Schuhler Louis
BTS SIO
2ème année
Option SISR

42 avenue de l'Europe
68000 Colmar
Téléphone : 03 89 22 25 00

Rapport de Stage

Paul Hartmann SAS

9 route de Sélestat
67730 Châtenois

Période : du 02 mars au 10 avril 2026

Sommaire

1.- Remerciements

Je tiens tout particulièrement à remercier **Monsieur Christophe Hauert**, Architecte Infrastructure, mon Responsable et **Monsieur Jordan Durringer,** Ingénieur Infrastructure, mon tuteur durant mes 6 semaines de stage.

Grâce à eux, j'ai pu mettre en pratique certaines compétences acquises durant mon BTS et développer mes connaissances en informatique.
Je suis particulièrement sensible à leur compréhension par rapport à mes difficultés.

Je tiens également à remercier tous les collaborateurs de la société Paul Hartmann SAS qui m'ont aidé pendant toute la durée de mon stage et en particulier, mes collègues du service informatique.

J'ai trouvé auprès d'eux une grande disponibilité, de la bienveillance et un accueil chaleureux.

Enfin, je tiens tout particulièrement à remercier M. Jean-Jacques Husser, Responsable projets logistiques et solutions clients de Hartmann Group, sans qui ce stage n'aurait pu avoir lieu.

2.-Introduction

2.1- Présentation de l'élève :

Après mon baccalauréat professionnel Systèmes numériques Option C « Réseaux informatiques et systèmes communicants » au lycée Couffignal à Strasbourg, j'ai obtenu le récent diplôme post-baccalauréat, Mention complémentaire, cursus « Services Numériques aux Organisations ».
Puis durant deux ans, j'ai suivi des formations en informatique, à distance.

Souhaitant poursuivre mes études en informatique et plus précisément dans la programmation, j'ai intégré en septembre 2024 le BTS SIO au lycée Camille Sée à Colmar.

Progressivement, je me suis particulièrement intéressé aux problématiques liées à la sécurisation des systèmes d'information : détection des vulnérabilités, protection des données, gestion des accès et mise en place de mécanismes de défense adaptés face aux menaces numériques. Cette passion m'incite à m'informer régulièrement des solutions robustes aux défis nouveaux et majeurs de cybersécurité.

C'est la raison pour laquelle, je souhaiterais, après l'obtention de mon BTS, pouvoir poursuivre mes compétences dans le domaine des systèmes, des réseaux et de la cybersécurité.

2.2 Missions réalisées :

- Mise en place et configuration d'une infrastructure réseau (switch, VLAN, routage) ;
- Installation et configuration d'une solution de virtualisation avec Proxmox ;
- Déploiement de machines virtuelles (Ubuntu et Windows Server) ;
- Mise en place de solutions de stockage (NAS et SAN) ;
- Installation de services (Docker, VPN WireGuard, supervision) ;
- Sécurisation du réseau (SSH, pare-feu pfSense) ;
- Réalisation de tests de performance et de validation.

3.- Présentation de l'entreprise

3.1- D'hier à aujourd'hui :

Tout commence il y a plus de 200 ans en Allemagne avec la filature de coton de Ludwig von Hartmann qui devient la plus grande du Wurtemberg.

En 1870, fasciné par les progrès de la médecine, son fils, Paul Hartmann, décide d'orienter la société vers un nouveau secteur : la fabrique de textiles pour pansements. C'est ainsi que la ouate devient pansement. Il démarre la production industrielle de ouate pour pansement et fonde la première usine en Allemagne. Des partenaires, médecins et scientifiques, l'aident à améliorer les produits en lui faisant bénéficier de leurs découvertes telles que le dégraissage du coton ou le premier pansement germicide (qui tue les germes microbiens).

Ces avancées ont contribué fortement à améliorer le traitement des plaies.

En 1919, la perte des filiales étrangères en raison de la Première guerre mondiale, est compensée par l'introduction de nouveaux produits. Désormais, la société fabrique aussi des pansements adhésifs et des pommades, innovations dues au département pharmacie nouvellement créé.

Deux décennies plus tard, Hartmann développe sa première compresse imprégnée destinée aux brûlures : elle n'adhère pas à la plaie et peut être remplacée pratiquement sans douleur.

Dans les années 60, est créée la compresse à bords rentrés. Sa grande capacité d'absorption et sa perméabilité à l'air en font un classique dans le soin des plaies. On retrouve alors ce produit chez la plupart des médecins.

A l'aube des années 2000, la société imagine un concept thérapeutique déterminant pour le soin des plaies en milieu humide, sur la base de trois pansements hydroactifs.
Plus récemment, en 2018, elle développe et commercialise des pansements techniques hydrocellulaires en silicone.

Depuis elle contribue régulièrement aux développements de solutions complètes et innovantes mais aussi à la mise en place de bonnes pratiques dans les soins médicaux.

Aujourd'hui, le groupe Hartmann est une entreprise internationale, présente dans 36 pays et distribuant sa gamme professionnelle auprès de différents prestataires de services situés dans plus de 130 pays.

Le siège social de la société mère est toujours situé à Heidenheim an der Brenz.

3.2- Domaines d'activité :

Le groupe Hartmann est l'un des leaders européens des produits pour les professionnels de santé et l'hygiène.

Il propose des solutions médicales, commercialisées sous sa marque et constituées de dispositifs professionnels dans quatre domaines clés :

- l'hygiène et l'incontinence ;
- les soins et la cicatrisation ;
- la prévention des risques d'infection ;
- l'autodiagnostic et l'immobilisation.

3.3- Valeurs et mission :

Les valeurs de la société Hartmann visent à aider à améliorer la vie des patients grâce à ses produits et services. Pour ce faire, elle recherche constamment des moyens de proposer des solutions intelligentes et basées sur des expériences optimisées qui profitent autant aux patients qu'aux professionnels de santé.

Son ambition est d'être un acteur de premier plan sur le marché mondial de la santé et d'agir concrètement pour promouvoir la santé de tous.
Pour ce faire, Hartmann s'appuie sur trois valeurs fondamentales :

- la performance ;
- l'orientation client ;
- une passion profonde pour son travail.

Ces valeurs l'aident à rester fidèle à sa mission : aider, soigner et protéger.

3.4- Quelques données chiffrées :

Mi-mars 2025, Paul Hartmann AG (Aktiongesellschaft ou équivalent des sociétés anonymes en droit français) a communiqué ses résultats financiers pour l'exercice clos le 31 décembre 2025.

Sur l'année passée, la société a enregistré des ventes s'élevant à 2 458,98 millions d'euros, contre 2 425,8 millions d'euros un an plus tôt.

Le chiffre d'affaires s'est établi à 2 470,53 millions d'euros, comparativement aux 2 428,58 millions d'euros de l'exercice précédent.

Le résultat net s'est inscrit à 61,21 millions d'euros, contre 108,45 millions d'euros l'année dernière.
Fin 2025, le groupe Hartmann comptait plus de 10 000 collaborateurs.

Source : site zonebourse.com

3.5- Zoom sur la filiale française :

La société Paul Hartmann SAS est créée le 1er janvier 1973 et installe son siège à Châtenois, près de Sélestat.

Sa forme juridique est SAS, société par actions simplifiée, forme sociale commerciale la plus courante en France.

Immatriculée au RCS de Colmar sous le n°778 740 001, elle a un capital social de 20 millions d'euros.
Son domaine d'activité est la fabrication d'articles en papier à usage sanitaire ou domestique (code NAP ou APE est 17.22Z).

En 2023, elle était catégorisée Entreprise de Taille Intermédiaire, c'est-à-dire qu'elle a entre 250 et 4 999 salariés et un chiffre d'affaires inférieur à 1,5 milliard d'euros.

