RÉGION Nouvelle-Aquitaine

RAPPORT DE STAGE

BTS SIO 1ère année,

Du 27 Mai au 28 Juin 2024

Rayan BERRAHMOUNE
BTS SIO 1ère année

Sommaire

Tuteur : Lambert Guillaume

Fonction : Chef du service "Infrastructure systèmes et réseaux des lycées"

Professeur: Monsieur Sautour F.

Introduction

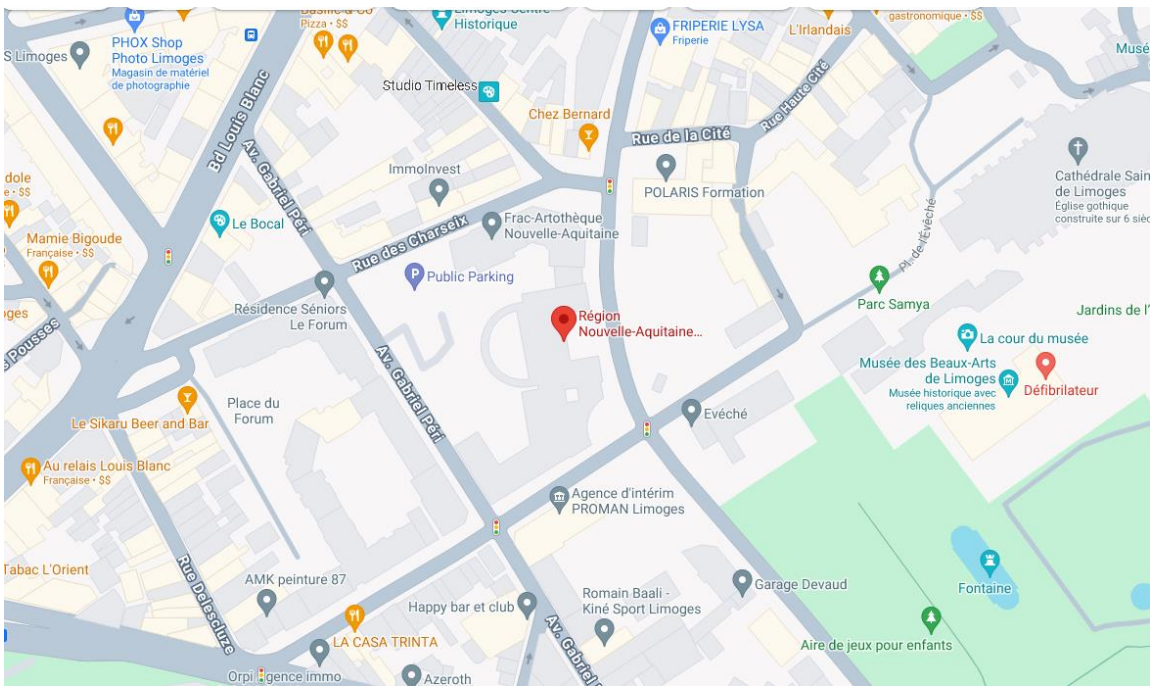
Pendant cette première année de BTS SIO en option SISR, j'ai effectué un stage dans le service Infrastructure systèmes et réseaux des lycées à la région de la Nouvelle-Aquitaine à limoges du 27 Mai au 28 Juin 2024.

Je remercie Mr Lambert de m'avoir permis d'effectuer mon stage, ainsi que les personnes du service.

Le service dédié à l'infrastructure des systèmes et réseaux des lycées de la région Nouvelle-Aquitaine, sous l'égide de la région, a été mis en place progressivement à partir de la création de la région Nouvelle-Aquitaine le 1er janvier 2016.

Ce service s'est développé pour répondre aux besoins spécifiques des lycées en matière de numérique et de technologie après cette date.

