

Administrateur d'Infrastructures
Sécurisées 2024-2026

Mémoire de projet professionnel

Remplacement du serveur de fichiers
administratif dans les collèges et
lycées

Bryan Girault
Entreprise : GIP RECIA
Tutrice : Chloé Fonck

Table des matières

1. Remerciements	4
2. Glossaire	5
3. Résumé	6
4. Introduction	7
4.1. Présentation du candidat	8
4.2. Présentation de l'entreprise	9
4.2.1. Organigramme	11
4.2.2. Missions et objectifs de l'entreprise	12
4.2.3. Services proposés	13
4.3. Mon service	15
4.3.1. Activités du centre de services	16
4.3.2. Organigramme du service	17
4.3.3. Présentation de l'équipe	18
4.4. Mon rôle	19
4.4.1. Descriptif du poste	19
4.4.2. Outils utilisés	20
4.4.3. Périmètre d'intervention	22
4.4.4. Schéma infrastructure type	23
4.4.5. Missions confiées et activités quotidiennes	25
5. Projet : remplacement du serveur administratif dans les collèges et lycées	26
5.1. Contexte du projet	26
5.2. Méthodologie	27
5.3. Outils existants	28
5.4. Analyse des besoins	30
5.5. Environnement à disposition	31
5.6. Objectifs du projet	32
5.7. Les contraintes	34
5.8. Déroulement du projet (vue macro)	35
6. Solution retenue : intégration au domaine existant et adaptations pour le service administratif	36
6.1. Choix et argumentaire de la solution retenue	36

6.2.	Planning de réalisation	38
6.3.	Ressources nécessaires.....	39
6.4.	Les différentes phases de mon projet (vue micro).....	41
6.4.1.	Phase de tests et de validation	41
6.4.2.	Déploiement du serveur de fichiers SFADM	42
6.4.3.	Enquête sur les usagers administratifs	44
6.4.4.	Préparation de la migration administrative	46
6.4.5.	Migration des postes administratifs	48
6.4.6.	Déclassement de l'ancien serveur Horus	50
6.5.	Mise en production	51
6.6.	Problèmes rencontrés et solutions apportées	52
6.7.	Analyse rétrospective et bilan	53
7.	Difficultés rencontrées et solutions apportées.....	54
7.1.	Difficultés rencontrées	54
7.2.	Solutions apportées.....	55
8.	Conclusion	56
9.	Annexes	57
9.1.	Processus détaillé	57
9.1.1.	Etape 1 - déploiement du serveur de fichiers SFADM	57
9.1.2.	Étape 2 - Enquête administrative et rangement du serveur Horus.....	58
9.1.3.	Étape 3 - Préparation de la migration administrative.....	59
9.1.4.	Étape 4 - Migration des postes administratifs	61
9.1.5.	Etape 5 - Déclassement du serveur HORUS en Horus Light.....	63
9.2.	Avant/après la migration : captures d'écrans HORUS et SFADM.....	64
9.3.	Pendant la migration : enquête administrative	66
9.4.	Pendant la migration : Migration des postes administratifs	68
9.5.	FAQ Migration	71
9.6.	Matrice des partages dans les collèges et lycées	73
9.7.	Suivi du projet.....	75
9.8.	Planning	76

1. Remerciements

Je souhaite, en premier lieu, exprimer ma gratitude à l'ensemble de l'équipe pédagogique de la 2iAcademy, ainsi qu'aux formateurs, pour m'avoir donné l'opportunité d'intégrer cette formation et pour la qualité des enseignements dispensés tout au long de mon parcours.

Je remercie également le GIP Recia et l'ensemble de ses collaborateurs pour leur accueil et leur intégration au sein des équipes. J'adresse plus particulièrement mes remerciements à son directeur, Olivier Jouin, pour la confiance accordée et pour m'avoir permis de découvrir le fonctionnement du monde professionnel dans le domaine de l'informatique et du numérique.

Je tiens à remercier l'ensemble du service GSI pour l'accompagnement dont j'ai bénéficié durant ces deux années de formation. La diversité des compétences et des expertises présentes au sein de ce service m'a permis de développer et d'approfondir mes connaissances, aussi bien sur le plan technique que sur le plan humain.

Je remercie également les chefs de pôles des équipes IDMS et ISSR, Nicolas Lebrun et Antoine Guevara, ainsi que l'ensemble des membres de leurs équipes, notamment pour leur soutien lors des phases finales de mon projet. Leur accompagnement et leurs conseils ont été déterminants dans la mise en œuvre d'actions clés et dans la prise de décisions parfois complexes.

Je tiens à remercier particulièrement mes superviseurs, Clément Blondeau et Julien Marchand, ainsi qu'à ma tutrice, Chloé Fonck, pour leur disponibilité, leur pédagogie et leur accompagnement constant. Leur soutien m'a permis d'acquérir de nombreuses compétences et de progresser tant sur le plan professionnel que personnel.

2. Glossaire

802.1X : norme IEEE qui permet un contrôle d'accès centralisé en vérifiant l'identité des appareils avant de leur accorder l'accès au réseau, qu'ils soient filaires ou sans fil.

CD18 : Conseil Départemental du Cher.

CDS : Service Centre de Services.

Contrôleur de domaine de type NT : ancienne technologie Microsoft permettant la gestion centralisée des comptes et des authentifications avant l'apparition d'Active Directory.

ENT : (Environnement Numérique de Travail) : plateforme permettant l'accès aux services numériques et servant notamment de source d'identité pour les utilisateurs.

GFC : Applicatif administratif où ces archives sont conservées sur HORUS en mode « Horus light ».

GIP RECIA : Groupement d'intérêt public Région Centre Interactive (<https://www.recia.fr/>).

GSI : Service Gestion des Services Informatiques.

HORUS : ancien environnement administratif des établissements de l'Éducation nationale reposant sur un contrôleur de domaine de type NT et un serveur de fichiers historiquement administrés par le rectorat.

ISSR : Service Infrastructures, Sécurité, Systèmes et Réseaux.

ITSM : Service IT Service Management.

MAB : (MAC Authentication Bypass) : mécanisme d'authentification réseau permettant d'autoriser un équipement à partir de son adresse MAC lorsqu'il ne prend pas en charge le protocole 802.1X.

NAC : (Network Access Control) : mécanisme de contrôle d'accès réseau permettant d'autoriser ou de refuser la connexion des utilisateurs et équipements selon des règles définies.

OMICO : outil interne permettant l'alimentation et la gestion des identités au sein de l'annuaire centralisé à partir des données de l'ENT et de l'annuaire fédérateur.

OPSI : interface d'administration de la solution OPSI permettant le déploiement, la configuration, la mise à jour et l'inventaire des postes de travail.

RECOR : (Réseau de Coopération Optique Régional) : réseau optique régional reliant les sites de recherche, d'enseignement supérieur et les établissements d'enseignement secondaire de la Région Centre-Val de Loire afin de fournir des liaisons à très haut débit, sécurisées et à faible latence vers le DataCentre Régional et le réseau RENATER.

SFADM : (Serveur de Fichiers Administratif) : solution mise en place pour remplacer HORUS, intégrant le stockage administratif et l'authentification dans l'infrastructure actuelle.

SNE : équipe de proximité intervenant directement dans les établissements pour réaliser les opérations techniques sur site, accompagner les utilisateurs et assurer le déploiement des évolutions d'infrastructure. Dans le cadre du projet SFADM, les équipes SNE interviennent notamment lors des phases de migration des postes administratifs et de l'accompagnement des établissements.

3. Résumé

Ce mémoire présente le projet de migration du serveur administratif au sein des établissements scolaires Éducation Nationale. Ce projet, nommé [SFADM](#), s'inscrit dans une démarche de modernisation des infrastructures numériques et de renforcement de la sécurité des systèmes d'information (le serveur [HORUS](#), géré par le Rectorat, devenu obsolète).

Face à l'incompatibilité du serveur HORUS avec les nouvelles versions de Windows, à l'absence de maintenance depuis plusieurs années et aux exigences croissantes en matière de traçabilité et de protection des données, une nouvelle solution devait être mise en place. Le projet SFADM avait donc pour objectif de proposer une infrastructure fiable, sécurisée et centralisée, permettant une meilleure gestion des accès et des données administratives.

La mise en œuvre de ce projet a nécessité une analyse approfondie de l'existant, l'identification des besoins des utilisateurs et la prise en compte des contraintes techniques, organisationnelles et humaines. Plusieurs solutions ont été étudiées avant de retenir une architecture reposant sur des serveurs virtualisés, un Samba Active Directory centralisé et des mécanismes de sauvegarde éprouvés.

Le déploiement s'est appuyé sur une méthodologie progressive, intégrant des phases pilotes, des enquêtes auprès des établissements, des tests techniques et un accompagnement renforcé des utilisateurs. Une attention particulière a été portée à la continuité de service, afin de limiter l'impact des migrations sur l'activité quotidienne des personnels administratifs.

Ce mémoire présente enfin les choix techniques réalisés, les difficultés rencontrées et les solutions mises en œuvre, tout en mettant en évidence les compétences développées en administration d'infrastructures sécurisées et en gestion de projet dans le cadre du diplôme Administrateur d'Infrastructures Sécurisées.

4. Introduction

La transformation numérique des établissements publics constitue aujourd'hui un enjeu majeur pour les collectivités territoriales. Elle implique non seulement la modernisation des infrastructures techniques, mais également une adaptation des pratiques, une sécurisation accrue des données et une meilleure maîtrise des systèmes d'information. Dans un contexte marqué par l'évolution rapide des technologies et le renforcement des exigences réglementaires, les infrastructures historiques doivent être repensées afin de garantir performance, continuité de service et conformité aux normes de sécurité.

C'est dans ce cadre que s'inscrit le projet présenté dans ce mémoire. Le [GIP RECIA](#), acteur central du numérique public en région Centre-Val de Loire, accompagne les établissements scolaires dans la gestion et l'évolution de leurs infrastructures informatiques. Parmi les enjeux récents figurait le remplacement du serveur administratif [HORUS](#), devenu obsolète et incompatible avec les nouvelles versions des systèmes d'exploitation, notamment Windows 11. Cette situation a rendu nécessaire la mise en place d'une nouvelle solution, plus sécurisée, plus homogène et mieux intégrée à l'écosystème existant.

Le projet SFADM (Serveur de Fichiers Administratif) vise ainsi à moderniser l'environnement administratif des établissements, à renforcer la traçabilité des actions, à supprimer les comptes partagés et à garantir une meilleure gestion des accès aux données sensibles. Il s'inscrit dans une volonté plus large de standardisation des infrastructures et de reprise complète de la maîtrise du réseau administratif par la collectivité territoriale.

Dans le cadre de mon alternance au sein du pôle Gestion des Systèmes Informatiques du GIP RECIA, j'ai participé activement à ce projet, ce qui m'a permis de développer des compétences en administration système, en sécurité, en virtualisation et en gestion de projet. Ce mémoire présente le contexte, les enjeux, la méthodologie et le déroulement du projet SFADM, ainsi que les compétences professionnelles acquises.

4.1. Présentation du candidat



Je m'appelle Bryan Girault et je suis actuellement alternant en deuxième année du diplôme Administrateur d'Infrastructures Sécurisées (AIS) au sein de l'école 2iAcademy d'Orléans et du GIP RECIA.

Cette formation, suivie sur la période 2024–2026, vise à me préparer à exercer des fonctions dans l'administration, la sécurisation et l'exploitation des systèmes d'information. Elle repose sur une alternance entre enseignements théoriques et mise en pratique en milieu professionnel, me permettant d'acquérir des compétences techniques solides et directement opérationnelles.

Au sein du GIP RECIA, j'ai intégré le pôle Gestion des Systèmes Informatiques, et plus particulièrement le Centre de Services. Cette immersion dans un environnement professionnel exigeant m'a permis de participer à des projets structurants, de prendre en charge des missions variées et de développer une autonomie progressive dans l'exercice de mes fonctions.

Mon parcours d'alternant m'a conduit à intervenir sur des problématiques liées à l'administration des postes de travail, à la gestion des identités, à la supervision des infrastructures, à la sécurité des accès et à l'accompagnement des utilisateurs. Ces missions m'ont permis de renforcer mes capacités d'analyse, de rigueur et d'organisation, tout en développant un sens des responsabilités adapté au contexte professionnel.

Le projet SFADM s'inscrit pleinement dans cette dynamique de formation. Il constitue une expérience représentative des missions confiées à un Administrateur d'Infrastructures Sécurisées, mobilisant à la fois des compétences techniques, organisationnelles et relationnelles. À travers ce projet, j'ai pu consolider mon projet professionnel et confirmer mon intérêt pour les métiers de l'administration et de la sécurité des systèmes d'information.

4.2. Présentation de l'entreprise

Le Groupement d'Intérêt Public Région Centre InterActive (GIP RECIA) a été créé le 8 octobre 2003 afin d'accompagner les collectivités territoriales et les établissements publics de la région Centre-Val de Loire dans le développement et la gestion de leurs infrastructures numériques. Son siège est situé à Orléans, au cœur d'un territoire fortement engagé dans la mutualisation des services informatiques.

Le GIP RECIA intervient en partenariat avec la Région Centre-Val de Loire, les départements, les établissements scolaires, les centres de formation et de nombreux acteurs institutionnels. Son financement repose principalement sur la Région, avec le soutien de l'État et de l'Union européenne. Cette organisation lui permet de proposer des services mutualisés, adaptés aux besoins des acteurs publics et inscrits dans une logique de développement durable.



Au fil des années, le GIP RECIA s'est imposé comme un acteur central du numérique public régional. Il assure aujourd'hui la gestion et la supervision des infrastructures informatiques de plus de 180 établissements scolaires et de formation. Ses missions couvrent notamment l'administration des réseaux et des systèmes, l'hébergement sécurisé des données, la cybersécurité, la gestion des identités numériques, la supervision des équipements ainsi que l'accompagnement technique des établissements.

Il intervient également dans la coordination de dispositifs régionaux structurants, tels que l'Environnement Numérique de Travail, les annuaires fédérateurs et les plateformes collaboratives. Ces outils contribuent à l'harmonisation des pratiques numériques sur l'ensemble du territoire et à la sécurisation des échanges de données.

L'organisation du GIP RECIA repose sur plusieurs pôles spécialisés travaillant de manière complémentaire. Le pôle Gestion des Systèmes Informatiques, auquel je suis rattaché, assure l'administration et le maintien en condition opérationnelle des infrastructures. Les pôles [ISSR](#) et IDMS

apportent leur expertise en matière d'infrastructures, de sécurité et de gestion des postes de travail. Cette structuration favorise la transversalité des projets et la mutualisation des compétences.

Le modèle du GIP RECIA repose sur la mutualisation des ressources humaines, techniques et financières. Cette approche permet d'optimiser les coûts, de standardiser les architectures et d'élever globalement le niveau de sécurité des systèmes d'information. Elle facilite également la mise en œuvre de projets d'envergure, tels que le projet SFADM présenté dans ce mémoire.

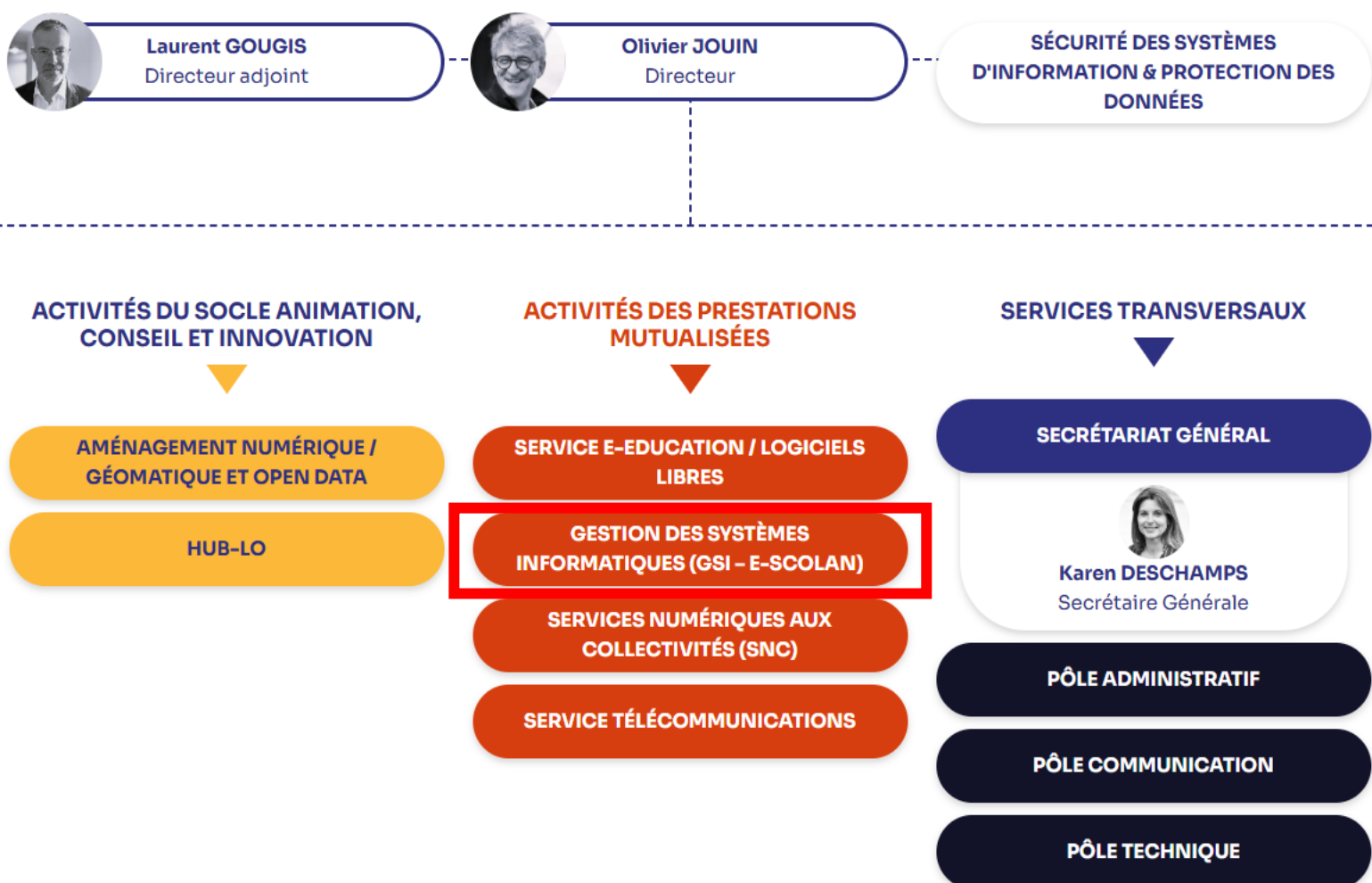
Dans un contexte marqué par l'évolution constante des technologies et des menaces informatiques, le GIP RECIA constitue un partenaire stratégique pour les établissements. Il contribue activement à la modernisation des infrastructures publiques et à la sécurisation durable des données administratives.



4.2.1. Organigramme

L'expertise des agents du GIP Recia, dans les réseaux informatiques, la programmation ou la télégestion à distance, ainsi que les infrastructures et outils numériques à sa disposition, leur permet de répondre à de nombreux enjeux techniques dans un large champ d'action : développement d'applications, audits, open data, inclusion numérique, outils de dématérialisation, protection des données, solutions matérielles pour les petites collectivités et les écoles, services informatiques mutualisés.

Dans ce cadre organisationnel, je suis intégré au pôle en charge de la Gestion des Systèmes Informatiques (GSI), qui intervient plus particulièrement sur l'administration, l'exploitation et le maintien en conditions opérationnelles des infrastructures informatiques du GIP RECIA.



4.2.2. Missions et objectifs de l'entreprise

Le GIP RECIA a pour mission principale d'accompagner les collectivités territoriales et les établissements publics de la région Centre-Val de Loire dans la gestion, la sécurisation et l'évolution de leurs systèmes d'information. Il intervient en tant qu'opérateur public de service numérique (OPSN), en mettant à disposition des infrastructures, des outils et des compétences spécialisées afin de répondre aux enjeux numériques du service public.

L'une de ses priorités est de garantir la continuité, la performance et la fiabilité des services informatiques proposés aux établissements. Cela implique la mise en œuvre d'architectures robustes, la supervision permanente des équipements et la maintenance des infrastructures. Le GIP RECIA veille également à assurer un haut niveau de sécurité, notamment à travers la gestion des accès, la protection des données sensibles et la conformité aux exigences réglementaires.

Le groupement a également pour objectif d'harmoniser les pratiques numériques sur l'ensemble du territoire régional. En proposant des solutions standardisées et mutualisées, il facilite l'administration à distance, améliore la réactivité du support technique et réduit les disparités entre les établissements. Cette homogénéisation contribue à une meilleure maîtrise des coûts et à une optimisation des ressources.

Par ailleurs, le GIP RECIA accompagne les établissements dans l'évolution de leurs usages numériques. Il participe à la mise en place d'environnements collaboratifs, d'outils pédagogiques et de services dématérialisés, favorisant ainsi la modernisation des pratiques professionnelles et administratives.

Le GIP RECIA s'inscrit dans une démarche d'amélioration continue. Il développe des projets structurants, tels que le projet SFADM, afin d'anticiper les évolutions technologiques, de renforcer l'autonomie des collectivités et de garantir la pérennité des infrastructures numériques. À travers ces actions, il contribue activement à la transformation numérique durable du territoire.

4.2.3. Services proposés

Le GIP RECIA propose une offre de services numériques large et structurée, conçue pour répondre aux besoins variés des acteurs publics de la région Centre-Val de Loire. Ces services s'inscrivent dans une logique de mutualisation et de cohérence territoriale, permettant aux collectivités et établissements accompagnés de bénéficier de solutions performantes tout en maîtrisant leurs coûts et leurs contraintes organisationnelles.

