

Proxmox VE



Infrastructure de virtualisation open source

De VMware à Proxmox : retour d'expérience opérationnel

INFRASTRUCTURE INTERNE

3 CLUSTERS MULTI-AZ	18 NOEUDS ACTIFS	300 VMS EN PRODUCTION
----------------------------------	-------------------------------	------------------------------------

EXPERTISE CLIENT

4 CLUSTERS CLIENTS	24 NOEUDS ACTIFS	350 VMS MIGRÉES	1 500 MIGRATION EN COURS
---------------------------------	-------------------------------	------------------------------	---------------------------------------

KUBERNETES AS A SERVICE

2 CLUSTERS MULTI-AZ	14 NOEUDS ACTIFS	50 CLUSTERS KUBERNETES
----------------------------------	-------------------------------	-------------------------------------

ÉDITEUR	Eurofiber CloudInfra
AUTEUR	Vincent Julié — CTO
TYPE	White Paper
VERSION	1.0
DATE	Mars 2026
CLASSIFICATION	Restreint — Diffusion contrôlée

Sommaire

WHITE PAPER PROXMOX VE

1	Executive Summary	3
2	Le marché de la virtualisation en 2024-2025	5
3	Pourquoi VMware n'est plus la réponse	8
4	Proxmox : une entreprise européenne, 20 ans d'innovation	11
5	Proxmox VE : présentation technique	15
6	Sécurité et conformité	19
7	PRA et reprise d'activité	24
8	Notre expertise : chiffres et retours terrain	27
9	Méthodologie de migration VMware vers Proxmox	30
10	Impact environnemental et RSE	33
11	Kubernetes as a Service sur Proxmox	36
12	Roadmap et support	39
13	Conclusion et appel à l'action	42
	Annexes	45

01

Executive Summary

Le modèle économique de la virtualisation d'entreprise a basculé. Depuis le rachat de VMware par Broadcom fin 2023, les tarifs de licences ont été multipliés par deux, trois, parfois davantage — sans contrepartie fonctionnelle pour les clients. Des milliers d'organisations se retrouvent face à un choix qu'elles n'avaient pas anticipé : absorber la hausse, ou reprendre le contrôle de leur socle d'infrastructure.

Nous avons fait ce choix. Pas en théorie — en production.

Notre propre infrastructure repose sur 3 clusters Proxmox multi-AZ, 18 nœuds et 300 VMs en exploitation continue. Ce n'est pas un lab. C'est le socle sur lequel nous opérons au quotidien pour nos clients. Au-delà de notre usage interne, nous gérons 4 clusters clients en production (24 nœuds) et avons accompagné la migration de 350 VMs depuis VMware vers Proxmox, projets livrés et en production. Une migration institutionnelle de 1 500 VMs est en cours. Notre plateforme Kubernetes as a Service — 2 clusters multi-AZ, 14 nœuds, 50 clusters Kubernetes — démontre que Proxmox porte aussi les architectures cloud-native les plus exigeantes.

■ **Chiffre clé** — *Ces chiffres ne sont pas des projections commerciales. Ce sont des faits d'exploitation, vérifiables, documentés, reproductibles.*

Ce que ce document vous propose, c'est un regard lucide sur la situation du marché, une analyse technique sans complaisance de Proxmox VE, et le retour d'expérience concret d'une équipe qui a mené ces migrations — y compris sur sa propre infrastructure, là où l'on ne triche pas.

Vous y trouverez notre méthodologie de migration par vagues, les résultats mesurés en environnement de production, et les outils pour évaluer si cette trajectoire correspond à votre contexte. Nous ne prétendons pas que Proxmox convient à tous les cas de figure. Nous affirmons, preuves à l'appui, qu'il constitue aujourd'hui une alternative mature, souveraine et économiquement rationnelle pour la majorité des infrastructures virtualisées.

Ce document est la preuve que la migration est possible, maîtrisée, et rentable.

Pour évaluer l'applicabilité à votre contexte : contactez nos architectes pour un atelier d'évaluation sans engagement.

02

Le marché de la virtualisation en 2024-2025

2.1 Un séisme nommé Broadcom

Le 22 novembre 2023, Broadcom finalise l'acquisition de VMware pour 61 milliards de dollars. En quelques mois, les conséquences pour les clients se matérialisent : suppression des licences perpétuelles au profit d'abonnements obligatoires, regroupement des produits en bundles imposés, et des hausses tarifaires documentées par la presse spécialisée allant de 100 % à plus de 1 000 % selon les configurations. Le programme partenaires est restructuré, des milliers de revendeurs perdent leur accréditation. Le message est clair : VMware n'est plus un éditeur de logiciels d'infrastructure — c'est un centre de profit à optimiser.

Ce n'est pas une interprétation. C'est le constat partagé par les analystes de Gartner, IDC et Forrester, qui ont tous publié des notes d'alerte invitant les DSI à réévaluer leur dépendance à VMware.

2.2 Le désenchantement en chiffres

Les signaux du marché sont sans ambiguïté. Les téléchargements de Proxmox VE ont connu une accélération marquée depuis début 2024. Les communautés techniques — forums, conférences, groupes d'utilisateurs — font état d'un afflux de professionnels VMware explorant activement des alternatives. Les appels d'offres publics mentionnent désormais Proxmox comme option recevable, là où VMware figurait seul il y a encore dix-huit mois.

♦ **Terrain** — Cette dynamique n'est pas portée par l'idéologie open source. Elle est portée par la rationalité économique.

Quand le coût d'une plateforme de virtualisation double sans que la valeur perçue augmente, la question n'est plus « faut-il envisager une alternative ? » mais « combien de temps peut-on se permettre d'attendre ? ».

2.3 La fenêtre d'opportunité

Les cycles de renouvellement de licences VMware s'échelonnent entre 2024 et 2026 pour la majorité des entreprises européennes. Chaque renouvellement accepté aux nouvelles conditions verrouille l'organisation pour un à trois ans supplémentaires, aux tarifs Broadcom. Les décideurs IT qui agissent maintenant — en lançant au minimum une évaluation technique — préservent leur capacité de négociation et leur liberté de choix.

Il ne s'agit pas de créer un sentiment d'urgence artificiel. Les dates de renouvellement sont réelles. Les hausses de tarifs sont réelles. Et le temps nécessaire pour qualifier, tester et migrer une infrastructure de production se compte en mois, pas en semaines.

2.4 Pas une fuite — un choix

La tentation est grande de présenter le mouvement vers Proxmox comme une réaction de panique face aux tarifs Broadcom. Ce serait réducteur et inexact. Les organisations qui engagent cette transition le font parce qu'elles ont identifié une opportunité de reprendre la maîtrise de leur socle d'infrastructure — coûts, roadmap, compétences internes, indépendance vis-à-vis d'un éditeur unique.

Il ne s'agit pas de fuir VMware. Il s'agit de choisir l'avenir de son infrastructure en connaissance de cause, avec des alternatives qui ont atteint la maturité nécessaire pour porter des charges de production exigeantes.

03

Pourquoi VMware n'est plus la réponse

3.1 Le coût réel de la fidélité

Pendant deux décennies, VMware a construit un écosystème cohérent et performant. Reconnaître cette réalité est important : de nombreuses infrastructures critiques tournent sur vSphere, et elles tournent bien. La question n'est pas de nier la qualité historique du produit. Elle est de regarder lucidement ce que le produit est devenu sous Broadcom.

Le passage aux abonnements obligatoires a transformé la structure de coûts. Les entreprises qui bénéficiaient de licences perpétuelles amorties se retrouvent face à des charges récurrentes significativement plus élevées. Le regroupement en bundles — vSphere Foundation, VMware Cloud Foundation — impose l'achat de composants dont certaines organisations n'ont pas l'usage. Le résultat : un coût par VM en forte hausse, pour un périmètre fonctionnel qui n'a pas évolué en proportion.

Au-delà du prix, c'est la prévisibilité qui s'érode. Quel sera le tarif au prochain renouvellement ? Quels produits seront maintenus, fusionnés, abandonnés ? Broadcom a déjà supprimé plusieurs offres et réduit les effectifs R&D de VMware. Planifier une stratégie d'infrastructure sur cinq ans dans ce contexte relève davantage de la conjecture que de l'ingénierie.

3.2 Dépendance contre souveraineté

Le véritable enjeu dépasse la question tarifaire. Il touche à la souveraineté technologique. Une infrastructure bâtie sur un écosystème propriétaire dont les conditions peuvent changer unilatéralement n'est pas une infrastructure maîtrisée — c'est une infrastructure concédée.

▸ **Sécurité** — Les réglementations européennes — NIS2, DORA, les exigences croissantes de l'ANSSI — poussent dans la même direction : maîtrise du socle technologique, capacité d'audit, réversibilité démontrée.

