Mise en place d'un cloud privé hautement disponible
(Proxmox® - Ceph – Terraform – Ansible)

Soutenu par : RECULE Damien
Organisme de formation : NEXT FORMATION – Paris
Période du 11/09/2025 au 21/04/2026
Confidentialité : Document réservé aux membres du jury et au cadre pédagogique.
Version du document : 3.1

Projet réalisé dans le cadre de la validation du titre professionnel

Administrateur d'Infrastructures Sécurisées

nextformation

NOVATECH
SOLUTIONS

NEBTECH.FR

Mise en place d’un cloud privé hautement disponible

(Proxmox® - Ceph – Terraform – Ansible - Jenkins)

Table des mises à jours du document

Version	Date	Auteur	Description de la mise à jour
1.0	20/09/2025	RECULE Damien	Création initiale du document
1.1	22/09/2025	RECULE Damien	Ajout structure initiale et sommaire
1.2	25/09/2025	RECULE Damien	Ajout de l'introduction, préface
1.3	02/10/2026	RECULE Damien	Remerciements et présentation du contexte.
1.4	05/10/2026	RECULE Damien	Ajout de la présentation des entreprises
1.5	07/10/2025	RECULE Damien	Rédaction complète de l'analyse du besoin, objectifs, QQQQCCP et diagrammes
1.6	10/10/2025	RECULE Damien	Ajout du diagramme de la bête à cornes, pieuvre, Ishikawa et analyse fonctionnelle.
1.7	17/10/2025	RECULE Damien	Ajout du Cahier des Charges Fonctionnel et Technique (CDCF & CDCT).
1.8	20/10/2025	RECULE Damien	Méthodes, risques (AMDEC) et Gantt prévisionnel
1.9	21/10/2025	RECULE Damien	Ajout de la conception technique : architecture réseau, Ceph, OPNSense, Proxmox.
2.0	03/11/2025	RECULE Damien	Ajout diagrammes UML, WBS
2.1	07/11/2025	RECULE Damien	Ajout de la matrice RACI
2.2	10/11/2025	RECULE Damien	Ajout organigramme fonctionnel, architecture globale.
2.3	12/11/2025	RECULE Damien	Ajout du schéma réseau
2.4	15/12/2025	RECULE Damien	Rédaction de la phase de réalisation : installation, configuration, Dashboard Flask.
2.5	16/12/2025	RECULE Damien	Mise à jour du budget : matériel, licences, coût TCO / ROI.
2.6	22/12/2025	RECULE Damien	Mise à jour risques, finalisation des annexes techniques.
2.7	23/12/2025	RECULE Damien	Corrections globales
2.8	24/12/2025	RECULE Damien	Uniformisation du style, ajout des légendes et schémas
2.9	28/12/2025	RECULE Damien	Finalisation du document pour soutenance
3.0	29/12/2025	RECULE Damien	Relecture et mise en forme.
3.1	23/01/2026	RECULE Damien	Relecture finale et mise en forme définitive.

Table des illustrations

Liste des abréviations

Abréviation	Signification	Description / Contexte projet
VM	Virtual Machine	Machine virtuelle déployée via Terraform sur Proxmox.
IAC	Infrastructure As Code	Concept d'automatisation de l'infrastructure via du code (Terraform, Ansible).
CI/CD	Continuous Intégration Continuous Deployment	Pipeline automatisé (Jenkins) pour déployer, tester et livrer en continu.
API	Application Programming Interface	Interface utilisée par Terraform pour communiquer avec Proxmox.
LAN	Local Area Network	Réseau interne (VLANs 10 / 20 / 30 / 40).
WAN	Wide Area Network	Accès Internet via box Free (port SFP+).
VLAN	Virtual Local Area Network	Segmentation réseau (Prod, Storage, Management…).
HA	High Availability	Haute disponibilité (Proxmox + Ceph).
HDD/SSD/NVMe	Hard Drive / Solid State Drive / Non-Volatile Memory Express	Types de stockage des nœuds Proxmox.
RBD	RADOS Block Device	Format de disque distribué utilisé par Ceph.
OSD	Object Storage Daemon	Processus Ceph stockant physiquement les données.
MON	Monitor	Service Ceph qui gère le quorum du cluster.
MGR	Manager	Service Ceph qui fournit la supervision et les métriques.
PBS	Proxmox Backup Server	Solution de sauvegarde utilisée pour les VM.
PVE	Proxmox Virtual Environment	Hyperviseur utilisé pour le cluster.
QEMU	Quick Emulator	Technologie de virtualisation utilisée par Proxmox.
LXC	Linux Container	Conteneur léger géré par Proxmox (optionnel).
SSH	Secure Shell	Accès sécurisé utilisé par Ansible et les administrateurs.
YAML	Yet Another Markup Language	Format utilisé par cloud-init et Ansible.
JSON	JavaScript Object Notation	Format utilisé pour certaines API et configs Terraform.
DNS	Domain Name System	Résolution de noms pour les VM et services.
ACL	Access Control List	Règles d'accès sur OPNSense / Ceph / Proxmox.
TFA / MFA	Two-Factor Authentication Multi-Factor Authentication	Sécurisation des comptes Proxmox / Jenkins.
UPS	Uninterruptible Power Supply	Onduleur pour sécuriser l'alimentation.
PDU	Power Distribution Unit	Barre d'alimentation intelligente dans la baie.
SFP+	Small Form-Factor Pluggable Plus	Port 10 Gbit utilisé pour uplinks switch ↔ OPNSense ↔ Freebox.
NIC	Network Interface Card	Carte réseau utilisée pour les VLAN, Ceph, management.
GUI	Graphical User Interface	Interface graphique (Proxmox WebUI, Dashboard Flask).
CLI	Command Line Interface	Ligne de commande (Terraform, Ansible, Jenkins CI).
HTTP(S)	HyperText Transfer Protocol (Secure)	Accès web à Proxmox, OPNSense, dashboard.
FW	Firewall	OPNSense dans ton projet.
IaC Pipeline	Infrastructure As Code Pipeline	Chaîne Terraform → Ansible → Jenkins.
MAC	Media Access Control	Adresse matérielle réseau.
IPAM	IP Address Management	Gestion des adresses IP (répartition VLAN).
OIDC	OpenID Connect	Authentification possible pour Proxmox / Jenkins.
CA	Certificate Authority	Autorité de certification (sécurisation TLS).
RBAC	Role-Based Access Control	Gestion des permissions sous Proxmox / Jenkins.
PKI	Public Key Infrastructure	Infrastructure de certificats TLS.
PoE	Power over Ethernet	Switch administrable qui peut fournir de l'alimentation
VPN	Virtual Private Network	WireGuard sur OPNSense (accès admin distant).
WG	Wireguard	Protocol VPN utilisé pour l'administration sécurisée.
AD	Active Directory	Service d'annuaire Microsoft

Table des matières

I. Préface

Présentation et objectifs personnels

Depuis mon enfance, l'informatique occupe une place essentielle dans mes centres d'intérêt. C'est au début des années 80 que j'ai découvert mes premiers ordinateurs (Atari STE, Amiga), puis plus tard les plateformes Intel 80486DX et 80486DXII 66. Ils ont éveillé en moi une passion profonde pour les systèmes, la logique et la technologie. Cette curiosité initiale ne m'a jamais quitté, même lorsque mon parcours professionnel m'a orienté vers un tout autre domaine.

Après une scolarité classique, j'ai rejoint le secteur automobile et intégré le groupe Renault, où j'ai travaillé près de trente ans au sein des chaînes de production. J'y ai progressivement évolué jusqu'à devenir responsable de la programmation des robots industriels, notamment via les systèmes professionnels KUKA.

Cette expérience m'a permis de développer une grande rigueur technique, une capacité d'analyse aiguisée et une méthodologie structurée, des compétences que l'on retrouve naturellement dans l'administration système et réseau.

En 2022, porté par l'envie de me consacrer plus amplement à ma passion pour l'informatique, j'ai entamé une reconversion professionnelle. J'ai d'abord appris en autodidacte les bases des systèmes, des réseaux et des environnements Windows et Linux, avant d'intégrer la formation de *Technicien Supérieur Systèmes et Réseaux* au sein de l'organisme de formation NextFormation. Cette première étape a renforcé mon intérêt pour les infrastructures, la sécurité et l'automatisation, ce qui m'a conduit naturellement vers la formation d'*Administrateur d'Infrastructures Sécurisées,* que je poursuis aujourd'hui avec motivation et détermination.

En parallèle de mon parcours technique et après 30 ans d'étude en égyptien hiéroglyphique au sein de l'Institut Khéops et l'école du Louvre, je suis depuis plus de treize ans pigiste pour un magazine spécialisé en égyptologie (Pharaon Magazine), où je traduis des textes littéraires en hiéroglyphes. Cette activité, exigeant patience, précision et sens du détail, complète parfaitement les qualités nécessaires au travail d'un administrateur systèmes et réseaux : constance, minutie, grande rigueur documentaire et maîtrise des outils intellectuels.

C'est dans ce contexte mêlant reconversion, passion ancienne et montée en compétences progressive que s'inscrit ce projet de fin d'étude. La conception d'un cloud privé automatisé, associé à un Dashboard complet développé en Flask/Python, représente pour moi bien plus qu'un exercice technique, c'est la synthèse de mon expérience industrielle, de ma méthodologie acquise en formation, et de ma volonté d'apprendre et de créer par moi-même.

À l'issue de ma formation d'*Administrateur d'Infrastructures Sécurisées*, j'ambitionne de poursuivre mon parcours au sein de NextFormation en préparant la certification de *Formateur pour Adultes,* afin de transmettre à mon tour les compétences que j'ai acquises et accompagner d'autres apprenants dans leur évolution professionnelle.

Ce rapport traduit non seulement le travail technique fourni, mais également le chemin parcouru, la reconversion accomplie et la passion qui continue de me guider.

RECULE Damien

II. Introduction

II.1 Contexte et objectifs du document

Ce mémoire de fin d'études est réalisé dans le cadre de l'obtention du titre d'*Administrateur d'Infrastructures Sécurisées*. Il sera soutenu devant un jury composé de professionnels du secteur et s'appuiera sur un projet concret et particulièrement enrichissant : la mise en place d'un cloud privé hautement disponible, que j'ai eu l'opportunité de concevoir et de déployer cette année au sein de mon infrastructure personnelle. J'atteste que ce document est le fruit de mon travail personnel et des efforts que j'ai consacrés à sa réalisation.

II.2 Remerciements

Je souhaite exprimer ma profonde gratitude à l'ensemble des personnes qui ont contribué, de près ou de loin, à l'élaboration de ce mémoire. Leur accompagnement, leur confiance et leurs encouragements ont constitué une aide précieuse tout au long de ce projet.
Je remercie tout particulièrement mes deux tuteurs de stages, Maxime Glorieux et Edouard COT ainsi que l'ensemble de mes formateurs, dont les conseils avisés, la disponibilité constante et l'expertise professionnelle ont guidé chacune des étapes de mon travail. Leur exigence bienveillante et leur sens du partage ont largement participé à l'enrichissement de mes connaissances et au développement de mes compétences.
J'adresse également mes sincères remerciements à mes collègues et camarades, dont le soutien, les échanges constructifs et l'esprit de collaboration ont favorisé un climat d'apprentissage stimulant et motivant.
Enfin, je tiens à exprimer toute ma reconnaissance à ma famille et à mes proches. Leur patience, leur compréhension et leur présence indéfectible ont été pour moi une source essentielle de réconfort et de motivation tout au long de la rédaction de ce document.

II.3 Les parties prenantes

Dans le cadre de ce projet, plusieurs parties prenantes interviennent et contribuent directement ou indirectement à sa réussite.

A. Le porteur du projet (Parcours et missions réalisées)

Le premier acteur est moi-même, en tant qu'auteur et concepteur du projet.
Mon rôle a consisté à définir les besoins techniques et fonctionnels, concevoir l'architecture de la solution, développer le Dashboard en Flask/Python, intégrer et automatiser les outils (Proxmox, Terraform, Ansible, Jenkins), assurer les tests, la documentation et la mise en production.
Mon implication personnelle est centrale, le projet s'inscrivant dans un parcours de reconversion professionnelle, d'autoformation et de montée en compétence continue.

Au cours de ma formation et de mes expériences professionnelles en reconversion, j'ai été amené à participer à plusieurs projets techniques et organisationnels qui ont consolidé mes compétences en administration système, en gestion d'infrastructures, en cyber sécurité et en gestion de projet.
Ces missions m'ont permis d'acquérir une vision globale du fonctionnement d'un système d'information moderne, tout en développant une méthodologie rigoureuse et une capacité d'adaptation essentielle au métier d'administrateur d'infrastructures sécurisées.

A.1 Mise en œuvre d'un serveur de stockage pour le service PAO

Dans le cadre de mon stage qui s'est déroulé du 10/02/2026 au 10/04/2026, j'ai été amené à participer à l'amélioration des performances et de la gestion des ressources du service PAO des *Caisses d'allocations familiales* respectivement situées 82 rue Brûle-Maison à Lille et 124 boulevard Gambetta à Roubaix.

Cette mission comportait les actions suivantes :

- Analyse des besoins en capacité, redondance et performances.
- Sélection d'une architecture de stockage adaptée (NAS/SAN).
- Installation et configuration du serveur (système, RAID, services).
- Mise en place des partages réseau (SMB/NFS) et gestion fine des ACL.
- Optimisation des performances en fonction des charges PAO.
- Réalisation des tests, validation, documentation et mise en production.

Ce projet m'a permis de développer des compétences solides en gestion du stockage, en administration système et en sécurisation de données critiques.

A.2 Participation à une campagne de sensibilisation à la sécurité informatique

Conscient des risques liés aux comportements utilisateurs, j'ai également contribué à l'élaboration d'un programme interne de sensibilisation à la cyber sécurité.
Cette campagne avait pour objectif d'améliorer la posture de sécurité globale de l'entreprise.

Mes actions :

- Identification des failles organisationnelles liées aux usages.
- Rédaction de supports pédagogiques : affiches, guides, communications internes.
- Création de contenus liés au phishing, à la gestion des mots de passe, aux usages mobiles.
- Vulgarisation de notions techniques pour les rendre accessibles à tous.
- Participation au déploiement de la campagne dans les différents services.

Cette mission m'a permis de renforcer mes compétences en cyber sécurité, communication, pédagogie et conduite du changement.

A.3 Réalisation d'un projet « Maison de Santé du Bidou »

Avant de réaliser le projet de Cloud Privé présenté dans ce dossier, j'ai conçu et mené à terme un premier projet complet d'infrastructure informatique : *la Maison de Santé du Bidou*.

Ce projet, effectué dans un contexte pédagogique, m'a permis de consolider mes compétences techniques et méthodologiques à travers une architecture réseau multi-VLAN, sécurisée et opérationnelle.

Présentation générale du projet

La *Maison de Santé du Bidou* est un établissement fictif regroupant plusieurs professionnels de santé (médecins, infirmiers, psychologues, secrétariat, dentistes, sécurité, etc.).

L'objectif était de concevoir une infrastructure informatique complète, intégrant :

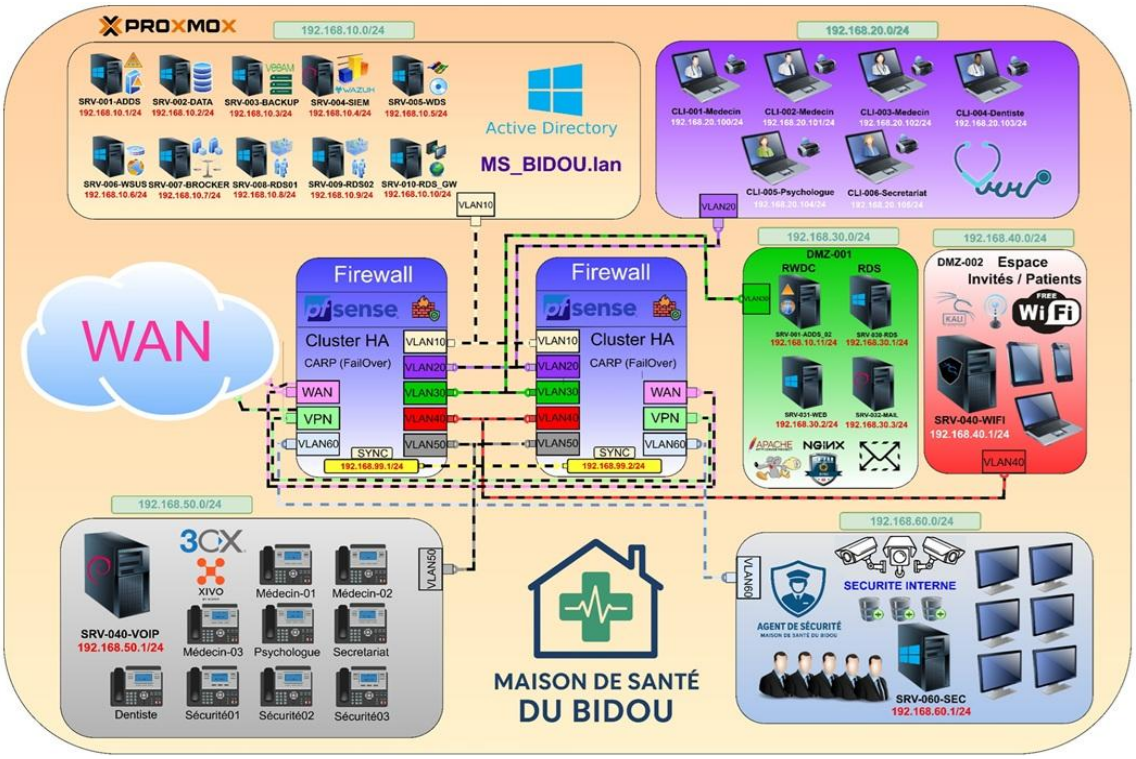
- Un réseau isolées et sécurisées.
- Des postes et serveurs répartis en VLAN.
- Une haute disponibilité firewall (PFSense HA CARP).
- Des services Active Directory, RDS, Web, VoIP, caméra IP.
- Une DMZ sécurisée pour les accès externes et les invités.

- Une supervision et une gestion des logs.

L'infrastructure conçue devait répondre aux besoins d'un établissement médical moderne : sécurité, confidentialité, disponibilité, résilience, gestion fine des réseaux métiers et invités.

Architecture réseau mise en place

L'architecture complète est représentée dans le schéma ci-dessous :



Projet Maison de santé du Bidou

Détails de l'infrastructure

Cluster de virtualisation Proxmox

- Segmentation réseau par VLAN (10 / 20 / 30 / 40 / 50 / 60).
- Firewalling – PFSense - cluster HA (CARP)
- Réseaux WAN, VPN, DMZ, invités.
- Interface SYNC dédiée pour HA.
- Active Directory : domaine *MS_BIDOU.lan*
- DNS, DHCP, WSUS, WDS.
- Serveur Web / Mail / RDS.

DMZ

- Services Web et accès distant sécurisés.
- Bornes Wifi invité isolées.

Téléphonie VoIP

- Serveur VoIP (3CX / XIVO).
- Postes téléphoniques dédiés aux médecins, secrétariat, dentiste.

Vidéo-protection & sécurité

- VLAN caméra dédié.

- Serveur supervision interne.

L'ensemble a été conçu de manière professionnelle, segmentée, sécurisée et conforme aux bonnes pratiques (séparation des flux, zones de confiance, DMZ, accès invités isolés…).

Compétences mobilisées

Conception et administration d'un réseau sécurisé

- Mise en place d'un plan d'adressage structuré.
- Segmentation du réseau en VLAN métiers, invités, caméra, DMZ.
- Déploiement d'une infrastructure firewall en haute disponibilité (OPNSense HA CARP).
- Rédaction et application de politiques de filtrage et de routage sécurisées.
- Isolation réseau des flux sensibles (AD, caméras).

Mise en œuvre d'un environnement Active Directory sécurisé

- Installation d'ADDS (domaine : MS_BIDOU.lan).
- Mise en place d'un DNS/DHCP AD-intégrés.
- Structuration des OU, GPO de sécurité et gestion des stratégies utilisateur.
- Déploiement de services complémentaires (WSUS, WDS, RDS).

Administration des systèmes virtualisés

- Création et gestion des VM sous Proxmox.
- Isolation réseau via bridges + VLAN.
- Mise en place de snapshots et bonnes pratiques de virtualisation.

Déploiement d'un cluster virtualisé

- Utilisation de Proxmox VE pour centraliser les services du SI.
- Virtualisation des firewalls, serveurs métier et services AD.
- Gestion de la disponibilité élevée via la duplication des firewalls.

Services en DMZ et gestion des zones exposées

- Déploiement de services Web et Email en zone isolée.
- Mise en place d'une DMZ sécurisée pour accès externes.
- Architecture multizones conforme aux bonnes pratiques (LAN, DMZ, WAN, Guests)

Téléphonie IP et infrastructure VoIP

- Déploiement d'un serveur 3CX/XIVO virtualisé.
- Intégration des postes VoIP dans le VLAN téléphonie.

Sécurité interne et vidéo-protection

- Intégration d'un réseau caméra IP dédié.
- Mise en place d'un serveur de supervision du système de sécurité.
- Isolation totale du VLAN caméra du reste du SI.

Documentation, supervision et gestion des incidents

- Documentation technique complète (schémas, plan IP, topologie).
- Centralisation des logs via OPNSense + supervision des serveurs.
- Analyse et résolution des incidents de connectivité (routage, ACL, VLAN).

Méthodologie et gestion de projet (C12)

- Analyse des besoins et rédaction du cahier des charges initiales.
- Réalisation du schéma d'architecture final.
- Planification, organisation des tâches et justification des choix techniques.
- Présentation du projet finalisé (communication professionnelle).

A.4 Formation complémentaire

Dans le cadre de ma reconversion et afin de renforcer mes compétences techniques au-delà du programme officiel de la formation d'Administrateur d'Infrastructures Sécurisées, j'ai suivi plusieurs formations supplémentaires, toutes validées par des certifications.
Ces apprentissages volontaires témoignent de ma volonté de monter rapidement en compétence, d'acquérir une autonomie technique solide et de maîtriser les technologies indispensables à la mise en place d'infrastructures modernes.

Certifications obtenues

- **Certification - Docker – Conteneurisation & orchestration avancé**

Cette formation m'a permis d'acquérir une compréhension avancée des principes de conteneurisation, de la gestion des images et de l'isolation applicative.
Utilisé pour effectuer des test hors production, cette compétence a renforcé ma compréhension des environnements virtualisés et des pipelines DevOps.

- **Certification - Python – La formation complète**

Python étant au cœur de mon projet (backend du dashboard, interactions API, monitoring), cette certification a constitué une base essentielle pour développer une application robuste, sécurisée et maintenable.

- **Certification - Flask – Développement Web Python avec Flask**

Cette formation m'a permis de comprendre et mettre en œuvre la structure d'une application Flask complète, la gestion des routes, des templates et des sessions, l'intégration d'API externes (ici : API Proxmox) et la sécurisation des applications web (HTTPS, authentification).
C'est grâce à ces compétences que j'ai pu développer intégralement le Dashboard utilisé dans ce projet.

- **Certification - Windows Server 2025 – Administration & Sécurité**

Cette formation couvre la gestion de l'Active Directory, la mise en place d'ADCS (PKI), utilisée ici pour générer un certificat HTTPS, les stratégies de sécurité avancées, la supervision et les bonnes pratiques de durcissement.
Elle a contribué directement à sécuriser mon infrastructure et à comprendre les enjeux d'authentification centralisée.

- **Certificats - Kubernetes - Installation & Configuration**

Cette formation apporte les bases techniques et méthodologiques nécessaires à la mise en œuvre de clusters Kubernetes, en couvrant l'architecture, le réseau, le déploiement d'applications conteneurisées et la gestion de la haute disponibilité en environnement de production.

- **Certificats – ANSSI**

Dans le cadre de sa mission de sensibilisation, l'ANSSI propose SecNum*académie* pour former le plus grand nombre de citoyens à la sécurité du numérique. Ce nouveau support de cours en ligne a pour objectif de sensibiliser les utilisateurs en milieu professionnel à la sécurité du numérique afin qu'ils deviennent acteurs de leur sécurité et de celle de leur entreprise.

Apport au projet

Ces certifications m'ont permis d'acquérir une vision transversale des technologies modernes, couvrant la virtualisation, la sécurité, l'automatisation et le développement.

Elles ont constitué des leviers essentiels pour concevoir et développer un dashboard fiable, sécurisé et ergonomique, mettre en œuvre des automatisations cohérentes via Terraform et Ansible, renforcer la sécurité globale de l'environnement, et structurer une architecture pérenne alignée sur les pratiques professionnelles et les recommandations actuelles.

Elles ont également contribué à une meilleure prise en compte des enjeux d'exploitation, de supervision et d'évolutivité dès la phase de conception.

L'ensemble des certificats est fourni en annexe du dossier.

B. L'organisme de formation

nextformation

Mon organisme de formation, NextFormation (Paris), joue un rôle central dans la création de mon projet, en assurant l'accompagnement pédagogique, la mise à disposition des ressources techniques, ainsi que le suivi méthodologique nécessaire à la bonne conduite du projet.

Son rôle a été d'assurer la transmission des compétences techniques fondamentales, d'encadrer méthodologiquement le projet et de fournir un cadre pédagogique pour mener à bien cette réalisation.

Les formateurs m'ont apporté leur expertise en sécurité informatique, administration système et gestion d'infrastructures, garantissant la cohérence technique et la conformité aux bonnes pratiques du métier.

De plus, l'équipe pédagogique a assuré un suivi régulier, des retours constructifs et un cadre structuré permettant d'orienter le projet vers des objectifs réalistes et opérationnels.

Enfin, les autres acteurs tels que les apprenants du groupe et les professionnels rencontrés contribuent eux aussi par leurs échanges et leurs retours d'expérience faisant de ce projet un travail collaboratif s'inscrivant pleinement dans un contexte professionnel.

C. Les éditeurs et communautés open source

Bien que n'ayant pas pris part directement à la conduite du projet, les communautés et les éditeurs des technologies mobilisées (notamment Proxmox, Ansible, Jenkins, Python/Flask, Ceph, Terraform, Graylog, Postfix et Docker) doivent également être considérés comme des parties prenantes « externes » à part entière.

En effet, leur contribution dépasse largement la simple mise à disposition d'outils. Elle s'incarne dans la qualité et l'accessibilité de la documentation officielle, dans la richesse des forums d'entraide et des espaces collaboratifs, ainsi que dans la production continue de guides, de recommandations méthodologiques et de bonnes pratiques relatives au déploiement, à l'automatisation et à l'observabilité des systèmes.

L'expertise collective issue de ces communautés techniques constitue un socle de connaissances essentiel, dont la maturité et la fiabilité ont permis d'élaborer une solution robuste, conforme aux standards contemporains de l'ingénierie logicielle et de l'infrastructure informatique. Leur apport s'avère ainsi déterminant dans l'intégration, l'optimisation et la pérennisation des différentes briques technologiques mises en œuvre au sein du projet.

II.4 Présentation de l'entreprise NebTech (Prestataire)

A. Historique et activité

Située à Saint Amand-les-eaux (59), NebTech a été fondée en 2010 par un groupe d'ingénieurs spécialisés en informatique et télécommunications. L'objectif initial de l'entreprise était de fournir des services d'hébergement pour les petites entreprises et de gérer leurs infrastructures informatiques de manière externalisée.

Au fil des années, elle s'est développée rapidement et a élargi ses services pour inclure l'infogérance complète (administration des systèmes et réseaux).

Figure 1 Entreprise NebTech

Aujourd'hui, NebTech compte plusieurs dizaines de collaborateurs et gère plus de 100 clients actifs sur son infrastructure.

L'activité principale de NebTech Solutions repose sur l'hébergement et l'infogérance d'infrastructures IT pour ses clients. Les services proposés incluent l'hébergement de serveurs et d'applications ainsi que la mise à disposition de serveurs physiques et virtuels pour les clients. Elle propose également la gestion et la maintenance des systèmes (suivi, mise à jour et sécurisation des serveurs et des applications), la sauvegarde (sécurité des données), tout comme la virtualisation de serveurs et de postes de travail.

Elle intervient enfin dans le déploiement de clusters Proxmox, VMware ou autres solutions cloud, le support technique et l'assistance hotline, l'intervention sur site et à distance et dans les audits de sécurité.

Chiffre d'affaires

Le chiffre d'affaires de la NebTech présente une croissance régulière sur la période 2020–2025, passant de 1,5 M€ à une prévision de 3,2 M€ en 2025, soit une progression de plus de 113 % en 5 ans.

- **2020** : 1,5 millions d'euros
- **2021** : 2,3 millions d'euros
- **2022** : 2,5 millions d'euros

2023 : 2,7 millions d'euros

2024 : 2,5 millions d'euros

2025 (Prévision) : 3,2 millions d'euros

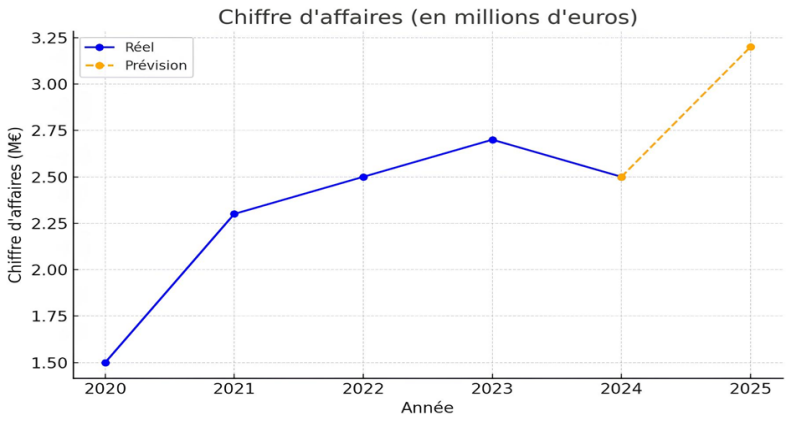


Figure 2 Chiffre d'affaires NebTech

B. Organisation et rôle dans le projet

Organigramme

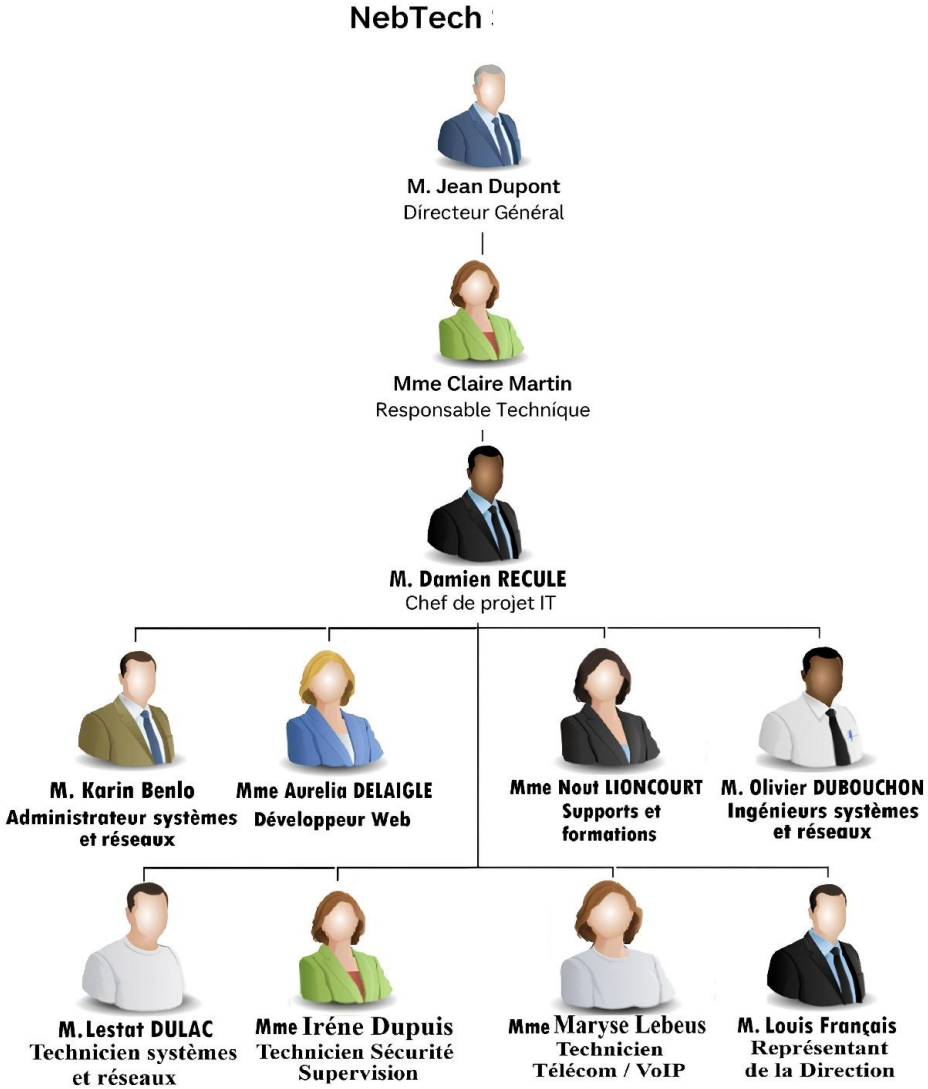


Figure 3 Organigramme NebTech

Rôle de NebTech dans le projet

NebTech intervient en tant que prestataire informatique et intégrateur technique chargé de la conception, du déploiement et de l'automatisation du cloud privé de NovaTechSolutions. L'entreprise met à disposition une équipe pluridisciplinaire composée d'un chef de projet IT, d'administrateurs systèmes et réseaux, de spécialistes sécurité, d'un développeur web et d'un pôle support/formation.

Les interactions entre NebTech, NovaTechSolutions et les autres acteurs du projet sont analysées plus en détail dans la phase d'analyse fonctionnelle, notamment à travers les diagrammes de la pieuvre et le diagramme RACI.

II.5 Présentation de l'entreprise NovaTechSolutions (Client)

A. Historique et activité

Fondée en 2019**,** NovaTechSolutions est une entreprise française basée à Lille**,** spécialisée dans le développement de logiciels d'entreprise**,** la gestion de données et les solutions numériques pour PME.

Depuis sa création, NovaTechSolutions a grandi rapidement et s'est imposée comme un acteur clé dans la gestion d'applications métiers, l'édition de logiciels internes, le traitement de données structurées ainsi que le support informatique pour entreprises locales.

L'entreprise est née de la volonté de trois ingénieurs passionnés d'infrastructure IT, de cyber sécurité et d'automatisation, qui ont constaté que de nombreuses PME françaises manquaient d'outils modernes pour exploiter le plein potentiel des solutions numériques.

Figure 4 Entreprise NovaTechSolutions

NovaTechSolutions ambitionne de transformer le numérique des PME en simplifiant l'accès aux technologies modernes. Son objectif est de fournir un environnement logiciel fiable, sécurisé et évolutif, capable d'accompagner la croissance des entreprises locales.

Positionnée dans un marché en croissance, NovaTechSolutions développe et maintien des solutions logicielles utilisées dans la logistique, la santé, les services financiers, les commerces de proximité ou encore l'industrie légère, notamment des applications web internes, des outils de gestion de stock, des plateformes de suivi client et des applications d'analyses et de reporting.

Chiffre d'affaires

Le chiffre d'affaires de NovaTechSolutions présente une croissance plutôt régulière depuis 2021, passant de 1,5 M€ à une prévision de 1.9 M€ en 2025, soit une progression de plus de 26.7 % en 4 ans.

2019 : 1,3 millions d'euros

2020 : 1,1 millions d'euros

2021 : 1,5 millions d'euros

2022 : 1,7 millions d'euros

2023 : 1,5 millions d'euros

2024 : 1,4 millions d'euros

2025 : (Prévision) : 1.9 millions d'euros

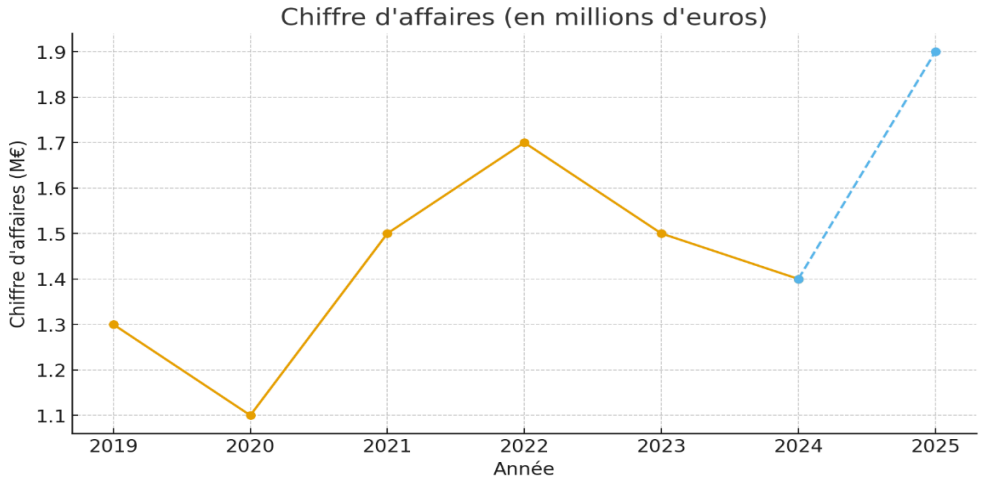


Figure 5 Chiffre d'affaires NovaTechSolutions

B. Organisation et rôle dans le projet

Organigramme

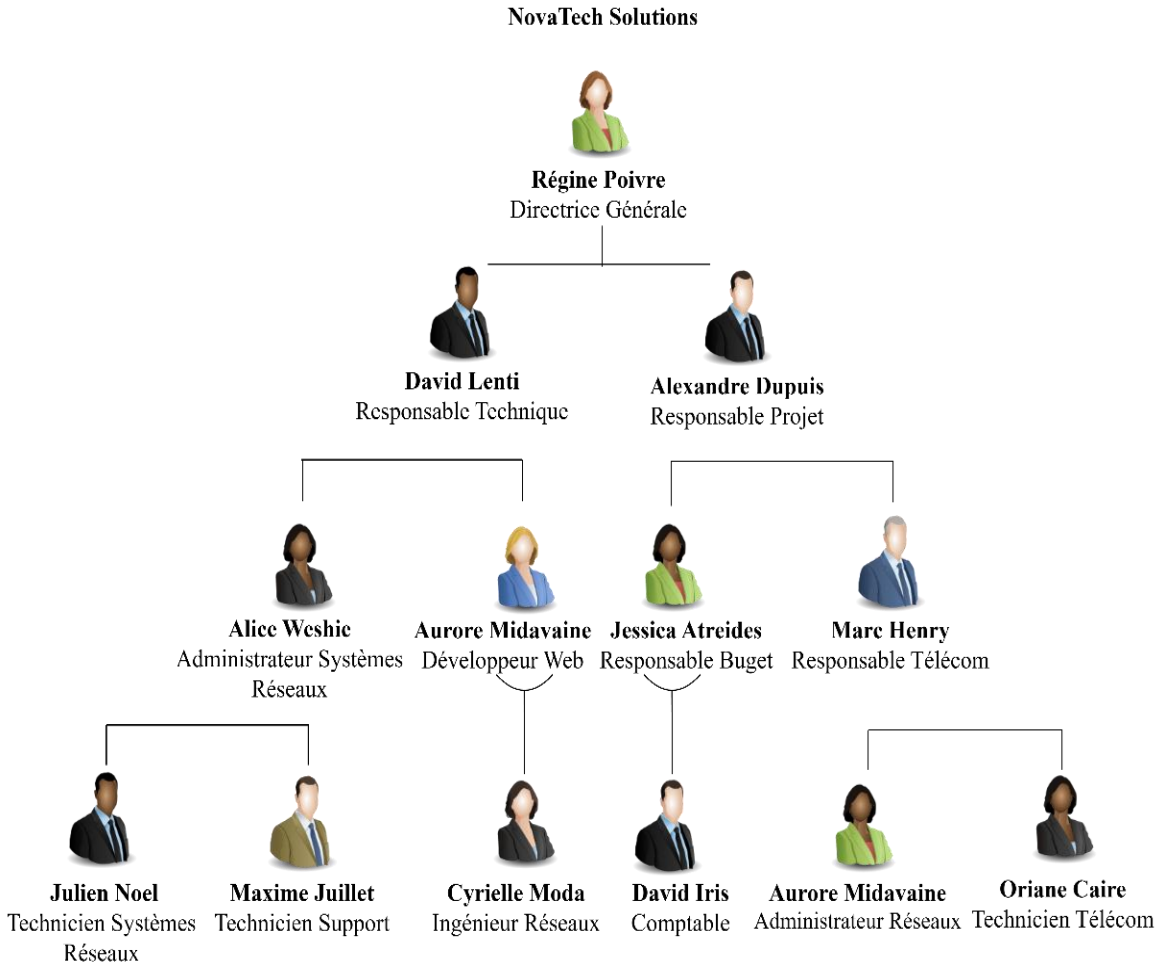


Figure 6 Organigramme NovaTechSolutions

Rôle dans le projet

NovaTechSolutions intervient dans ce projet en tant qu'entreprise cliente et bénéficiaire de la solution mise en œuvre.
À ce titre, elle exprime les besoins fonctionnels et opérationnels, définit les contraintes métiers et valide les orientations proposées tout au long du projet.
L'entreprise fournit également l'environnement existant servant de base à l'audit initial, permettant d'identifier les axes d'amélioration et de construire une architecture cible adaptée à ses enjeux.
NovaTechSolutions participe aux phases de validation, notamment lors des étapes de recette fonctionnelle et de mise en production, afin de s'assurer que la solution répond aux attentes en matière de performance, de sécurité et d'exploitabilité.
Enfin, l'entreprise est destinataire des livrables techniques et documentaires, ainsi que de la formation associée, garantissant une appropriation durable de la solution.

III. Audit Initial et analyse de l'existant

(Rapports d'audit en Annexe du document).

III.1 Objectifs et périmètre de l'audit

A. Objectif de l'audit

L'audit a pour objectif d'évaluer le niveau de maturité de l'infrastructure existante de NovaTechSolutions afin d'identifier les axes d'amélioration en matière de :

- Disponibilité et continuité de service.
- Sécurité des accès et des données.
- Automatisation et industrialisation.
- Supervision et exploitation quotidienne.

Cet audit vise à fournir une base factuelle permettant de définir une architecture cible plus résiliente, sécurisée et adaptée à un usage en production.

B. Périmètre de l'audit

L'audit porte sur :

- L'infrastructure de virtualisation Proxmox VE.
- L'architecture réseau et les flux.
- Les mécanismes de sécurité et de contrôle des accès.
- Les processus d'exploitation (déploiement, supervision, sauvegarde).

Le matériel n'est pas remis en cause : l'audit se concentre sur les pratiques, l'architecture et l'exploitation.

III.2 Méthodologie d'audit retenue

L'audit s'appuie sur une démarche de type audit de maturité, inspirée des bonnes pratiques :

- ISO 27001 (sécurité de l'information).
- Recommandations de l'ANSSI.
- Exigences MIS1 / MIS2.

A. Étapes de la méthodologie

1. Analyse documentaire (schémas, configurations existantes)
2. Observation de l'architecture en place
3. Identification des dysfonctionnements et risques
4. Analyse des causes (diagramme d'Ishikawa)
5. Synthèse des constats et priorisation des axes d'amélioration

Cette approche permet de ne pas traiter uniquement les symptômes, mais bien les causes racines.

III.3 Constat de l'infrastructure existante

A. Architecture et exploitation

L'infrastructure existante repose sur :

- Un unique nœud Proxmox VE.
- Absence de haute disponibilité.
- Stockage local externe (USB).

Les principales limites identifiées sont :

- Absence de tolérance à la panne.
- Indisponibilité totale en cas de défaillance du nœud.
- Processus de création et de gestion des machines virtuelles entièrement manuels.
- Temps de déploiement long et non standardisé.

L'architecture est fonctionnelle, mais peu adaptée à un contexte de production.

B. Sécurité et gestion des accès

L'audit met en évidence :

- Une gestion des accès peu centralisée.
- L'absence d'authentification forte généralisée.
- Des accès d'administration reposant principalement sur des identifiants classiques.
- Une segmentation réseau limitée.

Les contrôles de sécurité sont présents mais hétérogènes, ce qui complique :

- La traçabilité.
- La gestion des droits.
- La réduction de la surface d'attaque.

C. Supervision et sauvegardes

L'infrastructure existante ne dispose pas de :

- Supervision centralisée.
- Centralisation des journaux d'événements.
- Visibilité globale sur l'état du système.

Les sauvegardes sont :

- Ponctuelles.
- Non automatisées.
- Sans véritable stratégie formalisée.

En cas d'incident, le temps de diagnostic et de reprise d'activité est élevé.

D. Identification des SPOF (Single Point of Failure)

L'audit met en évidence plusieurs points de défaillance uniques :

- Le nœud Proxmox unique.
- Le stockage local non redondé.

- L’absence de redondance réseau.
- L’absence de mécanisme de bascule automatique.

Ces SPOF représentent un risque majeur pour la continuité de service et constituent un frein à une exploitation fiable en production.

III.4 Synthèse des constats et axes d’amélioration

L’audit de l’infrastructure existante met en évidence un niveau de maturité limité, principalement en matière de disponibilité, de sécurité et d’exploitation.
Les principaux risques identifiés concernent l’indisponibilité des services, la dépendance à des composants uniques (SPOF), le manque de traçabilité des accès et l’absence d’automatisation des opérations critiques.
Ces constats justifient la mise en place d’une nouvelle architecture cible visant à renforcer la résilience globale, à sécuriser les accès, à industrialiser les déploiements et à améliorer la supervision de l’environnement.
Les axes d’amélioration identifiés servent de fondement aux choix techniques et organisationnels présentés dans les chapitres suivants.

Tableau de correspondance – ANSSI (MIS) / ISO 27001 / Mesures mises en place

Objectif : démontrer l’alignement du projet avec les bonnes pratiques (sans viser une certification). Les références ISO sont indiquées à titre de correspondance (Annexe A, catégories de contrôles).

