DOSSIER
SUPPORT PEDAGOGIQUE

NOA

2026

- Noa Ollier Housni Alaoui
- Site Web : noa-ollier.fr

- Promotion : 24-26
- N°Candidat : 2541481984
- Epreuve E5 - Support et la mise à disposition de services informatiques BTS SIO (services informatiques aux organisations) - Option SISR (Solutions d’infrastructure, Systèmes et Réseaux)

SOMMAIRE

TABLEAU DES COMPÉTENCES

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

Tableau de synthèse des réalisations professionnelles

NOM et prénom : OLLIER HOUSNI ALAOUI Noa	**N° candidat : 254148984**
Centre de formation :	**Option : ☒ SISR ☐ SLAM**
Lien Portefeuille de compétences : https://noa-ollier.fr/	

Compétences mises en œuvre / *Réalisations professionnelles (intitulé et liste des documents et productions associés)*	*Période (sous la forme du JJ/MM/AA au JJ/MM/AA)*	Gérer le patrimoine informatique	Répondre aux incidents et aux demandes d'assistance et d'évolution	Développer la présence en ligne de l'organisation	Travailler en mode projet	Mettre à disposition des utilisateurs un service informatique	Organiser son développement professionnel
		• Recenser et organiser ses ressources numériques • Exploiter des référentiels, normes et standards adoptés par le prestataire informatique • Mettre en place et vérifier les niveaux d'habilitation associés à un service • Vérifier les conditions de la continuité d'un service informatique • Gérer des sauvegardes • Vérifier le respect des règles d'utilisation des ressources numériques	• Collecter, suivre et orienter des demandes • Traiter des demandes concernant les services réseau et systèmes, applicatifs • Traiter des demandes concernant les applications	• Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques • Référencer les services en ligne de l'organisation et mesurer leur visibilité • Participer à l'évolution d'un site Web exploitant les données de l'organisation	• Analyser les objectifs et les modalités d'organisation d'un projet • Planifier les activités • Évaluer les indicateurs de suivi d'un projet et analyser les écarts	• Réaliser les tests d'intégration et d'acceptation d'un service • Déployer un service • Accompagner les utilisateurs dans la mise en place d'un service	• Mettre en place son environnement d'apprentissage personnel • Mettre en œuvre des outils et stratégies de veille informationnelle • Gérer son identité professionnelle • Développer son projet professionnel
Réalisation en cours de formation							
Réalisations en milieu professionnel en cours de première année							
Conformité Intune	**02/09/24 au 28/02/25**	☒	☒			☒	
Préparation de Poste	**03/03/25 au 30/04/25**	☒			☒	☒	
Authentification multifacteur (MFA)	**05/05/25 au 30/05/25**	☒				☒	☒
Réalisations en milieu professionnel en cours de seconde année							
Déploiement et Sécurisation (GPO)	**01/09/25 au 30/09/25**	☒	☒			☒	
Audit et Cartographie Réseau	**06/10/25 au 19/12/25**	☒			☒		
GPO Connexion ERP	**05/01/26 au 30/01/26**		☒			☒	
Supervision Icinga	**02/02/26 au 27/03/26**		☒	☒	☒	☒	

REMERCIEMENTS

Je tiens tout d'abord à exprimer ma profonde gratitude à mon tuteur, pour sa confiance, sa disponibilité et la liberté qu'il m'a accordée sur des projets structurants. Son expertise m'a permis de transformer mes connaissances théoriques en compétences professionnelles solides.

Mes remerciements s'adressent également à l'ensemble de l'équipe DSI du groupe OLGA. Travailler à vos côtés a été une chance immense : vous m'avez permis de découvrir la réalité et la complémentarité des métiers de l'informatique. Grâce à votre pédagogie, j'ai pu monter en compétences sur des domaines variés :

- **L'administration Workplace et Office 365 :** pour la gestion moderne du parc et des environnements collaborateurs.
- **L'administration Système et Réseau :** pour le maintien en condition opérationnelle de l'infrastructure et de la supervision via Icinga.
- **La Cybersécurité :** pour l'apprentissage des bonnes pratiques de sécurisation des accès et des flux de données.

Cette immersion totale au sein d'une équipe passionnée a été le moteur de ma réussite durant ces deux années.

INTRODUCTION

Ce dossier retrace mes deux années d'alternance au sein de la Direction des Systèmes d'Information du groupe **OLGA**. En tant qu'apprenti **Administrateur Système et Réseau**, j'ai été intégré au cœur d'un environnement industriel où l'informatique est un outil critique pour la production et la logistique.

Ma mission principale a été d'assurer le maintien en condition opérationnelle (MCO) de l'infrastructure tout en participant activement à sa modernisation. Durant cette période, j'ai dû faire preuve de polyvalence pour répondre aux enjeux de disponibilité du réseau, de gestion du parc informatique et de sécurisation des accès.

L'objectif de ce mémoire est de démontrer ma capacité à analyser des problématiques techniques et à déployer des solutions adaptées aux besoins des métiers d'OLGA. Au-delà de l'aspect technique, cette expérience m'a permis de comprendre l'importance d'un Système d'Information fiable et réactif pour accompagner la croissance d'un grand groupe.

CURRICULUM VITAE

Noa
Ollier Housni Alaoui

Contact

06.08.52.67.18

ollier.noaa@gmail.com

Boistrudan, France

Permis B

Langues

Anglais

Français

Compétences

Systèmes & Cloud

- Windows (Client/Serveur), Intune, Office 365, macOS, Linux

Infra & Supervision

- VMware vSphere, Switching, Wi-Fi (Airwave), Icinga, Centreon

Développement & Data

- HTML5, CSS3, JavaScript, Python, PowerShell, SQL +Vibe Coding (Cursor)

Centre d'intérêt

- Peche
- Voyage

EXPÉRIENCES PROFESSIONNELLES

BTS: Alternance chez OLGA en DSI en tant que Technicien Informatique.

Terminal pro: Stage d'un mois chez Yumens MV Group en DSI (Résolution des problèmes des intervenants, création de compte, installation de postes, migration de domaines).

Terminal pro: Stage d'un mois chez Olga en DSI (Installation de postes, résolution de problèmes de conformité de chaques utilisateurs via intune, résolution des problèmes des intervenants)

1nd pro: Stage de 5 semaines chez Ouest Consulting, mise en place du monitoring des équipements réseaux pour le client EAG (Club de foot En avant de Guingamp) sur l'outil Centréon.

1nd pro: Stage de 3 semaines chez Yumens MV Group en DSI (Résolution des problèmes des intervenants, création de compte, installation de postes, migration de domaines).

2nd pro: Stage de deux fois trois semaines chez Yumens, Projet d'automatisation de VM à partir d'un template sur un serveur vsphere en powershell, powercli.

3éme: stage d'une semaine chez Gosselin, création d'un blog de pêche en html css (Agence de développement et intégration web) à Vern-sur-seiche

4éme: stage d'observation pendant 3 jours chez Yes we dev (Agence de développement et intégration web)

FORMATIONS

BTS SIO (en cours) Services Informatiques aux Organisations (En Alternance Chez Olga)

Terminal RISC Réseaux informatiques et système communicants dans les domaines des télécommunications et réseaux.

Première RISC Réseaux informatiques et système communicants dans les domaines des télécommunications et réseaux.

Seconde MTNE (Métiers de la Transition Numérique et Énergétique) Lycée Coëtlogon (Rennes) Assemblage PC, Installation et maintenance d'OS, Mise en réseau, Virtualisation, Habilitation électrique, Lois générales de l'électricité.

DIPLOME

Brevet Mention bien

Bac Mention bien

PRÉSENTATION

Présentation de l'entreprise Olga

Olga, anciennement connue sous le nom de **Triballat Noyal**, est une entreprise familiale française indépendante fondée en 1951 à Noyal-sur-Vilaine, en Bretagne.

Acteur majeur de l'**agroalimentaire**, l'entreprise se distingue par sa spécialisation dans les produits laitiers, les solutions végétales et les céréales bio. Elle est aujourd'hui portée par des marques emblématiques telles que **Sojasun**, **Vrai**, **Sojade**, ou encore **Grillon d'Or**.

Pionnière de l'agriculture biologique depuis **1975**, Olga place le respect de l'environnement et la santé humaine au cœur de sa stratégie. En **2022**, l'entreprise a officialisée son nouveau nom, Olga, en hommage à sa cofondatrice, marquant ainsi une nouvelle étape dans son engagement pour la **transition écologique et sociétale**.

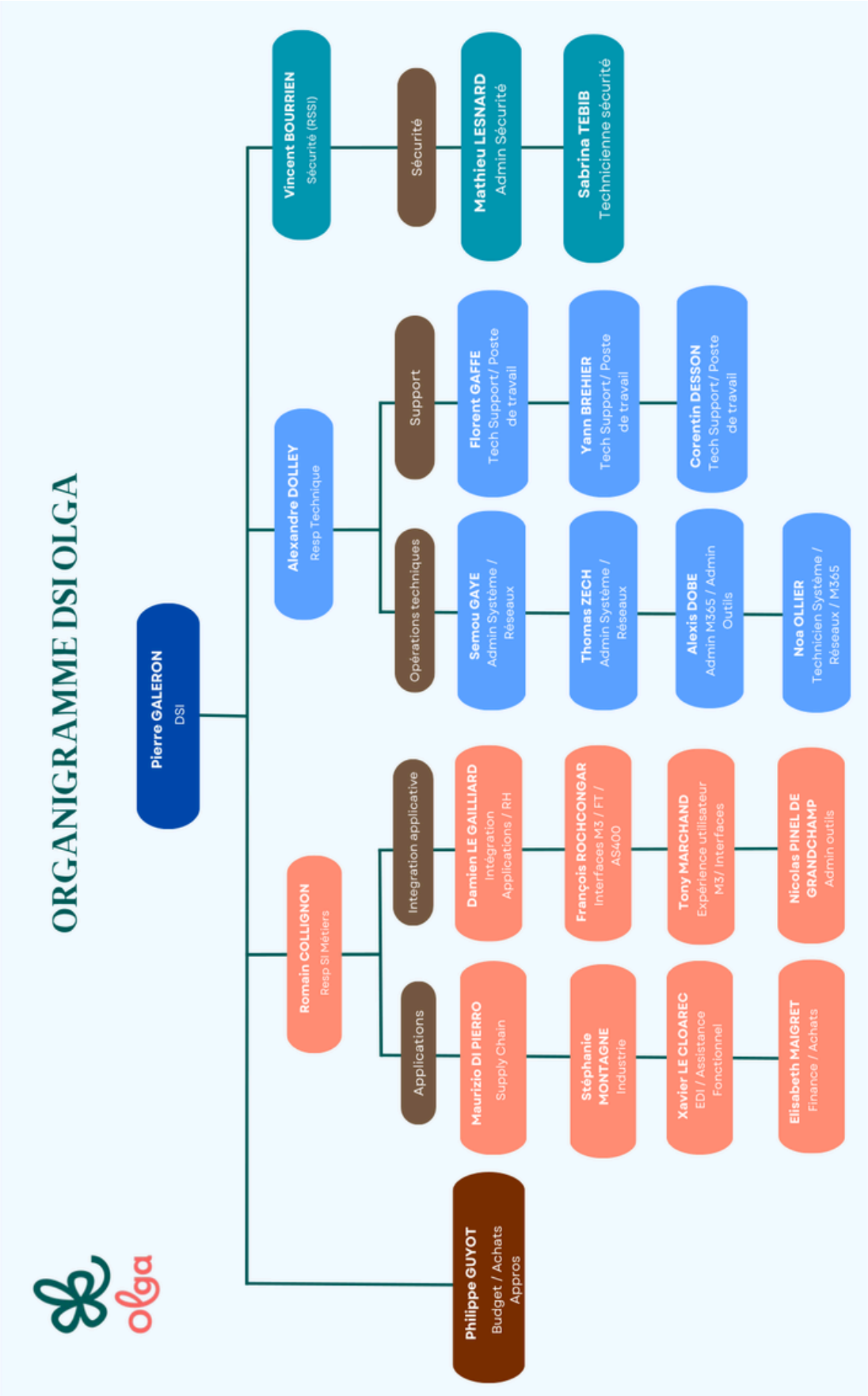
Quelques chiffres clés :

1 350 Collaborateurs

18 Sites de Production

335 millions d'euros de chiffre d'affaire

Organigramme de la DSI



Présentation de la direction des systèmes d'informations

L'organisation informatique de l'entreprise Olga est structurée pour répondre aux enjeux de transformation numérique et garantir la continuité de service sur l'ensemble des sites. La DSI, pilotée par **Pierre GALERON**, se décompose en quatre pôles complémentaires :

1. **Mon positionnement au sein de la structure**

En tant qu'apprenti technicien réseaux et systèmes, je suis rattaché au **Pôle Technique**, sous la responsabilité d'**Alexandre DOLLEY**.

Mon rôle s'articule entre le **Support**, pour garantir l'assistance aux utilisateurs, et les **Opérations Techniques**, pour participer au maintien en condition opérationnelle (MCO) de l'infrastructure. Cette position centrale me permet d'intervenir sur la gestion du parc informatique, la sécurité des accès et le déploiement de nouvelles solutions (comme la mise en place du MFA évoquée dans ma veille technologique).

2. **Organisation des pôles d'expertise**

- **Pôle Technique**: Piloté par **Alexandre DOLLEY**, ce pôle assure la stabilité des infrastructures. Il se divise entre les **Opérations Techniques** (mon équipe, avec Semou GAYE et Thomas ZECH sur l'administration système, réseaux et M365) et le **Support** (assistance utilisateurs).

- **Pôle SI Métiers**: Sous la direction de **Romain COLLIGNON**, il gère la partie logicielle via les équipes Applications (support ERP M3) et **Intégration Applicative** (flux et interfaces).

- **Sécurité**: Une cellule dédiée à la cybersécurité, pilotée par **Vincent BOURRIEN** (RSSI), assure la protection des accès et des données.

- **Budget & Achats**: **Philippe GUYOT** gère les ressources financières et les approvisionnements matériels de la direction.

3. **Enjeux du fonctionnement en équipe**

Cette structure hiérarchique et fonctionnelle permet une gestion efficace des incidents et des projets. Mon intégration au sein de cette équipe me permet de comprendre les flux d'escalade : d'un besoin utilisateur identifié au support jusqu'à la mise en œuvre d'une solution technique complexe par les administrateurs systèmes et réseaux.

ACTIVITÉS EFFECTUÉES DURANT LES DEUX ANNÉES

ACTIVITÉ N° 1

Résolution des problèmes de conformité des postes sous Intune

Objectifs et Enjeux

L'objectif principal est de maintenir un niveau de sécurité maximal sur l'ensemble du parc informatique d'Olga. L'enjeu est de détecter les vulnérabilités en temps réel via le Cloud et d'intervenir rapidement pour que chaque appareil respecte la politique de conformité (**Compliance**) définie par la DSI.

1. Surveillance du parc via Microsoft Intune

Le pilotage de nos équipements s'effectue via **Microsoft Intune**, notre solution de **MDM** (Mobile Device Management). Tous les appareils de l'entreprise y sont centralisés et font l'objet d'un contrôle automatique quotidien.

Intune analyse plusieurs points critiques pour déclarer un PC "Conforme" :

- L'état du chiffrement des données (**BitLocker**).
- L'activation des sécurités matérielles (**Secure Boot** et puce **TPM 2.0**).
- La gestion des profils (Un utilisateur unique par poste).
- La présence d'un antivirus à jour et l'état d'activité du système.

Mon rôle est de surveiller quotidiennement le tableau de bord pour identifier les postes marqués comme "**Non-conformes**" et d'analyser les causes précises de ces échecs de sécurité.

Résolution des problèmes de conformité des postes sous Intune

2. Comprendre la conformité Intune et ses enjeux

Avant de détailler mes actions, il est essentiel de définir ce qu'est la conformité (Compliance) au sein de Microsoft Intune.

La conformité est un système de "check-list" automatique basée sur les règles de sécurité édictées par la DSI d'Olga. Son rôle est de s'assurer que chaque poste de travail répond à des critères stricts avant d'être autorisé à accéder aux ressources de l'entreprise (mails, serveurs, documents Cloud).

- Le principe : Un agent présent sur le PC communique en permanence avec le Cloud. Si un seul critère (BitLocker, Antivirus, Secure Boot) manque à l'appel, le PC est marqué comme "Non-conforme".

