Page de présentation à faire

1. Introduction

1.1. Contexte et objectifs du projet

Le présent projet s'inscrit dans le cadre de la préparation au titre professionnel **Administrateur d'Infrastructure Sécurisée (AIS)**. L'objectif est de concevoir, déployer et maintenir une infrastructure réseau et applicative représentative d'un environnement de production réel, tout en intégrant des mesures de sécurité conformes aux bonnes pratiques en vigueur.
L'infrastructure mise en place doit répondre à deux finalités principales :

- **Pédagogique** : démontrer la capacité à concevoir une architecture sécurisée et fonctionnelle, capable d'évoluer et de résister à des scénarios d'attaques réalistes.
- **Technique** : fournir une base opérationnelle documentée qui illustre la maîtrise des principaux services réseau (authentification, stockage, sauvegarde, applicatifs métiers, supervision) et leur sécurisation.

1.2. Présentation de la clinique Cleanic

Le scénario repose sur une structure fictive, la **clinique Cleanic**, établissement de santé nécessitant une infrastructure informatique fiable pour assurer la continuité de ses activités. Les besoins identifiés couvrent plusieurs volets :

- **Gestion des identités et des accès** pour les médecins, infirmiers, services administratifs, support et IT.

- **Hébergement des données médicales sensibles** (rendez-vous, dossiers médicales, prescriptions) sur une base de données et dossiers partagés.

- **Partage de fichiers et collaboration interne** entre les différents services.

- **Accès distant sécurisé** pour l'IT et le personnel en télémédecine.

- **Supervision et détection des incidents** afin de répondre rapidement aux menaces.

La clinique Cleanic doit donc s'appuyer sur une infrastructure segmentée, disponible et résiliente, intégrant des mécanismes de protection avancés, tout en restant adaptée à la taille et aux moyens d'un établissement de santé de dimension moyenne.

1.3. Contraintes réglementaires et choix assumés

Les activités de la clinique impliquent la **gestion de données de santé sensibles**, soumises au **Règlement Général sur la Protection des Données (RGPD)** ainsi qu'aux recommandations de l'**ANSSI** concernant la sécurité des systèmes d'information de santé.
Ces contraintes imposent :

- la mise en place de contrôles d'accès stricts,
- l'authentification forte et la traçabilité des actions,
- le chiffrement des communications sensibles (TLS, LDAPS, SQL chiffré dans le backend),
- la protection contre les intrusions et les tentatives de compromission.

Dans le cadre de ce projet, certains choix ont volontairement été simplifiés afin de rester cohérents avec un environnement de formation :

- **Haute disponibilité** non implémentée, considérée comme surdimensionnée (« overkill ») et coûteuse dans ce contexte.
- **Certificats autosignés** utilisés en lab, alors qu'en production, l'usage de certificats émis par une autorité de confiance serait impératif.
- **RAID 10 non implémenté**, car nécessitant plusieurs disques physiques.
- **Cloud**, car nécessitant un réel budget, ce qui est non-nécessaire.

Ces arbitrages permettent de démontrer les compétences techniques attendues tout en distinguant les aspects pédagogiques des contraintes d'un déploiement en production.

1.4. Portée et périmètre de l'infrastructure

L'infrastructure déployée couvre les services essentiels : gestion des identités, base de données, application web sécurisée, stockage des fichiers, sauvegardes redondantes, système de relais, monitoring centralisé et contrôles de sécurité réseau.
Elle est conçue pour refléter une infrastructure maintenable et réaliste, adaptée à un établissement de santé de taille moyenne, tout en respectant les contraintes

budgétaires qui ont guidé les choix techniques et exclu certaines briques jugées non prioritaires dans ce contexte (par ex. haute disponibilité).

2. Analyse des besoins

2.1. Besoins métiers

- **Gestion des patients** : stockage sécurisé des données médicales (identité, diagnostics, rendez-vous).

- **Application web** : Présentation de la clinique et accès professionnel simple pour le personnel afin de consulter et gérer les rendez-vous.

- **Partage de documents** : mise à disposition de dossiers médicaux via un serveur de fichiers avec accès basé sur les rôles.

- **Centralisation des comptes** : gestion des utilisateurs et des permissions via Active Directory.

- **Continuité des soins** : assurer la disponibilité minimale des systèmes critiques (application, base de données, AD, File Server), avec relais pour une restauration rapide.

2.2. Besoins techniques

- **Sécurité réseau** : segmentation par VLAN, pfSense avec règles strictes, DMZ pour l'exposition limitée au web.

- **Accès distant sécurisé** : VPN pour le personnel autorisé.

- **Supervision et alerting** : Détection d'anomalies, alertes sur tentatives d'intrusion, erreurs système ou actions suspectes.

- **Sauvegardes** : backups journaliers de la base de données et du serveur de fichiers et un stockage extérieur pour portabilité et 3-2-1.

- **Service externalisé**: utilisation d'une plateforme cloud (Medical Cloud) spécialisée pour héberger les services de santé avec sécurité renforcée, scalabilité, haute disponibilité et conformité réglementaire.

- **Tolérance aux pannes** : pfSense master/backup, redémarrage automatique des services critiques et relais via .

- **Gestion IT** : postes administrateurs dédiés, accès via SSH/RDP aux serveurs et équipements réseau.

2.3. Besoins réglementaires

Le projet Cleanic respecte les exigences clés du RGPD pour la protection des données de santé :

- **Article 5 – Principes relatifs au traitement des données** : minimisation des données collectées et finalité clairement définie.

- **Article 20 – Portabilité des données** : les données patients sont répliquées sur le *Medical Cloud*, permettant leur restauration en cas de panne et assurant le respect de la règle de sauvegarde 3-2-1 (3 copies, 2 supports différents, 1 hors site).

- **Article 25 – Protection des données dès la conception et par défaut** : segmentation réseau, contrôle d'accès strict, mesures de sécurité intégrées.

- **Article 32 – Sécurité du traitement** : chiffrement, sauvegardes locales et cloud, contrôle d'accès, durcissement des serveurs et monitoring centralisé.

- **Article 33 – Notification en cas de violation de données** : alerting et procédures internes de réponse aux incidents.

Les autres dispositions RGPD sont respectées implicitement ou ne sont pas directement applicables à l'infrastructure mise en place.

3. Network Architecture

3.1. Architecture globale

L'infrastructure réseau de Cleanic a été conçue selon une logique en **couches cloisonnées** afin d'assurer sécurité, maintenabilité et résilience.

- La **couche WAN** permet uniquement la sortie vers Internet via le pare-feu pfSense, avec filtrage strict et redondance grâce à un cluster maître/esclave.

- La **couche DMZ** héberge le frontend web, seul composant exposé publiquement. Il est isolé des autres ressources internes et soumis à des règles de communication limitées.

- La **couche LAN interne** regroupe les VLANs métiers : base de données, backend, Active Directory, serveur de fichiers, administration IT, employés, sauvegardes et monitoring. Chaque VLAN est strictement limité à son usage.

- Un **VLAN dédié au monitoring (99)** centralise les journaux et événements de sécurité via Wazuh.