Appliquée | Partiellement appliquée | Programmée | Non applicable / hors périmètre

Contexte : Cloud privé on-premise • Proxmox/Ceph • IaC • Graylog • MFA + mTLS

RÉF. ANSSI (MIS)	ISO 27001:2022	MESURES MISES EN PLACE DANS LE PROJET	ÉLÉMENTS DE PREUVE / LIVRABLES	STATUT
MIS1/MIS2 Gestion des accès	**A.5 / A.6** IAM & contrôle d’accès	Authentification forte pour l’accès au dashboard : **ID/MDP** + **TOTP** + **certificat client (mTLS)**. Séparation des zones réseau (VLAN) pour limiter la surface d’attaque.	Procédure d’accès • schéma MFA • règles d’accès • config reverse-proxy `mTLS` / `TOTP`	Appliquée
MIS1 Segmentation réseau	**A.8** Sécurité des réseaux	Segmentation par VLAN (stockage, automatisation, administration, VPN, production). Filtrage en frontal via cluster pfSense et règles par zone.	Schéma réseau • plan d’adressage IP • règles pfSense (exemples)	Appliquée
MIS2 Journalisation	**A.8 / A.5** Logs & traçabilité	Centralisation des logs via Graylog (pfSense, Proxmox, Linux, dashboard). Mise en place d’alertes sur événements critiques (auth, accès admin, santé cluster).	Architecture supervision • règles d’alerting • runbook incident	Partiellement appliquée
MIS1 Sauvegardes	**A.8** Résilience & sauvegarde	Stratégie de sauvegarde **3-2-1** : copies multiples, supports distincts, copie hors site. Tests de restauration planifiés.	Stratégie 3-2-1 • procédures • résultats de tests (chapitre tests)	Appliquée
MIS2 Durcissement	**A.8** Configuration sécurisée	Durcissement des systèmes (services nécessaires uniquement, règles firewall, accès admin restreints). Standardisation via templates et automatisation Ansible.	Playbooks Ansible • templates VM • checklist hardening	Partiellement appliquée
MIS1 Disponibilité	**A.8** Continuité / disponibilité	Mise en place d’un cluster Proxmox (3 nœuds) avec stockage distribué Ceph. Objectif : tolérance à la panne d’un nœud et redémarrage automatique des VMs (HA).	Schéma d’architecture • analyse SPOF • tests de bascule / HA	Appliquée
MIS2 Réponse à incident	**A.5** Gestion des incidents	Mise en place d’une approche SOC “PME” : collecte, corrélation, alertes, runbook (qualification → confinement → remédiation).	Runbook incident • scénarios d’alertes • procédures d’escalade	Programmée
MIS1 Accès distant	**A.8** Accès réseau	Accès distant sécurisé via VPN WireGuard (pfSense) + filtrage. Le dashboard reste protégé en plus par MFA + mTLS (défense en profondeur).	Config VPN • règles pfSense • schéma sécurité “défense en profondeur”	Appliquée
MIS2 Patch management	**A.8** Gestion des vulnérabilités	Évolution prévue : industrialisation des mises à jour (WSUS pour Windows, Ansible pour Linux), avec suivi et reporting.	Roadmap améliorations • procédures patch management (à formaliser)	Programmée
MIS1/MIS2 Automatisation	**A.8** Maîtrise de l’exploitation	Infrastructure as Code : Terraform (provisioning), Ansible (configuration), Jenkins (orchestration), pilotés via un dashboard sécurisé (Flask/Python).	Pipelines • playbooks • scripts • manuel d’utilisation dashboard	Appliquée

Note : ce tableau illustre l’alignement du projet avec un socle de bonnes pratiques (ANSSI / ISO 27001). Les références ISO sont données à titre indicatif pour faciliter la lecture par le jury et structurer la démarche.

Figure 7 ANSSI (MIS) / ISO27001

A. Recommandations ANSSI (MIS1 / MIS2)

Le projet s’appuie sur les recommandations publiées par l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI), et plus particulièrement sur les Mesures d’Hygiène de Sécurité (MIS1 et MIS2).
Ces recommandations constituent un socle de bonnes pratiques visant à améliorer le niveau de sécurité

des systèmes d'information, notamment en matière de gestion des accès, de journalisation, de segmentation réseau et de sauvegarde des données.
Dans le cadre de ce projet, les principes MIS1 et MIS2 ont servi de référentiel pour identifier les écarts de sécurité de l'infrastructure existante et orienter la conception d'une architecture plus résiliente et sécurisée, adaptée à un environnement de production.

B. ISO/IEC 27001 – Bonnes pratiques

Les bonnes pratiques issues de la norme ISO/IEC 27001 ont été prises en compte afin d'inscrire le projet dans une démarche structurée de gestion des risques liés à la sécurité de l'information.
Sans viser une certification formelle, cette norme a servi de cadre méthodologique pour aborder les notions de gouvernance, de contrôle des accès, de traçabilité, de gestion des incidents et d'amélioration continue.
L'approche adoptée permet de poser les bases d'un système de management de la sécurité de l'information (SMSI) cohérent, proportionné au contexte et à la taille de l'entreprise.

C. RGPD – Principes généraux

Le projet intègre les principes fondamentaux du Règlement Général sur la Protection des Données (RGPD), en particulier en matière de confidentialité, de sécurité et de traçabilité des accès aux données.
Les mécanismes mis en œuvre, tels que le contrôle strict des accès, la journalisation des événements et la sécurisation des communications, contribuent à limiter les risques de compromission et à garantir une meilleure protection des données traitées par le système.
Cette prise en compte du RGPD s'inscrit dans une démarche de conformité pragmatique, visant à renforcer la protection des données sans alourdir excessivement l'exploitation de l'infrastructure.

IV. Analyse du besoin

IV.1 Problématique initiale

A. Constats sur l'infrastructure initiale de NovaTechSolutions

La figure ci-dessus présente l'architecture actuelle de l'infrastructure informatique de NovaTechSolutions. L'accès aux services de l'entreprise s'effectue depuis le réseau WAN, via la box opérateur, puis transite par un firewall unique, ne disposant pas de mécanisme de haute disponibilité. Ce firewall constitue un point critique de l'infrastructure : en cas de panne ou de défaillance, l'ensemble des services devient indisponible.

L'environnement de virtualisation repose sur un unique hyperviseur Proxmox VE fonctionnant sur un seul nœud physique. L'ensemble des applications et machines virtuelles est hébergé sur ce serveur unique, sans possibilité de bascule automatique ni de répartition de charge. Cette architecture crée un point de défaillance unique (*Single Point of Failure*), augmentant significativement les risques d'interruption de service.

Les données applicatives sont stockées sur une base de données non redondante, sans mécanisme de réplication ou de tolérance aux pannes. En cas de défaillance matérielle ou logicielle, la perte de données pourrait être totale. La stratégie de sauvegarde repose uniquement sur une sauvegarde locale sur support USB. Cette méthode, bien que simple à mettre en œuvre, présente plusieurs limites majeures : absence d'automatisation, dépendance à des manipulations manuelles, absence de redondance et impossibilité de restauration rapide en cas de sinistre majeur (incendie, vol, panne matérielle critique).

Enfin, les postes de travail accèdent directement aux machines virtuelles et aux applications hébergées sur l'hyperviseur, sans segmentation réseau avancée ni isolation stricte des flux, ce qui limite les capacités de sécurisation et de contrôle.

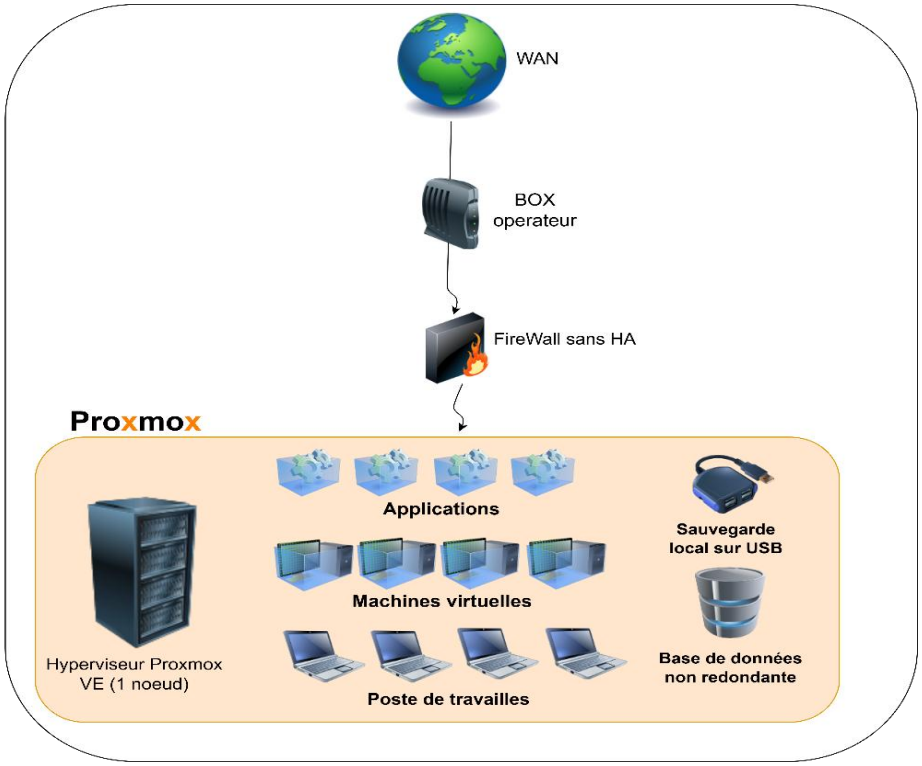


Figure 8 Infrastructure initiale

B. Limites des dysfonctionnements identifiés – Processus AS IS / TO-BE

L'analyse de l'infrastructure existante (AS IS) de NovaTechSolutions met en évidence plusieurs limites structurelles et fonctionnelles qui impactent directement la disponibilité des services, la sécurité des données et l'efficacité opérationnelle des équipes IT.

B1. Limites du processus AS IS (existant)

Le fonctionnement actuel repose sur des processus majoritairement manuels et peu industrialisés.

Les principales limites identifiées sont les suivantes :

Absence de haute disponibilité
L'infrastructure s'appuie sur un unique hyperviseur Proxmox et un firewall sans mécanisme de redondance. Cette architecture introduit plusieurs *Single Points of Failure*. Une panne matérielle ou logicielle entraîne une indisponibilité totale des services hébergés.

Gestion manuelle du cycle de vie des machines virtuelles
La création, la configuration et la maintenance des machines virtuelles nécessitent des interventions manuelles, directement depuis l'interface Proxmox ou en ligne de commande. Cette approche augmente le temps de déploiement et le risque d'erreurs humaines.

Absence d'automatisation et de standardisation
Les machines virtuelles ne reposent pas sur des templates homogènes ni sur une approche Infrastructure as Code. Chaque déploiement est traité comme un cas isolé, rendant difficile la reproductibilité et la traçabilité des actions.

Stratégie de sauvegarde insuffisante
Les sauvegardes sont réalisées localement sur support USB, sans automatisation, sans redondance et sans externalisation. Ce mode opératoire ne répond pas aux exigences de continuité d'activité (PCA/PRA) et expose l'entreprise à un risque élevé de perte de données.

Supervision et visibilité limitées
L'infrastructure ne dispose pas de solution centralisée de supervision ou de journalisation. Il est difficile d'avoir une vision globale de l'état des ressources (CPU, RAM, stockage, services), ce qui limite la capacité d'anticipation et de réaction face aux incidents.

Sécurité perfectible
L'absence de segmentation réseau avancée, de journalisation centralisée et de contrôle fin des accès limite le niveau de sécurité global de l'infrastructure et complique la détection d'événements anormaux.

B2. Objectifs du processus TO-BE (cible)

Face à ces limites, le projet vise à transformer en profondeur le fonctionnement de l'infrastructure en mettant en place un processus TO-BE moderne, automatisé et résilient.

Le processus cible repose sur les principes suivants :

Haute disponibilité et résilience
Mise en place d'un cluster Proxmox multi-nœuds associé à un stockage distribué Ceph, permettant la tolérance à la panne d'un serveur ou d'un disque sans interruption de service.

Automatisation complète du cycle de vie des VMs
Utilisation de Terraform pour le provisioning automatisé des machines virtuelles et d'Ansible pour leur configuration post-déploiement, garantissant rapidité, homogénéité et fiabilité.

Centralisation des opérations
Développement d'un dashboard web unique permettant de piloter l'ensemble des actions : déploiement, supervision, maintenance et consultation des logs, sans intervention directe sur les outils sous-jacents.

Sécurisation renforcée
Implémentation d'un accès sécurisé au dashboard (HTTPS, authentification renforcée, 2FA), segmentation réseau par VLAN, firewall en haute disponibilité et accès distant sécurisé via VPN.

Supervision et traçabilité
Centralisation des journaux et des métriques via des outils de supervision et de logging (Graylog), offrant une visibilité complète et en temps réel sur l'état de l'infrastructure.

B3. Synthèse AS IS / TO-BE

La transition du processus AS IS vers le processus TO-BE permet de passer d'une infrastructure fragile à une plateforme hautement disponible, d'opérations manuelles à une automatisation complète, d'une gestion dispersée à un pilotage centralisé et d'une sécurité minimale à une sécurité maîtrisée et auditable.

Cette évolution constitue le socle du projet de Cloud Privé pour NovaTechSolutions.

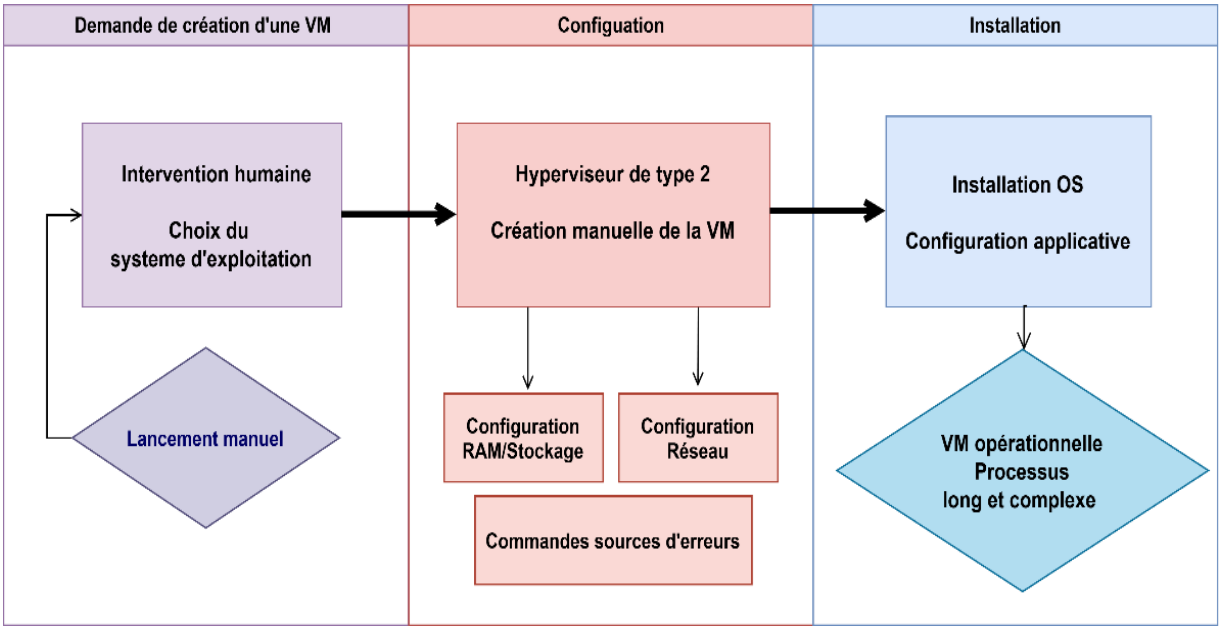


Figure 9 Gestion d'une machine virtuelle (AS IS)

IV.2 Méthodologie d'analyse

A. Le besoin

La mise en place d'une infrastructure Cloud Privé pour NovaTechSolutions répond à plusieurs motivations stratégiques, techniques et organisationnelles. L'entreprise fait face à une croissance soutenue, à des besoins de virtualisation de plus en plus importants et à une dépendance forte aux services Cloud externes, générant des coûts et des risques supplémentaires.

Face à ces enjeux, NovaTechSolutions souhaite disposer d'une infrastructure moderne, automatisée et totalement maîtrisée, capable d'assurer la continuité de service et l'autonomie technologique.
Afin de garantir la cohérence stratégique du projet, il est essentiel d'en comprendre les fondements économiques et organisationnels.
Le diagramme ci-dessous présente une synthèse claire et structurée du Business Plan associé au projet, en mettant en évidence les éléments clés qui orientent les choix techniques et financiers.

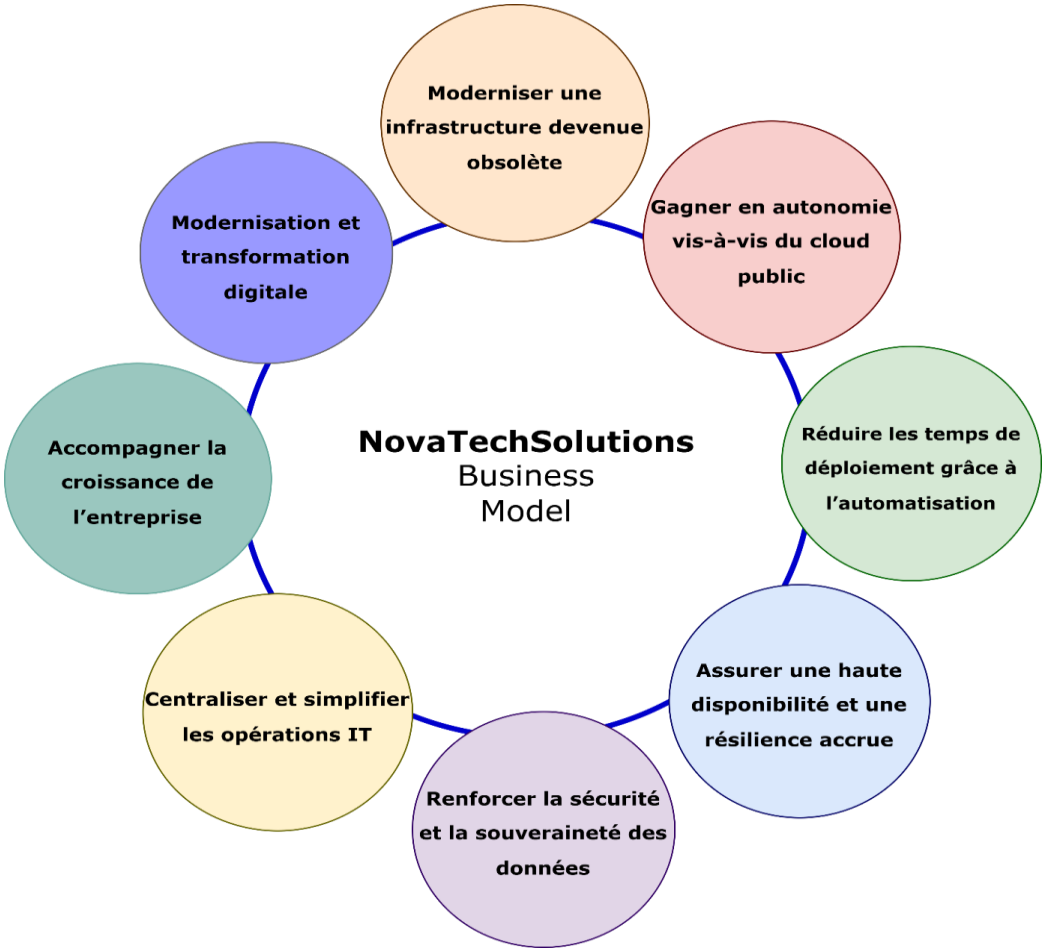


Figure 10 Business Model NovaTechSolutions

Moderniser une infrastructure devenue obsolète

Les serveurs actuels de NovaTechSolutions manquent de performance, de redondance et d'outils de gestion modernes.
Le projet vise donc à mettre fin aux déploiements manuels, réduire les risques de panne et à standardiser les environnements de travails.

Gagner en autonomie vis-à-vis du cloud public

Actuellement, une partie des services repose sur des ressources Cloud externes (AWS).
Or, cette solution externe augmente les coûts mensuels, limitent la flexibilité et exposent à la dépendance fournisseur.
Le Cloud Privé apporte, quant à lui, l'autonomie complète sur le matériel, les données et la sécurité.

Réduire les temps de déploiement grâce à l'automatisation

L'un des objectifs majeurs est de réduire drastiquement le temps nécessaire pour créer une nouvelle VM.
Grâce à Terraform, Ansible et aux Template cloud-init, NovaTechSolutions pourra créer une VM en quelques dizaines de secondes, réduire les erreurs humaines et ainsi disposer d'un pipeline CI/CD géré par Jenkins.

Assurer une haute disponibilité et une résilience accrue

L'infrastructure doit être capable de supporter la panne d'un serveur ou d'un disque de stockage sans interruption de service.

Le cluster Proxmox et la technologie Ceph apporte réplication des données, tolérance aux pannes et continuité d'activité.

Renforcer la sécurité et la souveraineté des données

Le Cloud Privé permet de conserver les données dans l'entreprise, protégées par un Firewall, une segmentation réseau (VLAN), un VPN sécurisé, une stratégie de sauvegarde via Proxmox Backup Server (PBS) et une gestion fine des accès aux ressources.

Avec le Dashboard Cloud développé en Python/Flask, NovaTechSolutions obtient un portail interne unique, un accès Terraform Plan / Apply dynamique, un historique des déploiements et une interface simple pour les administrateurs.
Ainsi, cela professionnalise la gestion interne.

Accompagner la croissance de l'entreprise

NovaTechSolutions prévoit une croissance de son activité et du nombre de clients dans un avenir proche, aussi le Cloud Privé répond à l'augmentation des besoins, à la montée en charge et à la nécessité d'être efficace dans les déploiements.

Ce projet s'inscrit donc dans une démarche visant à fiabiliser l'infrastructure, à préparer l'avenir, à soutenir la stratégie digitale et à réduire les coûts opérationnels à long terme.

B. Problématiques

Comment moderniser l'infrastructure interne afin de disposer d'un cloud privé HA, automatisé et scalable, capable d'héberger les services internes de manière fiable, tout en réduisant la dépendance au cloud public ?
Actuellement, l'infrastructure IT de l'entreprise repose sur des serveurs physiques vieillissants et des machines virtuelles déployées de manière manuelle, sans système de haute disponibilité ni solution de sauvegarde centralisée.

Aussi, NovaTech Solutions fait face à une infrastructure fragile, peu résiliente et difficile à maintenir, qui ne répond plus aux standards modernes d'hébergement et d'infogérance.
L'objectif du projet est donc de moderniser l'infrastructure, de mettre en place une plateforme virtualisée, automatisée et résiliente, permettant de réduire les interruptions, d'améliorer la sécurité et la gestion des données, et de faciliter la montée en charge et le déploiement rapide de nouvelles applications.

IV.3 Analyse fonctionnelle

A. Méthode QQQQCCP

Afin de comprendre précisément le besoin réel de NovaTechSolutions et de définir correctement les contours du projet de Cloud Privé, une analyse préliminaire a été réalisée à l'aide de la méthode QQQQCCP (Qui ? Quoi ? Où ? Quand ? Comment ? Combien ? Pourquoi ?).

Cette méthode structurée permet d'examiner le contexte sous tous ses angles et de clarifier les enjeux, les acteurs impliqués, les contraintes techniques et organisationnelles, ainsi que les motivations profondes qui justifient la mise en place d'une infrastructure privée moderne et automatisée.

Il met en évidence les attentes fonctionnelles de NovaTechSolutions, les problématiques identifiées dans l'infrastructure actuelle, et les résultats attendus en termes de disponibilité, sécurité, scalabilité et automatisation. Cette analyse est essentielle pour cadrer le projet, orienter les choix techniques et garantir que la solution proposée par NebTech réponde pleinement aux objectifs opérationnels et stratégiques du client.

Quoi ?	Mise en place d'un Cloud Privé complet hébergé chez NovaTechSolutions, basé sur un cluster Proxmox, un stockage Ceph, un firewall OPNSense, et un dashboard automatisé permettant le déploiement de VM via Terraform.
Qui ?	NebTech : Conception, déploiement, supervision du projet. NovaTechSolutions : Client final, PME de finance et gestion documentaire.
Où ?	Sur le site informatique de NovaTechSolutions à Lille.
Quand ?	Projet initié en 2024. Mise en place du 26/09/2025 au 31/10/2025.
Comment ?	En construisant une architecture moderne et segmentée : Cluster Proxmox 3 nœuds (VLAN 10) Ceph OSD & HA Templates Windows/Linux (Terraform, Ansible, Jenkins, Docker, K8s, OPNSense Firewall) En automatisant tout le cycle de vie des VM grâce à : Terraform + provider Proxmox Cloud-init Un dashboard Flask pour déploiement en un clic Logging des déploiements
Combien ?	Coût total estimé : ~20k–25k € (hors main d'œuvre client)
Pourquoi ?	Pour résoudre les problèmes actuels de NovaTechSolutions : Déploiement de VM trop lent et manuel Absence d'automatisation / pas d'Infrastructure as Code Manque de standardisation (Templates hétérogènes) Risques de sécurité liés aux interventions manuelles Et apporter : Un cloud privé sur mesure, sécurisé et évolutif Une maîtrise totale des ressources Une réduction des erreurs humaines Une base solide pour le déploiement des Vms

Figure 11 Méthode QQQQCCP

B. Limites de l'infrastructure existante (Diagramme d'Ishikawa)

L'infrastructure actuelle de NovaTechSolutions présente plusieurs limitations qui impactent directement la qualité du service proposé aux clients, aussi un diagramme d'Ishikawa a été établi.

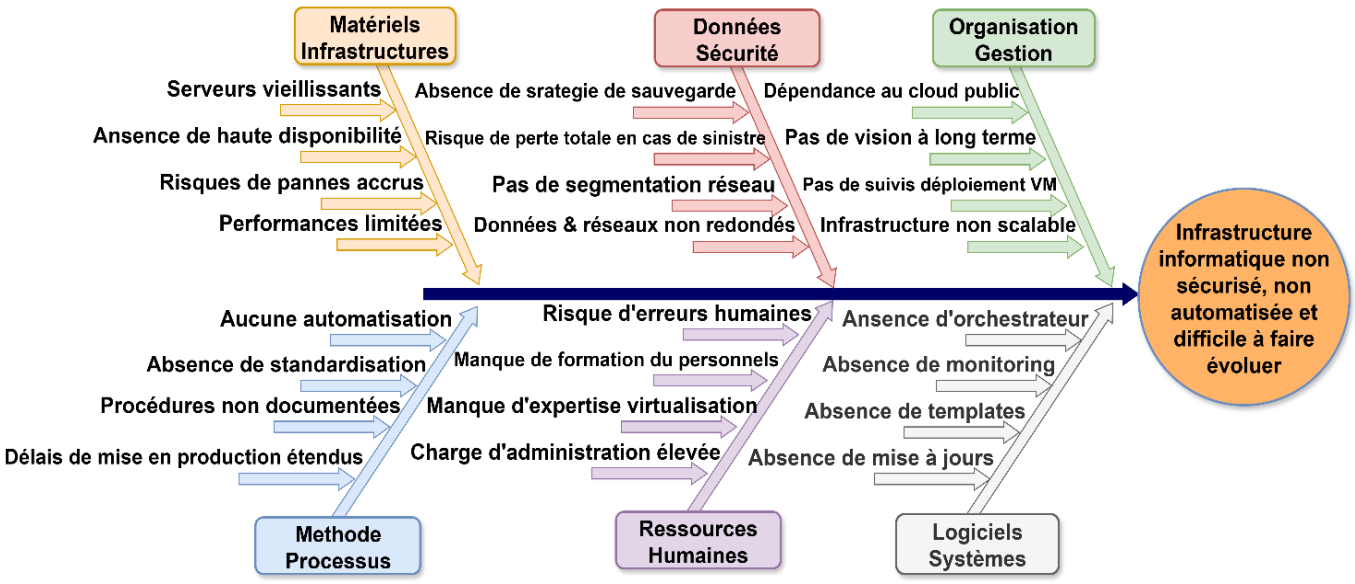


Figure 12 Diagramme d'Ishikawa

Le diagramme présenté ci-dessus permet d'identifier, classifier et visualiser l'ensemble des causes qui conduisent à une infrastructure informatique mal sécurisée, non automatisée et difficile à faire évoluer.

Chaque catégorie regroupe plusieurs problèmes contribuant à la situation actuelle de NovaTech Solutions.

1. **Matériels & Infrastructures**

Dans cette branche, le diagramme met en évidence des problèmes physiques et structurels :
Infrastructures vieillissantes
Absence de haute disponibilité
Risques de pannes accrus
Performances limitées

- ⇨ Ces éléments rappellent que l'infrastructure repose sur du matériel obsolète et non redondé, entraînant des risques de coupures et des limitations techniques.

2. **Données & Sécurité**

Cette branche identifie les risques liés à la protection des données :
Absence de stratégie de sauvegarde
Risque de perte totale en cas de sinistre
Données non redondées
Absence de segmentation réseau

- ⇨ Ces faiblesses exposent l'entreprise à des pertes majeures et compromettent la continuité d'activité.

3. **Organisation & Gestion**

Ici, l'analyse cible les lacunes dans le pilotage stratégique :
Dépendance au cloud public
Absence de vision long terme
Pas de suivi des déploiements et infrastructure non scalable

- ⇨ Ces problèmes montrent un manque de projection dans la croissance future de l'entreprise.

4. **Méthodes & Processus**

Cette catégorie regroupe les problèmes liés aux manières de travailler :
Absence d'automatisation des VMs
Procédures non documentées
Délai de mise en production étendu et absence de standardisation

- ⇨ Ces éléments contribuent à un fonctionnement artisanal, lent et source d'erreurs.

5. **Ressources humaines**

Cette section concerne les compétences et la disponibilité des équipes :
Risques d'erreurs humaines
Manque de formation du personnel
Charge de travail élevée et manque d'expertise virtualisation

- ⇨ Ces éléments entravent la maintenance et l'évolution cohérente du système d'information.

6. **Logiciels & Systèmes**

Cette dernière branche regroupe les lacunes techniques :
Absence d'outils d'orchestration et de Templates normalisées.
Absence de monitoring.
Retards dans les mises à jour logiciels

- ⇨ Ces manquements empêchent l'automatisation, la supervision et la stabilité de l'infrastructure.

C. Diagramme de la bête à cornes

Issu des méthodes de conception centrées sur le besoin, ce diagramme permet de représenter, de manière simple et visuelle, l'intention fondamentale du système, en répondant à trois questions essentielles : À qui le système rend-il service ? Sur quoi agit-il ? Et dans quel but existe-t-il ?

Dans ce projet, ce diagramme a permis d'identifier clairement les attentes de NovaTechSolutions en termes de fiabilité, d'automatisation, de rapidité de déploiement et de sécurisation des services.
Elle constitue donc une étape fondamentale pour aligner la solution technique proposée par NebTech avec les enjeux stratégiques et opérationnels du client.

Dans le cadre de ce projet, la bête à cornes a permis de clarifier et de formaliser l'intention du futur cloud privé.

Elle met en évidence :

- **Le bénéficiaire principal** : NovaTechSolutions, qui s'appuie sur NebTech pour moderniser et automatiser son infrastructure.
- **L'objet d'action du système** : une infrastructure interne vieillissante, difficile à maintenir, non automatisée et dépourvue de mécanismes avancés de supervision.
- **Les moyens d'action** : les technologies d'automatisation telles que Terraform, Ansible, Jenkins, associées à un cluster Proxmox et à un stockage distribué Ceph.
- **Le but final** : mettre en place un cloud privé hautement disponible, scalable, automatisé et capable d'héberger les services internes tout en réduisant la dépendance à des solutions externes.

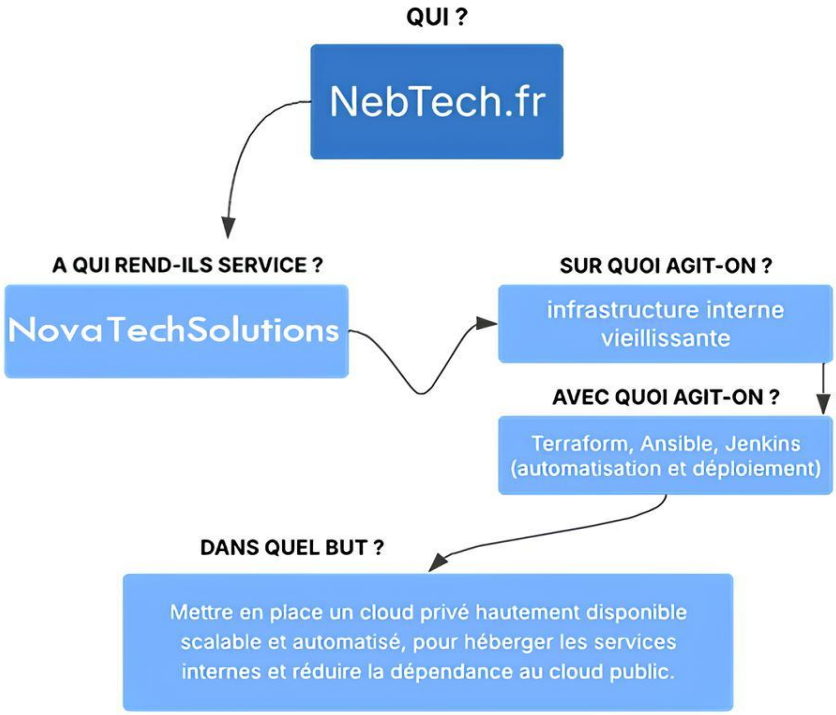


Figure 13 Diagramme Bête à cornes

D. Diagramme pieuvre

Ce diagramme de la pieuvre, issu de l'analyse fonctionnelle, va servir à définir clairement les frontières fonctionnelles du système, les acteurs externes, et le rôle que joue chacun dans le fonctionnement global.

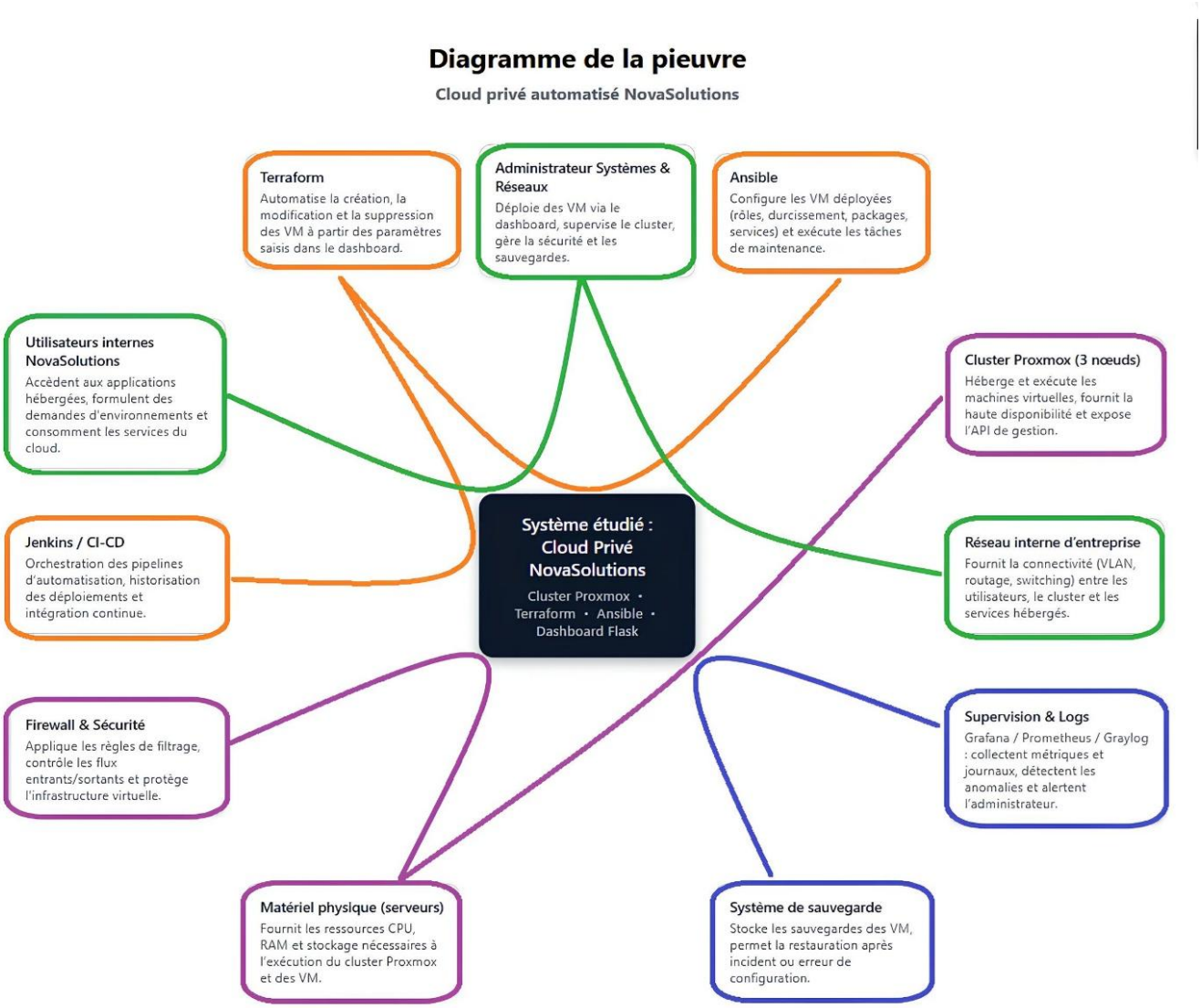


Figure 14 Diagramme de la pieuvre

Au centre, le système étudié représente le *Cloud Privé NovaTechSolutions*, qui regroupe l'ensemble des briques d'automatisation et d'infrastructure nécessaires au déploiement et à la gestion des environnements virtualisés.

E. Acteurs externes

Administrateur Systèmes & Réseaux

Il constitue l'utilisateur principal du système qui interagit directement avec le dashboard pour déployer des machines virtuelles, gérer l'infrastructure et superviser l'ensemble des services. C'est lui qui pilote la plupart des actions via l'automatisation.

Terraform

C'est cette solution qui reçoit les paramètres envoyés depuis le dashboard et qui exécute les actions d'infrastructure nécessaires : création, mise à jour ou suppression des machines virtuelles.
Il constitue le lien direct entre la demande utilisateur et Proxmox.

Ansible

Une fois les VMs déployées, Ansible prend le relais pour la configuration automatique (ajout de rôles, durcissement, installation de dépendances et automatisation des tâches de maintenance).

Cluster Proxmox
Il est composé de trois nœuds, il est l'environnement d'exécution du cloud privé. Il fournit la haute disponibilité, la gestion de ressources (CPU/RAM/stockage) et est l'API utilisée par Terraform pour le déploiement.

F. Acteurs internes

Ils bénéficient du résultat final : les services et applications hébergés sur le cloud. Ils sont des consommateurs directs de l'infrastructure.

Jenkins / CI-CD
Il assure l'automatisation avancée des pipelines, la cohérence des déploiements, la remontée d'état et la centralisation de l'historique d'exécution.

Réseau interne de l'entreprise
Il fournit la connectivité et assure le transport de tous les flux entre les différents acteurs du système : API, supervision, interfaces graphiques, SSH.

Firewall & Sécurité
Cet acteur est indispensable pour garantir l'intégrité et la confidentialité des échanges car il protège l'infrastructure en filtrant les flux et en limitant l'exposition des services essentiels.

Supervision & Logs (Syslog / Graylog / Dashboard Flask/API)
Ils collectent les métriques de performances (CPU, RAM, IO, réseaux), les journaux d'activité, les alertes systèmes et assurent la détection précoce d'événements anormaux et permettent un suivi fin de l'infrastructure.

Matériel physique (Cluster Proxmox)
Cet acteur représente les ressources matérielles supportant Proxmox : CPU, RAM, stockage, réseau. C'est lui qui garantit la disponibilité et les performances du cloud.

Système de sauvegarde
Il assure la protection des données et permet la restauration en cas d'incident. C'est une brique essentielle pour la continuité d'activité (PRA/PCA).

Ce diagramme va servir de base à la rédaction du Cahier des Charges Fonctionnel et à la préparation du diagramme de flux qui en découlera.

G. Objectifs fonctionnels

Les objectifs fonctionnels définissent ce que le Cloud Privé doit savoir faire du point de vue du client, indépendamment des solutions techniques utilisées. Ils décrivent les services rendus par l'infrastructure et les fonctionnalités attendues par les utilisateurs finaux (administrateurs).

Dans le cadre du projet de Cloud Privé pour NovaTechSolutions, les objectifs fonctionnels ont été définis afin de répondre aux problématiques identifiées : besoin d'automatisation, rapidité de déploiement, réduction des erreurs humaines, disponibilité élevée et sécurisation des ressources.
Ces objectifs constituent le fil conducteur du développement du Cloud Privé et garantissent que la solution finale réponde pleinement aux besoins opérationnels et stratégiques de l'entreprise.

Objectifs fonctionnels du Cloud privé NovaTechSolutions

N°	Objectif fonctionnel	Description
OF1	Déployer automatiquement une VM	Permettre le déploiement d'une machine virtuelle complète (nom, ressources, réseau, template) en un clic via le dashboard Terraform / Flask.
OF2	Gérer et standardiser les templates	Fournir des images Linux et Windows prêtes à l'emploi, mises à jour et homogènes, pour limiter la variabilité des configurations.
OF3	Automatiser la configuration des services	Utiliser Ansible pour configurer automatiquement les services (paquets, rôles, sécurité) sur les VM déployées.
OF4	Réduire les erreurs humaines	Mettre en place des contrôles de cohérence (ID VM, datastore, bridge, ressources) et des champs pré-remplis afin de limiter les erreurs de saisie.
OF5	Garantir une haute disponibilité	Assurer la continuité de service grâce au cluster Proxmox et au stockage distribué Ceph, tolérant aux pannes matérielles.
OF6	Superviser l'état du cluster	Fournir une vision centralisée de l'état des nœuds, des VM, du stockage, et des performances globales de l'infrastructure.
OF7	Faciliter la maintenance	Standardiser les déploiements, historiser les actions et s'appuyer sur Proxmox Backup Server pour restaurer rapidement en cas de problème.
OF8	Accélérer la mise en production	Réduire le temps de provisionnement d'une VM prête à l'usage à moins de quelques minutes grâce à Terraform, cloud-init et Ansible.
OF9	Assurer la sécurité du système	Renforcer la sécurité réseau (VLAN, pfSense, VPN), les accès (SSH, droits Proxmox) et les sauvegardes (règle 3–2–1).
OF10	Offrir une interface simple d'utilisation	Proposer un dashboard clair et ergonomique pour les équipes IT, incluant la sélection du template, la saisie des ressources et l'historique des déploiements.

Figure 15 Objectifs fonctionnels

H. Carte Radar (Analyse visuelle)

Pour évaluer l'apport réel du projet et mesurer l'écart entre la situation actuelle de NovaTechSolutions et la solution finale proposée par NebTech, une analyse visuelle sous forme de carte radar a été réalisée.
Ce diagramme permet de comparer plusieurs critères essentiels d'un cloud moderne — automatisation, disponibilité, sécurité, rapidité de déploiement, scalabilité, standardisation et maintenabilité — selon différents niveaux de maturité.

Respectivement, la situation actuelle de l'infrastructure de NovaTechSolutions, un scénario intermédiaire (correspondant à une modernisation partielle) et la situation finale, obtenue après la mise en place du cloud privé NebTech. L'objectif idéal, servant de référence

La carte radar permet ainsi d'identifier immédiatement les axes où les améliorations sont les plus significatives, notamment en matière d'automatisation, de standardisation et de déploiement rapide.
Ce visuel met clairement en évidence la montée en maturité technologique apportée par le projet, ainsi que la cohérence globale des choix techniques retenus.

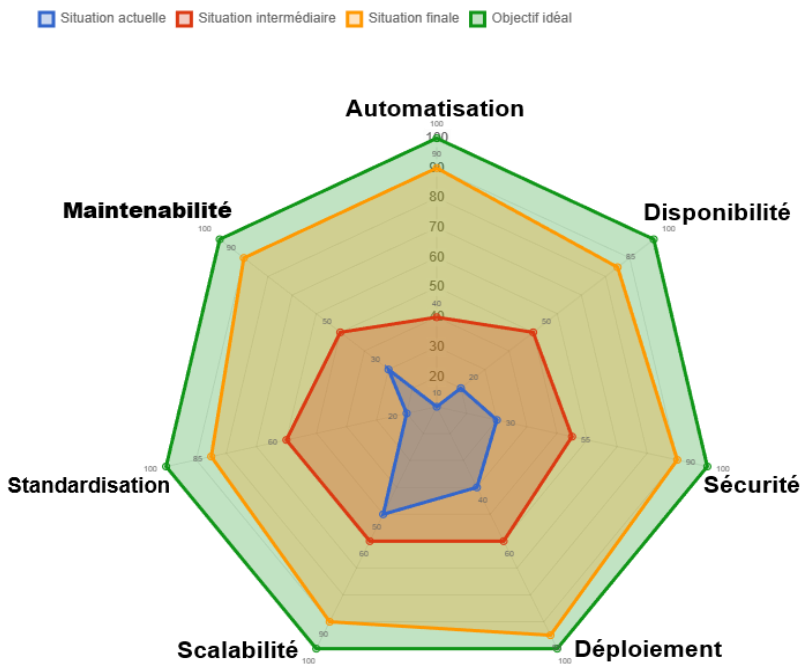


Figure 16 Carte Radar

I. Objectifs opérationnels et stratégiques

Afin de garantir la réussite du projet de cloud privé pour NovaTechSolutions, il est essentiel de définir clairement les objectifs à atteindre.

Ces objectifs se répartissent en deux catégories complémentaires :

Les objectifs opérationnels, qui concernent le fonctionnement quotidien de l'infrastructure, sa performance, sa sécurité et son automatisation.

Les objectifs stratégiques, qui s'inscrivent dans une vision long terme et définissent la manière dont le cloud privé contribuera au développement, à la modernisation et à la compétitivité de l'entreprise.

Le tableau ci-dessous synthétise ces objectifs, afin d'offrir une vision claire des enjeux du projet et d'aligner la solution technique avec les attentes réelles de NovaTechSolutions.

I.1 Objectifs opérationnels

Concrètement, les objectifs opérationnels et stratégiques n'agissent pas au même niveau, mais ils sont étroitement liés et complémentaires.

Les objectifs opérationnels concernent le fonctionnement quotidien du cloud privé, répondent à la question "Comment garantir une infrastructure fiable, performante et sécurisée au jour le jour ?" et portent sur :

- La disponibilité des services.
- La performance du cluster Proxmox et du stockage Ceph.
- L'automatisation des déploiements.
- La sécurité opérationnelle (pare-feu, accès, backups).
- La rapidité de mise en production des VMs.
- La réduction des erreurs humaines via Terraform et Ansible.

Ils ont donc une portée court terme et tangible, car ils influencent directement l'activité quotidienne de NovaTechSolutions.

Figure 17 Diagramme des objectifs techniques

Comparatif des modèles de déploiement Cloud

Synthèse des différences entre cloud privé, cloud public et cloud hybride selon les critères techniques, organisationnels et financiers.