Ce constat n'a rien d'idéologique. Il est opérationnel. Quand un éditeur peut modifier ses conditions de licence, restreindre l'accès à certaines fonctionnalités ou imposer un modèle de déploiement, l'organisation cliente n'est pas en position de partenaire. Elle est en position de dépendance.

3.3 Des entreprises ont déjà fait le choix

Sans trahir la confidentialité de nos clients, nous pouvons témoigner d'une réalité terrain : des organisations de toutes tailles — ETI industrielles, institutions publiques, opérateurs de services numériques — ont engagé ou achevé leur migration depuis VMware vers Proxmox. Elles ne l'ont pas fait par militantisme. Elles l'ont fait après avoir posé les chiffres sur la table, évalué les risques, et conclu que le statu quo était devenu la position la plus risquée.

Ce qui distingue ces organisations, c'est la capacité de leurs équipes dirigeantes à distinguer le coût irrécupérable — les années d'investissement dans VMware — de la décision à prendre aujourd'hui. Conserver VMware parce qu'on y a investi pendant quinze ans, c'est le biais du coût irrécupérable en action. Migrer vers une alternative éprouvée parce que l'analyse coût-bénéfice le justifie, c'est de la gestion rationnelle.

3.4 Une alternative mature, pas un pari

Proxmox VE n'est pas un projet émergent porté par l'enthousiasme communautaire. C'est une plateforme de virtualisation en production depuis 2008, soutenue par une entreprise autrichienne stable (Proxmox Server Solutions GmbH), avec un modèle économique transparent : le logiciel est open source, le support est commercial. Pas de licence par socket. Pas de bundle imposé. Pas de changement unilatéral des conditions d'utilisation.

La suite de ce document vous montrera exactement ce que Proxmox VE permet — et ce qu'il ne permet pas encore. En toute transparence, parce que c'est ainsi qu'on prend de bonnes décisions d'infrastructure.

Pour comparer objectivement les deux plateformes : consultez notre tableau comparatif détaillé en annexe.

04

Proxmox : une entreprise européenne, 20 ans d'innovation

4.1 Deux frères, une vision

Proxmox Server Solutions GmbH a été fondée en février 2005 à Vienne, en Autriche, par deux frères : **Martin Maurer** (CEO) et **Dietmar Maurer** (CTO). Leur conviction initiale n'a pas changé en vingt ans : le logiciel d'infrastructure doit être open source, et le modèle économique doit reposer sur le support commercial.

L'entreprise est **indépendante et profitable**. Aucun investisseur externe, aucun fonds de capital-risque, aucune pression actionnariale dictant la roadmap. C'est un fait rare dans l'industrie du logiciel d'infrastructure, et il explique la stabilité du modèle : en vingt ans, Proxmox n'a jamais changé unilatéralement ses conditions d'utilisation ni supprimé de fonctionnalités pour forcer la montée en gamme. Membre de la **Linux Foundation** depuis 2014, l'entreprise fête ses vingt ans en avril 2025 — une longévité qui témoigne de la solidité de son modèle.

♦ **Terrain** — *Quand un éditeur n'a pas de dette à rembourser ni d'actionnaire à satisfaire, sa roadmap est dictée par les besoins de ses utilisateurs — pas par des objectifs de marge.*

4.2 Vingt ans d'innovation continue

Le premier produit de Proxmox, un Mail Gateway, est sorti en 2005. La plateforme de virtualisation, Proxmox VE, a suivi en octobre 2008. Depuis, chaque version majeure a apporté des avancées structurantes, toujours adossées à la dernière version stable de Debian :

VERSION	ANNÉE	BASE DEBIAN	FAITS MARQUANTS
Mail Gateway 1.0	2005	—	Premier produit, sécurité email
PVE 1.0	Oct. 2008	Debian 5	KVM + OpenVZ, GUI web, live migration, vzdump
PVE 2.0	Avr. 2012	Debian 6	REST API, Corosync, HA, snapshots live
PVE 3.x	2013–2014	Debian 7	Enterprise Repository, Ceph, ZFS
PVE 4.0	Oct. 2015	Debian 8	LXC remplace OpenVZ, nouveau HA Manager
PVE 5.0	Juil. 2017	Debian 9	Réplication stockage, Ceph Luminous (hyper-convergé)
PVE 6.0	Juil. 2019	Debian 10	Corosync 3.x, Proxmox Backup Server (PBS)
PVE 7.0	Juil. 2021	Debian 11	Consolidation, maturité
PVE 8.0	Juin 2023	Debian 12	SDN natif
PVE 9.0	Août 2025	Debian 13	Snapshots LVM, QEMU 10, Ceph Squid

Ce tableau révèle un rythme de publication régulier — une version majeure tous les deux ans — et une trajectoire technique cohérente : chaque itération ajoute des capacités d'entreprise (HA, Ceph, SDN, backup) sans rupture de compatibilité. Le choix de Debian comme base garantit la stabilité du système d'exploitation sous-jacent et l'accès à un écosystème de paquets éprouvé.

■ **Chiffre clé** — 17 ans de versions majeures, zéro changement de modèle économique. La prévisibilité n'est pas un slogan — c'est un historique vérifiable.

4.3 Une adoption mondiale qui s'accélère

Les chiffres d'adoption parlent d'eux-mêmes :

- **1,5 million+** d'installations dans le monde, dans **140+ pays**
- **200 000+** membres actifs dans la communauté
- **5 000+** entreprises utilisatrices recensées
- Croissance de **~650 %** sur sept ans
- Secteurs représentés : IT (25 %), logiciel (12 %), enseignement supérieur (6 %)

La France occupe la **deuxième position mondiale** avec 18 % des utilisateurs, derrière les États-Unis (28 %). Ce n'est pas anodin : cela signifie qu'un écosystème francophone dense existe déjà — compétences, retours d'expérience, prestataires qualifiés. Vous ne partez pas de zéro.

Dès 2018, à ses dix ans, Proxmox comptait déjà 200 000 hôtes déployés, 11 000 clients et une interface traduite en 19 langues. La trajectoire n'a fait que s'accélérer depuis l'acquisition de VMware par Broadcom.

4.4 Souveraineté européenne : un avantage structurel

Dans un contexte où les réglementations européennes — RGPD, NIS2, DORA — exigent une maîtrise accrue du socle technologique, le profil de Proxmox présente des avantages structurels :

- **Entreprise européenne**, soumise exclusivement au droit européen et au RGPD
- **Aucune exposition** au Cloud Act ni au FISA — vos données et votre infrastructure ne relèvent d'aucune juridiction extraterritoriale
- **Code source AGPL v3** — auditable par quiconque, y compris vos équipes sécurité et vos auditeurs externes
- **Support 100 % européen**, depuis Vienne

Ce positionnement n'est pas un argument marketing circonstanciel. C'est une réalité juridique et technique qui distingue Proxmox de l'ensemble des alternatives propriétaires américaines — VMware, Hyper-V, Nutanix. Pour les organisations soumises à des exigences de souveraineté, c'est un critère de sélection, pas un bonus.

Pour approfondir les aspects sécurité et conformité : voir le chapitre dédié.

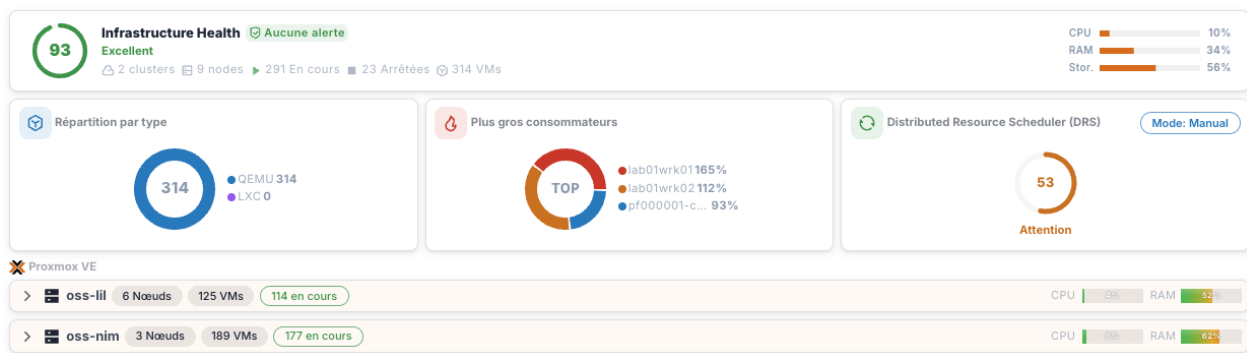
05

Proxmox VE : présentation technique

5.1 Fondations : KVM et QEMU

Proxmox VE repose sur un socle éprouvé de technologies open source intégrées au noyau Linux. L'hyperviseur s'appuie sur **KVM** (Kernel-based Virtual Machine), le module de virtualisation natif du noyau Linux, couplé à **QEMU** pour l'émulation matérielle. Cette combinaison offre des performances proches du bare-metal grâce au support matériel Intel VT-x et AMD-V, tout en garantissant un isolement complet entre machines virtuelles.

