TALIS ASTON ECOLE IT

econocom LIVE TECH

# Technicien(ne) Systèmes, Réseaux et Sécurité

Dossier de Validation

| | |
|---|---|
| Nom Prénom | BAÏ Azdine |
| Nom(s) Prénom(s) du ou des tuteurs | DESREUMAUX, Joël VANDEVELDE,Julien |
| Acronyme de la certification IPI visée | TSRS |
| Niveau visé | 5 |
| Date de la soutenance | 25 juillet 2025 |
| Lieu de la soutenance | Aston Lille |

ipi ÉCOLE D'INFORMATIQUE Certificateur de compétences

UNE ÉCOLE DU GROUPE IGS

# PRÉAMBULE

Actuellement en alternance en tant que technicien systèmes, réseaux et sécurité chez ECONOCOM à Villeneuve-d'Ascq, tout en suivant la formation Technicien Systèmes Réseaux et Sécurité à Aston IT à Lille.

En 2019, j'ai obtenu un baccalauréat Sciences et Technologies de Laboratoire (STL) avec une spécialisation en biotechnologies au lycée de Douai. À cette époque, je n'avais pas encore de projet professionnel clairement défini, c'est pourquoi je me suis orienté vers un BTS Métiers de la Chimie. Toutefois, en 2020, après une réflexion personnelle, j'ai décidé d'interrompre cette formation car elle ne correspondait pas à mes attentes. S'en est suivie une période d'incertitude durant laquelle j'ai occupé divers emplois tout en découvrant une nouvelle passion : l'informatique. C'est au cours de cette période que j'ai monté mon premier PC, expérience déterminante qui a déclenché chez moi une véritable envie d'explorer ce domaine professionnellement.

En 2022, attiré initialement par un métier orienté vers l'action, j'ai envisagé de devenir pompier de Paris et j'ai suivi une formation en sécurité privée afin de me préparer à cette voie. Cette expérience m'a permis de réaliser que ce qui me motivait profondément n'était pas un métier d'action en soi, mais plutôt un métier nourri par la passion et l'apprentissage permanent.

Ainsi, à l'été 2023, j'ai décidé de reprendre mes études et de m'orienter pleinement vers l'informatique. Après avoir étudié plusieurs formations possibles, j'ai découvert l'école Aston IT où je me suis inscrit après un entretien en août 2023. Cependant, la principale difficulté à laquelle j'ai dû faire face a été la recherche d'une alternance : sans aucune expérience préalable dans l'informatique, décrocher ne serait-ce qu'un entretien représentait un véritable défi. Ma persévérance m'a finalement permis d'obtenir une alternance au sein d'Econocom, ce qui représente une grande étape dans mon parcours.

À travers ce mémoire, je souhaite non seulement présenter les compétences techniques et professionnelles acquises, mais aussi montrer mon évolution personnelle, illustrant ainsi qu'il est possible de se réorienter professionnellement avec succès dans un domaine complètement nouveau.

# TABLE DES MATIERES

# Présentation de l’entreprise

## Présentation d’Econocom

Fondé en 1974 par Jean-Louis Bouchard, Econocom est un groupe européen spécialisé dans la transformation numérique des organisations. Présent sur 4 continents et dans 16 pays, le groupe regroupe plus de 8 800 collaborateurs et a réalisé un chiffre d’affaires de 2,74 milliards d’euros en 2024.

Il intervient dans tous les secteurs : santé, éducation, industrie, finance, retail et services publics.

Son modèle unique repose sur quatre domaines d’expertise complémentaires :

- Products & Solutions : distribution, personnalisation, déploiement et recyclage d’équipements numériques
- Services : infogérance, support utilisateur, modernisation des infrastructures et migration cloud
- Technology Management & Financing : financement technologique et gestion de parc
- Audiovisuel & Digital Signage : intégration de solutions immersives pour la collaboration et la communication visuelle

Le groupe est également fortement engagé dans une démarche RSE[1] : économie circulaire, reconditionnement, réduction de l’empreinte carbone, et politique d’inclusion.

En France, Econocom s’appuie sur plusieurs centres de services techniques, dont le Centre de Services 2IP Nord à Villeneuve-d’Ascq, que j’ai intégré dans le cadre de mon alternance.

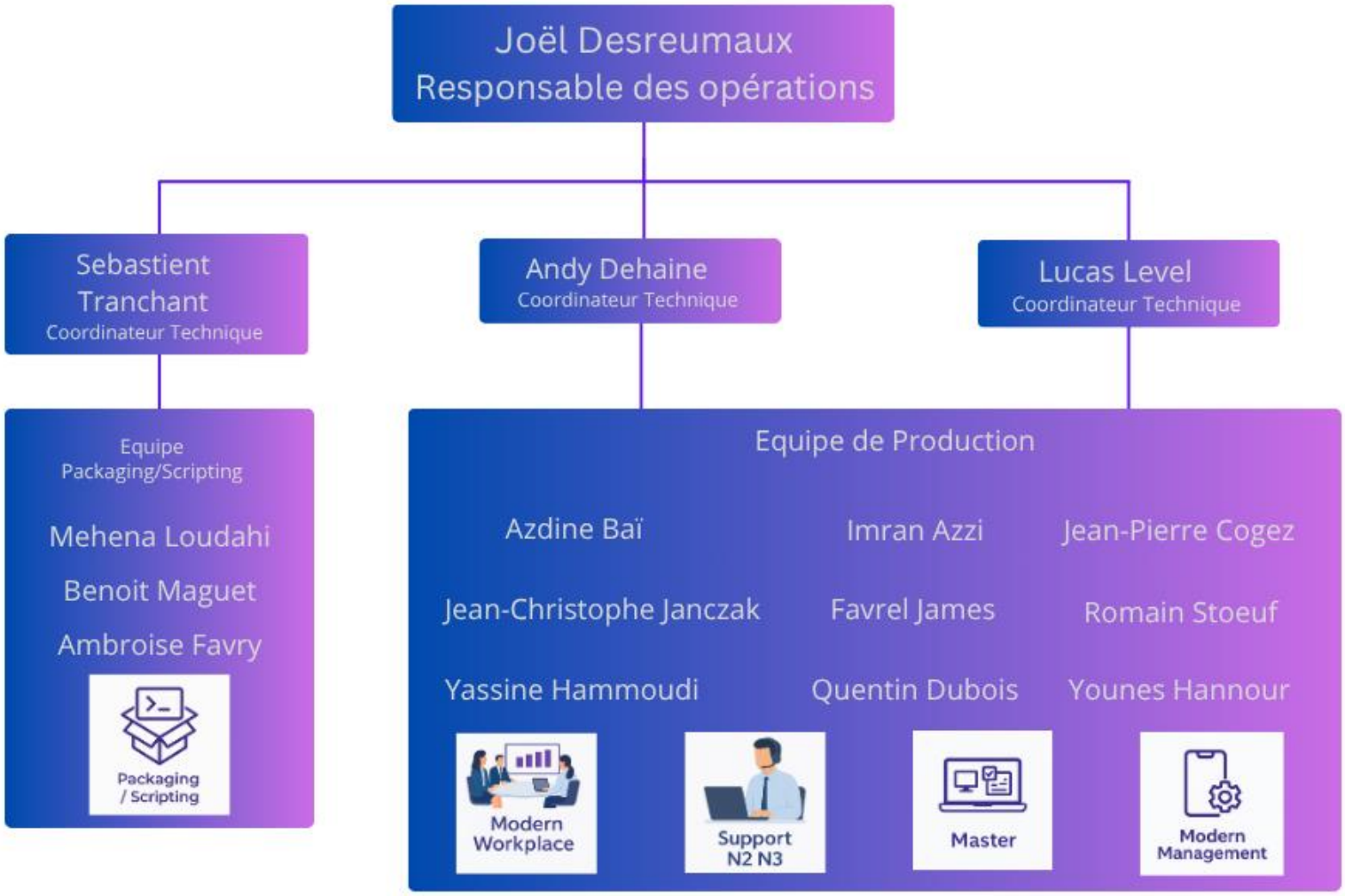
[1] Responsabilité Sociétale des Entreprises : Intégration volontaire des enjeux sociaux et environnementaux dans les activités de l’entreprise.

## Organigramme et services de l’entreprise

Au-delà de son organisation par pôles métiers, Econocom fonde son action sur trois valeurs essentielles :

- Audace, pour oser entreprendre et innover,
- Bonne foi, pour construire des relations basées sur la confiance et la transparence,
- Réactivité, pour s’adapter en permanence aux besoins de ses clients. Ces valeurs se traduisent au quotidien par un esprit d’initiative, une communication directe et une capacité à rebondir face aux défis.

## Organigramme du Centre de Service 2IP Nord



## Présentation du Centre de Service 2IP Nord

Le Centre de Services 2IP Nord, basé à Villeneuve-d'Ascq, constitue une structure technique de référence pour Econocom. Il regroupe plusieurs pôles spécialisés qui assurent des prestations complètes autour du poste de travail, des serveurs, du réseau et des outils de supervision.

Ce centre est structuré selon quatre grands domaines de compétences :

Ingénierie et Run Workplace : prise en charge de la maîtrise d'œuvre sur le poste de travail, création de masters, packaging d'applications, déploiement et maintien des environnements utilisateurs.

Exploitation et Production : gestion de la supervision, traitement des alertes, maintenance opérationnelle et actions curatives dans le cadre de la continuité de service.

Administration Systèmes & Réseaux : configuration réseau, administration de serveurs, virtualisation et gestion de l'infrastructure Windows.

Expertise et Support Niveau 3 : traitement des incidents complexes (systèmes, réseaux, bases de données, Modern Workplace).

En complément de ces activités, le Centre de Services 2IP Nord assure également la fourniture et la gestion de licences Veeam pour la sauvegarde et la restauration des environnements, ainsi que la gestion de MECM[2] pour le déploiement et l'administration centralisée des postes de travail.

[2] Microsoft endpoint configuration manager

## Mon rôle au sein d'Econocom

J'ai commencé mon alternance chez Econocom au sein du Helpdesk dédié au client Bonduelle. Intégré à une équipe chargée du support utilisateur de niveau 0 à 1, j'assurais la gestion des incidents via la plateforme EasyDesk, la prise en main à distance avec les outils BeyondTrust et Wallix, ainsi que le suivi rigoureux des interventions dans le respect des engagements de service (SLA[3]). Cette première expérience m'a permis d'acquérir des compétences solides en assistance technique, en diagnostic d'incidents et en communication professionnelle avec des utilisateurs variés.

Fort de ces premières compétences, j'ai eu l'opportunité, à partir de novembre dernier, de rejoindre l'équipe d'ingénierie poste de travail du Centre de Services 2IP Nord, tout en continuant à assurer mes missions initiales à l'Helpdesk. J'interviens désormais deux jours par semaine au sein de l'ingénierie, où je participe au déploiement de masters Windows avec MDT[4], à la gestion de terminaux mobiles via Intune, ainsi qu'à la gestion de l'infrastructure du service. Ce travail m'a permis de découvrir les enjeux liés à l'automatisation du poste de travail et de consolider mes compétences en déploiement d'environnements numériques.

Aujourd'hui, je suis intégré à l'équipe Workstation du Centre de Services 2IP Nord, sous la supervision d'un coordinateur technique. Mon rôle s'inscrit dans une dynamique transverse : je travaille en collaboration étroite avec les équipes Helpdesk, Infrastructure Réseau et Support de Proximité, ce qui me permet d'intervenir aussi bien sur des projets structurants que sur des opérations de support quotidien. Cette polyvalence a renforcé ma capacité à évoluer dans des environnements techniques complexes et exigeants.

[3] Service Level Agreement
[4] Microsoft Deployment Toolkit

## Fiche de poste actuelle : Technicien systèmes, réseaux et sécurité

Je suis intégré au Centre de Services 2IP Nord d'Econocom à Villeneuve-d'Ascq, où j'interviens principalement pour le client Bonduelle. Mon rôle s'inscrit à la croisée du support utilisateur et de l'ingénierie poste de travail.

