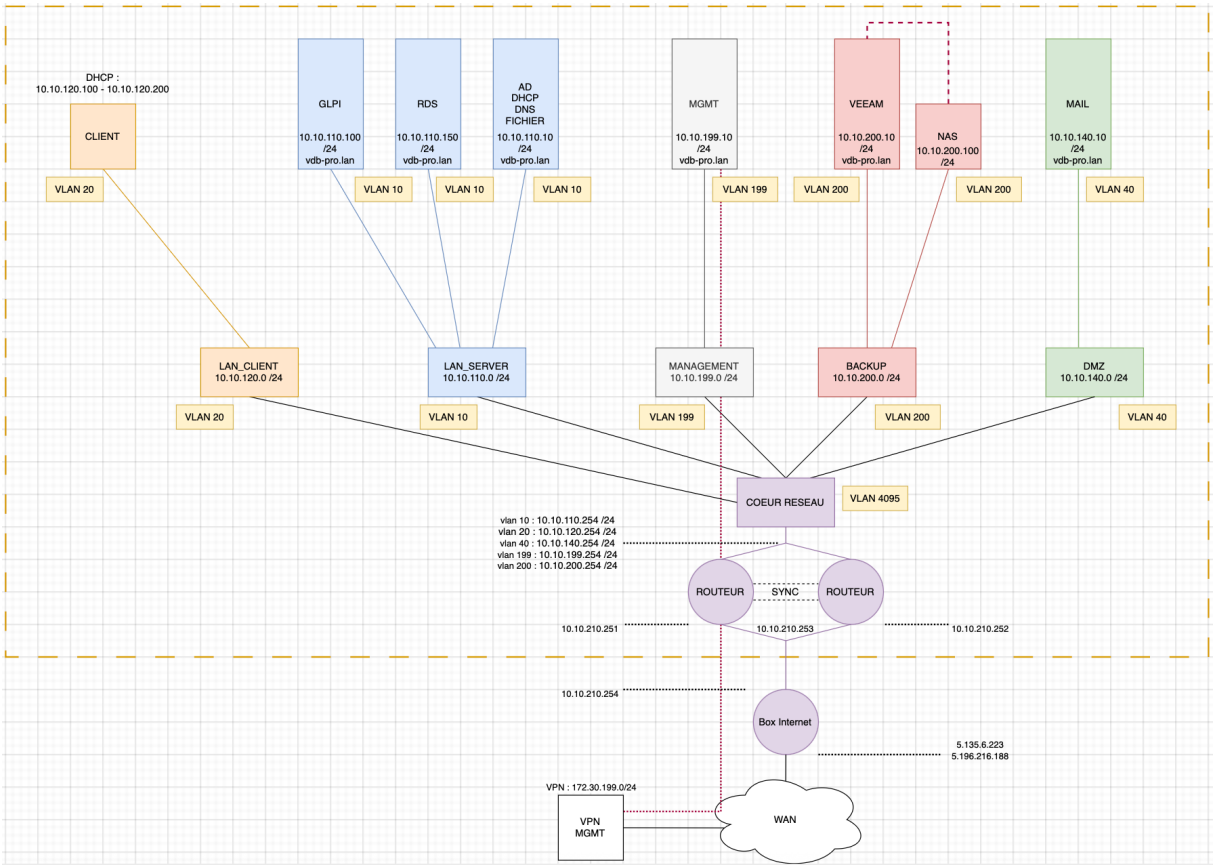
Réalisation d’une maquette informatique complète dans le cadre de mon BTS

Au cours de ma formation en BTS, j’ai conçu et mis en œuvre une maquette informatique complète. Ce projet incluait la création d’un schéma réseau détaillé, la mise en place de plusieurs machines virtuelles (VM), la configuration de règles de pare-feu adaptées, ainsi que l’intégration de nombreuses réalisations professionnelles en lien direct avec cette infrastructure. Ce travail m’a permis de mettre en pratique mes compétences en administration réseau, sécurité informatique et virtualisation, tout en répondant à des objectifs techniques concrets.

Schéma réseau de la maquette

Vous trouverez ci-dessous une représentation complète du schéma réseau utilisé pour la réalisation de ma maquette. Ce schéma détaille l’ensemble des interconnexions entre les machines virtuelles, les cartes réseau, les VLAN (le cas échéant), ainsi que les équipements réseau simulés ou physiques impliqués.



Liste des machines virtuelles (VM) créées dans l'hyperviseur ESXi

L'ensemble des machines virtuelles déployées sur mon serveur ESXi dans le cadre de cette maquette est listé ci-dessous, avec leurs caractéristiques principales (nom, rôle, système d'exploitation, IP, etc.) :

Machine virtuelle	État	Espace utilisé	SE invité	Nom d'hôte	CPU d'hôte	Mémoire d'hôte
VP-PFSENSE	Norm...	11,18 Go	FreeBSD 13 (64 bits)	Inconnu	222 MHz	2,04 Go
VP-DC1	Norm...	27,04 Go	Microsoft Windows Serve...	VP-DC1.vdb-pro.lan	132 MHz	6,09 Go
VP-EXCHANGE	Norm...	80,49 Go	Microsoft Windows Serve...	VP-EXCHANGE.vdb-pro...	433 MHz	10,09 Go
VP-CLIENT	Norm...	4,08 Go	Microsoft Windows 10 (64...	Inconnu	8 MHz	4,06 Go
VP-BACKUP	Norm...	58,27 Go	Microsoft Windows Serve...	VP-BACKUP	833 MHz	6,07 Go
VP-MGMT	Norm...	4,08 Go	Microsoft Windows 10 (64...	PO-MGMT.vdb-pro.lan	70 MHz	4,07 Go
VP-GLPI	Norm...	5,95 Go	Debian GNU/Linux 12 (64 ...	VP-GLPI	13 MHz	3,02 Go
VP-NEXTCLOUD	Norm...	6,03 Go	Debian GNU/Linux 12 (64 ...	vp-debian	13 MHz	2,05 Go
VP-RDS1	Norm...	80,25 Go	Microsoft Windows Serve...	VP-RDS1.vdb-pro.lan	31 MHz	10,2 Go
VP-TrueNAS	Norm...	5,76 Go	FreeBSD 13 (64 bits)	truenas.local	56 MHz	4 Go
VP-PFSENSE2	Norm...	2,08 Go	FreeBSD 13 (64 bits)	Inconnu	55 MHz	2,01 Go

Cartes réseau configurées dans ESXi pour cette maquette

Les interfaces réseau virtuelles configurées dans l'hyperviseur ESXi sont les suivantes :

Nom	Ports actifs	ID du VLAN	Type	vSwitch	VM
WAN	2	0	Groupe de ports standard	vSwitch0	2
MGMT LAN	1	0	Groupe de ports standard	vSwitch0	S/O
VLANCLIENT	1	20	Groupe de ports standard	vSwitchLAN	1
VLANBACKUP	3	200	Groupe de ports standard	vSwitchLAN	S/O
VLANMGMT	1	199	Groupe de ports standard	vSwitchLAN	1
LAN	2	4095	Groupe de ports standard	vSwitchLAN	2
VLANDMZ	1	40	Groupe de ports standard	vSwitchLAN	1
VLANSERVER	4	10	Groupe de ports standard	vSwitchLAN	4

Règles de pare-feu et de filtrage mises en place

Pour sécuriser les communications entre les différentes machines virtuelles et les segments de réseau, les règles suivantes ont été définies :

Firewall / Rules / WAN

Floating | WAN | LAN | VLANSERVER | VLANCLIENT | VLANDMZ | VLANMGMT | VLANBACKUP | SYNC | OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
MGMT										
0/25 KiB	IPv4 UDP	*	*	10.10.210.253	10999	*	none		VPN MGMT	
0/0 B	IPv4 TCP	*	*	WAN address	10001	*	none		PF MGMT	
7/2.12 MiB	IPv4 TCP	*	*	10.10.210.253	10001	*	none		PF MGMT	
VP-EXCHANGE										
0/16.85 MiB	IPv4 TCP	*	*	VP_EXCHANGE	443 (HTTPS)	*	none		NAT	
0/1.39 MiB	IPv4 TCP	*	*	VP_EXCHANGE	80 (HTTP)	*	none		NAT	
0/680 KiB	IPv4 TCP	*	*	VP_EXCHANGE	25 (SMTP)	*	none		NAT	
0/0 B	IPv4 *	*	*	*	*	*	none		block any	

Firewall / Rules / VLANCLIENT

Floating | WAN | LAN | VLANSERVER | VLANCLIENT | VLANDMZ | VLANMGMT | VLANBACKUP | SYNC | OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
0/0 B	IPv4 *	*	*	*	*	*	none			

Firewall / Rules / VLANSERVER

Floating | WAN | LAN | VLANSERVER | VLANCLIENT | VLANDMZ | VLANMGMT | VLANBACKUP | SYNC | OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 ICMP any	*	*	*	*	*	none		PING	
0/16.03 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		HTTPS	
0/98.18 MiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		HTTP	
1/5.11 MiB	IPv4 TCP/UDP	VP_AD1	*	*	*	*	none		FLUX AD	
0/27 KiB	IPv4 UDP	VP_GLPI	*	*	123 (NTP)	*	none		GLPI TO NTP	
0/26 KiB	IPv4 UDP	VP_NEXTCLOUD	*	*	123 (NTP)	*	none		NEXTCLOUD TO NTP	
0/211 KiB	IPv4 *	*	*	*	*	*	none		Block any	

Firewall / Rules / VLANDMZ

Floating | WAN | LAN | VLANSERVER | VLANCLIENT | VLANDMZ | VLANMGMT | VLANBACKUP | SYNC | OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
0/1.54 GiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		HTTPS	
0/29.65 MiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		HTTP	
15/7.44 GiB	IPv4 TCP/UDP	AD_to_EXCHANGE	*	AD_to_EXCHANGE	*	*	none			
0/1.16 MiB	IPv4 *	*	*	*	*	*	none			

Firewall / Rules / VLANBACKUP

Floating | WAN | LAN | VLANSERVER | VLANCLIENT | VLANDMZ | VLANMGMT | VLANBACKUP | SYNC | OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
0/1.62 MiB	IPv4 UDP	VP_BACKUP	*	VP_AD1	53 (DNS)	*	none		BACKUP TO DNS	
0/52 KiB	IPv4 UDP	VP_BACKUP	*	*	123 (NTP)	*	none		BACKUP TO NTP	
0/105.01 MiB	IPv4 TCP	VP_BACKUP	*	*	BACKUP_TO_ESXi	*	none		BACKUP TO ESXi	
0/1.95 MiB	IPv4 *	*	*	*	*	*	none		block any	

Firewall / Rules / OpenVPN

Floating | WAN | LAN | VLANSERVER | VLANCLIENT | VLANDMZ | VLANMGMT | VLANBACKUP | SYNC | OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/117 KiB	IPv4 TCP	*	*	10.10.199.10	3389 (MS RDP)	*	none		RDP MGMT	
0/7 KiB	IPv4 *	*	*	*	*	*	none		block any	

Firewall / Rules / VLANMGMT

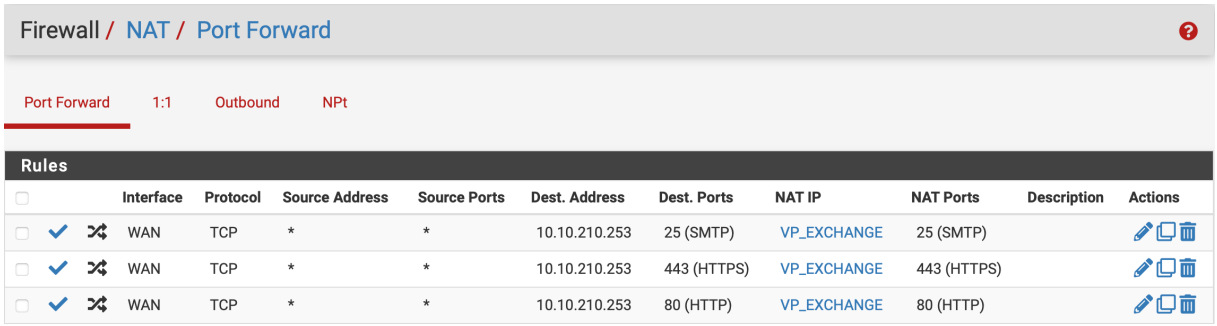
Floating | WAN | LAN | VLANSERVER | VLANCLIENT | VLANDMZ | VLANMGMT | VLANBACKUP | SYNC | OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0/32.72 MiB	IPv4 ICMP any	*	*	*	*	*	none			
✓	2/24.45 MiB	IPv4 TCP/UDP	AD_to_MGMT	*	AD_to_MGMT	*	*	none		AD to MGMT	
PfSense											
✓	0/0 B	IPv4 TCP	VP_MGMT	*	10.10.210.254	65443	*	none		MGMT PF BTSSIO	
✓	0/0 B	IPv4 TCP	VP_MGMT	*	10.10.199.254	10001	*	none		MGMT PF MGMT	
✓	0/0 B	IPv4 TCP	VP_MGMT	*	10.10.199.252	10001	*	none		MGMT PF MGMT 2	
✓	0/0 B	IPv4 TCP	VP_MGMT	*	10.10.199.251	10001	*	none		MGMT PF MGMT 1	
MGMT TO HTTP/HTTPS											
✓	0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
✓	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
✓	0/0 B	IPv4 TCP	VP_MGMT	*	10.10.200.100	80 (HTTP)	*	none		MGMT HTTP TRUENAS TEMP	
✓	0/0 B	IPv4 TCP	VP_MGMT	*	10.10.200.100	443 (HTTPS)	*	none		MGMT HTTP TRUENAS TEMP	
✓	0/0 B	IPv4 TCP	VP_MGMT	*	10.10.110.100	80 (HTTP)	*	none		MGMT HTTP GLPI	
✓	0/0 B	IPv4 TCP	VP_MGMT	*	10.10.110.100	443 (HTTPS)	*	none		MGMT HTTPS GLPI	
✓	0/0 B	IPv4 TCP	VP_MGMT	*	10.10.110.101	80 (HTTP)	*	none		MGMT HTTP NEXTCLOUD TEMP	
MGMT TO NETWORK											
✓	0/0 B	IPv4 TCP/UDP	*	*	VLANSERVER subnets	MGMT	*	none		MGMT SERVER	
✓	0/0 B	IPv4 TCP/UDP	*	*	VLANCLIENT subnets	MGMT	*	none		MGMT CLIENT	
✓	0/0 B	IPv4 TCP/UDP	*	*	VLANDMZ subnets	MGMT	*	none		MGMT DMZ	
✓	0/0 B	IPv4 TCP/UDP	*	*	VLANMGMT subnets	MGMT	*	none		MGMT MGMT	
✓	0/0 B	IPv4 TCP/UDP	*	*	VLANBACKUP subnets	MGMT	*	none		MGMT BACKUP	
✗	0/4.72 MiB	IPv4 *	*	*	*	*	*	none		block any	

Règles de traduction d'adresses (NAT)

Des règles NAT ont été mises en œuvre pour permettre aux machines internes d'accéder à Internet ou d'être accessibles depuis l'extérieur, tout en masquant leur IP privée :



	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
	WAN	TCP	*	*	10.10.210.253	25 (SMTP)	VP_EXCHANGE	25 (SMTP)		
	WAN	TCP	*	*	10.10.210.253	443 (HTTPS)	VP_EXCHANGE	443 (HTTPS)		
	WAN	TCP	*	*	10.10.210.253	80 (HTTP)	VP_EXCHANGE	80 (HTTP)		

Réalisations professionnelles liées à la maquette

Les compétences techniques et professionnelles mises en œuvre dans le cadre de cette maquette sont les suivantes :

BTS Services informatiques aux organisations- SISR

Session 2025

E5 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :

Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- **Layer Bureautique et Informatique** est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro.
- La problématique principale réside dans le besoin garantir une **haute disponibilité** de ses services informatiques pour l'ensemble de ses utilisateurs. Afin d'assurer la continuité d'activité, tous les services doivent rester accessibles à tout moment, sans interruption, même en cas de défaillance d'un composant réseau clé, tel qu'un pare-feu.
- La solution choisie consiste à déployer un second pare-feu pfSense pour assurer la haute disponibilité (HA) du réseau. Grâce à l'utilisation d'adresses IP virtuelles (VIP), de la synchronisation pfsync et du service CARP, la continuité d'accès aux services est garantie en cas de défaillance d'un équipement.

Intitulé de la réalisation professionnelle

Haute disponibilité réseau : installation d'un cluster pfSense

Période de réalisation : 20/08/24- 21/08/24 **Lieu :** AUXERRE

Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE
- GERER LE PATRIMOINE INFORMATIQUE

Conditions de réalisation

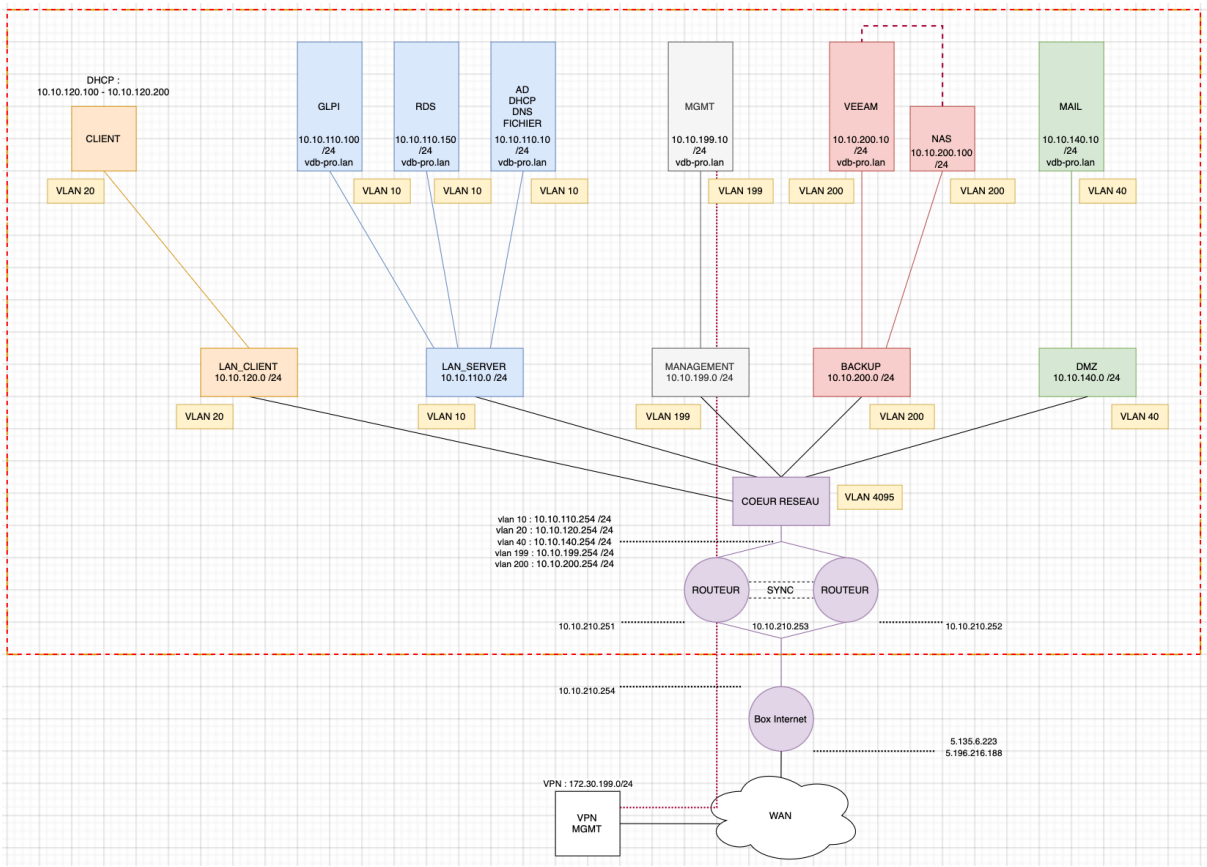
- **Ressources disponibles (Situation avant RP)**
  L'infrastructure disposait d'un serveur ESXi opérationnel pour l'hébergement des différents services de l'entreprise. Un seul pare-feu pfSense était en place pour gérer l'ensemble des flux réseau, assurer la sécurité et garantir la disponibilité des services.
- **Résultats attendus (Situation après RP)**
  Après la mise en place de la haute disponibilité avec pfSense, le réseau de l'entreprise reste opérationnel même en cas de panne d'un pare-feu, grâce à une bascule automatique et transparente, garantissant ainsi une continuité d'accès aux services.
- **Durée de réalisation**
  L'intervention a duré 2 jours, comprenant l'installation, la configuration, la sécurisation ainsi que la phase de tests de la solution. La partie la plus longue a été la gestion des différents réseaux un par un afin d'éviter toute coupure générale des services et ainsi prévenir un arrêt de la production.

Modalités d'accès à cette réalisation professionnelle.

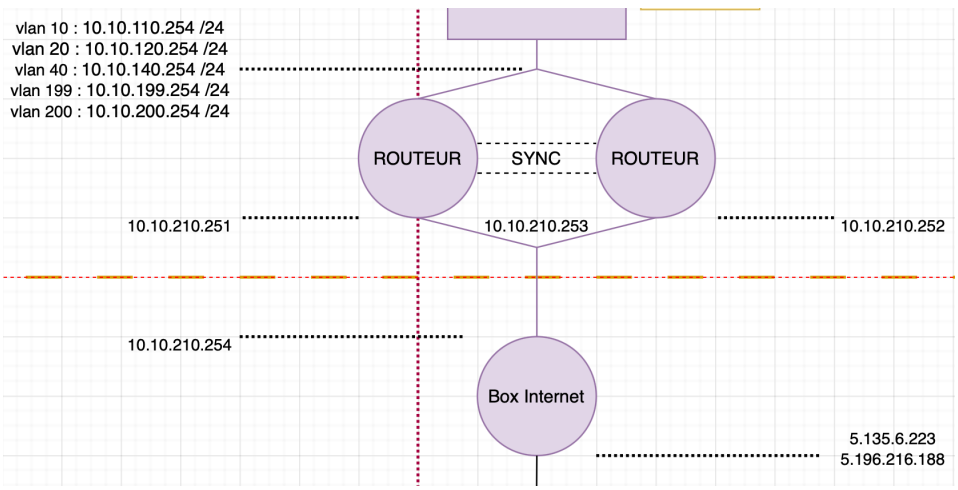
https://portfolio.vdb-pro.fr mdp : *Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

Dans le cadre de ma mission, j'ai réalisé un projet professionnel visant à assurer la haute disponibilité du réseau de l'entreprise. Pour cela, j'ai déployé une solution basée sur pfSense en mode CARP, permettant la mise en place d'un cluster de pare-feux pour garantir la redondance et la continuité des services. Ce projet m'a permis de développer des compétences en gestion de réseau, administration de pare-feu, sécurité des infrastructures et haute disponibilité.



L'élément le plus important dans ce schéma est la partie réseau, en particulier l'intégration des pare-feux pfSense.



Configuration du premier PfSense

Je commence par me connecter au premier pfSense déjà en place. Je configure les adresses IP de toutes les interfaces en terminant par .251, ce qui permet de mémoriser facilement qu'il s'agit du pfSense principal (pfSense 1 = .251). J'ajoute ensuite une nouvelle interface nommée **SYNC**, dédiée à la synchronisation entre les deux pfSense. Cette interface permet de répliquer automatiquement la configuration via le service **pfsync**.

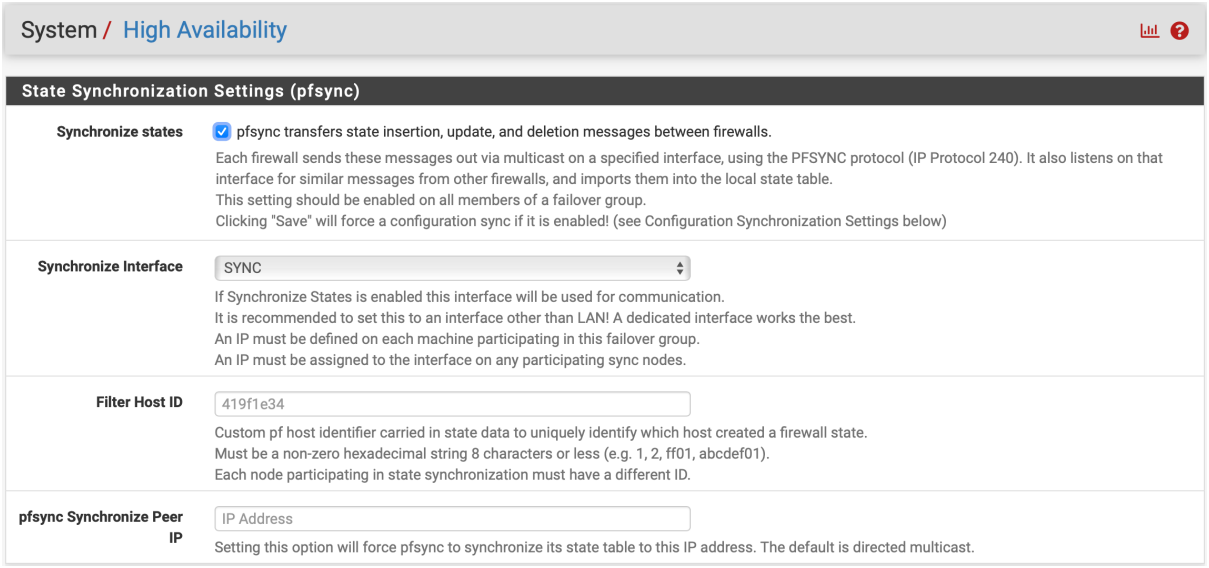
Interfaces			
WAN	↑	autoselect	10.10.210.251
LAN	↑	autoselect	n/a
VLANSERVER	↑	autoselect	10.10.110.251
VLANCLIENT	↑	autoselect	10.10.120.251
VLANDMZ	↑	autoselect	10.10.140.251
VLANMGMT	↑	autoselect	10.10.199.251
VLANBACKUP	↑	autoselect	10.10.200.251
SYNC	↑	autoselect	172.29.100.251

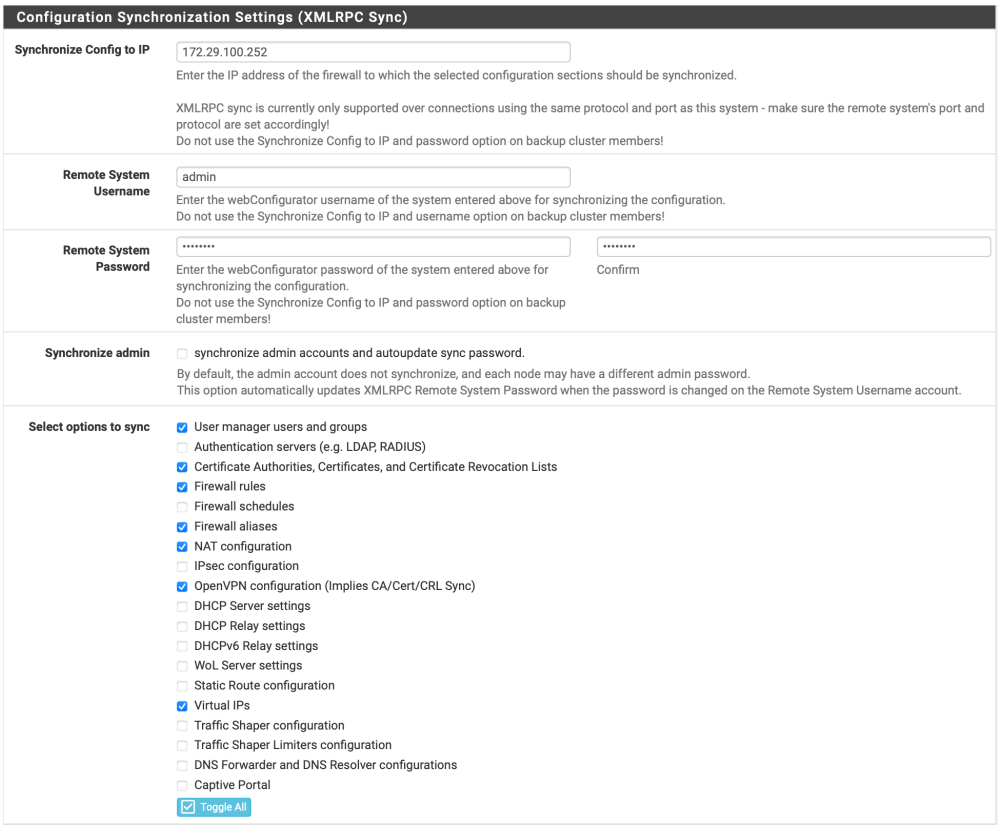
Une fois les interfaces créées sur le premier pfSense, j'ajoute les mêmes interfaces, nommées à l'identique, sur le second pfSense, en particulier l'interface **SYNC**. Celle-ci est essentielle pour mettre en place la synchronisation en temps réel entre les deux pare-feux. Grâce à cette configuration, toute modification effectuée sur le pfSense principal est automatiquement répliquée sur le second, ce qui permet d'éviter une double saisie et assure une cohérence parfaite entre les deux systèmes.

Interfaces			
WAN	↑	autoselect	10.10.210.252
LAN	↑	autoselect	n/a
VLANSERVER	↑	autoselect	10.10.110.252
VLANCLIENT	↑	autoselect	10.10.120.252
VLANDMZ	↑	autoselect	10.10.140.252
VLANMGMT	↑	autoselect	10.10.199.252
VLANBACKUP	↑	autoselect	10.10.200.252
SYNC	↑	autoselect	172.29.100.252

Mise en place du Pfsync

Je configure la synchronisation entre les deux pfSense à l'aide de **pfsync**. Comme mentionné précédemment, il est essentiel que les interfaces soient identiques et nommées de la même manière sur les deux pare-feux, sans quoi la synchronisation ne fonctionnera pas correctement. La configuration s'effectue depuis l'onglet **High Availability Sync** sur le pfSense principal (ici, le pfSense 1). On y sélectionne l'interface dédiée à la synchronisation (dans notre cas, **SYNC**), puis on renseigne l'adresse IP du pfSense secondaire, ainsi que les identifiants (login/mot de passe) permettant la connexion. Enfin, il est recommandé de sélectionner uniquement les éléments réellement utilisés pour éviter des erreurs ou conflits lors de la synchronisation.





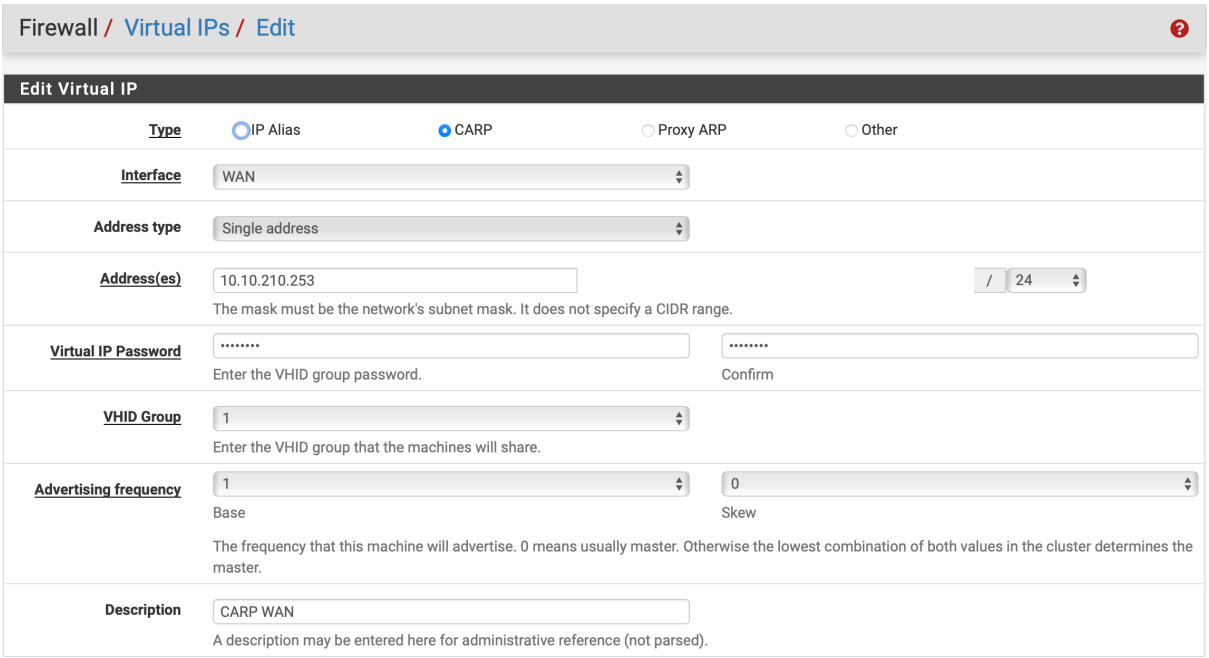
Mise en place des IP virtuelles (VIP) et du service CARP

Maintenant que la synchronisation entre les deux pfSense est opérationnelle, il est possible de tout configurer directement depuis le pfSense principal, les changements étant automatiquement répliqués sur le second.

L'étape suivante consiste à créer des **adresses IP virtuelles (VIP)**, nécessaires pour activer le service **CARP**. Ce service permet la mise en place d'un système de **failover** : en cas de panne du pfSense principal, le second prend immédiatement le relais, assurant ainsi une redondance automatique. On parle alors de bascule : le pfSense secondaire devient maître (Master), tandis que l'autre passe en mode secours (Backup). Une fois le pfSense principal à nouveau fonctionnel, il reprend automatiquement son rôle de maître.

Pour que ce mécanisme fonctionne correctement, un système de **priorités** est défini, permettant à chaque pare-feu de savoir s'il doit être maître ou backup selon la situation.

Il est important de noter que lorsque l'option **pfsync** est activée, le pfSense maître se voit automatiquement attribuer une priorité plus élevée que le pfSense en mode backup, ce qui garantit un comportement logique lors des bascules.



Une fois toutes les **adresses IP virtuelles (VIP)** correctement configurées, il est possible de vérifier l'état du service **CARP** via l'interface d'administration afin de s'assurer que la redondance est bien active et fonctionnelle.

Firewall / Virtual IPs

Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
10.10.210.253/24 (vhid: 1)	WAN	CARP	CARP WAN	
10.10.110.254/24 (vhid: 2)	VLANSERVER	CARP	CARP SERVER	
10.10.120.254/24 (vhid: 3)	VLANCLIENT	CARP	CARP CLIENT	
10.10.140.254/32 (vhid: 4)	VLANDMZ	CARP	CARP DMZ	
10.10.199.254/24 (vhid: 5)	VLANMGMT	CARP	CARP MGMT	
10.10.200.254/24 (vhid: 6)	VLANBACKUP	CARP	CARP BACKUP	

pfSense 1 (Maitre) :

Status / CARP

CARP Maintenance

Temporarily Disable CARP | Enter Persistent CARP Maintenance Mode

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
WAN@1	10.10.210.253/24	CARP WAN	MASTER
VLANSERVER@2	10.10.110.254/24	CARP SERVER	MASTER
VLANCLIENT@3	10.10.120.254/24	CARP CLIENT	MASTER
VLANDMZ@4	10.10.140.254/32	CARP DMZ	MASTER
VLANMGMT@5	10.10.199.254/24	CARP MGMT	MASTER
VLANBACKUP@6	10.10.200.254/24	CARP BACKUP	MASTER

pfSense 2 (Backup) :

Status / CARP

CARP Maintenance

Temporarily Disable CARP | Enter Persistent CARP Maintenance Mode

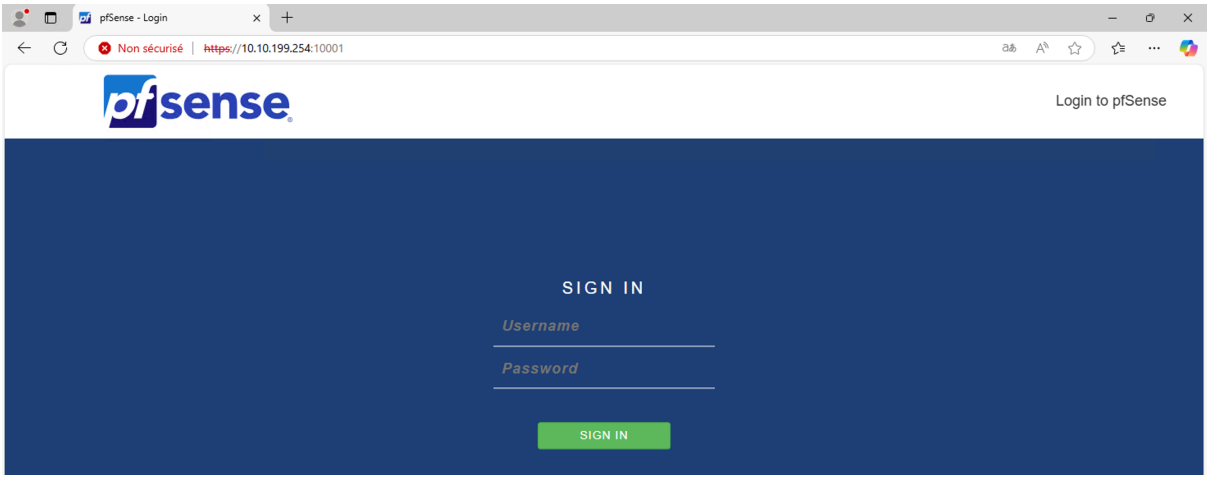
CARP Status

Interface and VHID	Virtual IP Address	Description	Status
WAN@1	10.10.210.253/24	CARP WAN	BACKUP
VLANSERVER@2	10.10.110.254/24	CARP SERVER	BACKUP
VLANCLIENT@3	10.10.120.254/24	CARP CLIENT	BACKUP
VLANDMZ@4	10.10.140.254/32	CARP DMZ	BACKUP
VLANMGMT@5	10.10.199.254/24	CARP MGMT	BACKUP
VLANBACKUP@6	10.10.200.254/24	CARP BACKUP	BACKUP

Partie 2 – Validation

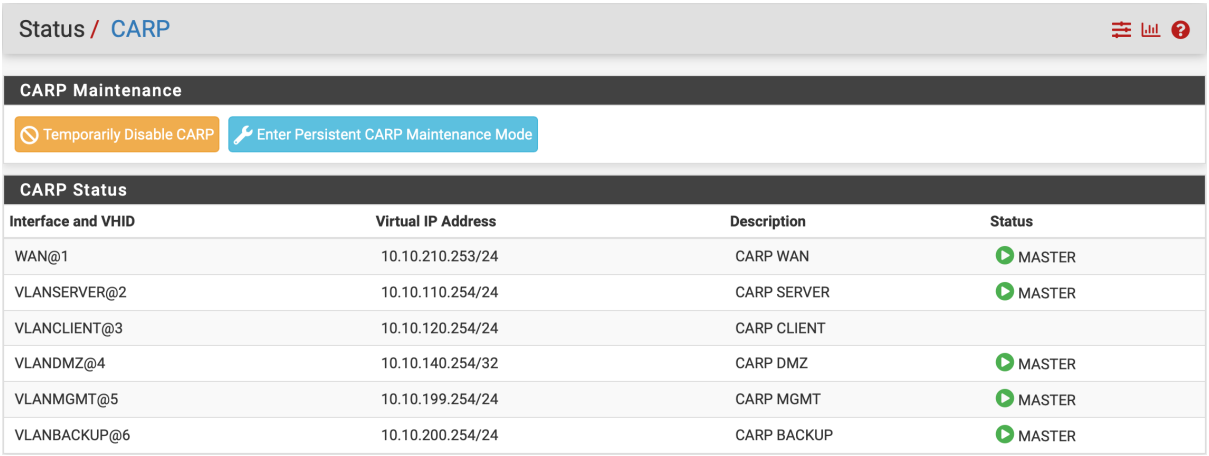
Pour valider le bon fonctionnement de la synchronisation **pfsync**, il suffit de créer une règle sur le pfSense 1, puis de vérifier que celle-ci est bien répliquée instantanément sur le pfSense 2.

Concernant les **adresses IP virtuelles**, leur fonctionnement peut être testé en se connectant à l'interface d'administration via l'une de ces IP, comme le **VLANMGMT** en **.254**, qui correspond à une IP virtuelle partagée.



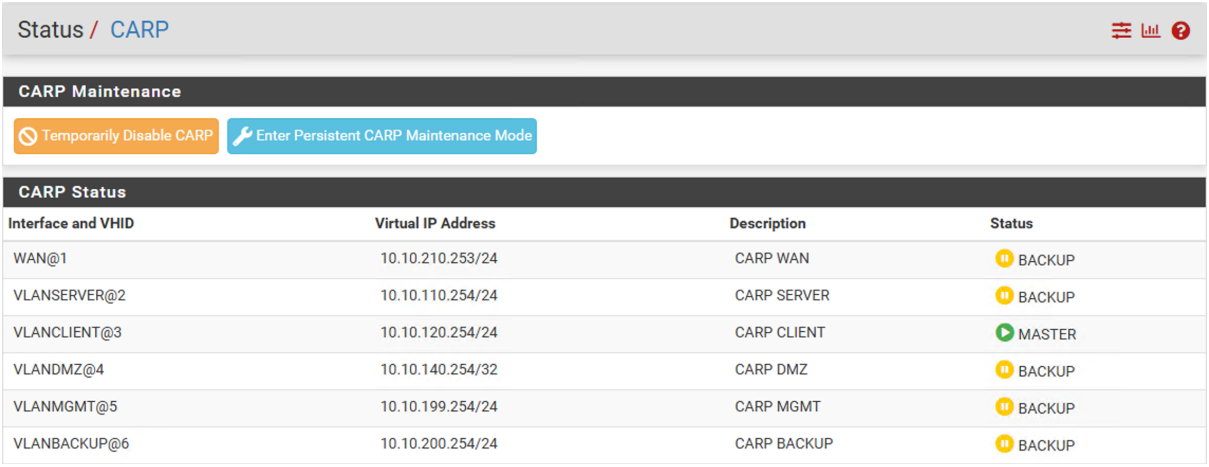
Ensuite, pour tester le service **CARP**, il est possible de désactiver temporairement l'interface **VLANCLIENT** sur le pfSense principal. Cela permet d'observer si le pfSense secondaire prend bien le relais automatiquement sur ce réseau, validant ainsi le mécanisme de bascule.

pfSense 1 : Panne de VLANCLIENT

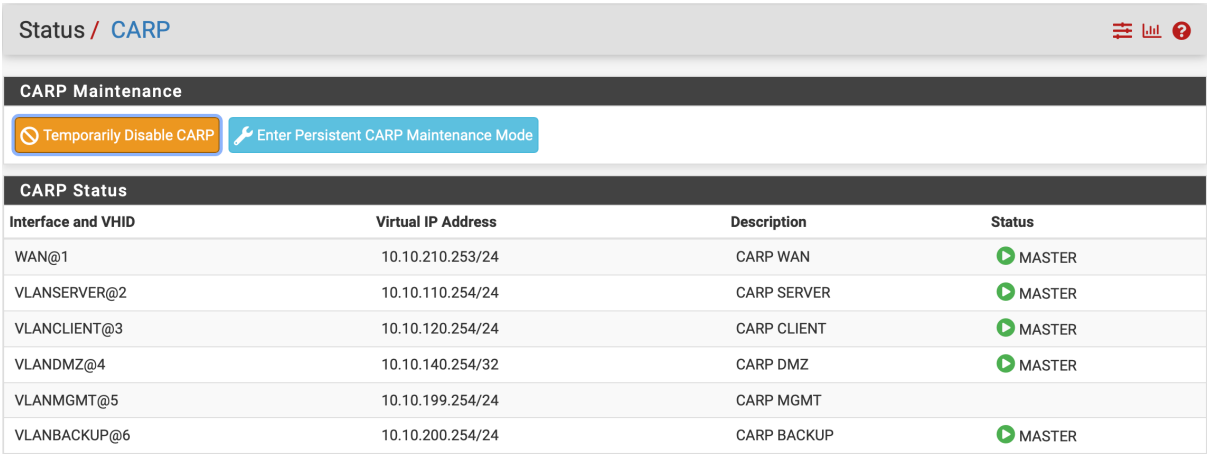


Interface and VHID	Virtual IP Address	Description	Status
WAN@1	10.10.210.253/24	CARP WAN	MASTER
VLANSERVER@2	10.10.110.254/24	CARP SERVER	MASTER
VLANCLIENT@3	10.10.120.254/24	CARP CLIENT	
VLANDMZ@4	10.10.140.254/32	CARP DMZ	MASTER
VLANMGMT@5	10.10.199.254/24	CARP MGMT	MASTER
VLANBACKUP@6	10.10.200.254/24	CARP BACKUP	MASTER

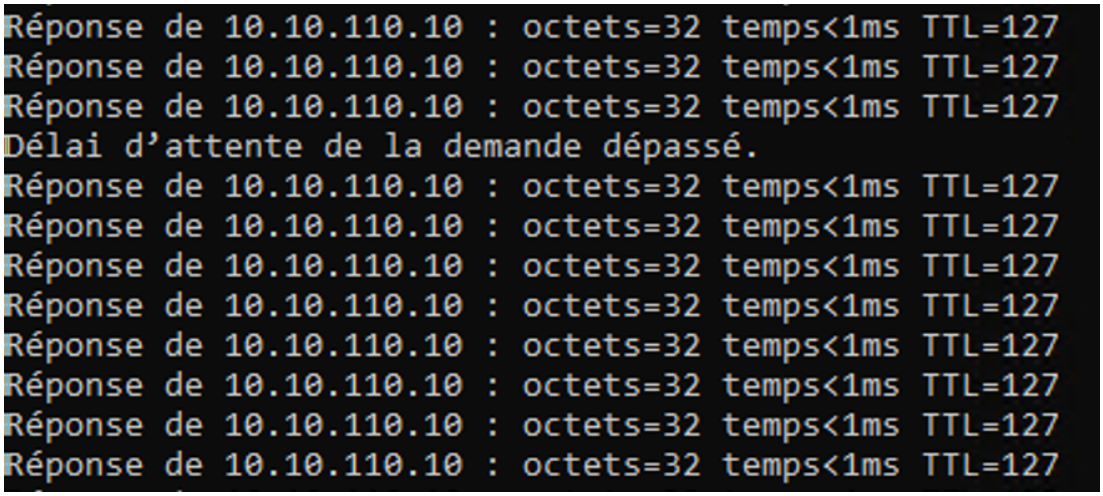
pfSense 2 : Devient « Maitre » de VLANCLIENT



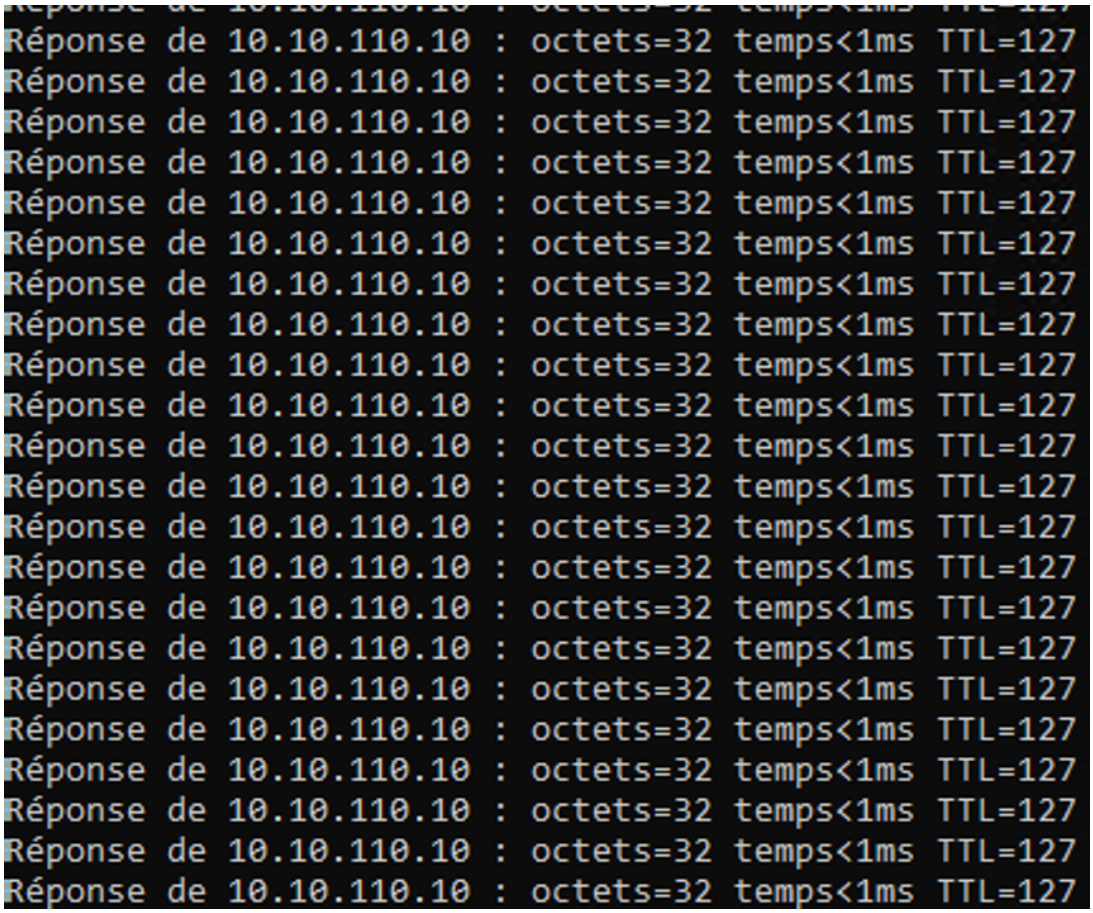
Enfin, pour valider pleinement le fonctionnement du **failover** de pfSense, le test le plus significatif consiste à observer le comportement du trafic en cas de panne du pfSense principal. Pour cela, j'effectue un **ping continu** depuis le poste de management, ce qui permet de mesurer la perte éventuelle de paquets lors de la coupure, ainsi que la reprise du service lorsque le pfSense maître redevient actif.



Après la coupure du pfSense 1, une seule perte de paquet est observée, ce qui reste négligeable et sans impact notable, mis à part une brève déconnexion du VPN, qui se reconnecte automatiquement.



Lorsque le pfSense 1 redevient maître et reprend le contrôle des interfaces, la bascule se fait de manière totalement transparente : aucune perte de paquet n'est constatée, et la reconnexion s'effectue immédiatement, sans que l'utilisateur ne perçoive le moindre changement.



Partie 3 – Veille Technologique

Dans le cadre de ce projet, une veille technologique a été réalisée afin d'explorer les différentes solutions existantes en matière de haute disponibilité réseau et de redondance de pare-feux. L'objectif était de comparer pfSense avec d'autres solutions open source ou commerciales telles que OPNsense, FortiGate HA, Sophos ou encore Cisco ASA avec failover.

Cette veille a permis de constater que pfSense, en plus d'être gratuit et open source, offre des fonctionnalités robustes comme CARP, pfsync, et une interface web complète, tout en restant flexible et simple à mettre en œuvre dans un environnement virtualisé. Des recherches ont également été menées sur les bonnes pratiques de configuration, la gestion des priorités CARP, la sécurité des synchronisations inter-pare-feux et la résilience en cas de panne.

La solution pfSense avec CARP présente plusieurs avantages notables : elle est **gratuite**, **open source**, relativement simple à déployer, et permet une **haute disponibilité efficace** grâce à la redondance automatique. L'interface web est intuitive, et les fonctionnalités comme **pfsync** ou les **VIP** facilitent la gestion du cluster. Cependant, cette solution comporte aussi quelques inconvénients, notamment une **configuration sensible** à la cohérence des interfaces, un **manque de support officiel** comparé aux solutions commerciales, et une **documentation parfois dispersée**, ce qui peut rallonger le temps de mise en œuvre en cas de problème.

Lors de ma veille technologique, j'ai également étudié **OPNsense**, une alternative directe à pfSense. Cette solution m'a semblé **très légère, optimisée et stable**, ce qui en fait un excellent choix pour des environnements à faibles ressources. Toutefois, malgré ses atouts techniques, j'ai trouvé son interface **moins intuitive** et **moins conviviale** à mon goût que celle de pfSense, en particulier pour une gestion quotidienne. Ayant été formé sur pfSense depuis longtemps, je suis plus à l'aise avec son environnement, ce qui a naturellement orienté mon choix vers cette solution. Cela dit, je reste **ouvert aux autres technologies** et je teste régulièrement **de nouveaux outils** afin de développer des compétences variées et rester à jour dans le domaine des infrastructures réseau.

Enfin, cette veille a mis en lumière l'importance croissante de la haute disponibilité dans les infrastructures modernes, en particulier avec la montée en charge des services hébergés localement ou en cloud, et les attentes élevées en termes de continuité de service pour les utilisateurs.

BTS Services informatiques aux organisations - SISR

Session 2025

E5 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :

Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- ***Layer Bureautique et Informatique*** *est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro.*

- *La problématique principale réside dans le manque d'infrastructure pour accueillir les collaborateurs, malgré la présence d'un ESXi puissant.*

- *La solution choisie consiste à déployer une infrastructure hautement disponible et sécurisée, avec une réplication AD/DNS entre deux serveurs. Des scripts d'automatisation ont été utilisés pour la création d'unités organisationnelles, d'utilisateurs et de groupes afin d'optimiser la gestion des ressources et des permissions.*

Intitulé de la réalisation professionnelle

Mise en place d'une infrastructure Active Directory hautement disponible

Période de réalisation : 20/05/24 - 21/05/24 **Lieu :** Auxerre

Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE
- GERER LE PATRIMOINE INFORMATIQUE

Conditions de réalisation

- **Ressources présentes (situation avant la RP)**
  Un ESXi suffisamment puissant est disponible, mais aucune infrastructure n'a été créée pour accueillir des collaborateurs.

- **Résultats attendus (situation après la RP)**
  Une infrastructure hautement disponible, sécurisée et optimisée pour accueillir des collaborateurs.

- **Durée de réalisation**
  La mise en place de cette infrastructure m'a pris environ 2 jours, les scripts étant la partie la plus longue à réaliser.

Modalités d'accès à cette réalisation professionnelle.

https://portfolio.vdb-pro.fr *mdp : Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

Dans le cadre de ma mission chez Layer Bureautique et Informatique, j'ai conçu une infrastructure Active Directory (AD) hautement disponible avec deux serveurs AD, l'un en mode graphique et l'autre en mode ligne de commande (server Core) pour le client vdb-pro. J'ai assuré la réplication entre ces serveurs pour garantir la redondance et la disponibilité continue des services. De plus, j'ai automatisé la création d'Unités Organisationnelles (OU) et d'utilisateurs à l'aide de scripts, simplifiant ainsi la gestion de l'AD.

Création des machines virtuelles (VM) dans ESXi

La virtualisation via ESXi permet de créer et gérer plusieurs machines virtuelles (VM) sur un seul serveur physique. En utilisant un hyperviseur comme ESXi, on peut isoler les différents services et rôles réseau dans des environnements séparés, ce qui est essentiel pour tester et sécuriser l'infrastructure. Cela réduit également les coûts matériels et améliore la gestion des ressources.

La création des VM dans ESXi permet de déployer un environnement virtuel sécurisé pour la mise en place des différents services (pare-feu, contrôleurs de domaine, client) dans une infrastructure isolée. Cela facilite la gestion, l'expérimentation et la restauration en cas d'erreur sans impacter un réseau physique.

Créer une VM dans ESXi implique de spécifier des paramètres comme l'allocation de mémoire vive (RAM), le nombre de cœurs CPU, et l'espace disque. Ces ressources sont ajustées selon les besoins de chaque service pour garantir des performances optimales. Une fois les VM créées, elles pourront être démarrées et configurées individuellement.

Schéma ESXi

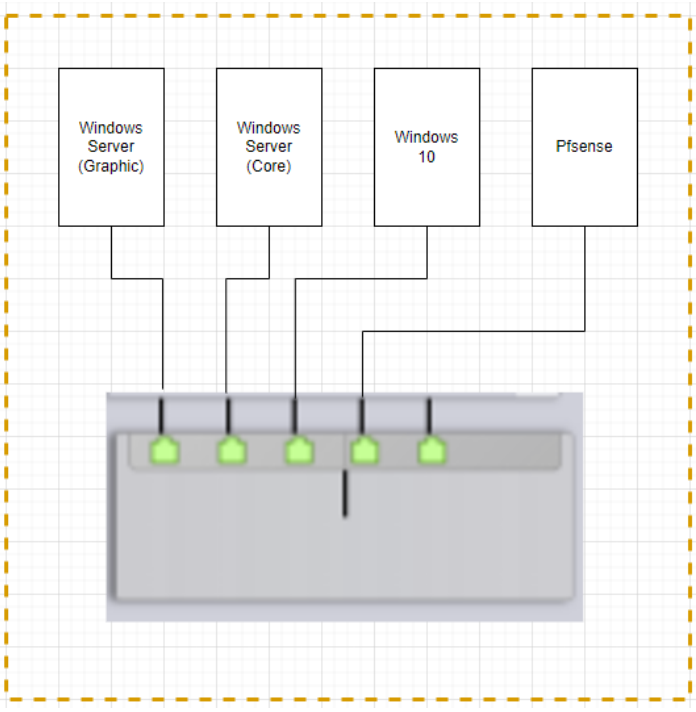
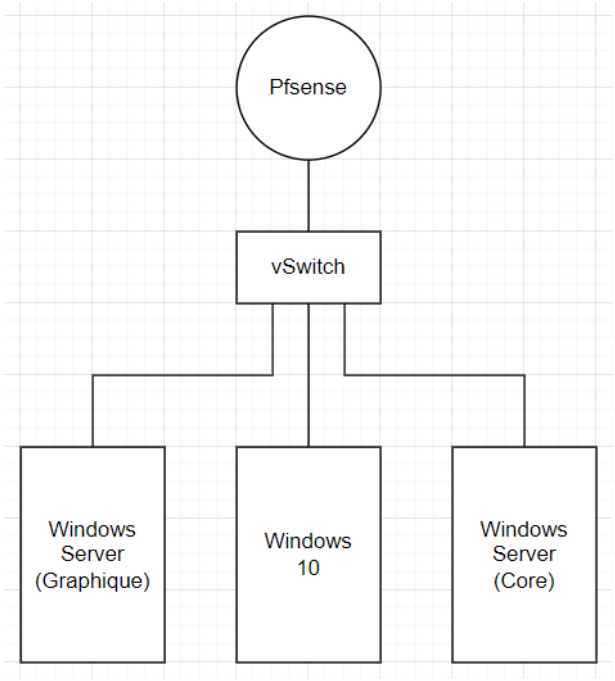


Schéma logique

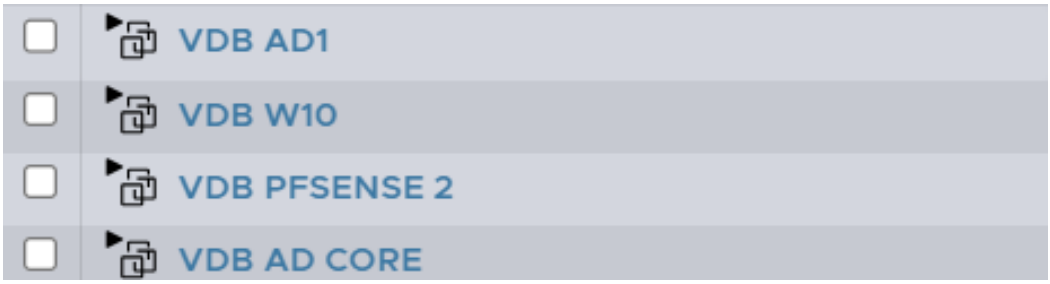


- **PfSense :** Joue le rôle de pare-feu pour filtrer le trafic et assurer la sécurité réseau.

- **Windows Server 2019 (GUI) :** Ce serveur est le contrôleur de domaine principal, il prend en charge les rôles AD (Active Directory) et DNS pour la gestion centralisée des ressources réseau.

- **Windows Server 2019 Core :** Servira de contrôleur de domaine secondaire et de serveur DNS répliqué, permettant la redondance et la résilience du service.

- **Windows 10 :** Client qui sera utilisé pour valider l'intégration et la connectivité dans le domaine Active Directory.



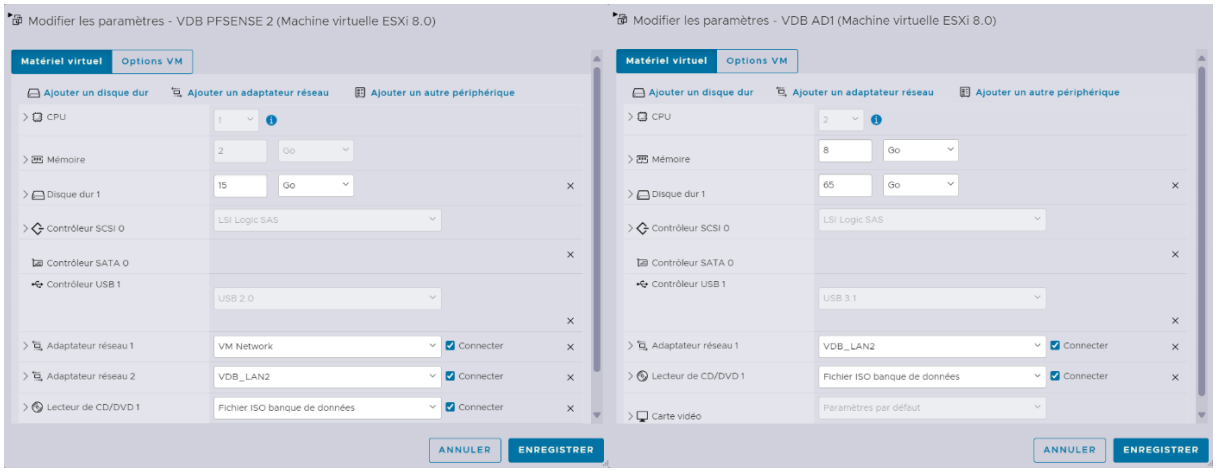
Configuration d'ESXi et des paramètres de VM (performance/réseau)

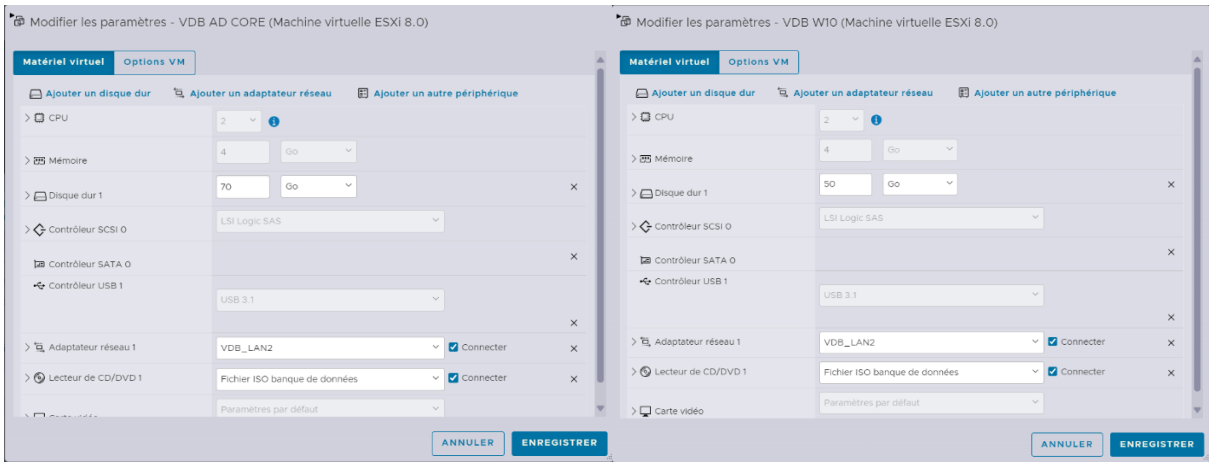
La configuration des ressources sur ESXi assure que les VM reçoivent les ressources nécessaires pour fonctionner sans ralentissement. Le réseau virtuel permet aux machines de communiquer en interne sans accès direct à Internet, assurant ainsi la sécurité et l'isolation de l'environnement.

Configurer ESXi et les paramètres des VM optimise l'allocation de ressources pour éviter les goulets d'étranglement et garantir un fonctionnement fluide de l'environnement. De plus, la configuration réseau permet aux VM de communiquer entre elles dans un environnement isolé.

Configuration des performances des VM dans ESXi :

Ajustement des ressources allouées aux VM (CPU, RAM, disque) selon les besoins du projet pour garantir une réactivité optimale.

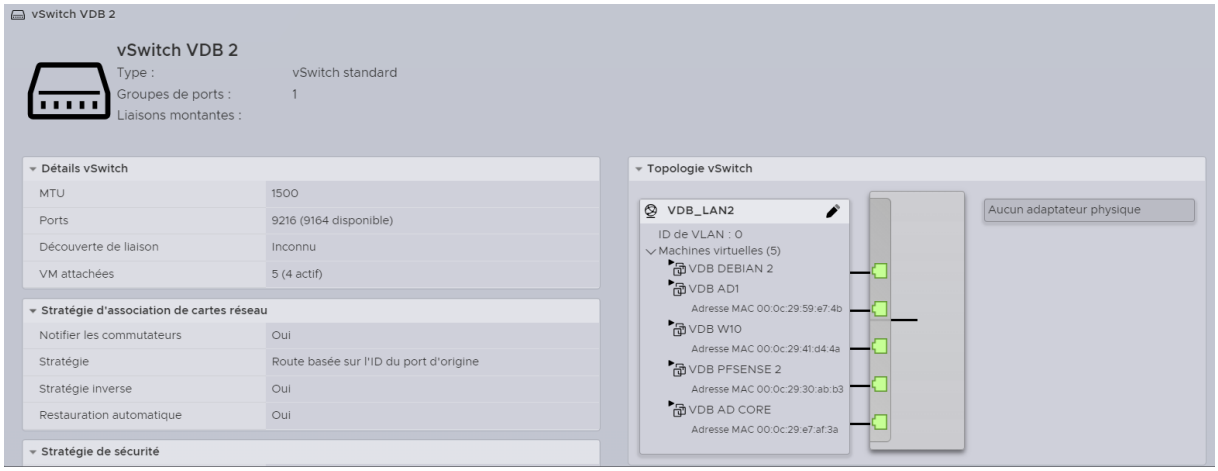




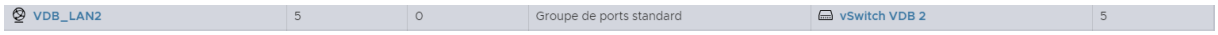
Paramètre supplémentaire que l'on peut configurer est l'allocation de mémoire, la réservation de ressources et la limitation d'IO pour chaque VM.

Configuration réseau dans ESXi :

Création d'un vSwitch (vSwitch VDB 2) : Ce vSwitch permet de créer un réseau isolé pour les machines virtuelles (VM), assurant ainsi une sécurité accrue en restreignant l'accès aux VM et en empêchant toute communication non autorisée avec le réseau externe.



Création d'un groupe de ports (VDB_LAN2) : Ce groupe de ports est associé au vSwitch, offrant une interface de communication dédiée pour toutes les VM connectées. Il garantit une communication fluide et sécurisée entre les VM tout en optimisant la gestion du trafic réseau interne.



Configuration de PfSense pour isoler le réseau

PfSense est une solution pare-feu open source. Dans notre architecture, il protège et isole le réseau virtuel. Ce pare-feu sert également de routeur, permettant de filtrer le trafic entrant et sortant et d'autoriser uniquement les connexions nécessaires. Dans un environnement de production, cela limite l'exposition de l'infrastructure aux menaces extérieures.

Configurer PfSense avec une adresse **WAN** pour la connexion externe 10.5.0.29 et une adresse **LAN** pour le réseau interne 172.17.129.126. Les règles de pare-feu dans PfSense permettent de restreindre le trafic en fonction des besoins, et les règles NAT (Network Address Translation) permettent l'accès RDP sécurisé depuis l'extérieur.

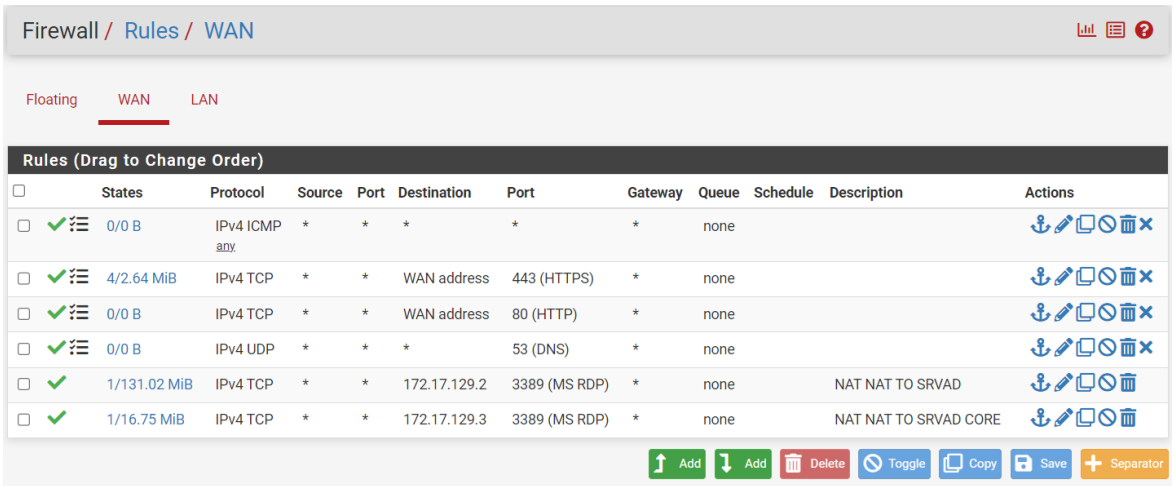
Paramètres réseau :

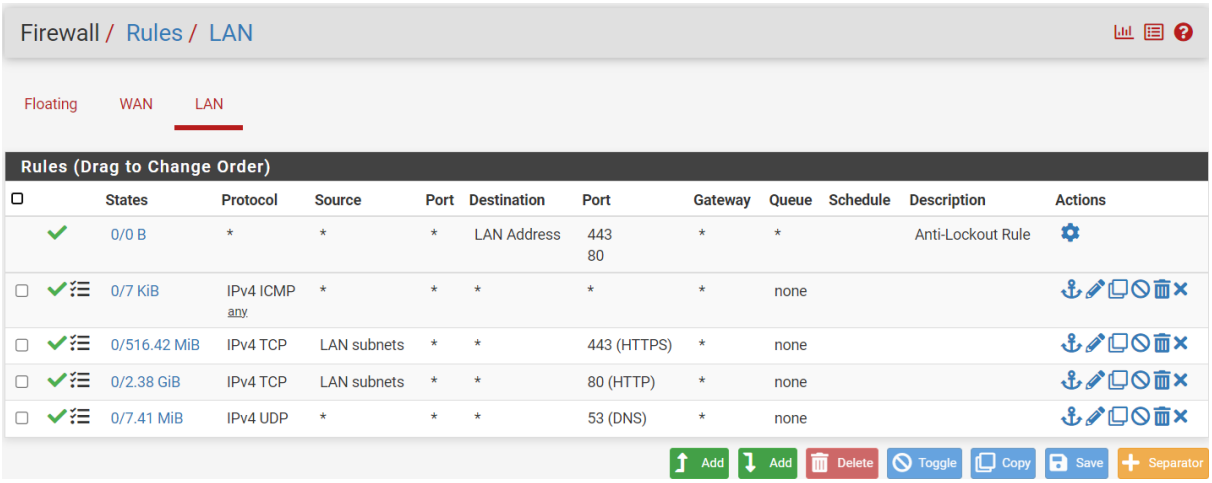
- **WAN :** Adresse IP 10.5.0.29 /16, connectée au réseau externe.
- **LAN :** Adresse IP 172.17.129.126 /25, pour le réseau interne entre les VM.

