Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
Parcours cybersécurité

Supervision du réseaux et serveurs d'entreprise

POITOU Théo

DuranSia

Responsable entreprise : Alexandre CALISSI-BARRAL
Responsable académique : Delphine ROUSSEAU

2023

Table des matières

I) Introduction

J'ai effectué mon stage au sein du service informatique dans le groupe coopératif agricole DuranSia. Ce service compte deux collaborateurs. L'objectif principal de mon stage était d'installer une solution de supervision et de mettre en place un outil de ticketing destiné au service informatique.
Dans ce rapport, je présenterai tout d'abord l'entreprise DuranSia, en mettant en évidence son historique, ses activités et ses implantations géographiques. Ensuite, je décrirai le cadre technique du projet, notamment l'organisation du service informatique, la présentation du réseau et un schéma des flux applicatifs. Je détaillerai également les objectifs spécifiques du stage, en mettant l'accent sur l'outil de ticketing et l'outil de monitoring. Par la suite, je présenterai le travail réalisé, en incluant l'étude de faisabilité, le paramétrage des solutions, le recettage et la mise en production pour chaque outil. Enfin, je conclurai ce rapport en résumant les résultats obtenus et en discutant des perspectives d'amélioration pour l'avenir.

II) Présentation de l'entreprise

1) Historique de DuranSia

La coopérative DuranSia, dont le siège social est situé à Peyruis (04), a été créée en 2022. Depuis sa fondation, elle s'est développée avec succès en établissant quatre filiales, spécialisée dans le domaine agricole en Provence. Son objectif est d'accompagner les agriculteurs à toutes les étapes, de la production à la vente de leurs produits. Grâce à son expertise et à son réseau étendu, la coopérative offre des solutions complètes et adaptées aux besoins spécifiques des agriculteurs, favorisant ainsi leur réussite et leur pérennité.

2) Activités et valeurs de l'entreprise

Les missions de DuranSia se résument comme suit :

- Créer et développer des filières agricoles à forte valeur ajoutée, en établissant des contrats pour assurer la durabilité des activités.
- Fournir un accompagnement quotidien aux agriculteurs, en les conseillant et en les aidant à transformer leurs savoir-faire agricoles.
- Promouvoir les circuits courts et favoriser la proximité en encourageant les échanges locaux. DuranSia s'engage à rassembler une communauté d'agriculteurs dynamiques.
- Envisager l'avenir de l'agriculture en Provence-Alpes et s'inscrire dans une démarche de durabilité. DuranSia cherche à anticiper les évolutions et à contribuer à un avenir durable pour les agriculteurs et la région.

Les visions / valeurs de DuranSia :

La vision de DuranSia est de créer un écosystème vertueux à long terme en Provence, plaçant l'agriculture et les agriculteurs au centre de ses préoccupations.

Les valeurs de DuranSia se déclinent comme suit :

- Orientation adhérents et clients : DuranSia place ses adhérents et ses clients au cœur de ses actions, en répondant à leurs besoins et en leur fournissant un service de qualité.

- Proximité : DuranSia valorise la proximité en entretenant des relations étroites avec ses adhérents, ses clients et les acteurs locaux. Cette proximité favorise la compréhension mutuelle et la réactivité.

- Performance : DuranSia vise l'excellence en mettant en œuvre des pratiques qui permettent de valoriser au mieux les productions agricoles et d'atteindre une sérénité économique pérenne.

- Innovation : DuranSia encourage l'innovation dans le secteur agricole en développant des filières durables, innovantes et créatrices de valeur à partager. L'innovation est au cœur de sa démarche pour répondre aux défis actuels et futurs.

- Collectif : DuranSia favorise la collaboration et le travail collectif, en rassemblant les agriculteurs et les parties prenantes pour créer une communauté dynamique et solidaire.

En s'appuyant sur ces valeurs, DuranSia s'engage à favoriser la biodiversité, à garantir des produits éthiques, de qualité et locaux pour les consommateurs, ainsi qu'à soutenir le développement du territoire de la Provence-Alpes en créant des emplois, en valorisant la valeur locale et en renforçant son attractivité globale.

3) Implantation géographique

Le Groupe Coopératif Agricole DuranSia est présent sur les départements des Alpes de Hautes Provence et des Hautes-Alpes :

11 sites industriels : silos ou usines

Chorges, Gap, Serres, Lazer, Aubignosc, Oraison, Brunet, Manosque, Sainte-Tulle, Montagnac, Vinon -sur-Verdon

11 magasins professionnels : dépôts

Gap, Laragne-Montéglin, Baratier, Barcelonnette, Sisteron, Digne les bains, Forcalquier, Saint André les Alpes, Manosque, Brunet, Oraison

8 enseignes Gamm 'Vert
Laragne-Montéglin, Baratier, Barcelonnette, Sisteron, Digne les bains, Forcalquier, Saint André les Alpes, Manosque

Figure 1 : Carte des Alpes de Haute Provence et Hautes-Alpes

III) Présentation du cadre technique du projet

1) Organisation du Service Informatique

Le service informatique de DuranSia est composé de deux personnes dédiées à la gestion et au maintien du système informatique de l'entreprise. Leur rôle est de maintenir en condition opérationnelle tous les sites DuranSia. Ils assurent la planification, la coordination et la gestion des ressources informatiques de l'entreprise. Leurs missions consistent à aligner les objectifs stratégiques de l'entreprise avec les besoins technologiques, en garantissant la disponibilité, la sécurité et la performance des systèmes.

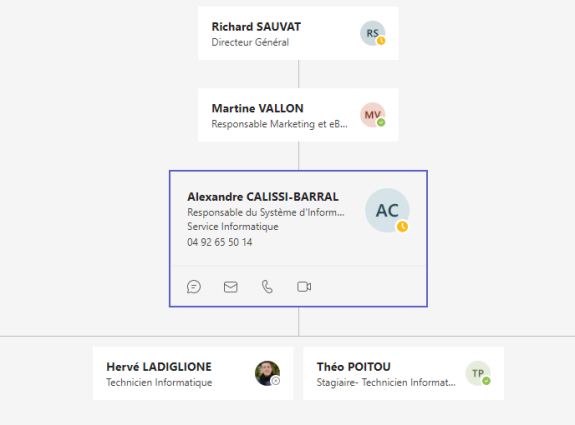

Figure 2 : Organigramme du service informatique

2) Présentation du réseau

Actuellement, DuranSia compte 31 sites raccordés sur l'ensemble du territoire via, pour la plupart, un MPLS opérateur avec un échappement en cœur de réseau. Certains sites n'étant pas ouverts toute l'année, il a été choisi de mettre en place des liaisons VPN IPSEC afin de limiter les coûts. DuranSia gère ces salles serveurs en hybride, une partie On-premise et une partie cloud.
La gestion de ce réseau est assurée par le service informatique, avec le soutien de Suderiane, une entreprise indépendante qui apporte son expertise pour la gestion des serveurs et du réseau.

