Mise en place de la haute disponibilité dans l’infrastructure informatique de « Entreprise »

1 Table des matières

2 Table des illustrations

3 Introduction

Abstract (anglais)

This document presents the design of a highly available and secure IT infrastructure for Kali-Brazza, an accounting firm. The project relies on a redundant pfSense firewall cluster, centralized identity management via Active Directory, secure remote access through a VPN and a Guacamole bastion, and a 3-2-1 backup strategy across local storage, cloud storage and a disaster recovery site. Network segmentation, monitoring and vulnerability auditing complete the security posture, delivered through an Agile Scrumban approach.

Traduction française

Ce projet présente la conception d'une infrastructure informatique sécurisée et hautement disponible pour Kali-Brazza, un cabinet d'expertise comptable. Le projet repose sur un cluster de pare-feux pfSense redondant, une gestion centralisée des identités via Active Directory, un accès distant sécurisé via un VPN et un bastion Guacamole, ainsi qu'une stratégie de sauvegarde 3-2-1 combinant stockage local, stockage cloud et un site de secours. La segmentation réseau, la supervision et l'audit de vulnérabilités complètent le dispositif de sécurité, le tout mené selon une approche Agile Scrumban.

4 Le projet

4.1 Le Besoin

Kali-Brazza est un cabinet d'expertise comptable spécialisé dans l'accompagnement des entreprises et la gestion de dossiers clients.
Il utilise des outils informatiques pour gérer les dossiers comptables, les données clients et les échanges avec ses partenaires ce qui nécessite une infrastructure réseau sécurisée, fiable et disponible en permanence.

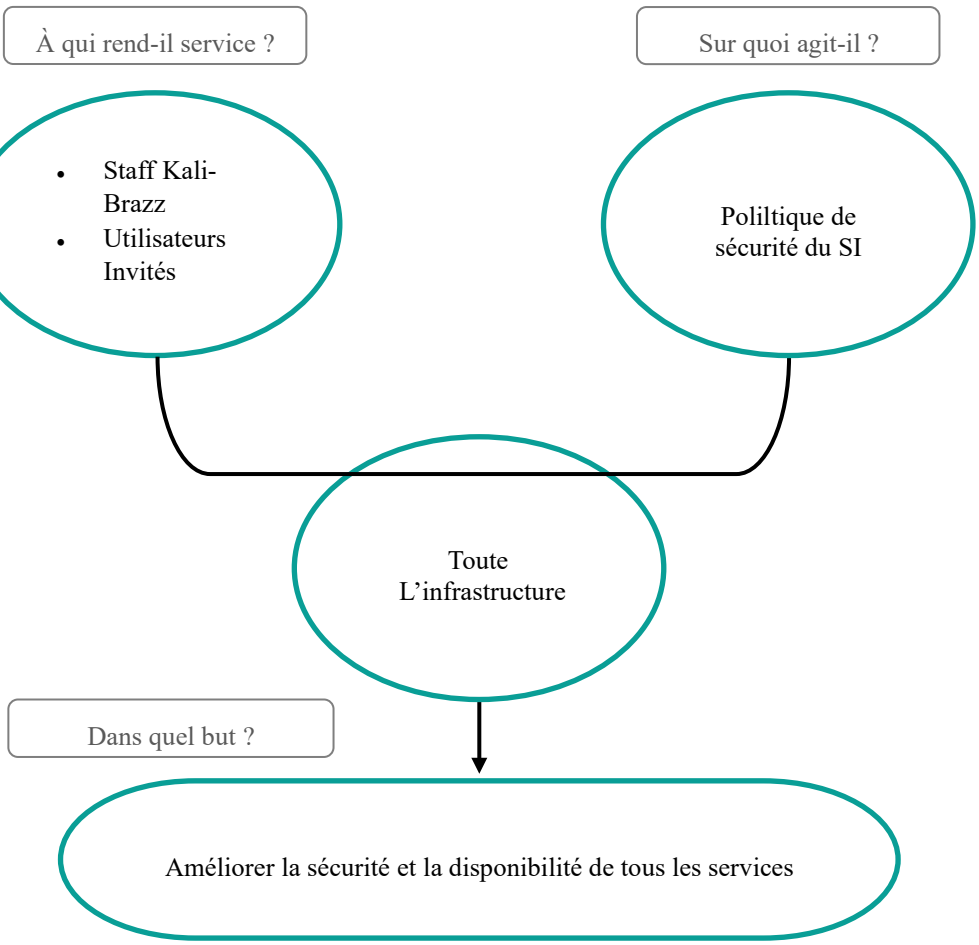
Le projet visait à répondre à plusieurs besoins essentiels de l'entreprise, notamment :

- Assurer la sécurité du réseau et des données
- Garantir la continuité de service, même en cas de panne
- Mettre en place une architecture fiable et évolutive
- Permettre un accès distant sécurisé grâce à un VPN
- Centraliser l'authentification des utilisateurs via un annuaire (Active Directory / LDAP)
- Mettre en place une supervision pour surveiller les équipements et services
- Gérer les logs pour faciliter l'analyse des incidents
- Mettre en place des sauvegardes pour protéger les données
- Segmenter le réseau à l'aide de VLAN pour améliorer la sécurité

Pour répondre à ces besoins, le choix s'est porté sur la mise en place d'un cluster pfSense en haute disponibilité, qui constitue la base de l'architecture du projet.

4.2 L'analyse fonctionnelle

Dans l'objectif de satisfaire une exigence fondamentale de notre entreprise, j'ai opté pour l'adoption d'un schéma conceptuel de « Bête à cornes » :



Ce diagramme a été conçu dans le but d'identifier de manière précise les parties prenantes clés ainsi que les acteurs susceptibles d'être affectés par une éventuelle interruption de nos opérations. Son utilisation permet d'évaluer de manière stratégique si le produit envisagé répondra efficacement aux besoins des collaborateurs impliqués.

4.3 Le cahiers des charges (CDC)

4.3.1 Cahier des charges fonctionnel (CDCF) (besoins fonctionnels et la manière dont la solution y répond)

Contexte et définition du problème

L'entreprise est un cabinet d'expertise comptable qui gère des dossiers clients sensibles et des échanges avec des partenaires. Son infrastructure informatique était peu sécurisée, peu surveillée et ne garantissait pas une continuité de service suffisante.

Plusieurs problèmes ont été identifiés :

- Absence de haute disponibilité en cas de panne réseau
- Accès distant inexistant
- Manque de centralisation de l'authentification
- Faible supervision et absence de gestion des logs
- Risque de perte de données par manque de sauvegardes structurées
- Réseau peu segmenté, augmentant les risques de sécurité

Ces limites exposaient l'entreprise à des risques de cyberattaques, de perte de données et d'interruption de service, ce qui est critique pour une activité dépendante du numérique.

Objectif du projet

L'objectif principal du projet est de concevoir et mettre en place une infrastructure informatique sécurisée, fiable et évolutive, capable alors de répondre à ces besoins :

Garantir la confidentialité, l'intégrité et la disponibilité des données

Assurer la continuité de service grâce à la haute disponibilité

Offrir un accès distant sécurisé aux employés

Centraliser l'authentification des utilisateurs

Mettre en place une supervision efficace et une gestion des incidents rapide

Sécuriser les postes de travail et les serveurs

Périmètre

Le projet couvre :

- La mise en place d'un cluster pfSense en haute disponibilité
- La sécurisation du réseau interne de l'agence
- La mise en œuvre d'un VPN sécurisé
- L'intégration d'une authentification centralisée (Active Directory / LDAP)
- La mise en œuvre d'un bastion d'accès distant (Apache Guacamole) authentifié via l'annuaire
- La supervision des équipements et services
- L'audit et le scan de vulnérabilités
- La gestion des logs
- La mise en place de sauvegardes
- La segmentation du réseau via des VLAN

<u>Le projet ne couvre pas</u> :

- Le développement d'applications métiers

- Le remplacement du matériel informatique existant (sauf nécessité liée à la sécurité comme des vieilles box pas sécurisés)

- Le remplacement du logiciel métier de comptabilité existant

Description fonctionnelle des besoins

Besoin fonctionnel	Description	Réponse de la solution
Sécurité réseau	Protéger le réseau contre les intrusions	Mise en place de pare-feu pfSense avec règles strictes
Continuité de service	Éviter les interruptions en cas de panne	Cluster pfSense en haute disponibilité
Accès distant sécurisé	Permettre le télétravail en toute sécurité	VPN obligatoire (authentification LDAP/AD) avec chiffrement + bastion Apache Guacamole pour l'accès RDP, sans exposition directe du LAN
Authentification centralisée	Gérer les accès via un annuaire	Intégration Active Directory / LDAP
Supervision	Surveiller les équipements et services	Outil de supervision : Zabbix
Gestion des logs	Centraliser et analyser les événements	Serveur de logs centralisé : Wazuh
Audit de vulnérabilités	Identifier et corriger les failles de sécurité	Scanner Nessus, campagnes de scan régulières
Sauvegardes	Protéger les données et configurations	Sauvegardes automatiques planifiées vers un stockage local et une destination cloud externalisée
Segmentation réseau	Isoler les différents services	Mise en place de VLAN
Continuité d'activité (PRA)	Garantir la reprise du service en cas de sinistre du site principal	Site de secours distant, réplication Veeam, tunnel VPN Site-à-Site

Enveloppe budgétaire

Poste de dépense	**Description**	**Coût estimé**
Matériel réseau	2 boîtiers pare-feu Netgate 4200 MAX (cluster HA du site principal) + 1 boîtier Netgate 2100 (site de secours) + 2 onduleurs* APC Smart-UPS 1500VA	2 840 €
Serveurs / virtualisation	Réutilisation des 2 hôtes ESXi existants (licence vSphere Enterprise Plus déjà acquise)	800 €/an
Stockage de sauvegarde	Disques virtuels TrueNAS (site principal et site de secours), thin-provisionnés sur l'infrastructure ESXi existante	0 €
Licences logicielles	Windows Server 2022 Standard (contrôleur de domaine Active Directory)	1 020 €
Solutions open source	pfSense, Zabbix, Wazuh, Duplicati, TrueNAS, Apache Guacamole, OpenVPN, Veeam Backup & Replication Community Edition	0 €
Audit de vulnérabilités	Nessus Essentials (gratuit jusqu'à 16 adresses IP, suffisant pour le périmètre du cabinet)	0 €
Sauvegarde cloud externalisée	Backblaze B2 (stockage hors site, ~2 To)	≈ 132 €/an

Poste de dépense	Description	Coût estimé
Formation	Montée en compétence de l'équipe sur pfSense, Active Directory, ESXi et TrueNAS	1 000 €
Temps de déploiement	Configuration, migration, tests (estimé à 15 jours-homme)	4 500 €
Maintenance annuelle	Support, mises à jour, supervision continue	1 200 €/an
Total investissement initial	-	**≈ 9 360 €**
Coût de fonctionnement annuel	-	**≈ 2 132 €/an**

Délais

Le projet est prévu sur une période de plusieurs semaines, découpée en phases :

Semaine 1 : Analyse des besoins et rédaction du cahier des charges

Semaine 2 : Conception de l'architecture réseau

Semaine 3 : Mise en place du cluster pfSense

Semaine 4 : Configuration du VPN et de l'authentification

Semaine 5 : Mise en place de la supervision et des sauvegardes

Semaine 6 : Tests, validation et documentation

8.3.2 Cahier des charges technique (exigences et contraintes techniques du produit)

Exigences techniques :

- Cluster pfSense en haute disponibilité (CARP + pfSync) avec bascule automatique sans interruption de service

- Segmentation réseau en VLAN (Admin, Serveurs, Utilisateurs, DMZ, Supervision, Sauvegardes), portés en trunk 802.1Q sur une interface unique par pare-feu

- Annuaire Active Directory centralisant l'authentification (postes, VPN, bastion Guacamole)

- Accès distant sécurisé via VPN chiffré (authentification LDAP) et bastion applicatif, sans exposition directe du réseau interne

- Supervision temps réel de l'infrastructure (Zabbix) et centralisation des journaux de sécurité (Wazuh)

- Audit périodique des vulnérabilités (Nessus)

- Sauvegarde automatisée selon la règle 3-2-1 (copie locale TrueNAS, copie cloud Backblaze B2, copie sur le site de secours)

- Plan de reprise d'activité avec site de secours distant et réplication (Veeam Backup & Replication)

Contraintes techniques :

- Réutilisation de l'infrastructure ESXi existante (deux hôtes sous licence vSphere Enterprise Plus), sans achat de matériel serveur supplémentaire

- Une seule interface réseau physique disponible sur l'hôte principal, imposant une architecture réseau reposant sur des vSwitches internes et un trunk VLAN plutôt que sur des cartes physiques dédiées par flux

- Absence de vCenter Server, contraignant la réplication et le failover à s'appuyer sur des hôtes ESXi autonomes (standalone)

- Espace disque limité sur l'hôte principal (48 Go), nécessitant un dimensionnement au plus juste du stockage de sauvegarde local

- Solutions retenues majoritairement open source, pour limiter les coûts de licence

4.4 Choix de la méthode de gestion de projets

4.4.1 Organisation en sprints

Pour la conduite de ce projet, la méthode **Agile Scrumban** a été retenue : elle a permis de découper le projet en sprints courts, chacun validé avant de passer au suivant.

Le projet a ainsi été découpé en 6 sprints d'une semaine, calés sur les 6 grandes phases définies dans le cahier des charges (cf. 4.3.1).

Chaque sprint démarre par une réunion de planification et se termine par une réunion de revue permettant de valider les livrables, d'ajuster les tâches restantes et de remonter les éventuels blocages.

Sprint	Période	Objectif du sprint	Tâches réalisées (backlog)	Livrable / Revue de sprint
Sprint 0 – Cadrage	01/12 – 05/12/2025	Cadrer le besoin et lancer le projet	Analyse du besoin, rédaction du CDC fonctionnel et technique, choix des solutions (pfSense, AD, Zabbix, Wazuh, Nessus, Duplicati/Backblaze, TrueNAS), préparation du lab VMware	CDC validé, environnement VMware opérationnel
Sprint 1 – Conception	08/12 – 12/12/2025	Concevoir l'architecture cible	Schéma logique et physique, plan d'adressage IP/VLAN, matrice des flux inter-VLAN	Schémas validés, tableau d'adressage figé (cf. 4.5)
Sprint 2 – Socle réseau HA	15/12 – 19/12/2025	Bâtir un cœur de réseau résilient	Configuration des interfaces et VLAN (10/20/30/40/50/60), cluster pfSense CARP + pfSync, règles de pare-feu inter-VLAN	Bascule Master/Backup testée sans coupure (4.9.1)
Sprint 3 – IAM et accès distant	05/01 – 09/01/2026	Centraliser les identités et sécuriser le télétravail	Déploiement AD DS (OU, utilisateurs, groupes), Apache Guacamole en DMZ, serveur VPN interfacé en LDAP	VPN + Guacamole fonctionnels avec un compte AD (4.9.2, 4.9.3)
Sprint 4 – Durcissement et supervision	12/01 – 16/01/2026	Durcir le parc et superviser l'infrastructure	GPO de sécurité, scan Nessus et remédiation, déploiement Zabbix et Wazuh	Rapport Nessus post-remédiation, dashboards Zabbix/Wazuh opérationnels (4.9.4 à 4.9.7)
Sprint 5 – Sauvegarde, PRA et recette	19/01 – 23/01/2026	Sécuriser la donnée et clôturer le projet	Duplicati + Backblaze B2, tunnel VPN Site-à-Site, TrueNAS/ZFS et snapshots, tests de bascule, documentation	Recette fonctionnelle, documentation livrée (cf. 9.1 et 9.2)

Une pause de deux semaines liée aux congés de fin d'année a été intégrée entre le Sprint 2 et le Sprint 3, sans impact sur le contenu du backlog.

Cette organisation en sprints courts, propre au Scrumban, a permis de détecter rapidement les blocages, par exemple les problèmes de « split-brain » lors des premiers tests de bascule CARP et d'adapter le périmètre des sprints suivants sans remettre en cause la date de fin de projet.

4.5 Conception (technique, architecture...)

Schéma logique :

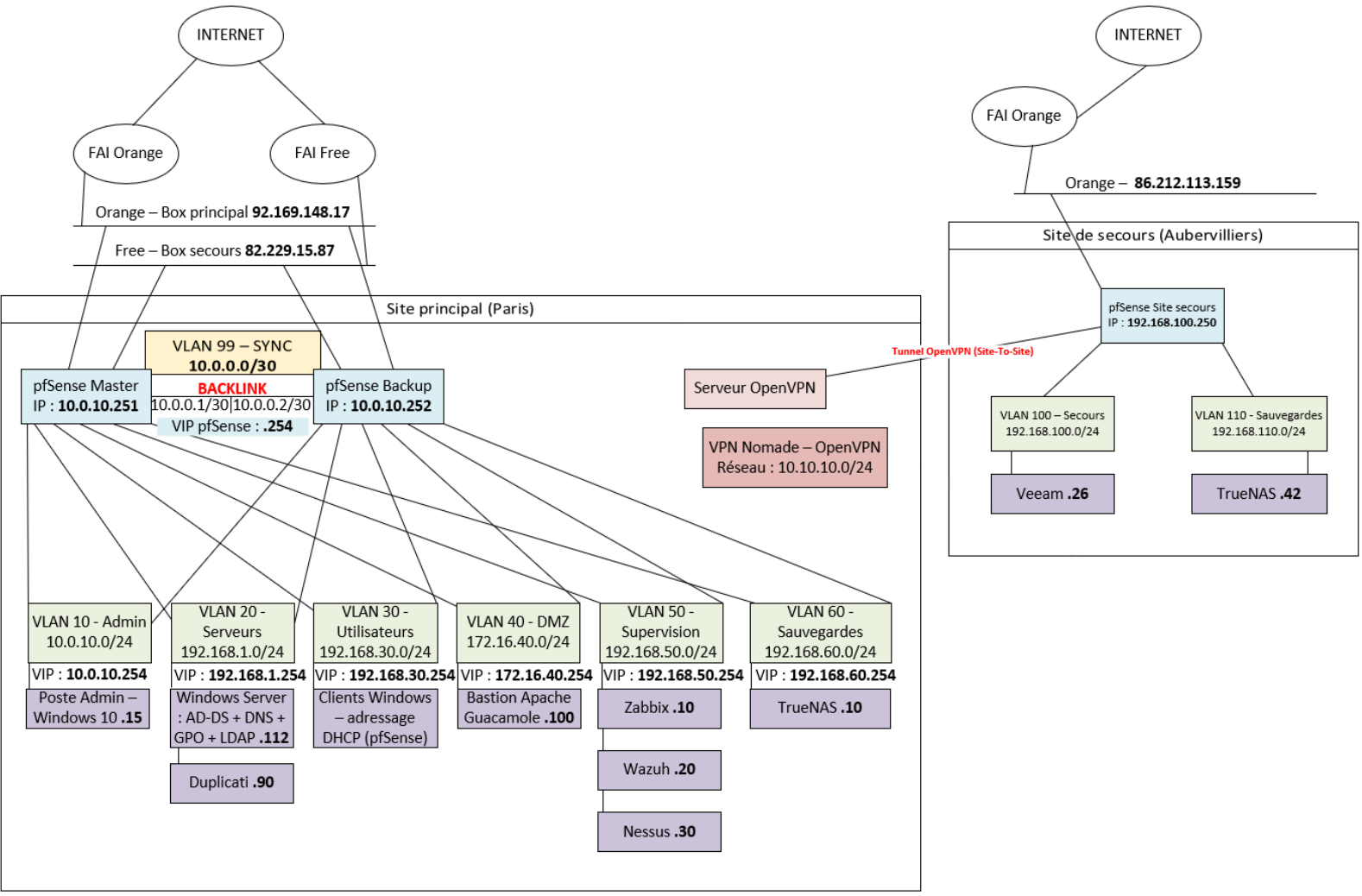

INTERNET
FAI Orange
FAI Free
Orange – Box principal 92.169.148.17
Free – Box secours 82.229.15.87
Site principal (Paris)
VLAN 99 – SYNC
10.0.0.0/30
pfSense Master
IP : 10.0.10.251
BACKLINK
10.0.0.1/30|10.0.0.2/30
VIP pfSense : .254
pfSense Backup
IP : 10.0.10.252
Serveur OpenVPN
VPN Nomade – OpenVPN
Réseau : 10.10.10.0/24
Tunnel OpenVPN (Site-To-Site)
INTERNET
FAI Orange
Orange – 86.212.113.159
Site de secours (Aubervilliers)
pfSense Site secours
IP : 192.168.100.250
VLAN 100 – Secours
192.168.100.0/24
VLAN 110 - Sauvegardes
192.168.110.0/24
Veeam .26
TrueNAS .42
VLAN 10 - Admin
10.0.10.0/24
VIP : 10.0.10.254
Poste Admin – Windows 10 .15
VLAN 20 - Serveurs
192.168.1.0/24
VIP : 192.168.1.254
Windows Server : AD-DS + DNS + GPO + LDAP .112
Duplicati .90
VLAN 30 - Utilisateurs
192.168.30.0/24
VIP : 192.168.30.254
Clients Windows – adressage DHCP (pfSense)
VLAN 40 - DMZ
172.16.40.0/24
VIP : 172.16.40.254
Bastion Apache Guacamole .100
VLAN 50 - Supervision
192.168.50.0/24
VIP : 192.168.50.254
Zabbix .10
Wazuh .20
Nessus .30
VLAN 60 - Sauvegardes
192.168.60.0/24
VIP : 192.168.60.254
TrueNAS .10

Schéma physique :