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense2 ***

WAN (wan)       -> vmx0       -> v4/DHCP4: 10.5.0.29/16
LAN (lan)       -> vmx1       -> v4: 172.17.129.126/25

0) Logout (SSH only)                  9) pfTop
1) Assign Interfaces                 10) Filter Logs
2) Set interface(s) IP address       11) Restart webConfigurator
3) Reset webConfigurator password    12) PHP shell + pfSense tools
4) Reset to factory defaults         13) Update from console
5) Reboot system                     14) Enable Secure Shell (sshd)
6) Halt system                       15) Restore recent configuration
7) Ping host                         16) Restart PHP-FPM
8) Shell
```

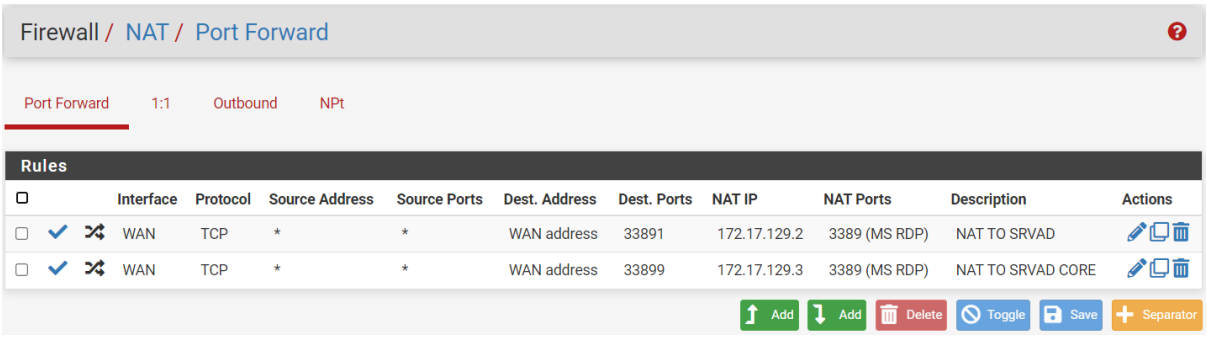
Règles PfSense :

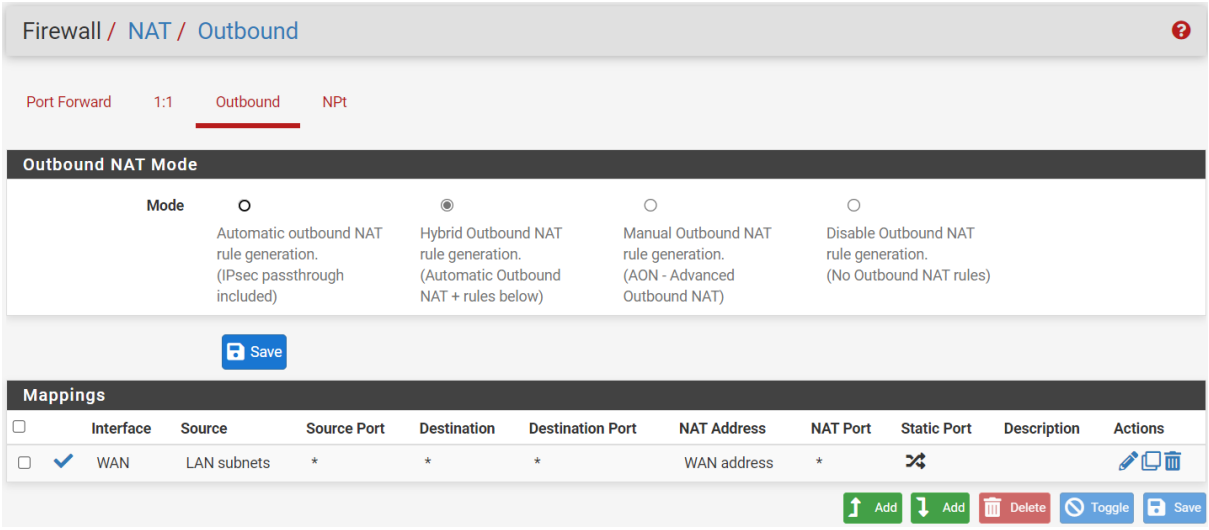
Rules : Configuration de règles de pare-feu pour contrôler l'accès et la circulation entre le réseau interne et externe.





NAT : Paramétrage de la redirection de port (RDP) pour accéder aux VM en interne depuis l'extérieur





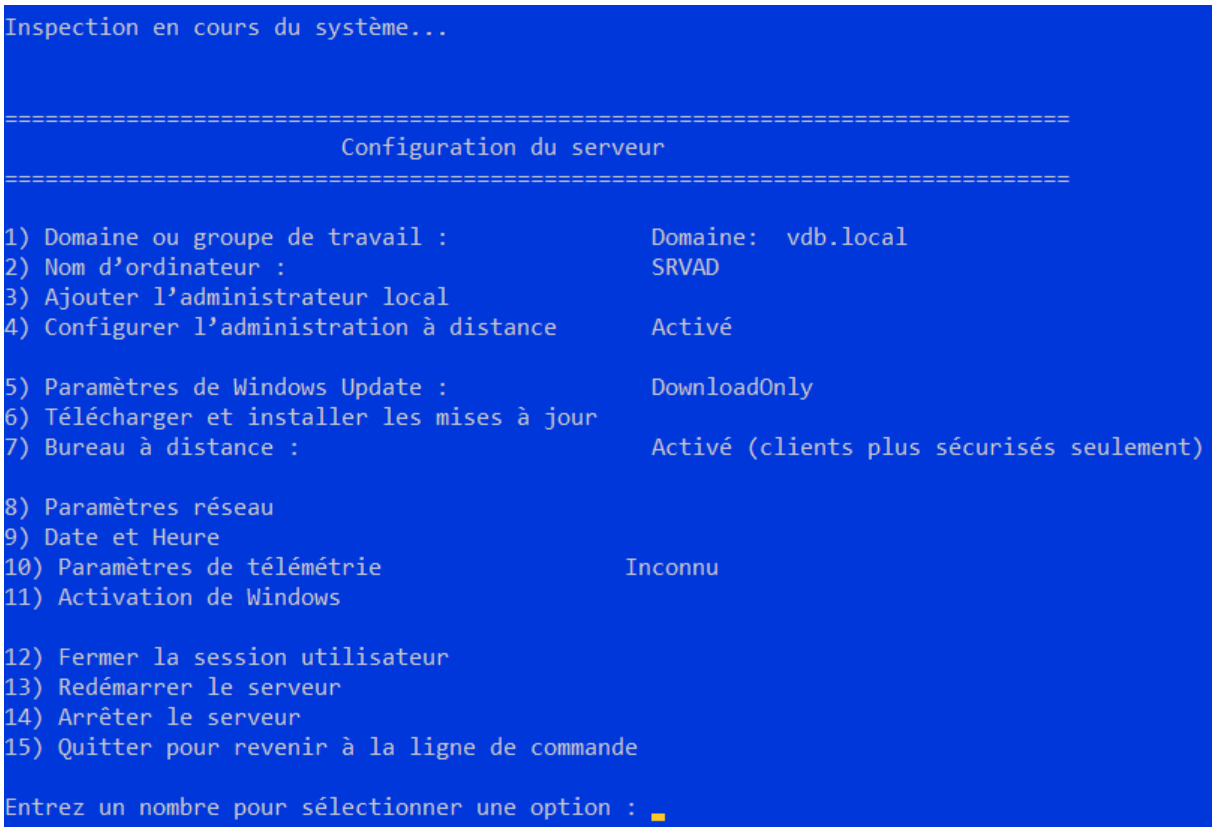
Installation et configuration de Windows Server 2022 (Interface graphique)

Le serveur Windows avec interface graphique est le principal contrôleur de domaine. L'interface facilite la gestion d'Active Directory, un service essentiel pour centraliser les utilisateurs, les groupes et les politiques de sécurité d'un réseau. C'est ce serveur qui initie le domaine vdb.local, fournissant les services d'authentification, de DNS et de DHCP.

Prise en main : Accès à la VM via ESXi pour effectuer les configurations de base.
Paramétrage réseau avec PowerShell « *sconfig* » : Configure l'adresse IP, la passerelle et le DNS pour que le serveur soit accessible aux autres machines.

Adresse IP : 172.17.129.2 /25
Passerelle : 172.17.129.126
DNS : Utilisation de l'adresse IP locale pour le DNS (172.17.129.2).

Activation de RDP : Permet d'utiliser le bureau à distance pour gérer le serveur de manière plus fluide. Activation de RDP via sconfig pour faciliter la gestion.

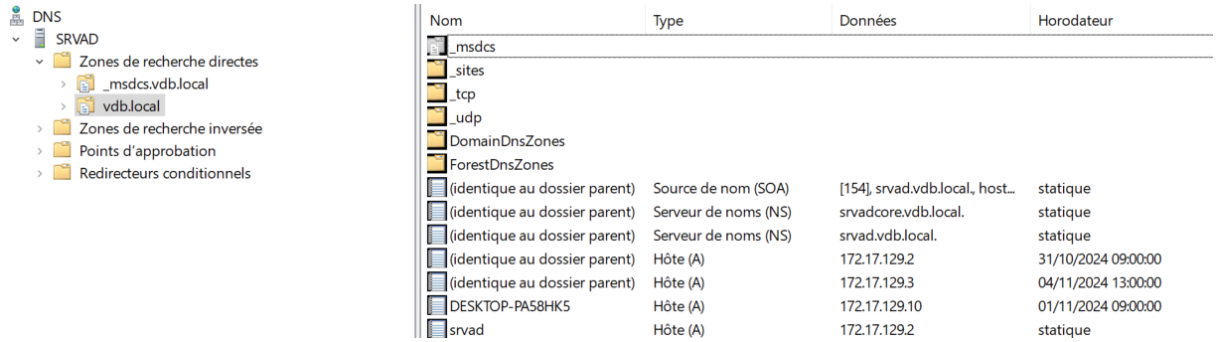


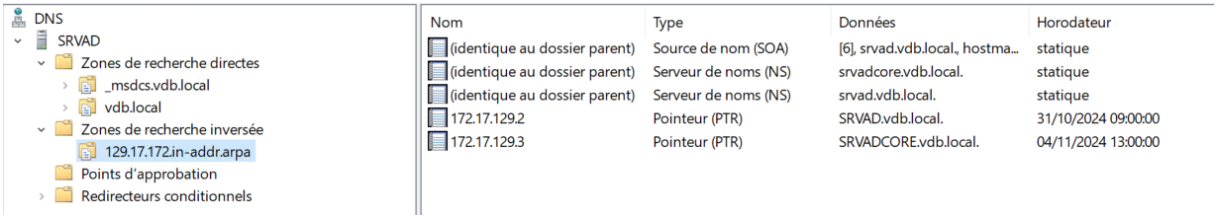
Installation des rôles DNS et AD DS (Active Directory Domain Services) :

Via le Gestionnaire de Serveur, les services AD et DNS sont installés. Le serveur est ensuite promu en tant que Domain Controller (DC), créant une forêt et un domaine vdb.local.

Le rôle de contrôleur de domaine et de DNS permet de gérer les ressources du domaine, les identités des utilisateurs, et de faciliter la résolution de noms. L'activation de RDP et les réglages réseau facilitent l'administration à distance.

Je configure donc les **zones DNS**, à la fois la **zone directe** (Forward Lookup Zone) et la **zone inversée** (Reverse Lookup Zone). Ces configurations sont essentielles pour assurer la résolution des noms dans notre infrastructure réseau, permettant aux machines de se trouver mutuellement de manière efficace.





Je procède à la promotion du serveur en tant que **contrôleur de domaine principal** dans **une nouvelle forêt** appelée **vdb.local**. Cette étape est cruciale pour la mise en place de notre infrastructure Active Directory, car elle établit un environnement centralisé pour la gestion des utilisateurs, des groupes, des ordinateurs, et des ressources au sein du réseau.

Je configure les **sites Active Directory** en ajoutant un **nouveau sous-réseau** (réseau LAN 2). L'objectif est d'assurer que tous les **contrôleurs de domaine** situés sur ce réseau soient automatiquement rattachés au **SiteA**.

Cela permet d'optimiser la **réplication Active Directory** en garantissant que le trafic réseau reste localisé et que les clients du réseau LAN 2 interagissent prioritairement avec les contrôleurs de domaine du SiteA, améliorant ainsi la performance et la résilience de l'infrastructure.

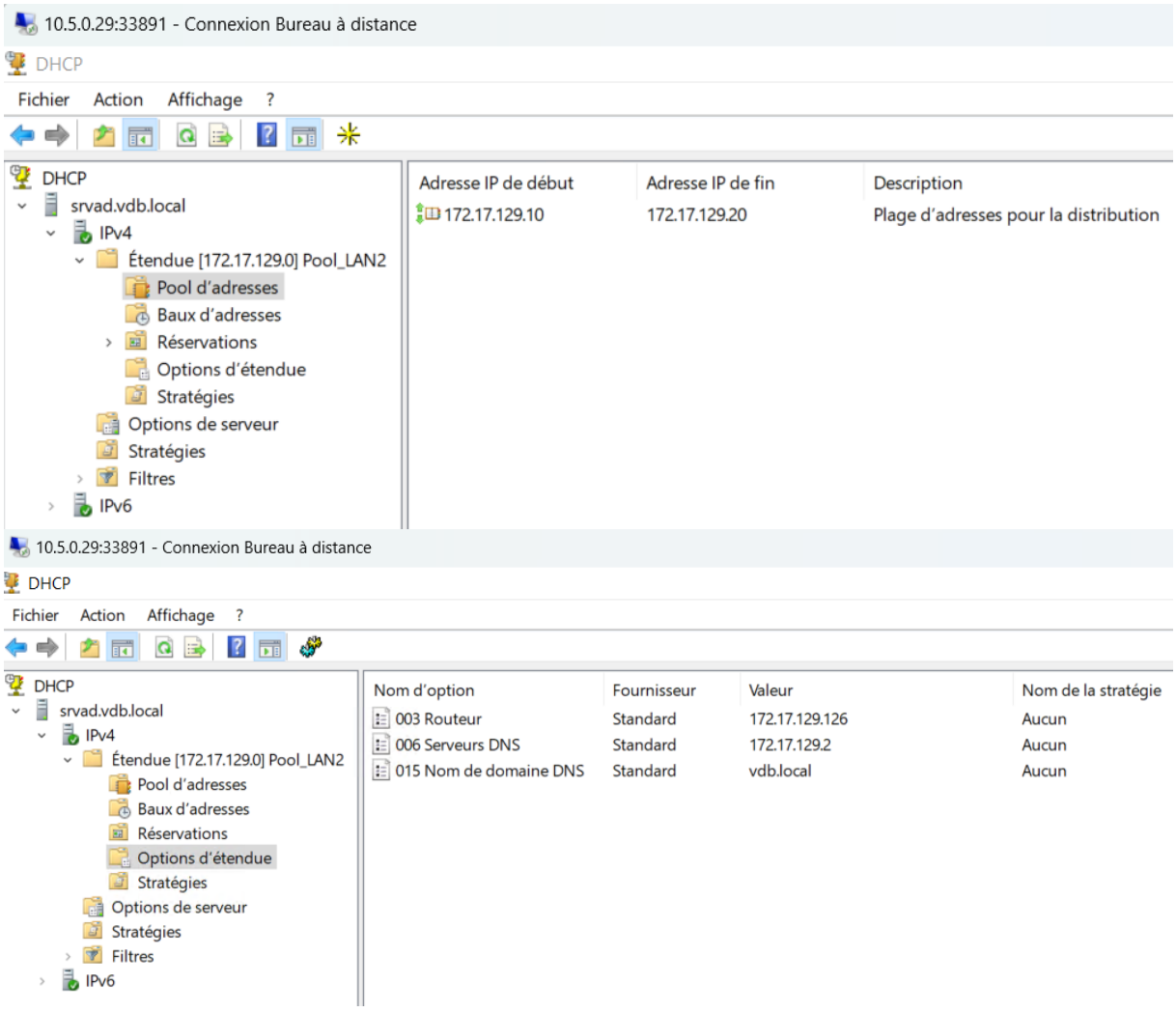
Configuration DHCP

Un serveur DHCP attribue automatiquement des adresses IP aux clients du réseau, simplifiant ainsi la gestion des configurations réseau, notamment pour les postes utilisateurs qui se connectent dynamiquement.

Dans le Gestionnaire DHCP, un pool d'adresses IP est créé pour le sous-réseau de l'environnement (par ex., 172.17.129.0/25). Le serveur DHCP attribuera ces adresses aux clients Windows 10, leur fournissant également l'adresse DNS du domaine.

Le DHCP garantit que les clients reçoivent des adresses IP valides et conformes à la topologie du réseau, simplifiant la configuration pour chaque nouvel utilisateur ou dispositif.

Configuration du pool d'adresses IP : Depuis le Gestionnaire DHCP, un pool d'adresses est défini pour le sous-réseau utilisé par les clients, par exemple 172.17.129.10 - 172.17.129.100. Le serveur DHCP transmet également l'adresse du DNS et l'adresse du routeur (gateway).



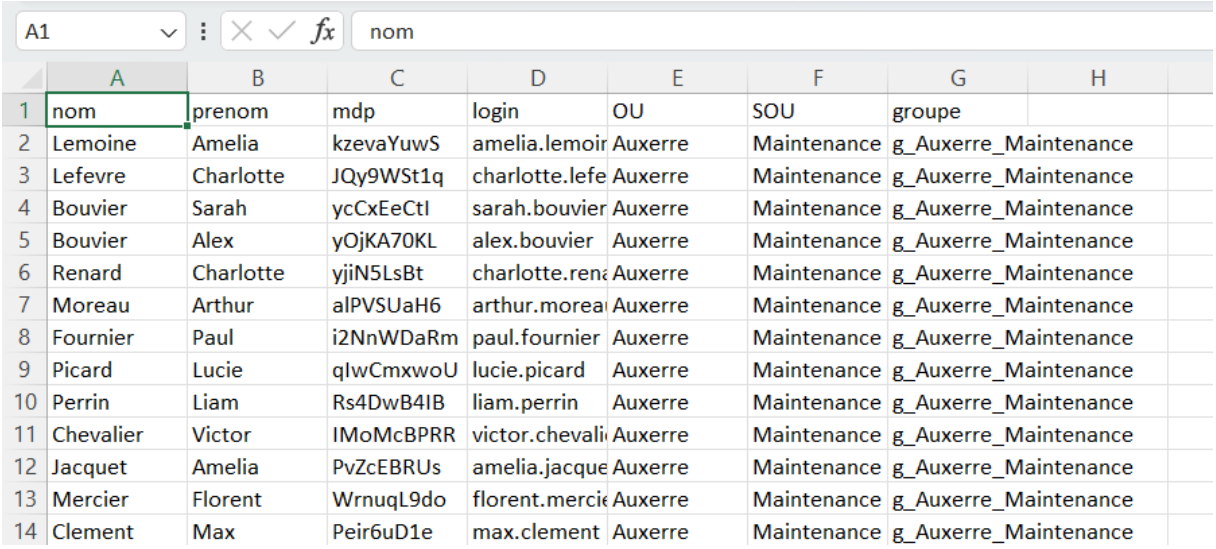
Je peux également configurer des réservations DHCP, ce qui permet de garantir que ces machines reçoivent toujours la même adresse IP, même si elles utilisent le protocole DHCP pour leur configuration réseau.

Création de scripts pour l'AD (OU, utilisateurs, groupes)

L'automatisation permet d'accélérer la création et la gestion des comptes et groupes dans l'Active Directory, évitant ainsi des opérations manuelles répétitives qui peuvent être sources d'erreurs. Cette étape est cruciale pour uniformiser la gestion des droits d'accès et la structure de l'annuaire.

J'ai créé plusieurs scripts PowerShell en utilisant l'IA comme aide afin d'automatiser la gestion d'Active Directory. Ces scripts permettent de créer automatiquement des Unités d'Organisation (OU) comme Technique et Maintenance, d'ajouter en masse des utilisateurs avec des informations prédéfinies (nom, mot de passe, login) et de gérer les groupes en y ajoutant les utilisateurs nécessaires.

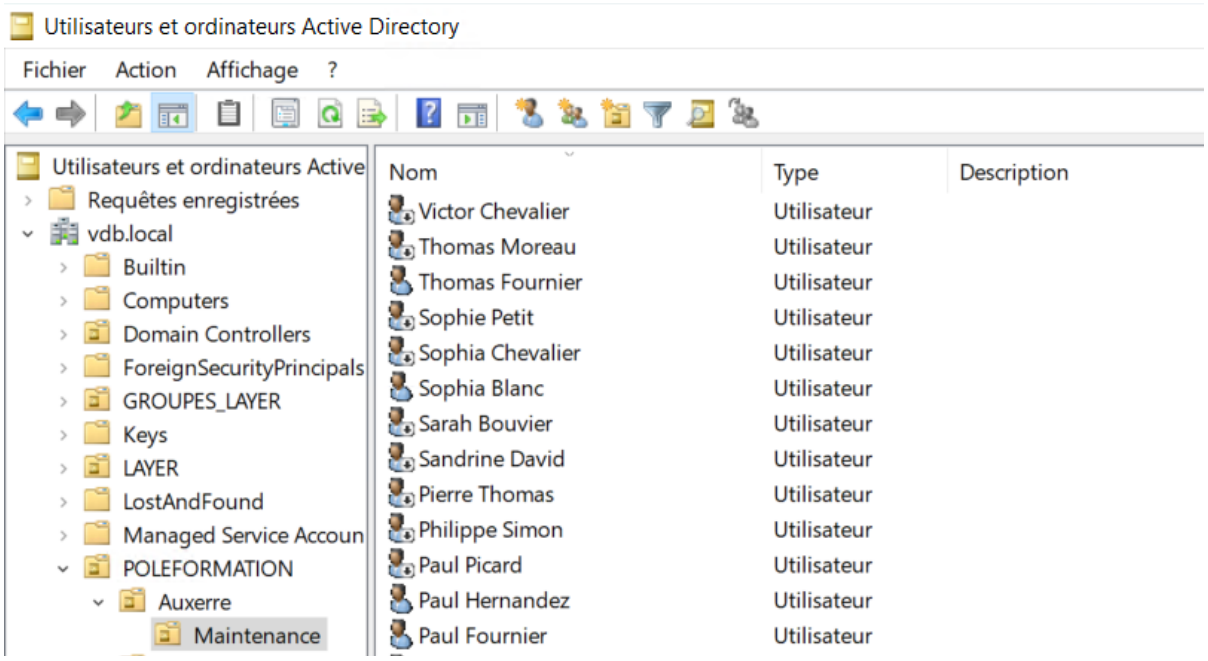
Voici un script PowerShell qui permet de créer des comptes utilisateurs en masse en important les informations depuis un fichier CSV. Ce script facilite la gestion des utilisateurs en automatisant leur création dans Active Directory avec des informations telles que le nom, le prénom, le login, le mot de passe, ainsi que les Unités d'Organisation (OU) et les groupes auxquels ils appartiennent.

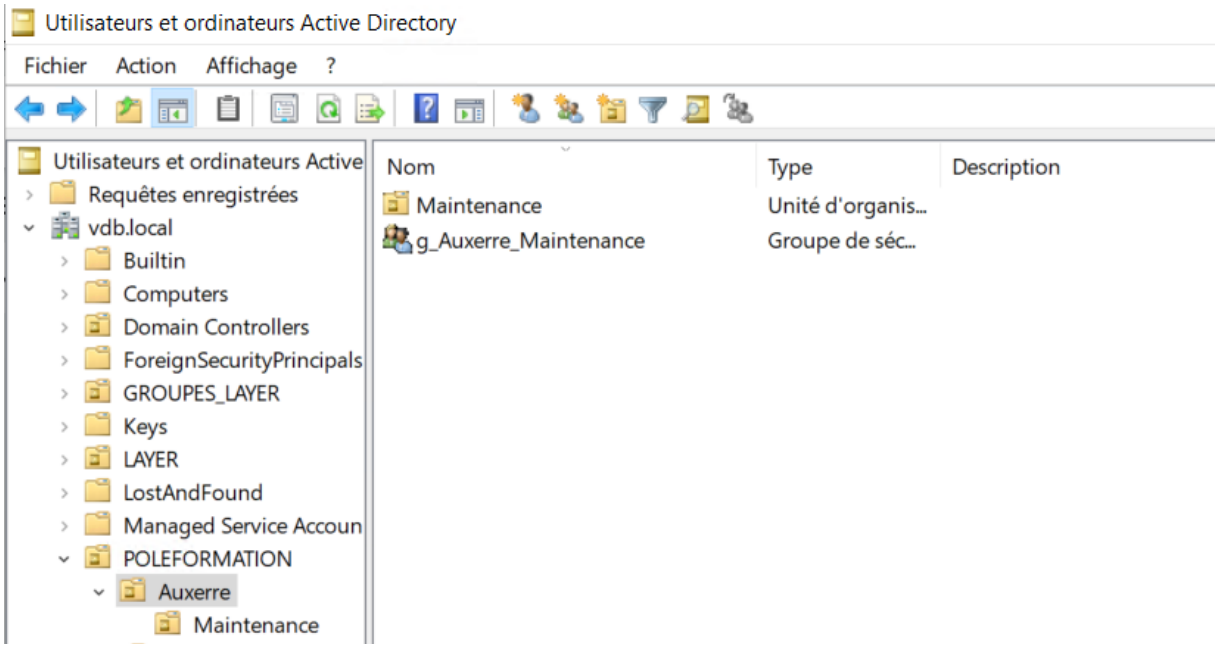


A1 | nom

	A	B	C	D	E	F	G	H
1	nom	prenom	mdp	login	OU	SOU	groupe	
2	Lemoine	Amelia	kzevaYuwS	amelia.lemoir	Auxerre	Maintenance	g_Auxerre_Maintenance	
3	Lefevre	Charlotte	JQy9WSt1q	charlotte.lefe	Auxerre	Maintenance	g_Auxerre_Maintenance	
4	Bouvier	Sarah	ycCxEeCtI	sarah.bouvier	Auxerre	Maintenance	g_Auxerre_Maintenance	
5	Bouvier	Alex	yOjKA70KL	alex.bouvier	Auxerre	Maintenance	g_Auxerre_Maintenance	
6	Renard	Charlotte	yjiN5LsBt	charlotte.rena	Auxerre	Maintenance	g_Auxerre_Maintenance	
7	Moreau	Arthur	alPVSUaH6	arthur.moreau	Auxerre	Maintenance	g_Auxerre_Maintenance	
8	Fournier	Paul	i2NnWDaRm	paul.fournier	Auxerre	Maintenance	g_Auxerre_Maintenance	
9	Picard	Lucie	qIwCmxwoU	lucie.picard	Auxerre	Maintenance	g_Auxerre_Maintenance	
10	Perrin	Liam	Rs4DwB4IB	liam.perrin	Auxerre	Maintenance	g_Auxerre_Maintenance	
11	Chevalier	Victor	IMoMcBPRR	victor.chevali	Auxerre	Maintenance	g_Auxerre_Maintenance	
12	Jacquet	Amelia	PvZcEBRUs	amelia.jacque	Auxerre	Maintenance	g_Auxerre_Maintenance	
13	Mercier	Florent	WrnuqL9do	florent.mercie	Auxerre	Maintenance	g_Auxerre_Maintenance	
14	Clement	Max	Peir6uD1e	max.clement	Auxerre	Maintenance	g_Auxerre_Maintenance	

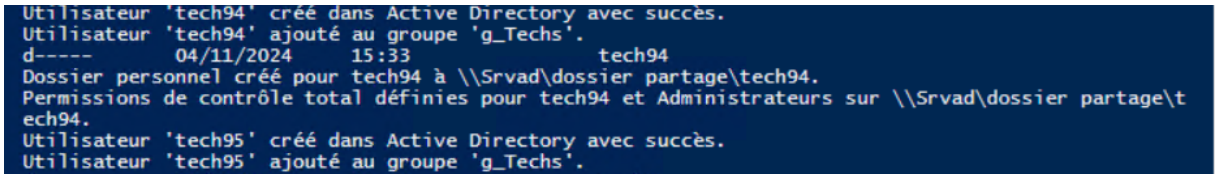
```
$users = Import-Csv -Path "C:\Users\Administrateur\Desktop\european_users_expanded.csv" -Delimiter ";"

# Créer l'OU racine si elle n'existe pas
if (-not (Get-ADOrganizationalUnit -Filter {Name -eq "POLEFORMATION"})) {
    New-ADOrganizationalUnit -Name "POLEFORMATION" -Path "dc=vdb,dc=local"
}

foreach ($user in $users) {
    # OU
    $ou = $user.OU
    $sou = $user.SOU

    # Vérifier et créer l'OU principale
    $ouPath = "ou=$ou,ou=POLEFORMATION,dc=vdb,dc=local"
    if (-not (Get-ADOrganizationalUnit -Filter {Name -eq $ou} -SearchBase "ou=POLEFORMATION,dc=vdb,dc=local")) {
        New-ADOrganizationalUnit -Name $ou -Path "ou=POLEFORMATION,dc=vdb,dc=local"
    }

    # Vérifier et créer l'OU secondaire
    $souPath = "ou=$sou,$ouPath"
    if (-not (Get-ADOrganizationalUnit -Filter {Name -eq $sou} -SearchBase $ouPath)) {
        New-ADOrganizationalUnit -Name $sou -Path $ouPath
    }

    # Groupe
    $group = $user.Groupe
    if (-not (Get-ADGroup -Filter {Name -eq $group} -SearchBase $ouPath)) {
        New-ADGroup -Name $group -Path $ouPath -GroupScope Global -GroupCategory Security
    }

    # Utilisateurs
    $nom = $user.Nom
    $prenom = $user.Prenom
    $login = $user.Login
    $mdp = $user.mdp

    # Créer l'utilisateur si non existant
    if (-not (Get-ADUser -Filter {SamAccountName -eq $login})) {
        New-ADUser -Name "$prenom $nom" `
                -Path $souPath `
                -SamAccountName $login `
                -AccountPassword (ConvertTo-SecureString $mdp -AsPlainText -Force) `
                -DisplayName "$prenom $nom" `
                -Enabled $true `
                -ChangePasswordAtLogon $true
    }
}
```

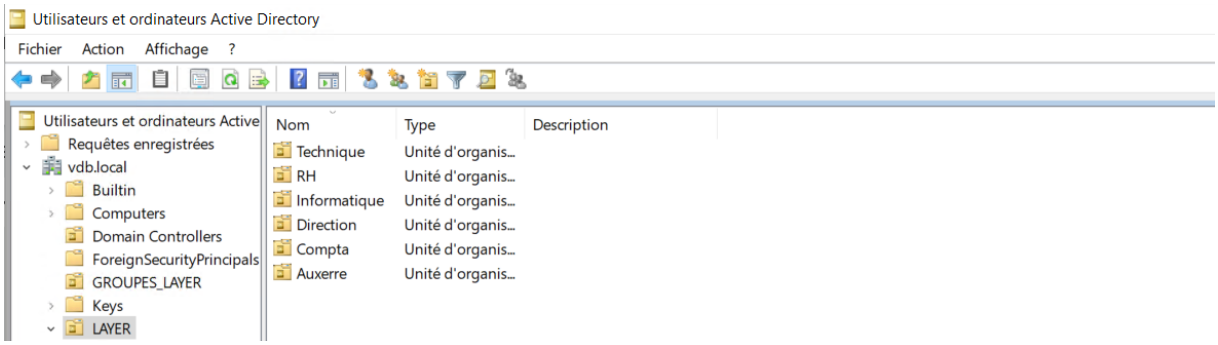

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
vdb.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
GROUPES_LAYER
Keys
LAYER
LostAndFound
Managed Service Accoun
POLEFORMATION
Auxerre
Maintenance
Nom
Type
Description
Victor Chevalier Utilisateur
Thomas Moreau Utilisateur
Thomas Fournier Utilisateur
Sophie Petit Utilisateur
Sophia Chevalier Utilisateur
Sophia Blanc Utilisateur
Sarah Bouvier Utilisateur
Sandrine David Utilisateur
Pierre Thomas Utilisateur
Philippe Simon Utilisateur
Paul Picard Utilisateur
Paul Hernandez Utilisateur
Paul Fournier Utilisateur

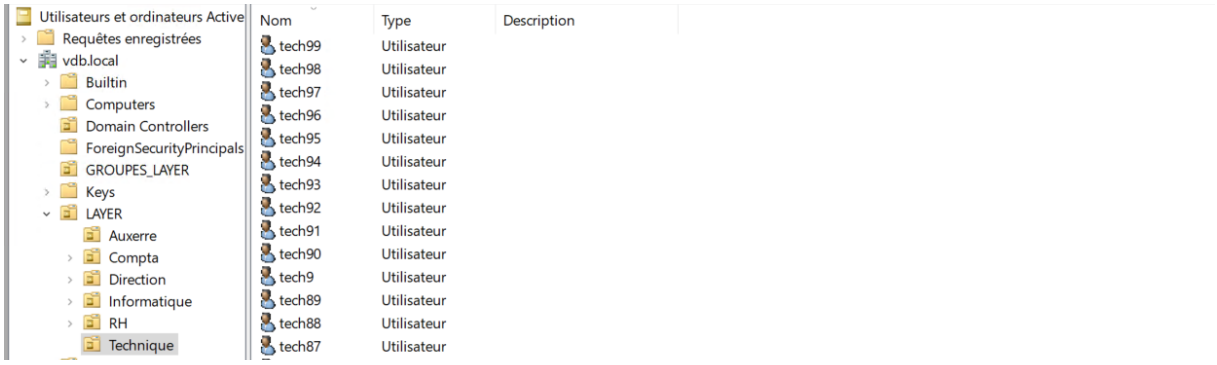

Utilisateurs et ordinateurs Active Directory
Fichier Action Affichage ?
Utilisateurs et ordinateurs Active
Requêtes enregistrées
vdb.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
GROUPES_LAYER
Keys
LAYER
LostAndFound
Managed Service Accoun
POLEFORMATION
Auxerre
Maintenance
Nom
Type
Description
Maintenance Unité d'organis...
g_Auxerre_Maintenance Groupe de séc...

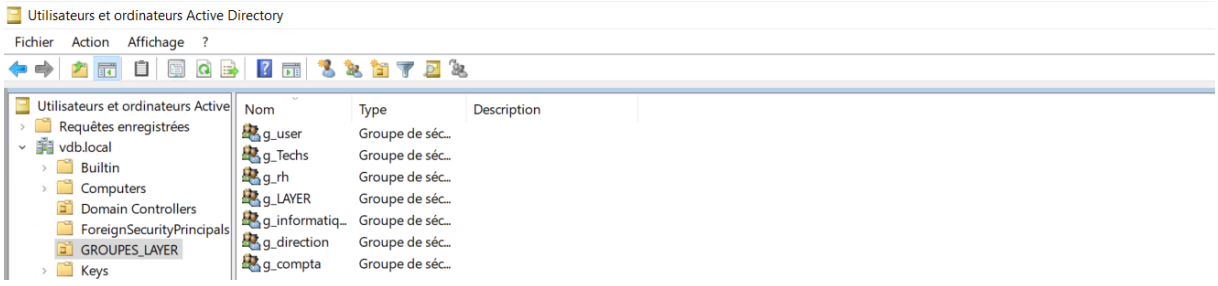
J'ai également créé des scripts toujours via IA permettant d'ajouter des utilisateurs directement via le script, sans avoir besoin de passer par un fichier CSV. Ces scripts sont conçus pour créer rapidement des comptes utilisateurs dans Active Directory en spécifiant directement les informations nécessaires telles que le nom, le prénom, le login, le mot de passe, ainsi que les groupes et les Unités d'Organisation (OU) auxquels ils doivent appartenir.

<u>Voir Script En Annexe</u>





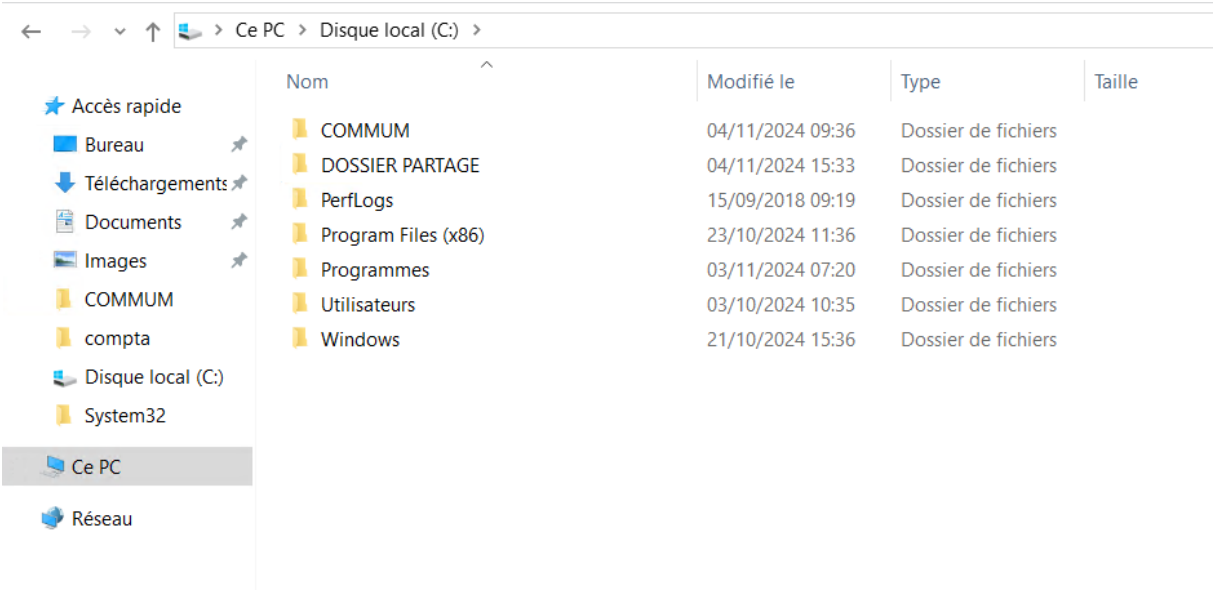


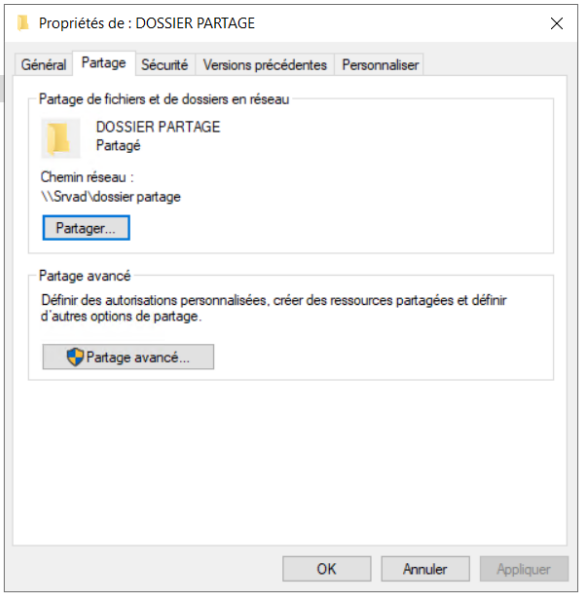


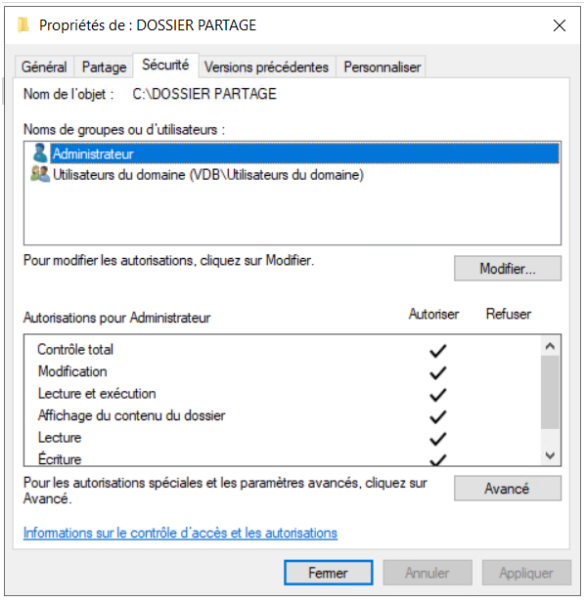
Le script que j'ai créé inclut également la création de dossiers personnels pour chaque utilisateur dans un dossier partagé réseau, tel que \\srvad\dossier_partage. Chaque utilisateur se voit attribuer un répertoire individuel qui lui est propre.

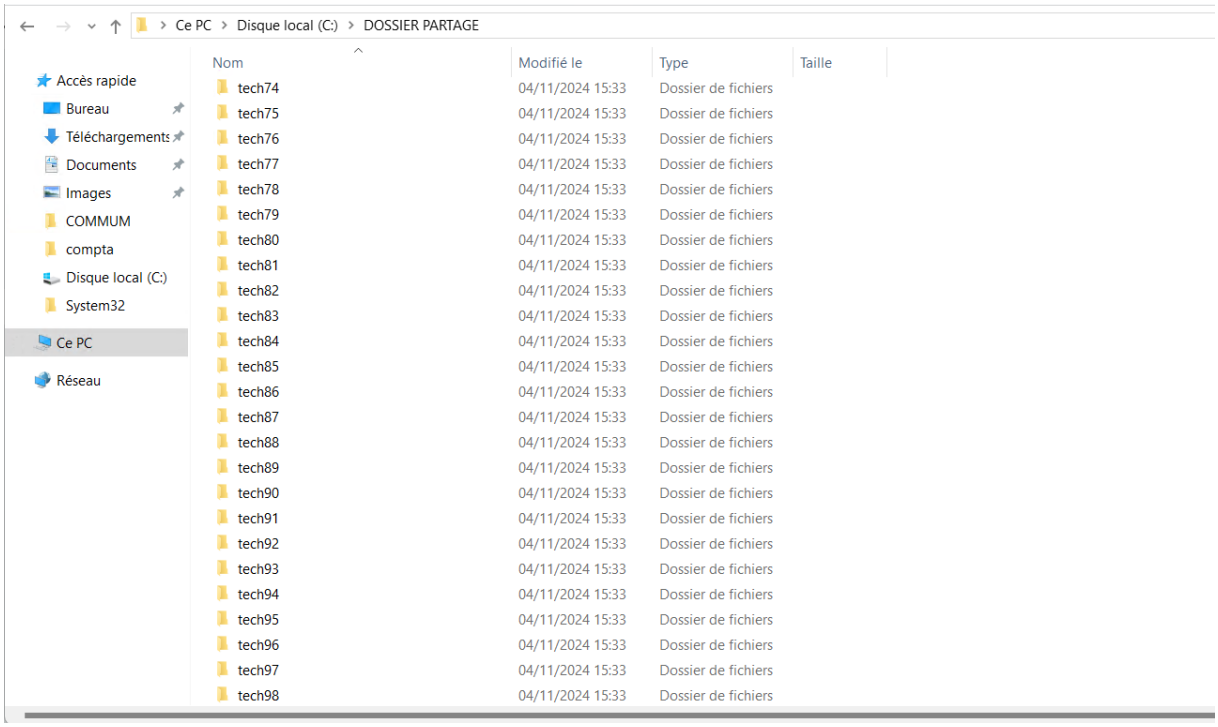
En parallèle, le script gère la configuration des droits ACL (Access Control List) sur ces dossiers personnels. Cela permet de définir des permissions d'accès précises pour chaque utilisateur, tout en assurant que le groupe Administrateurs ait des droits appropriés sur ces répertoires.

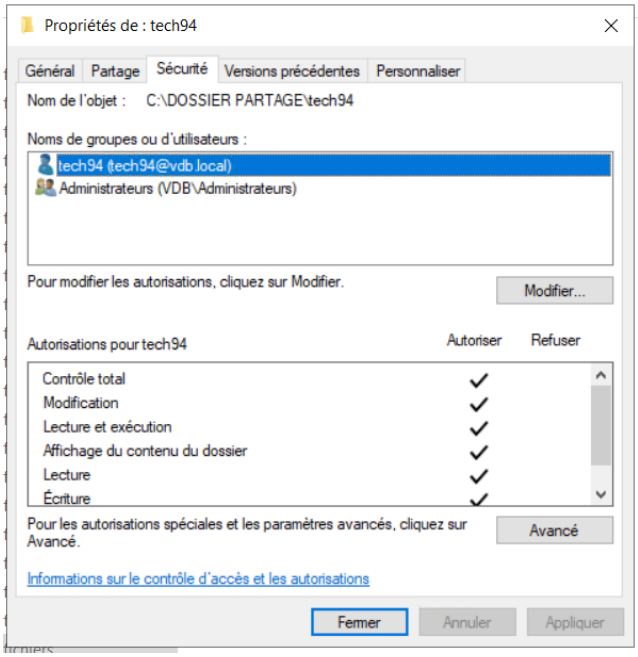
Ainsi, chaque utilisateur a son propre espace de stockage dans le réseau, avec des permissions adaptées à son rôle, tout en garantissant que les administrateurs conservent un contrôle total sur ces ressources partagées.











Cette automatisation rend la gestion des comptes beaucoup plus rapide et moins sujette aux erreurs. Les scripts permettent également de garder une structure d'AD homogène, essentielle pour une administration efficace et pour garantir la sécurité.

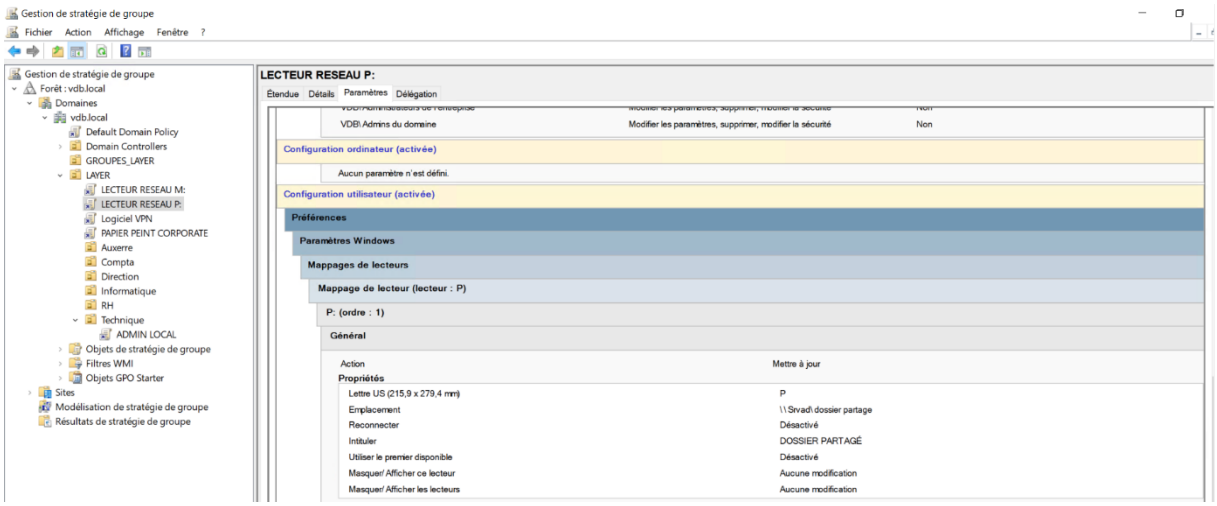
Configuration des GPO (Group Policy Objects)

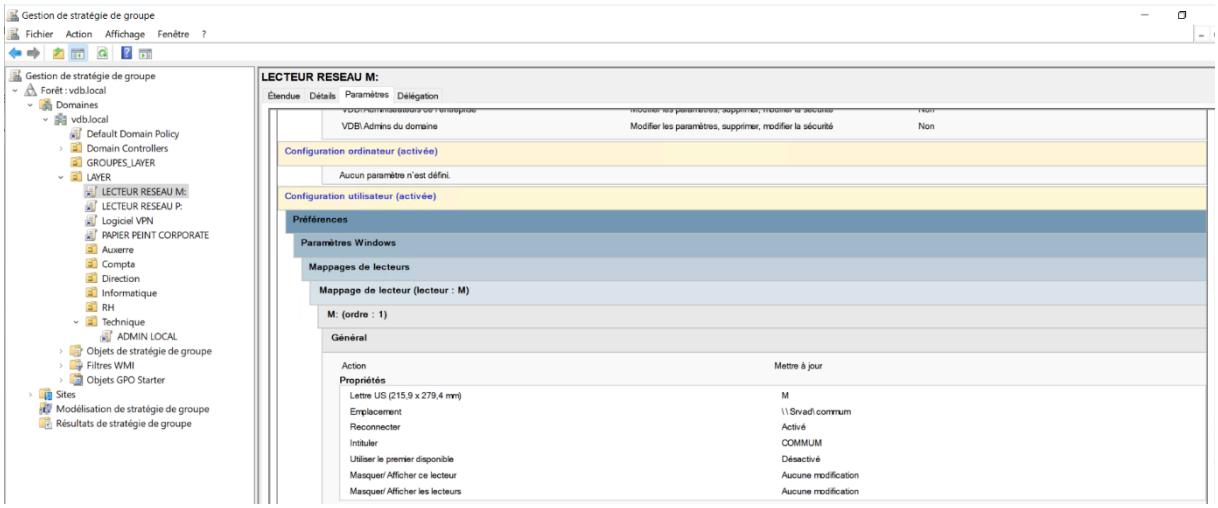
Les GPO permettent d'appliquer des politiques de sécurité, des restrictions et des configurations de manière centralisée aux utilisateurs et aux ordinateurs du domaine. Elles sont essentielles pour contrôler l'environnement utilisateur et s'assurer du respect des normes de sécurité.

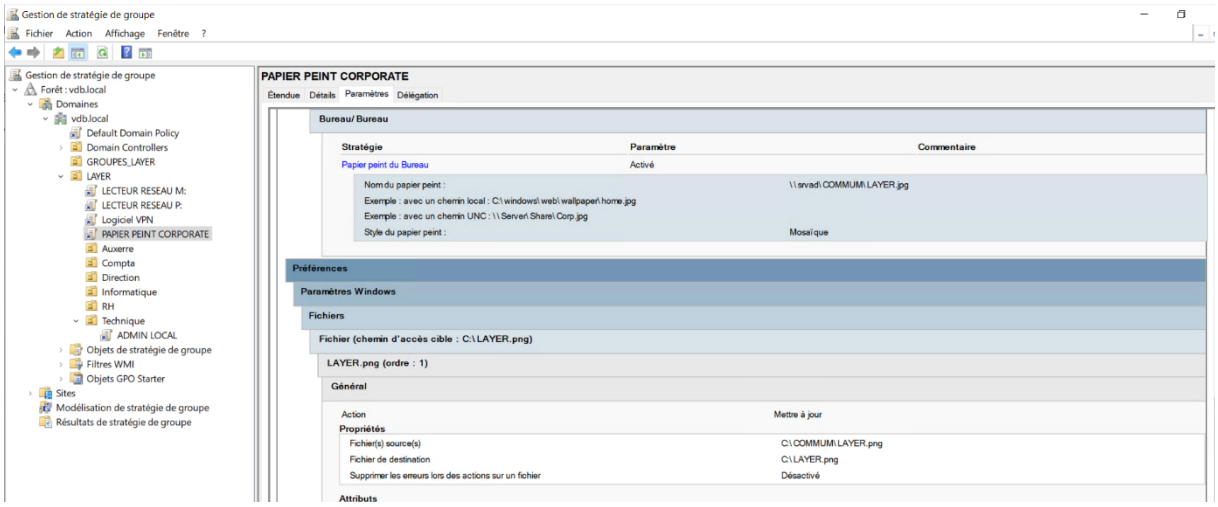
Les GPO peuvent être configurées dans le Gestionnaire de stratégie de groupe (GPMC) en spécifiant des paramètres comme les restrictions d'accès, les scripts de connexion et d'autres règles de sécurité. Les GPO sont ensuite appliquées aux OU ou aux groupes d'utilisateurs/ordinateurs spécifiques.

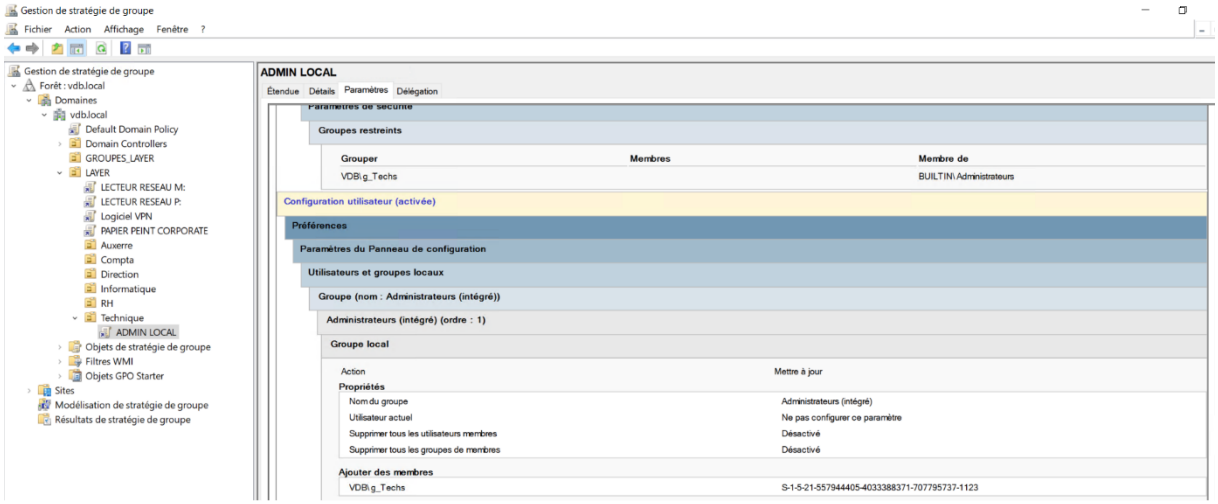
J'ai créé plusieurs **stratégies de groupe (GPO)** pour standardiser l'environnement utilisateur, telles que :

- **Lecteurs réseau** pour monter automatiquement des ressources partagées.
- **Papier peint corporate** pour appliquer un fond d'écran uniforme sur tous les postes.
- **Activation du compte local des techniciens en administrateur local** pour faciliter la gestion des machines par les techniciens.






Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : vdb.local
Domaines
vdb.local
Default Domain Policy
Domain Controllers
GROUPES_LAYER
LAYER
LECTEUR RESEAU M:
LECTEUR RESEAU P:
Logiciel VPN
PAPIER PEINT CORPORATE
Auxerre
Compta
Direction
Informatique
RH
Technique
ADMIN LOCAL
Objets de stratégie de groupe
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie de groupe
Résultats de stratégie de groupe
PAPIER PEINT CORPORATE
Étendue Détails Paramètres Délégation
Bureau/ Bureau
Stratégie
Paramètre
Commentaire
Papier peint du Bureau
Activé
Nom du papier peint :
\\ srvad\ COMMUM\ LAYER.jpg
Exemple : avec un chemin local : C:\ windows\ web\ wallpaper\ home.jpg
Exemple : avec un chemin UNC : \\ Server\ Share\ Corp.jpg
Style du papier peint :
Mosaïque
Préférences
Paramètres Windows
Fichiers
Fichier (chemin d'accès cible : C:\LAYER.png)
LAYER.png (ordre : 1)
Général
Action
Mettre à jour
Propriétés
Fichier(s) source(s)
C:\ COMMUM\ LAYER.png
Fichier de destination
C:\ LAYER.png
Supprimer les erreurs lors des actions sur un fichier
Désactivé
Attributs


Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
Gestion de stratégie de groupe
Forêt : vdb.local
Domaines
vdb.local
Default Domain Policy
Domain Controllers
GROUPES_LAYER
LAYER
LECTEUR RESEAU M:
LECTEUR RESEAU P:
Logiciel VPN
PAPIER PEINT CORPORATE
Auxerre
Compta
Direction
Informatique
RH
Technique
ADMIN LOCAL
Objets de stratégie de groupe
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie de groupe
Résultats de stratégie de groupe
ADMIN LOCAL
Étendue Détails Paramètres Délégation
Groupes restreints
Grouper
Membres
Membre de
VDB\g_Techs
BUILTIN\Administrateurs
Configuration utilisateur (activée)
Préférences
Paramètres du Panneau de configuration
Utilisateurs et groupes locaux
Groupe (nom : Administrateurs (intégré))
Administrateurs (intégré) (ordre : 1)
Groupe local
Action
Mettre à jour
Propriétés
Nom du groupe
Administrateurs (intégré)
Utilisateur actuel
Ne pas configurer ce paramètre
Supprimer tous les utilisateurs membres
Désactivé
Supprimer tous les groupes de membres
Désactivé
Ajouter des membres
VDB\g_Techs
S-1-5-21-557944405-4033388371-707795737-1123

Installation de Windows 10

Les **stations de travail** (Windows 10) doivent être intégrées au domaine pour permettre aux utilisateurs de se connecter à l'aide de leurs identifiants Active Directory (AD). Cela simplifie également la gestion des permissions et des ressources auxquelles les utilisateurs peuvent accéder.

Windows 10 est utilisé pour simuler un poste de travail client, afin de vérifier l'intégration correcte au domaine, la fonctionnalité des services AD/DNS, ainsi que l'accès aux ressources et l'application des GPO.

Configuration du client DNS :

Chaque **poste de travail** est configuré pour utiliser l'adresse **DNS du serveur principal**. Cela garantit une résolution correcte des noms et permet la connexion au domaine sans problème.

Intégration au Domaine :

Pour intégrer une machine Windows 10 au domaine **vdb.local**, on utilise la commande **netdom join**, une méthode simple et rapide en ligne de commande pour rejoindre le domaine. Cela établit une connexion sécurisée entre le poste de travail et le contrôleur de domaine, facilitant ainsi la gestion centralisée des utilisateurs et des politiques.

Configuration de Windows Server 2022 Core

Le **serveur Core** sera configuré en tant que **contrôleur de domaine secondaire**, ce qui offrira une **redondance** pour les services **Active Directory** et **DNS**, contribuant ainsi à renforcer la résilience du domaine.

Prise en main :

La connexion initiale s'effectuera via **ESXi**, qui permet l'accès à la machine virtuelle.

Paramètres réseau via PowerShell :

Pour afficher les **adaptateurs réseau**, la commande utilisée est :

```
Get-NetAdapter
```

Pour configurer l'**adresse IP**, le **masque** et la **passerelle**, on utilise les commandes suivantes :

```
New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress "172.17.10.5" -PrefixLength 24 -DefaultGateway "172.17.10.1"
```

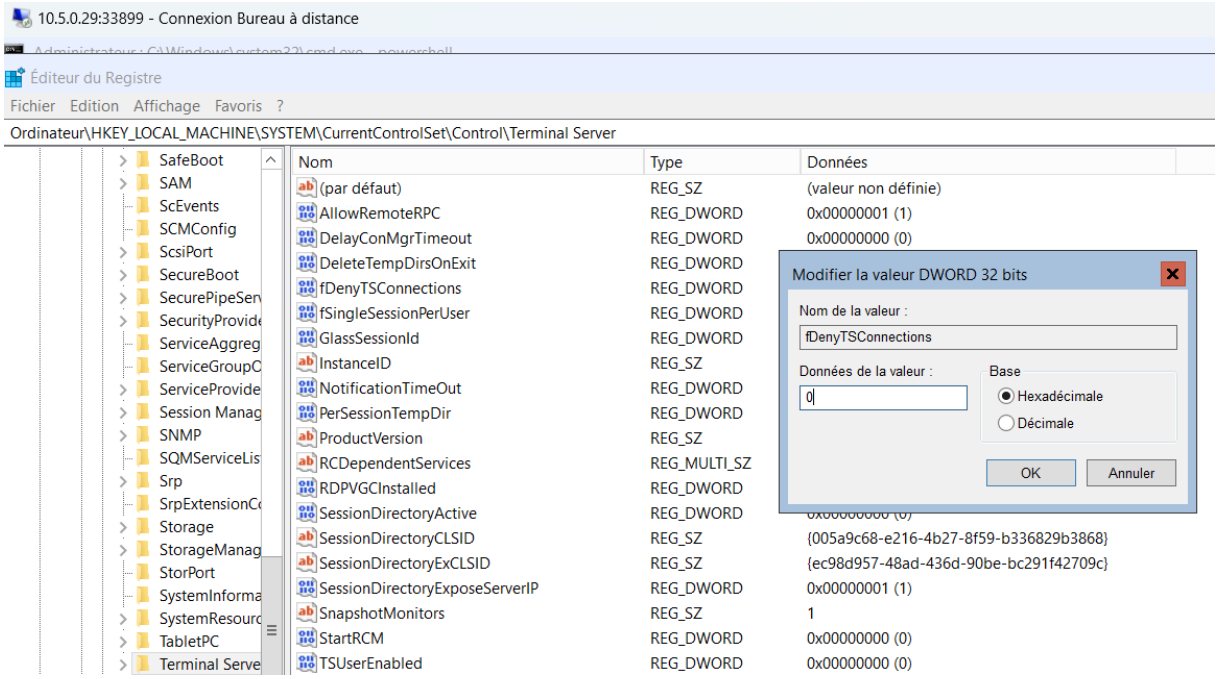
Pour spécifier le serveur DNS, la commande est :

```
Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ServerAddresses "172.17.10.2"
```

Activation du bureau à distance :

Le bureau à distance est activé via une modification du registre. On utilise la commande suivante pour permettre les connexions RDP sur le serveur Core :

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v "fDenyTSConnections" /t REG_DWORD /d 0 /f
```




```
PS C:\Users\Administrateur.VDB> Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server" | Select-Object fDenyTSConnections
>>

fDenyTSConnections
------------------
                0
```

Cela permet d'activer les connexions à distance et de gérer le serveur Core depuis une machine cliente.

Cette configuration prépare le serveur pour son rôle de contrôleur de domaine secondaire, tout en assurant une gestion réseau optimale et une facilité d'administration à distance.

Installation des services AD et DNS sur le serveur Core

La promotion du serveur **Core** en tant que **contrôleur de domaine secondaire** et en **serveur DNS répliqué** est essentielle pour garantir que les services **Active Directory** (AD) et **DNS** sont toujours disponibles, même en cas d'indisponibilité du serveur principal. Cela assure la **continuité du service** et minimise les risques d'interruptions pour les utilisateurs et les applications.

Installation des services AD et DNS :

1. **Commande pour installer les fonctionnalités AD et DNS** :
   Le serveur **Core** doit avoir les services nécessaires pour gérer l'Active Directory et le DNS. La commande suivante permet d'installer **Active Directory Domain Services** (AD-DS) et **DNS** :

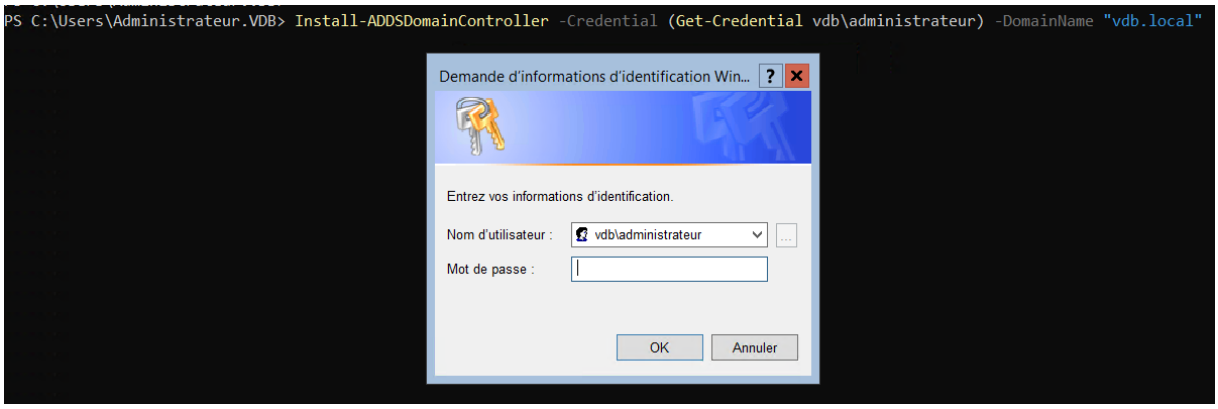
```
Install-WindowsFeature -Name AD-Domain-Services, DNS -IncludeManagementTools
```

Cette commande installe les services requis ainsi que les outils de gestion pour administrer le serveur AD et DNS.

Promotion du serveur Core en contrôleur de domaine secondaire :

Une fois les services installés, le serveur doit être promu en contrôleur de domaine secondaire pour assurer la **réplication**de l'AD et du DNS. La commande de promotion est la suivante :

```
Install-ADDSDomainController -Credential (Get-Credential vdb\administrateur) -DomainName "vdb.local"
```



- Cette commande démarre le processus de promotion et associe le serveur à l'AD existant dans le domaine **vdb.local**.
- **Get-Credential** vous invite à entrer les informations d'identification d'un utilisateur ayant les privilèges nécessaires (comme **administrateur**).
- Le serveur Core sera alors configuré pour répliquer les données du serveur principal et devenir un contrôleur de domaine secondaire.

L'objectif est de garantir que l'Active Directory et le DNS du serveur principal sont répliqués vers le serveur Core. Cela crée une **redondance** qui assure la disponibilité continue des services, même si le serveur principal devient indisponible.

Impact de la redondance :

La mise en place de cette redondance pour **l'Active Directory** et le **DNS** assure non seulement une **résilience accrue** de l'infrastructure, mais elle permet également une **continuité de service** sans interruption pour les utilisateurs et le réseau en cas de défaillance du serveur principal.

Ainsi, ce processus rend le serveur Core pleinement opérationnel en tant que contrôleur de domaine et serveur DNS secondaire, tout en offrant une haute disponibilité pour l'infrastructure Active Directory.

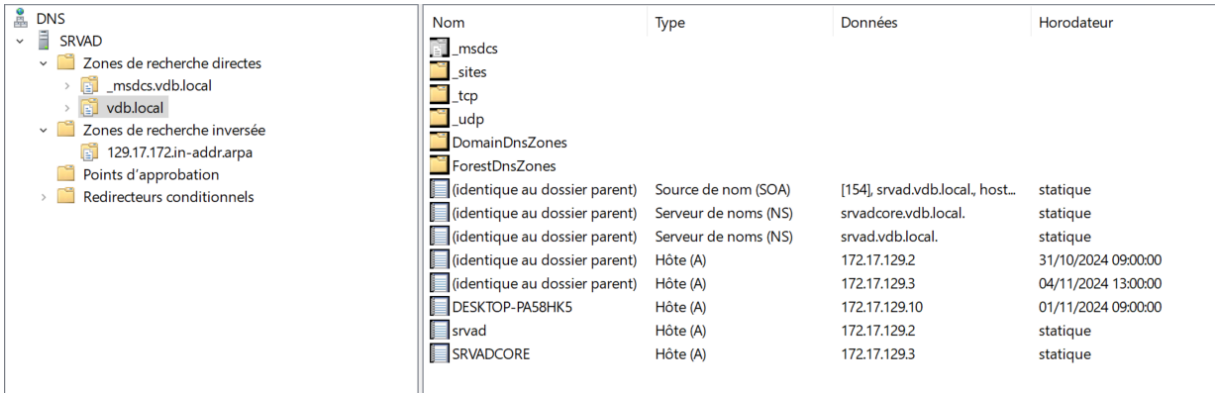
Partie 2 – Validation

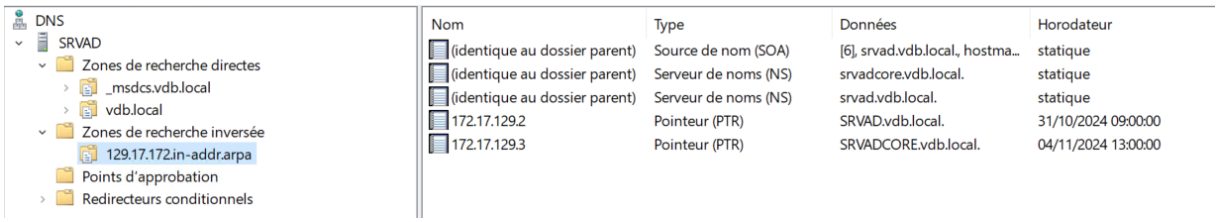
Vérifications de la Réplication

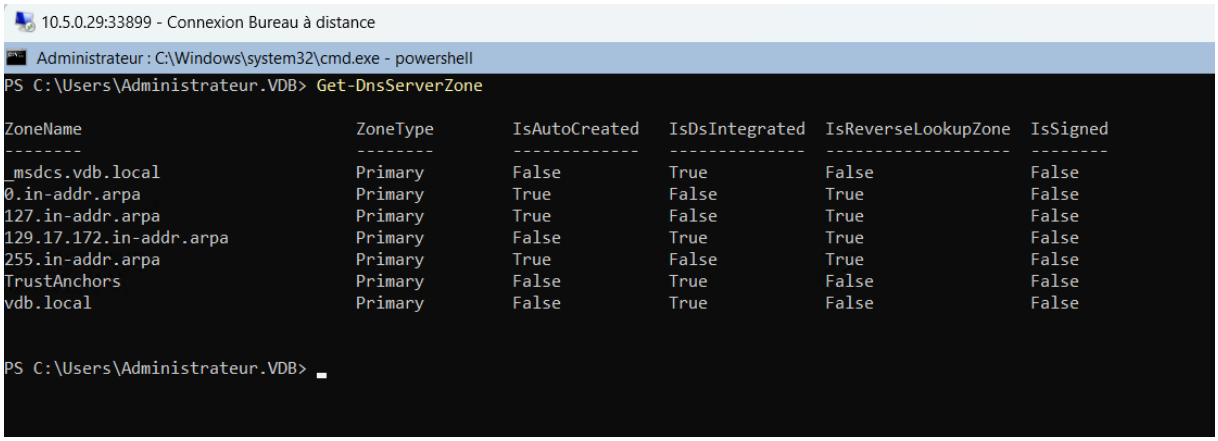
Il est essentiel de vérifier régulièrement la **réplication** entre les contrôleurs de domaine pour assurer la **cohérence** et la **disponibilité** des données dans l'Active Directory (AD) et les services DNS. Cela garantit que les informations sur les utilisateurs, groupes et autres objets AD, ainsi que les enregistrements DNS, sont bien synchronisées entre tous les contrôleurs de domaine, assurant une gestion fluide et une authentification correcte.