Mes missions couvrent plusieurs volets techniques :

- Support utilisateur de niveau 1 et 2, en proximité et à distance
- Déploiement, configuration et maintenance des postes de travail (physiques ou virtuels)
- Gestion des équipements réseaux : switchs, VLAN[5]s, bornes Wifi, câblage RJ45
- Déploiement automatisé via MDT et Microsoft Intune
- Installation et paramétrage des logiciels, en respectant les contraintes de licences
- Administration du parc informatique : suivi, documentation, traçabilité des interventions
- Maintenance préventive et reconditionnement de matériel

Mon environnement de travail inclut : Windows 10/11, Active Directory, MDT, Intune, Proxmox, et divers outils de ticketing. J'interviens aussi bien sur site client que depuis le centre de services.

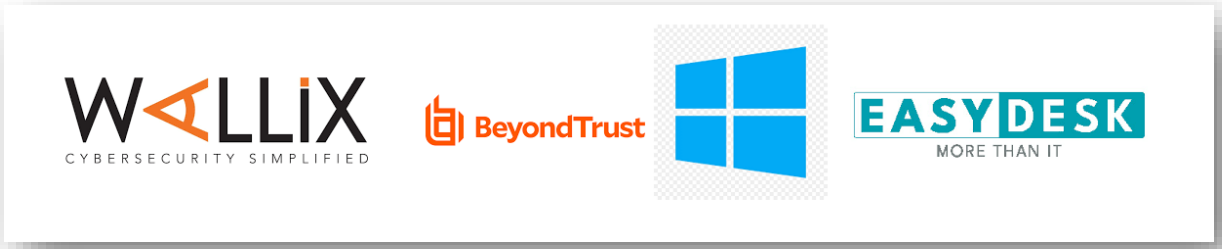
[5] Virtual Local Area Network

## Outils et environnements techniques utilisés

Dans le cadre de mon alternance, j'évolue dans un environnement technique hybride, combinant des infrastructures physiques et virtualisées. J'utilise :

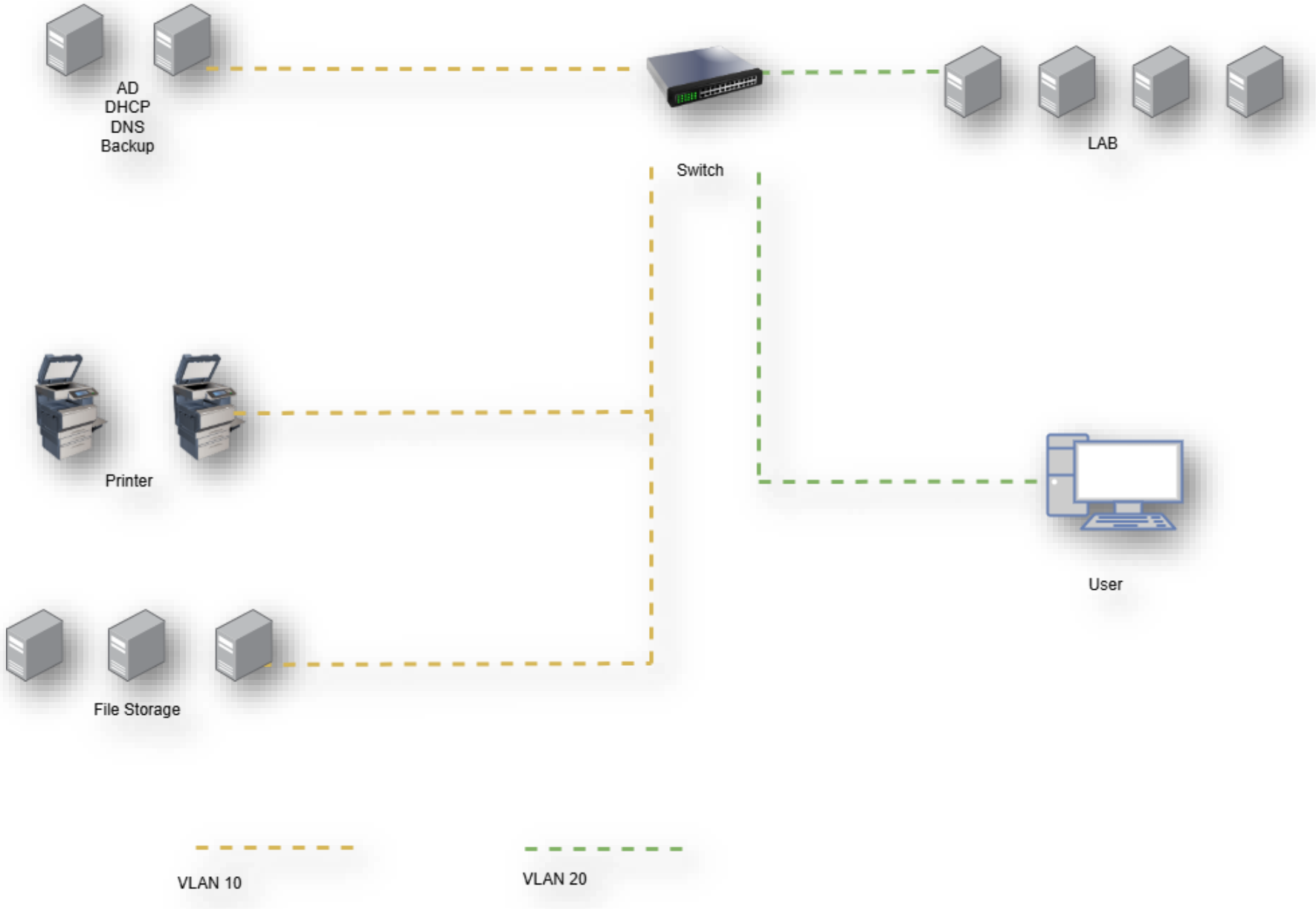
- BeyondTrust Remote Support pour la prise en main à distance
- Wallix Access Manager pour accéder aux machines virtuelles des serveurs.
- MDT avec WDS[6], ce qui me permet de gérer efficacement l'installation des systèmes d'exploitation.
- Je travaille dans des environnements basés sur Windows Server 2022 et Windows 11, en lien avec des infrastructures multisites et virtualisées.
- La gestion du parc et des interventions utilisateurs est centralisée à l'aide d'EasyDesk
- Microsoft Intune me permet de gérer à distance les postes clients, de déployer des configurations et de renforcer la sécurité des terminaux.

L'ensemble de ces outils me permet d'assurer l'administration, le support et la sécurisation du système d'information de manière rigoureuse et organisée.




[6] Windows Deployment Services

## Schéma simplifié du SI



# Mission 1 – Problème d'imprimante réseau

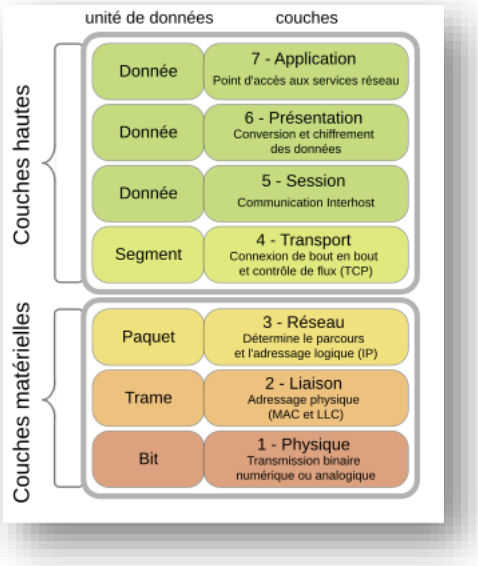
## Contexte de l'intervention

Dans le cadre de ma mission au sein de l'équipe support utilisateur chez Econocom pour le client Bonduelle, j'étais chargé du traitement des incidents de niveau 0 à 1. Les demandes étaient centralisées via la plateforme de ticketing EasyDesk, sur laquelle les utilisateurs ouvraient leurs tickets. Mon rôle consistait ensuite à analyser la demande, contacter l'utilisateur et résoudre l'incident dans les meilleurs délais, tout en respectant les procédures internes et les SLA définis.

Pour les interventions à distance, j'utilisais BeyondTrust Remote Support pour prendre la main sur les postes utilisateurs, et Wallix Access Manager pour accéder aux VM[7] hébergeant les serveurs d'impression. La traçabilité de chaque intervention était assurée par la rédaction de rapports et l'ajout de captures d'écran dans les tickets.

L'incident en question concerne une imprimante réseau qui ne répondait plus aux requêtes d'impression. L'utilisateur avait précisé dans son ticket que l'imprimante n'imprimait plus aucun document, sans qu'aucun message d'erreur ne soit affiché à l'écran.

Ce genre de problème peut avoir des origines multiples, allant d'un défaut matériel à un blocage logiciel, en passant par une erreur réseau. J'ai donc adopté une démarche structurée, inspirée du modèle OSI[8], afin d'isoler l'origine de la panne de manière méthodique, tout en restant pragmatique et orienté utilisateur.




[7] Virtual machine
[8] Open Systems Interconnection

## Mise en œuvre

Après avoir pris en charge le ticket EasyDesk, j'ai contacté l'utilisateur par téléphone. L'objectif à ce stade était de :

Vérifier s'il s'agissait d'un incident isolé ou global

Récupérer les informations essentielles : modèle de l'imprimante, emplacement, adresse IP[9]

Confirmer l'absence de message d'erreur à l'écran ou sur l'imprimante elle-même

Dès le début, l'hypothèse d'un problème logiciel ou réseau semblait plausible. Voici les étapes techniques que j'ai mises en œuvre.

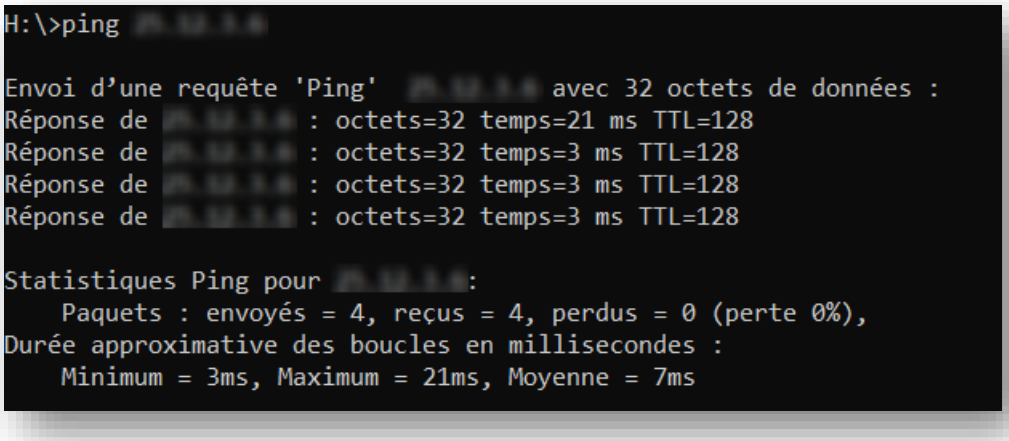
1. Vérification physique et réseau local

Je demande à l'utilisateur de débrancher puis rebrancher l'alimentation de l'imprimante. Cela permet de s'assurer que l'équipement redémarre correctement.

Je lui fais également vérifier la présence de diodes vertes sur le port Ethernet de l'imprimante. Celles-ci étant actives, je peux écarter un problème de liaison physique.

