PROJET MODERNISATION DE L'INFRASTRUCTURE SYSTEME RESEAU ET SECURITE DE SOLARIS

Projet réalisé par Kevin TASSA FONGUENG

Table des matières

Table de figures

Un Plan de Reprise d'Activité, (PRA) vise à rétablir le système d'information de l'entreprise au plus vite en cas de sinistre. Le PRA vise à minimiser les temps d'arrêt de l'entreprise en maintenant l'accès aux infrastructure informatiques et aux applications critiques.

Table des tableaux

ABSTRACT

This study focuses on the modernization of the information system of *Groupe Solaris*, a leading French company in industrial ecology, in collaboration with *NetPro Consulting*, an IT engineering services provider. The project aims to address significant limitations in Solaris' current IT infrastructure, which suffers from outdated hardware and software, security vulnerabilities, and insufficient scalability to support business growth.

The objectives of the project are to conduct a comprehensive audit of the existing infrastructure, identify the causes of dysfunctions, and design a more secure, efficient, and sustainable architecture. Key areas of improvement include network segmentation through VLAN redesign, the implementation of high availability and redundancy, system upgrades to supported platforms, enhanced data backup and disaster recovery strategies, and the integration of modern security protocols.

The methodology combines project management best practices (PBS, WBS, RACI, and Gantt scheduling) with risk analysis (FMEA), ensuring a structured approach to planning, resource allocation, and risk mitigation. Constraints such as budget, deadlines, quality, and compliance with regulations (including GDPR) were carefully considered.

The proposed solutions are expected to reduce operational costs, improve system reliability and data security, and increase productivity, particularly under crisis conditions. This project highlights the importance of IT infrastructure modernization for ensuring both technological resilience and regulatory compliance in industrial environments.

I. Présentation des entreprises

A. Présentation du client Groupe Solaris

Groupe Solaris est un acteur prédominant du monde écologique qui recherche, développe et commercialise des solutions vertes centrées sur les besoins des entreprises conscientes de l'impact grandissant de la pollution industrielle sur le milieu naturel. Depuis sa création en janvier 2011, Solaris a su s'imposer comme un leader dans le domaine de l'écologie industrielle, en mettant l'accent sur quatre plateformes de croissance essentielles :

- La prise en charge des résidus radioactifs produits par l'industrie nucléaire
- La gestion des déchets chimiques
- Le développement de produits innovants dans le domaine du tri sélectif
- La prise en charge des déchets médicaux produits par les hôpitaux

Groupe Solaris emploie environ 1000 collaborateurs repartit sur deux sites et dispose de plusieurs centres de traitement répartis stratégiquement sur le territoire. L'entreprise met un point d'honneur à la recherche et développement pour proposer des solutions de recyclage et de gestion des déchets toujours plus performantes et respectueuses de l'environnement.

2. Renseignements juridiques

Information	Détails
Nom de la Société	Groupe Solaris
Date création entreprise	01/01/2011
Forme juridique	Société à responsabilité limitée (SARL)
Nom commercial	Solaris
Téléphone	01 56 78 90 12
Adresse postale	
Site	www.Solaris-eco.com
Email	contact@solaris-eco.com
Numéros d'identification	
Numéro SIREN	4507683312
Numéro SIRET (siège)	450768331200045
Numéro TVA Intracommunautaire	FR5090850857212
Numéro RCS	Paris B 4507683312
Catégorie	Ecologie industrielle
Activité (Code NAF ou APE)	Traitement et élimination des déchets dangereux (3822Z)
Informations juridiques	
Statut RCS	INSCRITE - au greffe de Paris
Statut INSEE	INSCRITE

Date d'immatriculation RCS	Immatriculée au RCS le 10-02-2011
Date d'enregistrement INSEE	Enregistrée à l'INSEE le 05-02-2011
Taille de l'entreprise	1000
Capital social	15 000 000,00 €
Chiffre d'affaires	120 500 000,00 €

Tableau 1 : Renseignement juridique Solaris

3. Géolocalisation

Le siège social de Groupe Solaris se situe dans le 2e arrondissement de Paris, offrant une accessibilité optimale à ses partenaires et clients. L'entreprise dispose également d'un autre site à Lyon.

Figure 1 : Géolocalisation Solaris

4. Organigramme du groupe Solaris

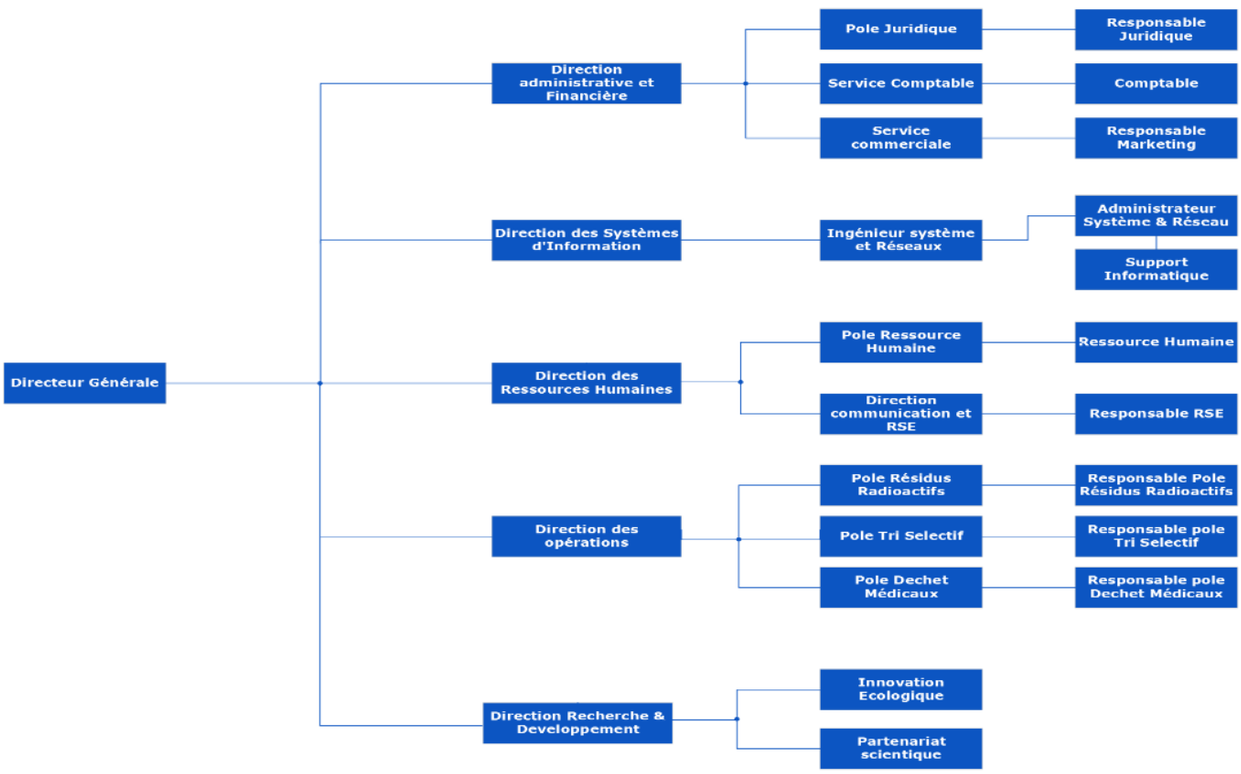


Figure 2 : Organigramme du groupe Solaris

B. Présentation du prestataire NetPro Consulting

NetPro Consulting est une société de services du type ESN (Entreprise de Service du Numérique) en ingénierie informatique SSII, fondée en 2010 par un ancien employé de Microsoft. Avec 13 ans d'expérience dans le domaine des services informatiques et de l'ingénierie système, NetPro Consulting accompagne ses clients dans la conception, la mise à niveau et la sécurisation de leurs infrastructures IT.

Domaines d'intervention :

- **Système et réseaux** (Sécurité IT, Conception et mise à niveau des infrastructures, Installation Serveur, VPN)
- **Consulting IT** (Cahier des charges, Audit des besoins informatiques, gestion de projet)
- **Services Cloud et virtualisation** (Sauvegarde, Stockage et Migration)

1. Renseignements juridiques

Information	Détails
Nom de la Société	NetPro Consulting
Date création entreprise	08/07/2010
Forme juridique	Société à responsabilité limitée (SARL)
Noms commerciaux	NetPro Consulting
Téléphone	01 48 98 78 10
Adresse postale	1 Passage du Chemin Vert, 75011 Paris
Site	www.netproconsulting.com
Email	contact@netproconsulting.com
Numéros d'identification	
Numéro SIREN	3407683312
Numéro SIRET (siège)	340768331200032
Numéro TVA Intracommunautaire	FR51420857212
Numéro RCS	Paris B 420 857 212
Activité (Code NAF ou APE)	Ingénierie, études techniques (7112B)
Statut RCS	INSCRITE - au greffe de Paris
Statut INSEE	INSCRITE
Date d'immatriculation RCS	15-07-2010
Date d'enregistrement INSEE	08-07-2010
Tranche d'effectif	110
Capital social	900 000,00 €
Chiffre d'affaires 2021	45 000 000,00 €

Tableau 2: Renseignement juridique Netpro Consulting

2. Géolocalisation

Le siège social de NetPro Consulting se situe à **Paris**, facilitant ainsi les rencontres avec ses clients et partenaires.

Figure 3:Géolocalisation NetPro Consulting

3. Organigramme du NetPro Consulting

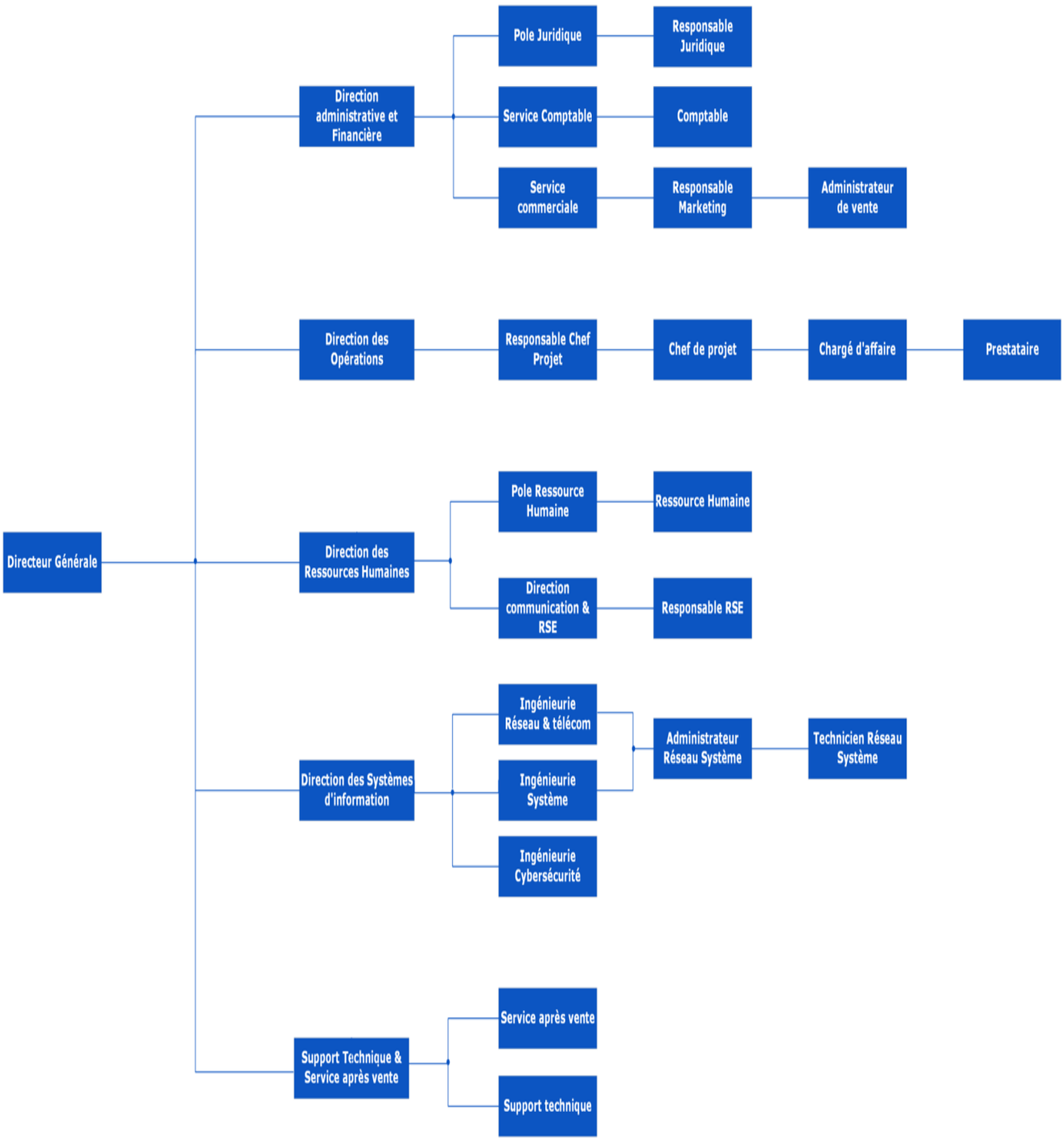


Figure 4: Organigramme NetPro Consulting

4. Nos Partenaires et certificat

II. Présentation du projet

1. Contexte

Ce projet a pour objectif de faire **évoluer l'infrastructure informatique du groupe Solaris** et sa **maintenance ultérieure**. Il doit permettre la **recherche de la meilleure proposition d'intervention**, sur les plans techniques et méthodologiques ainsi qu'en matière **de coût** et **d'impact sur l'activité du groupe Solaris**. L'évolution concerne la totalité du SI des deux sites, **leur infrastructure réseau**, tant **matérielle que logicielle**, les **serveurs et les stations de travail**, les services et applications bureautiques, les **procédures de maintenance courantes** et de **sécurité**, **leur pérennité et leur organisation à tous les niveaux**. Solaris entend également recevoir des recommandations sur les éléments qu'il n'aurait pas prévus d'inclure au présent projet mais dont **NetPro consulting**, du fait de sa compétence technique, estimerait l'évolution nécessaire.

2. Objectif des besoins

- Identifier les éléments existants et les causes des dysfonctionnements.
- Proposer un diagnostic global du Système d'Information et des solutions d'amélioration.
- Si nécessaire, refondre l'architecture physique et logique de tout ou partie du SI.
- Recommander le remplacement ou la mise à jour des équipements obsolètes dans le cadre de la nouvelle architecture.
- Après la mise en place de l'infrastructure, réaliser un audit de sécurité.
- Diminuer les coûts de fonctionnement tout en améliorant la fiabilité du système, en respectant les législations et réglementations relatives à la sécurité des données.
- Augmenter la productivité, en particulier dans les situations de crise, pour répondre à la croissance des demandes, à la mobilité sur le terrain, et à la rapidité de déploiement de nouveaux sites, qu'ils soient temporaires ou fixes.

L'ensemble des solutions proposées devra tenir compte de la confidentialité extrême des données de l'entreprise, très impactée par la réglementation RGPD.

3. Présentation des acteurs

Chef de projet (MOE)	Membre de l'équipe projet	Client (MOA)	Membre de l'équipe projet	Acteurs institutionnels
NetPro Consulting	Chef de projet	Groupe Solaris	DSI du Client	Représentant de l'Etat
	Chargé d'affaire		Directeur Financier	
	Ingénieurs réseaux & télécom		Ingénieurs systèmes & réseaux	
	Ingénieurs systèmes			
	Ingénieurs Cybersécurité			
	Administrateurs réseaux & systèmes		Administrateur systèmes & réseaux	
	Techniciens systèmes & réseaux			
	Prestataires Externes		Support informatique	

Tableau 3 : Présentation des acteurs

4. Garantie qualité des solutions mises en place

Une panne informatique peut avoir des conséquences importantes, tant sur la gestion de votre parc que sur le plan financier et humain. Il est donc essentiel d'anticiper ces risques en tenant compte des garanties disponibles, qu'elles soient proposées par le constructeur ou le revendeur. À noter : la qualité du service après-vente (SAV) varie fortement selon les marques et les niveaux de service souscrits.

Avant tout achat, il est recommandé de bien évaluer ces éléments afin d'éviter des complications en cas de défaillance du matériel.

Trois critères déterminent la qualité d'un SAV :

- Le délai de prise en charge,
- Le temps d'intervention,
- Et les modalités de traitement de l'incident.

En général, la garantie standard et ses éventuelles extensions permettent de bénéficier du SAV pendant une période allant de 1 à 5 ans. Selon le contrat, le support pourra être joint via un portail en ligne, un helpdesk à distance (en France ou à l'étranger), ou par téléphone. La plage horaire de disponibilité du support technique est aussi un facteur déterminant.

Plusieurs scénarios de prise en charge sont possibles :

- Diagnostic à distance,
- Retour du matériel défectueux,
- Ou intervention d'un technicien sur site.

Les constructeurs s'engagent alors à intervenir selon des délais définis dans les SLA (Service Level Agreements), avec des interventions possibles dès le lendemain (J+1) dans les cas les plus rapides.

Enfin, il est important d'intégrer les coûts des extensions de garantie dans le calcul du Coût Total de Possession (CTP).

La garantie de base est incluse dans le prix d'achat de l'équipement. En revanche, les extensions — dont le tarif varie de 70 € à plus de 350 € — dépendent de leur durée et des délais d'intervention prévus. Ces coûts supplémentaires, liés au niveau de couverture et à la qualité du SAV, doivent être pris en compte dans la stratégie d'investissement IT.

5. Contrainte

a. Coûts

- Coût des ressources matérielles : achat de nouveaux serveurs, licences logicielles (Windows Server, SQL, Exchange, antivirus, etc.), renouvellement de postes clients, outils de supervision.
- Coûts des ressources humaines : formation du personnel, assistance technique externe, interruption temporaire des services, tests/migrations.
- Optimisation attendue : le coût est une contrainte forte, mais certaines évolutions (migration cloud, modernisation du parc) peuvent générer des économies à long terme.
- Budget disponible :

b. Délais

- Disponibilité des ressources humaines : internes (DSI, techniciens) et externes (prestataires, intégrateurs).

- Limiter les fenêtres de déploiement : éviter de solliciter systématiquement des autorisations pour la réalisation des tâches.
- Temps de test et des migrations : notamment sur les services critiques (AD, Exchange, SQL). Contrainte lieu à hétérogénéité des environnements.
- Délais d'approvisionnement : matériel (PC, serveurs) ou licences.

c. Qualité

- Maintien de la qualité de service (QoS) : garantir un accès continu aux outils pour les utilisateurs.
- Compatibilité applicative : les mises à jour ne doivent pas perturber PolarisAid ou d'autres outils métiers.
- Fiabilité des sauvegardes et PRA : éviter toute perte de données.
- Conformité au Référentiel (Version 4) : Chaque étape du projet est menée en accord avec les normes et exigences définies dans le référentiel version 4.
- Documentation : assurer une traçabilité technique pour toute l'évolution.

d. Contraintes sanitaires

- Télétravail / Mobilité : nécessité de garantir un accès sécurisé aux ressources depuis l'extérieur (VPN, M365, SSO, MFA).
- Implémentation des outils de prise en main à distance : réduction des interventions physiques.
- Réunions à distance : coordination entre les équipes et les prestataires via outils collaboratifs (Teams, Zoom...).
- Santé et sécurité du personnel : planification des interventions en rapport avec les règles du QHSE.

e. Synthèse des contraintes

Contrainte	Impact	Solution / Atténuation
Coûts	Budget limité	Étaler le projet, prioriser, viser le ROI
Délais	Risque de blocage métier	Planification fine, tests préalables
Qualité	Risque sur la production	POC, validation profile utilisateurs
Sanitaire	Intervention limitée	Déploiement distant, sécurité du télétravail

Tableau 4 : Synthèse des contraintes

III. Gestion de project

1. PBS (Product Breakdown Structure)

Le PBS, ou structure de découpage du produit, est une méthode qui consiste à décomposer un produit final en sous-éléments ou composants plus petits et plus faciles à gérer. Cela permet de visualiser tous les livrables attendus d'un projet, sans se concentrer sur les tâches, mais uniquement sur la structure du produit à livrer.

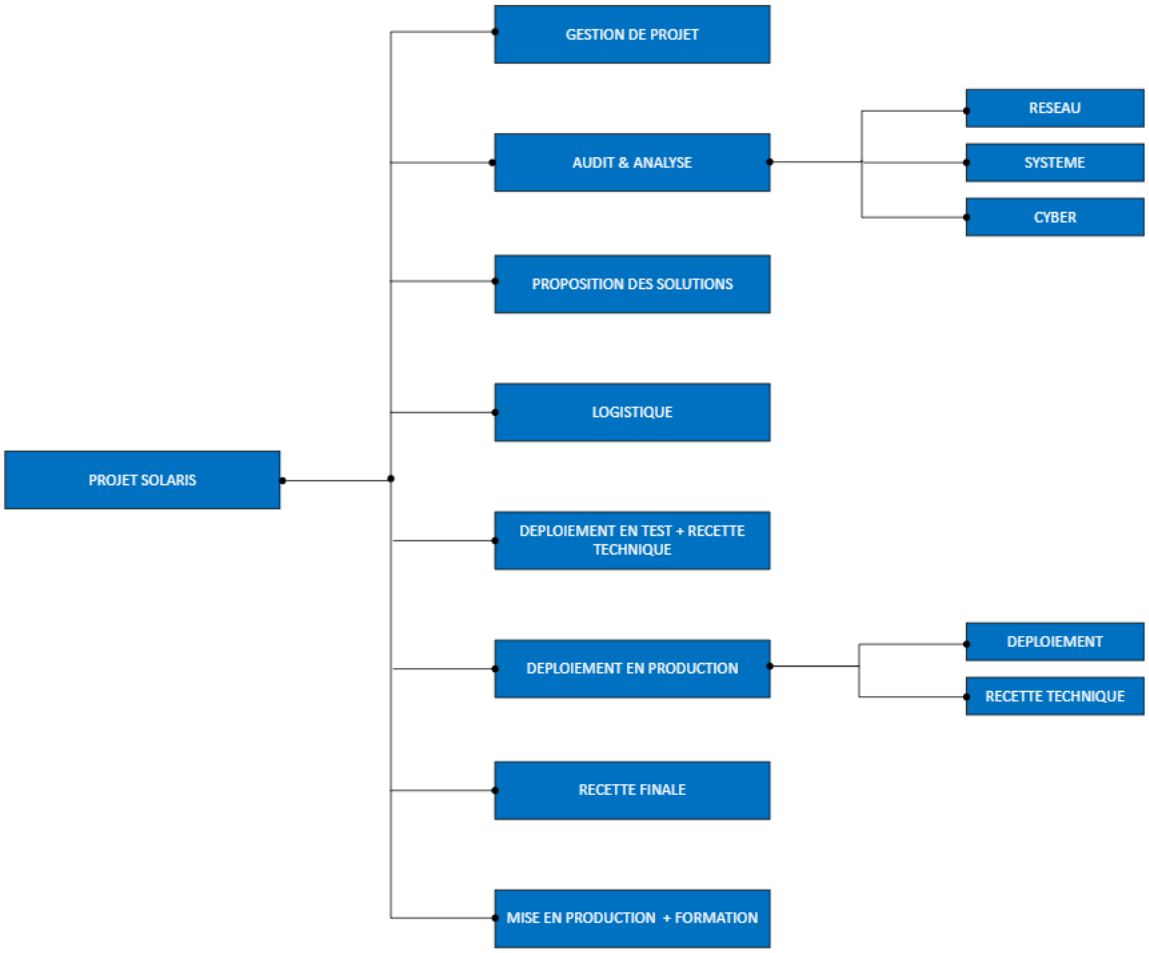


Figure 5 : PBS

2. WBS (Work Breakdown Structure)

Pour assurer la réussite de ses projets, NetPro Consulting a structuré son approche autour de huit tâches principales, chacune déclinée en sous-tâches selon la méthode WBS (Work Breakdown Structure).

Ces huit grandes tâches définissent le périmètre des livrables du projet. Il est important de préciser que le plan WBS présenté ci-dessous correspond à l'organisation prévue en amont de la phase de mise en œuvre.

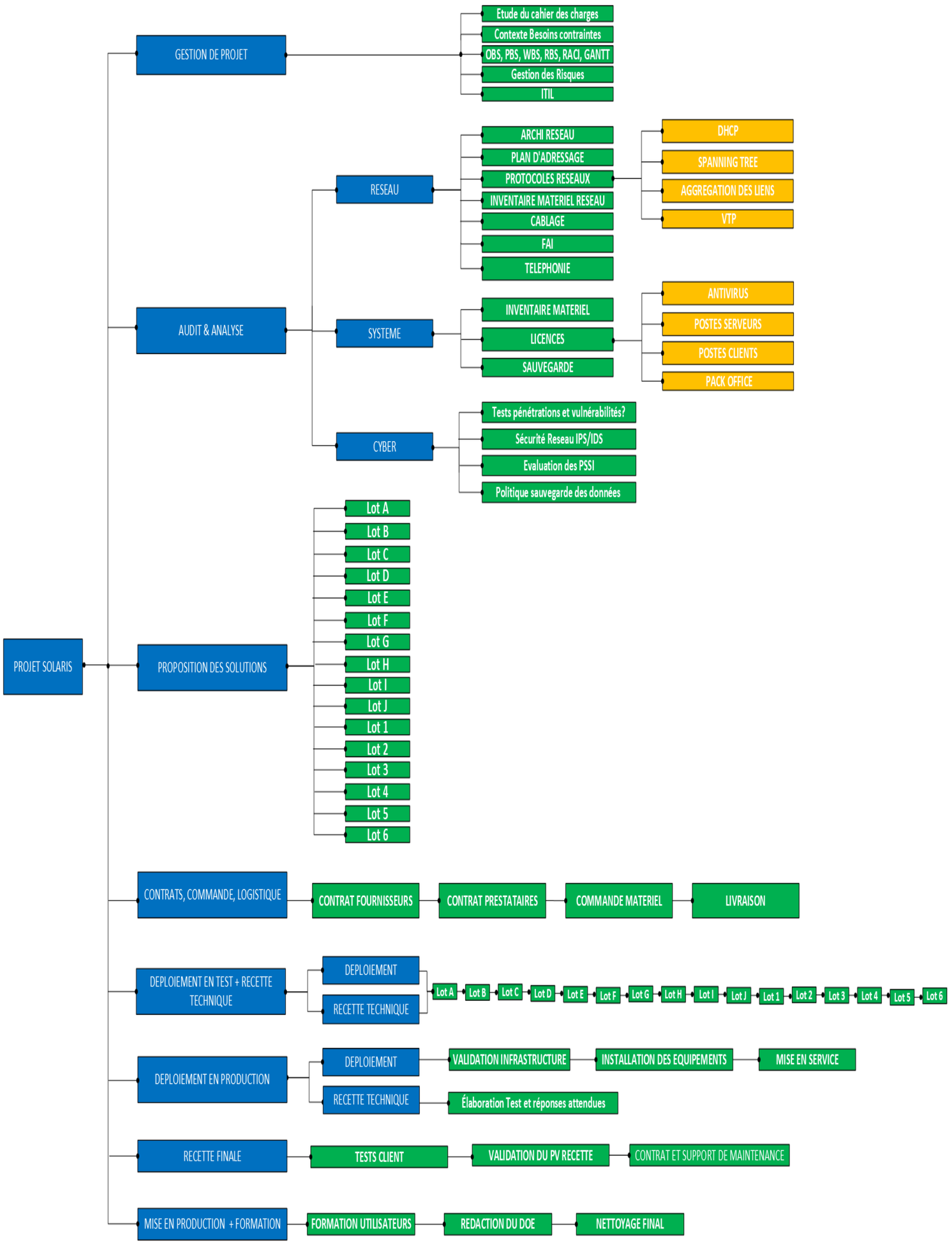

PROJET SOLARIS
GESTION DE PROJET
Etude du cahier des charges
Contexte Besoins contraintes
OBS, PBS, WBS, RBS, RACI, GANTT
Gestion des Risques
ITIL
AUDIT & ANALYSE
RESEAU
ARCHI RESEAU
PLAN D'ADRESSAGE
PROTOCOLES RESEAUX
INVENTAIRE MATERIEL RESEAU
CABLAGE
FAI
TELEPHONIE
DHCP
SPANNING TREE
AGGREGATION DES LIENS
VTP
SYSTEME
INVENTAIRE MATERIEL
LICENCES
SAUVEGARDE
ANTIVIRUS
POSTES SERVEURS
POSTES CLIENTS
PACK OFFICE
CYBER
Tests pénétrations et vulnérabilités?
Sécurité Reseau IPS/IDS
Evaluation des PSSI
Politique sauvegarde des données
PROPOSITION DES SOLUTIONS
Lot A
Lot B
Lot C
Lot D
Lot E
Lot F
Lot G
Lot H
Lot I
Lot J
Lot 1
Lot 2
Lot 3
Lot 4
Lot 5
Lot 6
CONTRATS, COMMANDE, LOGISTIQUE
CONTRAT FOURNISSEURS
CONTRAT PRESTATAIRES
COMMANDE MATERIEL
LIVRAISON
DEPLOIEMENT EN TEST + RECETTE TECHNIQUE
DEPLOIEMENT
RECETTE TECHNIQUE
Lot A
Lot B
Lot C
Lot D
Lot E
Lot F
Lot G
Lot H
Lot I
Lot J
Lot 1
Lot 2
Lot 3
Lot 4
Lot 5
Lot 6
DEPLOIEMENT EN PRODUCTION
DEPLOIEMENT
RECETTE TECHNIQUE
VALIDATION INFRASTRUCTURE
INSTALLATION DES EQUIPEMENTS
MISE EN SERVICE
Élaboration Test et réponses attendues
RECETTE FINALE
TESTS CLIENT
VALIDATION DU PV RECETTE
CONTRAT ET SUPPORT DE MAINTENANCE
MISE EN PRODUCTION + FORMATION
FORMATION UTILISATEURS
REDACTION DU DOE
NETTOYAGE FINAL

Figure 6 : WBS

3. OBS (Organisationnel Breakdown Structure)

Dans le cadre de ce projet, les équipes informatiques de NetPro Consulting et du Groupe Solaris collaboreront étroitement à sa mise en œuvre.

Du côté de NetPro Consulting, le chef de projet assumera l'entière responsabilité de la supervision globale du projet.

Côté Groupe Solaris, NetPro Consulting coopérera avec les services administratifs et financiers pour garantir l'approvisionnement nécessaire à l'équipe technique. Une collaboration avec l'équipe informatique interne du Groupe Solaris sera également assurée afin de maintenir la continuité des services tout au long du projet.

