Rapport de stage

KADA Amine – BTS SIO SISR 2026

18 Mai 2026 au 24 Juin 2026

Tuteur de l'entreprise : Julien TASSE & Sylvain HENRIOT

Tuteur pédagogique : David BALNY

Entreprise d'accueil : Conseil Départemental Touraine

Établissement : Paul-Louis Courier

Remerciements

Je tiens à remercier mes maîtres de stage, Julien TASSE et Sylvain HENRIOT, pour leur encadrement tout au long de mon stage. Leur expertise a grandement contribué à mon apprentissage dans le domaine.

Sous leur supervision, j'ai pu découvrir de nouvelles perspectives et approfondir mes connaissances.

Je suis reconnaissant envers l'équipe du Conseil départemental pour sa disponibilité et sa patience. Elle a su répondre à toutes mes questions et m'orienter dans mes démarches, me permettant ainsi d'acquérir une expérience pratique enrichissante.

Enfin, je tiens à exprimer ma gratitude pour l'opportunité qui m'a été offerte de réaliser ce stage au sein de leur équipe. Cette expérience m'a permis de développer davantage mes compétences.

En conclusion, je remercie Julien TASSE et Sylvain HENRIOT pour leur confiance, leur soutien et leur accompagnement durant mon stage. Leur contribution significative a grandement enrichi mon parcours professionnel, et je leur suis reconnaissant de les avoir eus comme maîtres de stage.

Sommaire

Introduction

Au cours de l'année 2025-2026, la réalisation d'un stage en milieu professionnel est un prérequis obligatoire pour obtenir la certification du BTS SIO de la deuxième année.

Ce stage dure 5 semaines et 3 jours, soit environ 1 mois, et a pour objectif de renforcer nos connaissances en matière d'infrastructure réseaux, de services et de systèmes, tout en enrichissant notre expérience. De plus, ce stage représente un atout indéniable pour le curriculum vitae (CV), en offrant une expérience concrète du monde du travail.

Mon stage se déroule au Conseil Départemental au service collège numérique de la Touraine, dont une entité je ferai la présentation à la page suivante.

Ce rapport de stage a pour objectif de présenter plusieurs aspects du monde professionnels. Tout d'abord, une introduction à l'entreprise sera présentée, suivie d'une étude de son infrastructure réseau. Enfin, nous approfondirons les différentes missions effectuées pendant le stage. Le rapport se conclura par une brève synthèse ainsi qu'une annexe contenant les fiches de procédure qui m'ont permis de réaliser mes missions lors de ce stage.

1.1 - Présentation globale de la division

Le service informatique des collèges du Conseil départemental d'Indre-et-Loire, une collectivité territoriale chargée de la gestion et de l'organisation du département. Ce service dépend plus précisément de la direction des systèmes d'information (DSI), qui assure le bon fonctionnement des équipements et des infrastructures numériques utilisés dans les collèges du département.

Le service informatique des collèges a pour mission principale de gérer, maintenir et sécuriser les outils informatiques mis à disposition des établissements scolaires. Cela comprend notamment :

- L'installation et la maintenance des ordinateurs ;
- La gestion des réseaux informatiques et d'Internet ;
- Le support technique auprès des utilisateurs ;
- La sécurisation des données et des systèmes ;
- Le déploiement de nouveaux équipements numériques dans les collèges.

Ce service joue un rôle essentiel dans le fonctionnement quotidien des établissements scolaires, car il permet aux élèves, aux enseignants et au personnel administratif de travailler dans de bonnes conditions numériques.

Le Conseil départemental agit également dans plusieurs domaines importants tels que :

- L'éducation ;
- Les routes et transports ;
- L'action sociale ;
- La culture et le sport ;
- L'aménagement du territoire.

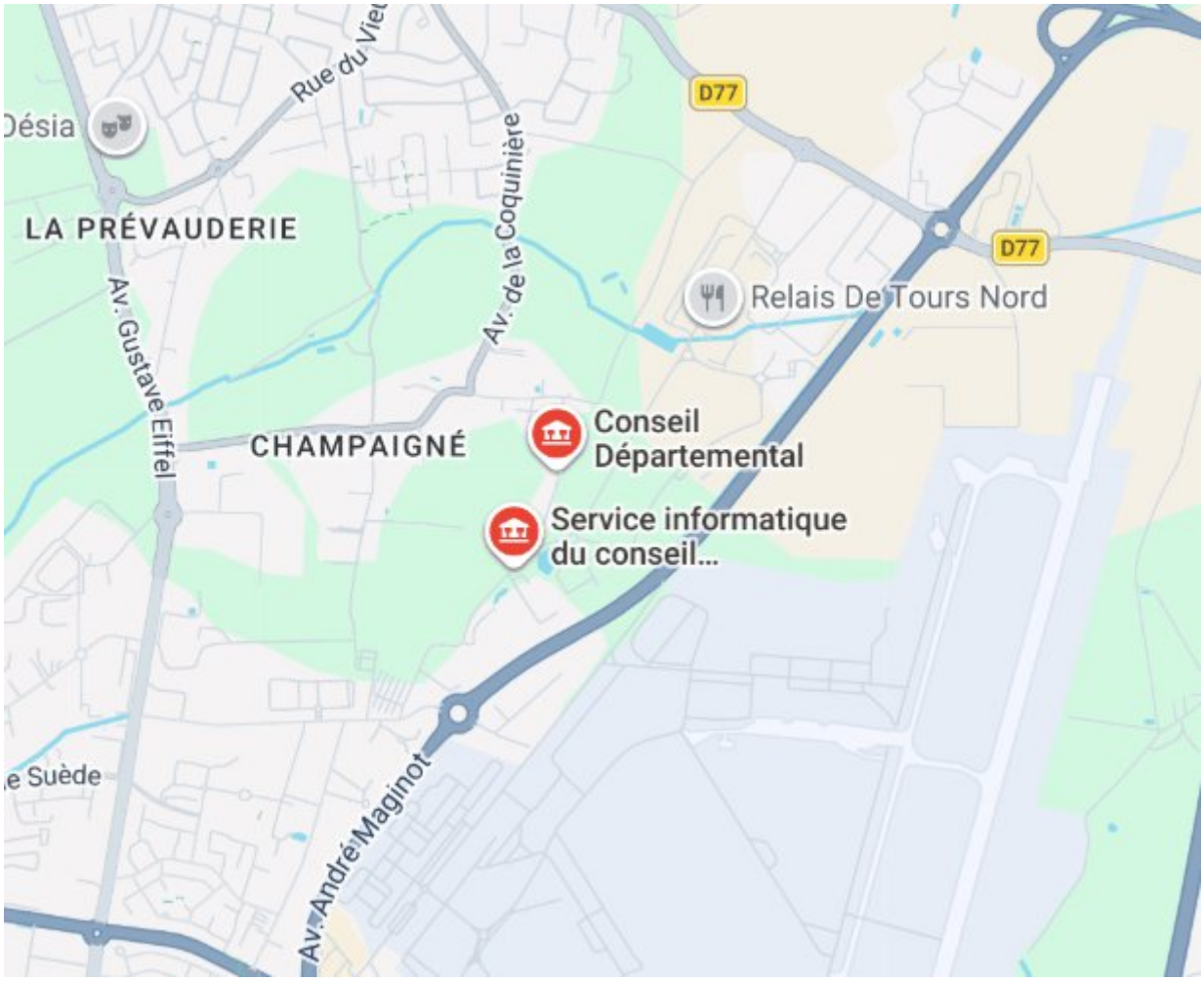
Grâce à son service informatique, le Conseil départemental participe activement à la modernisation numérique des collèges et à l'amélioration des conditions d'apprentissage des élèves.

1.2 - Situation géographique

Le service est situé au :

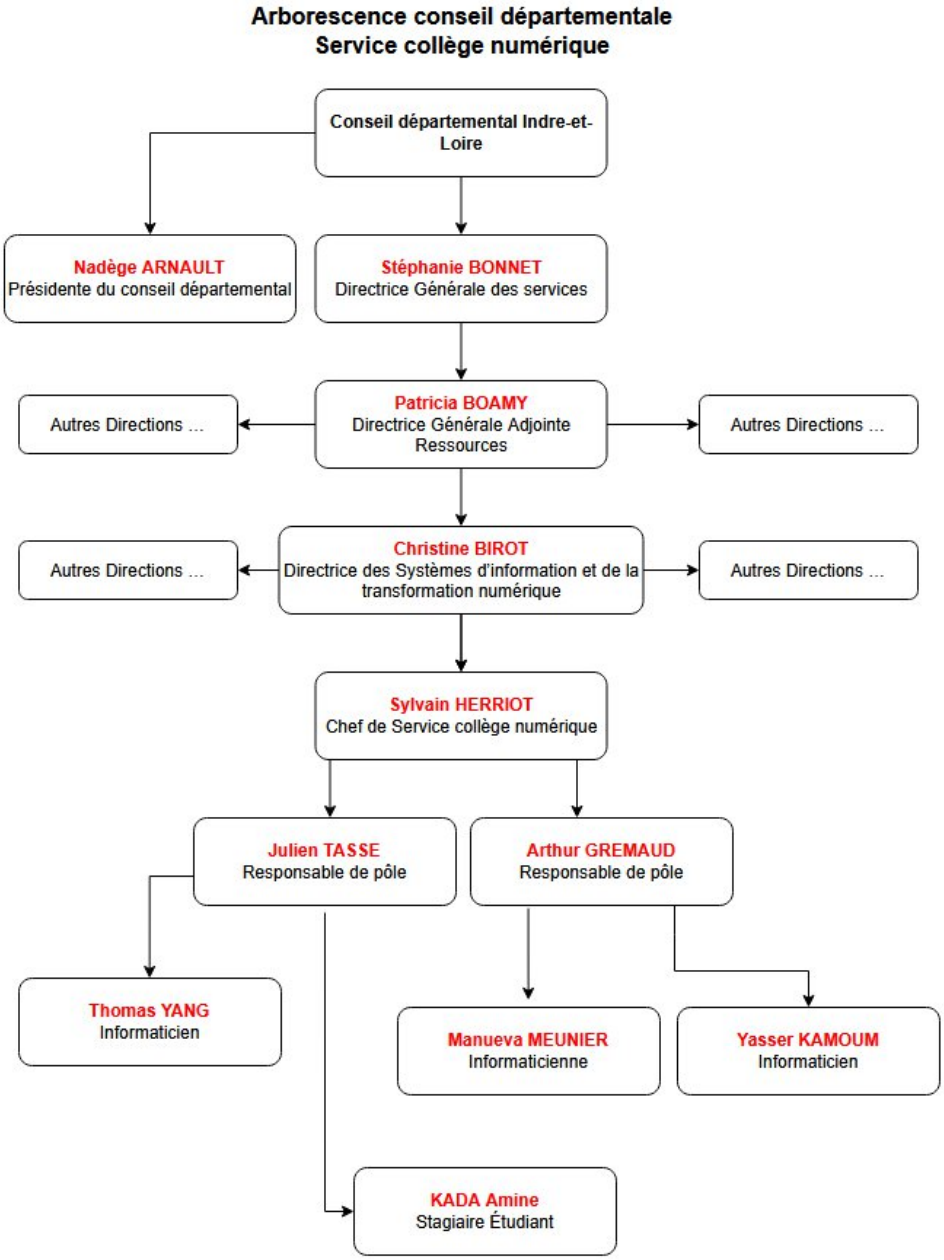
2 Rue de l'Aviation, 37210 Parçay-Meslay, France, à proximité de Tours et de l'aéroport Tours Val de Loire.

Donnée cartographique de Google maps - 2026.



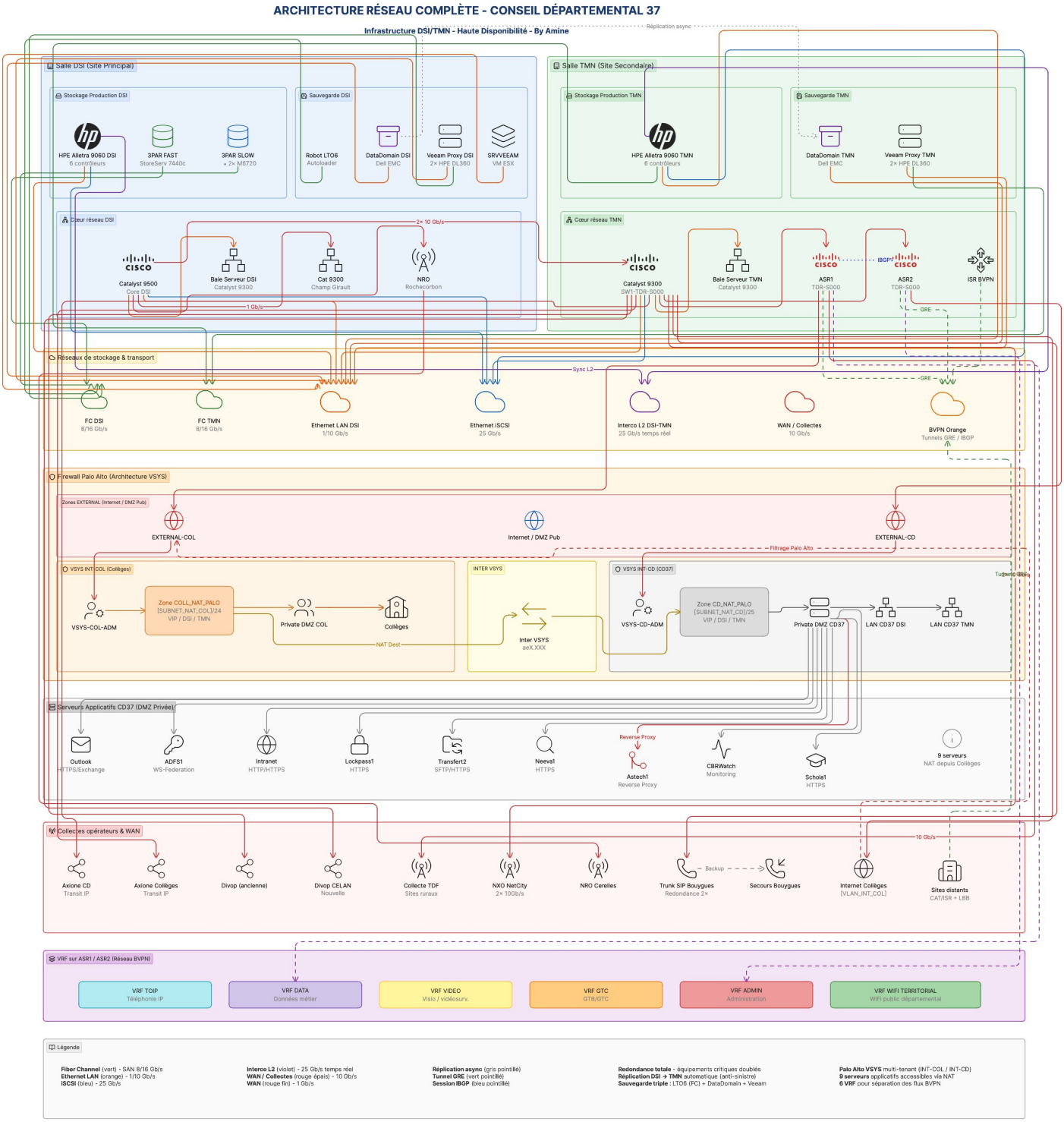
1.3 – Organigramme hiérarchique CD37

Le conseil départemental dispose d'une équipe importante et de plusieurs services. Dans mon cas, je me suis basé uniquement sur le service informatique où s'est déroulé mon stage, ainsi que sur les personnes qui m'ont accompagné durant celui-ci, aussi bien en interne qu'en externe, sans oublier les supérieurs qui dirigent le service.