2. Tests de connectivité IP

Depuis BeyondTrust, je lance un ping de l'imprimante depuis le poste de l'utilisateur. La réponse est positive avec un temps de latence stable. Ce qui veut dire du coté client il est possible de joindre l'imprimante




[9] Internet protocol

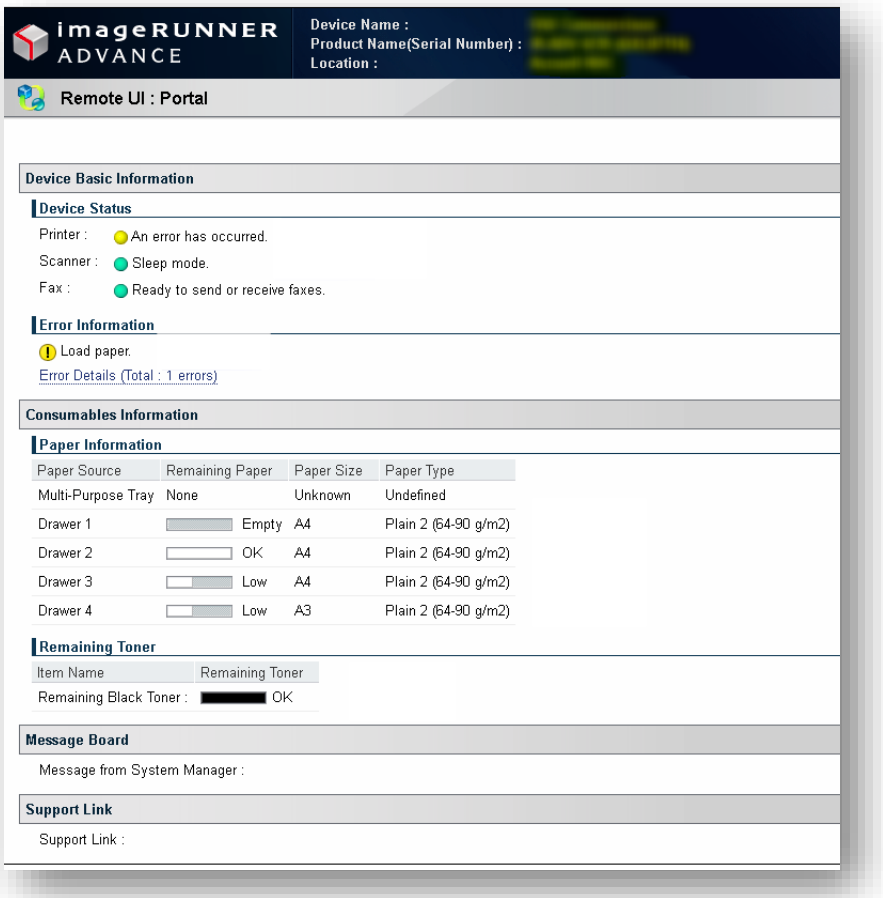
Je réplique le test depuis une VM via Wallix pour m'assurer que la connectivité est aussi bonne depuis le réseau d'administration. Là aussi, le ping est concluant. Sinon le problème serait probablement du coté du serveur d'impression.

Je note les captures de ces tests dans le ticket, ce qui me permet de valider que la couche réseau (niveau 3 OSI) est fonctionnelle.

3. Accès à l'interface web de l'imprimante

Depuis le serveur, je me connecte à l'adresse IP de l'imprimante dans Google Chrome. Cela me permet d'accéder à son interface d'administration. Celle-ci est accessible sans latence, ce qui confirme à nouveau la bonne connectivité.

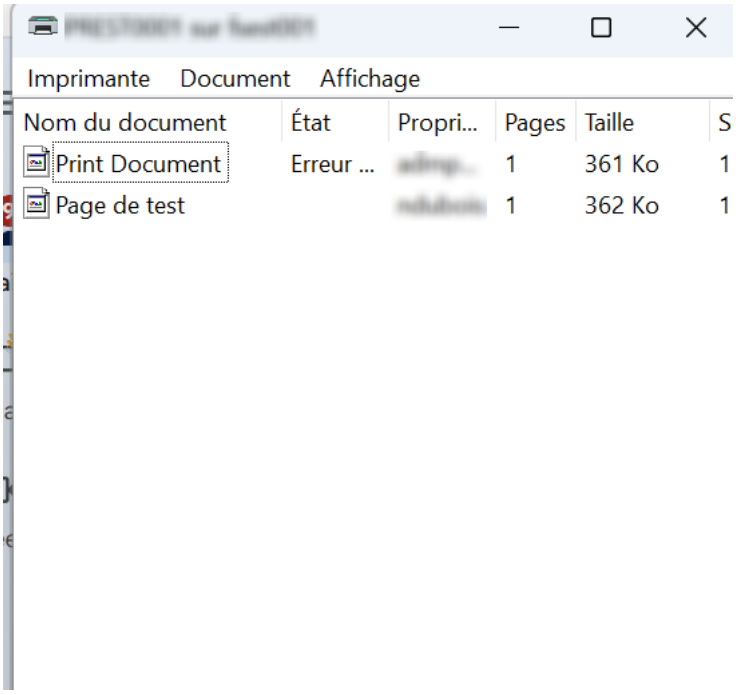
Sur la page d'accueil, je remarque immédiatement une alerte en jaune indiquant que le bac papier principal est vide. Ce détail, pourtant essentiel, n'était pas remonté à l'utilisateur. Je l'informe de la situation par téléphone et il procède au rechargement du papier.



Je relance ensuite une impression test, mais le document reste bloqué dans la file.

4. Analyse du spooler local

Depuis la session BeyondTrust, j'accède à la file d'attente d'impression locale. Plusieurs documents sont en erreur. Cela peut indiquer une corruption du spooler ou un problème de communication avec le service d'impression.




5. Redémarrage du spooler serveur

En parallèle, je me connecte via Wallix Access Manager au serveur d'impression du site. Je vérifie les services Windows actifs, en particulier spooler, et les journaux d'événement.

Par mesure de sécurité, je redémarre le service avec les commandes suivantes :

net stop spooler

net start spooler

Le service repart sans erreur. Je vérifie que l'imprimante est bien détectée par le serveur.

6. Test final

Une fois tous les éléments réinitialisés, je lance une impression test depuis le poste utilisateur. Cette fois, le document est transmis et l'impression est effectuée avec succès.

Je demande à l'utilisateur de confirmer la bonne réception du document et je clos le ticket.

7. Documentation et suivi

Mise à jour du ticket EasyDesk à chaque étape (prise en charge, contact, diagnostic, résolution)

Captures d'écran ajoutées : résultats de ping, interface imprimante, fichier d'impression relancé

Rapport d'intervention rédigé et joint

Enrichissement de la base de connaissances interne avec une fiche de procédure type "imprimante bloquée – bac vide + spooler"

## Bilan et apprentissages

Cette intervention m'a permis de consolider mes réflexes de diagnostic multi-niveaux, et surtout de ne pas m'arrêter à une hypothèse trop rapidement. Même si le bac papier vide était une cause évidente, la persistance du blocage m'a poussé à explorer plus loin, ce qui s'est révélé pertinent.

J'ai également pu manipuler de manière fluide les outils professionnels mis à disposition :

- BeyondTrust, qui offre une prise en main rapide et stable
- Wallix, indispensable pour accéder aux serveurs distants en toute sécurité

Enfin, cette mission m'a rappelé l'importance de la communication proactive : informer l'utilisateur, vulgariser les manipulations, proposer un suivi. Cela permet non seulement de résoudre un incident, mais aussi de renforcer la relation de confiance avec les utilisateurs.

# Mission 2 : Conception et mise en place d'une infrastructure réseau sécurisée et redondante

## Contexte de l'intervention

J'ai été chargé de déployer une infrastructure réseau complète dans une salle récemment aménagée pour accueillir un service interne. L'objectif était de garantir à chaque poste de travail une connectivité réseau stable et sécurisée, tout en répondant à des exigences de redondance, de sécurité physique et de facilité de maintenance.

Cette mission m'a été confiée, ainsi qu'a deux collègues qui m'ont accompagné pas à pas. Je devais prendre en compte le dimensionnement des câbles, le choix de leur agencement, la mise en place du matériel réseau, et le brassage dans la baie. L'objectif était de garantir la continuité de service pour l'ensemble des utilisateurs et d'assurer une intervention rapide en cas de panne, grâce à une nomenclature claire et une organisation rigoureuse du câblage.

L'environnement technique incluait :

Une baie 16U [10]sécurisée ;

Deux switchs Cisco 2960X configurés en stack redondant (modèle illustré ci-dessous) ;

Une double rocade RJ45 en cuivre reliant la baie murale à la salle serveur.

Cette mission s'inscrivait dans une logique de mise en place d'infrastructure robuste, évolutive et facilement maintenable, en adéquation avec les exigences métiers.

[10] Unité de hauteur : Unité de mesure standard pour la hauteur des équipements en baie (1U = 44,45 mm).

Mise en place des équipements

La pièce, d'une longueur de 9,50 mètres, nécessitait une optimisation de l'emplacement des postes de travail afin de respecter les distances de sécurité tout en maintenant une logique réseau cohérente. J'ai donc adapté le câblage en conséquence, en choisissant des longueurs adaptées (5 m, 10 m, 12 m) et en ajustant l'aménagement pour intégrer les modifications de dernière minute demandées par le client, notamment le retrait de 3 postes sur la dernière tulipe.

J'ai installé les deux switchs dans la baie 16U, configurés en stack redondant avec une boucle arrière (SW1 ↔ SW2) pour assurer la tolérance de panne. Chaque utilisateur devait avoir plusieurs connexions disponibles. Les câbles ont été posés selon la distance réelle entre les postes et la baie, avec des longueurs adaptées (5 m, 10 m, 12 m).

L'installation reposait sur une configuration en redondance, ce qui signifie que chaque utilisateur était relié à deux ports différents sur deux switchs différents, via un câblage en quinconce. Cette configuration permet de maintenir la connexion même si un switch ou un port venait à tomber. Elle garantit :

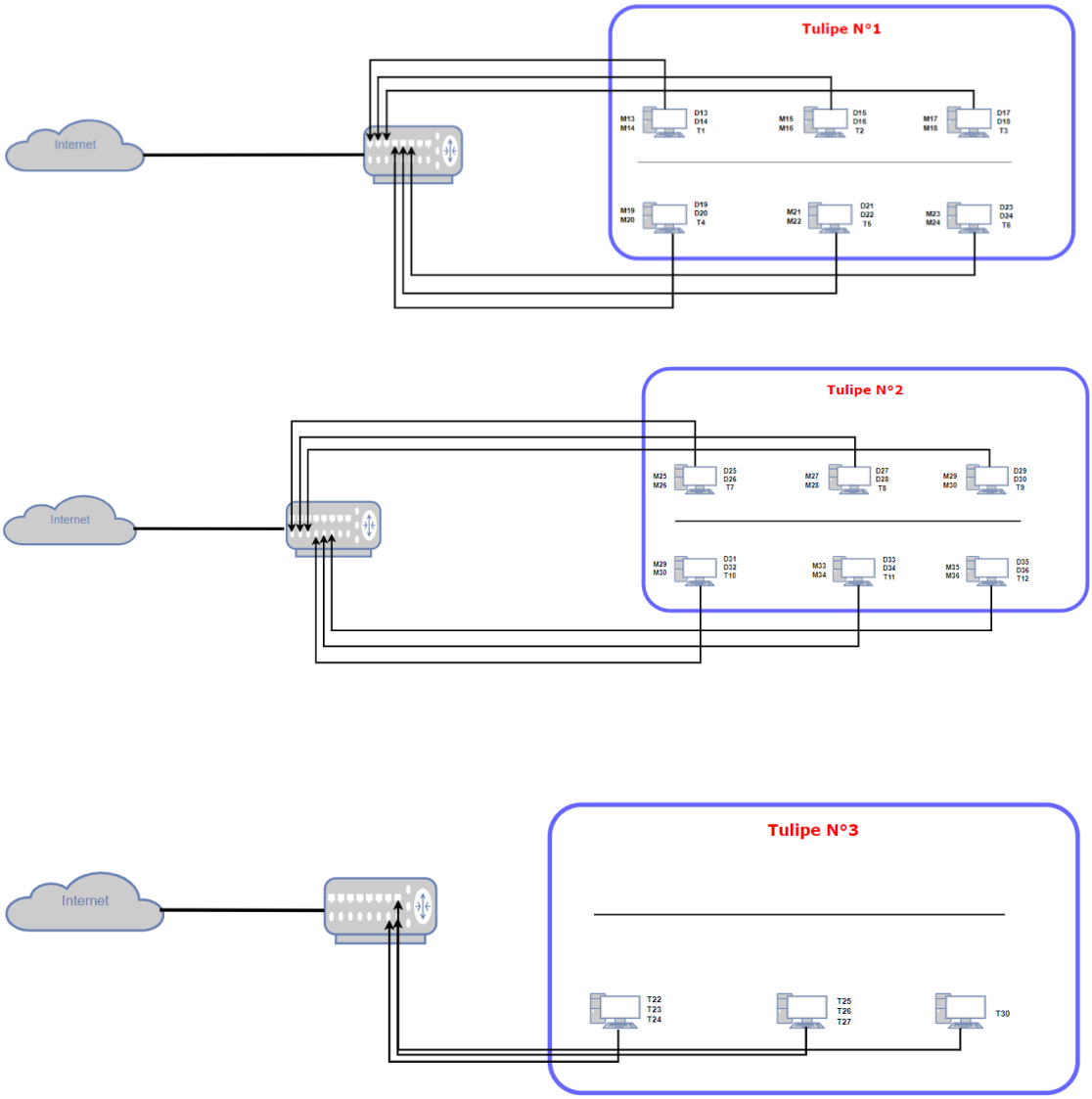
- La disponibilité du service en cas de panne d'un équipement ;
- Une répartition de la charge réseau entre les deux switchs ;
- Une continuité d'accès sans interruption visible pour les utilisateurs.