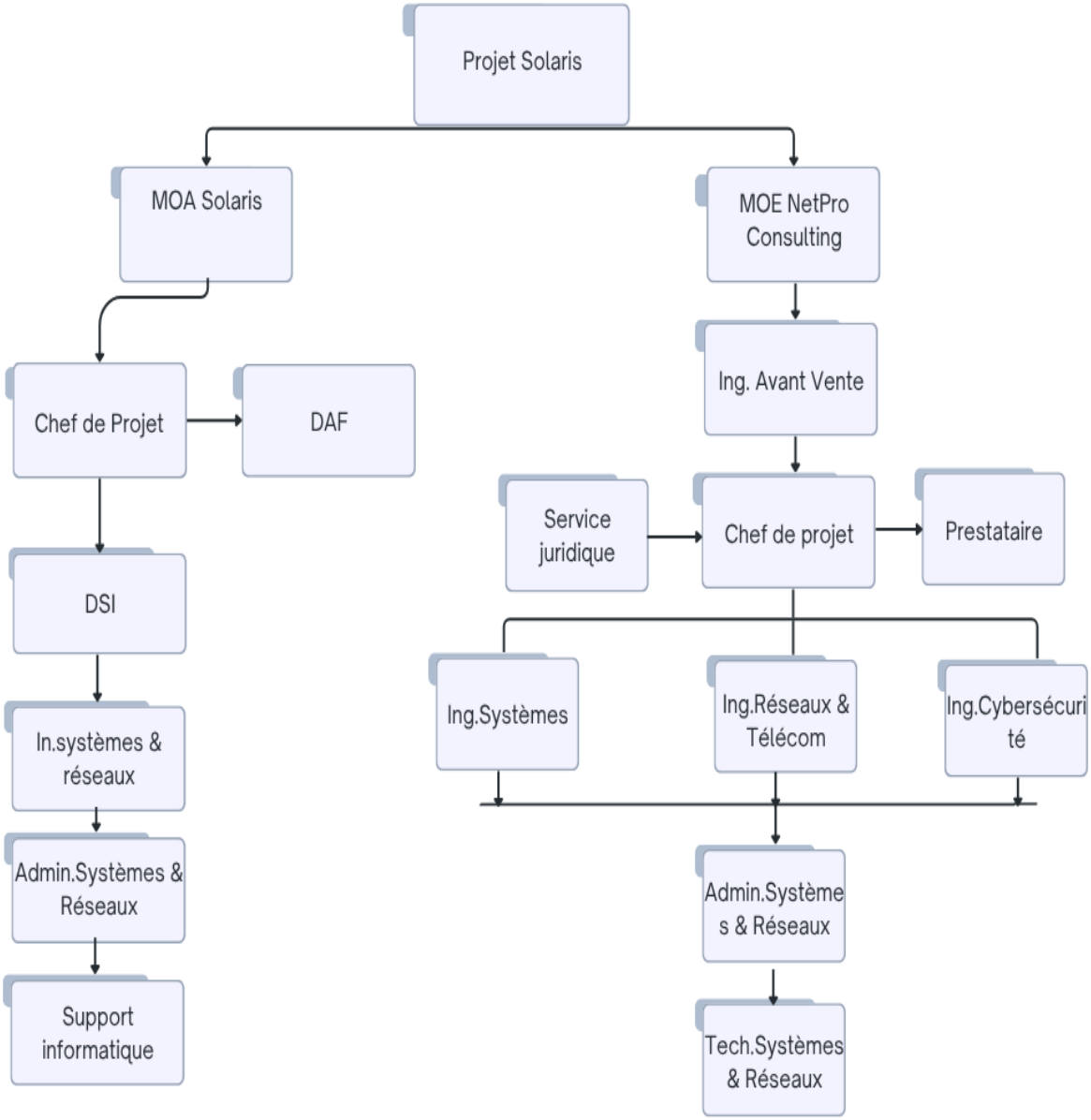
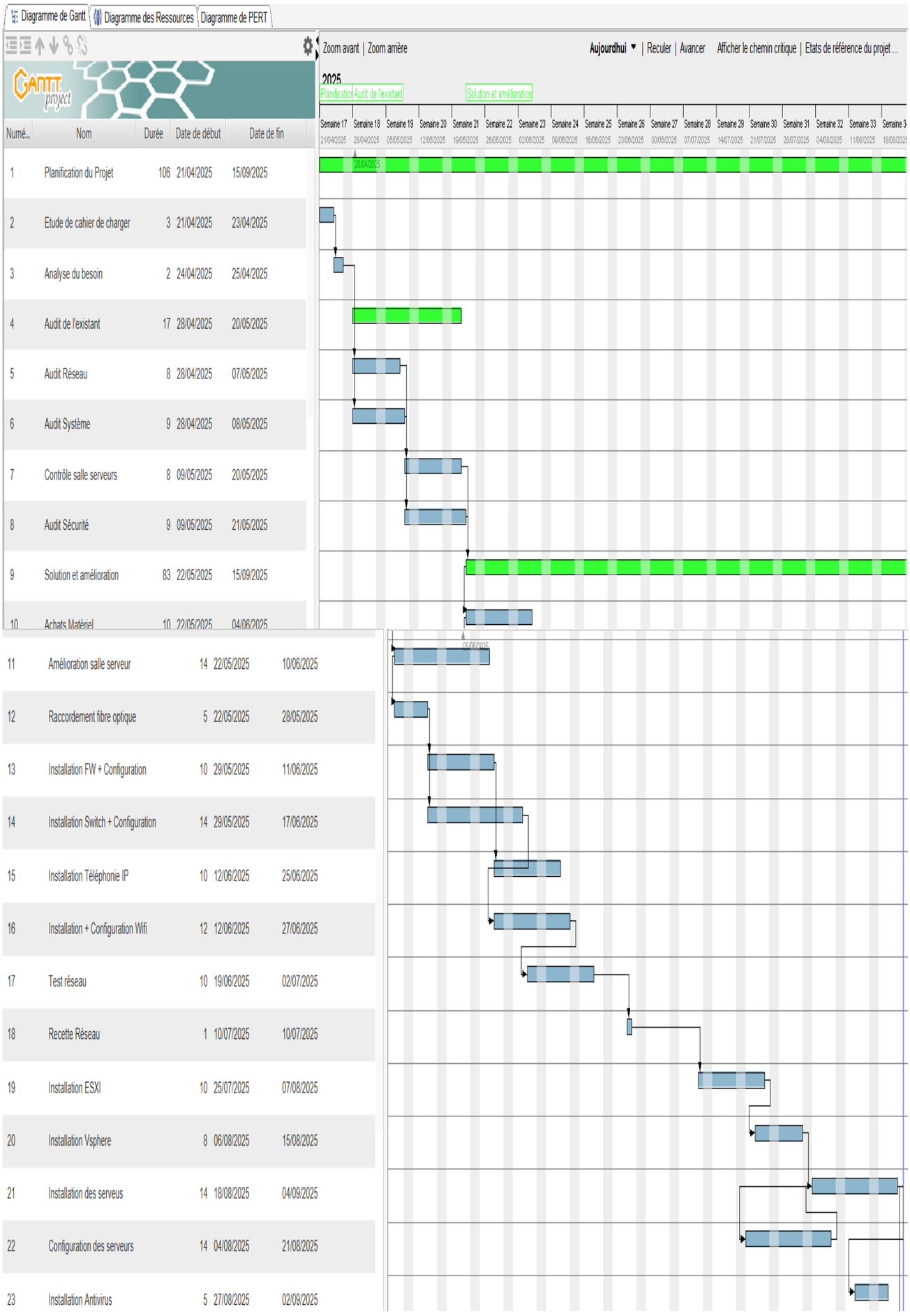


Figure 7 : OBS

4. Diagramme de Gantt

Le diagramme de Gantt est un outil de gestion de projet qui permet de visualiser l'avancement des tâches dans le temps. Il se présente sous forme de calendrier avec des barres horizontales représentant la durée de chaque tâche, leur enchaînement, leurs dépendances et les dates de début/fin. Il aide à planifier, suivre et coordonner les activités d'un projet.



24	Migration des Serveurs	25	05/09/2025	09/10/2025
25	Déploiement d'un SAN	8	23/09/2025	02/10/2025
26	Serveur web	6	29/09/2025	06/10/2025
27	Serveur AD	6	30/09/2025	07/10/2025
28	Serveur DATA	5	06/10/2025	10/10/2025
29	Test système	5	07/10/2025	13/10/2025
30	Recette système	1	13/10/2025	13/10/2025
31	Formation du personnel	14	14/10/2025	31/10/2025
32	Contrat de maintenance	1	05/11/2025	05/11/2025

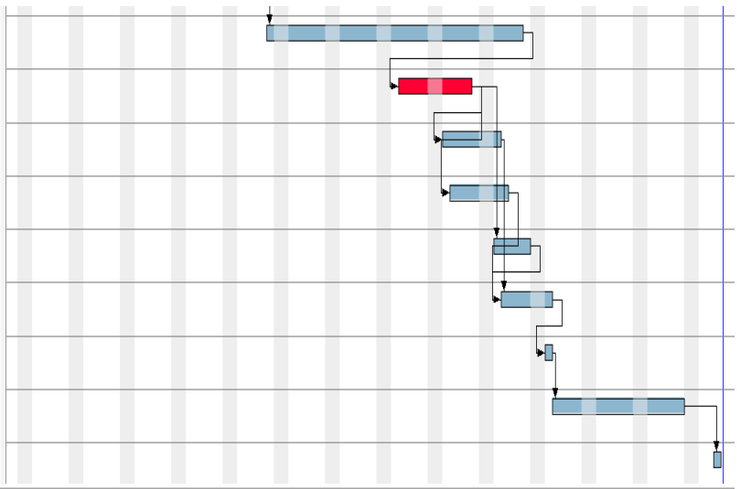
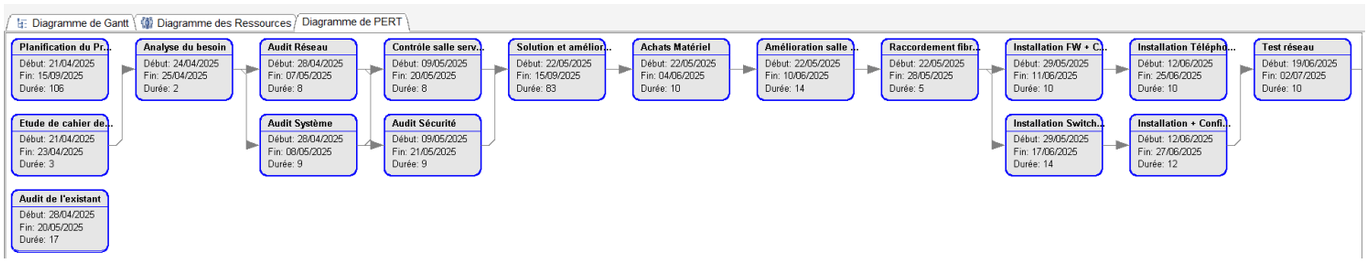


Figure 8 : Diagramme de Gantt

Diagramme de PERT



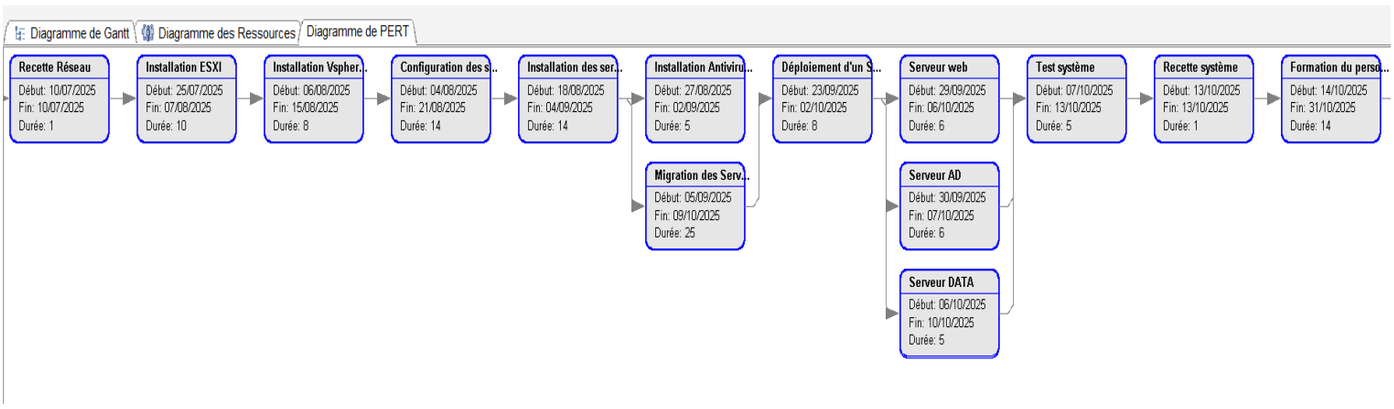


Figure 9 : Diagramme de PERT

5. Les responsabilités du projet (Matrice RACI)

La matrice RACI est un tableau qui définit les rôles et responsabilités de chaque membre de l'équipe projet pour chaque tâche ou livrable.

Légende :

- **R** = **R**éalisateur
- **A** = **A**pprobateur
- **C** = **C**onsultant
- **I** : **I**nformé

Matrix RACI Projet Solaris

ROLES	Chef de projet	Commercial et IAV	Ing Réseau	Ing Système	Ing Cyber	Admin Réseau & Système	Tech Réseau & Système	chargé d'affaire	Consultant audit et Resp RGPD	Prestataire	fournisseurs	Chef de projet	DAF	DSI	Ing Réseau sytème	Admin Système Réseau	support informatique
Taches du projet	MOE											MOA					
1. Gestionde projet																	
Etude du cahier des charges	R	C	I	I	I	I	I	I	C	-	-	A	I	C	I	I	I
Périmètre, cadrage et contraintes	R	C	I	I	I	I	I	I	C	-	-	A	I	C	I	I	I
Kickoff interne/externe	A	R	I	I	I	I	I	I	I	-	-	A	I	C	I	I	I
OBS, PBS, WBS, RBS, RACI, GANTT	R	I	C	C	C	C	C	I	I	-	-	A	I	A	C	C	I
Gestion des risques	R	I	C	C	C	C	C	I	C	-	-	A	I	A	C	C	I
ITIL	R	I	C	C	C	C	C	I	C	-	-	A	I	A	C	C	I
2. Audit et Analyse																	
Réseau																	
Archi réseau	I	I	R	C	C	A	R	I	C	I	-	A	I	C	R	A	I
Plan d'adressage	I	I	R	C	I	A	R	I	I	I	-	A	I	C	R	A	I
Protocoles Réseaux	I	I	R	C	I	A	R	I	I	I	-	A	I	C	R	A	I
Inventaire matériel	I	I	R	C	I	A	R	R	I	I	C	A	I	C	R	A	I
Cablage	I	I	A	I	I	C	I	A	I	R	C	A	I	C	A	R	I
FAI	I	R	C	I	I	A	R	I	I	I	A	A	I	C	C	A	I
Système																	
Sauvegarde	I	I	I	R	C	A	R	I	C	-	-	A	I	C	I	A	I
Téléphonie	I	R	I	R	I	A	R	I	I	R	-	A	I	C	I	A	I
Licences	I	R	I	R	I	A	R	I	I	I	C	A	I	C	I	A	I
Inventaires logiciels	I	I	I	R	C	A	R	I	C	-	-	A	I	C	I	A	I
Cyber																	
Tests pénétrations et vulnérabilités	I	I	I	I	R	A	R	I	A	-	-	A	I	C	I	A	I
Sécurité réseau IPS/IDS	I	I	R	I	R	A	R	I	A	-	-	A	I	C	R	A	I
SOC SIEM	I	I	I	I	R	A	R	I	A	-	-	A	I	C	I	A	I
Evaluation des PSSI	I	I	I	I	R	A	R	I	A	-	-	A	I	C	I	A	I
Evaluation DLP, WAF	I	I	I	I	R	A	R	I	A	-	-	A	I	C	I	A	I
Politique de sauvegarde des données	I	I	I	R	R	A	R	I	A	-	-	A	I	C	I	A	I
3. Proposition des solutions																	
Lots principaux																	
Archi réseau et services DHCP/DNS	I	I	R	C	I	A	R	I	I	-	-	A	I	C	R	A	I
Déploiement des postes clients	I	I	I	R	I	A	R	I	I	-	-	A	I	C	I	A	R
Migration des logiciels bureautique vers O365	I	I	I	R	I	A	R	I	I	-	-	A	I	C	I	A	R
Solution anti-virus centralisée	I	I	I	R	R	A	R	I	C	-	-	A	I	C	I	A	R
Système de prévention d'intrusion	I	I	R	I	R	A	R	I	C	-	-	A	I	C	R	A	I
Audit de sécurité	I	I	I	I	R	A	R	I	A	-	-	A	I	C	I	A	I
PRA / PCA	I	I	I	R	R	A	R	I	C	-	-	A	I	C	I	A	I
Monitoring et ticketing	I	I	I	R	I	A	R	I	I	-	-	A	I	C	I	A	R
Gestion de parc d'Informatique et Contrat de maintenance	I	I	I	R	I	A	R	I	I	-	-	A	I	C	I	A	R
Déploiements et mises à jour (OS et applications)	I	I	I	R	I	A	R	I	I	-	-	A	I	C	I	A	R

Lots supplémentaires																		
Stockage et sauvegarde	I	I	I	R	I	A	R	I	C	-	-	A	I	C	I	A	I
Annuaire LDAP	I	I	I	R	I	A	R	I	I	-	-	A	I	C	I	A	I
Virtualisation	I	I	I	R	I	A	R	I	I	-	-	A	I	C	I	A	I
Messagerie	I	I	I	R	I	A	R	I	I	-	-	A	I	C	I	A	I
Bases de données	I	I	I	R	I	A	R	I	I	-	-	A	I	C	I	A	I
VOIP	I	R	R	R	I	A	I	I	I	R	-	A	I	C	R	A	I
4. Contrat, commande et logistique																		
Contrat Fournisseurs	I	R	I	I	I	I	I	R	I	-	A	A	A	C	I	I	I
contrat prestatires	I	R	I	I	I	I	I	R	I	A	-	A	A	C	I	I	I
Commande matériel	I	I	I	I	I	I	I	A	I	-	R	A	A	C	I	I	I
Commande des liens opérateurs	I	R	R	I	I	A	I	I	I	-	R	A	I	C	R	A	I
Livraison matériel	I	I	I	I	I	I	I	A	I	R	R	A	I	C	I	I	I
5. Déploiement en test + Recette technique																		
Déploiement des Lots principaux + test unitaire																		
Archi réseau et services DHCP/DNS	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Déploiement des postes clients	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Migration des logiciels bureautique vers O365	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Solution anti-virus centralisée	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Système de prévention d'intrusion	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Audit de sécurité	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
PRA / PCA	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Monitoring et ticketing	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Gestion de parc d'Informatique et Contrat de maintenance	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Déploiements et mises à jour (OS et applications)	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
déploiement des Lots supplémentaires + test unitaire																		
Stockage et sauvegarde	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Annuaire LDAP	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Virtualisation	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Messagerie	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
Bases de données	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
VOIP	R	I	R	R	R	A	R	I	C	R	-	A	I	C	R	A	R
6. Déploiement en production																		
Déploiement																		
Validation de l'infrastructure	I	I	R	I	I	A	R	I	I	R	-	A	I	C	R	A	R
Installation des équipements	I	I	R	R	R	A	R	I	I	R	-	A	I	C	R	A	R
Mise en service	I	I	R	R	R	A	R	I	I	R	-	A	I	C	R	A	R
Recette technique																		
Elaboration des tests et réponses attendues	R	I	C	C	C	A	R	I	A	I	-	A	I	C	C	A	C
7. Recette finale																		
Tests client	I	R	I	I	I	I	I	I	A	I	-	A	I	C	I	I	I
Validation du PV recette	R	I	I	I	I	I	I	I	A	I	-	A	A	C	I	I	I
Contrat et support de maintenance	R	R	I	I	I	A	R	A	C	C	-	A	A	A	I	A	R
8. Mise en production + Formation																		
Formation utilisateurs	I	R	I	R	I	I	R	I	I	I	-	A	I	C	I	I	R
Rédaction du document d'ouvrage exécuté (DOE)	R	I	R	R	R	A	R	I	C	I	-	A	I	C	R	A	I
Nettoyage final	I	I	R	R	I	A	R	I	I	R	-	A	I	C	R	A	R

Figure 10 : Matrice RACI

6. Analyse et gestion des risques

La gestion des risques constitue une étape essentielle dans le projet de refonte du système d'information du Groupe Solaris. Elle vise à identifier les menaces potentielles, à évaluer leur impact, puis à définir des mesures préventives et correctives afin de garantir la réussite du projet en termes de coûts, délais, qualité et sécurité.

Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC)

Processus:	
Revu par :	
Le :	

IMPACT (I): de 1 impact négligeable à 10 impact catastrophique
PROBABILITE (P) : de 1 improbable à 10 presque inévitable
DETECTION (D) : de 1 détection presque certaine à 10 détection absolument incertaine
CRITICITE = I x P
RISQUE = I xP x D

Activités où Tâches du projet	Analyse des modes de défaillances actuelles									Recommandations			Mise en œuvre				
	Mode de défaillance potentielle	Effets de la défaillance potentielle	Date d'identification	IMPACT	Causes possibles de la défaillance	PROBABILITE	Contrôles actuels du processus	DETECTION	RISQUE	Actions recommandées	Porteur de l'action	Échéance	Actions mise en place	IMPACT	PROBABILITE	DETECTION	RISQUE
Refonte SI – Renouvellement infra	Obsolescence matérielle et logicielle	Interruption de service, incompatibilités		5	Vieillissement matériel, logiciels non maintenus	3	Sauvegardes, contrats de maintenance	2	30 %	Renouvellement progressif, virtualisation	Chef de projet IT		Tests de virtualisation lancés	1	1	1	1 %
	Manque de redondance / haute dispo	panne critique, indisponibilité totale du SI		5	Absence de PRA, absence de cluster	3	Sauvegardes, monitoring basique	3	45 %	Mise en place HA, PRA, sauvegardes renforcées	Responsable infrastructure		Renfort ponctuel déjà mobilisé	1	1	1	1 %
Gestion projet – Planification	Disponibilité limitée des équipes	Retard dans le projet, surcharge de travail		4	Sous-effectif, priorités concurrentes	4	Planification initiale	2	32 %	Recours prestataires externes, formation ciblée	Chef de projet + RH		Renfort ponctuel déjà mobilisé	1	1	1	1 %
Approvisionnement matériel	Retard d'approvisionnement	Décalage du calendrier projet		3	Dépendance fournisseur unique	3	Suivi commandes	2	18 %	Anticipation commandes, multi-fournisseurs	Responsable achats		Double fournisseur sélectionné	1	1	1	1 %
Gestion prestataires	Dépendance vis-à-vis des prestataires	Retard ou qualité insuffisante des livrables		3	Mauvaise contractualisation	3	Contrats existants	2	18 %	SLA précis, suivi rigoureux des livrables	Chef de projet		Suivi mensuel mis en place	1	1	1	1 %
Gestion RH	Absence ou départ d'un membre clé	Perte de compétences critiques		4	Départ imprévu, maladie	3	Documentation partielle	3	36 %	Plan de remplacement, documentation exhaustive	Responsable RH		Documentation centralisée	1	1	1	1 %
Risque lié aux Fournisseurs de Liens (Accès)	Retard de livraison des nouveaux liens d'accès par les opérateurs	Décallage du planning projet, retard de mise en service		4	Délais opérateurs non maîtrisés, indisponibilité ressources	3	Suivi planning théorique opérateurs	3	36 %	Commander liens très en amont, contractualiser pénalités de retard, prévoir liaison de secours	FAI		Commandes passées avec dates contractuelles	1	1	1	1 %
Risque de Migration et Bascule	Retard de livraison des nouveaux liens d'accès par les opérateurs	Décallage du planning projet, retard de mise en service		4	Délais opérateurs non maîtrisés, indisponibilité ressources	3	Suivi planning théorique opérateurs	3	36 %	Commander liens très en amont, contractualiser pénalités de retard, prévoir liaison de	NetPro consulting		Commandes passées avec dates contractuelles	1	2	1	2 %
Continuité activité	Indisponibilité des locaux (incendie, inondation, autorisation prefecturale)	Arrêt total d'activité		5	Sinistre, catastrophe naturelle	2	Sauvegardes internes	3	30 %	PRA/PCA, sauvegardes externalisées, site de secours	Direction générale		PRA déjà en test	1	2	2	4 %

Tableau 5 : Analyse des risques

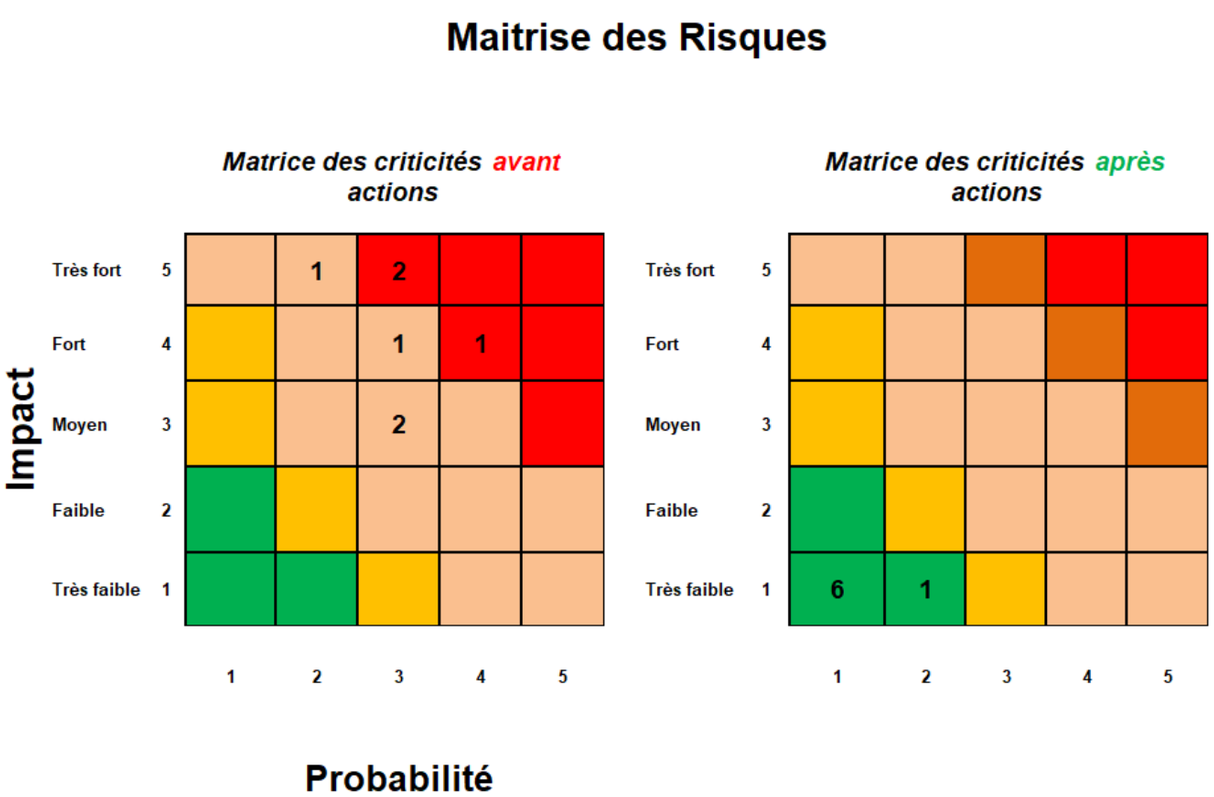


Figure 11: Matrice des risques

IV. AUDIT ET ANALYSE

A. Audit et Analyse Réseau

1. Architecture réseau

L'architecture réseau du groupe Solaris demeure cohérente dans son ensemble. Toutefois, plusieurs failles de sécurité sont à relever.

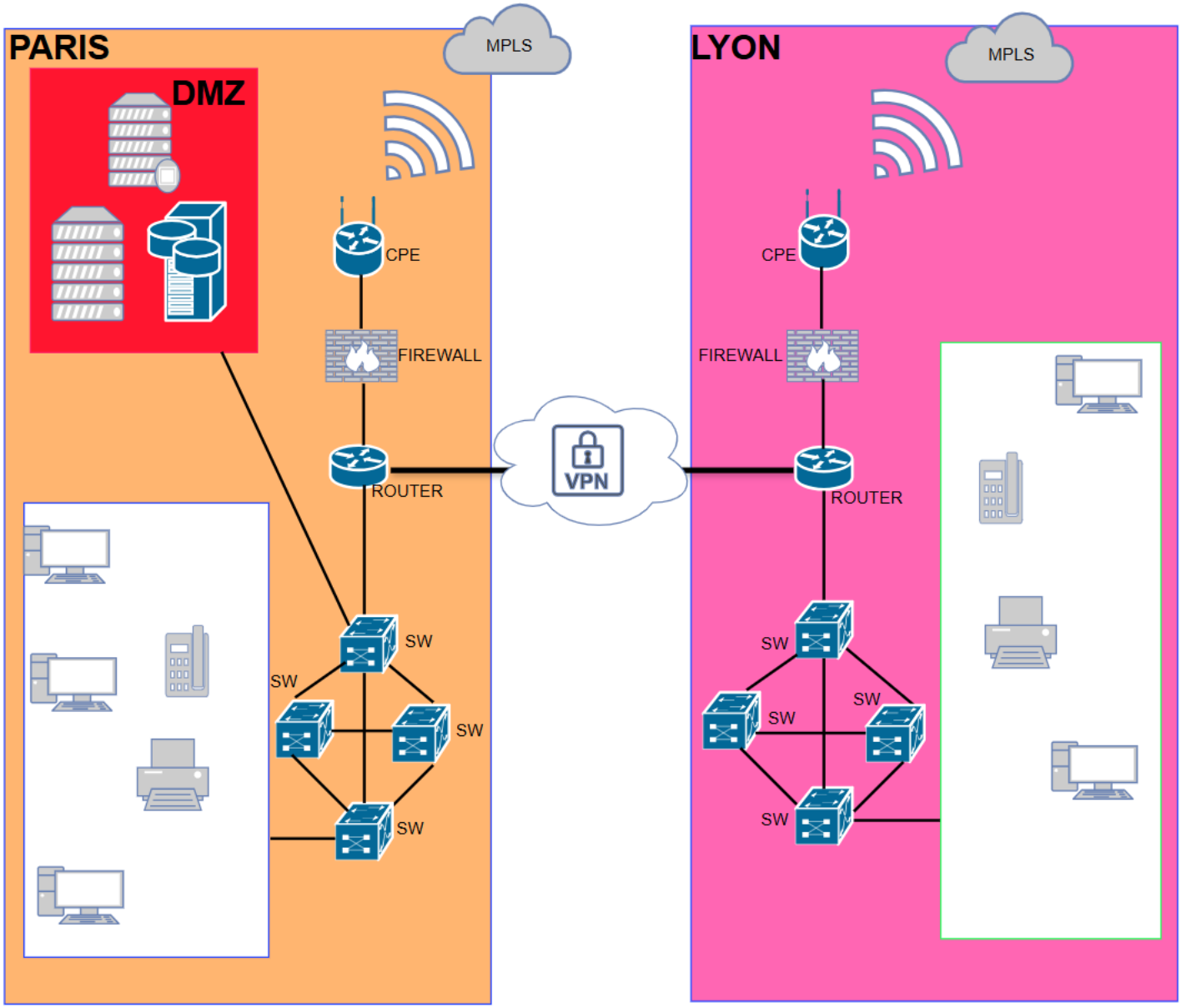


Figure 12 : Architecture réseau existante

2. Plan d'adressage

Le plan de découpage réseau est globalement cohérent en ce qui concerne la répartition des vlans. Bien que nous constations une absence de segmentation réseau entre les différents services.

Vlan n°	Service	@Réseau	@Masque	Plage d'adressage	@ Diffusion	Hôtes disponibles
Siège Paris						
10	VLAN GUEST	172.16.1.0	/24	172.16.1.1 - 172.1.1.254	172.16.1.255	254
20	VLAN LAN	192.168.0.0	/22	192.168.0.1 - 192.168.3.254	192.168.3.255	1022
30	VLAN IMPRIMANTE	192.168.4.0	/23	192.168.4.1 - 192.168.5.254	192.168.5.255	510
Site Lyon						
40	VLAN GUEST	172.17.0.0	/24	172.17.0.1 - 172.17.0.254	172.17.0.255	65 534
50	VLAN LAN	192.168.8.0	/22	192.168.8.1 - 192.168.11.254	192.168.11.255	1022
60	VLAN IMPRIMANTE	192.168.12.0	/23	192.168.12.1 - 192.168.13.254	192.168.13.255	510

Tableau 6 : Plan d'adressage existant

3. Protocole

a. DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole de type client/serveur qui permet d'attribuer automatiquement à un hôte une adresse IP, ainsi que d'autres paramètres de configuration réseau, tels que le masque de sous-réseau et la passerelle par défaut Défini par les RFC 2131 et 2132, DHCP est une norme de l'IETF (Internet Engineering Task Force), basée sur le protocole BOOTP, avec lequel il partage de nombreux aspects techniques et d'implémentation.

Ce protocole facilite la configuration réseau des hôtes en leur fournissant automatiquement les informations nécessaires pour fonctionner avec le protocole TCP/IP.
Dans l'infrastructure actuelle, les services DHCP sont hébergés sur deux serveurs virtuels Windows Server 2016, chacun dédié à l'un des deux sites.

b. Protocole STP

Le **STP** (*Spanning Tree Protocol*), ou **protocole Spanning Tree**, est un protocole réseau de couche 2 qui permet d'éviter les boucles de commutation dans un réseau Ethernet comportant des

liaisons redondantes. Il repose sur **l'algorithme de l'arbre recouvrant**, défini par **Radia Perlman en 1985**, et est normalisé sous le **IEEE 802.1D.**

Une étude plus approfondie de ce protocole sera faite dans la rubrique **Solution réseau**

c. Protocole VTP

Il s'agit d'un protocole conçu pour simplifier la gestion centralisée des VLANs au sein du réseau.Les commutateurs de cœur de réseau (backbone) sont configurés en mode VTP serveur, tandis que les switchs Cisco 2960 fonctionnent en mode VTP client.