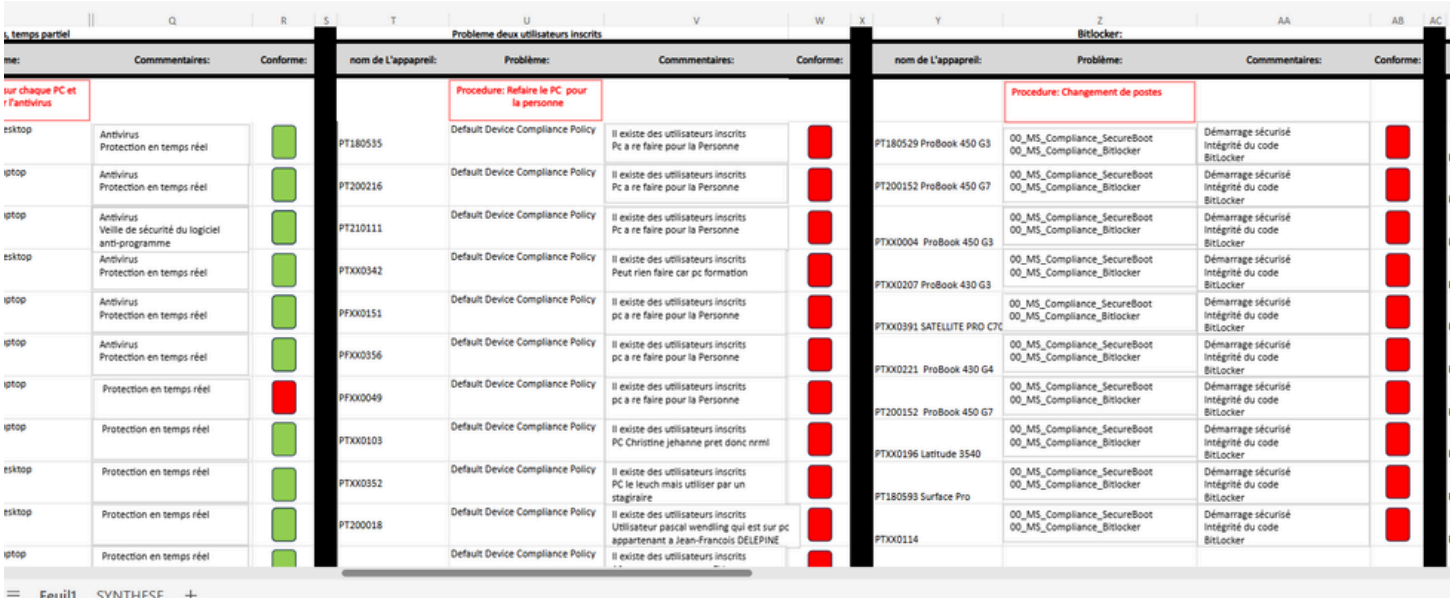
- L'enjeu :Un poste non-conforme génère immédiatement une alerte sur la console d'administration, ce qui nous permet d'identifier une faille de sécurité potentielle sur le parc.

Résolution des problèmes de conformité des postes sous Intune

3. Stratégie de Remise en Conformité des 240 Poste

À mon arrivée, j'ai été confronté à une situation critique : plus de 240 machines présentaient des défauts de conformité dans la console Intune. Pour traiter ce volume important sans perdre d'informations, j'ai mis en place une organisation rigoureuse :

- **L'inventaire d'audit (Excel)** : J'ai créé un tableau de bord répertoriant chaque PC en échec, son utilisateur, et le type de défaut constaté.
- **Classification par typologie** : J'ai regroupé les erreurs pour les traiter par catégories. Cela m'a permis de gagner en efficacité en appliquant des solutions groupées.
- **Suivi et relation utilisateur** : Ce travail a demandé plusieurs mois de suivi. Chaque ligne de mon Excel impliquait de contacter l'utilisateur, de diagnostiquer le poste à distance et de vérifier la remontée d'informations dans le Cloud.

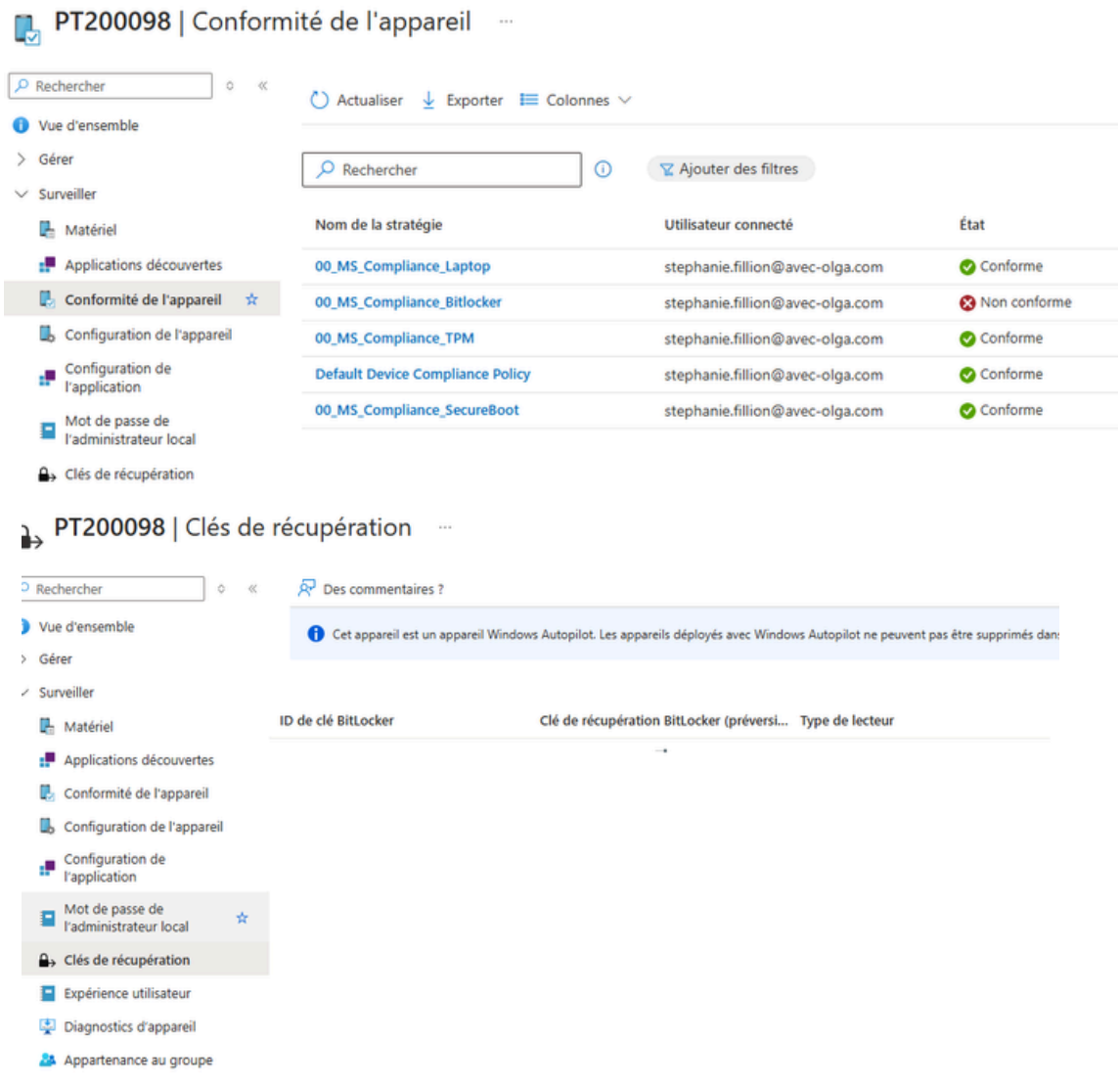


Résolution des problèmes de conformité des postes sous Intune

4. Analyse technique et résolution des non-conformités

J'ai identifié et traité trois problématiques majeures qui bloquaient la conformité des postes :

- **Le chiffrement BitLocker (Protection des données) :**
  - **Le problème** : Le disque dur n'était pas crypté, rendant les données lisibles en cas de vol du PC.
  - **Analyse et action** : J'ai diagnostiqué si l'échec était logiciel ou matériel. Si l'activation forcée via PowerShell échouait, cela révélait souvent un disque défaillant ou trop ancien, nécessitant une réinstallation complète.



ACTIVITÉ N° 1-4

Résolution des problèmes de conformité des postes sous Intune

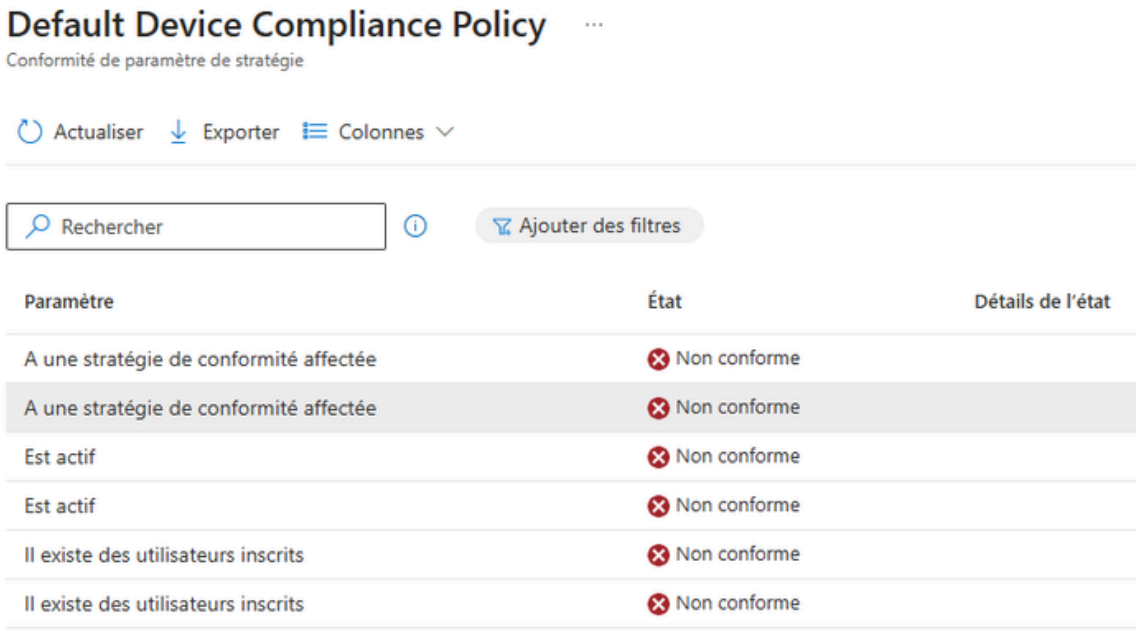
Conflits de sessions (Utilisateurs inscrits) :

- **Le problème** : Plusieurs sessions utilisateur sont détectées sur un même poste. La règle de la DSI est stricte : "Un PC est personnel et destiné à un seul utilisateur". Le partage de session crée des failles de sécurité et empêche Intune de savoir qui est le responsable de la machine.

- **Action** : J'ai contacté l'utilisateur principal pour comprendre pourquoi d'autres personnes se connectaient sur son poste.

- **Le constat** : Souvent, des collaborateurs s'échangeaient les PC entre eux sans passer par la DSI. Un nouvel arrivant se connectait simplement sur le PC d'un ancien collègue.

- **La solution** : J'ai rappelé la règle de sécurité aux utilisateurs. Pour corriger le problème, j'ai identifié le besoin de chaque personne. Si le PC devait changer de main, j'ai procédé à une **réinstallation complète (Wipe)** pour que la machine soit propre et officiellement attribuée au nouvel utilisateur. Cela permet de garantir que le PC est bien configuré pour la bonne personne dès le départ.



ACTIVITÉ N° 1-5

Résolution des problèmes de conformité des postes sous Intune

Postes inactifs (Délai de connexion dépassé) :

- **Le problème** : Le poste n'a pas communiqué avec le Cloud (Intune) depuis plus de 30 jours. Il passe automatiquement en "Non-conforme"
- **Lien Logique** : J'ai mené une enquête pour chaque cas : contact avec l'utilisateur ou le manager pour savoir si le PC est utilisé (congé maternité, arrêt long, ou oubli dans un placard). Cela permet de détecter les postes perdus ou volés et de les sortir de l'inventaire pour sécuriser la base de données.

ACTIVITÉ N° 1-6

Résolution des problèmes de conformité des postes sous Intune

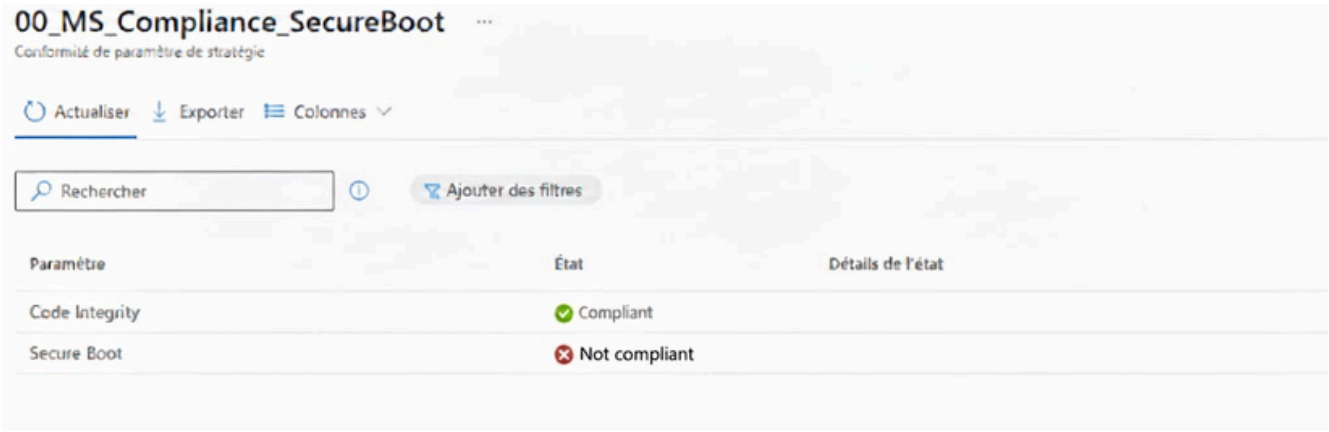
Absence de Secure Boot et TPM 2.0 (Limites matérielles) :

- **Le problème** : Le Secure Boot est une fonctionnalité de sécurité qui garantit que le PC ne démarre qu'avec des logiciels approuvés par le fabricant. Pour fonctionner, il nécessite souvent une puce de sécurité physique appelée TPM 2.0. Sur la console Intune, de nombreux postes (environ 40) remontaient en "Non-conforme" car ces options étaient désactivées ou absentes.

- **Action** : Après analyse, j'ai constaté que ce problème concernait principalement les anciens modèles (comme les HP G3). Ces machines utilisaient un BIOS configuré en mode "Legacy" (ancien mode) qui ne supporte pas les normes de sécurité actuelles.

- **Le constat critique** : Aucune manipulation logicielle ou configuration à distance via Intune ne pouvait corriger ce défaut. J'ai donc répertorié ces machines dans mon tableau Excel comme "Matériel obsolète".

- **Lien avec l'Activité 2** : Ce diagnostic a été l'élément déclencheur du renouvellement d'une partie du parc. Puisque ces 40 postes ne pouvaient plus être sécurisés selon les normes d'Olga, j'ai validé la nécessité de les remplacer par des machines neuves. **C'est ce processus de préparation et de déploiement via Autopilot que je détaille dans l'activité suivante.**



Résolution des problèmes de conformité des postes sous Intune

5. Conclusion de l'activité :

Cette mission d'audit sur **240 machines** m'a permis de découvrir concrètement la gestion moderne d'un parc informatique et ses enjeux de sécurité.

J'ai appris qu'administrer un parc nécessite une surveillance constante via le Cloud (Intune). Cette expérience m'a permis de maîtriser les standards de sécurité actuels : savoir interpréter un défaut de conformité, comme un **BitLocker** inactif ou un **Secure Boot** absent, est devenu essentiel pour protéger les données d'Olga.

Grâce à la rigueur de mon suivi Excel, j'ai pu isoler les limites de notre matériel. Ce projet a été le point de départ de ma réflexion stratégique : c'est ce diagnostic précis qui a justifié techniquement le remplacement des 40 postes obsolètes.

Enfin, j'ai acquis la rigueur nécessaire pour assurer la traçabilité dans EasyVista et la communication avec les utilisateurs. Ce travail d'audit a été la fondation indispensable pour lancer le projet de renouvellement via **Autopilot**, détaillé dans mon activité suivante.

ACTIVITÉ N° 2

Préparation de postes

Objectifs et Enjeux

Le but principal de cette mission était de garantir l'intégrité et la sécurité du parc informatique. L'enjeu était de répondre aux exigences de la DSI en assurant que 100% des postes de travail soient "Compliants" (conformes) vis-à-vis des politiques de sécurité modernes.

1. **Analyse et diagnostic du parc via Microsoft Intune**

Tout a commencé par une analyse sur **Microsoft Intune**, notre outil de gestion à distance (**MDM**). J'ai remarqué qu'environ 40 postes (**modèles HP G3**) étaient marqués en "Non-conforme".

En creusant, j'ai identifié que le point de blocage était le **Secure Boot** (le système qui vérifie que le PC ne démarre pas sur un logiciel malveillant). Techniquement, ces postes étaient configurés en mode **Legacy BIOS** (ancien mode de démarrage).

Pour activer la sécurité moderne, il aurait fallu :

- Passer en mode **UEFI** (nécessitant une conversion de disque).
- Posséder une puce **TPM 2.0** (un processeur de sécurité qui sert de coffre-fort matériel pour les clés de chiffrement).

Comme les modèles G3 n'avaient pas cette puce physique, j'ai dû organiser leur remplacement par des PC neufs pour garantir la sécurité de l'entreprise.

Préparation de postes

2. Préparation et enrôlement avec Windows Autopilot

Pour les nouveaux PC, j'utilise la procédure Autopilot. C'est un service Cloud qui permet de configurer un ordinateur automatiquement sans avoir besoin de créer une image système (ISO) sur une clé USB.

