
Rapport de stage

novarina

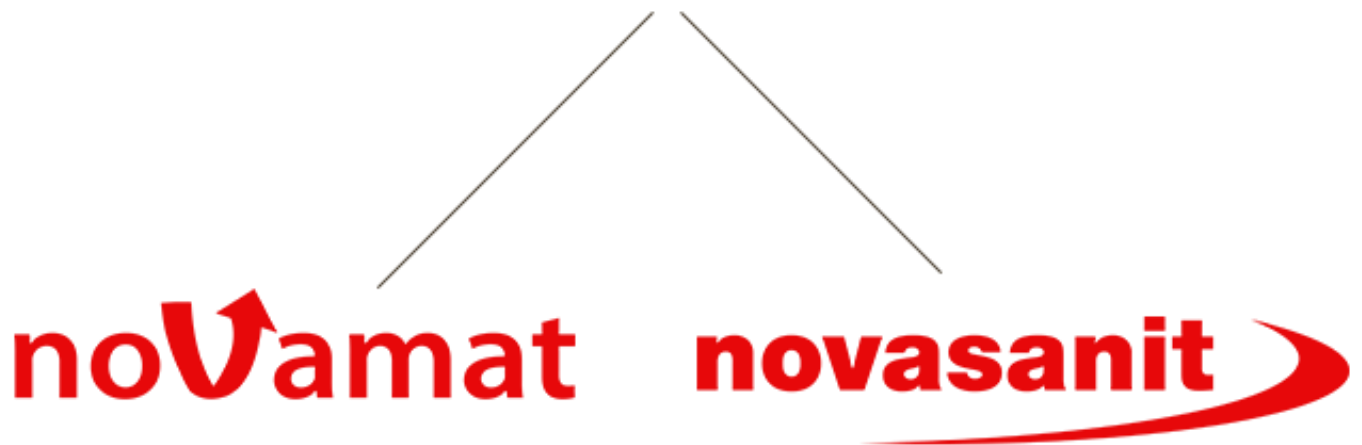


Table des matières

Matériel mis à disposition	3
<i>Physiques</i> :	3
<i>Outils et Logiciels</i> :	4
Présentation des baies de brassages	6
<i>Baie 1</i> :	6
<i>Baie 2</i> :	7
Plan des bureaux Novarina	8
<i>Visuel technique</i>	8
Présentation de GLPI et ses outils	9
<i>Profil</i> :	9
<i>Inventaire automatique</i> :	9
<i>Gestion des tickets</i>	10
<i>Supervision via SNMP</i>	10
Déploiement d'un gestionnaire de mots de passe	12
<i>Contexte et objectif</i>	12
<i>Organisation et Méthodologie</i>	13
<i>Chronologie</i>	13
<i>Mise au point</i>	14
<i>Gestion de projet</i>	15
<i>Mise en œuvre</i>	16
<i>Configuration</i> :	16
<i>Réunion de lancement</i>	18
Parc d'impression (Mission secondaire)	19
<i>Contexte et objectif</i>	19
<i>Réalisation</i>	20
<i>Imprimante ThononR-ADM</i> :	20
Gestion des partages et autorisations (Mission secondaire)	32
<i>Contexte et objectif</i>	32
<i>Réalisation</i>	32
Assainissement de l'Active Directory (Mission secondaire)	37
<i>Contexte et objectif</i>	37
<i>Réalisation</i>	37

Matériel mis à disposition

Physiques :

PC Portable :

- **Fabricant** : Acer
- **Modèle** TravelMateP414-51
- **OS** : Microsoft Windows 11 Professionnel
- **Processeur** : 11h Gen Intel(R) Core (™) i5-1135G7 @ 2.40GHz, 2419 MHz, 4 cœurs, 8 processeurs logiques
- **Mémoire** : 8 GB

Ecran :

- **Modèle** : DELL P2723DE
- **Fabricant** : Dell
- **Mode Bureau** : 2560 * 1440, 60Hz

Clavier :

- **Fabricant** : Clavier standard
- **Modèle** : Clavier standard PS/2

Souris :

- **Fabricant** : HID
- **Modèle** : Souris HID

Casque :

- **Fabricant** : Microsoft
- **Modèle** : Microsoft Modern USB HeadSet
- **Port** : USB-A

Outils et Logiciels :

Compte AD avec plusieurs ressources

Licence : Microsoft 365 Business Standard

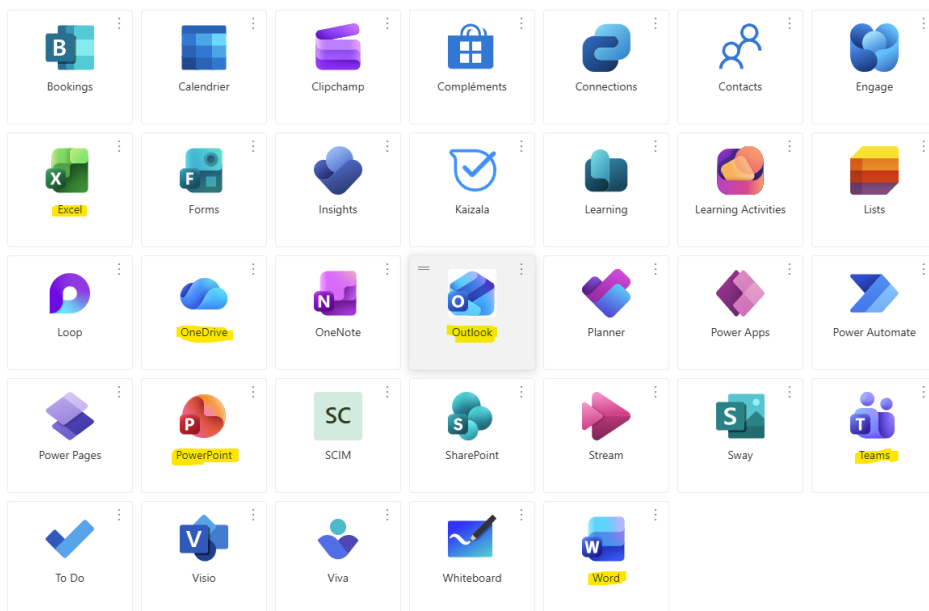
Tableau de bord des applications

Ajouter des applications Créer une collection Personnaliser la vue

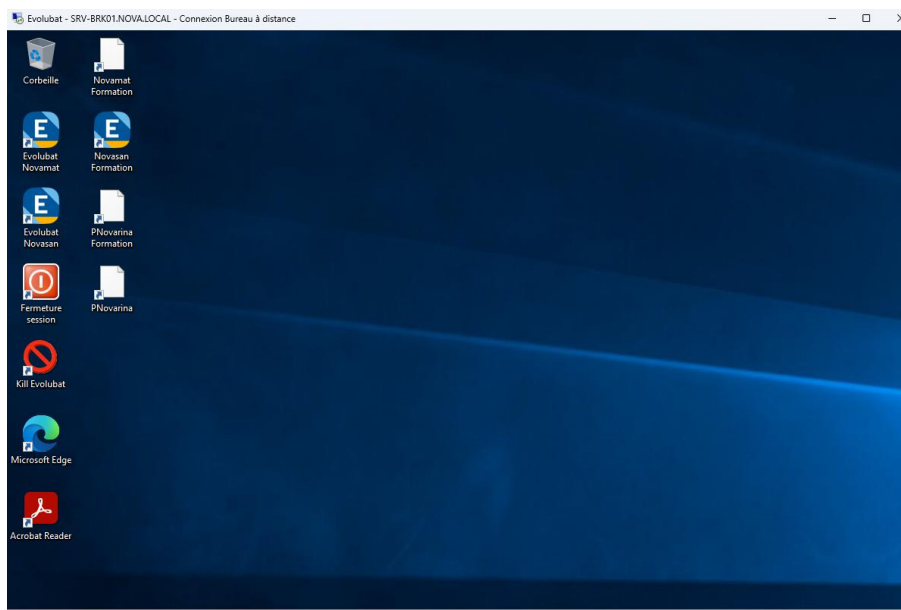
Apps

Apps

Paramètres



Evolubat, PGI de l'entreprise (Progiciel de Gestion Intégrée), connexion en RDP



VPN

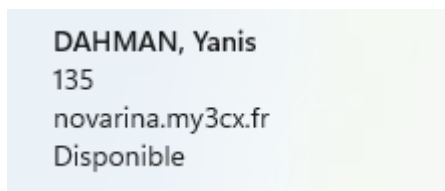
En cas de déplacement à l'extérieur, vous aurez besoin de vous connecter au VPN pour avoir accès à Evolubat et aux fichiers partagés.



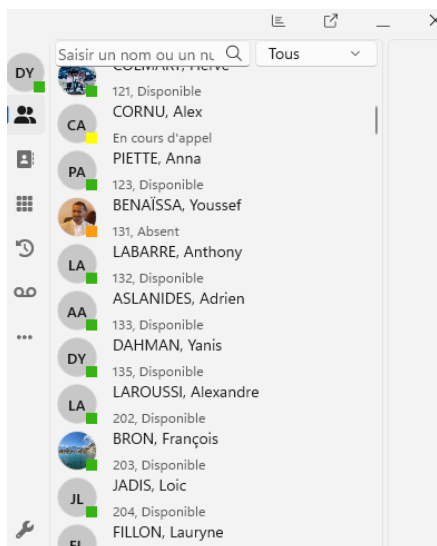
Attention, le VPN ne fonctionne pas lorsque nous sommes connectées au réseau de l'agence.