Vérification de la réplication DNS :

- Vérifier que les enregistrements DNS sur les contrôleurs de domaine sont synchronisés est crucial pour garantir que la résolution des noms fonctionne correctement.
- **Commande de vérification DNS** : Utilisez des outils comme **nslookup** ou **dnscmd** pour vérifier que les enregistrements DNS sont répliqués entre les serveurs DNS.

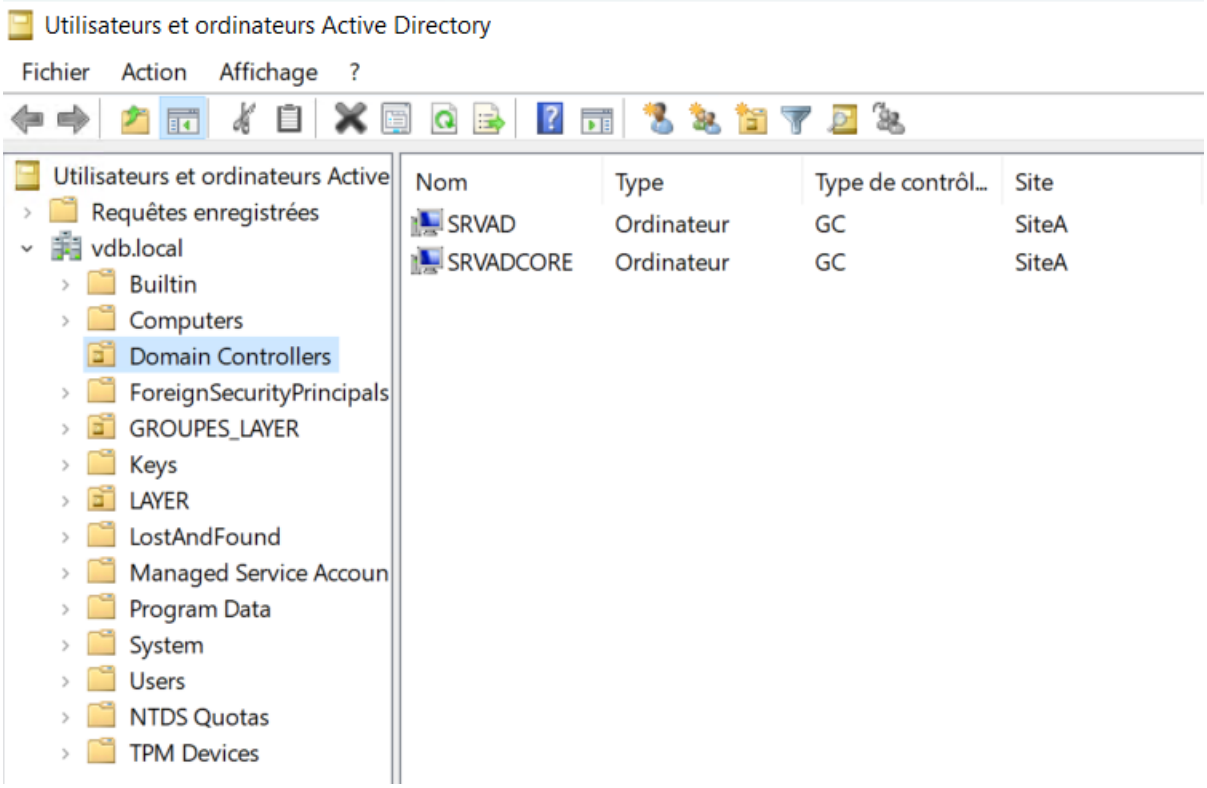






Vérification de la réplication de l'Active Directory :

- Il est important de confirmer que **les utilisateurs**, **les groupes** et **les autres objets AD** sont bien répliqués entre les contrôleurs de domaine.




```
PS C:\Users\Administrateur.VDB> Get-ADOrganizationalUnit -Filter * | Select-Object Name, DistinguishedName
>>

Name               DistinguishedName
----               -----------------
Domain Controllers OU=Domain Controllers,DC=vdb,DC=local
LAYER              OU=LAYER,DC=vdb,DC=local
Compta             OU=Compta,OU=LAYER,DC=vdb,DC=local
RH                 OU=RH,OU=LAYER,DC=vdb,DC=local
Direction          OU=Direction,OU=LAYER,DC=vdb,DC=local
Informatique       OU=Informatique,OU=LAYER,DC=vdb,DC=local
Technique          OU=Technique,OU=LAYER,DC=vdb,DC=local
GROUPES_LAYER      OU=GROUPES_LAYER,DC=vdb,DC=local
Auxerre            OU=Auxerre,OU=LAYER,DC=vdb,DC=local


PS C:\Users\Administrateur.VDB> _
```

- **Commande de vérification AD** : La commande suivante permet de vérifier l'état de la réplication des objets AD :

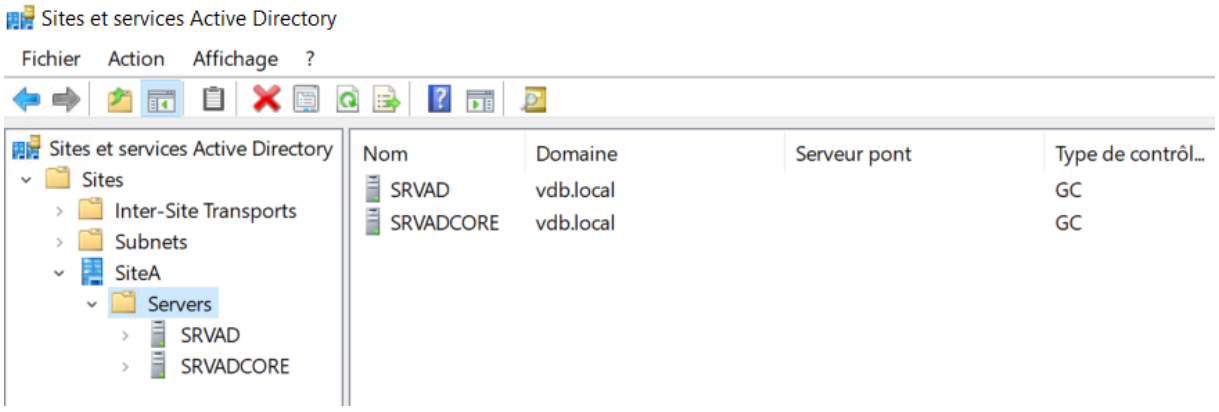
repadmin /replsummary

```
PS C:\Users\Administrateur.VDB> repadmin /replsummary
>>
Heure de début du résumé de la réplication : 2024-11-04 15:55:59

Début de la collecte des données pour le résumé de la réplication ;
cette opération peut prendre un certain temps :
  .....


DSA source              différence max    nb échecs %%   erreur
 SRVAD                      01m:27s    0 /   5    0
 SRVADCORE                  05m:39s    0 /   5    0


DSA de destination      différence max    nb échecs %%   erreur
 SRVAD                      05m:39s    0 /   5    0
 SRVADCORE                  01m:27s    0 /   5    0


PS C:\Users\Administrateur.VDB>
```

Cette commande fournit un résumé de la réplication des contrôleurs de domaine, indiquant si la réplication a réussi ou échoué, ainsi que des détails sur les erreurs potentielles.

Vérification des Sites et Sous-Réseaux :

- Il est également important de vérifier que les **configurations de sites** AD et **les sous-réseaux** associés sont correctement configurés et répliqués. Les sites et sous-réseaux permettent de contrôler la manière dont la réplication se fait entre les contrôleurs de domaine en fonction de leur emplacement géographique et réseau.



Commandes de vérification de la réplication :

1. **repadmin /replsummary** : Cette commande fournit un aperçu de l'état global de la réplication entre tous les contrôleurs de domaine dans le domaine. Elle aide à identifier les problèmes de réplication, y compris les erreurs de connexion et les divergences de données.

2. **w32tm /query /status** : Cette commande permet de vérifier l'état de la **synchronisation du temps** entre les serveurs. La synchronisation horaire est essentielle pour éviter les erreurs liées à des horloges de serveurs désynchronisées, ce qui peut affecter la réplication AD.

```
PS C:\Users\Administrateur.VDB> w32tm /query /status
>>
Indicateur de dérive : 0(Aucun avertissement)
Couche : 2 (Référence secondaire, synchronisée par (S)NTP)
Précision : -23 (119.209ns par battement)
Délai de racine : 0.0015947s
Dispersion de racine : 10.0213984s
ID de référence : 0xAC118102 (IP de la source :  172.17.129.2)
Heure de la dernière synchronisation réussie : 04/11/2024 15:59:24
Source : SRVAD.vdb.local
Intervalle d'interrogation : 7 (128s)

PS C:\Users\Administrateur.VDB>
```

3. **w32tm /resync** : Si des problèmes de synchronisation du temps sont détectés, cette commande force la **synchronisation de l'horloge** entre le serveur local et un serveur NTP (Network Time Protocol), garantissant ainsi la précision de l'heure pour la réplication et les services AD.

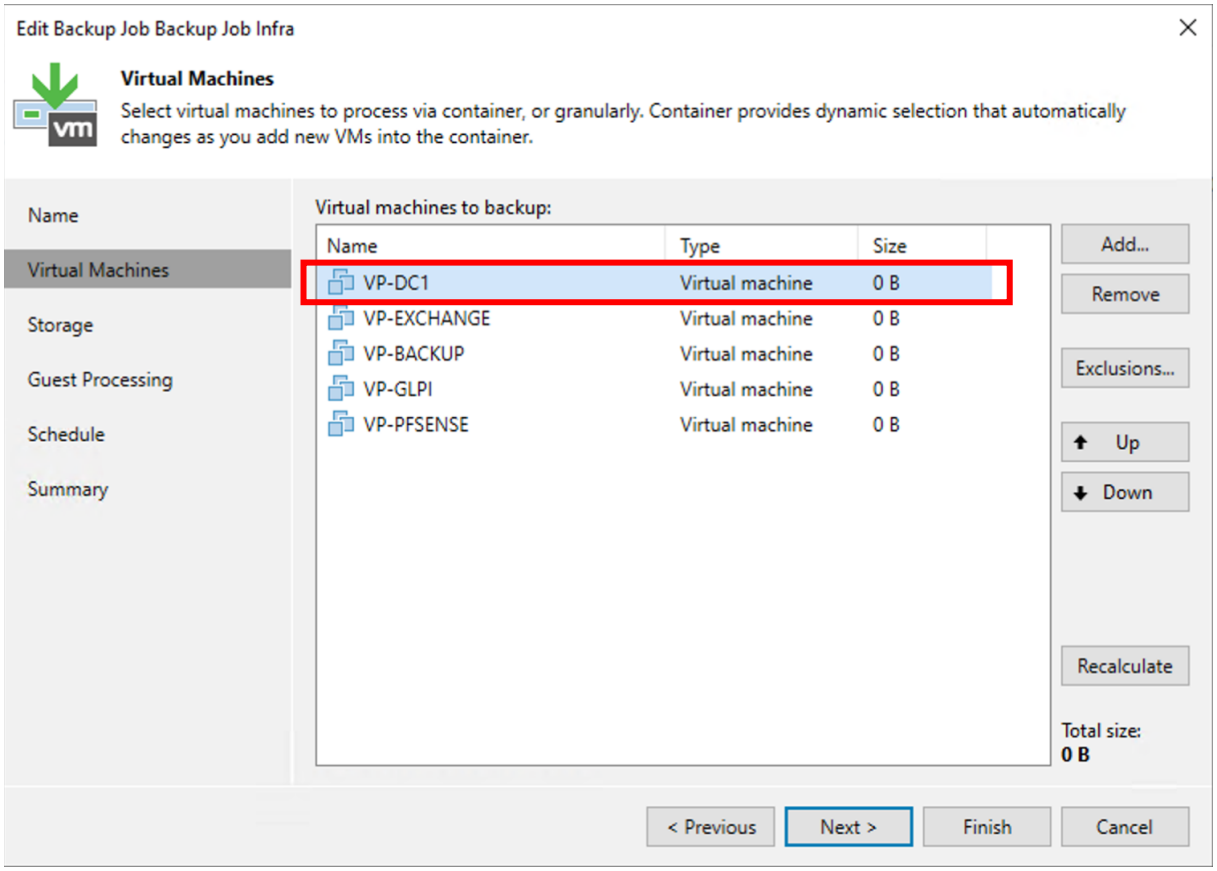
Importance de la réplication et de la vérification de la synchronisation :

La réplication garantit que les utilisateurs et groupes peuvent **s'authentifier** et **accéder** aux ressources indépendamment du contrôleur de domaine auquel ils se connectent. Cela permet de maintenir une **continuité des services** et évite les interruptions de service dues à une divergence des données entre les contrôleurs de domaine.

Les **vérifications de synchronisation** permettent de détecter tout problème de **latence** ou de divergence de données, assurant ainsi que les deux serveurs restent parfaitement alignés.

Gérer le patrimoine informatique

L'ensemble du patrimoine informatique est rigoureusement recensé à l'aide d'un outil de gestion des actifs, assurant une traçabilité complète de l'infrastructure. La redondance du service Active Directory est assurée grâce à la réplication entre un contrôleur de domaine principal (interface graphique) et un contrôleur secondaire sous Windows Server Core, garantissant la disponibilité continue des services d'annuaire et DNS. Les référentiels et bonnes pratiques sont respectés pour assurer une gestion cohérente des droits, attribués selon les habilitations des utilisateurs. La continuité de service est renforcée par la solution de sauvegarde Veeam, déployée par l'entreprise, qui permet des sauvegardes régulières et fiables. Les restaurations sont testées et validées, assurant un retour rapide à la normale en cas d'incident. Enfin, tout écart vis-à-vis des règles d'usage des ressources numériques est systématiquement détecté et signalé pour maintenir un environnement sécurisé et conforme.



Partie 3 – Veille technologique

Afin de garantir la pérennité, la sécurité et l'efficacité de l'infrastructure mise en place, plusieurs axes d'amélioration sont envisagés pour optimiser les performances, la gestion des ressources et renforcer la résilience des services. Voici un aperçu des évolutions possibles pour cette infrastructure fraîchement configurée :

Amélioration des ressources et de l'isolation réseau :

- **Allocation dynamique des ressources** : Grâce à ESXi, il est possible d'ajuster automatiquement les ressources allouées à chaque machine virtuelle en fonction de ses besoins, optimisant ainsi les performances et l'efficacité.
- **Isolation réseau renforcée** : La mise en place de VLANs (Virtual LANs) permet de segmenter davantage les sous-réseaux internes, offrant ainsi une meilleure sécurité et une gestion plus fine du trafic réseau entre les différentes zones de l'infrastructure.

Amélioration de la gestion du trafic et des services réseau :

- **Segmentation avancée du trafic** : En ajoutant des règles spécifiques, il est possible de séparer plus efficacement le trafic interne par type de service, comme les requêtes DNS ou les authentifications AD, améliorant ainsi la sécurité et la gestion des flux réseau.
- **Serveur DHCP sur pfSense** : Configurer pfSense en tant que serveur DHCP permet de gérer dynamiquement les adresses IP des machines virtuelles, réduisant la dépendance à un serveur Windows pour cette fonction et offrant davantage de flexibilité et de contrôle sur la distribution des adresses.

Amélioration de la configuration DHCP :

- **Temps de bail optimisé** : Réduire le temps de bail pour les réseaux à forte mobilité, où les appareils se connectent fréquemment et temporairement, permet une gestion plus dynamique des adresses IP et une utilisation plus efficace des ressources réseau.
- **Redondance DHCP (Failover)** : Mettre en place un serveur DHCP secondaire en mode failover pour assurer la continuité du service en cas de défaillance du serveur principal, garantissant ainsi une distribution ininterrompue des adresses IP et la résilience du réseau.

Amélioration de la gestion des ressources et de la sécurité :

- **Attribution de permissions spécifiques** : Ajouter des commandes **Set-ACL** dans les scripts pour appliquer des permissions personnalisées sur les ressources partagées, assurant ainsi un contrôle d'accès précis en fonction des rôles et des besoins des utilisateurs.
- **Gestion des mots de passe** : Générer des mots de passe temporaires pour les nouveaux utilisateurs et configurer l'obligation de modification lors de leur première connexion, renforçant ainsi la sécurité et garantissant que chaque utilisateur choisisse un mot de passe personnel et sécurisé.

Amélioration de la gestion des groupes et de l'automatisation :

- **Groupes de sécurité GPO** : Associer des **GPO** spécifiques aux groupes de sécurité **Active Directory** pour affiner le contrôle d'accès, en appliquant des politiques de sécurité adaptées à chaque groupe d'utilisateurs ou de machines.
- **Scripts automatisés** : Déployer automatiquement des imprimantes réseau ou des unités mappées via des scripts, simplifiant ainsi la gestion des ressources et garantissant une configuration cohérente et rapide sur toutes les stations de travail.

Amélioration de l'intégration et de la gestion des profils utilisateurs :

- **Scripts d'intégration** : Mettre en place un script de pré-configuration pour automatiser le processus de jonction des machines au domaine, réduisant ainsi les erreurs manuelles et accélérant le déploiement.
- **Redirection de profil utilisateur** : Configurer la redirection des profils utilisateurs vers un serveur dédié pour centraliser et sécuriser les données utilisateurs, tout en facilitant la gestion des profils dans un environnement de domaine.

Centralisation des logs et surveillance :

- Mettre en place une **solution de gestion des logs centralisée** SexiLog pour collecter, analyser et alerter sur des événements de sécurité ou des dysfonctionnements dans l'infrastructure.
- Configurer des **alertes proactives** avec par exemple **PRTG** pour avertir en temps réel des problèmes éventuels sur les serveurs, les services AD/DNS ou les machines clients.

Gestion des mises à jour et patching :

- Installer un **serveur WSUS** pour centraliser les mises à jour Windows et assurer qu'aucun patch de sécurité ne soit omis.
- Installer un **logiciel tiers** pour centraliser les mises à jour de l'infrastructure et assurer qu'aucun patch de sécurité ne soit omis.

Sauvegarde et récupération de données :

- Intégrer une **solution de sauvegarde automatique** pour les données sensibles et les configurations critiques de l'infrastructure (comme les bases de données AD, DNS et les fichiers partagés).
- Tester et affiner régulièrement le processus de **récupération après sinistre (DRP)** afin de garantir la résilience de l'infrastructure en cas de défaillance majeure.

Conclusion

Ces améliorations futures permettraient non seulement d'optimiser les performances, la sécurité et la fiabilité de l'infrastructure, mais aussi d'envisager une évolutivité à long terme en s'adaptant aux besoins croissants de l'entreprise. Chaque étape sera évaluée et mise en œuvre de manière progressive pour garantir une infrastructure stable et résiliente.

ANNEXE

```
# Paramètres de base pour créer plusieurs utilisateurs
$nomDeBase = "tech"  # Nom de base des utilisateurs
$nombreUtilisateurs = 100  # Nombre d'utilisateurs à créer
$cheminDeBase = "\\Srvad\dossier partage"  # Chemin de base pour les dossiers personnels

# Variable pour définir dynamiquement le chemin de l'OU pour les utilisateurs dans AD
$ouPath = "OU=Technique,OU=LAYER,DC=vdb,DC=local"  # Modifie ce chemin si nécessaire
$ouName = "Technique"  # Nom de l'OU cible à vérifier et créer si nécessaire

# Chemin de l'OU pour les groupes
$groupOUPath = "OU=GROUPES_LAYER,DC=vdb,DC=local"  # OU spécifique pour les groupes

# Mot de passe pour chaque utilisateur
$motDePasse = "btssio89$"

# Nom du groupe ou de l'utilisateur administrateur ayant le contrôle
$administrateur = "Administrateurs"  # Nom du groupe administrateur local

# Variable pour définir dynamiquement le groupe dans lequel ajouter les utilisateurs
$groupName = "g_Techs"  # Nom du groupe à créer et auquel ajouter les utilisateurs

# Vérifier si l'OU pour les utilisateurs existe et la créer si elle est absente
if (-Not (Get-ADOrganizationalUnit -Filter {Name -eq $ouName} -SearchBase
"OU=LAYER,DC=vdb,DC=local" -ErrorAction SilentlyContinue)) {
New-ADOrganizationalUnit -Name $ouName -Path "OU=LAYER,DC=vdb,DC=local"
Write-Host "L'OU '$ouName' a été créée dans 'OU=LAYER,DC=vdb,DC=local'."
} else {
Write-Host "L'OU '$ouName' existe déjà dans 'OU=LAYER,DC=vdb,DC=local'."
}

# Vérifier si le groupe existe dans l'OU pour les groupes et le créer si nécessaire
if (-Not (Get-ADGroup -Filter {Name -eq $groupName} -SearchBase $groupOUPath -ErrorAction
SilentlyContinue)) {
New-ADGroup -Name $groupName -GroupScope Global -Path $groupOUPath -GroupCategory
Security
Write-Host "Le groupe '$groupName' a été créé dans '$groupOUPath'."
} else {
Write-Host "Le groupe '$groupName' existe déjà dans '$groupOUPath'."
}

# Boucle pour créer chaque utilisateur avec un numéro incrémental
for ($i = 1; $i -le $nombreUtilisateurs; $i++) {
# Définir les informations de l'utilisateur
$samAccountName = "$nomDeBase$i"  # Exemple : user1, user2, user3...
$userPrincipalName = "$samAccountName@vdb.local"
$repertoirePersonnel = Join-Path -Path $cheminDeBase -ChildPath $samAccountName

# Création de l'utilisateur dans Active Directory
New-ADUser `
-Name $samAccountName `
```

```
-Path $ouPath `
-AccountPassword (ConvertTo-SecureString $motDePasse -AsPlainText -Force) `
-UserPrincipalName $userPrincipalName `
-SamAccountName $samAccountName `
-Enabled $true

Write-Host "Utilisateur '$samAccountName' créé dans Active Directory avec succès."

# Ajouter l'utilisateur au groupe spécifié
Add-ADGroupMember -Identity $groupName -Members $samAccountName
Write-Host "Utilisateur '$samAccountName' ajouté au groupe '$groupName'."

# Vérifier si le dossier personnel existe déjà
if (-Not (Test-Path -Path $repertoirePersonnel)) {
# Créer le répertoire personnel
New-Item -ItemType Directory -Path $repertoirePersonnel -Force
Write-Host "Dossier personnel créé pour $samAccountName à $repertoirePersonnel."
} else {
Write-Host "Le dossier personnel pour $samAccountName existe déjà à $repertoirePersonnel."
}

# Récupérer les ACL du dossier personnel
$acl = Get-Acl -Path $repertoirePersonnel

# Désactiver l'héritage et supprimer les permissions héritées
$acl.SetAccessRuleProtection($true, $false)

# Supprimer toutes les règles d'accès existantes
$acl.Access | ForEach-Object { $acl.RemoveAccessRuleAll($_) }

# Ajouter les droits de contrôle total pour l'utilisateur
$userAccessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule("$samAccountName", "FullControl",
"ContainerInherit,ObjectInherit", "None", "Allow")
$acl.AddAccessRule($userAccessRule)

# Ajouter les droits de contrôle total pour les administrateurs
$adminAccessRule = New-Object
System.Security.AccessControl.FileSystemAccessRule("$administrateur", "FullControl",
"ContainerInherit,ObjectInherit", "None", "Allow")
$acl.AddAccessRule($adminAccessRule)

# Appliquer les modifications ACL sur le dossier
Set-Acl -Path $repertoirePersonnel -AclObject $acl

Write-Host "Permissions de contrôle total définies pour $samAccountName et $administrateur sur
$repertoirePersonnel."
}
```

BTS Services informatiques aux organisations - SISR
Session 2025

E6 – Support et mise à disposition de services informatiques
Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :
Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- ***Layer Bureautique et Informatique*** *est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro.*
- *La problématique principale réside dans le besoin fondamental d'un service de messagerie fiable, permettant aux utilisateurs de communiquer efficacement par courriel au sein de l'organisation. Ce service doit offrir à la fois sécurité, continuité et facilité d'intégration avec les outils internes de l'entreprise.*
- *La solution choisie consiste à mettre en place un serveur de messagerie Exchange, reconnu pour sa robustesse et sa capacité à gérer de manière centralisée les courriels, les calendriers et les contacts. Cette solution permettra également de bénéficier d'une gestion simplifiée et d'une intégration étroite avec Active Directory.*

Intitulé de la réalisation professionnelle

Déploiement d'une Solution de Messagerie via Exchange

Période de réalisation : 17/02/25 - 20/02/2025 **Lieu :** Auxerre
Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE
- GERER LE PATRIMOINE INFORMATIQUE
- ORGANISER SON DEVELOPPEMENT PROFESIONNEL
- DEVELOPPER LA PRESENCE EN LIGNE DE L'ORGANISATION

Conditions de réalisation

- **Ressources disponibles (Situation avant RP)**
  Nous disposons d'un serveur ESXi, une infrastructure fonctionnelle comprenant un Active Directory avec un service DNS fonctionnel, ainsi que d'un domaine public configuré pour l'entreprise.
- **Résultats attendus (Situation après RP)**
  Une solution de messagerie Exchange fonctionnelle et sécurisée, permettant à l'ensemble des utilisateurs de communiquer par courriel électronique de manière fiable et protégée.
- **Durée de réalisation**
  La mise en place de la solution a duré environ 4 jours, incluant les réunions, le temps nécessaire à l'installation du serveur et à la recherche d'informations pertinentes pour la configuration.

Modalités d'accès à cette réalisation professionnelle.

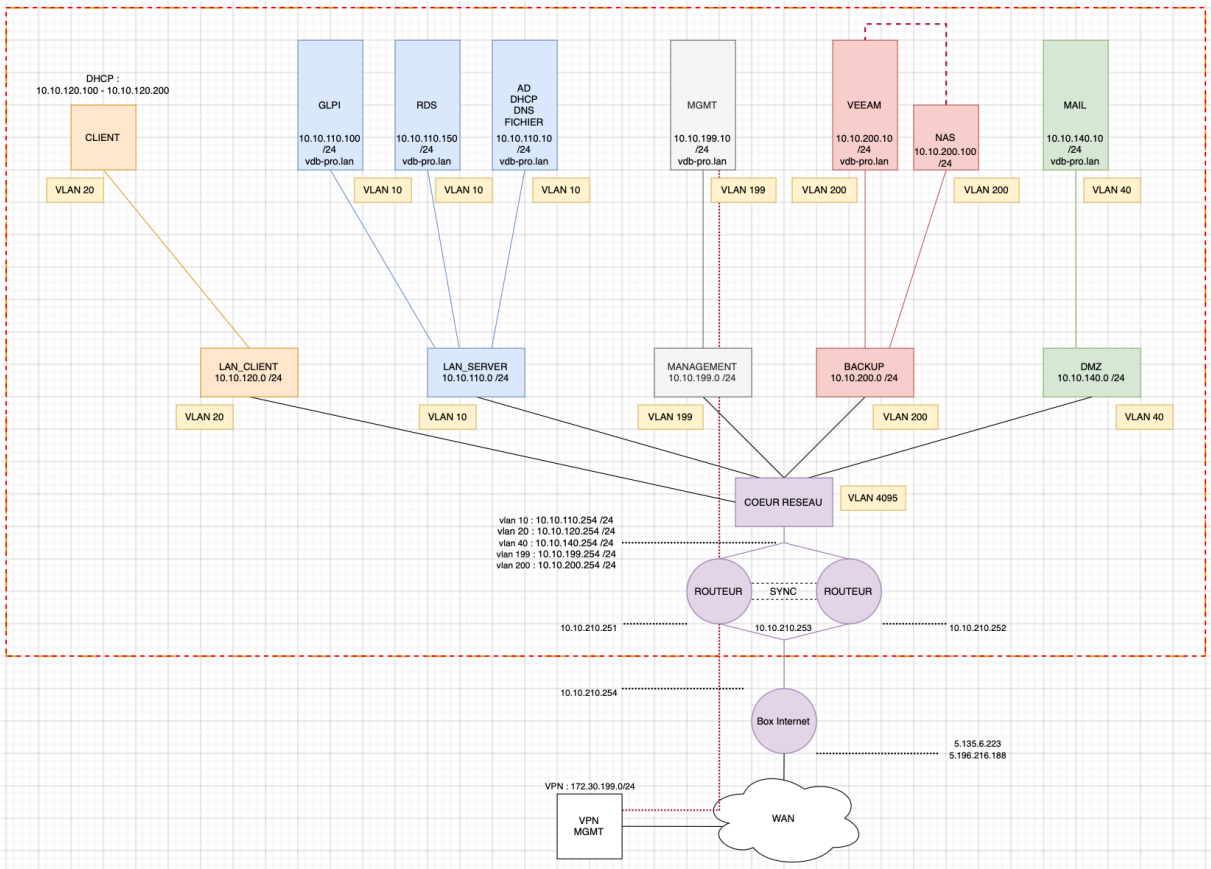
https://portfolio.vdb-pro.fr *mdp : Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

Dans le cadre de l'infrastructure personnelle que j'ai mise en place pour l'entreprise **vdb-pro**, j'ai conçu un environnement réseau complet intégrant un service de messagerie basé sur un serveur **Microsoft Exchange 2019**. Ce serveur permet aux utilisateurs de l'entreprise d'envoyer et de recevoir des courriels de manière sécurisée, tout en assurant la fiabilité des communications internes et externes.

Il offrira également un accès à une interface web sécurisé par un certificat, permettant la consultation des messages à distance via un simple navigateur internet.

La gestion des comptes utilisateurs et des droits d'accès à ce service de messagerie sera assurée par **l'Active Directory**, préalablement mis en place dans le cadre d'une autre Réalisation Professionnelle. Cela garantit une centralisation de l'authentification et une meilleure gestion des ressources au sein de l'organisation.



Mise en place d'une machine virtuelle

Dans le cadre de la mise en œuvre d'un service de messagerie via Microsoft Exchange Server 2019, une machine virtuelle dédiée a été provisionnée. Cette VM repose sur le système d'exploitation **Windows Server 2022**, et ses ressources ont été ajustées en fonction des recommandations Microsoft et des contraintes de la maquette.

Configuration recommandée par Microsoft :	Configuration utilisée dans la maquette :
Système d'exploitation : - Windows Server 2022 **Mémoire vive (RAM)** : - 16 Go **Processeur** : - 4 vCPU **Stockage** : - Volume **NTFS** pour le système - Volume **NTFS** ou **ReFS** pour la BDD	**Système d'exploitation** : - Windows Server 2022 **Mémoire vive (RAM)** : - 10 Go **Processeur** : - 4 vCPU **Stockage** : - Volume **NTFS** 100 Go OS - Volume **ReFS** 100Go BDD

Remarque : Exchange Server prend en charge les volumes formatés en **NTFS** ou **ReFS** selon l'usage. Toutefois, **ReFS ne peut pas être utilisé** pour les fichiers binaires ou l'installation du système.

Exigences en termes d'espace disque

D'après la documentation officielle de Microsoft, les prérequis en matière d'espace disque sont les suivants :

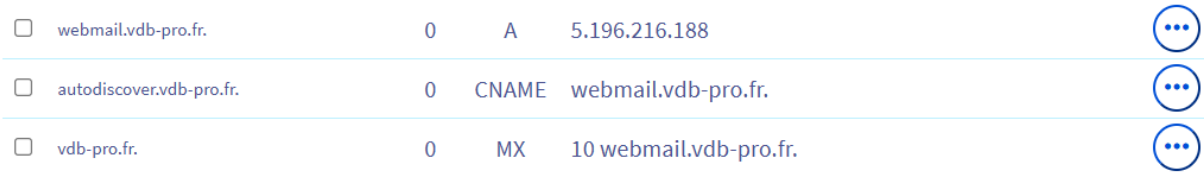
- Minimum **30 Go** d'espace libre sur la partition d'installation d'Exchange
- Minimum **200 Mo** libres sur la partition système
- Minimum **500 Mo** libres sur la partition dédiée à la base de données de file d'attente
- Il est toutefois recommandé de prévoir un espace **beaucoup plus conséquent** pour les bases de données, en fonction du nombre d'utilisateurs et de l'usage de la messagerie.

Préparation DNS et intégration au domaine

Preparation du DNS publique

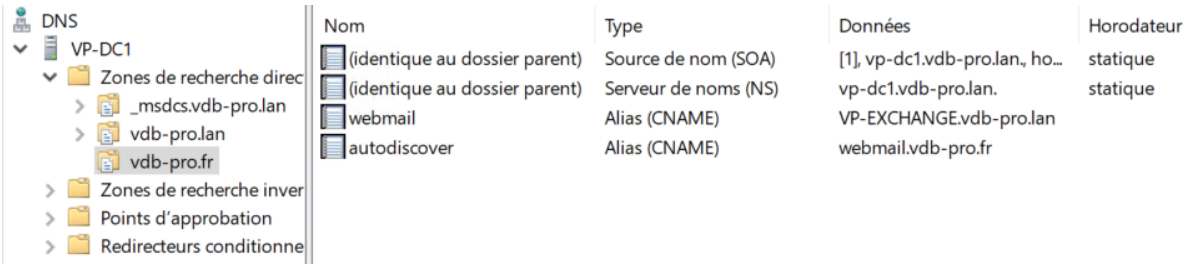
Afin d'assurer la résolution correcte du serveur Exchange, les enregistrements DNS suivants doivent être configurés sur le fournisseur du domain publique :

Type	Nom DNS	Valeur	Priorité
A	webmail.vdb-pro.fr	5.196.216.188	-
CNAME	autodiscover.vdb-pro.fr	webmail.vdb-pro.fr	-
MX	@	webmail.vdb-pro.fr	10
SFP	@	v=spf1 mx ip4:5.196.216.188 include:mx.ovh.com -all	



Preparation du DNS interne

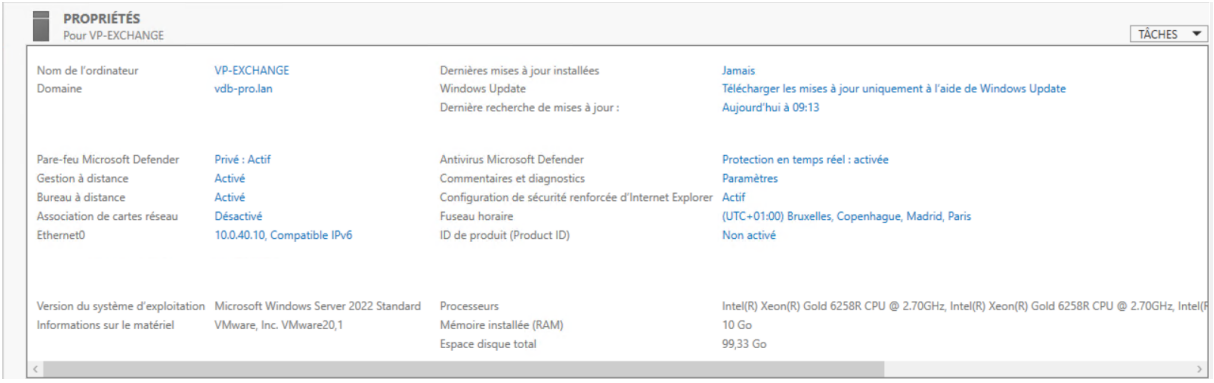
Afin que la résolution de noms en interne se fasse correctement, sans passer par Internet ni créer une boucle de résolution, j'ai dû ajouter manuellement les entrées DNS correspondantes dans le serveur DNS de l'entreprise.



Cette configuration est essentielle pour garantir que les services, tels que le Webmail ou l'autodiscover d'Exchange, soient accessibles localement sans dépendre de la résolution externe. Cela permet non seulement de réduire la latence, mais aussi de mieux contrôler et sécuriser les flux réseau internes, tout en évitant des requêtes DNS inutiles vers l'extérieur.

Pour vérifier ces enregistrements, les commandes PowerShell suivantes peuvent être utilisées
Resolve-DnsName -Type A webmail.vdb-pro.fr | ft -AutoSize
Resolve-DnsName -Type MX vdb-pro.fr | ft -AutoSize
Le serveur Exchange doit également :

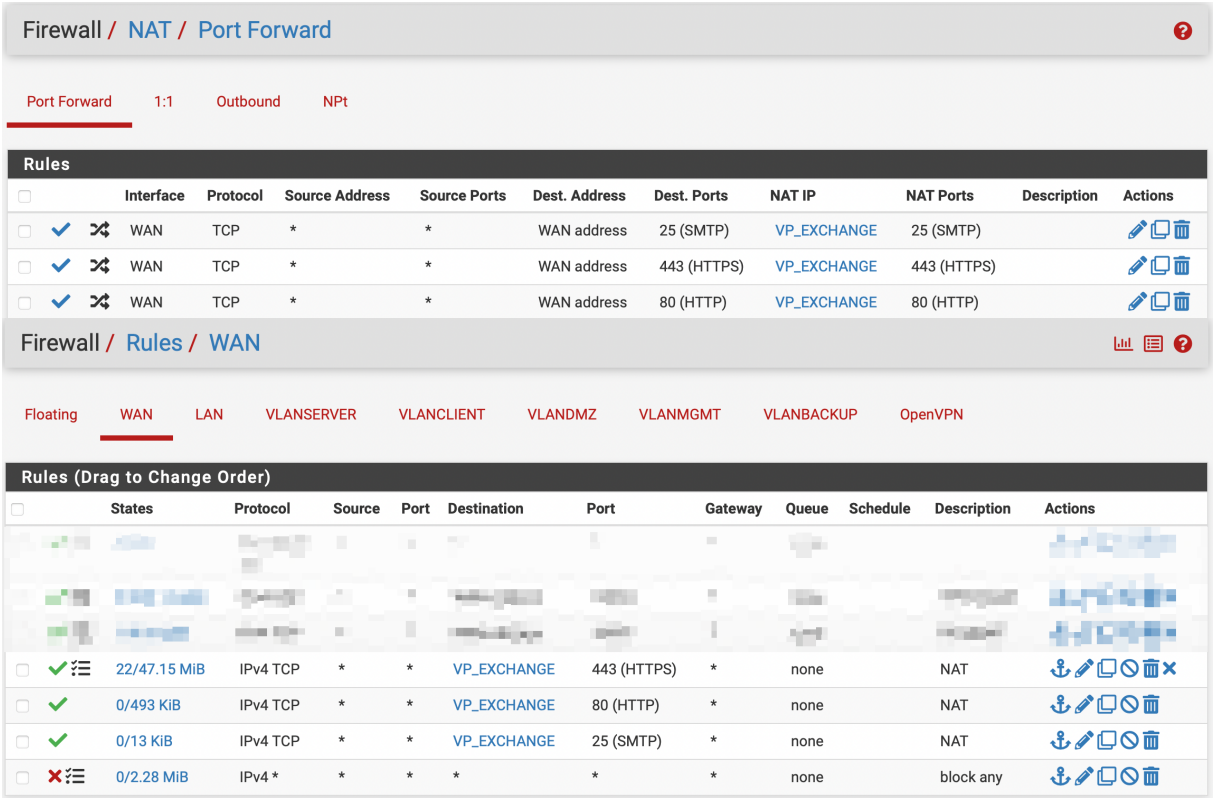
- Être **membre du domaine Active Directory** (commande : Add-Computer -DomainName vdb-pro.lan)
- Avoir une **forêt Active Directory** avec un niveau fonctionnel **Windows Server 2012 R2** minimum (Get-ADForest | fl Name,ForestMode)
- Être utilisé avec **Microsoft Outlook 2013** minimum pour garantir la compatibilité avec Exchange 2019



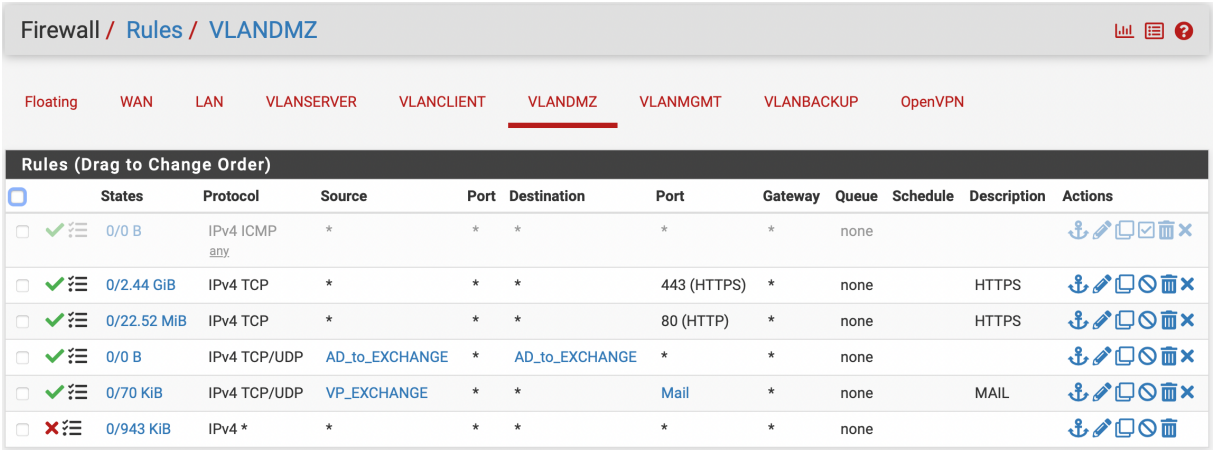
Préparation Firewall

En amont, une règle a été configurée afin de rediriger l'ensemble des flux en provenance de l'IP publique 5.196.216.188 vers mon routeur ayant l'adresse IP interne 10.10.210.253. Grâce à cette configuration, tous les flux sont désormais acheminés vers mon pare-feu PfSense.

Pour commencer, j'ai mis en place des redirections de ports via des règles NAT (Port Forwarding). Les règles sont automatiquement ajoutées dans la section WAN de PfSense, ce qui permet d'autoriser les flux entrants en fonction des services que l'on souhaite exposer.



Enfin, je vais définir les règles nécessaires pour gérer les flux sortants depuis le réseau LAN DMZ où se trouve mon serveur Exchange, afin d'assurer une communication sécurisée.



Installation des composants prérequis

Avant de procéder à l'installation d'Exchange Server, certains composants doivent être installés sur le serveur.

A. .NET Framework 4.8

Déjà installé par défaut sur Windows Server 2022. Si besoin, il est téléchargeable depuis le site Microsoft.

B. Visual C++ Redistributable Packages

- Visual Studio 2012
- Visual Studio 2013

Ces packages sont nécessaires au bon fonctionnement d'Exchange.

C. Unified Communications Managed API (UCMA) 4.0

Ce runtime est indispensable au fonctionnement de certains services Exchange. Il peut être téléchargé directement depuis Microsoft.

D. Fonctionnalités Windows à installer via PowerShell

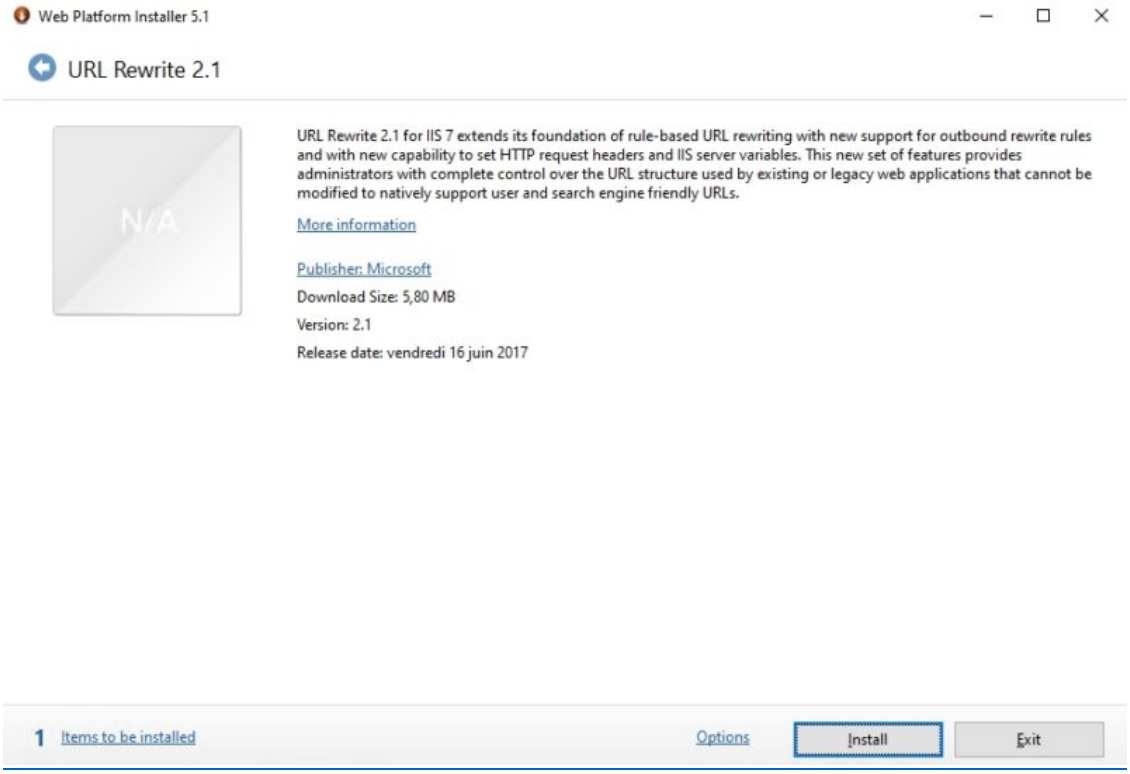
Voici la commande à exécuter pour installer l'ensemble des rôles et fonctionnalités nécessaires :

```
Install-WindowsFeature Server-Media-Foundation, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, RSAT-Clustering-Mgmt, RSAT-Clustering-PowerShell, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation, RSAT-ADDS
```

Cette commande installe notamment IIS (nécessaire pour le Webmail) et d'autres services liés à l'administration, aux protocoles de communication et à la sécurité.

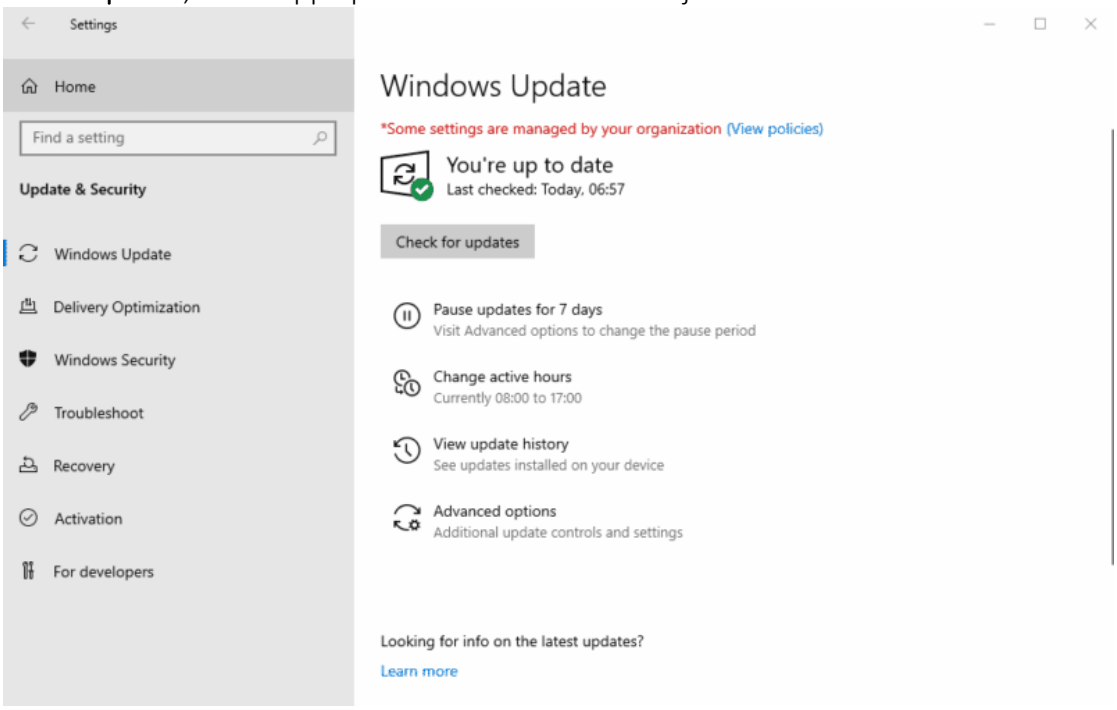
E. Installation du module URL Rewrite 2.1

Ce module est requis pour le bon fonctionnement d'Outlook Web Access (OWA) via le serveur IIS. Il est à installer manuellement.



F. Mise à jour du système

Avant de lancer l'installation d'Exchange Server, il est impératif de mettre à jour le système via **Windows Update**, afin d'appliquer les dernières mises à jour cumulatives.



Une fois l'ensemble des prérequis installés et correctement configurés sur le serveur, celui-ci est prêt à accueillir le service de messagerie Microsoft Exchange.

Dans ce cadre, j'ai réalisé un résumé structuré des étapes clés de l'installation d'Exchange Server 2019, en mettant en avant les points essentiels à retenir pour assurer une mise en œuvre réussie.

Installation de Microsoft Exchange Server 2019

Préparation avant installation

Avant de débuter l'installation d'Exchange Server 2019, il est impératif de :

- Se connecter au serveur avec un **compte membre du groupe "Administrateurs du domaine"**
- **Redémarrer le serveur** pour s'assurer qu'aucune mise à jour en attente n'interfère avec l'installation

Téléchargement et montage de l'ISO

L'installation nécessite de télécharger l'image ISO officielle d'Exchange. Dans cette maquette, l'installation est réalisée à partir de **Microsoft Exchange Server 2019 – Cumulative Update 15**.

- Lien officiel de téléchargement : Microsoft Exchange Server 2019 CU15
- Taille du fichier ISO : environ **5,8 Go**

Une fois le fichier téléchargé :

1. **Monter l'image ISO** (clic droit > Monter)
2. Exécuter le fichier setup.exe **en tant qu'administrateur**

Démarrage de l'assistant d'installation

Étapes initiales :

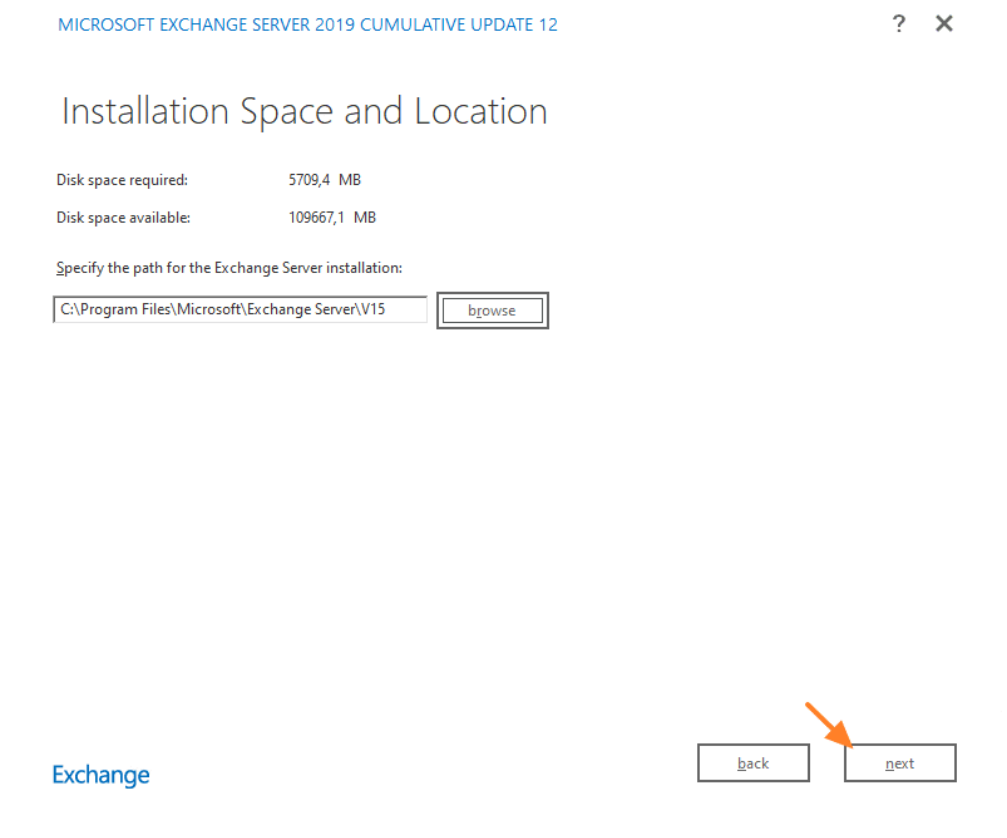
- Sélectionner l'option **"Connect to the Internet and check for updates"** afin de vérifier la présence de mises à jour plus récentes
- Attendre la fin de la phase **"Copying files"**
- Poursuivre jusqu'à l'étape d'**Introduction**, puis accepter les termes du contrat de licence

Choix des rôles :

- Sélectionner le **"Mailbox role"** (boîte aux lettres), rôle principal pour les services Exchange
- L'option **"Automatically install Windows Server roles and features..."** peut être décochée car les prérequis ont déjà été installés en amont via PowerShel

Répertoire d'installation :

L'installation par défaut se fait sur le disque [C:\] et nécessite environ **5,7 Go d'espace disponible**



Configuration de l'organisation

- **Nom de l'organisation Exchange** : à personnaliser (ex. : nom de l'entreprise ou de la maquette)

- **Option "Apply Active Directory split permissions security model"** : laisser **désactivée** si le même administrateur gère Active Directory et Exchange

Une fois ces points validés :

- Cliquer sur **"Install"** pour démarrer l'installation
- **Durée approximative** : 30 minutes à 1 heure, en fonction des ressources de la machine

Fin de l'installation

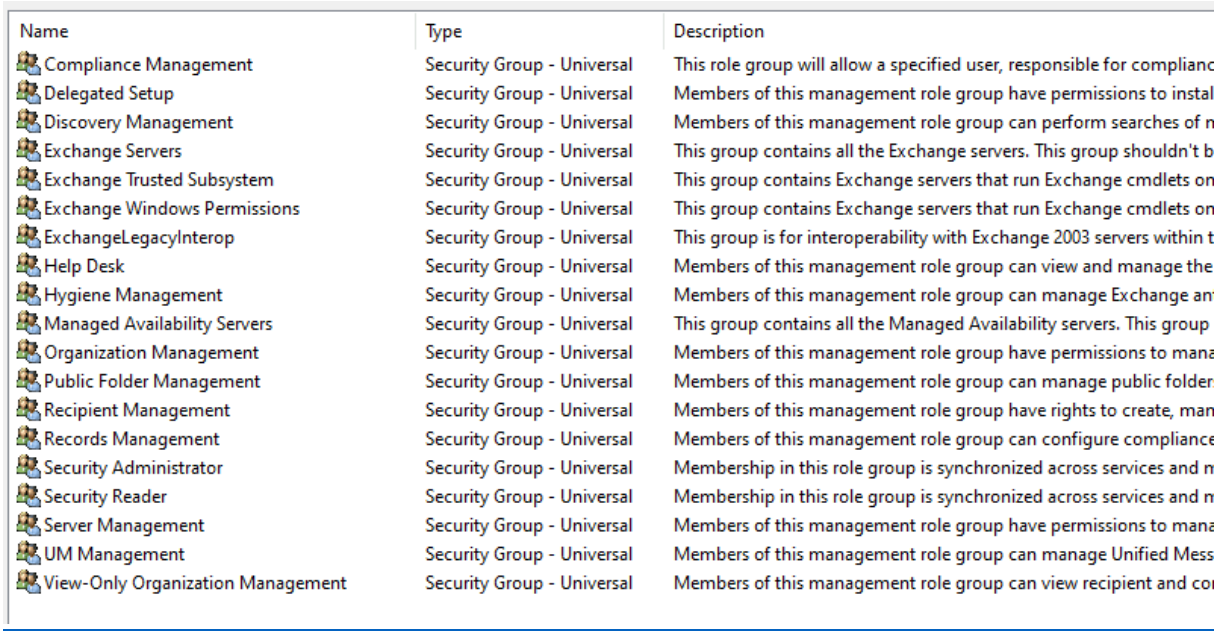
Une fois l'installation terminée :

- **Redémarrer le serveur** pour finaliser le processus

Conséquences de l'installation

À l'issue de l'installation, une nouvelle **Unité d'Organisation (OU)** est automatiquement créée dans Active Directory :

- **Microsoft Exchange Security Groups**
- Elle contient l'ensemble des **groupes d'administration** nécessaires à la gestion du serveur Exchange (droits, délégations, sécurité, etc.)



Name	Type	Description
Compliance Management	Security Group - Universal	This role group will allow a specified user, responsible for complianc
Delegated Setup	Security Group - Universal	Members of this management role group have permissions to instal
Discovery Management	Security Group - Universal	Members of this management role group can perform searches of n
Exchange Servers	Security Group - Universal	This group contains all the Exchange servers. This group shouldn't b
Exchange Trusted Subsystem	Security Group - Universal	This group contains Exchange servers that run Exchange cmdlets on
Exchange Windows Permissions	Security Group - Universal	This group contains Exchange servers that run Exchange cmdlets on
ExchangeLegacyInterop	Security Group - Universal	This group is for interoperability with Exchange 2003 servers within t
Help Desk	Security Group - Universal	Members of this management role group can view and manage the
Hygiene Management	Security Group - Universal	Members of this management role group can manage Exchange an
Managed Availability Servers	Security Group - Universal	This group contains all the Managed Availability servers. This group
Organization Management	Security Group - Universal	Members of this management role group have permissions to mana
Public Folder Management	Security Group - Universal	Members of this management role group can manage public folder
Recipient Management	Security Group - Universal	Members of this management role group have rights to create, man
Records Management	Security Group - Universal	Members of this management role group can configure compliance
Security Administrator	Security Group - Universal	Membership in this role group is synchronized across services and n
Security Reader	Security Group - Universal	Membership in this role group is synchronized across services and n
Server Management	Security Group - Universal	Members of this management role group have permissions to mana
UM Management	Security Group - Universal	Members of this management role group can manage Unified Mess
View-Only Organization Management	Security Group - Universal	Members of this management role group can view recipient and co

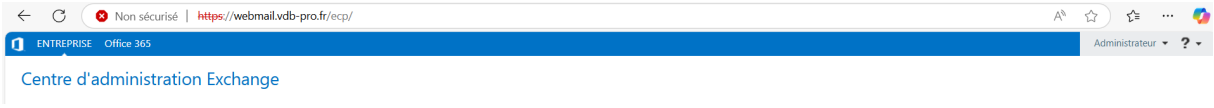
Première utilisation d'Exchange

Centre d'administration Exchange et Exchange Management Shell

L'administration d'Exchange s'effectue au travers d'un portail d'administration en mode Web, ainsi que de commandes PowerShell. Le portail d'administration appelé "Centre d'administration Exchange" est accessible à cette adresse :

# En local sur le serveur	# À partir d'une machine du réseau local	# À partir de l'extérieur
https://localhost/ecp	https://vp-exchange/ecp	https://webmail.vdb-pro.fr/ecp

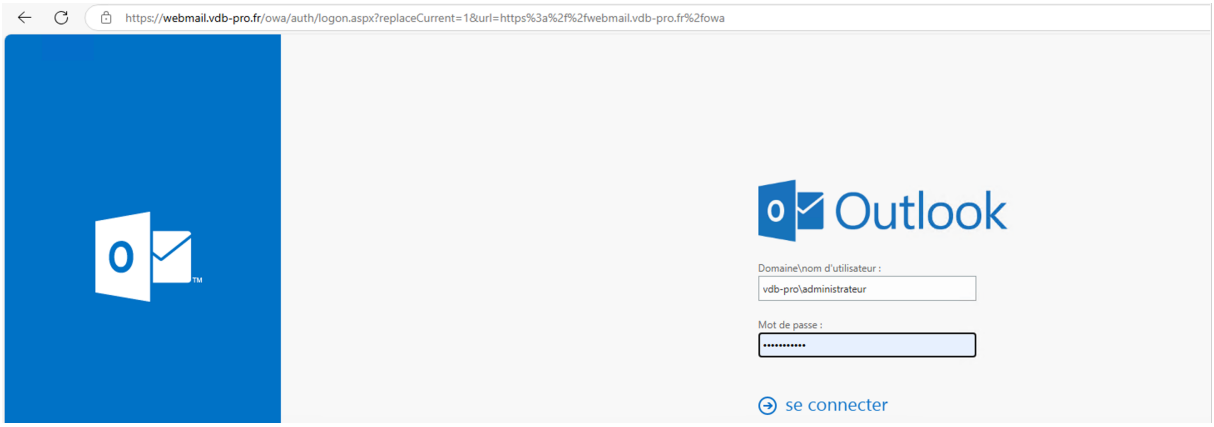
Sur cette interface, vous pouvez vous authentifier avec un compte administrateur du domaine.



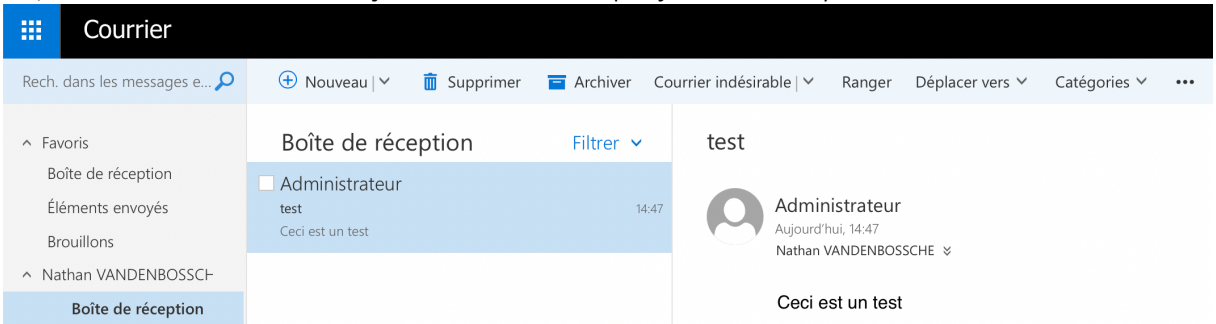
Webmail d'Exchange Server 2019

En ce qui concerne les utilisateurs, ils ont le choix entre un client de messagerie type Outlook, ou un accès via le webmail. Ce dernier étant accessible à l'adresse suivante : https://webmail.vdb-pro.fr/owa

Le sigle "OWA" fait référence à Outlook Web Access. L'utilisateur doit se connecter avec ses identifiants Active Directory (*au préalable, j'ai créé les BAL*).



Ah, mon utilisateur à bien reçu l'e-mail de test que je lui ai envoyé !



Déplacer la base de données Exchange

Suite à l'installation de Microsoft Exchange, je constate que la base de données (au format EDB) et les journaux sont initialement stockés dans l'emplacement par défaut, à côté des binaires d'Exchange : C:\Program Files\Microsoft\Exchange Server\V15\Mailbox\Mailbox Database 0780012571\Mailbox Database 0780012571.edb

Il est toutefois recommandé de déplacer cette base de données sur un autre volume, tout comme les journaux, afin d'optimiser les performances et la gestion des données. Dans un environnement de production, il est préférable d'utiliser au moins deux volumes distincts : un pour la base de données et un autre pour les journaux. Dans mon cas, je vais profiter du fait que le serveur vient juste d'être installé, ce qui rend cette opération relativement simple et rapide à effectuer.

Mon objectif ici est de déplacer la base de données et les journaux vers un volume ReFS (Resilient File System) pour bénéficier d'une meilleure intégrité des données et de performances accrues. Le chemin que j'ai choisi pour ce déplacement est le suivant : E:\MsExchange_DB\

En même temps, je vais renommer la base de données. En effet, le nom par défaut, "Mailbox Database 0780012571.edb", n'est pas particulièrement explicite. Je préfère attribuer un nom plus pertinent, à savoir "Mailbox vdb-pro", afin de faciliter la gestion à long terme.

Pour ce faire, je vais d'abord ouvrir l'Exchange Management Shell. Ensuite, je lance la commande suivante pour renommer la base de données :

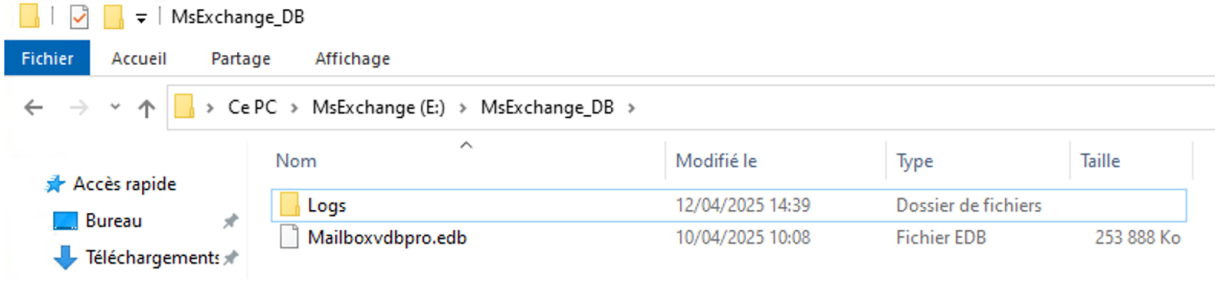
```
Get-MailboxDatabase "Mailbox Database 0780012571" | Set-MailboxDatabase -Name "Mailbox IT-Connect"
```

Ensuite, je passe à l'étape suivante : déplacer la base de données et les journaux vers leur nouvel emplacement. Pour cela, j'utilise la commande Move-DatabasePath :

```
Move-DatabasePath "Mailbox vdb-pro" -EdbFilePath "E:\MsExchange_DB\Mailboxvdbpro.edb" -LogFolderPath "E:\MsExchange_DB\Logs\"
```

L'opération est relativement rapide, mais il est important de noter que pendant cette opération, la base de données sera temporairement indisponible.

Une fois cette étape terminée, ma base de données et ses journaux seront déplacés avec succès

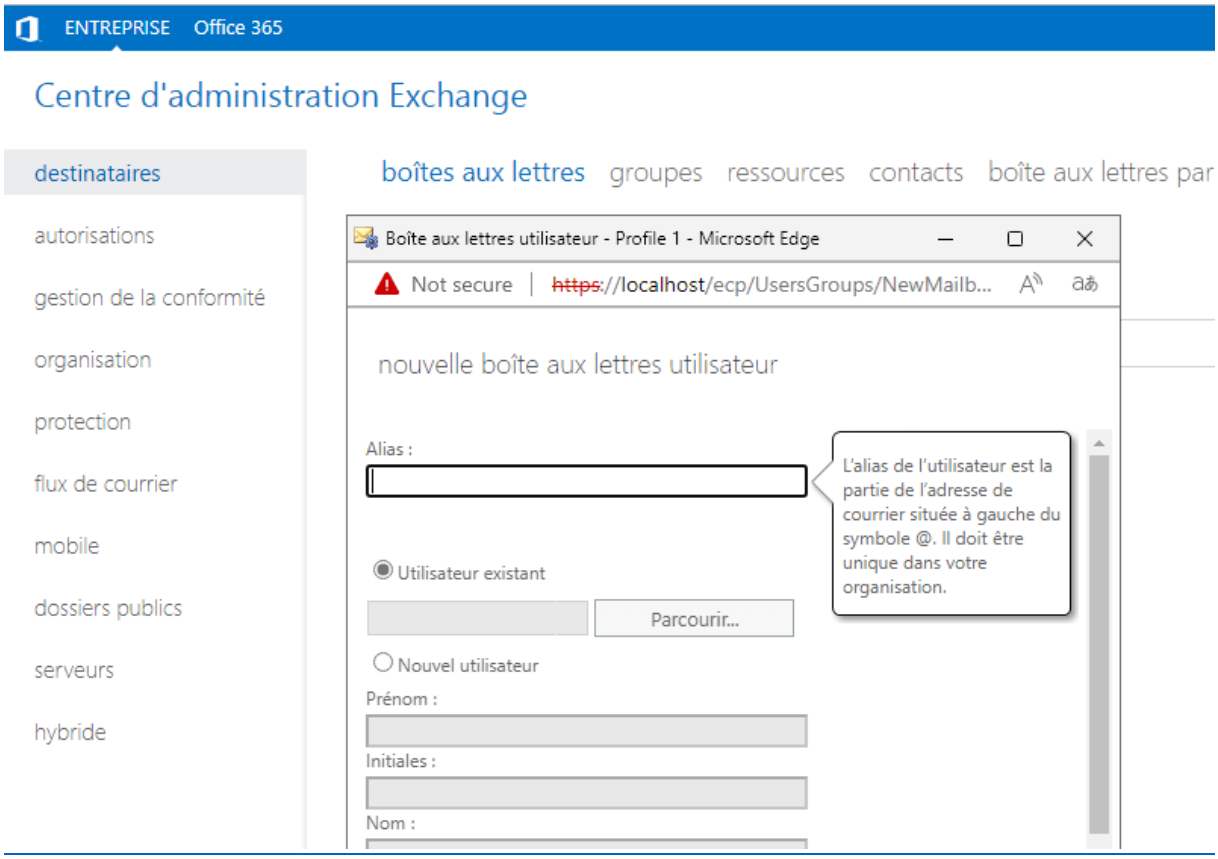


Créer une nouvelle boite aux lettres Exchange

Pour créer une boîte aux lettres (*appelée aussi "BAL"*) pour un utilisateur, Je commence par me rendre dans le menu **Destinataire** puis **Boîtes aux lettres**. Une fois sur cette page, je clique sur le bouton **"+"** pour ajouter une nouvelle boîte aux lettres.

Dans ce formulaire, j'ai le choix entre **sélectionner un utilisateur existant** dans l'annuaire Active Directory ou **créer un utilisateur** en même temps que la boîte aux lettres. Il est important de souligner que dans Exchange, les comptes utilisateurs et les boîtes aux lettres sont étroitement liés. Cela signifie que lorsque je crée une boîte aux lettres pour un utilisateur, celle-ci est directement associée à son compte dans Active Directory.

