

PAGE DE GARDE DU DOSSIER PROFESSIONNEL
BREVET DE TECHNICIEN SUPÉRIEUR SERVICES INFORMATIQUES AUX
ORGANISATIONS
Session 2026

DOSSIER PROFESSIONNEL

NOM : CHAUVEL

Prénom : Corentin

Établissement de formation (sur un seul des deux exemplaires du dossier)

Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

Nom et qualité du signataire	Date	Signature

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné(e), CHAUVEL _____, Corentin _____, certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à Bouguenais
Date 22/04/2026

Signature

Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 1
Nom, prénom : CHAUVEL Corentin		N° candidat : 02542581385
Épreuve ponctuelle <input type="checkbox"/>	Contrôle en cours de formation <input checked="" type="checkbox"/>	Date : 29 / 05 /2026
Organisation support de la réalisation professionnelle Entreprise fictive Oasis et prestataire NTxSystem		
Intitulé de la réalisation professionnelle Mise en place d'une solution de sauvegarde avec Veeam		
Période de réalisation : 2024 – 2026 Lieu : CFA Fab'Academy Bouguenais (UIMM)		
Modalité : <input type="checkbox"/> Seul(e) <input checked="" type="checkbox"/> En équipe		
Compétences travaillées <input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation¹ (ressources fournies, résultats attendus) Mise en place d'une solution de sauvegarde et de restauration avec l'outil Veeam, afin de répondre aux exigences de OASIS. La solution doit permettre d'assurer la protection, la disponibilité et la restauration rapide des infrastructures virtualisées et sécurisées, ainsi que des services essentiels, en garantissant l'intégrité des données, la gestion des sauvegardes automatisées et la reprise d'activité en cas d'incident.		
Description des ressources documentaires, matérielles et logicielles utilisées² Différentes ressources ont été utilisées pour la mise en place de la solution de sauvegarde, tout d'abord pour les ressources documentaires, la ressource principale utilisée a été la documentation officielle de Veeam et la documentation it-connect, pour les ressources matérielles, un Serveur HP en tant qu'hyperviseur a été utilisé et deux NAS externe, pour les ressources logicielles, ESXI VMware, Veeam backup & replication.		
Modalités d'accès aux productions³ et à leur documentation⁴ L'ensemble des documents liés à l'infrastructure est disponible sur le partage réseau accessible depuis le réseau BTS SIO. Cet emplacement est dédié au stockage des informations relatives à la section. Il contient notamment des documentations sur l'environnement virtuel déployé, l'ensemble de la configuration de l'infrastructure mise en place, les différentes solutions étudiées, le plan d'adressage ainsi que les différents schémas réalisés de l'infrastructure. L'ensemble des mots de passe de l'infrastructure sont conservés dans notre gestionnaire de mot de passe Bitwarden. Partage Réseau Documentation NTxSystem : \\partage.btssio.nte\fichiers\BAIES-PEDA\NTXSYSTEM Identifiant Bitwarden : ntxsystem@proton.me Mot de passe Bitwarden : NTxbitwarden44. Lien Bitwarden : https://vault.bitwarden.com		

¹ En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

² Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

³ Conformément au référentiel du BTS SIO « Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve. ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

⁴ Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

**Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)****Épreuve E6 - Administration des systèmes et des réseaux (option SISR)****Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs**

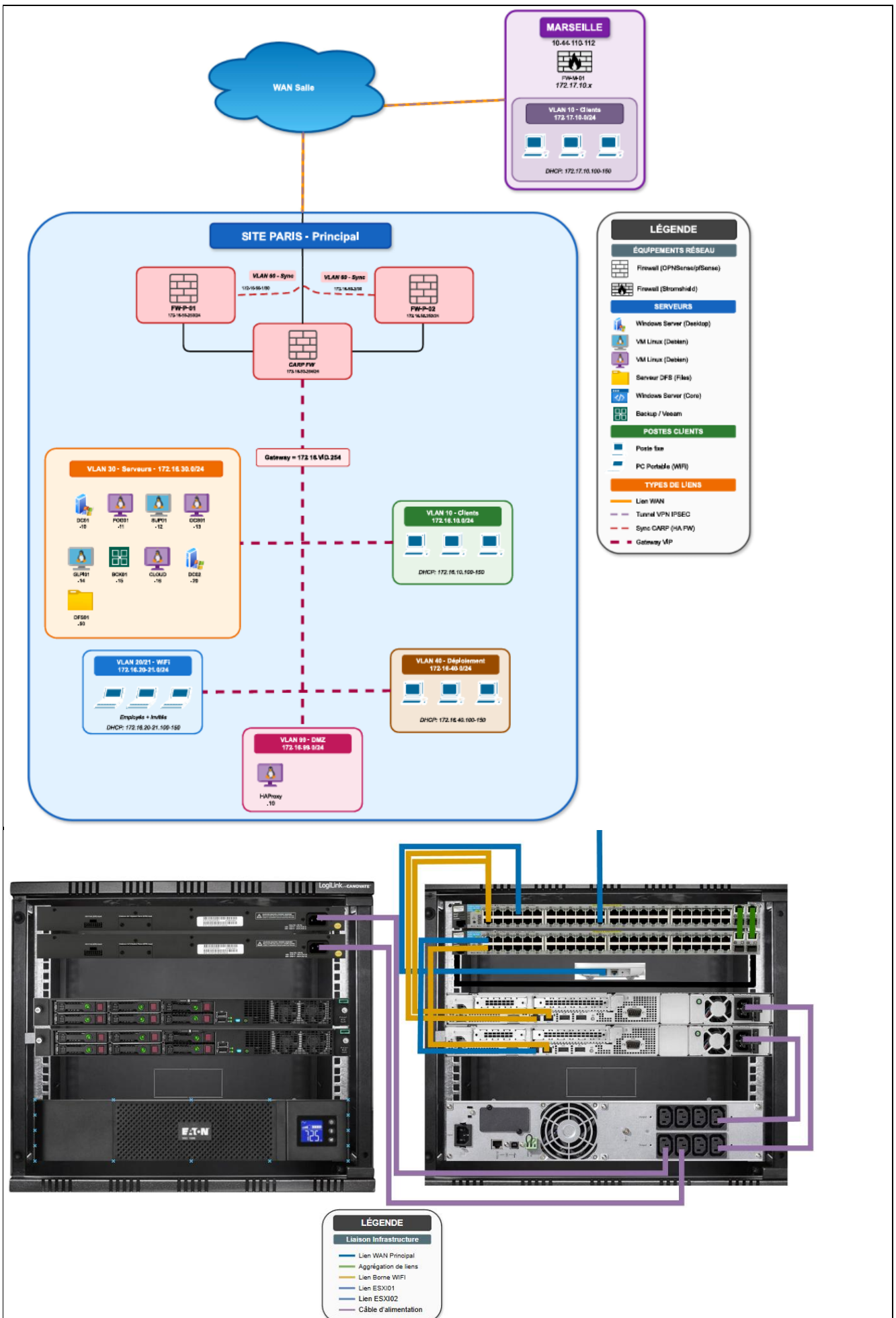
A travers cette réalisation professionnelle portant sur la sauvegarde, différents outils ont été monté au sein de l'infrastructure, tout l'environnement est virtualisé sur deux serveurs HP utilisant VMware ESXI et il y a différentes machines virtuelles dédiées à différents services.

Cette infrastructure a été construite sur deux sites, le premier correspondant au site commun au groupe NTxSystem, le site de Paris et le second le site de Marseille.

L'objectif principal de cette réalisation était de mettre en place une solution permettant d'assurer la sauvegarde et la restauration des données de manière centralisée. Pour répondre à ce besoin, j'ai utilisé l'outil Veeam afin d'automatiser les processus de sauvegarde des serveurs et des infrastructures virtualisées.

Cette solution s'appuie sur la planification de sauvegardes régulières, la gestion des points de restauration et la vérification de l'intégrité des données. Elle permet ainsi de simplifier la gestion des sauvegardes, de sécuriser les données critiques et de réduire les interventions manuelles, tout en garantissant une reprise rapide en cas d'incident.

Ci-dessous les schémas logique et physique ainsi que le plan d'adressage de l'infrastructure.



Pour plus de détails, les deux schémas montrant l'ensemble de l'infrastructure peuvent être trouvés en Annexe n°4 pour le schéma logique et schéma physique.

Paris :

VLAN 10

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.10.252	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-01 VLAN 10
FW-P-01	172.16.10.253	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-02 VLAN 10
CARP Firewall	172.16.10.254	255.255.255.0	172.16.10.0	172.16.10.254	Passerelle du VLAN 10
DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.10.100-150	172.16.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Paris

VLAN 20

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
B-P-WIFI	172.16.20.50	255.255.255.0	172.16.20.0	172.16.20.254	Administration borne Wifi
FW-P-02	172.16.20.252	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-02 VLAN 20
FW-P-01	172.16.20.253	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-01 VLAN 20
CARP Firewall	172.16.20.254	255.255.255.0	172.16.20.0	172.16.20.254	Passerelle du VLAN 20
DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.20.100-150	172.16.20.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Employés

VLAN 21

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.21.252	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-02 VLAN 21
FW-P-01	172.16.21.253	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-01 VLAN 21
CARP Firewall	172.16.21.254	255.255.255.0	172.16.21.0	172.16.21.254	Passerelle du VLAN 21
DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.21.100-150	172.16.21.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Invité

VLAN 30

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-DC01	172.16.30.10	255.255.255.0	172.16.30.0	172.16.30.254	DC 1
SRV-P-DC02	172.16.30.20	255.255.255.0	172.16.30.0	172.16.30.254	DC 2
SRV-P-DFS01	172.16.30.50	255.255.255.0	172.16.30.0	172.16.30.254	DFS01
SRV-P-FOG01	172.16.30.11	255.255.255.0	172.16.30.0	172.16.30.254	Fog
SRV-P-OCS01	172.16.30.13	255.255.255.0	172.16.30.0	172.16.30.254	OCS Inventory
SRV-P-GLPI01	172.16.30.14	255.255.255.0	172.16.30.0	172.16.30.254	GLPI
SRV-P-BCK01	172.16.30.15	255.255.255.0	172.16.30.0	172.16.30.254	Veeam
SRV-P-CLOUD01	172.16.30.16	255.255.255.0	172.16.30.0	172.16.30.254	Nextcloud
SRV-P-RSAT-T0	172.16.30.30	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T0
SRV-P-RSAT-T1	172.16.30.31	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T1
SRV-P-RSAT-T2	172.16.30.32	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T2
SRV-P-EDR01	172.16.30.19	255.255.255.0	172.16.30.0	172.16.30.254	EDR
SRV-P-ANS01	172.16.30.21	255.255.255.0	172.16.30.0	172.16.30.254	Ansible Lille
SRV-P-NETBOX01	172.16.30.22	255.255.255.0	172.16.30.0	172.16.30.254	Outil d'infrastructure
SRV-P-POL01	172.16.30.25	255.255.255.0	172.16.30.0	172.16.30.254	Centreon Poller
FW-P-02	172.16.30.252	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-02 VLAN 30
FW-P-01	172.16.30.253	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-01 VLAN 30
CARP Firewall	172.16.30.254	255.255.255.0	172.16.30.0	172.16.30.254	Passerelle du VLAN 30

VLAN 40

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.40.252	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-02 VLAN 40
FW-P-01	172.16.40.253	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-01 VLAN 40
CARP Firewall	172.16.40.254	255.255.255.0	172.16.40.0	172.16.40.254	Passerelle du VLAN 40
DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.40.100-150	172.16.40.254	172.16.30.10	172.16.30.20	Plage DHCP Déploiement

VLAN 50

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SW-P-01	172.16.50.1	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 1 Paris
SW-P-02	172.16.50.2	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 2 Paris
SRV-P-ESXI01	172.16.50.10	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
SRV-P-ESXI02	172.16.50.20	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
PAW-P-T0	172.16.50.50	255.255.255.0	172.16.50.0	172.16.50.254	Machine d'administration
FW-P-02	172.16.50.252	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-02 VLAN 50
FW-P-01	172.16.50.253	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-01 VLAN 50
CARP Firewall	172.16.50.254	255.255.255.0	172.16.50.0	172.16.50.254	Passerelle du VLAN 50

VLAN 60

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-01	172.16.60.1	255.255.255.252	172.16.60.0	-	IP FW-P-01 VLAN 60
FW-P-02	172.16.60.2	255.255.255.252	172.16.60.0	-	IP FW-P-02 VLAN 60

VLAN 99

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-HAProxy	172.16.99.10	255.255.255.0	172.16.99.0	172.16.99.254	HAProxy
FW-P-02	172.16.99.252	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-02 VLAN 99
FW-P-01	172.16.99.253	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-01 VLAN 99
CARP Firewall	172.16.99.254	255.255.255.0	172.16.99.0	172.16.99.254	Passerelle du VLAN 99

Marseille :

Marseille

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-M-01	172.17.10.254	255.255.255.0	172.17.10.0	172.17.10.254	IP FW-M-01 VLAN 10 Marseille
FW-M-01	10.44.110.112	255.255.255.0	10.44.110.0	10.44.110.254	IP WAN Marseille
DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.17.10.100-150	172.17.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Marseille

BTS Services informatiques aux organisations SESSION 2026**ANNEXE 10-A : Outil d'aide à l'appréciation de l'environnement technologique mobilisé par la personne candidate****Épreuve E6 - Administration des systèmes et des réseaux (option SISR)****CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE**

En référence à l'annexe II.E – « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification⁵	Fab'Academy, 9 Rue de l'Halbrane, 44340 Bouguenais	SISR
-----------------------------------	--	-------------

1. Environnement commun aux deux options**1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :**

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un service d'authentification	Active Directory Windows	
Un SGBD	MySQL / MariaDB	
Un accès sécurisé à internet	Firewall, OPNsense, Stormshield	
Un environnement de travail collaboratif	Nextcloud	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (<i>open source</i>)	GLPI (Debian), Windows Server 2022	

⁵ Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E – « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution de sauvegarde	Veeam B&R	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Nextcloud, DFS/R	
Deux types de terminaux dont un mobile (type <i>smartphone</i> ou encore tablette)	Tablette / PC Portable via connexion Wifi	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Gestion des incidents	GLPI	
Détection et prévention des intrusions	Wazuh, Stormshield	
Chiffrement	TLS, IPsec, SSH, PKI	
Analyse de trafic	Wireshark	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

ANNEXE 10-A (suite) : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : « Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée. »

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Un réseau comportant plusieurs périmètres de sécurité	Segmentation VLANs via Switch	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Partage Réseau avec droits d'accès via DFS/R suivant méthode AGDLP	
Un logiciel d'analyse de trames	Wireshark	
Un logiciel de gestion des configurations	Ansible, GPO	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	SSH, RDP, HTTPS	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Centreon	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	Firewall OPNsense, HaProxy, VPN	

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution garantissant la continuité d'un service	Veeam B&R, Haute disponibilité OPNsense	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	RAID 1, redondance switch et Firewall OPNsense	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	DFS/R , DHCP, DNS, Firewall OPNsense	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)	Remarques de la commission d'interrogation
Une solution permettant la connexion sécurisée entre deux sites distants	VPN IPsec	
Une solution permettant le déploiement des solutions techniques d'accès	FOG, Ansible	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de <i>scripting</i>	Ansible, Batch GPO	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	Stormshield IPS, Wazuh	

Table des matières

1.	Introduction	14
2.	Présentation de l'entreprise NTxSYSTEM	14
3.	Présentation de l'entreprise OASIS	14
4.	Projet Sauvegarde	15
4.1.	Contexte du projet	15
4.2.	Schéma du réseau d'OASIS	16
4.2.1.	Couche la plus haute : Réseau WAN	17
4.2.2.	Site distant	17
4.2.3.	Les tunnels VPN / synchronisation inter-sites.....	17
4.2.4.	Site principale Paris	17
4.2.5.	Segmentation réseau par VLAN	17
4.3.	Etude de Faisabilité.....	18
4.3.1.	Analyse des besoins.....	18
4.3.2.	Étude des solutions.....	18
4.3.2.1.	Solution 1 : Veeam	18
4.3.2.2.	Solution 2 : Bareos	19
4.3.2.3.	Solution 3 : Bacula	19
4.3.3.	Synthèse des solutions	20
4.3.4.	Conclusion de l'étude de faisabilité	20
4.4.	Schéma d'architecture des sauvegardes	21
4.5.	Stratégie de sauvegarde	21
4.5.1.	Job de sauvegarde principal	22
4.5.2.	Job Backup Copy – NAS 1	22
4.5.3.	Job Backup Copy – NAS 2	23
4.6.	Planification du projet :	23
4.7.	Mise en production de la solution	24
4.7.1.	Règle Firewall	24
4.7.2.	Installation et configuration de Veeam backup & replication.....	24
4.7.2.1.	Installation	25
4.7.2.2.	Configuration.....	29
4.7.2.2.1.	Ajout du disque local pour les sauvegardes.....	29
4.7.2.2.2.	Ajout des NAS pour la sauvegarde externe.....	36
4.7.2.2.3.	Ajout des ESXI dans Veeam pour la sauvegarde.....	40
4.7.2.2.4.	Mise en place d'un Job de sauvegarde.....	45

4.7.2.2.5.	Mise en place des Backup Copy Job (copie externe) vers le NAS 1	47
4.7.2.2.6.	Mise en place d'un Backup Copy Job (copie externe) vers le NAS 2.....	52
4.8.	Procédure de restauration complète et partielle	56
4.8.1.	Restaurer une VM entière (configuration + disques) à partir d'un backup.....	56
4.8.2.	Restaurer un disque spécifique sans restaurer toute la VM.....	60
4.9.	Plan de reprise d'activité (PRA) détaillé.....	63
4.9.1.	Contexte.....	63
4.9.2.	Objectifs du PRA	64
4.9.3.	Architecture technique.....	64
4.9.3.1.	Infrastructure principale (Paris)	64
4.9.3.2.	Infrastructure secondaire (Marseille)	64
4.9.3.3.	Réseau	65
4.9.4.	Sauvegarde et réplication	65
4.9.4.1.	Sauvegardes	65
4.9.4.2.	Réplication	65
4.9.5.	Scénarios de sinistre	66
4.9.5.1.	Panne serveur (Paris)	66
4.9.5.2.	Cyberattaque (ransomware).....	66
4.9.5.3.	Perte du site principal	66
4.9.5.4.	Perte du lien VPN	66
4.9.6.	Procédures de reprise technique	66
4.9.6.1.	Cas : panne serveur	66
4.9.6.2.	Cas : cyberattaque.....	66
4.9.6.3.	Cas : perte du site Paris.....	66
4.9.6.4.	Cas : coupure VPN	67
4.9.7.	Gestion des accès utilisateurs.....	67
4.9.8.	Plan de communication	67
4.9.9.	Reprise opérationnelle	67
4.9.10.	Tests et validation	67
4.9.11.	Maintenance.....	68
4.9.12.	Conclusion	68
4.10.	Phase de test.....	68
4.10.1.	Vérification de l'exécution automatique des sauvegardes planifiées	68
4.10.2.	Test de restauration	70
4.10.2.1.	Restauration d'un fichier sur un serveur Windows	70
4.10.2.2.	Restauration d'un fichier sur un serveur Linux Debian.....	76

4.10.2.3.	Restauration d'une VM complète	82
4.10.3.	Simulation de perte de liaison réseau et reprise des sauvegardes différées	85
4.10.3.1.	Coupure de la carte réseau du serveur Veeam lors d'une exécution d'un Backup Copy	85
4.10.3.2.	Coupure depuis le Firewall lors d'une exécution d'un Backup Copy	87
4.10.3.3.	Coupure Firewall pour un job ESXi	89
4.10.4.	Vérification de la conformité de la politique de rétention	90
4.10.5.	Analyse des journaux et des alertes.	91
4.11.	Axe amélioration	93
4.12.	Conclusion	94
5.	Annexe.....	95
5.1.	Annexe 1 : Documentation Installation Windows Serveur	95
5.2.	Annexe 2 : Glossaire.....	98
5.3.	Annexe 3 : Plan d'adressage IP	100
5.3.1.	Site de Paris.....	100
5.3.2.	Site Marseille	101
5.4.	Annexe 4 : Schéma logique de l'ensemble de l'infrastructure d'OASIS et physique du site de Paris.....	102

1. Introduction

Dans le cadre de ma formation en BTS SIO, j'ai eu l'opportunité d'intervenir sur un projet de mise en place d'une solution de sauvegarde pour l'entreprise Oasis.

Ce projet vise à accompagner Oasis dans la mise en place d'une solution de sauvegarde et dans le suivi de son infrastructure informatique, afin d'assurer la continuité et la fiabilité des équipements et des services sur l'ensemble de ses sites. L'objectif est de déployer une solution de sauvegarde des machines virtuelles (VM) garantissant une restauration rapide et une réactivité optimale en cas d'incident.

Pour répondre à ces besoins, j'ai été amené à déployer une solution de sauvegarde basée sur Veeam Backup & Replication. Cette solution permet de sauvegarder les différentes machines virtuelles et serveurs, de centraliser la gestion des sauvegardes et d'assurer leur fiabilité. Elle offre également des mécanismes de restauration rapide et une gestion efficace des incidents.

2. Présentation de l'entreprise NTxSYSTEM

NTxSystem est une entreprise prestataire spécialisée dans les solutions informatiques pour les professionnels. Dans le cadre de l'expansion d'Oasis, NTxSystem a été chargé de concevoir et déployer l'ensemble de l'infrastructure réseau des agences de Paris et Marseille.

Les enjeux de ce projet sont multiples : centralisation des services, virtualisation des ressources, gestion des utilisateurs, sécurisation des communications inter-sites et mise en place d'un environnement stable et évolutif.

Pour répondre aux différentes exigences d'Oasis, l'ensemble de l'infrastructure est déployé dans un environnement virtualisé VMware ESXi.



3. Présentation de l'entreprise OASIS

L'entreprise Oasis est une société parisienne spécialisée dans la conception de voyages sur mesure pour une clientèle exigeante, à la recherche d'expériences uniques, loin des circuits touristiques classiques.

Créé en 2017, elle s'est rapidement imposée comme un acteur innovant dans le secteur du tourisme personnalisé, grâce à une approche centrée sur l'écoute client, la

connaissance culturelle approfondie des destinations, et un réseau de partenaires locaux dans plus de 30 pays.

Après plusieurs années de forte croissance, Oasis a décidé d'ouvrir une nouvelle agence à Marseille, pour mieux couvrir le sud de la France et répondre à une demande croissante dans cette zone. L'agence parisienne reste le siège social et le cœur de la stratégie de conception et de relation client haut de gamme.

En 2024, Oasis a atteint un chiffre d'affaires de 2,3 millions d'euros, et ambitionne désormais de renforcer sa structure numérique afin d'améliorer la coordination entre les sites, la sécurité des données clients, et la fluidité de l'expérience interne.

C'est dans ce contexte de croissance que NTxSystem a été sollicitée pour concevoir et déployer une infrastructure informatique adaptée aux besoins d'Oasis que ce soit pour l'agence parisienne, le siège social ou pour l'agence de Marseille

4. Projet Sauvegarde

4.1. Contexte du projet

Dans le cadre de la mission pour Oasis, nous intervenons en tant que prestataire informatique pour accompagner l'entreprise dans la conception et la mise en place de son infrastructure. La direction technique attend une centralisation des services, la virtualisation des ressources, la gestion des utilisateurs, la communication inter-sites, ainsi qu'un environnement stable, évolutif et sécurisé, d'abord testé dans un environnement isolé avant déploiement réel.

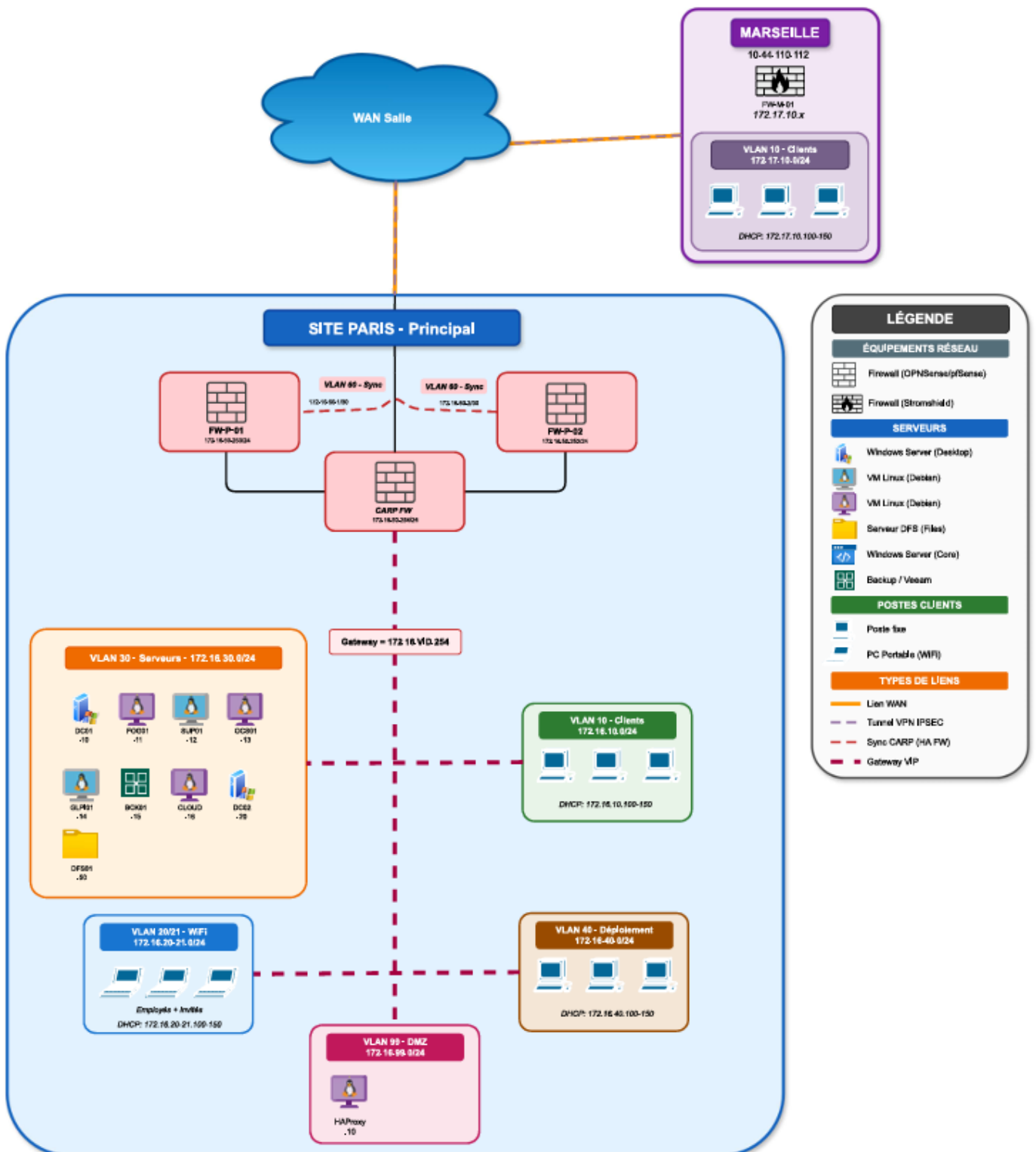
L'entreprise Oasis, désormais structurée autour de son siège à Paris et de son agence à Marseille, dispose d'infrastructures informatiques locales, interconnectées et sécurisées. Les collaborateurs utilisent quotidiennement des services critiques : annuaire d'entreprise, partage de fichiers, outils collaboratifs, bases de données clients et applications internes.

La direction a pris conscience que la perte de données ou l'interruption de service prolongée entraînerait des conséquences graves sur la continuité de ses activités.

Afin de garantir la sécurité des informations sensibles (dossiers clients, contrats, devis, données comptables, etc.) et d'assurer une reprise rapide en cas d'incident (panne matérielle, attaque, erreur humaine), Oasis souhaite mettre en place une politique de sauvegarde centralisée et un plan de reprise d'activité (PRA) adapté à sa taille.

4.2. Schéma du réseau d'OASIS

Voici le schéma :



4.2.1. Couche la plus haute : Réseau WAN

Depuis Internet, un réseau WAN est connecté.

Les lignes orange représentent donc le réseau WAN principal.

4.2.2. Site distant

- Marseille

4.2.3. Les tunnels VPN / synchronisation inter-sites

Les lignes violettes pointillées représentent : VPN Site-to-Site

Ces tunnels servent à connecter le site de Marseille au site principal.

4.2.4. Site principale Paris

Un cluster de firewall pour avoir de la haute disponibilité, ils sont reliés avec le VLAN 50-Sync. Ce VLAN sert à la synchronisation des firewalls, l'état des sessions, réplication de configuration.

4.2.5. Segmentation réseau par VLAN

VLAN séparés pour :

- CLIENTS
- WIFI
- WIFI CLIENTS
- SERVEUR
- DEPLOIEMENT
- ADMIN
- DMZ
- SYNC
- NATIF

4.3. Etude de Faisabilité

4.3.1. Analyse des besoins

Les besoins identifiés sont donc les suivants :

- Identifier les données et services critiques à sauvegarder (serveurs, fichiers utilisateurs, bases de données, configurations réseau).
- Définir une politique de sauvegarde :
 - o Type(s) de sauvegarde (complète, incrémentielle, différentielle)
 - o Fréquence (quotidienne, hebdomadaire, mensuelle)
 - o Rétention (durée de conservation des sauvegardes)
 - o Localisation des sauvegardes (locale, distante, mixte)
- Établir un plan de reprise d'activité (PRA) simple précisant les étapes de restauration.

4.3.2. Étude des solutions

Dans le cadre de la mise en place d'une solution de sauvegarde fiable et adaptée aux besoins de l'infrastructure, plusieurs outils ont été étudiés : Veeam, Bareos et Bacula.

4.3.2.1. Solution 1 : Veeam

Veeam Backup & Replication est une solution de sauvegarde, de restauration et de réplication largement utilisée dans les environnements virtualisés et cloud.

Elle repose sur une architecture centralisée permettant de gérer l'ensemble des sauvegardes depuis une seule console d'administration. Elle est particulièrement optimisée pour les environnements utilisant des hyperviseurs comme VMware ou Hyper-V.

Ses principales caractéristiques sont :

- Une interface graphique intuitive facilitant la prise en main et la configuration.
- La mise en place de sauvegardes complètes, incrémentielles et différentielles, permettant d'optimiser l'espace de stockage.
- La restauration instantanée de machines virtuelles (Instant VM Recovery), réduisant fortement le RTO (Recovery Time Objective).
- La réplication des machines virtuelles pour assurer une continuité de service en cas de panne.
- Une gestion centralisée avec planification des tâches automatisées.

Veeam permet ainsi de garantir un bon équilibre entre performance, sécurité des données et rapidité de restauration. Il est particulièrement adapté aux PME souhaitant une solution fiable sans nécessiter une forte expertise technique.

4.3.2.2. Solution 2 : Bareos

Bareos est une solution de sauvegarde open source issue du projet Bacula. Elle fonctionne selon une architecture client-serveur, composée notamment d'un Director (gestion), d'un Storage Daemon (stockage) et de File Daemons (clients).

Ses principales caractéristiques sont :

- Une grande flexibilité grâce à une configuration entièrement personnalisable via des fichiers texte.
- La prise en charge de multiples systèmes d'exploitation (Linux, Windows, macOS), ce qui le rend adapté aux environnements hétérogènes.
- Des fonctions avancées d'archivage et de restauration des données.

Cependant, Bareos présente certaines limites dans un contexte professionnel non spécialisé :

- Absence d'interface graphique avancée (ou limitée selon les versions).
- Configuration complexe nécessitant de bonnes compétences en administration système.
- Temps de mise en œuvre plus long.

Bareos est donc particulièrement adapté aux infrastructures disposant de compétences techniques internes et nécessitant une solution open source très personnalisable.

4.3.2.3. Solution 3 : Bacula

Bacula est une solution de sauvegarde open source reconnue pour sa robustesse et sa modularité. Elle est conçue pour gérer des infrastructures de grande taille et des environnements complexes. Son fonctionnement repose également sur une architecture client-serveur similaire à Bareos.

Elle propose :

- Une sauvegarde automatisée avec planification avancée des tâches.
- Une gestion avancée des supports de sauvegarde (disques, bandes, etc.).
- Une forte capacité d'adaptation grâce à sa modularité.

Néanmoins, Bacula présente plusieurs inconvénients :

- Une configuration complexe basée sur des fichiers de configuration.
- Une courbe d'apprentissage importante.
- Une interface utilisateur peu intuitive.

Ainsi, Bacula est davantage destiné aux grandes organisations ou aux administrateurs expérimentés capables de gérer une solution technique avancée.

4.3.3. Synthèse des solutions

Afin de comparer les différentes solutions étudiées, un tableau récapitulatif a été réalisé selon plusieurs critères techniques et fonctionnels.

EF : Synthèse des solutions

Les solutions	Solution 1	Solution 2	Solution 3
Intitulé	Veeam	Bareos	Bacula
Faisabilité technique (Oui / Non, en précisant pourquoi)	Oui – Solution clé en main, bien intégrée aux environnements virtualisés	Oui – Configuration possible avec ressources techniques internes	Oui – Nécessite une expertise technique plus poussée
Besoins RH (Internes et/ou Externes)	Interne	Interne	Interne
Besoin Matériel et Immatériel	VM	VM	VM
Coût total estimé	0 (si version gratuite Community)	0	0
Temps Jours / Hommes	1	1	
Durée de réalisation estimée	4h	5h	6h
Points forts	<ul style="list-style-type: none"> • PF: Facilité d'usage : Très simple 	<ul style="list-style-type: none"> • PF: Facilité d'usage : Moyenne 	<ul style="list-style-type: none"> • PF: Puissance, stabilité, hautement personnalisable
Points faibles	<ul style="list-style-type: none"> • Pf: Nécessite licence commerciale pour fonctionnalités avancées 	<ul style="list-style-type: none"> • Pf: Support communautaire, Open Source, configuration plus complexe 	<ul style="list-style-type: none"> • Pf: Configuration plus lourde, documentation dense, courbe d'apprentissage élevée

4.3.4. Conclusion de l'étude de faisabilité

Au terme de l'analyse technique, financière et organisationnelle, le choix s'est porté sur Veeam Backup & Replication.

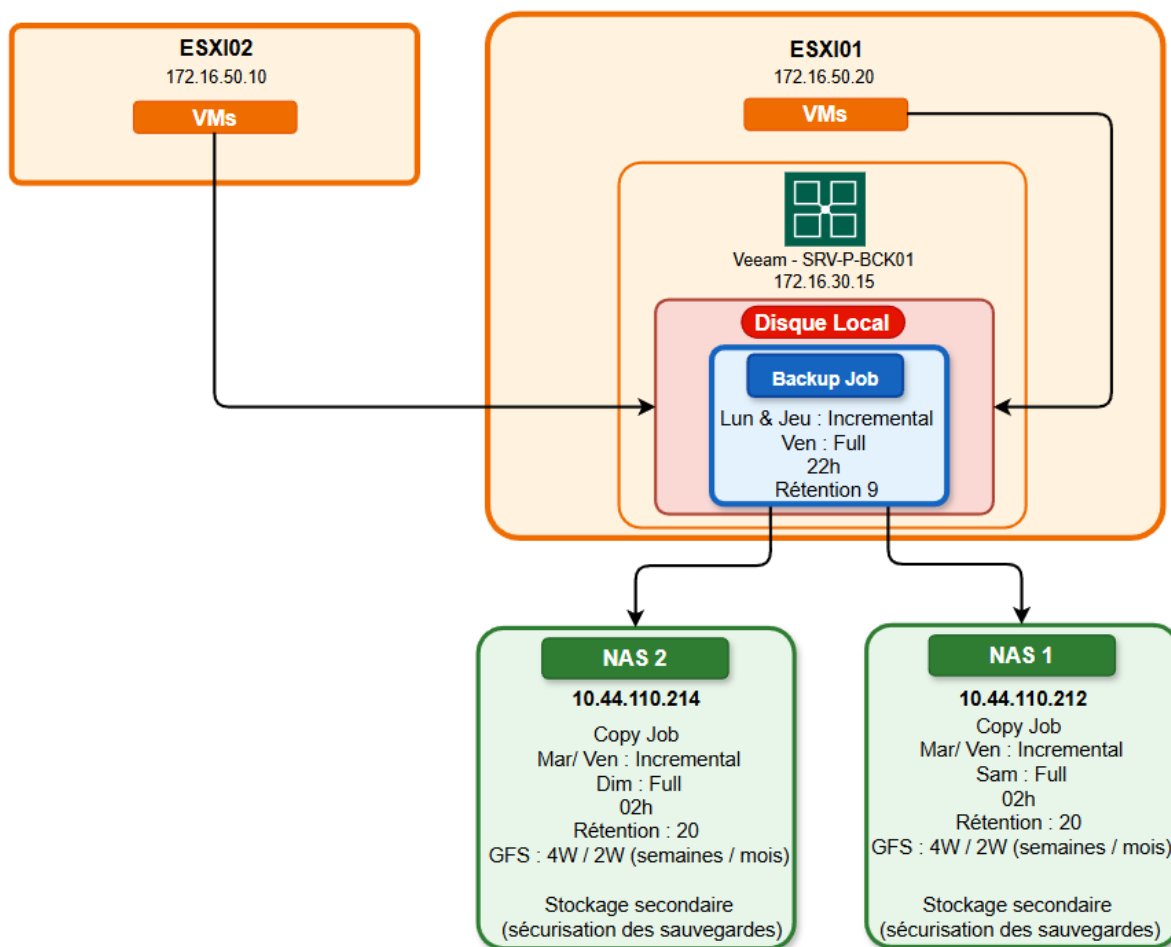
Ce choix se justifie par plusieurs éléments :

- Une mise en œuvre rapide et une administration simplifiée.
- Une solution fiable et reconnue dans le monde professionnel.
- La disponibilité d'une version gratuite permettant la gestion de jusqu'à 10 hôtes, suffisante pour l'infrastructure étudiée.

Contrairement à Bareos et Bacula, qui nécessitent une expertise technique plus avancée, Veeam permet de déployer rapidement une solution opérationnelle tout en garantissant un bon niveau de sécurité des données.

Ainsi, Veeam représente le meilleur compromis entre simplicité, performance et coût, ce qui en fait la solution la plus adaptée dans le cadre de ce projet.

4.4. Schéma d'architecture des sauvegardes



Les sauvegardes sont centralisées via Veeam Backup & Replication hébergé sur un hôte VMware ESXi, puis répliquées vers deux NAS distincts afin d'assurer la redondance et la sécurisation des données.

Pour consulter le plan d'adressage IP, se référer à l'annexe 3.

Voici les VMs qui seront sauvegardées via Veeam :

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-DC01	172.16.30.10	255.255.255.0	172.16.30.0	172.16.30.254	DC 1
SRV-P-DC02	172.16.30.20	255.255.255.0	172.16.30.0	172.16.30.254	DC 2
FW-P-01	172.16.30.253	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-01 VLAN 30
SRV-P-FOG01	172.16.30.11	255.255.255.0	172.16.30.0	172.16.30.254	Fog
SRV-P-OCS01	172.16.30.13	255.255.255.0	172.16.30.0	172.16.30.254	OCS Inventory
SRV-P-NETBOX01	172.16.30.22	255.255.255.0	172.16.30.0	172.16.30.254	Outil d'infrastructure
SRV-P-EDR01	172.16.30.19	255.255.255.0	172.16.30.0	172.16.30.254	EDR
SRV-P-POL01	172.16.30.25	255.255.255.0	172.16.30.0	172.16.30.254	Centreon Poller
SRV-P-DFS01	172.16.30.50	255.255.255.0	172.16.30.0	172.16.30.254	DFS01
SRV-P-GLPI01	172.16.30.14	255.255.255.0	172.16.30.0	172.16.30.254	GLPI

4.5. Stratégie de sauvegarde

L'infrastructure de sauvegarde repose sur le logiciel Veeam Backup & Replication et couvre 10 machines virtuelles hébergées sur des hôtes VMware ESXi.

Ce job assure une copie secondaire des sauvegardes vers un NAS dédié. La copie est décalée dans le temps afin d'éviter les conflits avec les jobs principaux.

La configuration GFS permet une conservation hebdomadaire sur 4 semaines et conservation mensuelle sur 2 mois.

4.5.3. Job Backup Copy – NAS 2

Élément	Configuration
Type	Backup Copy Job
Source	Backup Job ESXI (Job de sauvegarde principal)
Destination	NAS 2
Planification	Mardi, Vendredi (incrémental) / Dimanche (full) à 02h
Rétention	20 points de restauration
GFS	4 weekly / 2 monthly

Ce second job de copie introduit une redondance supplémentaire avec un décalage sur la copie du full (dimanche), renforçant la résilience globale du système.

Stratégie de protection

Cette architecture répond aux objectifs suivants :

- Disponibilité rapide grâce aux sauvegardes locales
- Redondance avec deux copies distinctes
- Protection contre la perte de données via la multiplication des supports
- Archivage avec la politique GFS

On essaie de se rapprocher le plus possible de la règle 3-2-1, voir annexe 2 pour explication.

4.6. Planification du projet :

Une fois toutes les informations recueillies, j'ai pu débiter la planification des différents créneaux d'intervention. Pour cela, j'ai structuré l'avancement sous forme de projet dans un fichier Excel, présenté au format diagramme de Gantt.