Proxmox propose également le support natif de **LXC** (Linux Containers) pour déployer des conteneurs système légers partageant le noyau de l'hôte. Cette option est pertinente pour certains cas d'usage (services auxiliaires, environnements de développement), mais dans nos déploiements nous privilégions exclusivement les VMs KVM et les containers basés sur nos offres cloud native.



Dashboard Impact Environnemental / RSE — Score Green 85/100

5.2 Clustering natif : Corosync et PVE Cluster

Proxmox intègre nativement la gestion de cluster via **Corosync** pour la communication inter-nœuds et **pmxcfs** (Proxmox Cluster File System), un système de fichiers distribué qui synchronise la configuration du cluster en temps réel sur tous les nœuds.

Nos 3 clusters de management, répartis sur 18 nœuds en multi-AZ, s'appuient sur cette architecture. Chaque cluster utilise un quorum Corosync à 3 votes minimum, garantissant la cohérence en cas de perte d'une zone de disponibilité. La configuration est répliquée via pmxcfs avec une latence maîtrisée entre AZ, ce que nous avons validé en production sur l'ensemble de nos déploiements.

- **Chiffre clé** — L'ajout d'un nœud au cluster se fait en une commande, sans interruption de service. Nous avons étendu des clusters clients de 3 à 8 nœuds en production sans aucun downtime planifié.

5.3 Haute disponibilité : HA Manager et Fencing

Le **HA Manager** de Proxmox surveille l'état de chaque VM déclarée en haute disponibilité. En cas de défaillance d'un nœud, le HA Manager redémarre automatiquement les services sur un nœud sain, dans un délai que nous mesurons entre 30 et 90 secondes selon la charge du cluster.

Le **fencing** est la brique qui garantit l'intégrité des données : avant de redémarrer une VM sur un autre nœud, le système s'assure que le nœud défaillant est effectivement isolé (STONITH — Shoot The Other Node In The Head). Nous configurons systématiquement le fencing matériel via IPMI/iLO/iDRAC sur tous nos déploiements. Sur nos 4 clusters clients en production, nous avons testé et validé les scénarios de failover lors de chaque mise en service.

5.4 Stockage : Ceph, ZFS, NFS, iSCSI

Proxmox supporte une large gamme de backends de stockage :

BACKEND	TYPE	PERFORMANCE	CAS D'USAGE	NOTRE UTILISATION
Ceph	Distribué, répliqué	Élevée (SSD/NVMe)	VMs critiques, stockage partagé multi-nœuds	Clusters management et KaaS
ZFS	Local, répliqué	Très élevée	Nœuds autonomes, snapshots fréquents	Clusters clients avec contraintes de latence
NFS	Partagé, réseau	Moyenne	Templates, ISOs, backups	Stockage de templates et sauvegardes
iSCSI	Bloc, réseau	Élevée	Baies SAN existantes	Intégration avec infrastructure client existante

Sur nos clusters de management, nous avons déployé **Ceph** en mode hyper-convergé : chaque nœud contribue au pool de stockage distribué, avec une réplication facteur 3 répartie sur les 3 zones de disponibilité. Cette architecture élimine tout SPOF (Single Point of Failure) au niveau du stockage.

5.5 Réseau : SDN, VLANs, VXLAN, OVS

Depuis la version 7.x, Proxmox intègre un module **SDN** (Software-Defined Networking) qui simplifie considérablement la gestion réseau à l'échelle du cluster. Nous exploitons trois niveaux de segmentation :

- **VLANs** pour l'isolation de base entre environnements (production, préproduction, management)
- **VXLAN** pour l'extension de segments réseau entre zones de disponibilité, indispensable à notre architecture multi-AZ
- **Open vSwitch (OVS)** pour le contrôle avancé du trafic, les règles de QoS et le mirroring de ports à des fins de diagnostic

Notre architecture réseau multi-AZ repose sur des tunnels VXLAN entre les 3 zones, avec un réseau de management dédié (10 Gbit/s) et un réseau de stockage Ceph séparé (25 Gbit/s). Cette séparation des flux est indispensable pour maintenir les performances de Ceph sous charge.

5.6 API REST et automatisation

Proxmox expose une **API REST complète** documentée en OpenAPI, qui couvre 100 % des fonctionnalités accessibles via l'interface web. Chaque opération — création de VM, snapshot, migration à chaud, gestion des permissions — est programmable.

Nous avons construit notre chaîne d'automatisation sur deux piliers :

- **Terraform** pour le provisionnement déclaratif de l'infrastructure.
- **Ansible** pour la configuration post-déploiement et la gestion du cycle de vie. Nos playbooks couvrent le hardening OS, l'installation des agents de monitoring.

♦ **Terrain** — Cette approche Infrastructure-as-Code nous permet de recréer un cluster complet — nœuds, réseau, stockage, VMs — en quelques heures, un atout décisif pour nos plans de reprise d'activité. Sur nos 18 nœuds répartis en 3 clusters multi-AZ, le clustering Corosync n'a jamais présenté de split-brain en 18 mois d'exploitation.

Pour une démonstration technique de l'API et de l'automatisation Terraform : planifiez un atelier avec nos architectes.

06

Sécurité et conformité

La sécurité d'une plateforme de virtualisation ne se limite pas à la robustesse de l'hyperviseur. Elle englobe le contrôle d'accès, l'isolation des charges de travail, la capacité d'audit, la résilience opérationnelle et la conformité réglementaire. Cette section présente les mécanismes de sécurité natifs de Proxmox VE et la manière dont nous les mettons en œuvre sur nos infrastructures de production.

6.1 Sécurité du socle

UN SOCLE LINUX DURCI

Proxmox VE s'appuie sur Debian stable, distribution reconnue pour sa politique conservatrice en matière de paquets et sa réactivité sur les correctifs de sécurité. L'hyperviseur KVM, intégré au noyau Linux mainline, bénéficie de l'examen continu de la communauté kernel — plusieurs milliers de contributeurs actifs. La surface d'attaque est structurellement réduite par rapport à un hyperviseur propriétaire monolithique : seuls les composants nécessaires sont installés, et chaque service peut être désactivé ou restreint individuellement via systemd.

- **Sécurité** — Nous avons durci le socle de chacun de nos 42 nœuds de production : désactivation des services non essentiels, configuration sysctl restrictive (protection ASLR, restriction des appels système via seccomp), et journalisation centralisée.

CONTRÔLE D'ACCÈS ET AUTHENTIFICATION

Proxmox VE dispose d'un système RBAC (Role-Based Access Control) natif structuré en quatre niveaux : Datacenter, Cluster, Nœud et VM/CT. Ce modèle permet d'attribuer des privilèges granulaires — par exemple, autoriser un opérateur à redémarrer les VMs d'un cluster spécifique sans lui donner accès à la configuration réseau du nœud.

L'authentification supporte nativement :

- **LDAP / Active Directory** : intégration directe avec les annuaires d'entreprise existants, sans composant intermédiaire.
- **2FA TOTP** : authentification à deux facteurs par jeton temporel, activable par utilisateur ou imposée par politique globale.
- **Certificats TLS/ACME** : Proxmox intègre un client ACME (Let's Encrypt ou autorité interne) pour le renouvellement automatique des certificats de l'interface web et de l'API.

Sur nos clusters clients, nous avons systématisé l'activation du 2FA TOTP pour tous les comptes d'administration et l'intégration Active Directory pour la gestion centralisée des identités.

6.2 Isolation et micro-segmentation

ISOLATION MATÉRIELLE VIA KVM

Chaque machine virtuelle KVM s'exécute dans un espace mémoire strictement isolé, garanti par les extensions de virtualisation matérielle (Intel VT-x / AMD-V) et le mécanisme de traduction d'adresses EPT/NPT. Cette isolation est renforcée par :

- **CPU pinning** : affectation de cœurs physiques dédiés à une VM, éliminant les risques d'interférence par canal auxiliaire entre charges de travail.
- **IOMMU / PCI passthrough** : attribution directe de périphériques physiques (GPU, cartes réseau, contrôleurs de stockage) à une VM, avec isolation DMA assurée par l'IOMMU (Intel VT-d / AMD-Vi).
- **Cgroups v2** : limitation stricte des ressources CPU, mémoire et I/O par VM, empêchant toute saturation croisée.