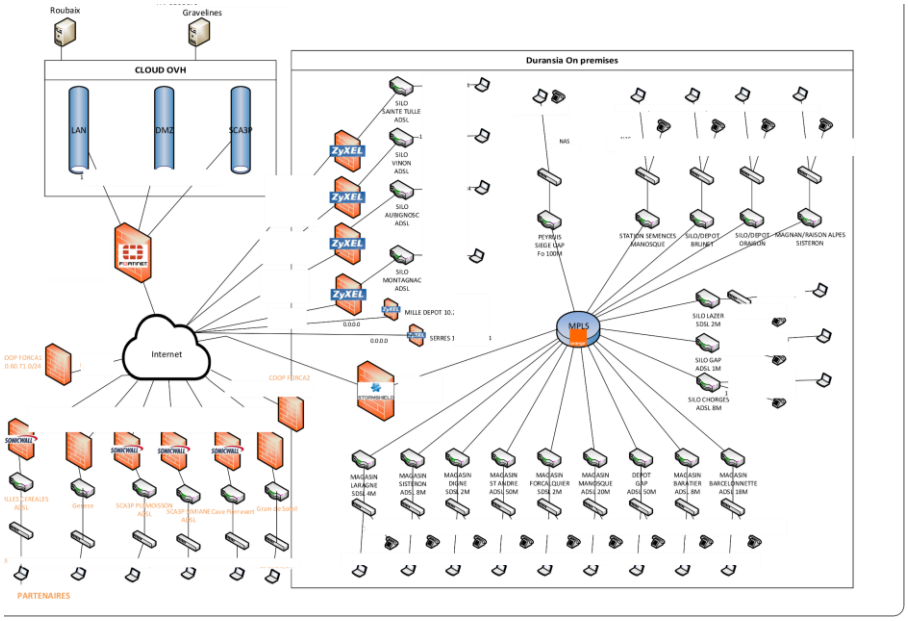

Figure 3 : Schéma du Système d'information

3) Schéma des flux applicatifs

Un schéma des flux applicatifs est établi pour illustrer la manière dont les différentes applications interagissent entre-elles. Cela permet d'avoir une vue synthétique de l'interopérabilité des applications. Chaque année, le système d'information de DuranSia est en constante évolution. Cela se traduit par des migrations vers des applicatifs plus récents ou des montées en version tout en vérifiant les effets de bords que pourront avoir les applications entre elles.

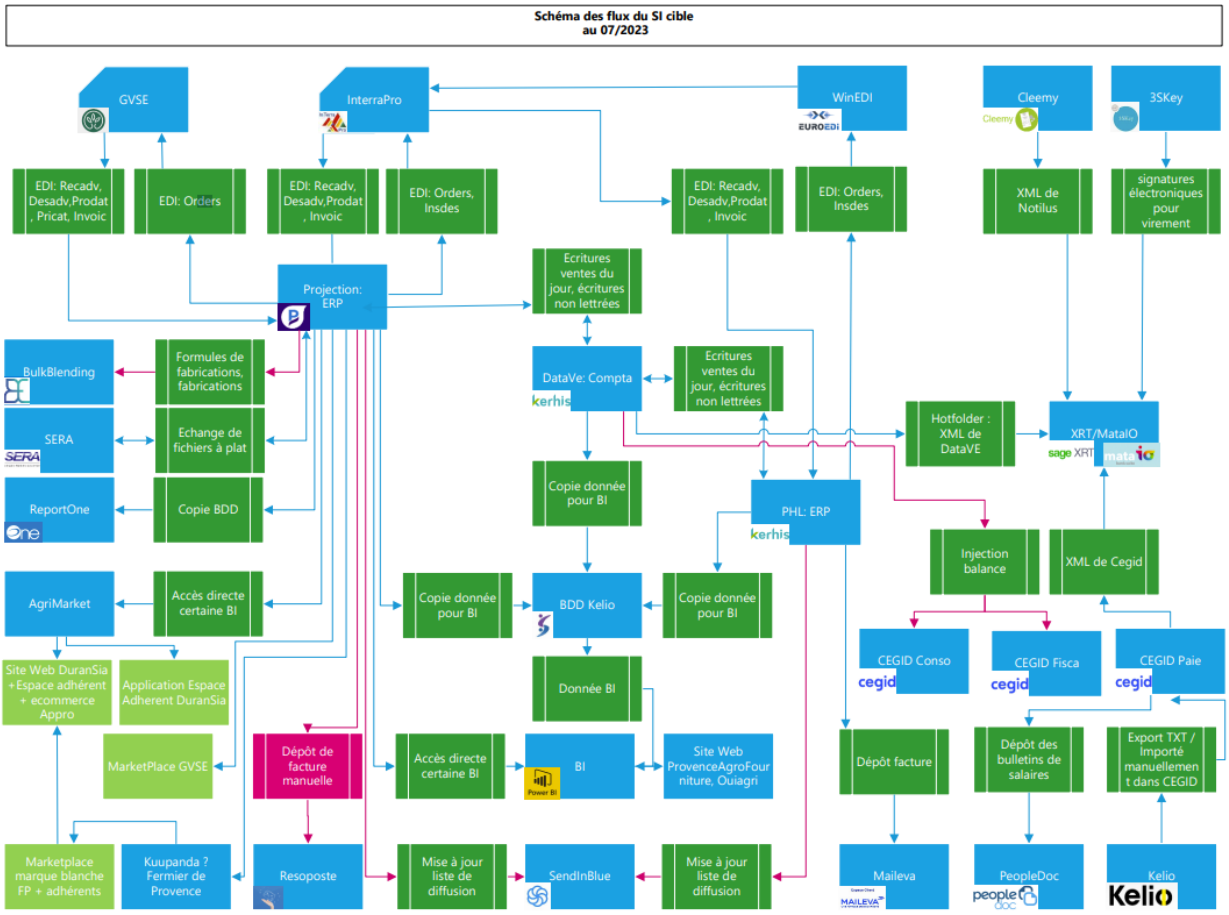

Figure 4 : Schéma des flux applicatifs de DuranSia

4) Définition des objectifs du stage

A) Outil de monitoring

Lors de mon stage au service informatique de DuranSia, mon projet initial était de déployer une solution de supervision de réseau d'entreprise appelée Eyes Of Network. Cette solution, basée sur le protocole SNMP (Simple Network Management Protocol), permet de répertorier tous les sites de l'entreprise situés dans la région Paca (04 et 05), afin d'apporter un suivi en temps réel du trafic réseau sur chaque site ainsi que de surveiller la santé des serveurs, des switchs, des bornes wifi, (temps de réponse, occupation mémoire, occupation RAM, …). Cela permet d'anticiper certaines pannes ou dysfonctionnement possibles. Ce projet m'a permis d'acquérir des compétences en supervision de réseau, en intégration logicielle et en gestion des tickets, tout en contribuant au bon fonctionnement de l'infrastructure informatique de DuranSia.

Qu'est-ce que le protocole SNMP ?

Afin d'assurer l'intégration des données récupérées dans les bases de données du logiciel de supervision, il est nécessaire d'utiliser un protocole normalisé qui est présent sur tous les équipements du réseau. Le protocole SNMP (Simple Network Management Protocol).

Le SNMP repose sur deux éléments principaux : un superviseur et des agents. Le superviseur est l'interface permettant à l'administrateur réseau d'exécuter des requêtes SNMP, tandis que les agents se situent au niveau des interfaces connectant les équipements supervisés au réseau. Les agents permettent de récupérer les informations de supervision spécifiques à chaque équipement.

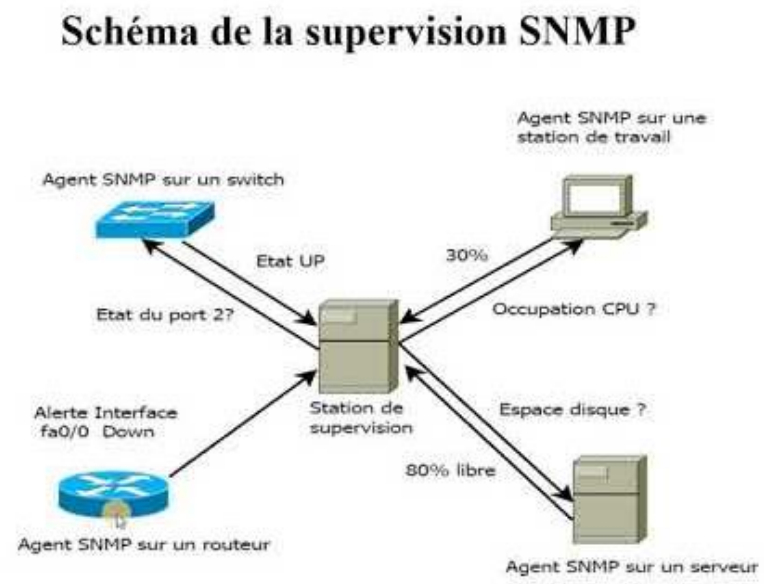

Figure 5 : Présentation du SNMP en schéma

Ces informations peuvent varier en fonction du type d'équipement géré. Par exemple, pour un routeur, il est possible de récupérer des données concernant l'utilisation de son unité centrale, l'utilisation de la mémoire ou encore l'état de ses interfaces.
Les informations sont récupérées grâce à des requêtes SNMP. Il en existe cinq types :

Requête « Get » (Get Request) : Cette requête est utilisée par le superviseur pour demander la valeur d'une variable spécifique à un agent. L'agent répond en renvoyant la valeur demandée.