3CX

Logiciel permettant de gérer la communication dans toutes l'entreprises en passant par internet plutôt que des signaux téléphoniques classiques

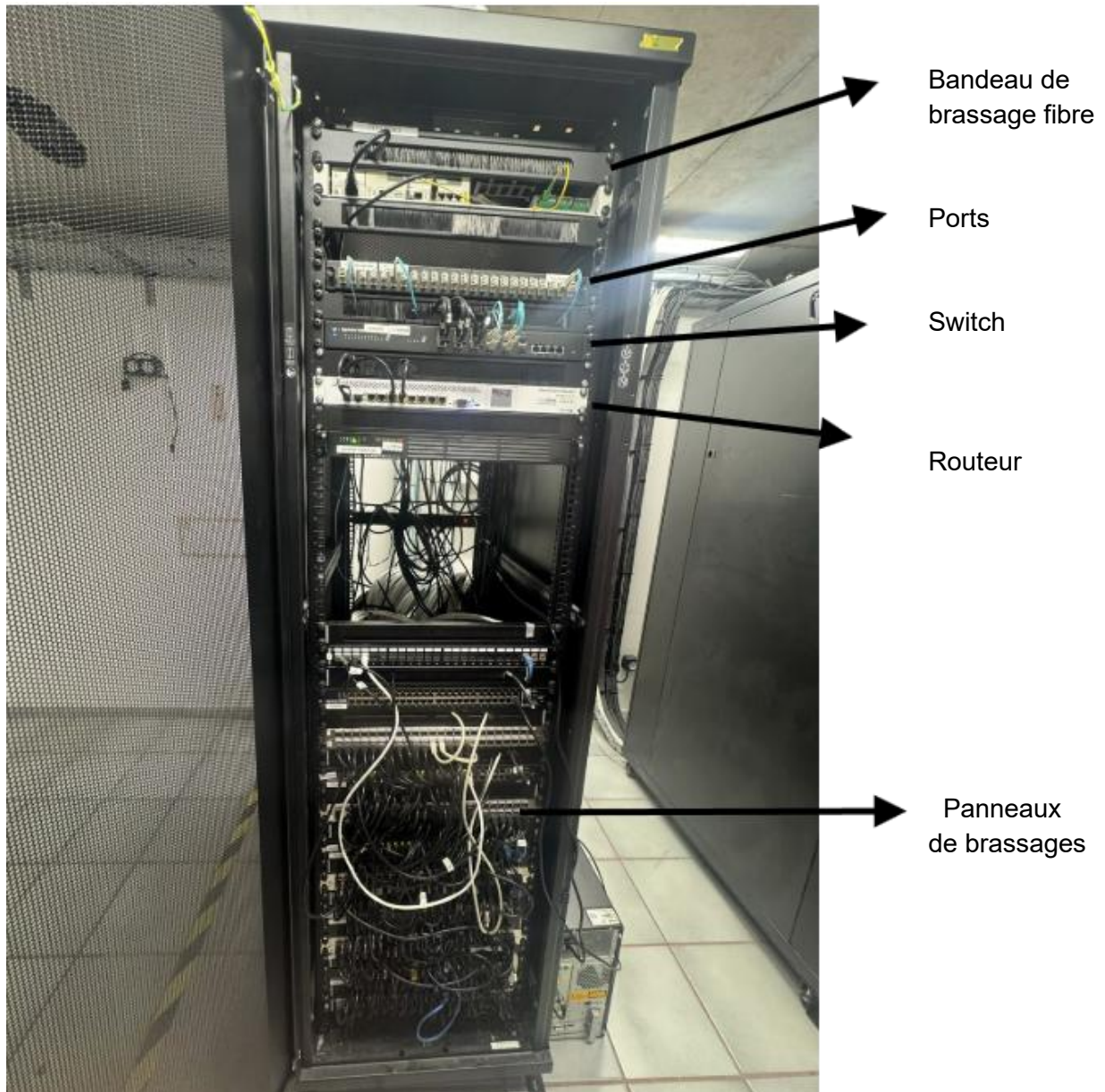


On peut voir ci dessus mon **id** avec lequel j'ai pue me connecter au **serveur de téléphonie** et ainsi je peux directement communiquer avec tout le personnel de l'entreprises

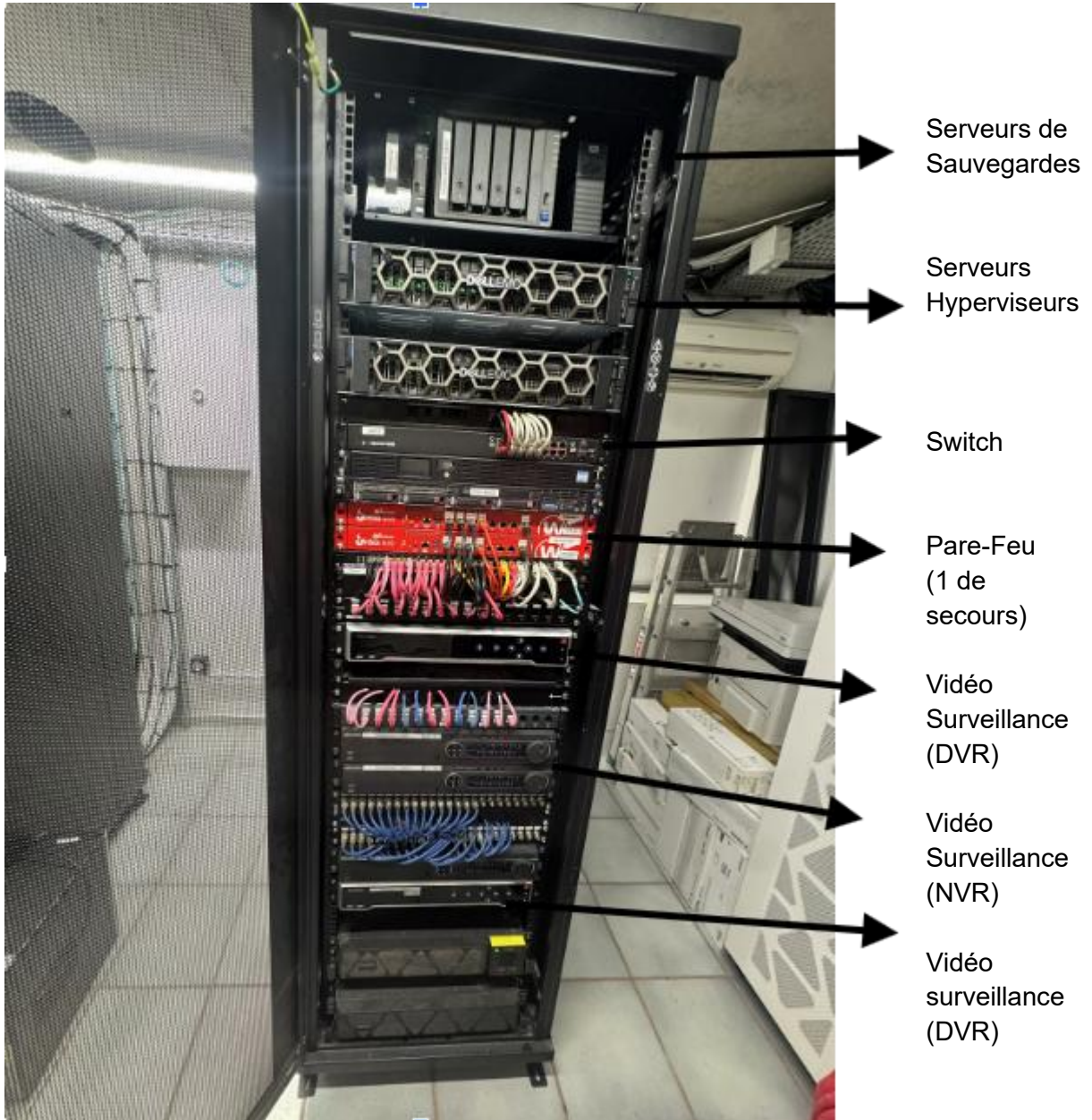


Présentation des baies de brassages

Baie 1 :



Baie 2 :