Enfin, pour garantir la lisibilité de l'installation et faciliter la maintenance, j'ai mis en place une nomenclature précise pour chaque câble :

- D pour Desktop ;
- M pour Murale ;
- T pour Client T ;

Ce système permet d'identifier rapidement les connexions en cas d'incident réseau, et de faciliter les interventions sans perte de temps.

## Schéma technique



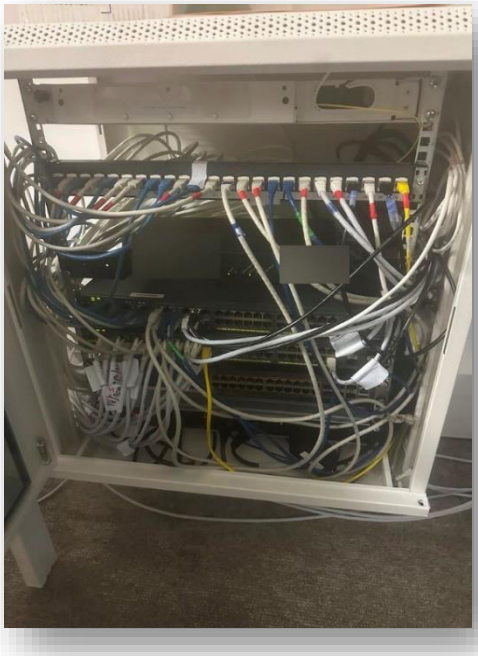
## Mise en œuvre

Étude de la salle et planification

La salle concernée mesurait 9,50 mètres de long, ce qui limitait l'aménagement à trois tulipes (îlots de 6 postes). Afin de respecter les consignes de sécurité au travail, seuls 15 postes ont été câblés, les trois derniers ayant été retirés à la demande du client. J'ai ensuite procédé à la planification du câblage, en calculant les longueurs nécessaires selon l'espacement de chaque bureau par rapport à la baie de brassage. Trois longueurs de câbles ont été utilisées : 5 m, 10 m et 12 m.

Brassage et connexion

Chaque tulipe[11] était reliée au stack de switchs via des connexions en quinconce. Cette disposition permet de maintenir la connectivité pour les utilisateurs même en cas de défaillance partielle d'un lien réseau ou d'un port.



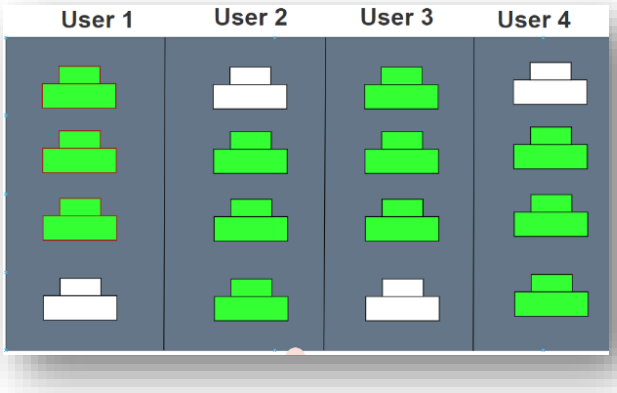



*Image 1. Brassage effectué dans la baie 1*

*Schéma 1. disposition des ports 1*

[11] Ilot de postes de travail

Sur la troisième tulipe, seuls trois utilisateurs ont été câblés au lieu de six, conformément aux consignes du client. Deux utilisateurs ont bénéficié d'une redondance, tandis que le troisième a été raccordé via un seul port réseau.

Une fois l'installation terminée, j'ai procédé aux tests de connectivité sur chaque prise à l'aide d'un ordinateur portable connecté au réseau. J'ai utilité la commande *ping -t XXX.XXX.XXX.XXX* afin de vérifier que tout fonctionnait correctement.

Après vérification je fais vérifier par mon tuteur le cablâge afin de clôturer ma mission.

## Bilan et apprentissages

Cette mission m'a permis de mettre en pratique plusieurs compétences liées au bloc 1 du référentiel TSRS, notamment : la planification du câblage, l'installation physique du réseau, le brassage, la gestion de la redondance, ainsi que le respect des normes de sécurité.

Au cours de cette mission, j'ai été confronté à plusieurs défis techniques et organisationnels. L'optimisation de l'espace a représenté une première difficulté : l'agencement de la salle m'a contraint à recalculer les distances entre les postes et la baie, et à adapter les longueurs de câbles en conséquence. Il s'agissait d'éviter toute tension ou surplus inutilisable, ce qui aurait pu nuire à la lisibilité et à la maintenance de l'installation. J'ai également dû faire face à des changements de dernière minute, notamment le retrait de certains postes de travail sur demande du client. Cette évolution m'a obligé à ajuster rapidement le plan de câblage initial.

Ces contraintes m'ont permis de tirer plusieurs enseignements concrets. J'ai compris l'importance d'une préparation en amont, en incluant la réalisation de plans, le choix de longueurs de câbles adaptées et l'anticipation des imprévus. J'ai aussi pu mesurer l'efficacité d'une nomenclature rigoureuse dans la gestion et la maintenance du réseau : un repérage câble facilité les interventions ultérieures. Enfin, la mise en place d'une infrastructure redondante, que je n'avais encore jamais réalisée, m'a permis de mieux appréhender les enjeux de continuité de service des équipements réseau.

# Mission 3 : Mise à jour de la base de données de procédures

## Contexte de l'intervention

Au sein de l'équipe Helpdesk en charge du SPOC[12] Bonduelle, nous utilisons une base de données interne de procédures qui nous guide dans le traitement des demandes utilisateurs. Cette base, construite il y a près de 8 ans, n'avait jamais été revue dans sa globalité. Mon objectif dans cette mission était d'identifier les procédures obsolètes, manquantes ou imprécises afin de les mettre à jour ou de les faire valider auprès des équipes concernées.

## Mise en œuvre

Extraction des tickets

J'ai commencé par extraire l'ensemble des tickets enregistrés entre janvier 2023 et janvier 2024 depuis notre outil de ticketing EasyDesk. Cette extraction, réalisée au format CSV, m'a permis d'obtenir une vue d'ensemble des demandes traitées pendant l'année. J'ai importé ces données dans Excel afin de les trier plus facilement.

Filtrage par EC

À partir du fichier CSV[13], j'ai filtré les tickets par EC[14] afin de ne garder qu'un seul ticket représentatif par EC. Cette méthode m'a permis d'éviter la redondance tout en conservant une vision claire des problématiques associées. J'ai ainsi identifié 114 EC différentes à comparer avec les 103 procédures disponibles dans la base EasyDesk.

Vérification de la pertinence des procédures

Pour chaque EC, j'ai vérifié si elle faisait toujours partie du périmètre du support Helpdesk. Lorsqu'elle était toujours en charge, j'ai analysé la procédure associée pour voir si elle était toujours applicable.

[12] Single point of contact
[13] Format de fichier texte permettant de stocker des données tabulaires séparées par des virgules.
[14] Entité de Contact

C’est à cette étape que j’ai repéré plusieurs procédures obsolètes. Par exemple, certaines expliquaient encore comment effectuer un reset de mot de passe via Active Directory. Or, Bonduelle migre progressivement vers une gestion centralisée des identités avec Entra ID. La procédure a donc dû être mise à jour pour refléter ce changement d’environnement.

Rédaction et validation des modifications

Lorsqu’une procédure nécessitait une mise à jour, je rédigeais une nouvelle version au format Word. Je la transmettais ensuite à l’administrateur EasyDesk, qui en assurait la validation en concertation avec les responsables des services concernés. Je n’ai pas supprimé d’EC, mais toutes les modifications ont été soumises à validation avant publication.

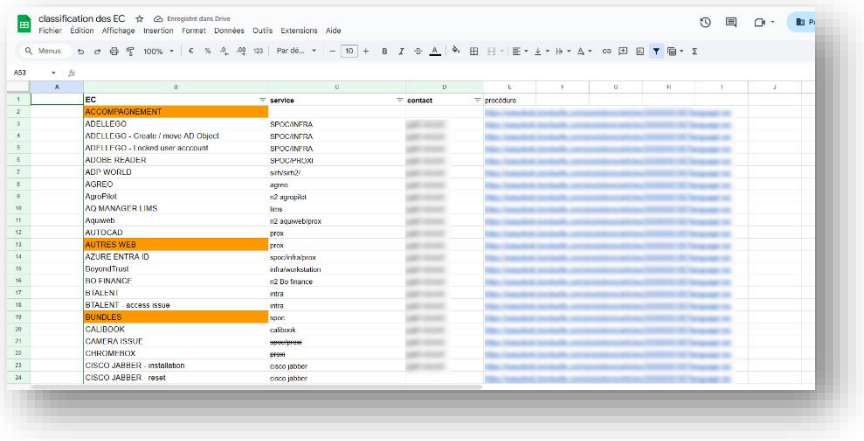
Je n’ai pas eu à créer de procédures pour Bonduelle spécifiquement, mais j’ai été amené à en rédiger pour d’autres services. Cela m’a permis de renforcer mes compétences en rédaction technique.

Pour savoir si la procédure était correct je la faisait réaliser par un collègue administrateur ainsi qu’a un autre alternant afin de voir si elle pouvait être comprise par tout le monde dans l’équipe, j’appliquais les conseils lorsque certaines choses n’étaient pas claires.

Mise en place d’un tableau de suivi

Pour organiser mon travail, j’ai mis en place un tableau de suivi contenant plusieurs colonnes : nom de l’EC, service en charge, contact technique, présence d’une procédure. Ce tableau m’a permis de garder une vue d’ensemble des actions menées,

de savoir quelles EC relevaient toujours de notre périmètre, et de faciliter la communication avec les interlocuteurs techniques.




## Bilan et apprentissages

Cette mission m'a permis de mesurer l'importance d'une documentation à jour dans un environnement de support. Une procédure claire améliore la qualité du service, accélère la résolution des incidents et facilite l'intégration des nouveaux arrivants.

J'ai également développé ma capacité à échanger efficacement avec des interlocuteurs variés, à structurer mes tâches dans le temps, et à rédiger des procédures compréhensibles même par des personnes non techniques. Ce travail m'a aussi fait prendre conscience de l'importance de l'organisation dans une mission longue et peu technique.

Même si cette mission n'était pas ma préférée en termes de contenu, car très chronophage et exigeant un gros travail rédactionnel, elle m'a permis d'acquérir des compétences essentielles en communication, rigueur documentaire et gestion de projet transversal.

Bonduelle ayant une base de données pour ses solutions it depuis plus de 10 ans mon objectif était de regarder les procédures concernant l'helpdesk et de voir celles qui étaient daté et de les mettre à jour ou les supprimer si elles n'étaient plus appliquées

# Mission 4 : Configuration d’un switch manageable HP – Mise en place de VLANs et d’une redondance réseau

## Contexte de l’intervention

Pour répondre à un besoin de l’équipe workstation chez Econocom, j’ai été amené à configurer un switch HP manageable afin de séparer deux environnements réseau : d’un côté, le réseau utilisé pour Proxmox (qui regroupe l’AD, les imprimantes, le stockage, etc.) et de l’autre, un réseau destiné à des tests internes.

L’objectif était de mieux organiser le trafic réseau, d’éviter les interférences entre les flux, et permettre une meilleure gestion des équipements.