(Source : KADA Amine – By Draw.io)

1.4 – Organisation SI du Conseil Départemental



(Voir Glossaire Technique & Annexe n°13)

2. Missions

Cette section présente les principales missions et interventions réalisées au cours du stage au sein du service informatique du Conseil Départemental d'Indre-et-Loire. Les missions sont regroupées par thématique technique et couvrent la gestion de l'infrastructure réseau, le déploiement de postes, la supervision des équipements et la maintenance applicative.

2.1 - Mission n°1 : Découverte et audit de la salle serveur DSI

2.1.1. Problématique

Comment le Conseil Départemental garantit-il la disponibilité, la sécurité physique et la résilience de son infrastructure serveur, qui héberge les services informatiques de l'ensemble des collèges du département ?

2.1.2. Contexte

Lors de la première journée de stage, une visite complète de la salle serveur du Conseil Départemental a été organisée. Cette visite avait pour objectif de comprendre l'organisation physique et logique de l'infrastructure, les mesures de sécurité en place et la stratégie de sauvegarde adoptée.

2.1.3. Sécurité physique et environnementale

La salle serveur bénéficie d'un niveau de protection physique élevé, structuré autour de plusieurs couches de sécurité complémentaires :

- Contrôle d'accès par badge magnétique avec gestion stricte des droits et traçabilité complète via un système de logs.
- Vidéosurveillance active en continu pour enregistrer tout mouvement dans la salle.
- Surveillance du Radon, gaz radioactif naturel incolore et inodore détecté sous la salle, nécessitant un suivi.
- Système anti-incendie par gaz étouffant, qui supprime l'oxygène de la pièce sans endommager les équipements électroniques (contrairement à l'eau).

2.1.4. Infrastructure électrique et refroidissement

La continuité d'alimentation est assurée par une architecture redondante à plusieurs niveaux :

- Alimentation principale fournie par EDF, couplée à des onduleurs par serveur.
- Groupe électrogène offrant une autonomie de 2 jours en cas de coupure totale du fournisseur.
- Double carte réseau fibre par serveur pour garantir la haute disponibilité des connexions.
- Climatisation avec un seuil critique fixé à 60 °C maximum, déclenchant des alertes automatiques.
- Opérateurs FAI : Bouygues et Axionne (réseau Orange) pour la redondance de la connectivité Internet.

2.1.5. Stratégie de sauvegarde : la règle du 3-2-1

Le Conseil Départemental applique la règle de sauvegarde 3-2-1, considérée comme la norme de référence en matière de protection des données. Cette stratégie garantit qu'une copie des données reste disponible même en cas de sinistre majeur (incendie, vol, ransomware).

Règle	Description	Mise en œuvre au Conseil Départemental
3 Copies	Trois exemplaires distincts des données.	• Sauvegarde immuable (serveur DataDomaine) — rétention 2 mois • Sauvegarde différentielle (serveur Rack) — rétention 1 mois • Bande magnétique — rétention 1 an
2 Supports	Deux sites géographiquement distincts.	• Site principal (DSI) : salle serveur du Conseil Départemental • Site secondaire : salle serveur distant (derrière la zone aéroport Tours Nord - TMN) (Les deux sites sont reliés ensemble en fibre monomode)
1 Hors ligne	Une copie déconnectée du réseau, protégée contre les ransomwares.	Bande magnétique stockée dans un coffre-fort physique en salle serveur.

2.1.6. Fonctionnement des 2 sites de l'architecture réseau

L'étude du schéma d'architecture globale du Conseil Départemental m'a permis de comprendre les enjeux de Haute Disponibilité et de sécurisation des données à grande échelle. L'infrastructure se base autour de deux datacenters physiquement distincts : la salle DSI (site principal) et la salle TMN (site secondaire).

Cette conception répond à des exigences strictes de continuité de service :

- Interconnexion et réplication des sites : Les deux salles serveurs sont reliées par une liaison fibre optique de niveau 2 (FTTH) offrant un très haut débit (25 Gb/s) avec une latence minimale. Ce lien capacitaire permet une réplication asynchrone des données entre les baies de stockage de production (HPE Alletra 6050). Ainsi, le site secondaire possède en permanence une copie à jour des données du site principal.
- Automatisation des sauvegardes et archivage : La politique de protection des données est entièrement automatisée et orchestrée par le serveur Veeam Backup & Replication. L'architecture technique fait une distinction claire entre deux processus complémentaires :

    - La sauvegarde (Backup) : Utilisée pour la restauration rapide et courante en cas d'incident (suppression accidentelle, corruption, ransomware). Les données chaudes sont stockées sur des appliances à disques rapides et dédupliqués (Dell EMC DataDomain).
    - L'archivage : Utilisé pour la conservation à long terme et légale des données froides. Il est géré de manière mécanique par un Robot LTO8 Automator, ce qui permet de stocker les données sur des bandes magnétiques externalisables.
- Plan de Reprise d'Activité (PRA) : La redondance totale du matériel critique (cœur de réseau Cisco Catalyst 9500, pare-feux Palo Alto, baies de stockage et de sauvegarde) répartie sur les deux sites constitue un véritable PRA "anti-sinistre". En cas de perte majeure ou totale de la salle DSI principale (incendie, inondation, coupure électrique prolongée), l'architecture permet un basculement des services vers la salle TMN, garantissant ainsi la continuité des opérations pour les agents et les collèges du département.

2.1.7. Supervision de l'infrastructure avec Zabbix

L'ensemble des équipements des collèges du département est supervisé en temps réel depuis le Conseil Départemental via l'outil Zabbix. Cet outil permet de centraliser la surveillance de tous les équipements réseau (commutateurs, routeurs, bornes Wi-Fi) et des serveurs critiques (SRV-01 à SRV-04). La gestion de cette supervision constituant un enjeu technique majeur, son analyse détaillée et sa mise en œuvre pratique feront l'objet d'une étude complète dans la **Mission n°5** de ce rapport. (Voir **Annexe n°11**)

2.1.8. Conclusion

Cette première journée m'a permis d'appréhender la complexité d'une infrastructure mutualisée à l'échelle d'un département. Le Conseil Départemental gère en effet un parc d'une cinquantaine de collèges, ce qui implique une organisation rigoureuse, une redondance à tous les niveaux (électrique, réseau, sauvegarde) et des outils de supervision centralisés pour maintenir un niveau de service constant.

2.2 - Mission n°2 : Mise en place de la téléphonie VoIP

2.2.1. Problématique

Comment remplacer un ancien autocom (PABX) géré par un prestataire privé par une solution de téléphonie IP centralisée et supervisée directement par le Conseil Départemental, sans interruption de service pour les utilisateurs du collège ?

2.2.2. Contexte

Une intervention a été menée au Collège Montaigne (Parçay-Meslay) pour déployer le nouveau système de téléphonie IP. Auparavant, la téléphonie de chaque collège était assurée par un autocom (Alcatel-Lucent OmniPCX) géré par des prestataires privés, à la charge financière directe du collège. Le Conseil Départemental a décidé d'internaliser cette gestion pour réduire les coûts et centraliser la supervision.

2.2.3. Solutions techniques possibles

Deux approches étaient envisageables pour cette migration :

- Maintien de l'autocom existant avec ajout d'un trunk SIP : solution peu coûteuse à court terme mais ne permettant pas la centralisation ni la supervision unifiée.
- Remplacement complet par une téléphonie IP (VoIP) centralisée sur les serveurs du Conseil Départemental : solution retenue, offrant supervision, réduction des coûts et plan de numérotation unifié à l'échelle du département.

2.2.4. Solution retenue et mise en œuvre

La solution retenue est de s'appuyer sur l'infrastructure locale du Collège Montaigne pour raccorder les postes à l'IPBX centralisé au Conseil Départemental.

Note sur l'architecture et la séparation des rôles : Afin de garantir la sécurité et la continuité de service, le Serveur 01 (SRV-01) agit comme un hôte de virtualisation. Les rôles ne sont pas cumulés sur le même système d'exploitation. Ils sont isolés sur des machines virtuelles (VM) distinctes : une VM est dédiée exclusivement au service d'annuaire (AD DS), et une autre est dédiée au service DHCP. Cette séparation évite qu'une défaillance ou une compromission d'un service n'impacte l'autre.

La procédure de basculement s'est déroulée en plusieurs étapes clés :

- Accès réseau : Connexion du poste de supervision sur un port libre d'un commutateur de niveau 2 du réseau pédagogique.
- Configuration du Provisioning (DHCP) : Connexion à la VM hébergeant le rôle DHCP avec les droits administrateurs pour activer le pool préalablement configuré avec un plan d'adressage spécifique au VLAN Voix (VLAN 13). Ce pool intègre les options DHCP nécessaires pour transmettre aux téléphones l'adresse IP de l'IPBX centralisé où ils doivent télécharger leur profil.

- Basculement réseau : Déconnexion du câble Ethernet reliant le commutateur à l'ancien autocom. En perdant leur connexion, les téléphones IP sont forcés de redémarrer, d'interroger la VM DHCP locale pour récupérer leur nouvelle configuration (IP, masque, passerelle, options de provisionning), et de s'enregistrer automatiquement sur la nouvelle architecture.
- Recette : Tests de connectivité systématiques (appels internes et externes) dans toutes les salles équipées de postes fixes pour valider le bon enregistrement SIP.
- Démantèlement : Retrait physique définitif de l'ancien autocom de la baie de brassage.

2.2.5. Architecture de la nouvelle téléphonie

La nouvelle architecture repose sur un IPBX centralisé **Alcatel-Lucent OmniPCX Enterprise (OXE)**, hébergé au cœur de réseau du Conseil Départemental. La gestion, la création des usagers et l'administration des postes se font à distance via la suite logicielle **Alcatel-Lucent OmniVista**. (Voir **Annexe n°14**)

Le nouveau plan de numérotation géré par cet IPBX centralisé est structuré comme suit :

- **Appels externes (SDA — Sélection Directe à l'Arrivée) :** certains services stratégiques (Direction, Accueil, Secrétariat) disposent d'un numéro direct depuis l'extérieur.
- **Appels internes :** plan à 5 chiffres (ex : 50011 pour l'Intendance, 50015 pour le Secrétariat).
- **Interconnexion départementale :** ce plan à 5 chiffres permet de joindre gratuitement n'importe quel collège du département raccordé à cette infrastructure.
- **Administration et Supervision :** Configuration de la téléphonie via **OmniVista**, et supervision réseau à distance via Zabbix et mRemoteNG, le tout sans aucune intervention physique sur site.

2.2.6. Charte de câblage réseau

Pour faciliter la maintenance et le repérage dans les baies de brassage, le Conseil Départemental applique une charte de couleurs stricte pour les câbles Ethernet, associant chaque couleur à un VLAN et un usage précis :

Couleur	Usage / Destination	VLAN associé	Spécificité
Rouge	Impression (imprimantes / copieurs)	VLAN 12	—
Vert	Bornes Wi-Fi	VLAN 20 / 21 / 22 / 23 / 24	Alimentation PoE
Jaune	Réseau pédagogique + Téléphonie IP	VLAN 20 / VLAN 13	Alimentation PoE
Bleu	Réseau administratif + Téléphonie IP	VLAN 8 / VLAN 13	Alimentation PoE
Noir	Réseau administratif seul	VLAN 8	—
Violet	Gestion Technique Centralisée (GTC)	VLAN 35	—
Orange	Téléphone IP dédié	VLAN 13	Alimentation PoE
Gris	Réseau pédagogique seul	VLAN 20	—

2.2.7. Conclusion

Cette mission m'a permis d'observer une migration téléphonique complète en conditions réelles. L'enjeu principal était de ne pas interrompre la communication du collège pendant l'intervention. La centralisation de la téléphonie au niveau du Conseil Départemental représente un gain significatif : réduction des coûts de prestataire, supervision unifiée, et plan de numérotation cohérent à l'échelle du département.

2.3 - Mission n°3 : Baie de brassage collège Henri Becquerel

2.3.1. Problématique

Comment restructurer physiquement et logiquement les baies de brassage d'un collège lors d'un remplacement complet des équipements actifs, tout en intégrant simultanément une nouvelle solution de téléphonie IP et en maintenant la continuité de service ?

2.3.2. Contexte

Une intervention au Collège Henri Becquerel (Avoine) a consisté en la rénovation complète des trois baies de brassage du collège en après-midi pour ne pas perturber l'administration comme les cours. Cette intervention comprenait le remplacement des commutateurs (Switchs), le recâblage complet selon la charte de couleurs départementale, et le déploiement des nouveaux équipements actifs Cisco déjà préparer par la configuration qui respecte leur charte des collèges. (Voir **Annexe n°15**)

2.3.3. Équipements déployés

Les nouveaux commutateurs installés sont les suivants :

- 2 × Cisco Catalyst 1300 48P (PoE) — ports alimentés pour bornes Wi-Fi et téléphones IP.
- 1 × Cisco Catalyst 1300 48T (Non PoE) — réseau pédagogique classique.
- 1 × Cisco Catalyst 1300 24P (PoE) — baie de plus petite taille.