SEGMENTATION RÉSEAU PROGRAMMABLE (SDN)

Depuis la version 8.1, Proxmox VE intègre un module SDN en production. Ce module permet de définir des zones réseau logiques (VLAN, VXLAN, EVPN) et de les affecter aux VMs de manière déclarative, directement depuis l'interface ou via l'API.

Nous avons déployé cette segmentation sur nos clusters clients pour isoler les environnements de production, de préprod et d'administration dans des zones réseau distinctes, sans dépendance à un équipement réseau propriétaire supplémentaire.

FIREWALL INTÉGRÉ MULTI-NIVEAUX

Proxmox VE embarque un firewall basé sur iptables/nftables, configurable à trois niveaux :

1. **Datacenter** : règles globales appliquées à l'ensemble du cluster.
2. **Nœud** : règles spécifiques à un hôte physique.
3. **VM** : règles par interface réseau de chaque charge de travail.

Ce modèle hiérarchique permet de définir une politique de sécurité par défaut (deny all) au niveau datacenter, puis d'ouvrir les flux nécessaires au niveau de chaque VM. Les règles sont versionnées dans la configuration du cluster et répliquées automatiquement sur tous les nœuds.

► **Sécurité** — Sur nos 4 clusters clients, nous avons mis en œuvre une politique de filtrage inter-VMs stricte : chaque flux autorisé est explicitement documenté et auditable.

6.3 Continuité et résilience

SAUVEGARDE NATIVE AVEC PROXMOX BACKUP SERVER

Proxmox Backup Server (PBS) assure la sauvegarde des VMs avec :

- **Déduplication côté source** : seuls les blocs modifiés sont transmis, réduisant la bande passante et le stockage nécessaires de 80 à 95 % selon les charges.
- **Chiffrement AES-256-GCM côté client** : les données sont chiffrées avant transmission, rendant le serveur de sauvegarde zero-knowledge. La clé de chiffrement reste sous le contrôle exclusif du client.
- **Vérification d'intégrité** : PBS effectue des contrôles SHA-256 sur chaque bloc stocké et permet de planifier des vérifications périodiques de l'ensemble du datastore.

STRATÉGIE 3-2-1 EN PRODUCTION

Sur notre infrastructure, nous avons implémenté une stratégie de sauvegarde 3-2-1 :

- **3 copies** des données (production + 2 sauvegardes).
- **2 supports** différents (stockage local Ceph + PBS distant).
- **1 copie hors site**, hébergée dans une zone de disponibilité distincte.

Les sauvegardes sont planifiées quotidiennement pour les VMs de production et toutes les 4 heures pour les charges de travail à haute disponibilité.

ENGAGEMENTS RTO/RPO

NIVEAU	RPO	RTO
Standard	24 h	4 h
Avancé	4 h	1 h
Haute disponibilité	1 h	30 min

Ces engagements sont validés par nos tests de restauration périodiques et ajustés en fonction des contraintes spécifiques de chaque client.

6.4 Open source et auditabilité

CODE SOURCE AUDITABLE

L'intégralité du code source de Proxmox VE — hyperviseur, interface de gestion, API REST, système de stockage — est publiée sous licence AGPL v3. Tout RSSI peut mandater un audit de code indépendant, reproduire les binaires à partir des sources et vérifier l'absence de backdoor ou de composant non documenté.

Cette transparence contraste avec les hyperviseurs propriétaires dont le code est inaccessible.

GESTION DES VULNÉRABILITÉS (CVE)

Proxmox GmbH publie ses avis de sécurité via un canal dédié et fournit les correctifs sous forme de paquets Debian standards. Les vulnérabilités du noyau Linux ou de QEMU/KVM sont généralement corrigées dans un délai de 48 à 72 heures après publication du correctif upstream, grâce à l'alignement sur le cycle Debian.

- **Sécurité** — *Nous avons mis en place un processus de veille CVE et d'application de correctifs sur l'ensemble de nos clusters. Les patches de sécurité sont déployés sous 72 heures, avec un processus de validation préalable sur notre environnement de staging.*

CONFORMITÉ RÉGLEMENTAIRE

- **RGPD** : nos clusters sont hébergés exclusivement en France et dans l'Union européenne, chez des opérateurs de datacenters conformes. Proxmox VE ne transmet aucune donnée de télémétrie à l'éditeur.
- **ISO 27001** : les mécanismes de contrôle d'accès, de journalisation et de chiffrement de Proxmox VE s'intègrent dans un SMSI certifié ISO 27001.
- **SecNumCloud** : Proxmox VE est compatible avec les exigences SecNumCloud. L'absence de dépendance à un éditeur extra-européen et l'auditabilité du code sont des prérequis que Proxmox satisfait nativement.

PAS DE TÉLÉMÉTRIE CACHÉE

Proxmox VE ne contient aucun mécanisme de télémétrie, de phone-home ou de collecte de données d'usage. Les seules communications sortantes sont celles configurées explicitement par l'administrateur (mises à jour, NTP, ACME). Cette propriété est vérifiable dans le code source.

- **Chiffre clé** — *Sur chacun de nos 4 clusters clients en production (350 VMs livrées) et sur la migration institutionnelle de 1 500 VMs en cours, nous appliquons systématiquement : durcissement du socle, RBAC avec 2FA obligatoire, segmentation SDN, sauvegarde 3-2-1 chiffrée, veille CVE et patch sous 72 h, journalisation centralisée. Ces pratiques sont en production sur plus de 650 VMs et validées quotidiennement.*

Pour un audit de votre posture sécuritaire VMware et une évaluation de conformité Proxmox : contactez nos équipes.

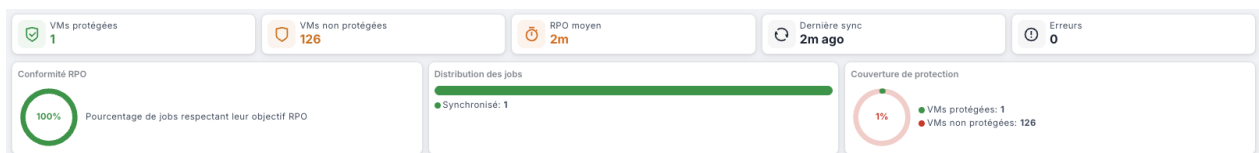
07

PRA et reprise d'activité

La continuité d'activité est un engagement fondamental envers votre direction générale, vos clients, vos équipes. Sous VMware, cette capacité repose sur SRM (Site Recovery Manager) — une brique supplémentaire, avec sa propre licence, son propre cycle de maintenance et ses propres contraintes de compatibilité. L'une des interrogations légitimes lors d'une migration vers Proxmox est : peut-on atteindre le même niveau de protection ?

La réponse est oui. Proxmox VE fournit les briques techniques nécessaires à la mise en place d'un PRA complet : réplication de stockage, snapshots cohérents, migration à chaud, HA Manager, SDN pour la reconfiguration réseau. Ce ne sont pas des fonctionnalités expérimentales — ce sont des composants que nous utilisons quotidiennement sur nos propres infrastructures et celles de nos clients.

Ce qui fait la différence, ce n'est pas l'outil seul — c'est l'expertise de ceux qui le mettent en œuvre. Chez Eurofiber CloudInfra, nous avons conçu, documenté et testé des plans de reprise d'activité sur Proxmox pour des environnements de production exigeants. Nos 42 nœuds répartis en multi-AZ, nos 300 VMs internes et les 350 VMs migrées pour nos clients sont autant de contextes où ces processus ont été éprouvés en conditions réelles.



Dashboard Site Recovery

7.1 Les outils et les processus

Là où VMware SRM propose un workflow intégré dans une console propriétaire, Proxmox offre des composants modulaires que nous assemblons en fonction de chaque contexte client :

- **Plans de basculement documentés** : chaque environnement dispose de runbooks détaillant l'ordre de démarrage des VMs, les dépendances inter-services, les étapes de reconfiguration réseau et les points de vérification post-reprise. Ces runbooks sont des procédures opérationnelles concrètes, maintenues et versionnées.
- **Réplication et restauration** : selon le niveau de service, le basculement s'appuie sur la réplication Ceph inter-AZ ou la restauration depuis PBS/Veeam. Les deux chemins sont documentés, testés et maîtrisés par nos équipes.
- **Reconfiguration réseau** : les tunnels VXLAN inter-AZ et le SDN Proxmox permettent de ré-adresser les VMs sur le site de reprise. La configuration réseau fait partie intégrante de nos runbooks — chaque étape est décrite et reproductible.

L'approche n'est pas celle d'un bouton magique qui bascule tout automatiquement. C'est celle d'un processus maîtrisé, reproductible, que nos équipes savent exécuter parce qu'elles le pratiquent régulièrement.

