SAE Legends CUP

Rapport SAE

Groupe E

Membre :

Thomas CAPHAM

Alexandre DUSSAUX

Louis JULE

Morgan SALHI

Pierre EYSSERIC

Elouan ORDY

Axel THÉVENOUX

UNIVERSITÉ CÔTE D'AZUR

Intégris

Réponse à appel d’offre

Modernisation de l’infrastructure IT et sécurisation des sites

Client : TechNova

Sommaire

Présentation d’Intégris

Integris est née d'une promesse forte : restaurer l'intégrité des systèmes d'information, bien trop longtemps négligée par bon nombre d’entreprises. Basée au cœur de l'Éco-Vallée à Nice, notre entreprise bénéficie d'un positionnement stratégique à la jonction de la technopole de Sophia Antipolis et de l'Aéroport International. Nous nous positionnons comme des "**architectes d'un monde connecté**" et agissons comme le nœud de raccordement entre la complexité technique de nos projets et notre ouverture aux divers entreprises européennes.

Notre histoire

Depuis nos débuts, Integris n'a cessé de grandir pour passer du statut de petite start-up niçoise à celui de véritable plateforme européenne :

- 2014 - Année de la création d'Integris. L'entreprise s'implante à l'Éco-Vallée de Nice et devient rapidement un prestataire local majeur, capable d'accompagner chaque partenaire tout au long de son développement.

- 2018 - Cherchant à s'exporter, Integris fait le pari de reprendre les rênes d'une petite start-up polonaise à Varsovie. Cette étape nous a permis d'élargir nos champs de compétences et de nous approprier de nouveaux talents.

- 2020 - L'Allemagne nous ouvre ses portes sur de nouveaux marchés, nous permettant d'être au contact de l'écosystème start-up le plus dynamique d'Europe à Berlin.

- 2022 - Dans le but de fluidifier nos opérations logistiques et de faciliter le support pour l'Europe du Sud, Integris s'implante à Barcelone.

Aujourd'hui, le siège de Nice agit comme une tour de contrôle qui synchronise l'innovation berlinoise, la puissance technique varsovienne et l'agilité barcelonaise. Faire appel à Integris, c'est s'offrir l'accès à un réseau de compétences interconnectées à l'échelle européenne.

Nos compétences

Notre savoir-faire technique s'articule autour de quatre grands domaines d'expertise :

- Audit & Création : Nous réalisons une cartographie et une analyse approfondie de l'infrastructure existante ainsi que de votre demande.
- Conception : Nous gérons l'API Management et la conception de développements sur-mesure, portés par notre pôle de Varsovie.
- Mise en œuvre : Nous prenons en charge la conception du réseau, ainsi que des différents systèmes et services à mettre en place dans l'entreprise cliente, afin de pouvoir réaliser l'infrastructure complète.
- Accompagnement : Nous assurons la conduite du changement en proposant des formations adaptées pour garantir une parfaite adaptation des employés aux nouveaux systèmes.

Notre philosophie

Philosophie et RSE

L'identité d'Integris repose sur la conviction que la performance technologique ne peut être dissociée d'une responsabilité éthique et environnementale forte. Pleinement conscients de l'impact écologique généré par les solutions numériques modernes, nous plaçons la durabilité au centre de notre ingénierie. Cette démarche concrète nous pousse à optimiser chacune de nos infrastructures pour qu'elle soit la plus pérenne possible, privilégiant ainsi la longévité du matériel et l'éco-conception logicielle pour réduire l'empreinte carbone de nos partenaires.

Cette vision d'un numérique responsable s'accompagne d'une volonté farouche de rendre la technologie plus humaine et accessible. Dans un secteur souvent perçu comme opaque ou fermé, nous militons pour une inclusion réelle, tant dans la conception de nos outils que dans notre culture d'entreprise. Ainsi, nos solutions sont vulgarisées pour être intelligibles par des non-experts, tandis que notre politique de recrutement s'appuie sur une stricte égalité des chances. Chez Integris, la compétence est l'unique critère de sélection, garantissant une mixité de genre et d'origine qui fait la richesse de nos pôles européens.

Toutefois, cet engagement éthique ne prend tout son sens que s'il est soutenu par une rigueur opérationnelle sans faille. C'est pourquoi la qualité de nos services est systématiquement validée par une expertise technique de haut niveau. Tous les techniciens et ingénieurs d'Integris sont formés et certifiés selon les standards les plus exigeants de l'industrie, tels que les normes ISO ou les certifications constructeurs (Cisco, Stormshield). Cette alliance entre conscience sociale et excellence technique nous permet de livrer des solutions qui sont non seulement porteuses de valeurs, mais aussi hautement sécurisées et performantes.

Le cycle en 5 temps

Notre approche s'articule autour d'un cycle rigoureux en 5 étapes, conçu au cours de nos nombreuses années d'expériences pour assurer le succès de chaque projet. Cette méthodologie repose sur un principe fondamental qui guide toutes nos actions :

"On ne code rien avant d'avoir audité, on ne livre rien sans former."

1. *Audit et conseil*

Cette première étape est cruciale pour comprendre votre environnement. Elle consiste en une cartographie et une analyse approfondie de l'infrastructure existante, ainsi que de vos demandes spécifiques. L'objectif est d'identifier les forces, les faiblesses et les axes d'amélioration de votre système d'information avant toute intervention.

2. *Architecture*

Sur la base de l'audit, nous passons à la phase de conception. Nous élaborons une architecture sur-mesure, qu'il s'agisse de la conception du réseau ou de la réalisation d'infrastructures complètes comme ici.

3. *Intégration*

C'est la phase de mise en œuvre. Nos équipes techniques déploient les solutions validées lors de la phase d'architecture. Nous procédons à l'installation matérielle, logicielle et réseau, en veillant à l'intégration fluide de ces nouveaux outils au sein de votre environnement, tout en minimisant les interruptions de service.

4. *Formation*

La réussite d'un projet technologique dépend de son adoption par les utilisateurs. Nous proposons un accompagnement complet et une formation adaptée. Nous gérons la conduite du changement pour garantir que vos employés s'approprient les nouveaux outils et processus de manière optimale.

5. *Support*

Notre engagement ne s'arrête pas à la livraison du projet. Nous assurons également un support continu pour garantir la stabilité, la sécurité et l'évolution de votre infrastructure. Cela inclut la maintenance, la résolution d'incidents et l'assistance à vos équipes au quotidien.

Nos normes et certifications

La solidité opérationnelle d'Integris s'appuie sur une conformité rigoureuse aux standards internationaux, garantissant un niveau de sécurité et de confiance optimal pour nos clients. Pour nos activités liées au Cloud et au SaaS, nous avons ainsi validé la certification SOC 2 Type II, qui constitue un gage de fiabilité majeur pour nos partenaires internationaux. Cette exigence de protection des données est renforcée par notre mise en conformité avec le Texas Data Privacy and Security Act (TDPSA), obligatoire depuis 2024, ainsi que par notre adhésion au Data Privacy Framework qui sécurise juridiquement les flux d'informations entre l'Union Européenne et les États-Unis.

Cette rigueur normative est indissociable du savoir-faire hautement spécialisé de nos équipes de terrain. L'expertise d'Integris est continuellement attestée par les plus grandes certifications de l'industrie, notamment celles délivrées par Cisco, allant des fondamentaux réseau jusqu'au niveau expert CCIE en Routing & Switching, incluant des spécialisations Wireless et Sécurité. En complément, nous maîtrisons les solutions de protection périmétrique les plus avancées grâce à nos certifications Stormshield, telles que les titres CSNTS et OSEE. C'est cette alliance entre le respect des cadres réglementaires et une maîtrise technique certifiée qui nous permet d'assurer l'intégrité et la résilience des systèmes d'information que nous déployons.

Nous sommes également certifiés par la marque Ubiquiti avec les certifications UniFi Full Stack Professional (UFSP), UniFi Wireless Admin (UWA), UniFi Routing, Switching & Cybersecurity Admin (URSCA) et UniFi Network Professional (UNP). Ces certifications attestent de notre maîtrise complète de l'écosystème UniFi et démontrent notre capacité à concevoir, déployer et maintenir des infrastructures conformes aux standards et aux bonnes pratiques du constructeur.

Nos chiffres

La solidité d'Integris se traduit par une croissance constante et une présence affirmée sur le marché européen de l'intégration de systèmes. Depuis sa création en 2014, l'entreprise a su s'imposer comme un acteur de référence, atteignant aujourd'hui un chiffre d'affaires de 48,5 millions d'euros. Cette réussite repose sur l'expertise de nos 140 collaborateurs, répartis à travers un réseau de quatre hubs stratégiques situés à Nice, Berlin, Barcelone et Varsovie. Ce maillage européen nous permet d'allier proximité locale et puissance d'intervention internationale pour répondre aux enjeux technologiques de nos clients.

Résumer de l’appel d’offre

La société TechNova Industries, fondée en 1999, s’est imposée comme une PME internationale de référence dans le secteur de l’IoT industriel, s’appuyant sur une croissance rapide portée par ses innovations dans les capteurs intelligents et les plateformes cloud. Forte de ses 650 collaborateurs répartis sur huit sites stratégiques incluant le siège à Paris, des centres de R&D à Lyon et des unités de production à Lille et Rabat l’entreprise fait aujourd'hui face à un défi structurel majeur. En effet, son infrastructure informatique n’a pas suivi cette expansion et présente désormais des faiblesses critiques identifiées lors d'un audit interne, menaçant la cohérence et la sécurité globale du groupe.

Le diagnostic actuel révèle une dette technologique hétérogène sur plusieurs piliers fondamentaux. L’Active Directory, reposant sur un domaine unique, souffre d’un vieillissement des stratégies de groupe (GPO), d'une gestion défaillante des comptes à privilèges et d'une segmentation insuffisante. Parallèlement, le réseau international, interconnecté via des tunnels VPN IPsec, repose sur un mélange complexe de marques et de matériels souvent obsolètes, avec une segmentation VLAN trop faible pour les standards actuels. Le parc bureautique n’est pas épargné, avec des stations de travail sous Windows 7 ou 10 et un système de téléphonie en cuivre totalement dissocié de l’informatique, générant des coûts d'exploitation élevés.

Pour remédier à ces vulnérabilités, TechNova Industries engage une refonte globale sous un délai de 24 mois. Ce plan ambitieux prévoit une remise à plat de l’Active Directory via un modèle de tiering et une possible migration hybride vers Azure AD, intégrant systématiquement l’authentification multi-facteurs. La modernisation du réseau vise à uniformiser les équipements vers des solutions managées de nouvelle génération (NGFW), à instaurer une architecture Zero Trust et à déployer un Wi-Fi sécurisé aux normes WPA3-Enterprise. Un volet spécifique est également dédié au nouveau complexe R&D de Lyon-Bron, exigeant une sécurisation physique renforcée incluant vidéosurveillance et contrôle d’accès ainsi que des solutions de stockage numérique garantissant le secret des recherches.

Enfin, le projet doit intégrer des dimensions prospectives et innovantes pour pérenniser l'activité de l'entreprise. Cela inclut l'évolution du SOC interne vers une version plus mature capable de monitorer l'ensemble des sites, ainsi que l'exploitation de l'intelligence artificielle pour la cyberdéfense et la prévention des fuites de données liées à l'IA générative. L'ensemble de la migration doit impérativement minimiser l'impact sur la production industrielle, respecter les contraintes de conformité GDPR et démontrer sa viabilité technique à travers une Preuve de Concept (POC) fonctionnelle réalisable en moins de huit heures.

Notre solution proposer

Introduction

Fidèles à la promesse fondamentale d'Integris de restaurer l'intégrité des systèmes d'information, nous avons conçu une solution technique sur-mesure répondant précisément aux enjeux identifiés lors de notre phase préalable d'audit. Notre réponse technique s'articule autour des trois piliers qui font notre force :

“Intégrer, Optimiser et Innover.”

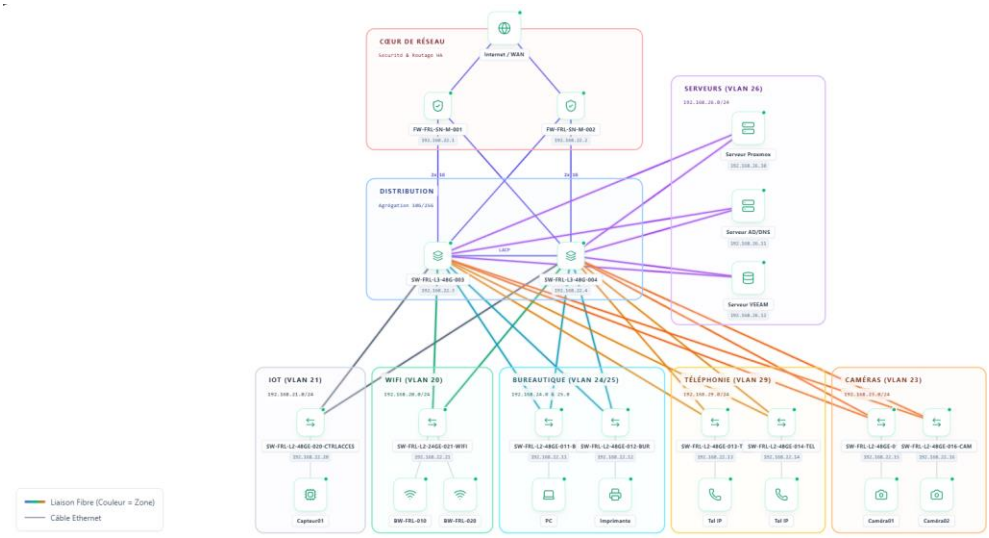
La solution globale que nous vous présentons aujourd'hui a été pensée pour allier excellence technologique, sécurité de bout en bout et respect de nos engagements RSE (notamment via la prolongation de la vie du matériel). Elle repose sur des choix stratégiques forts :

- Sécurité et Compartimentation : Une protection granulaire limitant drastiquement la surface d'attaque grâce à des équipements de pointe.
- Souveraineté et Résilience : Une maîtrise totale de l'hébergement et des stratégies de sauvegarde immuables répondant aux standards internationaux.
- Haute Disponibilité : Des solutions matérielles et logicielles capables de soutenir votre productivité et de garantir une véritable continuité d'activité.

Nous n'ajoutons aucune brique applicative ou serveur sans avoir préalablement consolidé le terrain. Une infrastructure performante exige un socle de communication sans faille. C’est la raison pour laquelle notre solution prend racine dans la conception, l'optimisation et la sécurisation de votre Architecture Réseau (LAN).

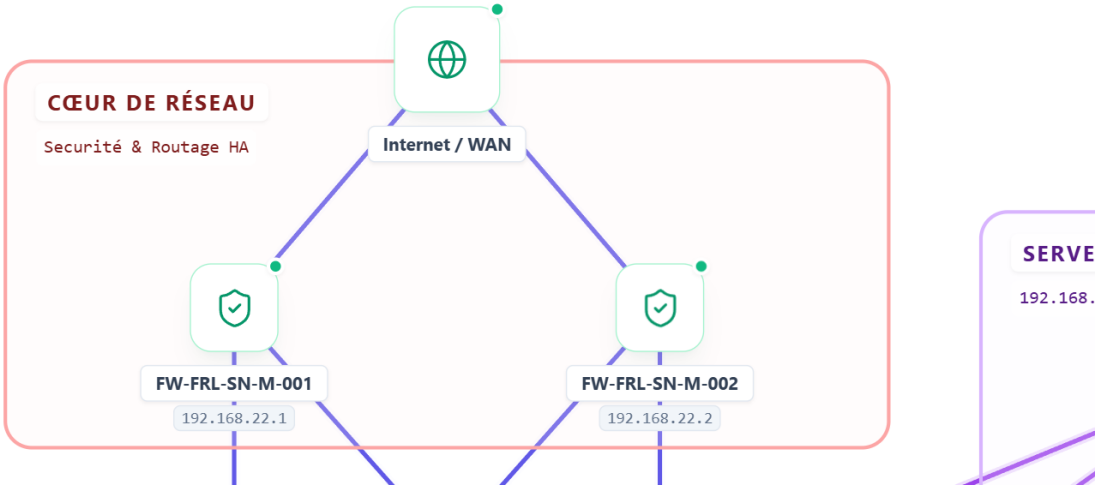
Architecture réseaux

Notre architecture réseau a été pensée pour répondre à une double exigence : assurer une communication fluide et performante entre les différents sites tout en garantissant une étanchéité stricte pour des raisons de cybersécurité.

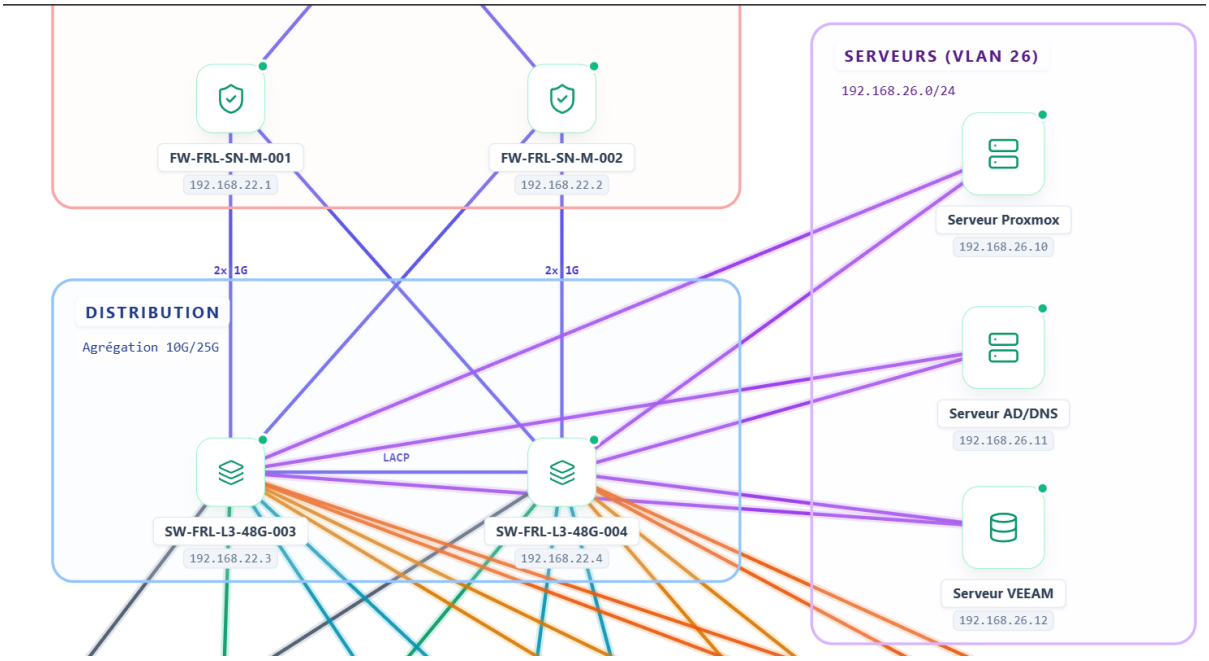


Le réseau s'articule autour d'une conception hiérarchique en trois couches, garantissant une haute disponibilité et une tolérance aux pannes :

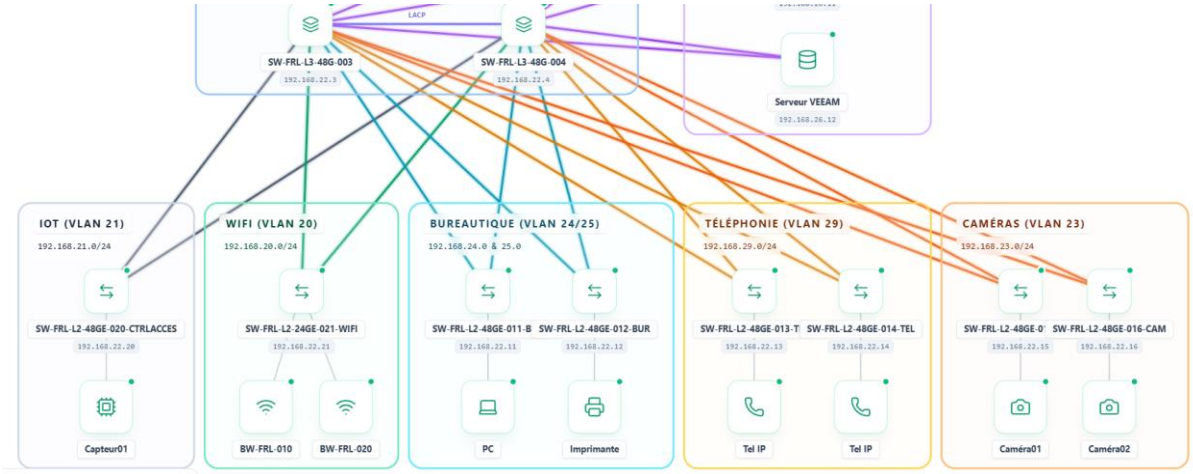
- Couche Cœur de Réseau : C'est le point d'entrée vers Internet (WAN). Elle est constituée de pare-feux déployés en Haute Disponibilité (HA), assurant à la fois le routage intelligent entre les différents sites de l'entreprise via des flux VPN IPSec, et aussi le filtrage strict des paquets (Next-Gen Firewalling) en appliquant des règles de sécurité à l'entrée et à la sortie de chaque site.



- Couche de Distribution : En dessous, le trafic est centralisé via des commutateurs de niveau 3 SFP. Pour répondre aux besoins importants en bande passante (notamment pour l'hébergement serveur / DMZ et les sauvegardes), ces liaisons d'agrégation sont dimensionnées pour supporter des débits allant de 10G à 25G.



- Couche d'Accès : C'est à ce niveau que les différents équipements finaux seront connectés (PC, téléphones, caméras, bornes WiFi et autres équipements IOT). Nous avons déployé des commutateurs de niveau 2 (L2) spécialisés et physiquement répartis selon les besoins des différents services.



La couche d’accès demande une attention toute particulière. En effet, pour des raisons de sécurité évidentes et d'optimisation des performances (réduction des domaines de diffusion ou broadcast), nous avons catégoriquement rejeté l'idée d'un réseau "plat", nous permettant ainsi de conserver la logique de base, tout en l’améliorant pour appliquer les meilleurs pratiques. Le réseau a donc été rigoureusement segmenté via la mise en place de réseaux locaux virtuels (VLAN) supplémentaires dans le range IP 192.168.X.X/24, garantissant une compartimentation des services propre et uniforme pour chaque site (avec certain VLAN supplémentaires pour des services spécifique).

Site	VLAN	Service	Sous réseaux
Tous	999	Trash	X
Paris	10	Wifi	192.168.10.0/24
Paris	11	IOT	192.168.11.0/24
Paris	12	Administration réseau	192.168.12.0/24
Paris	13	Caméras	192.168.13.0/24
Paris	14	Imprimantes	192.168.14.0/24
Paris	15	Bureautique	192.168.15.0/24
Paris	16	Serveurs (Datacenter)	192.168.16.0/24
Paris	17	DMZ (partenaire)	192.168.17.0/24
Paris	18	AD / Exchange	192.168.18.0/24
Paris	19	Téléphonie	192.168.19.0/24
Paris	**421**	**Natif**	**X**
Lyon	20	Wifi	192.168.20.0/24
Lyon	21	IOT	192.168.21.0/24
Lyon	22	Administration réseau	192.168.22.0/24
Lyon	23	Caméras	192.168.23.0/24
Lyon	24	Imprimantes	192.168.24.0/24
Lyon	25	Bureautique	192.168.25.0/24
Lyon	26	Serveurs (R&D)	192.168.26.0/24
Lyon	27	DMZ	192.168.27.0/24
Lyon	28	AD / Exchange	192.168.28.0/24
Lyon	29	Téléphonie	192.168.29.0/24
Lyon	**120**	**Développement IOT**	**192.168.120.0/24**
Lyon	**422**	**Natif**	**X**

Chaque type de flux, d'utilisateur ou d'équipement (Serveurs, IoT, Vidéosurveillance, Téléphonie, etc.) est isolé dans son propre sous-réseau. Cette compartimentation, en plus de permettre une distribution des flux contrôlés et équilibrés, empêche le déroulement de certaines attaques sur la couche d’accès, comme un potentiel logiciel malveillant qui pourrait se propager d'un poste de travail bureautique vers les serveurs critiques ou les équipements d'administration (Tier 0).

En plus des VLAN implémentés pour les différents services, nous avons ajouté un "VLAN Trash" (999), qui sera configuré par défaut sur tous les ports non utilisés pour parer aux tentatives d'intrusion physiques, et un “VLAN Natif”, permettant le transfert des trames non taguées sur un VLAN différent du VLAN par défaut. En effet, il est fondamental de

sécuriser ce VLAN afin d'éviter les attaques de type VLAN Hopping, permettant d'utiliser les trames non taguées pour passer d'un VLAN à un autre sans autorisations.

Firewall et routage

La solution retenue repose sur le déploiement de deux firewalls par site, interconnectés via un réseau privé virtuel (VPN) IPsec en topologie maillée (Full Mesh), intégrant le routage inter VLAN des sites, ainsi que des capacités avancées de filtrage de flux et la gestion locale du service DHCP.

Ces choix techniques structurants ont été pensés pour répondre aux exigences suivantes :

- Continuité d'activité et Haute Disponibilité (Deux pare-feux par site) : Le déploiement d'un cluster de firewalls (en mode actif/passif ou actif/actif) sur chaque site permet d'éliminer les points de défaillance uniques (Single Point of Failure). En cas de panne matérielle ou de maintenance sur un équipement, le second prend immédiatement le relais, garantissant une continuité de service transparente pour les utilisateurs.
- Sécurité et performance des interconnexions (VPN IPsec en maille) : Le protocole IPsec assure un chiffrement robuste et garantit l'intégrité et la confidentialité des données transitant entre les sites. Le choix d'une topologie en maille permet à chaque site de communiquer directement avec les autres, sans transiter par un site central. Cela réduit drastiquement la latence, optimise la bande passante et empêche la congestion du réseau.
- Protection et segmentation (Filtrage de flux) : Les firewalls assureront un filtrage granulaire des flux réseau entrants, sortants et inter-sites. Cette approche "Zero Trust" permet de limiter les accès aux strictes nécessités métiers, de bloquer les menaces externes (malwares, intrusions) et de confiner d'éventuelles attaques internes grâce à une segmentation réseau stricte.
- Simplification de l'infrastructure locale (Service DHCP) : L'hébergement du service DHCP directement sur les firewalls permet d'attribuer dynamiquement les adresses IP aux équipements de chaque site. Cela réduit la complexité de l'infrastructure matérielle locale (en évitant l'installation de serveurs dédiés à ce service) tout en centralisant la gestion réseau sur l'équipement de sécurité.

En combinant résilience, chiffrement, contrôle d'accès strict et simplification de la gestion locale, cette nouvelle architecture dote l'entreprise d'un socle réseau robuste, évolutif et prêt à soutenir ses futurs besoins.

Réseaux LAN

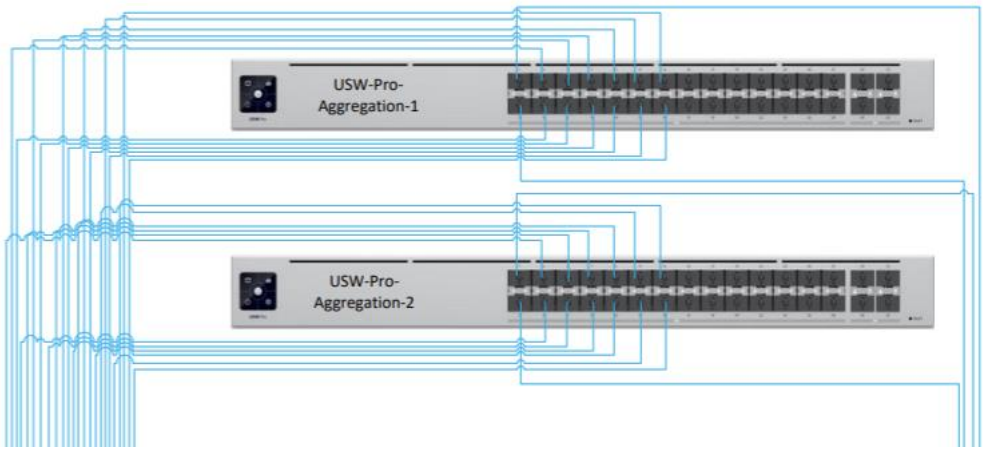
Pour ce qui concerne le réseau interne que nous vous proposons de déployer sur l'ensemble de vos différents sites, celui-ci a été entièrement conçu en réponse à votre demande. Vous souhaitiez une infrastructure offrant un maximum de performances et de fonctionnalités tout en conservant un coût compétitif. C'est pour cette raison que nous avons fait le choix d'implémenter des équipements de la marque Ubiquiti Inc, la gamme Unifi, constructeur avec lequel nous travaillons régulièrement et dont les solutions offrent un excellent compromis entre performance, fiabilité et budget.

Ubiquiti Inc. est un fabricant américain spécialisé dans les équipements réseau professionnels. La marque est reconnue pour ses solutions centralisées, simples à administrer et sans aucune licence.

Nous utiliserons leurs switches pour assurer la couche d'accès ainsi que la couche de distribution, notamment des modèles issus de la gamme professionnelle Pro / Pro HD.

Pour le cœur du réseau interne, correspondant à la couche de distribution, nous avons retenu des switches d'agrégation afin d'assurer la centralisation des flux provenant des switches d'accès. Le modèle choisi est le USW-Pro-Aggregation de chez Ubiquiti Inc.. Il s'agit d'un switch disposant de 28 ports SFP+ en 10 Gb/s ainsi que de 4 ports SFP28 en 25 Gb/s, ces derniers étant principalement utilisés pour les liaisons à très haut débit, notamment pour l'interconnexion entre les deux équipements du cœur de réseau.

Ces switches seront déployés par paire sur chaque site pour des raisons de redondance et de haute disponibilité. Cette architecture permet d'assurer une continuité de service en cas de défaillance d'un des équipements et d'éviter tout point unique de défaillance au niveau de la distribution.

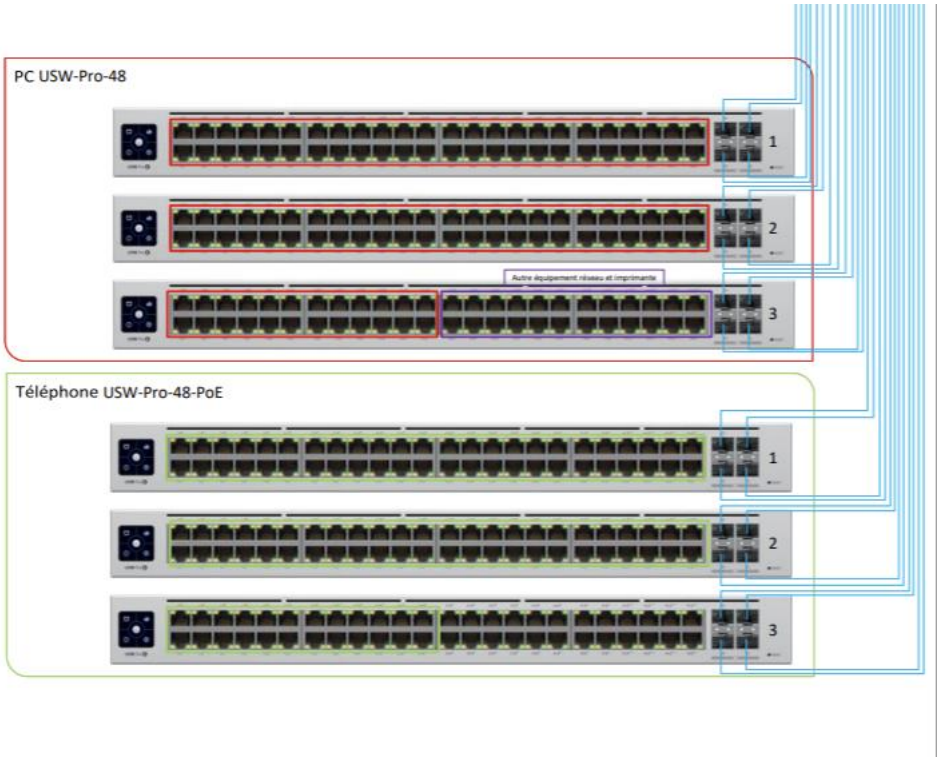


Le dimensionnement du nombre de switches nécessaires a été réalisé à partir des données que vous nous avez fournies concernant le nombre de postes de travail par site.

Chaque employé nécessite une liaison RJ45 pour son poste informatique, mais également une liaison dédiée pour son téléphone IP. Il est courant que l'ordinateur soit raccordé directement au téléphone, ce qui permet de mutualiser une seule prise réseau. Toutefois, cette pratique n'est pas recommandée dans un environnement professionnel. En cas de défaillance du téléphone ou de problème matériel, l'utilisateur perdrait également la connectivité de son poste informatique. Nous avons donc privilégié une architecture plus robuste avec deux prises distinctes par poste.

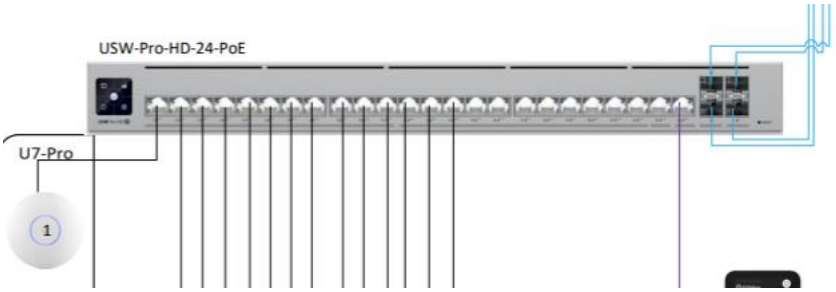
Cela implique qu'une des liaisons devra supporter l'alimentation électrique du téléphone via la technologie PoE (Power over Ethernet). Ce protocole permet de transmettre une alimentation basse tension directement à travers le câble réseau, ce qui évite l'utilisation d'alimentations externes et simplifie l'installation. Afin de répondre à ce besoin, nous avons prévu l'utilisation de deux modèles de switches différents : le modèle USW-Pro-48, qui dispose de 48 ports Gigabit Ethernet ainsi que de 4 ports uplink SFP+ en 10 Gb/s pour les interconnexions montantes, et sa version PoE, le USW-Pro-48-PoE, destinée à l'alimentation des téléphones IP.

Par exemple, pour le site de Paris qui compte 120 employés, nous devons prévoir 120 connexions pour les postes informatiques et 120 connexions PoE pour la téléphonie. En tenant compte de la capacité de 48 ports par switch, cela représente trois switches dédiés aux postes informatiques et trois switches dédiés à la téléphonie, soit un total de six équipements. Cette architecture permet également de conserver des ports disponibles pour d'éventuels besoins futurs, comme le raccordement d'imprimantes réseau ou d'équipements IoT. Sur le site de Paris, cette conception laisse une réserve d'environ 24 ports disponibles, garantissant ainsi une certaine évolutivité de l'infrastructure.



En ce qui concerne les switches dédiés au réseau WiFi, nous resterons également sur la gamme UniFi du constructeur Ubiquiti Inc.. Toutefois, en raison des exigences techniques liées aux bornes retenues, nous devons monter en gamme par rapport aux switches utilisés pour les postes utilisateurs. Les points d'accès choisis sont compatibles WiFi 7 et offrent des débits élevés, ce qui nécessite une liaison montante en 2,5 Gb/s afin d'éviter tout goulot d'étranglement au niveau du réseau filaire.

Comme pour la téléphonie IP, l'alimentation des bornes sera assurée via la technologie PoE, ce qui permet de simplifier le câblage et d'éviter l'ajout d'alimentations externes. Le modèle retenu est le USW-Pro-HD-24-PoE, un switch 24 ports dont 22 ports 2,5 Gb/s compatibles PoE++ ainsi que 2 ports Ethernet 10 Gb/s également en PoE++. L'équipement dispose en complément de 4 ports SFP+ en 10 Gb/s destinés aux uplinks vers la couche de distribution, garantissant ainsi une capacité suffisante pour absorber le trafic généré par les bornes WiFi 7 et assurer une évolutivité à long terme de l'infrastructure.

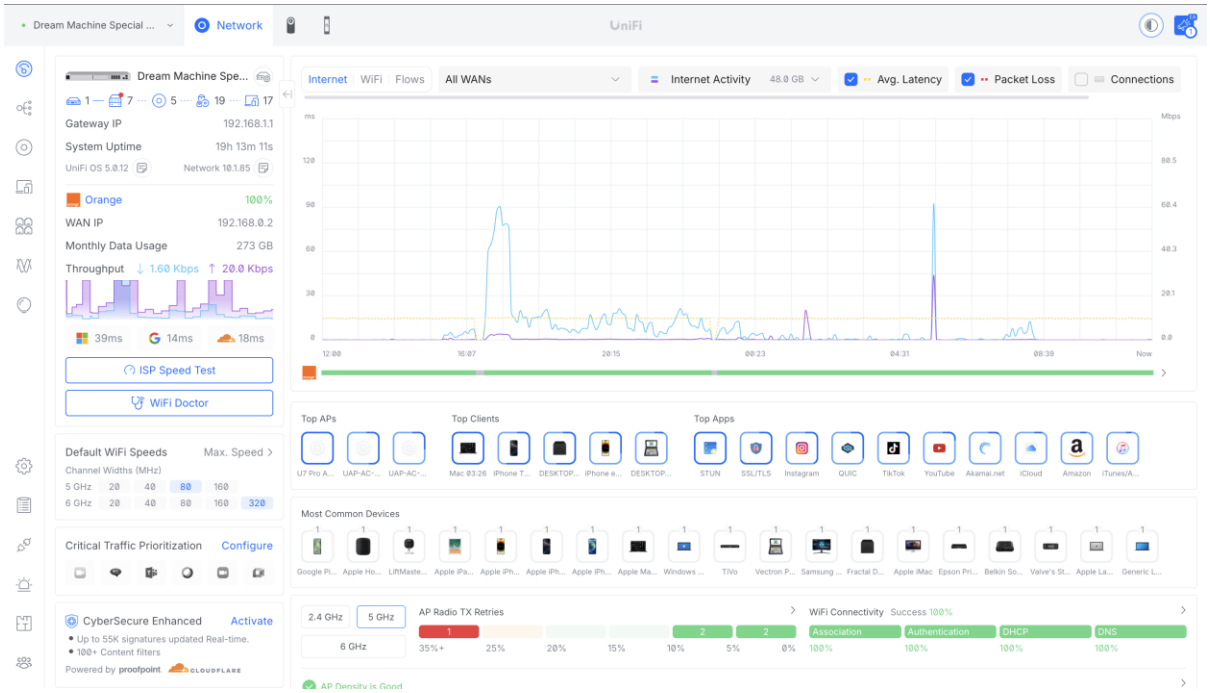


Management

En ce qui concerne la gestion de l'ensemble des équipements réseau, nous mettrons en place un contrôleur centralisé. Ce contrôleur est l'élément clé de l'infrastructure UniFi : il assure la communication avec tous les équipements, centralise les journaux (logs), collecte les statistiques et applique les configurations vers les switches et les bornes WiFi. Les équipements ne sont donc pas configurés individuellement, mais administrés de manière globale et cohérente depuis une plateforme unique.