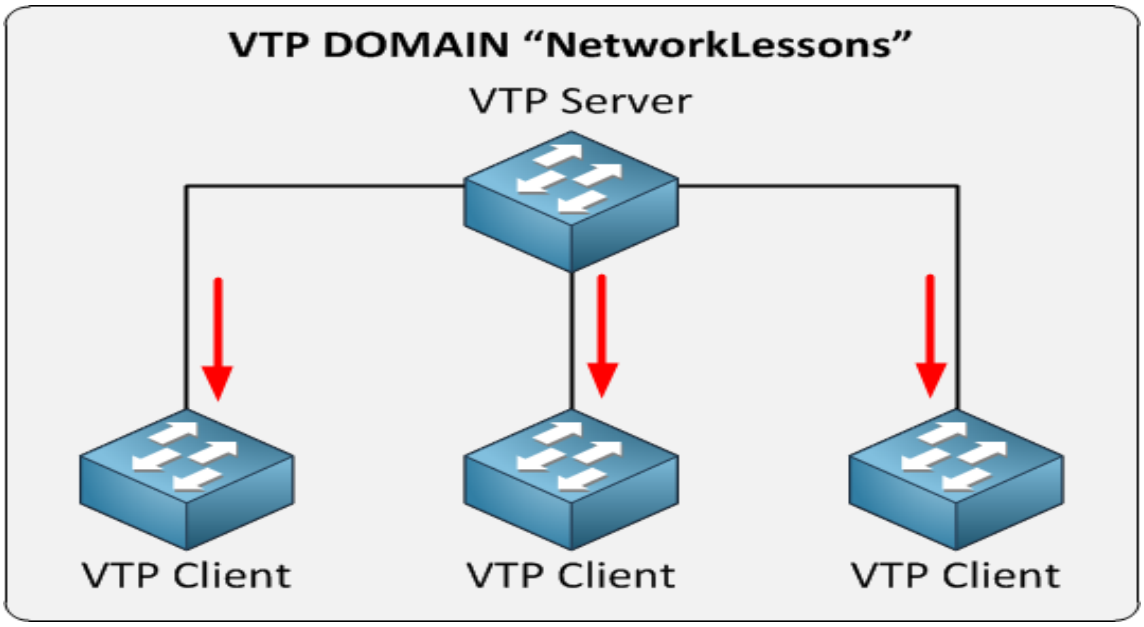


Figure 13 : Protocole VTP

4. Inventaire matériels réseau

Élément	Site de Paris	Site de Lyon	Modèle	Remarques
Nombre d'utilisateurs	850	130		
Switches (24 ports)	15 switches	3 switches	C 2960	Capacité suffisante avec réserve Interconnectés entre eux et au cœur réseau
Switches (24 ports)	13 switches	2 switches	C 3560	
Switches (24 ports)	11 switches	2 switches	C 3750	
Switches (32 ports)	3 switches	1 switch	C 3850	
Switches (32 ports)	2 switches	0	Juniper EX4500	
Points d'accès Wi-Fi	24 AP Wi-Fi	6 AP Wi-Fi	C 9105	Cisco WAP581
Points d'accès Wi-Fi	25	10	HPE Aruba AP-215	Un point d'accès professionnel bi-bande (2,4 GHz et 5 GHz)
CPE (équipements opérateur)	1	1	Cisco 877	Fournis par l'opérateur télécom
Pare-feu (firewalls)	1	1	Cisco ASA 5506X	Ancienne génération
Routeurs	1	1	Cisco 1841	Pour liaison WAN / Internet

Téléphonie IP	500	75	Cisco Unified, série 6901	Utilisation téléphonique simple est suffisante
Téléphonie IP	350	90	Grandstream GXP-2130	un téléphone IP professionnel doté de 3 lignes
Distance entre switches d'accès et distribution	>= 100 m (Backbone)	Idem		Respect des normes Ethernet (1000BASE-T)

Tableau 7 : Inventaire matériels réseau

5. Salle de serveur, Câblage et baie de stockage

La société Solaris dispose d'une infrastructure serveur diversifiée et répartie comme suit :

- **Un serveur dédié** à l'hébergement de l'application métier propre à Solaris ;
- **Deux serveurs Linux** hébergeant l'application ERP, utilisée par les services Ressources Humaines, Comptabilité et Commercial, ainsi que la base de données Oracle associée ;
- **Un serveur de fichiers** sous Windows Server 2016 assurant le stockage des répertoires personnels des utilisateurs et des partages de fichiers communs à chaque service ;
- **Une dizaine de serveurs rack** hébergeant les services de messagerie, les applications web, un serveur de fax, ainsi que les bases de données associées aux applications métiers et à l'ERP ;
- **Une baie de stockage** unique centralise l'ensemble des données ;
- **Deux robots de sauvegarde** sont présents pour assurer la protection des données.

En raison de la sensibilité et de la charge thermique générée par ces équipements, il est impératif que la salle serveurs soit équipée d'un système de climatisation fiable et opérationnel.
Un test approfondi a été réalisé sur l'ensemble de l'infrastructure réseau de Solaris.
Plusieurs vulnérabilités majeures ont été identifiées :

- **Absence de tolérance aux pannes** : Aucun dispositif de haute disponibilité ou de redondance n'est en place. Une panne même mineure, pourrait avoir des conséquences critiques sur la production.
- **Protocole de routage obsolète** : Le réseau utilise IGRP, un protocole de routage classful à vecteur de distance, désormais dépassé. Ce protocole ne prend pas en charge CIDR ni VLSM, ce qui empêche une utilisation optimisée des adresses IP. Il est également propriétaire et peu efficace en cas de congestion.
- **Équipements réseau obsolètes ou hors garantie** : Une grande partie du matériel réseau n'est plus couvert par la garantie constructrice, voire techniquement obsolète. De plus, l'infrastructure souffre d'un manque d'homogénéité technologique, entraînant des difficultés de maintenance et de compatibilité.
- **Câblage inadapté :** Le réseau repose exclusivement sur des câbles de catégorie 4 et 4e, limitant fortement les débits et les performances réseau. Ce type de câblage est incompatible avec les exigences actuelles en matière de bande passante**.**
- **Firewall obsolète** : Le pare-feu en place n'est plus maintenu par son constructeur, les mises à jour de sécurité ne sont plus disponibles. Cela représente une faille critique**,** exposant l'ensemble du système aux risques d'intrusion, de malware ou d'attaque ciblée.

6. FAI

Type de connexion : ADSL

Débit réel mesuré : 100 Mbps download / 60 Mbps upload

Technologie d'accès : routeur Netgear DG834G v4 obsolète. Plus de mise à jour depuis plus de 10 ans.

Fiabilité constatée :

- Coupures fréquentes / lenteurs en heures de pointe
- Latence élevée lors de l'utilisation de la visioconférence / VPN

Sécurité :

- Pas de pare-feu dédié / règles mal définies
- Absence de filtrage avancé

Disponibilité :

- Pas de lien de secours / SLA non respecté

7. Téléphonie IP

La solution actuellement utilisée par Solaris repose sur **Acrobits Softphone**, une application iOS de téléphonie VoIP. Cependant, cette technologie est aujourd'hui obsolète et ne répond plus aux exigences opérationnelles, technologiques et sécuritaires actuelles. Les limitations identifiées :

- Manque de mobilité multi-plateforme ;
- Absence d'intégration Cloud et outils collaboratifs ;
- Fonctionnalités limitées, l'absence de mise à jour régulière, de gestion des identités centralisée (SSO/MFA) et application non conçue pour des déploiements à grande échelle ;

B. Audit et Analyse système

1. Inventaire matériels système

Le Groupe Solaris dispose de plusieurs éléments d'infrastructure informatique, notamment des serveurs applicatifs, un serveur de fichiers, une dizaine de serveurs en rack dédiés à la messagerie, aux applications web, aux services de fax ainsi qu'aux bases de données. Le présent audit a pour objectif de dresser un état des lieux des équipements et ressources existants au sein du système d'information du Groupe Solaris.

Équipements	Service et matériel informatique	Support	Commentaire
Active Directory	Environnement Windows Server 2016		Version ancienne
Messagerie	MS Exchange 2013		Obsolescence/ Fin de support 11-avr-2023
Applications Métier	PolarisAid & SolarisAid (CRM et intranet)		Dépendance forte, base SQL 2012 obsolète
500 PC	Pc Portable HP Core i5 8GB RAM 500GB SSD		La configuration du PC est bonne mais le système doit être migré à W11
350 PC	Pc Asus Core i5 8GB RAM 500GB SSD		La configuration du PC est bonne mais le système doit être migré à W11
125 PC	Pc Acer Core i3 8GB RAM 250GB SSD		Configuration très faible pour supporter W11

120 PC	Pc Lenovo Core i3 8GB RAM 250GB HDD		Configuration très faible pour supporter W11
1100 Moniteur	Tour HP Core i3 8GB RAM SSD		Configuration très faible pour supporter W11
575 Téléphonie IP	Acrobit Softphone		Fin de support 06-jun-2018 Technologie pertinente, mais elles manquent aujourd'hui de nombreuses fonctionnalités modernes
465 Téléphonie IP	Acrobit Softphone		
440 Téléphonie IP	Grandstream GXP-2130		Acheté 2020
48 WIFI	Cisco WAP581 Wireless-AC Dual Radio Wave 2 Access Point with 2.5GbE LAN		Fin de support 03-Août-2021
35 WIFI	HPE Aruba AP-215		Fin de support 2018
Bases de données	SQL Server 2012, Oracle		Versions obsolètes
Systèmes Linux	2 serveurs applicatifs (RH, finance, etc.)		Supervision, mises à jour non précisées
Serveur de fichiers	Windows Server 2016		Accès, sauvegardes ? Sauvegarde centralisée ?
Infrastructure physique	Baie de stockage unique		Risque de panne
Sauvegardes	2 robots de sauvegarde, bandes stockées au sous-sol		Risques incendie/inondation, restauration non testée
2 serveurs	Veeam Backup & Réplication 7.5		Fin de support 01-01-2019
10 serveurs	SAN		Changer les disques
4 Serveurs	HP Storageworks D2700 6G SAS 3G SATA Plateau de Disque pour 25x 4TB		Toujours en Bon Etat
18 switches	Cisco Catalyst 2960		Fin de support 2021
15 switches	Cisco Catalyst 3560		Fin de support juillet-2015
13 switches	Cisco Catalyst 3750		Fin de support juillet-2015
4 switches	Cisco Catalyst 3850		Fin de support Oct-2025
2 switches	Juniper EX4500		Fin de support 30-juin-2024
Serveurs rack	10 serveurs (messagerie, web, fax, bases métier)		Configuration hétérogène, pas de virtualisation précisée
480 Cameras	Cisco vidéo Surveillance 7000 Series IP Cameras		Fin de support 31-oct-2023
Navigateurs	IE Internet Explorer 7 V.7.00.6		Failles de sécurité critiques, incompatibilités web. Fin de support 10-oct-2023

Navigateurs	IE Internet Explorer 9 V.9.0		Failles de sécurité critiques, incompatibilités web. Fin de support 14-jan-2020
Logiciel	Adobe CS3		Fin de support 31-Mai-2014
Logiciel IMove	Apple création vidéo		IMove
Logiciel Final Cut Pro 7	Apple création vidéo		Obsolète depuis 2011
Firewall	Licence Firewall		Expire en 2025
23 Imprimantes	Imprimantes Brother MFP		Les drivers ne sont plus disponibles
68 Imprimantes	Imprimantes CANON MFP		Les drivers ne sont plus disponibles
14 Imprimantes	Imprimantes HP LaserJet		Achetée en 2022
1100 Environnement bureautique	MS Office 2007		Fin de support 09-09-2012
940 Environnement bureautique	MS office 2016		Fin de support le 13 octobre 2020
Environnement bureautique	OpenOffice		Fin de sortie des patchs jan-2011

Tableau 8 : Inventaire système

Support de base en cours	
Bientôt à expiration	
Fin de support	

2. Licences

Solaris a déployé une solution de sécurité intégrant des licences antivirus pour les postes serveurs (y compris Veeam Backup & Replication 7.5 et le serveur NAS) ainsi que pour les postes de travail, accompagnés des suites Microsoft Office 2007 et 2016.
Toutefois, deux points de vigilance sont à noter :

- Office 2007, obsolète depuis 2017, représente une faille de sécurité importante.
- Un antivirus expiré ou non mis à jour expose les postes aux menaces, faute de définitions virales à jour.

3. Sauvegarde

Solaris à une bonne solution de sauvegarde qui repose sur Veeam Backup & Replication 7.5, installée sur deux serveurs physiques configurés en haute disponibilité (HA).
Ce déploiement vise à garantir la continuité de service et la résilience de l'infrastructure : en cas de défaillance de l'un des serveurs, le second prend automatiquement le relais.
Les deux serveurs partagent un stockage centralisé et synchronisé, basé sur un SAN servant de repository pour les sauvegardes.
Cependant, malgré la redondance des serveurs, cette architecture présente une dépendance critique au stockage partagé :

En cas de panne du SAN, les deux serveurs Veeam deviennent inopérants, rendant la haute disponibilité inefficace dans ce scénario.
Par ailleurs, Veeam 7.5 ne prend pas en charge le clustering natif de ses services. La haute disponibilité doit donc être assurée via une couche externe, comme un hyperviseur avec VMware HA ou un cluster de bas niveau.

Enfin, l'infrastructure Veeam n'est pas isolée du reste du réseau, elle peut devenir une cible prioritaire des ransomwares, qui visent fréquemment les environnements de sauvegarde.

C. Audit et Analyse de sécurité

L'audit mené au sein du Groupe Solaris et de ses sites distants a mis en évidence plusieurs faiblesses notables, notamment en matière de :

- Vulnérabilités au niveau du réseau
- Vulnérabilités au niveau des systèmes

1. Vulnérabilités réseau

L'architecture réseau du groupe Solaris présente plusieurs failles de sécurité parmi lesquelles :

- **DMZ**

Bien que le client ait mis en place une DMZ, celle-ci est configurée sur le même segment réseau que le LAN. Ce qui crée une faille de sécurité importante.

- **Wifi**

Le client a installé deux réseaux distincts : interne et invité. Le réseau interne reste connecté au LAN principal du client, ce qui constitue un risque en matière de sécurité.

- **Connexion VPN**

La connexion VPN entre les deux sites repose sur un protocole IPsec site-to-site, offrant une sécurité solide, mais cette configuration rend l'ajout d'un nouveau site côté client complexe.

- **Plan d'adressage**

Nous avons constaté que le nombre d'hôtes alloués à chaque VLAN est largement surdimensionné, ce qui entraîne un gaspillage significatif d'adresses IP sur l'ensemble des VLANs des différents sites. Cette surallocation peut également provoquer des latences significatives sur le réseau, notamment lors des diffusions broadcast.

- **Mise à jour**

Plusieurs équipements réseau sont obsolètes et ne reçoivent plus les mises à jour nécessaires, ce qui constitue une vulnérabilité majeure sur le plan de la sécurité.

2. Vulnérabilités système

Les vulnérabilités identifiées au sein du système d'information mettent en évidence plusieurs insuffisances qui empêchent le groupe Solaris disposer d'une infrastructure optimale, en adéquation avec ses besoins métiers.

- **Serveur de base de données SQL**

L'application SolarisAid repose sur une architecture vieillissante, combinant un serveur d'application dédié, des bases de données SQL Server 2012 (en fin de support) et Oracle, le tout intégré à un environnement Active Directory 2016. Cette infrastructure présente plusieurs limites : une scalabilité réduite, une absence de redondance, des technologies obsolètes exposées à des failles de sécurité, et une difficulté à évoluer vers des standards modernes (cloud, microservices, cybersécurité). La fin de support du serveur SQL, pièce centrale du système, accentue les risques d'interruptions et de non-conformité.

- **Active Directory**

Les serveurs Active Directory sont isolés sur chaque site, ce qui complique la centralisation et la gestion des données. Par ailleurs, ces serveurs remplissent également la fonction de serveur de fichiers, ce qui pose un problème de séparation des rôles.

- **Stockage et sauvegarde**

La centralisation des sauvegardes ne garantit pas la récupération des données en cas de sinistre majeur, comme un incendie au siège du groupe Solaris. Cette situation met en péril la continuité d'activité.

- **Systèmes d'exploitation**

Un grand nombre de postes clients et de serveurs fonctionnent encore sous des systèmes d'exploitation obsolètes, dont le support par les éditeurs n'est plus assuré. Cela constitue un risque de sécurité majeur.

- **Antivirus**

Bien que les licences antivirus soient à jour, l'absence de centralisation de la console d'administration limite considérablement la gestion des exceptions, des autorisations et le déploiement de politiques de sécurité homogènes.

- **GPO (Group Policy Object)**

Les GPO mises en place ne sont pas structurées de manière à faciliter leur évolution. Cette organisation complexe complique l'intégration de nouveaux collaborateurs en fonction de leur rôle ou de leur service.

D. Résumé de l'audit et l'analyse

L'infrastructure réseau et système du Groupe Solaris présente une base fonctionnelle mais souffre de nombreuses obsolescences, de failles de sécurité, et d'un manque de flexibilité pour l'évolution. Des mises à jour matérielles et logicielles, ainsi qu'une restructuration des rôles, VLANs et politiques de sécurité, sont fortement recommandées pour garantir la pérennité et la sécurité du système d'information.

Comment adapter l'infrastructure système et réseau du Groupe Solaris, aujourd'hui obsolète et rigide, aux besoins actuels et futurs de l'entreprise ?

IV. SOLUTION

A. Lot A : Solution Réseau

Dans le cadre de l'évolution de l'infrastructure informatique de Solaris, un audit réseau a été mené afin d'évaluer l'état actuel du système, d'identifier les points de défaillance potentiels et de proposer une architecture plus robuste, performante, résiliente et évolutive.

Cet audit a mis en lumière plusieurs enjeux clés :

- La nécessité de garantir une **haute disponibilité** des services critiques ;
- L'importance de **renforcer la sécurité** du réseau, notamment au niveau des interconnexions entre sites et des accès distants ;
- La centralisation de la **DMZ au niveau du siège**, ce qui impose une interconnexion efficace et sécurisée avec les autres sites ;
- Le besoin d'un réseau **plus facilement administrable et scalable**, en adéquation avec la croissance de l'activité ;

En réponse à ces constats, nous proposons une nouvelle **architecture réseau hiérarchique à 3 niveaux** qui garantir la **CID** (**C**onfidentialité, **I**ntégrité et la **D**isponibilité) de l'information. Cette architecture intègre les équipements **Cisco Meraki MX250 (**Siège) et **MX100 (**site de Lyon) pour la sécurité et l'interconnexion entre les sites.

1. Présentation des équipements

d. Switch WAN : Arista 7280R-16

C'est un équipement réseau de couche 2 qui joue un rôle clé dans la gestion des connexions WAN. Il nous permettra de regrouper les 2 liens WAN sur un même équipements (switch Wan) essentielle pour configurer la redondance sur nos MX.

Figure 14 : Arista 7280R-16

e. Meraki MX 250/100

Solution tout-en-un pour réseaux d'entreprise offrant :

- **Pare-feu nouvelle génération** (NGFW) avec inspection approfondie du trafic
- **Gestion unifiée** via plateforme cloud Meraki
- **Connectivité SD-WAN** basée sur SDN pour :
  - Interconnexion automatique des sites
  - Optimisation des liens multiples (MPLS, Internet, 4G)
  - Qualité de Service intégrée

PERFORMANCES	CONNECTIVITE	REDONDANCE & HA
Débit Firewall : 2 Gbps	2 ports WAN SFP+	Mode HA : Actif/passif
Débit VPN : 4 Gbps	8 ports LAN SFP+	Mode HA : Actif/Actif
Débit du Pare-feu NAT : 7,5 Gbps	8 ports LAN SFP	WAN Failover
Nombre d'appareils recommandés : 2 000	8 ports GigaEthernet RJ45	

Tableau 9 : fiche technique MX250

Figure 15 : Meraki MX 250

f. Switch Core : C9500-24Y4C

Rôle principal : Transport rapide et fiable du trafic entre les différents bâtiments, étages ou parties du réseau.

- **Fonction :** C'est la « colonne vertébrale » (backbone) du réseau.
- **Caractéristiques :**

- Haute capacité de commutation et faible latence ;
- Intègre les fonctionnalités de niveau 3 (routage) pour interconnecter les VLANs et sous-réseaux ;
- Pas ou très peu de fonctions d'accès utilisateur ;
- Redondance maximale (alimentation, liens, châssis) ;
  - **Objectif :** Acheminer rapidement de gros volumes de trafic entre zones, avec fiabilité.

Figure 16 : C9500-24Y4C

C9500-24Y4C: Cisco Catalyst 9500 Series high-performance switch with 24x 1/10/25G Gigabit Ethernet + 4x 40/100G Uplink

g. Switch de distribution : C9500-48Y4C

Rôle principal : Point intermédiaire qui agrège le trafic venant des switches d'accès et applique les politiques réseau.

- **Fonction :**

- Agréger plusieurs switches d'accès.
- Effectuer le routage inter-VLAN (équipement de coucheL3).
- Appliquer les politiques de sécurité (ACL, QoS).
- Fournir une redondance entre accès et cœur.

❖ **Caractéristiques :**

- Débit élevé, mais moins que le cœur.
- Peut implémenter des protocoles de redondance (HSRP, VRRP, GLBP).

❖ **Objectif :** Filtrer, contrôler et optimiser le trafic avant qu'il atteigne le cœur.

Figure 17 : C9500-48Y4C

C9500-48Y4C: Cisco Catalyst 9500 Series high-performance switch with 48x 1/10/25G Gigabit Ethernet + 4x 40/100G Uplink

h. Switch d'accès : Netgear GS752TSB

Rôle principal : Point de connexion directe des utilisateurs et équipements finaux.

❖ **Fonction :**

- Connecter les postes de travail, téléphones IP …
- Fournir l'alimentation PoE (Power over Ethernet) aux périphériques.
- Appliquer les VLANs pour séparer logiquement le réseau.

❖ **Caractéristiques :**

- Equipements de couche 2
- Support PoE/PoE+ pour périphériques.
- Nombre élevé de ports 52 RJ45.
- 4 Ports SFP dédiés pour l'uplink et le stack
- 2 ports combo cuivre/SFP

❖ **Objectif :** Fournir la connectivité physique et logique aux terminaux.

Figure 18 : Netgear GS752TSB

i. Différence entre switch core, distribution et accès

Niveau	Rôle principal	Fonctions typiques	Protocoles courants	Débit attendu	Exemples de modèles
Cœur (Core)	Backbone du réseau, transport rapide entre zones	Routage L3 haute vitesse, interconnexion des bâtiments/sites, redondance	OSPF, IS-IS, BGP, MPLS	Très élevé (40G, 100G, voire plus)	Cisco Nexus 9500, Catalyst 9600, Juniper QFX10000
Distribution	Agrégation des accès et application des politiques	Routage L3 inter-VLAN, filtrage ACL, QoS, agrégation LACP/MLAG, haute disponibilité	OSPF, EIGRP, HSRP, VRRP, GLBP	Élevé (10G, 40G)	Cisco Catalyst 9300/9500, Juniper EX4300/EX4600, Arista 7050X
Accès	Connexion directe des utilisateurs et périphériques	VLANs, PoE pour téléphones IP et Wi-Fi, filtrage L2, sécurité port-based (802.1X)	STP/RSTP/MSTP, VLAN 802.1Q, LACP	1G (par port), parfois 2.5G/5G	Cisco Catalyst 9200, 2960X, Juniper EX2300/EX3400

Tableau 10 : Tableau de comparaison entre les switchs accès, coeur et distribution

2. Présentation des liens d'accès : WAN

Nous procéderons au déploiement d'une double connexion Internet via la fibre optique, en faisant appel à deux opérateurs distincts. Cette configuration vise à garantir la redondance en cas de défaillance d'un des liens. Les liens d'accès seront de type fibre dédiée, à savoir **FTTO** (Fibre To The Office) et **FTTH**. Les opérateurs nous fourniront le **CPE** (Customer Premises Equipment). Pour une liaison FTTO, on parlera d'un RAD (Routeur d'accès aux données) et pour un lien FTTH on parlera soit de l'ONT.

Site	Paris	Lyon
Lien Principal	**FTTO** Orange : 3 Gbps	**FTTO** Bouygues : 1 Gbps
Lien Secondaire	**FTTO** Hub One : 2 Gbps	**FTTH** COVAGE : 1000 Mbps

Tableau 11 : lien d'accès

3. Présentation de quelques Protocoles

a. DHCP

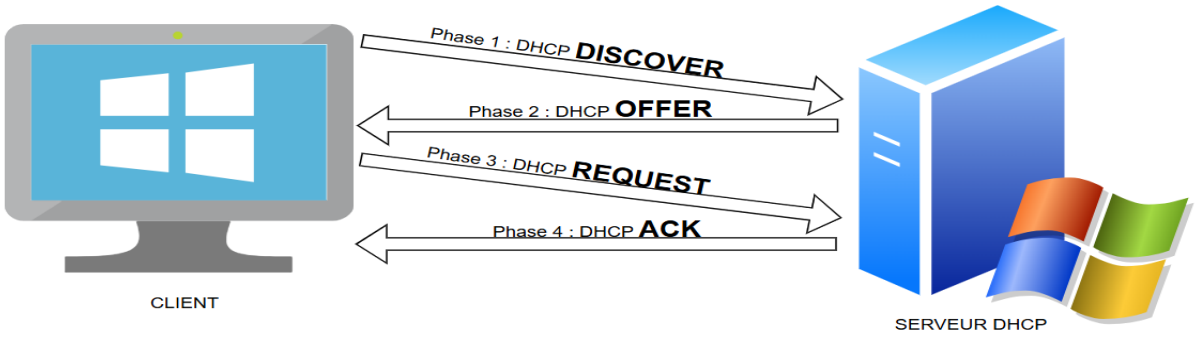


Figure 19 : principe DHCP

Le **DHCP** (Dynamic Host Configuration Protocol) est un protocole réseau qui permet d'attribuer automatiquement à un poste client une adresse IP ainsi que d'autres paramètres réseau, tels que le masque de sous-réseau et la passerelle par défaut.

Normalisé par l'**IETF** dans les **RFC 2131** et **RFC 2132**, il facilite la configuration TCP/IP des machines en leur fournissant dynamiquement les informations nécessaires via un serveur DHCP.

b. Protocole STP

Le **STP** (*Spanning Tree Protocol*), ou protocole Spanning Tree, est un protocole réseau de couche 2 qui permet d'éviter les boucles de commutation dans un réseau Ethernet comportant des liaisons redondantes. Il repose sur **l'**algorithme de l'arbre recouvrant, défini par Radia Perlman en 1985, et est normalisé sous le IEEE 802.1D**.**
Ce protocole comprend 5 états à savoir :

- **Blocking (BLK)**
  - Le port ne transmet pas de données, mais écoute les BPDUs ;
  - Aucune donnée utilisateur n'est transmise ;
- **Listening**
  - Le port écoute activement les BPDUs et participe à l'élection du réseau.
  - Pas encore de transmission de données utilisateur.
- **Learning**
  - Le port apprend les adresses MAC à partir des trames reçues.
  - Il ne transmet pas encore de données, mais construit sa table MAC.
- **Forwarding (BLK)**
  - Le port transmet normalement les données utilisateur et les BPDUs.
  - Il est pleinement opérationnel dans le réseau.
- **Disabled**
  - Le port est administrativement désactivé ou hors service.
  - Il ne participe pas au STP.

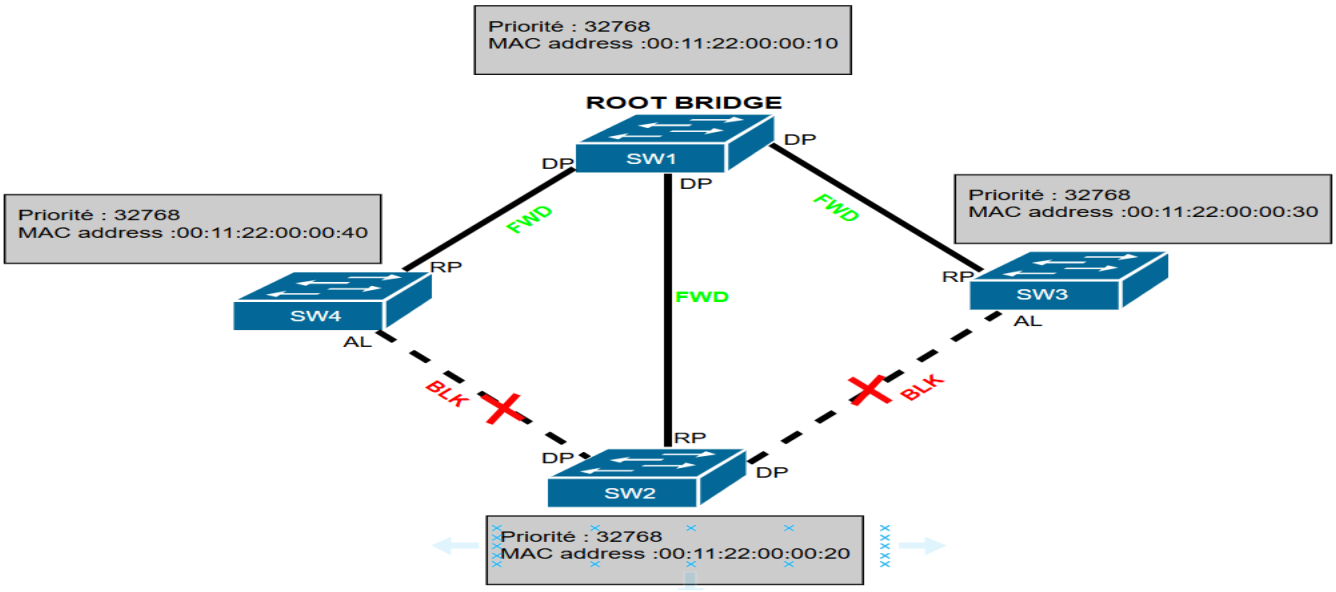


Figure 20 : protocole STP

c. DMZ

La DMZ est une zone réseau intermédiaire, placée entre le réseau interne (LAN) et l'Internet. Elle accueille les services accessibles depuis l'extérieur (publics), tout en protégeant le reste du réseau interne. Entre autres, on pourra citer :

- **Serveur web (HTTP/HTTPS)** : pour héberger le site web accessible au public ;
- **Serveur de messagerie (SMTP)** : pour envoyer/recevoir des e-mails ;
- **Serveur DNS** : pour la résolution de noms publique ;
- **Serveur FTP/SFTP** : pour le transfert de fichiers ;
- **Serveur proxy ou reverse proxy** : pour sécuriser et distribuer les requêtes vers les serveurs internes ;

L'objectif étant de limiter l'exposition du réseau interne aux menaces externes.

Avantages

- ✓ Protection du **réseau interne** en cas de compromission d'un service public.
- ✓ Limitation de la **surface d'attaque**.
- ✓ Gestion centralisée de la sécurité (pare-feu, IDS/IPS).

j. Tableau comparatif des protocoles STP

Protocole	États des ports	Timers par défaut	Convergence	Multi-VLAN support	Particularités
STP (802.1D)	Disabled, Blocking, Listening, Learning, Forwarding	Hello = 2s MaxAge = 20s Forward Delay = 15s	30s (chgt local)~50s (perte root)	Non (un seul arbre pour tout le réseau)	Standard d'origine (1988), très lent
PVST+ (Cisco)	Même que STP (802.1D)	Hello = 2s MaxAge = 20s Forward Delay = 15s	30–50s	Oui (1 instance STP par VLAN)	Propriétaire Cisco, utilise ISL/802.1Q
RSTP (802.1w)	Discarding, Learning, Forwarding	Hello = 2s(pas de Forward Delay)	1–3s	Non (un seul arbre global)	Amélioration de STP avec handshakes Proposal/Agreement
RPVST+ (Cisco)	Discarding, Learning, Forwarding	Hello = 2s	1–3s	Oui (1 instance par VLAN)	Propriétaire Cisco, combine RSTP + PVST+
MSTP (802.1s)	Discarding, Learning, Forwarding	Hello = 2s	1–3s	Oui (groupement de VLANs en instances STP)	Standard, scalable pour grands réseaux multi-VLAN

Tableau 12 : Tableau comparatif des protocoles STP

Pour des raisons de **haute disponibilité** et de **scalabité**, nous avons opté pour l'implémentation du protocole **MSTP** (**M**ultiple **S**panning **T**ree **P**rotocole).

d. Agrégations des liens

L'agrégation de liens consiste à regrouper plusieurs liens identiques, présentant les mêmes caractéristiques, en un seul lien logique.

Cette technique présente deux avantages majeurs :

- L'augmentation de la bande passante entre deux équipements
- La redondance : en cas de défaillance d'un lien, le trafic est automatiquement redirigé vers les liens restants, assurant ainsi la continuité du service sans interruption.