- Enfin, un **relais Medical Cloud** est intégré au design. Il permet de stocker une copie des sauvegardes en mode hors-site, garantissant la règle 3-2-1 et la reprise d'activité en cas de sinistre.

Cette approche permet d'isoler les services critiques tout en gardant une vision maintenable et adaptée aux besoins d'une clinique de taille moyenne.

3.2. Segmentation VLAN

VLAN	Usage	Sous-réseau	Remarques
10	DMZ (Frontend)	192.168.10.0/28	Application web exposée (HTTPS)

20	Backend	192.168.20.0/28	Communication vers DB et AD
30	Database	192.168.30.0/28	PostgreSQL, accès uniquement depuis backend
40	IT/Admin	192.168.40.0/28	Postes dédiés à l'administration (SSH/RDP)
50	File Server	192.168.50.0/28	Partage fichiers (SMB, LDAP)
60	Employés	192.168.60.0/28	Postes de travail, accès restreint
70	Active Directory	192.168.70.0/28	Gestion des identités, LDAPs, Kerberos
80	Backup NAS	192.168.80.0/28	Sauvegardes locales chiffrées
99	Monitoring	192.168.99.0/28	Centralisation logs via Wazuh

Le **switch L2** gère cette segmentation VLAN et communique avec pfSense via des trunks en LACP pour assurer bande passante et redondance.

3.3. Flux réseau critiques

Les flux réseau sont gérés par **pfSense** selon une approche **"deny by default"**, ne permettant que les communications strictement nécessaires au fonctionnement des services. Cette logique suit les bonnes pratiques de l'ANSSI en matière de cloisonnement, de moindre privilège et de réduction de la surface d'attaque. De plus,

pfSense fonctionne en mode **stateful**, ce qui signifie qu'il suit l'état des connexions réseau (TCP, UDP, etc.) : lorsqu'un paquet entrant correspond à une connexion initiée depuis l'intérieur du réseau, il est automatiquement autorisé, tandis que tout paquet non lié à une session existante est bloqué. Ce mécanisme assure une protection fine et dynamique, tout en simplifiant la gestion des règles de filtrage et en renforçant la sécurité globale du périmètre.

Source	**Destination**	**Port/Service**	**Justification**
Internet	DMZ (Frontend)	TCP 443	Accès HTTPS des patients/médecins – seul service exposé publiquement
Internet	DMZ (Frontend)	UDP 51820	VPN WireGuard pour accès distant sécurisé (tunnel chiffré)
DMZ (Frontend)	Backend	TCP 3000	Transmission contrôlée des requêtes applicatives, filtrée par firewall
Backend	Database	TCP 5432 (chiffré)	Requêtes SQL vers la base patients, aucun autre flux ouvert
Backend	AD	TCP 636 (LDAPS)	Authentification sécurisée des utilisateurs applicatifs
Database	Backup NAS (192.168.80.2)	2049 (NFS)	Sauvegardes locales régulières
File Server	AD	TCP 88, 636	Intégration Kerberos et LDAP pour gestion des accès

File Server	Employés	TCP 445	Accès contrôlé (RBAC, GPO) aux partages de fichiers
Employés	AD	TCP/UDP 53, 88, 636	Résolution DNS interne et authentification Kerberos/LDAPS
Employés	DMZ (Frontend)	TCP 443	Accès interne à l'application web
Backup NAS (x.x.80.3)	File Server	TCP 445 (SMB)	Sauvegardes locales régulières
Tous les VLANs	Monitoring (Wazuh)	TCP/UDP 1514	Collecte de logs (tentatives d'accès, élévations de privilège, erreurs systèmes)
IT/Admin	Tous les VLANs autorisés	TCP 22/3389	Accès d'administration restreint et journalisé
VPN (WG)	LAN interne	Ports spécifiques	Accès nomade, profilés par règles firewall précis

Narratif complémentaire :

- Les **flux applicatifs critiques** (frontend ↔ backend ↔ DB) sont restreints aux seuls ports nécessaires conformément au principe de **moindre privilège**.

- L'**Active Directory** est cloisonné dans un VLAN dédié, jouant un rôle central de gestion des identités. Les flux sont chiffrés via LDAPS/Kerberos pour limiter les risques d'écoute réseau.

- Le **Wazuh manager (VLAN 99)** est en position d'observateur, recevant des logs de toutes les zones pour corrélation et détection d'incidents (notamment injection SQL, SSH/RDP, élévation de privilèges, redémarrage de services

critiques).

- L'**accès distant** est strictement limité au VPN WireGuard. Les clés privées/publiques sont gérées par l'IT et seules les adresses IP de confiance peuvent se connecter.

- Le Medical Cloud n'est pas intégré aux flux temps réel, mais il sert à la fois de **cible de sauvegarde hors-site** et de **relais opérationnel en cas de panne locale**. Cette approche réduit son exposition réseau tout en renforçant la résilience globale de l'infrastructure.

Cette organisation respecte une logique **EBIOS.**

4. Choix Technologiques et Techniques

4.1. Principes directeurs

- **Sécurité by design** (segmentation, moindre privilège, chiffrement en transit, durcissement OS).

- **Simplicité & maintenabilité** (standards de marché, peu de technos différentes : Debian/Windows).

- **Réalisme budgétaire** (pas de haute disponibilité car estimé "overkill"; redondance ciblée : pfSense master/backup, backups 3-2-1 via Medical Cloud).

- **Conformité RGPD** (art. 5/20/25/32/33) et bonnes pratiques ANSSI (cloisonnement, surveillance, EBIOS en fil conducteur).

4.2. Frontend – VLAN 10 (192.168.10.0/28)

Le Frontend constitue la porte d'entrée externe de l'infrastructure et repose sur une stack Debian + Nginx, combinant serveur web et reverse-proxy. Nginx a été retenu pour sa capacité à centraliser l'accès aux applications critiques de la clinique, telles que la gestion des patients, le portail de rendez-vous ou l'imagerie médicale, tout en offrant sécurité, performance et haute disponibilité. Il masque la topologie interne, effectue le SSL termination pour soulager les serveurs backend, filtre les requêtes

suspectes et peut intégrer un WAF (ex. ModSecurity) afin de se conformer aux normes HDS et RGPD. Cette configuration assure une disponibilité optimale même sur du matériel modeste, indispensable dans un environnement médical où chaque minute compte.

L'interface utilisateur repose sur du JavaScript statique, garantissant des pages légères, rapides à charger et faciles à maintenir. L'usage de JavaScript statique limite la surface d'attaque côté client tout en permettant des interactions essentielles telles que la validation des formulaires, la gestion des tokens JWT ou la prévention des tentatives de bruteforce.

Le Frontend héberge deux services distincts : la page vitrine publique accessible en HTTPS et le portail professionnel, qui constitue le point d'accès principal aux applications métiers et est protégé par une authentification stricte. Pour renforcer la sécurité applicative, plusieurs mécanismes sont déployés : l'authentification repose sur des JWT purgés automatiquement à l'expiration, les en-têtes HTTP sont configurés pour limiter la mise en cache et le stockage des informations sensibles (no-store, no-cache, Authorization: Bearer), les appels API sont protégés contre les attaques CSRF via des tokens dédiés, et Fail2Ban, couplé aux logs Nginx, bloque les tentatives répétées d'accès. La validation côté client et serveur limite l'exposition aux attaques XSS et aux injections simples.