Cinq décennies plus tard, cette filiale française est devenue la 2ème plus importante du groupe en se développant progressivement à la fois par ses activités propres et par l'intégration de nouvelles sociétés (entre 1990 et 2019).

Actuellement, elle compte quatre implantations sur le territoire français :

- le siège social et établissement principal à Châtenois (67) ;
- l'usine, un centre logistique, le centre Recherches et Développement et la qualité à Lièpvre (68) ;
- un centre logistique à Belleville-en-Beaujolais (69) ;
- le site administratif à Arcueil (94).

Sources : sites Hartmann et Pappers

Au 31 décembre 2024, elle réalise un chiffre d'affaires de 429,1 millions d'euros et un résultat net de 14,2 millions d'euros. Elle emploie 886 collaborateurs.

4.- Aspects techniques

4.1- Description de la principale mission confiée :

La mission qui m'a été confiée consistait à concevoir et mettre en place une infrastructure informatique complète, fiable et sécurisée, capable d'héberger plusieurs services tout en assurant une communication efficace entre les équipements.

L'objectif principal était de déployer un environnement cohérent intégrant plusieurs composantes : un réseau segmenté à l'aide de VLANs, des serveurs virtualisés avec Proxmox, des solutions de stockage (NAS et SAN) ainsi que des services accessibles de manière sécurisée (VPN, Docker, supervision).

Cette infrastructure devait permettre de centraliser les services, d'améliorer leur disponibilité et de faciliter leur administration. Elle devait également être suffisamment flexible pour évoluer en fonction des besoins futurs.

Dans ce contexte, plusieurs enjeux ont été pris en compte. Il était nécessaire de garantir une bonne performance du système, une disponibilité des services ainsi qu'un niveau de sécurité adapté, notamment grâce à la segmentation du réseau et à la mise en place d'un pare-feu pfSense.

La virtualisation optimise l'utilisation des ressources matérielles en limitant le nombre de serveurs physiques nécessaires, tout en facilitant le déploiement et la gestion des machines virtuelles.

Par ailleurs, une attention particulière a été portée à l'administration de l'infrastructure. L'utilisation d'outils centralisés permet de simplifier la supervision, la gestion des services et la maintenance du système.

La mise en œuvre de cette solution a permis d'obtenir une infrastructure performante, évolutive et sécurisée, répondant aux besoins définis en début de projet et apportant une réelle valeur ajoutée en termes de gestion, de sécurité et d'optimisation des ressources.

4.2- Description des tâches réalisées :

Afin de répondre à cette problématique, plusieurs tâches ont été réalisées.

Dans un premier temps, j'ai mis en place l'infrastructure réseau en configurant un switch Cisco Catalyst 2960-X, élément central du réseau. Ce switch permet d'interconnecter l'ensemble des équipements et de gérer la segmentation du réseau. J'ai ainsi créé plusieurs VLANs (VLAN 10, 20 et 30) afin de segmenter le réseau et d'isoler les différents types de trafic (utilisateurs, serveurs et administration).

Cette segmentation a permis d'améliorer significativement la sécurité en limitant les communications non autorisées entre les différents segments du réseau mais aussi de mieux organiser les flux et de faciliter l'administration quotidienne de l'infrastructure.

J'ai choisi d'utiliser des VLANs afin d'isoler les différents types de trafic, ce qui limite les risques en cas d'attaque. Une autre solution aurait été l'utilisation de réseaux physiques séparés mais cette approche aurait été plus coûteuse et moins flexible, spécialement en cas d'évolution de l'infrastructure.

L'infrastructure repose sur plusieurs équipements complémentaires. Deux serveurs physiques ont été déployés : un serveur Dell EMC PowerEdge R740 et un serveur HP ProLiant DL380. Ces serveurs hébergent la solution de virtualisation Proxmox permettant de créer et de gérer plusieurs machines virtuelles.

L'utilisation de la virtualisation optimisent les ressources matérielles en hébergeant plusieurs systèmes sur un même serveur physique. Le déploiement d'une machine virtuelle peut ainsi être réalisé en quelques minutes contre plusieurs heures pour une installation physique classique, ce qui représente un gain de temps significatif.

J'ai procédé au déploiement de plusieurs machines virtuelles, notamment sous Ubuntu et Windows Server. Chaque machine a été configurée avec une adresse IP et des services spécifiques en fonction de son rôle, permettant une organisation claire et efficace des services.

Afin de structurer l'infrastructure et de faciliter son administration, un plan d'adressage IP a été défini pour l'ensemble des équipements :

Nom de l'appareil	Adresse IP	Port	Utilisateur	Uptime Kuma
Connexion Internet	8.8.8.8	--	--	oui
Passerelle réseau	192.168.30.1	--	--	oui
pfSense	192.168.50.1	--	admin	oui
Switch	192.168.30.60	--	root	oui
MikroTik	192.168.30.61	--	admin	oui
Proxmox Dell	192.168.30.75	8005	root	oui
Proxmox HP	192.168.30.76	8006	root	oui
Proxmox Backup	192.168.30.77	8007	root	oui
VM Windows Server	192.168.30.78	--	administrator	oui
VM Ubuntu	192.168.30.87	--	louis	oui
Portainer	192.168.30.87	9000	admin	oui
Uptime Kuma	192.168.30.87	3001	root	oui
WGDashboard	192.168.30.87	10086	louis	oui
Vaultwarden	192.168.30.87	8080	louis	oui
n8n	192.168.30.87	5678	-	oui
Stockage Dell Contrôleur A	192.168.30.91	443	manage	oui

Stockage Dell Contrôleur B	192.168.30.92	443	manage	oui
Synology RackStation	192.168.30.93	5000	louis	oui
Synology DiskStation	192.168.30.94	5050	louis	oui
Serveur Dell iDRAC	192.168.30.70	443	root	oui
Serveur HP iLO	192.168.30.71	--	administrator	oui
Ordinateur portable	192.168.30.100	--	louis	oui

Par ailleurs, j'ai mis en place des solutions de stockage avec un NAS Synology et un SAN Dell EMC PowerVault. Le NAS permet le partage de fichiers sur le réseau, tandis que le SAN est utilisé pour héberger les machines virtuelles avec de meilleures performances, particulièrement en termes de rapidité d'accès aux données et de fiabilité.

En complément, j'ai installé plusieurs services, notamment Docker pour la gestion de conteneurs et WireGuard pour la mise en place d'un VPN sécurisé. L'utilisation de Docker permet de déployer rapidement des services en quelques secondes, tout en facilitant leur gestion et leur maintenance.

Un pare-feu pfSense a également été configuré afin d'assurer le routage entre les différents réseaux et de sécuriser les flux grâce à des règles de filtrage précises. Cette configuration permet de contrôler efficacement les accès et de renforcer la sécurité globale de l'infrastructure.
Enfin, des tests ont été réalisés à chaque étape du projet, comme des tests de connectivité, de performance et de sécurité. Les vérifications d'accès aux services (interface web, SSH, ping) ont rendu possible la validation du bon fonctionnement de l'ensemble de l'infrastructure et l'assurance de sa stabilité.

Afin d'évaluer plus précisément les performances de l'infrastructure mise en place, plusieurs observations ont été réalisées sur le fonctionnement global du système.

L'utilisation de la virtualisation avec Proxmox a permis de constater une optimisation significative des ressources matérielles. En effet, plusieurs machines virtuelles ont pu être exécutées simultanément sur un même serveur physique, tout en maintenant un bon niveau de performance. Cette approche vise à réduire les coûts liés à l'achat de matériel supplémentaire et d'améliorer la flexibilité du système.

De plus, le déploiement des machines virtuelles s'est révélé particulièrement rapide. Là où une installation physique peut nécessiter plusieurs heures, la création d'une machine virtuelle fonctionnelle a pu être réalisée en quelques minutes seulement. Ce gain de temps constitue un avantage important dans un contexte professionnel où la réactivité est essentielle.

