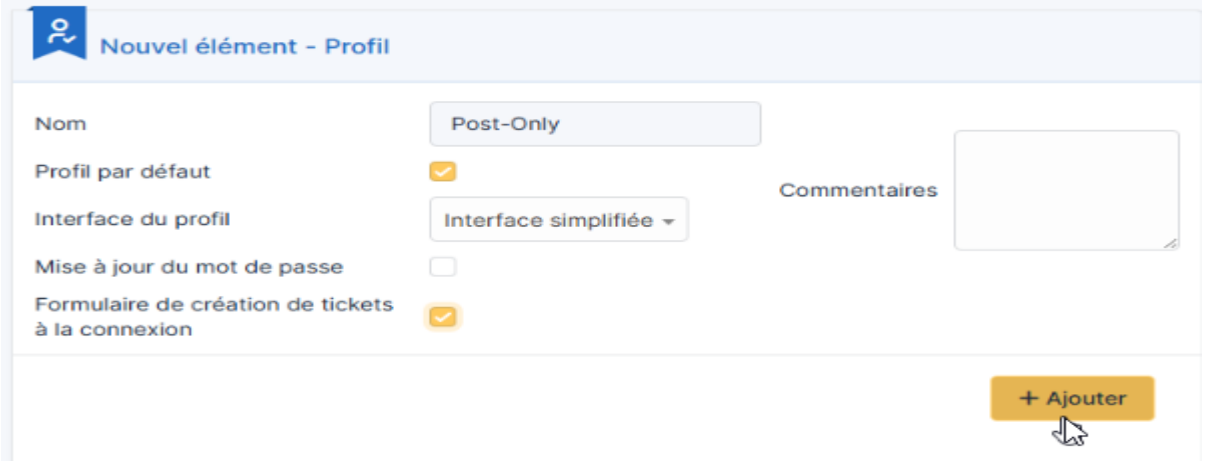
Action : Importer :

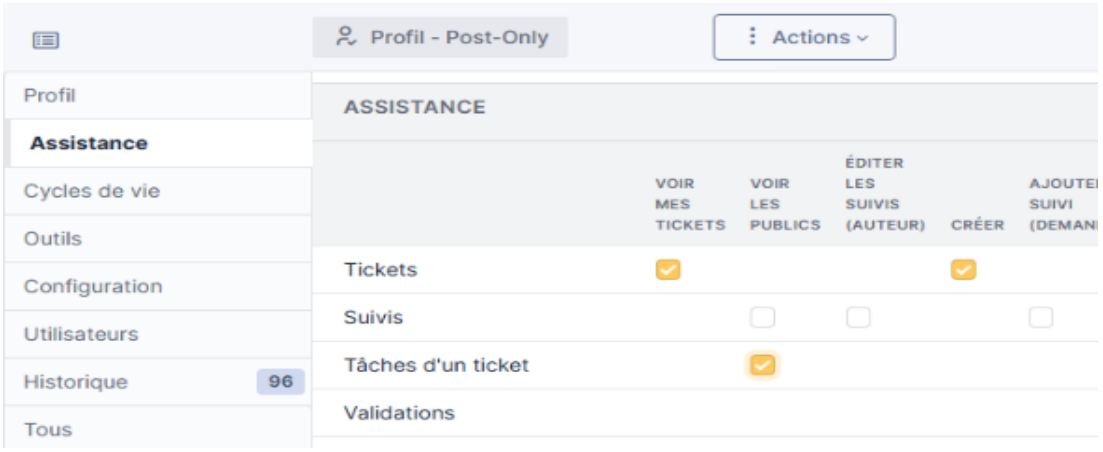


Création d'un profil Post-Only ->



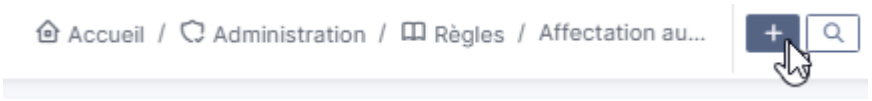




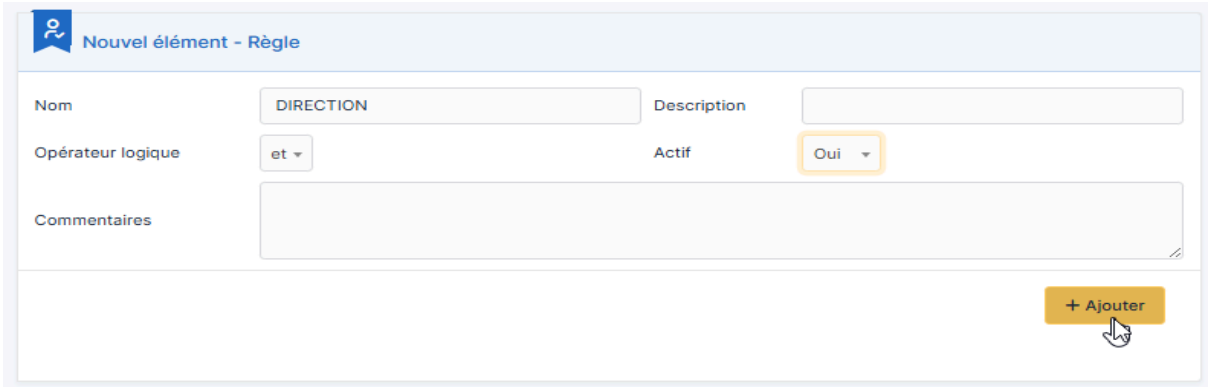


Création d'une règle d'affectation d'habilitations pour des groupes :
Administration > Règles > Règles d'affectation d'habilitations à un utilisateur

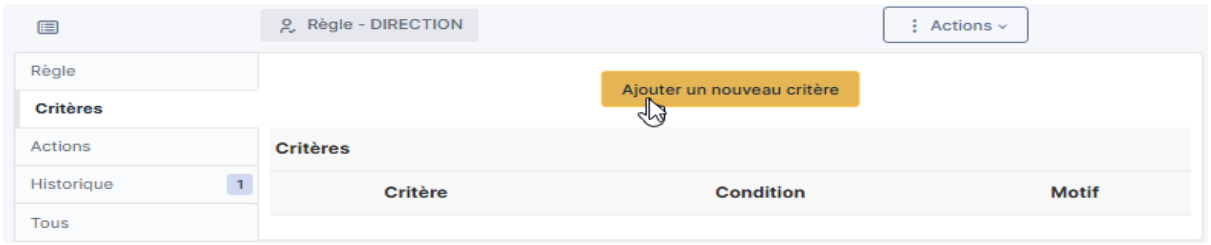
Dans le bandeau cliquez sur +



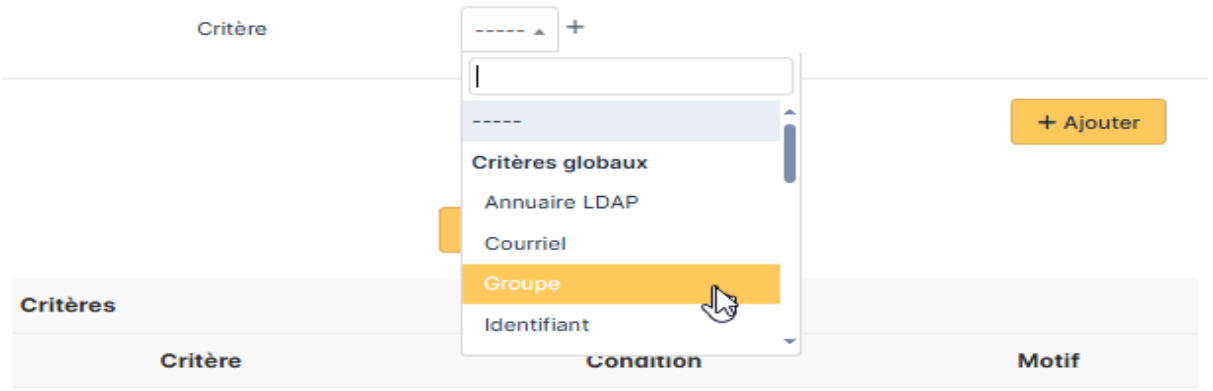
Nommez la règle, rendez l'a actif et ajoutez



Maintenant cliquez sur critères puis ajouter un nouveau critère

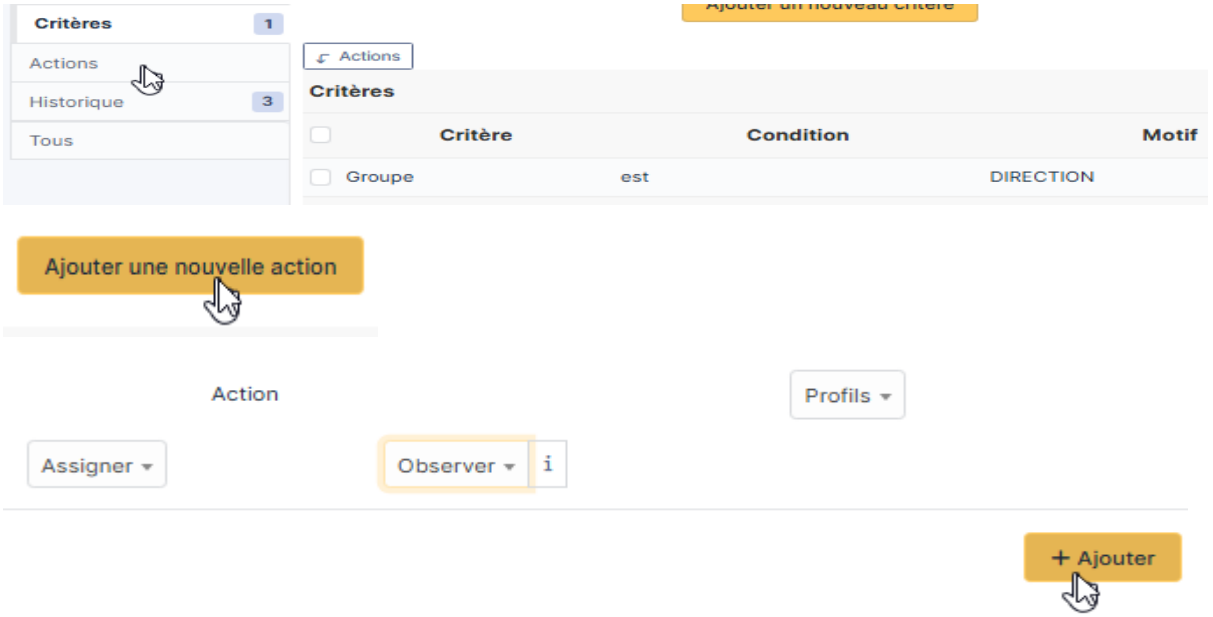


Ajout d'un nouveau critère, en l'occurrence Groupe



On choisi le groupe DIRECTION, puis on ajoute

Et on assigne l'action, ici le groupe DIRECTION auras le droit d'observer et créer des tickets



Maintenant, je réitère pour DSI et COLLABORATEURS

Récapitulatif :

Règle	Groupe LDAP	Profil attribué
Import DSI	DSI	Admin
Import DIRECTION	DIRECTION	Post-only
Import COLLABORATEUR	COLLABORATEUR	Post-only

- Planification d’une tâche CRON pour la synchro LDAP

sur glpi-web :

```
root@glpi-web:~# crontab -e
```

Ajout de ligne suivante dans le crontab :

0 2 * * * /usr/bin/php /var/www/html/bin/console glpi:ldap:synchronize_users --no-interaction >> /var/log/glpi-ldap.log 2>&1

La synchronisation fonctionne

```
root@glpi-web:~# cat /var/log/glpi-ldap.log
Fri May 23 16:56:01 UTC 2025 Start Sync
Serveur LDAP "AD 3nz.corp" en cours de traitement ...
Importation des utilisateurs du serveur "AD 3nz.corp" ...
 0/2 [>----------------------------]   0%
 2/2 [==============================] 100%
Synchronisation des utilisateurs avec le serveur "AD 3nz.corp" ...
  0/19 [>----------------------------]   0%
  4/19 [=====>----------------------]  21%
  8/19 [===========>----------------]  42%
 12/19 [=================>----------]  63%
 16/19 [======================>-----]  84%
 19/19 [==============================] 100%
+--------------+---------+-------------+--------------------------+----------------------------------+
| Serveur LDAP | Importé | Synchronisé | Supprimé du serveur LDAP | Restauré depuis un annuaire LDAP |
+--------------+---------+-------------+--------------------------+----------------------------------+
| AD 3nz.corp  | 0       | 19          | 0                        | 0                                |
+--------------+---------+-------------+--------------------------+----------------------------------+
```

Maintenant, créer un enregistrement DNS pour le glpi (192.168.50.3)

```
PS C:\Users\Administrateur> Add-DnsServerResourceRecordA -Name "glpi" -ZoneName "3nz.corp" -IPv4Address "192.168.50.3"
```

Pour la suite des événements et pour plus de facilité, je vais avoir besoin d’installer RSAT sur mon serveur :

```
Add-WindowsFeature -Name RSAT-RemoteAccess
```

Installation du module Active Directory sur le PC de l’admin sys :

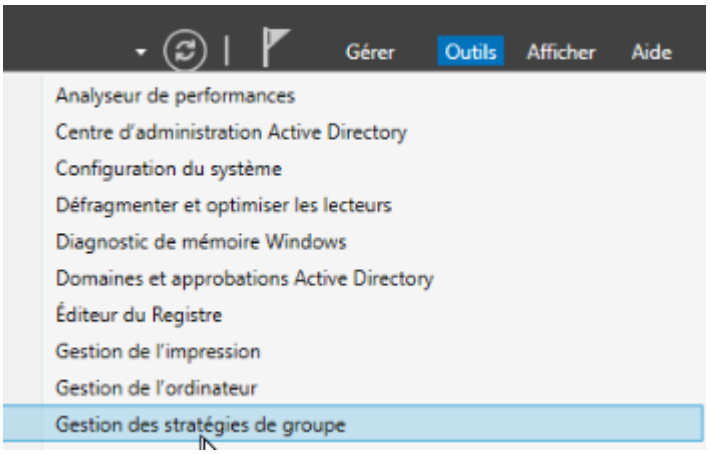
```
Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0"
```

