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.

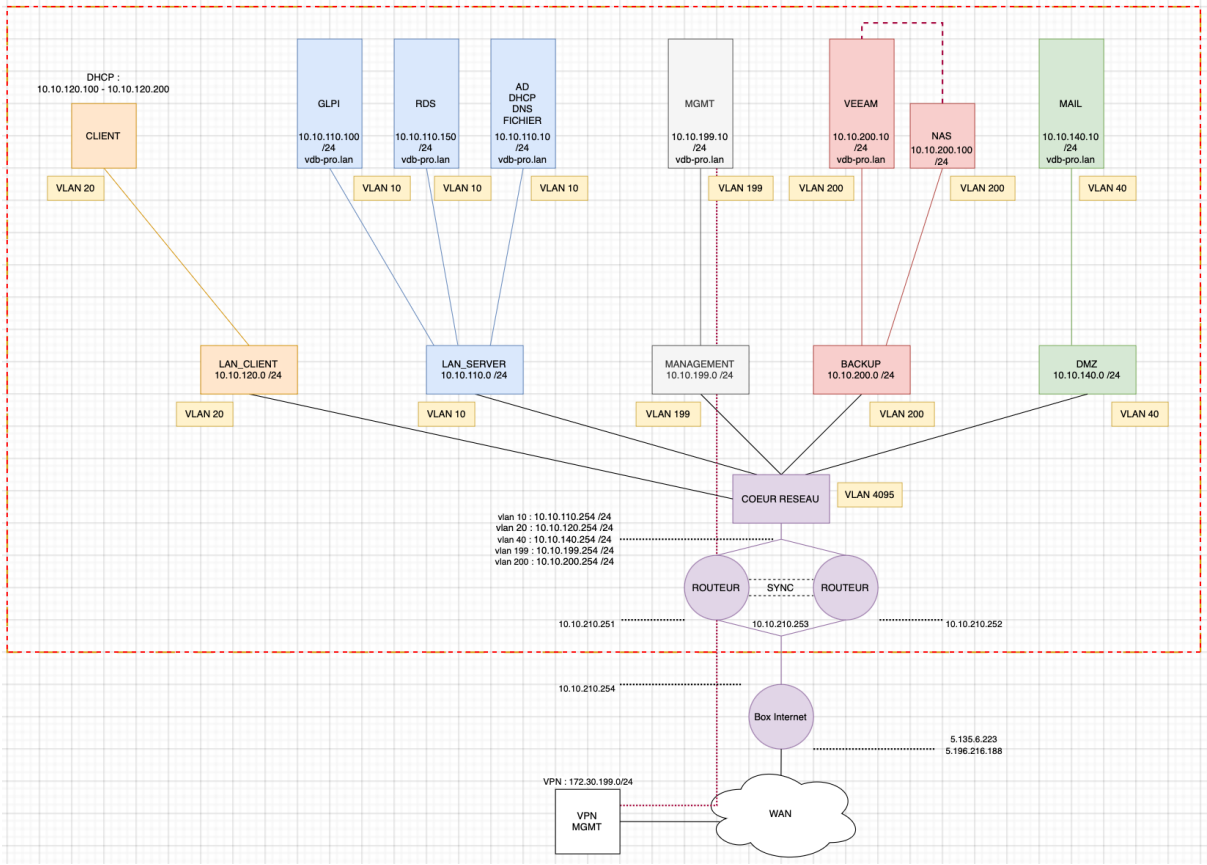
https://portfolio.vdb-pro.fr mdp : *Cyb3r-M@P89$*

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.

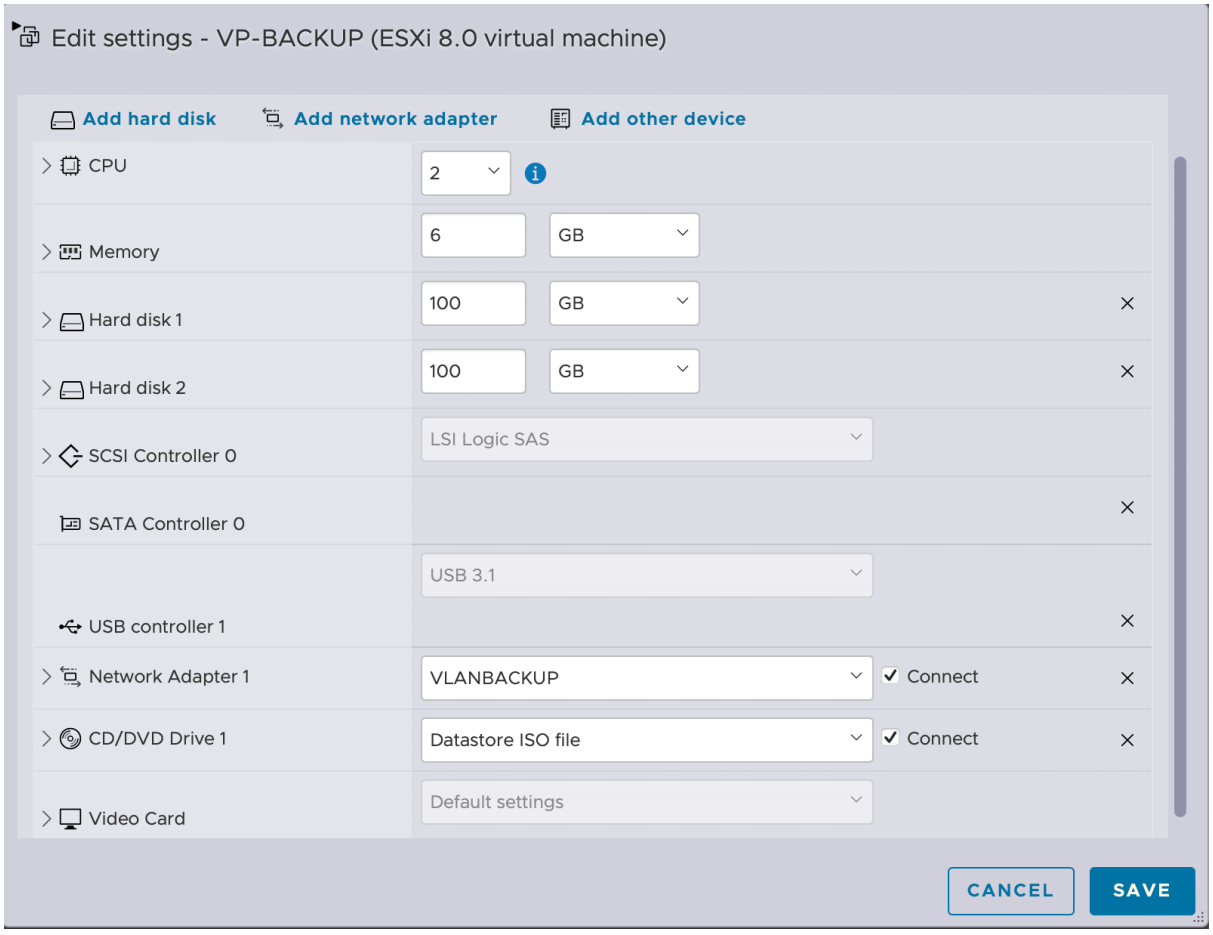
Dans une logique d'optimisation et d'ouverture technologique, une **veille** a également été réalisée afin d'identifier les alternatives existantes et les tendances actuelles du secteur.



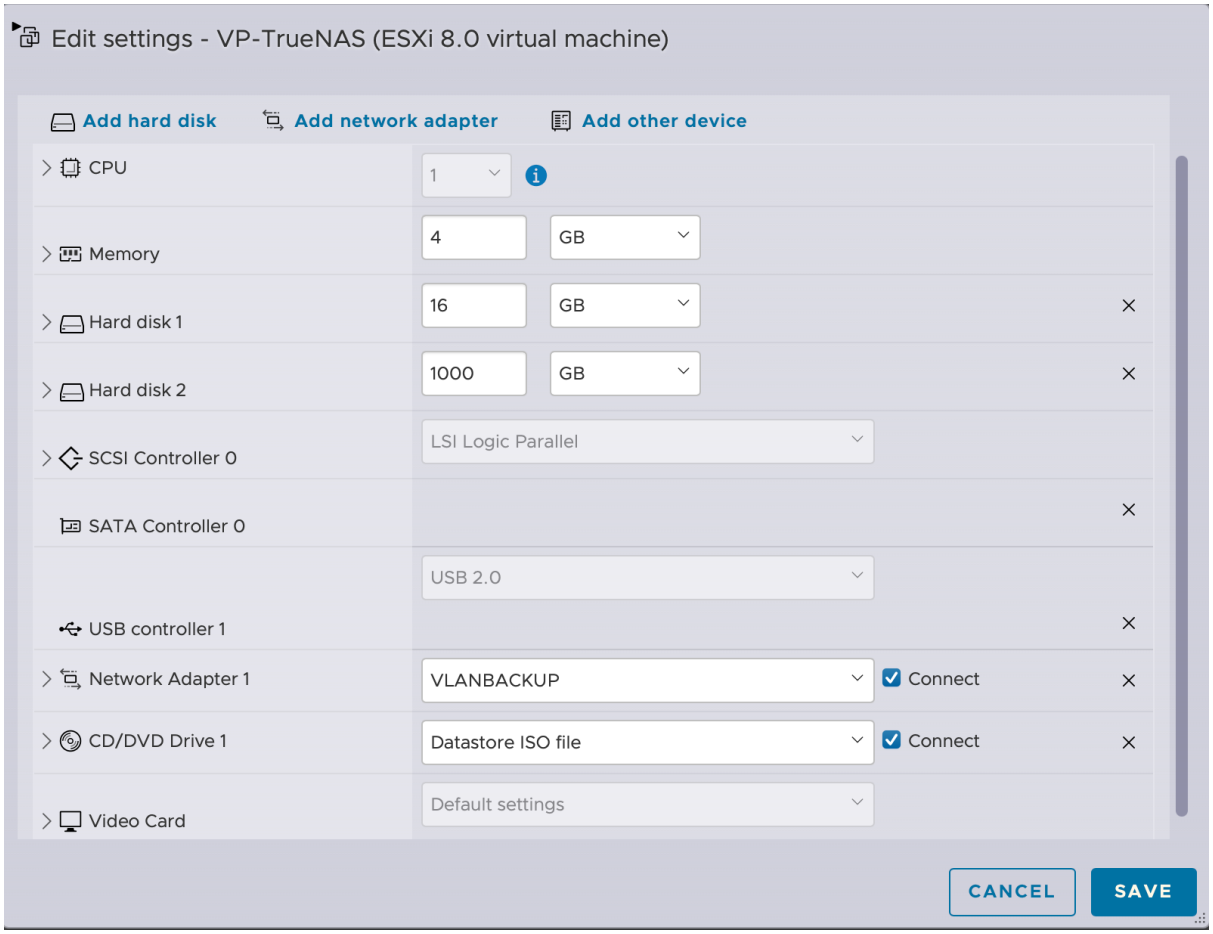
Création des machines virtuelles

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	

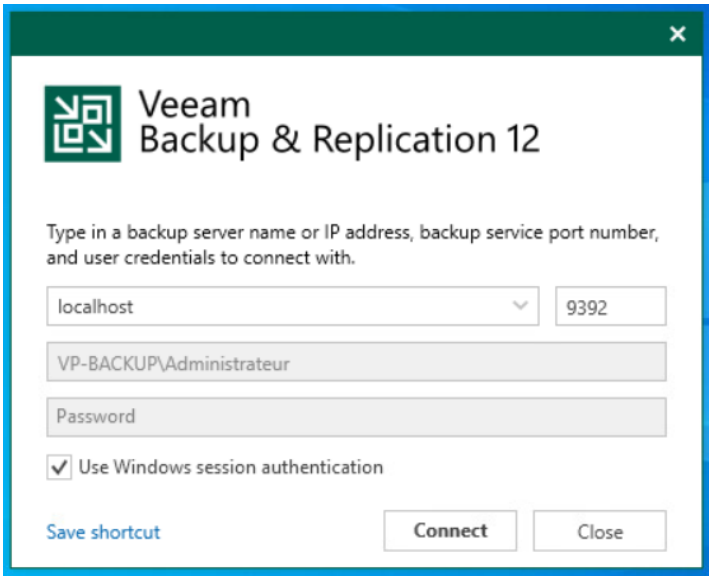
Par souci de sécurité et de cloisonnement, le serveur de sauvegarde n'est pas intégré au domaine Active Directory. Il fonctionne en autonomie avec un compte administrateur local protégé par un mot de passe fort. Cette isolation volontaire permet de limiter les risques de propagation en cas de compromission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

Installation de VEEAM Backup and Replication

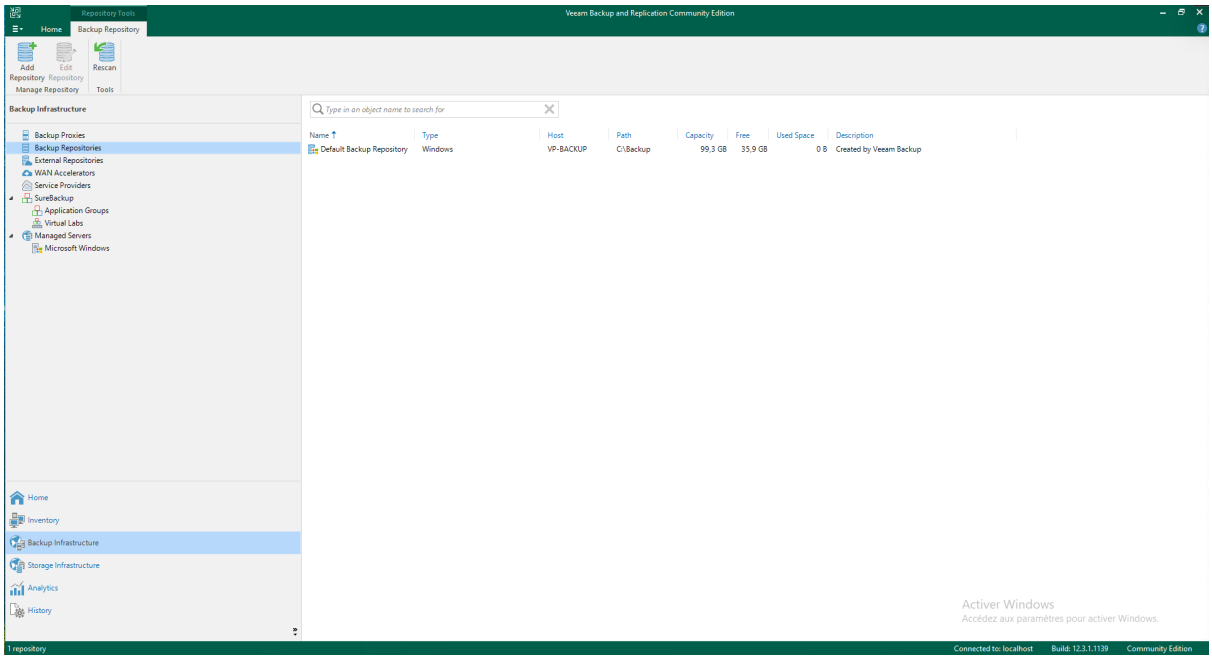
Une fois Windows Server 2022 installé sur la machine virtuelle, je procède au téléchargement de la dernière version de Veeam Backup & Replication, à savoir la version 12.3. Pour cela, je me connecte à mon espace client Veeam afin de récupérer l'ISO officielle. Cette méthode me permet d'installer une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



