Plan de Reprise d'Activité

Veeam Backup & Replication v13

Infrastructure VMware ESXi - Site principal / Site de secours

Dylan Pockot

Version 1.0 - Mars 2026

Glossaire et définitions

Ce document emploie des termes techniques dont la maîtrise est indispensable à la compréhension du Plan de Reprise d'Activité. Les définitions suivantes sont données dans leur contexte informatique.

- **RPO (Recovery Point Objective) - Objectif de point de reprise :** Désigne la durée maximale de perte de données tolérée en cas de sinistre. Un RPO de 2 heures signifie que le système peut perdre au maximum 2 heures de transactions

- **RTO (Recovery Time Objective) - Objectif de durée de reprise :** Durée maximale acceptable pour remettre un service en production après un incident. Un RTO de 4 heures signifie que le service doit redevenir opérationnel dans les 4 heures suivant la déclaration du sinistre.

- **PRA (Plan de Reprise d'Activité) :** Ensemble des procédures et ressources techniques destinés à redémarrer le Système d'Information après un sinistre majeur (incendie, ransomware, panne matérielle critique). À distinguer du PCA (Plan de Continuité d'Activité) qui vise à maintenir le service sans interruption.

- **PCA (Plan de Continuité d'Activité) :** Stratégie visant à maintenir la disponibilité des services sans coupure, même en cas de défaillance partielle. Le PCA inclut la haute disponibilité (clustering, CARP) tandis que le PRA intègre les scénarios de reprise après arrêt.

- **ERP (Enterprise Resource Planning) - Progiciel de gestion intégré :** Logiciel centralisant la gestion des processus métier d'une entreprise (finances, RH, achats, logistique). Dans le contexte d'un PRA, l'ERP est classé Tier 1 (service critique) car son indisponibilité paralyse l'activité opérationnelle.

- **CRM (Customer Relationship Management) - Gestion de la relation client :** Application métier centralisant les interactions avec les clients (Salesforce, Dynamics, Dolibarr, etc.). Classé Tier 1 pour les entreprises dont l'activité commerciale dépend de la disponibilité en temps réel de la base clients.

- **Ransomware :** Logiciel malveillant chiffrant les fichiers et données d'une organisation, rendant le Système d'Information inutilisable jusqu'au paiement d'une rançon. L'immutabilité des sauvegardes et l'isolation réseau du repository constituent les contre-mesures principales.

- **Air-gapé :** Isolation physique ou logique d'un système de sauvegarde vis-à-vis du réseau de production. Une copie air-gapée ne peut être atteinte par un ransomware circulant sur le réseau. Cette isolation peut être réalisée par déconnexion physique, VLAN dédié ou stockage hors ligne.
- **Immutabilité :** Propriété d'une donnée qui ne peut être modifiée ni supprimée pendant une période définie. Veeam implémente l'immutabilité via le système

de fichiers ReFS sur Windows ou XFS avec l'option Object Lock sur Linux. Indispensable pour résister aux ransomwares.

- **Failover :** Basculement automatique ou manuel de la charge de travail depuis le site principal vers le site de secours. Dans Veeam, le Failover démarre les VM réplicas sur l'ESXi secondaire.

- **Failback :** Opération inverse du Failover : resynchronisation des données accumulées sur le site de secours vers le site principal, puis redémarrage de la production sur l'infrastructure d'origine.

- **ReFS (Resilient File System) :** Système de fichiers Microsoft conçu pour la résilience aux corruptions. Utilisé comme repository Veeam, il permet les blocs FastClone (sauvegardes synthétiques instant), l'immutabilité native et la détection automatique des erreurs de données.

- **CARP (Common Address Redundancy Protocol) :** Protocole pfSense de rédondance de passerelle. Deux pare-feux partagent une adresse IP virtuelle (VIP). En cas de défaillance du Master, le Backup prend automatiquement la VIP sans interruption de service.

- **VSS (Volume Shadow Copy Service) :** Service Windows qui fige de manière transactionnelle les bases de données des applications (Active Directory, SQL Server, Exchange) avant que Veeam effectue un snapshot. Garantit la cohérence applicative des sauvegardes.

- **Thin Provisioning :** Technique d'allocation dynamique de l'espace disque : la machine virtuelle ne consomme sur le datastore que l'espace réellement utilisé, même si un disque de 100 Go a été déclaré.

- **Thick Provisioning :** Allocation statique : l'ESXi réserve immédiatement l'intégralité de l'espace déclaré sur le datastore, garantissant la disponibilité de cet espace quoi qu'il arrive.

- **FQDN (Fully Qualified Domain Name) :** Nom de domaine complet d'un hôte, incluant son nom propre et le domaine. Exemple : veeam.lab.local où "veeam" est le nom de la machine et "lab.local" le domaine DNS.

- **PoC (Proof of Concept) :** Démonstration technique en environnement de laboratoire visant à valider la faisabilité d'une solution avant son déploiement en production.

1. Introduction et objectifs

Dans un contexte de recrudescence des cyberattaques, la mise en place d'une stratégie de sauvegarde robuste est devenue une priorité absolue.

Ce projet naît de la volonté de concevoir une infrastructure capable de résister aux ransomwares, dont les conséquences peuvent être dévastatrices pour toute organisation.

Pour ce projet, mon choix s'est porté sur Veeam Backup & Replication v13.

Contrairement à d'autres solutions, Veeam offre une accessibilité immédiate grâce à sa version "Community Edition", facilitant son déploiement en environnement de test. Au-delà de sa facilité de téléchargement, c'est sa réputation de fiabilité et sa position de leader sur le marché (utilisé par plus de 80 % des entreprises du Fortune 500) qui ont motivé ce choix.

Ses fonctionnalités natives d'immutabilité sont aujourd'hui une réponse technique efficace contre le ransomware.

L'implémentation de cette solution s'inscrit directement dans mon cursus académique. Elle me permet de maîtriser des concepts critiques tels que la Haute Disponibilité et la continuité de service.

En assurant la protection des données, je valide ma capacité à sécuriser les actifs les plus précieux d'une entreprise tout en garantissant un redémarrage rapide des services en cas d'incident majeur.

Ce document décrit la conception, le déploiement et la validation d'un Plan de Reprise d'Activité (PRA) basé sur Veeam Backup & Replication v13, implémenté sur une infrastructure de virtualisation VMware ESXi en environnement de laboratoire.

L'objectif : Garantir la capacité à redémarrer l'ensemble des services critiques en moins de 10 minutes après un sinistre majeur, via la réplication des machines virtuelles sur un site de secours dédié.

Ce projet illustre les compétences suivantes : virtualisation VMware ESXi, gestion des réseaux virtuels (VLAN, pfSense, CARP), sauvegarde et réplication avec Veeam, et application des principes de cybersécurité.

2. Principes fondamentaux du PRA

2.1. La règle 3-2-1-1-0 (standard Veeam 2026)

Dans le cadre de ce laboratoire, l'objectif était de tendre vers ce standard industriel.

Voici l'analyse des cases cochées dans ce projet :

- **3 copies** : [COCHÉ] La production (ESXi 1) et la réplique (ESXi 2) sont actives.

Une troisième copie sous forme de fichier de sauvegarde est stockée sur le disque ReFS dédié.

- **2 supports** : [NON COCHÉ] Par contrainte technique, les copies restent sur des disques virtuels.

En production, il faudrait ajouter un stockage NAS ou Cloud S3 (Simple Storage Service) : service de stockage Cloud.

- **1 hors-site** : [COCHÉ] La réplication entre deux hôtes ESXi physiques distincts simule la déportation des données sur un site secondaire.

- **1 immuable** : [NON COCHÉ] Les sauvegardes ne sont pas verrouillées contre l'effacement. L'évolution logique serait l'ajout d'un Hardened Repository Linux.

- **0 erreur** : [COCHÉ] Ce critère est validé par les tests de basculement manuels (Failover) et les rapports de succès des jobs Veeam.

2.2. Autres principes de sécurité

- Séparation stricte entre l'infrastructure de sauvegarde et les réseaux de production (VLAN dédié, comptes de service isolés).

- Principe du moindre privilège : chaque compte technique ne dispose que des droits strictement nécessaires à son rôle.

- Authentification multi-facteurs (MFA) sur tous les accès d'administration.

- Immutabilité et chiffrement des sauvegardes pour garantir leur intégrité.

- Tests PRA semestriels ou annuels pour s'assurer de la validité opérationnelle du plan.

3. Architecture de l'infrastructure

3.1. Topologie réseau et segmentation VLAN - pfSense CARP

L'infrastructure repose sur deux nœuds pfSense (Master et Backup) configurables en haute disponibilité via le protocole CARP.

Chaque nœud expose une adresse IP virtuelle (VIP) par VLAN : en cas de défaillance du Master, le Backup prend instantanément la VIP sans interruption de service pour les postes clients.

Interface	Port Group	pfSense-A (Master)	pfSense-B (Backup)	VIP CARP	Justification
WAN	DMZ-WAN	DHCP	DHCP	Aucune	Accès Internet via vSwitch0
LAN-MGMT	LAN-MGMT	192.168.1.251	192.168.1.252	192.168.1.254	Gestion & Serveurs (VLAN 10)
LAN-CLIENT	LAN-CLIENT	192.168.2.251	192.168.2.252	192.168.2.254	Clients & Tests (VLAN 20)
IOT-VIDEO	IOT-VIDEO	172.16.0.251/22	172.16.0.252/22	172.16.0.254	Caméras IP (VLAN 30)
SYNC	PFSENSE-SYNC	10.0.0.1/30	10.0.0.2/30	Aucune	Synchro CARP (VLAN 99)

Justification des masques réseau adoptés :

- **Masque /22 pour le VLAN IOT-VIDEO (255.255.252.0) :** Ce masque adresse jusqu'à 1 022 hôtes, prévoyant l'extension du parc de caméras IP sans refonte du plan d'adressage.
- **Masque /30 pour le VLAN SYNC (255.255.255.252) :** Lien point-à-point entre les deux nœuds pfSense, limitant la surface d'attaque en n'autorisant que 2 hôtes sur ce segment de synchronisation CARP critique.