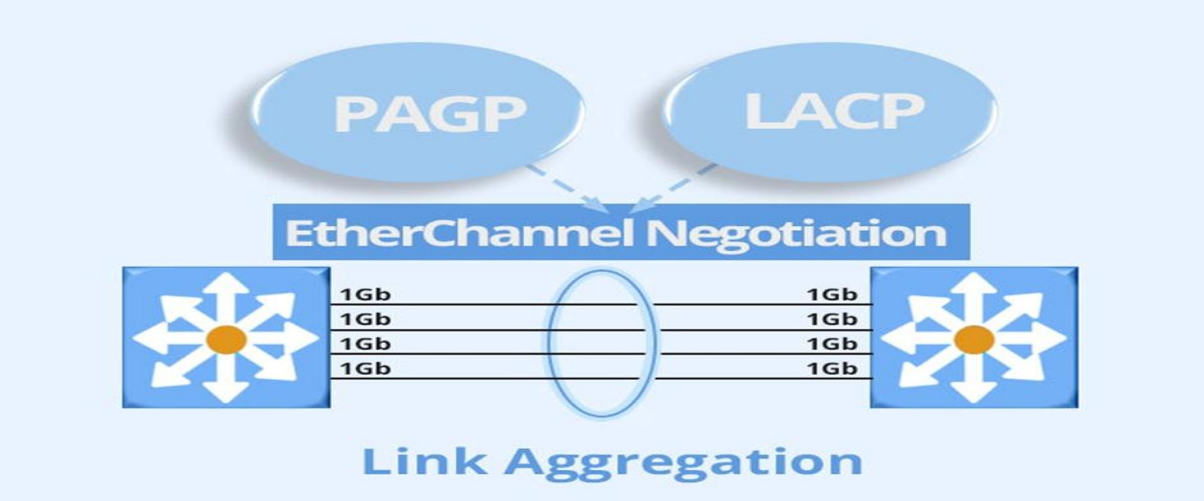


Figure 21 : Agrégation des liens etherchanel

e. MLAG

MLAG (**M**ulti-Chassis **L**ink **A**ggregation **G**roup) est une technologie qui permet de créer une agrégation de liens (**LACP**) entre un équipement en downstream (dans notre cas un routeur WAN) et deux switchs distincts vus comme un seul équipement logique.
Autrement dit, un port-channel (**LAG**) peut s'étendre sur deux switchs physiques, offrant **résilience** + **load-balancing**, sans protocole de bouclage (STP n'a pas besoin de bloquer les liens).

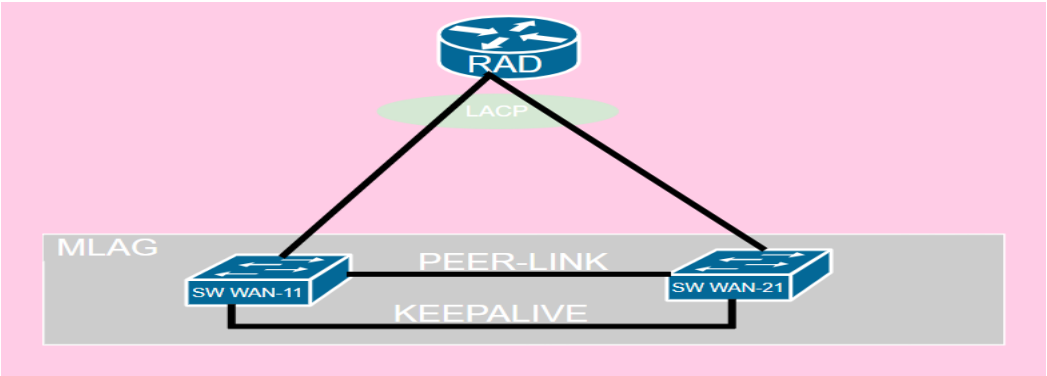


Figure 22 : Archi MLAG

Fonctionnement :

- **Switch Pair** : deux switchs forment un cluster MLAG.
- **Peer-Link** : un lien de synchronisation entre les deux switchs MLAG (échange des états MAC, ARP, etc.).
- **Keepalive Link** : lien de heartbeat pour détecter la perte d'un membre MLAG.
- **Downstream Devices** (RAD dans notre cas) configurent un **LACP port-channel** vers les deux switchs.

f. StackWise Virtuel

StackWise Virtual permet d'agréger deux switchs physiques (généralement de distribution ou cœur de réseau) pour qu'ils apparaissent comme un seul switch logique dans le réseau.
C'est une évolution du **VSS** (**V**irtual **S**witching **S**ystem) et une alternative au châssis modulaire.

Fonctionnement :

- Un switch est élu **Active** (contrôle le plan de management).
- L'autre est **Standby** (partage la table de forwarding et prend le relais si l'Active tombe).
- **Les deux switches transmettent le trafic (actif/actif)** au niveau des data-plane (contrairement à STP qui bloquerait un lien).
- Pour les équipements connectés (ex. serveurs, firewalls), les deux switchs forment **un seul point logique**.

Avantages :

✓ **Pas de boucle STP** : tous les liens sont actifs.
✓ **Redondance totale** (plan de contrôle + plan de données).
✓ **Gestion centralisée** : une seule configuration à maintenir.
✓ **Équilibrage de charge** via EtherChannel vers les deux switchs.

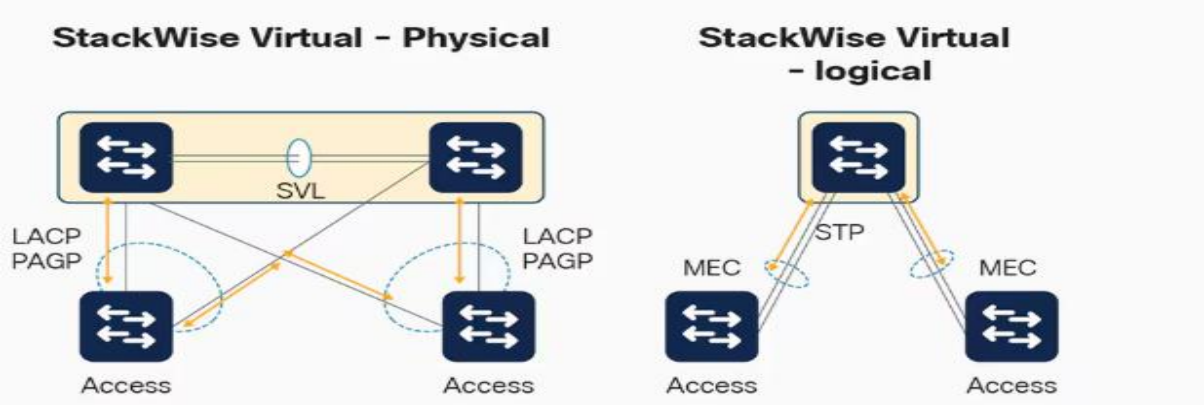
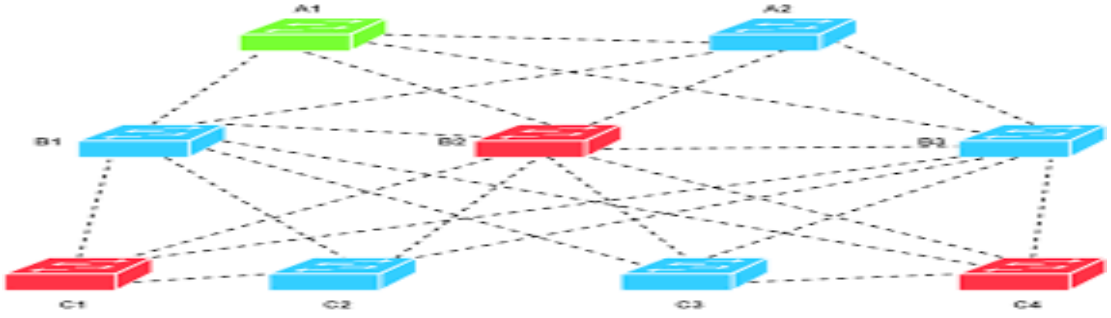


Figure 23 : Présentation Stackwise virtuel

MEC (Multi-Chassis **E**ther**C**hannel**)** : Liens vers des serveurs/équipements.

g. Protocol VTP

Le protocole VTP (**V**LAN **T**runking **P**rotocol) simplifie la gestion des VLANs dans un réseau commuté. Lorsqu'un nouveau VLAN est configuré sur un serveur VTP, celui-ci est automatiquement propagé à l'ensemble des commutateurs appartenant au même domaine VTP. Cela permet d'éviter une configuration manuelle répétitive sur chaque équipement du réseau.
VTP est un protocole propriétaire de Cisco, intégré à la majorité des commutateurs de la gamme Cisco Catalyst.



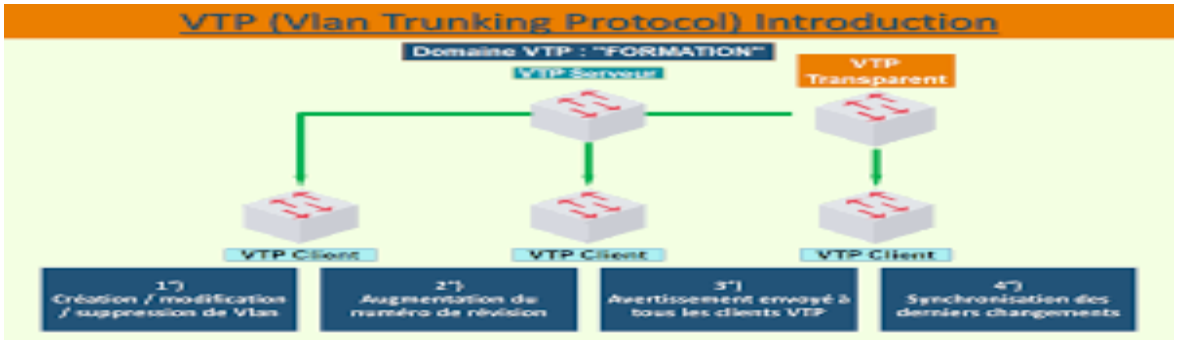


Figure 24 : protocole VTP

h. Protocole IPsec

IPSec est un ensemble de règles ou de protocoles de communication permettant d'établir des connexions sécurisées sur un réseau. Le protocole Internet (IP) est la norme commune qui détermine comment les données circulent sur Internet. IPSec ajoute le chiffrement et l'authentification pour rendre le protocole plus sûr.

Le **VPN** (**V**irtual **P**rivate **N**etwork) est un réseau privé virtuel qui permet aux utilisateurs de naviguer sur Internet de manière anonyme et sécurisée. Un VPN IPSec utilise le protocole IPSec pour créer des tunnels chiffrés sur Internet. Il fournit un chiffrement de bout en bout, ce qui signifie que les données sont brouillées sur l'ordinateur et décodées sur le serveur de réception.

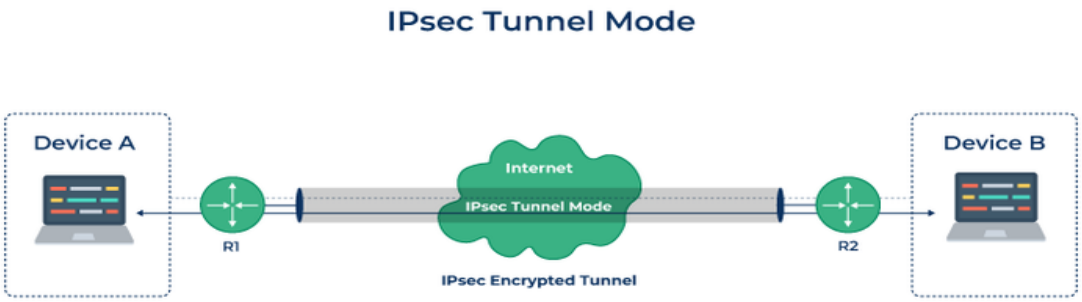


Figure 25 : Protocole IPsec

i. Autres protocoles

❖ **Portfast**

Portfast permet de mettre immédiatement un port en **état Forwarding** sans passer par les états **Listening** et **Learning**.

Portfast se configure uniquement sur les **ports d'accès** (connexion PC, imprimante, téléphone IP, serveur, etc.). Ainsi les ports d'accès ne reçoivent pas les échanges de BPDUs lors du changement de topologie.

Pourquoi l'activer sur les ports de connexion des PC ?

1. **Réduction du délai de 30 seconds imposés** par STP au démarrage : le PC a directement accès au réseau.

- Exemple : un PC qui démarre peut manquer son **bail DHCP** si STP bloque la communication pendant 30s.

2. **Meilleure expérience utilisateur** :

- Connexion plus rapide au réseau après démarrage ou branchement.
- Pas de coupure intempestive lors des reconnexions.

3. **Optimisation pour les postes terminaux** :

- Un PC n'introduit pas de boucle réseau : pas besoin que STP attende et calcule sur ce port.
- On réserve le vrai calcul STP pour les **liens entre switchs**.

❖ **Root Guard**

Root Guard est une fonctionnalité de sécurité du Spanning Tree Protocol**.** Son rôle est d'empêcher qu'un port ne devienne le **Root Port** et donc de protéger le Root Bridge légitime du réseau.

Fonctionnement

- STP élit un **Root Bridge** (le switch racine) en fonction de la **Bridge ID** (priorité + adresse MAC).
- Normalement, seul le switch choisi doit être Root.
- Mais si un switch non autorisé est branché avec une **priorité plus faible**, il peut **forcer l'élection** et devenir Root : cela perturbe tout le réseau.

En clair : Root Guard **verrouille le rôle de Root Bridge** sur l'équipement désigné par l'administrateur.

Si vous configurez un port avec **Root Guard** vers n'importe quel commutateur, chaque fois qu'un **BPDU supérieur** provient de ce commutateur, le port passe à l'état **ErrDisabled**. Cette BPDU supérieure peut provenir de n'importe quel commutateur non fiable ou d'un commutateur que vous ne souhaitez pas voir comme un **pont racine**. Par conséquent, vous utilisez la fonction STP **Root Guard** pour éviter cette situation. En d'autres termes, vous gérez les élections de pont racine.

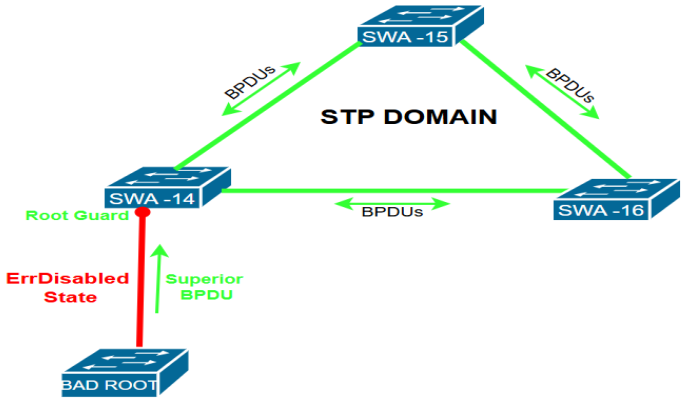


Figure 26 : Fonctionnement du Root Guard

4. Architecture réseau

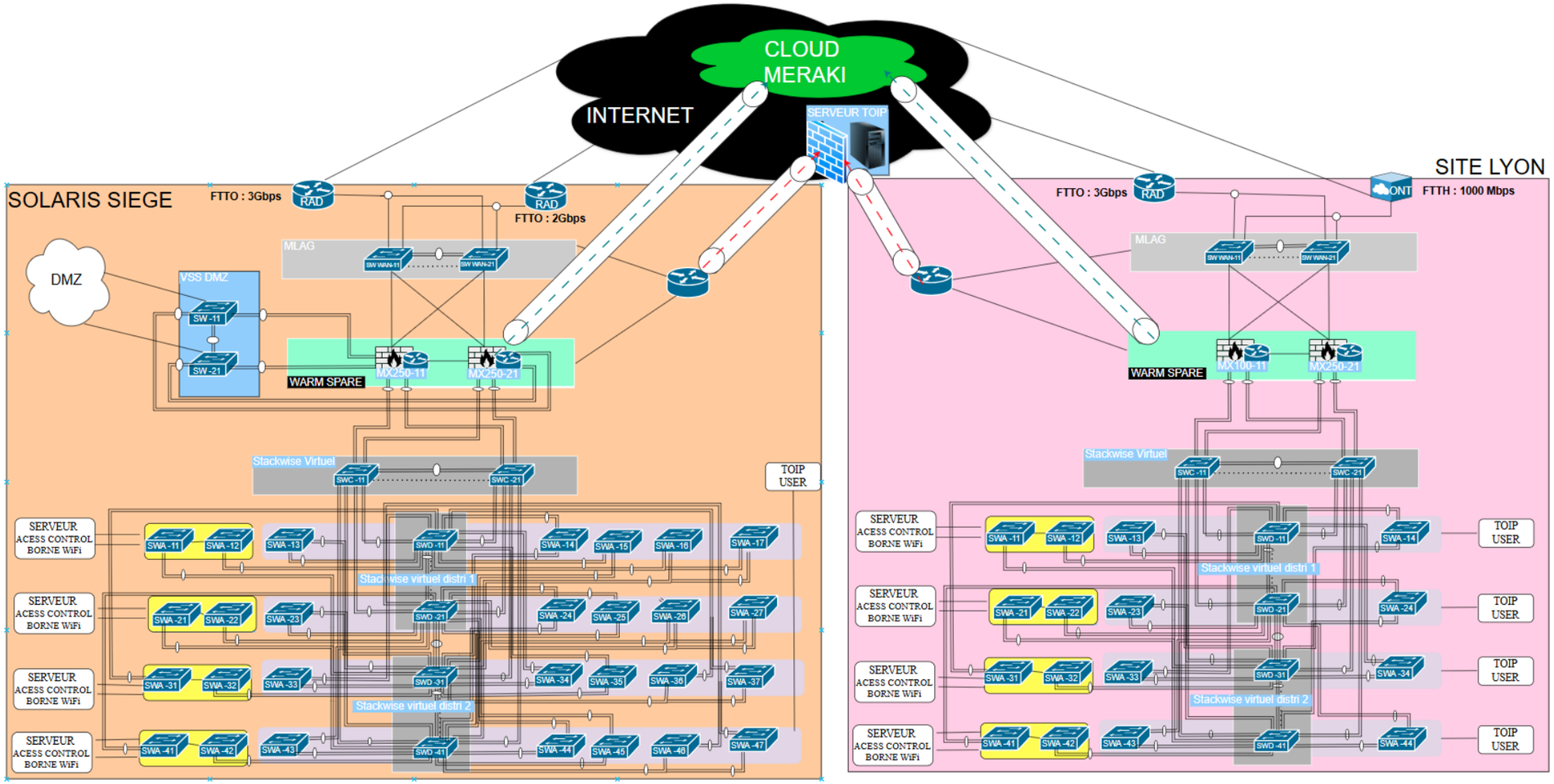


Figure 27 : Architecture Réseau

5. Plan d'adressage IP

Dans ce nouveau plan d'adressage, nous adoptons la notion de VLSM (Variable Length Subnet Masking), un adressage IP sans classe. Cette méthode, principalement utilisée dans les réseaux locaux, permet une gestion optimisée des sous-réseaux en adaptant le masque de sous-réseau à la taille réelle de chaque segment réseau.

Nous utiliserons le bloc d'adresses CIDR suivant : **172.168.0.0/16**

Par conséquent, nous passons de 3 à 16 VLANs, correspondant aux services et besoins suivants :

UTILISATEURS

Service	Nombre d'utilisateurs Paris	Nombre d'utilisateurs Lyon
Direction Générale	25	10
Pole juridique	10	5
Service comptable	40	10
Service commerciale	60	15
Pole RH	20	5
Direction communication et RSE	10	3
Direction des opérations	630	70
Direction Recherche et Développement	30	7
DSI	25	10
Imprimantes	10	5
DMZ	40	
Management des équipements	100	60
VOIP	900	150
Infra Wi-Fi	1500	200
Wifi Invité	350	150
LAN invité	100	100
Adresse réseau utilisé	**172.10.0.0/16**	**172.20.0.0/16**

Tableau 13 : collecte de données par services

Chaque VLAN se verra attribuer un sous-réseau propre via **VLSM**, avec une marge de croissance de 20%, assurant ainsi une meilleure répartition des adresses IP tout en évitant le gaspillage.

- **Site Paris**

VLAN	Service	Sous-réseau	CIDR	Masque	Plage d'adresses utilisables	Gateway
10	**Infra Wi-Fi**	**172.10.0.0**	**/21**	**255.255.248.0**	**172.10.0.1 172.10.7.254**	**172.10.0.1**
20	**VOIP**	**172.10.8.0**	**/22**	**255.255.252.0**	**172.10.8.1 172.10.11.254**	**172.10.8.1**
30	**Direction des opérations**	**172.10.12.0**	**/23**	**255.255.254.0**	**172.10.12.1 172.10.13.254**	**172.10.12.1**
40	**Wifi Invité**	**172.10.14.0**	**/23**	**255.255.254.0**	**172.10.14.1 172.10.15.254**	**172.10.14.1**

50	Management des équipements	172.10.16.0	/25	255.255.255.128	172.10.16.1 172.10.16.126	172.10.16.1
60	LAN invité	172.10.16.128	/25	255.255.255.128	172.10.16.129 172.10.16.254	172.10.16.129
70	Service commerciale	172.10.17.0	/26	255.255.255.192	172.10.17.1 172.10.17.62	172.10.17.1
80	Service comptable	172.10.17.64	/26	255.255.255.192	172.10.17.65 172.10.17.126	172.10.17.65
90	DMZ	172.10.17.128	/26	255.255.255.192	172.10.17.129 172.10.17.190	172.10.17.129
100	Direction Recherche et Dév	172.10.17.192	/27	255.255.255.224	172.10.17.193 172.10.17.222	172.10.17.193
110	Direction Générale	172.10.18.0	/27	255.255.255.224	172.10.18.1 172.10.18.30	172.10.18.1
120	DSI	172.10.18.32	/27	255.255.255.224	172.10.18.33 172.10.18.62	172.10.18.33
130	Pôle RH	172.10.18.64	/27	255.255.255.224	172.10.18.65 172.10.18.94	172.10.18.65
140	Pôle juridique	172.10.18.96	/28	255.255.255.240	172.10.18.97 172.10.18.110	172.10.18.97
150	Direction communication & RSE	172.10.18.112	/28	255.255.255.240	172.10.18.113 172.10.18.126	172.10.18.113
160	Imprimantes	172.10.18.128	/28	255.255.255.240	172.10.18.129 172.10.18.142	172.10.18.129

Tableau 14 : plan d'adressage Paris

❖ **Site de Lyon**

VLAN	Service	Sous-réseau	CIDR	Masque	Plage d'adresses utilisables	Gateway
10	Infra Wi-Fi	172.20.0.0	/24	255.255.255.0	172.20.0.1 172.20.0.254	172.20.0.1
20	VOIP	172.20.1.0	/24	255.255.255.0	172.20.1.1 172.20.1.254	172.20.1.1
30	Wifi Invité	172.20.2.0	/24	255.255.255.0	172.20.2.1 172.20.2.254	172.20.2.1
40	LAN invité	172.20.3.0	/25	255.255.255.128	172.20.3.1 172.20.3.126	172.20.3.1
50	Management des équipements	172.20.3.128	/26	255.255.255.192	172.20.3.129 172.20.3.190	172.20.3.129
60	Direction des opérations	172.20.4.0	/25	255.255.255.128	172.20.4.1 172.20.4.126	172.20.4.1
70	Service commerciale	172.20.4.128	/27	255.255.255.224	172.20.4.129 172.20.4.158	172.20.4.129
80	Service comptable	172.20.4.160	/28	255.255.255.240	172.20.4.161 172.20.4.174	172.20.4.161
90	Direction Recherche et Dév	172.20.4.176	/28	255.255.255.240	172.20.4.177 172.20.4.190	172.20.4.177
100	Direction Générale	172.20.4.192	/28	255.255.255.240	172.20.4.193 172.20.4.206	172.20.4.193
110	DSI	172.20.4.208	/28	255.255.255.240	172.20.4.209	172.20.4.209

					172.20.4.222	
120	Pôle RH	172.20.4.224	/29	255.255.255.248	172.20.4.225 172.20.4.230	172.20.4.225
130	Pôle juridique	172.20.4.232	/29	255.255.255.248	172.20.4.233 172.20.4.238	172.20.4.233
140	Direction communication & RSE	172.20.4.240	/29	255.255.255.248	172.20.4.241 172.20.4.246	172.20.4.241
150	Imprimantes	172.20.4.248	/29	255.255.255.248	172.20.4.249 172.20.4.254	172.20.4.249

Tableau 15 : plan d'adressage Lyon

6. Accès distant : AnyConnect Secure Client

Dans le cadre de l'accès distant, les utilisateurs doivent pouvoir se connecter au réseau de l'entreprise de manière sécurisée lorsqu'ils sont en **télétravail**, en **déplacement** ou sur **site client**.

Pour répondre à ce besoin, Netpro Consulting propose **Cisco AnyConnect Secure Client**, une solution **VPN** permettant d'assurer la **CID** (**C**onfidentialité **I**ntégrité **D**isponibilité) des communications.

Présentation de Cisco AnyConnect

AnyConnect est un client VPN multiplateforme (Windows, macOS, Linux, iOS, Android). Il permet différents types de connexions sécurisées :

- **SSL VPN** (via HTTPS, plus simple et flexible) ;
- **IPSec/IKEv2 VPN** (plus robuste et adapté aux environnements exigeants) ;
- Il s'intègre avec **les pares-feux et appliances de sécurité Cisco** ;

Fonctionnalités principales

- **Authentification forte** (certificats, Active Directory, MFA).
- **Chiffrement** du trafic avec TLS/SSL ou IPSec.
- **Accès conditionnel** basé sur l'identité et la posture de l'équipement**.**
- **Contrôle de posture** : vérification que le poste client est conforme (antivirus à jour, OS sécurisé).
- **Expérience utilisateur fluide** : connexion automatique au VPN, reconnexion après coupure réseau.
- **Visibilité et logs** centralisés pour les administrateurs.

Mode de fonctionnement

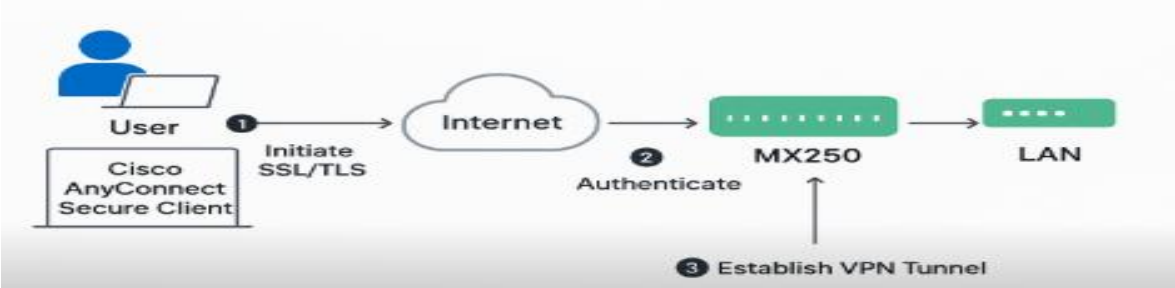


Figure 28 : Fonctionnement de AnyConnect

1. **Utilisateur** : Lance **Cisco AnyConnect Secure Client** sur son PC/téléphone.

- Il saisit **l'adresse publique du MX250** (ou un FQDN).
- **AnyConnect** initie une connexion **SSL/TLS** (port TCP 443 ou UDP 443 pour DTLS).

2. **MX250** → Authentifie l'utilisateur (base locale Meraki, Active Directory, RADIUS, ou SAML/MFA).
3. Si authentification validée → **Tunnel VPN** chiffré établi.
4. L'utilisateur accède aux ressources internes de l'entreprise comme s'il était sur le LAN.

Avantages

✓ Sécurisation des accès distants sans compromettre le réseau interne.
✓ Solution évolutive et intégrée à l'écosystème Cisco.
✓ Support du BYOD (**B**ring **Y**our **O**wn **D**evice) avec contrôle de conformité.
✓ Améliore la productivité des collaborateurs en télétravail.

7. Inventaire des équipements réseaux

	EQUIPEMENTS	QUANTITE
SWITCH WAN	Arista 7280R-16	4
FIREWALL	MX 250	2
	MX 100	2
SWITCH COEUR	C9500-24Y4C	4
SWITCH DISTRIBUTION	C9500-48Y4C	8
SWITCH ACCESS	Netgear GS752TSB	44
	Panneau de brassage cuivre 48 ports RJ45	44
SWITCH DMZ	C9500-24Y4C	2
CABLAGE	Rocade fibre OM4 Multimode (6 brins)	166
	Rocade fibre OS2 Single-mode (12 brins)	8
	Cable RJ45 cat 6	1150
	Cable RJ45 cat 6A	100
Baie stockage	Baie 42 U	10
climatiseur	split inverter de 2.6 kW (9 000 BTU/h) chacun par salle	32

Tableau 16 : Inventaire des équipements réseau

B. Lot B : Déploiement des postes clients : client léger, client lourd

1. Analyse de l'existant

L'audit s'est déroulé en **deux phases** : la création d'un inventaire automatisé du matériel et des logiciels à l'aide des outils GLPI et OCS Inventory ; et la réalisation de tests d'évaluation de performance et de sécurité sur un échantillon représentatif de postes.

Les principaux constats sont les suivants :

- **80 % des postes de travail** utilisaient encore **Windows 8**, un système obsolète non pris en charge depuis **janvier 2016**, exposant ces postes à des vulnérabilités critiques ;
- **25 % des disques durs mécaniques** présentaient des signes de défaillance imminente, comme l'indique l'alerte SMART ;
- **20 % des postes de travail** n'étaient pas équipés d'une solution antivirus active et homogène, ce qui créait d'importantes failles de sécurité ;

- **40 % du parc** n'avait pas reçu de mises à jour de sécurité depuis plus de six mois, compromettant ainsi la protection contre les menaces ;

Aucun chiffrement des disques n'était en place, ce qui contrevenait aux exigences du **RGPD/CNIL** concernant la protection des données en cas de vol ou de perte des appareils.

2. Solutions déployées

Un client est dit **lourd** lorsque l'application est directement installée sur l'ordinateur de l'utilisateur. Le traitement des données et une partie de la logique applicative se font **localement.**

Un client est dit **léger** lorsque le poste de l'utilisateur sert surtout d'**interface**. Le traitement des données et la logique applicative se font **sur le serveur** ou dans **le cloud**.

Critère / Poste	Client lourd		Client léger	
	PARIS / LYON	Commentaire	PARIS / LYON	Commentaire
Postes techniques / métiers spécialisés	**660** / **70**	**logiciels lourds** nécessitent puissance locale	0 / 0	**Non** – pas adapté aux traitements intensifs
Postes bureautiques standards (secrétariat, administratif, RH)	0 / 0	Pas nécessaire	**45** / **15**	Oui – messagerie, bureautique en ligne suffisent
Postes mobiles / en déplacement (commerciaux, ...)	**60** / **15**	Oui – autonomie hors connexion	0 / 0	Non – dépend trop de la connexion
Postes mutualisés / partagés (Usine de production, salles de formation, ...)	0 / 0	Non – maintenance compliquée	**50** / **25**	Oui – pas de données locales, plus sécurisé
Postes avec données sensibles (comptabilité, …)	0 / 0	Oui – si besoin de garder des données locales chiffrées	**40** / **10**	Oui – si on préfère centraliser pour éviter les fuites
TOTAL	**720** / **85**	805	**135** / **50**	185

Tableau 17 : client lourd et léger

a. Renouvellement des postes clients

Dans le cadre de l'amélioration de l'infrastructure informatique, une attention particulière a été portée au renouvellement des postes de travail. Cette façon de faire à deux objectifs : **Premièrement**, résoudre les problèmes liés aux équipements anciens ou cassés qui pourraient ralentir ou arrêter le travail.

Deuxièmement, rendre le parc plus rapide et plus fiable afin qu'il puisse bien fonctionner avec différents types de logiciels et durer longtemps.

- **La première partie** du plan a permis de réparer **40 stations** qui étaient très importantes mais qui présentaient des problèmes avec leur technologie. Ces nouveaux appareils disposent de beaucoup d'espace de stockage et de mémoire, ce qui les rend plus rapides et plus fluides à utiliser. Le choix s'est également porté sur des modèles **ergonomiques** conforment à la norme **ENERGIE STAR** de réduction de l'impact environnemental et de responsabilité sociale.
- **La deuxième partie** du plan nous a permis de récupérer environ **200 Postes** qui pourront être utiliser comme client léger.
- Le reste des postes du parc ne respectaient pas les règles du département informatique en matière d'utilisation des logiciels. Nous allons commander les nouveaux postes pour uniformiser le parc.

Il y'a eu 900 postes clients renouveler afin d'avoir un stock également.