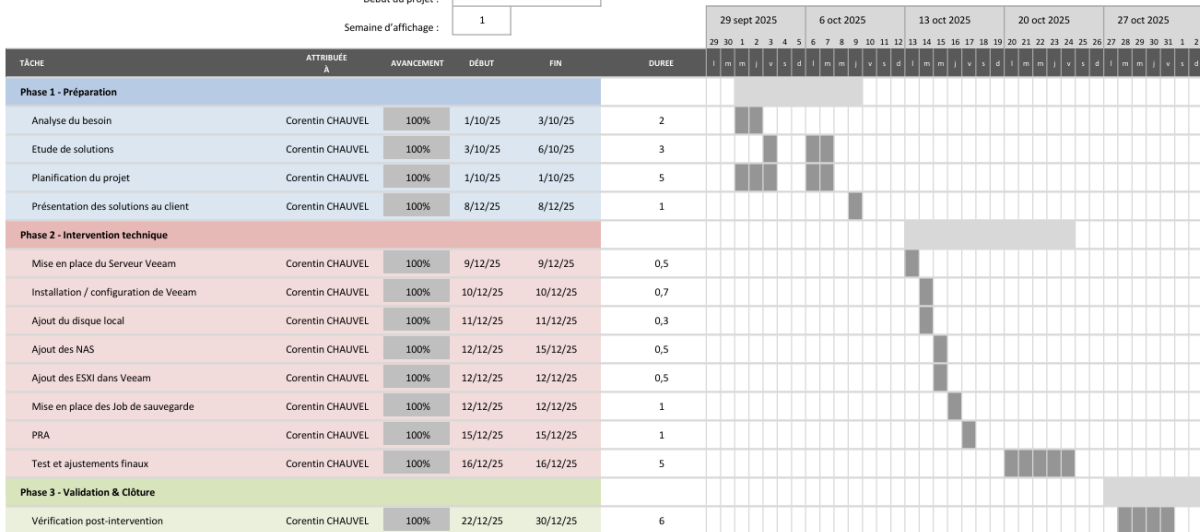
Mise en place Veeam

NTxSYSTEM

Chef de projet : Corentin CHAUVEL

DIAGRAMME DE GANTT

Début du projet : 01/10/2025
Semaine d'affichage : 1



4.7. Mise en production de la solution

4.7.1. Règle Firewall

Pour la mise en production du serveur Veeam, il a été nécessaire d'ouvrir certains flux sur le pare-feu.

À cet effet, deux règles ont été créées sur l'interface VLAN30_SERVEUR, dans lequel se trouve le serveur Veeam :

- Une première règle autorise le serveur Veeam à communiquer sur des ports spécifiques avec les deux hôtes ESXi.
- Une seconde règle permet au serveur Veeam de communiquer avec les deux NAS.

Les communications pour ces deux règles utilisent les protocoles TCP et UDP.



4.7.2. Installation et configuration de Veeam backup & replication

Voir l'annexe 1 pour l'installation de Windows Serveur.

Le serveur Veeam est configuré avec 4 vCPU, 12 Go de mémoire vive, 60 Go de stockage et une interface réseau connectée au réseau SERVEUR (Vlan 30). Et un disque de 850go pour les sauvegardes. Pour des raisons de sécurité, le serveur est maintenu hors

domaine. Les accès sont strictement limités au compte administrateur, garantissant un contrôle renforcé des connexions.

Modifier les paramètres - SRV-P-BCK01 (Machine virtuelle ESXi 8.0 U2)

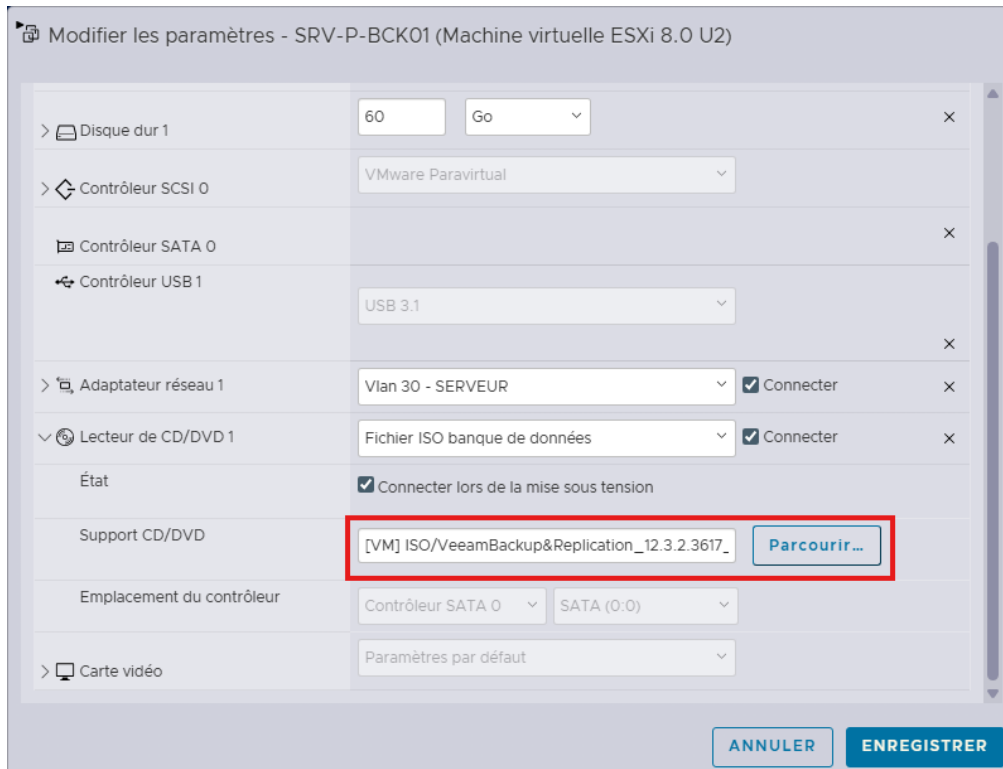
Matériel virtuel Options VM

Ajouter un disque dur Ajouter un adaptateur réseau Ajouter un autre périphérique

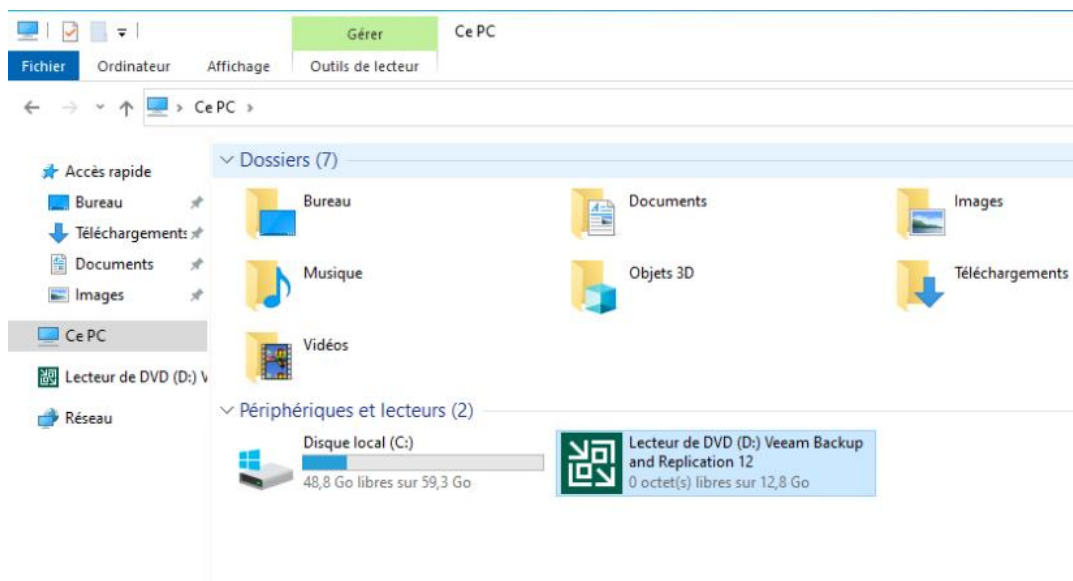
> CPU	4	<input type="button" value="Go"/>	<input type="button" value="X"/>
> Mémoire	12	<input type="button" value="Go"/>	<input type="button" value="X"/>
> Disque dur 1	60	<input type="button" value="Go"/>	<input type="button" value="X"/>
> Disque dur 2	850	<input type="button" value="Go"/>	<input type="button" value="X"/>
> Contrôleur SCSI 0	VMware Paravirtual		
Contrôleur SATA 0			<input type="button" value="X"/>
Contrôleur USB 1	USB 3.1		<input type="button" value="X"/>
> Adaptateur réseau 1	Vlan 30 - SERVEUR	<input checked="" type="checkbox"/> Connecter	<input type="button" value="X"/>
> Lecteur de CD/DVD 1	Fichier ISO banque de données	<input checked="" type="checkbox"/> Connecter	<input type="button" value="X"/>

4.7.2.1. Installation

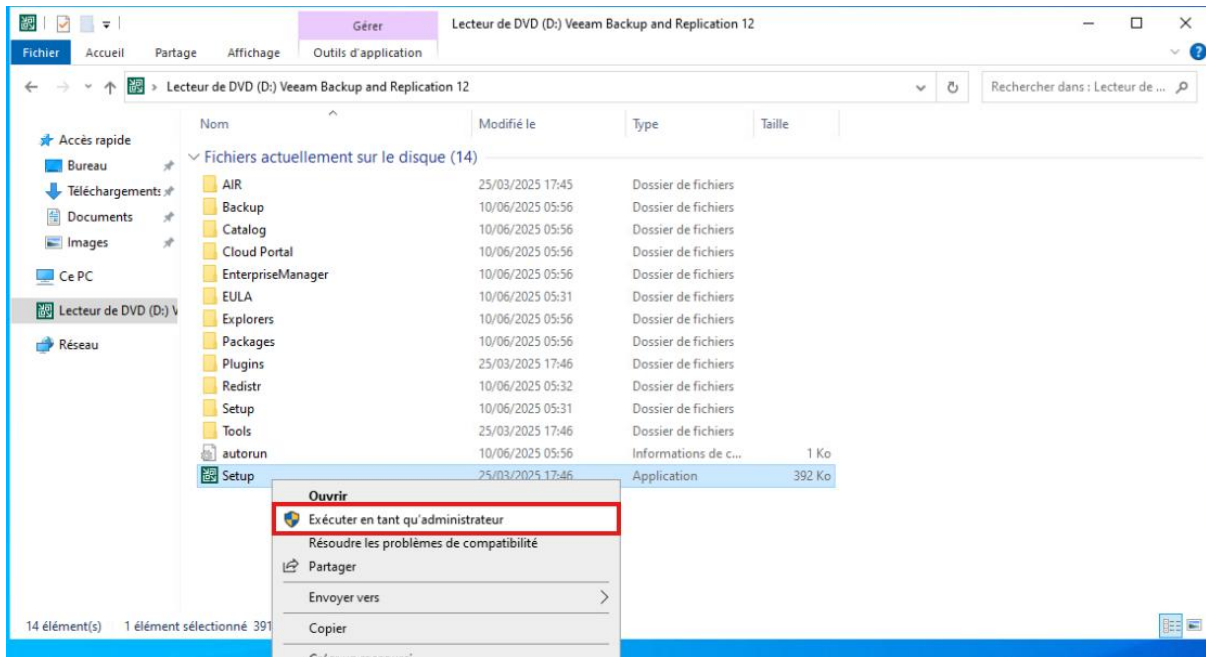
Une fois la VM installée sur l'ESXi 1, il faut dans la configuration de la machine virtuelle sur l'ESXi, ajouter l'ISO (veeam backup & replication) d'installation dans le lecteur CD/DVD.



Puis, rendez-vous sur le serveur et cliquez sur le lecteur DVD visible dans « Ce PC ».

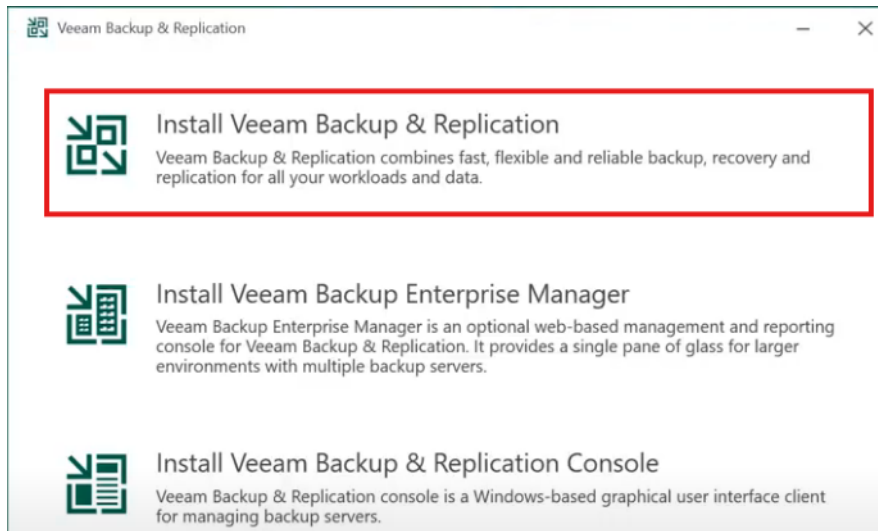


Dans ce lecteur, exécutez le programme d'installation (Setup) en tant qu'administrateur.

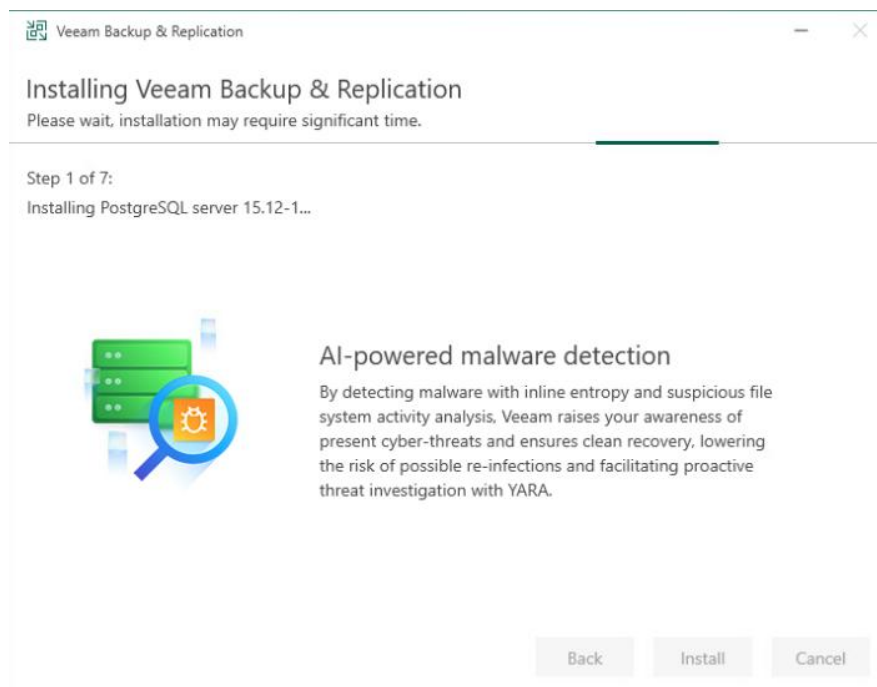


Lorsque celui-ci est lancé, cliquez sur « Install », puis sélectionnez « Install Veeam Backup & Replication » pour démarrer l'installation.

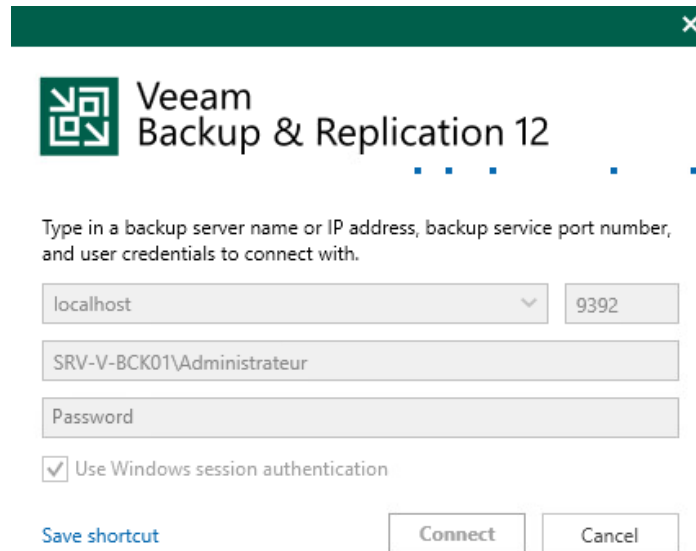




Une série de 7 étapes s'exécute ensuite : Veeam vérifie la compatibilité du système et installe les différents packages nécessaires.



Une fois les 7 étapes terminées, Veeam est installé et vous pouvez vous connecter à l'interface « Veeam Backup & Replication ».

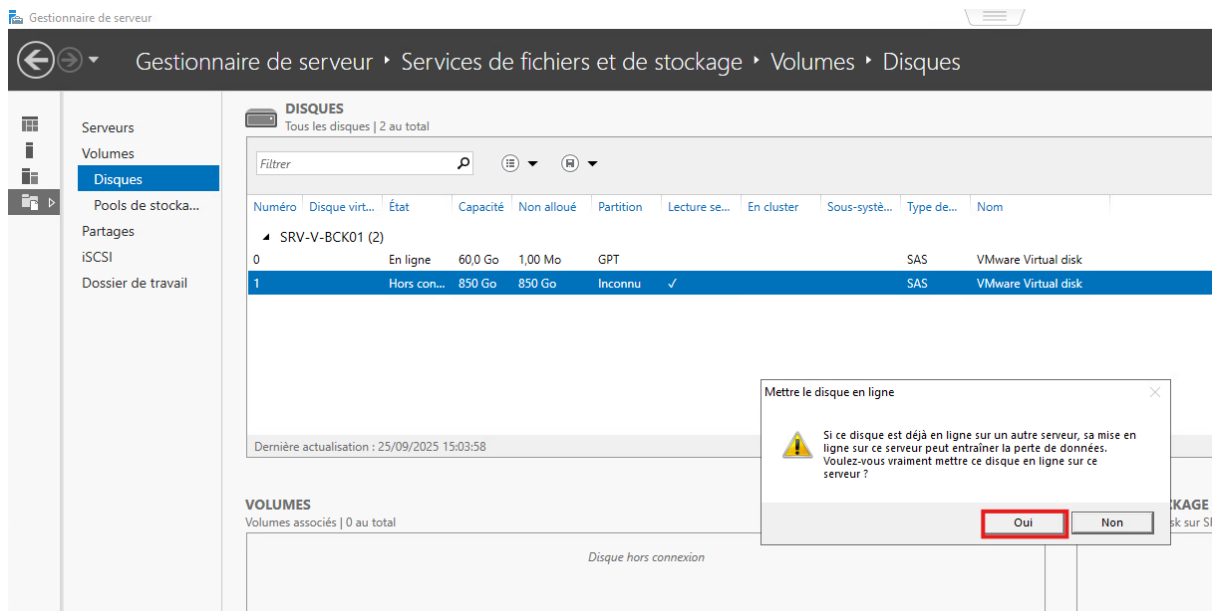


4.7.2.2. Configuration

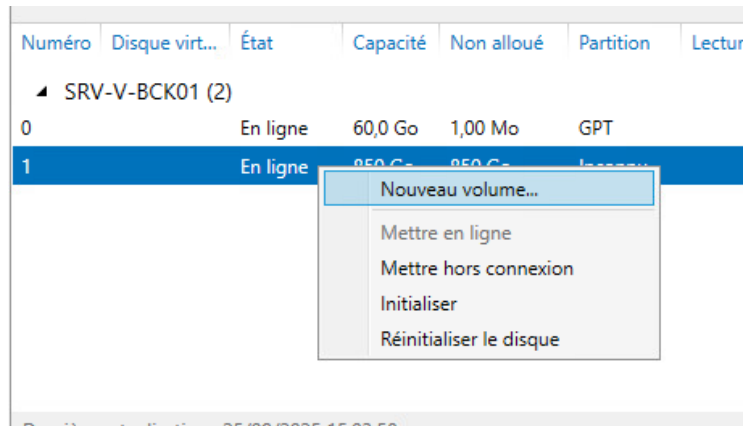
4.7.2.2.1. Ajout du disque local pour les sauvegardes

Dans un premier temps, il faut configurer le disque de sauvegarde local sur la VM. Ce disque, d'une capacité de 850 Go, sera dédié aux sauvegardes.

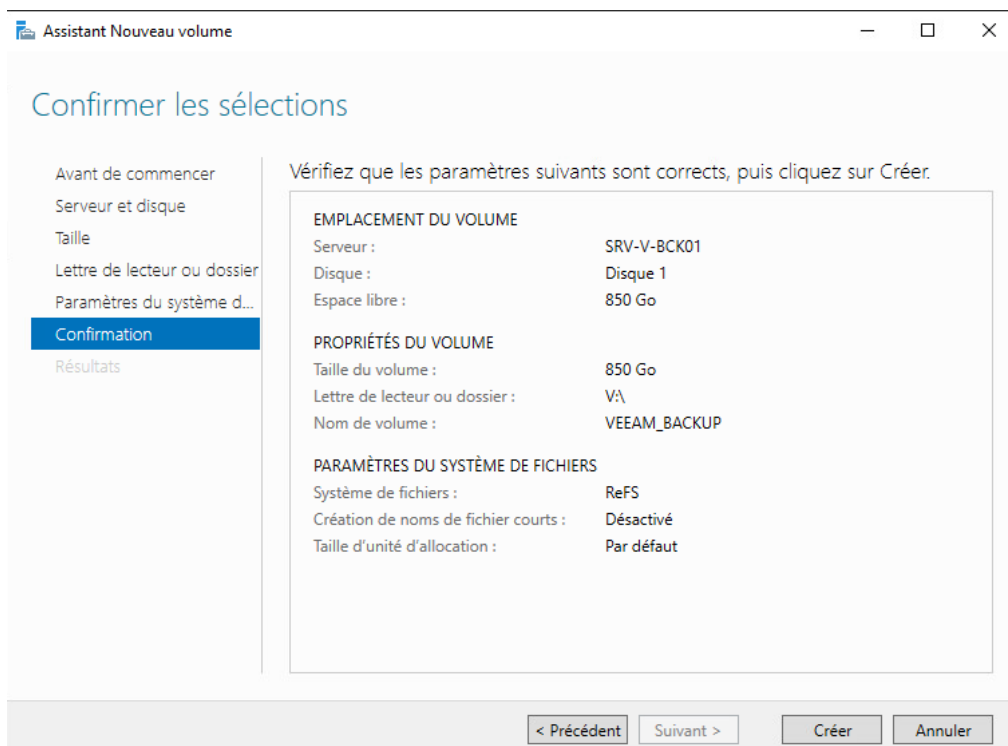
Dans le Gestionnaire de serveur, allez dans « Services de fichiers et de stockage » > « Volumes » > « Disques ». Le disque de 850 Go apparaît comme « Hors connexion » : il faut le mettre en ligne.



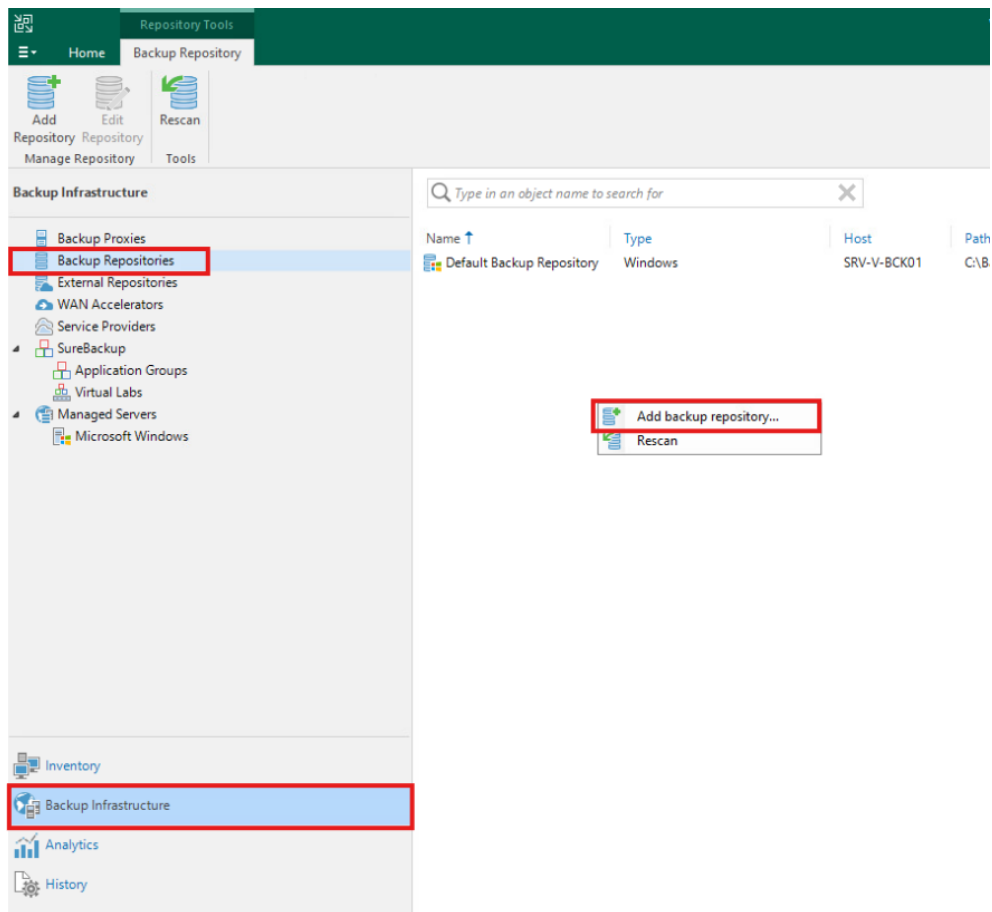
Ajoutez ensuite un nouveau volume sur le disque.



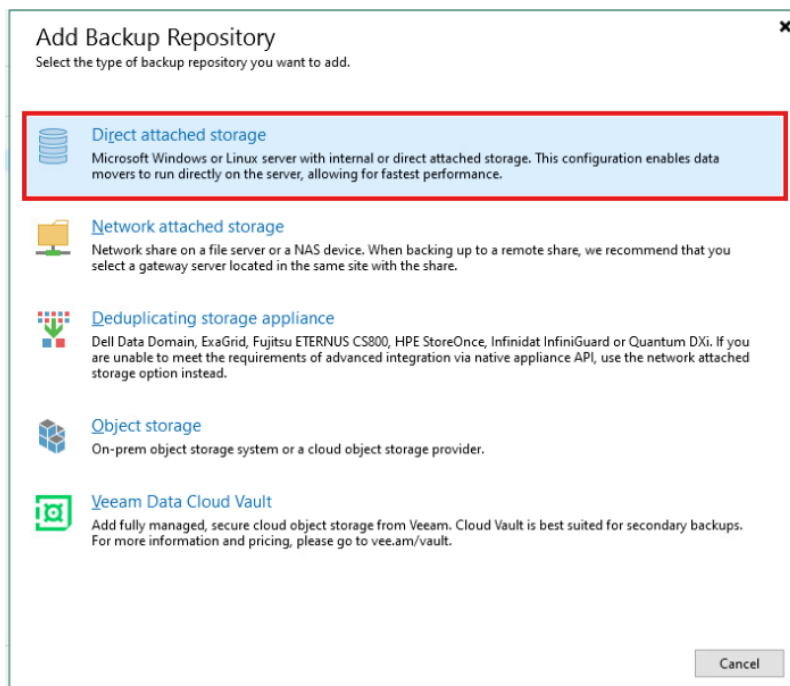
Suivez l'assistant de configuration jusqu'au bout à la fin, vous devez obtenir la configuration suivante.



Une fois la création terminée, connectez-vous à l'interface Veeam Backup & Replication. Dans « Backup Infrastructure » > « Backup Repositories », cliquez sur « Add Backup Repository ».

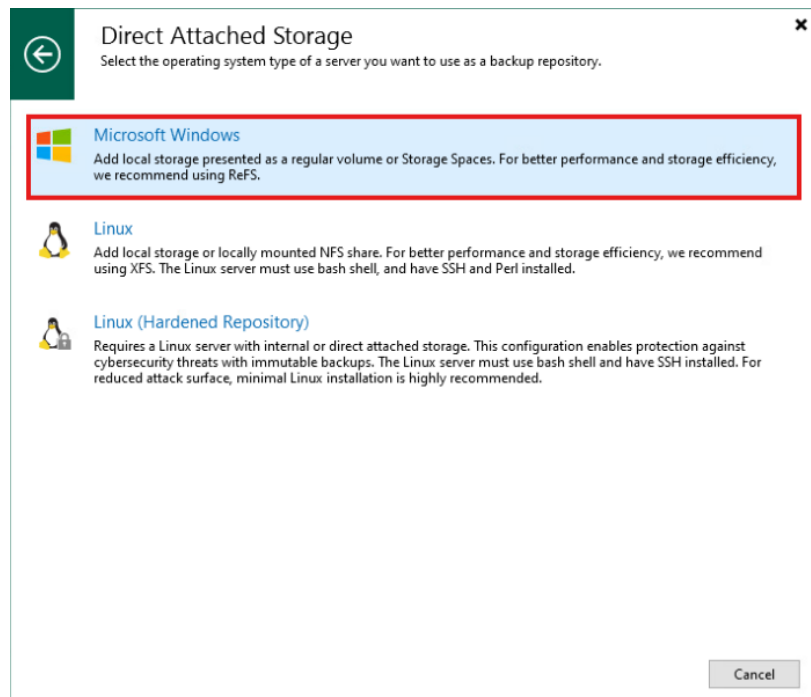


Sélectionnez « Direct Attached Storage » afin d'ajouter le disque à l'infrastructure de sauvegarde.

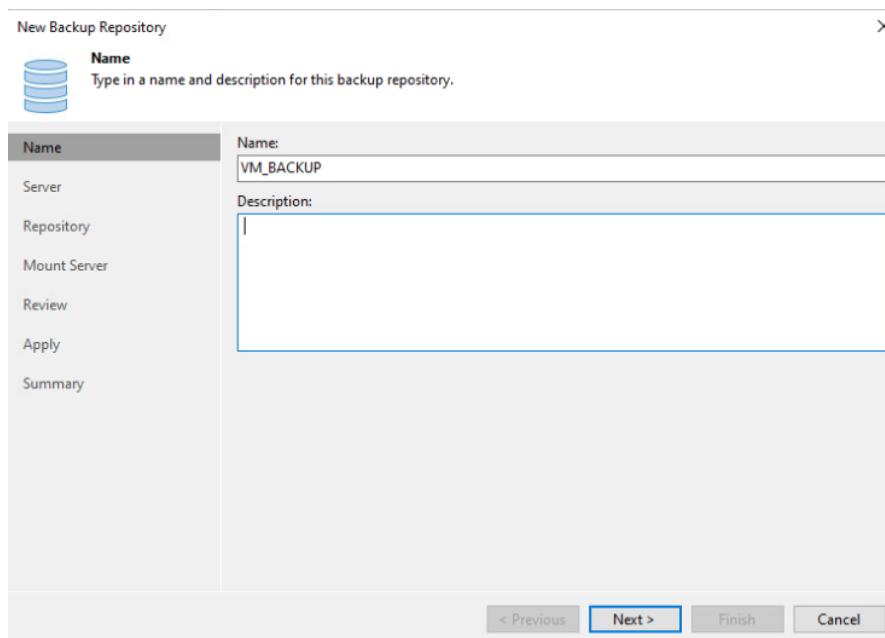


Dans cette étape, il faut choisir le type de stockage à ajouter comme dépôt de sauvegarde.

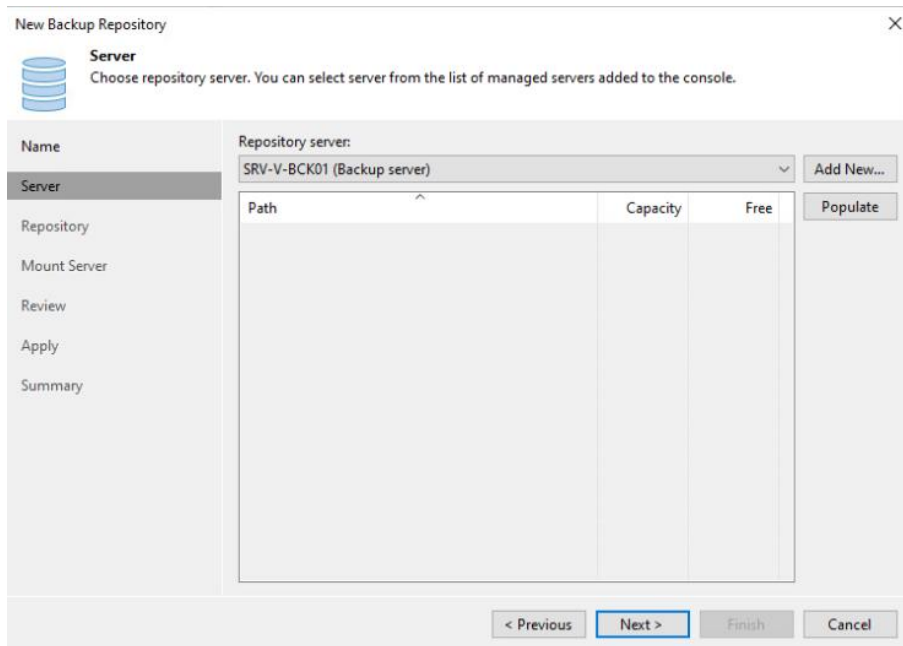
Sélectionnez « Microsoft Windows », comme indiqué sur l'image, afin d'utiliser le disque local de 850go de la machine virtuelle. Ce choix permet d'ajouter un stockage directement attaché (disque local) en tant que dépôt de sauvegarde Veeam.



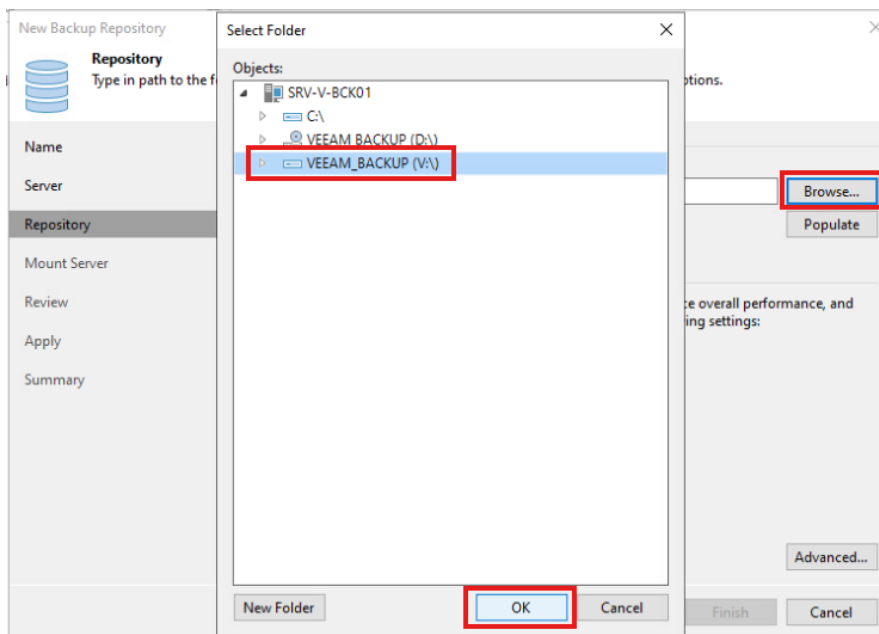
Ensuite définition du dépôt de sauvegarde, Saisir le nom du repository (VM_BACKUP) et ajouter une description optionnelle pour identifier son usage.



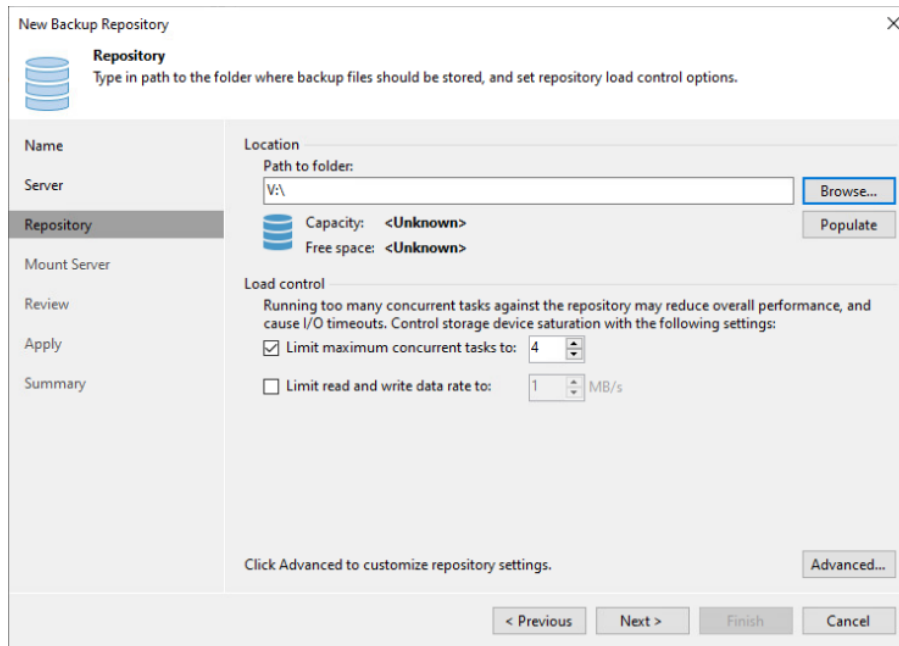
Dans un second temps, le choix du serveur de stockage : il faut sélectionner le serveur Veeam qui hébergera les fichiers de sauvegarde.



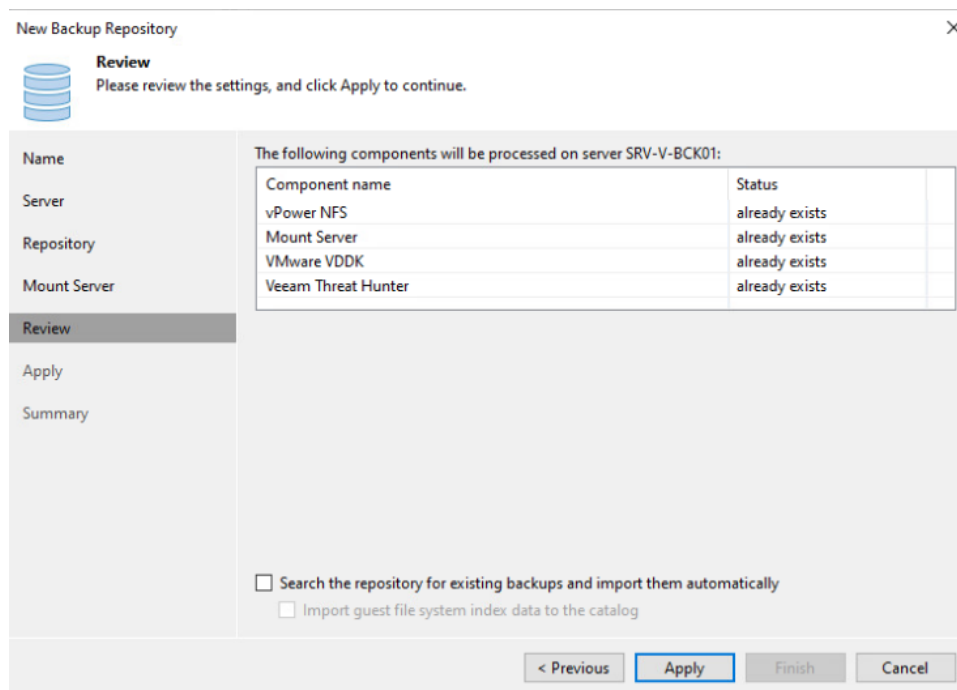
Cliquez sur Browse, choisissez le disque VEEAM_BACKUP (V:), puis validez avec OK.



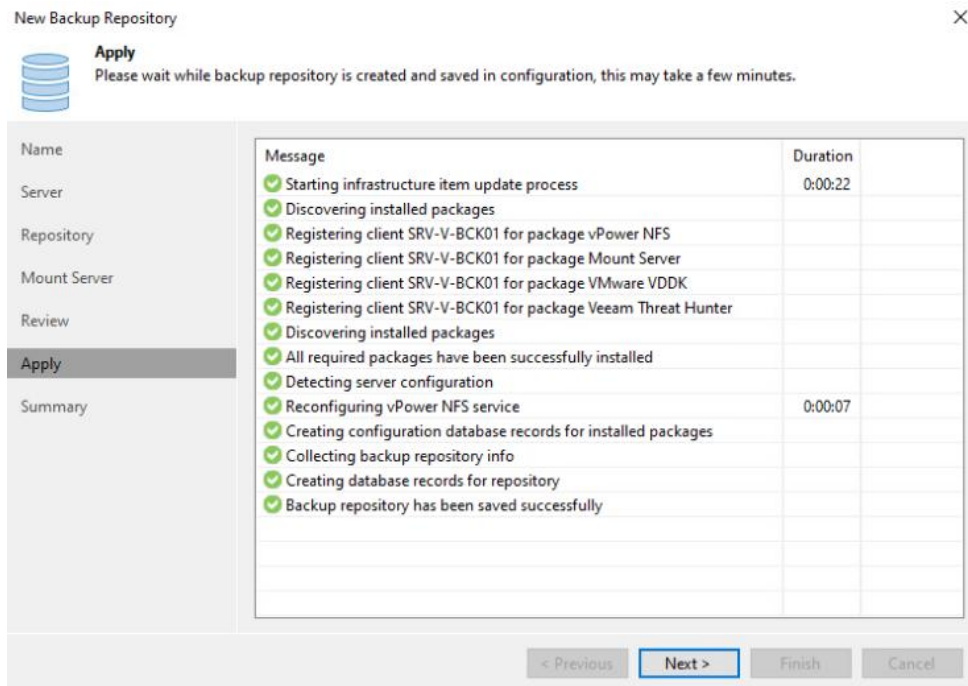
Définissez le chemin de stockage (V:\) et configurez les paramètres de performance si besoin ; pour que les sauvegardes soient effectuées directement à la racine.