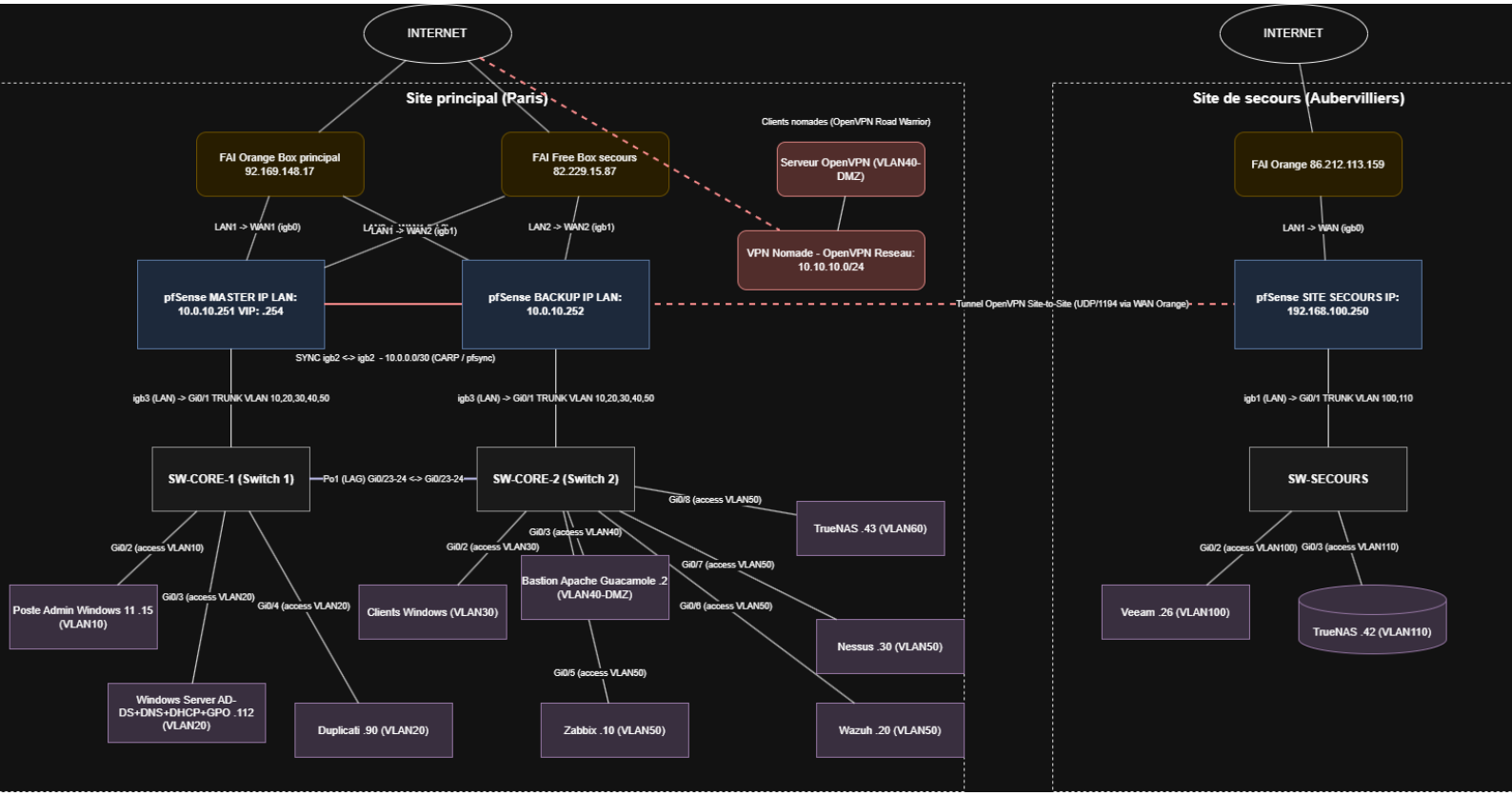


Tableau d'adressage :

Nom reçu dans VMware	Nom reçu dans FreeBSD	Nom attribué dans le pare-feu pfSense	Adresse IP fixe attribuée	Masque de sous-réseau	Dans le réseau virtuel	Commentaire
Network Adapter	em0	WAN	DHCP (172.16.20.x)	/23	VMnet0 (Bridged / réseau de l'établissement)	Côté WAN, sortie Internet simulée sur le réseau de l'école

Nom reçu dans VMware	Nom reçu dans FreeBSD	Nom attribué dans le pare-feu pfSense	Adresse IP fixe attribuée	Masque de sous-réseau	Dans le réseau virtuel	Commentaire
Network Adapter 2	em1	SYNC	10.0.0.1	/30	VMnet3 (Host-only), renommé HA_99	Lien de contrôle principal de la haute disponibilité (CARP/pfSync)
Network Adapter 3	em2	LAN_TRUNK	Pas d'IP sur le parent	-	VMnet2 (Host-only), port group VLAN ID 4095	Trunk 802.1Q portant les VLAN internes 10/20/30/50/60
Network Adapter 4	em3	DMZ	172.16.40.251	/24	VMnet4 (Host-only), renommé DMZ_40	DMZ - Bastion Apache Guacamole
Network Adapter 5	em4	WAN2	192.168.9.1	/29	VMnet-WAN2 (isolé, sans uplink physique)	Seconde sortie Internet simulée (redondance FAI)
Network Adapter 3 (802.1Q)	em2.10	VLAN10_ADMIN	10.0.10.251	/24	VMnet2 (Host-only), sous-interface taguée	VLAN 10 - Admin
Network Adapter 3 (802.1Q)	em2.20	VLAN20_SRV	192.168.1.251	/24	VMnet2 (Host-only), sous-interface taguée	VLAN 20 - Serveurs (AD/LDAP)
Network Adapter 3 (802.1Q)	em2.30	VLAN30_USR	192.168.30.251	/24	VMnet2 (Host-only), sous-interface taguée	VLAN 30 - Utilisateurs (postes durcis par GPO)
Network Adapter 3 (802.1Q)	em2.50	VLAN50_SUPV	192.168.50.251	/24	VMnet2 (Host-only), sous-interface taguée	VLAN 50 - Supervision (Zabbix, Wazuh, Nessus)
Network Adapter 3 (802.1Q)	em2.60	VLAN60_BACKUP	192.168.60.251	/24	VMnet2 (Host-only), sous-interface taguée	VLAN 60 - Sauvegardes (TrueNAS local, Duplicati)

Les VLAN 10, 20, 30, 50 et 60 sont portés par la même interface physique (em2) grâce à un tag 802.1Q ; seuls le VLAN 40 (DMZ) et le lien SYNC (VLAN 99) disposent d'une interface physique dédiée dans le lab ESXi.

Le tableau ci-dessous synthétise l'adressage partagé entre les deux nœuds du cluster (CARP) :

Interface / VLAN	IP pfSense MASTER	IP pfSense BACKUP	VIP CARP partagée
LAN (VLAN 10 - Admin)	10.0.10.251	10.0.10.252	10.0.10.254
VLAN 20 - Serveurs	192.168.1.251	192.168.1.252	192.168.1.254
VLAN 30 - Utilisateurs	192.168.30.251	192.168.30.252	192.168.30.254

Interface / VLAN	IP pfSense MASTER	IP pfSense BACKUP	VIP CARP partagée
DMZ (VLAN 40)	172.16.40.251	172.16.40.252	172.16.40.254
VLAN 50 - Supervision	192.168.50.251	192.168.50.252	192.168.50.254
VLAN 60 - Sauvegardes	192.168.60.251	192.168.60.252	192.168.60.254
WAN2	192.168.9.1	192.168.9.2	192.168.9.4 (gateway simulée : 192.168.9.3)
SYNC (VLAN 99)	10.0.0.1	10.0.0.2	(lien pfSync point-à-point, pas de VIP)

Adressage du site de secours (Aubervilliers), hébergé sur un second hôte ESXi et relié au Site Principal par le tunnel VPN Site-à-Site :

Interface	Adresse IP	Masque	Commentaire
WAN	Fournie par le FAI d'Aubervilliers (Orange, 86.212.113.159)	-	Sortie Internet du site de secours
VLAN 100 - Secours	192.168.100.250	/24	Réseau hébergeant Veeam Backup & Replication (.26)
VLAN 110 - Sauvegardes	192.168.110.250	/24	Sauvegardes - héberge le serveur TrueNAS-secours (.42), pool ZFS en mirror
Tunnel VPN S2S	192.168.100.0/24 et 192.168.110.0/24 routés	/24	Réseaux distants accessibles depuis le Site Principal via le tunnel OpenVPN Site-à-Site

Aucune VIP CARP côté site de secours : un seul nœud pfSense y est déployé, sans cluster HA à cet endroit.

4.6 Les tâches

Pour mener à bien ce projet, le travail a été découpé en plusieurs tâches techniques réparties sur différents sprints :

Tâches d'Architecture et Réseau (Couche 2 & 3) :

- Configuration des interfaces réseau et création des VLAN du site principal (10, 20, 30, 40, 50, 60) et du site de secours (100, 110)

- Mise en place de la Haute Disponibilité (CARP/pfSync) sur le cluster pfSense

- Écriture et application des règles de pare-feu restrictives (inter-VLAN)

Tâches de Gestion des Identités et des Accès (IAM) :

- Installation et configuration du rôle AD DS sur Windows Server

- Création des Unités Organisationnelles, utilisateurs, et groupes de sécurité

- Déploiement et configuration d'Apache Guacamole dans la DMZ

- Mise en place du serveur VPN et interfaçage de Guacamole et du VPN avec l'AD via LDAP

Tâches de Durcissement et Sécurité Applicative :

- Création et déploiement des GPO de sécurité (Verrouillage écran, blocage USB, mots de passe)

- Lancement des scans Nessus, analyse des rapports et application des correctifs (remédiation)

Tâches de Supervision et de SIEM :

- Déploiement du serveur central Zabbix pour la supervision de l'infrastructure

- Supervision de l'état CARP du cluster pfSense (statut Master/Backup)

- Supervision du trafic Internet sur l'interface WAN de pfSense

- Supervision de la disponibilité du service DNS sur le Windows Server

- Supervision du service LDAP/AD DS sur le Windows Server via le template Zabbix dédié (threads LDAP actifs, sessions clientes, statut du port LDAP, recherches/sec, écritures/sec)

- Déploiement du serveur Wazuh (Manager)

- Déploiement des agents Wazuh sur les cibles et création des règles d'alertes

Tâches de Sauvegarde et de PRA :

- Configuration de Duplicati (sauvegarde locale vers TrueNAS et cloud vers Backblaze), création du bucket de destination sur Backblaze Cloud

- Configuration du serveur TrueNAS du site principal, création du pool de stockage ZFS et automatisation des snapshots

- Déploiement du pare-feu et du serveur TrueNAS-secours (pool ZFS en mirror) sur le site de secours

- Montage du tunnel VPN Site-à-Site entre le Site Principal et le Site de Secours

- Déploiement de Veeam Backup & Replication et configuration du job de réplication du contrôleur de domaine, avec règles de re-IP pour le failover vers le site de secours

4.7 Les ressources

4.7.1 Humaines (RACI)

La matrice RACI ci-dessous précise, pour chaque grand lot du projet, qui Réalise (R), qui Approuve (A), qui est Consulté (C) et qui est Informé (I).

Lot / Livrable	Alternant (Administrateur Sys. et Réseaux)	Tuteur entreprise	Direction Kali-Brazza	Collaborateurs / utilisateurs
Cadrage et cahier des charges	R	A	C	I
Conception (schémas, adressage)	R	A	I	I
Cluster pfSense HA (CARP/pfSync)	R	A	I	I
AD/LDAP, VPN, Guacamole	R	A	C	I
Durcissement (GPO, scans Nessus)	R	A	I	I

Supervision (Zabbix, Wazuh)	R	A	I	I
Sauvegarde / PRA (Duplicati, TrueNAS)	R	A	C	I
Recette et formation des utilisateurs	R	A	C	C
Site de secours et PRA	R	A	C	I

R = Réalisateur, A = Approbateur, C = Consulté, I = Informé.

4.7.2 Budgetaires

Le prototype de ce projet a été déployé sur l'infrastructure ESXi existante de l'établissement (deux hôtes sous licence vSphere Enterprise Plus), sans achat de matériel serveur supplémentaire. Le tableau ci-dessous chiffre néanmoins un déploiement réel en production chez Kali-Brazza, sur la base de tarifs publics relevés en 2026.

Catégorie	Élément	Qté	Coût unitaire	Coût total	Récurrence
Matériel réseau	Netgate 4200 MAX (pfSense+, cluster Master/Backup)	2	599 $ (~550 €)	~1 100 €	Achat unique
Matériel réseau	Netgate 2100 BASE (pfSense site de secours)	1	412 $ (~380 €)	~380 €	Achat unique
Matériel réseau	Onduleur APC Smart-UPS 1500VA rack (1 par site)	2	~680 € HT	~1 360 €	Achat unique
Licence	Windows Server 2022 Standard (16 cœurs)	1	~1 020 € HT	~1 020 €	Licence perpétuelle
Licence	Nessus Essentials (gratuit, jusqu'à 16 adresses IP)	1	0 €	0 €	-
Licence	pfSense CE, Zabbix, Wazuh, Duplicati, TrueNAS, Apache Guacamole, Veeam CE	-	0 € (open source / gratuit)	0 €	-
Cloud	Backblaze B2 (sauvegardes externalisées, ~2 To)	2 To	6 $/To/mois (~5,50 €)	~11 €/mois	Mensuel
Divers	Câblage, switch d'accès, imprévus (~10%)	-	-	~660 €	Achat unique
Formation	Montée en compétence de l'équipe sur pfSense, Active Directory, ESXi et TrueNAS	-	-	1 000 €	Achat unique
Temps de déploiement	Configuration, migration, tests (estimé à 15 jours-homme)	-	-	4 500 €	Achat unique
Maintenance	Support, mises à jour, supervision continue	-	-	1 200 €	Annuel

Soit un investissement initial d'environ 9 360 € (matériel, licences, formation et temps de déploiement), auquel s'ajoutent environ 2 132 €/an de fonctionnement (maintenance et stockage Backblaze B2) - Nessus Essentials, gratuit jusqu'à 16 adresses IP, étant suffisant pour le périmètre du cabinet et n'entraînant aucun coût de licence récurrent. Sources : boutique Netgate, comparateur idealo.fr, Backblaze (tarifs consultés en 2026).

4.7.3 Matérielles

L'infrastructure repose sur deux hôtes ESXi déjà existants au sein de l'établissement (un par site), sans achat de serveur supplémentaire. Le tableau suivant liste les ressources matérielles et virtuelles mobilisées sur chacun des deux sites :

Ressource	Caractéristiques	Rôle
Hôte ESXi - Site principal	Infrastructure existante de l'établissement, licence vSphere Enterprise Plus, ~48 Go d'espace disque disponible, 1 seule carte réseau physique	Héberge le cluster pfSense HA et l'ensemble des VM du site principal
Hôte ESXi - Site de secours	Infrastructure existante de l'établissement (2e hôte), licence vSphere Enterprise Plus, ~350 Go d'espace disque disponible	Héberge pfSense-secours, TrueNAS-secours et Veeam
VM pfSense MASTER / BACKUP	2 vCPU, 2 Go RAM, 20 Go disque, 5 interfaces réseau	Cluster pare-feu haute disponibilité (CARP/pfSync)
VM pfSense Secours	2 vCPU, 2 Go RAM, 20 Go disque, 2 interfaces réseau	Pare-feu du site de secours (Aubervilliers)
VM Windows Server (AD DS/DNS/DHCP/LDAP)	2 vCPU, 4 Go RAM, 60 Go disque	Annuaire, DNS, DHCP centralisés
VM Apache Guacamole	2 vCPU, 2 Go RAM, 20 Go disque	Bastion d'accès distant (DMZ)
VM Supervision (Zabbix + Wazuh + Nessus mutualisés)	4 vCPU, 8 Go RAM, 50 Go disque	Supervision, SIEM et audit de vulnérabilités - mutualisés sur une VM unique par contrainte de ressources
VM TrueNAS - Site principal (VLAN 60)	2 vCPU, 4 Go RAM, disque de boot 8 Go + pool ZFS simple 40 Go (sans mirror, contrainte d'espace disque assumée)	Stockage local des sauvegardes Duplicati
VM TrueNAS - Site de secours	2 vCPU, 8 Go RAM, disque de boot 16 Go + pool ZFS en mirror 2x100 Go	Stockage de secours (PRA), snapshots immuables

Ressource	Caractéristiques	Rôle
VM Veeam Backup & Replication (Community Edition)	2 vCPU, 4 Go RAM, 40 Go disque	Réplication et failover du contrôleur de domaine vers le site de secours
Postes clients Windows (VLAN 30)	2 vCPU, 4 Go RAM	Postes utilisateurs de test, durcis par GPO

4.7.4 Phasing (Diagramme de Gantt avec jalon, avancement, liaisons...)

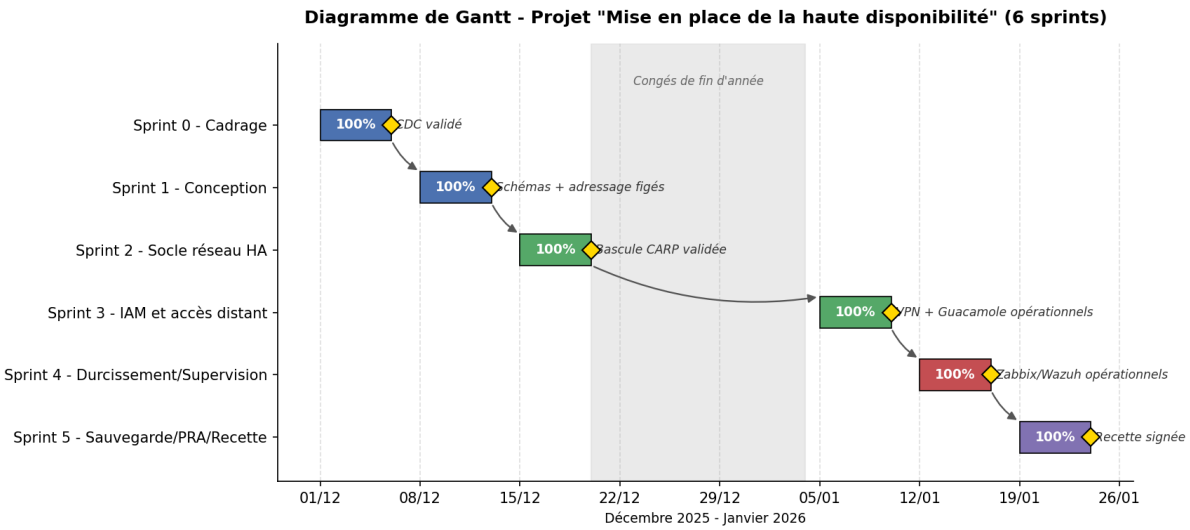


Figure 1: Diagramme de Gantt du projet - 6 sprints, jalons (losanges) et liaisons fin-début entre sprints

4.8 Gestion des risque (Methode AMDEC)

Ce projet comporte des risques inhérents à sa réalisation ainsi qu'à la continuité d'activité de l'entreprise une fois l'infrastructure en production. Ils sont calculés par rapport à la capacité de l'entreprise à maintenir son activité. Pour cela, j'utilise la méthode AMDEC.

Le tableau ci-dessous rappelle l'échelle de criticité utilisée (Fréquence x Gravité) pour coter chaque risque du tableau AMDEC : plus la case est foncée, plus le risque est critique et prioritaire à traiter.

Fréquence \ Gravité	Faible (1)	Moyenne (2)	Grave (3)	Très grave (4)
Très probable (4)	4	16	36	64

Probable (3)	3	12	27	48
Improbable (2)	2	8	18	32
Très improbable (1)	1	4	9	16

Vert = risque acceptable en l'état, jaune/orange = risque à surveiller avec un plan d'action, rouge = risque critique nécessitant une réponse immédiate (cf. colonne Solutions du tableau ci-dessous).

ID	Risques	Solutions	Fréq.	Grav.	Crit.	Impact
Risques internes						
INT1	Suppression des données par erreur humaine	Se référer au PRA prévu à cet effet	1	4	**4**	Délai et performances
INT2	Panne matériel	Se référer au PRA prévu à cet effet	1	2	**2**	Performance, délais et coût
INT3	Solution inutilisable ou non fonctionnelle	Informer l'architecte de la solution	2	3	**6**	Délai et performances
INT4	Vols de données	Protection des données par gestion des permissions et mots de passe forts	1	2	**2**	Performance et coût
Risques externes						
EXT1	Coupure de service au niveau du FAI	Se tenir informé des délais auprès du FAI	1	3	**3**	Performance, délais et coût
EXT2	Coupure du service OVH	Se tenir informé des délais auprès du fournisseur OVH	1	3	**3**	Performance, délais et coût
EXT3	Coupure de courant	Se tenir informé auprès des services municipaux	1	3	**3**	Performance, délais et coût
Risques climatiques, naturels et technologiques						
CNT1	Inondation	Rester en alerte en cas d'avertissement par les autorités compétentes	1	2	**4**	Performance, délais et coût
CNT2	Incendie	Rester en alerte en cas d'avertissement par les autorités compétentes	1	4	**4**	Performance, délais et coût
CNT3	Vol de matériel	S'informer sur les recours auprès des autorités compétentes	1	4	**4**	Performance, délais et coût
CNT4	Tempête	Rester en alerte en cas d'avertissement par les autorités compétentes	1	4	**4**	Performance, délais et coût
CNT5	Cyberattaque	Se référer au PRA prévu à cet effet	2	4	**8**	Performance, délais et coût

4.9 Réalisation

Cette section détaille la mise en œuvre technique de l'infrastructure sécurisée de Kali-Brazza. L'objectif a été de concevoir une architecture hautement disponible, en segmentant les flux et en appliquant le principe du moindre privilège.

4.9.1 Le socle de l'infrastructure

Le cluster pfSense en Haute Disponibilité (CARP) est la toute première brique de cette refonte : la mise en place du cœur de réseau. Pour garantir la continuité de service (exigence forte du projet), un cluster de deux pare-feux pfSense (Master et Backup) a été déployé, sur la base de six interfaces réseau par nœud (WAN, WAN2, SYNC, DMZ, et le trunk portant les VLAN 10/20/30/50/60).

La haute disponibilité repose sur le protocole CARP couplé à pfSync. pfSync se charge de synchroniser l'état des connexions entre les deux nœuds via un lien dédié (VLAN 99 - SYNC), tandis que CARP gère

les adresses IP virtuelles (VIP) sur chaque interface partagée. Ainsi, si le nœud Master subit une panne, le nœud Backup prend le relais, de manière transparente pour les utilisateurs du cabinet.

La segmentation réseau en VLAN, associée à des règles de pare-feu spécifiques par segment (moindre privilège), complète ce socle en cloisonnant les flux entre l'administration, les serveurs, les utilisateurs, la DMZ et la supervision.