Requête « GetNext » (GetNext Request) : Cette requête permet au superviseur de récupérer la valeur de la variable suivante dans la séquence d'objets gérés. Cela permet de parcourir les informations disponibles sur un agent.

Requête « GetBulk » (GetBulk Request) : Cette requête permet au superviseur de récupérer un grand nombre de variables en une seule requête, réduisant ainsi le nombre de requêtes nécessaires pour obtenir les informations souhaitées.

Requête « Set » (Set Request) : Cette requête est utilisée pour définir la valeur d'une variable sur un agent. Elle permet de modifier la configuration ou les paramètres d'un équipement réseau.

Requête « Trap » : Contrairement aux requêtes précédentes qui sont initiées par le superviseur, la requête Trap est envoyée par l'agent de manière proactive pour signaler un événement ou une condition exceptionnelle au superviseur. Cela permet à l'agent d'informer le superviseur en temps réel de certains événements importants.

Ces types de requêtes SNMP permettent au superviseur de collecter des informations sur les équipements réseau, de surveiller leur état, de gérer leur configuration et de recevoir des notifications en cas d'événements importants.

Les requêtes SNMP sont répondues par des GetResponse. A chaque évènement indésirable ou inattendu qui se produit sur l'agent, il en informe le manager (la station de supervision) via une Trap.

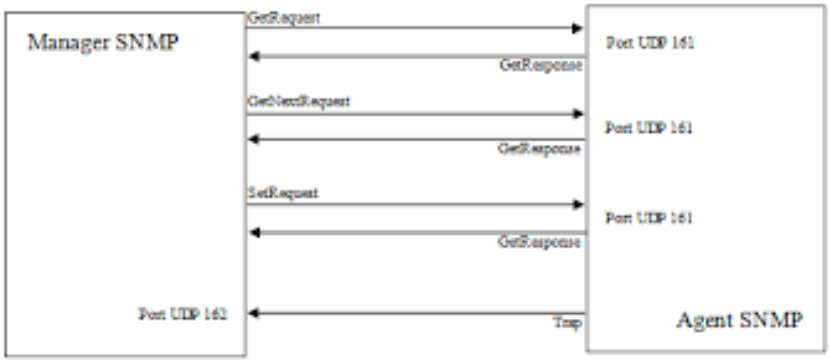

Figure 6 : Présentation des échanges SNMP

B) Outil de ticketing

En plus de déployer le logiciel de supervision, ma deuxième mission consistait à mettre en place un outil de ticketing permettant de faciliter la communication entre les utilisateurs, les employés et l'équipe informatique de DuranSia.

Voici le déroulement de ce processus :

1. Le collaborateur crée un ticket dans GLPI pour signaler un problème ou une demande.
2. L'assistance qualifie le ticket pour déterminer son niveau d'urgence et désigne un intervenant approprié pour le traiter.
3. GLPI notifie le collaborateur de la prise en charge du ticket et informe également l'intervenant désigné.
4. L'intervenant résout le ticket en prenant les mesures nécessaires et en effectuant l'intervention requise. Il enregistre un rapport détaillé de l'intervention effectuée.
5. Une fois le ticket résolu, GLPI envoie une notification au collaborateur pour l'informer que le problème a été résolu et que l'intervention est terminée.

Ce processus permet d'établir une communication claire et transparente entre le collaborateur, l'assistance et l'intervenant, tout en assurant un suivi efficace des tickets et une résolution rapide des problèmes.

Cet outil permet de centraliser toutes les résolutions de problèmes que les utilisateurs pourraient rencontrer. Après avoir discuté avec l'équipe informatique, nous avons choisi d'installer l'outil GLPI, car il offre des avantages supplémentaires comme le ticketing ou même notamment la gestion de l'inventaire du parc informatique. DuranSia ne disposant pas d'un suivi de son parc informatique, cet outil pourrait les aider à suivre les appareils présents sur les différents sites et à anticiper l'obsolescence de certains appareils vieillissants.

1) Qu'est-ce qu'un outil de ticketing ?

Un outil de ticketing, également connu sous le nom de système de gestion des tickets, est une application logicielle utilisée pour faciliter la communication, le suivi et la résolution des problèmes au sein d'une organisation.

L'outil de ticketing fonctionne en créant un enregistrement ou un "ticket" pour chaque demande ou problème signalé par un utilisateur, un client ou un membre de l'équipe. Chaque ticket contient des informations détaillées sur le problème, y compris sa priorité, sa description, ses étapes de reproduction et toute autre information pertinente. Les tickets sont ensuite assignés à des membres de l'équipe chargés de les traiter.

L'outil de ticketing facilite le suivi et la gestion des problèmes de manière organisée. Il permet de centraliser toutes les demandes et les problèmes au même endroit, ce qui facilite leur suivi, leur assignation et leur résolution. Les fonctionnalités courantes d'un outil de ticketing comprennent la création automatique de numéros de ticket, l'attribution des tickets aux membres de l'équipe appropriée, la mise en place de délais et d'alertes, la gestion des priorités, la communication avec les utilisateurs ou les clients, le suivi de l'état et de l'avancement des tickets, ainsi que la génération de rapports et de statistiques.

L'utilisation d'un outil de ticketing permet une meilleure traçabilité des demandes et des problèmes, garantissant ainsi qu'aucune demande ne soit oubliée ou négligée. Il facilite la collaboration entre les membres de l'équipe, car ils peuvent partager des informations, des notes et des mises à jour sur les tickets. De plus, il permet d'améliorer la satisfaction des utilisateurs ou des clients, car ces derniers peuvent être informés de l'état d'avancement de leurs demandes et recevoir des réponses dans des délais raisonnables.

En résumé, un outil de ticketing est un système de gestion des tickets qui facilite la communication, le suivi et la résolution des problèmes au sein d'une organisation. Il contribue à une meilleure organisation, une collaboration efficace et une satisfaction accrue des utilisateurs ou des clients.

2) Qu'est-ce que la partie inventaire présente dans GLPI ?

GLPI est un logiciel open source de gestion des services informatiques qui propose une fonctionnalité d'inventaire pour suivre et gérer les actifs matériels et logiciels d'une organisation. La partie inventaire de GLPI permet de centraliser et de gérer les informations relatives à ces actifs, offrant ainsi une vue complète et détaillée de l'environnement informatique.

L'inventaire de GLPI se compose de plusieurs fonctionnalités clés :

1. Gestion des actifs matériels : GLPI permet d'enregistrer et de suivre les informations sur les équipements physiques tels que les ordinateurs, les serveurs, les imprimantes, les périphériques, etc… Chaque actif peut être associé à des détails tels que la marque, le modèle, le numéro de série, la date d'achat, la localisation, l'état. Cela facilite la gestion du cycle de vie des actifs, y compris les mouvements, les réparations et les retraits.