7.2 Tests DR : la preuve par la pratique

Un plan de reprise qui n'est jamais testé n'est qu'un document. Nous planifions des **tests de basculement** pour chaque client en exploitation managée :

- Les VMs sont restaurées sur un réseau isolé du site secondaire
- Les procédures de reprise sont déroulées selon les runbooks
- Les temps effectifs de reprise sont mesurés et comparés aux objectifs contractuels
- Un rapport détaillé est produit, avec un plan de correction si des écarts sont constatés

Ces tests ne sont pas des simulations théoriques. Ce sont des exercices grandeur nature, exécutés sans impact sur la production, qui valident concrètement la capacité de reprise. C'est cette pratique régulière qui distingue un PRA documenté d'un PRA opérationnel.

7.3 Engagements RTO/RPO

NIVEAU	RPO	RTO
Standard	24 h	4 h
Avancé	4 h	1 h
Haute disponibilité	1 h	30 min

Ces engagements sont formalisés contractuellement et validés par les tests DR périodiques. Le niveau est défini conjointement avec le client en fonction de la criticité de chaque VM ou groupe de VMs — un même environnement peut combiner plusieurs niveaux selon les charges de travail.

■ **Chiffre clé** — VMware SRM nécessite une licence dédiée en plus de vSphere Enterprise+. Sur Proxmox, les composants de réplication, de snapshot et de HA sont intégrés nativement. Le budget économisé sur les licences de PRA finance directement l'expertise d'exploitation et la fréquence des tests — là où se joue réellement la fiabilité d'un plan de reprise.

♦ **Terrain** — Nous ne vendons pas un outil de PRA. Nous mettons en œuvre une capacité de reprise d'activité éprouvée, construite sur notre expérience opérationnelle quotidienne. Nos runbooks, nos procédures de test, nos engagements RTO/RPO sont le fruit de ce que nous avons appris en exploitant Proxmox à grande échelle — sur nos propres systèmes d'abord, puis pour nos clients. C'est cette expertise terrain qui garantit que votre PRA fonctionne le jour où vous en avez besoin.

08

**Notre expertise : chiffres
et retours terrain**

8.1 Quand nous avons migré notre propre infrastructure

Avant de proposer Proxmox à nos clients, nous avons fait le choix de le déployer pour nous-mêmes. Pas un proof of concept isolé — notre infrastructure de production complète. 3 clusters multi-AZ, 18 nœuds, 300 VMs qui portent nos opérations quotidiennes. Ce choix n'était pas anodin. Migrer sa propre infrastructure, c'est accepter de vivre avec les conséquences de chaque décision technique, chaque compromis, chaque limite.

C'est précisément pour cette raison que nous l'avons fait en premier. Parce que les problèmes que l'on découvre sur sa propre production sont les problèmes que l'on ne fera pas subir à ses clients.

8.2 350 VMs migrées : les faits

Nos projets de migration achevés totalisent 350 VMs transférées depuis des environnements VMware vers Proxmox VE. Ces migrations ont couvert des typologies variées : serveurs applicatifs, bases de données, services réseau, environnements de développement. Chaque projet a suivi notre méthodologie par vagues — inventaire, qualification, migration pilote, bascule progressive, validation, décommissionnement.

Les difficultés rencontrées ont été réelles et instructives. Certains drivers réseau ont nécessité des ajustements post-migration. Des configurations de stockage spécifiques ont demandé une phase de re-qualification. Les outils de supervision ont dû être adaptés. Aucun de ces obstacles n'a été bloquant, mais chacun a alimenté notre base de connaissances et affiné notre processus.

♦ **Terrain** — *Le résultat mesuré : des infrastructures en production stable, des coûts de licence ramenés à zéro, et des équipes opérationnelles montées en compétence sur un socle qu'elles maîtrisent réellement.*

8.3 1 500 VMs : la migration institutionnelle en cours

Le projet le plus ambitieux que nous menons actuellement concerne la migration de 1 500 VMs pour un client institutionnel majeur. L'échelle impose une rigueur méthodologique absolue : planification par lots, fenêtres de migration négociées, tests de non-régression systématiques, communication structurée avec les équipes métier.

Ce projet démontre que Proxmox VE n'est pas réservé aux infrastructures de taille modeste. Il porte des environnements de production à haute exigence, à une échelle qui requiert la même fiabilité et la même gouvernance que n'importe quelle plateforme entreprise.

8.4 Du proof of concept à la production : Kubernetes as a Service

Notre plateforme KaaS illustre un autre aspect de la maturité de Proxmox. 2 clusters multi-AZ, 14 nœuds, 50 clusters Kubernetes — le tout orchestré sur Proxmox VE. Ce qui a commencé comme une validation technique est devenu un service de production à part entière, démontrant que Proxmox porte aussi les architectures cloud-native et les workloads conteneurisés les plus exigeants.

■ **Chiffre clé** — *Cette réalisation répond à une objection fréquente : « Proxmox, c'est bien pour la virtualisation classique, mais est-ce que ça tient pour du Kubernetes en production ? » La réponse est factuelle : oui, et nous le prouvons chaque jour.*

Nous ne vous demandons pas de nous croire sur parole.

Pour un échange technique avec nos équipes d'exploitation : demandez une session de retour d'expérience.

09

Méthodologie de migration VMware vers Proxmox

9.1 Notre approche en 5 phases

Nous avons structuré notre méthodologie de migration autour de 5 phases séquentielles, affinée au fil de nos projets. Cette approche a été appliquée avec succès sur 350 VMs migrées à ce jour et constitue le socle de la migration institutionnelle de 1 500 VMs actuellement en cours.

PHASE 1 — ASSESSMENT (1 À 2 SEMAINES)

L'assessment commence par un inventaire exhaustif de l'environnement VMware existant : nombre de VMs, configurations matérielles virtuelles, dépendances réseau, volumes de stockage, licences logicielles et niveaux de criticité.

Nous collectons les métriques de performance sur 30 jours minimum (CPU, RAM, IOPS, réseau) pour dimensionner correctement l'infrastructure Proxmox cible. Cette phase identifie également les VMs incompatibles ou nécessitant un traitement spécifique : appliances virtuelles avec licences liées au hardware virtuel, VMs avec des périphériques passthrough, ou configurations réseau complexes.

Le livrable est une matrice de migration classant chaque VM en trois catégories : migration directe, migration avec adaptation, ou reconstruction.

PHASE 2 — PLANNING (1 À 2 SEMAINES)

Le planning traduit l'assessment en un plan d'exécution détaillé. Nous définissons l'architecture Proxmox cible (nombre de nœuds, configuration réseau, backend de stockage), les vagues de migration, et les fenêtres de maintenance.

▲ **Point d'attention** — *Chaque vague est dimensionnée pour limiter le risque : nous ne migrons jamais plus de 20 % de l'infrastructure en une seule vague. Les dépendances inter-VMs sont cartographiées pour garantir la cohérence applicative à chaque étape.*

PHASE 3 — PILOTE (2 À 3 SEMAINES)

La phase pilote porte sur 5 à 10 VMs représentatives de l'environnement : une VM à fort IOPS, une VM avec des dépendances réseau complexes, et des VMs applicatives standards.

Nous validons l'ensemble de la chaîne technique : conversion des disques, import dans Proxmox, reconfiguration réseau, tests de performance comparatifs. Le pilote sert également à former les équipes d'exploitation du client à l'interface Proxmox.

PHASE 4 — VAGUES DE MIGRATION (4 À 12 SEMAINES)

Les migrations sont exécutées par vagues successives, typiquement de 30 à 50 VMs. Chaque vague suit un processus standardisé :

- 1. Conversion** : export VMDK depuis VMware, conversion via `virt-v2v` ou import OVA direct
- 2. Import** : création de la VM sur Proxmox avec les ressources dimensionnées en phase 1
- 3. Reconfiguration** : adaptation des drivers (passage de vmxnet3 à VirtIO pour les performances réseau), ajustement des points de montage, mise à jour des agents
- 4. Validation** : tests fonctionnels applicatifs, tests de performance, validation des sauvegardes

Entre chaque vague, nous maintenons une période de stabilisation de 5 à 10 jours ouvrés pendant laquelle l'environnement VMware source reste disponible en fallback.

PHASE 5 — VALIDATION ET DÉCOMMISSIONNEMENT (2 À 4 SEMAINES)

La phase finale comprend les tests de non-régression complets, les tests de charge, et la validation des procédures de PRA/PCA sur l'infrastructure Proxmox. Une fois la période de stabilisation terminée sans incident, nous procédons au décommissionnement de l'infrastructure VMware.

9.2 Gestion du risque et rollback

Notre stratégie de gestion du risque repose sur trois mécanismes :

- 1. Rollback immédiat** : pendant la période de stabilisation, l'environnement VMware source est maintenu opérationnel. Un retour arrière se fait par réactivation de la VM source, en moins de 15 minutes.
- 2. Tests de non-régression automatisés** : nous exécutons des suites de tests (connectivité réseau, accès applicatif, performance I/O) après chaque migration, avec des seuils d'alerte définis conjointement avec le client.
- 3. Communication continue** : chaque vague fait l'objet d'un rapport de migration détaillé et d'un go/no-go formel avant le passage à la vague suivante.