Une part importante des services du GIP RECIA concerne la mise à disposition et l'exploitation de solutions numériques destinées à soutenir les usages quotidiens des structures publiques. Cela inclut notamment des solutions logicielles adaptées aux besoins métiers, qu'il s'agisse d'outils de gestion, de plateformes collaboratives ou de services numériques dédiés au secteur éducatif et administratif. Ces solutions sont conçues pour être évolutives, interopérables et compatibles avec les exigences réglementaires du secteur public.

Le GIP RECIA intervient également dans le domaine des infrastructures et des télécommunications, en accompagnant les acteurs publics dans la conception, le déploiement et l'exploitation de leurs infrastructures réseau et systèmes. Ces services visent à garantir la disponibilité, la performance et la fiabilité des environnements numériques, tout en intégrant des exigences fortes en matière de sécurité et de continuité de service. Cette expertise permet aux structures accompagnées de s'appuyer sur des infrastructures adaptées à leurs usages actuels et futurs.

Les activités de conseil et d'accompagnement constituent un autre volet essentiel des services proposés. Le GIP RECIA apporte un appui méthodologique et technique aux collectivités et établissements dans la définition de leurs projets numériques, depuis les phases de réflexion et d'analyse jusqu'à la mise en œuvre opérationnelle. Cet accompagnement contribue à sécuriser les choix techniques et organisationnels, tout en favorisant la cohérence des projets à l'échelle du territoire.

Par ailleurs, le GIP RECIA assure des missions de maintenance et d'assistance afin de garantir la pérennité et le bon fonctionnement des services déployés. Ces interventions permettent d'assurer un suivi dans la durée, de répondre aux incidents et d'accompagner les utilisateurs dans l'appropriation des outils numériques mis à leur disposition. Cette dimension opérationnelle est essentielle pour maintenir un niveau de service conforme aux attentes des structures publiques.

Le GIP RECIA s'inscrit dans une dynamique d'innovation à travers des actions de recherche et développement, ainsi que par l'animation du territoire numérique régional. En favorisant l'expérimentation, le partage d'expériences et la coopération entre acteurs, il contribue à faire émerger de nouveaux usages et à accompagner l'évolution des services publics numériques. L'ensemble de ces services positionne le GIP RECIA comme un acteur central de l'écosystème numérique régional, capable de répondre de manière globale et cohérente aux enjeux actuels et futurs des territoires.

Solutions logicielles

- Environnement Numérique de Travail (ENT) pour les écoles-collèges-lycées
- E-Administration



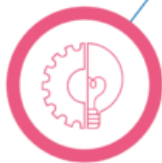
Conseils & Accompagnement

- Protection des données (Conformité RGPD)
- DSI mutualisée
- Cybersécurité



Recherche & Développements

- Innovation
- Logiciels libres
- Expérimentations
- Projets spécifiques



Infrastructures & Télécommunications

- Conception et urbanisation des infrastructures
 - Réseaux fibre optique (ReCOR)
 - Accès internet (RRHD)
 - Téléphonie mobile



Animation du territoire

- Stratégies numériques régionales (SCORAN)
- Réseau régional des données territoriales (DoTeRR) et géomatique (GéoCentre)
 - Inclusion et médiation numérique (Hub-Lo)
 - Open data



Maintenance & Assistance

- Supervision et maintenance des systèmes informatiques et des postes de travail
- Déploiement de solutions logicielles et maintenance applicative
 - Centre d'appels et assistance
 - Maintenance de proximité
- Centre de réponses aux incidents cyber (CSIRT)

ACTIVITÉS ET SERVICES DU GIP RECIA

4.3. Mon service

Je suis rattaché au pôle Gestion des Systèmes Informatiques (GSI), qui constitue le cœur opérationnel de l'administration des infrastructures des établissements scolaires et de formation. Ce pôle regroupe l'ensemble des compétences nécessaires à la gestion, à la sécurisation et à l'évolution des systèmes d'information des établissements.

Le pôle GSI est organisé autour de trois services complémentaires.

- Le Centre de Services (CDS) assure supervision des infrastructures et la relation quotidienne avec les utilisateurs, il constitue le point d'entrée principal pour les sollicitations.
- Le service Infrastructures, Sécurité, Systèmes et Réseaux (ISSR) est chargé de la conception, du déploiement et de la sécurisation des infrastructures techniques.
- Le service Intégration, Déploiement et Maintenance des Stations (IDMS) intervient sur la gestion des environnements de travail : le développement des paquets applicatifs, la configuration des environnements et la maintenance des parcs informatiques, ainsi que des tablettes

Ces trois services travaillent en étroite collaboration afin d'assurer une prise en charge complète des besoins des établissements. Cette organisation permet de traiter efficacement les problématiques, depuis le signalement d'un incident jusqu'à sa résolution technique.

Dans le cadre de mon alternance, j'ai intégré le Centre de Services, ce qui me place au contact direct des utilisateurs et des équipes techniques spécialisées. Cette position me permet d'avoir une vision globale du fonctionnement des infrastructures, tout en participant activement à leur exploitation.

Mon rattachement au [CDS](#) m'amène à collaborer régulièrement avec les équipes ISSR et IDMS, notamment dans le cadre de projets transversaux tels que le projet SFADM. Cette collaboration favorise le partage des connaissances et l'amélioration continue des pratiques professionnelles.

Mon service constitue un maillon essentiel dans l'organisation du GIP RECIA, en assurant la continuité de service, la qualité du support et la coordination des actions techniques.



50 000 postes
de travail



500 serveurs
physiques



3000 machines
virtuelles



15000 matériels
réseaux
(commutateur, ap-
wifi, autres dispositifs
techniques...)



3500 imprimantes

4.3.1. Activités du centre de services

Le Centre de Services du GIP RECIA constitue le point d'entrée principal pour l'ensemble des établissements accompagnés dans la gestion de leurs infrastructures informatiques. Il assure un rôle central dans le support opérationnel, la supervision et l'accompagnement quotidien des utilisateurs, en garantissant la continuité et la qualité des services numériques.

La mission principale du Centre de Services consiste à prendre en charge les sollicitations formulées par les utilisateurs. Les sollicitations sont prises en charges sur l'application ITSM iTop, de l'éditeur Combodo, les utilisateurs peuvent les ouvrir par le portail web, mail ou par téléphone. Chaque demande fait l'objet d'un enregistrement, d'une qualification et d'un suivi rigoureux, permettant d'assurer une traçabilité complète des interventions. Les techniciens analysent les problématiques rencontrées, réalisent les premiers diagnostics et apportent des solutions adaptées, ou orientent les dossiers vers les équipes spécialisées lorsque cela s'avère nécessaire.

Le traitement des incidents de supervision est également une tâche réalisée par le Centre de Services. L'équipe utilise l'application Icinga pour la supervision de l'infrastructure. Les équipes sont en mesure de détecter rapidement les anomalies ou les dysfonctionnements. Cette supervision proactive permet d'anticiper certains incidents avant qu'ils n'impactent les utilisateurs, contribuant ainsi à maintenir un haut niveau de disponibilité des services.

La gestion des accès et des identités constitue un autre axe majeur des activités du Centre de Services. Les équipes participent à la création, à la modification et à la suppression des comptes utilisateurs, en lien avec les outils de gestion centralisée tels que [OMICO](#) (production interne) et le Samba Active Directory. Elles veillent à l'application du principe du moindre privilège, en attribuant aux utilisateurs uniquement les droits nécessaires à leurs fonctions. Cette démarche contribue à renforcer la sécurité des infrastructures et à limiter les risques liés aux usages inappropriés.

Le Centre de Services intervient également dans la gestion du parc informatique. Il assure le suivi des postes de travail, la mise à jour des systèmes d'exploitation, le déploiement des logiciels et au diagnostic des pannes (logicielles ou matérielles). À l'aide de l'outil [OPSI](#) (éditeur UIB), les équipes peuvent automatiser certaines opérations et intervenir à distance, ce qui permet d'optimiser les délais de traitement et de réduire les déplacements sur site.

Par ailleurs, le service participe activement aux projets d'évolution des infrastructures, en collaboration avec les pôles ISSR et IDMS. Il intervient notamment lors des phases de test, de déploiement et de mise en production des nouvelles solutions. Dans le cadre du projet SFADM, par exemple, le Centre de Services a joué un rôle essentiel dans la communication avec les établissements, le suivi des enquêtes administratives, l'assistance lors des migrations et la gestion des incidents liés au changement d'environnement.

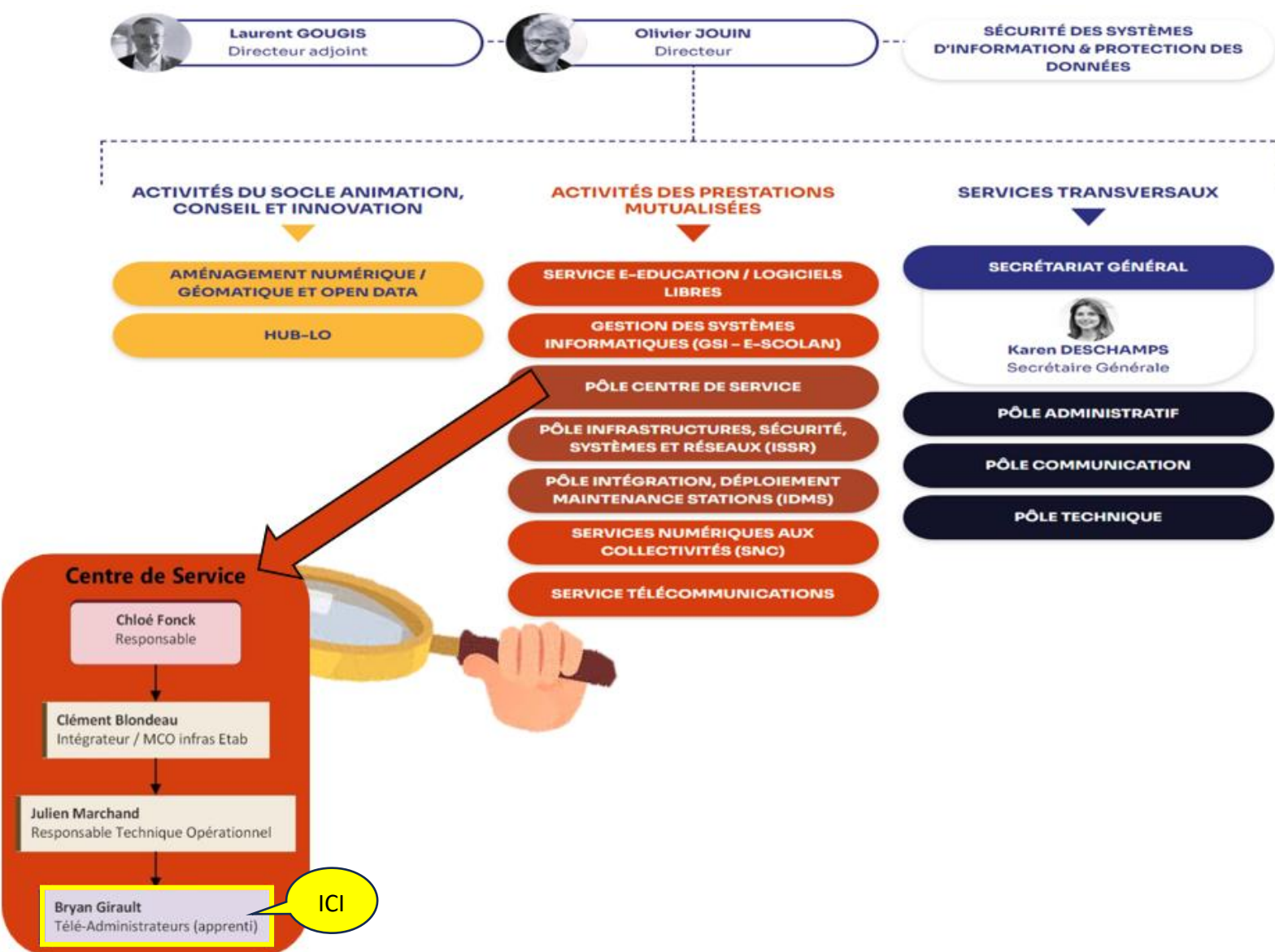
Le service s'inscrit dans une démarche d'amélioration continue. Les retours des utilisateurs, l'analyse des incidents récurrents et le suivi des indicateurs de performance permettent d'optimiser les processus internes et d'adapter les méthodes de travail. Cette dynamique contribue à renforcer l'efficacité du service et à améliorer durablement la qualité du support proposé aux établissements.

QUELQUES CHIFFRES

- 1 600 sollicitations / mois
- 80% des résolutions sont réalisées à distance

4.3.2. Organigramme du service

L'organigramme ci-dessous présente l'organisation du Centre de Services ainsi que les différents rôles et niveaux de responsabilité au sein du service.



4.3.3. Présentation de l'équipe

Au sein du GIP RECIA, j'évolue dans le Centre de Services, une équipe organisée afin d'assurer le support, l'administration et le maintien en conditions opérationnelles des infrastructures numériques. Son rôle est d'assurer l'interface entre les utilisateurs et les équipes techniques tout en garantissant la disponibilité et la qualité des services.

L'équipe est composée des fonctions suivantes :

- **Responsable de service**
Assure le pilotage global de l'activité, le suivi des indicateurs, l'organisation des ressources et le respect des engagements de service.
- **Intégrateur**
Intervient sur les sujets techniques complexes, participe au maintien en conditions opérationnelles des infrastructures et accompagne l'intégration des évolutions dans les environnements existants.
- **Responsable technique opérationnel**
Coordonne les activités techniques quotidiennes, accompagne les équipes sur les problématiques opérationnelles et assure le suivi des interventions.
- **Télé-administrateurs** (environ une dizaine de collaborateurs)
Prennent en charge le support aux utilisateurs, le traitement des incidents et demandes, les opérations d'administration courante ainsi que le suivi des alertes issues de la supervision. Ils interviennent également dans les projets d'évolution des infrastructures et collaborent avec les autres pôles du GIP RECIA.

J'exerce mes missions au sein de cette équipe en tant qu'apprenti télé-administrateur. Cette organisation me permet de participer aux activités opérationnelles du service tout en bénéficiant d'un accompagnement technique favorisant ma montée en compétences et le développement d'une vision globale des infrastructures administrées.

4.4. Mon rôle

4.4.1. Descriptif du poste

J'occupe le poste d'apprenti télé-administrateur dans le cadre de ma formation d'Administrateur d'Infrastructures Sécurisées. Cela consiste à une participation active aux activités de support, d'administration et de supervision des infrastructures informatiques des établissements.

Au quotidien, je prends en charge les demandes et incidents signalés par les utilisateurs via l'outil de ticket ou par téléphone. Cette mission comprend l'analyse et le diagnostic des problématiques rencontrées, l'identification de leur origine ainsi que l'application des procédures adaptées afin de rétablir le fonctionnement des services. Elle implique également la réalisation d'actions techniques, le suivi des interventions, la mise à jour ou la création de documentations techniques et l'accompagnement des utilisateurs jusqu'à la résolution complète des incidents. Les sollicitations concernent notamment les accès aux services, les postes de travail, les ressources réseau, les droits utilisateurs et les environnements serveurs.

Je participe également à des actions d'administration système et réseau, telles que la configuration des équipements, la gestion des accès par authentification ou encore la mise à jour des informations dans les outils de gestion. J'interviens également dans le traitement et la correction des alertes remontées par les outils de supervision concernant les équipements réseau et les serveurs. Dans le cadre du maintien en conditions opérationnelles, je participe au suivi des mises à niveau des systèmes d'exploitation à l'aide d'outils d'industrialisation et d'automatisation. Je suis aussi amené à développer ou adapter des scripts, notamment en PowerShell ou en Bash, afin de corriger certaines configurations, automatiser des actions techniques ou faciliter les opérations d'administration. Ces interventions contribuent directement au maintien en conditions opérationnelles et à la sécurisation des infrastructures.

Dans le cadre de projets transversaux, notamment le projet SFADM, j'interviens sur des environnements virtualisés, j'applique des procédures de migration et je communique avec les autres équipes sur l'avancement. Ces missions me permettent de développer une vision globale des systèmes d'information et de renforcer mes compétences techniques.

Mon poste exige rigueur, autonomie, sens de l'organisation et une capacité à communiquer efficacement avec les utilisateurs. Il implique également une forte responsabilité dans la gestion des accès et des données. Ces missions correspondent parfaitement au rôle d'Administrateur d'Infrastructures Sécurisées, car elles me placent au centre des défis liés à l'efficacité, à la protection et à la disponibilité des systèmes.

Mon poste m'amène également à intervenir sur certains aspects liés aux infrastructures réseau et aux mécanismes de contrôle d'accès. Je peux notamment réaliser des configurations sur les équipements de commutation, participer au suivi des authentifications réseau [802.1X](#) avec [MAB](#) (MAC Address Bypass) ou encore vérifier la conformité des équipements autorisés à accéder aux différents environnements. Ces missions renforcent ma compréhension des enjeux liés à la sécurisation des accès, à la segmentation réseau et à la continuité de service au sein des infrastructures administrées.

4.4.2. Outils utilisés

J'utilise au quotidien les différents outils d'administration, de supervision et de gestion des infrastructures informatiques. Ces solutions permettent d'assurer le maintien en conditions opérationnelles des équipements, la sécurisation des accès, le support aux utilisateurs ainsi que le suivi des infrastructures déployées dans les établissements accompagnés.

Systèmes d'exploitation :

- **50 000 Windows 10/11 et Linux** : systèmes d'exploitation des postes utilisateurs.
- **500 Serveurs Linux** : gestion des services d'infrastructure (Samba Active Directory, partages de fichiers, services réseau, etc.).
- **3000 Machines virtuelles Linux** : hébergement des services virtualisés des établissements.

Outils de supervision :

- **Icinga** : supervision proactive des équipements systèmes et réseaux (13630 équipements) , détection des anomalies et suivi de l'état des services (36292 services).

Outils de virtualisation :

- **Proxmox** : gestion des serveurs physiques et des machines virtuelles en production.

Équipements réseau :

- **180 OPNsense DEC750/DEC3800** : pare-feu assurant le filtrage, la sécurisation et le routage des flux réseau.
- **1500 Aruba 2930F** : commutateurs d'accès pour la distribution réseau.
- **2500 HPE 5130** : commutateurs cœur/distribution, supportant notamment la téléphonie.
- **1000 Cisco 2960** : commutateurs d'accès pour la connectivité des postes.
- **3500 imprimantes** : équipements d'impression administrés
- **8000 Bornes wifi** : équipements assurant la couverture réseau sans fil des établissements.

Outils de gestion de parc :

- **OPSI** : déploiement des postes, installation et mise à jour des logiciels, prise en main à distance et automatisation des actions d'administration.

Outils de gestion des identités et des accès :

- **OMICO** : création et alimentation des comptes utilisateurs (environ 150 000 comptes) à partir de l'annuaire fédérateur.
- **ra-ad-tools** : gestion des objets Samba Active Directory.
- **ENT** : gestion des comptes et des accès utilisateurs.

Outils de sécurité réseau et postes :

- **PacketFence** : contrôle d'accès au réseau via [802.1X](#) et [MAB](#).
- **WithSecure** : protection des postes et détection des menaces.

Outils de support et de gestion des incidents :

- **iTop** : gestion des tickets (environ 1600 sollicitations par mois) et CMDB, suivi des demandes et incidents.

Outils de communication :

- **Thunderbird** : messagerie interne.
- **3CX** : téléphonie pour la prise d'appels.

Outils de documentation :

- **XWiki** : documentation technique et procédures internes.

4.4.3. Périmètre d'intervention

J'interviens au sein du Centre de Services, dont le périmètre couvre un large ensemble d'établissements scolaires et de formation répartis sur le territoire régional. Le service assure l'accompagnement informatique de 180 établissements, comprenant les lycées publics et agricoles de la Région Centre-Val de Loire, l'ensemble des collèges du département du Cher, des écoles de formations sanitaires et sociales, ainsi que sept centres de formation d'apprentis adhérents au dispositif. Cette diversité d'établissements implique une grande hétérogénéité des environnements informatiques et des usages, nécessitant une capacité d'adaptation permanente.

Dans ce cadre, mes interventions portent sur un périmètre technique varié, couvrant à la fois les infrastructures centrales et les équipements déployés dans les établissements. Les actions réalisées concernent notamment les serveurs virtualisés hébergeant les services d'infrastructure, les postes de travail sous Windows et Linux ainsi que les équipements utilisés quotidiennement par les utilisateurs. Les imprimantes réseau, les bornes Wi-Fi et les commutateurs assurant la connectivité des établissements font également partie des éléments administrés et supervisés.

Ce périmètre nécessite une compréhension globale des infrastructures systèmes et réseaux, ainsi qu'une bonne maîtrise des interactions entre les différents services informatiques. Il implique également de prendre en compte les enjeux liés à la sécurité, à la disponibilité des services et au maintien en conditions opérationnelles des équipements. La diversité des environnements rencontrés m'amène à intervenir sur des problématiques techniques variées et à adapter les méthodes d'administration en fonction des contraintes propres à chaque établissement.

4.4.4. Schéma infrastructure type

L'infrastructure réseau type d'un établissement administré par le GIP RECIA repose sur une architecture hiérarchisée conçue pour assurer la segmentation des usages, la sécurisation des accès et la continuité des services informatiques. Elle s'organise autour d'un cœur de réseau, assuré par un commutateur de niveau trois, chargé du routage inter-VLAN et de la centralisation des flux internes et externes.