Installation GPMC :

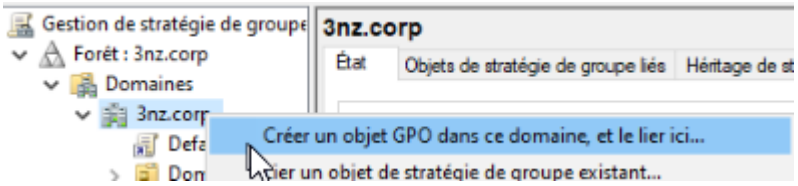
o

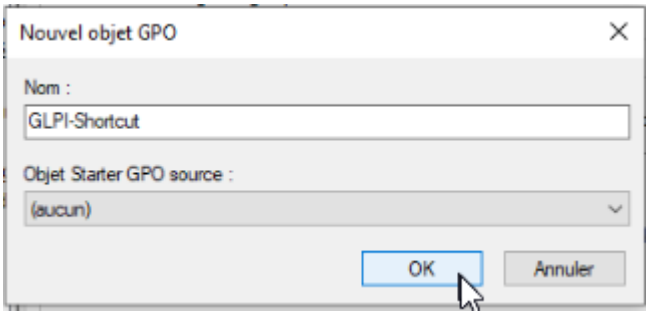
- Déploiement de l’agent GLPI via GPO

Création d’une GPO créant un raccourci sur chaque session utilisateurs :
Gestionnaire de serveur > Outils > Gestion des stratégies de groupe :

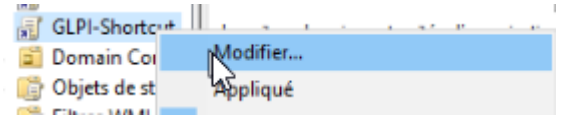


Forêt : 3nz.corp > Domaines > clic droit sur le domaine > Créer un GPO..

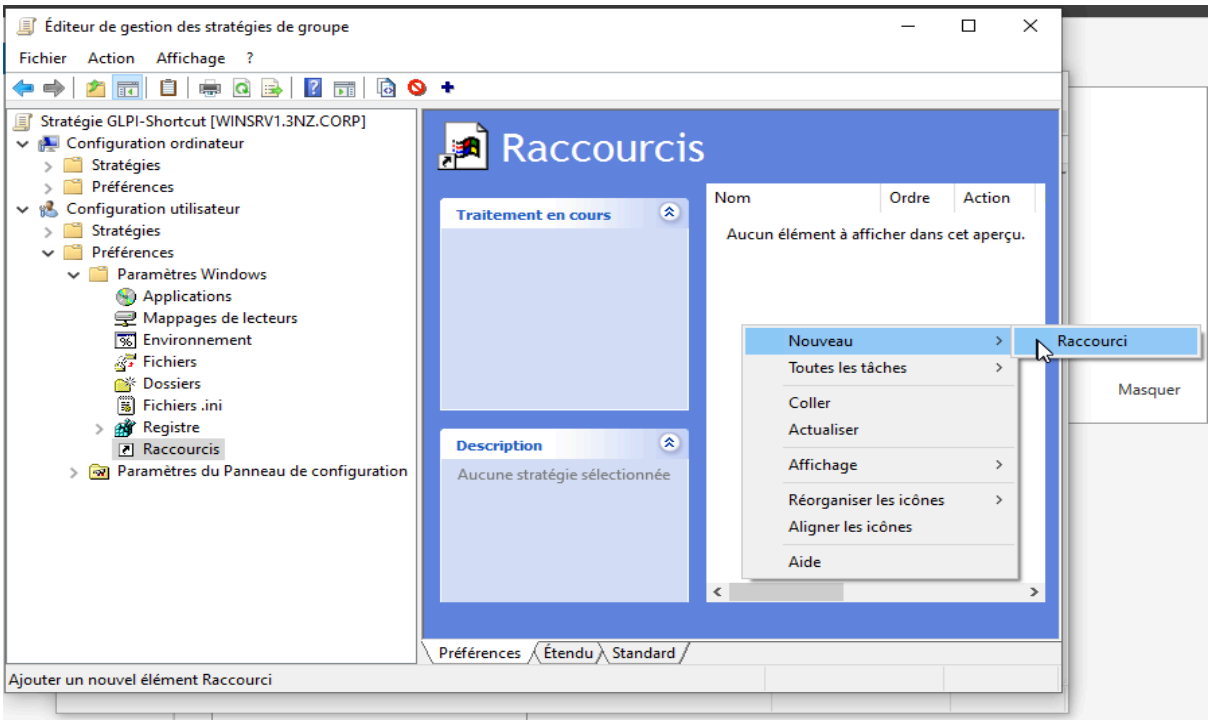


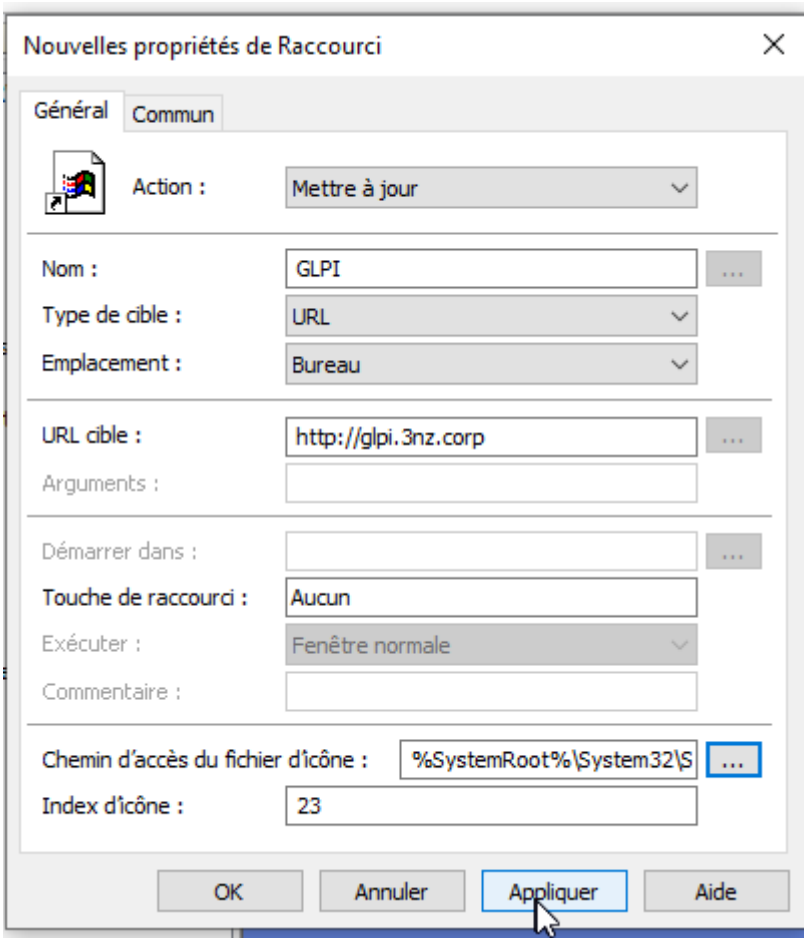


clic droit modifier (sur la GPO créer)



Parcourez l'arborescence
Configuration utilisateur > Préférences > Paramètres Windows > Raccourcis
Clic droit sur la fenêtre blanche > Nouveau > Raccourci






```
C:\Windows\system32>gpupdate /force
```

- Activation HTTPS pour sécuriser GLPI

Maintenant que glpi est déployé sur tous les postes, je décide, par mesure de sécurité, d'activer le HTTPS, en effet cela permettra de crypter les flux.

Sur glpi-web :

```
apt install openssl -y
```

Création d'un nouveau dossier ou sera stocké le certificat :

```
mkdir /etc/ssl/custom
```

Génération du certificat :

```
openssl req -x509 -nodes -days 365 -newkey rsa:4096 -sha256 -out /etc/ssl/custom/glpi.crt -keyout /etc/ssl/custom/glpi.key
```

```
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Hérault
Locality Name (eg, city) []:Montpellier
Organization Name (eg, company) [Internet Widgits Pty Ltd]:3nz
Organizational Unit Name (eg, section) []:Corp
Common Name (e.g. server FQDN or YOUR name) []:3NZ CORP
Email Address []:elemesle.info@gmail.com
```

Je mets seulement les droits de lecture sur le fichier

```
chmod 440 /etc/ssl/custom/glpi.crt
```

Création d'un fichier de conf pour l'HTTPS dans /etc/apache2/sites-available :

```
vim glpi-TLS.conf
```

```
<VirtualHost *:443>
#Adresse e-mail de l'admin du serveur
        ServerAdmin elemesle.info@gmail.com

#Nom et adresse IP du serveur
        ServerName 192.168.50.3
        ServerAlias glpi.3nz.corp

#Emplacement des fichiers du site web
        DocumentRoot /var/www/glpi/glpi

#Configuration SSL
        SSLEngine on
        SSLCertificateFile /etc/ssl/custom/glpi.crt
        SSLCertificateKeyFile /etc/ssl/custom/glpi.key

#Autoriser l'accs aux fichiers dans le rpertoir DocumentRoot
        <Directory /var/www/glpi/glpi>
                Require all granted
                AllowOverride FileInfo
        </Directory>

#Journalisation
        ErrorLog ${APACHE_LOG_DIR}/glpi_TLS_error.log
        CustomLog ${APACHE_LOG_DIR}/glpi_TLS_access.log combined
</VirtualHost>
```

Démarrage du module SSL pour Apache :

```
a2enmod ssl
```

Création d'un lien symbolique :

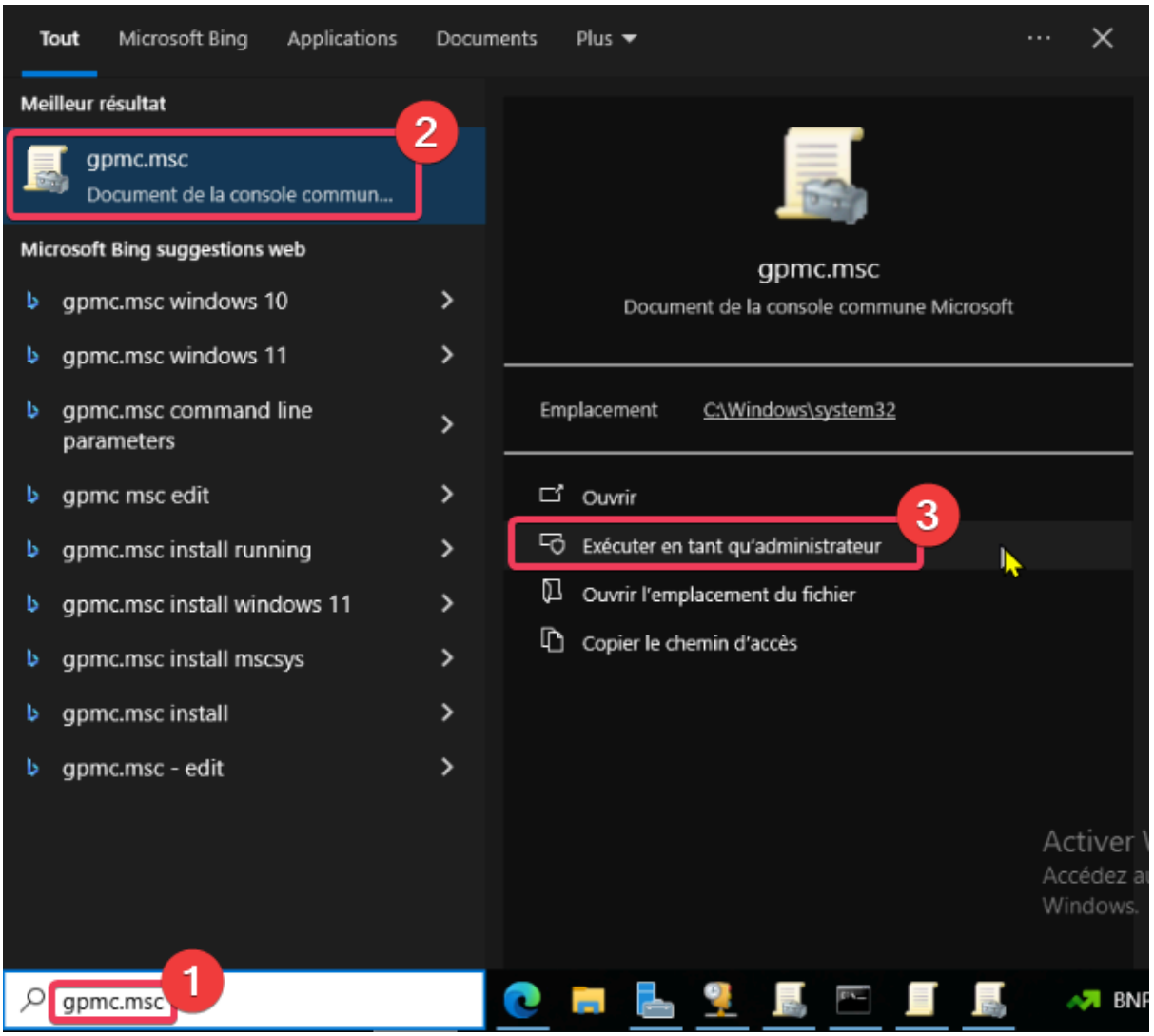
```
ln -s /etc/apache2/sites-available/glpi-TLS.conf /etc/apache2/sites-enabled/
```

Ajout d'une redirection de port :