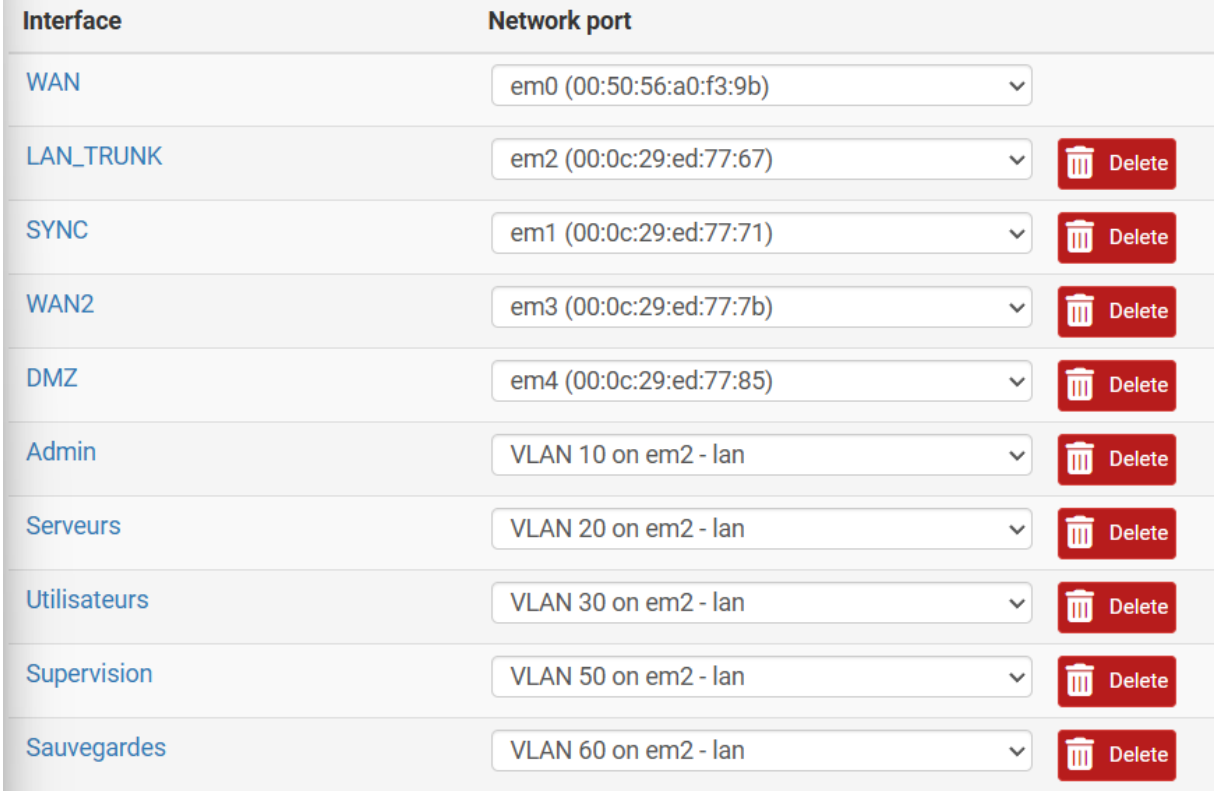


Figure 2 : Tableau des VLAN et de leurs tags sur l'interface parente (trunk)

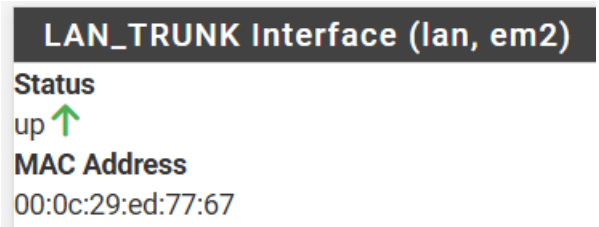


Figure 3 : Statut de l'interface LAN_TRUNK affichant « up »

Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
192.168.9.4/29 (vhid: 2)	WAN2	CARP		
172.16.40.254/24 (vhid: 40)	DMZ	CARP		
10.0.10.254/24 (vhid: 10)	ADMIN	CARP		
192.168.1.254/24 (vhid: 20)	SERVEURS	CARP		
192.168.30.254/24 (vhid: 30)	UTILISATEURS	CARP		
192.168.50.254/24 (vhid: 50)	SUPERVISION	CARP		
192.168.60.254/24 (vhid: 60)	SAUVEGARDES	CARP		

Figure 4 : Liste des adresses IP virtuelles (VIP) CARP configurées

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
WAN2@2	192.168.9.4/29		MASTER
DMZ@40	172.16.40.254/24		MASTER
ADMIN@10	10.0.10.254/24		MASTER
SERVEURS@20	192.168.1.254/24		MASTER
UTILISATEURS@30	192.168.30.254/24		MASTER
SUPERVISION@50	192.168.50.254/24		MASTER
SAUVEGARDES@60	192.168.60.254/24		MASTER

State Synchronization Status

State Creator Host IDs:

- 2728cc4d
- 6a8f0683 (This node)

Figure 5 : Statut CARP : pf1 en MASTER

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
WAN2@2	192.168.9.4/29		BACKUP
DMZ@40	172.16.40.254/24		BACKUP
ADMIN@10	10.0.10.254/24		BACKUP
SERVEURS@20	192.168.1.254/24		BACKUP
UTILISATEURS@30	192.168.30.254/24		BACKUP
SUPERVISION@50	192.168.50.254/24		BACKUP
SAUVEGARDES@60	192.168.60.254/24		BACKUP

State Synchronization Status

State Creator Host IDs:
- 2728cc4d (This node)
- 6a8f0683

Figure 6 : Statut CARP : pf2 en Backup

Lors d'une simulation de panne (extinction volontaire du nœud principal pf1), le mécanisme de bascule s'opère instantanément : le nœud secondaire (pf2) détecte la perte des battements de cœur (heartbeats) et prend automatiquement le rôle de Master, garantissant la continuité de service sans interruption perceptible pour les utilisateurs.

CARP Status

Interface and VHID	Virtual IP Address	Description	Status
WAN2@2	192.168.9.4/29		MASTER
DMZ@40	172.16.40.254/24		MASTER
ADMIN@10	10.0.10.254/24		MASTER
SERVEURS@20	192.168.1.254/24		MASTER
UTILISATEURS@30	192.168.30.254/24		MASTER
SUPERVISION@50	192.168.50.254/24		MASTER
SAUVEGARDES@60	192.168.60.254/24		MASTER

State Synchronization Status

State Creator Host IDs:
- 2728cc4d (This node)
- 6a8f0683

Figure 7 : Statut CARP : pf2 passe en Master suite à l'interruption de pf1

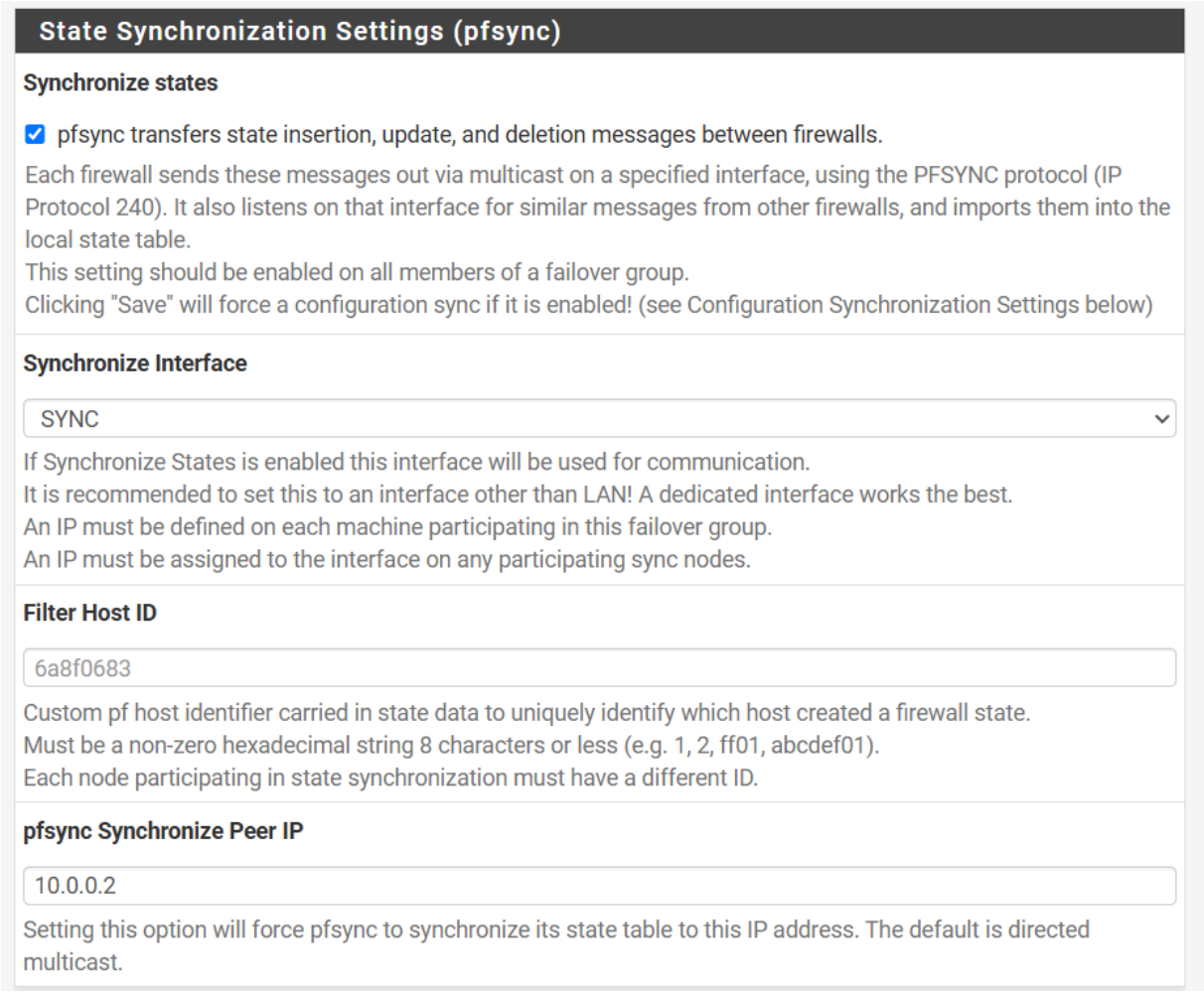


Figure 8 : Configuration de la synchronisation pfSync et XMLRPC Config Sync

4.9.2 Le cœur des identités

L'authentification centralisée (AD / LDAP) : une fois le réseau sécurisé et redondé, la centralisation des identités a été traitée. Déployé au sein du VLAN 20 (Serveurs) sur le Site Principal, le serveur Active Directory (AD/LDAP) est l'unique source de confiance pour l'authentification. Le cluster pfSense (VPN), le portail Apache Guacamole interrogent ce serveur. Cela garantit qu'une personne quittant le cabinet voit tous ses accès (réseau, VPN, applicatifs) coupés instantanément en une seule manipulation.

La mise en service de cet annuaire a nécessité un travail de diagnostic précis : la recherche LDAP échouait initialement tant que le chemin exact de l'organisation (OU) et le bon compte de service (Bind DN) n'étaient pas identifiés dans l'arborescence réelle de l'annuaire.

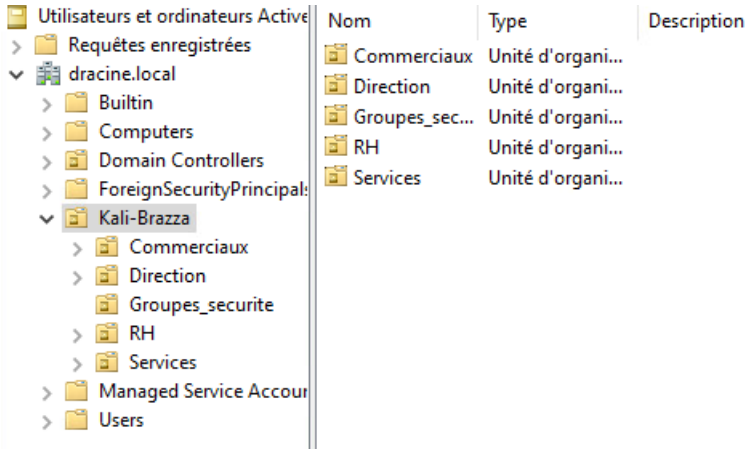


Figure 9 : Arborescence Active Directory (OU Kali-Brazza et sous-OU Commerciaux, Direction, RH, Services)

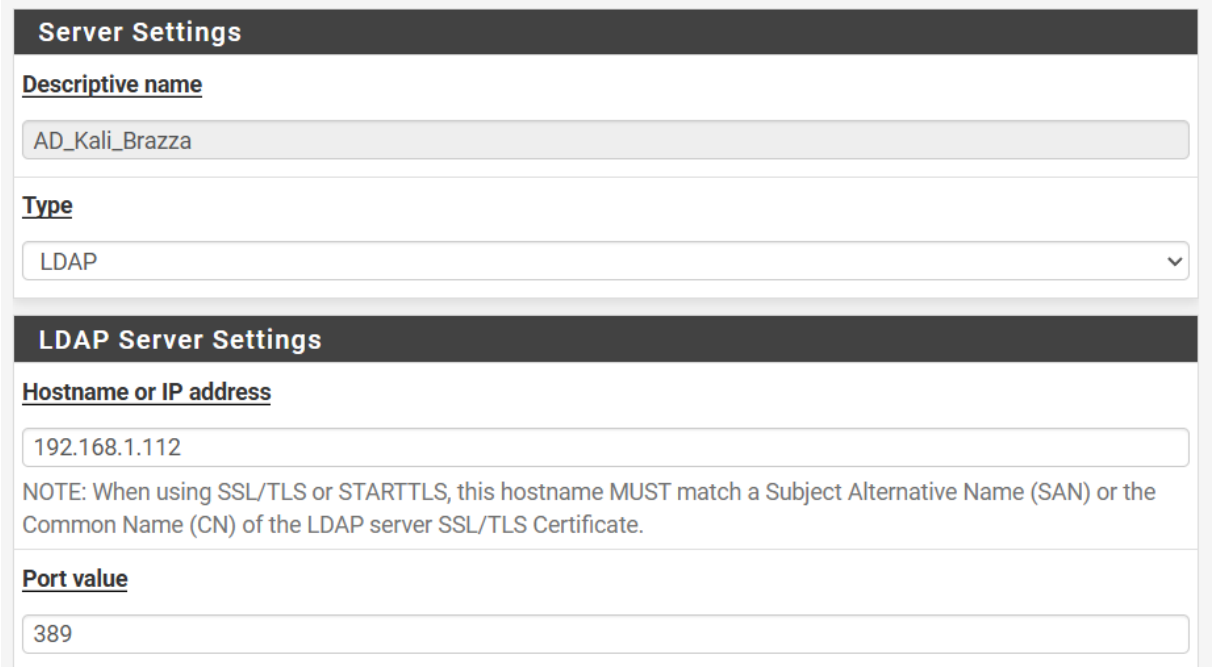


Figure 10 : Déclaration du serveur d'authentification LDAP (adresse IP et port)

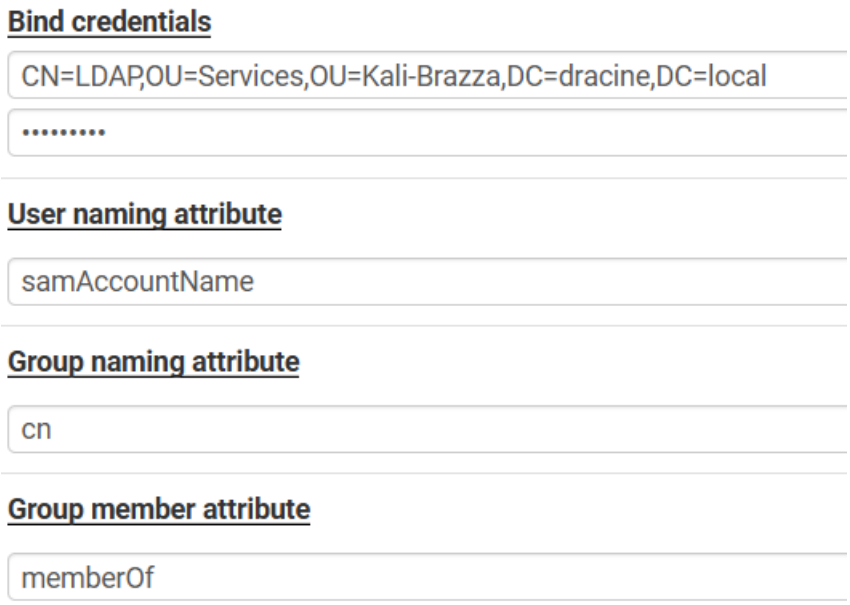


Figure 11 : Configuration du compte de service (Bind Credentials) LDAP sur pfSense

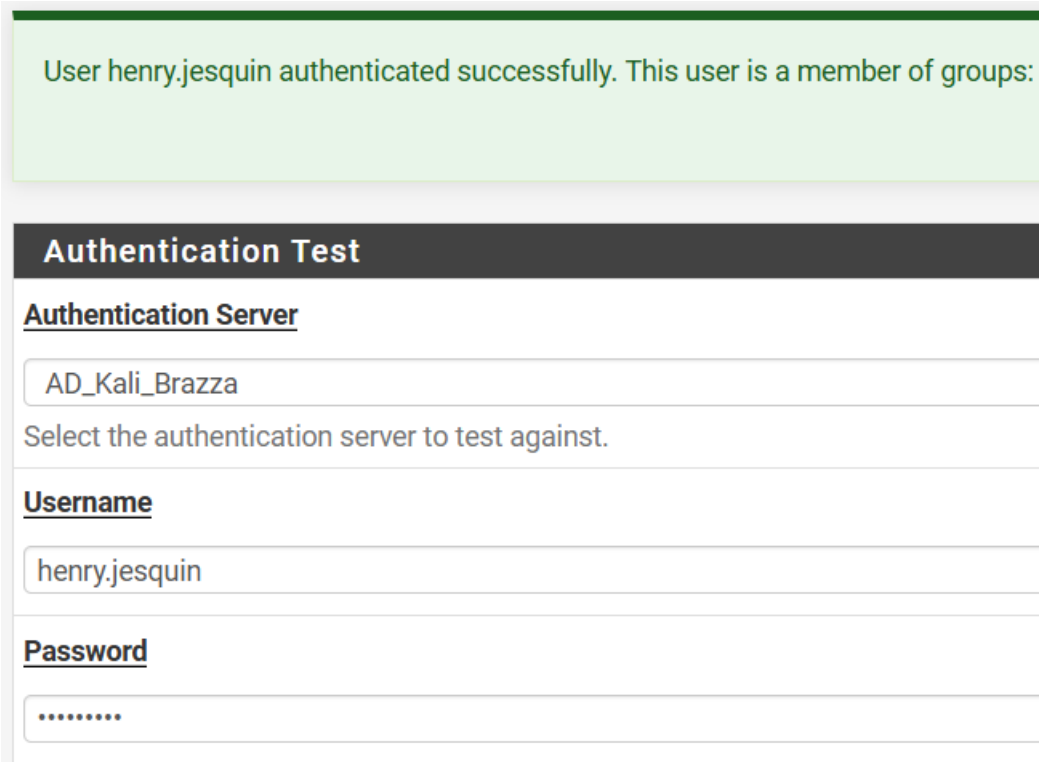


Figure 12 : Validation de l'authentification LDAP (Diagnostics -> Authentication) avec un compte réel

4.9.3 Stratégie Zero Trust

Le VPN et le bastion (Guacamole) : pour sécuriser le télétravail, une stratégie « double sécurité » a été implémentée.

L'utilisateur distant se connecte d'abord via un tunnel VPN monté sur le cluster pfSense et authentifié contre l'annuaire AD ; une fois connecté, il n'a pas d'accès direct au réseau de production. Il doit ensuite s'authentifier sur le portail web Apache Guacamole, situé dans la DMZ (VLAN 40), avec les mêmes identifiants AD grâce à l'extension guacamole-auth-ldap.

Guacamole agit comme un bastion pour accéder aux ressources internes (RDP) directement depuis le navigateur, empêchant tout flux direct entre le poste nomade et les serveurs critiques.

Pour que ce scénario soit exploitable dans la durée, le poste cible de chaque utilisateur bénéficie d'une réservation DHCP par adresse MAC, garantissant que la connexion Guacamole pointe toujours vers la bonne machine malgré l'attribution dynamique des adresses.

Common Name	Real Address	Virtual Address
henry.jesquin henry.jesquin	30.0.0.3:51881	10.10.10.2

Figure 13 : Client OpenVPN connecté avec succès via un compte Active Directory

Pour le poste concerné, une réservation d'adresse IP statique via DHCP (appairage par adresse MAC) a ainsi été appliquée.

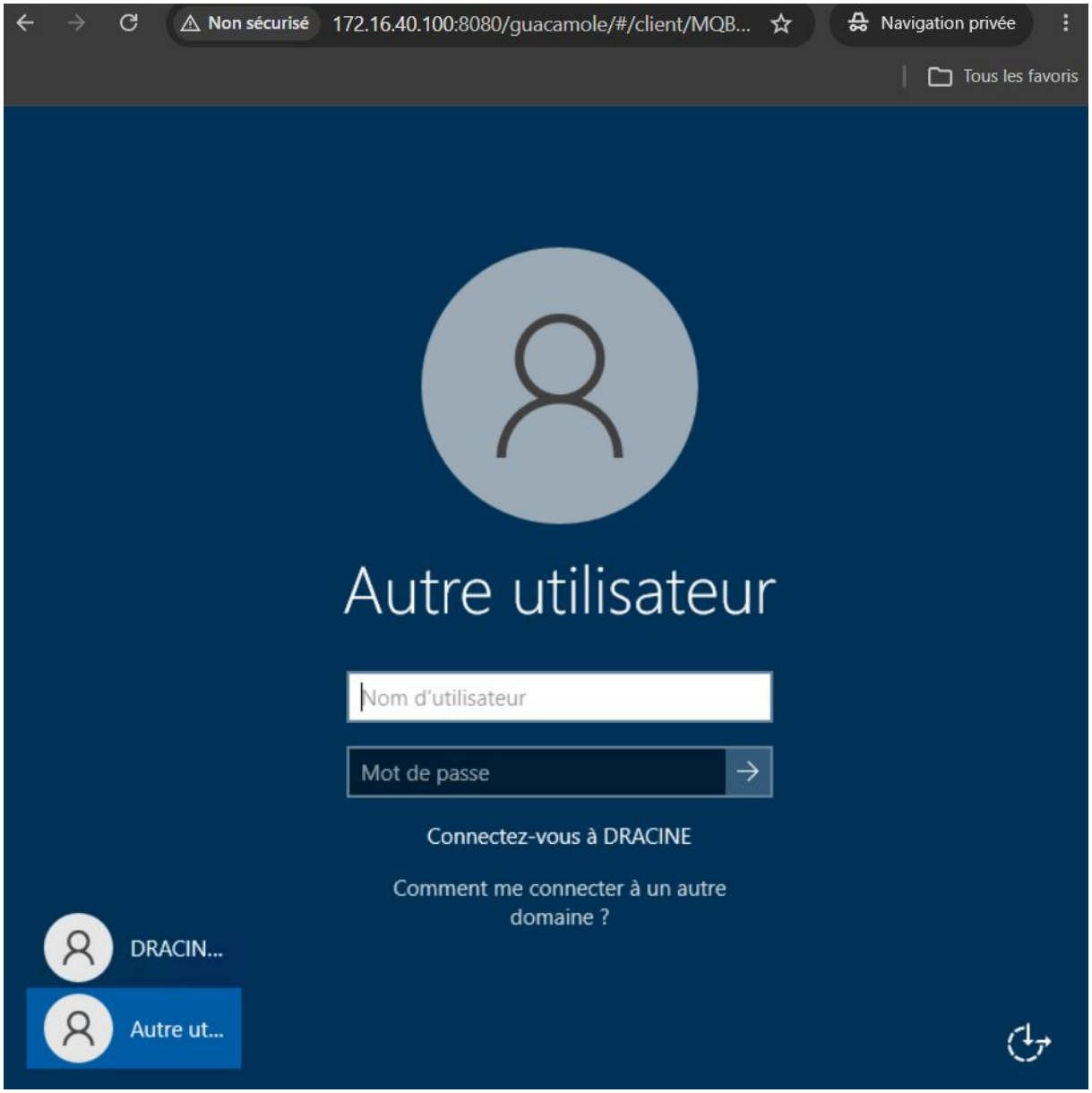


Figure 14 : Page de connexion et session ouverte sur le bastion Guacamole via AD

4.9.4 Cartographie et remédiation

L'audit de sécurité (Nessus) : pour valider la robustesse de ces premières défenses, un scanner de vulnérabilités Nessus a été déployé sur la VM Supervision (VLAN 50), mutualisée avec Zabbix et Wazuh par contrainte de ressources. Un scan de type Basic Network Scan a été configuré et lancé sur le contrôleur de domaine (AD/Windows Server), en mode authentifié (identifiants Windows renseignés dans le scan) afin d'obtenir une cartographie précise des vulnérabilités, y compris celles internes au système, et non uniquement celles visibles depuis l'extérieur.