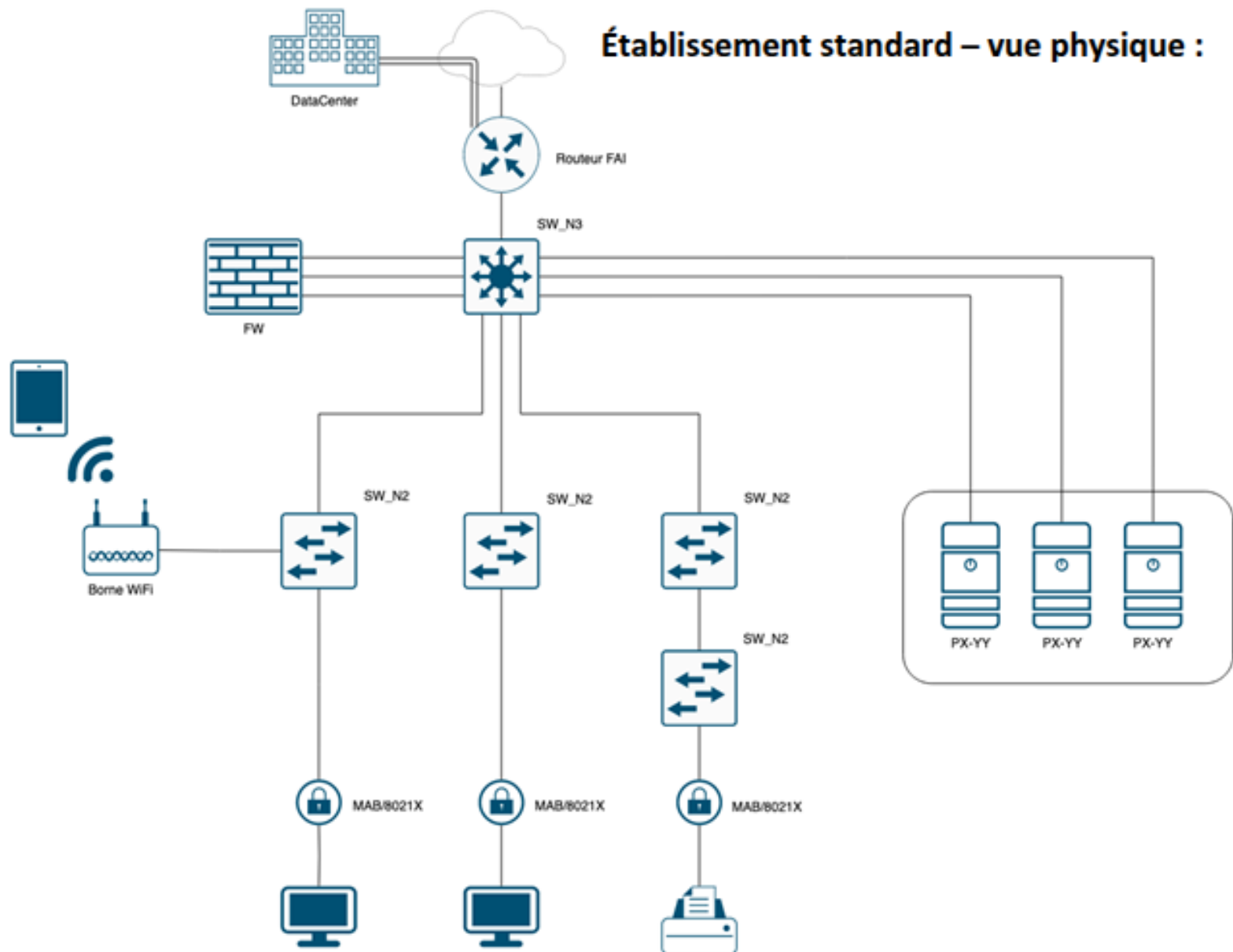
Ce cœur de réseau est relié au routeur d'accès Internet ainsi qu'aux équipements de sécurité, puis distribue la connectivité vers les commutateurs de niveau deux présents dans les différents bâtiments. Ces équipements assurent le raccordement des postes de travail, des imprimantes réseau, des bornes Wi-Fi et des équipements techniques.

L'architecture repose également sur une segmentation logique du réseau à l'aide de VLANs dédiés aux différents usages. Les principaux VLANs concernent notamment le réseau administratif, le réseau pédagogique, la téléphonie IP, l'impression, les équipements techniques ou encore les accès Wi-Fi et invités. Cette séparation permet d'isoler les flux, de limiter les risques de sécurité et de faciliter l'administration des infrastructures.

L'établissement dispose également d'une infrastructure serveur locale composée de trois serveurs physiques virtualisés sous Proxmox, hébergeant plusieurs machines virtuelles dédiées à l'authentification, au stockage et aux services applicatifs. La virtualisation facilite l'optimisation des ressources matérielles, la maintenance et l'amélioration de la disponibilité des services.

L'accès au réseau est sécurisé grâce aux mécanismes d'authentification [802.1X](#) et MAB, permettant de contrôler l'identité des équipements avant leur connexion au réseau. Cette architecture fournit ainsi un environnement structuré, sécurisé et adapté aux besoins des établissements accompagnés.

Établissement standard – vue physique :



4.4.5. Missions confiées et activités quotidiennes

Au sein du Centre de Services du GIP RECIA, mes missions s'inscrivent dans l'exploitation, l'administration et la sécurisation des infrastructures informatiques des établissements accompagnés. Mon activité combine support opérationnel, gestion des postes, administration réseau et participation aux actions de cybersécurité.

Je participe quotidiennement au traitement des sollicitations et incidents signalés par les utilisateurs via l'outil de ticket ou par téléphone. Ces interventions concernent notamment les postes de travail, les accès utilisateurs, les ressources réseau ou encore les dysfonctionnements liés aux services informatiques.

Je participe à l'administration des postes de travail à travers la gestion des mises à jour, l'installation et la maintenance des logiciels, ainsi que le déploiement de postes sous Windows 11 intégrant les stratégies de sécurité définies. Les déploiements sont réalisés à partir d'images système standardisées et préconfigurées, permettant d'assurer une homogénéité du parc, un gain de temps lors des installations et une meilleure maîtrise des configurations appliquées. Ces opérations garantissent la conformité, la sécurisation et l'homogénéité du parc informatique, tout en assurant la continuité de service pour les utilisateurs.

Sur le plan réseau, j'interviens dans l'administration de la solution de contrôle d'accès réseau ([NAC](#)) reposant sur les mécanismes d'authentification [802.1X](#) et MAB. Ces dispositifs permettent de contrôler et sécuriser l'accès au réseau en fonction de l'identité des équipements et des utilisateurs, tout en assurant une meilleure traçabilité des connexions et une limitation des accès non autorisés.

Je participe également à la supervision des infrastructures et au traitement des alertes de sécurité à travers l'analyse des journaux système ainsi que l'investigation des alertes remontées par les outils de supervision et de protection des postes, tels qu'Icinga et WithSecure. Ces actions permettent d'identifier rapidement les anomalies et de rétablir les services en cas de dysfonctionnement.

J'applique une politique de gestion des accès fondée sur le principe du moindre privilège, en limitant les droits accordés aux utilisateurs et aux équipements. Cette approche participe directement à la réduction des risques liés aux usages inappropriés ou aux erreurs de manipulation.

Ces missions me permettent de développer des compétences en administration et sécurisation des infrastructures, en cohérence avec le métier d'administrateur d'infrastructures sécurisées.

5. Projet : remplacement du serveur administratif dans les collèges et lycées

5.1. Contexte du projet

En 2023, la mise hors service du serveur administratif HORUS devient une nécessité technique et réglementaire. Ce serveur, dont la dernière mise à jour remonte à 2018, ne répond plus aux exigences actuelles en matière de sécurité, de compatibilité logicielle et de maintien en conditions opérationnelles. Il ne permet notamment plus d'assurer correctement le rôle de contrôleur de domaine pour les postes migrés sous Windows 11, en particulier depuis la version 23H2, devenue incompatible avec son architecture.

Cette situation s'inscrit dans un contexte plus large d'évolution des systèmes d'information des établissements de l'Éducation nationale. La loi de refondation de l'école a renforcé les responsabilités des collectivités territoriales en matière de gestion et de sécurisation des infrastructures numériques. Par ailleurs, l'arrêt programmé du support de Windows 10 rend indispensable l'adoption de Windows 11 et l'adaptation des infrastructures associées.

Dans ce contexte, la transformation des environnements administratifs devient incontournable. Le projet ne se limite pas au remplacement d'un serveur de fichiers mais vise une refonte plus globale des services administratifs : abandon du contrôleur de domaine HORUS, intégration de l'authentification administrative dans l'infrastructure existante, centralisation de la gestion des identités et modernisation des mécanismes d'accès aux ressources.

L'authentification repose désormais sur un annuaire Samba Active Directory unique, commun aux personnels administratifs, enseignants et élèves, avec des comptes nominatifs issus de l'ENT. Le projet intègre également un nouveau serveur de fichiers administratifs, fondé sur une gestion des droits selon les fonctions exercées, afin de sécuriser les données et de faciliter leur accès.

Ce projet s'inscrit ainsi dans une démarche globale de modernisation, de sécurisation et de rationalisation des infrastructures informatiques des établissements.

5.2. Méthodologie

Le projet a été mené selon une méthodologie structurée afin d'assurer la continuité de service et de limiter l'impact sur les utilisateurs.

Cette approche a permis d'organiser le projet de manière progressive, tout en tenant compte des contraintes propres aux établissements concernés.

Sur le plan organisationnel, le projet a été conduit en collaboration avec les équipes du Centre de Services et les pôles techniques de la Gestion des Systèmes Informatiques (GSI). Cette coordination transversale a facilité le partage d'informations, la validation des choix techniques et l'anticipation des contraintes opérationnelles spécifiques à chaque établissement.

La démarche adoptée repose sur un découpage en phases successives, depuis l'analyse de l'existant jusqu'à la mise en production. Une phase préalable d'étude a permis d'identifier les limites du serveur HORUS, les exigences liées à Windows 11 et les attentes des utilisateurs, afin de définir les objectifs et d'orienter les choix techniques.

La gestion du projet s'est inscrite dans une logique pragmatique, inspirée des méthodes de gestion de projet en environnement informatique. Le suivi des tâches et des échéances a été assuré à l'aide d'outils collaboratifs, favorisant une bonne visibilité sur l'avancement et une adaptation continue aux contraintes du terrain.

Une attention particulière a été portée aux aspects de sécurité et de fiabilité. Les décisions techniques se sont appuyées sur la politique de sécurité des systèmes d'information de l'État (PSSIE) et les recommandations de l'ANSSI, notamment en matière de gestion des accès, de centralisation des identités et de protection des données. Des phases de tests et de validation ont été intégrées avant chaque étape critique.

La méthodologie retenue a privilégié une migration progressive afin de limiter les risques d'interruption de service et de réduire l'impact sur les utilisateurs. Ce choix s'explique notamment par l'hétérogénéité des environnements administratifs, la présence de données sensibles ainsi que les différences d'organisation entre les établissements. La migration par étapes, accompagnée d'un suivi utilisateur et de phases de validation, a permis d'identifier plus facilement les anomalies, d'ajuster les procédures lorsque nécessaire et de sécuriser le déploiement à grande échelle de la solution SFADM.

5.3. Outils existants

Le projet de mise en place du serveur de fichiers administratif SFADM s'est appuyé sur une infrastructure déjà mature et éprouvée au sein du GIP RECIA. L'environnement de virtualisation reposait sur une plateforme Proxmox en production depuis plusieurs années, hébergeant des machines virtuelles critiques telles que les contrôleurs de domaine, les services réseau et divers serveurs applicatifs. Cette infrastructure était organisée en cluster composé de trois serveurs physiques, permettant une répartition des charges et une meilleure disponibilité des services. La machine virtuelle SFADM a ainsi été intégrée à ce cluster existant sans modification majeure de l'architecture.

Les mécanismes de sauvegarde étaient également déjà en place avant le projet. Les données et machines virtuelles étaient protégées à l'aide de solutions de sauvegarde automatisées reposant sur rdiff-backup et backup-ninja, garantissant la conservation des données et la possibilité de restauration en cas d'incident. L'intégration de SFADM dans ce système de sauvegarde existant a permis d'assurer immédiatement un niveau de sécurité et de résilience conforme aux exigences de l'infrastructure.

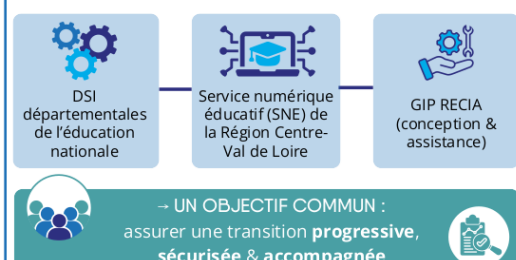
Concernant la gestion des identités, l'outil OMICO alimentait déjà l'annuaire Samba Active Directory utilisé pour la partie pédagogique via les sources issues de l'ENT et de l'annuaire fédérateur. Les identifiants nominatifs des personnels administratifs (nommés prénom.nom) étaient déjà disponibles dans cet annuaire, mais l'environnement HORUS fonctionnait avec son propre mode d'authentification, distinct de celui utilisé pour la partie pédagogique. Les utilisateurs disposent de la possibilité de gérer leur mot de passe directement depuis leur espace ENT, facilitant l'adoption du nouvel environnement d'authentification unifié.

L'ancien environnement HORUS reposait sur un [contrôleur de domaine de type NT](#), avec une gestion des accès moins adaptée aux besoins actuels d'industrialisation et de traçabilité. Dans le cadre du projet SFADM, un groupe de travail a donc défini une arborescence commune pour le serveur de fichiers administratif, afin d'obtenir une base identique dans l'ensemble des établissements. Cette arborescence standardisée permet d'associer les répertoires à des groupes de fonctions issus de l'annuaire Samba Active Directory, puis d'appliquer les droits d'accès de manière cohérente selon le rôle des utilisateurs. Ce choix facilite le déploiement à grande échelle, limite les adaptations manuelles établissement par établissement et renforce la maîtrise des permissions sur les données administratives.

Le projet SFADM s'inscrivait également dans une continuité d'expérience, le GIP RECIA exploitant depuis de nombreuses années un serveur de fichiers dédié à la partie pédagogique. Cette solution, en production depuis plus de dix ans, a servi de référence technique et organisationnelle. L'architecture globale (Samba Active Directory, virtualisation, sauvegardes) a été conservée, tandis que les groupes de sécurité et les stratégies de groupe (GPO) ont été spécifiquement conçus pour répondre aux besoins administratifs.

L'existant présentait plusieurs limites ayant motivé le projet de migration. Le serveur HORUS reposait sur des comptes fonctionnels et pas nominatifs, largement partagés entre utilisateurs, entraînant des risques importants en matière de sécurité, d'audit et de traçabilité des actions. De plus, ce serveur était totalement isolé de l'annuaire Samba Active Directory principal, étant historiquement géré par le rectorat et non par le GIP RECIA.

1 Qui participe à ce projet ?



2 Ce que vous aviez avant (HORUS)

- Des partages historiques, organisés par fonction.
- De multiples personnalisation, parfois non maîtrisées.
- Des comptes fonctionnels (incompatibles avec la politique de sécurité actuelle)



Organisation
hétérogène &
difficile à
maintenir dans le
temps

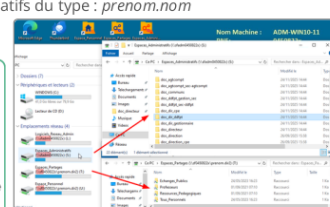
[illegible]

3 Ce que vous aurez après (SEADM)

- Une nouvelle arborescence de partage : chaque dossier porte le nom de la fonction de ses utilisateurs
- Un transfert automatique de l'ancien serveur (M:) vers SFADM
- Des comptes nominatifs du type : *prenom.nom*



- Organisation + claire
- Sécurité renforcée
- Gestion simplifiée



4 Déroulement du projet

Phase 1 – Enquête & préparation (7 semaines)

1. **Enquête** à l'ouverture de session sur chaque poste de travail → **à remplir obligatoirement par chaque personnel**
2. Création sur l'ancien serveur d'une **arborescence temporaire** correspondant aux nouveaux dossiers du SFADM (lecteur M:)
3. **Déplacement des fichiers** lorsque la correspondance est évidente
4. **Archivage ou suppression** des fichiers les plus anciens
5. **Normalisation** du poste de travail

PropMig

Situation Actuelle

Votre email nouveau :

Votre login actuel :

Votre domaine de connexion :

Fonction principale :

Fonction secondaire :

Tester son login / Mot de passe du nouveau message

Identifier l'usage :

Tester la configuration de son message

Utilisez-vous les logiciels suivants ?

☐ GPG ☐ Pseudo ☐ Sexe ARD

☐ Général

Phase 2 - Migration (1 session)

1. **Changement d'identification**
(ouverture de session)
2. **Lancement automatique** de l'outil de récupération des anciennes données à la première ouverture de session

Changement de réseau administratif

En changeant de réseau administratif, vous automatiquement à des nouvelles. Cet utilisateur ne pourra plus accéder aux anciennes données.

Options du fax

Associer l'utilisateur à :

Qu'en est-ce d'utiliser les listes :

- Transférer des documents PERSON (0 MB) > l'ancien réseau
- Transférer de l'ancien Bureau (0 MB) > 0 MB > 10 MB
- Transférer des documents locaux personnalisés du poste (0 MB) > 0 MB > 2 MB
- Transférer des documents locaux Personnels du poste (0 MB) > 0 MB
- Transférer de l'abonnement (0 MB) > 0 MB
- Transférer des personnalisations Person (0 MB) > 0 MB
- Transférer des personnalisations Chrono (0 MB) > 0 MB
- Transférer des personnalisations Équipe (0 MB) > 0 MB
- Transférer des 30x30x30 Personnelles (0 MB) > 0 MB

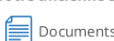
Fermer

Accompagnement des **DSI départementales** via
télé-assistance

Intervention des équipes du **SNE** en présentiel
Télé-assistance par les équipes du **GIP RECIA**

5 En quoi ce changement vous concerne-t-il directement ?

Un nouveau compte utilisateur sera créé sur votre poste de travail.
Votre ancienne session ne sera plus utilisée !



→ Ils doivent être récupérés.

Pour que l'outil puisse récupérer vos données, il est indispensable de connaître la correspondance : ancien compte ↔ nouveau compte.

POINT ESSENTIEL À RETENIR

- participation : aucune récupération
- ne repartez avec un poste vide

Votre implication est indispensable pour

Assurer la continuité de votre tra

5.4. Analyse des besoins

L'analyse des besoins du projet a permis d'identifier plusieurs attentes essentielles liées au fonctionnement quotidien des services administratifs des établissements scolaires. La solution devait avant tout permettre aux utilisateurs de disposer d'un compte nominatif unique pour accéder aux ressources du réseau administratif, tout en garantissant une authentification sécurisée et une meilleure traçabilité des actions réalisées sur les systèmes.

Un besoin important concernait également le stockage des données administratives. Les utilisateurs devaient disposer d'espaces de stockage adaptés aux différents usages, avec une distinction entre les données courantes et les données sensibles nécessitant des restrictions d'accès plus importantes. La gestion des droits devait ainsi permettre de limiter l'accès à certains dossiers en fonction des fonctions exercées au sein de l'établissement.

La solution attendue devait également garantir la continuité de service, la sauvegarde régulière des données, la centralisation de l'administration des comptes ainsi qu'une meilleure homogénéité des infrastructures entre les établissements. Enfin, le projet devait permettre de simplifier l'administration technique tout en renforçant le niveau global de sécurité des environnements administratifs.

Sur le plan organisationnel, la collectivité et le GIP RECIA avaient pour objectif de reprendre pleinement la maîtrise de l'infrastructure administrative, auparavant dépendante du rectorat via le serveur HORUS. Cette reprise de compétence visait à renforcer la sécurité, la cohérence technique et la capacité d'évolution des systèmes d'information des établissements.

Plusieurs solutions ont été envisagées lors de l'étude du projet. La possibilité de maintenir ou de moderniser le serveur HORUS a rapidement été écartée en raison de son abandon par le rectorat et de son obsolescence avancée. La création d'un annuaire administratif totalement distinct a également été étudiée, mais cette approche aurait engendré une complexité accrue, des coûts supplémentaires et une gestion plus lourde pour les équipes techniques. L'externalisation du stockage, bien qu'évoquée lors de l'étude du projet, n'a pas été retenue en raison des contraintes liées à la capacité de stockage et à la bande passante nécessaires pour centraliser l'ensemble des données des établissements.

Le choix s'est donc porté sur la mutualisation avec l'annuaire Samba Active Directory existant, en y intégrant les usages administratifs via le serveur SFADM. Cette solution permet de capitaliser sur une architecture maîtrisée, robuste et déjà en production depuis plusieurs années, tout en mettant en œuvre une segmentation logique des droits, des groupes dédiés et des politiques de sécurité adaptées aux besoins administratifs. Ce choix stratégique a également permis de réduire les délais de déploiement, un facteur critique compte tenu de l'arrêt programmé de Windows 10 et de l'urgence liée à la migration vers Windows 11.

Le projet SFADM répond ainsi à l'ensemble des besoins techniques, fonctionnels et sécuritaires, en modernisant l'infrastructure administrative, en renforçant la gouvernance des accès et en garantissant une continuité de service conforme aux exigences actuelles des établissements scolaires et de la collectivité.

5.5. Environnement à disposition

Le projet SFADM s'appuie sur l'infrastructure déjà déployée dans les établissements et exploitée par le GIP RECIA. Cette approche permet de capitaliser sur les composants existants tout en limitant les évolutions nécessaires au déploiement de la nouvelle solution.