2. Gestion des logiciels : GLPI permet également de gérer les informations sur les logiciels installés sur les équipements. Il peut détecter automatiquement les logiciels présents sur les machines et enregistrer les licences associées. Cela permet de suivre les licences logicielles, de s'assurer de la conformité et d'effectuer des audits logiciels.

3. Gestion des consommables : GLPI offre la possibilité de gérer les consommables tels que les cartouches d'encre, les toners, les batteries. Les informations sur les consommables, comme les

quantités disponibles, les seuils de réapprovisionnement et les fournisseurs, peuvent être enregistrées pour faciliter la gestion des stocks.

4. Gestion des contrats : GLPI permet de gérer les contrats liés aux actifs, tels que les contrats de maintenance, les contrats de location, les contrats de garantie. Les détails du contrat, tels que les dates, les conditions et les fournisseurs, peuvent être enregistrés pour un suivi efficace des engagements contractuels.

5. Relations entre les actifs : GLPI permet d'établir des liens entre les actifs pour refléter les relations hiérarchiques ou de dépendance. Par exemple, il est possible de lier un ordinateur à un utilisateur, un serveur à une salle, ou un logiciel à un équipement spécifique. Cela permet d'avoir une vision globale des relations entre les différents actifs.

L'inventaire de GLPI offre une interface conviviale pour rechercher, filtrer et afficher les informations relatives aux actifs. Il permet de générer des rapports détaillés sur les actifs par exemple, les licences, les contrats, les mouvements, offrant ainsi une vue d'ensemble de l'environnement informatique de l'organisation.
En résumé, la partie inventaire de GLPI est une fonctionnalité essentielle qui permet de gérer de manière centralisée les informations sur les actifs matériels et logiciels d'une organisation. Elle facilite le suivi, la gestion et le reporting des actifs, contribuant ainsi à une meilleure organisation et à une utilisation efficace des ressources informatiques.

IV) Présentation du travail réalisé

1) Outil de monitoring

J'ai entrepris l'installation d'Eyes Of Network, explorant toutes ses fonctionnalités disponibles. Ensuite, j'ai ajouté les périphériques d'un site spécifique pour effectuer des tests. Cependant, il est rapidement apparu que Eyes Of Network n'était pas adapté à DuranSia. En effet, il exigeait l'ajout manuel de chaque hôte du réseau, ce qui n'était ni représentatif ni adapté à tous les sites de l'entreprise. Par conséquent, il a été décidé de rechercher une autre solution plus adaptée à DuranSia.
Au cours de mes recherches, j'ai découvert Zabbix, une solution open source permettant la découverte automatique des périphériques réseau en utilisant une plage d'adresses IP. Zabbix a été installé et présenté au service informatique, qui a rapidement adhéré à cette idée. Cette expérience m'a démontré qu'il est parfois nécessaire de remettre en question les choix initiaux et de rechercher des alternatives mieux adaptées à nos besoins.

J'ai débuté en configurant des règles de découverte dans Zabbix, ce qui m'a permis de filtrer les adresses IP par site et de les ajouter dans le système. L'avantage de cette approche est que je peux spécifier qu'une plage d'adresses IP doit être attribuée à un groupe d'hôtes spécifique. Dans le cas de DuranSia, où tous les commutateurs sont configurés avec des adresses se terminant par X.X.X.2, j'ai pu configurer Zabbix pour ajouter automatiquement ces adresses IP au groupe "switch" et activer SNMP sur ces appareils.

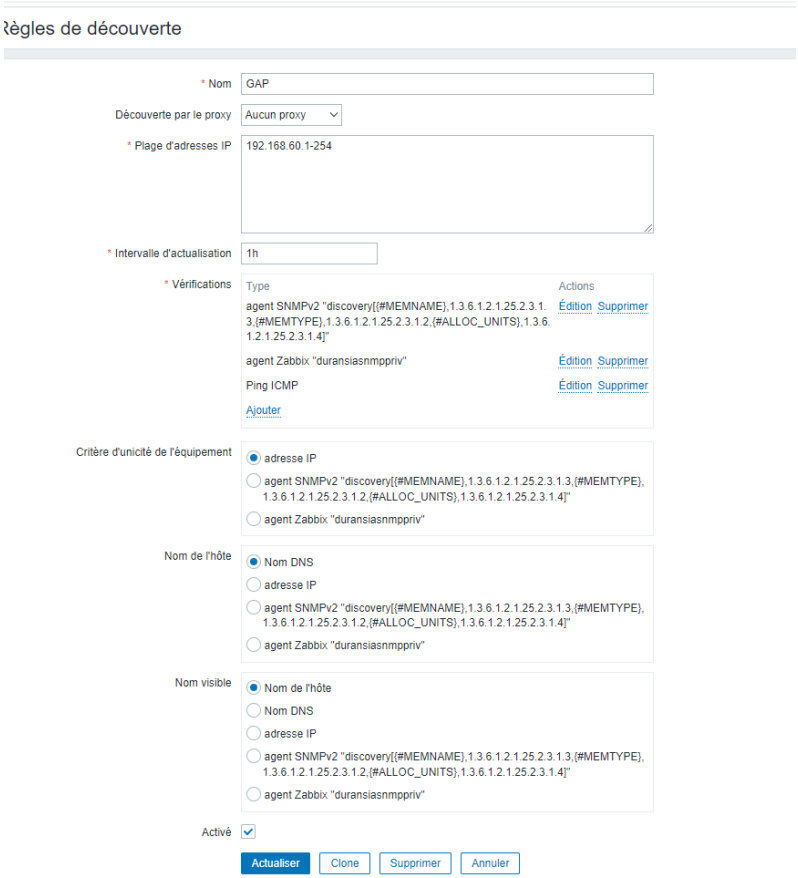

Figure 7 : Configuration règle de découverte sur Zabbix

Une fois que chaque site a été ajouté à Zabbix, chaque appareil connecté au réseau est automatiquement enregistré en tant que nouvel hôte dans Zabbix, ce qui constitue un gain de temps et une pratique appréciable. Ensuite, j'ai procédé à la configuration SNMP sur tous les commutateurs présents sur les sites. Ces commutateurs fonctionnent sous le système d'exploitation ARUBA et j'ai spécifié la communauté SNMP privée de DuranSia.

2) Pourquoi utiliser une communauté privée ?

La configuration de base des équipements actifs d'un réseau sont configurés avec une communauté SNMP « public ». DuranSia utilise une communauté SNMP privée plutôt que publique pour des raisons de sécurité. En optant pour une communauté privée, l'accès aux informations de supervision et de gestion du réseau est restreint aux seuls utilisateurs autorisés. Cela permet de prévenir les accès non autorisés et de protéger les données sensibles de l'entreprise.

L'utilisation d'une communauté privée garantit également la confidentialité des informations échangées entre les agents SNMP et le superviseur. Les données de supervision peuvent contenir des informations critiques sur les performances, les configurations et les vulnérabilités du réseau. En maintenant une communauté privée, DuranSia réduit les risques d'interception ou de manipulation de ces données par des personnes non autorisées.

En résumé, l'utilisation d'une communauté SNMP privée par DuranSia contribue à renforcer la sécurité de son réseau en limitant l'accès aux informations sensibles, en garantissant la confidentialité des données échangées et en permettant une gestion plus rigoureuse des autorisations d'accès.