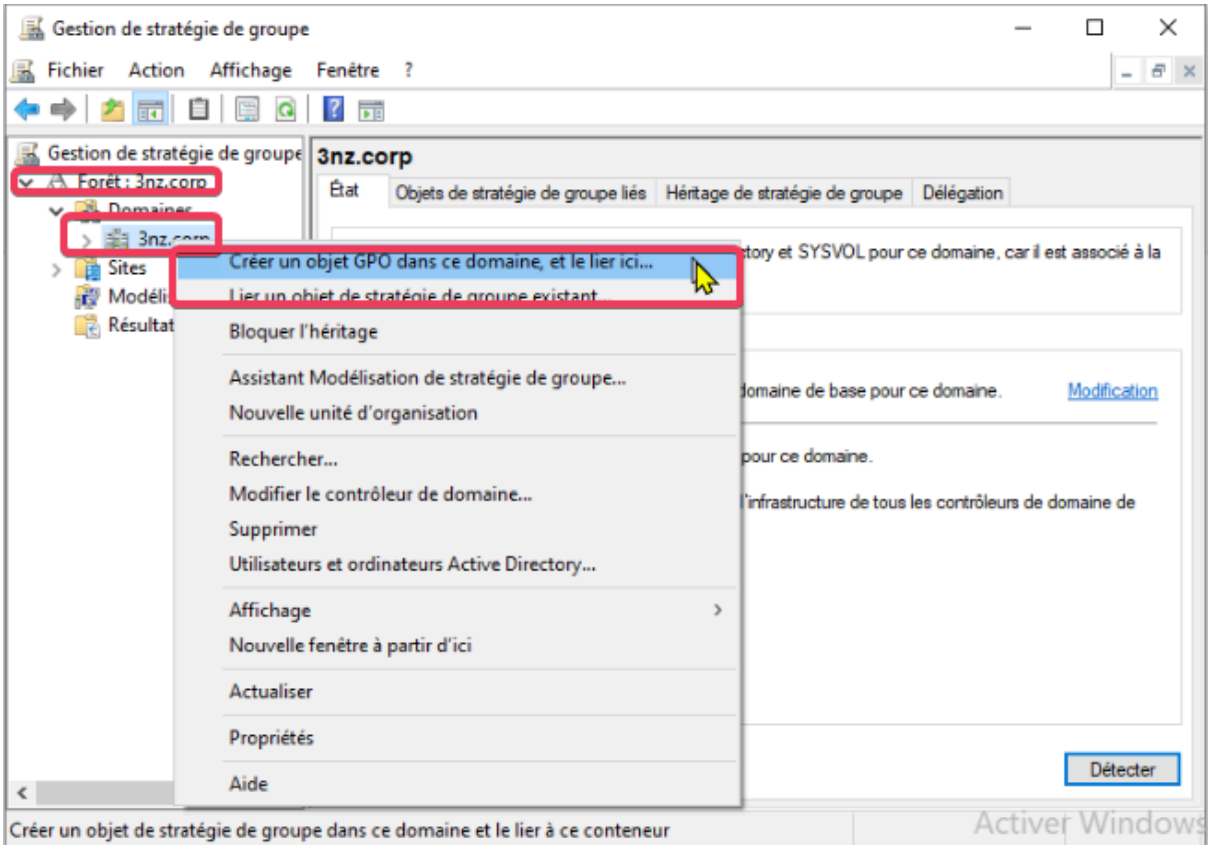
```
<VirtualHost *:80>
        ServerName glpi.3nz.corp
        ServerAlias glpi.3nz.corp

#Redirection permanente vers HTTPS
        Redirect 301 / https://glpi.3nz.corp/
</VirtualHost>
```

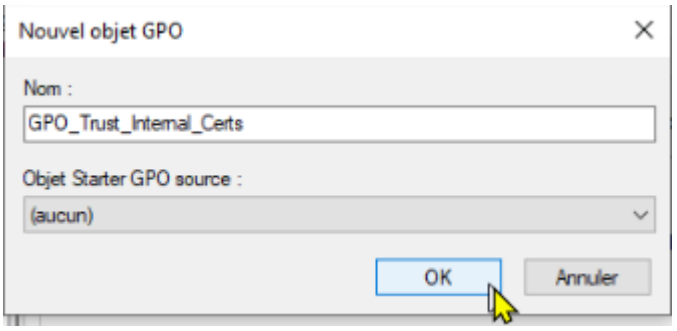
Pour activer le https, il faut aussi faire de l'autorité de certification (auto-signé) soit autorisé sur le serveur, pour ce faire :

Tapez gpmc.msc sur un poste d'administration de vos serveurs :

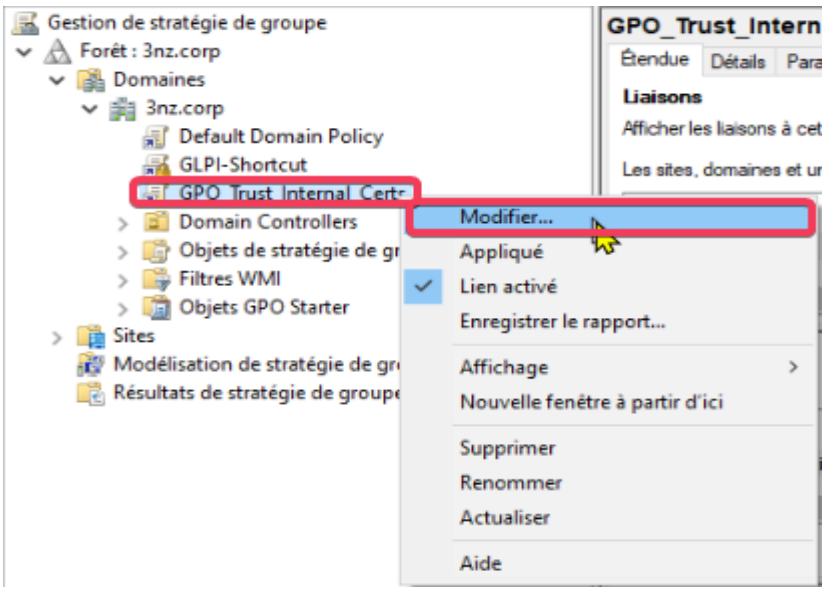


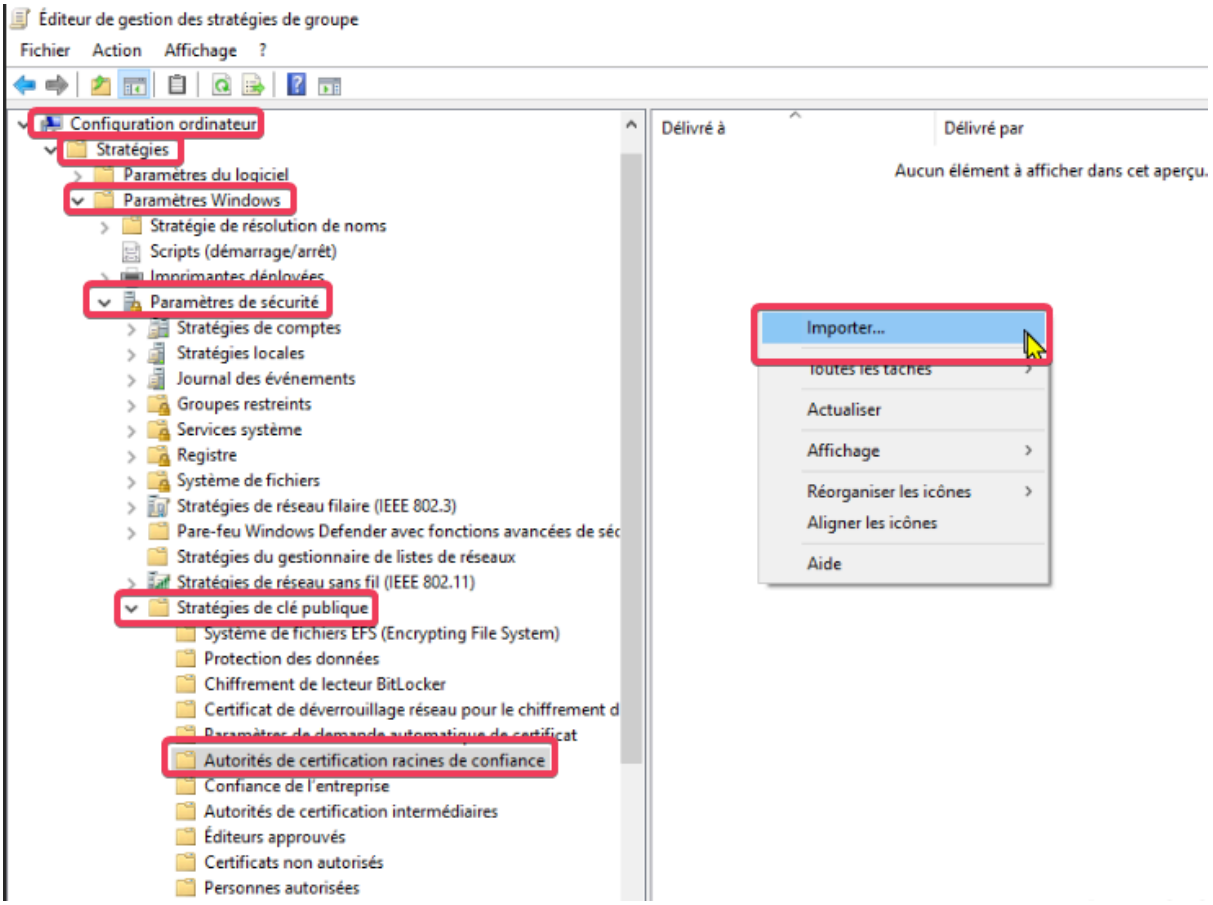
Créer une nouvelle GPO :

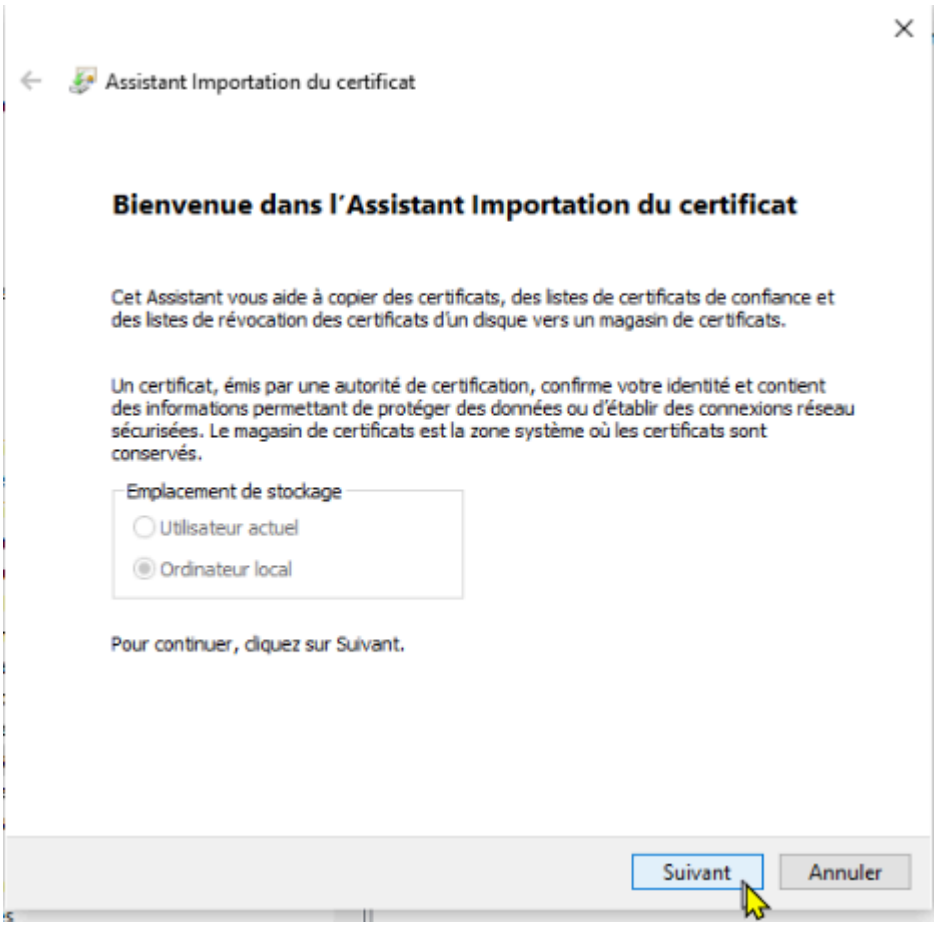




Clic-droit, modifier sur la GPO créée :