Chaque établissement dispose d'une infrastructure serveur locale composée de trois serveurs physiques virtualisés sous Proxmox. Ces hôtes hébergent plusieurs machines virtuelles assurant les services d'infrastructure nécessaires au fonctionnement de l'établissement, notamment l'authentification, les services réseau, les sauvegardes et désormais le serveur de fichiers administratif SFADM. L'ajout de cette nouvelle machine virtuelle a été réalisé en réutilisant les ressources disponibles sur les environnements existants.

Le stockage reste indépendant pour chaque établissement afin de conserver l'autonomie des sites et de limiter les contraintes liées aux volumes de données et à la bande passante. Les données sont stockées localement sur l'infrastructure de l'établissement et protégées par des mécanismes de sauvegarde déjà en place. Les sauvegardes reposent notamment sur les outils rdiff-backup et backup-ninja, permettant d'assurer la protection des données et la restauration en cas d'incident.

Sur le plan logiciel, le projet s'appuie sur l'annuaire Samba Active Directory déjà utilisé pour les usages pédagogiques et alimenté par OMICO à partir des données issues de l'annuaire fédérateur et de l'ENT. Cette infrastructure fournit les informations nécessaires sur l'identité et les fonctions des utilisateurs afin d'automatiser l'attribution des droits d'accès aux ressources administratives.

Des outils d'automatisation et de déploiement déjà utilisés au sein du GIP RECIA ont également été réemployés afin de standardiser la création des serveurs, appliquer les configurations attendues et faciliter le déploiement de la solution sur l'ensemble des établissements.

Le projet n'a pas nécessité d'investissement matériel supplémentaire. La mise en œuvre a principalement reposé sur les ressources humaines mobilisées pour la préparation des migrations, les phases de validation, le déploiement progressif et l'amélioration continue des procédures au fil des établissements migrés.

5.6. Objectifs du projet

Le projet SFADM a pour objectif d'accompagner l'arrêt progressif du serveur HORUS et d'intégrer les usages administratifs dans l'infrastructure déjà exploitée par le GIP RECIA. Au-delà du remplacement d'un serveur existant, le projet vise une évolution globale de l'environnement administratif afin de le rendre compatible avec les standards techniques et de sécurité actuels.

Les objectifs définis pour le projet sont les suivants :

Authentification et gestion des identités

- Remplacer le mécanisme d'authentification historique de HORUS par une authentification centralisée.
- Utiliser les comptes nominatifs déjà présents dans l'annuaire alimenté par l'ENT.
- Supprimer progressivement les comptes génériques afin d'améliorer la traçabilité des actions.

Gestion et protection des données administratives

- Mettre à disposition un serveur de fichiers administratif dédié.
- Séparer les données courantes des données sensibles grâce à une gestion des droits par fonction.
- Garantir la sauvegarde et la disponibilité des données.

Standardisation et administration de l'infrastructure

- Définir une arborescence commune à l'ensemble des établissements.
- Uniformiser les mécanismes d'attribution des droits.
- Faciliter le déploiement, la maintenance et le support grâce à une infrastructure standardisée.

Compatibilité et évolution du système d'information

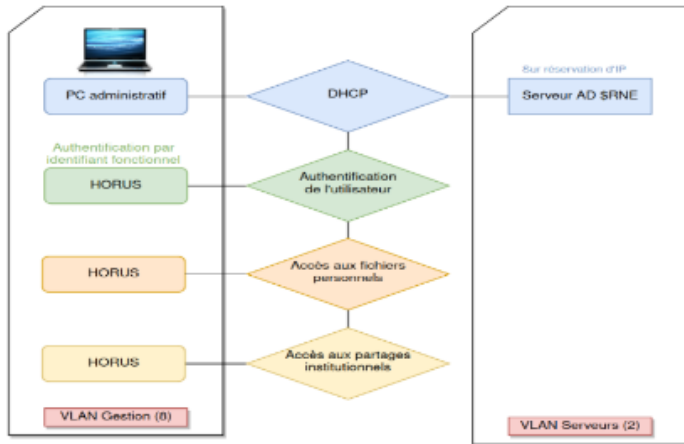
- Assurer la compatibilité avec Windows 11.
- Réutiliser les composants déjà maîtrisés par le GIP RECIA (Samba Active Directory, Proxmox, outils d'automatisation).
- Permettre un déploiement progressif sans interruption majeure de service.

Sécurité et gouvernance

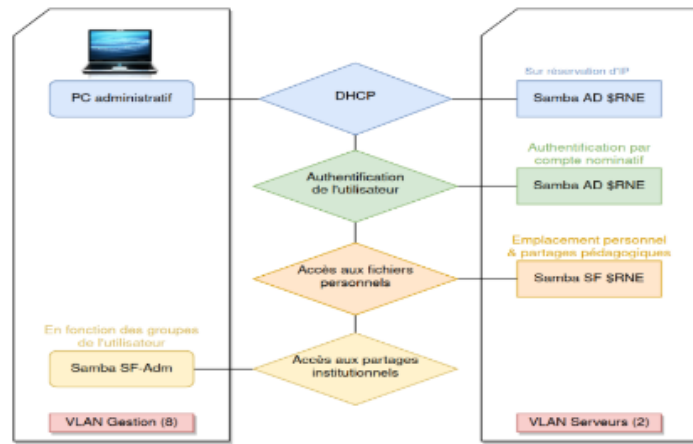
- Reprendre la maîtrise de l'infrastructure administrative auparavant dépendante du rectorat.
- Renforcer le contrôle des accès et la traçabilité.
- Appliquer les politiques de sécurité déjà utilisées sur les autres infrastructures administrées.

Le projet SFADM répond ainsi à des objectifs à la fois techniques, organisationnels et sécuritaires, tout en préparant l'évolution future des services administratifs des établissements.

Avant



Après



5.7. Les contraintes

Le projet SFADM s'est inscrit dans un contexte fortement contraint, aussi bien sur les plans technique, organisationnel que fonctionnel. L'objectif n'était pas uniquement de remplacer un serveur de fichiers, mais de reprendre l'ensemble des usages administratifs historiquement dépendants de l'environnement HORUS tout en maintenant la continuité d'activité des établissements.

La première contrainte concernait la continuité de service. Les personnels administratifs utilisent quotidiennement leurs postes, leurs espaces de stockage et certaines applications métiers indispensables au fonctionnement des établissements. Les opérations de migration devaient donc limiter au maximum les interruptions et être planifiées sur des périodes courtes. Cette exigence a conduit à mettre en place un processus progressif comprenant une phase préparatoire, une migration des postes, puis une validation avant fermeture définitive de l'environnement historique.

Une contrainte majeure provenait également de la coexistence temporaire avec les applications encore dépendantes de HORUS, notamment [GFC](#) avant le déploiement complet d'Op@le. Il n'était pas envisageable de supprimer immédiatement l'ensemble des serveurs existants. Une solution intermédiaire de type Horus Light a donc été retenue afin de conserver uniquement les services encore nécessaires tout en permettant le transfert progressif des usages administratifs vers SFADM.

Sur le plan technique, le projet devait s'appuyer sur l'infrastructure existante sans augmentation significative des ressources matérielles. Le stockage des données administratives est resté distribué au niveau des établissements et certaines contraintes de capacité ont conduit à écarter les scénarios de centralisation complète des données. La migration devait également rester compatible avec le calendrier de déploiement de Windows 11 et avec l'infrastructure d'authentification déjà en place.

Les contraintes de sécurité ont également fortement orienté le projet. La suppression progressive des comptes génériques, l'introduction d'une authentification nominative et la mise en œuvre d'une gestion des accès par fonctions ont nécessité une évolution importante des pratiques utilisateurs. Certaines données administratives présentant un niveau de sensibilité élevé (financières, sociales ou de santé), il a été décidé de conserver un stockage dédié sur le réseau administratif et de ne pas ouvrir l'accès depuis l'extérieur.

La conduite du changement a constitué une contrainte importante. Les utilisateurs devaient adopter de nouveaux identifiants, de nouvelles règles de stockage et parfois de nouveaux outils. L'accompagnement des établissements, la communication entre les différents acteurs du projet ainsi que la préparation des utilisateurs ont donc représenté une part importante de la réussite du déploiement.

5.8. Déroulement du projet (vue macro)

Le projet SFADM a été conduit selon une organisation progressive et structurée afin de permettre la reprise des usages administratifs historiquement portés par HORUS tout en garantissant la continuité de service des établissements. Compte tenu du nombre d'acteurs impliqués et du volume d'établissements concernés, une approche industrialisée a été retenue afin d'assurer un déploiement homogène et reproductible.

Le projet a été mené selon un planning formalisé, intégrant des phases de cadrage, des expérimentations sur environnements pilotes, des fenêtres de migration planifiées ainsi qu'une mise en production progressive. Cette organisation a permis de maintenir l'exploitation normale des infrastructures existantes pendant toute la durée du projet et de limiter les interruptions de service.

Le pilotage opérationnel reposait sur une organisation par établissements avec un suivi centralisé dans l'outil iTop. Pour chaque migration, plusieurs tickets étaient ouverts afin d'assurer le suivi des actions, la coordination entre les équipes et la communication avec les établissements. Les chefs d'établissement et leurs adjoints étaient intégrés au processus afin d'assurer la circulation des informations et d'anticiper les besoins spécifiques.

À l'échelle globale, le projet s'est déroulé selon les grandes étapes suivantes :

1. **Définition de la cible et préparation du projet**
Étude des limites de l'environnement HORUS, définition des besoins fonctionnels et techniques, validation de l'architecture cible et préparation des outils nécessaires au déploiement.
2. **Validation de la solution**
Réalisation de phases de tests sur maquette puis sur des établissements pilotes afin de valider les mécanismes d'authentification, les règles de gestion des accès, l'organisation des données et les procédures de migration.
3. **Industrialisation du déploiement**
Mise en place des mécanismes d'automatisation, des procédures standardisées et des outils de suivi permettant de reproduire les opérations sur l'ensemble des établissements.
4. **Déploiement progressif et accompagnement des établissements**
Migration réalisée selon un calendrier défini, accompagnée d'actions de communication, de préparation des utilisateurs et d'un suivi renforcé pendant les périodes de bascule.
5. **Stabilisation et amélioration continue**
Analyse des retours terrain, ajustement des procédures et amélioration progressive des méthodes afin d'optimiser les migrations suivantes.

Cette approche progressive a permis d'adapter le projet aux contraintes des établissements tout en capitalisant sur les retours d'expérience. Elle a également contribué à homogénéiser les pratiques d'administration et à sécuriser le déploiement à grande échelle de la nouvelle infrastructure administrative.

6. Solution retenue : intégration au domaine existant et adaptations pour le service administratif

6.1. Choix et argumentaire de la solution retenue

Le choix de la solution mise en œuvre dans le cadre du projet de migration du réseau administratif n'a pas été réalisé directement par moi, mais par un groupe de travail constitué de personnes des différentes équipes, notamment le Centre de Services, l'ISSR et l'IDMS. Mon rôle a consisté à comprendre, appliquer et mettre en œuvre cette solution dans le cadre des opérations de migration. Au regard de l'infrastructure existante et des contraintes du projet, ce choix s'inscrit dans une logique cohérente sur les plans technique, organisationnel et économique.

L'abandon du serveur HORUS s'imposait pour plusieurs raisons : le serveur ne bénéficie plus des mises à jour et n'était plus maintenue par le Rectorat, ce qui posait des problématiques en matière de sécurité. Elle n'était également plus compatible avec les évolutions des postes utilisateurs, notamment avec l'arrivée de Windows 11. Enfin, la dépendance au rectorat compliquait les opérations de maintenance et allongeait les délais d'intervention.

La solution SFADM a été retenue afin de répondre à ces problématiques. Elle repose sur un serveur de fichiers administratif dédié, déployé localement dans chaque établissement et intégré dans une architecture maîtrisée par le GIP RECIA. Cette solution permet de centraliser la gestion des comptes utilisateurs via OMICO, en s'appuyant sur les données issues de l'annuaire fédérateur de l'ENT. L'authentification repose désormais sur des comptes nominatifs de type prénom.nom, garantissant une meilleure traçabilité des actions.

La gestion des droits d'accès constitue également un point fort. Les accès aux dossiers sont définis en fonction des fonctions exercées par les utilisateurs au sein de l'établissement, telles que déclarées dans l'ENT. Cette approche permet d'assurer une meilleure sécurisation des données tout en simplifiant la gestion des autorisations. L'administration est également facilitée par l'utilisation d'outils déjà maîtrisés, permettant d'unifier les pratiques entre les environnements pédagogiques et administratifs.

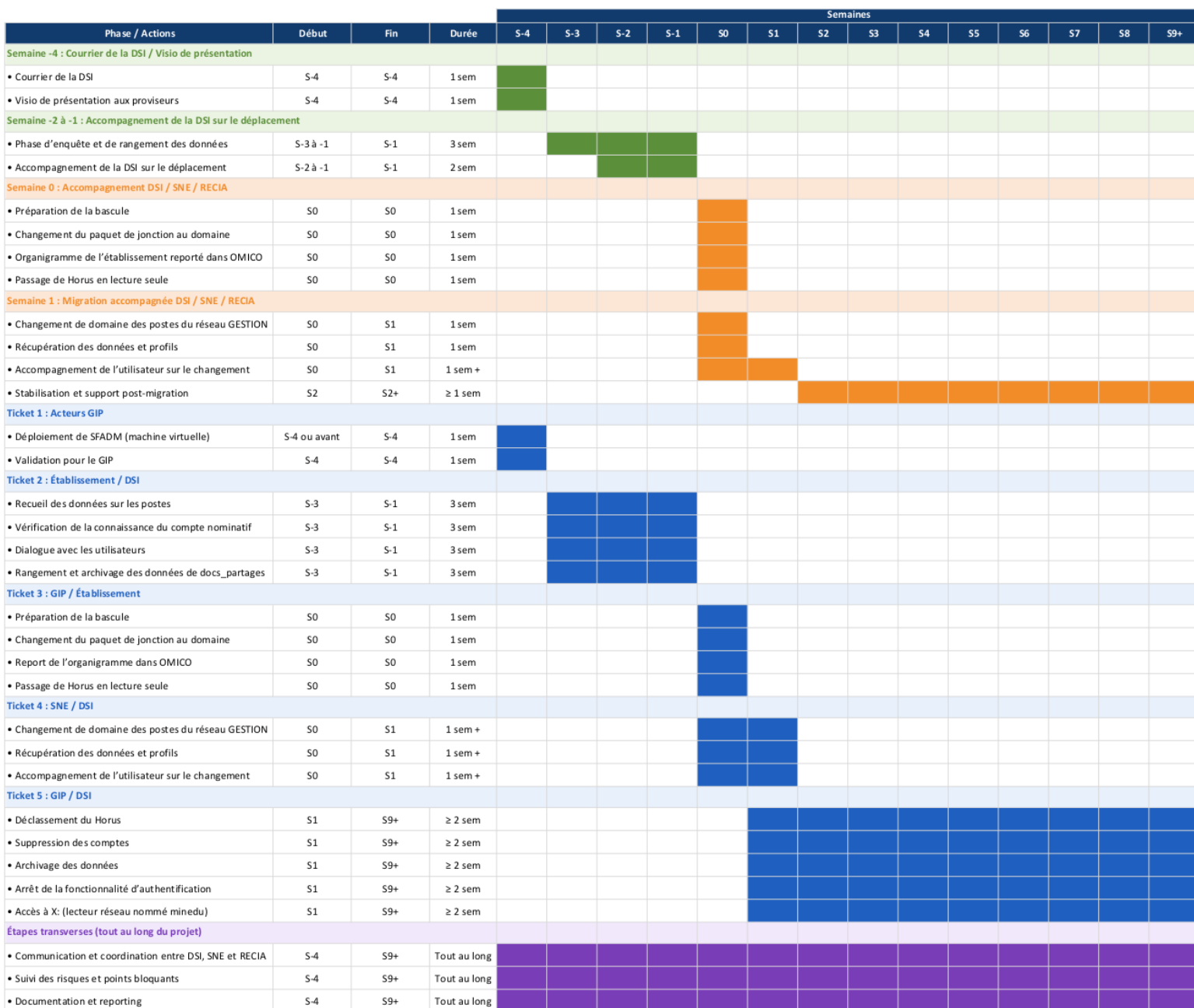
Le choix d'une infrastructure basée sur des machines virtuelles locales répond à des enjeux de performance et de résilience. Chaque établissement dispose de son propre serveur SFADM hébergé sur Proxmox, limitant l'impact en cas d'incident. Cette architecture permet également de réduire la latence, d'assurer une autonomie locale et de répondre aux exigences de sécurité, les données restant hébergées en interne avec un accès distant limité via VPN.

Le projet a également été contraint par des objectifs de maîtrise des coûts et de déploiement à grande échelle. La réutilisation de l'infrastructure existante a permis de répondre à ces contraintes tout en garantissant la compatibilité avec le système d'information en place. Cette approche a favorisé la mise en place d'une architecture standardisée et reproductible.

Sur le plan des avantages, la solution permet une meilleure maîtrise de l'infrastructure, facilitant le support et les interventions. Elle améliore la sécurité grâce à l'authentification nominative et à la gestion des droits, tout en permettant une standardisation des environnements. Toutefois, certaines limites subsistent, notamment une dépendance aux données issues de l'ENT et une arborescence standardisée pouvant manquer de flexibilité. Malgré ces contraintes, la solution SFADM constitue un choix pertinent au regard des objectifs du projet.

6.2. Planning de réalisation

Le planning du projet repose sur un découpage en cinq tickets successifs pour chaque établissement. Après une phase de préparation et de recueil des données, la bascule est réalisée en semaine 0, suivie de la migration des postes sur une courte période. Une phase finale de stabilisation et de déclassement du serveur HORUS permet de clôturer le projet. Le détail est présenté dans le diagramme de Gantt ci-après.



Légende du diagramme

	Préparation avec la DSI
	Accompagnement / Migration
	Tâches techniques (ticket)
	Transverse

Repères

- Jour J / semaine 0 : bascule de l'entrée dans le domaine / serveur Horus en lecture seule
- Ticket 1 : J – 4 semaines : déploiement de SFADM / visio de présentation aux fournisseurs
- Ticket 2 : J – 3 semaines : recueil des données sur les postes, dialogue utilisateur, rangement et archivage des données de docs_partages
- Ticket 3 : J0 : préparation de la bascule (paquet de jonction, organigramme dans OMICO, Horus en lecture seule)
- Ticket 4 : J+0 à J+5 : changement de domaine, récupération des données et profils, accompagnement de l'utilisateur
- Ticket 5 : post-migration : déclassement du Horus, suppression des comptes, archivage des données, arrêt de l'authentification

6.3. Ressources nécessaires

La mise en œuvre du projet SFADM s'est appuyée principalement sur les ressources existantes, tant sur le plan matériel que logiciel, ce qui a permis de respecter une contrainte forte de maîtrise des coûts. Chaque établissement disposait déjà d'une infrastructure composée de trois serveurs physiques, généralement des serveurs de type Dell, hébergeant un environnement de virtualisation sous Proxmox. Le serveur de fichiers administratif SFADM a ainsi été déployé sous forme d'une machine virtuelle dédiée, à raison d'une instance par établissement, sans nécessiter d'investissement matériel supplémentaire. Cette architecture a permis de répartir les ressources existantes tout en garantissant des performances adaptées aux besoins des utilisateurs.

Sur le plan logiciel, le projet s'est appuyé sur un ensemble d'outils déjà en place au sein du GIP RECIA. Le serveur SFADM repose sur un système Debian GNU/Linux, assurant un environnement stable et maîtrisé. La gestion des comptes utilisateurs et des droits d'accès est assurée via OMICO, en lien avec les données issues de l'ENT. Les opérations de déploiement et de migration des postes ont été réalisées à l'aide d'outils tels qu'[OPSI](#) et l'application Migration Admin faisant parti de l'outillage créé pour automatiser les actions le jour de la migration, tandis que le suivi des actions et la gestion des tickets étaient centralisés dans iTop. Enfin, la supervision des infrastructures, notamment du serveur SFADM, était assurée via Icinga, garantissant un suivi continu du bon fonctionnement des services.

Les ressources humaines ont constitué un élément central du projet. Plusieurs équipes du pôle [GSI](#) ont été mobilisées, notamment l'équipe [ISSR](#) pour le déploiement et la gestion des infrastructures, l'équipe IDMS pour les outils de migration, et l'équipe [CDS](#) pour le suivi opérationnel et le support aux utilisateurs. Ainsi que les techniciens de proximité intervenant directement dans les établissements afin d'assurer l'assistance aux utilisateurs. Au sein du Centre de Services, les interventions étaient réparties entre plusieurs acteurs, incluant notamment des télé-administrateurs, un intégrateur, une responsable de service ainsi que des apprentis, dont moi-même. Cette organisation a permis de gérer simultanément plusieurs migrations, avec un rythme moyen de trois à quatre établissements par semaine.

La charge de travail était significative, chaque migration d'établissement s'étalant en moyenne sur une semaine, avec une phase critique concentrée sur une journée afin de limiter l'impact sur l'activité des utilisateurs. Le nombre de postes concernés variait selon les établissements, avec environ 10 postes pour les collèges, 20 postes pour les lycées, et jusqu'à 50 pour les plus gros établissements. Ce qui impliquait une adaptation constante des ressources en fonction de la taille et de la complexité des structures.

Dans ce contexte, mon rôle consistait à participer activement au suivi des tickets, à la vérification des comptes utilisateurs, ainsi qu'à l'assistance technique lors des migrations. J'intervenais notamment en support, à distance ou par téléphone, pour accompagner les utilisateurs et résoudre les incidents liés à l'accès aux données ou aux droits. Cette implication m'a permis de contribuer directement au bon déroulement des opérations, tout en développant une vision globale de la gestion des ressources dans un projet de cette envergure.