CS 3116 cedex, 27 Bd de la Corderie 1, 87000 Limoges, Lien vers le site



Présentation Générale du Travail Effectué

1. Solution de Sécurité WAZUH

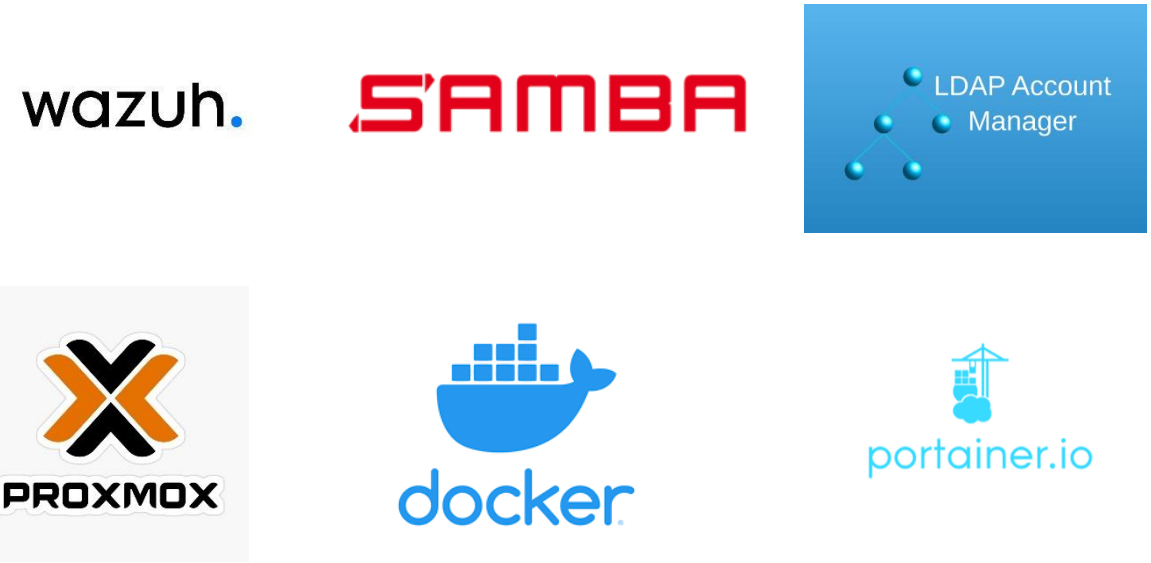
J'ai installé, configuré et utilisé WAZUH qui est conçue pour offrir une protection avancée contre les menaces et assurer la conformité dans les environnements informatiques.

2. Partage de Fichiers avec SAMBA et Authentification LAM

J'utilise Samba pour gérer les services d'annuaire et de partage de fichiers. En intégrant LDAP Account Manager (LAM), j'ai simplifié l'authentification et la gestion des utilisateurs, permettant une administration centralisée et sécurisée des accès au sein des lycées.

3. Virtualisation avec Proxmox, Docker et Portainer

Proxmox m'a permis de créer des machines virtuelles et déployer des applications avec Docker. Portainer a simplifié la gestion des conteneurs, optimisant ainsi les ressources informatiques.



Déroulement

Contexte

Le 1er janvier 2016, plusieurs régions se sont unies pour former la Nouvelle-Aquitaine. Cette fusion a conduit à la centralisation des services administratifs, avec un seul rectorat désormais en place pour superviser la région. Dans le cadre de cette réorganisation, les lycées de la région ont été segmentés en deux VLAN distincts : un pour les activités pédagogiques et un autre pour les tâches administratives.

Afin de gérer et de sécuriser efficacement les infrastructures réseau et système de ces 300 lycées, le Service d'Infrastructure Système et Réseau a été créée. Mon stage s'inscrit dans ce vaste projet de déploiement et de sécurisation des établissements scolaires de la région.

J'ai tout d'abord installé mon poste de travail composé d'un serveur sous Debian 12, un switch, un écran et une souris ainsi qu'un PC portable pour réaliser mes tests et l'utiliser pour rédiger mes documentations.

Après avoir configuré mon environnement initial, j'ai commencé par installer Proxmox VE, une plateforme de virtualisation open-source basée sur Debian, qui m'a permis de gérer efficacement mes machines virtuelles.

Mission 1 : Samba AD, Wazuh

Samba AD

Ma première tâche était de créer un domaine nommé "admin.lan" et d'y intégrer deux utilisateurs. Pour accomplir cette étape importante de gestion des identités et des accès, j'ai utilisé Samba Active Directory (Samba AD), une solution open source bien connue pour mettre en place et gérer des services d'annuaire dans les systèmes Linux.