Ayant une remise avec notre partenaire de 25 %

POSTE	QUANTITE	PRIX UNITAIRE (€)	TOTAL HT (€)
PC portable I5/16Go/512Go	900	825	742500
Garantie Carepack 5 ans	900	90	81000
Total HT			823500
TVa			164700
Total TTC			988200

PC Portable

Un raccourci vers le formulaire GLPI sera placé sur le bureau de chaque utilisateur afin de faciliter la saisie de leurs demandes d'évolution ou de signalement d'incidents informatiques.

b. Uniformisation des logiciels

Nous avons installé une copie de l'ensemble du système sur tous les ordinateurs, qui comprend Windows 11 Pro 24H2, Office 365 et les éléments dont nous avons besoin pour travailler. Nous utilisons Microsoft Intune pour exécuter et contrôler ce déploiement. Microsoft Intune nous aide à mettre à jour, à suivre et à configurer ce déploiement tout en uniformisant et en centralisant le parc informatique.

c. Renforcement de la sécurité

SentinelOne est le seul logiciel antivirus présent sur tous les postes de travail. Il est surveillé et contrôlé depuis un emplacement central pour garantir que tout le monde bénéficie du même niveau de protection.

BitLocker est une fonctionnalité qui crypte le disque dur d'un ordinateur, le rendant illisible sans mot de passe. L'ordinateur reçoit également chaque mois de nouvelles mises à jour de sécurité pour le protéger des nouvelles menaces.

d. Conformité aux règles RGPD/CNIL

- **OneDrive Entreprise** constitue l'unique emplacement autorisé pour l'enregistrement des données sensibles.
- Les informations sensibles y sont **systématiquement sécurisées** et **maintenues à jour**.
- Les postes de travail ne conservent aucune donnée sensible en local : tout enregistrement s'effectue exclusivement sur OneDrive Entreprise.
- De plus, les utilisateurs bénéficieront d'une **formation dédiée** à la **protection des données**, renforçant leur sensibilisation à la **sécurité et à la confidentialité** de leurs **informations personnelles**.

3. Recommandations CNIL

- Utilisez des **mots de passe difficiles** à deviner et comportant au **moins 12 caractères**. Ils doivent avoir différents types de lettres, de chiffres et de symboles. Il faut les changer chaque année.
- Cryptage des disques des ordinateurs et autres appareils qui stockent les données. Réduction du stockage local des données personnelles au profit d'un cloud interne sécurisé.
- Gardez une trace de la manière dont les données sont collectées à partir des applications sur les postes de travail.
- Les utilisateurs doivent savoir comment protéger leurs données en toute sécurité.

4. Modernisation des serveurs applicatifs

Deux serveurs Linux, dédiés à des fonctions de gestion telles que l'administration, la finance, la planification et la paie, ainsi qu'à l'hébergement de bases de données Oracle, ont été virtualisés et transférés vers un cluster de serveurs fonctionnant sous **VMware vSphere 8**. Cette démarche de virtualisation confère une résilience accrue face aux pannes, une évolutivité améliorée et un contrôle centralisé des ressources. Les bases de données Oracle sont désormais situées dans un environnement conçu pour garantir une haute disponibilité, assurant ainsi la continuité des services pour les applications critiques.

5. Migration du serveur de fichiers

Le serveur de fichiers traditionnel sous Windows Server 2016 a été remplacé par un cluster de fichiers basé sur Windows Server 2022, intégrant **DFS** (**D**istributed **F**ile **S**ystem) pour la duplication et la robustesse. Les répertoires des utilisateurs et les partages communs sont à présent redondants et sauvegardés automatiquement, assurant une sécurité accrue et un accès ininterrompu aux données.

6. Consolidation des serveurs de messagerie et applicatifs

Par ailleurs, une dizaine de serveurs en rack, dédiés à la **messagerie**, aux **applications web** et aux **bases de données métiers**, ont été intégrés au sein d'une infrastructure **hyperconvergée Nutanix**. Cette approche innovante permet de réduire la consommation énergétique, d'optimiser l'espace au sein des racks et de simplifier la gestion des serveurs grâce à une interface unifiée. De plus, une surveillance centralisée a été mise en place via l'outil **Centreon**, permettant une gestion proactive des ressources.

7. Sécurisation de la baie de stockage

L'ensemble des données, auparavant stockées sur une unique baie, a été transféré vers une solution de stockage **NAS** configuré en **RAID5** favorisant la résilience et la haute disponibilité des

ressources. Pour éviter toute perte de données en cas de défaillance, un système de réplication synchronisé a été instauré entre deux bâies distinctes, situées au siège et sur le site secondaire.

8. Recommandations CNIL

- **Confidentialité des données** : chiffrement obligatoire des bases de données sensibles (Oracle, paie) et des sauvegardes (bandes et cloud).
- **Traçabilité** : maintien d'un registre des traitements automatisés relatifs aux applications hébergées (gestion administrative, paie, finances).
- **Sauvegardes externalisées** : conservation des bandes dans un site externe certifié, conformément aux bonnes pratiques CNIL (**confère lot 1** pour plus de détail)
- **Minimisation des données** : archivage des anciennes données inutiles, avec suppression sécurisée (procédure d'effacement certifiée).
- **Accès aux données** : mise en œuvre d'un contrôle d'accès strict basé sur l'AD et le principe du moindre privilège.
- **Sensibilisation** : formations régulières pour les administrateurs et les utilisateurs concernant les obligations RGPD (accès, portabilité, droit à l'oubli).

C. Lot C : Migration des logiciels de bureautique vers Office 365

1. Contexte et enjeux

Jusqu'à présent, l'entreprise avait recours à diverses versions disparates de Microsoft Office (2010, 2013, 2016), ce qui engendrait des difficultés de compatibilité et une diminution de la productivité. La transition vers Microsoft Office 365 visait à atteindre plusieurs objectifs :

- **Assurer une uniformité de la suite bureautique** à travers l'ensemble du parc informatique ;
- **Stimuler la collaboration** entre les équipes grâce aux outils basés sur le cloud ;
- **Renforcer la mobilité** ainsi que l'accès sécurisé aux documents ;
- **Garantir le respect des normes de sécurité** ainsi que des exigences imposées par le RGPD et la CNIL ;

2. Analyse de l'existant

a. Problèmes connus avant audit

- La coexistence de versions logicielles variées engendre **des incompatibilités** lors des échanges de fichiers ;
- Des mises à jour hétérogènes, souvent retardées, accentuent **les vulnérabilités** en matière de sécurité.
- La forte utilisation d'un serveur de fichiers local, peu adapté aux exigences du partage collaboratif, pose des problèmes.
- Le travail à distance s'avère difficile en raison de l'absence d'outils modernes de visioconférence et d'espaces collaboratifs sécurisés.

b. Problèmes mis en lumière par l'audit

- Il existe un **manque de politique centralisée** pour la gestion des licences Office. Une dépendance excessive aux courriels pour le partage de documents entraîne des **doublons et une perte de temps considérable.**
- Le stockage de données sensibles sur des serveurs internes non chiffrés comporte un risque de **non-conformité au RGPD**.
- Il n'existe aucune solution fiable pour assurer la traçabilité des accès aux documents partagés

3. Solutions mises en œuvre

a. Uniformisation des logiciels

- Mise en œuvre d'une suite unique : **Microsoft 365 Apps for Enterprise**, déployée sur tous les postes via **Microsoft Intune**.
- **Standardisation de l'environnement bureautique**.
- **Mise à jour automatique et continue des logiciels**.
- **Diminution de incidents de compatibilité.**

b. Renforcement de la sécurité

- Introduction de l'authentification **multi-facteur (MFA)** pour l'accès aux services cloud.
- Application du **chiffrement natif des données** via OneDrive Entreprise.
- Intégration d'un système de classification des données grâce à **Microsoft Information Protection**.
- **Centralisation de la supervision** à travers le portail de sécurité de Microsoft 365.

c. Collaboration et productivité

- L'introduction de **Microsoft Teams** en tant que plateforme intégrée de communication, englobant la **messagerie instantanée**, les **visioconférences** et la **gestion de projets**.
- Le partage des documents collaboratifs vers **SharePoint Online**, accompagnée de l'allocation de **1 To de stockage OneDrive Entreprise** pour chaque utilisateur.
- La possibilité de simultanément des documents Word, Excel et PowerPoint en temps réel.

4. Recommendations CNIL

- Établir une politique rigoureuse de classification des informations au sein de SharePoint et OneDrive ;
- Restreindre le partage externe des documents uniquement aux situations véritablement nécessaires et documentées ;
- Tenir à jour un registre des traitements de données précisant les objectifs et les destinataires concernés ;
- Mettre en place des sessions de sensibilisation régulières pour les utilisateurs, axées sur la gestion et le partage des données sensibles ;
- Effectuer des audits réguliers de la sécurité et des accès à travers le portail Microsoft 365 Compliance ;

5.Coût

Poste	Quantité	Prix unitaire (€)	Total HT (€)	Facturation
Microsoft 365 E3 – Clients lourds	900	268.8	241920	Par an
Microsoft 365 E3 – Clients leger	200	268.8	53760	Par an
Total par an			295680	

D. Lot D : Solution antivirus centralisée

1. Contexte & Besoins

- **Problématique** :
  - Protection contre les **malwares, ransomwares, phishing**.
  - Gestion **centralisée** des postes (Paris + Lyon).
  - Conformité aux **politiques de sécurité** (RGPD, ISO 27001).
- **Exigences** :
  - Solution **scalable** (adaptée à la croissance).
  - **Déploiement automatisé** et mises à jour silencieuses.
  - **Reporting** et supervision en temps réel.

2. Solution Proposée : SentinelOne

Pourquoi SentinelOne ?

✓ **Gestion Unifiée** :
  - Console centrale pour administrer **tous les postes** (Paris + Lyon) depuis un seul point.
  - Politiques de sécurité **granulaires** (par site, groupe métier).

✓ **Protection Avancée** :
  - Détection **comportementale** (IA + Sandboxing) contre **zero-day**.
  - Module anti-ransomware **spécialisé**.

✓ **Déploiement Simplifié** :
  - Installation **silencieuse** via GPO ou scripts.
  - Mises à jour **automatisées** (pas d'impact utilisateur).

✓ **Reporting & Conformité** :
  - Tableaux de bord **temps réel** (menaces bloquées, vulnérabilités).

- Audit automatisé pour **certifications** (RGPD).

✓ **Coût Maîtrisé** :

- Licences **volumétriques** (tarif dégressif pour environ 980 postes).
- Réduction des coûts de support (moins d'incidents)

Certifié par l'**ANSSI**, données hébergées en UE (RGPD), et 80% des entreprises du **CAC40** l'utilisent.

3. Architecture Proposée

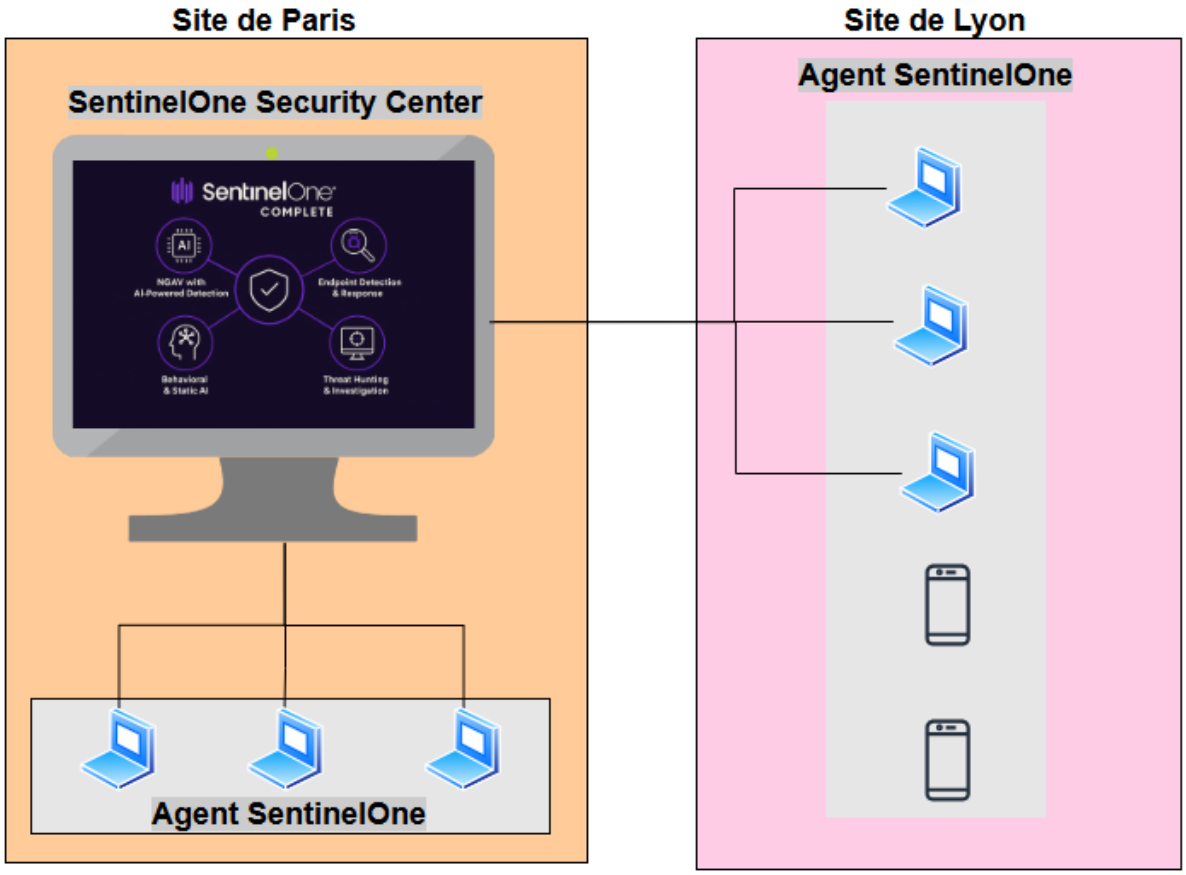


Figure 29 : Architecture Antivirus centralisée

- **Serveur Central** : Hébergé à Paris.
- **Agents légers** : Installés sur tous les postes (Windows/macOS).
- **Optimisation bande passante** : Mises à jour en peer-to-peer local.

4. Comparatif avec les Alternatives

Critère	SentinelOne	Symantec	Microsoft Defender
Gestion Centralisée	Excellente	Bonne	Limitée
Protection Zero-Day	IA + Sandbox	Signature + ML	Basique (ML seule)
Coût (980 postes)	Compétitif	Cher	Gratuit (mais limité)
Support Français	Direct	Partenaire	Community

Figure 30 : Comparatif des solutions d'antivirus

SentinelOne offre le meilleur ratio efficacité/coût pour un parc de cette taille**.**

5. Justification du Choix

- **Unifié** : Une seule console pour Paris + Lyon.
- **Sécurisé** : Détection proactive des ransomwares (critique pour les données clients).
- **Économique** : Pas de surcoût lié à la gestion de deux solutions distinctes.
- **Compatible** : Supporte les anciens OS (ex. Windows 10/11, macOS).

E. Lot E : (Sécurisation réseau – Détection et prévention des intrusions)

1. Système de détection d'intrusion IDS

Un système de détection des intrusions (IDS) est une solution logicielle chargée de surveiller le trafic réseau afin d'identifier des menaces connues, ainsi que des activités suspectes ou malveillantes. Lorsqu'une anomalie ou un risque de sécurité est détecté, l'IDS génère des alertes à destination des équipes informatiques et de sécurité pour leur permettre d'intervenir rapidement. Nous déployons des solutions NIDS au sein du réseau afin de surveiller le trafic entrant et sortant. Ces systèmes IDS permettent de détecter les activités malveillantes ou suspectes en analysant les communications échangées entre les différents appareils connectés au réseau et l'extérieur.

Nous déployons également un système HIDS, installé directement sur des appareils individuels connectés à Internet et au réseau interne de Solaris. Ce type de solution permet de détecter des paquets provenant de l'intérieur de l'entreprise, ainsi que du trafic malveillant que les systèmes NIDS pourraient ne pas identifier. Le HIDS est également capable d'identifier des menaces provenant de l'hôte lui-même, comme un appareil infecté par un malware tentant de se propager au sein du système de Solaris.

2. Système de prévention d'intrusion IPS

Un système de prévention des intrusions (IPS) va plus loin en bloquant activement les risques de sécurité. Il ne se contente pas de surveiller les activités malveillantes, mais peut également intervenir en temps réel pour empêcher qu'une attaque ne se concrétise.

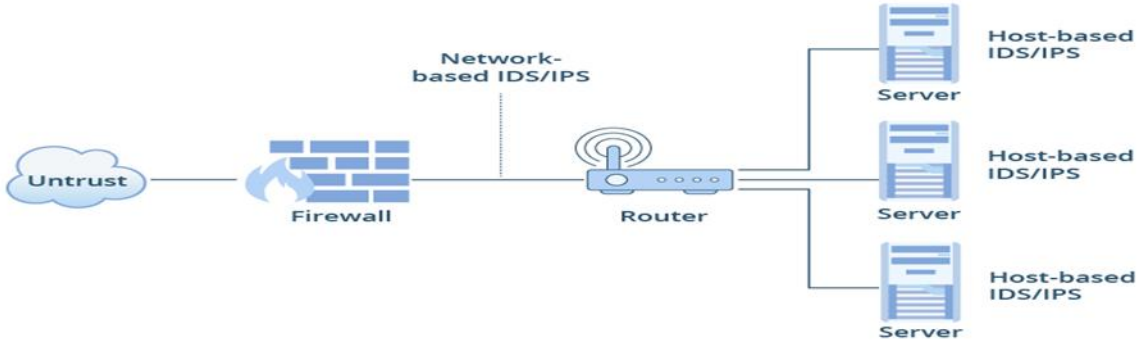


Figure 31 : Schéma IDS/IPS

F. Lot F : Audit de sécurité

1. Contexte et enjeux

La société Solaris centralise une partie essentielle de son système d'information au sein de son siège social. Les serveurs, systèmes de messagerie et les applications métiers sont logés dans une salle technique dédiée. De plus, les baies de stockage et les dispositifs de sauvegarde y sont également hébergés.

La protection physique de ces infrastructures revêt une importance cruciale : un événement tel qu'un incendie, une inondation, une intrusion ou une coupure prolongée d'électricité pourrait entraîner une interruption complète des opérations de l'entreprise, ainsi qu'une perte définitive de données.

Ainsi, **l'objectif de l'audit** consiste **à évaluer la solidité des mesures de sécurité physique et environnementale en place**, tout en formulant des recommandations correctives appropriées.

2. Analyse de l'existant

a. Problèmes connus avant l'audit

- Les serveurs, la baie de stockage et les robots de sauvegarde sont concentrés dans une seule salle au siège ;
- Les bandes de sauvegarde sont conservées dans les sous-sols, exposées aux risques d'inondation et d'incendie ;
- La salle serveurs dispose d'une climatisation simple (non redondante) ;
- L'extinction d'incendie repose uniquement sur des extincteurs classiques, inadaptés aux matériels informatiques ;
- Le contrôle d'accès est limité à une serrure mécanique, sans traçabilité ;

b. Problèmes mis en lumière par l'audit

- Absence de redondance géographique : un sinistre majeur au siège pourrait anéantir l'ensemble du SI ;
- La continuité énergétique n'est pas garantie : pas de groupe électrogène, seulement quelques onduleurs non supervisés ;
- Vulnérabilité climatique : absence de monitoring automatisé (température/humidité) et pas d'alerte en cas de défaillance ;
- Les procédures d'évacuation et de reprise ne sont ni documentées ni testées régulièrement ;

3. Solutions mises en œuvre

NetPro Consulting a proposé de segmenter correctement le réseau en isolant la DMZ du LAN et en cloisonnant le Wi-Fi interne (**ref Lot A**). La mise à jour ou le remplacement des équipements obsolètes est prioritaire (**Ref Lot J**), tout comme la migration des serveurs SQL (**Ref Lot 5**) et Active Directory vers des versions supportées, avec une centralisation de leur gestion (**Ref Lot 2**). Le plan d'adressage pour optimiser et éviter le gaspillage en améliorer les performances réseau (**Ref Lot A** partie plage d'adressage). Il est également crucial de renforcer la **stratégie de sauvegarde** avec une externalisation partielle pour assurer la continuité d'activité (**Ref Lot 1**). La centralisation des consoles antivirus (**Ref Lot D**), la refonte des GPO et l'uniformisation des politiques de sécurité permettront une gestion plus efficace et conforme aux exigences RGPD et à la PSSI. Ces mesures doivent être supervisées par le RSSI.

G. Lot G : PCA/PRA

Le Plan de continuité des Activités (**PCA**) se réfère aux mesures à prendre pour maintenir et poursuivre les activités d'une organisation face aux menaces potentielles. Le plan garantit que les opérations de l'entreprise, dans son ensemble, sont capables de fonctionner en cas d'incident.

Un Plan de Reprise d'Activité, (PRA) vise à rétablir le système d'information de l'entreprise au plus vite en cas de sinistre. Le PRA vise à minimiser les temps d'arrêt de l'entreprise en maintenant l'accès aux infrastructure informatiques et aux applications critiques.

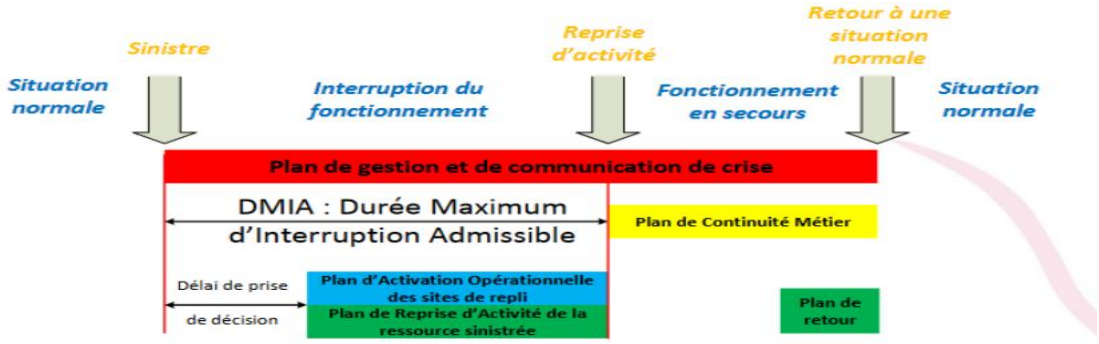


Figure 32 : PCA/PRA

Le **PCA/PRA** a pour but de garantir une certaine protection des données de l'entreprise face aux menaces pouvant exister.

Etape 1 : Totalité des activités de l'entreprise

Solaris regorge à son sein plusieurs activités entre autres on peut citer :

- Service cotisations, gestion de dossiers assurés et remboursements
- Service Markéting
- Service juridique
- Gestionnaires d'actifs
- Le service financier
- Les Gestionnaires de comptes adhérant
- Le Top Management
- Gestion administrative
- Experts médicaux
- Conseillers mutualistes itinérants
- Centre d'appels et ticket
- Service informatique
- Service d'impression
- Service commercial

Le **BIA** sera constitué en fonction du **PMDT** (**P**erte **M**aximal de **D**onnées **T**olérable) ET **DMIA**

(**D**urée **M**aximale d'**I**nterruption **A**dmissible) qui nous ont été communiqué par le comité de

Direction.

Ci-dessous, l'illustration de la position dans le temps du PMDT et DMIA lors de la survenance d'un évènement perturbateur.

Pour chaque activité, la **BIA** évaluera le **DMIA**, le **PMDT** et **OMCA** (**O**bjectif **M**inimal de **C**ontinuité d'**A**ctivité). Pour qualifier les activités prioritaires, on justifiera le DMIA, la PMDT et l'OMCA en mesurant les impacts en termes de :

- Pertes financières ;
- Pertes d'images ;
- Pertes de productivité liée à la désorganisation ;
- Pénalités contractuelles ou réglementaires ;

Etapes 2 : Référentiel qualificatif des impacts

Nous allons qualifier un référentiel unique de comparaison de la gravité des impacts qui va nous permettre de classer les activités de l'entreprise par priorité.

Etapes 3 : évaluons les impacts d'une interruption d'activités

Ci-dessous un tableau illustrant les impacts d'une interruption dans les différents services :

Activité	Perte financière	Pertes d'images	Perte de productivité	Pénalité contractuelle réglementaire	DMIA	PMDT
Service d'impression	Mineur	Majeur	Majeur	Mineur	J+1	0h
Gestionnaires de comptes adhérents	Majeur	Majeur	Majeur	Majeur	J+1	0h
Commerciaux	Majeur	Majeur	Majeur	Mineur		0h
Direction administrative et financière	Majeur	Majeur	Majeur	Mineur	J+1	24h
Experts médicaux	Majeur	Majeur	Majeur	Majeur	J+1	0h
Responsable de service	Mineur	Mineur	Mineur	Mineur	J+1	24h
Plateau maintenance informatique	Mineur	Majeur	Majeur	Majeur	J+2	0h
Markéting	Majeur	Majeur	Majeur	Mineur	J+5	24h
Comptabilité ADV	Mineur	Majeur	Majeur	Majeure	J+1	24h

Tableau 18 : Evaluation des impacts en cas d'interruption d'activités

Etapes : Ressources/moyens nécessaires aux activités

Après cette analyse, il en ressort que les activités prioritaires sont le service administratif et financier les ressources humaines, le service médical, le service d'impression et le service de gestion des comptes adhérents.
Quels sont donc pour ces activités les exigences et besoins en termes de ressources (postes de travail, applications informatique, serveurs, services DHCP, DNS, LDAP, et autres) pour un mode de fonctionnement jugé acceptable qui n'est pas forcément le mode nominal (mode de fonctionnement tel qu'il était lors de la survenance de l'événement perturbateur).

Activité	Ressources/Moyens
RH	PayFit
Direction administrative et financière	MS office 365, MS Exchange
Experts Médicaux	Données Médicales/ERP
Informatique	Outil de monitoring/Centreon

Marketing	Contrats clients/SAP Marketing
Comptabilité et ADV	Cegid Loop
Le service d'impression	Données clients/GED
Service de Gestion des comptes adhérents	Base de données/Oracle et SQL Server

Tableau 19 : Ressources/moyens nécessaires aux activités

1. Identification des risques :

a. Ressources exposées à risques :

Bâtiment et infrastructure, informatique, RH, outils et flux de production, réseaux (transports, énergie, télécoms, eau, électricité), IoT Internet des Objets

b. Types de risques majeurs

Naturels (inondation, séisme, aléa climatique), pandémie, cybermenace, mouvements sociaux, terrorisme…

2. Scénario de risques

R1 : Bâtiment impraticable ;

R2 : Site informatique indisponible ;

R3 : Cyberattaque ;

R4 : Fournisseur défaillant ;

R5 : Inondation fluviale ;

R6 : Mouvement social ;

R7 : Coupure alimentation électrique ;

R8 : Coupure physique de fibre ;

R9 : Interdiction préfectorale d'accès dans les locaux.

3. Niveau de criticité des risques

	Faible	Modérée	Forte	Elevée
Risques		*R2 : Site informatique indisponible*	R1 : Bâtiment impraticable R3 : Cyber attaque	
		R7 : Coupure alimentation électrique	*R4 : Fournisseur défaillant* *R8 : Coupure physique fibre optique*	
		R6 : Indisponibilité massive RH	R9 : Interdiction préfectorale d'accès dans les locaux	*R5 : Inondation fluviale*
		R6 : Mouvement Social		

Tableau 20 : Niveau de criticité des risques

Matrice des risques

- À traiter immédiatement (rouge, gras) ; • À traiter à court/moyen terme (orange, italique);
- Acceptable en l'état (vert, normal).

4. Mesure de traitement des risques

R2 : **Site informatique indisponible**

Réplication des serveurs virtuels sur des serveurs de secours

R7 : **Coupure alimentation électrique**

Utilisation du circuit d'onduleur plus groupe électrogène. Acquérir un générateur d'alimentation électrique et son alimentation périodique.

R3 : **Cyberattaque**

Afin d'assurer la continuité d'activité des services indispensables, nous avons mis en place un système de sauvegarde suivant la règle **2-3-1** qui stipule la copie de 2 données sur 3 support différents une copie étant sauvegardé à distance.

R9 : Interdiction préfectorale d'accès dans les locaux.

Utilisation des PC portables mis à disposition des employés pour des connexion au siège à partir au VPN

R8 : Coupure physique de fibre

Mise en place de deux liens d'accès chez 2 opérateurs différents. Chaque lien d'accès est connecté sur les deux Firewalls. Si le lien principal tombe, le lien Secondaire assure la continuité.

R1 : Bâtiment impraticable

Connexion des utilisateurs à distance à partir du VPN

R5 : Inondation fluviale

Sauvegarde des données dans des DATA Center d'un prestataire de Sauvegarde situé à Lyon. Sauvegarde complète des serveurs avec rétention de 15 jours.

Les salles serveurs et locaux informatiques sont situés à partir du Premier étage sur tous les sites de Solaris.

H. Lot H: Monitoring et ticketing

1. Solution de Monitoring

c. Outil proposé : Centreon IT Edition

Centreon IT Edition est une solution professionnelle de supervision des infrastructures IT, basée sur une technologie éprouvée et enrichie de modules et de connecteurs officiels. Elle offre une vue **unifiée** et **centralisée** sur l'état du système d'information, avec des capacités d'analyse avancées et une intégration facilitée dans les environnements critiques.

d. Fonctionnalités clés :

- **Supervision complète** des serveurs, réseaux, bases de données et applications.
- **Tableaux de bord avancés** et personnalisables pour la visualisation des performances.
- **Système d'alertes multi-canaux** (email, SMS, …).
- **Connecteurs officiels** pour les principaux constructeurs et éditeurs (Cisco, VMware, Microsoft, etc.).
- **Reporting avancé** pour le suivi des SLA et de la disponibilité des services.

e. Justification du choix:

Critères	Centreon IT Edition	Zabbix	Nagios Core	PRTG Network Monitor
Licence	Édition commerciale (support inclus)	Open-source (gratuit)	Open-source (gratuit)	Licence commerciale (capex/opex)
Facilité d'usage	Interface moderne, ergonomique	Interface basique, nécessite expertise	Interface minimaliste, peu intuitive	Interface conviviale mais fermée
Fonctionnalités	Supervision complète + reporting SLA	Supervision complète, peu de reporting avancé	Supervision basique, reporting limité	Supervision réseau + alertes, reporting correct
Support constructeur	Connecteurs officiels (Cisco, VMware, etc.)	Communauté active, pas de support officiel	Communauté uniquement	Support éditeur officiel
Évolutivité	Haute, adaptée aux grandes infrastructures	Haute, mais complexe à maintenir	Moyenne, nécessite plugins tiers	Moyenne, dépend des licences
Intégration ITSM	Oui (GLPI, ServiceNow, etc.)	Possible via connecteurs tiers	Nécessite développement tiers	Possible mais limité

Tableau 21 : Comparatif des solutions de Monitoring

2. Solution de Ticketing

a. Outil proposé : GLPI (Gestion Libre de Parc Informatique)

GLPI est une solution open-source de gestion de parc informatique et d'helpdesk. Elle permet de gérer les incidents, demandes, changements et d'assurer un suivi structuré des interventions.

b. Fonctionnalités clés :

- **Portail utilisateur** pour déclarer des incidents/demandes.
- **Gestion des tickets** avec workflow configurable.
- **Suivi des SLA** (Service Level Agreement).
- **Inventaire du matériel** et intégration possible avec l'annuaire AD.
- **Génération de rapports et statistiques**.

c. Justification du choix :

- **Solution complète** et largement adoptée en entreprise.
- **Interface intuitive**, utilisable par les techniciens et les utilisateurs finaux.
- **Supporte des intégrations avec Centreon IT Edition** pour créer automatiquement des tickets en cas d'alerte.
- **Permet un suivi précis** de l'activité et améliore la communication entre l'IT et les métiers.

La combinaison **Centreon IT Edition (Monitoring)** et **GLPI (Ticketing)** constitue une solution robuste et adaptée aux besoins des entreprises. Elle assure une supervision fiable et centralisée de l'infrastructure tout en offrant un système de gestion des incidents performant. Leur intégration permet d'automatiser la création de tickets à partir d'alertes de supervision, améliorant ainsi la rapidité d'intervention et la qualité globale du service IT.

I. LOT I Gestion de parc informatique et Contrat de maintenance

1. Gestion de Parc Informatique

La gestion de parc informatique, également appelée gestion des actifs IT, consiste à superviser, maintenir et optimiser l'ensemble des ressources informatiques d'une organisation. Cela inclut l'administration, la maintenance et la mise à jour des équipements (ordinateurs, serveurs, imprimantes, etc.) ainsi que des logiciels utilisés.

2. Contrat de Maintenance

Le contrat de maintenance informatique est un accord par lequel une entreprise de services informatiques s'engage, contre rémunération, à assurer l'entretien et le bon fonctionnement du parc informatique de son client. Étant généralement conclu sur une base récurrente, ce type de contrat permet souvent une facturation au forfait.
Solaris bénéficie de contrats de maintenance couvrant plusieurs solutions, notamment :

- L'outil de gestion des tickets
- Les serveurs
- Les applications métiers
- Les bases de données
- Les logiciels de sécurité
- La téléphonie

Le tableau ci-dessous récapitule l'ensemble des contrats de maintenance en cours, classés par type d'équipement ou de service concerné.