Le projet a dû être mené en parallèle des activités quotidiennes du Centre de Service, ce qui a nécessité une capacité d'adaptation et une bonne organisation des équipes. Les ressources étant mutualisées, il

a été essentiel d'ajuster les priorités afin de concilier les exigences du projet avec le maintien des autres services, garantissant ainsi la continuité de service pour l'ensemble des établissements.

6.4. Les différentes phases de mon projet (vue micro)

6.4.1. Phase de tests et de validation

Avant le déploiement à grande échelle de la solution SFADM, une phase de tests et de validation a été mise en place afin de sécuriser la migration et de limiter les risques d'incident en production. Cette phase s'est appuyée sur plusieurs environnements complémentaires, incluant une maquette technique, des tests en conditions réelles sur des établissements pilotes, ainsi qu'une validation progressive des fonctionnalités.

Dans un premier temps, les tests ont été réalisés sur une maquette reproduisant fidèlement l'infrastructure des établissements. Cette maquette permettait de simuler l'ensemble du processus de migration, depuis le déploiement de la machine virtuelle SFADM jusqu'à la configuration des services. Elle a notamment été utilisée pour valider la configuration du serveur sous Debian, la mise en place du service de fichiers Samba, ainsi que l'intégration avec les outils existants tels qu'OMICO et les annuaires.

Une fois la solution validée en environnement de test, des expérimentations ont été menées sur des établissements pilotes, à savoir un collège et un lycée volontaires. Ces tests en conditions réelles ont permis de vérifier le comportement de la solution face aux usages des utilisateurs administratifs. Les éléments testés comprenaient l'accès au serveur de fichiers, la gestion des droits en fonction des fonctions, la récupération des données depuis HORUS, le changement de domaine des postes, ainsi que la compatibilité avec les applications métiers.

La validation reposait à la fois sur des critères techniques et fonctionnels. D'un point de vue technique, les équipes s'appuyaient sur les journaux système, les tests d'accès et les outils de supervision pour vérifier le bon fonctionnement des services. D'un point de vue utilisateur, la validation passait par les retours des personnels administratifs et des équipes de direction, permettant de confirmer que les données étaient accessibles et que les usages restaient conformes aux attentes.

Plusieurs difficultés ont été identifiées lors de cette phase, notamment des problèmes de droits d'accès, des données mal organisées ou encore des comptes utilisateurs non correctement reconnus. Ces anomalies ont permis d'ajuster les configurations, d'améliorer les outils de migration et de faire évoluer les procédures. Des optimisations ont également été apportées, notamment en matière d'automatisation via l'outil Salt, permettant de garantir une configuration homogène et reproductible sur l'ensemble des établissements.

À l'issue de cette phase de validation, le projet a pu être déployé progressivement, en commençant par les collèges, puis en étendant la migration aux lycées. Cette montée en charge maîtrisée a permis d'améliorer les processus au fil des déploiements et de fiabiliser la solution avant sa généralisation.

6.4.2. Déploiement du serveur de fichiers SFADM

Le déploiement du serveur de fichiers SFADM constitue la première étape opérationnelle du projet de migration. Cette phase est organisée autour du ticket 1, dédié à la mise en place de la machine virtuelle, et du ticket 1bis, consacré à sa configuration et à l'ajustement des ressources.

Le ticket 1, pris en charge par l'équipe ISSR, consiste à déployer la machine virtuelle SFADM au sein de l'infrastructure Proxmox de chaque établissement. Cette opération s'appuie sur une logique d'industrialisation via l'outil Salt, permettant de standardiser le déploiement sur l'ensemble des établissements. Le serveur SFADM est ainsi provisionné automatiquement à partir d'un modèle validé en amont, garantissant une configuration homogène et conforme aux exigences du projet.

Une fois la machine déployée, le ticket 1bis permet d'adapter les ressources du serveur en fonction des besoins réels de l'établissement. Cette étape est réalisée par le Centre de Services, notamment par les superviseurs, avec lesquels j'ai également été amené à intervenir. Elle consiste principalement à ajuster la capacité de stockage de la machine virtuelle SFADM.

Pour cela, une analyse préalable est effectuée à partir de l'ancien serveur HORUS. L'espace disque utilisé est comparé afin de définir une allocation adaptée sur le nouveau serveur. Par exemple, pour un serveur HORUS disposant de 700 Go dont 530 Go utilisés, une allocation de 768 Go peut être définie pour SFADM afin d'anticiper les besoins futurs. Cette opération est réalisée directement dans Proxmox, permettant une modification rapide et sans interruption majeure de service.

En parallèle, une attention particulière est portée à la gestion des sauvegardes. Une machine virtuelle dédiée est utilisée pour centraliser les sauvegardes des différentes machines, dont SFADM. Cette VM est hébergée sur un serveur distinct afin de se rapprocher du principe de sauvegarde 3-2-1, même si, dans la réalité, les serveurs sont souvent situés dans une même baie physique. L'espace de stockage de cette VM de sauvegarde est également ajusté afin de prendre en compte l'ajout du serveur SFADM.

Des mécanismes de supervision sont mis en place dès le déploiement afin d'anticiper les risques de saturation. Des alertes permettent de détecter un manque d'espace disque, ce qui est essentiel pour garantir le bon fonctionnement des sauvegardes et éviter toute interruption de service. Cette supervision s'inscrit dans une logique proactive, permettant d'intervenir avant qu'un incident ne survienne.

Ainsi, cette phase de déploiement repose sur une combinaison d'automatisation, d'adaptation aux besoins et de supervision, garantissant une mise en place fiable et homogène du serveur SFADM sur l'ensemble des établissements.

6.4.3. Enquête sur les usagers administratifs

La phase d'enquête sur les usagers administratifs correspond au ticket 2 du projet et constitue une étape clé de préparation à la migration. Elle a pour objectif de collecter les informations nécessaires à la bonne configuration des comptes utilisateurs, des droits d'accès et de l'organisation des données dans le futur environnement SFADM.

Cette phase débute par le déploiement d'un outil de préparation à la migration sur l'ensemble des postes administratifs, à l'aide de la solution OPSI. L'application est installée sur tous les postes concernés, à l'exception de certains équipements spécifiques, notamment ceux de la vie scolaire (AED), qui basculent vers le réseau pédagogique. Avant ce déploiement, un travail d'analyse est réalisé afin d'identifier les postes obsolètes, non utilisés ou à exclure, permettant de garantir la cohérence du périmètre de migration.

L'enquête administrative se présente sous la forme d'un utilitaire exécuté directement sur les postes utilisateurs. Lors de son lancement, les personnels administratifs doivent renseigner plusieurs informations essentielles, telles que leur fonction principale, leur éventuelle fonction secondaire, la connaissance de leurs identifiants réseau, ainsi que la configuration de leur messagerie. Ces éléments permettent de reconstituer un organigramme précis de l'établissement et d'identifier les besoins spécifiques liés à certains usages ou logiciels.

Les données collectées sont ensuite centralisées et exploitées afin de préparer la migration. Elles permettent notamment d'attribuer les droits d'accès aux futurs espaces de stockage en fonction des fonctions déclarées, garantissant ainsi une organisation cohérente et sécurisée des données. Cette étape est essentielle pour éviter les erreurs d'attribution de droits lors de la bascule vers SFADM.

Le suivi de l'enquête est réalisé de manière régulière via des outils de supervision et des commandes spécifiques permettant d'obtenir un état d'avancement détaillé. Les utilisateurs n'ayant pas complété l'enquête sont relancés, notamment par communication via les tickets iTop. Des mécanismes de contrainte peuvent également être activés, rendant l'enquête obligatoire afin d'assurer un taux de complétion maximal.

À la fin de cette phase, une vérification est effectuée afin de s'assurer que les comptes utilisateurs sont correctement présents dans le système d'information et associés aux fonctions déclarées, notamment via OMICO. Une communication est ensuite réalisée auprès des établissements pour annoncer la fin de l'enquête et le passage à la phase suivante de migration.

Cette étape préparatoire joue un rôle déterminant dans la réussite du projet, en permettant de structurer les données, de sécuriser les accès et de limiter les incidents lors de la migration des postes utilisateurs.

Inventaire Préparation Migration Administratif - 0450066c - 20260320

pc	login_horus	login_ad	fonction	fonction2	finalise	migrated
adm-bde-2	christophe.ody	christophe.ody	@bde		True	NON
adm-atelier-73	atelier	frederic.magret5	@agent-encadrant		True	NON
adm-adm3-22	gestion7	s.tatygabriel	@gestionnaire		True	NON
adm-cpe2-51	cpe2	samir.trimeche	@cpe		True	NON
adm-adm2-21	gestion5	sylvie.lesourd	@sec-gestion	@sec-gestion	True	NON
adm-sec-146	secret1	chloe.lezeaud	@sec-eleve		True	NON
adm-popc-45	accueil		@agents		False	NON
adm-prov-74	prov	stephane.debenest	@dir		True	NON
adm-cpe1-50	cpe2	christele.gracieux	@cpe		True	NON
adm-cpe3-103	survei1		@cpe		False	NON
adm-adl-207	cuis1		@agent-encadrant-cuisine		False	NON
adm-adm5-24	gestion2	emilie.brimboeuf	@sec-gestion	@sec-gestion	True	NON
adm-mag2-41	mag2		@agents		False	NON
adm-adm4-23	gestion6	emilie.brimboeuf	@sec-gestion	@sec-gestion	True	NON
adm-adm1-20	secret3	e.goncalves	@sec-dir		True	NON
adm-infirm-56	infirm1		@infirmierie		False	NON
adm-adjddf-59	gestion10	damien.michelet	@ddfpt		True	NON
adm-psy-18					false	NON
adm-ddfpt-70					false	NON
adm-survan-75					false	NON
adm-assoc-11	AVANT	APRES			false	NON
adm-aps1-40					false	NON
adm-adl-206					false	NON
adm-provadj-83					false	NON

6.4.4. Préparation de la migration administrative

La phase de préparation de la migration correspond au ticket 3 et constitue une étape critique du projet. Réalisée en amont de la bascule des postes, elle a pour objectif de garantir la cohérence des données, la continuité de service et la réussite de la migration.

Cette phase est principalement prise en charge par l'équipe IDMS et consiste à préparer l'environnement technique ainsi que les données utilisateurs. Elle débute par une phase d'anticipation menée plusieurs semaines avant la migration, durant laquelle les utilisateurs sont invités à organiser leurs données. Une arborescence cible, identique à celle du futur serveur SFADM, est mise à disposition sur le serveur HORUS afin de faciliter le rangement des fichiers. Cette étape permet aux utilisateurs de s'approprier la nouvelle organisation et de limiter les opérations à réaliser le jour de la migration.

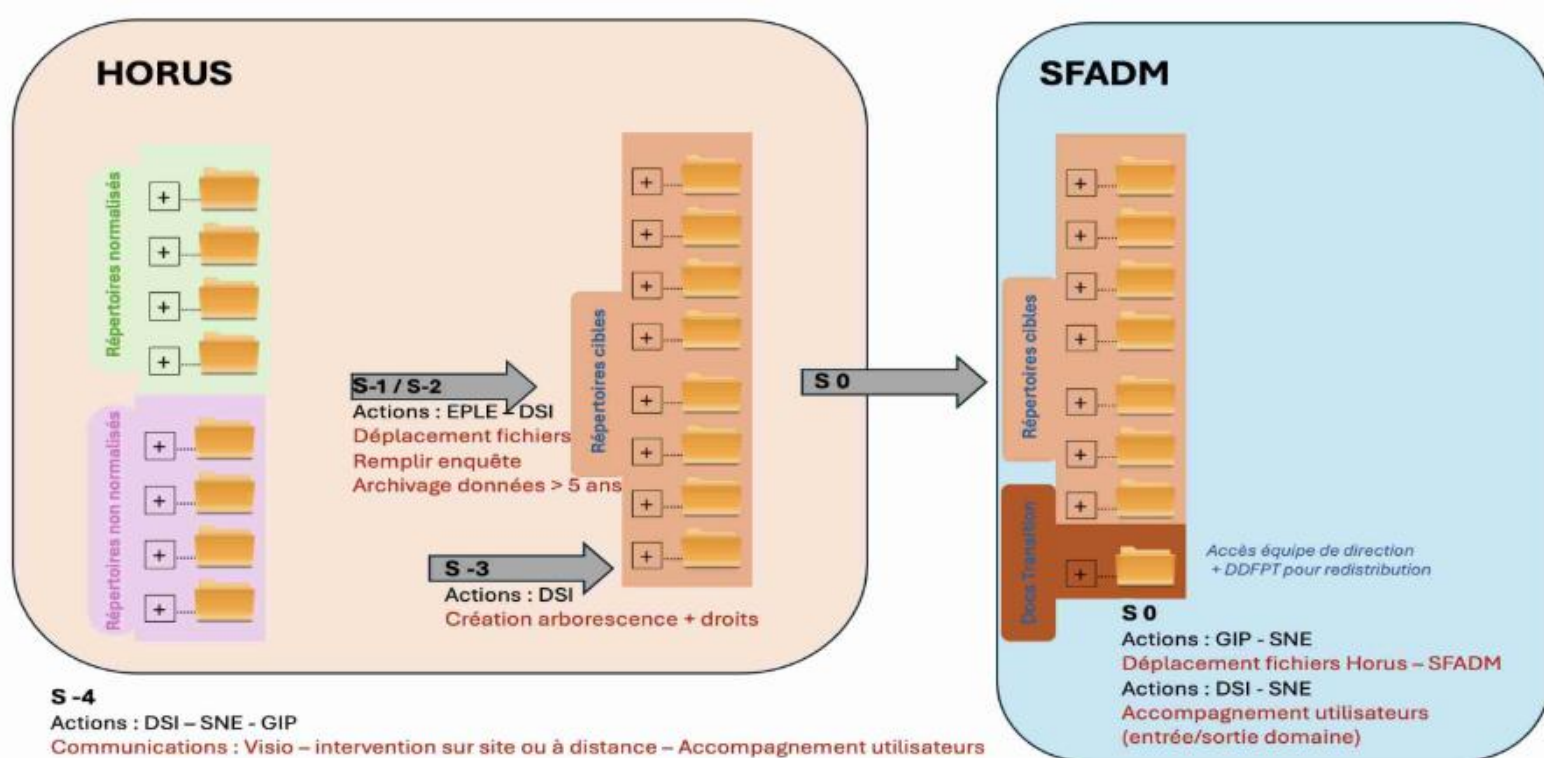
La veille de la migration, des opérations techniques sont réalisées sur les serveurs. Sur le serveur SFADM, une synchronisation des données est effectuée à l'aide de scripts spécifiques, permettant de transférer les données depuis HORUS tout en appliquant les droits d'accès et les permissions adaptés. Les ACL sont ajustées afin de garantir une cohérence avec les comptes utilisateurs issus de l'annuaire.

En parallèle, des modifications sont apportées au serveur OPSI afin de préparer le changement de domaine. La configuration du paquet de jonction au domaine est adaptée pour que les postes ne s'authentifient plus sur HORUS mais sur le nouvel environnement. Les scripts de connexion sont également modifiés afin d'afficher les nouveaux lecteurs réseau, notamment le lecteur S: correspondant aux espaces administratifs.

Le serveur HORUS est ensuite basculé en lecture seule, empêchant toute modification des données. Cette étape est essentielle pour éviter les incohérences entre les deux environnements. Les données sont alors transférées vers le serveur SFADM selon deux logiques : les données préalablement rangées sont directement intégrées dans les espaces administratifs, tandis que les autres sont placées dans un espace temporaire accessible uniquement à la direction pour finalisation.

Des vérifications sont ensuite réalisées afin de s'assurer du bon fonctionnement de l'ensemble du dispositif, notamment en testant la connexion des postes au nouveau domaine et l'accès aux données. Une communication est enfin effectuée auprès des utilisateurs pour les informer de la migration et des consignes à respecter, notamment l'arrêt de l'utilisation de l'ancien serveur.

Cette phase de préparation permet de sécuriser la transition entre les deux environnements en combinant anticipation des usages, synchronisation des données et adaptation des configurations techniques.



6.4.5. Migration des postes administratifs

La migration des postes administratifs correspond au ticket 4 du projet et constitue l'étape centrale de la transition vers le nouvel environnement SFADM. Elle est réalisée en semaine 0, une fois la phase de préparation validée, et est principalement prise en charge par les équipes [SNE](#), avec le support du Centre de Services.

Cette phase consiste à basculer les postes du domaine administratif historique vers un domaine unique, commun avec les environnements pédagogiques. Les utilisateurs n'utilisent plus de comptes fonctionnels génériques, mais des comptes nominatifs issus de l'ENT, ce qui permet d'améliorer la traçabilité et la sécurité des accès.

La migration débute généralement par les postes de direction (proviseur, secrétariat, gestion), afin de garantir la bonne organisation des données sensibles. Ces profils disposent des droits nécessaires pour réorganiser les fichiers si certaines données ont été mal classées lors des phases préparatoires.

Techniquement, la migration repose sur un outil dédié, déployé automatiquement sur les postes. Celui-ci prend en charge la récupération des données de l'ancien environnement, notamment les documents personnels, les profils utilisateurs et les configurations applicatives (navigateurs, messagerie). Lors du lancement, l'utilisateur doit renseigner les identifiants de son ancien compte afin de permettre l'accès aux données à migrer.

L'outil effectue ensuite une série de transferts automatisés vers le nouvel environnement, en adaptant les emplacements en fonction du type de poste. Un récapitulatif des opérations est généré en fin de traitement, permettant de vérifier le bon déroulement de la migration. La durée de cette opération varie en fonction du volume de données et des performances du poste.

Durant cette phase, un accompagnement est assuré auprès des utilisateurs, notamment en cas de difficulté d'accès aux fichiers ou de perte de repères liée au changement d'environnement. Ce support est réalisé à distance ou par téléphone, afin de garantir une continuité de service et de limiter l'impact sur l'activité des établissements.

La migration des postes constitue une étape clé du projet, combinant automatisation technique et accompagnement des utilisateurs, afin d'assurer une transition fluide vers le nouvel environnement SFADM.

En changeant de réseau administratif, votre environnement a été réinitialisé.
Cet utilitaire est là pour vous aider à récupérer vos anciennes données.

Ordinateur Fixe

Ancien identifiant : prov

Nouvel identifiant : prenom.dir2

Ce que cet utilitaire va faire :

- Transfert des documents PERSO (U:\) de l'ancien réseau
- Transfert de l'ancien Bureau (0 MB -> 0 MB)
- Transfert des documents locaux personnels du poste (3570 MB -> 2166 MB)
- Transfert des Images locales personnelles du poste (18 MB -> 18 MB)
- Transfert des documents NextCloud locaux du poste (0 MB -> 0 MB)
- Transfert de Thunderbird (16 MB -> 16 MB)
- Transfert des personnalisations Firefox (53 MB -> 53 MB)
- Transfert des personnalisations Chrome (185 MB -> 176 MB)
- Transfert des personnalisations Edge (686 MB -> 686 MB)
- Transfert des StickyNotes/Pense-bêtes (0 MB -> 0 MB)

Lancer la recuperation

Fermer

Version : 1.8.4

6.4.6. Déclassement de l'ancien serveur Horus

La phase de déclassement du serveur HORUS correspond au ticket 5 et intervient une fois la migration des postes administratifs finalisée. Elle a pour objectif de mettre fin à l'utilisation de l'ancien serveur tout en assurant la continuité de service pour certaines applications spécifiques, notamment [GFC](#).

Dans un premier temps, des vérifications sont effectuées afin de déterminer si le serveur HORUS est encore utilisé. Cette analyse repose notamment sur l'identification des comptes accédant à certains partages, permettant de détecter un éventuel usage résiduel de GFC ou d'autres applications. En fonction des résultats, deux scénarios sont possibles.

Si aucun usage n'est détecté, le serveur peut être totalement déclassé. Il est alors arrêté et retiré de l'infrastructure, ce qui permet de simplifier l'environnement technique et de libérer des ressources. En revanche, si des usages persistent, le serveur est conservé en mode « Horus Light ». Dans ce mode, seules les fonctionnalités nécessaires sont maintenues, notamment l'accès aux données ou aux applications encore utilisées, sans permettre de nouvelles modifications.

Cette étape implique également une coordination avec les équipes du rectorat, notamment pour la validation des usages restants et la mise en place du mode dégradé. Une fois les actions réalisées, le serveur est documenté comme étant en fin de vie ou en fonctionnement limité, assurant une traçabilité des opérations.

Le déclassement du serveur HORUS permet de finaliser la migration en sécurisant l'abandon de l'ancien système, tout en garantissant une transition progressive lorsque cela est nécessaire.

6.5. Mise en production

La mise en production de la solution SFADM est effective à l'issue de la migration complète des postes administratifs, une fois le ticket 4 validé et clôturé. Elle correspond au moment où l'ensemble des utilisateurs accède au nouvel environnement sans dépendre du serveur HORUS et où le fonctionnement des services est jugé conforme aux attentes.

Après la migration, plusieurs vérifications sont réalisées afin de s'assurer du bon fonctionnement de l'environnement. Celles-ci incluent notamment le contrôle de l'accès au lecteur réseau S:, la validation des droits utilisateurs, l'ouverture des fichiers ainsi que le bon fonctionnement des applications administratives. Ces tests permettent de confirmer que les données sont accessibles et correctement organisées.

La supervision joue également un rôle essentiel dans cette phase. Le serveur SFADM est intégré dès son déploiement dans l'outil Icinga, permettant un suivi continu de son état. Les contrôles portent notamment sur la disponibilité du serveur, l'espace disque, la charge système ainsi que le bon fonctionnement des services critiques tels que Samba. Cette surveillance permet de détecter rapidement toute anomalie.