L'utilisation du stockage SAN a également a rendu possible l'amélioration des performances d'accès aux données, notamment pour les machines virtuelles. Les temps de réponse observés ont été satisfaisants et ont contribué à garantir une bonne fluidité dans l'utilisation des services.

Par ailleurs, la mise en place de la segmentation réseau via les VLANs a permis de limiter efficacement les communications non autorisées entre les différents segments. Cette organisation renforce la sécurité globale de l'infrastructure tout en facilitant l'identification et la gestion des flux réseau.

Enfin, la centralisation des services à l'aide de Docker simplifie le déploiement et la maintenance des applications. Les services peuvent être rapidement mis à jour ou redéployés, ce qui améliore la gestion globale du système et réduit les temps d'intervention en cas de problème.

5.- Compétences mobilisées du bloc 1

Au cours de mon stage, j'ai mobilisé plusieurs compétences du bloc 1 du BTS SIO, en lien direct avec la conception, le déploiement et la sécurisation d'une infrastructure informatique complète.

5.1- Gérer le patrimoine informatique :

Dans le cadre de ma mission, j'ai participé à la gestion du patrimoine informatique en mettant en place une infrastructure réseau structurée.

J'ai ainsi configuré un switch Cisco Catalyst 2960-X en créant plusieurs VLANs (VLAN 10, 20 et 30) afin de segmenter les flux (utilisateurs, serveurs, administration). Cette segmentation permet d'améliorer la sécurité et de mieux organiser les communications réseau.

J'ai également déployé des solutions de stockage avec un NAS Synology et un SAN Dell EMC PowerVault, permettant de centraliser les données et d'assurer leur disponibilité. Cette centralisation facilite la gestion des ressources et améliore la fiabilité du système d'information.

5.2- Répondre aux incidents et aux demandes :

Au cours du déploiement de l'infrastructure, j'ai été confronté à plusieurs incidents techniques, comme des problèmes de configuration réseau, de communication entre VLANs et de fonctionnement de certains services.

J'ai su analyser ces dysfonctionnements en utilisant une démarche structurée : identification du problème, analyse de la configuration, réalisation de tests et mise en place d'une solution adaptée.

Par exemple, lors d'un problème de communication entre VLANs, j'ai identifié une mauvaise affectation des ports sur le switch Cisco. Après correction de la configuration, la communication entre les équipements a été rétablie.

Cette expérience m'a permis de développer une méthodologie efficace de résolution d'incidents, basée sur l'analyse et la validation des solutions mises en place.

5.3- Mettre à disposition un service informatique :

J'ai participé au déploiement de plusieurs services informatiques : machines virtuelles avec Proxmox, conteneurs Docker et VPN sécurisé avec WireGuard.

Le déploiement de ces services a permis de rendre l'infrastructure fonctionnelle et accessible, tout en garantissant un niveau de sécurité adapté.

J'ai également réalisé des tests de connectivité, de performance et de sécurité (ping, accès web, SSH) afin de valider le bon fonctionnement des services.

Ces actions ont assuré la disponibilité, la fiabilité et la sécurité des services mis à disposition des utilisateurs.

5.4- Travailler en mode projet :

Durant ce stage, j'ai organisé mon travail en suivant une démarche structurée, comprenant l'analyse des besoins, la conception de l'infrastructure, le déploiement des services et la phase de tests.

J'ai planifié les différentes tâches en tenant compte des priorités et des contraintes techniques. Ainsi, j'ai pu suivre l'avancement du projet et respecter les objectifs fixés.

Cette organisation m'a permis de mener à bien le projet dans les délais impartis, tout en garantissant la qualité et la cohérence de l'infrastructure mise en place.

6.- Veille technologique

6.1- Définition et objectif :

La veille technologique consiste à surveiller en continu les évolutions des technologies, des outils et des pratiques afin d'anticiper les besoins et de s'adapter aux évolutions du secteur informatique.

Dans le domaine des systèmes et réseaux, elle est essentielle pour maintenir des infrastructures performantes, sécurisées et adaptées aux nouvelles contraintes technologiques.

Dans le cadre de mon stage, cette veille m'a aidé à mieux comprendre les solutions mises en place et de justifier les choix techniques réalisés.

6.2- Sujet de la veille :

Le sujet de ma veille technologique porte sur la virtualisation et la conteneurisation dans les infrastructures informatiques modernes.

Ce choix est directement lié aux technologies utilisées durant mon stage, comme Proxmox pour la virtualisation et Docker pour la conteneurisation.

Ces technologies sont aujourd'hui au cœur des infrastructures professionnelles telles que les environnements cloud et DevOps.

6.3- Virtualisation :

La virtualisation permet d'exécuter plusieurs systèmes d'exploitation sur un même serveur physique grâce à un hyperviseur.

Chaque machine virtuelle fonctionne de manière indépendante, avec son propre système d'exploitation et ses ressources dédiées.

Dans ce projet, la solution Proxmox a été utilisée. Elle permet de gérer des machines virtuelles via une interface web centralisée et facilite l'administration de l'infrastructure.

Les principaux avantages sont :
- l'optimisation des ressources matérielles ;
- la réduction des coûts ;
- l'isolation des environnements ;
- la facilité de gestion.

6.4- Conteneurisation :

La conteneurisation permet d'exécuter des applications dans des environnements isolés appelés conteneurs.

Contrairement à la virtualisation, les conteneurs partagent le noyau du système hôte, ce qui les rend plus légers et plus rapides.

Docker est une solution largement utilisée qui permet de déployer rapidement des applications de manière reproductible.

Les avantages sont :
- la rapidité de déploiement ;
- la faible consommation de ressources ;
- la portabilité ;
- la facilité de gestion.

6.5- Comparaison virtualisation / conteneurisation :

Critère	**Virtualisation**	**Conteneurisation**
Système	OS complet	Partage du noyau
Performance	Plus lourde	Plus légère
Isolation	Très forte	Moyenne
Démarrage	Lent	Très rapide

La virtualisation est adaptée pour héberger des systèmes complets, tandis que la conteneurisation est plus adaptée au déploiement rapide d'applications.

Ces deux technologies sont complémentaires et souvent utilisées ensemble dans les infrastructures modernes.

6.6- Évolution des technologies :

Aujourd'hui, les infrastructures informatiques évoluent vers des architectures hybrides combinant virtualisation, conteneurisation et cloud.

Des outils comme Kubernetes permettent d'orchestrer automatiquement les conteneurs, facilitant la gestion des applications à grande échelle.

Les entreprises adoptent de plus en plus ces technologies afin d'améliorer la flexibilité, la scalabilité et la disponibilité de leurs services.

Cette évolution montre l'importance de maîtriser ces outils pour répondre aux besoins actuels du marché.

Cette évolution s'accompagne également d'une transformation des pratiques professionnelles dans le domaine de l'informatique. Les entreprises cherchent aujourd'hui à automatiser un maximum afin de gagner en efficacité, en fiabilité et en rapidité de déploiement.

Dans ce contexte, les approches DevOps prennent une place de plus en plus importante. Elles visent à rapprocher les équipes de développement et d'exploitation afin d'améliorer la collaboration et de réduire les délais de mise en production.

Par ailleurs, le concept d'Infrastructure As Code (IaC) consiste à gérer et déployer les infrastructures informatiques à l'aide de fichiers de configuration plutôt que par des manipulations manuelles.

Cette approche permet de reproduire facilement un environnement, de limiter les erreurs humaines et d'assurer une meilleure traçabilité des modifications.

Ces nouvelles pratiques illustrent l'évolution des métiers des systèmes et réseaux vers des profils plus polyvalents, capables non seulement de gérer des infrastructures, mais aussi de les automatiser et de les optimiser en continu.

Ainsi, la maîtrise de ces outils et de ces concepts constitue un atout majeur pour répondre aux exigences actuelles du marché du travail.