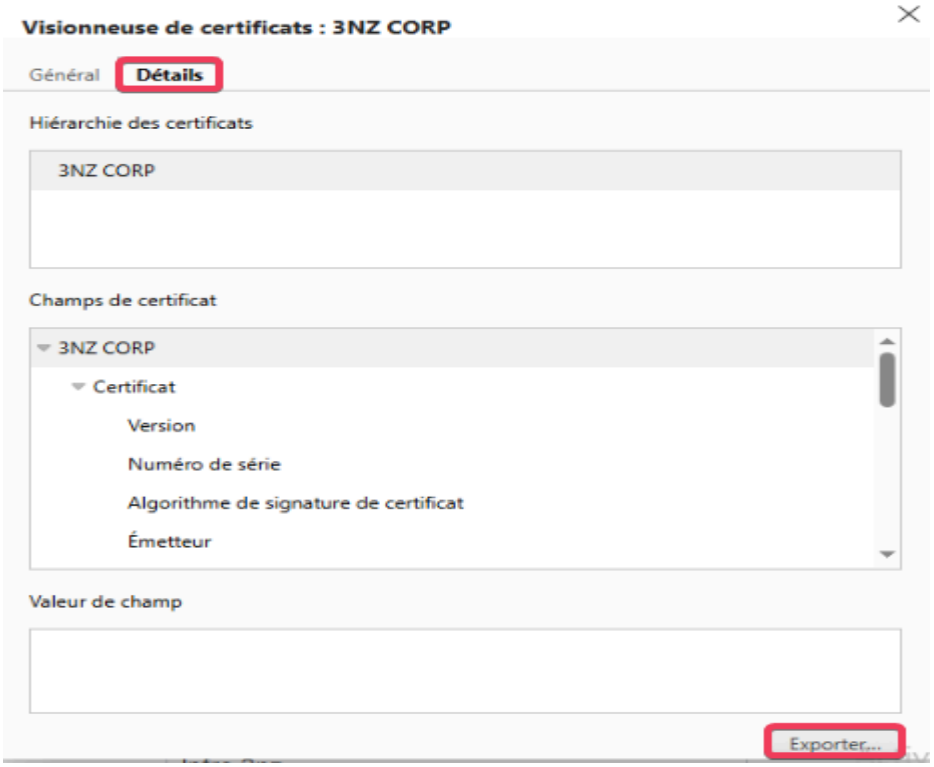

Éditeur de gestion des stratégies de groupe
Fichier Action Affichage ?
Configuration ordinateur
Stratégies
Paramètres du logiciel
Paramètres Windows
Stratégie de résolution de noms
Scripts (démarrage/arrêt)
Imprimantes déployées
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau filaire (IEEE 802.3)
Pare-feu Windows Defender avec fonctions avancées de séc
Stratégies du gestionnaire de listes de réseaux
Stratégies de réseau sans fil (IEEE 802.11)
Stratégies de clé publique
Système de fichiers EFS (Encrypting File System)
Protection des données
Chiffrement de lecteur BitLocker
Certificat de déverrouillage réseau pour le chiffrement d
Paramètres de demande automatique de certificat
Autorités de certification racines de confiance
Confiance de l'entreprise
Autorités de certification intermédiaires
Éditeurs approuvés
Certificats non autorisés
Personnes autorisées
Délivré à
Délivré par
Aucun élément à afficher dans cet aperçu.
Importer...
Toutes les tâches
Actualiser
Affichage
Réorganiser les icônes
Aligner les icônes
Aide


Assistant Importation du certificat
Bienvenue dans l'Assistant Importation du certificat
Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un disque vers un magasin de certificats.
Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.
Emplacement de stockage
Utilisateur actuel
Ordinateur local
Pour continuer, cliquez sur Suivant.
Suivant
Annuler

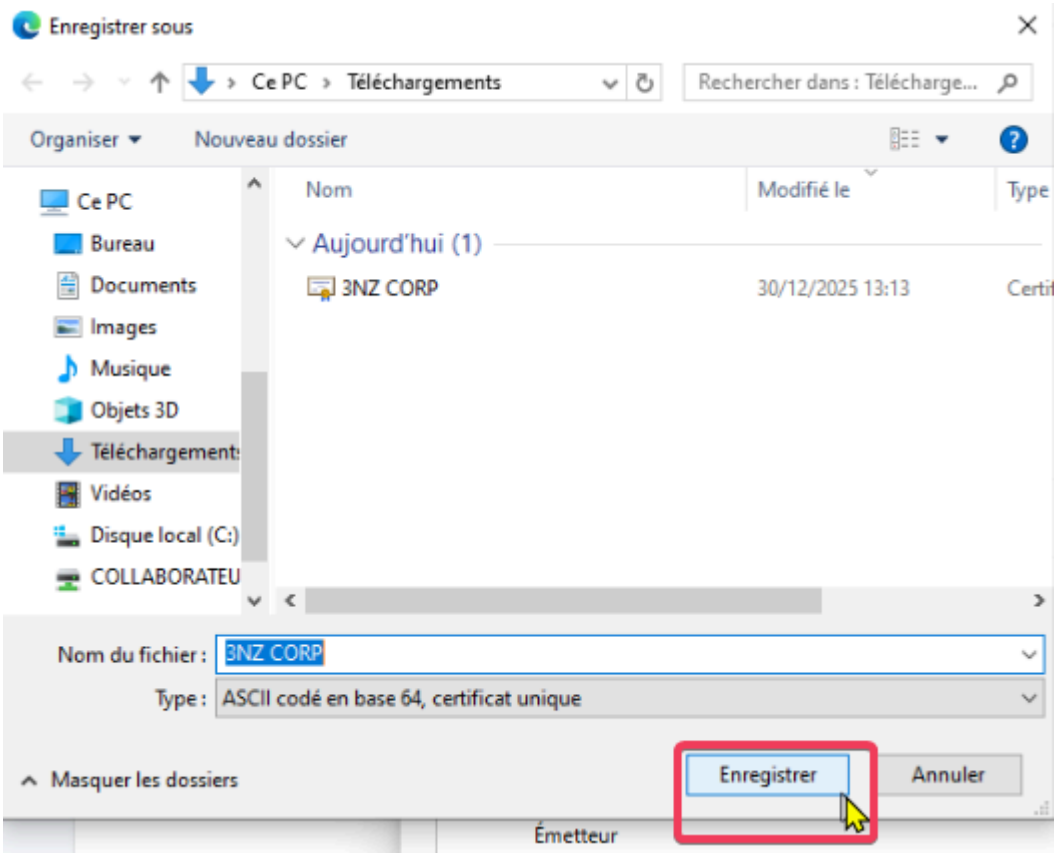
Rendez-vous sur le site glpi.3nz.corp, cliquez sur l'onglet rouge, non sécurisé, cliquez sur La connexion à ce site n'est pas sécurisée :

Ensuite, cliquez sur le logo des certifications :

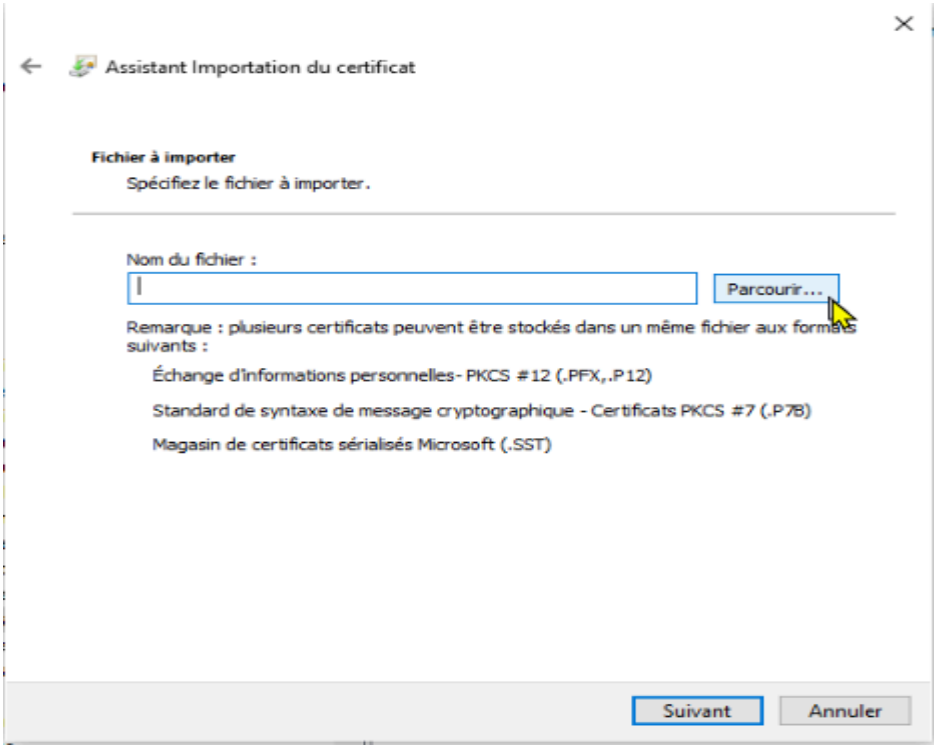
Cliquez sur l'onglet Détails, puis en bas à droite Exporter…

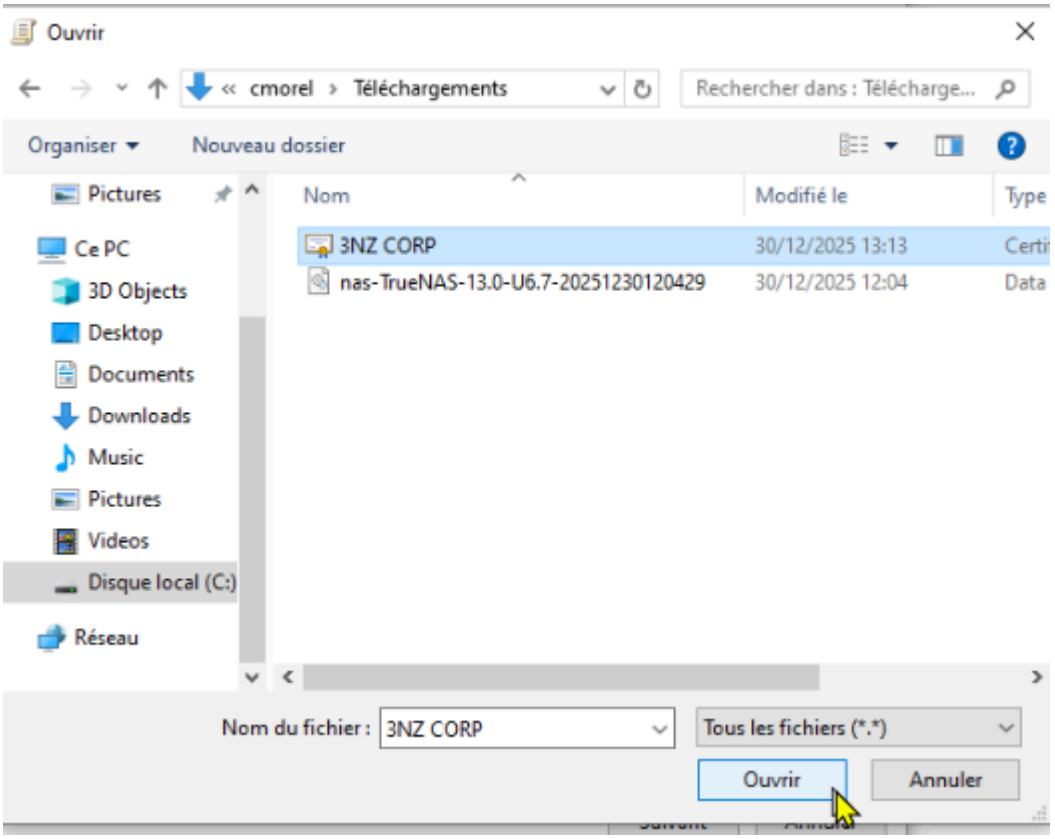


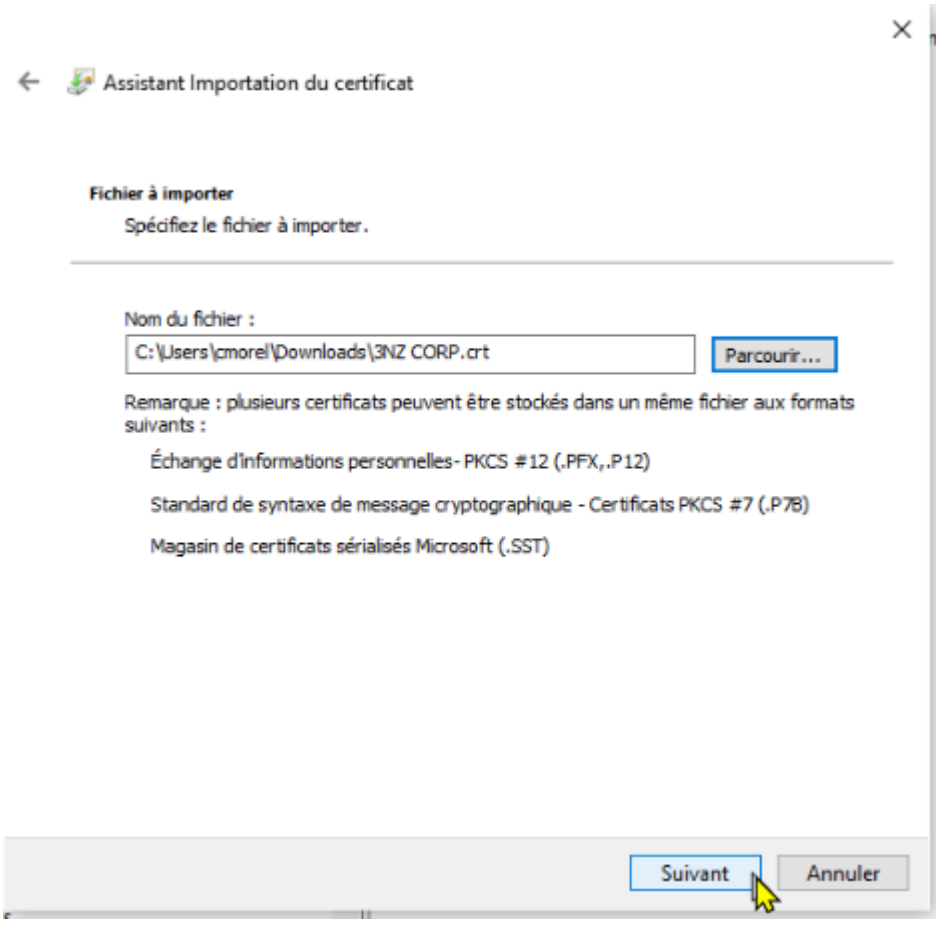
Puis Enregistrer le certificat :