Je dois également garder à l'esprit un aspect crucial : si je **supprime une boîte aux lettres** dans Exchange, l'utilisateur associé dans Active Directory sera également **supprimé**. Cela peut avoir des conséquences importantes, car cela supprimera non seulement la boîte aux lettres, mais également l'accès de l'utilisateur à son compte AD. Il est donc primordial d'être vigilant lors de la gestion de ces boîtes aux lettres.

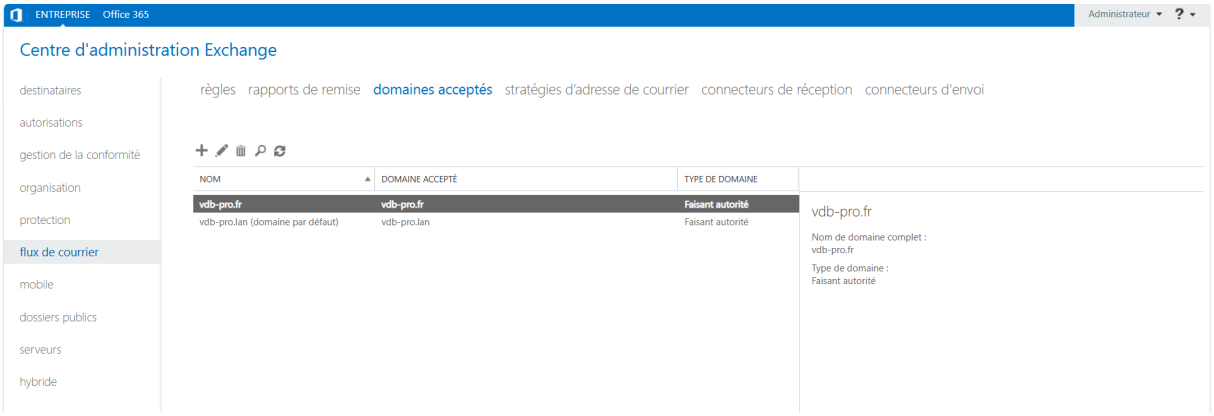


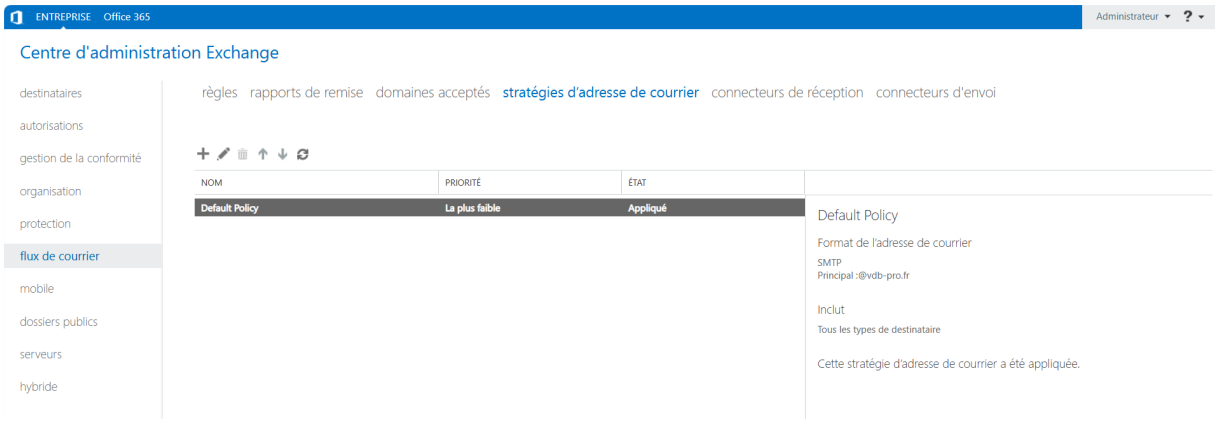
Ajout d’un domain et strategie d’adresse de courrier

Actuellement mon serveur Exchange est installé sur un domaine Active Directory avec un domaine non routable (vdb-pro.lan) je rencontre une situation où le domaine de l'adresse e-mail interne ne correspondra pas à celui utilisé pour la communication avec l'extérieur.

En effet, les domaines non routables (tels que ".local" ou ".lan") ne sont pas accessibles via Internet, ce qui pose un problème pour l'envoi ou la réception d'emails en dehors du réseau interne. Par conséquent, je dois configurer un domaine différent dans Exchange, qui sera routable et capable de communiquer avec l'extérieur.

Pour cela, je vais d'abord déclarer ce nouveau domaine dans Exchange. Ensuite, je l’associe à une politique d'adresses e-mails pour que les utilisateurs de mon serveur Exchange puissent recevoir et envoyer des emails en utilisant ce domaine public.





Cette opération garantit que les adresses e-mails de mes utilisateurs auront un domaine valide et accessible de manière routable, ce qui est essentiel pour toute communication en dehors du réseau local. Cette étape est nécessaire pour assurer une connectivité correcte de mes utilisateurs Exchange avec l'extérieur, tout en préservant l'intégrité et l'accessibilité des boîtes aux lettres internes.

Une fois que c'est fait, je peux créer des boites aux lettres : par défaut, elles bénéficieront d'une adresse e-mail principale en "@vdb-pro.fr".

Ajout d’un certificat SSL pour Exchange

Une étape cruciale dans le processus de création d’un serveur de messagerie Exchange est l’ajout d’un certificat SSL/TLS.

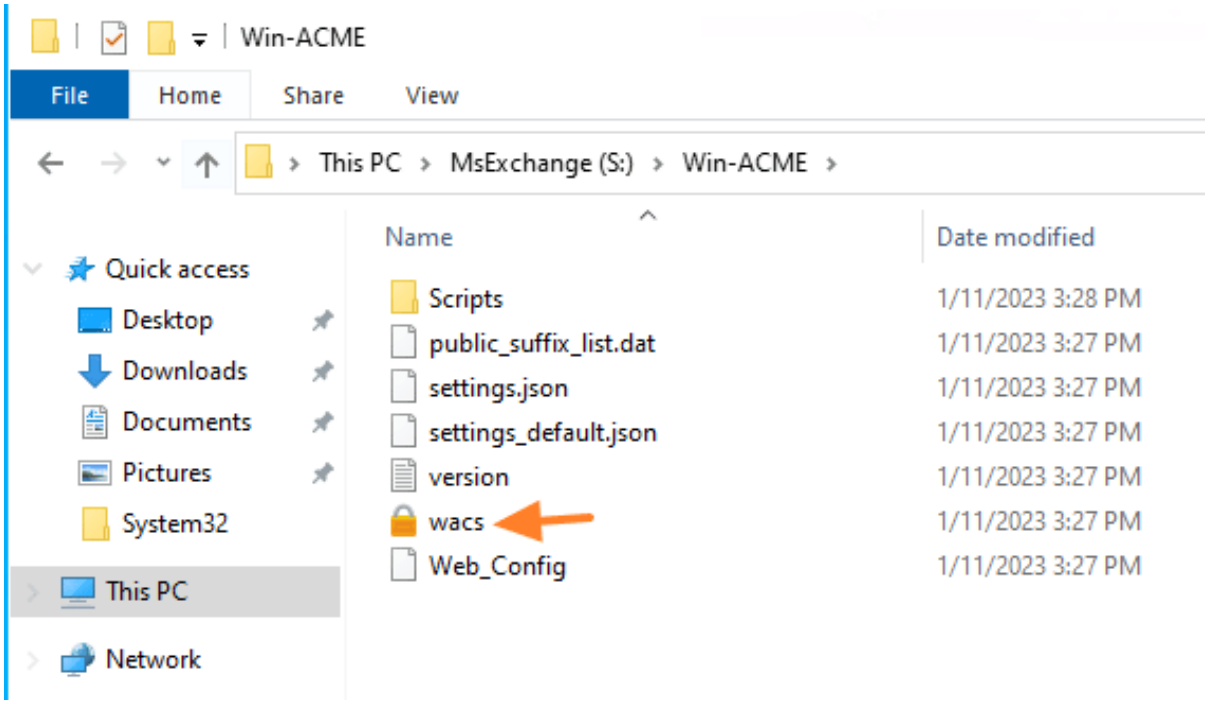
Ce certificat est essentiel pour garantir que mon serveur Exchange soit accessible en toute sécurité depuis l'extérieur, notamment pour les utilisateurs qui se connectent à distance via des clients de messagerie comme Outlook ou des applications mobiles. Le certificat assure que les communications entre les utilisateurs et le serveur Exchange sont cryptées, protégeant ainsi les données sensibles contre les interceptions.

Pour ce faire, je vais obtenir un certificat auprès d'une autorité de certification (CA) reconnue. Le certificat permet également d'éviter les avertissements de sécurité lorsque les utilisateurs se connectent à leur boîte aux lettres, renforçant ainsi la confiance et la sécurité de l'infrastructure de messagerie.

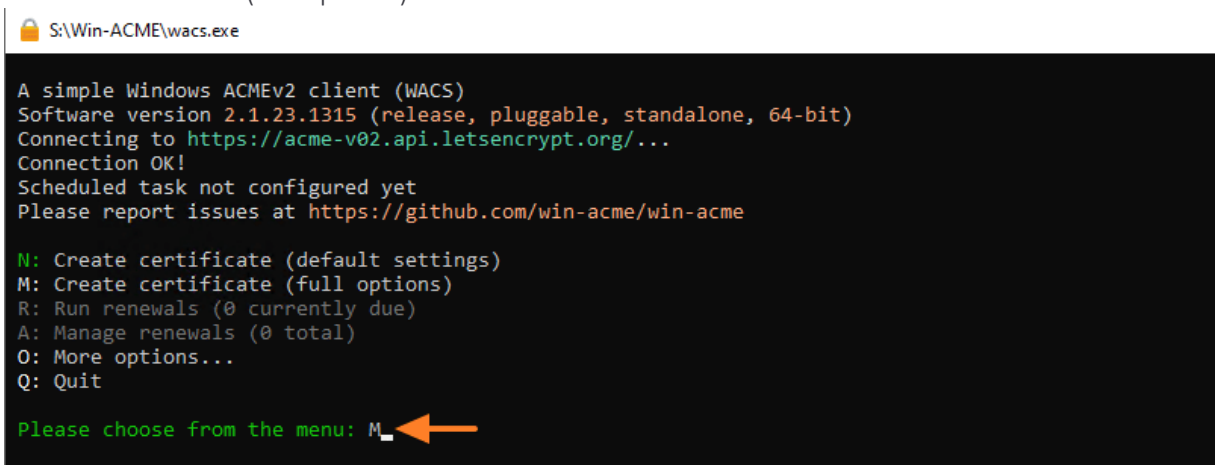
L'ajout de ce certificat est indispensable pour garantir une connexion sécurisée, conforme aux bonnes pratiques de sécurité et pour protéger l'intégrité des communications via Exchange.

Demander un certificat SSL avec Win-ACME

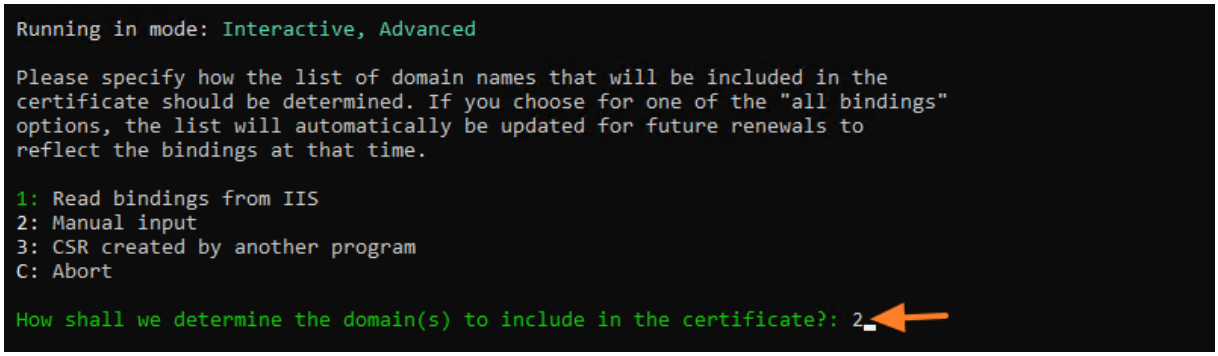
Je commence par télécharger le client Win-ACME, par extraire le contenu et exécuter en tant qu'administrateur "wacs.exe".



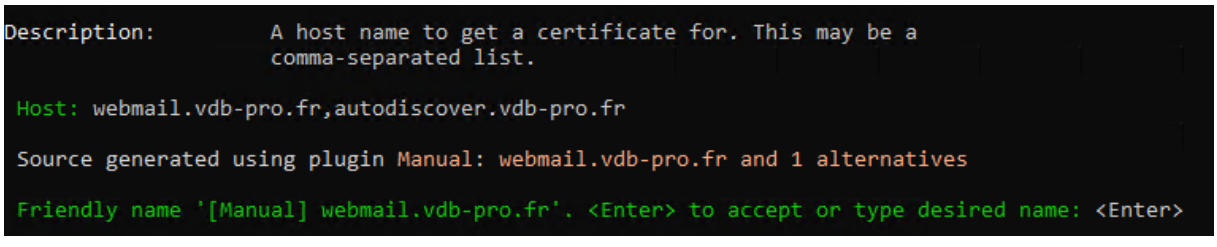
Bien qu'il soit possible d'effectuer une demande de certificat en ligne de commandes en précisant tous les arguments, nous allons procéder étape par étape, via le mode interactif. De ce fait, j'exécute "wacs.exe" en tant qu'administrateur et choisi l'option "M" correspondante à "Create certificate (full options)".



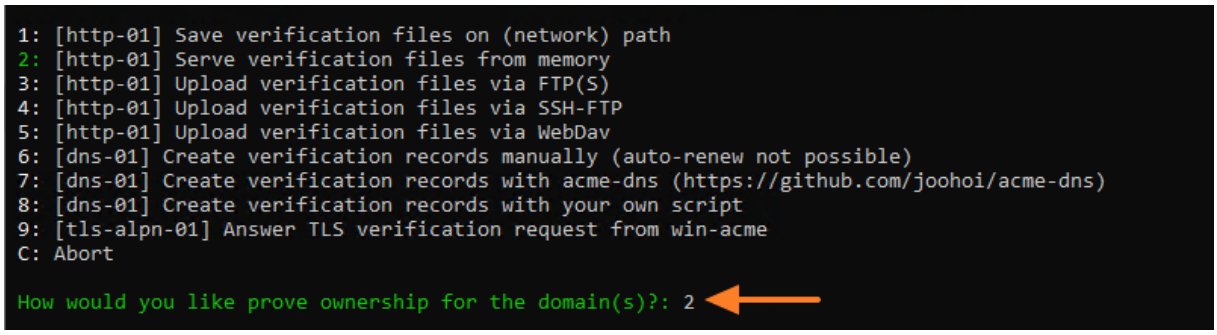
Je dois préciser les noms DNS à couvrir avec le certificat SSL. Pour cela, je sélectionne l'option "2" pour effectuer une saisie manuelle.



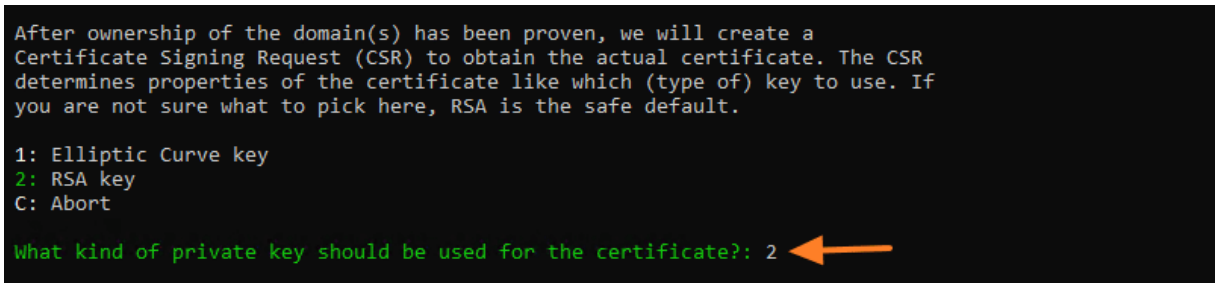
Je vais ensuite indiquer toutes les adresses Web utilisées par mon serveur Exchange. Dans mon cas, il y en a deux : **webmail.vdb-pro.fr** et **autodiscover.vdb-pro.fr**. Je peux aussi indiquer un nom convivial pour le certificat, mais cela reste optionnel. Si je ne souhaite pas le faire, je peux simplement appuyer sur **Entrée** pour passer cette étape.



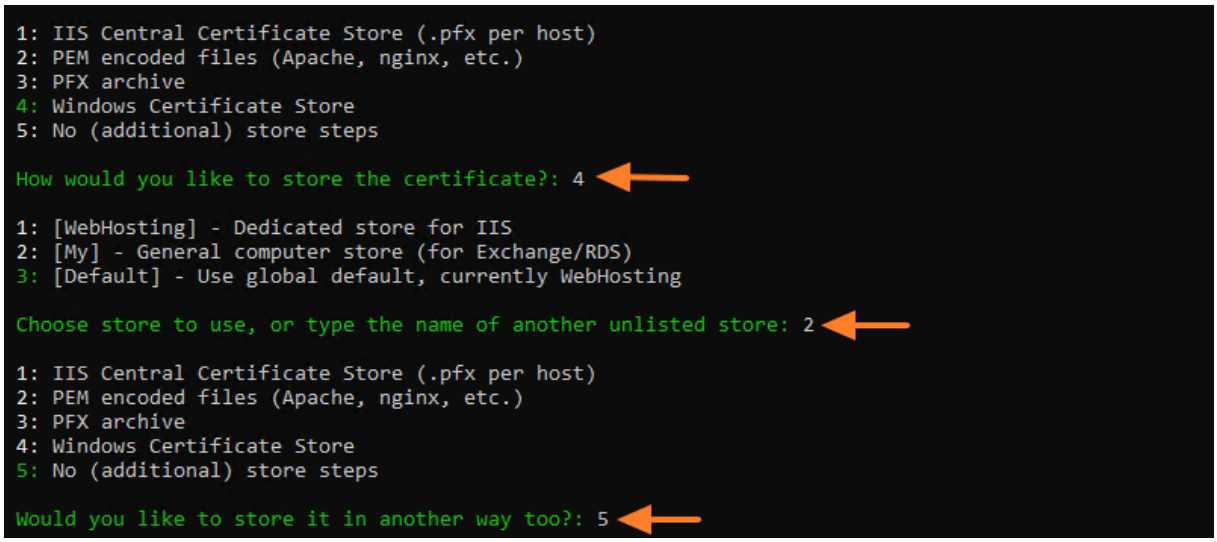
Concernant la méthode de validation, je vais commencer par tester la méthode par défaut en sélectionnant l'option "2".



Ensuite, je dois choisir le type de clé privée à utiliser. Dans ce cas, je sélectionne l'option **"2" pour RSA Key**, qui est la méthode la plus courante et recommandée.



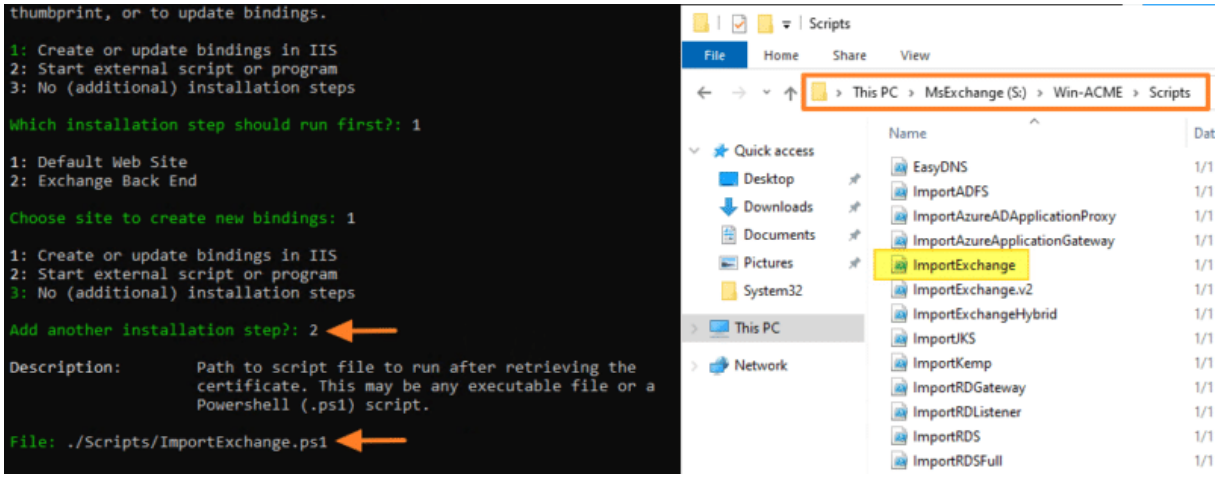
L'assistant me demande où je souhaite stocker le certificat. Pour cela, je choisis **"4"** afin qu'il soit stocké dans le magasin des certificats Windows. Lors de la question suivante, je dois indiquer le magasin où il sera stocké, et je sélectionne **"2"**pour le **magasin personnel**, ce qui est recommandé pour Exchange, selon les indications de l'assistant. Une fois cela fait, je sélectionne **"5"** pour passer à l'étape suivante, car il n'y a pas d'autres emplacements à spécifier.



Win-ACME me propose ensuite de mettre à jour les liaisons dans IIS pour intégrer le certificat SSL. Je confirme cette action en sélectionnant **"1"** une première fois, puis une seconde fois pour appliquer le certificat au niveau du site **"Default Web Site"** dans IIS.

```
1: Create or update bindings in IIS
2: Start external script or program
3: No (additional) installation steps

Which installation step should run first?: 1

1: Default Web Site
2: Exchange Back End

Choose site to create new bindings: 1
```

L'assistant me demande ensuite si je souhaite ajouter une étape d'installation supplémentaire. Je réponds **"oui"** car je dois exécuter un script supplémentaire. Pour cela, je choisis **"2"**, ce qui me permet de spécifier le chemin du script PowerShell intégré à Win-ACME, **ImportExchange.ps1**. Le chemin à entrer est : « ./Scripts/ImportExchange.ps1 »



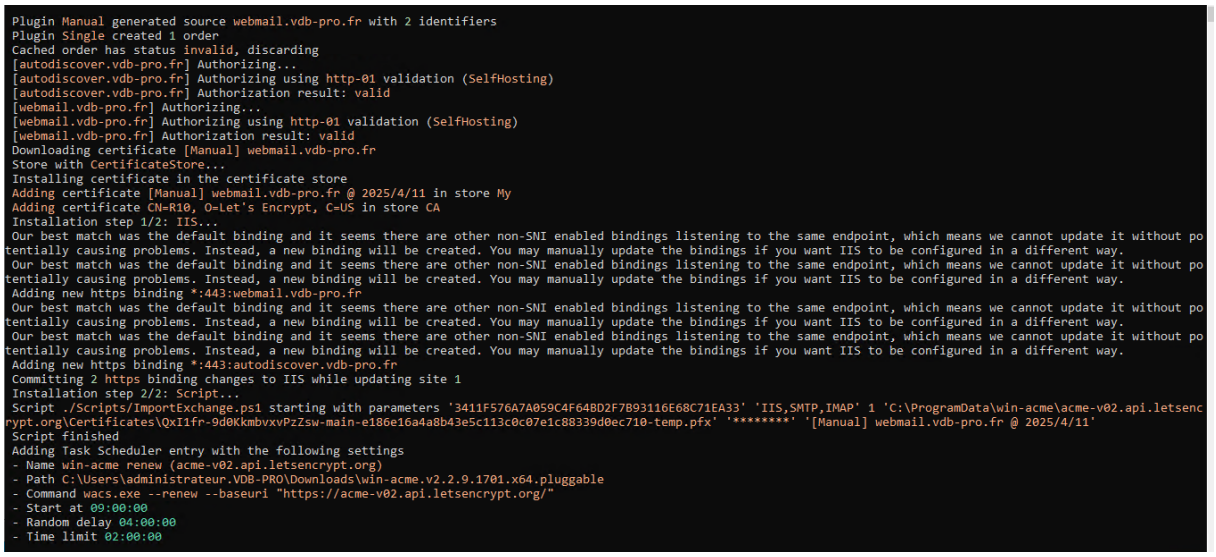
Je vais ensuite préciser les paramètres nécessaires à l'exécution de ce script. Pour cela, je saisis les informations suivantes pour Microsoft Exchange Server :

'{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}'

```
Parameters: '{CertThumbprint}' 'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}' '{CertFriendlyName}'
```

Une fois cela fait, je sélectionne **"3"** pour indiquer qu'il n'y a pas d'autres étapes d'installation à ajouter.

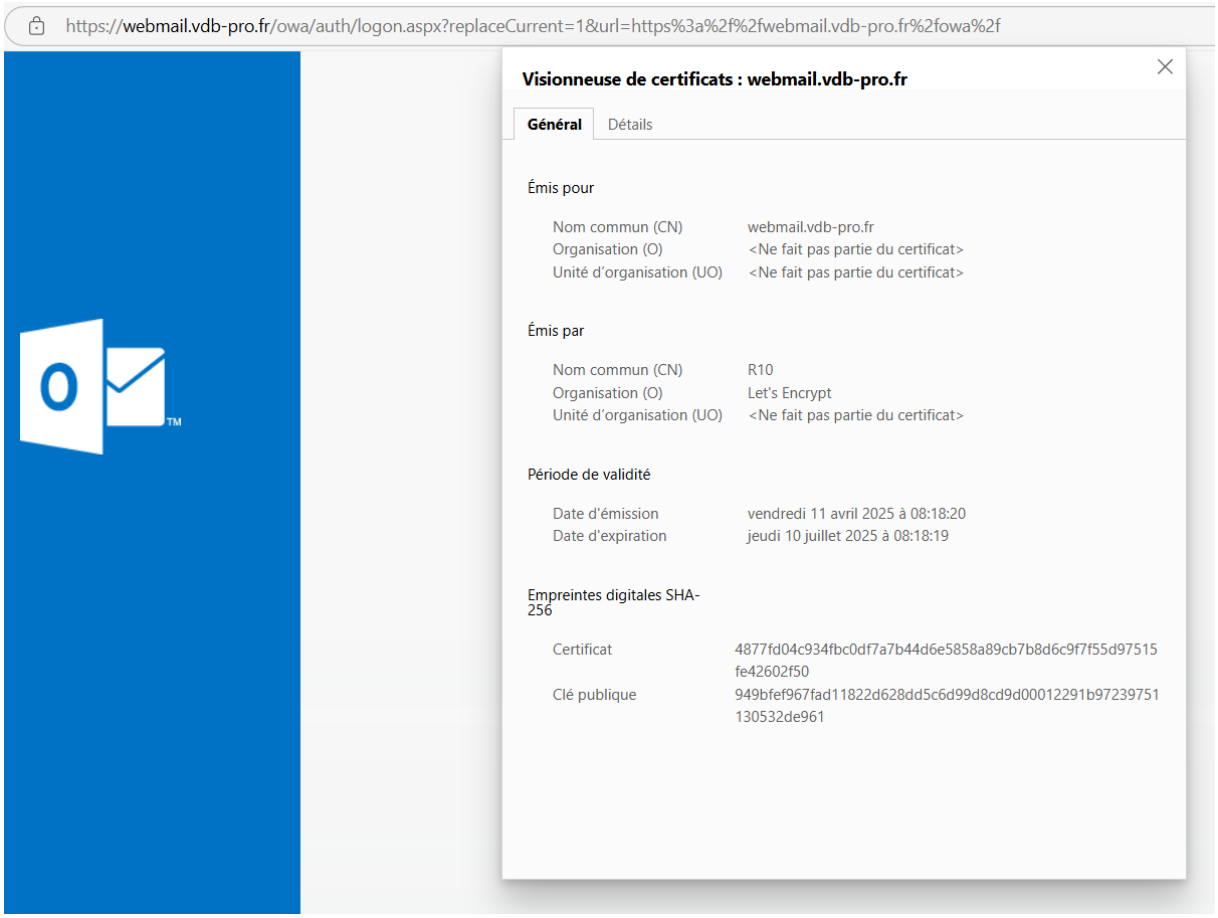
À partir de là, le client Win-ACME va émettre une requête pour obtenir le certificat SSL. Si la requête est acceptée, le certificat sera installé dans le magasin de certificats du serveur et IIS sera configuré pour utiliser ce certificat au sein des liaisons HTTPS. De plus, une tâche planifiée nommée **"win-acme renew (acme-v02.api.letsencrypt.org)"** sera créée sur le serveur pour assurer le renouvellement automatique du certificat, qui sera valable pour une durée de 90 jours à chaque renouvellement.



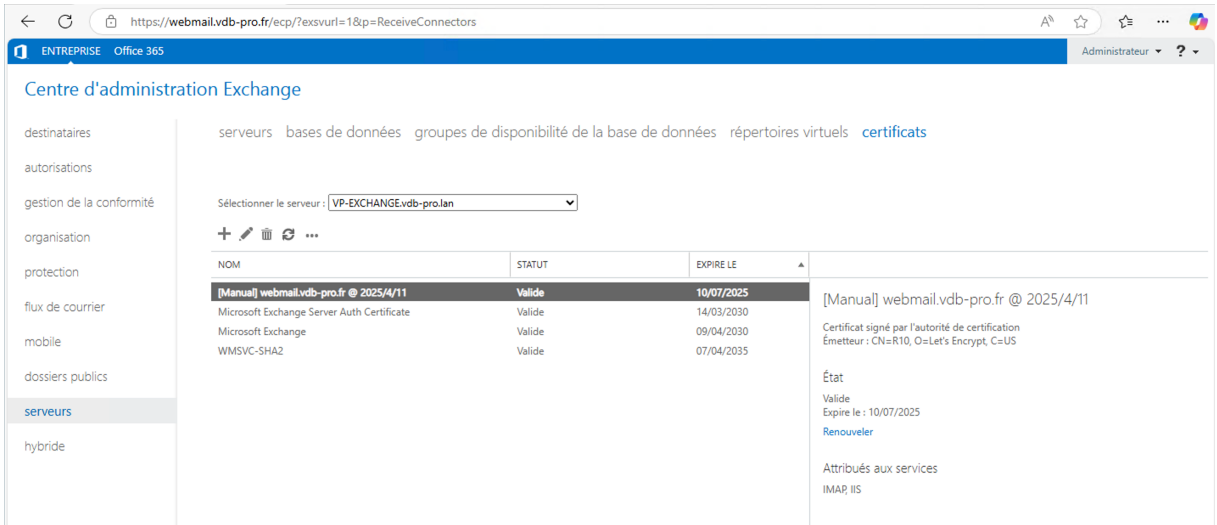
Au final, mon serveur aura récupéré et installé le certificat SSL de Let's Encrypt, qui sera ensuite intégré à Exchange et IIS. La console me fournit des informations sur la tâche planifiée de renouvellement du certificat SSL. L'assistant me demande enfin si je souhaite exécuter cette tâche avec un utilisateur spécifique, et je réponds **"no"**.

Vérification de la présence du certificat dans Exchange

À partir de ce moment, je peux me connecter à l'OWA (Webmail) d'Exchange pour vérifier que la connexion est bien sécurisée. En consultant les détails du certificat, je m'assure qu'il s'agit bien d'un certificat SSL valide de **Let's Encrypt**.



Enfin, je peux vérifier la présence du certificat SSL dans le Centre d'administration Exchange, à l'emplacement suivant : **Serveurs > Certificats**.



Protéger le centre d'administration

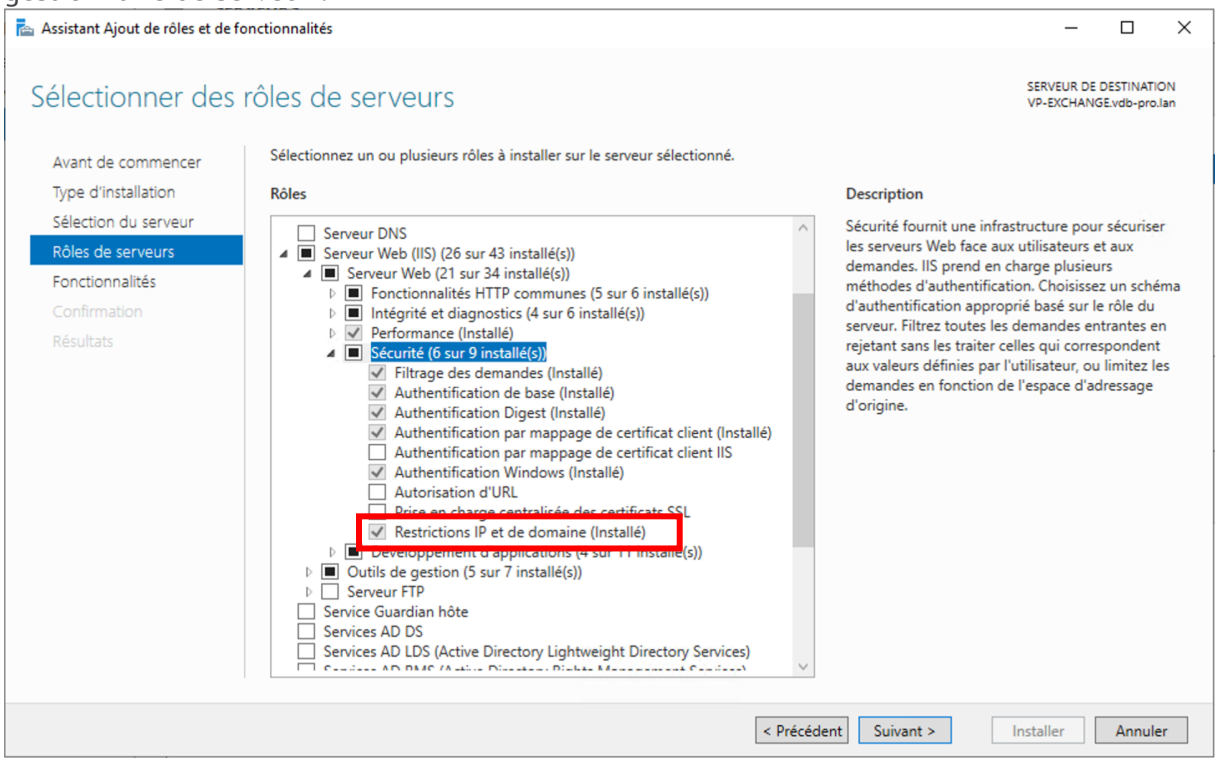
Je vous rappelle que par défaut, le Centre d'administration Exchange est accessible depuis le serveur Exchange en lui-même, depuis une machine du réseau local, mais aussi à partir d'Internet (si vous avez autorisé le flux HTTPS pour un accès au Webmail). Pour des raisons évidentes de sécurité, il est préférable de limiter l'accès à la console d'administration à partir de certaines adresses IP, ou au pire, à partir du réseau local. Il vaut mieux éviter que cette console soit accessible depuis l'extérieur.

Puisque le protocole HTTPS est utilisé aussi pour accéder au Webmail, nous ne pouvons pas jouer directement avec le pare-feu de Windows, car on couperait aussi l'accès au Webmail. La restriction doit être appliquée sur une couche supérieure, je vais configurer le serveur Web IIS grâce au module de restriction par adresses IP

Installer la fonction "Restrictions par adresse IP et domaine"

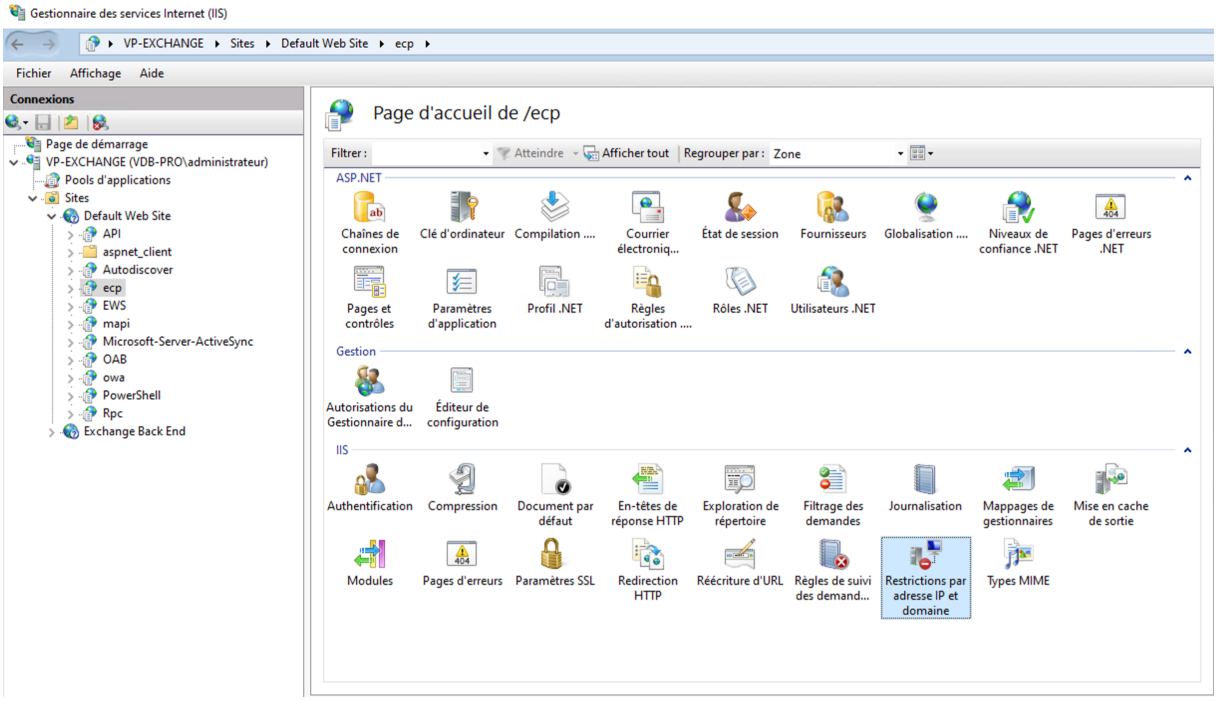
Sur votre serveur Exchange, dégainez la console PowerShell en tant qu'administrateur et exécutez la commande suivante : « Install-WindowsFeature -Name Web-IP-Security »

Cette commande revient à installer la fonctionnalité suivante dans IIS, à partir du gestionnaire de serveur :

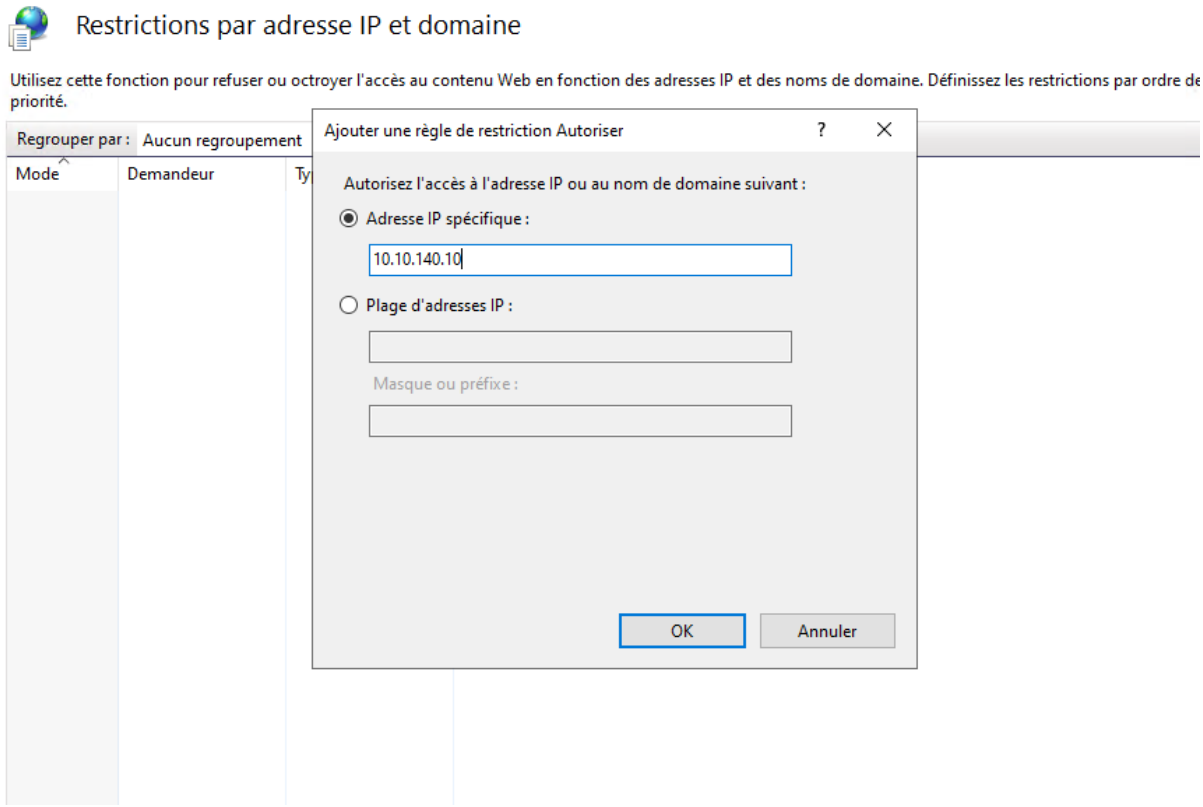


Restreindre l'accès à l'ECP d'Exchange

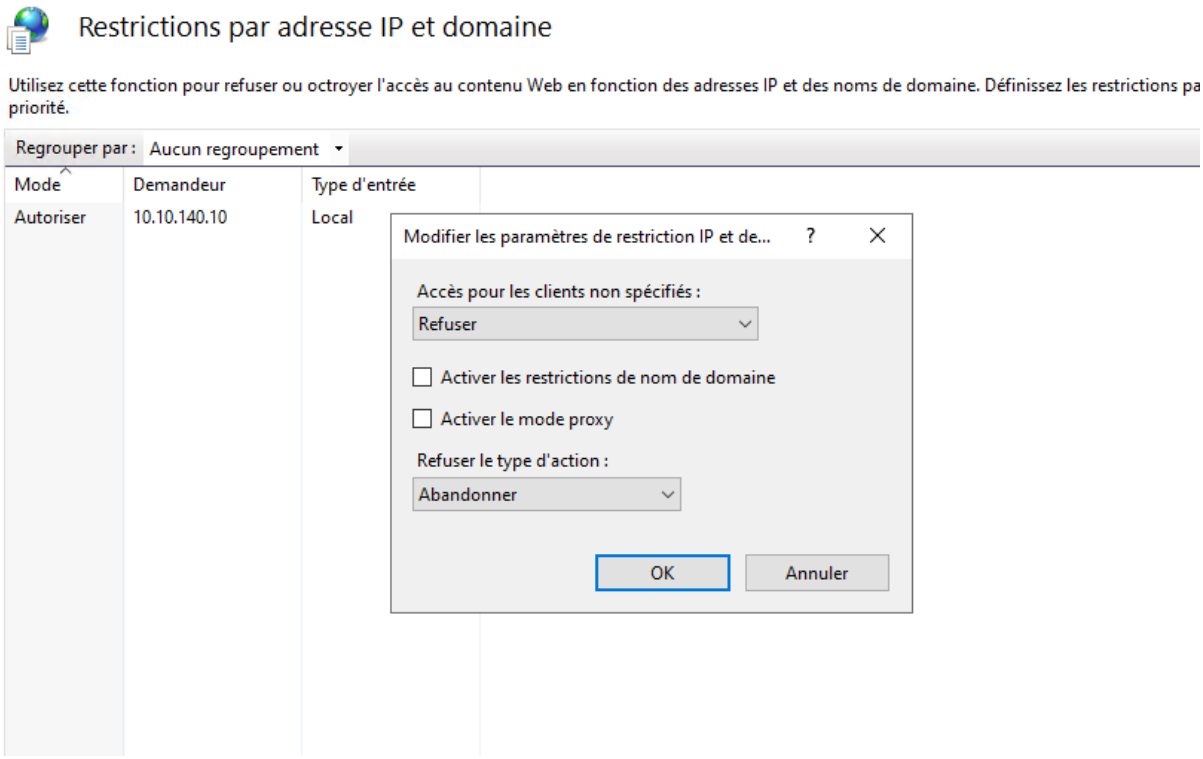
Ouvrez la console de management d'**IIS** et déroulez la section "**Sites**". Ici, cliquez sur "Default Web Site" (1), puis sur "ecp" (2) afin d'accéder à Restrictions par adresse IP et domaine.



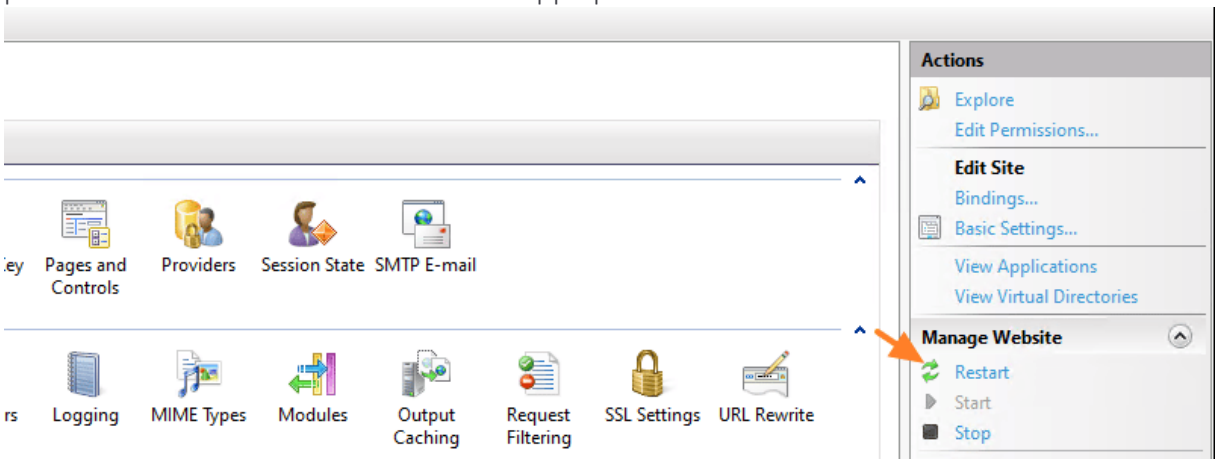
Dans la section qui s'ouvre, cliquez sur "Ajouter une entrée d'autorisation" pour ajouter une nouvelle autorisation. L'objectif ici est d'indiquer quel est la machine ou le sous-réseau autorisé à accéder au Centre d'administration Exchange. Il est possible d'ajouter plusieurs règles d'autorisation. Dans cet exemple, j'autorise les connexions à ECP depuis la machine VP-EXCHANGE "*10.10.140.10*". Quand c'est fait, validez avec "OK".



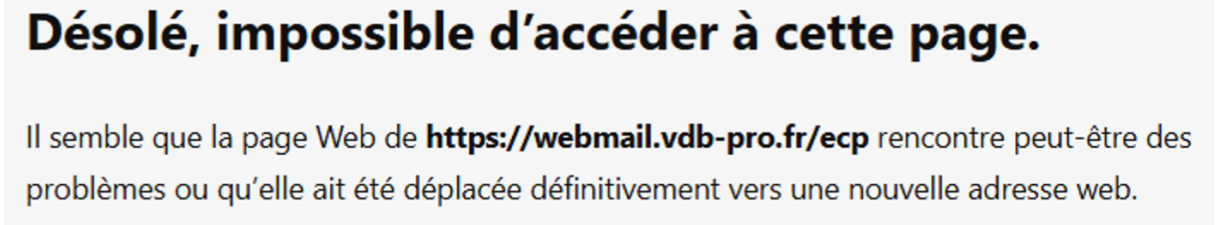
Une fois que votre règle est définie (c'est modifiable par la suite), cliquez sur "Modifier les paramètres de fonction" afin de modifier l'action à appliquer pour les clients non autorisés. Par défaut, c'est autorisé, donc nous devons inverser ce comportement. Choisissez "Refuser" et pour l'action à réaliser, choisissez "Abandonner" pour couper la connexion avec le client qui tente de se connecter. Validez avec "OK".



Pour finir, cliquez sur "Default Web Site" à gauche puis à droite sur le bouton "Redemarrer" pour redémarrer le site IIS dans le but d'appliquer la modification.



À partir d'un client autorisé, l'accès au Centre d'administration Exchange doit fonctionner normalement. Tandis qu'à partir d'un client non autorisé, une erreur doit s'afficher, comme ceci



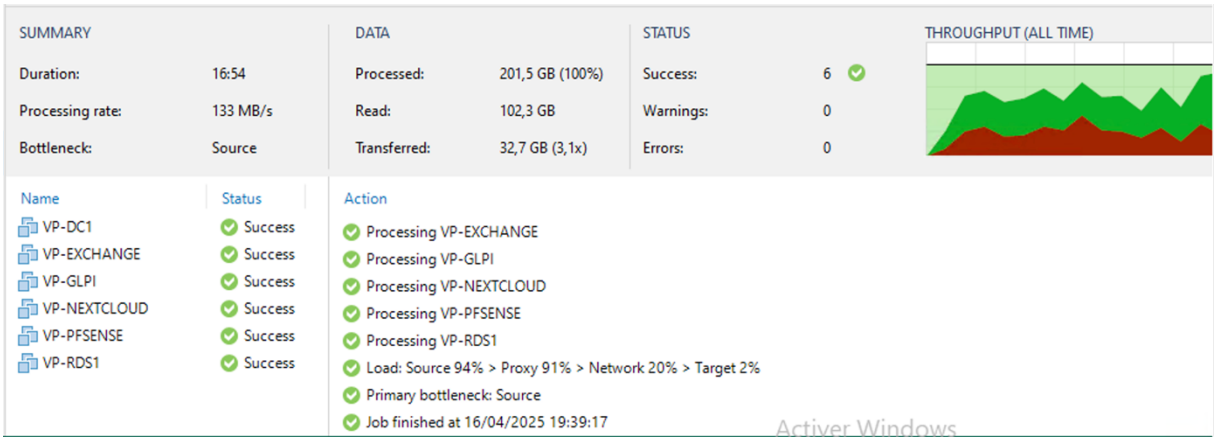
Gérer le patrimoine informatique

L'infrastructure informatique de l'entreprise **vdb-pro** repose sur un recensement rigoureux et exhaustif de l'ensemble du patrimoine informatique, réalisé à l'aide d'un outil de gestion des actifs. L'**Active Directory** constitue la base centrale de cette gestion, permettant l'organisation des utilisateurs, des groupes et des machines, tandis que d'autres services essentiels, tels qu'un serveur de **sauvegarde**, sont également en place. Le serveur **Exchange 2019**, nouvellement déployé, a été intégré à ce patrimoine et enregistré comme ressource critique de l'infrastructure.

Les droits d'accès ont été configurés en fonction des **habilitations spécifiques de chaque utilisateur**. Par exemple, l'accès au **Centre d'administration Exchange (ECP)** est strictement réservé aux administrateurs, garantissant ainsi une gestion sécurisée des paramètres sensibles, tandis que les utilisateurs classiques ne disposent que des droits nécessaires à l'usage quotidien de la messagerie.

Afin d'assurer la **continuité de service** et d'être alerté en cas de dysfonctionnement, j'ai mis en place un **système de surveillance** qui envoie des notifications par e-mail en cas de panne du serveur Exchange. Cela permet une réactivité rapide en cas d'incident.

Concernant la **sauvegarde**, un **job de sauvegarde dédié** a été mis en place pour la **machine virtuelle** hébergeant le serveur Exchange, en conformité avec le **plan de sauvegarde** de l'entreprise. Des **tests de restauration** ont été effectués avec succès afin de valider l'intégrité des sauvegardes et la capacité de reprise en cas de sinistre.



Enfin, un **système de supervision** permet de détecter et de signaler les **écarts par rapport aux règles d'utilisation des ressources numériques**, assurant un respect constant des politiques de sécurité et un usage conforme aux bonnes pratiques internes.

Développer la présence en ligne de l'organisation

L'image de l'entreprise **vdb-pro** est conforme aux attentes et soigneusement valorisée à travers une infrastructure numérique fiable, professionnelle et sécurisée. Le déploiement du serveur de messagerie Exchange participe pleinement à cette image en offrant un service de communication moderne, stable et conforme aux standards professionnels.

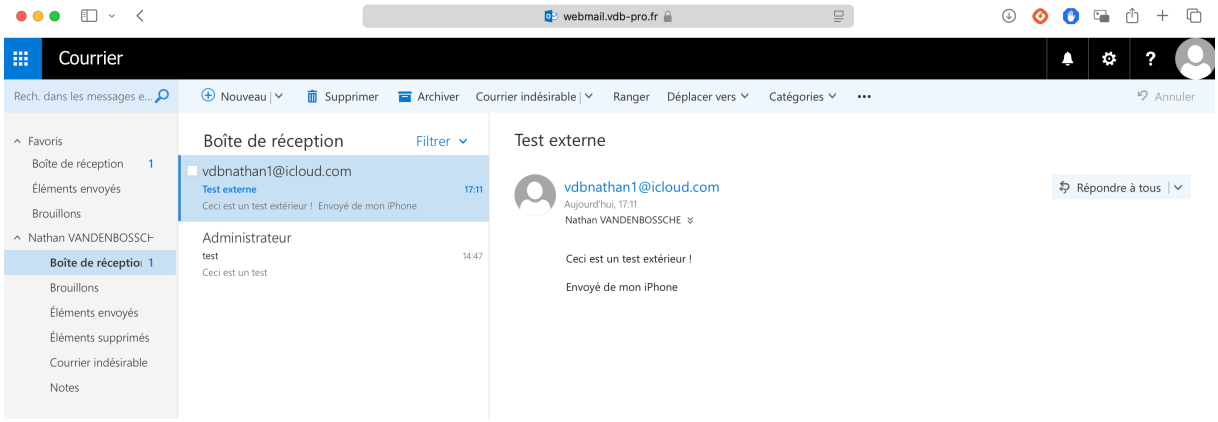
Les **enjeux économiques liés à l'image** sont clairement identifiés, notamment en ce qui concerne la confiance des partenaires et clients dans la qualité des services proposés.

La **visibilité des services en ligne**, notamment grâce au **Webmail sécurisé (OWA)**, est satisfaisante et permet aux utilisateurs d'accéder facilement aux services de messagerie, que ce soit depuis l'intérieur ou l'extérieur de l'entreprise.

De plus, les **adresses mail professionnelles des collaborateurs** sont utilisées de manière stratégique pour renforcer l'image et la cohérence de l'entreprise. Elles sont intégrées dans les **signatures mail**, ce qui contribue à véhiculer une identité visuelle professionnelle et homogène. Certaines adresses spécifiques, comme **contact@vdb-pro.fr**, sont également publiées sur le **site web officiel**, renforçant ainsi la **présence en ligne** de vdb-pro et facilitant les échanges avec les clients, partenaires ou prospects. Cette démarche améliore la visibilité de l'entreprise tout en inspirant confiance et crédibilité.

Partie 2 – Validation

Pour valider ce projet, je peux confirmer que mon serveur Exchange est correctement mis en place. Il est sécurisé à travers des règles de pare-feu strictes, garantissant la protection des flux entrants et sortants. Un certificat SSL valide a été installé, assurant ainsi la sécurité des connexions au serveur. L'accès Webmail (OWA) fonctionne parfaitement, permettant aux utilisateurs de se connecter en toute sécurité depuis n'importe quel appareil. De plus, un contrôle d'accès strict a été mis en place pour le Centre d'administration d'Exchange. En restreignant l'accès à ce centre aux administrateurs uniquement via le serveur VP-EXCHANGE, j'ai renforcé la sécurité contre les accès non autorisés. Enfin, les services de messagerie, tant pour l'envoi que la réception de mails, qu'ils soient internes ou externes, sont pleinement opérationnels, garantissant ainsi un service de messagerie fiable et sécurisé pour l'entreprise.



Conclusion

La solution de messagerie Exchange a été correctement déployée, offrant ainsi un environnement de communication sécurisé et fiable pour tous les utilisateurs de l'entreprise. Les résultats attendus ont été atteints, avec un service de messagerie entièrement fonctionnel, accessible et sécurisé, permettant à l'entreprise de répondre à ses besoins de communication électronique à court et long terme.

Partie 3 – Veille technologique

Dans le cadre de la mise en place de mon serveur de messagerie Exchange, j'ai réalisé une veille technologique approfondie pour me tenir informé des dernières innovations et solutions alternatives susceptibles d'améliorer l'efficacité et la sécurité de la solution déployée. Cette veille m'a permis d'explorer diverses options disponibles sur le marché, ainsi que de suivre les mises à jour proposées par Microsoft, notamment les **Cumulative Updates (CU)** pour Exchange Server.

Les **Cumulative Updates (CU)** jouent un rôle crucial dans l'optimisation des performances et la correction de vulnérabilités. Chaque CU apporte des améliorations fonctionnelles et de sécurité, et il est essentiel de suivre les nouvelles versions afin de garantir que le serveur Exchange reste à jour et sécurisé. Les Cumulative Updates sont publiés régulièrement et contiennent des correctifs importants pour des problèmes de performance, de stabilité et de sécurité. En outre, je me suis assuré d'utiliser la derniere CU pour garantir une securité infaillible.

Dans le cadre de ma veille, j'ai également exploré des **solutions alternatives** à Microsoft Exchange, telles que **Zimbra** et **Grommunio**, qui offrent des fonctionnalités similaires en matière de messagerie, de calendrier et de contacts. Ces solutions open-source ou basées sur des modèles de licences plus flexibles peuvent constituer des options intéressantes, en fonction des besoins spécifiques de l'entreprise.

Enfin, ma veille a inclus la surveillance des **meilleures pratiques de cybersécurité** liées à Exchange, telles que l'utilisation d'authentification multi-facteurs (MFA) pour protéger les connexions des utilisateurs, l'analyse des logs de sécurité pour détecter des comportements suspects, et l'intégration de solutions anti-spam et anti-phishing pour renforcer la sécurité du service de messagerie que j'envisagerai de mettre en place prochainement.

Organiser son développement professionnel

Mon **environnement d'apprentissage personnel** est structuré autour d'un laboratoire virtuel comprenant plusieurs machines virtuelles (Exchange, Active Directory, serveur de sauvegarde, etc.), me permettant de tester, configurer et valider des solutions sans impacter l'environnement de production. Cet espace est essentiel pour renforcer mes compétences techniques tout en expérimentant en toute sécurité.

Je mène également une **veille technologique régulière**, avec pour objectifs de **suivre les évolutions des mises à jour cumulatives (CU) d'Exchange**, repérer les **nouveautés et meilleures pratiques** dans le domaine de la messagerie et de la cybersécurité, et d'identifier les **alternatives potentielles** comme Zimbra ou Microsoft 365. J'utilise des sources fiables telles que les blogs officiels de Microsoft

BTS Services informatiques aux organisations- SISR

Session 2025

E6 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :

Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- **Layer Bureautique et Informatique** est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro.
- La problématique principale réside dans le besoin pour les utilisateurs d'accéder à un environnement de travail distant, centralisé et sécurisé pour avoir accès au logiciel ERP Dolibarr, tout en assurant une gestion efficace des droits et des flux réseau.
- La solution choisie consiste à déployer d'un serveur RDS sous Windows Server 2022 intégré à l'Active Directory, avec gestion des accès via GPO et séparation des réseaux via VLAN.

Intitulé de la réalisation professionnelle

Déploiement d'une Solution de Bureau à Distance

Période de réalisation : 10/02/25- 12/02/25 **Lieu :** Auxerre

Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE
- ORGANISER SON DEVELOPPEMENT PROFESIONNEL
- GERER LE PATRIMOINE INFORMATIQUE

Conditions de réalisation

- **Ressources disponibles (Situation avant RP)**
  L'infrastructure de départ comprend un serveur ESXi opérationnel pour l'hébergement de machines virtuelles, ainsi qu'un contrôleur de domaine Active Directory déjà en place, incluant un service DNS fonctionnel. D'autres services réseau de base (DHCP, VLANs, pare-feu) sont également configurés pour permettre le bon déroulement de la réalisation.
- **Résultats attendus (Situation après RP)**
  Les utilisateurs doivent pouvoir se connecter à distance à un environnement de travail virtualisé via RDS, avec des droits restreints et sécurisés pour accéder à l'**ERP Dolibarr**. L'intégration est complète au domaine Active Directory. L'administration doit être centralisée, et les flux réseau correctement segmentés par VLAN.
- **Durée de réalisation**
  Cela à pris 3 jours, incluant installation, configuration, sécurisation et phase de test.

Modalités d'accès à cette réalisation professionnelle.

https://portfolio.vdb-pro.fr mdp : *Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

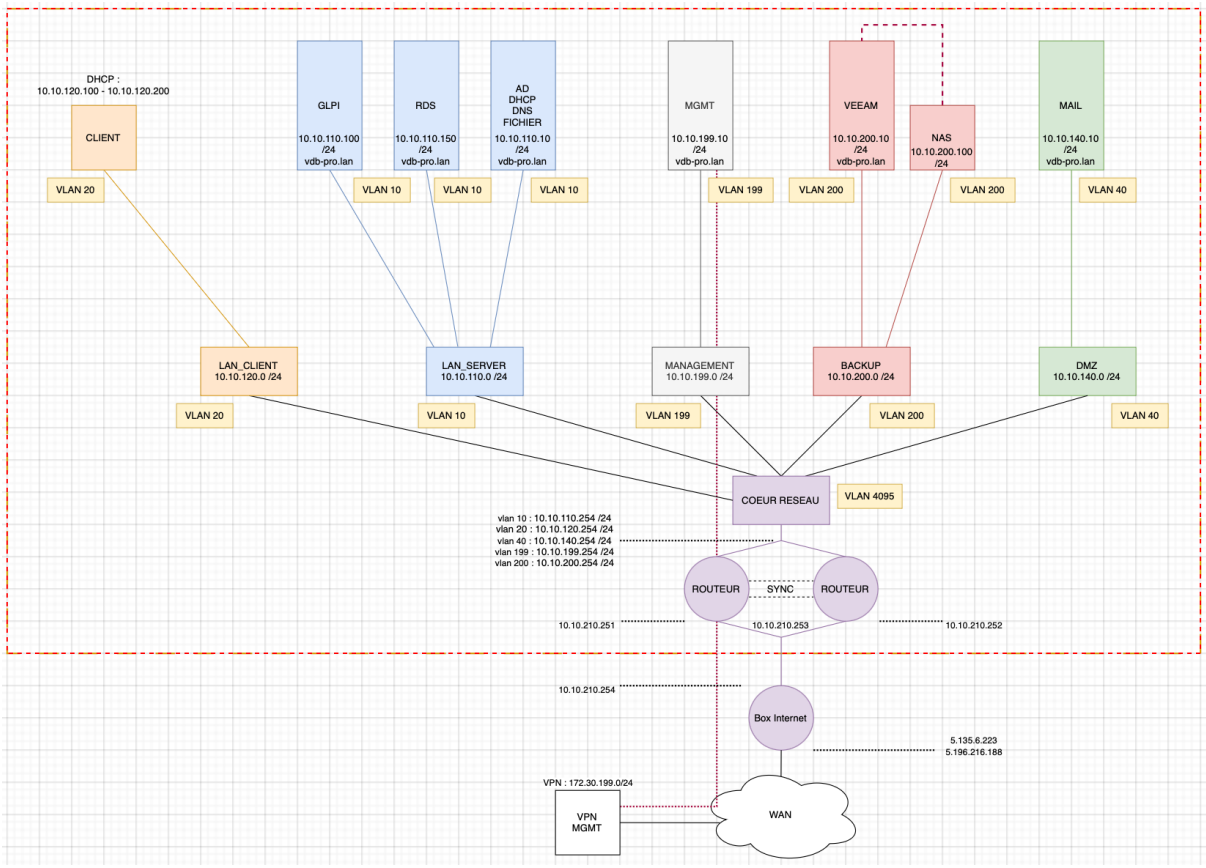
Dans le cadre de l'infrastructure informatique que j'ai mise en place pour l'entreprise, **vdb-pro,** j'ai conçu et déployé un réseau interne visant un environnement professionnel sécurisé et fonctionnel. Une composante essentielle de cette architecture repose sur la mise en place d'un service de bureau à distance, basé sur Microsoft Windows Server 2022 et utilisant le rôle Remote Desktop Services (RDS).

Cette solution permet aux utilisateurs d'accéder à un environnement de travail distant (session Windows virtuelle) depuis n'importe quel poste client autorisé, tout en assurant une sécurité, une centralisation et une gestion simplifiée.

La gestion des comptes utilisateurs et des droits d'accès à ce service sera assurée par l'Active Directory, préalablement mis en place dans le cadre d'une autre Réalisation Professionnelle. Cela garantit une centralisation de l'authentification et une meilleure gestion des ressources au sein de l'organisation.

Objectifs de la réalisation

L'objectif principal de cette réalisation au sein de mon entreprise *vdb-pro* était de déployer un **serveur Windows Server 2022** configuré avec le rôle **Remote Desktop Services (RDS)**, afin de fournir un environnement de travail distant, stable et sécurisé aux utilisateurs pour qu'ils accèdent au logiciel ERP Dolibarr. Ce serveur devait permettre aux collaborateurs d'accéder à une session de bureau virtuelle, sans avoir un accès physique direct aux machines hôtes. Pour garantir une **authentification centralisée** et une gestion efficace des droits d'accès, le serveur RDS a été intégré à une **infrastructure Active Directory** préexistante. Par ailleurs, une **segmentation réseau par VLAN** a été mise en place afin de séparer les flux entre les postes utilisateurs et les serveurs, renforçant ainsi la sécurité de l'architecture. L'ensemble de la solution repose sur une **gestion centralisée des comptes utilisateurs et des autorisations**, assurant une administration simplifiée et conforme aux bonnes pratiques en entreprise.

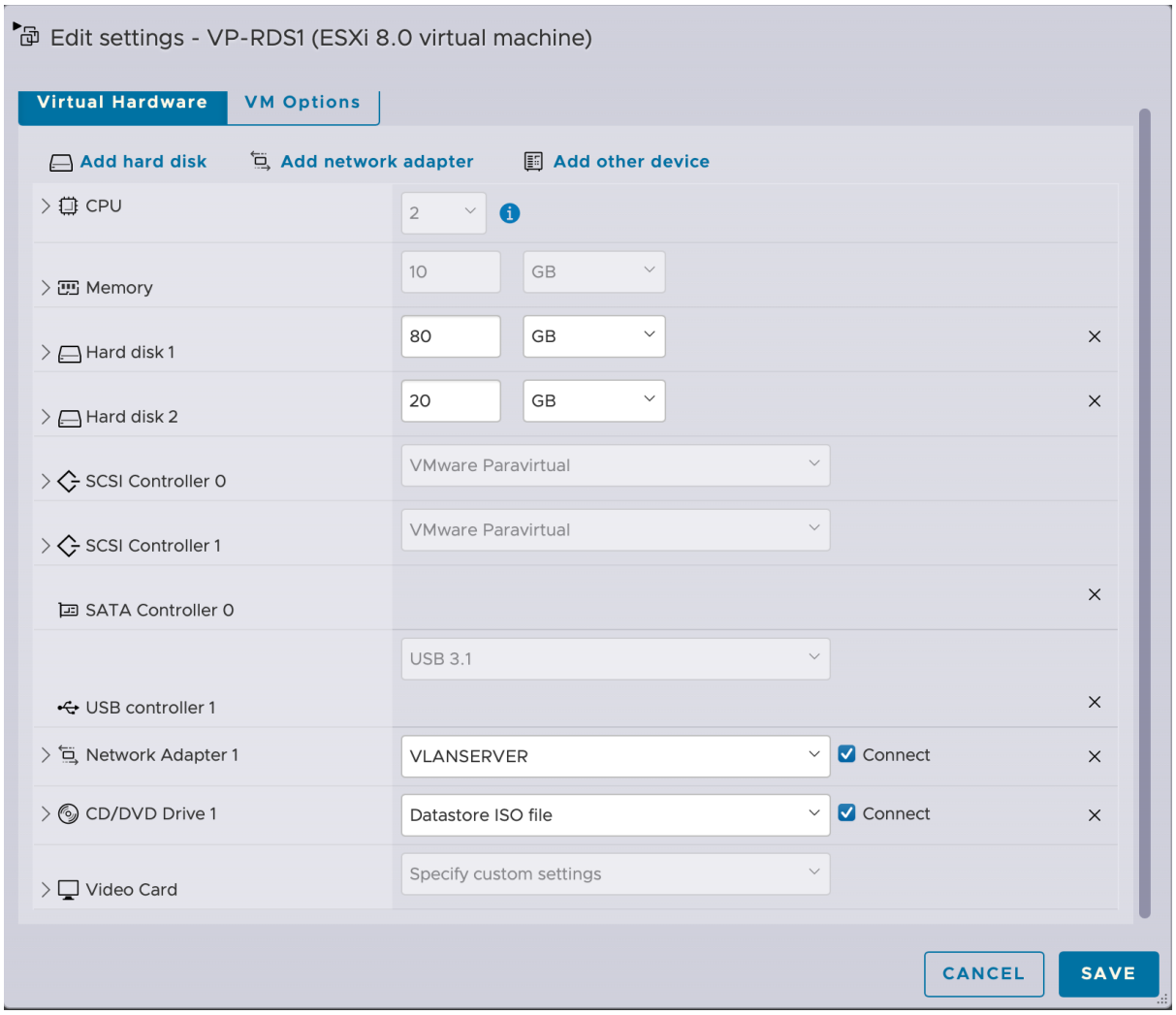


Infrastructure et environnement technique

L'infrastructure déployée au sein de *vdb-pro* repose sur un environnement **virtualisé sous VMware ESXi**, dans lequel a été installé un **serveur Windows Server 2022** dédié au rôle **Remote Desktop Services (RDS)**, avec un **déploiement de type Session-Based**. Ce serveur a été intégré à un **contrôleur de domaine Active Directory**, également sous Windows Server 2022, déjà mis en place dans le cadre d'une autre réalisation. Les **clients RDS** sont constitués de postes de travail sous **Windows 10 et 11**, tous intégrés au domaine, permettant une gestion centralisée des connexions. Sur le plan réseau, l'architecture est segmentée en deux VLANs distincts : le **VLAN 10 (LAN_SERVER)**, réservé aux serveurs, notamment le RDS, et le **VLAN 20 (LAN_CLIENTS)**, dédié aux utilisateurs finaux. Cette séparation permet un **meilleur contrôle des flux réseau et une sécurisation accrue** de l'environnement. Divers **outils d'administration** ont été utilisés pour cette réalisation, tels que les **stratégies de groupe (GPO)** pour restreindre l'environnement utilisateur sur les sessions distantes, le **gestionnaire de serveur RDS** pour le déploiement et la gestion des services, ainsi que le **pare-feu Windows**, configuré pour assurer un **filtrage strict entre les VLANs**.