Au niveau réseau, le Frontend est isolé en VLAN 10 et n'expose vers Internet que le port 443/TCP. Les flux vers le Backend sont strictement limités à TCP/3000 via le firewall pfSense, garantissant une surface d'attaque minimale et une séparation claire des responsabilités entre les couches applicatives (cf. 3.3).

4.3. Backend – VLAN 20 (192.168.20.0/28)

Le Backend constitue le cœur applicatif de l'infrastructure et repose sur Debian avec Node.js/Express. Ce choix a été motivé par sa capacité à gérer efficacement des flux simultanés, sa compatibilité native avec JSON et son large écosystème de modules sécurisés. Il assure la logique métier, la validation des utilisateurs via Active Directory, l'émission et la vérification des JWT, ainsi que la communication avec la base de données et les services internes.

L'utilisation de Node.js permet d'exécuter du JavaScript côté serveur, assurant une homogénéité avec le Frontend et simplifiant la maintenance en réduisant la complexité de la base de code et en facilitant la réutilisation des modules côté client et serveur. L'écosystème npm offre des modules dédiés à la sécurité, à l'audit et à la gestion des utilisateurs, et les mises à jour fréquentes garantissent un environnement robuste.

La sécurité applicative repose sur plusieurs mesures : les secrets critiques sont gérés via des fichiers `.env`, avec arrêt immédiat si une variable obligatoire est manquante. Le parsing JSON est limité à 1 MB pour réduire la surface d'attaque, et la gestion centralisée des erreurs 404/500 empêche la divulgation d'informations sensibles. Les requêtes SQL vers PostgreSQL sont paramétrées pour éviter les injections, et la communication avec Active Directory s'effectue en LDAPS (TCP 636). En cas de crash, le backend redémarre automatiquement toutes les cinq secondes, tandis que Wazuh supervise le système en continu pour détecter anomalies, tentatives d'accès suspectes et erreurs runtime.

Au niveau réseau, le Backend est isolé et accessible uniquement depuis le Frontend via TCP 3000. Les flux vers la base de données s'effectuent sur TCP 5432 avec chiffrement côté serveur, et vers Active Directory sur TCP 636. Cette isolation stricte garantit la sécurité et la séparation des responsabilités entre les couches applicatives (cf 3.3).

Node.js/Express a été retenu pour sa gestion performante des Entrées/Sorties concurrentes, adaptée aux applications critiques multi-utilisateurs, pour la création d'API REST sécurisées et la possibilité de communication en temps réel via WebSocket pour les notifications urgentes. Son écosystème riche via npm permet l'intégration de modules pour la sécurité, l'audit et la gestion des utilisateurs.
Les alternatives considérées, Python/Flask et Java/Spring, étaient respectivement moins adaptées aux flux intensifs ou trop lourdes et complexes pour le matériel utilisé. Cette approche garantit performance, sécurité et facilité de maintenance, tout en assurant une intégration fluide avec le Frontend et la base de données, répondant pleinement aux besoins métiers et techniques de la clinique..

4.4. Database – VLAN 30 (192.168.30.0/28)

La base de données stocke les rendez-vous patients/personnels de la clinique. Elle repose sur PostgreSQL, déployée sur Debian et isolée via Docker pour garantir la séparation et la portabilité des données. PostgreSQL a été retenu pour sa stricte conformité aux règles ACID, assurant une intégrité maximale des informations critiques concernant les rendez-vous et les utilisateurs autorisés (personnel médical et administratif).

Cette base offre des fonctionnalités avancées utiles pour la gestion des rendez-vous : index optimisés pour les recherches temporelles et relationnelles, requêtes SQL performantes pour des consultations multiples et jointures entre patients et personnel. Elle permet également un contrôle d'accès très précis, avec des permissions configurables par table, colonne et ligne via Row Level Security, limitant strictement l'accès aux données selon le rôle des utilisateurs. Des

extensions comme pgAudit sont utilisées pour auditer les accès et garantir la conformité aux exigences HDS et RGPD.

Les flux réseau sont strictement restreints : seuls le Backend et les postes IT/Admin autorisés peuvent communiquer avec la base sur le port TCP 5432, avec chiffrement côté serveur. Cette séparation réseau, combinée à la supervision Wazuh, assure que toute tentative d'accès non autorisée ou anomalie est détectée et remontée rapidement (cf 3.3).

Enfin, PostgreSQL a été retenu plutôt que MySQL/MariaDB pour sa robustesse et sa conformité ACID stricte, et plutôt que des solutions NoSQL qui ne permettent pas le même niveau de garantie d'intégrité transactionnelle pour les rendez-vous critiques. Ce choix assure sécurité, fiabilité et évolutivité de l'application de planification médicale.

4.5. Active Directory – VLAN 70 (192.168.70.0/28)

L'Active Directory constitue le socle de gestion des identités et des accès de l'infrastructure. Déployé sur **Windows Server 2022**, il centralise l'administration des comptes utilisateurs, des groupes et des permissions, assurant un provisioning rapide et une désactivation immédiate en cas de départ ou de perte d'accès. Cette centralisation est particulièrement critique en environnement médical, où les logiciels métiers (gestion des patients, imagerie, facturation) reposent quasi exclusivement sur Windows et nécessitent une intégration native.

L'AD offre une précision avancée dans la gestion des droits : politiques de mots de passe strictes, support natif du MFA (Multi-Factor Authentication), affectation des autorisations par rôle ou service (ex. accès limité aux dossiers médicaux pour les seuls médecins). Les **Group Policy Objects (GPO)** renforcent cette approche en appliquant automatiquement des politiques de sécurité uniformes : verrouillage automatique des sessions inactives, blocage des périphériques non autorisés, restrictions sur PowerShell/CMD, ou encore durcissement de l'accès RDP réservé uniquement au service IT. Ces mécanismes réduisent le risque d'intrusion, améliorent la conformité RGPD/HDS et garantissent la cohérence opérationnelle sur l'ensemble du parc.

Sur le plan organisationnel, l'AD est structuré en **Unités Organisationnelles (OU)** représentant les services clés : *Médical* (médecins, infirmiers, secrétariat), *Support* (finances, restauration, logistique), *IT*, et *Administratif*. Des OU distinctes sont également définies pour les postes de travail par service, permettant un déploiement ciblé des GPO. L'usage combiné de **groupes globaux** (rattachés aux rôles métiers) et de **groupes locaux de domaine** (attribuant des ressources spécifiques à une

clinique donnée) optimise la gestion des accès et la réutilisabilité des règles dans un environnement multi-cliniques.

La sécurité et la traçabilité sont renforcées par l'audit natif d'Active Directory, intégré à **Wazuh** pour centraliser les journaux (logons réussis/échoués, modifications de GPO, tentatives suspectes d'accès). Cette intégration SIEM assure une détection proactive des anomalies et permet de démontrer la conformité lors des audits.