Grâce à ce contrôleur, nous disposons d'un tableau de bord centralisé permettant de superviser l'état du réseau en temps réel, de visualiser les performances, de détecter d'éventuelles anomalies et d'intervenir rapidement en cas de problème. L'accès à cette interface peut se faire en local, mais également à distance de manière sécurisée, ce qui facilite considérablement l'administration multi-sites et la maintenance.

Ce contrôleur peut être déployé sous différentes formes. La solution la plus simple consiste à utiliser un équipement dédié, comme la Cloud Key Gen2, qui est un petit appareil autonome se connectant directement au réseau. Il est également possible de virtualiser le contrôleur, par exemple au sein de votre infrastructure serveur existante sous Proxmox. Cette seconde solution permet d'intégrer le management réseau dans votre environnement de virtualisation, d'optimiser les ressources et de faciliter les sauvegardes ainsi que la haute disponibilité.



Wifi

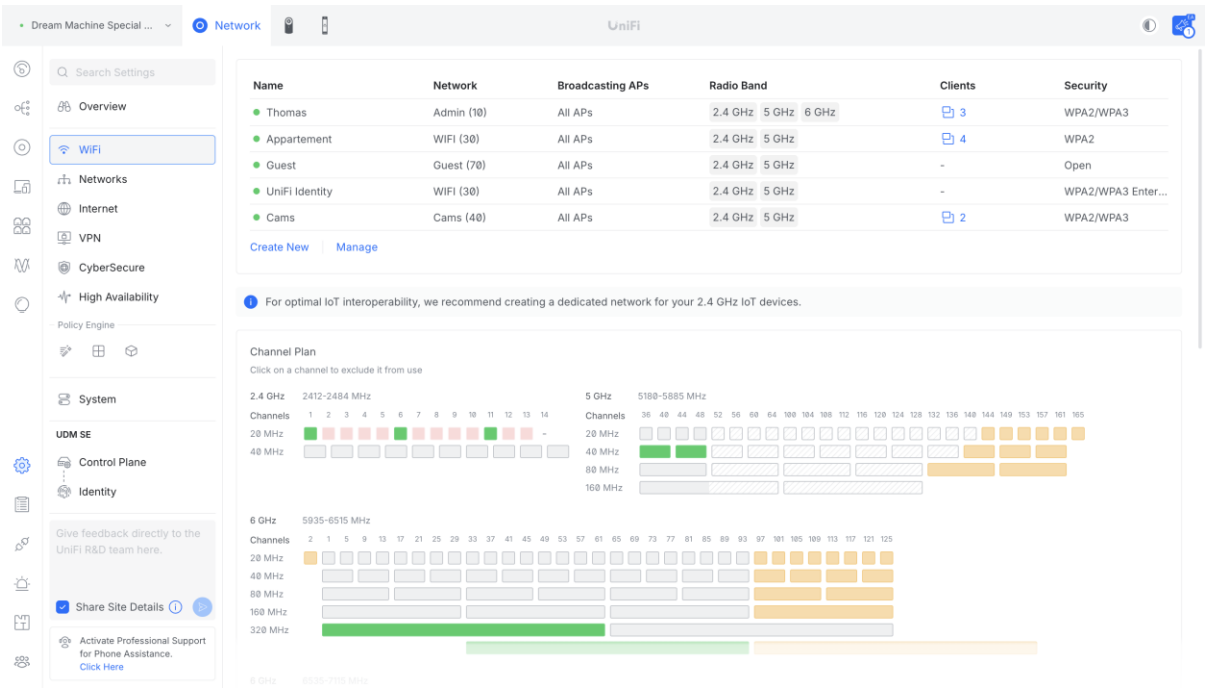
Le réseau WiFi occupe aujourd'hui une place essentielle au sein d'une entreprise. Il permet la mobilité des collaborateurs grâce aux ordinateurs portables, smartphones et tablettes, mais il est également utilisé par certains équipements professionnels tels que les terminaux mobiles, les scanners ou encore les équipements IoT. Un réseau sans fil performant et stable est donc indispensable pour garantir la productivité, la flexibilité des usages et le confort de travail des utilisateurs.

Pour le WiFi qui sera déployé sur l'ensemble de vos sites, nous avons choisi de rester sur des équipements de la marque Ubiquiti Inc., au sein de la gamme UniFi. Ce constructeur fait partie des acteurs majeurs du marché du WiFi professionnel et figure parmi les premiers à avoir proposé des solutions compatibles WiFi 7, ce qui garantit une infrastructure moderne et pérenne.

Le choix des bornes a été réalisé à partir des informations que vous nous avez fournies concernant le nombre d'utilisateurs simultanés et la superficie de vos locaux. Le modèle retenu est la U7-Pro, une borne WiFi 7 tri-bande intégrant notamment la nouvelle bande 6 GHz. Cette technologie permet d'augmenter significativement les débits disponibles et de réduire la congestion radio. Chaque borne est capable de gérer plus de 300 clients connectés simultanément, ce qui est largement supérieur à vos besoins actuels et garantit une marge d'évolution confortable. Elle dispose également d'une interface Ethernet 2,5 Gb/s, indispensable pour exploiter pleinement les performances offertes par le WiFi 7 sans créer de limitation au niveau du réseau filaire.

En ce qui concerne la sécurité du Wi-Fi, les SSID principaux seront tous protégés par la norme WPA3, la dernière génération de sécurité Wi-Fi, offrant une protection bien supérieure à l'ancienne norme WPA2. Cependant, certains équipements, comme les objets IoT ou certaines imprimantes, ne sont pas compatibles avec WPA3. Pour ces cas, un SSID dédié sera mis en place, fonctionnant en WPA2 mais soumis à des règles d'accès beaucoup plus strictes, afin de limiter les risques tout en permettant la connectivité de ces appareils.

La gestion et la supervision des bornes seront assurées via la solution UniFi Network, utilisée également pour l'administration des switches. L'ensemble des équipements sera ainsi centralisé au sein d'une interface unique, accessible via une page web, ce qui simplifie la configuration, le déploiement et le suivi de l'infrastructure réseau sur tous vos sites.



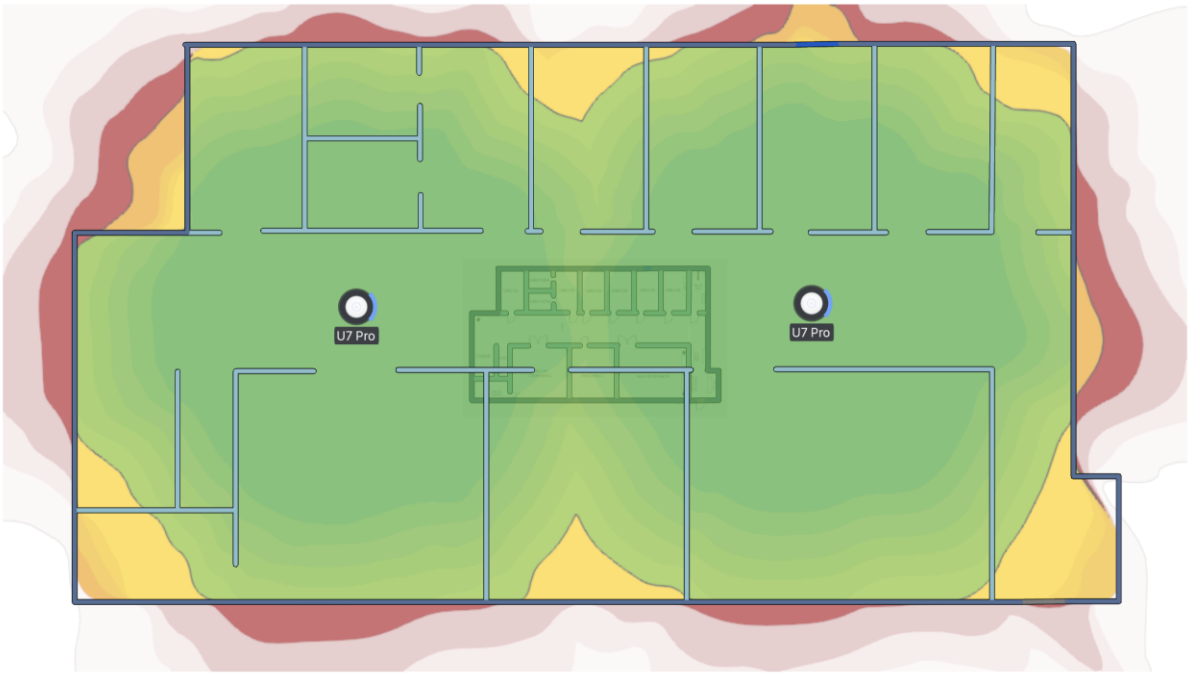
Pour le site de Lyon, nous avons pu accéder aux plans des bâtiments, ce qui nous a permis de réaliser une simulation de couverture Wi-Fi et de mener un audit afin de déterminer le meilleur emplacement pour les nouvelles bornes ainsi que la répartition optimale du signal à travers l'ensemble des bâtiments.

Vous trouverez ci-dessous les plans de couverture Wi-Fi réalisés dans le cadre de cette étude.

BAT R&D L3 - copy

Estimated 5GHz WiFi Coverage

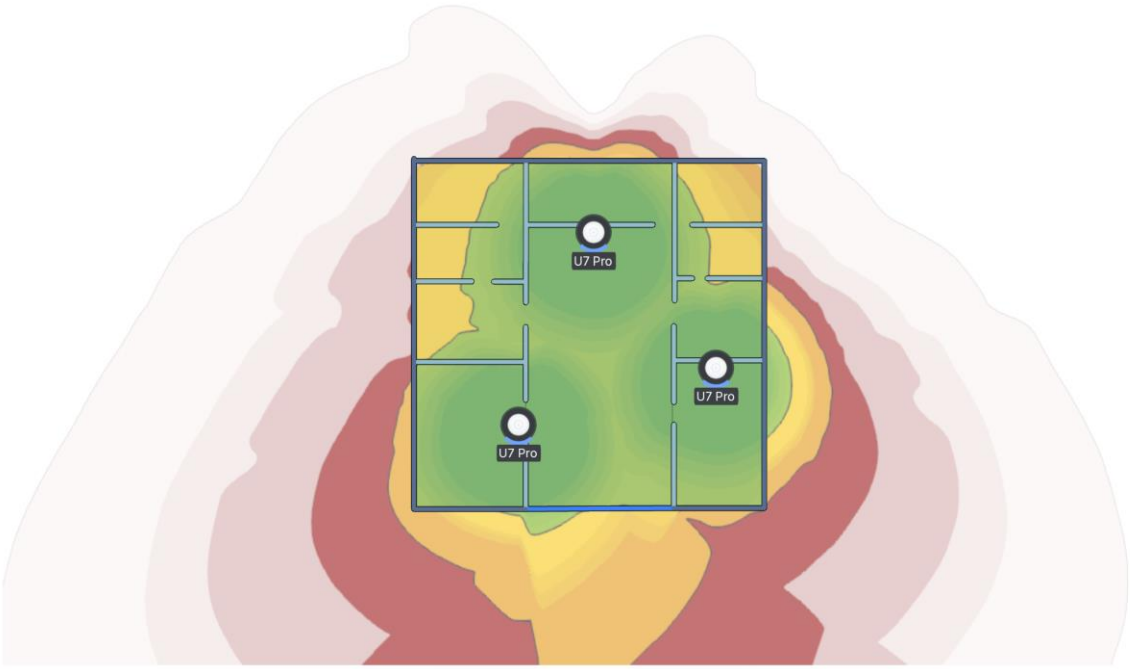
UniFi Design Center

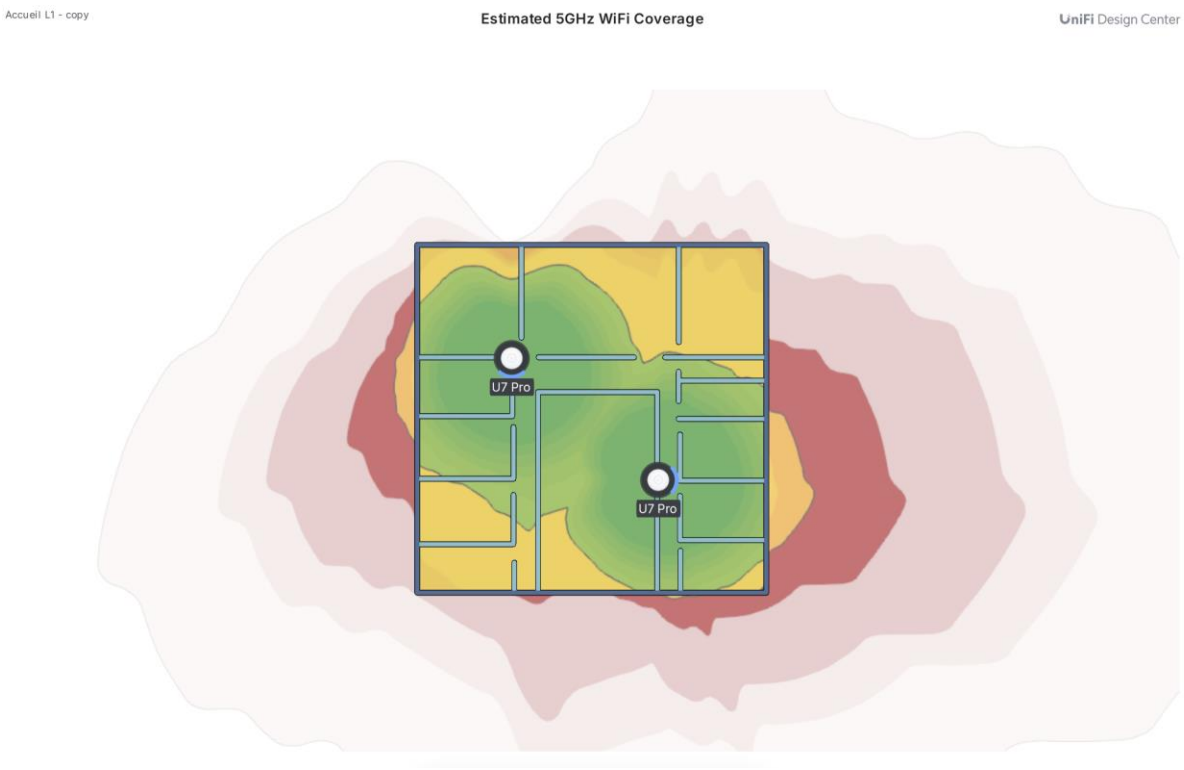


Accueil RDC - copy

Estimated 5GHz WiFi Coverage

UniFi Design Center





Sécurité LAN

Au-delà de la segmentation physique et logique que nous avons vu précédemment, la sécurité de notre infrastructure repose sur une configuration stricte des équipements réseau (switchs, firewall). Nous avons implémenté les standards de sécurité les plus élevés pour protéger à la fois le trafic utilisateur et le plan d'administration.

Sécurisation de l'Administration et de la Supervision

Il est impératif que les flux de gestion des équipements actifs soient indéchiffrables et parfaitement tracés :

- SSH v2 (Secure Shell version 2) au lieu de Telnet : Telnet transmet les données (y compris les mots de passe) en clair. Nous imposons SSHv2 qui chiffre de bout en bout la communication, empêchant toute interception d'identifiants par écoute du réseau (sniffing).
- HTTPS (Hypertext Transfert Protocol Secure) au lieu de HTTP : Pour les interfaces de gestion web (comme Proxmox ou Unifi), le HTTPS garantit l'authentification du serveur via des certificats et le chiffrement des sessions.
- SNMP v3 (Simple Network Management Protocol version 3) : SNMP est utilisé pour remonter l'état de santé de nos équipements, et est utilisé par l'interface de gestion Unifi. Contrairement aux versions précédentes, SNMPv3 apporte

l'authentification forte et le chiffrement des données, empêchant un attaquant de cartographier le réseau ou de modifier des configurations à distance.

- Syslog : Tous les événements et alertes des équipements seront centralisés vers un serveur Syslog. C'est indispensable pour notre démarche SOC (via l'implémentation d'un SIEM) afin d'avoir une traçabilité complète et d'auditer les incidents a posteriori.
- NTP (Network Time Protocol) : Sans horloges parfaitement synchronisées, l'analyse des logs (Syslog) est impossible et les certificats de sécurité peuvent être invalidés. Le NTP garantit une cohérence temporelle absolue sur tout le parc.

Protection de la Couche d'accès

La protection de la couche d'accès est encore de nos jours trop peu mis en avant, car l'idée d'une attaque informatique fait davantage réfléchir à comment se protéger des menaces extérieures plutôt que celles provenant de l'intérieur, alors que celles-ci sont bien réel. En fait, elles peuvent réduire à néant tous les efforts appliqués à la sécurisation des attaques extérieures. Nous avons donc choisi d'implémenter différents mécanismes qui pourront protéger le LAN contre les différentes attaques de la couche d'accès, pouvant être dues autant à des erreurs humaines qu'à des actes malveillants.

- RSTP (Rapid Spanning Tree Protocol) : Il empêche la formation de boucles réseau (qui feraient s'effondrer l'infrastructure) tout en offrant un temps de convergence très rapide (quelques millisecondes) en cas de coupure d'un lien.
- BPDU Guard : Couplé au RSTP, il désactive immédiatement un port utilisateur si un switch non autorisé y est branché. Cela empêche un individu de brancher son propre matériel et de détourner le trafic du réseau (attaque du Root Bridge).
- Port Security : Nous limitons le nombre d'adresses MAC autorisées par port physique. Cela bloque les attaques par inondation de la table MAC (MAC flooding) et empêche un utilisateur de brancher un hub non autorisé pour y connecter de multiples appareils personnels.
- DHCP Snooping : Cette fonction vitale empêche un attaquant de brancher un "faux" serveur DHCP sur le réseau. Le switch filtre et bloque les offres DHCP illégitimes, protégeant ainsi les utilisateurs contre les attaques de type "Man-in-the-Middle" (redirection de trafic).

Haute Disponibilité et Optimisation

- LACP (Link Aggregation Control Protocol) : Permet d'agréger plusieurs câbles physiques en un seul lien logique. Cela multiplie la bande passante (ex: 2x 10G = 20G) et assure la continuité de service si l'un des câbles est sectionné.
- VRRP (Virtual Router Redundancy Protocol) : Déployé sur le cœur de réseau (firewall), il crée une "passerelle virtuelle". Si notre firewall principal tombe en panne, le firewall secondaire prend le relais instantanément, sans aucune coupure ressentie par les utilisateurs.
- QoS (Quality of Service) : La QoS permet de prioriser les paquets réseau. Dans notre cas, elle garantit que les flux sensibles à la latence (comme la Téléphonie VoIP) ne soient jamais ralentis par des téléchargements massifs sur le réseau bureautique

Objets réseau

Dans un firewall comme ceux de Stormshield, un objet réseau est une représentation logique d'une adresse IP, d'un sous-réseau ou d'un groupe d'adresses. Au lieu d'écrire des IP directement dans les règles, on crée des objets qu'on réutilise dans la politique de sécurité. Voici ci-dessous les liaisons entre les noms et les réseaux.

WIFI_ALL (Groupe)	IOT_ALL (Groupe)	ADMIN_RESEAU_ALL (Groupe)	CAMERAS_ALL (Groupe)	IMPRIMANTES_ALL (Groupe)	BUREAUTIQUE_ALL (Groupe)	TELEPHONIE_ALL (Groupe)
192.168.10.0/24	192.168.11.0/24	192.168.12.0/24	192.168.13.0/24	192.168.14.0/24	192.168.15.0/24	192.168.19.0/24
192.168.20.0/24	192.168.21.0/24	192.168.22.0/24	192.168.23.0/24	192.168.24.0/24	192.168.25.0/24	192.168.29.0/24
192.168.30.0/24	192.168.31.0/24	192.168.32.0/24	192.168.33.0/24	192.168.34.0/24	192.168.35.0/24	192.168.39.0/24
192.168.40.0/24	192.168.41.0/24	192.168.42.0/24	192.168.43.0/24	192.168.44.0/24	192.168.45.0/24	192.168.49.0/24
192.168.50.0/24	192.168.51.0/24	192.168.52.0/24	192.168.53.0/24	192.168.54.0/24	192.168.55.0/24	192.168.59.0/24
192.168.60.0/24	192.168.61.0/24	192.168.62.0/24	192.168.63.0/24	192.168.64.0/24	192.168.65.0/24	192.168.69.0/24
192.168.70.0/24	192.168.71.0/24	192.168.72.0/24	192.168.73.0/24	192.168.74.0/24	192.168.75.0/24	192.168.79.0/24
192.168.80.0/24	192.168.81.0/24	192.168.82.0/24	192.168.83.0/24	192.168.84.0/2	192.168.85.0/24	192.168.89.0/24

Stratégie de Filtrage Cœur de Réseau

Nos firewalls Stormshield, placés en cœur de réseau, se verront appliquer une politique de filtrage qui repose sur le principe du "Zero Trust" (Confiance Zéro) et de l'interdiction par défaut. Sur cette base, voici les différentes règles qui seront implémentées :

Exemple du site de Paris :

#	Source	Destination	Service	Action	NAT	Commentaire
1	WIFI_ALL	Internet	HTTP, HTTPS, DNS, NTP	Allow	Oui	Accès Internet WiFi
2	WIFI_ALL	192.168.16.10	ALL	Allow	Non	WiFi → Contrôleur WiFi
3	IOT_ALL	192.168.16.11	ALL	Allow	Non	IoT → Contrôleur IoT
4	CAMERAS_ALL	192.168.16.12	ALL	Allow	Non	Caméras → Contrôleur
5	IMPRIMANTES_ALL	BUREAUTIQUE_ALL	TCP 9100, 515, 631	Allow	Non	Impression
6	ADMIN_RESEAU_ALL	BUREAUTIQUE_ALL	ALL	Allow	Non	Admin → Bureautique
7	BUREAUTIQUE_ALL	192.168.16.13	SMTP, HTTPS, MAPI, IMAPS	Allow	Non	Postes → Exchange
8	192.168.16.13	BUREAUTIQUE_ALL	SMTP, HTTPS, MAPI	Allow	Non	Exchange → Postes
9	BUREAUTIQUE_ALL	Internet	HTTP, HTTPS, DNS, NTP	Allow	Oui	Internet Bureautique
10	192.168.16.13	Internet	SMTP, HTTPS	Allow	Oui	Exchange → Internet
11	TELEPHONIE_ALL	192.168.16.14	SIP, RTP	Allow	Non	Téléphonie → Contrôleur
12	TELEPHONIE_ALL	BUREAUTIQUE_ALL	SIP, HTTP, HTTPS	Allow	Non	Téléphonie → Postes
13	TELEPHONIE_ALL	Internet	SIP, RTP	Allow	Oui	Téléphonie → Internet
14	ANY	ANY	ANY	Deny	-	Règle implicite

Isolation Inter-VLAN (Routage Interne) :

- Les VLANs n'ont pas le droit de communiquer entre eux par défaut (Zero Trust).
- Le VLAN "Bureautique" a accès à Internet et aux autres VLAN internes, mais n'a aucun accès au VLAN "Administration Réseau". Seuls les postes identifiés de l'équipe IT y auront accès.
- Les VLAN "IoT" et "Caméras" sont totalement isolés. Ils ne peuvent ni aller sur Internet, ni joindre la bureautique. Seul le serveur de supervision peut les interroger.

- Filtrage des accès Internet (Outbound) :
  - Le trafic sortant vers Internet n'est pas libre. Nous n'autorisons que les protocoles web standards (HTTP/HTTPS) en les passant dans un filtre d'inspection (Proxy).
  - Les requêtes DNS sortantes sont bloquées, sauf pour nos serveurs contrôleurs de domaine (AD) qui sont les seuls autorisés à résoudre des noms sur Internet.
- Protection de l'Hébergement (Inbound - DMZ) :
  - Les flux venant d'Internet vers notre réseau sont bloqués.
  - Seuls les flux ciblant des services spécifiques hébergés dans notre DMZ sont autorisés (ex: port 443 pour un serveur web), avec une inspection IDS (Intrusion Detection System) activée pour surveiller le trafic en temps réel.

Serveurs

Vous disposez actuellement de 284 machines virtuelles réparties sur votre infrastructure. Cette base installée connaît une croissance constante de 5% par an, ce qui représente un défi important en termes de planification et de dimensionnement. Pour bien comprendre l'ampleur de cette croissance, il est essentiel de projeter les besoins sur plusieurs années.

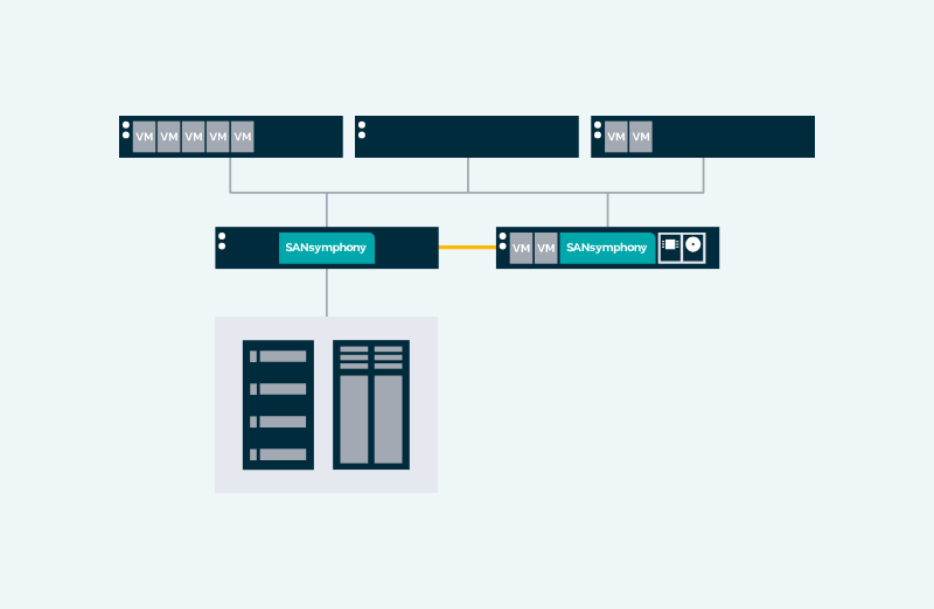
La première année, nous partons des 284 VMs actuelles. L'année suivante, avec une croissance de 5%, nous atteignons 298 VMs et cela pour finalement arriver à 362 VMs au bout de cinq ans. Cette projection montre une augmentation de presque 30% sur cinq ans, ce qui justifie amplement le dimensionnement de l'infrastructure.

Cette croissance soutenue nécessite une infrastructure non seulement capable de supporter la charge actuelle, mais également suffisamment évolutive pour absorber cette expansion sans nécessiter de refonte majeure à court ou moyen terme. C'est précisément pour répondre à ces enjeux que nous avons conçu cette architecture avec des marges de manœuvre confortables tout en optimisant les coûts sur le long terme.

Architecture Globale la redondance géographique

L'architecture que nous proposons repose sur un principe fondamental : la redondance géographique. Nous avons choisi de déployer deux serveurs strictement identiques sur deux sites distincts, le site principal étant situé à Paris et le site secondaire à Lyon. Ce choix n'est pas anodin et répond à plusieurs impératifs critiques pour la continuité d'activité du client.

La haute disponibilité est au cœur de cette décision. En cas de défaillance matérielle sur l'un des sites, qu'il s'agisse d'une panne de serveur, d'un problème de climatisation ou même d'une coupure électrique prolongée, le second site est immédiatement capable de prendre le relais. Cette bascule s'effectue de manière automatique grâce aux mécanismes de haute disponibilité intégrés dans DataCore, garantissant ainsi une continuité de service pour les utilisateurs finaux sans intervention humaine.



La distance géographique entre Paris et Lyon, qui s'élève à environ 460 kilomètres, offre une protection optimale contre les incidents localisés. Un incendie dans un datacenter, une inondation régionale, ou même une coupure de courant à l'échelle d'une ville n'affecteront qu'un seul site, laissant l'autre parfaitement opérationnel. Cette séparation géographique reste néanmoins dans un cadre national français, ce qui simplifie considérablement les questions de conformité RGPD et de souveraineté des données, des aspects de plus en plus scrutés par les autorités et les clients eux-mêmes.

La réplication asynchrone entre les deux sites constitue le lien vital de cette architecture. Chaque écriture effectuée sur le site principal est automatiquement répliquée vers le site secondaire avec un décalage minimal, généralement inférieur à cinq minutes. Cette approche garantit qu'une copie à jour des données existe toujours sur le site distant, permettant une reprise d'activité rapide et avec une perte de données minimale en cas de sinistre majeur. La réplication asynchrone a été préférée à la réplication synchrone car elle offre un meilleur compromis entre protection des données et performances, la distance de 460 kilomètres rendant la synchronisation temps réel techniquement complexe et potentiellement pénalisante pour les performances.

Les Serveurs DELL PowerEdge R660xs

Le choix du serveur Dell PowerEdge R660xs s'est imposé pour plusieurs raisons techniques majeures. Ce modèle représente actuellement l'un des meilleurs compromis du marché entre densité de calcul, capacité de stockage interne et évolutivité.

Les processeurs constituent le cerveau de cette infrastructure. Nous avons opté pour deux processeurs

- Intel Xeon offrant chacun 16 cœurs et 32 threads, soit un total de 32 cœurs physiques et 64 threads logiques par serveur.

Cette puissance de calcul n'est pas excessive au regard des besoins. Avec les 497 VMs projetées en cinquième année, chaque serveur devra potentiellement gérer environ 250 machines virtuelles en cas de défaillance de l'autre site. Cela représente un ratio d'environ 4 VMs par thread, ce qui est parfaitement gérable pour des charges de travail mixtes classiques comprenant des serveurs d'applications, des bases de données de taille moyenne et des serveurs de fichiers. Cette architecture permet également de réserver des ressources CPU dédiées à l'hyperviseur et aux services système sans compromettre les performances des VMs de production.

La mémoire vive représente souvent le facteur limitant dans les environnements virtualisés modernes. Nous avons dimensionné chaque serveur avec

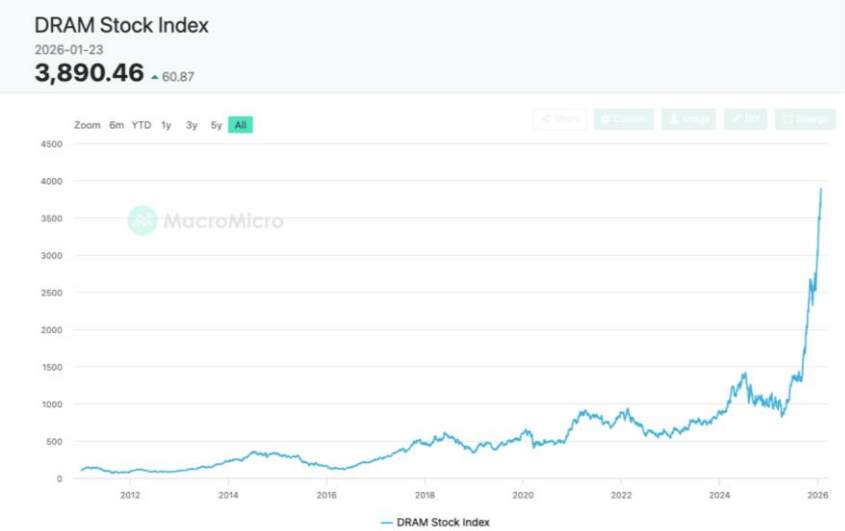
- 768 Go de RAM DDR5-4400

Ce qui peut sembler généreux mais s'avère nécessaire. En divisant cette capacité par les 250 VMs potentielles, nous obtenons environ 3 Go de RAM par VM en moyenne. Cette allocation permet de supporter confortablement des **VMs Windows Server** standard qui requièrent typiquement 2 à 4 Go de RAM, ainsi que des **serveurs Linux** plus légers.

Le choix de la **DDR5-4400** plutôt que de la DDR4 apporte un gain de performance substantiel, avec une bande passante mémoire supérieure d'environ 35%. Dans un

environnement virtualisé où des dizaines de VMs accèdent simultanément à la mémoire, cette augmentation de bande passante se traduit directement par de meilleures performances globales et une réduction des temps d'attente. Il est important de noter que sur ces 768 Go, environ 100 à 150 Go seront réservés pour l'hyperviseur lui-même et pour les services système, laissant effectivement 600 à 650 Go disponibles pour les VMs de production.

Toutefois, le contexte actuel de forte hausse des prix de la RAM et du stockage, lié aux tensions d'approvisionnement du marché, a significativement impacté les coûts. Heureusement, grâce à nos partenariats fournisseurs, nous sommes en mesure de limiter le surcoût lié à cette pénurie et d'optimiser l'investissement global.



Le contrôleur RAID PERC H755 avec 8 Go de cache joue un rôle absolument crucial dans les performances de stockage. Ce contrôleur matériel dédié prend en charge toute la gestion du RAID, libérant ainsi les processeurs principaux de cette tâche gourmande en ressources.

Le cache de 8 Go est particulièrement important pour les opérations d'écriture. Dans un environnement virtualisé, les écritures sont souvent de petite taille et aléatoires, un pattern d'accès particulièrement pénalisant pour les disques durs traditionnels.

Le cache du contrôleur permet de regrouper ces écritures et de les optimiser, multipliant les performances par un facteur pouvant aller jusqu'à 10 dans certains scénarios. Le support du RAID 6 est indispensable pour notre architecture car il offre une double parité, permettant au système de survivre à la défaillance simultanée de deux disques sans perte de données, une protection essentielle pour des données critiques d'entreprise.

Stockage

Architecture de Stockage

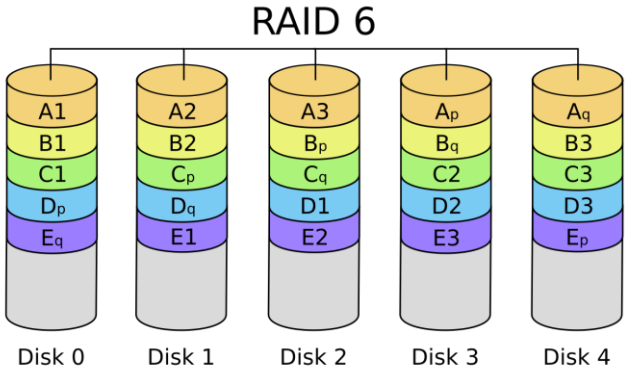
Le stockage représente l'épine dorsale de toute infrastructure virtualisée moderne. Notre approche repose sur une architecture hybride combinant différentes technologies de stockage, chacune optimisée pour un usage spécifique. Cette stratégie permet d'obtenir le meilleur rapport performance-coût tout en garantissant que chaque type de donnée bénéficie du support de stockage le plus adapté à ses besoins.

Chaque serveur embarque :

- Cinq disques SSD NVMe au format M.2,
- Une capacité unitaire de 7,68 To.

Ces cinq disques sont configurés en RAID 6, offrant une capacité brute de 38,4 To. Après déduction de l'espace requis pour la double parité du RAID 6, la capacité utilisable s'établit à environ 30,7 To par serveur, soit un total de 61 To de stockage haute performance sur les deux sites. Le choix de la technologie NVMe n'est pas un luxe mais une nécessité absolue pour les environnements virtualisés modernes.

Un SSD NVMe est capable de délivrer beaucoup plus d'opération quun disque dur traditionnel. Cette différence se traduit par une réactivité incomparable pour les machines virtuelles hébergées. Dans la pratique quotidienne, cela signifie des démarrages de VMs quasi instantanés, des bases de données répondant en temps réel, et une expérience utilisateur fluide même lors de charges importantes.



Le format M.2 présente un avantage architectural significatif. Ces disques se connectent directement sur la carte mère du serveur via des slots dédiés, libérant ainsi l'intégralité des baies de disques frontales pour d'autres usages. Cette particularité nous permet d'ajouter du stockage de capacité sous forme de disques durs traditionnels sans sacrifier le stockage haute performance.

Pour atteindre l'objectif de 300 To de stockage total, nous complétons les SSD NVMe par des disques durs traditionnels installés dans les baies frontales du serveur.

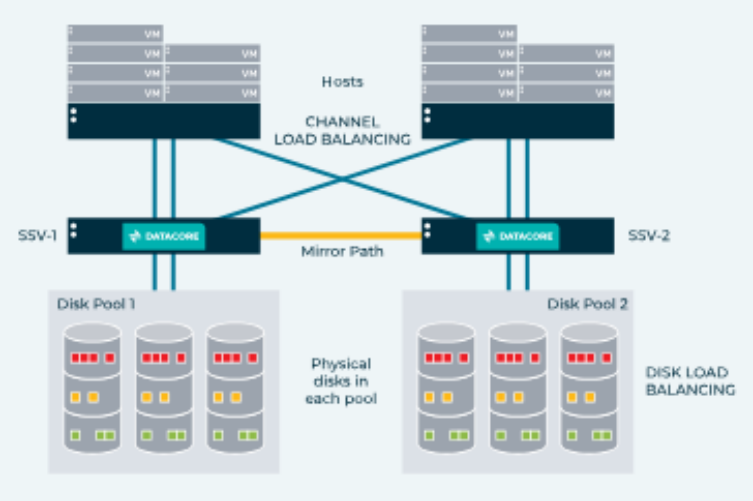
Le Dell PowerEdge R660xs peut accueillir jusqu'à 8 disques de format 2,5 pouces ou 4 disques de format 3,5 pouces. Nous recommandons l'installation de 8 disques durs SAS de 10 To tournant à 7200 tours par minute, également configurés en RAID 6 pour la protection des données. Cette configuration offre une capacité brute de 80 To par serveur et une capacité utilisable d'environ 60 To après parité, soit 120 To au total sur les deux sites. En combinant les 61 To de stockage NVMe et les 120 To de stockage HDD, nous obtenons environ 181 To de stockage utilisable. Cette capacité physique, associée aux mécanismes de déduplication et de compression de DataCore, permet de stocker logiquement les

- 300 To de données requis

Les disques durs conservent une place importante dans cette architecture pour plusieurs raisons économiques et techniques. Bien que nettement moins performants que les SSD, ils offrent un coût au téraoctet environ 5 fois inférieur. Pour des données d'archives, des anciens rapports ou des documents peu consultés, investir dans du stockage NVMe serait un gaspillage financier. Les disques durs modernes à 7200 tours par minute offrent des performances largement suffisantes pour ce type d'usage, avec des débits séquentiels pouvant atteindre 200 Mo par seconde. De plus, leur durabilité en termes d'endurance est excellente pour des données majoritairement stockées et rarement réécrites.

DataCore SANsymphony

DataCore SANsymphony s'agit d'une solution de stockage logiciel, communément appelée Software-Defined Storage, qui virtualise l'ensemble des ressources de stockage physique pour créer une infrastructure unifiée, flexible et intelligente. Contrairement aux solutions SAN traditionnelles reposant sur des baies matérielles propriétaires et coûteuses, DataCore transforme nos serveurs Dell en une véritable infrastructure SAN d'entreprise, avec toutes les fonctionnalités avancées qu'on attendrait d'une solution haut de gamme, mais avec une flexibilité et un rapport qualité-prix bien supérieurs.