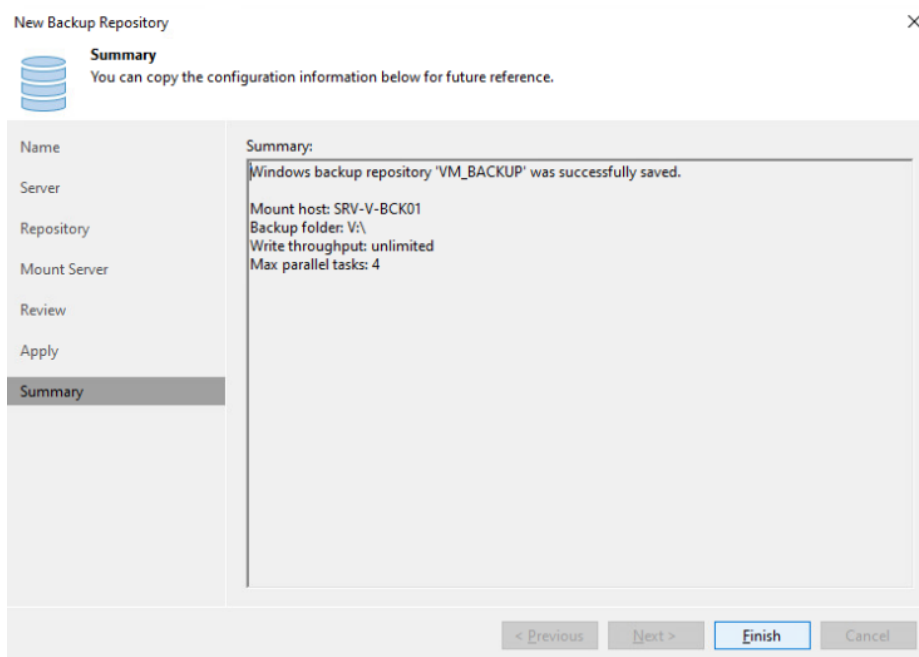
Vérifiez que tous les composants requis sont déjà installés sur le serveur.



Lancez la création du repository et attendez la validation complète des étapes.



Le repository VM_BACKUP a été créé avec succès.



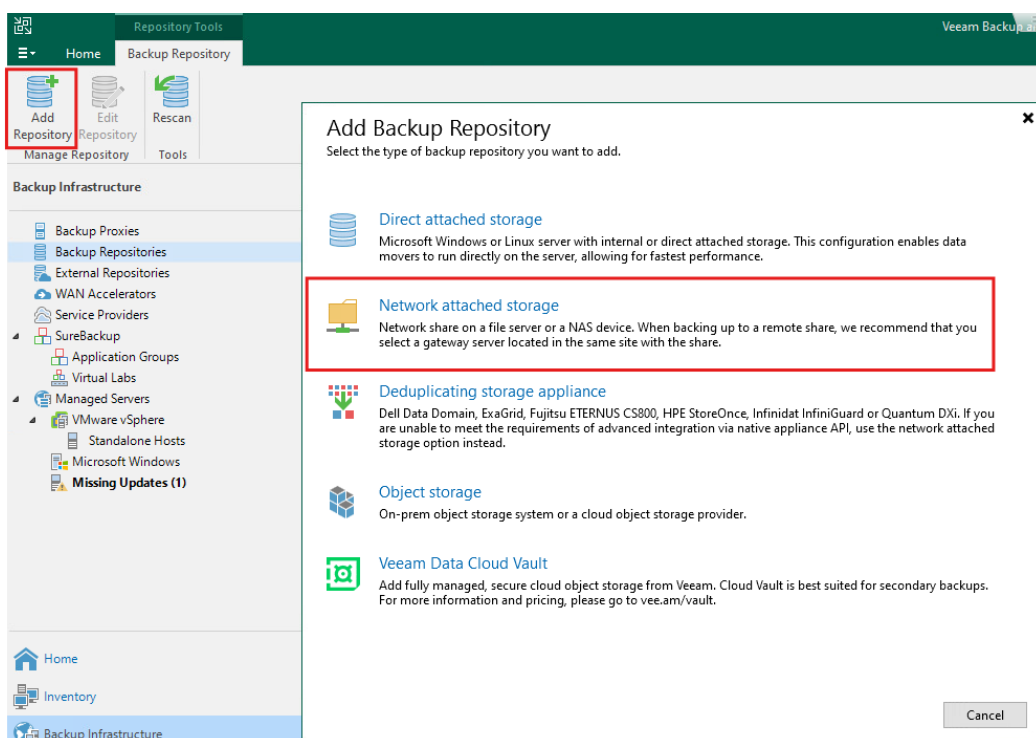
On peut ensuite supprimer le « Default Backup Repository », car il se trouve sur le disque système, il est donc recommandé d'éviter d'y stocker des sauvegardes.

Name ↑	Type	Host	Path	Capac...
Default Backup Repository	Windows	SRV-BACKUP	C:\Backup	59.4 GB
VM_BACKUP	Windows	SRV-BACKUP	Rescan	B

4.7.2.2.2. Ajout des NAS pour la sauvegarde externe

Le procédé présenté concerne le NAS 2. La même opération a été réalisée pour le NAS 1 en adaptant les adresses IP et le nom.

Sélection du type de repository dans Veeam Backup & Replication. Ici, on choisit Network attached storage, car le stockage cible est un NAS accessible via le réseau.



Définition du nom et de la description du dépôt de sauvegarde. Cela permet d'identifier facilement le NAS dans l'infrastructure (ex : NAS-BCK02).

New Backup Repository

Name
Type in a name and description for this backup repository.

Name:
NAS-BCK02

Description:
Created by SRV-V-BCK01\Administrateur at 26/03/2026 14:16.

< Previous **Next >** Finish Cancel

Saisie du chemin du partage réseau (ex : \\10.44.110.214\Ntxsystem). Choix du Gateway Server (automatique ici) qui servira d'intermédiaire entre Veeam et le NAS.

New Backup Repository

Share
Specify a file share to store backups in, and a gateway server to access NFS share through. Automatic gateway selection functionality requires that NFS Tools are installed on registered Linux servers.

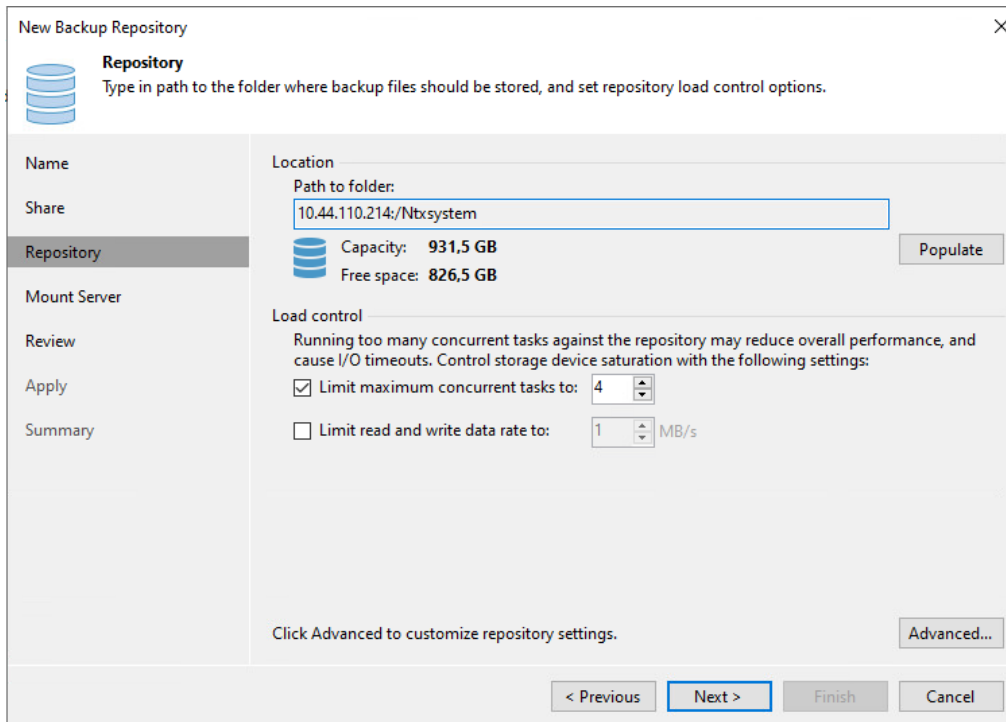
Shared folder:
10.44.110.214/Ntxsystem
Use server/folder format

Gateway server:
Automatic selection Choose...

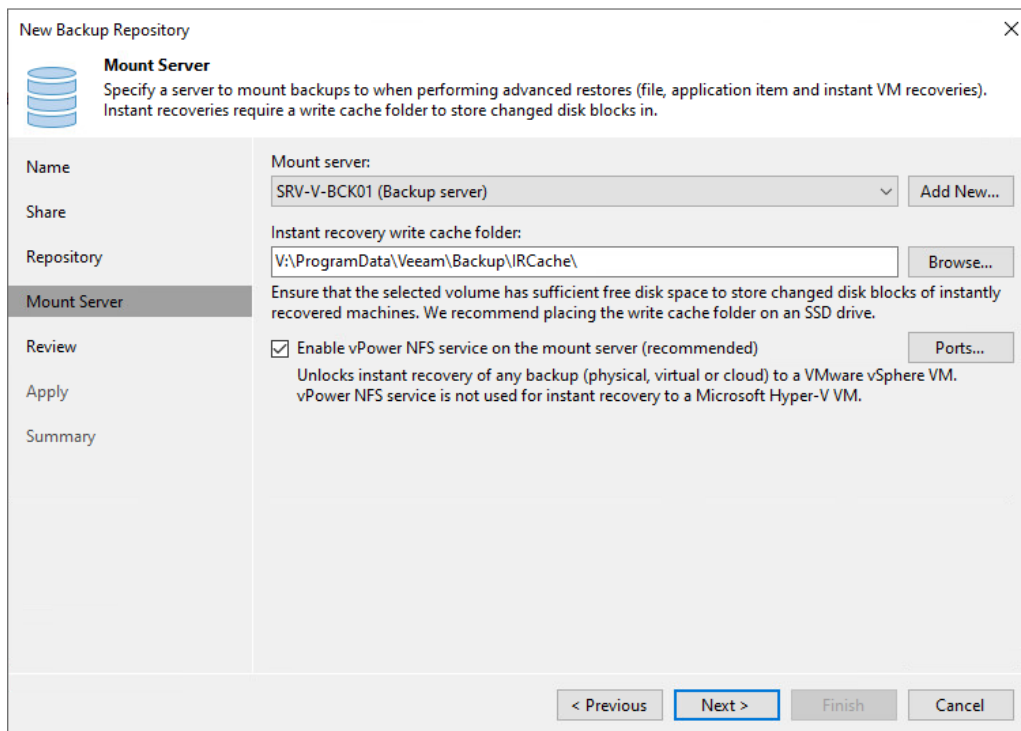
< Previous **Next >** Finish Cancel

Validation du chemin et affichage de la capacité du NAS.

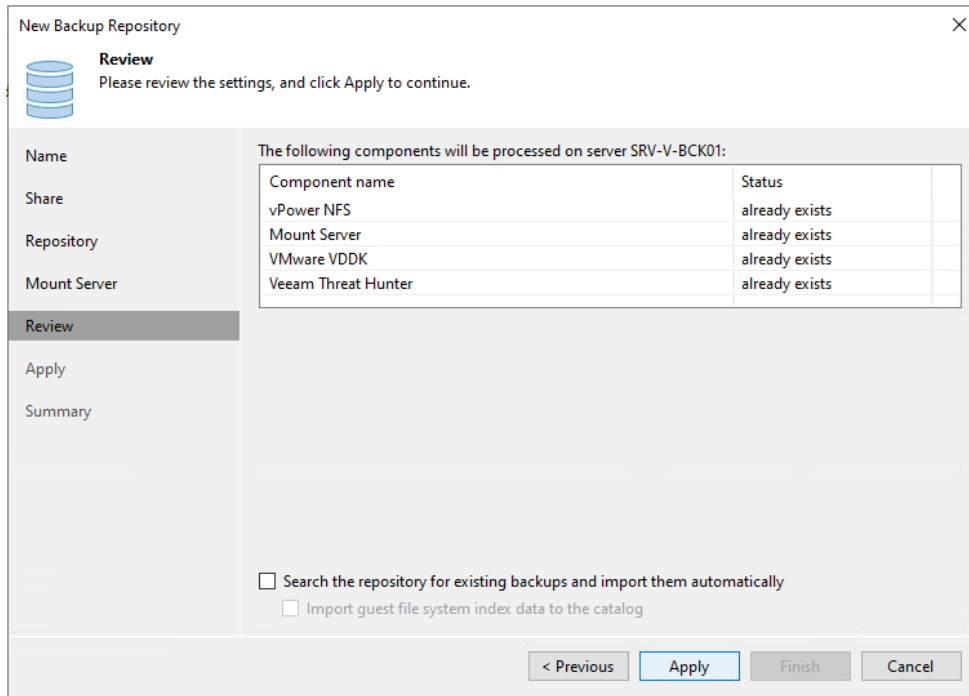
Configuration des performances : Limitation du nombre de tâches simultanées, option de limitation du débit (si nécessaire).



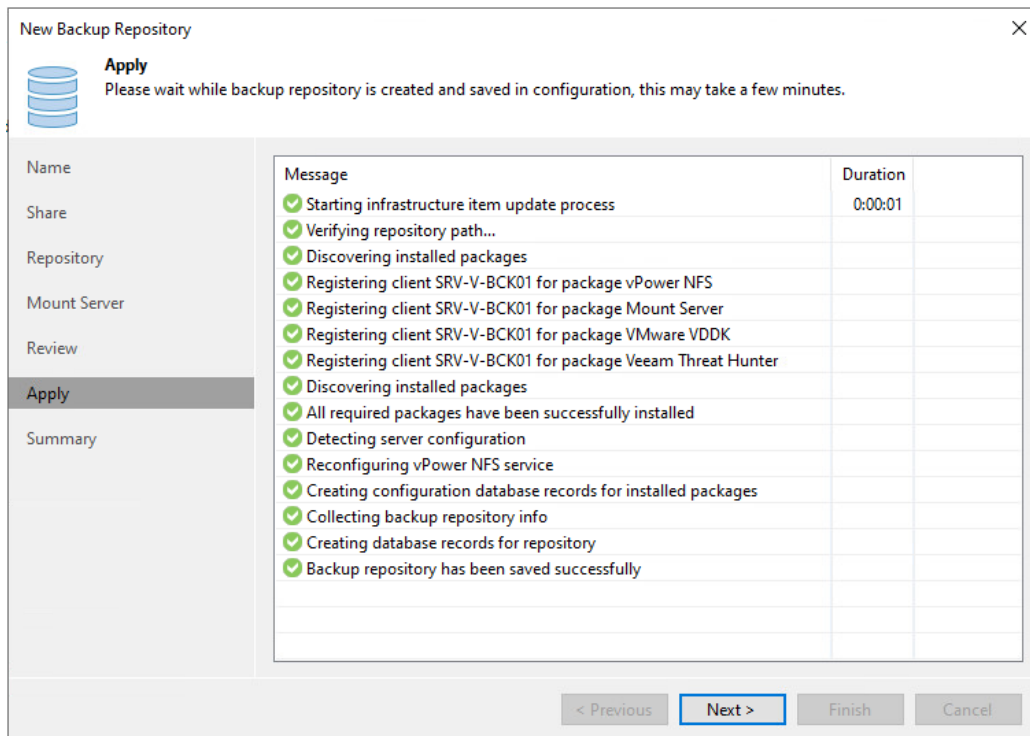
Définition du serveur utilisé pour : les restaurations avancées les Instant Recovery
 Configuration du dossier cache (important pour les performances). Option activée :
 service vPower NFS pour les restaurations rapides.



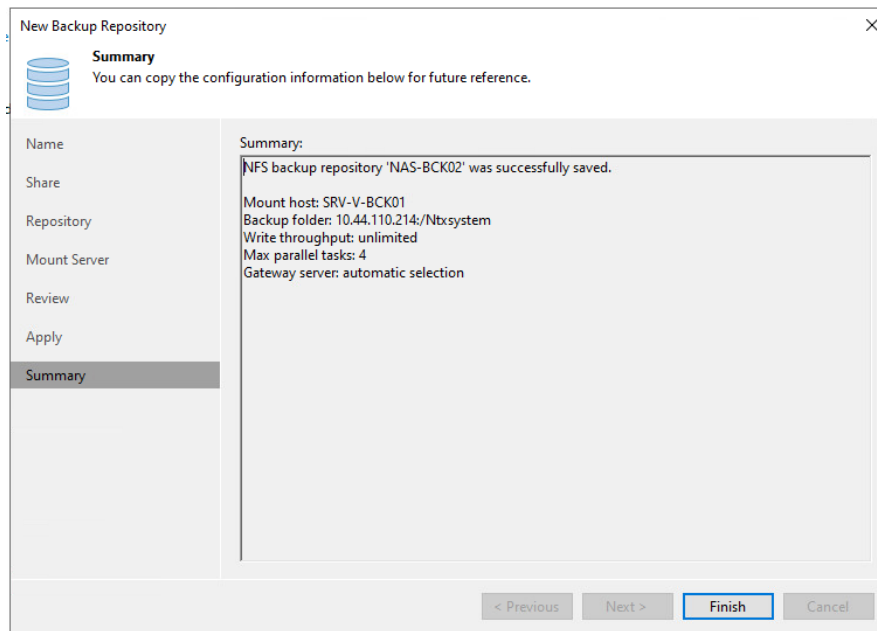
Résumé des composants utilisés sur le serveur (NFS, Mount Server, VDDK...). Permet de vérifier que tous les prérequis sont déjà installés avant validation.



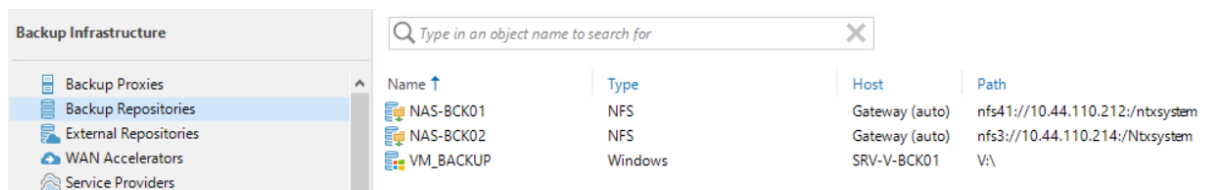
Veeam installe et configure automatiquement les composants nécessaires. Chaque étape est validée jusqu'à la création complète du repository.



Confirmation de la création du repository NAS. Le stockage NAS est maintenant prêt à être utilisé pour les sauvegardes externes.



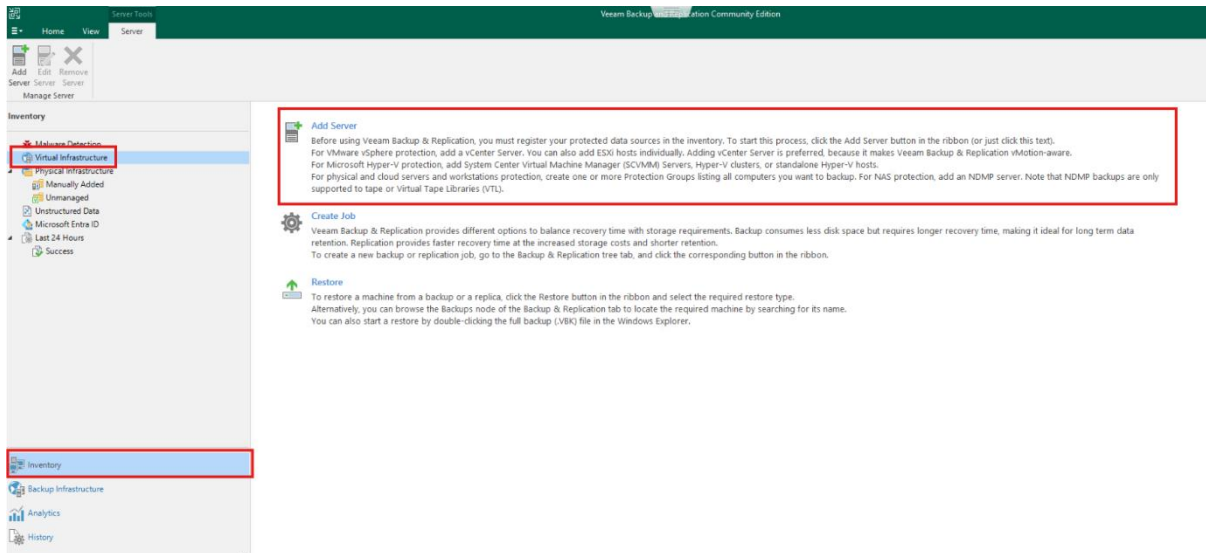
Voici le résultat obtenu après l'ajout des deux NAS dans Veeam.



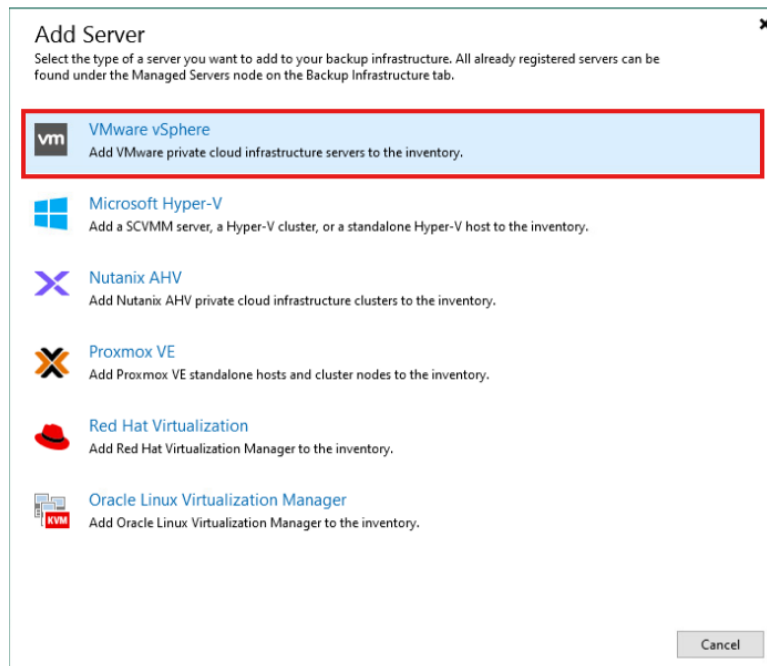
4.7.2.2.3. Ajout des ESXI dans Veeam pour la sauvegarde

Pour pouvoir faire les sauvegardes, il faut ajouter les deux esxi dans le serveur Veeam. C'est la même procédure pour les deux, je vais montrer pour le premier.

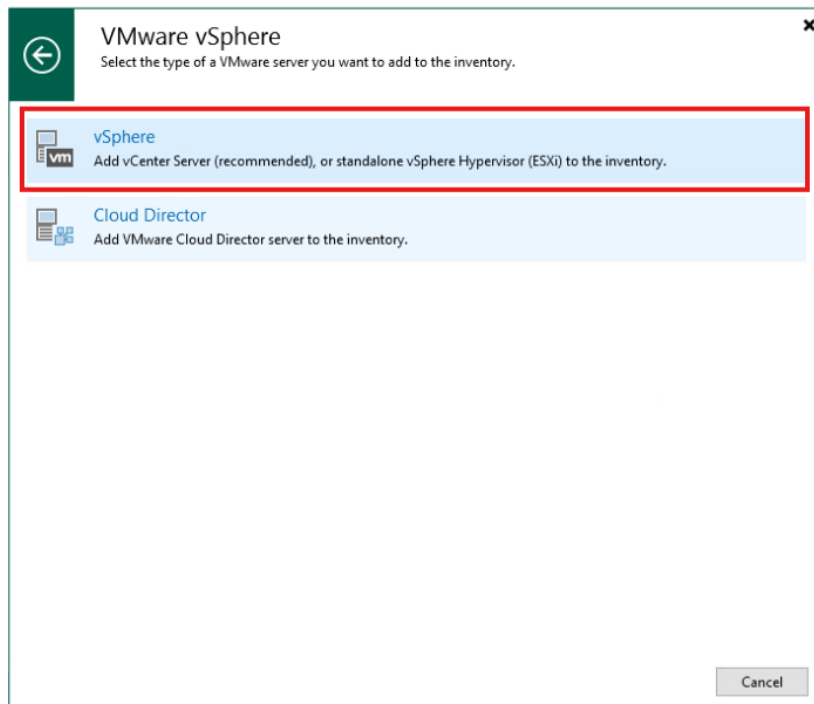
Dans l'interface de Veeam Backup & Replication, accéder au menu Inventory, puis Virtual Infrastructure et cliquer sur Add Server. Cette étape permet d'ajouter une nouvelle source de virtualisation à superviser.



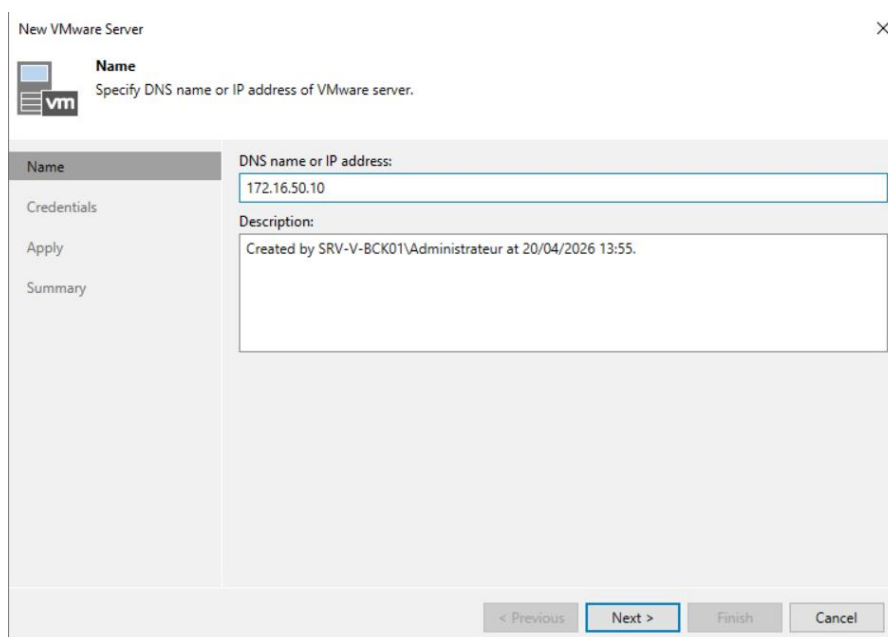
Dans la fenêtre Add Server, sélectionner VMware vSphere. Ce choix est nécessaire pour gérer un hôte ESXi.



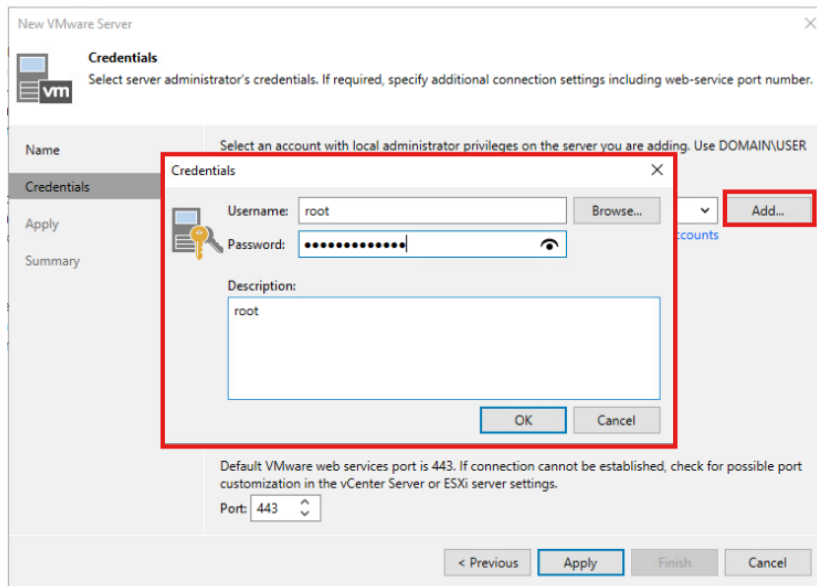
Confirmer la sélection de vSphere pour ajouter un hôte ESXi autonome.



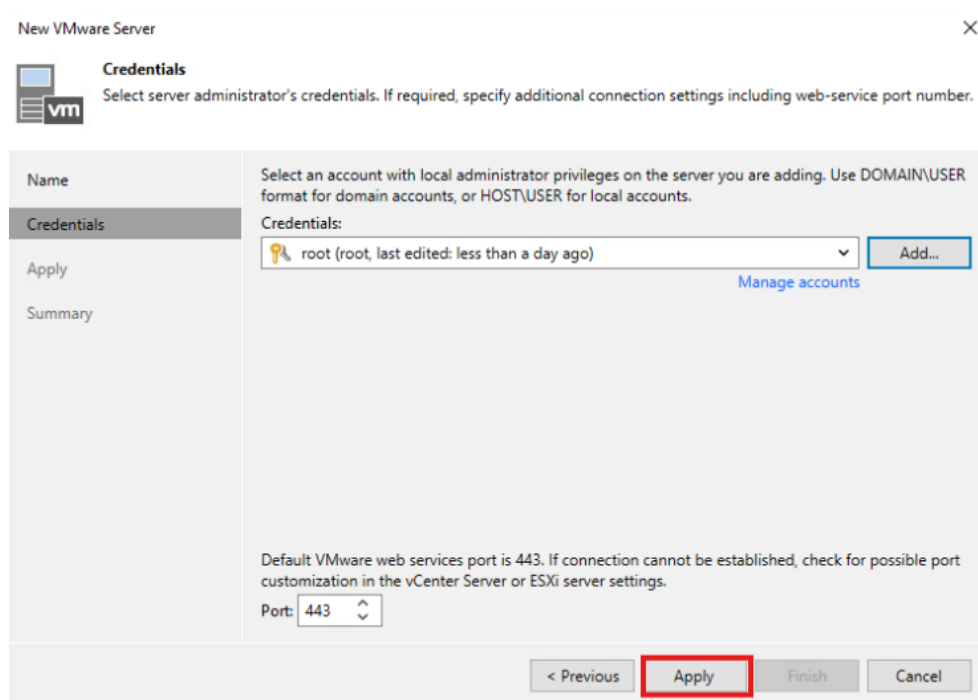
Entrer l'adresse IP de l'hôte ESXi à ajouter. Cette information permet à Veeam d'établir la connexion avec l'hyperviseur.



Cliquer sur Add pour renseigner les identifiants administrateur de l'ESXi. Ces identifiants doivent disposer des droits suffisants pour accéder à l'infrastructure (Il faut utiliser le compte root de l'ESXi.).



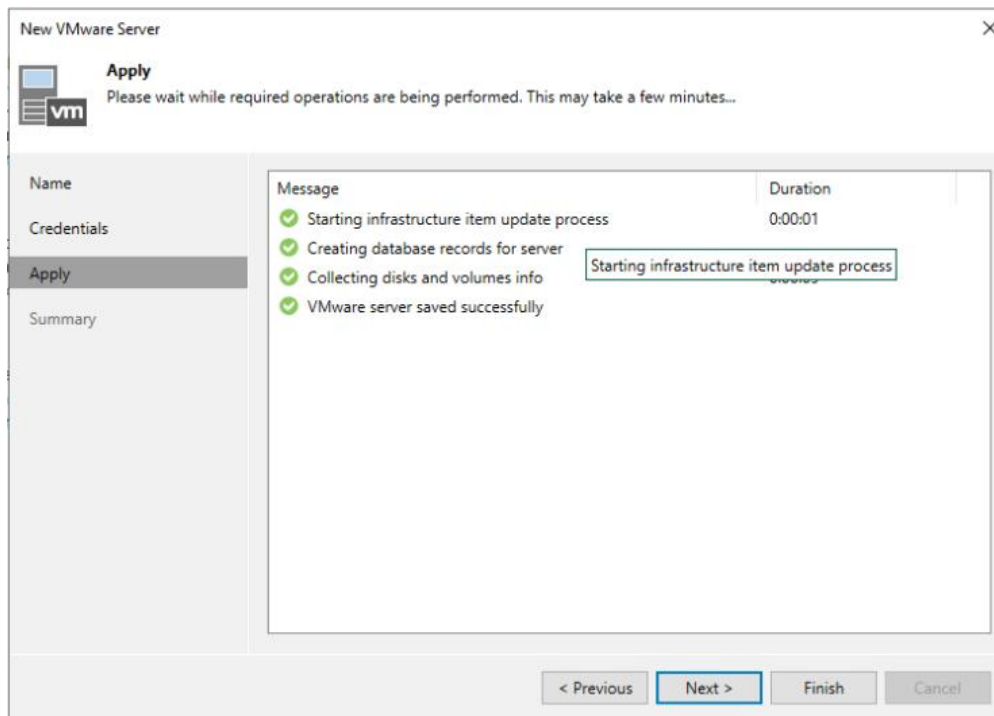
Vérifier que le compte ajouté apparaît bien dans la liste, puis cliquer sur Apply pour lancer la connexion au serveur.



Veeam lance automatiquement :

- La collecte des informations
- L'inventaire des disques et machines virtuelles,
- La validation de la connexion.

Tous les indicateurs doivent être au vert pour confirmer le bon ajout.

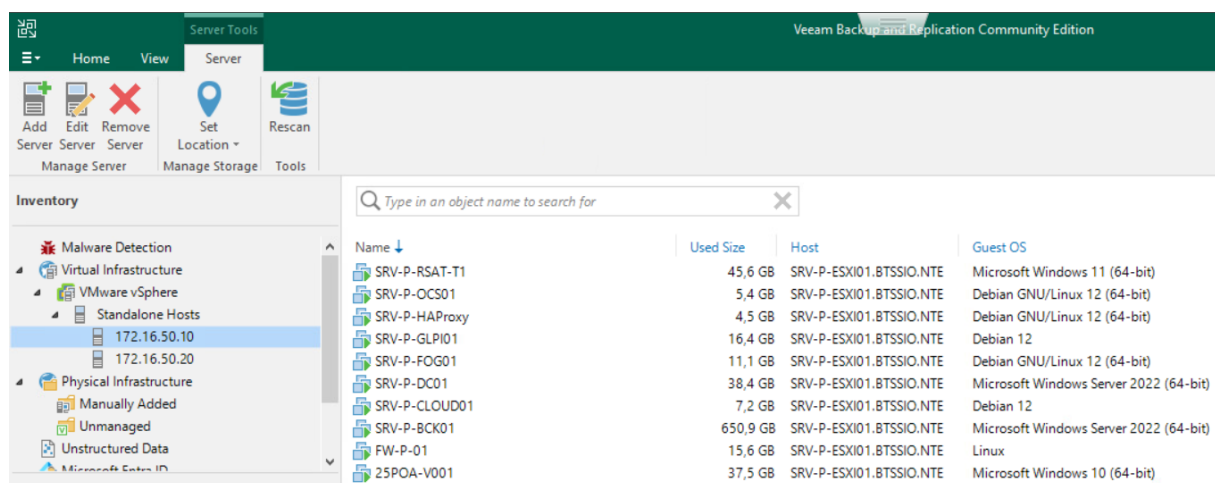


Un récapitulatif s'affiche avec :

- L'adresse du serveur ESXi
- Le port utilisé (443)
- L'utilisateur connecté

Cliquer sur Finish pour finaliser l'ajout.

L'hôte ESXi ajouté apparaît désormais dans l'inventaire Veeam avec ses machines virtuelles. Cela confirme que l'intégration est opérationnelle.



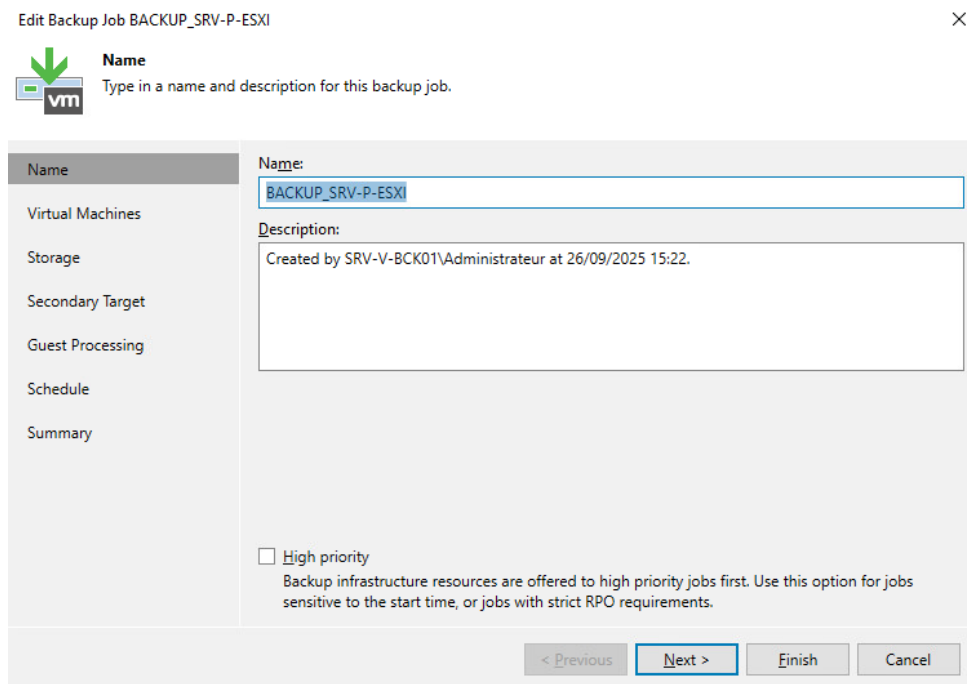
4.7.2.2.4. Mise en place d'un Job de sauvegarde

Ce job permettra de sauvegarder les VM que l'on a choisies sur les deux ESXi.

Depuis le menu principal, cliquer sur Backup Job puis Virtual machine. Cela permet de créer un job de sauvegarde pour les VM hébergées sur les ESXi.



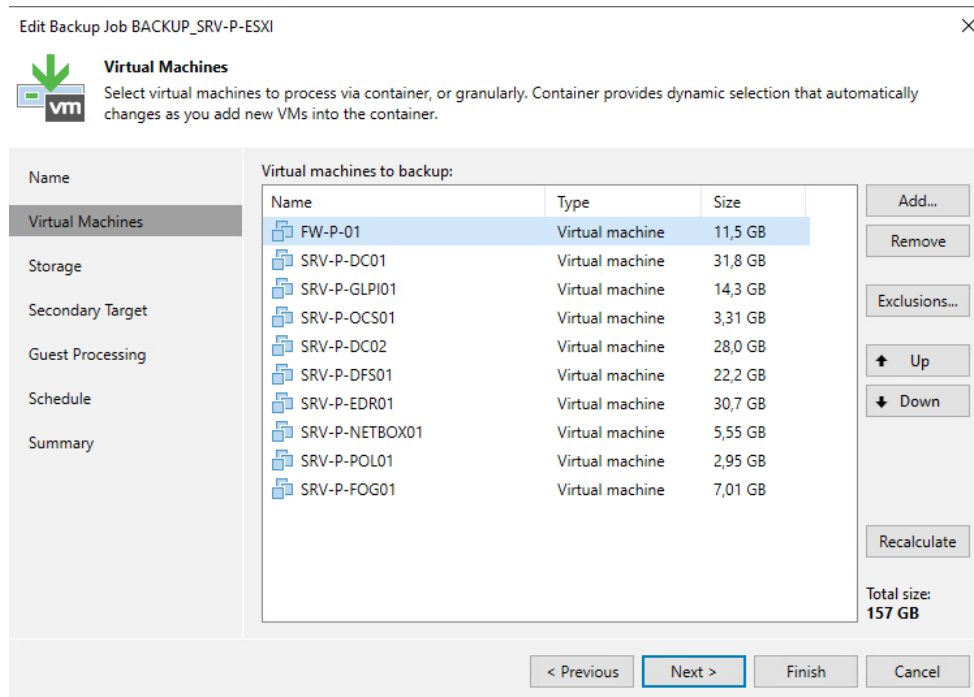
Renseigner un nom explicite pour le job (ex : BACKUP_SRV-P_ESXI).



Ajouter les VM à sauvegarder dans le job.