Ressource	Type de contrat	Durée	Entreprise
Téléphonie	Maintenance avec remplacement des équipements défectueux	3 ans (hors année en cours)	Ringcenter MVP
Wi-Fi	Maintenance sans remplacement des équipements	2 ans (hors année en cours)	NetPro Consulting
PayFit (Application RH)	Maintenance de l'application sur poste clients et serveurs	3 ans (hors année en cours)	PayFit
Sauvegarde Externe	Supervision et sauvegarde externalisée avec rétention de 15 jours mensuels	3 ans (hors année en cours)	XEFI
ERP (App comptablité)	Maintenance de l'application sur postes clients et serveurs	2 ans (hors année cours)	Cegid Loop
PC portables	Maintenance sans remplacement des pièces défectueux	3 ans + année en cours	NetPro Consulting
PC fixe	Maintenance sans remplacement des pièces défectueux	3 ans + année en cours	NetPro Consulting
Serveurs	Maintenance sans remplacement des pièces défectueux	2 ans + année en cours	NetPro Consulting
Imprimantes	Maintenance avec impression illimitée et remplacement du matériel défectueux	2 ans + année en cours	NetPro Consulting
Sauvegarde & supervision	Contrôle des sauvegardes et supervision du parc informatique	3 ans + année en cours	NetPro Consulting

Tableau 22 : Contrats de Maintenance

J. Lot J : Déploiements et mises à jour (OS et applications)

1. Comparaison entre divers outils de déploiement et mises à jour

Plusieurs outils sont repondus dans le domaine de l'informatique en ce qui concerne le déploiement automatique de logiciels et de mise à jour d'application.

Critère	Scripts/GPO	WSUS	SCCM	Intune
Coût	Faible	Faible	Élevé	Moyen (licence Microsoft 365 E3/E5)
Applications Microsoft	Oui	Oui	Oui	Oui
Applications tierces	Limité	Non	Oui	Oui
Reporting / suivi	Limité	Moyen	Excellent	Excellent
Télétravail / Cloud	Non	Non	Partiel (VPN)	Oui
Maintenance	Lourde	Moyenne	Lourde	Faible

Tableau 23 : Comparaison entre divers outils de déploiement et mises à jour

Après cette comparaison nous retiendrons l'outils **Intune** car elle est la solution la mieux adaptée à un contexte **multi-sites** + **télétravail**. En plus, elle intègre des kits de déploiement pour les applications mobiles.

2. Architecture

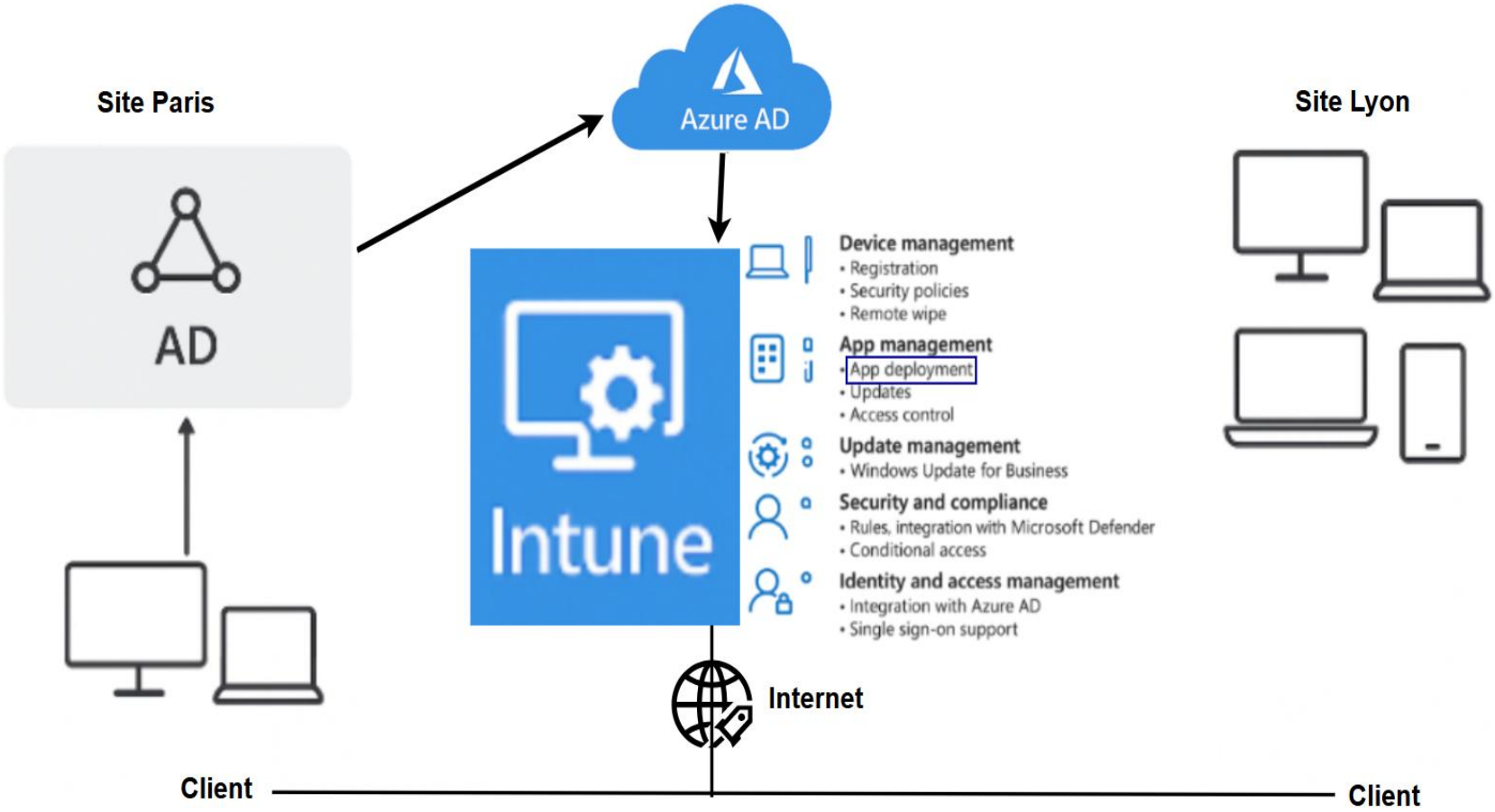


Figure 33 : Schéma fonctionnel d'Intune

3. Présentation et principe de fonctionnement

Microsoft **Intune** est une solution de **gestion unifiée des terminaux (UEM)** proposée en mode **Cloud**. Elle permet aux administrateurs informatiques de gérer les **appareils (Windows, macOS, iOS, Android)**, de contrôler les **applications** utilisées par les collaborateurs, et d'assurer la **sécurité et la conformité** du parc informatique.

Etant donné que Solaris dispose des sites à Paris et sur Lyon, Intune offrira une gestion **centralisée** et **automatisée** :

- Les applications et mises à jour sont déployées depuis le Cloud (via **App deployment** ou **Update** pour les mises à jour) ;
- Les utilisateurs et appareils se synchronisent via **Azure Active Directory** ;
- La connexion Internet suffit : pas besoin d'utiliser un VPN ;

K. LOT 1 Mise en place des solutions de stockage et de sauvegarde

1. Analyse de l'existant

Solaris utilisait un système de sauvegarde reposant sur Veeam Backup & Replication 7.5, avec un stockage centralisé et synchronisé, basé sur un SAN configuré en RAID 1, servant de repository pour les sauvegardes.
Toutefois, cette architecture présente une faiblesse majeure : en cas de panne du SAN, les deux serveurs Veeam deviennent inopérants. De plus, la configuration en RAID 1 où un disque sur deux est exclusivement dédié à la redondance engendre un coût élevé sans gain de capacité.

2. Solution Proposée

Pour répondre à ces limites, NetPro Consulting propose une migration vers une solution de sauvegarde basée sur **Veeam Backup & Replication v12**, utilisant un stockage sur un système **NAS** configuré en **RAID 5** et avec une **isolation réseau**. Ce type de système est plus économique, plus simple à gérer, et offre de meilleures performances ainsi qu'un niveau de sécurité optimisé.

	SAN	NAS
Signification	Storage Area Network	Network Attached Storage
Protocoles	SCSI, Fibre Channel ou SATA.	Serveur de fichiers, NFS ou CIFS.
Partage de l'information	Le partage de fichier repose sur le système d'exploitation.	Il permet un partage plus important notament entre les systèmes d'exploitation tels que Unix et NT.
Identification des données	Identifiez les données par bloc de disque.	Adresses les données par le nom de fichier et l'offset de l'octet.
Dispositif pouvant se connecter à la technologie	Seuls les périphériques appartenant à la classe de serveurs et dotés du canal <<Fibre Channel SCSI>>.	Chaque périphérique qui se connecte au réseau local qui utilise les protocoles NFS, CIFS ou http peut se connecter au NAS.
Coût et complexité	Cher et plus complexe.	Rentable et moins compliqué.

Tableau 24 : Comparaison SAN et NAS

L. LOT 2 Annuaire LDAP

LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) est un protocole ouvert et multiplateforme conçu pour permettre l'authentification et l'accès aux services d'annuaire. Il définit le langage de communication utilisé par les applications pour interagir avec des serveurs d'annuaire, facilitant ainsi la gestion centralisée des utilisateurs, des groupes et des ressources réseau.

Solaris a adopté cette solution, car la majorité des applications actuelles sont capables de déléguer leurs mécanismes d'authentification à un outil tiers.

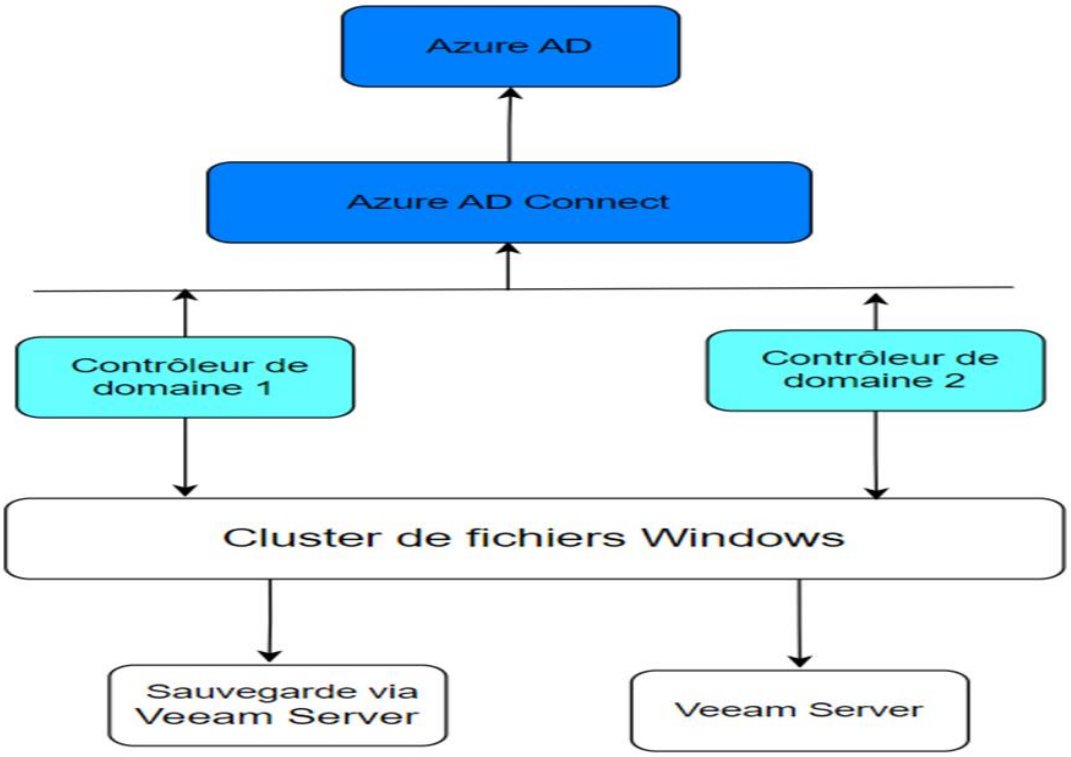
Elles s'appuient pour cela sur des protocoles standards tels que LDAP, RADIUS ou SQL. Pour exploiter cette capacité, nous mettons en place une infrastructure d'annuaire centralisée reposant sur le protocole LDAP.

NetPro Consulting propose :

- Une migration vers **Windows Server 2022**,
- **Un an après**, nous ferons la migration vers **Windows Server 2025 à nos frais :** si nous installons le windows server 2025, Solaris pourra être vulnérable aux failles de sécurité de type **Zero day** (le Système sera moins stable) ;
- Prévoir l'intégration de l'authentification multi-facteur (MFA) pour renforcer la sécurité et l'authentification des utilisateurs ;

Avec la migration vers Windows Server 2022, Solaris peut bénéficier des options d'intégration cloud avec un environnement hybride **AD + Azure AD**.

Déployer une infrastructure redondante, avec plusieurs contrôleurs de domaine (AD), clustering du serveur de fichiers et Sauvegarde/restauration automatisée (via Veeam). AD est un service



développé par Microsoft qui permet de gérer les utilisateurs, les ordinateurs, les groupes, et les ressources d'un réseau de manière centralisée. Il permet : L'authentification, Le contrôle des accès, La gestion centralisée via des stratégies de groupe (GPO) et l'organisation hiérarchique du réseau.

Figure 34 : Annuaire LDAP

M. Lot 3 Virtualisation

Solaris ne dispose d'aucune virtualisation. Dans le cadre de la mise à niveau de son infrastructure informatique, NetPro Consulting propose l'implémentation d'une solution de virtualisation. Cette démarche permettrait d'améliorer considérablement l'évolutivité et la résilience du réseau, deux critères essentiels pour accompagner la croissance et assurer la continuité des activités de l'entreprise.

Solution	Type	Version	Coût	Fonctionnalités clés	Points forts
Proxmox VE	Open source	9.0	Très faible	KVM + LXC, HA, interface web	Efficacité, flexibilité
VMware vSphere / ESXi	Propriétaire	8.0	Très élevé	vMotion, DRS, NSX, vCenter	Fonctionnalités avancées
Microsoft Hyper-V	Propriétaire	Via Windows server 2022 ou 2025	Élevé (licences Windows)	Intégration Windows, clustering	Bonne pour écosystème MS
Citrix DaaS / AVD / AWS	Cloud / SaaS		Coût incertain /élevé	Virtual Workstation cloud	Scalabilité, cloud-aspect

Tableau 25 : Tableau comparartif des solutions de virtualisations

NetPro Consulting recommande l'adoption de la solution de virtualisation VMware vSphere Enterprise Plus. Ce choix se justifie par la richesse fonctionnelle de la plateforme, notamment en matière de gestion avancée du stockage, de performances optimisées et d'une grande évolutivité. Cette version permet la création illimitée de machines virtuelles et inclut un support constructeur disponible 24h/24 et 7j/7, garantissant une assistance réactive en cas d'incident ou de besoin technique.

N. Lot 4 : Migration et sécurisation de la messagerie

1. Contexte et enjeux

La messagerie représente l'un des instruments de communication les plus essentiels pour le Groupe Solaris. Toutefois, l'infrastructure actuelle repose sur une dizaine de serveurs physiques qui hébergent Exchange en interne, ce qui engendre plusieurs problèmes :

- Une complexité administrative considérable,
- Des coûts énergétiques élevés,
- Une augmentation des risques de défaillances matérielles,
- Une vulnérabilité accrue face aux menaces contemporaines telles que le phishing, le spam et les ransomwares.

Ainsi, l'objectif de ce projet consiste à moderniser l'architecture de messagerie en la transférant vers une solution cloud sécurisée, tout en renforçant la protection contre les cyberattaques et en assurant la continuité des services.

2. Analyse de l'existant

a. Problèmes connus avant audit

- Une infrastructure obsolète, reposant sur Exchange 2016 et s'étendant sur plusieurs serveurs en rack.
- Une prolifération des points de défaut, avec différents serveurs physiques exclusivement consacrés à la messagerie et aux services connexes.
  - Une protection insuffisante contre le spam et le phishing.
- Des capacités de gestion de la mobilité restreinte pour les employés en télétravail.

b. Problèmes mis en lumière par l'audit

- Absence de plan de PRA spécifique pour la messagerie.
- Manque de redondance et haute disponibilité.
- Risque d'attaques ciblées (phishing avancé, compromission de comptes).
- Surconsommation énergétique et coût de maintenance disproportionnée.

3. Solutions mises en œuvre

a. Migration vers Office 365 Exchange Online

- Passage de la messagerie vers Exchange Online (Office 365).
- Suppression progressive des serveurs physiques Exchange on-premise.
- Synchronisation sécurisée des comptes via Azure AD Connect.
- Haute disponibilité native grâce aux datacenters Microsoft.

b. Renforcement de la sécurité

- Activation du MFA (Multi-Factor Authentication) pour tous les comptes de messagerie.
- Déploiement de Microsoft Defender for Office 365 (anti-phishing, anti-malware, sandboxing).
- Mise en place d'une solution de filtrage avancé Cisco Secure Email (CES) :
- Détection et mise en quarantaine des emails suspects ou provenant de domaines malveillants.
- Analyse en temps réel du contenu et des pièces jointes.
- Protection contre le spam, le spear-phishing et les fraudes par usurpation d'identité.
- Console centralisée permettant aux administrateurs de gérer les emails en quarantaine.
- Chiffrement des emails sensibles avec Azure Information Protection.
- Centralisation des logs et supervision des accès pour assurer la traçabilité.

c. Collaboration et productivité

- Intégration complète avec Teams et SharePoint Online pour améliorer la collaboration.
- Accès mobile sécurisé aux emails et calendriers.
- Partage de calendrier interservices et synchronisation instantanée.

d. Continuité et conformité

- Garantie de disponibilité à 99,9 % via SLA Microsoft.
- Sauvegarde supplémentaire des boîtes mails avec Veeam Backup for Office 365.
- Mise en conformité avec le RGPD et les recommandations CNIL (sécurisation des données, localisation, contrôle des accès).

O. LOT 5 Base de données

Afin de moderniser l'infrastructure de Solaris et d'en renforcer la performance, la sécurité ainsi que l'évolutivité.

NetPro Consulting recommandé de migrer la base de données SQL Server 2012 vers SQL Server 2022, une version plus récente, sécurisée et pleinement supportée, offrant des performances optimisées et des fonctionnalités avancées. Parallèlement, il est préconisé de faire évoluer les bases de données Oracle vers Oracle Database 21c, afin de bénéficier des dernières innovations de la plateforme tout en optimisant les coûts de licences grâce à une meilleure gestion des ressources. Enfin, une refonte de l'application SolarisAid sous la forme d'une architecture microservices est conseillée. Cette approche facilite le découpage de l'application en services fonctionnels indépendants, améliorant ainsi la maintenance, les déploiements, la scalabilité, et permettant une intégration progressive de nouvelles fonctionnalités dans un environnement cloud ou hybride.

Tableau comparatif des solutions moderne

Solution moderne	Cycle/support attendu	Avantages clés
SQL Server 2022	Support principal jusqu'en 2031 (estimé)	Sécurité renforcée, meilleures performances
PostgreSQL (open source)	Versions majeures maintenues environ 5 ans	Coût réduit, communauté active, évolutivité
Oracle Database 21c	Support principal jusqu'en 2031 (estimé)	Intégration native avec Azure, fonctionnalités avancées de sécurité

Tableau 26 : comparatif des solutions de Base de données

P. LOT 6 VOIP

La VoIP, ou **Voice over IP**, est une technologie qui permet de passer des appels téléphoniques via Internet, au lieu d'utiliser le réseau téléphonique traditionnel. Autrement dit, la voix est convertie en données numériques et transmise à travers un réseau IP (comme Internet), plutôt que par des lignes téléphoniques classiques. La VoIP est une technologie informatique qui permet la transmission de la voix sur des réseaux compatibles IP. Ces réseaux peuvent être : Privés (intranets), Publics (Internet), Filaire (câble, ADSL, fibre optique), Sans fil (satellite, Wi-Fi, réseaux mobiles).

De nombreuses solutions de téléphonie VoIP existent sur le marché, souvent basées sur le cloud, ce qui garantit : Une haute disponibilité des services et des contrats de support professionnels. Compte tenu de la confidentialité et du nombre d'utilisateurs chez Solaris, l'application RingCentral MVP présente des atouts majeurs pour répondre aux besoins liés à la refonte de la téléphonie au sein de Solaris.

RingCentral MVP est une solution d'entreprise sécurisée de téléphonie VoIP basée sur le cloud, proposée sous forme payante. Elle intègre non seulement toutes les fonctionnalités classiques de la téléphonie, mais aussi plusieurs fonctionnalités avancées.

Parmi ses principaux avantages, on peut citer :

- Une grande facilité d'utilisation
- Un déploiement rapide
- De nombreuses possibilités d'intégration avec d'autres outils

RingCentral MVP offre trois services principaux :

- La messagerie
- La téléphonie
- La vidéo

Un portail d'administration centralisé permet de gérer toutes les configurations.

La solution propose deux types de licences :

- Une licence mobile gratuite, qui permet d'effectuer des appels locaux, c'est-à-dire des appels entre collaborateurs au sein de la même entreprise.
- Une licence MVP (Message, Vidéo, Phone), qui permet d'effectuer des appels internes et externes à l'organisation.

Q. Lot supplémentaire : Stratégie Globale de Cybersécurité et Mise en place du SOC

1. Contexte et Objectifs

À l'issue de l'audit initial, il est apparu que la sécurité du Groupe Solaris reposait sur un ensemble de mesures techniques disparates et non harmonisées, sans stratégie globale claire. Ce lot a pour objectif de remédier à cette situation en définissant et en mettant en œuvre un cadre de sécurité cohérent et robuste. Les objectifs principaux sont :

- **Évaluer et renforcer** l'ensemble de la posture de sécurité existante.
- **Définir et documenter** les politiques, normes et procédures de sécurité de l'information.
- **Mettre en place un SOC (Security Operations Center)** pour une supervision centralisée, une détection proactive des menaces et une réponse aux incidents efficace.
- **Préparer l'organisation** à faire face aux cyber-crises via un plan de gestion dédié.

2. Analyse et Cadrage

a. Examen de l'existant et des besoins

Notre analyse s'est articulée autour des axes suivants, en cohérence avec les constats de l'audit initial :

- **Gouvernance & Politiques :** Absence de politique de sécurité formelle, de charte utilisateur récente et de procédures détaillées pour la gestion des incidents.
- **Architecture & Technologies :** Revue de l'architecture réseau sécurisée proposée (Lot A), des solutions antivirus (Lot D), de la segmentation (VLANs), et des équipements (Pare-feu Meraki, IDS/IPS). Identification des points de supervision manquants.
- **Processus Opérationnels :** Processus d'évaluation des vulnérabilités (VA) et de tests d'intrusion (PT) non formalisés. Absence de gestion centralisée des correctifs pour tous les assets.
- **Configuration et Hardening :** Examen des configurations des serveurs (Windows/Linux), des bases de données, des actifs réseau et des postes de travail pour s'aligner sur les meilleures pratiques (CIS Benchmarks).
- **Réponse aux Incidents :** Capacité de détection et de réponse limitée, sans équipe dédiée ni plateforme de corrélation (SIEM).

3. Solutions Proposées et Mises en Œuvre

Notre approche est holistique, couvrant la gouvernance, les processus et les technologies.

a. Gouvernance et Politiques de Sécurité

- **Rédaction et déploiement** d'une **Politique de Sécurité des Systèmes d'Information (PSSI)** cadre (
- **Création de procédures détaillées** :
  - Procédure de gestion des incidents de sécurité.

- Procédure de gestion des vulnérabilités et des correctifs.
- Politique de mot de passe et d'authentification forte (complétant le MFA déjà prévu).
- Politique d'utilisation acceptable des ressources IT (chartes utilisateurs).

- **Définition d'un modèle de responsabilité** (RACI) pour la sécurité.
- **Sensibilisation** obligatoire et régulière des utilisateurs aux risques cyber.

b. Renforcement de l'Architecture et des Configurations

- **Validation et hardening** de la nouvelle architecture réseau (Lot A) selon le principe du "Zero Trust" (jamais confier, toujours vérifier) :
- Audit des règles des pare-feu Meraki MX pour supprimer les règles trop permissives.
- Configuration fine des ACLs et de la segmentation VLAN pour limiter les flux Est-Ouest.
- **Mise en place d'une solution DLP (Data Loss Prevention)** pour contrôler les flux de données sensibles (en sortie du réseau et sur les postes de travail), critical pour la conformité RGPD.
- **Hardening systématique** :
- Application des benchmarks CIS sur tous les serveurs Windows/Linux déployés.
- Configuration sécurisée des bases de données (désactivation de services inutiles, chiffrement des données sensibles).
- Audit de configuration des switchs et routeurs (désactivation des services non utilisés comme Telnet, activation de SNMPv3).

c. Processus de Gestion des Vulnérabilités et Tests

- **Implémentation d'un processus formalisé de gestion des vulnérabilités** :
- **Évaluation Automatique (VA) :** Utilisation de l'outil **Tenable Nessus** pour des scans réguliers (mensuels) de l'ensemble du parc (serveurs, postes, équipements réseau).
- **Tests d'Intrusion (PT) :** Réalisation de tests d'intrusion annuels externes et internes par un prestataire tiers, ainsi que des tests de sécurité des applications web (via l'outil **OWASP**).
- **Gestion des Correctifs :** Intégration des résultats de VA dans GLPI pour prioriser et tracker la fermeture des vulnérabilités. Utilisation de **Microsoft Intune (Lot J)** pour le déploiement automatisé des correctifs clients et serveurs.

d. Mise en place du Security Operations Center (SOC)

Le SOC est le centre névralgique pour la surveillance et la réponse.

- **Architecture Technique du SOC :**
- **SIEM (Security Information and Event Management) :** Déploiement de **Splunk Enterprise** pour agréger et corréler les logs de tous les équipements (Pare-feu, Switch, Serveurs, AD, EDR SentinelOne).
- **Supervision :** Intégration des alertes du SIEM et de Centreon (Lot H) dans une console unique.

- **Intégration des solutions existantes :** Les alertes de **SentinelOne (Lot D)**, des **pare-feu Meraki (Lot A)**, et de l'**IDS/IPS (Lot E)** remontent dans le SIEM.

- **Processus du SOC :**
- **Monitoring 24/7:** Surveillance continue des alertes de sécurité.
- **Tri et Investigation :** Analyse des alertes pour distinguer les faux positifs des vraies menaces.
- **Réponse aux Incidents :** Déclenchement de la procédure de gestion d'incident en cas de détection d'une attaque confirmée.
- **Amélioration Continue :** Affinage régulier des règles de corrélation du SIEM basé sur les faux positifs/négatifs.

- **Plan de Formation** pour les administrateurs qui formeront l'équipe SOC interne de niveau 1.
- **Contrat de Support** avec un SOC externe de niveau 2/3 pour une expertise avancée en cas d'incident majeur.

e. 3.5. Préparation à la Gestion de Crise Cyber

- **Rédaction d'un Plan de Gestion de Cyber-Crise** distinct du PRA, détaillant :
- Les différents scénarios de crise (ransomware, fuite de données, déni de service).
- La composition de la cellule de crise (direction, IT, juridique, communication).
- Les procédures de communication interne et externe (clients, autorités comme l'ANSSI).
- Les décisions à prendre (faut-il payer une rançon ? Quand couper le réseau ?).
- **Organisation d'un exercice de crise** annuel pour tester le plan.

4. Livrables

a. Livrable 1 : Politique de Sécurité des Systèmes d'Information (PSSI)

Objet : Définir le cadre, les objectifs et les principes directeurs de la sécurité des systèmes d'information du Groupe Solaris.
Cible : Tous les collaborateurs, prestataires et partenaires du Groupe Solaris.
Statut : Document approuvé par la Direction.

Extrait des principaux chapitres :

1. **Introduction et Objectifs :** Affirmation de l'engagement de la Direction en faveur de la sécurité de l'information.
2. **Champ d'application :** S'applique à l'ensemble du SI, des données, des équipements et du personnel.
3. **Rôles et Responsabilités :**
    - **Direction :** Validation du budget, support de la stratégie.

- **RSSI (à désigner) :** Pilotage de la sécurité opérationnelle, animation du comité de sécurité.
- **DSI / Administrateurs :** Mise en œuvre technique des mesures de sécurité.
- **Utilisateurs :** Respect des règles de sécurité (cf. charte).

4. **Règles de classification des données :** Définition des niveaux de sensibilité (Publique, Interne, Confidentielle, Restreinte) et des mesures de protection associées.
5. **Principes de sécurité fondamentaux :**
   - **Sécurité des postes de travail :** Chiffrement (BitLocker), verrouillage de session, interdiction des logiciels non autorisés.
   - **Gestion des accès :** Principe du moindre privilège, révocation des accès en cas de départ.
   - **Sécurité physique :** Accès restreint aux salles serveurs.
   - **Sécurité réseau :** Segmentation, règles de pare-feu restrictives.
   - **Protection contre les codes malveillants :** Obligation d'utiliser la solution **SentinelOne** déployée.
   - **Sauvegarde et PRA :** Respect des procédures définies dans les lots dédiés.
6. **Conformité et Révision :** Cette politique est révisée annuellement.

(Annexe : Modèle de charte utilisateur à signer)

b. Livrable 2 : Architecture Technique du SOC

Objectif : Schématiser l'architecture de supervision et les flux de données.

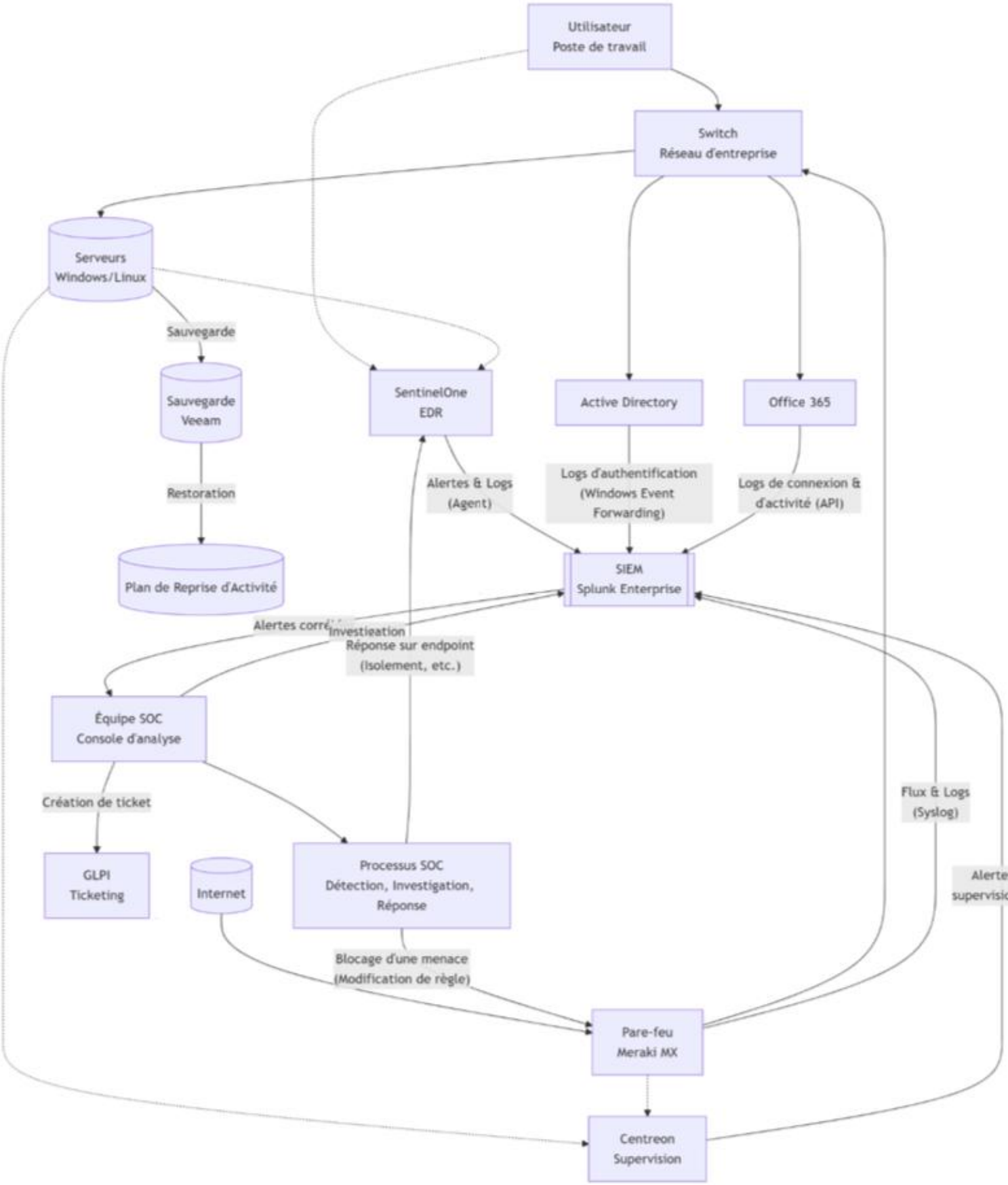


Figure 35 : archi technique SOC

Description :

1. **Sources de Logs :** Tous les équipements (pare-feu Meraki, switchs, serveurs Windows/Linux, Active Directory, SentinelOne, Office 365) envoient leurs logs via l'agent.
2. **Collecte et Corrélation (SIEM) :** Le serveur **Splunk Enterprise** centralise, normalise et corrèle les événements en temps réel.
3. **Console de Supervision :** Les analystes SOC utilisent l'interface Splunk pour investiguer les alertes générées par les règles de corrélation **(exemple : Connexion administrateur hors heures ouvrables + depuis une IP étrangère).**
4. **Intégrations :**
    - **Avec Centreon :** Remontée des alertes de disponibilité dans Splunk pour corrélation **(exemple : Service indisponible + alertes IDS sur le même serveur).**
    - **Avec GLPI :** Création automatique d'un ticket d'incident depuis une alerte Splunk critique.
    - **Avec SentinelOne :** Remontée des alertes EDR (Endpoint Detection and Response) pour une vision endpoint complète.
5. **Stockage :** Les logs sont stockés sur une période de 12 mois (rétention conforme aux bonnes pratiques et exigences légales).

c. Livrable 3 : Plan de Gestion de Cyber-Crise (Extrait)

Scénario : Attaque par Ransomware généralisée

1. **Détection & Alerte :**
    - Le SOC détecte une propagation massive de chiffrement via les alertes SentinelOne et les logs de fichiers.
    - **Action immédiate :** Isolation manuelle ou automatique (via SentinelOne) des premiers postes infectés. Alerte du RSSI et de la Direction.
2. **Activation de la Cellule de Crise :**
    - **Membres :** Directeur Général, RSSI, DSI, Responsable Communication, Responsable Juridique.
    - **Outils :** Canal de communication sécurisé alternatif.
3. **Diagnostic et Confinement :**
    - Évaluer l'étendue de l'attaque : nombre de postes/serveurs touchés, données impactées.
    - **Décision stratégique :** Déconnexion contrôlée des segments réseau critiques pour contenir la propagation.