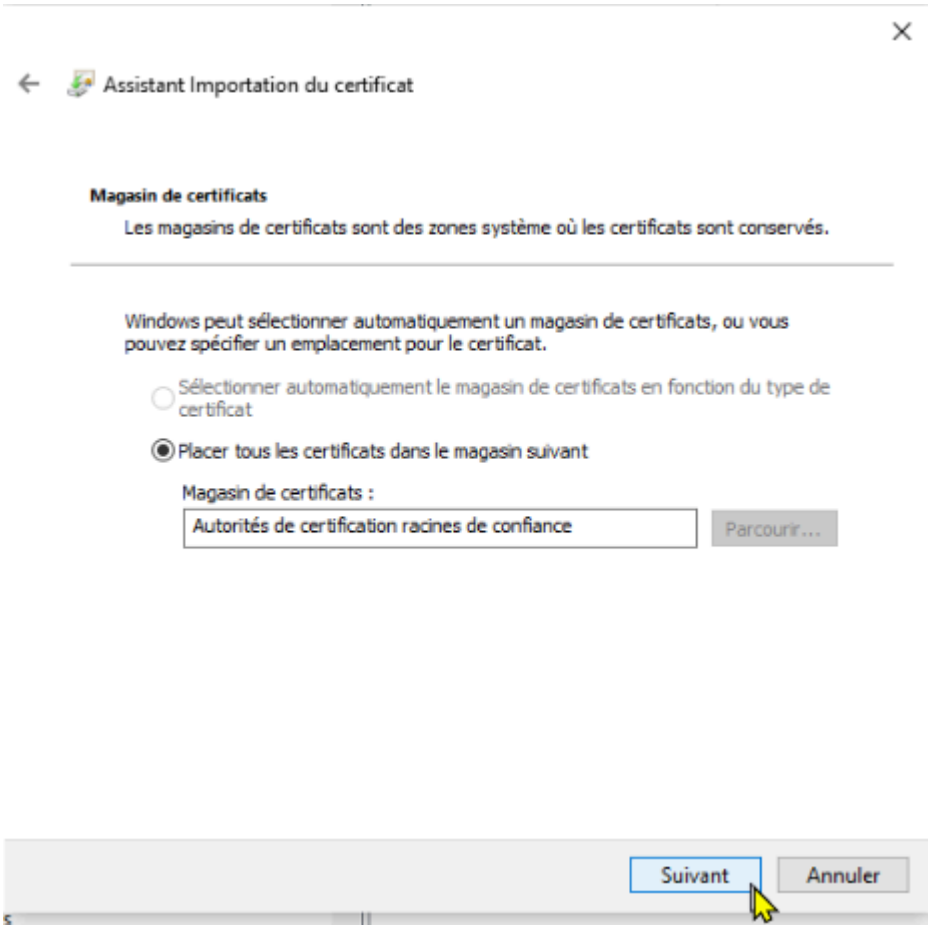


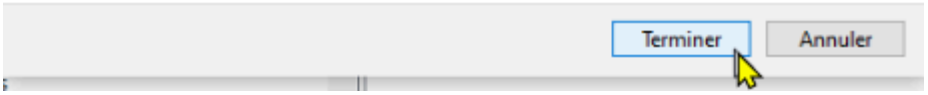
De retour dans l'assistant, parcourez le chemin jusqu'au certificat, en l'occurrence dans le dossier Téléchargements :



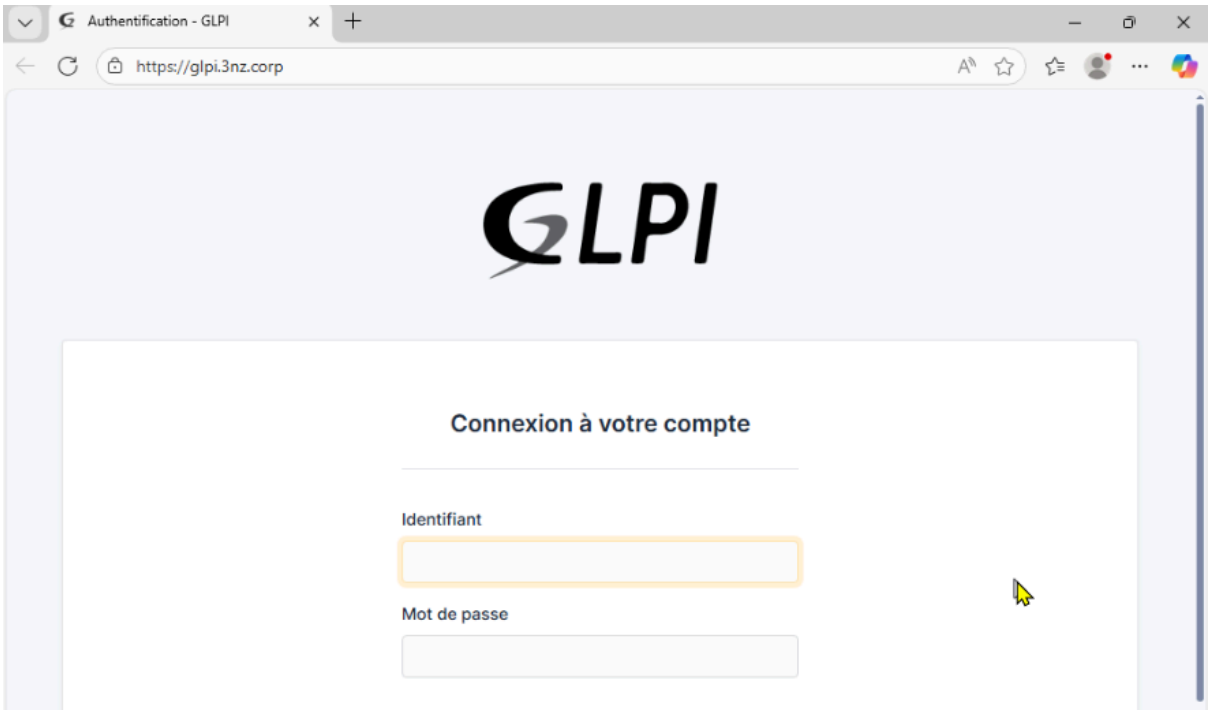

Ouvrir
« cmorel › Téléchargements
Rechercher dans : Télécharge...
Organiser
Nouveau dossier
Pictures
Ce PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Disque local (C:)
Réseau
Nom
Modifié le
Type
3NZ CORP
30/12/2025 13:13
nas-TrueNAS-13.0-U6.7-20251230120429
30/12/2025 12:04
Data
Nom du fichier :
3NZ CORP
Tous les fichiers (*.*)
Ouvrir
Annuler


Assistant Importation du certificat
Fichier à importer
Spécifiez le fichier à importer.
Nom du fichier :
C:\Users\cmorel\Downloads\3NZ CORP.crt
Parcourir...
Remarque : plusieurs certificats peuvent être stockés dans un même fichier aux formats suivants :
Échange d'informations personnelles- PKCS #12 (.PFX,.P12)
Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)
Magasin de certificats sérialisés Microsoft (.SST)
Suivant
Annuler


Assistant Importation du certificat
Magasin de certificats
Les magasins de certificats sont des zones système où les certificats sont conservés.
Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.
Sélectionner automatiquement le magasin de certificats en fonction du type de certificat
Placer tous les certificats dans le magasin suivant
Magasin de certificats :
Autorités de certification racines de confiance
Parcourir...
Suivant
Annuler



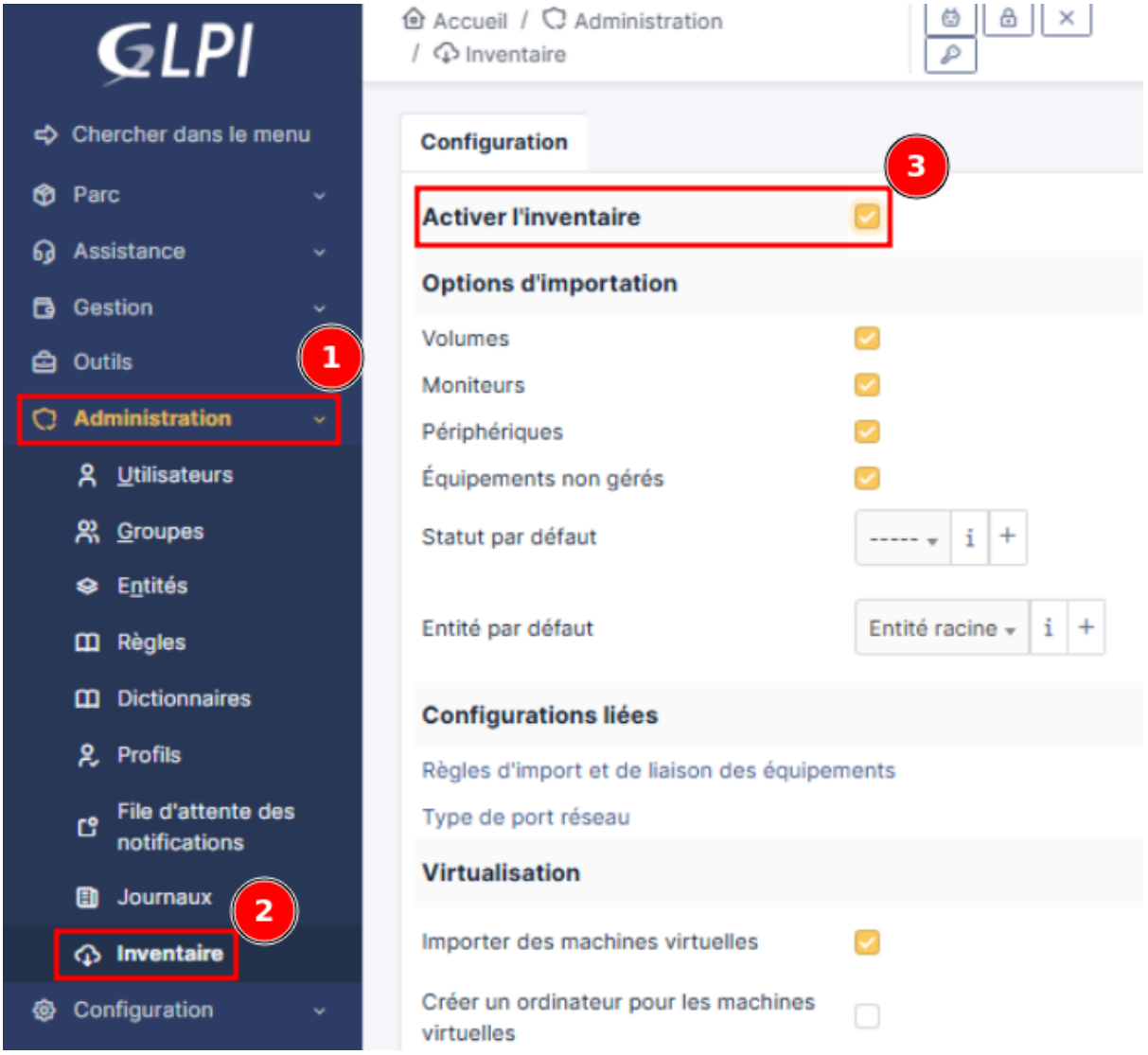
Et voilà ! Le certificat est accepté :



- Déploiement de l’agent GLPI via GPO

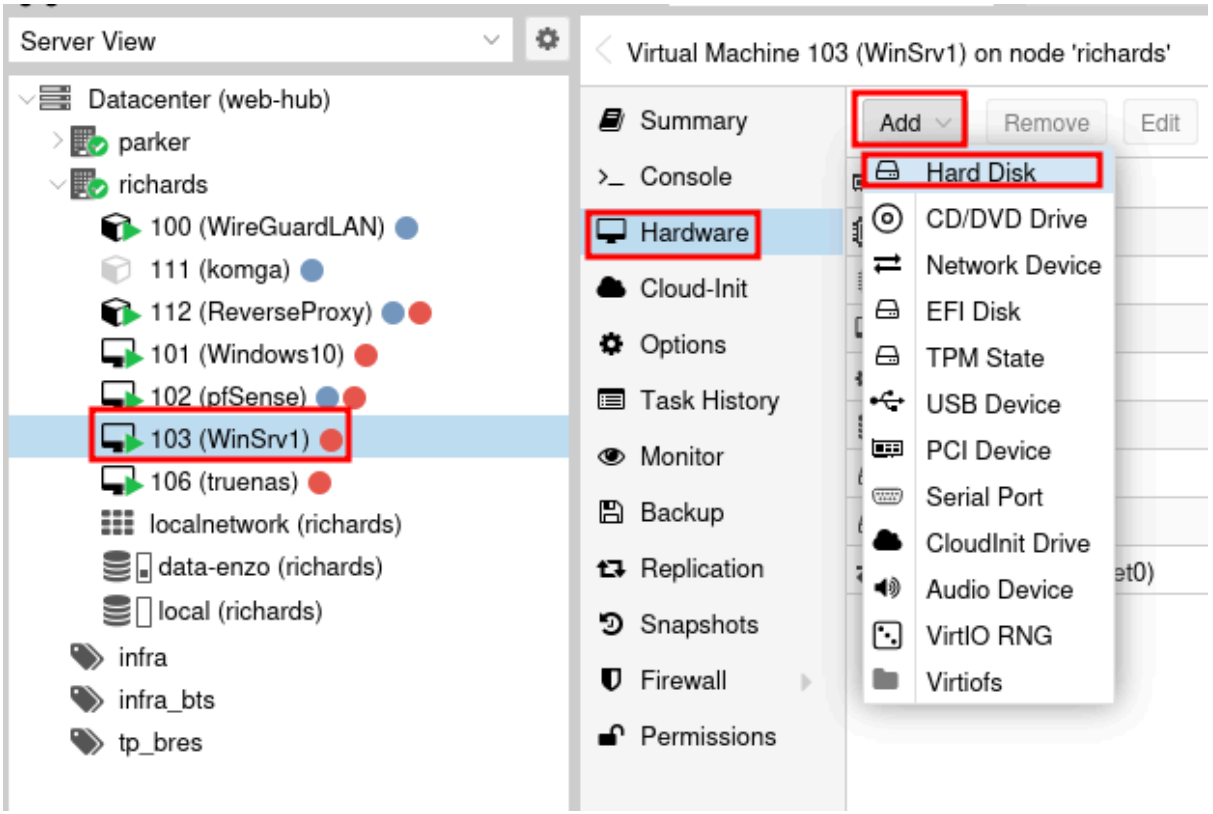
Déploiement agent glpi sur postes via GPO