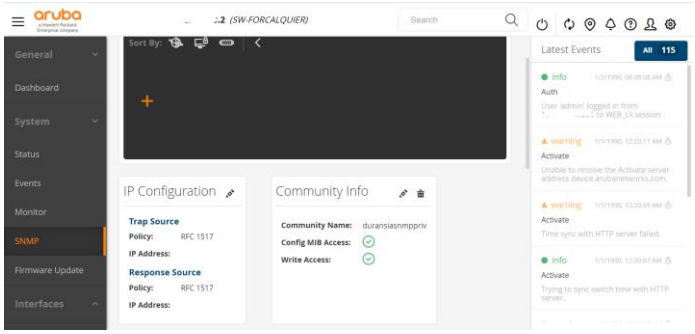

Figure 8 : Interface Switch aruba du Magasin de la commune de Forcalquier

Par la suite, nous commençons à observer l'intégration de nos commutateurs dans Zabbix, ce qui nous permet d'accéder à toutes les informations concernant les performances de nos commutateurs.

Figure 9 : Interface dernière données du logiciel Zabbix

Il offre également la possibilité d'effectuer un suivi graphique de toutes les activités sur un site, que ce soit pour surveiller la consommation de bande passante, effectuer un suivi du ping ICMP, l'utilisation de la mémoire ou processeur de l'appareil.

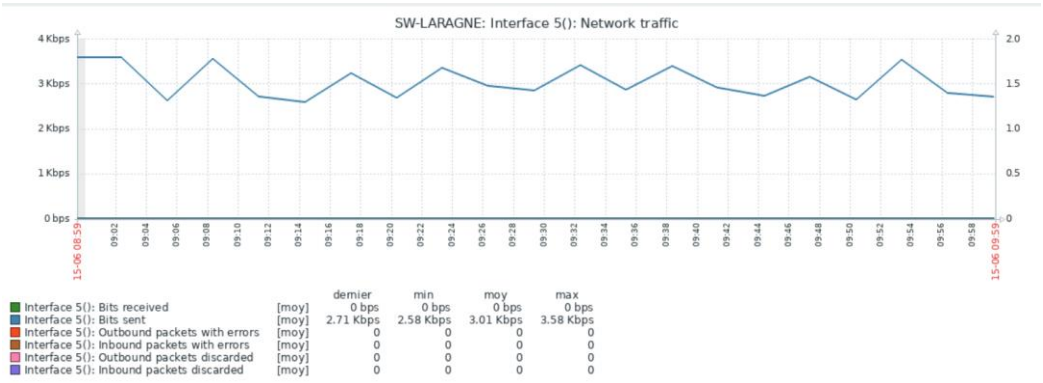

Figure 10 : Suivi graphique du Traffic de l'interface 5 du commutateur de Laragne

En conséquence, pour chaque hôte, il est possible d'attribuer ou de créer des alertes. Ces alertes sont utilisées pour notifier instantanément lorsqu'un événement critique se produit sur un appareil, et peuvent être configurées pour envoyer des notifications via la plateforme de notre choix, telle que SMS, Office 365 ou d'autres applications populaires. Pour DuranSia, j'ai configuré les alertes par mail en configurant un serveur SMTP et par Microsoft Teams qui est configurée dans une équipe qui notifie toute l'équipe informatique quand un problème survient.

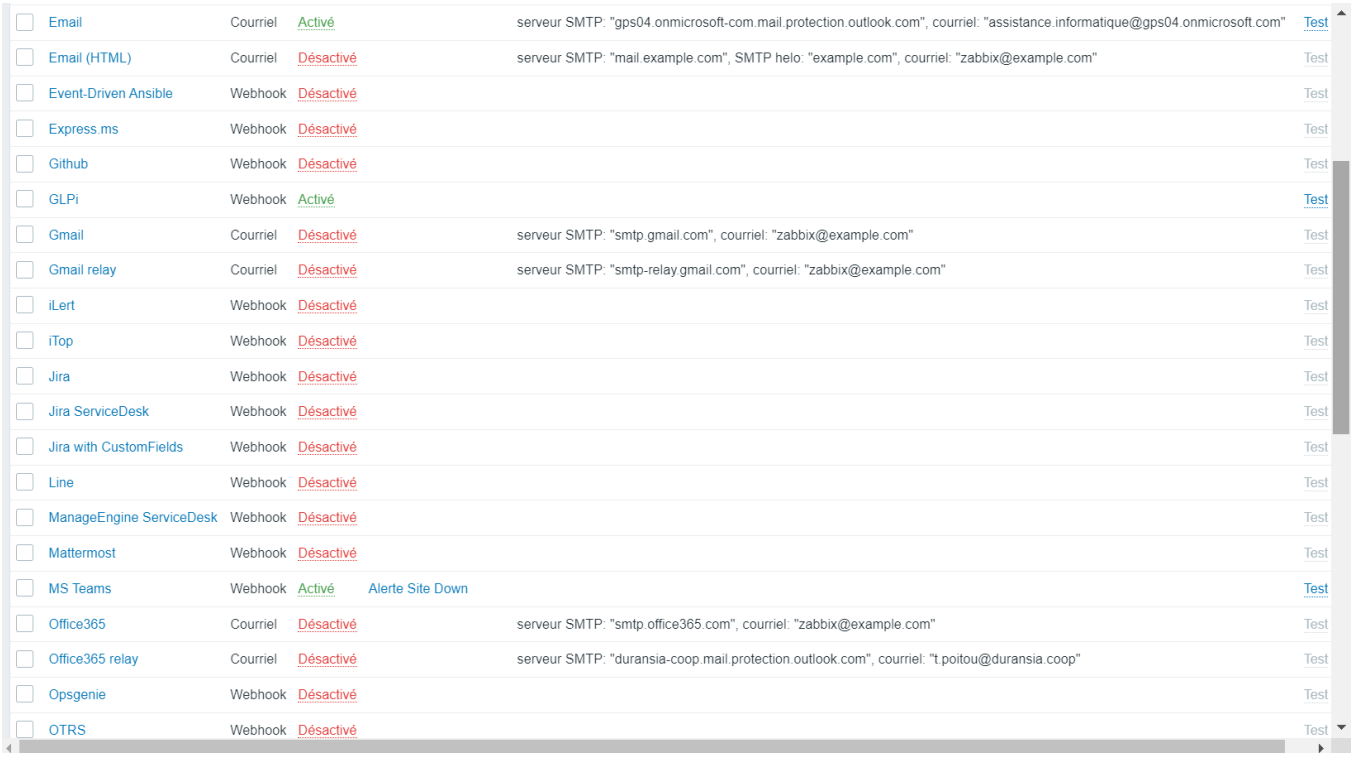

Figure 11 : Alertes configurables et possibles sur Zabbix.

La mise en place des règles de découverte dans Zabbix a été cruciale pour le déploiement du système de supervision chez DuranSia. Cette approche a simplifié la gestion du parc informatique en filtrant et en ajoutant automatiquement les adresses IP des commutateurs dans le système, regroupées par site et attribuées à des groupes d'hôtes spécifiques. La configuration SNMP sur les commutateurs ARUBA a permis de surveiller efficacement les performances du réseau, offrant une visualisation claire des activités grâce aux fonctionnalités graphiques de Zabbix. De plus, la possibilité de configurer des alertes personnalisées a amélioré la réactivité de l'équipe informatique, qui a pu être notifiée instantanément des événements critiques via e-mail et Microsoft Teams. En somme, Zabbix a renforcé la supervision du réseau chez DuranSia, permettant une meilleure gestion et une réactivité accrue face aux incidents.

3) Outil de Ticketing

Après avoir terminé l'installation de Zabbix, j'ai procédé à l'installation d'une autre machine virtuelle (VM) sur laquelle j'ai configuré GLPI. Tout comme avec Zabbix, j'ai exploré les nombreuses possibilités offertes par GLPI, mais les fonctionnalités qui intéressent particulièrement DuranSia sont le ticketing et l'inventaire du matériel informatique avec l'utilisation de l'agent GLPI.