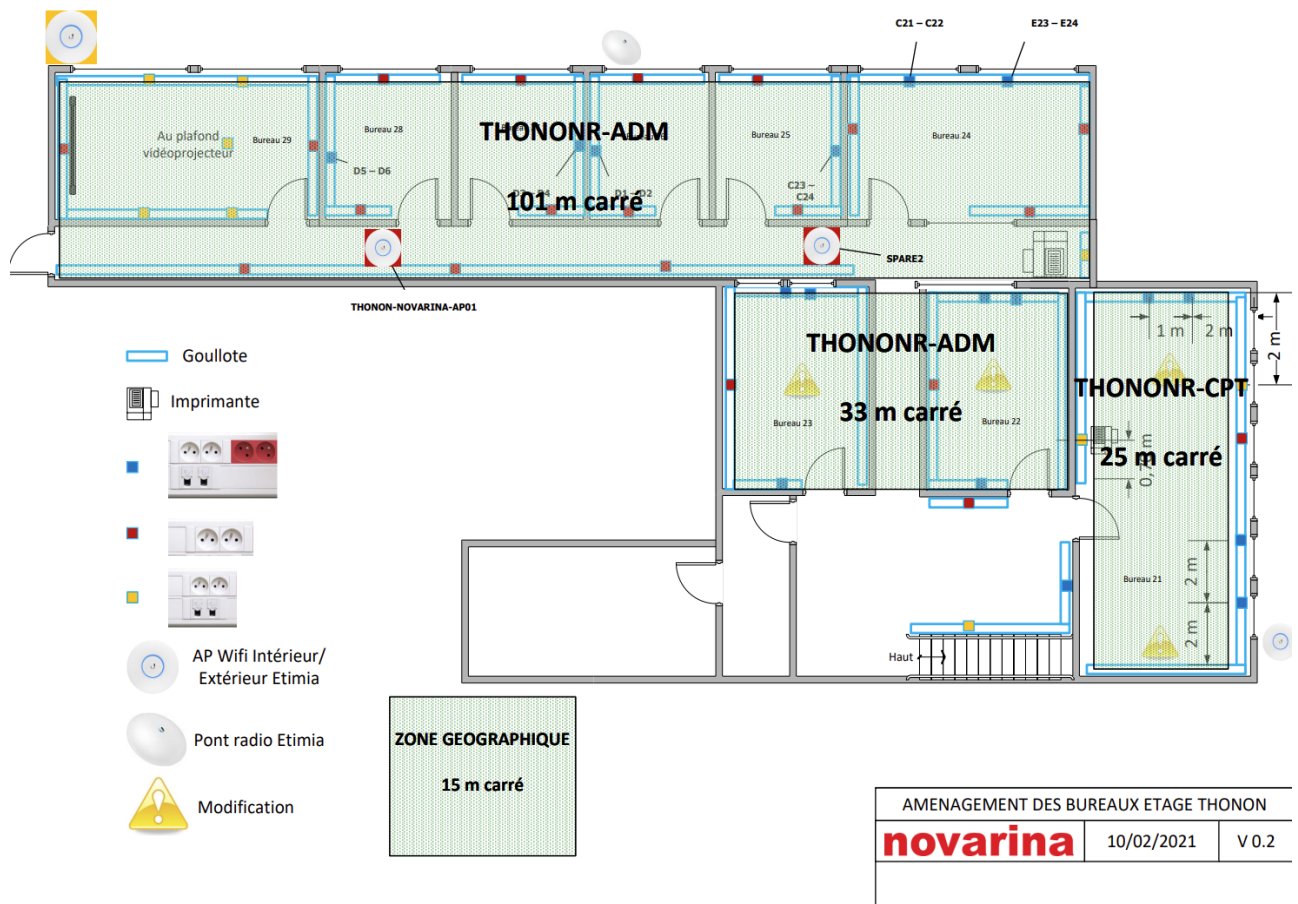


Plan des bureaux Novarina

Le siège social de **Novarina** se situe à Thonon-les-Bains.

Mon poste de travail est situé au **Bureau 22**, on y retrouve à l'intérieur 3 environnements de travail, 2 pour les techniciens en informatique et 1 pour les stagiaires.

Visuel technique



Le plan détaille l'emplacement des infrastructures techniques essentielles, comme les **bornes Wi-Fi**, les **imprimantes** et les **prises réseau**.

Présentation de GLPI et ses outils

Profil :

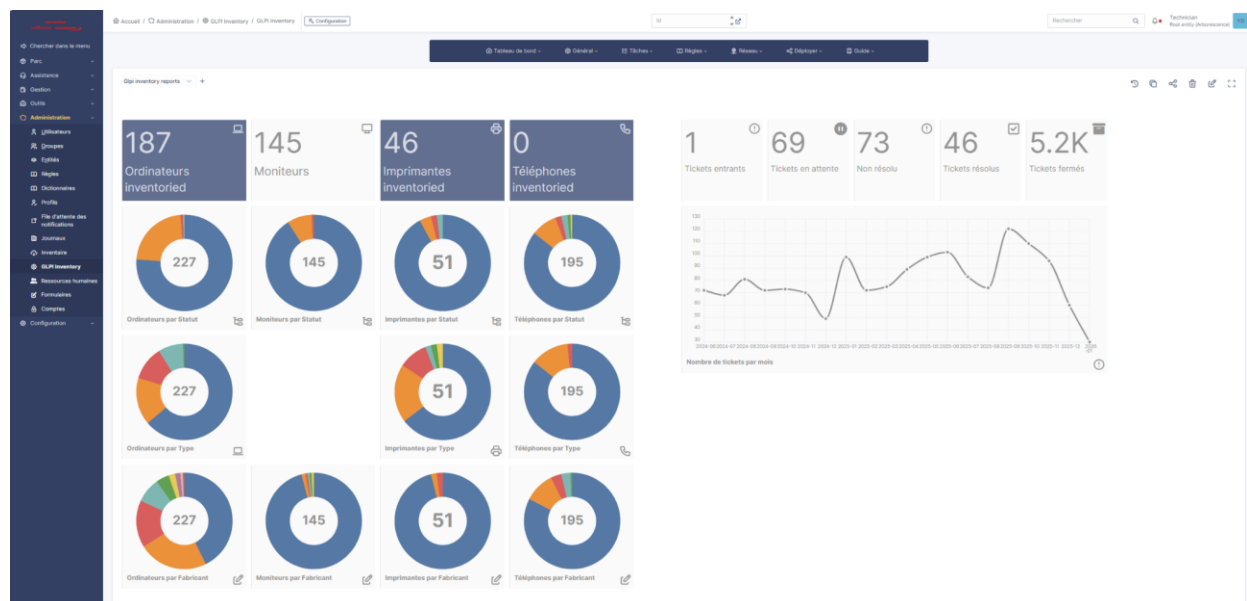
En tant que stagiaire, j'ai un accès **'Technicien'** qui me permet de voir l'inventaire et de traiter les tickets, sans modifier la configuration du serveur.



Inventaire automatique :

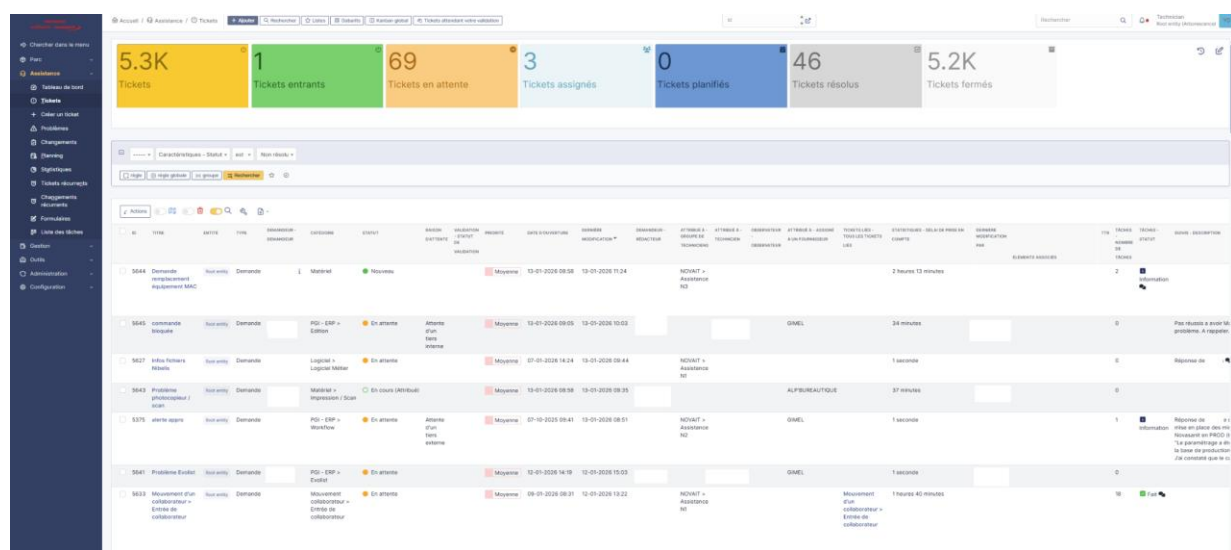
Le matériel est remonté automatiquement grâce aux agents configurés, ça a été configurer via des plugins.

Statut **'Inventoried'** = matériel suivi et actif, on voit qu'il a été répertorié à la fois les ordinateurs, les imprimantes, les moniteurs



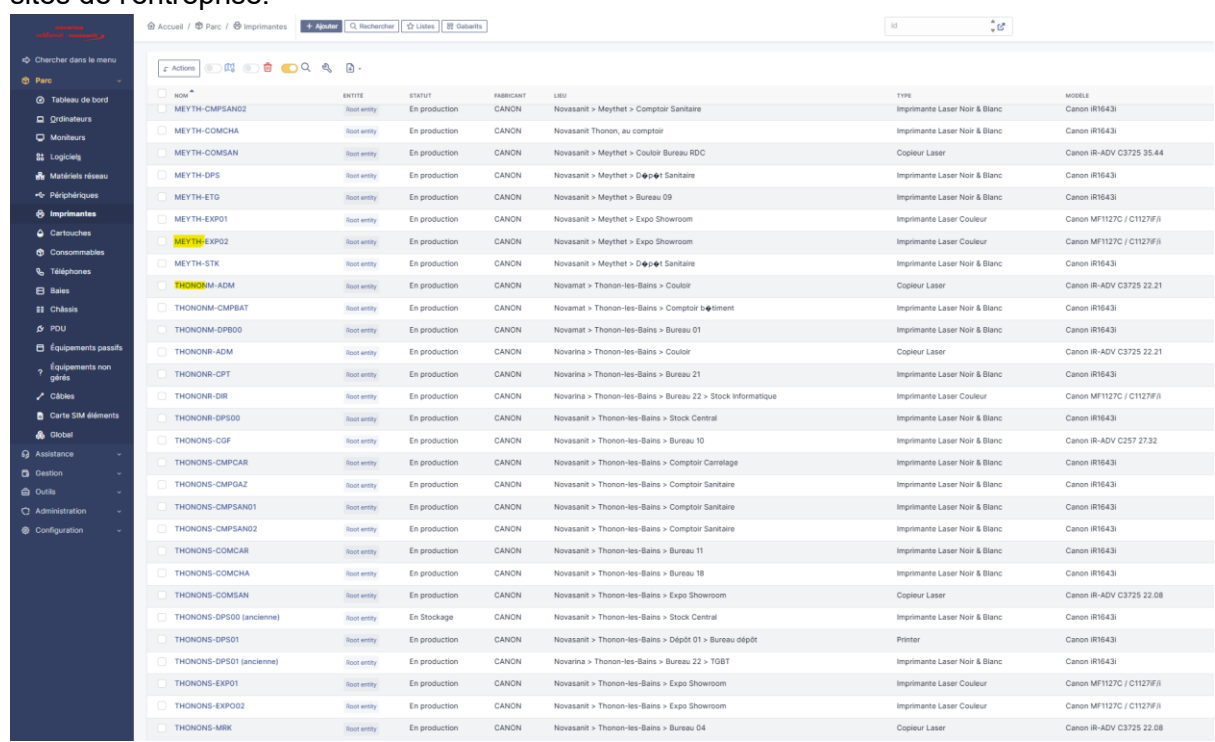
Gestion des tickets

L'interface de gestion des tickets me permet de visualiser la file d'attente. Je peux prioriser les demandes (**Urgence/Impact**) et suivre l'état d'avancement de chaque incident, de son ouverture jusqu'à sa clôture.