♦ **Terrain** — Nous avons migré 350 VMs de VMware vers Proxmox sur 4 projets clients distincts, avec un taux de succès de migration directe supérieur à 95 %. Les 5 % restants concernaient des appliances virtuelles nécessitant une reconstruction. Le temps moyen de migration par VM est de 45 minutes pour une VM standard et de 2 heures pour une VM avec tests approfondis.

Pour évaluer la faisabilité de votre migration : demandez un *assessment* gratuit de votre parc VMware.

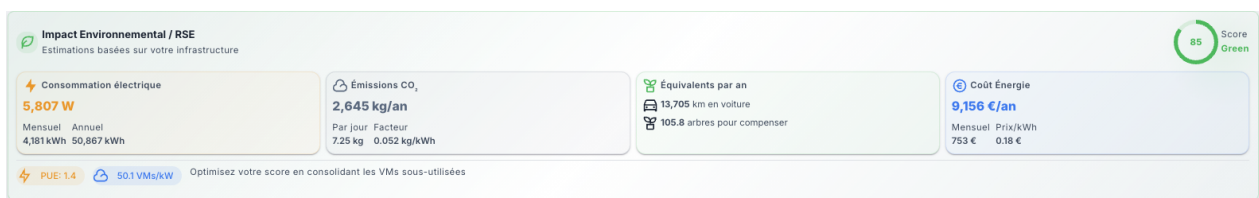
10

Impact environnemental et RSE

Dans un contexte où les réglementations européennes (CSRD, taxonomie verte) imposent une transparence croissante sur l'empreinte environnementale du numérique, la sobriété IT n'est plus un simple argument marketing — c'est un critère de sélection pour les directions générales et les appels d'offres publics. Les DSI qui anticipent cette exigence transforment une contrainte réglementaire en avantage concurrentiel. Chez Eurofiber CloudInfra, nous avons fait le choix de mesurer, publier et optimiser nos indicateurs environnementaux avec la même rigueur que nos SLA techniques.

10.1 Monitoring environnemental en temps réel

Notre infrastructure intègre un tableau de bord dédié à l'impact environnemental. Chaque cluster expose en continu ses indicateurs de consommation électrique, d'émissions carbone et de coût énergétique. Ces métriques ne sont pas des estimations théoriques : elles sont calculées à partir des relevés réels de nos équipements, avec un facteur d'émission de 0.052 kg CO₂/kWh correspondant au mix énergétique effectif de nos datacenters.



Dashboard Impact Environnemental / RSE — Score Green 85/100

Cette transparence permet à nos clients de suivre leur propre empreinte, de fixer des objectifs de réduction et de les documenter dans leurs rapports RSE ou leurs audits ISO 14001.

10.2 Des indicateurs d'efficacité concrets

Deux métriques résument la performance énergétique de notre plateforme :

- **PUE de 1.4** : pour chaque watt consommé par les serveurs, seulement 0.4 W est dépensé en refroidissement et infrastructure annexe. Ce ratio, inférieur à la moyenne européenne des datacenters (1.6), confirme l'efficacité de nos installations.
- **Densité de 50.1 VMs/kW** : ce ratio traduit notre capacité à héberger un nombre élevé de charges de travail par unité d'énergie consommée, fruit de la consolidation active et du dimensionnement juste des ressources.

10.3 Sobriété logicielle : l'avantage structurel de l'open source

L'approche Proxmox contribue à la sobriété numérique par un mécanisme souvent négligé : l'absence de sur-licensing. Avec VMware, chaque fonctionnalité avancée (DRS, vSAN, NSX) nécessite une licence dédiée, poussant les organisations à acquérir des suites complètes dont elles n'exploitent qu'une fraction. Ce modèle encourage le surdimensionnement logiciel et, par extension, le surdimensionnement matériel pour supporter des composants inutilisés.

Proxmox VE embarque nativement le clustering haute disponibilité, le stockage distribué (Ceph) et le réseau SDN sans couche de licence additionnelle. On déploie uniquement ce que l'on utilise. Cette architecture sobre se traduit par des nœuds moins sollicités par des agents superflus, une surface mémoire réduite et, in fine, une consommation électrique proportionnée au besoin réel.

♦ **Terrain** — *Sur nos 42 nœuds en production, aucun ne supporte de composant logiciel dont la seule justification serait une contrainte de licence. Chaque processus actif remplit une fonction opérationnelle.*

Les organisations qui ne mesurent pas encore leur empreinte IT ne seront pas seulement en retard sur leurs concurrents — elles seront en défaut vis-à-vis des obligations de reporting qui entrent en vigueur dès maintenant.

11

Kubernetes as a Service sur Proxmox

11.1 Proxmox comme socle cloud-native

L'exécution de Kubernetes sur un hyperviseur n'est pas un compromis : c'est un choix d'architecture qui combine l'isolation forte de la virtualisation avec la flexibilité des orchestrateurs de conteneurs. Proxmox offre les prérequis indispensables : API REST complète pour le provisionnement automatisé, support du nested virtualization pour les workloads spécifiques, réseau SDN pour la segmentation, et stockage distribué Ceph pour la persistance.

Contrairement à VMware vSphere + Tanzu, qui impose une stack propriétaire complète (NSX-T pour le réseau, vSAN pour le stockage, vCenter pour l'orchestration), notre approche sur Proxmox repose sur des composants open source interchangeables. Chaque couche peut être remplacée ou mise à jour indépendamment.

11.2 Notre architecture KaaS en production

Nous opérons **2 clusters Kubernetes multi-AZ** sur Proxmox, totalisant **14 nœuds** et **50 clusters Kubernetes**. Chaque cluster est réparti sur 2 zones de disponibilité, avec des control planes distribués pour garantir la résilience.

L'architecture type d'un cluster KaaS comprend :

- **3 VMs control plane** (une par AZ) avec etcd distribué
- **N VMs worker** dimensionnées selon les besoins du client (CPU-intensive, memory-intensive, GPU)
- **3 VMs infrastructure** pour l'ingress controller, le monitoring et le stockage

Le provisionnement est entièrement automatisé via Terraform (création des VMs sur Proxmox) et des opérateurs Kubernetes pour la gestion du cycle de vie des clusters. Nous déployons un nouveau cluster Kubernetes complet en moins de 30 minutes.

11.3 Stack technique et intégration

Notre stack KaaS s'intègre avec **Talos OS** comme système d'exploitation immuable pour les nœuds Kubernetes. Talos OS élimine SSH, le shell et les gestionnaires de paquets : le nœud est géré exclusivement via une API gRPC. Cette approche réduit drastiquement la surface d'attaque et simplifie les mises à jour (rolling upgrade du nœud complet).

Pour le réseau, nous utilisons Cilium en mode eBPF, qui remplace kube-proxy et offre une observabilité native du trafic inter-pods. Le stockage persistant est fourni par Ceph via le CSI driver Rook, exploitant directement le cluster Ceph de l'infrastructure Proxmox sous-jacente.

11.4 Comparaison avec VMware Tanzu

CRITÈRE	VMWARE TANZU	NOTRE KAAS SUR PROXMOX
Licence hyperviseur	vSphere Enterprise+ requis	Proxmox VE (open source, support optionnel)
Réseau	NSX-T obligatoire	Cilium eBPF (open source)
Stockage	vSAN ou baie certifiée	Ceph intégré ou tout backend Proxmox
Coût par cluster	50 000 à 150 000 EUR/an (licences)	Coût du support Proxmox + exploitation
Flexibilité K8s	Versions Tanzu imposées	Toute distribution (Talos, K3s, RKE2)
Verrouillage fournisseur	Élevé	Nul

■ **Chiffre clé** — Sur un périmètre comparable à nos 50 clusters Kubernetes KaaS, le différentiel de coût de licences est considérable. L'économie réalisée finance largement l'expertise d'exploitation d'une stack open source.

♦ **Terrain** — Nos 2 clusters KaaS multi-AZ supportent des workloads variés : applications web stateless et bases de données distribuées. Le provisionnement Terraform + Talos OS nous permet de livrer un cluster Kubernetes opérationnel en moins de 30 minutes. La combinaison Proxmox + Ceph + Cilium offre une stack cloud-native complète, sans aucune dépendance propriétaire.

Pour une démonstration de notre plateforme KaaS : planifiez une session avec nos architectes Kubernetes.