Le choix d'Active Directory s'impose par rapport à une solution LDAP Linux : bien que possible techniquement, cette dernière est moins intuitive pour les équipes non spécialisées, ne propose pas nativement les GPO, et n'offre pas la même compatibilité avec les logiciels métiers hospitaliers. De plus, la capacité d'AD à gérer plusieurs milliers d'utilisateurs, associée à la mise en place de **contrôleurs de domaine redondants**, garantit performance, haute disponibilité et continuité de service, essentielles dans un contexte médical.

Enfin, la politique de mots de passe a été définie en conformité avec les recommandations de l'ANSSI : longueur minimale de 12 à 16 caractères, combinaison de majuscules, minuscules, chiffres et caractères spéciaux, renouvellement tous les 90 jours. Les mots de passe temporaires sont générés de manière aléatoire et transmis de façon sécurisée, obligeant l'utilisateur à les modifier lors de sa première connexion. Les bases de données de mots de passe sont chiffrées, et une politique complémentaire interdit l'enregistrement automatique dans les navigateurs. En parallèle, une sensibilisation régulière aux attaques de type phishing et ingénierie sociale est organisée pour renforcer le facteur humain, souvent vecteur d'intrusion.

Ainsi, l'Active Directory constitue un **pilier de la sécurité et de la gouvernance des accès**, combinant centralisation, robustesse, compatibilité logicielle et traçabilité, tout en respectant les exigences réglementaires applicables au domaine de la santé.

4.6. File Server – VLAN 50 (192.168.50.0/28)

Le serveur de fichiers héberge l'ensemble des données critiques de la clinique, organisées par service et rôle : dossiers patients et diagnostics (médecins et infirmiers), finances (direction), plannings patients (secrétaires, infirmiers, médecins), plannings internes (tout le personnel) et transmissions médicales (médecins et infirmiers). Les permissions sont strictement adaptées aux métiers : par exemple, les médecins disposent de droits de lecture/écriture sur les diagnostics, tandis que les infirmiers ont uniquement un accès en lecture. Cette approche garantit que chaque utilisateur ne peut accéder qu'aux informations nécessaires à son activité, limitant ainsi les risques d'exposition ou de modification accidentelle des données sensibles.

Déployé sur **Windows Server 2022**, il exploite le protocole **SMB (Server Message Block)**, standard éprouvé dans les environnements Windows et parfaitement intégré à l'Active Directory. Ce choix assure une gestion fine des permissions via les **ACL** (Access Control List) **NTFS** et les groupes AD, garantissant que seuls les utilisateurs habilités accèdent aux données correspondant à leur rôle.

Les services fournis incluent le partage multi-appareils (postes de travail et terminaux mobiles), l'édition collaborative de documents, ainsi que l'intégration directe avec LDAP/AD pour une administration centralisée des droits. Le chiffrement est activé côté serveur et peut être étendu côté client, renforçant la confidentialité des données sensibles.

Sur le plan réseau, l'accès est strictement restreint : seuls les postes situés sur le **VLAN 60 (employés)** peuvent communiquer avec le serveur via le port **TCP 445**. Les flux vers les environnements externes sont bloqués, limitant l'exposition et réduisant le risque d'intrusion. Les sauvegardes régulières sont déportées vers un **NAS hébergé dans le VLAN 80**, assurant la résilience et la continuité de service en cas de défaillance ou de sinistre.

Pour renforcer la sécurité, plusieurs recommandations Microsoft et ANSSI sont appliquées : activation du **SMB signing** et du **chiffrement SMB**, limitation à **NTLMv2 uniquement**, et désactivation des versions antérieures considérées vulnérables (SMBv1). Ces mesures garantissent l'intégrité des échanges et la protection des identifiants lors de l'authentification.

Le choix de Windows Server 2022 avec SMB s'est imposé face à l'alternative Samba sous Linux. Bien que Samba offre une solution open-source, son intégration avancée avec les ACL Active Directory est plus complexe et requiert une expertise spécifique. Windows SMB offre en revanche une compatibilité native, une administration plus intuitive et une interopérabilité immédiate avec l'écosystème Windows déjà en place dans la clinique.

Ce File Server combine ainsi **centralisation, sécurité et intégration fluide** avec l'Active Directory, tout en respectant les contraintes réglementaires liées à la protection des données médicales.

4.7. IT/Admin – VLAN 40 (192.168.40.0/28)

Le VLAN IT/Admin constitue le **bastion interne de l'équipe informatique**, regroupant l'ensemble des postes d'administration et outils de gestion pour superviser et maintenir l'infrastructure de la clinique. La stack combine deux **postes administrateurs dédiés** (1 Debian et 1 Windows Server), servant de points

centraux pour l'administration des systèmes critiques, ainsi que des postes utilisateurs pour le reste de l'équipe IT.

- Le **poste Debian** est utilisé pour l'administration réseau, la gestion des conteneurs Docker et des connexions SSH vers le Backend, la base de données, les serveurs en DMZ, les sauvegardes et l'agent Wazuh.

- Le **poste Windows Server** centralise la gestion Active Directory, les partages de fichiers et les consoles d'administration internes via RDP.

Les autres postes IT se connectent exclusivement aux bastions administrateurs pour exécuter leurs tâches via **SSH (Linux) ou RDP (Windows)**. Cette approche permet d'appliquer le **principe du moindre privilège**, car les comptes à haut privilège ne sont disponibles que sur les postes dédiés aux administrateurs, minimisant ainsi l'exposition des systèmes critiques.

Toutes les actions réalisées depuis ces bastions sont tracées : les agents Wazuh collectent les événements administratifs et Fail2Ban bloque automatiquement les tentatives SSH suspectes côté Linux.

Cette architecture garantit que l'équipe IT peut intervenir efficacement sur l'ensemble de l'infrastructure tout en limitant l'exposition des systèmes sensibles et en assurant une **traçabilité complète des accès et actions administratives**, conformément aux bonnes pratiques de sécurité et aux exigences de conformité (HDS/RGPD).

4.8. Postes Employés – VLAN 60 (192.168.60.0/28)

Le VLAN **Employés** regroupe l'ensemble des postes de travail utilisés par le personnel de la clinique (médecins, infirmiers, secrétaires, direction, services support). Tous les postes fonctionnent sous **Windows 11 Pro**, intégrés au domaine Active Directory, garantissant une administration centralisée des comptes, des droits et des politiques de sécurité.

Sécurité et durcissement

La sécurité des postes repose sur un ensemble de **GPO de durcissement**, incluant:

- une **politique de mots de passe et de verrouillage** (longueur minimale, complexité, expiration, blocage après échecs répétés),

- la **restriction des outils sensibles** (CMD, PowerShell, Task Manager),

- le **verrouillage automatique** après 10 minutes d'inactivité,

- et l'application de configurations standardisées (accès réseau, restrictions USB, mises à jour).

Ces mesures réduisent le risque d'abus interne ou de compromission par ransomware et garantissent la conformité avec les exigences réglementaires (HDS, RGPD).

