Compte-rendu S6 Stage

Elaboré par

Yann Duffay

Promotion

1 TSIO

Année scolaire

2023-2024

Tuteur de stage : *M. Gilles Sorgiati*
Enseignant référent : *M. Bruno Jousseaume*
Enseignant chargé du suivi : *M. Philippe Guichard*

Établissement : *Lycée Polyvalent Chevrollier - 2 Rue Adrien Recouvreur 49035 Angers*
Entreprise d'accueil : *Ehpad Mer et Pins - 63 avenue de Bodon 44250 St Brévin les Pins*

SOMMAIRE

I. Rappel du contexte..... 2
1.1. Les Missions de l'EHPAD Mer et Pins.....3
1.2. Les Salariés.....3
1.3. Les Sites.....4
1.3.1 Site Mindin :.....4
1.3.2. Site des Sylphes :.....4
1.3.3. Site Fleur d'Ajonc :..... 4
1.3.4. Site Vent d'Ouest :.....4
II. Rappel des missions confiées..... 5
2.1. Les missions confiées..... 5
III. Missions réalisées (Outils-Difficultées-Solutions)..... 5
3.1. La Gestion du parc informatique..... 5
3.2. Le Ticketing..... 6
3.3. Le déploiement d'une solution de supervision en Open Source..... 8
IV. Bilan global Stage..... 11

I. Rappel du contexte

L’EHPAD Mer et Pins (Etablissement d'hébergement pour personnes âgées dépendantes et personnes handicapées âgées) est un établissement public médico-social relevant de la fonction publique hospitalière, c’est-à-dire qu'il fait partie du système de santé public français, sous la gestion et la réglementation des autorités sanitaires. L’établissement dispose d’une capacité de 310 lits, répartis entre plusieurs services sur le site administratif et trois autres sites de la commune de Saint-Brevin-Les-Pins.

1.1. Les Missions de l’EHPAD Mer et Pins

L’EHPAD Mer et Pins se donne pour mission d’accompagner les personnes âgées dans leur vie quotidienne en répondant au mieux à leurs besoins, tout en respectant leurs individualités. L’objectif est de créer un environnement où les résidents se sentent comme chez eux. Le projet d'établissement est structuré en objectifs sur cinq ans, visant à :

- ☐ Diversifier et adapter l'offre d'accueil, en se spécialisant notamment pour les personnes handicapées âgées.
- ☐ Optimiser le patrimoine immobilier et redéployer des lits.
- ☐ Promouvoir la participation des usagers et l'image de l'établissement.
- ☐ Engager une démarche qualité et renforcer l'ouverture vers l'extérieur.
- ☐ Définir les valeurs de l'établissement et encourager la réflexion éthique.

1.2. Les Salariés

L’EHPAD Mer et Pins c’est 230 professionnels répartis entre les différents services :

☐ *Administratifs*	☐ *Techniques*
☐ *Médicaux*	☐ *Soignants*
☐ *Animatrices*	☐ *Psychomotricienne*
☐ *Ergothérapeutes*	☐ *Psychologue*

En tant que stagiaire au service informatique, je travaille avec le responsable informatique, basé au siège administratif, mais je suis amené à me déplacer dans les différentes résidences pour des interventions.

1.3. Les Sites

1.3.1 Site Mindin :

Sur ce site nous retrouvons le siège administratif ainsi que la résidence Camélias/ Pervenches (étage).

La résidence accueille 78 résidents dont 15 places d'hébergement temporaire.

📍63 avenue de Bodon, 44250 Saint-Brevin-les-Pins

1.3.2. Site des Sylphes :

Elle accueille 60 résidents présentant des troubles cognitifs, notamment la maladie d'Alzheimer et des pathologies apparentées.

📍 121 avenue de Mindin, 44250 Saint-Brevin-les-Pins

1.3.3. Site Fleur d'Ajonc :

Elle dispose de 50 places pour des personnes âgées en perte d'autonomie.

📍 206 Av. Raymond Poincaré, 44250 Saint-Brevin-les-Pins

1.3.4. Site Vent d'Ouest :

Inaugurée en 2022, la résidence Vent d'Ouest accueille 122 personnes âgées réparties sur deux niveaux.