La fonctionnalité d'auto-tiering automatique constitue probablement l'avantage le plus significatif de DataCore dans notre architecture. DataCore identifie quelles données sont consultées fréquemment, lesquelles le sont occasionnellement, et lesquelles ne sont pratiquement jamais accédées. En fonction de cette analyse, le système déplace automatiquement les données entre les différents tiers de stockage disponibles. Les données chaudes, c'est-à-dire celles qui sont consultées plusieurs fois par heure ou par jour, sont automatiquement promues vers les SSD NVMe. Les données tièdes, accédées quelques fois par semaine, peuvent résider sur un tier intermédiaire. Enfin, les données froides, qui n'ont pas été consultées depuis plusieurs semaines ou mois, sont automatiquement reléguées vers les disques durs de capacité.

Les bénéfices économiques de cette approche sont considérables. Sans auto-tiering, il faudrait dimensionner l'intégralité du stockage en SSD NVMe pour garantir des performances optimales, ce qui multiplierait les coûts par un facteur cinq ou plus. Avec l'auto-tiering, seuls 20 à 30% des données actives monopolisent le stockage coûteux, le reste étant stocké de manière économique sur disques durs.

La haute disponibilité et la réplication asynchrone entre les sites de Paris et Lyon constituent un autre pilier fondamental de DataCore. Chaque fois qu'une donnée est écrite sur le site principal, elle est simultanément écrite sur le stockage local et placée dans une file d'attente de réplication. Le délai de réplication dépend de la quantité de données modifiées et de la bande passante disponible, mais il est généralement maintenu en dessous de cinq minutes. Cela signifie que le RPO, ou Recovery Point Objective, c'est-à-dire la quantité maximale de données que nous pourrions perdre en cas de sinistre majeur sur le site principal, est limité à ces cinq dernières minutes. C'est un niveau de protection extrêmement élevé qui garantit une perte de données minimale même dans les scénarios les plus catastrophiques.

Le mécanisme de basculement automatique, ou failover, complète ce dispositif de haute disponibilité. Si le site de Paris devient subitement indisponible, que ce soit en raison d'une panne matérielle, d'un incendie ou de tout autre incident, DataCore détecte automatiquement l'interruption et bascule l'ensemble des opérations vers le site de Lyon. Cette bascule s'effectue en quelques minutes seulement, et les machines virtuelles redémarrent sur le site secondaire en accédant à la copie répliquée des données. Pour les utilisateurs finaux, l'interruption de service se limite à ces quelques minutes de basculement, après quoi ils peuvent reprendre leur travail normalement. La synchronisation peut même être configurée en mode actif-actif pour certains scénarios, où les deux sites hébergent simultanément des VMs et se protègent mutuellement.

Les fonctionnalités de déduplication et de compression de DataCore permettent d'optimiser encore davantage l'utilisation du stockage physique. La déduplication identifie les blocs de données identiques présents à plusieurs endroits sur le système de stockage et les stocke une seule fois, les autres occurrences étant remplacées par de simples pointeurs. Dans un environnement virtualisé, cette technique est particulièrement efficace.

Les gains de compression varient énormément selon le type de données. Des fichiers texte, des documents Office ou des bases de données peuvent être compressés de 40 à 60%. En moyenne, sur un environnement mixte, on peut espérer un gain de compression

de 20 à 40%. En combinant déduplication et compression, il est réaliste d'atteindre un ratio global de 1,8 à 2,0, signifiant que 300 To de données logiques peuvent être stockés dans seulement 150 à 170 To de stockage physique.

DataCore offre également une interface de gestion centralisée qui simplifie considérablement l'administration au quotidien. Depuis une console unique, les administrateurs peuvent surveiller l'état de santé des deux sites, visualiser les performances en temps réel, configurer les politiques de réplication et de tiering, et recevoir des alertes proactives en cas d'anomalie. Cette centralisation est particulièrement précieuse dans une architecture multi-sites où elle évite de devoir se connecter séparément à chaque serveur pour des tâches de routine. Les rapports détaillés générés par le système permettent d'analyser les tendances d'utilisation, d'identifier les goulots d'étranglement potentiels et de planifier les évolutions futures de l'infrastructure.

Le coût de la licence DataCore SDS SE Edition pour le tier 100-250 TB s'élève à environ 65 000 euros par serveur et par an, soit 130 000 euros annuels pour les deux sites. Ce montant peut sembler élevé au premier abord, mais il doit être mis en perspective avec les alternatives. L'acquisition d'une baie SAN matérielle équivalente d'un constructeur comme Dell EMC Unity ou NetApp représenterait un investissement initial de 150 000 à 200 000 euros, auquel s'ajouteraient des coûts annuels de maintenance de 15 à 20% de la valeur d'achat. Sur un cycle de cinq ans, le coût total de possession d'une solution SAN matérielle serait donc comparable, voire supérieur, tout en offrant moins de flexibilité. De plus, DataCore fonctionne avec n'importe quel matériel serveur standard, nous libérant de la dépendance à un constructeur spécifique et nous permettant de choisir le meilleur rapport qualité-prix à chaque renouvellement. La licence inclut également le support premium avec assistance 24h/24 et 7j/7, les mises à jour logicielles et les correctifs de sécurité, autant d'éléments qui seraient facturés séparément avec d'autres solutions.

Sauvegarde

Sauvegarde sur Bandes Magnétiques

Dans le contexte actuel de multiplication des attaques par ransomware, la stratégie de sauvegarde revêt une importance absolument critique. Les cybercriminels ont considérablement perfectionné leurs techniques et ciblent désormais systématiquement les systèmes de sauvegarde pour maximiser la pression sur leurs victimes. Une fois qu'ils ont chiffré les données de production et détruit ou chiffré les

sauvegardes, les organisations n'ont plus d'autre choix que de payer la rançon ou perdre définitivement leurs données. C'est précisément pour contrer cette menace que nous avons intégré un système de sauvegarde sur bandes magnétiques avec immuabilité.

Le lecteur HPE StoreEver LTO-8 Ultrium représente la dernière génération de technologie de bandes magnétiques. Chaque cartouche LTO-8 offre une capacité native de 12 téraoctets, pouvant atteindre 30 téraoctets avec compression activée. Nous avons prévu un jeu initial de 20 cartouches, ce qui représente une capacité native totale de 240 téraoctets ou 600 téraoctets compressés, largement suffisant pour sauvegarder l'intégralité de l'infrastructure plusieurs fois. L'interface SAS 12 Gigabits par seconde garantit des vitesses de sauvegarde pouvant atteindre 360 mégaoctets par seconde en mode compressé, permettant de sauvegarder plusieurs téraoctets en une seule nuit.

Le concept d'immuabilité est au cœur de cette stratégie de protection. Les cartouches LTO-8 supportent nativement le mode WORM, acronyme de Write Once Read Many, qui signifie "écrire une fois, lire plusieurs fois". Lorsqu'une cartouche est initialisée en mode WORM, toute donnée qui y est écrite devient définitivement non modifiable et non supprimable. Ce n'est pas une simple protection logicielle que des logiciels malveillants pourraient contourner, mais bien une limitation physique de la cartouche elle-même. Une fois les données écrites, même un administrateur disposant de tous les privilèges ne peut les altérer ou les détruire. Cette caractéristique rend les bandes magnétiques complètement imperméables aux ransomwares, qui peuvent chiffrer ou détruire des fichiers sur disque mais sont totalement impuissants face à des bandes en mode WORM.

La période d'immuabilité de trois mois que nous avons configurée répond à un équilibre judicieux entre protection et coût. Voici comment fonctionne concrètement notre schéma de sauvegarde. Chaque dimanche, une sauvegarde complète de l'ensemble de l'infrastructure est effectuée sur une cartouche LTO-8 vierge. Cette sauvegarde complète capture l'état exact de toutes les machines virtuelles, de tous les fichiers et de toutes les configurations. Du lundi au samedi, des sauvegardes incrémentielles quotidiennes sont réalisées, ne capturant que les données qui ont changé depuis la dernière sauvegarde. Ces incrémentielles sont beaucoup plus rapides et consomment beaucoup moins d'espace que les sauvegardes complètes.

Le cycle de rotation des bandes s'organise ainsi. Les quatre dernières sauvegardes hebdomadaires complètes sont conservées en ligne, c'est-à-dire dans le lecteur de bandes ou dans une bibliothèque de bandes à proximité immédiate du serveur, permettant une restauration rapide en cas de besoin. Ces quatre semaines offrent une première couche de protection contre les erreurs humaines, les corruptions de données ou les pannes matérielles. Au-delà de ces quatre semaines, nous conservons des sauvegardes mensuelles pendant trois mois supplémentaires, soit douze bandes au total.

Ces bandes mensuelles sont extraites du lecteur et stockées dans un coffre-fort ignifuge, idéalement dans un bâtiment séparé du datacenter. Cette séparation physique crée ce qu'on appelle un "air gap", c'est-à-dire une isolation totale du réseau informatique, rendant impossible toute attaque à distance contre ces sauvegardes.

Au-delà de la protection contre les ransomwares, les bandes magnétiques présentent des avantages supplémentaires non négligeables. Leur durée de vie est exceptionnellement longue, avec une garantie constructeur de 30 ans de conservation des données dans des conditions de stockage appropriées. Cette longévité dépasse largement celle des disques durs ou des SSD. Pour l'archivage à long terme de données peu consultées, les bandes représentent donc la solution la plus économique disponible sur le marché. Enfin, la possibilité de stocker physiquement les cartouches hors site, dans un coffre-fort bancaire ou un site de stockage sécurisé spécialisé, offre une

protection ultime contre les catastrophes naturelles majeures comme les incendies de grande ampleur, les inondations ou même les actes de malveillance physique visant le datacenter.

VEEAM Backup & Replication

Pour assurer la protection et la récupération des données critiques de l'infrastructure, nous avons choisi de déployer Veeam Backup & Replication comme solution centrale de sauvegarde. Cette décision stratégique répond à un besoin fondamental de toute infrastructure de production : garantir qu'en cas de sinistre, d'erreur humaine ou de cyberattaque, les données peuvent être restaurées rapidement et de manière fiable.

L'approche agentless de Veeam constitue un avantage majeur pour la simplicité d'administration. Contrairement aux solutions traditionnelles nécessitant l'installation d'un agent logiciel sur chaque machine virtuelle à sauvegarder, Veeam communique directement avec l'hyperviseur Proxmox. Cette architecture signifie qu'il n'y a rien à installer, configurer ou maintenir à jour sur les 284 machines virtuelles actuelles, et qu'aucune intervention ne sera nécessaire sur les centaines de VMs qui seront créées au fil des années. Lorsqu'une nouvelle VM est déployée, il suffit de l'ajouter à un job de sauvegarde Veeam existant et elle est immédiatement protégée. Cette simplicité réduit considérablement la charge administrative et élimine les risques d'oubli de protection de certaines VMs.

Protection Contre les Ransomwares

Dans le contexte actuel de menace croissante des ransomwares, les capacités de protection spécifiques de Veeam contre ces attaques constituent un argument décisif. Veeam intègre plusieurs mécanismes de défense en profondeur conçus pour détecter, bloquer et permettre la récupération suite à des attaques par ransomware.

La détection automatique de ransomware analyse les patterns d'activité de sauvegarde pour identifier les comportements anormaux caractéristiques d'une infection. Si soudainement un très grand nombre de fichiers sont modifiés simultanément sur une VM, ce qui est typique d'un ransomware chiffrant les données, Veeam peut déclencher des alertes et même suspendre automatiquement les sauvegardes de cette VM pour éviter de sauvegarder des données déjà chiffrées par le malware.

Les sauvegardes immuables constituent une protection essentielle. Veeam peut configurer ses référentiels de sauvegarde en mode immuable où les données écrites ne peuvent être modifiées ou supprimées pendant une période définie, typiquement 30 à 90 jours. Même si un ransomware compromet les identifiants administrateurs et tente de détruire les sauvegardes pour maximiser la pression sur l'organisation, les sauvegardes immuables résistent à cette tentative. Cette fonctionnalité se marie parfaitement avec nos bandes LTO-8 WORM qui offrent une couche d'immuabilité physique supplémentaire.

La restauration rapide depuis un point de restauration propre permet de minimiser l'impact d'une attaque réussie. Grâce aux multiples points de restauration conservés, il est possible d'identifier le dernier point sain avant l'infection et de restaurer l'ensemble de l'environnement vers cet état. Veeam peut restaurer des dizaines de VMs en parallèle, permettant une reprise d'activité en quelques heures même après une infection massive de

Les Cartes iDRAC

Les cartes iDRAC, acronyme de Integrated Dell Remote Access Controller, représentent bien plus qu'un simple accessoire optionnel dans notre architecture. Il s'agit d'un composant matériel embarqué physiquement dans chaque serveur Dell, fonctionnant de manière totalement indépendante du système d'exploitation principal. Cette indépendance est cruciale car elle permet d'administrer le serveur même lorsque celui-ci est complètement planté, que le système d'exploitation refuse de démarrer, ou même que les disques durs sont défaillants.

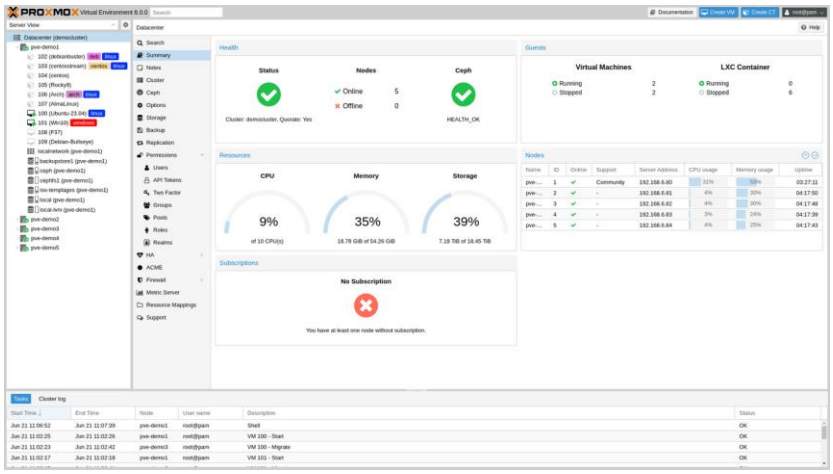
Les capacités d'administration à distance offertes par iDRAC sont extrêmement étendues. L'administrateur peut se connecter à la carte via une simple interface web depuis n'importe quel ordinateur du réseau, sans nécessiter de logiciel client spécifique. Une fois connecté, il dispose d'un accès complet à la console virtuelle du serveur, exactement comme s'il était physiquement présent devant l'écran et le clavier de la machine. Cette fonctionnalité KVM over IP, pour Keyboard Video Mouse over IP, permet de voir exactement ce qui s'affiche à l'écran du serveur, de contrôler le clavier et la souris, et d'interagir avec le BIOS ou avec l'écran de démarrage du système d'exploitation. Il est même possible de monter virtuellement des images ISO de CD-ROM ou DVD, permettant d'installer un système d'exploitation ou de lancer des outils de diagnostic sans jamais avoir à manipuler physiquement des médias.

Virtualisation

Architecture de Virtualisation Proxmox VE

Pour la couche de virtualisation de notre infrastructure, nous avons fait le choix stratégique de déployer Proxmox Virtual Environment dans sa version entreprise avec la licence de support maximum. Cette décision s'inscrit dans une approche pragmatique visant à obtenir une plateforme de virtualisation professionnelle, performante et évolutive tout en maîtrisant les coûts de licence qui peuvent rapidement devenir prohibitifs avec d'autres solutions du marché.

Proxmox VE est une solution de virtualisation open source basée sur l'hyperviseur KVM pour la virtualisation complète et sur LXC pour la conteneurisation légère. Cette double capacité offre une flexibilité remarquable car elle permet d'héberger aussi bien des machines virtuelles traditionnelles nécessitant une isolation complète qu'un système d'exploitation invité complet, que des conteneurs Linux ultra-légers pour des applications cloud-natives. L'architecture sous-jacente repose sur une distribution Debian Linux soigneusement optimisée et durcie pour un usage en production, garantissant stabilité et sécurité à long terme.



La Souscription Proxmox Enterprise

La souscription Proxmox que nous avons retenue est le niveau Enterprise de catégorie maximale, ce qui correspond techniquement à la souscription Premium avec support illimité pour un nombre illimité de CPU sockets. Cette souscription est souscrite séparément pour chaque serveur physique, donc nous aurons deux souscriptions distinctes, une pour le serveur de Paris et une pour celui de Lyon.

Cette souscription Premium débloque plusieurs avantages absolument cruciaux pour une infrastructure de production. Le premier et probablement le plus important est l'accès aux dépôts de paquets Enterprise. Ces dépôts contiennent des versions de Proxmox qui ont subi des phases de test rigoureuses et sont certifiées stables pour un usage en production. Chaque mise à jour publiée dans ces dépôts a été validée par les équipes de Proxmox et par des clients pilotes, réduisant drastiquement le risque de régression ou de bug introduit par une mise à jour. Les serveurs utilisant la souscription gratuite n'ont accès qu'aux dépôts Community où les mises à jour sont publiées plus rapidement mais avec moins de garanties de stabilité, ce qui peut être acceptable pour un environnement de test ou de développement mais certainement pas pour une infrastructure hébergeant 500 machines virtuelles en production.

Le support technique professionnel inclus dans la souscription Premium offre un accès direct aux ingénieurs de Proxmox via un portail de ticketing dédié. Les temps de réponse garantis dépendent de la criticité du ticket. Pour les incidents critiques bloquant l'ensemble de la production, le temps de première réponse est garanti sous 2 heures ouvrées, 24 heures sur 24 et 7 jours sur 7. Pour les problèmes majeurs affectant

partiellement la production, la réponse intervient sous 4 heures ouvrées. Pour les questions moins urgentes ou les demandes d'assistance, la réponse est garantie sous 8 heures ouvrées. Ces garanties de temps de réponse sont contractuelles et font l'objet de pénalités si elles ne sont pas respectées. De plus, le support Premium donne accès à un canal de communication prioritaire avec des ingénieurs seniors ayant une connaissance approfondie des architectures complexes et des configurations avancées, bien au-delà du support de premier niveau qui traite les questions basiques.

Bureautique

En ce qui concerne la bureautique, la demande initiale portait sur le renouvellement d'une partie du parc informatique devenu incompatible avec Windows 11, ainsi que sur l'équipement complet du nouveau site de Lyon. Parmi ces postes, certains devaient être des ordinateurs portables pour répondre aux besoins de mobilité, tandis que d'autres nécessitaient des performances plus élevées en fonction des usages métiers.

Pour les postes fixes standards, nous avons fait le choix de rester sur la marque Dell Technologies, déjà retenue pour les serveurs. Il s'agit d'un constructeur reconnu dans le domaine professionnel pour la fiabilité de ses équipements, la qualité de son support et la durabilité de son matériel en environnement d'entreprise.

Les postes seront équipés d'un processeur Intel® Core™ i5-14500 vPro®, doté de 14 cœurs, offrant des performances modernes et largement suffisantes pour l'ensemble des tâches de bureautique, de navigation web, de visioconférence et d'applications professionnelles courantes. Ils disposeront également de 16 Go de mémoire vive, garantissant une bonne fluidité en multitâche, ainsi que d'un disque SSD de 512 Go afin d'assurer des temps de démarrage rapides et une excellente réactivité générale du système. L'ensemble sera préinstallé sous Windows 11, conformément aux exigences de compatibilité et de sécurité actuelles.

Chaque poste sera fourni avec un kit de périphériques complet comprenant clavier, souris et écran 27 pouces, offrant un confort de travail adapté à un usage professionnel quotidien.

Pour les postes portables, nous avons également retenu des ordinateurs de la marque Dell Technologies, afin de conserver une homogénéité du parc informatique et de simplifier la gestion ainsi que le support. Les modèles sélectionnés seront équipés d'un écran 14 pouces, format idéal pour allier mobilité et confort d'utilisation.

Ils intégreront un processeur Intel® Core™ Ultra 5 235U doté de 12 cœurs, 16 Go de mémoire vive et un SSD de 512 Go. Cette configuration est largement suffisante pour répondre aux besoins de bureautique avancée, de visioconférence, d'accès aux applications métiers et de travail collaboratif, tout en garantissant une bonne autonomie et une excellente réactivité.

Afin d'assurer un confort optimal lors des périodes en présentiel au bureau, chaque ordinateur portable sera accompagné d'une station d'accueil (dock). Celle-ci permettra de connecter facilement un écran 27 pouces, ainsi que les différents périphériques (clavier, souris, réseau filaire), offrant ainsi une expérience proche d'un poste fixe tout en conservant la flexibilité du travail mobile.

Pour les postes nécessitant de très hautes performances, nous resterons également sur des stations de travail fixes de la marque Dell Technologies, mais avec une configuration nettement plus avancée afin de répondre aux besoins les plus exigeants.

Ces postes seront équipés d'un processeur Intel® Core™ Ultra 9 285K disposant de 24 cœurs, offrant une puissance de calcul importante pour les charges de travail intensives. Ils intégreront 32 Go de mémoire vive afin d'assurer une excellente fluidité lors de l'utilisation d'applications lourdes et en multitâche, ainsi qu'un SSD de 2 To garantissant à la fois rapidité d'exécution et espace de stockage confortable pour les projets volumineux. La partie graphique sera assurée par une carte dédiée GeForce RTX 5080, adaptée aux logiciels de modélisation 3D, de rendu, de simulation ou de traitement graphique avancé.

Avec ces caractéristiques, ces stations de travail seront en mesure de faire fonctionner sans difficulté l'ensemble des logiciels de modélisation et autres applications professionnelles gourmandes en ressources. Afin d'exploiter pleinement les capacités graphiques et d'améliorer le confort visuel, ces postes seront accompagnés d'un écran haute qualité de 32 pouces, offrant une meilleure surface d'affichage et une précision accrue pour les travaux nécessitant un haut niveau de détail.

Infrastructure de Bureautique et de Communication Microsoft 365

Pour répondre aux besoins de communication et de collaboration, notamment pour faciliter les échanges avec les prestataires externes, nous avons fait le choix stratégique de déployer Microsoft 365. Cette décision s'inscrit dans une approche globale visant à offrir aux utilisateurs un écosystème complet et parfaitement intégré d'outils de productivité et de communication professionnels.

Microsoft 365 représente bien plus qu'une simple suite bureautique. Il s'agit d'un ensemble complet de services cloud comprenant les applications de productivité traditionnelles que sont Word, Excel et PowerPoint, mais également des outils de communication comme Teams et Outlook, des solutions de stockage et de partage de fichiers avec OneDrive et SharePoint, ainsi que des fonctionnalités avancées de sécurité. Cette offre unifiée transforme la manière dont les équipes travaillent au quotidien en permettant une collaboration fluide aussi bien au sein de l'organisation qu'avec les partenaires et prestataires externes.

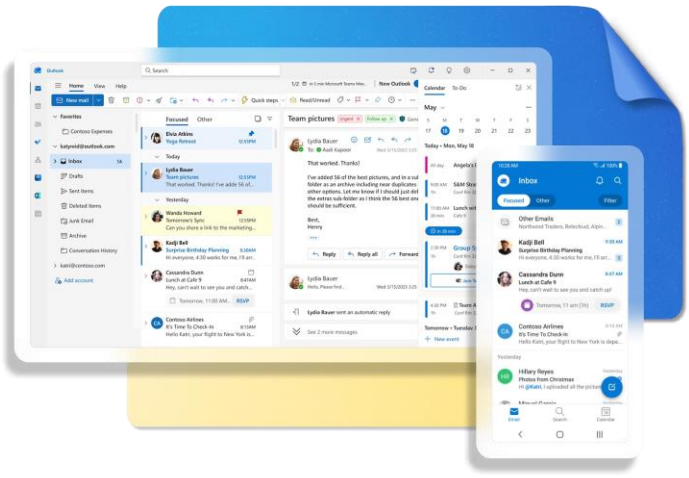
Microsoft Outlook

La migration de l'ensemble de la messagerie électronique vers Microsoft Outlook représente une décision structurante. Outlook n'est pas simplement un client de messagerie, c'est un véritable hub de communication et d'organisation personnelle qui centralise emails, calendriers, contacts, tâches et notes dans une interface unifiée.

La fonctionnalité de messagerie bénéficie de décennies d'évolution. Le moteur de recherche intégré permet de retrouver instantanément n'importe quel email parmi des années d'archives en utilisant des critères multiples comme l'expéditeur, le destinataire, le sujet, la période, ou même le contenu textuel des documents attachés. Les règles de tri automatique permettent de créer une organisation personnalisée des emails entrants, routant automatiquement certains messages vers des dossiers spécifiques, marquant d'autres comme importants, ou transférant certaines catégories d'emails vers des collègues appropriés.

La gestion des calendriers partagés représente un cas d'usage particulièrement important dans le contexte des échanges avec les prestataires. Lorsqu'un utilisateur souhaite organiser une réunion avec plusieurs participants, Outlook affiche automatiquement une vue consolidée montrant les plages horaires où tous les participants sont disponibles, éliminant les allers-retours fastidieux d'emails pour trouver un créneau convenable. Chaque utilisateur contrôle précisément ce qu'il partage de son calendrier personnel, permettant à ses collègues de voir ses plages occupées sans révéler les détails de ses rendez-vous.

L'intégration d'Outlook avec Exchange Online, la plateforme de messagerie cloud de Microsoft 365, apporte des fonctionnalités avancées impossibles avec de simples comptes de messagerie hébergés. La synchronisation en temps réel garantit que les emails, calendriers et contacts sont instantanément accessibles et identiques sur tous les appareils de l'utilisateur, que ce soit son ordinateur de bureau, son laptop, sa tablette ou son smartphone. Un email lu sur le smartphone en déplacement apparaît automatiquement comme lu sur l'ordinateur de bureau, un rendez-vous ajouté au calendrier depuis la tablette se reflète immédiatement partout.



Le filtrage anti-spam et anti-phishing utilise des algorithmes d'apprentissage automatique entraînés sur les milliards d'emails traités quotidiennement par Microsoft, détectant et bloquant automatiquement la quasi-totalité des messages malveillants. La protection contre les logiciels malveillants analyse toutes les pièces jointes en temps réel. Le chiffrement des emails en transit garantit que les communications avec les prestataires ne peuvent pas être interceptées lors de leur transmission sur Internet.

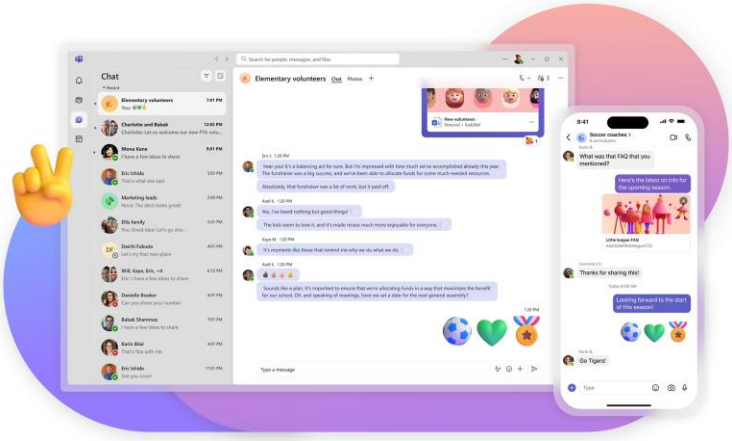
Microsoft Teams

Microsoft Teams s'est imposé comme la plateforme de référence pour la communication d'équipe et la collaboration en entreprise. Son adoption massive en a fait un standard que la plupart des prestataires externes connaissent déjà et utilisent quotidiennement. Cette familiarité généralisée facilite grandement la collaboration inter-organisationnelle car elle élimine le besoin de former les prestataires à l'utilisation d'outils spécifiques.

Teams organise la communication autour du concept de canaux regroupés dans des équipes. Une équipe correspond typiquement à un département, un projet ou un groupe de travail permanent. Au sein de chaque équipe, différents canaux permettent de segmenter les discussions par thématique ou par sous-projet. Cette organisation structurée prévient le chaos communicationnel qui peut rapidement s'installer lorsque toutes les discussions se mélangent dans un flux unique ingérable.

Pour le travail avec les prestataires, des équipes dédiées peuvent être créées pour chaque projet ou partenariat majeur. Les prestataires sont invités à rejoindre ces équipes en tant qu'invités externes, leur donnant accès uniquement aux canaux et documents pertinents pour leur collaboration sans exposer l'ensemble de l'infrastructure informatique de l'organisation. Cette granularité dans le contrôle d'accès est essentielle pour maintenir la sécurité tout en permettant une collaboration efficace.

Les fonctionnalités de visioconférence intégrées à Teams permettent d'organiser des réunions avec les prestataires sans nécessiter de solution tierce. Teams supporte des réunions pouvant accueillir jusqu'à 300 participants en simultané dans les licences standard, largement suffisant pour la plupart des besoins d'entreprise.



Word, Excel et PowerPoint

Les trois piliers traditionnels de la productivité bureautique que sont Word, Excel et PowerPoint conservent toute leur pertinence dans l'écosystème Microsoft 365, tout en bénéficiant de fonctionnalités modernes de collaboration qui transforment leur usage.

Microsoft Word reste l'outil de référence pour la création et l'édition de documents texte professionnels. L'intégration avec Microsoft 365 ajoute la co-édition en temps réel, permettant à plusieurs personnes de travailler simultanément sur le même document. Chaque utilisateur voit les modifications des autres apparaître instantanément sur son écran, avec un curseur coloré indiquant qui édite quelle partie du document. Cette fonctionnalité révolutionne la création collaborative de documents avec les prestataires, éliminant le cauchemar des versions multiples envoyées par email et fusionnées manuellement.

Microsoft Excel demeure l'outil incontournable pour tout ce qui concerne les données chiffrées, les budgets, les plannings et l'analyse. Les capacités de calcul, les fonctions financières et statistiques avancées, les tableaux croisés dynamiques pour l'analyse multidimensionnelle, et les graphiques sophistiqués en font un outil extrêmement puissant. La co-édition en temps réel permet à l'équipe interne et au prestataire de collaborer directement sur un même fichier budgétaire, chacun voyant les modifications de l'autre instantanément et pouvant commenter ou ajuster en direct.

Microsoft PowerPoint reste l'outil standard pour la création de présentations professionnelles. Que ce soit pour présenter un projet à un prestataire, pour que le prestataire présente ses propositions à l'équipe interne, ou pour créer des supports de formation, PowerPoint offre les outils nécessaires pour créer des diaporamas visuellement attractifs et professionnels.

Les modèles prédéfinis permettent de démarrer rapidement, les thèmes assurent une cohérence visuelle, et les animations apportent du dynamisme aux présentations. L'intégration avec Teams permet de partager et commenter des présentations directement dans les canaux, de les présenter en visioconférence avec des outils d'annotation en temps réel, et même de co-créer des présentations avec des collègues ou des prestataires.

Téléphonie

La téléphonie est un élément essentiel au sein de toute entreprise. Elle permet d'assurer la communication interne entre les collaborateurs, mais également les échanges avec l'extérieur, notamment avec vos clients et partenaires. Il s'agit donc d'un besoin stratégique pour garantir la continuité de votre activité. Aujourd'hui, les solutions de téléphonie VoIP associées à un PBX ont remplacé les anciens systèmes analogiques. Elles offrent davantage de fonctionnalités, une meilleure flexibilité et une intégration plus simple avec les outils numériques modernes.

Votre demande était de fournir une solution permettant à chaque employé de disposer d'un téléphone sur son poste de travail. Nous prévoyons donc l'installation d'un téléphone VoIP par utilisateur. Les modèles retenus seront des téléphones de la marque Yealink, reconnus pour leur fiabilité, leur simplicité d'utilisation et leur compatibilité avec les principales solutions de téléphonie IP du marché.

Dans une architecture VoIP, les téléphones seuls ne suffisent pas. Il est nécessaire de disposer d'un serveur téléphonique, appelé PBX, qui constitue le cœur du système. C'est lui qui gère les lignes entrantes et sortantes, la messagerie vocale, le standard téléphonique, les communications internes, le routage des appels ainsi que l'enregistrement des postes. Il centralise et orchestre l'ensemble des flux de communication.

Concernant le PBX, nous avons fait le choix d'une solution hébergée sur site, et non dans le cloud, afin de conserver une maîtrise complète de votre infrastructure téléphonique. Plutôt que d'installer un équipement physique dédié, le PBX sera virtualisé au sein de votre infrastructure Proxmox. Cette approche présente plusieurs avantages : une meilleure flexibilité, une optimisation des ressources matérielles existantes, ainsi qu'une possibilité de redondance facilitée dans votre environnement virtualisé.

Comme solution logicielle de PBX, nous avons retenu 3CX, qui est une solution reconnue, moderne et largement déployée en environnement professionnel. Elle offre une interface d'administration complète, de nombreuses fonctionnalités avancées et une grande compatibilité matérielle.

Un des avantages majeurs de 3CX est qu'il n'impose pas l'utilisation d'une marque spécifique de téléphones. Vous n'êtes donc pas dépendant d'un seul constructeur : la majorité des téléphones VoIP standards du marché sont compatibles. De plus, 3CX propose une solution de softphone, c'est-à-dire une application téléphonique virtuelle pouvant être installée sur les smartphones professionnels ou les ordinateurs portables de vos employés. Cette fonctionnalité est particulièrement utile pour les collaborateurs

en déplacement ou en télétravail, qui peuvent ainsi rester joignables sur leur numéro professionnel où qu'ils se trouvent.

Sécurité physique Site de Lyon

Dans le cahier des charges, le site de Lyon est identifié comme un site stratégique. En tant que nouveau site, vous souhaitez l'équiper entièrement, au même niveau que vos autres implantations, tout en y intégrant des technologies plus récentes. Cette modernisation ne concerne pas uniquement l'infrastructure informatique, mais également la sécurité physique des locaux.

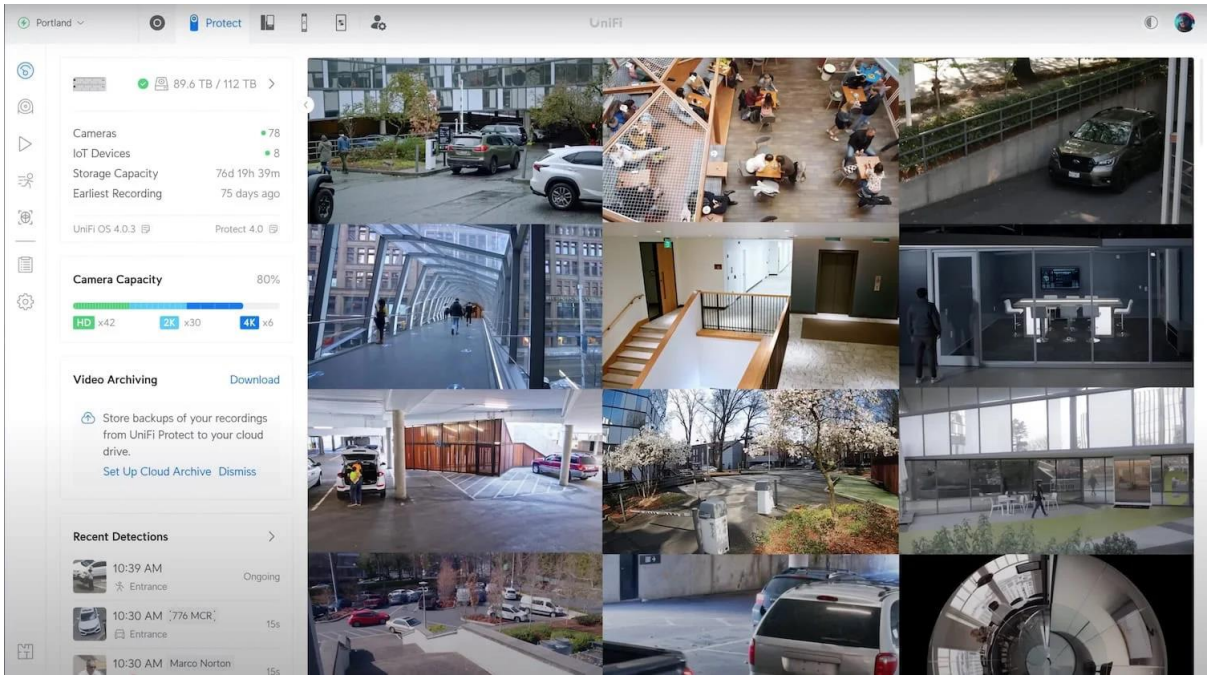
Cette exigence est d'autant plus importante que le site de Lyon accueille notamment le bâtiment dédié à la R&D de votre entreprise, et donc des activités sensibles ainsi que des informations à forte valeur stratégique. La protection de ces locaux et de vos secrets industriels constitue donc un enjeu majeur.

C'est pourquoi le site de Lyon fera l'objet de l'installation de nombreux équipements destinés à garantir un haut niveau de sécurité. Cela inclut la mise en place d'un système de vidéosurveillance, d'un contrôle d'accès, ainsi que de dispositifs d'alarme intrusion et d'alarme incendie. L'objectif est d'assurer à la fois la protection des personnes, des biens matériels et des données sensibles hébergées sur ce site.

Système de vidéosurveillance

Un élément central de tout système de sécurité est la vidéosurveillance. C'est elle qui permet d'assurer une surveillance continue de l'ensemble du site et de conserver des enregistrements exploitables en cas d'incident, comme un vol, une intrusion ou une dégradation. Un système efficace doit limiter au maximum les angles morts et s'appuyer sur des équipements performants afin de garantir une qualité d'image suffisante pour l'identification.

Pour cette partie, nous avons une nouvelle fois retenu la marque Ubiquiti Inc., au sein de la gamme UniFi Protect, dédiée aux caméras et aux NVR (Network Video Recorder). Ces dernières années, le constructeur a réalisé d'importantes évolutions, notamment en matière de qualité d'image et d'analyse intelligente. Les solutions proposées intègrent des fonctionnalités avancées telles que la détection de visages, la lecture de plaques d'immatriculation et la description automatique d'événements, ce qui renforce considérablement les capacités d'analyse et de recherche dans les enregistrements.