2.3.4. Procédure de rebrassage

L'intervention s'est déroulée en plusieurs phases successives :

1. Débrassage total des trois baies : retrait de tous les câbles existants, en s'appuyant sur les logs de ports actifs relevés en amont pour identifier les connexions à conserver.
2. Remplacement des anciens Switchs par les nouveaux modèles Cisco Catalyst 1300.
3. Rebrassage complet en appliquant la charte de couleurs départementale (rouge impression, vert Wi-Fi, bleu administratif, etc.).
4. Configuration des VLANs sur chaque port des nouveaux commutateurs selon le plan de segmentation réseau du Conseil Départemental.

(Voir exemple **Annexe n°17**)

2.3.5. Focus technique : l'empilement de Switchs (Stacking)

Sur la Baie 1, une configuration de stacking (empilement) a été mise en place entre un Cisco Catalyst 1300 48P PoE et un 48T. Cette technologie permet de relier physiquement plusieurs commutateurs pour qu'ils forment un seul équipement logique.

> 🔧 **Fonctionnement du Stacking** (Voir **Annexe n°12**)
> Les deux Switchs sont interconnectés par des câbles haute vitesse dédiés. L'un est élu « Maître » (Active) et l'autre « Esclave » (Standby). L'ensemble partage une seule table de routage, une seule configuration et une seule adresse IP de management.
>
> Avantages : L'administration unifiée de 96 ports depuis une seule interface, et redondance automatique si l'un des commutateurs tombe en panne.

2.3.6. Déploiement de la téléphonie en mode hybride

Contrairement au Collège Montaigne (intervention du mardi), la migration téléphonique au Collège Becquerel s'est faite en mode hybride : les nouveaux téléphones IP ont été déployés, mais l'ancien autocom a été maintenu en parallèle pendant une période de transition. Cette approche permet aux utilisateurs de se familiariser avec le nouveau système tout en conservant une solution de repli (rollback) en cas de problème.

2.3.7. Gestion des impressions sécurisées : PaperCut & Alternatif

L'intervention a également été l'occasion d'observer le fonctionnement du système d'impression centralisé PaperCut, déployé dans tous les collèges. Il s'agit d'une solution logicielle commerciale et propriétaire. PaperCut est connecté à l'Active Directory via le protocole LDAPS (LDAP over SSL) pour l'authentification sécurisée des utilisateurs. Pour libérer une impression, l'utilisateur doit s'authentifier directement sur l'imprimante par deux méthodes :

- Facteur de connaissance : saisie de l'identifiant sur l'écran tactile.
- Facteur de possession : passage du badge professionnel sur le lecteur RFID intégré. (Voir **Annexe n°8**)

Ce système répond à deux enjeux majeurs : la réduction des impressions inutiles (économique et écologique) et la confidentialité des documents sensibles (sécurité).

Alternative libre et prototypage : Dans le cadre d'une veille technologique ou pour la mise en place d'un prototype sans coût de licence, cette architecture pourrait être reproduite avec des solutions open source. Une alternative consisterait à déployer un serveur d'impression CUPS (Common UNIX Printing System) couplé à la solution libre SavaPage. Ce type de prototype permettrait de conserver les fonctionnalités clés :

- Connexion à l'annuaire LDAP,
- Rétention des impressions (Release Station)
- Gestion de l'authentification par badge NFC/RFID, tout en s'affranchissant des licences propriétaires.

2.3.8. Conclusion

Cette journée d'intervention au Collège Becquerel a été particulièrement formatrice. Elle m'a permis de travailler sur l'ensemble du cycle d'une refonte réseau : du démontage physique des équipements jusqu'à la configuration logique des VLANs sur les nouveaux Switchs. La gestion du stacking et la compréhension des différents VLANs départementaux (pédagogique, administratif, impression) ont été des apports techniques majeurs.

2.4 - Mission n°4 : Déploiement MECM (Microsoft)

2.4.1. Problématique

Comment mettre à jour en masse le BIOS et migrer le système d'exploitation d'un parc d'une soixantaine de postes portables vers Windows 11 Éducation, tout en garantissant l'intégration automatique au domaine Active Directory et en minimisant le temps d'intervention par machine ?

2.4.2. Contexte

La mission principale a consisté à déployer une mise à jour de BIOS et une migration vers Windows 11 Éducation sur un parc d'environ soixante ordinateurs portables (marques Lenovo et HP) dont les versions de BIOS dataient de 2020 à 2022.

L'outil utilisé est Microsoft Endpoint Configuration Manager (MECM/SCCM), solution de déploiement centralisé utilisée par le Conseil Départemental et nécessitant une licence, donc payante.

2.4.3. Solutions techniques possibles

- Déploiement manuel poste par poste : trop chronophage pour un parc de soixante machines, avec un risque d'erreur humaine élevé.
- Déploiement via WDS (Windows Deployment Services) : solution plus légère mais sans gestion du BIOS ni des pilotes.
- Déploiement via MECM avec séquence de tâches automatisée : solution retenue, permettant de gérer en un seul flux l'OS, les pilotes, la mise à jour BIOS, l'intégration AD et l'installation des applications.

2.4.4. Mise en œuvre

La séquence de tâches MECM se déroule en cinq étapes automatisées :

1. Gestion du disque : vérification de l'état de santé et de l'espace disponible.
2. Déploiement de l'OS : installation de l'image Windows 11 Éducation via démarrage PXE (réseau).
3. Gestion des pilotes : installation et mise à jour automatique des drivers matériels selon le modèle détecté. (Voir **Annexe n°5**)
4. Personnalisation via requête WMI : identification du modèle exact du portable pour déployer la version correcte du firmware BIOS. Une condition WMI est utilisée pour cibler précisément le bon modèle. (Voir **Annexe n°4** & **6**)
5. Installation des applications : déploiement des logiciels requis (disponibles dans le Software Center (Centre Logiciel) avec plus de 60 applications approuvées par l'administrateur). (Voir procédure en **Annexe n°17**)

> 🔍 **Focus technique : la requête WMI pour le ciblage BIOS**
> La requête WMI (Windows Management Instrumentation) permet à la séquence de tâches d'identifier automatiquement le modèle exact du laptop (ex : Lenovo ThinkPad L14 Gen 2) et de déployer uniquement le firmware BIOS correspondant, évitant tout risque de flash incorrect qui pourrait rendre la machine inutilisable.

2.4.5. Contrôle post-déploiement

Une fois l'installation terminée, une vérification manuelle est effectuée pour chaque machine :

- Connexion avec le compte administrateur de l'Active Directory (Voir **Annexe n°16**).
- Validation de l'intégration du poste dans l'Active Directory.
- Vérification de la nouvelle version du BIOS dans les paramètres UEFI (msinfo32).
- Contrôle de l'accès au Software Center et de la disponibilité des applications.
- Validation finale : mise de côté du poste prêt pour distribution.

2.4.6. Gestion d'inventaire : PYTHEAS et Cisco Business Dashboard

En parallèle du déploiement de postes, une mission de gestion d'inventaire a été menée pour mettre à jour la documentation suite à l'intervention au Collège Henri Becquerel (mercredi 20 mai) :

- PYTHEAS : saisie des entrées et sorties de matériel dans le logiciel de gestion d'inventaire départemental, enregistrement des nouveaux Switchs et désaffectation des anciens équipements via leurs numéro de séries. (Voir **Annexe n°9**)
- Cisco Business Dashboard : intégration des nouveaux commutateurs au contrôleur de supervision en leur attribuant leurs adresses IP de management. Cet outil offre une visibilité en temps réel sur l'état de tous les équipements Cisco du département (Switchs, bornes Wi-Fi). (Voir **Annexe n°1 à 3**)

2.4.7. Conclusion

Cette mission m'a permis de découvrir une solution de déploiement industrielle utilisée dans les grandes organisations. MECM représente un niveau de maturité bien supérieur aux outils comme FOG étudiés en cours : il intègre dans un seul flux la gestion du BIOS, de l'OS, des pilotes, de l'Active Directory et des applications.

2.5 - Mission n°5 : Mise en place d'un système de supervision réseau avec Zabbix

2.5.1. Problématique

Comment un technicien du service informatique peut-il superviser en temps réel l'état de santé de plusieurs centaines d'équipements réseau répartis dans des collèges du département, détecter proactivement les pannes avant qu'elles n'impactent les utilisateurs, et recevoir des alertes automatiques en cas d'anomalie ?

2.5.2. Contexte

Lors de mon stage au Conseil Départemental d'Indre-et-Loire, j'ai eu l'occasion d'observer l'utilisation quotidienne de l'outil de supervision Zabbix, déployé par le service informatique pour monitorer l'ensemble du parc des collèges du département. Zabbix centralise la surveillance de plusieurs dizaines d'équipements : serveurs Windows Server (AD, DHCP, impression, fichiers, déploiement), commutateurs Cisco, bornes Wi-Fi et accès distants via iLO (Integrated Lights-Out). Cette mission m'a permis de comprendre les enjeux de la supervision en milieu professionnel, puis de reproduire une architecture similaire dans un POC sur machine virtuelle.

2.5.3. Solutions techniques possibles

Critère	**Zabbix**	Nagios
Licence	Open Source (gratuit)	Open Source (gratuit)
Interface	Web moderne, tableaux de bord compréhensible	Interface plus complexe
Protocoles	SNMP, ICMP, agent, SSH, HTTP…	SNMP, ICMP, agent…
Scalabilité	Très élevée (proxy Zabbix)	Élevée
Alertes	Triggers, mail, SMS, webhook	Triggers, mail
Expérience	Certaines personnes en DSI l'utiliser déjà	Aucune connaissance
Adapter	Oui (solution retenue)	Possible, mais plus complexe

2.5.4. Justification du choix : Zabbix

Le Conseil Départemental a retenu Zabbix pour plusieurs raisons déterminantes :

- **Gratuité totale :** aucun coût de licence, ce qui est un critère essentiel pour une collectivité territoriale soumise à des contraintes budgétaires.
- **Scalabilité :** la fonctionnalité de proxy Zabbix permet de superviser des équipements situés dans des réseaux distants (les collèges) sans ouvrir de flux entrants depuis Internet, en faisant remonter les métriques au serveur central.
- **Richesse des protocoles :** Zabbix supporte nativement SNMP (pour les Switchs et bornes Wi-Fi), l'agent Zabbix (pour les serveurs Windows/Linux), ICMP (ping) et HTTP, couvrant ainsi la totalité des équipements du parc.
- **Tableaux de bord personnalisables :** l'interface web permet de créer des vues synthétiques par collège, par type d'équipement ou par criticité des alertes.
- **Triggers et alertes :** le système de déclencheurs (triggers) permet de définir des seuils précis (ex. : CPU > 90 % pendant 5 minutes, interface réseau DOWN) et d'envoyer automatiquement des alertes par mail aux techniciens.

2.5.5. Observation en stage : Zabbix au Conseil Départemental

Durant mon stage, j'ai pu observer l'utilisation de Zabbix pour le suivi des équipements du Collège Montaigne. Le tableau de bord centralise l'état de tous les hôtes surveillés avec un code couleur clair : vert (OK), orange (avertissement), rouge (problème critique). Les hôtes supervisés pour chaque collège comprennent typiquement :

- Les 4 serveurs Windows (SRV-01 à SRV-04) avec surveillance CPU, RAM, espace disque et disponibilité des services.
- Les commutateurs Cisco Catalyst via SNMP : état des interfaces, trafic entrant/sortant, charge CPU.
- Les bornes Wi-Fi : disponibilité, nombre de clients connectés, signal.
- L'administration out-of-band via iLO : permet d'intervenir sur un serveur même hors tension OS.

Apport professionnel

Observer Zabbix en production m'a permis de comprendre concrètement la notion de supervision dynamique : plutôt que d'attendre qu'un utilisateur signale une panne, le service informatique est alerté dès qu'un seuil critique est franchi, parfois avant même que les utilisateurs ne s'en aperçoivent.

2.5.6. POC (Proof of Concept) : Déploiement de Zabbix sur VM Linux

Afin de valider ma compréhension et d'aller plus loin que la simple observation, j'ai reproduit une architecture de supervision fonctionnelle sur ma machine personnelle à l'aide de VirtualBox, en installant Zabbix Server sur une VM Debian 12 et en surveillant un second hôte.

Architecture du POC

VM 1 — Zabbix Server (Debian 12) : IP 192.168.56.10 | Rôle : serveur de supervision, interface web, base de données MariaDB (MySQL trop de problème de crash).
VM 2 — Hôte supervisé (Debian 12) : IP 192.168.56.20 | Rôle : machine cible avec agent Zabbix installé.
Réseau : Host-only (VirtualBox) — les deux VMs communiquent sans accès Internet requis.

Étape 1 — Installation du serveur Zabbix

Installation de Zabbix 7.0 LTS sur Debian 12 depuis le dépôt officiel :

```
# Ajout du dépôt officiel Zabbix 7.0
wget https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_latest+debian12_all.deb
dpkg -i zabbix-release_latest+debian12_all.deb
apt update

# Installation des composants
apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf \ zabbix-sql-scripts zabbix-agent mariadb-server

# Création de la base de données
mysql -uroot -e "CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;"
mysql -uroot -e "CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'password123';"
mysql -uroot -e "GRANT ALL ON zabbix.* TO 'zabbix'@'localhost';"

# Import du schéma de base
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix

# Démarrage des services
systemctl enable --now zabbix-server zabbix-agent apache2
```

Une fois l'installation terminée, l'interface web Zabbix est accessible sur http://192.168.56.10/zabbix. L'assistant de configuration web permet de valider la connexion à la base de données et de créer le compte administrateur.

Étape 2 — Ajout d'un hôte supervisé avec l'agent Zabbix

Sur la VM hôte (192.168.56.20), installation et configuration de l'agent Zabbix pour qu'il remonte ses métriques au serveur :

```
# Sur la VM hôte (192.168.56.20)

apt install -y zabbix-agent

# Configuration de l'agent
nano /etc/zabbix/zabbix_agentd.conf
  Server=192.168.56.10            # IP du serveur Zabbix
  ServerActive=192.168.56.10    # Connexion active
  Hostname=VM-Hote-POC          # Nom de l'hôte dans Zabbix

systemctl enable —now zabbix-agent
```

Depuis l'interface web Zabbix, j'ai ensuite déclaré le nouvel hôte :

- Menu Configuration → Hôtes → Créer un hôte.
- Nom d'hôte : VM-Hote-POC — Interface : Agent — IP : 192.168.56.20 — Port : 10050.
- Application du modèle *Linux by Zabbix agent*, qui inclut automatiquement des métriques prédéfinies (CPU, RAM, disque, réseau).