Il est possible de :

- Sélectionner plusieurs VM
- Organiser l'ordre de traitement
- Exclure certains éléments si nécessaire

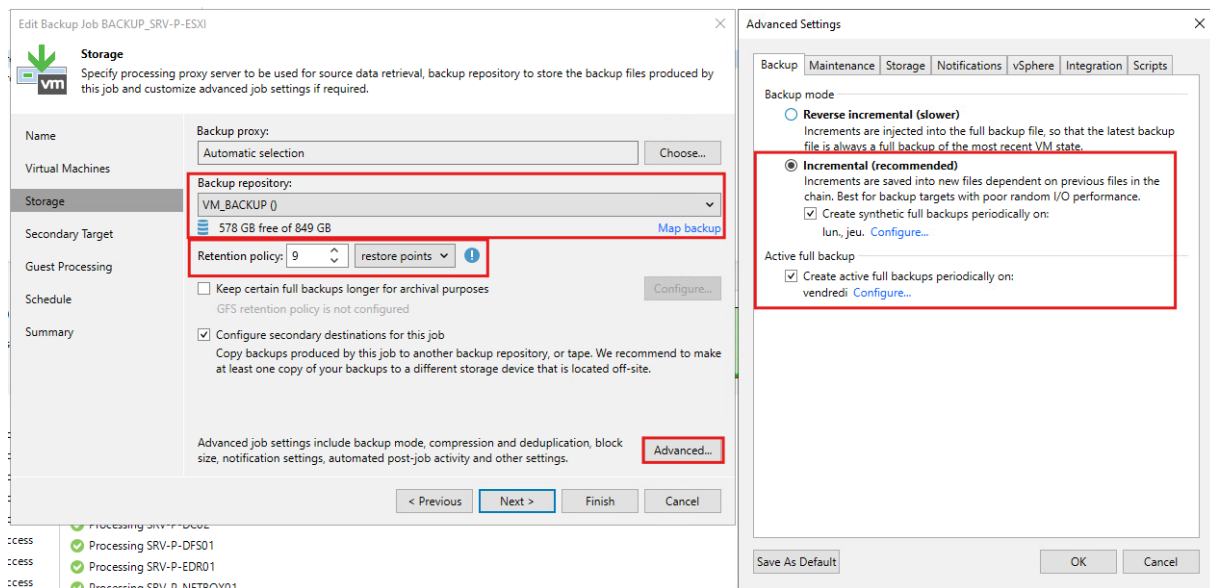


Choisir le repository de sauvegarde (emplacement de stockage).

Configurer également :

- La politique de rétention (nombre de points de restauration)
- Le type de sauvegarde

Ici, je choisis le disque de 850 Go (VM_BACKUP), une rétention de 9 points de restauration, avec une sauvegarde incrémentielle le lundi et le jeudi, et une sauvegarde complète (full) le vendredi.

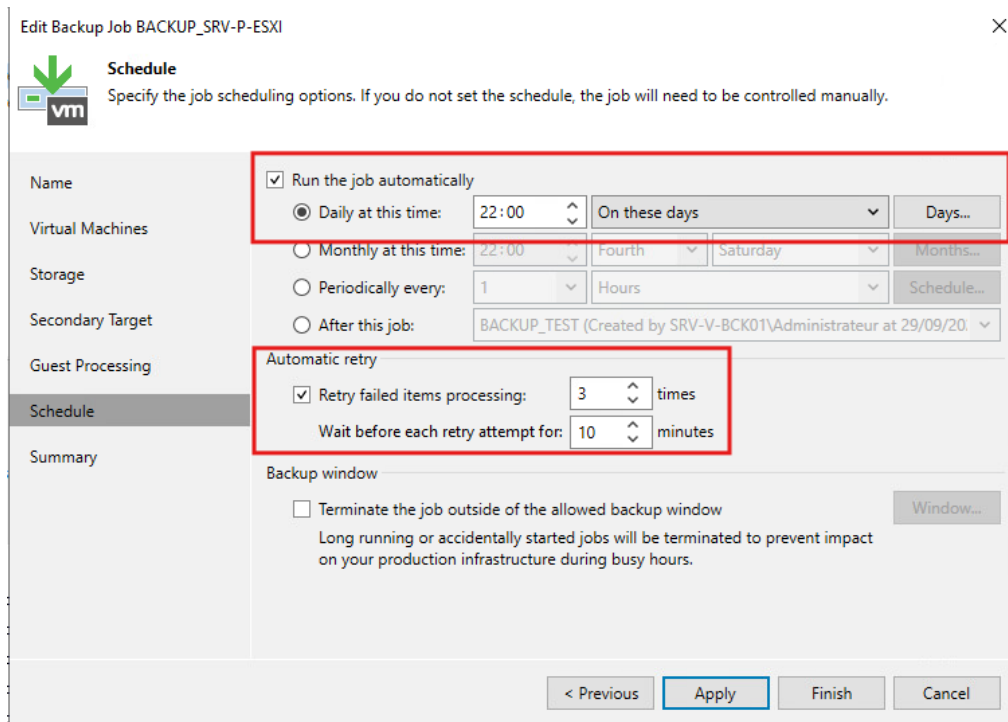


Configurer l'exécution automatique :

- Fréquence : ici lundi, jeudi et vendredi
- Heure de lancement : 22h00

Configurer aussi :

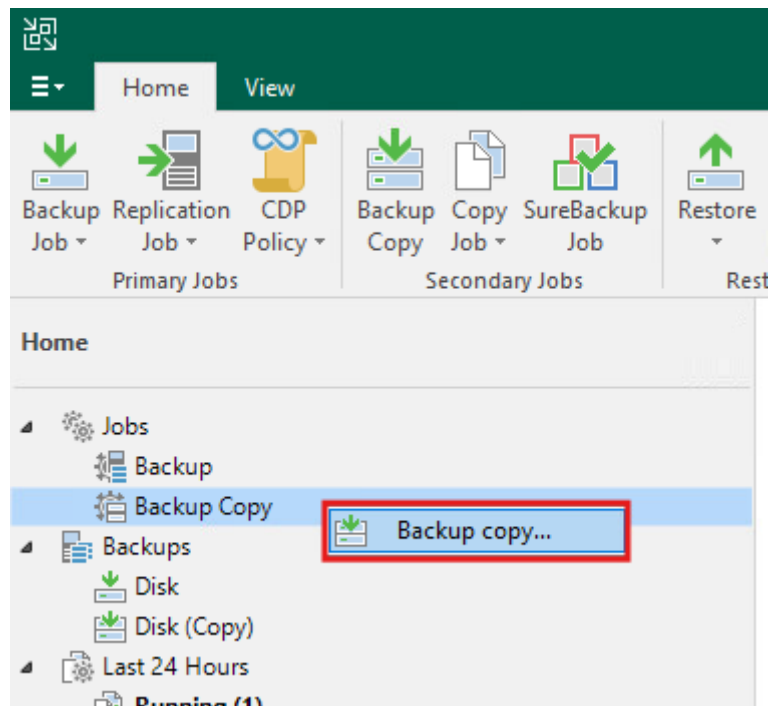
- Le nombre de tentatives en cas d'échec est de 3
- Le délai entre les tentatives est de 10min



4.7.2.2.5. Mise en place des Backup Copy Job (copie externe) vers le NAS 1

Ce job de copie permettra de dupliquer la sauvegarde réalisée par le job de sauvegarde des ESXi vers le NAS 1.

Dans le menu, cliquer sur Backup Copy. Ce type de job permet de copier les sauvegardes vers un autre stockage dans le nôtre un NAS.




Donner un nom au job (ex : NAS-BCK01_Externe).

Choisir le mode :

- Immediate copy : copie en temps réel
- Periodic copy : copie planifiée (recommandé pour optimiser la bande passante).

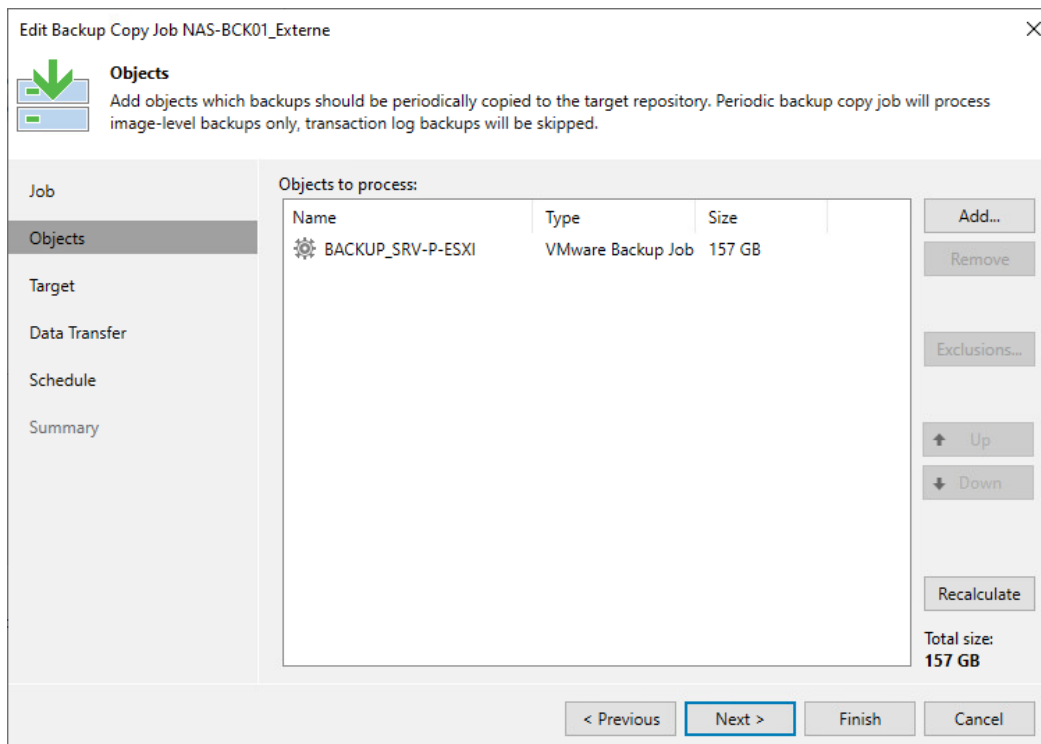
Dans notre cas, le mode Periodic va être choisi pour optimiser la bande passante.

Edit Backup Copy Job NAS-BCK01_Extene ×

 **Job**
Backup copy job efficiently creates local and remote copies of your backups, making it easy to maintain multiple copies of your data. Type in a name and description for the job, and specify backup copy interval.

Job	Name: <input type="text" value="NAS-BCK01_Extene"/>
Objects	Description: <input type="text" value="Created by SRV-V-BCK01\Administrateur at 23/01/2026 13:55."/>
Target	Copy mode: <input type="radio"/> Immediate copy (mirroring) Copies every restore point as soon as it appears in the primary backup repository. This mode will copy all backups created by selected backup jobs, including transaction log backups.
Data Transfer	<input checked="" type="radio"/> Periodic copy (pruning) Periodically copies the latest available restore point only. This mode also allows for selecting which backups to process, enabling you to further reduce bandwidth usage.
Schedule	
Summary	

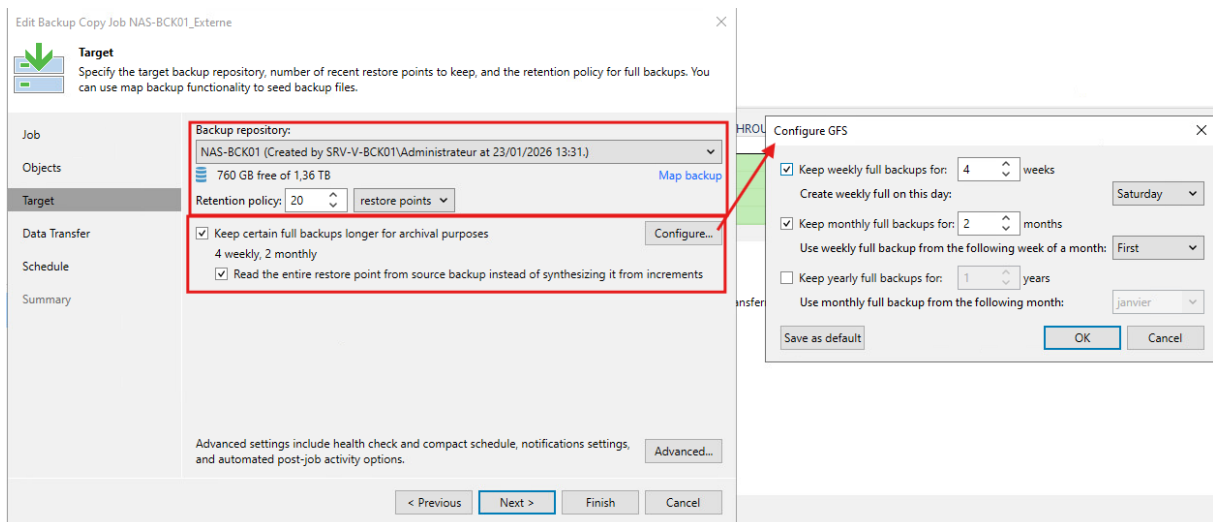
Choisir le job de sauvegarde précédemment créé (pour la sauvegarde des ESXI) comme source des données à copier.



Configurer :

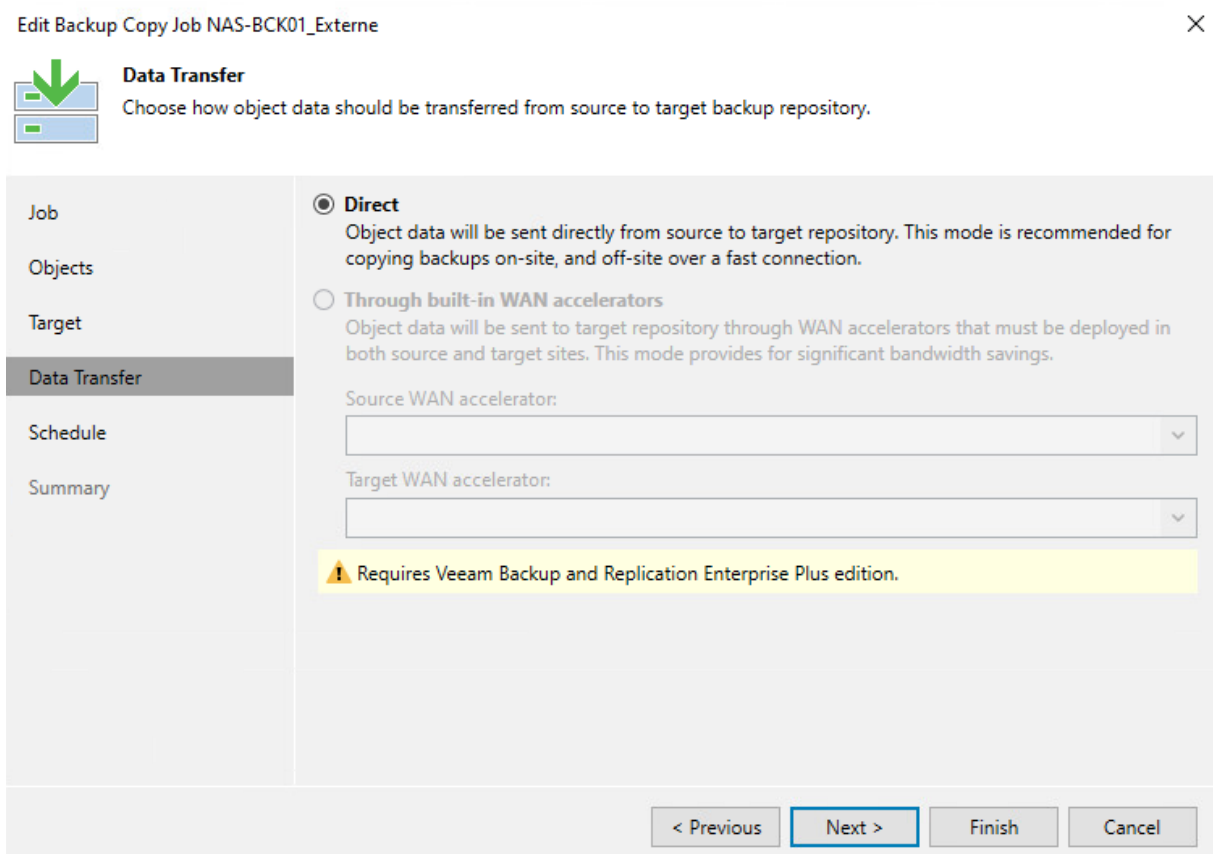
- L'emplacement de la sauvegarde : NAS-BCK01
- Les points de restauration à garder : 20
- Les règles GFS (stratégie de rotation des sauvegardes)
 - o Je garde 4 sauvegardes complètes hebdomadaires
 - o Une sauvegarde complète est faite chaque samedi
 - o Je garde 2 sauvegardes complètes mensuelles
 - o La sauvegarde mensuelle est prise la 1ère semaine de chaque mois

Pour résumé pour les sauvegardes hebdomadaires je peux remonter jusqu'à 4 semaines en arrière, avec un point de restauration par semaine. Et pour les sauvegardes mensuelles la sauvegarde du premier samedi du mois devient une sauvegarde mensuelle et je peux remonter sur 2 mois.



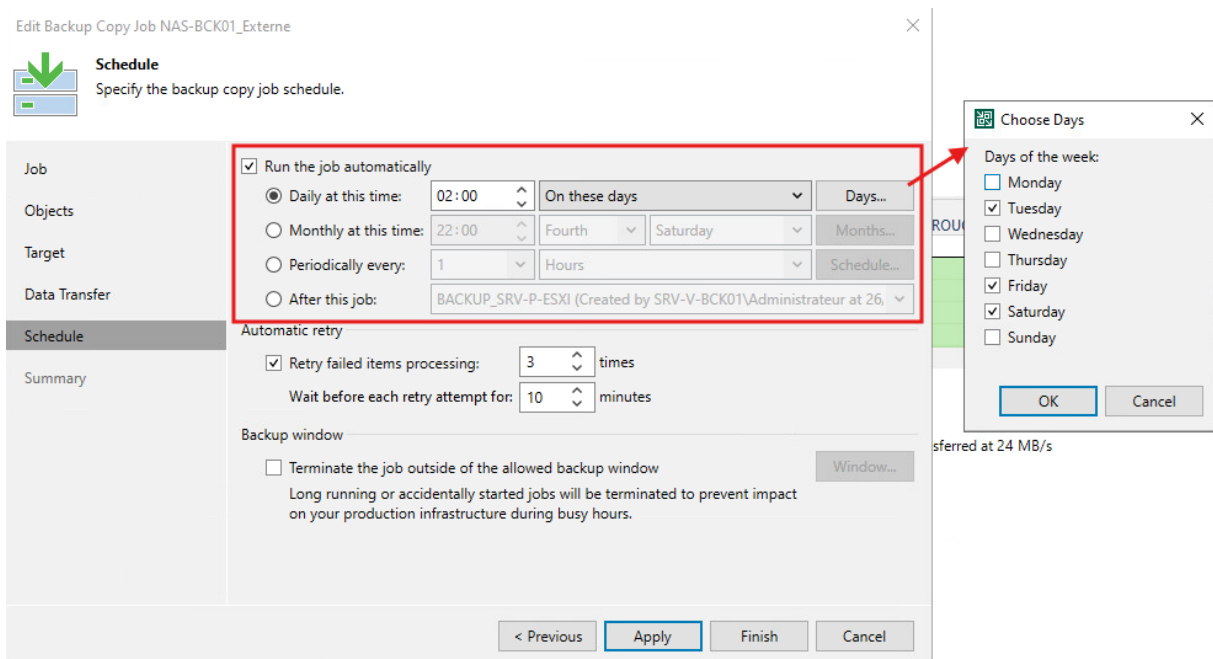
Dans cette étape, on définit la manière dont les données de sauvegarde seront transférées entre la source et la destination.

Sélectionner : Direct (Les données sont envoyées directement du repository source vers le repository cible.)



Cette étape définit quand le job de copie sera exécuté.

La planification configure une exécution automatique du Backup Copy Job les jours sélectionnés (mardi, vendredi et samedi) à 02h00, avec 3 tentatives de relance espacées de 10 minutes en cas d'échec afin d'assurer la continuité des copies.

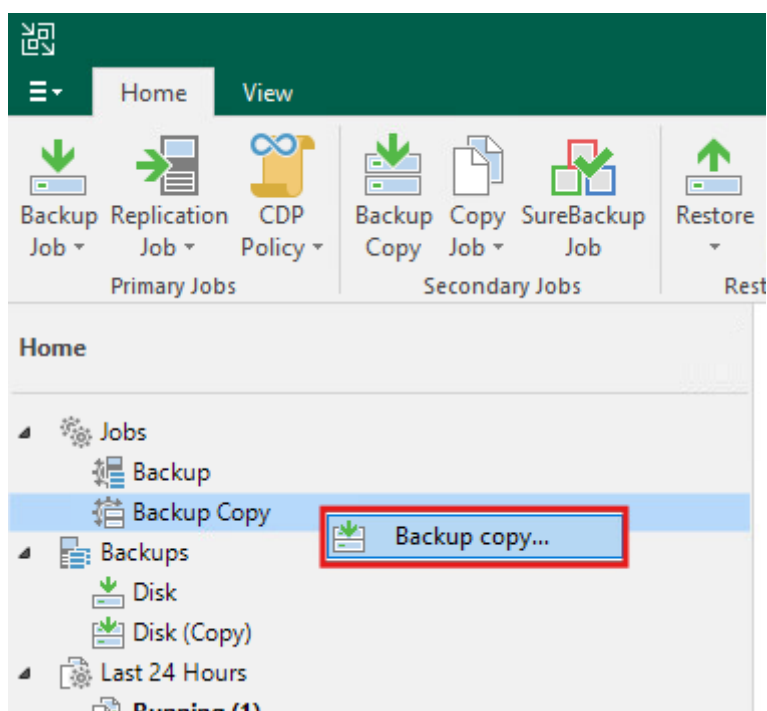


Le Copy Backup Job est maintenant opérationnelle.

4.7.2.2.6. Mise en place d'un Backup Copy Job (copie externe) vers le NAS 2

Ce job de copie permettra de dupliquer la sauvegarde réalisée par le job de sauvegarde des ESXi vers le NAS 2.

Dans le menu, cliquer sur Backup Copy. Ce type de job permet de copier les sauvegardes vers un autre stockage dans le nôtre un NAS.



Donner un nom au job (ex : NAS-BCK02_Externe).

Choisir le mode :

- Immediate copy : copie en temps réel
- Periodic copy : copie planifiée (recommandé pour optimiser la bande passante).

Dans notre cas, le mode Periodic va être choisi pour optimiser la bande passante.

Edit Backup Copy Job NAS-BCK02_Externe

Job
Backup copy job efficiently creates local and remote copies of your backups, making it easy to maintain multiple copies of your data. Type in a name and description for the job, and specify backup copy interval.

Job Name: NAS-BCK02_Externe

Objects Description: Created by SRV-V-BCK01\Administrateur at 26/03/2026 14:58.

Target

Data Transfer

Schedule

Summary

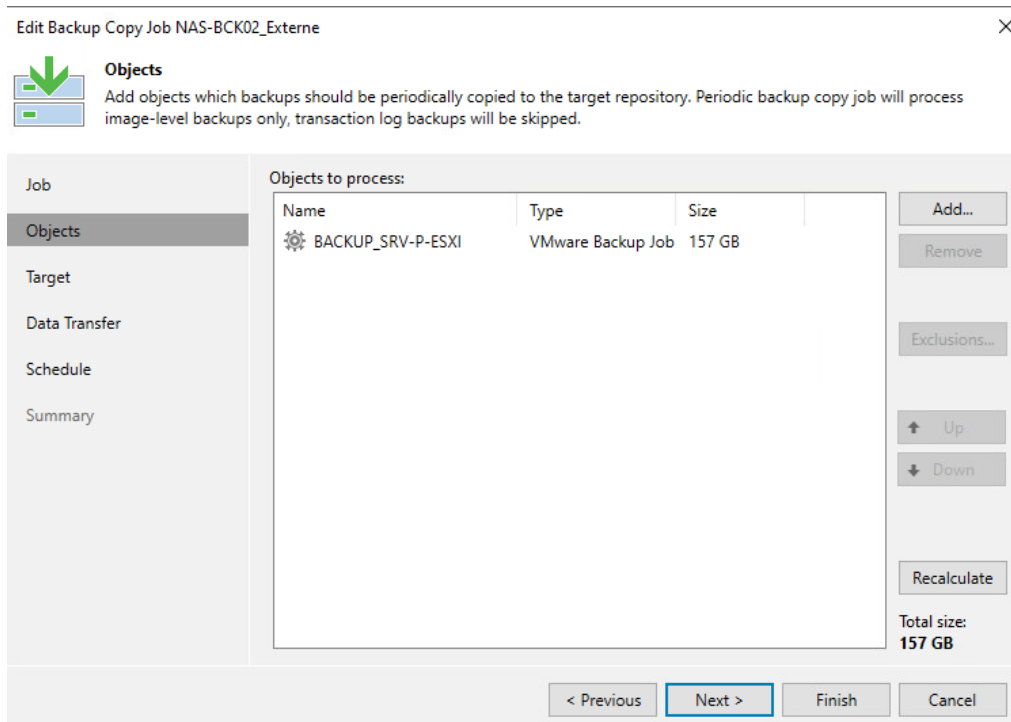
Copy mode:

Immediate copy (mirroring)
Copies every restore point as soon as it appears in the primary backup repository. This mode will copy all backups created by selected backup jobs, including transaction log backups.

Periodic copy (pruning)
Periodically copies the latest available restore point only. This mode also allows for selecting which backups to process, enabling you to further reduce bandwidth usage.

< Previous Next > Finish Cancel

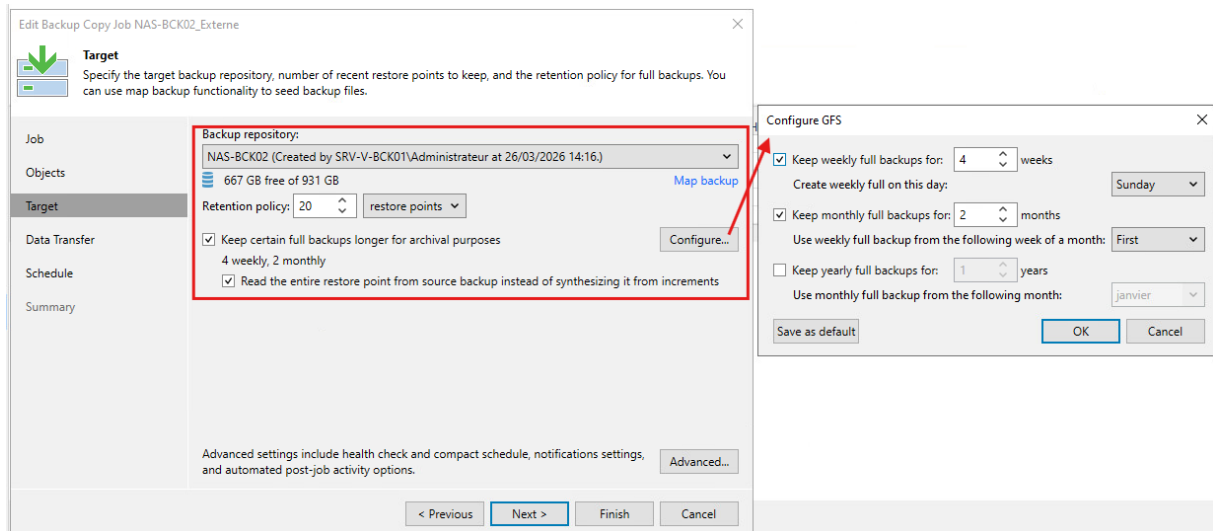
Choisir le job de sauvegarde précédemment créé (pour la sauvegarde des ESXI) comme source des données à copier.



Configurer :

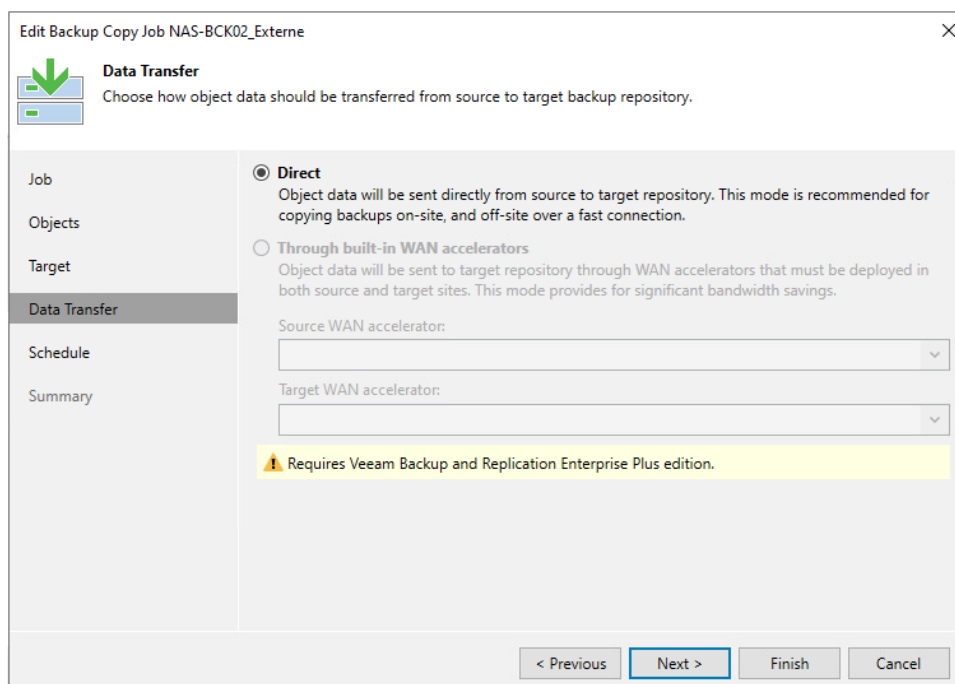
- L'emplacement de la sauvegarde : NAS-BCK02
- Les points de restauration à garder : 20
- Les règles GFS (stratégie de rotation des sauvegardes)
 - o Je garde 4 sauvegardes complètes hebdomadaires
 - o Une sauvegarde complète est faite chaque samedi
 - o Je garde 2 sauvegardes complètes mensuelles
 - o La sauvegarde mensuelle est prise la 1ère semaine de chaque mois

Pour résumé pour les sauvegardes hebdomadaires je peux remonter jusqu'à 4 semaines en arrière, avec un point de restauration par semaine. Et pour les sauvegardes mensuelles la sauvegarde du premier samedi du mois devient une sauvegarde mensuelle et je peux remonter sur 2 mois.



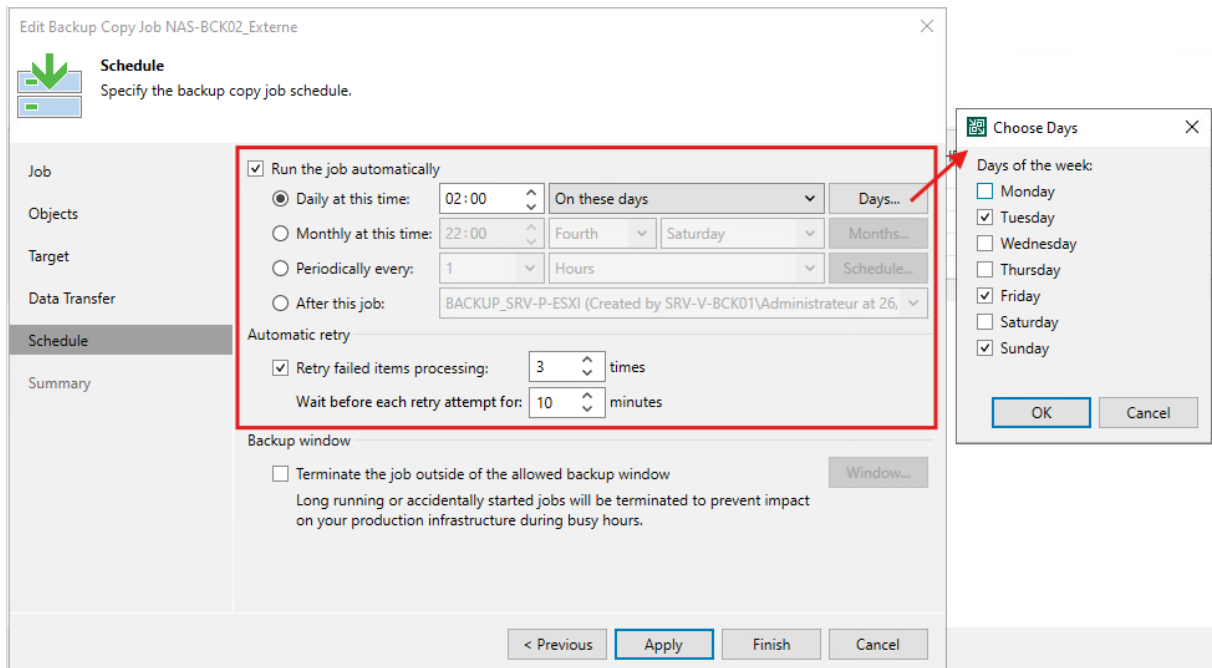
Dans cette étape, on définit la manière dont les données de sauvegarde seront transférées entre la source et la destination.

Sélectionner : Direct (Les données sont envoyées directement du repository source vers le repository cible.)



Cette étape définit quand le job de copie sera exécuté.

La planification configure une exécution automatique du Backup Copy Job les jours sélectionnés (mardi, vendredi et dimanche) à 02h00, avec 3 tentatives de relance espacées de 10 minutes en cas d'échec afin d'assurer la continuité des copies.



Le Copy Backup Job est maintenant opérationnelle.

4.8. Procédure de restauration complète et partielle

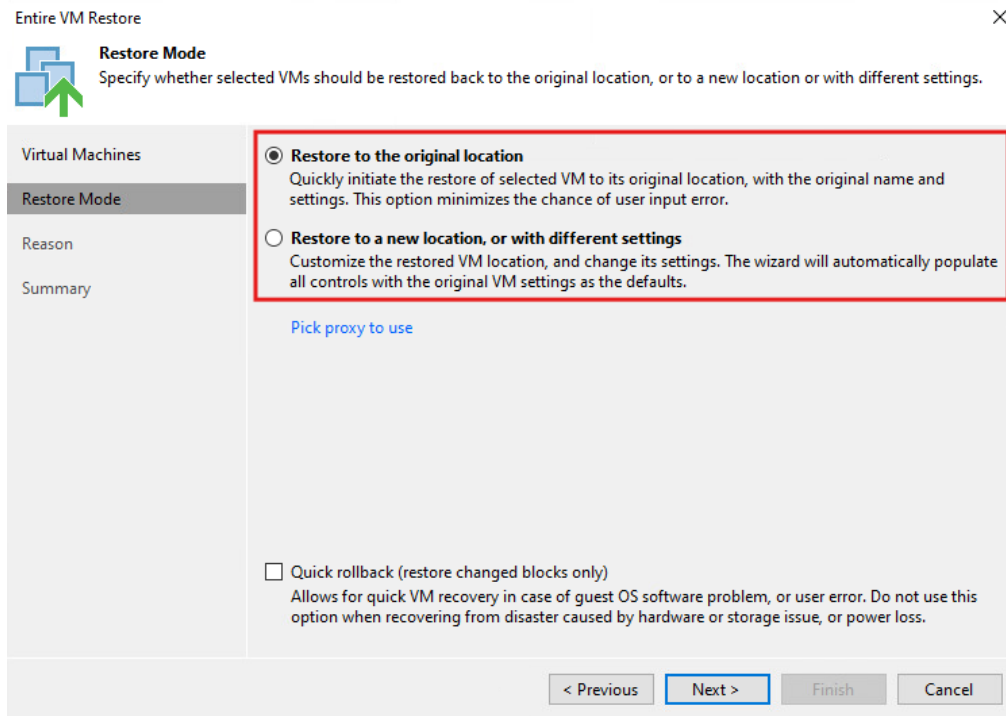
4.8.1. Restaurer une VM entière (configuration + disques) à partir d'un backup

Sélection du point de restauration Aller dans Home > Disk Clic droit sur la VM (ex : SRV-P-GLPI01).

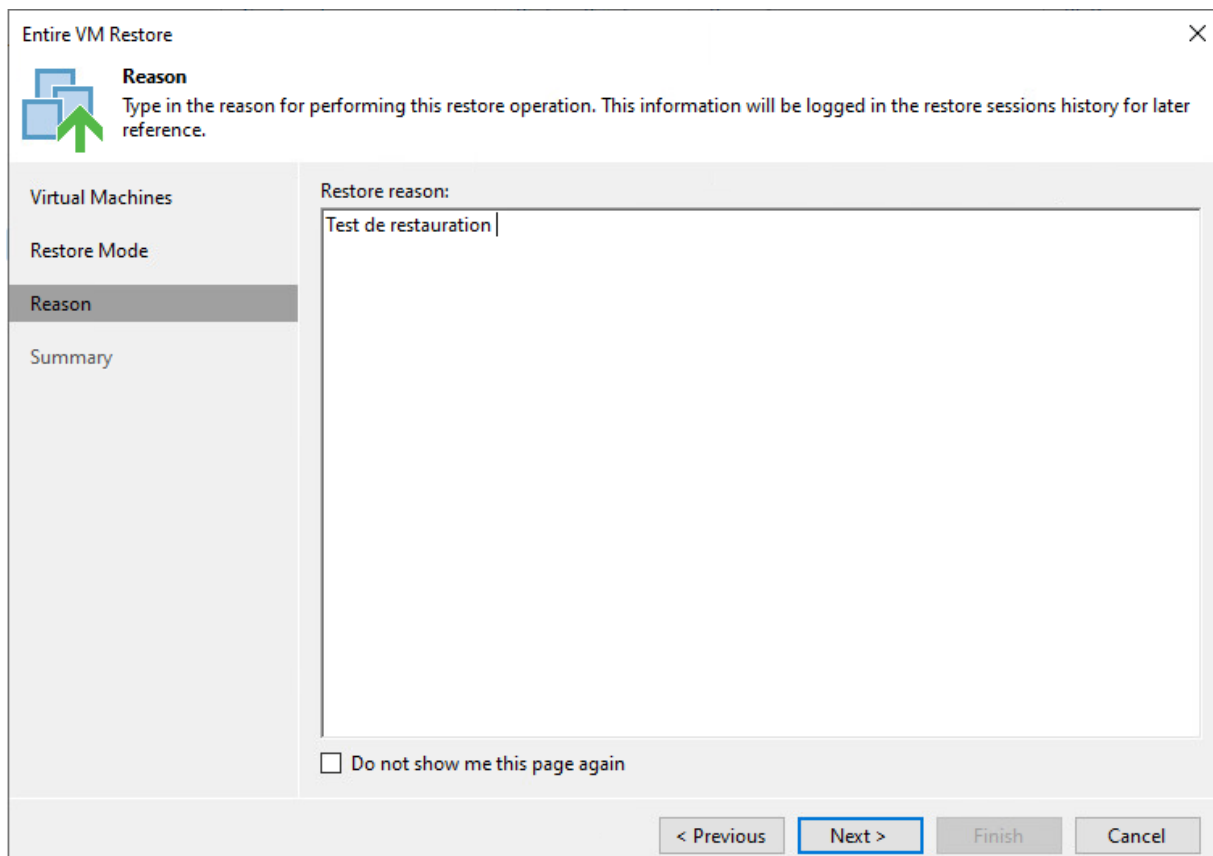
Cliquer sur Restore entire VM

- Utilisé pour cloner ou tester sans impacter la prod

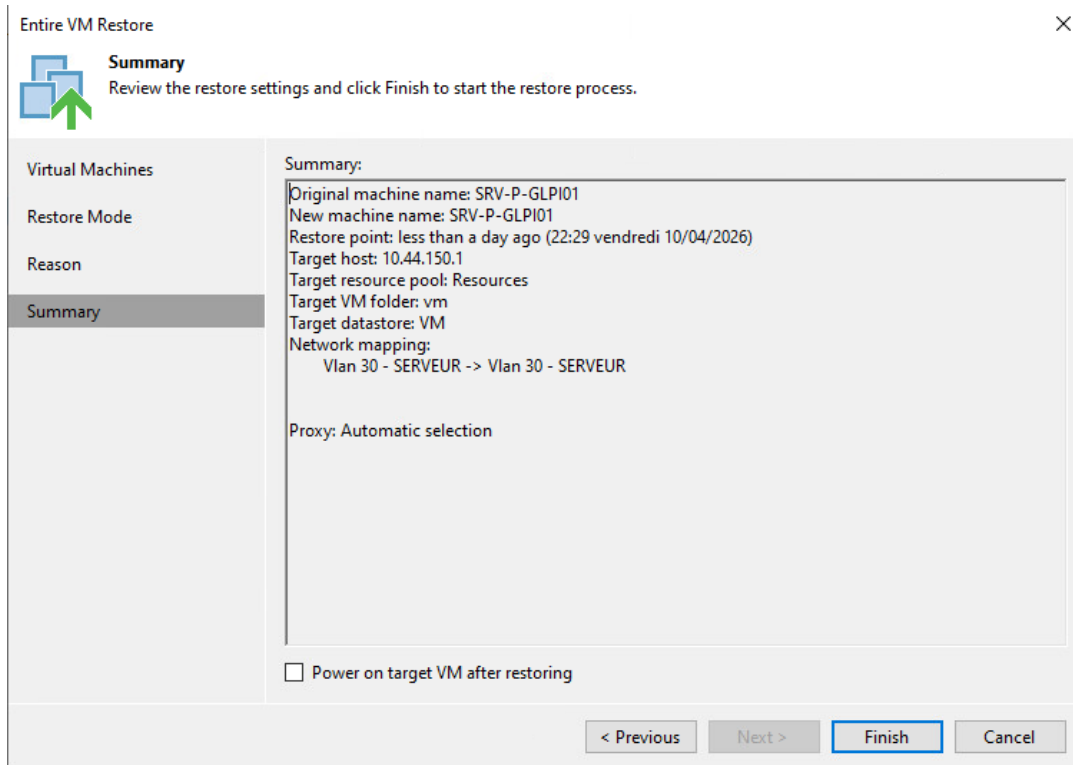
Je sélectionne restauration à l'emplacement d'origine



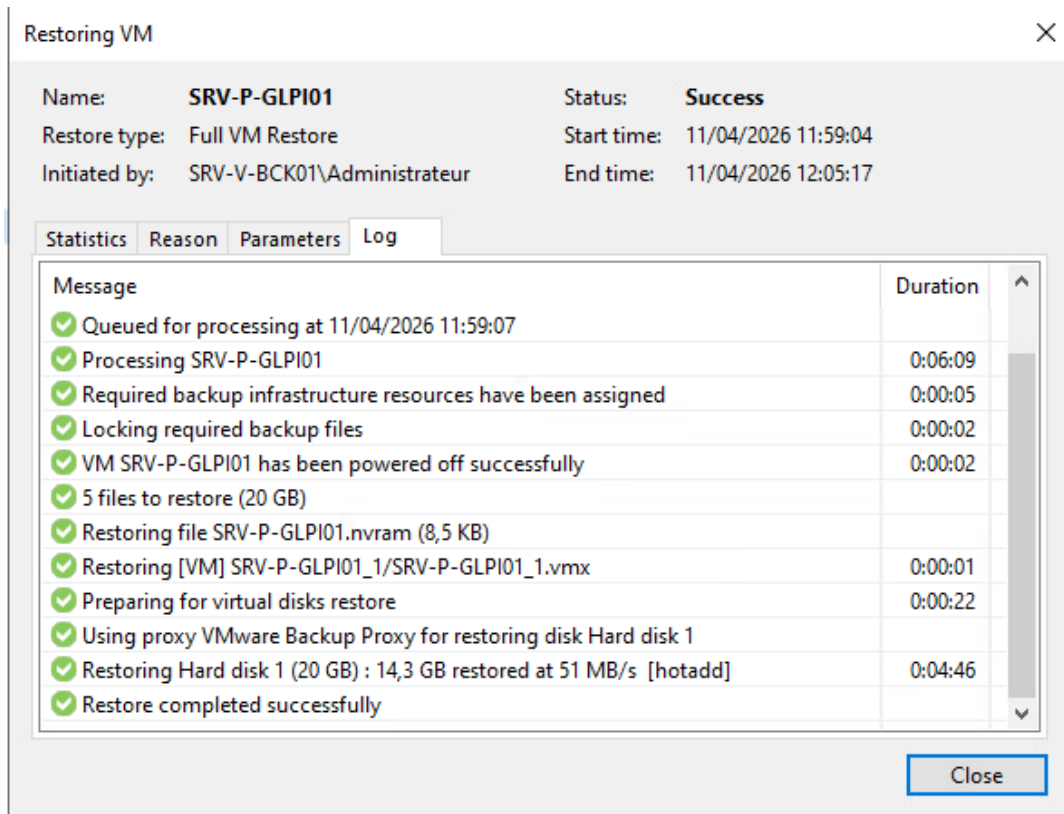
Raison de restauration (cela permet de repérer plus facilement pourquoi une restauration a été effectuée).