3.2. Inventaire des machines virtuelles

Le tableau suivant détaille l'ensemble des VM de l'infrastructure, leur rôle et leur adressage IP. La colonne FQDN (Fully Qualified Domain Name) indique l'enregistrement DNS associé à chaque service.

Nom de la VM	Système d'exploitation	Adresse IP	FQDN	Rôle / Service
SRV-AD-01	Windows Server 2022	192.168.1.10	ad01.lab.local	Contrôleur de Domaine / DNS
SRV-SUPERV	Debian 12	192.168.1.20	zabbix.lab.local	Supervision : Zabbix / Grafana

Nom de la VM	Système d'exploitation	Adresse IP	FQDN	Rôle / Service
SRV-GLPI	Ubuntu	192.168.1.21	glpi.lab.local	Gestion de parc
SRV-VIDEO	MotionEye (Linux)	172.16.0.27	video.lab.local	Vidéosurveillance (NVR)
CLI-WIN10	Windows 10	192.168.2.10	client01.lab.local	Poste de travail utilisateur
CLI-KALI	Kali Linux	192.168.2.50	kali.lab.local	Tests d'intrusion / Sécurité

3.3. Priorisation des VMs et niveaux de service (Tiering)

Toutes les machines virtuelles ne présentent pas le même niveau de criticité métier.

Une politique de réplication sélective a été appliquée : les ressources disponibles sur le site de secours ont été réservées aux services dont l'indisponibilité engendrerait un impact business immédiat.

Priorité	VM / Service	RPO cible	RTO cible	Stratégie
Tier 1 (Critique)	DC/AD, DNS/DHCP, ERP, CRM, pfSense, Veeam	15 min - 1 h	< 1 - 4 h	Réplication continue
Tier 2 (Important)	Web secondaires, messagerie, Zabbix/Grafana	1 - 4 h	4 - 12 h	Réplication si stockage
Tier 3 (Non critique)	NVR vidéo, VM de test/dev, archivage	> 4 h	> 24 h	Backup seul (Instant VM Recovery)

En raison des contraintes de stockage sur le site de secours, une politique de réplication sélective a été appliquée.

Les ressources ont été priorisées pour le Cœur de Réseau (pfSense) et les Services Communs (AD, DNS, Supervision). Les postes clients, étant non critiques et facilement redéployables par masterisation, ont été exclus du plan de réplication afin de garantir un espace disque suffisant aux snapshots de production.

4. Préparation de l'environnement

4.1. Configuration réseau de la VM Veeam

Le serveur Veeam Backup & Replication a été installé sur une machine virtuelle Windows Server hébergée sur l'ESXi 2 (site de secours). Son interface réseau a été rattachée au Port Group "DMZ-WAN" lui permettant de joindre les interfaces de gestion des deux ESXi pour orchestrer les transferts de données, tout en restant isolée des réseaux de production potentiellement compromis.

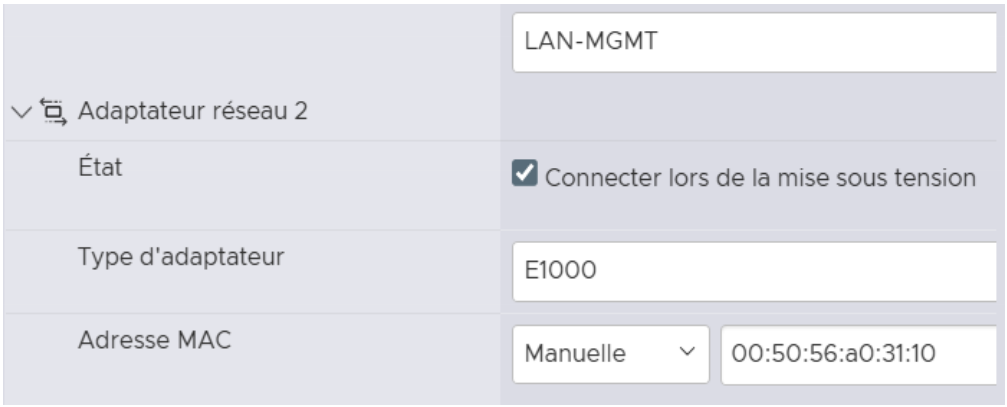

Figure 1 : Configuration de l'adaptateur réseau de la VM Veeam - rattachement au Port Group LAN-MGMT

Nom	Ports actifs	ID du VLAN ▲
DMZ-WAN	2	0
Management Network	1	0
LAN-MGMT	5	10
LAN-CLIENTS	2	11
IOT-VIDEO	2	30
SYNC	2	99

Figure 2 : Port Groups configurés sur l'ESXi de secours (VLANs 10, 11, 12, 30 et 99)

4.2. Préparation du stockage - Volume ReFS dédié

Afin de garantir la stabilité de l'hyperviseur de secours, une politique de réservation d'espace disque a été mise en place. Un disque virtuel de 100 Go en Thick Provisioning (allocation statique) a été ajouté à la VM Veeam via l'interface ESXi.

Ce disque a été formaté en système de fichiers ReFS avec une unité d'allocation de 64 Ko, configuration recommandée par Veeam pour activer les fonctionnalités de blocs FastClone et l'immutabilité native.

Cette isolation de 100 Go empêche toute saturation accidentelle du datastore global par les flux de sauvegarde, préservant ainsi la haute disponibilité des autres services virtuels. Les 200 Go restants sur le datastore constituent une marge de sécurité pour

la croissance des VM de production et les fichiers temporaires de snapshot.

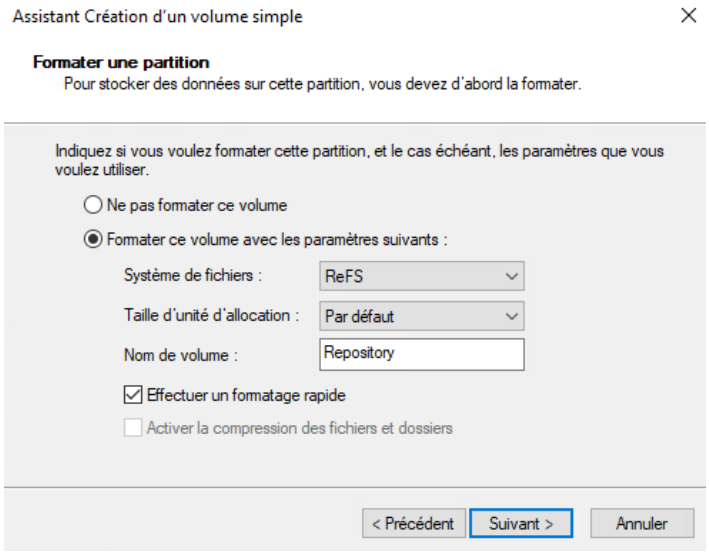

Figure 3 : Assistant Windows - formatage du volume en ReFS, nommé "Repository" pour le stockage Veeam

5. Installation de Veeam Backup & Replication v13

5.1. Prérequis et procédure d'installation

L'installation de Veeam Backup & Replication v13 nécessite les éléments suivants :

- Windows Server 2019 ou 2022 (64 bits) comme système hôte.
- ISO Veeam Backup & Replication (environ 15 Go), téléchargée depuis le portail officiel Veeam.
- Composants automatiquement installés : .NET Framework, Microsoft Visual C++ Redistributable, PostgreSQL (instance de base de données locale).
- Espace disque : minimum 10 Go pour l'installation, repository séparé sur le volume ReFS dédié.

La procédure d'installation en mode "Offline" a été choisie : l'ISO est importée dans le datastore de l'ESXi 2 et montée sur le lecteur CD virtuel de la VM. Cette approche garantit l'indépendance vis-à-vis de la connexion Internet du site de secours.

5.2. Configuration de la base de données

Lors de l'installation, Veeam crée une instance PostgreSQL locale pour stocker sa configuration (jobs, historique, métadonnées de réplication). L'option "Install new instance" a été retenue, ce qui permet à Veeam de gérer entièrement cette instance sans dépendance externe. L'authentification par compte Windows (Windows Authentication) a été préférée à l'authentification native PostgreSQL pour centraliser la gestion des accès.

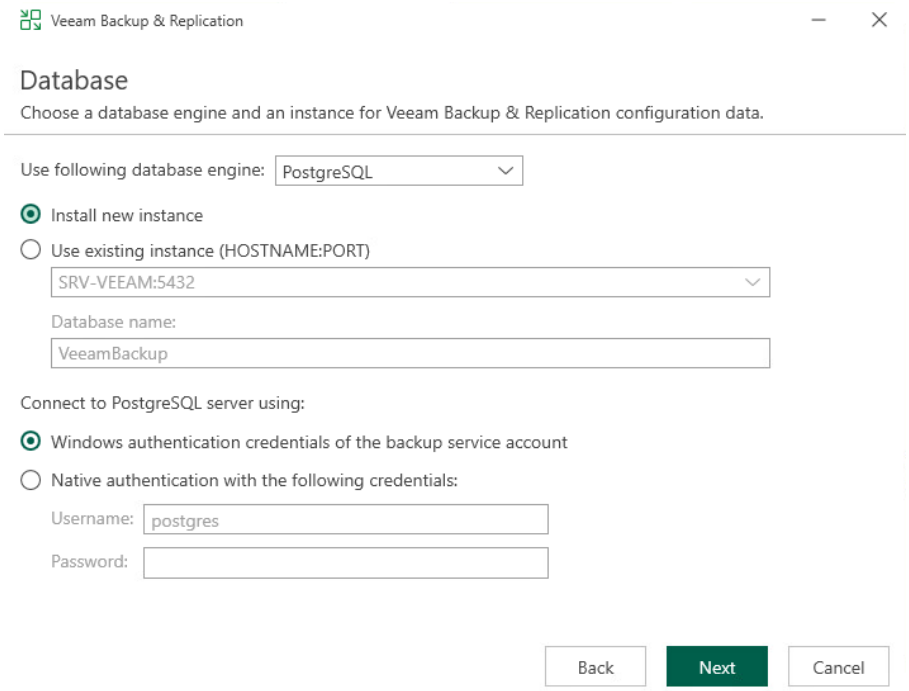

Figure 4 : Configuration de la base de données PostgreSQL lors de l'installation - instance locale sur SRV-VEEAM (port 5432)

6. Configuration de l'inventaire Veeam

6.1. Ajout des hôtes ESXi dans Veeam

La première étape de configuration consiste à déclarer les deux serveurs ESXi dans Veeam afin qu'il puisse interagir avec leur infrastructure de virtualisation : accéder aux disques virtuels pour la sauvegarde, créer des snapshots, et démarrer les réplicas lors d'un basculement.