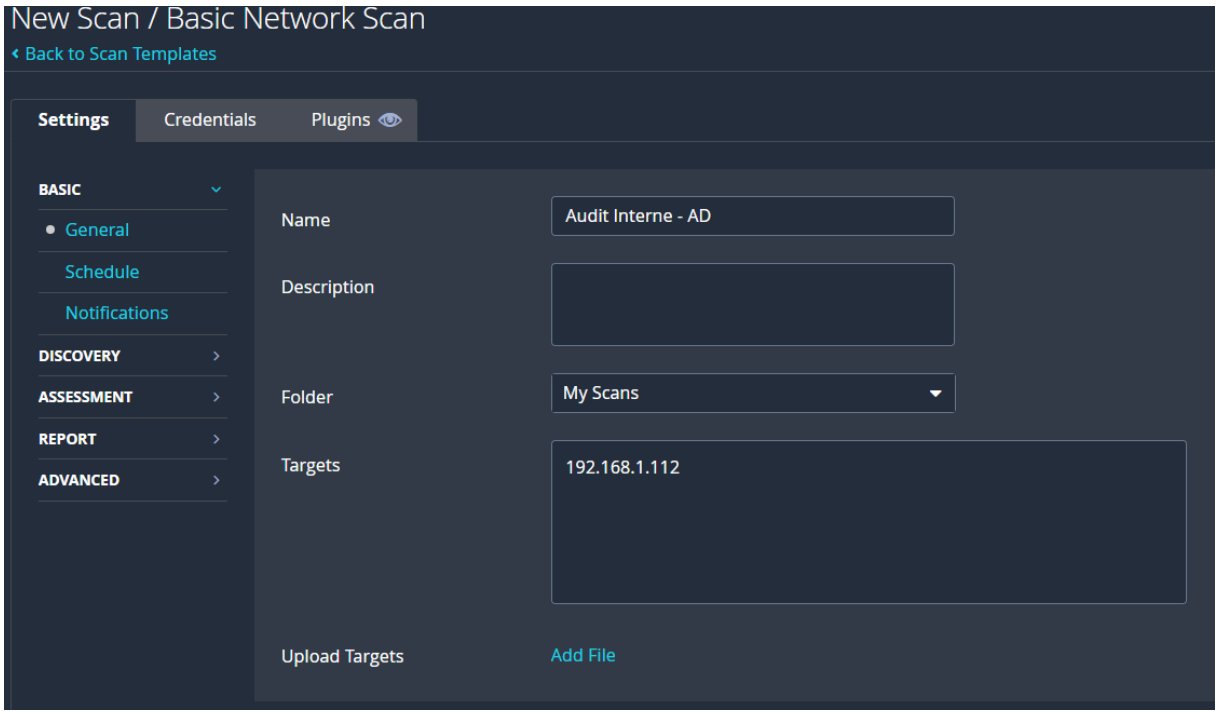


Figure 15 : Paramétrage d'un Basic Network Scan Nessus ciblant le contrôleur de domaine (AD)

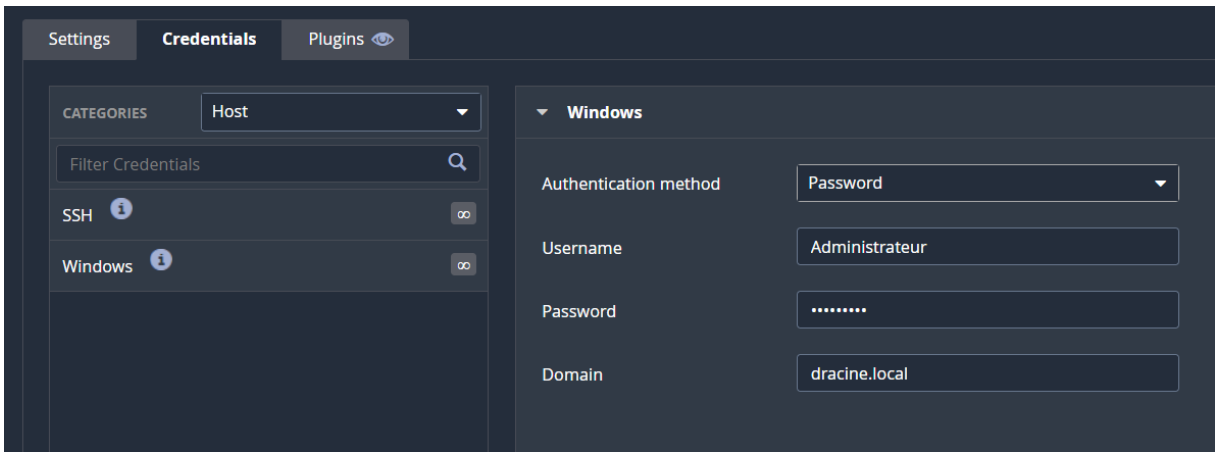


Figure 16 : Injection des identifiants Windows (Credentials) pour un scan authentifié en profondeur

Le scan a notamment révélé une vulnérabilité liée à une version obsolète de Microsoft Visual Studio Code installée sur le serveur, la solution recommandée par Nessus étant de procéder à sa mise à jour vers la version 1.119.1 ou ultérieure. Cette remédiation illustre la valeur opérationnelle de l'audit : identifier des logiciels non liés au cœur de l'infrastructure (ici un éditeur de code) mais qui constituent malgré tout une surface d'attaque supplémentaire sur un serveur critique.

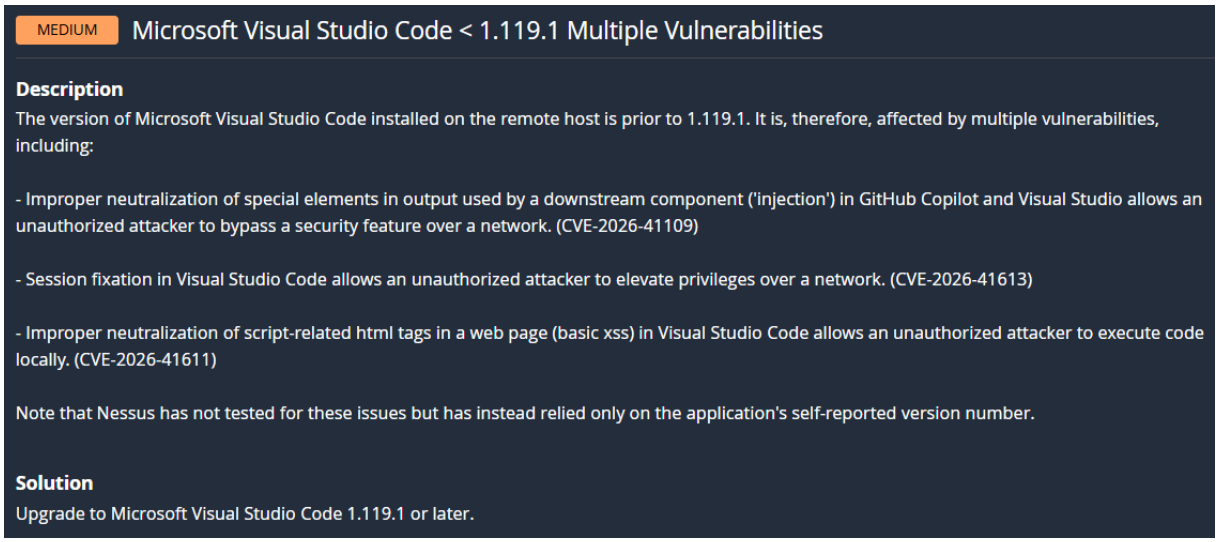


Figure 17 : Résultat du scan - vulnérabilité détectée nécessitant la mise à jour de Microsoft Visual Studio Code vers la version 1.119.1 ou ultérieure

4.9.5 La supervision ciblée

Zabbix : pour surveiller la santé de cette infrastructure, un serveur Zabbix a été déployé sur le VLAN 50 (Supervision). Plutôt qu'une architecture à sondes distribuées, la supervision a été ciblée sur les points critiques de l'infrastructure : le statut CARP du cluster pfSense, le trafic de l'interface WAN, la disponibilité du service DNS et celle du service LDAP/AD DS sur le Windows Server (nombre de threads LDAP actifs, sessions clientes, statut du port LDAP, recherches et écritures par seconde).

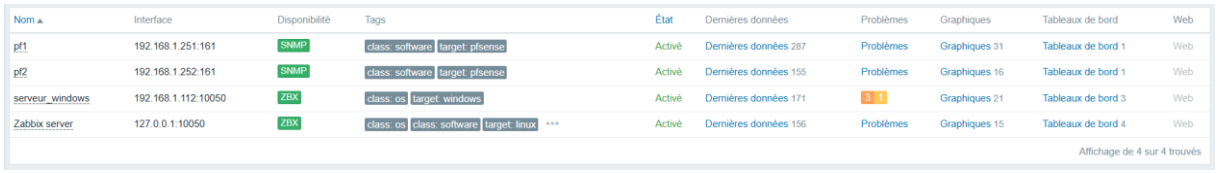


Figure 18 : Tableau de bord Zabbix des hôtes critiques supervisés (serveur Windows, pfSense)

Figure 19 : Supervision du service LDAP/AD DS (threads actifs, sessions clientes)

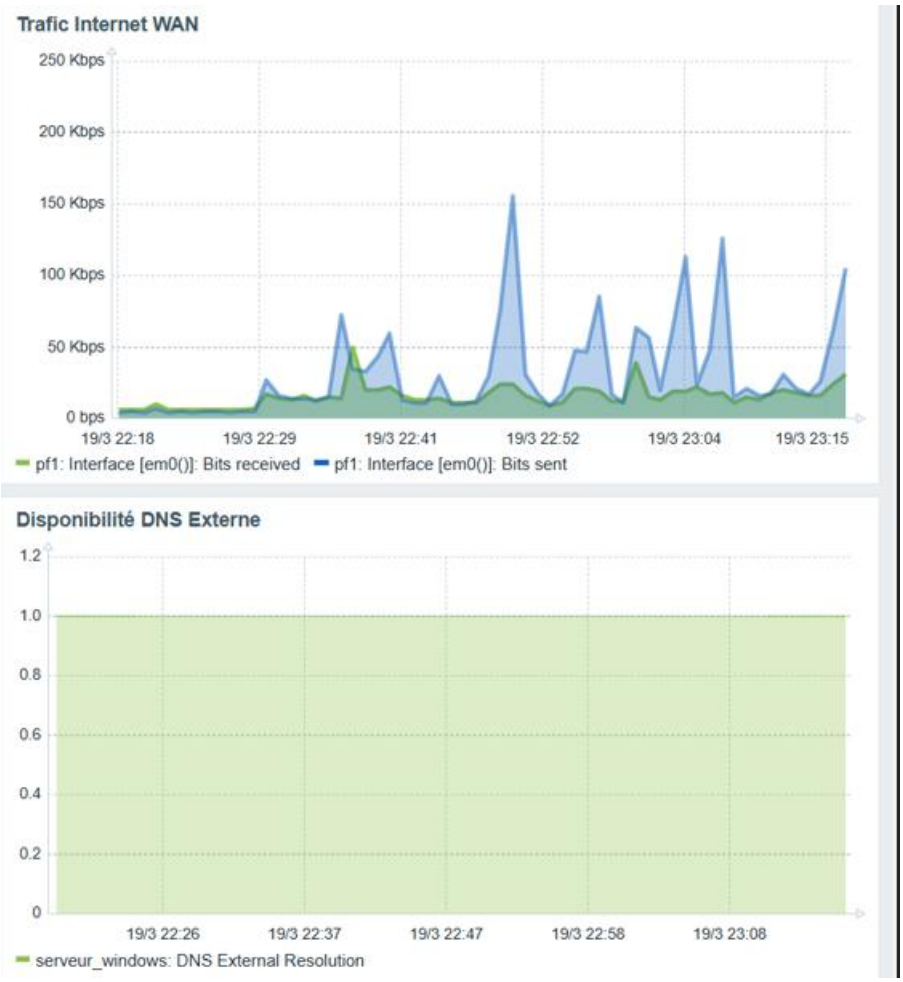


Figure 20 : Supervision du trafic de l'interface WAN pfSense et de la disponibilité du service DNS

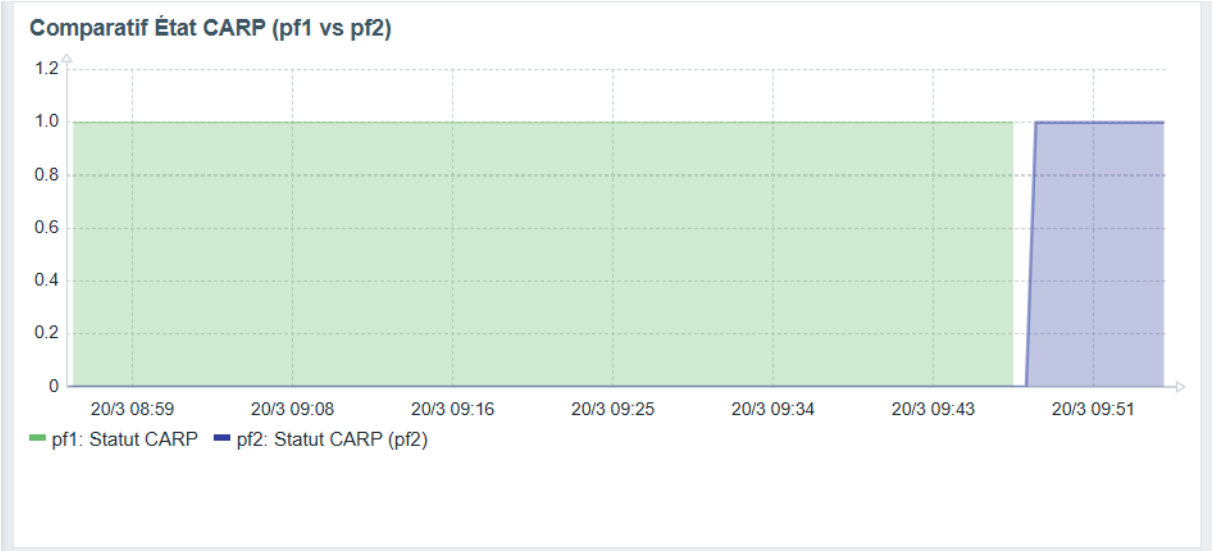


Figure 21 : Supervision de l'état CARP du cluster pfSense

4.9.6 Détection des menaces

Gestion et centralisation des logs (Wazuh) : en complément de la supervision de performance (Zabbix), la supervision de sécurité (SIEM) est assurée par Wazuh, installé sur la même VM du VLAN 50 (Supervision).

Les agents Wazuh déployés sur les serveurs Windows et Linux envoient leurs journaux de sécurité vers le manager central, permettant de détecter les comportements suspects (tentatives de connexion échouées, modifications de fichiers critiques) et de générer des alertes en temps réel, comme cela a pu être observé concrètement lors des tentatives d'authentification LDAP échouées rencontrées en cours de projet.

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	serveur_windows	192.168.1.112	default	Microsoft Windows Server 2022 Standard 10.0.20348.4648	node01	v4.7.5	●	

Figure 22 : Liste des agents Wazuh enrôlés (Windows Server, Guacamole, postes clients)

T1078		Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
T1078	T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
T1078	T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
T1078	T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122

Figure 23 : Détail d'une alerte de sécurité (tentative d'authentification échouée)

4.9.7 Conformité et durcissement (RGPD / ISO 27001 / ANSSI)

Pour garantir le respect des normes (ISO 27001) et du RGPD, le durcissement (hardening) du parc a été mené via le déploiement de stratégies de groupe (GPO) sur les postes du VLAN 30 (Utilisateurs). Trois axes ont été appliqués : une politique de mot de passe renforcée, la restriction des périphériques de stockage amovibles, et le verrouillage automatique des sessions inactives.

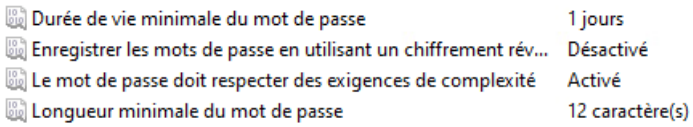


Figure 24 : Stratégie de mot de passe - longueur minimale fixée à 12 caractères

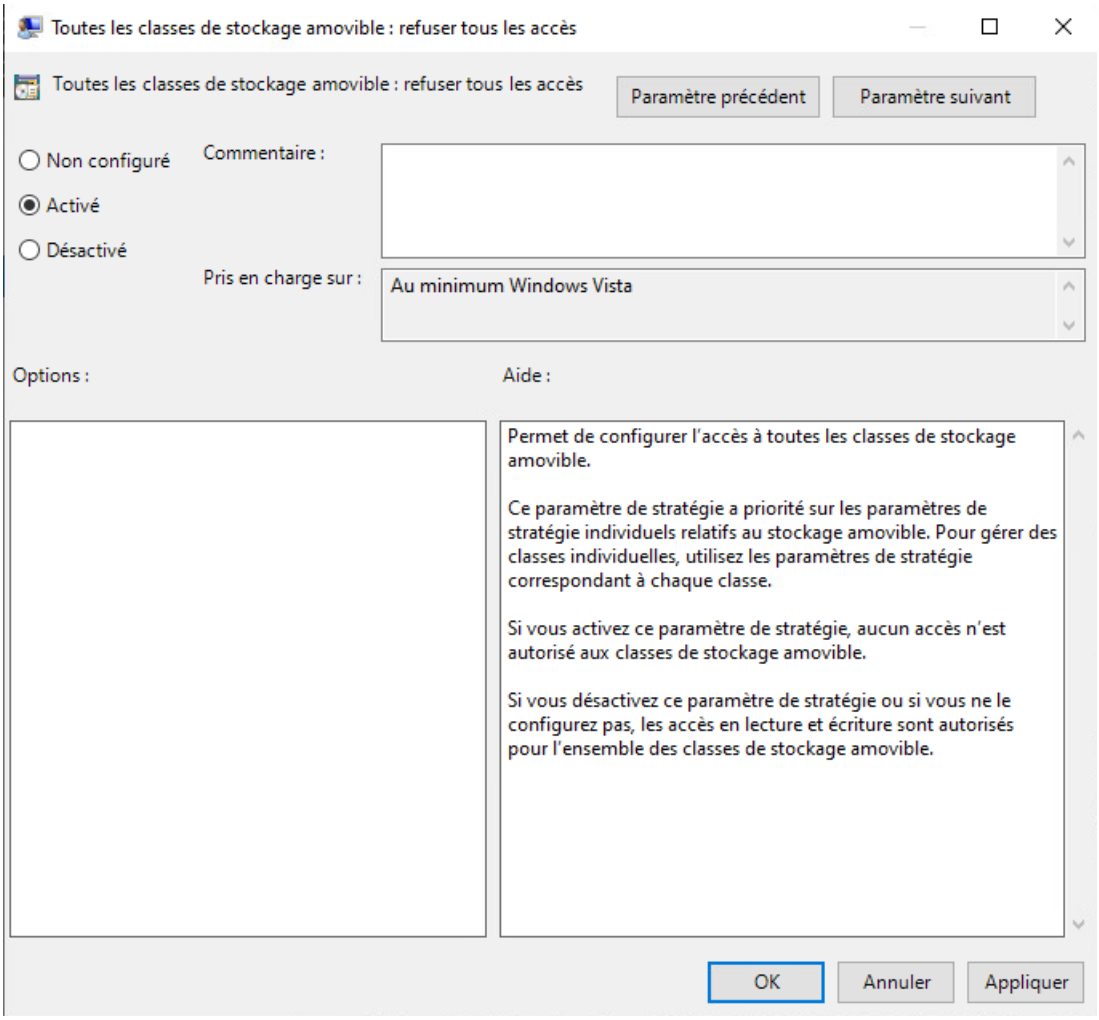


Figure 25 : Stratégie de restriction des périphériques - refus d'accès au stockage amovible activé

Activer l'écran de veille	Activé	Non
Empêcher la sélection de la taille de police du style visuel	Non configuré	Non
Empêcher de modifier la couleur et l'apparence	Non configuré	Non
Empêcher de modifier l'arrière-plan du Bureau	Non configuré	Non
Empêcher de modifier les icônes du Bureau	Non configuré	Non
Empêcher de modifier les pointeurs de la souris	Non configuré	Non
Empêcher de modifier l'écran de veille	Non configuré	Non
Empêcher de modifier les sons	Non configuré	Non
Un mot de passe protège l'écran de veille	Activé	Non
Dépassement du délai d'expiration de l'écran de veille	Activé	Non
Forcer un écran de veille spécifique	Non configuré	Non

Figure 26 : Stratégie d'écran de veille - activation du mot de passe à la reprise et configuration du délai d'expiration

4.9.8 Protection de la donnée

Sauvegarde locale et externalisée (Duplicati, TrueNAS, Backblaze B2) : pour prévenir la perte de données, Duplicati a été déployé sur la VM Supervision, avec deux jobs de sauvegarde distincts conformément à la règle 3-2-1.

Chaque sauvegarde est chiffrée en AES-256 dès la source, avant tout transfert. Un test de restauration a permis de confirmer, empreinte SHA-256 à l'appui, l'intégrité totale des données restaurées.

En amont du job Local, un script planifié (mysqldump) réalise l'export cohérent de la base Zabbix vers un fichier SQL, disponible en annexe. Le dossier ad-backup contient quant à lui le résultat généré par wbadmin (System State), également détaillé en annexe.