Critère	Cloud privé	Cloud public	Cloud hybride
Principe	Infrastructure dédiée à une seule organisation.	Infrastructure mutualisée partagée entre plusieurs clients.	Combinaison de ressources privées et publiques.
Hébergement	Sur site ou infrastructure dédiée externe.	Chez un fournisseur cloud tiers.	Privé et public selon les usages.
Mutualisation	Aucune mutualisation.	Ressources partagées.	Partielle.
Contrôle & personnalisation	Très élevé.	Limité.	Élevé côté privé, flexible côté public.
Sécurité & souveraineté	Maîtrise complète des données.	Dépend du fournisseur.	Données sensibles isolées en privé.
Conformité	Adapté aux environnements réglementés.	Sous conditions contractuelles.	Conformité facilitée.
Coûts	Investissement initial maîtrisé.	Facturation à l'usage.	Mix CAPEX / OPEX.
Évolutivité	Limitée par l'infrastructure.	Très élevée.	Optimisée.
Cas d'usage	SI critique, données sensibles.	Scalabilité, services managés.	SI mixte et évolutif.
Choix du projet : le cloud privé a été retenu pour garantir la souveraineté des données, un haut niveau de contrôle et une maîtrise des coûts à long terme.			

Figure 18 Comparatif Clouds

Types de clouds privés

Les clouds privés se déclinent en plusieurs modèles selon leur mode d'hébergement et de gestion.

Type de cloud privé	Description	Caractéristiques principales
Cloud privé sur site	Hébergé et administré directement par l'organisation dans son propre centre de données.	• Contrôle maximal • Sécurité et confidentialité élevées • Capacité limitée à l'infrastructure disponible
Cloud privé virtuel (VPC)	Environnement privé et isolé reposant sur une infrastructure de cloud public partagée.	• Isolation réseau dédiée • Flexibilité du cloud public • Mutualisation physique sous-jacente
Cloud privé hébergé	Ressources physiques dédiées hébergées chez un fournisseur tiers.	• Infrastructure non mutualisée • Scalabilité accrue • Gestion partiellement déléguée
Cloud privé géré	Environnement à locataire unique dont l'exploitation est entièrement confiée à un prestataire.	• Gestion complète externalisée • Maintenance et sécurité incluses • Réduction de la charge opérationnelle

Figure 19 Types de Clouds privés

I.2 Objectifs stratégiques

Ce projet de Cloud privé concerne la capacité du système à évoluer avec l'entreprise (scalabilité), la pérennité des données et des services, la maîtrise des coûts informatiques, la réduction de la dépendance au cloud public, l'amélioration de l'image de marque grâce à une infrastructure fiable ainsi que la montée en compétences du personnel. Ces objectifs ont une portée macro, car ils influencent la stratégie IT sur plusieurs années.

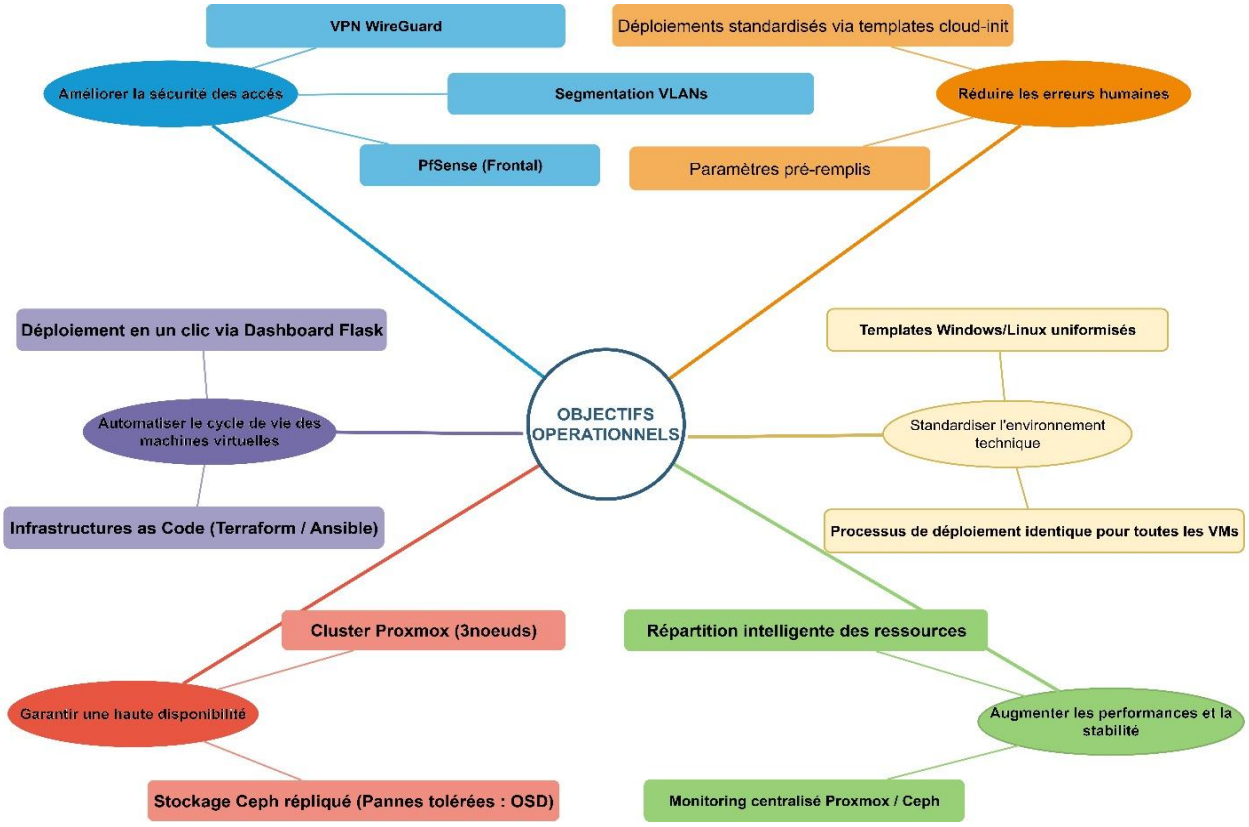


Figure 20 Objectifs opérationnels

Figure 21 Objectifs stratégiques

V. Gestion du projet

V.1 Objectif du projet

L'objectif principal du projet est de concevoir, déployer et automatiser un cloud privé complet pour NovaTechSolutions, afin de remplacer une infrastructure vieillissante, non résiliente et entièrement manuelle.

Ce cloud privé devra permettre :

- La création automatique de machines virtuelles via un dashboard simplifié (Flask + Terraform).
- Une infrastructure hautement disponible, basée sur un cluster Proxmox à 3 nœuds, avec stockage distribué Ceph.
- Une réduction drastique des erreurs humaines grâce à l'usage de l'Infrastructure as Code (IaC).
- Un environnement évolutif, capable d'accompagner la croissance de NovaTechSolutions.
- Une meilleure sécurité, via une segmentation réseau et un firewall OPNSense renforcé.
- La standardisation des déploiements grâce à des Template Windows/Linux préconfigurés.
- Une supervision simplifiée, permettant de monitorer l'état des services et du cluster.

En résumé, le projet vise à transformer une infrastructure traditionnelle en un cloud privé moderne, automatisé, sécurisé et souverain.

V.2 Périmètre et hors périmètre

Ce tableau permet d'établir un cadre précis, d'éviter les ambiguïtés, et de garantir une compréhension commune entre le porteur du projet, l'entreprise et les parties prenantes.

Catégorie	Élément	Description	Périmètre
Infrastructure matérielle			
Serveurs	Cluster Proxmox VE (3 nœuds)	Mise en place et configuration du cluster de virtualisation principal.	IN
Stockage	Cluster Ceph (MON/MGR/OSD)	Stockage distribué pour haute disponibilité des disques.	IN
Sauvegarde	Proxmox Backup Server (PBS)	Mise en place des sauvegardes de VM et application de la règle 3-2-1.	IN
Supervision infrastructure	Proxmox Datacenter Manager	Vue centralisée sur l'état du cluster Proxmox et des ressources.	IN
Baie & énergie	Baie 24U, PDU, onduleur, câblage	Organisation physique du matériel, distribution électrique et câblage réseau.	IN
Architecture réseau			
Firewall	pfSense (principal + secondaire)	Filtrage, routage, NAT et sécurisation des accès WAN/LAN.	IN
VLANs	VLAN 10 / 20 / 30 / 40 / 50	Segmentation réseau (cluster, stockage, templates, outils, VPN).	IN
VPN	WireGuard sur pfSense	Accès sécurisé au cloud privé à distance (admin / support).	IN
Architecture logicielle & automatisation			
Infrastructure as Code	Terraform + Provider Proxmox	Automatisation du déploiement des VMs à partir de templates.	IN
Configuration	Ansible	Configuration automatique des services et rôles sur les VMs.	IN
Orchestration	Jenkins (CI/CD)	Pipeline pour enchaîner Terraform, Ansible et déploiement applicatif.	IN
Dashboard	Dashboard Flask + Terraform	Interface web pour déployer des VMs à partir de templates en un clic.	IN
Templates	Templates Windows & Linux cloud-init	Standardisation des VMs avec pré-installation de services (DB, Docker, etc.).	IN
Hors périmètre (non inclus)			
Postes utilisateurs	PC / laptops NovaTech	Configuration et gestion des postes clients ne sont pas incluses.	OUT
Applications métier	ERP / CRM / Logiciels clients	Le projet fournit l'infrastructure, pas le paramétrage des applis métier.	OUT
Multi-site	Autres sites que Lille	Le projet est limité au datacenter/site principal de Lille.	OUT
Support 24/7	Exploitation continue	Seules les procédures et la documentation sont fournies, pas le support.	OUT

Figure 22 Tableau Périmètre - Hors Périmètre

A. Le projet couvre

Infrastructure matérielle

Mise en place d'un cluster Proxmox VE 9.1 à 3 nœuds.
Déploiement d'un stockage distribué Ceph (MON / MGR / OSD).
Installation d'un Proxmox Backup Server (PBS).
Installation du Proxmox Datacenter Manager (PDM) pour superviser le cluster.
Intégration d'une baie de brassage, d'un onduleur (UPS) et d'une PDU.

Architecture réseau

Mise en place d'un OPNSense principal + un OPNSense secondaire (redondance).

Création des VLANs :

VLAN10 : Management & Cluster Proxmox
VLAN20 : Réseau CEPH (OSD, MON, MGR)
VLAN30 : Automatisation & Services Internes
VLAN40 : VPN Wireguard et administration distante
VLAN50 : Production

Infrastructure logicielle

Mise en place d'un dashboard Flask pour le déploiement automatisé.
Génération automatique des fichiers dashboard.auto.tfvars.
Mise en place du pipeline Terraform → Ansible → Jenkins.
Création de templates cloud-init Windows et Linux.
Déploiement des serveurs internes :
Terraform, Ansible Jenkins et Docker / Flask

Automatisation & IaC

Déploiement entièrement automatisé des VMs.
Logging des déploiements dans le dashboard.
Configuration automatique (cloud-init / Ansible).
Pipeline CI/CD infrastructure.

Documentation & sécurité

Rédaction des procédures.
Diagrammes d'architecture.
Gestion des sauvegardes via PBS (règle 3-2-1).

B. Le projet ne couvre pas

La gestion du domaine Active Directory et des postes utilisateurs initiaux (production).

Organisation des tâches

La gestion des tâches a été structurée de manière rigoureuse afin de garantir une exécution fluide et contrôlée.

Chaque tâche a été définie avec une durée estimée, une date de début et de fin, un responsable, des dépendances avec les tâches précédentes et des livrables clairement identifiés.

Cette granularité permet de s'assurer que le projet avance de manière séquentielle, en validant chaque étape avant d'entamer la suivante.

Afin d'améliorer le pilotage du projet, chaque lot a également été traité comme un mini-cycle de travail, fonctionnant comme un "sprint technique" interne. Grâce à cette approche, la gestion du projet est restée fluide, tout en conservant la rigueur et la prévisibilité du modèle séquentiel.

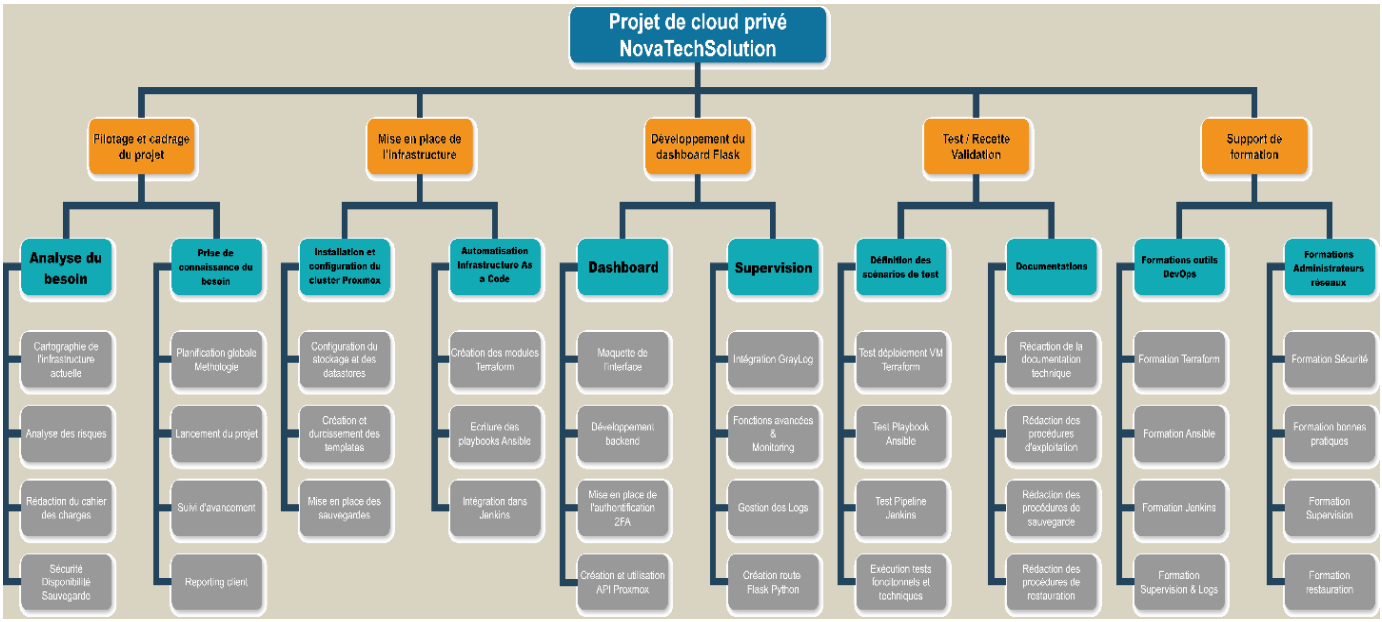


Figure 23 Structure WBS

V.3 Méthodologie retenue : approche en cascade

Pour la conduite de ce projet, j'ai retenu la méthode en cascade, un modèle séquentiel simple, structuré et particulièrement adapté aux projets dont les besoins sont clairement définis, stables et orientés qualité.
Son fonctionnement repose sur une progression par phases successives, chacune produisant un livrable validé avant de passer à l'étape suivante.

Ce modèle présente plusieurs avantages pour un projet d'infrastructure comme celui-ci :

- Une vision claire et anticipée de l'ensemble des étapes.
- Des responsabilités bien identifiées pour chaque phase.
- Un déroulement rigoureux permettant d'assurer la qualité technique avant d'avancer.

De plus, la validation entre chaque phase garantit que les prérequis sont satisfaits et en cas de problème majeur, un retour à l'étape précédente est possible.

Chaque phase est découpée en sous-tâches clairement identifiées et associées à une durée estimée, à une date de début (Start), à une date de fin prévisionnelle (ETA) et à un responsable NebTech.

Ce planning met en évidence la logique séquentielle du modèle en cascade, les dépendances entre les étapes et de garantir à NovaTechSolutions une vision précise de l'avancement et des livrables attendus.

A. Diagramme RACI

Le diagramme RACI présenté ci-dessous a pour objectif de clarifier qui fait quoi, d'assurer une communication fluide entre les équipes, d'éviter les zones d'ombre, les doublons ou les responsabilités non assumées et de garantir une exécution cohérente et maîtrisée du projet.
Ainsi, il permet d'assurer que chaque compétence est sollicitée au bon moment, et que chaque livrable dispose d'un responsable clairement identifié.

TÂCHES	TECHNICIENS			DÉVELOPPEURS		TÉLÉCOM		ADMINISTRATEURS	
NebTech ® pour NovaTechSolutions® ***Mise en place d'un Cloud Privé Hautement disponible*** Responsable du projet : RECULE Damien	RECULE Damien	Irène DUPUIS	Karim BENLO	RECULE Damien	Aurélia DELAIGLE	RECULE Damien	Maryse LEBEUS	RECULE Damien	Olivier DUBOUCHON
Début du projet									
Analyse des besoins	R	A	A	R	A	R	A	R	A
Validation par le client	R	A	A	R	A	R	A	R	A
Réalisation du projet									
Installation des 3 nœuds Proxmox	R	A	A	A	A	A	A	A	A
Mise en place du réseau & VLAN	R	A	A	A	A	R	A	A	A
Installation CEPH & OSD	R	A	A	A	A	A	A	A	A
Développement du Dashboard Flask	R	I	I	R	A	I	I	I	I
Fin du projet									
Validation par le client	A	I	I	A	I	A	I	A	I
Automatisation & Intégration									
Installation VM Terraform	R	A	A	A	A	I	I	A	A
Installation VM Ansible	R	A	A	A	A	I	I	A	A
Installation VM Jenkins	R	A	A	A	A	I	I	A	A
Intégration Terraform ↔ Proxmox API	R	A	A	R	A	I	I	A	A
Phase de tests									
Tests Déploiement VM automatisés	R	R	R	R	R	R	R	R	R
Tests de rollback (snapshot)	R	A	A	A	A	I	I	A	A
Tests HA (Ceph)	R	A	A	A	A	A	A	A	A
Tests de sécurité (pfSense)	R	A	A	I	I	R	A	A	A
Tests de conformité	C	A	A	C	C	C	C	R	R

Figure 24 Diagramme RACI

Légende RACI		
R	Responsable	Réalise la tâche et en porte la responsabilité principale
A	Acteur	Participe activement à la réalisation de la tâche
C	Consulté	Apporte son expertise ou un avis avant ou pendant l'action
I	Informé	Est tenu informé de l'avancement ou du résultat

V.4 Analyse des risques

Une analyse détaillée des risques a été réalisée afin d'anticiper les menaces pouvant impacter la réussite technique, opérationnelle et stratégique du déploiement.
Cette étude permet d'identifier les événements susceptibles d'altérer la disponibilité, la sécurité ou la performance de l'infrastructure, ainsi que les risques liés à la gouvernance, aux ressources humaines et au budget.

Cette approche permet de prioriser les actions préventives et correctives, d'assurer une meilleure maîtrise des aléas, et de garantir une mise en production fiable et pérenne de l'infrastructure cloud.
Le tableau ci-dessous présente la synthèse des risques, accompagnée de leur niveau de criticité (vert, jaune, orange, rouge) et des mesures proposées pour réduire leur occurrence ou leurs effets.

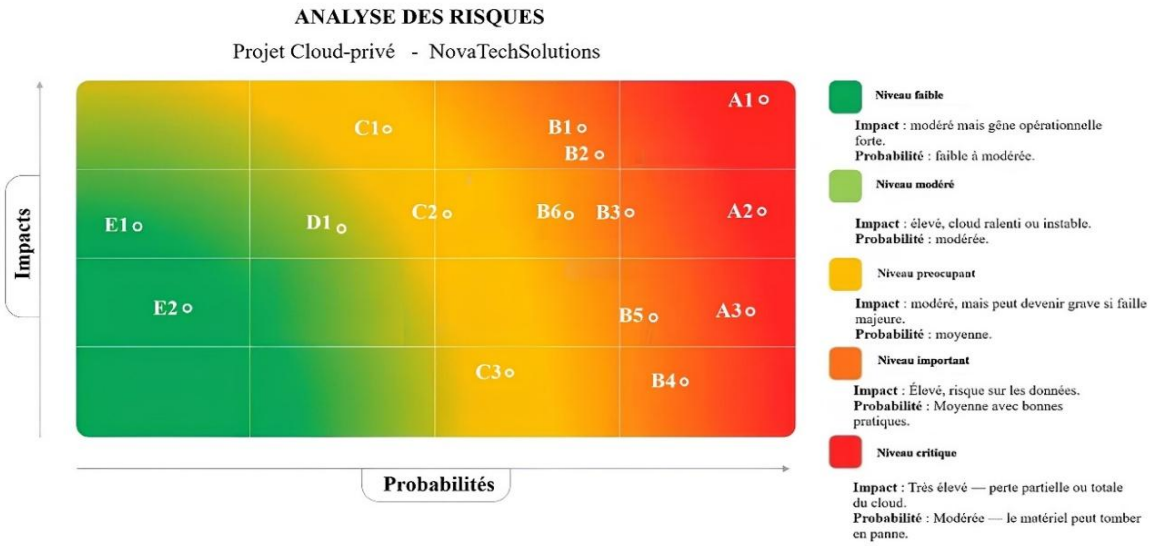


Figure 25 Carte des risques

PROBABILITÉ ▪ 1 – 5	IMPACT ▪ 1 – 16
1 - RARE	2 - INSIGNIFIANT
2 - PEU PROBABLE	2 - MINEUR
3 - POSSIBLE	4 - MODÉRÉ
4 - PROBABLE	8 - MAJEUR
5 - PRESQUE CERTAIN	16 - GRAVE

SCORES PI ▪ 1 – 80		NOMBRE
1 - 2	NEGLIGEABLE	2
3 – 8	MINEUR	1
3 – 4	MODÉRÉ	3
4 – 16	ÉLEVÉE	6
5 – 16	CRITIQUE	3

RISQUE TOTAL
15

Figure 26 Tableau - Carte des risques

Afin d'évaluer leur criticité, chaque risque a été classé selon deux critères, la probabilité d'occurrence ainsi que l'impact potentiel sur le projet et sur l'entreprise.

A. Tableau d'évaluation des risques

A. Risques opérationnels

ID	Risque	Criticité	Impact	Probabilité
OP1	Panne d'infrastructure (Proxmox, Ceph, pfSense)	Critique	Très élevé	Modérée
OP2	Erreur humaine (Dashboard / Terraform / Firewall)	Élevé	Élevé	Élevée
OP3	Risques cybersécurité (SSH, attaques, ransomware)	Élevé	Élevé	Moyenne
OP4	Mauvaise gestion des templates (obsolètes / non patchés)	Modéré	Modéré	Moyenne
OP5	Performances insuffisantes (CPU / I/O / Ceph saturé)	Élevé	Élevé	Modérée
OP6	Dépendance technologique (Terraform / Provider / Ceph)	Modéré	Modéré	Faible à modérée
OP7	Lenteur réseau pendant les sauvegardes	Faible	Faible	Faible
OP8	Perte temporaire d'accès au dashboard Terraform	Faible	Faible	Faible

B. Risques stratégiques

ID	Risque	Criticité	Impact	Probabilité
ST1	Mauvaise anticipation des besoins futurs (scalabilité)	Élevé	Élevé	Modérée
ST2	Absence de compétences internes	Modéré	Modéré	Élevée
ST3	Risque budgétaire (surcoûts, mauvaise estimation)	Élevé	Élevé	Modérée
ST4	Dépendance à un prestataire (NebTech)	Critique	Très élevé	Modérée
ST5	Mauvaise gouvernance (documentation, sauvegarde, monitoring)	Élevé	Élevé	Élevée
ST6	Impact sur l'image de marque (panne majeure)	Critique	Très élevé	Faible à modérée

Figure 27 Tableau - Evaluation des risques

Les risques ont été classés selon leur nature, leur impact potentiel et leur probabilité d'occurrence, permettant ainsi de prioriser les actions de prévention et de mitigation.

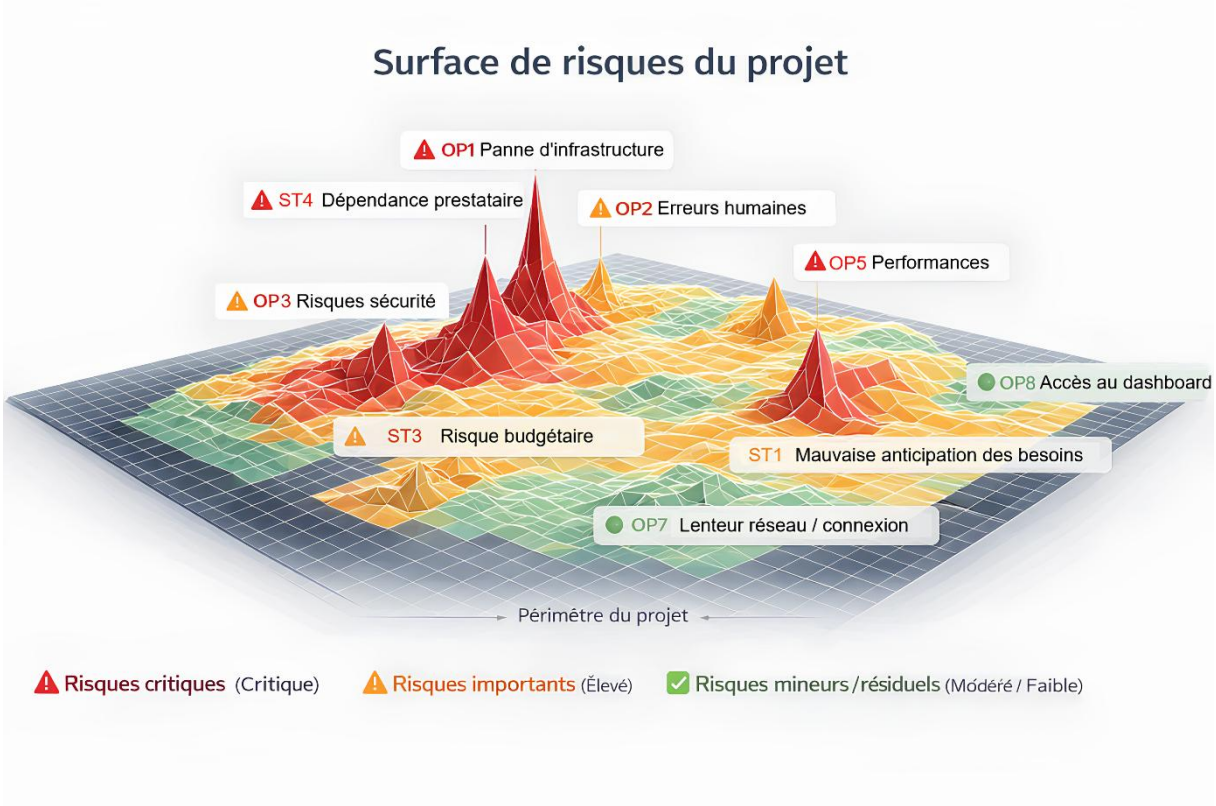


Figure 28 Surface de risques du projet

B. Risques opérationnels

Les risques opérationnels concernent directement l'exploitation technique de l'infrastructure et des outils mis en œuvre.

Le principal risque identifié est une panne d'infrastructure Proxmox, Ceph ou OPNSense, pouvant entraîner une indisponibilité des services. Ce risque est considéré comme critique en raison de son impact élevé, bien que sa probabilité soit modérée grâce à la mise en place d'une architecture redondante.

Des risques liés à la sécurité sont également pris en compte, notamment les erreurs de configuration réseau ou firewall. Ces risques sont atténués par la segmentation réseau, l'utilisation du chiffrement HTTPS et l'application de bonnes pratiques de sécurité.

L'automatisation, bien que source de gains importants, introduit des risques spécifiques, tels qu'une mauvaise gestion des templates ou une dépendance aux outils comme Terraform et Ceph. Ces risques restent modérés et sont maîtrisés par la standardisation des configurations et la documentation.

Enfin, des risques mineurs, comme une lenteur temporaire du dashboard ou une indisponibilité passagère de l'interface d'administration, ont été identifiés. Leur impact est faible car ils n'affectent pas directement la disponibilité de l'infrastructure, celle-ci restant administrable par les outils natifs.

C. Risques stratégiques

Les risques stratégiques concernent l'évolution du projet dans le temps et son adéquation avec les besoins de l'entreprise.

Parmi ceux-ci, une mauvaise anticipation des besoins futurs ou une absence de compétences internes peut limiter la capacité de l'entreprise à faire évoluer l'infrastructure. Ces risques sont pris en compte par la mise en place d'une architecture évolutive et par le transfert de compétences via la documentation et la formation.

La dépendance à un prestataire ou à des outils spécifiques constitue également un risque stratégique. Ce risque est toutefois atténué par le choix de solutions open source largement adoptées, réduisant l'effet de verrouillage technologique.

Enfin, des risques financiers et d'image, tels qu'un dépassement de budget ou un impact sur la réputation en cas d'incident majeur, ont été identifiés comme critiques. Ils justifient la mise en place d'une gouvernance projet rigoureuse et d'une stratégie de supervision proactive.

D. Spécifications techniques

Pour répondre à ces exigences, j'ai combiné plusieurs technologies complémentaires : Proxmox VE pour la virtualisation, Terraform pour le provisioning automatisé, Ansible pour la configuration, et Jenkins pour l'orchestration et le suivi des pipelines.

Afin de rendre l'utilisation de ces outils fluide et unifiée, j'ai développé un dashboard web sur mesure en Python/Flask, qui offre une interface unique permettant de piloter l'ensemble des opérations.

Les spécificités techniques présentées dans la suite du rapport détaillent la manière dont ces différentes briques interagissent, les choix architecturaux effectués, ainsi que les mécanismes d'automatisation mis en place pour garantir un cloud privé fiable, personnalisable et hautement accessible.

Exigences techniques

Cluster Proxmox VE 9.1 sur 3 nœuds (bare-métal)
Ceph cluster (MON/MGR/OSD)
Templates cloud-init pour VM
Terraform ≥1.5, Ansible ≥2.12, Jenkins LTS
Docker CE pour les applications conteneurisées

Fonctionnalités attendues

Création automatique de VMs via Terraform
Déploiement et configuration des services via Ansible
Pipeline Jenkins pour orchestrer Terraform → Ansible → Déploiement Docker
Templates stockés sur pool Ceph RBD partagé
Stockage Ceph répliqué pour HA

Indicateurs de succès

Tolérance à la panne d'un nœud Proxmox
Tolérance à la panne d'un OSD Ceph
Provisioning d'une VM en < 2 min & Groupe de VMs en < 5 min (pour 4 VMs).
Pipeline CI/CD opérationnel pour la création d'environnements de tests.

Création d'un dashboard

Création du squelette Flask sur Python
Appels API vers Proxmox, Terraform, Ansible et Jenkins
Routes pour l'interface utilisateur
Gestion des retours (logs, statuts, résultats d'exécution)
Sécurisation des accès (MFA, TOTP, Mtls).

V.5 Planification du projet

A. Diagramme de Gantt

Afin d'organiser efficacement les différentes phases du projet, un diagramme de Gantt a été élaboré. Cet outil permet de visualiser l'enchaînement des tâches, leurs durées respectives, les dépendances entre elles ainsi que les jalons clés. Chaque phase du projet (analyse, conception, installation, développement, tests, validation, documentation) est clairement positionnée dans le calendrier, ce qui garantit une exécution fluide et structurée.

Ce diagramme constitue ainsi un outil de pilotage indispensable, facilitant la communication avec les parties prenantes et permettant d'assurer un suivi rigoureux jusqu'à la livraison finale.

	Nom de la tâche	Durée	Détails	
1	**Analyse et préparation**	**8 jours**	**26.09.2025**	**03.10.2025**
1.1	Analyse des besoins de NovaTechSolutions	2 jours	26.09.2025	27.09.2025
1.2	Etude des risques	3 jours	28.09.2025	30.09.2025
1.3	Définition des exigences fonctionnelles	2 jours	01.10.2025	02.10.2025
1.4	Plan d'adressage	1 jour	03.10.2025	03.10.2025
2	**Mise en place de l'infrastructure**	**7 jours**	**04.10.2025**	**10.10.2025**
2.1	Installation des 3 noeuds Proxmox	3 jours	04.10.2025	06.10.2025
2.2	Mise en place du reseau Vlan (10,20,30,40)	1 jour	07.10.2025	07.10.2025
2.3	Installation Ceph (OSD01/OSD02/OSD03)	1 jour	08.10.2025	08.10.2025
2.4	Installation Proxmox Backup Server	1 jour	09.10.2025	09.10.2025
2.5	Installation Proxmox Data Center manager	1 jour	10.10.2025	10.10.2025
3	**Automatisation**	**7 jours**	**11.10.2025**	**17.10.2025**
3.1	Installation & configuration Terraform	4 jours	11.10.2025	14.10.2025
3.2	Installation & configuration Ansible	2 jours	13.10.2025	14.10.2025
3.3	Installation & configuration jenkins	2 jours	13.10.2025	14.10.2025
3.4	Création des templates Linux/Windows	1 jour	15.10.2025	15.10.2025
3.5	Développement du Dashboard Flask (Python)	1 jour	16.10.2025	16.10.2025
3.6	Intégration Terraform <--> Proxmox API	1 jour	17.10.2025	17.10.2025
3.7	Intégration Jenkins (CI-CD infra)	1 jour	17.10.2025	17.10.2025
4	**Tests**	**7 jours**	**18.10.2025**	**24.10.2025**
4.1	Test déploiement VM automatisées & VM groupes	3 jours	18.10.2025	20.10.2025
4.2	Test de restauration backup	1 jour	21.10.2025	21.10.2025
4.3	Test HA (FailOver Ceph / PfSense)	2 jours	22.10.2025	23.10.2025
4.4	Test sécurité - 2FA & HTTPS	2 jours	23.10.2025	24.10.2025
5	**Documentation**	**7 jours**	**25.10.2025**	**31.10.2025**
5.1	Documentation technique	2 jours	25.10.2025	27.10.2025
5.2	Documenttaion formation utilisateur	1 jour	27.10.2025	27.10.2025
5.3	Formation du personnels	2 jours	27.10.2025	28.10.2025
5.4	Mise en production	3 jours	29.10.2025	31.10.2025
		36 jours		

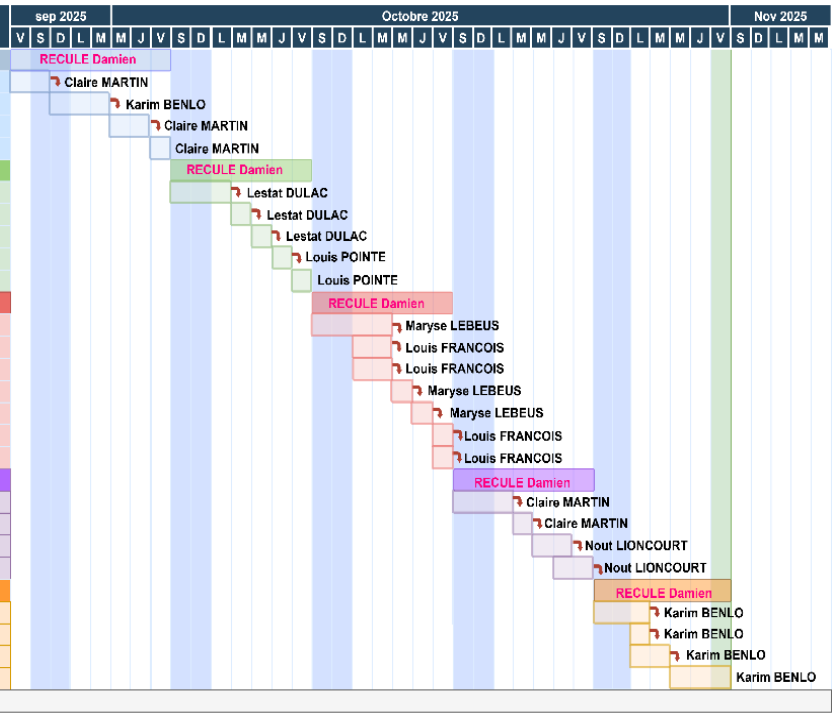


Figure 29 Diagramme de GANTT

VI. Cahier des charges

Le présent Cahier des charges a pour objectif de définir précisément les contraintes, exigences et critères de réussite nécessaires à la mise en place d'un Cloud Privé haute disponibilité pour la société NovaTechSolutions**.**

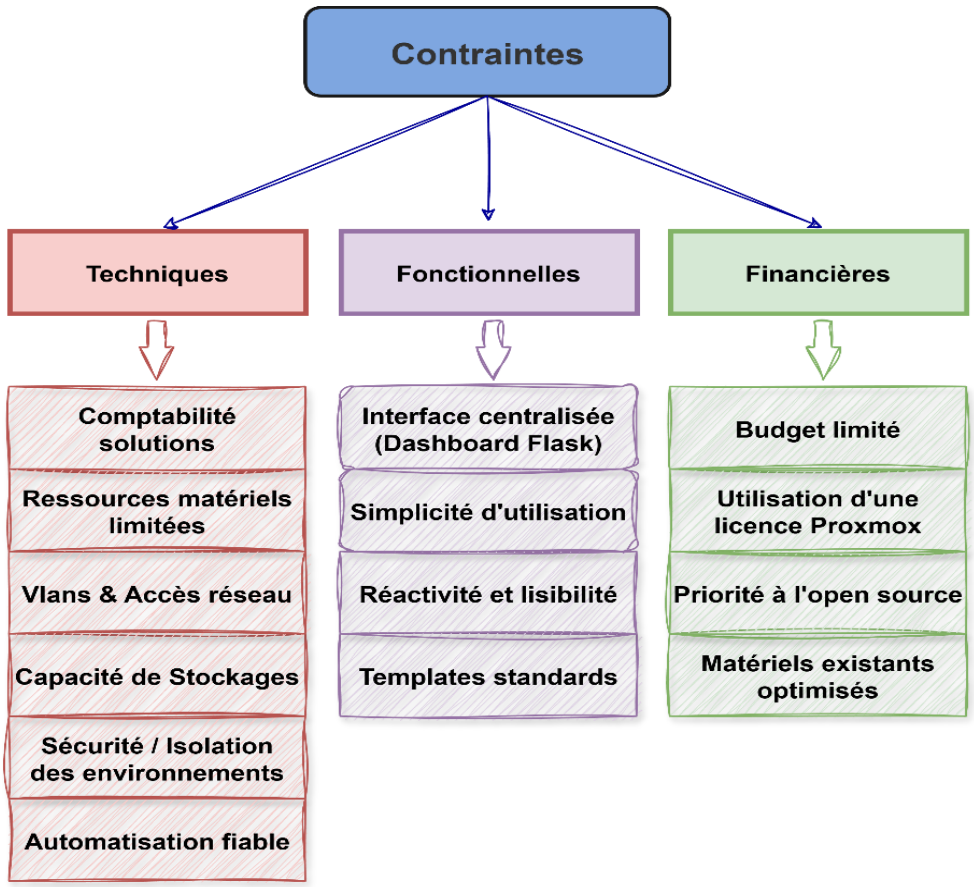


Figure 30 Diagramme des contraintes

VI.1 Cahier Des Charges Fonctionnel (CDCF)

Les besoins fonctionnels dérivent directement de l'analyse fonctionnelle (Bête à Cornes, Pieuvre, QQQQCCP) et doivent répondre aux problématiques initialement identifiées.

A. Besoins fonctionnels

Automatisation & Déploiement

- Permettre le déploiement automatisé d'une machine virtuelle à partir d'un Template choisi par l'utilisateur.
- Autoriser le déploiement d'environnements complets (groupes de VMs prédéfinis) en une seule action.
- Générer automatiquement les configurations nécessaires (VM ID, ressources, datastore, réseau) sans intervention avancée de l'utilisateur.

- Assurer la standardisation des machines déployées, grâce à des Template homogènes validés par l'entreprise.

Supervision & Visualisation

- Fournir une interface de supervision du cluster Proxmox, incluant :
- Charge CPU, RAM, stockage
- Disponibilité des nœuds
- Nombre de Vms actives
- Afficher en temps réel les logs systèmes provenant des nœuds du cluster Proxmox et des postes utilisateurs.
- Lister l'ensemble des machines virtuelles et leurs informations essentielles (ID, nom, état, nœud d'hébergement).

Actions sur les Vms

- Permettre les actions simples d'administration directement depuis le Dashboard :
- Démarrage / Redémarrage
- Arrêt
- Reset
- Migration
- Suppression sécurisée d'une VM

Maintenance & Automatisation complémentaire

- Mettre à disposition un module d'exécution de scripts Ansible (tests de connectivité, mises à jour, routines de maintenance).
- Centraliser l'accès aux outils d'administration externes.

B. Contraintes fonctionnelles

Les contraintes fonctionnelles définissent les limites, règles et obligations à respecter pour que la solution soit utilisable, intuitive et conforme au besoin initial.

Ergonomie & Accessibilité

- L'interface doit être simple et intuitive, utilisable par un technicien systèmes et réseaux sans compétences avancées en Proxmox ou Terraform.
- Le Dashboard doit être consultable via un navigateur web standard, notamment :

  Google Chrome

  Mozilla Firefox

  Microsoft Edge

Sécurité & Contrôle

- Un système d'authentification renforcé doit être mis en place, incluant un accès sécurisé par mot de passe et un second facteur (MFA - TOTP - mTLS)
- Les logs du système doivent être accessibles, mais ne doivent pas permettre de modifier la configuration sous-jacente.
- La suppression d'une VM doit faire l'objet d'une confirmation explicite, afin d'éviter toute erreur de manipulation de l'administrateur.

Fiabilité & Automatisation

- Le déploiement d'une VM doit être entièrement automatisé, sans recours à une intervention manuelle sur Proxmox.

- La solution doit offrir une expérience utilisateur fluide, même lors de phases de déploiement prolongées.

Intégration

- Le Dashboard doit s'intégrer avec les services existants (Proxmox, Jenkins, Ansible) sans nécessiter de modification majeure de l'infrastructure actuelle.

C. Diagramme SysML Requirements

Ce diagramme précise les exigences fonctionnelles et techniques, leur hiérarchie, et les relations de dépendance entre elles.
Il permet de structurer le projet selon une approche systémique et d'assurer la traçabilité.

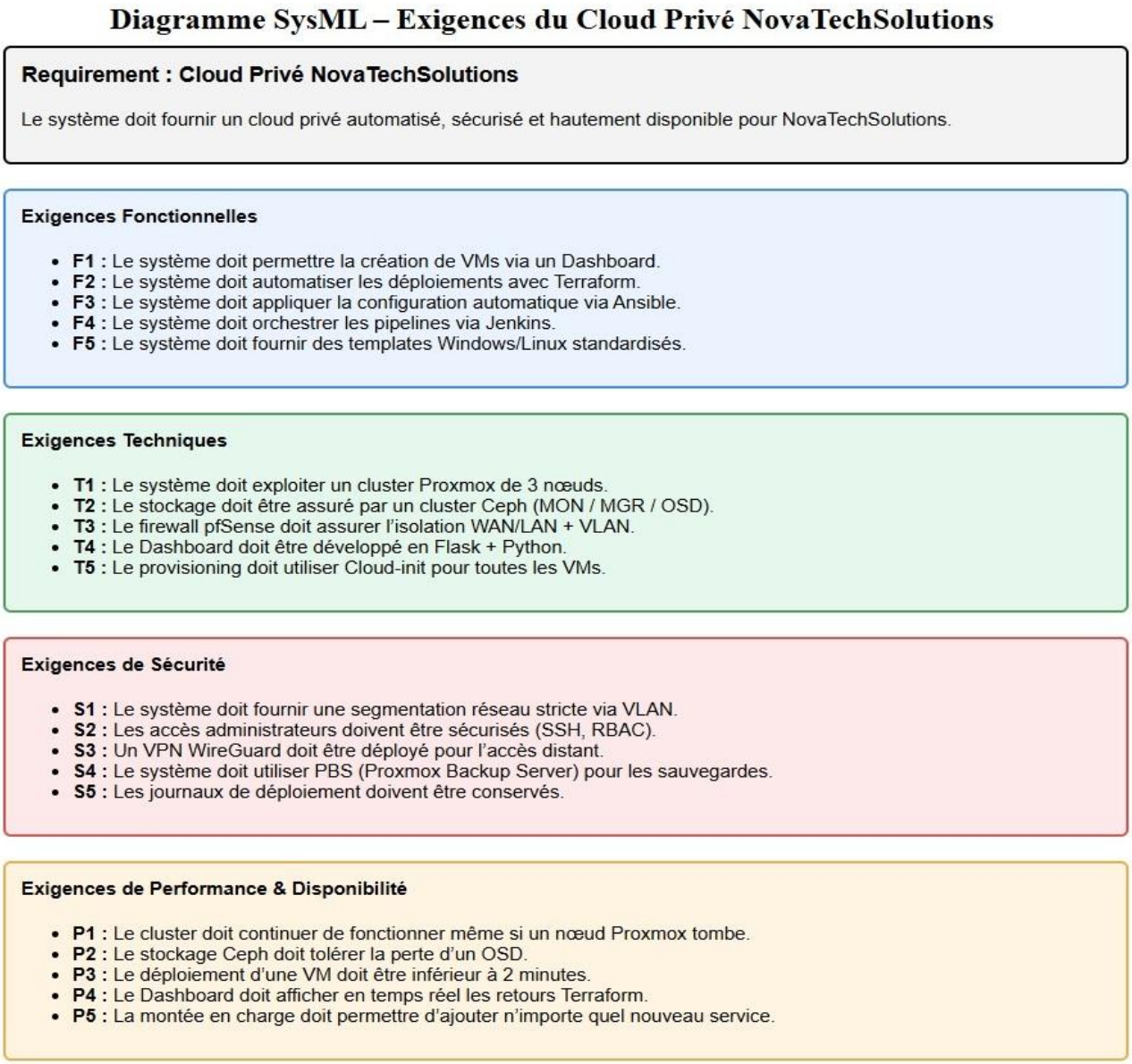


Figure 31 Diagramme SysML

D. Contraintes techniques, fonctionnelles, financières

D.1 Introduction au diagramme des contraintes

Dans le cadre de ce projet et afin de garantir un niveau de qualité conforme aux standards professionnels, j'ai porté une attention particulière aux contraintes liées à l'environnement, aux technologies employées et aux exigences fonctionnelles exprimées.

Bien que le budget alloué soit restreint, une licence Proxmox Enterprise a été intégrée à la solution afin d'assurer l'accès à des dépôts stables, à des correctifs certifiés ainsi qu'à un support technique renforcé.

Ce choix vise à garantir la stabilité de l'hyperviseur, cœur de l'infrastructure, tout en sécurisant les opérations de production. Pour l'ensemble des autres composants, j'ai privilégié des technologies *open source* reconnues telles que Terraform, Ansible, Jenkins, Ceph et Flask. Ces solutions, robustes et éprouvées, répondent pleinement aux besoins d'automatisation et d'orchestration sans entraîner de surcoûts logiciels.

La conception a également été pensée pour optimiser au maximum les ressources matérielles existantes. L'ensemble des serveurs, équipements réseau et capacités de stockage déjà disponibles ont été réutilisés afin de limiter les investissements additionnels tout en garantissant la performance attendue. Le diagramme présenté ci-après offre une vue synthétique et structurée de l'ensemble des contraintes techniques, fonctionnelles et financières qui ont orienté les choix d'architecture et de déploiement.