La procédure consiste à naviguer vers l'onglet Inventory > Virtual Infrastructure, puis à effectuer un clic droit sur VMware vSphere > Add Server.

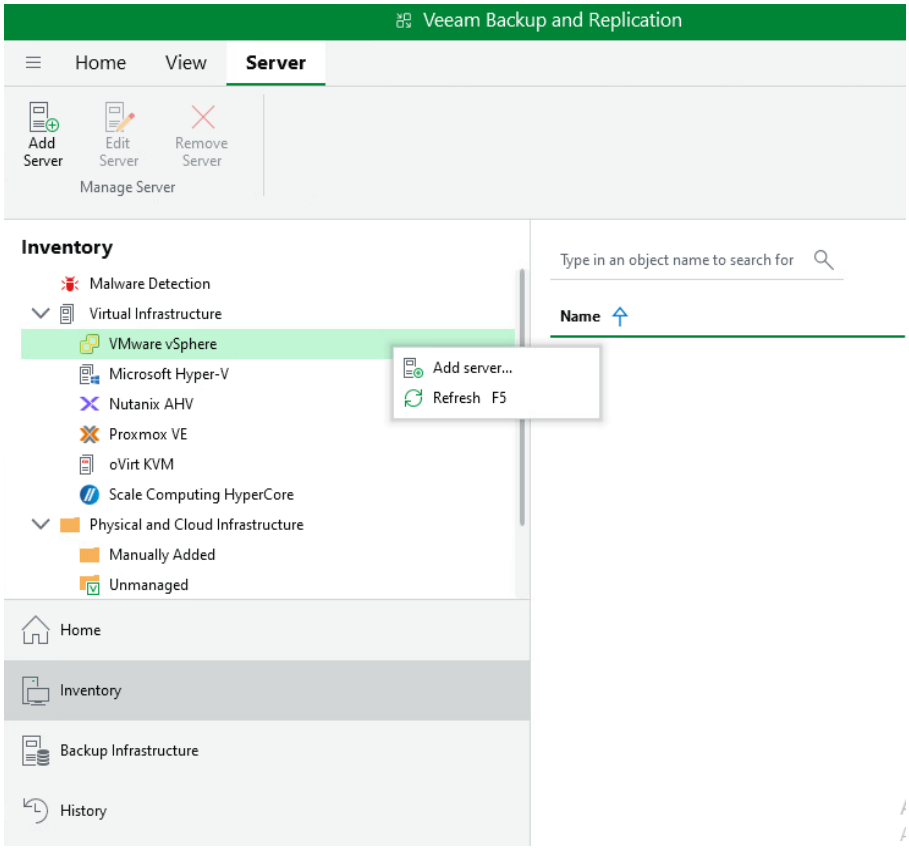

Figure 5 : Onglet Inventory de Veeam - accès au menu contextuel "Add Server" pour déclarer un hôte VMware

6.2. Ajout de l'ESXi de secours (20.0.0.42)

L'hôte de secours est le premier à être ajouté, car c'est sur ce serveur qu'est installé Veeam. Son adresse IP (20.0.0.42) et une description explicite sont renseignées pour faciliter l'identification dans les jobs.

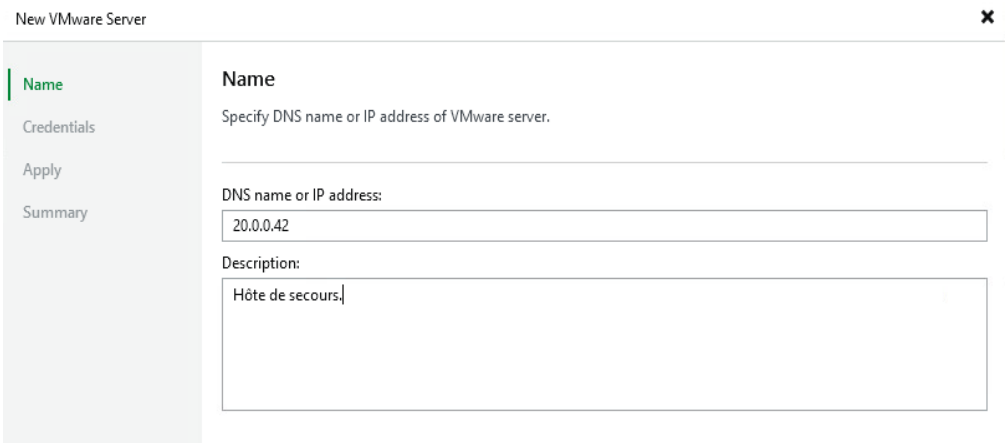

Figure 6 : Ajout de l'hôte ESXi de secours (20.0.0.42) dans l'inventaire Veeam avec sa description

Les identifiants administrateur de l'ESXi sont ensuite saisis. Le compte "root" est utilisé pour ce laboratoire ; en production, un compte de service dédié avec les droits minimaux nécessaires serait créé conformément au principe du moindre privilège.

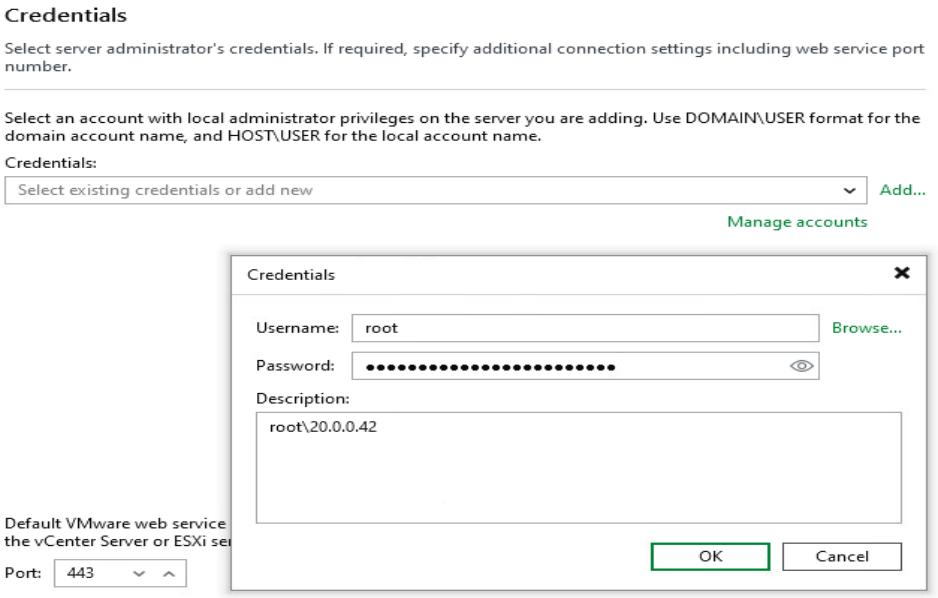

Figure 7 : Saisie des identifiants administrateur (compte root) pour l'hôte ESXi de secours

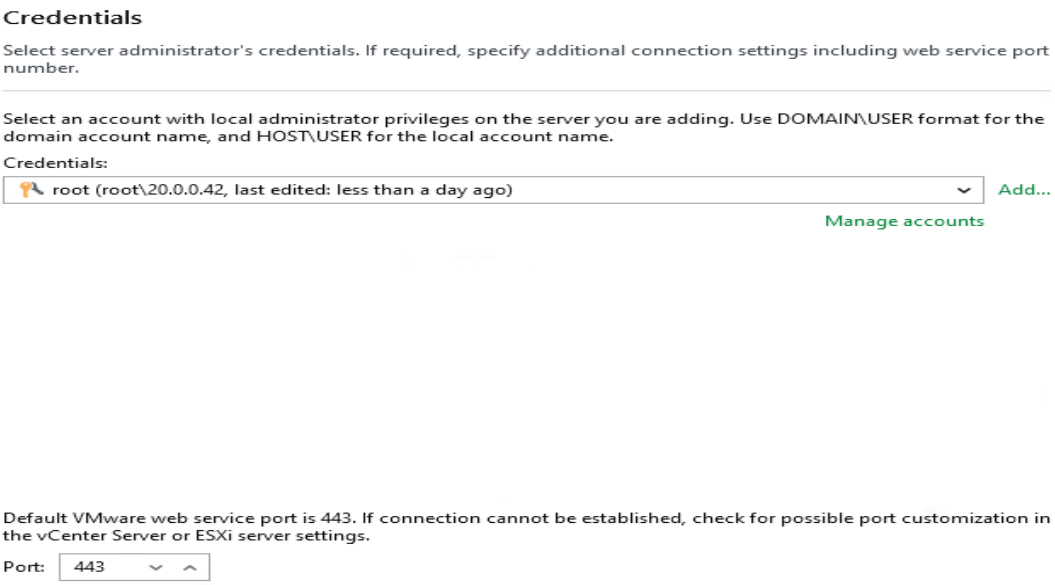

Figure 8 : Validation des credentials - sélection du compte root•0.0.42 dans la liste des crédentiels enregistrés

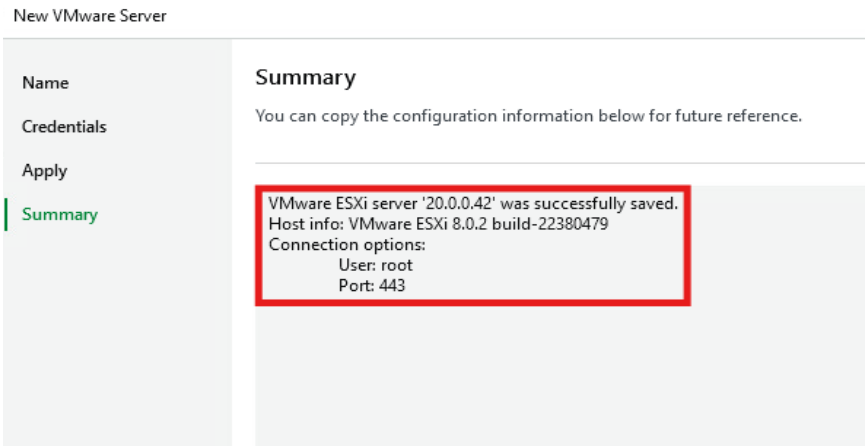

Figure 9 : Résumé de la connexion réussie à l'ESXi de secours - VMware ESXi 8.0.2 build 22380479, user root, port 443

6.3. Ajout de l'ESXi de production (20.0.0.43)

La même procédure est appliquée pour l'hôte de production. Les deux ESXi sont désormais visibles dans l'inventaire Veeam, ce qui permet de définir la source (ESXi 1) et la destination (ESXi 2) du job de réplication.