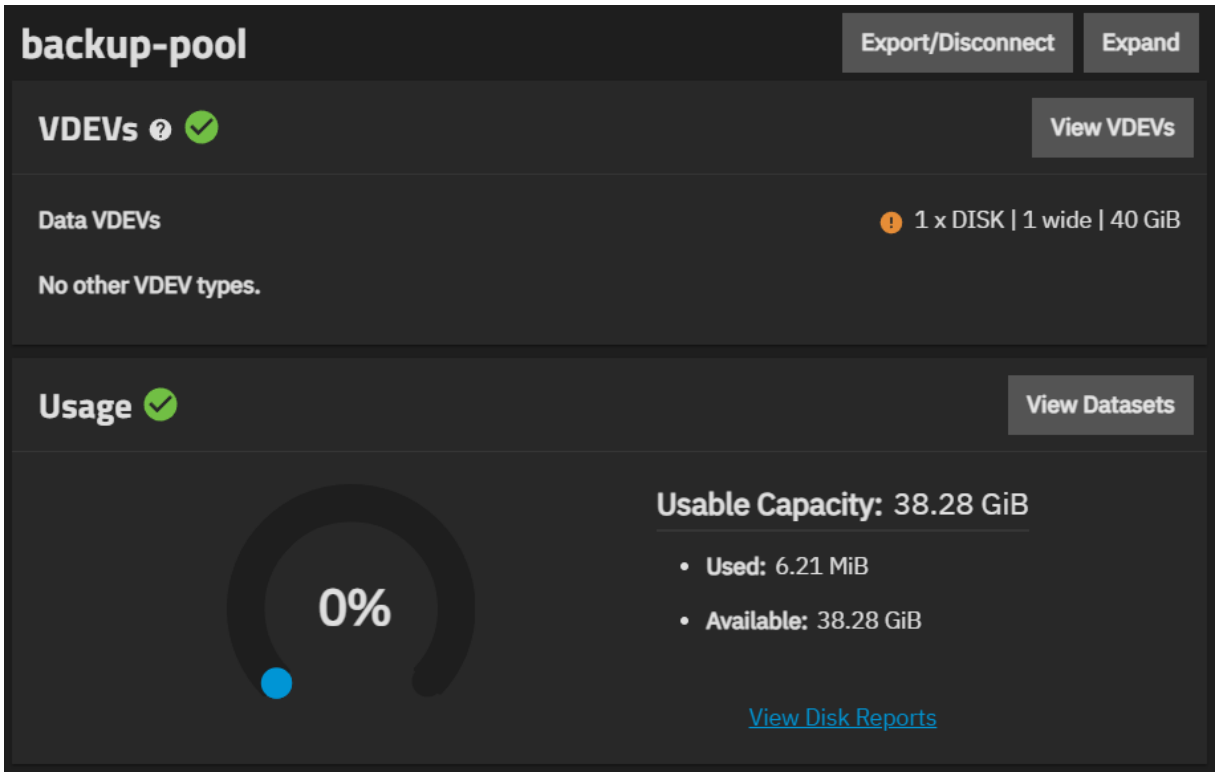


Figure 27 : Pool de stockage TrueNAS (backup-pool) et espace utilisé après le premier run Duplicati

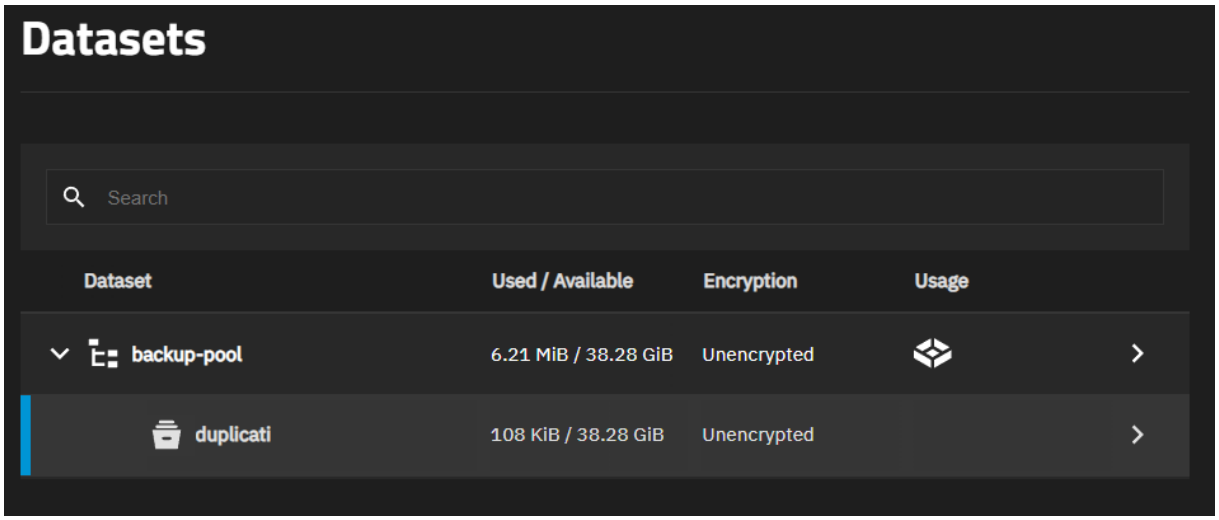


Figure 28 : Dataset dédié (duplicati) sur le pool TrueNAS

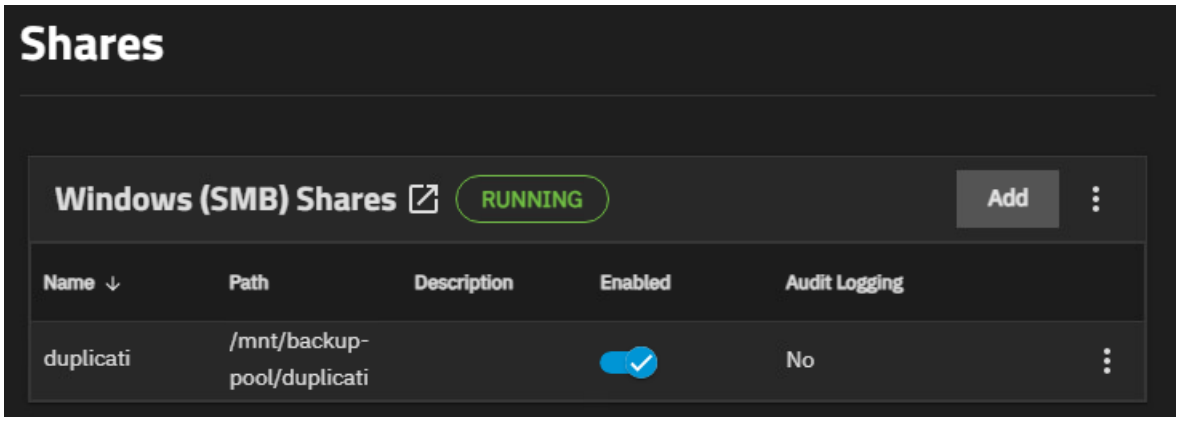


Figure 29 : Partage Windows (SMB) configuré sur TrueNAS

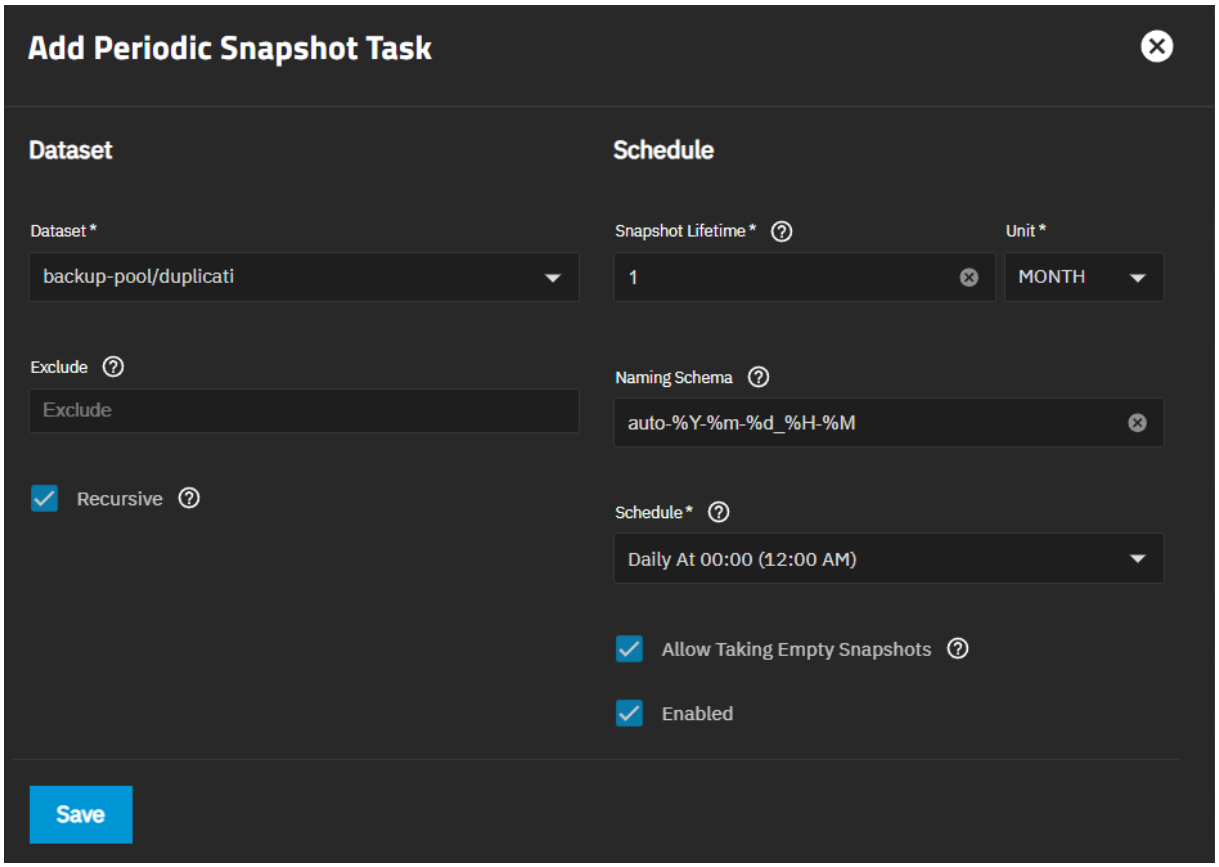


Figure 30 : Tâche de snapshot périodique planifiée sur TrueNAS

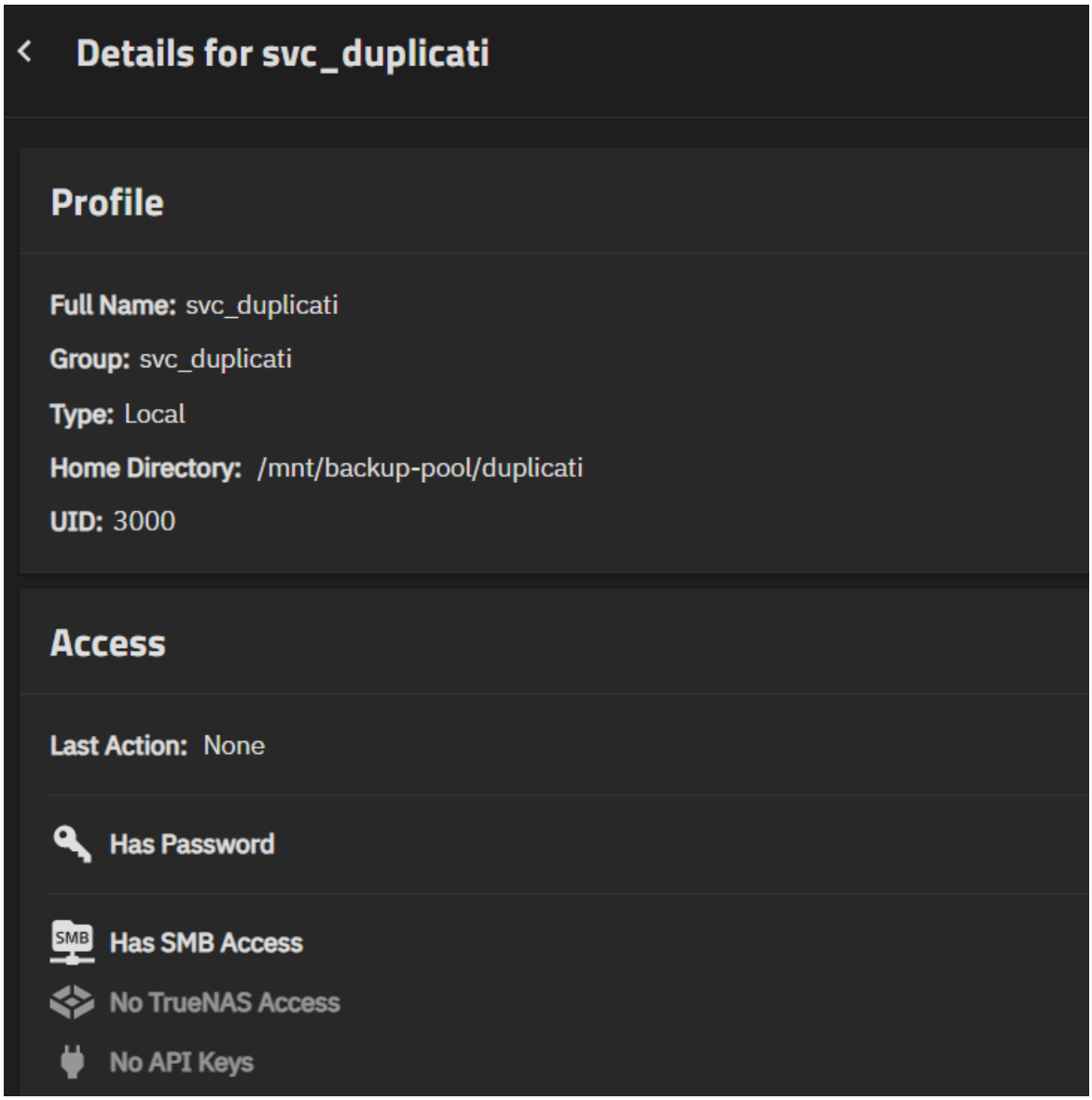


Figure 31 : Compte de service svc_duplicati (droits SMB uniquement)

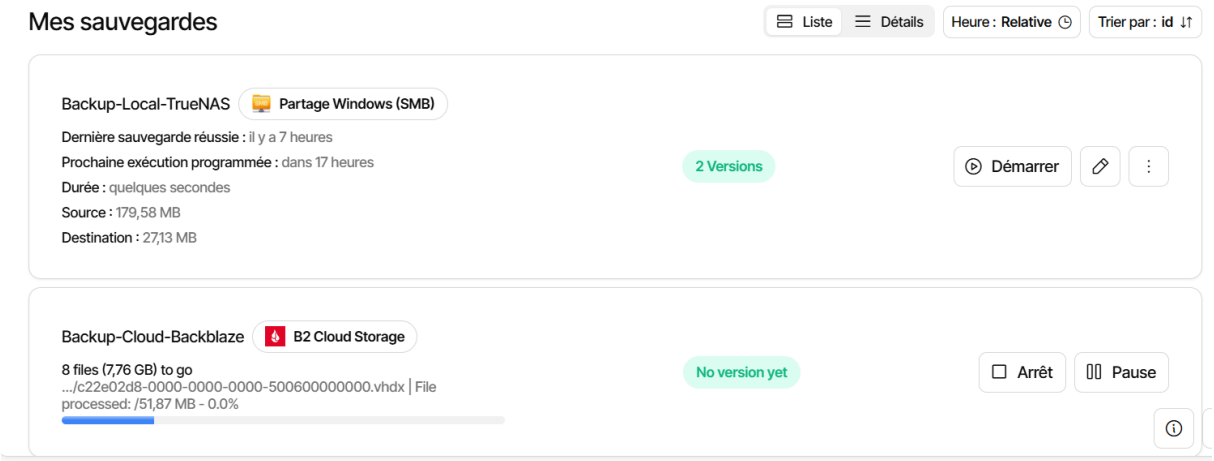


Figure 32 : Vue d'ensemble des deux jobs de sauvegarde Duplicati configurés

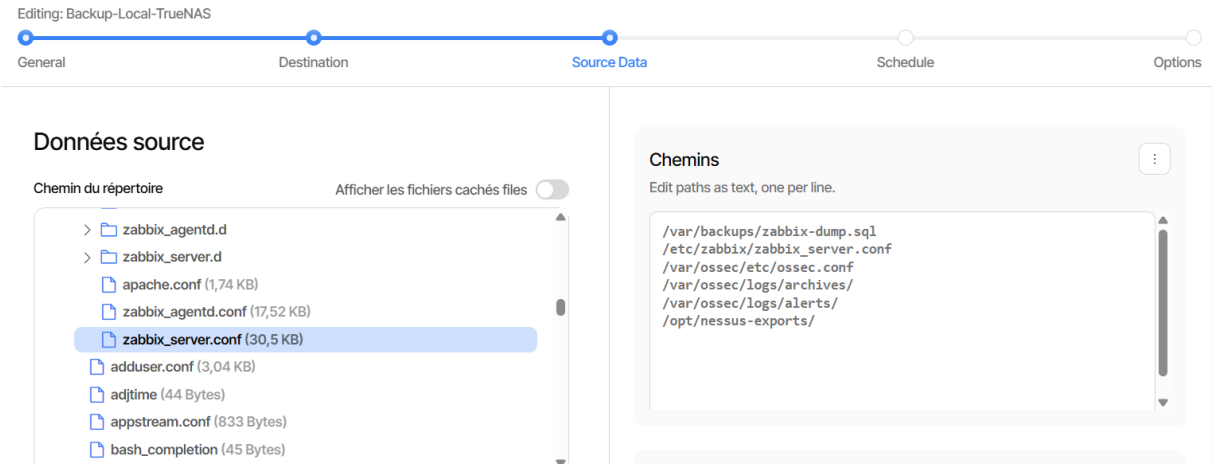


Figure 33 : Configuration du Job 1 Duplicati (Local -> TrueNAS)

Le job 1 « Local » sauvegarde la configuration Zabbix, les journaux Wazuh et les exports Nessus vers un serveur TrueNAS dédié (VLAN 60 - Sauvegardes).

La sauvegarde des rapports de vulnérabilité Nessus nécessite un export manuel préalable vers le répertoire dédié (/opt/nessus-exports/), garantissant ainsi leur inclusion dans le périmètre de sauvegarde de Duplicati.

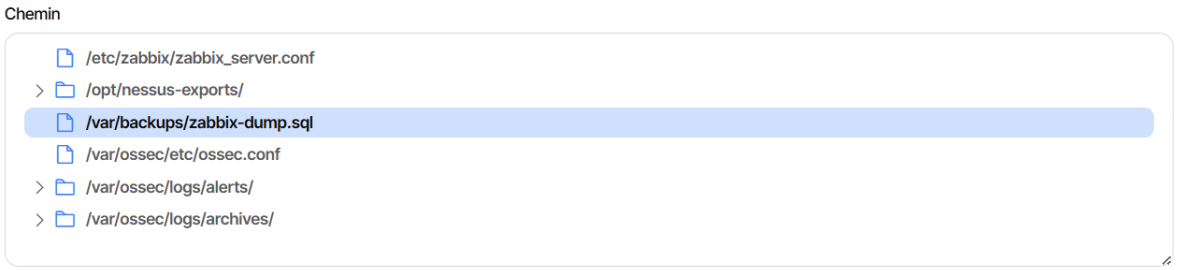


Figure 34 : Test de restauration de la base Zabbix via l'interface web Duplicati

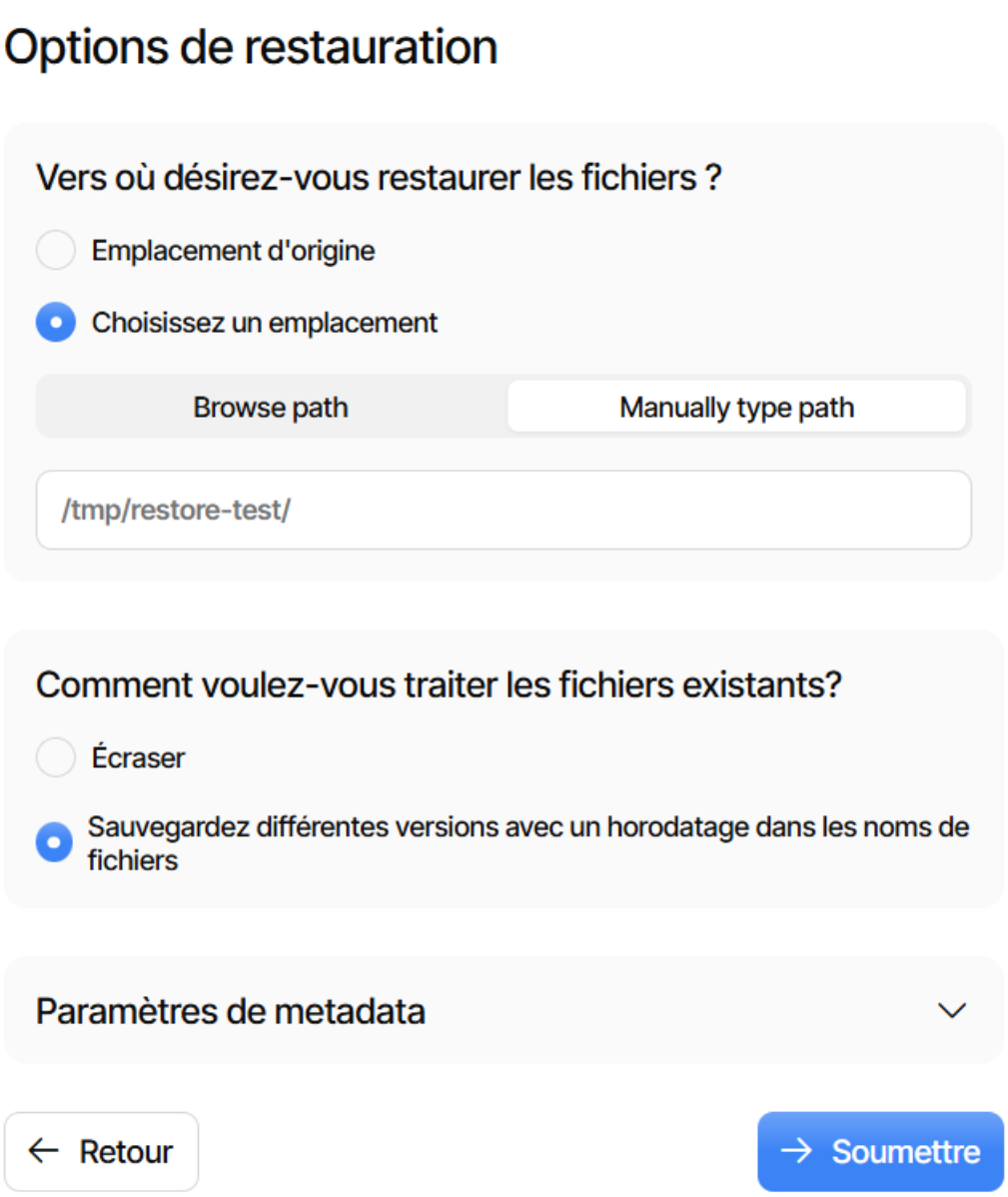


Figure 35 : Sélection du chemin de restauration dans l'assistant Duplicati

```
root@debian:~# ls -la /var/backups/zabbix-dump.sql
-rw-r--r-- 1 root root 41041869 15 juil. 17:45 /var/backups/zabbix-dump.sql
root@debian:~# ls -la /tmp/restore-test/zabbix-dump.sql
-rw-r--r-- 1 root root 41041869 15 juil. 17:45 /tmp/restore-test/zabbix-dump.sql
root@debian:~# sha256sum /var/backups/zabbix-dump.sql /tmp/restore-test/zabbix-d
ump.sql
8fd034ca4b4ef1b14fe59bb36b09b9245223f282e37577a14456812d85f787d6  /var/backups/z
abbix-dump.sql
8fd034ca4b4ef1b14fe59bb36b09b9245223f282e37577a14456812d85f787d6  /tmp/restore-t
est/zabbix-dump.sql
root@debian:~#
```

Figure 36 : Vérification en ligne de commande de l'intégrité du fichier restauré

Afin de valider que la sauvegarde Duplicati n'est pas seulement fonctionnelle en apparence mais garantit une restauration fidèle des données, deux vérifications complémentaires ont été effectuées sur le fichier restauré zabbix-dump.sql.