12

Roadmap et support

12.1 Ce que nous offrons : bien plus qu'une migration

Adopter Proxmox VE ne se résume pas à installer un hyperviseur et à convertir des disques virtuels. C'est un changement de socle technologique qui engage les équipes, les processus et les compétences. Nous avons structuré notre offre d'accompagnement autour de cette réalité, parce que nous savons — pour l'avoir vécu nous-mêmes — que la réussite d'une migration se joue autant dans la préparation et le suivi que dans l'exécution technique.

Notre accompagnement couvre trois axes complémentaires. Le **conseil et l'architecture** interviennent en amont : audit de l'existant, dimensionnement de la cible, définition de la trajectoire de migration et planification des vagues. L'**exécution et l'exploitation** assurent la continuité pendant et après la migration : conversion des VMs, reconfiguration réseau et stockage, intégration dans les chaînes de supervision, puis exploitation courante avec monitoring proactif. La **formation et le transfert de compétences** garantissent l'autonomie de vos équipes : sessions pratiques sur l'administration Proxmox, la gestion Ceph, l'automatisation Terraform et Ansible, et les procédures de PRA/PCA.

12.2 Niveaux de service

Nous proposons trois niveaux d'engagement adaptés à la maturité et aux besoins de chaque organisation :

NIVEAU	PÉRIMÈTRE	ENGAGEMENT
Conseil	Assessment, architecture cible, feuille de route	Intervention ponctuelle, livrables documentés
Accompagnement	Migration complète, formation, support post-migration 3 mois	Engagement projet avec jalons et recette formelle
Exploitation managée	Exploitation Proxmox, monitoring, patch management, PRA	Contrat récurrent avec SLA (RTO/RPO documentés)

Chaque niveau inclut un interlocuteur technique dédié et un reporting régulier. Les engagements de service sont formalisés, mesurables et ajustés à votre contexte — pas de grille générique appliquée sans discernement.

12.3 Engagement de continuité

Notre positionnement n'est pas celui d'un intégrateur qui recommande une technologie qu'il ne pratique pas. Nos infrastructures tournent sur Proxmox — chaque jour, en production. Quand nous corrigeons un problème pour un client, il est probable que nous l'ayons déjà rencontré et résolu sur notre propre infrastructure.

Nous ne vous vendons pas une solution, nous la vivons.

Cette proximité avec le terrain garantit que nos recommandations sont ancrées dans la réalité opérationnelle. Nous maintenons une veille active sur les évolutions de Proxmox VE, nous contribuons aux retours vers la communauté, et nous adaptons continuellement nos pratiques en fonction des retours de production.

Notre feuille de route d'accompagnement évolue avec l'écosystème Proxmox : intégration des nouvelles fonctionnalités SDN, amélioration continue de nos runbooks d'exploitation, enrichissement de notre base de connaissances de migration. Vous bénéficiez d'un partenaire qui progresse avec la plateforme, pas d'un prestataire figé sur une version.

♦ **Terrain** — *Chaque incident résolu sur notre propre infrastructure enrichit notre base de connaissances et raccourcit le temps de résolution pour nos clients. L'expertise que nous mettons à votre disposition est forgée par l'exploitation quotidienne, pas par la lecture de documentations.*

Pour définir le niveau d'accompagnement adapté à votre organisation : planifiez un échange avec notre équipe.

13

Conclusion et appel à l'action

13.1 Le moment du choix

Vous avez lu les chiffres du marché. Vous connaissez la trajectoire tarifaire de VMware sous Broadcom. Vous avez vu qu'une alternative technique mature existe, et qu'elle est déjà en production dans des environnements exigeants — y compris le nôtre.

La question n'est plus de savoir si Proxmox VE est prêt. Il l'est. La question est de savoir si votre organisation est prête à engager la réflexion — sereinement, méthodiquement, sans précipitation.

13.2 Ce que nous vous proposons

Nous ne vous demandons pas de prendre une décision aujourd'hui. Nous vous proposons de poser les bases d'une décision éclairée.

Notre approche commence toujours par l'écoute et l'analyse. Chaque infrastructure a son histoire, ses contraintes, ses priorités. Une migration réussie ne commence pas par l'installation de Proxmox — elle commence par la compréhension fine de ce qui tourne, pourquoi, et avec quelles dépendances.

C'est pourquoi nous avons conçu un atelier d'évaluation structuré, sans engagement, qui vous permet en quelques heures de répondre aux questions déterminantes : quel est mon coût VMware réel ? Quel serait mon coût cible sur Proxmox ? Quelles VMs migrer en priorité ? Quels sont les points de vigilance spécifiques à mon environnement ?

13.3 Deux façons d'avancer

Planifiez votre atelier d'évaluation gratuit. En une demi-journée, nos architectes analysent votre environnement actuel, identifient les quick wins et les zones de complexité, et vous remettent une feuille de route chiffrée. Vous repartez avec une vision claire — que vous choisissiez ensuite de travailler avec nous ou non.

Téléchargez notre grille d'audit VMware vers Proxmox. Si vous préférez avancer en autonomie, cet outil vous permet de cartographier votre parc, d'estimer les économies potentielles et d'identifier les prérequis techniques à votre rythme.

13.4 Le mot de la fin

Chaque mois qui passe aux conditions tarifaires actuelles est un mois de surcoût qui ne sera pas récupéré. Mais migrer dans la précipitation serait une erreur tout aussi coûteuse. La bonne trajectoire se situe entre l'immobilisme et l'improvisation : c'est une démarche structurée, progressive, réversible à chaque étape.

Les DSI et responsables d'infrastructure qui engagent cette réflexion aujourd'hui ne prennent pas un risque. Ils se donnent le temps de faire un choix maîtrisé, là où l'attente finira par imposer l'urgence.

Nous avons migré notre propre infrastructure. Nous avons accompagné nos clients. Nous documentons tout, nous partageons nos retours, nous assumons nos limites. Parce que la confiance ne se décrète pas — elle se démontre.

Parlons-en. Les faits sont de notre côté.

| Annexes

A. Glossaire

TERME	DÉFINITION
AZ (Availability Zone)	Zone de disponibilité — segment d'infrastructure physiquement séparé pour garantir la résilience
Ceph	Système de stockage distribué open source, intégré nativement à Proxmox VE
Corosync	Protocole de communication inter-nœuds pour la gestion du quorum dans les clusters Proxmox
eBPF	Extended Berkeley Packet Filter — technologie noyau Linux utilisée par Cilium pour le réseau Kubernetes
Fencing (STONITH)	Mécanisme d'isolation d'un nœud défaillant pour protéger l'intégrité des données en HA
KaaS	Kubernetes as a Service — plateforme de déploiement de clusters Kubernetes managés
KVM	Kernel-based Virtual Machine — module de virtualisation intégré au noyau Linux
LXC	Linux Containers — conteneurs système légers partageant le noyau de l'hôte (disponible dans Proxmox, non utilisé dans nos déploiements)
PBS	Proxmox Backup Server — solution de sauvegarde native avec déduplication et chiffrement
PCA	Plan de Continuité d'Activité
PRA	Plan de Reprise d'Activité
pmxcfs	Proxmox Cluster File System — système de fichiers distribué pour la configuration cluster
RBAC	Role-Based Access Control — contrôle d'accès basé sur les rôles
RPO	Recovery Point Objective — perte de données maximale admissible
RTO	Recovery Time Objective — durée maximale d'interruption admissible
SDN	Software-Defined Networking — gestion réseau programmable
SPOF	Single Point of Failure — point unique de défaillance
Talos OS	Système d'exploitation immuable conçu pour Kubernetes, géré exclusivement via API
VirtIO	Pilotes para-virtualisés pour KVM offrant des performances réseau et disque optimales
VXLAN	Virtual Extensible LAN — protocole d'encapsulation pour étendre les segments réseau entre AZ

B. Tableau comparatif VMware vs Proxmox VE

CRITÈRE	VMWARE VSPHERE	PROXMOX VE
Licence	Propriétaire, par socket/cœur	Open source (AGPLv3), support optionnel
Coût de licence annuel	Élevé, indexé sur le nombre de cœurs	Gratuit ou abonnement support modéré
Hyperviseur	ESXi (propriétaire)	KVM (Linux natif) + LXC disponible
Interface de gestion	vCenter (licence séparée)	Web UI intégrée (pas de coût additionnel)
API d'automatisation	vSphere API (SOAP/REST)	REST API native + CLI pvesh
Haute disponibilité	vSphere HA (licence Enterprise+)	HA intégré sans surcoût de licence
Live migration	vMotion (licence requise)	Migration à chaud intégrée
Stockage distribué	vSAN (licence additionnelle)	Ceph intégré nativement
Réseau logiciel (SDN)	NSX (produit séparé, coût élevé)	SDN intégré (VLAN, VXLAN, EVPN)
Conteneurs	Pas de support natif	LXC disponible + support Kubernetes
Sauvegarde intégrée	Non (Veeam ou équivalent requis)	Proxmox Backup Server (PBS)
Support multi-AZ	Configuration manuelle complexe	Clusters multi-sites natifs
Courbe d'apprentissage	Écosystème propriétaire à maîtriser	Compétences Linux transférables
Communauté	Forums VMware (accès restreint)	Communauté open source active
Verrouillage fournisseur	Fort (formats propriétaires)	Faible (standards ouverts, KVM)
Mise à jour de l'hyperviseur	Dépendante du cycle VMware	Basée sur Debian, cycle prévisible