D.2 Contraintes techniques

Compatibilité des solutions : Terraform, Ansible, Jenkins et Proxmox doivent pouvoir communiquer entre eux via API.

Ressources matérielles limitées : le projet repose sur une infrastructure Proxmox, ce qui exclut des solutions lourdes comme OpenStack.

VLANs et accès réseau : chaque composant (Proxmox, Ceph, Jenkins, Dashboard Flask…) doit être accessible sur des VLANs distincts tout en respectant les règles de filtrage.

Capacité de stockages : la mise en place d'un cluster Ceph (disponibilité de disques et de serveurs adaptés).

Sécurité et isolation : nécessité de séparer les environnements (Production, Déploiement, Stockage) et d'assurer une isolation maximale.

Automatisation fiable : les playbooks Ansible, scripts Terraform et pipelines Jenkins doivent être rédigés de manière robuste et idempotent.

D.3 Contraintes fonctionnelles

Interface centralisée : l'utilisateur final doit pouvoir tout piloter depuis un seul dashboard.

Simplicité d'utilisation : le but est de masquer la complexité des outils sous-jacents et de rendre les actions accessibles même à un utilisateur non expert.

Réactivité et lisibilité : affichage clair de l'état des déploiements, logs lisibles, messages d'erreur explicites.

Templates standardisés : toutes les VM doivent être déployées depuis un template préconfiguré pour garantir l'homogénéité et réduire les erreurs.

D.4 Contraintes financières

Budget limité : le projet est mis en place avec un budget limité, tout en prenant en compte la licence entreprise de Proxmox.

Priorité aux solutions open source : Proxmox, Ceph, Terraform, Ansible, Jenkins et Flask sont retenus car stables et largement documentés.

Optimisation du matériel existant : Certains des serveurs, switches, disques et ressources réseau utilisés proviennent du matériel existant, ce qui permet de limiter le budget matériel.

En adoptant une approche mêlant solutions open source éprouvées, optimisation des ressources existantes et recours ciblé à une licence Proxmox Enterprise, la solution proposée répond de manière équilibrée aux exigences de stabilité, de performance et de maîtrise des coûts.

Ces éléments ont permis d'établir une base solide pour la conception du système, d'assurer la cohérence des outils utilisés et de garantir la pérennité de l'environnement. La section suivante présente donc l'architecture détaillée ainsi que les mécanismes techniques mis en œuvre pour répondre à ces objectifs.

D.5 Indicateurs de succès (KPI)

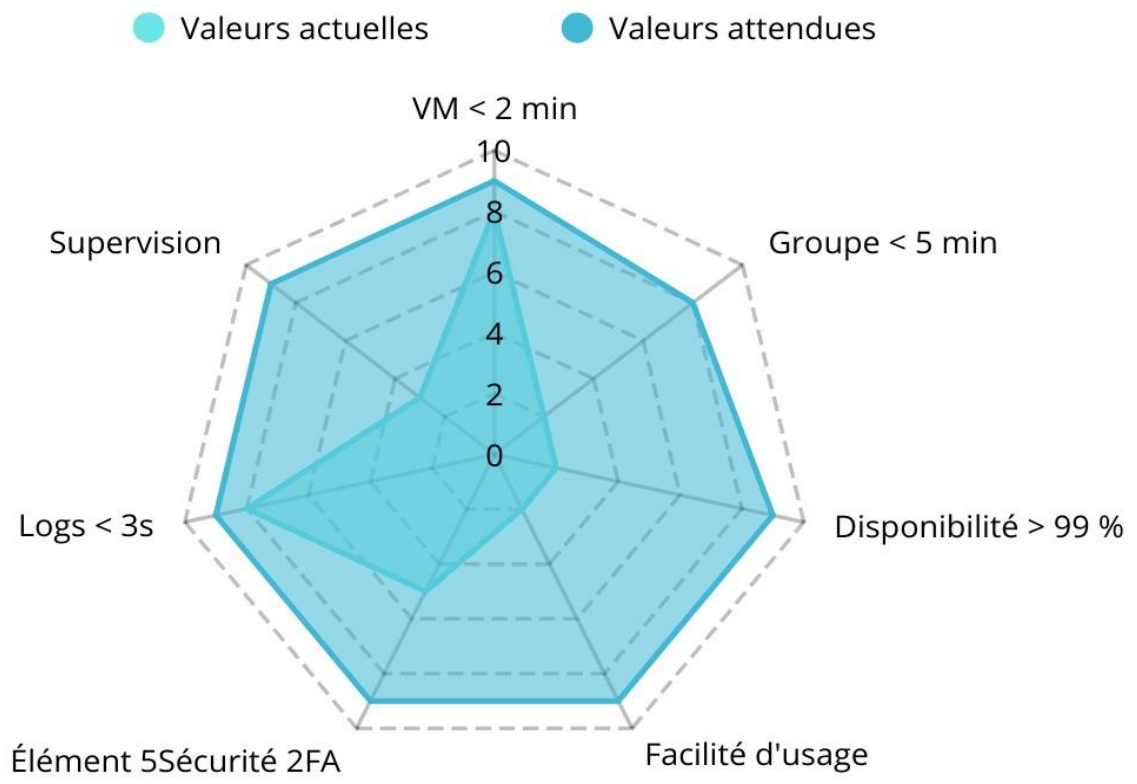


Figure 32 Radar KPI

Les indicateurs de succès permettent d'évaluer objectivement si la solution répond au besoin initial. Ils servent de base à la recette et à la validation finale du projet.

Performance & Automatisation

1. Temps de déploiement d'une VM (≤ 2 minutes après création depuis le dashboard).
2. Déploiement d'un groupe de VMs complet (≤ 5 minutes, selon le nombre de VMs).
3. Homogénéité garantie à 100 % entre les VMs déployées à partir du même Template.

Disponibilité & Supervision

4. Disponibilité du dashboard ≥ 99 % pendant les périodes prévues.
5. Actualisation des logs Proxmox ≤ 3 secondes.
6. Les logs des postes utilisateurs sont consultables à tout moment depuis le dashboard Graylog.
7. Prise en main complète par un administrateur en moins de 30 minutes, après une formation.

VI.2 Cahier des Charges Technique (CDCT)

Contrairement au CDCF, centré sur les besoins utilisateurs, le CDCT s'intéresse exclusivement aux moyens techniques nécessaires pour atteindre ces objectifs.

A. Exigences et Contraintes Techniques

Les exigences techniques décrivent le comportement attendu du système, les technologies retenues et les contraintes imposées par l'environnement de NovaTechSolutions.

A.1 Infrastructure système

Cluster Proxmox
Le projet repose sur un cluster Proxmox VE composé de 3 nœuds physiques : pve01, pve02, pve03.
La solution doit être compatible avec Proxmox VE ≥ 8.4.
Les VMs doivent être déployées dans le datastore *vmstore* (disque OSD) afin d'assurer une homogénéité et une meilleure gestion.
La communication avec l'API Proxmox doit s'effectuer via HTTPS sur le port 8006.

Templates
Tous les déploiements doivent être effectués uniquement via des Templates normalisés : Linux, Windows, images spécialisées.
Les Templates doivent intégrer Cloud-Init pour automatiser la personnalisation des VMs.

A.2 Automatisation Terraform

Exigences
Terraform doit être utilisé dans sa version ≥ 1.5.
Le provider Proxmox utilisé devra être bpg/Proxmox (v0.87.0).
Les déploiements Terraform doivent être effectués dans des environnements éphémères, stockés temporairement puis supprimés afin d'éviter toute pollution de configuration.
Ces fichiers doivent être générés à chaque déploiement :
main.tf / provider.tf / variables.tf / terraform.tfvars

Contraintes
Aucune configuration persistante ne doit rester sur le serveur près l'exécution.
Les erreurs Terraform doivent être capturées et remontées proprement dans l'interface.

A.3 Dashboard Web (Flask/Python)

Exigences techniques

Le service doit être développé avec Python ≥ 3.11 (Framework obligatoire : Flask).

Interface en HTML/CSS avec scripts JS pour la supervision Proxmox, les actions sur VMs, le monitoring en temps réel, l'affichage des logs, la gestion Ansible et la création de groupes complexes d'infrastructure.

Sécurité

Authentification obligatoire par identifiant + mot de passe.
Implémentation d'un second facteur d'authentification (MFA**)** avec TOTP.
Aucune information critique (mot de passe Proxmox, tokens API) ne doit être accessible côté client.
Contrôle lors de la connexion en HTTPS via mTLS.

Contraintes

Le serveur Flask doit être configuré en mode sécurisé (HTTPS).
Les logs d'accès et d'erreurs doivent être stockés localement.

A.4 Intégration Ansible

Exigences

La plateforme doit pouvoir exécuter des playbooks de tests (ping.yml), des playbooks de maintenance (maj.yml) et des playbooks de déploiements logiciels.
L'exécution doit se faire via SSH depuis le dashboard.
Un retour en temps réel doit être affiché dans l'interface.

Contraintes

Timeout maximum : 300 secondes.
L'utilisateur ne doit pas pouvoir exécuter un playbook non approuvé par des tests en amont.
Le serveur Ansible doit être joignable depuis le dashboard, tout comme Jenkins.

A.5 Supervision et Journaux d'évènements

Exigences

Le dashboard doit pouvoir interroger chaque nœud Proxmox (CPU, RAM, Stockage, Disponibilité , Nombre de VMs actives).
Les logs doivent être obtenus via la commande : journalctl -n 50 --no-pager.

Contraintes

Le rafraîchissement doit se faire toutes les 5 secondes pour le monitoring.
Les logs doivent être rafraîchis toutes les 3 secondes.

B. Etude comparative des solutions

B.1 Comparatif des hyperviseurs de type 1 (Proxmox, VMware, Hyper-V)

Une étude comparative a été menée entre VMware ESXi, Microsoft Hyper-V et Proxmox VE afin d'identifier la solution la plus adaptée aux besoins de NovaTechSolutions.

VMware ESXi constitue une référence du marché, reconnue pour sa maturité et son écosystème riche, mais implique des coûts de licences élevés et une forte dépendance éditeur.

Hyper-V offre des fonctionnalités avancées telles que la haute disponibilité, la reprise après sinistre et l'optimisation des coûts via la consolidation des serveurs, notamment grâce à son intégration avec Windows Server. Toutefois, cette solution reste fortement liée à l'environnement Microsoft.

Proxmox VE est une plateforme de virtualisation open source reposant sur Debian et combinant KVM pour les machines virtuelles et LXC pour les conteneurs, tout en intégrant nativement la haute disponibilité, le stockage logiciel et les capacités réseau. Cette approche garantit un haut niveau de flexibilité, de transparence technologique et de maîtrise des coûts.

Le choix de *Proxmox VE* s'est donc imposé pour plusieurs raisons :

- Cohérence avec l'infrastructure existante, déjà équipée d'un nœud Proxmox.
- Réduction des coûts de licences.
- Indépendance vis-à-vis d'un éditeur propriétaire.
- Richesse fonctionnelle compatible avec une architecture cloud privée.

Ce choix répond ainsi à une logique à la fois technique, économique et stratégique, tout en respectant la volonté du client de capitaliser sur son socle technologique actuel.

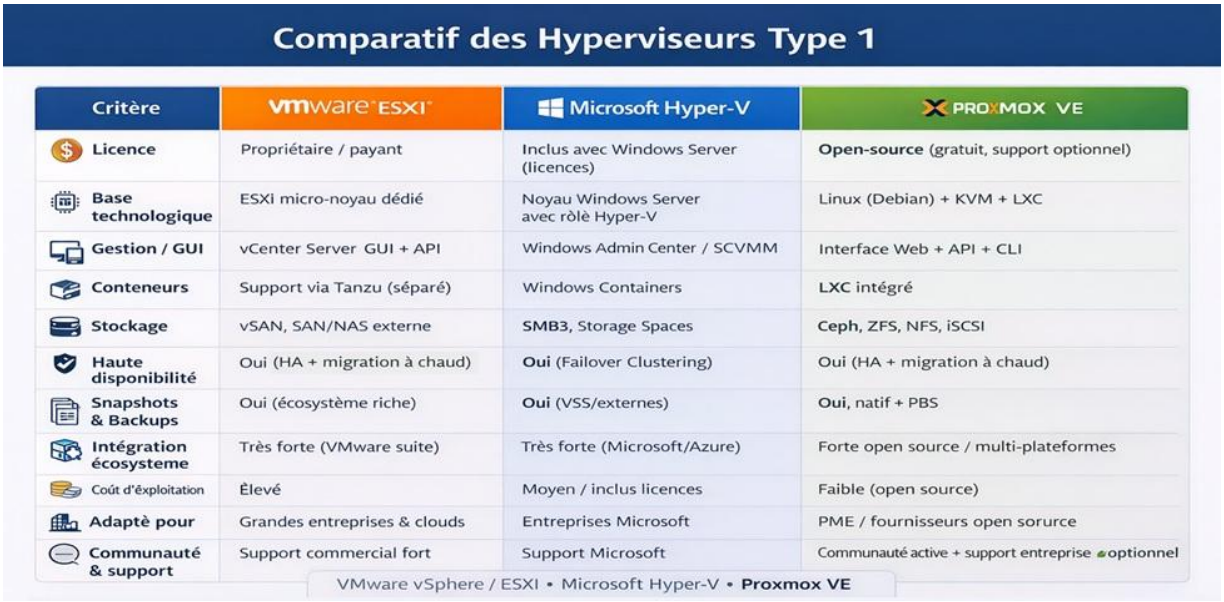


Figure 33 Comparatif des Hyperviseurs Type 1

B.2 Comparatif des prix de licences (Proxmox, VMware, Hyper-V)

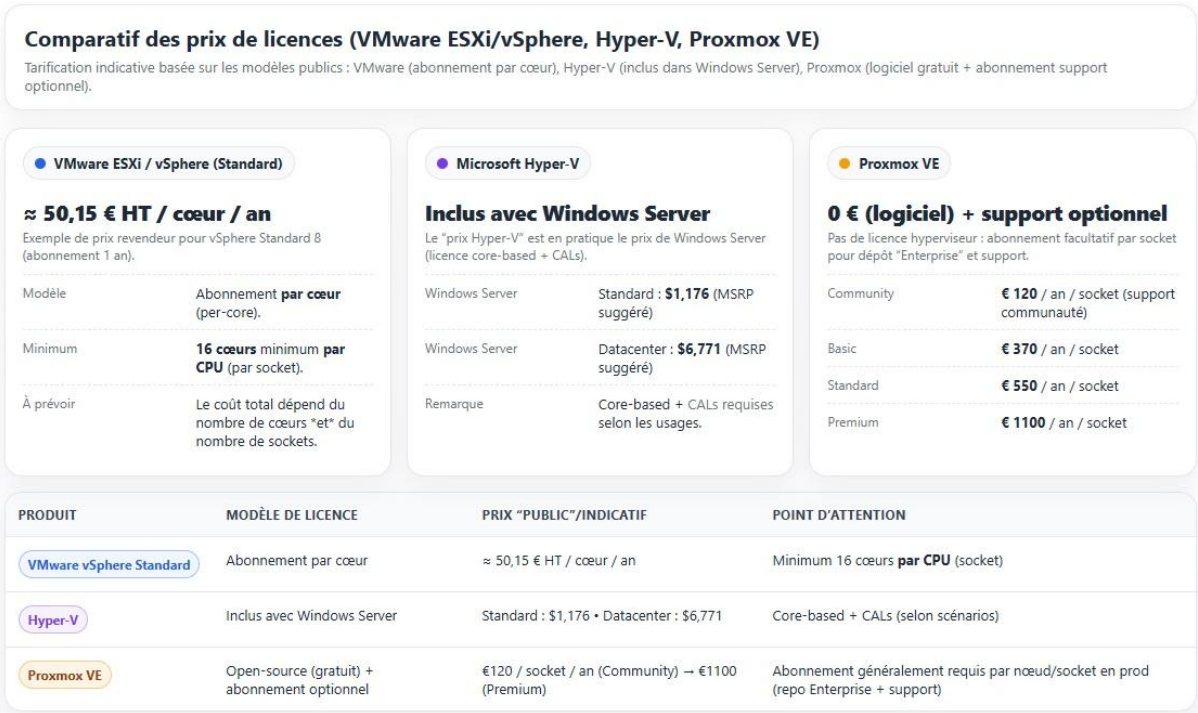


Figure 34 Comparatif des prix des licences Hyperviseur Type I

Choix de la solution : Proxmox VE

Dans le cadre de ce projet, j'ai choisi d'implémenter *Proxmox VE* comme solution de virtualisation.

Ce choix repose tout d'abord sur un critère économique. Contrairement à VMware ESXi ou à Hyper-V qui nécessitent des licences payantes (abonnement par cœur pour VMware, licence Windows Server pour Hyper-V), Proxmox est une solution open-source et gratuite. Cela permet de réduire considérablement les coûts d'infrastructure, notamment dans un contexte de projet pédagogique ou de petite/moyenne structure.

Au-delà de l'aspect financier, Proxmox propose des fonctionnalités avancées comparables aux solutions concurrentes : gestion centralisée, haute disponibilité, clustering, sauvegardes intégrées, support des machines virtuelles (KVM) et des conteneurs (LXC). L'interface web est complète, intuitive et permet une administration simple et efficace de l'environnement.

Proxmox offre également une grande flexibilité technique. Il repose sur Debian Linux, ce qui garantit stabilité, sécurité et mises à jour régulières. Son modèle d'abonnement reste optionnel et concerne principalement le support professionnel et l'accès au dépôt « Enterprise », ce qui laisse une liberté totale dans le mode d'exploitation.

Enfin, la communauté active autour de Proxmox constitue un véritable atout : documentation riche, forums techniques et retours d'expérience facilitent la prise en main et la résolution de problèmes.

De plus, l'entreprise NovaTechSolutions utilise déjà Proxmox dans son infrastructure, ce qui rend ce choix cohérent, pertinent et aligné avec l'environnement technique existant.

B.3 Comparatif des solutions de pare-feu (PFSense, OPNsense, Fortigate, Cisco, Sophos)

Synthèse du comparatif et choix de la solution

Solution	Type	Points forts	Limites	Profil recommandé
pfSense	Open source	Coût logiciel nul, très flexible, fonctionnalités réseau avancées (VPN, VLAN, filtrage, IDS/IPS via packages).	Administration plus technique, maintenance à assurer en interne.	PME avec compétences réseau/IT disponibles.
OPNsense	Open source	Interface moderne, mises à jour fréquentes, fonctionnalités similaires à pfSense (VPN, reporting, plugins).	Écosystème/ressources parfois moins "mainstream" que pfSense selon les équipes.	PME cherchant une alternative open source plus "user-friendly".
Fortinet FortiGate	NGFW (appliance)	Très bon compromis perf/sécurité, protection avancée (IPS/AV/Web), support pro, gestion centralisable.	Coût matériel + licences pour activer certaines fonctions de sécurité.	PME voulant une sécurité "pro" avec support éditeur.
Cisco (Secure Firewall / Meraki)	NGFW / Cloud	Fiabilité, intégration écosystème Cisco, Meraki très simple à administrer (cloud).	Souvent plus coûteux (licences/abonnements), peut être surdimensionné pour petite structure.	Entreprises avec budget plus confortable ou standard Cisco.
Sophos Firewall	NGFW (appliance/virtuel)	Interface claire, bon niveau de sécurité, intéressant si parc déjà équipé Sophos (intégrations).	Fonctions avancées dépendantes de la licence; perf selon modèle.	PME sans équipe cybersécurité dédiée, recherchant simplicité + protection.

Figure 35 Synthèse - Choix des solutions

L'étude des différentes solutions de pare-feu (PfSense, OPNsense, Fortinet, Cisco et Sophos) a permis d'identifier les outils capables de répondre aux besoins de sécurité d'une entreprise tout en respectant des contraintes budgétaires.

Les solutions open source comme PfSense et OPNsense sont reconnues pour leurs fonctionnalités avancées, leur sécurité robuste et leur grande flexibilité, ce qui explique leur adoption dans de nombreux environnements professionnels.
À l'inverse, les solutions propriétaires offrent souvent un support éditeur mais impliquent des coûts plus importants.

Après analyse, le choix s'est porté sur OPNSense, pourquoi ?

Plusieurs raisons justifient ce choix :

- Alternative économique aux pare-feu commerciaux : OPNSense fournit des fonctionnalités de niveau entreprise sans coûts élevés de licence.
- Flexibilité **:** la solution propose de nombreuses fonctionnalités personnalisables selon les besoins de l'entreprise.
- Sécurité élevée : elle offre une protection robuste grâce à un contrôle précis du trafic et au support de VPN assurant la confidentialité des données.

Par ailleurs, OPNSense est considéré comme une plateforme puissante, flexible et sécurisée, capable de maintenir un réseau fiable et efficace pour des organisations de toutes tailles.

Enfin, ce choix s'inscrit également dans une logique de continuité technique : l'entreprise utilise déjà OPNSense et souhaite conserver cette solution. Maintenir un outil existant permet de limiter les coûts de migration, de réduire le temps de déploiement et de capitaliser sur les compétences internes déjà acquises.

Conclusion

Le choix de OPNSense constitue donc une réponse cohérente aux enjeux de l'entreprise. Cette solution offre un équilibre pertinent entre sécurité, performance, maîtrise des coûts et simplicité d'intégration**,** tout en garantissant la pérennité de l'infrastructure réseau.

VI.3 Enveloppe budgétaire

Le projet s'appuie sur du matériel existant, ce qui réduit fortement les coûts.

A. Coûts directs estimés

Catégorie	Éléments	Quantité	Coût unitaire (€)	Coût total (€)
MATÉRIEL				
Serveurs Proxmox	3× nœuds Dell/HP Xeon + 64 Go RAM	3	2 000 €	6 000 €
Disques NVMe / SSD Ceph	6× NVMe 1 To (OSD)	6	120 €	720 €
Switch 10 Gbit/s	Switch VLAN + 10G Ceph	1	800 €	800 €
LOGICIELS				
Terraform, Ansible, Debian, Ubuntu, Graylog, pfSense CE	Logiciels libres	—	0 €	0 €
Licence Proxmox Enterprise	3× souscriptions (1 an)	3	370 €	1 110 €
Windows Server 2022 Standard	Licence + CALs	1	850 €	850 €
Windows 11 Pro	20 postes clients	20	150 €	3 000 €
MAIN D'ŒUVRE				
Conception + installation + automatisation	40h × 75 €/h	40 h	75 €	3 000 €
TOTAL GLOBAL				**≈ 14 480 €**

Figure 36 Tableau coûts directs estimés

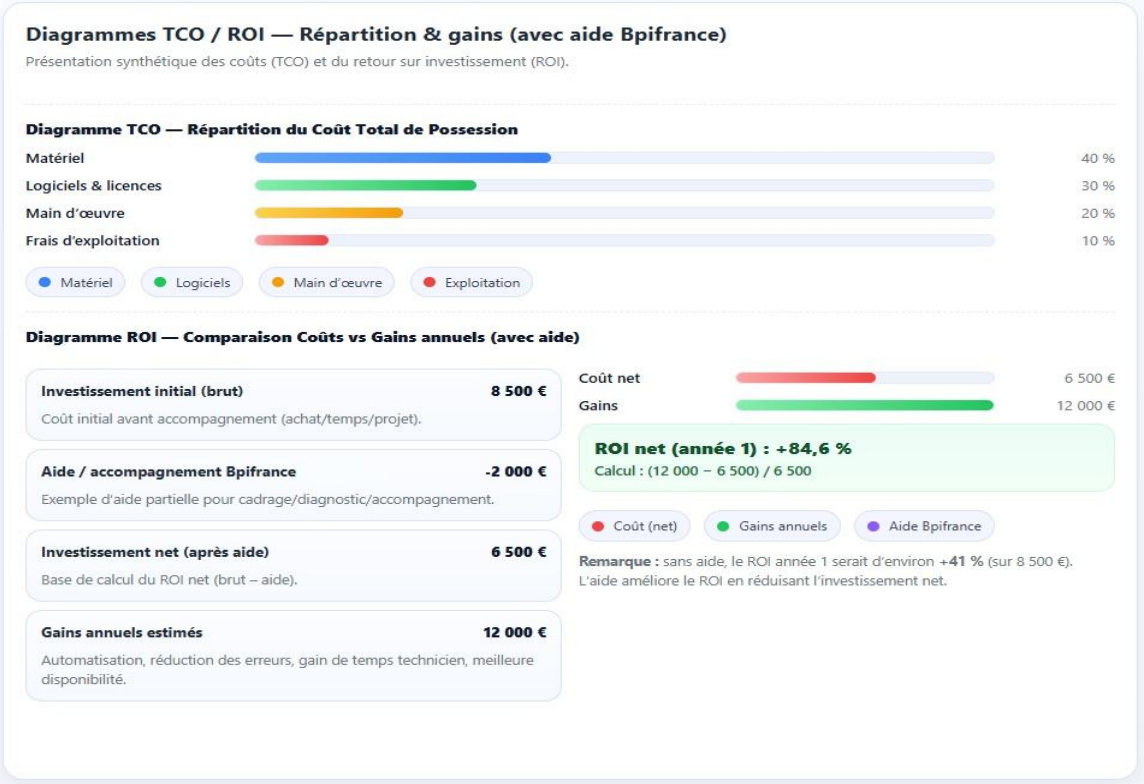


Figure 37 Diagramme TCO / ROI

Dispositifs d'accompagnement et d'aides à la transformation numérique

Dans le cadre de sa démarche de modernisation de l'infrastructure informatique, NovaTechSolutions a bénéficié d'un accompagnement proposé par Bpifrance, visant à soutenir les PME dans leurs projets de transformation numérique et de renforcement de la cyber sécurité.
L'appui de Bpifrance contribue à réduire les risques liés à l'investissement initial, à améliorer la maîtrise des coûts et à favoriser un retour sur investissement plus rapide, sans remettre en cause l'autonomie technique et opérationnelle de l'entreprise.

Figure 38 Estimation d'aide BPIFrance

Lien entre accompagnement Bpifrance et analyse financière

L'accompagnement de Bpifrance s'intègre dans la réflexion globale sur le coût total de possession (TCO) et le retour sur investissement (ROI) du projet.
En apportant un cadre méthodologique et une aide à la priorisation des actions, il permet de limiter les dépenses non essentielles, de sécuriser les investissements techniques et d'optimiser les coûts d'exploitation à moyen et long terme.
Cette démarche contribue à améliorer la rentabilité globale du projet tout en renforçant la résilience et la sécurité de l'infrastructure.

B. Délais (prévision)

Le tableau ci-dessous présente la décomposition du projet en phases structurées, chacune associée à une durée estimée et à une description précise des travaux réalisés.

Cette organisation facilite le suivi de l'avancement, la maîtrise des risques, la répartition du travail et la justification du planning.

Ces durées sont issues d'une estimation réaliste basée sur l'expérience acquise lors de la mise en œuvre du projet. Elles tiennent compte des temps de développement, d'intégration, de tests fonctionnels et techniques, ainsi que de la production des livrables nécessaires (documentation, supports de soutenance).

Délais prévisionnels du projet

Phase	Durée estimée	Description
Analyse & conception	1 semaine	Étude détaillée du besoin, analyse de l'existant, définition de l'architecture cible et rédaction du cahier des charges.
Développement du dashboard	3 semaines	Développement de l'interface Flask, intégration de Terraform, mise en place de l'authentification (login + 2FA) et des premiers écrans de supervision.
Intégration Ansible	1 semaine	Intégration des playbooks (ping, mises à jour, post-configuration), sécurisation SSH et tests de bout en bout.
Tests & recette	1 semaine	Campagne de tests techniques et fonctionnels, recette utilisateur, correction des anomalies et ajustements finaux.
Documentation & soutenance	1 semaine	Rédaction du rapport de projet, mise à jour des documents techniques et préparation de la soutenance (supports, démonstrations).

Durée totale estimée : 7 semaines.

Figure 39 Délais Prévisionnels du projet

C. Introduction du devis Cloud Privé pour NovaTechSolutions

Le devis sera établi par *NebTech* et détaillera les coûts associés à la conception, au déploiement et à la mise en production.

Ce devis couvrira l'ensemble des éléments nécessaires à la réalisation du projet :

- Matériel (serveurs, stockage, réseau, équipements de sécurité)
- Logiciels et composants open-source intégrés
- Conception et déploiement de l'architecture Proxmox + Ceph
- Mise en place des outils d'automatisation (Terraform, Ansible, Jenkins)
- Développement du dashboard Flask pour le déploiement des VMs
- Configuration réseau, VLAN, sécurité et VPN
- Sauvegarde et plan de reprise via Proxmox Backup Server
- Documentation technique complète et formation utilisateur

L'objectif de ce devis est d'offrir à NovaTechSolutions une vision financière claire, transparente et détaillée de l'ensemble du projet, tout en garantissant un excellent rapport qualité/prix grâce au choix de technologies robustes et open source. Il servira également de référence tout au long du projet, permettant à NovaTechSolutions de valider les coûts, d'anticiper les dépenses futures et d'assurer une maîtrise budgétaire complète.

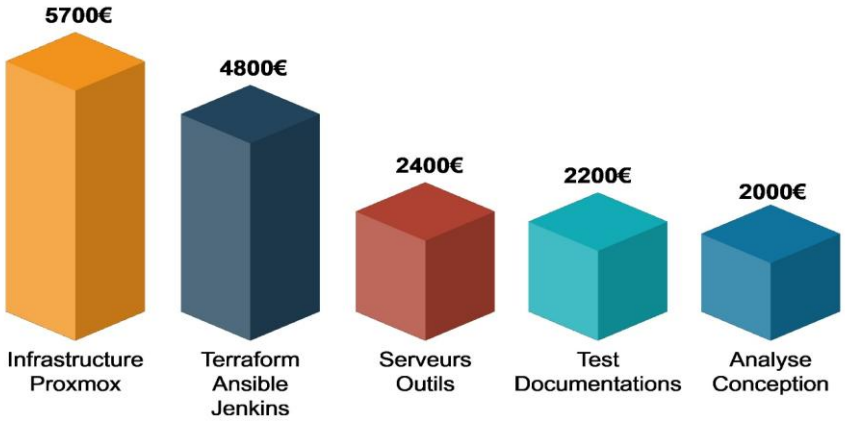


Figure 40 Budget – Prévision

Afin d'estimer l'investissement global nécessaire à la mise en place du cloud privé de NovaTechSolutions, un budget prévisionnel a été établi.

Ce budget prend en compte l'ensemble des dépenses matérielles, logicielles et humaines nécessaires au déploiement de l'infrastructure :

- Achat des serveurs, stockage Ceph et éléments réseau,
- Acquisition des licences Proxmox et du matériel associé,
- Mise en place physique (baie, PDU, onduleur, câblage),
- Temps de conception, de configuration et de validation,
- Coûts éventuels de formation et documentation.

L'objectif est de fournir une vision claire du coût total du projet, tout en assurant transparence et justification de chaque poste.
Ce budget permet également d'anticiper la scalabilité future du cloud privé et d'éviter les dépenses imprévues.

Catégorie	Équipement	Quantité	Prix unitaire	Total
Serveurs & Stockage				
Serveurs Proxmox	Bare-metal 64Go / NVMe	3	2 200 €	6 600 €
Cluster Ceph	Disques OSD (SSD/NVMe)	6	180 €	1 080 €
Proxmox Backup Server	Serveur PBS (32 Go RAM)	1	1 600 €	1 600 €
Proxmox Manager	Serveur dédié de supervision	1	1 400 €	1 400 €
Réseau				
Firewall	pfSense en HA (2 appliances)	2	650 €	1 300 €
Switch Cisco	C9300-24T + uplink SFP+	1	5 800 €	5 800 €
Câblage	Câbles RJ45/SFP+/fibre OM4	—	300 €	300 €
Énergie & baie				
Baie informatique	24U + roulettes	1	550 €	550 €
PDU	Barre d'alimentation 12 ports	1	180 €	180 €
Onduleur UPS	1500 VA / rackable	1	450 €	450 €
Licences				
Proxmox VE	Licence PVE Standard (x3)	3	380 €	1 140 €
Proxmox Backup	Licence PBS	1	380 €	380 €
Total matériel & licences				**≈ 22 280 €**

Figure 41 Détails du Budget prévisionnel

D. Budget main d'œuvre

Chef de projet : 12 jours × 450 € = 5 400 €
Ingénieur système (IaC) : 25 jours × 380 € = 9 500 €
Technicien réseaux : 10 jours × 320 € = 3 200 €
Rédaction & documentation : 5 jours × 280 € = 1 400 €
Total main d'œuvre = 19 500 €

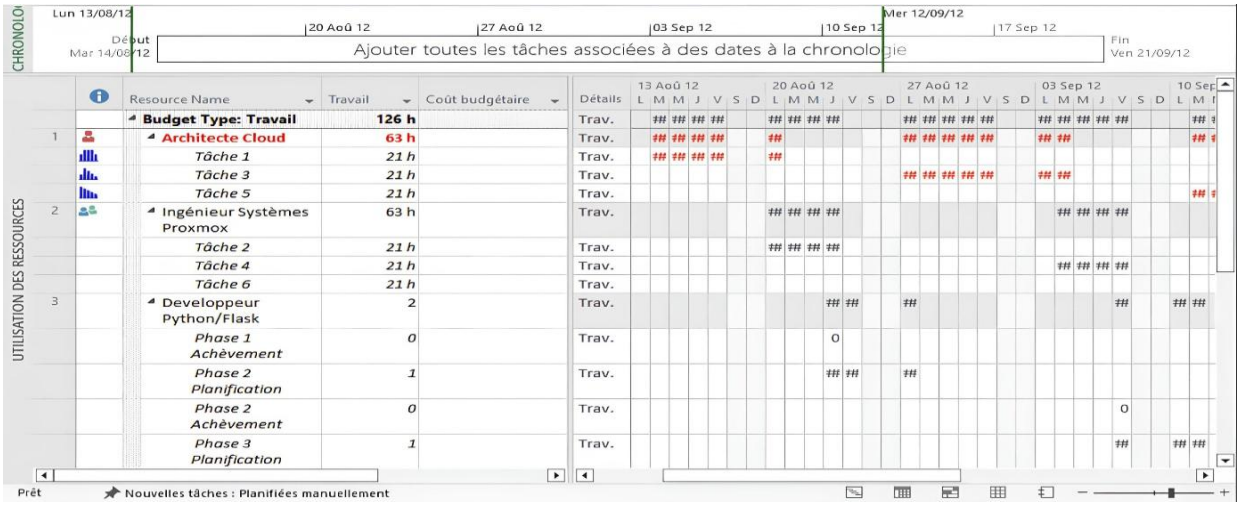


Figure 42 Tableau rémunération main-d'œuvre prévisionnelle.

Le budget détaillé et définitif est établi dans le chapitre **VIII**.

VII. Phase de conception

VII.1 Conception Fonctionnelle

Parcours utilisateur

Objectif : illustrer les principales interactions entre l'utilisateur et le système.

A. Diagramme de séquence « Déploiement VM » (Workflow UML)

Le diagramme suivant représente le processus complet de déploiement automatisé d'une machine virtuelle au sein du cloud privé NovaTechSolutions.
Il s'agit d'un diagramme de séquence UML, utilisé pour visualiser l'enchaînement des actions déclenchées par l'utilisateur, les interactions entre les différentes briques techniques (Flask, Terraform, API Proxmox, Ceph, Cloud-Init, Jenkins, Ansible), les points de contrôle, de validation et de gestion des erreurs. Le cheminement exact permettant la création d'une VM sans intervention manuelle.

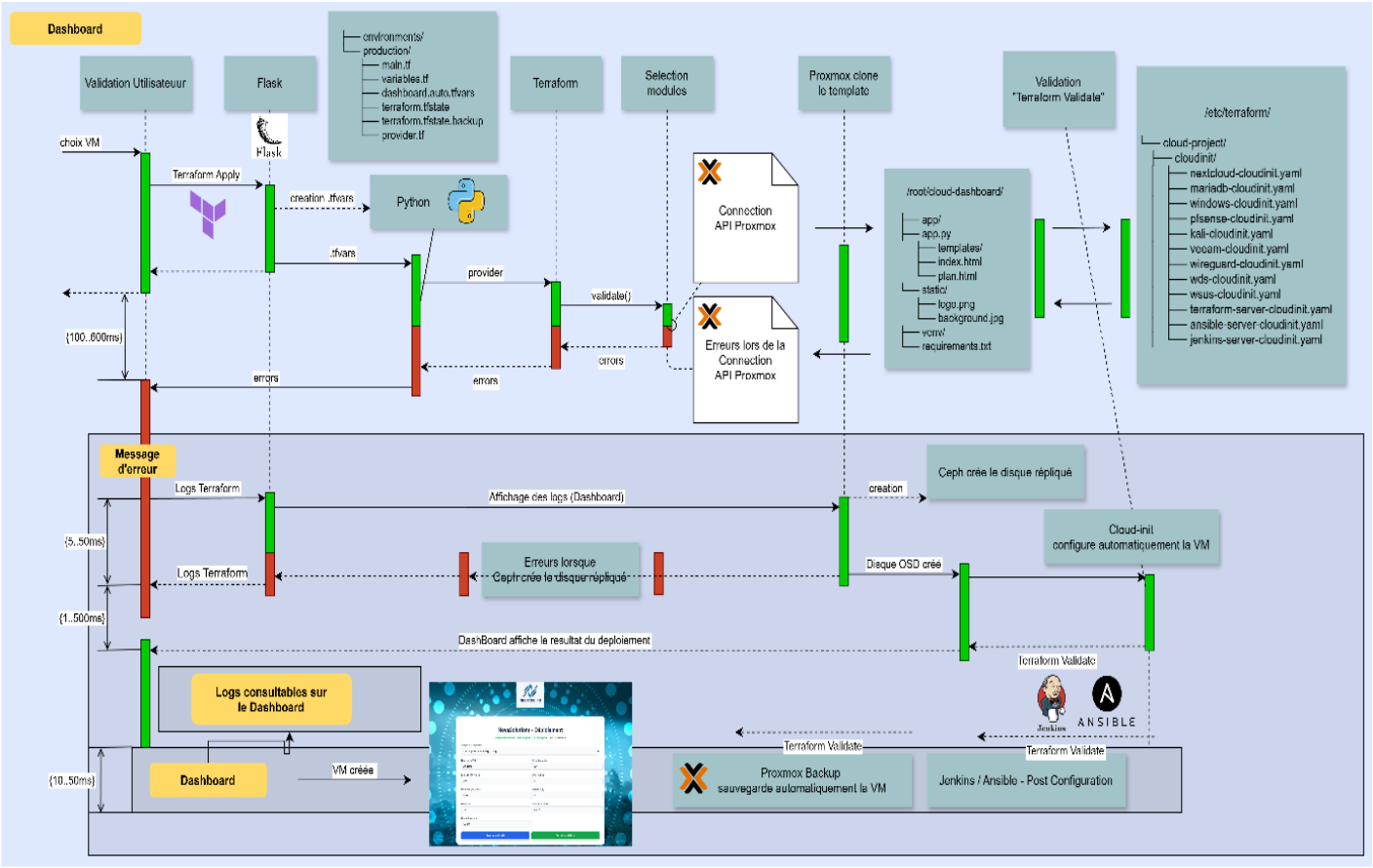


Figure 43 Diagramme Workflow UML1.

1. L'utilisateur se connecte au dashboard depuis un navigateur.
2. Il s'identifie avec des ID transmis par l'administrateur + MFA (QR Code/Mtls).
3. Depuis le dashboard, il sélection un Template et les caractéristiques souhaitées (RAM, CPU, Storage, ID, nœud).
4. La VM se déploiement et l'utilisateur peut consulter l'état du déploiement via le monitoring.
5. Plusieurs Actions sont disponibles (Start, Reset, Stop, Migration, Suppression, visualisation des logs, exécution de playbooks Ansible via un terminal ou depuis Jenkins).

VII.2 Conception Technique

A. Schéma d'architecture

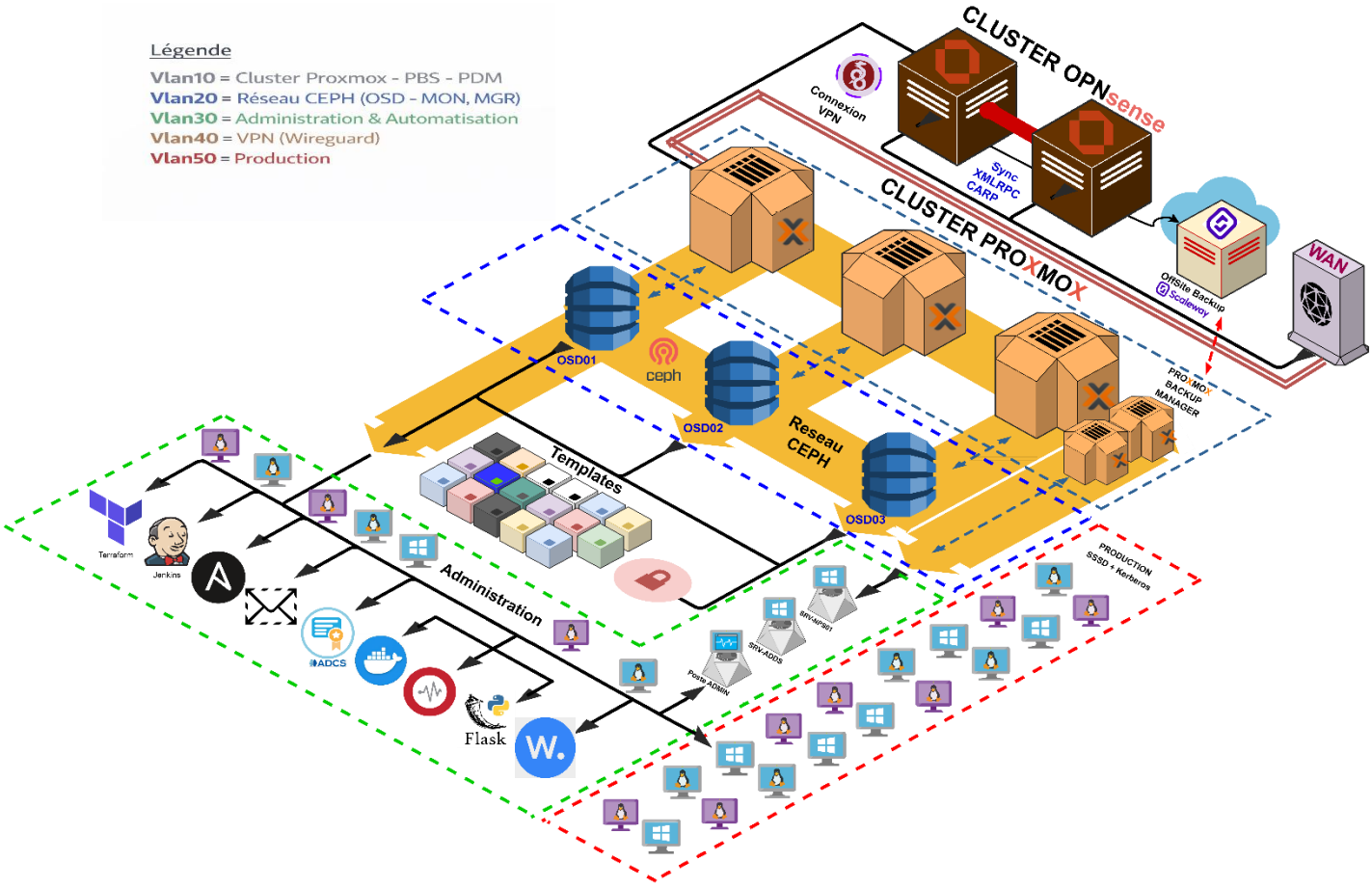


Figure 44 Schéma d'architecture

B. Analyse du schéma d'architecture

VLAN10 – Cluster Proxmox – PBS – PDM

Trafic d'administration :

- API Proxmox
- Cœur du cluster
- Accès administrateur

VLAN20 – Réseau Ceph (OSD, MON, MGR)

Assure la haute disponibilité du stockage :

- Synchronisation des blocs CEPH
- Réplication OSD ↔ OSD ↔ OSD
- Trafic MON ↔ OSD

VLAN30 – Automatisation & Administration

Permet de centraliser tous les outils d'orchestration :

- Terraform (exécution et drivers)
- Ansible (post-configuration automatisée)
- Jenkins (pipelines CI/CD)
- Dashboard Flask (interface administrateur)
- ADCS / Docker / Graylog / Wazuh

VLAN40 – VPN / Wireguard

Permet l'accès sécurisé à distance :

- Administrateurs distants
- Consoles internes
- API privées

VLAN50 – Production (VM Déployées)

Espace réseau dans lequel Terraform déploie automatiquement :

- Applications métiers
- Environnements de test
- Services internes

⇨ Isolation stricte vis-à-vis du réseau d'administration et du stockage.