Sur le PC neuf, j'ouvre une console de commande (Shift + F10) et je lance PowerShell. Voici les commandes que j'exécute pour lier le PC à l'entreprise :

- Set-ExecutionPolicy Bypass : J'autorise l'ordinateur à lancer mes scripts
- Install-Script Get-WindowsAutopilotInfo : Je télécharge l'outil de liaison.
- Get-WindowsAutopilotInfo.ps1 -online -grouptag AutopilotPROD : Cette commande est cruciale. Elle extrait l'identifiant unique du PC (le Hardware ID) et l'envoie sur notre tenant Olga.

```
PS C:\Windows\System32> Get-WindowsAutopilotinfo.ps1 -online -grouptag autopilotProd
AVERTISSEMENT : Note: Sign in by Web Account Manager (WAM) is enabled by default on Windows. If usin
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.
NOTE: Sign in by Web Account Manager (WAM) is enabled by default on Windows systems and cannot be di
To disable WAM run Set-MgGraphOption -DisableLoginByWAM $true and then use a custom ClientId.

Connected to Intune tenant 4df56e47-4f77-4adb-ac33-7feb500a2573
Gathered details for device with serial number: 5CD943GFL2
Waiting for 1 of 1 to be imported
Waiting for 1 of 1 to be imported
Waiting for 1 of 1 to be imported
Waiting for 0 of 1 to be imported
5CD943GFL2: complete 0 None
1 devices imported successfully.  Elapsed time to complete import: 93 seconds
Waiting for 0 of 1 to be synced
All devices synced.  Elapsed time to complete sync: 1 seconds
PS C:\Windows\System32>
```

Préparation de postes

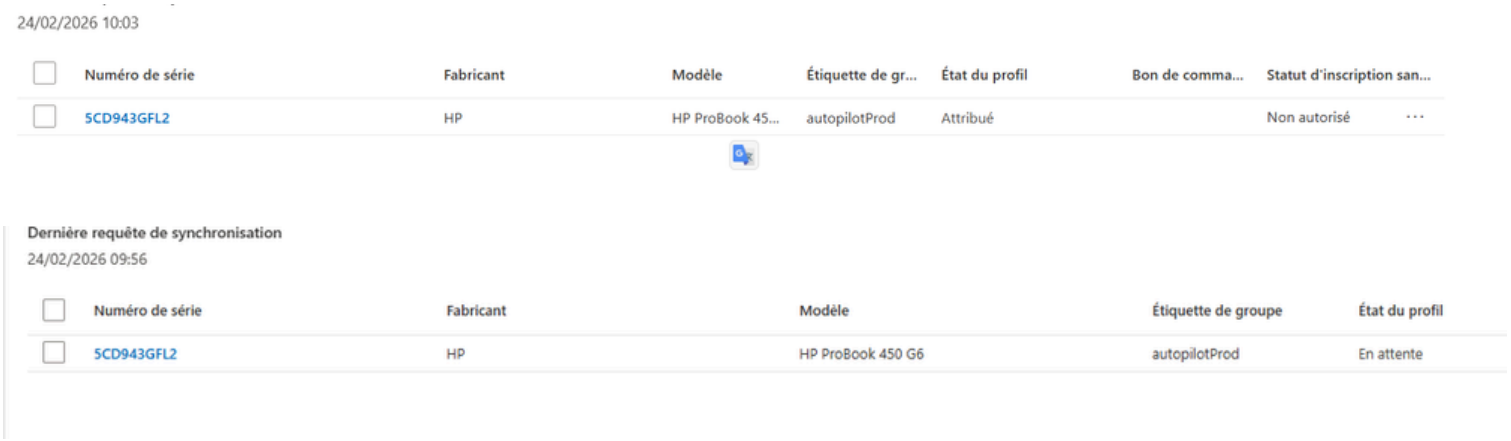
3. Vérification sur la console Intune (Côté Admin)

Avant de redémarrer le PC, je dois m'assurer que l'importation est réussie sur la console Microsoft Intune (section "Appareils Windows | Inscription Windows").

- Contrôle du Numéro de Série : Je vérifie que le numéro de série du PC apparaît bien dans la liste.

- État du profil de déploiement : Je regarde la colonne "Profil d'attribution".
  - Si c'est marqué "En attente" : Il faut patienter, le Cloud traite la demande.

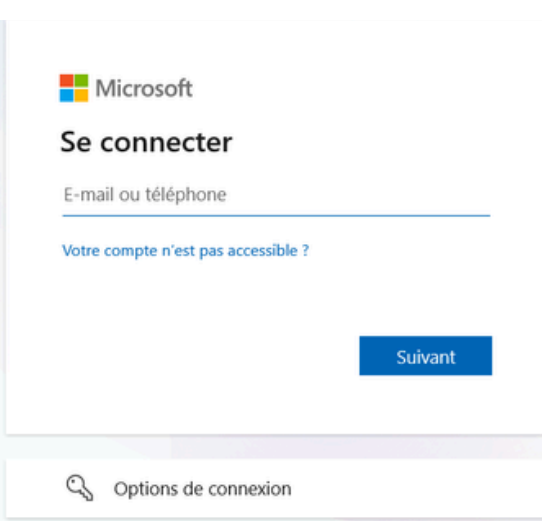
  - Si c'est marqué "Attribué" : Le PC a bien reçu son profil de configuration

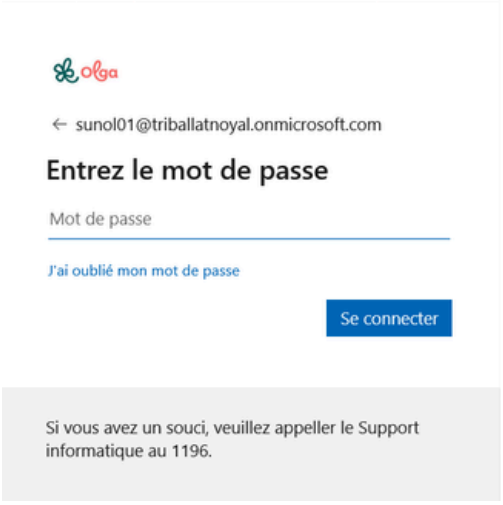


Préparation de postes

3. Authentification Administrateur et Redémarrage

À ce moment-là, une fenêtre Microsoft s'ouvre : je dois rentrer un compte admin du tenant pour prouver que c'est bien un technicien d'Olga qui autorise ce nouveau PC. Une fois fini, je tape shutdown /r /t 0 pour redémarrer.





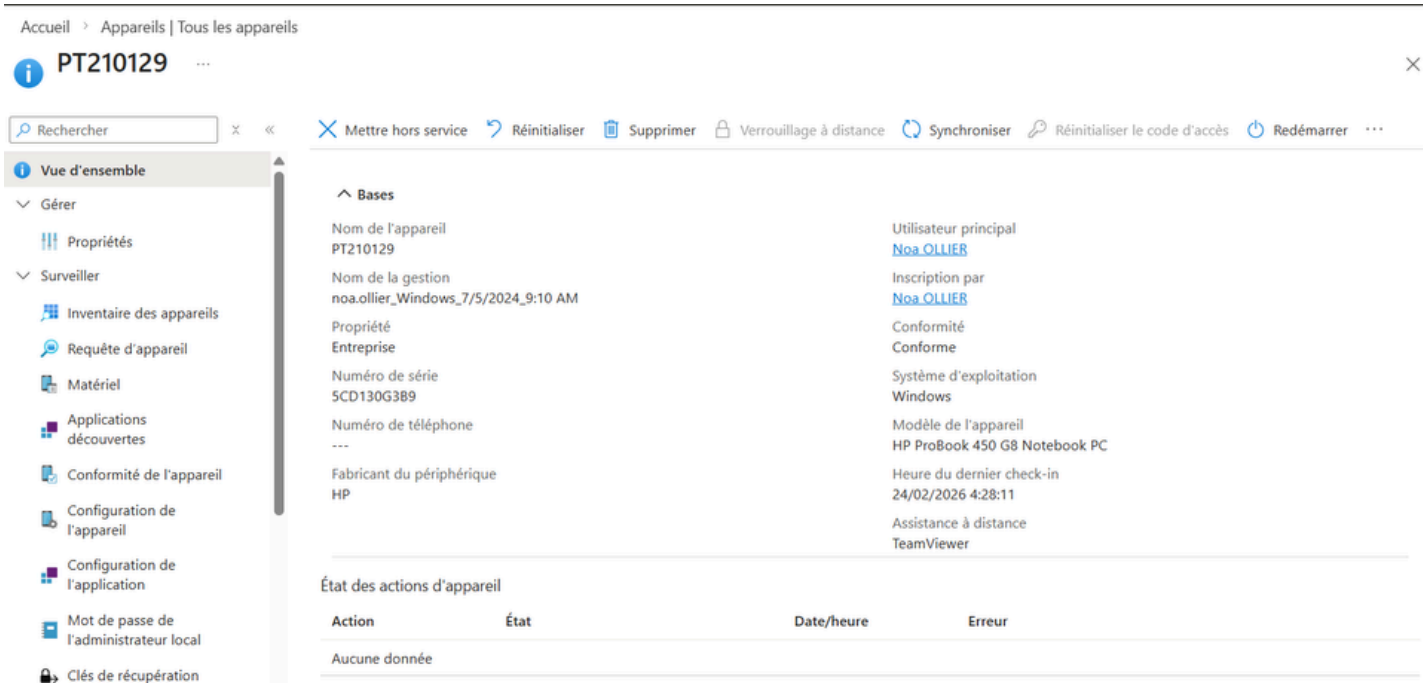
Préparation de postes

4. Phase finale : Configuration et Maintien en Condition Opérationnelle (MCO)

Une fois que l'utilisateur s'est connecté et que l'installation est finie, le PC apparaît désormais dans la liste principale des appareils de la console Intune.

À quoi sert cette gestion centralisée ?

- **Gestion des applications** : Intune "pousse" automatiquement les logiciels (Office 365, M3) sans intervention manuelle.
- **Stratégies de configuration** : On applique à distance les paramètres Wi-Fi, les certificats et les restrictions de sécurité.
- **Sécurité et Conformité** : On surveille en temps réel si le PC est à jour et si son chiffrement BitLocker est actif. En cas de vol, je peux même bloquer ou effacer le PC à distance. (Voir activité 2)

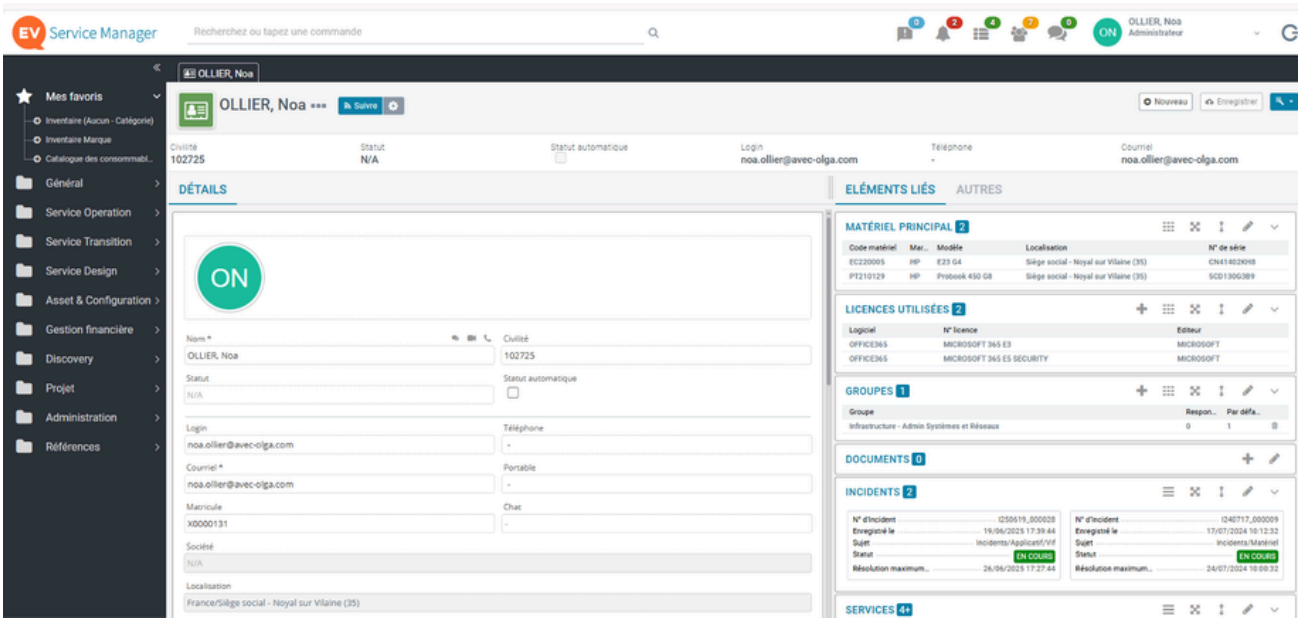


Préparation de postes

5. Mise à jour de l'inventaire dans EasyVista

Je termine par la gestion de l'inventaire dans notre outil **ITSM EasyVista**.

- Je déclare l'ancien poste HP G3 comme "Sorti du parc".
- Je rattache le nouveau PC et son écran à la fiche de l'utilisateur (ex: **Noa OLLIER**). Cela garantit une traçabilité parfaite pour le support technique



6. Conclusion de l'activité

Ce projet a été pour moi l'occasion de découvrir concrètement la gestion moderne d'un parc informatique.

J'ai appris qu'avec le couple **Autopilot et Intune**, on peut automatiser entièrement la configuration d'un PC (logiciels et sécurité) à distance, sans installation manuelle. J'ai aussi compris l'importance de la sécurité matérielle : savoir identifier un poste obsolète (sans puce **TPM** ou en **Legacy BIOS**) est devenu essentiel pour protéger les données.

Enfin, j'ai acquis la rigueur nécessaire pour assurer la traçabilité du matériel dans **EasyVista**, garantissant ainsi un inventaire toujours à jour et un meilleur support pour les utilisateurs.

ACTIVITÉ N° 3

Déploiyement automatisé et sécurisation logicielle (GPO)

Objectifs et Enjeux

L'objectif principal est d'éradiquer une vulnérabilité critique au sein du parc informatique d'Olga. L'enjeu est de garantir qu'aucun poste de travail ne reste exposé à des failles de sécurité connues (CVE), tout en assurant un déploiement totalement transparent (silencieux) pour les utilisateurs, sans interrompre leur travail.

1. Contexte : La faille de sécurité 7-Zip

Une faille de sécurité majeure a été détectée sur toutes les versions de 7-Zip inférieures à la 24.04. Cette vulnérabilité permet à un attaquant d'exécuter du code à distance ou d'élever ses privilèges sur la machine.

- Le constat : Après une première vague de mises à jour via SCCM, environ 40 postes (dont le poste témoin PT190012) sont restés en échec ou n'ont pas reçu la mise à jour.

- Ma mission : Concevoir une solution de secours "industrielle" via les services de domaine Active Directory pour forcer la mise à jour et désinstaller les versions obsolètes de manière définitive.

Déploiyement automatisé et sécurisation logicielle (GPO)

2. L'outil de déploiement : La GPO (Group Policy Object)

Pour diffuser mon correctif sur les 40 postes restants, j'ai utilisé les GPO de l'Active Directory. Il était nécessaire de comprendre cet outil avant de lancer l'automatisation.

- **Qu'est-ce qu'une GPO** ? C'est une "stratégie de groupe" gérée depuis le contrôleur de domaine. Elle permet d'appliquer des configurations ou d'exécuter des actions sur un ensemble de machines de manière centralisée.

- **Pourquoi ce choix** ? La GPO permet de lancer mon script au démarrage de l'ordinateur (Startup Script). L'avantage majeur est que le script s'exécute avec les droits "SYSTEM" : il possède les privilèges nécessaires pour désinstaller et installer des logiciels, même si l'utilisateur n'est pas administrateur de sa session.

- **Ciblage et organisation**: J'ai configuré la GPO pour qu'elle cible uniquement l'Unité d'Organisation (OU) contenant les postes de travail. Cela garantit que la règle ne s'applique qu'aux ordinateurs concernés par la faille de sécurité.

Déploiyement automatisé et sécurisation logicielle (GPO)

3. Approche Stratégique : Méthodologie et Scripting conditionnel

Une fois l'outil (la GPO) choisi, j'ai défini une méthodologie rigoureuse pour garantir que le déploiement soit "propre", automatisé et sans échec. Ma stratégie repose sur trois piliers :

- **Le stockage centralisé sur le SYSVOL** : J'ai déposé le script PowerShell et le fichier d'installation (.msi) dans le répertoire SYSVOL du contrôleur de domaine. C'est un dossier partagé sécurisé, répliqué sur tout le réseau, ce qui garantit que chaque PC peut y accéder au démarrage, même sans session utilisateur ouverte.

- **Le caractère "Silencieux" et transparent** : L'enjeu majeur était que l'utilisateur ne soit pas interrompu dans son travail. L'installation s'exécute en arrière-plan (mode silent) : aucune fenêtre n'apparaît à l'écran, et aucun redémarrage forcé n'est imposé à l'utilisateur.

- **L'intelligence du script (Installation conditionnelle)** : Au lieu de forcer l'installation de manière aveugle, j'ai conçu un script conditionnel.

    - **Analyse** : Le script analyse d'abord le poste. S'il détecte que la version 24.04 est déjà présente, il s'arrête immédiatement pour économiser les ressources réseau.