Accès applicatifs et réseau

Les flux sortants des postes employés sont strictement **limités aux besoins métiers** :

- **TCP 443** vers la DMZ (accès aux portails et applications médicales via le Frontend/Backend),

- **TCP 445** vers le FileServer (partage de fichiers collaboratifs),

- **TCP/UDP 53, TCP 88 et 636** vers Active Directory (résolution DNS, Kerberos, authentification LDAPS).

Cette segmentation réseau, combinée aux ACL configurées dans pfSense, limite la surface d'attaque et empêche tout accès direct aux systèmes critiques (base de données, sauvegardes, bastions IT).

Journalisation et supervision

Tous les postes employés sont équipés d'un **agent Wazuh**, qui centralise les journaux d'événements (logons, échecs de connexion, tentatives d'élévation de privilège, blocages GPO, etc.). Cela assure une visibilité continue sur les activités des utilisateurs et permet une détection rapide en cas de comportement suspect ou d'incident de sécurité.

4.9. Backups – VLAN 80 (192.168.80.0/28)

Les sauvegardes constituent un **pilier essentiel** de la résilience de l'infrastructure de la clinique. Elles visent à garantir la continuité des activités médicales et administratives en cas d'incident majeur (panne matérielle, ransomware, erreur humaine).

Architecture technique

La stratégie repose sur deux **NAS Debian**, chacun spécialisé :

- **NAS Database** : reçoit les dumps PostgreSQL via **NFS (TCP 2049)**. Ce montage réseau permet des sauvegardes automatisées directes depuis le serveur DB vers le NAS.

- **NAS File Server** : reçoit les données depuis le **File Server Windows (SMB/TCP 445)**. Dans ce scénario, c'est le NAS qui **initie une tâche de sauvegarde "pull"** vers le File Server : il se connecte en SMB, parcourt les partages définis (Diagnostics, Dossiers patients, Finances, Plannings, Transmissions) et copie les fichiers de manière incrémentale/complète selon la politique définie.

Cette approche évite d'exécuter la sauvegarde côté File Server (charge et exposition réduites), tout en s'intégrant nativement avec le protocole SMB et les ACL Windows.

Politique de sauvegarde

Les sauvegardes sont exécutées **chaque jour à 03:00**, avec :

- **dump complet** des bases PostgreSQL,

- **sauvegarde incrémentale** des fichiers (journalière) + **complète** chaque semaine,

- **chiffrement systématique** des sauvegardes avant stockage local.

Une **réplication automatisée** est effectuée vers le **Medical Cloud**, suivant la règle du **3-2-1** (3 copies, 2 supports différents, 1 hors site).

Sécurité et conformité

Les sauvegardes sont **chiffrées au repos et en transit**. L'accès aux NAS est limité aux serveurs concernés (DB, File Server) et aux administrateurs via VLAN 40, avec journalisation renforcée (Wazuh).
Ce modèle respecte les contraintes **HDS** et **RGPD**, en garantissant confidentialité, traçabilité et isolation des données sensibles.

Test et restauration

Une **procédure documentée** de restauration est maintenue et régulièrement validée. Les objectifs fixés sont :

- **RPO (Recovery Point Objective)** ≤ 24h → perte maximale tolérée d'une journée de données,

- **RTO (Recovery Time Objective)** ≤ 1 jour → délai maximal pour retour en production.

Ces paramètres sont dimensionnés pour répondre aux enjeux médicaux : continuité des soins, accès immédiat aux diagnostics, disponibilité des plannings et données critiques de la clinique.

4.10. Monitoring & SIEM – VLAN 99 (192.168.99.0/28)

Le monitoring centralisé est un élément clé de la posture de sécurité et d'exploitation de Cleanic. La solution retenue est **Wazuh** (serveur sur Ubuntu 22.04) avec agents déployés sur l'ensemble des machines. Son rôle principal est la centralisation des logs, la détection d'anomalies et l'alerte opérationnelle, afin d'assurer visibilité, traçabilité et réaction rapide aux incidents.

Plutôt que de disperser les mentions de Wazuh dans chaque section technique, chaque composant documente ses sources de logs et points d'alerte, tandis que la **configuration, la corrélation et les playbooks d'alerte sont regroupés et maintenus dans la gouvernance SIEM**.

Wazuh collecte un large périmètre de données : logs systèmes (Linux/Windows), événements Active Directory, traces Nginx, logs applicatifs Node.js, journaux PostgreSQL, alertes Fail2Ban, flux pfSense, journaux NAS ainsi que les résultats des contrôles d'intégrité (FIM). Les agents communiquent via un canal sécurisé vers le serveur central, qui assure corrélation, enrichissement et stockage. Les règles sont adaptées au contexte clinique (sensibilité des données, exigences RGPD/HDS).

Chaque alerte est enrichie (user, host, IP, hash, timeline) et **classée par priorité** afin d'alimenter des playbooks d'intervention automatisés. En complément, certaines mesures de **réponse opérationnelle immédiate** sont couplées à Wazuh via Fail2Ban : par exemple, le blocage d'IP en cas de bruteforce SSH ou RDP.

Pour répondre aux exigences d'audit et de conformité (RGPD, HDS), les logs sont conservés selon une politique différenciée :

- **90 jours** pour l'exploitation courante,

- **1 an** pour les journaux critiques (accès AD, modifications GPO).
  Les exports sont chiffrés et signés, et des rapports automatisés sont générés (quotidien, hebdomadaire, mensuel) couvrant tentatives d'accès, incidents bloqués, état des agents et santé des sauvegardes.

La résilience est assurée par l'usage d'**Elasticsearch/Opensearch** comme back-end de stockage et d'indexation, garantissant une continuité en cas de surcharge ou de montée en volumétrie. Le serveur Wazuh lui-même est supervisé (queue, espace disque, latence d'ingestion), et une procédure de reprise documentée permet un redémarrage contrôlé si nécessaire.

Enfin, Wazuh a été retenu pour son **modèle agenté**, ses règles prêtes à l'emploi et son coût (open-source). Il demande un tuning initial et un effort d'ingénierie pour corréler efficacement les flux applicatifs (par exemple, corrélation injection SQL = logs applicatifs + logs base de données), mais fournit une solution intégrée, maîtrisable et conforme aux besoins d'audit. Les alternatives (ELK « nu » ou Splunk) ont été étudiées puis écartées : le premier pour la charge d'intégration, le second pour son coût.

4.11. Sécurité réseau – pfSense & VPN

pfSense constitue le pare-feu périmétrique et le routeur central de l'infrastructure. Il assure la segmentation inter-VLAN, la gestion des flux entrants/sortants et la défense du périmètre. Basé sur un filtrage stateful, pfSense permet un contrôle fin des flux par IP, port et protocole, complété par des fonctions avancées telles que la détection d'intrusion (Snort/Suricata) et le blocage DNS/IP malveillants via pfBlockerNG. Sa fiabilité et sa flexibilité en font l'élément central de la sécurité réseau de Cleanic.