Un support utilisateur est assuré en parallèle afin d'accompagner la prise en main du nouvel environnement. Les principales sollicitations concernent des problèmes d'accès aux fichiers, des droits incorrects ou des raccourcis obsolètes. Ces interventions permettent d'ajuster la configuration et de limiter l'impact sur l'activité.

Des ajustements techniques peuvent également être réalisés après la mise en production, notamment l'augmentation de l'espace disque des machines virtuelles, la correction des droits d'accès ou la mise à jour des informations dans OMICO.

La validation finale repose sur la stabilisation de l'environnement, caractérisée par une diminution des incidents et des retours utilisateurs positifs, marquant la réussite de la migration et l'adoption de la solution SFADM.

6.6. Problèmes rencontrés et solutions apportées

Au cours du projet de migration vers SFADM, plusieurs difficultés techniques et organisationnelles ont été rencontrées. Leur résolution a permis d'améliorer le processus et de renforcer la fiabilité de la solution.

Un premier problème concernait la qualité des données issues du serveur HORUS. Les arborescences étaient souvent hétérogènes, avec des données mal rangées ou obsolètes, compliquant la migration automatique. Pour y remédier, une phase de préparation a été mise en place afin de trier, archiver et réorganiser les données avant leur transfert.

Un autre point bloquant concernait les comptes utilisateurs non nominatifs ou incomplets. Certains utilisateurs ne connaissaient pas leurs identifiants ou utilisaient des comptes génériques, empêchant une migration correcte vers l'Active Directory. L'enquête administrative a permis de collecter les informations nécessaires et de corriger ces incohérences en amont.

Des difficultés ont également été rencontrées lors de la migration des profils utilisateurs, avec des erreurs de récupération (profils corrompus, fichiers verrouillés, chemins incorrects). L'utilisation d'un outil automatisé a permis de standardiser les transferts, complétée par des interventions manuelles si nécessaire.

La gestion des droits d'accès a aussi nécessité des ajustements. Des écarts entre les fonctions déclarées et les droits attribués ont entraîné des problèmes d'accès, corrigés via des modifications dans OMICO et une mise à jour des groupes de sécurité.

Des contraintes liées aux ressources systèmes, notamment l'espace disque, ont été observées. Des mécanismes de supervision ont permis d'anticiper les seuils critiques et d'ajuster les ressources.

L'ensemble de ces problématiques a permis d'améliorer le processus de migration, en industrialisant les opérations et en sécurisant les déploiements à grande échelle.

6.7. Analyse rétrospective et bilan

Le projet de migration vers SFADM m'a permis de développer des compétences techniques, méthodologiques et relationnelles essentielles au métier d'administrateur d'infrastructures sécurisées.

Sur le plan technique, j'ai consolidé mes connaissances en administration systèmes et réseaux, notamment autour des environnements virtualisés sous Proxmox, de la gestion des comptes via Active Directory et des mécanismes de partage de fichiers avec Samba. La manipulation d'outils tels qu'Icinga, OMICO ou encore OPSI m'a également permis de mieux comprendre le fonctionnement global d'une infrastructure centralisée et industrialisée.

Ce projet m'a également permis d'acquérir une vision concrète des enjeux liés à la migration d'un système d'information. J'ai pu appréhender les problématiques de compatibilité, de gestion des données, de droits d'accès et de continuité de service. La participation aux différentes phases du projet, de la préparation à la mise en production, m'a permis de comprendre l'importance de l'anticipation, des tests et de la supervision.

Sur le plan organisationnel, j'ai appris à travailler dans un environnement structuré, basé sur la gestion de tickets et la coordination entre plusieurs équipes ([CDS](#), ISSR, IDMS). Cette expérience m'a permis de développer ma rigueur, ma capacité à suivre des procédures et à m'adapter aux contraintes opérationnelles tout en respectant les délais.

Ce projet a renforcé mes compétences relationnelles, notamment dans le cadre du support utilisateur. J'ai été amené à accompagner des utilisateurs lors de la migration, à répondre à leurs problématiques et à vulgariser des aspects techniques. Cette dimension m'a permis de développer ma communication et ma capacité à m'adapter à différents interlocuteurs.

Ce projet constitue une expérience significative dans mon parcours, en me permettant de mobiliser et de développer les compétences attendues pour le métier d'administrateur d'infrastructure sécurisée, tout en me confrontant à des situations concrètes et professionnalisantes.

7. Difficultés rencontrées et solutions apportées

7.1. Difficultés rencontrées

Dans le cadre du projet de migration vers SFADM, plusieurs difficultés d'ordre organisationnel, humain et technique ont été rencontrées, en lien avec la reprise du réseau administratif des établissements.

Sur le plan organisationnel, la principale difficulté résidait dans l'hétérogénéité des environnements existants. Les infrastructures et les pratiques variaient fortement d'un établissement à l'autre, rendant difficile l'application d'un processus standardisé. De plus, l'absence initiale d'un état des lieux précis des équipements, des comptes et des données a complexifié la préparation des migrations.

Sur le plan humain, la conduite du changement a constitué un enjeu important. Certains utilisateurs étaient peu préparés à la migration, notamment en raison de l'abandon des comptes génériques au profit de comptes nominatifs. Cela a entraîné des incompréhensions, des difficultés d'authentification et une perte de repères dans l'organisation des fichiers. Il a également été parfois difficile de mobiliser les utilisateurs pour réaliser les actions préparatoires.

La communication a également représenté un point sensible. La coordination entre les différents acteurs nécessitait un suivi rigoureux afin de garantir la bonne transmission des informations et le respect du planning. Toute absence de communication pouvait entraîner des retards ou des blocages dans le processus de migration.

Ce projet a impliqué une montée en compétences progressive. La compréhension des outils et des mécanismes de migration, ainsi que des interactions entre les systèmes (OMICO, Active Directory, SFADM), a nécessité un temps d'apprentissage, facilité par la pratique et l'accompagnement des équipes.

Ces difficultés ont permis d'améliorer progressivement l'organisation du projet, notamment en renforçant la communication, en structurant les procédures et en accompagnant les utilisateurs de manière plus adaptée.

7.2. Solutions apportées

Afin de répondre aux difficultés rencontrées lors du projet de migration vers SFADM, plusieurs solutions ont été mises en place sur les plans organisationnel, technique et humain.

Sur le plan organisationnel, une structuration rigoureuse du processus a été adoptée. Le découpage en tickets (ticket1 à ticket5) a permis de mieux organiser les étapes, de suivre l'avancement et de répartir les tâches entre les équipes, tout en facilitant la coordination entre les pôles [CDS](#), ISSR et IDMS. Cette méthode a aussi permis de mieux identifier les responsabilités de chaque acteur.

Concernant les utilisateurs, un effort a été porté sur la communication et l'accompagnement. Des messages réguliers ont permis d'expliquer les étapes et les actions attendues. L'enquête administrative a préparé les utilisateurs en amont en limitant les erreurs liées aux comptes et aux droits. Cet accompagnement a également facilité l'adhésion au changement.

La gestion des données a également été améliorée grâce à la mise en place d'une arborescence cible et à l'accompagnement des utilisateurs dans le rangement de leurs fichiers. Des espaces temporaires sur SFADM ont permis de faciliter la reprise des données non triées et de limiter les pertes d'information.

Sur le plan technique, l'automatisation des déploiements via Salt et l'utilisation d'outils de migration ont permis d'industrialiser le processus et d'assurer une homogénéité entre les établissements. La supervision via Icinga a permis d'anticiper les incidents et de garantir la stabilité des infrastructures.

La montée en compétences des équipes a contribué à améliorer progressivement les pratiques et à gagner en efficacité. La répétition des migrations a permis d'affiner la méthode et de sécuriser davantage les opérations.

L'ensemble de ces solutions a permis de sécuriser le projet, d'améliorer l'expérience utilisateur et de garantir une migration progressive et maîtrisée vers SFADM.

8. Conclusion

Ce mémoire retrace mon expérience en tant qu'alternant au sein du GIP RECIA, avec un focus particulier sur le projet de migration des serveurs de fichiers administratifs vers la solution SFADM. Ce projet, essentiel pour la modernisation et la sécurisation des infrastructures, a permis de remplacer une solution obsolète par un environnement plus fiable, standardisé et maîtrisé. Sa mise en œuvre progressive, accompagnée d'une démarche structurée et d'outils adaptés, a permis d'assurer une transition efficace tout en garantissant la continuité de service pour les établissements.

Cette alternance m'a permis de développer des compétences techniques en administration systèmes et réseaux, tout en mettant en pratique des méthodes de gestion de projet en environnement réel. J'ai pu approfondir ma compréhension des infrastructures informatiques, tout en améliorant ma capacité à analyser des problématiques concrètes et à proposer des solutions adaptées.

Au-delà des aspects techniques, cette expérience a confirmé mon intérêt pour le domaine de l'administration et de la sécurisation des infrastructures. Elle m'a également permis de prendre conscience de l'importance de la rigueur, de l'organisation et de la communication dans la réussite d'un projet informatique, notamment dans des contextes impliquant de nombreux utilisateurs.

Dans la continuité de cette expérience, je souhaite poursuivre le développement de mes compétences dans le domaine des systèmes et réseaux, avec une orientation vers des fonctions d'ingénierie ou de cybersécurité. L'alternance m'a apporté une vision concrète des réalités du métier et a renforcé ma motivation à évoluer dans ce secteur.

Cette expérience au GIP RECIA constitue ainsi une étape importante dans mon parcours professionnel, en me permettant de participer à un projet d'envergure tout en consolidant mes compétences techniques et mon savoir-faire.

9. Annexes

9.1. Processus détaillé

9.1.1. Etape 1 - déploiement du serveur de fichiers SFADM

Ticket 1 : Tâches préalables à la migration

[MIG-ADM] Tk1 : déploiement du serveur de fichiers SFADM

- **Transparent pour les utilisateurs** : il s'agit de mettre en service le nouveau serveur de fichiers administratif qui remplacera le serveur HORUS
- Le serveur de fichier Administratif SFADM est déployé sur l'établissement et sa taille de disque ajustée, nous allons en outre déployer une machine virtuelle pour vérification à distance (adm-vrt\$RNE)
- Nous déployons sur toutes les machines administratives un exécutable permettant de recueillir les données (nom d'utilisateur, prénom, nom, fonction)

The screenshot displays the 'itop' service management interface. On the left is a dark sidebar with navigation links: 'Toutes les Organisations', 'Bienvenue', 'Gestion des configurations', 'Gestion du parc d'IPs', 'Gestion du DHCP', 'Gestion des événements', 'Gestion des demandes', 'Gestion des incidents', 'Gestion des problèmes', 'Gestion des changements', and 'Gestion des services'. The main area shows a ticket titled '[0280864M] - R-238250' with the status 'Fermée (Demande Utilisateur)'. The ticket details are organized into sections: 'Informations générales' (Client: [0280864M] - Lycée professionnel Elsa Triolet (LEN-MI), Demandeur: Mickael ROBIN, Etat: Fermée, Origine: Portail, Titre: [MIG-ADM] Tk1 : déploiement du serveur de fichiers SFADM, Description: Ce ticket est ouvert par le support : Dans le cadre de la migration de l'administratif, ce premier ticket est ouvert pour le déploiement du serveur SFADM (nouveau serveur de fichiers, remplaçant d'Horus)), 'Qualification' (Type de Requête: demande de service, Impact: Individuel (une personne ou un ordinateur), Urgence: Basse, Priorité calculée: Basse), 'Informations complémentaires' (Famille de services: 03 - Projets, prestations personnalisées, communication, Service: Projets / Conseils, Sous catégorie: non défini), 'Contacts' (Equipe: Equipe GSI Superviseur, Agent: Clément BLONDEAU), and 'Dates' (Relance le: , Date de rdv: , Date de création: 2025-06-27 11:04:10). On the right, a chat window shows messages from Vincent MONTAGNE and a system message about disk space allocation.

Informations générales

Client: [0280864M] - Lycée professionnel Elsa Triolet (LEN-MI)

Demandeur: Mickael ROBIN

Etat: Fermée

Origine: Portail

Titre: [MIG-ADM] Tk1 : déploiement du serveur de fichiers SFADM

Description ✕

Ce ticket est ouvert par le support : Dans le cadre de la migration de l'administratif, ce premier ticket est ouvert pour le déploiement du serveur SFADM (nouveau serveur de fichiers, remplaçant d'Horus)

Qualification

Type de Requête: demande de service

Impact: Individuel (une personne ou un ordinateur)

Urgence: Basse

Priorité calculée: Basse

Informations complémentaires

Famille de services: 03 - Projets, prestations personnalisées, communication

Service: Projets / Conseils

Sous catégorie: non défini

Contacts

Equipe: Equipe GSI Superviseur

Agent: Clément BLONDEAU

Dates

Relance le:

Date de rdv:

Date de création: 2025-06-27 11:04:10

Journal privé

Pas d'augmentation de l'allocation d'espace sur le serveur de sauvegarde.

Étiquette	Valeur	Min	Max	Avertissement	Critique
/srv	701,67 GB	0,00 TB	4,33 TB	3,46 TB	3,90 TB

2025-07-02 18:04:02

Horus = 200 Go alloué / 175 Go consommé
Il serait déjà en seuil d'avertissement si on remet la même allocation => passage de sfadm de 32Go à 256Go.

2025-07-02 18:01:28

@Vincent MONTAGNE
Je me permet de rouvrir car il faut augmenter la taille du disque.
Est-ce que tu préfères transmettre à Clément ?

2025-07-02 17:53:47

vm creer avec espace disque par defaut

2025-07-02 13:47:59

9.1.2. Étape 2 - Enquête administrative et rangement du serveur Horus

Ticket 2 : [MIG-ADM] Tk2 : Enquête sur les usagers administratifs / Rangement du serveur Horus

Cette phase doit être une phase de dialogue intense entre les divers acteurs ! C'est l'une des clefs de la réussite d'une migration fluide.

Les personnels administratifs sont invités à renseigner l'enquête administrative : l'application (Migration administrative) est mise à disposition sur les bureaux de l'environnement utilisateur, elle est destinée à recueillir les informations concernant les personnels, et notamment vérifier leur connaissance de leur login /mot de passe pédagogique (celui qu'ils utilisent peut-être pour le WIFI). En effet, la connexion au nouveau serveur administratif se fera avec l'identifiant/mot de passe pédagogique, c'est-à-dire "prénom.nom", et non plus avec une fonction comme, par exemple, "gestion1".

En parallèle, les techniciens de la DSI départementale et du [SNE](#) commence le **rangement et l'archivage des données de docs_partages** afin de préparer une recopie sans heurts.

- **Tâche GIP** : Le paquet OPSI recia-migration-admin doit être en dernière version sur tous les postes administratifs.
- Dans ce dossier, le GIP Récia et l'établissement vont communiquer afin d'avoir les éléments nécessaires
 - liste des personnels et leur compte Horus qui continueront à utiliser GFC
 - fourniture de l'organigramme connu de l'établissement
 - liste des logiciels demandant des droits d'administration : GFC, liste à compléter
- La migration ne pourra avoir lieu qu'une fois que ce dossier sera finalisé : **Enquête complète et docs_partage de Horus rangé**

The screenshot displays the Recia itop interface. On the left is a sidebar with navigation links like 'Bienvenue', 'Gestion des configurations', 'Gestion du parc d'IPs', etc. The main area shows a ticket titled '[0280864M] - R-238251' with a status of 'Fermée (Demande Utilisateur)'. The ticket details are organized into several sections: 'Informations générales' (Client: Lycée professionnel Elsa Triolet, Demandeur: Mickael ROBIN, Etat: Fermée), 'Qualification' (Type de Requête: demande de service, Impact: Individuel, Urgence: Basse, Priorité calculée: Basse), 'Informations complémentaires' (Famille de services: O3 - Projets, prestations personnalisées, communication; Service: Projets / Conseils), and 'Dates' (Relance le: Date de rdv, Date de création: 2025-06-27 11:04:12). On the right, a chat window shows messages from Nicolas Lebrun, including one dated 2025-07-02 13:06:32 and another dated 2025-06-30 15:45:45.

9.1.3. Étape 3 - Préparation de la migration administrative

Ticket 3 : [MIG-ADM] TK3 - Préparation de la migration administrative – \$DATE

Le matin de la migration, à distance, le GIP Recia prépare les éléments de migration :

Transparent pour les utilisateurs : les actions engagées dans ce ticket sont réalisées juste avant d'entamer la migration administrative (**Jour J**), ce sont les suivantes :

- dossier docs_partage de Horus passe en lecture seule et les dossiers normalisés du Horus sont docs_partages est recopié vers le dossier docs_direction sur SFADM
- le paquet opsi-domain-join est adapté pour entrer dans le domaine unique / La configuration du serveur OPSI est effectuée pour mémoriser que le serveur d'authentification administratif n'est plus le serveur Horus
- script de logon est modifié pour afficher le lecteur réseau S: des Espaces_Administratifs.

En fin de cette phase de préparation, il convient de communiquer vers tous les personnels qu'ils ne doivent plus utiliser de fichiers de doc_partages. Durant le temps de la migration, les fichiers nécessaires doivent être recopiés en local sur les postes.

En fin de cette phase de préparation, il convient de communiquer **vers tous les personnels qu'ils ne doivent plus utiliser de fichiers de doc_partages**. Durant le temps de la migration, les fichiers nécessaires doivent être recopiés en local sur les postes et être déposé sur le nouveau serveur de fichier SFADM après migration de l'ordinateur.

The screenshot displays the iTop ITSM interface. On the left is a dark sidebar with navigation links: 'Toutes les Organisations', 'Bienvenue', 'Gestion des configurations', 'Gestion du parc d'IPs', 'Gestion du DHCP', 'Gestion des événements', 'Gestion des demandes', 'Gestion des incidents', 'Gestion des problèmes', 'Gestion des changements', 'Gestion des services', and 'Configuration'. The main area shows a ticket titled '[0280864M] - R-238252' with the status 'Fermée (Demande Utilisateur)'. The ticket details are organized into several sections: 'Informations générales' (Client: Lycée professionnel Elsa Triolet, Demandeur: Mickael ROBIN, Etat: Fermée, Origine: Portail, Titre: IMIG-ADM TK3 - Préparation de la migration administrative - 04/07/2025), 'Qualification' (Type de Requête: demande de service, Impact: Individuel, Urgence: Basse, Priorité calculée: Basse), 'Relations' (Événement source: non défini, Requête parente: non défini, Incident parent: non défini, Problème lié: non défini, Changement parent: C-238223), 'Informations complémentaires' (Famille de services: 03 - Projets, prestations personnalisées, communication; Service: Projets / Conseils), 'Dates' (Relance le: 2025-06-27 11:04:12, Date de rdv: 2025-06-27 11:04:12, Date de début: 2025-06-27 11:04:12, Dernière mise à jour: 2025-07-20 03:00:04, Date d'assignation: 2025-07-20 03:00:04), 'Résolution' (Code de résolution: Assistance, Solution: Préparation effectuée, Délai de résolution: 6j 22h 11min 29s, Satisfaction client: Sans avis), and 'Rapport SLA' (SLA TTO dépassé: non). A right-hand pane shows a 'Journal privé' with a log of preparatory steps for the migration, including the preparation of OPSI tools, domain migration, and data archiving. At the bottom of this pane, a list of files to be copied is provided: administratf: doc, communs; atelier: doc, gestion, agent-encadrant; cpe: doc, cpe; cuisine: doc, gestion, cuisine; direction: doc, direction; gestion: doc, gestionnaire; gestion secretaire: doc, gestion, sec-gest; secretaire direction: doc, direction, sec-dir. The log concludes with a note about the installation of logiciels and a closing message.

Recia itop.

Toutes les Organisations

Bienvenue

Gestion des configurations

Gestion du parc d'IPs

Gestion du DHCP

Gestion des événements

Gestion des demandes

Gestion des incidents

Gestion des problèmes

Gestion des changements

Gestion des services

Bonjour Bryan !

5 nouvelles messages

IP-RECIA

IP-RECIA COLLECT

10200664MI - D...

administratifs

Identifiant

1 carine.delmotte

2 christelle.roux

3 d.bureau d'allan

4 deborah.croquet

5 diane.duquesnoy

6 herve.fontaine

7 isabelle.frain

8 jeangabriel.gandon

9 laura.boyaval

10 ludvine.sibade

11 ludovic.arrould

12 marlou.rousseau

13 mariya.kazatskaya

14 mathilde.reydellet

15 mickael.robin1

16 olivier.pignolo

17 sarah.el-arabi

18 serena.amaral

19 valerie.boureille

20 yohann.le-pape

21 yvon.baillieu1

22 flore.germain

23 laura.vallee

24 fabienne.raby

25 marie-agnes.neil2

26 vanessa.touze

agent-encadrant

Identifiant

1 yvon.baillieu1

agent-encadrant-cuisine

Identifiant

1 carine.delmotte

agents

Identifiant

1 fabienne.raby

cpe

Identifiant

1 d.bureau d'allan

ddlpt

Identifiant

1 ludovic.arrould

dir

Identifiant

1 mickael.robin1

gestionnaire

Identifiant

1 jeangabriel.gandon

2 olivier.pignolo

3 flore.germain

infirmerie

Identifiant

1 valerie.boureille

sec-ddlpt

Identifiant

1 vanessa.touze

sec-dr

Identifiant

1 laura.vallee

sec-gestion

Identifiant

1 marie-agnes.neil2

Informations complémentaires

2025-07-03 12:09:07

9.1.4. Étape 4 - Migration des postes administratifs

Ticket 4 : Jour J Bascule des postes d'un SI à l'autre Changement de domaine des postes - Première connexion - **[MIG-ADM] TK4 - Migration des postes administratifs – \$DATE**

Les équipes de proximité sont en intervention sur site pour accompagner la migration de chaque poste.