Supervision via SNMP

Les imprimantes remontées dans l'inventaire incluent le nom de leur ville dans leur identifiant. Ça permet de visualiser l'ensemble du parc d'impression réparti sur les différents sites de l'entreprise.



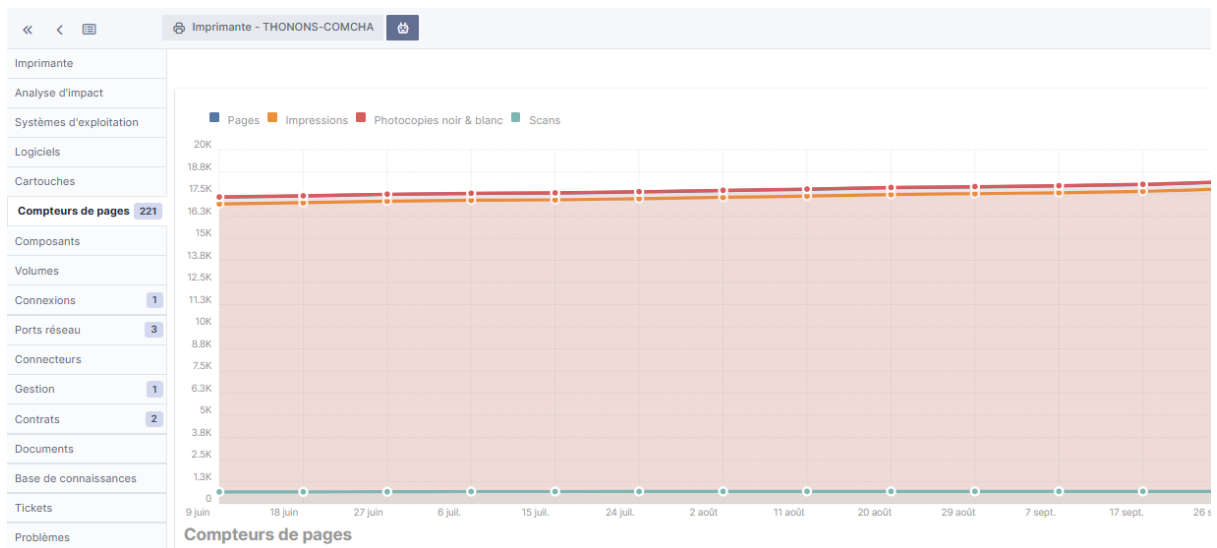
Je sélectionne une imprimante à proximité



Cette étape valide la concordance entre l'identifiant SNMP utilisé dans GLPI et la chaîne de communauté (Community String) définie sur l'interface de l'imprimante.

Identifiant SNMP ▼ i

Et on peut observer ici, la **supervision** du volume d'impression et de l'évolution des compteurs



Enfin, ici on peut voir la remontée des cartouches d'encre

Cartouche - Informations inventoriées

Propriété	Valeur
Tambour Noir	75%
Tambour Cyan	75%
Tambour Magenta	75%
Tambour Jaune	75%
Kit unité de fusion	75%
Kit d'entretien	75%
Toner Noir	85%
Toner Cyan	33%
Toner Magenta	34%
Toner Jaune	75%
Corbeille	75%

Déploiement d'un gestionnaire de mots de passe

Contexte et objectif

La sécurité informatique est un enjeu majeur pour les entreprises.

Une mauvaise gestion des mots de passe (mots de passe trop simples, réutilisés ou notés sur des supports non sécurisés) peut entraîner des risques importants : accès non autorisés, perte de données ou incidents de sécurité.

Dans ce contexte, l'entreprise souhaite mettre en place un outil de gestionnaire de mots de passe permettant aux collaborateurs de stocker et d'utiliser leurs mots de passe de manière sécurisée.

Je participe donc activement à ce projet, depuis la compréhension du besoin jusqu'au déploiement de la solution et à l'accompagnement des utilisateurs.

Objectif principal

Mettre en place et déployer une solution de gestionnaire de mots de passe destinée aux collaborateurs de l'entreprise.

Objectifs pédagogiques

À l'issue du stage, Je devrais être capable de :

- Comprendre les enjeux de base de la sécurité des systèmes d'information
- Suivre une méthodologie simple de gestion de projet
- Participer à l'analyse et au choix d'une solution informatique
- Rédiger des documents clairs (guides, procédures, synthèses)
- Communiquer avec des utilisateurs non techniques

Organisation et Méthodologie

Pour organiser et suivre mon stage, mon tuteur a mis en place un espace de travail collaboratif sur Microsoft Loop.

Cette page centralise l'ensemble des ressources nécessaires au bon déroulement de ma mission :

Chronologie

- **Semaines 1-2** (Intégration) : Phase de découverte et travaux préparatoires.
- **Semaines 3-6** (Mission) : Cœur du projet technique.
- **Semaines 6-7** (Compte rendu) : Finalisation du rapport, bilan et support aux utilisateurs en fin de projet.



Stagiaire - Premier semestre 2026

- 👤 Nom : DAHMAN Yanis
- 🎓 Formation : BTS SIO (SISR)
- 📍 Établissement : Lycée Gabriel Faure
- 📅 Stage du : 12/01/2026 ~ 06/03/2026
- 🕒 Horaire : 8h30~12h00 13h30~17h00
- 👤 Tuteur de stage : BENAÏSSA Youssef
- 🎯 Objectifs du stage : Sécurité informatique > Déployer un gestionnaire de mot de passe

- ▶ 🌱 Travail préparatoire
- ▶ 📅 Mission(s) du stage
- ▶ 📄 Moyens à utiliser
- ▶ 📅 Semaine 1~2 - Intégration
- ▶ 📅 Semaine 3~6 - Mission
- ▶ 📅 Semaine 6~7 - Compte rendu
- ▶ 📄 Suivi de stage

Mise au point

En complément de l'espace collaboratif Loop, un rythme de suivi régulier a été instauré avec mon tuteur (RSI) pour garantir la bonne dynamique du projet :

- **Fréquence des réunions** : Des points d'étape sont planifiés de manière hebdomadaire, chaque **mercredi et vendredi**.

- **Objectifs de ces points de suivi** :
 - **Mesurer l'avancement** : Faire le point sur les tâches réalisées depuis la dernière réunion.
 - **Lever les blocages** : Discuter des difficultés techniques ou organisationnelles rencontrées pour trouver des solutions rapides.
 - **Validation des livrables** : Présenter et faire valider les documents ou réalisations techniques attendus

Gestion de projet

Pour structurer la mission et valider chaque étape avec mon tuteur, j'ai produit les livrables suivants :

- **Planning prévisionnel du déroulement du projet**



PlanningPrévisionnelGMP.png

Ce document présente le calendrier du projet sur 6 semaines de stage, détaillant chaque phase, de l'étude à la mise en production

- **Livable consulté avec mon tuteur chaque mercredi et vendredi**



Livable.pdf

Ce document regroupe la phase de découverte des gestionnaires de mots de passe, la phase de recherche ainsi que l'étude comparative, le choix de la solution, la procédure technique ainsi que le plan d'action final de déploiement au sein de l'entreprise.

- **Guide Utilisateur**

Le guide utilisateur contient plusieurs documents, la vidéo de présentation du logiciel et de ses fonctionnalités et la procédure d'importation des mots de passe



PresentationFonctionnalités.mp4



ConnexionBitwarden.mp4



GuideD'importationMDP.mp4

- **Guide Administrateur**

Une documentation réservée à l'équipe technique qui regroupe les informations nécessaires pour administrer la plateforme



GuideAdministrateur.pdf

Mise en œuvre

Une fois le choix du gestionnaire de mots de passe validé avec mon tuteur, j'ai procédé à son installation sur mon poste.

Nous avons ensuite souscrit à la version "Entreprise" afin de débiter la configuration technique de la solution.

Configuration :

Configuration du SSO via le protocole SAML

L'entreprise utilisant déjà l'écosystème Microsoft pour la gestion des identités, j'ai configuré une **liaison SAML 2.0** entre Bitwarden et **Microsoft Entra ID**.

- **Côté Entra ID** : J'ai créé et configuré une application d'entreprise dédiée à Bitwarden pour générer les jetons d'authentification.
- **Côté Bitwarden** : J'ai configuré le service pour qu'il délègue la vérification de l'identité à Microsoft via ce flux SAML.

Résultat : Le **SSO** devient la seule porte d'entrée.

-L'utilisateur clique sur "Connexion avec SSO", tape son mail, et Microsoft valide son identité.

Configuration de l'approvisionnement SCIM

- J'ai configuré ce protocole pour synchroniser automatiquement les utilisateurs depuis Microsoft Entra ID vers Bitwarden.
- Cela permet de créer ou de supprimer des accès instantanément sans intervention manuelle.
- Résultat : Si un compte est coupé chez Microsoft, l'accès au coffre-fort est révoqué automatiquement.