L'architecture repose sur **deux pare-feux pfSense** configurés en **haute disponibilité (HA)** : un **pfSense Master** et un **pfSense Backup**. Leurs états et règles sont synchronisés via un **lien dédié VLAN 254 (sync)**, permettant la réplication en temps réel des configurations et des sessions actives. En cas de panne du Master, le Backup prend automatiquement le relais grâce au protocole CARP (Common Address Redundancy Protocol), assurant la continuité de service et évitant toute coupure réseau.

Cette mise en cluster renforce la **résilience** de l'infrastructure et garantit une **disponibilité 24/7**, indispensable dans un contexte médical où l'accès aux systèmes critiques ne peut être interrompu.

L’accès distant sécurisé repose sur WireGuard, déployé directement comme interface virtuelle au sein de pfSense. Les connexions VPN sont établies via un échange de clés publiques/privées, avec le WAN du pare-feu comme point d’entrée. Les clients sont attribués à un sous-réseau dédié 10.6.0.0/28, chaque pair disposant d’une adresse unique. Le chiffrement est celui fourni par WireGuard par défaut, considéré comme robuste et éprouvé dans un contexte clinique.

Le trafic VPN est intégré de façon contrôlée dans la segmentation réseau :

- Médecins en télémédecine : accès autorisé uniquement vers le File Server (445, 5985) et l’Active Directory (636, 88, 53).

- Équipe IT en remote : règles alignées sur le VLAN IT interne, avec accès d’administration aux backends, bases de données et composants critiques.

Ainsi, l’infrastructure distingue les profils d’usage (télémédecine vs administration IT), sans créer de sous-réseaux dédiés par métier, mais en assignant des adresses individuelles et traçables. Cette précision simplifie la supervision et permet un contrôle strict des flux via les ACL pfSense.
La combinaison pfSense + WireGuard apporte donc :

- Un périmètre réseau robuste et segmenté.

- Un accès distant chiffré, performant et adapté à la télémédecine comme à l’administration IT.

- Une gestion fine des autorisations, réduisant la surface d’attaque et assurant la conformité aux exigences RGPD/HDS.

4.12. Durcissement, chiffrement & certificats

L’infrastructure de Cleanic applique une politique de sécurité uniforme sur l’ensemble des composants :

- **Chiffrement** : TLS pour les frontends (certificats AC publique en production, HSTS activable), LDAPS obligatoire pour Active Directory, flux SQL chiffrés côté client.

- **Contrôles d’accès** : principe du moindre privilège généralisé via RBAC, groupes AD et ACL, complété par des règles de pare-feu strictes.

- **Durcissement des systèmes et services** : GPO Windows pour les postes et serveurs, fail2ban sur Linux pour limiter les tentatives d'intrusion.

- **Journalisation centralisée** : tous les logs convergent vers Wazuh pour la corrélation, l'alerte et la traçabilité, avec rétention conforme aux exigences de sécurité et d'audit.

- **Synchronisation temporelle** : NTP centralisé via pfSense et AD pour garantir la cohérence des horodatages.

Cette approche transversale assure la résilience, la traçabilité et la conformité HDS/RGPD, en complément des mesures spécifiques appliquées à chaque composant de l'infrastructure.

4.13. Considérations budgétaires

Référence : budget informatique d'une clinique type

En France, une clinique pluridisciplinaire constitue souvent une structure de 2 à 5 médecins, dont 3 en moyenne pour les pratiques généralistes (commonwealthfund.org). Ce contexte justifie l'échelle de notre estimation.

Estimation de l'infrastructure matérielle

Hypothèses retenues :

- **Médecins** : 3 postes Windows 11 Pro

- **Autres employés** : 1 pour tout les infirmiers, 1 secrétaire, 1 directeur

- **Postes IT** : 2 administrateurs + 3 techniciens IT

- **Serveurs physiques Debian/Ubuntu** : 8 machines

- **NAS** : 2 unités 4 baies chacun en RAID 10 avec 4 disques de 4 To

- **Infrastructure physique** : switch, pfSense, câblage, baie/rack, onduleur

- **Licences Windows Server / CALs + Windows 11** incluses

Estimation des prix

Composant	Quantité estimée	Coût unitaire estimé	Total approximatif
pfSense appliance (Netgate SG-2100)	2	~509 €	~1018 €
Cisco Catalyst L2 switch	1	~383 €	~383 €
NAS Synology 4 baies	2	~610 € chacun	~1 220 €
Disques 4 To SATA	8 (2 NAS × 4)	~100 €	~800 €
UPS (onduleur tour)	1	~214 €	~214 €
Baie/rack & câblage	—	Forfait estimé ~800 €	~800 €
PC postes Méd./Inf./Secr./Dir.	6 × ~800 €	~800 € (config légère)	~4 800 €
PC postes IT (5)	5 × ~1 200 €	~1 200 € (config pro)	~6 000 €
Serveurs physiques (8)	8 × ~1 000 €	~1 000 € (rackable)	~8 000 €
Windows Server 2022 licenses	3 × ~64 €	~64 €	~192 €
Windows 11 Pro licences	~14 postes × ~40 €	~40 € (activation pack)	~560 €
Total matériel + licences	—	—	**≈ 24 158 €**

Coûts récurrents (Medical Cloud)

- **Medical Cloud Pro (100 Go)** : 40 €/mois → ~ 480 €/an
- **Medical Cloud Premium (300 Go)** : 80 €/mois → ~ 960 €/an

Analyse

- L'investissement initial se situe autour de **24 000 €**, pour une infrastructure complète et pérenne.

- Les coûts récurrents restent limités (≈ 1 000 €/an pour le cloud), ce qui est compatible avec les budgets des cliniques de taille moyenne.

- La configuration permet des extensions futures (plus de postes, augmentation des capacités de stockage, migration vers un Medical Cloud dédié si besoin).

Recommandations

- Prévoir une **garantie 3 ans** (ANSSI) sur les serveurs, NAS et UPS.

- Allouer un budget opérationnel récurrent de **1 500 à 3 000 € / an** pour support, licences, bande passante et renouvellement progressif du matériel.

- Réévaluer les besoins Medical Cloud annuellement selon la volumétrie réelle.

Sources prix matériels

Les prix ont été établis à partir de références disponibles sur **LDLC.pro** (serveurs, PC, NAS, Windows Server 2022, Windows 11 Pro), ainsi que sur les catalogues constructeurs (Netgate, Cisco) et revendeurs professionnels (APC pour les onduleurs). Ces tarifs sont indicatifs et peuvent varier selon les périodes de commande et options de garantie choisies.

4.14. Résumé exécutif

L'architecture technologique de la clinique repose sur des choix pragmatiques et cohérents, visant à concilier **sécurité**, **interopérabilité** et **maîtrise des coûts**.

- **Cœur du système** : un Active Directory déployé sur Windows Server 2022, garantissant une intégration native avec les postes Windows 11 Pro du personnel, la gestion centralisée des accès et l'application fine des GPO de durcissement.

- **Applications critiques** : un backend Node.js/Express, un frontend Nginx et une base de données PostgreSQL (conteneurisée sous Debian), choisis pour leur robustesse, leur conformité ACID et leur capacité à gérer efficacement

des charges concurrentes.