Dès que le TK3 est résolu, le travail de migration proprement dit peut commencer. Sur chaque poste administratif, l'opération minimale suivante est effectuée :

Cas typique sans difficulté :

Nous avons réalisé une petite vidéo visible [ici](#) pour montrer les actions

- Dès lors que la préparation de la migration a bien été faite, l'ordinateur est sorti du domaine Horus.
- Après redémarrage, il est intégré au domaine pédagogique.
- Après redémarrage, l'utilisateur doit effectuer sa première connexion avec son compte "pédago"
 - L'application Migration est lancée et permet de récupérer les éléments de l'ancien compte Horus.
 - On récupère les données locales dans c:\users\nom_horus, et les éléments de profil Thunderbird, Firefox, Chrome et Edge.
 - Selon le volume de données, la durée de récupération est plus ou moins longue mais ne saurait excéder 15 minutes
 - Récupération des données "personnelles" du **U: de Horus** vers le **U: de SF**. En fin de migration, un texte récapitulatif est fourni, nous vous conseillons de l'enregistrer.

Cas d'un poste GFC :

- En cas d'utilisation de GFC sur le poste, nous devons configurer quelques éléments supplémentaires sur le serveur OPSI afin d'assurer le montage du lecteur X: (Minedu) et d'accorder les droits d'administration.
- En plus des actions précédentes, il faut s'assurer que GFC fonctionne toujours

Cas des postes de vie scolaire :

Les postes de vie scolaire sont redéployés dans le réseau pédagogique.

Cas des postes fournis par la DSDEN :

Les personnels de fonctions suivantes ont normalement un portable fourni par l'État. Ces personnels devraient avoir leur machine enregistrée dans nos bases afin de leur accorder un accès filaire au réseau administratif de l'établissement.

Un travail est à mener pour que, soit l'accès au serveur sfadm est possible, soit les fichiers sont partagés via un outil en ligne (NextCloud ENT, NextCloud etat, ETNA, RESANA... etc)

Recia

itop.

Toutes les Organisations

Bienvenue

Gestion des configurations

Gestion du parc d'IPs

Gestion du DHCP

Gestion des événements

Gestion des demandes

Gestion des incidents

Gestion des problèmes

Gestion des changements

Gestion des services

Bonjour Bryan !

5 nouveau(x) message(s)

(GIP-RECIA) - GIP Recia (COLL-TER)

[0280864M] - R-238253

Fermée (Demande Utilisateur)

Propriétés

Cls

Contacts

Requêtes filtres

Tâches

Pièces jointes

Informations générales

Cliant

[0280864M] - Lycée professionnel Elsa Triolet (LEN-MI)

Demandeur

Mickaël ROBIN

Etat

Fermée

Origine

Portail

Titre

[MIG-ADM] Tk4 - Migration des postes administratifs - 04 et 07/07/2025

Description

Ce dossier est ouvert pour la migration proprement dite des postes administratifs. La migration ne sera déclenchée que lorsque les actions du Tk3 seront effectuées.

Qualification

Type de Requête

demande de service

Impact

Individuel (une personne ou un ordinateur)

Urgence

Basse

Priorité calculée

Basse

Informations complémentaires

Famille de services

03 - Projets, prestations personnalisées, communication

Service

Projets / Conseils

Sous catégorie de service

non défini

Contacts

Equipe

Equipe SNE Nord

Agent

Sylvain DAVAUX

Dates

Relance le

Date de rdv

Date de création

2025-06-27 11:04:13

Journal privé

Journal public

Activité

Journaux

Statuts

Modif.

1

Bonjour M. Robin,

Je me permets de passer en résolu ce dossier concernant la migration des postes administratifs.

Cordialement,
Nicolas Lebrun

2025-07-18 11:18:33

9.1.5. Etape 5 - Déclassement du serveur HORUS en Horus Light

Ticket 5 : [MIG-ADM] TK5 - Déclassement du serveur HORUS en Horus Light si GFC encore présent

Transparent pour les utilisateurs : les services du serveur HORUS désormais inutilisés (authentification, serveur de fichiers) sont déclassés.

Les fichiers qui ont été utilisés en local sur les postes et qui venait de doc_partages doivent être remis sur le partage afférent des Espaces_administratifs.

Le GIP Recia désinstalle recia-migration-admin sur tous les postes, la machine virtuelle adm-vrt\$RNE est arrêtée.

Le ticket est ensuite confié à la DSI du Rectorat pour passage en version Horus "Light" qui n'assure que la partie gestion de GFC. Il ne doit normalement pas y avoir d'impact. Les utilisateurs de GFC sont préservés, les autres comptes sont désactivés sur le serveur Horus.

The screenshot displays the Recia itop interface. On the left is a sidebar with navigation links. The main area shows a ticket for '[O180769N] - R-239901' with the title '[MIG-ADM] TK5 - Déclassement du serveur HORUS en Horus Light si GFC encore présent'. The ticket is marked as 'Fermée (Demande Utilisateur)'. The description states: 'La migration des postes administratifs étant effectuée, le serveur Horus n'est plus utile dans sa fonction de partage de fichiers. Les données ont été transférées. Si l'établissement utilise encore GFC, le partage Minedu est préservé et les comptes qui l'utilisent sont maintenus. Les comptes utilisés sont précisés dans le journal public.' The ticket is assigned to the 'Equipe DSI Eole' and the agent 'Emmanuel BACOS'. The date of creation is '2025-08-06 15:20:33'. On the right, a 'Journal public' shows a message from 'tydie.boucher' dated '2025-08-06 15:42:56'.

Informations générales

Client	[O180769N] - Collège Jean Moulin (CEN-MI)
Demandeur	Chloe BONNEUIL
Etat	Fermée
Origine	Portail
Titre	[MIG-ADM] TK5 - Déclassement du serveur Horus en Horus Light si GFC encore présent

Description

La migration des postes administratifs étant effectuée, le serveur Horus n'est plus utile dans sa fonction de partage de fichiers. Les données ont été transférées. Si l'établissement utilise encore GFC, le partage Minedu est préservé et les comptes qui l'utilisent sont maintenus. Les comptes utilisés sont précisés dans le journal public.

Qualification

Type de Requête	demande de service
Impact	Individuel (une personne ou un ordinateur)
Urgence	Basse
Priorité calculée	Basse

Contacts

Equipe	Equipe DSI Eole
Agent	Emmanuel BACOS

Dates

Relance le	
Date de rdv	
Date de création	2025-08-06 15:20:33

Informations complémentaires

Famille de services	CD18 - Infrastructure et câblage
---------------------	----------------------------------

Journal public

Bonjour,

La migration des postes administratifs étant effectuée, le serveur Horus n'est plus utile dans sa fonction de partage de fichiers. Les données ont été transférées.

L'établissement utilise encore GFC, le partage Minedu est préservé et les comptes qui l'utilisent doivent être maintenus.

Les comptes utilisés pour l'accès à Minedu sont les suivants :

- tydie.boucher

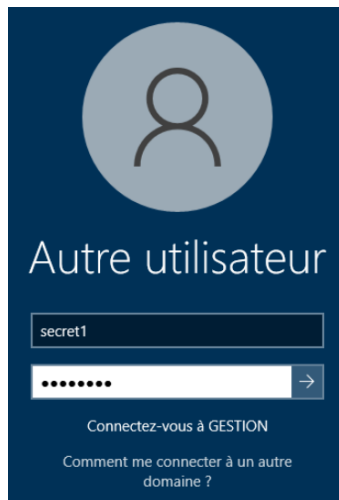
Ces comptes doivent donc être préservés. Je confie le passage en Horus Light aux collègues de la DRASI du rectorat.

Cordialement,
Nicolas Lebrun

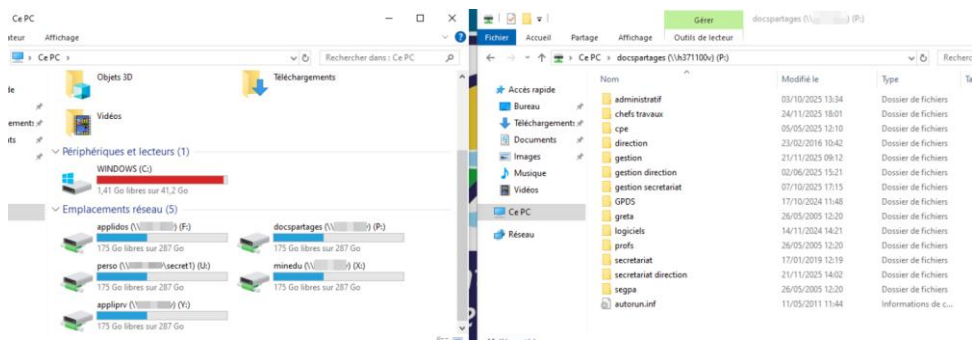
2025-08-06 15:42:56

9.2. Avant/après la migration : captures d'écrans HORUS et SFADM

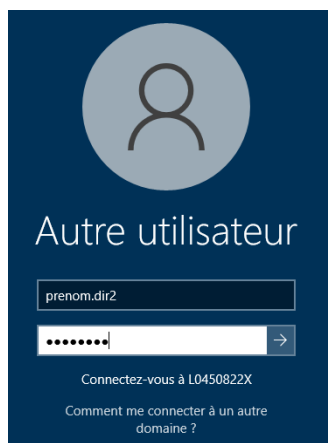
HORUS : Ouverture de session sur le domaine GESTION : login fonctionnel



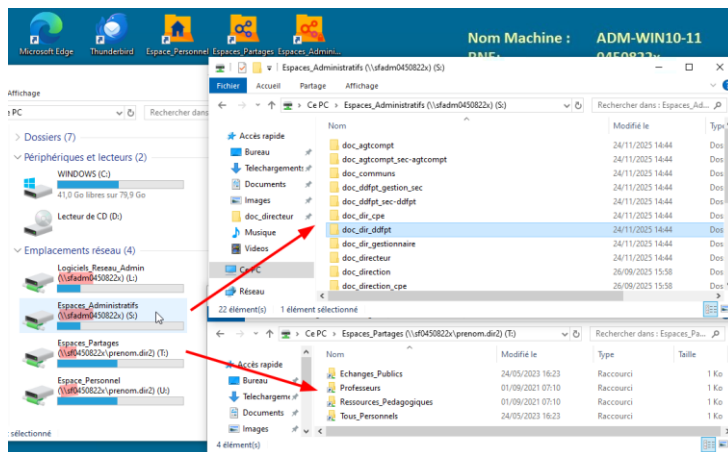
Explorateur de fichiers :



SFADM : Ouverture de session sur le domaine de l'établissement : login nominatif



Ici, le domaine de l'établissement s'appelle L0450822X (L pour Lycée, suivi du **RNE** de l'établissement)



A quoi servent ces différents partages ?

- **Logiciels_Reseau_admin** : sur SFADM : logiciels réseaux utilisés uniquement sur le réseau administratif : Exemple : ARD,
- **Espaces_Administratifs** : sur SFADM : Échange de fichiers entre personnels administratifs.
- **Espaces_Partages** : sur le serveur de fichiers pédagogique SF : Échanges de fichiers
 - entre Professeurs (Professeurs),
 - entre Professeurs et Élèves (Echanges_Publics)
 - entre personnels administratifs et Professeurs (Tous_Personnels)
- **Espaces_Personnel** : Sur le serveur SF : Dossier propre à chaque utilisateur. Stockage de documents personnels

Remarque :

Le partage **minedu** (sur l'ancien HORUS) peut être présent pour les personnels qui ont encore besoin de GFC

9.3. Pendant la migration : enquête administrative

La migration HORUS vers SFADM : étape préparatoire, l'Enquête administrative

Pour vous, utilisateur, le changement de domaine et de serveur de fichiers va se passer en deux étapes :

- une **première phase de préparation à la migration** : cette page vous détaille l'enquête administrative
- une deuxième [phase de migration](#) proprement dite.

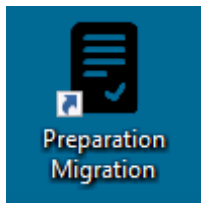
Pour faciliter la transition et la migration des données personnelles, nous avons prévu un utilitaire pour vous assister. Il s'agit de l'enquête administrative. Elle sera lancée en semaine -3 de la migration.

Entre ces deux phases, nous effectuerons des opérations techniques sur les serveurs pour basculer dans le nouveau mode.

En quoi consiste l'Enquête administrative ?

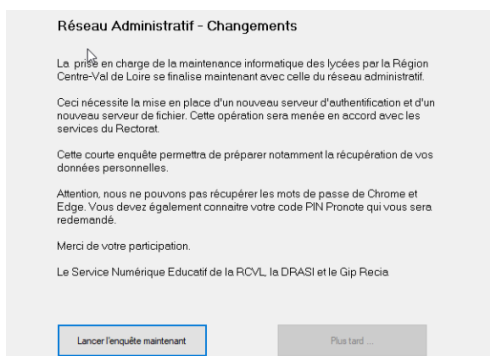
Il s'agit d'un utilitaire qui sera **déployé sur tous les postes administratifs**. L'objectif est que **chaque personnel** la complète afin que nous collections un **organigramme** précis de l'établissement et les éventuelles difficultés avec des **logiciels non pris en charge**.

Un nouveau raccourci va apparaître sur votre bureau :



Le logiciel est lancé **automatiquement à la connexion** tant que vous n'aurez pas exécuté cette application avec succès.

Au démarrage, une première fenêtre vous présente l'application. Vous pouvez soit l'exécuter maintenant, soit la repousser à plus tard.



Si vous acceptez :

4 informations sont à saisir :

- Votre fonction principale (et dans certains cas une fonction secondaire - ex : Secrétariat Gestion et Secrétariat DDFPT)
- Vérification que vous connaissez votre login/mot de passe du réseau pédagogique (si vous ne les connaissez pas : procédure à suivre « Récupérer ses identifiants pédagogiques depuis l'ENT »)
- Vérification de la configuration de votre messagerie (POP interdit).
- Utilisation de logiciels particuliers

Les 2 tests sont considérés comme réussis si une coche verte apparaît

Cliquer sur **Fermer** pour clore l'application.

Si les 3 informations demandées (Fonction, Login et Messagerie) sont correctes, l'enquête est considérée comme remplie et le programme ne s'exécutera pas à la prochaine connexion.

Dans le cas contraire, elle sera relancée à la prochaine connexion au poste

Il n'est pas nécessaire de renseigner l'enquête administrative sur les postes **non attribués** à des personnels. (exemple poste dédié à l'usage de turboself)

Quelle est la prochaine étape pour les utilisateurs ?

Lorsque tous les personnels administratifs de l'établissement auront convenablement complété l'enquête administrative, le GIP Recia recueillera les données et s'assurera de la conformité du SI.

En semaine 0, la [migration des postes](#) sera réalisée. Nous vous informerons de cette bascule et vous accompagnerons afin qu'elle se déroule sans heurts.

9.4. Pendant la migration : Migration des postes administratifs

La migration HORUS vers SFADM : semaine 0, la migration des stations

Pour vous, utilisateur, le changement de domaine et de serveur de fichiers va se passer en deux étapes :

- une première phase de préparation à la migration ([enquête administrative](#))
- **une deuxième phase de migration proprement dite : cette page vous détaille la migration des postes administratifs**

En pratique, votre poste de travail va être sorti du domaine GESTION actuel et basculé dans le même domaine que les postes pédagogiques. Vous n'utiliserez donc plus votre compte fonctionnel (gestion, princ, secret1... par exemple), mais votre compte nominatif issu de l'ENT Chercan ou NetOCentre (celui que vous avez renseigné lors de l'enquête)

Rassurez-vous, au quotidien, cela changera peu de choses... quelques emplacements de documents, votre connexion, mais c'est à peu près tout.

En quoi consiste la migration des postes de travail ?

Une fois que votre poste aura changé de domaine, lors de votre première connexion avec vos identifiants nominatifs, vous aurez perdu tout votre environnement habituel (vos personnalisations dans Firefox, Chrome, votre fond d'écran, votre messagerie Thunderbird)... mais l'outil que nous avons mis en place devrait vous permettre d'en retrouver l'essentiel.

L'outil qui va vous permettre de récupérer tout cela est le suivant.

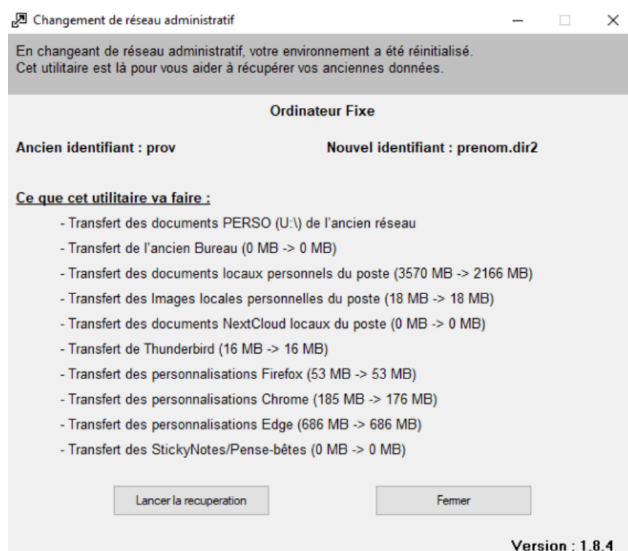


Cet outil se lance automatiquement, mais si ce n'était pas le cas, double cliquez dessus.

Le logiciel détecte votre type de station : **Portable** ou **Fixe**.

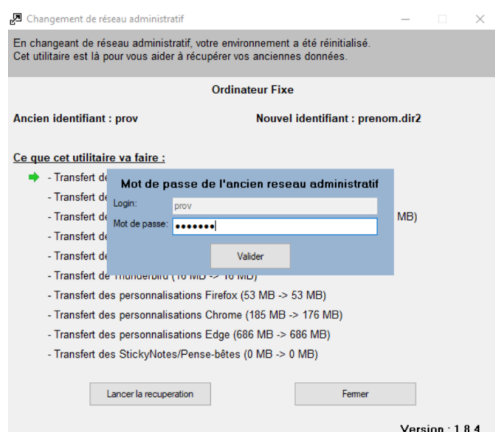
Suivant ce type, la recopie ne se fait pas au même endroit :

- Vers U:\Documents_AncienProfil sur le nouveau serveur de fichier (SFADM) pour un ordinateur fixe
- Vers C:\Users\SESSION_PEDAGO\Documents pour un ordinateur portable

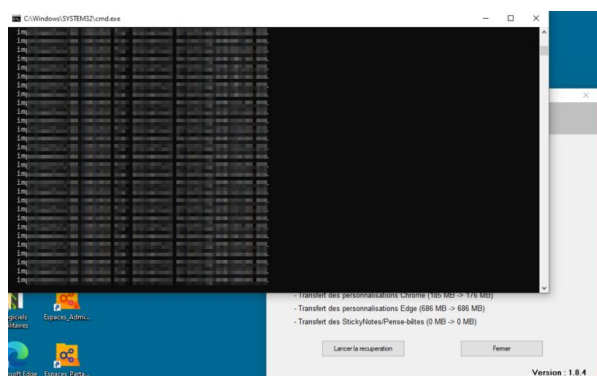


En cliquant sur le bouton "Lancer la récupération" vous déclenchez le déplacement des données.

Le **mot de passe de votre ancien compte** vous est alors demandé.



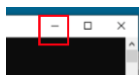
Les actions de transfert vont alors commencer. Plusieurs fenêtres sur fond noir vont apparaître pour chacun des transferts.



Si les fenêtres vous gênent, vous pouvez la réduire en cliquant sur le bouton.

Selon la quantité de données et la qualité de votre machine/ réseau, le transfert peut être long.

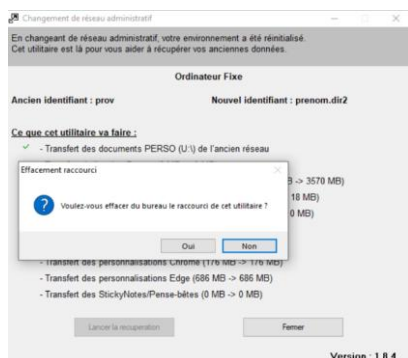
Il est cependant recommandé d'attendre la fin des transferts avant de lancer les programmes suivants : Firefox / Chrome / Edge / Thunderbird puisque les données sont en cours de recopie.



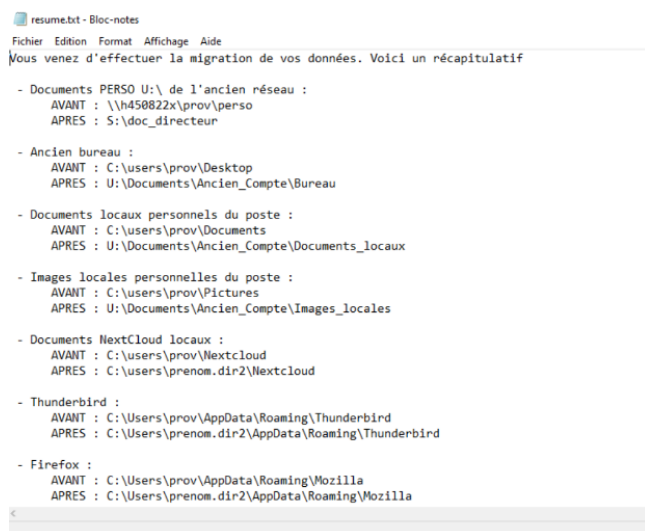
Eviter de cliquer sur le bouton fermer (la croix). Vous interrompriez le processus de récupération et vous seriez obligé de le relancer.