Étape 3 — Création d'un trigger (déclencheur d'alerte)

J'ai créé un trigger personnalisé pour simuler une alerte réelle : une notification dès que la charge CPU de la VM dépasse 80 % pendant plus de 2 minutes.

Configuration du trigger

- **Nom :** CPU élevé sur {HOST.NAME}
- **Expression :** avg(/VM-Hote-POC/system.cpu.util,2m) > 80
- **Sévérité :** Avertissement (Warning)
- **Description :** La charge CPU dépasse 80 % depuis plus de 2 minutes — vérifier les processus en cours.

Pour déclencher l'alerte en condition réelle, j'ai simulé une charge CPU élevée sur la VM hôte avec la commande stress :

```
# Simulation d'une charge CPU élevée (pendant 3 minutes)

apt install -y stress
stress —cpu 4 —timeout 180
```

Étape 4 — Configuration des alertes par e-mail

J'ai configuré le canal de notification par e-mail dans Zabbix pour simuler l'envoi automatique d'une alerte à un technicien :

- Menu Administration → Média types → Email → configuration du serveur SMTP.
- Création d'une action d'alerte : envoi automatique d'un mail lors du déclenchement d'un trigger de sévérité ≥ Warning.
- Test de l'envoi via le bouton « Test » de l'interface Zabbix.

2.5.12. Conclusion

Cette mission m'a permis de passer de l'observation à la pratique sur un outil professionnel réel. En stage, j'ai compris comment le Conseil Départemental exploite Zabbix pour maintenir une vision centralisée de l'état de santé de dizaines d'équipements répartis sur tout le département. Le POC m'a permis de maîtriser les concepts clés : installation du serveur, déploiement de l'agent, création de triggers conditionnels et mise en place des alertes automatiques. En comparaison avec les outils étudiés en cours (comme le monitoring basique via ping), Zabbix apporte une couche d'analyse bien plus profonde grâce aux métriques SNMP, aux graphes historiques et aux tableaux de bord personnalisables par site. Cette compétence est directement valorisable dans le cadre du BTS SIO SISR et correspond à la compétence « Exploiter des outils de supervision ».

2.6 - Mission n°6 : Restructuration du réseau de déploiement MECM (10 Gb/s) et serveur DHCP dédié

2.6.1. Problématique

Comment optimiser et isoler les flux réseau lors des déploiements massifs de postes informatiques afin de réduire drastiquement les temps d'installation, tout en évitant de saturer le serveur DHCP principal de l'infrastructure du Conseil Départemental ?

2.6.2. Contexte

Durant la dernière semaine de mon stage, j'ai été chargé d'améliorer l'infrastructure de l'atelier de préparation des postes. Auparavant, les déploiements de machines via MECM s'effectuaient sur des liens en 1 Gb/s et s'appuyaient sur l'ancien serveur DHCP central, qui gérait l'intégralité de l'infrastructure du CD37. Avec le volume important de postes à masteriser, cette architecture créait des goulots d'étranglement (lenteur de déploiement) et surchargeait inutilement le serveur DHCP principal.

2.6.3. Solutions techniques et architecture retenue

Pour répondre à ce besoin d'optimisation et d'isolation, nous avons opté pour la création d'une nouvelle architecture dédiée exclusivement aux déploiements MECM dans l'atelier :

Mise à niveau de la bande passante : Passage de l'ensemble des liens de l'atelier de 1 Gb/s à 10 Gb/s grâce à l'utilisation de modules SFP (Fibre/DAC).

Création de DMZ dédiées (VLANs) : Segmentation du réseau pour isoler le trafic de déploiement de la production. Quatre VLANs spécifiques ont été créés (830, 831, 832 et 840), le **VLAN 832** (DMZ-Deploiement_Atelier) étant spécifiquement réservé aux postes en cours d'installation.

Nouveau serveur DHCP autonome : Installation d'un nouveau système Windows Server intégré au domaine de la collectivité. Ce serveur a reçu le rôle DHCP de manière exclusive pour répondre aux requêtes PXE des postes de l'atelier, soulageant ainsi l'ancien serveur central.

Équipement physique : Mise en place de deux switchs KVM de 8 ports sur les bancs de l'atelier, permettant de connecter et de masteriser jusqu'à 16 postes simultanément avec un seul ensemble clavier/écran/souris.

2.6.4. Mise en œuvre

L'intervention s'est déroulée en plusieurs étapes logiques et physiques (Voir **Annexe n°19**) :

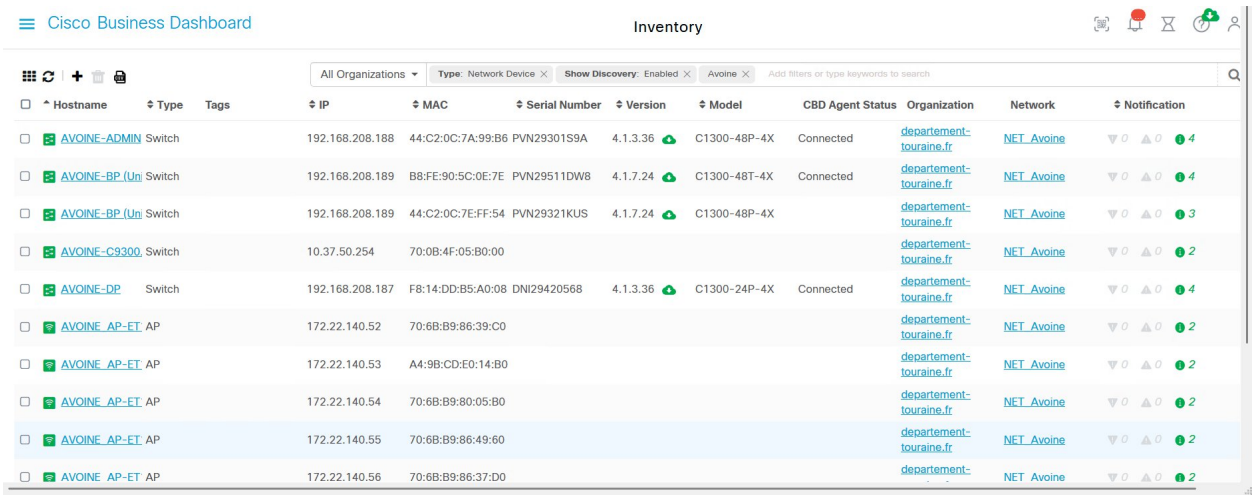
1. **Câblage et configuration réseau :**
    - Interconnexion des deux commutateurs de l'atelier (**SW-ATELIER-G** et **SW-ATELIER-D**) vers l'infrastructure centrale (Infra CD37) via des liens SFP 10 Gb/s.
    - Configuration des ports en mode **Trunk** pour faire transiter les VLANs DMZ (830, 831, 832, 840) entre les switchs.
1. **Préparation du serveur DHCP :**
    - Installation de l'OS Windows Server.
    - Intégration du serveur au domaine Active Directory du Conseil Départemental.
    - Configuration de la carte réseau du serveur avec l'adresse IP fixe 192.168.12.150 et raccordement sur le switch **SW-ATELIER-D** sur un port configuré en mode **Access sur le VLAN 832**.
1. **Configuration du rôle DHCP :**
    - Création de l'étendue (Scope) correspondant à l'adressage du VLAN 832.
    - Configuration des options DHCP spécifiques (notamment les options 66 et 67 pour le démarrage réseau PXE) afin de diriger les postes clients vers le serveur MECM lors de leur démarrage.
1. **Installation de l'atelier :**
    - Câblage réseau et vidéo des 16 emplacements sur les bancs de préparation, reliés aux deux nouveaux switchs KVM.

2.6.5. Conclusion

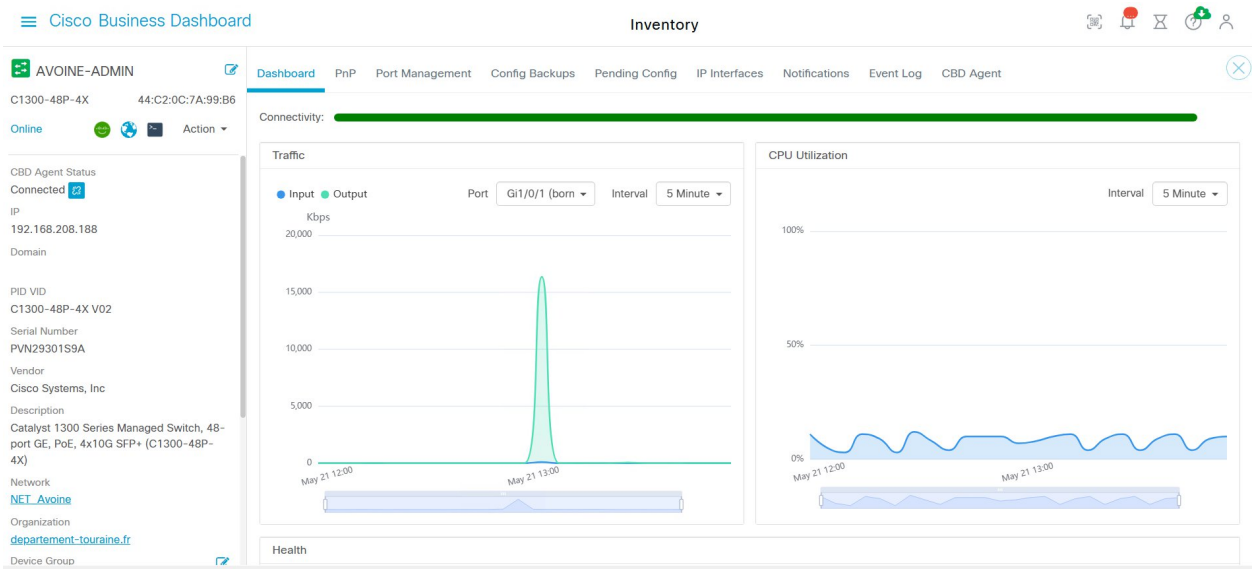
Ce projet complet de fin de stage a été une grande réussite. Le passage d'une connectivité 1 Gb/s à 10 Gb/s, couplé à un serveur DHCP localisé dans le VLAN 832, a permis d'accélérer considérablement le téléchargement des images Windows (fichiers WIM) via MECM. De plus, la création de cette DMZ dédiée sécurise le réseau de production principal en isolant complètement le trafic intensif lié aux installations en masse. L'utilisation des KVM offre désormais un confort de travail optimal pour les techniciens du helpdesk.

3. Annexes

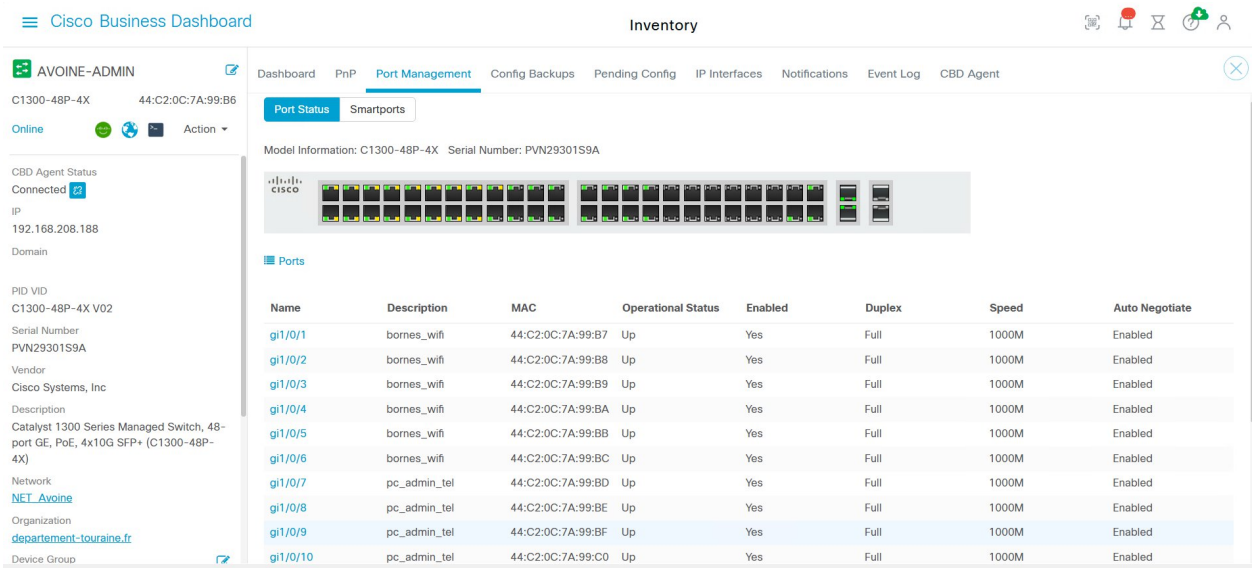
Annexe n°1 : *Dashboard Cisco « L'inventaire Cisco ».*



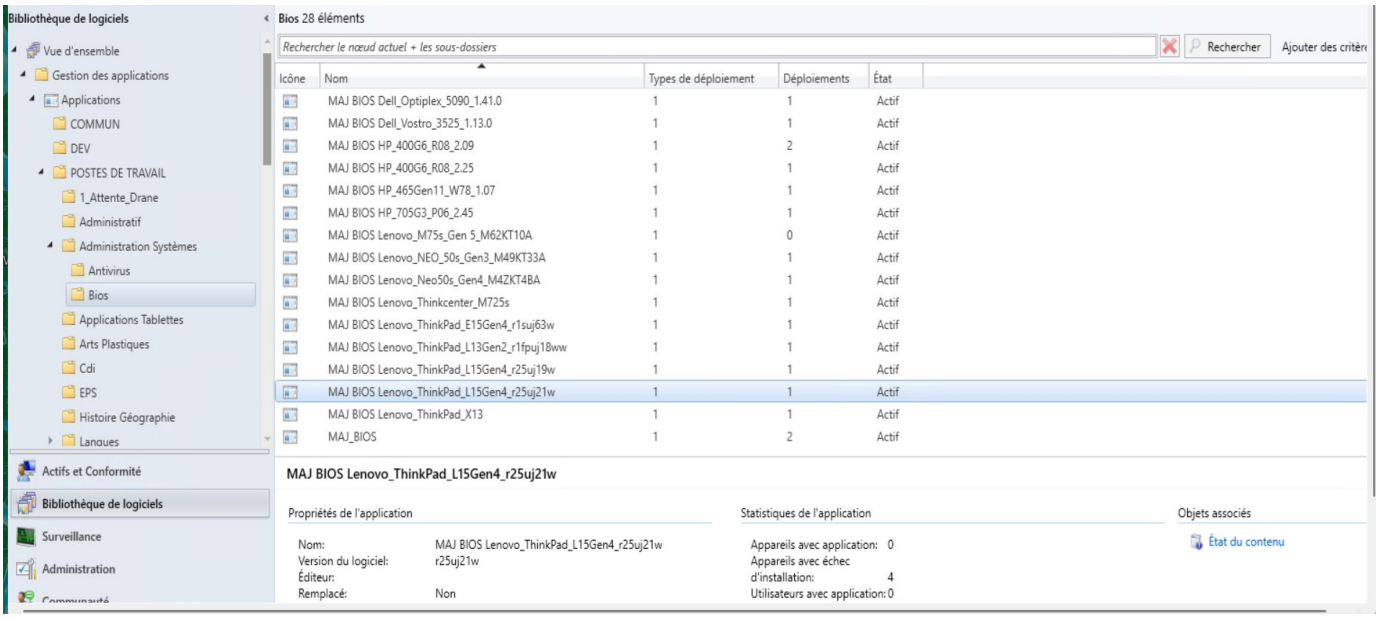
Annexe n°2 : *Aperçus détailler du Switch Cisco « AVOINE-ADMIN ».*