C. Schéma d'Architecture Réseau Final

Architecture physique / Cluster Proxmox / NovaTechSolutions

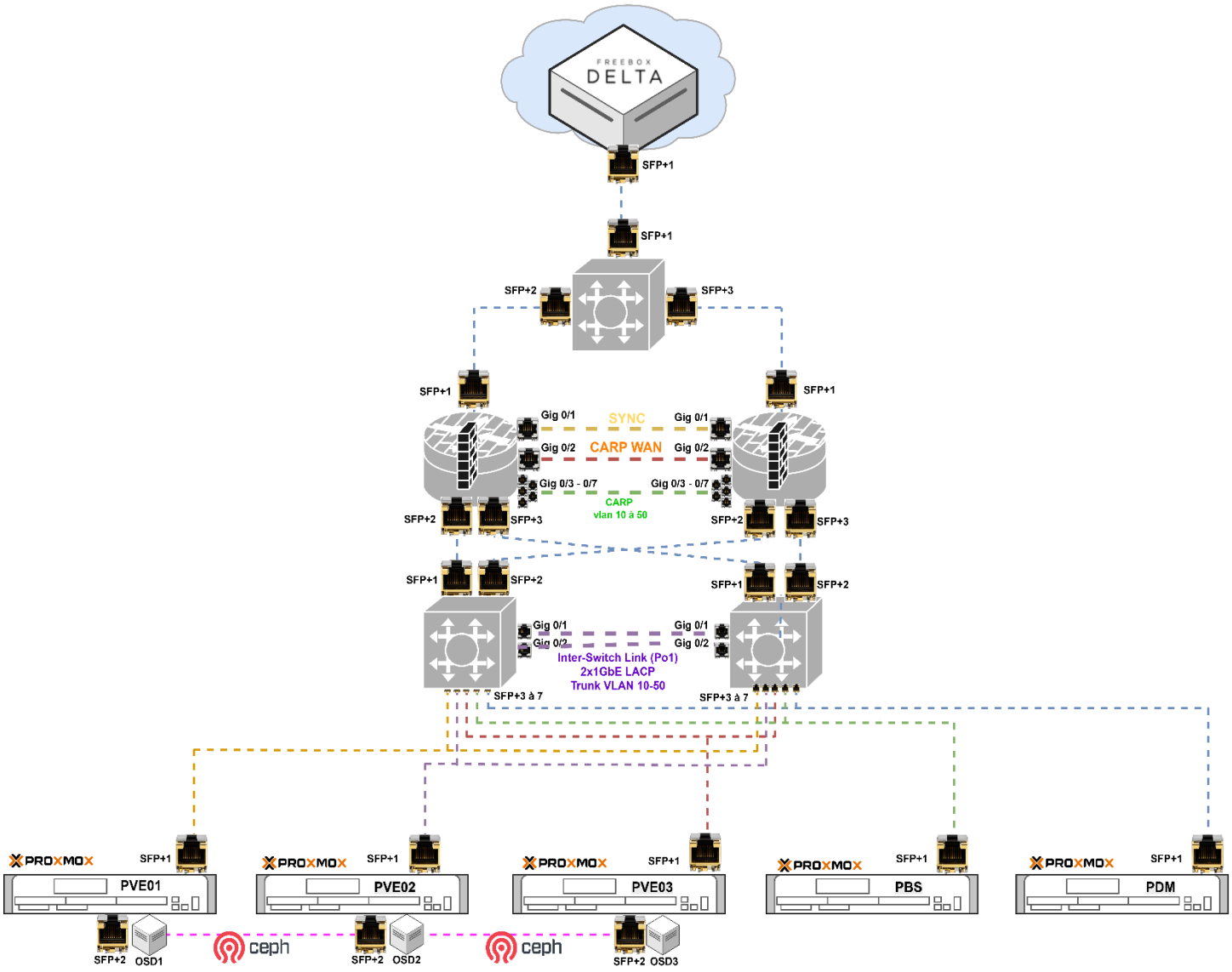


Figure 45 Schéma d'architecture réseau

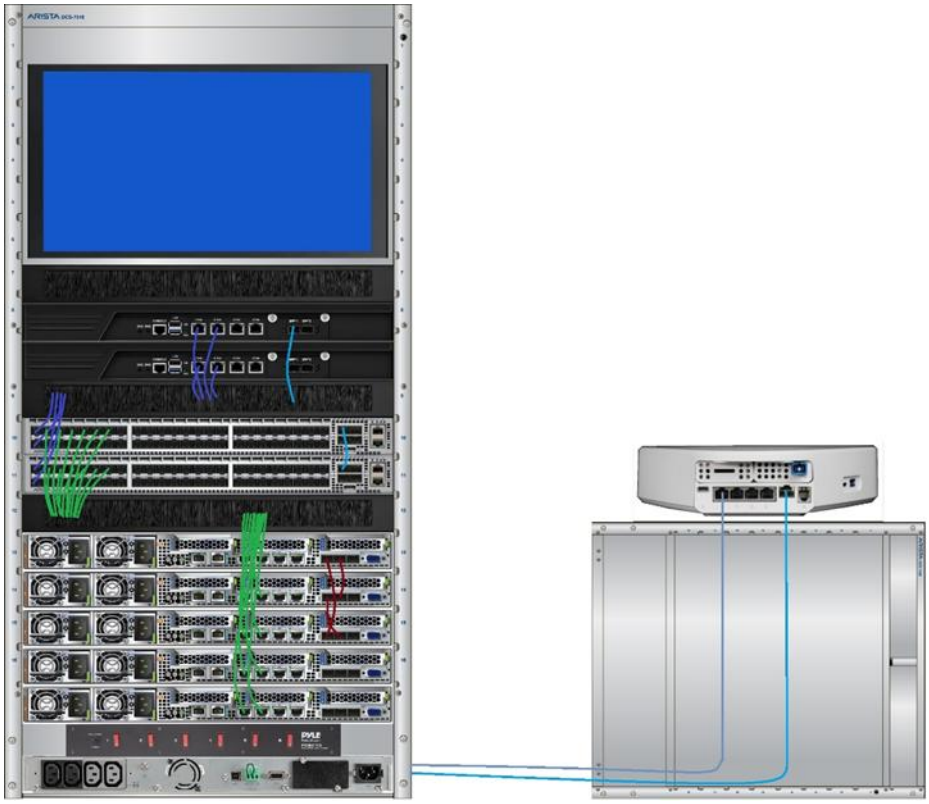


Figure 46 Représentation matériel sur site

D. Plan d'adressage IP

Plan d'adressage IP — Cloud privé hautement disponible

Segmentation VLAN, CIDR optimisé, adressage privé RFC1918 (10.0.0.0/8)

Version : v1.1
Portée : Proxmox + Ceph + pfSense HA + VPN + Prod

1. Synthèse des réseaux

Zone	VLAN	CIDR	Masque	Gateway / VIP	Plage utilisable	Broadcast	Capacité
MGMT (Cluster/PBS/PDM)	10	10.10.10.0/27	255.255.255.224	10.10.10.1 (CARP)	10.10.10.1 → 10.10.10.30	10.10.10.31	30 hôtes
CEPH (OSD/MON/MGR)	20	10.10.20.0/28	255.255.255.240	(isolé / optionnel)	10.10.20.1 → 10.10.20.14	10.10.20.15	14 hôtes
Services internes / Automatisation	30	10.10.30.0/27	255.255.255.224	10.10.30.1 (CARP)	10.10.30.1 → 10.10.30.30	10.10.30.31	30 hôtes
VPN (WireGuard)	40	10.10.40.0/28	255.255.255.240	10.10.40.1 (CARP)	10.10.40.1 → 10.10.40.14	10.10.40.15	14 hôtes
Production	50	10.10.50.0/26	255.255.255.192	10.10.50.1 (CARP)	10.10.50.1 → 10.10.50.62	10.10.50.63	62 hôtes
SYNC FW (HA)	254	10.10.254.0/30	255.255.255.252	N/A	10.10.254.1 → 10.10.254.2	10.10.254.3	2 hôtes

WAN : l'interface WAN utilise l'IP fournie par l'opérateur (DHCP/Statique). Non incluse dans RFC1918.
Principe : CARP fournit la passerelle virtuelle par VLAN ; le lien SYNC (VLAN254) est dédié au HA (pfsync/XMLRPC).

2. VLAN10 — Management (10.10.10.0/27)

Équipement / VM	Rôle	IP	Masque	Gateway	Remarques
FW-VIP-MGMT	Passerelle virtuelle (CARP)	10.10.10.1	/27	—	Point d'entrée L3 du VLAN10
pfSense-1	Firewall HA (nœud 1) — interface VLAN10	10.10.10.2	/27	10.10.10.1	Admin / supervision
pfSense-2	Firewall HA (nœud 2) — interface VLAN10	10.10.10.3	/27	10.10.10.1	Admin / supervision
PBS	Proxmox Backup Server	10.10.10.4	/27	10.10.10.1	Backups locaux + réplication offsite
PDM	Proxmox Datacenter Manager	10.10.10.5	/27	10.10.10.1	Gestion/supervision cluster
PVE01	Proxmox Node 1	10.10.10.11	/27	10.10.10.1	Hyperviseur
PVE02	Proxmox Node 2	10.10.10.12	/27	10.10.10.1	Hyperviseur
PVE03	Proxmox Node 3	10.10.10.13	/27	10.10.10.1	Hyperviseur
Réserves	Extensions cluster / outils	10.10.10.6–10 , 10.10.10.14–30	/27	10.10.10.1	Marge pour ajout de nœuds/VMs mgmt

Figure 47 Plan d'adressage IP

3. VLAN20 — CEPH (10.10.20.0/28)

Équipement	Rôle	IP	Masque	Remarques
OSD01	OSD	`10.10.20.1`	`/28`	Trafic stockage (isolé)
OSD02	OSD	`10.10.20.2`	`/28`	Trafic stockage
OSD03	OSD	`10.10.20.3`	`/28`	Trafic stockage
MON01	Monitor	`10.10.20.11`	`/28`	Quorum
MON02	Monitor	`10.10.20.12`	`/28`	Quorum
MON03	Monitor	`10.10.20.13`	`/28`	Quorum
MGR	Manager	`10.10.20.14`	`/28`	Ceph Manager
Réserves	Ceph	`10.10.20.4–10`	`/28`	OSD/MON supplémentaires, services Ceph

4. VLAN30 — Automatisation & Services internes (10.10.30.0/27)

Service	Rôle	IP	Masque	Gateway	Remarques
FW-VIP-SRV	Passerelle VLAN30 (CARP)	`10.10.30.1`	`/27`	—	Routage inter-VLAN selon politique
Terraform	IaC / Déploiements	`10.10.30.11`	`/27`	`10.10.30.1`	Provisioning
Ansible	Automatisation	`10.10.30.12`	`/27`	`10.10.30.1`	Configuration
Jenkins	CI/CD	`10.10.30.13`	`/27`	`10.10.30.1`	Pipelines
ADCS	PKI / Certificats	`10.10.30.14`	`/27`	`10.10.30.1`	Certificats internes
Docker	Services conteneurisés	`10.10.30.15`	`/27`	`10.10.30.1`	Plateforme applicative
Monitoring	Supervision	`10.10.30.16`	`/27`	`10.10.30.1`	Alerting / métriques
Graylog	Centralisation logs	`10.10.30.17`	`/27`	`10.10.30.1`	Audit
Flask	Appli interne	`10.10.30.18`	`/27`	`10.10.30.1`	Service API/web
Réserves	Services futurs	`10.10.30.2–10`, `10.10.30.19–30`	`/27`	`10.10.30.1`	Registry, bastion, SSO, etc.

5. VLAN40 — VPN WireGuard (10.10.40.0/28)

Élément	Rôle	IP	Masque	Remarques
FW-VIP-VPN	Passerelle VLAN40 (CARP)	`10.10.40.1`	`/28`	IP virtuelle pour routage/filtrage
WG-SERVER	Terminaison WireGuard	`10.10.40.2`	`/28`	WireGuard
Pool clients VPN	Postes nomades / admins	`10.10.40.10–14`	`/28`	Pool (statique par peer)

6. VLAN50 — Production (10.10.50.0/26)

Élément	Rôle	IP	Masque	Gateway	Remarques
FW-VIP-PROD	Passerelle Production (CARP)	`10.10.50.1`	`/26`	—	Routage vers WAN / autres VLAN selon politique
Plage VMs PROD	Workloads production	`10.10.50.10–62`	`/26`	`10.10.50.1`	Réserver `.2–.9` pour VIP/LB/infra si besoin

7. VLAN254 — Synchronisation HA Firewalls (10.10.254.0/30)

Équipement	Rôle	IP	Masque	Remarques
pfSense-1	pfsync/XMLRPC	`10.10.254.1`	`/30`	Réseau dédié (recommandé)
pfSense-2	pfsync/XMLRPC	`10.10.254.2`	`/30`	Réseau dédié (recommandé)

VII.3 Vision d'exploitation et de production

A. Diagramme d'Architecture Technique Global

Le diagramme d'architecture technique globale présenté ci-après offre une vision synthétique et structurée de l'ensemble des composants du cloud privé NovaTechSolutions et de leurs interactions. Il permet au lecteur de comprendre rapidement la logique d'ensemble du système, depuis l'interface utilisateur jusqu'à l'exécution automatique du déploiement.

Ce schéma met en évidence :

- Le Dashboard Flask, point d'entrée pour l'utilisateur final, permettant les actions de déploiement, consultation et administration.
- Terraform, moteur d'infrastructure as code chargé de la création automatique des machines virtuelles sur Proxmox.
- Ansible, utilisé pour la configuration post-déploiement des VM (durcissement, rôles, services).
- Le cluster Proxmox, plateforme de virtualisation haute disponibilité assurant l'exécution des environnements.

- Le stockage distribué Ceph, garantissant la résilience, la réplication et la performance des données.
- Les outils de supervision et de journalisation, dont Graylog, permettant la collecte centralisée des logs et le suivi de l'infrastructure.

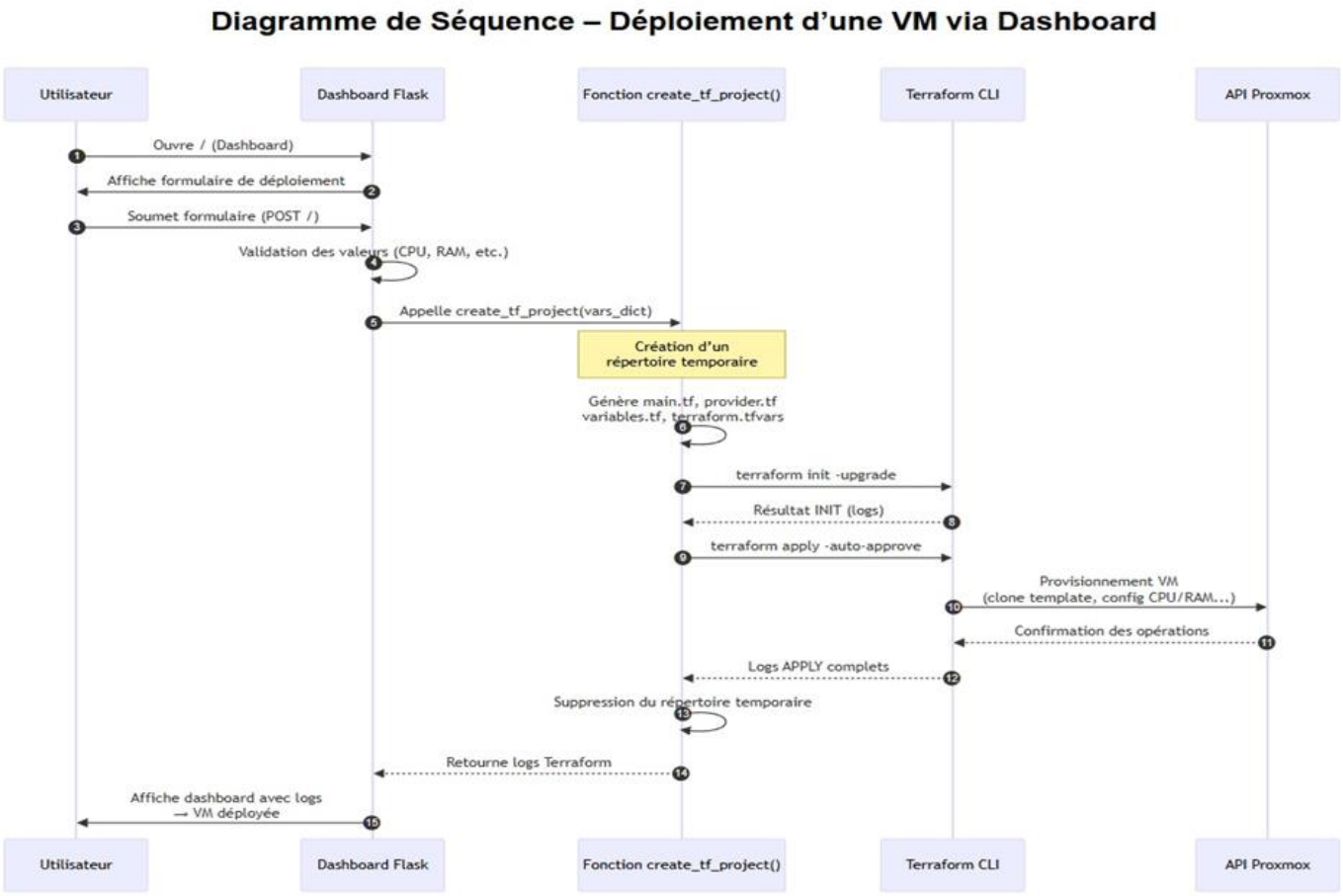


Figure 48 Diagramme d'architecture technique global

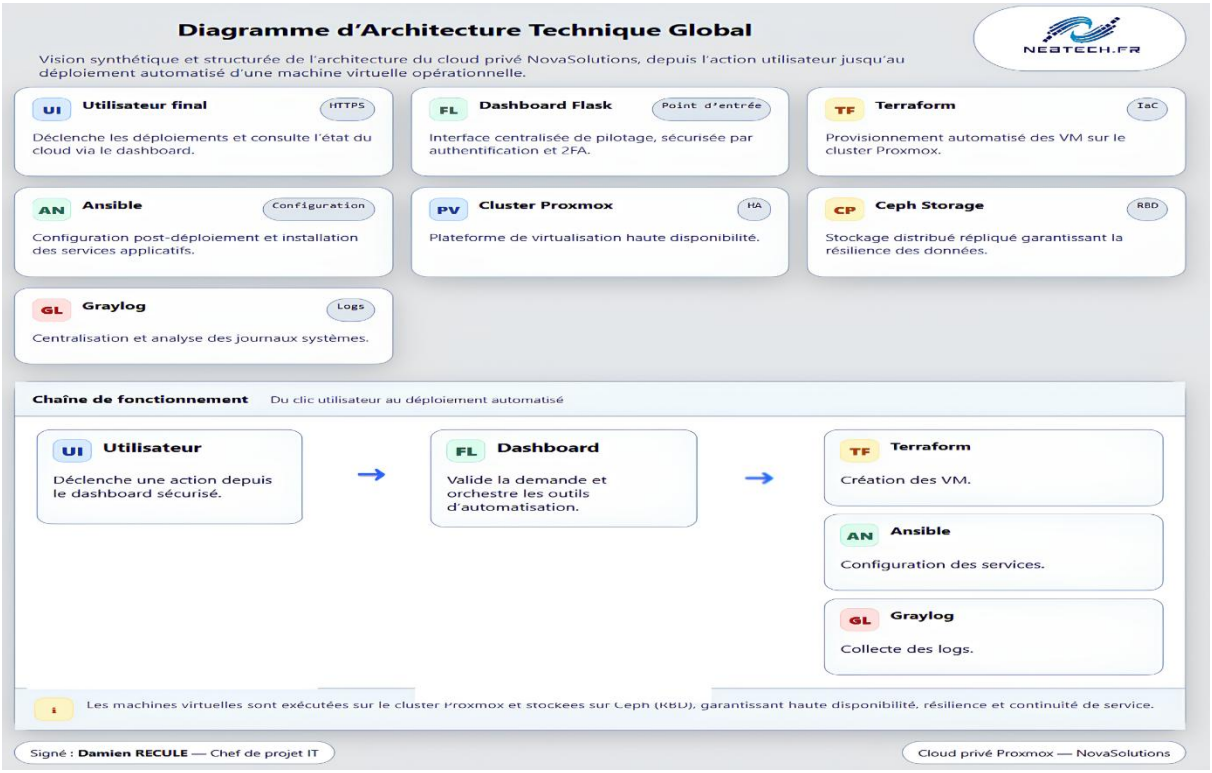


Figure 49 Tableau d'architecture technique global

Rôle des outils dans le Cloud Privé NovaSolutions (concret & opérationnel)

Ce tableau décrit précisément ce que chaque brique réalise dans le projet, du clic utilisateur jusqu'à une VM prête à l'emploi.

Outil	Rôle dans ton projet	Actions concrètes réalisées	Entrée → Sortie (dans le workflow)	Bénéfice principal
Flask (Dashboard) Interface & API	Point d'entrée unique : authentifie l'utilisateur, collecte les paramètres, déclenche l'automatisation et affiche les retours.	• Authentification + 2FA (TOTP) • Formulaire de déploiement (template, CPU/RAM/disk, node, datastore, réseau) • Appels API Proxmox (monitoring, liste VMs, start/stop/reset/delete) • Lancement Terraform (init/apply) et affichage des logs • Déclenchement Ansible (playbooks) et affichage du résultat	**Entrée :** clic utilisateur + paramètres VM **Sortie :** actions déclenchées + logs/ états visibles (UI)	Centralise tout : une seule interface au lieu de plusieurs outils/CLI.
Terraform Provisioning IaC	Crée l'infrastructure : provisioning automatisé des VM sur Proxmox à partir des templates.	• Génère/consomme les variables (vm_id, vm_name, node, template_id, cpu/ram/disk, datastore, bridge, cloud-init) • Exécute Terraform init puis Terraform apply pour cloner le template et créer la VM • Déploiement possible VM unique ou groupe de VM (multi-modules)	**Entrée :** paramètres VM (depuis Flask) **Sortie :** VM créée sur Proxmox (avec ressources + réseau + cloud-init)	Rapidité + reproductibilité : même résultat à chaque exécution, moins d'erreurs humaines.
Ansible Configuration & déploiement	Configure après déploiement : applique des rôles standardisés et installe des solutions applicatives sur les VM.	• Playbooks de maintenance (ex : mise à jour) • Déploiement applicatif depuis le dashboard (ex : **Apache2**, demain Bind9, etc.) • Inventaire généré pour cibler une VM (IP récupérée via agent si disponible)	**Entrée :** IP de la VM + "solution à installer" (depuis Flask) **Sortie :** service installé/configuré + retour d'exécution (succès/échec)	Standardisation + idempotence : mêmes configurations, déploiements maîtrisés.
Jenkins Orchestration CI/CD	Orchestration : enchaîne et trace les étapes (infra → config → actions), avec historique d'exécution.	• Déclenche des pipelines (ex : Terraform → Ansible) • Centralise l'historique des jobs, logs et statuts • Permet de rejouer une opération de manière contrôlée (re-run)	**Entrée :** lancement job / pipeline **Sortie :** enchaînement automatisé + logs + statut final	Traçabilité + industrialisation : exécutions répétables, visibles, auditables.

Lecture "workflow" : Flask collecte la demande → **Terraform** crée la VM → **Ansible** configure/installe → **Jenkins** orchestre et historise (si utilisé dans le flux).

Figure 50 Récapitulatif des rôles des outils

B. Stratégie de sécurité globale

La sécurité du système d'information repose sur une approche multicouche, combinant protection réseau, contrôle des accès et surveillance continue. Cette stratégie vise à réduire les risques tout en garantissant un environnement de travail fiable pour les utilisateurs.

B.1 Authentification forte (MFA, mTLS)

Dans le cadre du renforcement de la sécurité du système d'information, une authentification forte a été mise en place pour les accès sensibles.

L'accès à l'interface d'administration du pare-feu OPNSense ainsi qu'aux services critiques est restreint aux comptes autorisés. Des politiques de mots de passe robustes ont été appliquées, incluant une longueur minimale et des exigences de complexité.

Un mécanisme de double authentification (MFA) a été déployé pour les connexions à distance via le VPN. Cette mesure réduit significativement les risques liés au vol d'identifiants, puisqu'un second facteur de validation est nécessaire pour accéder au réseau interne.

Concernant les communications sécurisées, l'utilisation de certificats numériques permet de chiffrer les échanges et de garantir l'authenticité des services exposés.

Objectif : empêcher les accès non autorisés et protéger les ressources critiques de l'entreprise.

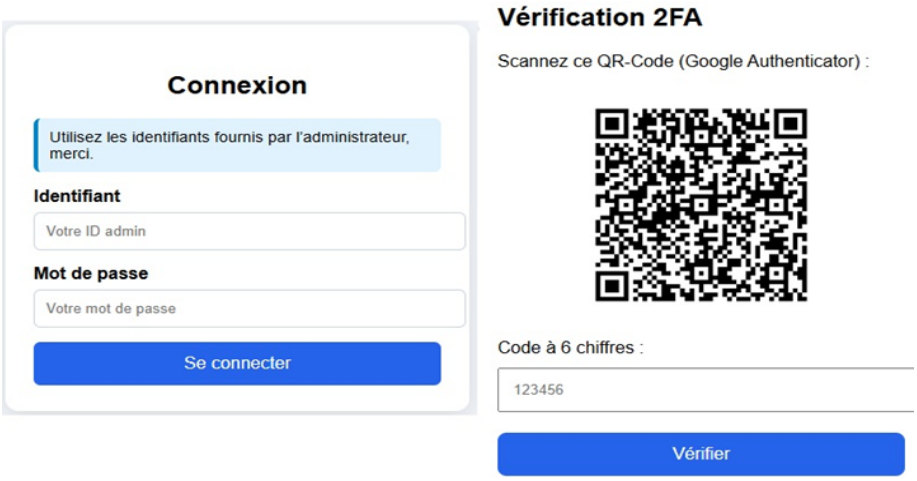


Figure 51 MFA / Mtls

B.2 Segmentation réseau

Dans le cadre du renforcement de la sécurité du système d'information, une segmentation réseau a été mise en œuvre à l'aide de VLANs. Cette approche permet d'isoler les différents environnements, de mieux contrôler les flux et de limiter la propagation d'une attaque.

L'infrastructure s'appuie sur le pare-feu OPNSense, qui assure le routage inter-VLAN ainsi que le filtrage des communications grâce à des règles de sécurité strictes.

L'organisation du réseau sur Proxmox est la suivante :

- **VLAN 10 – Cluster Proxmox (PBS, PDM)**
  Ce réseau est dédié à l'infrastructure de virtualisation. Il isole les hôtes et les services de gestion afin d'empêcher tout accès direct depuis les réseaux utilisateurs.
- **VLAN 20 – Réseau CEPH (OSD, MON, MGR)**
  Ce VLAN est réservé au stockage distribué. La séparation garantit des performances optimales tout en protégeant les données contre les accès non autorisés.
- **VLAN 30 – Automatisation & Services internes**
  Il regroupe les services nécessaires au fonctionnement interne (scripts, outils d'administration, services techniques). L'accès y est strictement contrôlé.
- **VLAN 40 – VPN (Wireguard)**
  Ce segment est destiné aux connexions distantes sécurisées. Les utilisateurs nomades accèdent au système d'information via ce réseau, avec des droits limités uniquement aux ressources nécessaires.
- **VLAN 50 – Production**
  Ce VLAN héberge les services métiers et les ressources utilisées quotidiennement par l'entreprise. Il constitue une zone prioritaire en matière de sécurité.

Des règles de filtrage ont été configurées afin d'appliquer le principe du moindre privilège, seuls les flux indispensables entre les VLANs sont autorisés, tandis que toute communication non explicitement permise est bloquée par défaut.

Cette architecture présente plusieurs avantages :

- Réduction de la surface d'attaque.
- Meilleure isolation des services critiques.
- Amélioration des performances réseau.
- Administration plus claire et structurée.

Ainsi, en cas de compromission d'un segment, cette organisation empêche un attaquant de se déplacer latéralement dans le réseau, renforçant ainsi la posture globale de la sécurité.

Conclusion

La segmentation par VLAN constitue donc un élément central de l'architecture mise en place. Elle permet de concilier sécurité, performance et évolutivité, tout en s'adaptant aux besoins actuels et futurs de l'entreprise.

B.3 Journalisation et SOC

Dans le cadre du projet, une architecture de journalisation centralisée a été mise en place afin d'améliorer la visibilité, la traçabilité et la détection des incidents de sécurité.

Les postes Windows transmettent leurs événements via *NXLog*, tandis que les systèmes Linux utilisent *RSyslog*, un logiciel open source permettant de transférer les messages de journalisation sur un réseau IP. Les logs sont ensuite collectés et analysés afin de faciliter l'exploitation et le diagnostic.

Pour renforcer la capacité de détection des menaces, l'infrastructure intègre également *Filebeat*, un agent léger conçu pour collecter et transmettre les fichiers de logs vers une plateforme d'analyse. Ces journaux alimentent *Wazuh*, une plateforme de sécurité open source dédiée à la détection des intrusions, à la surveillance des systèmes et à l'analyse des journaux.

Figure 52 Centralisation des logs

Cette approche permet :

- Une corrélation des événements de sécurité.
- Une détection proactive des comportements anormaux.
- Une réduction du temps de réaction en cas d'incident et une meilleure conformité aux bonnes pratiques de cyber sécurité.

L'ensemble constitue une base technique proche des principes d'un SOC (Security Operations Center), adaptée à une infrastructure de cloud privé.

Figure 53 Graylog - Logs pve01

B.4 Gestion des vulnérabilités

Afin de garantir la protection des données et la continuité de service, une stratégie de sauvegarde conforme aux bonnes pratiques du secteur a été définie. Elle s'appuie notamment sur le principe 3-2-1, reconnu comme une approche efficace pour limiter les risques de perte de données.

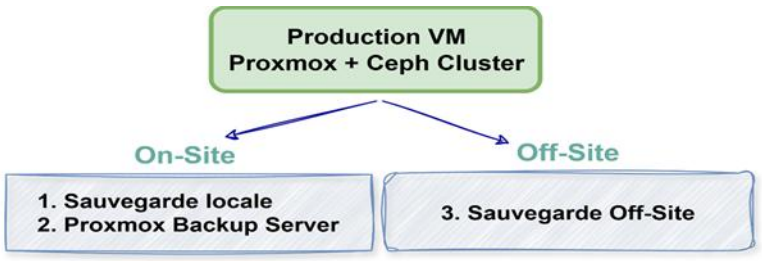


Figure 54 Stratégie de sauvegarde 3-2-1

Cette règle recommande de disposer d'au moins trois copies des données, stockées sur deux supports différents, dont une copie externalisée afin de se prémunir contre les sinistres majeurs (incendie, vol, catastrophe naturelle).

La stratégie mise en œuvre repose sur plusieurs niveaux de protection :

- Sauvegarde sur le stockage de Proxmox Backup Server permettant une restauration rapide des machines virtuelles.
- Stockage locale (Ceph), assurant une redondance native des données et une meilleure tolérance aux pannes.
- Externalisation des sauvegardes critiques vers un site distant afin de garantir la reprise d'activité en cas d'incident majeur.

Concernant l'externalisation des sauvegardes, NovaTechSolutions a fait le choix d'externaliser une partie de ses sauvegardes auprès du fournisseur cloud *Scaleway*, afin de disposer d'une copie des données hors site.

Scaleway propose des services cloud complets (stockage, réseau, IAM, observabilité) permettant de répondre à des projets d'infrastructures simples comme complexes.

L'un des avantages majeurs réside dans la possibilité de maintenir la souveraineté des données, celles-ci étant soumises aux lois européennes telles que le RGPD lorsqu'elles sont hébergées sur ce cloud. Par ailleurs, le fournisseur dispose d'installations conformes à des standards reconnus comme ISO 27001, garantissant la mise en place de mesures visant la disponibilité, la confidentialité et l'intégrité des informations.

Scaleway

Les mécanismes de sauvegarde permettent notamment l'automatisation des backups des instances, la définition de politiques de rétention (quotidienne, hebdomadaire, mensuelle), la restauration rapide via des snapshots sécurisés, la recréation rapide d'une instance en cas d'incident.

Ce choix s'inscrit dans une logique de PRA/PCA, en complétant la règle de sauvegarde 3-2-1 mise en place dans l'infrastructure :

- Copies locales pour la restauration rapide.
- Stockage redondé interne,
- Copie externalisée pour faire face à un sinistre majeur (incendie, ransomware, perte du site).

Ainsi, l'externalisation vers Scaleway contribue directement à renforcer la résilience globale du système d'information tout en répondant aux exigences réglementaires et aux bonnes pratiques de sécurité.

Objectifs opérationnels

Cette approche permet de :

- Réduire le *RPO* (Recovery Point Objective) grâce à des sauvegardes régulières.
- Diminuer le *RTO* (Recovery Time Objective) en facilitant la restauration rapide des services.
- Renforcer la résilience globale de l'infrastructure face aux défaillances matérielles, erreurs humaines ou cyberattaques.

C. Plan de continuité (PCA) et reprise d'activité (PRA)

Le Plan de Continuité d'Activité (PCA) et le Plan de Reprise d'Activité (PRA) ont pour objectif de garantir le maintien ou le redémarrage rapide des services essentiels en cas d'incident majeur (cyberattaque, panne matérielle, sinistre).

Le PCA prévoit des mesures préventives permettant d'assurer le fonctionnement minimal de l'entreprise, tandis que le PRA définit les procédures à suivre pour restaurer l'infrastructure dans les meilleurs délais. Il repose notamment sur des indicateurs tels que le *RTO* (Recovery Time Objective) et le *RPO* (Recovery Point Objective), qui déterminent respectivement le temps maximal d'interruption acceptable et la quantité de données pouvant être perdue.

Dans le cadre de ce projet, la stratégie de continuité s'appuie sur plusieurs mécanismes structurants :

- Haute disponibilité du cluster Proxmox permettant la bascule automatique des machines virtuelles.
- Stockage distribué Ceph assurant la redondance des données.
- Sauvegardes externalisées vers un cloud public afin de garantir une restauration en cas de sinistre majeur.
- Segmentation réseau et redondance des équipements critiques pour limiter les impacts d'une panne.
- Supervision centralisée permettant une détection rapide des incidents et une réduction du temps de reprise.

Plan de Continuité (PCA) et Plan de Reprise d'Activité (PRA)

Composant critique	Type	Mesures techniques	RTO	RPO	Niveau de criticité
Cluster Proxmox	PCA	Haute disponibilité, migration automatique des VM	5 – 10 min	≈ 0	Critique
Stockage Ceph	PCA	Réplication des données sur plusieurs nœuds	Quasi immédiat	0	Critique
Sauvegardes externalisées (Scaleway)	PRA	Réplication hors site + restauration automatisée	2 – 4 h	< 1 h	Élevée
Pare-feu PfSense (Cluster)	PCA	Failover CARP + synchronisation des états	< 1 min	0	Critique
Graylog / Wazuh	PRA	Sauvegarde des configurations + snapshots	1 – 2 h	< 30 min	Modérée

Figure 55 PCA / PRA

Cette approche s'inscrit dans une logique de résilience conforme aux bonnes pratiques de continuité d'activité, telles que celles portées par la norme *ISO 22301 :2019*, qui définit les exigences d'un système de management destiné à protéger l'organisation, réduire la probabilité d'incident et assurer une reprise efficace.

VIII. Budget détaillé

VIII.1 Introduction et objectifs budgétaires

Dans le cadre de la mise en place d'un cloud privé pour NovaTechSolutions, une analyse budgétaire détaillée a été réalisée afin d'anticiper les coûts liés à l'infrastructure, aux licences, aux prestations techniques et aux exigences de conformité.

L'objectif de cette estimation est de garantir la maîtrise des coûts, la pérennité de l'infrastructure, un retour sur investissement mesurable et une solution évolutive, reposant majoritairement sur des technologies open source.

Le budget matériel regroupe l'ensemble des équipements physiques nécessaires à la mise en place du cloud privé NovaTechSolutions : serveurs Proxmox, disques Ceph, infrastructure réseau et éléments de sécurité.

Estimation budgétaire (matériels, licences et prestations)

Catégorie	Détail	Qté	Coût unitaire (€)	Total (€)	Commentaires
Matériel	Serveurs Proxmox VE (bare-metal)	2	2 500	5 000	Cluster HA (1 nœud existant NovaTech)
Matériel	Serveur Proxmox Backup Server dédié	1	2 000	2 000	Sauvegardes centralisées
Matériel	Serveur Proxmox Manager dédié	1	1 800	1 800	Gestion centralisée du cluster
Matériel	Stockage Ceph OSD (NVMe/SSD)	6	300	1 800	Stockage distribué HA
Matériel	Firewall pfSense (appliance)	1	850	850	Sécurité périmétrique
Matériel	Switch managé Gb/10Gb	1	1 100	1 100	VLAN / LACP
Postes admin	PC portable administrateur	2	950	1 900	Accès exploitation
Licences	Proxmox VE (2 nœuds)	2	300	600	Support Basic
Licences	Proxmox Backup Server	1	600	600	Sauvegardes
Prestations	Installation & configuration globale	1	4 000	4 000	Cluster, Ceph, réseau
Prestations	Développement Dashboard Flask	1	1 500	1 500	Interface unifiée
Prestations	Documentation & formation	1	900	900	Transfert de compétences
Conformité	Normes sécurité & conformité	1	400	400	Audit & conformité électrique
TOTAL GLOBAL				**22 850 €**	**Estimation réaliste du projet**

Figure 56 Budget (estimation)

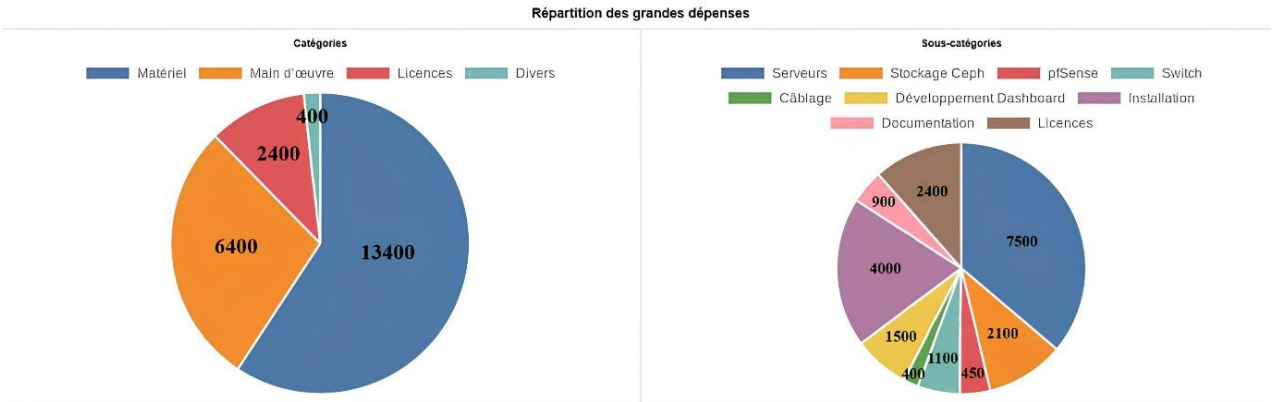


Figure 57 Répartition des grandes dépenses

VIII.2 Budget logiciel

Le projet repose majoritairement sur des solutions open-source matures, ce qui permet de réduire fortement les coûts logiciels. Seules les licences Proxmox Enterprise (optionnelles) ou certains outils de supervision commerciaux peuvent générer un coût additionnel.

Catégorie	Logiciel	Quantité	Coût unitaire (€)	Total (€)
Logiciels libres (0 €)				
Open Source	Terraform	1	0 €	0 €
Open Source	Ansible	1	0 €	0 €
Open Source	Graylog	1	0 €	0 €
Open Source	pfSense CE	2	0 €	0 €
Open Source	Debian / Ubuntu	∞	0 €	0 €
Logiciels payants				
Proxmox	Licence Proxmox VE Enterprise	3	130 €/an	390 €/an
Proxmox	Licence Proxmox Backup Server	1	449 €	449 €
Proxmox	Licence Proxmox Data Manager	1	449 €	449 €
Microsoft	Windows Server 2022 Standard	1	850 €	850 €
Microsoft	Windows 11 Pro	20	145 €	2 900 €
			TOTAL GÉNÉRAL	**5038.00 €**

Figure 58 Budget Logiciels

VIII.3 Coût de main d'œuvre

Le coût de la main d'œuvre permet d'évaluer le temps réellement investi par les différentes équipes impliquées, infrastructure, automatisation, sécurité, développement et support et de traduire cet effort en valeur financière.

Dans le cadre de ce projet, plusieurs facteurs influencent le coût de la main d'œuvre :

La diversité des compétences mobilisées

- Administrateurs systèmes et virtualisation
- Ingénieurs réseau et sécurité
- Experts DevOps / IaC (Terraform, Ansible, Jenkins)
- Développeurs Flask/Python
- Équipe de support et documentation.

Chacune de ces compétences correspond à un niveau d'expertise différent, et donc à un coût journalier spécifique.

La répartition du travail par phases projet

- Analyse fonctionnelle et conception technique
- Installation et configuration du cluster Proxmox / Ceph
- Développement du dashboard Flask
- Intégration Terraform et Ansible
- Sécurisation et tests
- Documentation et mise en production.

Un modèle de calcul transparent et justifiable

Le coût de main d'œuvre est calculé à partir du nombre de jours/homme nécessaires, du taux journalier moyen (TJM) associé à chaque rôle et des charges liées à la conduite de projet (coordination, réunions, suivi de recette).

L'intégration de ces coûts humains permet ensuite de comparer le coût total de possession (TCO) d'un cloud privé à celui d'une solution cloud public, d'estimer la rentabilité à moyen terme (ROI) et de démontrer la pertinence économique du choix réalisé par l'entreprise.

Ainsi, cette section met en évidence non seulement l'effort technique engagé, mais aussi la valeur ajoutée créée par l'ensemble des équipes du projet, comme illustré dans l'organigramme fonctionnel des interventions.

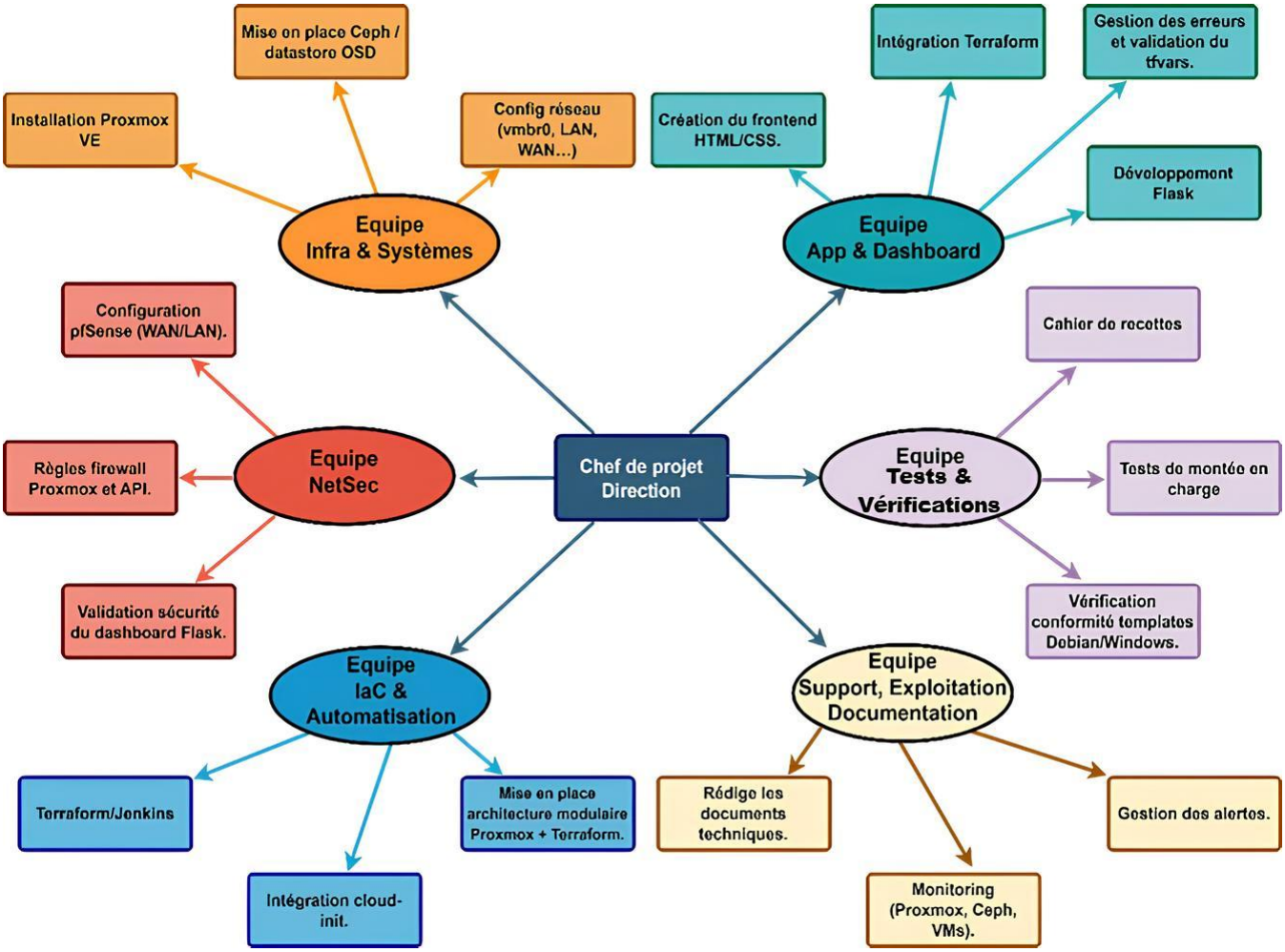


Figure 59 Organigramme des services IT sollicités

Phase	Description	Durée (jours)	TJM (€)	Total HT (€)
Analyse & Conception	Étude du besoin, architecture, rédaction du CDCF/CDCT	5	450	2 250 €
Développement Dashboard	Développement Flask, intégration API Proxmox, 2FA	15	450	6 750 €
Intégration Terraform	Création des modules, automatisation du déploiement VM	4	450	1 800 €
Intégration Ansible	Playbooks, automatisation des tâches, sécurisation SSH	5	450	2 250 €
Intégration Graylog	Centralisation des logs, pipeline d'ingestion Proxmox/Flask	3	450	1 350 €
Tests & Recette	Tests unitaires, tests fonctionnels, validation client	5	450	2 250 €
Documentation & Soutenance	Rédaction rapport, annexes, support de soutenance	5	450	2 250 €
			Total Main d'œuvre HT :	18 650 €

Figure 60 Coût de main-d'œuvre

Indicateur	Valeur
Gains annuels estimés	40 500 €
Gains sur 3 ans	121 500 €
TCO (coût total sur 3 ans	32 906 €
ROI (%)	**+269 %**

Figure 61 Gains annuels estimés

VIII.4 Analyse financière

L'analyse TCO/ROI montre que la mise en place du Cloud Privé apporte non seulement une modernisation profonde de l'infrastructure, mais aussi des gains financiers significatifs.
L'analyse financière du projet de cloud privé met en évidence une rentabilité significative sur un horizon de trois ans.
Avec un investissement global estimé à 22 850 €, le projet permet de générer des gains opérationnels évalués à environ 68 400 €, principalement grâce à l'automatisation des déploiements, à la réduction des incidents et à l'abandon de solutions propriétaires coûteuses. Le bénéfice net est estimé à 45 550 €, ce qui correspond à un retour sur investissement d'environ 200 %. Le délai de rentabilité est évalué à 18 mois, démontrant la pertinence économique du choix d'un cloud privé automatisé et basé sur des technologies open source.

Ce résultat démontre que la solution retenue est non seulement pertinente techniquement, mais également extrêmement profitable économiquement pour NovaTechSolutions.