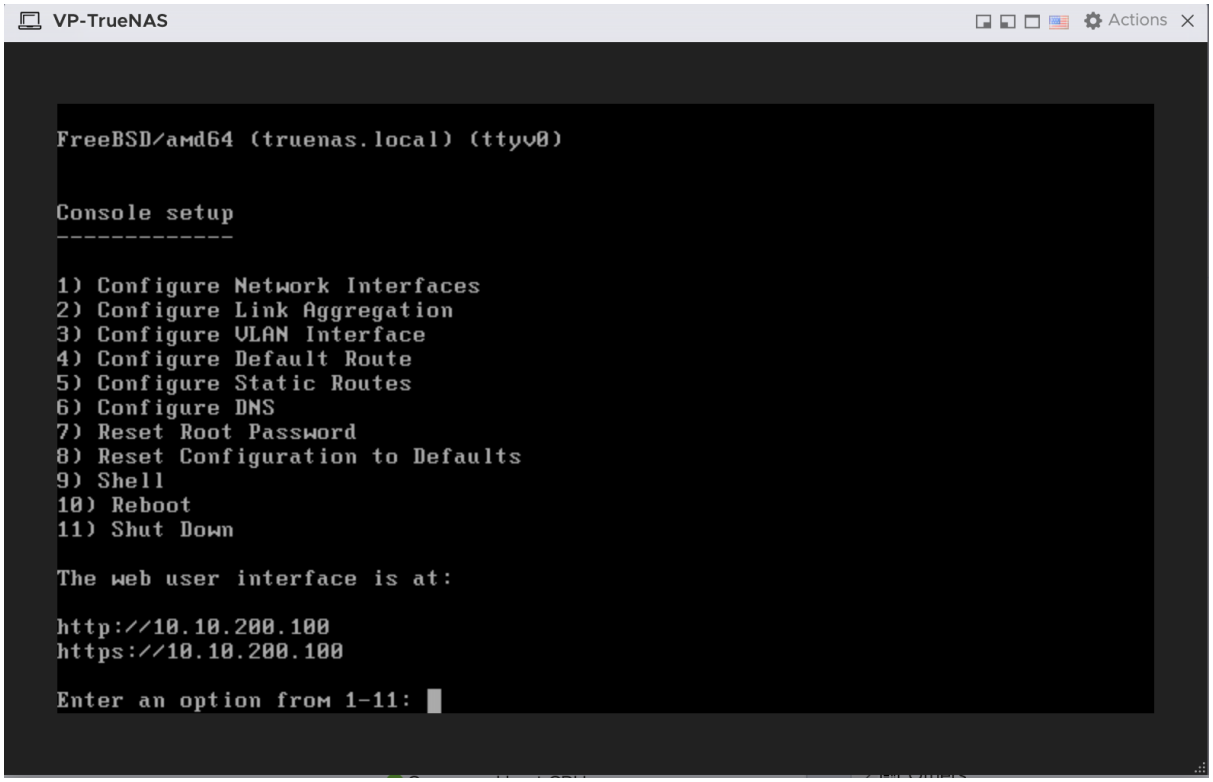
Création d'un stockage via TrueNAS

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.

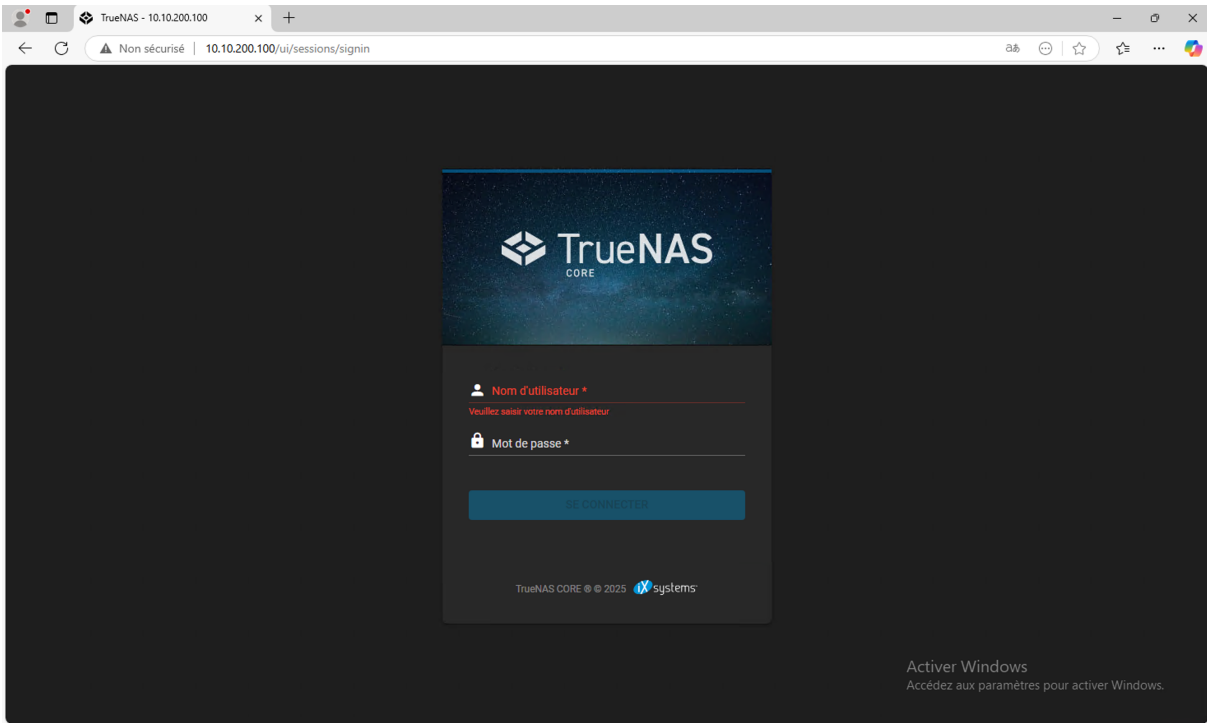
Configuration de TrueNAS en CLI

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.



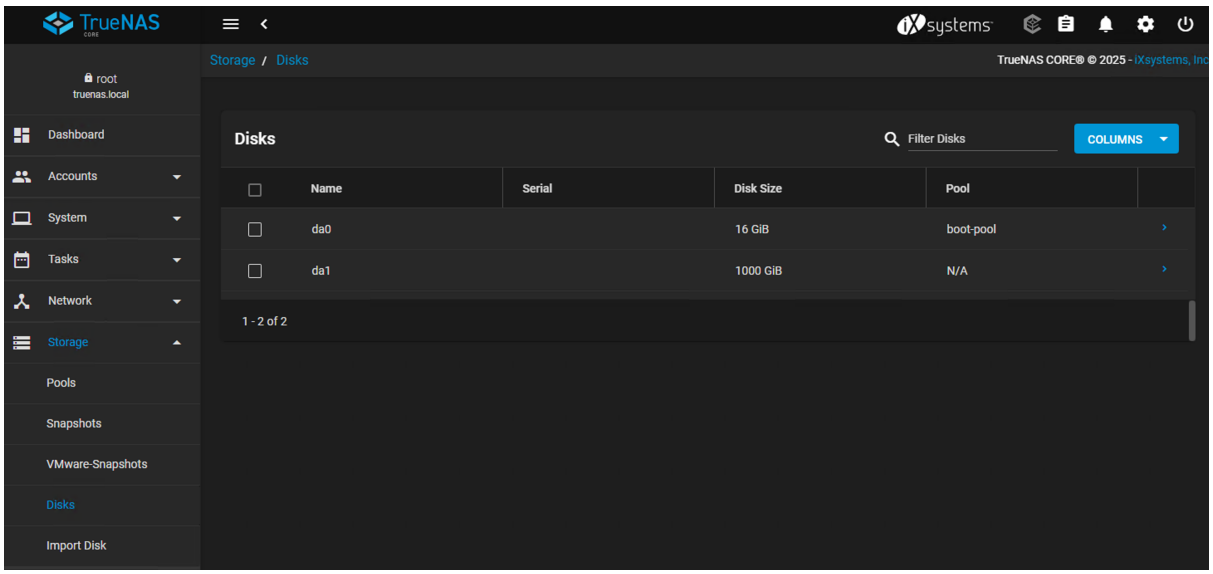
Configuration de TrueNAS en interface web

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.

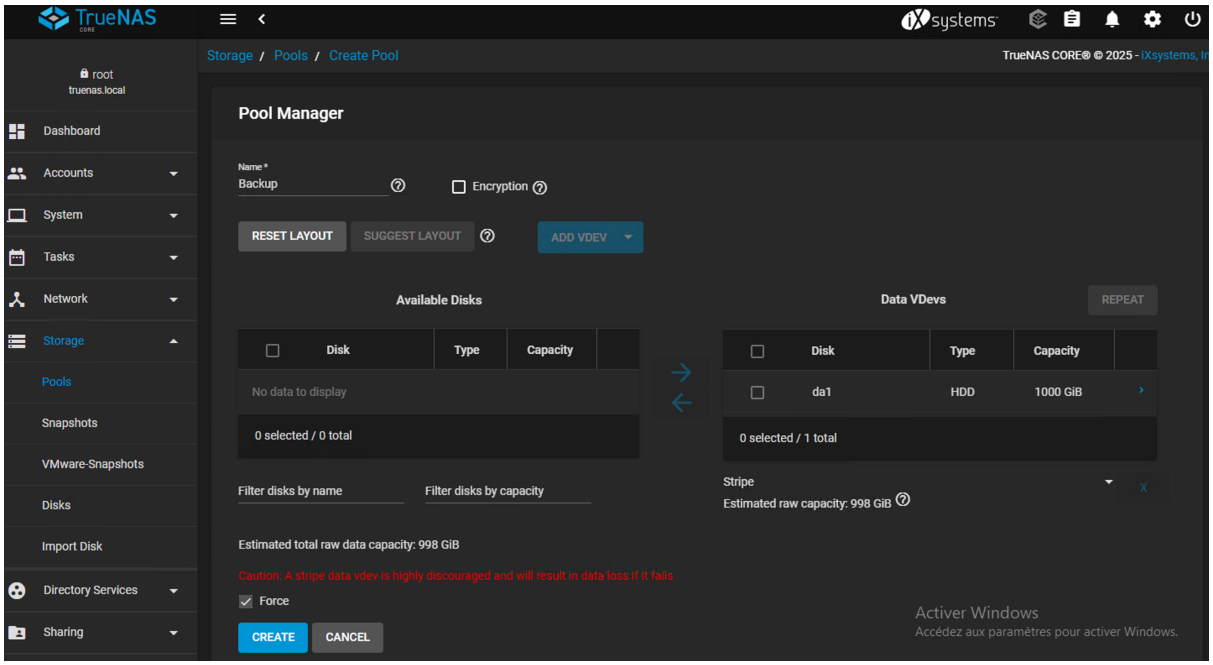


Configuration d'un pool de stockage

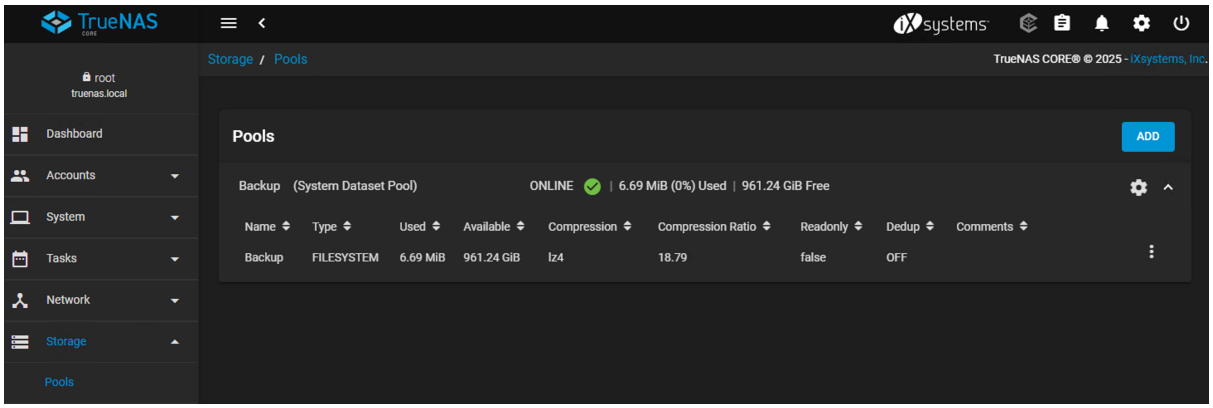
Dans un premier temps, je me rends dans le menu Storage, puis dans la section Disks, afin de vérifier que le disque de 1 To destiné aux sauvegardes est bien détecté par le système.



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.