J'ai commencé par configurer le serveur pour qu'il fonctionne en tant que contrôleur de domaine. Cela a impliqué l'installation des logiciels nécessaires et la configuration du fichier principal de Samba, appelé `smb.conf`, où j'ai spécifié les détails spécifiques pour le domaine "admin.lan". Ensuite, j'ai utilisé l'outil `samba-tool` pour provisionner le domaine, en fournissant des informations telles que le nom du domaine, le type de domaine et les paramètres DNS nécessaires.

Une fois le domaine établi avec succès, j'ai ajouté les utilisateurs au domaine "admin.lan". Pour chaque utilisateur, j'ai créé un compte dédié dans Samba AD. Cette étape garantissait que chaque utilisateur pouvait se connecter au domaine et accéder aux ressources partagées conformément aux règles de sécurité établies.

Wazuh

Ensuite j'ai créé une seconde Machine Virtuelle afin d'installer Wazuh. Wazuh est une plateforme de sécurité open-source qui offre la détection avancée des menaces, la surveillance de la conformité et la réponse aux incidents.

Wazuh est composé de 3 outils,

Wazuh indexer est utilisé pour l'indexation, le stockage et la recherche des données de logs et des événements de sécurité collectés par Wazuh.

Wazuh server analyse les données des agents, identifie les menaces et déclenche des alertes. Il gère aussi la configuration des agents et surveille leur état.

Le **Wazuh dashboard** est une interface web intuitive pour analyser et visualiser les données de sécurité, avec des tableaux de bord prêts à l'emploi.

Pour l'installation de Wazuh il suffisait d'installer les paquages `'wazuh-manager, wazuh-api'` et modifier les fichiers de configuration pour adapter les paramètres de base comme les adresse IP et les ports. Puis de déployé les agents wazuh sur les machines qu'on souhaite

Les agents Wazuh sont installés sur chaque machine à surveiller dans un réseau informatique. Leur rôle principal est de collecter activement les logs générés par le système d'exploitation, les applications installées et les services en cours d'exécution, ainsi que les événements de sécurité pertinents tels que les tentatives de connexion, les modifications de fichiers sensibles et les comportements

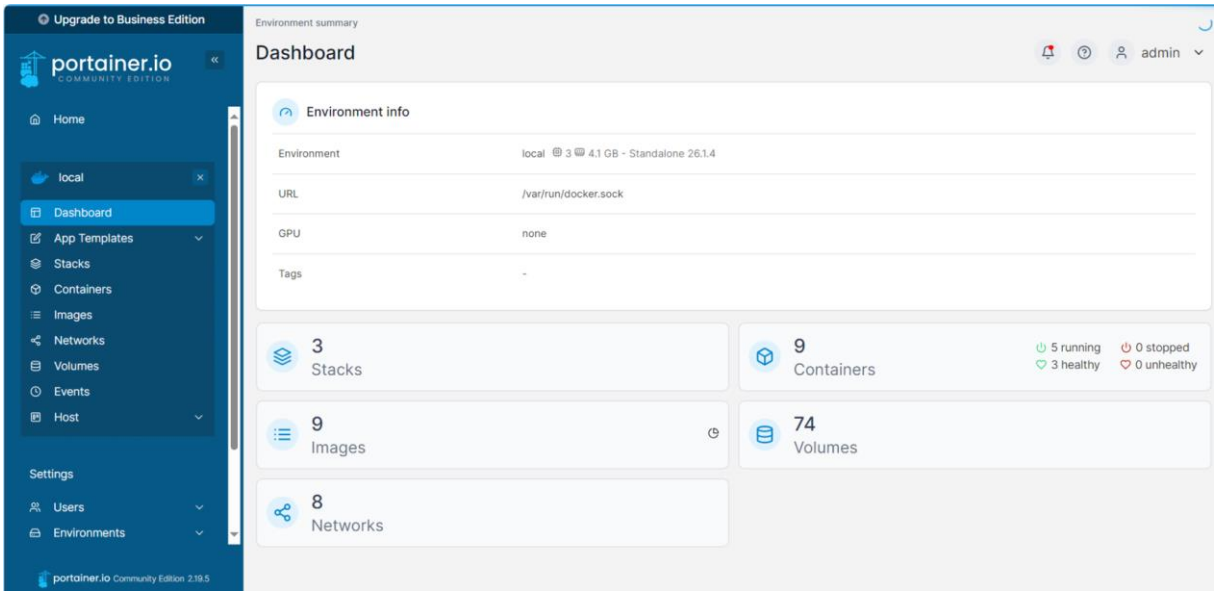
anormaux. Une fois collectées, ces données sont transmises de manière sécurisée au Wazuh Server centralisé pour analyse approfondie.