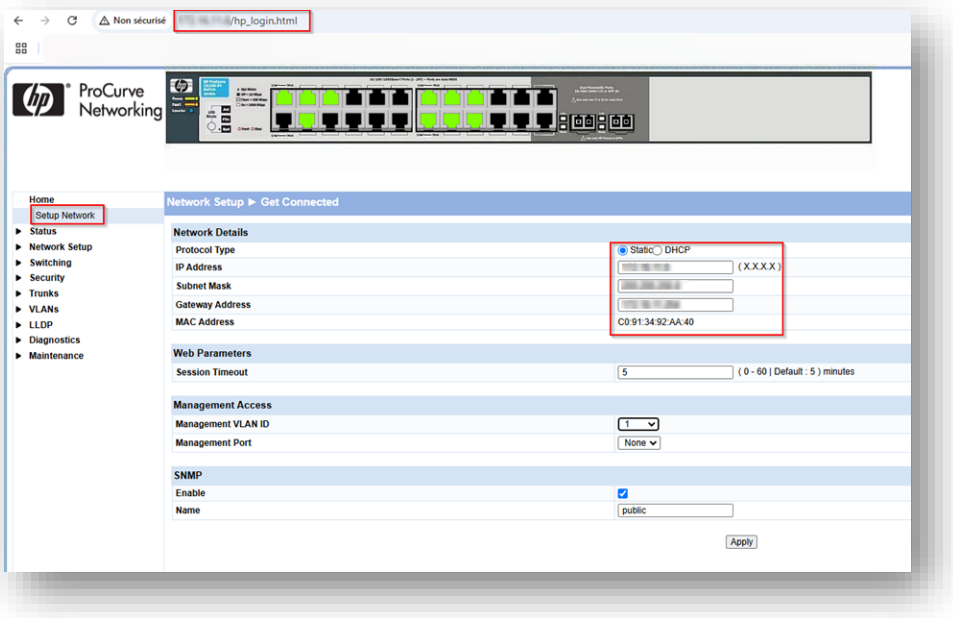
## Mise en œuvre

1. Accès au switch et configuration réseau de base

La première étape a été de remettre le switch HP 1810-24G à zéro, pour repartir sur une base propre. Une fois le reset effectué, je me suis connecté à l'interface d'administration via l'adresse IP par défaut du switch (*192.168.2.10*), en configurant manuellement l'IP de mon poste dans cette même plage (*192.168.2.x*).

Après authentification, j'ai changé l'IP de gestion du switch pour qu'elle soit compatible avec le plan d'adressage interne de l'entreprise, comme me la demander l'admin réseau qui était en charge du service.

J'ai donc renseigné l'adresse de la passerelle qui pointait vers le pare-feu. Cette configuration permettait une gestion centralisée et un accès distant sécurisé au switch.



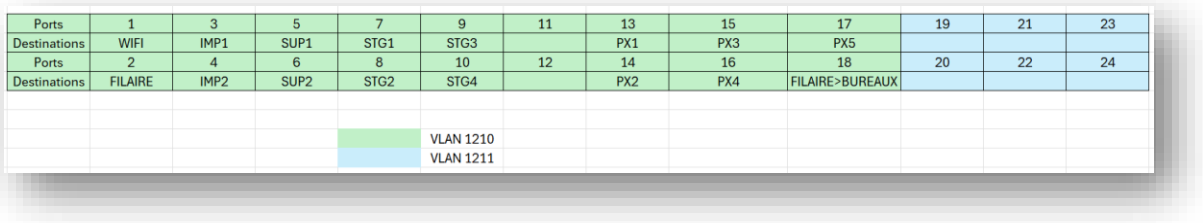
2. Création et configuration des VLANs

L'objectif était de segmenter le réseau en deux VLANs bien distincts :

- Le VLAN 10, destiné à l'environnement Proxmox (*stockage, AD, imprimantes, etc.*)
- Le VLAN 20, réservé aux tests

Depuis l'interface web, je suis allé dans les menus "VLAN Management" > "Create VLAN" pour ajouter les deux VLANs. Une fois les VLANs créés, j'ai affecté les ports comme suit :

- Ports 1 à 18 : affectés au VLAN 10 en mode untagged
- Ports 19 à 23 : affectés au VLAN 20, également en untagged



| Ports | 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Destinations | WIFI | IMP1 | SUP1 | STG1 | STG3 | | PX1 | PX3 | PX5 | | | |
| Ports | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 |
| Destinations | FILAIRE | IMP2 | SUP2 | STG2 | STG4 | | PX2 | PX4 | FILAIRE>BUREAUX | | | |

VLAN 1210
VLAN 1211

- Le port 24 a été configuré en trunk, pour transporter les VLANs via un seul lien physique grâce au protocole 802.1Q[15]. Ce protocole permet aux équipements compatibles de reconnaître à quel VLAN appartient chaque trame réseau.

3. Application et sauvegarde des paramètres

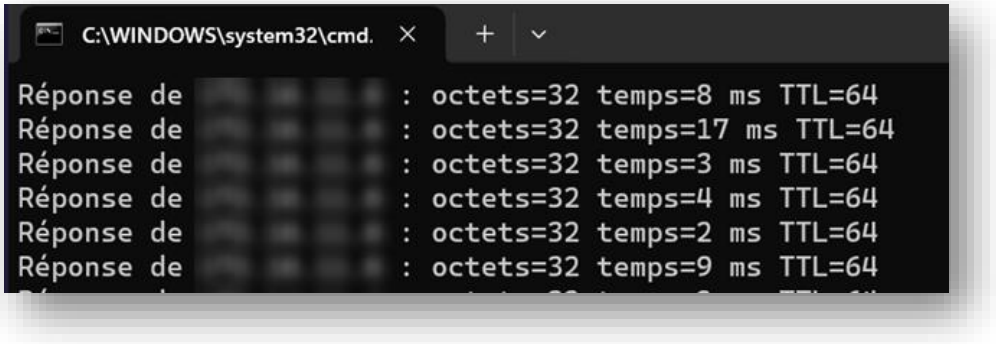
Après chaque modification, j'ai utilisé le bouton "Apply" pour l'appliquer en temps réel. Ensuite, pour éviter toute perte en cas de redémarrage, j'ai sauvegardé l'ensemble de la configuration dans la mémoire permanente du switch via "Maintenance > Save Configuration".

[15] Norme IEEE définissant le marquage des trames Ethernet pour le transport de plusieurs VLANs sur un même lien physiqu

4. Tests de validation

Pour m'assurer que la segmentation réseau fonctionnait comme prévu, j'ai mené plusieurs tests de connectivité :

Des pings entre des machines connectées sur des ports de VLANs différents, pour vérifier l'isolement (*pas de communication entre VLAN 10 et 20, comme attendu).*




Des pings entre deux postes sur le même VLAN, pour confirmer que les communications internes fonctionnaient normalement.

Un test du port trunk, connecté à un hôte Proxmox, pour vérifier la bonne réception des VLANs tagués.

Aucune ACL [16]n'a été mise en place ici : la séparation logique via les VLANs suffisait amplement.

## Bilan et apprentissages

Cette mission m'a permis de renforcer mes compétences en administration réseau, en particulier sur la gestion des VLANs, l'usage du tagging 802.1Q, la configuration de trunk, et la segmentation du trafic. J'ai pu intervenir sur un switch en conditions réelles, en comprenant les enjeux concrets de disponibilité, d'organisation du réseau et de sécurité.

[16] Access Control List

# Mission 5 – Vérification de matériel, inventaire et montage d'un PC à partir de composants récupérés

## Contexte de l'intervention

On m'a confié la réalisation d'un poste informatique destiné à servir de machine de test. La configuration souhaitée était précise : 16 Go de RAM, deux disques durs de 1 To en RAID matériel, un SSD pour l'OS et une carte graphique. J'ai mené cette mission en autonomie, avec pour seule consigne de récupérer les composants nécessaires à partir du stock de Workstation disponibles.

En parallèle, on m'a demandé de réaliser un inventaire complet du stock dont le contenu n'était pas clairement identifié via un classeur Excel. L'objectif était donc double : monter un poste fonctionnel pouvant supporter la charge d'un serveur MDT et de VM de test ainsi que recenser les composants utilisables ou défectueux présents dans les différentes machines.

## Mise en œuvre

1. Analyse du stock

J'ai commencé par analyser le contenu des Workstation disponibles dans notre salle de stockage, la salle contient tout le matériel informatique du bâtiment, cela va des câble au casque ainsi qu'au écran, mais ce que je ne devais me concentrer que sur les tours Workstation suivante : HP Z400 et HP Z420. Certaines machines disposaient de composants plus intéressants que d'autres, notamment en termes de quantité de RAM, de type de disque ou de présence de carte graphique. Cela m'a conduit à démonter plusieurs unités afin d'identifier les composants réutilisables.

2. Vérification des composants

Lors de cette phase, j'ai vérifié manuellement les modules de RAM en notant leur nombre et leur capacité (2 Go, 4 Go, 8 Go). J'ai également examiné les disques durs pour identifier leur capacité, leur type (HDD Green, Blue ou SSD) et leur état général. La présence ou non de carte graphique a aussi été systématiquement relevée. Enfin, j'ai identifié les modèles de machines pour mieux gérer les compatibilités matérielles.

Toutes ces vérifications ont été effectuées sans outil logiciel, uniquement par observation et test direct lors du montage.

3. Fusion des composants et assemblage

Une fois les composants identifiés, j'ai procédé à l'assemblage en récupérant les meilleurs éléments disponibles sur plusieurs machines. J'ai fusionné les pièces afin de constituer une configuration conforme à la demande. Le poste final comportait 16 Go de RAM, deux disques durs de 1 To montés en RAID matériel, un SSD pour le système d'exploitation, et une carte graphique dédiée. Le tout a été monté dans une seule machine stable et fonctionnelle.

4. Tests de validation des composants

Une fois le poste assemblé, j'ai procédé à une série de tests pour m'assurer de la fiabilité des composants récupérés. Pour vérifier la stabilité de la mémoire vive, j'ai utilisé Windows Memory Diagnostic, ce qui m'a permis de détecter d'éventuelles erreurs de fonctionnement sur les barrettes de RAM. Aucun problème n'a été relevé à l'issue du test.

Concernant les disques durs, j'ai utilisé l'outil CrystalDiskInfo afin d'obtenir un état SMART[17] détaillé de chacun d'eux. Les deux disques de 1 To ont été analysés, et bien qu'ils présentaient des heures de fonctionnement relativement élevées, aucun secteur défectueux ni alerte critique n'a été signalé. Le SSD a également été vérifié de la même manière.

Enfin, pour valider la mise en place du RAID matériel, je suis passé par l'interface BIOS[18] RAID. J'y ai contrôlé la bonne détection des deux disques en RAID 1 ainsi que le statut du volume, qui indiquait une synchronisation réussie et un fonctionnement normal. Cela m'a permis de m'assurer que la machine répondait bien aux spécifications initiales et qu'elle était prête à être utilisée pour les tests de masterisation.

5. Objectif de la machine

[17] Self-Monitoring, Analysis and Reporting Technology
[18] Basic Input/Output System

La machine ainsi montée a été remise à un collègue pour servir de support à des tests de déploiement de master. L'objectif était de vérifier si la configuration en RAID matériel était compatible avec les outils de déploiement utilisés, notamment dans le cadre d'un usage quotidien en entreprise.

6. Documentation et suivi

Pour organiser le travail et suivre l'état des composants, j'ai créé un fichier Excel d'inventaire. J'y ai noté les pièces récupérées, leur état, leur origine, ainsi que les éléments manquants ou inutilisables. Cette démarche a permis de clarifier le contenu du stock et d'optimiser l'utilisation des ressources disponibles. Les seuls composants jetés ont été des câbles SATA[19] endommagés ou arrachés.

## Bilan et apprentissages

Cette mission m'a permis de renforcer mes compétences en organisation, en diagnostic matériel, et en réutilisation de composants dans une logique d'économie et d'écoconception. J'ai appris à trier efficacement des pièces, à monter une machine en partant de rien, et à travailler en autonomie en respectant un cahier des charges précis. Cela m'a également permis de mieux comprendre l'intérêt de maintenir un inventaire clair et à jour, notamment lorsqu'il s'agit de valoriser du matériel existant.