6.7- Sources de la veille :

Cette veille a été réalisée à partir de sources fiables telles que :
- la documentation officielle de Proxmox ;
- la documentation officielle de Docker ;
- la documentation Kubernetes ;
- les sites spécialisés en administration systèmes et réseaux ;
- les forums techniques et retours d'expérience.

6.8- Apports de la veille :

Cette veille technologique m'a permis d'approfondir ma compréhension des technologies utilisées durant mon stage, par exemple la virtualisation avec Proxmox et la conteneurisation avec Docker. Elle m'a également aidé à justifier les choix techniques réalisés lors de la mise en place de l'infrastructure.

Grâce à cette veille, j'ai saisi les différences et la complémentarité entre les machines virtuelles et les conteneurs. Par exemple, la virtualisation est particulièrement adaptée pour isoler des systèmes complets tandis que la conteneurisation permet un déploiement rapide et flexible des applications.
J'ai ainsi mieux appréhendé les choix effectués dans mon projet, en particulier l'utilisation combinée de machines virtuelles et de conteneurs pour optimiser à la fois les performances, la flexibilité et la gestion des ressources.

Par ailleurs, cette veille m'a aussi sensibilisé aux évolutions actuelles du secteur, comme l'essor des architectures hybrides et des outils d'orchestration tels que Kubernetes, qui permettent d'automatiser le déploiement et la gestion des applications à grande échelle.

J'ai ainsi pu développer mes compétences en recherche d'information, en sélection de sources fiables et en analyse critique et comparaison de technologies.

Enfin, cette démarche de veille constitue un élément essentiel dans mon développement professionnel, mais aussi dans la perspective de poursuivre mes études dans le domaine des systèmes, des réseaux et de la cybersécurité, où les technologies évoluent rapidement.

7.- Conclusion du rapport

Durant les 6 semaines de mon stage, j'ai participé à la conception et à la mise en place d'une infrastructure informatique complète intégrant le réseau, la virtualisation, le stockage et les services.

Ce stage a été l'occasion pour moi de développer des compétences techniques solides en administration systèmes et réseaux, en particulier dans la configuration d'équipements réseau, la virtualisation avec Proxmox, la mise en place de services avec Docker ainsi que la sécurisation de l'infrastructure à l'aide de solutions comme pfSense et WireGuard.

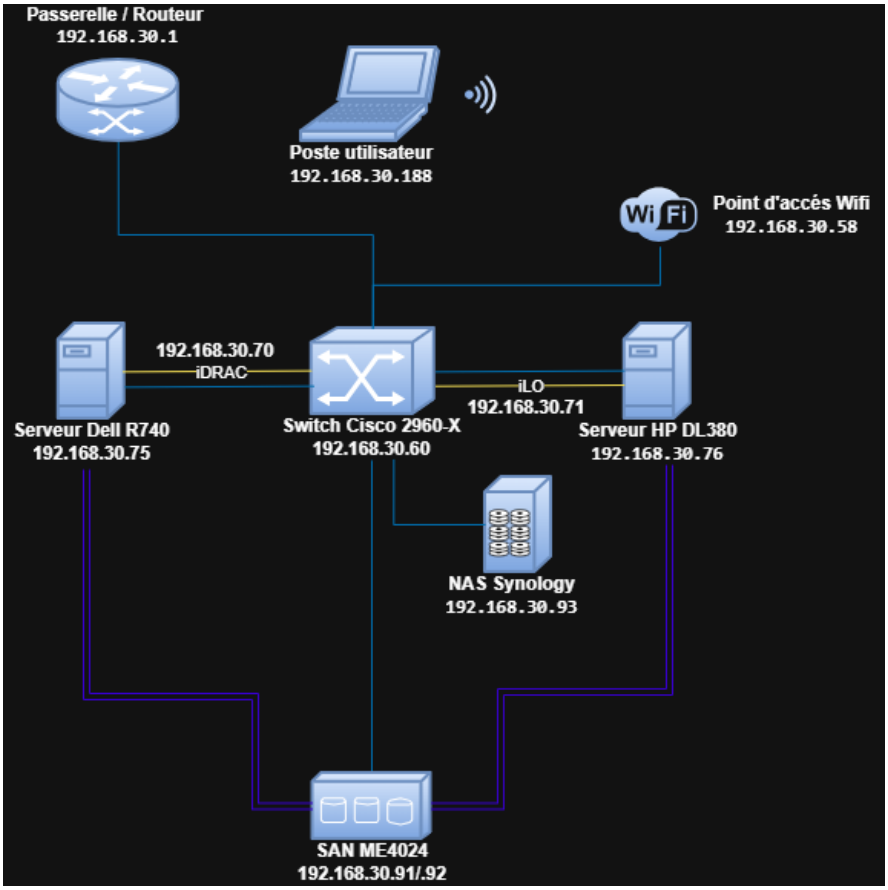
J'ai également été confronté à des problématiques concrètes. Pour les résoudre, j'ai dû recourir à une méthodologie de résolution d'incidents basée sur l'analyse, les tests et la validation des solutions.

Au-delà des compétences techniques, cette expérience m'a permis d'améliorer certaines qualités professionnelles telles que l'autonomie, la rigueur et la capacité à travailler en équipe. Elle a également été une occasion de mieux comprendre les enjeux liés à la gestion d'un système d'information en environnement professionnel.

Enfin, ce stage a confirmé mon projet professionnel, qui est de poursuivre mes études dans le domaine des systèmes et réseaux avec une spécialisation en cybersécurité.

Annexes

Annexe 1 : Schéma de l'infrastructure réseau



Le schéma ci-dessus représente l'architecture globale de l'infrastructure mise en place durant le stage. Il met en évidence les différents équipements ainsi que leurs interconnexions au sein du réseau :

- Le routeur (192.168.30.1) assurant l'accès au réseau et aux communications externes
- Le switch Cisco Catalyst 2960-X (192.168.30.60), élément central du réseau, permettant l'interconnexion de l'ensemble des équipements
- Les serveurs :
  - Dell PowerEdge R740 (192.168.30.75)
  - HP ProLiant DL380 (192.168.30.76)
- Les interfaces de gestion à distance :
  - iDRAC (192.168.30.70)
  - iLO (192.168.30.71)
- Les solutions de stockage :
  - SAN Dell ME4024 (192.168.30.91/92) pour le stockage des machines virtuelles
  - NAS Synology (192.168.30.93) pour le partage de fichiers
- Les équipements utilisateurs :
  - Poste client (192.168.30.188)
  - Point d'accès Wi-Fi (192.168.30.58)