Mission 2 : Samba AD, Wazuh, Windows, Portainer, LAM, RSAT

Pour cette mission, j'ai utilisé Docker pour virtualiser et gérer de manière conteneurisée plusieurs services essentiels. Chaque service a été configuré dans un conteneur distinct pour garantir une gestion optimisée et sécurisée de l'infrastructure.

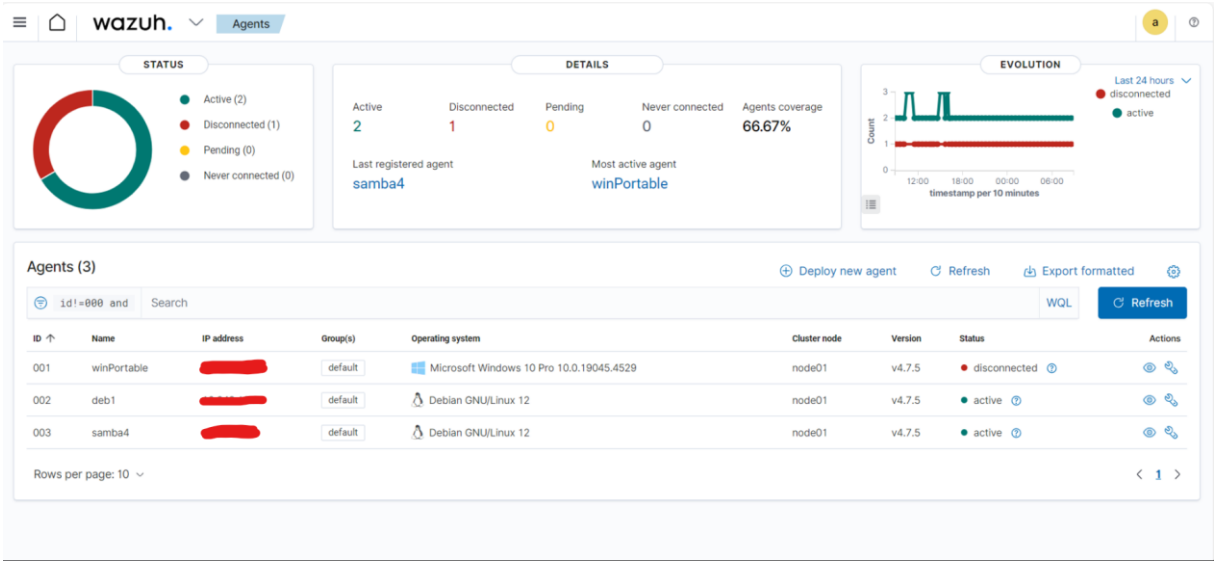
Dans un premier temps, j'ai reproduit tout mon infrastructure qui été héberger sur des VMs directement dans des containers Docker qui été composé de Samba AD avec son domaine admin.lan et de Wazuh.

Et je gère mes containers avec l'interface web Portainer qui est aussi héberger par Docker.



Ensuite, j'ai créé un nouveau container pour héberger Windows 10, Ce conteneur permet d'utiliser Remote Server Administration Tools (RSAT) qui est un ensemble d'outils fourni par Microsoft pour permettre l'administration à distance de serveurs Windows, et j'ai installé SCOOP qui est un gestionnaire de paquets gratuit en ligne de commande utilisé sur PowerShell.

Puis j'ai déployé mes deux agents wazuh sur le container Samba AD et le container Windows 10.



J'ai ensuite fait des tests de détection d'attaque sur la Windows avec un « Anti malware testfile » du site Eicar.org.