- **Stockage** : un serveur de fichiers Windows (SMB), intégré à l'AD, avec segmentation par métier (médecins, infirmiers, administratif, direction) et permissions différenciées (ex. diagnostics : lecture seule pour infirmiers, écriture pour médecins).

- **Sécurité périmétrique et segmentation** : pfSense en haute disponibilité, assurant isolation VLAN, filtrage réseau, blocage des flux malveillants et accès VPN WireGuard pour l'IT en remote et la télémédecine.

- **Supervision & détection** : une plateforme Wazuh centralise les logs de tous les systèmes (AD, NAS, pfSense, serveurs applicatifs, endpoints), corrèle les événements et alimente des playbooks de réponse adaptés au contexte clinique.

- **Sauvegardes & continuité** : une double infrastructure NAS (PostgreSQL via NFS, File Server via SMB), avec réplication vers un cloud certifié HDS, garantissant un RPO ≤ 24h et un RTO ≤ 1 jour.

- **Environnement utilisateur** : postes Windows 11 Pro durcis par GPO, avec accès limité aux seuls services nécessaires (443 vers DMZ, 445 vers FileServer, 53/88/636 vers AD).

- **Gouvernance transversale** : principe du moindre privilège appliqué à tous les niveaux (RBAC, ACL, firewall), chiffrement systématique des flux sensibles (TLS, LDAPS, SQL chiffré), cohérence des horodatages via NTP, et centralisation des journaux pour audit RGPD/HDS.

Ces choix assurent une **infrastructure sécurisée, résiliente et conforme** aux exigences cliniques, tout en restant financièrement soutenable grâce à une combinaison raisonnée de solutions open-source et de briques Windows indispensables pour l'interopérabilité métier.

5. Contrôles de Sécurité

L'architecture de sécurité repose sur une combinaison de mesures préventives, détectives et correctives, articulées autour d'une segmentation réseau stricte, d'un contrôle des accès rigoureux, d'un chiffrement systématique des communications critiques et d'une supervision centralisée.

Segmentation et cloisonnement

Le périmètre est protégé par un cluster **pfSense en haute disponibilité** (Master/Backup) synchronisé via **VLAN 254**. Le pare-feu assure la segmentation entre les différentes zones (WAN, DMZ, Backend, Database, Active Directory, File Server, IT, VPN). Les flux sont réduits au strict nécessaire selon le principe du *zero trust*. Depuis l'extérieur, seuls les ports **443 (HTTPS)** et **51820 (WireGuard)** sont ouverts. Les employés n'ont pas d'accès direct à Internet : tout transite via la DMZ. Les flux internes sont restreints : la DMZ n'accède au Backend que sur le port **3000**, la base de données n'est joignable que par le Backend et son **NAS de sauvegarde (NFS/2049)**, et le File Server est sauvegardé via **SMB/445 vers son NAS dédié**.

Chiffrement et durcissement

Toutes les communications critiques sont protégées :

- TLS systématique côté Frontend (HTTPS, HSTS).
- **LDAPS (636)** pour l'authentification Active Directory.
- **PostgreSQL** chiffré côté serveur pour les échanges avec le Backend.
- **WireGuard** pour les connexions VPN (UDP/51820).

Les postes et serveurs sont durcis :

- **GPO restrictives** sur Windows (restriction d'outils, lockout après 3 échecs).
- **Fail2Ban** sur Debian (blocage bruteforce SSH/services).
- Sessions verrouillées automatiquement, mises à jour régulières, ACL NTFS strictes.

Gestion des identités et accès

Tous les comptes sont centralisés dans **Active Directory**. Les politiques de mots de passe suivent les **recommandations de l'ANSSI** : longueur minimale 12 caractères, complexité, rotation périodique et verrouillage après échecs répétés. Le contrôle d'accès est affiné par métier via **OU, groupes globaux/locaux et ACL**. L'application

métier applique en parallèle un **RBAC** (médecins, infirmiers, direction, IT) pour limiter les droits au strict nécessaire.

Supervision et détection

La supervision est centralisée dans **Wazuh** (agents sur tous les systèmes). Les logs système, applicatifs et réseau sont corrélés pour détecter les anomalies (authentifications anormales, injections SQL, escalades de privilèges, scans réseau). Wazuh est complété par des mécanismes de blocage local (ex. Fail2Ban). Les alertes sont enrichies et classées par criticité afin de guider la réponse opérationnelle.

Sauvegardes et résilience

Les données critiques sont protégées par une stratégie de **sauvegarde 3-2-1** :

- **Base de données** sauvegardée via NFS vers un NAS dédié.
- **File Server** sauvegardé via SMB vers un second NAS.
- Réplication chiffrée et externalisée vers le **Medical Cloud HDS**.

Ce dispositif assure intégrité, disponibilité et conformité aux exigences réglementaires (RGPD/HDS).

Pistes d'amélioration

Quelques points restent à renforcer :

- Remplacer les **certificats auto-signés** par des certificats émis par une AC reconnue.
- Déployer le **MFA** pour les comptes sensibles.
- Ajouter un **bastion d'administration** pour renforcer la traçabilité et réduire la surface d'attaque.

6. Risk Analysis

6.1. Introduction

Dans un environnement médical, l'analyse des risques est essentielle pour assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des données de santé, tout en respectant les obligations légales (RGPD, HDS).

La méthodologie appliquée s'inspire d'EBIOS et du scoring CVSS (1–10), permettant d'évaluer chaque risque selon sa probabilité, son impact sur les actifs métier et son score global, classé comme suit : Faible (0,1–3,9) / Moyen (4,0–6,9) / Élevé (7,0–8,9) / Critique (9,0–10).

Cette analyse est itérative et sera actualisée au fur et à mesure de l'évolution de l'infrastructure et des menaces.

6.2. Matrices des risques

Menace	**Vulnérabilité / Cause**	**Impact**	**Score CVSS**
M1 – Accès non autorisé aux données patients	Compte AD compromis, MFA absent, mot de passe faible	Violation RGPD, perte de confidentialité	9.0
M2 – Injection SQL / XSS	Validation insuffisante côté backend/frontend	Fuite ou modification de données	8.0
M3 – Ransomware / Chiffrement DB	Backend exposé via l'application, sauvegarde hors-ligne absente	Indisponibilité des soins, perte de données	10.0
M4 – Déni de service interne / applicatif	Payloads massifs, absence de redondance backend	Indisponibilité temporaire	7.0
M5 – Interception de données	Absence de chiffrement complet en transit	Exposition des données sensibles	9.0

M6 – Perte ou corruption de données	Crash disque, tests de sauvegarde insuffisants	Indisponibilité ou corruption	9.0
M7 – Escalade de privilèges internes	Droits AD mal gérés, mots de passe faibles	Compromission partielle	8.0
M8 – Propagation de malware interne	Périphériques USB/email, postes non durcis	Indisponibilité postes / fuite données	7.0
M9 – Perte de connectivité réseau	Dépendance à un seul FAI	Retard dans soins / services indisponibles	6.0
M10 – Défaillance pfSense Master/Backup	Lien VLAN 254 mal configuré ou panne simultanée	Interruption du firewall / perte d'accès réseau	7.0
M11 – Configuration incorrecte des NAS	Permissions SMB/NFS mal appliquées	Perte de données ou accès non autorisé	7.0

6.3. Analyse et mesures

M1 – Accès non autorisé aux données patients
Mesures : authentification AD + MFA, journalisation centralisée (Wazuh), contrôle d'accès RBAC/ACL stricts, Fail2Ban sur services critiques.
RGPD : Articles 5, 25, 32, 33.