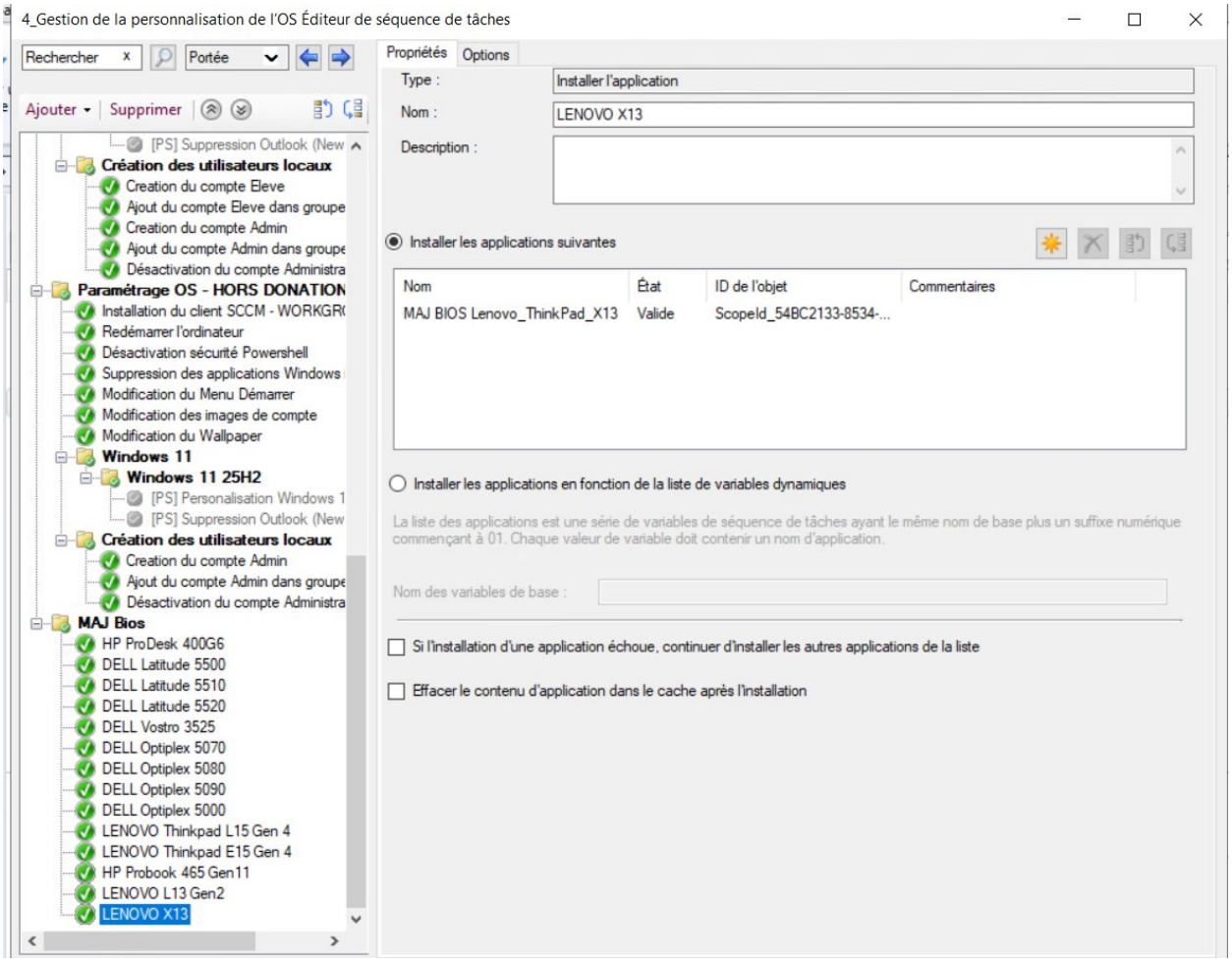
Annexe n°3 : *Aperçus des ports actifs du Switch Cisco « AVOINE-ADMIN ».*



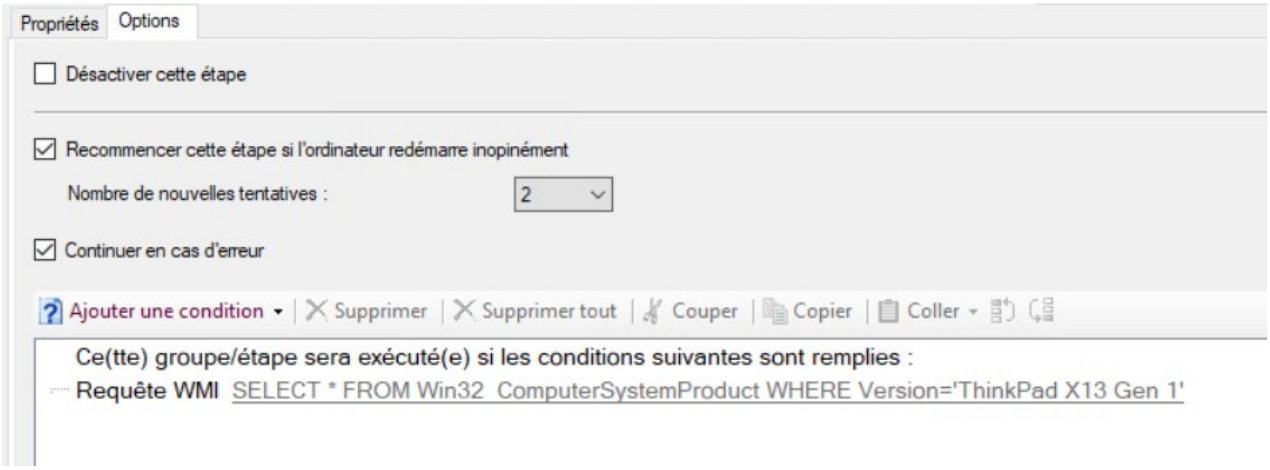
Annexe n°4 : *Aperçus du dossier « Bios » sur le logiciel MECM dans Bibliothèque de logiciels.*



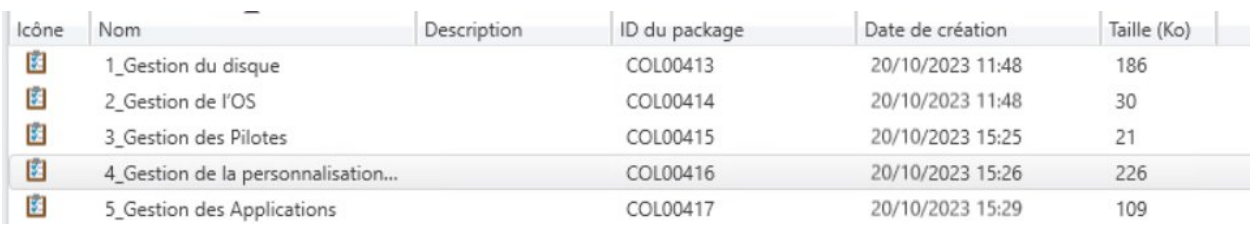
Annexe n°5 : *Aperçus de la tâche numéro 4, pour intégrer la séquence pour le Lenovo X13.*



Annexe n°6 : *Aperçus de la condition WMI pour valider la version du laptop Lenovo X13.*

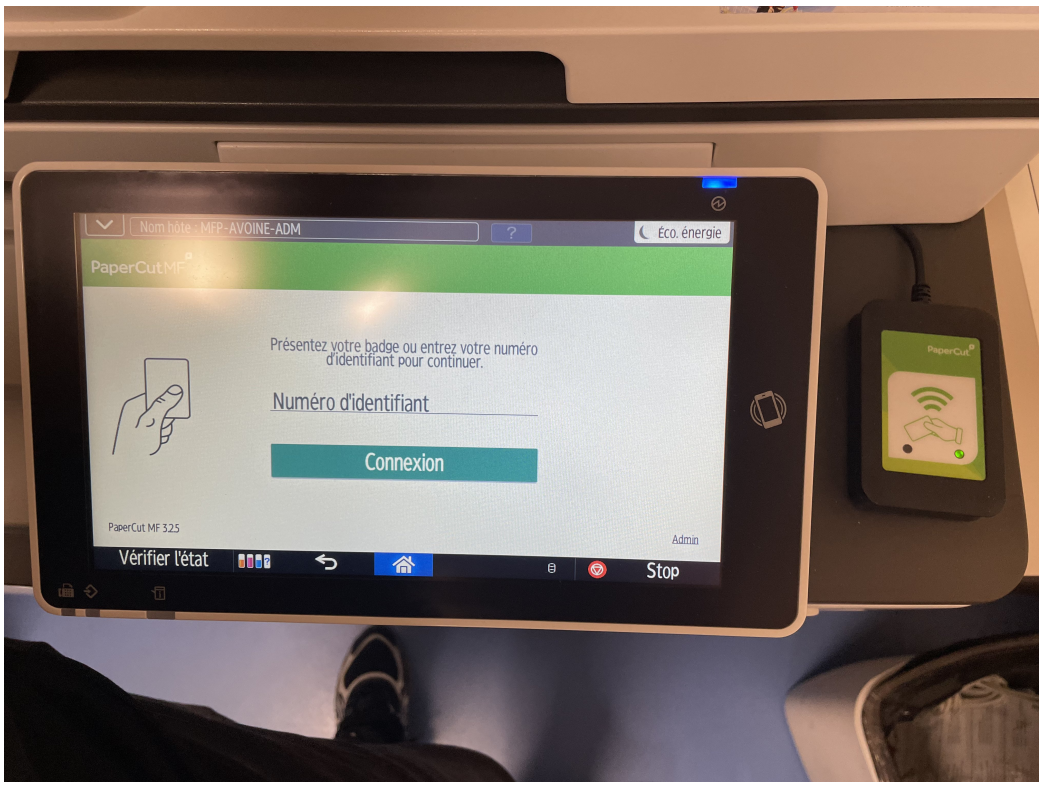


Annexe n°7 : *Ordre de séquence lors du déploiement via PXE.*

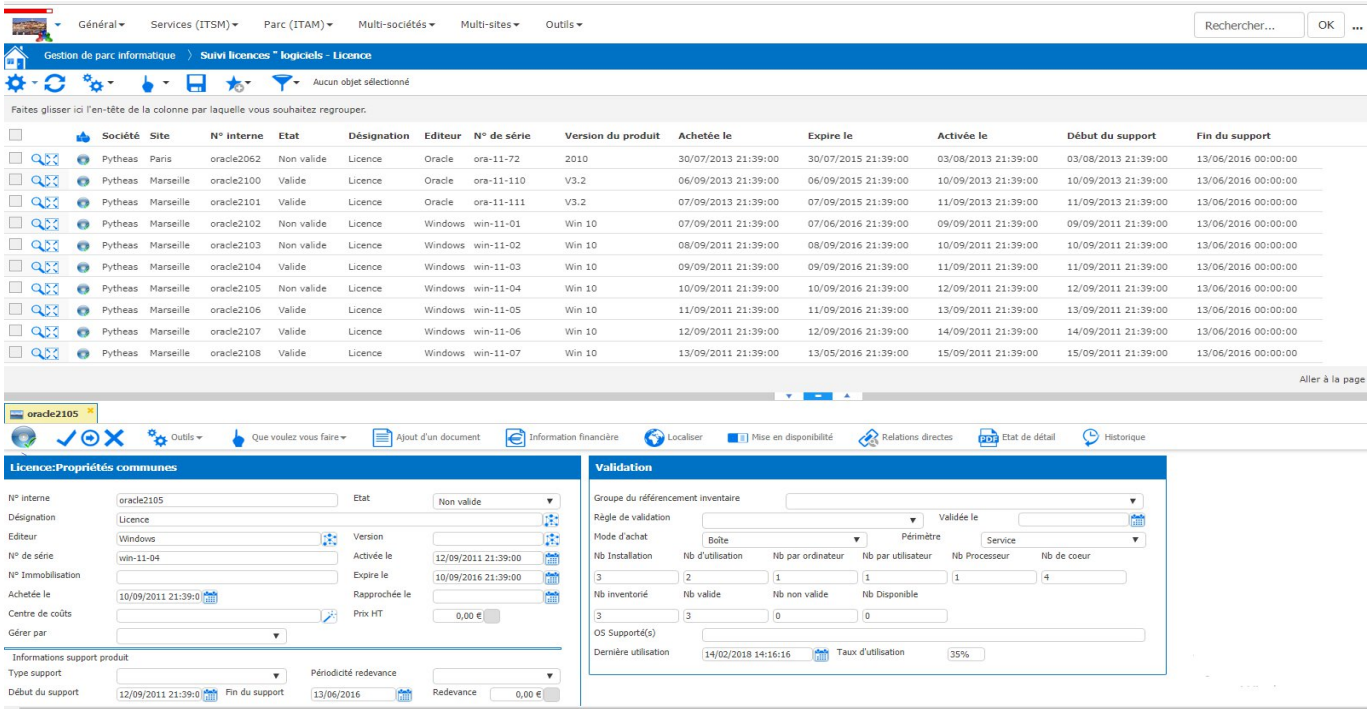


Icône	Nom	Description	ID du package	Date de création	Taille (Ko)
	1_Gestion du disque		COL00413	20/10/2023 11:48	186
	2_Gestion de l'OS		COL00414	20/10/2023 11:48	30
	3_Gestion des Pilotes		COL00415	20/10/2023 15:25	21
	4_Gestion de la personnalisation...		COL00416	20/10/2023 15:26	226
	5_Gestion des Applications		COL00417	20/10/2023 15:29	109