La commande ls -la affiche les métadonnées d'un fichier, dont sa taille en octets ; elle montre ici que le fichier original (/var/backups/zabbix-dump.sql) et sa copie restaurée (/tmp/restore-test/zabbix-dump.sql) font exactement la même taille (41 041 869 octets), ce qui est un premier indicateur, mais insuffisant à lui seul : deux fichiers de taille identique ne sont pas nécessairement identiques bit à bit.

La commande sha256sum calcule une empreinte unique à partir du contenu exact d'un fichier : la moindre différence, même d'un seul bit, produirait un résultat totalement différent. Le fait que les deux fichiers produisent exactement la même empreinte (8fd034ca4b4ef1b14fe59bb36b09b9245223f282e37577a14456812d85f787d6) constitue la preuve formelle que le fichier restauré est rigoureusement identique à l'original, confirmant que le cycle complet sauvegarde → compression → stockage sur TrueNAS → restauration ne provoque aucune perte ni corruption de données.

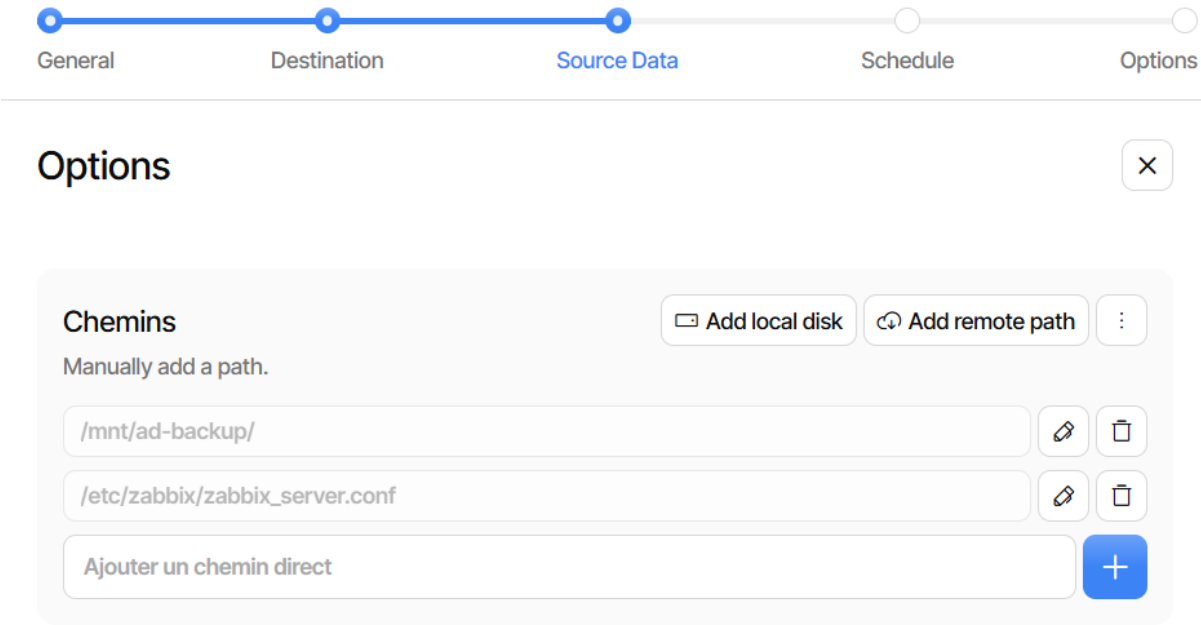


Figure 37 : Configuration du Job 2 Duplicati (Cloud -> Backblaze B2)

Le job 2 « Cloud » externalise en parallèle l'annuaire Active Directory (System State, sauvegardé au préalable via Windows Server Backup) et la configuration Zabbix vers Backblaze B2.

```
PS C:\Users\Administrateur> wbadmin start systemstatebackup -backupTarget:\\192.168.60.10\duplicati\ad-ba
ckup -quiet
wbadmin 1.0 - Outil en ligne de commande de sauvegarde
(C) Copyright Microsoft Corporation. Tous droits réservés.

Démarrage de la sauvegarde de l'état du système [15/07/2026 19:57]...
Récupération des informations de volume...
Cette opération va sauvegarder l'état du système du ou des volumes Réservé au système (100.00 Mo),(C:),(\
\?\Volume{c22e02d8-0000-0000-0000-60dc0e000000}\) vers \\192.168.60.10\duplicati\ad-backup.
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Création d'un cliché instantané des volumes spécifiés pour la sauvegarde...
Veuillez patienter le temps que les fichiers sur l'état du système à sauvegarder
soient identifiés. Cette opération peut prendre plusieurs minutes...
La Sauvegarde Windows Server met à jour la sauvegarde existante pour supprimer les fichiers
qui ont été supprimés du serveur depuis la dernière sauvegarde.
Cette opération peut prendre quelques minutes.
Veuillez patienter le temps que les fichiers sur l'état du système à sauvegarder
soient identifiés. Cette opération peut prendre plusieurs minutes...
(220) fichiers trouvés.
(284) fichiers trouvés.
```

Figure 38 : Commande PowerShell (wbadmin) de sauvegarde du System State Active Directory

La sauvegarde de l'annuaire mérite une précision technique : Windows Server Backup (wbadmin) écrit le System State directement sur un partage réseau SMB hébergé par TrueNAS (chemin UNC \\192.168.60.10\duplicati\ad-backup), sans jamais transiter par la VM Linux.

Cette dernière monte séparément ce même partage en local (CIFS, point de montage /mnt/ad-backup) : Duplicati y lit alors les fichiers comme s'ils étaient locaux, avant de les inclure dans le job Cloud vers Backblaze. TrueNAS agit ainsi comme point de rendez-vous entre les deux systèmes, sans qu'aucune connexion directe Windows/Linux ne soit nécessaire.

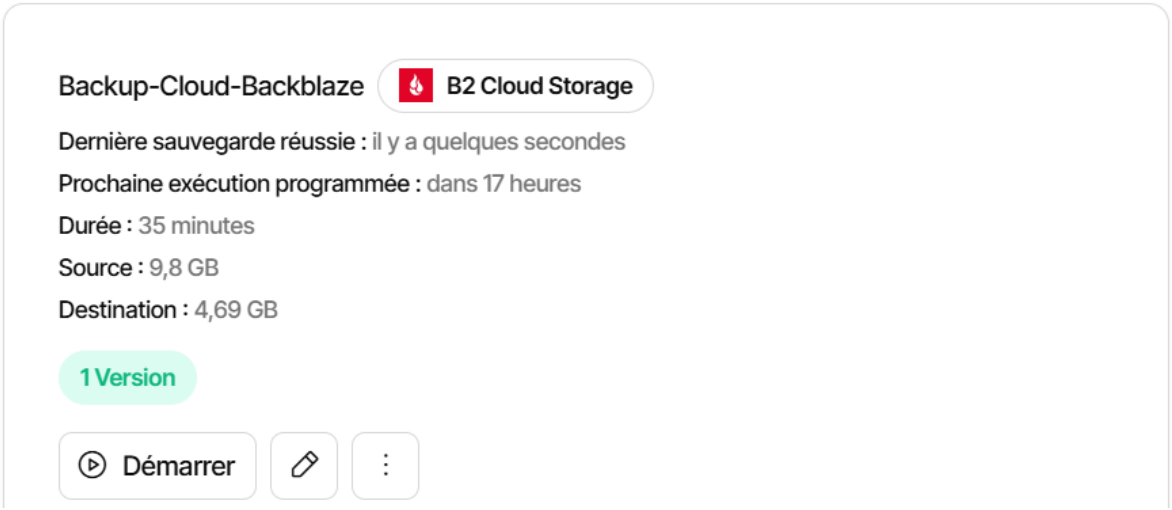


Figure 39 : Résultat du premier run Duplicati : statut Success, taille transférée, durée

4.9.9 Le rempart final

Le PRA et TrueNAS-secours : l'étape finale est le plan de reprise d'activité. Le trafic transite par un tunnel OpenVPN Site-à-Site chiffré vers le site de secours (Aubervilliers). Les fichiers de sauvegarde (configuration, journaux, annuaire) y sont répliqués vers un second serveur TrueNAS (VLAN 110), dont le pool ZFS en mirror génère des snapshots immuables en lecture seule. Cette réplication native ZFS (zfs send/receive via SSH) est planifiée chaque nuit à 5h00, avec une rétention de 15 jours côté destination, offrant une protection contre les attaques par ransomware.

La mise en place de cette réplication ZFS nécessite au préalable l'établissement d'une connexion SSH sécurisée par clés asymétriques entre le serveur TrueNAS de production et celui de secours. Une fois cette liaison établie, la tâche de réplication peut être configurée :

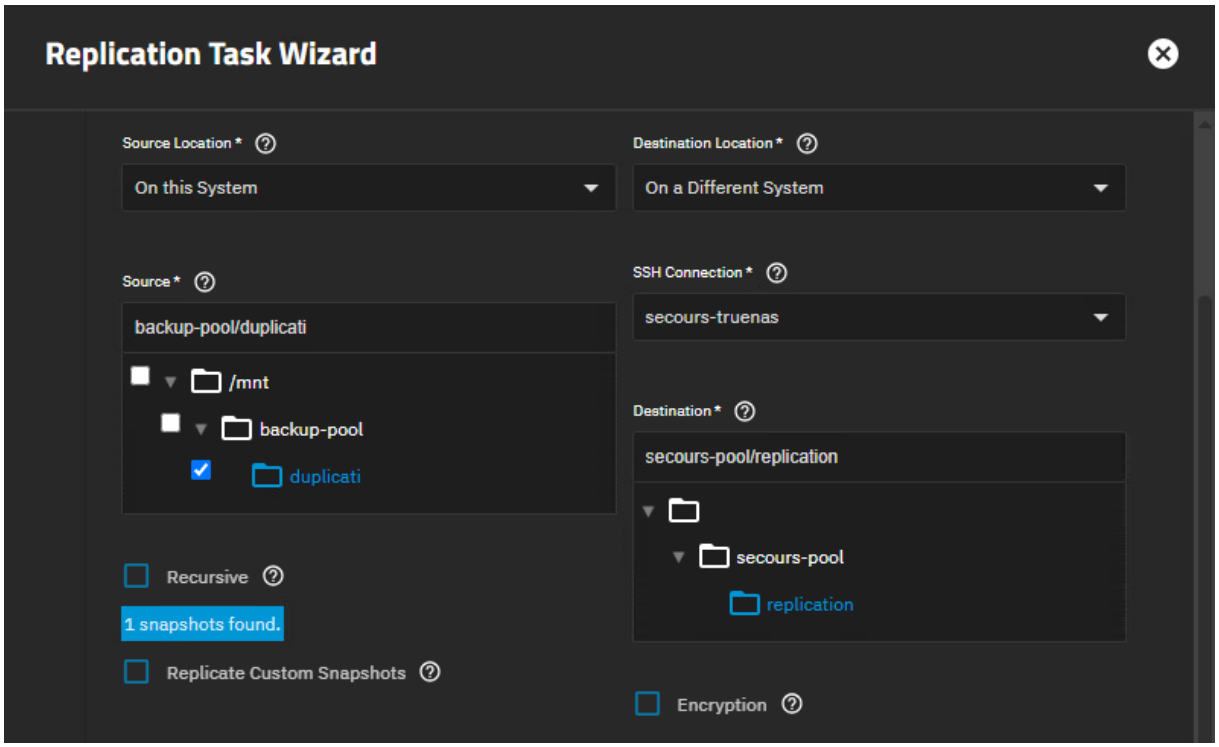


Figure 40 : Tâche de réplication ZFS planifiée (source, destination)

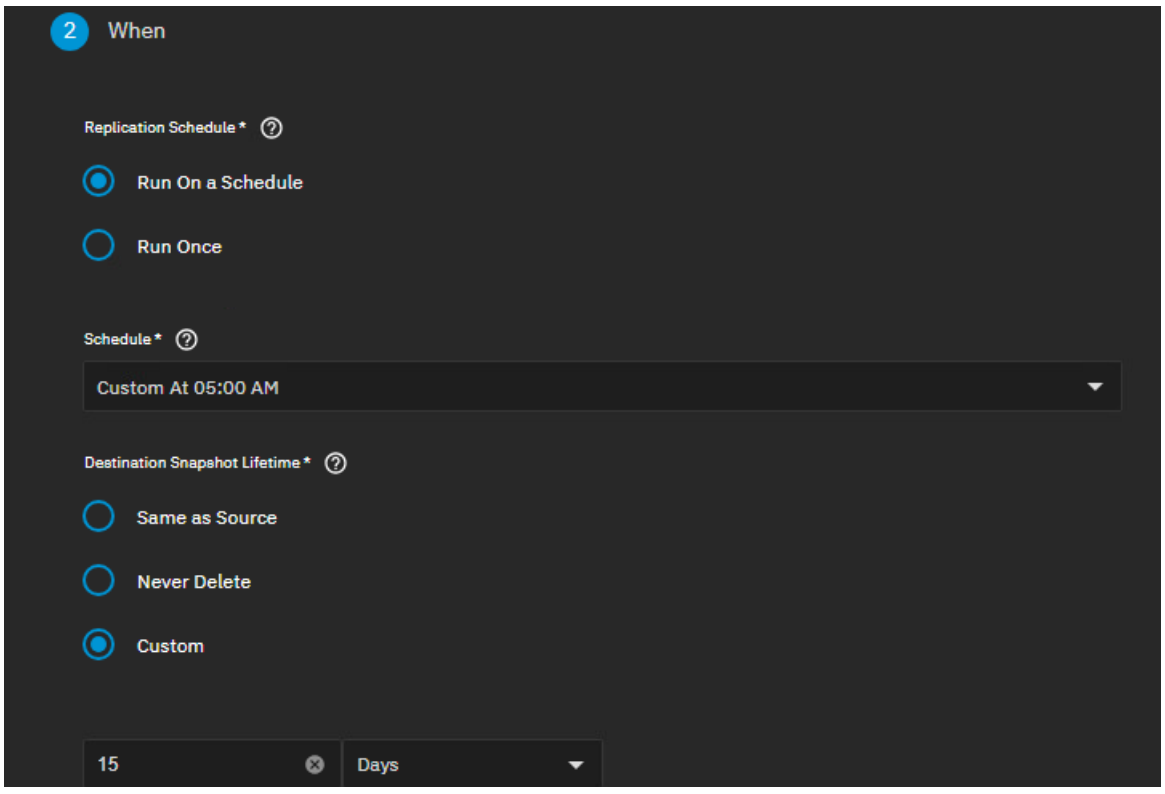


Figure 41 : Tâche de réplication ZFS planifiée (horaire)

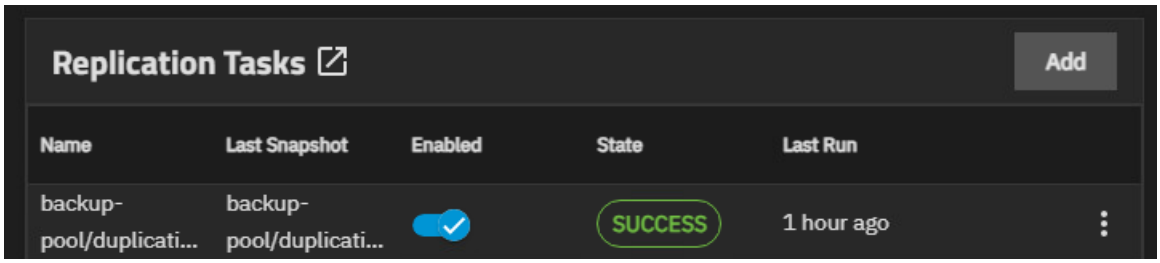


Figure 42 : Résultat d'une exécution de la réplication et contenu répliqué côté TrueNAS-secours

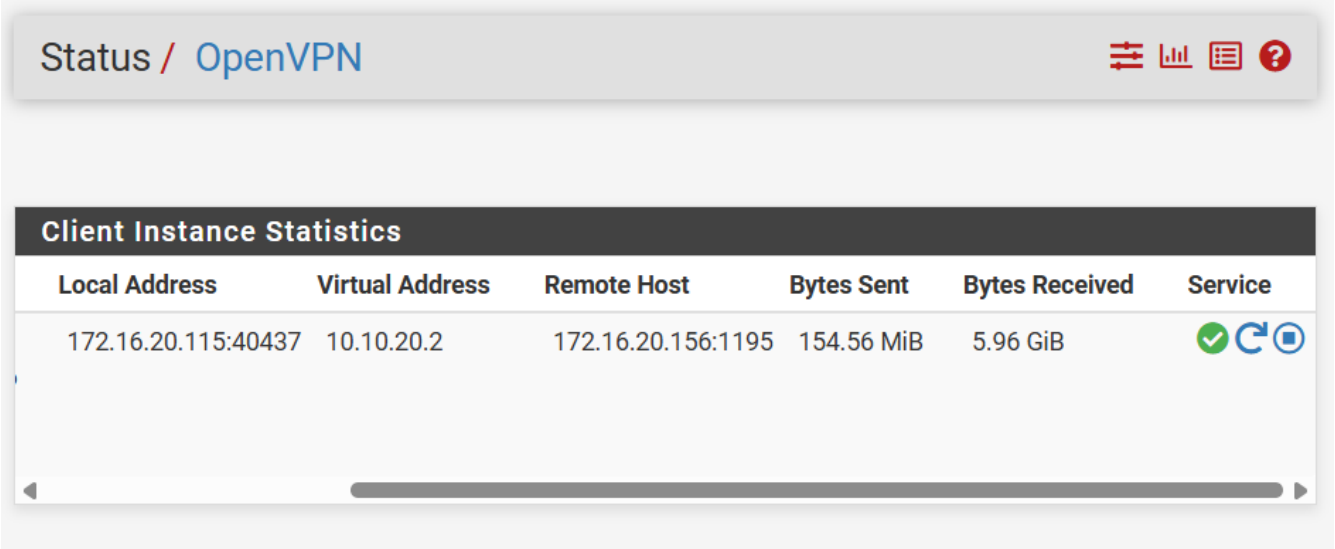


Figure 43 : Statut du tunnel VPN Site-à-Site sur le pfSense de secours

Validation de Veeam Backup & Replication (test préalable)

En complément de la réplication ZFS, une validation de Veeam Backup & Replication a été menée en amont sur une architecture comparable (cluster pfSense, contrôleur Active Directory, serveur applicatif Debian), avant l'intégration sur l'infrastructure finale du projet.

L'hôte ESXi de secours a d'abord été déclaré dans l'inventaire Veeam, puis l'hôte ESXi de production a été ajouté selon le même paramétrage, les deux étant gérés en mode standalone, sans vCenter Server.

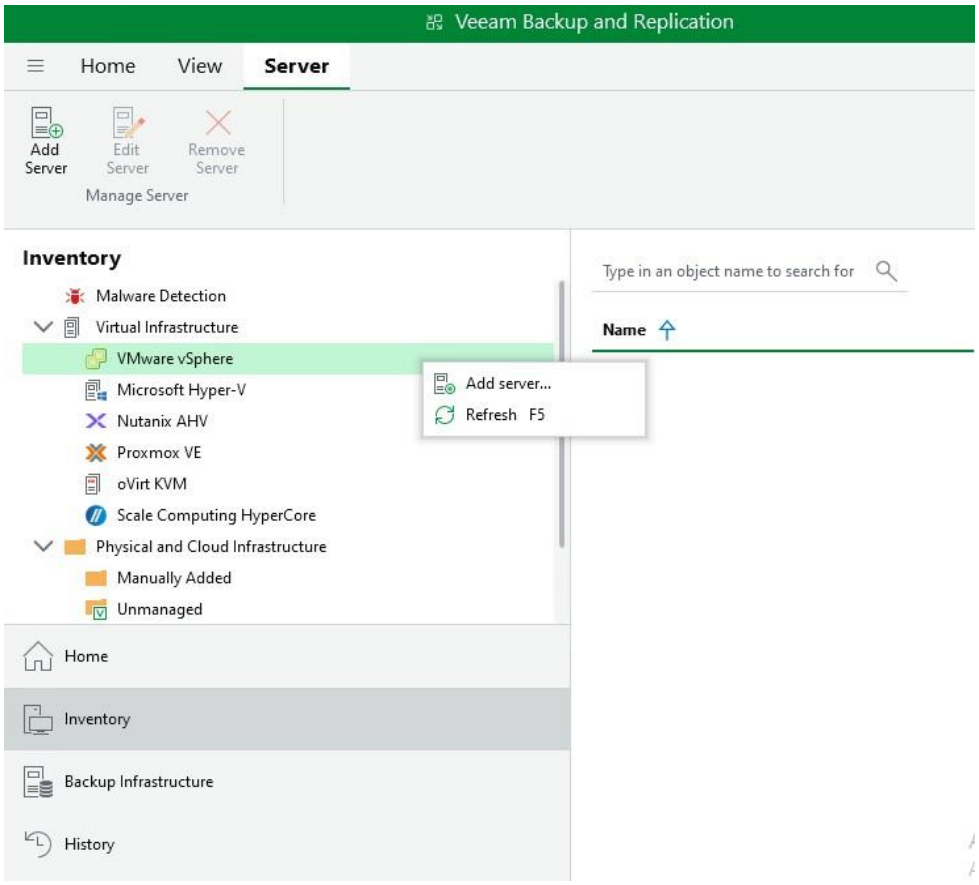


Figure 44 : Onglet Inventory de Veeam - menu contextuel « Add Server » pour déclarer un hôte VMware

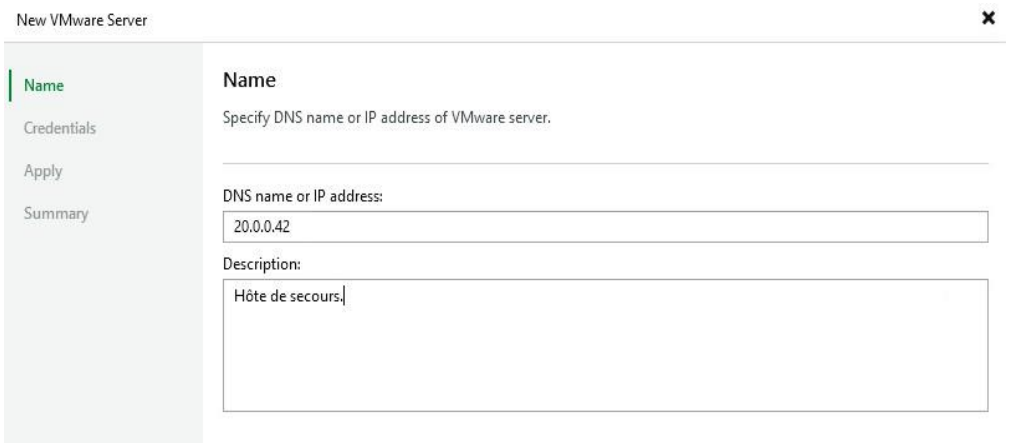


Figure 45 : Ajout de l'hôte ESXi de secours dans l'inventaire Veeam, avec sa description