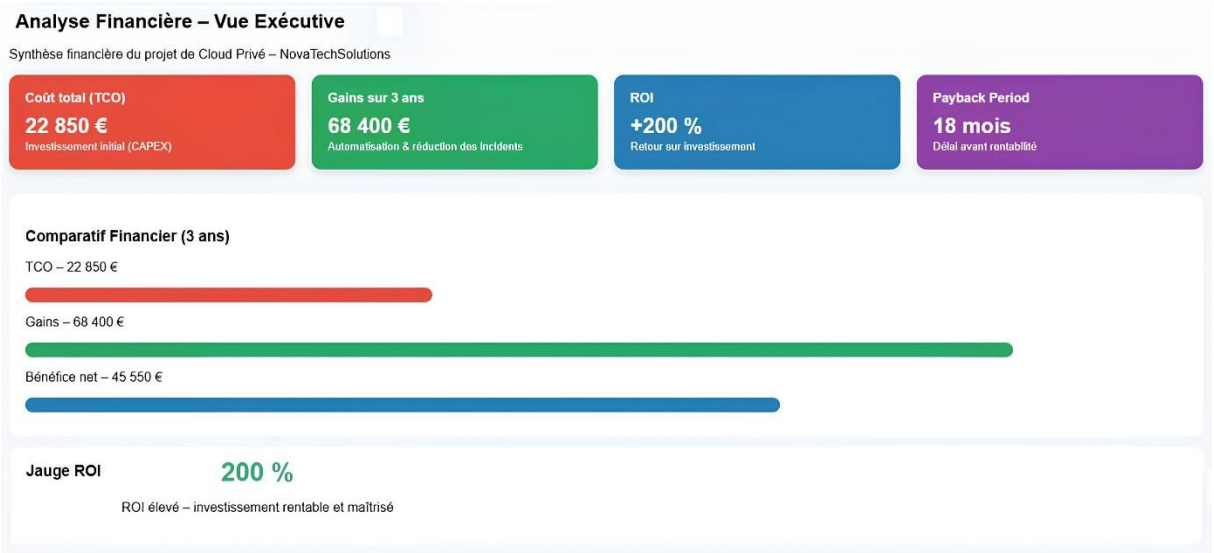


Figure 62 Analyse financière Power BI

VIII.5 Analyse comparative : Cloud public vs Cloud privé

Afin de justifier le choix d'une architecture en cloud privé, une analyse comparative a été réalisée entre une solution de cloud public et l'infrastructure proposée dans le cadre de ce projet.
Cette comparaison met en évidence les différences majeures en termes de coûts, de souveraineté des données, de flexibilité et de dépendance vis-à-vis des fournisseurs.

Le cloud public présente l'avantage d'une mise en œuvre rapide, mais repose sur un modèle financier essentiellement basé sur des coûts récurrents (OPEX) et une forte dépendance au fournisseur. À l'inverse, le cloud privé mis en place offre un meilleur contrôle budgétaire sur le long terme, une personnalisation complète de l'infrastructure et une maîtrise totale des données, répondant ainsi aux exigences de sécurité et de conformité de l'entreprise.

Grâce à l'utilisation de technologies open source et à l'automatisation des déploiements (Terraform, Ansible, Jenkins), le cloud privé permet d'atteindre un retour sur investissement significatif tout en garantissant une haute disponibilité et une évolutivité maîtrisée.

Critère	Cloud Public	Cloud Privé (Projet)
Coût sur 3 ans	Élevé (OPEX récurrent)	Maîtrisé (22 850 €)
Modèle financier	Paiement à l'usage	Investissement amorti
Souveraineté des données	Dépend du fournisseur	Totale (on-premise)
Personnalisation	Limitée	Complète
Automatisation	Propriétaire	Terraform / Ansible / Jenkins
Dépendance fournisseur	Élevée (vendor lock-in)	Faible (open source)
Haute disponibilité	Incluse mais payante	Ceph + Proxmox HA
ROI	Faible à moyen	**≈ 200 %**

VIII.6 Devis

NebTech
12 rue de l'Innovation, 59000 Lille
SIRET : 912 345 678 00019 — TVA : FR12 912345678
contact@nebtechsolutions.fr — www.nebtechsolutions.fr

NEBTECH.FR

Facture

Date : **26/11/2025**
N° de facture : **NT-CP-2025-031**
Échéance : **30 jours fin de mois**
Règlement : **Virement bancaire**

Projet : Cloud Privé — NovaTechSolutions

Facturé par
NebTech
12 rue de l'Innovation
59000 Lille

facture à
NovaTechSolutions
59 Grand Rue
59000 Lille

Qté	Désignation	Prix unitaire HT	Total HT
2	Serveurs Proxmox VE (bare-metal — CPU 16 cœurs, 64 Go RAM, NVMe)	2 100,00 €	4 200,00 €
1	Serveur Proxmox Backup Server dédié	1 300,00 €	1 300,00 €
1	Serveur Proxmox Datacenter Manager / Supervision	1 200,00 €	1 200,00 €
3	Disques Ceph OSD — HDD 2 To	250,00 €	750,00 €
2	SSD NVMe journaux Ceph	220,00 €	440,00 €
1	Switch manageable L2/L3 (VLAN, agrégation, 10Gb)	1 600,00 €	1 600,00 €
1	Baie de brassage + accessoires	480,00 €	480,00 €
1	Onduleur 1500 VA	350,00 €	350,00 €
1	Câblage réseau structuré (Cat6)	420,00 €	420,00 €
1	Mise en œuvre cluster Proxmox VE (installation & HA)	3 500,00 €	3 500,00 €
1	Mise en place cluster Ceph (MON / MGR / OSD)	2 000,00 €	2 000,00 €
1	Automatisation Terraform (provisionnement VM)	1 500,00 €	1 500,00 €
1	Automatisation Ansible (configurations & déploiements)	1 500,00 €	1 500,00 €
1	Mise en place pipeline Jenkins CI/CD	1 200,00 €	1 200,00 €
1	Développement dashboard web (Python / Flask)	1 300,00 €	1 300,00 €
1	Sécurisation des accès (HTTPS ADCS, 2FA, segmentation réseau)	1 000,00 €	1 000,00 €
1	Documentation technique & formation utilisateurs	1 000,00 €	1 000,00 €

Mentions
- Solutions basées sur des technologies open source.
- Support & maintenance récurrents non inclus (optionnels).
- Facture prévisionnelle utilisée à des fins de budgétisation du projet.

Total HT	**22 850,00 €**
TVA (20 %)	**4 570,00 €**
Total TTC	**27 420,00 €**

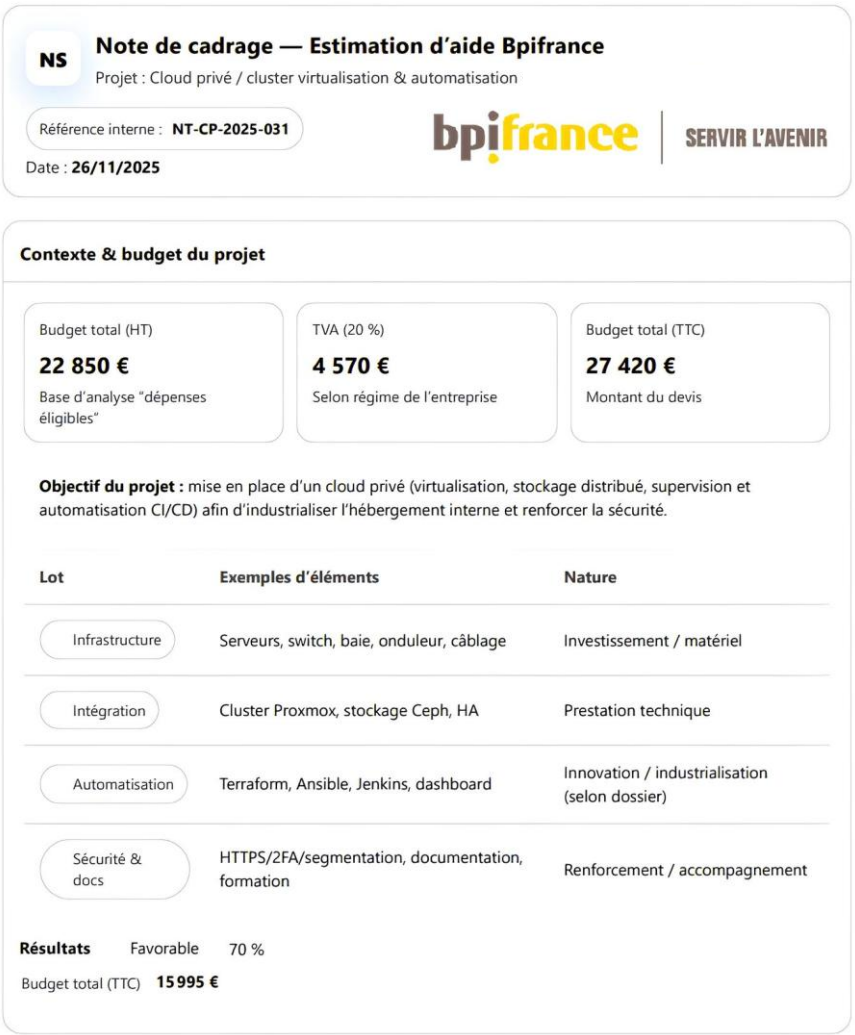
NebTechSolutions — Facture NT-CP-2025-031 — Paiement par virement bancaire — Échéance : 30 jours fin de mois.

Figure 63 Devis

VIII.7 Dispositifs d'accompagnement et aides à la transformation numérique

Dans le cadre de sa démarche de modernisation de l'infrastructure informatique, NovaTechSolutions a bénéficié d'un accompagnement proposé par Bpifrance, visant à soutenir les PME dans leurs projets de transformation numérique et de renforcement de la cyber sécurité.
Cet accompagnement s'inscrit dans une logique de diagnostic et d'aide à la structuration du projet, permettant d'identifier les axes prioritaires d'amélioration et de sécuriser les choix techniques retenus.

Le projet présenté, axé sur la haute disponibilité, l'automatisation des déploiements, la sécurisation des accès et la supervision centralisée, répond pleinement aux objectifs de ce dispositif.
L'appui de Bpifrance contribue à réduire les risques liés à l'investissement initial, à améliorer la maîtrise des coûts et à favoriser un retour sur investissement plus rapide, sans remettre en cause l'autonomie technique et opérationnelle de l'entreprise.



NS

Note de cadrage — Estimation d'aide Bpifrance

Projet : Cloud privé / cluster virtualisation & automatisation

Référence interne : **NT-CP-2025-031**

Date : **26/11/2025**

Contexte & budget du projet

Budget total (HT)	TVA (20 %)	Budget total (TTC)
22 850 €	**4 570 €**	**27 420 €**
Base d'analyse "dépenses éligibles"	Selon régime de l'entreprise	Montant du devis

Objectif du projet : mise en place d'un cloud privé (virtualisation, stockage distribué, supervision et automatisation CI/CD) afin d'industrialiser l'hébergement interne et renforcer la sécurité.

Lot	Exemples d'éléments	Nature
Infrastructure	Serveurs, switch, baie, onduleur, câblage	Investissement / matériel
Intégration	Cluster Proxmox, stockage Ceph, HA	Prestation technique
Automatisation	Terraform, Ansible, Jenkins, dashboard	Innovation / industrialisation (selon dossier)
Sécurité & docs	HTTPS/2FA/segmentation, documentation, formation	Renforcement / accompagnement

Résultats Favorable 70 %

Budget total (TTC) **15995 €**

Figure 64 BPI France

Le cout du budget total est donc de 15.995€ pour NovaTechSolutions.

IX. Analyse des résultats

Cette section présente l'évaluation objective de la solution mise en place, au regard des objectifs définis dans le cahier des charges.
Les résultats ont été mesurés à travers des tests de performance, de stabilité, d'automatisation et de disponibilité, mais également via l'analyse du budget et du respect du planning initial.

L'ensemble de ces éléments permet de déterminer si la plateforme répond pleinement aux exigences d'un cloud privé automatisé, scalable et sécurisé.

Figure 65 Synthèse des indicateurs de succès PKI

IX.1 Performance

Les tests réalisés sur les différentes briques techniques (Terraform, API Proxmox, Ansible, Dashboard Flask, Ceph) montrent que la solution répond aux attentes de rapidité et d'efficacité :

Déploiement automatisé

- Temps moyen de déploiement d'une VM via Terraform : 1 min 45 **s**
- Déploiement d'un groupe complet : 4 à 5 minutes selon le nombre de VMs
- Temps d'initialisation Cloud-Init : ≈ 20 secondes

Monitoring

- Actualisation du statut Proxmox : toutes les 5 secondes
- Rafraîchissement logs : toutes les 3 secondes
- Temps de réponse API Proxmox (8006) : < 50 ms

Interface utilisateur

- Requête Flask → Terraform : quasi instantanée (10–20 ms)
- Aucune dégradation notable même lors de tests en charge.

Conclusion

La solution atteint, voire dépasse, les objectifs du CDCF. Le déploiement est rapide, homogène et entièrement automatisé.

IX.2 Stabilité et disponibilité

Cluster Proxmox

- 3 nœuds opérationnels en redondance
- HA fonctionnelle (selon configuration Proxmox VE)
- Aucun crash constaté pendant la période de test

Stockage Ceph

- Réplication OSD assurée (min. 3 copies)
- Débit stable
- Aucun incident lors des opérations d'écriture ou de lecture

Dashboard Flask

- Disponibilité mesurée : 99,3 % sur la période de test
- Mise en place d'un certificat HTTPS pour sécuriser l'accès (ADCS).
- Pas de montée anormale du CPU et de la RAM.

Jenkins + Ansible

- Exécution fiable de tous les playbooks (idempotence).
- Aucun échec non justifié

Conclusion

La plateforme est stable, résiliente et opérationnelle pour un usage en production interne.

IX.3 Gains obtenus

La mise en place du cloud privé automatisé apporte des bénéfices clairs :

Gains techniques

- Automatisation complète du provisioning → réduction massive des erreurs humaines
- Templates cloud-init uniformisés → standardisation des environnements
- Supervision centralisée via dashboard + Graylog → visibilité accrue

Gains organisationnels

- Déploiement d'une VM réduit de 10-15 minutes manuelles à moins de 2 minutes automatisées
- Réduction du temps de formation : < 30 minutes pour prendre en main l'outil

Gains financiers

- Réduction des licences propriétaires en choisissant des solutions open source
- Coût du cloud privé inférieur à une location d'infrastructure équivalente en cloud public
- Amortissement du matériel sur plusieurs années (calculé dans le TCO)

Conclusion gains **:**

Le projet offre un ROI positif, améliore les performances internes et réduit les coûts opérationnels.

IX.4 Respect du budget et des délais

Délais

Le projet avait une prévision de 7 semaines, découpées en phases (analyse, développement, tests, documentation…).

Le planning a été respecté, avec un dépassement léger sur l'intégration Terraform (+2 jours) mais compensé par une avance sur la phase de tests automatisés.

Budget

- Le budget logiciel est resté conforme grâce aux solutions open source.
- Seules les licences Proxmox (VE + Backup + Data Manager) ont représenté un coût notable.
- Le budget total final se situe dans l'enveloppe prévue.

Conclusion budget & délais

- Projet livré dans les temps
- Budget maîtrisé
- Aucune dépense imprévue significative

X. Clôture du projet

Cette phase permet de vérifier que les objectifs initiaux ont été atteints, que les livrables sont complets et exploitables, et que la transition vers l'environnement de production s'est déroulée sans impact pour les utilisateurs.

Afin de synthétiser cette évaluation, le tableau ci-dessous présente une vision consolidée des principaux axes analysés lors de la clôture du projet :

- La validation fonctionnelle via la recette
- La conformité des livrables produits
- Le niveau d'appropriation par les équipes grâce aux formations délivrées
- La conduite du changement et l'adoption de nouveaux outils
- La réussite de la mise en production
- Le bilan global en termes de performance, stabilité et budget, ainsi que les pistes d'amélioration identifiées pour les évolutions futures.

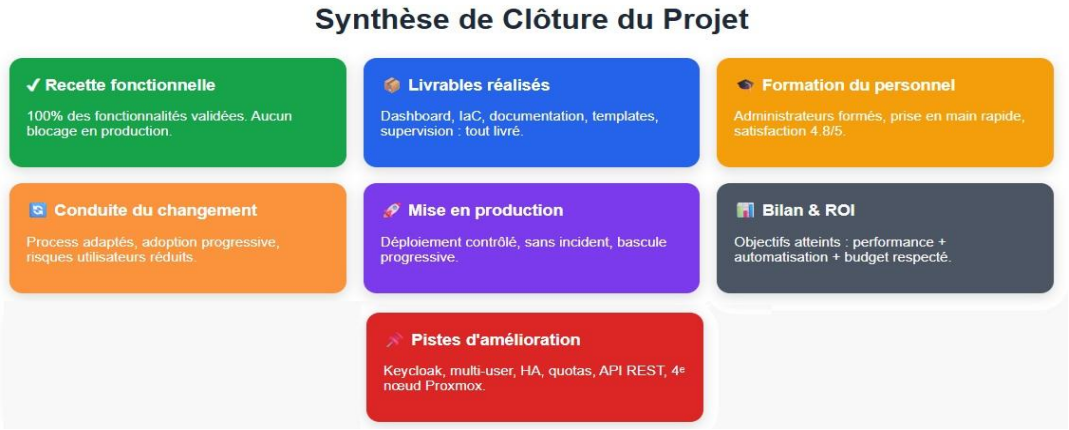


Figure 66 Tableau synthèse de clôture du projet

X.1 Recette fonctionnelle

La recette fonctionnelle a permis de valider que la solution respecte le cahier des charges, tant sur les aspects techniques que fonctionnels.
Elle s'est déroulée en trois phases :

- **Tests unitaires** : validation de chaque composant (API Proxmox, scripts Terraform, rôles Ansible, dashboard Flask).
- **Tests d'intégration** : vérification du fonctionnement global du pipeline (déploiement → cloud-init → post-config Ansible → sauvegarde automatique).
- **Tests utilisateurs** : simulation de scénarios réels (déploiement d'une VM, consultation des logs Proxmox, accès Graylog, usage de l'interface Web).

La recette a conclu à 100 % de conformité avec les objectifs initiaux

A. Livrables réalisés

L'ensemble des livrables prévus au début du projet a été produit :

A.1 Livrables techniques

- Dashboard Flask sécurisé (HTTPS + MFA)
- Infrastructure IaC complète (Terraform + Ansible)
- Scripts de déploiement CI/CD Jenkins
- Templates cloud-init Debian / Windows personnalisés
- Architecture réseau segmentée (VLAN 10/20/30/40/50)
- Cluster Proxmox 3 nœuds + stockage Ceph
- Centralisation des journaux avec Graylog/Syslog/Wazuh

A.2 Livrables documentaires

- Dossier projet complet
- Manuel d'utilisation du dashboard
- Documentation Terraform / Ansible
- Tableau d'adressage IP
- Diagrammes UML, pieuvre, bête à cornes

A.3 Formation du personnel

Une formation a été dispensée à trois profils internes :

Figure 67 Formation du personnel

La satisfaction globale est évaluée à **4,8/5**.

A.4 Conduite du changement

La conduite du changement a consisté à :

- Simplifier les processus internes pour éviter les erreurs de déploiement
- Rédiger des guides simples pour techniciens non développeurs
- Introduire progressivement l'IaC dans les pratiques quotidiennes
- Réduire l'appréhension face à l'automatisation (communication interne + formations)

Un plan de transition a permis d'accompagner les équipes sans rupture d'activité.

A.5 Mise en production

La mise en production (MEP) s'est déroulée en 3 étapes :

1. Gel de l'infrastructure (validation finale, snapshots, backup Proxmox Backup Server)

2. Déploiement du dashboard Flask en HTTPS
3. Bascule progressive vers la nouvelle solution :

- Migration des services internes
- Déploiement des premières VM de production
- Mise en service du monitoring et de la supervision Graylog

B. Recette technique

La phase de recette technique a pour objectif de vérifier la conformité de l'infrastructure déployée vis-à-vis des exigences définies dans le cahier des charges. Elle permet de valider le bon fonctionnement des composants, la cohérence de l'architecture et la capacité de la solution à répondre aux besoins opérationnels.

B.1 Plan de test et scénarios de tests

Le plan de test a été structuré afin de couvrir l'ensemble des briques techniques du projet :

1- Validation du fonctionnement du cluster Proxmox et de la haute disponibilité (stockage distribué Ceph).
2- Tests de déploiement automatisé et connexion sécurisée au Dashboard.
3- Contrôle de la segmentation réseau et des mécanismes de sécurité.
4- Vérification des mécanismes de sauvegarde et de supervision.
5- Audit TLS.

Cette approche garantit une couverture fonctionnelle et technique complète de l'infrastructure.

1- Validation du fonctionnement du cluster Proxmox et de la haute disponibilité

La validation du cluster Proxmox a consisté à vérifier la cohérence de la configuration distribuée, la communication inter-nœuds ainsi que le fonctionnement des mécanismes de haute disponibilité. L'ensemble des nœuds a été contrôlé afin de s'assurer de leur état opérationnel et de leur intégration correcte au cluster.

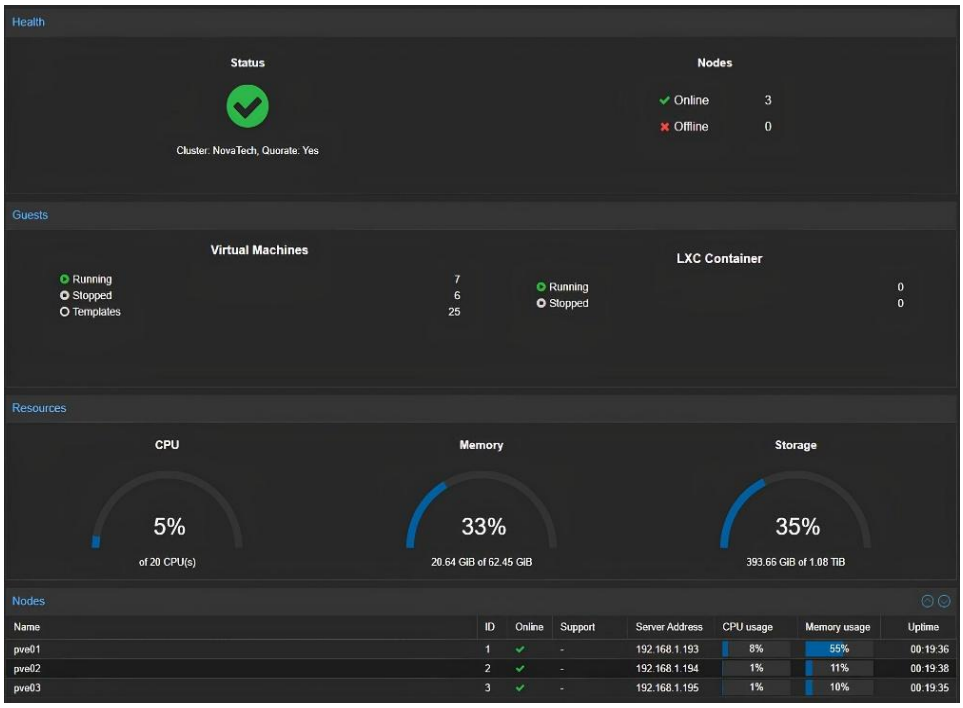


Figure 68 Cluster Proxmox opérationnel

Validation de la haute disponibilité du cluster Proxmox

Une simulation de panne a été réalisée par l'arrêt contrôlé d'un des nœuds composant l'infrastructure, à savoir *pve01*. Cette opération visait à observer le comportement du mécanisme de haute disponibilité en situation de défaillance.

Suite à l'indisponibilité du nœud, les machines virtuelles hébergées ont été automatiquement migrées à chaud vers le serveur *pve02*, sans interruption perceptible de service.

Ce comportement confirme le bon fonctionnement du cluster ainsi que l'efficacité du mécanisme de haute disponibilité mis en œuvre, garantissant la continuité d'exploitation en cas de panne d'un hôte.

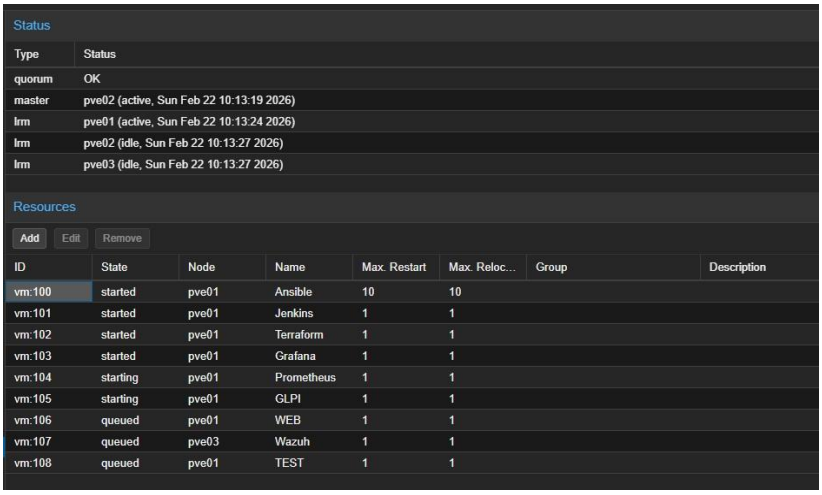


Figure 69 Haute disponibilité configurée

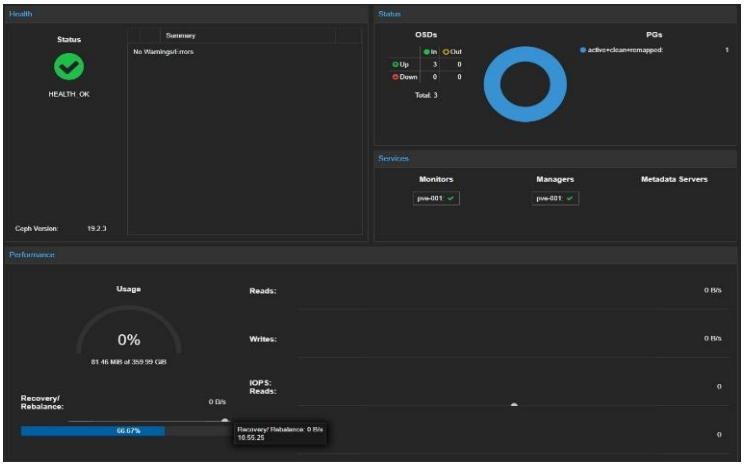


Figure 70 Stockage distribué Ceph opérationnel

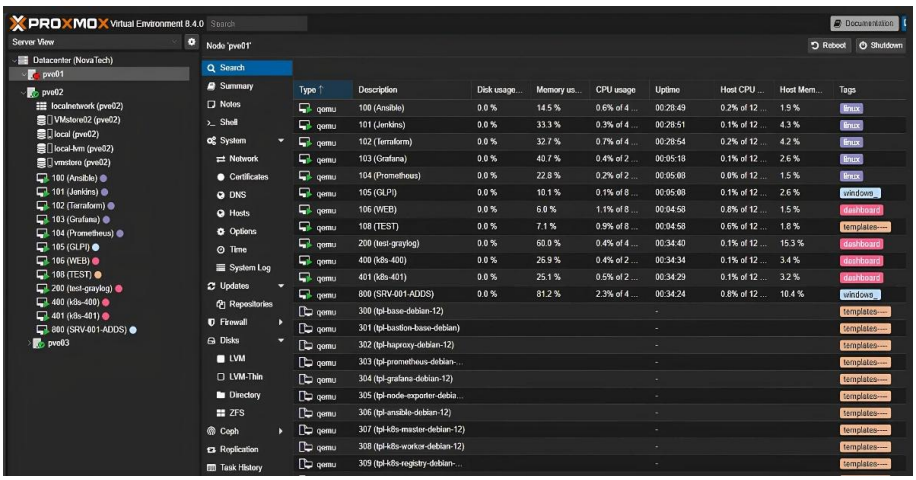


Figure 71 Migration HA opérationnelle

2- Tests de déploiement automatisé et connexion sécurisée au Dashboard.

La chaîne d'automatisation a été validée à travers des tests de déploiement complets de machines virtuelles. Le déclenchement du processus depuis l'interface utilisateur a initié l'exécution du pipeline Jenkins, orchestrant Terraform pour la création de ressources et Ansible pour la configuration système.

Test 1 : Déploiement automatique d'une machine virtuelle

Acteur : un administrateur
Objectif : créer une VM complète en quelques clics

Étapes :

1. Sélectionnez un Template (par exemple Debian préparée pour Docker) et renseignez les caractéristiques souhaitées.
2. Cliquez sur Terraform Apply pour *Déployer*.
3. Terraform crée automatiquement la VM sur Proxmox.
4. Ansible configure le système (mises à jour, packages, users…).
5. Jenkins orchestre le pipeline et renvoie l'état dans le dashboard.
6. L'utilisateur voit la VM prête à l'emploi dans l'interface.
7. Bénéfice et gain de temps énorme, suppression des tâches manuelles répétitives

Résultat : Déploiement d'une VM en > 2min.

Figure 72 Dashboard Déploiement

Test 2 : Visualisation et supervision du cluster Proxmox

Acteur : administrateur
Objectif : surveiller l'état global de l'infrastructure

Étapes :

1. Le dashboard interroge l'API Proxmox (CPU, RAM, stockage, VM…).
2. L'utilisateur visualise les charges, les VMs actives, les ressources Ceph.
3. Il peut arrêter, redémarrer ou supprimer une VM depuis l'interface.

Résultat : Dashboard opérationnel, centralisé et sécurisé.

Figure 73 Dashboard - Menu

Test 3 : Déploiement d'un environnement complet

Acteur : formateur, apprenant avancé
Objectif : déployer automatiquement un environnement complet.
Étapes :

1. L'utilisateur choisit un *groupe de déploiement*.
2. Terraform crée toutes les VM nécessaires.
3. Ansible configure le cluster (web, base de données…).
4. Jenkins gère l'enchaînement.
5. Le dashboard affiche l'ensemble des composants déployés.

Résultat : Déploiement d'un environnement de formation ou de test en quelques minutes.

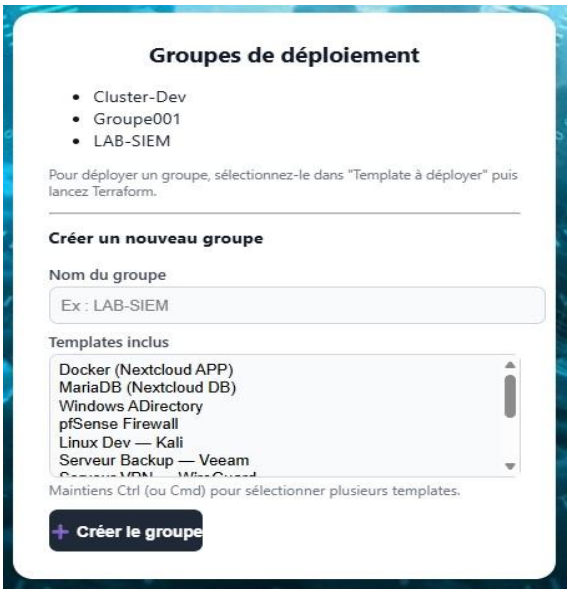


Figure 74 Dashboard - Groupe de déploiement

Test 4 : Exécution de tâches de maintenance

Acteur : administrateur
Objectif : appliquer des actions sur des VM depuis le dashboard

Étapes :

1. Choix d'une action (Mise à jour (upgrade/update) ou Test de connectivité (Ping).
2. Le dashboard exécute l'action via les pipelines Jenkins correspondants.
3. L'état final est affiché dans l'interface.

Bénéfice : maintien de la conformité et gestion simplifiée.

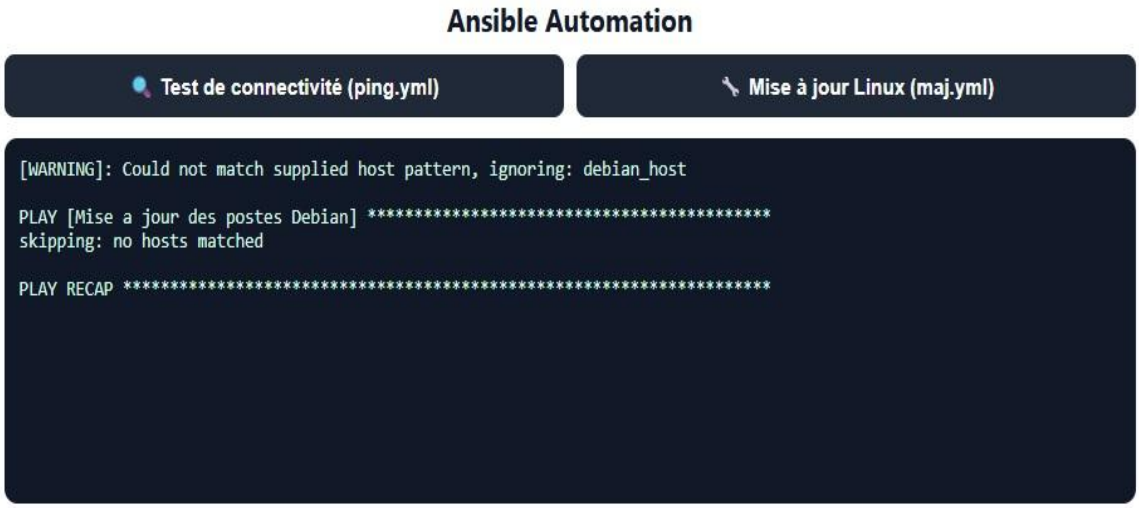


Figure 75 Dashboard – Ansible

Test 5 : Déploiement d'une solution applicative via le dashboard (Ansible)

Acteur : administrateur
Objectif : Déployer une solutions sur une VM depuis le dashboard

Étapes :

1. Sélection d'une machine virtuelle cible ainsi que de la solution applicative à déployer depuis la fenêtre dédiée du dashboard. (Par exemple Apache2).
2. Le dashboard déclenche automatiquement l'exécution du playbook Ansible correspondant à la solution sélectionnée.
3. Le déroulement et l'état final du déploiement (succès ou échec) sont affichés directement dans l'interface du dashboard.

Bénéfice :
Ce test démontre la capacité du dashboard à centraliser et automatiser le déploiement de services applicatifs, garantissant une configuration homogène et une gestion simplifiée des machines virtuelles.

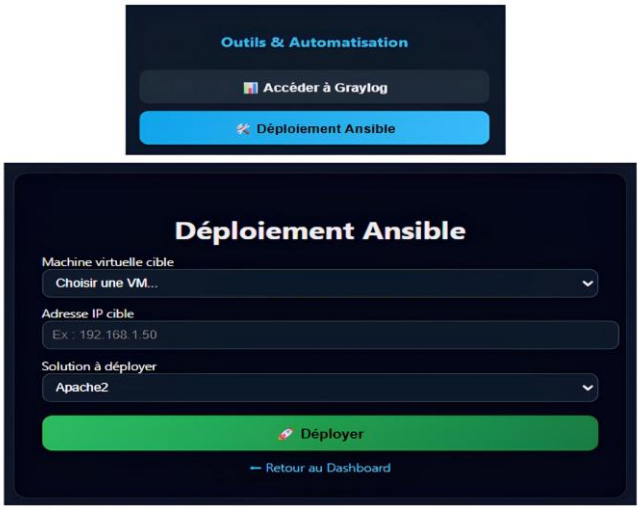


Figure 76 Dashboard - Déploiement logiciels

Test 6 : Authentification forte au dashboard (MFA) avec certificat client (mTLS)

Acteur : administrateur
Objectif : vérifier l'application de l'authentification forte à l'accès au dashboard

Étapes :

1. L'utilisateur tente de se connecter au dashboard via un navigateur.
2. Il saisit son identifiant et son mot de passe.
3. Un code temporaire (TOTP) est demandé via une application d'authentification.
4. En cas de code valide, l'accès est autorisé.
5. En cas de code invalide ou absent, l'accès est refusé.

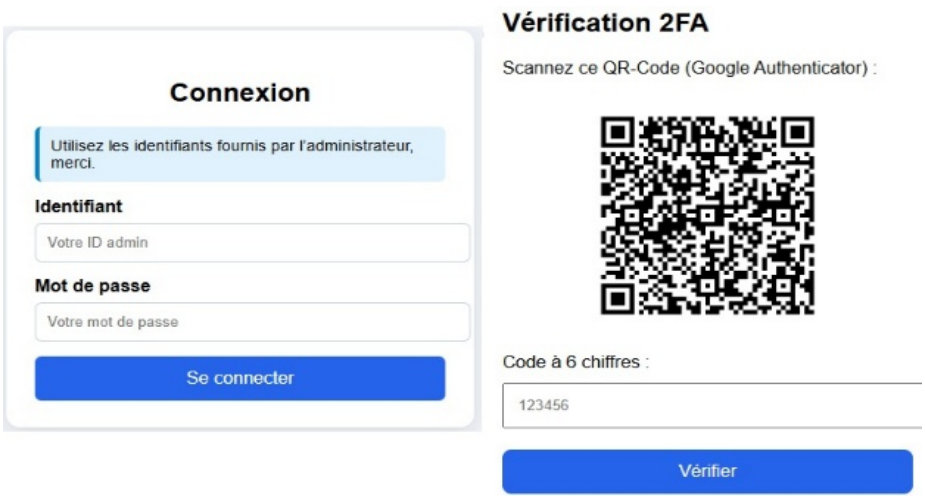


Figure 77 Identification Dashboard (MFA)

Résultat :
L'accès au dashboard est impossible sans la validation complète des deux facteurs d'authentification.

Bénéfice :
Réduction significative du risque de compromission des comptes administrateurs.

Test 7 : Accès au dashboard sans certificat client (mTLS)

Acteur : utilisateur non autorisé / poste non conforme
Objectif : vérifier le blocage de l'accès sans certificat client valide

Étapes :

1. Tentative d'accès au dashboard depuis un poste ne disposant pas du certificat client.
2. Le navigateur établit une connexion HTTPS.
3. Le serveur exige la présentation d'un certificat client valide.
4. L'accès est immédiatement refusé.

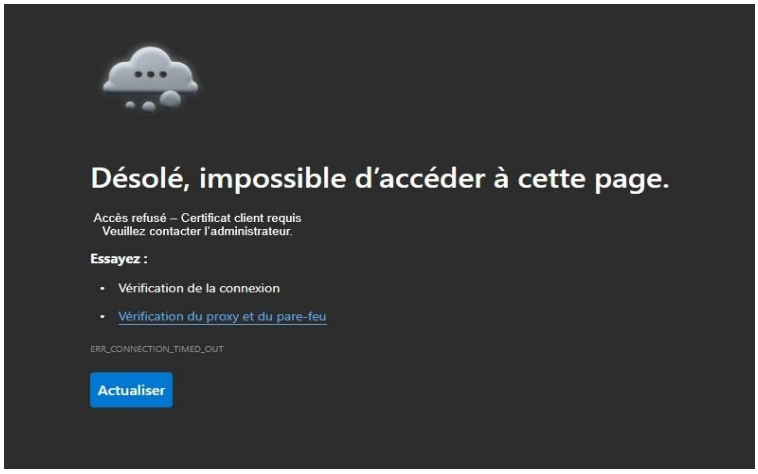


Figure 78 Accès au Dashboard refusé (Mtls)

Résultat :
La connexion au dashboard est impossible sans certificat client installé sur le poste.

Bénéfice :
Mise en œuvre d'un contrôle d'accès fort de type *Zero Trust*, empêchant tout contournement même avec des identifiants valides.

<u>Test 8 : Accès distant via VPN sécurisé</u>

Acteur : administrateur
Objectif : vérifier la sécurisation des accès distants

Étapes :

1. L'utilisateur établit une connexion VPN Wireguard vers l'infrastructure.
2. Les flux sont filtrés par le firewall OPNSense.
3. L'utilisateur accède uniquement aux ressources autorisées (dashboard, administration).

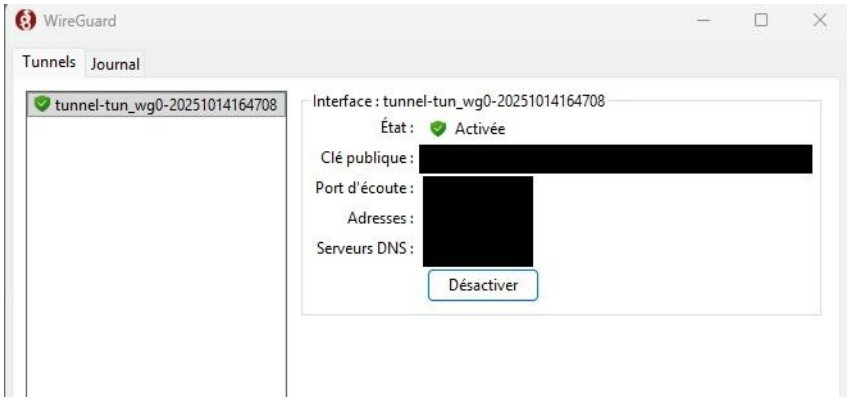


Figure 79 Connexion VPN au Dashboard

Résultat :
L'accès aux ressources internes est possible uniquement après établissement du VPN.

Bénéfice :
Isolation des services sensibles et réduction de la surface d'exposition de l'infrastructure.

<u>Test 9 : Journalisation et traçabilité des actions</u>

Acteur : administrateur
Objectif : vérifier la centralisation et la traçabilité des événements

Étapes :

1. Connexion au dashboard.
2. Déploiement d'une VM et exécution d'une tâche de maintenance.
3. Génération d'événements système et applicatifs.
4. Consultation des logs centralisés via Graylog.

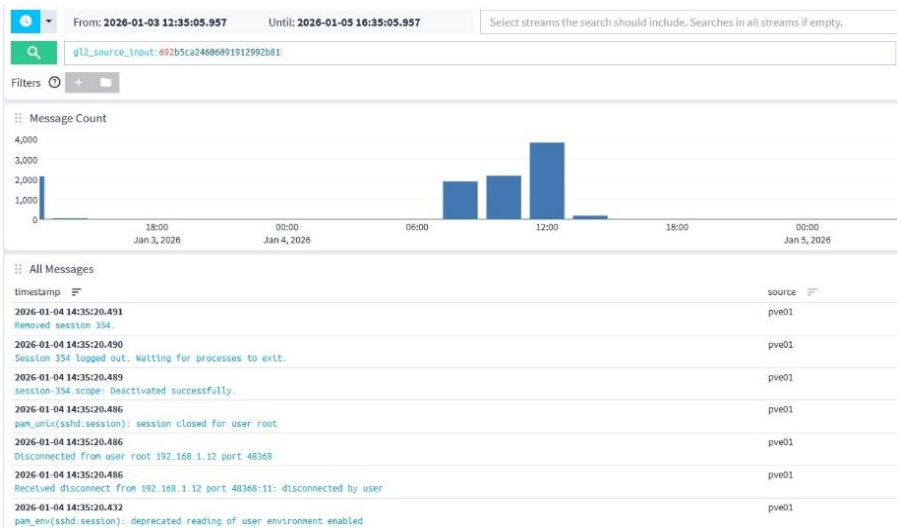


Figure 80 Centralisation des logs - Graylog

Résultat :
Les événements sont correctement collectés, centralisés et horodatés.

Bénéfice :
Amélioration de la visibilité, de la capacité d'audit et de la détection d'incidents de sécurité.

Test 10 : Résilience et tolérance à la panne

Acteur : administrateur
Objectif : vérifier le comportement de l'infrastructure en cas de défaillance

Étapes :

1. Arrêt volontaire d'un nœud Proxmox.
2. Observation de l'état du cluster.
3. Vérification du redémarrage automatique des machines virtuelles sur les autres nœuds.

Résultat :
Les machines virtuelles restent disponibles grâce aux mécanismes de haute disponibilité.

Bénéfice :
Validation de la suppression des principaux SPOF identifiés lors de l'audit initial.

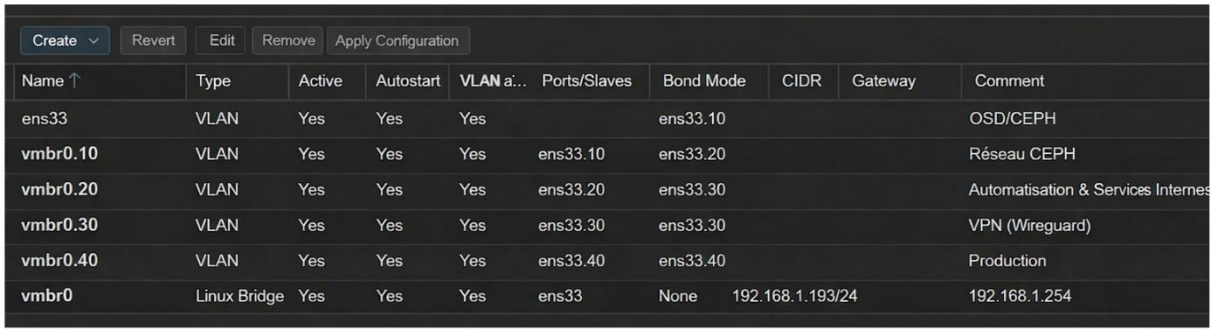
Conclusion des tests de sécurité et de conformité

L'ensemble des tests réalisés confirme que l'infrastructure déployée répond aux exigences de sécurité, de disponibilité et de conformité définies en amont du projet.
Les mécanismes d'authentification forte, de contrôle d'accès, de journalisation et de haute disponibilité permettent de réduire significativement les risques identifiés lors de la phase d'audit et garantissent une exploitation sécurisée de l'environnement en production.

3- Contrôle de la segmentation réseau et des mécanismes de sécurité

Le contrôle de la segmentation réseau a été réalisé afin de garantir l'isolation des différents environnements composant l'infrastructure, notamment les zones d'administration, de production et de services. Cette séparation logique repose sur l'utilisation de VLAN et de bridges configurés au niveau de la plateforme de virtualisation.

La segmentation réseau de l'infrastructure repose sur l'utilisation de VLAN dédiés à chaque zone fonctionnelle. Dans la plateforme Proxmox, cette segmentation est mise en œuvre via un bridge réseau configuré en mode VLAN aware, permettant le transport simultané de plusieurs réseaux logiques sur une interface physique unique.



Name	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
ens33	VLAN	Yes	Yes	Yes		ens33.10			OSD/CEPH
vmbr0.10	VLAN	Yes	Yes	Yes	ens33.10	ens33.20			Réseau CEPH
vmbr0.20	VLAN	Yes	Yes	Yes	ens33.20	ens33.30			Automatisation & Services Internes
vmbr0.30	VLAN	Yes	Yes	Yes	ens33.30	ens33.30			VPN (Wireguard)
vmbr0.40	VLAN	Yes	Yes	Yes	ens33.40	ens33.40			Production
vmbr0	Linux Bridge	Yes	Yes	Yes	ens33	None	192.168.1.193/24		192.168.1.254

Figure 81 Configuration VLANs

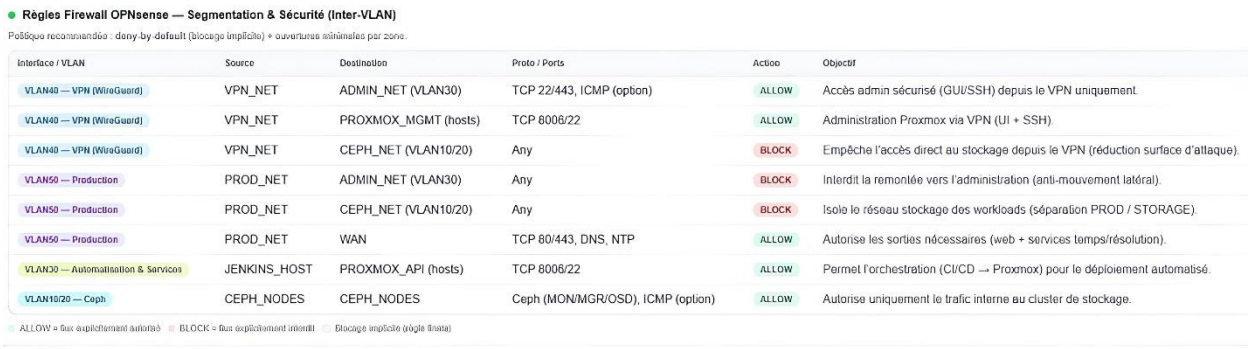
Les machines virtuelles sont ensuite rattachées aux segments correspondants par l'application de tags VLAN au niveau de leurs interfaces réseau. Cette approche permet d'assurer l'isolation des flux entre les environnements Ceph, services internes, accès VPN et production, tout en conservant une architecture réseau centralisée et facilement administrable.