Mise en place d'une machine virtuelle

J'ai procédé à la création d'une **machine virtuelle dédiée au rôle RDS** sur mon **hyperviseur VMware ESXi**. Cette machine a été configurée avec un **disque principal de 80 Go** destiné au système d'exploitation, ainsi qu'un **second disque de 20 Go** utilisé comme espace de **swap**, afin d'optimiser les performances de la machine en cas de surcharge mémoire. Pour assurer un **contrôle précis des disques virtuels** et améliorer les performances d'E/S, j'ai configuré deux **contrôleurs SCSI** en mode **VMware Paravirtual (PVSCSI)**, une option recommandée pour les environnements fortement sollicités en lecture/écriture. Côté réseau, la machine a été rattachée au **réseau LAN_SERVER (VLAN 10)** afin de garantir un cloisonnement logique avec les autres segments du réseau. Enfin, j'ai effectué une **réservation de 10 Go de mémoire vive (RAM)** exclusivement pour ce serveur, afin d'éviter toute contention de ressources avec d'autres machines virtuelles hébergées sur l'ESXi, et d'assurer une **stabilité optimale** pour les sessions distantes hébergées.



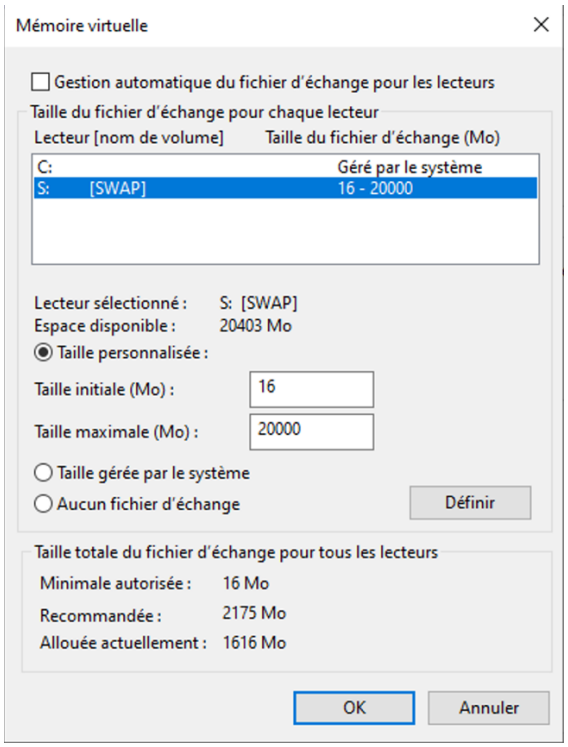
Installation de Windows Server 2022 et Intégration au Domain

J'ai commencé par procéder à l'installation du système d'exploitation Windows Server 2022. Avant son intégration au domaine, j'ai effectué une configuration initiale comprenant la définition du nom d'hôte en tant que VP-RDS1. Ce nom a été choisi dans une logique d'évolutivité, afin de prévoir la possibilité d'ajouter ultérieurement d'autres serveurs RDS (ex. VP-RDS2, VP-RDS3, etc.) pour constituer une ferme RDS complète en fonction des besoins futurs de mon entreprise vdb-pro.

La configuration réseau statique du serveur a été réalisée manuellement avec l'attribution d'une adresse IP fixe, la passerelle (Gateway) par défaut et les serveurs DNS, en cohérence avec le plan d'adressage défini pour le VLAN 10 (LAN_SERVER). Une fois cette configuration terminée, le serveur a été rejoint au domaine Active Directory "VDB-PRO", préalablement mis en place. J'ai ensuite vérifié la bonne remontée des enregistrements DNS dans le gestionnaire DNS du contrôleur de domaine, afin de m'assurer que le serveur VP-RDS1 pouvait être résolu correctement par les clients du réseau. Cette étape est essentielle pour garantir une intégration cohérente dans l'infrastructure existante.

Configuration du PageFile.sys sur un autre disque

Afin d'optimiser la gestion de la mémoire virtuelle du serveur, j'ai déplacé le fichier **pagefile.sys** (fichier d'échange) vers un **disque différent de celui contenant le système d'exploitation**. Cette configuration permet de **réduire la charge sur le disque principal**, d'**améliorer les performances en cas de surallocation de la mémoire RAM**, et de mieux répartir les ressources du système. Pour ce faire, je suis passé par les **paramètres système avancés** de Windows, dans l'onglet **"Performances" > "Paramètres" > "Avancé"**, puis j'ai défini manuellement l'emplacement et la taille du fichier d'échange sur le second disque.

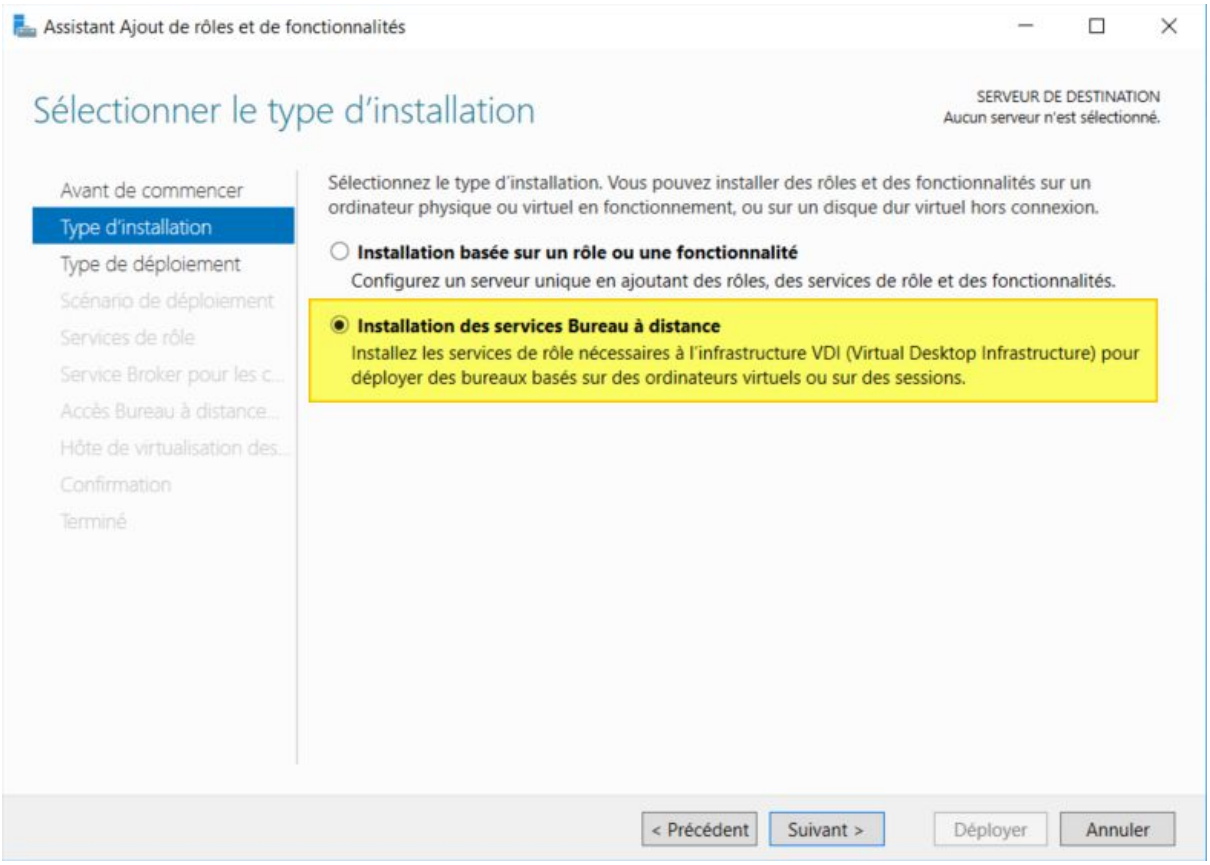


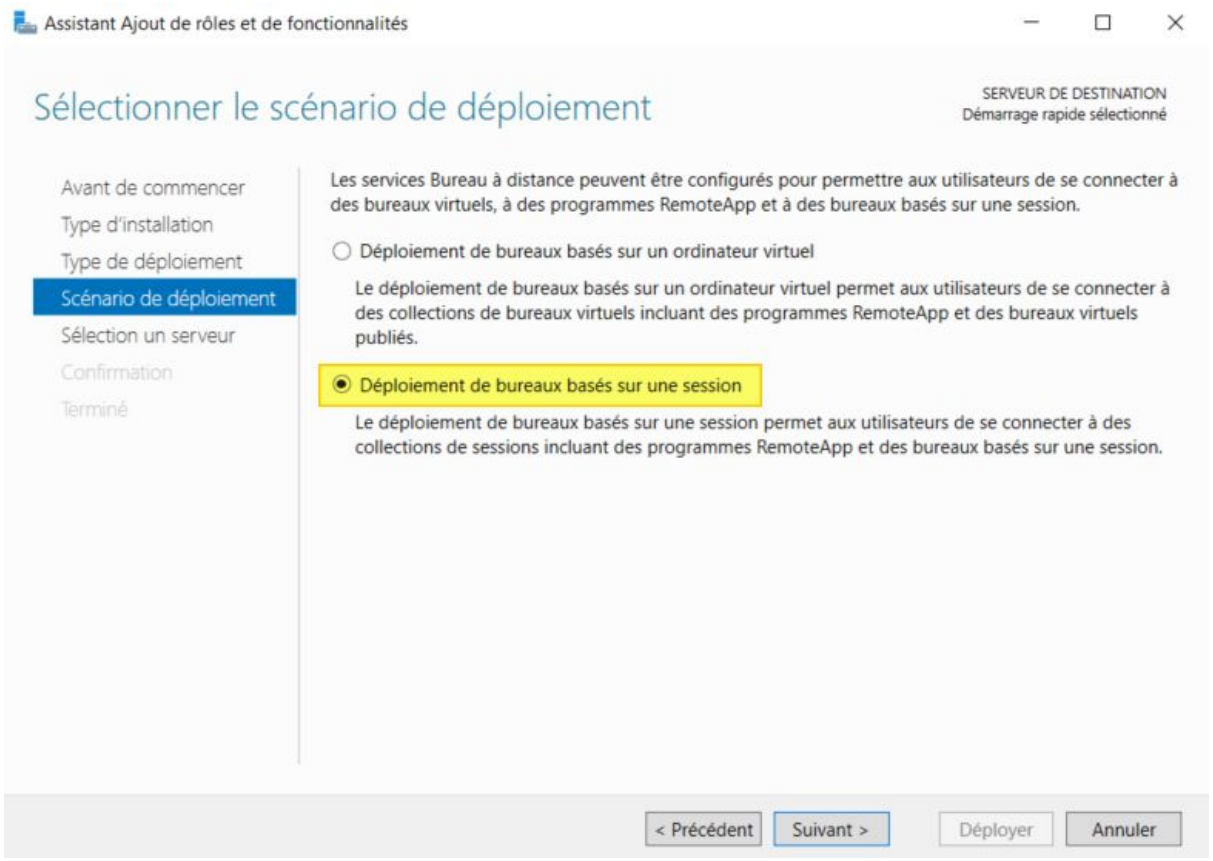
Installation des services Remote Desktop Services

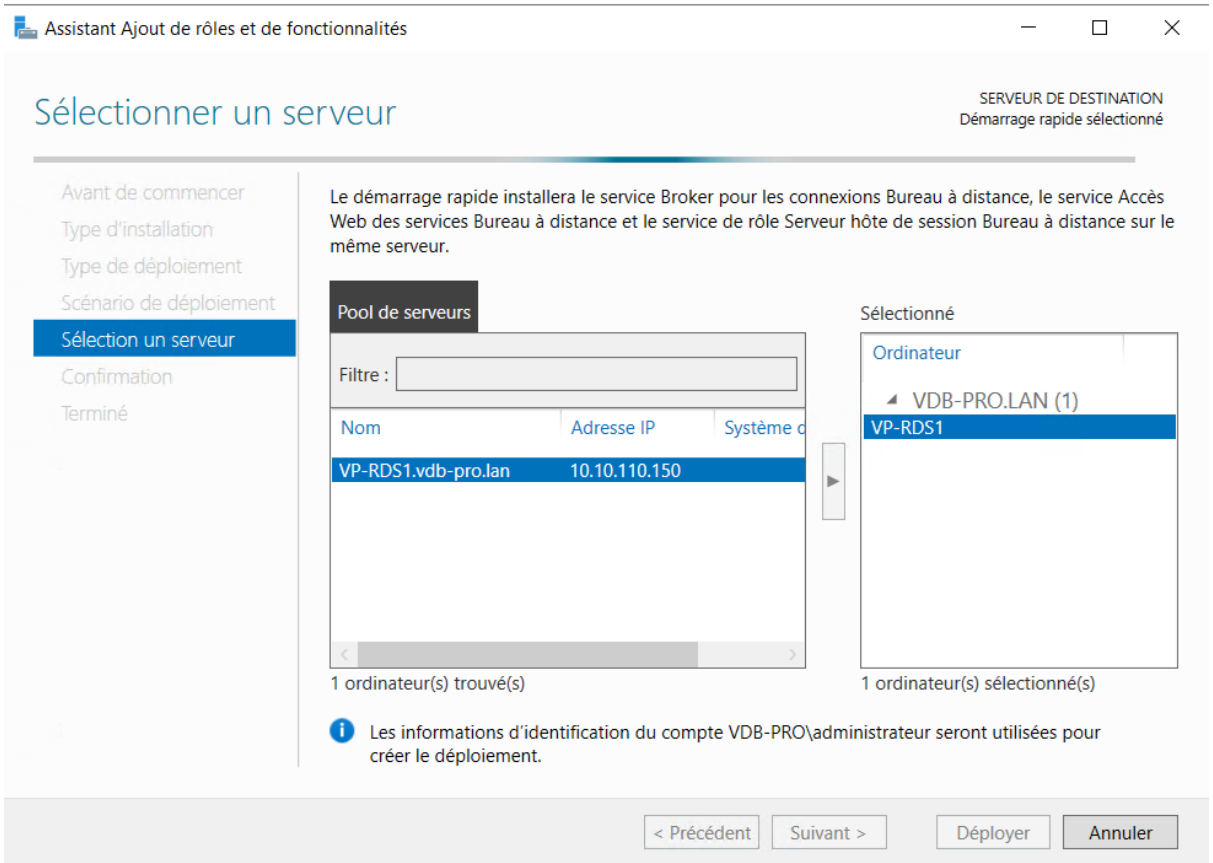
Par la suite, j'ai procédé à l'installation des services essentiels au bon fonctionnement de Remote Desktop Services (RDS) sur le serveur VP-RDS1. Pour cela, j'ai utilisé le Gestionnaire de serveur afin d'ajouter les rôles nécessaires à la mise en place d'un environnement RDS basé sur les sessions. Les services installés incluent notamment :

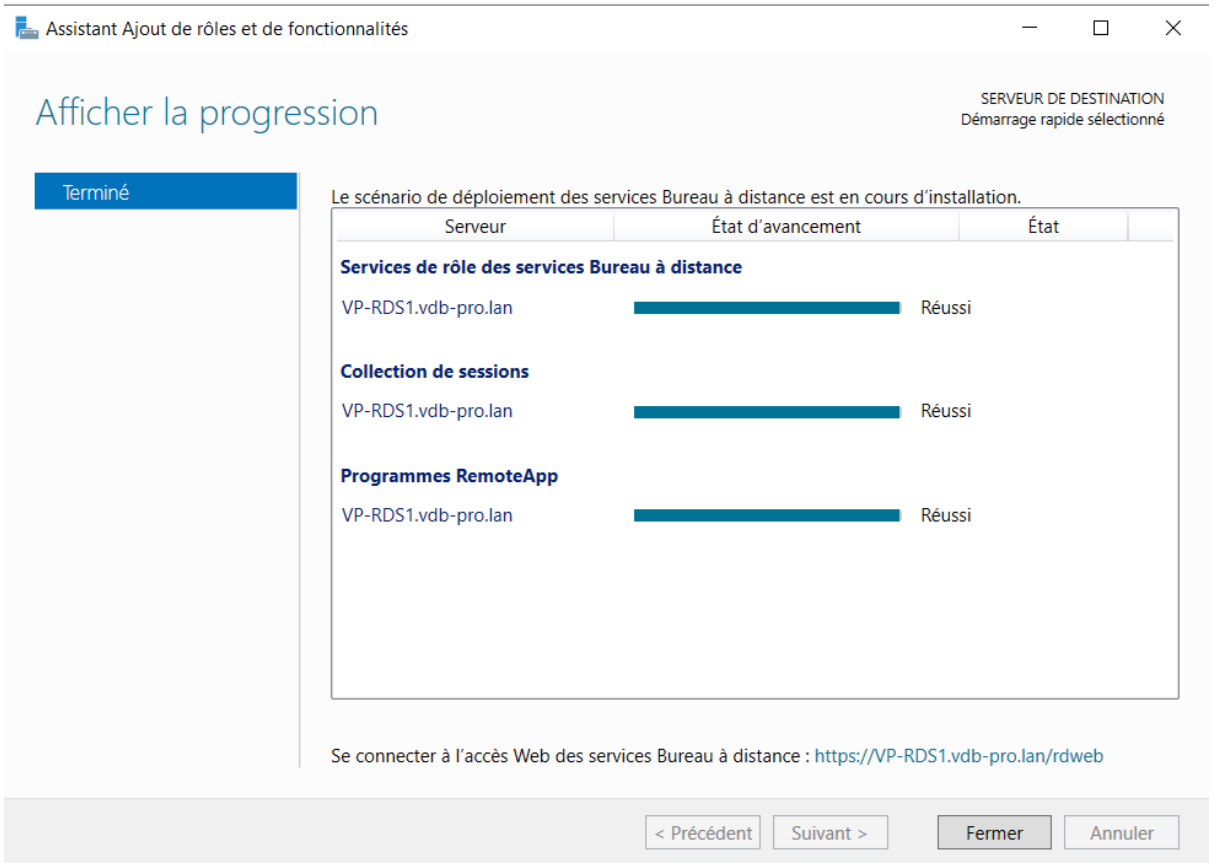
- Remote Desktop Session Host (RDSH) : service principal permettant d'héberger les sessions de bureau à distance auxquelles les utilisateurs se connectent. (Page 6-7)
- Remote Desktop Web Access (facultatif selon le besoin) : permet l'accès aux ressources via un navigateur Web sécurisé. (Page 6-7)
- Remote Desktop Licensing (prévu pour une mise en conformité future) : gestion des licences d'accès client (CAL) RDS. (Page 8-9)

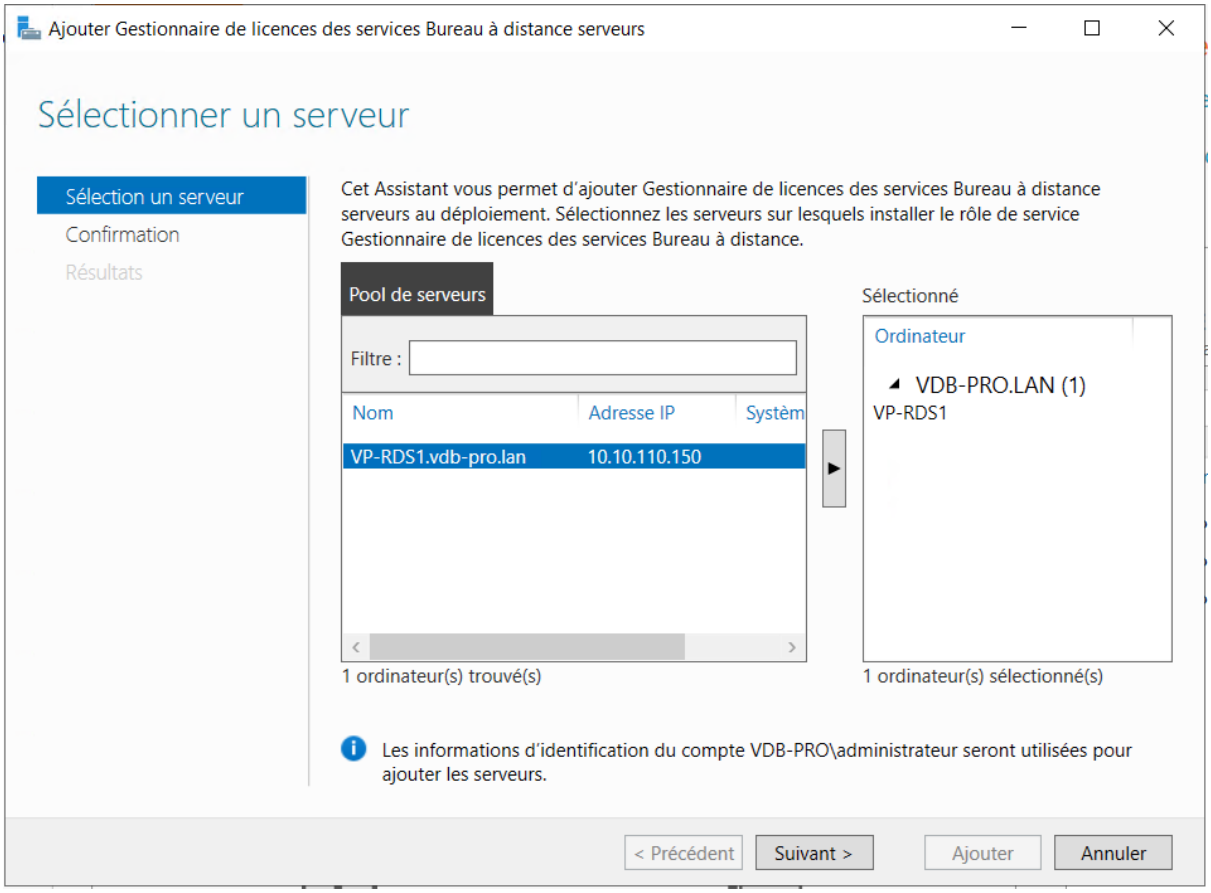
Chaque rôle a été installé de manière à respecter les bonnes pratiques de sécurité et à permettre une évolution progressive de l'infrastructure RDS. L'installation a été suivie d'un redémarrage du serveur et d'une vérification de l'état des services RDS via la console d'administration, afin de garantir que tous les composants soient opérationnels.

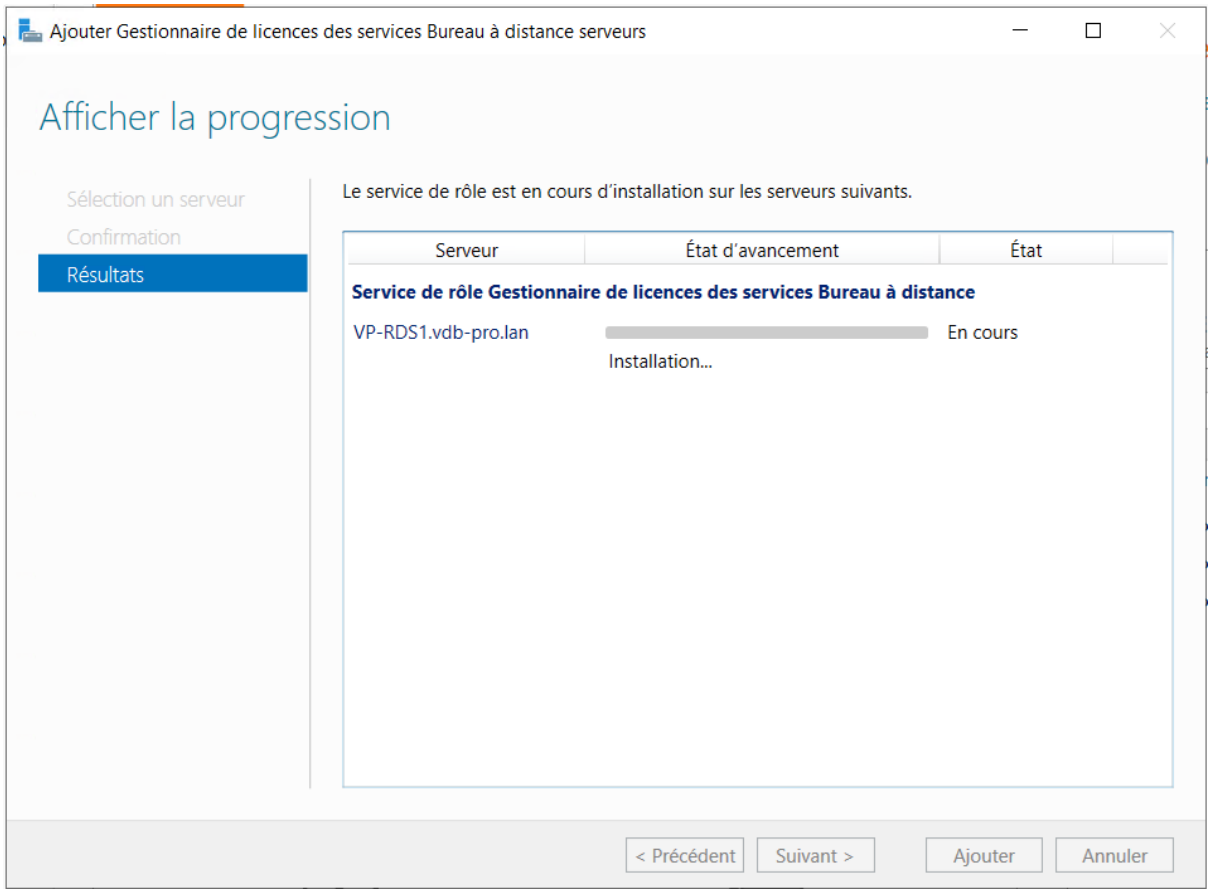


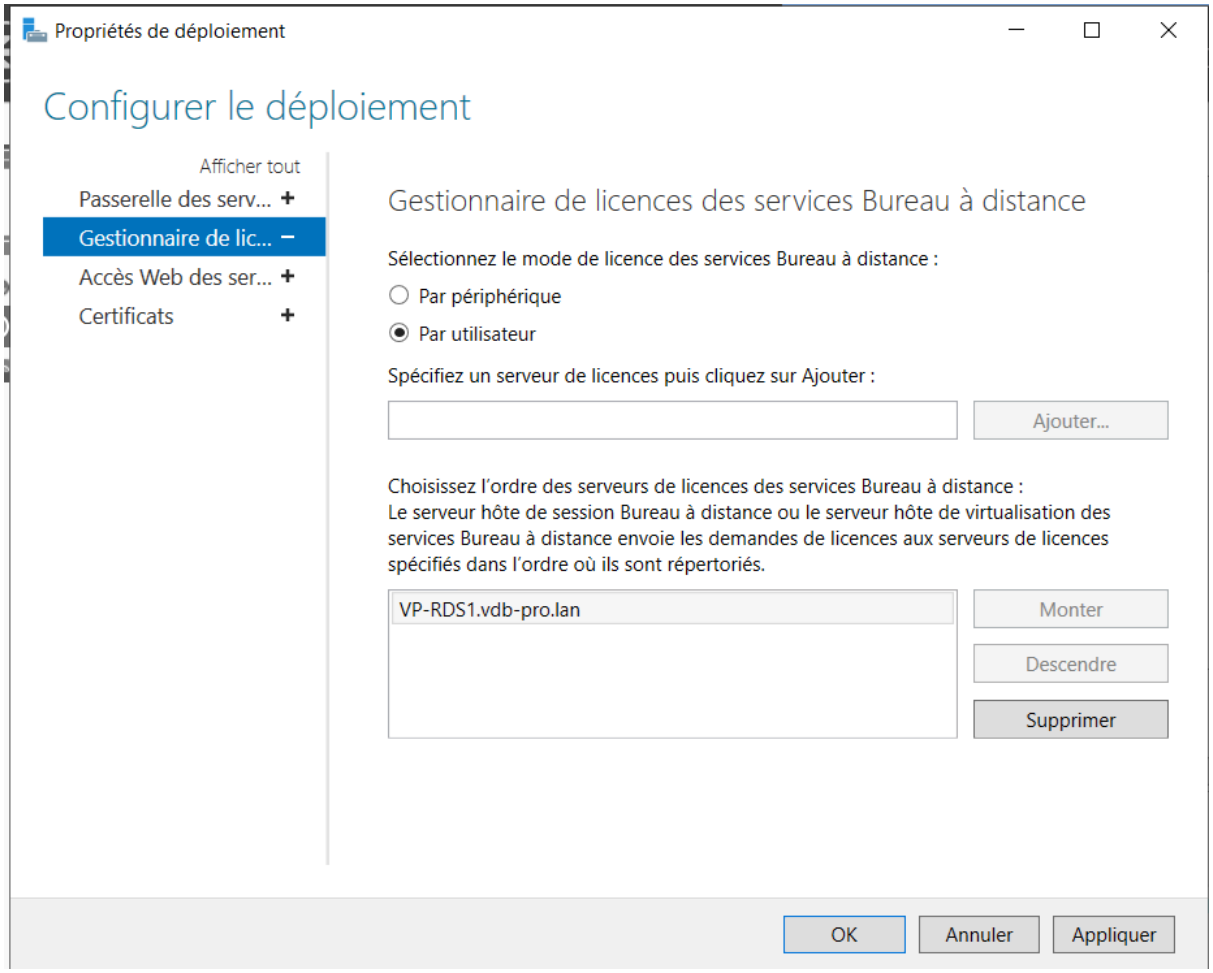

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le scénario de déploiement
SERVEUR DE DESTINATION
Démarrage rapide sélectionné
Avant de commencer
Type d'installation
Type de déploiement
Scénario de déploiement
Sélection un serveur
Confirmation
Terminé
Les services Bureau à distance peuvent être configurés pour permettre aux utilisateurs de se connecter à des bureaux virtuels, à des programmes RemoteApp et à des bureaux basés sur une session.
Déploiement de bureaux basés sur un ordinateur virtuel
Le déploiement de bureaux basés sur un ordinateur virtuel permet aux utilisateurs de se connecter à des collections de bureaux virtuels incluant des programmes RemoteApp et des bureaux virtuels publiés.
Déploiement de bureaux basés sur une session
Le déploiement de bureaux basés sur une session permet aux utilisateurs de se connecter à des collections de sessions incluant des programmes RemoteApp et des bureaux basés sur une session.
< Précédent
Suivant >
Déployer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Sélectionner un serveur
SERVEUR DE DESTINATION
Démarrage rapide sélectionné
Avant de commencer
Type d'installation
Type de déploiement
Scénario de déploiement
Sélection un serveur
Confirmation
Terminé
Le démarrage rapide installera le service Broker pour les connexions Bureau à distance, le service Accès Web des services Bureau à distance et le service de rôle Serveur hôte de session Bureau à distance sur le même serveur.
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d
VP-RDS1.vdb-pro.lan
10.10.110.150
1 ordinateur(s) trouvé(s)
Sélectionné
Ordinateur
VDB-PRO.LAN (1)
VP-RDS1
1 ordinateur(s) sélectionné(s)
Les informations d'identification du compte VDB-PRO\administrateur seront utilisées pour créer le déploiement.
< Précédent
Suivant >
Déployer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Afficher la progression
SERVEUR DE DESTINATION
Démarrage rapide sélectionné
Terminé
Le scénario de déploiement des services Bureau à distance est en cours d'installation.
Serveur
État d'avancement
État
Services de rôle des services Bureau à distance
VP-RDS1.vdb-pro.lan
Réussi
Collection de sessions
VP-RDS1.vdb-pro.lan
Réussi
Programmes RemoteApp
VP-RDS1.vdb-pro.lan
Réussi
Se connecter à l'accès Web des services Bureau à distance : https://VP-RDS1.vdb-pro.lan/rdweb
< Précédent
Suivant >
Fermer
Annuler

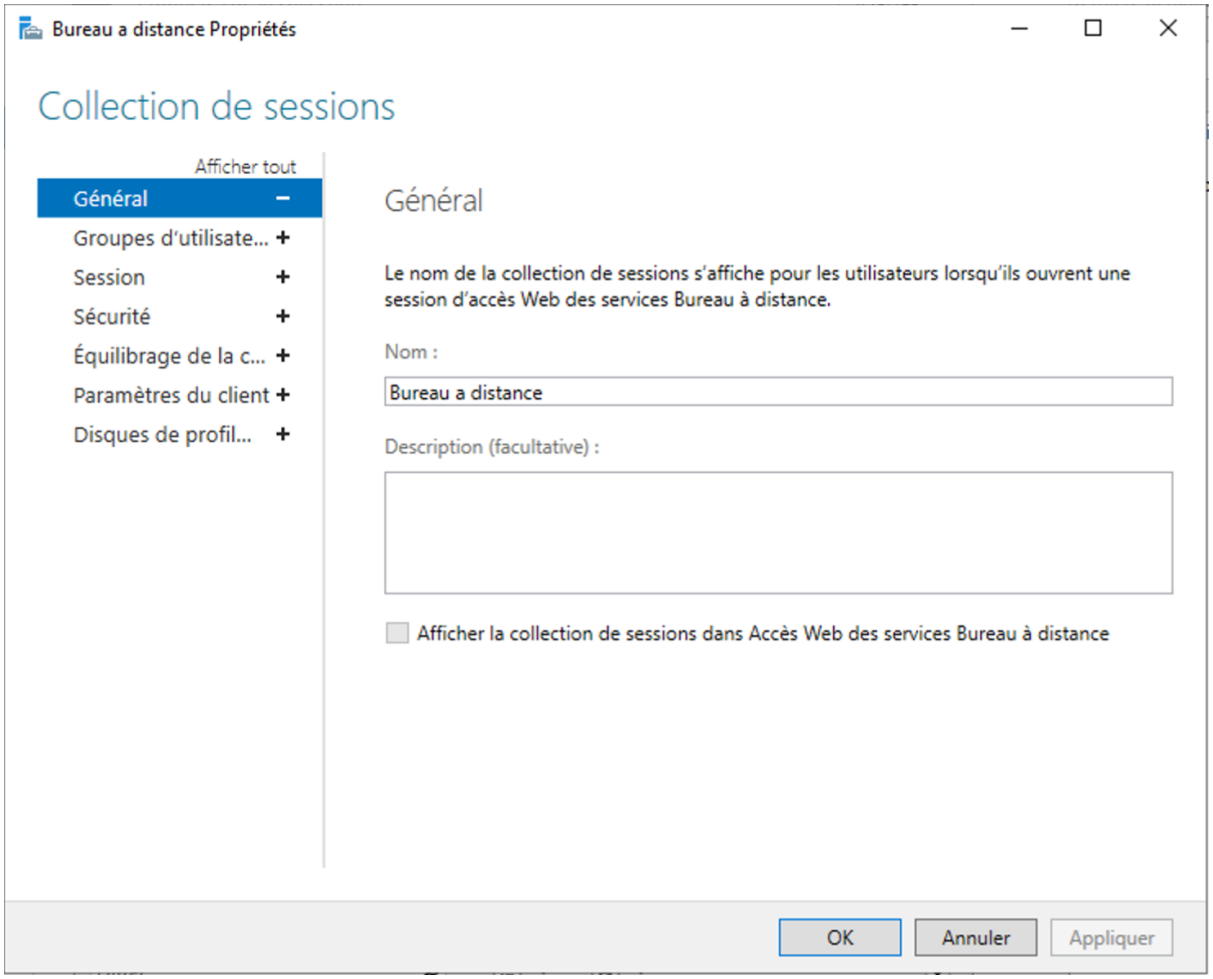

Ajouter Gestionnaire de licences des services Bureau à distance serveurs
Sélectionner un serveur
Sélection un serveur
Confirmation
Résultats
Cet Assistant vous permet d'ajouter Gestionnaire de licences des services Bureau à distance serveurs au déploiement. Sélectionnez les serveurs sur lesquels installer le rôle de service Gestionnaire de licences des services Bureau à distance.
Pool de serveurs
Filtre :
Nom
Adresse IP
Systèm
VP-RDS1.vdb-pro.lan
10.10.110.150
1 ordinateur(s) trouvé(s)
Sélectionné
Ordinateur
VDB-PRO.LAN (1)
VP-RDS1
1 ordinateur(s) sélectionné(s)
Les informations d'identification du compte VDB-PRO\administrateur seront utilisées pour ajouter les serveurs.
< Précédent
Suivant >
Ajouter
Annuler


Ajouter Gestionnaire de licences des services Bureau à distance serveurs
Afficher la progression
Sélection un serveur
Confirmation
Résultats
Le service de rôle est en cours d'installation sur les serveurs suivants.
Serveur
État d'avancement
État
Service de rôle Gestionnaire de licences des services Bureau à distance
VP-RDS1.vdb-pro.lan
En cours
Installation...
< Précédent
Suivant >
Ajouter
Annuler


Propriétés de déploiement
Configurer le déploiement
Afficher tout
Passerelle des serv...
Gestionnaire de lic...
Accès Web des ser...
Certificats
Gestionnaire de licences des services Bureau à distance
Sélectionnez le mode de licence des services Bureau à distance :
Par périphérique
Par utilisateur
Spécifiez un serveur de licences puis cliquez sur Ajouter :
Ajouter...
Choisissez l'ordre des serveurs de licences des services Bureau à distance :
Le serveur hôte de session Bureau à distance ou le serveur hôte de virtualisation des services Bureau à distance envoie les demandes de licences aux serveurs de licences spécifiés dans l'ordre où ils sont répertoriés.
VP-RDS1.vdb-pro.lan
Monter
Descendre
Supprimer
OK
Annuler
Appliquer

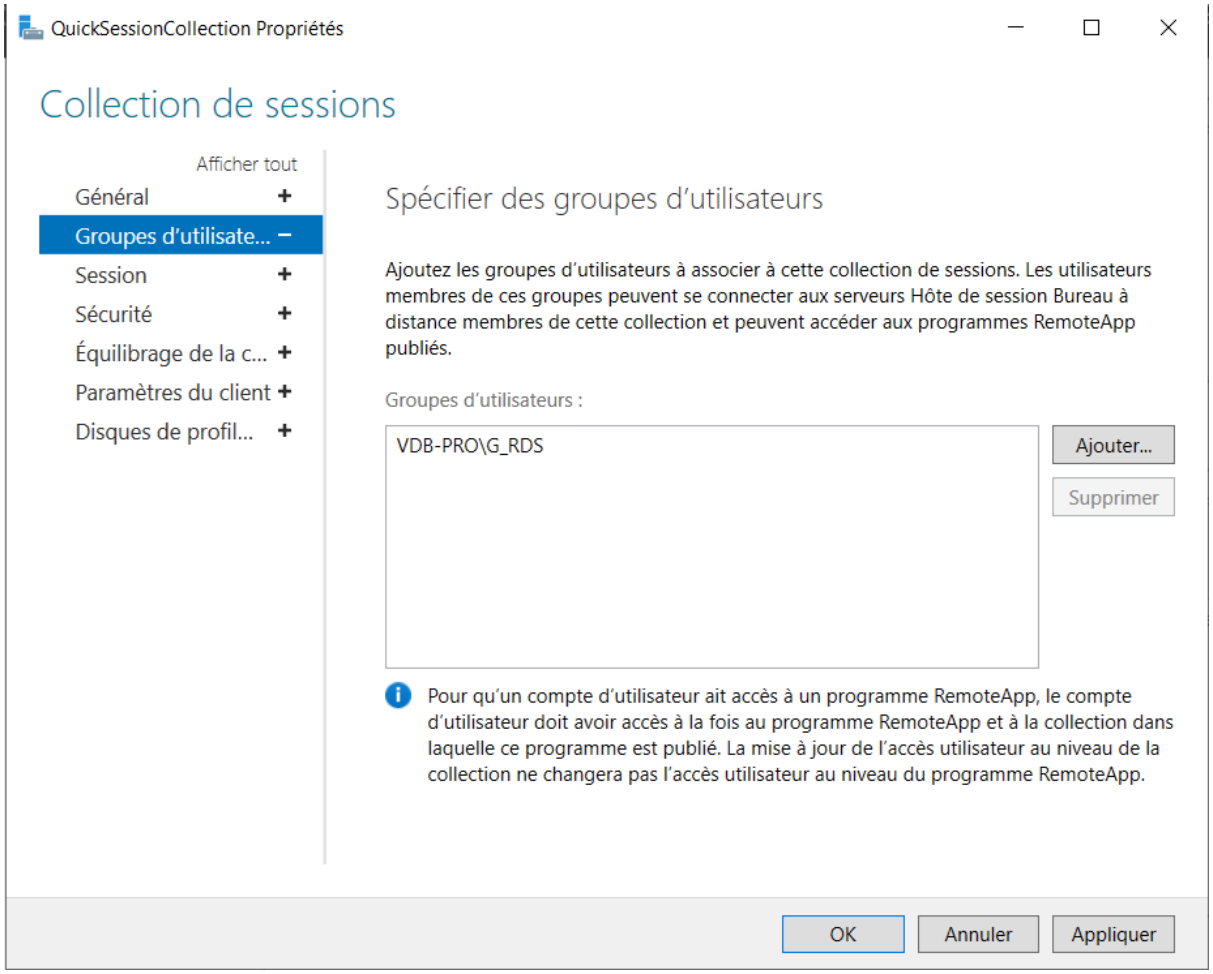
Configuration d'une collection de session

Une fois les rôles RDS installés, j'ai procédé à la création d'une collection de sessions, qui constitue l'élément central dans la gestion des connexions utilisateurs au sein d'un environnement Remote Desktop Services. La collection de sessions permet de définir les règles de fonctionnement des bureaux à distance : elle regroupe les utilisateurs autorisés, les ressources disponibles, et permet de gérer la façon dont les sessions sont ouvertes et administrées.

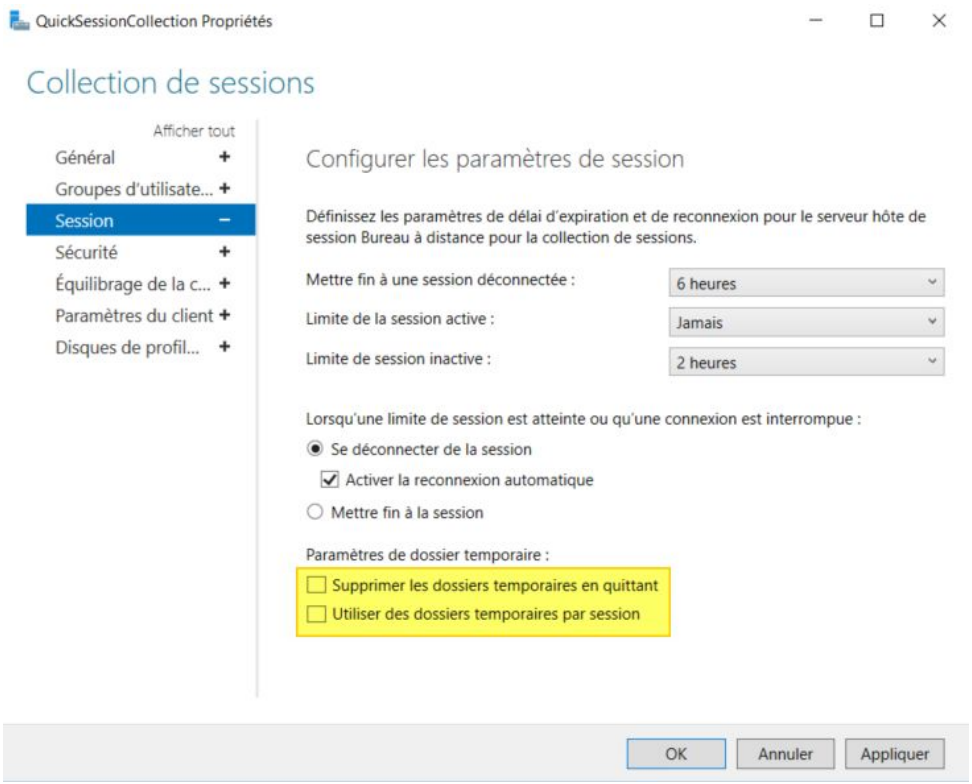


Au sein de cette collection, plusieurs paramètres peuvent être configurés afin de contrôler finement l'utilisation du service. Parmi ceux-ci, on peut notamment :

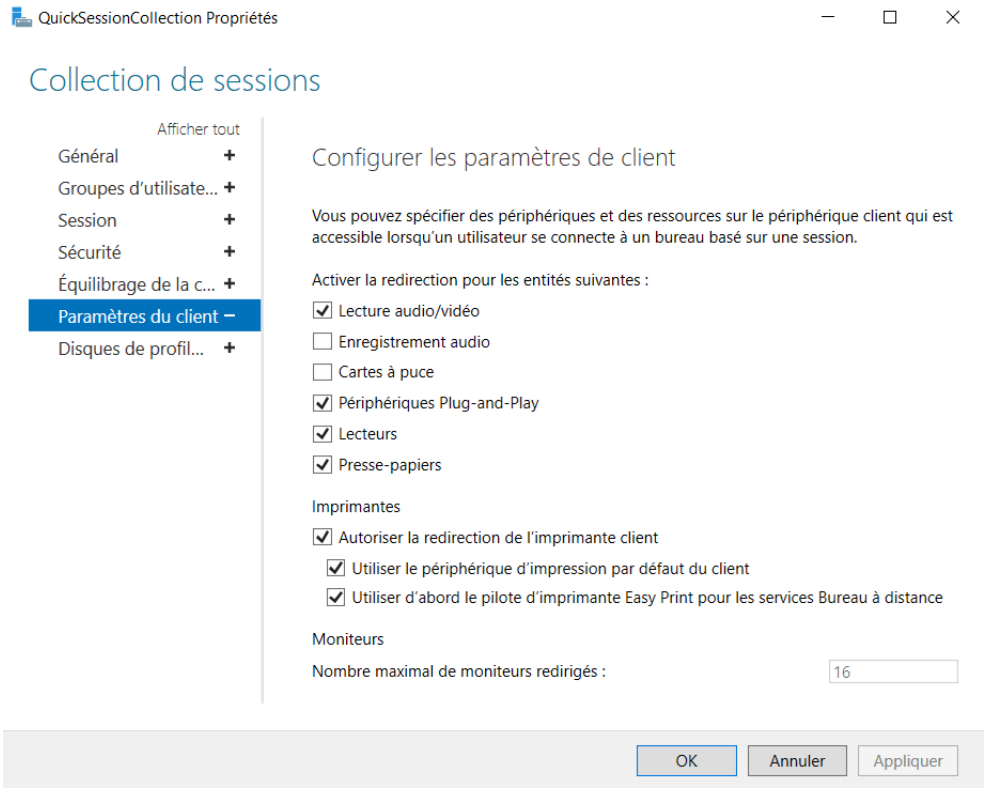
- Définir un dossier de profil utilisateur centralisé pour uniformiser l'environnement de travail,
- Déployer automatiquement des applications spécifiques via un environnement de type RemoteApp (si besoin).
- Restreindre l'accès à certains utilisateurs ou groupes Active Directory,



- Configurer des limites de temps d'inactivité ou de déconnexion automatique pour des raisons de sécurité,

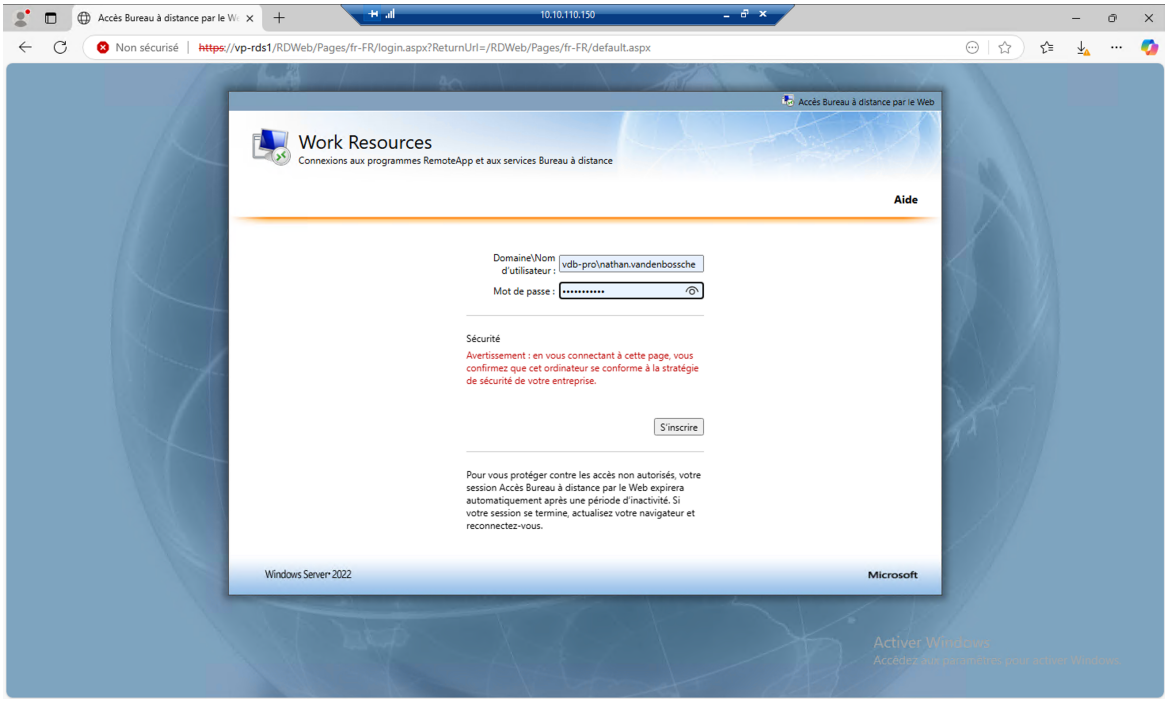


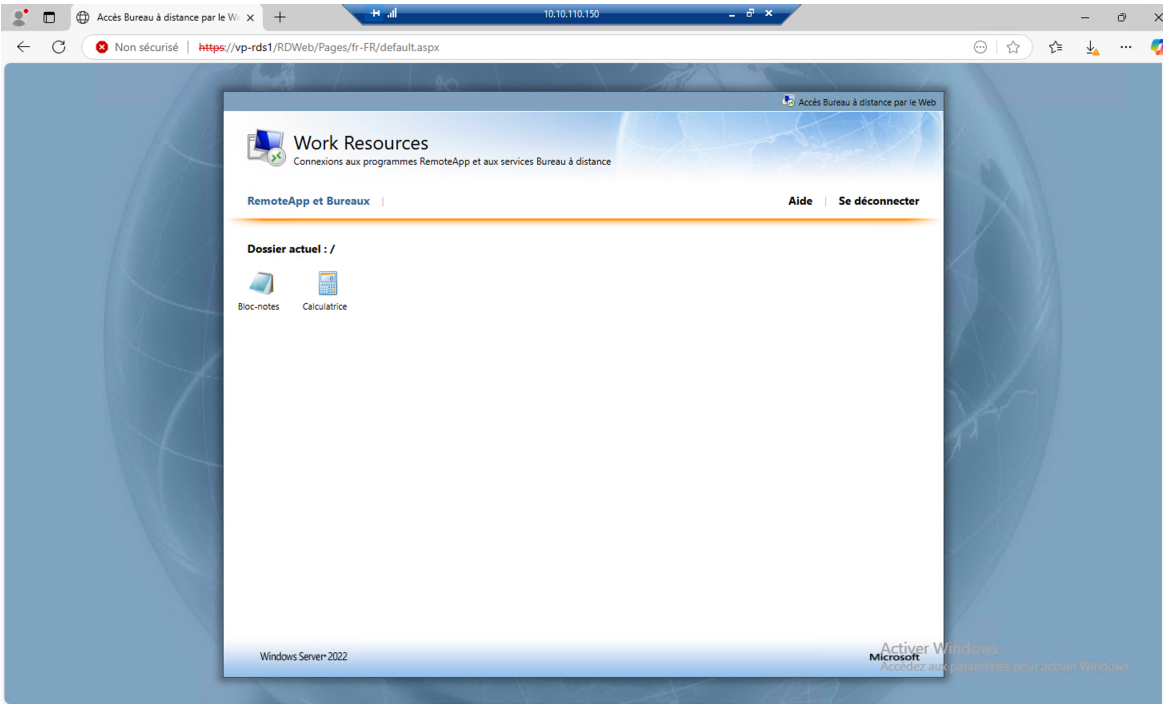
- Activer ou désactiver la redirection des périphériques (clés USB, imprimantes, presse-papiers),



Configuration du RemoteApp Web

J'ai également mis en place la fonctionnalité **RemoteApp via l'interface Web**, permettant aux utilisateurs autorisés de se connecter à un portail web RDS. Grâce à cette interface, ils peuvent lancer des applications spécifiques publiées sur le serveur, comme le Bloc-notes ou la Calculatrice, directement depuis leur poste local. Bien que l'application semble s'exécuter localement, elle est en réalité hébergée et traitée sur le serveur RDS. Cette solution permet une **expérience utilisateur fluide**, tout en **centralisant l'exécution des applications** et en **réduisant la charge sur les postes clients**.

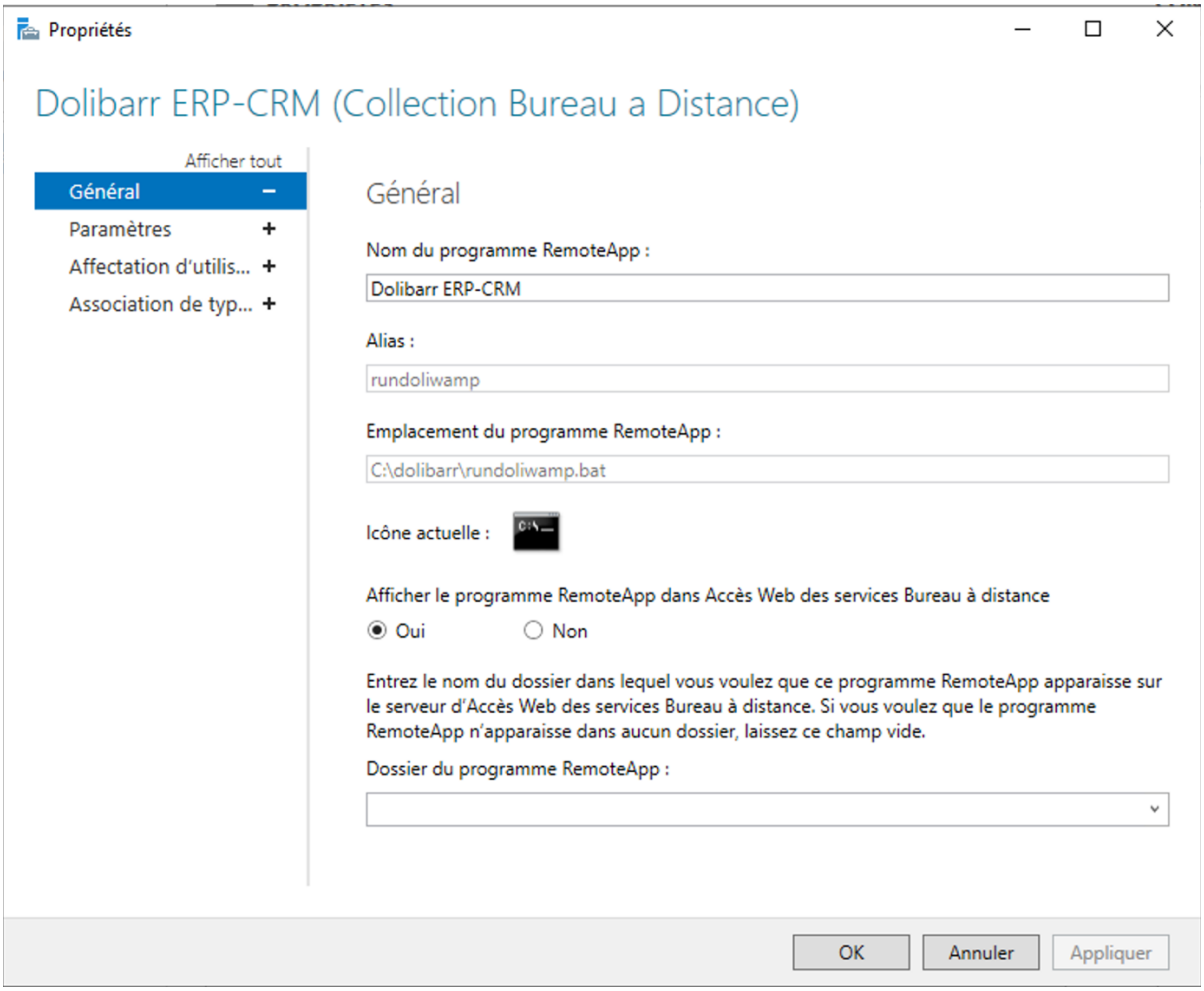




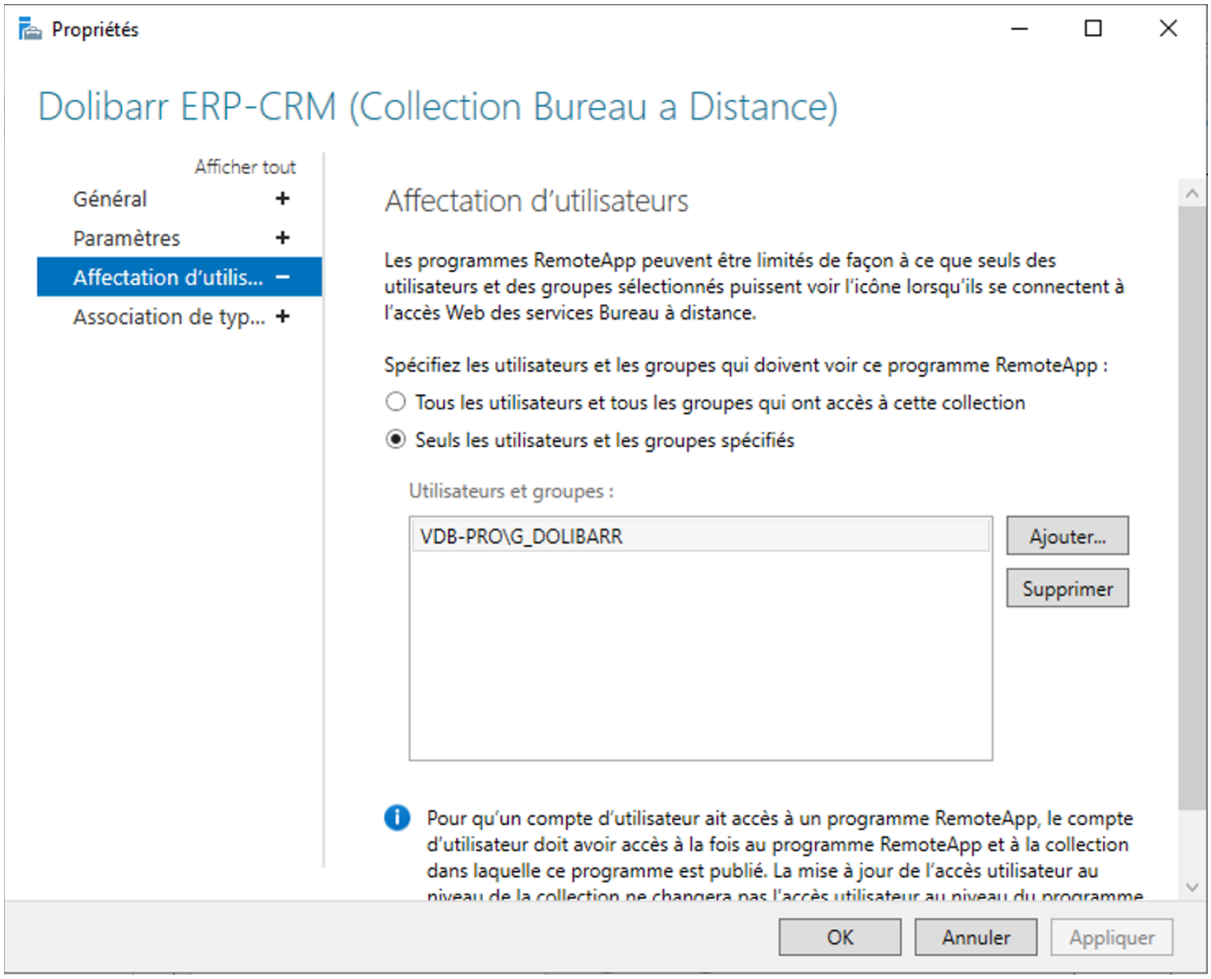
Ajout du logiciel ERP Dolibarr au RemoteApp Web

Pour ajouter le logiciel Dolibarr au portail RemoteApp, je me rends dans le **Gestionnaire de serveur RDS**, puis je clique sur **"Programmes RemoteApp"**, ensuite sur **"Tâches" > "Publier des programmes RemoteApp"**. Une fenêtre s'ouvre, affichant la liste des applications installées sur le serveur.

Je sélectionne **Dolibarr** parmi les programmes disponibles, puis je passe à l'étape suivante : **"Affectation des utilisateurs"**.



À ce niveau, je choisis de restreindre l'accès à l'application uniquement aux membres du **groupe de sécurité Active Directory** G_DOLIBARR, garantissant ainsi que seuls les utilisateurs autorisés puissent y accéder via RDWeb.



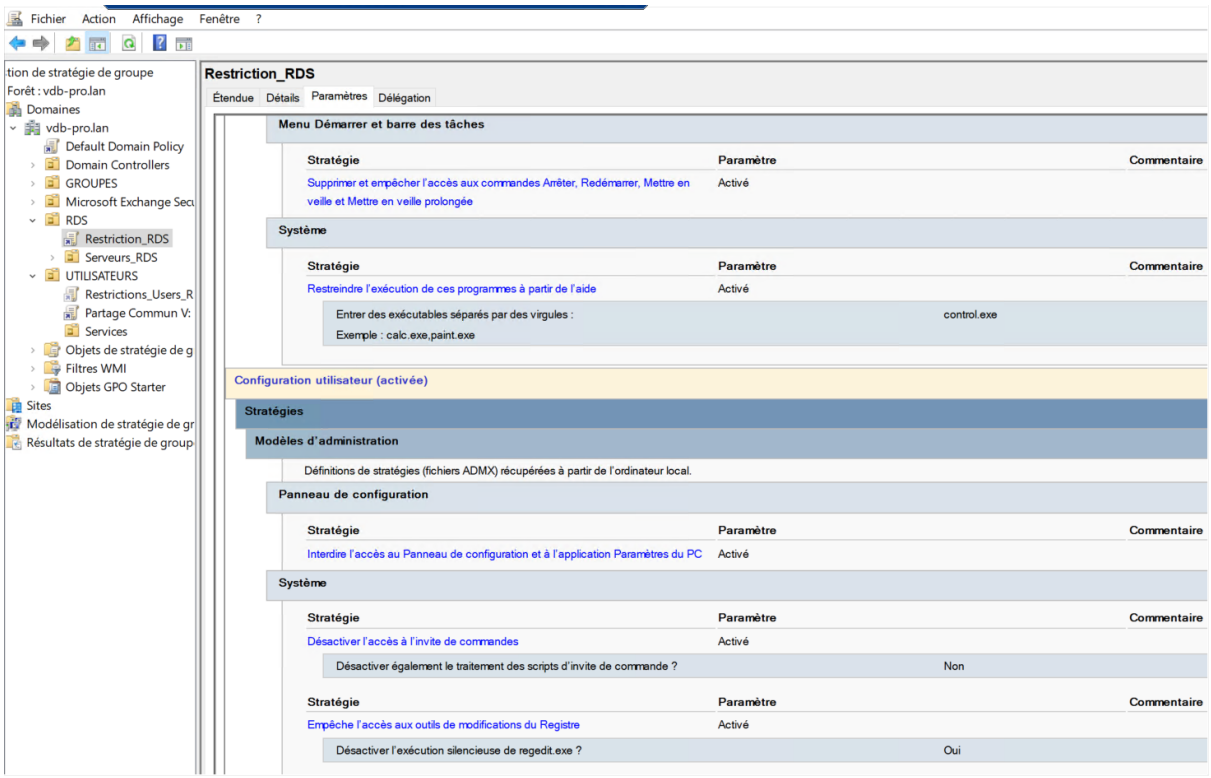
Configuration de GPO pour restreindre

Afin de renforcer la sécurité et de maîtriser l'environnement utilisateur sur les sessions distantes, j'ai mis en place un ensemble de restrictions à l'aide des stratégies de groupe (GPO). Ces GPO ont été appliquées spécifiquement aux utilisateurs de la collection RDS, via une unité d'organisation (OU) dédiée dans l'Active Directory.

Les restrictions mises en œuvre avaient pour objectif de limiter les fonctionnalités disponibles au sein de la session RDS, afin de garantir une utilisation conforme aux besoins de l'entreprise vdb-pro tout en réduisant les risques de mauvaise manipulation ou d'accès non autorisé à certaines fonctions du système.

Parmi les paramètres restreints via GPO, on peut citer :

- La désactivation de l'accès au panneau de configuration et aux paramètres système,
- La désactivation de l'accès au modificateur de registre,
- La désactivaiton de l'accès au terminal,
- La désactivation de l'installation de périphériques ou de logiciels,
- Le blocage de la commande Exécuter, de l'accès au gestionnaire des tâches et à certaines touches du clavier (Ctrl+Alt+Suppr, etc.),
- La redirection de certains dossiers vers des lecteurs réseau (ex : Bureau, Documents),



Cette configuration GPO contribue à créer un espace de travail distant stable, cohérent et sécurisé, adapté à une utilisation en entreprise. Elle permet également de réduire la charge de support technique en limitant les possibilités de modification du système par les utilisateurs.

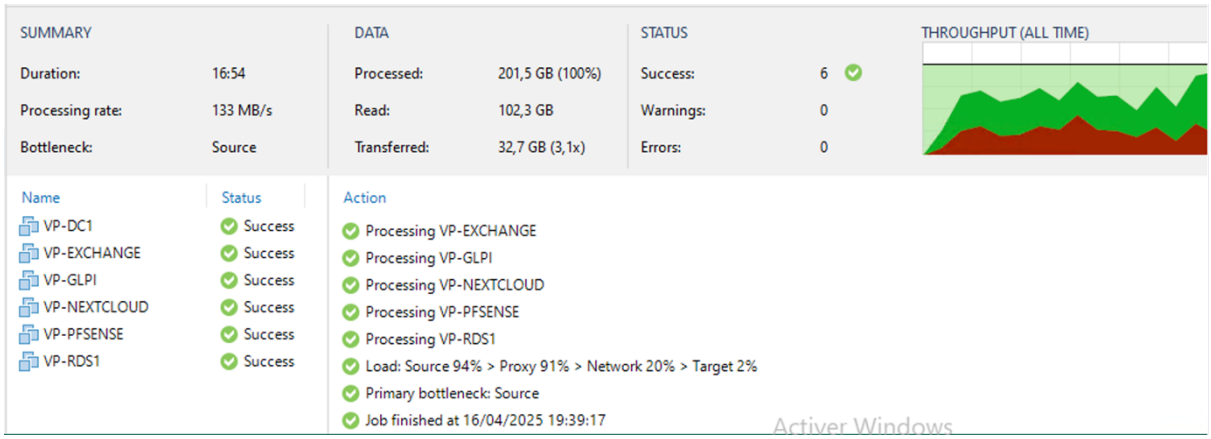
Gérer le patrimoine informatique

La mise en place de l'environnement RDS au sein de vdb-pro, une attention particulière a été portée à la gestion différenciée des droits d'accès entre les utilisateurs standards et les administrateurs système. Pour cela, j'ai configuré des stratégies de groupe (GPO) de manière ciblée, en appliquant des restrictions uniquement aux utilisateurs finaux, tout en laissant les administrateurs avec un accès complet à l'environnement distant.

Concrètement, les GPO restrictives (suppression du panneau de configuration, blocage de la commande Exécuter, désactivation du gestionnaire des tâches, etc.) sont liées à une unité d'organisation (OU) spécifique dans laquelle seuls les comptes utilisateurs standards sont placés. Les comptes d'administration, quant à eux, sont conservés en dehors de cette OU ou sont explicitement exclus de l'application des GPO via des filtres de sécurité et la fonctionnalité de filtrage par groupe de sécurité intégrée à Active Directory.

Cette approche permet de garantir une sécurité renforcée pour les utilisateurs, tout en maintenant la souplesse d'administration nécessaire pour les techniciens et les responsables informatiques, notamment lors des phases de maintenance, de supervision ou de dépannage sur les sessions RDS.

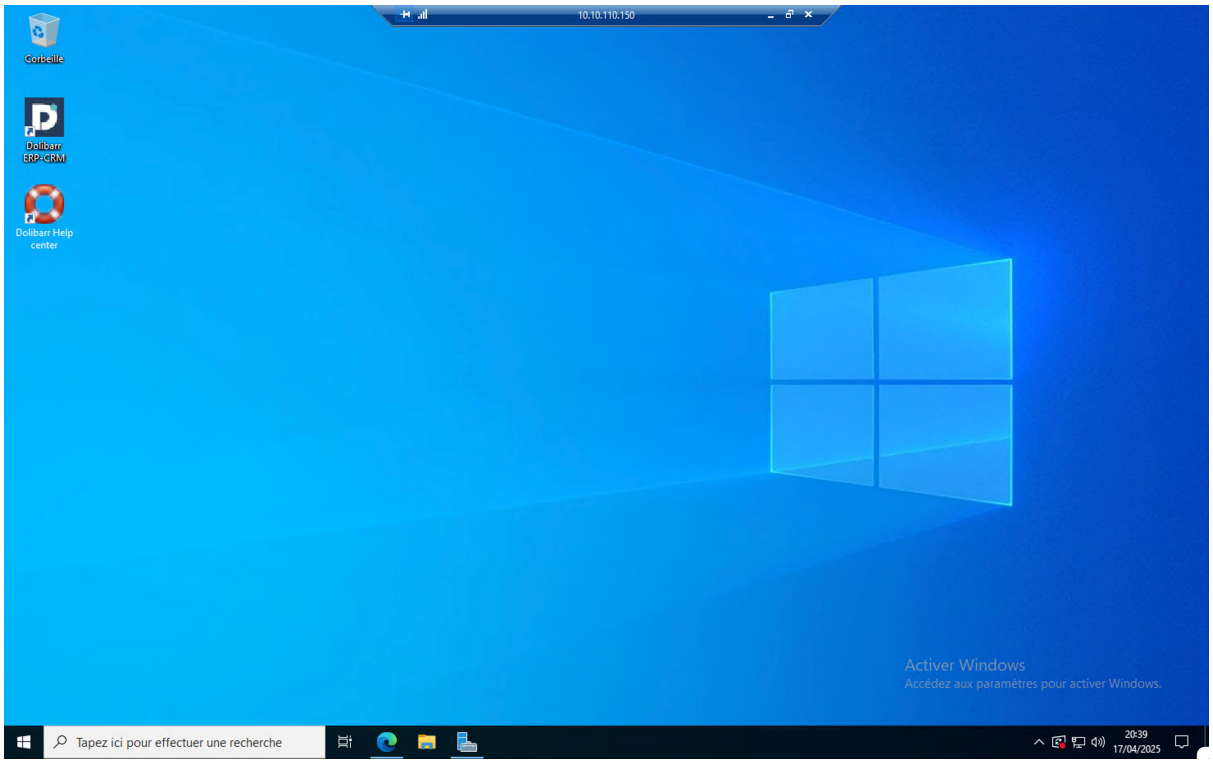
De plus, afin de garantir la pérennité des données et de pouvoir restaurer rapidement le service en cas d'incident, j'ai intégré le serveur RDS à un job de sauvegarde quotidien. Cette sauvegarde est planifiée via la solution de sauvegarde de l'entreprise VEEAM. Cette stratégie s'inscrit dans une politique de continuité de service et de gestion des risques liée à l'infrastructure.