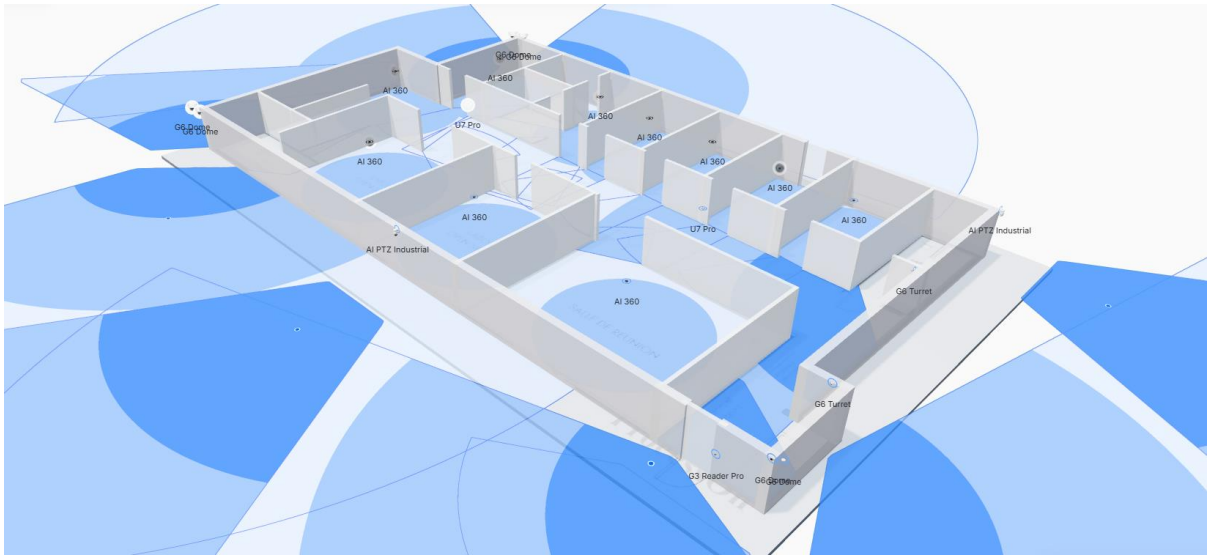


Pour les deux bâtiments du site de Lyon, les rez-de-chaussée constituent des zones critiques, puisqu'ils représentent les principaux points d'accès. Le périmètre extérieur sera donc entièrement couvert par des caméras dôme renforcées, résistantes au vandalisme, notamment des modèles UniFi Protect G6 Dome. En complément, des caméras motorisées de type PTZ, comme les UniFi Protect AI PTZ Industrial, seront déployées afin de permettre un zoom optique puissant et un suivi manuel ou automatique des personnes et des événements extérieurs. L'ensemble des caméras

installées sera en résolution 4K, offrant une haute qualité d'image et la possibilité d'exploiter efficacement les fonctions de zoom pour une identification précise.

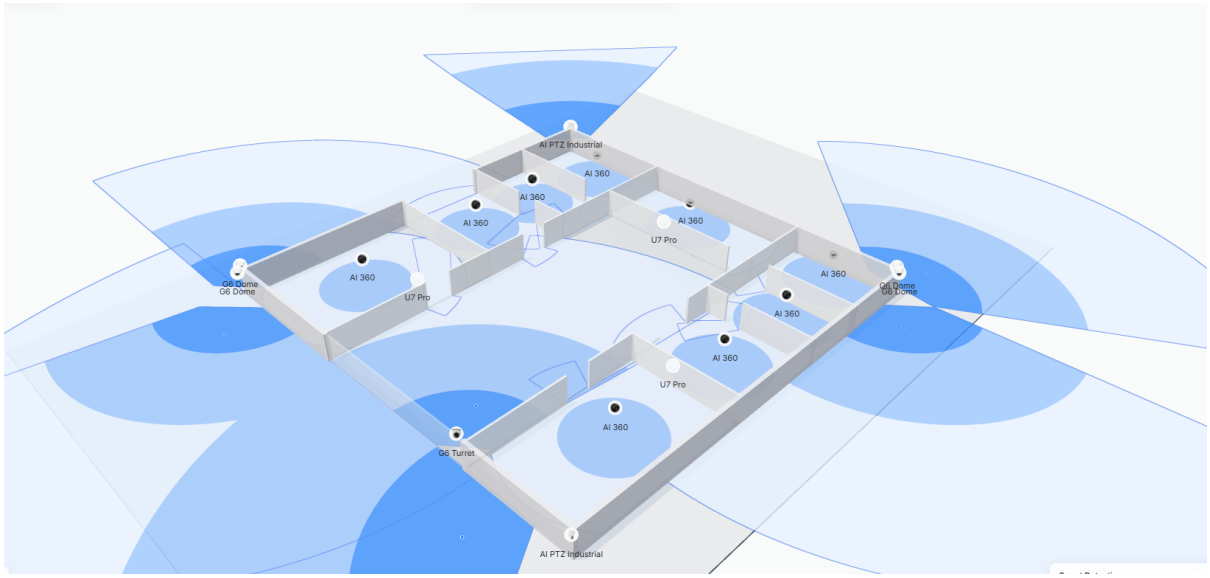
Pour l'intérieur du bâtiment R&D, chaque étage suivra la même logique de sécurisation. À partir des plans fournis, nous avons fait le choix, afin de garantir un niveau de sécurité maximal dans ce bâtiment sensible, d'installer une caméra par pièce. Les modèles retenus seront des UniFi Protect G6 360, des caméras fisheye 360 degrés permettant de couvrir l'intégralité d'une pièce sans angle mort. Ce type d'équipement est particulièrement adapté aux environnements où une surveillance complète est requise.

Pour les zones de circulation ainsi que les points d'entrée, nous utiliserons des UniFi Protect G6 Turret, des caméras 4K au format compact, offrant une bonne discrétion tout en maintenant une excellente qualité d'image.



Concernant le bâtiment principal, qui comprend l'accueil et les bureaux administratifs, la logique reste similaire. Au rez-de-chaussée, notamment au niveau de l'accueil, la surveillance du périmètre extérieur sera assurée par des caméras dôme UniFi Protect G6 Dome ainsi que par des caméras motorisées de type UniFi Protect AI PTZ Industrial, permettant un suivi dynamique et un zoom optique sur des événements spécifiques.

À l'intérieur du rez-de-chaussée, une caméra sera également installée par espace, notamment dans les salles de réunion et les zones ouvertes accessibles à différents collaborateurs ou visiteurs. Ces espaces nécessitent une surveillance adaptée compte tenu de leur fréquentation. Nous utiliserons principalement des modèles UniFi Protect G6 360 pour une couverture complète, complétés par des UniFi Protect G6 Turret selon la configuration des lieux.



En ce qui concerne les étages dédiés aux espaces de travail, nous ne prévoyons pas d'installer de caméras à l'intérieur des bureaux individuels ou des open spaces afin de respecter la réglementation en vigueur, notamment les exigences de la CNIL en matière

de protection de la vie privée. En revanche, les couloirs et zones de circulation seront équipés de caméras UniFi Protect G6 Turret, garantissant une surveillance des déplacements tout en restant conforme au cadre légal.

En ce qui concerne le stockage et le traitement des analyses, ceux-ci seront assurés par un NVR (Network Video Recorder). Cet équipement est responsable de l'exécution de la solution UniFi Protect de Ubiquiti Inc., de la gestion centralisée des caméras, mais également de l'enregistrement et de l'analyse des flux vidéo provenant de l'ensemble des équipements déployés sur le site. Il constitue ainsi le cœur du système de vidéosurveillance.

Au-delà du simple enregistrement, le NVR intègre des fonctions d'analyse avancée. Il est capable d'exploiter les capacités d'intelligence embarquées dans les caméras pour détecter et répertorier les visages, identifier des plaques d'immatriculation, différencier les personnes des véhicules, et classifier automatiquement les événements (mouvement, intrusion, présence prolongée, etc.). Ces fonctionnalités permettent d'effectuer des recherches rapides et précises dans les enregistrements, par exemple en filtrant par type d'événement ou par reconnaissance faciale, ce qui représente un véritable gain de temps en cas d'investigation.

Le NVR sera dimensionné avec 12 disques durs de 24 To, offrant une capacité de stockage conséquente. Cette configuration permettra d'assurer une rétention des images d'environ 30 jours, correspondant à la durée maximale généralement admise par le cadre réglementaire en vigueur, et suffisante pour exploiter les enregistrements en cas d'incident.

Par ailleurs, la solution retenue reste évolutive. En cas d'ajout de nouvelles caméras à l'avenir, le NVR UniFi est capable de supporter un nombre supérieur à celui actuellement déployé, garantissant ainsi une marge d'évolution sans nécessiter de remplacement immédiat de l'infrastructure existante.

Control d’accès

Le contrôle d’accès est également un élément fondamental de la sécurité d’un bâtiment, qu’il repose sur des serrures mécaniques traditionnelles ou sur des dispositifs électroniques. Il permet de définir précisément qui peut accéder à quelles zones et à quels moments. Aujourd’hui, la grande majorité des systèmes professionnels reposent sur des solutions électroniques utilisant des ventouses ou des gâches électriques, associées à un système de badge ou d’authentification avancée.

Pour le site de Lyon et ses deux bâtiments, nous avons retenu des équipements de la marque Ubiquiti Inc. au sein de la gamme UniFi Access. Cette homogénéité de marque permet de centraliser l’ensemble de la sécurité (vidéosurveillance, contrôle d’accès et supervision) au sein d’une interface unique. Cela facilite l’administration et permet des interactions entre les différents systèmes, par exemple le lien entre une ouverture de porte et l’enregistrement vidéo correspondant.

Chaque porte sera équipée d’un lecteur de badge. Selon le niveau de sensibilité de la zone concernée, nous déploierons soit un lecteur standard comme le UniFi Access Reader G3, soit un modèle plus avancé tel que le UniFi Access Reader G3 Pro. Ce dernier intègre un écran et une caméra, permettant non seulement la lecture de badge, mais également l’utilisation d’un code ou de la reconnaissance faciale. Il sera installé sur les accès principaux ainsi que sur les zones sensibles, tandis que les lecteurs standards seront utilisés pour les portes intérieures de salles ou de bureaux.

Chaque porte sera également équipée d’une gâche électrique ou d’une ventouse électromagnétique selon les contraintes techniques et les scénarios de sécurité définis. Un bouton de sortie sera intégré à l’intérieur des zones sécurisées, ainsi qu’un déclencheur manuel de secours afin de garantir une évacuation rapide en cas d’urgence.

L’ensemble du système sera piloté par des contrôleurs centraux, les UniFi Access Hub Enterprise, qui constituent la pièce maîtresse de l’installation. Chaque hub est capable de gérer jusqu’à huit portes et assure l’interconnexion entre les lecteurs, les dispositifs de verrouillage et le système de gestion centralisé, garantissant ainsi un fonctionnement cohérent et sécurisé de l’ensemble du contrôle d’accès.

Chaque employé disposera ainsi d’un badge nominatif associé à son profil dans le système, ainsi que d’un code personnel pour accéder aux bâtiments. Cette double méthode d’authentification permet de renforcer la sécurité tout en conservant une utilisation simple au quotidien.

Les droits d’accès seront configurés individuellement ou par groupe (service, fonction, niveau d’habilitation), ce qui permettra de définir précisément les zones accessibles et les plages horaires autorisées pour chaque collaborateur. Cette gestion fine garantit à la

fois la sécurité des zones sensibles, notamment au sein du bâtiment R&D, et une traçabilité complète des entrées et sorties.

Alarme

Le système d'alarme est l'un des dispositifs de sécurité les plus anciens, mais il reste aujourd'hui indispensable, même à l'ère de la vidéosurveillance et des technologies intelligentes. Il permet une détection immédiate en cas d'intrusion ou d'anomalie et constitue une couche de protection complémentaire aux caméras et au contrôle d'accès.

Le système comprendra des capteurs positionnés sur les points sensibles des bâtiments afin d'être alerté rapidement en cas de problème. Nous installerons des détecteurs infrarouges (IR) de la marque Bosch, reconnus pour leur fiabilité, dans l'ensemble des rez-de-chaussée et des couloirs. Des contacts d'ouverture (CO), également de marque Bosch, seront installés sur toutes les portes et fenêtres situées au rez-de-chaussée.

Dans une logique d'uniformisation du système de sécurité, nous utiliserons également une solution UniFi pour la gestion de l'alarme, via l'UniFi Alarm Hub. Ce contrôleur permettra de relier l'ensemble des capteurs filaires et d'assurer la remontée des informations vers l'interface centralisée. Il gérera les différents scénarios de déclenchement, les droits d'armement et de désarmement selon les profils utilisateurs, ainsi que l'activation des sirènes en cas d'alerte.

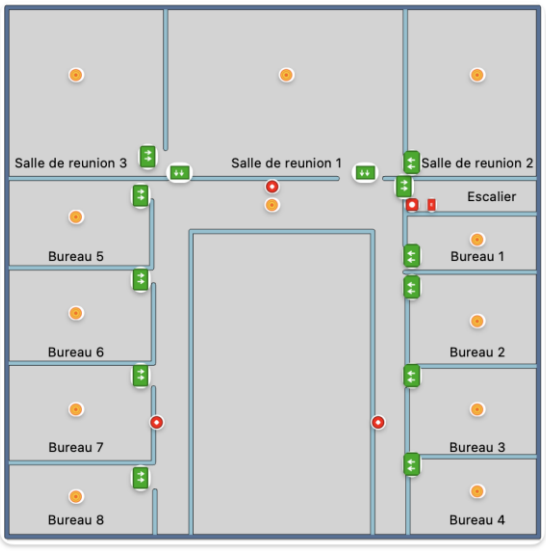
Alarme incendie

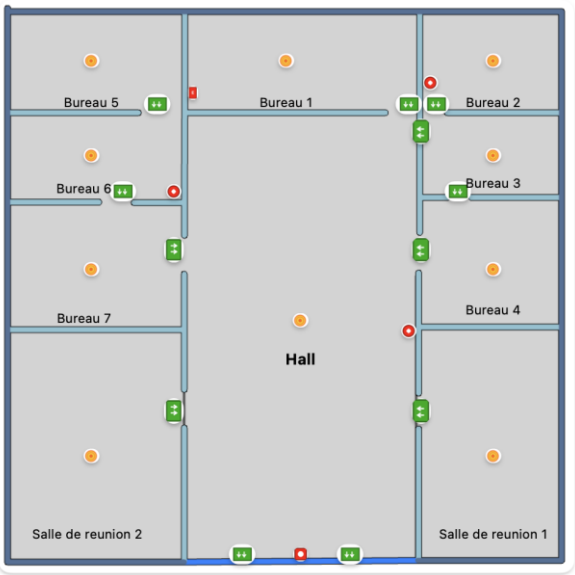
Le système d'alarme incendie constitue un élément obligatoire et essentiel pour assurer la sécurité des personnes et la protection des locaux. Contrairement aux autres dispositifs de sécurité orientés intrusion, il a pour objectif principal de détecter rapidement un départ de feu et de permettre une évacuation immédiate et organisée du bâtiment.

Des détecteurs incendie ont été installés dans l'ensemble des pièces afin d'assurer une détection précoce de fumée ou de chaleur. Des déclencheurs manuels (DM) seront positionnés à proximité des portes et des issues de secours, permettant à toute personne constatant un départ de feu d'activer l'alarme immédiatement. Le système comprendra également des diffuseurs sonores répartis stratégiquement dans les bâtiments afin de garantir que le signal d'alerte soit audible dans toutes les zones.

En complément du dispositif de détection et d'alerte, des extincteurs seront placés aux emplacements clés conformément aux normes en vigueur, notamment dans les zones à risque et à proximité des circulations principales. L'ensemble de ces équipements est représenté sur les plans ci-dessous, permettant de visualiser précisément leur implantation au sein des bâtiments.


LABO 01
LABO 02bis
LABO 02Ter
LABO 02
LABO 03
LABO 04
LABO 04
LABO 05
salle de bains
couloir
CUISINE
STOCK
LABO 06
OPEN SPACE
LABO 07
OPEN SPACE
SALLE DE REUNION
Salle des machines
Clim
Armoire à vêtements
salle d'accueil des visiteurs
Legende
DÉCLENCHEUR MANUEL
ISSUE DE SECOURS
EXTINCTEUR
SIRÈNE D'ALARME
CENTRALE ALARME INCENDIE
DÉTECTEUR DE FUMÉE


Salle de reunion 3
Salle de reunion 1
Salle de reunion 2
Escalier
Bureau 5
Bureau 1
Bureau 6
Bureau 2
Bureau 7
Bureau 3
Bureau 8
Bureau 4
Legende


Bureau 5
Bureau 1
Bureau 2
Bureau 6
Bureau 3
Bureau 7
Bureau 4
Hall
Salle de reunion 2
Salle de reunion 1
Legende

Active Directory

Introduction

L'annuaire Active Directory (AD) constitue la colonne vertébrale du système d'information de Technova. En centralisant les identités, les politiques de sécurité et l'accès aux ressources, il est le garant de la continuité d'activité et de la confidentialité des données. Toutefois, dans un contexte de menaces cybernétiques croissantes (ransomwares, attaques par rebond), un Active Directory mal configuré devient le vecteur d'attaque privilégié pour compromettre l'ensemble du réseau.

Les diagnostics initiaux, remontés par les équipes techniques de Technova, ont mis en lumière une dette technique importante et plusieurs vulnérabilités critiques affectant l'infrastructure actuelle. Parmi les faiblesses identifiées figurent une gestion perfectible du cycle de vie des comptes, une accumulation de droits d'administration (groupes à hauts privilèges surpeuplés) et une architecture de stratégies de groupe (GPO) devenue obsolète et complexe à maintenir.

Cette section du rapport a pour objectif de détailler la stratégie de refonte complète de l'annuaire, conçue pour répondre à ces enjeux de sécurité et d'évolutivité. Notre approche s'articule autour de quatre axes majeurs :

1. L'architecture et la Résilience : Le déploiement d'une nouvelle topologie multi-sites (Hub & Spoke) adaptée aux contraintes géographiques de l'entreprise.
2. L'Assainissement (Hygiène) : La mise en place de plans de remédiation pour nettoyer l'existant et réduire la surface d'attaque immédiate.
3. Le Durcissement Structurel (Security by Design) : L'implémentation du modèle de Tiering (cloisonnement des privilèges) via la solution HardenAD et l'instauration de stations d'administration sécurisées (PAW).
4. La Modernisation des Accès : Le renforcement de l'authentification via le MFA (MultiOTP) et la préparation de l'environnement vers une future hybridation avec Azure Active Directory.

Nous détaillerons ci-après les choix techniques et organisationnels retenus pour transformer l'Active Directory de Technova en une forteresse numérique.

Analyse de l'Existant et Diagnostic des Risques

Avant d'entamer la refonte de l'architecture, une phase d'analyse a été nécessaire pour comprendre l'étendue de la dette technique accumulée. Ce diagnostic ne repose pas sur un audit externe réalisé lors de ce projet, mais sur une synthèse des incidents et des vulnérabilités remontés directement par la Direction des Systèmes d'Information (DSI) de Technova. Ces remontées terrain ont permis de dresser une cartographie précise des défaillances de l'infrastructure actuelle

Synthèse des Faiblesses Identifiées

Les dysfonctionnements signalés par les équipes de Technova se concentrent sur quatre axes critiques, mettant en péril l'intégrité et la disponibilité du système d'information :

- Une gestion déficiente du cycle de vie des objets (Hygiène AD) : L'annuaire est pollué par une quantité significative d'objets obsolètes. De nombreux comptes utilisateurs (départs non traités) et comptes d'ordinateurs (machines réformées) sont toujours actifs. Ces comptes "fantômes" augmentent inutilement la surface d'attaque et peuvent servir de porte dérobée (backdoor) en cas de compromission.
- Une prolifération des privilèges élevés : Le constat le plus alarmant concerne le non-respect du principe de moindre privilège. Les groupes critiques tels que "Administrateurs du domaine" (Domain Admins) et "Administrateurs de l'entreprise" (Enterprise Admins) comptent un nombre excessif de membres. Cette situation banalise l'usage des droits d'administration pour des tâches courantes, facilitant grandement le vol d'identifiants à privilèges.
- Une obsolescence des Stratégies de Groupe (GPO) : L'architecture des GPO est décrite comme hétérogène et vieillissante. L'absence de maintenance a conduit à des conflits d'héritage, des temps d'ouverture de session allongés et, surtout, l'absence de paramètres de durcissement (Hardening) pour les OS modernes (Windows 10/11 et Windows Server 2019/2022).

La persistance de protocoles et configurations vulnérables : L'infrastructure supporte encore des protocoles dépréciés (tels que NTLMv1 ou SMBv1) pour des raisons historiques de compatibilité, exposant le réseau à des attaques classiques de type Relay ou Man-in-the-Middle.

Impacts et Nécessité de Refonte

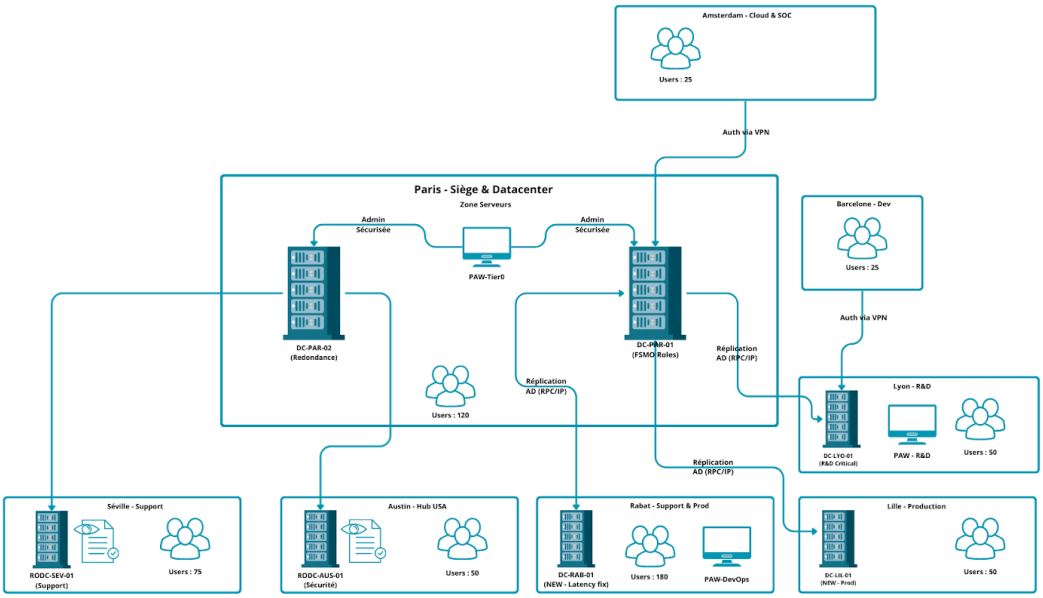
Cette configuration "par défaut" et non maintenue expose Technova à des risques majeurs :

1. Risque de Mouvements Latéraux : La surabondance d'administrateurs permet à un attaquant, une fois entré sur le réseau, de rebondir facilement de machine en machine jusqu'au contrôleur de domaine.
2. Risque de Ransomware total : L'absence de segmentation et de durcissement offre un boulevard pour la propagation rapide de logiciels malveillants à l'ensemble des sites.

Face à ce constat, une simple correction ponctuelle (patching) est insuffisante. C'est une refonte structurelle qui a été décidée, visant à reconstruire l'annuaire sur des bases saines (Security by Design) et segmentées.

Nouvelle Architecture Multi-Sites (Hub & Spoke)

Pour répondre aux besoins de croissance de Technova et garantir une disponibilité optimale des services d'identité sur l'ensemble des sites géographiques, nous avons conçu une architecture en étoile (Hub & Spoke). Cette structure permet une gestion centralisée au siège tout en offrant une autonomie locale aux sites de production et de recherche.



Stratégie de Déploiement Local

Le choix de l'infrastructure sur site repose sur une règle de dimensionnement stricte afin de ne pas surcharger les liens VPN et de garantir une expérience utilisateur fluide :

- Seuil de 50 personnes : Chaque site atteignant ou dépassant cet effectif bénéficie d'un Contrôleur de Domaine (DC) physique local. Cela permet de traiter les requêtes d'authentification et les GPO localement.
- Typologie des serveurs : Selon les besoins métiers et les contraintes de sécurité, ces serveurs sont déployés soit en lecture/écriture (RWDC) pour l'autonomie, soit en lecture seule (RODC) pour la sécurité des sites distants.

Sites nomades et accès distants : Les utilisateurs se connectant via VPN (comme pour le site d'Amsterdam) sont dirigés vers le site le plus proche géographiquement pour optimiser les temps de réponse.

Logique de Réplication (Flux AD)

Conformément au schéma d'architecture, la réplication AD (RPC/IP) suit une hiérarchie optimisée pour minimiser les flux inter-sites :

- Cœur de Forêt : La réplication s'opère de manière bidirectionnelle entre les deux serveurs du siège à Paris (DC-PAR-01 et DC-PAR-02).
- Réplication depuis le Hub : Les sites de Lyon, Lille, Rabat et Austin répliquent directement depuis le partenaire de réplication principal à Paris.
- Réplication en cascade : Le site de Barcelone, pour des raisons d'optimisation géographique, réplique ses données depuis le serveur de Lyon.

Sites RODC : Les sites de Séville et Austin reçoivent une réplication unidirectionnelle, protégeant ainsi l'intégrité de la forêt en cas de compromission locale.

Rôles et Dimensionnement par Site

Site	Type de DC	Justification métier
Paris (Siège)	2 x **RWDC**	Hub central, détention des 5 rôles FSMO et redondance critique.
Lyon (R&D)	**RWDC**	Site de plus de 50 personnes avec besoins R&D critiques.
Lille (Prod)	**RWDC**	Site de plus de 50 personnes, autonomie de production nécessaire.
Barcelone (Dev)	**RWDC**	Site de plus de 50 personnes, réplication via Lyon.
Rabat (Support)	**RWDC**	Plus de 180 personnes, autonomie locale impérative face à la latence.

Austin (Hub USA)	**RODC**	50 personnes, sécurité renforcée via le mode lecture seule.
Séville (Support)	**RODC**	75 personnes, haute sécurité pour le site de support.
Amsterdam (Cloud)	**VPN Only**	Effectif réduit (25 personnes), authentification via le VPN sur le site le plus proche.

Stratégie de Durcissement et Modèle de Tiering (HardenAD)

Pour remédier à la prolifération des privilèges et aux risques de mouvements latéraux identifiés chez Technova, la refonte s'appuie sur une segmentation stricte de l'annuaire. Cette stratégie repose sur le modèle de Tiering (ou Enterprise Access Model) de Microsoft, mis en œuvre de manière automatisée et rigoureuse via la solution HardenAD.

Le Modèle de Tiering : Cloisonnement des Identités

L'objectif est de créer des zones de sécurité étanches pour s'assurer que la compromission d'un poste utilisateur (Tier 2) ne puisse jamais conduire à la prise de contrôle des administrateurs du domaine (Tier 0).

- Tier 0 (Niveau Critique) : Comprend les contrôleurs de domaine, les administrateurs du domaine et de l'entreprise, ainsi que les serveurs hébergeant des agents de sécurité critiques. C'est le périmètre de confiance absolue.
- Tier 1 (Niveau Serveurs) : Regroupe les serveurs d'applications métiers (R&D à Lyon, Production à Lille) et leurs administrateurs respectifs.

Tier 2 (Niveau Utilisateurs) : Englobe les postes de travail standards, les utilisateurs lambda et les administrateurs de proximité.

Implémentation via HardenAD

Le script HardenAD a été utilisé comme socle de configuration pour transformer l'AD de Technova en une infrastructure "Secured by Design". Les actions suivantes ont été réalisées :

- Restructuration de l'Arborescence : Création d'Unités d'Organisation (OU) dédiées (Harden_T0, Harden_T12, _Administration) permettant d'isoler physiquement les objets selon leur niveau de criticité.

- Délégation de droits granulaire : Réinitialisation des listes de contrôle d'accès (ACL) sur les conteneurs sensibles. Désormais, un administrateur de Tier 1 n'a aucun droit de lecture ou d'écriture sur les objets du Tier 0.

Déplacement des objets : Tous les utilisateurs et ordinateurs ont été déplacés depuis les conteneurs par défaut (Users et Computers) vers cette nouvelle structure sécurisée pour éviter l'application de stratégies trop permissives

Administration Sécurisée : Les Stations PAW

L'un des piliers de cette refonte est l'interdiction formelle d'administrer l'annuaire depuis un poste de travail standard.

- Postes PAW (Privileged Access Workstations) : Des machines virtuelles durcies et isolées ont été déployées sur chaque site (Paris, Lyon, etc.) pour les administrateurs.

Flux étanches : Seules ces stations PAW sont autorisées à ouvrir des sessions d'administration sur les contrôleurs de domaine. Un administrateur de Paris utilise sa PAW Tier 0 pour gérer DC-PAR-01, garantissant qu'aucun identifiant à haut privilège ne transite sur une machine potentiellement infectée.

Durcissement par GPO (Hardening)

La refonte des stratégies de groupe a permis d'appliquer des paramètres de sécurité conformes aux recommandations de l'ANSSI et aux benchmarks CIS :

- Désactivation des protocoles à risque : Blocage systématique de SMBv1, NTLMv1 et du spouleur d'impression sur les serveurs.
- Restriction des connexions : Les administrateurs de Tier 0 ne peuvent pas se connecter (interdiction d'ouverture de session locale ou RDP) sur des machines de Tier 1 ou Tier 2.

LAPS (Local Administrator Password Solution) : Déploiement de LAPS pour gérer de manière unique et aléatoire les mots de passe des comptes "Administrateur" locaux sur chaque poste et serveur, empêchant ainsi la propagation de compromissions par compte local.

Gestion des Accès et Authentification (MFA & LAPS)

Pour répondre aux exigences de Technova en matière de protection contre le vol d'identifiants, nous avons implémenté des mécanismes d'authentification forte et une gestion dynamique des comptes locaux. Ces mesures viennent compléter le durcissement structurel pour garantir qu'un mot de passe compromis ne suffise plus à pénétrer le système d'information.

Authentification Multi-Facteurs (MFA) avec MultiOTP

L'authentification simple (login/mot de passe) est aujourd'hui considérée comme insuffisante pour les accès sensibles. Nous avons retenu la solution MultiOTP pour son interopérabilité et sa capacité à s'intégrer nativement à l'Active Directory.

- Périmètre d'application : Le MFA est imposé pour toutes les connexions jugées critiques :
    - Accès VPN : Chaque collaborateur (notamment pour le site d'Amsterdam ou les nomades) doit valider son identité via un second facteur lors de la connexion.
    - Sessions d'Administration : L'ouverture de session sur les consoles de gestion et les serveurs de Tier 0 et Tier 1 requiert une validation MFA.

Fonctionnement technique : MultiOTP génère des codes à usage unique (TOTP) synchronisés avec l'annuaire. Ce mécanisme empêche toute attaque par "Replay" ou utilisation frauduleuse de mots de passe dérobés par *phishing*.

Gestion des mots de passe locaux (LAPS)

L'une des vulnérabilités signalées par Technova était l'utilisation de comptes administrateurs locaux identiques sur de nombreux postes. Pour y remédier, nous avons déployé Windows LAPS (*Local Administrator Password Solution*) :

- Individualisation des secrets : LAPS génère automatiquement un mot de passe complexe et unique pour le compte administrateur local de chaque machine (postes Tier 2 et serveurs Tier 1).
- Stockage sécurisé : Ces mots de passe sont stockés de manière chiffrée dans un attribut protégé de l'objet ordinateur au sein de l'AD.

Rotation automatique : Le mot de passe est renouvelé périodiquement sans intervention humaine, éliminant ainsi le risque de propagation d'une compromission via des comptes locaux communs.

Protection des comptes à privilèges

En complément des outils techniques, une politique de restriction stricte a été appliquée :

- Interdiction du "Logon" croisé : Les comptes du Tier 0 ne peuvent techniquement pas ouvrir de session sur des postes du Tier 2 (Postes utilisateurs). Cela protège les comptes d'administration contre le vol de jetons de session sur des machines moins sécurisées.

Épuration des groupes : Suite au diagnostic de Technova, les groupes "Administrateurs du domaine" ont été vidés de leurs membres permanents au profit d'une gestion nominative et auditée sur les stations PAW.

Refonte et Déploiement des Stratégies de Groupe (GPO)

Pour pallier l'obsolescence de l'ancienne architecture signalée par Technova, une nouvelle structure de GPO a été mise en œuvre. Cette refonte vise à transformer les stratégies de groupe d'un simple outil de configuration en un véritable levier de sécurité proactive et de gestion granulaire des accès.

Organisation et Nomenclature

L'approche retenue sépare strictement les configurations de confort des règles de sécurité. Chaque GPO suit une nomenclature normalisée (ex: SEC_W10_Hardening ou CONF_Users_Mappages) pour faciliter l'audit et la maintenance.

- GPO de Sécurité (SEC) : Prioritaires, elles sont liées au plus haut niveau de l'arborescence (Tiers) et ne tolèrent aucune exception non justifiée.
- GPO de Configuration (CONF) : Elles gèrent l'environnement de travail utilisateur et les paramètres métiers spécifiques à chaque site (Paris, Lyon, etc.)

Les GPO de Durcissement (Hardening)

Le but principal est de réduire la surface d'attaque des postes et serveurs en s'appuyant sur les recommandations de l'ANSSI et les benchmarks CIS :

- Restriction des protocoles obsolètes : Désactivation forcée de SMBv1 et NTLMv1 sur l'ensemble du parc pour prévenir les attaques de type *Relay* et les ransomwares.
- Protection du Spouleur d'impression : Désactivation du service *Print Spooler* sur tous les contrôleurs de domaine afin de neutraliser les vulnérabilités de type *PrintNightmare*.
- Contrôle des privilèges locaux : Interdiction aux utilisateurs "lambda" d'ajouter des périphériques non autorisés ou de modifier des paramètres système critiques.

Durcissement réseau : Activation et configuration du pare-feu Windows via GPO pour bloquer les flux entrants non nécessaires, limitant ainsi les capacités de scan interne d'un attaquant.

GPO de Segmentation et de Restriction de Session

Ces stratégies sont le bras armé du modèle de Tiering mis en place avec HardenAD :

- Interdiction de connexion croisée : Une GPO spécifique interdit techniquement aux comptes de Tier 0 (Administrateurs) de se connecter sur des postes de Tier 2 (Utilisateurs). Cela empêche le vol de jetons d'administration (*Token Theft*) sur des machines exposées.

Sessions PAW : Restriction des accès RDP et physiques aux seuls postes d'administration sécurisés pour la gestion des serveurs critiques

GPO Fonctionnelles et Accès aux Données

Enfin, des stratégies ciblées répondent aux besoins métiers spécifiques de Technova :

- Accès R&D Lyon : Mise en place de GPO de filtrage de sécurité pour restreindre l'accès aux partages de données du site de Lyon. Seuls les utilisateurs membres du groupe "R&D_Lyon" voient les lecteurs réseaux mappés, garantissant la confidentialité des projets de recherche.
- Gestion du Site de Lille : Configuration des paramètres de production spécifiques (imprimantes industrielles, accès serveurs locaux) via des GPO filtrées par site (WMI Filtering).

Mise à jour et Conformité : Pilotage des cycles de mises à jour Windows Update pour s'assurer que l'ensemble des sites (Paris, Barcelone, Austin, etc.) maintient un niveau de correctifs homogène.

Conclusion et Trajectoire vers le Cloud (Azure AD / Entra ID)

La refonte de l'Active Directory de Technova ne constitue pas une fin en soi, mais le socle nécessaire à une modernisation globale du Système d'Information. En assainissant l'infrastructure locale et en instaurant un modèle de sécurité rigoureux, nous avons préparé le terrain pour une transition fluide vers un environnement **hybride**.

Préparation à l'Hybridation (Outil IdFix)

Avant d'envisager la synchronisation avec le Cloud, l'intégrité des objets de l'annuaire doit être irréprochable. L'utilisation de l'outil IdFix (Microsoft Directory Synchronization Error Remediation Tool) est préconisée pour :

- Détection d'erreurs : Identifier les doublons, les formats d'attributs invalides (caractères spéciaux, espaces) ou les adresses SMTP non conformes.
- Correction en masse : Harmoniser les objets pour garantir qu'aucune erreur ne bloque le processus de synchronisation avec Azure AD Connect.

Validation du schéma : S'assurer que les identités locales sont prêtes à devenir des identités Cloud cohérentes.

Stratégie de Migration et Identité Hybride

La trajectoire technologique pour Technova repose sur le déploiement d'Azure AD Connect (Entra Connect) pour lier l'AD local à un tenant Azure. Cette stratégie permet :

- Le Single Sign-On (SSO) : Offrir aux collaborateurs une expérience de connexion unique pour leurs applications locales et leurs outils SaaS (Microsoft 365, etc.).
- La gestion moderne (Intune) : Commencer à gérer les postes nomades (notamment pour le site d'Amsterdam) via des politiques MDM, complétant ainsi les GPO traditionnelles.

Sécurité renforcée : Bénéficier des capacités d'analyse de risques de Microsoft (Entra ID Protection) pour détecter des connexions suspectes sur les comptes synchronisés.

Conclusion de la section

En conclusion, la réponse apportée aux problématiques de Technova transforme une infrastructure vulnérable et fragmentée en un annuaire **centralisé, segmenté et audité**.

Grâce à la topologie **Hub & Spoke**, au modèle de **Tiering**, à l'automatisation via **HardenAD** et au renforcement de l'authentification (**MFA/LAPS**), Technova dispose désormais d'une identité numérique sécurisée "by design". Cette nouvelle base de confiance permet non seulement de protéger les actifs critiques de l'entreprise (comme la R&D à Lyon), mais aussi d'amorcer sereinement la transformation vers le Cloud et la mobilité.

Sécurisation surveillance

Règles Suricata

Voici les règles Suricata que l'on pourrait mettre en place au sein de votre entreprise pour détecter les attaques et pouvoir réagir contre l'attaquant par la suite.

Légende : le X représente un nombre en fonction de la partie hôte de l'adresse de l'hôte.