[19] Serial Advanced Technology Attachment

# Mission 6 – Mise en place d'un serveur MDT/WDS et création d'un deployement share

## Contexte de l'intervention

Un environnement de lab m'a été mis à disposition afin de développer mes compétences en toute autonomie, sans impacter l'infrastructure de production. Pour cela, mon équipe m'a fourni une workstation HP Z420 ainsi qu'un Dell Latitude 3540 destiné à être masterisé

L'objectif de cette mission était de mettre en place un serveur Microsoft Deployment Toolkit (MDT) associé à Windows Deployment Services (WDS), afin de pouvoir déployer Windows 11 23H2, intégrer les drivers spécifiques du Latitude 3540, et automatiser l'installation de plusieurs applications de base. Ce projet s'inscrivait dans une démarche d'apprentissage du déploiement d'images systèmes à destination d'un parc informatique.

## Mise en œuvre

Étape 1 : Installation et préparation de l'environnement serveur

La première phase de cette mission a consisté à installer Windows Server 2022 sur la workstation Z420. Après l'installation du système, j'ai ajouté les rôles nécessaires, notamment Windows Deployment Services (WDS), et installé Microsoft Deployment Toolkit (MDT) ainsi que ses composants complémentaires, à savoir Windows ADK [20]et le module WinPE[21].

Très rapidement, j'ai été confronté à une difficulté technique : le service WDS ne démarrait pas correctement. Après avoir consulté les journaux d'événements et effectué plusieurs recherches, j'ai identifié un problème de compatibilité avec la version du rôle installée. J'ai donc désinstallé WDS puis installé une version antérieure, ce qui a permis de stabiliser la plateforme et de poursuivre la configuration du serveur.

[20] Assessment and Deployment Kit
[21] Windows Preinstallation Environment

Étape 2 : Création du Deployment Share, intégration des ressources et mise en place du monitoring

Après avoir sécurisé l'environnement serveur, j'ai créé le Deployment Share dans MDT afin de centraliser toutes les ressources nécessaires au déploiement.

*Création du Deployment Share :*

Depuis Deployment Workbench, j'ai lancé la création d'un nouveau Deployment Share en le positionnant sur le disque D:\DeploymentShare, tout en désactivant autant que possible les étapes interactives pour fluidifier le processus de déploiement.

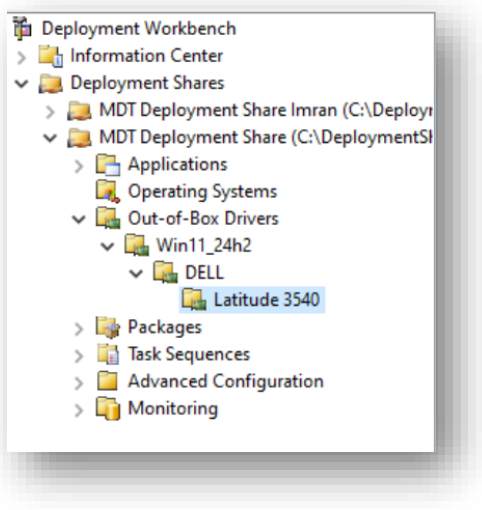
*Import de l'image système Windows 11 23H2 :*

J'ai extrait les fichiers de l'ISO[22] de Windows 11 23H2 dans un dossier temporaire. Dans MDT, à travers l'option « Import Operating System », j'ai ajouté ces fichiers comme « Full set of source files », rendant ainsi l'image exploitable pour les futures Task Sequences.

[22] International Organization for Standardization

*Organisation et import des drivers du Dell Latitude 3540 :*

J'ai téléchargé le Driver Pack complet du Latitude 3540 compatible Windows 11 depuis le site constructeur. Afin d'assurer une organisation professionnelle et évolutive, j'ai structuré les drivers dans MDT sous la forme suivante : win22h2 > dell > latitude3450. Cette hiérarchisation permet de retrouver rapidement les pilotes adaptés à chaque modèle de machine et chaque version de Windows.




*Ajout des applications à installer automatiquement :*

J'ai intégré trois applications standards :

- 7-Zip avec la commande silencieuse /S
- PDFCreator avec l'option /VERYSILENT
- Google Chrome avec les paramètres /silent /install

Chaque application a été ajoutée en utilisant l'option « Application with source files » dans MDT.

Validation du Deployment Share :Après l'importation de l'ensemble des ressources, j'ai mis à jour le Deployment Share et généré les images de démarrage LiteTouchPE, en veillant à intégrer les drivers réseau nécessaires pour le démarrage en PXE[23].

[23] Preboot Execution Environment

Mise en place du monitoring MDT :

J’ai démarré le service « Microsoft Deployment Toolkit Monitor Service » et ouvert le port TCP 9800 dans le pare-feu Windows.

Ce port est utilisé par défaut par MDT pour permettre la communication entre le serveur et les postes clients pendant le déploiement. Il a été choisi par Microsoft car il est rarement utilisé par d’autres services, ce qui évite les conflits et facilite le filtrage dans un environnement sécurisé.

Grâce à cette configuration, j’ai pu visualiser depuis la console MDT l’état d’avancement des déploiements, identifier les machines actives et détecter rapidement d’éventuelles erreurs, apportant ainsi un suivi industrialisé et professionnel au processus.

Étape 3 : Conception de la Task Sequence

Après la mise en place du Deployment Share, j’ai créé une Task Sequence dans MDT. J’ai configuré cette séquence pour automatiser l’ensemble du processus de déploiement, en commençant par le formatage du disque dur de la machine, suivi de l’installation de Windows 11 23H2.

La Task Sequence incluait également l’installation automatique des drivers du Latitude 3540 en fonction de l’identification du modèle, ainsi que l’installation silencieuse des applications importées précédemment. Chaque étape a été soigneusement validée afin d’assurer un déploiement totalement autonome sans intervention de l’utilisateur.

Étape 4 : Mise en place du démarrage PXE

Pour automatiser totalement le déploiement sur les postes, j’ai configuré WDS pour autoriser le démarrage via PXE. J’ai veillé à ce que le serveur réponde correctement aux requêtes DHCP envoyées par les postes au boot réseau, garantissant ainsi une détection immédiate du serveur MDT au démarrage des clients.

Cela permettait au Dell Latitude 3540 de démarrer directement sur le réseau, charger l'environnement LiteTouchPE et initier le processus de déploiement automatiquement.

Étape 5 : Test de déploiement

Pour valider l'ensemble de la configuration, j'ai effectué un test complet sur le Dell Latitude 3540. Après avoir configuré l'ordre de démarrage dans le BIOS pour privilégier le réseau, le poste a bien détecté le serveur MDT via PXE.

La Task Sequence s'est déroulée sans incident : formatage du disque, installation de Windows 11, intégration des drivers, puis installation silencieuse de 7-Zip, PDFCreator et Google Chrome.

À l'issue du processus, le poste était parfaitement fonctionnel, prêt à l'utilisation et conforme aux standards de l'entreprise.

## Bilan et apprentissages

Cette mission a représenté une étape importante dans ma progression technique. Elle m'a permis de comprendre en profondeur le fonctionnement d'un environnement de déploiement automatisé à travers MDT et WDS, et d'apprendre à résoudre les problèmes techniques liés aux services et à la compatibilité logicielle.

La mise en place du monitoring m'a également sensibilisé à l'importance du suivi en temps réel pour fiabiliser et industrialiser le processus de déploiement.

Enfin, cette expérience a renforcé mon envie de continuer à me spécialiser dans l'automatisation et la gestion de parc informatique, en poursuivant mon apprentissage sur des solutions plus avancées comme MECM et Microsoft Intune.

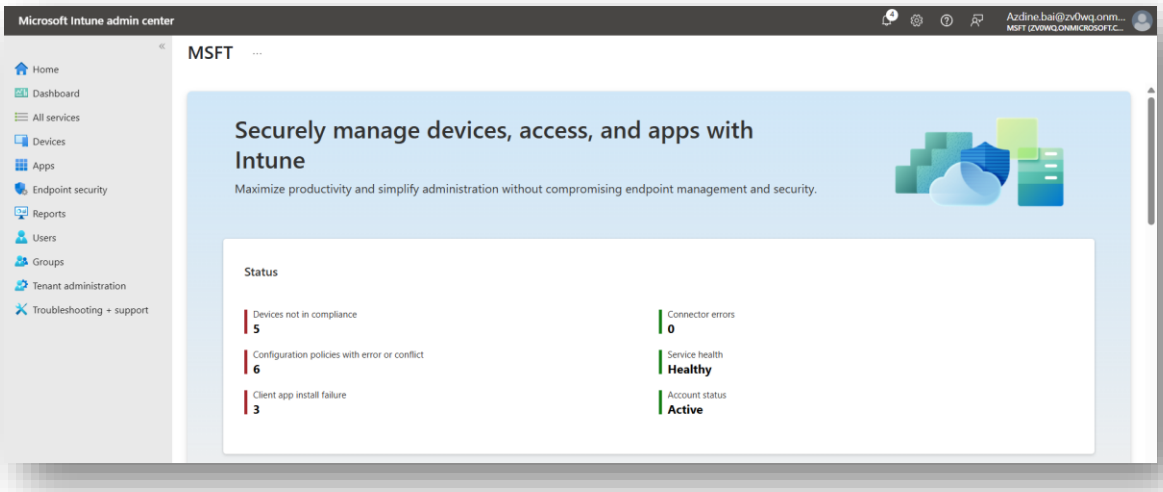
# Mission 7 - Création d’un profil de déploiement sur Intune

## Contexte de l’intervention

Lors d’un projet de renouvellement du parc informatique d’un établissement scolaire, j’ai été chargé de mettre en place une solution de déploiement automatique des postes via Microsoft Intune et Windows Autopilot. Le parc comprenait environ 300 ordinateurs sous Windows 11, répartis entre les usages pédagogiques et administratifs.

L’objectif était multiple :

- Automatiser l’enrôlement des appareils sans intervention manuelle,
- Standardiser la configuration des postes,
- Remplacer une solution obsolète basée sur MDT,
- Gagner du temps lors des déploiements de masse,
- Assurer une gestion centralisée dans une optique cloud-first.



## Mise en œuvre

Étape 1 : Création d'un groupe dynamique basé sur le Group Tag

Dans Entra ID, j'ai créé un groupe dynamique de type "Dynamic Device", destiné à recevoir automatiquement les machines enregistrées dans Autopilot avec un Group Tag spécifique.

J'ai utilisé la règle suivante :

(device.devicePhysicalIds -any (_ -eq "[OrderID]:ECOLE-INTUNE"))

Ce groupe m'a permis d'assigner automatiquement le profil de déploiement et les stratégies associées aux bons équipements dès leur importation.

Étape 2 : Création du profil ESP (Enrollment Status Page)

Via le portail Intune (Devices > Windows > Enrollment > Enrollment Status Page), j'ai créé un profil ESP (Enrollment Status Page) qui :

- Affiche à l'utilisateur la progression du déploiement,
- Permet l'installation automatique des applications obligatoires,
- Applique les paramètres de sécurité et de configuration dès le premier démarrage.
- Ce profil a été affecté au groupe dynamique précédemment créé.