M2 – Injection SQL / XSS
Mesures : requêtes paramétrées PostgreSQL, validation backend/frontend, en-têtes de sécurité Nginx, détection anomalies via Wazuh, tests réguliers d'intrusion.
RGPD : Articles 5, 32.

M3 – Ransomware / Chiffrement DB
Mesures : sauvegardes quotidiennes locales + NAS + Medical Cloud (3-2-1), segmentation réseau, monitoring Wazuh, PRA documenté.
RGPD : Articles 32, 33.

M4 – Déni de service interne / applicatif
Mesures : limitation taille payloads, rate-limiting via pfSense, redémarrage automatique services (PM2), HA envisagé via HAProxy.
RGPD : Article 32.

M5 – Interception de données
Mesures : TLS obligatoire frontend ↔ backend ↔ DB, LDAPS pour AD, VPN WireGuard pour accès distant, certificats renouvelés automatiquement.
RGPD : Article 32.

M6 – Perte ou corruption de données
Mesures : RAID 10 sur DB, tests de restauration mensuels, vérification des sauvegardes par hash, supervision FIM via Wazuh.
RGPD : Articles 5, 20, 32.

M7 – Escalade de privilèges internes
Mesures : comptes séparés par rôle, GPO restrictives, ACL fines, audits réguliers, alerting Wazuh, coffre-fort pour secrets.
RGPD : Articles 25, 32.

M8 – Propagation de malware interne
Mesures : blocage périphériques USB via GPO, EDR sur postes Windows, sandboxing des pièces jointes, sensibilisation utilisateurs.
RGPD : Article 32.

M9 – Perte de connectivité réseau
Mesures : redondance WAN envisagée, procédures de bascule documentées, QoS pour trafic critique.
RGPD : Articles 32, 33.

M10 – Défaillance pfSense Master/Backup
Mesures : lien VLAN 254 synchronisé pour état actif/passif, tests périodiques de bascule automatique.
RGPD : Articles 32, 33.

M11 – Configuration incorrecte des NAS
Mesures : contrôle strict des permissions SMB/NFS, chiffrement des sauvegardes, tests de restauration documentés, monitoring via Wazuh.
RGPD : Articles 5, 32.

7. Compliance

L'infrastructure Cleanic a été conçue pour garantir la conformité avec le **RGPD** et faciliter les audits de sécurité. Les mesures techniques et organisationnelles sont intégrées dès la conception et documentées afin de démontrer la protection effective des données sensibles.

Article RGPD	Mesures mises en œuvre	Explication
Article 5 – Principes relatifs au traitement des données	Contrôle d'accès RBAC/ACL, segmentation VLAN, restriction accès selon rôle	Seules les données strictement nécessaires sont accessibles aux utilisateurs concernés, garantissant confidentialité et finalité.
Article 20 – Portabilité des données	Sauvegardes locales et cloud (Medical Cloud HDS) avec règle 3-2-1	Les données peuvent être restaurées rapidement, assurant continuité des soins et portabilité pour les patients.
Article 25 – Protection des données dès la conception et par défaut	Ségrégation des VLAN, firewall pfSense, VPN WireGuard, politiques GPO et durcissement des hôtes	Les mesures limitent la surface d'attaque et appliquent le principe de sécurité par défaut dès la conception des services.
Article 32 – Sécurité du traitement	Chiffrement TLS/LDAPS, monitoring centralisé Wazuh, Fail2Ban, sauvegardes chiffrées, contrôle d'accès strict	Garantit l'intégrité, la disponibilité et la confidentialité des données, avec alerting proactif et corrélation centralisée des incidents.
Article 33 – Notification en cas de violation	Playbooks d'alerte Wazuh, procédures internes de réponse aux incidents documentées	Toute tentative de compromission est détectée et notifiée, permettant une réaction rapide conforme aux exigences légales.

Synthèse : L'infrastructure combine isolation réseau, contrôles d'accès stricts, chiffrement, supervision centralisée et sauvegardes redondantes. Ces mesures sont **traçables, auditées et facilement démontrables** pour assurer le respect du RGPD et des obligations HDS. Les procédures documentées permettent de garantir une conformité durable et d'adapter les contrôles aux évolutions réglementaires ou aux nouveaux risques.

8. Conclusion

Le projet **Cleanic** a permis de concevoir et simuler une infrastructure complète pour une clinique pluridisciplinaire de taille moyenne, répondant aux besoins métiers, techniques et réglementaires. L'architecture couvre l'ensemble des services essentiels : gestion des identités via **Active Directory**, application web sécurisée, base de données **PostgreSQL**, serveur de fichiers, sauvegardes redondantes, monitoring centralisé avec **Wazuh**, et contrôles de sécurité réseau stricts. Les choix technologiques (**Debian** pour les serveurs applicatifs, **Windows Server** pour AD et le file server, **PostgreSQL** pour la DB, **NGINX** pour le frontend, **WireGuard** pour le VPN) ont été guidés par la sécurité, la maintenabilité et la conformité **RGPD/HDS**.

Les mécanismes de protection déployés incluent : segmentation VLAN, règles firewall précis, flux chiffrés (TLS, LDAPS, VPN), authentification forte, RBAC/ACL pour la gestion des accès, supervision centralisée et alerting via Wazuh, ainsi que des sauvegardes selon la règle **3-2-1** et un RAID 10. Cette combinaison minimise les risques sur la confidentialité, l'intégrité et la disponibilité des données, tout en garantissant une continuité d'activité crédible.

Certaines limites subsistent : la haute disponibilité complète n'est pas implémentée sur tous les services, les NAS ont une capacité physique limitée et certains flux internes restent concentrés sur des points uniques, créant des risques de défaillance. Le RAID 10 protège contre les pannes matérielles mais ne remplace pas les sauvegardes hors site ni la protection contre les ransomwares.

Les évolutions recommandées incluent : haute disponibilité pour le backend et services critiques, corrélation avancée des logs dans le SIEM, réplication en temps réel des bases de données, chiffrement étendu des flux internes, et :

- mise en place d'un VPN site-à-site pour connecter plusieurs sites,
- automatisation des correctifs et mises à jour de sécurité,
- tests d'intrusion réguliers pour valider la robustesse,
- extension des politiques de sauvegarde pour couvrir de nouveaux types de données ou services critiques.

En résumé, **Cleanic** illustre une infrastructure sécurisée, réaliste et conforme aux standards de protection des données, démontrant la capacité du projet à anticiper les menaces, appliquer des mesures de mitigation cohérentes et préparer l'évolution future d'un environnement de soins sécurisé.