Partie 2 – Validation

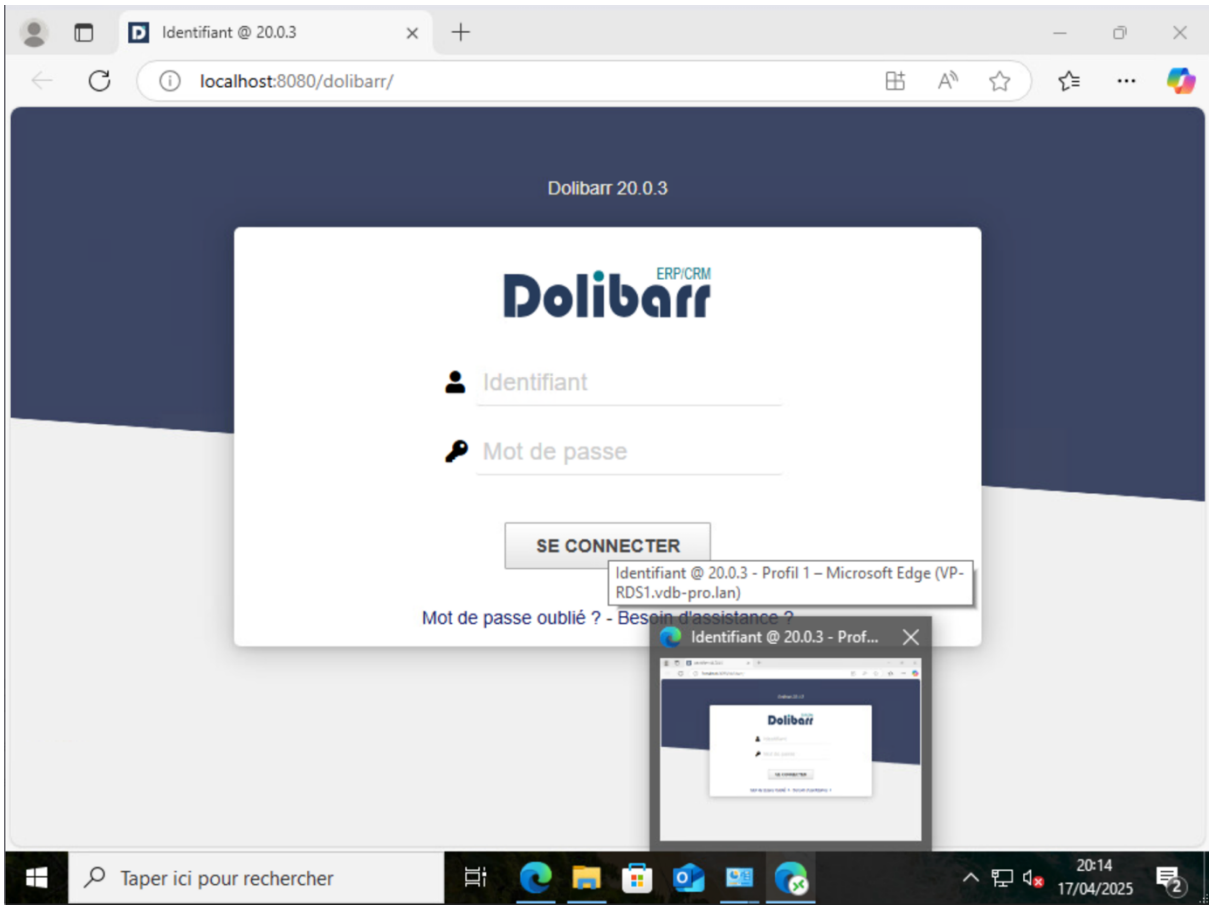
Pour valider le bon fonctionnement de l'installation et de la configuration du serveur RDS, j'ai réalisé une phase de tests fonctionnels à l'aide d'un compte utilisateur créé à mon nom dans l'Active Directory. Ce test a été réalisé depuis un poste client situé sur le VLAN 20 (LAN_CLIENTS), afin de simuler une connexion utilisateur réelle dans les conditions prévues par l'architecture réseau de l'entreprise vdb-pro.

Lors de la connexion à la session distante, j'ai pu vérifier que l'accès au bureau à distance était opérationnel, et que l'environnement chargé correspondait bien aux paramètres définis dans la collection de sessions RDS. J'ai également contrôlé que les stratégies de groupe (GPO) appliquées à l'unité d'organisation de l'utilisateur étaient bien effectives : restrictions d'accès, suppression de fonctionnalités système, redirections éventuelles, etc.

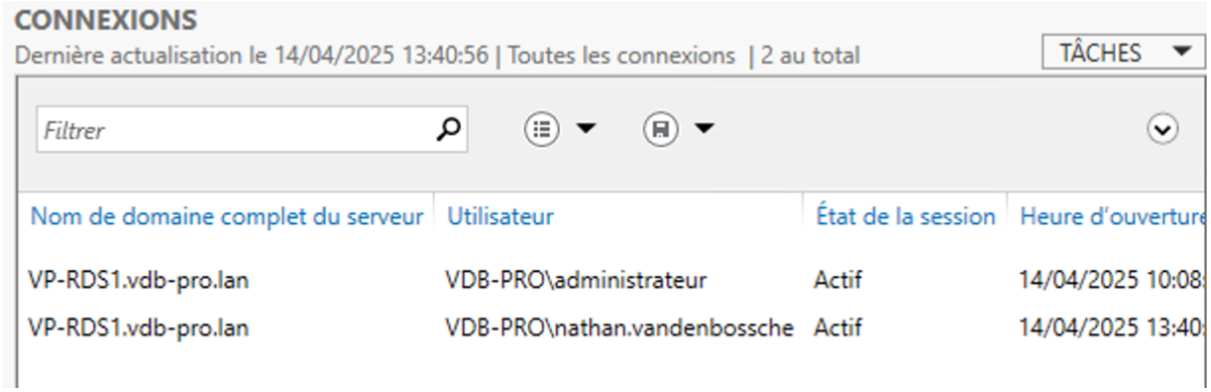


Le logiciel **Dolibarr ERP**, que j'ai installé sur le serveur, est également disponible via l'interface **RemoteApp Web**. Les utilisateurs autorisés peuvent ainsi **télécharger le fichier** .RDP **généré automatiquement**, puis l'exécuter depuis leur poste local. Une fois lancé, l'application **s'ouvre directement dans une session distante**, tout en donnant l'impression qu'elle est utilisée localement.

Dolibarr fonctionne en mode client/serveur, et l'ensemble des données saisies sont **synchronisées en temps réel avec la base de données hébergée sur le serveur RDS1**, garantissant **centralisation, sécurité et accessibilité** des informations métiers.



Enfin, depuis le serveur VP-RDS1, j'ai utilisé les outils d'administration RDS pour surveiller en temps réel la session de l'utilisateur connecté. Cela m'a permis de confirmer que l'utilisateur était bien enregistré comme actif sur le serveur, que sa session avait été correctement initiée, et qu'aucune erreur n'était présente dans les journaux d'événements liés à la connexion.



Ces vérifications m'ont permis de valider la conformité de la solution déployée, tant sur le plan fonctionnel que sur le plan de la sécurité et de la gestion centralisée.

Partie 3 – Veille Technologique

Dans le cadre de cette réalisation, j'ai également mené une veille technologique afin de m'informer sur les alternatives aux services Remote Desktop Services (RDS) de Microsoft, les évolutions possibles de l'infrastructure, ainsi que les bonnes pratiques en matière de sécurité informatique.

Organiser son développement professionnel

Environnement d'apprentissage personnel

Mon environnement d'apprentissage personnel est clairement défini : je travaille principalement sur une infrastructure virtualisée via VMware ESXi, ce qui me permet de simuler des environnements professionnels. Cela comprend des machines virtuelles Windows Server, des postes clients, des VLANs configurés, et des services comme Active Directory, DNS, RDS, etc. Cet environnement me permet de tester, apprendre de mes erreurs et développer mes compétences techniques en autonomie.

Mise en œuvre d'une veille technologique

Ma veille est régulière et structurée. Elle a pour objectif :

- de repérer les technologies émergentes dans les domaines des systèmes, réseaux et de la cybersécurité (par exemple : solutions cloud, alternatives à RDS comme Citrix, ou innovations en MFA),
- d'utiliser des moyens fiables et variés de recherche, tels que Feedly, les blogs officiels Microsoft, CERT-FR, ZDNet, GitHub ou encore des forums techniques spécialisés,
- et de renforcer mes compétences sur des sujets techniques spécifiques ou en lien avec la sécurité des systèmes d'information.

Alternatives à RDS

Parmi les solutions concurrentes à Microsoft RDS, Citrix Virtual Apps and Desktops se démarque comme une alternative robuste et performante. Elle propose des fonctionnalités avancées comme :

- Une meilleure gestion des ressources avec le protocole HDX, plus optimisé que RDP,
- Une expérience utilisateur plus fluide, notamment pour les applications graphiques ou en cas de faible bande passante,
- Des capacités d'intégration cloud plus poussées (Azure, AWS),
- Un niveau de granularité plus élevé dans la gestion des accès et des ressources.

Cependant, cette solution est plus complexe à déployer et nécessite une licence payante généralement plus onéreuse que celle de Microsoft RDS.

Améliorations possibles

À court ou moyen terme, plusieurs pistes d'évolution peuvent être envisagées pour faire monter en puissance l'infrastructure :

- Mise en place d'un serveur de licences RDS pour une gestion conforme des accès,
- Déploiement de RemoteApp, pour publier uniquement certaines applications sans donner accès au bureau complet,
- Implémentation d'un broker de connexion pour permettre la tolérance de panne et le rééquilibrage de charge en environnement multi-RDS,
- Intégration d'une solution de supervision (type Centreon ou Zabbix) pour surveiller les performances et les connexions.
- L'implémentation de solutions de double authentification (MFA) pour renforcer l'accès distant,

Veille sécurité

Du point de vue de la sécurité, la veille porte sur :

- Les vulnérabilités RDP recensées dans la base CVE (Common Vulnerabilities and Exposures),
- L'utilisation du chiffrement TLS et la désactivation des anciennes versions du protocole RDP (RDP 5.0 et antérieurs),
- La segmentation réseau renforcée et la journalisation des accès via un SIEM (Security Information and Event Management).

BTS Services informatiques aux organisations - SISR
Session 2025

E5 – Support et mise à disposition de services informatiques
Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :
Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- **Layer Bureautique et Informatique** est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro.
- La problématique principale réside dans le besoin pour l'entreprise d'avoir un outil centralisé permettant à la fois de gérer efficacement son parc informatique, d'assurer la traçabilité des équipements et d'optimiser la gestion des incidents. De plus, un système de tickets est nécessaire pour traiter les demandes internes des utilisateurs, qu'elles concernent des pannes, des demandes d'assistance ou des améliorations.
- La solution choisie consiste à déployer un serveur GLPI, une plateforme de gestion de parc et de tickets qui offre des fonctionnalités étendues pour suivre l'inventaire des équipements, gérer les interventions et garantir un service de support efficace. Ce système permettra également de centraliser l'historique des demandes des utilisateurs et de faciliter la communication entre les administrateurs et les utilisateurs finaux.

Intitulé de la réalisation professionnelle

Déploiement d'une Solution de Ticketing GLPI

Période de réalisation : 21/04/2025 - 23/04/25 **Lieu :** AUXERRE
Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE
- REPONDRE AUX INCIDENTS ET AUX DEMANDES D'ASSISTANCE ET D'EVOLUTION

Conditions de réalisation

- **Ressources disponibles (Situation avant RP)**
  L'infrastructure de départ comprend un serveur ESXi opérationnel pour l'hébergement de machines virtuelles, ainsi qu'un contrôleur de domaine Active Directory déjà en place, incluant un service DNS fonctionnel. D'autres services réseau de base (DHCP, VLANs, pare-feu) sont également configurés pour permettre le bon déroulement de la réalisation.
- **Résultats attendus (Situation après RP)**
  La solution déployée doit permettre la création et le suivi de tickets utilisateurs en cas d'incidents, ainsi que la gestion complète du parc informatique avec un inventaire précis des équipements. L'ensemble doit être pleinement opérationnel à l'issue de la réalisation.
- **Durée de réalisation**
  Cela a pris 3 jours, incluant installation de GLPI, configuration et sécurisation des utilisateurs et des droits ainsi que les phases de test.

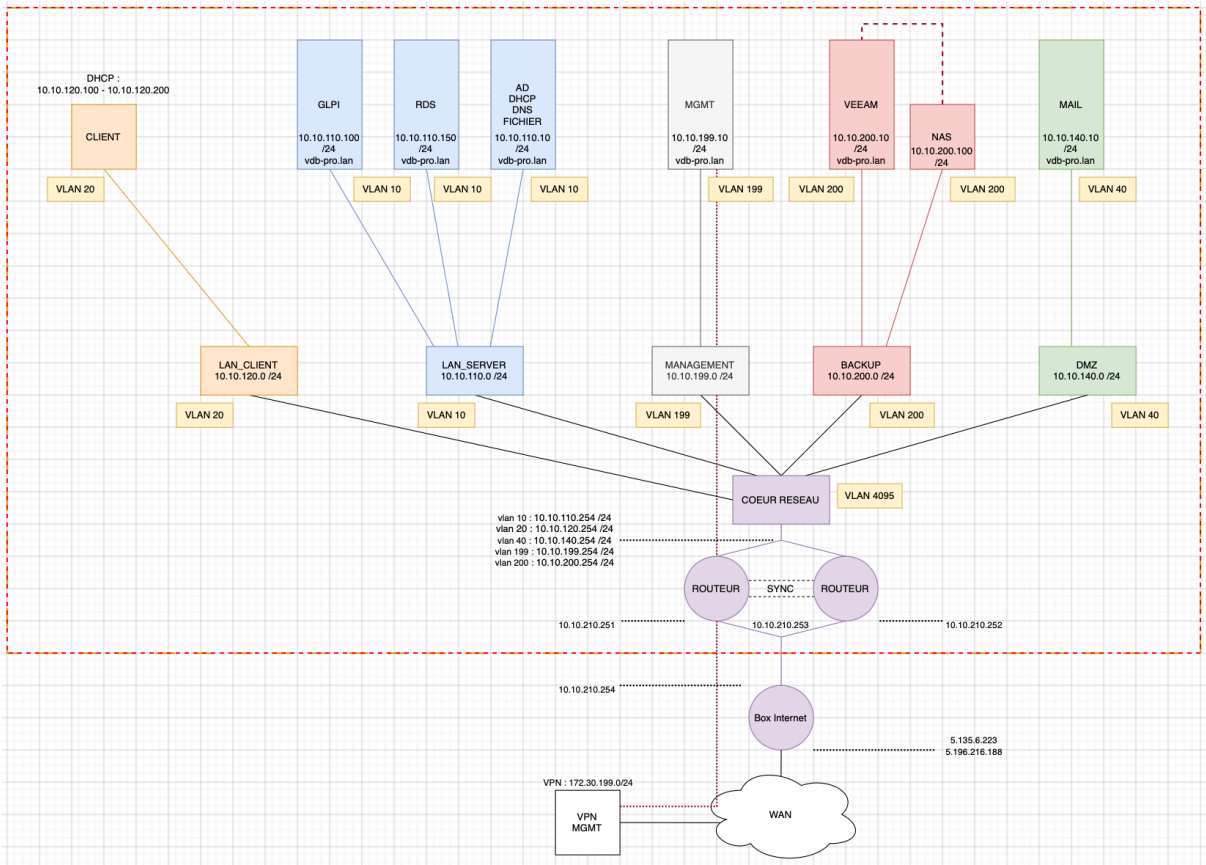
Modalités d'accès à cette réalisation professionnelle.

https://portfolio.vdb-pro.fr mdp : *Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

Dans le cadre de ma mission, j'ai réalisé une réalisation professionnelle pour le client vdb-pro, dont l'objectif était de mettre en place une solution complète de gestion de parc informatique et de ticketing.

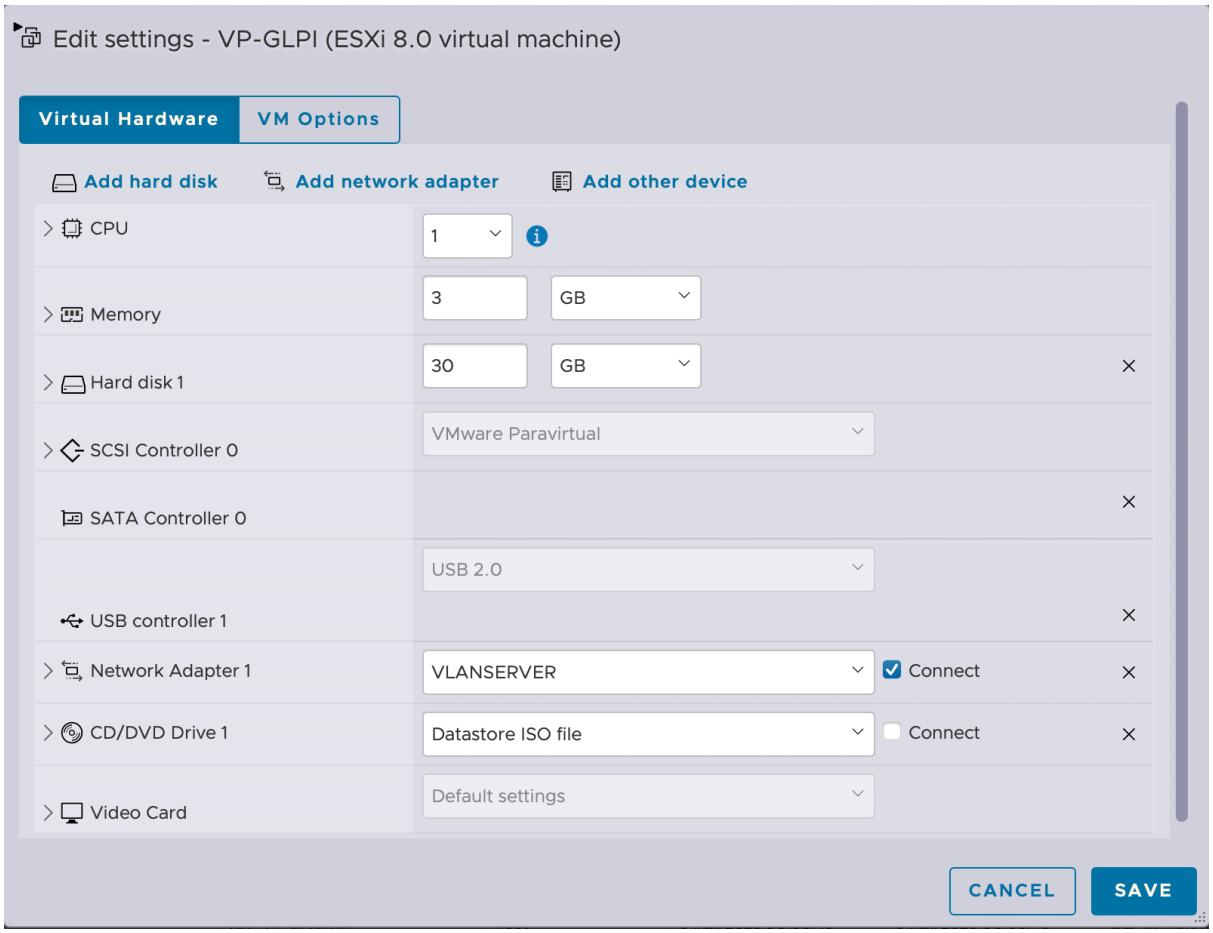
Pour cela, j'ai procédé au déploiement d'un serveur Debian sur lequel j'ai installé le logiciel GLPI. Cette solution permet à l'entreprise de recenser et suivre l'ensemble de son parc informatique, mais également de centraliser les demandes internes via un système de tickets. Les utilisateurs peuvent ainsi déclarer des incidents ou des besoins, et les administrateurs système et réseau peuvent y répondre efficacement, en assurant un suivi clair jusqu'à la résolution.



Creation de la machine virtuelle

La première étape a consisté à créer une machine virtuelle sur l'hyperviseur VMware ESXi de l'entreprise. Celle-ci est basée sur une distribution Debian 12, à laquelle j'ai attribué les ressources suivantes : 30 Go de stockage et 3 Go de mémoire vive, afin de garantir une bonne réactivité du site web proposé par le logiciel GLPI, même en cas de connexions simultanées.

La machine a été intégrée au VLAN SERVER, conformément à l'architecture réseau déjà en place au sein de l'entreprise.



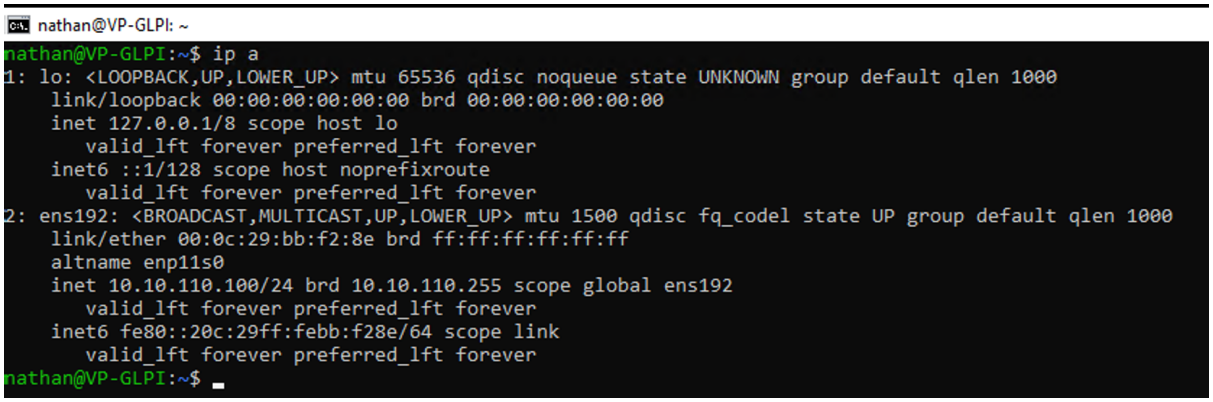
Configunratio de Debian 12

Une fois la machine virtuelle créée, j'ai procédé à l'installation de Debian 12. Ce système servira de base pour l'installation des différents services nécessaires au bon fonctionnement de GLPI.

L'objectif est de mettre en place une pile LAMP (Linux, Apache, MariaDB, PHP), qui constitue l'environnement requis pour faire tourner GLPI. Dès l'installation terminée, j'ai également configuré les paramètres réseau de la machine afin qu'elle soit accessible au sein du VLAN SERVER et puisse communiquer avec le reste de l'infrastructure.

Accès à distance via SSH

Pour faciliter les configurations ultérieures, j'ai également installé et activé le service **SSH** sur le serveur. Cela me permet de **prendre le contrôle à distance** de la machine depuis le poste de management, rendant les opérations de configuration et de maintenance plus pratiques et efficaces.



Installation de la pile LAMP (Linux, Apache, MariaDB, PHP)

Une fois Debian installée et le réseau configuré, j'ai procédé à l'installation des composants nécessaires à la mise en place de GLPI. Il s'agit de la pile LAMP, composée de Linux, Apache, MariaDB et PHP, ainsi que des modules PHP indispensables au bon fonctionnement de l'application.

Pour commencer, j'ai installé tous les paquets nécessaires à l'aide de la commande suivante :

```
apt-get install apache2 mariadb-server php php-mysql php-curl php-gd php-json php-ldap
php-mbstring php-xml php-zip
```

1. Apache

Le serveur web Apache2 est utilisé pour héberger l'interface web de GLPI. Une fois installé, le service a été démarré et activé pour se lancer automatiquement au démarrage du système :

```
systemctl start apache2
systemctl enable apache2
```

2. MariaDB

J'ai ensuite installé MariaDB, qui servira à stocker toutes les données utilisées par GLPI. Après le lancement du service, j'ai créé une base de données dédiée ainsi qu'un utilisateur avec les droits appropriés :

```
CREATE DATABASE db25_glpi;
CREATE USER 'glpi_adm'@'localhost' IDENTIFIED BY '************';
GRANT ALL PRIVILEGES ON db25_glpi.* TO 'glpi_adm'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Remarque : Le mot de passe de l'utilisateur GLPI a été personnalisé et sécurisé.

3. PHP

Enfin, PHP et les modules nécessaires à GLPI (tels que php-mysql, php-xml, php-curl, etc.) ont été installés pour garantir la compatibilité et le bon fonctionnement du logiciel.

Une fois tous ces éléments installés et configurés, l'environnement LAMP était complet et prêt à accueillir l'installation de GLPI.

Installation du logiciel GLPI

L'installation de GLPI s'effectue à partir d'un dépôt en ligne officiel fourni par l'éditeur du logiciel. J'utilise l'outil wgetpour télécharger l'archive de la dernière version stable disponible.

```
wget https://github.com/glpi-project/glpi/releases/download/10.0.10/glpi-10.0.10.tgz
```

Une fois l'archive téléchargée, je la décompresse dans le répertoire d'hébergement web d'Apache :

```
tar -zxvf glpi-10.0.10.tgz -C /var/www/glpi/public
```

Ensuite, j'attribue les droits d'accès nécessaires afin que le serveur web puisse lire et exécuter les fichiers de GLPI. Pour cela, j'utilise les commandes suivantes :

```
chown -R www-data:www-data /var/www/glpi/public
chmod -R 755 /var/www/glpi/public
```

Ces permissions permettent à l'utilisateur Apache (www-data) d'avoir le contrôle sur le dossier GLPI, tout en assurant une sécurité minimale au niveau des droits d'accès.

Création du certificat auto-signé

Activer le module SSL d'Apache

```
a2enmod ssl
```

Pour permettre le chiffrement des échanges entre les utilisateurs et le serveur, j'ai utilisé le module OpenSSL afin de générer un certificat auto-signé. Ce certificat est utilisé à titre temporaire, dans le cadre des phases de test et de mise en place de l'environnement.

Il sera par la suite remplacé par un certificat officiel émis par Let's Encrypt, garantissant une meilleure fiabilité et reconnaissance par les navigateurs.

Configuration d'un hôte virtuel Apache pour GLPI

Configuration d'un hôte virtuel sur le port 443

Pour rendre GLPI accessible via le navigateur, je crée un fichier de configuration Apache spécifique à l'aide de l'éditeur de texte nano :

```
nano /etc/apache2/sites-available/glpi.conf
```

Dans ce fichier, je définis un hôte virtuel écoutant sur le port 443. Le contenu du fichier glpi.conf est le suivant :

```
<VirtualHost *:443>
        ServerName supportglpi.vdb-pro.lan
        DocumentRoot /var/www/glpi/public

# If you want to place GLPI in a subfolder of your site (e.g. your virtual host is serving multiple applications),
# you can use an Alias directive. If you do this, the DocumentRoot directive MUST NOT target the GLPI directory itself.
# Alias "/glpi" "/var/www/glpi/public"

        <Directory /var/www/glpi/public>
                Require all granted
                RewriteEngine On
                # Redirect all requests to GLPI router, unless file exists.
                RewriteCond %{REQUEST_FILENAME} !-f
                RewriteRule ^(.*)$ index.php [QSA,L]
        </Directory>
        SSLEngine on
        SSLCertificateFile /etc/ssl/certs/glpi-cert.pem
        SSLCertificateKeyFile /etc/ssl/private/glpi-key.pem

        <FilesMatch \.php$>
        SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"
        </FilesMatch>
</VirtualHost>
```

Une fois ce fichier configuré, je l'active à l'aide des commandes suivantes :