C. Comparaison sécurité détaillée

CRITÈRE	VMWARE VSPHERE / VCENTER	PROXMOX VE 8.X	COMMENTAIRE
RBAC	Granulaire via vCenter (facturé séparément)	Natif, 4 niveaux hiérarchiques, inclus	Proxmox ne requiert aucun composant supplémentaire
MFA / 2FA	Via vCenter SSO + IdP externe	2FA TOTP natif intégré	Proxmox offre le 2FA sans dépendance tierce
Audit logs	vCenter Events + vRealize Log Insight (licence)	Syslog standard, intégration SIEM directe	Proxmox s'intègre dans les SIEM existants
Chiffrement stockage	vSAN Encryption (licence Enterprise Plus)	AES-256-GCM (PBS) + LUKS + ZFS encryption	VMware plus intégré mais à coût de licence élevé
SDN	NSX-T (licence séparée, coût élevé)	SDN intégré (VLAN, VXLAN, EVPN) inclus	NSX-T plus riche, mais investissement majeur
Firewall natif	NSX DFW (licence NSX requise)	iptables/nftables, 3 niveaux, inclus	Proxmox offre un firewall fonctionnel sans surcoût
Code auditable	Non (propriétaire)	Oui (AGPL v3, code source intégral)	Avantage structurel pour l'auditabilité
Télémétrie	CEIP actif par défaut	Aucune télémétrie, vérifiable dans le code	Proxmox garantit l'absence de fuite de données
Support souverain	Broadcom (USA)	Proxmox GmbH (Autriche, UE) + partenaires FR	Chaîne de support intégralement européenne

D. ROI migration — Postes de coût

POSTE DE COÛT	VMWARE (ANNUEL ESTIMÉ)	PROXMOX (ANNUEL ESTIMÉ)	OBSERVATION
Licences hyperviseur	Élevé	Gratuit ou support standard	Suppression du poste principal
Licence vCenter	Modéré à élevé	Inclus (Web UI)	Pas de composant de gestion séparé
Licence vSAN	Modéré à élevé	Inclus (Ceph natif)	Stockage distribué sans surcoût
Licence NSX	Élevé	Inclus (SDN natif)	Réseau logiciel intégré
Licence sauvegarde (Veeam)	Modéré	PBS inclus	Outil de sauvegarde natif
Support éditeur	Élevé (contrat obligatoire)	Abonnement optionnel	Choix du niveau de support
Formation équipes	Modéré	Modéré (compétences Linux)	Investissement comparable
Coût de migration	N/A	Ponctuel	Coût projet, non récurrent
Total annuel récurrent	Très élevé	Faible	Réduction constatée de 60 à 80 %

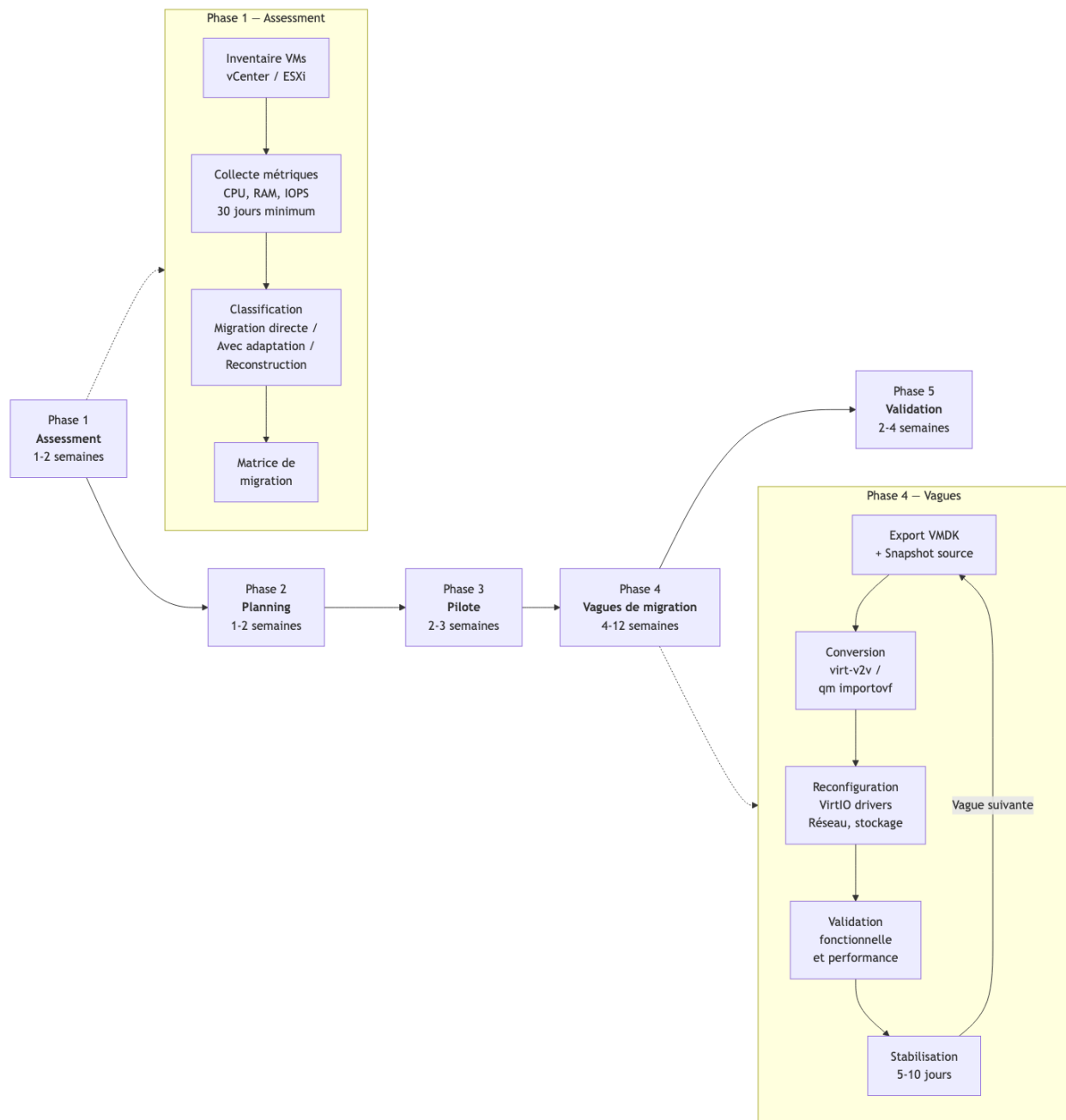
■ **Chiffre clé** — Les économies de licence récurrentes financent le projet de migration dès la première année.

E. Phases de migration — Durées indicatives

PHASE	ACTIVITÉS	DURÉE INDICATIVE	LIVRABLES
1. Assessment	Inventaire VMs, cartographie réseau, analyse des dépendances, audit licences	2 à 4 semaines	Rapport d'inventaire, matrice de dépendances
2. Planning	Matrice de compatibilité, ordonnancement des lots, plan de rollback, dimensionnement cible	2 à 3 semaines	Plan de migration, planning lot par lot
3. Pilote	Migration de 10-20 VMs non critiques, tests fonctionnels, mesure de performance	3 à 4 semaines	Rapport pilote, métriques de référence
4. Vagues de migration	Lots de 50-100 VMs, migration à chaud ou à froid selon criticité, validation par lot	8 à 16 semaines	PV de recette par lot, suivi des incidents
5. Validation finale	Tests de charge, audit sécurité, conformité, transfert de compétences, décommissionnement VMware	2 à 4 semaines	Rapport final, documentation opérationnelle
Total estimé		17 à 31 semaines	

♦ **Terrain** — Ces durées sont issues de nos projets réels. Le programme de 1 500 VMs est structuré en vagues successives avec validation intermédiaire à chaque lot.

F. Pipeline de migration VMware vers Proxmox



Pipeline de migration VMware vers Proxmox

Légende : Méthodologie en 5 phases, validée sur 350 VMs migrées, appliquée au programme de 1 500 VMs. Taux de migration directe supérieur à 95 %. Temps moyen : 45 min par VM standard, 2 h par VM avec tests approfondis. Rollback en moins de 15 minutes.