Résumé et lancement de la restauration ne pas oublier de vérifier le nom VM, Host cible, Datastore et Réseau.



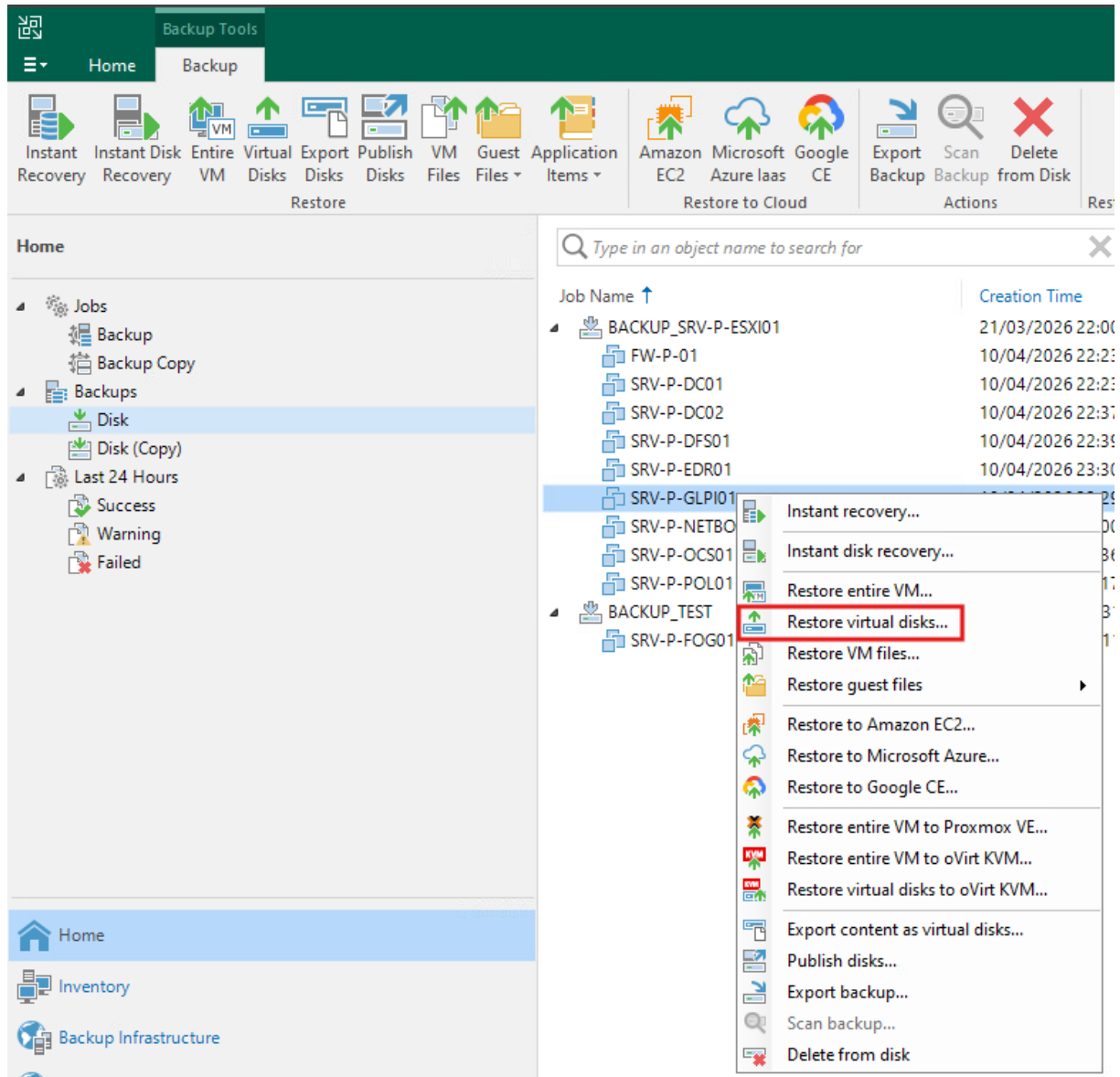
Résultat de l'opération, avec comme statut Success, une durée d'environ 6min.



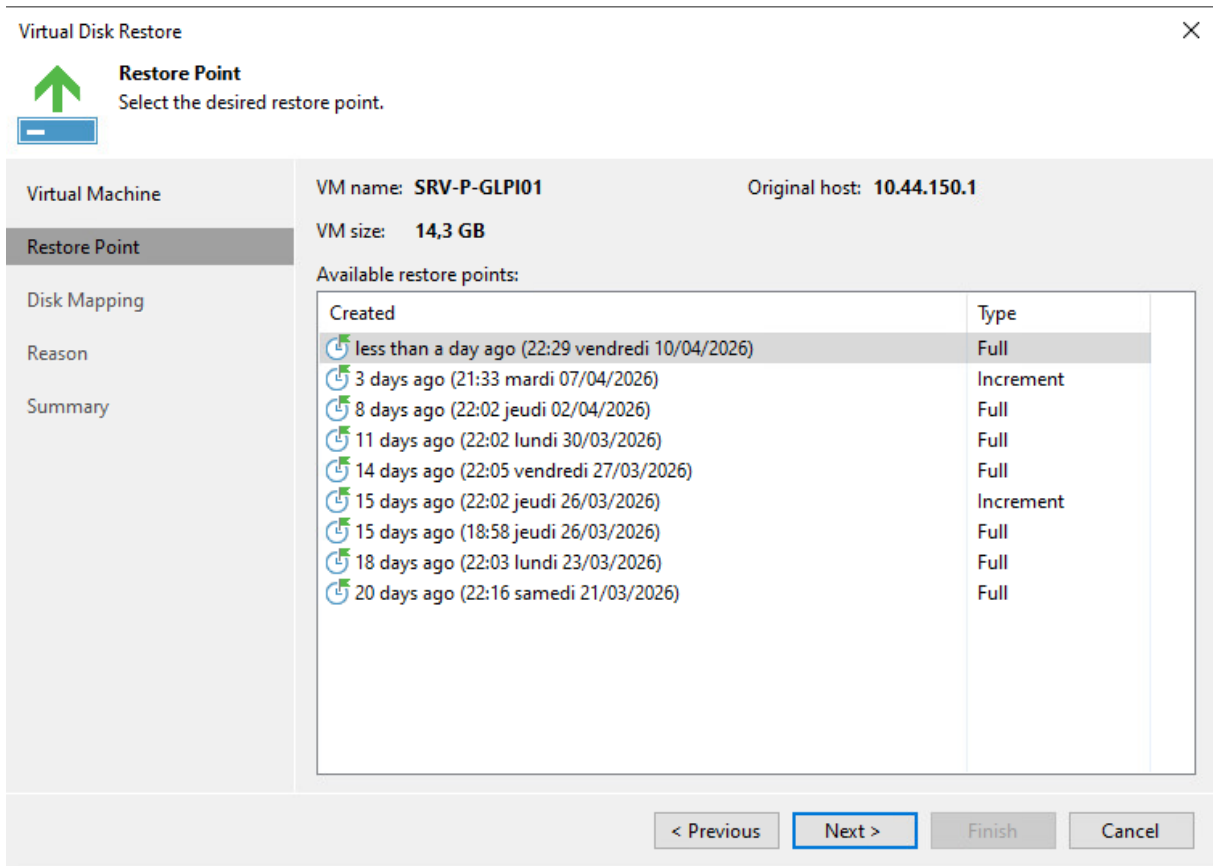
On peut ensuite constater que la VM restaurée apparaît bien sur l'ESXi. La VM fonctionne correctement et les services GLPI sont opérationnels.

4.8.2. Restaurer un disque spécifique sans restaurer toute la VM.

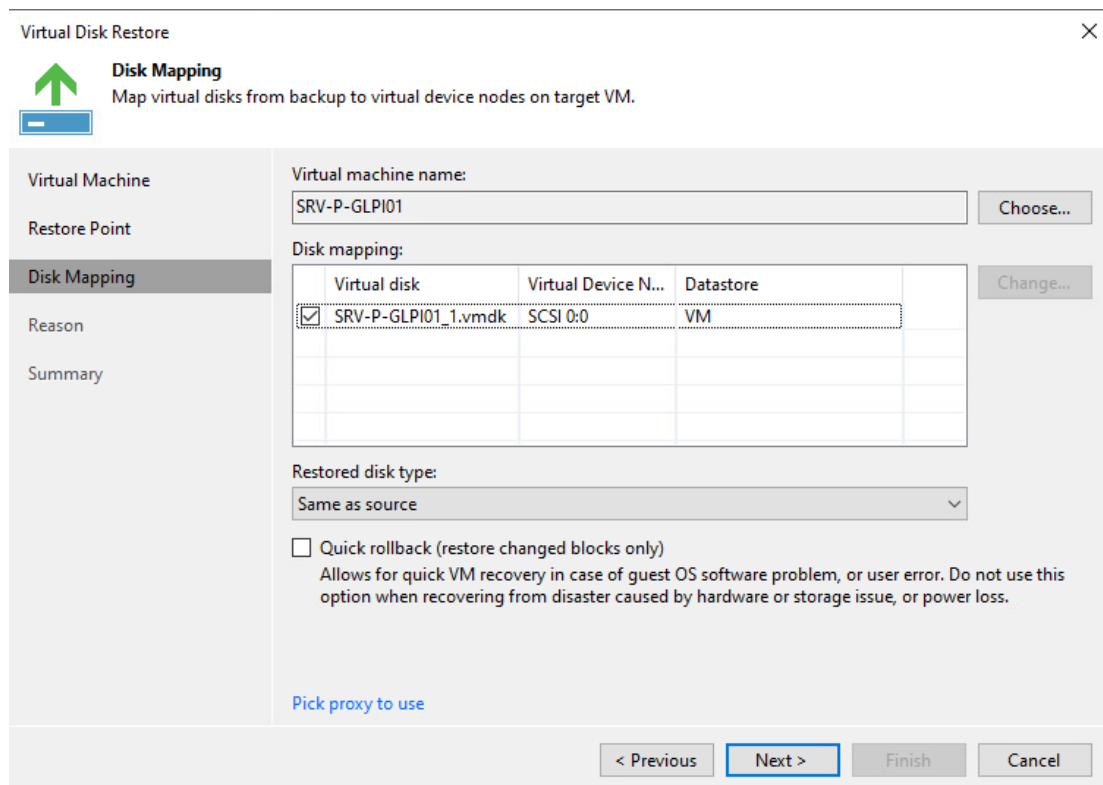
Sélection du point de restauration Aller dans Home > Backups > Disk, Sélection Clic droit sur la VM et choisir Restore virtual disks.

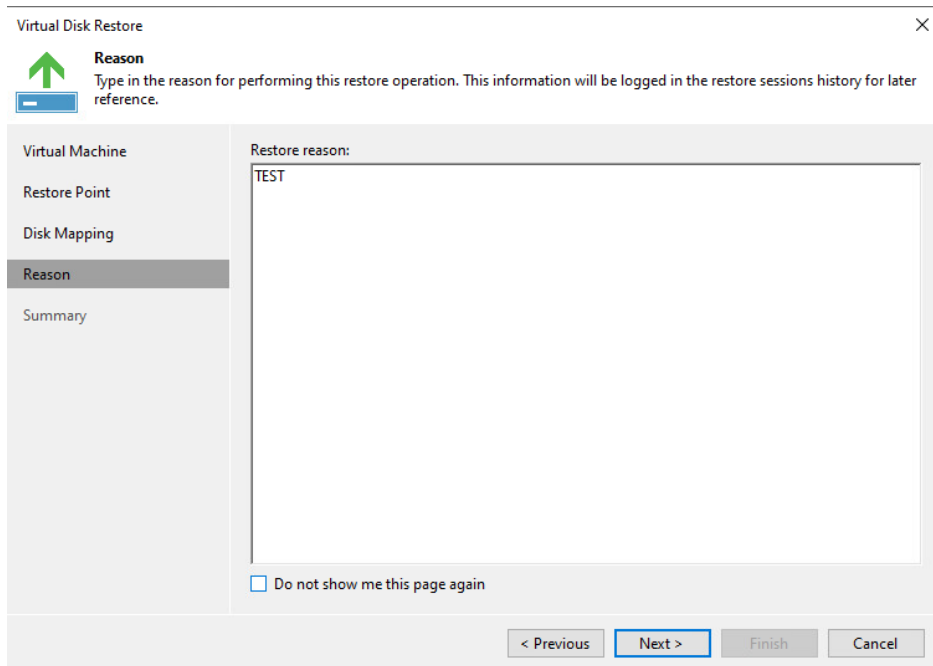


Choix du point de restauration : Sélectionner la date souhaitée ici Restore point : "less than a day ago".

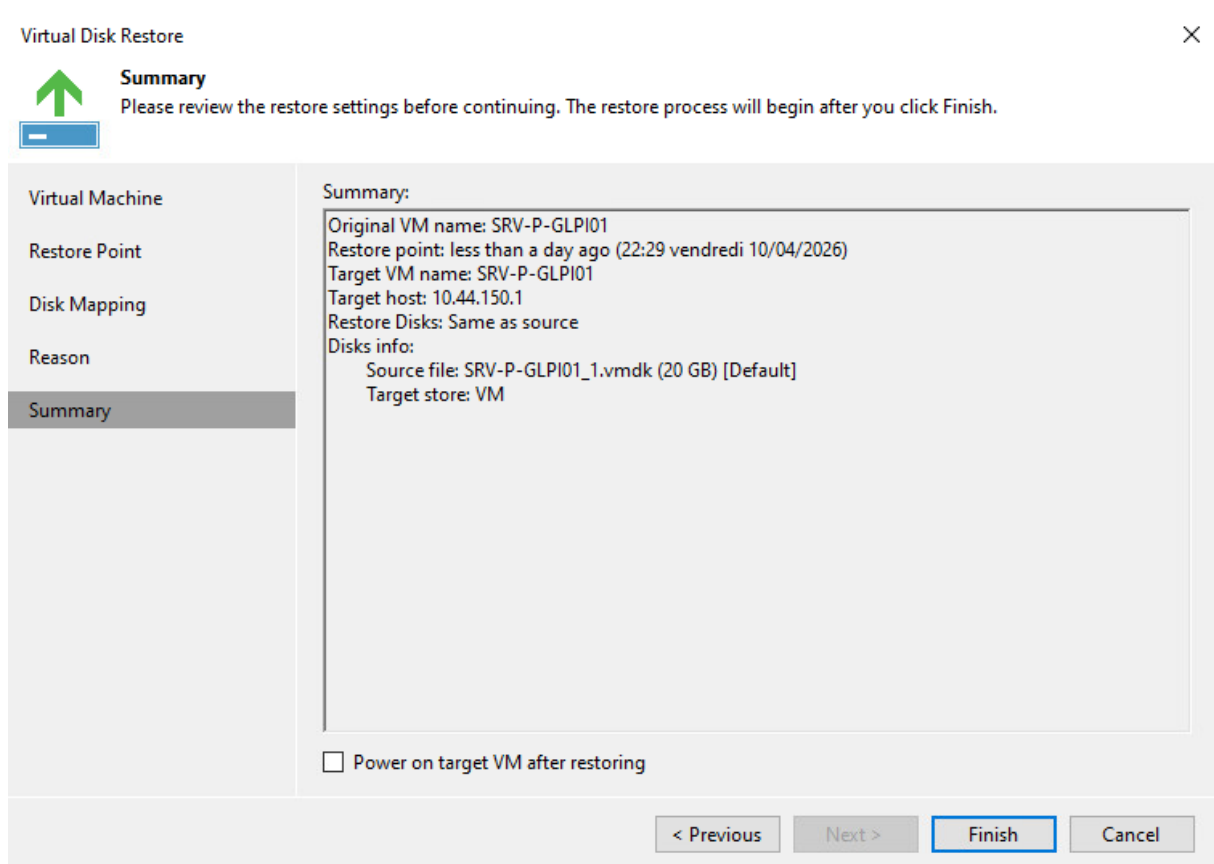


Sélection du disque que l'on souhaite restaurer sur une VM comportant plusieurs disques : on peut choisir précisément le disque que l'on veut restaurer.

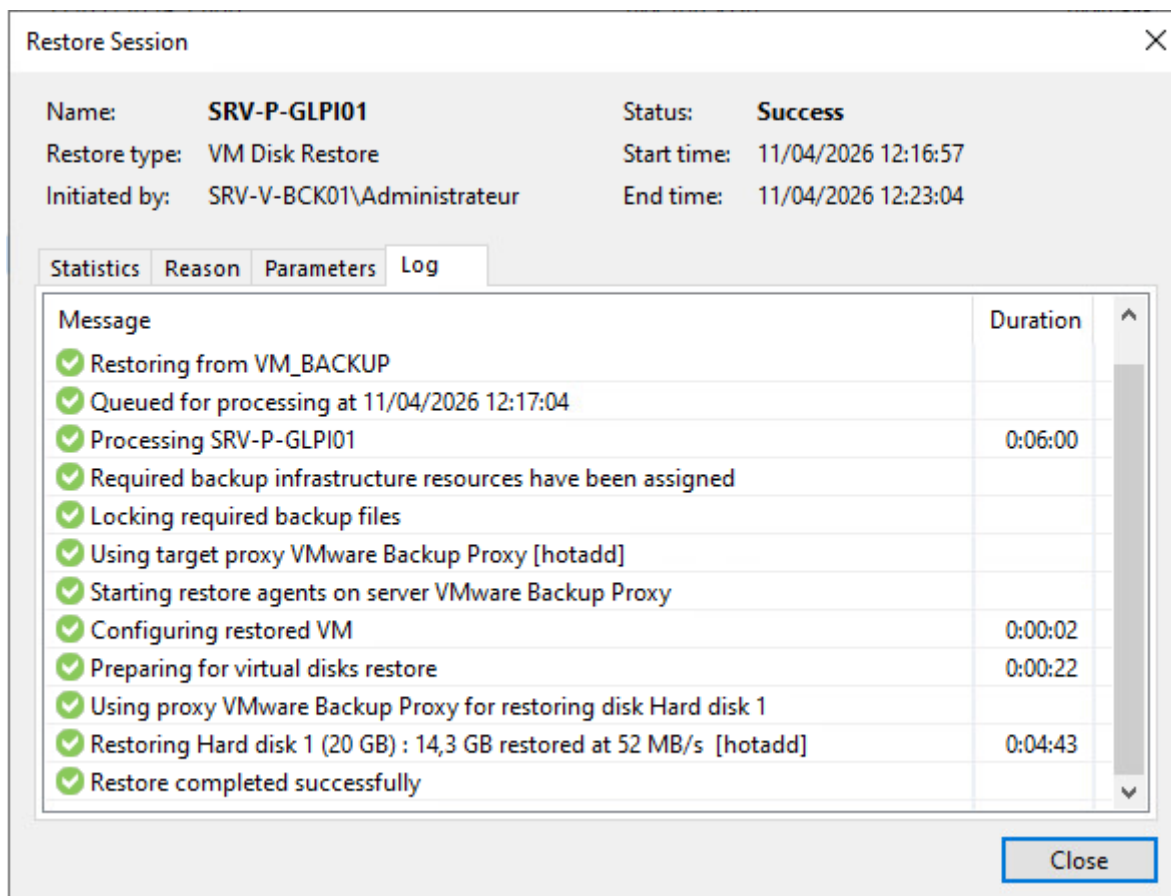




Résumé et lancement de la restauration ne pas oublier de vérifier le nom VM, Host cible, Datastore, disque et Réseau.



Résultat de l'opération, avec comme statut Success, une durée d'environ 6min.



On peut ensuite constater que le disque restauré apparaît bien sur l'ESXi. La VM fonctionne correctement et les services GLPI sont opérationnels.

4.9. Plan de reprise d'activité (PRA) détaillé

4.9.1. Contexte

L'entreprise Oasis dispose de deux sites :

- Siège principal à Paris
- Agence secondaire à Marseille

L'infrastructure informatique repose sur :

- Une architecture virtualisée
- Des services centralisés au siège
- Une interconnexion sécurisée entre les sites via VPN

Les services critiques incluent :

- Active Directory (gestion des utilisateurs)

- Serveurs de fichiers
- Applications métiers

4.9.2. Objectifs du PRA

Le PRA vise à :

- Garantir la reprise rapide des services critiques
- Assurer la disponibilité des ressources IT
- Limiter la perte de données
- Maintenir la communication entre sites

Indicateurs

- RTO : 4 heures (services critiques)
- RPO : 48 heures

RTO : La durée maximale d'interruption admissible est l'expression de besoin de disponibilité des différents métiers ou services, dans une organisation.

RPO : La perte de données maximale admissible ou perte de données maximale tolérable.

Voir annexe 2 pour définition.

4.9.3. Architecture technique

4.9.3.1. Infrastructure principale (Paris)

Le site principal héberge :

- Serveurs virtualisés (VMware)
- Contrôleur de domaine (AD)
- Serveur de fichiers (DFS/R)
- Serveur applicatif
- Pare-feu
- Switch réseau

4.9.3.2. Infrastructure secondaire (Marseille)

- Postes clients
- Accès aux services via VPN
- Pare-feu (Stormshield)

4.9.3.3. Réseau

- VLAN segmentés :
 - Vlan CLIENTS
 - Vlan WIFI
 - Vlan WIFI CLIENTS
 - Vlan SERVEUR
 - Vlan DEPLOIEMENT
 - Vlan ADMIN
 - Vlan SYNC
 - Vlan DMZ
 - Vlan NATIF
- Interconnexion :
 - VPN site-à-site entre Paris et Marseille
 - Accès sécurisé aux ressources centralisées

4.9.4. Sauvegarde et réplication

4.9.4.1. Sauvegardes

- Sauvegarde des machines virtuelles
- Stockage :
 - Local sécurisé
 - NAS externe

4.9.4.2. Réplication

- Réplication des VM critiques
- Snapshots réguliers
- Possibilité de redémarrage sur infrastructure secondaire

4.9.5. Scénarios de sinistre

4.9.5.1. Panne serveur (Paris)

- Indisponibilité des services centralisés

4.9.5.2. Cyberattaque (ransomware)

- Chiffrement des données
- Accès bloqué

4.9.5.3. Perte du site principal

- Incendie / panne électrique majeure

4.9.5.4. Perte du lien VPN

- Coupure communication Marseille > Paris

4.9.6. Procédures de reprise technique

4.9.6.1. Cas : panne serveur

1. Identification de la panne
2. Redémarrage de la VM
3. Si échec > restauration
4. Vérification services (AD, fichiers)

4.9.6.2. Cas : cyberattaque

1. Arrêt des machines infectées
2. Suppression des accès compromis
3. Restauration des VM depuis sauvegarde saine
4. Redémarrage progressif

4.9.6.3. Cas : perte du site Paris

1. Activation PRA
2. Redémarrage des VM critiques
3. Redirection des accès utilisateurs

4.9.6.4. Cas : coupure VPN

1. Diagnostic réseau
2. Réparation tunnel VPN
3. Rétablissement complet

4.9.7. Gestion des accès utilisateurs

- Authentification via Active Directory
- Droits utilisateurs restaurés automatiquement

4.9.8. Plan de communication

Interne

- Notification immédiate
- Consignes aux utilisateurs

Externe

- Information clients
- Maintien de la confiance

4.9.9. Reprise opérationnelle

Priorités :

1. Accès aux données clients
2. Communication client
3. Activité commerciale

4.9.10. Tests et validation

- Tests PRA en environnement isolé
- Simulation de panne serveur
- Simulation de cyberattaque
- Vérification des RTO / RPO

4.9.11. Maintenance

- Mise à jour régulière du PRA
- Adaptation aux évolutions réseau
- Tests semestriels

4.9.12. Conclusion

Le PRA d'Oasis repose sur une infrastructure moderne, virtualisée et sécurisée.

Il permet :

- Une reprise rapide des services
- Une protection des données critiques
- Une continuité de service entre les sites

Ce dispositif garantit la résilience de l'entreprise face aux incidents majeurs.

4.10. Phase de test

4.10.1. Vérification de l'exécution automatique des sauvegardes planifiées

Pour vérifier l'exécution des sauvegardes planifiées, j'ai généré des rapports sur les différents jobs créés.

Dans un premier temps, on peut constater que le job de sauvegarde des ESXi s'est bien lancé le lundi 13 avril à 22h00, conformément à la planification.

Backup job: BACKUP_SRV-P-ESXI								
Created by SRV-V-BCK01\Administrateur at 26/09/2025 15:22.								
lundi 13 avril 2026 22:00:03								
Success	10	Start time	22:00:03	Total size	498 GB	Backup size	4,7 GB	
Warning	0	End time	22:28:29	Data read	27,4 GB	Dedupe	1,2x	
Error	0	Duration	0:28:26	Transferred	4,6 GB	Compression	2,9x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
FW-P-01	Success	22:00:21	22:01:44	20 GB	2,3 GB	1,3 GB	0:01:23	
SRV-P-DC01	Success	22:00:21	22:02:16	70 GB	1,8 GB	758,7 MB	0:01:55	
SRV-P-GLPI01	Success	22:01:37	22:03:15	20 GB	5,3 GB	32,3 MB	0:01:38	
SRV-P-OCS01	Success	22:01:52	22:03:19	10 GB	655 MB	14,4 MB	0:01:27	
SRV-P-DC02	Success	22:02:54	22:08:11	70 GB	1,4 GB	560,1 MB	0:05:17	
SRV-P-DFS01	Success	22:03:04	22:08:18	98 GB	1,7 GB	731,8 MB	0:05:14	
SRV-P-EDR01	Success	22:07:51	22:28:27	35 GB	11 GB	1,2 GB	0:20:36	
SRV-P-NETBOX01	Success	22:08:01	22:12:14	25 GB	1,2 GB	21,5 MB	0:04:13	
SRV-P-POL01	Success	22:11:59	22:14:44	20 GB	903 MB	21,8 MB	0:02:45	
SRV-P-FOG01	Success	22:14:35	22:16:28	130 GB	1,2 GB	26,5 MB	0:01:53	

Ensuite, le job de copie vers le NAS 1 s'est bien exécuté à 2h00 le samedi 11 avril, comme prévu par la planification.

Backup Copy job: NAS-BCK01_Externe					
Created by SRV-V-BCK01\Administrateur at 23/01/2026 13:55.					
samedi 11 avril 2026 02:00:22					
Jobs	1	Success	1	Processed	368 GB
Items	9	Warning	0	Read	138,7 GB
Processed	9	Error	0	Transferred	65 GB
Details					
Source job	Status	Details			
BACKUP_SRV-P-ESXI	Success				

De même, le job de copie vers le NAS 2 fonctionne correctement, avec une exécution réalisée au bon jour et à la bonne heure.

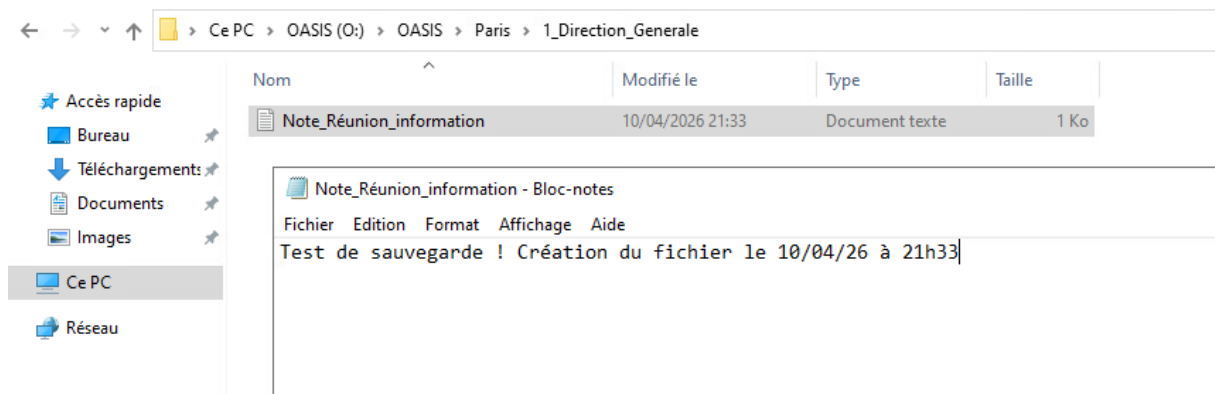
Backup Copy job: NAS-BCK02_Externe					
Created by SRV-V-BCK01\Administrateur at 26/03/2026 14:58.					
mardi 14 avril 2026 02:00:05					
Jobs	1	Success	1	Processed	498 GB
Items	10	Warning	0	Read	28,6 GB
Processed	10	Error	0	Transferred	13,2 GB
Details					
Source job	Status	Details			
BACKUP_SRV-P-ESXI	Success				

4.10.2. Test de restauration

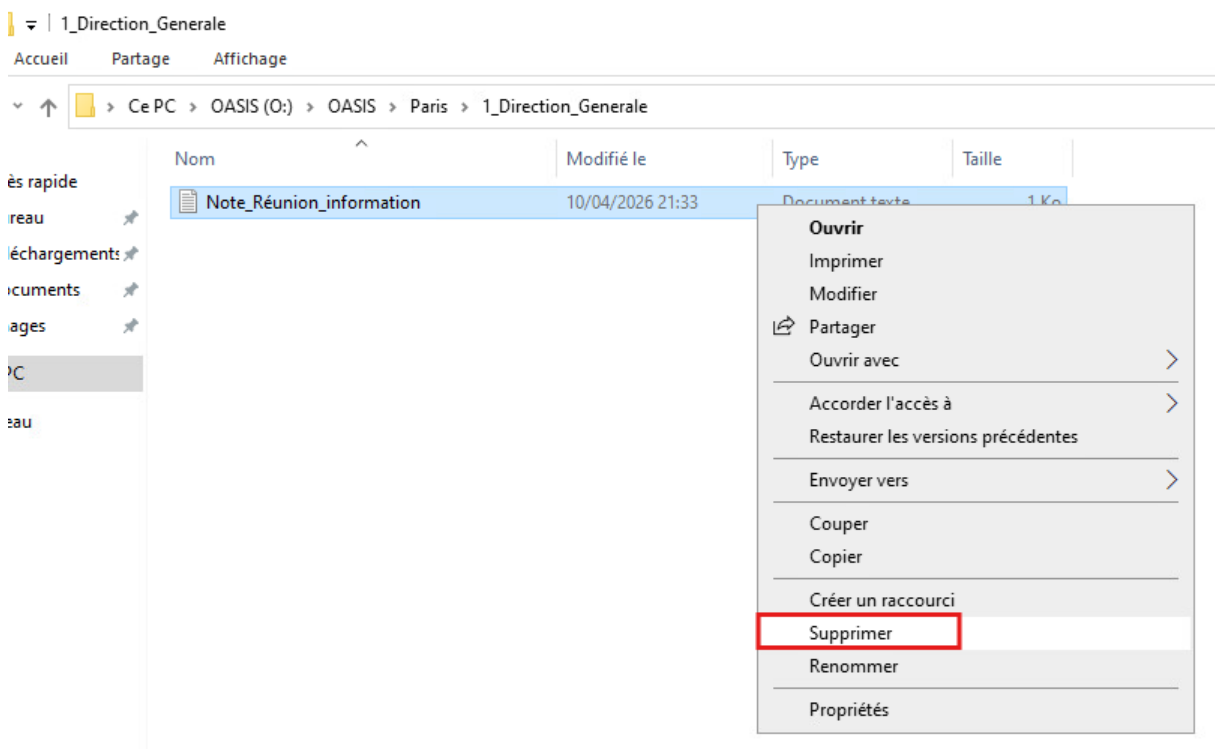
4.10.2.1. Restauration d'un fichier sur un serveur Windows

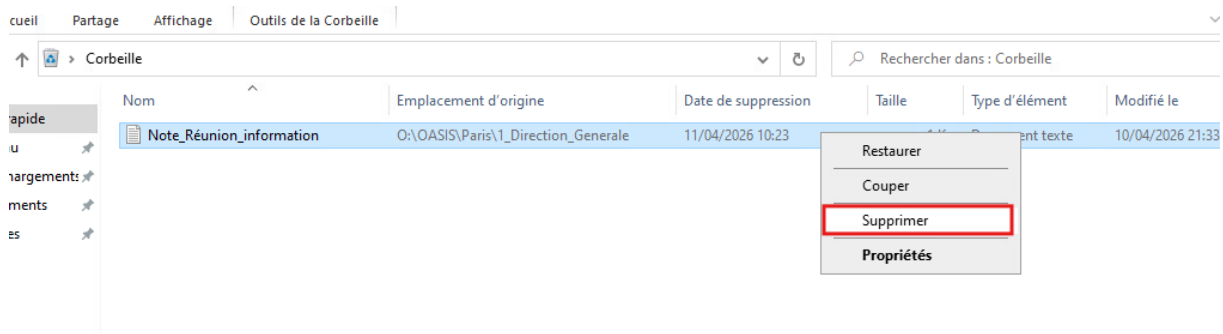
L'objectif est de vérifier la capacité à restaurer un fichier supprimé ainsi que la fiabilité du processus de restauration via Veeam Backup & Replication.

Dans un premier temps, création d'un fichier de test sur le partage de fichiers (DFS/R), accessible depuis les différents postes. Cela permet de disposer d'un élément identifiable pour tester la restauration.



Le fichier est supprimé manuellement depuis l'explorateur Windows, puis également supprimé de la corbeille. Cette action simule une perte réelle de donnée côté utilisateur.



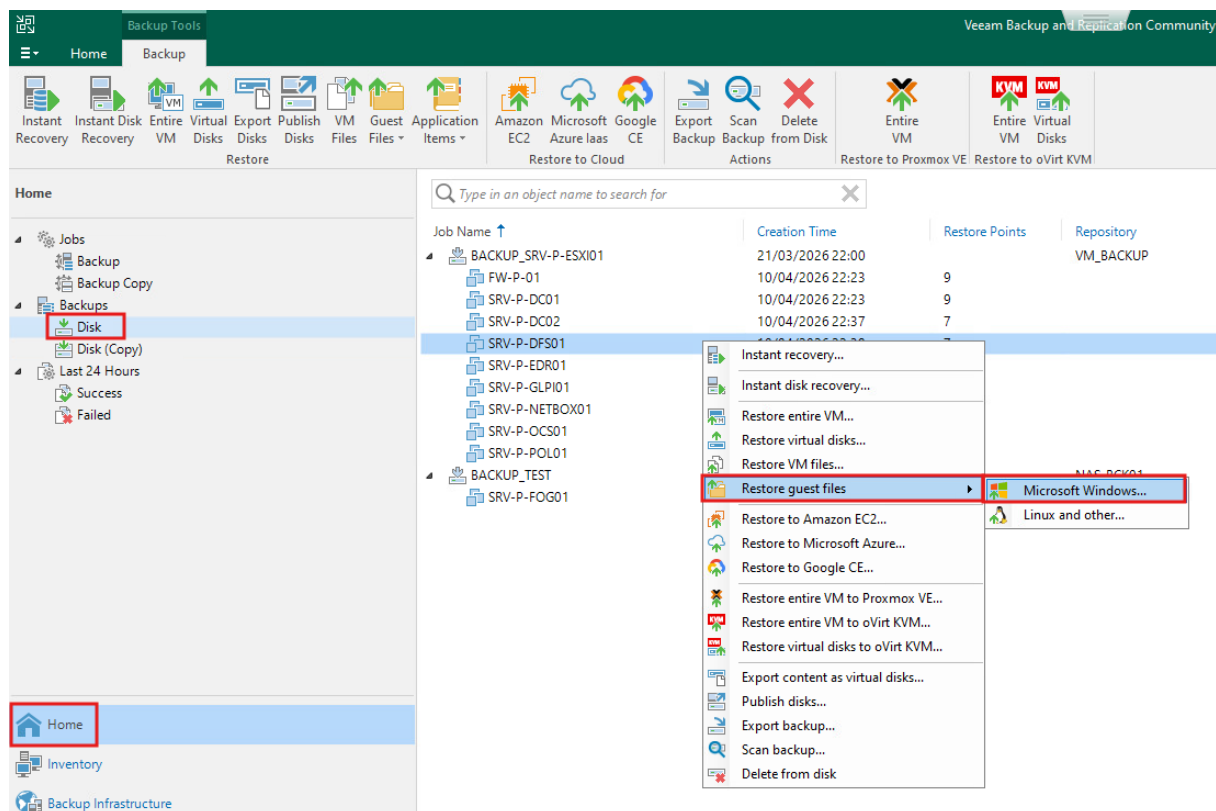


L'utilisateur contacte le service informatique, car un fichier a été supprimé par erreur.

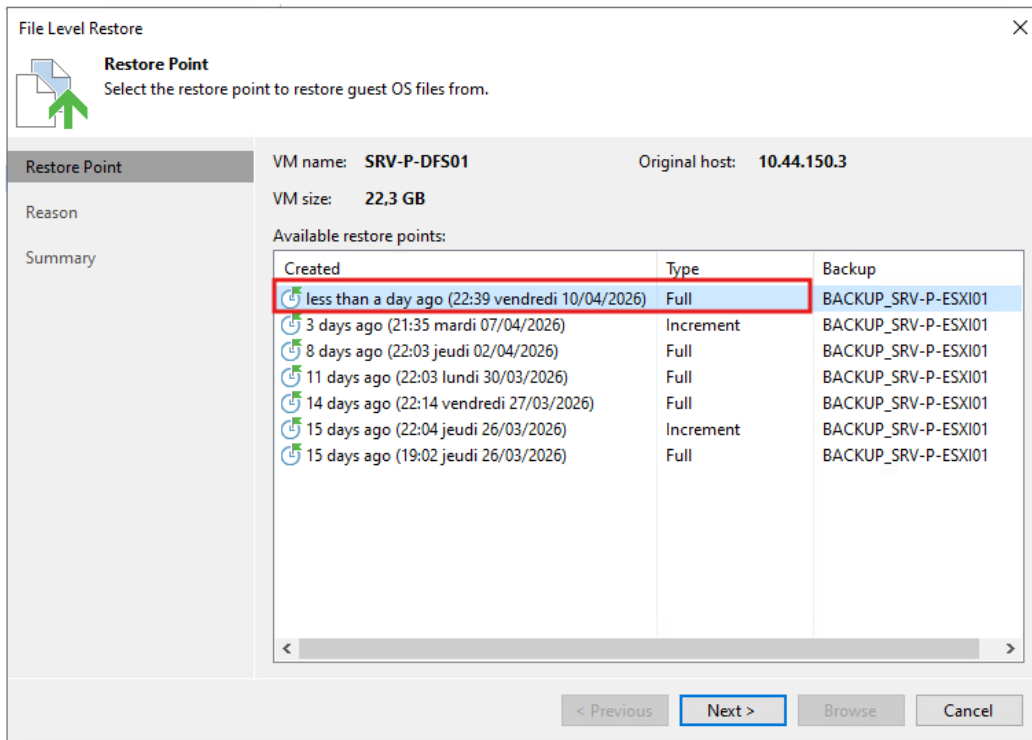
Lancement de la restauration, depuis la console Veeam :

- Accès à l'onglet des Backups > Disk
- Clic droit sur la machine concernée : Ici le serveur DFS/R
- Sélection de Restore guest files > Microsoft Windows

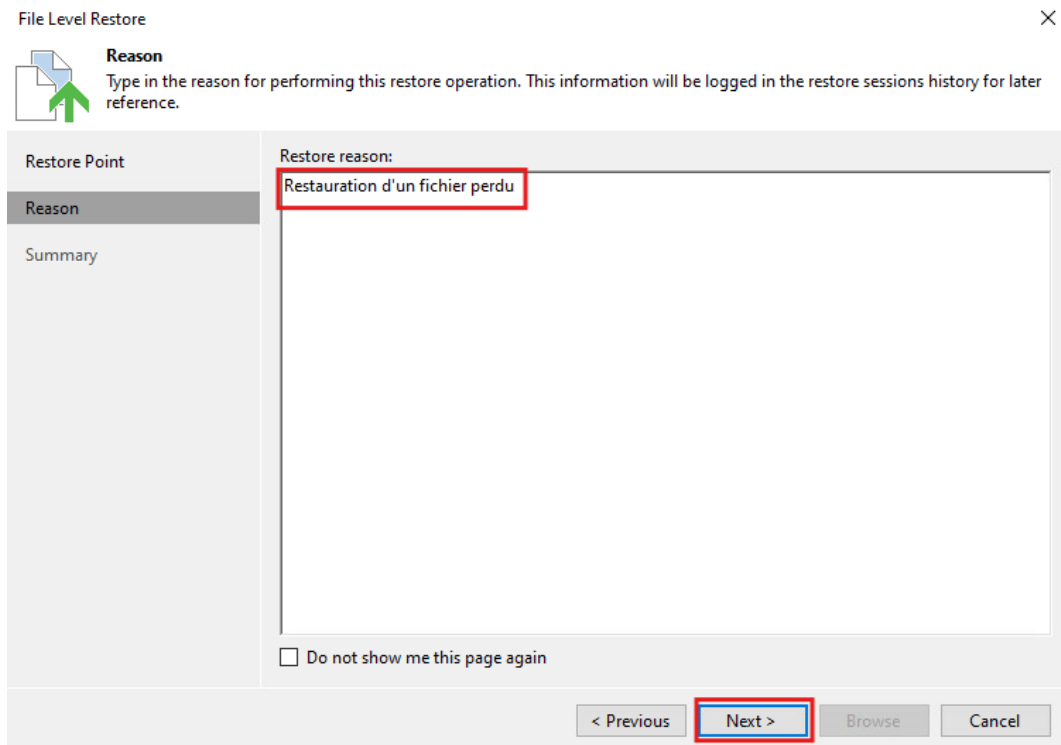
Cette option permet de restaurer uniquement les fichiers sans restaurer toute la machine.