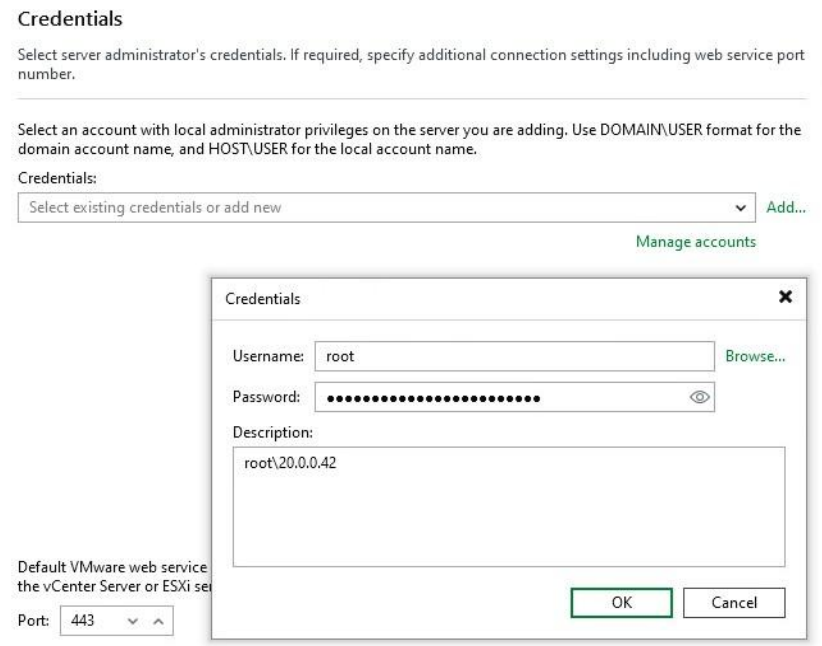


Figure 46 : Saisie des identifiants administrateur (compte root) pour l'hôte ESXi de secours

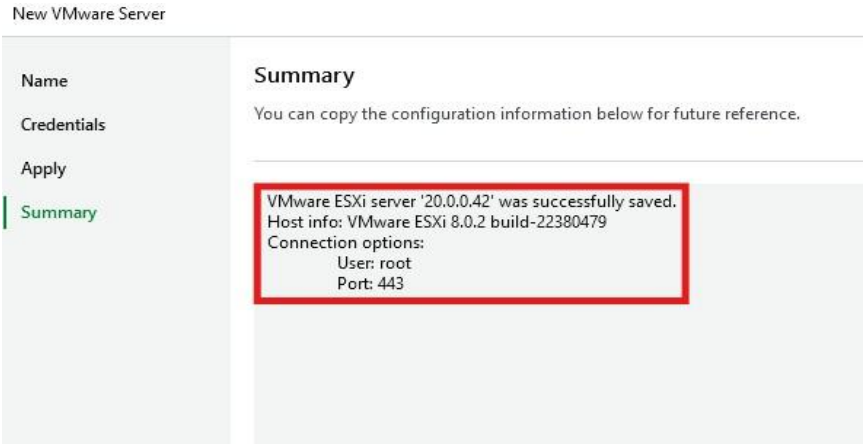


Figure 47 : Résumé de la connexion réussie à l'hôte ESXi de secours (VMware ESXi 8.0.2, port 443)

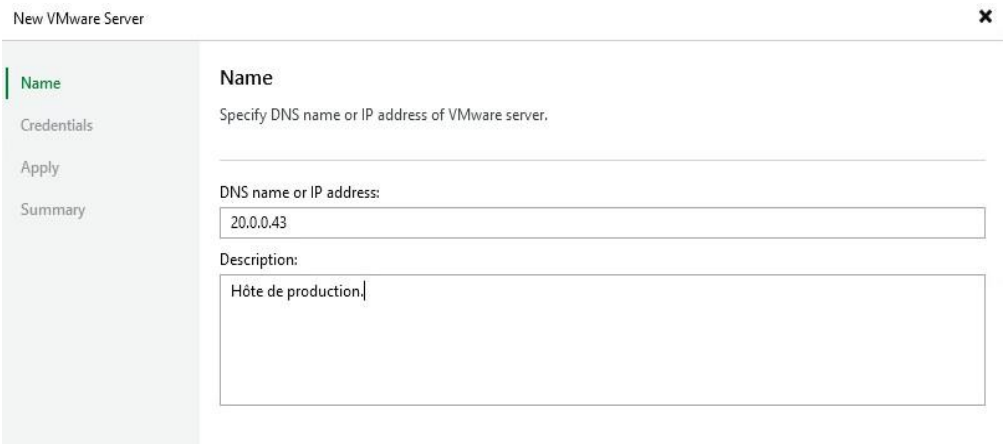


Figure 48 : Ajout de l'hôte ESXi de production, paramétrage identique à l'hôte de secours

Un job de réplication a ensuite été créé, ciblant les quatre machines virtuelles critiques du lab (les deux pare-feux pfSense, le contrôleur AD et le serveur Debian), pour un volume total de 110 Go. Le test de Guest Processing a confirmé un traitement réussi pour le serveur AD (agent Windows), un échec attendu pour les VM non-Windows qui ne supportent pas nativement cette fonctionnalité. Le job a été planifié pour s'exécuter toutes les deux heures, avec trois tentatives automatiques en cas d'échec.

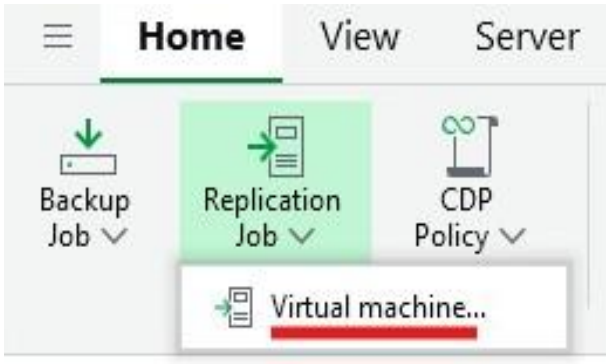


Figure 49 : Création d'un nouveau job de réplication depuis le menu Home de Veeam

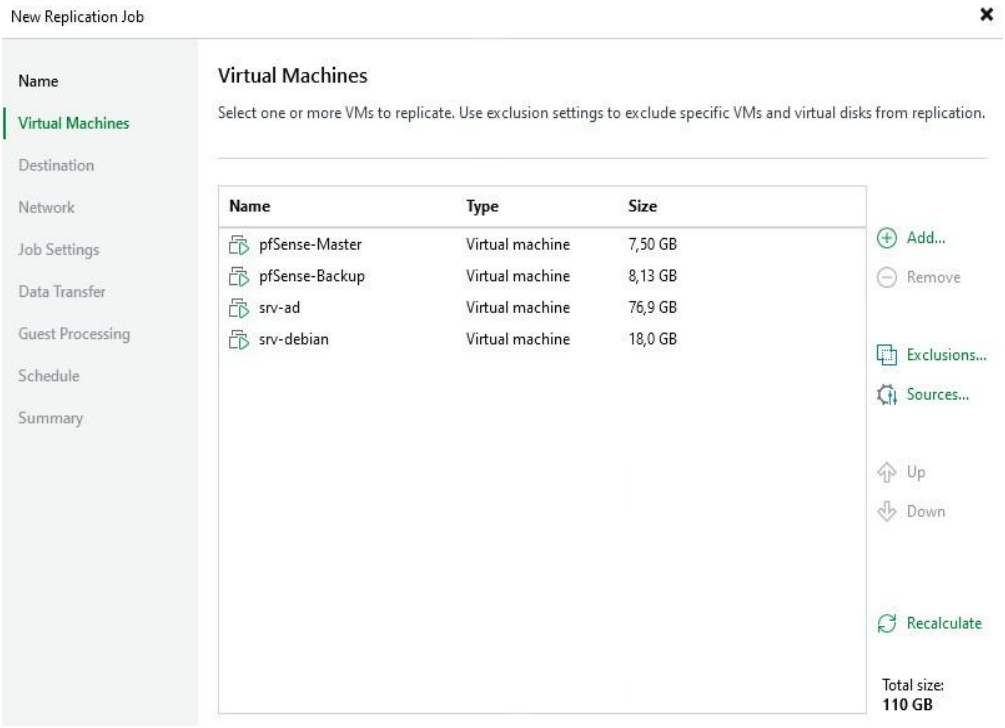


Figure 50 : Sélection des quatre machines virtuelles critiques à répliquer - taille totale 110 Go

Figure 51 : Résultat du test Guest Processing - succès pour le serveur AD, échec attendu pour pfSense et le serveur Debian (non-Windows)

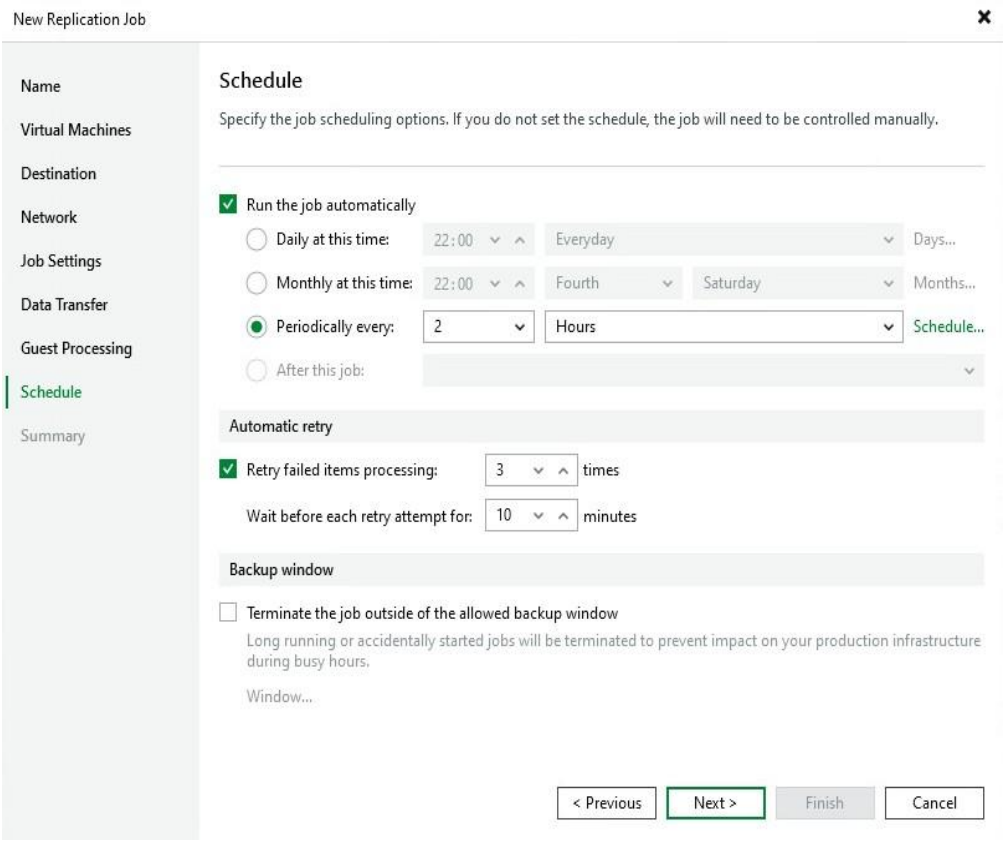


Figure 52 : Planification du job de réplication - exécution toutes les 2 heures avec 3 tentatives automatiques

La première sauvegarde complète a traité 138,9 Go en 48 minutes (débit de 42 Mo/s, 4 VM en succès), tandis qu'une sauvegarde incrémentielle suivante n'a nécessité que 1,7 Go en moins de 7 minutes grâce au Changed Block Tracking (CBT), qui n'identifie que les blocs modifiés depuis le dernier point de restauration.

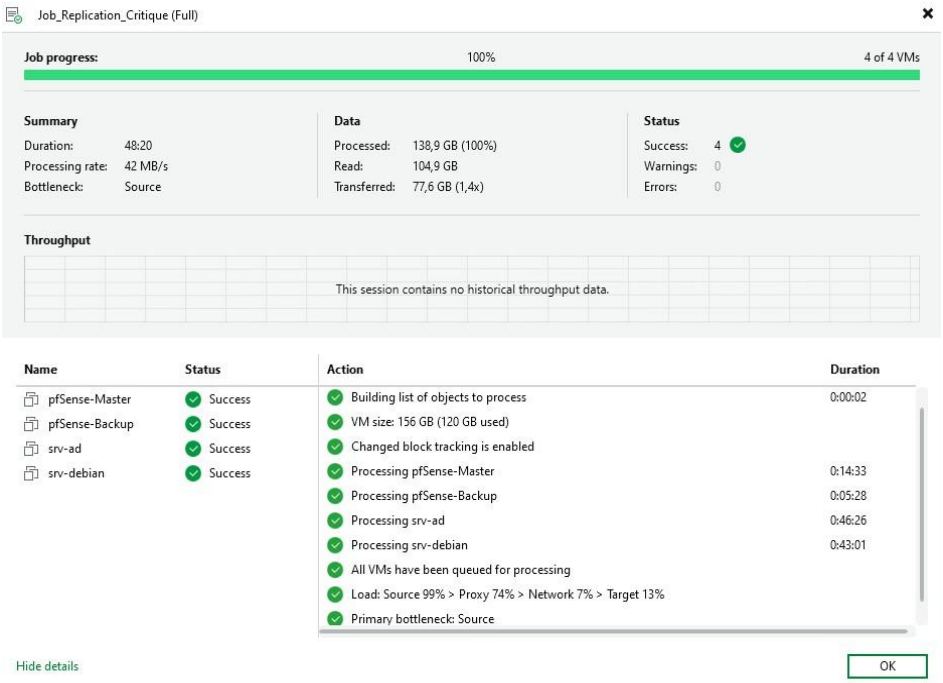


Figure 53 : Rapport de la sauvegarde complète initiale - 138,9 Go traités en 48 min, 4/4 VM en succès, débit 42 Mo/s

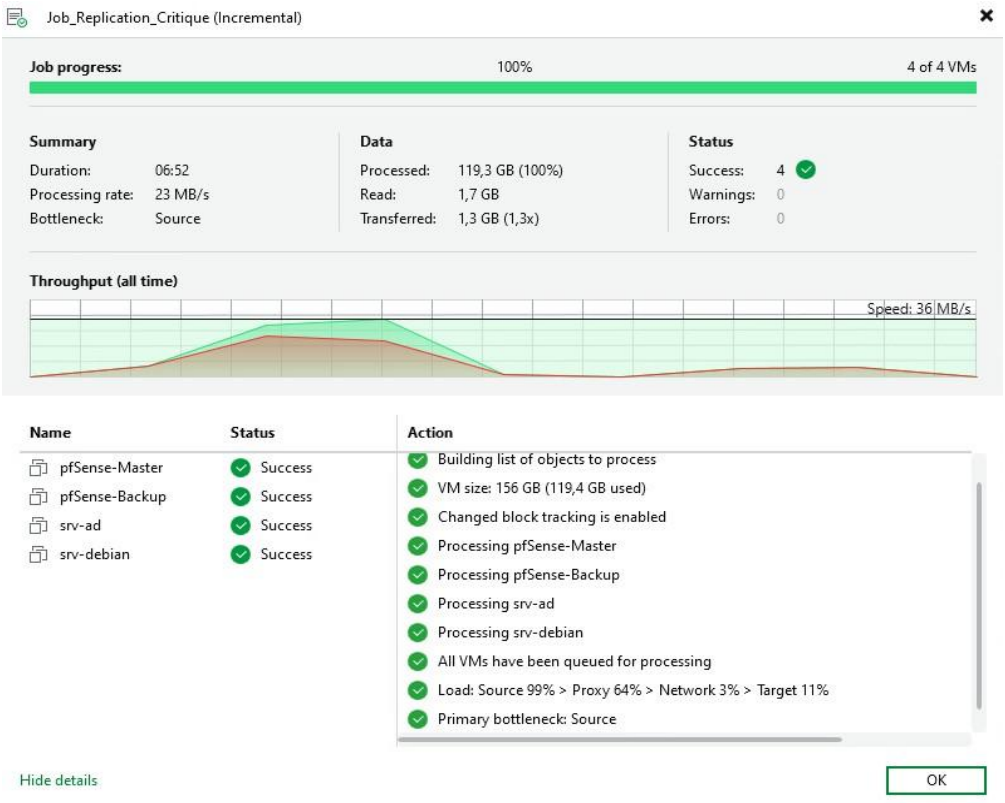


Figure 54 : Rapport de la sauvegarde incrémentielle - 1,7 Go traité en 6 min 52 s grâce au CBT

Un test de failover complet a ensuite été réalisé : le tableau de bord affichait les quatre réplicas en statut « Failover », avec deux points de restauration disponibles par VM. L'assistant de bascule a demandé de motiver le déclenchement (« Désastre, le site principal ne répond plus ! ») avant de démarrer effectivement les quatre VM répliquées sur l'hôte de secours.

Un test de failback, permettant de resynchroniser les réplicas vers le site de production une fois celui-ci rétabli, a également été initié.

Figure 55 : Tableau de bord Veeam - 4 réplicas en statut Failover, 2 points de restauration par VM

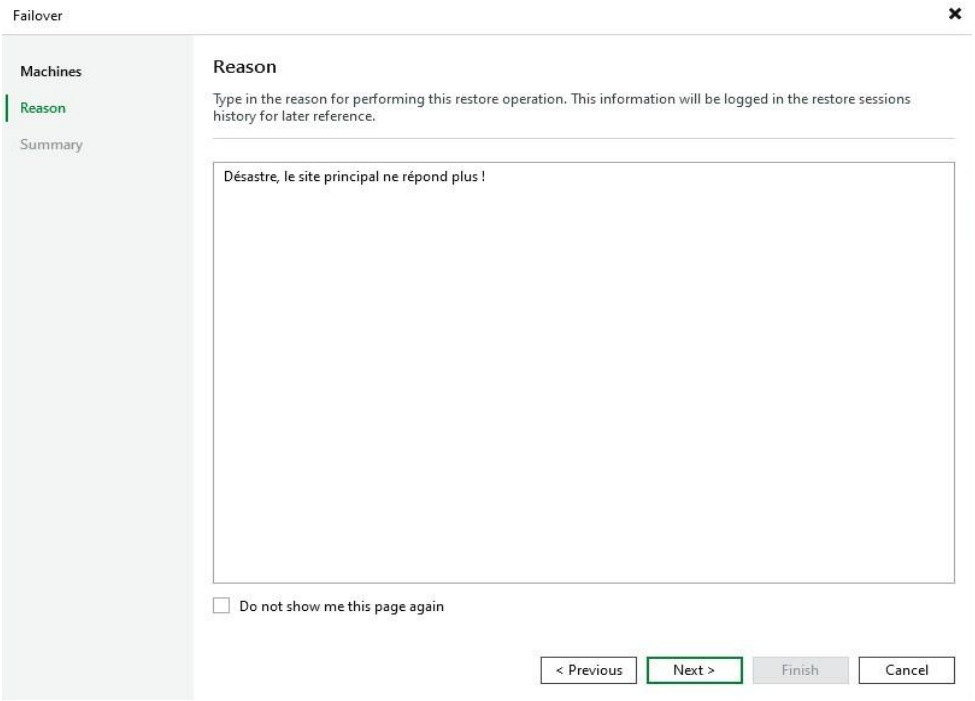


Figure 56 : Saisie de la raison du basculement dans l'assistant Failover

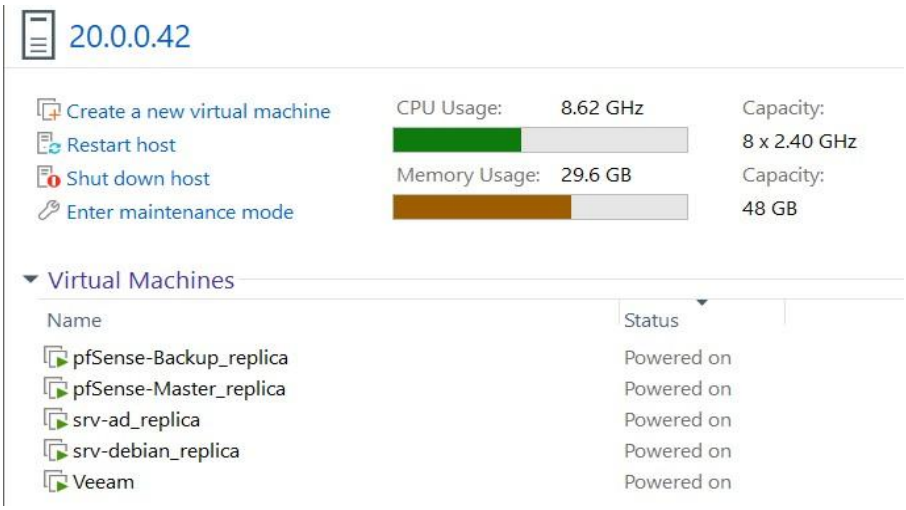


Figure 57 : Hôte ESXi de secours - les 4 VM réplicas et Veeam démarrés et en cours d'exécution

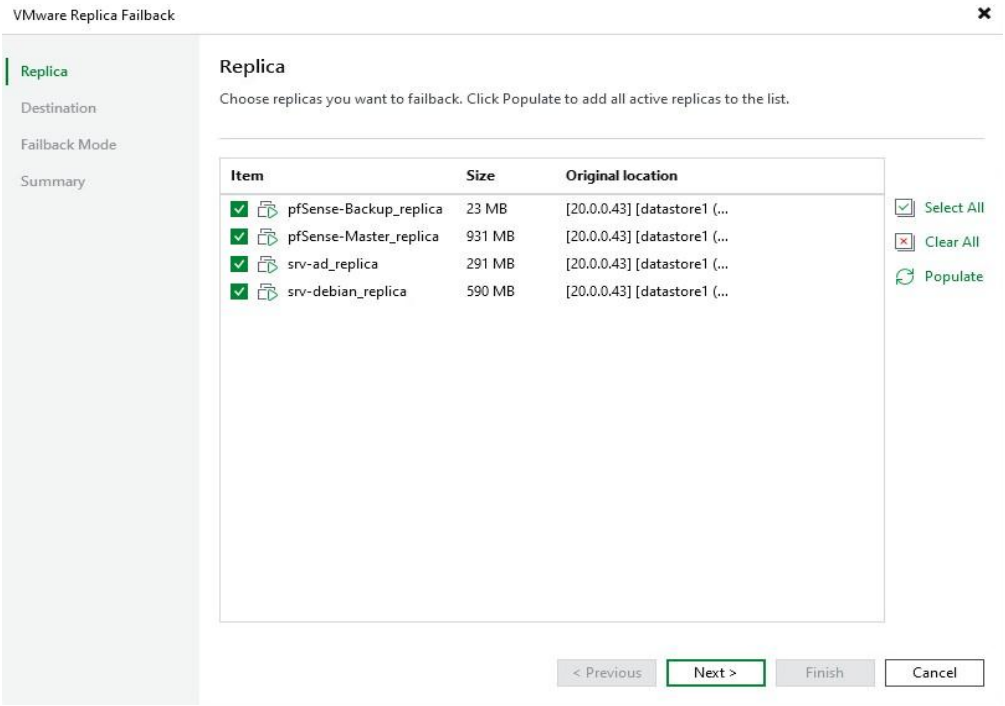


Figure 58 : Assistant Failback - sélection des 4 réplicas à resynchroniser vers le site de production

5 Conclusion

Ce projet répondait à un besoin concret de Kali-Brazza : une infrastructure informatique jusque-là peu sécurisée, peu surveillée et sans réelle continuité de service, alors même que l'activité du cabinet repose entièrement sur la disponibilité de ses outils numériques.