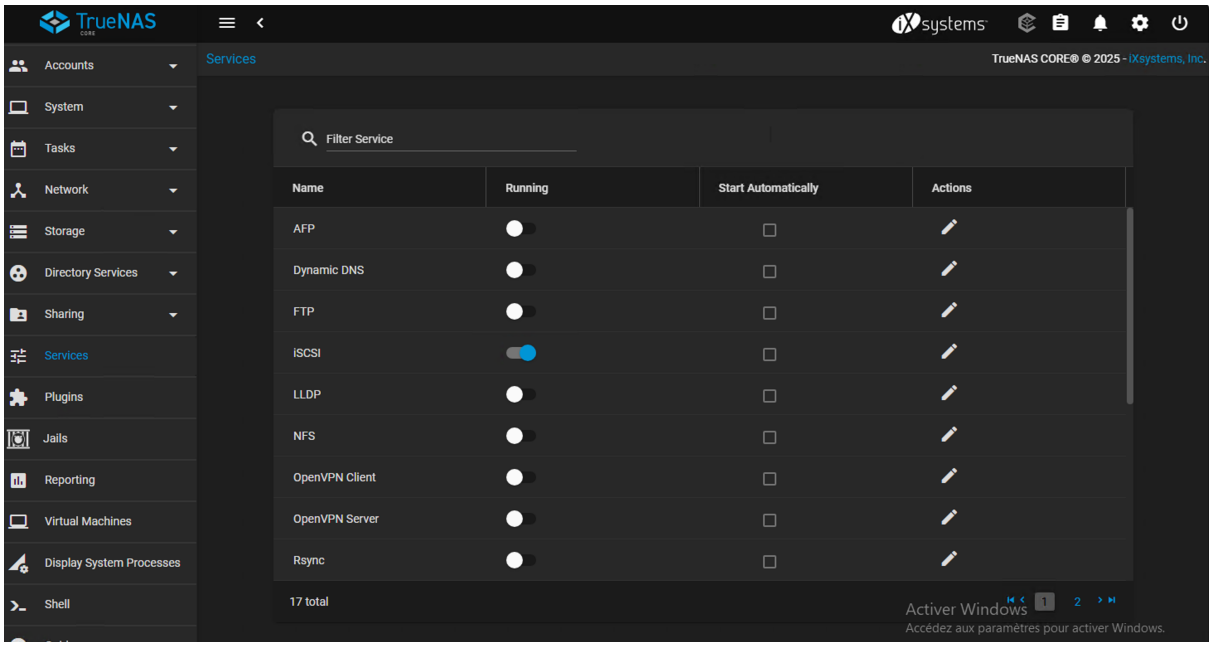


Configuration d'un lien ISCSI

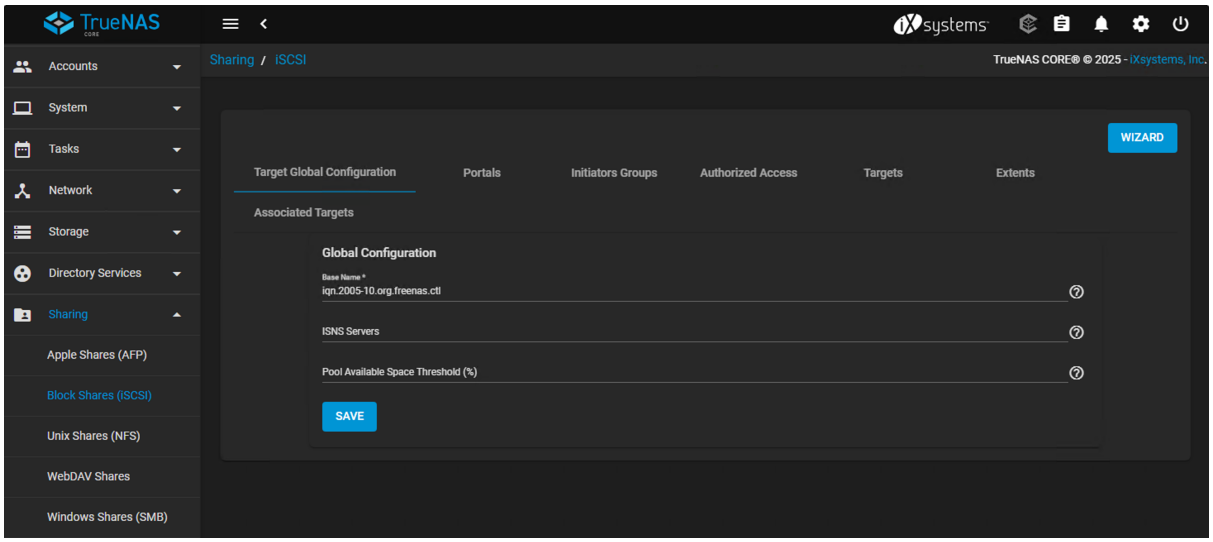
Configuration du service ISCSI sur TrueNAS

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.

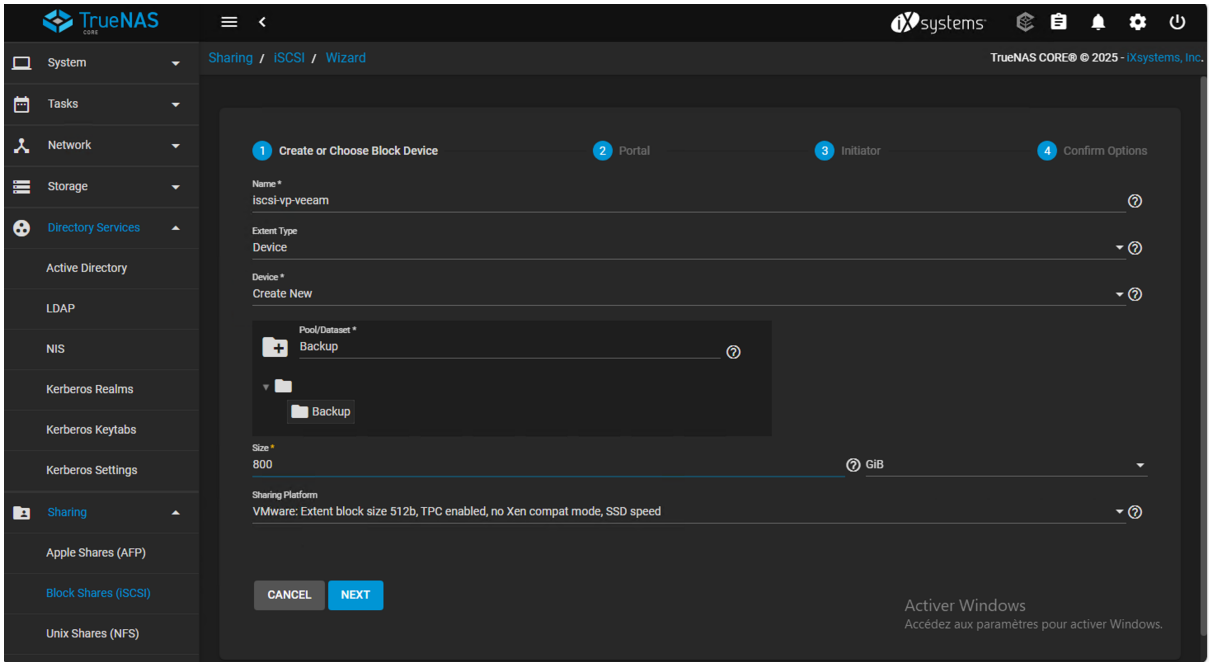
Je me rends dans l'onglet Services, puis j'active le service iSCSI.



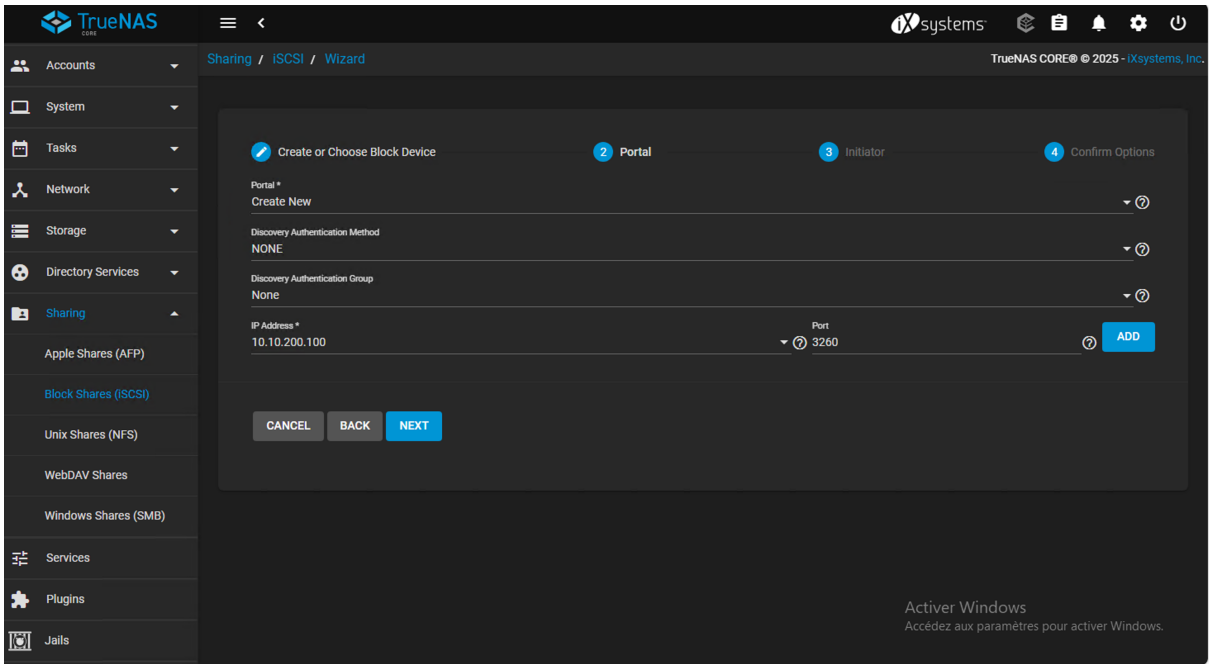
Ensuite, je clique sur l'icône en forme de stylo pour accéder à la configuration, puis je lance l'assistant en cliquant sur Wizard.



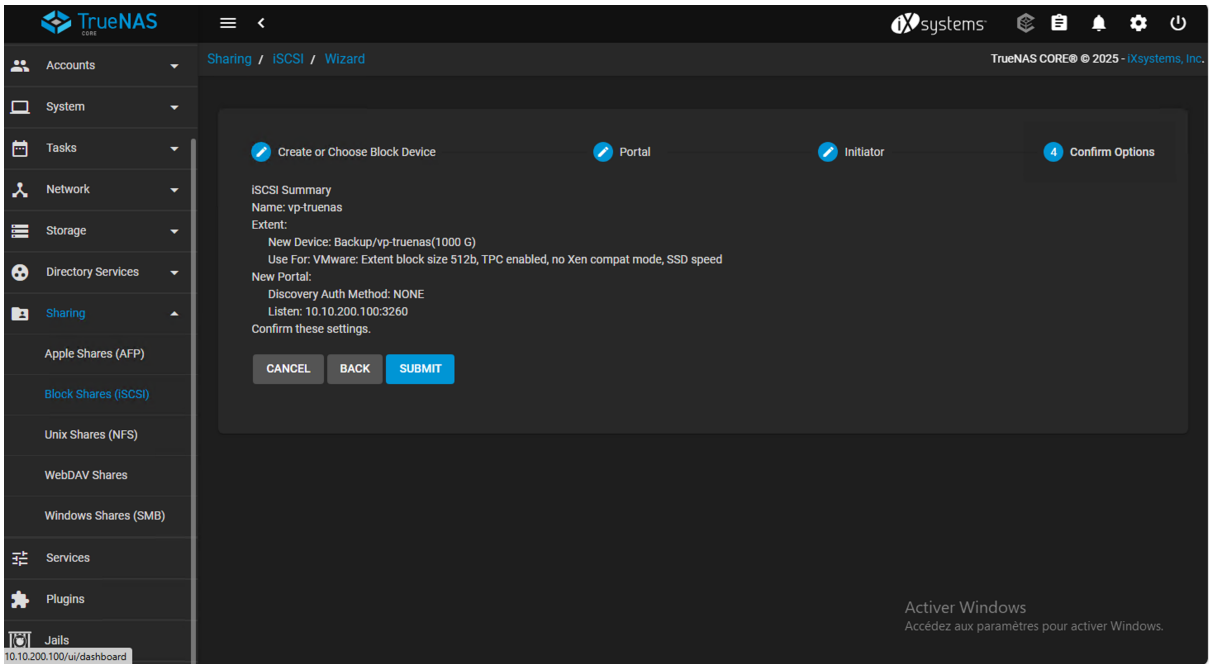
L’assistant me guide dans la création d’un Block Device, c’est-à-dire une unité de stockage en mode bloc. Je définis un nom pour ce bloc, et je lui attribue une capacité de 750 Go, en suivant la recommandation de TrueNAS qui suggère de conserver environ 20 % de l’espace total libre pour garantir de bonnes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



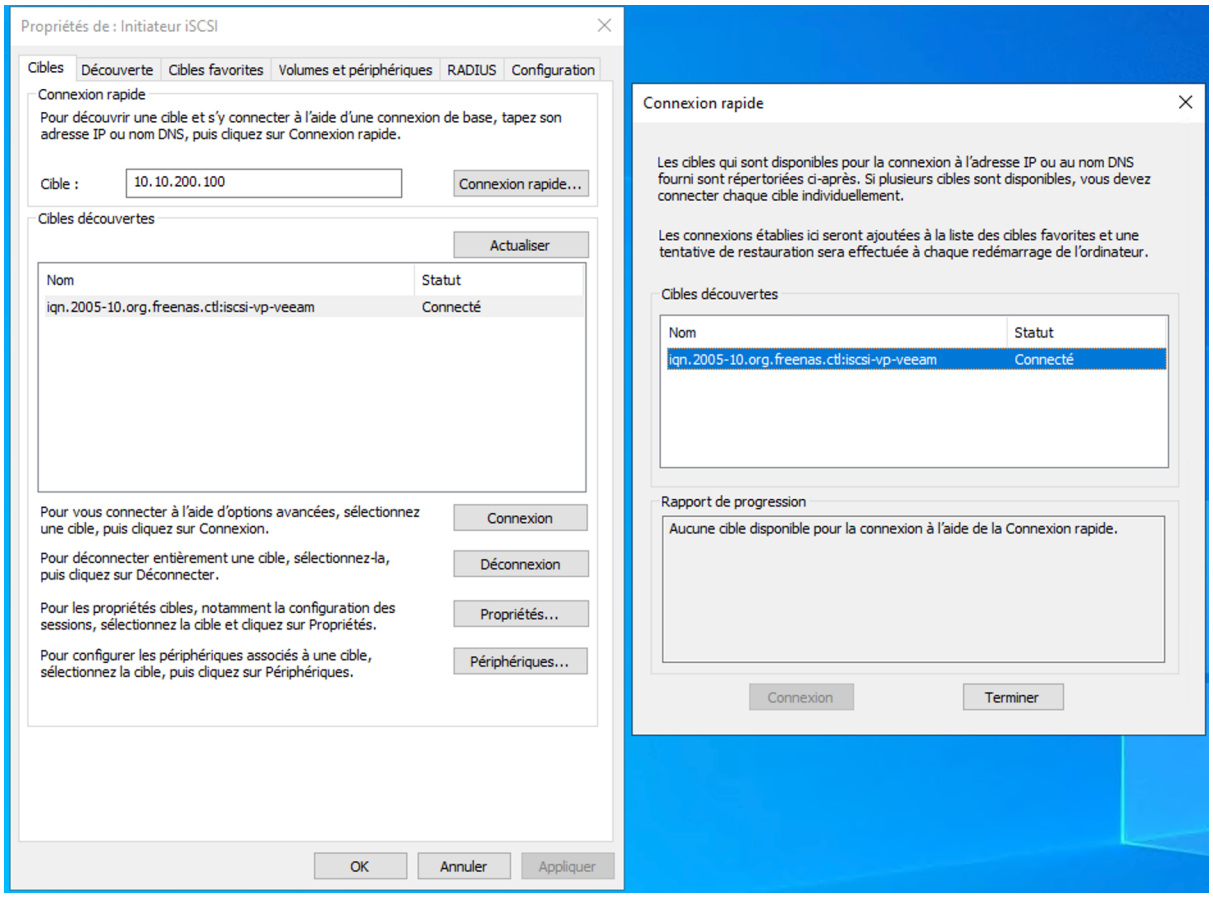
Une fois tous les paramètres renseignés, je clique sur Submit afin de valider et finaliser la configuration. Le service iSCSI est désormais opérationnel et prêt à être monté sur le serveur Veeam.