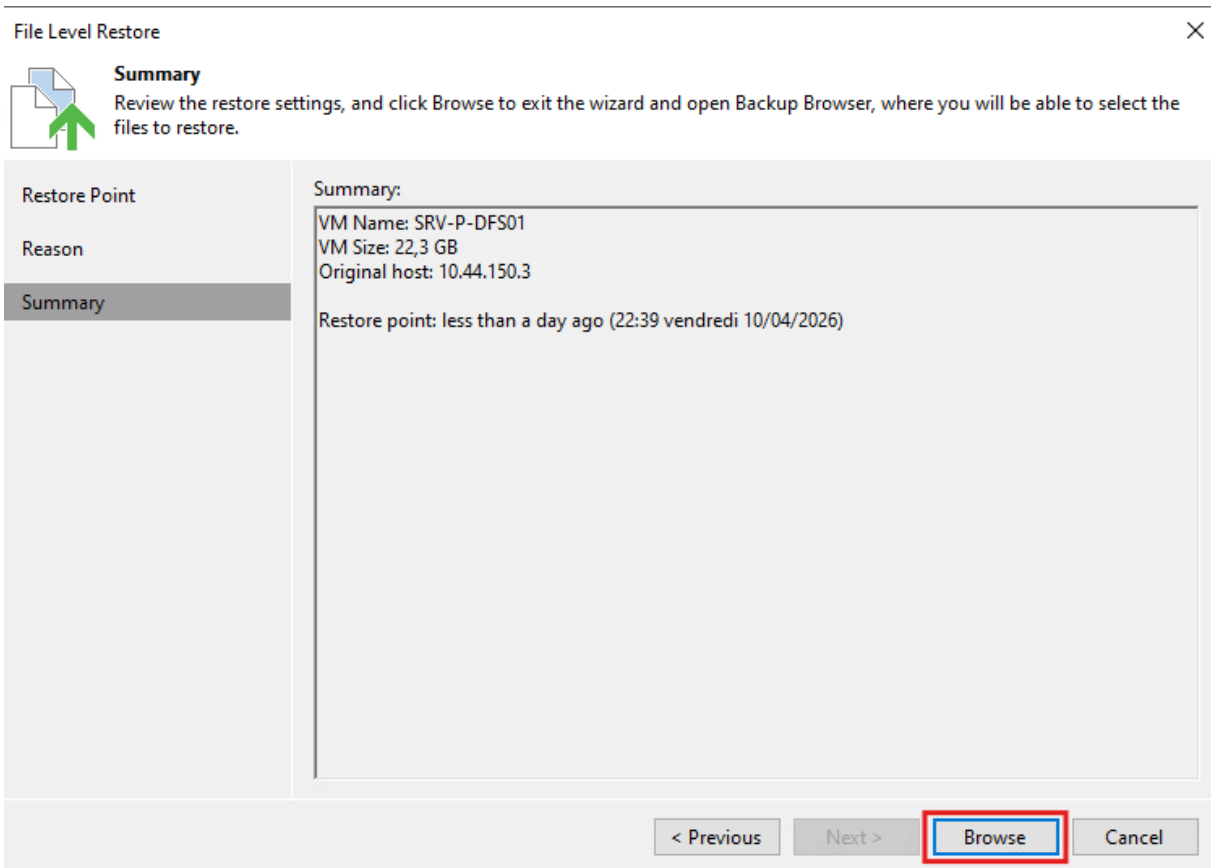
Sélection du point de restauration. Un point de restauration récent est sélectionné (moins d'un jour).



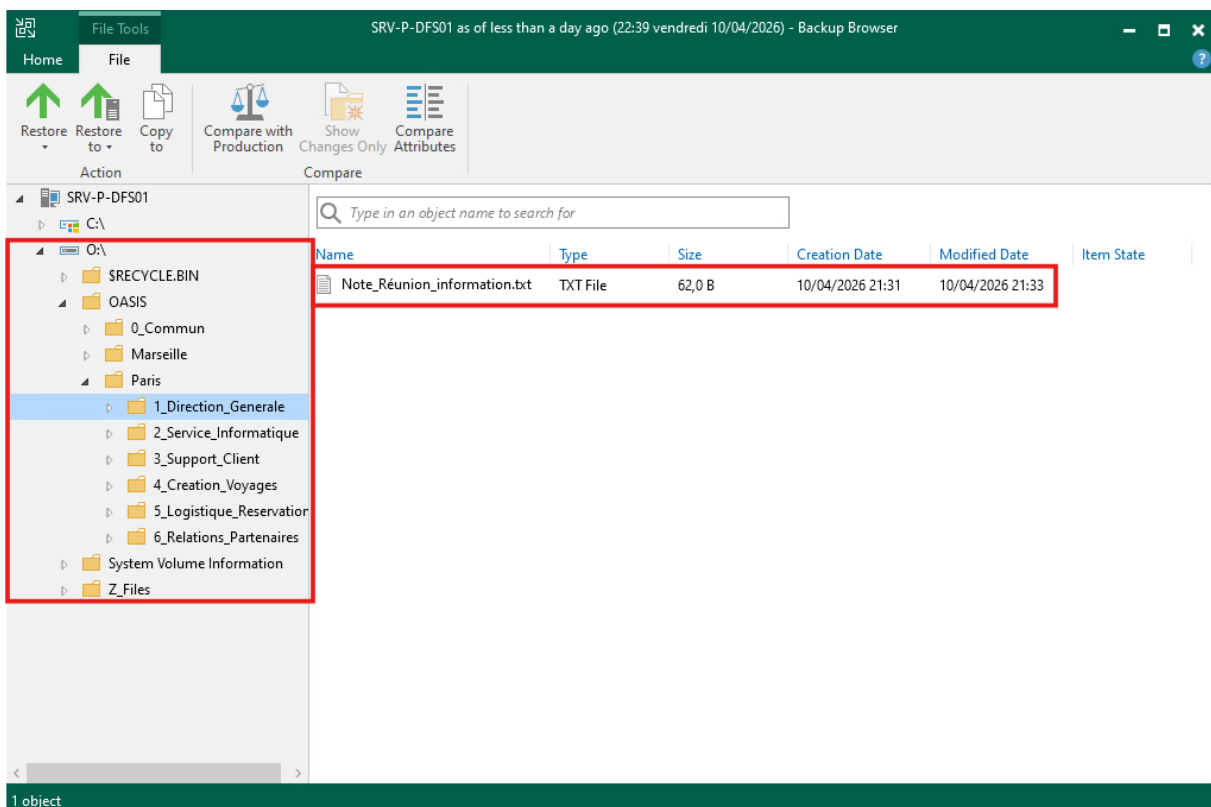
Ajout d'une description (Restauration d'un fichier perdu).



Validation du résumé, ouverture du navigateur de fichiers (Backup Browser).



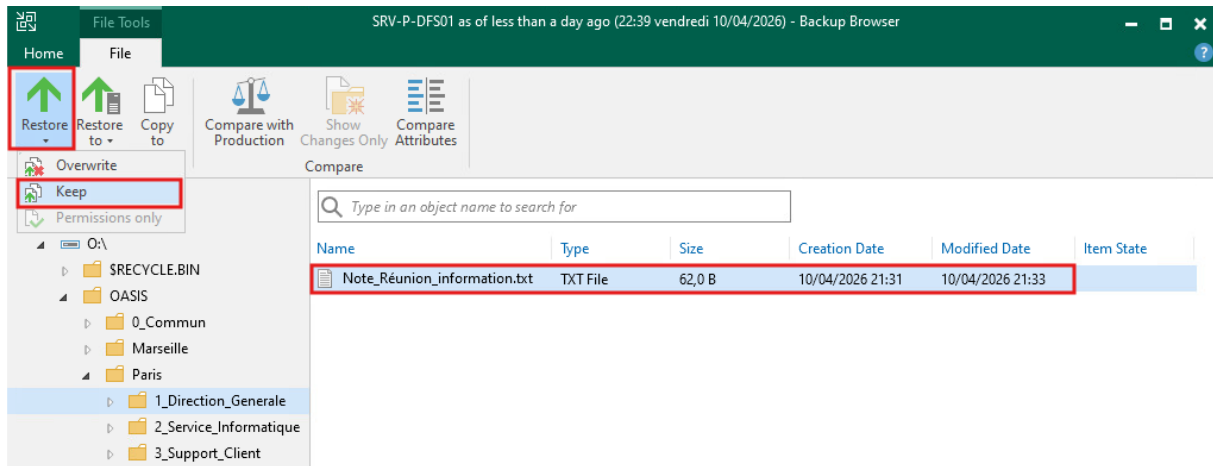
Recherche du fichier dans l'explorateur de sauvegarde. Navigation dans l'arborescence et localisation du fichier Note_Réunion_information.txt. Le fichier apparaît bien dans la sauvegarde.



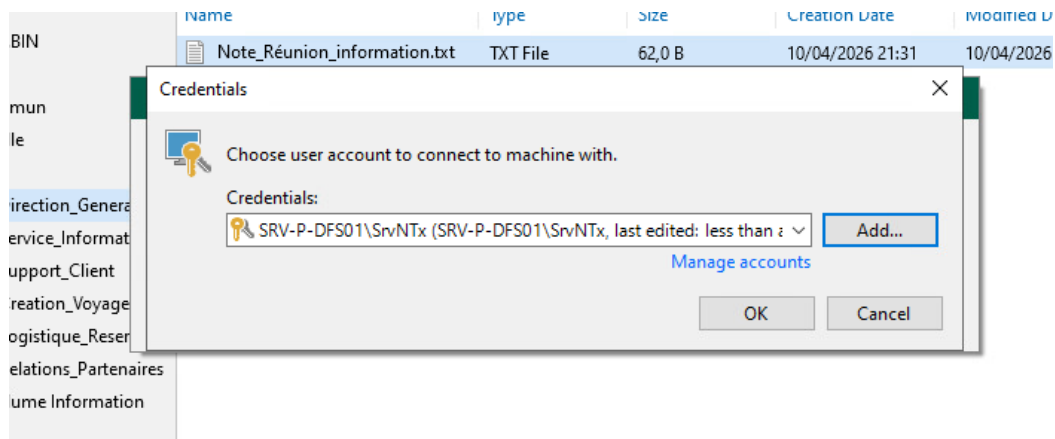
Restauration du fichier, deux options sont possibles :

- Restore : restauration à l'emplacement d'origine
- Keep : conservation du fichier existant si nécessaire

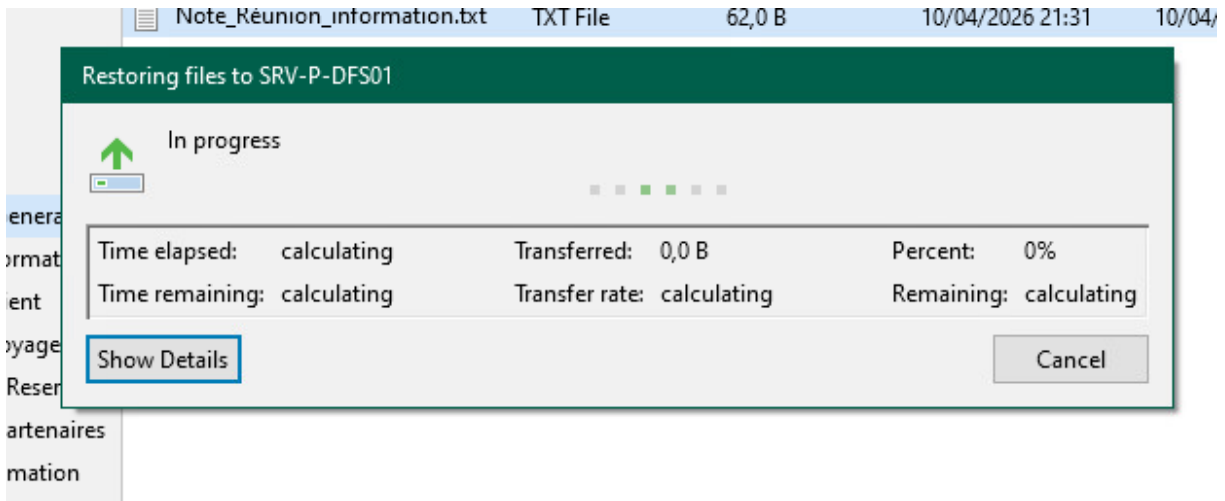
Dans ce test, la restauration sera lancée vers l'emplacement initial.



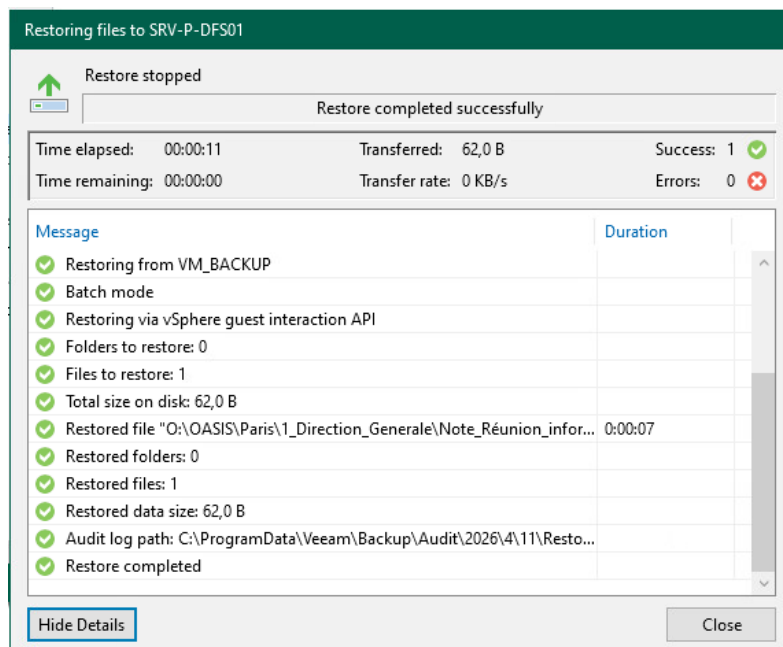
Une authentification est demandée pour accéder à la machine cible. Cela garantit la sécurité des opérations de restauration.



Une fenêtre affiche la progression avec le temps de restauration, le volume transféré et le statut de l'opération.



Et une fois terminé le résultat : Succès de la restauration et aucune erreur détectée.

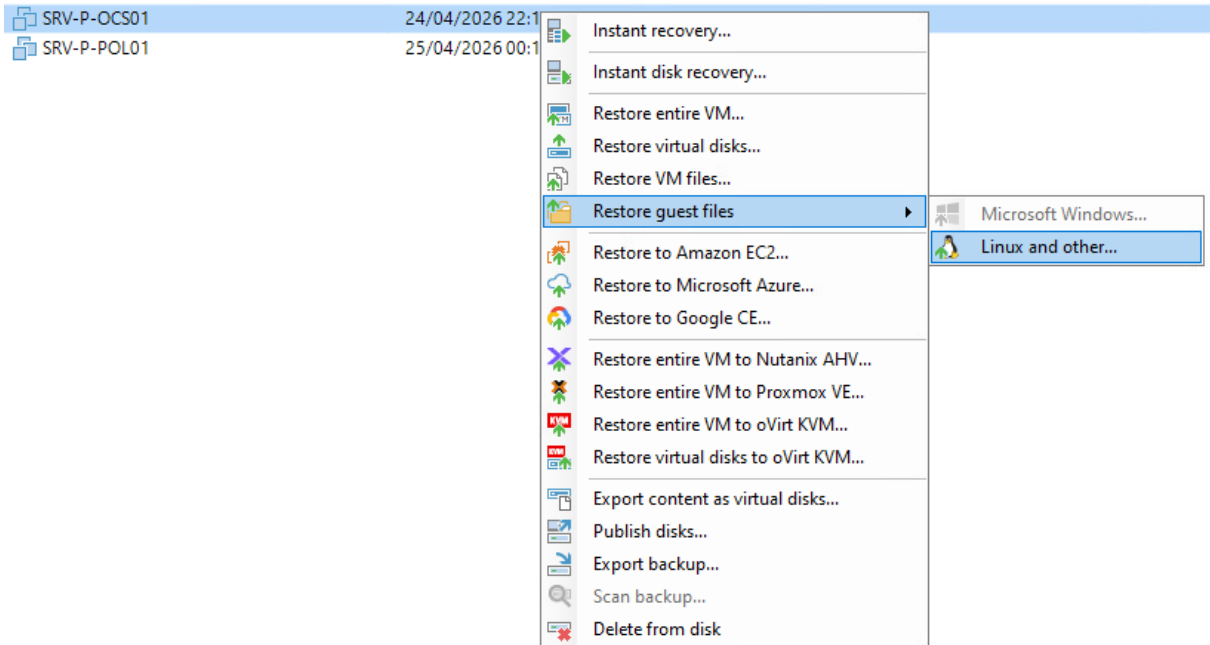


Ensuite vérification que le fichier restauré est visible dans son répertoire d'origine. Cela confirme que la sauvegarde est fonctionnelle, la restauration est opérationnelle.

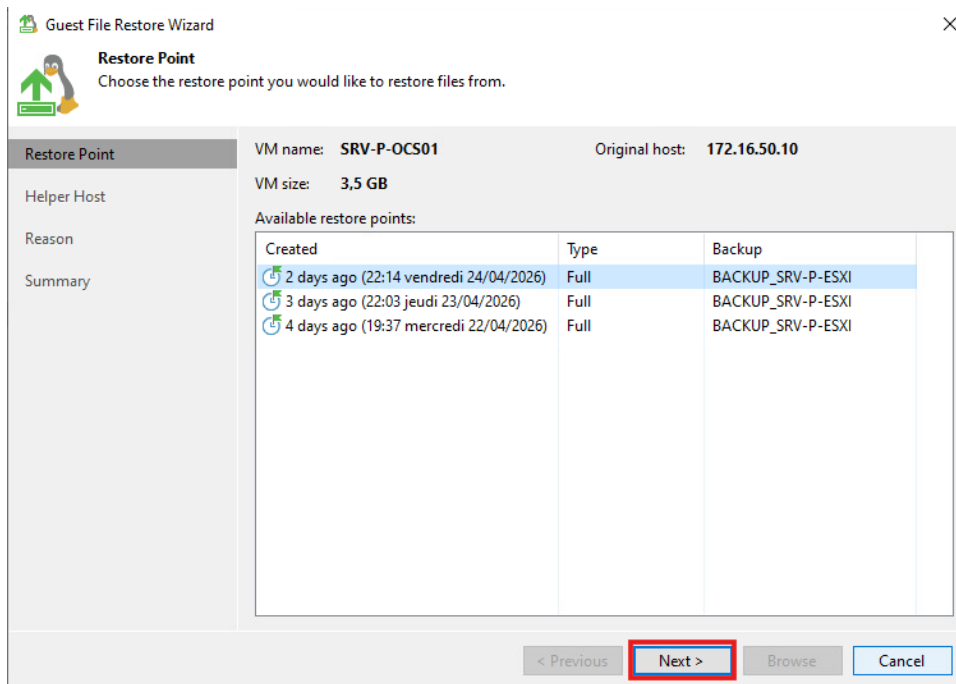


4.10.2.2. Restauration d'un fichier sur un serveur Linux Debian

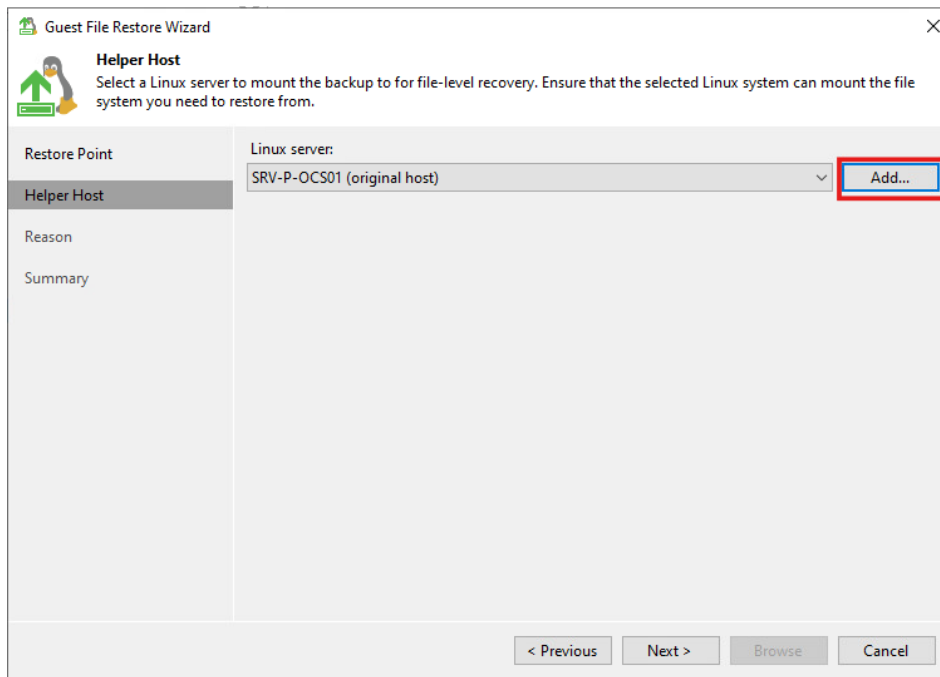
Lancement de l'assistant de restauration : clic droit sur la sauvegarde, puis sélection de Restore guest files > Linux and other afin de démarrer la restauration de fichiers pour la machine Linux.



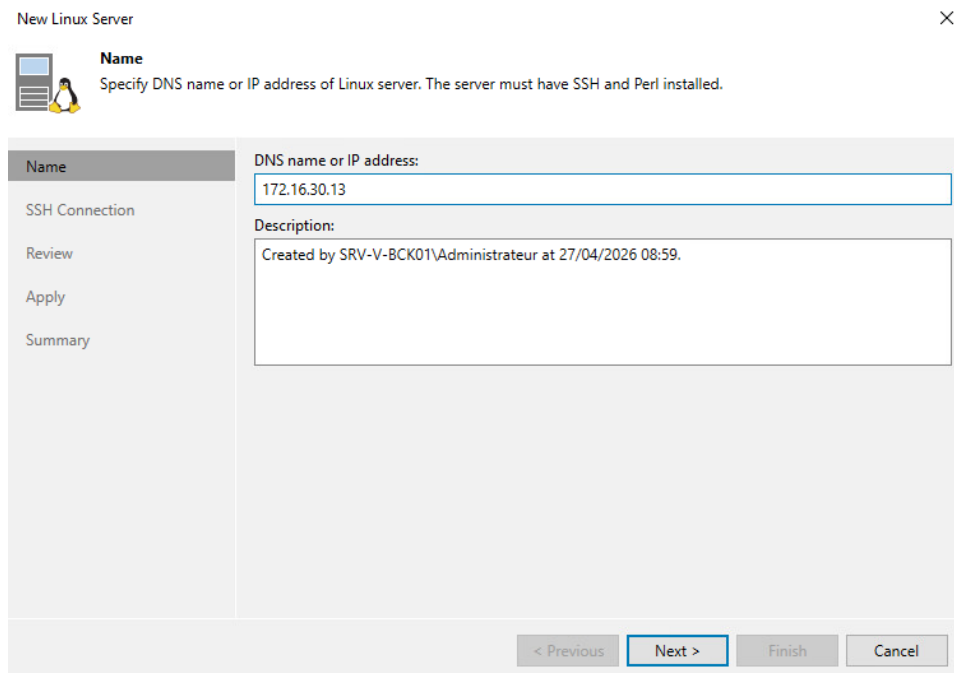
Sélection du point de restauration souhaité (date et heure de la sauvegarde) à partir duquel les fichiers seront récupérés, puis clic sur Next.



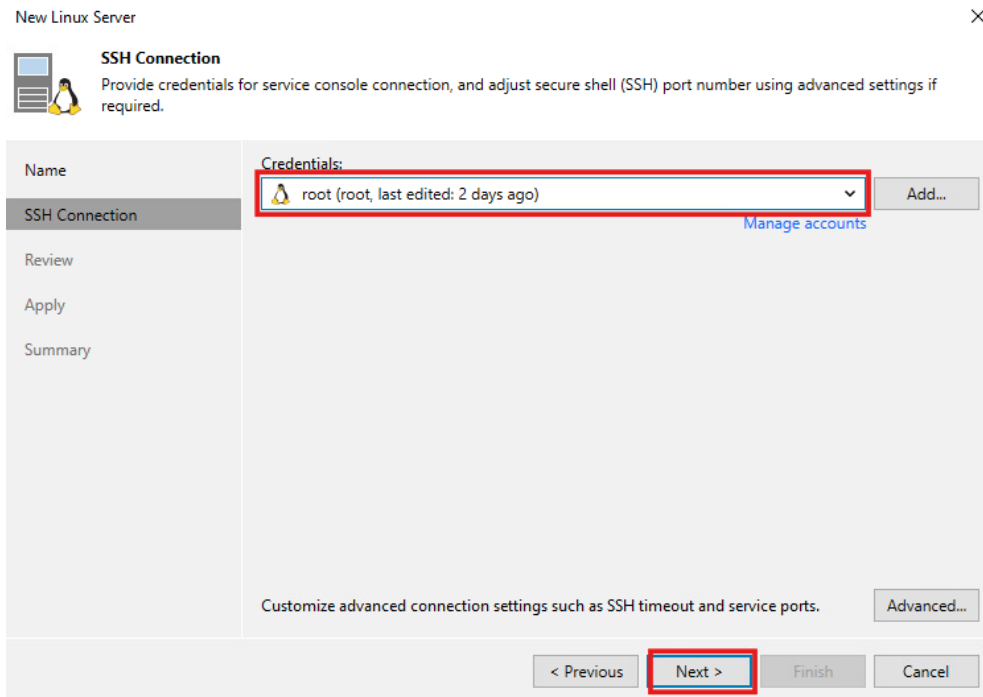
Ajout du serveur Linux qui sera utilisé pour monter la sauvegarde et permettre la restauration des fichiers.



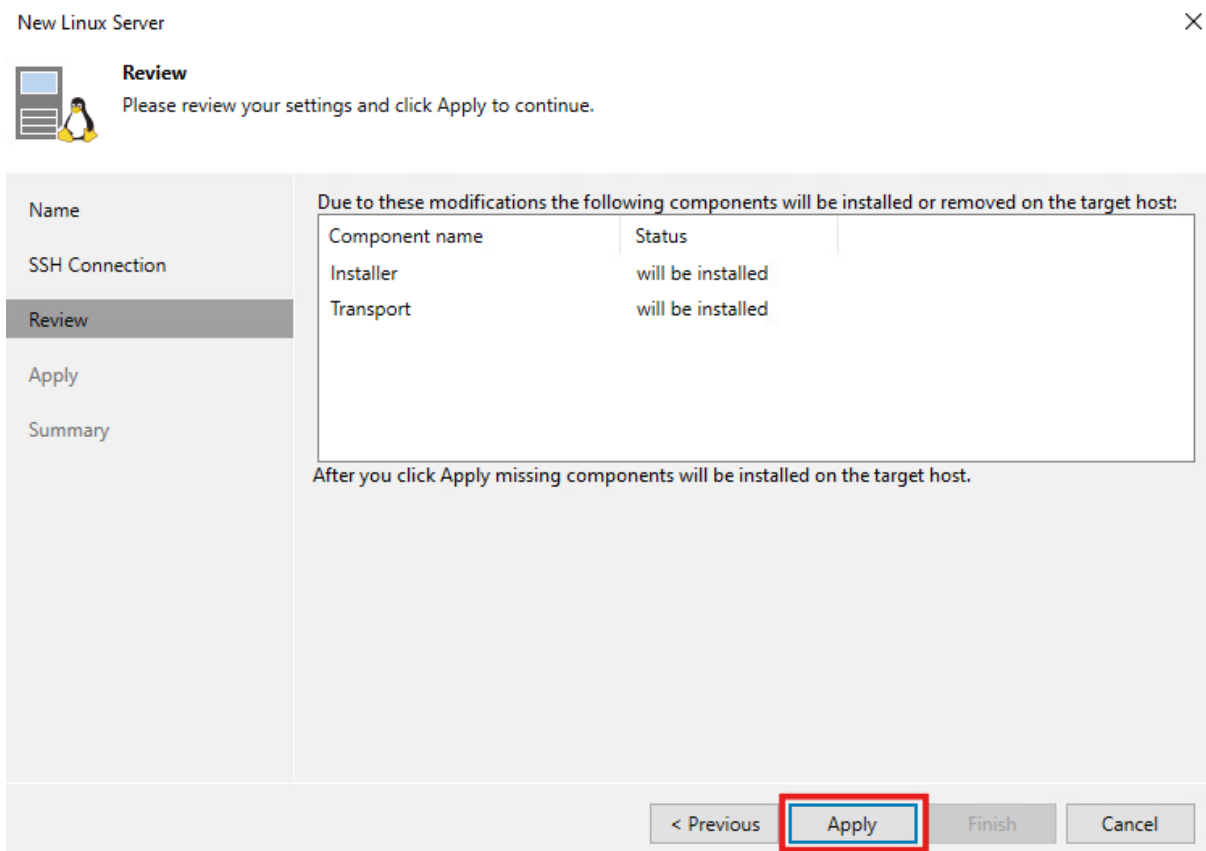
Saisie l'adresse IP du serveur Linux cible, puis validation avec Next.



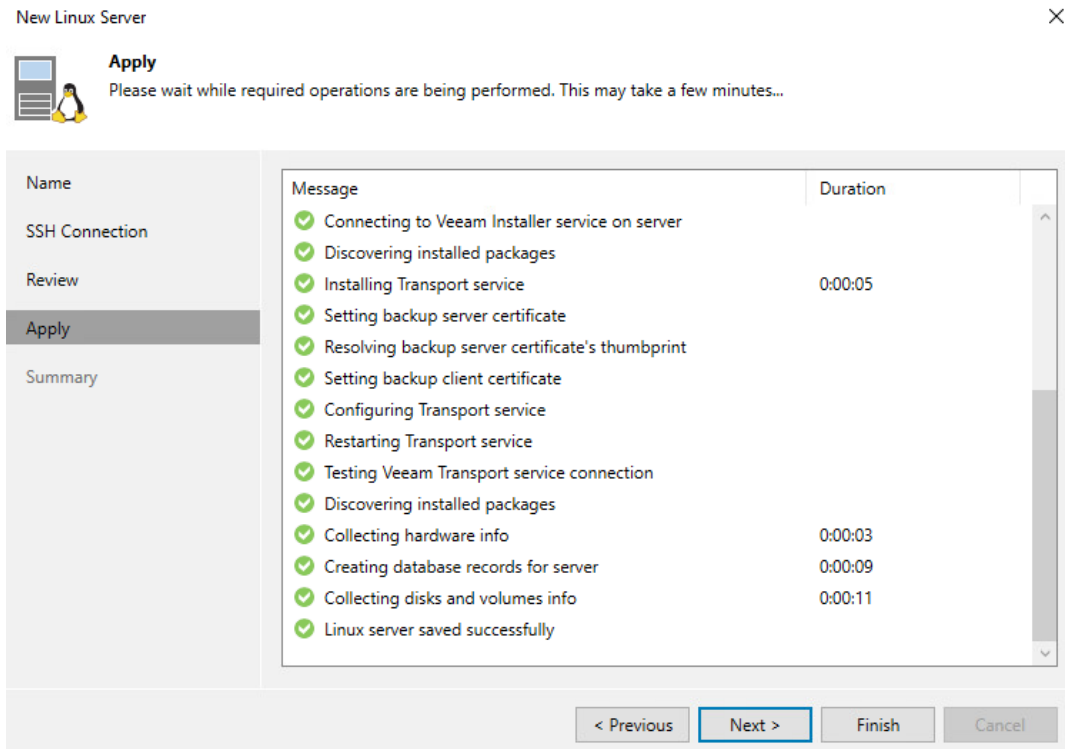
Configuration de la connexion SSH : sélection du compte « root » permettant de se connecter au serveur Linux.



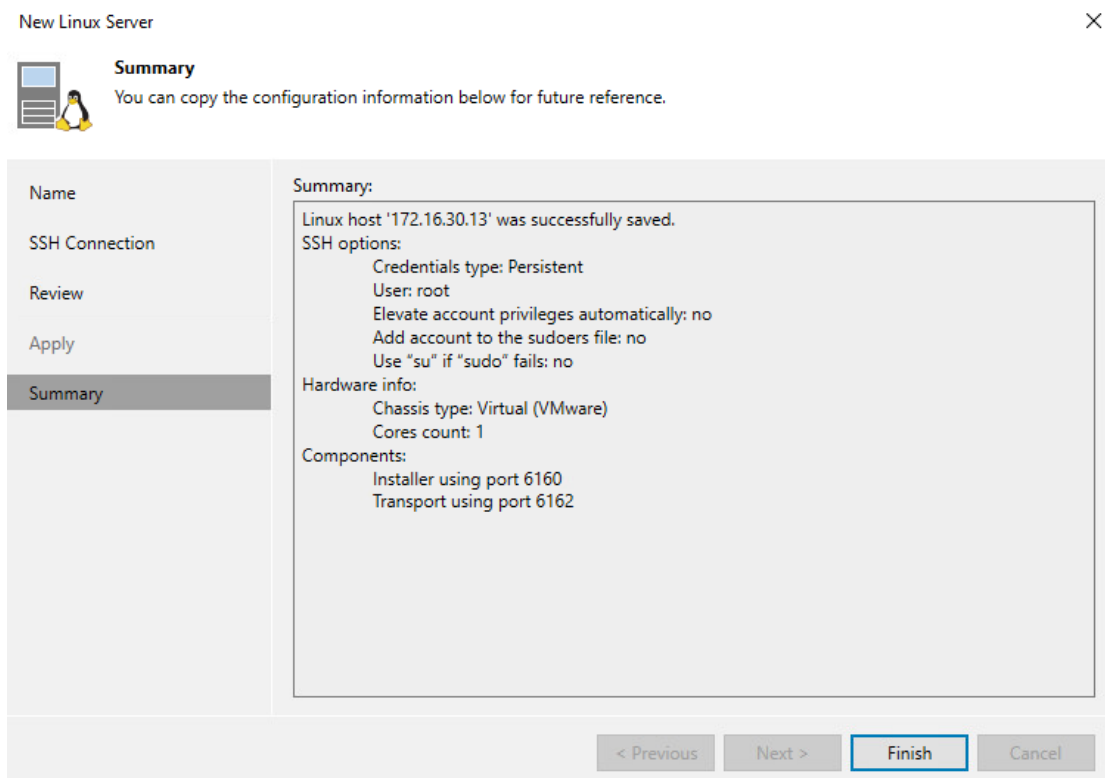
Vérification du résumé des composants à installer (Transport, Installer), puis lancement de la configuration avec Apply.



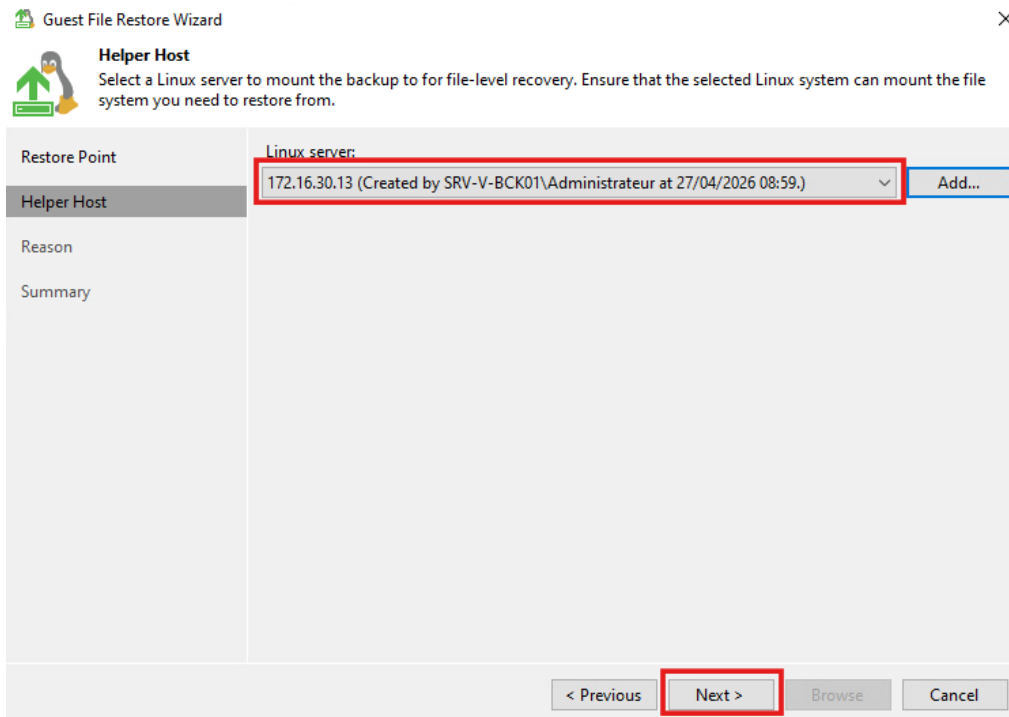
Suivi de l'installation automatique des composants nécessaires sur le serveur Linux (services Veeam, transport, certificats, etc.).



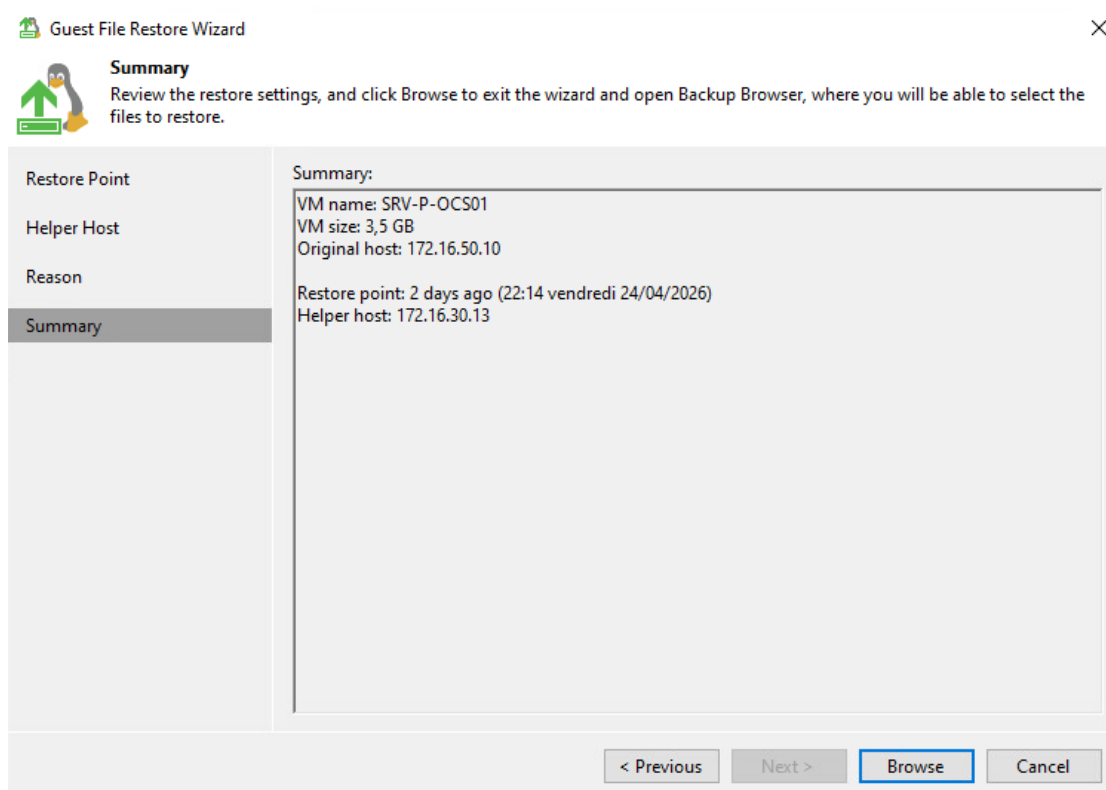
Confirmation que le serveur Linux a bien été ajouté avec succès et que tous les composants sont opérationnels.