PROTECTION ACTIVE DIRECTORY (PRIORITÉ 1)

Alerte si LDAP est accédé depuis l'extérieur du réseau interne

alert tcp !$HOME_NET any -> 192.168.16.0/24 389 (msg:"[CRITIQUE] LDAP accès externe détecté"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:1; sid:2000001; rev:1;)

alert tcp !$HOME_NET any -> 192.168.16.0/24 636 (msg:"[CRITIQUE] LDAPS accès externe détecté"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:1; sid:2000002; rev:1;)

Détecte tentatives Kerberoasting ou Pass-the-Ticket

alert tcp any any -> 192.168.16.0/24 88 (msg:"[CRITIQUE] Kerberos - Volume anormal de requêtes TGS"; flow:to_server; content:"|6b 82|"; depth:2; threshold:type both, track by_src, count 50, seconds 60; classtype:attempted-admin; priority:1; sid:2000003; rev:1;)

PROTECTION VEEAM BACKUP (PRIORITÉ 1)

alert tcp !192.168.16.0/24 any -> 192.168.16.X 9392 (msg:"[CRITIQUE] Veeam - Accès console depuis réseau non autorisé"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:1; sid:2000010; rev:1;)

alert tcp any any -> 192.168.16.X 10006 (msg:"[CRITIQUE] Veeam - Tentative connexion service de sauvegarde"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:1; sid:2000011; rev:1;)

PROTECTION EXCHANGE SERVER (PRIORITÉ 2)

Détection scan SMTP / énumération d'utilisateurs

alert tcp any any -> 192.168.16.13 25 (msg:"[ÉLEVÉ] Exchange - Scan SMTP ou énumération"; flow:to_server; content:"VRFY"; nocase; threshold:type both, track by_src, count 10, seconds 60; classtype:attempted-recon; priority:2; sid:2000020; rev:1;)

Détection brute force OWA

alert tcp any any -> 192.168.16.13 443 (msg:"[ÉLEVÉ] Exchange - Brute force OWA détecté"; flow:to_server,established; content:"POST"; http_method; content:"/owa/auth.owa"; http_uri; threshold:type both, track by_src, count 10, seconds 120; classtype:attempted-admin; priority:2; sid:2000021; rev:1;)

Détection ProxyLogon / ProxyShell

alert tcp any any -> 192.168.16.13 443 (msg:"[CRITIQUE] Exchange - Tentative exploitation ProxyLogon"; flow:to_server,established; content:"POST"; http_method; content:"/autodiscover/autodiscover.json"; http_uri; content:"powershell"; nocase; classtype:web-application-attack; priority:1; sid:2000022; rev:1;)

PROTECTION 3CX (PRIORITÉ 2)

Détection brute force SIP (attaque sur extensions)

alert udp any any -> 192.168.16.14 5060 (msg:"[ÉLEVÉ] 3CX - Brute force SIP détecté"; content:"REGISTER"; nocase; threshold:type both, track by_src, count 20, seconds 60; classtype:attempted-admin; priority:2; sid:2000030; rev:1;)

alert tcp any any -> 192.168.16.14 5061 (msg:"[ÉLEVÉ] 3CX - Brute force SIP TLS détecté"; flow:to_server,established; content:"REGISTER"; nocase; threshold:type both, track by_src, count 20, seconds 60; classtype:attempted-admin; priority:2; sid:2000031; rev:1;)

Détection scan SIP (reconnaissance)

alert udp any any -> 192.168.16.14 5060 (msg:"[MOYEN] 3CX - Scan SIP OPTIONS détecté"; content:"OPTIONS"; nocase; threshold:type both, track by_src, count 50, seconds 60; classtype:attempted-recon; priority:3; sid:2000032; rev:1;)

Détection exploitation invite-based attacks

alert udp any any -> 192.168.16.14 5060 (msg:"[ÉLEVÉ] 3CX - Tentative INVITE flooding"; content:"INVITE"; nocase; threshold:type both, track by_src, count 100, seconds 60; classtype:attempted-dos; priority:2; sid:2000033; rev:1;)

PROTECTION UNIFI CONTROLLER

Protection interface web UniFi

alert tcp !192.168.16.0/24 any -> 192.168.16.X 8443 (msg:"[MOYEN] UniFi - Accès admin depuis réseau non autorisé"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:3; sid:2000040; rev:1;)

Détection brute force login UniFi

alert tcp any any -> 192.168.16.X 8443 (msg:"[MOYEN] UniFi - Tentative brute force login"; flow:to_server,established; content:"POST"; http_method; content:"/api/login"; http_uri; threshold:type both, track by_src, count 5, seconds 120; classtype:attempted-admin; priority:3; sid:2000041; rev:1;)

PROTECTION WSUS

alert tcp !192.168.16.0/24 any -> 192.168.16.X 8530 (msg:"[MOYEN] WSUS - Accès HTTP depuis réseau externe"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:3; sid:2000050; rev:1;)

alert tcp !192.168.16.0/24 any -> 192.168.16.X 8531 (msg:"[MOYEN] WSUS - Accès HTTPS depuis réseau externe"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:3; sid:2000051; rev:1;)

PROTECTION RDP

Protection contre brute force RDP

alert tcp any any -> 192.168.16.0/24 3389 (msg:"[ÉLEVÉ] RDP - Tentative brute force détectée"; flow:to_server; threshold:type both, track by_src, count 5, seconds 60; classtype:attempted-admin; priority:2; sid:2000060; rev:1;)

Détection scan RDP

alert tcp any any -> 192.168.16.0/24 3389 (msg:"[MOYEN] RDP - Scan de ports détecté"; flow:to_server; flags:S; threshold:type both, track by_src, count 10, seconds 60; classtype:attempted-recon; priority:3; sid:2000061; rev:1;)

PROTECTION SMB

Détection scan SMB

alert tcp any any -> 192.168.16.0/24 445 (msg:"[MOYEN] SMB - Scan réseau détecté"; flow:to_server; flags:S; threshold:type both, track by_src, count 20, seconds 60; classtype:attempted-recon; priority:3; sid:2000070; rev:1;)

Détection EternalBlue (MS17-010)

alert tcp any any -> 192.168.16.0/24 445 (msg:"[CRITIQUE] SMB - Tentative exploitation EternalBlue"; flow:to_server,established; content:"|ff|SMB|73|"; depth:5; content:"|00 00 00 00 00 00 00|"; distance:0; classtype:attempted-admin; priority:1; sid:2000071; rev:1;)

Détection brute force SMB

alert tcp any any -> 192.168.16.0/24 445 (msg:"[ÉLEVÉ] SMB - Tentative brute force authentification"; flow:to_server; content:"NTLMSSP"; nocase; threshold:type both, track by_src, count 10, seconds 120; classtype:attempted-admin; priority:2; sid:2000072; rev:1;)

Règles Wazuh

Les règles ci-dessous ne sont pas créées, mais voici, en principe, ce qu'ont vas faire pour crée la règle.

Règles 1

RÈGLE 100001 : Détection création compte administrateur

Niveau : 12 (Élevé)

Parent : 60103

Condition : Event ID 4720 ET nom contient "admin" ou "adm"

Description : Nouveau compte administrateur créé

MITRE : T1136.002 (Create Account: Domain Account)

Pourquoi : La création non planifiée de comptes admin est un indicateur majeur de compromission. Un attaquant qui a pris le contrôle d'un DC va créer un compte admin pour maintenir l'accès.

Événements Windows surveillés :

- Event ID 4720 : "A user account was created"
- Filtre sur le nom du compte créé

Règles 2

RÈGLE 100002 : Détection brute force Active Directory

Niveau : 10 (Moyen)

Parent : 60122

Fréquence : 5 échecs en 60 secondes

Condition : Event ID 4625 depuis la même IP source

Description : Tentative brute force - 5+ échecs de connexion en 1 minute

MITRE : T1110 (Brute Force)

Pourquoi : 5 échecs de connexion en 1 minute est anormal et indique une tentative d'accès par force brute. Les utilisateurs légitimes se trompent rarement plus de 2-3 fois de suite.

Événements Windows surveillés :

- Event ID 4625 : "An account failed to log on"
- Corrélation par IP source

Règles 3

RÈGLE 100003 : Détection modification Group Policy Object

Niveau : 12 (Élevé)

Parent : 60103

Condition : Event ID 5136/5137/5141 ET objectClass = groupPolicyContainer

Description : Modification de GPO détectée

MITRE : T1484.001 (Domain Policy Modification: Group Policy Modification)

Pourquoi : Les GPO contrôlent TOUT dans un environnement Windows. Une modification non autorisée peut déployer du malware, désactiver l'antivirus, créer des tâches planifiées malveillantes sur tous les postes du domaine.

Événements Windows surveillés :

- Event ID 5136 : "A directory service object was modified"

- Event ID 5137 : "A directory service object was created"

- Event ID 5141 : "A directory service object was deleted"

Règles 4

RÈGLE 100004 : Détection ajout à groupe privilégié

Niveau : 12 (Élevé)

Parent : 60103

Condition : Event ID 4728/4732/4756 ET groupe = Domain Admins/Enterprise Admins/Administrators

Description : Ajout d'un membre à un groupe administrateur

MITRE : T1098 (Account Manipulation)

Pourquoi : L'élévation de privilèges est souvent la première action après une

Compromission initiale. Un attaquant va s'ajouter aux groupes privilégiés pour

obtenir un accès complet.

Événements Windows surveillés :

- Event ID 4728 : "A member was added to a security-enabled global group"

- Event ID 4732 : "A member was added to a security-enabled local group"

- Event ID 4756 : "A member was added to a security-enabled universal group"

Règles 5

RÈGLE 100010 : Détection suppression de backup

Niveau : 15 (Critique)

Condition : Log contient "VeeamBackup" ET action = Delete/Remove

Description : Tentative de suppression de sauvegarde

MITRE : T1490 (Inhibit System Recovery)

Pourquoi : Les ransomwares ciblent Veeam en PREMIER pour détruire les sauvegardes avant de chiffrer les données. Sans backup, la victime n'a pas d'autre choix que de payer la rançon.

Logs surveillés :

- Logs applicatifs Veeam
- Recherche de commandes Delete/Remove sur les backups

Règles 6

RÈGLE 100011 : Détection arrêt service Veeam

Niveau : 12 (Élevé)

Parent : 60103

Condition : Event ID 7036 ET service contient "Veeam" ET état = stopped

Description : Service Veeam arrêté - possible attaque ransomware

MITRE : T1489 (Service Stop)

Pourquoi : Arrêter le service Veeam empêche les nouvelles sauvegardes et permet à un attaquant de détruire les backups existants sans que le système ne réagisse.

Événements Windows surveillés :

- Event ID 7036 : "The X service entered the Y state"
- Filtre sur les services Veeam

Règles 7

RÈGLE 100012 : Détection connexion en dehors des heures

Niveau : 10 (Moyen)

Parent : 60103

Condition : Event ID 4624 ET serveur = VEEAM-SERVER ET heure entre 22h-6h

Description : Connexion au serveur Veeam en dehors des heures normales

##À CONFIGURER : Remplacez "VEEAM-SERVER" par le nom réel de votre serveur##

Pourquoi : Les sauvegardes Veeam s'exécutent généralement durant la journée ou en début de soirée. Une connexion à 3h du matin est suspecte.

Événements Windows surveillés :

- Event ID 4624 : "An account was successfully logged on"
- Filtre par plage horaire

Règles 8

RÈGLE 100020 : Détection modification configuration Exchange

Niveau : 12 (Élevé)

Condition : Log contient "MSExchange" ET Event ID 1/6005/6006

Description : Modification de configuration Exchange détectée

MITRE : T1484 (Domain Policy Modification)

Pourquoi : Les modifications de configuration Exchange peuvent créer des règles de redirection d'emails, désactiver la sécurité, ou permettre l'exfiltration de données.

Logs surveillés :

- Logs Exchange Management
- Event ID 1 : Démarrage Exchange
- Event ID 6005/6006 : Modifications de configuration

Règles 9

RÈGLE 100021 : Détection brute force OWA/ECP

Niveau : 10 (Moyen)

Fréquence : 5 échecs en 120 secondes

Condition : Log MSExchange Logon ET résultat = Failed/Failure depuis même IP

Description : Brute force OWA/ECP - 5+ échecs en 2 minutes

MITRE : T1110 (Brute Force)

Pourquoi : OWA (Outlook Web Access) est souvent exposé sur Internet et constitue une cible privilégiée pour l'accès initial aux boîtes mail.

Logs surveillés :

- Logs Exchange IIS
- Logs authentification OWA/ECP

Règles 10

RÈGLE 100022 : Détection export de boîte mail

Niveau : 12 (Élevé)

Condition : Log MSExchange ET cmdlet = New-MailboxExportRequest

Description : Export de boîte mail initié - possible exfiltration

MITRE : T1114 (Email Collection)

Pourquoi : L'export de boîtes mail est rarement légitime. Un attaquant peut exporter toutes les boîtes pour voler des données sensibles (emails de direction, documents confidentiels, etc.).

Logs surveillés :

- PowerShell Exchange Management
- Cmdlet New-MailboxExportRequest

Règles 11

RÈGLE 100050 : Détection modification configuration WSUS

Niveau : 10 (Moyen)

Condition : Log contient "WSUS" ET Event ID 364/382

Description : Modification de configuration WSUS

Pourquoi : WSUS distribue les mises à jour Windows à tous les postes. Une modification peut permettre à un attaquant de distribuer de fausses mises à jour contenant du malware.

Événements Windows surveillés :

- Event ID 364 : Configuration change
- Event ID 382 : Server settings modified

Règles 12

RÈGLE 100051 : Détection ajout mise à jour non approuvée

Niveau : 12 (Élevé)

Condition : Log contient "WSUS" ET updateStatus = Unapproved

Description : Mise à jour non approuvée ajoutée - possible empoisonnement

MITRE : T1195.002 (Supply Chain Compromise: Software Supply Chain)

Pourquoi : Les mises à jour WSUS doivent être approuvées manuellement. Une mise à jour qui apparaît sans approbation peut être un malware déguisé en patch Microsoft.

Logs surveillés :

- WSUS Update Services logs
- Statut des mises à jour

Planning des Interventions

Le planning des interventions est un élément clé de tout projet. Compte tenu de l'ampleur de celui-ci, il est normal que des coupures temporaires de votre infrastructure actuelle soient nécessaires afin de procéder à son remplacement. Nous mettons cependant tout en œuvre pour que ces interruptions soient les plus courtes et les moins impactantes possible, afin de limiter au maximum la perte d'activité pour vos équipes.

La majorité des travaux liés au renouvellement de l'infrastructure concernera le site de Paris. En effet, l'infrastructure réseau y sera entièrement remplacée, tout comme l'ensemble des serveurs, ce qui représente la partie la plus conséquente du projet.

Afin de minimiser les interruptions de service, nos équipes travailleront en parallèle de votre infrastructure existante. Les nouveaux équipements (routeurs, switches et autres composants réseau) seront installés temporairement en parallèle afin d'être intégralement configurés et testés avant toute intervention sur l'existant. De cette manière, la nouvelle infrastructure réseau sera pleinement opérationnelle avant le basculement.

De plus, la mise en place des nouveaux serveurs et des services associés pourra être réalisée en amont sur cette nouvelle infrastructure, prête à être activée au moment du basculement.

Pour mener à bien ces opérations, nos équipes interviendront pendant une semaine sur le site de Paris : une équipe dédiée à l'infrastructure réseau et une équipe spécialisée en administration systèmes pour la partie serveurs.

Le basculement définitif de l'infrastructure sera réalisé durant un week-end afin de réduire l'impact sur votre activité. Cette phase comprendra le démontage de l'ancienne infrastructure, l'installation définitive de la nouvelle, ainsi que le paramétrage final des équipements et services, notamment l'intégration et l'adoption des postes de travail dans le nouvel Active Directory, afin d'assurer un fonctionnement optimal dès la reprise d'activité.

En ce qui concerne le site de Lyon, où l'ensemble de l'infrastructure sera déployé à neuf dans le cadre de la construction du site, le planning des interventions sera établi en coordination avec vos équipes présentes sur place ainsi qu'avec les différents corps de métier du chantier.

L’installation des équipements réseau ainsi que de l’ensemble des éléments de sécurité physique (vidéosurveillance, contrôle d’accès, etc.) sera réalisée en fonction de l’avancement des travaux, dès que les conditions techniques le permettront.

Nous travaillerons tout au long du chantier afin de garantir une installation propre, structurée et conforme aux standards, tant sur le plan technique qu’esthétique, assurant ainsi une mise en service optimale du site dès son ouverture.

En ce qui concerne le déploiement sur le reste de vos sites, nous appliquerons la même méthodologie que celle utilisée pour le site de Paris. En semaine, nos équipes interviendront pour installer et configurer les nouveaux équipements en parallèle de l’infrastructure existante, sans interruption de production pour vos équipes. Cette phase préparatoire pourra durer de quelques jours à une semaine selon la taille et la complexité du site.

Une fois cette étape finalisée, nous planifierons la bascule entre l’ancienne et la nouvelle infrastructure lors d’une journée non ouvrée, afin de minimiser l’impact sur votre activité.

Après chaque basculement, un processus complet de vérification et de tests des équipements et systèmes sera réalisé afin de garantir que l’ensemble fonctionne correctement avant le retour de vos équipes. Par ailleurs, des sessions de formation seront organisées pour vos équipes IT dès l’installation de la nouvelle infrastructure, afin d’assurer une prise en main efficace et autonome des nouveaux environnements.

Budget

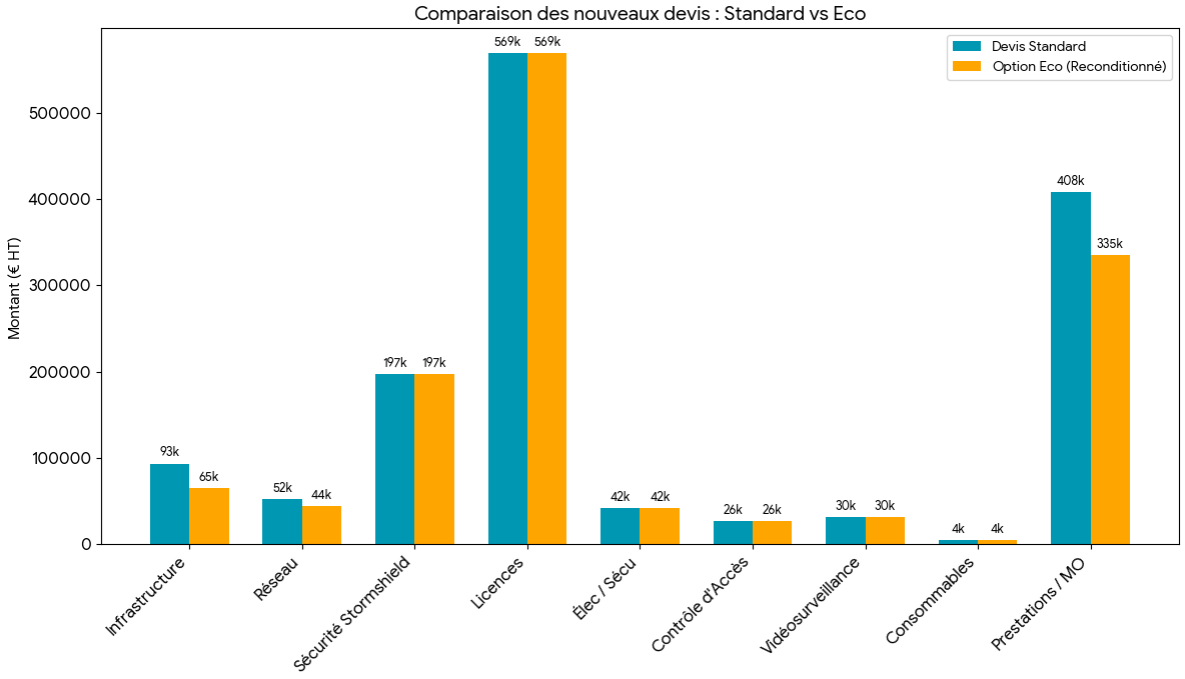
Le déploiement de l'infrastructure d'Integris a été chiffré selon deux axes stratégiques afin de répondre précisément aux exigences de performance tout en respectant les impératifs économiques du projet. La première option repose sur une solution composée intégralement d'équipements neufs, garantissant une pérennité maximale et bénéficiant des garanties standards constructeurs les plus étendues. Pour cette configuration de référence, l'investissement total s'élève à 1 425 000 € HT, soit un montant global de 1 710 000 € TTC après application de la TVA à 20 %. Ce budget couvre l'intégralité des serveurs Dell PowerEdge, les solutions réseau haute densité, la sécurité Stormshield ainsi que l'ensemble des prestations d'ingénierie et d'installation.

TOTAL HT	**1 425 000 €**
TVA (20%)	285 000 €
TOTAL TTC	**1 710 000 €**

En parfaite adéquation avec nos valeurs de durabilité et de Green IT, une seconde alternative a été étudiée sous la forme d'une option mixte incluant du matériel reconditionné de Grade A. Cette approche permet de réduire significativement l'empreinte carbone du projet tout en optimisant l'enveloppe budgétaire sans compromis sur la fiabilité opérationnelle. Dans ce cadre, le montant total de l'investissement est ramené à 1 250 000 € HT, correspondant à un total de 1 500 000 € TTC. Cette solution représente une économie de 200 000 € par rapport à l'option neuve, réalisée principalement sur les postes serveurs et certains équipements réseau, tout en conservant des licences et des prestations de services identiques pour assurer la qualité du déploiement.

TOTAL HT	**1 250 000 €**
TVA (20%)	250 000 €
TOTAL TTC	**1 500 000 €**

La comparaison directe de ces deux enveloppes budgétaires met en évidence l'avantage financier de la solution éco-responsable. Le graphique ci-dessous illustre l'écart significatif entre l'investissement standard et l'option optimisée, offrant ainsi une flexibilité décisionnelle pour l'allocation des ressources financières du groupe.

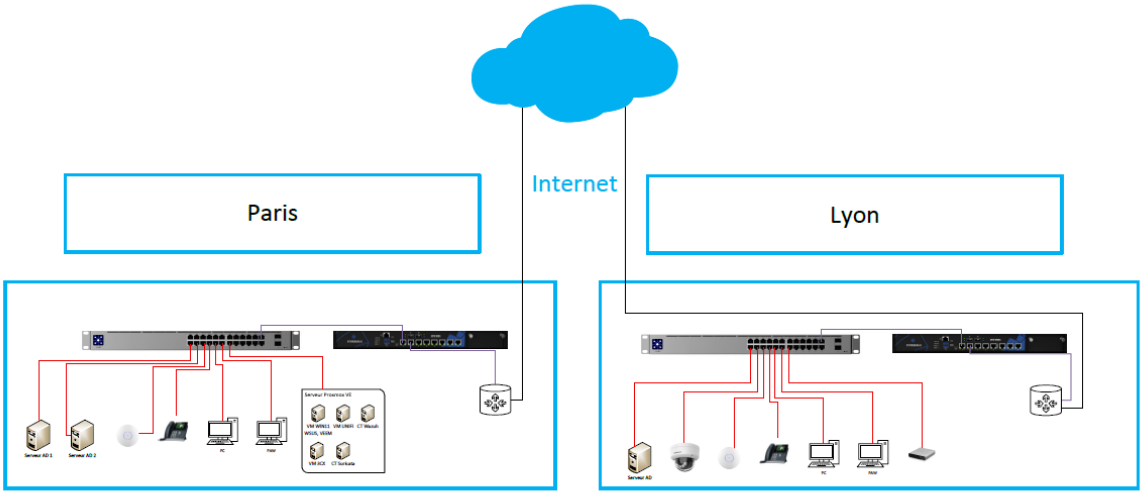


Preuve de Concept

Introduction

Fidèles à notre méthodologie où l'audit et le test précèdent tout déploiement en production, nous avons mis en place un Proof of Concept (PoC) complet. L'objectif de cette maquette à échelle réduite est de valider la viabilité, la résilience et le niveau de sécurité de l'architecture que nous avons pensée, en simulant les sites de Paris et de Lyon.

Ce laboratoire virtuel et physique nous permet d'éprouver la configuration de nos équipements et de garantir une transition sans couture lors du déploiement final.



Topologie Globale et Interconnexion (WAN)

Notre environnement de test simule de manière réaliste l'interconnexion des deux sites principaux : Paris et Lyon. Pour représenter le réseau public (Internet), nous avons intégré deux routeurs Cisco, chacun reliés à deux firewalls agissant comme cœurs de réseau WAN. La communication entre les deux sites est sécurisée de bout en bout grâce à l'établissement d'un tunnel VPN IPsec robuste entre les firewalls, garantissant la confidentialité et l'intégrité des échanges inter-sites.

Haute Disponibilité et Cœur de Réseau

Pour ce PoC, le routage inter-VLAN et la sécurité périmétrique seront centralisés sur nos firewall. Chaque site est équipé d'un firewall Stormshield. Cela nous permettra de tester la bascule automatique (failover) en cas de panne matérielle d'un boîtier.

Les firewalls seront connectés directement à des commutateurs de niveau 2 (Switchs L2). Pour garantir la redondance et maximiser la bande passante, ces liaisons utilisent le protocole d'agrégation de liens LACP (dans le cadre exclusif de ce PoC, les switchs de niveau 3 ont été écartés afin de faciliter sa mise en place).

Compartimentation et Sécurité LAN

Le PoC intègre l'ensemble de notre plan d'adressage et de notre compartimentation VLAN pour les sites de Paris et Lyon. Tous les mécanismes de durcissement (Hardening) préalablement définis y sont appliqués et testés en conditions réelles :

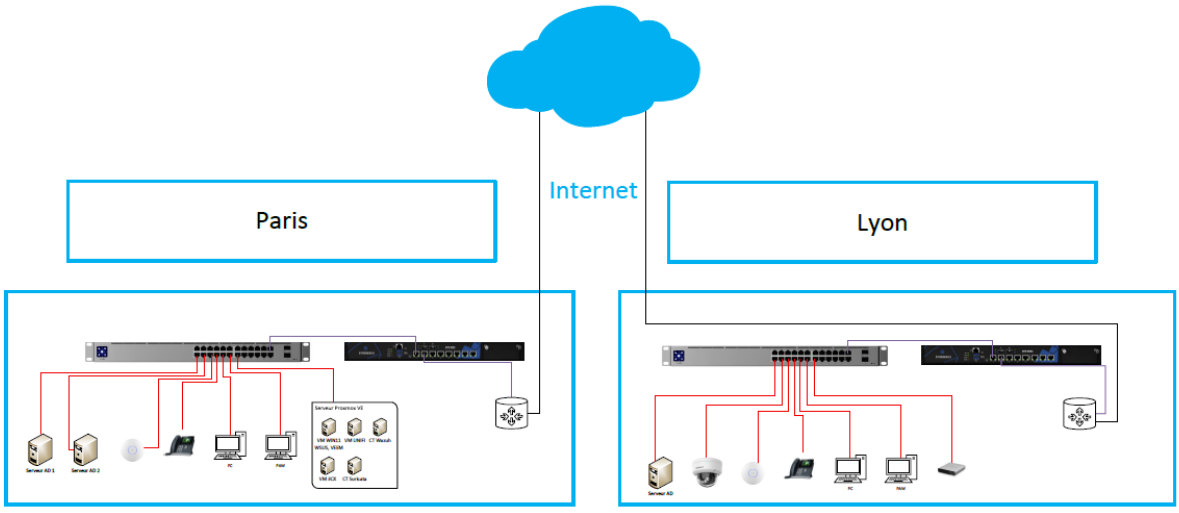
- Prévention des boucles avec RSTP et BPDU Guard.
- Contrôle des accès avec le Port Security.
- Sécurisation des attributions IP avec le DHCP Snooping.
- Administration chiffrée (SSHv2, HTTPS).

Écosystème Systèmes, Services et Endpoints

Afin de valider le comportement du réseau face à des flux réels, nous avons intégré un panel représentatif d'équipements et de services :

- Infrastructure Active Directory : Déploiement de deux contrôleurs de domaine (AD) physiques sur le site de Paris et d'un contrôleur sur le site de Lyon. Nous validons ainsi la réplication inter-sites et la haute disponibilité de l'annuaire.
- Virtualisation et SOC : Mise en place d'un hyperviseur Proxmox hébergeant nos briques critiques : le serveur de sauvegarde VEEAM, ainsi que nos solutions de cybersécurité Wazuh (SIEM) et Suricata (IDS/IPS).
- Endpoints représentatifs : Sur chaque site, des périphériques de test sont connectés et assignés à leurs VLANs respectifs : un PC bureautique, un Téléphone IP (VoIP), une borne WiFi, et un poste PAW (Privileged Access Workstation) strictement dédié à l'administration sécurisée (Tier 0).
- Spécificité du site de Lyon : Le PoC lyonnais intègre en supplément une caméra de vidéosurveillance ainsi qu'un switch Unifi dédié à sa gestion, afin de valider les flux du réseau IoT/CCTV.

Architecture du PoC



Firewall et routage

Concernant les règles de pare-feu, nous utiliserons les mêmes que celles affichées pour le site de Paris, disponibles dans la rubrique « Stratégie de filtrage Cœur de réseau ».

Pour la connexion intersite, un VPN IPsec sera mis en place entre les deux sites.

Réseaux LAN

En ce qui concerne le réseau LAN interne déployé lors du POC, nous mettrons en place une version simplifiée et miniaturisée de la solution finale. La couche de distribution ne sera pas déployée, car elle n'est pas nécessaire dans le cadre de cette phase de test.

Pour la couche d'accès, un seul switch sera utilisé. Celui-ci sera largement suffisant pour déployer les différents VLAN ainsi que l'ensemble des équipements nécessaires à la réalisation du POC. Nous utiliserons un switch UniFi dont nous disposons déjà, par exemple un modèle de type US-24-250W.

Concernant les contrôleurs, pour le site de Paris, le contrôleur sera virtualisé, soit sur un environnement Proxmox, soit au sein d'une machine virtuelle Windows. Il permettra de gérer l'ensemble des équipements du site.

Pour le site de Lyon, étant donné la nécessité d'intégrer également un NVR, nous utiliserons une Cloud Key Gen2+ qui hébergera l'application UniFi Network et assurera la gestion locale de l'infrastructure durant le POC.

Matrices d'Affectation des Ports

Site de Paris

Port	Équipement	Mode	VLANs	PoE	Sécurité & Bonnes Pratiques
1	Serveur AD 1 (VMware)	Access	18	Off	BPDU Guard, RSTP Edge
2	Serveur AD 2 (VMware)	Access	18	Off	BPDU Guard, RSTP Edge
3	Serveur Proxmox PE	Trunk	All (Native: 421)	Off	RSTP Edge (Trunk)
4	Borne WiFi Ubiquiti	Trunk	10, 11, 12 (Native: 421)	**PoE+**	LLDP-MED, Trust DHCP
5	Téléphone IP 3CX	Access	19	**PoE**	LLDP-MED, Voice VLAN, BPDU Guard
6	PC Bureautique	Access	15	Off	BPDU Guard,

					802.1X ou MAC Sec
7	PAW (Admin)	Access	12	Off	BPDU Guard, Port Security (Sticky)
...	*Ports 8 à 23*	Access	999	Off	*Shutdown (Désactivés)*
24	Stormshield SN-M (Node 2)	LACP	All (Native: 421)	Off	DHCP Trust

Site de Lyon

Port	Équipement	Mode	VLANs	PoE	Sécurité & Bonnes Pratiques
1	Serveur AD 1 (VMware)	Access	18	Off	BPDU Guard, RSTP Edge
2	Serveur AD 2 (VMware)	Access	18	Off	BPDU Guard, RSTP Edge
3	Caméra Hikvision	Access	13	**PoE+**	BPDU Guard, MAC Security (Limit 1)
4	Borne WiFi Ubiquiti	Trunk	10, 11, 12 (Native: 421)	**PoE+**	LLDP-MED, Trust DHCP
5	Téléphone IP 3CX	Access	19	**PoE**	LLDP-MED, Voice VLAN, BPDU Guard

6	PC Bureautique	Access	15	Off	BPDU Guard, 802.1X ou MAC Sec
7	PAW (Admin)	Access	12	Off	BPDU Guard, Port Security (Sticky)
8	Switch UniFi Protect	Trunk	12, 13 (Native: 421)	Off	Uplink downstream
...	*Ports 9 à 23*	Access	999	Off	*Shutdown (Désactivés)*
24	Stormshield SN-M (Node 2)	LACP	All (Native: 421)	Off	DHCP Trust

Wifi

En ce qui concerne le Wi-Fi lors du POC, nous utiliserons une à deux bornes par site, de type AC Pro et AC Lite, afin de diffuser les différents SSID et de réaliser l'ensemble de nos tests (segmentation, performances, roaming, sécurité, etc.).

Les points d'accès seront administrés via l'application UniFi Network. Pour le site de Paris, celle-ci sera virtualisée (hébergée sur l'infrastructure prévue pour le POC). Pour le site de Lyon, la gestion sera assurée directement depuis la Cloud Key Gen2+, qui centralisera l'administration des équipements réseau déployés sur place.

Serveurs

Nous avons choisi de déployer Veeam Backup & Replication sous forme de machine virtuelle directement sur l'infrastructure Proxmox. Cette approche présente plusieurs avantages significatifs par rapport à une installation sur serveur physique dédié. La VM Veeam sera hébergée sur le stockage haute performance NVMe pour garantir des performances optimales lors des opérations de sauvegarde et de restauration.

La machine virtuelle Veeam sera dimensionnée avec des ressources généreuses pour assurer des performances optimales. Nous prévoyons d'allouer environ 500 Go de stockage pour le système d'exploitation Windows Server et l'application Veeam elle-même. Ces ressources permettront à Veeam de gérer simultanément de nombreux jobs de sauvegarde et de restauration sans ralentissement.

Le déploiement sous forme de VM plutôt que sur serveur physique offre une flexibilité appréciable. Si les besoins en ressources augmentent avec la croissance de l'infrastructure, il sera simple d'ajouter des cœurs CPU ou de la RAM à la VM sans intervention matérielle. De plus, la VM Veeam elle-même peut être protégée par des snapshots Proxmox et être migrée entre les sites si nécessaire.

Périmètre de Sauvegarde : VMs et Partage de Fichiers

Le périmètre de sauvegarde couvert par Veeam est volontairement exhaustif pour garantir une protection complète de l'infrastructure. Veeam sauvegardera l'intégralité des machines virtuelles hébergées sur les deux serveurs Proxmox de Paris et Lyon, actuellement au nombre de 284.

L'approche de sauvegarde au niveau de l'hyperviseur utilisée par Veeam présente des avantages considérables par rapport aux sauvegardes traditionnelles au niveau du système d'exploitation. Veeam communique directement avec Proxmox via ses API pour créer des snapshots des VMs, capture l'intégralité de la machine virtuelle incluant le système d'exploitation, les applications, les données et la configuration, puis transfère ces données vers le référentiel de sauvegarde. Cette méthode agentless, ne nécessitant pas l'installation de logiciel sur chaque VM, simplifie considérablement l'administration et réduit les risques de conflits ou de dysfonctionnements.

Veeam peut sauvegarder ces données soit en traitant les serveurs de fichiers comme des VMs ordinaires si les partages sont exposés via des VMs dédiées, soit en utilisant des agents Veeam spécifiques pour Windows ou Linux qui s'installent sur les serveurs hébergeant les partages.

Virtualisation

Type Hyperviseurs

Un hyperviseur est un logiciel (ou un micro-noyau spécialisé) qui permet d'exécuter plusieurs systèmes d'exploitation sur une même machine physique. Il crée et isole des machines virtuelles (VM) en partageant les ressources matérielles : processeur, mémoire, stockage et réseau entre plusieurs environnements indépendants. L'objectif principal est l'optimisation des ressources, l'isolation des services et la flexibilité opérationnelle.

On distingue deux grandes catégories d'hyperviseurs. Les hyperviseurs de type 1, dits « bare metal », s'installent directement sur le matériel sans passer par un système d'exploitation hôte. Ils offrent de meilleures performances, une meilleure stabilité et un niveau d'isolation plus élevé. Des solutions comme VMware ESXi, Microsoft Hyper-V ou Proxmox VE appartiennent à cette catégorie. Les hyperviseurs de type 2, quant à eux, s'installent au-dessus d'un système d'exploitation existant. Ils sont souvent utilisés pour des environnements de test ou des postes de travail, comme VirtualBox ou VMware Workstation.

Le rôle technique d'un hyperviseur consiste à virtualiser le matériel grâce aux extensions CPU (Intel VT-x ou AMD-V), à planifier l'accès aux ressources et à garantir l'isolation entre les machines virtuelles. Il gère également les périphériques virtuels (cartes réseau virtuelles, disques virtuels, contrôleurs SCSI, etc.) et peut proposer des fonctions avancées comme la haute disponibilité, la migration à chaud ou la sauvegarde centralisée.

Proxmox VE c'est quoi ?

Proxmox VE (Proxmox Virtual Environment) est un hyperviseur de type 1 basé sur Debian. Il combine deux technologies majeures : KVM pour la virtualisation complète de machines virtuelles et LXC pour la virtualisation légère par conteneurs. Cette double approche permet d'exécuter à la fois des systèmes d'exploitation complets (Windows, Linux, etc.) et des conteneurs plus légers partageant le noyau Linux de l'hôte.

Son fonctionnement repose sur plusieurs composants. Le noyau Linux agit comme base du système. KVM transforme ce noyau en hyperviseur capable d'exécuter des machines virtuelles avec virtualisation matérielle. LXC permet la création de conteneurs isolés, plus légers et plus rapides à déployer. L'interface d'administration web centralise la gestion des VM, du stockage, du réseau et des sauvegardes.

Proxmox intègre également une gestion avancée du stockage. Il prend en charge différents types de backends comme les disques locaux, NFS, iSCSI ou Ceph. Il supporte

ZFS, qui apporte des fonctionnalités telles que les snapshots, la réplication et la protection contre la corruption des données. En environnement cluster, plusieurs nœuds Proxmox peuvent être regroupés afin de permettre la migration à chaud des machines virtuelles et la haute disponibilité.

Le réseau dans Proxmox repose sur des bridges Linux et peut intégrer des VLAN. Cela permet de connecter les VM directement aux segments réseau physiques ou logiques, ce qui est particulièrement utile dans une architecture segmentée avec plusieurs VLAN, comme dans ton projet.

Les avantages de Proxmox VE

Proxmox présente plusieurs avantages importants, notamment dans un contexte d'infrastructure professionnelle ou de laboratoire technique avancé.

Le premier avantage est son modèle open source. Contrairement à certaines solutions propriétaires, Proxmox ne nécessite pas de licence coûteuse pour fonctionner. Cela permet de réduire significativement les coûts d'infrastructure tout en conservant des fonctionnalités avancées.

Un autre avantage majeur est l'intégration native de la virtualisation et des conteneurs. Pouvoir gérer à la fois des VM complètes et des conteneurs LXC sur la même plateforme offre une grande flexibilité. Les services nécessitant une isolation forte peuvent être déployés en VM, tandis que les services plus légers peuvent fonctionner en conteneurs pour optimiser les ressources.

La gestion du stockage est également un point fort, en particulier avec ZFS. Les snapshots, la réplication et la gestion fine des volumes facilitent la sauvegarde et la reprise après incident. Cela est particulièrement intéressant dans un projet incluant des serveurs de fichiers, des serveurs mail ou des services critiques.

Proxmox propose aussi des fonctionnalités avancées habituellement réservées aux environnements d'entreprise : clustering, haute disponibilité, migration à chaud des VM et sauvegardes planifiées. Ces capacités permettent d'assurer la continuité de service et d'améliorer la résilience de l'infrastructure.

Enfin, l'interface web centralisée simplifie l'administration. Elle permet de gérer l'ensemble des ressources depuis un navigateur sans nécessiter d'outils externes complexes. Pour un administrateur réseau ou système, cela représente un gain de temps important dans la gestion quotidienne.

Téléphonie

Au niveau de la téléphonie, nous mettrons en place exactement le même principe que dans la solution finale. Le serveur 3CX sera virtualisé, soit sur l'infrastructure Proxmox du POC, soit au sein d'une machine virtuelle Windows.

Nous avons également souscrit à une licence de test d'un mois afin de pouvoir réaliser l'ensemble des configurations et des essais dans des conditions proches du réel.

Plusieurs téléphones IP seront déployés ainsi que différents comptes SIP de test, afin de simuler une situation réelle d'entreprise (appels internes, transferts, files d'attente, messagerie vocale, etc.) et valider le bon fonctionnement global de la solution.

Sécurité physique Site de Lyon

Pour ce qui concerne la sécurité physique du site de Lyon, nous allons déployer une version simplifiée de la solution réelle, en utilisant des équipements de test représentant la solution finale. Pour cela, une Cloud Key Gen2+ sera installée sur le site de Lyon et fera fonctionner UniFi Protect, de la même manière que le NVR dans la solution complète. Pour tester la vidéosurveillance, une caméra sera connectée et des enregistrements seront réalisés afin de vérifier le bon fonctionnement du système.