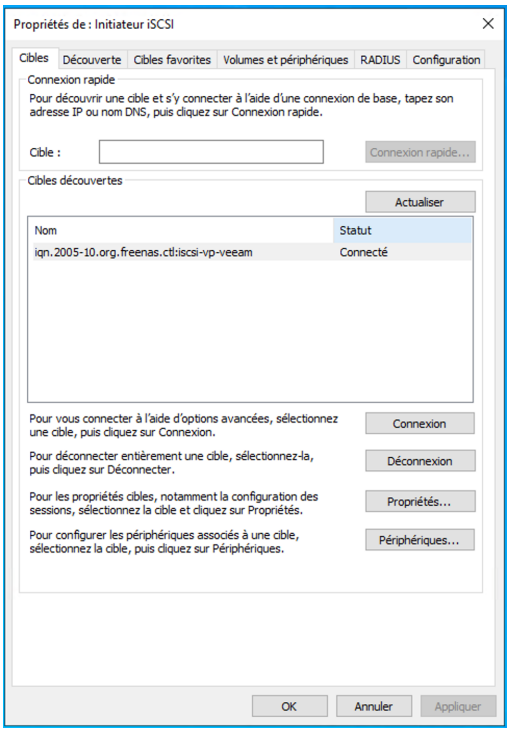
Configuration du service ISCSI sur Windows Server 2022

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



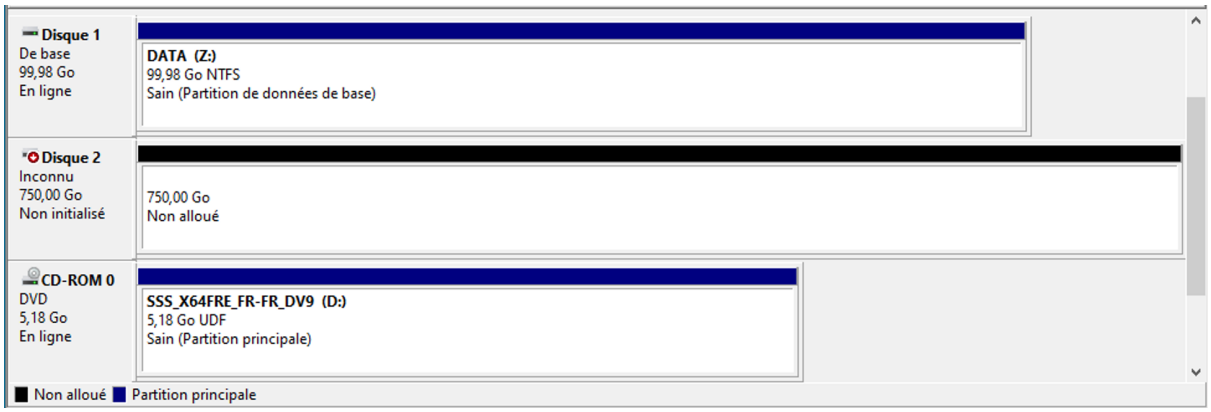
Une fois la cible détectée, je la sélectionne, puis je clique sur Connecter afin d'établir la liaison entre le serveur Windows et le volume iSCSI hébergé sur TrueNAS. Le disque est alors reconnu par le système et prêt à être initialisé et formaté via la gestion des disques.



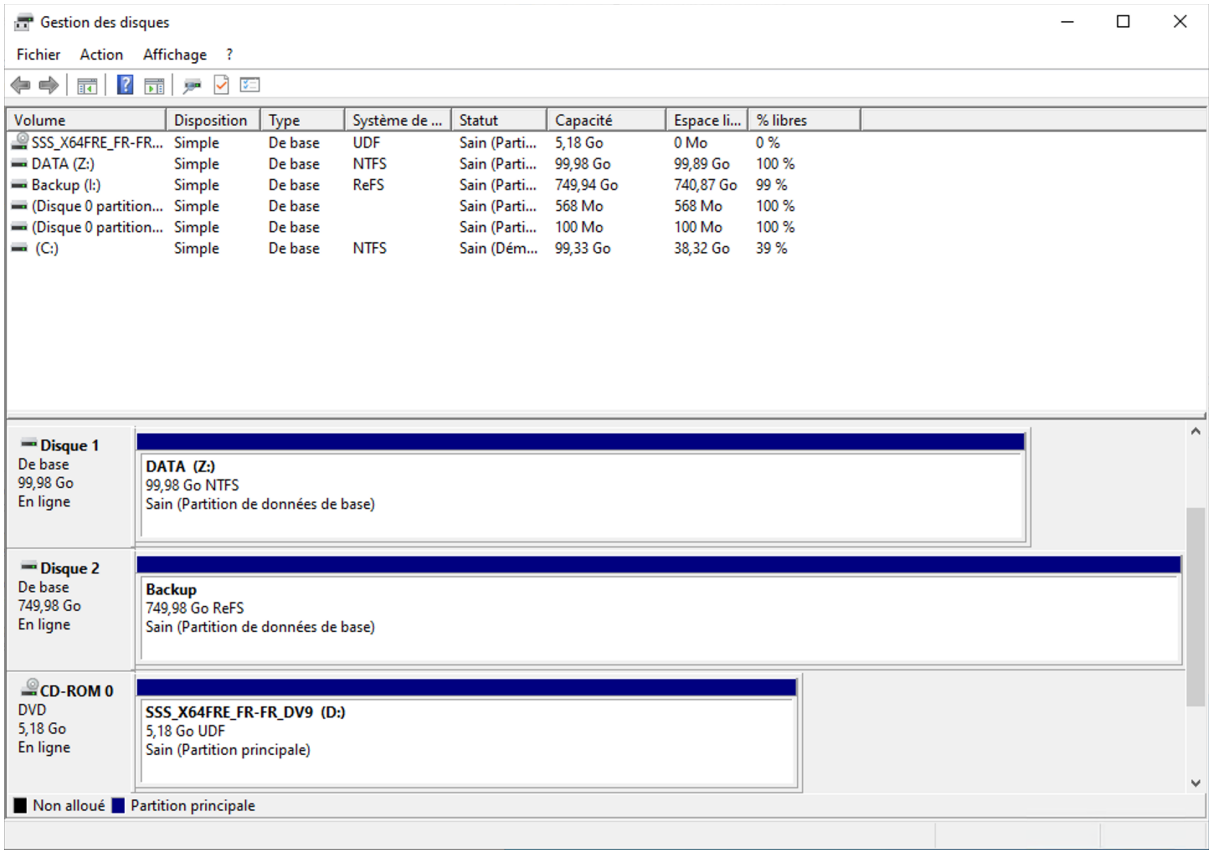
Initialisation du disque iSCSI dans Windows Server

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.



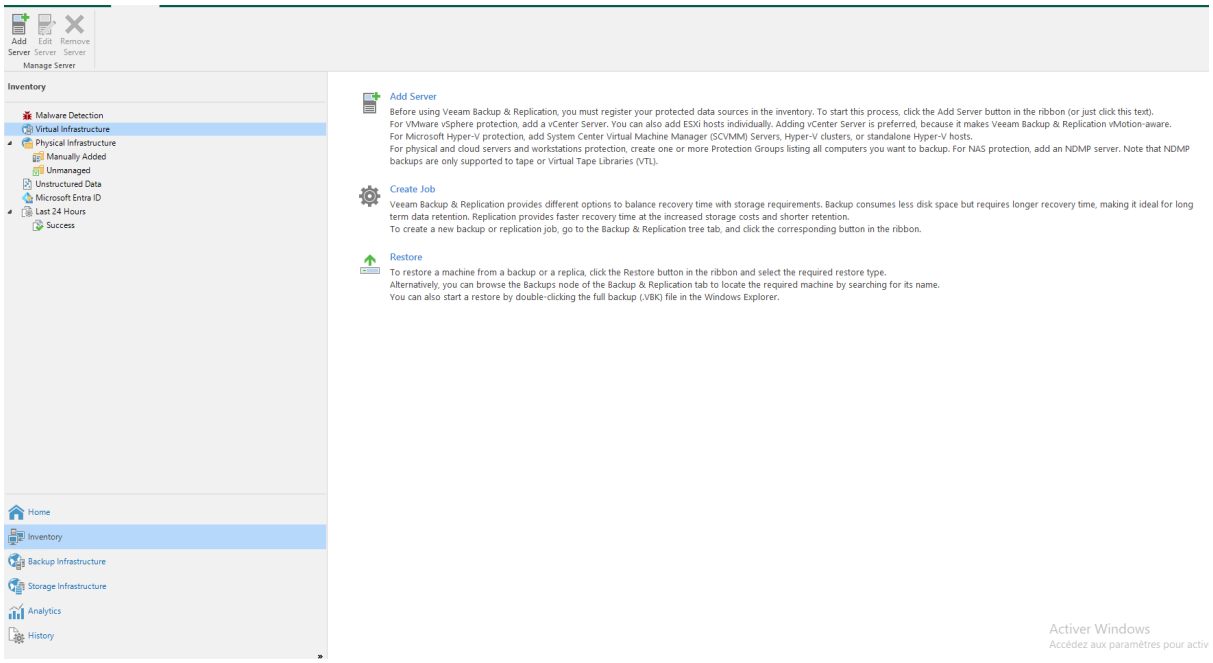
Une fois le volume créé et formaté en ReFS, il est monté dans le système Windows sous forme de lecteur, prêt à accueillir les données de sauvegarde générées par Veeam.

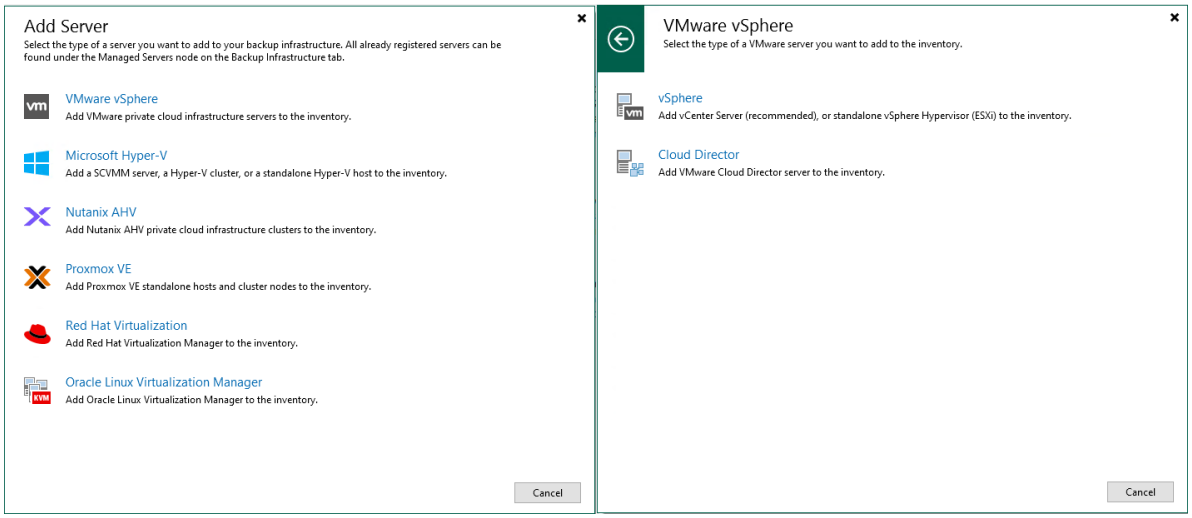


Ajout des cibles de sauvegardes

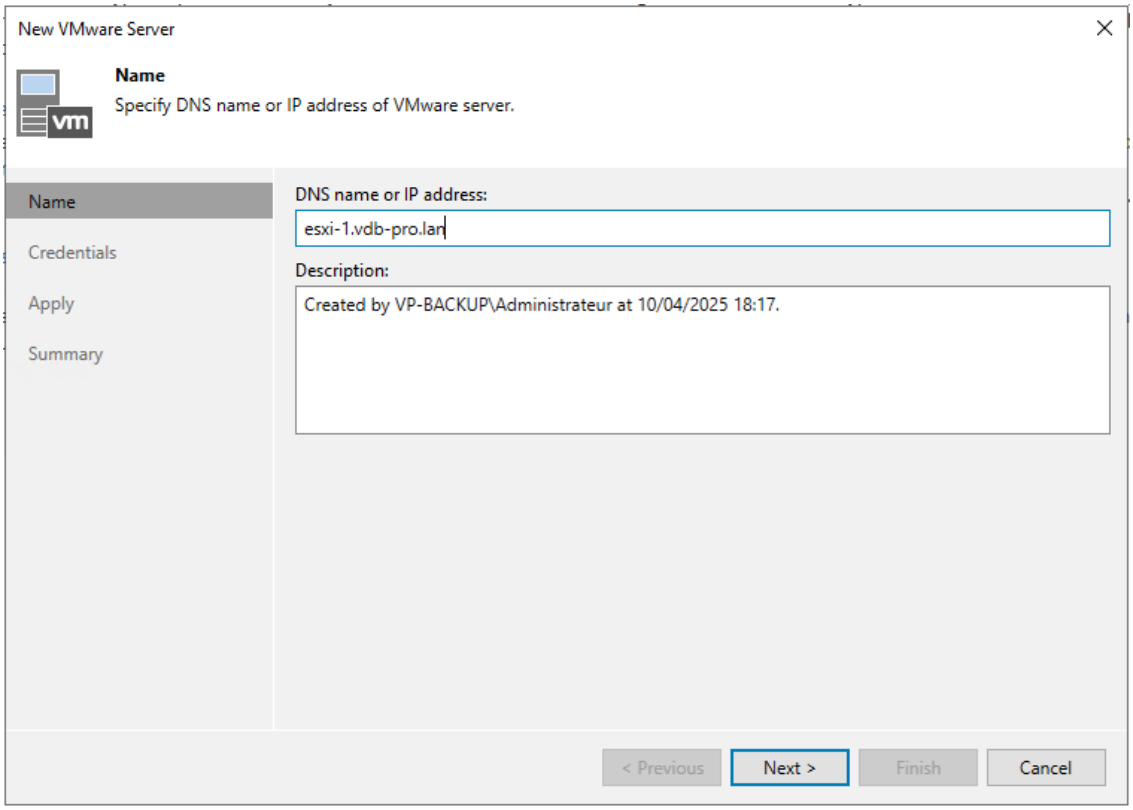
Depuis l'interface de Veeam, les machines virtuelles à sauvegarder sont ajoutées en tant que cibles. Dans ce projet, il s'agit de machines virtuelles hébergées sur un serveur ESXi. L'accès à ces VM est effectué à l'aide des identifiants administrateur, via une connexion sécurisée, ce qui permet à Veeam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