Étape 3 : Création du profil de déploiement Autopilot

Toujours dans Intune (Devices > Windows > Enrollment > Deployment Profiles), j'ai ensuite créé un profil de déploiement Windows Autopilot avec les paramètres suivants :

Convert all targeted devices to Autopilot : Oui

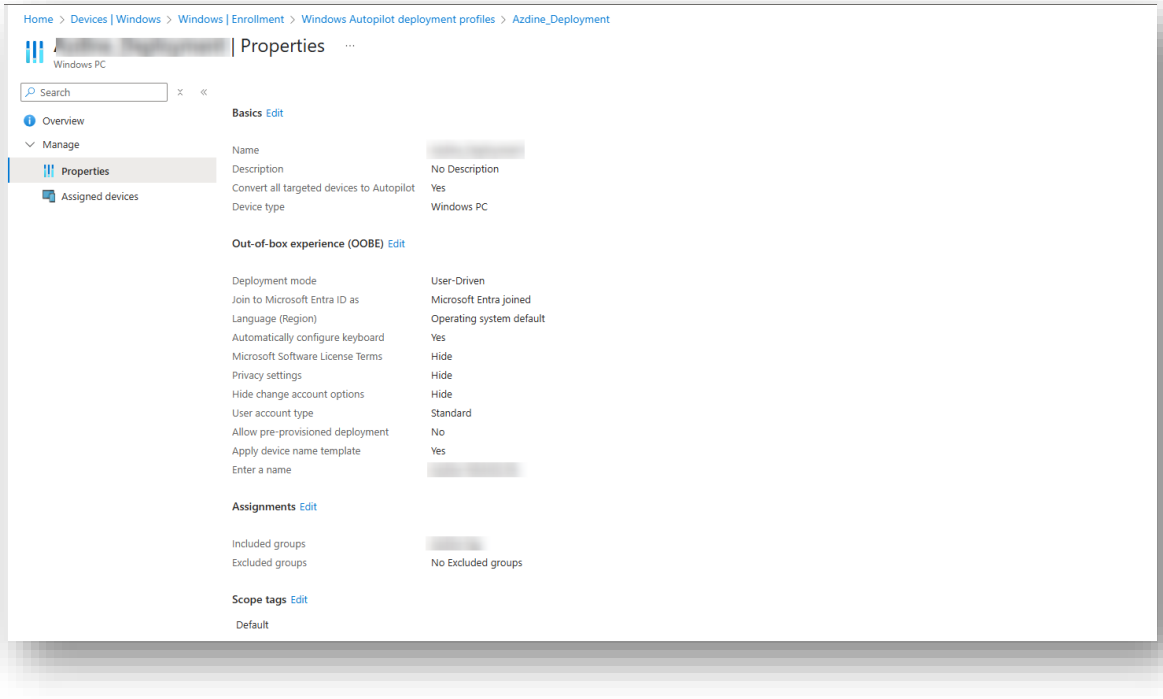
Join to Microsoft Entra ID as : Microsoft Entra joined

Allow Pre-provisioned deployment (anciennement White Glove) : No

Nom du poste : WINPC-%RAND%

Attribution automatique d’un utilisateur principal

Assignation du profil : groupe dynamique basé sur le Group Tag




Ce profil permet de configurer automatiquement les paramètres système, réseau et sécurité, tout en attribuant le poste à un utilisateur.

Étape 4 : Enregistrement manuel d’un poste dans Autopilot

Sur un poste neuf (Out Of The Box), j’ai effectué l’enrôlement dans Autopilot manuellement via PowerShell :

À l’étape de configuration de Windows, j’ai ouvert une invite de commande avec Shift + F10.

J’ai saisi Powershell pour passer en mode PowerShell.

J’ai exécuté la commande :

Set-ExecutionPolicy Bypass

Cette commande permet de désactiver temporairement la politique de restriction d’exécution des scripts PowerShell. Elle est nécessaire ici pour autoriser l’installation et l’exécution du script `Get-WindowsAutopilotInfo`, car, par défaut, Windows bloque les scripts non signés pour des raisons de sécurité.

J’ai ensuite installé le script de récupération d'identifiants matériels :

Install-Script Get-WindowsAutopilotInfo

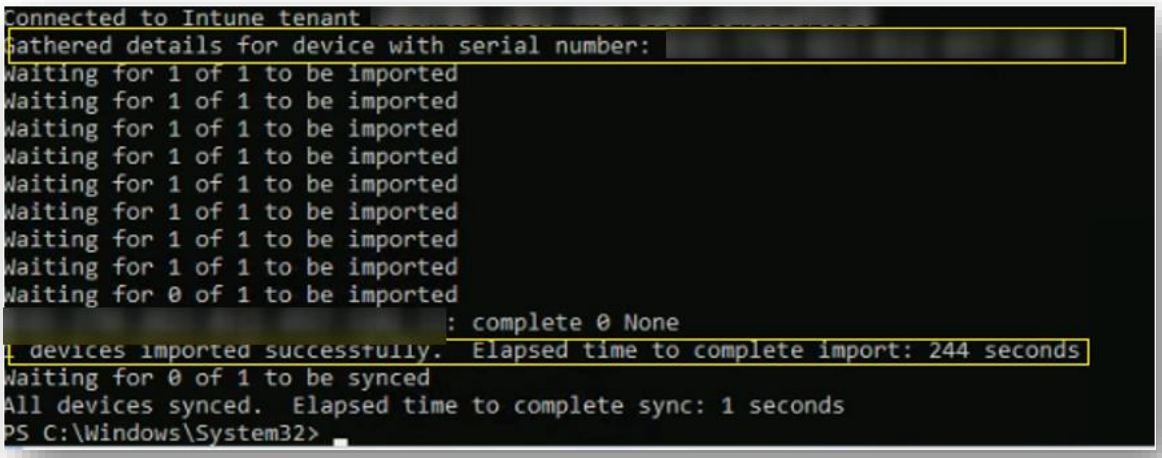
Trois lignes d’autorisation apparaissent, j’ai validé chacune en tapant O.

Enfin, j’ai lancé l’import dans Autopilot avec la commande :

Get-WindowsAutopilotInfo.ps1 -Online -GroupTag "ECOLE-INTUNE"

Une fenêtre de connexion Microsoft s’est ouverte. J’ai renseigné un compte administrateur disposant des droits d’enrôlement dans Intune.

Après connexion, un message de confirmation s’est affiché : “1 device imported successfully”




Le poste a alors été visible dans Intune, correctement associé au Group Tag et prêt à recevoir le profil de déploiement.

Étape 5 : Lancement du déploiement

Après un redémarrage du poste (shutdown /s /t 0), j’ai procédé à l’installation classique de Windows. À l’écran demandant s’il s’agit d’un usage personnel ou professionnel, j’ai choisi “Utilisation scolaire ou professionnelle”.

Le poste a alors automatiquement :

- Rejoint le tenant via Entra ID,
- Appliqué le profil de déploiement Autopilot,
- Installé les applications et paramètres de sécurité,

Enfin, la session s’est ouverte automatiquement avec l’utilisateur assigné, ce qui m’a permis de lui présenter un poste entièrement opérationnel et conforme aux attentes.

## Bilan et apprentissages

Cette mission m’a permis de :

Mettre en œuvre un déploiement cloud natif et automatisé avec Autopilot,

Utiliser Intune de manière structurée : groupe dynamique, ESP[24], profils personnalisés,

Renforcer mes compétences sur PowerShell et les outils d'enrôlement manuel,

Corriger des erreurs de syntaxe (ex. Group Tag mal interprété) en analysant et adaptant la documentation officielle.

L’enregistrement d’un poste complet, prêt à l’emploi et conforme aux politiques de sécurité, ne prend désormais plus que 20 à 30 minutes.

Cette solution apporte flexibilité, gain de temps et homogénéité sur l’ensemble du parc. Elle constitue une base solide pour le pilotage de la gestion des périphériques dans une logique moderne et centralisée.

[24] Enrollment Status Page : Interface affichée pendant le déploiement Autopilot pour suivre l’installation des applications et des paramètres de configuration.

# Mission 8 – Création de stratégies de sécurité sur Intune

## Contexte de l'intervention

Pour accompagner un client dans la modernisation de son poste de travail et la migration de son infrastructure vers Microsoft Intune, j'ai été chargé de créer et de tester différentes stratégies de sécurité. Microsoft Intune est une solution de gestion unifiée des terminaux UEM qui permet d'administrer à distance les appareils, les utilisateurs et les données d'une entreprise, tout en assurant leur conformité aux politiques de sécurité définies.

L'objectif de cette mission était de concevoir et valider plusieurs stratégies de sécurité à appliquer via Intune, dans un environnement cloud géré. Ces stratégies visent à :

• Protéger les données locales des postes de travail (BitLocker),

• Sécuriser les comptes administrateurs locaux LAPS[25],

• Maintenir un parc propre en supprimant automatiquement les appareils inactifs (nettoyage),

• Empêcher l'utilisation de périphériques de stockage amovibles (clés USB, disques externes).

Toutes les configurations ont été testées sur deux machines virtuelles, l'une sous Windows 10, l'autre sous Windows 11.

[25] Local Administrator Password Solution

## Mise en œuvre

1. Mise en place du chiffrement BitLocker

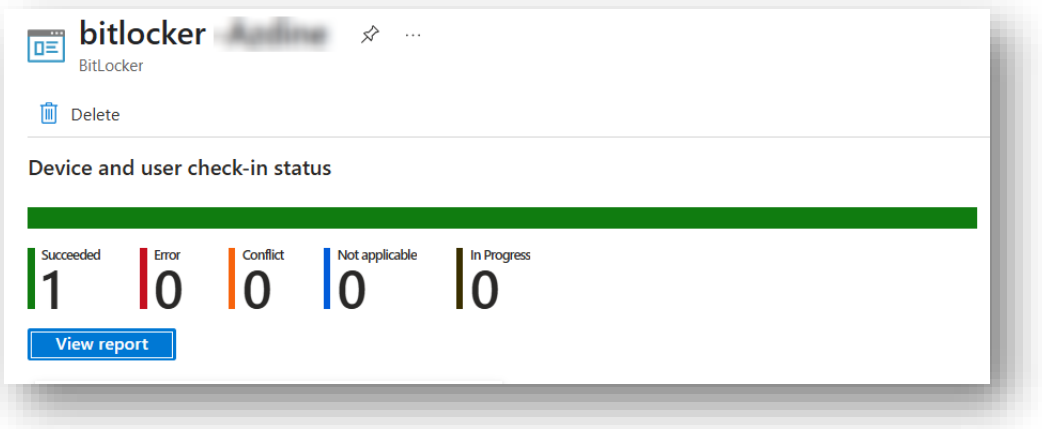
Pour sécuriser les données présentes sur les postes, j'ai commencé par déployer une stratégie de chiffrement des disques avec BitLocker, directement depuis l'interface d'administration de Microsoft Intune.

Je me suis connecté à https://endpoint.microsoft.com, puis je suis allé dans Appareils > Profils de configuration > Créer un profil. J'ai choisi la plateforme Windows 10 et ultérieur, puis le type de configuration Modèle > Endpoint Protection.

Dans la section BitLocker, j'ai configuré les paramètres suivants :

- Activation du chiffrement du disque système
- Chiffrement complet du disque dur pour protéger l'ensemble des partitions
- Exigence de la présence d'un module TPM 2.0 pour garantir la sécurité matérielle
- Sauvegarde automatique de la clé de récupération dans Azure AD.

J'ai ensuite affecté ce profil à un groupe de test constitué de deux machines virtuelles. Après synchronisation des stratégies depuis les machines, j'ai contrôlé que le chiffrement était bien actif dans la console Intune, et que les clés étaient correctement sauvegardées dans Azure. Le test s'est révélé concluant.




Cette stratégie a été testée avec succès sur mes deux machines virtuelles, en simulant le comportement attendu dans un environnement réel.

## 2. Déploiement de LAPS (Local Administrator Password Solution)

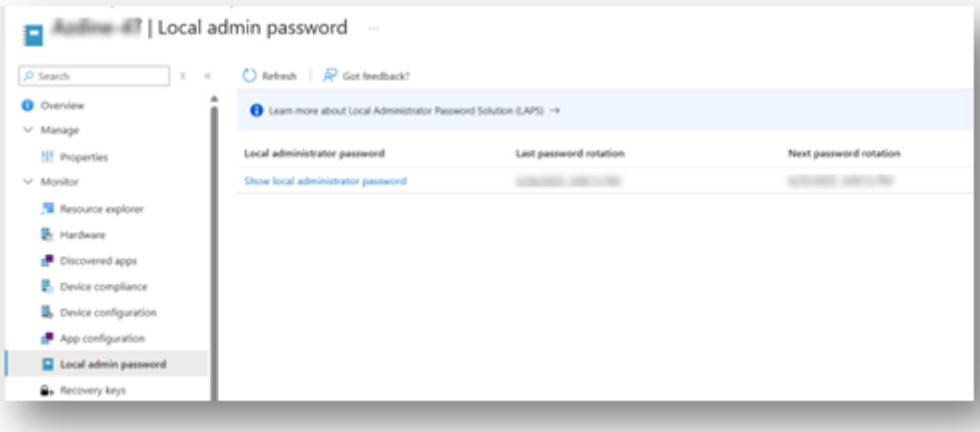
L'objectif ici était de remplacer les mots de passe fixes utilisés pour les comptes administrateurs locaux par des mots de passe uniques, sécurisés et renouvelés automatiquement. Intune permet d'utiliser Windows LAPS pour cela.