En ce qui concerne le contrôle d'accès, un Hub Mini sera déployé. Il fonctionne de la même manière qu'un Enterprise Hub, mais pour une seule porte. Il sera accompagné d'un lecteur G3 et d'une ventouse magnétique simulant une porte, permettant de tester les fonctionnalités de gestion d'accès et d'authentification.

Lors du POC, nous ne testerons pas les systèmes d'alarme ni les dispositifs d'alarme incendie, car leur mise en œuvre serait trop complexe pour cette phase de test.

Active Directory PoC

Objectifs du POC

La réalisation de cette preuve de concept vise à valider techniquement la refonte de l'annuaire avant son déploiement à grande échelle. Le POC se concentre sur trois axes majeurs :

- L'interconnexion multi-sites : Simulation de la réplication et de la gestion des ressources entre le siège (Paris) et un site de production (Lyon).
- La sécurité "Zero Trust" : Validation du modèle de Tiering, du durcissement HardenAD et des scores d'audit.

L'expérience utilisateur et admin : Démonstration de l'usage des stations PAW, du MFA et de la gestion granulaire des partages de fichiers.

Déploiement de l'Infrastructure Physique

Le laboratoire est structuré pour isoler et simuler les deux sites géographiques majeurs :

Simulation du Site de Paris (Siège)

- Contrôleurs de Domaine (DC) : Mise en place de deux serveurs physiques (PAR-DC01 et PAR-DC02). Ils fonctionnent en haute disponibilité (RWDC) avec réplication active.
- Poste d'Administration (PAR-PAW01) : Une station PAW dédiée exclusivement aux tâches de Tier 0. Elle sert de point d'entrée unique pour toute modification sur l'infrastructure.
- Poste Client (PAR-PC-USER) : Un PC utilisateur standard utilisé pour démontrer le login classique et l'application des GPO de base.

Simulation du Site de Lyon (R&D)

- Contrôleur de Domaine (LYO-DC-01) : Un serveur local gérant l'authentification du site pour garantir l'autonomie métier.
- Poste d'Administration (LYO-PAW-01) : Une station dédiée à l'administration du site de Lyon (Tier 1).
- Poste Client (LYO-PC-USER) : Une machine client destinée à la démonstration spécifique des accès aux dossiers partagés de la R&D.

Mise en œuvre de la Sécurité

La sécurité du POC repose sur trois piliers technologiques testés en conditions réelles :

- Durcissement via HardenAD : L'arborescence des Unités d'Organisation (OU) est segmentée. Les privilèges sont cloisonnés pour empêcher tout mouvement latéral entre les postes utilisateurs et les serveurs.
- Authentification Multi-Facteurs (MFA) : Intégration de MultiOTP. Chaque accès aux stations PAW ou toute session sensible nécessite la validation d'un second facteur (TOTP), sécurisant ainsi l'identité même en cas de vol de mot de passe.

Gestion des Comptes Locaux (LAPS) : Déploiement de la solution pour garantir que chaque machine possède un mot de passe administrateur local unique et chiffré dans l'AD.

Validation par l'Audit (Objectifs chiffrés)

La conformité du POC est mesurée par deux outils d'audit de référence :

- PingCastle : L'infrastructure est configurée pour obtenir un Domain Risk Level de 0/100. Ce score atteste de l'absence de vulnérabilités de configuration et du respect des bonnes pratiques d'hygiène AD.

- Purple Knight : L'objectif est d'atteindre le score le plus élevé possible (grade A ou B+). Les seuls points non obtenus correspondent aux alertes de "modifications récentes" (création massive d'objets lors du montage du lab), lesquelles sont inhérentes au déploiement du POC.

Scénarios de Démonstration (Cas d'usage)

Le POC permet de valider concrètement les règles de gestion suivantes :

1. Démonstration des FileShare : Utilisation du poste utilisateur de Lyon pour prouver que les droits d'accès aux données R&D sont strictement limités par GPO. Les dossiers sont inaccessibles (et masqués) pour les utilisateurs ne faisant pas partie du groupe métier.
2. Validation du Tiering : Tentative de connexion (échouée) d'un administrateur Tier 0 sur un PC utilisateur lambda pour prouver l'étanchéité des sessions.

Réplication Inter-Sites : Création d'un utilisateur à Paris et vérification de sa réplication sur le serveur de Lyon, validant ainsi la fluidité de la topologie Hub & Spoke.

Sécurisation surveillance

Dans le cadre de notre engagement pour la restauration de l'intégrité des systèmes d'information, la mise en place d'une surveillance continue est un pilier fondamental de notre phase de « Support ». Pour répondre aux exigences de la norme ISO 27001 et garantir une réactivité optimale face aux menaces, nous avons fait le choix d'implémenter un centre d'opérations de sécurité (SOC) basé sur l'alliance de deux solutions de pointe : Wazuh (SIEM/XDR) et Suricata (IDS/IPS).

L'infrastructure, répartie sur plusieurs sites (Paris, Lyon) et reposant sur une architecture segmentée en VLAN, nécessite une visibilité à la fois sur les hôtes et sur les flux réseaux. Notre approche repose sur le principe du « Zero Trust » et la centralisation systématique des journaux via le protocole Syslog, indispensable pour l'audit a posteriori.

Suricata est déployé stratégiquement au niveau du cœur de réseau, en interface avec nos pare-feux Stormshield et nos commutateurs d'agrégation Ubiquiti USW-Pro.

- Analyse des flux Est-Ouest : Grâce à la configuration de ports miroirs (SPAN) sur nos switches de distribution, Suricata analyse le trafic entre les différents VLAN (Bureautique, Serveurs, IoT). Il permet de détecter toute tentative de mouvement latéral d'un attaquant qui aurait réussi à pénétrer un poste de travail.
- Détection d'intrusions (IDS) : Suricata utilise des signatures (règles) régulièrement mises à jour pour identifier des schémas d'attaque connus (scans de ports, exploitation de vulnérabilités, trafic vers des IP malveillantes).

- Analyse de protocoles : Il inspecte les flux non chiffrés et peut extraire des métadonnées précieuses sur les requêtes DNS ou les échanges HTTP, complétant ainsi le filtrage strict appliqué par nos firewalls

Wazuh constitue le socle central de notre surveillance. Il assure la collecte, l'analyse et l'indexation de l'ensemble des événements de sécurité de l'infrastructure.

- Surveillance des agents (HIDS) : Des agents Wazuh sont déployés sur tous les serveurs critiques (Dell PowerEdge) sous Proxmox, ainsi que sur les contrôleurs Active Directory. Ils surveillent en temps réel :
    - L'intégrité des fichiers (FIM) : Pour détecter toute modification suspecte de fichiers système ou de configuration.
    - Les processus et les logs système : Identification des connexions frauduleuses ou des élévations de privilèges.
- Centralisation des logs réseaux : Les équipements Ubiquiti UniFi (switches et bornes WiFi 7) ainsi que les firewalls Stormshield exportent leurs journaux de sécurité (logs de connexion, alertes de protection de couche d'accès comme le BPDU Guard ou le DHCP Snooping) vers Wazuh via Syslog.

- Évaluation de la conformité : Wazuh scanne régulièrement nos systèmes pour vérifier leur alignement avec les bonnes pratiques de durcissement (CIS Benchmarks), assurant ainsi que nos serveurs et postes de travail Windows 11 Pro conservent un niveau de sécurité optima

L'intérêt majeur de notre solution réside dans l'intégration native de Suricata au sein de Wazuh. Les alertes générées par Suricata au niveau réseau sont automatiquement ingérées par Wazuh, permettant une corrélation puissante :

- Exemple de scénario : Si Suricata détecte un trafic malveillant provenant d'un poste de travail à Paris (VLAN 15), Wazuh peut immédiatement corréler cette alerte avec les logs de l'agent installé sur ce même poste pour identifier le processus précis à l'origine de l'attaque.

Conformément à l'utilisation du protocole NTP, l'ensemble de nos logs est synchronisé temporellement, permettant une analyse forensique précise en cas d'incident. Le SOC permet ainsi :

1. Alerte en temps réel : Notification immédiate des équipes techniques via le tableau de bord centralisé ou par email.
2. Investigation : Capacité de remonter l'historique d'un attaquant sur plusieurs jours grâce à l'indexation massive des données.

3. Amélioration continue : Chaque incident détecté permet d'affiner nos règles de filtrage Stormshield et de renforcer la segmentation de notre architecture LAN.

En combinant la puissance d'analyse réseau de Suricata et la capacité de gestion d'événements de Wazuh, Intégris garantit une infrastructure non seulement performante, mais résiliente, capable de s'adapter aux menaces persistantes modernes.

Nous allons réaliser un POC (Proof of Concept) en utilisant les règles importantes de Suricata et de Wazuh afin de tester leur efficacité dans la détection et la prévention des attaques au sein de notre environnement. Cela permettra d'évaluer leur pertinence avant un déploiement à plus grande échelle.

Voici ci-dessous les règles les plus importantes pour Wazuh et Suricata.

Suricata

Alerte si LDAP est accédé depuis l'extérieur du réseau interne

alert tcp !$HOME_NET any -> 192.168.16.0/24 389 (msg:"[CRITIQUE] LDAP accès externe détecté"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:1; sid:2000001; rev:1;)

alert tcp !$HOME_NET any -> 192.168.16.0/24 636 (msg:"[CRITIQUE] LDAPS accès externe détecté"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:1; sid:2000002; rev:1;)

Détection brute force login UniFi

alert tcp any any -> 192.168.16.X 8443 (msg:"[MOYEN] UniFi - Tentative brute force login"; flow:to_server,established; content:"POST"; http_method; content:"/api/login"; http_uri; threshold:type both, track by_src, count 5, seconds 120; classtype:attempted-admin; priority:3; sid:2000041; rev:1;)

Protection WSUS

alert tcp !192.168.16.0/24 any -> 192.168.16.X 8530 (msg:"[MOYEN] WSUS - Accès HTTP depuis réseau externe"; flow:to_server,established; threshold:type limit, track by_src, count 1, seconds 300; classtype:attempted-admin; priority:3; sid:2000050; rev:1;)

alert tcp !192.168.16.0/24 any -> 192.168.16.X 8531 (msg:"[MOYEN] WSUS - Accès HTTPS depuis réseau externe"; flow:to_server,established; threshold:type limit, track

by_src, count 1, seconds 300; classtype:attempted-admin; priority:3; sid:2000051; rev:1;)

Wazuh

Les règles les plus importantes pour assurer le bon fonctionnement du POC sont celles présentées ci-dessous.

RÈGLE 100001 : Détection création compte administrateur

RÈGLE 100002 : Détection brute force Active Directory

RÈGLE 100003 : Détection modification Group Policy Object

RÈGLE 100010 : Détection suppression de backup

Annexe

Mise en œuvre du Laboratoire Active Directory (Siège Paris)

Contexte et Objectifs

La présente annexe a pour vocation de détailler les spécifications techniques et les configurations appliquées lors du déploiement de l'environnement de laboratoire ("Lab"). L'objectif principal de cette maquette est de simuler fidèlement l'infrastructure Active Directory du siège social de Paris, afin de valider les mécanismes d'authentification, de réplication et d'administration sécurisée avant toute mise en production.

Architecture de Virtualisation

L'ensemble de l'infrastructure est hébergé sur un hyperviseur Proxmox VE. Ce choix permet de garantir l'isolation des environnements tout en offrant la flexibilité nécessaire à la gestion des ressources virtuelles.

Le périmètre de ce laboratoire comprend le déploiement des machines virtuelles et l'utilisation des outils suivants :

- **Infrastructure d'Annuaire (Haute Disponibilité) :**
  - Déploiement de deux contrôleurs de domaine (DC).
  - Configuration de la réplication Active Directory entre ces deux nœuds pour assurer la redondance et la continuité de service.
- **Sécurisation de l'Administration :**
  - Mise en place d'une **PAW (Privileged Access Workstation)**. Cette station dédiée est strictement réservée aux tâches d'administration afin de cloisonner les accès à privilèges (modèle *Tiering*).
- **Environnement Utilisateur :**
  - Intégration d'un poste client standard ("PC User Lambda").
  - Ce poste servira à valider l'application des stratégies de groupe (GPO) et l'expérience utilisateur finale.
- **Audit et Validation de la Sécurité :**
  - Réalisation de scans de vulnérabilités et d'audits de configuration post-déploiement.

Utilisation des solutions **PingCastle** et **Purple Knight** pour cartographier les risques et mesurer le niveau de sécurité de l'Active Directory (AD Security Score).

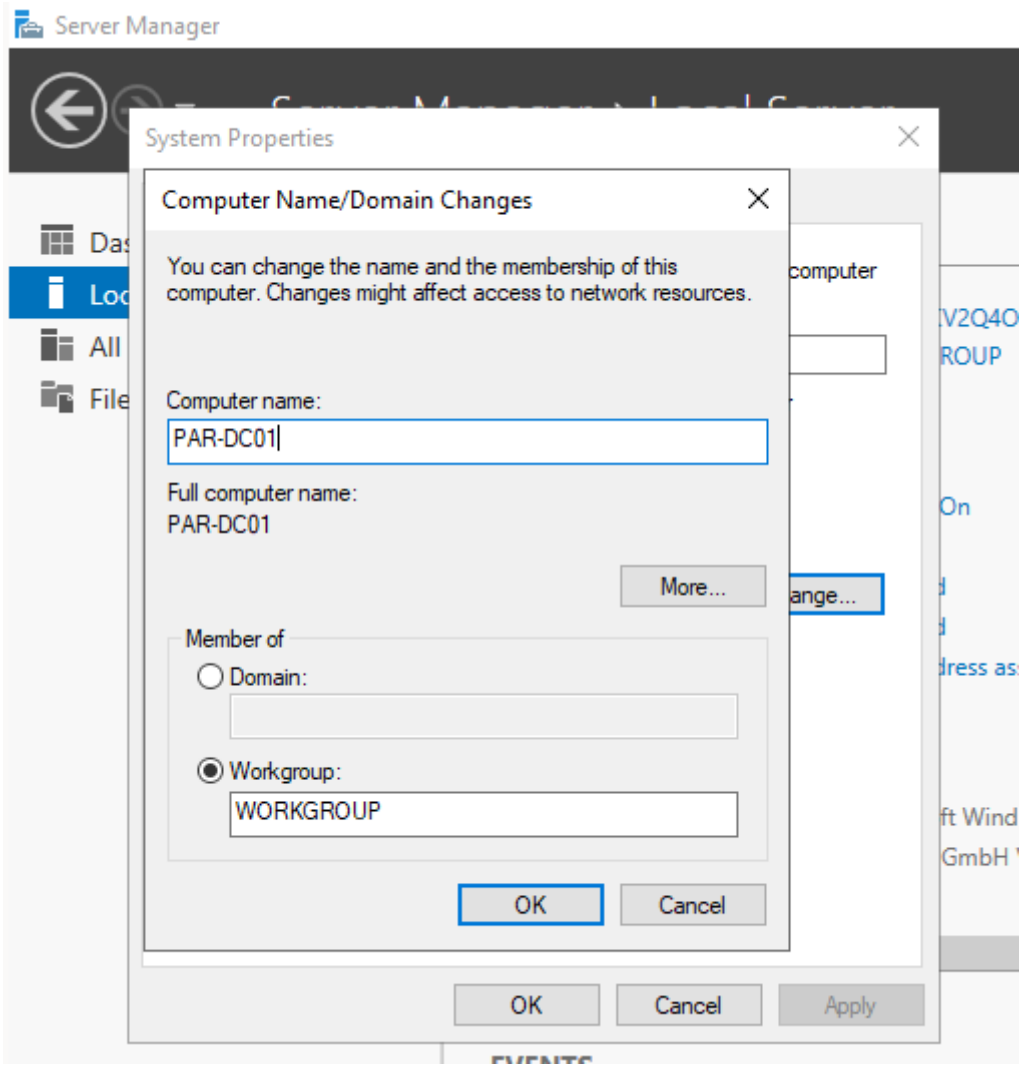
Mise en place du Premier Contrôleur de Domaine (PAR-DC01)

Cette section décrit le déploiement du contrôleur de domaine racine de la forêt, pierre angulaire de l'infrastructure Active Directory du site de Paris.

Préparation et Identité du Serveur

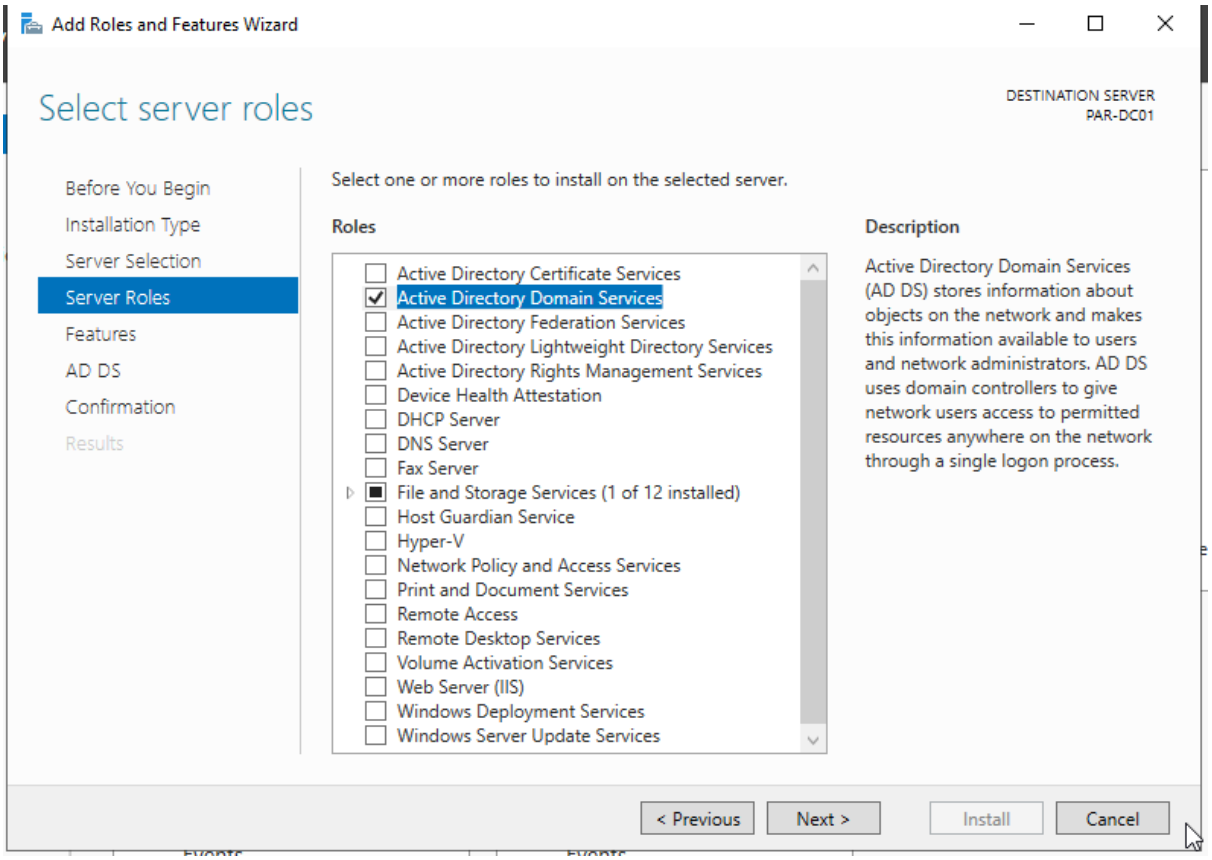
Avant toute installation de rôle, l'identité du serveur a été normalisée pour respecter la convention de nommage définie pour le site de Paris (Paris - Domain Controller - 01).

- Nom d'hôte : PAR-DC01

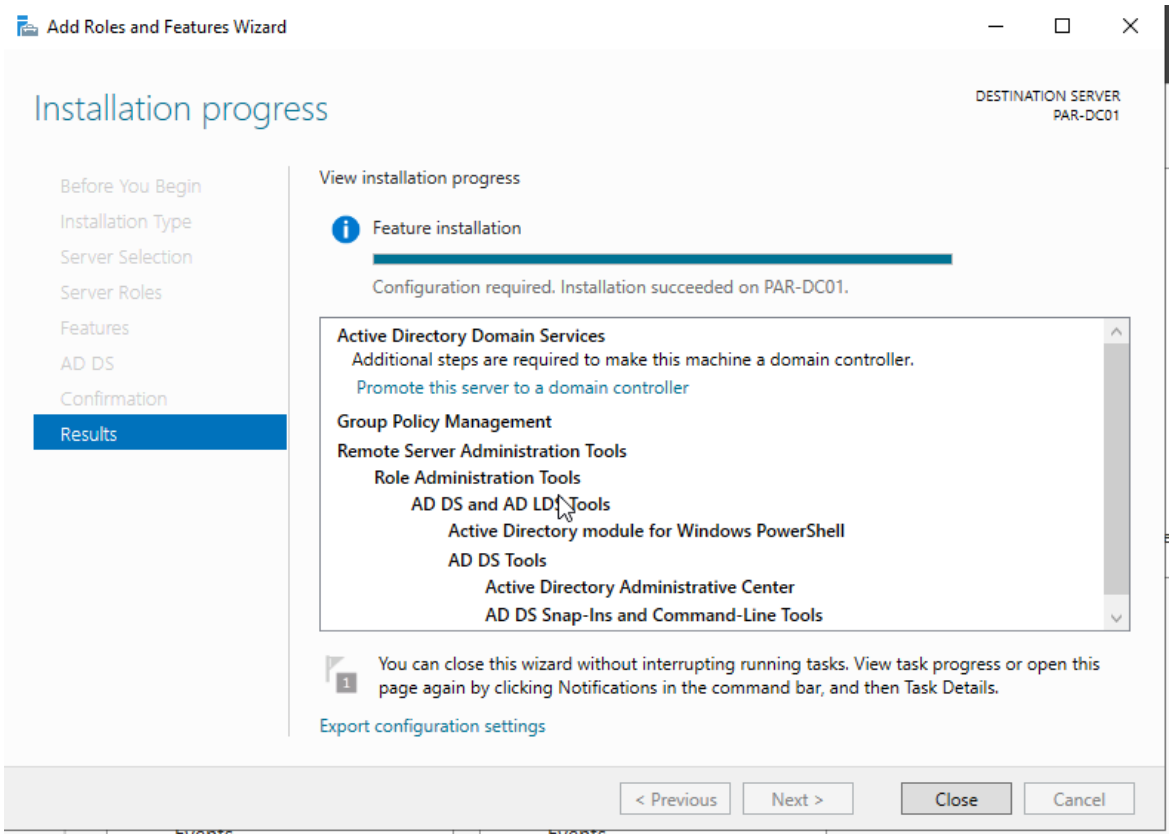


Installation du Rôle AD DS

Le rôle Active Directory Domain Services (AD DS) a été installé via le gestionnaire de serveur. Cette étape déploie les binaires nécessaires à la gestion de l'annuaire sans toutefois activer le service ni créer le domaine à ce stade.



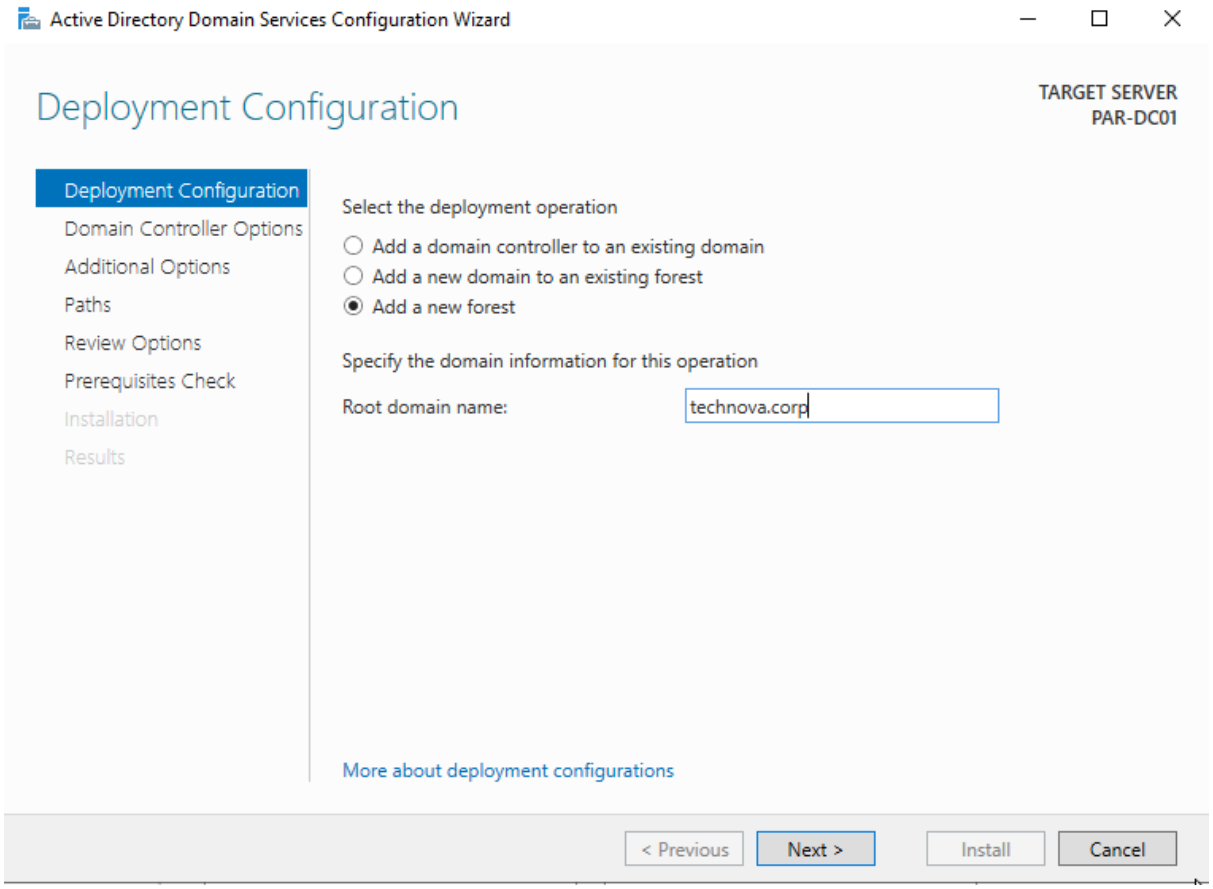
Une fois l'installation des fichiers terminée, le processus de promotion a été initié via le lien "Promote this server to a domain controller".



Configuration du Déploiement et Création de la Forêt

S'agissant du tout premier serveur de l'infrastructure, l'opération de déploiement choisie est : "Ajouter une nouvelle forêt".

- Nom de domaine racine (FQDN) : technova.corp

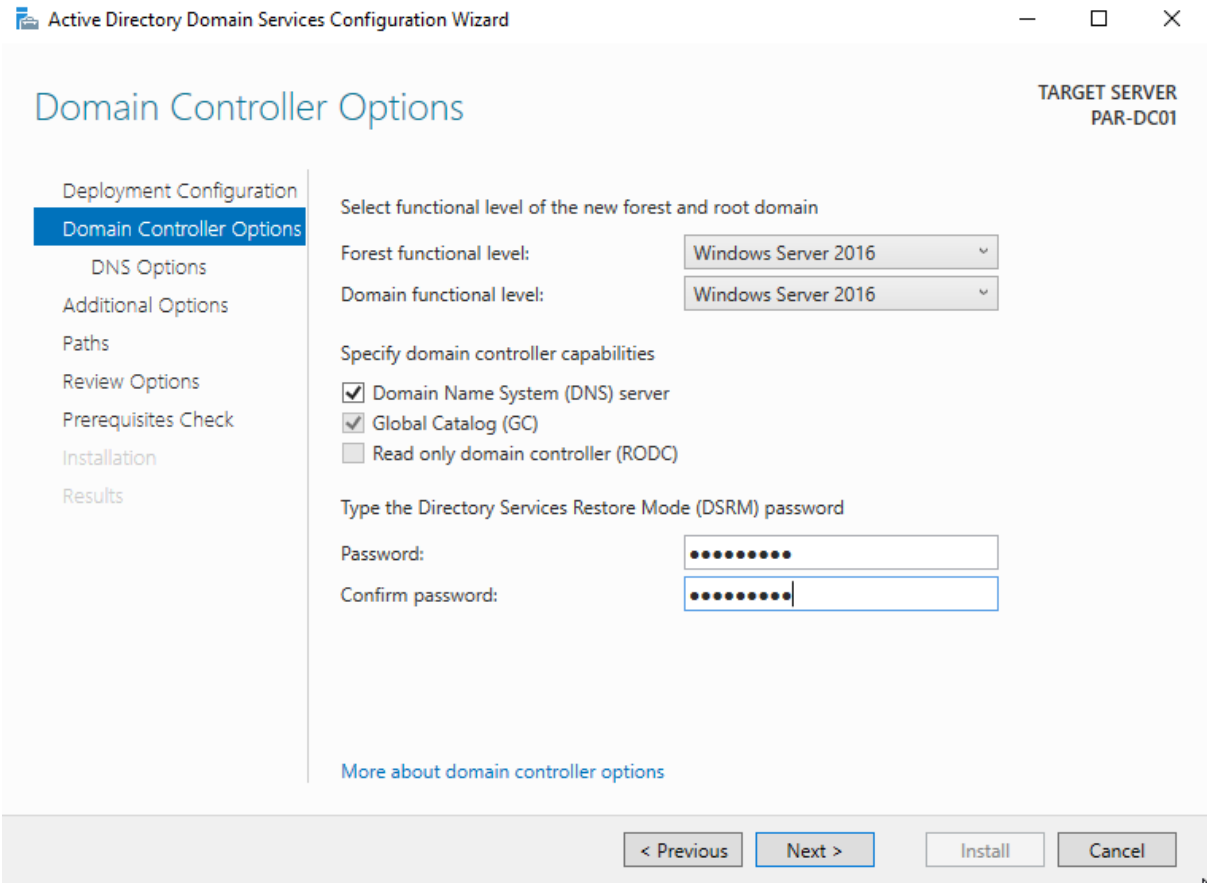


Options du Contrôleur de Domaine

La configuration technique du contrôleur a été définie avec les paramètres suivants :

- **Niveaux fonctionnels :** Le niveau fonctionnel de la forêt et du domaine a été fixé à **Windows Server 2016**. Ce choix assure un socle de fonctionnalités récent tout en maintenant une compatibilité standard.
- **Capacités du serveur :**
  - **Serveur DNS :** Intégré à l'AD pour la résolution de noms internes.
  - **Catalogue Global (GC) :** Indispensable pour stocker une réplique partielle de tous les objets de la forêt (coché par défaut pour le premier DC).

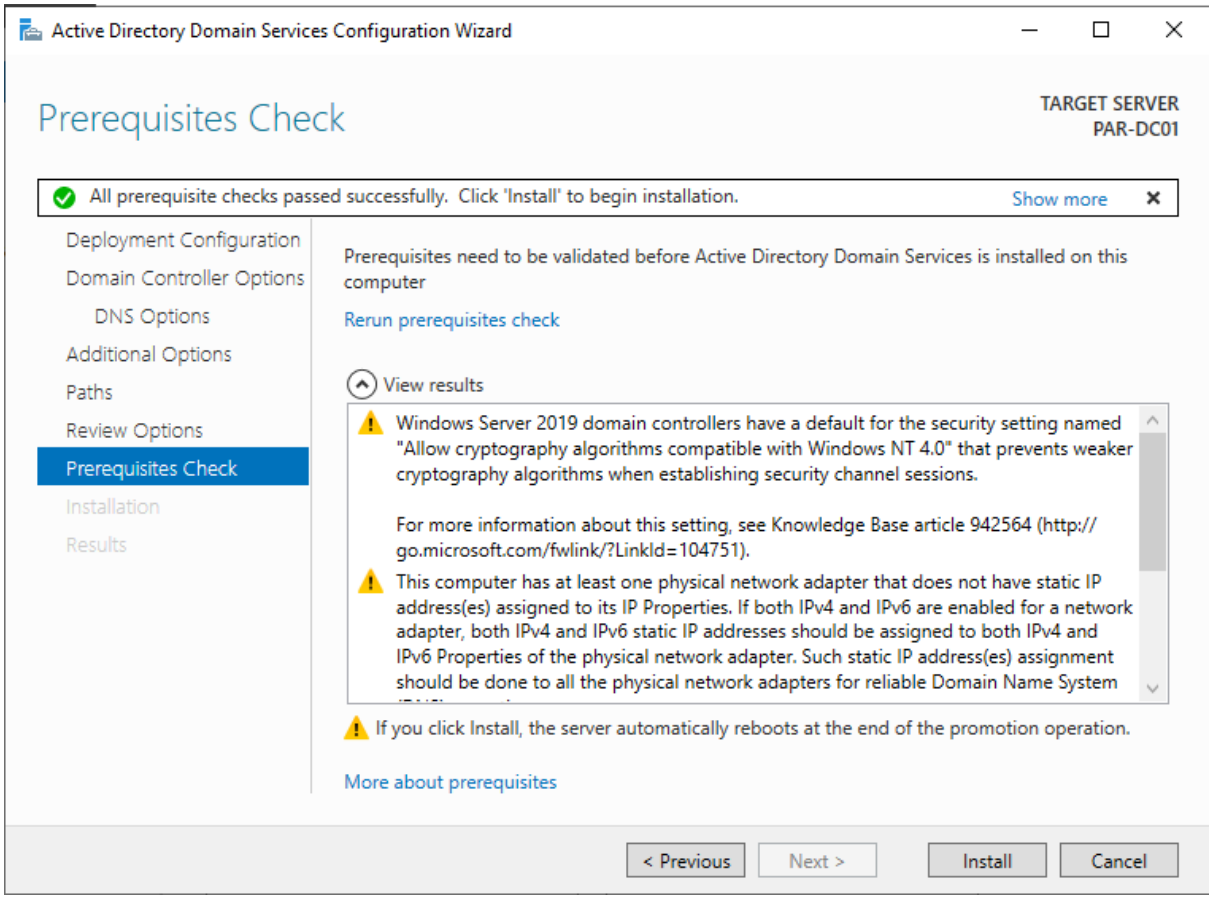
Mot de passe DSRM : Un mot de passe complexe a été défini pour le *Directory Services Restore Mode*, nécessaire en cas de restauration de l'annuaire hors ligne.



Finalisation et Validation

NetBIOS : Le nom NetBIOS généré automatiquement est TECHNOVA.

Vérification des prérequis : L'assistant a validé la conformité du serveur. Les avertissements affichés (concernant la cryptographie NT 4.0 et les interfaces réseau physiques) sont standards dans un contexte de virtualisation et n'ont pas bloqué l'installation.



Suite à cette validation, l'installation a été lancée, entraînant le redémarrage automatique du serveur pour finaliser sa promotion en tant que Contrôleur de Domaine.

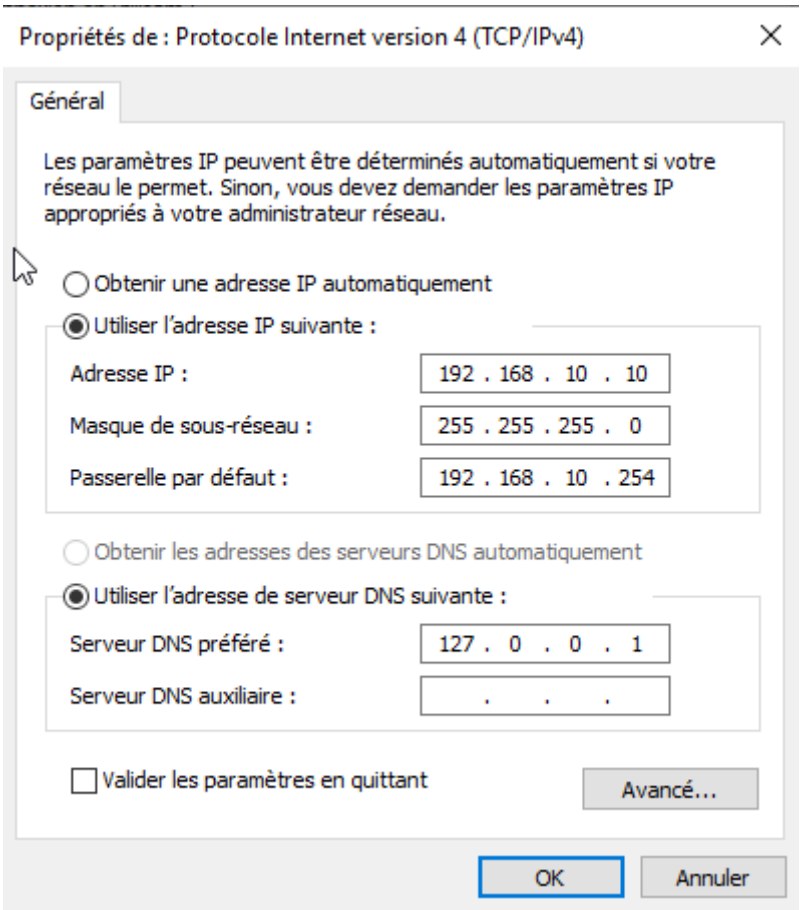
Validation de la Configuration Réseau (Post-Déploiement)

Suite au redémarrage du serveur nécessaire à sa promotion, la configuration TCP/IP a été validée définitivement. L'attribution d'une adresse IP statique est impérative pour garantir la disponibilité des services d'authentification et de résolution de noms pour l'ensemble du réseau.

Les paramètres appliqués sur l'interface réseau de PAR-DC01 sont les suivants :

Paramètre	Valeur	Description
Adresse IP	192.168.10.10	IP fixe du contrôleur de domaine principal.

Masque	255.255.255.0	Masque de sous-réseau standard (/24).
Passerelle	192.168.10.254	IP du routeur/pare-feu de sortie.
DNS Préféré	127.0.0.1	Adresse de bouclage (*loopback*). Le serveur s'interroge lui-même, hébergeant désormais la zone DNS du domaine technova.corp.

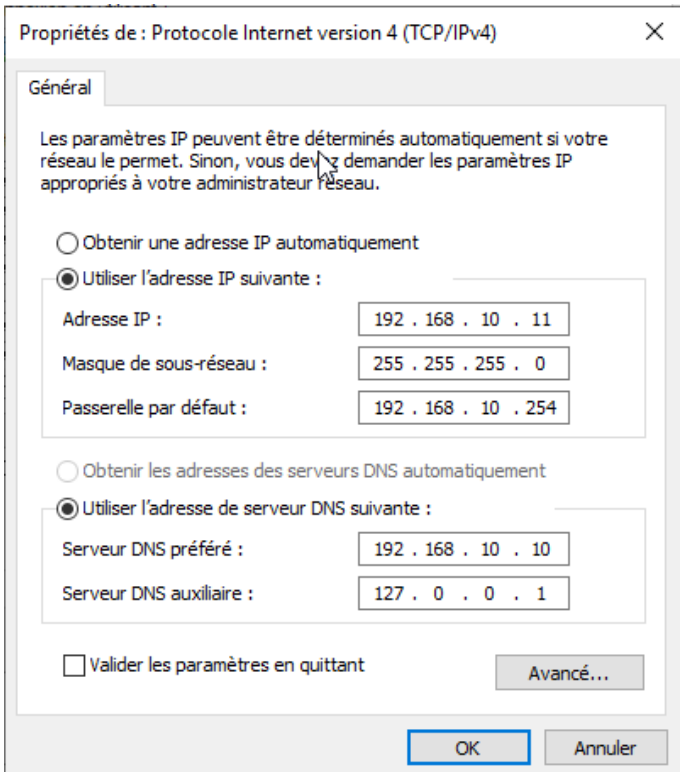


Mise en place de la Haute Disponibilité (PAR-DC02)

Afin d'assurer la résilience du service d'annuaire et la tolérance aux pannes, un second contrôleur de domaine, nommé PAR-DC02, a été déployé. Cette redondance garantit que l'authentification et la résolution DNS restent fonctionnelles même en cas d'indisponibilité du serveur principal.