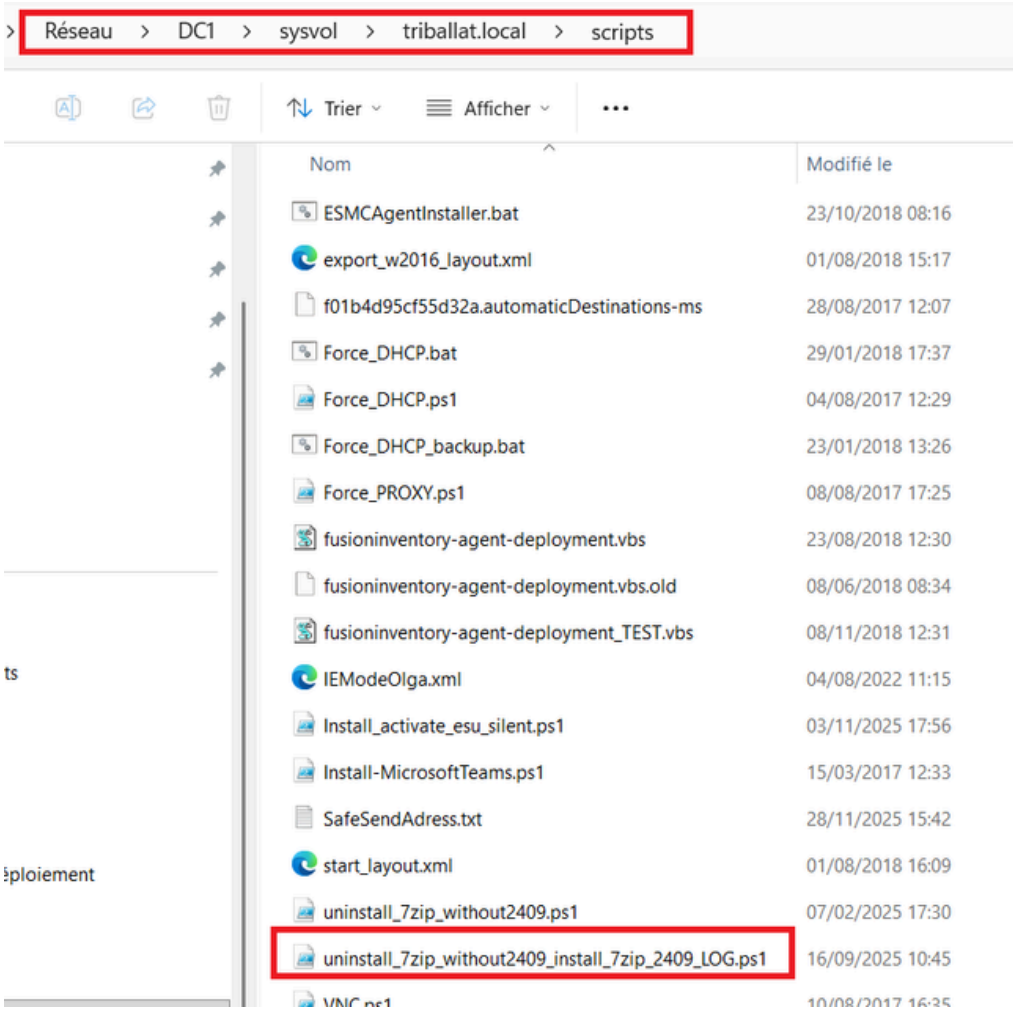
    - **Remédiation** : S'il détecte une version ancienne (comme la 16.04 sur le poste PT190012), il déclenche automatiquement le protocole de mise à jour.

ACTIVITÉ N° 3-3

Déploiement automatisé et sécurisation logicielle (GPO)

4. Mise en œuvre technique : Industrialisation du déploiement

Pour traiter efficacement les **40 postes** restants, j'ai mis en place une solution automatisée s'appuyant sur l'infrastructure Windows Server d'Olga. La première étape a consisté à préparer l'environnement de diffusion en utilisant le répertoire **SYSVOL** du contrôleur de domaine. J'y ai déposé le script PowerShell et l'installeur .msi, garantissant ainsi que les sources soient accessibles en permanence par tous les PC du parc, avec les droits nécessaires pour une exécution avant l'ouverture de session.

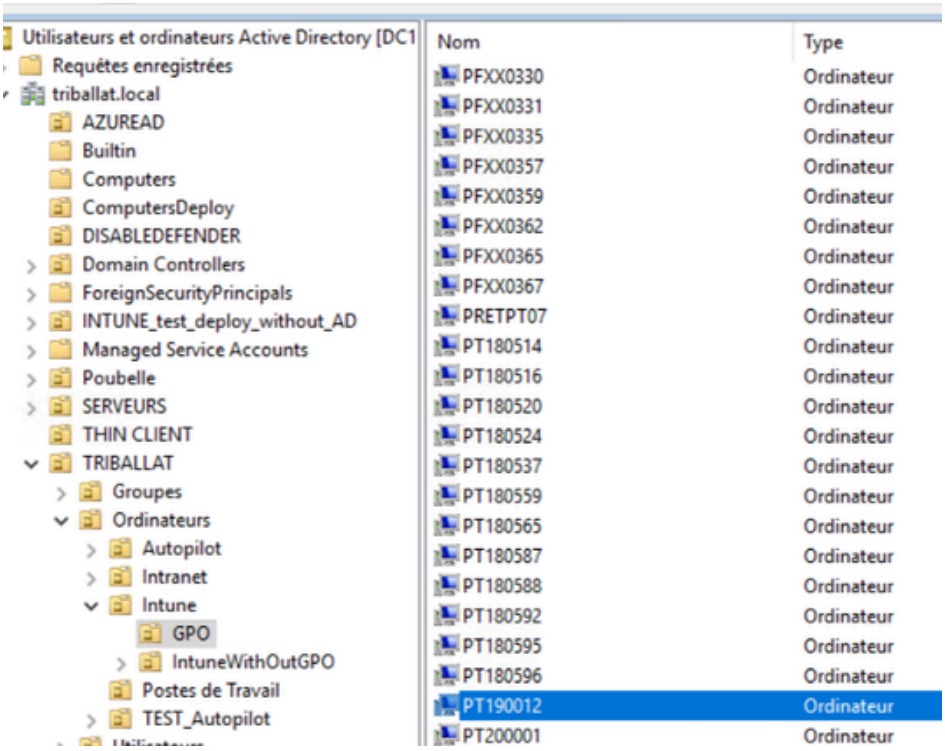


ACTIVITÉ N° 3-4

Déploiyement automatisé et sécurisation logicielle (GPO)

Le cœur de mon intervention a été la conception d'un script PowerShell "intelligent". Au lieu de forcer une installation systématique qui pourrait ralentir les postes déjà à jour, j'ai programmé une vérification conditionnelle. Le script analyse les clés de registre du système pour détecter la version exacte de 7-Zip. S'il identifie une version vulnérable (inférieure à 24.04), il récupère automatiquement son identifiant unique (GUID) pour déclencher une désinstallation propre avant de lancer la nouvelle installation.

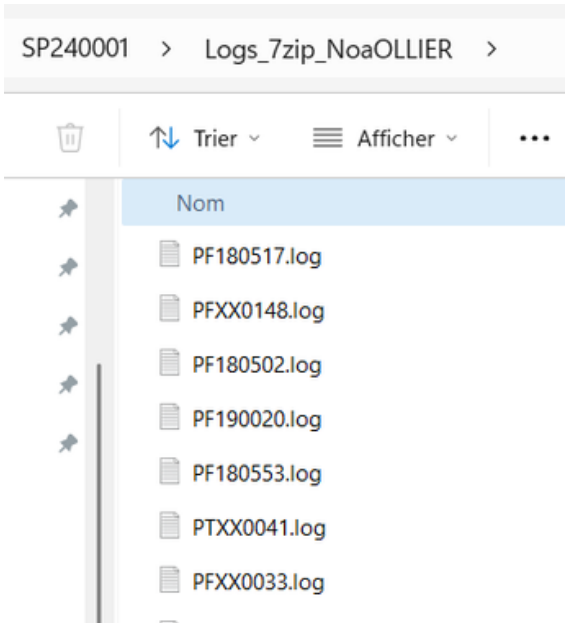
Pour déployer cette logique, j'ai créé et paramétré une GPO (Group Policy Object) nommée "DEPLOY_7ZIP_24.04" au sein de la console de Gestion des stratégies de groupe. En liant cette stratégie à l'Unité d'Organisation des postes de travail et en configurant le script en "Démarrage ordinateur", j'ai assuré une exécution avec les droits SYSTEM. Cela permet de contourner les restrictions des comptes utilisateurs standards et de garantir la réussite du déploiement en arrière-plan.



Déploiement automatisé et sécurisation logicielle (GPO)

5. Validation et Traçabilité centralisée (Le cas du poste PT190012)

Pour assurer un suivi rigoureux de l'opération, j'ai intégré une fonction de journalisation (logs) avancée dans mon script. Plutôt que de laisser un fichier isolé sur chaque machine, j'ai configuré le script pour qu'il écrive directement sur un partage réseau dédié : \\Serveur\Logs_7zip_NoaOLLIER.



- **Suivi en temps réel** : Chaque PC du parc possède les droits d'écriture sur ce dossier. Dès que le script s'exécute, il crée un fichier texte portant le **nom du PC** (ex: PT190012.txt). Cela me permet, depuis mon poste d'administrateur, de savoir instantanément quels postes sont à jour et lesquels présentent une erreur.

- J'ai validé le dispositif sur le poste témoin PT190012. Pour assurer un suivi rigoureux, mon script génère un fichier de log local. En consultant ce fichier, j'ai pu confirmer qu'à **14:59:57**, la version **16.04** a été détectée et désinstallée avec succès (Code 0), suivie immédiatement de l'installation de la version correcte.

```
06/19/2025 14:59:56 - Début du script GPO 7-Zip
06/19/2025 14:59:57 - Version installée détectée:  7-Zip [64] 16.04 : Copyright (c) 1999-2016 Igor Pavl
06/19/2025 14:59:57 - Version détectée dans le registre: 7-Zip 16.04 (x64 edition) - Version: 16.04.00.
06/19/2025 14:59:57 - Début désinstallation de la version 16.04.00.0
06/19/2025 14:59:59 - Désinstallation réussie via GUID (code 0)
06/19/2025 14:59:59 - Début copie depuis SYSVOL
06/19/2025 15:00:06 - Installation en cours...
06/19/2025 15:00:11 - Installation réussie (code 0)
06/19/2025 15:00:11 - Version installée confirmée:  7-Zip 24.09 (x64) : Copyright (c) 1999-2024 Igor Pa
06/19/2025 15:00:11 - Script terminé
```

Déploiyement automatisé et sécurisation logicielle (GPO)

- La vérification finale sur le poste a confirmé que la version **24.04** était bien active. Cette méthode a permis d'éradiquer la faille de sécurité CVE sur l'ensemble des postes ciblés. Ce travail garantit une traçabilité parfaite de l'intervention et remet le parc en conformité avec les exigences de sécurité de la DSI.

6. Conclusion de l'activité

Ce projet m'a permis de maîtriser l'automatisation logicielle et la gestion de parc via l'Active Directory. J'ai appris qu'un déploiement réussi repose sur une préparation minutieuse : savoir isoler une vulnérabilité, concevoir un script adaptable et, surtout, **centraliser les rapports d'exécution** pour garantir une traçabilité totale.

Grâce à cette méthode de logs centralisés, j'ai pu valider la sécurisation des 40 postes vulnérables sans aucune intervention physique. Cette expérience renforce ma capacité à gérer des déploiements massifs tout en garantissant la sécurité et la conformité du système d'information d'Olga.

ACTIVITÉ N° 4

Audit et Cartographie des infrastructures réseaux

Objectifs et Enjeux

L'objectif principal de cette mission est de remettre à jour et de moderniser les schémas d'architecture réseau des sites majeurs d'Olga. L'enjeu est de garantir à la DSI une visibilité parfaite sur les équipements critiques afin d'accélérer le diagnostic en cas de panne et d'assurer la continuité de service des lignes de production.

1. Contexte : Obsolescence de la documentation existante

Lors de mon arrivée, les schémas réseau des pôles de Châteaubourg (Sojasun, Nutrisun) et de Noyal-sur-Vilaine (La Rivière : Vrai, Bordier, Petit Billy) ne reflétaient plus la réalité du terrain. Suite à de nombreuses évolutions matérielles, la documentation était devenue incomplète et difficilement exploitable.

- Le constat : L'absence de plans à jour ralentissait les interventions techniques, car l'emplacement des antennes et les ports de raccordement n'étaient pas identifiés précisément.

- Ma mission : Réaliser un audit complet du parc (switchs, bornes Wi-Fi, interconnexions fibre) pour reconstruire des schémas dynamiques et précis sous Microsoft Visio.

ACTIVITÉ N° 4-1

Audit et Cartographie des infrastructures réseaux

2. Méthodologie : Audit et supervision du parc via AirWave et Guacamole

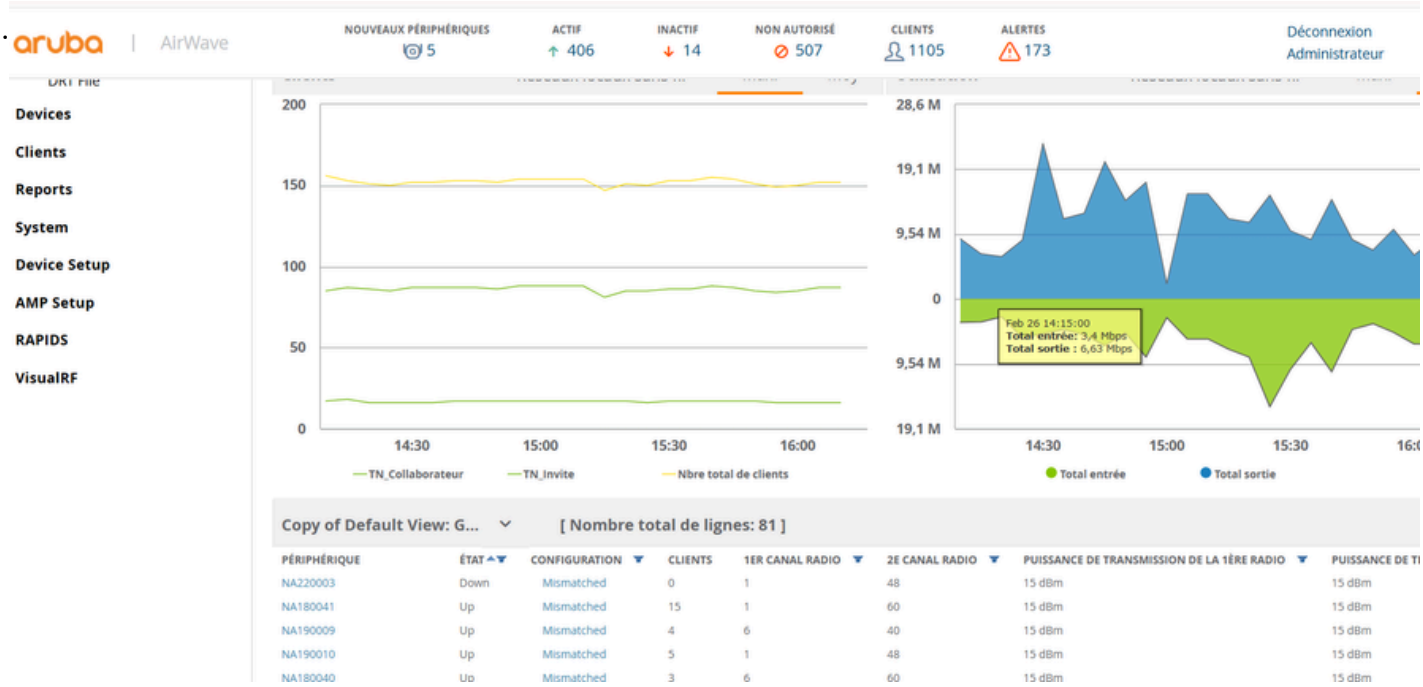
Pour reconstruire ces plans sans erreurs, j'ai mis en place une méthodologie d'audit basée sur l'extraction de données réelles provenant des outils d'administration de la DSI :

- **Aruba AirWave (La plateforme de management)** : C'est l'outil central chez Olga pour l'administration complète du réseau filaire et sans fil. Il remplit trois rôles majeurs :

- **Configuration centralisée** : AirWave permet de pousser des configurations ou des mises à jour sur des groupes entiers de switchs et d'antennes sans intervenir sur chaque appareil.

- **Supervision et Alerting** : Il surveille l'état de santé du réseau, analyse le trafic et alerte la DSI en temps réel en cas de panne d'un équipement sur un site de production.

- **Inventaire et Filtrage** : L'interface est organisée par sites (ex: Châteaubourg, Noyal). J'ai pu appliquer des filtres pour isoler les équipements souhaités et réaliser des **exports de données** précis. Ces listes m'ont fourni le nom, l'IP, le modèle et surtout le port de switch exact de chaque antenne pour mes schémas



ACTIVITÉ N° 4-2

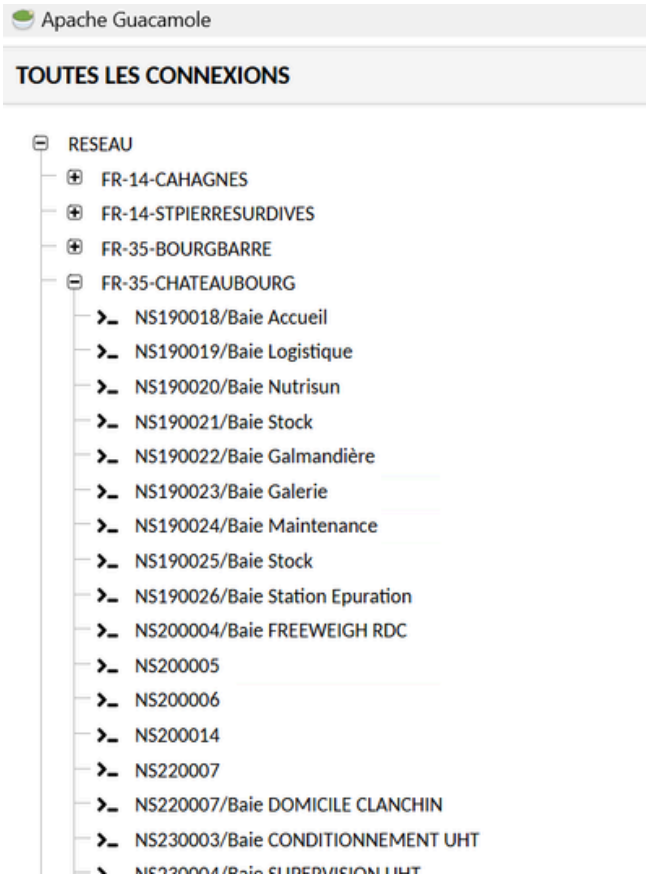
Audit et Cartographie des infrastructures réseaux

Apache Guacamole (L'accès distant sécurisé) : C'est un outil critique de la DSI pour l'administration à distance.