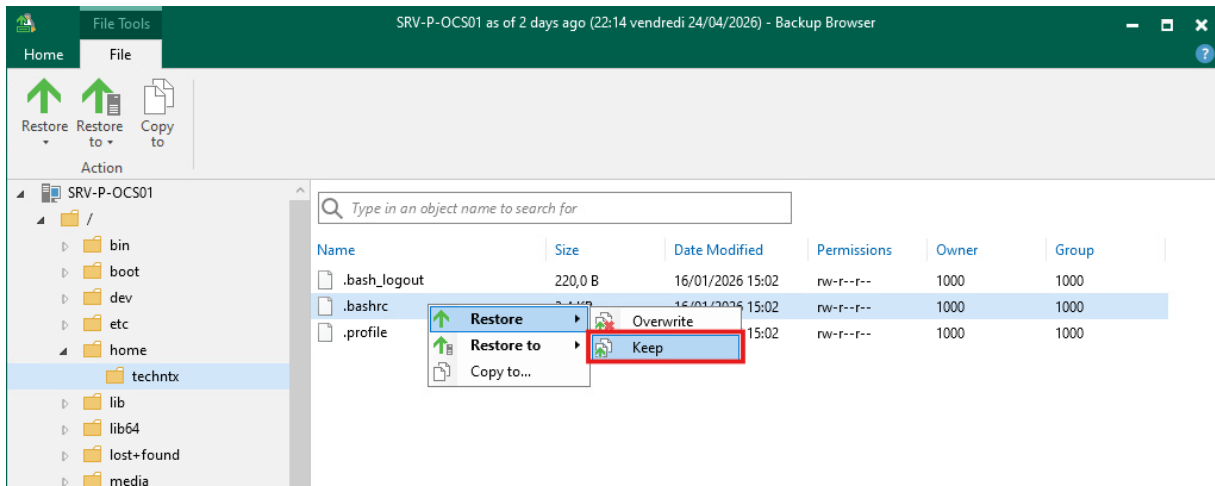
Sélection du serveur Linux nouvellement ajouté, puis clic sur Next pour continuer.



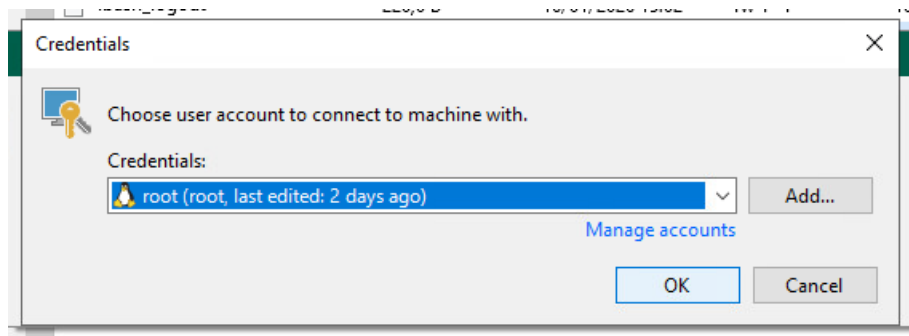
Résumé de la tâche de restauration : point de restauration choisi, machine source et serveur utilisé.



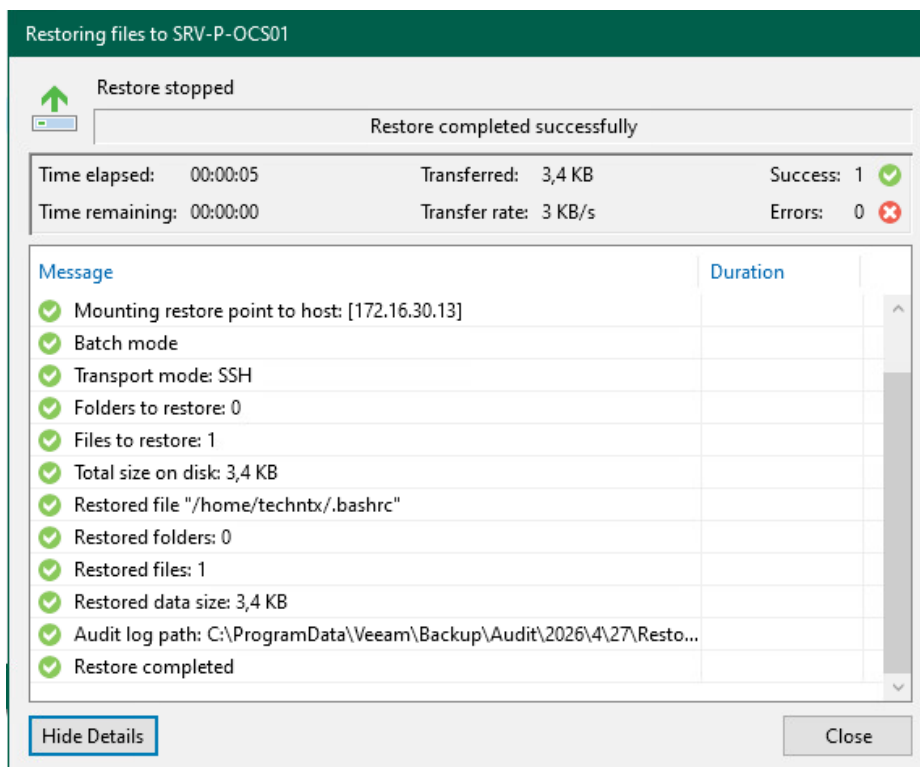
Exploration des fichiers sauvegardés via le navigateur : sélection du fichier à restaurer puis clic sur Restore.



Authentification sur le serveur Linux cible avec les identifiants SSH pour autoriser la restauration.



Exécution de la restauration : le fichier est transféré vers le serveur Linux et le processus se termine avec succès.



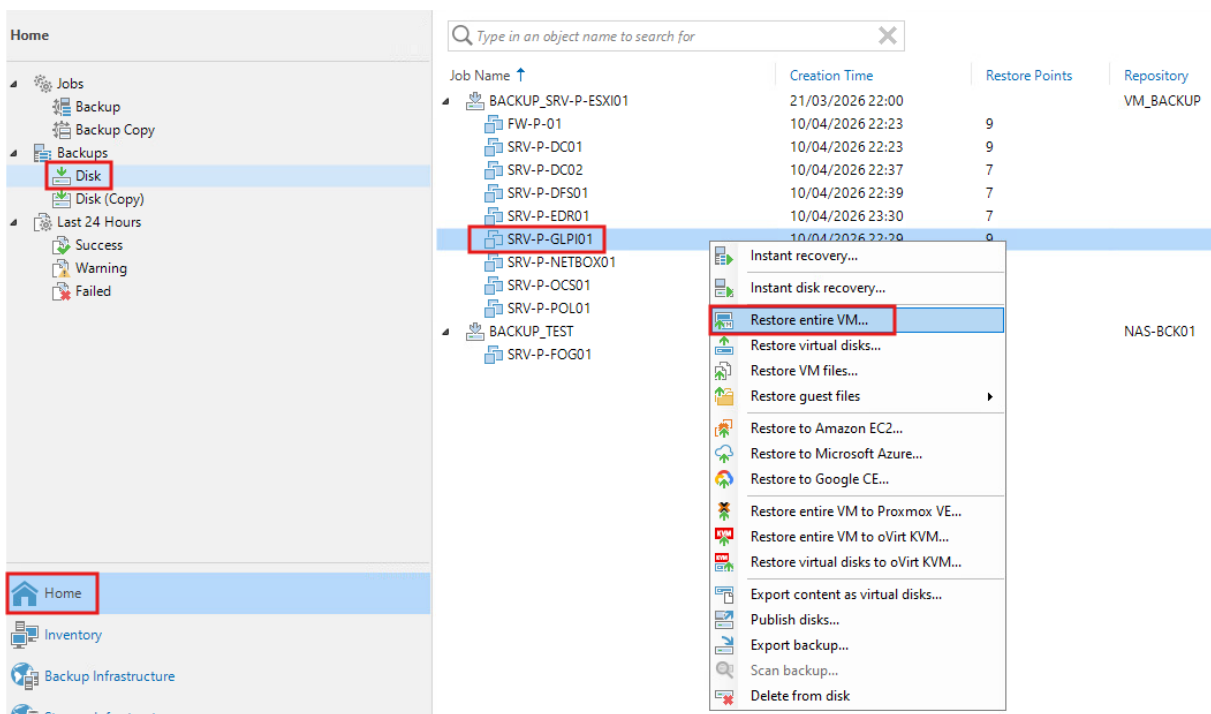
Sur la machine, on peut voir le fichier restauré.

```
root@SRV-P-OCS01:/home/techntx# ll
total 24K
drwx----- 2 techntx techntx 4,0K 27 avril 09:08 .
drwxr-xr-x  3 root    root    4,0K 16 janv. 15:02 ..
-rw-r--r--  1 techntx techntx 220 16 janv. 15:02 .bash_logout
-rw-r--r--  1 techntx techntx 3,5K 16 janv. 15:02 .bashrc
-rw-r--r--  1 techntx techntx 3,5K 16 janv. 15:02 .bashrc_RESTORED_20260427_090813
-rw-r--r--  1 techntx techntx 807 16 janv. 15:02 .profile
root@SRV-P-OCS01:/home/techntx# _
```

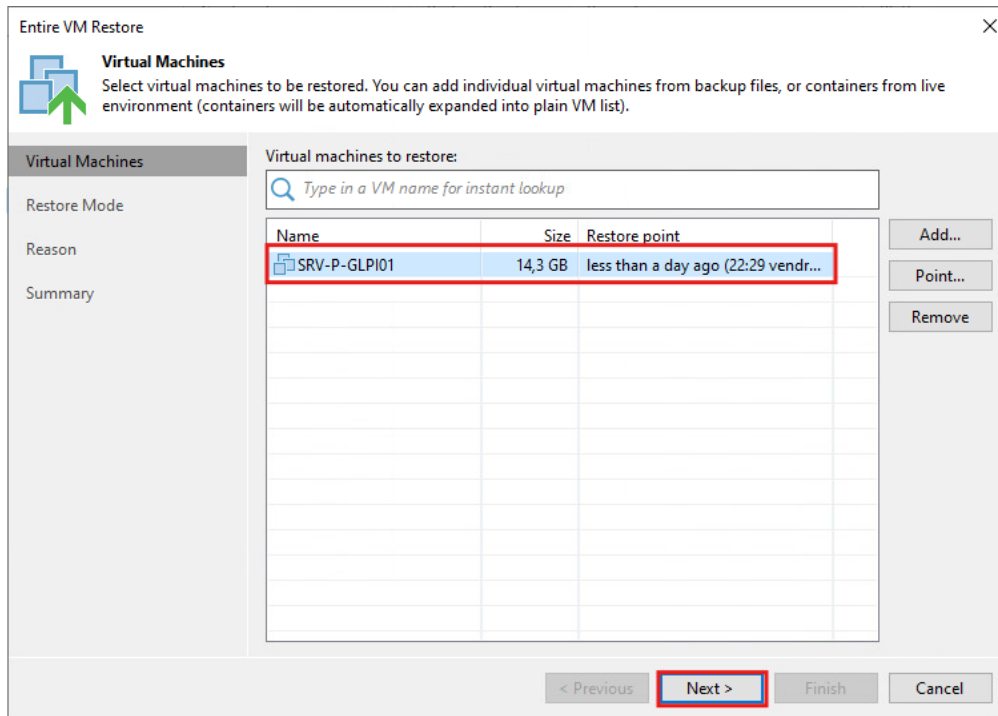
4.10.2.3. Restauration d'une VM complète

Sélection du point de restauration Aller dans Home > Disk Clic droit sur la VM (ex : SRV-P-GLPI01).

Cliquer sur Restore entire VM



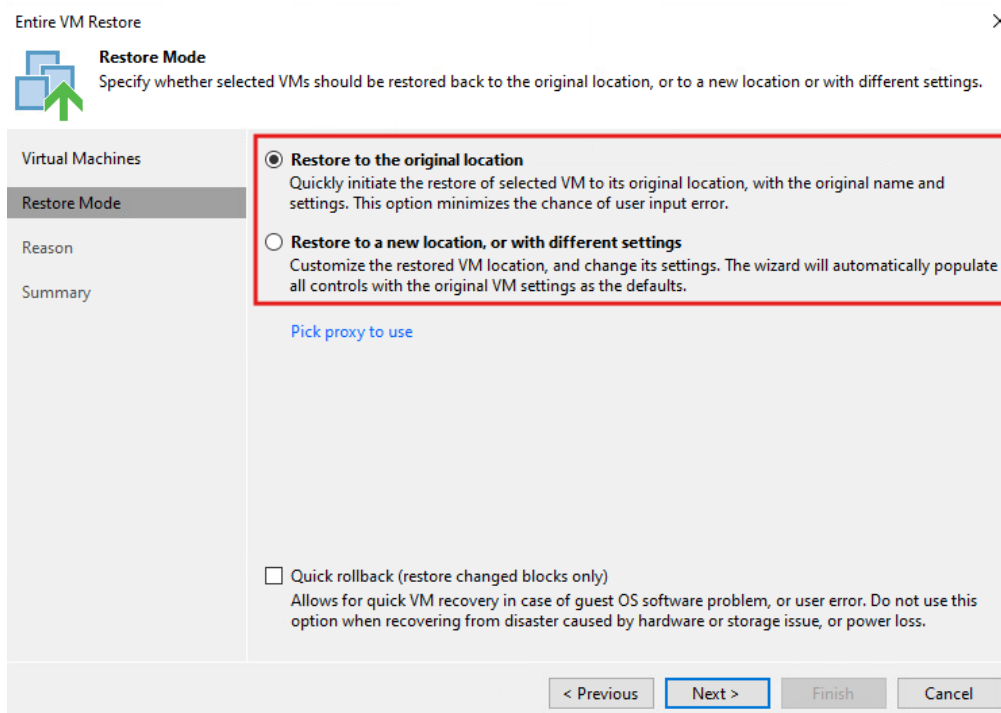
Dans la fenêtre, choisir le point de restauration (par exemple : « less than a day ago »). Il est également possible de sélectionner un point de sauvegarde plus ancien si nécessaire.



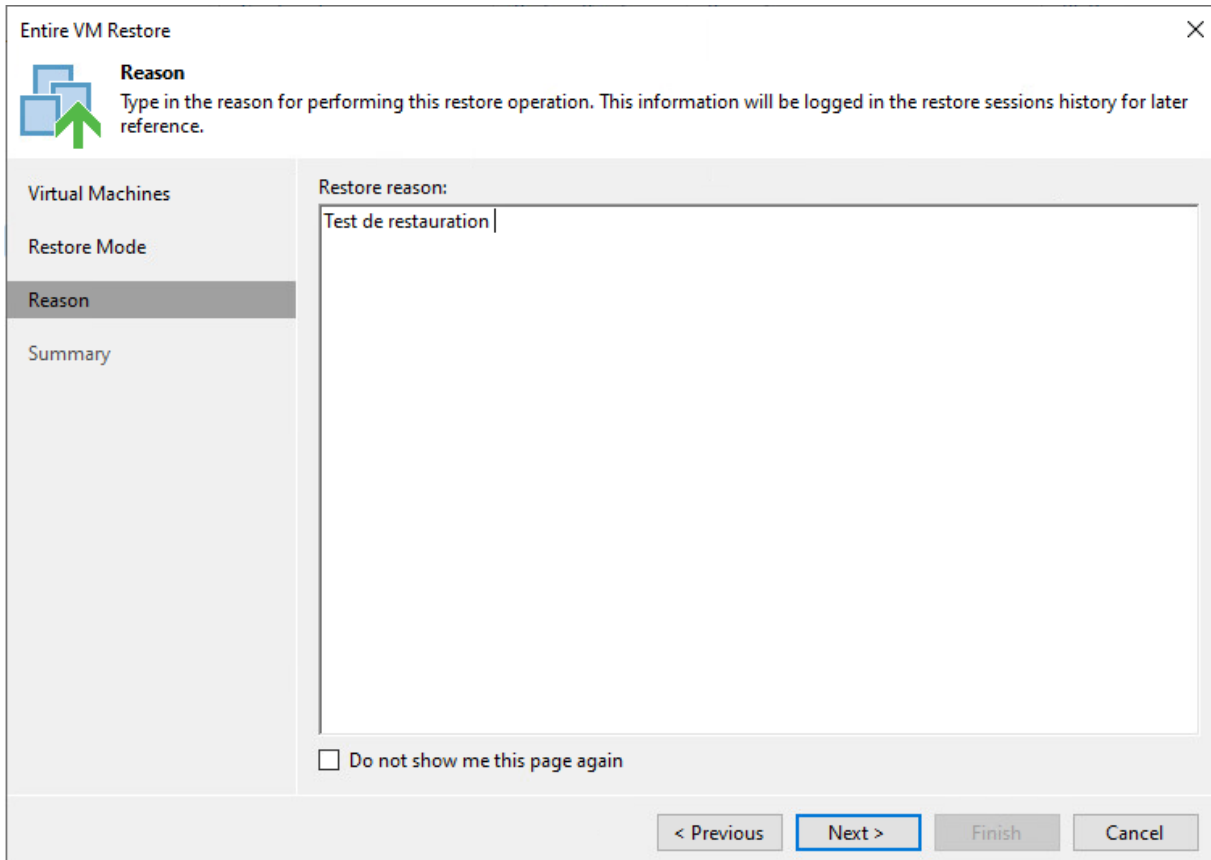
Choix du mode de restauration, il y a deux options :

- Restore to the original location (choisi dans le test)
 - o Restaure la VM à son emplacement d'origine
 - o Même nom, même configuration
- Restore to a new location
 - o Utilisé pour cloner ou tester sans impacter la prod

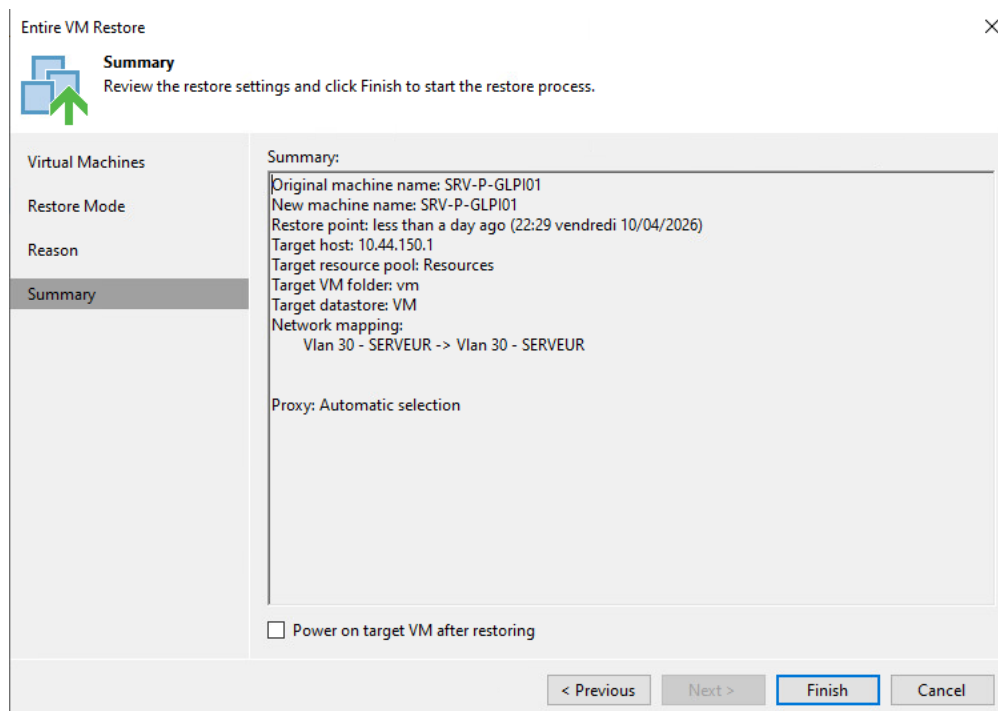
Je sélectionne restauration à l'emplacement d'origine



Raison de restauration (cela permet de repérer plus facilement pourquoi une restauration a été effectuée).



Résumé et lancement de la restauration ne pas oublier de vérifier le nom VM, Host cible, Datastore et Réseau.



Résultat de l'opération, avec comme statut Success, une durée d'environ 6min.

Restoring VM

Name: **SRV-P-GLPI01** Status: **Success**
Restore type: Full VM Restore Start time: 11/04/2026 11:59:04
Initiated by: SRV-V-BCK01\Administrateur End time: 11/04/2026 12:05:17

Statistics Reason Parameters Log

Message	Duration
✓ Queued for processing at 11/04/2026 11:59:07	
✓ Processing SRV-P-GLPI01	0:06:09
✓ Required backup infrastructure resources have been assigned	0:00:05
✓ Locking required backup files	0:00:02
✓ VM SRV-P-GLPI01 has been powered off successfully	0:00:02
✓ 5 files to restore (20 GB)	
✓ Restoring file SRV-P-GLPI01.nvram (8,5 KB)	
✓ Restoring [VM] SRV-P-GLPI01_1/SRV-P-GLPI01_1.vmx	0:00:01
✓ Preparing for virtual disks restore	0:00:22
✓ Using proxy VMware Backup Proxy for restoring disk Hard disk 1	
✓ Restoring Hard disk 1 (20 GB) : 14,3 GB restored at 51 MB/s [hotadd]	0:04:46
✓ Restore completed successfully	

Close

On peut ensuite constater que la VM restaurée apparaît bien sur l'ESXi. La VM fonctionne correctement et les services GLPI sont opérationnels.

4.10.3. Simulation de perte de liaison réseau et reprise des sauvegardes différées

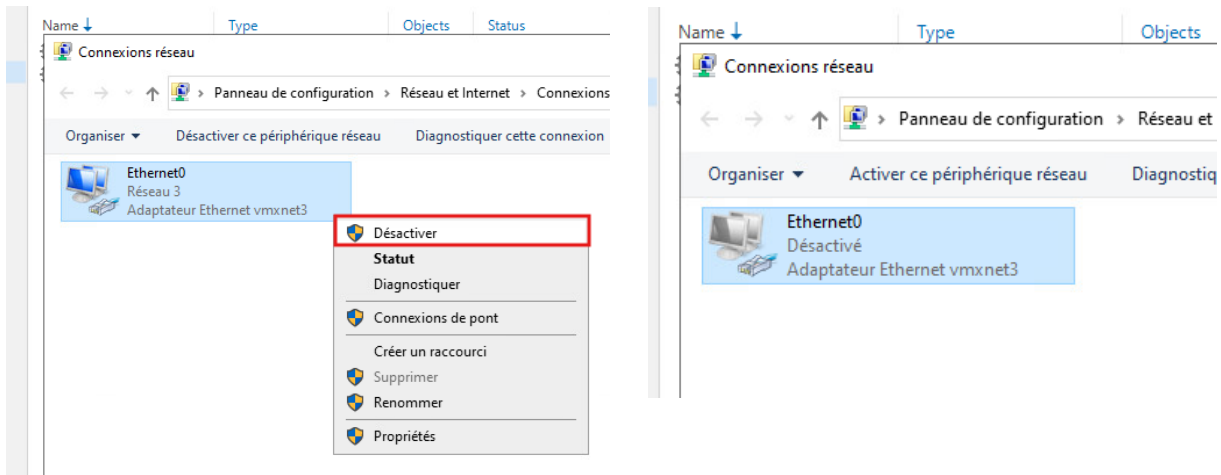
L'objectif de ce test est de valider le comportement de la solution de sauvegarde en cas de perte de connectivité réseau, ainsi que sa capacité à reprendre automatiquement les traitements après rétablissement du lien.

Trois scénarios ont été testés :

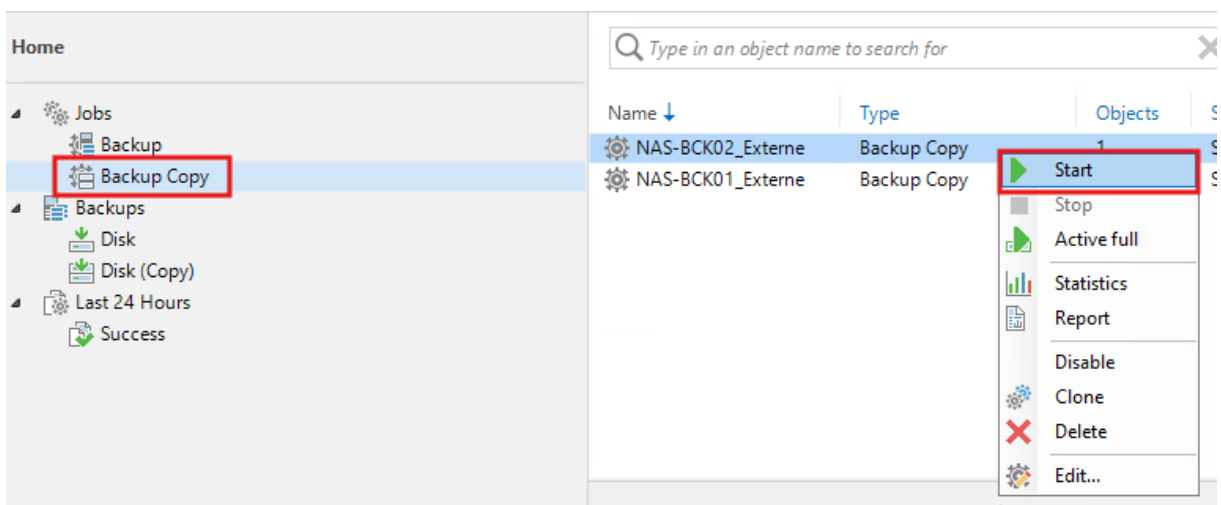
- Coupure de la carte réseau du serveur de sauvegarde
- Coupure réseau via le firewall pendant un Backup Copy
- Coupure réseau via le firewall pendant un job ESXi

4.10.3.1. Coupure de la carte réseau du serveur Veeam lors d'une exécution d'un Backup Copy

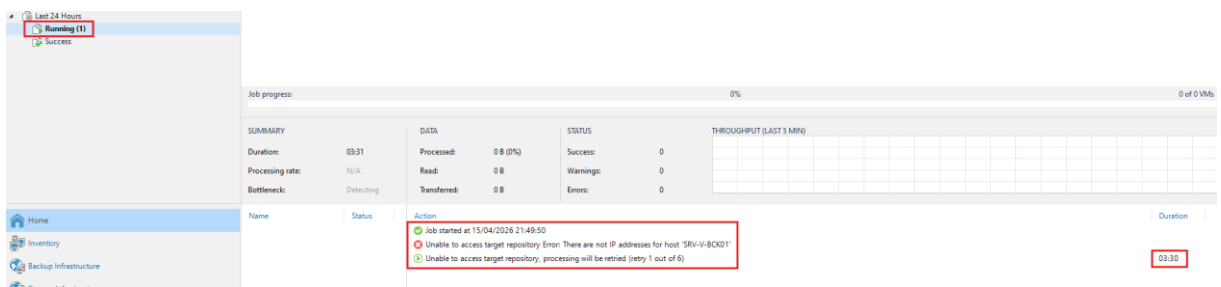
Désactivation de la carte réseau du serveur de sauvegarde via les connexions réseau Windows.



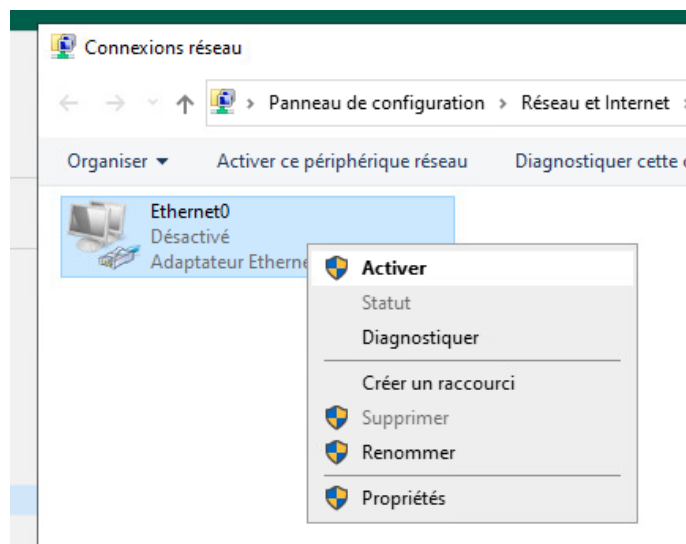
Simulation d'un lancement de sauvegarde automatique, d'un job Backup Copy.



Observation du comportement du job en cours.



Réactivation de la carte réseau après quelques minutes.



Comportement observé :

Dès la coupure réseau, le job ne peut plus communiquer avec les sources ou la cible de sauvegarde. Le processus reste actif pendant un certain temps, correspondant aux délais d'attente (timeouts réseau, résolution DNS, etc.). Après expiration de ces délais, certaines tâches passent en échec ou en attente. Le système déclenche automatiquement des tentatives de reprise (retry).

Une fois la connectivité restaurée, veeam relance automatiquement les opérations échouées selon sa logique interne de retry.

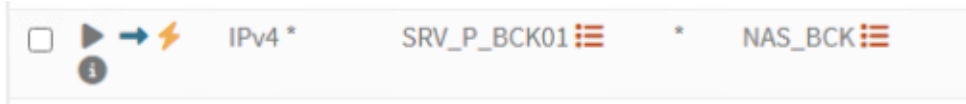
SUMMARY		DATA		STATUS		THROUGHPUT (ALL TIME)	
Duration:	11:22	Processed:	N/A	Success:	10		
Processing rate:	N/A	Read:	N/A	Warnings:	0		
Bottleneck:	N/A	Transferred:	N/A	Errors:	0		

Name	Status	Action	Duration
SRV-P-NETBOX01	Success	Job started at 15/04/2026 21:49:50	
FW-P-01	Success	Unable to access target repository Error: There are not IP addresses for host 'SRV-V-BCK01'	10:01
SRV-P-QCS01	Success	Unable to access target repository, processing will be retried (retry 1 out of 6)	10:01
SRV-P-DFS01	Success	Unable to access target repository Error: There are not IP addresses for host 'SRV-V-BCK01'	05:00
SRV-P-POL01	Success	Unable to access target repository, processing will be retried (retry 2 out of 6)	05:00
SRV-P-DC01	Success	Building VMs list	00:01
SRV-P-DC02	Success	Job finished at 15/04/2026 22:01:13	
SRV-P-EDR01	Success		
SRV-P-FOG01	Success		
SRV-P-GLP01	Success		

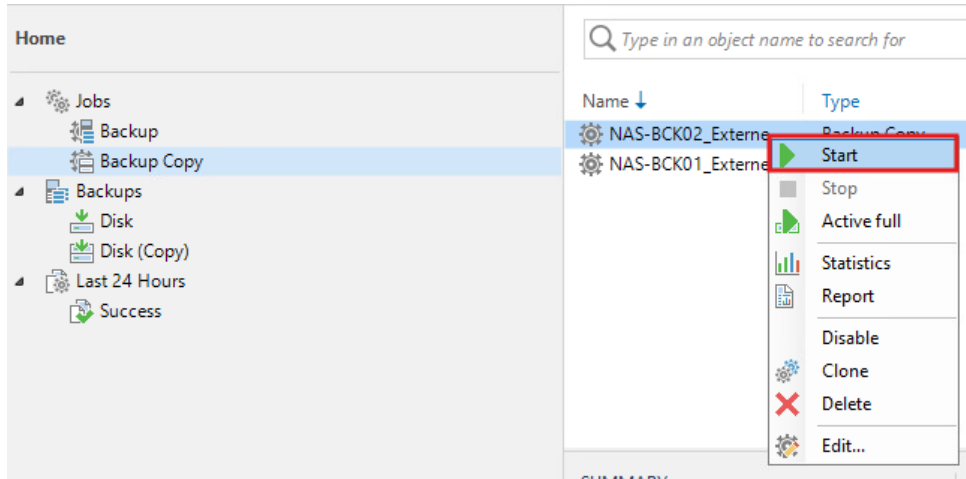
Le délai de 10 minutes correspond au délai maximum entre cycles complets. Mais certaines étapes internes (DNS resolution, timeout réseau) consomment déjà du temps le retry peut être déclenché plus tôt après un échec rapide. Du coup, dans les logs, un intervalle réel plus court.

4.10.3.2. Coupure depuis le Firewall lors d'une exécution d'un Backup Copy

Blocage des flux réseau au niveau du firewall du serveur Veeam vers les NAS.



Démarrage d'un job Backup Copy.



Réactivation de la règle au bout de 5 minutes.



Comportement observé :

- La coupure via firewall simule une perte réseau plus "propre" (pas d'interface désactivée, mais flux bloqués).
- Le job continue temporairement en attente de réponse. (6min27s)
- Le système déclenche automatiquement des tentatives de reprise (retry).
- Après rétablissement des flux, le job reprend sans intervention manuelle.

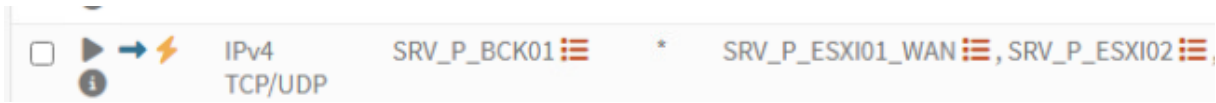
SUMMARY		DATA	STATUS	THROUGHPUT (LAST 5 MIN)
Duration:	11:08	Processed:	0 B (0%)	
Processing rate:	N/A	Read:	0 B	
Bottleneck:	Detecting	Transferred:	0 B	
		Success:	0	
		Warnings:	0	
		Errors:	0	

Name	Status	Action	Duration
FW-P-01	Pending	Job started at 15/04/2026 22:08:39	
SRV-P-DC02	Pending	Unable to access target repository Error: Selected server SRV-V-BCK01 is unavailable.	06:27
SRV-P-DFS01	Pending	Unable to access target repository, processing will be retried (retry 1 out of 6)	06:27
SRV-P-EDR01	Pending	Building VMs list	00:01
SRV-D-NETROVM1	Pending		

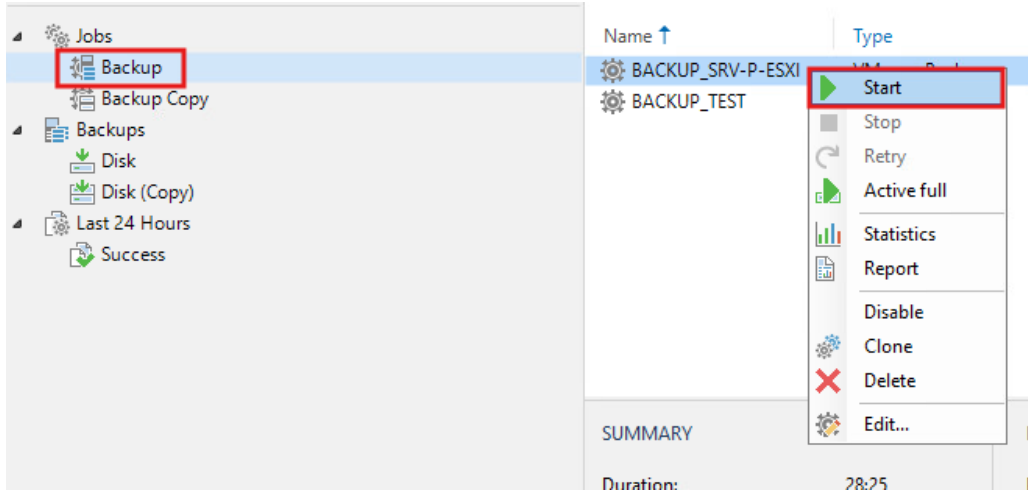
Ce scénario met en évidence la gestion des interruptions réseau côté transport : Les flux étant bloqués mais non supprimés, les délais de détection peuvent être plus longs. Le mécanisme de retry permet une reprise sans relancer complètement le job.

4.10.3.3. Coupure Firewall pour un job ESXi

Coupure des flux réseau entre le serveur de sauvegarde et les hôtes ESXi via le firewall.



Lancement du job de sauvegarde des VMs hébergées sur ESXi.



Observation de l'avancement des VM en cours de traitement.

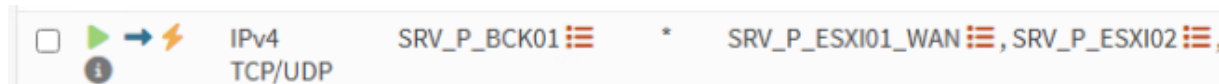
SUMMARY		DATA		STATUS
Duration:	08:37	Processed:	0 B (0%)	Success:
Processing rate:	N/A	Read:	0 B	Warnings:
Bottleneck:	Detecting	Transferred:	0 B	Errors:

Name	Status	Action
FW-P-01	Failed	Job started at 15/04/2026 22:26:06
SRV-P-DC01	Failed	Building list of objects to process
SRV-P-GLPI01	0%	VM size: 498 GB (154 GB used)
SRV-P-OCS01	0%	Changed block tracking is enabled
SRV-P-DC02	Pending	Processing FW-P-01
SRV-P-DFS01	Pending	Processing SRV-P-DC01
SRV-P-EDR01	Pending	Processing SRV-P-GLPI01
SRV-P-NETBOX01	Pending	Processing SRV-P-OCS01
SRV-P-POL01	Pending	Waiting for the next task
SRV-P-FQDN01	Pending	

Les VM en cours de traitement échouent progressivement. Les VM non encore traitées restent en attente. Le job continue son exécution globale malgré les erreurs.

Name	Status	Action	Duration
FW-P-01	Failed	Queued for processing at 15/04/2026 22:26:14	
SRV-P-DC01	Failed	Required backup infrastructure resources have been assigned	00:00
SRV-P-GLPI01	0%	Processing FW-P-01 Error: NFC storage connection is unavailable. Storage: [stg:684adf81-c233ae2c-1f34-5cba2c572afc,nfchostha-host.conn:10.44.150.1]. Storage display name: [VM Essentiel]. Failed to create N...	05:59
SRV-P-DC02	0%	VM processing started at 15/04/2026 22:26:19	
SRV-P-DFS01	Pending	VM size: 20 GB (11,5 GB used)	
SRV-P-EDR01	Pending	Getting VM info from vSphere	05:57
SRV-P-EDR01	Pending	Error: NFC storage connection is unavailable. Storage: [stg:684adf81-c233ae2c-1f34-5cba2c572afc,nfchostha-host.conn:10.44.150.1]. Storage display name: [VM Essentiel]. Failed to create NFC download stream...	
SRV-P-NETBOX01	Pending	Processing finished with errors at 15/04/2026 22:32:19	

Rétablissement des flux réseau.



Avancement directement sur les VM suivante

Name	Status	Action	Duration
FW-P-01	Failed	Queued for processing at 15/04/2026 22:26:14	
SRV-P-DC01	Failed	Required backup infrastructure resources have been assigned	06:03
SRV-P-GLPI01	0%	Processing SRV-P-GLPI01	03:53
SRV-P-DC02	0%	VM processing started at 15/04/2026 22:32:21	
SRV-P-DFS01	Pending	VM size: 20 GB (14,3 GB used)	
SRV-P-EDR01	Pending	Getting VM info from vSphere	03:30
SRV-P-EDR01	Pending	Creating VM snapshot	00:14
SRV-P-NETBOX01	Pending	Saving [VM] SRV-P-GLPI01_1/SRV-P-GLPI01_1.vmx	00:00
SRV-P-POL01	Pending	Saving [VM] SRV-P-GLPI01_1/SRV-P-GLPI01.lnvrnm	00:00
SRV-P-FOG01	Pending	Preparing backup proxy VMware Backup Proxy for disk Hard disk 1 [hotadd]	00:05

Le traitement est effectué 2 VM par 2 VM, une coupure n'impacte pas nécessairement l'ensemble du job immédiatement.

4.10.4. Vérification de la conformité de la politique de rétention

L'objectif est de s'assurer que la politique de rétention des sauvegardes est correctement appliquée dans Veeam Backup & Replication.

On observe notamment que le job BACKUP_SRV-P-ESXI conserve jusqu'à 9 points de restauration, tandis que le job BACKUP_EXTERNE peut en conserver jusqu'à 20.

Il est également important de noter que certaines machines virtuelles ne présentent pas encore le nombre maximal de points de restauration, car elles n'ont pas encore été sauvegardées un nombre de fois suffisant pour atteindre la limite définie par la politique de rétention.