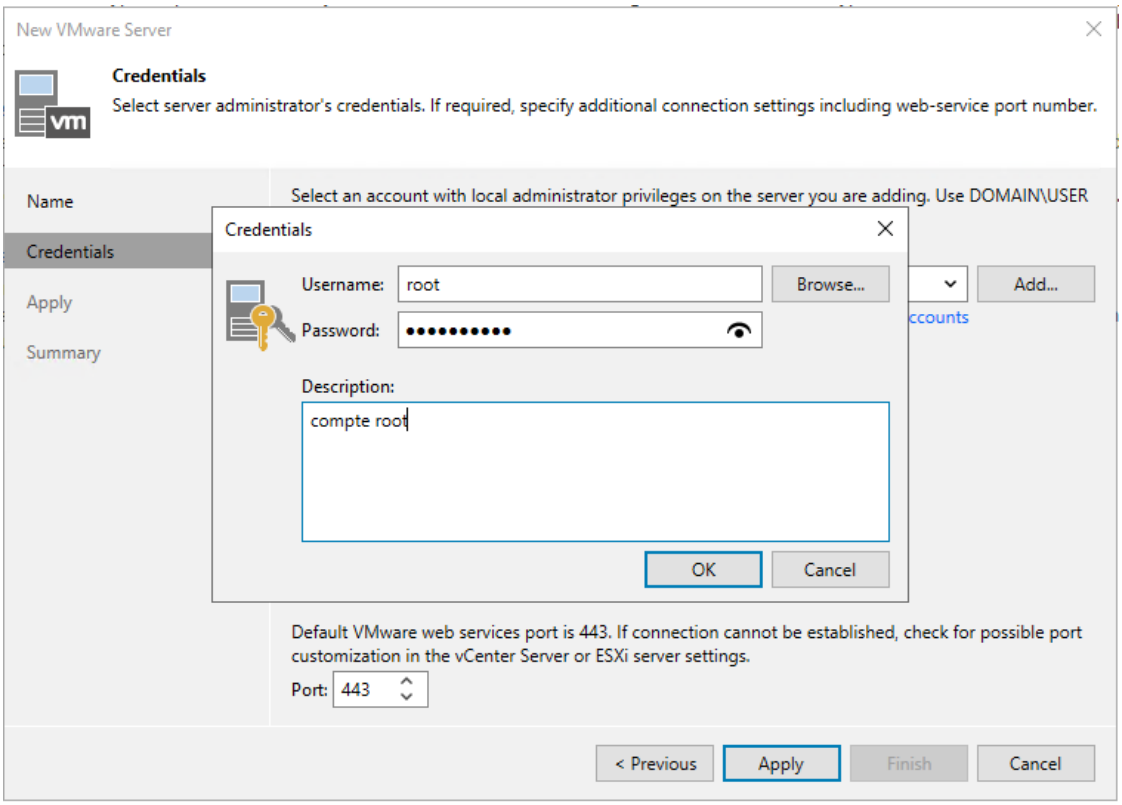
Pour cela, je me rends dans l'onglet Inventory, puis dans la section Virtual Infrastructure. À cet endroit, je procède à l'ajout d'un serveur en sélectionnant l'option VMware vSphere. Deux possibilités s'offrent alors : ajouter un vCenter Server, ou directement un hôte ESXi en standalone. Le vCenter 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.



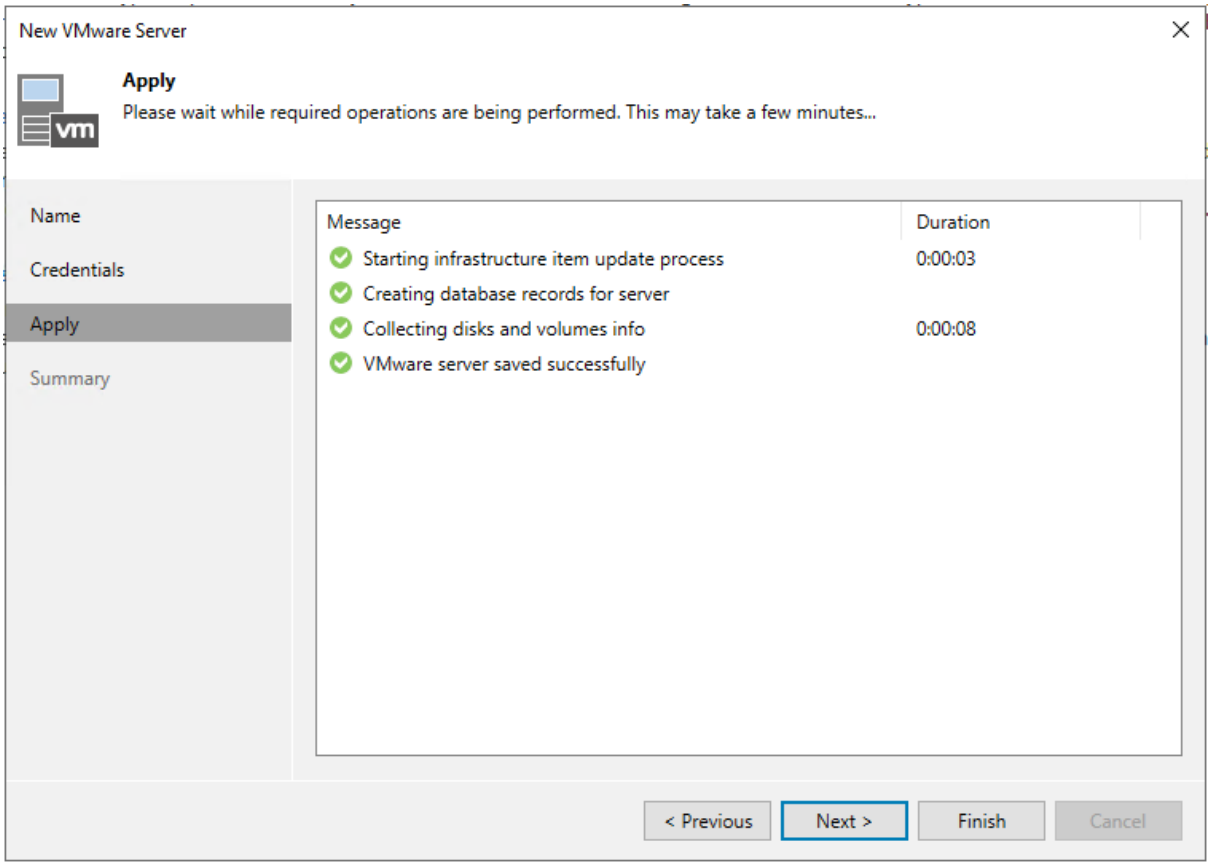


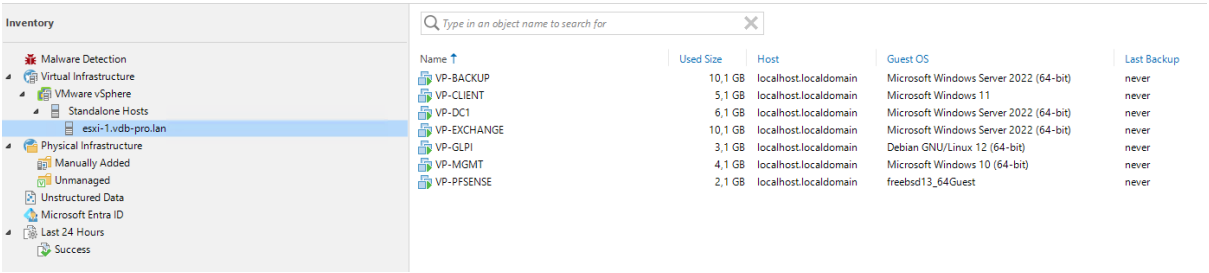
Lors de l'ajout, j'indique soit l'adresse IP, soit le nom DNS de l'hôte. Ayant préalablement configuré un enregistrement DNS pointant vers mon serveur (par exemple : esxi-1.vdb-pro.lan → 10.10.210.31), j'utilise ce nom DNS dans la configuration. Ensuite, je saisis les identifiants d'accès à l'ESXi, ici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





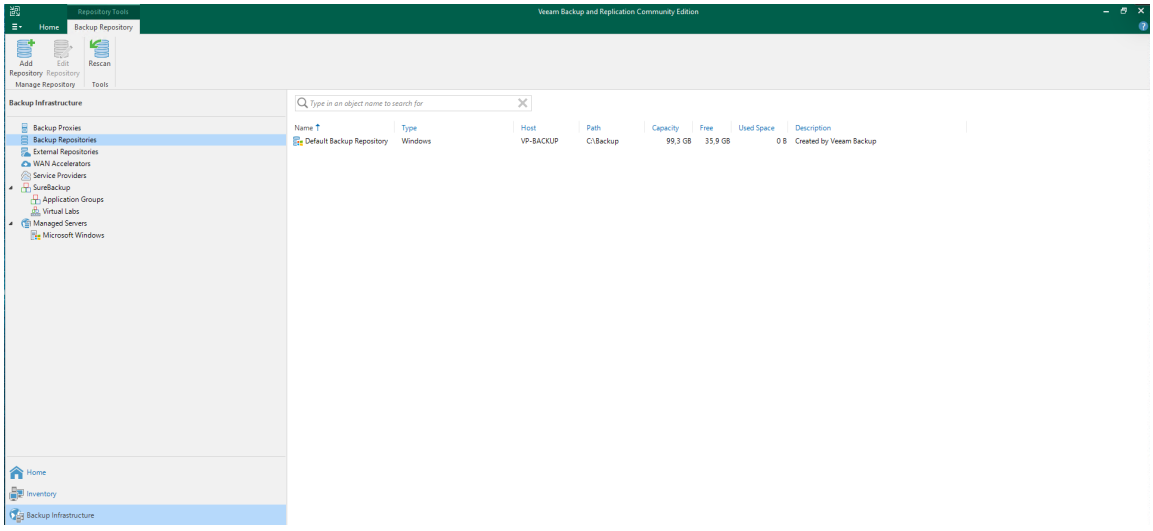
Ajout des Target de sauvegardes

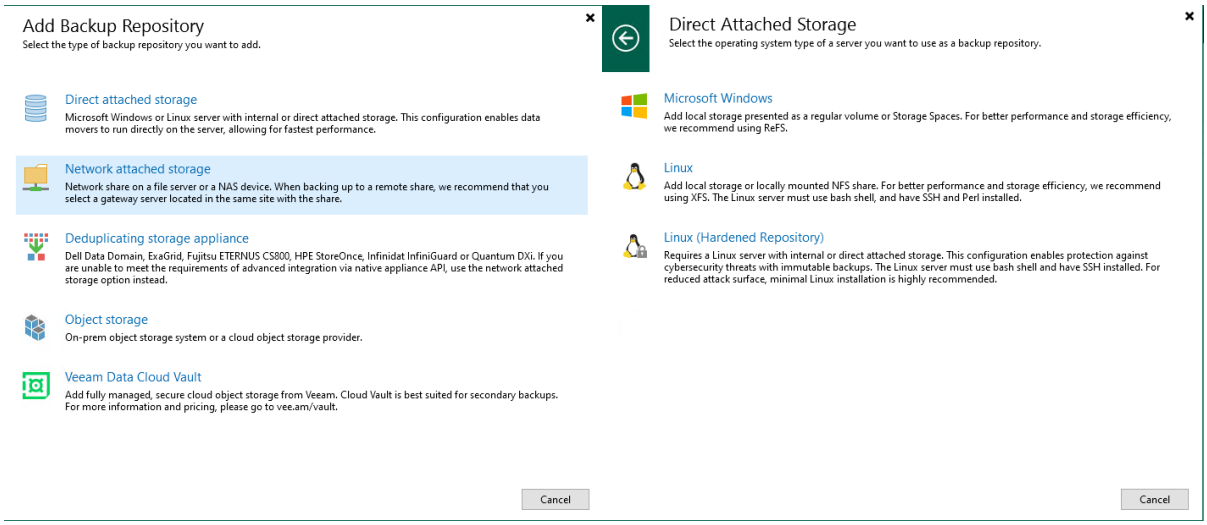
Une fois les sources de données identifiées, il est nécessaire de définir un espace de stockage destiné à accueillir les sauvegardes. Pour cela, un NAS externe a été ajouté dans Veeam en tant que dépôt de sauvegarde (backup repository). Ce NAS étant accessible via le réseau local, il permet une écriture 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 :

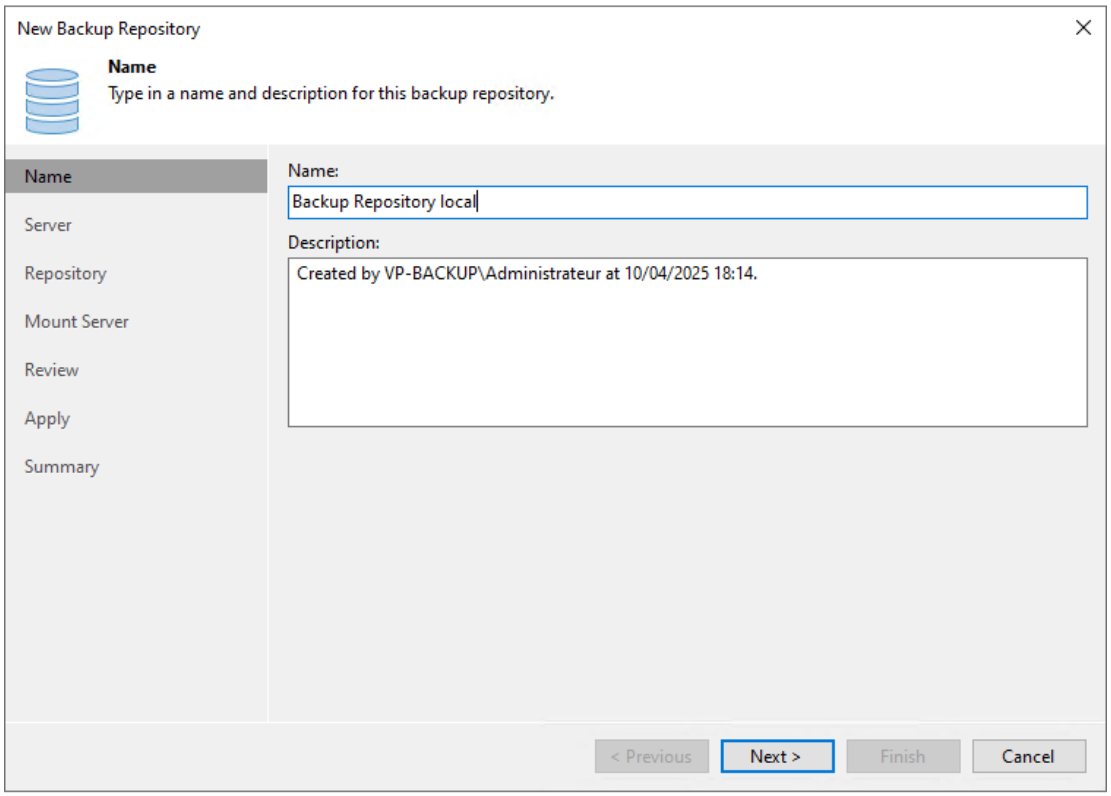
1. Le lecteur Z:\DATA, qui correspond à un repository local hébergé sur le serveur VP-BACKUP. Ce dépôt est principalement utilisé pour effectuer des copies de sauvegarde (Backup Copy) ou pour stocker les fichiers de configuration de Veeam.
2. Le lecteur I:\Backup, qui est un disque monté via iSCSI, connecté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