- **Sécurisation** : Guacamole sert de passerelle sécurisée pour accéder aux infrastructures sans exposition directe sur le réseau.
- **Accès SSH** : Il m'a permis d'ouvrir des sessions SSH sur les switchs directement depuis un navigateur web pour vérifier les interconnexions physiques sans me déplacer dans chaque baie.

Audit de terrain : En complément, je me suis déplacé dans les salles serveurs avec l'administrateur réseau pour valider physiquement la disposition réelle des équipements dans les baies

.



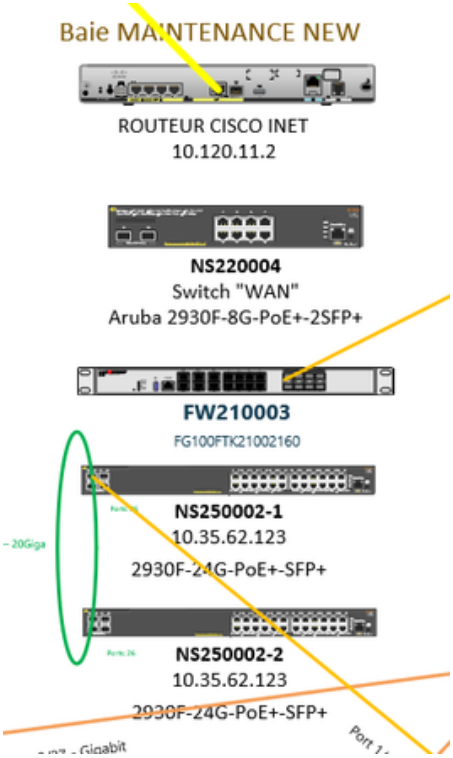
Apache Guacamole™

Audit et Cartographie des infrastructures réseaux

3. Analyse technique et modélisation réaliste sous Visio

J'ai totalement repensé l'aspect visuel de la documentation sous Microsoft Visio pour la rendre plus opérationnelle:

- Utilisation de modèles réalistes (Visio Café) : Contrairement aux anciens schémas qui utilisaient des formes génériques (simples carrés), j'ai intégré des bibliothèques d'icônes réalistes. Chaque équipement (Switch Aruba, Pare-feu Fortigate, Routeur Cisco) est désormais représenté par son image réelle, permettant de visualiser physiquement la façade du matériel.



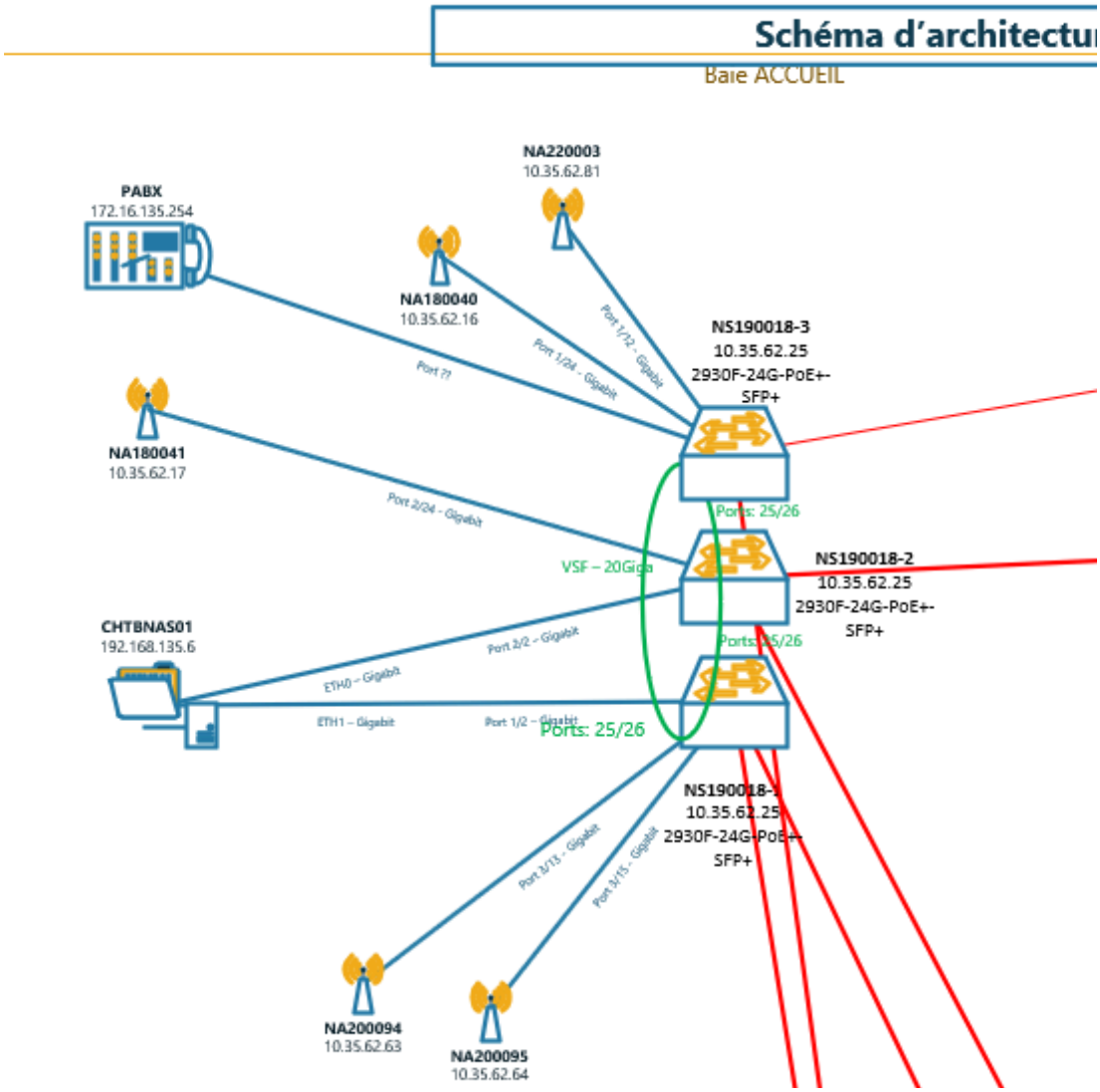
- Précision du câblage "Port par Port" : Grâce à ces modèles détaillés, j'ai pu relier chaque câble au port exact du switch (ex: Port 1/24, SFP+). Cette précision est capitale pour le brassage : on sait exactement où est connectée l'antenne Wi-Fi d'une unité comme Sojasun, Vrai, Bordier ou Petit Billy.

5. Comparaison : La remise à jour du Système d'Information

Cette étape démontre la valeur ajoutée du projet en comparant l'état initial (obsolète) et le résultat final (opérationnel).

A. Site de Châteaubourg (Sojasun / Nutrisun)

- Avant : Un schéma qui n'était plus à jour suite aux dernières évolutions matérielles, rendant le dépannage complexe.

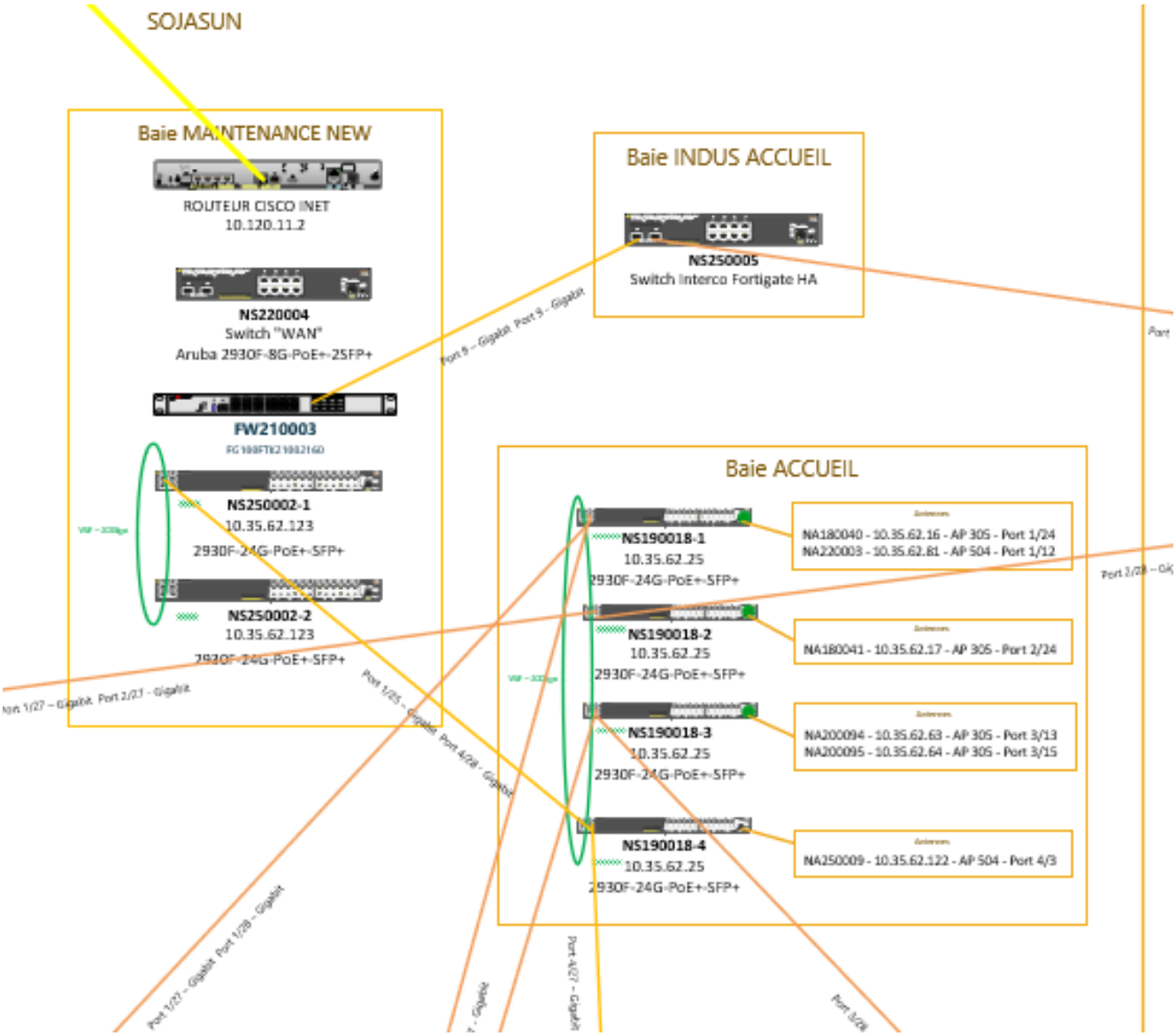


ACTIVITÉ N° 4-5

Audit et Cartographie des infrastructures réseaux

A. Site de Châteaubourg (Sojasun / Nutrisun)

- Après : Une cartographie incluant les nouvelles baies (Maintenance, Accueil, Nutrisun) avec tous les switchs et antennes correctement positionnés

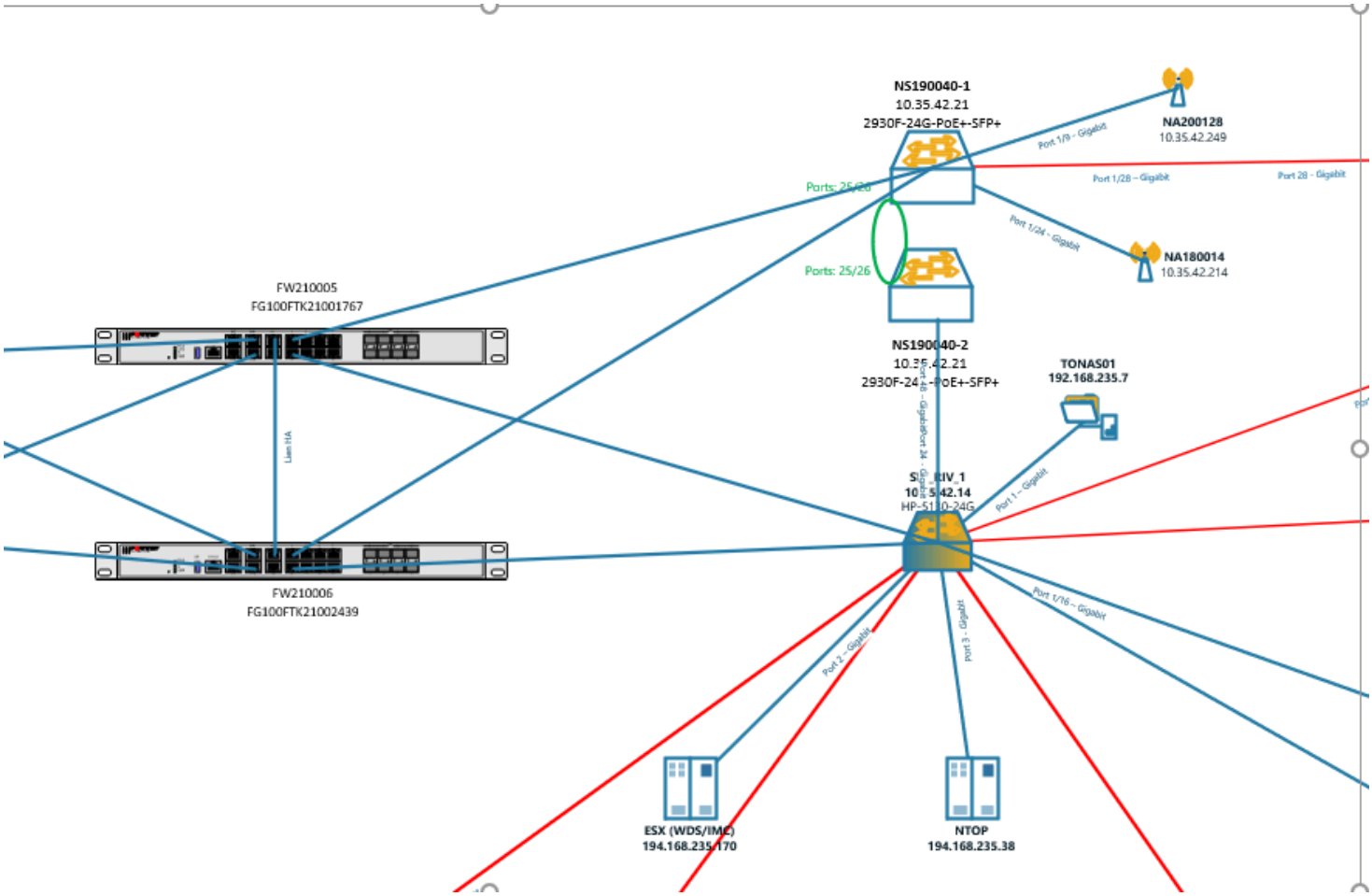


ACTIVITÉ N° 4-6

Audit et Cartographie des infrastructures réseaux

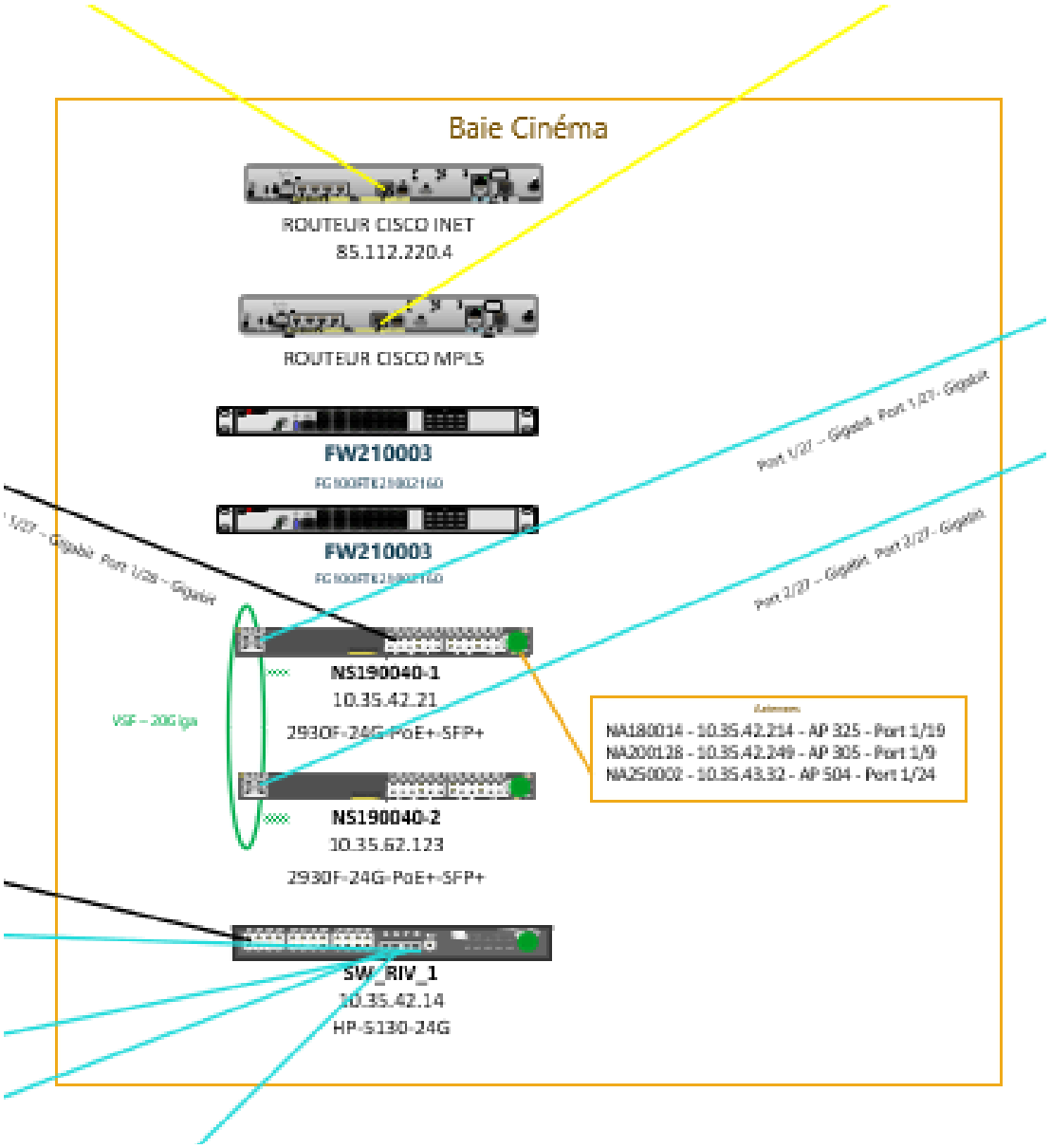
B. Site de Noyal-sur-Vilaine (La Rivière : Vrai / Bordier / Petit Billy)

- Avant : Une documentation illisible où les interconnexions entre les unités de production (Vrai, Bordier) n'étaient pas détaillées.