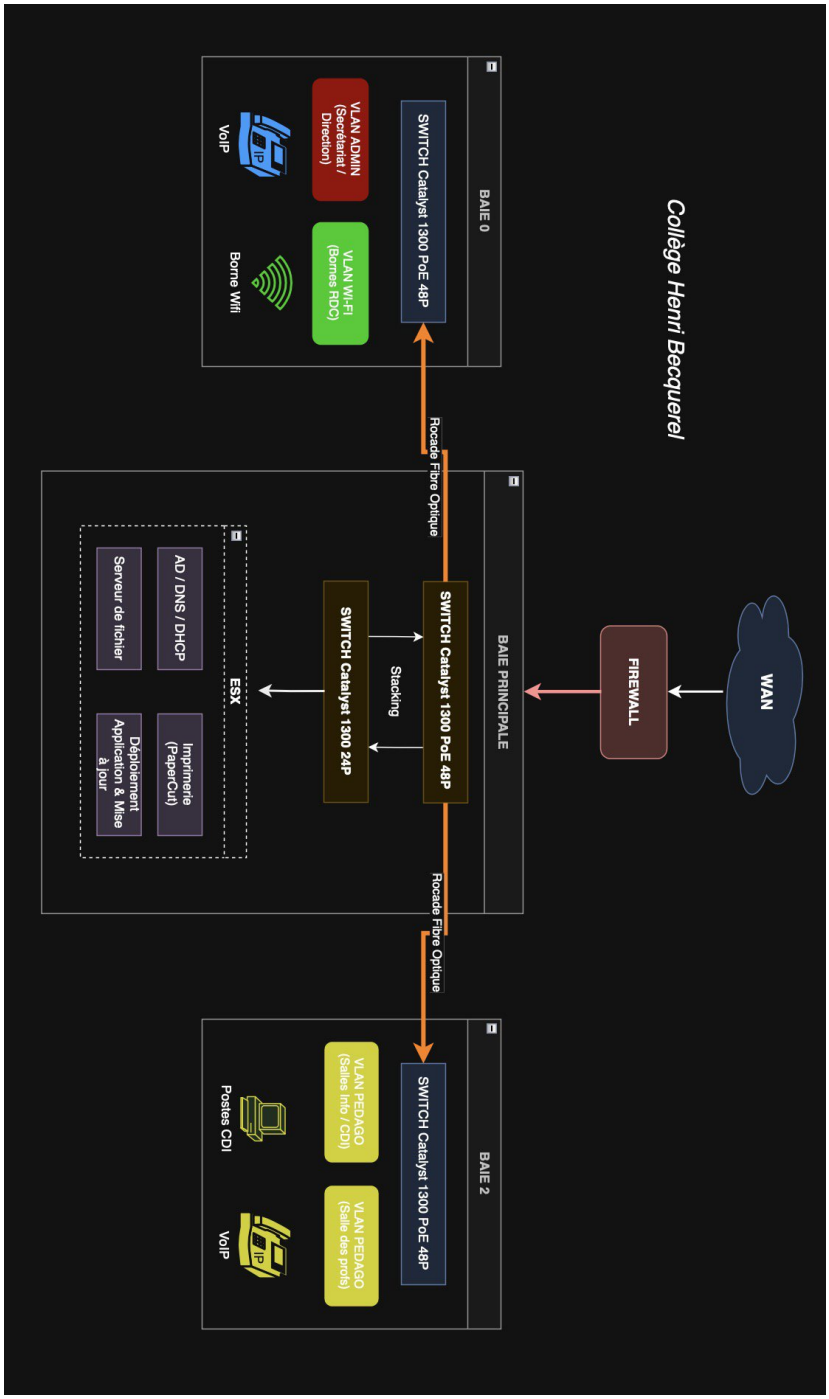
Annexe n°8 : *Image prise en photo d'une imprimante avec le système PaperCut.*



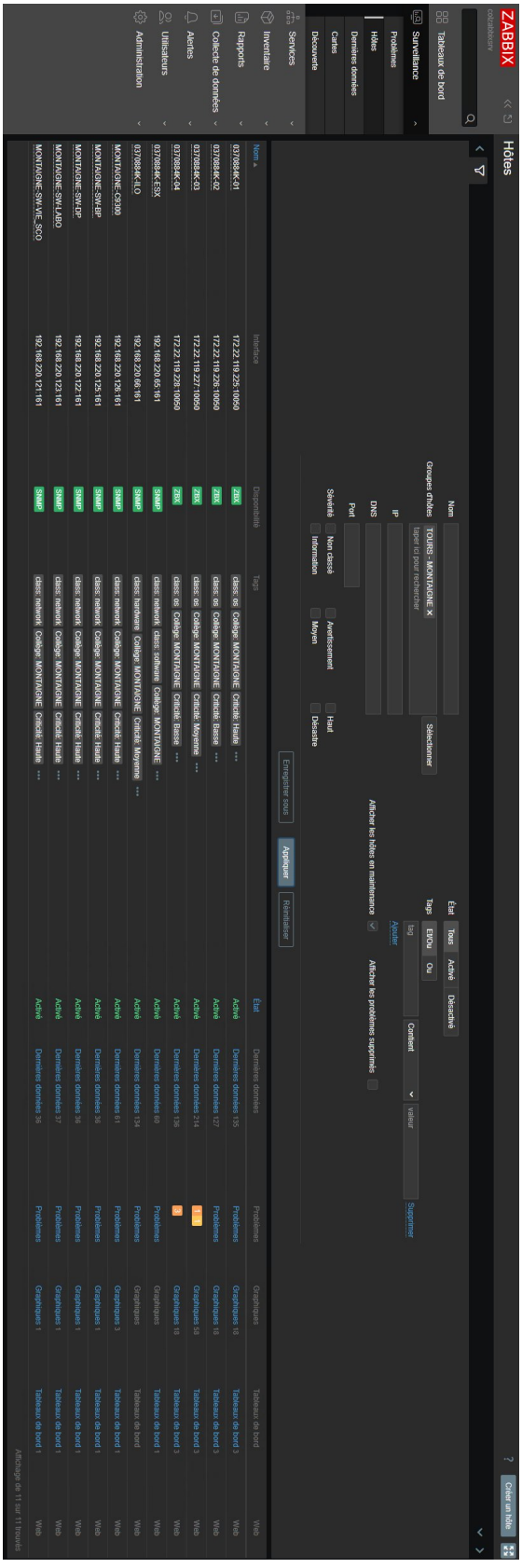
Annexe n°9 : *Exemple du logiciel PYTHEAS prise sur Google* (source : https://www.pytheas.com/img/cms/audit_logiciels.png).

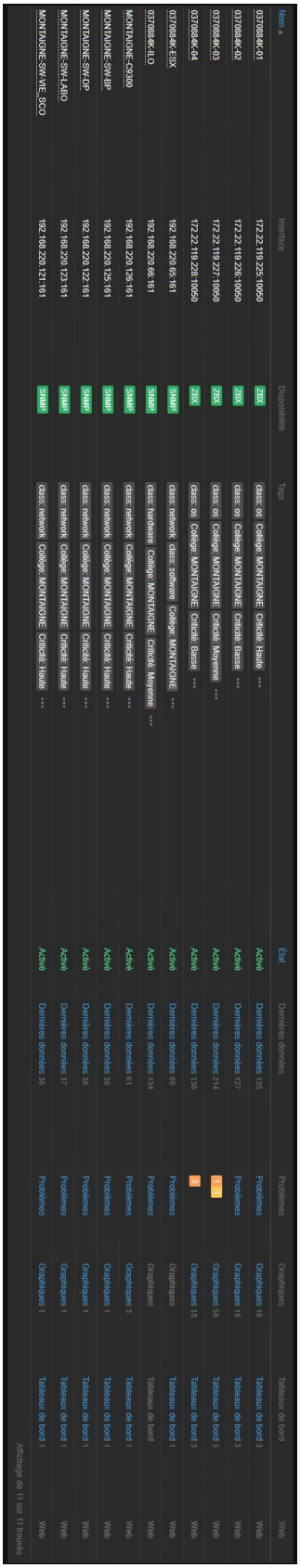


Annexe n°10 : *Constitution schéma technique des baie brassage du collège Henri Becquerel (Réaliser sur https://diagrams.net).*

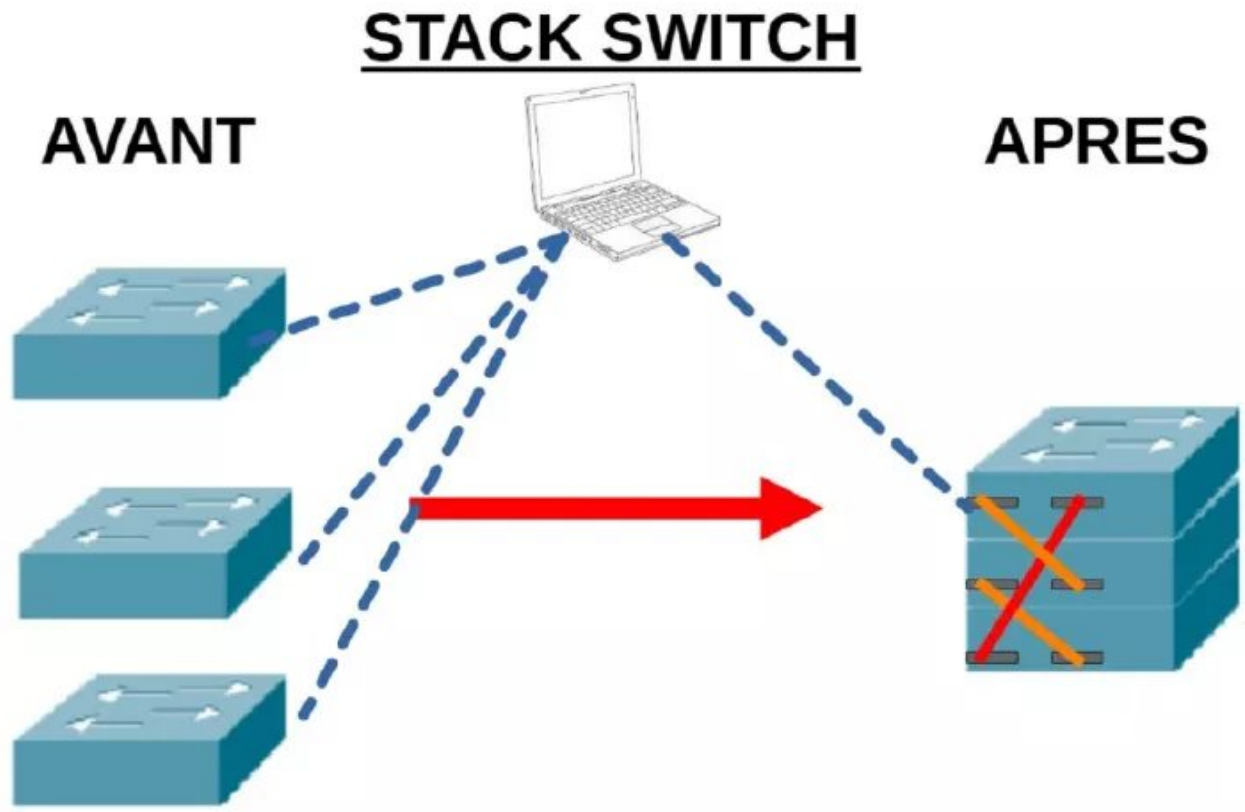


Annexe n°11 : *Exemple des hôtes en surveillances sur Zabbix du Collège Montaigne.*