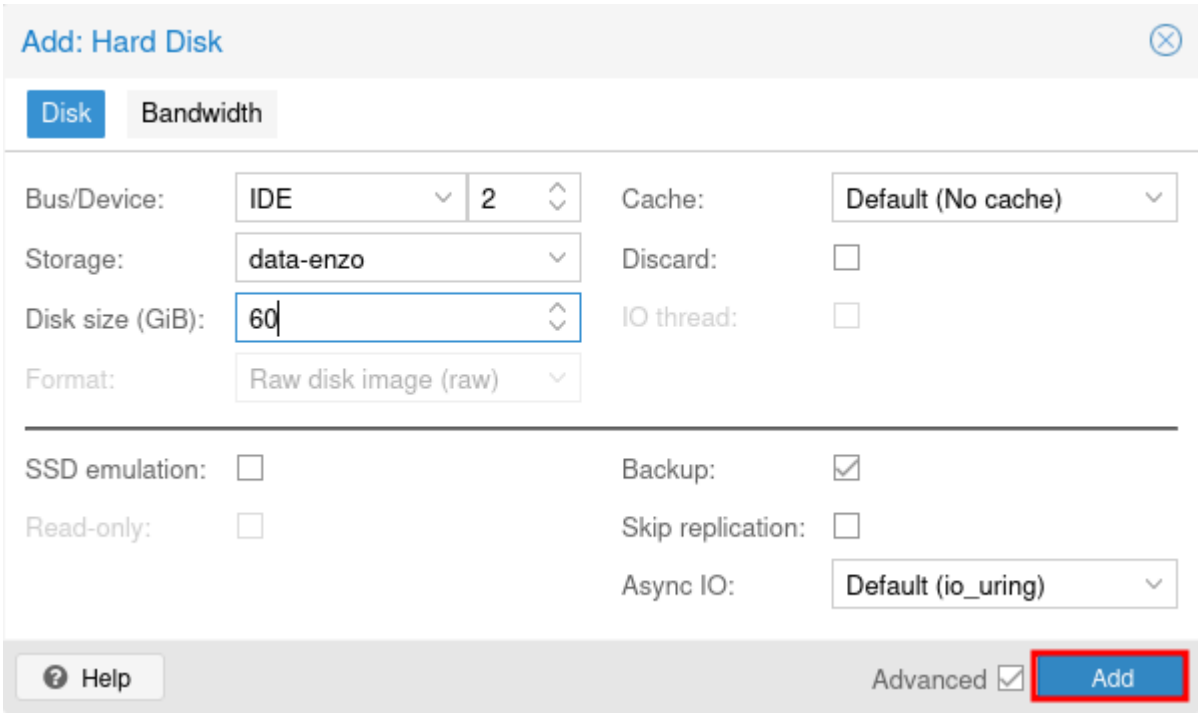
Activation de l’inventaire GLPI, se mettre en Super-Admin dans la base interne de GLPI puis :



Ensuite, sauvegardez votre modification.

Maintenant, sur le windows server éteint, je rajoute un disque :





Une fois ajouté, il faut l'initialiser :

```
PS C:\Users\Administrateur> Get-Disk

Number Friendly Name Serial Number                  HealthStatus         OperationalStatus      Total Size Partition
                                                                                                        Style
------ ------------- -------------                  ------------         -----------------      ---------- ----------
0      QEMU HARDDISK QM00001                        Healthy              Online                     60 GB MBR
1      QEMU HARDDISK QM00002                        Healthy              Online                     60 GB RAW


PS C:\Users\Administrateur> Initialize-Disk -Number 1 -PartitionStyle GPT
PS C:\Users\Administrateur> New-Partition -DiskNumber 1 -UseMaximumSize -DriveLetter D


   DiskPath :
\\?\ide#diskqemu_harddisk_____________________2.5+___#5&25b02e98&0&0.1.0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}

PartitionNumber  DriveLetter Offset                                        Size Type
---------------  ----------- ------                                        ---- ----
2                D           16777216                                  59.98 GB Basic
```

```
PS C:\Users\Administrateur> Format-Volume -DriveLetter D -FileSystem NTFS -NewFileSystemLabel "Data"

DriveLetter FriendlyName FileSystemType DriveType HealthStatus OperationalStatus SizeRemaining      Size
----------- ------------ -------------- --------- ------------ ----------------- -------------      ----
D           Data         NTFS           Fixed     Healthy      OK                    59.89 GB 59.98 GB
```

Création du dossier partagé :

New-Item -Path "D:\Agent-GLPI" -ItemType Directory

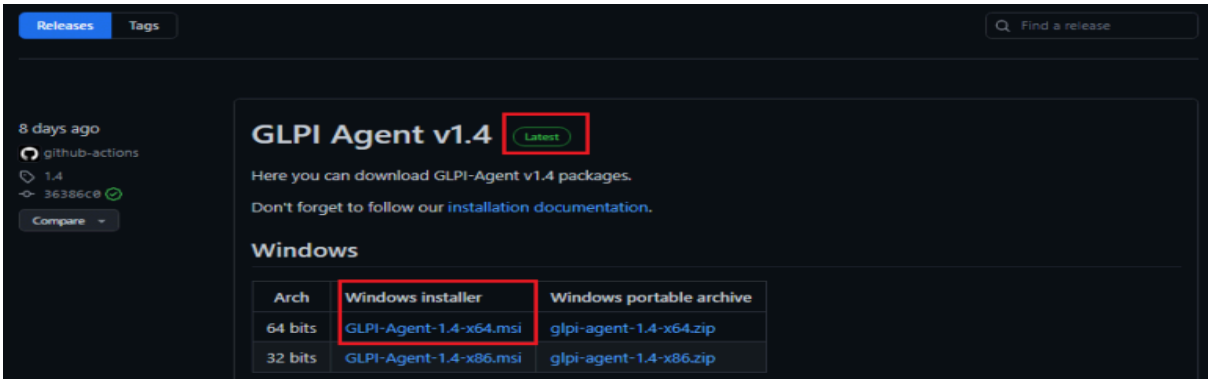
```
PS C:\Users\Administrateur> New-SmbShare -Name "Agent-GLPI" -Path "D:\Agent-GLPI" -FullAccess "Administrateurs" -ReadAcc
ess "Tout le monde"

Name       ScopeName Path          Description
----       --------- ----          -----------
Agent-GLPI *         D:\Agent-GLPI
```

J'enlève "Tout le monde" et j'ajoute "Ordinateurs du domaine" à la place :

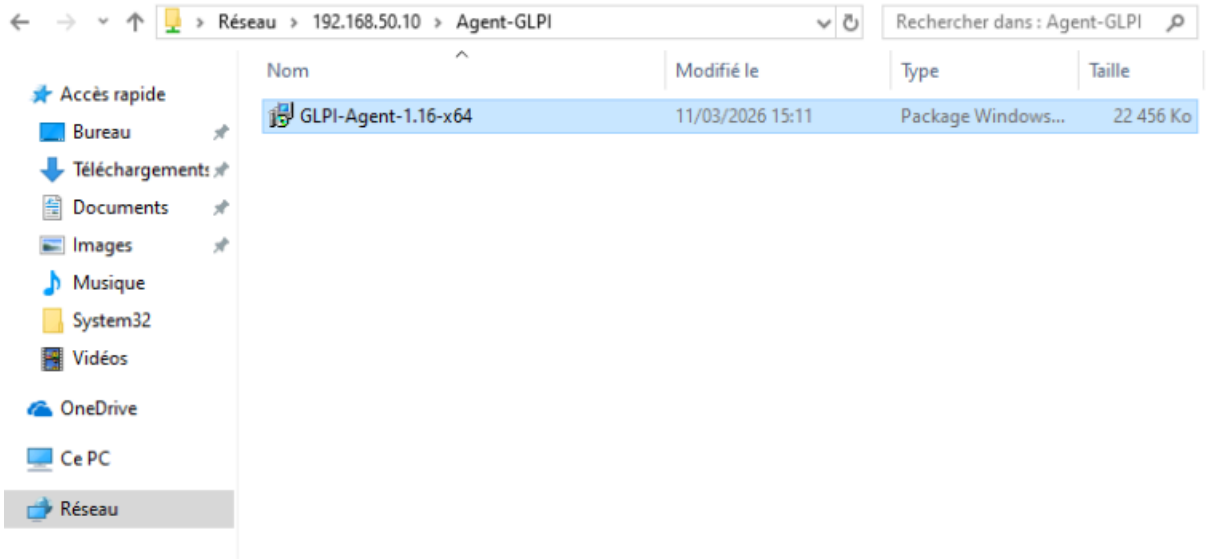
```
PS C:\Users\Administrateur> Revoke-SmbShareAccess -Name "Agent-GLPI" -AccountName "Tout le monde" -Force

Name       ScopeName AccountName             AccessControlType AccessRight
----       --------- -----------             ----------------- -----------
Agent-GLPI *         BUILTIN\Administrateurs Allow             Full
```

```
PS C:\Users\Administrateur> Grant-SmbShareAccess -Name "Agent-GLPI" -AccountName "Ordinateurs du domaine" -AccessRight R
ead -Force

Name       ScopeName AccountName               AccessControlType AccessRight
----       --------- -----------               ----------------- -----------
Agent-GLPI *         BUILTIN\Administrateurs    Allow             Full
Agent-GLPI *         3NZ\Ordinateurs du domaine Allow             Read
```

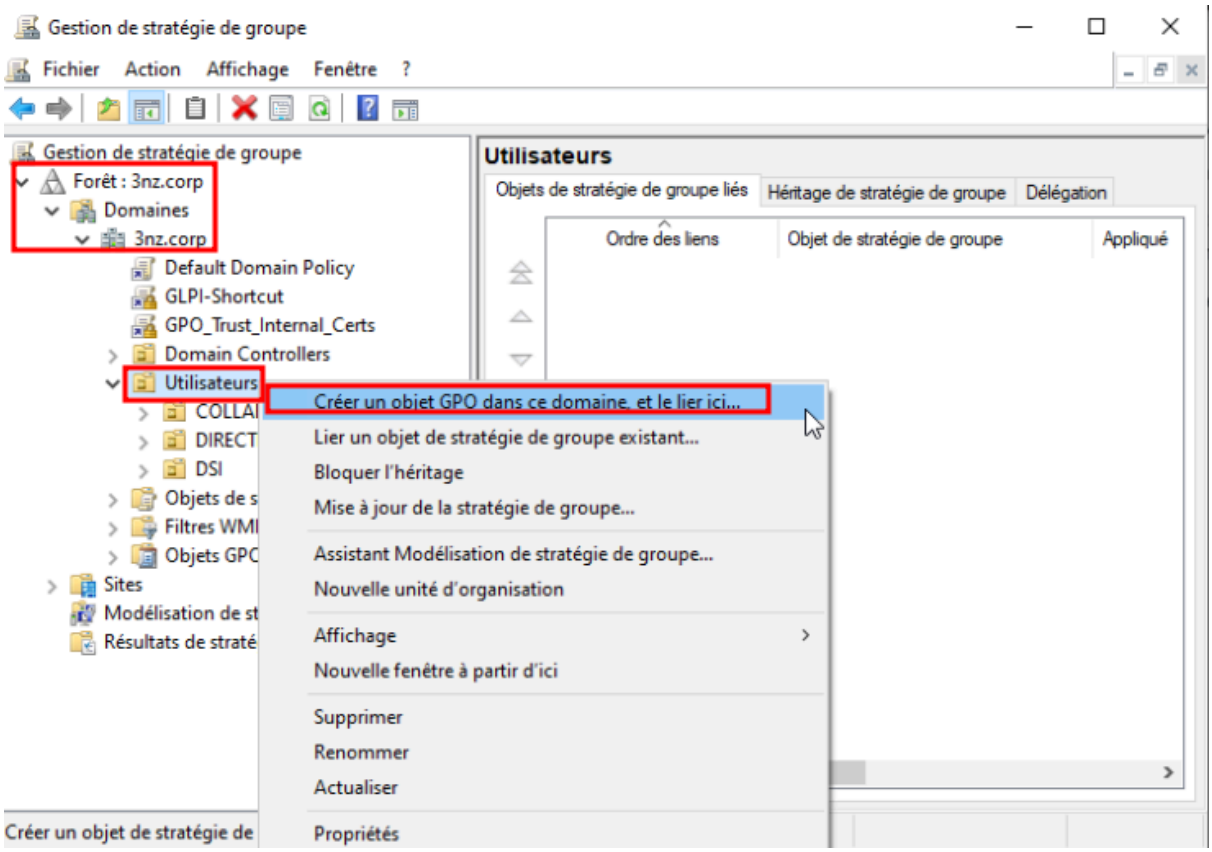
Une fois cela fait, je télécharge l'agent GLPI sur ce lien :
https://github.com/glpi-project/glpi-agent/releases/

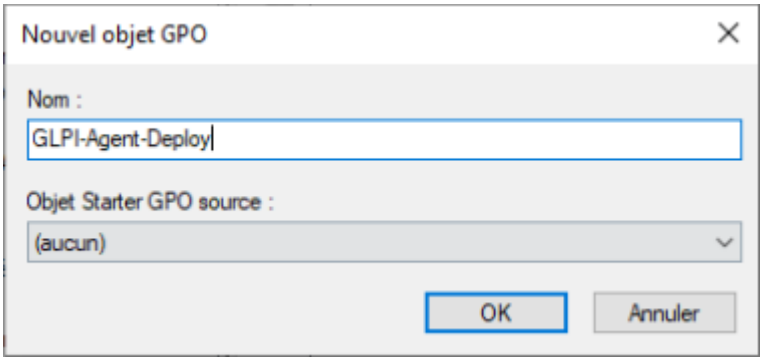


Je place le .msi dans le dossier Agent-GLPI :