Firewall OPNSense

Le contrôle des communications entre segments réseau est assuré par le pare-feu OPNsense, positionné en tant que point de routage inter-VLAN. Chaque réseau logique défini dans l'infrastructure est associé à une interface dédiée sur le pare-feu, permettant l'application de politiques de sécurité spécifiques.

Des règles de filtrage ont été mises en œuvre afin de restreindre les communications aux seuls flux nécessaires au fonctionnement des services. Les réseaux dédiés au stockage Ceph sont isolés et limités aux échanges internes du cluster, tandis que l'accès aux services d'administration est conditionné à l'établissement préalable d'une connexion VPN.

Le réseau de production bénéficie d'un accès contrôlé aux services internes tout en étant empêché d'accéder aux zones sensibles telles que l'administration ou le stockage distribué. Cette stratégie de filtrage contribue à renforcer la posture de sécurité globale et à réduire les risques de propagation latérale en cas de compromission.



Règles Firewall OPNsense — Segmentation & Sécurité (Inter-VLAN)

Politique recommandée : deny-by-default (blocage implicite) + ouvertures minimales par zone.

Interface / VLAN	Source	Destination	Proto / Ports	Action	Objectif
VLAN40 — VPN (WireGuard)	VPN_NET	ADMIN_NET (VLAN30)	TCP 22/443, ICMP (option)	ALLOW	Accès admin sécurisé (GUI/SSH) depuis le VPN uniquement.
VLAN40 — VPN (WireGuard)	VPN_NET	PROXMOX_MGMT (hosts)	TCP 8006/22	ALLOW	Administration Proxmox via VPN (UI + SSH).
VLAN40 — VPN (WireGuard)	VPN_NET	CEPH_NET (VLAN10/20)	Any	BLOCK	Empêche l'accès direct au stockage depuis le VPN (réduction surface d'attaque).
VLAN50 — Production	PROD_NET	ADMIN_NET (VLAN30)	Any	BLOCK	Interdit la remontée vers l'administration (anti-mouvement latéral).
VLAN50 — Production	PROD_NET	CEPH_NET (VLAN10/20)	Any	BLOCK	Isole le réseau stockage des workloads (séparation PROD / STORAGE).
VLAN50 — Production	PROD_NET	WAN	TCP 80/443, DNS, NTP	ALLOW	Autorise les sorties nécessaires (web + services temps/résolution).
VLAN30 — Automatisation & Services	JENKINS_HOST	PROXMOX_API (hosts)	TCP 8006/22	ALLOW	Permet l'orchestration (CI/CD → Proxmox) pour le déploiement automatisé.
VLAN10/20 — Ceph	CEPH_NODES	CEPH_NODES	Ceph (MON/MGR/OSD), ICMP (option)	ALLOW	Autorise uniquement le trafic interne au cluster de stockage.

ALLOW = flux explicitement autorisé · BLOCK = flux explicitement interdit · Blocage implicite (règle finale)

Figure 82 Règles du trafic sur Cluster OPNSense

4- Vérification des mécanismes de sauvegarde et de supervision

Les mécanismes de sauvegarde ont été validés à travers l'exécution de tâches planifiées et la réalisation d'une opération de restauration. Les sauvegardes générées ont été vérifiées en termes d'intégrité et de disponibilité.

Par ailleurs, la supervision et la centralisation des journaux ont été contrôlées afin de garantir la visibilité opérationnelle de l'infrastructure. Les événements remontés ont permis de confirmer la bonne collecte des métriques et logs.

Restauration d'une VM

Afin de valider le dispositif de sauvegarde, un test de restauration complète d'une machine virtuelle a été réalisé. L'objectif était de vérifier l'intégrité des sauvegardes, la cohérence des données restaurées ainsi que la capacité à remettre en service une VM en condition d'exploitation.

La procédure a consisté à sélectionner une sauvegarde existante, à lancer une restauration sur le cluster Proxmox, puis à démarrer la VM restaurée et réaliser des contrôles de bon fonctionnement (accès au système, services applicatifs, réseau).

Scénario d'une sauvegarde

Un scénario de test de restauration a été mis en œuvre afin de simuler la perte complète d'une machine virtuelle. La VM sélectionnée, préalablement sauvegardée sur Proxmox Backup Server, a été volontairement supprimée du nœud d'hébergement pve01 afin de reproduire une situation d'incident réel, telle qu'une corruption, une erreur de manipulation ou une défaillance système.

Suite à cette suppression, une procédure de restauration a été engagée en s'appuyant sur le point de sauvegarde disponible dans Proxmox Backup Server. La restauration a été effectuée vers le cluster Proxmox en conservant la configuration initiale de la machine virtuelle.

Une fois la tâche de restauration terminée, la VM a été démise en service et son fonctionnement a été vérifié à travers l'accès à la console ainsi que des tests de connectivité réseau. Ce scénario a permis de confirmer l'intégrité des sauvegardes produites et la capacité de l'infrastructure à assurer la remise en service d'une machine virtuelle à partir d'un point de sauvegarde valide, démontrant ainsi l'efficacité du mécanisme de continuité d'activité mis en place.

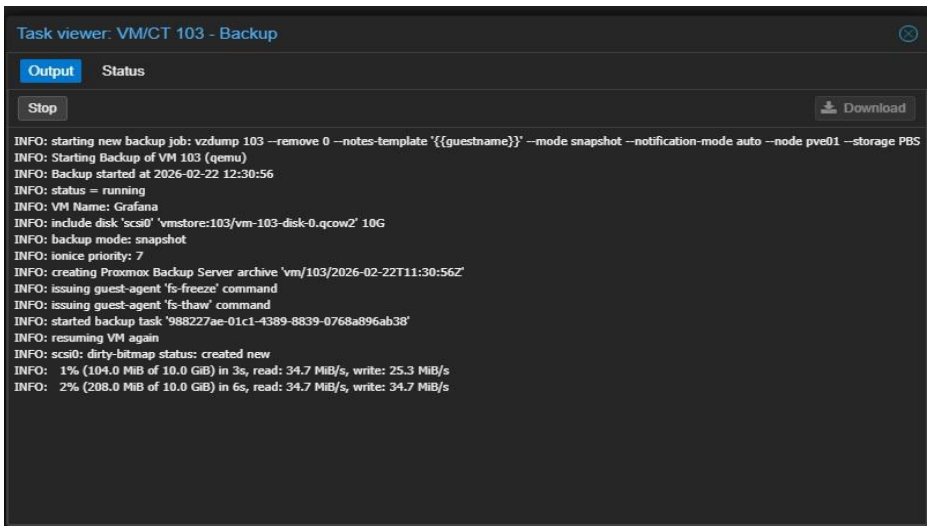


Figure 83 Test de sauvegarde d'un VM

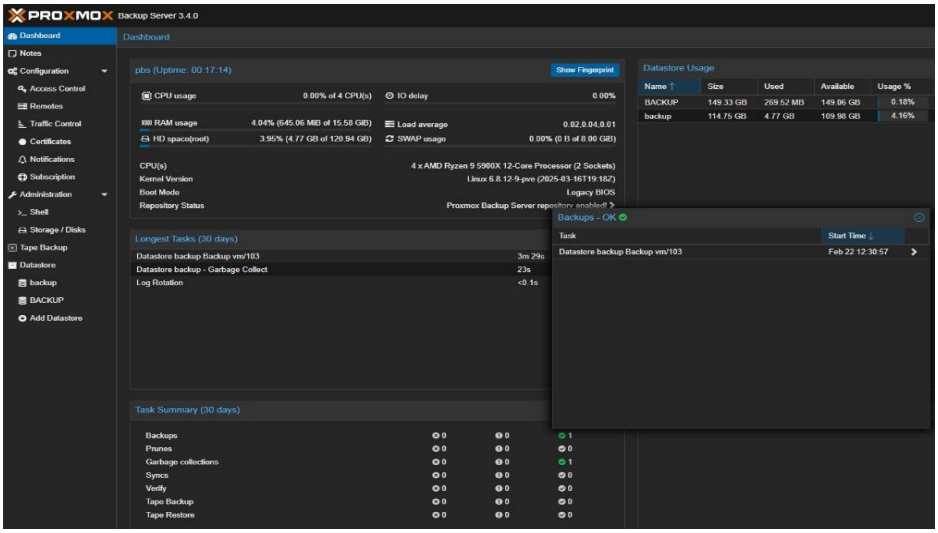


Figure 84 Sauvegarde Proxmox Backup opérationnelle

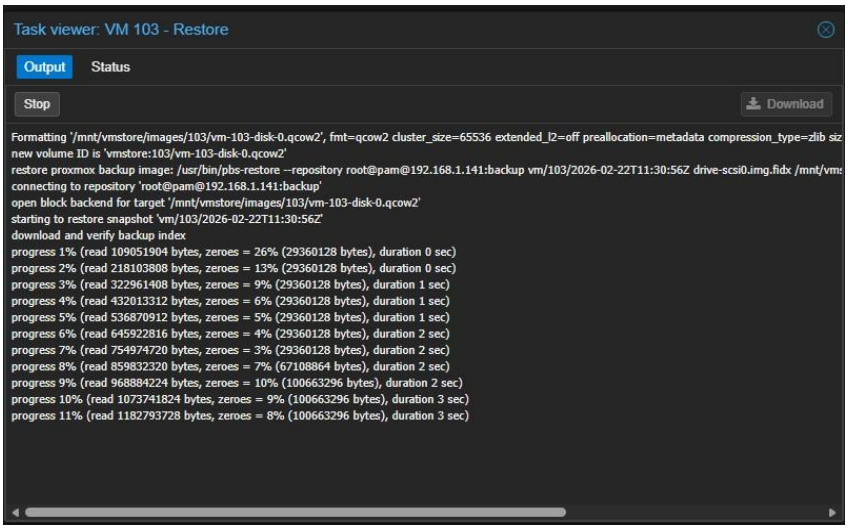


Figure 85 Restauration VM en cours

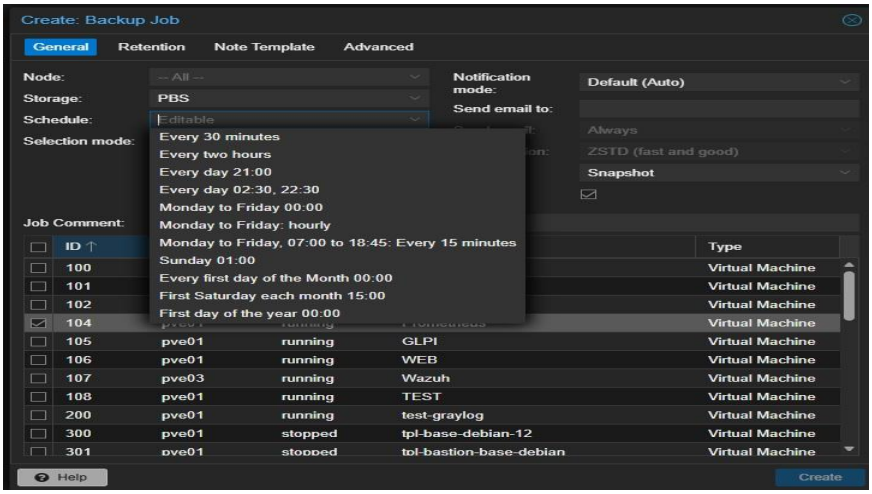


Figure 86 Création d'une sauvegarde journalière

Le test a permis de confirmer que la sauvegarde était restaurable et que la machine virtuelle retrouvait un état opérationnel cohérent avec le point de sauvegarde retenu.

Ce résultat valide la fiabilité du mécanisme de sauvegarde et la capacité de l'infrastructure à assurer une reprise de service en cas d'incident ou de perte d'une VM et ces tests démontrent la capacité de la solution à assurer la continuité d'exploitation et la détection d'incidents.

Supervision Graylog & Wazuh

La supervision et la centralisation des journaux ont été validées afin de garantir la visibilité opérationnelle et la capacité de détection d'événements au sein de l'infrastructure.

La solution mise en œuvre repose sur Graylog pour la collecte et l'agrégation des logs, ainsi que sur Wazuh pour l'analyse de sécurité et la détection d'anomalies.

Des événements issus de différentes machines virtuelles et composants de l'infrastructure ont été générés puis observés dans Graylog, confirmant la bonne remontée des journaux vers la plateforme de centralisation. Parallèlement, ces événements ont été corrélés par Wazuh, permettant la génération d'alertes de sécurité et la mise en évidence d'activités anormales.

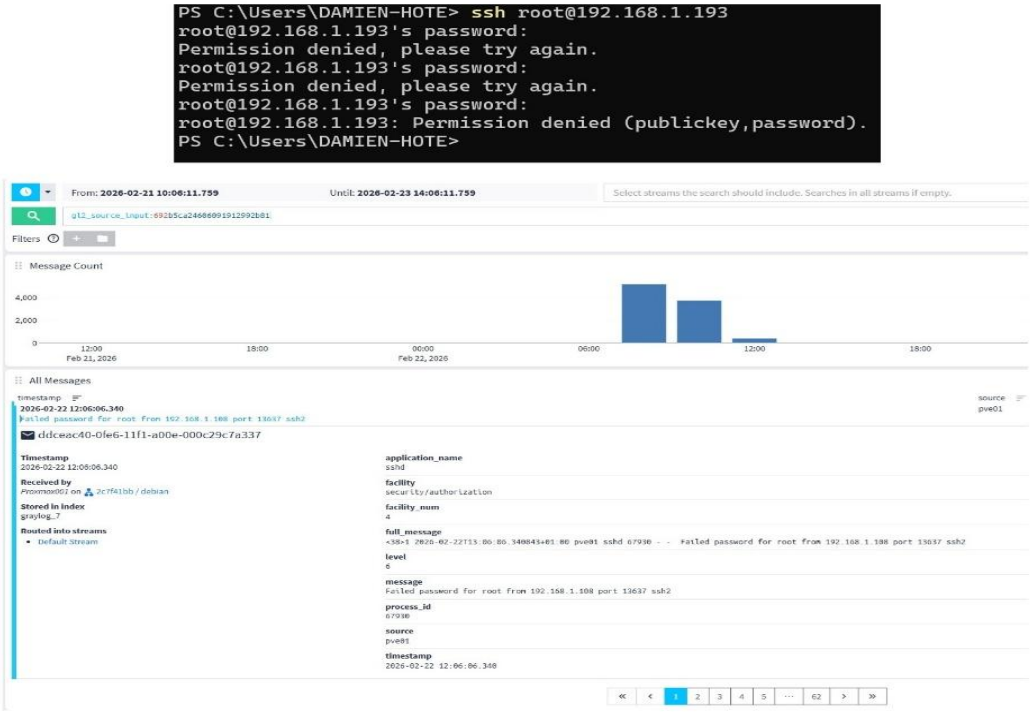


Figure 87 Exemple de tentative de connexion ssh

Figure 88 Wazuh - Alertes intrusions 'logs Windows & Linux"

Figure 89 Wazuh - Réception des logs Vlan-Production

Ces vérifications démontrent la capacité de l'infrastructure à fournir une visibilité globale sur l'état du système et à détecter des événements susceptibles d'impacter la sécurité ou la disponibilité des services

Alerte en cas d'une connexion SSH non autorisée

Un test de sécurité a été réalisé afin de valider la détection d'accès SSH non autorisés.
Une tentative de connexion anormale a été simulée sur une machine supervisée, ce qui a déclenché une alerte dans Wazuh grâce aux règles de corrélation des logs.
Ce test a permis de confirmer la capacité de la plateforme à détecter rapidement les comportements suspects et à renforcer la supervision de sécurité de l'infrastructure.

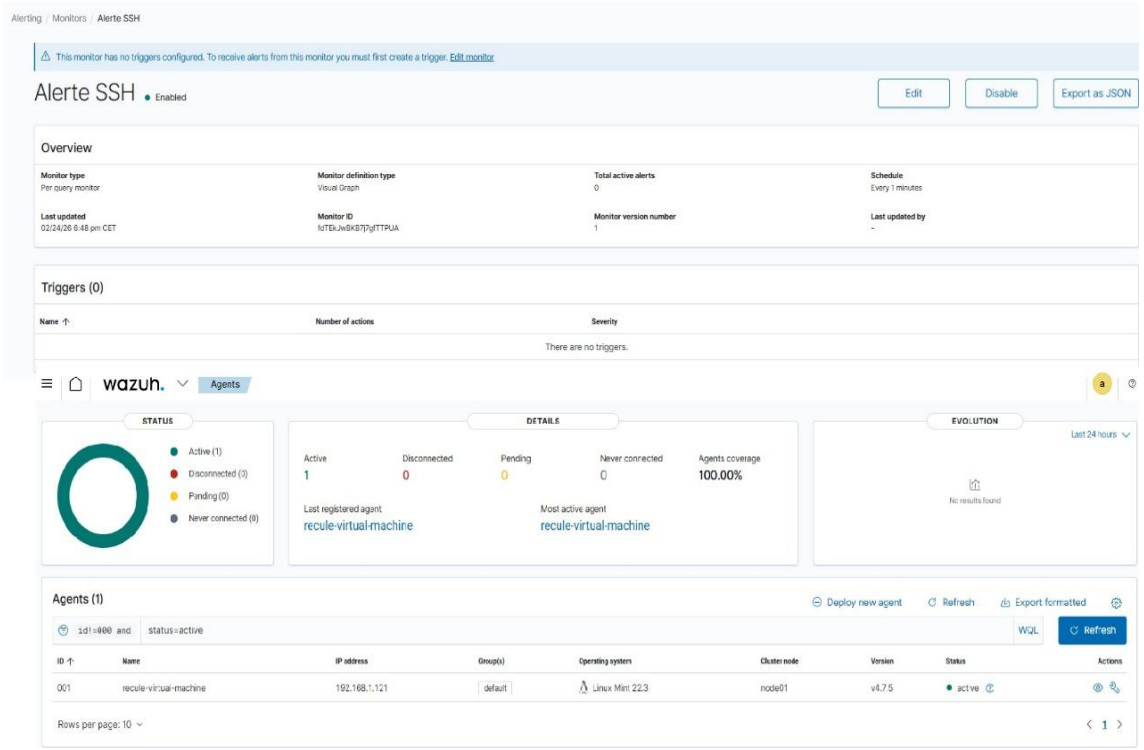


Figure 90 Alertes connexion SSH – Wazuh

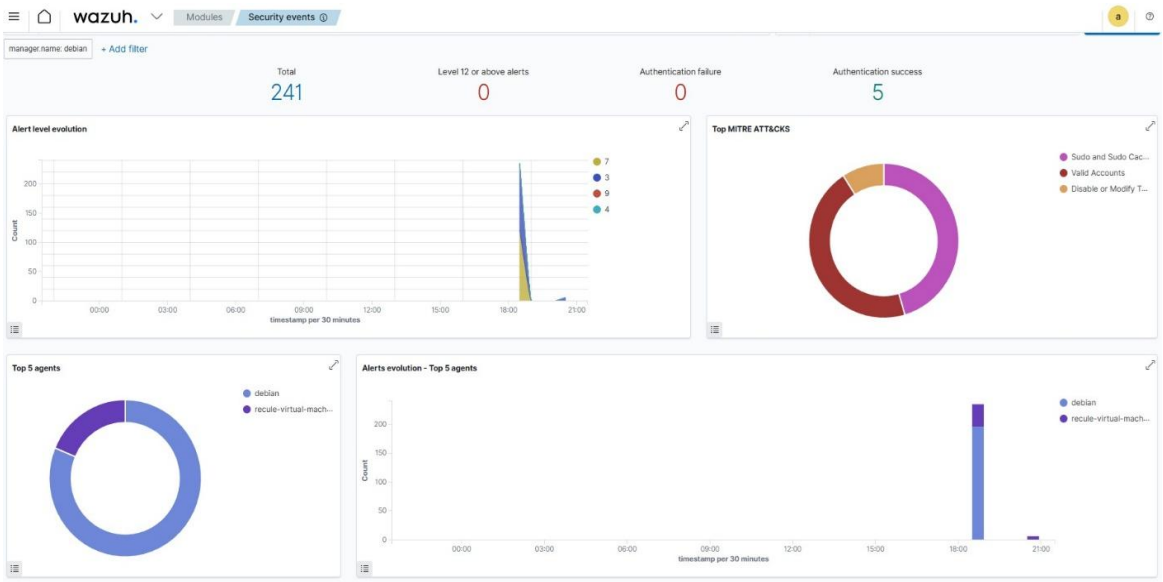


Figure 91 Wazuh - Evolutions des différentes alertes

B.2 Résultats et validation

Ainsi, les résultats obtenus ont démontré la conformité de la solution un déploiement automatisé fonctionnel et rapide (< 2 minutes pour une VM).

Une continuité de service assurée lors des tests de panne, des sauvegardes restaurable et cohérentes, une supervision et une journalisation opérationnelles (Accès sécurisés conformes aux exigences).

La recette technique a ainsi permis de valider la mise en production de l'infrastructure.

Fonction testée	Description	Résultat	Statut
Authentification + 2FA	Accès sécurisé au dashboard avec login et validation TOTP via QR Code.	Conforme	✓
Statut des services	Vérification Jenkins, Ansible, Terraform, Graylog, Docker et Proxmox.	Conforme	✓
Monitoring Proxmox	Collecte CPU, RAM, DISK, latence et nombre de VM sur PVE01 à PVE03.	Conforme	✓
Gestion des VM	Démarrage, arrêt, redémarrage et suppression des VM via API Proxmox.	Conforme	✓
Déploiement Terraform (VM unique)	Création éphémère d'une VM depuis template avec retour console.	Conforme	✓
Déploiement par groupe	Déploiement multi-VM automatisé via groupes Terraform.	Conforme	✓
Ansible – Ping & MAJ	Lancement de playbooks Ansible depuis le dashboard avec retour d'état.	Conforme	✓
Déploiement Apache2	Installation automatisée d'Apache2 sur VM cible via Ansible.	Conforme	✓
Logs Proxmox	Consultation des journaux système Proxmox en temps réel.	Conforme	✓
HTTPS & certificats	Intégration de certificats ADCS sur Proxmox VE.	Conforme	✓

Figure 92 Plan de test (Recette technique)

5- Audit TLS

(Audit intégral en annexe)

NTS **NovaTechSolutions**
Rapport officiel — Audit de sécurité TLS

Référence NTS-TLS-2026-02-27 | **Date** 27/02/2026 | **Version** 1.0 | **Classification** Interne

Audit TLS — dashboard.novatechsolutions.fr

Ce document présente les résultats d'un audit de configuration TLS visant à valider la conformité, la robustesse cryptographique et la résistance aux vulnérabilités connues du point d'entrée `82.224.192.24:18443`.

1) Périmètre & contexte

Service	Dashboard cloud privé (HTTP sur TLS)
FQDN	dashboard.novatechsolutions.fr
Adresse/Port	82.224.192.24:18443
rDNS	bob75-3_migr-82-224-192-24.fbx.proxad.net
Outil	testssl.sh 3.2.3 (2d2e665 — 2026-02-18)
Méthode	Scan protocoles, suites, certificat, en-têtes, vulnérabilités

TLS 1.3 | TLS 1.2 | Forward Secrecy | AEAD | Durcissement OK

✓ **Statut global : Conforme**
Configuration TLS moderne, certificat valide et chaîne de confiance complète.

A+ Note globale (interne)

2) Synthèse exécutive

- **Protocoles obsolètes désactivés** (SSLv2/SSLv3/TLS1.0/TLS1.1).
- **TLS 1.2 et 1.3** activés avec préférences serveur.
- **Suites fortes** : AES-GCM & ChaCha20-Poly1305 (AEAD), Forward Secrecy.
- **Certificat public conforme** : SAN présent, correspondance domaine, chaîne complète.
- **Aucune vulnérabilité critique** détectée (Heartbleed/ROBOT/DROWN/FREAK/LOGJAM/...).

✔ **Audit validé pour exposition Internet**

3) Résultats détaillés

Contrôle	Résultat	Commentaire
Protocoles	OK	TLS 1.2 et TLS 1.3 uniquement. Aucun protocole obsolète offert.
Chiffrement (Suites)	OK	AEAD priorisé (AES-GCM / ChaCha20-Poly1305), suites faibles non proposées.
Forward Secrecy	OK	ECDHE activé, courbes modernes (X25519/prime256v1/secp384r1).
Certificat & PKI	OK	Certificat valide, SAN présent, correspondance FQDN, chaîne complète, durée conforme.
Vulnérabilités TLS	OK	Non vulnérable aux attaques majeures testées (incluant Heartbleed, ROBOT, DROWN...).
En-têtes de sécurité	OK	HSTS activé, redirection HTTPS cohérente, surface HTTP durcie.
Compatibilité clients	OK	Compatibilité assurée avec navigateurs modernes et clients TLS actuels (Chrome/Firefox/Edge/Safari/Java).

4) Recommandations

Aucun point bloquant n'a été identifié. Recommandations de maintien en conditions de sécurité :

- Surveiller les évolutions de vulnérabilités TLS/OpenSSL et re-scanner après mises à jour majeures.
- Maintenir la politique "TLS 1.2/1.3 only" et la priorisation AEAD + Forward Secrecy.
- Renouveler le certificat avant échéance et conserver une chaîne complète et publique.
- Conserver HSTS actif et homogénéiser les en-têtes de sécurité sur toutes les routes (login / API).

Figure 93 Audit TLS

Rapport d'audit TLS

Cible : dashboard.novatechsolutions.fr
Date : 27 février 2026
Outil utilisé : testssl.sh v3.2.3

Objectif de l'audit

Dans le cadre du renforcement de la sécurité de mon Dashboard cloud privé, un audit complet de la configuration TLS a été réalisé afin d'évaluer :

- La conformité aux standards de sécurité actuels.
- La robustesse des protocoles et suites cryptographiques.
- La validité et la chaîne de confiance du certificat.
- L'exposition aux vulnérabilités connues.
- Le niveau global de protection côté client.

Résumé exécutif

L'audit met en évidence une configuration TLS robuste, moderne et conforme aux meilleures pratiques de sécurité actuelles.

L'ensemble des indicateurs techniques est au vert, garantissant une confidentialité forte des échanges, une authentification fiable du serveur, une protection contre les attaques connues et une compatibilité optimale avec les navigateurs modernes.

Analyse technique détaillée

Niveau protocoles, le serveur n'accepte que TLS 1.2 et TLS 1.3.

Les protocoles obsolètes (SSLv2, SSLv3, TLS 1.0, TLS 1.1) sont désactivés, supprimant toute surface d'attaque liée aux anciennes vulnérabilités (POODLE, BEAST, etc.).

Suites cryptographiques

La configuration privilégie exclusivement :

- AES-GCM
- ChaCha20-Poly1305
- ECDHE pour le Perfect Forward Secrecy
- Courbes modernes (X25519, secp384r1)

Aucune suite faible, export, RC4, 3DES ou CBC obsolète n'est activée.

Le serveur impose son ordre de préférence, garantissant l'utilisation des algorithmes les plus robustes.

Perfect Forward Secrecy

La Forward Secrecy est pleinement activée via ECDHE, assurant que la compromission future de la clé privée ne permettrait pas de déchiffrer des sessions passées. Ainsi, les échanges sont protégés même en cas d'exposition ultérieure de secrets.

Certificat

Le certificat correspond exactement au nom de domaine, il est mis par une autorité de certification reconnue, fournissant une chaîne de certification complète et conforme aux exigences modernes de durée de validité.

La signature est effectuée avec un algorithme sécurisé (SHA-256) et une clé RSA 24096 bits.

Vulnérabilités

Aucune vulnérabilité critique ou connue n'a été détectée et l'implémentation TLS est saine et correctement durcie :

- Heartbleed : non vulnérable
- ROBOT : non vulnérable

- DROWN : non vulnérable
- FREAK : non vulnérable
- LOGJAM : non vulnérable
- SWEET32 : non vulnérable
- BEAST : non vulnérable
- CRIME / BREACH : non vulnérable

Compatibilité client

Les simulations montrent une compatibilité complète avec les navigateurs modernes (Chrome, Firefox, Edge, Safari), les systèmes Android et iOS récents. Les anciens clients obsolètes ne sont pas supportés, conformément à une politique de sécurité moderne.

Conclusion

La configuration TLS du Dashboard cloud privé est conforme aux standards actuels, sécurisée contre les attaques connues, optimisée pour la performance et la robustesse et adaptée à une exposition publique sécurisée

Aussi, l'architecture cryptographique mise en place garantit un haut niveau de confiance et de protection des données.

C. Bilan des tests

Les tests ont couvert l'ensemble des briques techniques du projet, notamment :

- **Sécurisation de l'accès** : validation du mécanisme d'authentification avec double facteur (2FA via TOTP/QR Code).
- **Supervision des services** : vérification de la disponibilité et du bon fonctionnement des composants critiques (Jenkins, Ansible, Terraform, Graylog, Docker et Proxmox).
- **Monitoring de l'infrastructure Proxmox** : contrôle de la collecte des métriques (CPU, RAM, disque, latence, nombre de VM) sur les différents nœuds.
- **Gestion du cycle de vie des VM** : tests de démarrage, arrêt, redémarrage et suppression via API Proxmox.
- **Déploiement automatisé** :
    - Création unitaire de VM via Terraform.
    - Déploiement multi-VM par groupes.
    - Exécution de playbooks Ansible (ping, mises à jour, installation d'Apache2).
- **Consultation des logs** : vérification de l'accès en temps réel aux journaux système Proxmox.
- **Gestion des certificats HTTPS** : intégration et validation des certificats ADCS.

L'ensemble des scénarios testés a été déclaré **conforme**, attestant la fiabilité des mécanismes d'automatisation, la cohérence des workflows DevOps implémentés, la bonne intégration entre les différents outils de l'écosystème ainsi que le respect des exigences de sécurité et de traçabilité.

Ces résultats confirment que la solution est opérationnelle en production, stable et répond aux objectifs initiaux du projet, tant sur le plan fonctionnel que technique.

XI. Pistes d'amélioration futures

XI.1 Contexte et démarche d'amélioration continue

Les pistes d'amélioration présentées ci-après s'inscrivent dans une logique d'évolution continue de l'infrastructure Cloud privé mise en place pour NovaTechSolutions.
Elles visent à accompagner la croissance future de l'entreprise, à anticiper les besoins métiers émergents et à renforcer la maturité technique et organisationnelle du système d'information.

Ces évolutions ne remettent pas en cause l'architecture actuelle, qui répond pleinement aux objectifs initiaux du projet, mais constituent des axes d'optimisation et d'industrialisation à moyen et long terme.

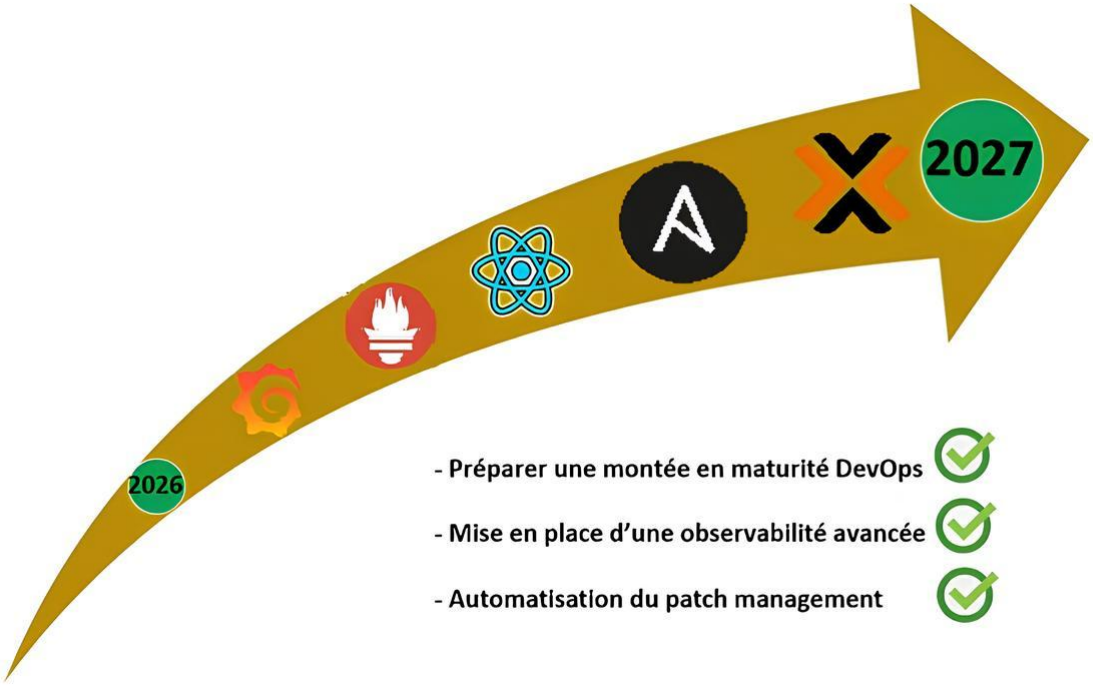


Figure 94 Améliorations futures

XI.2 Montée en maturité DevOps

Une première piste d'amélioration concerne la montée en maturité DevOps de l'infrastructure.

Si le projet intègre déjà des principes DevOps tels que l'automatisation des déploiements via Terraform et Ansible, ainsi que l'orchestration par Jenkins, plusieurs axes peuvent être approfondis :

- Mise en place de pipelines CI/CD plus avancés intégrant des contrôles qualité (tests automatisés et validation des configurations).
- Mise à jour régulière de l'infrastructure (Infrastructure as Code) avec gestion des environnements (Dev, test, production).
- Standardisation des workflows de déploiement pour réduire les erreurs humaines et améliorer la reproductibilité.

Cette évolution permettrait d'améliorer la fiabilité des mises en production tout en réduisant les délais de déploiement.

XI.3 Mise en place d'une observabilité avancée

Le projet actuel intègre déjà des mécanismes de supervision et de centralisation des journaux.
Une amélioration future consisterait à mettre en œuvre une observabilité avancée couvrant l'ensemble de l'infrastructure.
Cette observabilité pourrait s'appuyer sur :

- La collecte centralisée des métriques système et applicatives (CPU, mémoire, latence, disponibilité).
- La corrélation des logs et des événements afin de faciliter le diagnostic des incidents.
- La mise en place de tableaux de bord décisionnels permettant une vision en temps réel de l'état de l'infrastructure.

L'objectif est de passer d'une supervision réactive à une supervision proactive, capable d'anticiper les incidents avant qu'ils n'impactent les utilisateurs.

XI.4 Automatisation du patch management

Une autre piste d'amélioration concerne l'automatisation complète du patch management.
Bien que les mises à jour puissent déjà être exécutées manuellement ou via Ansible, une industrialisation plus poussée permettrait :

- Le déploiement automatique des correctifs de sécurité selon des fenêtres de maintenance définies.
- La validation des mises à jour dans un environnement de test avant déploiement en production.
- La génération de rapports de conformité et de traçabilité des correctifs appliqués.

Cette approche renforcerait la sécurité globale du système d'information tout en garantissant une meilleure conformité aux bonnes pratiques et aux exigences réglementaires.

XI.5 Évolutivité et industrialisation de l'architecture

À moyen terme, l'architecture pourrait évoluer vers une industrialisation accrue, notamment par :

- L'intégration de solutions de conteneurisation et d'orchestration (Docker, Kubernetes).
- La standardisation des services applicatifs sous forme de catalogues de services.
- L'extension du cluster Proxmox et du stockage Ceph pour accompagner la montée en charge.

Ces évolutions permettraient à NovaTechSolutions de disposer d'un cloud privé plus flexible, plus scalable et capable de s'adapter rapidement aux nouveaux besoins métiers.

XI.6 Bénéfices attendus des améliorations futures

La mise en œuvre de ces pistes d'amélioration apporterait plusieurs bénéfices :

- Amélioration de la disponibilité et de la résilience de l'infrastructure.
- Réduction des risques opérationnels et de sécurité.
- Gain de temps pour les équipes IT grâce à une automatisation accrue.
- Meilleure capacité d'anticipation et de pilotage du système d'information.

Ces évolutions positionnent le cloud privé comme un levier stratégique pour l'entreprise, au-delà d'un simple projet technique.

XII. Compétences couvertes par le projet

Le tableau ci-dessous présente la correspondance entre le référentiel d'activités et de compétences (REAC) et les réalisations concrètes du projet de Cloud Privé NovaTechSolutions.
Il met en évidence la manière dont chaque activité professionnelle attendue est traduite en actions techniques réelles, mesurables et documentées à travers la conception, le déploiement et l'exploitation d'un cloud privé automatisé.

Ainsi, chaque compétence identifiée dans le REAC est associée à des activités effectivement réalisées, ainsi qu'à des preuves et livrables concrets (architectures, configurations, scripts, procédures, journaux), garantissant la traçabilité et la validation des acquis professionnels.

Correspondance REAC ⇄ Réalisations du projet

Dashboard Cloud – Infrastructure, automatisation et supervision

N° AT	Activités types	N° CP	Compétences professionnelles	Activités réalisées dans le projet	Preuves / livrables
1	**Administrer et sécuriser les infrastructures**				
1	Administration globale de l'infrastructure	1	**Appliquer les bonnes pratiques dans l'administration des infrastructures**	Standardisation des déploiements, templates VM, procédures automatisées, centralisation des actions via un dashboard unifié.	• Templates Proxmox • Dashboard Cloud • Procédures d'exploitation
1	Infrastructure réseau	2	**Administrer et sécuriser les infrastructures réseaux**	Mise en place d'accès sécurisés, HTTPS, contrôle des flux d'administration et accès aux outils d'exploitation.	• Configuration HTTPS • Schéma réseau
1	Systèmes	3	**Administrer et sécuriser les infrastructures systèmes**	Automatisation des tâches systèmes Linux via Ansible (tests, mises à jour, déploiements applicatifs).	• Playbooks Ansible • Logs d'exécution
1	Virtualisation	4	**Administrer et sécuriser les infrastructures virtualisées**	Conception et exploitation d'un cloud privé Proxmox multi-nœuds, gestion complète des VM via API.	• Architecture Proxmox • API intégrée • Fonctions VM
2	**Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution**				
2	Conception de solution	5	**Concevoir une solution technique répondant à des besoins d'évolution**	Conception d'un dashboard cloud unifié pour piloter l'infrastructure, l'automatisation et la supervision.	• Analyse du besoin • Schéma d'architecture • Code source
2	Mise en production	6	**Mettre en production des évolutions de l'infrastructure**	Déploiement automatisé de VM avec Terraform et déploiement applicatif via Ansible.	• Modules Terraform • Playbooks Ansible
2	Supervision	7	**Mettre en œuvre et optimiser la supervision**	Supervision centralisée de l'infrastructure via Graylog et monitoring Proxmox.	• Graylog • Dashboard de supervision
3	**Participer à la gestion de la cybersécurité**				
3	Sécurité	8	**Analyser le niveau de sécurité de l'infrastructure**	Mise en œuvre d'une authentification sécurisée, HTTPS, certificats et centralisation des événements.	• TLS / certificats • 2FA • Logs de sécurité
3	Politique de sécurité	9	**Participer à la mise en œuvre de la politique de sécurité**	Définition des règles d'accès, standardisation et sécurisation des processus.	• Règles d'accès • Templates sécurisés
3	Gestion des incidents	10	**Détecter et traiter les incidents de sécurité**	Centralisation et analyse des logs pour faciliter la détection d'incidents.	• Graylog • Logs Proxmox

Figure 95 Correspondances REAC – Projet

XIII. Glossaire

2

2FA, 8, 41, 45, 49, 51, 55, 75, 76, 78, 82, 89, 92

A

ACL, 9, 18, 22
Active Directory, 10, 19, 20, 21, 37, 74
Administrateur, 1, 11, 12, 18, 30, 82
Ansible, 1, 8, 9, 12, 13, 18, 25, 27, 31, 34, 37, 41, 45, 46, 47, 49, 50, 51, 53, 55, 57, 60, 64, 65, 74, 75, 78, 79, 80, 82, 83, 88
API, 6, 9, 31, 41, 47, 49, 50, 55, 57, 63, 64, 65, 74, 75, 79, 82, 83, 84, 85, 86, 88, 90
Applications, 57
Automatisation, 18, 37, 44, 45, 47, 48, 49, 57, 75
AWS, 63

B

besoin, 4, 23, 24, 26, 29, 31, 45, 48, 63, 86, 93
bête à cornes, 4, 29, 76
budget, 4, 39, 46, 54, 61, 63, 69

C

CARP, 19, 20, 21, 76
CD, 9, 18, 25, 31, 37, 41, 57, 65, 74
CDCF, 4, 44, 49
CDCT, 4, 49
Ceph, 1, 4, 9, 13, 18, 26, 27, 34, 36, 37, 41, 46, 47, 53, 54, 55, 57, 58, 60, 61, 66, 74, 75, 79, 81
charges, 18, 22, 44, 79
CI, 9, 18, 25, 31, 37, 41, 57, 65, 74
cloud, 1, 9, 11, 12, 14, 16, 18, 24, 25, 26, 27, 28, 31, 32, 33, 34, 36, 37, 39, 41, 53, 54, 55, 59, 60, 61, 63, 64, 65, 66, 75, 76, 80, 81, 83, 91
cluster, 9, 18, 20, 21, 24, 26, 27, 34, 36, 37, 41, 45, 47, 49, 57, 60, 63, 64, 65, 66, 74, 75, 79, 81
Conception, 21, 27, 53, 55, 56

D

Dashboard, 7, 8, 9, 18, 26, 31, 47, 49, 50, 57, 60, 78, 79, 80, 82, 89, 92
DHCP, 20, 21
DMZ, 20, 21
DNS, 9, 20, 21
Docker, 13, 27, 37, 41, 74, 78, 87, 88

F

Flask, 4, 6, 9, 11, 12, 13, 18, 19, 26, 27, 31, 36, 37, 41, 46, 47, 49, 50, 53, 55, 57, 60, 64, 65, 66, 74, 75, 78, 82, 87
flux, 21, 31, 66, 76, 81

G

Graylog, 13, 31, 60, 75, 82, 87, 88

H

I

J

K

L

M

N

O

P

Q

R

S

T

V

W

XIV. Bibliographie

Ayari, K. (2015). *Active Directory et Windows PowerShell en action*. Éditions ENI.

Bonnet, N. (2023). *Windows Server 2022 – Installation, gestion du stockage et des traitements*. Éditions ENI.

Deffaix Rémy, C. (2022). *Programmation Shell sous Unix/Linux – ksh, bash, norme POSIX (avec exercices corrigés)* (7e éd.). Éditions ENI.

Espolin, M. (2024). *Terraform – Le P'tit Guide*. Éditions Independently published.

Wittouck, J. (2024). *L'infrastructure as Code avec Terraform – Déployez votre infrastructure sur le Cloud*. Éditions ENI.

Lemesle Romain. (2018). *PowerShell Core et Windows PowerShell – Les fondamentaux du langage* (2e éd.). Éditions ENI.

Perrin Damien. (2022). *Automatiser les réseaux avec Ansible : Guide technique pour l'administrateur*. Edition Independently published.

Cloux Pierre-Yves. (2022). *Docker et conteneurs* (3e éd.) : *Architectures, développement, usages et outils.* Éditions ENI.

Perré Yannig. (2023). *Ansible – Gérez la configuration de vos serveurs et le déploiement de vos applications* (3e éd.). Éditions ENI.

Chazallet Sébastien. (2024). *Python 3 – Traitement de données et techniques de programmation* (2e éd.). Éditions ENI.

Reed Amélia. (2025). *Maîtrise de Jenkins : Jobs, Pipelines, CI/CD et DevOps pour les débutants absolus*. Éditions ENI.

XV. Webographie

Classée par Technologies

Virtualisation & Infrastructure Proxmox VE
Documentation officielle Proxmox

https://pve.proxmox.com/pve-docs/
Wiki Proxmox VE
https://pve.proxmox.com/wiki/Main_Page
API REST Proxmox
https://pve.proxmox.com/pve-docs/api-viewer/
HA & Clustering
https://pve.proxmox.com/wiki/High_Availability_Cluster_4.x
Utilisé pour : configuration du cluster, gestion HA, gestion des VMs, API appelée par ton dashboard Flask.

Stockage Distribué Ceph

Documentation Ceph
https://docs.ceph.com/en/latest/
Architecture RADOS (OSD, MON, MGR)

https://docs.ceph.com/en/latest/rados/

Best practices Ceph sur Proxmox
https://pve.proxmox.com/wiki/Ceph_Server
Utilisé pour : stockage distribué, réplication, tolérance aux pannes, choix de l'architecture Ceph dans ton cluster.

Infrastructure as Code (IaC) – Terraform

Documentation Terraform
https://developer.hashicorp.com/terraform/docs
Provider Proxmox (Telmate)
https://registry.terraform.io/providers/Telmate/proxmox/latest/docs
Syntaxe HCL
https://developer.hashicorp.com/terraform/language
Meilleures pratiques Terraform
https://developer.hashicorp.com/terraform/cloud-docs/best-practices
Utilisé pour : déploiement automatisé des VMs, modules personnalisés, gestion du cycle de vie des machines (plan/apply).

Automatisation & Configuration – Ansible

Documentation Ansible
https://docs.ansible.com/
Ansible Galaxy
https://galaxy.ansible.com/
Bonnes pratiques Ansible
https://docs.ansible.com/ansible/latest/tips_tricks/index.html
Ansible Vault (sécurisation secrets)
https://docs.ansible.com/ansible/latest/user_guide/vault.html
Utilisé pour : automatisation post-déploiement, exécution de playbooks depuis ton dashboard, sécurisation SSH.

Développement Web – Flask & Python

Documentation Flask
https://flask.palletsprojects.com/
Documentation Jinja2
https://jinja.palletsprojects.com/
Werkzeug (serveur HTTP Flask)
https://werkzeug.palletsprojects.com/
Python Standard Library
https://docs.python.org/3/library/
Utilisé pour : développement du dashboard, communication API, mise en place du HTTPS, génération du frontend dynamique.