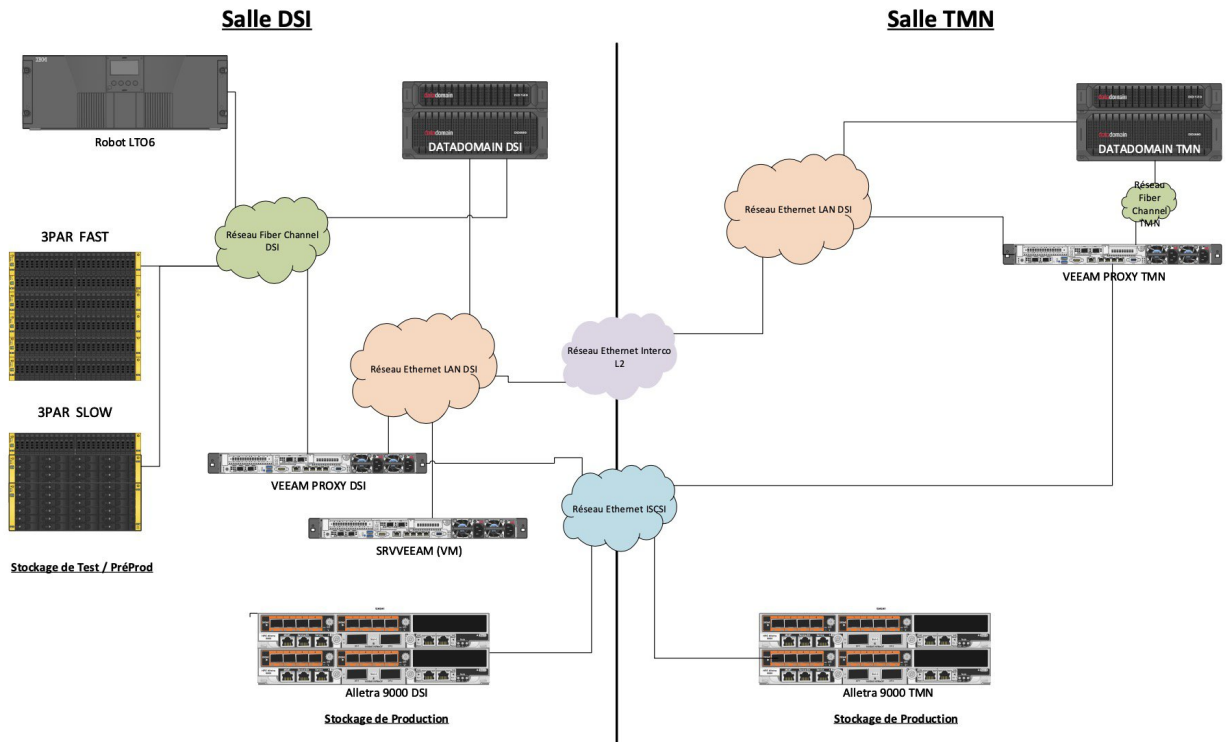




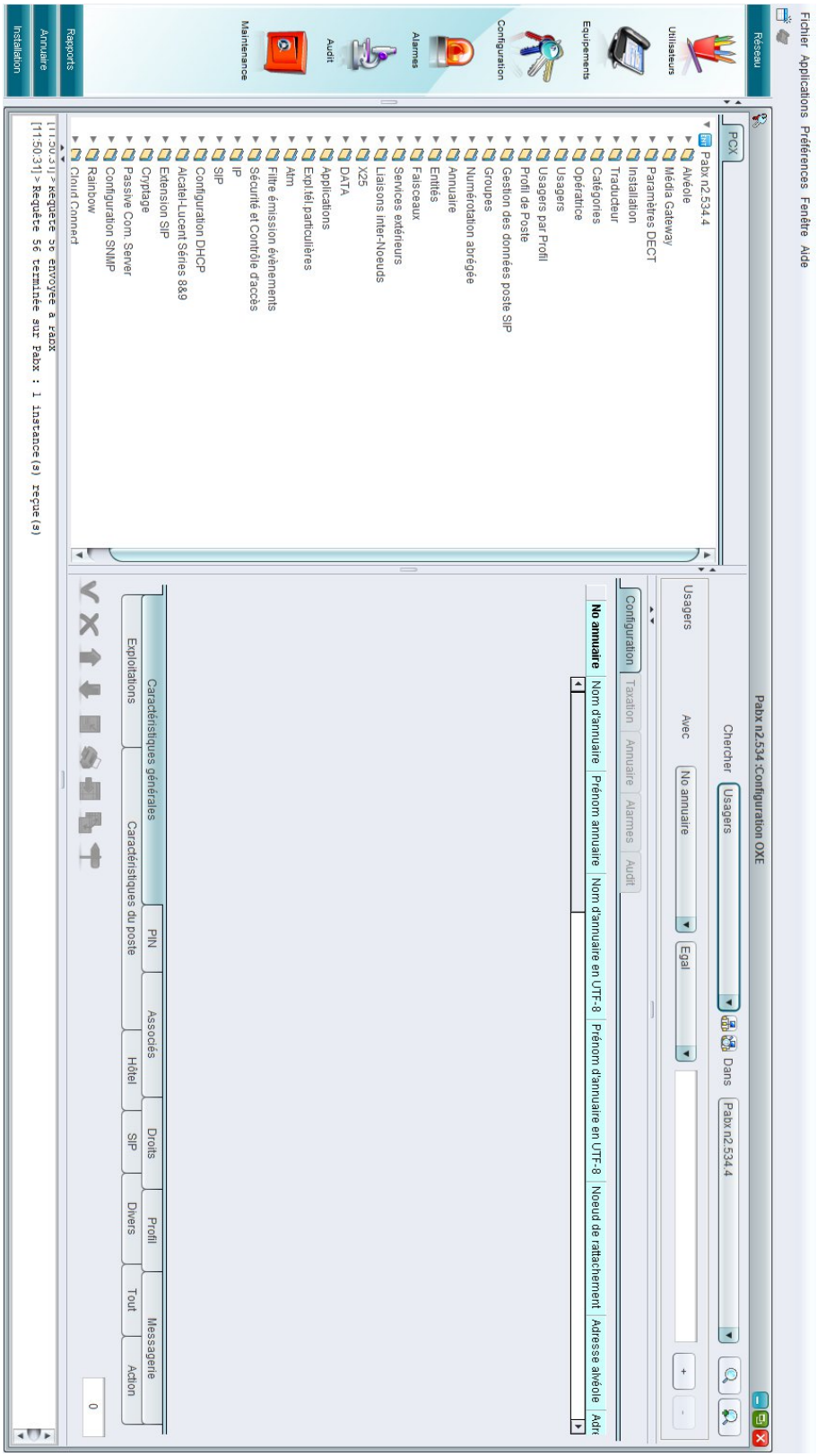
Annexe n°12 : *Schéma claire du fonctionnement du Stacking.*



Annexe n°13 : *Vu sur le schéma des deux salles serveurs en simple (DSI & TMN).*



Annexe n°14 : *Logiciel système de supervision des réseaux de communications.*



Annexe n°15 : *Charte de configuration des Switchs des collèges.*

La configuration des Switchs est standardisée pour tous les collèges afin de faciliter la maintenance et le dépannage. Les seuls éléments qui diffèrent sont :

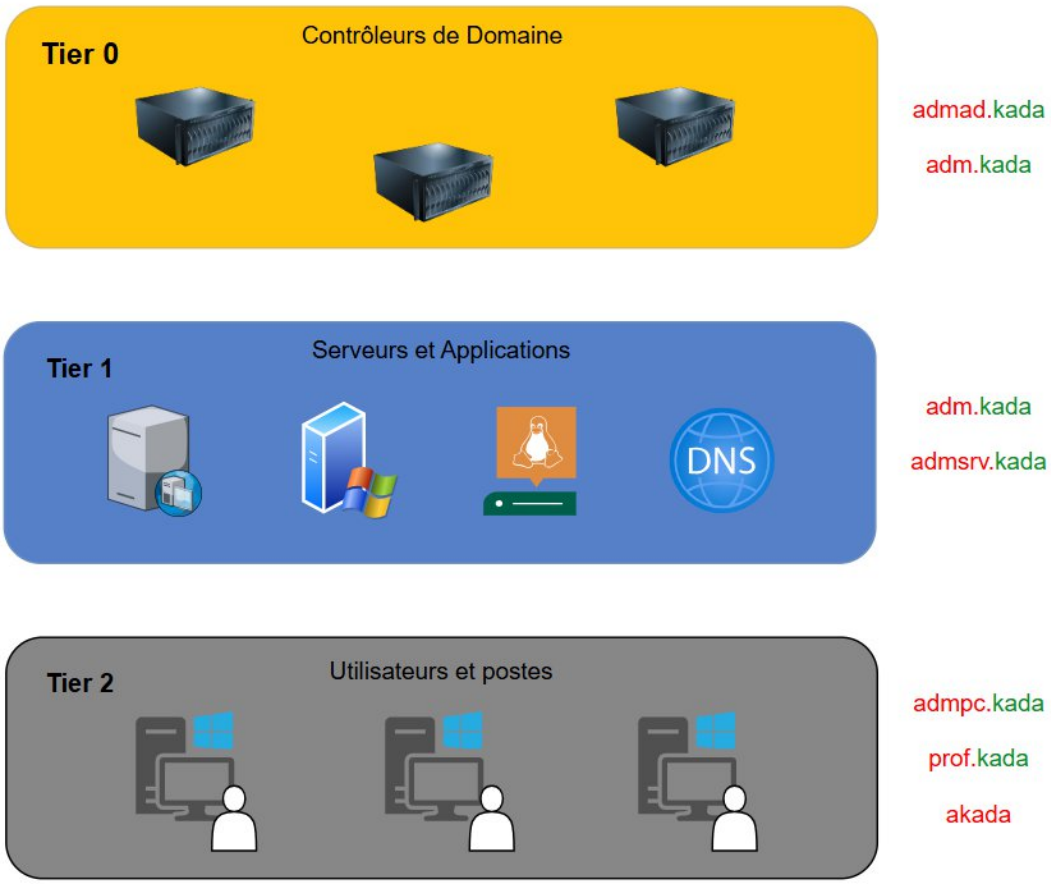
- Le nom de l'équipement (hostname)
- Les adresses IP (passerelle et VLAN de management)
- L'affectation des ports selon les besoins locaux

```
ssd-control-start
ssd config
ssd file passphrase control unrestricted
no ssd file integrity control
ssd-control-end cb0a3fdb1f3a1af4e4430033719968c0
cdp device-id format hostname
spanning-tree pathcost method short
vlan database
vlan 8,12-13,20-24,35,100
exit
voice vlan id 13
y
voice vlan state auto-enabled
voice vlan oui-table add 0001e3 Siemens_AG_phone
voice vlan oui-table add 00036b Cisco_phone
voice vlan oui-table add 00096e Avaya
voice vlan oui-table add 000fe2 H3C_Aolynk
voice vlan oui-table add 0060b9 Philips_and_NEC_AG_phone
voice vlan oui-table add 00d01e Pingtel_phone
voice vlan oui-table add 00e075 Polycom/Veritel_phone
voice vlan oui-table add 00e0bb 3Com_phone
errdisable recovery cause loopback-detection
errdisable recovery cause port-security
errdisable recovery cause dot1x-src-address
errdisable recovery cause acl-deny
errdisable recovery cause stp-bpdu-guard
errdisable recovery cause stp-loopback-guard
errdisable recovery cause udld
errdisable recovery cause storm-control
bonjour interface range vlan 1
qos wrr-queue wrtd
hostname XXXX-XX
encrypted radius-server host 192.168.xx.xx deadtime 2 key
Cwr0Y203driuSyNffSbV2/mAYdGHIoesE5F+NZIvnoE= usage login
ip http authentication aaa login-authentication https radius local
aaa authentication login login_radius radius local
aaa authentication enable login_radius radius enable
line ssh
login authentication login_radius
enable authentication login_radius
```

```
exit
ip ssh server
ip ssh logging enable
ip ssh password-auth
snmp-server server
snmp-server location XXXX-XX
snmp-server contact xxx@departement-touraine.fr
no snmp-server enable traps
no snmp-server trap authentication
snmp-server community cg37 rw view Default
clock timezone CET +1
clock summer-time CET recurring eu
sntp server 192.168.x.x poll
interface vlan 8
name adminstration
interface vlan 12
name impression
interface vlan 13
name telephonie
interface vlan 20
name pedago
interface vlan 21
name bornes_wifi
interface vlan 22
name invite
interface vlan 23
name ls
interface vlan 24
name eduroam
interface vlan 35
name gtc
interface vlan 100
name maintenance
ip address 192.168.x.x 255.255.x.x
ip dhcp snooping
ip dhcp snooping database
ip dhcp snooping information option allowed-untrusted
ip dhcp snooping vlan 1
ip dhcp snooping vlan 8
ip dhcp snooping vlan 12
ip dhcp snooping vlan 13
ip dhcp snooping vlan 20
ip dhcp snooping vlan 21
ip dhcp snooping vlan 22
ip dhcp snooping vlan 23
ip dhcp snooping vlan 24
ip dhcp snooping vlan 35
exit
ip default-gateway 192.168.x.x
```

```
 int range GigabitEthernet1/0/1-5
description pc_admin_tel
no spanning-tree portfast
Switchport mode trunk
Switchport trunk native vlan 8
Switchport trunk allowed vlan 8,13
 int range GigabitEthernet1/0/6-7
description pc_pedago
spanning-tree portfast
spanning-tree bpduguard enable
Switchport access vlan 20
 int range GigabitEthernet1/0/8
description imprimante
spanning-tree portfast
spanning-tree bpduguard enable
Switchport access vlan 12
```

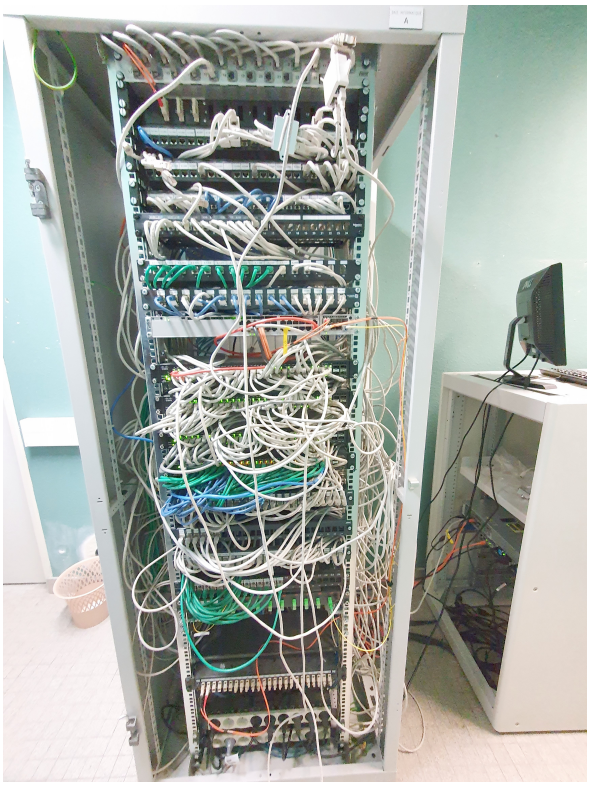
Annexe n°16 : *Tier Microsoft utiliser au Conseil Départemental, avec une authentification forte pour chaque compte (+4 comptes).*



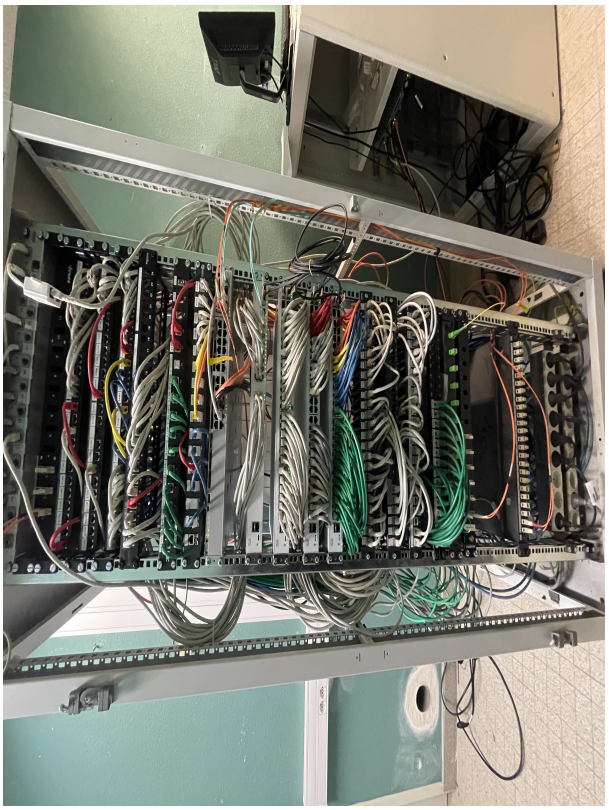
(Source : KADA Amine – By Draw.io)

Annexe n°17 : *Image d'une baie de brassage avant et après notre intervention.*

1. Avant



2. Après



Annexe n°18 : *Procédure MECM – CD37*

Intégration d'une image Windows

La première étape consiste à récupérer une image de Windows sur le site Microsoft. Cette image est téléchargée sous forme de fichier ISO. Une fois téléchargée, je l'ai copiée sur un serveur de l'entreprise afin qu'elle soit accessible par MECM.