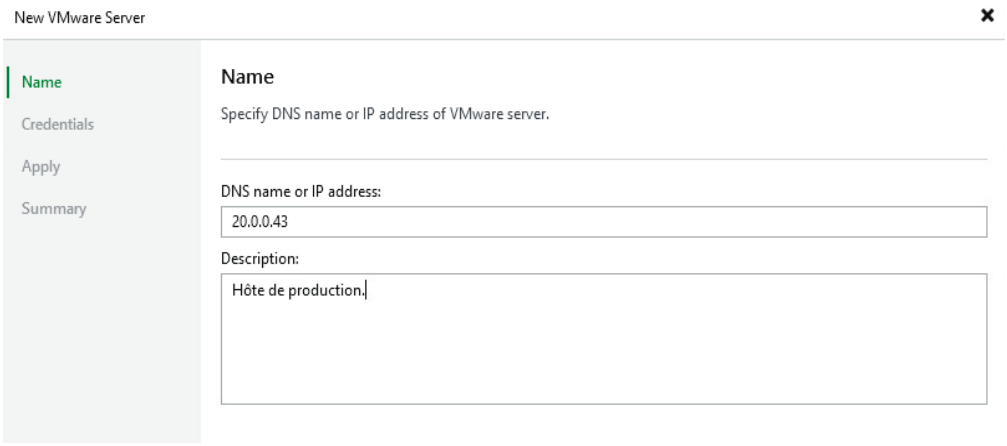

Figure 10 : Ajout de l'hôte ESXi de production (20.0.0.43) - paramétrage identique à l'hôte de secours

7. Création du job de réplication

Le job de réplication est le cœur du PRA. Il copie en continu les machines virtuelles critiques depuis le site de production (ESXi 1) vers le site de secours (ESXi 2), maintenant en permanence des réplicas prêts à être démarrés en cas de sinistre.

7.1. Création du job

Le job est créé depuis Home > Replication Job > Virtual Machine.

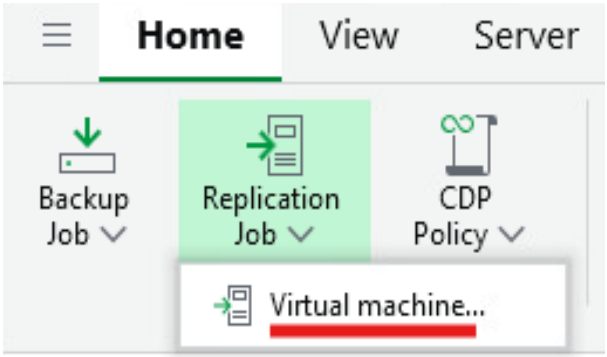

Figure 11 : Création d'un nouveau job de réplication depuis le menu Home de Veeam

7.2. Paramétrage du nom et des options avancées

Le job est nommé "Job_Replication_Critique". Les options avancées sont :

- **Network remapping (coché) :** Indispensable. Veeam doit confirmer explicitement la correspondance des cartes réseau virtuelles entre les deux ESXi, même si les Port Groups portent des noms identiques. Sans ce mapping, les VM réplicas pourraient démarrer en mode "déconnecté" sans accès réseau.

- **Replica seeding (non coché) :** Cette option est réservée aux environnements avec des To de données et une bande passante limitée (envoi d'un disque physique). Dans ce laboratoire, les deux ESXi sont sur le même réseau local.

- **Replica re-IP (non coché) :** Le PRA vise la transparence totale pour les services DNS et les applications. Les VM réplicas doivent conserver les mêmes adresses IP que les VM de production (.10, .20, .30, etc.).

- **High Priority (coché) :** Assure que ce job passe en premier si plusieurs jobs sont en file d'attente sur l'infrastructure Veeam. En entreprise, cette option est réservée aux VM ultra-critiques (DC, base de production).

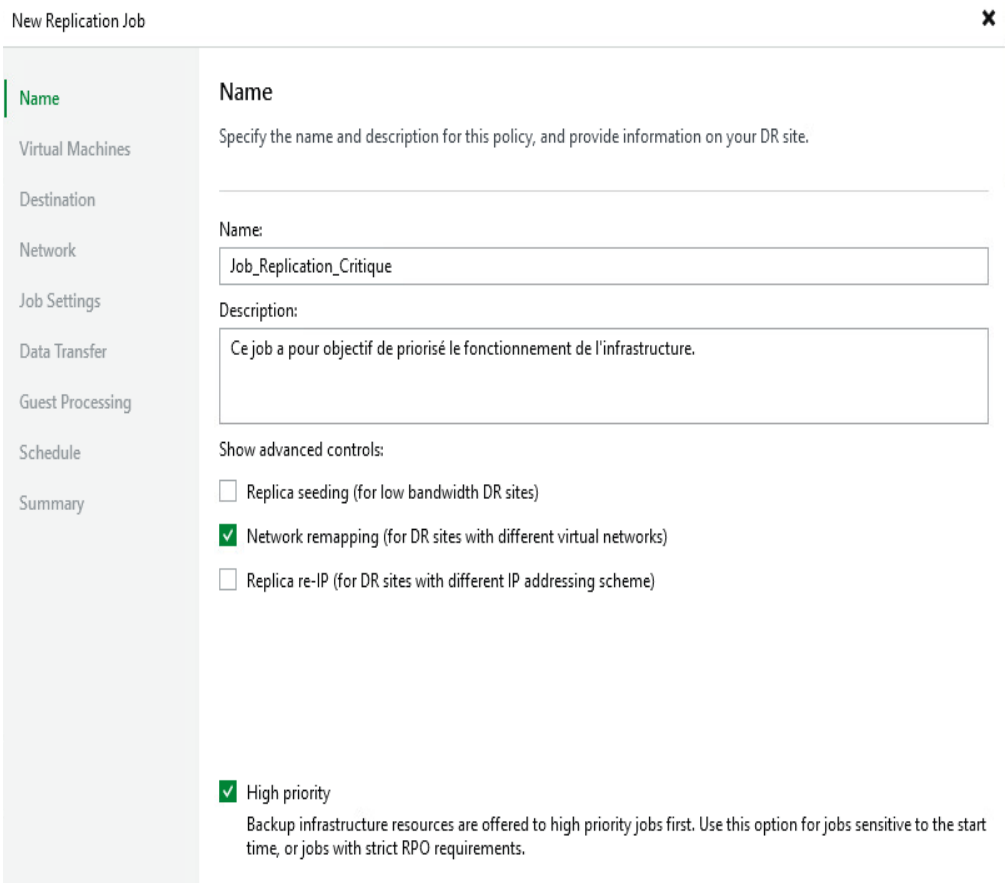

Figure 12 : Paramétrage du job de réplication - nom, description, Network remapping activé, High Priority coché

7.3. Sélection des machines virtuelles à répliquer

Conformément à la politique de réplication sélective (Tiering), seules les VM de niveau Tier 1 sont incluses dans ce job :

- pfSense-Master (7,50 Go) - Pare-feu et passerelle principale.
- pfSense-Backup (8,13 Go) - Pare-feu de secours (CARP).
- srv-ad (76,9 Go) - Contrôleur de domaine Active Directory et DNS.
- srv-debian (18,0 Go) - Serveur de supervision et d'applications (Zabbix, GLPI…). Services regroupés en 1 VM sur ce projet pour des raisons de stockage.

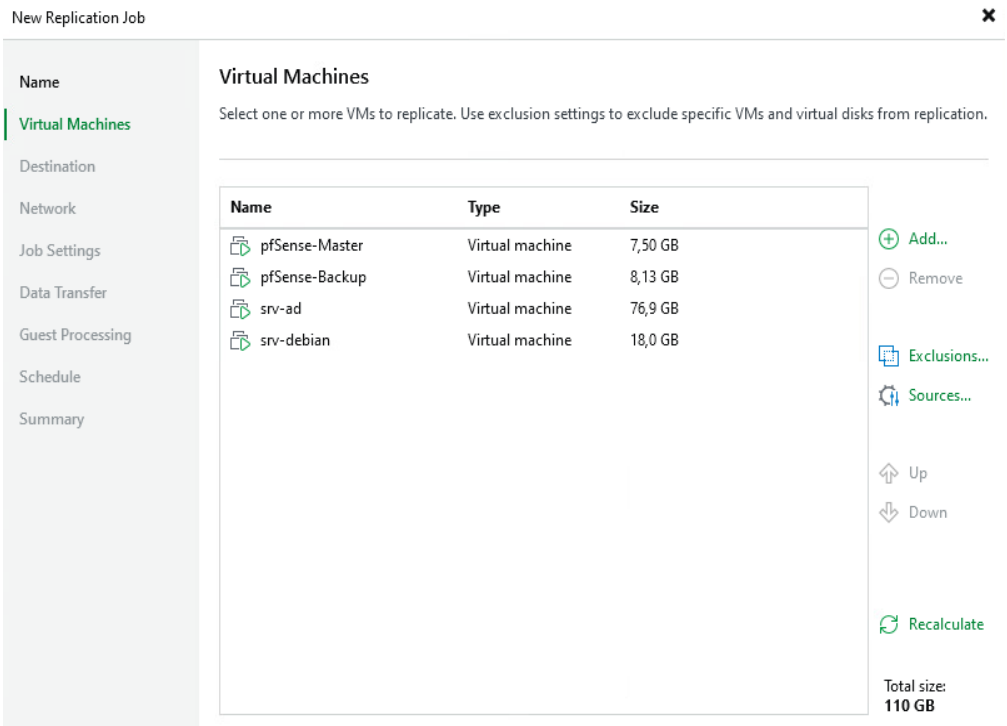

Figure 13 : Sélection des 4 machines virtuelles critiques à répliquer - taille totale : 110 Go

7.4. Network Mapping - correspondance des réseaux

Le Network Mapping garantit que chaque interface réseau des VM réplicas se connecte au bon Port Group sur l'ESXi de secours. La correspondance est ici identique car les Port Groups ont été créés avec les mêmes noms sur les deux ESXi, ce qui est une bonne pratique de standardisation.