Dans le but de faciliter l'expérience utilisateur et simplifier les processus, j'ai mis en place une intégration en Single Sign-On (SSO) entre le serveur GLPI et l'Active Directory. Cette intégration permet aux utilisateurs d'utiliser leurs identifiants de session d'ordinateur pour se connecter au serveur GLPI. Ainsi, ils n'ont pas besoin de gérer des identifiants supplémentaires, ce qui rend l'accès au serveur GLPI plus pratique et efficace. J'ai configuré mon annuaire LDAP pour récupérer initialement uniquement les utilisateurs qui sont membres du groupe "siège" dans l'Active Directory.

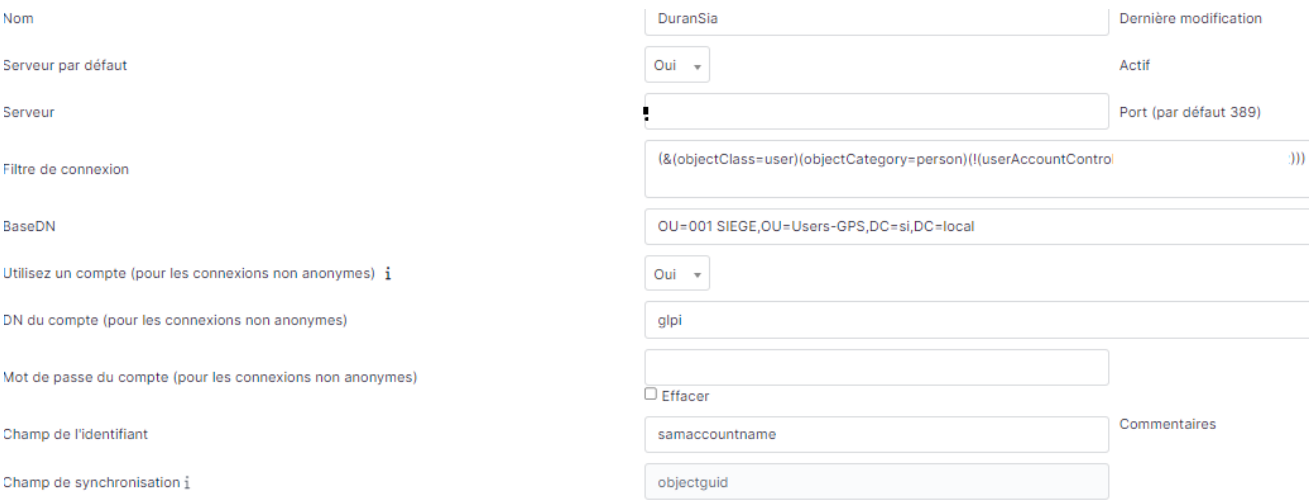

Figure 12 : Configuration de l'active Directory dans GLPI

J'ai ensuite commencé par me concentrer sur la partie inventaire et j'ai réussi à établir une connexion avec le serveur Active Directory de DuranSia.
En utilisant les stratégies de groupe (GPO), j'ai déployé un agent spécifiquement créé par GLPI, qui s'installe silencieusement sur les machines clientes et se connecte directement à mon serveur GLPI. Cela permet de remonter automatiquement les informations liées aux licences, au modèle, au numéro de série, aux écrans et aux imprimantes connectés à chaque ordinateur, offrant ainsi un suivi précis du matériel utilisé au sein de DuranSia.

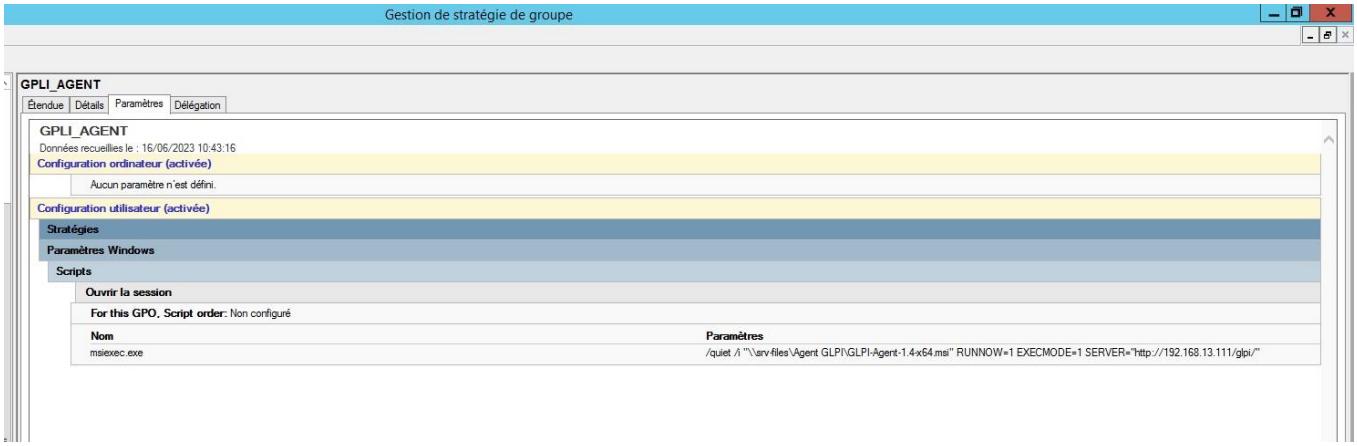

Figure 12 : Déploiement de la GPO via l'Active Directory local de DuranSia.

Script de la GPO : « /quiet /i '\\srv-files\Agent GLPI\GLPI-Agent-1.4x64.msi' RUNNOW=1 EXECMODE=1 SERVER='https://assistance.duransia.coop' »

Explication du script :

- /quiet : Cela correspond à une installation silencieuse, l'utilisateur ne voit pas l'installation.
- /i : Ce paramètre spécifie que l'action à effectuer est une installation.
- '\srv-files\Agent GLPI\GLPI-Agent-1.4x64.msi' : Il s'agit du chemin d'accès au fichier d'installation MSI de l'agent GLPI. Le script utilise ce chemin pour localiser le fichier et l'exécuter. Le partage et les droits NTFS appliqués permettent aux utilisateurs authentifiés d'accéder à ce dossier.

- RUNNOW=1 : Ce paramètre indique à l'agent GLPI d'exécuter immédiatement après son installation.
- EXECMODE=1 : Ce paramètre spécifie le mode d'exécution de l'agent GLPI en tant que service.
- SERVER='https://assistance.duransia.coop' : Ce paramètre spécifie l'adresse du serveur GLPI auquel l'agent doit se connecter pour la gestion des tickets d'assistance.

En résumé, ce script de GPO est utilisé pour installer l'agent GLPI de manière silencieuse sur les machines du réseau, le configurer pour s'exécuter en tant que service, et le connecter au serveur GLPI pour la gestion des tickets d'assistance sur le site 'https://assistance.duransia.coop'.

Enfin, sur l'interface GLPI, on a directement des catégories qui sont créées : Ordinateurs, License, Imprimante.

Figure 11 : Interface GLPI pour l'inventaire

A) Phase de test :

La phase de test du déploiement de la solution s'est déroulée en plusieurs étapes. Tout d'abord, des tests ont été effectués au sein du service informatique pour vérifier qu'il n'y avait aucune erreur d'installation et de configuration de base. Ensuite, la solution a été testée au siège de l'entreprise, où les utilisateurs sont plus expérimentés et utilisent régulièrement des ordinateurs dans le cadre de leur travail. Une fois que le service informatique aura évalué les résultats du test sur le siège social, le déploiement sera effectué sur l'ensemble des sites de l'entreprise. Toutefois, il est certain que cela sera plus complexe étant donné que ces sites ont une utilisation moins fréquente des ordinateurs.

B) L'interface utilisateur.