Ensuite, j'ai extrait le contenu de ce fichier ISO pour récupérer le fichier WIM situé dans le dossier « sources ». Ce fichier correspond à l'image du système d'exploitation utilisée pour installer Windows sur les postes.

Dans la console MECM, je suis allé dans la partie « Bibliothèque de logiciels », puis dans « Systèmes d'exploitation » afin d'ajouter une nouvelle image. J'ai sélectionné le fichier WIM et choisi la version de Windows à utiliser.

Une fois l'image ajoutée, je l'ai distribuée sur les points de distribution pour qu'elle soit accessible aux machines du réseau. Cette étape est importante pour permettre le déploiement sur les différents ordinateurs.

J'ai ensuite utilisé une séquence de tâches, qui permet d'automatiser l'installation de Windows. Cette séquence réalise plusieurs actions comme l'installation du système et la configuration de base. J'ai testé cette opération sur une machine virtuelle pour vérifier que tout fonctionnait correctement.

Déploiement d'une application

J'ai également appris à déployer une application avec MECM. Pour cela, je suis allé dans « Bibliothèque de logiciels », puis « Gestion des applications », et enfin « Applications ».

J'ai créé une nouvelle application en renseignant les informations principales comme le nom, la version, l'éditeur et une description. Ces informations permettent de mieux organiser les applications dans l'outil et de les rendre compréhensibles.

Ensuite, j'ai configuré l'apparence de l'application dans le Centre logiciel, qui est l'interface utilisée par les utilisateurs. J'ai ajouté une description, des mots-clés ainsi qu'une icône pour rendre l'application plus claire.

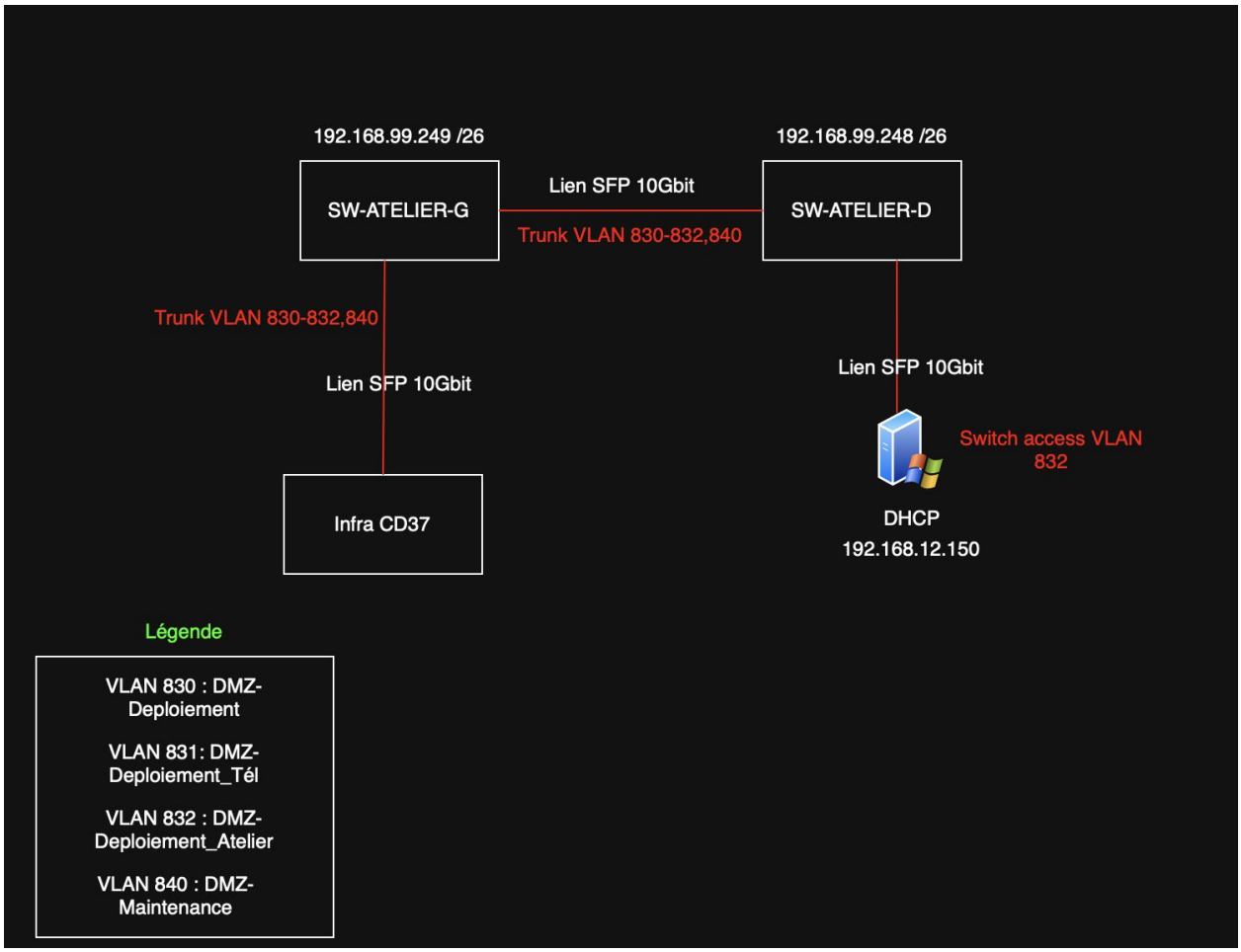
Après cela, j'ai défini le type de déploiement. Cela comprend le chemin vers les fichiers d'installation ainsi que les commandes permettant d'installer et de désinstaller l'application.

J'ai aussi configuré une règle de détection. Cette règle permet au logiciel de vérifier si l'application est déjà installée sur un poste, par exemple grâce à un fichier ou une clé de registre. Cela évite les erreurs d'installation.

Enfin, j'ai déployé l'application sur un groupe d'ordinateurs. Selon le paramétrage, elle peut être installée automatiquement ou laissée disponible dans le Centre logiciel pour que l'utilisateur puisse l'installer lui-même.

Annexe n°19 : *Schéma réseau de la nouvelle structure de l'atelier MECM.*

Pour sécuriser ce nouvel environnement, l'isolation logique de la DMZ de déploiement (VLAN 832) est gérée directement par les règles de filtrage du pare-feu Palo Alto, empêchant ainsi qu'un équipement de l'atelier puisse communiquer librement avec les serveurs de production du Conseil Départemental.



4. Glossaire Technique

1. Stockage et Sauvegarde

- **HPE Alletra 9060 / 3PAR (FAST & SLOW) :** Ce sont des baies de stockage d'entreprise. *Alletra* est une gamme très performante (souvent 100% Flash/NVMe). *3PAR* est l'ancienne génération ; "FAST" désigne des disques rapides (SSD/SAS) et "SLOW" des disques capacitifs plus lents (SATA/NL-SAS) pour le stockage de masse.
- **Robot LTO8 (Autoloader) :** Un système de sauvegarde sur bandes magnétiques (technologie LTO, génération 8). L'"Autoloader" est un bras robotisé qui insère et retire automatiquement les cartouches pour automatiser les backups longue durée ou hors ligne (air-gap).
- **DataDomain (Dell EMC) :** Une appliance matérielle de sauvegarde spécialisée dans la déduplication (suppression des données en double pour économiser énormément d'espace disque).
- **Veeam (SRV / Proxy) :** Logiciel de sauvegarde de référence. Le *SRV* (Serveur) gère les tâches. Le *Proxy* est un serveur intermédiaire qui s'occupe de traiter et compresser les données ("le muscle") pour ne pas surcharger le serveur principal.
- **SAN (Storage Area Network) :** Réseau haute performance dédié uniquement au stockage (mode bloc), séparé du réseau utilisateur.
- **Fibre Channel (FC) :** Le protocole réseau historique et ultra-rapide utilisé dans les réseaux SAN. Il nécessite des câbles et des Switchs spécifiques.
- **iSCSI :** Protocole permettant de faire transiter des commandes de stockage (SCSI) sur un réseau IP/Ethernet standard. C'est une alternative moins coûteuse au Fibre Channel.

2. Équipements et Concepts Réseau

- **Cisco Catalyst (9500 / 9300) :** Famille de commutateurs (Switchs) d'entreprise. Les *9500* sont très puissants et servent de "Cœur de réseau" (Core), tandis que les *9300* servent à distribuer la connexion vers les serveurs.
- **Cisco ASR (Aggregation Services Router) / ISR (Integrated Services Router) :** Gammes de routeurs Cisco. Les *ASR* sont conçus pour agréger de gros volumes de trafic à la frontière du réseau (edge/WAN). Les *ISR* sont des routeurs multiservices souvent utilisés pour les connexions de sites distants.
- **NRO (Nœud de Raccordement Optique) :** Point de concentration physique des fibres optiques d'un opérateur (ex: Orange, Axione) avant d'arriver chez le client.
- **Interco L2 (Interconnexion de niveau 2) :** Lien réseau direct permettant d'étendre un même réseau local (LAN/VLAN) entre deux sites physiques distants, comme s'ils étaient branchés sur le même Switch.
- **WAN (Wide Area Network) :** Réseau étendu (à l'échelle d'une région ou du pays), généralement fourni par des opérateurs télécoms pour relier les différents sites d'une entreprise.
- **BVPN (Business Virtual Private Network) :** Une offre opérateur (par Orange) fournissant un réseau privé virtuel inter-sites sécurisé, reposant généralement sur la technologie MPLS.
- **PABX IP** : C'est un autocommutateur téléphonique privé utilisant le protocole Internet pour gérer les appels téléphoniques d'une entreprise, en interne sur son réseau local.

3. Routage et Protocoles

- **GRE (Generic Routing Encapsulation) :** Un protocole permettant de créer un tunnel virtuel point à point pour encapsuler et transporter des paquets réseau à travers Internet ou un WAN.
- **BGP (Border Gateway Protocol) :** Le principal protocole de routage d'Internet et des très grands réseaux. Il permet aux routeurs d'échanger des informations sur les chemins disponibles pour atteindre d'autres réseaux.
- **VRF (Virtual Routing and Forwarding) :** Technologie permettant de créer plusieurs tables de routage indépendantes à l'intérieur d'un même routeur physique. Cela permet d'isoler totalement différents flux réseau (ex: isoler la ToIP de la DATA) de manière sécurisée.

4. Sécurité

- **Firewall Palo Alto :** Marque de pare-feu de nouvelle génération (NGFW) très réputée pour son inspection applicative profonde.
- **VSYS (Virtual Systems) :** Fonctionnalité spécifique à Palo Alto permettant de découper un pare-feu physique en plusieurs pare-feux virtuels totalement indépendants (avec leurs propres règles, interfaces et administrateurs).
- **DMZ (Demilitarized Zone) :** Sous-réseau isolé par le pare-feu. On y place les serveurs qui doivent être accessibles depuis l'extérieur (Internet), afin que s'ils sont piratés, le réseau interne (LAN) reste protégé. (Mais au Conseil Départemental, leur DMZ reste privé pas accessible de l'extérieur mais que de l'interne.)
- **NAT (Network Address Translation) :** Mécanisme modifiant l'adresse IP des paquets réseau. Souvent utilisé pour traduire une adresse IP privée interne en une adresse IP publique routable sur Internet.

5. Serveurs, Virtualisation et Applicatifs

- **VM ESX / VMware ESXi :** Hyperviseur dit "Bare-Metal" (Type 1) qui s'installe directement sur le matériel physique du serveur pour créer et faire tourner des machines virtuelles (VM).
- **ADFS (Active Directory Federation Services) / WS-Federation :** Service Microsoft permettant l'authentification unique (SSO). Il permet à un utilisateur de se connecter une seule fois avec son compte Windows (Active Directory) pour accéder à de multiples applications web, même externes.
- **Reverse Proxy :** Serveur placé devant des serveurs web internes. Il intercepte les requêtes venant d'Internet, les filtre (sécurité, répartition de charge), et les transfère au bon serveur interne.
- **Trunk SIP :** Connexion téléphonique sur IP (VoIP) reliant le système téléphonique de l'entreprise (PABX/IPBX) au réseau de l'opérateur télécom.
- **GTC (Gestion Technique Centralisée) :** Système informatique réseau permettant de superviser et contrôler les équipements techniques d'un bâtiment (chauffage, climatisation, alarmes, ascenseurs, etc.).

5. Conclusion Générale

Ce stage de 6 semaines au sein du service informatique des collèges du Conseil Départemental d'Indre-et-Loire a été une expérience extrêmement enrichissante et formatrice. Ce que j'ai particulièrement apprécié lors de cette immersion, c'est l'opportunité de travailler sur une infrastructure de très grande envergure (un parc réparti sur une cinquantaine de collèges) et de constater comment des concepts théoriques vus en cours sont appliqués industriellement en entreprise. L'autonomie qui m'a été accordée et les missions ont rendu chaque journée stimulante.

Sur le plan technique, ce stage m'a permis d'acquérir et de consolider de nombreuses compétences fondamentales pour un futur technicien système et réseau. J'ai pu manipuler des équipements professionnels (Cisco Catalyst) et appréhender des architectures complexes comme le Stacking et Radius. J'ai également découvert des outils de déploiement massif de niveau entreprise, tels que Microsoft Endpoint Configuration Manager (MECM), me permettant de gérer des mises à jour de BIOS et des migrations d'OS à grande échelle. Enfin, de la supervision via Zabbix m'a initié à la gestion générale d'un parc informatique, une compétence technique importante.

Sur le plan relationnel, cette expérience a été tout aussi bénéfique. L'intégration au sein de l'équipe informatique m'a permis de comprendre l'importance de la communication et de la coordination lors d'interventions critiques (comme la migration sans gêné les utilisateurs du collèges). J'ai appris à échanger avec des professionnels expérimentés, notamment mon tuteurs Julien TASSE, qui a su m'accompagner avec pédagogie. Ce stage a ainsi conforté mon choix d'orientation vers les métiers de l'infrastructure réseau et me donne une base solide pour aborder ma deuxième année de BTS SIO.