La mise en place du cluster pfSense en haute disponibilité (CARP/pfSync) a apporté la continuité de service recherchée, tandis que la centralisation de l'authentification via Active Directory, le VPN couplé au bastion Apache Guacamole et la segmentation en VLAN ont considérablement réduit la surface d'attaque.

Les briques de supervision (Zabbix, Wazuh) et d'audit (Nessus) donnent désormais à l'IT une visibilité qu'elle n'avait pas, et le couple Duplicati/Backblaze associé au PRA sur le site de secours d'Aubervilliers sécurise durablement les données de l'agence, y compris contre un scénario de ransomware.

La méthode Scrumban, déclinée en six sprints courts, a permis d'avancer de façon itérative sur un projet technique dense, en validant chaque brique avant de passer à la suivante tout en gardant la flexibilité nécessaire pour absorber les aléas rencontrés en cours de route.

Sur le plan personnel, ce projet m'a permis de mettre en pratique, sur un cas réel, l'ensemble des compétences que j'ai développées en administration systèmes, réseaux et sécurité : conception réseau, haute disponibilité, gestion des identités, durcissement système et supervision. Il m'a également confronté à des problématiques de gestion de projet (arbitrages budgétaires, priorisation du backlog…) qui dépassent le strict cadre technique.

Plusieurs pistes d'amélioration restent envisageables pour la suite : ajout d'une sonde IDS/IPS (Suricata) sur le cluster pfSense, automatisation du déploiement des VM par de l'Infrastructure as Code, mise en place d'un second contrôleur de domaine AD pour renforcer la haute disponibilité de l'annuaire, ainsi qu'une augmentation des ressources du site secondaire afin de permettre une réplication IP parfaite (mêmes VLAN, autant de VLAN pfSense que sur le site principal).

6 Glossaire

Active Directory (AD) : Service d'annuaire développé par Microsoft. Il permet de centraliser la gestion des identités, des droits d'accès et des politiques de sécurité pour l'ensemble des utilisateurs et ordinateurs du réseau.

AES-256 (Advanced Encryption Standard) : Algorithme de chiffrement symétrique utilisant une clé de 256 bits. Il est reconnu comme l'un des standards de cryptographie les plus robustes pour sécuriser la confidentialité des données.

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information. Autorité française chargée d'accompagner et de sécuriser le développement du numérique, notamment en éditant des référentiels et des guides de bonnes pratiques.

RGPD (Règlement Général sur la Protection des Données) : règlement européen de 2018 imposant aux organisations des mesures techniques et organisationnelles pour protéger les données personnelles qu'elles traitent.

ISO 27001 : norme internationale de référence en matière de management de la sécurité de l'information (SMSI), définissant un ensemble de mesures de sécurité organisées en annexes.

Apache Guacamole (ou Bastion) : Passerelle d'accès à distance (bastion) permettant de se connecter de manière sécurisée et tracée aux serveurs internes (via les protocoles RDP ou SSH) directement depuis un navigateur web, sans exposer directement les ports du réseau interne.

Backblaze / S3 : Service de stockage cloud de type objet (compatible avec le standard S3). Utilisé dans ce projet pour l'externalisation des sauvegardes afin de garantir la disponibilité des données hors site.

CARP (Common Address Redundancy Protocol) : Protocole réseau de redondance permettant à plusieurs routeurs ou pare-feux (ici, pfSense) de partager une même adresse IP virtuelle. Il assure la haute disponibilité en basculant automatiquement le trafic vers un équipement de secours en cas de panne du maître (failover).

Chiffrement : Procédé de cryptographie consistant à transformer une donnée lisible en un format inintelligible, nécessitant une clé spécifique pour être déchiffrée et exploitée.

Cluster : Grappe de serveurs ou d'équipements réseau configurés pour fonctionner de concert, augmentant ainsi la tolérance aux pannes et la disponibilité globale des services.

DMZ (Zone Démilitarisée) : Sous-réseau informatique isolé de part et d'autre par des pare-feux, servant de zone tampon entre le réseau interne de l'entreprise (LAN) et Internet. Elle héberge les services devant être accessibles depuis l'extérieur.

Duplicati : Logiciel de sauvegarde open source permettant de chiffrer les données à la source avant de les transférer de manière automatisée vers un espace de stockage distant.

Failover (Bascule) : Processus automatisé par lequel un équipement ou un système de secours prend le relais d'un composant principal défaillant, garantissant la continuité de service.

GPO (Group Policy Object) : Stratégie de groupe Microsoft permettant d'appliquer, de distribuer et de forcer de manière centralisée des configurations de sécurité et des restrictions (ex : verrouillage des sessions, blocage des ports USB) sur les postes membres du domaine.

LDAP (Lightweight Directory Access Protocol) : Protocole réseau standard permettant d'interroger et de modifier un annuaire centralisé pour l'authentification et l'autorisation des utilisateurs.

Nessus : Outil professionnel d'évaluation des vulnérabilités. Il analyse les systèmes et le réseau pour identifier les failles de sécurité, les erreurs de configuration et les correctifs logiciels manquants.

pfSense : Solution de pare-feu et de routage open source basée sur le système d'exploitation FreeBSD. Elle assure la protection du périmètre réseau, le filtrage des flux et la gestion des VPN.

PRA (Plan de Reprise d'Activité) : Ensemble de procédures techniques et organisationnelles documentées, conçues pour restaurer rapidement le système d'information de l'entreprise après un sinistre majeur (cyberattaque, incendie).

Ransomware (Rançongiciel) : Logiciel malveillant qui bloque l'accès aux données d'une organisation (généralement par un chiffrement fort) et exige le paiement d'une rançon pour en restituer l'accès.

Remédiation : Ensemble des actions correctives appliquées sur un système d'information (application de patchs, reconfiguration) suite à la découverte d'une vulnérabilité.

SIEM (Security Information and Event Management) : Solution de sécurité (comme Wazuh) permettant de collecter, corréler et analyser en temps réel les journaux d'événements (logs) pour détecter et alerter sur les incidents de sécurité.

SNMP (Simple Network Management Protocol) : Protocole de communication permettant à un serveur de supervision de collecter des métriques d'état et de performance (CPU, statut des interfaces) sur des équipements réseau distants.

TrueNAS / ZFS : TrueNAS est un système d'exploitation orienté stockage réseau (NAS). ZFS est le système de fichiers sous-jacent, reconnu pour sa robustesse, sa détection automatique de la corruption des données et sa gestion optimisée des snapshots.

VLAN (Virtual Local Area Network) : Réseau local virtuel permettant de segmenter logiquement une infrastructure réseau physique en plusieurs domaines de diffusion isolés, limitant ainsi la surface d'attaque et améliorant les performances.

VPN (Virtual Private Network) : Technologie établissant un tunnel chiffré et authentifié sur un réseau public (Internet), permettant d'interconnecter des sites distants ou de sécuriser les accès nomades.

Zabbix : Plateforme logicielle open source de supervision réseau et applicative. Elle permet de surveiller la disponibilité, la capacité et la santé des équipements en temps réel via le déploiement de sondes ou d'agents.

Zero Trust : Modèle d'architecture de sécurité fondé sur le principe du "ne jamais faire confiance, toujours vérifier". Toute tentative d'accès au réseau ou aux ressources nécessite une authentification et une autorisation strictes et continues, quelle que soit la provenance de la connexion (interne ou externe).

7 Webographie

Sécurité / réglementaire

https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-mise-en-oeuvre-dun-systeme-de-journalisation/ (ANSSI-PA-012, export des logs)

https://www.cnil.fr/fr/la-cnil-adopte-une-recommandation-relative-aux-mesures-de-journalisation (CNIL, durée de conservation des logs)

Matériel et tarifs (budget 4.7.2)

https://www.netgate.com/appliances (boîtiers Netgate 4200/2100)

https://www.backblaze.com/cloud-storage/pricing (tarifs Backblaze B2)

https://www.idealo.fr (comparateur, licence Windows Server)

https://www.tenable.com/products/nessus/nessus-essentials (Nessus Essentials, gratuit ≤16 IP)

pfSense / réseau

https://docs.netgate.com/pfsense/en/latest/ (documentation officielle pfSense CE)

Active Directory / Guacamole

https://guacamole.apache.org/doc/gug/ldap-auth.html (extension guacamole-auth-ldap)

Supervision / SIEM

https://www.zabbix.com/documentation (Zabbix)

https://documentation.wazuh.com/ (Wazuh)

Sauvegarde / stockage

https://github.com/duplicati/duplicati (Duplicati, releases et documentation)

https://www.truenas.com/docs/scale/ (TrueNAS SCALE)

https://www.veeam.com/community-edition-free-backup.html (Veeam Backup & Replication Community Edition)

8 Annexes

Annexe A - Scripts de sauvegarde

1. Sauvegarde automatisée de la base Zabbix (dump SQL planifié)

Ce script réalise un export cohérent de la base de données Zabbix avant chaque exécution du job Duplicati, afin d'éviter toute incohérence liée à une copie de fichiers bruts pendant que la base est active. Il est placé sur la VM Supervision, dans /usr/local/bin/dump-zabbix.sh :

```
#!/bin/bash
mkdir -p /var/backups
mysqldump --single-transaction -u root -p'MotDePasseRoot' zabbix > /var/backups/zabbix-dump.sql
```

Le script est rendu exécutable puis planifié quotidiennement via crontab, à 2h50 du matin (10 minutes avant le job Duplicati de 3h00) :

```
chmod +x /usr/local/bin/dump-zabbix.sh

# Entrée crontab (crontab -e) :
50 2 * * * /usr/local/bin/dump-zabbix.sh
```

2. Sauvegarde du contrôleur de domaine (System State via Windows Server Backup)

Sur le contrôleur de domaine, la fonctionnalité Windows Server Backup est installée puis utilisée pour sauvegarder le System State (annuaire Active Directory) directement vers un partage réseau hébergé sur le TrueNAS local (VLAN 60). Les identifiants du partage sont d'abord enregistrés dans le gestionnaire d'identification Windows, afin que la tâche planifiée puisse s'authentifier sans intervention humaine :

```
Install-WindowsFeature Windows-Server-Backup

cmdkey /add:192.168.60.10 /user:svc_duplicati /pass:MotDePasseDuCompte

wbadmin start systemstatebackup -backupTarget:\\192.168.60.10\duplicati\ad-backup -quiet
```

Cette commande est ensuite planifiée quotidiennement via le Planificateur de tâches Windows (exécution « que l'utilisateur soit connecté ou non »), déclenchant chaque nuit une sauvegarde complète du System State vers le partage \\192.168.60.10\duplicati\ad-backup. Le contenu généré est ensuite lu par la VM Supervision (montage CIFS local sous /mnt/ad-backup) puis inclus dans le job Duplicati « Cloud » à destination de Backblaze B2.

Annexe B - Règles de pare-feu (version réelle, contrainte de ressources)

Le tableau ci-dessous synthétise les règles de pare-feu réellement appliquées sur les trois pare-feux du projet. Les règles du site principal (pf1 Master et pf2 Backup) sont identiques sur les deux nœuds grâce à la synchronisation de configuration XMLRPC ; seul le site de secours dispose d'un jeu de règles propre, plus restreint, en l'absence de cluster HA à cet endroit.

VLAN / Interface	Règle	Justification
Site principal - pf1 (Master) et pf2 (Backup) - configuration identique répliquée par XMLRPC Config Sync		
VLAN10 - Admin (10.0.10.0/24)		
VLAN10	Allow -> VLAN50 VIP (80/443, 8834, 443)	Accès admin aux consoles web Zabbix, Nessus et Wazuh
VLAN10	Allow -> VLAN20 (8200, 3389)	Accès à la console Duplicati et RDP admin vers le Windows Server
VLAN10	Allow -> DMZ VIP (443)	Administration du portail Guacamole
VLAN10	Allow -> This Firewall (443)	Accès WebGUI pfSense
VLAN10	Block -> any	Règle finale, moindre privilège
VLAN20 - Serveurs (192.168.1.0/24)		
VLAN20	Allow -> VLAN50 VIP (10051, 1514)	Remontée agents Zabbix/Wazuh du serveur vers la supervision
VLAN20	Allow -> WAN (443)	Duplicati vers Backblaze B2 / mises à jour Windows
VLAN20	Allow -> VLAN60 (445)	Sauvegarde locale (wbadmin, Duplicati) vers TrueNAS
VLAN20	Block -> VLAN30	Un serveur n'initie jamais vers les postes utilisateurs
VLAN20	Block -> any	Règle finale
VLAN30 - Utilisateurs (192.168.30.0/24)		
VLAN30	Allow -> VLAN20 VIP (88, 389, 445, 53, 123)	Authentification AD, LDAP, SMB, DNS, NTP
VLAN30	Allow -> VLAN50 VIP (1514, 1515)	Agent Wazuh du poste
VLAN30	Allow -> any (80, 443)	Navigation Internet via NAT
VLAN30	Block -> VLAN10	Pas d'accès direct à l'administration
VLAN30	Block -> DMZ	Passe par le VPN + Guacamole, jamais en direct
VLAN30	Block -> any	Règle finale
DMZ (172.16.40.0/24)		
DMZ	Allow -> VLAN20 VIP (3389)	Guacamole relaie une session RDP vers le serveur
DMZ	Allow -> VLAN30 (3389)	Guacamole relaie une session RDP vers un poste utilisateur
DMZ	Allow -> VLAN50 VIP (1514)	Agent Wazuh sur Guacamole (zone la plus exposée)
DMZ	Allow -> VLAN20 VIP (389)	Authentification LDAP de Guacamole auprès de l'AD
DMZ	Block -> VLAN10	La DMZ ne remonte jamais vers l'admin, même compromise
DMZ	Block -> any	Règle finale - zone la plus restreinte
VLAN50 - Supervision (192.168.50.0/24) - Zabbix, Wazuh, Nessus mutualisés sur une VM unique		

VLAN50	Allow -> VLAN20/30/DMZ (10050)	Zabbix interroge les agents en mode passif
VLAN50	Allow -> VLAN20/30/DMZ (1515)	Wazuh manager enrôle un agent
VLAN50	Allow -> VLAN10/20/30/DMZ (any)	Exception assumée : scans Nessus, accès large nécessaire
VLAN50	Allow -> VLAN60 (445)	Duplicati vers TrueNAS local
VLAN50	Allow -> any (443)	Mises à jour plugins Nessus / définitions Zabbix-Wazuh / Backblaze
VLAN50	Block -> any	Règle finale
VLAN60 - Sauvegardes (192.168.60.0/24)		
VLAN60	Allow depuis VLAN20/50 uniquement (445)	Seules les sources légitimes de sauvegarde écrivent ici
VLAN60	Block -> any (sortant)	Le repository ne doit jamais initier de connexion
OpenVPN (VPN nomade, 10.10.10.0/24)		
OpenVPN	Allow -> VLAN20 VIP (389)	Authentification LDAP du VPN auprès de l'AD
OpenVPN	Allow -> DMZ VIP (443)	Accès au portail Guacamole depuis le VPN
OpenVPN	Allow -> VLAN60 (443)	Accès admin ponctuel à l'interface TrueNAS via le VPN
OpenVPN	Block -> any	Règle finale
WAN (site principal)		
WAN	Allow UDP -> WAN address (1195)	Négociation du tunnel OpenVPN Site-à-Site entrant
Site de secours - pfSense-secours (nœud unique, sans CARP) **VLAN100 - Secours (192.168.100.0/24)**		
VLAN100	Allow -> VLAN110 (445 ou SSH)	Accès de Veeam au stockage de secours si nécessaire
VLAN100	Allow -> This Firewall (443)	Accès WebGUI pfSense-secours
VLAN100	Block -> any	Règle finale
VLAN110 - Sauvegardes (192.168.110.0/24)		
VLAN110	Allow depuis VLAN60 (site principal, via tunnel S2S)	Réplication ZFS TrueNAS local -> TrueNAS-secours
VLAN110	Block -> any (sortant)	Le repository de secours ne doit jamais initier de connexion
WAN (site de secours)		
WAN	Allow UDP -> WAN address (1195)	Négociation du tunnel OpenVPN Site-à-Site (côté client)

Annexe C - Règles de pare-feu (version sans contrainte de ressources)

Version idéale des règles de pare-feu, si chaque brique (Zabbix, Wazuh, Nessus, Duplicati) disposait de sa propre VM plutôt que d'être mutualisée par contrainte de ressources sur une seule machine du VLAN 50.

VLAN / Interface	Règle	Justification

Site principal - pf1 (Master) et pf2 (Backup) - configuration identique répliquée par XMLRPC Config Sync		
VLAN10 - Admin (10.0.10.0/24)		
VLAN10	Allow -> VLAN50 VIP (80/443, 8834, 443)	Accès admin aux consoles web Zabbix, Nessus et Wazuh
VLAN10	Allow -> VLAN20 (8200, 3389)	Accès à la console Duplicati et RDP admin vers le Windows Server
VLAN10	Allow -> DMZ VIP (443)	Administration du portail Guacamole
VLAN10	Allow -> This Firewall (443)	Accès WebGUI pfSense
VLAN10	Block -> any	Règle finale, moindre privilège
VLAN20 - Serveurs (192.168.1.0/24) - Windows Server .112 et Duplicati .90 sur VM distinctes		
VLAN20	Allow (Windows Server) -> VLAN50 (10051, 1514)	Remontée agents Zabbix/Wazuh du serveur vers la supervision
VLAN20	Allow (Duplicati .90) -> WAN (443)	Duplicati vers Backblaze B2
VLAN20	Allow (Duplicati .90) -> VLAN60 (445)	Sauvegarde locale Duplicati vers TrueNAS
VLAN20	Allow (Windows Server) -> VLAN60 (445)	wbadmin (System State AD) vers TrueNAS
VLAN20	Block -> VLAN30	Un serveur n'initie jamais vers les postes utilisateurs
VLAN20	Block -> any	Règle finale
VLAN30 - Utilisateurs (192.168.30.0/24)		
VLAN30	Allow -> VLAN20 VIP (88, 389, 445, 53, 123)	Authentification AD, LDAP, SMB, DNS, NTP
VLAN30	Allow -> VLAN50 VIP (1514, 1515)	Agent Wazuh du poste
VLAN30	Allow -> any (80, 443)	Navigation Internet via NAT
VLAN30	Block -> VLAN10	Pas d'accès direct à l'administration
VLAN30	Block -> DMZ	Passe par le VPN + Guacamole, jamais en direct
VLAN30	Block -> any	Règle finale
DMZ (172.16.40.0/24)		
DMZ	Allow -> VLAN20 VIP (3389)	Guacamole relaie une session RDP vers le serveur
DMZ	Allow -> VLAN30 (3389)	Guacamole relaie une session RDP vers un poste utilisateur
DMZ	Allow -> VLAN50 VIP (1514)	Agent Wazuh sur Guacamole (zone la plus exposée)
DMZ	Allow -> VLAN20 VIP (389)	Authentification LDAP de Guacamole auprès de l'AD
DMZ	Block -> VLAN10	La DMZ ne remonte jamais vers l'admin, même compromise
DMZ	Block -> any	Règle finale - zone la plus restreinte
VLAN50 - Supervision (192.168.50.0/24) - Zabbix .10, Wazuh .20, Nessus .30 sur VM distinctes		
VLAN50	Allow (Zabbix .10) -> VLAN20/30/DMZ (10050)	Zabbix interroge les agents en mode passif

VLAN50	Allow (Zabbix .10) -> any (443)	Mise à jour des définitions Zabbix
VLAN50	Allow (Wazuh .20) -> VLAN20/30/DMZ (1515)	Wazuh manager enrôle un agent
VLAN50	Allow (Wazuh .20) -> any (443)	Mise à jour des règles Wazuh
VLAN50	Allow (Nessus .30) -> VLAN10/20/30/DMZ (any)	Exception assumée : scans Nessus, accès large nécessaire
VLAN50	Allow (Nessus .30) -> any (443)	Mise à jour des plugins Nessus
VLAN50	Block -> any	Règle finale
VLAN60 - Sauvegardes (192.168.60.0/24)		
VLAN60	Allow depuis VLAN20/50 uniquement (445)	Seules les sources légitimes de sauvegarde écrivent ici
VLAN60	Block -> any (sortant)	Le repository ne doit jamais initier de connexion
OpenVPN (VPN nomade, 10.10.10.0/24)		
OpenVPN	Allow -> VLAN20 VIP (389)	Authentification LDAP du VPN auprès de l'AD
OpenVPN	Allow -> DMZ VIP (443)	Accès au portail Guacamole depuis le VPN
OpenVPN	Allow -> VLAN60 (443)	Accès admin ponctuel à l'interface TrueNAS via le VPN
OpenVPN	Block -> any	Règle finale
WAN (site principal)		
WAN	Allow UDP -> WAN address (1195)	Négociation du tunnel OpenVPN Site-à-Site entrant
Site de secours - pfSense-secours (nœud unique, sans CARP) **VLAN100 - Secours (192.168.100.0/24)**		
VLAN100	Allow -> VLAN110 (445 ou SSH)	Accès de Veeam au stockage de secours si nécessaire
VLAN100	Allow -> This Firewall (443)	Accès WebGUI pfSense-secours
VLAN100	Block -> any	Règle finale
VLAN110 - Sauvegardes (192.168.110.0/24)		
VLAN110	Allow depuis VLAN60 (site principal, via tunnel S2S)	Réplication ZFS TrueNAS local -> TrueNAS-secours
VLAN110	Block -> any (sortant)	Le repository de secours ne doit jamais initier de connexion
WAN (site de secours)		
WAN	Allow UDP -> WAN address (1195)	Négociation du tunnel OpenVPN Site-à-Site (côté client)