4. **Communication :**
    - **Interne :** Informer les employés via un canal sain (email externe, affichage) sans divulguer de détails techniques.
    - **Externe :** Préparer un communiqué pour les clients/partenaires. Notification à l'ANSSI (obligation légale en cas de fuite de données).
5. **Éradication et Récupération :**
    - Identifier et corriger le vecteur d'entrée (ex.: faille non patchée, email de phishing).
    - Restaurer les systèmes à partir des sauvegardes saines (**ref. Lot 1**).
    - Ré-imager complètement les postes de travail infectés.
6. **Post-Mortem :**
    - Analyse rétrospective ("Lessons Learned") pour améliorer les processus et les défenses.
    - Mise à jour du présent plan de crise.

d. Livrable 4 : Tableau de Bord des Métriques Cybersécurité (KPI)

Objectif : Mesurer l'efficacité des contrôles de sécurité et la performance du SOC.

Métrique	Calcul	Cible	Fréquence
Temps Moyen de Détection (MTTD)	(Heure de détection - Heure de début de l'incident) / Nbr d'incidents	< 1 heure	Mensuelle
Temps Moyen de Réponse (MTTR)	(Heure de résolution - Heure de détection) / Nbr d'incidents	< 4 heures	Mensuelle
% de Correctifs Critiques Appliqués	(Nbr de systèmes patchés / Nbr total de systèmes) x 100	> 95% en 7j	Hebdomadaire
Taux d'Alertes Traitées	(Nbr d'alertes traitées / Nbr total d'alertes) x 100	100%	Quotidienne
Nombre d'Incidents de Sécurité	Nombre total d'incidents confirmés	Tendance à la baisse	Mensuelle

Métrique	Calcul	Cible	Fréquence
Taux de Réussite des Tests de Phishing	(Nbr de clics / Nbr de mails envoyés) x 100	< 5%	Trimestrielle

Tableau 27 : Tableau de Bord des Métriques Cybersécurité (KPI)

e. Livrable 5 : Plan de Formation de l'Équipe SOC Niveau 1

Objectif : Former les administrateurs système existants aux fondamentaux de l'analyse SOC.

- **Module 1 : Fondamentaux de la Cybersécurité (2 j)**
  - Paysage des menaces, types d'attaques, Kill Chain.
- **Module 2 : Lecture et Analyse des Logs (3 j)**
  - Formats de logs (Syslog, EVTX), analyse des logs Windows (AD, authentification) et réseau (pare-feu).
- **Module 3 : Utilisation Avancée de Splunk (5 j)**
  - SPL (Search Processing Language), création d'alertes et de tableaux de bord.
- **Module 4 : Initiation à la Réponse aux Incidents (3 j)**
  - Méthodologie (NIST SP 800-61), utilisation des outils d'investigation (EDR SentinelOne).
- **Hands-On :** Exercices sur plateforme de test, simulation de crise.

R. Simulation des tests clients par lot

1. Lot A – Solution Réseau

- Test client : connexion au réseau depuis un poste sur le site de Lyon et navigation Internet fluide. Test du VPN AnyConnect pour un accès distant.
- Résultat attendu : obtention d'une adresse IP conforme au plan d'adressage, résolution DNS opérationnelle, latence < 50 ms vers Paris, VPN stable et authentifié MFA.

2. Lot B – Postes clients (légers et lourds)

- Test client : connexion sur un poste lourd et un poste léger avec un compte utilisateur LDAP.
- Résultat attendu : démarrage < 45 sec, accès au bureau personnalisé, applications standards disponibles (Office, navigateur sécurisé).

3. Lot C – Migration Office 365

- Test client : ouverture Outlook, accès Teams et OneDrive.
- Résultat attendu : authentification MFA, boîtes mails synchronisées, fichiers collaboratifs accessibles et partage SharePoint fonctionnel.

4. Lot D – Antivirus centralisé (SentinelOne)

- Test client : simulation d'un fichier de test EICAR.
- Résultat attendu : détection instantanée, alerte dans la console centrale, fichier bloqué sans impact utilisateur.

5. Lot E – IDS/IPS

- Test client : tentative de scan réseau depuis un poste de test.
- Résultat attendu : alerte générée dans le SIEM, blocage de l'adresse source par l'IPS.

6. Lot F – Audit de sécurité

- Test client : vérification des correctifs sur un poste Windows.
- Résultat attendu : OS et applications à jour, absence de vulnérabilités critiques dans OpenVAS.

7. Lot G – PCA/PRA

- Test client : simulation d'une panne serveur principal (arrêt volontaire d'un hôte virtualisé).
- Résultat attendu : bascule automatique sur site de secours, temps de reprise (RTO) < 2h, perte de données < 15 min (RPO).

8. Lot H – Monitoring & Ticketing

- Test client : arrêt d'un service applicatif (ex. DHCP).
- Résultat attendu : alerte Centreon en < 2 min, création automatique d'un ticket GLPI attribué au support.

9. Lot I – Gestion de parc et maintenance

- Test client : inventaire automatique d'un nouveau poste ajouté au réseau.
- Résultat attendu : détection dans GLPI, installation des agents, rattachement automatique au bon site.

10. Lot J – Déploiements et mises à jour

- Test client : envoi d'une mise à jour Windows sur un groupe de 10 postes.
- Résultat attendu : installation silencieuse, redémarrage planifié, reporting Intune confirmant le succès à 100 %.

11. Lot 1 – Stockage et sauvegarde

- Test client : restauration d'un fichier supprimé dans OneDrive et depuis Veeam Backup.
- Résultat attendu : récupération possible via interface utilisateur et via console d'admin.

12. Lot 2 – LDAP

- Test client : connexion unique (SSO) à Outlook et SAP Marketing.
- Résultat attendu : authentification unique réussie, logs centralisés dans AD.

13. Lot 3 – Virtualisation

- Test client : lancement d'une nouvelle VM depuis vCenter.
- Résultat attendu : déploiement via template < 10 min, VM opérationnelle.

14. Lot 4 – Migration Messagerie

- Test client : envoi d'un mail externe avec pièce jointe suspecte.
- Résultat attendu : mail bloqué/quarantaine, log visible dans Defender for O365 et Cisco Secure Email.

15. Lot 5 – Base de données

- Test client : requête SQL sur la base Oracle migrée.
- Résultat attendu : temps de réponse < 1 sec, intégrité et cohérence des données vérifiées.

16. Lot 6 – VOIP

- Test client : appel interne Paris ↔ Lyon et appel externe.
- Résultat attendu : qualité audio HD (MOS > 4), absence de coupures, enregistrement et supervision disponibles.

Proposition de Devis – Projet Solaris

Affaire suivie par
Abcdee trezsz
☎ 01 70 03 85
E-mail : **abcdee.trezsz@netproconsulting.fr**

SOLARIS

A l'attention de Yacine DELAPIERRE

Paris, le 01 Mars 2025

Proposition Commerciale

Réf : VEN/DEV/OZ/Solaris/25/OP-7860039396

Objet : Modernisation du parc informatique Solaris

Monsieur,

Pour donner suite à notre étude sur site, vous trouverez ci-dessous notre offre commerciale concernant la prestation en objet.

Lot / Poste	Montant (€ HT)
Lot A – Réseau (switchs, firewalls, Wi-Fi, WAN)	1 050 000 €
Lot B – Postes clients + Serveurs	1 050 000 €
Lot C – Licences O365 (3 ans, 1000 users)	1 200 000 €
Lot D – Antivirus SentinelOne (3 ans)	300 000 €
Lot E – IDS/IPS	150 000 €
Lot F – Audit sécurité	50 000 €
Lot G – PCA/PRA	400 000 €
Lot H – Monitoring & Ticketing	100 000 €
Lot I – Gestion de parc & maintenance	180 000 €
Lot J – Déploiements & mises à jour	100 000 €
Lot 1 – Stockage & sauvegarde	500 000 €
Lot 2 – LDAP	80 000 €
Lot 3 – Virtualisation (VMware + serveurs)	420 000 €
Lot 4 – Migration messagerie	150 000 €
Lot 5 – Base de données	150 000 €

Lot 6 – VOIP (1000 téléphones + infra)	320 000 €
Sécurité physique (clim + détection incendie 8 salles)	480 000 €
Lot supplémentaire – Cybersécurité & SOC	1 850 000 €
Main d'œuvre & services (intégration, migration, formation, support 3 ans)	800 000 €
TOTAL HT	9 330 000 €
TVA (20%)	1 866 000 €
TOTAL TTC	11 196 000 €

Durée de validité de la proposition

Cette proposition commerciale est valable 2 mois. Au-delà de cette date, **Netpro consulting** se réserve le droit d'en modifier les conditions.

Délais

Le délai de livraison du projet est de 8 mois à réception de la commande.

Facturation

La signature du PV de recette déclenchera le paiement des frais d'installation et le début des redevances mensuels

Espérant avoir répondu à vos attentes, et restant à votre disposition pour tout renseignement

Complémentaire, nous vous prions de croire, Monsieur, en l'expression de nos salutations distinguées.

PV de recette finale

Objet : Validation des solutions déployées dans le cadre du projet Solaris
Participants : Équipe projet NetPro Consulting et projet Solaris.

Constats :
L'ensemble des lots **A à J** et **1 à 6** ainsi que le lot supplémentaire (Cybersécurité et SOC) ont fait l'objet de tests fonctionnels et techniques. Tous les scénarios clients définis dans le cahier de recette ont été exécutés.

Résultats :

- 100 % des tests sont concluants.
- Aucune anomalie bloquante n'a été constatée.
- Des ajustements mineurs (documentation utilisateur, formation complémentaire) seront suivis en phase d'exploitation.

Réserve :

- Pour des raisons de sécurité, nous avons installé **Windows server 2022**, car installé windows server 2025 à date d'aujourd'hui sera exposé l'entreprise aux attaques de type **zero day**. Nous reviendrons dans un an pour installer Windows server 2025 à nos frais toute charge comprise.

Décision :
Le PV de recette est **validé** sous réserve mentionnée et le projet peut être transféré en exploitation courante.

Fait à Paris, le 10 novembre 2025

Signatures :

Chef de projet NetPro Consulting	Responsable DSI Solaris	Chef de projet Solaris

En l'absence de réserves formulées par le client dans les 20 jours ouvrés suivant la date d'émission de ce PV de réception, le service sera réputé accepté par le client à la date de mise en service indiquée sur le présent document.

Conclusion

La modernisation de l'infrastructure informatique du Groupe Solaris, réalisée en par NetPro Consulting, constitue une étape stratégique pour assurer la pérennité, la performance et la sécurité du système d'information. L'audit initial a permis de mettre en évidence de nombreuses faiblesses matérielles et logicielles, ainsi que des risques majeurs en termes de cybersécurité et de continuité de service.

Grâce aux solutions proposées : refonte de l'architecture réseau, mise à jour des systèmes, déploiement de technologies de haute disponibilité, centralisation des sauvegardes et intégration d'outils de sécurité avancés. Solaris dispose désormais d'une infrastructure robuste, évolutive et conforme aux standards actuels.

Ce projet ne se limite pas à une simple mise à niveau technique : il s'inscrit dans une démarche globale visant à améliorer la productivité, à réduire les coûts opérationnels et à garantir la résilience de l'entreprise face aux crises. En consolidant son infrastructure IT, Solaris renforce également sa capacité à accompagner sa croissance et à soutenir ses engagements en matière d'écologie industrielle.

Ainsi, cette modernisation représente non seulement une réponse immédiate aux enjeux identifiés, mais aussi une base solide pour relever les défis futurs du numérique et de la cybersécurité.

Annexes

PBS (Product Breakdown Structure)

WBS (Work Breakdown Structure)

OBS (Organisationnel Breakdown Structure)

PoE (Power over Ethernet)

BYOD (Bring Your Own Device)

STP (*Spanning Tree Protocol*)

MPLS (Multiprotocole Label Switing)

MSTP (Multiple Spanning Tree Protocole)

MLAG (Multi-Chassis Link Aggregation Group)

SV (StackWise Virtual)

VSS (Virtual Switching System)

VTP (VLAN Trunking Protocol)

IPSec (Internet Protocol Security)

VPN (Virtual Private Networks)

FTTO (Fibre To The Office)

FTTH (Fibre To The Home)

CPE (Customer Premises Equipment)

MEC (Multi-Chassis EtherChannel)

VLSM (Variable Length Subnet Masking)

BYOD (Bring Your Own Device)

IDS (système de détection des intrusions)

IPS (système de prévention des intrusions)

PCA (Plan de continuité des Activités)

PRA (Plan de Reprise d'Activité)

PMDT (Perte Maximal de Données Tolérable)

DMIA (Durée Maximale d'Interruption Admissible)

OMCA (Objectif Minimal de Continuité d'Activité)

GLPI (Gestion Libre de Parc Informatique)

LDAP (Lightweight Directory Access Protocol)

MFA (Multi-Factor Authentication)

S. MANUEL DE CONFIGURATION DES EQUIPEMENTS RESEAUX :

1. Matrice de brassage

Equipement Source	Ports Source (Exemple)	Equipement Destination	Ports Destination (Exemple)	Type de Lien
WAN / Firewalls				
FAI 1	Fibre	MX250-1	ge-0/0/0	Fibre
FAI 2	Fibre	MX250-2	ge-0/0/0	Fibre
MX250-1 (Lien DMZ)	ge-0/0/1	SW-DMZ-1	Gi1/0/1	Cuivre
MX250-2 (Lien DMZ)	ge-0/0/1	SW-DMZ-2	Gi1/0/1	Cuivre
Cœur de Réseau (SWC)				
SWC-1	Te1/1/1, Te1/1/2	MX250-1	ge-0/0/2, ge-0/0/3	Fibre
SWC-2	Te2/1/1, Te2/1/2	MX250-2	ge-0/0/2, ge-0/0/3	Fibre
Distribution -> Cœur				
SWD-1 (Stack 1)	Gi1/1/1, Gi1/1/2	SWC-1	Te1/1/3, Te1/1/4	Fibre
SWD-1 (Stack 1)	Gi1/1/3, Gi1/1/4	SWC-2	Te2/1/3, Te2/1/4	Fibre
SWD-2 (Stack 1)	Gi2/1/1, Gi2/1/2	SWC-1	Te1/1/5, Te1/1/6	Fibre
SWD-2 (Stack 1)	Gi2/1/3, Gi2/1/4	SWC-2	Te2/1/5, Te2/1/6	Fibre
… on fera de même pour chaque **SWD**	…	…	…	…
Accès -> Distribution				
Stack Accès 1 (SWA1-1, SWA1-2)	Gi1/0/49, Gi1/0/50 (SWA1-1)	SWD-1 (Stack 1)	Gi1/1/5, Gi1/1/6	Fibre
Stack Accès 1 (SWA1-1, SWA1-2)	Gi2/0/49, Gi2/0/50 (SWA1-2)	SWD-3 (Stack 2)	Gi2/1/5, Gi2/1/6	Fibre
Stack Accès 2 (SWA2-1, SWA2-2)	Gi1/0/49, Gi1/0/50 (SWA2-1)	SWD-1 (Stack 1)	Gi1/1/7, Gi1/1/8	Fibre
Stack Accès 2 (SWA2-1, SWA2-2)	Gi2/0/49, Gi2/0/50 (SWA2-2)	SWD-3 (Stack 2)	Gi2/1/7, Gi2/1/8	Fibre
… on fera de meme pour	…	…	…	…

chaque **stack d'accès**				
Terminaux finaux -> Accès				
Pc client	RJ45	SWA	Gi 1/0/0 à Gi 1/0/48	Cuivre cat6
Pc serveur	RJ45	SWA	Gi 1/0/0 à Gi 1/0/49	Cuivre cat6A

Tableau 28 : Matrice de brassage

2. Procédures de Configuration

Voici les procédures type pour chaque type d'équipement.

a. Configuration des Switchs de Cœur (SWC1 & SWC2) - StackWise Virtuel

Objectif : Créer le domaine SVL, configurer le routage inter-VLAN, et les liens uplink/downlink redondants.

Étape 1: **Configuration de Base & StackWise Virtuel**

Faire cette configuration sur les deux switchs individuellement AVANT de connecter le lien de contrôle SVL.

- **Sur SWC-1 (Switch Actuel)**

hostname SWC-CORE

switch virtual domain 10

switch 1 priority 15

switch 2 priority 14

- **Sur SWC-2**

hostname SWC-CORE

switch virtual domain 10

switch 1 priority 14

switchC-2 priority 15

- Sur les deux switches, assigner les ports dédiés au lien de contrôle SVL : Cela va REBOOTER les switches pour former le stack.

interface HundredGigabitEthernet1/0/1

description SVL-Link-to-SWC-2

switch virtual link 1

no shutdown

- Répéter sur le deuxième port pour la redondance

interface HundredGigabitEthernet1/0/2

description SVL-Link-to-SWC-2

switch virtual link 1

no shutdown

Étape 2: Création des VLANs

La configuration est répliquée automatiquement sur les deux membres du stack.

```
vlan 10
 name Infra-Wi-Fi
… créer chaque vlan
```

Étape 3: Configuration des Interfaces LAG (Uplink vers Firewalls)

Ces commandes créent un canal logique regroupant 2 liens physiques.

```
interface Port-channel10
 description LAG-PEER-MX250-1
 no switchport ! Met le port en mode L3 pour le routage
 ip address 172.10.255.1 255.255.255.252 ! IP sur un /30 point-à-point
```

Assigner les ports physiques vers ce groupe

```
interface TenGigabitEthernet1/1/1
 description To-MX250-1-P1
 no switchport
 channel-group 10 mode active ! Protocol LACP
 no shutdown
interface TenGigabitEthernet2/1/1
 description To-MX250-1-P2
 no switchport
 channel-group 10 mode active
 no shutdown
interface Port-channel11
 description LAG-PEER-MX250-2
 no switchport
 ip address 172.10.255.5 255.255.255.252
interface TenGigabitEthernet1/1/2
 description To-MX250-2-P1
 no switchport
 channel-group 11 mode active
 no shutdown
interface TenGigabitEthernet2/1/2
```

description To-MX250-2-P2

no switchport

channel-group 11 mode active

no shutdown

Étape 4: Configuration des Interfaces LAG (Downlink vers Distribution)

interface Port-channel20

description LAG-PEER-SWD-Stack1

switchport mode trunk

switchport trunk native vlan 50 ##VLAN de management comme native

switchport trunk allowed vlan 10,20,30,40,50,60,70,80,100,110,120,130,140,150,160 ! Liste tous les VLANs nécessaires aux users

interface TenGigabitEthernet1/1/3

description To-SWD1-Stack1-P1

channel-group 20 mode active

no shutdown

interface TenGigabitEthernet1/1/4

description To-SWD1-Stack1-P2

channel-group 20 mode active

no shutdown

Répéter pour le lien vers SWD-Stack2 (Port-channel21)

Étape 5: Configuration du Routage Inter-VLAN

Activer le routage IP

ip routing

Créer une Interface VLAN (SVI) pour chaque VLAN qui doit être routé au cœur

interface Vlan50

description Gateway-Management

ip address 172.10.16.1 255.255.255.128

! interface Vlan10

! description Gateway-Infra-WiFi

! ip address 172.10.0.1 255.255.248.0

! ... (Configurer les SVIs pour tous les VLANs qui ont une Gateway)

Étape 6: Routage Statique vers les Firewalls

ip route 0.0.0.0 0.0.0.0 172.10.255.2 ##Next-hop vers MX250-1

ip route 0.0.0.0 0.0.0.0 172.10.255.6 ## Next-hop vers MX250-2

Étape 7: Management

Définir l'IP de management sur le VLAN dédié

interface Vlan50

ip address 172.10.16.2 255.255.255.128

Configurer un utilisateur et activer SSH

username **admin** privilege 15 secret 0 **V0tr3_M0t2d3P@ss3**

line vty 0 15

transport input ssh

login local

Configurer la passerelle par défaut pour le trafic management

ip default-gateway 172.10.16.1

b. Configuration des Switchs de Distribution (SWD1 & SWD2) - StackWise Virtuel

Objectif : Agréger les liens des switchs d'accès et faire remonter le trafic vers le cœur. Ils agissent principalement comme des switches L2.

Étape 1: Configuration du StackWise Virtuel (Similaire au Cœur)

hostname SWD-DISTRIB

switch virtual domain 20

- Sur le premier switch du stack

switch 1 priority 15

- Sur le deuxième switch du stack

switch 2 priority 14

- Configurer les liens SVL sur les deux switches

interface HundredGigabitEthernet1/0/1

switch virtual link 1

no shutdown

interface HundredGigabitEthernet1/0/2

switch virtual link 1

no shutdown

Étape 2: Création des VLANs

vlan 10,20,30,40,50,60,70,80,100,110,120,130,140,150,160

Étape 3: Configuration des Uplinks vers le Cœur (LAG en Trunk)

```
interface Port-channel10
 description LAG-PEER-SWC-CORE
 switchport mode trunk
 switchport trunk native vlan 50
 switchport trunk allowed vlan 10,20,30,40,50,60,70,80,100,110,120,130,140,150,160
## Assigner les ports physiques
interface TwentyFiveGigE1/1/1
 description To-SWC1-P1
 channel-group 10 mode active
 no shutdown
interface TwentyFiveGigE1/1/2
 description To-SWC1-P2
 channel-group 10 mode active
 no shutdown
## Répéter pour le 2ème LAG (Port-channel11) vers SWC-2
```

Étape 4: Configuration des Downlinks vers les Stacks d'Accès (LAG en Trunk)

```
interface Port-channel20
 description LAG-PEER-SWA-Stack1
 switchport mode trunk
 switchport trunk native vlan 50
 switchport trunk allowed vlan 10,20,30,40,60,70,80,100,110,120,130,140,150,160! VLANs nécessaires pour ce stack d'accès
interface GigabitEthernet1/1/5
 description To-SWA-Stack1-P1
 channel-group 20 mode active
 no shutdown
interface GigabitEthernet1/1/6
 description To-SWA-Stack1-P2
 channel-group 20 mode active
 no shutdown
## Répéter pour chaque stack d'accès (Port-channel21, 22)
```

Étape 5: Management

```
interface Vlan50
 ip address 172.10.16.3 255.255.255.128 ! .3 pour le switch de distri
ip default-gateway 172.10.16.1 ! Gateway = SVI du VLAN 50 sur le Cœur
username admin privilege 15 secret 0 V0tr3_M0t2d3P@ss3
line vty 0 15
 transport input ssh
 login local
```

c. Configuration des Switchs d'Accès (SWA) - Stack Physique

Objectif : Fournir un accès réseau aux utilisateurs finaux.

Étape 1: Configuration du Stack Physique

- Sur le premier switch (Master)

```
switch 1 provision ws-c3850-48x ! Remplacer par le bon modèle
```

- Sur le deuxième switch (Member)

```
switch 2 provision ws-c3850-48x
```

Étape 2: Configuration de Base du Stack

```
hostname SWA-ACCESS-STACK1
## Créer les VLANs qui seront utilisés sur les ports d'accès de CE stack
vlan 10,20,30,70,80,160
```

Étape 3: Configuration des Uplinks vers la Distribution (LAG en Trunk)

```
interface Port-channel10
 description LAG-PEER-SWD-DISTRIB
 switchport mode trunk
 switchport trunk native vlan 50
 switchport trunk allowed vlan 10,20,30,70,80,160,50
## Lier un port physique du premier switch au premier switch de distribution
interface GigabitEthernet1/0/49
 description To-SWD1-Gi1/1/5
 channel-group 10 mode active
 no shutdown
## Lier un port physique du deuxième switch au deuxième switch de distribution
interface GigabitEthernet2/0/49
 description To-SWD2-Gi2/1/5
```

```
 channel-group 10 mode active
 no shutdown
```

Étape 4: Configuration des Ports d'Accès Utilisateurs

```
interface range GigabitEthernet1/0/1-24, GigabitEthernet2/0/1-24
 switchport mode access
 switchport access vlan 70
 switchport voice vlan 20 ! Si VoIP directement sur le port PC
 spanning-tree portfast
 spanning-tree bpduguard enable
## Exemple pour un port dans le VLAN 160 (Imprimante)
interface GigabitEthernet1/0/48
 description Printer-Room1
 switchport mode access
 switchport access vlan 160
 spanning-tree portfast
 spanning-tree bpduguard enable
 no shutdown
```

Étape 5: Management

```
interface Vlan50
 ip address 172.10.16.4 255.255.255.128 ! .4 pour ce stack d'accès
ip default-gateway 172.10.16.1 ! Gateway = SVI du VLAN 50 sur le Cœur
username admin privilege 15 secret 0 V0tr3_M0t2d3P@ss3
line vty 0 15
 transport input ssh
 login local
```

T. Déploiement de Splunk Enterprise

1. Configurations Serveur splunk

a. Installation de splunk entreprise

- **Création d'un compte ;**
- **Téléchargement de Splunk Enterprise 9.4.1**

wget -O splunk-9.4.1-e3bdab203ac8-linux-amd64.deb https://download.splunk.com/products/splunk/releases/9.4.1/linux/splunk-9.4.1-e3bdab203ac8-linux-amd64.deb

- **Extraction des fichiers**

sudo dpkg -i splunk-9.4.1-e3bdab203ac8-linux-amd64.deb

- **Accepter la licence et démarrer Splunk Enterprise 9.4.1**

cd /opt/splunk/bin

sudo ./Splunk start --accept-license

*Suite à cette commande on vous invitera à créer un **user** et un **mot de passe***

b. Configuration du port 9997 et activation du ssh

lancer localhost:8000 dans un navigateur
aller dans setting
puis server setting
General setting
activer ssh
puis dans forwading and receiving
dans Receive data
ajouter le port 9997

c. Autoriser le port 9997 via le pare-feu

sudo ufw allow 9997/tcp

sudo ufw enable

2. Configuration client Ubuntu

a. Installation de splunkforwader

- **Téléchargement de splunkforwader**

wget -O splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb https://download.splunk.com/products/universalforwarder/releases/9.4.1/linux/splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb

```
kevin@ubuntu:~$ wget -O splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb "https://download.splunk.com/products/uni
alforwarder/releases/9.4.1/linux/splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb"
--2025-04-17 10:13:46--  https://download.splunk.com/products/universalforwarder/releases/9.4.1/linux/splunkforwarde
4.1-e3bdab203ac8-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 99.86.91.80, 99.86.91.10, 99.86.91.2, ...
Connecting to download.splunk.com (download.splunk.com)|99.86.91.80|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 99029222 (94M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb'

splunkforwarder-9.4.1-e3bdab2 100%[================================================>]  94,44M   385KB/s    in 2m 0s

2025-04-17 10:15:48 (803 KB/s) - 'splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb' saved [99029222/99029222]
```

- **Extraction des fichiers**

dpkg -i splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb

```
kevin@ubuntu:~$ sudo dpkg -i splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb
[sudo] password for kevin:
Sélection du paquet splunkforwarder précédemment désélectionné.
(Lecture de la base de données... 110334 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb ...
no need to run the pre-install check
Dépaquetage de splunkforwarder (9.4.1) ...
Paramétrage de splunkforwarder (9.4.1) ...
find: '/opt/splunkforwarder/lib/python3.7/site-packages': No such file or directory
find: '/opt/splunkforwarder/lib/python3.9/site-packages': No such file or directory
complete
```

- **Accepter la licence et démarrer Splunkforwader**

cd /opt/splunk/bin

sudo ./Splunk start --accept-license

*Suite à cette commande on vous invitera à créer un **user** et un **mot de passe***

```
kevin@ubuntu:~$ cd /opt/splunkforwarder/bin
kevin@ubuntu:/opt/splunkforwarder/bin$ sudo ./splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: Administrateur
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.
```

b. Vérification du status du splunkforwarder

La commande *Sudo /opt/splunkforwarder/bin/splunk status* permet de vérifier le status. Si le splunkforwarder est bien installé et fonctionne correctement, on aura ce résultat.

```
kevin@ubuntu:/opt/splunkforwarder/bin$ sudo /opt/splunkforwarder/bin/splunk status
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
splunkd is running (PID: 15010).
splunk helpers are running (PIDs: 15046).
```

c. Configuration du Splunkforwarder pour qu'il pointe vers le serveur Splunk

- **Configuration du Splunkloader pour qu'il envoie ses logs au serveur Splunk**

Sudo /opt/splunkforwarder/bin/splunk add forward-server ipserveur:9997 -auth user:mdp

```
kevin@ubuntu:/opt/splunkforwarder/bin$ sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168
.1.150:9997 -auth Azerty1234@:Azerty1234@
[sudo] password for kevin:
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 192.168.1.150:9997.
```

- **Configuration du splunkforwader pour qu'il se connecte au serveur de déploiement**

Sudo /opt/splunkforwarder/bin/splunk set deploy-poll ipserveur:8089 -auth user:mdp

```
kevin@ubuntu:/opt/splunkforwarder/bin$ sudo /opt/splunkforwarder/bin/splunk set deploy-poll 192.168.1.
150:8089 -auth Azerty1234@:Azerty1234@
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Configuration updated.
```