Enfin, j'ai installé LDAP Account Manager (LAM), un outil web qui simplifie la gestion des comptes utilisateurs dans un environnement LDAP. LAM offre une interface pour administrer les utilisateurs, groupes et autre, rendant l'administration plus accessible et efficace.

Je l'ai ensuite connecté à mon serveur Samba AD pour une gestion centralisée des comptes utilisateurs dans le domaine "admin.lan". Dans le cas de mon entreprise, LAM est utilisé pour permettre aux lycées de gérer les comptes des élèves.

Cette configuration facilite le support de niveau 1, permettant gérer facilement les comptes utilisateurs et d'effectuer des tâches courantes comme les réinitialisations de mot de passe et les mises à jour de profils, sans nécessiter de compétences techniques avancées.

J'ai réalisé mes deux missions avec un second stagiaire. Pour ma première mission, je n'ai rencontré aucune difficulté majeure. En revanche, la deuxième mission a été plus complexe, notamment pour mettre en place la machine Windows sous Docker et réussir à établir une connexion RDP. Nous avons également rencontré des difficultés à connecter le conteneur LDAP Account Manager au serveur Samba AD, en raison de problèmes liés au DNS et au pare-feu, nécessitant un effort supplémentaire pour résoudre ces problèmes.

Bilan

L'infrastructure que j'ai mise en place est spécifiquement conçue pour répondre aux besoins complexes des lycées en matière de gestion informatique et de sécurité. Grâce à Samba AD, les établissements peuvent centraliser et sécuriser l'accès aux données, tout en facilitant la collaboration entre les différents utilisateurs. Wazuh assure une surveillance proactive des menaces, crucial pour maintenir la sécurité des systèmes éducatifs face aux menaces numériques actuelles. En utilisant Docker et Portainer, nous pouvons rapidement déployer de nouvelles instances de services tout en optimisant les ressources disponibles, assurant ainsi une gestion efficace des infrastructures informatiques des lycées.

De plus, l'architecture basée sur des conteneurs comme Docker facilite la duplication et le déploiement de cette infrastructure dans les 300 lycées de la région Nouvelle-Aquitaine. Chaque lycée peut bénéficier d'une instance autonome de Samba AD et de Wazuh, configurée et gérée de manière centralisée grâce à Portainer. Cette approche permet une expansion rapide et harmonisée des capacités informatiques, assurant une uniformité dans la sécurité et la gestion des données à travers tous les établissements scolaires.

Ce stage m'a permis de découvrir de nouveaux logiciels, notamment Docker que j’ai redécouvert et approfondi mes connaissances, ainsi que LAM, RSAT et Samba pour la gestion, des outils que je ne connaissais pas auparavant. Ce stage m'a également permis de découvrir Wazuh que j'ai découvert et mise en œuvre pour améliorer la protection des systèmes d'information. Grâce à ces expériences, j'ai