Mise en place des politiques de sécurité

J'ai activé l'ensemble des politiques suivantes pour verrouiller l'environnement de l'entreprise :

- **Authentification SSO exigée**
- **Connexion automatique avec SSO**
- **Générateur de mot de passe**
- **Activer le remplissage automatique**
- **Options Send :**
- **Administration de récupération du compte**

Attributions des droits et privilèges

- **Service Informatique** : J'ai attribué des droits d'administration totale à l'équipe IT. Cela leur permet de gérer les utilisateurs, de configurer les politiques de sécurité et d'accéder à l'ensemble des collections de l'entreprise.
- **Utilisateurs (Autres services)** : Les autres collaborateurs ont des droits restreints. Ils peuvent utiliser les identifiants partagés, mais ne peuvent pas modifier les paramètres de l'organisation ni voir les mots de passe des autres services.

Déploiement de 2 GPO (Extension, favoris)

L'entreprise utilise **Microsoft Edge** comme navigateur principal. Pour faciliter l'adoption de l'outil par les collaborateurs, j'ai mis en place deux stratégies de groupe (GPO) :

- **Déploiement d'un favori** : J'ai configuré une GPO pour ajouter automatiquement le lien du coffre-fort (Vault) dans la barre de favoris des utilisateurs. Cela leur permet d'accéder à l'interface de gestion en un clic.
- **Installation forcée de l'extension** : Une seconde GPO permet d'installer automatiquement l'extension Bitwarden sur tous les navigateurs Edge du parc. L'utilisateur n'a aucune manipulation technique à faire, l'outil est présent dès l'ouverture de sa session

Réunion de lancement

Une fois la configuration technique terminée, j'ai organisé une réunion de lancement avec mes deux collègues du service informatique.

L'objectif était de leur présenter officiellement la solution avant le déploiement global.

- **Présentation en salle de réunion** : À l'aide du grand écran, j'ai effectué une démonstration complète en conditions réelles.
- **Démonstration du flux de connexion** : Je leur ai montré la procédure de première connexion via le SSO (Microsoft Entra ID) pour prouver la simplicité et la sécurité du système.
- **Formation sur les fonctionnalités** : Nous avons parcouru ensemble les outils quotidiens comme le générateur de mots de passe, le système de "Send" et la saisie automatique sur les sites web.
- **Explication des droits et permissions** : J'ai détaillé leurs privilèges en tant qu'administrateurs du service informatique par rapport aux droits restreints des futurs utilisateurs.

Cette présentation a permis de valider les derniers réglages avec l'équipe. Suite à cet échange positif, j'ai pu lancer officiellement le déploiement du logiciel sur l'ensemble du parc informatique de **Novarina**.

Parc d'impression (Mission secondaire)

Contexte et objectif

Mon travail débute par une phase de repérage et d'analyse globale du parc. Dans un second temps, je me déplace directement sur l'interface des imprimantes pour faire l'analyse directe.

Etat des lieux :

- Identifier le nombre d'imprimantes disponibles et vérifier qu'elles sont toutes la
- Vérifier leur fonctionnement
- Scanner par mail

Failles de sécurité existantes sur un parc d'impression :

- Accès non autorisés sur des imprimantes connectés dû aux identifiants parfois non changés
- Exploitation de faille si des mises à jour ne sont pas faites, pilotes et firmware (logiciel interne)

Vérification :

- Vérifier les droits d'accès des utilisateurs à chacune des imprimantes et ne pas donner trop de droits à ceux qui n'en ont pas besoin
- Vérifier les identifiants mdp de l'imprimante et qu'il soit conforme robuste et qu'ils n'aient pas été modifiée
- Vérifier si le firmware (logiciel interne de l'imprimante est à jour) sinon mettre à jour à la dernière version pour éviter des failles de sécurité
- Vérifier si les pilotes de chacune des imprimantes sont à jour
- Vérifier s'il n'y a pas d'accès distant non autorisé sur une des imprimantes
- En cas de failles vérifier les logs, journaux d'activités

Réalisation

Imprimante ThononR-ADM :

Vérification et conformité de la configuration IP :

Plage d'adresse **DHCP** imprimantes onduleurs, sur l'inventaire GLPI

Nom	imprimante-onduleur Thonon			
Début de la plage IP	10	1	60	200
Fin de la plage IP	10	1	60	231
Entité	Root entity ▼ i +			

Configuration **IPv4** bien conforme à la plage d'adresse de l'inventaire GLPI

Réglages adresse IP

Utiliser IPv4

ProtocoleSélectionner : Non ▼

Utiliser adresse IP auto.

Adresse IP :

Masque de sous-réseau :

Adresse de passerelle :

L'imprimante est bien dans le **domaine** de l'entreprise

Réglages DNS

Adresse du serveur DNS primaire :

Adresse du serveur DNS secondaire :

Nom d'hôte :

Nom de domaine :

Effectuer Mise à jour dynamique DNS

Vérification avec un test de connexion :

```
Invite de commandes - ping · × + ▼
Microsoft Windows [version 10.0.26100.6725]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\yanis.dahman>ping 10.1.60.200

Envoi d'une requête 'Ping' 10.1.60.200 avec 32 octets de données :
Réponse de 10.1.60.200 : octets=32 temps=1 ms TTL=64
Réponse de 10.1.60.200 : octets=32 temps=1 ms TTL=64
Réponse de 10.1.60.200 : octets=32 temps=1 ms TTL=64
```

Le test est un succès, l'imprimante est bien connectée au réseau de Thonon.

Vérification et conformité des réglages SNMP :

Protocole SNMP sur GLPI :

<input type="checkbox"/> Identifiants SNMP	Version	Par ordre de priorité
<input type="checkbox"/> Public community v1	1	2
<input type="checkbox"/> Public community v2c	2c	3
<input type="checkbox"/> Onduleur V3	3	4

Protocole SNMP sur l'interface de l'imprimante dans le réseau de Thonon

Réglages SNMP

Dernière mise à jour : 12/01 2026 16:22:5

OK

Annuler

Utiliser SNMPv1

Utiliser communauté dédiée

Autorisation accès MIB :

Utiliser Nom communautaire 1

Autorisation accès MIB :

Nom communautaire :

Utiliser Nom communautaire 2

Autorisation accès MIB :

Nom communautaire :

Utiliser SNMPv3

Réglages administrateur :

Réglages de l'utilisateur :

Obtenir infos de gestion d'impression depuis hôte

Refuser les paquets SNMP lorsque la machine est en mode veille

On observe que quand GLPI va scanner le réseau, il va tester l'identifiant "**Public community v1**" qu'on voit plus haut, l'imprimante va répondre "OK" et GLPI pourra remonter les informations.

Donc les réglages SNMP de GLPI sont bien conformes aux réglages de l'imprimante.

Optimisation possible des réglages SNMP

Le protocole de supervision SNMP est actuellement configuré avec les paramètres par défaut, donc le mot de passe communautaire "public"

Solutions possibles :

Modifier le paramètre d'accès MIB **sur l'interface de l'imprimante** pour passer de "Lecture/Ecriture" à "**Lecture seule**".

Remplacer le nom de communauté par défaut "**public**" par un nom complexe à la fois sur l'imprimante et dans la configuration GLPI.

Abandonner le protocole **SNMPv1** qui est la version officielle et la plus ancienne, malgré sa facilité d'utilisation

Passer sur la dernière version, **SNMPv3** qui offre des solutions de sécurité garantis comme on peut le voir ci-dessous.

Du côté de l'administrateur on peut voir les différents réglages sécurisés ainsi que l'accès en **RW**.

Utiliser administrateur

Nom d'utilisateur : Administrateur

Autorisation accès MIB : Lecture/Ecriture

Règlages de sécurité : Auth. Oui/Crypt. Oui

Algorithme d'authentification : SHA2-512

Algorithme de cryptage : AES

Utiliser le même mot de passe que pour l'authentification

Définir/Modifier le mot de passe

Mot de passe de cryptage : (8-16 caractères)

Confirmer : (8-16 caractères)

Ici, du côté de l'utilisateur on peut voir que les réglages sont toujours présents.

Réglages de l'utilisateur

Sélectionner	Oui/Non	Nom d'utilisateur	Autorisation accès MIB	Réglages de sécurité
<input type="radio"/>	<input checked="" type="radio"/> Oui	username	Lecture/Ecriture	Auth. Oui/Crypt. Oui

Mais il serait préférable de garder les autorisations des utilisateurs en **lecture** seulement.

Donc en cas de changement, modifier l'ordre de priorité pour mettre **Onduleur v3** en priorité face aux autres.

<input type="checkbox"/> Identifiants SNMP	Version	Par ordre de priorité
<input type="checkbox"/> Public community v1	1	2
<input type="checkbox"/> Public community v2c	2c	3
<input type="checkbox"/> Onduleur V3	3	4

Ou alors sélectionner uniquement **SNMPv3** ici

Utiliser SNMPv1

Utiliser communauté dédiée

Autorisation accès MIB :

Utiliser Nom communautaire 1

Autorisation accès MIB :

Nom communautaire :

Utiliser Nom communautaire 2

Autorisation accès MIB :

Nom communautaire :

Utiliser SNMPv3

Réglages administrateur :

Réglages de l'utilisateur :

Obtenir infos de gestion d'impression depuis hôte

Refuser les paquets SNMP lorsque la machine est en mode veille

Qu'est-ce que ça va impliquer ?

Pour les utilisateurs (Les employés) : AUCUN changement

On peut modifier les réglages SNMP pendant que les gens travaillent, cela ne coupera pas leurs impressions ou leurs scans.

Au niveau de la sécurité : Renforcement

Moins de risques de subir une attaque

Pour l'administrateur :

Changer directement sur GLPI, pour éviter que la supervision ne se coupe

Test de la solution :

Passage en SNMPv3

Déjà choisir réglages administrateur

Utiliser SNMPv3

Réglages administrateur : Réglages administrateur..

Réglages de l'utilisateur : Réglages utilisateur...