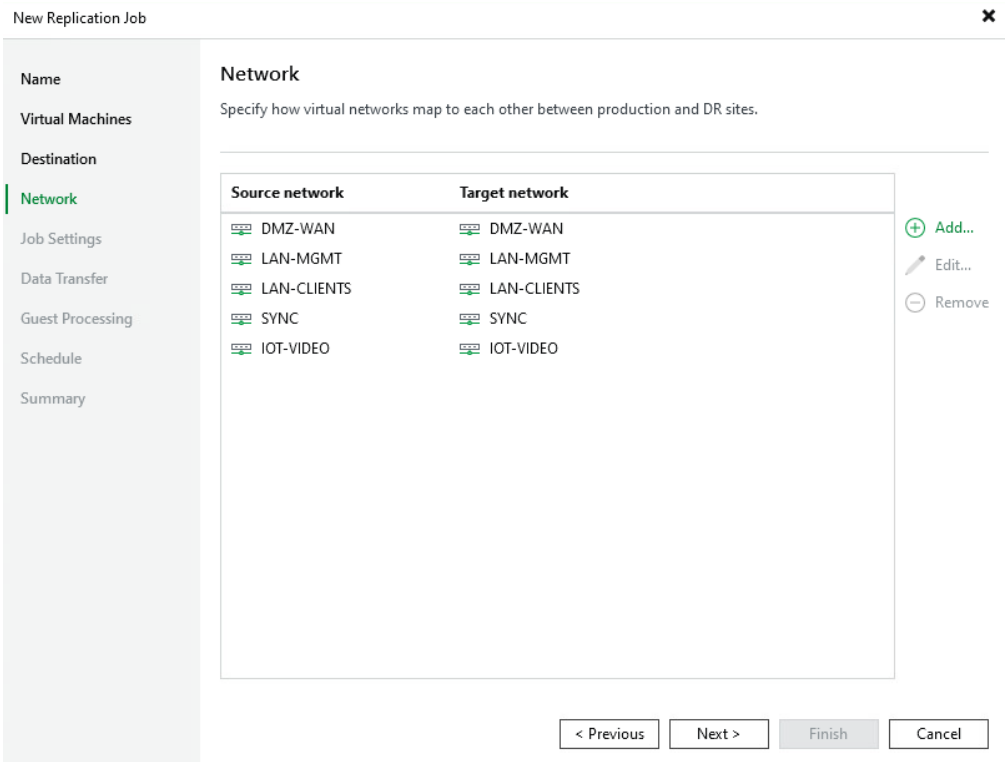

Figure 14 : Configuration du Network Mapping - correspondance 1:1 des Port Groups entre ESXi de production et de secours

7.5. Guest Processing - cohérence applicative (VSS)

L'Application-Aware Processing (via les **VSS** de Microsoft) garantit la cohérence transactionnelle des bases de données applicatives au moment du snapshot. Sans cette option, le snapshot du disque de l'Active Directory pourrait capturer la base NTDS.dit dans un état incomplet, générant des erreurs USN Rollback ou une corruption de base à la restauration.

En activant cette option, Veeam dialogue avec le service VSS de Windows pour "figer" proprement les bases de données (AD, SQL) avant la prise du snapshot, garantissant que le réplica redémarrera sans erreur d'intégrité.

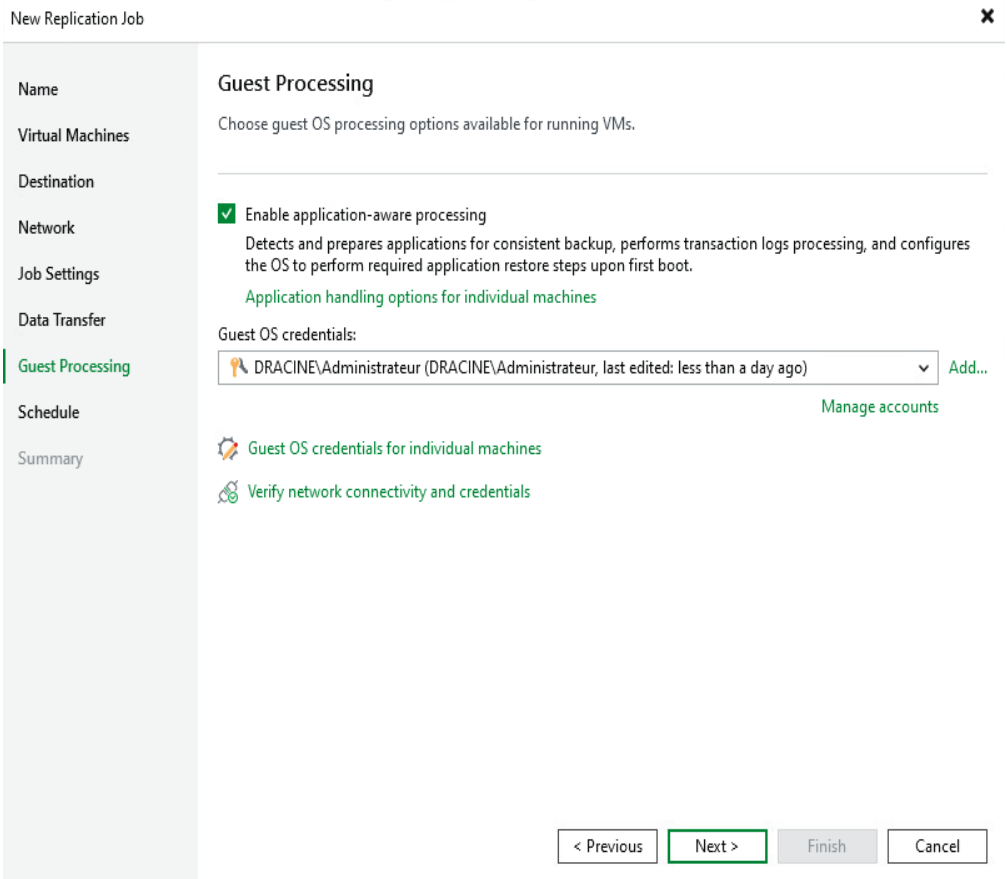

Figure 15 : Activation du Guest Processing (Application-Aware) avec les credentials du domaine DRACINE•Administrateur

Le test de connexion Guest Processing confirme que Veeam peut accéder à l'intérieur des VM Windows pour orchestrer les VSS. Dans ce lab, seul srv-ad est concerné (pfSense et srv-debian étant des systèmes non-Windows, sans service VSS).

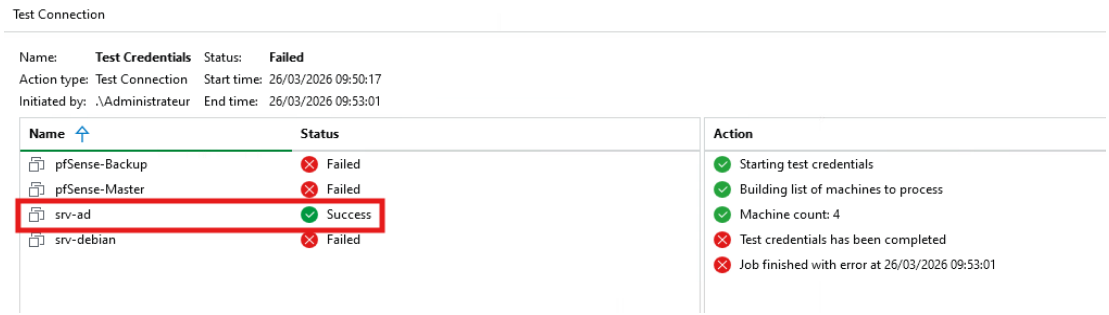

Figure 16 : Résultat du test Guest Processing - srv-ad en succès, pfSense et srv-debian en échec attendu (non-Windows)

7.6. Planification automatique du job

Le job est configuré pour s'exécuter automatiquement toutes les 2 heures. Ce paramétrage définit le RPO (Recovery Point Objective) du PRA : en cas de sinistre, la perte de données maximale est de 2 heures. En cas d'échec, Veeam effectue automatiquement 3 tentatives de relance avec un intervalle de 10 minutes entre chacune.