```
a2ensite glpi.conf
systemctl reload apache2
```

Cette étape permet de rendre l'interface GLPI accessible via un navigateur à l'adresse IP du serveur, en spécifiant le port 443.

Configuration d'un hôte virtuel sur le port 80

Afin d'assurer une connexion sécurisée à l'interface de GLPI, j'ai mis en place une redirection automatique du port 80 (HTTP) vers le port 443 (HTTPS). Pour cela, j'ai créé un deuxième hôte virtuel dans Apache, dédié uniquement à cette redirection.

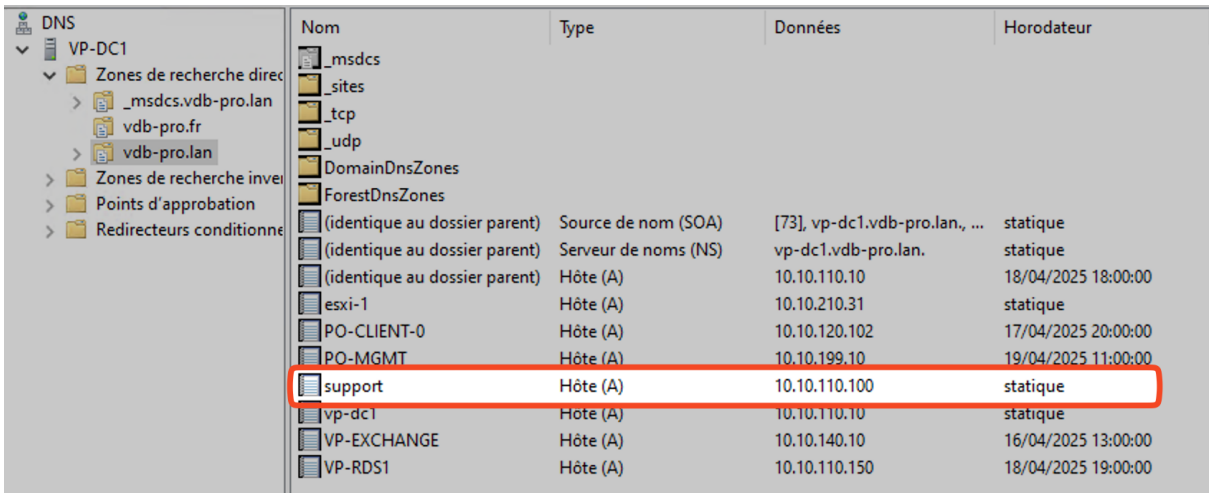
```
<VirtualHost *:80>
   ServerName support.vdb-pro.lan
   Redirect permanent / https://support.vdb-pro.lan/
</VirtualHost>
```

Cette configuration permet de **forcer toutes les connexions HTTP vers la version HTTPS** du site, garantissant ainsi que les échanges entre l'utilisateur et le serveur soient toujours chiffrés.

Ajout d'une entrée DNS sur le serveur de noms

Sur le serveur DNS interne, qui est également le contrôleur de domaine Active Directory, j'ajoute un enregistrement de type A correspondant au nom support.vdb-pro.lan. Cet enregistrement permet aux utilisateurs du réseau local d'accéder à l'interface GLPI via un nom de domaine convivial, plutôt que par une adresse IP.

Dans le cadre d'un futur accès externe, une entrée DNS publique devra également être créée avec le même nom de domaine, pointant vers l'adresse IP publique du serveur GLPI. Cela assurera l'accessibilité du service depuis l'extérieur du réseau de l'entreprise.



Configuration de GLPI par le site Web

À partir de cette étape, **l'ensemble de la configuration est réalisé directement via l'interface web de GLPI**, accessible à l'adresse suivante : https://support.vdb-pro.lan

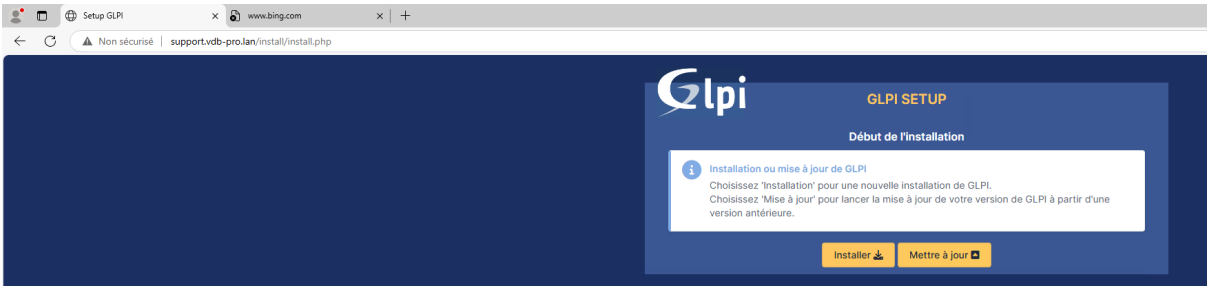
Cette interface permet de finaliser l'installation du logiciel, de le connecter à la base de données, puis de configurer les différents éléments liés à son usage, tels que :

- La création des comptes utilisateurs et administrateurs
- La configuration du parc informatique (matériel, logiciels, etc.)
- La mise en place du système de gestion des tickets

Étapes initiales :

Je me rends sur l'adresse du site nouvellement mis en place : https://support.vdb-pro.lan

L'assistant d'installation de GLPI s'ouvre automatiquement. Je sélectionne l'option **"Installer"** pour lancer la procédure.

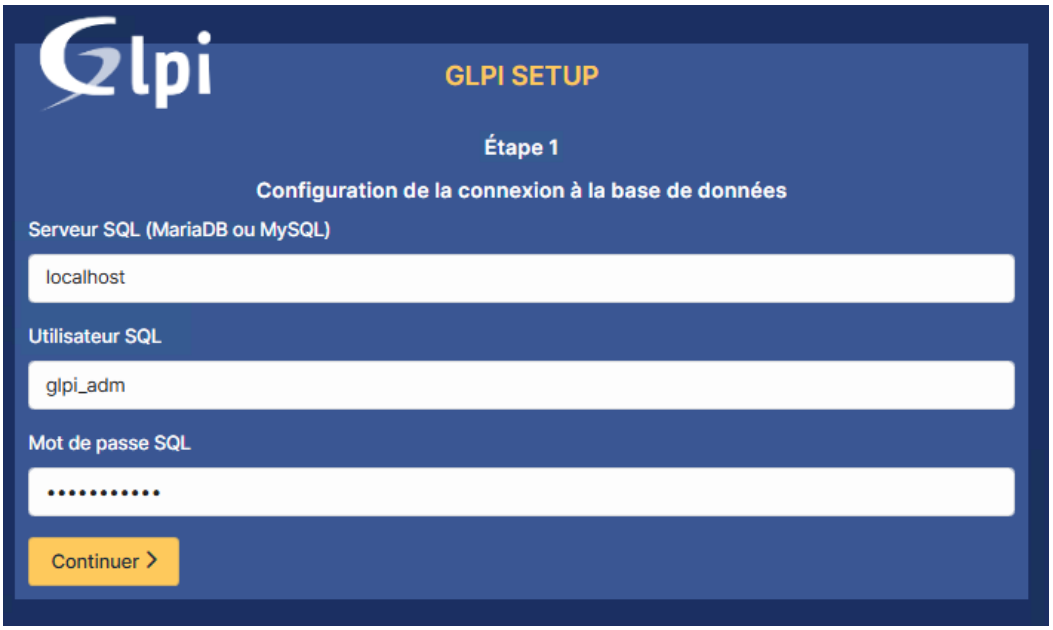


GLPI procède alors à une **vérification des prérequis** nécessaires à son bon fonctionnement (version PHP, extensions, droits sur les dossiers, etc.). Si tout est conforme, je clique sur **"Continuer"** pour passer à l'étape suivante.

Une fois les prérequis validés, l'étape suivante consiste à configurer l'accès à la base de données. Étant donné que le serveur GLPI héberge également la base de données MariaDB, l'adresse à renseigner est simplement localhost.

Je saisis ensuite les identifiants de l'utilisateur de la base de données créés précédemment :

- Utilisateur : glpi_adm / Mot de passe : [mot de passe défini lors de la création]



Si les droits ont été correctement attribués à cet utilisateur, la liste des bases de données disponibles apparaîtra automatiquement. Il suffira alors de sélectionner la base db25_glpi.

Si aucune base ne s'affiche, il est nécessaire de vérifier les privilèges SQL de l'utilisateur, ainsi que la connectivité à la base.

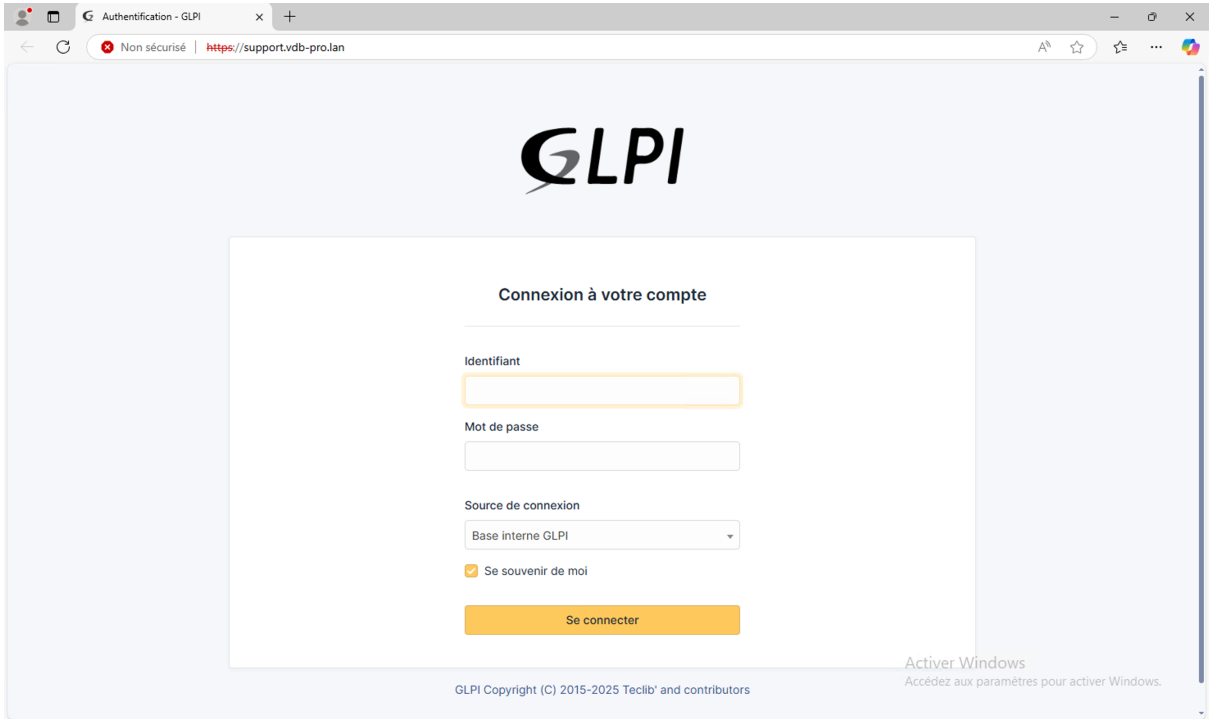
Une fois cette étape validée, un message de confirmation s'affiche indiquant que la connexion à la base de données a été correctement établie.

Connexion initiale à l'interface GLPI

L'installation étant maintenant terminée, je suis redirigé vers la page de connexion de GLPI. Les identifiants par défaut sont :

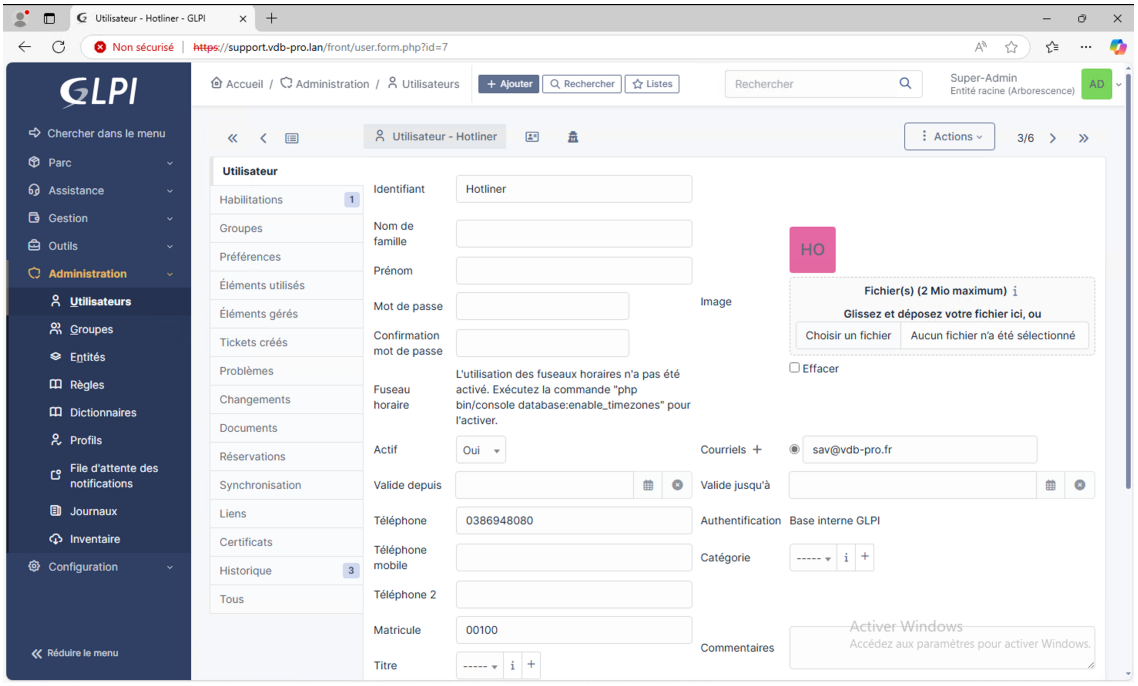
- Nom d'utilisateur : glpi
- Mot de passe : glpi

Il est fortement recommandé de modifier ces identifiants immédiatement après la première connexion, afin de sécuriser l'accès à l'interface d'administration.

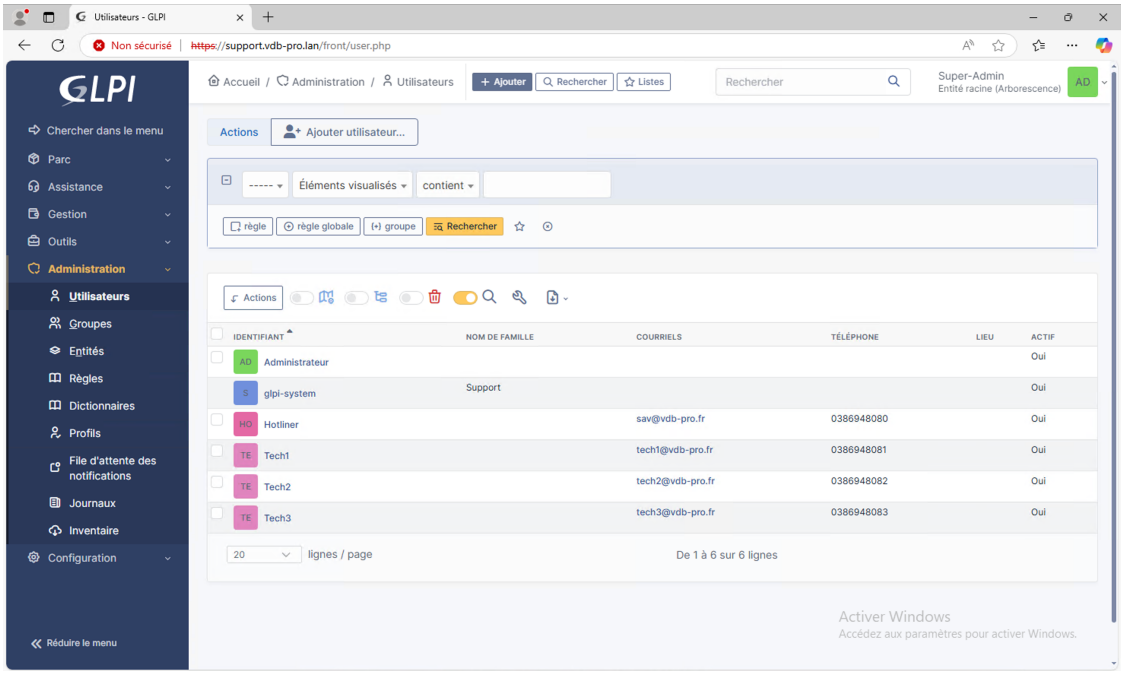


Création des utilisateurs

Depuis le menu **« Administration » > « Utilisateurs »**, il est possible d'ajouter et de gérer les différents comptes selon leur rôle dans l'organisation, Technicien ou Hotliner. Le rôle Hotliner a pour mission de **créer les tickets d'incidents** à la suite des demandes formulées par les utilisateurs finaux (par téléphone, mail ou en direct). Le Hotliner assure également **le suivi initial** du traitement des tickets.

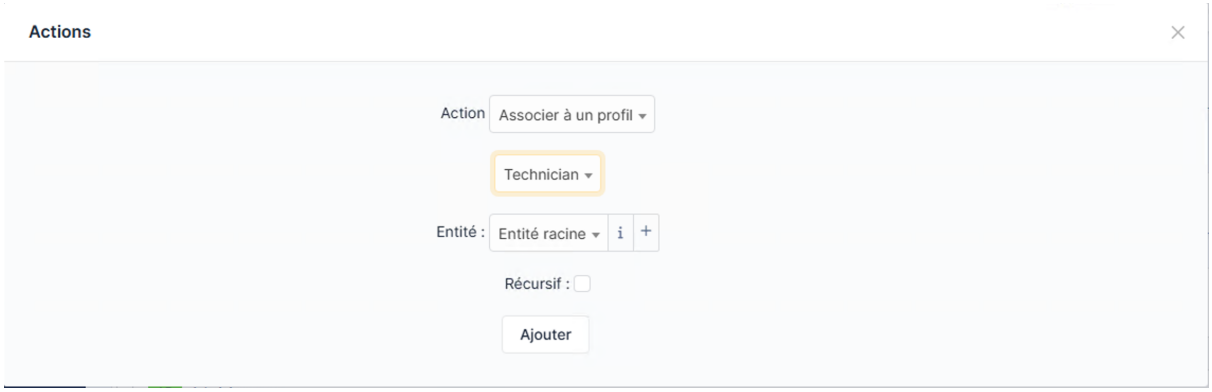


Le rôle technicien a pour responsabilité de **prendre en charge, diagnostiquer, résoudre et clôturer** les tickets ouverts par le Hotliner. Ils disposent de droits étendus sur les modules de traitement des demandes, la gestion des interventions et la communication avec les utilisateurs.



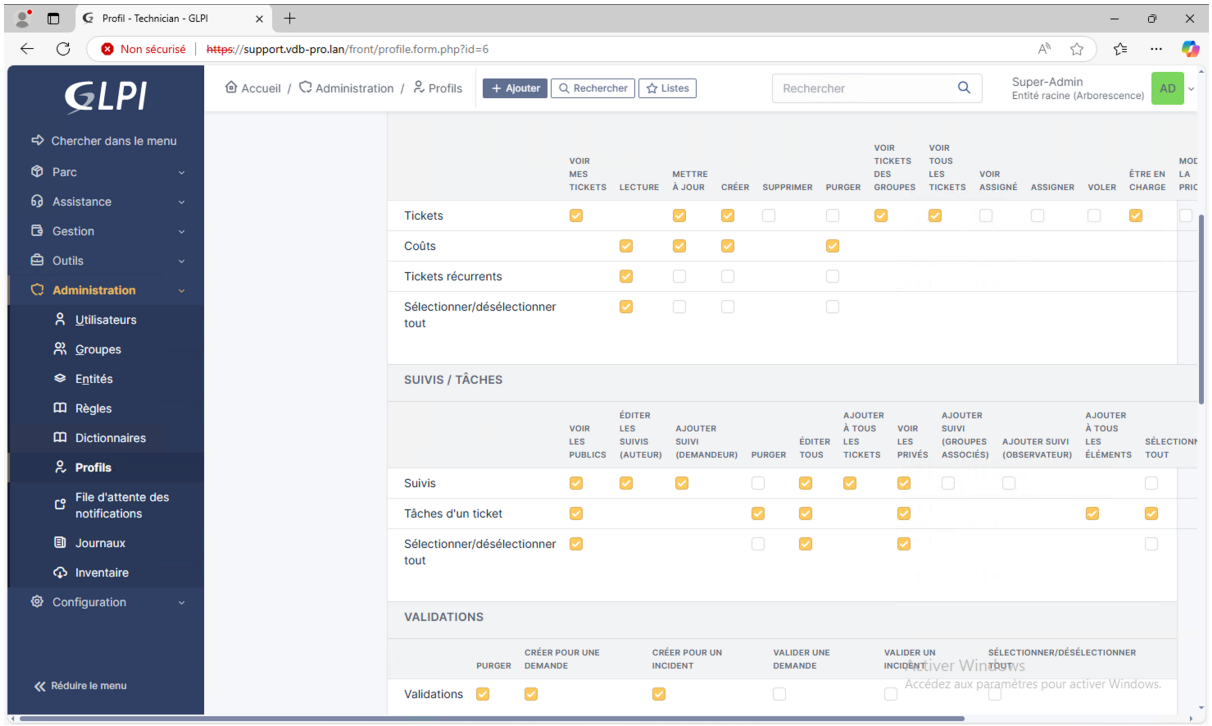
Attribution des droits et profils

Chaque utilisateur se voit attribuer un profil correspondant à son rôle dans le système de gestion GLPI. Les droits sont gérés via des profils prédéfinis qui facilitent l'attribution rapide et homogène des permissions.



- Profil Hotliner :
  Accès limité à la création, au suivi des tickets et à la consultation de base. L'utilisateur ne peut ni attribuer ni clôturer un ticket.
- Profil Technicien :
  Dispose de droits élargis : il peut modifier l'état, assigner, traiter et clôturer les tickets. Il peut également accéder à la base de connaissances et à certains éléments du parc.

Les profils sont créés et gérés depuis le menu « Administration » > « Profils ». Cela permet de créer de véritables modèles de rôles (templates) applicables à plusieurs utilisateurs, garantissant une cohérence dans la gestion des permissions.



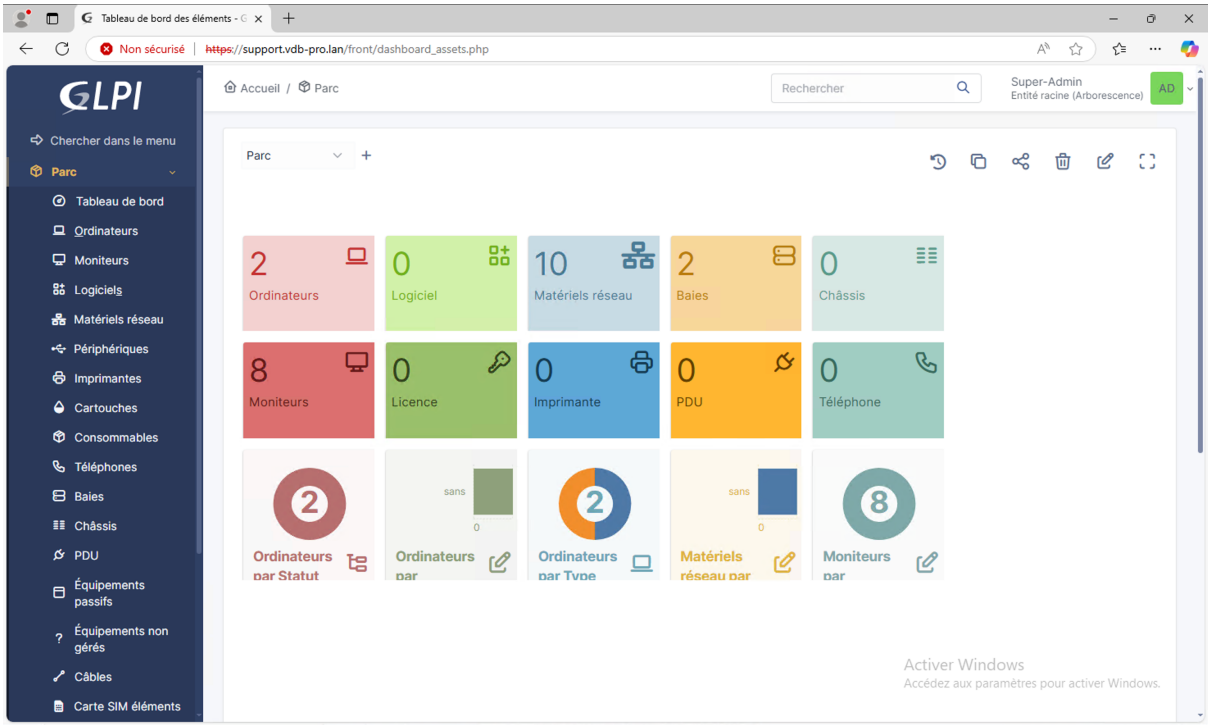
Gestion du parc informatique

GLPI offre une interface complète pour l'organisation et le suivi du parc informatique de l'entreprise. Depuis l'onglet « Parc », un tableau de bord centralise l'ensemble des équipements enregistrés dans le système.

Parmi les fonctionnalités proposées, on retrouve :

- L'ajout d'équipements : ordinateurs, imprimantes, équipements réseau, moniteurs, périphériques, etc.
- Un inventaire détaillé de chaque élément (numéro de série, marque, modèle, emplacement, état, garantie…).
- Le rattachement des équipements à un utilisateur, à une entité ou à un ticket spécifique, ce qui permet un meilleur suivi des interventions.

Il est également possible de naviguer par catégories (comme "Moniteurs", "Ordinateurs", ou "Réseau") pour filtrer et visualiser plus précisément les types d'équipements gérés.



Quelques fonctionnalités clés de GLPI

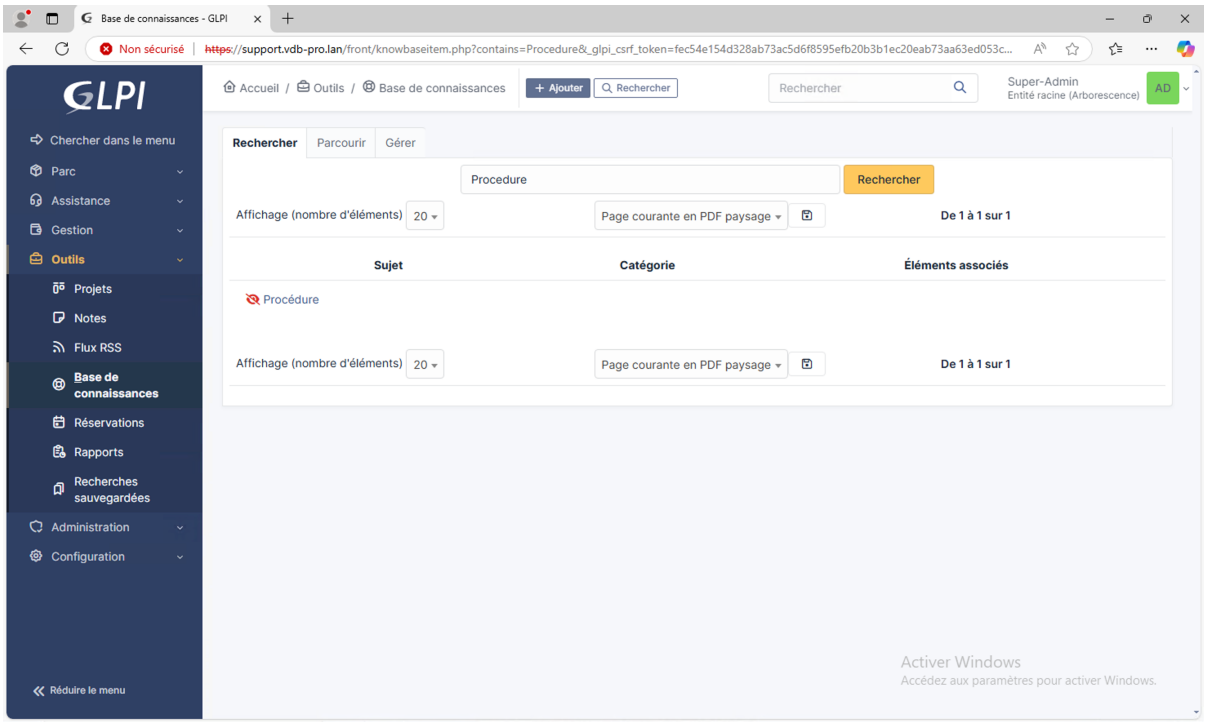
GLPI intègre plusieurs fonctionnalités avancées qui facilitent la gestion informatique au quotidien. Parmi les plus utiles :

- Planification des interventions :
  Il est possible de créer un planning avec des affectations d'interventions par technicien, avec dates, durées et statuts.
- Suivi d'activité et statistiques :
  Des tableaux de bord et rapports sont disponibles pour visualiser le nombre de tickets traités, les délais de résolution, ou encore les équipements les plus sollicités.
- Base de connaissances :
  Permet de centraliser des procédures internes, des tutoriels, des retours d'expérience ou des solutions à des problèmes récurrents.

Très utile en cas de turn-over, pour former de nouveaux techniciens, ou tout simplement pour archiver des résolutions et y accéder rapidement.

Cette base doit être gérée exclusivement par un administrateur afin d'éviter les doublons ou l'ajout de contenus inutiles.

Elle peut être liée directement aux tickets, notamment dans les résolutions : lorsqu'un problème est résolu, un compte rendu clair peut être enregistré pour servir de référence à d'autres techniciens.

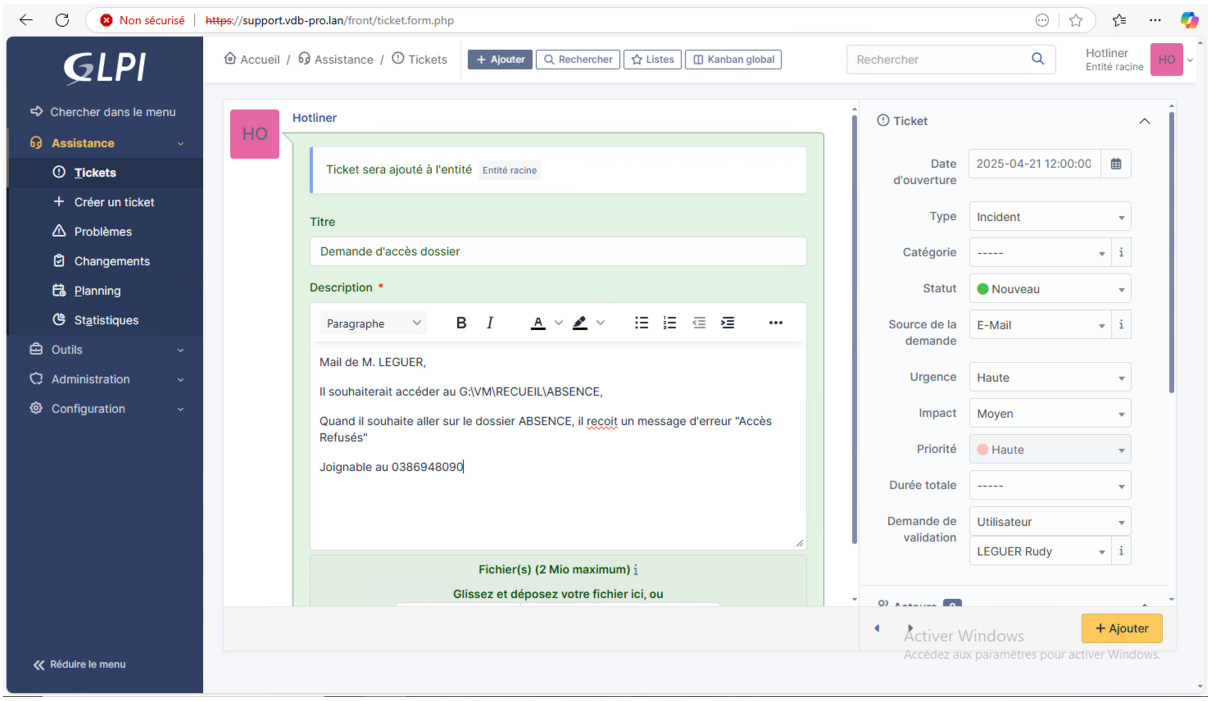


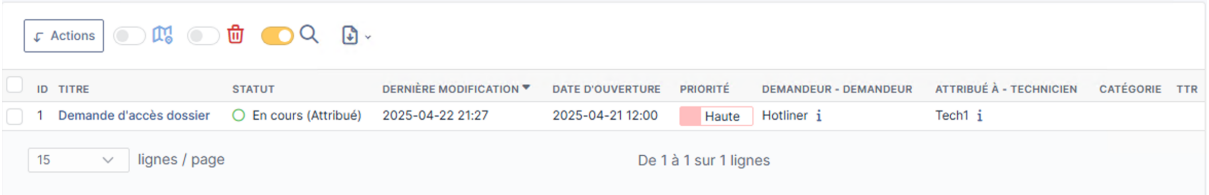
Partie 2 : Validation de la solution

Simulation de la gestion d'un ticket

Création d'un ticket :

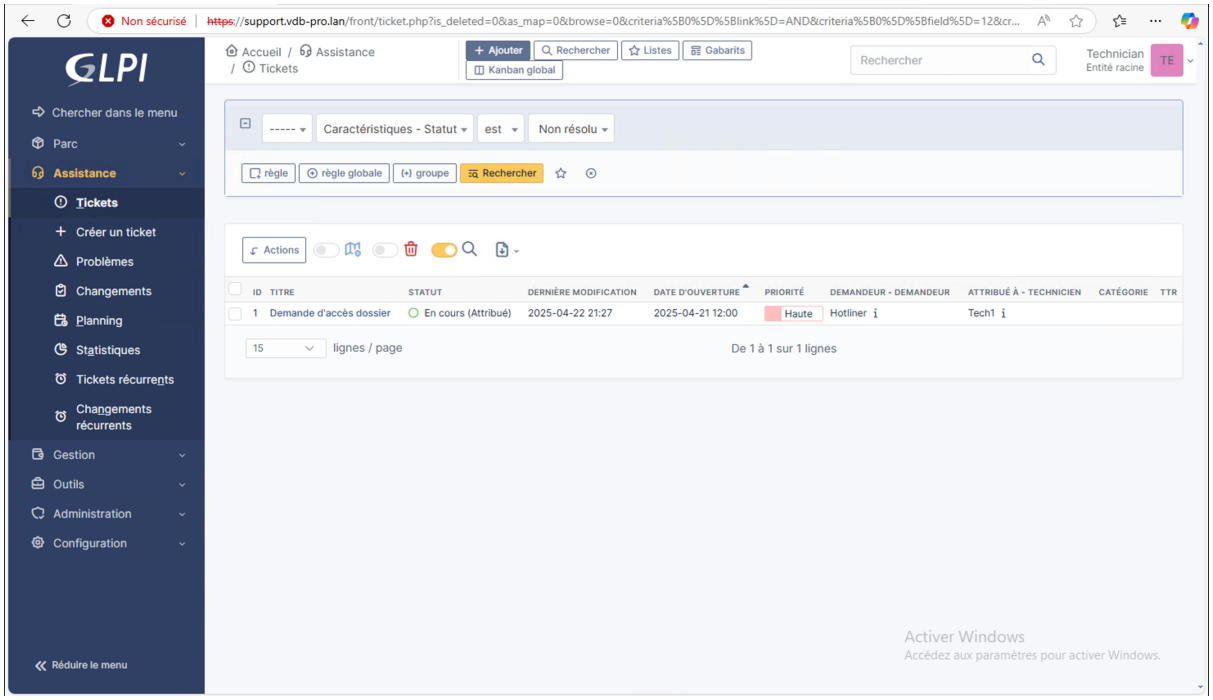
L'utilisateur **Hotliner** procède à la création d'un nouveau ticket dans GLPI, par exemple pour signaler un problème d'accès au réseau. Lors de la saisie, le formulaire permet d'apporter un grand niveau de détail : une description complète de l'incident peut être rédigée, accompagnée d'informations sur l'utilisateur concerné, la date et l'heure de création, le niveau de priorité, le délai estimé de traitement, ainsi que la personne ou le groupe chargé de résoudre le problème. Cette approche permet de structurer efficacement la demande dès sa création, facilitant ainsi la prise en charge rapide par les techniciens et assurant un meilleur suivi tout au long du cycle de vie du ticket.

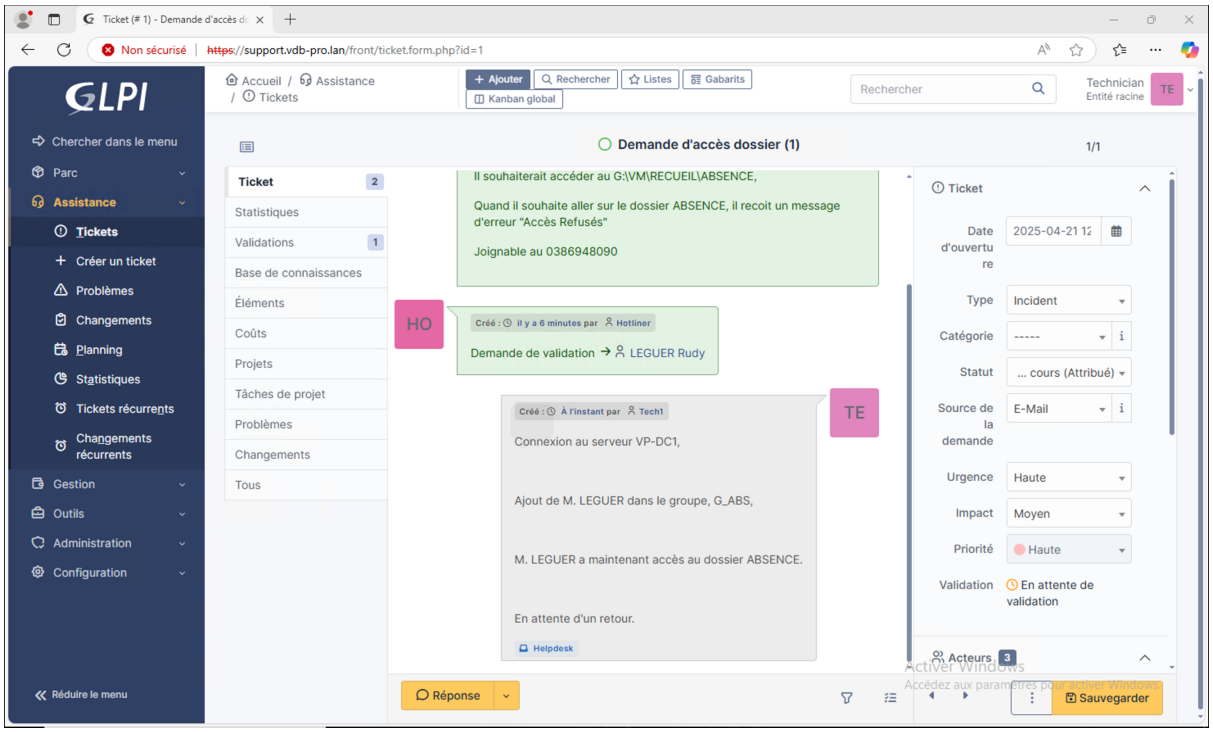




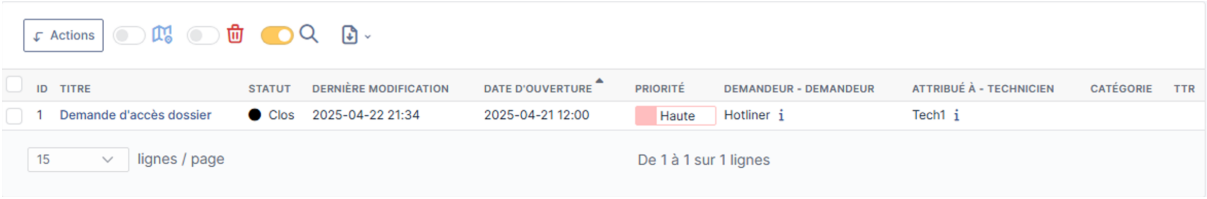
Prise en charge et résolution :

Le technicien « Tech1 » prend en charge le ticket attribué. Dès la prise en main, il renseigne un diagnostic détaillé, puis effectue les actions nécessaires pour résoudre le problème signalé. Une fois la solution appliquée, il complète le ticket avec un compte rendu d'intervention, permettant de tracer précisément ce qui a été réalisé.





Le ticket peut ensuite être clôturé, soit par le technicien lui-même une fois la résolution confirmée, soit par l'utilisateur final après validation de la solution apportée. Ce processus garantit un suivi complet et transparent de chaque intervention.



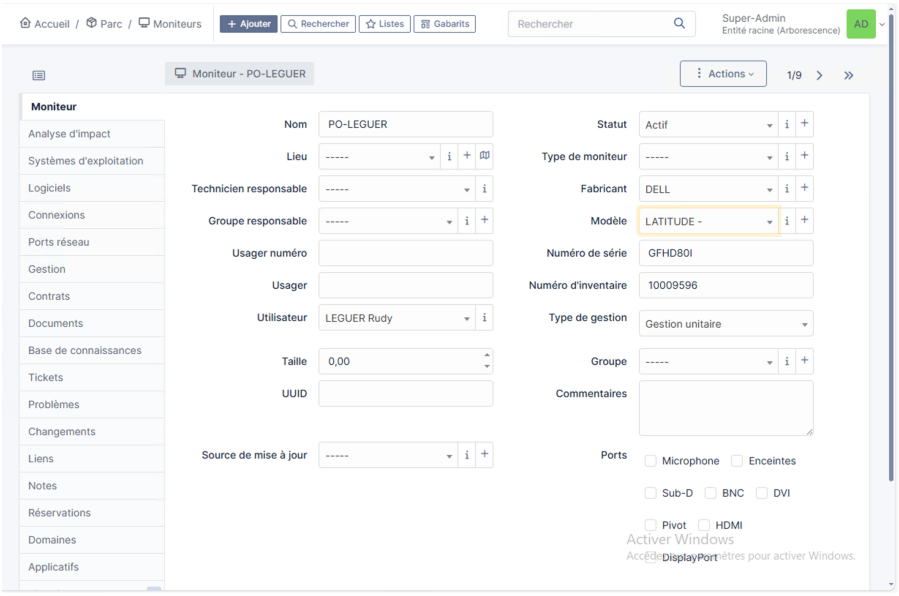
Cette étape finale permet de valider le bon déroulement du processus de gestion des incidents dans GLPI. Depuis la création du ticket par le Hotliner, en passant par sa prise en charge, son diagnostic, la mise en œuvre d'une solution par le technicien, jusqu'à sa clôture, l'ensemble du workflow a pu être testé et confirmé comme fonctionnel. Cette simulation démontre ainsi l'efficacité et la cohérence du circuit de traitement des demandes dans l'outil.

Gestion du parc informatique

GLPI permet également de gérer efficacement les équipements de l'entreprise. Pour illustrer cette fonctionnalité, un **équipement réseau** a été ajouté manuellement dans le parc.

Depuis l'onglet **« Parc »**, il suffit de sélectionner la catégorie souhaitée (dans ce cas, "Équipements réseau") puis de cliquer sur **« Ajouter »**. Un formulaire s'ouvre permettant de renseigner des informations précises sur l'équipement : **nom, type, marque, numéro de série, adresse IP, localisation physique, date d'achat, garantie**, etc.

L'équipement peut ensuite être **rattaché à un utilisateur**, à un site ou encore à un ticket spécifique, ce qui permet un suivi précis de son historique et des interventions associées.



Grâce à cette centralisation, l'inventaire est toujours à jour, et les informations sont facilement accessibles pour l'équipe technique.

Partie 3 : Veille technologique

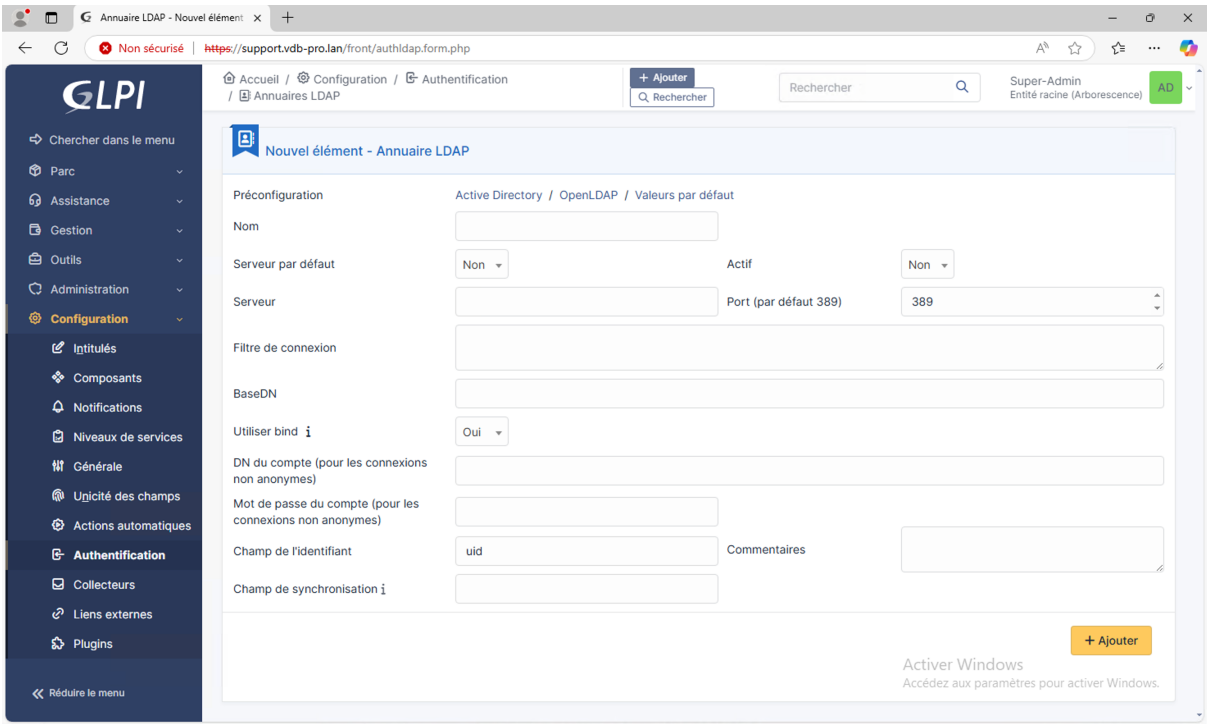
Dans le cadre de ce projet, une veille technologique a été réalisée afin d'explorer des axes d'amélioration et d'anticiper les évolutions possibles de la solution. Un premier point a porté sur l'intégration d'un annuaire LDAP, permettant une **authentification centralisée** des utilisateurs. Cette approche offrirait un gain de temps considérable en synchronisant automatiquement les comptes présents dans l'Active Directory avec GLPI, tout en renforçant la cohérence des accès.

En parallèle, plusieurs **alternatives à GLPI** ont été brièvement étudiées, notamment *OTRS*, *iTop* et *Freshservice*, afin de comparer les fonctionnalités, les modèles d'hébergement (cloud ou local), et la facilité d'intégration dans une infrastructure existante.

Enfin, un volet **cybersécurité** a été pris en compte : mise en place d'un certificat SSL auto-signé pour les tests, sécurisation des accès via HTTPS, gestion des rôles et permissions strictement définis selon les profils utilisateurs. Ces réflexions permettent d'assurer une solution à la fois efficace, évolutive et sécurisée, en adéquation avec les besoins actuels et futurs de l'entreprise.

Intégration de l'annuaire LDAP

L'intégration d'un annuaire LDAP (comme Active Directory) permet de centraliser la gestion des comptes utilisateurs. Les utilisateurs peuvent alors se connecter à GLPI avec leurs identifiants réseau, et les droits peuvent être synchronisés automatiquement.



Alternatives à GLPI

Une veille technologique a été réalisée afin d'explorer différentes solutions de gestion de parc et de tickets. Parmi les outils analysés, **OCS Inventory NG**, souvent couplé à GLPI, permet une gestion automatique des inventaires matériels et est particulièrement efficace dans un environnement avec de nombreux équipements. **iTop** se distingue par sa conformité ITIL, offrant des fonctionnalités robustes pour la gestion de services, mais avec une interface plus complexe. **Freshservice**, une solution Cloud moderne, est idéale pour les entreprises recherchant une interface intuitive et une intégration SaaS, tandis que **Spiceworks Helpdesk** se montre attractif grâce à son modèle gratuit, bien que limité sur l'évolutivité et la gestion d'inventaire. Chaque outil offre des avantages spécifiques selon les besoins de l'entreprise, que ce soit en termes d'intégration, d'interface ou de mode de déploiement.

Cybersécurité GLPI

Du point de vue **cybersécurité**, plusieurs actions ont été entreprises pour assurer la sécurité de l'infrastructure GLPI. La communication entre le serveur GLPI et ses utilisateurs a été sécurisée par un certificat SSL, d'abord auto-signé pour les tests, mais qui pourra être remplacé par un certificat officiel de **Let's Encrypt**. L'utilisation de HTTPS a permis de garantir le chiffrement des données échangées. De plus, une attention particulière a été portée à la gestion des **rôles et permissions** au sein de GLPI, afin de restreindre l'accès aux données sensibles en fonction des profils utilisateurs. La mise en place de telles mesures sécuritaires est essentielle pour protéger les données confidentielles de l'entreprise et garantir l'intégrité du système.

BTS Services informatiques aux organisations- SISR

Session 2025

E5 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :

Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- **Layer Bureautique et Informatique** est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro.
- La problématique principale réside dans besoin crucial d'une solution de sauvegarde fiable pour protéger ses données critiques et garantir la continuité de service. Sans cette protection, le risque de perte de données et d'interruption de service serait trop élevé.
- La solution choisie consiste à déployer un serveur Veeam Backup & Replication, configuré pour effectuer des sauvegardes automatiques. Les données seront stockées sur un NAS externe, offrant ainsi une sécurité renforcée et une gestion simplifiée des sauvegardes.

Intitulé de la réalisation professionnelle

Déploiement d'une Solution Backup VEEAM

Période de réalisation : 15/04/25- 17/04/25 **Lieu :** AUXERRE

Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE
- GERER LE PATRIMOINE INFORMATIQUE

Conditions de réalisation

- **Ressources disponibles (Situation avant RP)**
  L'infrastructure de départ comprend un serveur ESXi opérationnel pour l'hébergement de machines virtuelles, ainsi qu'un contrôleur de domaine Active Directory déjà en place, incluant un service DNS fonctionnel. D'autres services réseau de base (DHCP, VLANs, pare-feu) sont également configurés pour permettre le bon déroulement de la réalisation.
- **Résultats attendus (Situation après RP)**
  Un serveur Veeam sera installé et configuré pour exécuter des sauvegardes régulières des machines virtuelles. Les données seront sauvegardées sur un NAS externe, assurant une meilleure sécurité et une capacité de restauration rapide en cas de besoin. L'infrastructure bénéficiera ainsi d'un système de sauvegarde automatisé et fiable.
- **Durée de réalisation**
  Cela a pris 3 jours, incluant installation, configuration, sécurisation et phase de test.

Modalités d'accès à cette réalisation professionnelle.

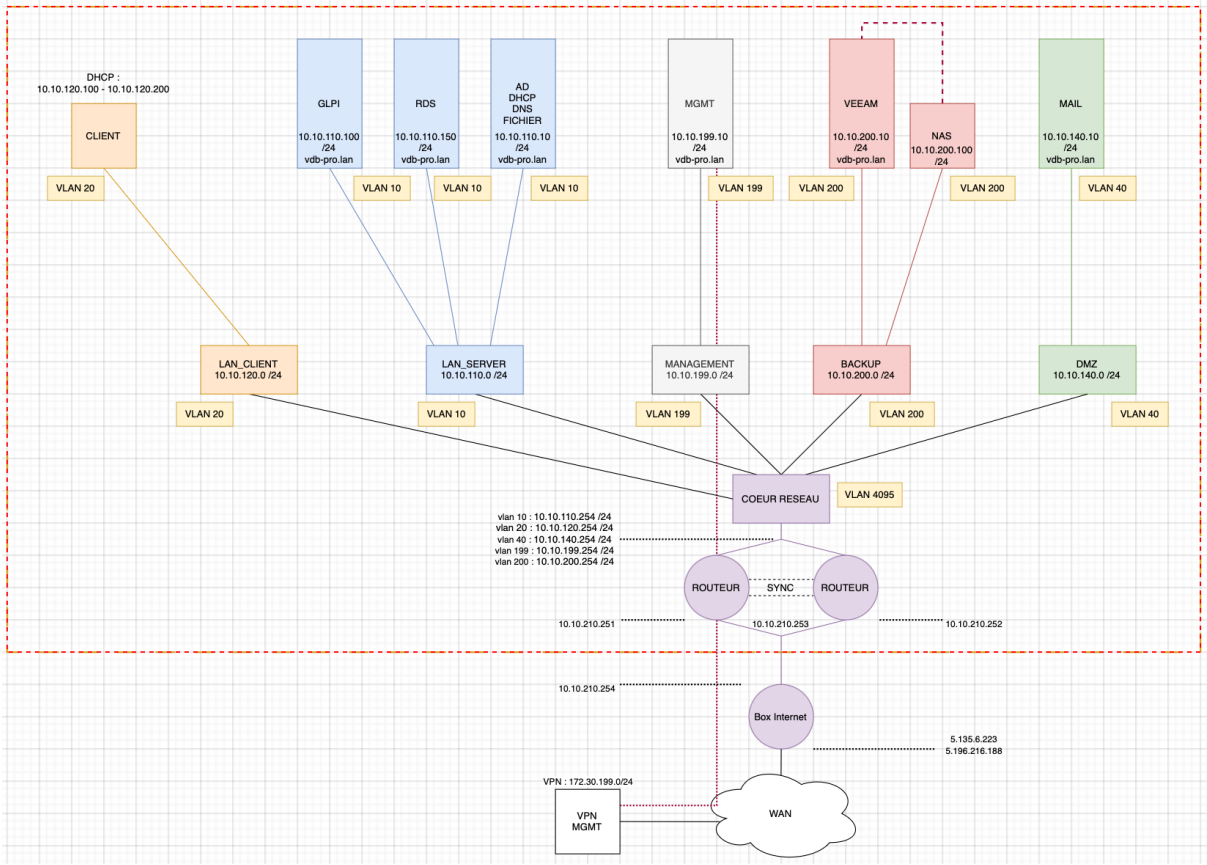
https://portfolio.vdb-pro.fr mdp : *Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

Dans le cadre de ma mission, j'ai réalisé un projet professionnel pour le client vdb-pro visant à mettre en place une solution complète de **sauvegarde d'infrastructure virtuelle**.

Pour cela, j'ai déployé un serveur de sauvegarde basé sur **Veeam Backup & Replication**, couplé à un stockage réseau (NAS) virtualisé sous **TrueNAS**. Ce projet m'a permis de développer des compétences en virtualisation, administration système, sécurité des données et gestion des ressources réseau.

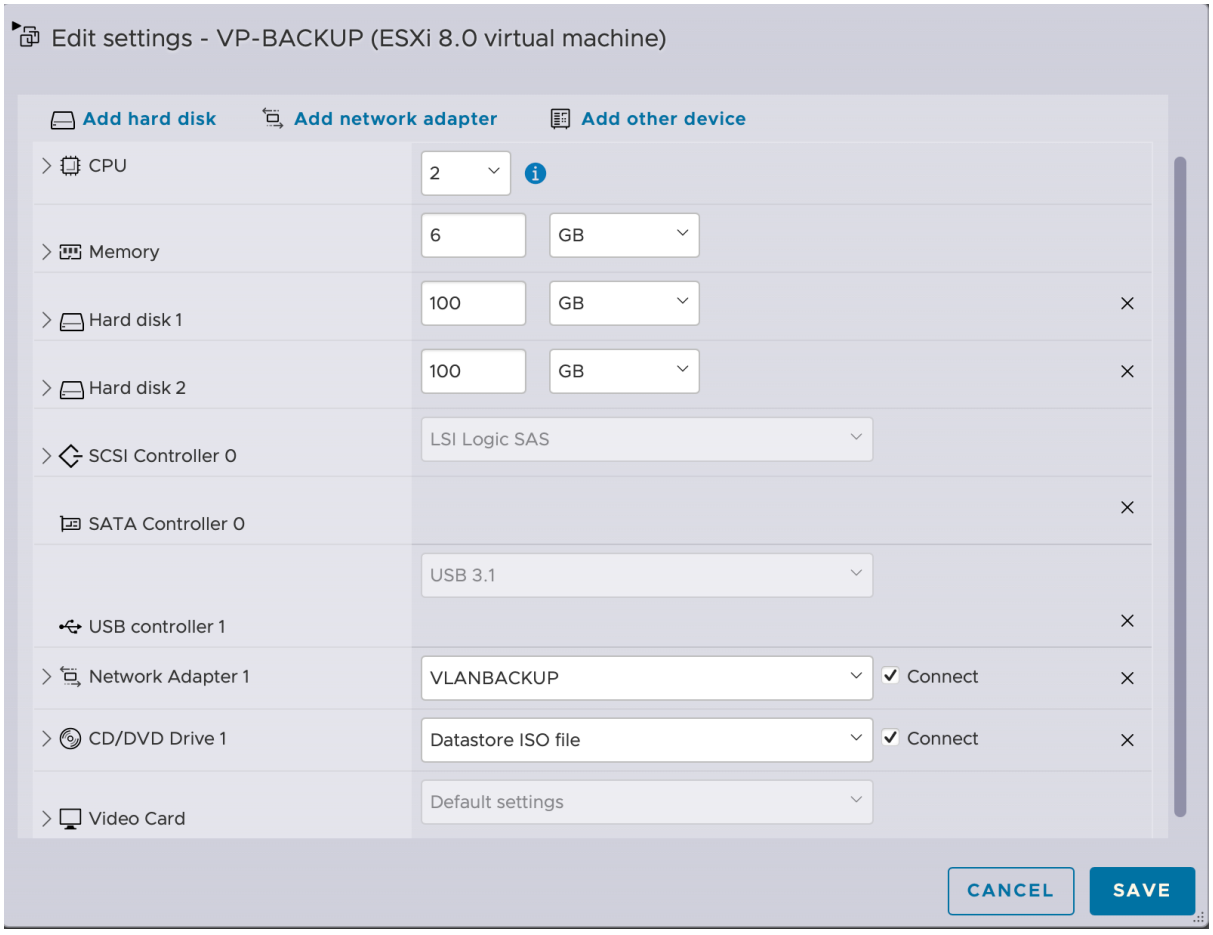
Dans une logique d'optimisation et d'ouverture technologique, une **veille** a également été réalisée afin d'identifier les alternatives existantes et les tendances actuelles du secteur.



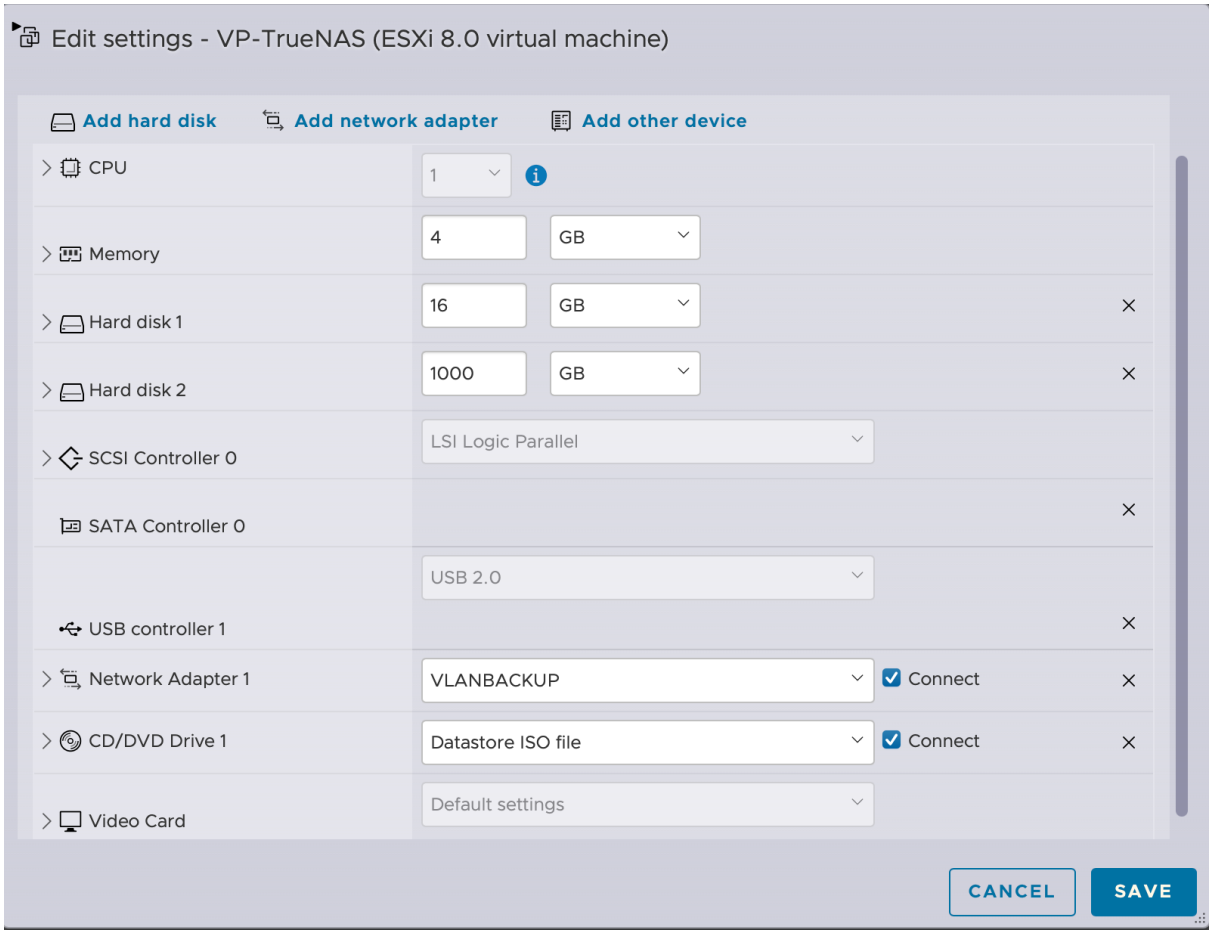
Création des machines virtuelles

Pour héberger le service de sauvegarde, une machine virtuelle dédiée a été créée sur le serveur ESXi. Cette VM est configurée avec un système d'exploitation Windows Server, une allocation de ressources adaptée (RAM, CPU, stockage) et intégrée au réseau existant. Elle constitue la base du futur serveur Veeam. Cette étape permet de préparer un environnement isolé et maîtrisé pour héberger la solution.

Dans un premier temps, je procède à la création d'une machine virtuelle dédiée à l'infrastructure de sauvegarde. Celle-ci est configurée avec 2 vCPU, 10 Go de mémoire vive, ainsi que deux disques durs virtuels de 100 Go chacun. Le premier disque est alloué au système d'exploitation, tandis que le second est réservé aux sauvegardes ponctuelles, notamment pour la conservation de fichiers de configuration ou d'autres données critiques.



Par la suite, je mets en place une seconde machine virtuelle, destinée à héberger un NAS sous TrueNAS. Cette VM est configurée avec 1 vCPU, 2 Go de RAM, un disque système de 15 Go, et un disque de 1 To dédié au stockage des sauvegardes. Ce serveur TrueNAS servira d'espace centralisé pour sauvegarder les VMs dans une zone sécurisée, en complément de la solution de sauvegarde.



Configuration du routeur pour sécuriser les sauvegardes

Afin d'assurer la sécurité du réseau dédié aux sauvegardes, j'ai mis en place une stratégie de filtrage sur le routeur. Dans un premier temps, une règle temporaire de type "any" a été appliquée pour laisser transiter l'ensemble du trafic, ce qui m'a permis d'analyser les logs et d'identifier les flux réellement nécessaires au bon fonctionnement du serveur de sauvegarde.

De plus j'ai consulté la documentation officielle de Veeam concernant les ports réseau utilisés par le logiciel. Cette ressource, disponible sur leur site officiel, m'a permis d'identifier précisément les **ports à ouvrir sur le pare-feu** afin d'assurer une connectivité optimale tout en maintenant un niveau de sécurité adapté.

https://helpcenter.veeam.com/docs/backup/vsphere/used_ports.html?ver=120

216 Matched Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✓	Apr 16 15:25:20	VLANBACKUP	temp (1744301274)	10.10.200.10:123	51.137.137.111:123	UDP
✓	Apr 16 15:25:52	VLANBACKUP	temp (1744301274)	10.10.200.10:138	10.10.200.255:138	UDP
✓	Apr 16 15:31:58	VLANBACKUP	temp (1744301274)	10.10.200.10:60336	10.10.110.10:53	UDP
✓	Apr 16 15:31:58	VLANBACKUP	temp (1744301274)	10.10.200.10:62418	13.78.111.198:443	TCP:SEC
✓	Apr 16 15:32:59	VLANBACKUP	temp (1744301274)	10.10.200.10:64343	10.10.110.10:53	UDP
✓	Apr 16 15:32:59	VLANBACKUP	temp (1744301274)	10.10.200.10:62461	184.51.142.113:80	TCP:SEC