Annexe 2 : Segmentation du réseau par VLAN

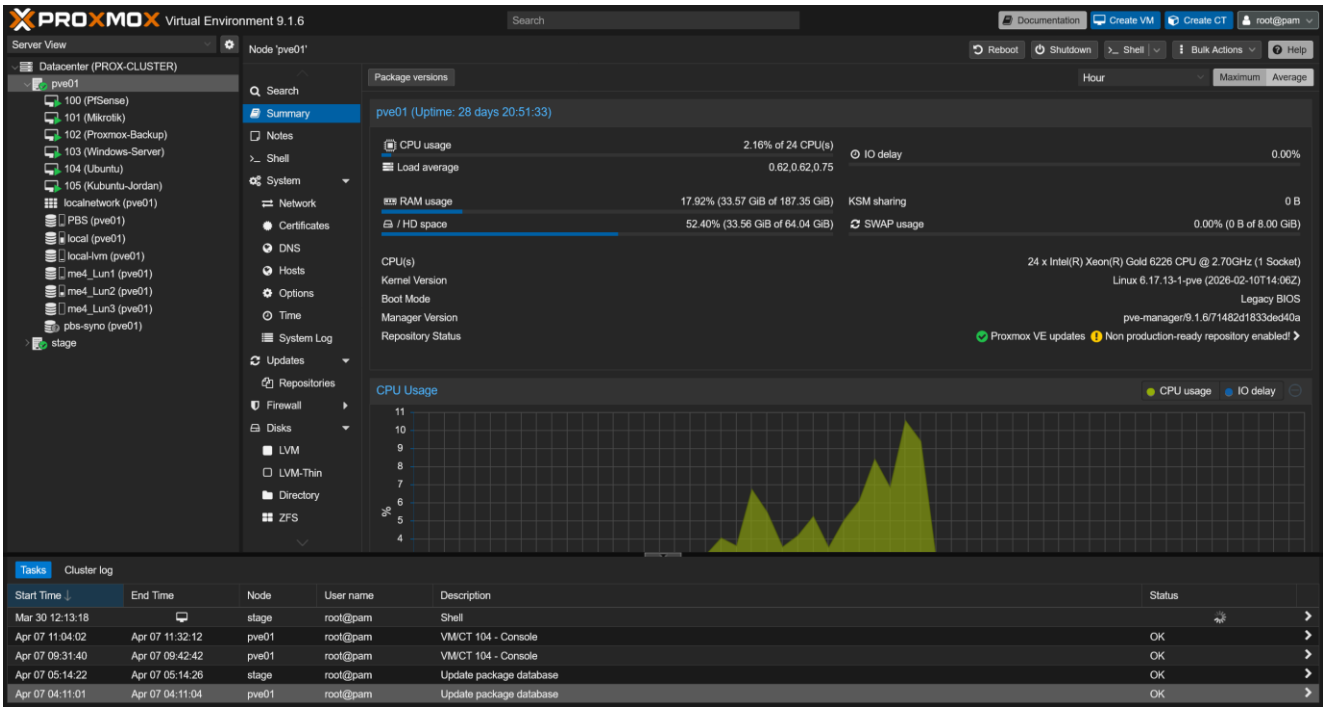
VLAN	Nom	Plage IP	Équipements	Rôle
VLAN 10	Utilisateurs	192.168.10.0/24	Postes clients, Wi-Fi	Accès aux services
VLAN 20	Serveurs	192.168.20.0/24	Serveurs, machines virtuelles	Hébergement des services
VLAN 30	Administration	192.168.30.0/24	iDRAC, iLO	Gestion de l'infrastructure

Ce tableau reprend la segmentation du réseau mise en place à l'aide des VLANs.

Chaque VLAN correspond à un réseau logique distinct permettant de séparer les différents types de trafic (utilisateurs, serveurs, administration).

Cette organisation permet d'améliorer la sécurité, de limiter les communications non autorisées et de faciliter l'administration du réseau.

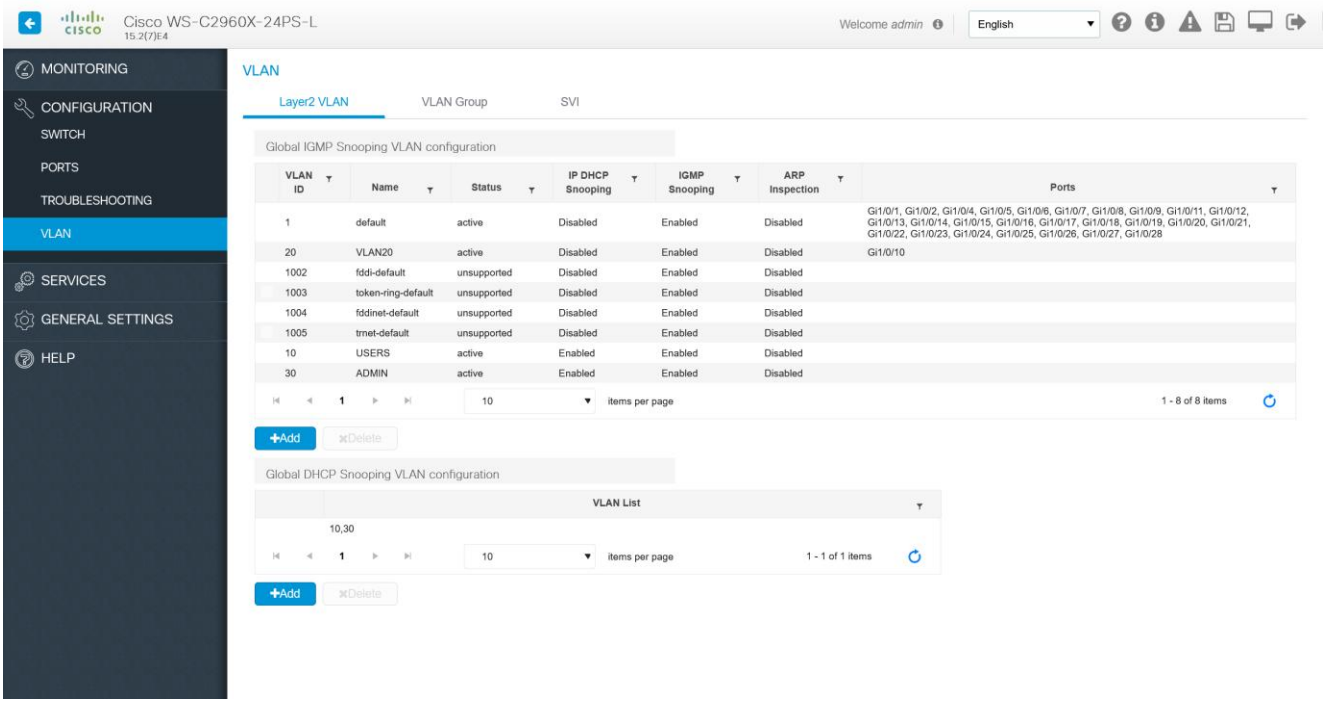
Annexe 3 : Interface Proxmox



Cette capture d'écran présente l'interface web de Proxmox utilisée pour administrer les machines virtuelles.

On y observe le nœud principal « pve01 », ainsi que plusieurs machines virtuelles déployées, notamment pfSense, Ubuntu et Windows Server.
Les informations de supervision telles que l'utilisation du CPU, de la mémoire et du stockage sont également visibles, permettant de contrôler l'état et les performances de l'infrastructure en temps réel.

Annexe 4 : Switch Cisco (VLAN / SSH)



Cette capture d'écran montre la configuration des VLANs sur le switch Cisco.

On y observe plusieurs VLANs créés afin de segmenter le réseau selon les usages :

- VLAN 10 pour les utilisateurs ;
- VLAN 20 pour les services ;
- VLAN 30 pour l'administration.

Cette segmentation permet d'isoler les flux réseau, d'améliorer la sécurité et de mieux organiser l'infrastructure.