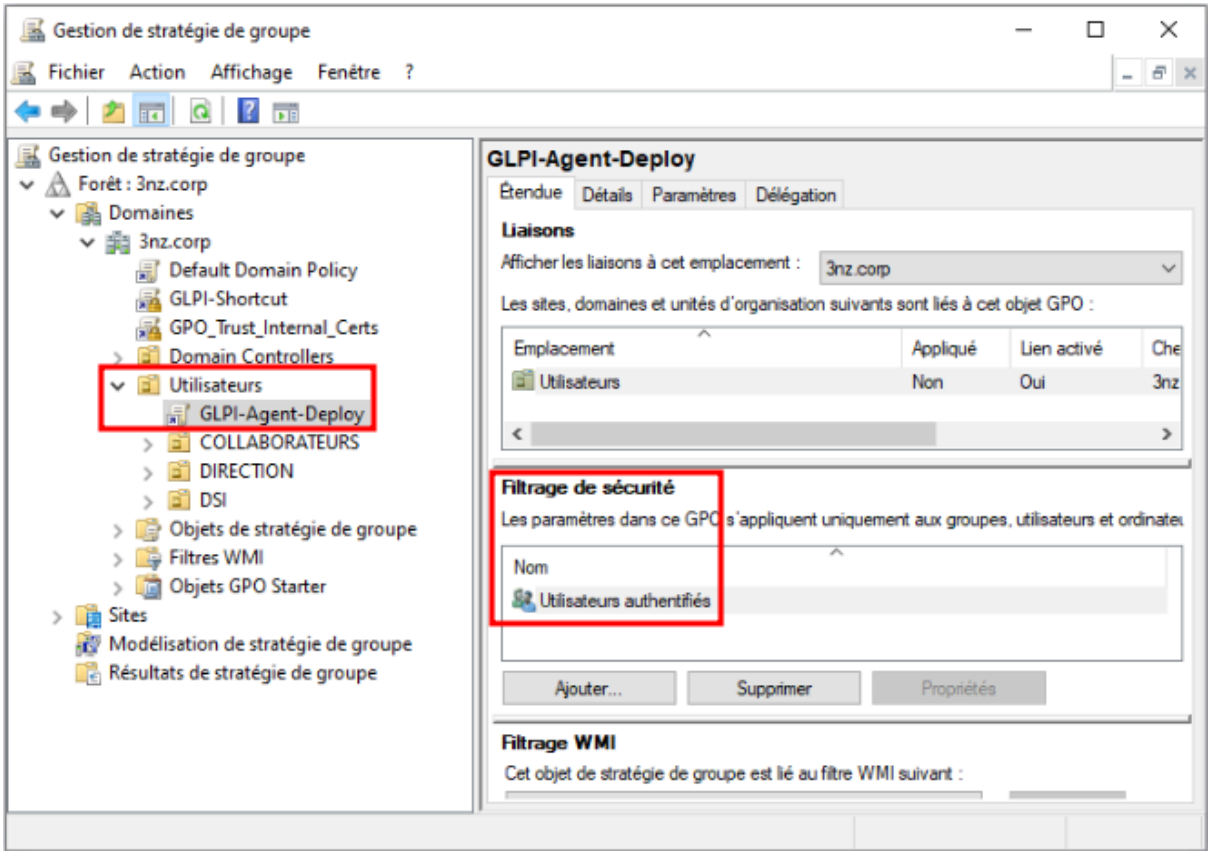


Ensuite, j'ouvre gestion de stratégie de groupe en admin

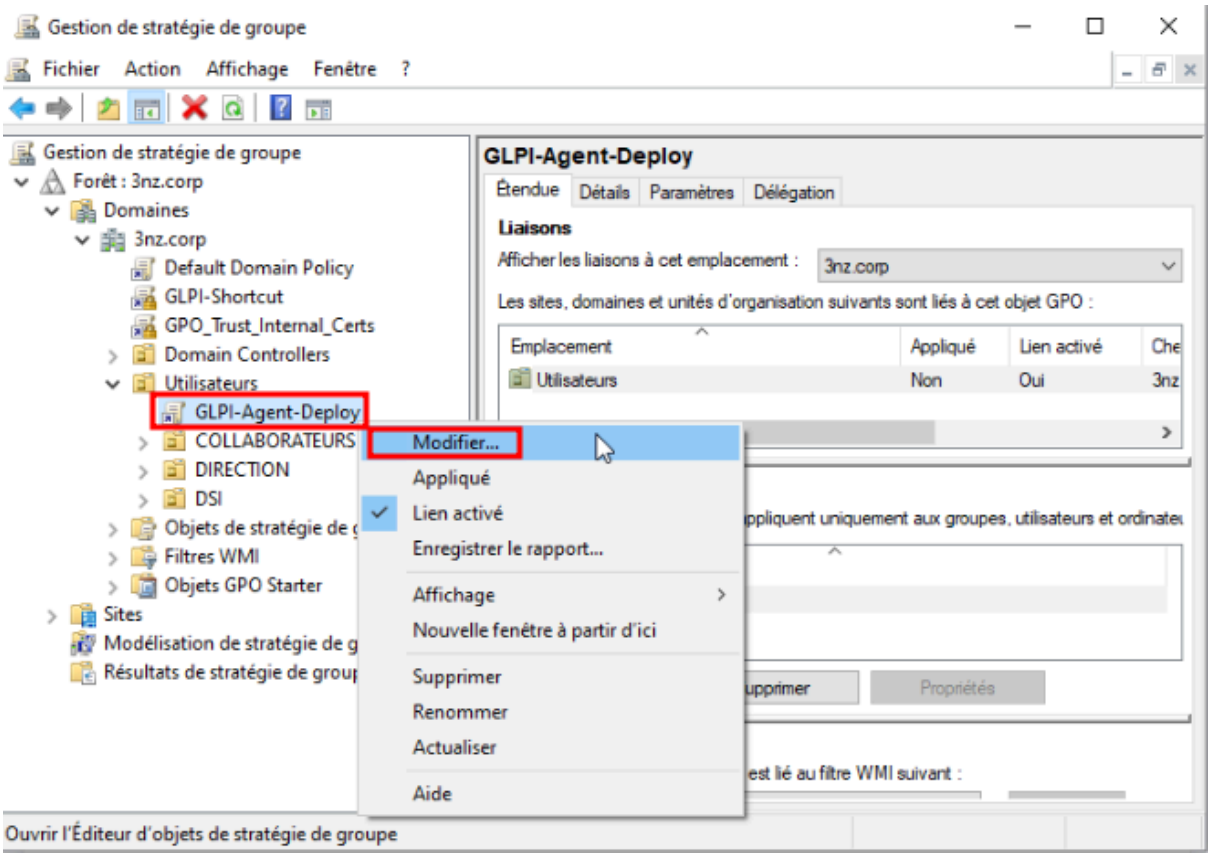


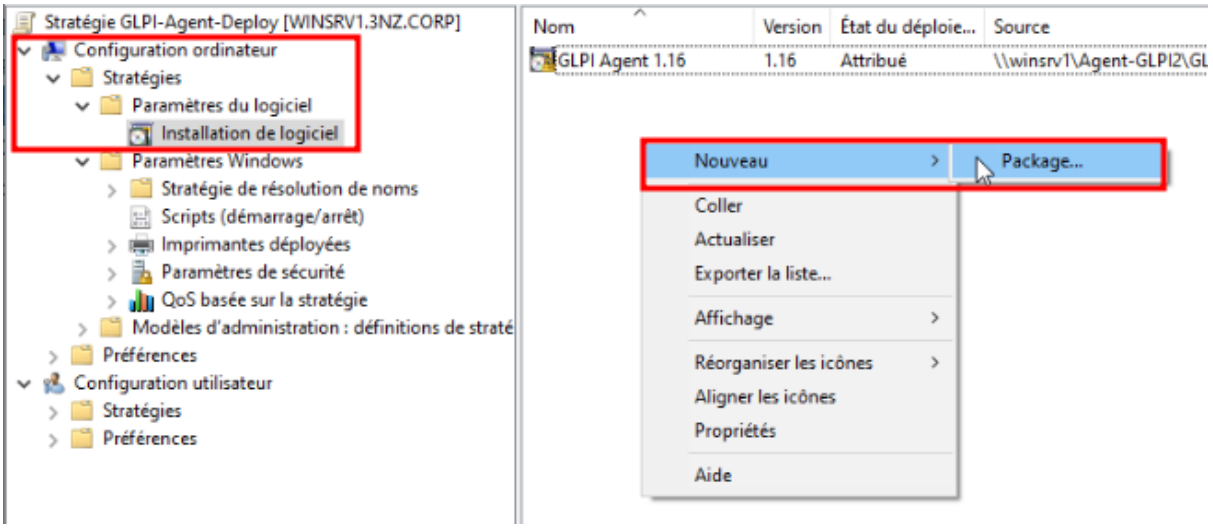


Ma GPO est bien créée dans mon OU utilisateurs, l'agent va donc se déployer à tous les utilisateurs/groupes présent dans l'OU Utilisateurs :

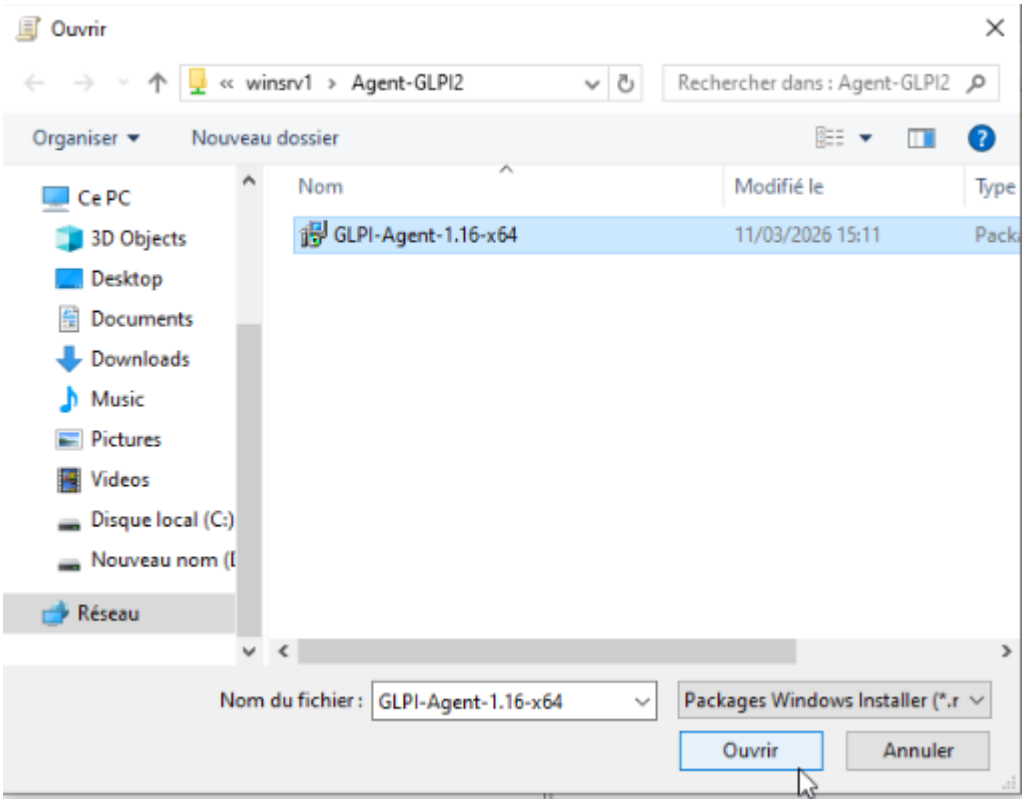


A ce stade, la GPO est vide, nous allons donc la remplir :