- **Verification si le client est connecté au server splunk**

La commande *Sudo /opt/splunkforwarder/bin/splunk list forward-server* permet de vérifier si le client est connecté au serveur Splunk. Si les configurations ont été bien effectuées on aura cette capture d'écran.

```
kevin@ubuntu:/opt/splunkforwarder/bin$ sudo /opt/splunkforwarder/bin/splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Active forwards:
        192.168.1.150:9997
Configured but inactive forwards:
        None
```

d. Redémarrer la machine cliente ubuntu

reboot

3. Collecte des logs systèmes de ubuntu (Splunkforwarder) sur le serveur Splunk

a. Configuration de l'indexe

lancer localhost:8000 dans un navigateur

aller dans setting

puis indexes

new index

ajouter ubuntu

ubuntu	Edit	Delete	Disable	Events	search	1 MB	500 GB	0		$SPLUNK_DB/ubuntu/db	N/A	✓ Enabled

b. Ajout de ubuntu aux forwarder

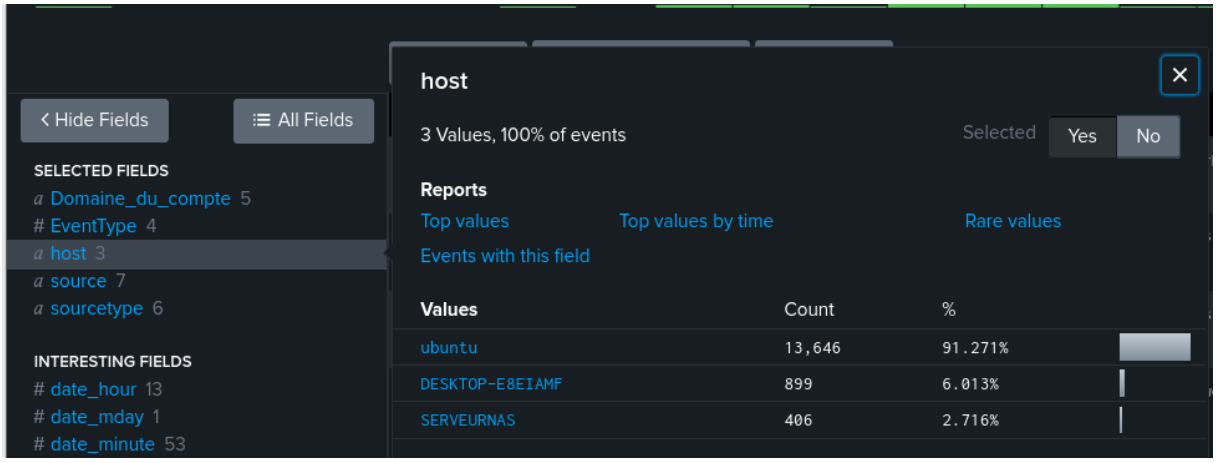
lancer localhost:8000 dans un navigateur

aller dans setting

puis Add Data

Forward

***ajouter ubuntu* puis poursuivre l'installation jusqu'au bout.**



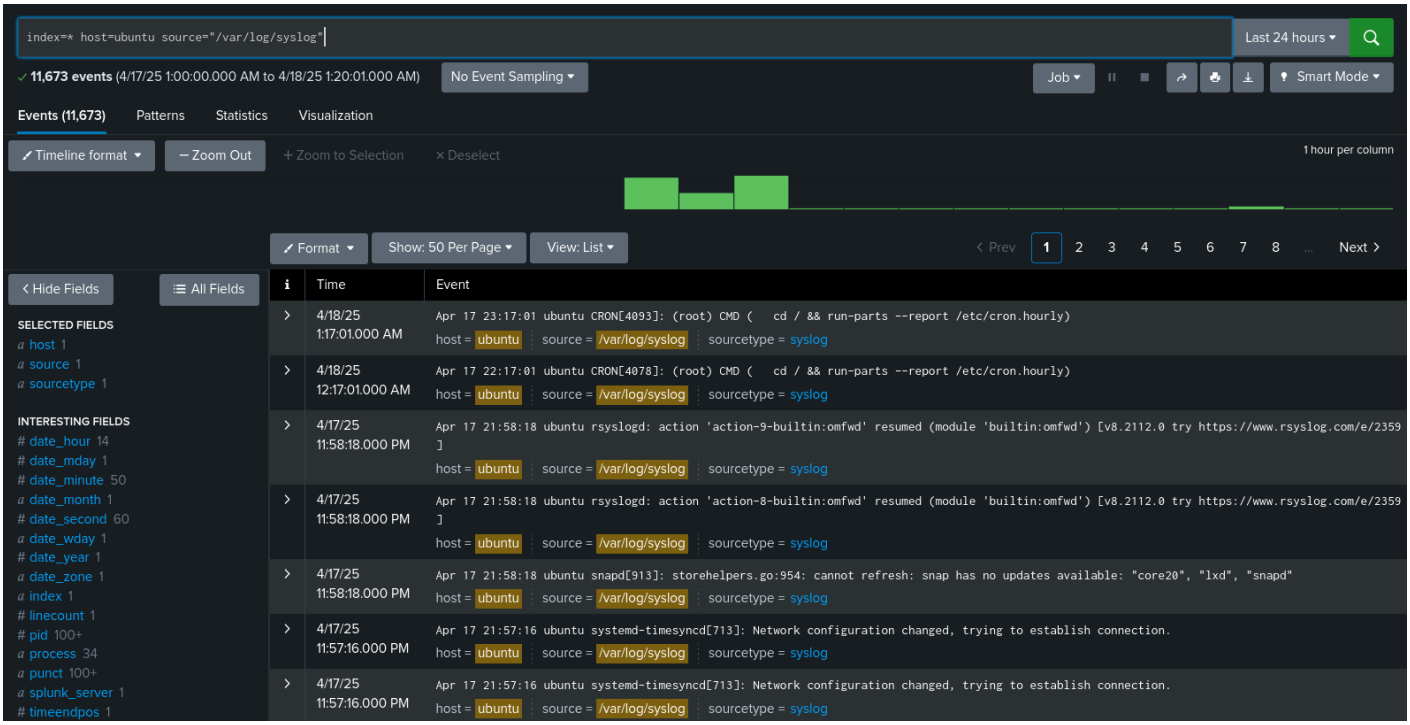
c. Collecte des logs systèmes de la machine ubuntu

lancer localhost:8000 dans un navigateur

cliquez sur splunk>enterprise *puis* Search & Reporting

dans la barre de recherche, saisissez la requête

index= host=ubuntu source="/var/log/syslog"*



4. Cas pratique 1 : Simulation d'une attaque Brute Force sur le port RDP (Remote Desktop Protocol)

L'attaque par Force brute consiste à deviner ou casser un mot de passe ou une clé secrète en testant automatiquement toutes les combinaisons possibles, ou en parcourant une liste de mots de passe courants jusqu'à trouver le bon.

Dans ce TP je vais configurer le RDP sur windows, puis je vais simuler une attaque par force brute à partir de ma machine ubuntu (IP 192.168.1.152).

L'objectif est de pouvoir obtenir les informations (ip, nom de ma machine, …) sur la machine utilisée par l'attaquant à partir des logs remontés dans Splunk.

a. Configurer RDP sur Windows (machine cible)

Etapes de configuration :

*Allez dans **Paramètres → Système → Bureau à distance**.*

*Active **Autoriser les connexions à distance à cet ordinateur**.*

b. Simulation d'attaque brute force via RDP (Ubuntu attackant)

Pour simuler une attaque de brute force sur RDP, on peut utiliser un outil comme **Hydra**. Hydra tente plusieurs combinaisons de mots de passe sur un service donné. Voici comment l'utiliser :

Depuis une machine attaquante (ubuntu),

Installer hydra : Sudo apt install hydra
Créer un fichier contenant plusieurs mots de passe (password-list.txt)
Exécute cette commande pour simuler l'attack:

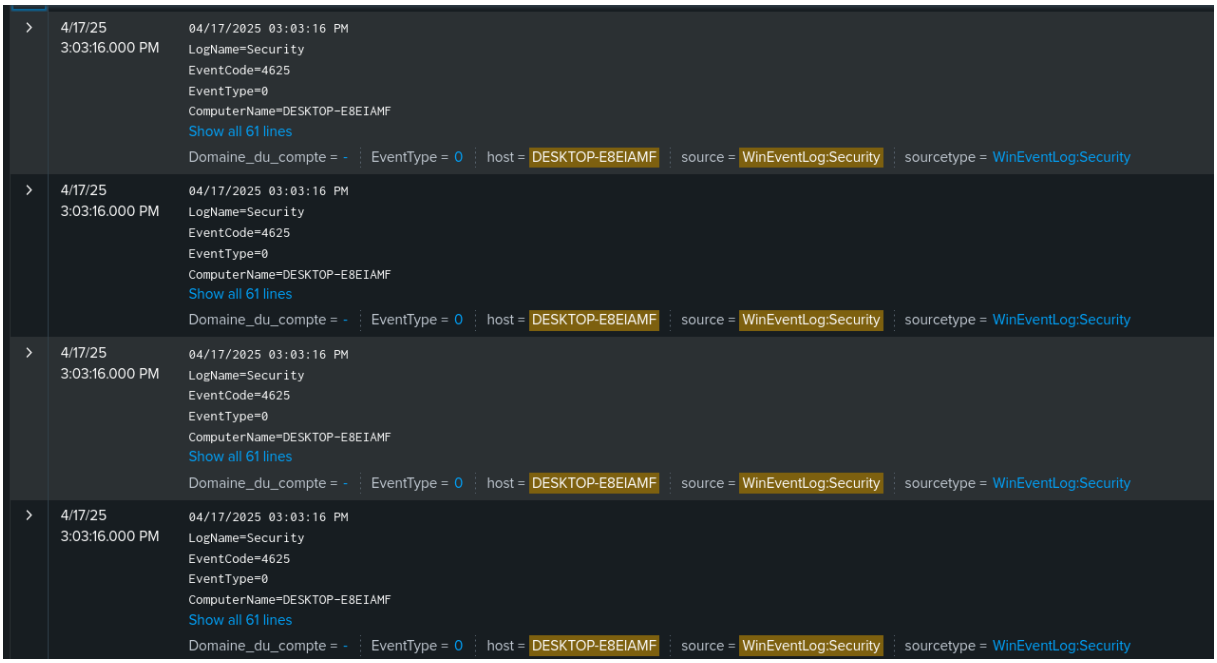
hydra -l admin -P /home/kevin/password-list.txt rdp://192.168.1.153

```
kevin@ubuntu:~$ hydra -l Administrateur -P /home/kevin/password-list.txt rdp://192.168.1.153
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-17 13:03:14
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections a
nd -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 20 login tries (l:1/p:20), ~5 tries per task
[DATA] attacking rdp://192.168.1.153:3389/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-04-17 13:03:16
kevin@ubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
```

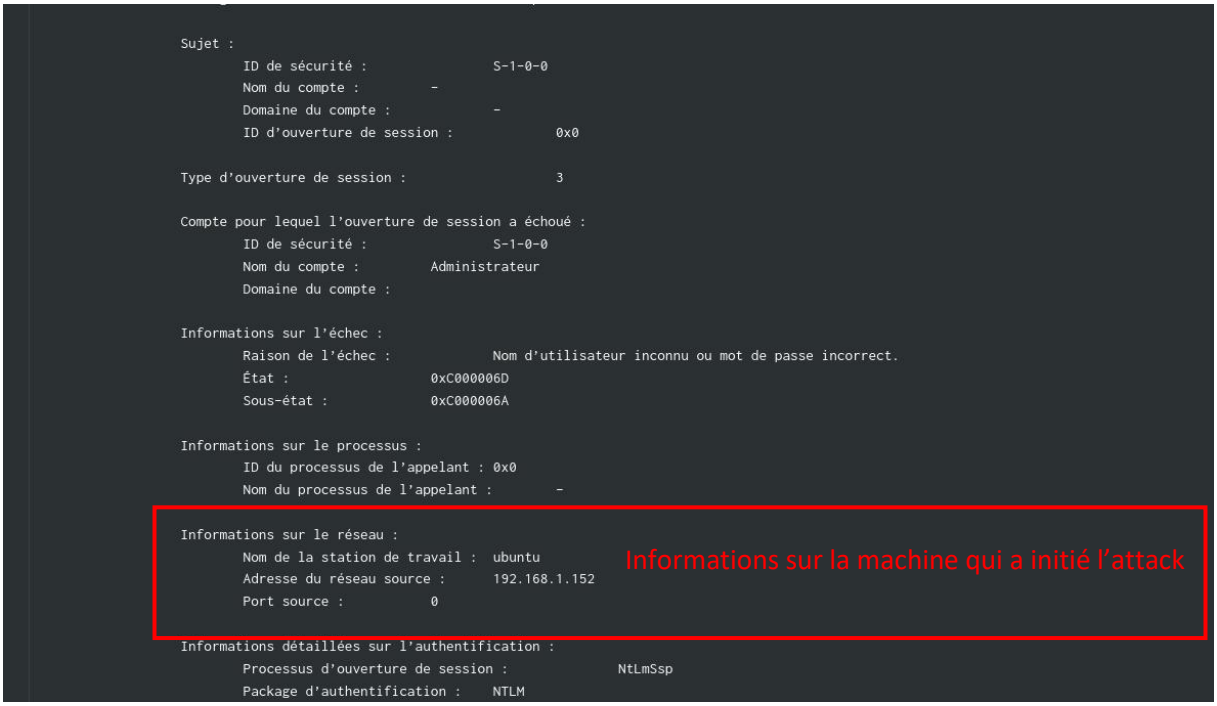
c. Résultat : Analyse des Logs sur Splunk

Nous allons lancer la recherche

index=* host="DESKTOP-E8EIAMF" source="WinEventLog:Security" EventCode=4625



Si on clique sur Show all lines, on peut avoir les informations sur la machine qui essaie de se connecter au bureau à distance. Sur cette capture on voit que la connexion provient d'une station de travail **ubuntu** avec pour adresse **192 .168.1.152.**



5. Cas pratique 2 : Ajout suspect d'un nouvel utilisateur administrateur

Objectif :

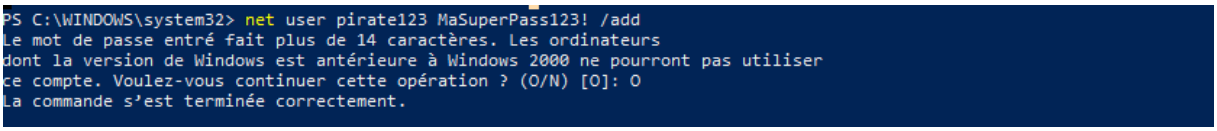
Simuler un pirate qui crée un compte utilisateur local avec les droits administrateurs. C'est une attaque classique utilisée pour maintenir un accès sur la machine.

a. Étapes sur le client Windows

Ouvrir **PowerShell en administrateur** et exécute les commandes suivantes :

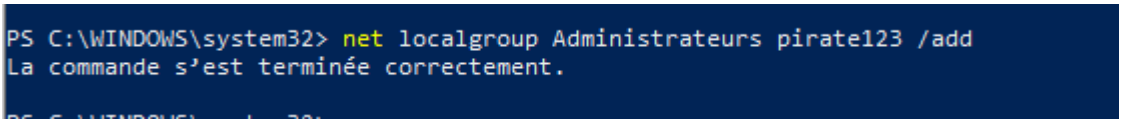
- **Créer un utilisateur :**

net user pirate123 MaSuperPass123! /add



- **Ajouter l'utilisateur au groupe des administrateurs :**

net localgroup Administrateurs pirate123 /add

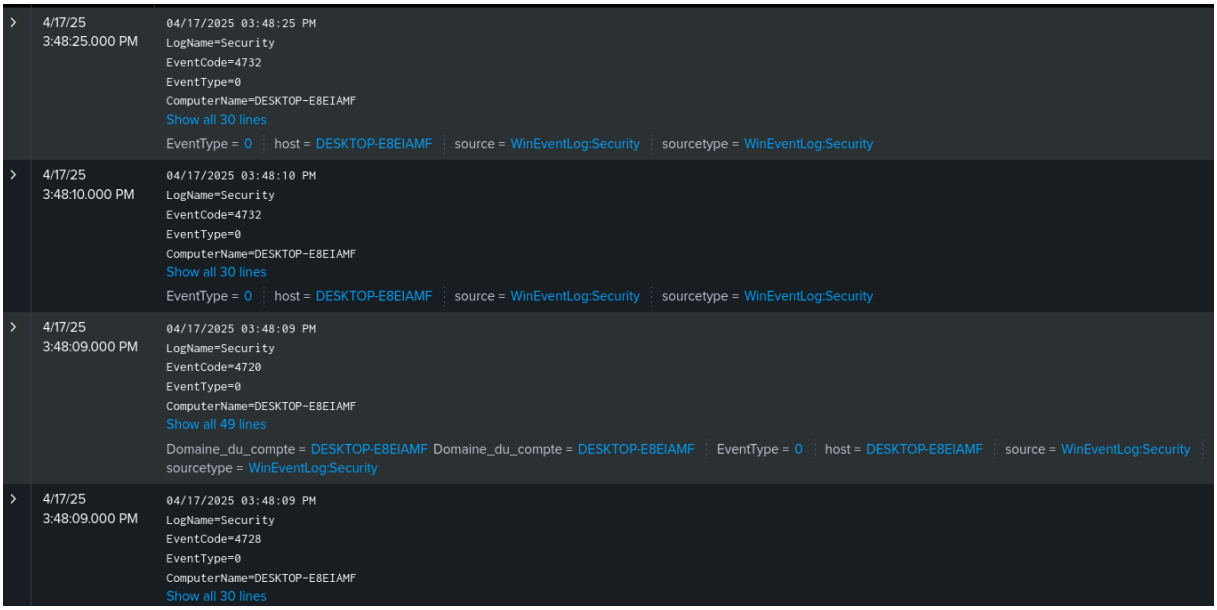


On vient de simuler une compromission où un attaquant a pris le contrôle et ajouté un utilisateur persistant avec les droits admin.

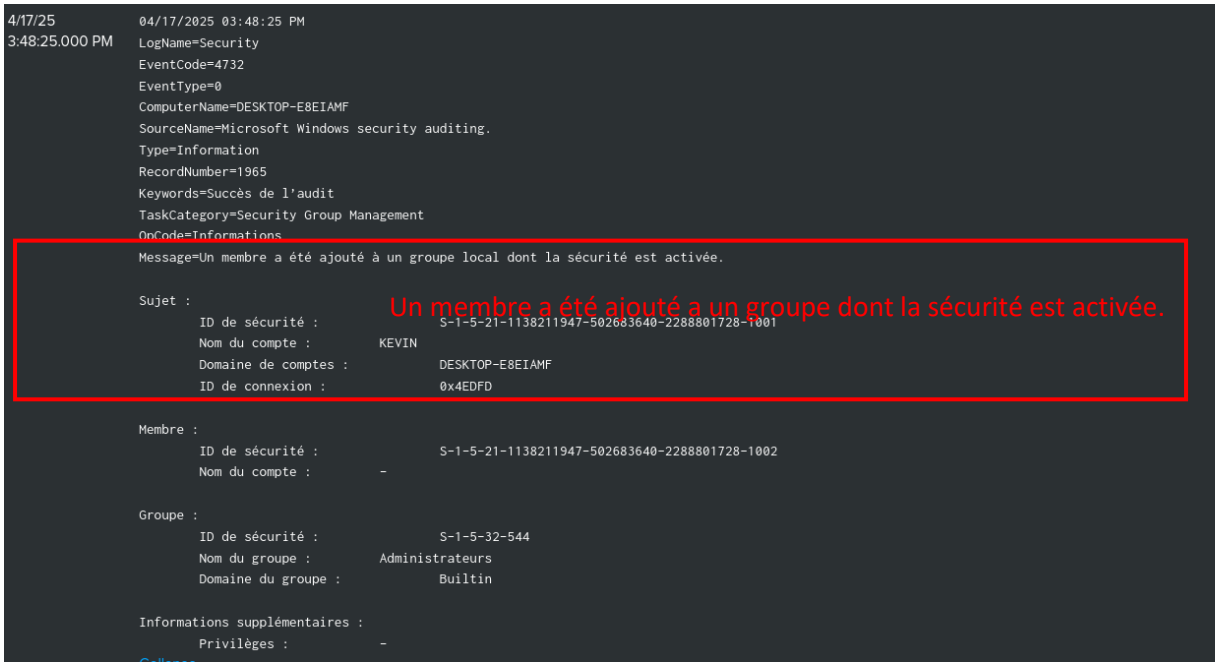
b. Résultat à l'issue de la requete sur le serveur Splunk

Requête Splunk pour les comptes utilisateurs :

index=* EventCode=4720 OR EventCode=4728 OR EventCode=4732



En cliquant sur show all 30 lines, on obtient cette capture



U. Annexe à la PSSI - Charte d'Utilisation des Systèmes d'Information du Groupe Solaris

Préambule :

Les systèmes d'information (SI) sont un patrimoine essentiel au développement et à la pérennité du Groupe Solaris. Cette charte définit les règles que chaque collaborateur, prestataire ou partenaire (**l'Utilisateur**) doit respecter pour garantir la sécurité, la confidentialité et l'intégrité de ce patrimoine commun. Son objectif est de protéger à la fois les intérêts de l'entreprise et ceux de ses collaborateurs.

En accédant aux ressources informatiques du Groupe Solaris (poste de travail, messagerie, réseau, applications), l'Utilisateur accepte sans réserve les stipulations de la présente charte.

Article 1 : Règles Générales de Comportement

1.1. **Identification et Authentification :**

- L'Utilisateur se voit attribuer un identifiant et un mot de passe personnels et strictement confidentiels.
- Il est interdit de divulguer ses codes d'accès, de les inscrire sur un support accessible à autrui ou d'utiliser ceux d'un collègue.
- Le mot de passe doit être robuste (> 12 caractères, mélange de lettres, chiffres, caractères spéciaux) et être changé tous les 3 mois.
- L'authentification multi-facteur (MFA) doit être activée et utilisée dès qu'elle est requise.

1.2. **Utilisation du Matériel :**

- Le matériel informatique (PC, écran, téléphone) est confié à l'Utilisateur pour un usage professionnel. Un usage personnel raisonnable et ponctuel est toléré s'il n'affecte pas la sécurité, les performances ou n'entraîne pas de coûts supplémentaires pour l'entreprise.
- L'Utilisateur est responsable du matériel qui lui est confié et doit signaler immédiatement toute perte, vol ou dégradation au service informatique.

1.3. **Protection des Données :**

- L'Utilisateur traite les informations de l'entreprise avec la plus grande confidentialité, pendant et après son contrat.
- Les données sensibles (données clients, personnelles, financières, stratégiques) **doivent impérativement** être stockées sur les espaces de stockage sécurisés désignés (**OneDrive Entreprise, SharePoint**). Le stockage sur le poste de travail local ou sur des supports amovibles personnels (clés USB) est interdit pour ce type de données.
- Le chiffrement (BitLocker) est activé sur tous les postes portables. Il est de la responsabilité de l'Utilisateur de verrouiller sa session (Windows + L) dès qu'il s'éloigne de son poste.

Article 2 : Règles d'Utilisation d'Internet et de la Messagerie

2.1. **Accès Internet :**

- L'accès Internet est destiné en priorité à l'activité professionnelle. L'entreprise se réserve le droit de contrôler et de filtrer l'accès à certains sites (réseaux sociaux, streaming, jeux, etc.) jugés non pertinents ou à risque.
- Il est strictement interdit de consulter, stocker ou diffuser des contenus illicites, diffamatoires, racistes, pornographiques ou contraires à l'éthique de l'entreprise.

2.2. **Messagerie Électronique :**

- La messagerie est un outil professionnel. Son utilisation à des fins personnelles doit rester exceptionnelle.
- L'Utilisateur doit exercer une vigilance extrême face aux emails suspects (phishing) : expéditeur inconnu, orthographe douteuse, pièce jointe ou lien inattendu. **Ne jamais ouvrir une pièce jointe ou cliquer sur un lien suspect.** Signaler immédiatement tout email douteux au service informatique.
- L'Utilisateur ne doit pas diffuser de messages à caractère commercial, publicitaire ou politique sans autorisation.

Article 3 : Règles Interdites et Sanctions

3.1. **Interdictions Absolues :**

- Installer, sans autorisation préalable du service informatique, tout logiciel, application ou plugin sur son poste de travail.
- Tenter de contourner les mesures de sécurité (pare-feu, proxy, politiques de groupe).
- Se connecter à des réseaux Wi-Fi publics non sécurisés pour accéder aux ressources internes de l'entreprise sans utiliser le VPN sécurisé (**Cisco AnyConnect**).
- Utiliser des services de cloud personnels (Dropbox, Google Drive, WeTransfer) pour transférer ou stocker des données professionnelles.
- Interconnecter des équipements personnels (smartphone, ordinateur personnel) au réseau de l'entreprise sans autorisation.

3.2. **Sanctions :**

- Le non-respect des règles énoncées dans cette charte expose son auteur à des sanctions disciplinaires, pouvant aller jusqu'au licenciement pour faute grave, sans exclure d'éventuelles poursuites pénales si les faits le justifient.

Article 4 : Engagements de l'Entreprise

- L'entreprise s'engage à mettre à disposition des Utilisateurs les outils nécessaires à leur travail dans le respect des règles de sécurité.

- L'entreprise s'engage à respecter la vie privée des Utilisateurs dans le cadre des contrôles nécessaires à la sécurité du SI, effectués dans le respect de la réglementation (RGPD, Code du Travail).

Article 5 : Acceptation de la Charte

Je, soussigné(e),

Nom : _____
Prénom : _____
Fonction : _____
Service : _____

Déclare avoir pris connaissance de l'ensemble des règles de la présente charte, les comprendre et m'engage à les respecter intégralement.

Fait à _____**, le //**

Signature :

V. Déploiement et Recette technique de migration

SQL Server 2022

Installation de SQL Server 2022 sous Ubuntu

```
Bash

sudo apt-get install mssql-server-extensibility libssl-dev
```

Acceptez le contrat de licence

```
Bash

sudo /opt/mssql/bin/mssql-conf set EULA accepteulaml Y
```

```
Bash

sudo systemctl restart mssql-server
```

Installation du runtime R et des paquets nécessaire

```
install.packages("iterators", lib="/usr/lib/R/library")
install.packages("foreach", lib="/usr/lib/R/library")
install.packages("R6", lib="/usr/lib/R/library")
install.packages("jsonlite", lib="/usr/lib/R/library")
```

```
install.packages("https://aka.ms/sqlml/r4.2/linux/CompatibilityAPI_1.1.0_R_x86_64-pc-
install.packages("https://aka.ms/sqlml/r4.2/linux/RevoScaleR_10.0.1_R_x86_64-pc-linux
```

Configurer le runtime R avec SQL Server

```
sudo /opt/mssql/bin/mssql-conf set extensibility rbinpath /usr/lib/R/bin/R
sudo /opt/mssql/bin/mssql-conf set extensibility datadirectories /usr/lib/R
```

Configurer la prise en charge de Python

```
sudo pip install dill numpy==1.22.0 pandas patsy python-dateutil
sudo pip install https://aka.ms/sqlml/python3.10/linux/revoscalepy-10.0.1-py3-none-an
```

Configurer le runtime Python avec SQL Server

```
sudo /opt/mssql/bin/mssql-conf set extensibility pythonbinpath /usr/bin/python3.10
sudo /opt/mssql/bin/mssql-conf set extensibility datadirectories /usr/lib:/usr/lib/pyt
```

```
systemctl restart mssql-launchpadd.service
```

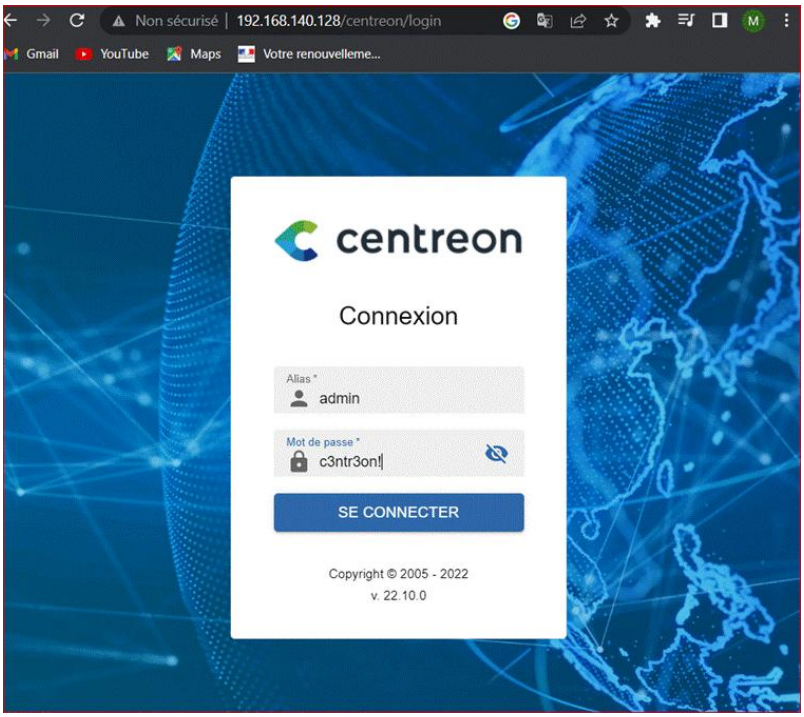
Validation post-migration

```sql
-- 🔹 5. Mise à jour des statistiques
USE [MaBase];
EXEC sp_updatestats;

-- 🔹 6. Liste des jobs à vérifier
SELECT name, enabled FROM msdb.dbo.sysjobs;

-- 🔹 7. Vérification des connexions post-migration
SELECT
    session_id,
    login_name,
    program_name,
    host_name,
    status
FROM sys.dm_exec_sessions
WHERE database_id = DB_ID('MaBase');
```

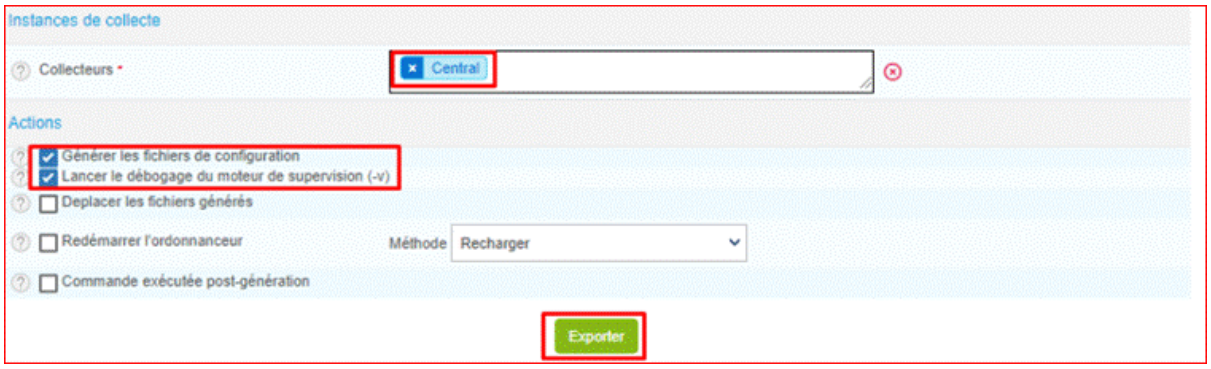
```sql
-- 🔹 1. Sauvegarde de la base (à exécuter sur SQL Server 2012)
BACKUP DATABASE [MaBase]
TO DISK = 'D:\Backup\MABASE_FULL.bak'
WITH INIT, COMPRESSION, STATS = 10;

-- 🔹 2. Script de restauration (sur SQL Server 2022)
RESTORE DATABASE [MaBase]
FROM DISK = 'D:\Backup\MABASE_FULL.bak'
WITH MOVE 'MaBase_Data' TO 'D:\SQLData\MaBase.mdf',
     MOVE 'MaBase_Log' TO 'D:\SQLLogs\MaBase.ldf',
     REPLACE, STATS = 10;

-- 🔹 3. Mise à jour du niveau de compatibilité
ALTER DATABASE [MaBase] SET COMPATIBILITY_LEVEL = 160;

-- 🔹 4. Vérification de l'intégrité
DBCC CHECKDB([MaBase]);
```

W. Déploiement Centreon

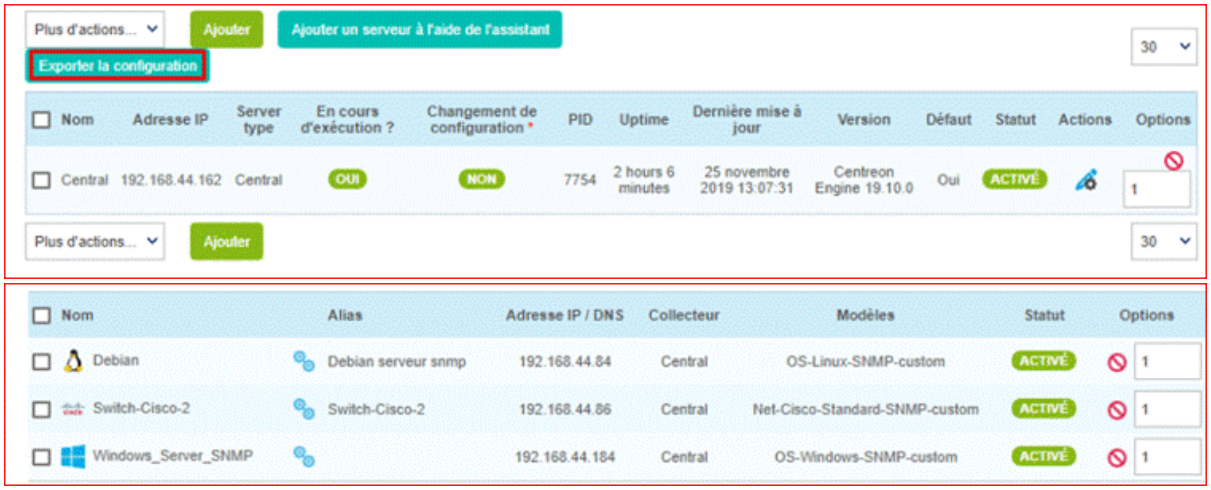
Installation de superviseur Centreon



Configuration des collectes de données



Remonte des machines clients



Collecté des tests d'intrusion