B. Site de Noyal-sur-Vilaine (La Rivière : Vrai / Bordier / Petit Billy)

- Après : Une architecture claire où l'on visualise chaque lien fibre et chaque port utilisé pour les marques du groupe



6. Conclusion de l'activité

Ce projet m'a permis de transformer une documentation obsolète en un véritable outil d'aide au diagnostic. J'ai appris qu'un schéma réseau n'est utile que s'il est **vivant** et **précis au port près**.

Grâce à cette modernisation, la DSI d'Olga dispose désormais d'un référentiel fiable. En cas de panne sur une antenne ou un lien fibre, l'origine du problème est immédiatement localisée, garantissant la réactivité du support et la continuité de l'activité industrielle sur tous les sites de production.

ACTIVITÉ N° 5

Configuration et déploiement d'un navigateur par défaut pour Application métier

1. Objectifs et Enjeux

L'objectif était de rétablir la fonctionnalité de géocodage au sein de l'ERP Copilote, utilisé par Cerreco (filiale d'OLGA). L'enjeu était d'assurer la compatibilité entre l'application et les services API de Google Maps, essentiels pour la localisation des fournisseurs et clients.

2. Contexte : Obsolescence d'Internet Explorer et dysfonctionnement de l'API

Le problème provenait du fait que Copilote ouvrait ses liens API via le navigateur par défaut du serveur RDS.

- **Le constat :** Internet Explorer s'ouvrait par défaut. Or, Google Maps a déprécié ce navigateur, affichant un message d'erreur demandant une mise à jour et bloquant l'affichage de la localisation.

- L**a demande :** Les utilisateurs ont sollicité la DSI pour passer sur un navigateur moderne (Google Chrome ou Microsoft Edge) afin de retrouver l'usage des cartes.

ACTIVITÉ N° 5-1

Configuration et déploiement d'un navigateur par défaut pour Application métier

2. Méthodologie : Comprendre l'infrastructure RemoteApp et RDS

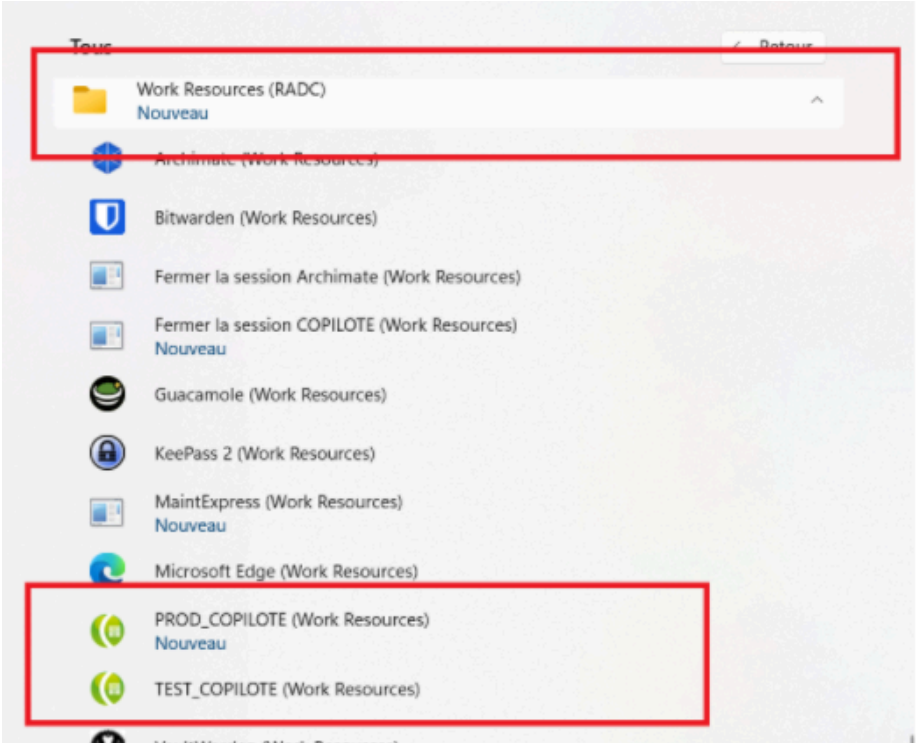
Avant de déployer la solution, il est essentiel de comprendre l'environnement technique dans lequel travaillent les utilisateurs de **Cerreco**:

- **L'ERP Copilote :** C'est l'outil de gestion principal (ERP) utilisé par la filiale. Il centralise toutes les données : fiches fournisseurs, commandes et logistique.

- **Le serveur RDS (Remote Desktop Services) :** Au lieu d'installer Copilote sur chaque PC individuellement, l'application est hébergée sur deux serveurs centraux (serveurs RDS). Cela permet une gestion simplifiée des mises à jour et une meilleure sécurité des données.

- **Le Connection Broker :** C'est l'élément qui gère les connexions. Il répartit les utilisateurs entre les serveurs et surtout, il permet aux utilisateurs de retrouver leur session intacte s'ils ont été déconnectés.

- **La technologie RemoteApp :** C'est la manière dont Copilote est diffusé aux utilisateurs. Pour l'employé, l'application s'affiche dans une fenêtre sur son bureau comme si elle était installée localement, mais en réalité, elle s'exécute sur le serveur distant.

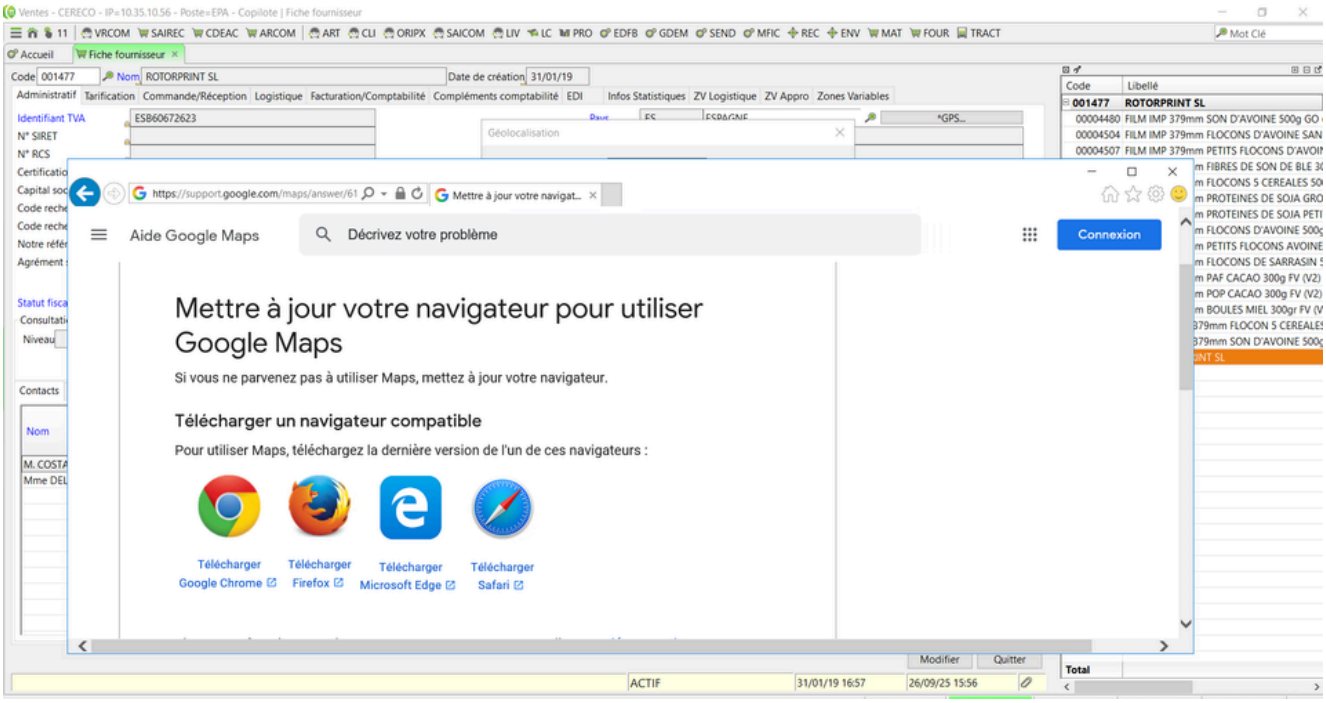


ACTIVITÉ N° 5-2

Configuration et déploiement d'un navigateur par défaut pour Application métier

2. Méthodologie : Comprendre l'infrastructure RemoteApp et RDS

Le Problème constaté : Lorsqu'on clique sur le bouton **"Géocodage"** dans Copilote pour localiser un fournisseur, le serveur RDS ouvrait automatiquement **Internet Explorer** par défaut. Comme ce navigateur est devenu obsolète, Google Maps refusait de s'afficher, bloquant ainsi le travail des utilisateurs.



Configuration et déploiement d'un navigateur par défaut pour Application métier

3. Analyse technique et création de la solution

Pour corriger ce problème, j'ai dû forcer l'utilisation de **Microsoft Edge** à la place d'Internet Explorer.

- **Le fichier de configuration XML :** J'ai utilisé un script pour générer un fichier nommé EdgeDefault.xml. Ce fichier contient les "associations par défaut", c'est-à-dire les règles qui disent au système : "Pour ouvrir un lien internet (HTTP/HTTPS), utilise Microsoft Edge".

EdgeDefault.xml

```xml
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
  <Association Identifier="http" ProgId="MSEdgeHTM" ApplicationName="Microsoft Edge" />
  <Association Identifier="https" ProgId="MSEdgeHTM" ApplicationName="Microsoft Edge" />

  <Association Identifier=".htm" ProgId="MSEdgeHTM" ApplicationName="Microsoft Edge" />
  <Association Identifier=".html" ProgId="MSEdgeHTM" ApplicationName="Microsoft Edge" />
</DefaultAssociations>
```

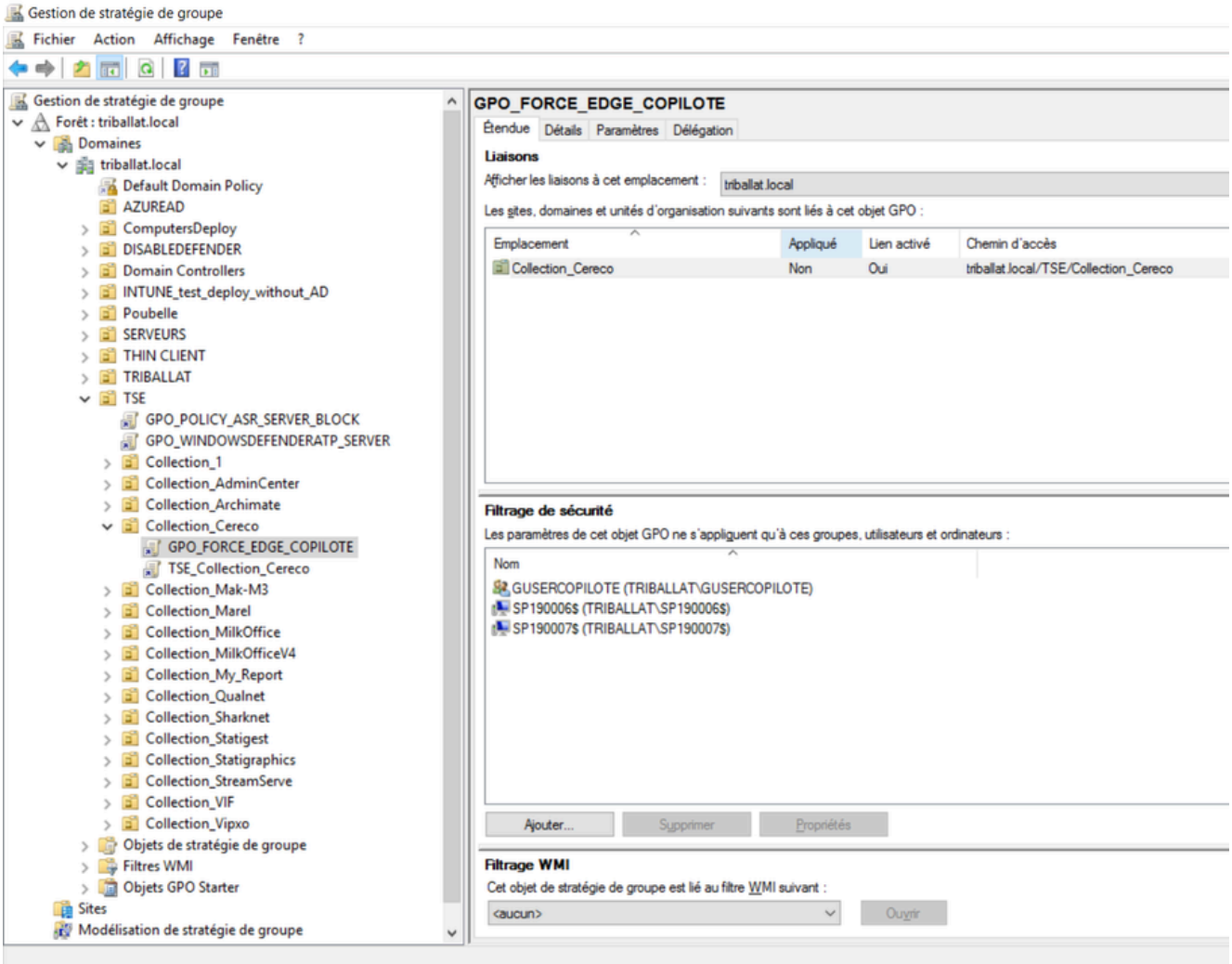
ACTIVITÉ N° 5-4

Configuration et déploiement d'un navigateur par défaut pour Application métier

3. Analyse technique et création de la solution

Le déploiement par GPO : J'ai créé une stratégie de groupe (GPO) intitulée "**FORCE EDGE COPILOTE**" sur le contrôleur de domaine.

- J'ai ciblé les deux serveurs RDS qui distribuent l'application.
- J'ai filtré la sécurité pour que cela s'applique au groupe "**GuserCopilote**", qui regroupe tous les utilisateurs ayant accès à l'application.

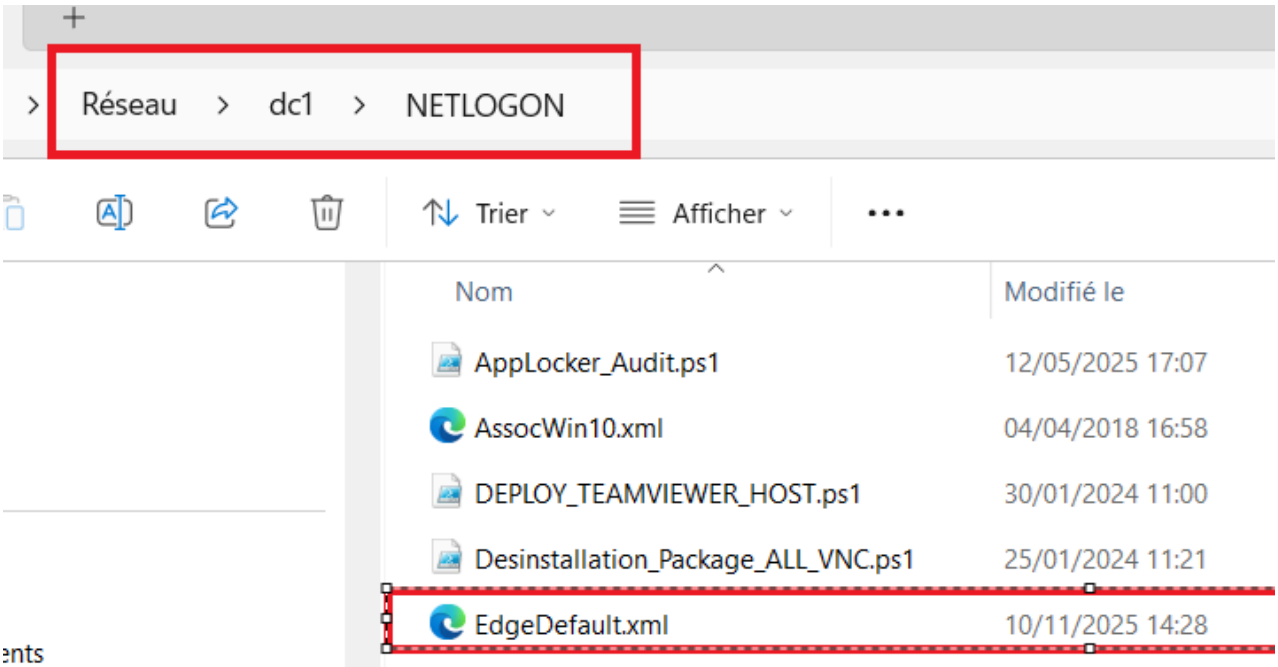


Configuration et déploiement d'un navigateur par défaut pour Application métier

4. Mise en œuvre et automatisation (Le rôle du Broker et de la GPO)

Pour que le changement de navigateur soit efficace et transparent pour la cinquantaine d'utilisateurs de **Cerreco**, j'ai dû prendre en compte la gestion des sessions par le serveur.