On fait un constat de toutes ces informations car il va falloir les transmettre dans GLPI

Utiliser administrateur

Nom d'utilisateur : Administrateur

Autorisation accès MIB : Lecture/Ecriture

Réglages de sécurité : Auth. Oui/Crypt. Oui

Algorithme d'authentification : SHA2-512

Algorithme de cryptage : AES

Utiliser le même mot de passe que pour l'authentification

Définir/Modifier le mot de passe

Mot de passe de cryptage : (8-16 caractères)

Confirmer : (8-16 caractères)

Ensuite, il va falloir se rendre dans [GLPI/Inventaire/Identifiants SNMP](#) → créer nouvel identifiant SNMP

Nouvel élément - Identifiant SNMP

Nom Version SNMP *

Utilisateurs

Protocole de chiffrement pour l'authentification

Mot de passe

Effacer

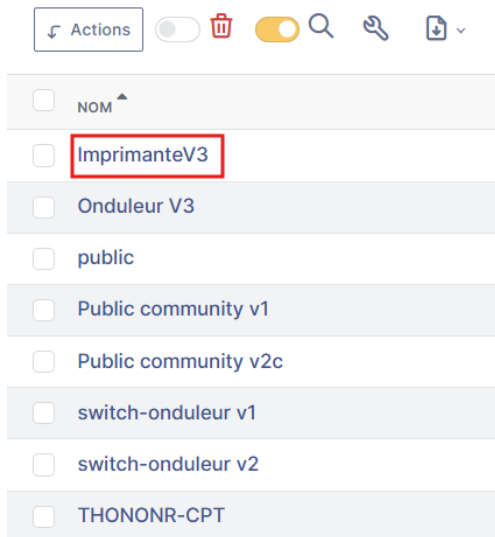
Protocole de chiffrement pour les données

Mot de passe

Effacer

Version SNMPv3	Remplace la version v1 (non sécurisée) pour chiffrer les échanges.
Utilisateurs	Doit correspondre exactement au "Nom d'utilisateurs" administrateur de l'imprimante
Chiffrements	Algorithme de hachage sécurisé pour protéger le mot de passe. Algorithme de chiffrement pour rendre les données illisibles sur le réseau.
Mot de passe	On a généré un mot de passe robuste puis on l'a importer dans l'interface et GLPI

Comme on voit ci-dessous, il figure bien dans la liste des identifiants snmp.

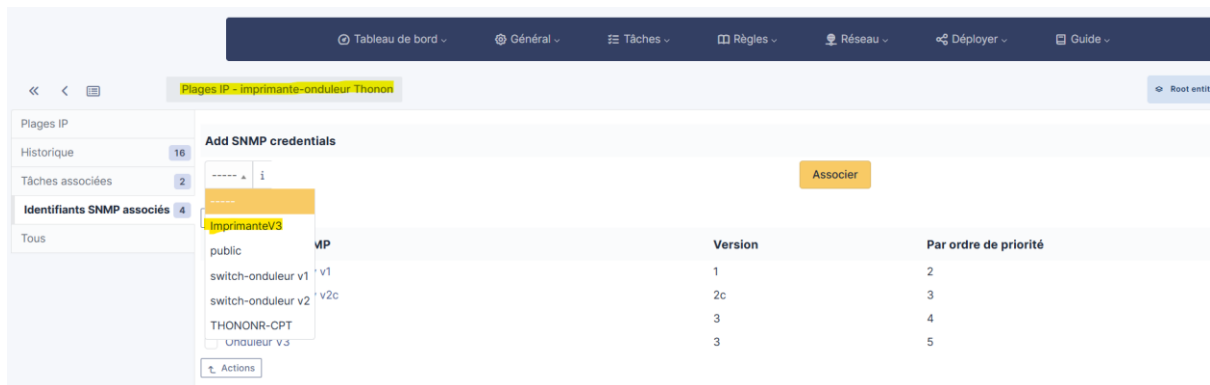


Se rendre dans [GLPI/Administration/GLPI inventory/Plages IP](#)

Sélectionner le réseau qui correspond à l'imprimante que j'ai choisie

J'observe que lorsque je veux ajouter un id snmp a cet imprimante, ImprimanteV3 apparaît bien.

Il manquerait plus qu'à modifier l'ordre de priorité pour le mettre inférieur aux autres.



Plages IP imprimante-onduleur Thonon → Réseau d'imprimantes choisies

Add SNMP credentials

----- i

Actions

Identifiants SNMP

Public community v1

Public community v2c

Onduleur V3

Onduleur V3

ImprimanteV3

Comme on peut voir, l'ID que j'ai créé est bien ici

Langages de chiffrements utilisés pour la configuration du SNMP :

SHA512	J'ai choisi l'algorithme SHA-2-512 pour sécuriser l'authentification. C'est une fonction de hachage cryptographique très robuste. Elle permet de transformer le mot de passe en une empreinte illisible.
AES128	Pour la confidentialité des données, j'ai choisi l'algorithme AES-128 (Advanced Encryptions Standard).

Je consulte l'historique de l'inventaire dans GLPI pour valider la migration.
On constate que la remontée des données (compteur de pages, date) continue de fonctionner normalement après le passage en SNMPv3, confirmant ainsi la réussite de la configuration

31075106	14-01-2026 15:25	inventory	Date de dernier inventaire	Changement de 14-01-2026 15:12 à <u>14-01-2026 15:25</u>
31072236	14-01-2026 15:12	inventory	Compteur de page actuel	Changement de 332893 à <u>333084</u>
31072235	14-01-2026 15:12	inventory	Date de dernier inventaire	Changement de 13-01-2026 15:14 à <u>14-01-2026 15:12</u>

Solutions plus sécurisées de scans PDF → Mails

Solutions :

Activer le protocole TLS (TX SMTP) ça va permettre de rendre l'interception du fichier scanner impossible à intercepter durant son transfert.

“**TLS**” est un protocole qui permet de sécuriser l'échange des données

“**TX**” fait référence à la transmission de données

“**SMTP**” Protocole de transferts de courriers entre serveurs de messageries

Réglages SMTP/POP
*Le réglage pour [Serveur SMTP] sera appliqué à [Vérifier la connexion SMTP], et le réglage pour [Serveur POP], [Nom de connexion POP] et [Mot de passe POP] sera appliqué à [Vérifier la connexion POP].

RX SMTP :
 RX POP

Serveur SMTP :

Adresse e-mail :

Serveur POP :

Nom de connexion POP :

Mot de passe POP :

Confirmer :

Intervalle POP : min (0=Non/1-99)

Spécifier le numéro de port pour TX SMTP/RX POP

TX SMTP : (1-65535)
RX POP : (1-65535)

Réglages d'authentification/cryptage

Autoriser TLS (POP)
Méthode d'authentification POP :

Utiliser l'authentification POP avant l'envoi
 Confirmer certificat TLS pour RX POP
 Ajouter CN à la liste des éléments à vérifier

Autoriser TLS (TX SMTP)

Utiliser l'authentification SMTP (AUTH SMTP)
Nom d'utilisateur : (64 caractères max.)
 Modifier le mot de passe
Mot de passe : (32 caractères max.)
Confirmer : (32 caractères max.)

Afficher l'écran d'authentification lors de l'envoi
 Confirmer certificat TLS pour TX SMTP
 Ajouter CN à la liste des éléments à vérifier

Autoriser TLS (RX SMTP) :

On observe que le port par défaut de SMTP est 25

Spécifier le numéro de port pour TX SMTP/RX POP



TX SMTP : (1-65535)

Comme on peut le voir ci-dessous, la clé cryptographique qui va permettre de sécuriser les scans de l'imprimante vers la boîte mail existe déjà, elle a été générée par défaut

Réglages de cryptage/clé

Réglages de cryptage	
Réglages de cryptage	
Utiliser un faible niveau de cryptage :	Ne pas interdire
Réglages méthode de cryptage	
Formater Méthode de cryptage en FIPS 140-2 :	Non

Réglages de clé et de certificat

Clé et certificat mémorisés		
Nom de clé		Utilisation de clé
	Default Key	[TLS]
	AMS	[Contrôle d'accès]

Vérification de la connexion SMTP :

J'effectue un test de connexion pour vérifier que le serveur de messagerie SMTP mis en place fonctionne bien

Réglages SMTP/POP

*Le réglage pour [Serveur SMTP] sera appliqué à [Vérifier la connexion SMTP], et le réglage pour [Serveur POP], [Nom de connexion POP] et [Mot de passe POP] sera appliqué à [Vérifier la connexion POP].

Vérifier la connexion SMTP Vérifier la connexion POP

On observe que le test est un succès

Connexion au serveur réussie.

OK

L'imprimante a accès à Internet : Elle sort bien du réseau.

L'adresse du serveur est bonne : L'adresse novasanit-fr.mail.protection.outlook.com est correcte.

Test de la solution proposée :

Test de la solution proposée : Après en avoir **discuté** avec l'entreprise, j'ai effectué le test de **scanner** un document pour le recevoir en PDF sur la boîte mail

Donc autoriser cette option dans les paramètres [/Envoi/Réglages](#)

Autoriser TLS (TX SMTP)

On valide les paramètres dans un premier temps, puis on fait vérifier la connexion SMTP pour être sûr que le scan a bien fonctionné.

Réglages SMTP/POP

*Le réglage pour [Serveur SMTP] sera appliqué à [Vérifier la connexion SMTP], et le réglage pour [Serveur POP], [Nom de connexion POP] et [Mot de passe POP] sera appliqué à [Vérifier la connexion POP].

Vérifier la connexion SMTP

Vérifier la connexion POP

Connexion au serveur réussie.

OK

Après vérification sur la messagerie de mon collègue, le test est concluant. Le chiffrement TLS a permis de sécuriser le transfert des données.