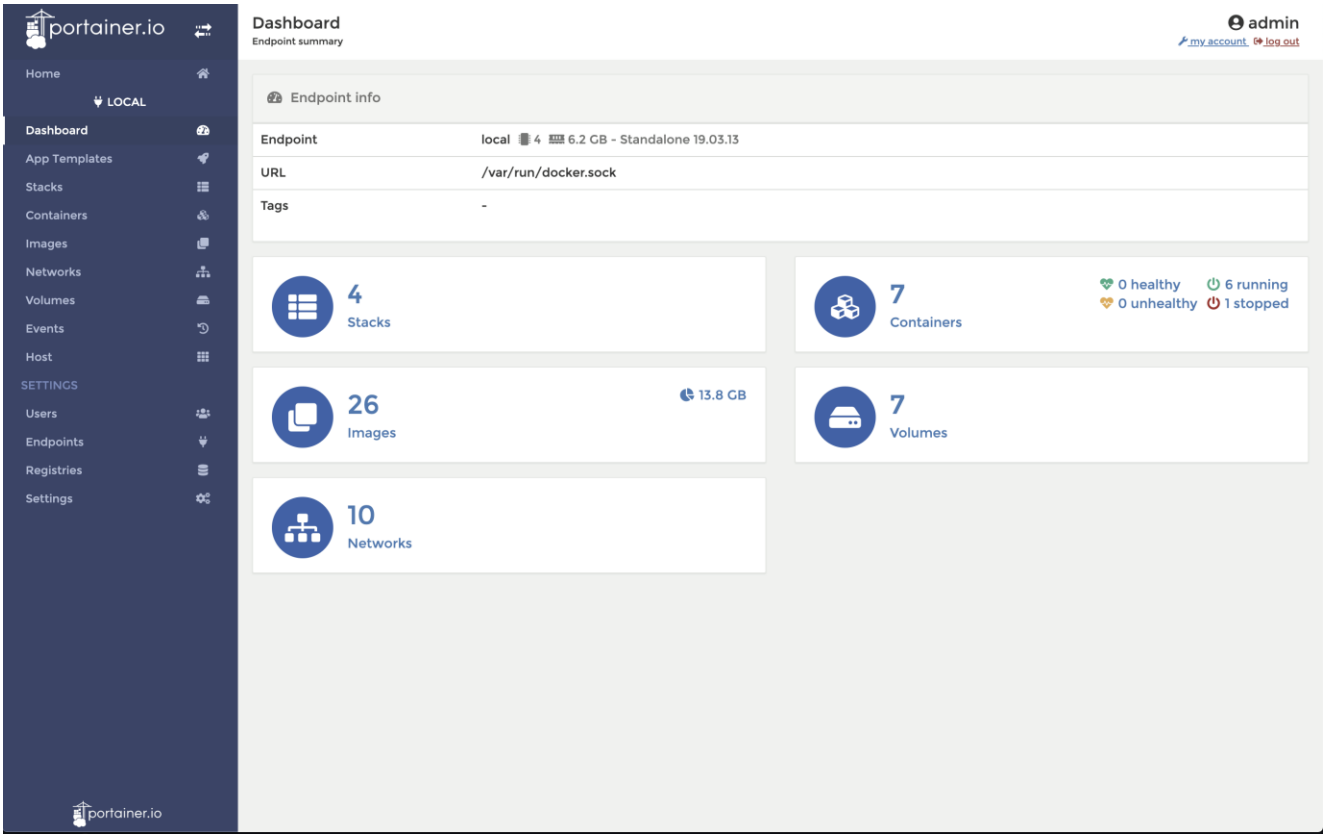
Annexe 5 : Règles PfSense

Ordre	Interface	Source	Destination	Port	Action	Description
n°1	WAN	Any	LAN	Any	Block	Bloquer tout accès externe
n°2	VLAN 30 (Admin)	Admin	Tous réseaux	Any	Allow	Accès complet administrateur
n°3	VLAN 20 (Servers)	Servers	Internet	Any	Allow	Mises à jour serveurs
n°4	VLAN 20 (Servers)	Servers	VLAN 10	Any	Block	Isolation serveurs → utilisateurs
n°5	VLAN 10 (Users)	Users	VLAN 30 (Admin)	Any	Block	Isolation utilisateurs → admin

n°6	VLAN 10 (Users)	Users	VLAN 20 (Servers)	HTTP/HTTPS	Allow	Accès aux services web
n°7	VLAN 10 (Users)	Users	Internet	Any	Allow	Accès Internet utilisateurs
n°8	VPN WireGuard	VPN clients	LAN	Ports spécifiques	Allow	Accès distant sécurisé
n°9	VPN WireGuard	VPN clients	Internet	Any	Allow	Accès Internet via VPN

Les règles ont été organisées selon un ordre logique, du plus restrictif au plus permissif, afin de garantir un niveau de sécurité optimal et d'appliquer le principe du moindre privilège.

Annexe 6 : Docker / Portainer

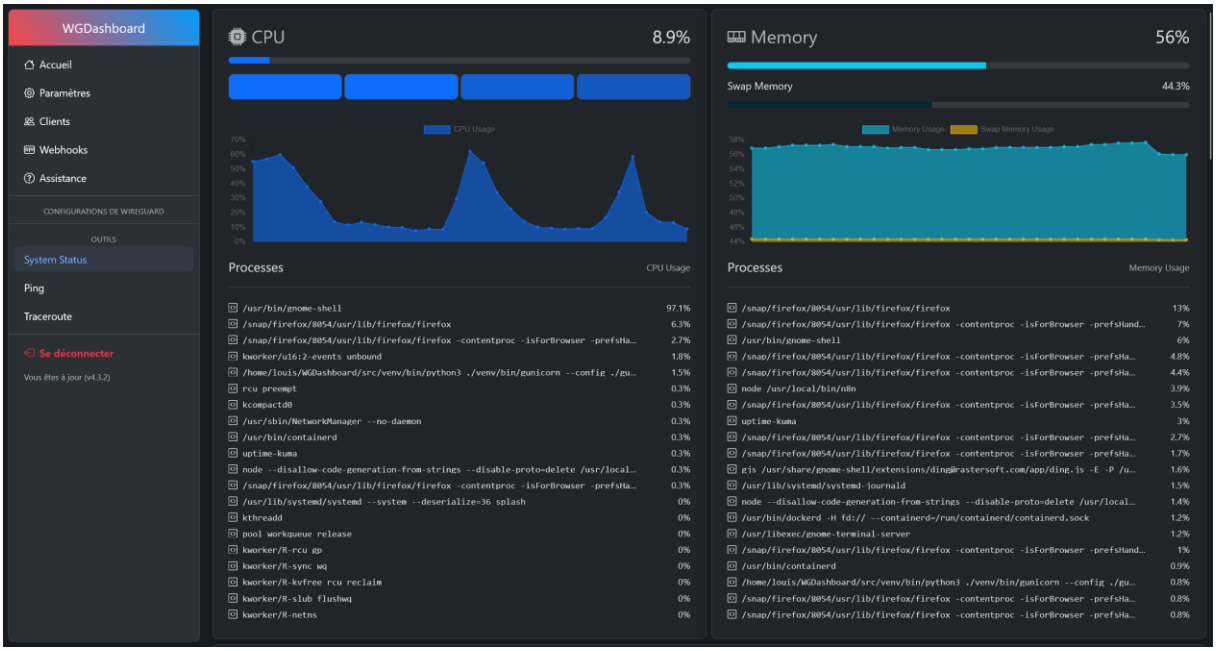


Cette capture d'écran affiche l'interface de gestion Docker via Portainer, utilisée pour administrer les conteneurs déployés sur l'infrastructure.

On y observe plusieurs services exécutés sous forme de conteneurs, notamment Portainer, Uptime Kuma, Vaultwarden et n8n.

L'utilisation de Docker permet de déployer rapidement des services tout en assurant leur isolation, leur maintenance simplifiée et leur mise à jour centralisée.
Quant à Portainer, il facilite l'administration de ces conteneurs grâce à une interface web centralisée, permettant de superviser leur état et de gérer leur déploiement.