- **Le défi du Broker RDS :** Le **Broker** est le "chef d'orchestre" de l'infrastructure. Son rôle est de mémoriser l'état des sessions. Chez Cerreco, les utilisateurs ne ferment pas toujours leur session ; ils se déconnectent simplement, et le Broker garde leur session "enregistrée" (en attente) pour qu'ils retrouvent leur travail intact plus tard.
    - Le problème : Habituellement, une GPO d'association d'applications ne s'applique qu'à la création d'un nouveau profil (première connexion). Les sessions déjà gérées par le Broker n'auraient donc pas reçu la mise à jour.
- **Stockage sur le NETLOGON :** J'ai placé mon fichier de configuration EdgeDefault.xml dans le dossier \\Dc1\netlogon. C'est un emplacement stratégique et sécurisé car il est répliqué sur tous les contrôleurs de domaine et accessible en lecture seule pour tous les serveurs et PC au moment de la connexion.

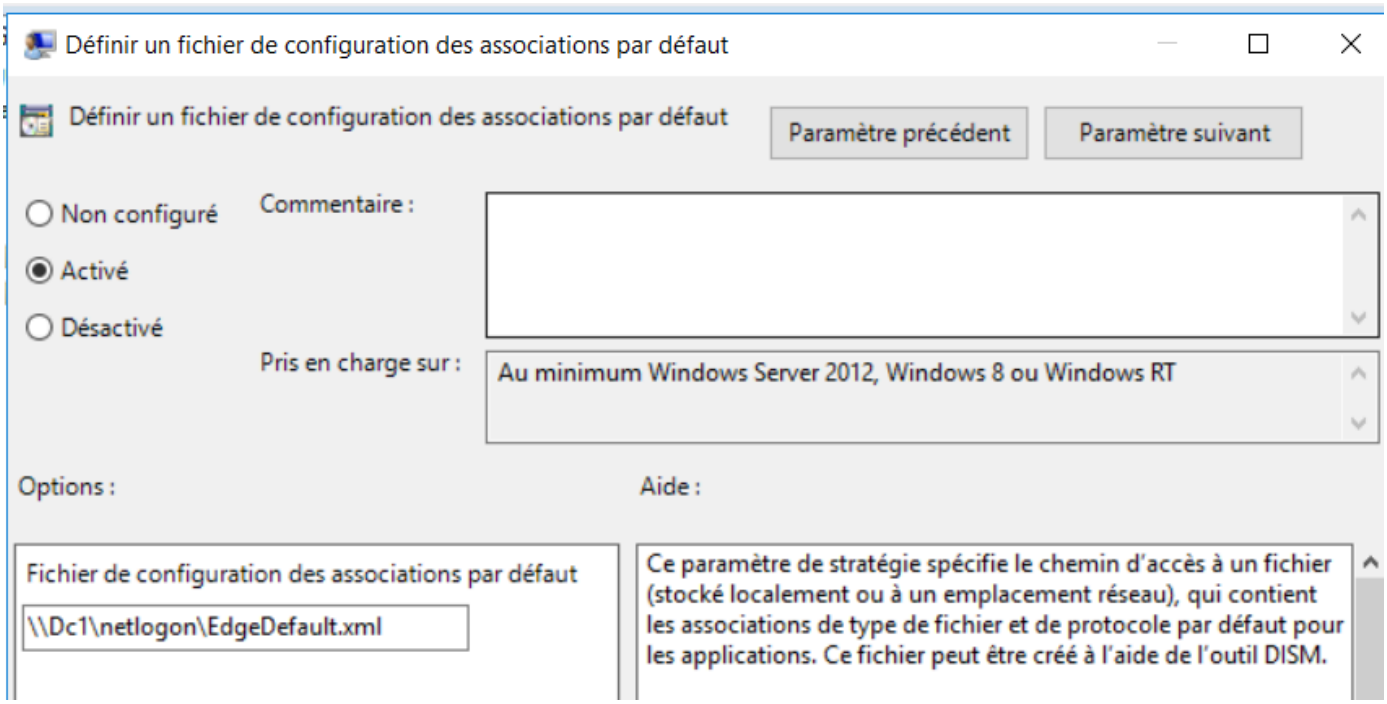


ACTIVITÉ N° 5-6

Configuration et déploiement d'un navigateur par défaut pour Application métier

4. Mise en œuvre et automatisation (Le rôle du Broker et de la GPO)

- **Configuration de la stratégie et forçage :** Dans l'éditeur de gestion des GPO, j'ai activé l'option "Définir un fichier de configuration des associations par défaut".
    - **Ma solution pour le Broker :** Pour éviter de devoir redémarrer les serveurs ou de forcer la déconnexion de tout le monde, j'ai configuré la GPO pour qu'elle force l'écriture des nouvelles associations directement dans le registre Windows.
-
    - **Résultat :** Même pour les sessions qui étaient déjà enregistrées dans le Broker, le système a pris en compte Microsoft Edge dès que l'utilisateur a relancé son RemoteApp Copilote. Cela a permis une continuité de service totale sans aucune interruption de travail.



Configuration et déploiement d'un navigateur par défaut pour Application métier

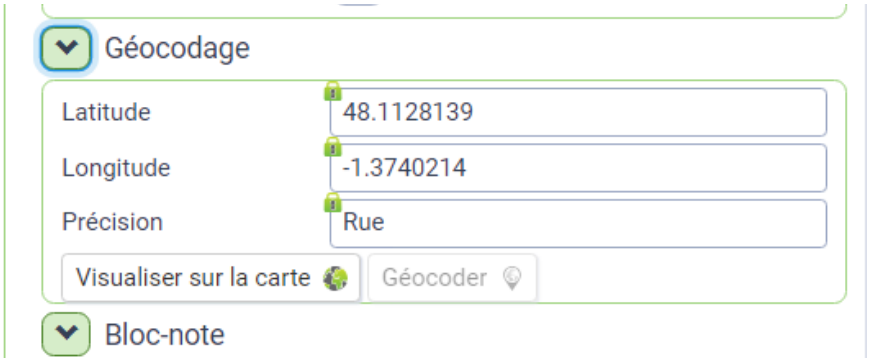
5. Validation et Résultat final

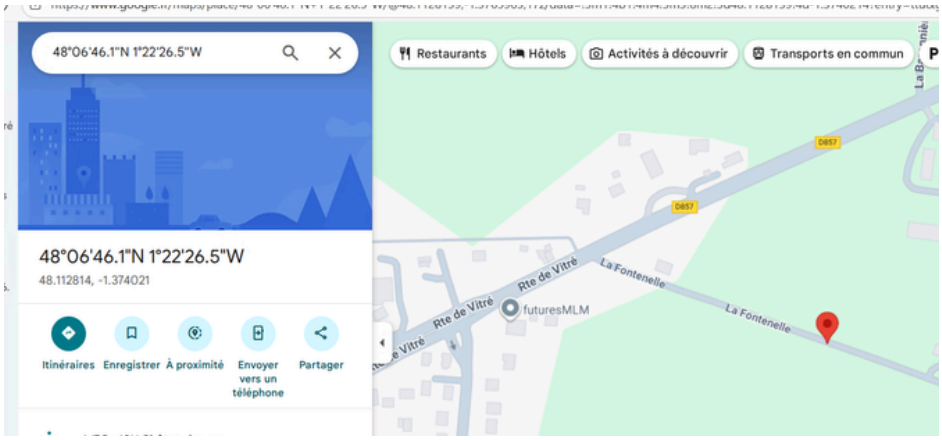
Une fois la GPO propagée et le forçage des registres effectué, j'ai procédé à une phase de test pour vérifier que la solution était bien prise en compte, même pour les utilisateurs déjà connectés au Broker.

- **L'action utilisateur :** L'utilisateur ouvre sa session RemoteApp, accède à la fiche d'un fournisseur (comme ROTORPRINT) et clique sur le bouton "**Visualiser sur la carte**".

- **Le résultat technique** : Le système détecte immédiatement la nouvelle association. Au lieu d'ouvrir Internet Explorer, il lance Microsoft Edge.

- **Le succès :** La carte Google Maps s'affiche instantanément. L'API transmet les coordonnées de Latitude et Longitude sans erreur. L'utilisateur peut cliquer sur "Visualiser sur la carte" pour voir l'emplacement précis du tiers.





Configuration et déploiement d'un navigateur par défaut pour Application métier

6. Conclusion de l'activité

Ce projet m'a permis de résoudre un blocage métier critique tout en maîtrisant les spécificités d'une infrastructure **RDS**. J'ai appris qu'une intervention réussie doit être invisible pour l'utilisateur : grâce à ma gestion du Broker, j'ai pu déployer la solution sans aucune coupure de service.

Désormais, tous les postes de **Cerreco** peuvent utiliser la fonction de géocodage normalement. L'accès à Google Maps est rétabli pour l'ensemble des sessions.

ACTIVITÉ N° 6

Développement et modernisation d'une Weather map de supervision

1. Objectifs et Enjeux

L'objectif était de moderniser l'outil de visualisation réseau (**Weather Map**) utilisé par le pôle support de la DSI. L'enjeu était de passer d'une carte archaïque et illisible à une interface moderne permettant de surveiller en temps réel la charge des liens (Internet et MPLS) sur chaque site industriel d'Olga.a.

2. Contexte : Une supervision archaïque

L'ancienne Weather Map présentait plusieurs défauts majeurs pour une exploitation quotidienne :

- **Défaut d'affichage :** Sur les écrans géants de la salle de supervision, les informations étaient trop petites et sombres. Le support ne pouvait pas distinguer les alertes de loin.
- **Manque de précision :** On ne voyait pas clairement la séparation entre les liens principaux et les liens de secours, ni le débit exact consommé par site.
- **Besoin métier :** Il fallait savoir instantanément si un site était saturé ou si un lien était "Down" pour intervenir avant que la production ne soit impactée.

Développement et modernisation d'une Weather map de supervision

3. Méthodologie : L'infrastructure technique et le rôle d'Icinga

Pour construire cet outil, je me suis appuyé sur l'infrastructure de supervision déjà en place chez Olga :

- **C'est quoi Icinga** ? Icinga est l'outil de supervision principal de la DSI. Il surveille en permanence l'état des serveurs et des routeurs. Grâce au protocole **SNMP**, Icinga interroge chaque routeur sur tous les sites (Noyal, Châteaubourg, etc.) pour connaître le trafic exact qui passe par les ports WAN.

- **L'utilité d'une Weather Map sur écran de supervision :** Au sein du support DSI, nous avons un ecran qui affiche la "santé" du réseau. Une Weather Map est essentielle car :

  - Elle offre une **vue d'ensemble immédiate** : pas besoin de fouiller dans des listes de données, on voit tout d'un coup.

  - Elle permet d'être **proactif** : si une jauge passe à l'orange, le support voit tout de suite qu'un site sature avant même que les utilisateurs ne s'en plaignent.

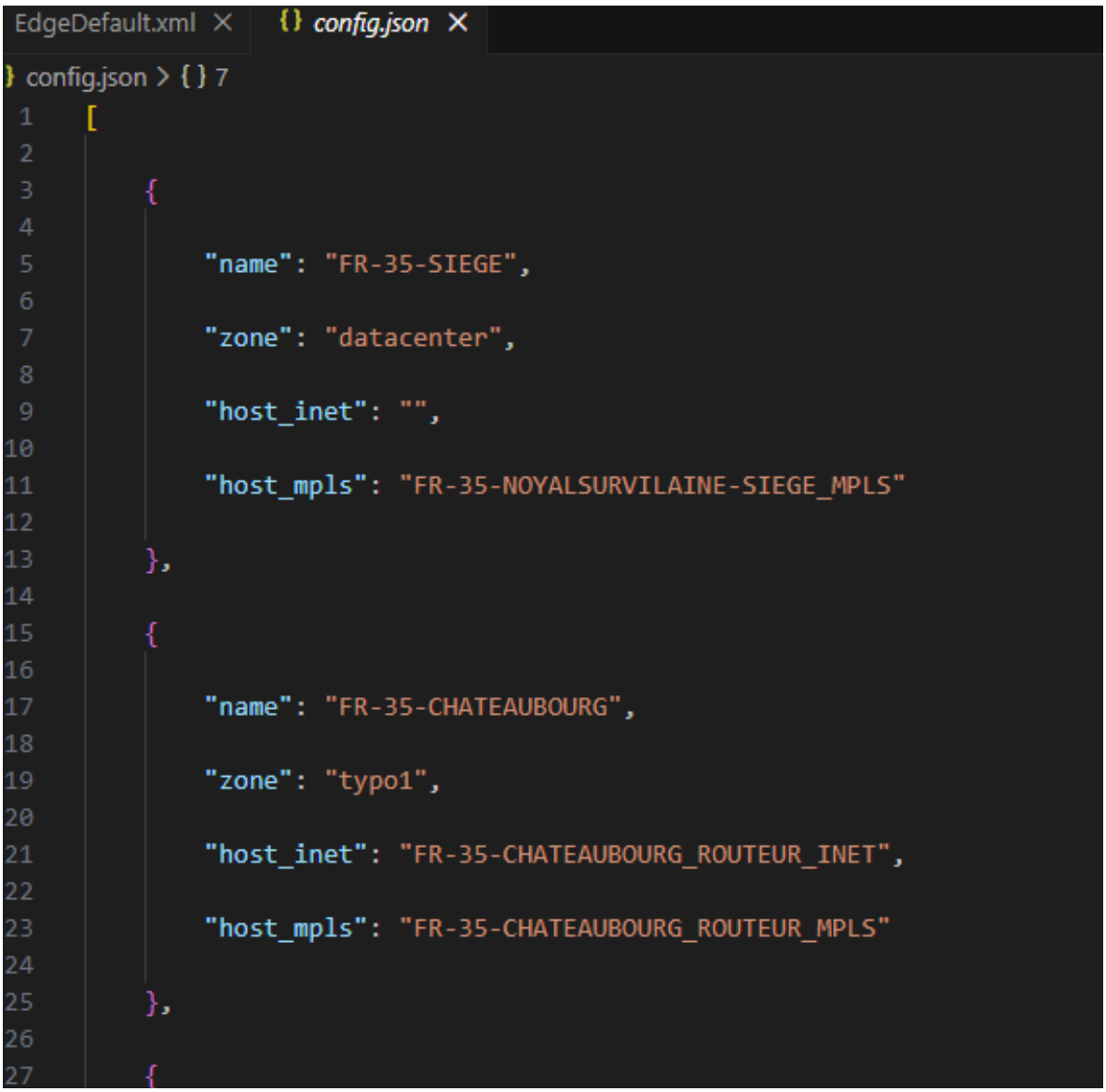
  - Elle facilite le **diagnostic** : on voit immédiatement si c'est le lien MPLS (réseau interne) ou le lien Internet qui pose problème.

Développement et modernisation d'une Weather map de supervision

4. Développement : La structure du code (Les 3 fichiers)

Pour passer des données brutes d'Icinga à un affichage moderne, j'ai développé trois fichiers complémentaires :

- **config.json** (Le référentiel) : Ce fichier contient la liste de tous les sites d'Olga (ex: FR-35-CHATEAUBOURG). Pour chaque site, on lui donne son nom et surtout l'adresse IP des routeurs (INET et MPLS) qu'Icinga doit surveiller.



Développement et modernisation d'une Weather map de supervision

4. Développement : La structure du code (Les 3 fichiers)

- **api.php (Le moteur de données) :** C'est le fichier "cerveau". Il se connecte à la base de données d'Icinga (InfluxDB) pour récupérer les métriques de trafic. Il calcule ensuite le pourcentage d'utilisation par rapport à la capacité maximale du lien.