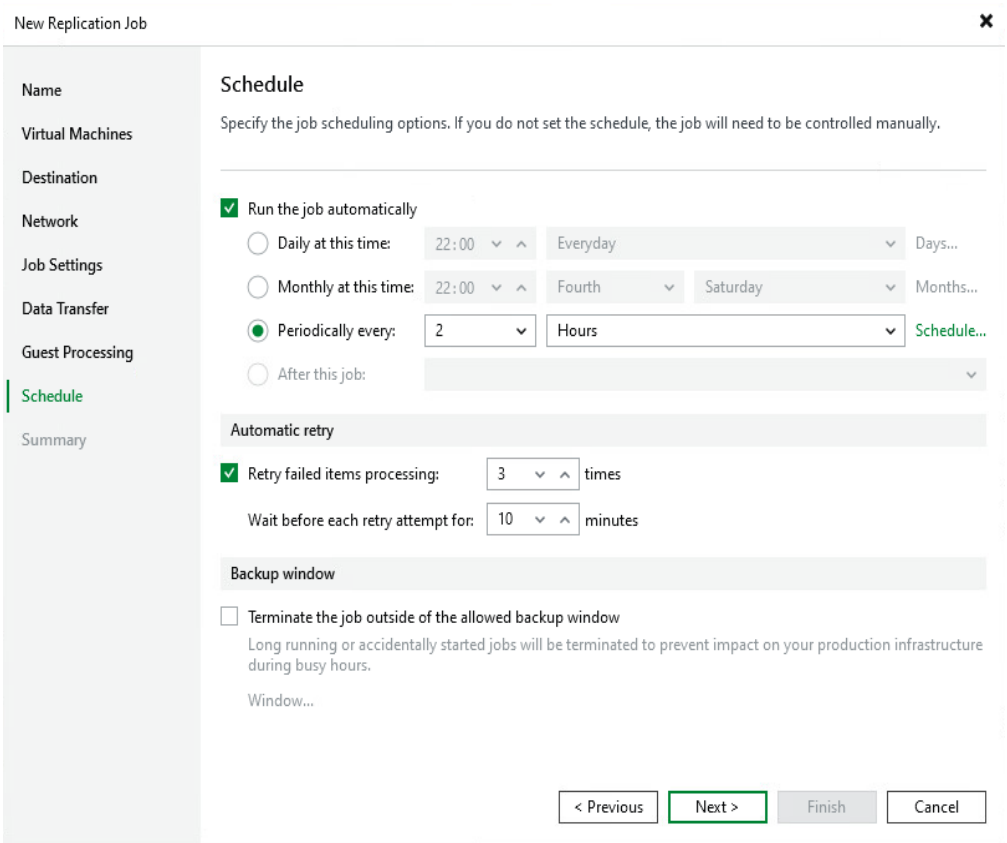

Figure 17 : Planification du job de réplication - exécution périodique toutes les 2 heures avec retry automatique (3 fois, délai 10 min)

8. Exécution et validation des sauvegardes

8.1. Sauvegarde complète initiale (Full Backup)

La stratégie de sauvegarde repose sur une Full Backup initiale suivie de sauvegardes incrémentielles quotidiennes. La Full Backup constitue la référence de base : elle copie l'intégralité des blocs de données de chaque VM vers le repository ReFS.

Cette opération est plus longue et plus consommatrice en bande passante, mais elle est nécessaire pour initialiser la chaîne de points de restauration.

La première exécution du job a traité 138,9 Go de données (4 VM) en 48 minutes 20 secondes, avec un taux de transfert de 42 MB/s. Les 4 VM ont été traitées avec succès (0 erreur, 0 avertissement).

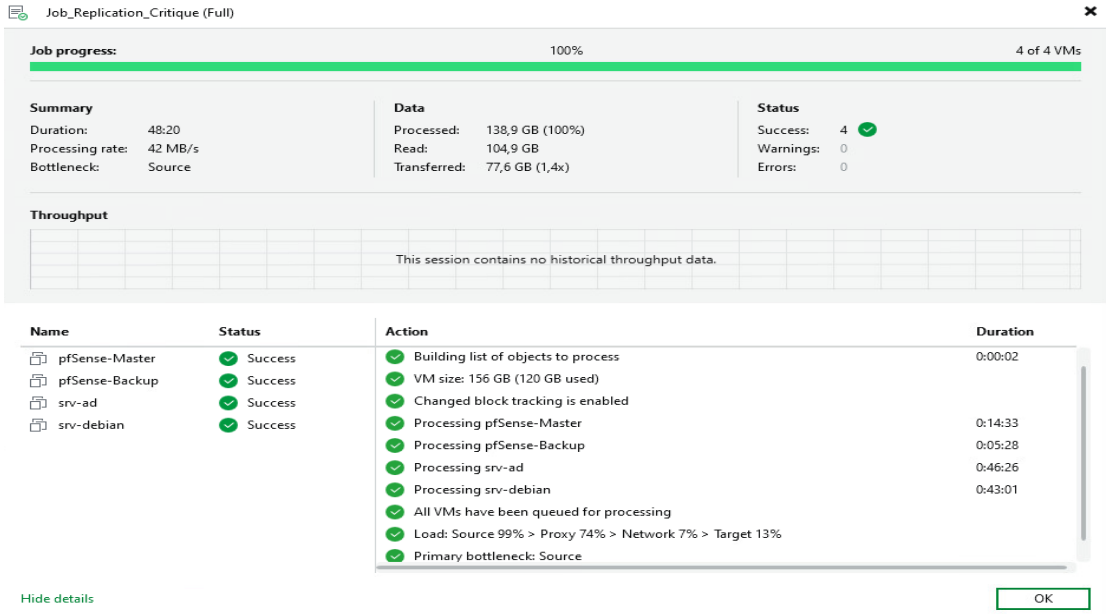

Figure 18 : Rapport de la sauvegarde complète initiale - 138,9 Go traités en 48 min, 4/4 VM en succès, taux 42 MB/s

8.2. Sauvegarde incrémentielle

Les sauvegardes incrémentielles suivantes ne transfèrent que les blocs modifiés depuis la dernière sauvegarde, grâce à la technologie CBT (Changed Block Tracking) de VMware.

La différence de performance est significative : 1,7 Go lus en 6 minutes 52 secondes, contre 138,9 Go pour la Full Backup. Cela réduit considérablement l'impact sur les performances de production et la fenêtre de sauvegarde.

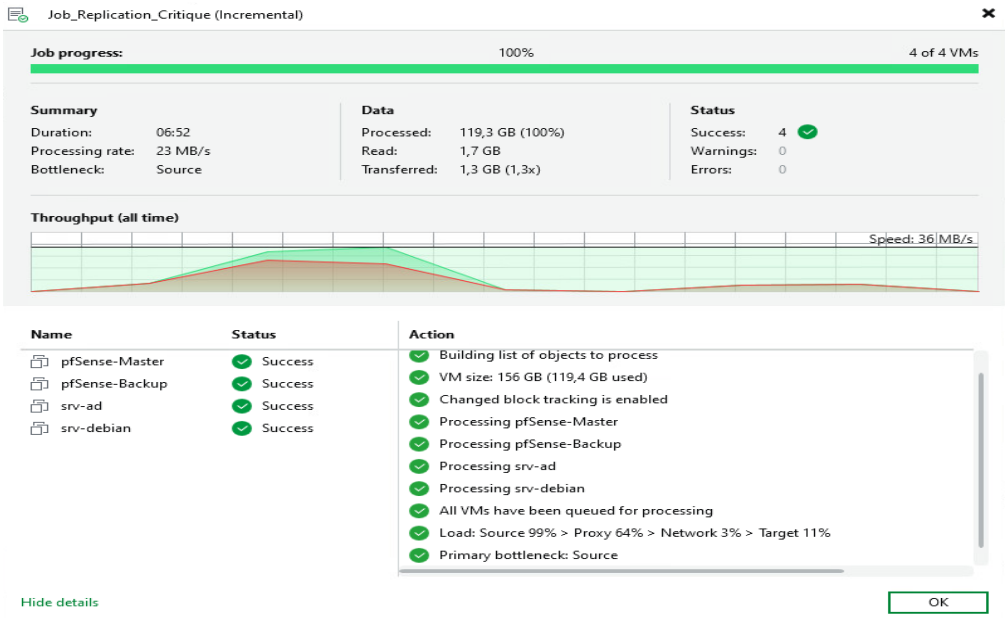

Figure 19 : Rapport de la sauvegarde incrémentielle - seulement 1,7 Go lus en 6 min 52 s grâce au Changed Block Tracking (CBT)

9. Test et validation du Failover (basculement)

9.1. Présentation du scénario

Ce test représente le scénario ultime du PRA : simuler une panne totale de l'ESXi de production (20.0.0.43) et démontrer que l'ensemble des services critiques peut être remis en ligne sur le site de secours (20.0.0.42) en moins de 10 minutes.

Dans le cadre de ce Proof of Concept (PoC) réalisé avec la version Community de Veeam, l'orchestration automatisée via Failover Plan n'a pas été déployée.

Le basculement a été validé par une procédure de Failover Manuel, respectant rigoureusement l'ordre de priorité des services.

9.2. Étape 1 - Nettoyage initial (Undo Failover)

Avant de déclencher le scénario de sinistre, un Undo Failover est effectué pour remettre l'environnement dans un état propre : les réplicas précédemment allumés pour tests sont éteints et leurs modifications temporaires supprimées. Les VM de production sur l'ESXi 1 restent les seules actives.

9.3. Étape 2 - Simulation du sinistre

L'ESXi de production (20.0.0.43) est éteint brutalement pour simuler une coupure d'alimentation ou une panne matérielle critique. Veeam détecte l'indisponibilité des VM sources.