✓	Apr 16 15:32:59	VLANBACKUP	temp (1744301274)	10.10.200.10:55022	10.10.110.10:53	UDP
✓	Apr 16 15:32:59	VLANBACKUP	temp (1744301274)	10.10.200.10:62462	199.232.210.172:80	TCP:SEC
✓	Apr 16 15:33:17	VLANBACKUP	temp (1744301274)	10.10.200.10:62473	10.10.210.31:443	TCP:SEC

Après analyse, seules les communications indispensables ont été conservées : la liaison avec le serveur ESXi pour l'accès aux machines virtuelles, ainsi qu'un accès limité au contrôleur de domaine pour la résolution DNS. Enfin, une règle spécifique a été ajoutée pour autoriser la synchronisation horaire (NTP) afin de garantir la cohérence des journaux de sauvegarde et la planification des tâches.

Firewall / Rules / VLANBACKUP

Floating | WAN | LAN | VLANSERVER | VLANCLIENT | VLANDMZ | VLANMGMT | VLANBACKUP | SYNC | OpenVPN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
	1/15 KiB	IPv4 UDP	VP_BACKUP	*	VP_AD1	53 (DNS)	*	none		BACKUP TO DNS	
	1/2 KiB	IPv4 UDP	VP_BACKUP	*	*	123 (NTP)	*	none		BACKUP TO NTP	
	0/1.38 MiB	IPv4 TCP	VP_BACKUP	*	ESXi	BACKUP_TO_ESXi	*	none		BACKUP TO ESXi	
	0/7 KiB	IPv4 *	*	*	*	*	*	none		block any	

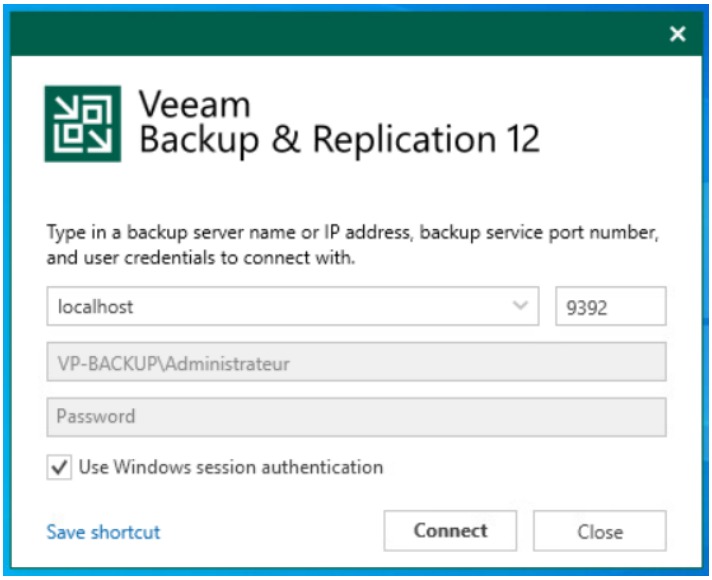
Par souci de sécurité et de cloisonnement, le serveur de sauvegarde n'est pas intégré au domaine Active Directory. Il fonctionne en autonomie avec un compte administrateur local protégé par un mot de passe fort. Cette isolation volontaire permet de limiter les risques de propagation en cas de compromission du domaine principal.

Installation de VEEAM Backup and Replication

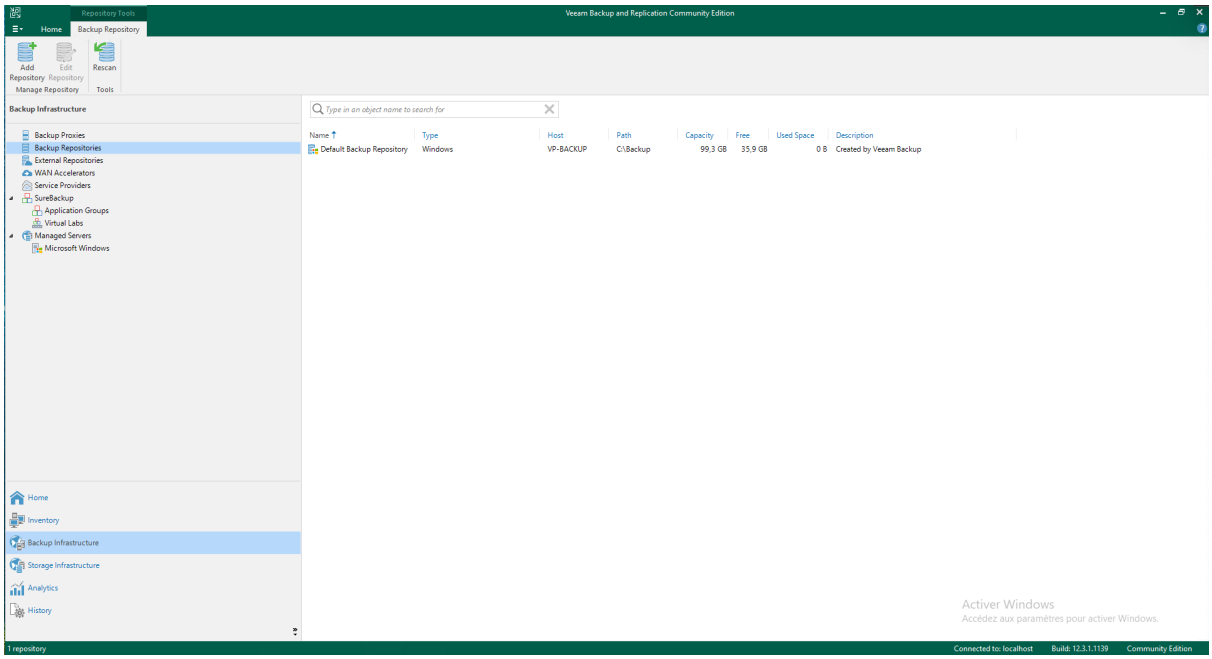
Une fois Windows Server 2022 installé sur la machine virtuelle, je procède au téléchargement de la dernière version de Veeam Backup & Replication, à savoir la version 12.3. Pour cela, je me connecte à mon espace client Veeam afin de récupérer l'ISO officielle. Cette méthode me permet d'installer une version à jour du logiciel, incluant les dernières fonctionnalités et correctifs de sécurité.

Le logiciel Veeam Backup & Replication a été téléchargé puis installé sur la machine virtuelle. L'installation comprend l'ajout de plusieurs composants nécessaires au bon fonctionnement du service, tels que le serveur SQL Express et les services Veeam.

Une fois Veeam installé, je peux accéder à l'interface du logiciel. L'authentification se fait à l'aide des identifiants du compte utilisateur actuellement connecté sur Windows. Dans ce cas précis, la machine n'étant pas intégrée à un domaine, les identifiants utilisés sont ceux du compte local, à savoir le nom d'utilisateur "VP-BACKUP\Administrateur" accompagné de son mot de passe.



L'installation terminée et la connexion effectuée, l'interface de gestion de Veeam devient accessible et prête à être configurée. Elle se présente sous forme d'une console centralisée comprenant plusieurs onglets essentiels à la mise en place de la solution de sauvegarde. Parmi eux, les sections "Home", "Inventory" et "Backup Infrastructure" sont particulièrement importantes, car elles permettent respectivement de gérer les tâches de sauvegarde, d'ajouter les ressources à protéger, et de configurer l'infrastructure de sauvegarde.



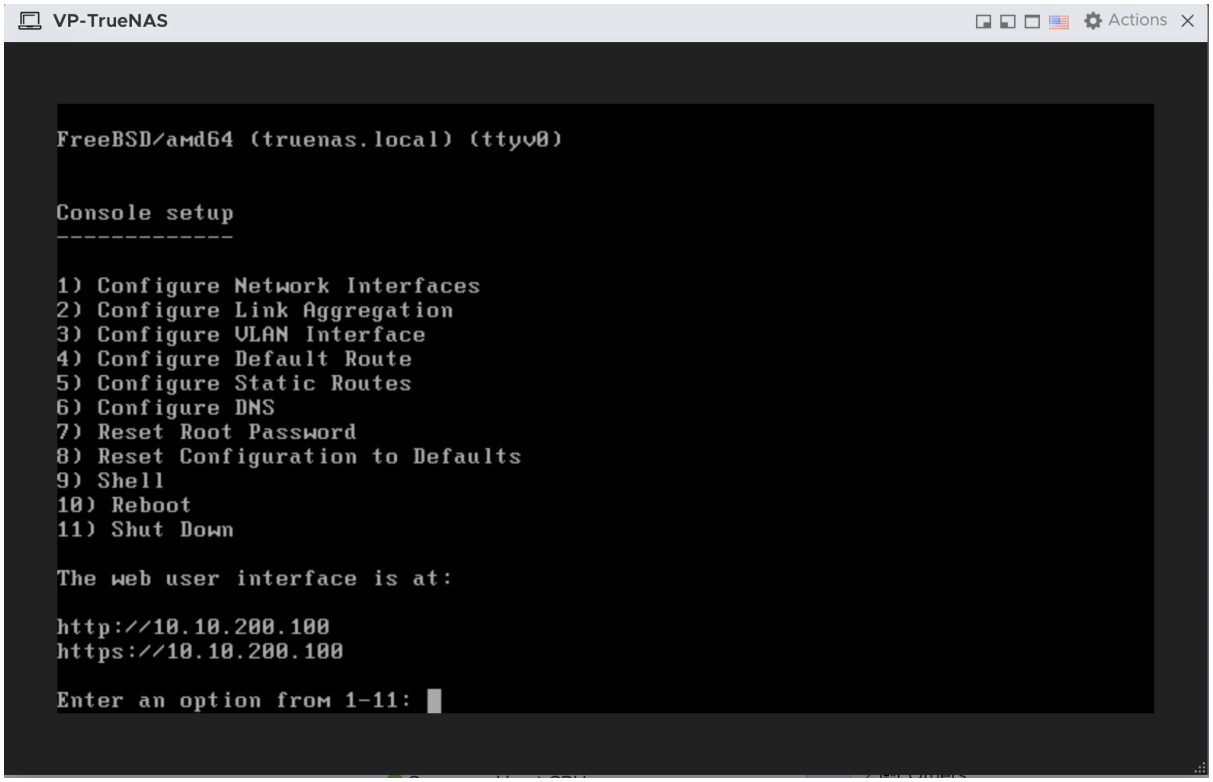
Création d'un stockage via TrueNAS

L'installation de Veeam finalisée, je passe à la mise en place du stockage destiné à accueillir les sauvegardes. Par manque de matériel physique, le NAS sera déployé sous forme de machine virtuelle.

Je télécharge l'image ISO de TrueNAS depuis le site officiel, en veillant à choisir la dernière version stable disponible. L'installation se fait de manière classique, en suivant l'assistant pas à pas ("suivant-suivant"), tout en veillant à bien sélectionner le disque destiné au démarrage du système.

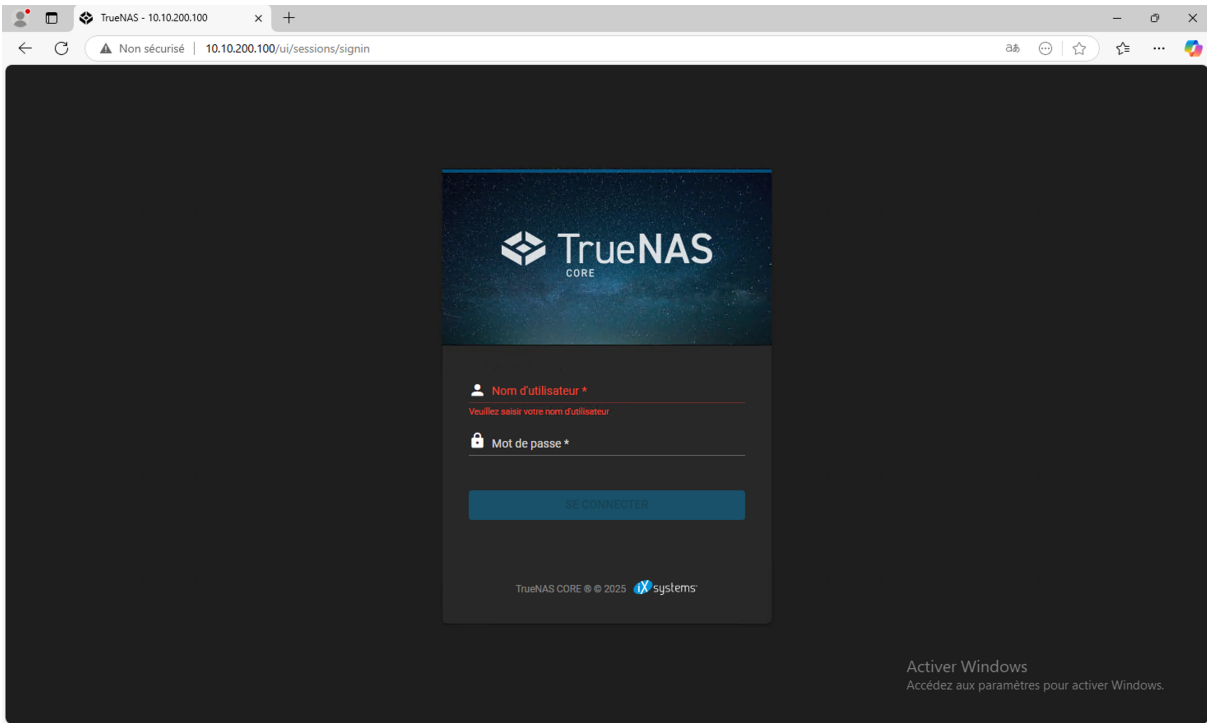
Configuration de TrueNAS en CLI

Une fois le système installé, je procède à la configuration réseau de la machine. Depuis le menu de démarrage de TrueNAS, je choisis l'option 1 pour configurer l'adresse IP. J'attribue l'adresse 10.10.200.100 à l'interface réseau puis je choisis l'option 4 pour configurer la gateway, ce qui permet à la machine d'être accessible sur le VLAN BACKUP.



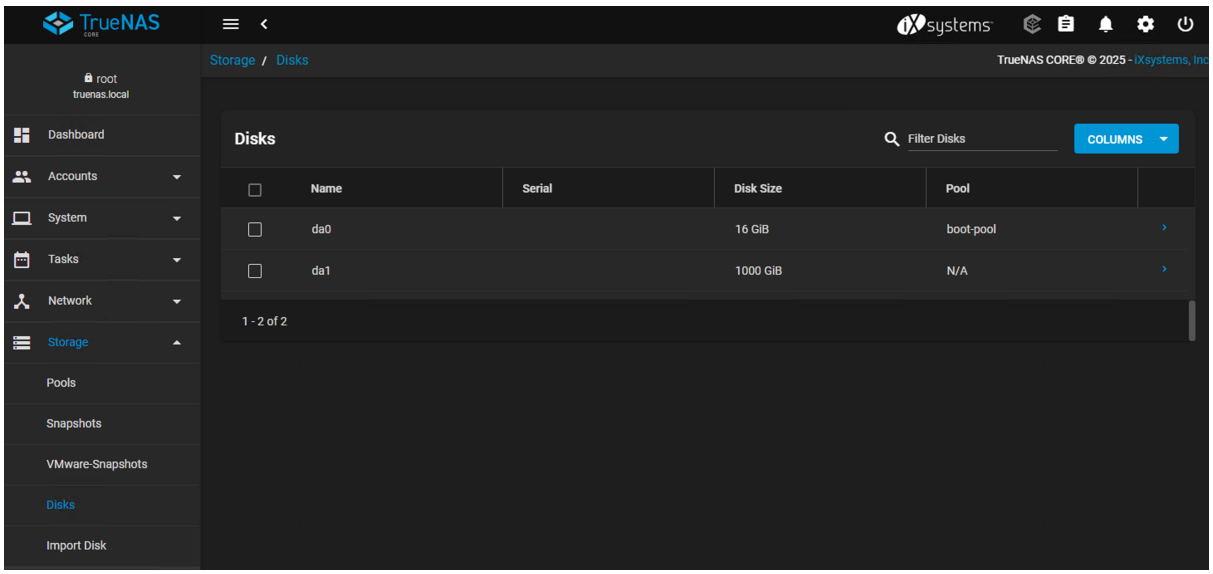
Configuration de TrueNAS en interface web

La suite de la configuration s'effectue via l'interface web de TrueNAS, accessible depuis un navigateur à l'adresse IP précédemment définie (10.10.200.100) via https://10.10.200.100.

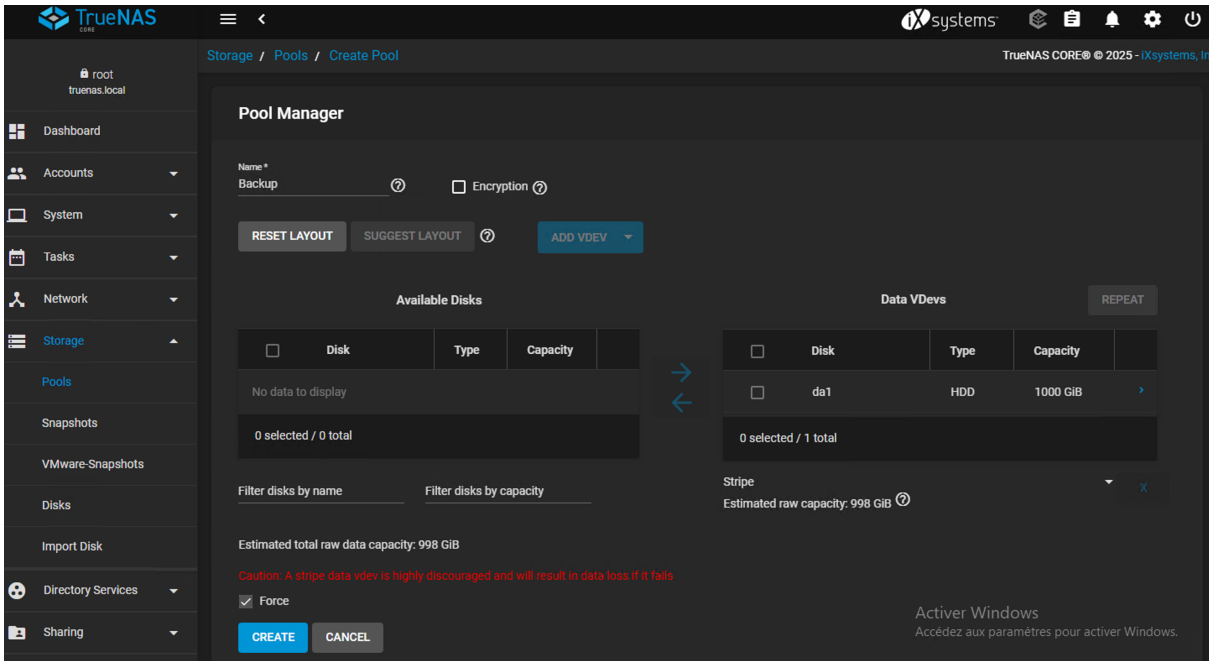


Configuration d'un pool de stockage

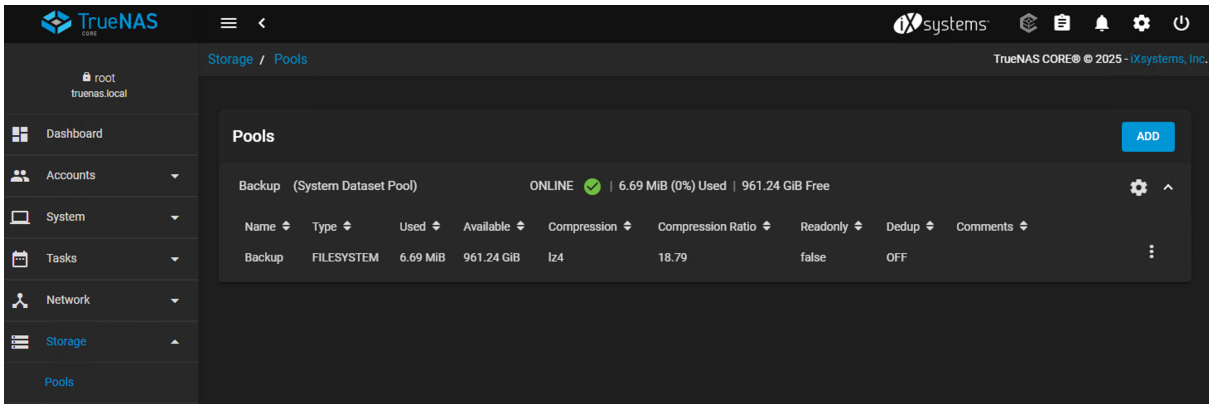
Dans un premier temps, je me rends dans le menu Storage, puis dans la section Disks, afin de vérifier que le disque de 1 To destiné aux sauvegardes est bien détecté par le système.



Une fois la présence du disque confirmée, je me rends dans l'onglet Pools pour créer un nouveau pool de stockage. Je lance l'assistant de création, donne au pool le nom "Backup", puis j'ajoute le disque de 1 To à cette configuration.



Une fois le processus terminé, le pool apparaît dans l'interface avec le statut "Online", ce qui confirme qu'il est opérationnel et prêt à être utilisé pour héberger les données de sauvegarde.

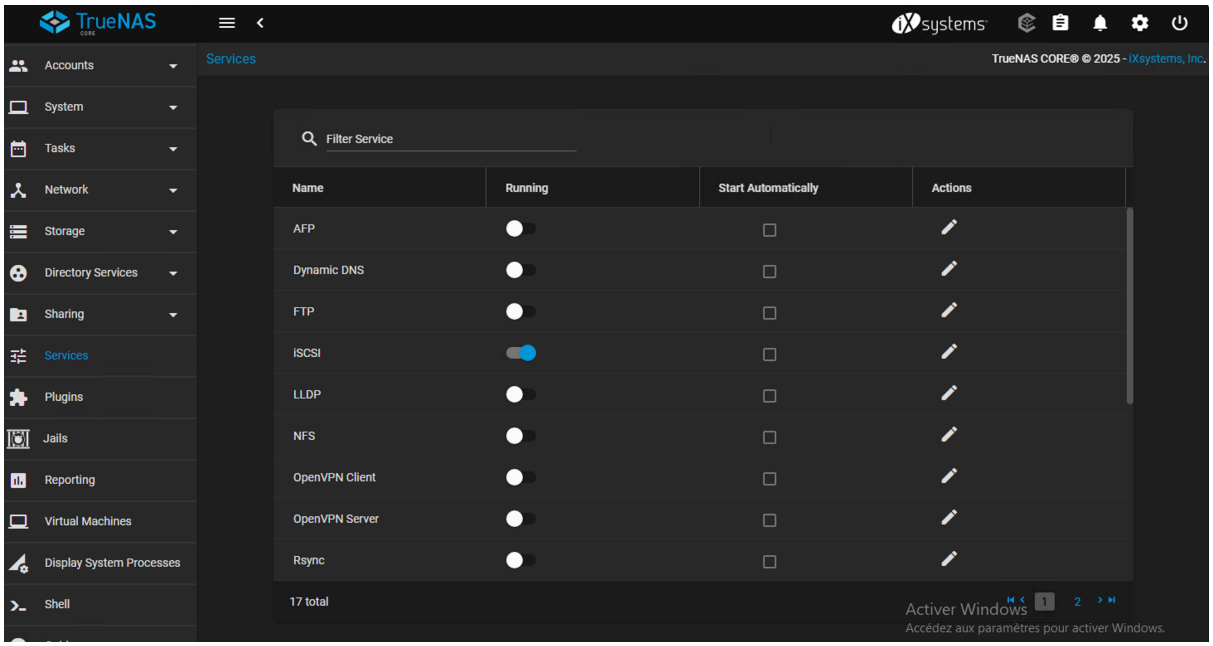


Configuration d'un lien ISCSI

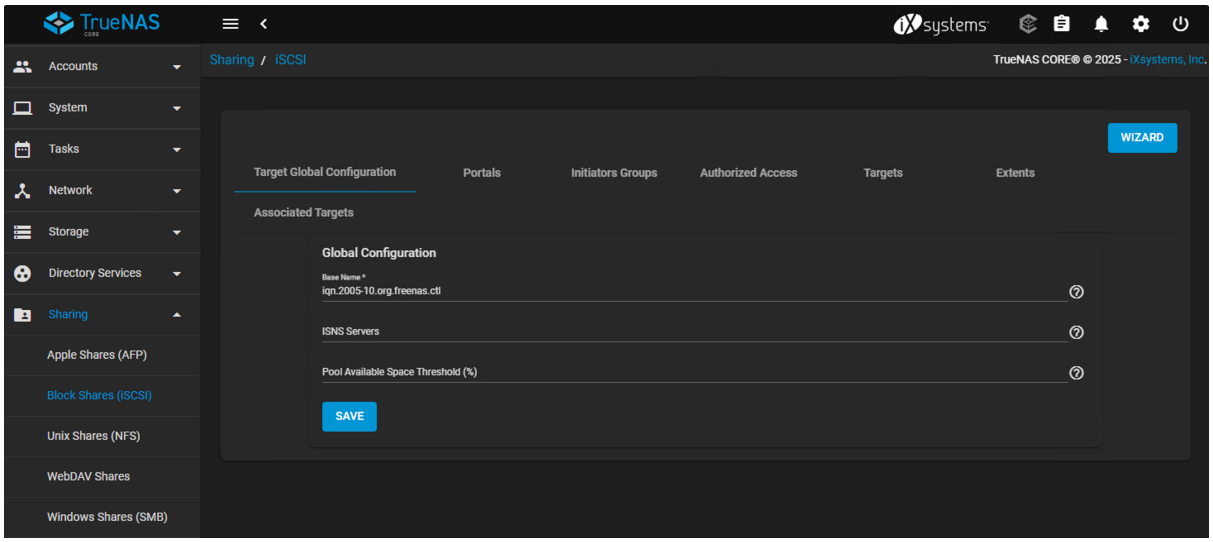
Configuration du service ISCSI sur TrueNAS

Pour permettre à Veeam d'utiliser le NAS comme cible de sauvegarde via le protocole iSCSI, je configure le service correspondant depuis l'interface web de TrueNAS.

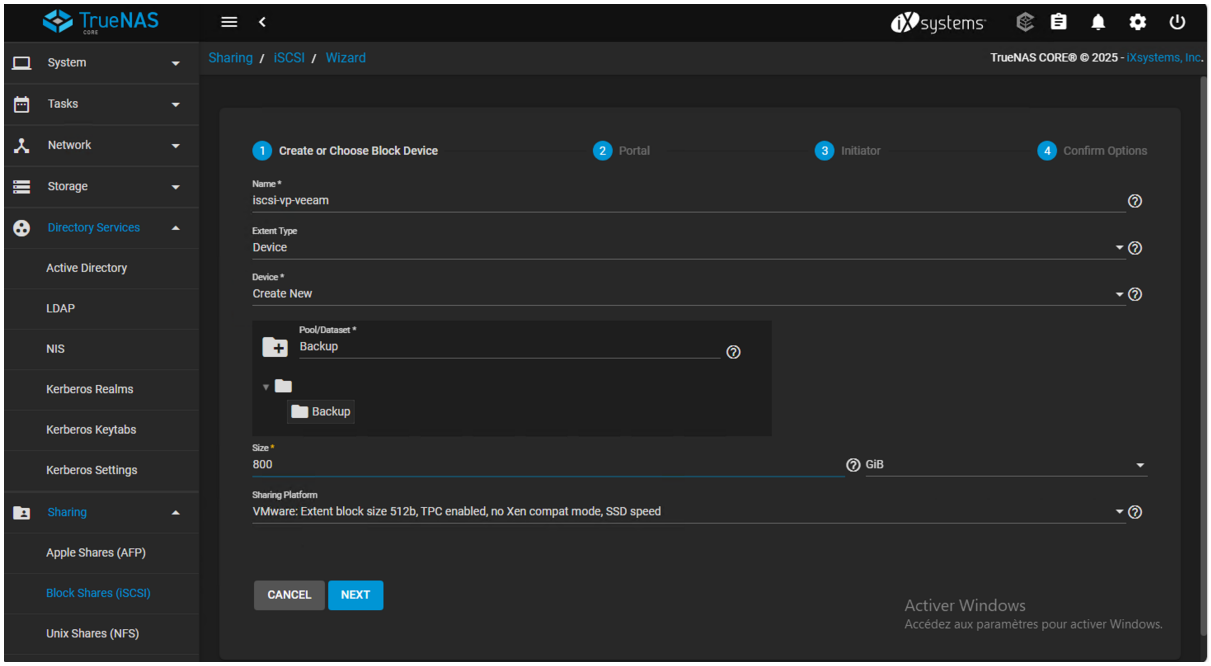
Je me rends dans l'onglet Services, puis j'active le service iSCSI.



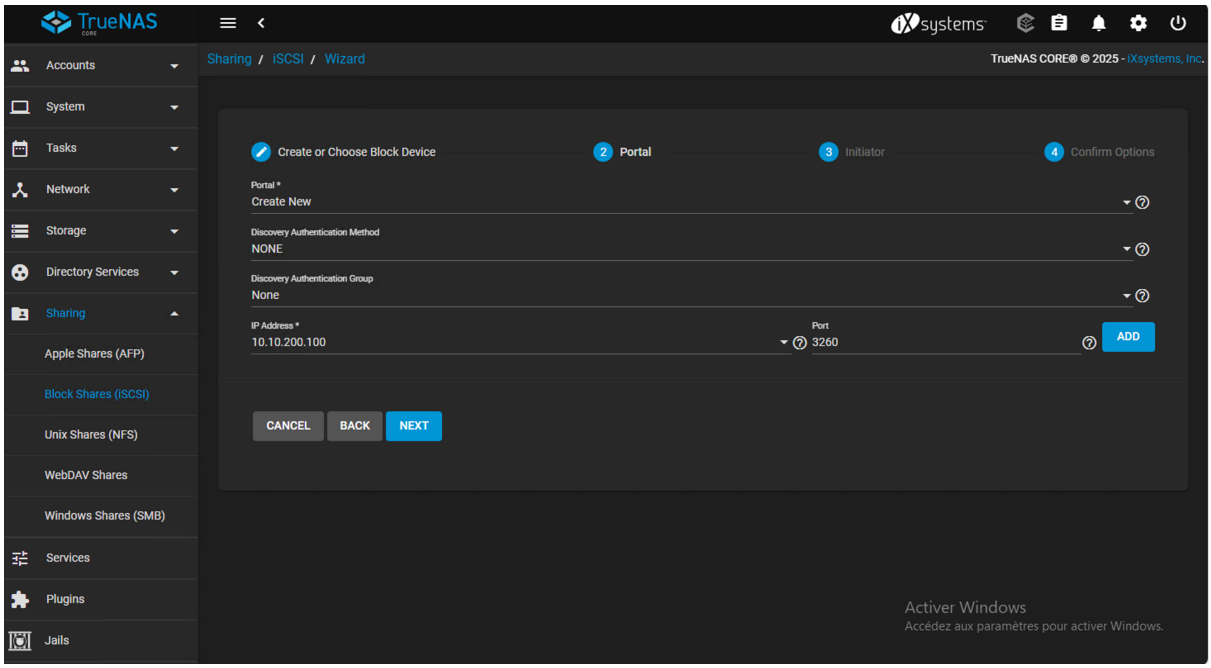
Ensuite, je clique sur l'icône en forme de stylo pour accéder à la configuration, puis je lance l'assistant en cliquant sur Wizard.



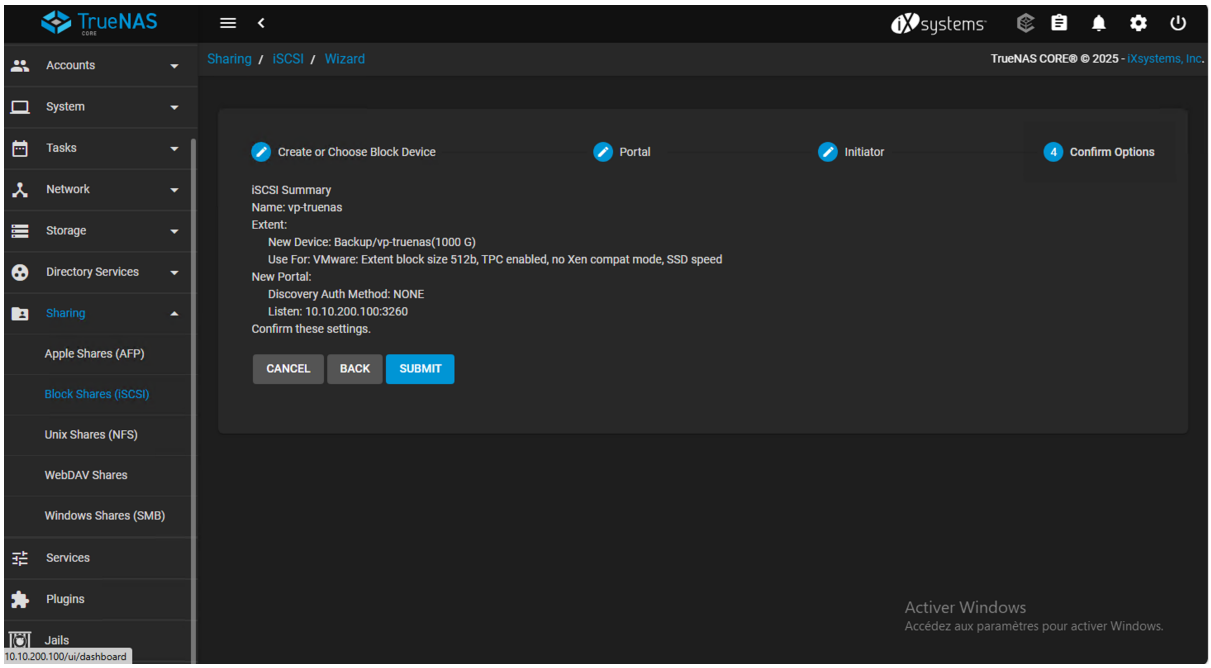
L’assistant me guide dans la création d’un Block Device, c’est-à-dire une unité de stockage en mode bloc. Je définis un nom pour ce bloc, et je lui attribue une capacité de 750 Go, en suivant la recommandation de TrueNAS qui suggère de conserver environ 20 % de l’espace total libre pour garantir de bonnes performances et une meilleure stabilité.



Je configure ensuite un Portal, c’est-à-dire le point d’accès au service iSCSI, en indiquant l’adresse IP du serveur TrueNAS (10.10.200.100) et le port par défaut 3260.



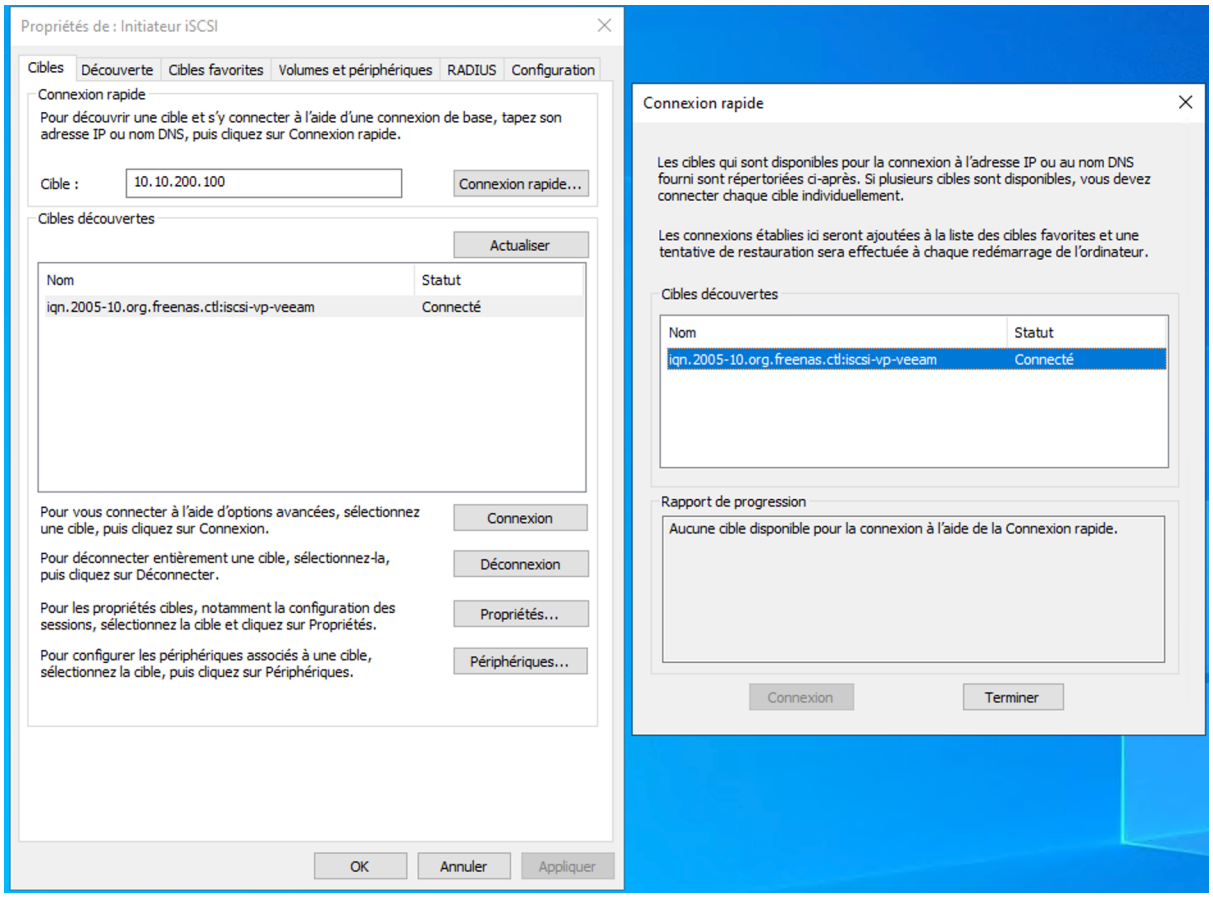
Une fois tous les paramètres renseignés, je clique sur Submit afin de valider et finaliser la configuration. Le service iSCSI est désormais opérationnel et prêt à être monté sur le serveur Veeam.



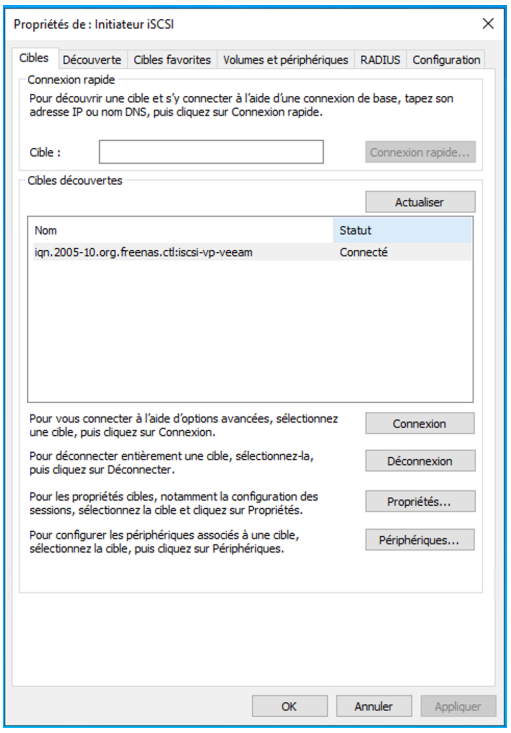
Configuration du service ISCSI sur Windows Server 2022

Sur le serveur VP-BACKUP, je procède à la connexion au stockage iSCSI précédemment configuré sur TrueNAS. Pour cela, je lance l'outil Initiateur iSCSI depuis le menu Démarrer de Windows.

Dans l'onglet Cible, je saisis l'adresse IP du serveur TrueNAS, à savoir 10.10.200.100, puis je clique sur Rapide connexion. L'initiateur détecte automatiquement la cible iSCSI disponible, identifiée par son IQN (iSCSI Qualified Name), qui est ici : iqn.2005-10.org.freenas.ctl:iscsi-vp-truenas



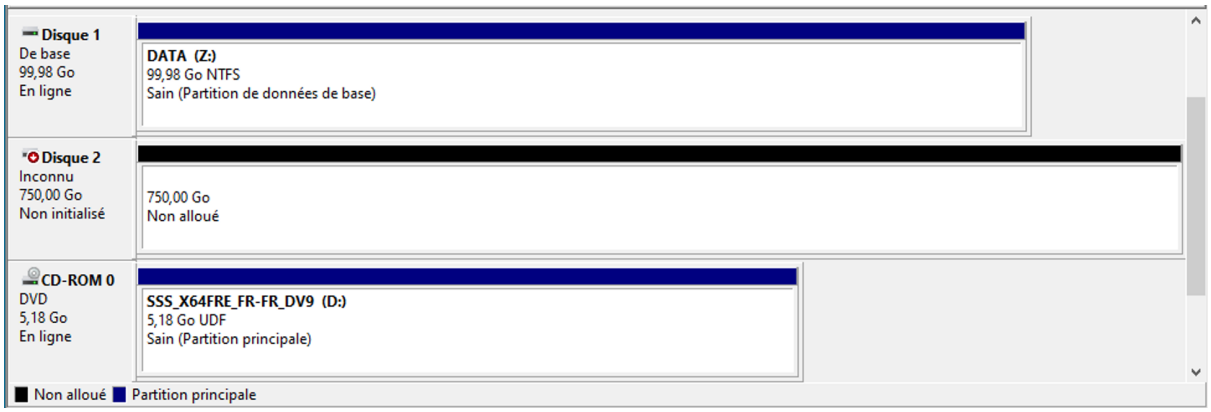
Une fois la cible détectée, je la sélectionne, puis je clique sur Connecter afin d'établir la liaison entre le serveur Windows et le volume iSCSI hébergé sur TrueNAS. Le disque est alors reconnu par le système et prêt à être initialisé et formaté via la gestion des disques.



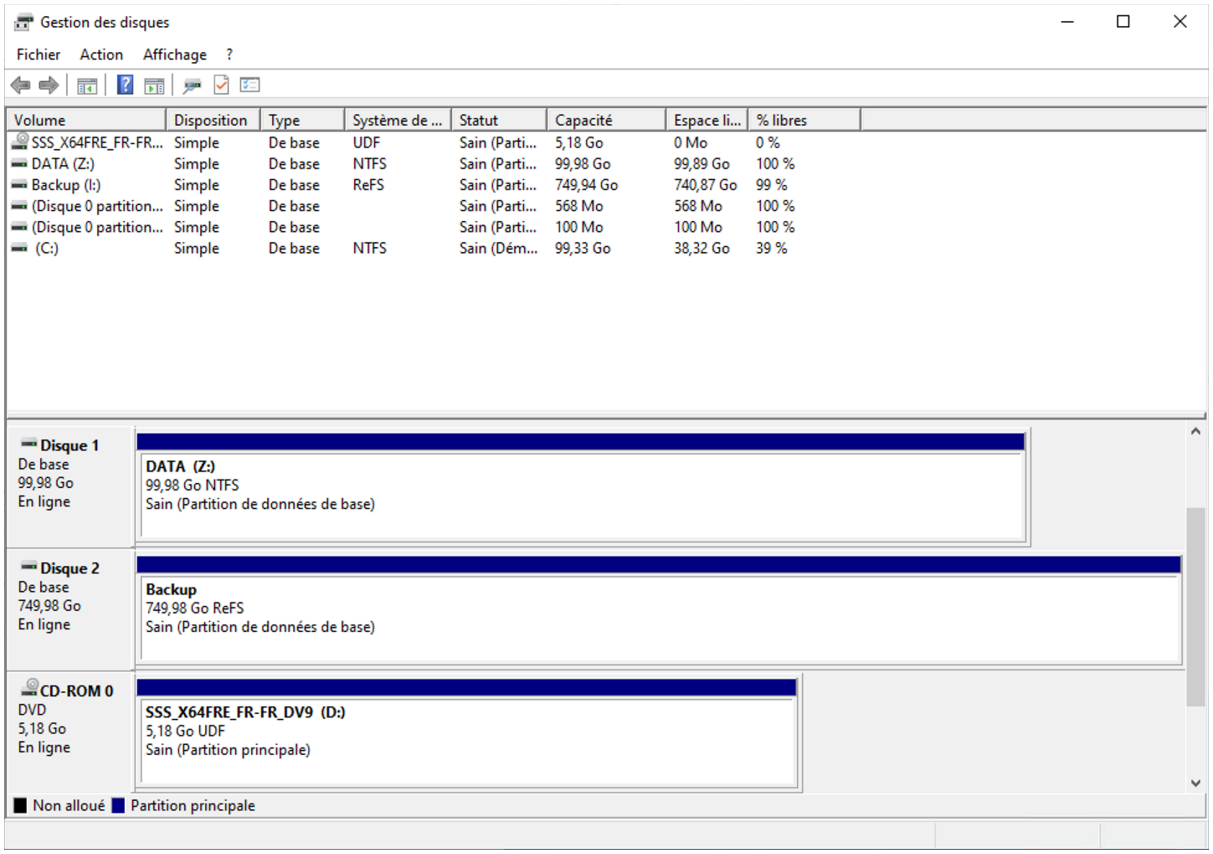
Initialisation du disque iSCSI dans Windows Server

Une fois la connexion à la cible iSCSI établie depuis l'initiateur iSCSI, le disque distant devient visible dans le **Gestionnaire de disques** de Windows Server.

Je procède alors à l'**initialisation du disque**, en le convertissant au format GPT (GUID Partition Table), puis je crée un **nouveau volume simple** en utilisant l'espace alloué de **750 Go**. Cette taille correspond à l'espace disponible sur le NAS, TrueNAS ayant réservé environ 20 % de la capacité totale pour son propre fonctionnement et garantir la stabilité du système.



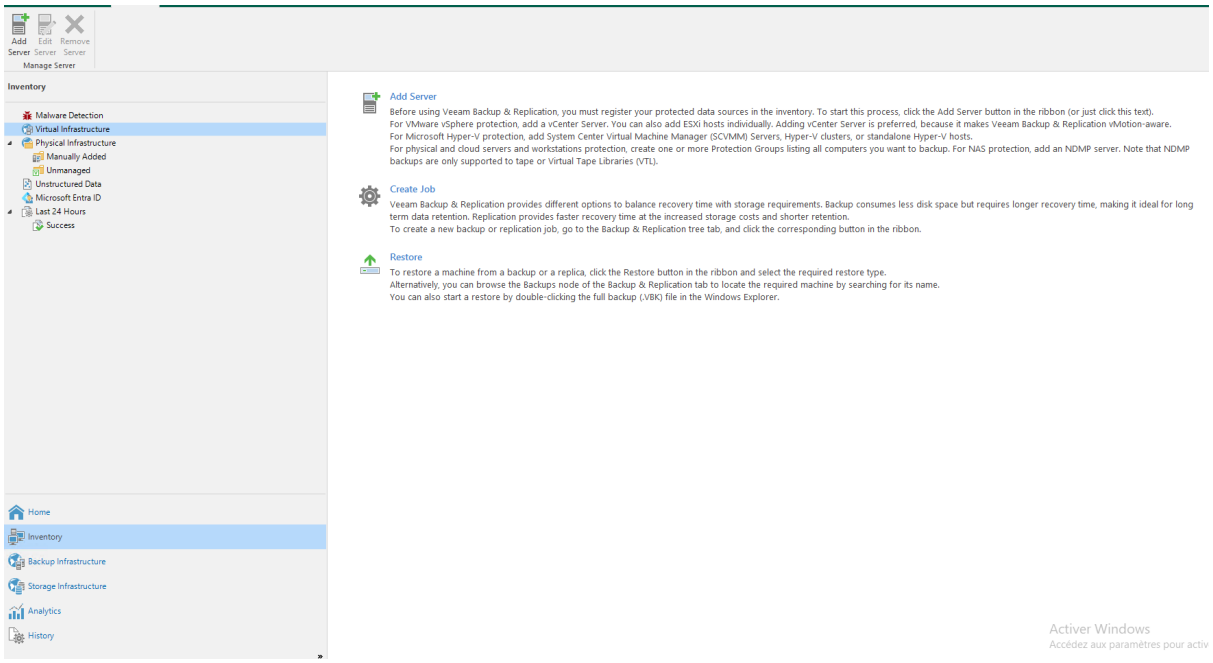
Une fois le volume créé et formaté en ReFS, il est monté dans le système Windows sous forme de lecteur, prêt à accueillir les données de sauvegarde générées par Veeam.

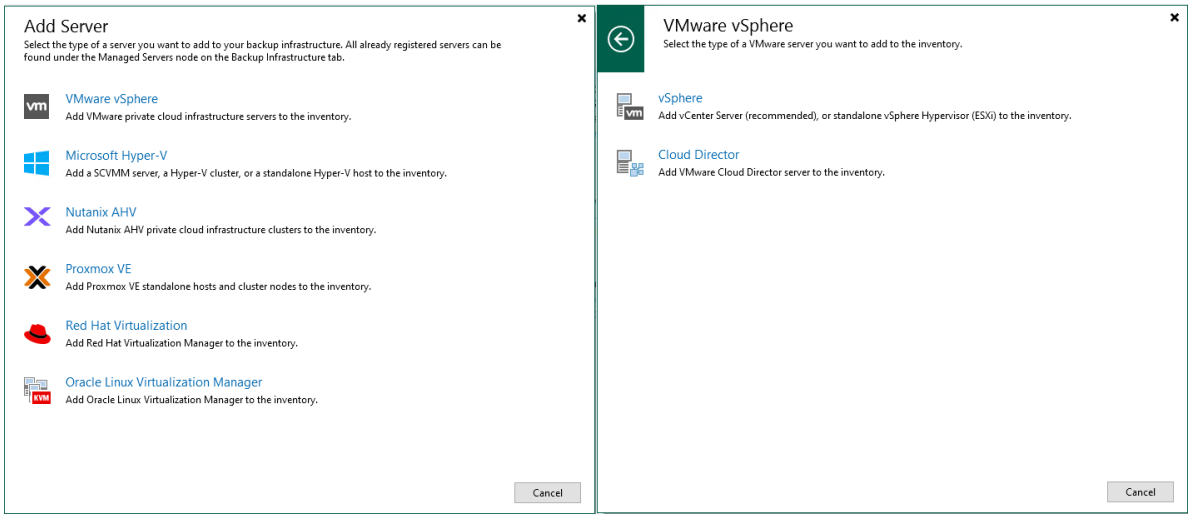


Ajout des cibles de sauvegardes

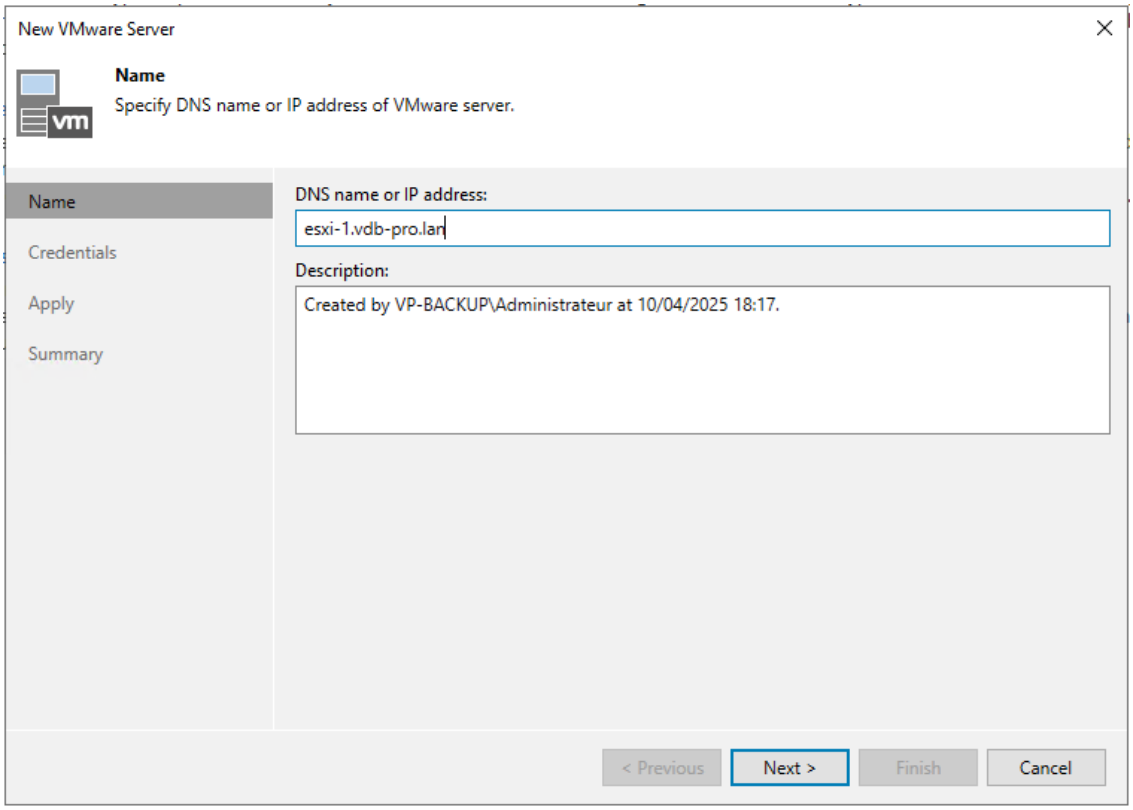
Depuis l'interface de Veeam, les machines virtuelles à sauvegarder sont ajoutées en tant que cibles. Dans ce projet, il s'agit de machines virtuelles hébergées sur un serveur ESXi. L'accès à ces VM est effectué à l'aide des identifiants administrateur, via une connexion sécurisée, ce qui permet à Veeam de détecter automatiquement les systèmes présents sur l'hôte et d'y accéder.

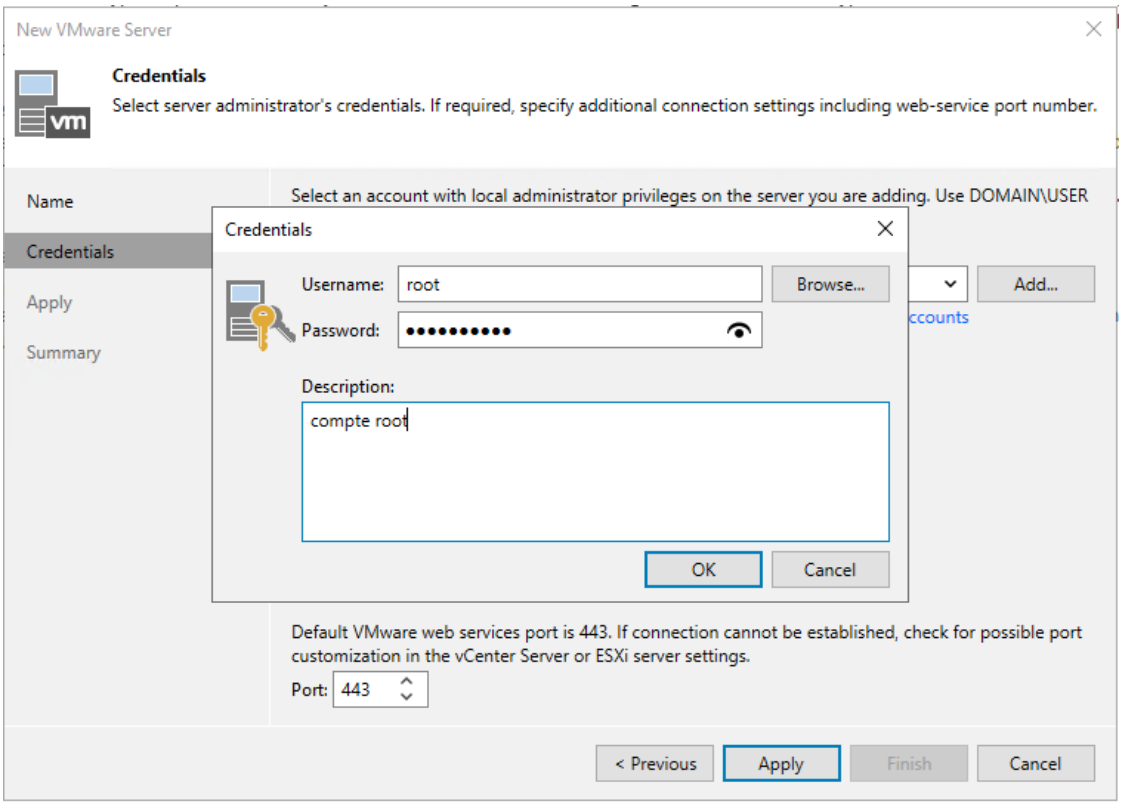
Pour cela, je me rends dans l'onglet Inventory, puis dans la section Virtual Infrastructure. À cet endroit, je procède à l'ajout d'un serveur en sélectionnant l'option VMware vSphere. Deux possibilités s'offrent alors : ajouter un vCenter Server, ou directement un hôte ESXi en standalone. Le vCenter permet de centraliser la gestion de plusieurs hôtes ESXi, mais dans mon cas, n'ayant pas mis en place un vCenter, j'opte pour l'ajout de mon ESXi de manière autonome.



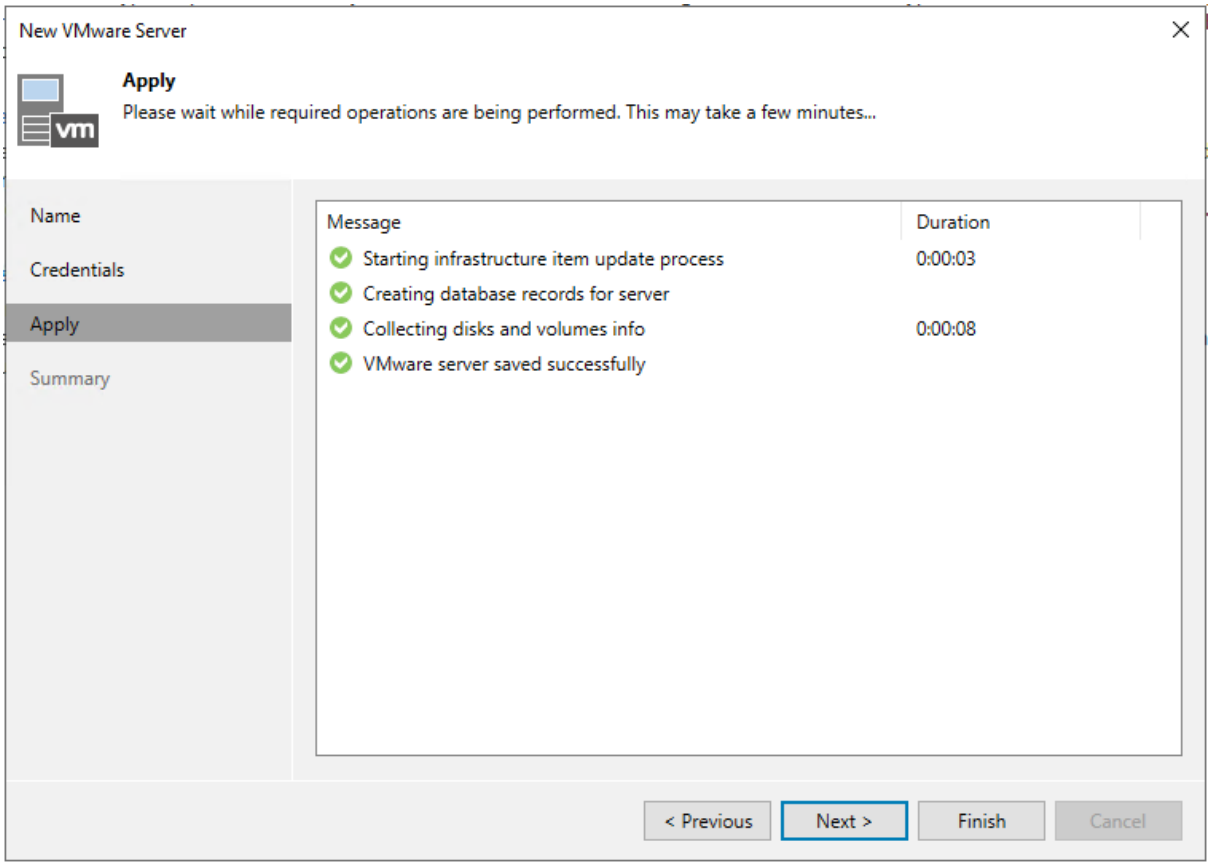


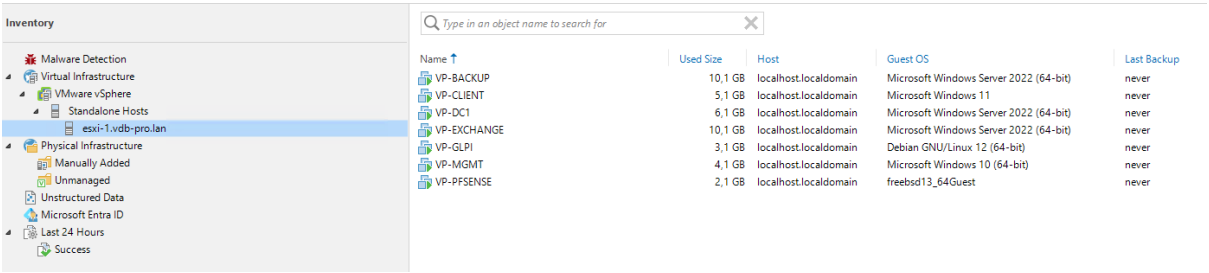
Lors de l'ajout, j'indique soit l'adresse IP, soit le nom DNS de l'hôte. Ayant préalablement configuré un enregistrement DNS pointant vers mon serveur (par exemple : esxi-1.vdb-pro.lan → 10.10.210.31), j'utilise ce nom DNS dans la configuration. Ensuite, je saisis les identifiants d'accès à l'ESXi, ici l'utilisateur root et son mot de passe.





Une fois ces informations renseignées, Veeam procède à un scan de l'hôte afin de vérifier sa disponibilité et d'identifier les machines virtuelles qui y sont hébergées. Ces VM apparaissent alors dans l'interface, prêtes à être sélectionnées pour les futures tâches de sauvegarde.





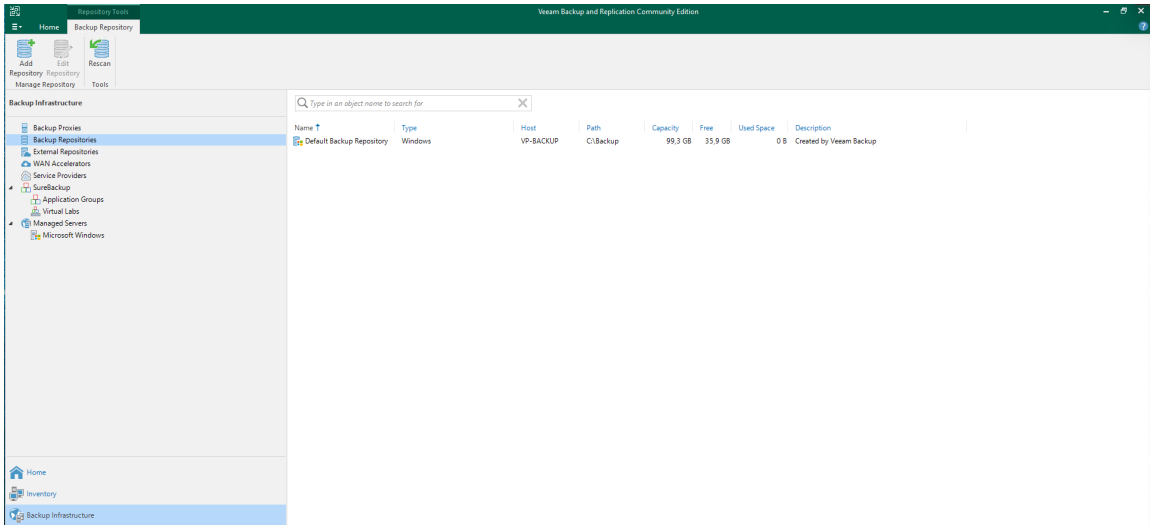
Ajout des Target de sauvegardes

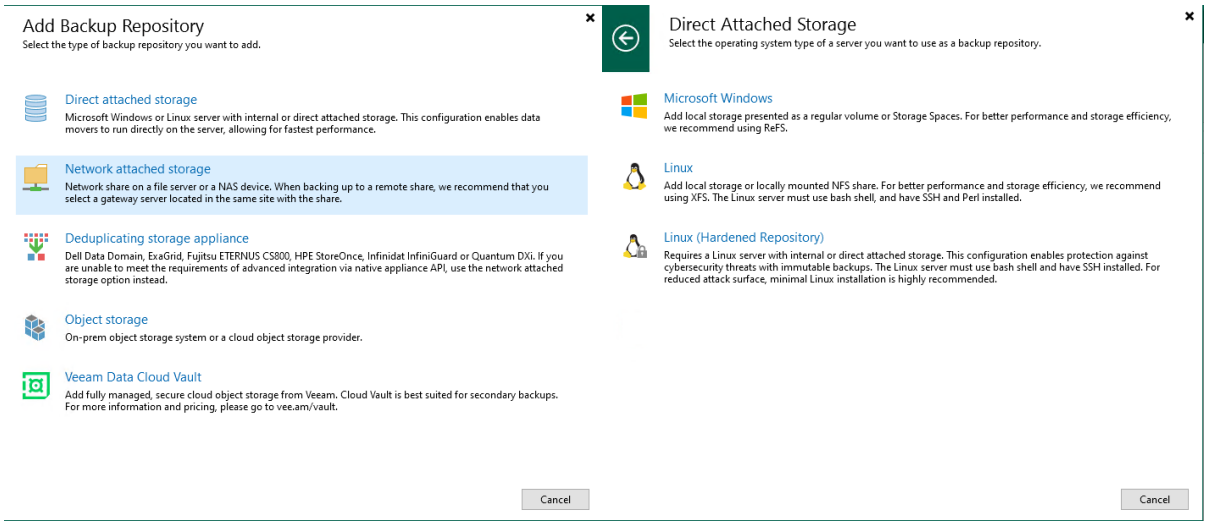
Une fois les sources de données identifiées, il est nécessaire de définir un espace de stockage destiné à accueillir les sauvegardes. Pour cela, un NAS externe a été ajouté dans Veeam en tant que dépôt de sauvegarde (backup repository). Ce NAS étant accessible via le réseau local, il permet une écriture rapide et fiable des données, ce qui est essentiel pour garantir la sécurité et la rétention des sauvegardes.

Dans un premier temps, je configure deux dépôts distincts :

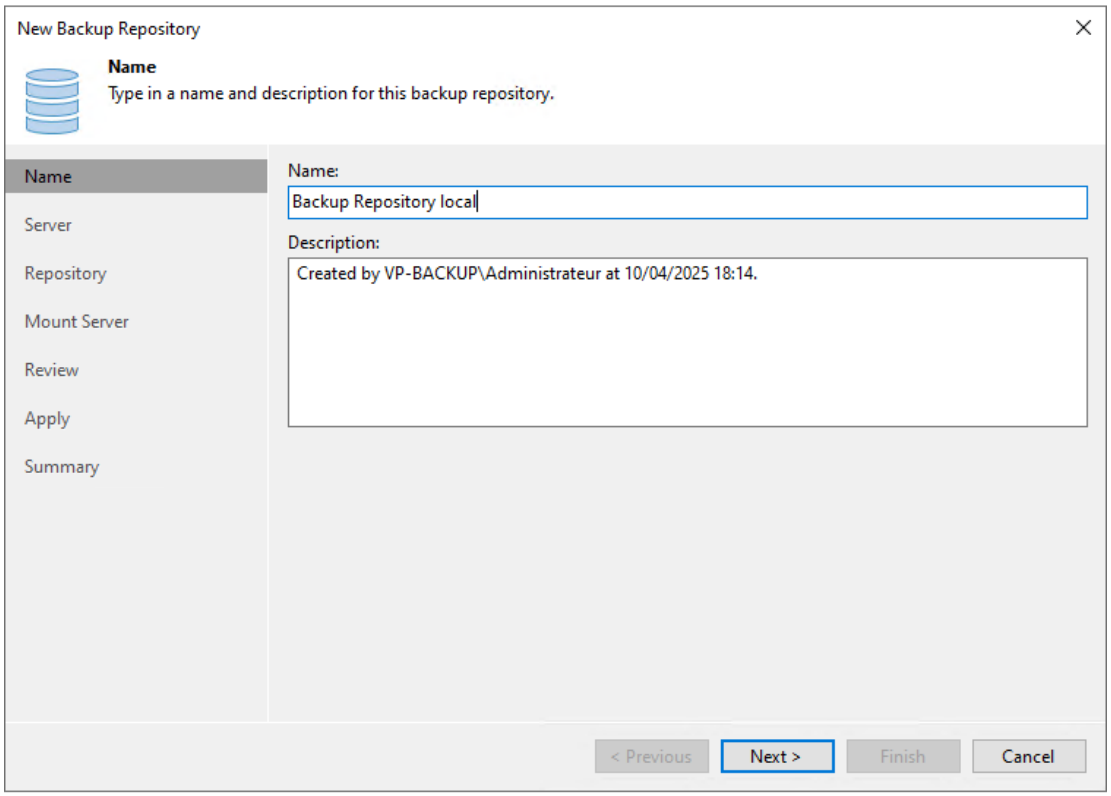
1. Le lecteur Z:\DATA, qui correspond à un repository local hébergé sur le serveur VP-BACKUP. Ce dépôt est principalement utilisé pour effectuer des copies de sauvegarde (Backup Copy) ou pour stocker les fichiers de configuration de Veeam.
2. Le lecteur I:\Backup, qui est un disque monté via iSCSI, connecté au TrueNAS. Ce dépôt sera utilisé comme destination principale pour les sauvegardes des machines virtuelles.

Pour ajouter ces dépôts, je me rends dans l'onglet Backup Infrastructure, puis dans la section Backup Repositories. Je lance l'assistant d'ajout et sélectionne le type Network Attached Storage, avec le format Microsoft Windows.

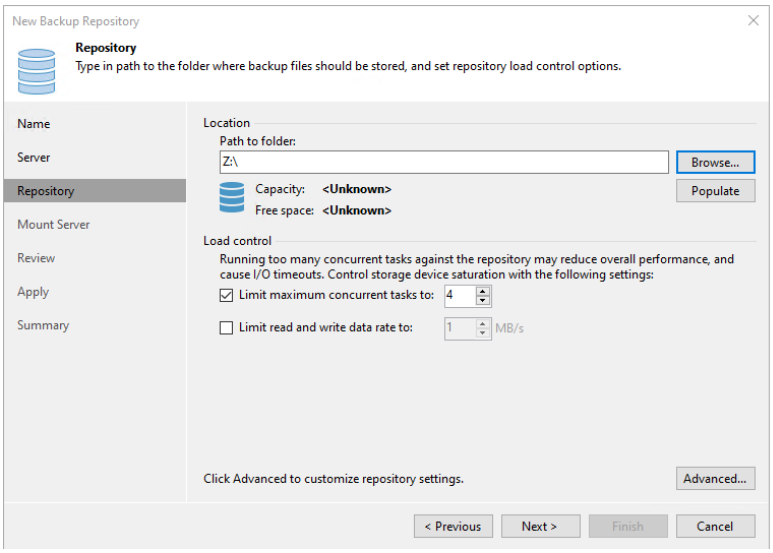


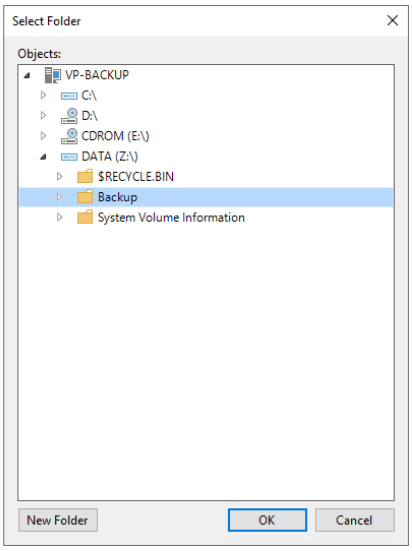


Je donne ensuite un nom au repository, par exemple "Backup Repository Local", qui sera affiché dans l'interface Veeam.

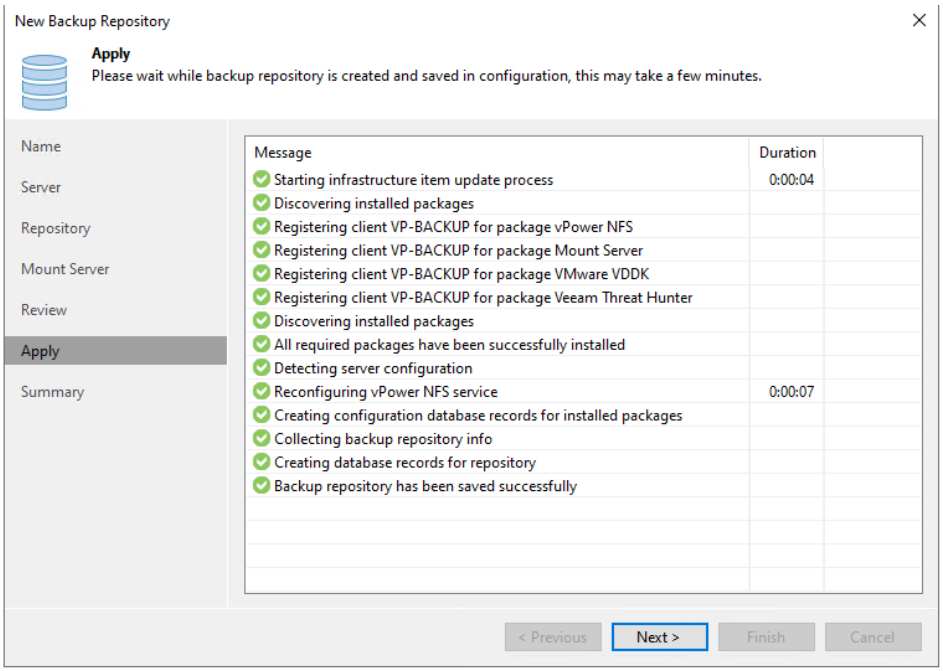


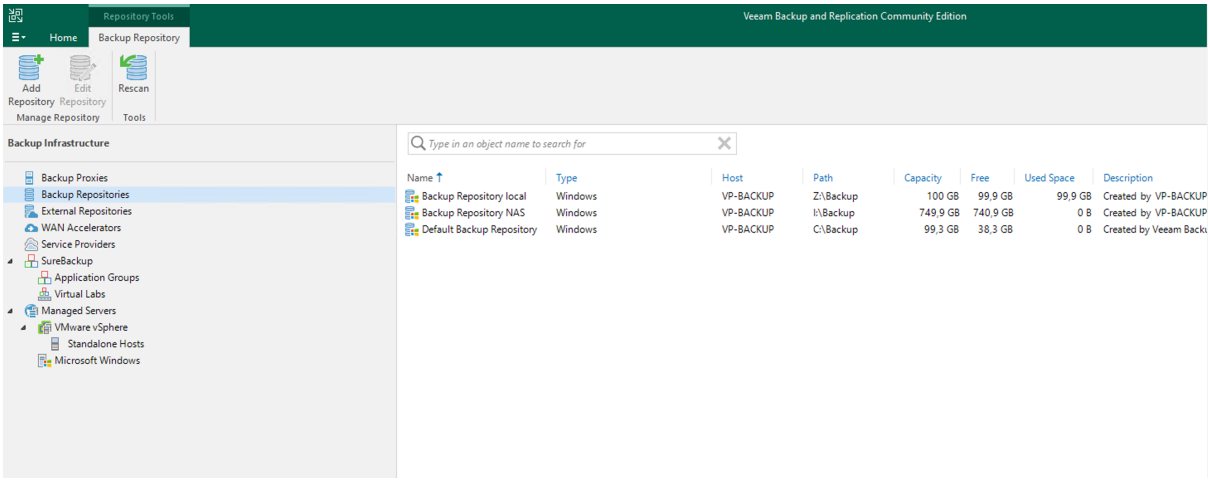
Je choisis le serveur VP-BACKUP comme hôte du dépôt, puis je sélectionne le lecteur Z:\ ainsi que le dossier Backup, que j'avais préalablement créé à cet emplacement.





Une fois tous les paramètres définis, je clique sur Finish pour valider la configuration. Veeam effectue alors une vérification des paramètres, et si tout est correctement configuré, l'état passe au vert, indiquant que le repository est prêt à être utilisé.



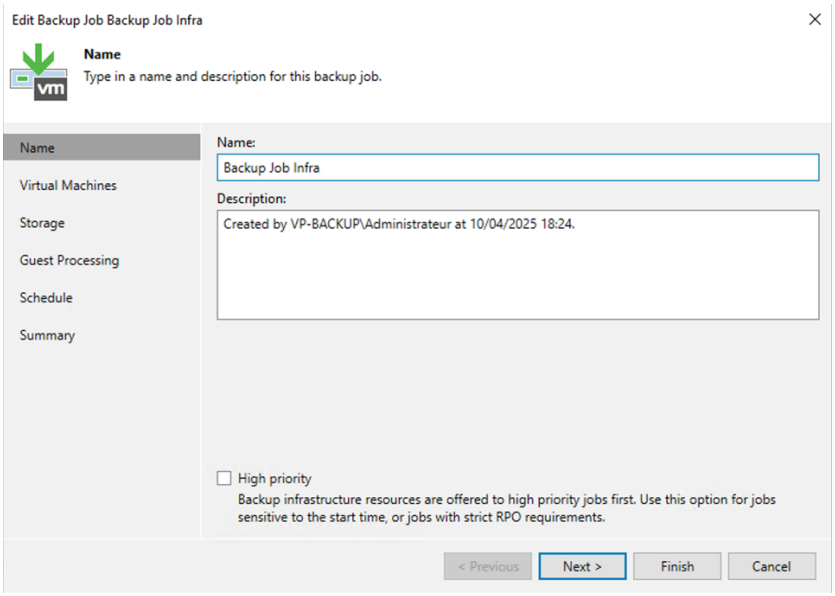


Création des jobs

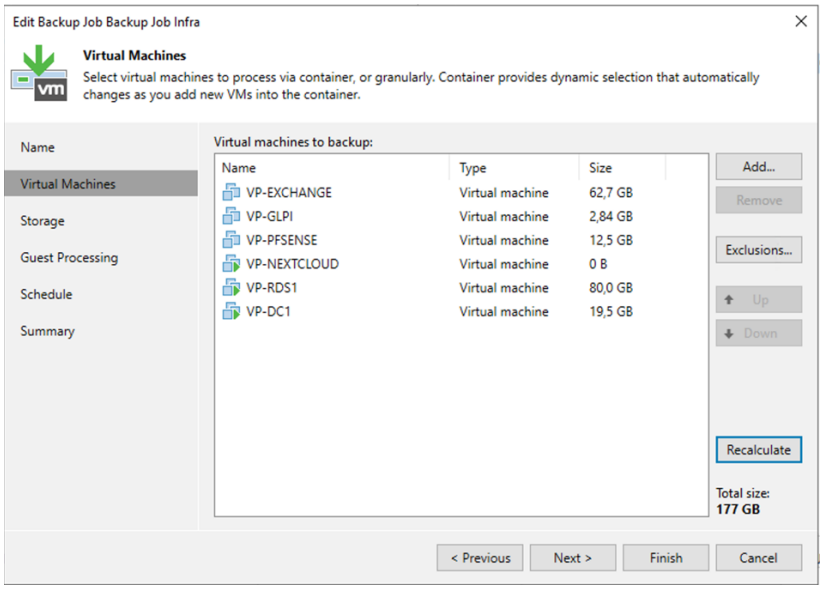
Une fois les dépôts de sauvegarde configurés, je procède à la création des **jobs de sauvegarde** dans l'interface de Veeam. Chaque job est défini avec les paramètres suivants : sélection des machines virtuelles à sauvegarder, planification automatique (quotidienne ou hebdomadaire), stratégie de rétention, ainsi que des options avancées telles que la **compression**, le **chiffrement** et les **notifications par e-mail** afin d'assurer un suivi efficace.

Job principal : sauvegarde de l'infrastructure

Je crée un premier job nommé **"Backup Job Infra"**, destiné à sauvegarder l'ensemble des machines virtuelles de l'infrastructure.

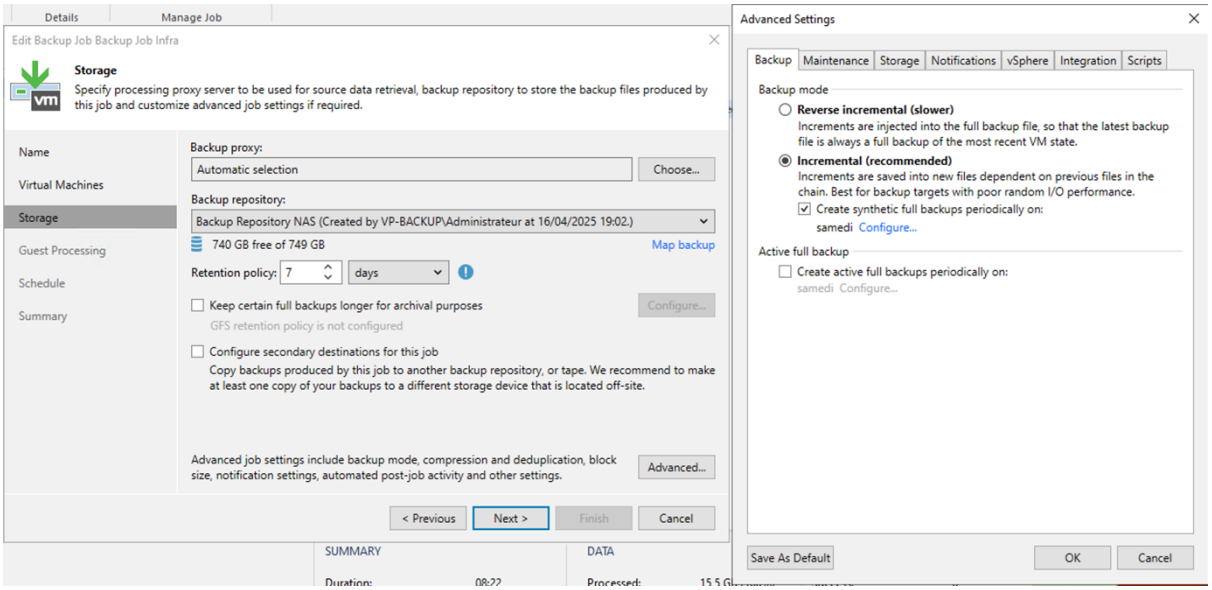


Dans l'onglet **Virtual Machines**, je sélectionne toutes les VMs critiques à protéger.

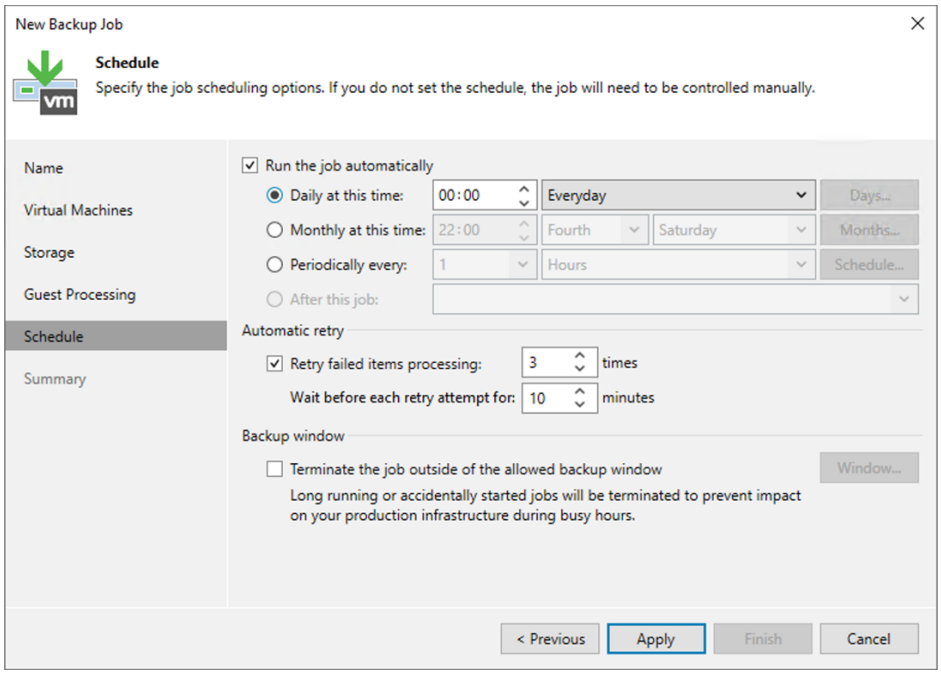


Ensuite, dans l'onglet **Storage**, je définis le dépôt de destination, en l'occurrence le **Backup Repository NAS**, configuré précédemment via le disque iSCSI monté.

Dans les **paramètres avancés**, je spécifie que des **sauvegardes complètes (Full Backup)** doivent être exécutées chaque **samedi**, et que la **compression** doit être réglée sur **High** afin d'optimiser l'espace utilisé, étant donné que l'espace disponible est limité à **750 Go**. J'applique une stratégie de rétention de **7 points de sauvegarde**, permettant ainsi de conserver les sauvegardes des 7 derniers jours.

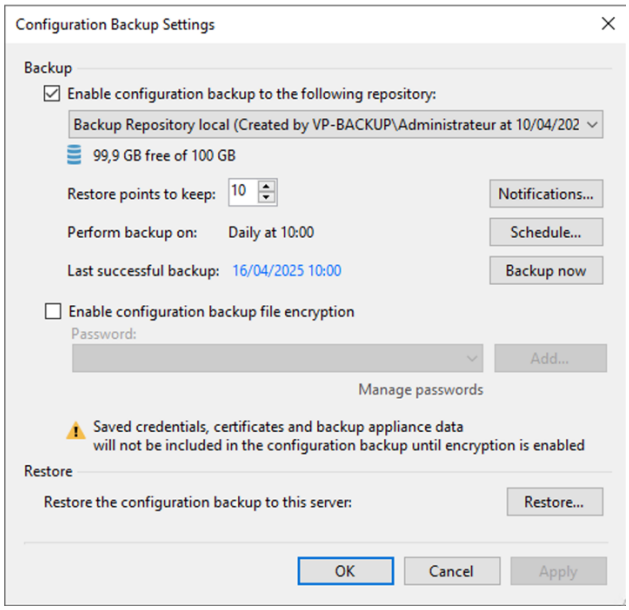


Enfin, dans l'onglet **Schedule**, je planifie l'exécution du job **tous les jours à minuit**, une heure stratégique où l'infrastructure n'est pas sollicitée, garantissant ainsi de meilleures performances de sauvegarde.

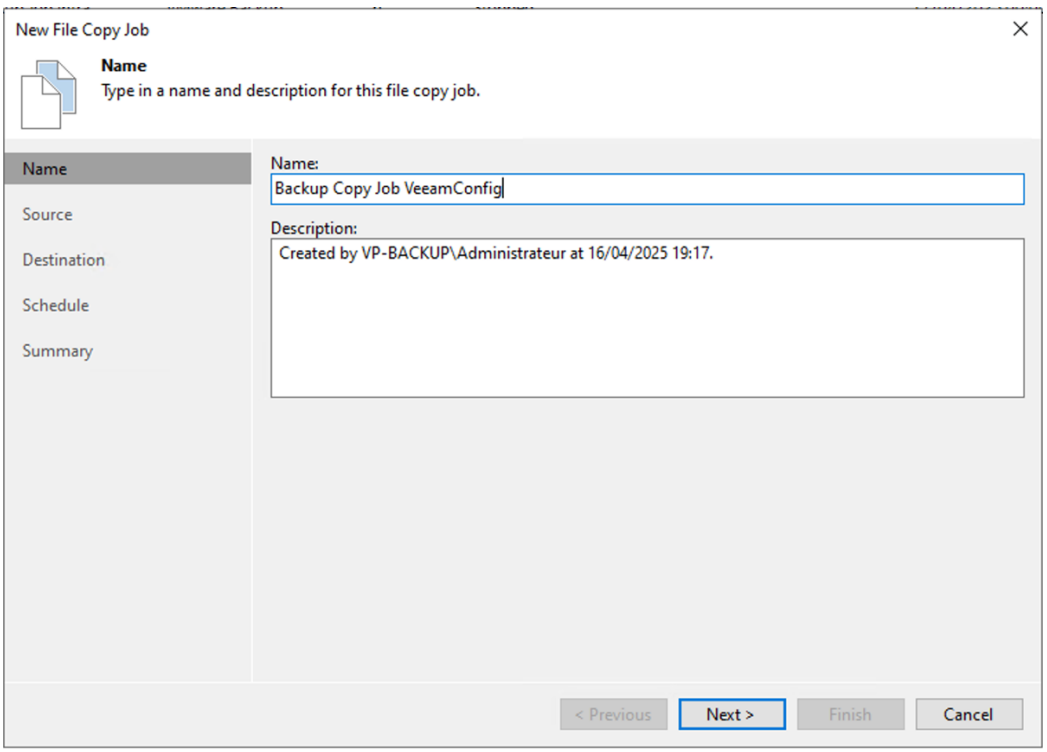


Job secondaire : sauvegarde du fichier de configuration Veeam

En complément, je mets en place un **job de type fichier (File Backup Job)**, dédié à la **sauvegarde du fichier de configuration de Veeam**. Par défaut, ce fichier est sauvegardé sur le disque local **C:**, mais j'ai modifié ce chemin pour qu'il soit redirigé vers le lecteur **Z:**, correspondant au dépôt local.



De plus, afin d'assurer une **redondance**, je copie également ce fichier de sauvegarde vers le NAS, ce qui permet de le restaurer facilement en cas de perte ou de corruption du serveur principal.



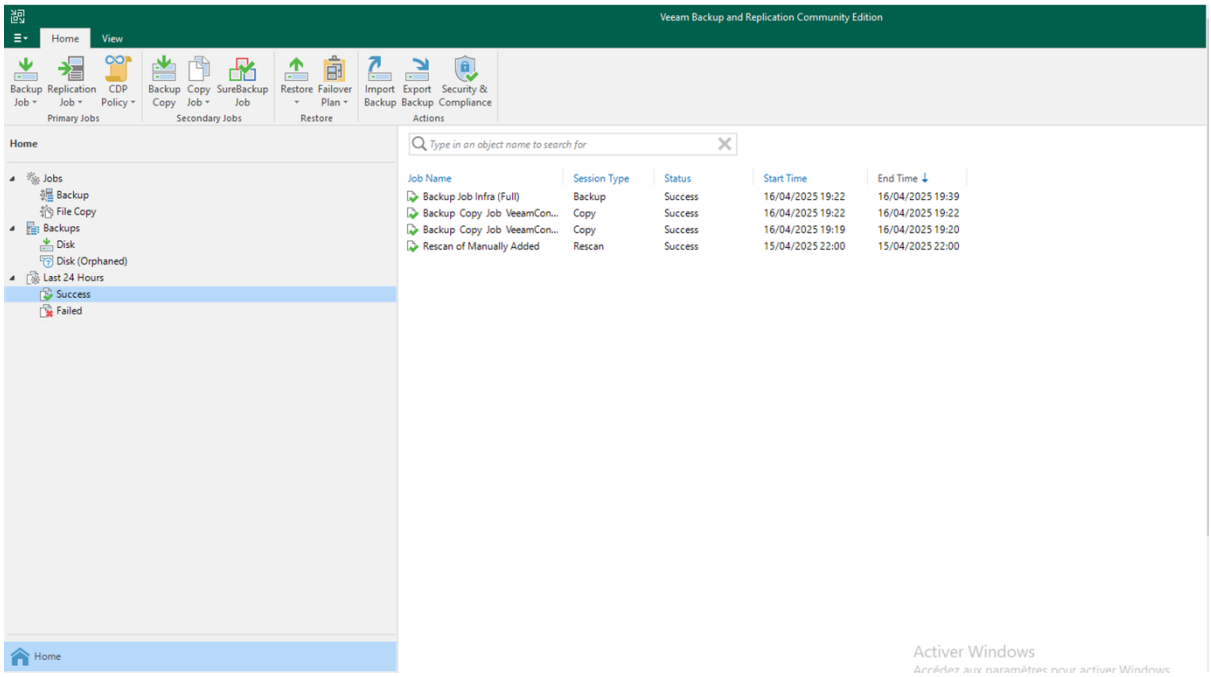
Partie 2 – Validation

Lancement des jobs

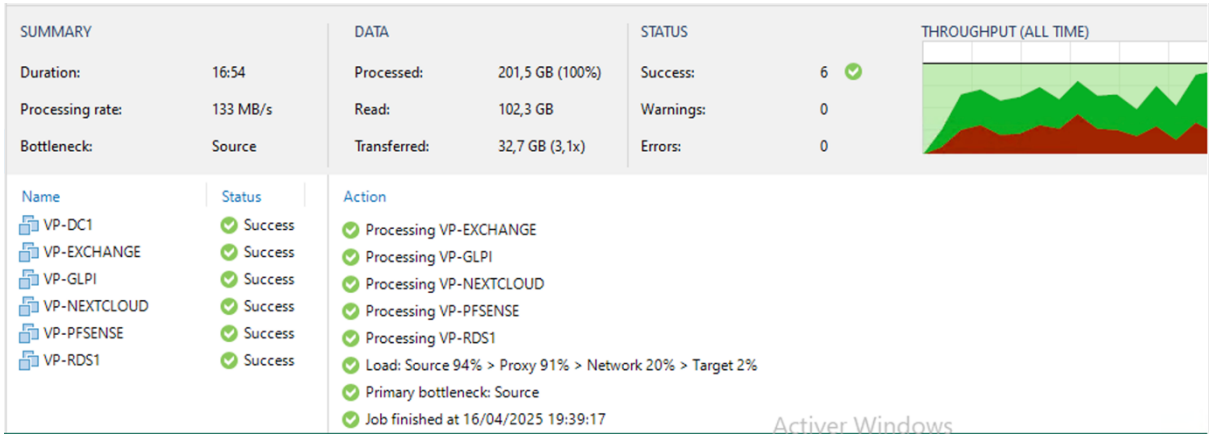
Pour m'assurer du bon fonctionnement de la solution mise en place, je lance manuellement les jobs de sauvegarde afin de valider l'ensemble du processus, ainsi que la connectivité avec le disque iSCSI.

Une fois les jobs terminés, je consulte l'interface de Veeam, dans l'onglet "Last 24 Hours", où apparaît l'historique des tâches exécutées. J'y retrouve notamment :

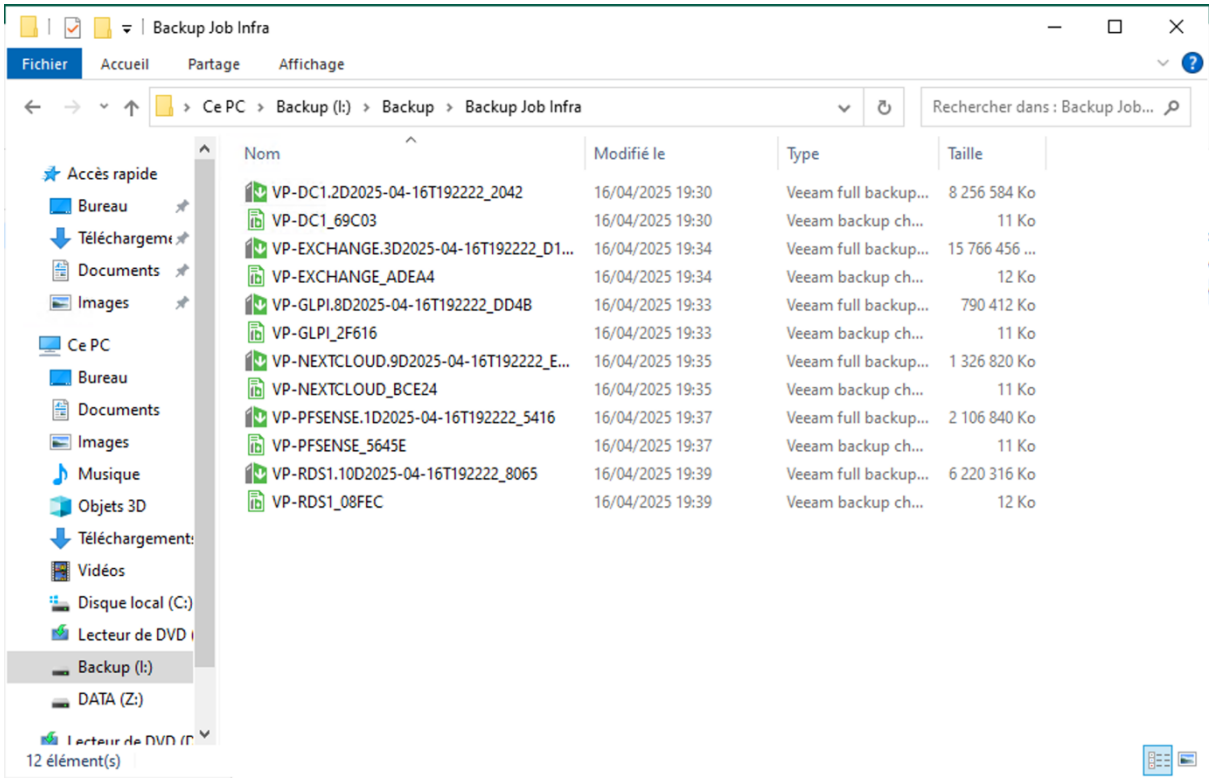
- Le job principal "Backup Job Infra", correspondant à la sauvegarde complète des machines virtuelles.
- Le job secondaire "Backup Copy Job VeeamConfig", qui contient le fichier de configuration de Veeam.



En double-cliquant sur "Backup Job Infra", je peux accéder au détail de la tâche. Toutes les machines virtuelles apparaissent avec le statut "Success", ce qui confirme que la sauvegarde s'est déroulée correctement.



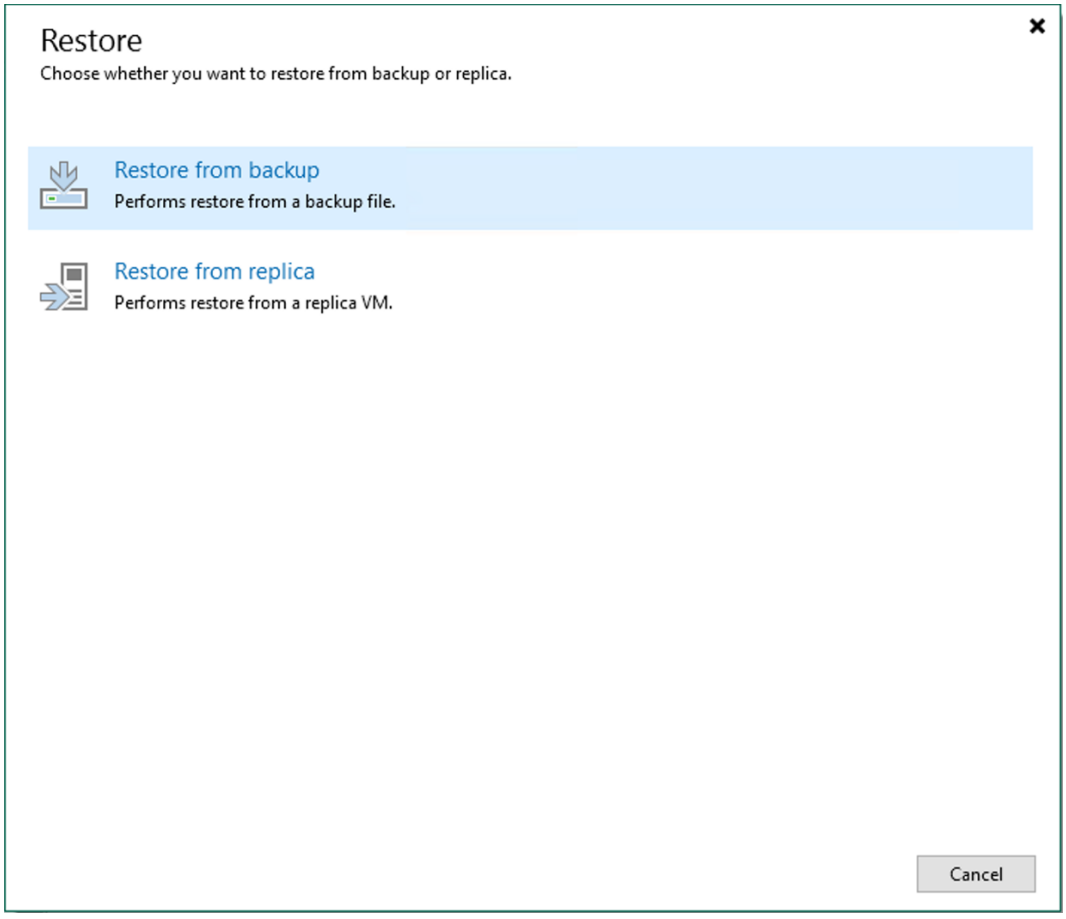
Pour une dernière vérification, je me rends dans l'explorateur de fichiers, dans le répertoire de destination du NAS. Je retrouve bien les fichiers de sauvegarde complète (Full Backup) générés par Veeam, ce qui valide à la fois le bon fonctionnement du job, du repository, et de la connexion iSCSI.



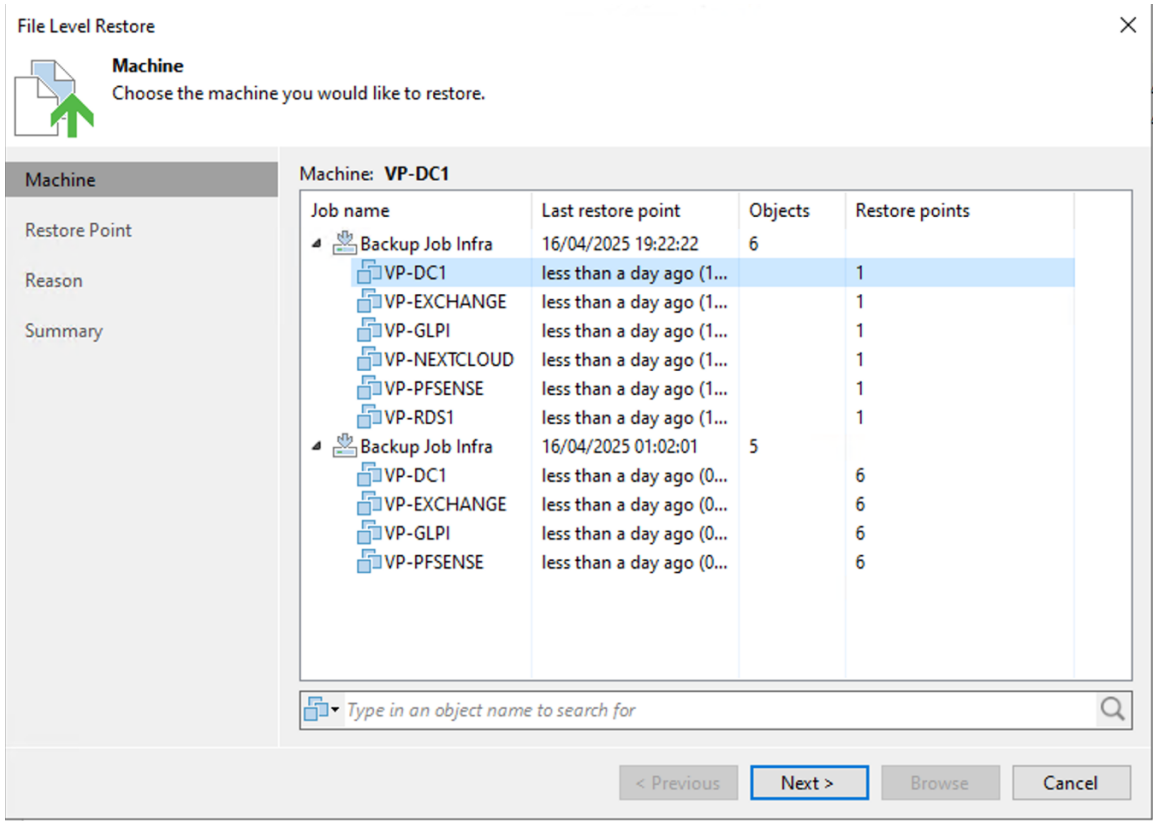
Test de restauration

Pour compléter la validation du système de sauvegarde, je procède à un test de restauration de fichiers. Bien qu'il soit également possible de restaurer une machine virtuelle complète, la restauration d'un fichier individuel permet déjà de confirmer que l'ensemble du processus (sauvegarde, stockage, accès et restauration) fonctionne correctement.

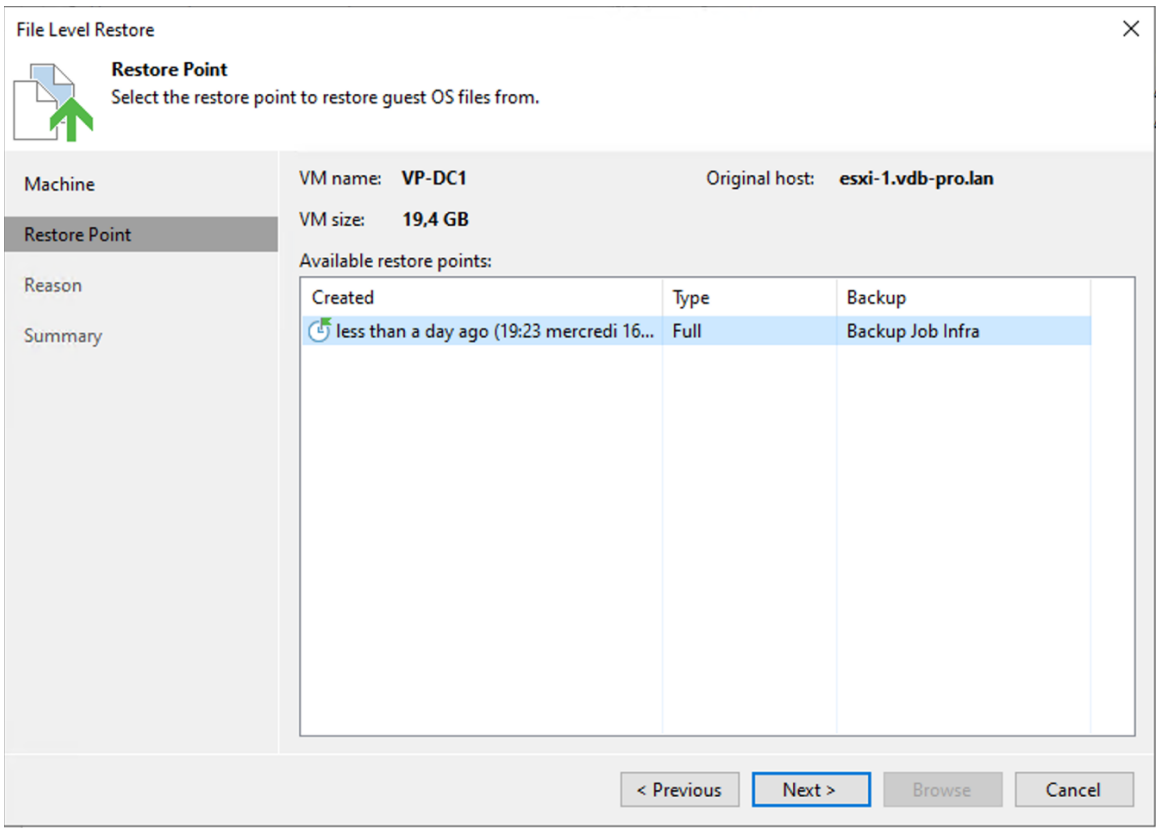
Depuis l'interface de Veeam, je clique sur "Restore", puis je sélectionne "Restore from Backup". Dans les options proposées, je choisis "Guest Files Restore", puis "Microsoft Windows", afin de restaurer un fichier à l'intérieur d'une machine virtuelle Windows.



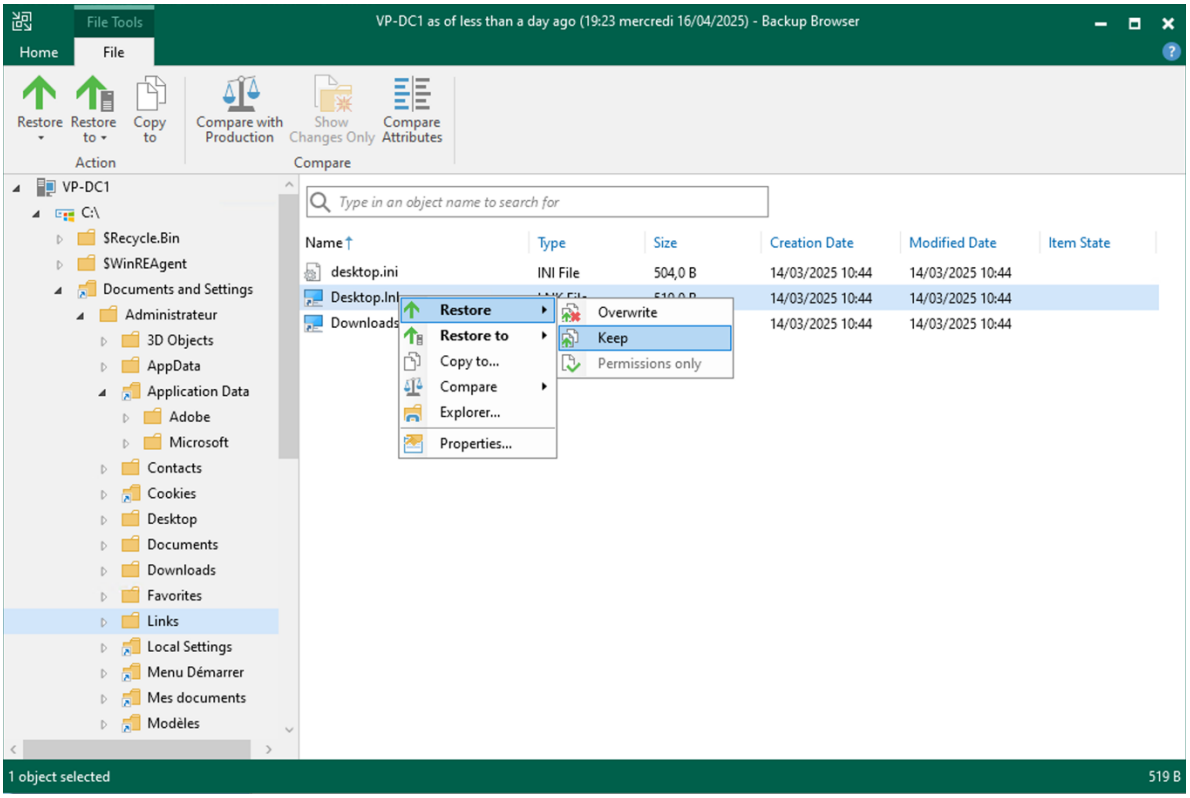
La liste des machines sauvegardées s'affiche. Pour ce test, je sélectionne la VM VP-DC1.

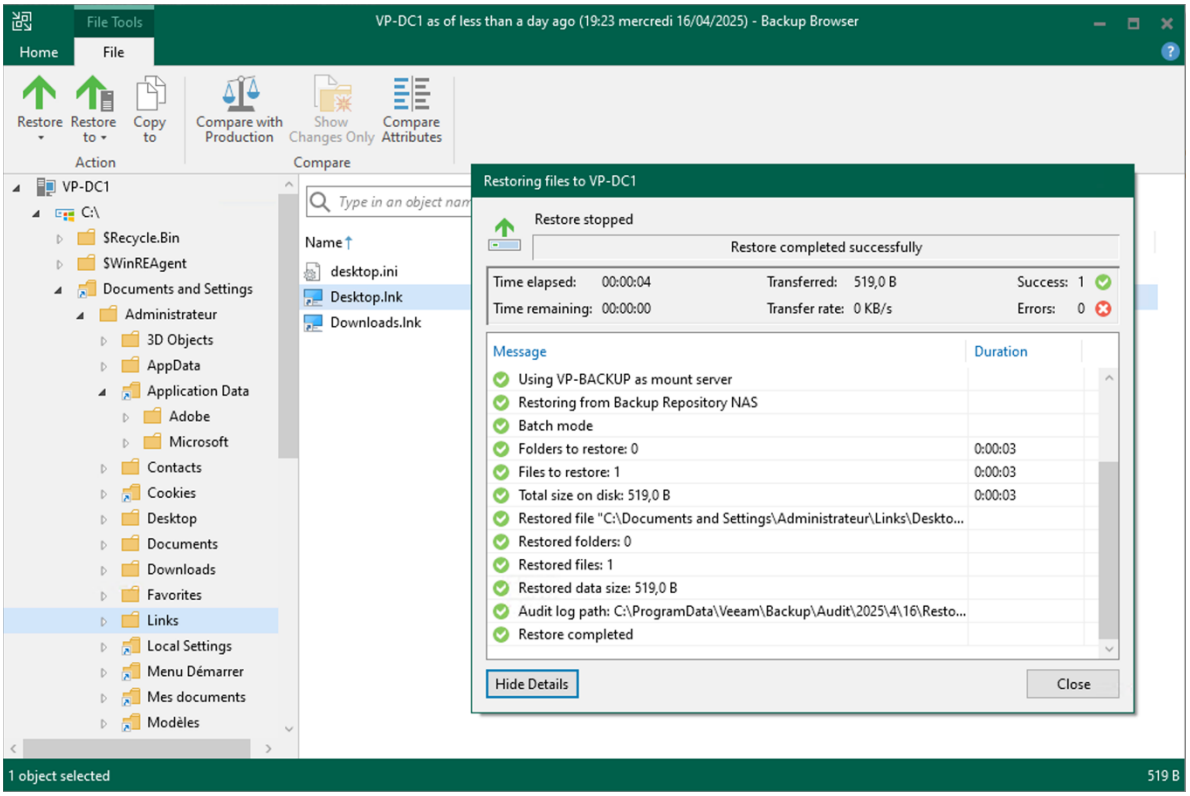


Je choisis le point de restauration le plus récent.

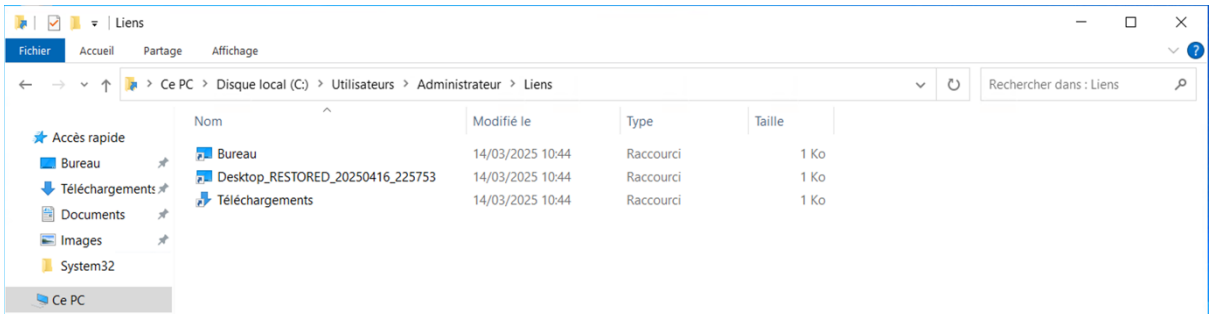


je sélectionne un fichier aléatoire, en l'occurrence un raccourci sur le bureau. Lors de la restauration, je choisis l'option "Keep" pour conserver l'ancienne version du fichier tout en restaurant la nouvelle, afin de ne pas écraser d'éventuelles données existantes.





Après la restauration, je me connecte à la machine VP-DC1. Le fichier restauré est bien présent, ce qui confirme le bon fonctionnement du processus de sauvegarde et de restauration via Veeam.



Partie 3 – Veille Technologique

Dans le cadre de la mise en place d'une infrastructure de sauvegarde, il est essentiel de s'informer sur les outils disponibles et les évolutions technologiques du secteur. Pour mon projet, j'ai utilisé Veeam Backup & Replicationcomme solution de sauvegarde, associé à TrueNAS pour le stockage réseau. Ces outils sont très performants, mais il existe aujourd'hui plusieurs alternatives intéressantes, à la fois open source, plus légères ou moins coûteuses.

Côté logiciels de sauvegarde, Veeam est une référence sur le marché pour les environnements VMware et Hyper-V. Il offre une interface intuitive, des options avancées (rétention, compression, restauration granulaire) et une excellente fiabilité. Toutefois, des solutions comme Nakivo Backup & Replication proposent une approche similaire à moindre coût, avec une interface web et un bon support multi-hyperviseur. Pour des environnements plus simples, UrBackup ou Bacula/Bareos permettent de mettre en place des systèmes de sauvegarde efficaces en open source. Acronis Cyber Protect, de son côté, combine sauvegarde et cybersécurité dans une seule solution.

Concernant le stockage réseau, TrueNAS se distingue grâce à son système de fichiers ZFS, sa robustesse et son interface web complète. Il est idéal pour gérer un NAS virtualisé ou physique. En alternative, OpenMediaVault est une option plus légère et facile à prendre en main, bien adaptée aux petites structures. Des solutions comme XigmaNAS, Rockstor ou encore UnRAID peuvent également répondre à des besoins spécifiques, comme la virtualisation ou la gestion flexible des disques.

Les tendances actuelles (2024–2025) montrent une montée en puissance des solutions hybrides, combinant sauvegarde locale et stockage cloud (Backblaze, Wasabi, AWS S3), ainsi qu'un intérêt croissant pour les sauvegardes sécurisées contre les ransomwares (backups immuables, snapshots ZFS). On observe aussi une intégration progressive de l'intelligence artificielle pour optimiser la gestion des sauvegardes, et une démocratisation des outils de sauvegarde de conteneurs (Kubernetes, Docker) dans les infrastructures modernes.

En conclusion, il est essentiel de connaître ces outils et évolutions afin de rester compétent dans le domaine de la cybersécurité et de l'administration système. Une bonne veille technologique permet de choisir la solution la plus adaptée aux besoins réels de l'entreprise tout en anticipant les futurs enjeux du métier.