Configuration Réseau et Pré-requis DNS

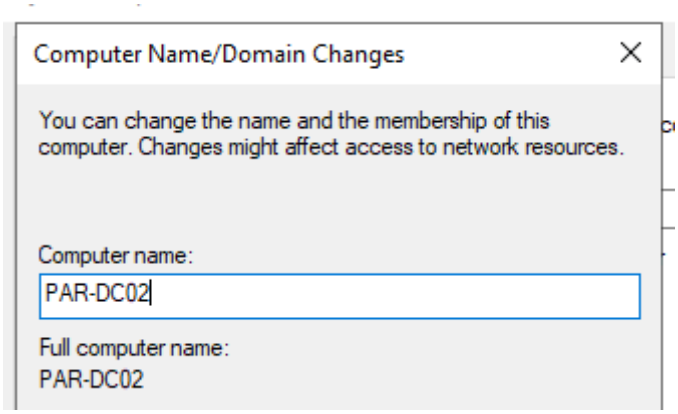
Contrairement au premier serveur, la configuration réseau de ce second nœud nécessite un paramétrage DNS spécifique pour lui permettre de joindre le domaine existant.
Comme illustré par les tests de connectivité (commande ping technova.corp), la résolution de nom est fonctionnelle grâce au pointage vers PAR-DC01.