Pour rendre cette nouvelle organisation plus conviviale, il est essentiel de se mettre à la place de l'utilisateur et de simplifier au maximum l'interface. Chez DuranSia, les utilisateurs peuvent avoir des niveaux de compétence variés, il est donc primordial de rendre l'outil aussi simple que possible.

Pour le champ "Type", j'ai choisi de proposer deux options : "Incident" ou "Demande". Cela permet à l'utilisateur de filtrer dès le départ s'il a une question ou s'il souhaite signaler un incident.

En ce qui concerne les catégories, il est important de ne pas perdre les utilisateurs dans des termes trop techniques. J'ai donc opté pour trois grandes catégories : "Liaison Internet", "Matériel" et "Logiciel". Chacune de ces catégories comporte des sous-catégories plus spécifiques. Par exemple, sous "Liaison Internet", on trouve les sous-catégories "Coupures" et "Lenteurs". Pour "Matériel", j'ai simplifié avec les options "Imprimante", "PC" et "Petits périphériques". Quant aux problèmes logiciels, j'ai créé une sous-catégorie regroupant tous les logiciels utilisés par DuranSia.

Le champ "Urgence" permet à l'utilisateur de classer lui-même l'importance de sa demande ou de son incident. Au lieu des cinq critères initiaux, j'ai limité les options à trois : "Faible", "Moyen" et "Urgent".

Pour les lieux, DuranSia peut avoir des sites comprenant à la fois un magasin et un dépôt. Afin de cibler précisément l'emplacement du problème, j'ai ajouté des options pour les lieux, et pour les sites comportant deux entités distinctes, telles qu'un dépôt, j'ai créé une sous-catégorie avec "Magasin" et "Dépôt".

Ensuite, l'utilisateur peut décrire l'objet du ticket ainsi qu'une description détaillée de la demande ou de l'incident.

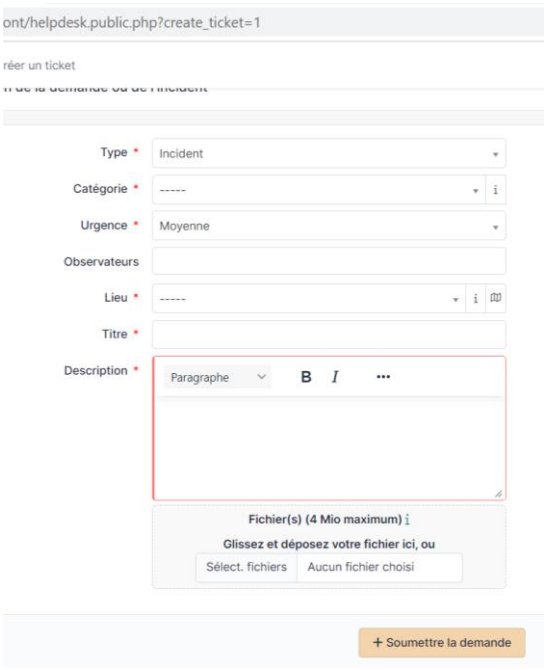

Figure 11 : Interface utilisateur sur GLPI

C) Point sécurité

A l'installation de GLPI, on a directement une banderole lors de la connexion en administrateur qui nous indique deux points :

- Pour des raisons de sécurité, veuillez supprimer le fichier : **install/install.php**
- Pour des raisons de sécurité, La configuration du dossier racine du serveur web n'est pas sécurisée car elle permet l'accès à des fichiers non publics. Référez-vous à la documentation d'installation pour plus de détails.

Premier point :
Si l'on ne supprime pas le **install.php** les conséquences peuvent être lourdes : n'importe qui peut relancer l'installation de GLPI et supprimer tout ce que l'on a fait avant. Ce serait problématique car si quelqu'un relance l'installation de GLPI cela ferait que les identifiants admins serait remis à zéro et l'attaquant aurait des accès administrateur.

Pour remédier à cela j'ai simplement supprimé le fichier install.php dans le dossier d'installation :
« rm /var/www/html/glpi/install/install.php »

Second point :
Plus complexe, j'ai dû créer un hôte virtuel et lui ajouter des directives. Il indique que la configuration de GLPI permet l'accès à des fichiers non publics. Cela pose un problème car cela veut dire qu'un utilisateur sans privilèges aurait accès à des fichiers qui peuvent être compromettants.

Comment j’ai résolu ce problème :

J’ai créé un hôte virtuel dans l’installation du serveur web Apache et lui ai ajouté une directive pour que le dossier « public » soit seulement accessible. Donc voici les directives que j’ai ajouté :

« <Directory /var/www/html/glpi/public>
Require all granted
RewriteEngine On
RewriteCond %{REQUEST_FILENAME} !-f
RewriteRule ^(.*)$ index.php [QSA,L]
RewriteRule .* https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L] »

Cette directive Apache est utilisée pour configurer le comportement du serveur web Apache dans un répertoire spécifique, à savoir "/var/www/html/glpi/public".

Description de la directive :

- "<Directory /var/www/html/glpi/public>" : Cette ligne spécifie le répertoire sur lequel s'appliqueront les directives ci-après. Dans ce cas, il s'agit du répertoire "/var/www/html/glpi/public".

- "Require all granted" : Cette ligne permet d'autoriser l'accès à tous les utilisateurs au répertoire spécifié. Elle permet à tous les utilisateurs d'accéder aux ressources présentes dans ce répertoire.

- "RewriteEngine On" : Cette ligne active le module de réécriture d'URL d'Apache, ce qui permet de rediriger ou de modifier les URL.

- "RewriteCond %{REQUEST_FILENAME} !-f" : Cette ligne définit une condition de réécriture d'URL. Elle spécifie que la réécriture ne s'applique que si le fichier demandé n'existe pas.

- "RewriteRule ^(.*)$ index.php [QSA,L]" : Cette ligne est une règle de réécriture d'URL. Elle redirige toutes les requêtes vers le fichier "index.php" situé dans le répertoire spécifié. Le [QSA,L] signifie que les paramètres de l'URL d'origine sont conservés lors de la redirection (QSA pour "Query String Append") et que la réécriture est terminée (L pour "Last").

- "RewriteRule .* https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]" : Cette ligne est une autre règle de réécriture d'URL. Elle redirige toutes les requêtes vers une URL sécurisée commençant par "https://". Le [R=301,L] indique qu'il s'agit d'une redirection permanente (301) et que la réécriture est terminée (L).

En résumé, cette directive Apache permet d'autoriser l'accès à un répertoire spécifique, de rediriger toutes les requêtes vers le fichier "index.php" s'il n'y a pas de fichier correspondant, et de rediriger toutes les requêtes vers une URL sécurisée en utilisant le protocole HTTPS.

Pour plus de facilité et de sécurité, j'ai ensuite proposé d'acheter un certificat SSL car à l'origine, GLPI est en http. Le passage en HTTPS offre une sécurité supplémentaire. Cela a permis également d'enlever une banderole rouge expliquant que le site est en http.
J'ai consulté mon responsable qui m'a autorisé à contacter l'entreprise Sudériane pour acheter ce certificat.
J'ai ensuite ajouté à mon hôte virtuel une redirection du port 80 vers 443 HTTP vers HTTPS.

Afin de créer le certificat SSL, j'ai dû établir le sous-domaine assistance.duransia.coop au sein du domaine duransia.coop.
Le serveur GLPI est accessible seulement depuis le réseau local car il a été décidé dans un premier temps, de ne pas l'héberger sur internet. Les utilisateurs ont tous accès à un VPN SSL qui les connecte directement au réseau local de DuranSia.

V) Conclusion

En conclusion, l'intégration de Zabbix et de GLPI a considérablement amélioré la gestion de l'infrastructure informatique de DuranSia, en offrant une supervision proactive, un suivi précis du matériel et une meilleure communication avec les utilisateurs. Ces outils constituent désormais une base solide pour soutenir les opérations informatiques de l'entreprise et anticiper les besoins futurs en matière de gestion de l'infrastructure.