Job Name ↑	Creation Time	Restore Points	Repository	Platform
BACKUP_SRV-P-ESXI01	21/03/2026 22:00		VM_BACKUP	VMware
FW-P-01	10/04/2026 22:23	9		
SRV-P-DC01	10/04/2026 22:23	9		
SRV-P-DC02	10/04/2026 22:37	7		
SRV-P-DFS01	10/04/2026 22:39	7		
SRV-P-EDR01	10/04/2026 23:30	7		
SRV-P-GLPI01	10/04/2026 22:29	9		
SRV-P-NETBOX01	11/04/2026 00:00	7		
SRV-P-DCS01	10/04/2026 22:36	7		
SRV-P-POL01	11/04/2026 00:17	5		

Job Name ↑	Creation Time	Restore Points	Repository
BACKUP_Externe	20/02/2026 10:39		NAS-BCK01
FW-P-01	10/04/2026 22:23	20	
SRV-P-DC01	10/04/2026 22:23	20	
SRV-P-DC02	10/04/2026 22:37	20	
SRV-P-DFS01	10/04/2026 22:39	5	
SRV-P-EDR01	10/04/2026 23:30	5	
SRV-P-GLPI01	10/04/2026 22:29	20	
SRV-P-NETBOX01	11/04/2026 00:00	5	
SRV-P-OCS01	10/04/2026 22:36	5	
SRV-P-POL01	11/04/2026 00:17	4	

La politique de rétention est correctement appliquée pour les différents sauvegarde (local et externe).

S'il y a un dépassement du nombre de points de restauration sur les NAS, c'est normal, car :

- La politique GFS conserve des sauvegardes indépendamment de la rétention principale
- Ces points ne sont pas inclus dans le calcul des 20 restore points
- Veeam privilégie la conservation des points GFS, ce qui peut augmenter temporairement ou durablement le nombre total de points

4.10.5. Analyse des journaux et des alertes.

Les captures ci-dessus présentent les rapports générés par Veeam Backup & Replication à la suite de l'exécution de plusieurs jobs de sauvegarde. Ces rapports permettent de vérifier le bon déroulement des sauvegardes, d'analyser les performances et d'identifier d'éventuelles anomalies.

Présentation générale d'un rapport de job :

Chaque bloc correspond à l'exécution d'un job de sauvegarde.

On y retrouve plusieurs informations essentielles :

- Date et heure d'exécution : permet de situer le job dans le temps
- Statut global :
 - o Success : sauvegarde réussie
 - o Warning : réussite avec avertissements
 - o Error : échec du job
- Durée (Duration) : temps total de la sauvegarde
- Volume total (Total size) : total des machines sauvegardées
- Données lues (Data read) : quantité réellement analysée

- Données transférées (Transferred) : volume effectivement envoyé vers le stockage
- Taille de sauvegarde (Backup size) : taille finale après optimisation

Voici des exemples de rapport de job de sauvegarde :

Backup job: BACKUP_SRV-P-ESXI								
Created by SRV-V-BCK01\Administrateur at 26/09/2025 15:22.								
lundi 13 avril 2026 22:00:03								
Success	10	Start time	22:00:03	Total size	498 GB	Backup size	4,7 GB	
Warning	0	End time	22:28:29	Data read	27,4 GB	Dedupe	1,2x	
Error	0	Duration	0:28:26	Transferred	4,6 GB	Compression	2,9x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
FW-P-01	Success	22:00:21	22:01:44	20 GB	2,3 GB	1,3 GB	0:01:23	
SRV-P-DC01	Success	22:00:21	22:02:16	70 GB	1,8 GB	758,7 MB	0:01:55	
SRV-P-GLPI01	Success	22:01:37	22:03:15	20 GB	5,3 GB	32,3 MB	0:01:38	
SRV-P-OCS01	Success	22:01:52	22:03:19	10 GB	655 MB	14,4 MB	0:01:27	
SRV-P-DC02	Success	22:02:54	22:08:11	70 GB	1,4 GB	560,1 MB	0:05:17	
SRV-P-DFS01	Success	22:03:04	22:08:18	98 GB	1,7 GB	731,8 MB	0:05:14	
SRV-P-EDR01	Success	22:07:51	22:28:27	35 GB	11 GB	1,2 GB	0:20:36	
SRV-P-NETBOX01	Success	22:08:01	22:12:14	25 GB	1,2 GB	21,5 MB	0:04:13	
SRV-P-POL01	Success	22:11:59	22:14:44	20 GB	903 MB	21,8 MB	0:02:45	
SRV-P-FOG01	Success	22:14:35	22:16:28	130 GB	1,2 GB	26,5 MB	0:01:53	

Backup job: BACKUP_SRV-P-ESXI01								
Created by SRV-V-BCK01\Administrateur at 26/09/2025 15:22.								
lundi 23 mars 2026 22:00:19								
Success	8	Start time	22:00:19	Total size	332 GB	Backup size	8,9 GB	
Warning	0	End time	22:11:45	Data read	24,1 GB	Dedupe	1,2x	
Error	0	Duration	0:11:26	Transferred	8,8 GB	Compression	2,2x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
FW-P-01	Success	22:00:37	22:02:38	20 GB	3,8 GB	2,3 GB	0:02:01	
SRV-P-DC01	Success	22:00:37	22:03:01	70 GB	4,3 GB	2 GB	0:02:24	
SRV-P-FOG01	Success	22:02:09	22:03:42	80 GB	902 MB	90,8 MB	0:01:33	
SRV-P-GLPI01	Success	22:02:44	22:04:13	20 GB	1,4 GB	82,3 MB	0:01:29	
SRV-P-SUP01	Success	22:03:20	22:05:16	30 GB	1,8 GB	110,1 MB	0:01:56	
SRV-P-HAProxy	Success	22:03:55	22:06:37	10 GB	703 MB	58,6 MB	0:02:42	
SRV-P-RSAT-T1	Success	22:04:41	22:11:42	70 GB	10,5 GB	4,1 GB	0:07:01	
SRV-P-CLOUD01	Success	22:05:16	22:08:19	32 GB	825 MB	71,4 MB	0:03:03	

Backup job: BACKUP_SRV-P-ESXI01 (Full)								
Created by SRV-V-BCK01\Administrateur at 26/09/2025 15:22.								
samedi 21 mars 2026 22:00:04								
Success	8	Start time	22:00:04	Total size	332 GB	Backup size	86,2 GB	
Warning	0	End time	22:44:24	Data read	140,6 GB	Dedupe	2,4x	
Error	0	Duration	0:44:20	Transferred	86,4 GB	Compression	1,6x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
FW-P-01	Success	22:00:18	22:05:23	20 GB	11,5 GB	7,8 GB	0:05:05	
SRV-P-DC01	Success	22:00:18	22:16:46	70 GB	26,8 GB	16,6 GB	0:16:28	
SRV-P-FOG01	Success	22:04:38	22:32:02	80 GB	39,7 GB	37,2 GB	0:27:24	
SRV-P-GLPI01	Success	22:15:57	22:24:58	20 GB	14,4 GB	1,6 GB	0:09:01	
SRV-P-SUP01	Success	22:24:27	22:31:33	30 GB	6,9 GB	2,2 GB	0:07:06	
SRV-P-HAProxy	Success	22:31:02	22:33:18	10 GB	2,4 GB	949,6 MB	0:02:16	
SRV-P-RSAT-T1	Success	22:31:58	22:44:22	70 GB	33,9 GB	17,8 GB	0:12:24	
SRV-P-CLOUD01	Success	22:33:11	22:39:15	32 GB	5,1 GB	2,3 GB	0:06:04	

Backup job: BACKUP_SRV-P-ESXI (Full)								
Created by SRV-V-BCK01\Administrateur at 26/09/2025 15:22.								
vendredi 10 avril 2026 22:22:29								
Success	9	Start time	22:22:29	Total size	368 GB	Backup size	65 GB	Virtual Machine SRV-P-FOG01 is unavailable and will be skipped from processing Job finished with error at 11/04/2026 00:45:30
Warning	0	End time	00:45:30	Data read	139,1 GB	Dedupe	2,7x	
Error	0	Duration	2:23:01	Transferred	65 GB	Compression	2,1x	
Details								
Name	Status	Start time	End time	Size	Read	Transferred	Duration	Details
FW-P-01	Success	22:22:42	22:29:32	20 GB	11,5 GB	7,5 GB	0:06:50	
SRV-P-DC01	Success	22:22:42	22:37:19	70 GB	27,7 GB	16,9 GB	0:14:37	
SRV-P-GLPI01	Success	22:28:30	22:36:32	20 GB	14,3 GB	1,6 GB	0:08:02	
SRV-P-OCS01	Success	22:35:58	22:38:42	10 GB	3,3 GB	1,3 GB	0:02:44	
SRV-P-DC02	Success	22:36:55	23:59:51	70 GB	24,6 GB	13,2 GB	1:22:56	
SRV-P-DFS01	Success	22:38:31	23:29:55	98 GB	18,4 GB	10,3 GB	0:51:24	
SRV-P-NETBOX01	Success	23:59:16	00:17:02	25 GB	5,6 GB	2,3 GB	0:17:46	
SRV-P-EDR01	Success	23:29:36	00:45:27	35 GB	30,7 GB	10,8 GB	1:15:51	
SRV-P-POL01	Success	00:16:53	00:26:55	20 GB	3 GB	1,1 GB	0:10:02	

4.11. Axe amélioration

Plusieurs axes d'amélioration peuvent être envisagés afin de faire évoluer la solution de sauvegarde mise en place avec Veeam Backup & Replication.

Tout d'abord, la mise en place d'un système de notifications par mail pourrait être envisagée. Actuellement absent, ce mécanisme permettrait d'informer automatiquement les équipes techniques en cas d'échec de sauvegarde, d'erreur ou d'événement critique.

Ensuite, bien que l'infrastructure actuelle repose déjà sur plusieurs supports, l'ensemble reste situé sur un même site. Cela constitue une limite en cas de sinistre majeur impactant le bâtiment. Il serait donc recommandé de mettre en place une copie des sauvegardes sur un site distant ou dans un autre bâtiment. Cette amélioration permettrait de se rapprocher davantage de la règle du « 3-2-1 » et d'assurer une meilleure résilience des données.

Il serait aussi pertinent de mettre en place des tests réguliers de restauration afin de valider l'intégrité et la fiabilité des sauvegardes.

Ces améliorations permettraient de renforcer, la sécurité et l'efficacité de la solution de sauvegarde, tout en répondant aux enjeux de continuité d'activité et de protection des données de l'entreprise OASIS.

4.12. Conclusion

En conclusion, ce projet m'a permis de développer de nombreuses compétences dans le domaine de la sauvegarde et de la gestion d'infrastructures. J'ai pu réaliser des tâches concrètes, telles que la mise en place et la configuration de la solution Veeam Backup & Replication afin d'assurer la protection des données de différents serveurs et environnements virtualisés. Cela m'a permis de mieux comprendre les enjeux liés à la continuité d'activité, à la sécurisation des données et à la gestion des sauvegardes.

La solution Veeam s'est révélée fiable et performante pour assurer la sauvegarde des données critiques, automatiser les tâches de protection et garantir une restauration rapide en cas d'incident. Cette expérience m'a permis de renforcer mes compétences techniques tout en développant ma capacité à anticiper les risques et à mettre en œuvre des solutions adaptées dans un environnement professionnel.

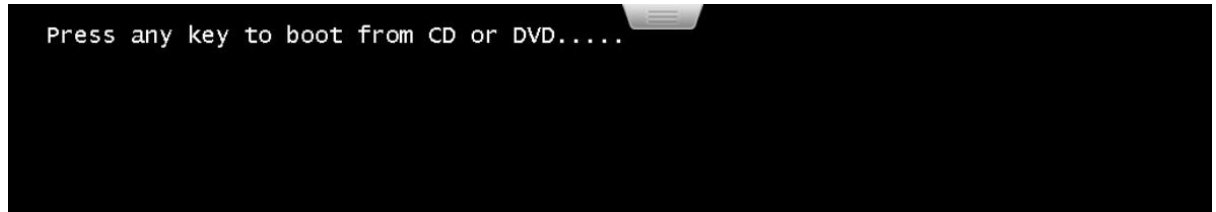
Pour terminer, ce projet m'a permis de valider plusieurs compétences du référentiel BTS SIO Option SISR :

- Gérer le patrimoine informatique
- Répondre aux incidents et aux demandes d'assistance et d'évolution
- Travailler en mode projet
- Mettre à disposition des utilisateurs un service informatique

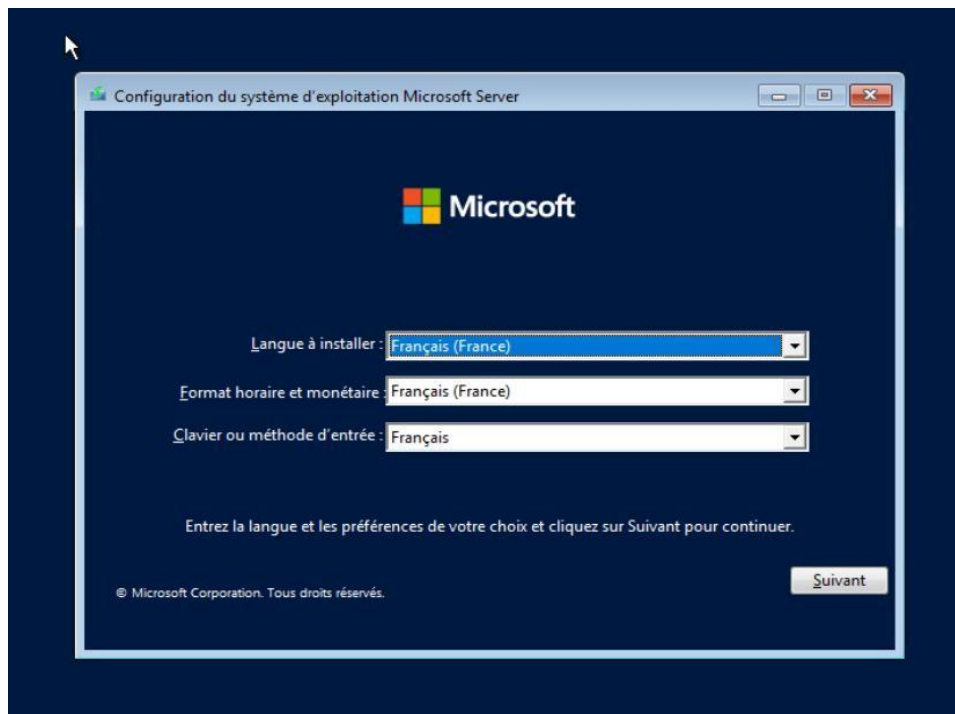
5. Annexe

5.1. Annexe 1 : Documentation Installation Windows Serveur

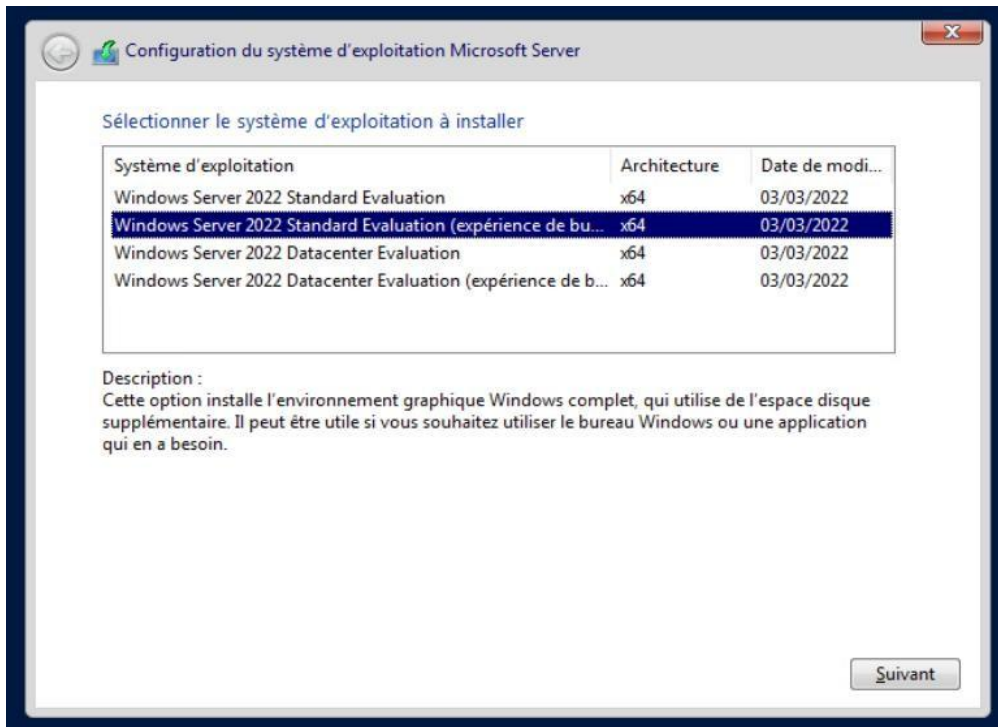
Boot sur le disque ISO Windows Server 2022



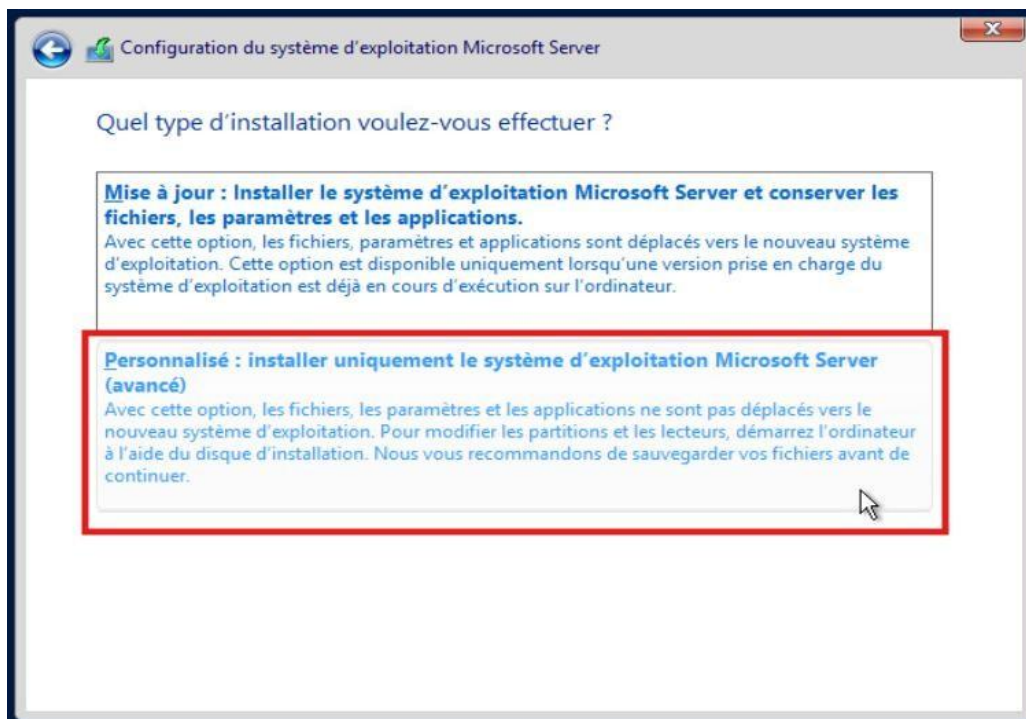
Choisir la langue « Français » :



Sélectionner le système d'exploitation « Windows Server 2022 Standard » avec l'expérience de bureau, afin d'obtenir une interface graphique.



Pour le type d'installation, choisir « Personnalisé », c'est une nouvelle machine, il faut installer le système, et non le mettre à jour.



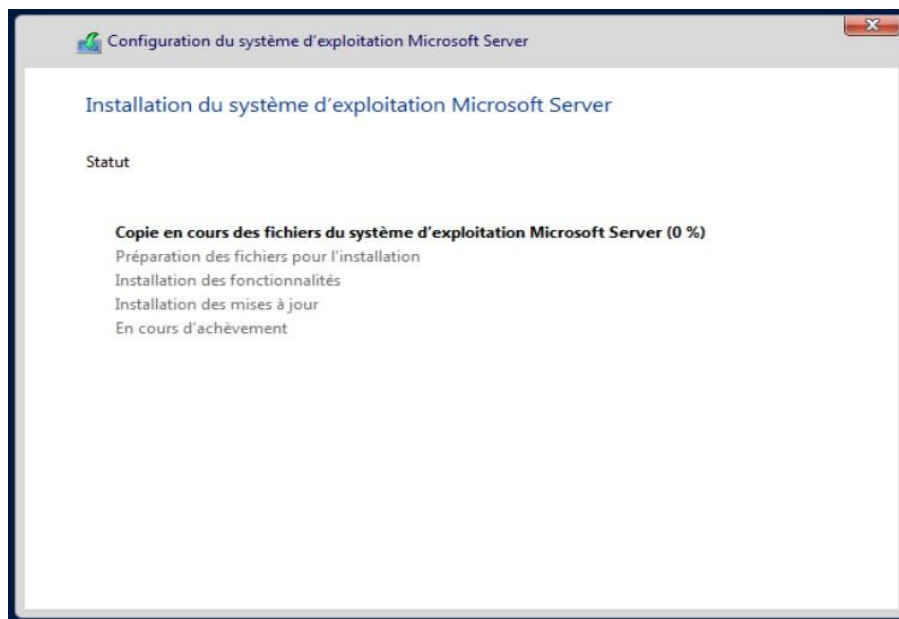
Initialiser les volumes en cliquant sur « Nouveau », puis une fois cela fait « Suivant »

Où voulez-vous installer le système d'exploitation ?

Nom	Taille totale	Espace libre	Type
 Lecteur 0 Partition 1	100.0 Mo	95.0 Mo	Système
 Lecteur 0 Partition 2	16.0 Mo	16.0 Mo	MSR (réservé)
 Lecteur 0 Partition 3	31.9 Go	31.9 Go	Principal

Actualiser Supprimer Formater Nouveau
Charger un pilote Étendre

L'installation du système commence, attendre quelques minutes.



Rentrer un mot de passe pour le compte Administrateur local.


Paramètres de personnalisation

Tapez un mot de passe pour le compte Administrateur intégré que vous pouvez utiliser pour vous connecter automatiquement à cet ordinateur.

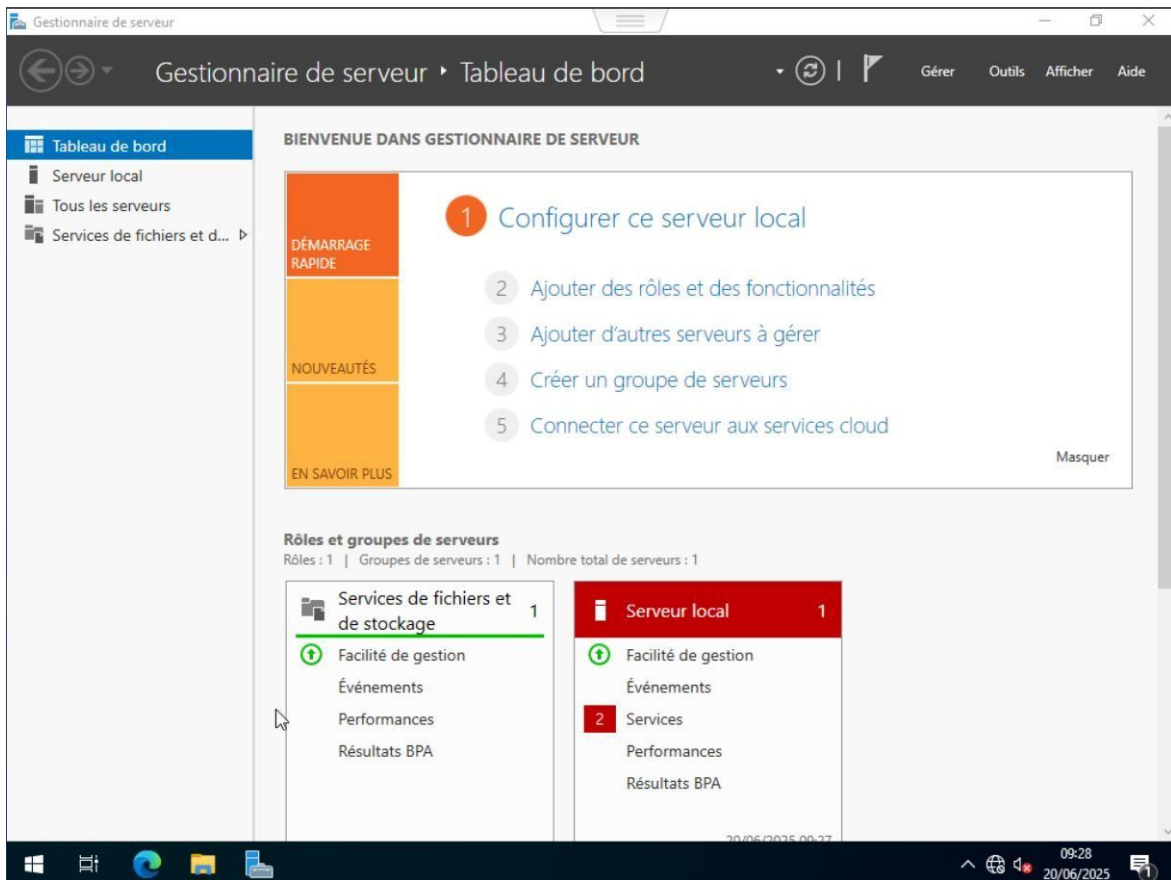
Nom d'utilisateur

Mot de passe

Entrez de nouveau le mot de passe

 Terminer

Une fois le serveur démarré, le gestionnaire de serveur s'ouvre.
Modifier le nom du serveur, l'adresse IP, désactiver la sécurité renforcée d'Internet Explorer, puis redémarrer.



5.2. Annexe 2 : Glossaire

UDP (User Datagram Protocol) : Protocole de transport non connecté permettant l'envoi rapide de données sans garantie de livraison, d'ordre ou de duplication. Utilisé notamment pour les services nécessitant de faibles latences (DNS, streaming, supervision SNMP).

TCP (Transmission Control Protocol) : Protocole de transport orienté connexion garantissant la livraison fiable, ordonnée et sans erreur des données. Utilisé pour des communications critiques (HTTP, SSH, bases de données).

WAN (Wide Area Network) : Réseau étendu reliant plusieurs réseaux locaux (LAN) sur de grandes distances géographiques, souvent via Internet ou des liaisons privées.

DMZ (Demilitarized Zone) : Zone réseau isolée située entre le réseau interne et Internet, utilisée pour héberger des services accessibles depuis l'extérieur (serveurs web, supervision, etc.) tout en renforçant la sécurité du réseau interne.

LAN (Local Area Network) : Réseau local reliant des équipements informatiques sur une zone géographique restreinte (bâtiment, entreprise, domicile).

VPN : Le VPN (Virtual Private Network) est un outil qui permet de créer un tunnel sécurisé entre deux réseaux distants. Il permet de chiffrer les communications afin de garantir la confidentialité des données échangées entre les différents sites.

Pare-feu (Firewall) : Un pare-feu est un outil de sécurité réseau qui permet de filtrer et de contrôler le trafic entrant et sortant d'un réseau.

RPO (Recovery Point Objective) : Le RPO représente la quantité maximale de données pouvant être perdue en cas d'incident. Il s'exprime généralement en durée (ex : 1 heure), correspondant à l'intervalle entre deux sauvegardes.

RTO (Recovery Time Objective) : Le RTO correspond au temps maximal acceptable pour restaurer un service après un incident. Il définit la durée pendant laquelle une activité peut être interrompue sans impact critique.

GFS (Grandfather-Father-Son) : Le GFS est une stratégie de rétention des sauvegardes basée sur plusieurs niveaux temporels. Cette méthode permet de conserver un historique sur le long terme.

Full (Sauvegarde complète) : Une sauvegarde complète consiste à copier l'intégralité des données sélectionnées à chaque exécution. Elle facilite la restauration mais nécessite plus de temps et d'espace de stockage.

Incrémental (Sauvegarde incrémentale) : Une sauvegarde incrémentale ne copie que les données modifiées depuis la dernière sauvegarde (complète ou incrémentale). Elle est plus rapide et consomme moins d'espace, mais la restauration peut nécessiter plusieurs fichiers de sauvegarde.

Sauvegarde différentielle (Differential Backup) : Une sauvegarde différentielle copie toutes les données modifiées depuis la dernière sauvegarde complète. Elle est plus rapide qu'une sauvegarde complète mais plus volumineuse qu'une incrémentale. La restauration nécessite uniquement la dernière sauvegarde complète et la dernière différentielle.

Backup Copy : Un Backup Copy est un type de job qui permet de copier automatiquement des sauvegardes existantes vers un autre emplacement (souvent distant). Il est utilisé pour renforcer la sécurité des données.

Repository (Dépôt de sauvegarde) : Un repository est l'emplacement de stockage où sont conservés les fichiers de sauvegarde. Il peut être local (disque, NAS) ou distant (site secondaire, cloud).

Job de sauvegarde (Backup Job) : Un job de sauvegarde est une tâche planifiée ou manuelle qui définit quelles données sont sauvegardées, à quelle fréquence et vers quel dépôt.

La règle 3-2-1 : Est une bonne pratique essentielle en matière de sauvegarde des données. Elle consiste à conserver trois copies des données, dont l'originale et deux sauvegardes, afin de limiter les risques de perte. Ces copies doivent être stockées sur au moins deux supports différents (par exemple un serveur local et un stockage externe), pour se prémunir contre les pannes matérielles. Enfin, une copie doit être conservée hors site, comme dans le cloud ou sur un site distant, afin de protéger les données contre des sinistres majeurs (incendie, vol, cyberattaque).

5.3. Annexe 3 : Plan d'adressage IP

5.3.1. Site de Paris

VLAN 10

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.10.252	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-01 VLAN 10
FW-P-01	172.16.10.253	255.255.255.0	172.16.10.0	172.16.10.254	IP FW-P-02 VLAN 10
CARP Firewall	172.16.10.254	255.255.255.0	172.16.10.0	172.16.10.254	Passerelle du VLAN 10

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.10.100-150	172.16.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Paris

VLAN 20

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
B-P-WIFI	172.16.20.50	255.255.255.0	172.16.20.0	172.16.20.254	Administration borne Wifi
FW-P-02	172.16.20.252	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-02 VLAN 20
FW-P-01	172.16.20.253	255.255.255.0	172.16.20.0	172.16.20.254	IP FW-P-01 VLAN 20
CARP Firewall	172.16.20.254	255.255.255.0	172.16.20.0	172.16.20.254	Passerelle du VLAN 20

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.20.100-150	172.16.20.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Employés

VLAN 21

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.21.252	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-02 VLAN 21
FW-P-01	172.16.21.253	255.255.255.0	172.16.21.0	172.16.21.254	IP FW-P-01 VLAN 21
CARP Firewall	172.16.21.254	255.255.255.0	172.16.21.0	172.16.21.254	Passerelle du VLAN 21

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.21.100-150	172.16.21.254	172.16.30.10	172.16.30.20	Plage DHCP WIFI Invité

VLAN 30

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-DC01	172.16.30.10	255.255.255.0	172.16.30.0	172.16.30.254	DC 1
SRV-P-DC02	172.16.30.20	255.255.255.0	172.16.30.0	172.16.30.254	DC 2
SRV-P-DFS01	172.16.30.50	255.255.255.0	172.16.30.0	172.16.30.254	DFS01
SRV-P-FOG01	172.16.30.11	255.255.255.0	172.16.30.0	172.16.30.254	Fog
SRV-P-OCS01	172.16.30.13	255.255.255.0	172.16.30.0	172.16.30.254	OCS Inventory
SRV-P-GLPI01	172.16.30.14	255.255.255.0	172.16.30.0	172.16.30.254	GLPI
SRV-P-BCK01	172.16.30.15	255.255.255.0	172.16.30.0	172.16.30.254	Veeam
SRV-P-CLOUD01	172.16.30.16	255.255.255.0	172.16.30.0	172.16.30.254	Nextcloud
SRV-P-RSAT-T0	172.16.30.30	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T0
SRV-P-RSAT-T1	172.16.30.31	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T1
SRV-P-RSAT-T2	172.16.30.32	255.255.255.0	172.16.30.0	172.16.30.254	RSAT T2
SRV-P-EDR01	172.16.30.19	255.255.255.0	172.16.30.0	172.16.30.254	EDR
SRV-P-ANS01	172.16.30.21	255.255.255.0	172.16.30.0	172.16.30.254	Ansible Lille
SRV-P-NETBOX01	172.16.30.22	255.255.255.0	172.16.30.0	172.16.30.254	Outil d'infrastructure
SRV-P-POL01	172.16.30.25	255.255.255.0	172.16.30.0	172.16.30.254	Centreon Poller
FW-P-02	172.16.30.252	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-02 VLAN 30
FW-P-01	172.16.30.253	255.255.255.0	172.16.30.0	172.16.30.254	IP FW-P-01 VLAN 30
CARP Firewall	172.16.30.254	255.255.255.0	172.16.30.0	172.16.30.254	Passerelle du VLAN 30

VLAN 40

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-02	172.16.40.252	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-02 VLAN 40
FW-P-01	172.16.40.253	255.255.255.0	172.16.40.0	172.16.40.254	IP FW-P-01 VLAN 40
CARP Firewall	172.16.40.254	255.255.255.0	172.16.40.0	172.16.40.254	Passerelle du VLAN 40

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.16.40.100-150	172.16.40.254	172.16.30.10	172.16.30.20	Plage DHCP Déploiement

VLAN 50

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SW-P-01	172.16.50.1	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 1 Paris
SW-P-02	172.16.50.2	255.255.255.0	172.16.50.0	172.16.50.254	VLAN 50 Switch 2 Paris
SRV-P-ESXI01	172.16.50.10	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
SRV-P-ESXI02	172.16.50.20	255.255.255.0	172.16.50.0	172.16.50.254	IP d'administration hyperviseur
PAW-P-T0	172.16.50.50	255.255.255.0	172.16.50.0	172.16.50.254	Machine d'administration
FW-P-02	172.16.50.252	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-02 VLAN 50
FW-P-01	172.16.50.253	255.255.255.0	172.16.50.0	172.16.50.254	IP FW-P-01 VLAN 50
CARP Firewall	172.16.50.254	255.255.255.0	172.16.50.0	172.16.50.254	Passerelle du VLAN 50

VLAN 60

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-P-01	172.16.60.1	255.255.255.252	172.16.60.0	-	IP FW-P-01 VLAN 60
FW-P-02	172.16.60.2	255.255.255.252	172.16.60.0	-	IP FW-P-02 VLAN 60

VLAN 99

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
SRV-P-HAProxy	172.16.99.10	255.255.255.0	172.16.99.0	172.16.99.254	HAProxy
FW-P-02	172.16.99.252	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-02 VLAN 99
FW-P-01	172.16.99.253	255.255.255.0	172.16.99.0	172.16.99.254	IP FW-P-01 VLAN 99
CARP Firewall	172.16.99.254	255.255.255.0	172.16.99.0	172.16.99.254	Passerelle du VLAN 99

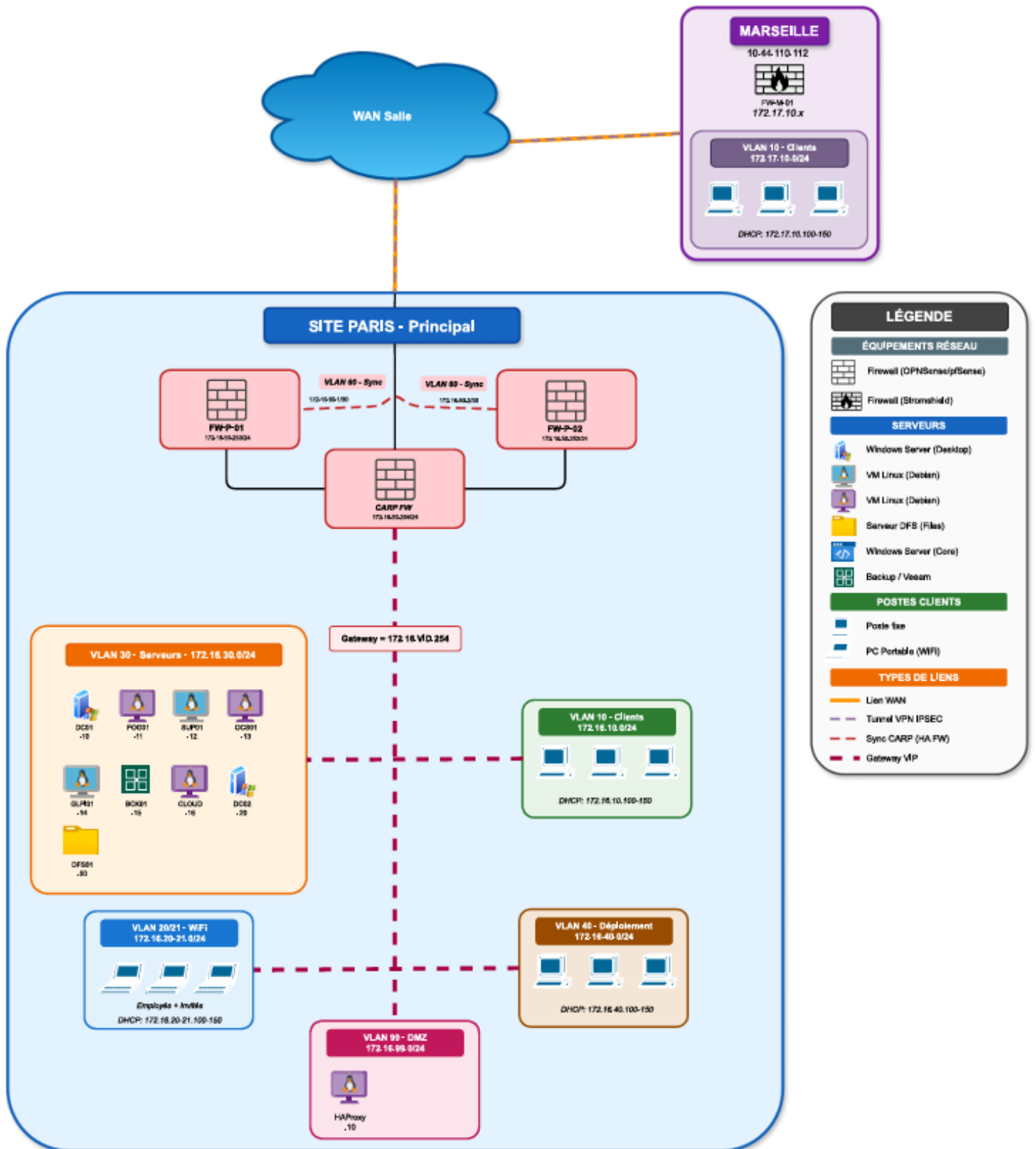
5.3.2. Site Marseille

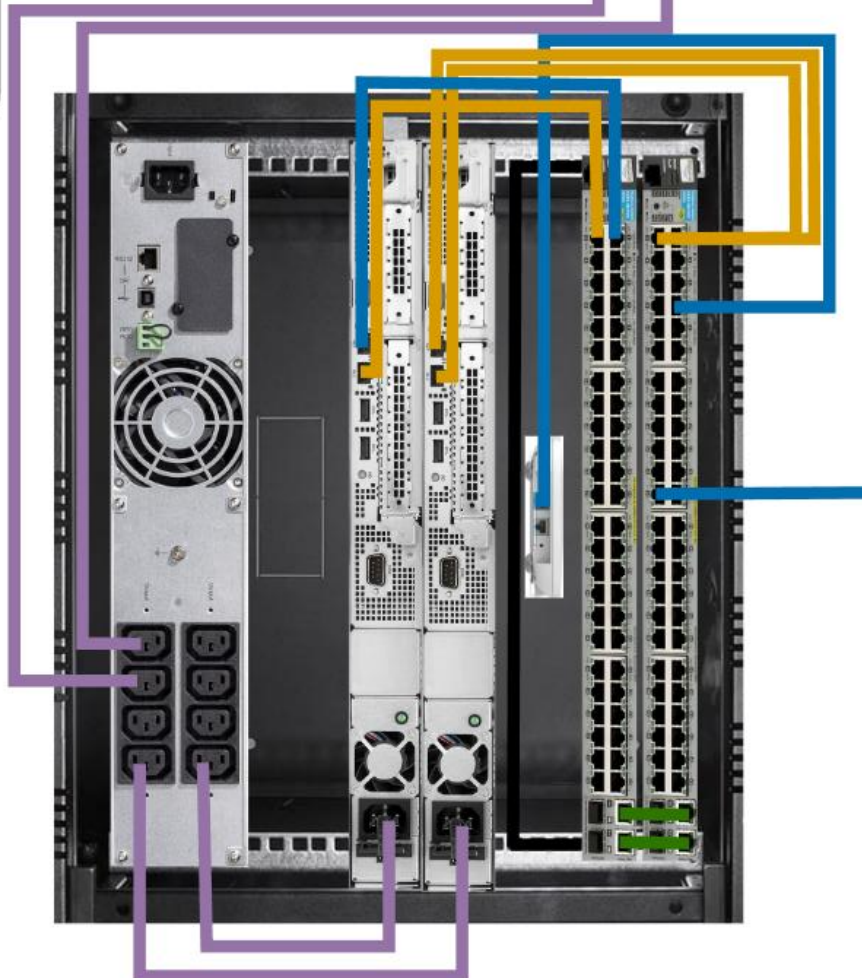
Marseille

Nom Machine	IP	MSR	Adresse Réseau	Passerelle	Description
FW-M-01	172.17.10.254	255.255.255.0	172.17.10.0	172.17.10.254	IP FW-M-01 VLAN 10 Marseille
FW-M-01	10.44.110.112	255.255.255.0	10.44.110.0	10.44.110.254	IP WAN Marseille

DHCP	Plage	Passerelle	DNS1	DNS2	Description
	172.17.10.100-150	172.17.10.254	172.16.30.10	172.16.30.20	Plage DHCP Client Marseille

5.4. Annexe 4 : Schéma logique de l'ensemble de l'infrastructure d'OASIS et physique du site de Paris





LEGENDE

Liaison Infrastructure

- Lien WAN Principal
- Aggrégation de liens
- Lien Borne WiFi
- Lien ESX101
- Lien ESX102
- Câble d'alimentation