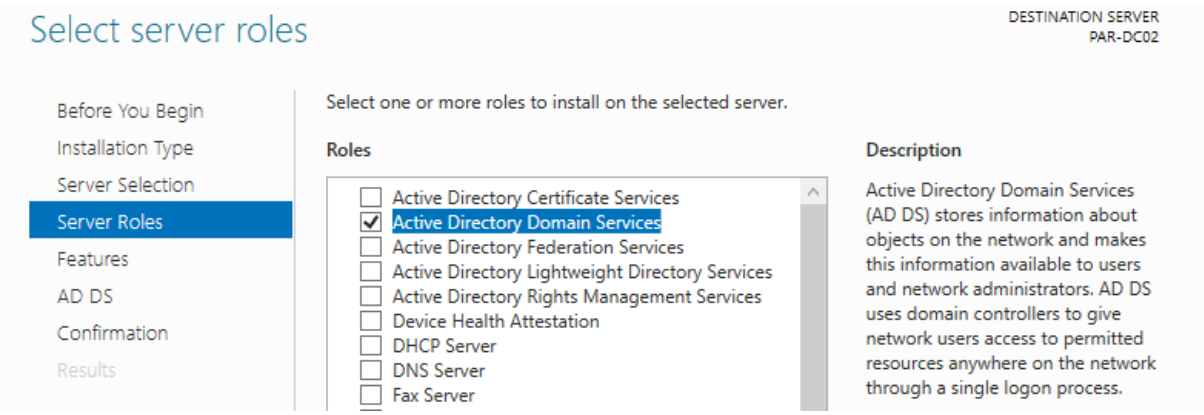



```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter #2
   Physical Address. . . . . . . . . : 08-00-27-44-16-5A
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.10.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DNS Servers . . . . . . . . . . . : 192.168.10.10
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Administrator>ping technova.corp

Pinging technova.corp [192.168.10.10] with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128
Reply from 192.168.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Préparation du Serveur

Avant l'installation des rôles, le serveur a été renommé PAR-DC02 pour respecter la convention de nommage, puis le rôle AD DS a été installé via le gestionnaire de serveur, de manière identique au premier nœud.

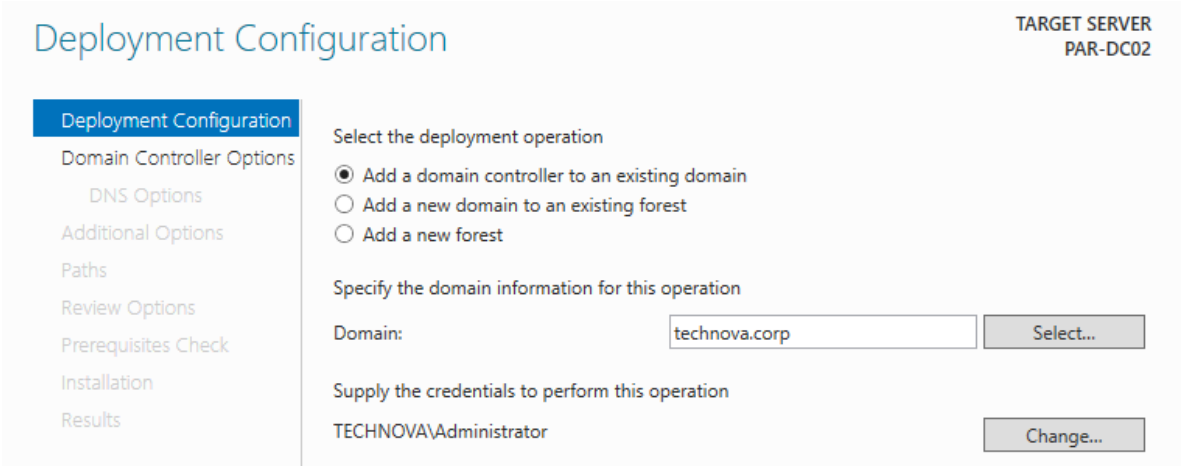




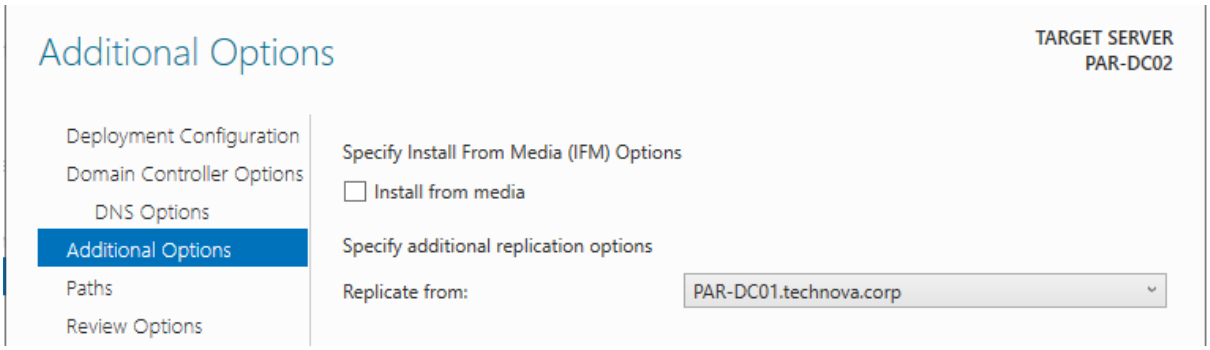
Promotion et Réplication

L'assistant de configuration a été lancé avec des paramètres spécifiques pour intégrer l'infrastructure existante :

- Opération de déploiement : Sélection de l'option "Ajouter un contrôleur de domaine à un domaine existant".
- Domaine cible : technova.corp.
- Identifiants : L'opération a été validée avec le compte Administrateur du domaine (TECHNOVA\Administrator).

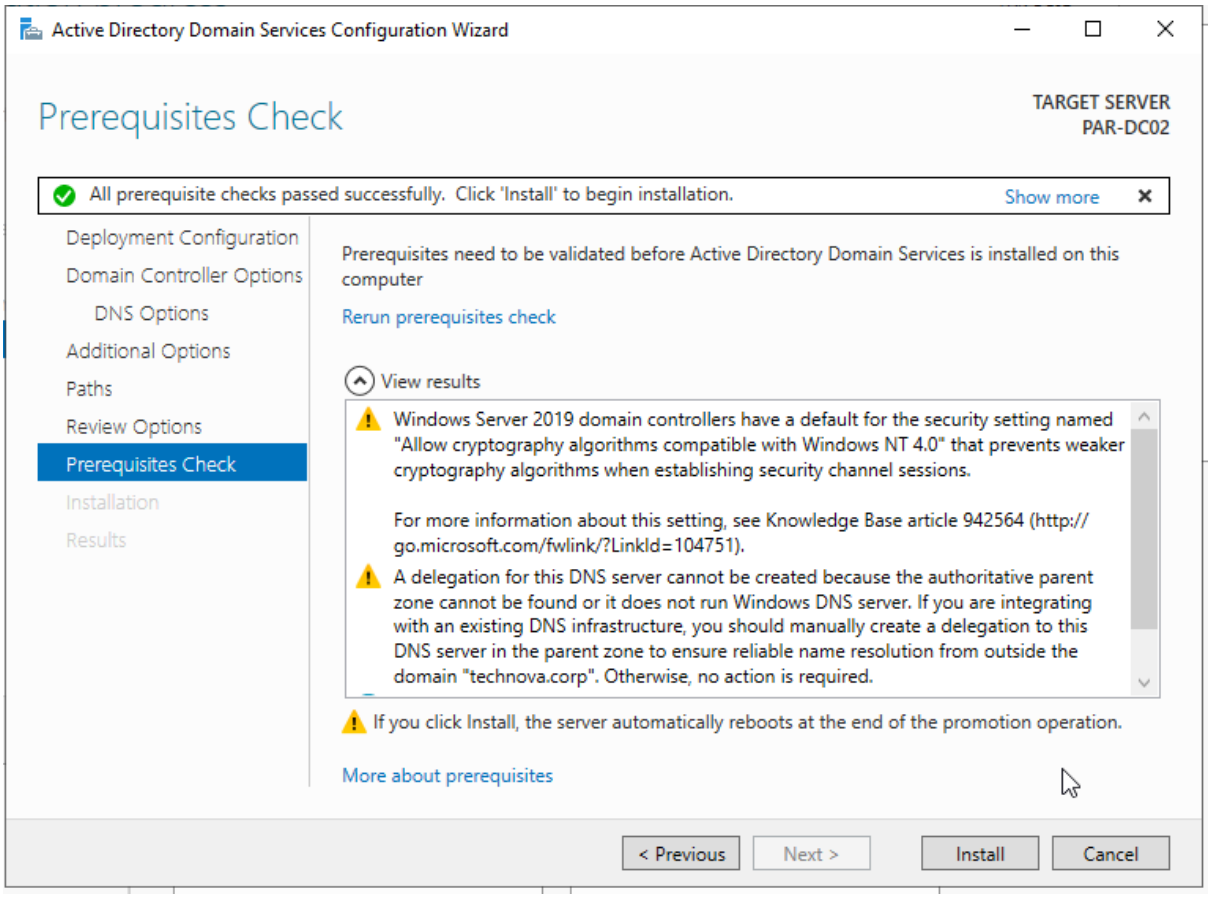


Stratégie de Réplication :
Lors de la configuration des options supplémentaires, le serveur PAR-DC01.technova.corp a été explicitement désigné comme partenaire de réplication initial (Replicate from). Cela permet de forcer la synchronisation initiale de la base de données Active Directory (NTDS.dit) et du dossier SYSVOL depuis le contrôleur racine validé.



Validation

Les vérifications de pré-requis ont confirmé que le serveur était prêt pour la promotion. Après l'installation et le redémarrage automatique, PAR-DC02 est devenu un contrôleur de domaine opérationnel, participant activement à la répartition de charge.



Déploiement de la Station d'Administration Sécurisée (PAW)

Dans une optique de sécurisation de l'Active Directory (modèle Tiering), l'administration des contrôleurs de domaine ne doit jamais se faire directement depuis les serveurs eux-mêmes, ni depuis un poste utilisateur standard.

Une station dédiée, nommée PAW (Privileged Access Workstation), a été déployée pour effectuer toutes les tâches de gestion sensibles.

Stratégie de Déploiement (Template Proxmox)

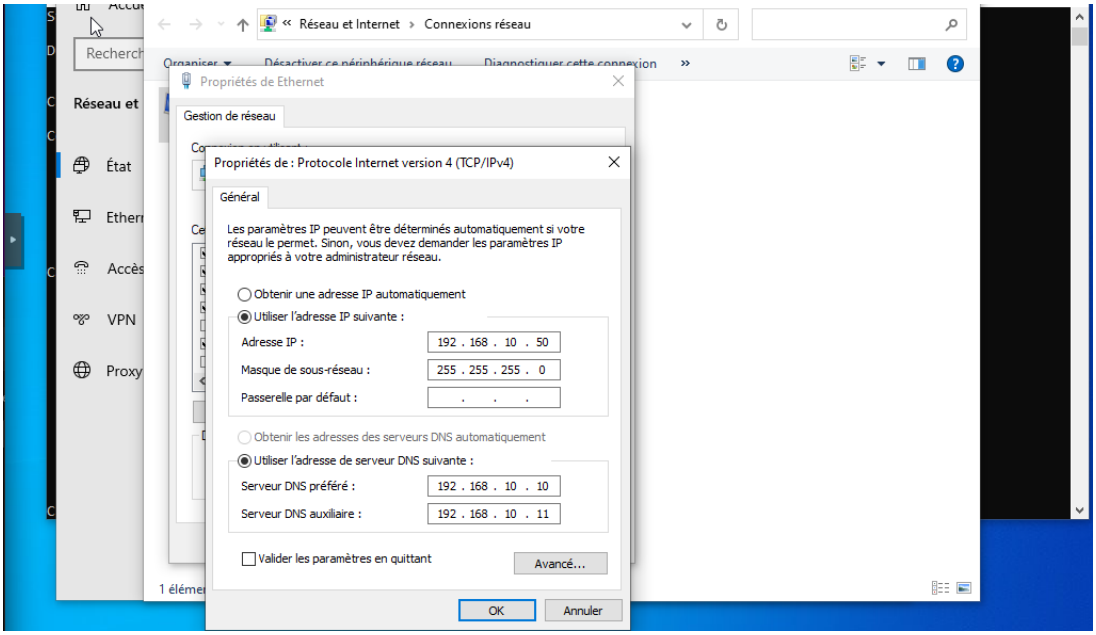
Afin d'optimiser le déploiement des postes clients (PAW et futurs PC utilisateurs) et de garantir une base saine, une stratégie de "Master Image" a été adoptée sur l'hyperviseur Proxmox :

1. Installation d'une machine virtuelle Windows 10 Pro.
2. Application de l'ensemble des mises à jour de sécurité Windows Update.
3. Exécution de l'outil Sysprep (System Preparation) pour généraliser l'installation (suppression des identifiants uniques de sécurité - SID, nettoyage des pilotes).
4. Conversion de la VM en Template Proxmox.

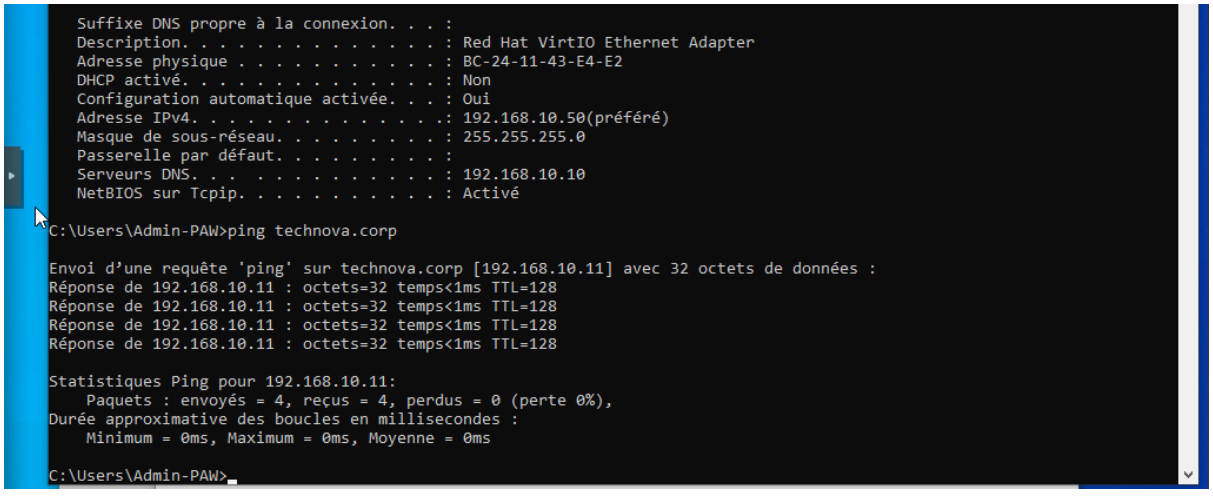
La machine PAR-PAW01 est donc un clone lié (linked clone) issu de ce template, assurant un déploiement rapide et standardisé.

Configuration Réseau et Connectivité

Une fois la machine instanciée, une configuration réseau statique a été appliquée pour garantir sa joignabilité et la résolution DNS vers l'infrastructure AD.

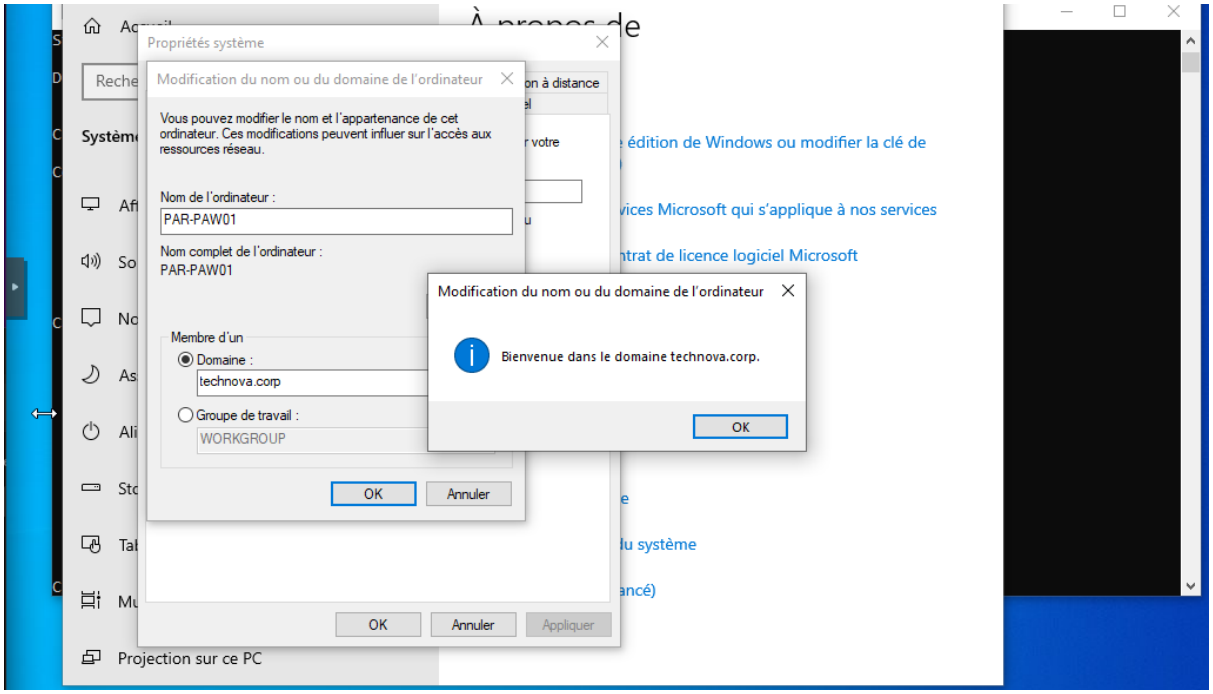


Des tests de connectivité (Ping) vers le nom de domaine technova.corp ont validé que la résolution de noms et le routage vers les deux contrôleurs de domaine étaient fonctionnels.



Identité et Jonction au Domaine

La machine a été renommée PAR-PAW01 pour respecter la charte de nommage du site de Paris. Elle a ensuite été intégrée au domaine technova.corp. Le message de bienvenue confirme l'établissement de la relation d'approbation entre la station et le domaine.



Installation des Outils d'Administration (RSAT)

Pour permettre l'administration à distance des serveurs, les fonctionnalités optionnelles RSAT (Remote Server Administration Tools) ont été installées sur la PAW. Les consoles suivantes sont désormais disponibles localement sur le poste :

- AD DS et AD LDS Tools : Pour la gestion des utilisateurs et ordinateurs.
- Group Policy Management Tools : Pour la gestion des GPO.
- DNS Server Tools : Pour la gestion des zones DNS.

Audit de Sécurité Initial et Remédiations (PingCastle)

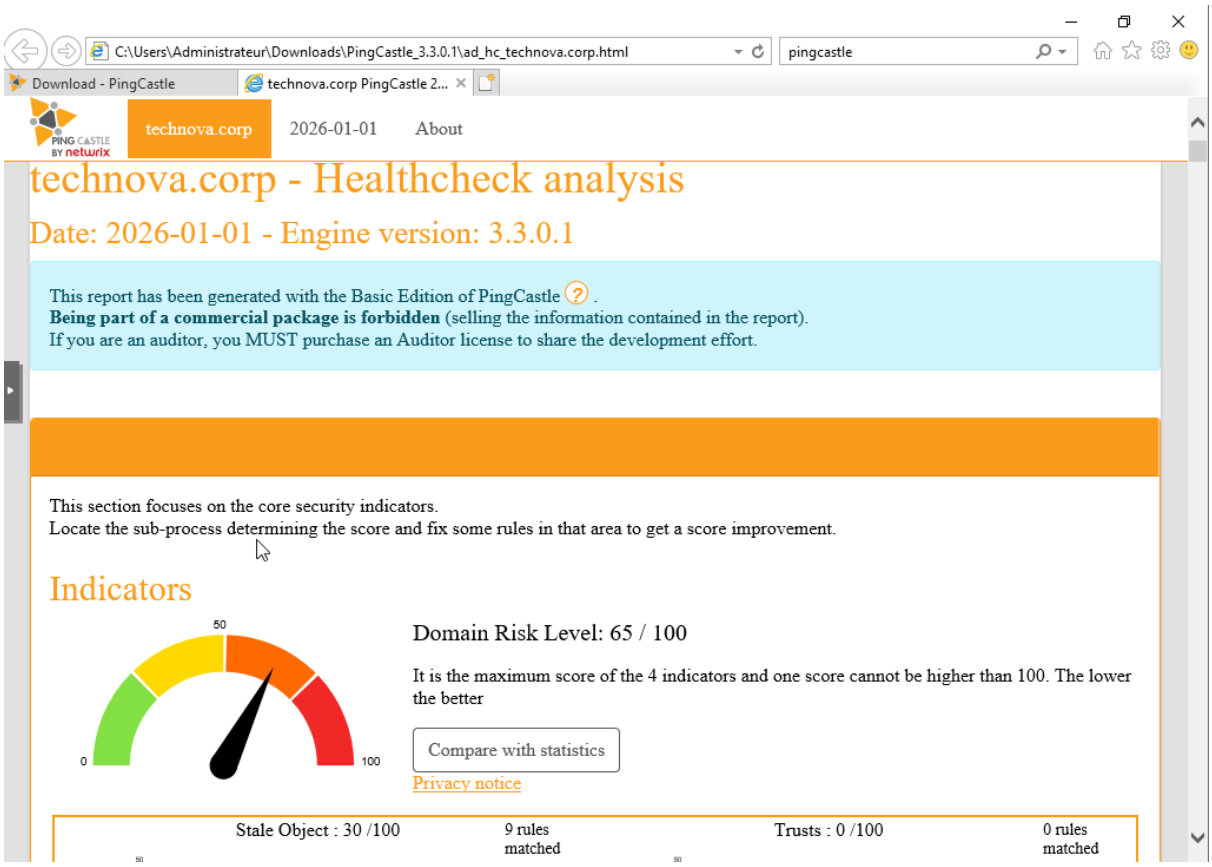
Une fois l'infrastructure de base opérationnelle (Contrôleurs de Domaine et PAW), une phase d'audit de sécurité a été initiée avant toute mise en production. L'objectif est d'identifier et de corriger les configurations par défaut de Microsoft qui présentent des risques de sécurité.

Méthodologie et Premier Scan

L'outil choisi pour cet audit est PingCastle. Il permet d'établir une cartographie des risques de l'Active Directory via un score de santé (Healthcheck Score). Plus le score est élevé, plus le risque est critique.

- Objectif : Réduire le score de risque initial pour tendre vers 0 (Risque nul).
- Préparation pour le Durcissement : Cet état des lieux est un prérequis indispensable avant l'application de scripts de durcissement plus agressifs (type HardenAD ou recommandations ANSSI).

Le premier scan a été lancé depuis la station d'administration (PAW) pour évaluer l'état "Sortie de boîte" (Out-of-the-box) de l'installation.



Analyse des Risques et Remédiations

Le premier rapport généré par PingCastle a mis en évidence un score de risque de 65/100 pour le domaine technova.corp. Ce résultat, bien que sur une installation neuve, démontre que les configurations par défaut de Microsoft privilégient la compatibilité ascendante plutôt

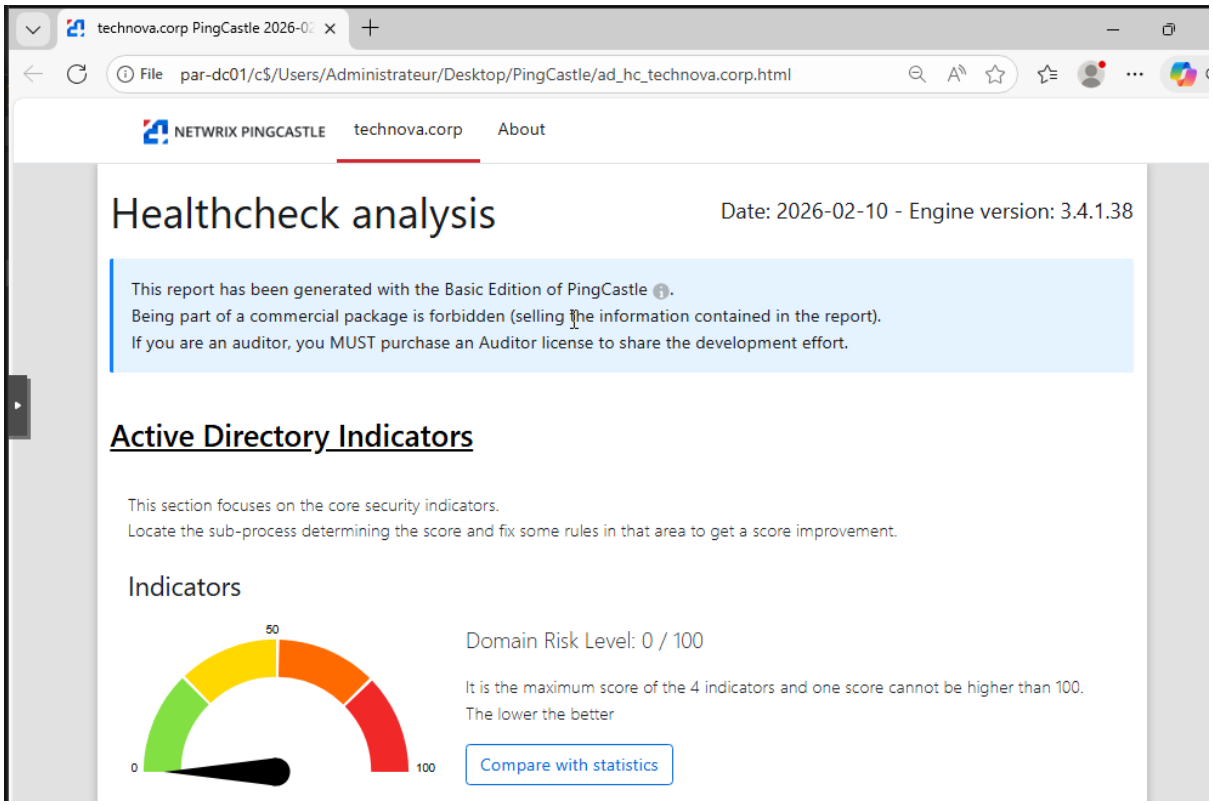
que la sécurité immédiate. Exemples de vulnérabilités corrigées : Sans entrer dans le détail exhaustif de chaque règle modifiée, les remédiations ont porté sur des "mauvaises pratiques" standards présentes nativement sur Windows Server :

- Activation de la Corbeille AD : Fonctionnalité inactive par défaut, pourtant critique pour la résilience en cas de suppression accidentelle d'objets.
- Désactivation du service Spouleur d'impression (Print Spooler) : Ce service, actif par défaut sur les contrôleurs de domaine, est un vecteur d'attaque majeur (ex: PrintNightmare). Il a été désactivé sur tous les DC.
- Protocole SMBv1 : Désactivation explicite de ce protocole obsolète et vulnérable aux ransomwares.
- Sécurisation des comptes à privilèges : Révision des délégations et protection contre les modifications accidentelles.

Validation Post-Remédiation

Suite à cette campagne de nettoyage, un second scan a été exécuté pour valider l'efficacité des mesures. Comme l'illustre le rapport de contrôle, le Domain Risk Level est désormais retombé à 0/100.

Cet état "propre" fournit une base saine et maîtrisée. L'infrastructure est désormais prête à recevoir des durcissements beaucoup plus stricts et granulaires via l'outil HardenAD, sans risque de confusions entre des erreurs de configuration basiques et des restrictions de sécurité avancées.



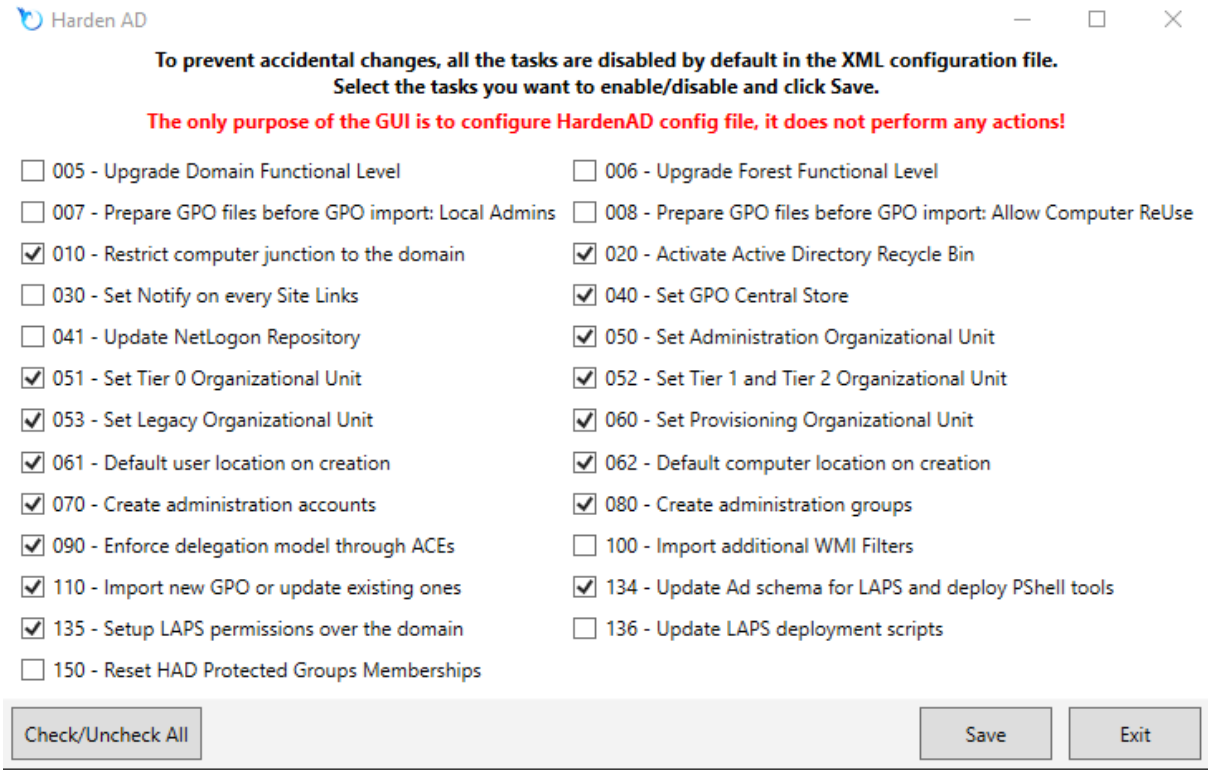
Durcissement Avancé et Modèle de Tiering (HardenAD)

Après avoir assaini les configurations par défaut, la sécurisation de l'infrastructure est passée à une étape supérieure avec le déploiement de la solution HardenAD. Cet outil a pour but d'instaurer une architecture basée sur le modèle de Tiering de Microsoft, visant à créer des zones de sécurité étanches pour empêcher les mouvements latéraux et l'escalade de privilèges.

Configuration et Déploiement

HardenAD agit comme une solution d'**Infrastructure as Code**, permettant de définir la posture de sécurité souhaitée de manière programmatique avant son application effective. Comme illustré par la capture de l'interface de configuration, une sélection rigoureuse de modules a été opérée pour constituer le socle de sécurité de l'infrastructure **technova.corp**:

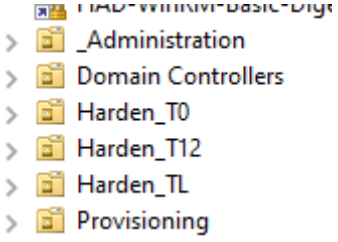
- **Restructuration de l'Annuaire (Modèle de Tiering) :** L'outil automatise la création d'une arborescence d'Unités d'Organisation (OU) étanches. Les options sélectionnées (**051, 052, 053**) permettent de séparer physiquement les actifs de **Tier 0** (systèmes critiques), de **Tier 1 et 2** (serveurs métiers et postes de travail), tout en isolant les objets hérités (*Legacy*).
- **Contrôle des Emplacements par Défaut :** Afin d'éviter que de nouveaux objets ne soient créés dans les conteneurs natifs non sécurisés, les modules **061** et **062** ont été activés. Ils redirigent automatiquement tout nouvel utilisateur ou ordinateur vers des conteneurs sécurisés et contrôlés.
- **Modèle de Délégation et Durcissement :** L'application du principe du moindre privilège est assurée par l'option **090**, qui impose un modèle de délégation strict via des entrées de contrôle d'accès (ACE) sur les objets de l'annuaire. De plus, la corbeille Active Directory est activée (**020**) pour garantir la résilience des données.
- **Gestion des Stratégies de Groupe (GPO) :** La sécurisation des politiques passe par la mise en place d'un magasin central (**040**) et l'importation de GPO durcies (**110**), assurant une application homogène des paramètres de sécurité sur l'ensemble du parc.
- **Intégration de LAPS (Local Administrator Password Solution) :** Les options **134** et **135** ont été cochées pour mettre à jour le schéma Active Directory et déployer les outils nécessaires à la gestion dynamique et sécurisée des mots de passe des administrateurs locaux.
- **Sécurisation des Jonctions au Domaine :** L'option **010** limite la capacité de joindre de nouvelles machines au domaine aux seuls comptes autorisés, bloquant ainsi un vecteur classique d'intrusion.



Nouvelle Architecture de l'Annuaire

Suite à l'exécution du script, la structure de l'Active Directory a été profondément remaniée pour refléter la séparation des pouvoirs. L'arborescence visible dans la console de gestion se décompose désormais ainsi :

- Harden_T0 (Tier 0) : Zone critique contenant les administrateurs du domaine et les contrôleurs de domaine. C'est le cœur de la confiance.
- Harden_T12 : Zone regroupant les serveurs d'application et les postes de travail (et leurs administrateurs respectifs), isolée du Tier 0.
- _Administration : OU dédiée aux comptes et groupes de gestion, strictement contrôlée par les délégations HardenAD.
- Provisioning : Zone tampon pour les nouveaux objets avant leur classement définitif.



Validation de la Conformité (Contre-Audit)

L'application de restrictions aussi fortes pouvant impacter le fonctionnement du domaine, une phase de vérification a été réalisée immédiatement après le déploiement. Un nouvel audit PingCastle a été exécuté pour s'assurer que :

1. Les nouvelles configurations n'ont pas introduit de régressions ou de nouvelles vulnérabilités.
2. Le score de risque du domaine se maintient à 0/100.

Ce maintien du score confirme que l'implémentation du Tiering s'est faite sur des bases saines.

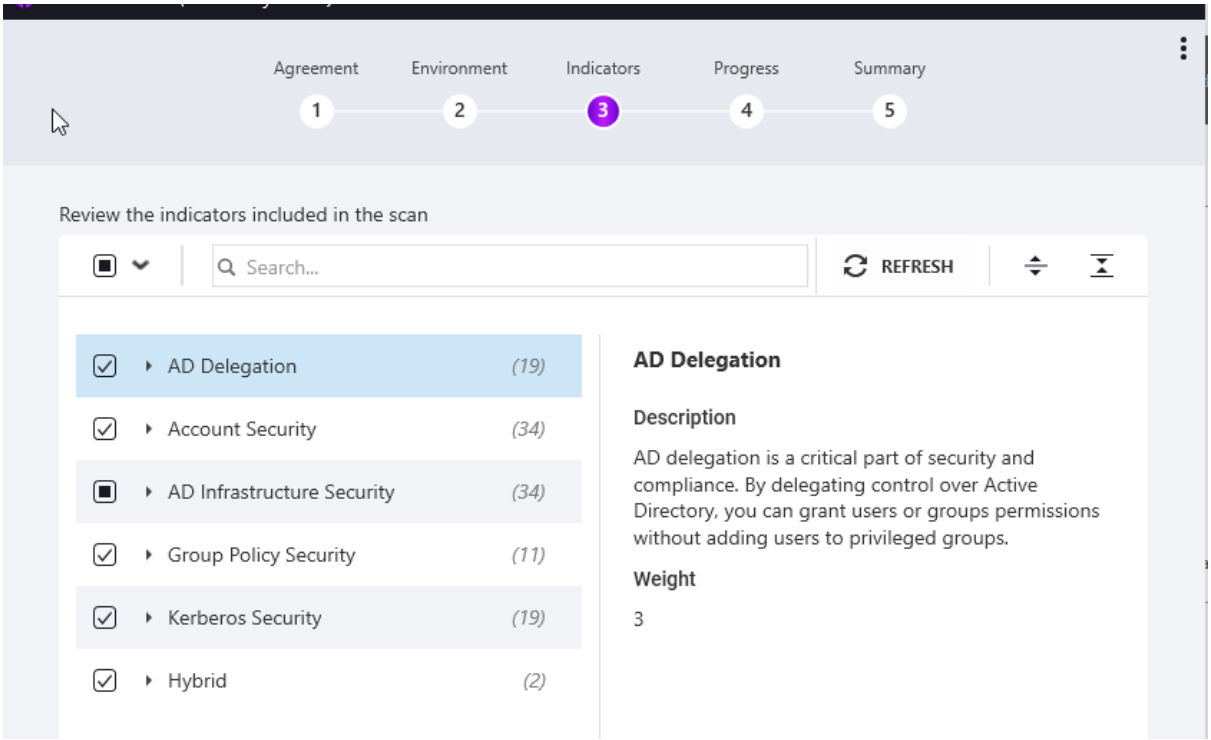
Validation Finale : Audit de Posture (Purple Knight)

Afin de compléter la vision sanitaire fournie par PingCastle, un audit de sécurité complémentaire a été réalisé avec Purple Knight. Si PingCastle excelle dans l'hygiène de l'AD, Purple Knight se concentre davantage sur la détection d'Indicateurs d'Exposition (IOEs) et de scénarios d'attaques complexes (chemins d'attaque, faiblesse Kerberos, délégations abusives).

Périmètre de l'analyse

L'audit a été configuré pour scanner l'intégralité du domaine technova.corp en ciblant des catégories critiques :

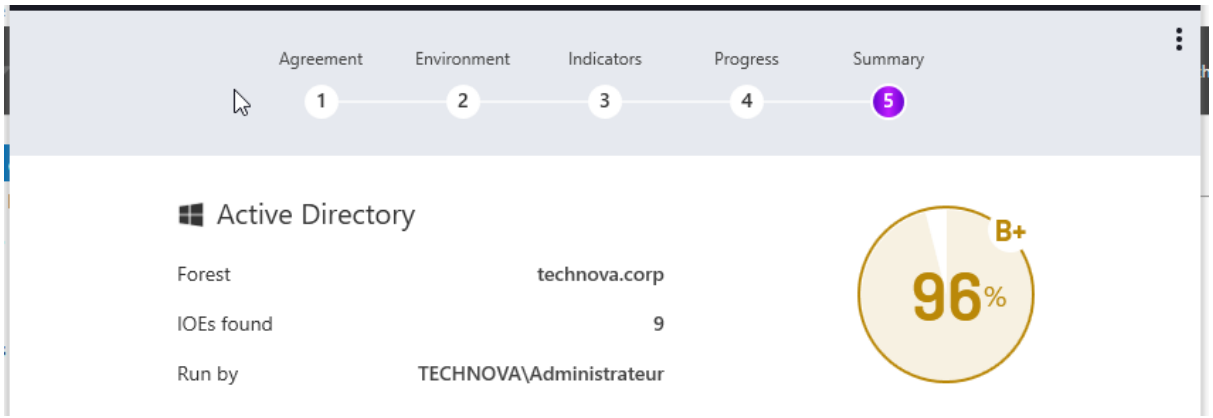
- AD Delegation : Vérification des permissions dangereuses.
- Account Security : Analyse des comptes à privilèges.
- AD Infrastructure Security : Sécurité des contrôleurs de domaine.
- Kerberos Security : Détection de faiblesses type Kerberoasting ou chiffrement faible



Résultats et Score de Sécurité

Le rapport final attribue au laboratoire un score de sécurité de 96% (Grade B+).

Ce résultat très élevé confirme l'efficacité du durcissement opéré par le script HardenAD et les remédiations précédentes. L'infrastructure présente une posture de sécurité robuste, largement supérieure aux standards par défaut.



Analyse des Alertes Résiduelles (Limites Temporelles)

Il est important de noter qu'atteindre le score théorique de 100% est techniquement impossible dans le contexte d'un déploiement récent ("Lab"). Les 4% de pénalités restantes correspondent exclusivement à des alertes liées à la fraîcheur de l'installation et non à des défauts de configuration.

Comme le montrent les détails du rapport, les avertissements (Warnings) concernent :

- "Recent privileged account creation activity" : Création récente de comptes admin.
- "Changes to privileged group membership in the last 7 days" : Peuplement initial des groupes d'administration.
- "Built-in domain Administrator account used within the last two weeks" : Utilisation inévitable du compte Administrateur pour l'installation initiale.
- "AD objects created within the last 10 days": Création de l'infrastructure elle-même.

Ces alertes sont des artefacts temporels. Elles ne nécessitent aucune action corrective et disparaîtront d'elles-mêmes une fois que l'environnement sera entré en phase d'exploitation (RUN) et que la période de "nouveauté" sera écoulée.

Extension du Périmètre et Gestion Granulaire des Accès

Afin de préserver la concision de cette annexe technique, la documentation détaillée s'est concentrée sur le déploiement du cœur de l'infrastructure au siège (Paris). Il est toutefois impératif de souligner que le laboratoire a été étendu pour simuler une véritable architecture d'entreprise multi-sites, incluant la création du site de Lyon.

Déploiement du Site Secondaire (Lyon)

Bien que non illustrée par des captures d'écran dans ce rapport, l'infrastructure du site de Lyon a été déployée suivant les mêmes standards de rigueur que le siège :

- Infrastructure AD : Ajout d'un contrôleur de domaine en lecture/écriture (RWDC) pour assurer l'authentification locale et la réplication inter-sites.
- Postes Clients : Déploiement d'une PAW dédiée à l'administration locale et d'un poste utilisateur standard, reproduisant le modèle de gestion du siège.

Stratégies de Groupe (GPO) et Sécurité des Données

Concernant l'application des stratégies de groupe, l'approche s'est faite en deux temps :

1. **Sécurité du Système (Socle) :** Comme détaillé précédemment, la sécurité structurelle de l'AD (Tiering, durcissement OS) est assurée par les GPO générées et maintenues par le framework HardenAD.

Sécurité des Données (Fonctionnel) : Des GPO manuelles spécifiques ont été ajoutées pour la gestion des partages de fichiers. Une attention particulière a été portée à la configuration du partage "Données R&D" du site de Lyon. Des règles strictes d'accès et de mappage de lecteurs ont été configurées pour garantir que seules les équipes autorisées puissent accéder à ces données sensibles, illustrant la capacité à gérer la confidentialité au-delà de la simple sécurité de l'annuaire.

Conclusion Annexe : Mise en œuvre du Laboratoire Active Directory (Siège Paris)

La mise en œuvre de ce laboratoire a permis de construire une infrastructure Active Directory simulant fidèlement les exigences d'un environnement de production critique. L'approche adoptée, résolument orientée vers le "Security by Design", démontre qu'il est possible de concilier opérabilité et robustesse dès les premières phases de déploiement.
Les travaux présentés dans cette annexe mettent en exergue trois piliers fondamentaux :

1. **La Résilience de l'Architecture :** L'utilisation de la virtualisation Proxmox et le déploiement de contrôleurs de domaine redondants assurent la haute disponibilité des services d'annuaire (Authentification, DNS), indispensable à la continuité d'activité du siège et des sites distants.
2. **Le Cloisonnement des Privilèges (Tiering) :** L'application stricte du modèle de Tiering via HardenAD et l'usage exclusif de stations d'administration sécurisées (PAW) constituent la réponse technique aux menaces modernes (mouvements latéraux, ransomwares). L'administration du domaine ne repose plus sur la confiance implicite, mais sur des barrières logiques étanches.
3. **La Validation Continue par l'Audit :** L'intégration d'outils d'audit (PingCastle, Purple Knight) au cœur du cycle de déploiement a permis d'éliminer la dette technique native de Microsoft. Les scores obtenus (Risque 0/100 et Score de Sécurité 96%) attestent objectivement de la qualité du durcissement.

En conclusion, si cette annexe s'est concentrée sur le socle technique du siège (Paris), elle pose les fondations saines nécessaires à l'extension vers le site de Lyon et à l'intégration des services utilisateurs. L'infrastructure technova.corp est désormais prête à passer en phase d'exploitation avec une surface d'attaque réduite au strict minimum.

Procédure de création d'un VPN IPsec

- Étape 1 : Création des objets (Sur Site A et Site B)
    - Prérequis :
        - Choisir les adresses IP publique des deux firewalls
        - Lister toutes les adresses des sous réseaux pour chaque site
        - Créer une clé partagée PSK
    - Définir les éléments suivants sur les deux firewalls :
        - Objet “Machine” => Adresse IP publique du firewall distant (WAN_Site_A et WAN_Site_B)

- Objet “Réseau” => Adresses IP du LAN (LAN_Site_A et LAN_Site_B)
- Objet “Réseau” => Adresse IP du LAN distant (LAN_Site_A et LAN_Site_B)

- Étape 2 : Configuration du VPN IPsec (Configuration > VPN > VPN IPsec > Politique IPsec)
  - Sur le Site A :
    - Onglet Correspondants (Ajouter > Correspondant site à site)
      - Nom : VPN_Vers_Site_B
      - Version IKE : IKEv2
      - Passerelle distante : objet WAN_Site_B.
      - Certificat / Clé partagée : Cochez "Clé pré-partagée (PSK)" en texte clair et entrez votre clé.
      - Profils IKE/IPsec : Laissez les profils par défaut (Strong ou Good), mais assurez-vous de choisir strictement les mêmes sur le Site B.
    - Onglet Trafic : Ajouter VPN_Vers_Site_B
      - Réseau local : LAN_Site_A.
      - Réseau distant : LAN_Site_B.
      - Activer la politique et Sauvegarder.
  - Sur le Site B : Répétez la procédure en inversant les rôles (Passerelle distante = WAN_Site_A, Réseau local = LAN_Site_B, Réseau distant = LAN_Site_A). Utilisez la même PSK et les mêmes profils.

- Étape 3 : Autoriser le trafic (Règles de filtrage)
  - Configuration > Politique de sécurité > Filtrage
  - Autoriser le montage du VPN (WAN vers WAN) :
    - État : ON
    - Action : pass
    - Source : WAN_Site_B
    - Destination : Firewall_out (objet natif représentant l'IP WAN locale)
    - Port de destination : ipsec (groupe natif contenant UDP 500, UDP 4500 et ESP)
  - Autoriser le trafic métier (LAN vers LAN) :
    - État : ON
    - Action : pass

        - Source : LAN_Site_A + LAN_Site_B (Mettre les deux permet au trafic d'aller dans les deux sens de manière symétrique).
        - Destination : LAN_Site_B + LAN_Site_A
        - Interface source : Toutes (ou IPsec et in)
        - Inspection : Laissez sur le profil d'inspection par défaut (ex: IPS_00).
    - Sauvegardez et appliquez la politique de filtrage.

- Étape 4 : Vérification et Monitoring

  Faire un ping depuis une machine du `LAN_Site_A` vers une machine du `LAN_Site_B`. Le tunnel devrait alors apparaître en vert dans le module de supervision des deux firewalls.

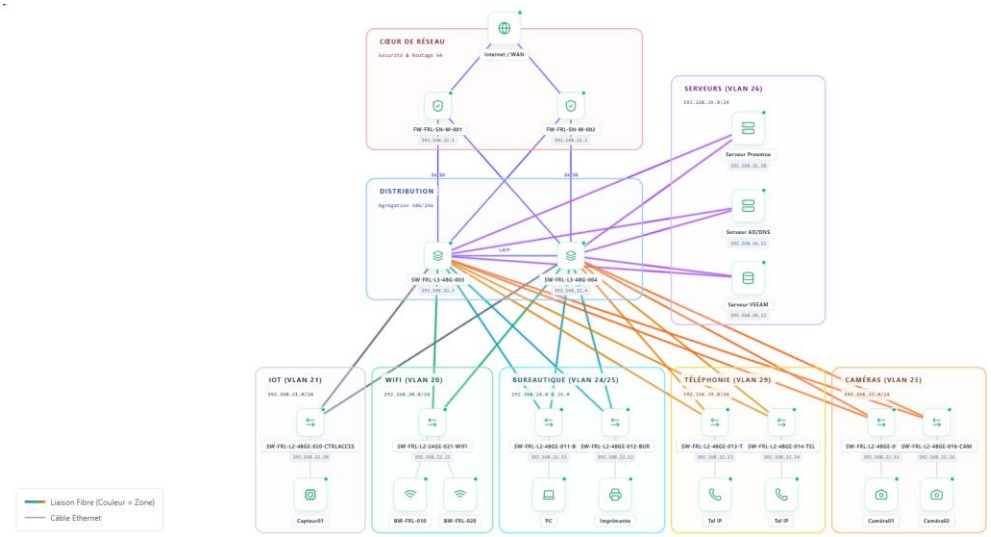
Plan d’adressage IP

Site	VLAN	Service	Sous réseaux
Tous	999	Trash	X
Paris	10	Wifi	192.168.10.0/24
Paris	11	IOT	192.168.11.0/24
Paris	12	Administration réseau	192.168.12.0/24
Paris	13	Caméras	192.168.13.0/24
Paris	14	Imprimantes	192.168.14.0/24
Paris	15	Bureautique	192.168.15.0/24
Paris	16	Serveurs (Datacenter)	192.168.16.0/24
Paris	17	DMZ (partenaire)	192.168.17.0/24
Paris	19	Téléphonie	192.168.19.0/24
Paris	**421**	**Natif**	**X**
Lyon	20	Wifi	192.168.20.0/24
Lyon	21	IOT	192.168.21.0/24
Lyon	22	Administration réseau	192.168.22.0/24
Lyon	23	Caméras	192.168.23.0/24
Lyon	24	Imprimantes	192.168.24.0/24
Lyon	25	Bureautique	192.168.25.0/24
Lyon	26	Serveurs (R&D)	192.168.26.0/24
Lyon	27	DMZ	192.168.27.0/24
Lyon	29	Téléphonie	192.168.29.0/24
Lyon	**120**	**Développement IOT**	**192.168.120.0/24**
Lyon	**422**	**Natif**	**X**
Lille	30	Wifi	192.168.30.0/24
Lille	31	IOT	192.168.31.0/24
Lille	32	Administration réseau	192.168.32.0/24
Lille	33	Caméras	192.168.33.0/24
Lille	34	Imprimantes	192.168.34.0/24
Lille	35	Bureautique	192.168.35.0/24
Lille	36	Serveurs	192.168.36.0/24
Lille	37	DMZ	192.168.37.0/24
Lille	39	Téléphonie	192.168.39.0/24
Lille	**423**	**Natif**	**X**
Barcelone	40	Wifi	192.168.40.0/24
Barcelone	41	IOT	192.168.41.0/24
Barcelone	42	Administration réseau	192.168.42.0/24
Barcelone	43	Caméras	192.168.43.0/24
Barcelone	44	Imprimantes	192.168.44.0/24
Barcelone	45	Bureautique	192.168.45.0/24
Barcelone	46	Serveurs (Cyber)	192.168.46.0/24
Barcelone	47	DMZ (logs externes et filiales)	192.168.47.0/24
Barcelone	49	Téléphonie	192.168.49.0/24
Barcelone	**140**	**Cluster**	**192.168.140.0/24**
Barcelone	**424**	**Natif**	**X**

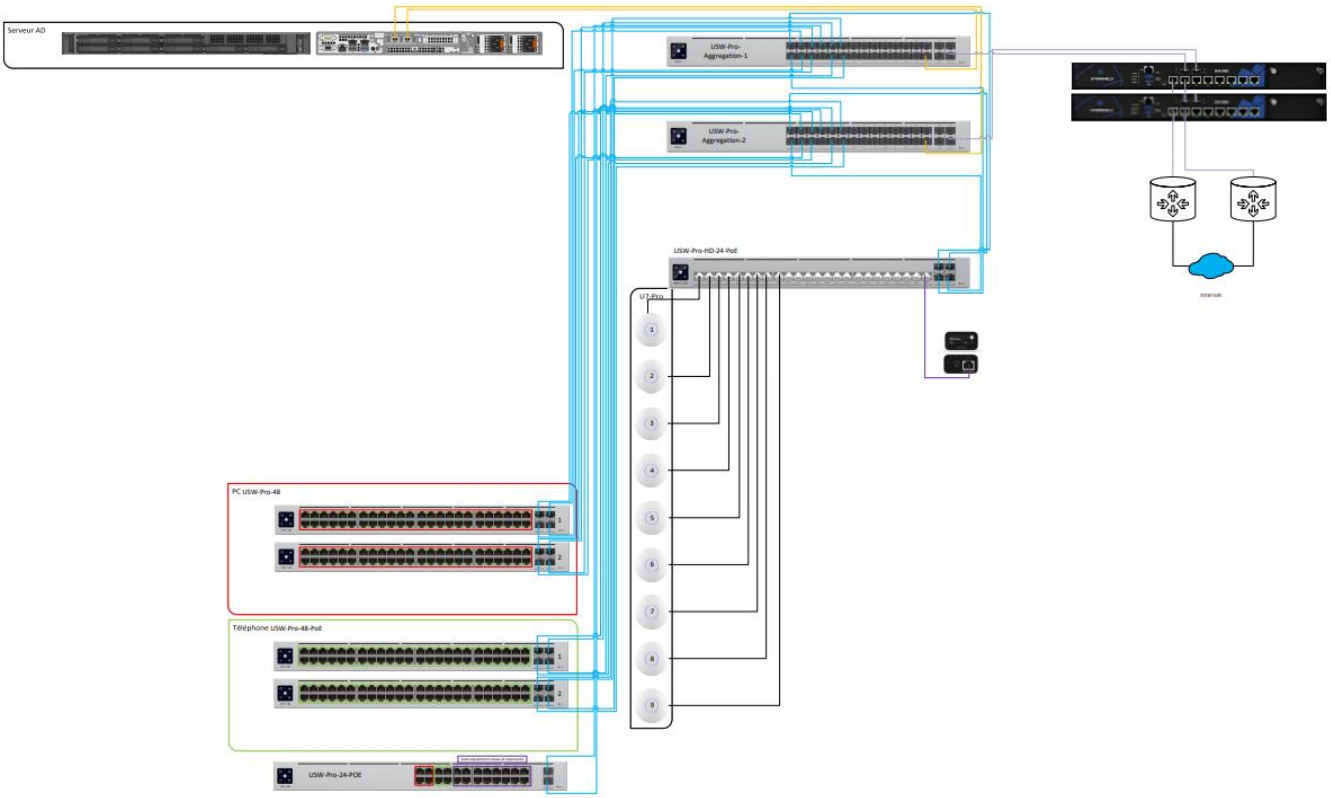
Séville	50	Wifi	192.168.50.0/24
Séville	51	IOT	192.168.51.0/24
Séville	52	Administration réseau	192.168.52.0/24
Séville	53	Caméras	192.168.53.0/24
Séville	54	Imprimantes	192.168.54.0/24
Séville	55	Bureautique	192.168.55.0/24
Séville	56	Serveurs	192.168.56.0/24
Séville	57	DMZ	192.168.57.0/24
Séville	59	Téléphonie	192.168.59.0/24
Séville	**425**	**Natif**	**X**
Amsterdam	60	Wifi	192.168.60.0/24
Amsterdam	61	IOT	192.168.61.0/24
Amsterdam	62	Administration réseau	192.168.62.0/24
Amsterdam	63	Caméras	192.168.63.0/24
Amsterdam	64	Imprimantes	192.168.64.0/24
Amsterdam	65	Bureautique	192.168.65.0/24
Amsterdam	66	Serveurs (VMWare)	192.168.66.0/24
Amsterdam	67	DMZ	192.168.67.0/24
Amsterdam	69	Téléphonie	192.168.69.0/24
Amsterdam	**426**	**Natif**	**X**
Rabat	70	Wifi	192.168.70.0/24
Rabat	71	IOT	192.168.71.0/24
Rabat	72	Administration réseau	192.168.72.0/24
Rabat	73	Caméras	192.168.73.0/24
Rabat	74	Imprimantes	192.168.74.0/24
Rabat	75	Bureautique	192.168.75.0/24
Rabat	76	Serveurs (Datacenter)	192.168.76.0/24
Rabat	77	DMZ	192.168.77.0/24
Rabat	79	Téléphonie	192.168.79.0/24
Rabat	**427**	**Natif**	**X**
Austin	80	Wifi	192.168.80.0/24
Austin	81	Sécurité	192.168.81.0/24
Austin	82	Administration réseau	192.168.82.0/24
Austin	83	Caméras	192.168.83.0/24
Austin	84	Imprimantes	192.168.84.0/24
Austin	85	Bureautique	192.168.85.0/24
Austin	86	Serveurs (Datacenter)	192.168.86.0/24
Austin	87	DMZ	192.168.87.0/24
Austin	89	Téléphonie	192.168.89.0/24
Austin	**180**	**Applications clients**	**192.168.180.0/24**
Austin	**428**	**Natif**	**X**

Architecture réseau

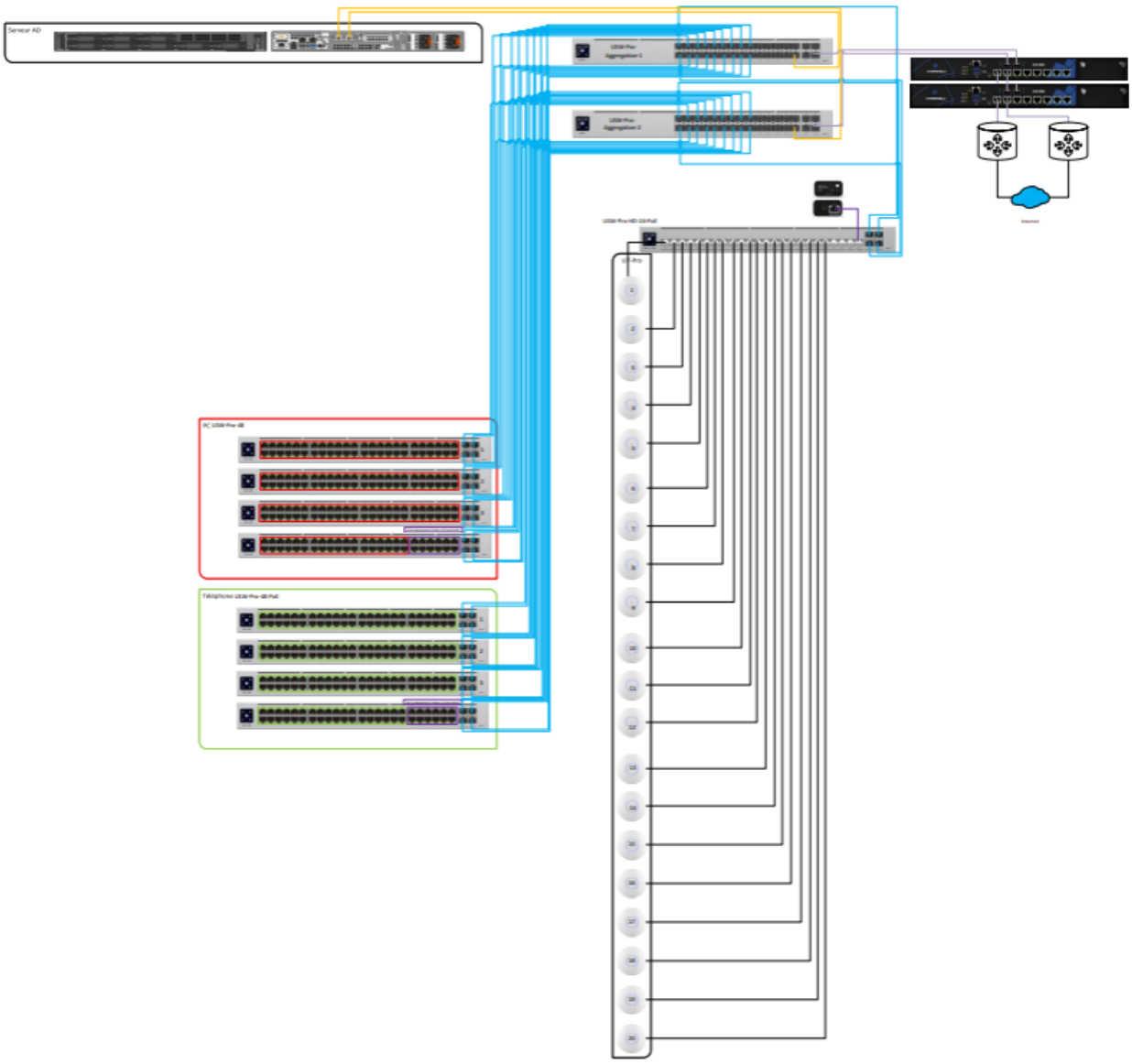
Schema typique de la méthodologie employée



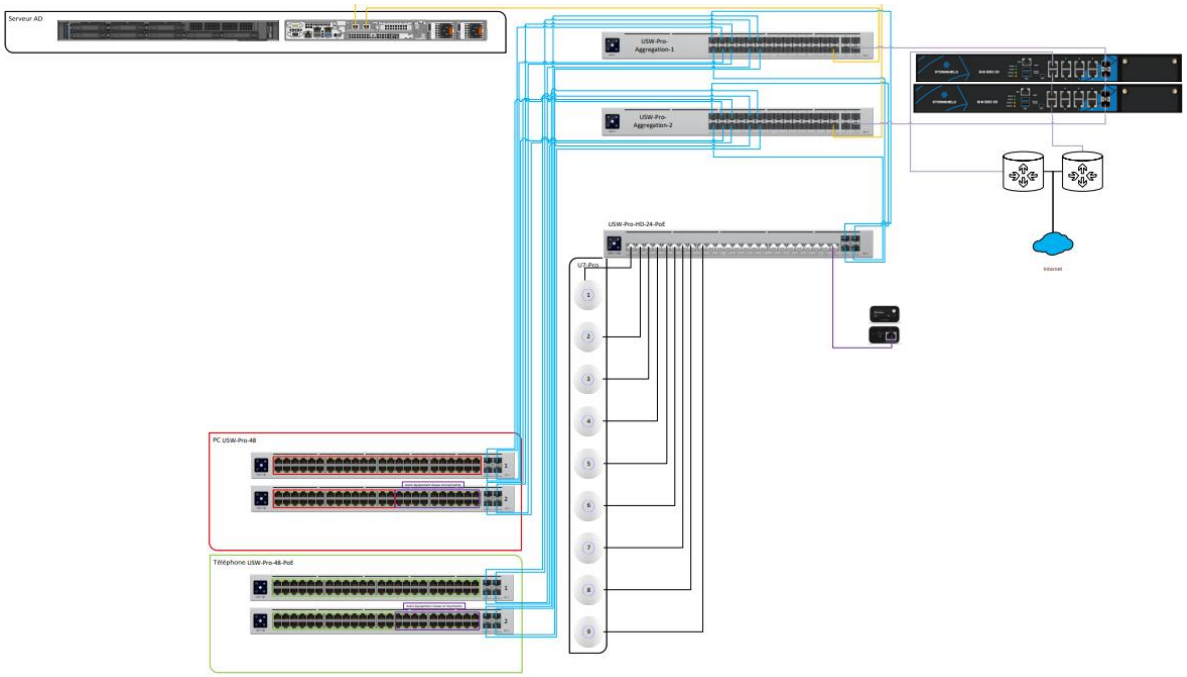
Lille :



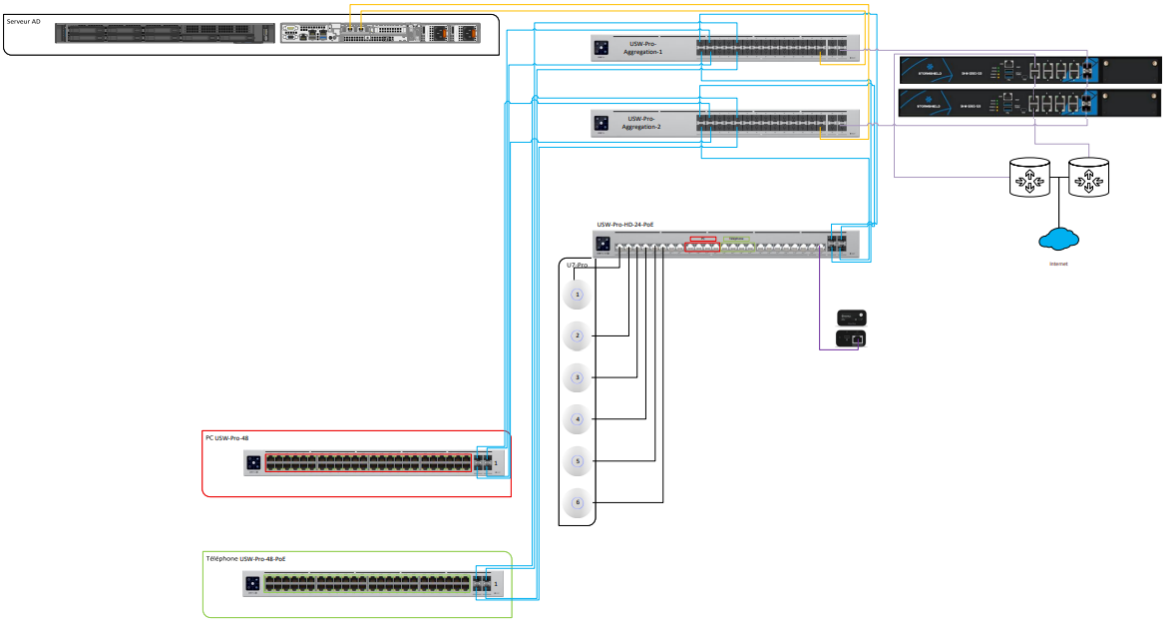
Rabat :



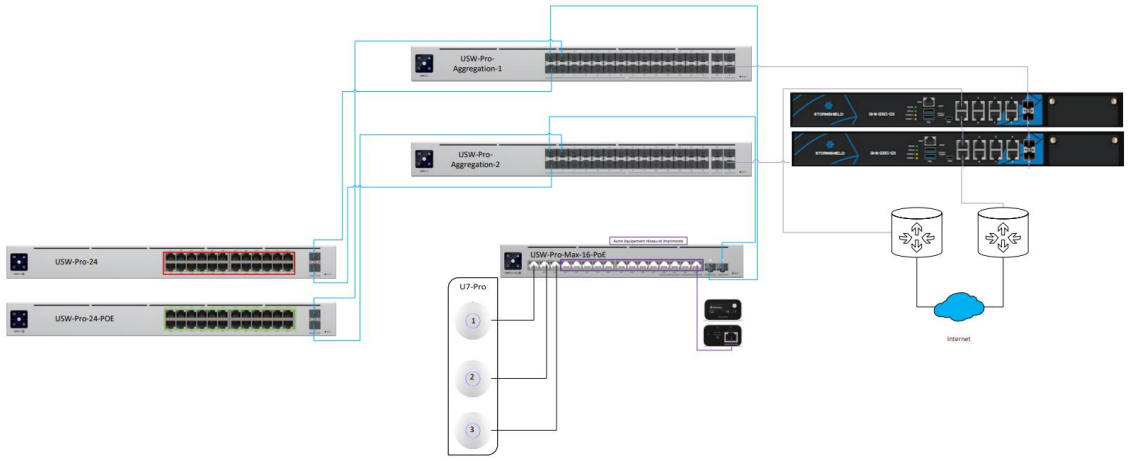
Seville :



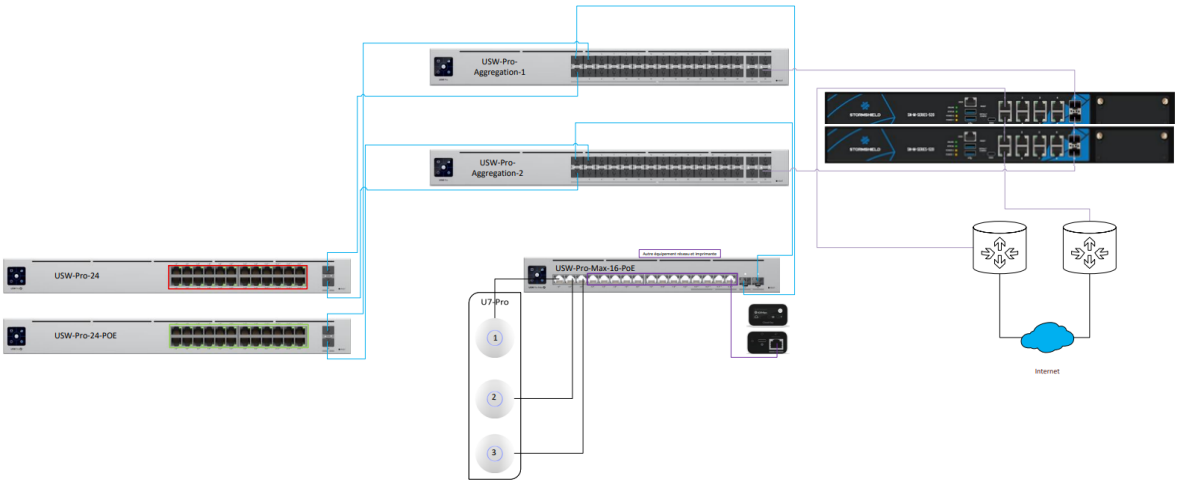
Austin :



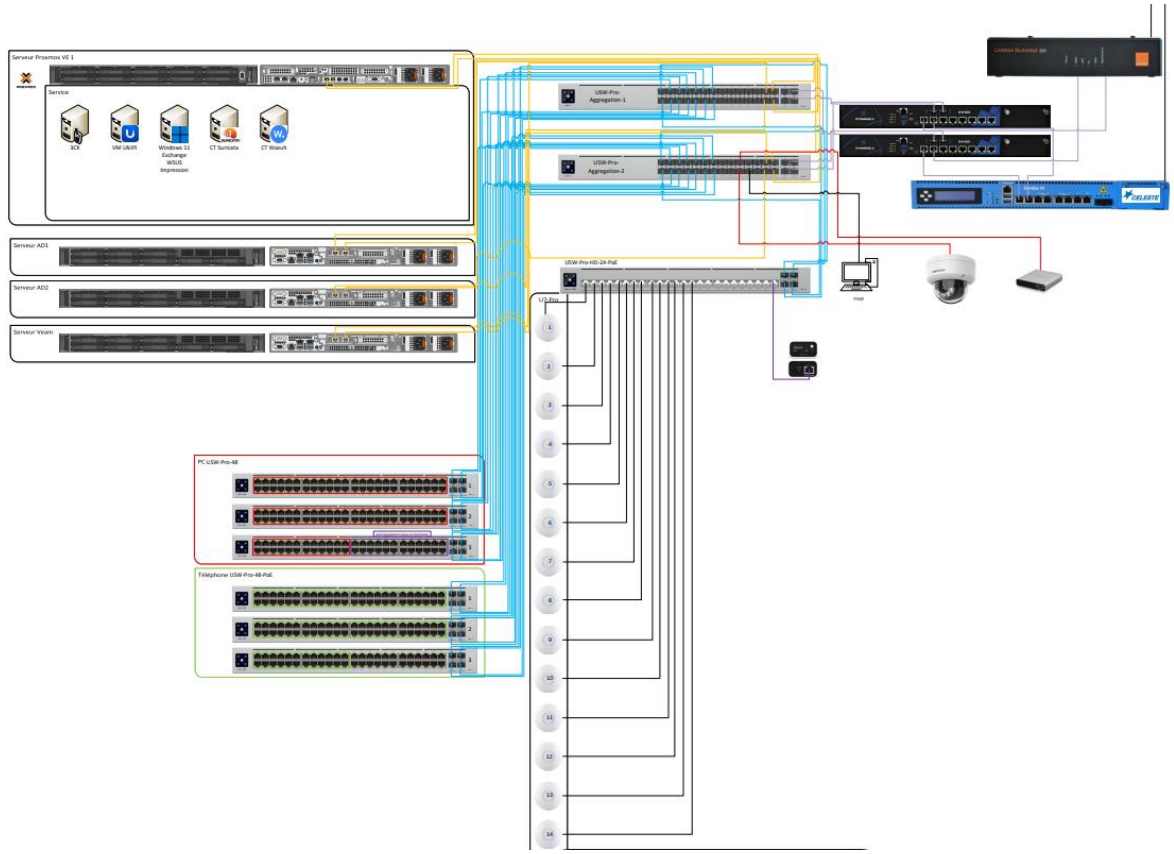
Amsterdam :



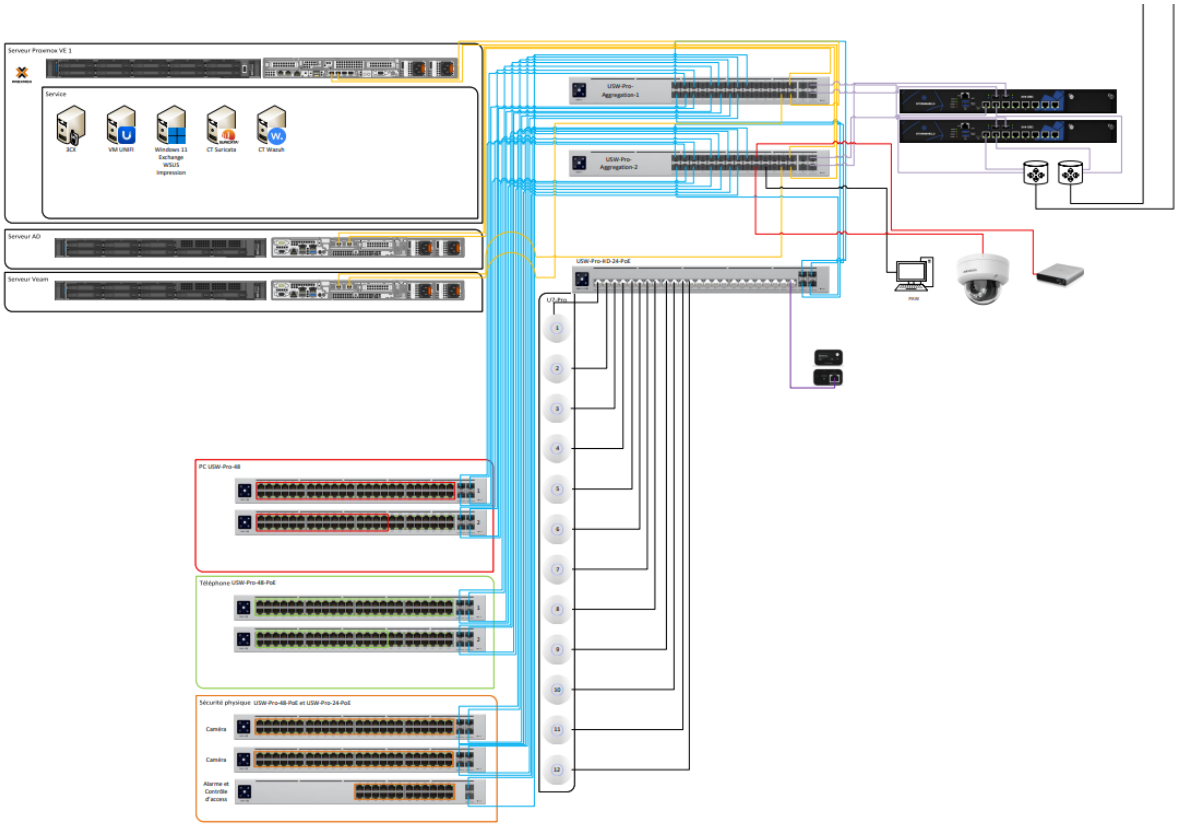
Barcelone :



Paris :



Lyon :


Serveur Proxmox VE 1
Service
3CX
VM UNIFI
Windows 11 Exchange WSUS Impression
CT Suricata
CT Wazuh
Serveur AD
Serveur Veeam
USW-Pro-Aggregation-1
USW-Pro-Aggregation-2
USW-Pro-XG-24-PoE
PC USW-Pro-48
Téléphone USW-Pro-48-PoE
Sécurité physique USW-Pro-48-PoE et USW-Pro-24-PoE
Caméra
Caméra
Alarme et Contrôle d'accès