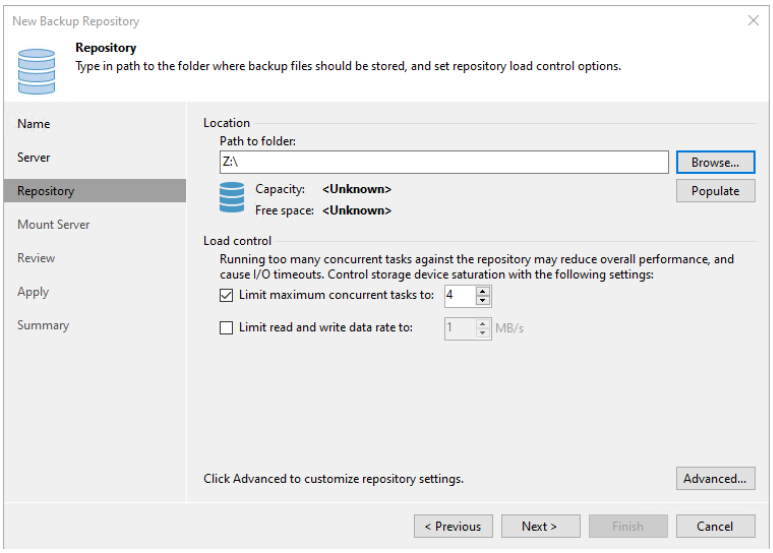


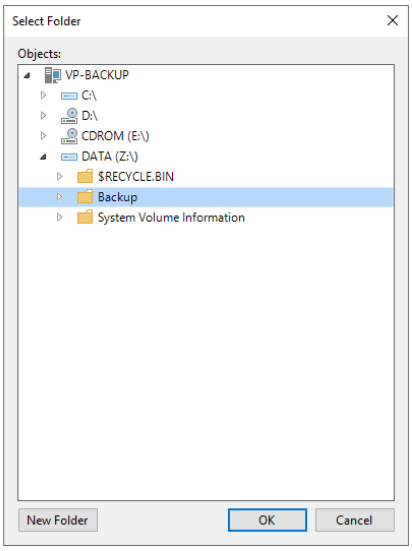


Je donne ensuite un nom au repository, par exemple "Backup Repository Local", qui sera affiché dans l'interface Veeam.

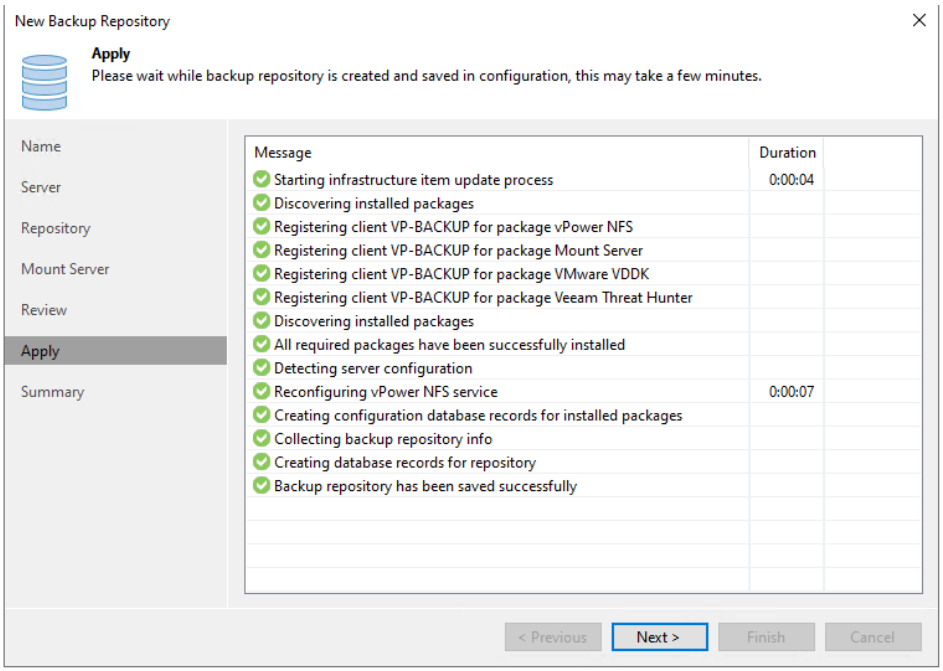


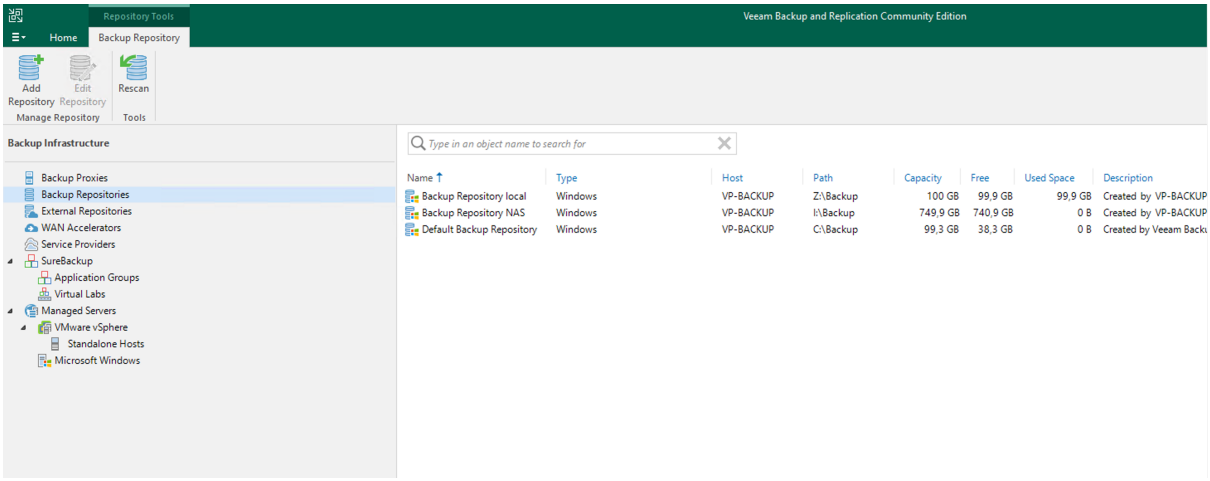
Je choisis le serveur VP-BACKUP comme hôte du dépôt, puis je sélectionne le lecteur Z:\ ainsi que le dossier Backup, que j'avais préalablement créé à cet emplacement.





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.



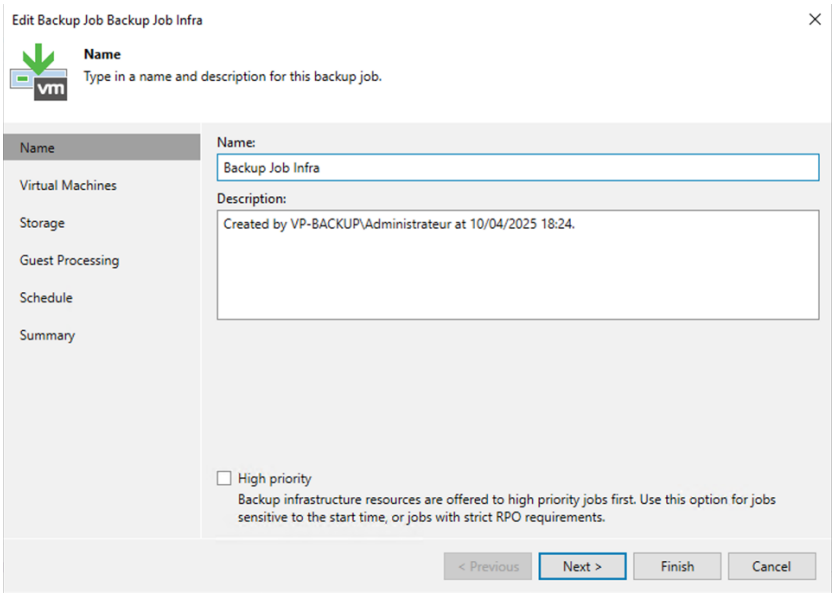


Création des jobs

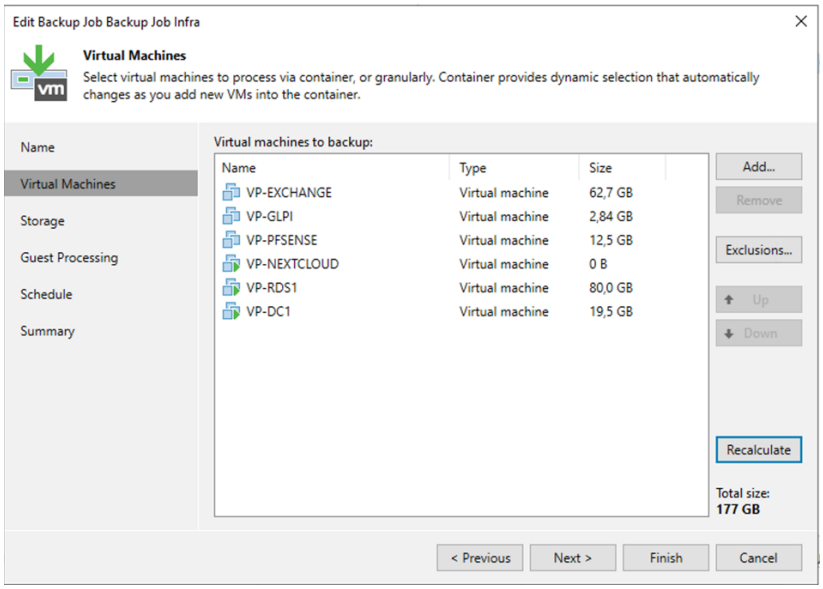
Une fois les dépôts de sauvegarde configurés, je procède à la création des **jobs de sauvegarde** dans l'interface de Veeam. Chaque job est défini avec les paramètres suivants : sélection des machines virtuelles à sauvegarder, planification automatique (quotidienne ou hebdomadaire), stratégie de rétention, 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.

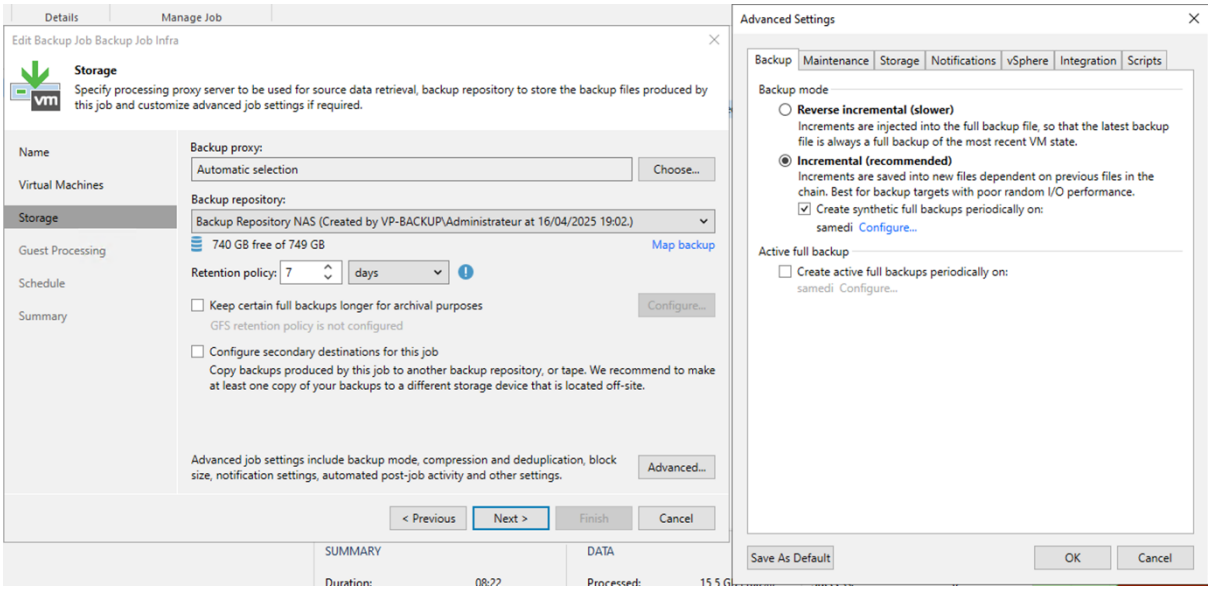


Dans l'onglet **Virtual Machines**, je sélectionne toutes les VMs critiques à protéger.

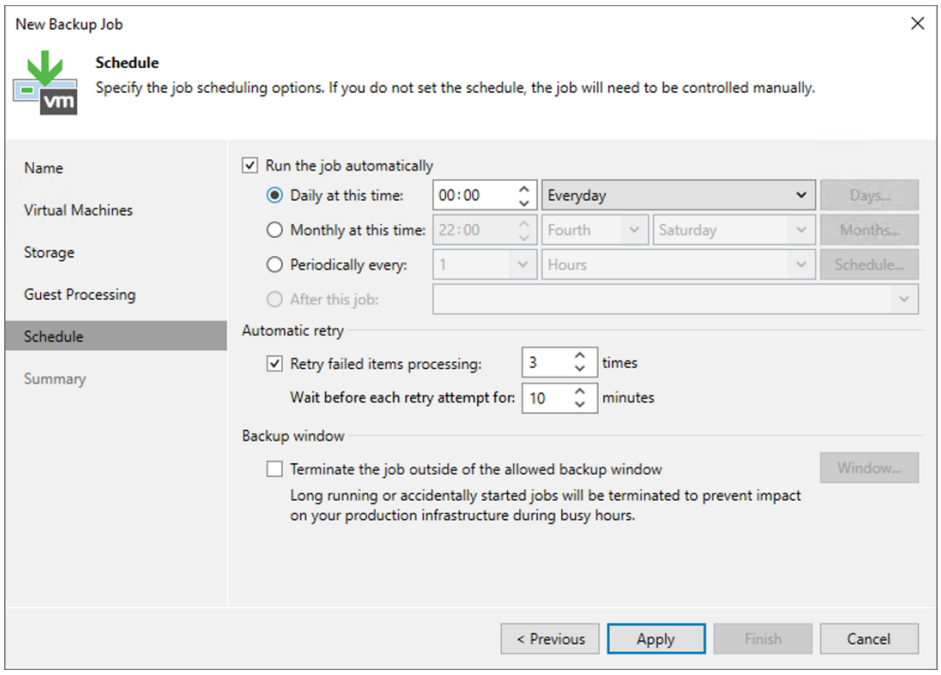


Ensuite, dans l'onglet **Storage**, je définis le dépôt de destination, en l'occurrence le **Backup Repository NAS**, configuré précédemment via le disque iSCSI monté.