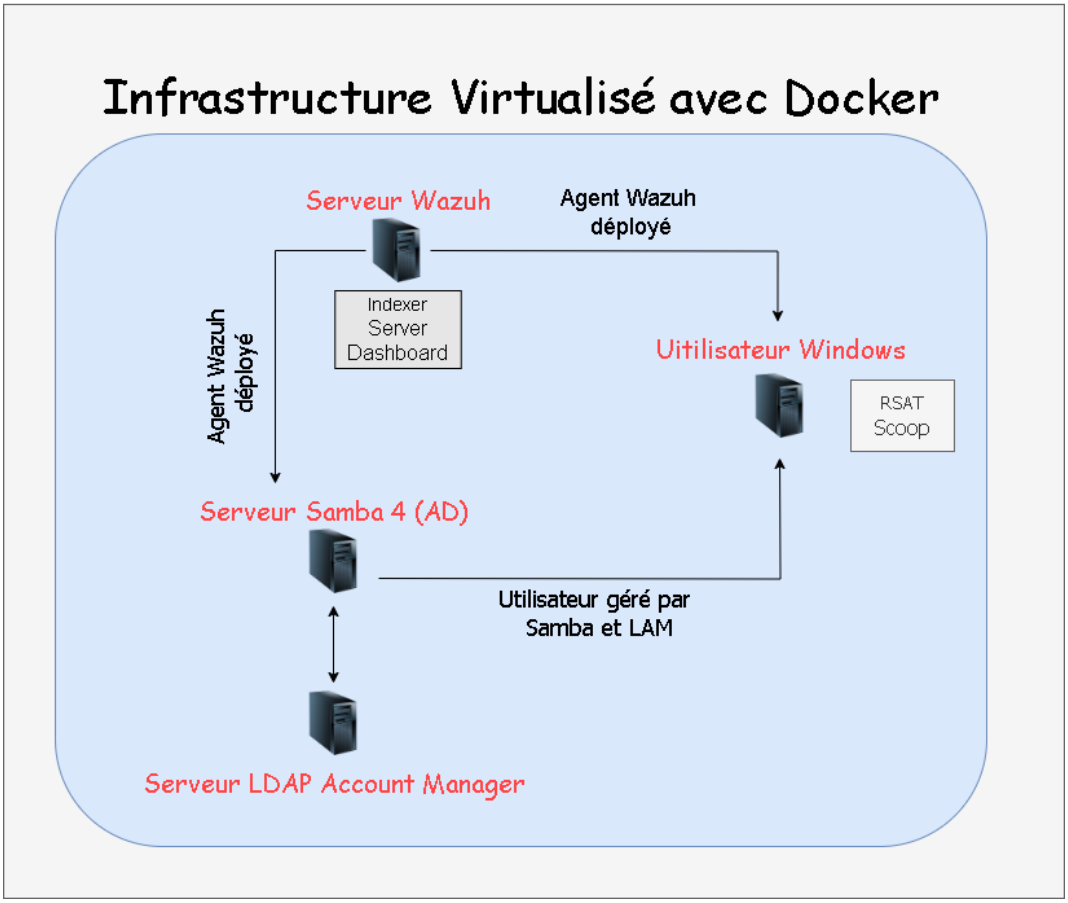
acquis des compétences précieuses dans la mise en place et la configuration d'infrastructures informatiques complexes, enrichissant ainsi mes connaissances.

En termes d'organisation et de gestion de projet, j'ai développé une meilleure compréhension des processus et des méthodologies utilisés pour planifier et exécuter des projets informatiques à grande échelle.

Hormis mes missions, j'ai également eu l'opportunité de suivre des formations complémentaires, notamment sur SaltStack (SALTproject.io), ce qui m'a permis d'en apprendre plus sur l'automatisation et la gestion de la configuration des systèmes informatiques.

(Voir ma prise de note dans l'annexe pour Salt)

Serveur sous Debian 12 hébergeant toutes l'infrastructure



Conclusion

Si j'avais la possibilité de refaire mon stage de seconde année à la Région, je le referais car j'ai trouvé cette expérience très enrichissante et passionnante, j'ai apprécié l'aspect concret des projets sur lesquels nous avons travaillé et que ça a un objectif clair : de déployés des solutions pour les lycées au niveau informatique.

Pour l'année prochaine, le type de stage qui m'intéresserait serait similaire, impliquant le travail sur des infrastructures et la sécurité informatique.

Annexe

CARTE D'IDENTITÉ D'ENTREPRISE

■ Dénomination :

Région Nouvelle-Aquitaine - Maison de Limoges

■ Siège social :

HOTEL DE REGION, 14 RUE FRANCOIS DE SOURDIS, 33000 BORDEAUX

■ Adresse du lieu de stage :

Maison de Limoges, 27 boulevard de la Corderie, CS 3116, 87031 Limoges Cedex 1, France

■ Nationalité :

Française

■ Secteur d'activité :

Administration publique régionale

■ Objet :

Gestion des affaires régionales

■ Forme juridique :

Entreprise publique ou privée Individuelle ou sociétaire et quel statut ?

Entreprise publique, Statut de la Fonction publique territorial

■ Capital :

Non applicable pour les administrations publiques.

■ Effectif :

Entre 5 000 et 10 000

■ Chiffre d'affaires :

Non disponible

■ Environnement juridique : Autonome ou dépendante d'un groupe, si oui lequel ? Description de ce groupe voire cotation en bourse ?

Autonome

Mes documentations :

Documentation Wazuh sous Docker

Documentation Portainer sous Docker

Création domaine Samba

Documentation Wazuh

Prise de note :

Prise de note Salt Project