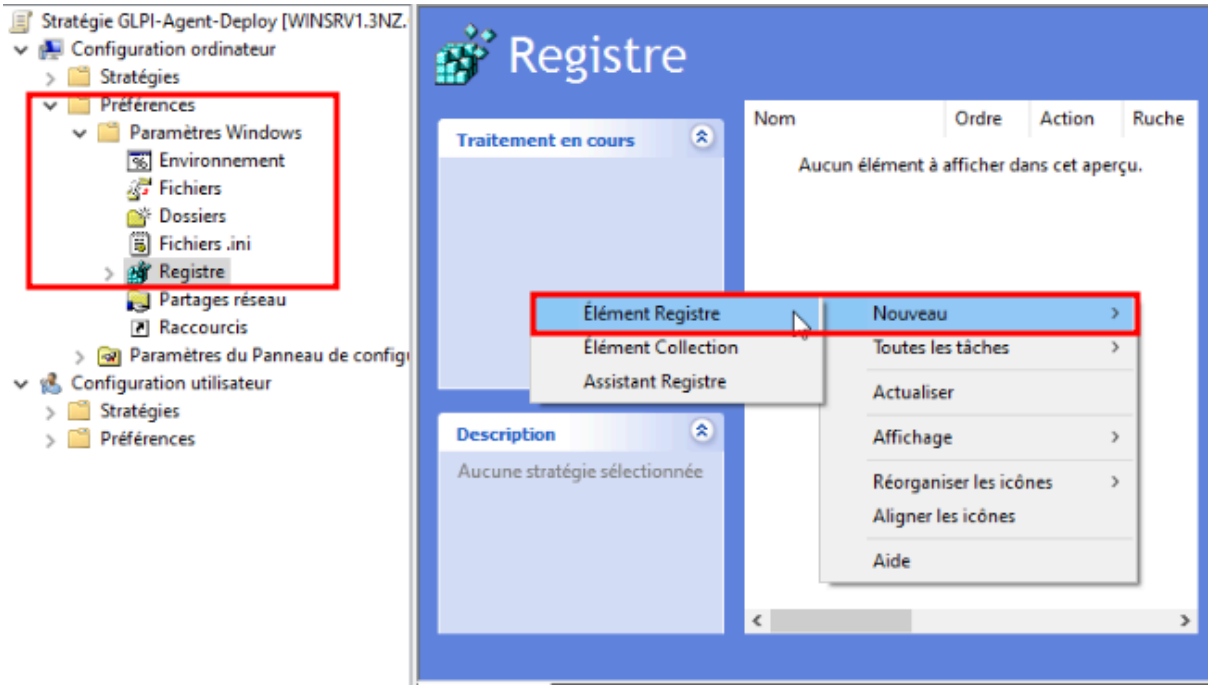




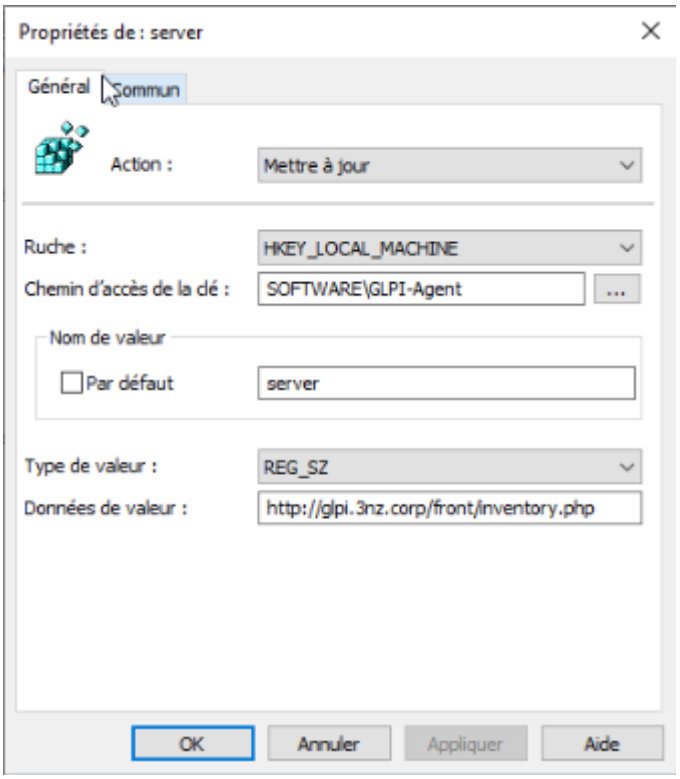
Ajouter le package de l'agent via le chemin réseau :



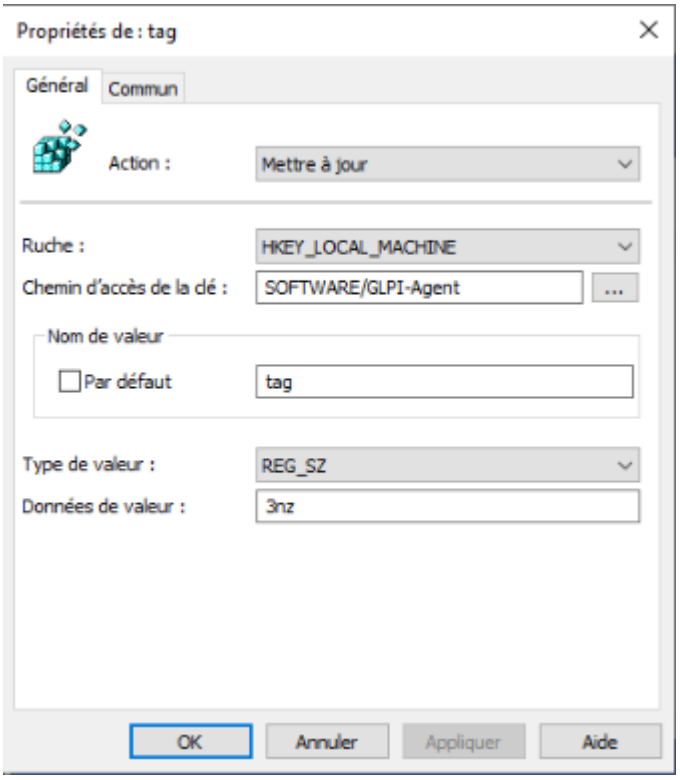
Modification d'une clé de registre afin de modifier les paramètres de l'agent GLPI avec la GPO :



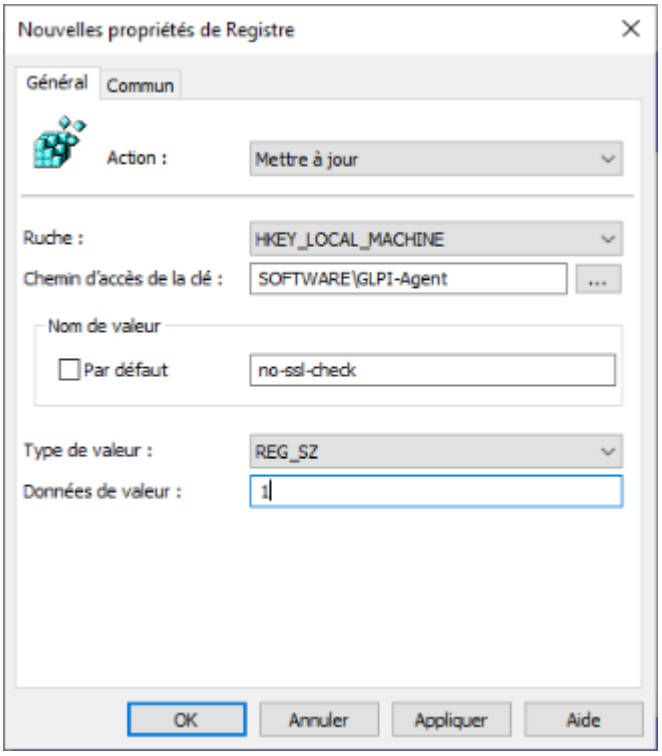
Comme ceci, appliquer, puis OK :



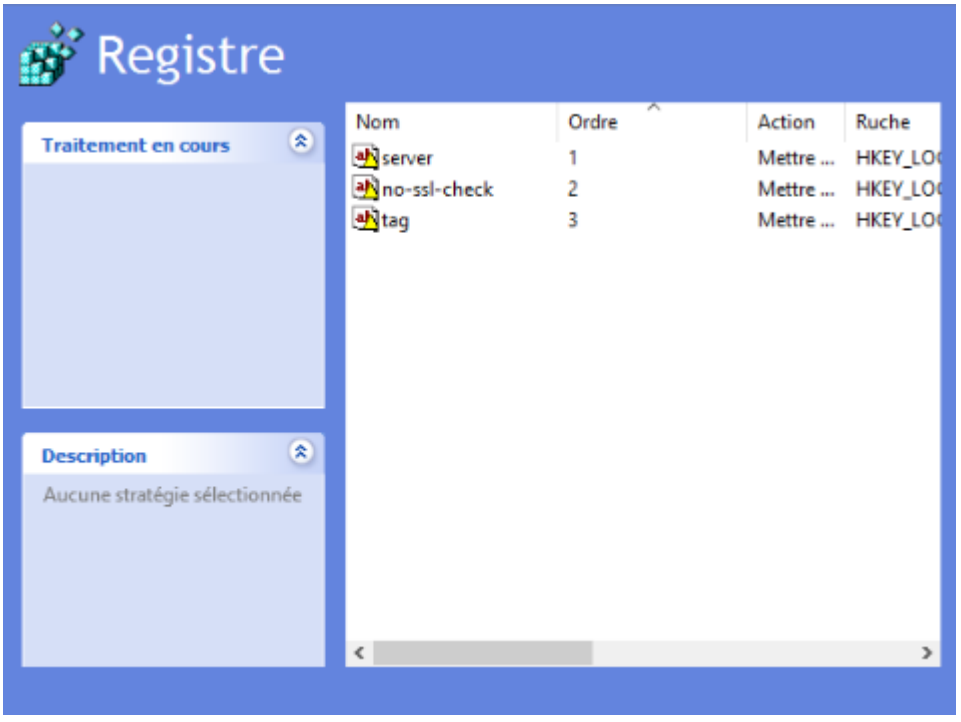
Répéter l'opération pour le tag :



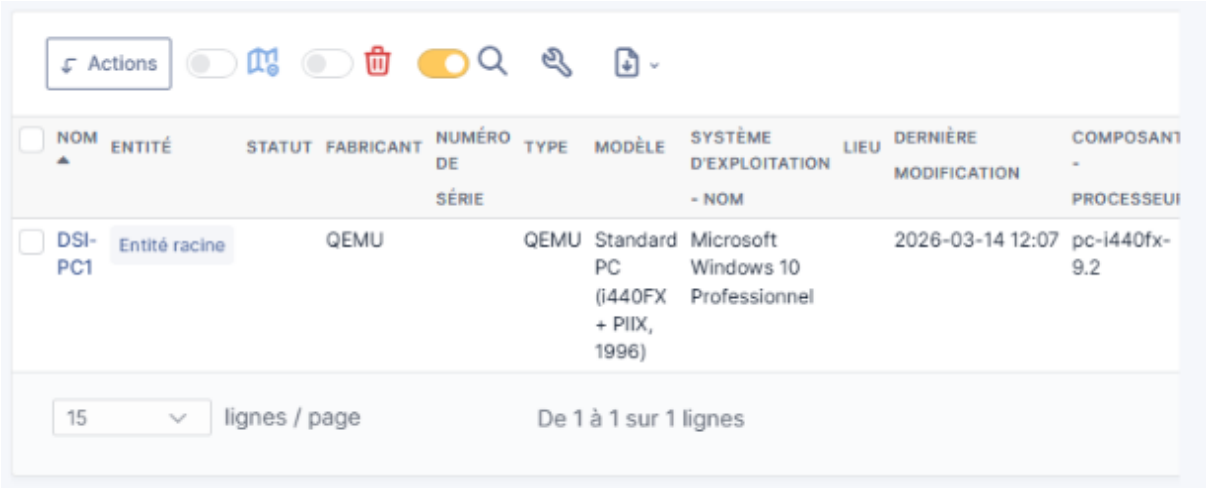
Avant que l'agent remonte, il faut faire une dernières modifications de clé de registre car la connexion sera bloqué à cause de mon certificat auto-signé, je modifie donc une nouvelle fois ma GPO :



Ensuite, je place mes clés dans le bon ordre :



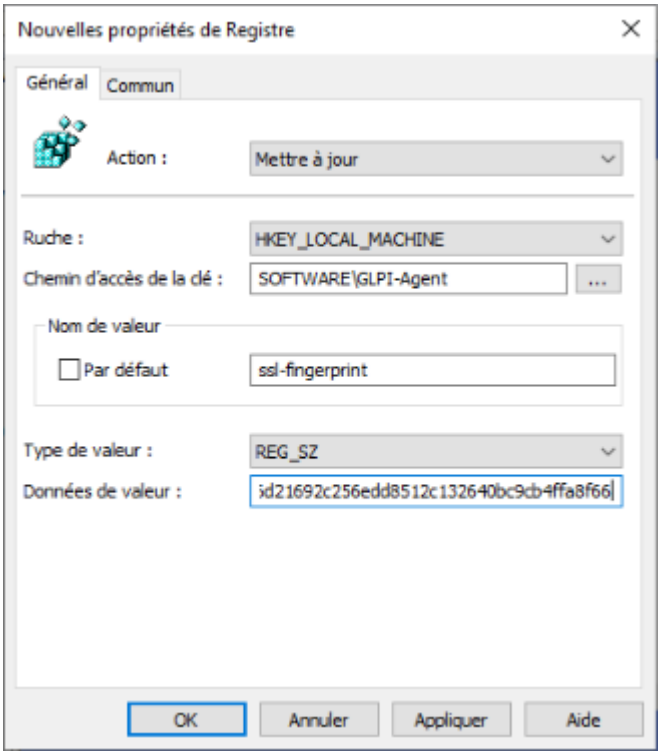
Le PC est correctement remonté !



Je vérifie les logs et l'agent me conseil de désactiver ma règle pour en faire une nouvelle qui autoriserait spécifiquement mon certificat :

```
[Sat Mar 14 12:05:22 2026][info] New inventory from DSI-PC1-2026-03-13-12-32-07 for server0
[Sat Mar 14 12:07:17 2026][info] [http client] SSL Client warning: Peer certificate not verified
[Sat Mar 14 12:07:17 2026][info] [http client] SSL Client info: Cert-Issuer: '/C=FR/ST=Occitanie/L=Montpellier/O=3nz Corp/OU=IT/CN=glpi.3nz.corp', Cert-Subject: '/C=FR
[Sat Mar 14 12:07:17 2026][info] [http client] SSL server certificate fingerprint: sha256$d733c6ba14fe7e2a2be5d20e5e6d21692c256edd8512c132640bc9cb4ffa8f66
[Sat Mar 14 12:07:17 2026][info] [http client] You can set it in conf as 'ssl-fingerprint' and disable 'no-ssl-check' option to trust that server certificate
```

Et voici :



Pourquoi faire ce changement ?

Option A : Rester comme ça (no-ssl-check = 1)

- **Avantage** : C'est simple. Si je renouvelle mon certificat GLPI l'année prochaine, rien ne casse.
- **Inconvénient** : C'est un peu moins sécurisé (vulnérable aux attaques de type "Man-in-the-middle" à l'intérieur de mon réseau).

Option B : Utiliser le ssl-fingerprint (Recommandé par les logs)

- **Avantage** : Très sécurisé, même avec un certificat auto-signé.
- **Inconvénient** : Si je change le certificat de mon serveur GLPI, **tous mes agents arrêteront de remonter** jusqu'à ce que je mette à jour l'empreinte dans la GPO.