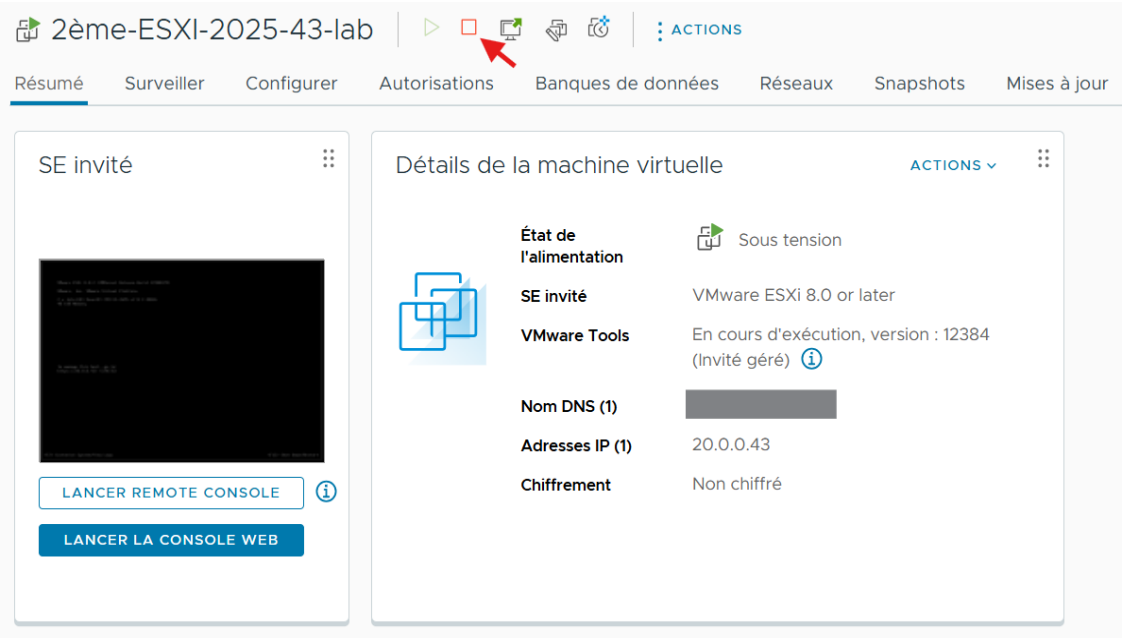

Figure 22 : Arrêt brutal de l'ESXi de production (20.0.0.43) via son interface web pour simuler le sinistre

Les réplicas disponibles sur l'ESXi de secours sont affichés dans Veeam avec le statut "Failover", confirmé que les données répliquées sont prêtes à être activées.

Figure 20 : Tableau de bord Veeam - 4 réplicas en statut "Failover" avec 2 points de restauration disponibles par VM

9.4. Étape 3 - Activation du PRA (Failover Now)

Le basculement est déclenché manuellement depuis Home > Replicas > Ready. L'ordre démarrage respecte la dépendance logique des services :

- **Priorité 1 - pfSense (réseau) :** Sans passerelle et pare-feu opérationnels, aucun autre service n'est joignable.
- **Priorité 2 - srv-ad (annuaire Active Directory) :** Le DC doit être disponible avant les applications métier pour permettre l'authentification.
- **Priorité 3 - srv-debian (applications/supervision) :** Zabbix, GLPI et les autres services applicatifs démarrent en dernier.

La raison du basculement est documentée dans l'interface Veeam pour traçabilité et audit.

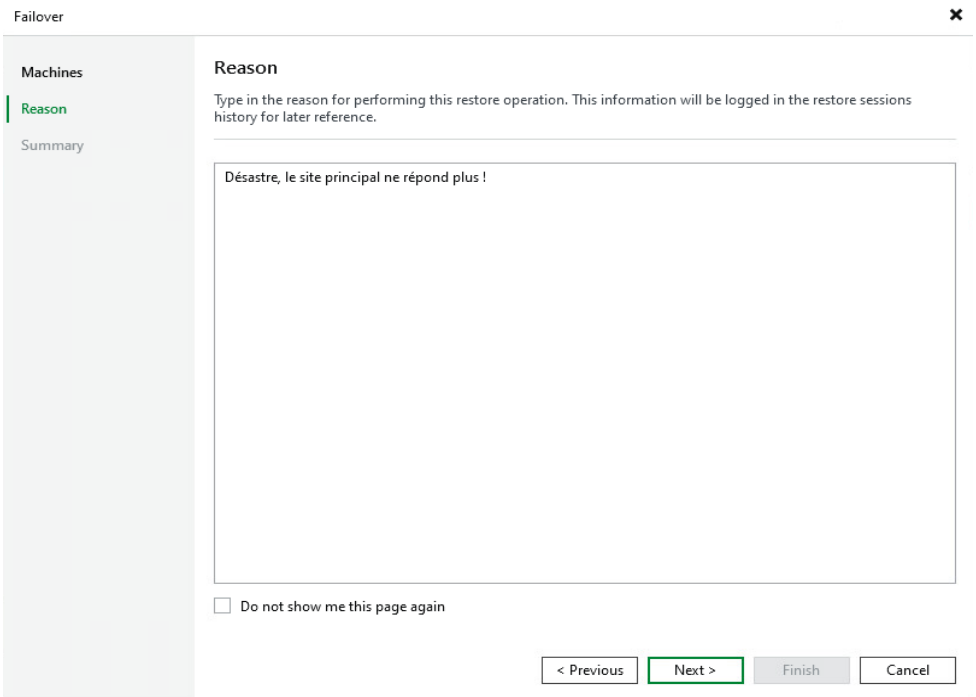

Figure 23 : Saisie de la raison du basculement dans l'assistant Failover - "Désastre, le site principal ne répond plus !"

9.5. Validation du PRA - services opérationnels sur le site de secours

Immédiatement après le Failover, les 4 VM réplicas sont allumées sur l'ESXi de secours (20.0.0.42).

Un test de connectivité réseau (ping vers 8.8.8.8) est exécuté depuis la console de pfSense-Master_replica pour confirmer que la passerelle Internet est opérationnelle.

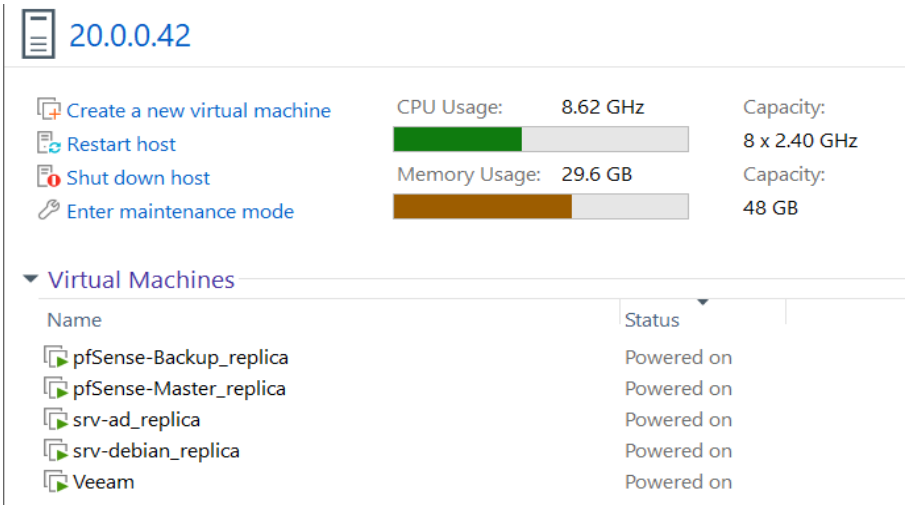

Figure 21 : ESXi de secours (20.0.0.42) - les 4 VM réplicas et Veeam sont démarrés et en cours d'exécution

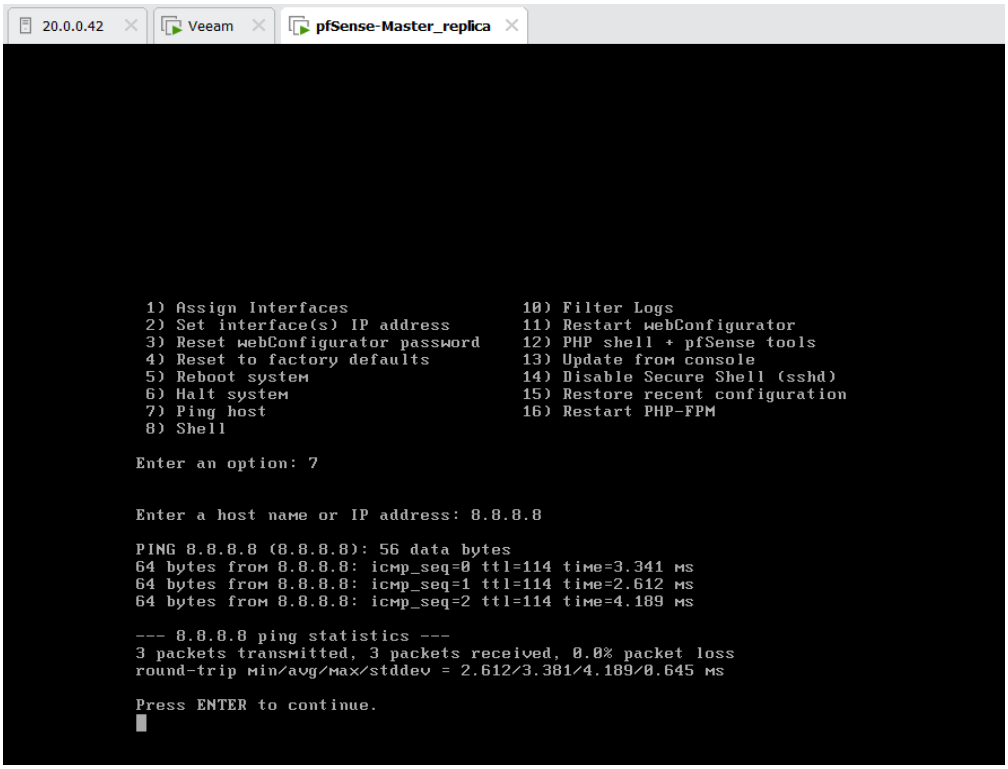

Figure 24 : Test de connectivité depuis pfSense-Master_replica - ping vers 8.8.8.8 réussi, 0% de perte de paquets

10. Retour en production (Failback)

Une fois l'ESXi de production réparé et reconnecté, la procédure de Failback permet de resynchroniser les données accumulées sur le site de secours pendant la période de sinistre, puis de redémarrer les VM sur l'infrastructure d'origine. Cette étape est cruciale pour éviter toute perte des transactions effectuées durant le basculement.