Supervision, Logs & Sécurité

Graylog – Documentation officielle
https://go2docs.graylog.org/
GELF (Graylog Extended Log Format)
https://docs.graylog.org/docs/gelf/
Sécurité TLS / HTTPS – Mozilla SSL Guidelines
https://ssl-config.mozilla.org/
CIS Benchmarks Linux (durcissement)
https://www.cisecurity.org/cis-benchmarks/
2FA Standards

https://authy.com/what-is-2fa/

Utilisé pour : supervision centralisée, intégration des logs Proxmox, durcissement du dash, mise en place HTTPS/2FA.

Réseaux & Sécurité – OPNSense, VLAN, Firewalling

Documentation OPNSense CE
https://docs.netgate.com/OPNsense/en/latest/
VLAN : Concepts & segmentation réseau (Cisco)
https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-a-vlan.html
Firewall Best Practices
https://www.sans.org/white-papers/firewalls/
Utilisé pour : segmentation réseau (VLAN 10/20/50/99), HA CARP, synchronisation OPNSense, sécurisation des flux.

Méthodologie & Gestion de Projet

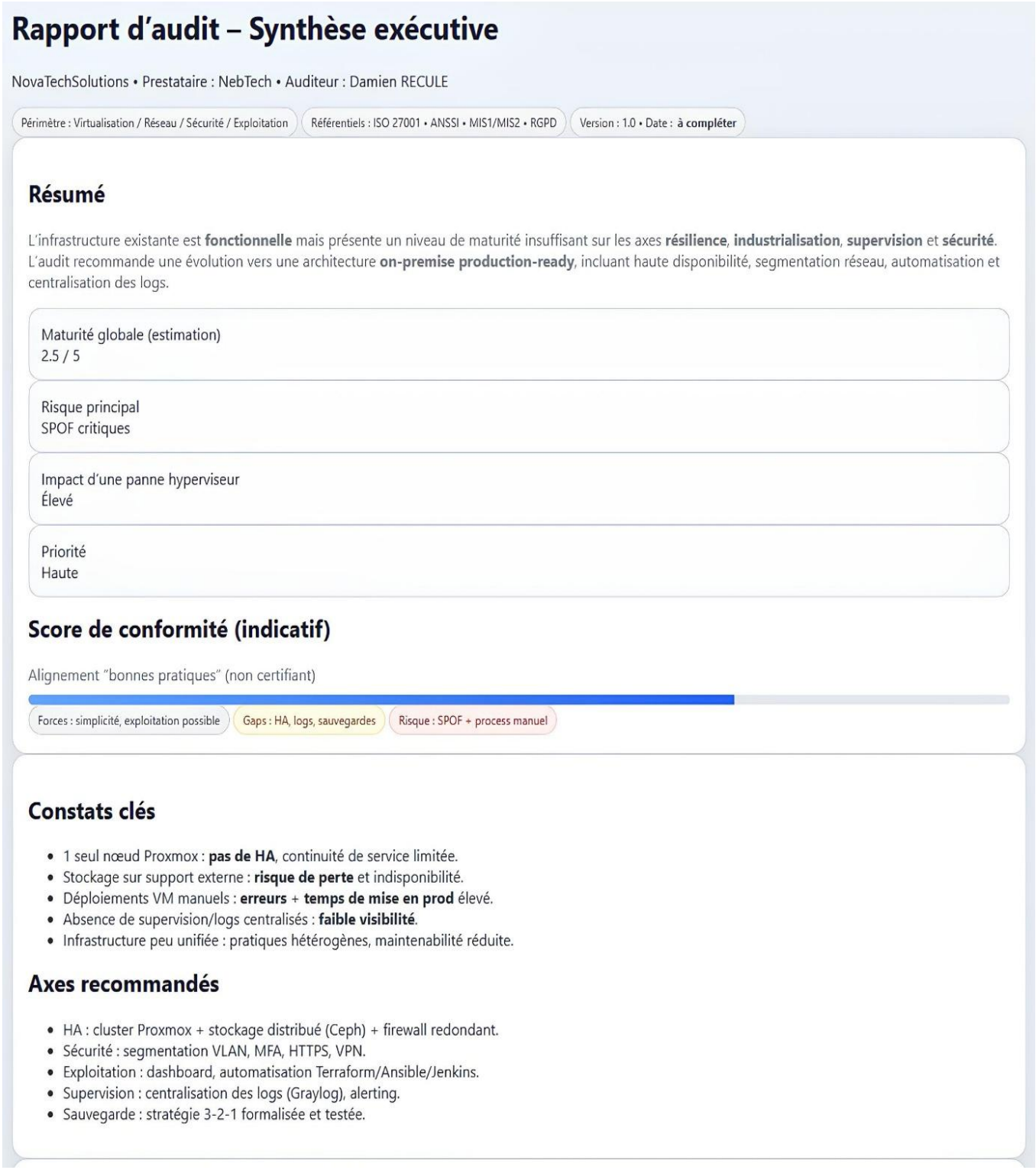
Cycle en V
https://www.commentcamarche.net/contents/595-cycle-en-v
Gantt – Référence méthodologique
https://asana.com/fr/resources/gantt-chart
AMDEC – Analyse des risques
https://fr.wikipedia.org/wiki/Analyse_des_modes_de_d%C3%A9faillance_et_de_leurs_effets
Diagrammes – UML
https://www.uml-diagrams.org/
Outil de modélisation (utilisé dans ton dossier)
https://www.diagrams.net/
Utilisé pour : analyse fonctionnelle (bête à cornes, pieuvre), WBS, RACI, Gantt, étude des risques, architecture globale.

Systèmes d'exploitation (Linux & Windows)

Debian Documentation
https://www.debian.org/doc/
Ubuntu Server Guide
https://ubuntu.com/server/docs
Windows Server 2022 Documentation
https://learn.microsoft.com/en-us/windows-server/
Windows 11 Pro – Admin Guide
https://learn.microsoft.com/en-us/windows/
Utilisé pour : templates Linux/Windows, configuration ADDS/ADCS, intégration des OS dans ton cloud privé.

XVI. Annexe

XVI.1 Rapports d'audit de l'infrastructure initiale de NovaTechSolutions



Rapport d'audit – Synthèse exécutive

NovaTechSolutions • Prestataire : NebTech • Auditeur : Damien RECULE

Périmètre : Virtualisation / Réseau / Sécurité / Exploitation | Référentiels : ISO 27001 • ANSSI • MIS1/MIS2 • RGPD | Version : 1.0 • Date : **à compléter**

Résumé

L'infrastructure existante est **fonctionnelle** mais présente un niveau de maturité insuffisant sur les axes **résilience**, **industrialisation**, **supervision** et **sécurité**. L'audit recommande une évolution vers une architecture **on-premise production-ready**, incluant haute disponibilité, segmentation réseau, automatisation et centralisation des logs.

Maturité globale (estimation)
2.5 / 5

Risque principal
SPOF critiques

Impact d'une panne hyperviseur
Élevé

Priorité
Haute

Score de conformité (indicatif)

Alignement "bonnes pratiques" (non certifiant)

Forces : simplicité, exploitation possible | Gaps : HA, logs, sauvegardes | Risque : SPOF + process manuel

Constats clés

- 1 seul nœud Proxmox : **pas de HA**, continuité de service limitée.
- Stockage sur support externe : **risque de perte** et indisponibilité.
- Déploiements VM manuels : **erreurs** + **temps de mise en prod** élevé.
- Absence de supervision/logs centralisés : **faible visibilité**.
- Infrastructure peu unifiée : pratiques hétérogènes, maintenabilité réduite.

Axes recommandés

- HA : cluster Proxmox + stockage distribué (Ceph) + firewall redondant.
- Sécurité : segmentation VLAN, MFA, HTTPS, VPN.
- Exploitation : dashboard, automatisation Terraform/Ansible/Jenkins.
- Supervision : centralisation des logs (Graylog), alerting.
- Sauvegarde : stratégie 3-2-1 formalisée et testée.

Figure 96 Résultats audit initial

Top risques (priorisés)

Priorité	Risque	Impact	Traitement recommandé
Critique	SPOF hyperviseur (panne Proxmox)	Arrêt global des VMs	Cluster Proxmox 3 nœuds + HA
Critique	Stockage non redondé	Perte/indispo données	Ceph + réplication + tests
Élevée	Absence logs centralisés	Détection tardive incidents	Graylog + alertes + rétention
Élevée	Déploiements manuels	Erreurs + délais	Templates + IaC + pipeline

Décision

L'audit conclut à la nécessité d'une évolution vers une architecture **plus mature**, avec un focus sur **résilience** (HA), **sécurité** (MFA/VLAN), et **industrialisation** (IaC, automatisation).

Livrable associé

- Rapport d'audit (ce document)
- Plan d'actions priorisé (P0/P1/P2)
- Registre des risques + SPOF
- Annexe conformité (ISO/MIS/RGPD/RGAA)

Audit – Constats détaillés & recommandations

NovaTechSolutions • NebTech • Périmètre : Proxmox / Réseau / Sécurité / Exploitation

Version 1.0 | Date : à compléter | Confidentiel

A. Architecture & exploitation

Constat

- Virtualisation sur **un seul nœud Proxmox** : absence de HA.
- Process de création VM **manuel** : variabilité, erreurs, délais.
- Standardisation limitée (templates/process non centralisés).

Recommandation

- Déployer un **cluster Proxmox 3 nœuds** avec HA.
- Introduire templates + cloud-init pour provisioning rapide.
- Industrialiser via Terraform/Ansible/Jenkins (IaC + orchestration).

Criticité : Élevée | Effort : Moyen | Gain : Fort

B. Sécurité & gestion des accès

Constat

- Authentification forte non généralisée.
- Accès admin perfectibles (principes "moindre privilège" à renforcer).
- Segmentation réseau limitée (zones de confiance / flux).

Recommandation

- Renforcer l'authentification : **MFA (MDP + TOTP)** et évolution possible **mTLS (certificat client ADCS)**.
- Segmenter par VLAN (admin / Ceph / automatisation / prod / VPN).
- Durcissement et politique d'accès : rôles, permissions, journalisation.

Criticité : Élevée | Effort : Moyen | Gain : Fort

C. Supervision & sauvegardes

Constat

- Absence de supervision centralisée et de visibilité consolidée.
- Logs non centralisés : faible capacité d'investigation.
- Sauvegardes ponctuelles, stratégie non formalisée.

Recommandation

- Centraliser les logs (Graylog) + règles d'alerting.
- Définir une stratégie **3-2-1** + tests de restauration.
- Rétention et traçabilité (RGPD : minimisation + durée).

Criticité : Élevée | Effort : Moyen | Gain : Fort

D. SPOF identifiés

Élément	Risque	Impact	Action	Priorité
Hyperviseur unique	Panne = arrêt global	Très élevé	Cluster Proxmox HA (3 nœuds)	P0
Stockage non redondé	Perte / corruption	Élevé	Ceph + réplication	P0
Accès distant	Accès non maîtrisé	Élevé	VPN WireGuard + règles	P1
Logs non centralisés	Détection tardive	Moyen	Graylog + alertes	P1

Plan d'actions (P0/P1/P2)

Priorité	Action	Objectif	Livrable	Indicateur
P0	Cluster Proxmox + Ceph	HA + résilience	Infra HA	Redémarrage auto VM
P0	Segmentation VLAN	Réduire surface d'attaque	Plan VLAN	Flux contrôlés
P1	IaC + pipeline	Déploiement rapide	Modules + Jenkins	VM < 2 min
P1	Logs centralisés	Visibilité + alertes	Graylog	Alertes incidents
P2	mTLS (certif client)	MFA renforcée	PKI + proxy	Accès restreint

Conformité – Mapping ISO 27001 / MIS1-MIS2 / RGPD / RGAA

Document d'alignement (non certifiant). Objectif : démontrer la prise en compte des bonnes pratiques et obligations.

En place · Partiel / en cours · À mettre en œuvre · Référentiels : ISO 27001 • ANSSI • MIS1/MIS2 • RGPD • RGAA

Thème	Référentiel	Exigence / bonne pratique	Mise en œuvre dans le projet	Statut	Preuves / livrables
Contrôle des accès	ISO 27001 / MIS	Moindre privilège, rôles, authentification forte	MFA (MDP + TOTP) + possibilité mTLS (certificat ADCS)	Partiel	Procédure MFA, schéma auth, logs accès
Segmentation réseau	ANSSI / MIS	Isoler les zones (admin, prod, stockage)	VLAN : admin / Ceph / DevOps / VPN / production	En place	Schéma réseau + plan VLAN + règles firewall
Journalisation	ISO 27001 / MIS	Centraliser les logs, traçabilité	Graylog (centralisation), alertes sur événements clés	En place	Dash Graylog + règles alerting + politique rétention
Disponibilité	ISO 27001 / MIS	Continuité, tolérance aux pannes	Proxmox HA (3 nœuds) + Ceph + pfSense HA	En place	Tests HA, rapport de validation
Sauvegardes	ISO 27001 / ANSSI	Stratégie 3-2-1, tests de restauration	3-2-1 (local + externe + copie hors site) + procédure de restore	Partiel	Procédure backup, journal de tests restore
RGPD (logs & données)	RGPD	Minimisation, accès, rétention, traçabilité	Rétention logs limitée, accès restreint, journalisation admin	Partiel	Politique rétention, matrice d'accès
Accessibilité dashboard	RGAA	Lisibilité, navigation, messages clairs	UI claire, contrastes, messages d'erreurs explicites	Partiel	Checklist RGAA, captures UI
Charte informatique	ISO 27001 / MIS	Règles d'usage, responsabilités	Charte informatique collaborateurs (annexe)	En place	Charte signable, diffusion interne
SOC (approche)	ISO 27001 / MIS	Supervision continue, détection & réponse	Graylog + alertes = 1ère brique SOC (niveau PME)	Partiel	Runbook alertes, workflow incident

NB : Ce document constitue un alignement "bonnes pratiques" et non une certification. Les éléments de preuve sont fournis via livrables, procédures et captures.

Registre des risques & matrice

Document projet • base : audit initial • priorisation P0/P1/P2

Registre des risques

ID	Risque	Prob.	Impact	Criticité	Mesures
R-01	Panne hyperviseur unique	2/5	5/5	Critique	Cluster Proxmox 3 nœuds + HA
R-02	Perte stockage non redondé	2/5	5/5	Critique	Ceph réplication + tests
R-03	Absence logs centralisés	3/5	4/5	Élevée	Graylog + alertes + rétention
R-04	Erreurs humaines déploiement	4/5	3/5	Élevée	IaC + templates + pipeline
R-05	Accès distant insuffisamment contrôlé	3/5	4/5	Élevée	VPN WireGuard + règles + MFA
R-06	Non conformité rétention logs (RGPD)	3/5	3/5	Moyenne	Politique rétention + accès restreint

Matrice (probabilité × impact)

Axe horizontal : Probabilité (1 faible → 5 forte) • Axe vertical : Impact (1 faible → 5 fort)

Lecture : les risques en zone rouge doivent être traités en priorité (P0). Les zones orange = P1. Vert = P2 / suivi.

Approche SOC – Supervision, alertes et runbook

Objectif : formaliser la supervision et la réponse aux incidents (niveau PME) • Outil : Graylog

Objectifs

- Centraliser les logs et améliorer la visibilité.
- Détecter rapidement les comportements suspects (auth, scans, erreurs).
- Déclencher des alertes et guider la réponse via un runbook.
- Conserver des preuves (traçabilité) selon une politique de rétention.

Sources de logs (exemples)

- pfSense : firewall / VPN / événements système
- Proxmox : cluster / tâches / authentification
- Linux : sshd, sudo, systemd
- Dashboard : authentification, actions admin, API

Alertes recommandées

Cas	Condition	Niveau	Action immédiate
Brute force SSH	≥ 10 échecs / 5 min	Critique	Bloquer IP, vérifier compte ciblé
Échec MFA répété	≥ 5 tentatives / 10 min	Élevé	Vérifier identité, reset si besoin
Connexion admin hors VPN	Source IP non autorisée	Critique	Couper session, vérifier règles
Dégradation cluster	Quorum/health KO	Élevé	Basculer charges, diagnostic HA

Runbook – Réponse à incident (workflow)

1) Qualification — N1

Identifier la source, l'horodatage, l'utilisateur, l'IP, et le périmètre impacté.

2) Confinement — N1/N2

Bloquer IP (pfSense), désactiver compte, couper accès externe si nécessaire.

3) Investigation — N2

Corréler logs (Proxmox, pfSense, Linux, dashboard) et confirmer le scénario.

4) Remédiation — N2/N3

Patch, durcissement, rotation secrets, ajustement règles et MFA, restauration si besoin.

5) Retour d'expérience — Post-mortem

Documenter, améliorer les règles, mettre à jour procédures/charte, ajuster la surveillance.

XVI.2 Rapports d'audit TLS – Dashboard Cloud Privé

```
###########################################################################
  testssl.sh version 3.2.3 from https://testssl.sh/
  (2d2e665 2026-02-18 10:39:22)

  This program is free software. Distribution and modification under
  GPLv2 permitted. USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!

  Please file bugs @ https://testssl.sh/bugs/
###########################################################################

  Using OpenSSL 1.0.2-bad (Mar 28 2025)  [~179 ciphers]
  on recule-Dbook-131:./bin/openssl.Linux.x86_64

 Start 2026-02-27 13:50:11        -->> 82.224.192.24:18443 (dashboard.no-
vatechsolutions.fr) <<--

 rDNS (82.224.192.24):   bob75-3_migr-82-224-192-24.fbx.proxad.net.
 Service detected:       HTTP

 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered (OK)
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)


 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits
Cipher Suite Name (IANA/RFC)
-----------------------------------------------------------------------------
-------------------------------------------------
SSLv2
 -
SSLv3
 -
TLSv1
 -
TLSv1.1
 -
TLSv1.2 (server order)
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 253   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xcca8   ECDHE-RSA-CHACHA20-POLY1305       ECDH 253   ChaCha20    256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
```

```
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 253   AESGCM      128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc028   ECDHE-RSA-AES256-SHA384           ECDH 253   AES         256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc027   ECDHE-RSA-AES128-SHA256           ECDH 253   AES         128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc014   ECDHE-RSA-AES256-SHA              ECDH 253   AES         256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 xc013   ECDHE-RSA-AES128-SHA              ECDH 253   AES         128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9d     AES256-GCM-SHA384                 RSA        AESGCM      256
TLS_RSA_WITH_AES_256_GCM_SHA384
 x9c     AES128-GCM-SHA256                 RSA        AESGCM      128
TLS_RSA_WITH_AES_128_GCM_SHA256
 x3d     AES256-SHA256                     RSA        AES         256
TLS_RSA_WITH_AES_256_CBC_SHA256
 x3c     AES128-SHA256                     RSA        AES         128
TLS_RSA_WITH_AES_128_CBC_SHA256
 x35     AES256-SHA                        RSA        AES         256
TLS_RSA_WITH_AES_256_CBC_SHA
 x2f     AES128-SHA                        RSA        AES         128
TLS_RSA_WITH_AES_128_CBC_SHA
TLSv1.3 (server order)
 x1302   TLS_AES_256_GCM_SHA384            ECDH 253   AESGCM      256
TLS_AES_256_GCM_SHA384
 x1303   TLS_CHACHA20_POLY1305_SHA256      ECDH 253   ChaCha20    256
TLS_CHACHA20_POLY1305_SHA256
 x1301   TLS_AES_128_GCM_SHA256            ECDH 253   AESGCM      128
TLS_AES_128_GCM_SHA256

 Has server cipher order?     yes (OK) -- TLS 1.3 and below


 Testing robust forward secrecy (FS) -- omitting Null Authentication/En-
cryption, 3DES, RC4

 FS is offered (OK)           TLS_AES_256_GCM_SHA384 TLS_CHA-
CHA20_POLY1305_SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES256-SHA
                              ECDHE-RSA-CHACHA20-POLY1305
TLS_AES_128_GCM_SHA256 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES128-SHA
 KEMs offered                 None
 Elliptic curves offered:     prime256v1 secp384r1 secp521r1 X25519 X448
 Finite field group:          ffdhe2048 ffdhe3072 ffdhe4096 ffdhe6144
ffdhe8192
 TLS 1.2 sig_algs offered:    RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-
PSS-RSAE+SHA512 RSA+SHA256 RSA+SHA384 RSA+SHA512 RSA+SHA224
 TLS 1.3 sig_algs offered:    RSA-PSS-RSAE+SHA256 RSA-PSS-RSAE+SHA384 RSA-
PSS-RSAE+SHA512

 Testing server defaults (Server Hello)

 TLS extensions (standard)    "max fragment length/#1" "sup-
ported_groups/#10" "EC point formats/#11" "encrypt-then-mac/#22" "extended
master secret/#23"
                              "session ticket/#35" "supported versions/#43"
"key share/#51" "renegotiation info/#65281"
 Session Ticket RFC 5077 hint 7200 seconds, session tickets keys seems to
be rotated < daily
 SSL Session ID support       yes
 Session Resumption           Tickets: yes, ID: no
 TLS clock skew               Random values, no fingerprinting possible
 Certificate Compression      none
```

```
 Client Authentication          none
 Signature Algorithm            SHA256 with RSA
 Server key size                RSA 2048 bits (exponent is 65537)
 Server key usage               Digital Signature, Key Encipherment
 Server extended key usage      TLS Web Server Authentication
 Serial                         540000000320C078FF179F408D000000000003 (OK:
length 19)
 Fingerprints                   SHA1 8DFFEF7ED5470A05401437942E3C0DB8EEC1B771
                                SHA256
98BC9310406BF64002CE229A5330FF0C5DE02AD08A689FDDC139B34F79ACEB5D
 Common Name (CN)               dashboard.novatechsolutions.lan
 subjectAltName (SAN)           missing(OK)-- Browsers are complaining
 Trust (hostname)               certificate (OK)
 Chain of trust                 (OK) (chain complete)
 EV cert (experimental)         no
 Certificate Validity (UTC)     646 >= 60 days (2025-12-05 22:16 --> 2027-12-
05 22:16)

ETS/"eTLS", visibility info  not present
 Certificate Revocation List  ldap:///CN=NovaTechSolutions-SRV-001-ADDS-
CA,CN=SRV-001-ADDS,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Confi-
guration,DC=NovaTechSolutions,DC=lan?certificateRevocationList?base?ob-
jectClass=cRLDistributionPoint
 OCSP URI                       --
 OCSP stapling                  offered (OK)
 OCSP must staple extension     --
 DNS CAA RR (experimental)      offered (OK)
 Certificate Transparency       --
 Certificates provided          1
 Issuer                         NovaTechSolutions-SRV-001-ADDS-CA (NovaTech-
Solutions.lan)
 Intermediate Bad OCSP (exp.) Ok


 Testing HTTP header response @ "/"

 HTTP Status Code               302 FOUND, redirecting to "/login"
 HTTP clock skew                0 sec from localtime
 Strict Transport Security      offered (OK)
 Public Key Pinning             --
 Server banner                  Werkzeug/3.1.3 Python/3.11.2'
 Application banner             --
 Cookie(s)                      (none issued at "/") -- maybe better try tar-
get URL of 30x
 Security headers               offered (OK)
 Reverse Proxy banner           offered (OK)


 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heart-
beat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    no gzip/deflate/compress/br HTTP
compression (OK)  - only supplied "/" tested
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3
support
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK), no
protocol below TLS 1.2 offered
```

```
 SWEET32 (CVE-2016-2183, CVE-2016-6329)     not vulnerable (OK)
 FREAK (CVE-2015-0204)                      not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)       not vulnerable on this host and
port (OK)
                                            make sure you don't use this
certificate elsewhere with SSLv2 enabled services, see
                                            https://search.cen-
sys.io/search?resource=hosts&virtual hosts=IN-
CLUDE&q=98BC9310406BF64002CE229A5330FF0C5DE02AD08A689FDDC139B34F79ACEB5D
 LOGJAM (CVE-2015-4000), experimental       not vulnerable (OK): no DH EX-
PORT ciphers, no DH key detected with <= TLS 1.2
 BEAST (CVE-2011-3389)                      not vulnerable (OK), no SSL3 or
TLS1
 LUCKY13 (CVE-2013-0169), experimental uses obsolete cipher block chaining
ciphers with TLS, see server prefs.
 Winshock (CVE-2014-6321), experimental     not vulnerable (OK)
 RC4 (CVE-2013-2566, CVE-2015-2808)         no RC4 ciphers detected (OK)
```

Running client simulations (HTTP) via sockets

```
 Browser                        Protocol  Cipher Suite Name (OpenSSL)
Forward Secrecy
------------------------------------------------------------------------------
----------------------
 Android 7.0 (native)           TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
256 bit ECDH (P-256)
 Android 8.1 (native)           TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
253 bit ECDH (X25519)
 Android 9.0 (native)           TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Android 10.0 (native)          TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Android 11/12 (native)         TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Android 13/14 (native)         TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Android 15 (native)            TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Chrome 101 (Win 10)            TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Chromium 137 (Win 11)          TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Firefox 100 (Win 10)           TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Firefox 137 (Win 11)           TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 IE 8 Win 7                     No connection
 IE 11 Win 7                    TLSv1.2   ECDHE-RSA-AES256-SHA384
256 bit ECDH (P-256)
 IE 11 Win 8.1                  TLSv1.2   ECDHE-RSA-AES256-SHA384
256 bit ECDH (P-256)
 IE 11 Win Phone 8.1            TLSv1.2   ECDHE-RSA-AES128-SHA256
256 bit ECDH (P-256)
 IE 11 Win 10                   TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
256 bit ECDH (P-256)
 Edge 15 Win 10                 TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
253 bit ECDH (X25519)
 Edge 101 Win 10 21H2           TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Edge 133 Win 11 23H2           TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Safari 18.4 (iOS 18.4)         TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
```

```
 Safari 15.4 (macOS 12.3.1)    TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Safari 18.4 (macOS 15.4)      TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Java 7u25                     No connection
 Java 8u442 (OpenJDK)          TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Java 11.0.2 (OpenJDK)         TLSv1.3   TLS_AES_256_GCM_SHA384
256 bit ECDH (P-256)
 Java 17.0.3 (OpenJDK)         TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Java 21.0.6 (OpenJDK)         TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 go 1.17.8                     TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 LibreSSL 3.3.6 (macOS)        TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 OpenSSL 1.0.2e                TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
256 bit ECDH (P-256)
 OpenSSL 1.1.1d (Debian)       TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 OpenSSL 3.0.15 (Debian)       TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 OpenSSL 3.5.0 (git)           TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)
 Apple Mail (16.0)             TLSv1.2   ECDHE-RSA-AES256-GCM-SHA384
256 bit ECDH (P-256)
 Thunderbird (91.9)            TLSv1.3   TLS_AES_256_GCM_SHA384
253 bit ECDH (X25519)


 Rating (experimental)

 Rating specs (complete)  SSL Labs's 'SSL Server Rating Guide' (version
2009r from 2025-05-16)
 Specification documentation  https://github.com/ssllabs/research/wiki/SSL-
Server-Rating-Guide
 Protocol Support (weighted)  0 (0)
 Key Exchange     (weighted)  0 (0)
 Cipher Strength  (weighted)  0 (0)
 Final Score                  0
 Overall Grade                M
 Grade cap reasons            Grade capped to M. Domain name mismatch
                              Grade capped to B. Issues with chain of trust
(chain complete)

 Done 2026-02-27 13:52:13 [ 126s] -->> 82.224.192.24:18443 (dashboard.no-
vatechsolutions.fr) <<--
```

XVI.3 Certificats de formations.

Les certificats présentés dans cette annexe correspondent à des formations complémentaires suivies en parallèle du cursus principal, principalement durant les week-ends et en autonomie.

Ces formations avaient pour objectif de renforcer mes compétences techniques sur des thématiques directement liées à la mise en œuvre du projet de cloud privé, notamment la virtualisation, l'automatisation, les réseaux et la sécurité des systèmes.

Elles m'ont permis d'approfondir certains concepts techniques abordés dans le cadre de la formation, d'acquérir des compétences pratiques directement applicables au projet et de garantir une mise en œuvre cohérente, fonctionnelle et réaliste de l'infrastructure présentée.

Ces apprentissages complémentaires s'inscrivent dans une démarche personnelle de montée en compétences continue, indispensable dans les métiers de l'informatique et plus particulièrement dans les domaines de l'administration systèmes, du cloud et du DevOps.

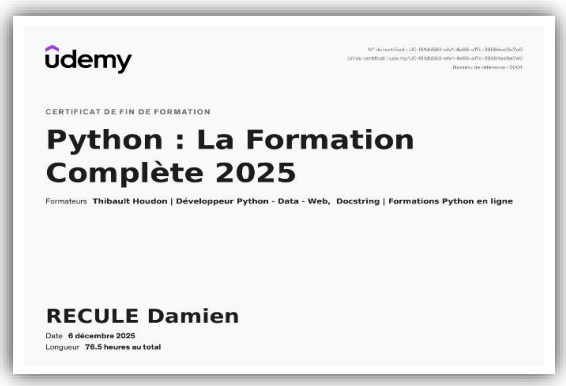


Figure 97 Python - La formation complète 2025

Figure 98 Programmez des applications avec Flask

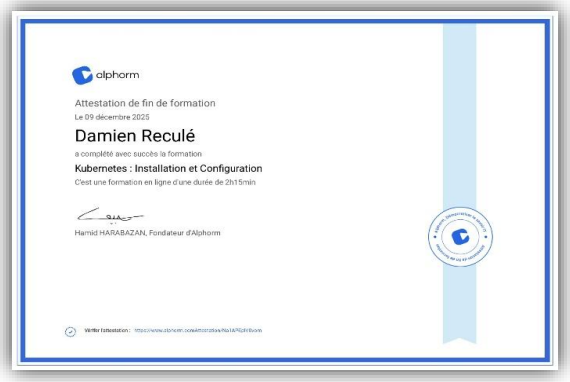


Figure 99 Kubernetes - Installation & Configuration

Figure 100 Windows Server 2025

Figure 101 Docker avancé

Figure 102 ANSSI MOOC

XVI.4 Annexe – Matérielles utilisés pour la mise en place du cloud privé

Les images suivantes présentent l'infrastructure physique mise en place par le porteur du projet afin de concevoir et tester le cloud privé de NovaTechSolutions dans un environnement représentatif d'une situation réelle en entreprise.

Cette infrastructure personnelle a été conçue comme une plateforme de travail professionnelle, reproduisant les contraintes techniques, organisationnelles et sécuritaires d'un environnement de production.

Elle comprend notamment les serveurs Proxmox VE, les équipements réseau ainsi que les dispositifs de sécurité nécessaires pour garantir la disponibilité, la performance et la sécurité de la plateforme.

Inventaire matériel – Infrastructure NovaTechSolutions

Catégorie	Équipement	Modèle / Configuration	Quantité	Rôle	Criticité
Compute	Nœuds Hyperviseurs	MSI MAG B550 TOMAHAWK MAX WIFI AMD Ryzen 9 5900X 128 Go RAM RAID 5 – 3x1To SSD Watercooling ASUS ROG RYUO IV SLC 360	5	Cluster Proxmox (3) Proxmox Backup Server (1) Proxmox Datacenter Manager (1)	Critique
Sécurité	Appliances Firewall HA	Netgate 6100 – Appliance pfSense+ Ports 10Gb SFP+ VPN haute performance Support CARP / Sync	2	Cluster haute disponibilité (Active/Passive) Protection périmétrique Segmentation réseau	Critique
Réseau	Switchs managés L3	Cisco CBS250-24T-4G VLAN, routage statique Administration Web / SSH	2	Redondance réseau Segmentation VLAN Backbone du cluster	Critique
Accès Internet	Routeur opérateur	Freebox Delta Débit jusqu'à 10 Gbps Connectivité SFP+	1	Accès WAN Publication des services VPN externe	Élevée
Postes & Exploitation	Stations administrateurs	Écrans Xiaomi 29.5" UltraWide	5	Supervision Administration Pilotage du cloud privé	Moyenne
Stockage	Infrastructure Ceph / RAID	Stockage distribué + RAID matériel	Cluster	Haute disponibilité des données Tolérance aux pannes	Critique

Figure 103 Inventaire matériels

Figure 104 Cluster - Serveur Proxmox VE. (3 nœuds)

Figure 105 Cluster OPNSense & Switch

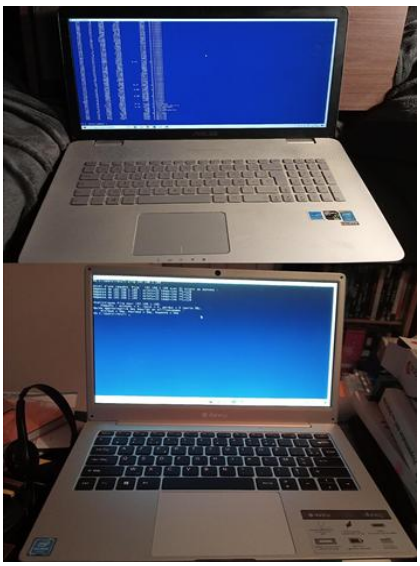


Figure 106 Postes utilisateurs

Figure 107 Serveur Proxmox Backup

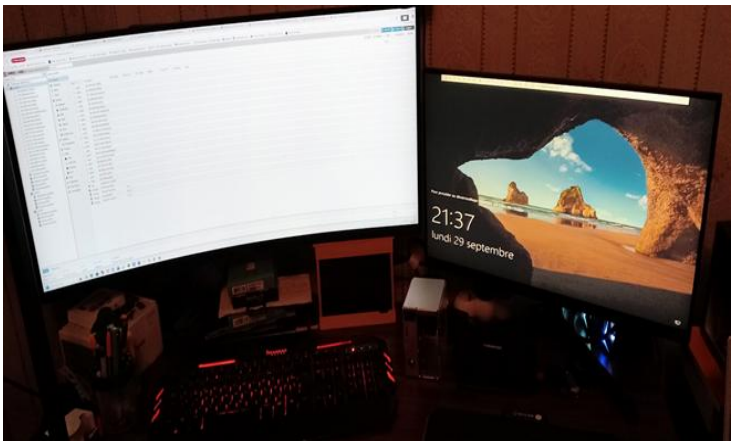


Figure 108 Serveur Proxmox Backup – SRV ADDS

Figure 109 Serveur Proxmox Datacenter

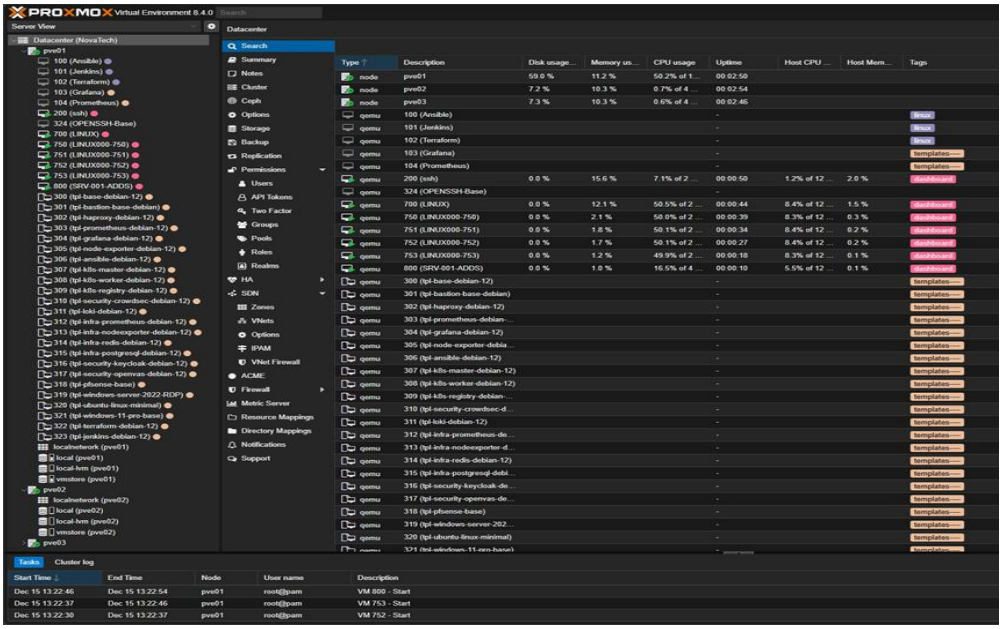


Figure 110 Dashboard Proxmox VE

XVI.5 Annexe techniques du Dashboard

Les annexes suivantes présentent des extraits ciblés du code source du dashboard Cloud Privé développé dans le cadre du projet NovaTechSolutions. Les extraits ont été volontairement sélectionnés afin d'illustrer les mécanismes clés de sécurité, d'automatisation et d'orchestration, sans alourdir le dossier par l'intégralité du code.

Annexe A – Sécurisation de l'accès au Dashboard (Authentification MFA)

Objectif : Garantir un accès sécurisé au Dashboard d'administration du cloud privé.

Le Dashboard implémente une authentification forte reposant sur une double étape :

- Authentification par identifiant et mot de passe.
- Validation par second facteur (2FA) via un code TOTP (Time-based One-Time Password).

Cette approche permet de réduire significativement les risques d'accès non autorisés, même en cas de compromission des identifiants.

```
ADMIN_USERNAME = "nebtech_admin"
ADMIN_PASSWORD = "********"
TOTP_SECRET = pyotp.random_base32()
@app.route("/login", methods=["GET", "POST"])
def login():


    if request.method == "POST":
        if (
            request.form.get("username") == ADMIN_USERNAME
            and request.form.get("password") == ADMIN_PASSWORD
        ):
            session["pre_2fa"] = True
            return redirect("/2fa")
    return render_template("login.html")

@app.route("/2fa", methods=["GET", "POST"])
def twofa():
    totp = pyotp.TOTP(TOTP_SECRET)
    if request.method == "POST":
        if totp.verify(request.form.get("code")):
            session["user"] = ADMIN_USERNAME
            return redirect("/")
```

Valeur ajoutée au projet : sécurité renforcée, conformité aux bonnes pratiques entreprise, maîtrise des accès administrateurs.

Annexe B – Supervision du cluster Proxmox via API REST

Objectif : Fournir une supervision centralisée et en temps réel du cluster Proxmox.

Le dashboard interroge l'API REST Proxmox afin de collecter les métriques essentielles (CPU, mémoire, disponibilité des nœuds). Cette approche évite toute manipulation manuelle sur les hyperviseurs.

```
response = requests.get(
    f"https://{node_ip}:8006/api2/json/nodes/{node_name}/status",
    headers=HEADERS_PVE,
    verify=False,
    timeout=4,
)
```

Valeur ajoutée au projet : supervision temps réel, centralisation des informations, réduction des opérations manuelles.

Annexe C – Orchestration de la configuration via Ansible

Objectif : Automatiser la configuration post-déploiement des machines virtuelles.

Après la création des VM, le dashboard permet d'exécuter des playbooks Ansible à la demande afin d'assurer le durcissement, l'installation de services ou les opérations de maintenance.

```
result = subprocess.check_output(
    [
        "ssh",
        "root@192.168.1.134",
        "ansible-playbook /etc/ansible/playbooks/deploy.yml -i /etc/ansible/inven-
tory.ini",
    ],
    stderr=subprocess.STDOUT,
    text=True,
)
```

Valeur ajoutée au projet : homogénéité des configurations, réduction des erreurs humaines, automatisation complète du cycle de vie.

Annexe D – Provisioning des machines virtuelles avec Terraform

Objectif : Mettre en œuvre le principe d'Infrastructure as Code (IaC).

Terraform est utilisé pour créer dynamiquement les machines virtuelles sur le cluster Proxmox à partir de templates standardisés. Les déploiements sont éphémères et entièrement automatisés.

```
output = ""
output += run(["terraform", "init", "-upgrade"])
output += run(["terraform", "apply", "-auto-approve"])
```

Valeur ajoutée au projet : déploiement rapide, reproductible et traçable des environnements.

Annexe E – Sécurisation HTTPS du dashboard

Objectif : Protéger les échanges entre les utilisateurs et le dashboard.

Le dashboard Flask est configuré pour fonctionner exclusivement en HTTPS, garantissant le chiffrement des flux et la confidentialité des données échangées.

```
if __name__ == "__main__":
    app.run(
        host="0.0.0.0",
        port=443,
        ssl_context=("dashboard.pem", "dashboard.key")
    )
```

Valeur ajoutée au projet : conformité aux standards de sécurité, protection contre les attaques de type interception (MITM).

Annexe F – Extraits de code du Dashboard Cloud (Python / Flask)

Extrait 1 – Initialisation du Dashboard Flask et sécurité

```
from flask import Flask
from flask_login import LoginManager
from flask_talisman import Talisman

app = Flask(__name__)
app.secret_key = os.environ.get("FLASK_SECRET_KEY")

Talisman(app, content_security_policy=None)

login_manager = LoginManager()

login_manager.init_app(app)
login_manager.login_view = "login"
```

Cet extrait illustre l'initialisation du dashboard Cloud développé en Python avec Flask.
L'application est sécurisée par HTTPS grâce à Flask-Talisman et repose sur une gestion des sessions utilisateurs via Flask-Login.
Cette approche garantit un accès contrôlé au dashboard, condition indispensable pour une interface pilotant des déploiements d'infrastructure critiques.

Extrait 2 – Route de déploiement automatisé via Terraform

```
@app.route("/deploy", methods=["POST"])
```

```
@login_required
def deploy_vm():
    subprocess.run(
        ["terraform", "apply", "-auto-approve"],
        cwd="/opt/terraform",
        capture_output=True,
        text=True
    )
    return redirect(url_for("status"))
```

Cette route illustre le cœur du projet : le déclenchement automatisé du provisioning des machines virtuelles via Terraform.
L'utilisateur, authentifié, initie le déploiement depuis le dashboard. Le provisioning est entièrement automatisé, reproductible et traçable, conformément aux principes de l'Infrastructure as Code.

Extrait 3 – Intégration Ansible / Jenkins pour la post-configuration

```
@app.route("/ansible/run/<playbook>")
@login_required
def run_playbook(playbook):
    subprocess.Popen(
        ["ansible-playbook", f"{playbook}.yml"],
        cwd="/opt/ansible"
    )
    return "Playbook lancé"
```

Après la création des machines virtuelles, Ansible est utilisé pour assurer la configuration automatique : durcissement, installation de services et standardisation des environnements.
Cette séparation claire entre provisioning (Terraform) et configuration (Ansible) garantit la maintenabilité et la robustesse de la solution.

Extrait 4 – Récupération des logs et supervision

```
@app.route("/logs")
@login_required
def logs():
    result = subprocess.run(
        ["journalctl", "-n", "50", "--no-pager"],
        capture_output=True,
        text=True
    )
    return render_template("logs.html", logs=result.stdout)
```

Cet extrait montre l'intégration de la supervision directement dans le dashboard.
Les journaux systèmes sont consultables sans accès SSH, ce qui améliore la visibilité opérationnelle tout en limitant les risques de manipulation directe sur les serveurs. Ces extraits démontrent la cohérence globale du projet, la maîtrise des outils DevOps et des bonnes pratiques de sécurité, ainsi que la capacité à concevoir une infrastructure cloud privée moderne, automatisée et sécurisée.

Annexe G – Organisation et arborescence des outils d'automatisation

Cette annexe a pour objectif de présenter l'organisation des répertoires utilisés pour l'automatisation du cloud privé NovaTechSolutions.
Elle permet au lecteur de comprendre rapidement la structuration du projet, la séparation des rôles entre les différents outils (Terraform, Ansible, Jenkins, Dashboard Flask) et la logique d'industrialisation retenue.

La structuration des fichiers est un élément essentiel pour garantir la maintenabilité du projet, faciliter les évolutions futures et assurer une exploitation claire et sécurisée.

G.1 Arborescence globale du projet

```
/opt/cloud-dashboard/
├── flask/
│   ├── app.py
│   ├── requirements.txt
│   └── templates/
```

```
│   │   ├── index.html
│   │   ├── login.html
│   │   ├── dashboard.html
│   │   └── logs.html
│   └── static/
│       ├── css/
│       └── js/
│
├── terraform/
│   ├── main.tf
│   ├── provider.tf
│   ├── variables.tf
│   ├── terraform.tfvars
│   ├── outputs.tf
│   └── modules/
│       └── vm_proxmox/
│           ├── main.tf
│           ├── variables.tf
│           └── outputs.tf
│
├── ansible/
│   ├── inventories/
│   │   └── production.ini
│   ├── playbooks/
│   │   ├── deploy_apache.yml
│   │   ├── deploy_docker.yml
│   │   ├── maintenance.yml
│   │   └── ping.yml
│   ├── roles/
│   │   ├── common/
│   │   ├── hardening/
│   │   └── webserver/
│   └── ansible.cfg
│
├── jenkins/
│   └── Jenkinsfile
│
├── logs/
│   ├── terraform.log
│   ├── ansible.log
│   └── dashboard.log
│
└── README.md
```

Description par composant

Dashboard Flask (Python)

Le dossier flask/ contient l'interface web du cloud privé.

Il centralise les interactions utilisateurs et déclenche les actions d'automatisation.

- app.py : cœur applicatif, routes, sécurité, orchestration
- Templates/ : vues HTML du dashboard
- static/ : styles CSS et scripts JavaScript

Rôle : point d'entrée unique, sécurisé et ergonomique.

Terraform – Infrastructure as Code

Le dossier terraform/ regroupe l'ensemble des fichiers nécessaires au provisioning automatisé des machines virtuelles sur le cluster Proxmox.

- provider.tf : configuration du provider Proxmox
- main.tf : définition des ressources (VM, réseaux, stockage)
- variables.tf / terraform.tfvars : paramétrage dynamique
- modules/ : factorisation et réutilisation du code

Rôle : création, modification et suppression reproductibles des VM.

Ansible – Configuration et déploiement applicatif

Le dossier Ansible/ est dédié à la configuration post-déploiement.

- inventories/ : définition des hôtes cibles
- playbooks/ : scénarios d'installation et de maintenance
- roles/ : standardisation des configurations
- ansible.cfg : paramètres globaux d'exécution

Rôle : automatiser les configurations, assurer l'homogénéité et le durcissement.

Jenkins – Orchestration CI/CD

Le dossier Jenkins/ contient les pipelines d'orchestration.

- jenkinsfile : enchaînement Terraform → Ansible → validation

Rôle : assurer la cohérence des déploiements et la traçabilité.

Logs & traçabilité

Le dossier logs/ centralise les journaux d'exécution :

- Retours Terraform
- Exécution des playbooks Ansible
- Événements du dashboard

Rôle : supervision, audit et diagnostic.

Cette structuration permet une séparation claire des responsabilités, une lecture rapide pour un nouvel intervenant, une évolutivité naturelle du projet ainsi qu'une industrialisation conforme aux bonnes pratiques DevOps.

---

coolLibri.com

IMPRIMÉ EN FRANCE
Achevé d'imprimer en mars 2026
chez Messages SAS
111, rue Nicolas Vauquelin - 31100 Toulouse
05 31 61 60 42
www.coollibri.com