Grâce à Zabbix, nous avons pu automatiser la découverte des périphériques réseau et surveiller leurs performances en temps réel. L'utilisation de règles de découverte a permis d'ajouter automatiquement les adresses IP des commutateurs dans les groupes appropriés, simplifiant ainsi la configuration et la surveillance. Les alertes configurables ont également permis de détecter rapidement les événements critiques et de notifier l'équipe informatique.

Quant à GLPI, il a permis d'établir un inventaire complet du matériel informatique de DuranSia. L'intégration de l'agent avec le serveur a facilité la collecte des informations liées aux licences, aux modèles, aux numéros de série, aux écrans et aux imprimantes. Le déploiement de l'agent GLPI via les stratégies de groupe a assuré une remontée automatique de ces données, offrant ainsi un suivi précis du matériel en service.
En mettant en place le système de ticketing, nous avons facilité la communication entre les utilisateurs et l'équipe informatique. Les utilisateurs doivent soumettre les demandes de support à l'aide d'un mail envoyé à informatique.assistance@duransia.coop ou en se connectant au Portail GLPI accessible depuis Office 365, teams ou depuis une url, ce qui permet un suivi efficace des problèmes rencontrés. De plus, le classement des problèmes par priorité permet à l'équipe informatique de prioriser les tâches et de résoudre les problèmes les plus critiques en premier.

Ce projet a été l'occasion d'appliquer les connaissances acquises lors de nos cours, notamment en matière de déploiement d'outils de supervision, de configuration de règles de découverte, de gestion de l'inventaire et de mise en place d'un système de ticketing. Il a également souligné l'importance de remettre en question les choix initiaux et de rechercher des solutions mieux adaptées aux besoins spécifiques de l'entreprise.

La vie en entreprise m'a apporté de précieuses leçons et enseignements tout au long de ce projet. J'ai pu apprendre l'importance de la communication et de la collaboration au sein d'une équipe. Travailler en étroite collaboration avec les membres du service informatique de DuranSia m'a permis de comprendre les besoins spécifiques de l'entreprise et de trouver des solutions qui correspondent à ces besoins. J'ai également réalisé que remettre en question les choix initiaux et être ouvert aux nouvelles idées sont des qualités essentielles pour mener à bien un projet. La flexibilité, l'adaptabilité et la capacité à résoudre les problèmes de manière créative sont des compétences clés dans un environnement professionnel. Enfin, cette expérience m'a également appris l'importance de la rigueur et de la précision dans le déploiement des outils, ainsi que la nécessité de bien documenter les procédures et les configurations pour une meilleure gestion à long terme.

VI) Remerciements

Je tiens à exprimer mes sincères remerciements à plusieurs personnes qui ont joué un rôle essentiel dans la réalisation de mon stage et dans la réussite de ce projet.

Tout d'abord, je tiens à remercier Alexandre CALISSI-BARRAL, mon tuteur de stage et Responsable du service informatique, pour sa précieuse guidance, son soutien constant et ses conseils avisés tout au long de cette expérience. Sa disponibilité, son expertise et sa confiance ont été des facteurs clés dans mon apprentissage et dans l'accomplissement de mes missions. Sa passion pour l'informatique et son professionnalisme m'ont inspiré et motivé à donner le meilleur de moi-même.

Je souhaite également exprimer ma gratitude envers Hervé LADIGLIONE, Technicien du service informatique de DuranSia, pour son accueil chaleureux, sa confiance et son ouverture d'esprit. Ses connaissances approfondies du domaine et son implication dans le projet ont été d'une grande valeur. Sa collaboration et ses précieux éclaircissements ont grandement facilité la réalisation des tâches assignées.

Mes remerciements vont également à Martine VALLON, responsable Marketing et eBusiness de DuranSia, pour son soutien et sa bienveillance tout au long de mon stage. Sa disponibilité et ses conseils m'ont permis de me sentir intégré et soutenu au sein de l'entreprise.

Enfin, je tiens à exprimer ma reconnaissance envers Richard SAUVAT, Directeur Général de DuranSia, pour m’avoir donné l'opportunité de réaliser ce stage au sein de cette entreprise. Sa vision, son leadership et son intérêt pour l'innovation technologique ont créé un environnement propice à l'apprentissage et au développement de compétences.

Je suis reconnaissant envers chacune de ces personnes pour leur contribution précieuse, leur confiance et leur support tout au long de mon stage. Leur implication a été déterminante dans mon expérience enrichissante chez DuranSia.

BUT : Bachelor Universitaire de Technologie

Switch : Un **switch**, commutateur ou commutateur réseau en français, est un équipement qui fonctionne comme un pont multiport et qui permet de relier plusieurs segments d'un réseau informatique entre eux.

Ticketing : Système de création de demande ou de déclaration d'incident destiné au service informatique.

Hybride : Le terme « cloud hybride » désigne une combinaison d'au moins 2 environnements de cloud computing qui échangent des informations entre eux et exécutent une série uniforme d'applications pour le compte d'une entreprise.

On-premise : Traduction de « sur site », les infrastructures informatiques et logicielles sont appelées « on-premise » lorsque celles-ci sont hébergées et maintenues par le propre service informatique de l'entreprise. On oppose généralement ce modèle « on-premise » à **l'Hybride**, où toute l'infrastructure est installée et gérée sur des serveurs distants.

MPLS : Le Multiprotocol Label Switching (MPLS) est une technologie conçue pour améliorer la vitesse et l'efficacité du transfert des données au sein de réseaux étendus. Il fonctionne dans un réseau privé virtuel (VPN) et s'intègre aux infrastructures sous-jacentes, comme les réseaux IP (Internet Protocol), Ethernet, FR (Frame Relay) et ATM (Asynchronous Transfer Mode). Il s'agit donc d'une option de mise en réseau évolutive à faible latence.

ERP : L'ERP (Enterprise Resource Planning) est une solution informatique dédiée aux entreprises afin de piloter un ensemble de processus liés à son activité. Il permet notamment d'administrer les opérations liées à la gestion financière, à la production, aux ressources humaines. L'ERP est un socle d'informations fiables et unifiées pour les entreprises, qui répond à des enjeux d'optimisation des ressources et des coûts.

Interopérabilité : L'interopérabilité définit un ensemble de systèmes capables de fonctionner et communiquer ensemble sans barrière (sémantique, syntaxique, technique, …).

Il existe plusieurs niveaux d'interopérabilité, ces niveaux permettent de définir des standards ou normes sur lesquels les acteurs doivent s'accorder afin de pouvoir échanger des données sans restriction.

ICMP : L'ICMP (Internet Control Message Protocol) est un protocole de signalement d'erreurs que les appareils de réseau comme les routeurs utilisent pour générer des messages d'erreur à l'adresse IP source lorsque des problèmes de réseau empêchent la livraison de paquets IP. L'Internet Control Message Protocol crée et envoie des messages à l'adresse IP source indiquant qu'une passerelle vers l'internet qu'un routeur, un service ou un hôte ne peut pas être atteint pour la livraison de paquets. Tout dispositif de réseau IP a la capacité d'envoyer, de recevoir ou de traiter des messages ICMP.

SMTP : Le protocole SMTP, pour Simple Mail Transfer Protocol, désigne un protocole standard de communication. Il est principalement employé pour le transfert du courrier électronique d'un serveur à un autre.

VII) Bibliographie / Sitographie

https://duransia.coop/ (Site Officiel de DuranSia.)

https://www.zabbix.com/ (Site Officiel de Zabbix)

https://glpi-install.readthedocs.io/en/latest/ (Site officiel de la documentation de GLPI)