10.1. Sélection des réplicas à retourner en production

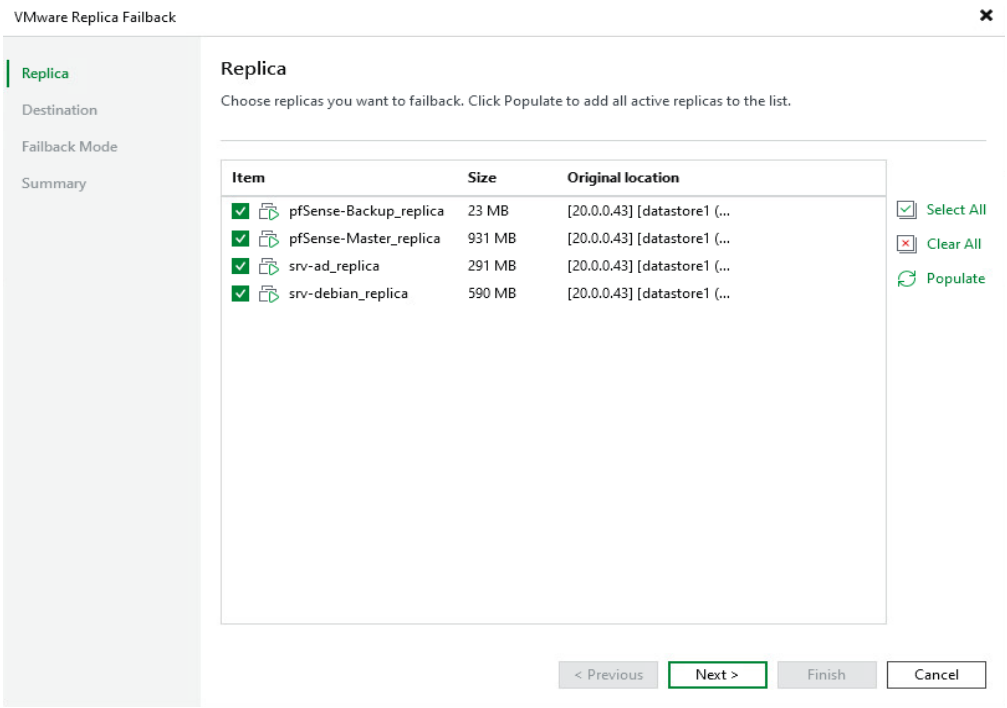

Figure 25 : Assistant Failback - sélection des 4 réplicas à resynchroniser vers le site de production

10.2. Configuration du mode de Failback

L'option "Failback to the original VM" est sélectionnée : Veeam compare les disques de la VM originale sur l'ESXi 1 avec l´état actuel du réplica sur l'ESXi 2, et ne retransfère que les blocs différents. L'option "Quick Rollback" est également activée pour accélérer la resynchronisation dans les scénarios où le sinistre était logiciel (et non matériel).

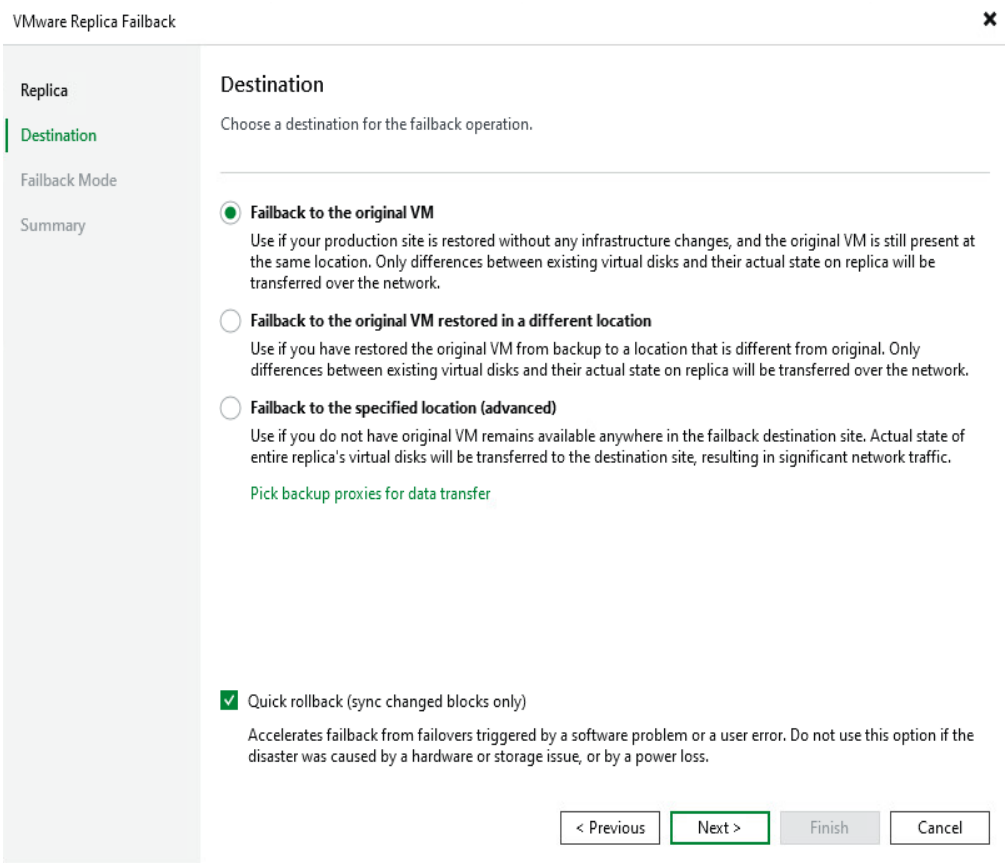

Figure 26 : Configuration du mode de Failback - retour sur la VM originale avec l'option Quick Rollback activée

10.3. Commit Failback - finalisation du retour en production

Après la resynchronisation des données, Veeam attend une confirmation manuelle (Commit Failback) avant définitivement éteindre les réplicas sur le site de secours. Cette sécurité permet de vérifier le bon fonctionnement des VM sur l'ESXi 1 avant de valider le retour complet.

Une fois le Commit effectué, le job de réplication reprend son cycle normal.

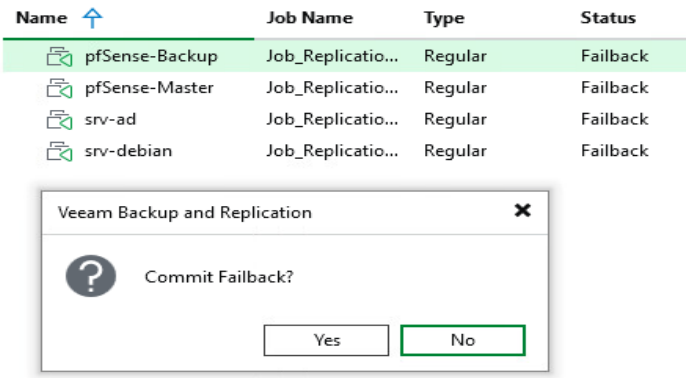

Figure 27 : Confirmation du Commit Failback - validation du retour définitif en production, les réplicas passent au statut "Failback"

11. Options de sortie après un Failover

Après l'activation d'un Failover, Veeam propose trois options permettant de gérer la suite des opérations selon l'état réel de l'infrastructure de production :

- **Undo Failover :** "C’était un test ou la panne est résolue immédiatement." Veeam éteint la VM sur l'ESXi 2 et supprime les modifications accumulées.

  Aucune donnée créée durant le basculement n'est conservée. À utiliser uniquement pour les tests ou les pannes très courtes.

- **Failback to Production :** "Le serveur principal est réparé."

  Veeam resynchronise les modifications accumulées sur l'ESXi 2 vers l'ESXi 1 et rallume les VM d'origine.

- **Permanent Failover :** "L'ESXi 1 est définitivement hors service."

  Les VM réplicas deviennent les nouvelles VM de production sur l'ESXi 2. Cette option est irréversible et nécessite une nouvelle infrastructure pour reconstruire la réplication.

12. Synthèse et indicateurs de performance du PRA

12.1. Résultats obtenus

- RPO mesuré : 2 heures (fréquence de réplication programmée). Configurable à 15 minutes pour les environnements avec exigences plus strictes.

- RTO mesuré : Inférieur à 10 minutes pour le redémarrage des 4 VM critiques sur le site de secours.

- Intégrité des données : Garantie par l'Application-Aware Processing (VSS) sur le contrôleur de domaine AD. Zéro corruption détectée lors des tests.

- **Transparence réseau :** Les VM réplicas conservent les mêmes adresses IP que les VM de production. Aucune modification de configuration DNS ou applicative n'est nécessaire lors du basculement.

12.2. Axes d'amélioration pour un déploiement en production

- Activation du Failover Plan automatisé (Veeam Enterprise) pour éliminer l'intervention manuelle et garantir l'ordre de démarrage.

- Mise en place d'une copie de sauvegarde immuable vers un stockage NAS ou Cloud par exemple (règle 3-2-1-1-0 complète).

- Intégration de la supervision Veeam dans Zabbix pour des alertes en temps réel sur l'état des jobs.

- Tests PRA semestriels documentés avec rapport de validation signé par la direction.

- Création d'un compte de service dédié Veeam avec les droits minimaux (principe du moindre privilège) plutôt que le compte root.

Conclusion

Ce Plan de Reprise d'Activité, basé sur Veeam Backup & Replication v13 et une architecture VMware ESXi dual-site, a démontré la viabilité technique d'une reprise d'activité rapide et fiable après un sinistre majeur.

Les machines virtuelles critiques (pfSense, Active Directory, Supervision) sont répliquées toutes les 2 heures sur le site de secours.

Les tests de basculement manuel ont confirmé que l'ensemble du Système d'Information peut être restauré en moins de 10 minutes, avec une perte de données maximale de 2 heures.

La cohérence applicative de l'Active Directory est garantie par l'Application-Aware Processing (VSS).

La procédure de Failback permet enfin un retour sécurisé en production sans perte des transactions effectuées durant la période de basculement.

Au-delà de l’aspect technique, ce projet démontre une réelle capacité à anticiper les sinistres et à garantir la résilience du Système d'Information.

En maîtrisant l'ensemble de la chaîne de protection (de l'isolation réseau à la validation des sauvegardes) j'ai mis en place une architecture capable de répondre aux exigences de continuité de service les plus strictes des entreprises modernes.

En combinant l'immutabilité des données et une stratégie de réplication granulaire, ce dispositif assure que l'entreprise ne subit pas le chantage des ransomwares.

Ce projet valide ainsi une approche de "sécurité par la conception", où la sauvegarde n'est plus un simple archivage, mais le dernier rempart stratégique de l'organisation.