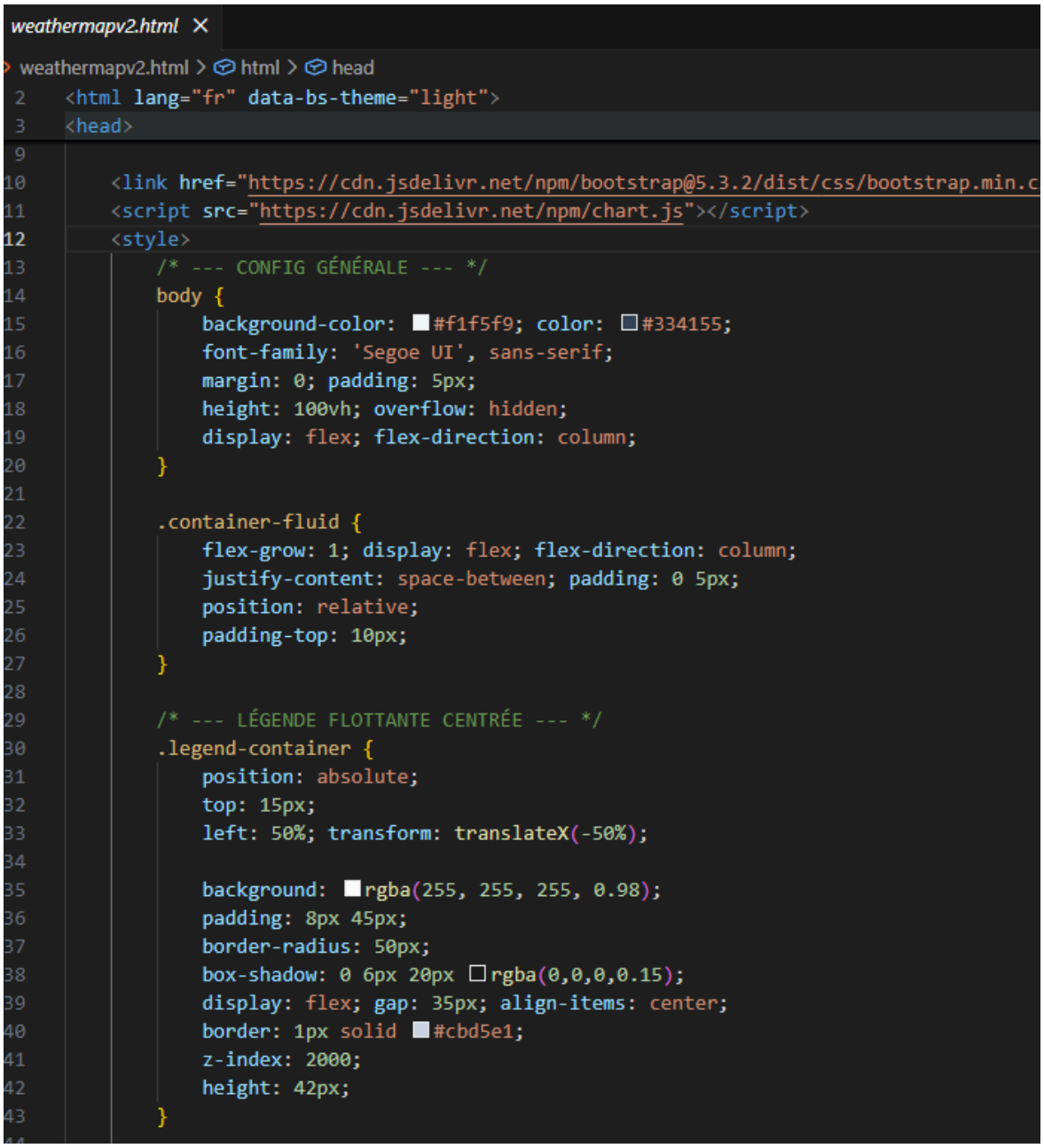
api.php

```
36    foreach ($sites as $site) {
37        $processLink = function($host, $mode_calcul = null) {
59            // Si mode "x8" (Siège/Octets) -> Conversion en bits
60            if ($mode_calcul === 'x8') {
61                $mb_in  = $val_in * 8;
62                $mb_out = $val_out * 8;
63            } else {
64                $mb_in = $val_in;
65                $mb_out = $val_out;
66            }
67
68            // Nettoyage si valeurs brutes énormes (parfois Icinga envoi
69            if ($mb_in > 10000) { $mb_in /= 1000000; }
70            if ($mb_out > 10000) { $mb_out /= 1000000; }
71
72            $pct = ($usage_in !== null && $usage_in <= 100) ? $usage_in
73
74            return [
75                'pct' => round($pct, 1),
76                'val_in' => round($mb_in, 2),
77                'val_out' => round($mb_out, 2),
78                'status' => 'ok',
79                'active' => true
80            ];
81        };
```

Développement et modernisation d'une Weather map de supervision

4. Développement : La structure du code (Les 3 fichiers)

- **weathermapv2.html (L'interface visuelle) :** C'est ce qui s'affiche à l'écran. J'ai utilisé du HTML/CSS pour créer des "cartes" par site et du JavaScript avec la librairie Chart.js pour dessiner les jauges circulaires qui se remplissent selon le trafic.



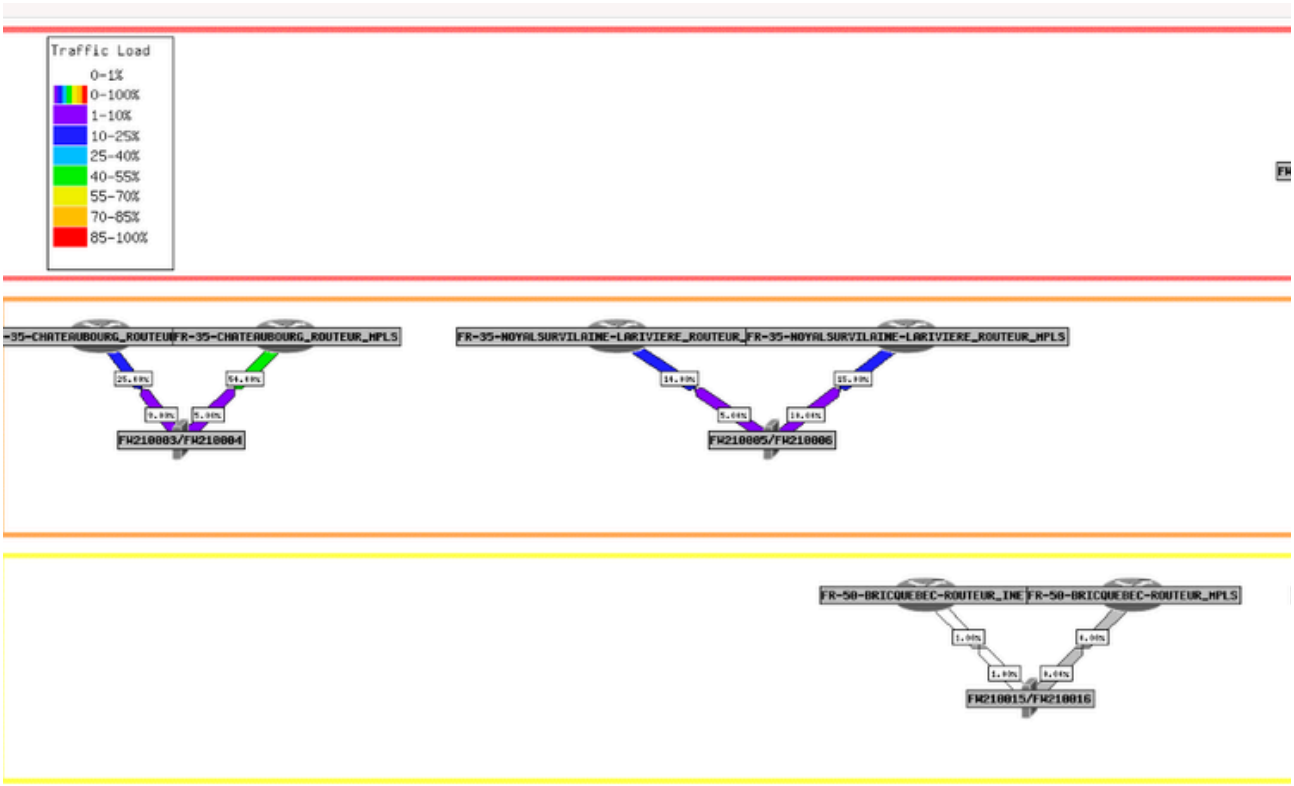
```
weathermapv2.html
weathermapv2.html > html > head
<html lang="fr" data-bs-theme="light">
<head>

    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.c
    <script src="https://cdn.jsdelivr.net/npm/chart.js"></script>
    <style>
        /* --- CONFIG GÉNÉRALE --- */
        body {
            background-color: #f1f5f9; color: #334155;
            font-family: 'Segoe UI', sans-serif;
            margin: 0; padding: 5px;
            height: 100vh; overflow: hidden;
            display: flex; flex-direction: column;
        }

        .container-fluid {
            flex-grow: 1; display: flex; flex-direction: column;
            justify-content: space-between; padding: 0 5px;
            position: relative;
            padding-top: 10px;
        }

        /* --- LÉGENDE FLOTTANTE CENTRÉE --- */
        .legend-container {
            position: absolute;
            top: 15px;
            left: 50%; transform: translateX(-50%);

            background: rgba(255, 255, 255, 0.98);
            padding: 8px 45px;
            border-radius: 50px;
            box-shadow: 0 6px 20px rgba(0,0,0,0.15);
            display: flex; gap: 35px; align-items: center;
            border: 1px solid #cbd5e1;
            z-index: 2000;
            height: 42px;
        }
```

Développement et modernisation d'une Weather map de supervision

5. Comparaison : La modernisation de l'affichage

Voici le résultat concret de mon travail de développement :

- **AVANT : L'ancienne Weather Map**
  - Le design était "archaïque" (style années 2000), très sombre et les textes étaient minuscules.
  - Sur les écrans de supervision, il était impossible de lire les débits à plus de 2 mètres. Le support perdait du temps à plisser les yeux pour voir si un site était en panne.

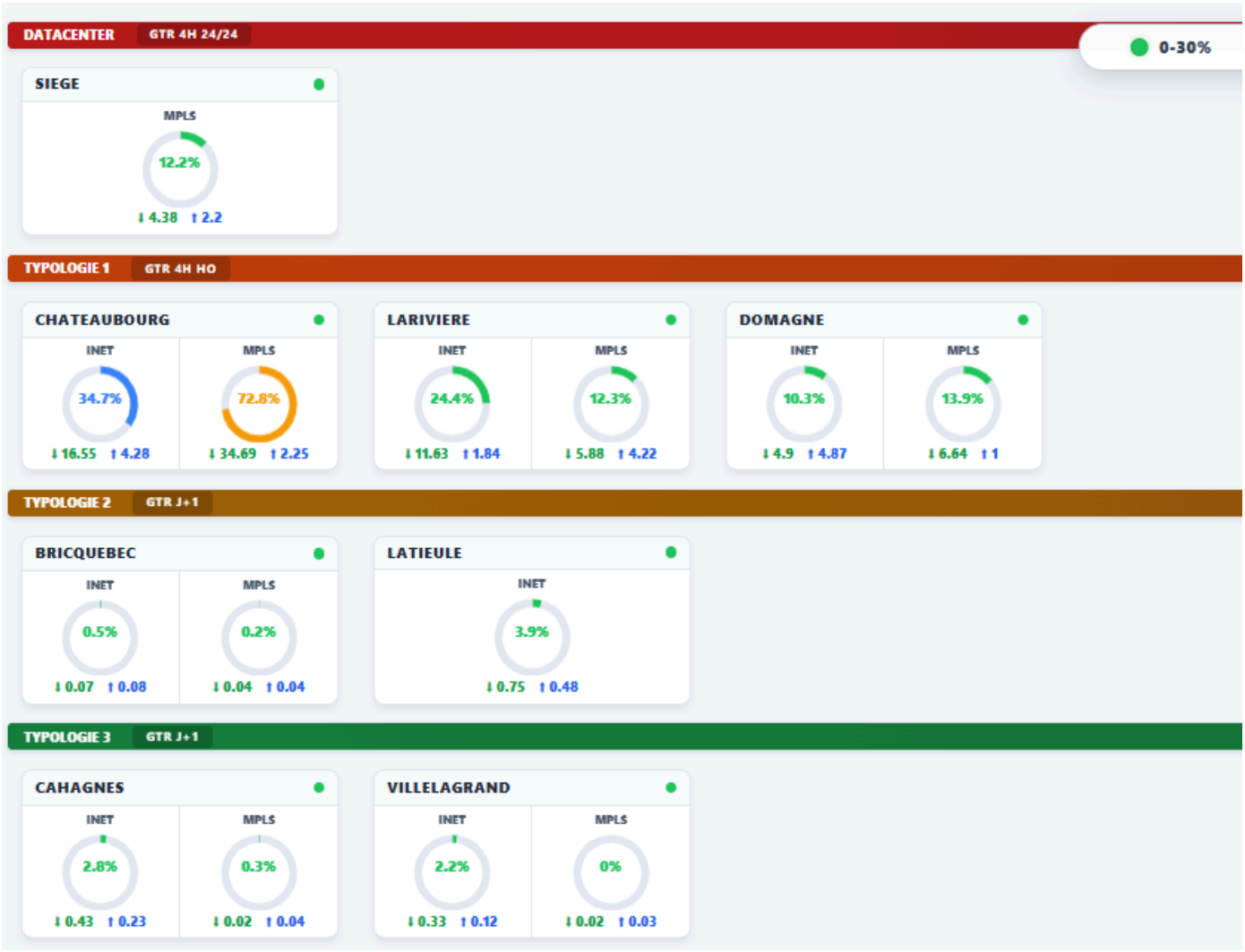


Développement et modernisation d'une Weather map de supervision

5. Comparaison : La modernisation de l'affichage

Voici le résultat concret de mon travail de développement :

- **APRÈS : Ma nouvelle Weather Map**
  - L'interface est épurée et lumineuse. On distingue clairement les deux liens par site.
  - J'ai ajouté des codes couleurs vifs : le support voit immédiatement si un lien est "Down" (Rouge) à l'autre bout de la pièce.
  - Les débits réels (Mbps) sont affichés en gros sous chaque jauge pour une précision maximale.



Développement et modernisation d'une Weather map de supervision

6. Conclusion de l'activité

Ce projet m'a permis de mettre mes compétences en **développement (HTML/PHP/JS)** au service du **réseau**. J'ai appris qu'un outil de supervision n'est efficace que s'il est visuellement simple : moins le technicien passe de temps à chercher l'information, plus il est rapide pour corriger la panne.

Désormais, grâce à ce "mur de supervision" modernisé, la DSI d'Olga peut garantir une surveillance 24h/24 des liens de production sans aucune zone d'ombre.

La Sècurisation des accès via le MFA

1. Contexte et Définition

Chez OLGA, la protection des comptes professionnels est une priorité stratégique. Face à la recrudescence du phishing et du vol de mots de passe, la simple combinaison "identifiant/mot de passe" ne suffit plus.

Dans ce cadre, j'ai mené une veille technologique sur l'**Authentification Multi-Facteurs (MFA)**. Cette méthode consiste à vérifier l'identité d'un utilisateur en exigeant au moins deux preuves distinctes. Le MFA repose sur la combinaison de trois facteurs :

- **Ce que l'on sait** : Un mot de passe ou un code PIN.
- **Ce que l'on possède** : Un smartphone professionnel ou une clé de sécurité physique (FIDO2).
- **Ce que l'on est** : La biométrie (empreinte digitale ou reconnaissance faciale via Windows Hello).

La Sècurisation des accès via le MFA

2. Fonctionnement et Mise en œuvre chez OLGA

La solution retenue par la DSI s'appuie sur l'écosystème **Microsoft Entra ID (Azure AD)** pour garantir un haut niveau de sécurité.

Les outils déployés :

- **Clés de sécurité FIDO2 :** Dispositifs physiques (type YubiKey) offrant une authentification forte "Passwordless" (sans mot de passe), impossible à pirater à distance.
- **Microsoft Authenticator :** Une application mobile qui génère des codes à usage unique ou des notifications d'approbation par simple clic.

La règle de sécurité appliquée : Une politique d'**Accès Conditionnel** a été mise en place. Dès qu'une connexion provient de l'**extérieur du réseau interne** (télétravail, déplacement, sites non reconnus), le MFA est obligatoirement sollicité :

- **Utilisateur avec mobile pro :** Utilisation prioritaire de l'application Microsoft Authenticator.
- **Utilisateur sans mobile pro :** Utilisation obligatoire de la clé FIDO2 pour valider l'accès.

La Sècurisation des accès via le MFA

3. Pourquoi cette veille technologique ?

La veille technologique ne s'arrête pas à l'installation d'un outil ; elle consiste à choisir la solution la plus adaptée au marché et aux besoins de l'entreprise.

- **Conformité et Standards :** Le choix de Microsoft et du standard FIDO2 assure à OLGA d'être en conformité avec les recommandations de l'ANSSI et les exigences réglementaires.
- **Renforcement de la posture de sécurité :** Cette veille a permis de bloquer 99,9 % des attaques basées sur l'identité (Credential Stuffing, Phishing). Même si un pirate vole un mot de passe, il ne peut rien faire sans le second facteur physique.
- **Accompagnement au changement :** La veille a aussi servi à évaluer l'ergonomie. Le but était de proposer une méthode rapide (clic sur le téléphone ou insertion de clé) pour ne pas ralentir le travail des collaborateurs tout en les protégeant.

4. Conclusion de la veille

Le déploiement du MFA représente un investissement stratégique dans la cybersécurité d'OLGA. Cette veille a permis de passer d'une sécurité périmétrique (basée sur le réseau du bureau) à une sécurité centrée sur l'identité, indispensable dans un monde où le télétravail est devenu la norme. C'est une barrière inviolable qui renforce la résilience du groupe face aux menaces numériques modernes.

CONCLUSION GÉNÉRALE

Ces deux années d'alternance au sein de la DSI du groupe OLGA ont été une étape déterminante de mon parcours professionnel. Elles m'ont permis de passer de la théorie académique à la réalité opérationnelle d'un environnement industriel complexe.

Un bilan technique et méthodologique

À travers les 6 activités présentées, j'ai pu explorer toutes les facettes du métier d'Administrateur Système et Réseau :

- L'infrastructure : De la modernisation de la cartographie réseau à la gestion des serveurs RDS.
- Le développement : La création d'outils de supervision sur-mesure pour faciliter le travail du support.
- La sécurité : La mise en œuvre de solutions d'authentification forte (MFA) pour protéger les accès distants.

Évolution personnelle

Au-delà de la technique, cette expérience m'a apporté :

- L'autonomie : Savoir mener des projets de A à Z, comme la refonte complète de la Weather Map.
- La réactivité : Apprendre à gérer les priorités lors des incidents critiques sur le réseau.
- Le sens du service : Comprendre que l'informatique est un outil au service des métiers (Logistique, RH, Production).

En conclusion, je suis fier d'avoir contribué à la modernisation et à la sécurisation du Système d'Information **d'OLGA**. Cette alternance confirme ma volonté de poursuivre ma carrière dans la gestion d'infrastructures informatiques, avec une attention constante portée à l'évolution du **Système et du Réseau.**

NOA