Vérification du statut du firmware (logiciel interne de l'imprimante)

On observe que le logiciel interne de l'imprimante a été mis à jour pour la dernière fois en 2021, toutes les autres tentatives ont été un échec.

```
[2021/02/04 10:06:54] firm download start [OK] 20201225.0222103 iAC3730V222103
[2021/02/04 10:08:30] firm download end [OK] 20201225.0222103 iAC3730V222103
[2021/02/04 10:09:30] firm update start [OK] 20201225.0222103 iAC3730V222103
[2021/02/04 10:16:38] firm update end [OK] 20201225.0222103 iAC3730V222103
[2023/06/22 10:20:10] firm download start [OK] 20230308.0301201 iAC3730V301201
[2023/06/22 10:23:52] firm download end [ERR] 20230308.0301201 iAC3730V301201
[2023/12/11 21:00:24] firm download start [OK] 20230915.0342401 iAC3730V342401
[2023/12/11 21:10:33] firm download end [ERR] 20230915.0342401 iAC3730V342401
```

De plus, un message d'erreur s'affiche lorsque nous essayons de voir la version du logiciel interne de l'imprimante

Mettre à jour microprogramme : Mise à jour distribuée

Mise à jour distribuée

Mise à jour :12/01 2026 17:04:36 ↻

Confirmer nouveau microprogramme

- Une erreur de distribution s'est produite.
11/12 2023 21:00:00, iAC3730V342401, 20230915.0342401, 8200bfff

Informations de mise à jour

Mettre à jour le statut :

Aucune information sur la
distribution

Appliquer microprogramme

Supprimer microprogramme

Les anciennes versions des firmwares peuvent éventuellement contenir des failles c'est pour ça qu'il faut avoir la dernière version à jour en permanent car des correctifs sont souvent ajoutés lorsque des failles sont trouvés.

État de santé du matériel

On observe que l'ensemble de fixation nécessite un remplacement prochain, ça montre une certaine usure de l'appareil

Informations sur l'erreur



Remplacement de l'unité de tambour magenta nécessaire.

Il est conseillé de remplacer l'unité de tambour magenta.

Si l'unité de tambour continue à être utilisée, la qualité d'impression ne peut pas être garantie.



Remplacement de l'unité de tambour jaune nécessaire.

Il est conseillé de remplacer l'unité de tambour jaune.

Si l'unité de tambour continue à être utilisée, la qualité d'impression ne peut pas être garantie.



Plus de papier.

Vérifier le panneau de commande, puis charger du papier.



Remplacement de l'ensemble de fixation bientôt nécessaire.

Solution 1 :

Vérifier la qualité de l'impression. Si la qualité est satisfaisante, l'ensemble de fixation actuel peut toujours être utilisé.

Solution 2 :

Vérifier la qualité de l'impression. Si la qualité n'est pas satisfaisante, contacter le revendeur Canon local agréé ou le SAV.

Gestion des partages et autorisations (Mission secondaire)

Contexte et objectif

Ma mission consistait à préparer l'arborescence des dossiers pour la nouvelle année.

J'ai dû configurer les autorisations de partage et les droits d'accès pour les dossiers contenant les **primes d'activités** des employés sur l'ensemble des sites de l'entreprise.

L'**enjeu principal** était de garantir la stricte confidentialité de ces données sensibles en dupliquant le modèle de droits du dossier "2025" vers le nouveau dossier "2026".

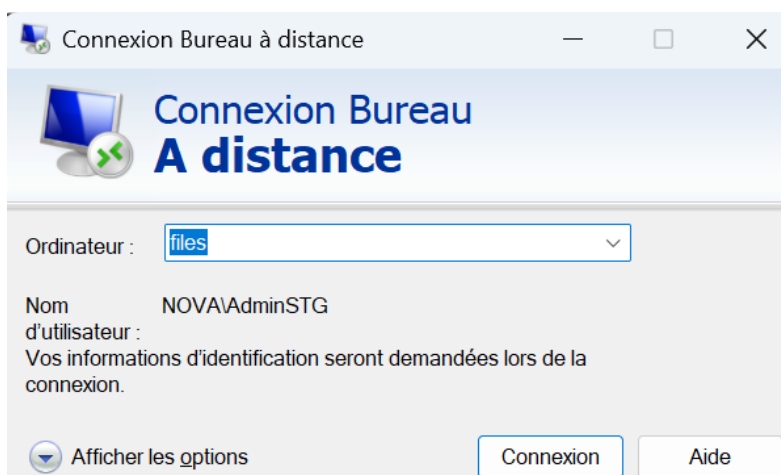
Réalisation

Connexion :

Pour accéder au serveur de fichiers et gérer les dossiers, je lance l'application **Connexion Bureau à distance** afin d'établir une session en **RDP (Remote Desktop Protocol)**

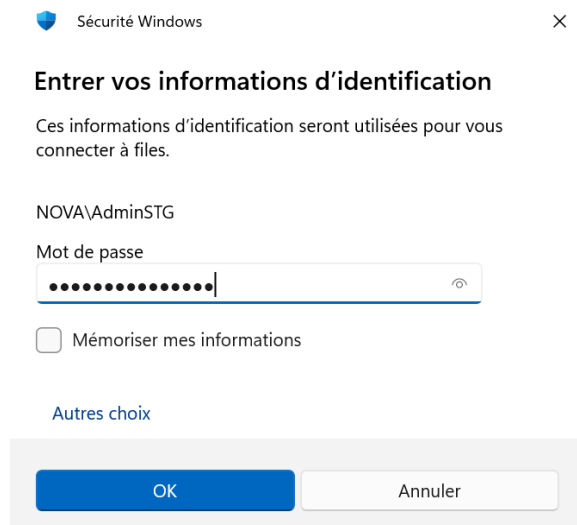


Dans la fenêtre de connexion, je renseigne le nom du **serveur de fichiers**.

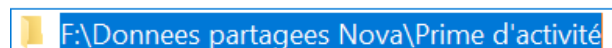


Je saisis le mot de passe du compte administrateur (**NOVA\AdminSTG**) et je valide en cliquant sur **OK**.

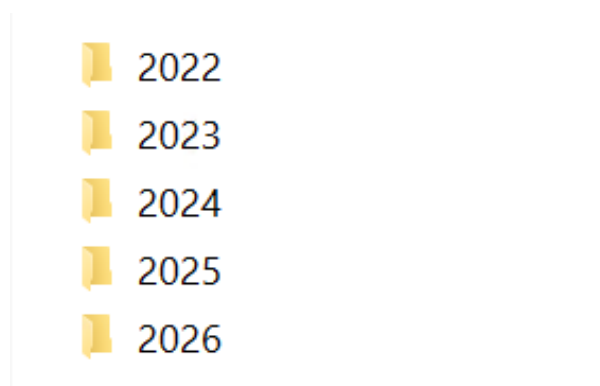
Cela finalise l'authentification et m'ouvre l'accès direct au serveur pour débiter la gestion des dossiers.



Une fois la session ouverte, je parcours l'arborescence du serveur pour accéder au répertoire cible : « F:\Donnees partagees Nova\Prime d'activité ».



Ce dossier racine centralise l'ensemble des documents liés aux primes d'activité pour tous les sites de l'entreprise.



Pré Requis :

Avant de pouvoir personnaliser les accès, j'ai dû **désactiver l'héritage** des droits sur chaque sous-dossier.

Par défaut, les permissions descendent du dossier parent et sont verrouillées en modification.

En cliquant sur ce bouton, je romps ce lien automatique, ce qui "débloque" les droits et me permet d'ajouter ou de supprimer des groupes d'utilisateurs librement pour chaque service.

Ajouter

Supprimer

Afficher

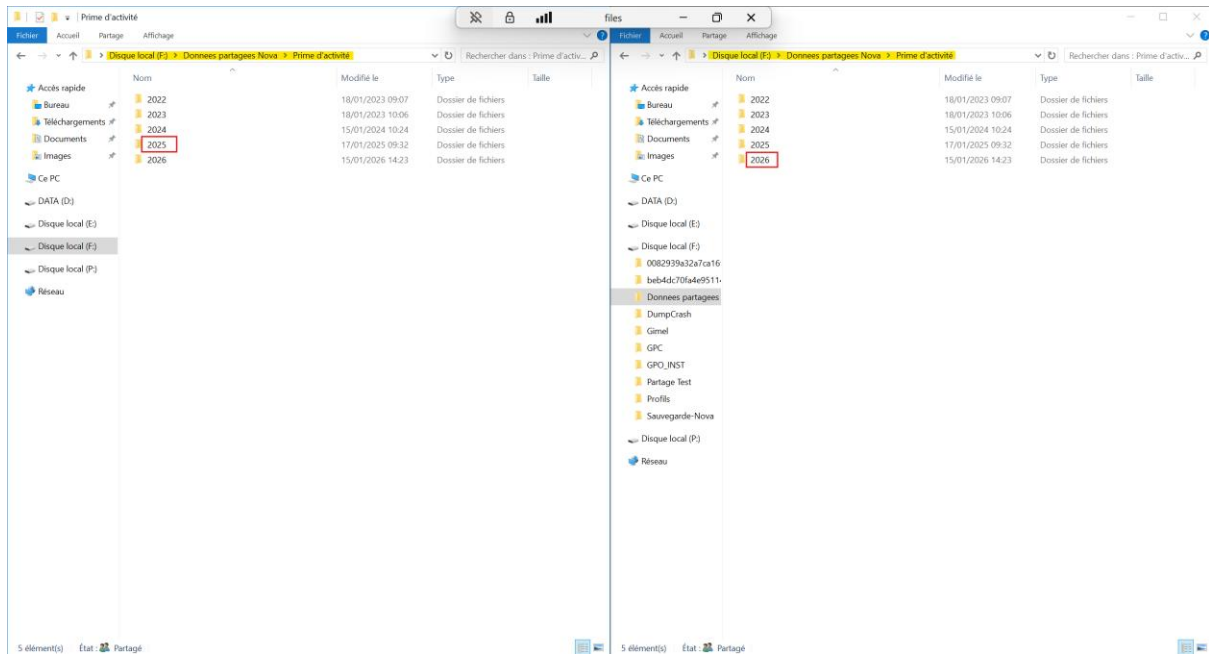
Désactiver l'héritage

Organisation :

J'organise mon espace de travail en ouvrant deux instances de l'explorateur de fichiers.