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.

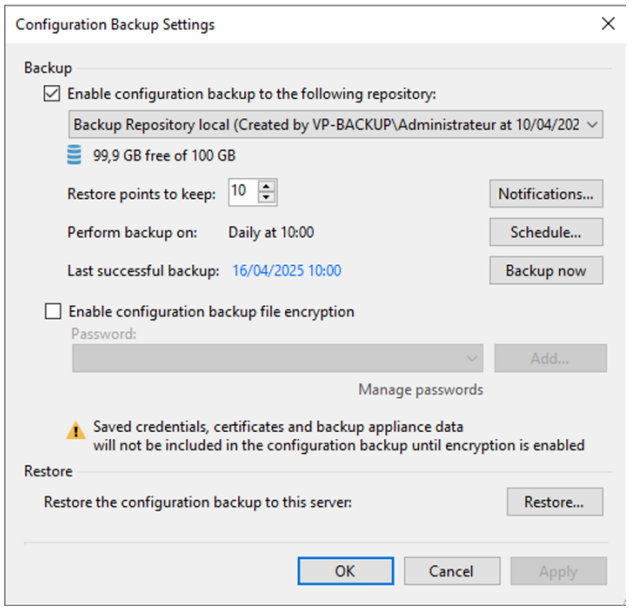


Enfin, dans l'onglet **Schedule**, je planifie l'exécution du job **tous les jours à minuit**, une heure stratégique où l'infrastructure n'est pas sollicitée, garantissant ainsi de meilleures performances de sauvegarde.

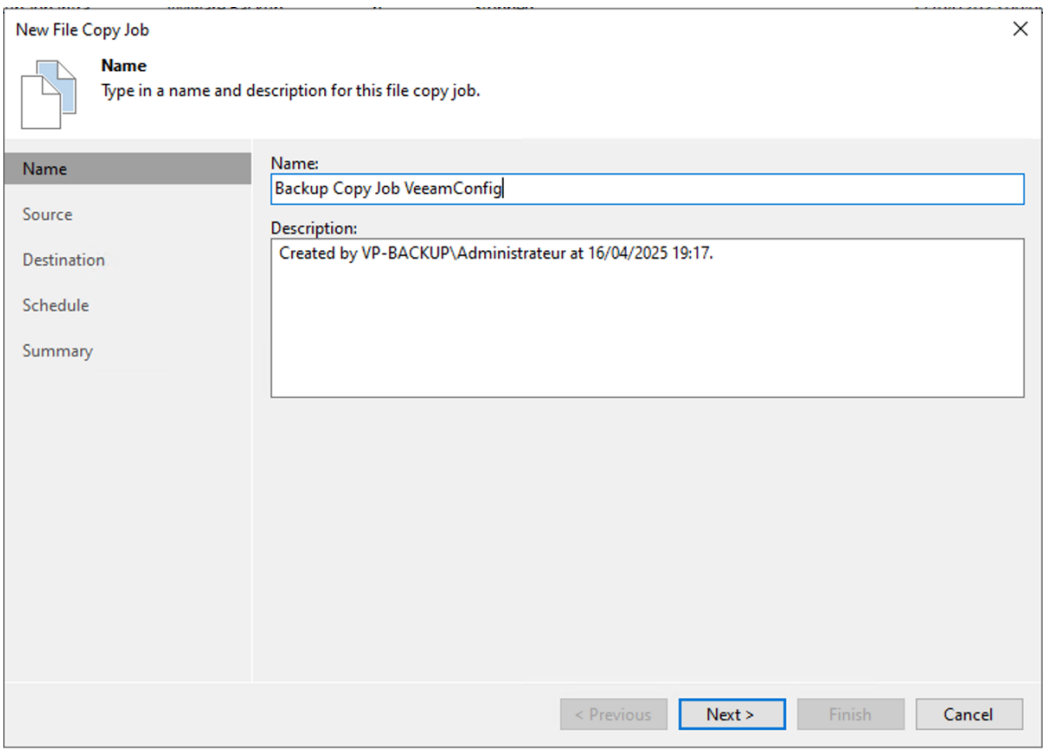


Job secondaire : sauvegarde du fichier de configuration Veeam

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.



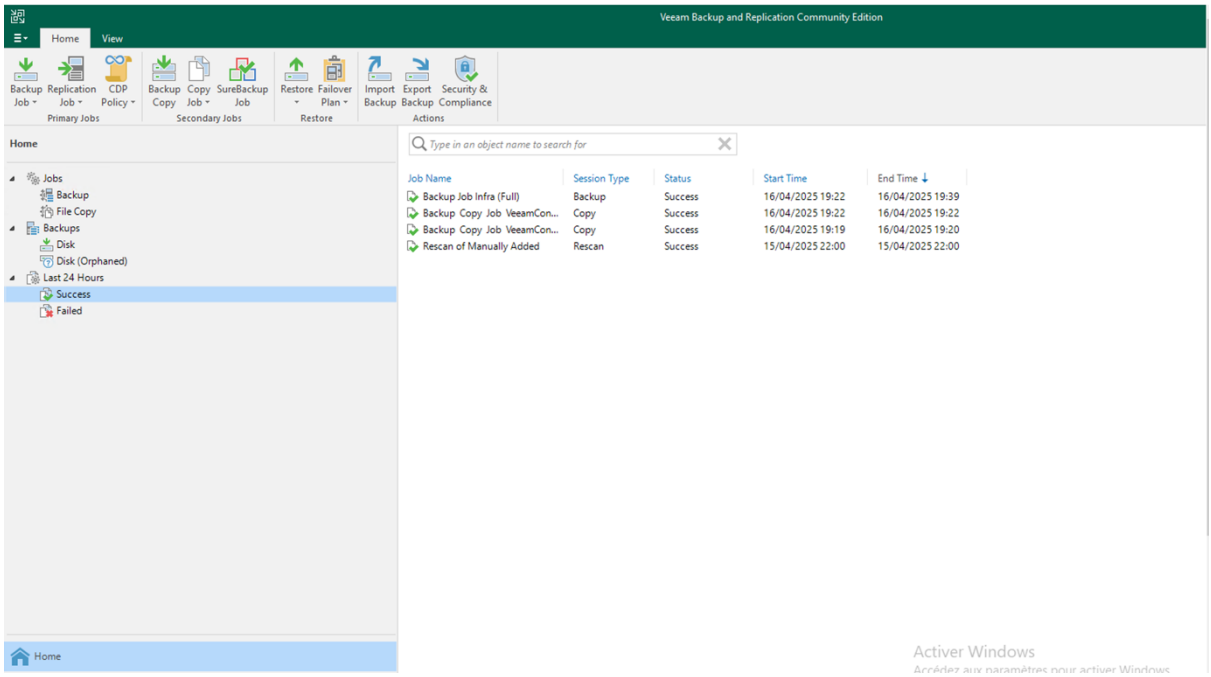
Partie 2 – Validation

Lancement des jobs

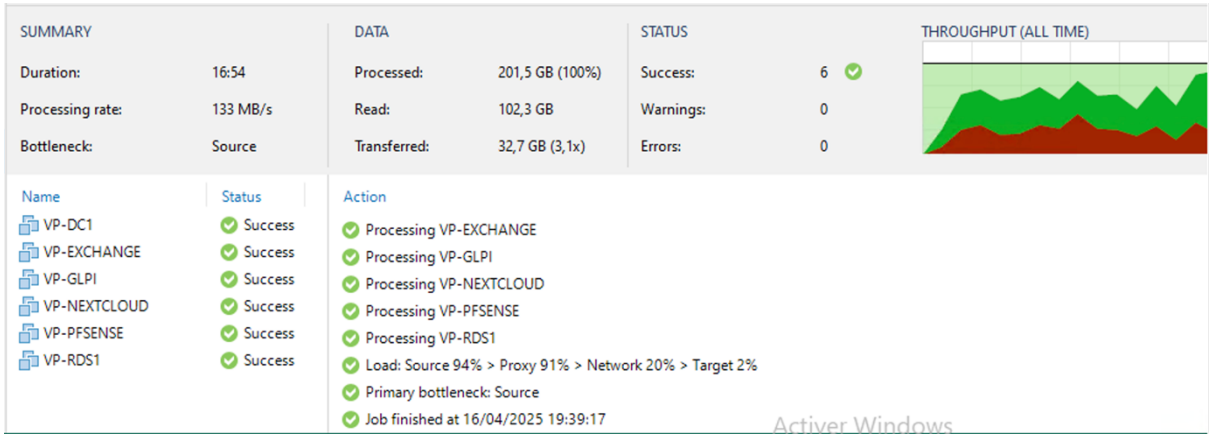
Pour m'assurer du bon fonctionnement de la solution mise en place, je lance manuellement les jobs de sauvegarde afin de valider l'ensemble du processus, ainsi que la connectivité avec le disque iSCSI.

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 :

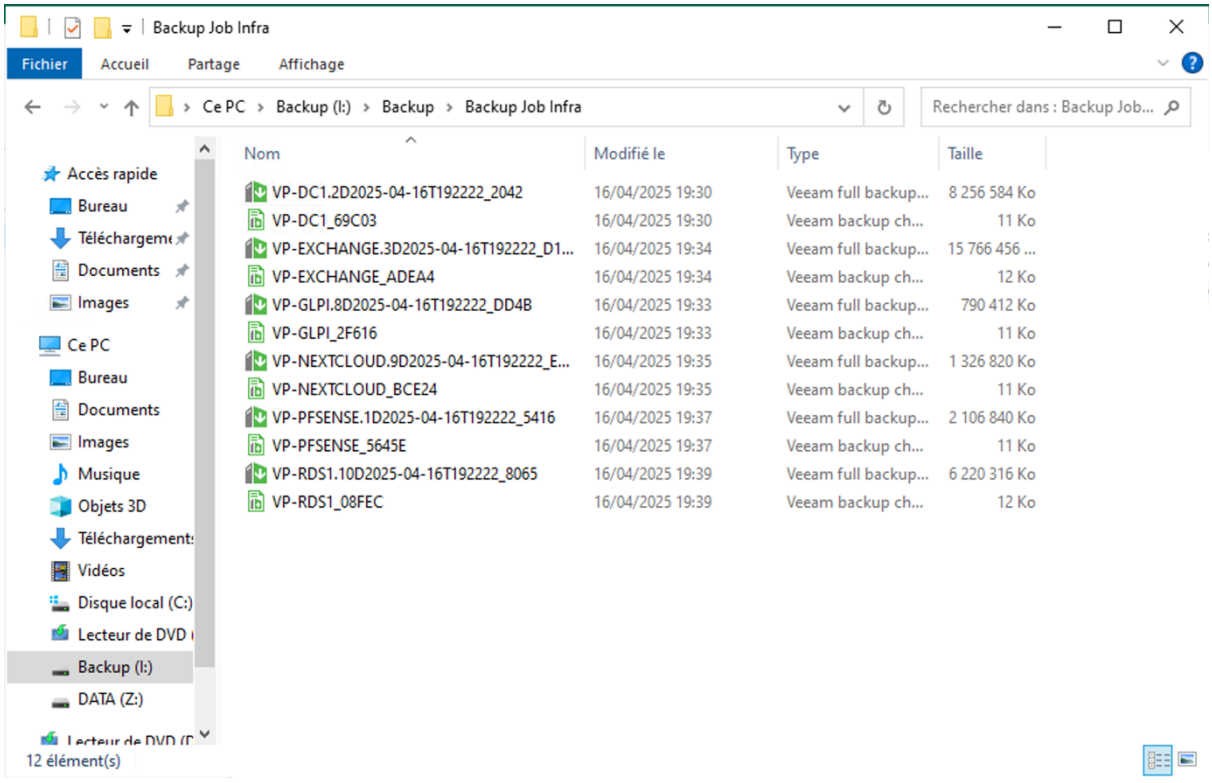
- Le job principal "Backup Job Infra", correspondant à la sauvegarde complète des machines virtuelles.
- Le job secondaire "Backup Copy Job VeeamConfig", qui contient le fichier de configuration de Veeam.



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.



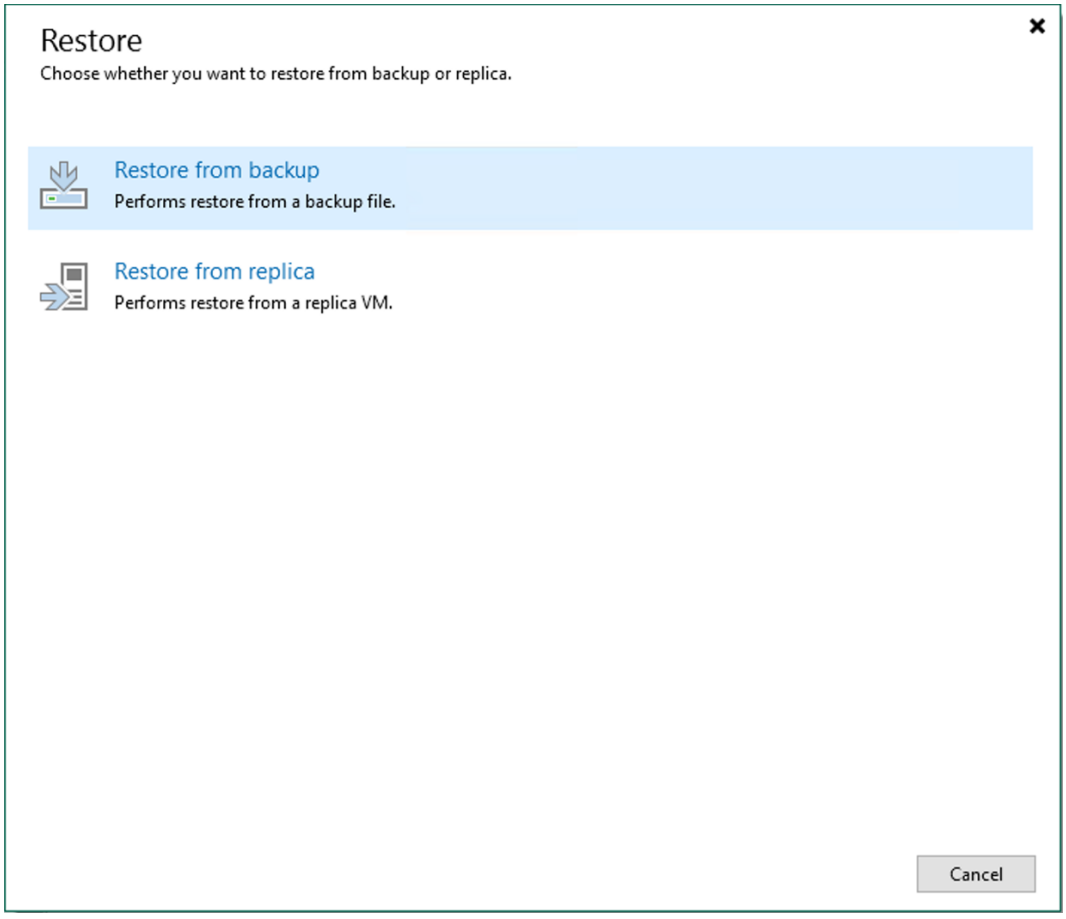
Pour une dernière vérification, je me rends dans l'explorateur de fichiers, dans le répertoire de destination du NAS. Je retrouve bien les fichiers de sauvegarde complète (Full Backup) générés par Veeam, ce qui valide à la fois le bon fonctionnement du job, du repository, et de la connexion iSCSI.