Annexe 7 : WireGuard

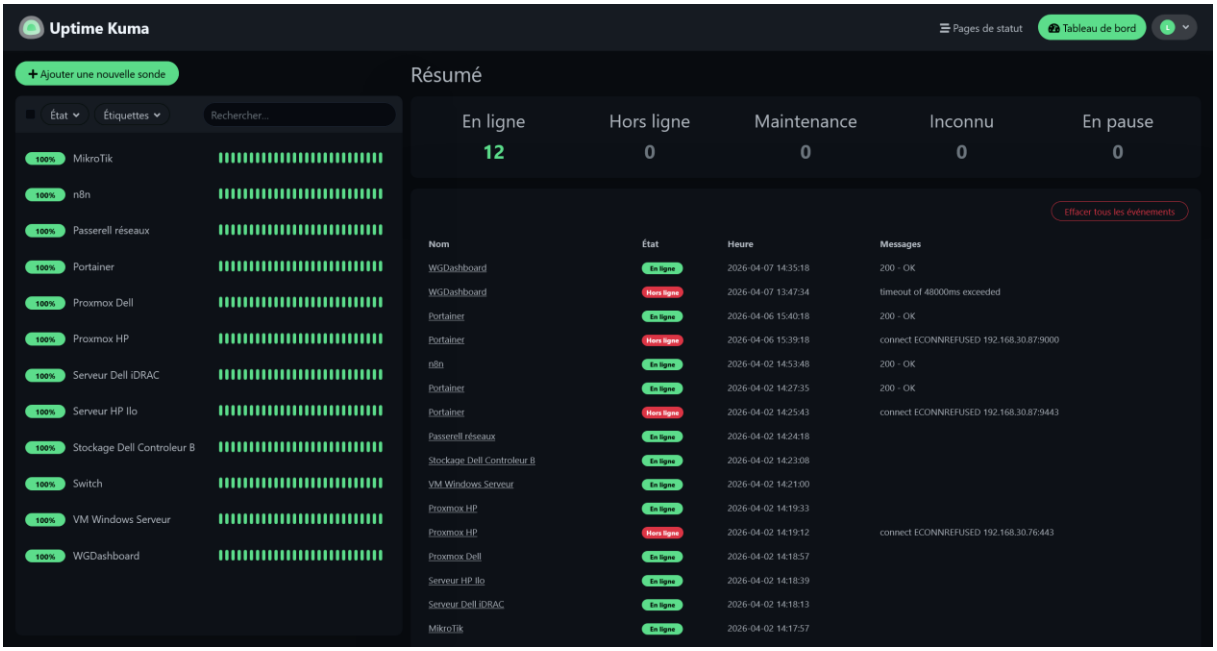


Cette capture d'écran montre l'interface WGDashboard utilisée pour administrer le VPN WireGuard.

Elle permet de superviser l'état du service ainsi que les ressources utilisées par le serveur, notamment l'utilisation du processeur, de la mémoire et les processus actifs.

WireGuard est un protocole VPN moderne permettant d'établir un tunnel sécurisé entre un client distant et le réseau interne.
Il permet aux utilisateurs autorisés d'accéder aux ressources de l'infrastructure de manière sécurisée.

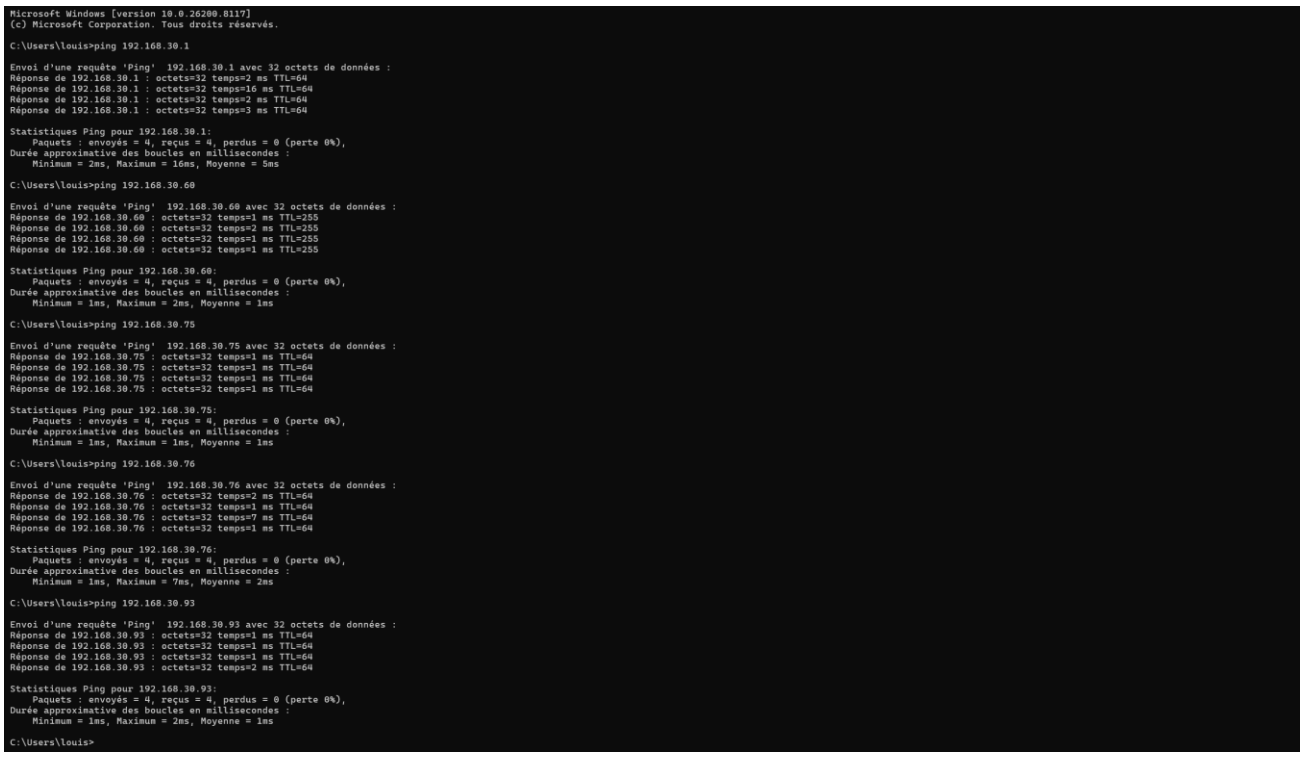
Annexe 8 : Uptime Kuma



Cette capture d'écran concerne l'outil de supervision Uptime Kuma utilisé pour surveiller la disponibilité des services de l'infrastructure.

Les différents services sont testés régulièrement afin de vérifier leur bon fonctionnement. En cas de panne ou d'indisponibilité, une alerte peut être générée, ce qui améliore la réactivité en cas d'incident.

Annexe 9 : Tests



Cette capture d'écran affiche les tests de connectivité réalisés depuis un poste client afin de valider le bon fonctionnement du réseau.

Des requêtes ping ont été effectuées vers plusieurs équipements de l'infrastructure :

- passerelle (192.168.30.1) ;
- switch (192.168.30.60) ;
- serveurs (192.168.30.75 et 192.168.30.76) ;
- NAS (192.168.30.93).

Les résultats montrent que tous les équipements répondent correctement, avec un taux de perte de paquets nul (0 %). Cela confirme la bonne communication au sein du réseau.

Annexe 10 : Exemple de résolution d'un incident

Lors de la mise en place de l'infrastructure, un problème de communication entre les VLANs a été rencontré. En effet, les machines situées dans différents réseaux ne pouvaient pas communiquer entre elles, empêchant l'accès à certains services.