Cette disposition me permet de consulter les propriétés de sécurité du dossier source "2025" tout en configurant simultanément celles du dossier "2026".

Cette comparaison visuelle directe facilite la mise à jour des permissions (ajout/suppression de groupes) et assure la cohérence des accès entre l'ancienne et la nouvelle année.



Cette vue d'ensemble présente l'arborescence du répertoire **"Prime d'activité"**.





On y retrouve les dossiers classés chronologiquement par année, ce qui permet de centraliser l'historique des primes

Disque local (F:) > Donnees partagees Nova > Prime d'activité >			
	Nom	Modifié le	Type
★	2022	18/01/2023 09:07	Dossier de fichiers
★	2023	18/01/2023 10:06	Dossier de fichiers
★	2024	15/01/2024 10:24	Dossier de fichiers
★	2025	17/01/2025 09:32	Dossier de fichiers
★	2026	15/01/2026 14:23	Dossier de fichiers

J'accède ensuite au contenu du dossier **2026**.

Celui-ci est structuré par site géographique (**ANNEMASSE, MEYTHET, THONON**) et contient également le fichier de gestion global (Matrice).

Chacun de ces répertoires parents abrite lui-même une arborescence de sous-dossiers spécifiques.

 ANNEMASSE	15/01/2026 14:23	Dossier de fichiers
 MEYTHET	15/01/2026 14:23	Dossier de fichiers
 THONON	15/01/2026 14:23	Dossier de fichiers
 Prime d'activité 2026 - Matrice.xlsm	13/01/2026 15:15	Fichier XLSM

Voici le détail du dossier **ANNEMASSE**.

On y retrouve les répertoires spécifiques à chaque équipe (**Accueil, Magasin, Réception**)

 Accueil Annemasse	15/01/2026 14:23	Dossier de fichiers
 Magasin LS Annemasse	15/01/2026 14:23	Dossier de fichiers
 Réception Expédition Annemasse	15/01/2026 16:39	Dossier de fichiers







Voici le détail du dossier **MEYTHET**.

On y retrouve les répertoires spécifiques à chaque équipe (**Accueil, Magasin, Réception**)

 Accueil Meythet	15/01/2026 14:23	Dossier de fichiers
 Magasin LS Meythet	15/01/2026 14:23	Dossier de fichiers
 Réception Expédition Meythet	15/01/2026 16:39	Dossier de fichiers

L'arborescence du site de **THONON** est la plus dense.

Elle intègre des départements spécifiques comme le **Dépôt client** ou le **Contrôle de Gestion**.

 Accueil Thonon	15/01/2026 14:23	Dossier de fichiers
 Carrelage	15/01/2026 14:23	Dossier de fichiers
 Contrôle de Gestion	15/01/2026 14:23	Dossier de fichiers
 Dépôt client	15/01/2026 14:23	Dossier de fichiers
 Magasin LS Thonon	15/01/2026 14:23	Dossier de fichiers
 Stock Central	15/01/2026 14:23	Dossier de fichiers

Assainissement de l'Active Directory (Mission secondaire)

Contexte et objectif

Lors de l'analyse de l'annuaire Active Directory, j'ai constaté la présence de nombreux comptes ordinateurs obsolètes.

Ces machines correspondaient à des collaborateurs ayant quittée l'entreprise

L'objectif de cette mission est de nettoyer l'arborescence pour :

- Renforcer la sécurité : Eviter qu'une ancienne machine puisse se connecter au réseau
- Conformité : Avoir une arborescence conforme au parc de GLPI.

Réalisation

Utilisateurs et ordinateurs Active Directory

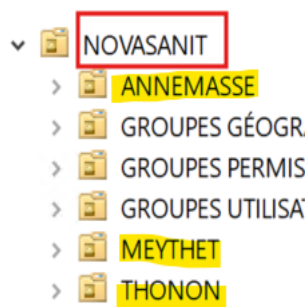
Liste des Unités d'Organisation contenant les objets ordinateurs et utilisateurs à nettoyer



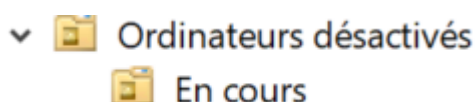
L'OU **Novamat** regroupe plusieurs unités d'organisation, qui abritent à leur tour d'autres niveaux de sous-OU.



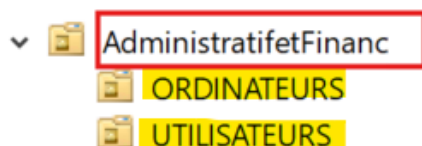
L'OU **Novasanit** regroupe plusieurs unités d'organisation, qui abritent à leur tour d'autres niveaux de sous-OU.



J'ai créé cette nouvelle Unité d'Organisation afin d'y **isoler** les machines identifiées. Je vais y déplacer l'ensemble des ordinateurs concernés avant de procéder à leur désactivation.

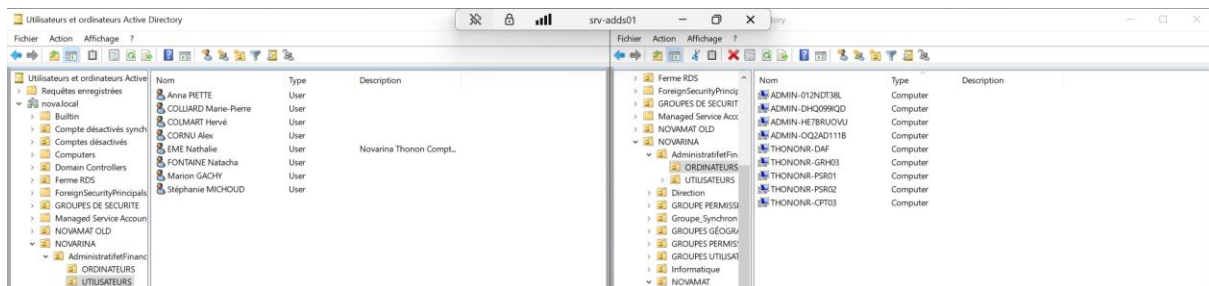


Cas pratique : Application de la procédure de nettoyage sur l'Unité d'Organisation **Administratif Financier**



Pour effectuer une **vérification croisée** efficace, j'ouvre deux instances de la console Active Directory.

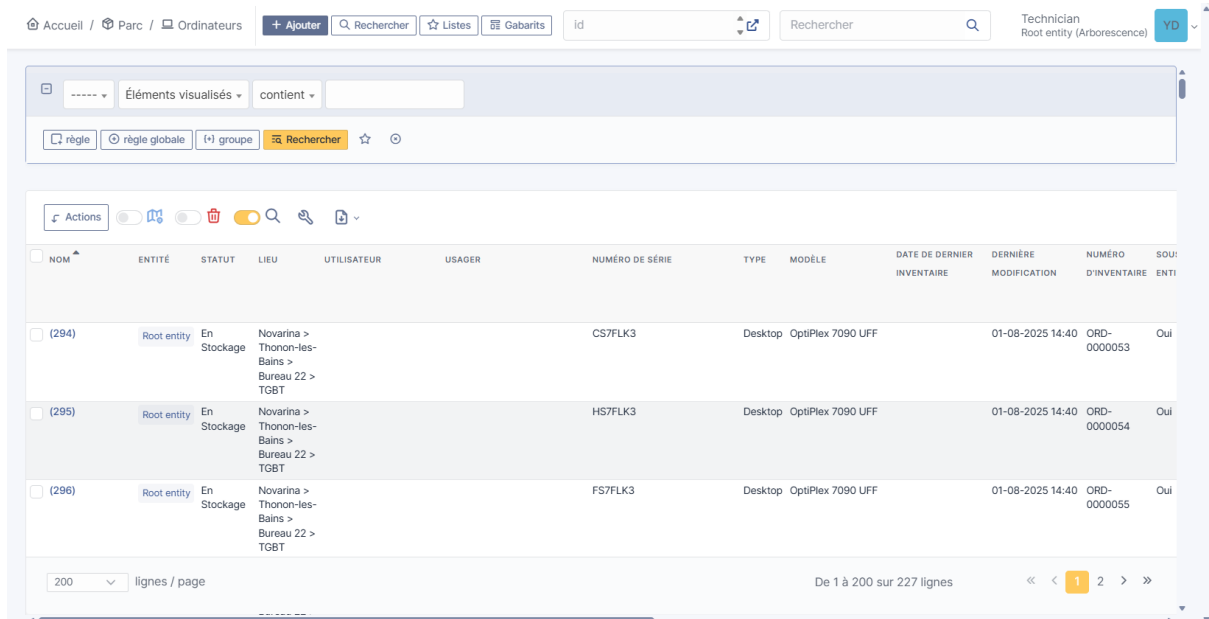
J'affiche l'Unité d'Organisation "**Utilisateurs**" sur la gauche et l'OU "**Ordinateurs**" sur la droite, ce qui me permet de comparer visuellement les correspondances en temps réel.



Le comptage fait apparaître un **surplus** : 9 machines pour 8 utilisateurs.
L'ordinateur non attribué sera donc déplacé vers l'archivage.

Pour vérifier lequel n'appartient à personne, il faut se rendre dans [GLPI](#) → Parc → [Ordinateurs](#)

Une fois sur cette vue, j'utilise le champ de recherche pour interroger l'annuaire.
Pour chaque utilisateur, je valide le poste informatique correspondant afin de repérer l'intrus.



En cas d'absence d'utilisateur associé dans l'inventaire **GLPI**, la machine est considérée sans propriétaire.

La procédure impose alors de **désactiver le compte** correspondant pour sécuriser le parc.