Depuis Endpoint Security > Account Protection, j'ai cliqué sur Créer une stratégie, puis sélectionné Local admin password solution (Windows LAPS).

J'ai défini les paramètres suivants :

- Activation de LAPS
- Sauvegarde automatique des mots de passe dans Azure AD
- Fréquence de renouvellement fixée à 1 jour.

Une fois la stratégie enregistrée, je l'ai appliquée à un groupe de test. Depuis la console d'administration, j'ai vérifié que les postes généraient bien un mot de passe stocké de manière sécurisée, et que seuls les administrateurs pouvaient y accéder.



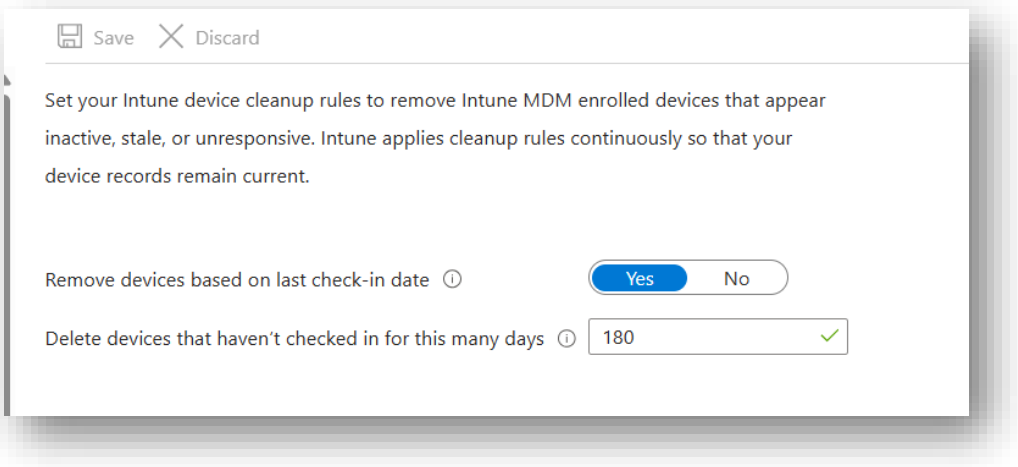

## 3. Suppression automatique des appareils inactifs

Afin d'éviter l'encombrement de l'environnement Intune avec des machines obsolètes ou non utilisées, j'ai mis en place une stratégie de nettoyage automatique.

Je me suis rendu dans le menu Appareils > Nettoyage, puis j'ai activé l'option de suppression automatique. J'ai défini un seuil d'inactivité de 180 jours, au-delà duquel

un appareil est automatiquement retiré du tenant Intune. J'ai appliqué cette règle à l'ensemble des groupes d'appareils.

Même si cette politique n'a pas encore pu être validée en situation réelle (aucun appareil n'ayant dépassé les 180 jours d'inactivité), elle est prête à être activée dès qu'un poste entre dans ce critère.




4. Blocage des périphériques de stockage amovibles (USB)

Pour empêcher l'utilisation non autorisée de périphériques de stockage externes (comme les clés USB ou disques durs externes), j'ai déployé une stratégie de restriction adaptée.

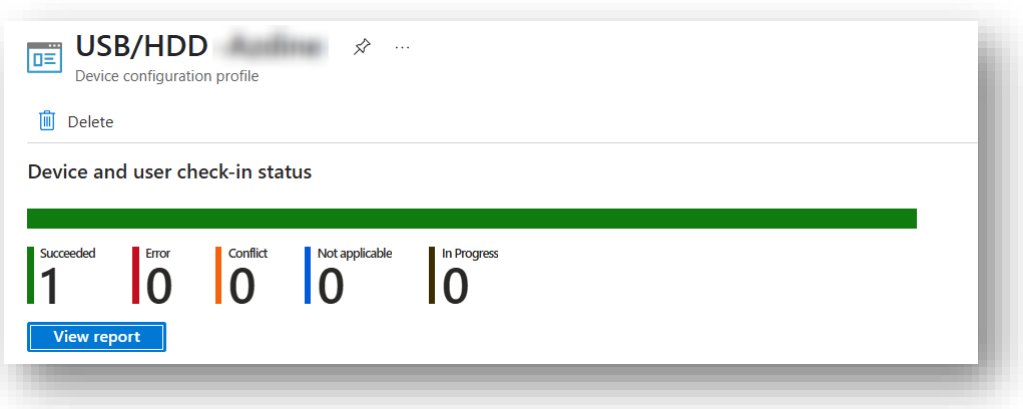
Dans Appareils > Profils de configuration > Créer un profil, j'ai sélectionné :

- Plateforme : Windows 10 et ultérieur ;
- Type : Modèle > Restrictions d'appareil.

Dans la section Stockage, j'ai désactivé l'option *"Autoriser le stockage amovible"*. Ce profil a été attribué uniquement à un groupe d'utilisateurs standards, afin de ne pas gêner les comptes administrateurs ou les utilisateurs techniques.

Pour tester la configuration, j'ai utilisé deux comptes utilisateurs issus des services marketing et administratif. J'ai connecté plusieurs types de périphériques (clé USB, disque dur externe) sur des machines virtuelles liées au groupe ciblé. Les périphériques ont été bloqués comme prévu, sans générer de messages d'erreur, ce qui confirme le bon fonctionnement de la stratégie.

Les comptes administrateurs et quelques groupes d'exception n'étaient pas concernés




## Bilan et apprentissages

Cette mission fut pour moi une étape importante dans la compréhension de la gestion de la sécurité dans un environnement cloud moderne. Elle m'a confronté à des concepts que je ne maîtrisais pas au départ, notamment la logique de déploiement dans Intune, très différente de celle de MDT que je connaissais déjà.

J'ai appris à créer des profils ciblés, à gérer la segmentation via les groupes Azure AD, à contrôler le bon déploiement des stratégies, et à tester leur application en conditions réelles. Même si le projet n'était pas encore finalisé pour une mise en production, j'ai pu en comprendre les enjeux techniques et opérationnels.

Cette mission m'a permis d'explorer plusieurs aspects de la gestion de la sécurité dans un environnement cloud, notamment le chiffrement des disques avec BitLocker, la gestion des mots de passe locaux avec LAPS, la suppression automatique des

appareils inactifs, ainsi que le blocage des périphériques USB, souvent négligé mais essentiel pour sécuriser les postes de travail.

## Difficultés rencontrées

Mon parcours vers ce métier n'a pas été linéaire. L'une des premières grandes difficultés a été de trouver une entreprise en alternance. N'étant pas issu du domaine informatique à l'origine, et ayant interrompu mes études pendant plusieurs années, j'ai dû faire face à un manque de légitimité aux yeux des recruteurs. J'ai essuyé de nombreux refus avant de pouvoir décrocher un entretien. Cette phase a été longue, parfois décourageante, mais elle m'a aussi appris la persévérance et l'importance de croire en son projet malgré les obstacles.

Une fois l'alternance commencée, j'ai dû m'adapter rapidement à un environnement technique que je découvrais. Cela a représenté une vraie remise à niveau, avec une exigence constante de compréhension et d'application concrète sur le terrain. Le décalage initial entre la théorie vue en formation et la réalité en entreprise a été parfois complexe à combler, mais chaque difficulté rencontrée a été une opportunité d'apprentissage.

## Retour personnel sur la rédaction du mémoire

La rédaction de ce mémoire a été pour moi un exercice à la fois formateur et introspectif. Il m'a permis de revenir sur deux années d'expérience, de mettre de l'ordre dans tout ce que j'ai appris, et surtout de prendre conscience de l'évolution que j'ai traversée, tant sur le plan technique que personnel.

Ce travail m'a demandé de structurer mes idées, de faire le lien entre mes missions et le métier visé, et de prendre du recul sur chaque situation vécue. J'ai également dû améliorer ma rigueur dans l'écriture, l'organisation des informations et la clarté du discours. Au-delà de l'aspect scolaire, ce mémoire représente pour moi un symbole de réussite dans une reconversion que j'ai construite pas à pas.

Il incarne la preuve que, même en venant d'un autre secteur et en reprenant les études après une pause, il est possible de trouver sa place dans un métier exigeant comme celui de technicien systèmes, réseaux et sécurité — et demain, dans la cybersécurité.

## Conclusion finale

Au terme de ces deux années d'alternance chez Econocom, cette expérience a marqué une transformation profonde dans mon parcours professionnel. Issu initialement d'un tout autre domaine, j'ai réussi à m'intégrer dans le secteur de l'informatique et à y développer des compétences techniques solides, en particulier autour des systèmes, des réseaux et de la sécurité.

Ces deux années m'ont permis de progresser étape par étape : j'ai commencé par le support utilisateur, puis évolué vers des missions plus techniques, en lien avec le déploiement de systèmes, la configuration réseau, la gestion de postes de travail et la sécurisation des environnements. Chaque mission m'a appris quelque chose de nouveau, m'a confronté à des défis concrets, et m'a poussé à monter en compétences dans des environnements professionnels réels.

Mais au-delà de l'aspect technique, cette alternance m'a aussi appris à travailler en équipe, à m'organiser, à documenter mes actions et à mieux communiquer avec les utilisateurs. Elle m'a donné confiance en moi, en mes capacités à apprendre, à m'adapter, et à devenir un professionnel à part entière dans le domaine de l'informatique.

Aujourd'hui, je me projette naturellement vers la suite : je souhaite continuer dans l'administration systèmes et réseaux, tout en me spécialisant progressivement dans la cybersécurité. C'est un domaine qui me passionne, qui correspond à mes valeurs, et qui représente pour moi une suite logique à ce que j'ai construit jusqu'à présent.

En résumé, cette alternance m'a permis non seulement de valider des compétences techniques, mais aussi de confirmer un véritable projet professionnel. Ce mémoire en est la synthèse, et je suis fier du chemin parcouru jusqu'ici.

# Remerciements

Je tiens à adresser mes plus sincères remerciements à l'entreprise Econocom, ainsi qu'à tous ses collaborateurs, pour m'avoir offert l'opportunité de vivre cette riche expérience professionnelle en tant que technicien informatique. Cette année d'alternance a été jalonnée de défis, et je n'aurais pas pu progresser autant sans le soutien indéfectible de mon équipe et de mes tuteurs.

Je souhaite exprimer ma profonde gratitude à mes tuteurs, Joël Desreumeaux et Julien Vandevelde, pour leur accompagnement tout au long de mon parcours. Leur expertise, leur pédagogie et leur disponibilité ont été des atouts précieux pour mon apprentissage. Ils m'ont non seulement transmis des compétences techniques essentielles, mais m'ont également montré ce qu'implique une posture professionnelle exemplaire. Grâce à eux, j'ai pu mieux appréhender les réalités du monde de l'entreprise et m'y intégrer efficacement.

Je tiens également à remercier mes collègues, qui ont toujours fait preuve d'un esprit d'équipe et d'un soutien bienveillant. Leur collaboration et leur patience m'ont permis de progresser rapidement et de me sentir pleinement impliqué dans les projets de l'entreprise. Leur attitude positive et leur esprit d'entraide m'ont inspiré et m'ont appris à relever les défis avec confiance et créativité.

Enfin, je souhaite également remercier chaleureusement mon école Aston IT, qui m'a offert le cadre et les outils nécessaires pour réussir cette alternance. Les enseignements dispensés par les formateurs ainsi que l'accompagnement de l'équipe administrative ont été essentiels à ma progression. Leur engagement envers leurs étudiants m'a permis de grandir et de m'épanouir dans cette voie.

# Table des sources


https://www.econocom.com/fr/nous-connaitre/groupe-econocom

https://www.econocom.com/fr

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html

https://support.hpe.com/hpesc/public/docDisplay?docId=c04541328&docLocale=en_US

https://h30434.www3.hp.com/psg/attachments/psg/Business-PC-Workstation-POS/39701/1/2013.4%20Z420%20QuickSpecs%20v17.pdf

https://learn.microsoft.com/fr-fr/intune/configmgr/mdt/

https://www.powershellgallery.com/packages/Get-WindowsAutopilotInfo/

https://learn.microsoft.com/fr-fr/intune/intune-service/