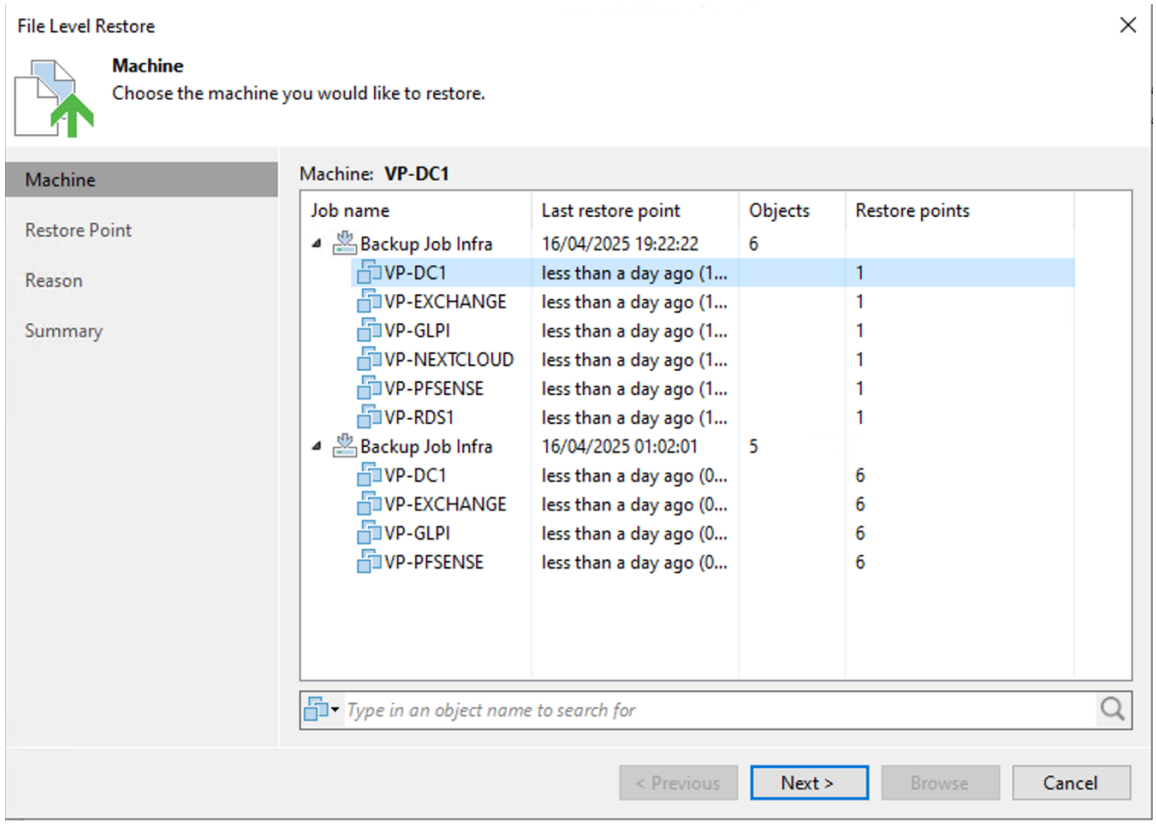
Test de restauration

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.

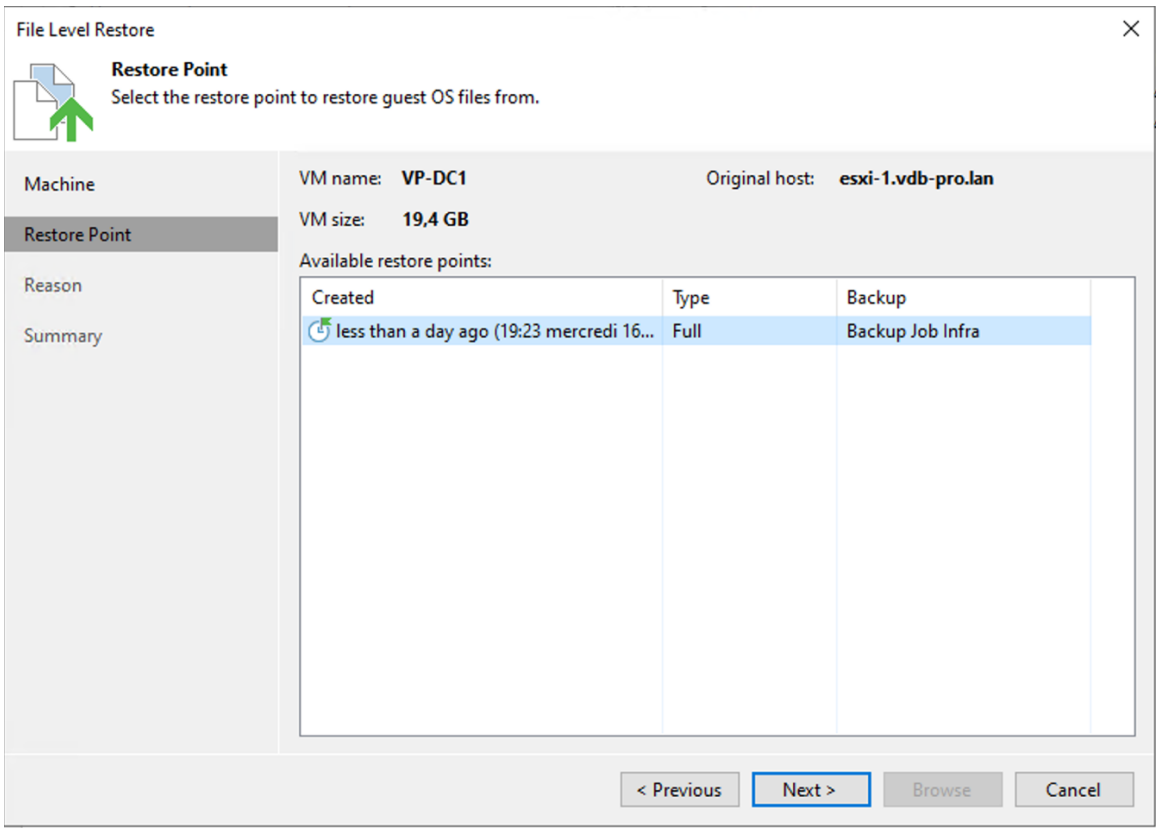
Depuis l'interface de Veeam, je clique sur "Restore", puis je sélectionne "Restore from Backup". Dans les options proposées, je choisis "Guest Files Restore", puis "Microsoft Windows", afin de restaurer un fichier à l'intérieur d'une machine virtuelle Windows.



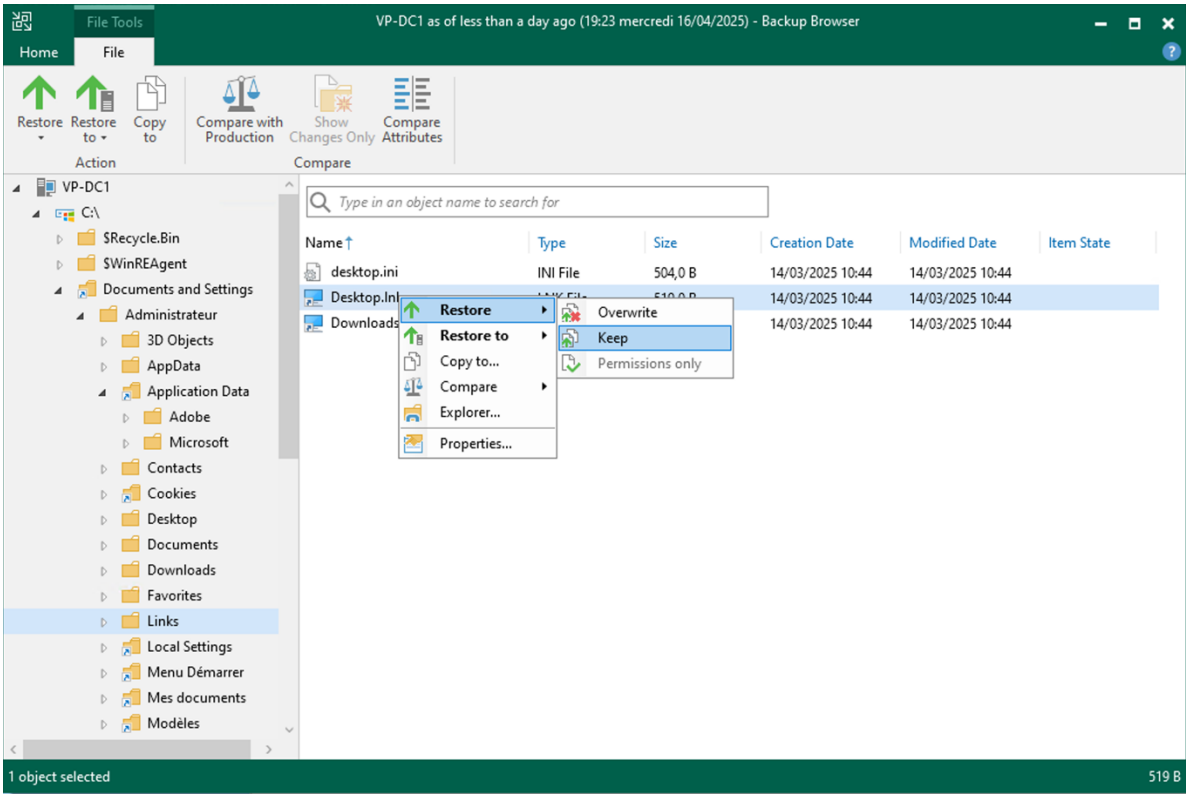
La liste des machines sauvegardées s'affiche. Pour ce test, je sélectionne la VM VP-DC1.

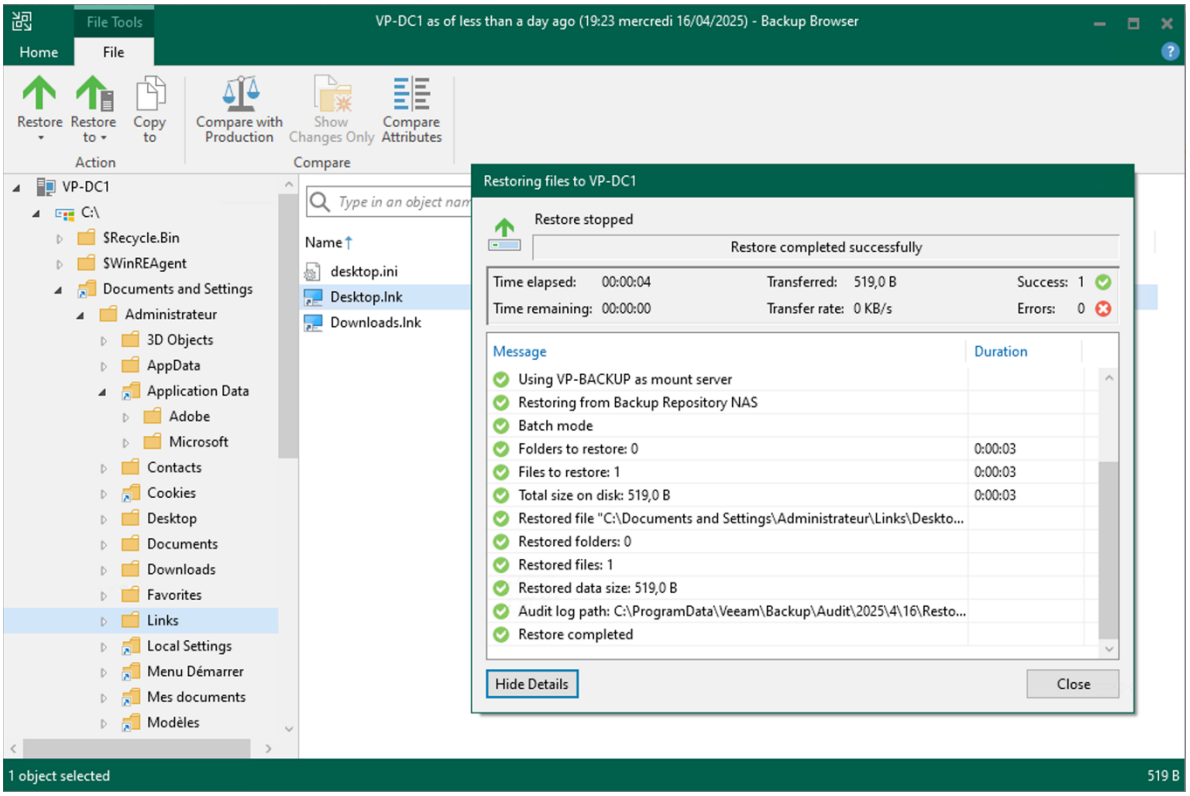


Je choisis le point de restauration le plus récent.

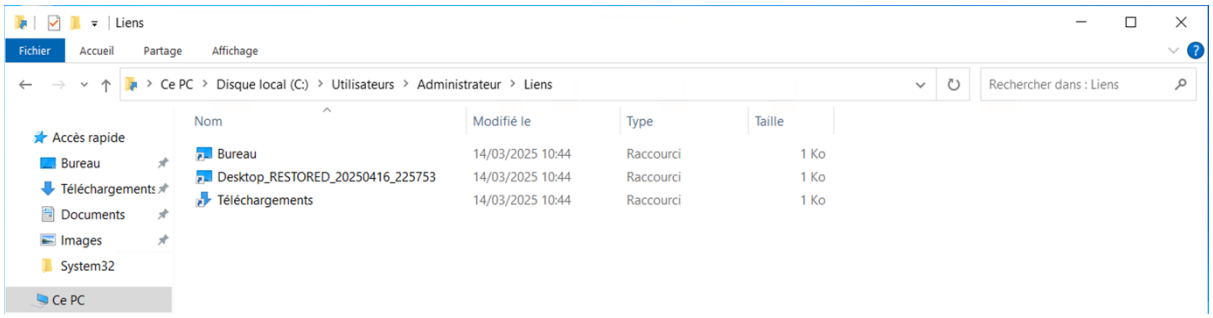


je sélectionne un fichier aléatoire, en l'occurrence un raccourci sur le bureau. Lors de la restauration, je choisis l'option "Keep" pour conserver l'ancienne version du fichier tout en restaurant la nouvelle, afin de ne pas écraser d'éventuelles données existantes.





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.