Le temps de récupération des données dépend du volume de celui-ci.

A la fin de la récupération, le bouton Fermer devient actif et vous propose d'enlever le raccourci (il sera réellement effacé à la prochaine connexion).



Lorsque vous cliquez sur Fermer, un résumé des actions entreprises est détaillé dans un Bloc-Notes. Nous vous recommandons de le sauvegarder.



Après cette étape, vous pouvez lancer les programmes **Firefox / Chrome / Edge / Thunderbird**.

Si le transfert s'est bien déroulé, vous devriez retrouver votre environnement habituel dans ces programmes, **à l'exception des mots de passe dans Edge et Chrome**.

En cas de souci, un agent du SNE, de la DSI ou une sollicitation du GIP Recia devrait nous permettre de vous dépanner.

9.5. FAQ Migration

Voici les questions qui nous sont le plus couramment posées sur la migration administrative

- **A quoi sert cette enquête de Préparation administrative ?**
 - L'objectif est double : tenter de recueillir l'ensemble des personnels utilisant les machines administratives (une sorte d'organigramme de l'établissement) et permettre aux personnels administratifs qui sont l'unique utilisateur d'une machine de récupérer une grande part de leur profil (données de navigation, profil Thunderbird).
- **Avez-vous un document à destination de mes personnels ?**
 - Nous espérons que ce [document](#) peut vous être utile
- **J'ai plusieurs utilisateurs qui utilisent la même machine administrative. Qui doit remplir l'enquête ?**
 - L'objectif étant de récupérer les personnalisations, nous n'avons pas prévu de multiples usagers sur la même machine, en conséquence, c'est le "principal utilisateur" de chaque machine qui doit remplir.
 - Dans le cas d'une machine non attribuée à un personnel, il n'est pas nécessaire de remplir l'enquête administrative (aucune personnalisation n'aura besoin d'être récupérée). La machine sera migrée et les personnels ayant besoin de l'utiliser s'y connecteront avec leurs nouveaux identifiants nominatifs après migration.
- **Je ne connais pas mes identifiants pédagogiques.**
 - Si vous avez déjà accédé à l'ENT, voir cette [page](#)
 - Si vous n'avez pas encore activé votre compte ENT, rendez-vous sur l'ENT, identifiez-vous et cliquez sur Activer mon compte ENT.
- **Les AED sont-ils concernés par l'enquête ?**
 - Sur demande du RSSI du Rectorat, les AED, et les postes vie scolaire, devront passer dans le réseau pédagogique et n'accéderont pas au serveur de fichiers administratifs. Si des documents étaient partagés sur Horus entre les CPE et les AED, il convient de passer sur un partage de fichier par Nextcloud.
- **Quel est le temps d'immobilisation de chaque machine ?**
 - Nous espérons le plus court possible, l'objectif de la préparation de la migration est que dans les cas "simples" (pas de GFC, pas de particularisme), l'utilisateur soit quasiment autonome. Il y a cependant un temps incompressible, celui de la sortie du domaine Horus et de l'entrée dans le domaine AD. Cette opération nécessite plusieurs redémarrages de la machine, et une mise à jour des paquets logiciels.
- **Transférez-vous les données d'Horus ?**
 - Les données du "docs_partage" d'Horus ayant été préparées, rangées et archivées, une recopie dans les dossiers correspondant est faite la veille du Jour J.

- Si des dossiers/fichiers ne sont pas dans un partage "normalisé" sont recopiés dans "doc_transitoire_migration". Ce dossier accessible aux membres de la direction permettra de redistribuer les données aux personnels adéquats.
- **Comment sont nommés les dossiers des partages du nouveau SFADM ?**
 - La description en est faite ici : [Matrice collèges](#) - [Matrice lycées](#)
Suite au travail en commission, les dossiers ne sont pas nommés sur leurs fonctionnalités, mais suivant la fonction des utilisateurs.
- **J'ai beaucoup de dossier dans SFADM dont beaucoup ne sont pas ou ne seront jamais utilisés.**
 - Lors de la commission de préparation de ce serveur, notre objectif a été d'avoir la même arborescence dans tous les établissements, les partages sont donc identiques dans tous les établissements du second degré gérés par le GIP Recia.
- **Pourra-t-on utiliser le ScanToFolder sur le nouveau SFADM ?**
 - Le scan to folder est abandonné au profit du scan to mail. La directive du RSSI est d'abandonner les "scans" qui pourrait contenir des données personnelles dans un partage non maîtrisé.
- **Après la migration les accès au terminal de paiement électronique, aux logiciels de type MYANTIRIADE ou TURBOSELF fonctionneront ils correctement ?**
 - La migration administrative ne touche ni aux logiciels installés sur les stations ni au réseau dans lequel sont intégrés les ordinateurs donc pas de raison que l'accès au terminal de paiement et aux logiciels MYANTIRIADE et TURBOSELF soit impacté. Seuls les logiciels installés dans le profil utilisateur pourraient être impactés. Il est nécessaire de vérifier que tous les logiciels utilisés couramment sont fonctionnels après migration.
- **L'accès au Dossier "Documents" sera-t-il toujours possible sur nos PC après la migration ?**
 - En ce qui concerne les données personnelles, 2 cas :
 - Tout ce qui est dans le perso des utilisateurs (lecteur U) est synchronisé dans le nouveau "perso" des usagers "Espace_Personnel" (toujours lecteur U)
 - Poste fixe : Tout ce qui est dans les documents en local (soit dans le profil utilisateur) est également reporté dans le nouveau "perso" des usagers "Espace_Personnel" (toujours lecteur U)
 - Poste portable : les documents locaux sont déplacés de l'ancien profil vers le nouveau (Recopie des documents locaux).
 - Mais il est essentiel de rappeler aux utilisateurs de sauvegarder régulièrement leurs données locales sur le serveur, donc dans le U:\Documents. Enfin, l'ancien profil n'est pas effacé (ce qui peut d'ailleurs poser des problèmes d'espace disque), les données sont toujours présentes.

9.6. Matrice des partages dans les collèges et lycées

Matrice des partages dans les collèges :

Groupe associé à la fonction																							
Version COLLEGE		@dir	@diradj	@sec-dir	@sec-eleve	@gestionnaire	@sec-gestion	@agtcompt	@sec-agtcompt	@cpe	@agent-encadrant	@agent-encadrant-cuisine	@agents	@infirmerie	@as	@psyen	@greta	@dir-segpa	@coord-ulis	@coord-mlds	@coord-classe-relais		
Membres																							
		Nom des groupes de fonctions (venant de l'ENT ou de OMICO)																					
doc_directeur		x																					
doc_direction		x	x																				
doc_direction_sec-dir		x	x	x																			
doc_direction_sec-eleves		x	x	x	x																		
doc_direction_cpe		x	x							x													
doc_direction_gestion		x	x			x																	
doc_direction_gestion_sec-dir		x	x	x		x																	
doc_direction_gestion_sec-dir_cpe		x	x	x		x				x													
doc_direction_cpe_infirmerie_social_psyen		x	x							x				x	x	x							
doc_direction_segpa		x	x															x					
doc_direction_ulis		x	x																x				
doc_direction_mlds		x	x																	x			
doc_direction_classe_relais		x	x																		x		
doc_gestionnaire						x																	
doc_dir_gestionnaire		x				x																	
doc_gestion_sec-gest		x				x	x																
doc_gestion_agent-encadrant		x				x	x					x											
doc_gestion_cuisine		x				x	x						x										
doc_agtcompt		x						x															
doc_agtcompt_sec-agtcompt		x						x	x														
doc_cpe										x													
doc_dir_cpe		x								x													
doc_infirmerie		Nom des dossiers													x								
doc_social		Les membres es groupes														x							
doc_psyen		cochés ont le droit de lecture-															x						
doc_infirmerie_social_psyen		écriture sur le dossier													x	x	x						
doc_segpa		x																	x				
doc_ulis		x																		x			
doc_mlds		x																			x		
doc_classe_relais		x																			x		
doc_communs		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		

Matrice des partages dans les lycées :

Groupe associé à la fonction		Version validée 14 nov 2025											
Version LYCEE		@dir	@diradj	@sec-dir	@sec-eleve	@ddfpt	@sec-ddfpt	@gestionnaire	@sec-gestion	@agtcompt	@sec-agtcompt	@cpe	@agent-encadrant
Nom des dossiers Les membres des groupes cochés ont le droit de lecture-écriture sur le dossier													
Membres													

doc_directeur doc_direction doc_direction_sec-dir doc_direction_sec-eleves doc_direction_ddfpt doc_direction_cpe doc_direction_gestion doc_direction_gestion_sec-dir doc_direction_gestion_sec-eleves	Nom des groupes de fonctions (venant de l'ENT ou de OMICO)											
	x											
	x	x										
	x	x	x									
	x	x	x	x								
	x	x	x		x							
	x	x				x						
	x	x										
	x	x										

doc_ddfpt doc_dir_ddfpt doc_ddfpt_gestion_sec doc_ddfpt_sec-ddfpt												
	x					x						
	x					x						
	x					x	x	x	x			

doc_gestionnaire doc_dir_gestionnaire doc_gestion_sec-gest doc_gestion_agent-encadrant doc_gestion_agents doc_gestion_cuisine												
	x							x				
	x							x	x			
	x							x	x			
	x							x	x			

doc_agtcompt doc_agtcompt_sec-agtcompt	x									x		
	x									x	x	

doc_cpe doc_dir_cpe												
	x											

doc_infirmierie												
-----------------	--	--	--	--	--	--	--	--	--	--	--	--

doc_communs	x	x	x	x	x	x	x	x	x	x	x	x
-------------	---	---	---	---	---	---	---	---	---	---	---	---

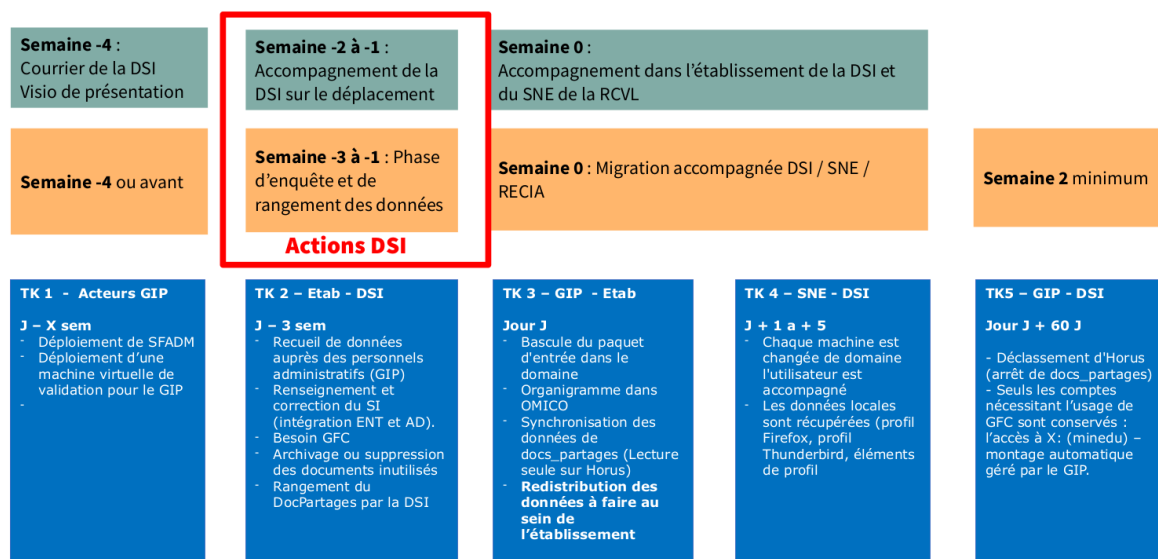
doc_transitoire_migration	x	x			x		x		x			
---------------------------	---	---	--	--	---	--	---	--	---	--	--	--

Supprimé à l'été 2026

9.7. Suivi du projet

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	UAI	Nom	SNE	Département	Nombre PC	Nom référent	Jours Ouverts avant migration	date de début mise en place GIP	injection tickets	date de fin mise en place GIP - DSU	Observations GIP - DSU	JOUR J Date début intervention SNE	Date fin intervention SNE	Observations SNE	Terminé	GFC ACTIF	ANNÉE du jour j	MOIS du jour j	JOUR du jour j	
2	0281197Z	Lycée Polyvalent Joséphine Baker		Nord	28	24	972.00	25/08/2022	SO	13/07/2022	SFADM sans migration de données	01/06/2022		Pas d'intervention SNE	oui	OUI	2022	6	1	
3	0280864M	LP Elsa TRIOLET	Nord	28	14		165.00	23/06/2025	oui	07/07/2025		04/07/2025	07/07/2025		oui	OUI	2025	7	4	
4	0180036S	Lycée Polyvalent HENRI BRISSON	Sud	18	40		82.00	22/09/2025	oui	01/10/2025		29/10/2025	07/11/2025		oui	OUI	2025	10	29	
5	0280925D	LP Gilbert COURTOIS	Nord	28	21		82.00	22/09/2025	oui	01/10/2025		29/10/2025	07/11/2025		oui	OUI	2025	10	29	
6	0360099P	LGT Pierre et Marie CURIE	Sud	36	33		82.00	22/09/2025	oui	01/10/2025		29/10/2025	07/11/2025		oui	OUI	2025	10	29	
7	0370037P	LGT CHOISEUL	Ouest	37	48		82.00	22/09/2025	oui	01/10/2025		29/10/2025	07/11/2025		oui	OUI	2025	10	29	
8	0410031L	LP André AMPÈRE	Ouest	41	24		82.00	22/09/2025	oui	01/10/2025		29/10/2025	07/11/2025		oui	OUI	2025	10	29	
9	0451442Y	LP Château BLANC	Est	45	33		82.00	22/09/2025	oui	01/10/2025		29/10/2025	07/11/2025		oui	NON	2025	10	29	
10	0281021H	LP SULLY	Nord	28	19		49.00	24/11/2025	oui	10/12/2025		15/12/2025	19/12/2025	Le 3 PC qui restent à migrer sont supprimés et vont être déclassés	oui	OUI	2025	12	15	
11	0360008N	Lycée Général Jean GIRAUDOUX	Sud	36	22		49.00	24/11/2025	oui	10/12/2025		15/12/2025	19/12/2025		oui	OUI	2025	12	15	
12	0370009J	Lycée Polyvalent RABELAIS	Ouest	37	30	M.Brethoux Nicolas	49.00	24/11/2025	oui	10/12/2025		15/12/2025	19/12/2025	6 postes encore présents à migrer	oui	OUI	2025	12	15	
13	0451304Y	Lycée Hotelier de L'Orléanais	Est	45	25		49.00	24/11/2025	oui	10/12/2025		15/12/2025	19/12/2025		oui	OUI	2025	12	15	
14	0180035R	Lycée Polyvalent Edouard VAILLANT	Sud	18	40		34.00	01/12/2025	oui	19/12/2025		05/01/2026			oui	NON	2026	1	5	
15	0280022X	LP Maurice VIOLLETTE	Nord	28	25		34.00	01/12/2025	oui	19/12/2025		05/01/2026			oui	NON	2026	1	5	
16	0410718H	LP Val de Cher	Ouest	41	16		34.00	01/12/2025	oui	19/12/2025		05/01/2026		les adm-cam -> vian technique (vian14)	oui	OUI	2026	1	5	
17	0451104F	EREA Simone VEIL	Est	45	18		34.00	01/12/2025	oui	19/12/2025		05/01/2026			oui	OUI	2026	1	5	
18	0280659P	EREA François TRUFFAUT	Nord	28	18		29.00	08/12/2025	oui	08/01/2026		12/01/2026		Reste 1 portable APS -> arrêt maladie	oui	OUI	2026	1	12	
19	0360024F	LPQ BALZAC D'ALEMBERT	Sud	36	29	Thomas Tourteik-Pisson	29.00	08/12/2025	oui	08/01/2026		12/01/2026			oui	OUI	2026	1	12	
20	0371099U	LP Henri BECQUEREL	Ouest	37	19	Mme VIKET Amélie	29.00	08/12/2025	oui	08/01/2026		12/01/2026			oui	OUI	2026	1	12	
21	0450786K	LP Paul GAUGUIN	Est	45	22		29.00	08/12/2025	oui	08/01/2026		12/01/2026			oui	OUI	2026	1	12	
22	0280700J	LP Jean-Félix PAULSEN	Nord	28	16		24.00	15/12/2025	oui	16/01/2026		19/01/2026		reste 1 poste (AS) - en vire	oui	OUI	2026	1	19	
23	0360050J	EREA Eric TABARLY	Sud	36	19		24.00	15/12/2025	oui	16/01/2026		19/01/2026		reste 1 poste inf en arrêt maladie	oui	NON	2026	1	19	
24	0371100V	LP Joseph CUGNOT	Ouest	37	17	Mme Simoneau-Le-Sager Angelique	24.00	15/12/2025	oui	16/01/2026		19/01/2026			oui	NON	2026	1	19	
25	0450043C	LP Jeannette VERDIER	Est	45	23		24.00	15/12/2025	oui	16/01/2026		19/01/2026			oui	OUI	2026	1	19	
26	0280009H	LP Philibert de L'ORME	Nord	28	21		19.00	05/01/2026	oui	23/01/2026		26/01/2026		Vie scolaire à finir	en cours	OUI	2026	1	26	
27	0360005K	Lycée Polyvalent PASTEUR	Sud	36	26		19.00	05/01/2026	oui	23/01/2026		26/01/2026		Mme Pascale ROGER assure l'indém de Mme AZEMA	oui	OUI	2026	1	26	
28	0410030K	LGT RONSARD	Ouest	41	27		19.00	05/01/2026	oui	23/01/2026		26/01/2026		Reste le serveur Alise	oui	OUI	2026	1	26	
29	0450750W	LP Jean de la TAILLE	Est	45	16		19.00	05/01/2026	oui	23/01/2026		26/01/2026			oui	OUI	2026	1	26	
30	0180023X	LP VAUVERT	Sud	18	17		14.00	12/01/2026	oui	30/01/2026		02/02/2026			oui	OUI	2026	2	2	
31	0280036M	Lycée Polyvalent Rémi BELLEAU	Nord	28	26		14.00	12/01/2026	oui	30/01/2026		02/02/2026		Inf à finir	oui	OUI	2026	2	2	
32	0371211R	LP BEAUREGARD	Ouest	37	18	Mme Camille Girard DOFFI	14.00	12/01/2026	oui	30/01/2026		02/02/2026			oui	OUI	2026	2	2	
33	0451037H	LP Marguerite AUDOUX	Est	45	28		14.00	12/01/2026	oui	30/01/2026		02/02/2026			oui	OUI	2026	2	2	
34	0180007K	LGT Jacques COEUR	Sud	18	44		9.00	19/01/2026	oui	09/02/2026		09/02/2026		2 postes à terminer	en cours	NON	2026	2	9	
35	0280007F	Lycée Général MARCEAU	Nord	28	29		9.00	19/01/2026	oui	09/02/2026		09/02/2026		Inf à finir	oui	OUI	2026	2	9	
36	0371123V	LP CHAPTAL	Ouest	37	21	M.Husson Gilles Proviseur	9.00	19/01/2026	oui	09/02/2026		09/02/2026			oui	OUI	2026	2	9	
37	0410832G	LP Sonia DELAUNAY	Est	41	19		9.00	19/01/2026	oui	09/02/2026		09/02/2026			oui	NON	2026	2	9	
38	0180024D	Lycée Polyvalent Jean MOULIN	Sud	18	24	David Quatry, secrétaire général	-8.00	26/01/2026	oui	16/02/2026		02/03/2026			en cours	OUI	2026	3	2	
39	0281077U	Lycée Polyvalent Silvia MONFORT	Nord	28	29		-8.00	26/01/2026	oui	16/02/2026		02/03/2026			en cours	OUI	2026	3	2	
40	0370054H	LP Martin NADAUD	Ouest	37	23	Mme MONTANE Christèle ProvADJ	-8.00	26/01/2026	oui	16/02/2026		02/03/2026			en cours	OUI	2026	3	2	
41	0450029M	LGT Bernard PALISSY	Est	45	36	Mme SAINCHIS Angéline, Provisseuse M. MERLANT Benoît, référent numérique	-8.00	26/01/2026	oui	16/02/2026		02/03/2026			en cours	OUI	2026	3	2	
42	0180025E	LP Jean GUEHENNO	Sud	18	25	Saskia SCHMID, secrétaire générale	-13.00	02/02/2026	oui	06/03/2026		09/03/2026			en cours	OUI	2026	3	9	

9.8. Planning



- **Jour j / semaine 0** : bascule de l'entrée dans le domaine / serveur Horus en lecture seule
- **Ticket 1 : J - 4 semaines** : déploiement de sfadm / visio de présentation aux provideurs.
- **Ticket 2 : J - 3 semaines** : Recueil des données sur les postes (application qui demande à l'utilisateur s'il connaît son compte) - **Dialogue nécessaire** / Rangement et archivage des données de docs_partages
- **Ticket 3 : J 0** : Une fois les **données intégralement recueillies**, la bascule est préparée :
 - Changement du paquet de jonction au domaine
 - Organigramme de l'établissement reporté dans Omico pour affectation aux groupes de fonctions
 - Passage de Horus en lecture seule
- **Ticket 4 : J+0 à +5 | Semaine 0** : Changement de domaine de chaque ordinateur du réseau GESTION, récupération des données et profils. Accompagnement de l'utilisateur sur le changement.
- **Ticket 5** : Déclassement du Horus (suppression des comptes / archivages des données / arrêt de la fonctionnalité d'authentification)

Durant les 3 semaines précédant la migration, des actions sont effectuées par les collègues des DSI départementales.