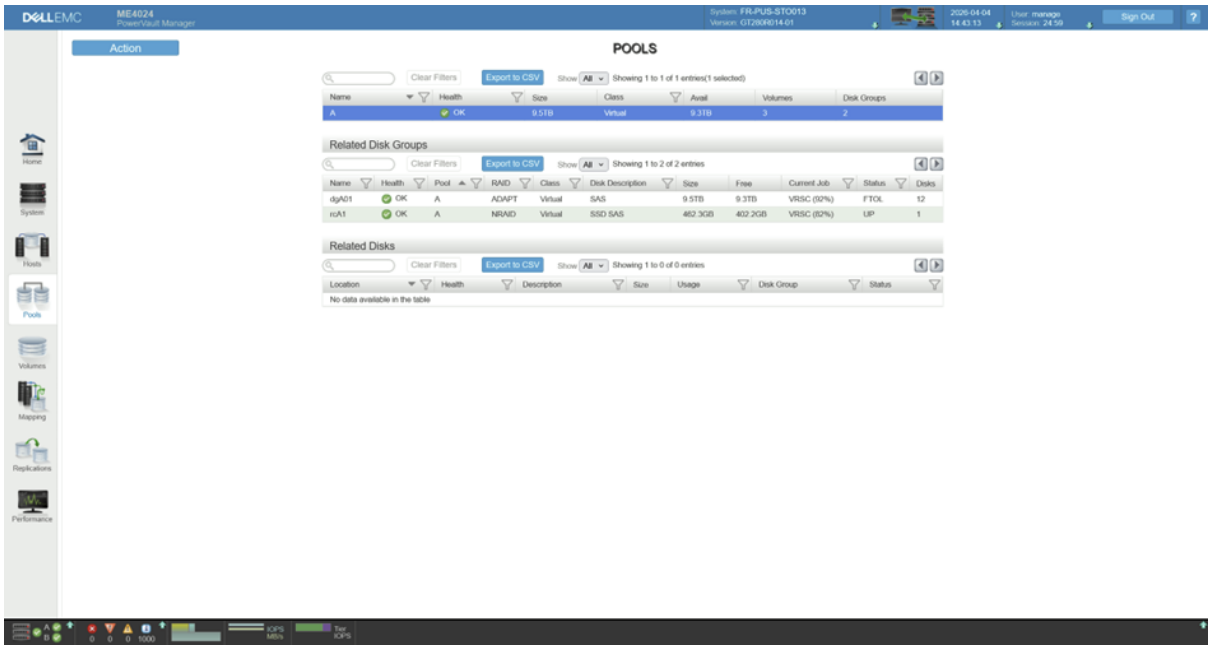
Après analyse, il a été constaté que certains ports du switch Cisco n'étaient pas correctement configurés dans les VLANs appropriés.

La configuration du switch a été corrigée en ajustant l'attribution des VLANs sur les ports concernés.

Des tests de connectivité ont ensuite été réalisés afin de valider la correction.

Après cette intervention, la communication entre les équipements a été rétablie et l'infrastructure est devenue pleinement opérationnelle.

Annexe 11 : Architecture et configuration du stockage



Cette capture d'écran reprend l'architecture de stockage du SAN Dell EMC ME4024.

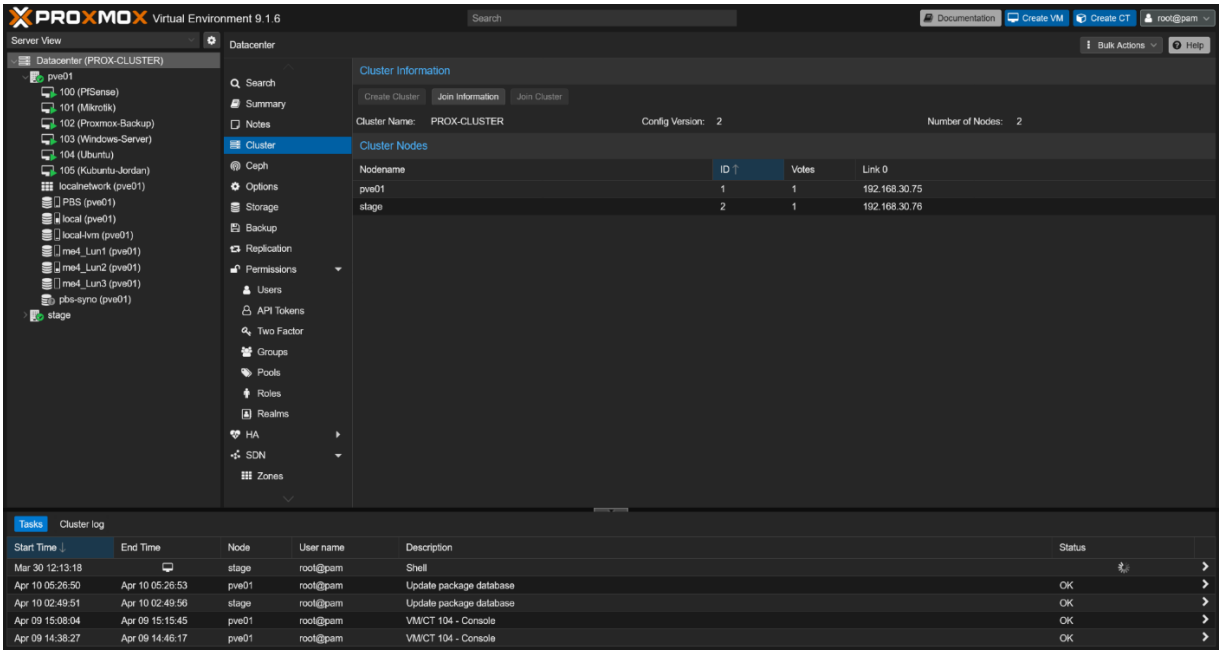
On y observe l'organisation des disques en pools de stockage ainsi que leur état, permettant d'assurer la fiabilité et les performances du système.

Le SAN est utilisé pour héberger les machines virtuelles et offre des performances élevées grâce à l'utilisation de disques configurés en RAID.

Un NAS Synology est également utilisé en complément pour le stockage de fichiers et les sauvegardes.

Pour rappel, cette organisation optimise les performances et améliore la disponibilité des données.

Annexe 12 : Cluster Proxmox



Cette capture d'écran vise le cluster Proxmox mis en place au sein de l'infrastructure.

On y observe les deux nœuds du cluster, permettant de regrouper plusieurs serveurs physiques afin de les administrer comme une seule entité.

Cette architecture permet une gestion centralisée des machines virtuelles ainsi qu'une meilleure répartition des ressources.

Le cluster améliore également la disponibilité des services et facilite l'administration de l'infrastructure. Il rend également possible la migration des machines virtuelles entre les différents nœuds.

Annexe 13 : Tableau des équipements de l'infrastructure

Nom de la VM	Système d'exploitation	Rôle
pfSense	FreeBSD	Pare-feu et routage réseau
Ubuntu	Linux (Ubuntu Server)	Hébergement des services Docker (Portainer, Uptime Kuma, WireGuard, n8n)
Windows Server	Windows Server	Services réseau et administration
Proxmox Backup	Linux	Sauvegarde des machines virtuelles
Mikrotik	RouterOS	Simulation réseau / routage

Ce tableau reprend les différentes machines virtuelles déployées au sein de l'infrastructure.

Chaque machine virtuelle remplit un rôle spécifique permettant de séparer les services et d'optimiser l'utilisation des ressources.

Cette organisation facilite la gestion, la maintenance et la sécurité de l'infrastructure.

Annexe 14 : Tableau des équipements de l'infrastructure

Équipement	Modèle	Adresse IP	Rôle
Routeur / Passerelle	—	192.168.30.1	Accès réseau / Internet
Switch	Cisco Catalyst 2960-X	192.168.30.60	Commutation réseau
Serveur 1	Dell PowerEdge R740	192.168.30.75	Virtualisation (Proxmox)
Serveur 2	HP ProLiant DL380	192.168.30.76	Virtualisation / cluster
iDRAC	Dell	192.168.30.70	Gestion serveur Dell
iLO	HP	192.168.30.71	Gestion serveur HP
SAN	Dell EMC ME4024	192.168.30.91 / 92	Stockage des VM
NAS	Synology	192.168.30.93	Stockage / partage de fichiers
Point d'accès Wifi	—	192.168.30.58	Accès réseau sans fil
Poste client	PC utilisateur	192.168.30.188	Accès utilisateur

Ce tableau énumère les principaux équipements composant l'infrastructure et permet d'identifier rapidement le matériel utilisé, son adresse IP ainsi que son rôle dans le réseau.

Cette vue synthétique facilite la compréhension globale de l'architecture mise en place.