Elle a permis de fermer le site des Cèdres concerné par la loi littorale et la montée des eaux.

📍 1 avenue Jacques Cassard, 44250 Saint-Brevin-les-Pins

II. Rappel des missions confiées

2.1. Les missions confiées

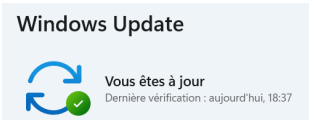
Durant le stage, diverses missions me sont confiées :

• *Gestion de parc/ Migration PC Win-10 en Win-11*
• *Ticketing (Informatique, Téléphonie)*
• *Administration serveurs (GPO, AD)*
• *Projet : Définition et déploiement d'une solution de supervision en Open Source*
• *Participation à la mise en place de mesures de cybersécurité*

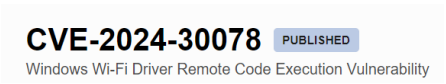
III. Missions réalisées (Outils-Difficultées-Solutions)

3.1. La Gestion du parc informatique

Il est indéniable que les mises à jour des PC sont essentielles pour garantir la sécurité, particulièrement dans les entreprises où le risque d'attaques est plus élevé.



Nous avons dû appliquer une mise à jour pour corriger une faille de sécurité majeure récemment découverte chez Microsoft, identifiée par le code CVE-2024-30078. Ce défaut dans le pilote Wi-Fi de Windows permettait à des attaquants d'exécuter du code arbitraire via des requêtes spécialement conçues.



Dans notre cas, les ordinateurs portables ont été la priorité, car certaines personnes sont amenées à travailler en télétravail et donc potentiellement à utiliser des Wifi publics ou le risque est très élevé.

J'ai pu également préparer des ordinateurs pour de nouveaux utilisateurs. Cela inclut plusieurs tâches : attribuer un nom au PC, effectuer les mises à jour nécessaires, configurer le Wi-Fi et le domaine, simplifier l'interface en ajoutant des icônes et des raccourcis URL pertinents, retirer les widgets non-essentiels, et configurer les imprimantes ainsi que la création de l'utilisateur dans l'Active Directory avec l'affection des groupes correspondants.

En collaboration avec le responsable informatique, nous avons également profité d'une coupure de courant pour retirer un switch qui n'était plus utilisé. C'est aussi une part

importante de la gestion du parc : éliminer ce qui n'est plus nécessaire ou utilisé afin d'optimiser les ressources disponibles.

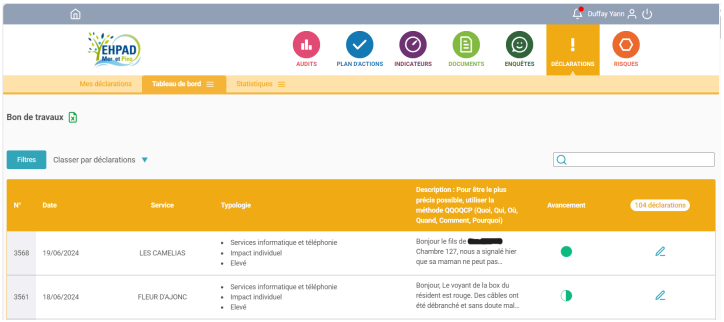
Cela permet également de mettre à jour l'inventaire du matériel et de vérifier les stocks restants. Par exemple, lorsque je devais remplacer une tablette, je mettais à jour le fichier Excel correspondant.

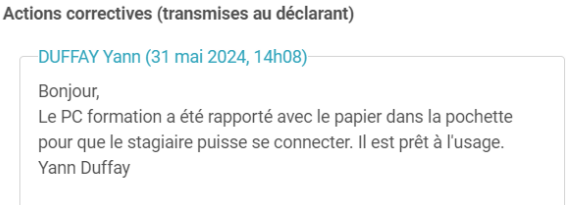
Enfin, régulièrement, lors de nos visites dans les résidences, nous vérifions si les machines peuvent être mises à niveau vers Windows 11. Nous établissons une liste de celles qui sont éligibles pour la mise à jour et nous examinons les options pour celles qui ne le sont pas. Le support de Windows 10 prendra fin en octobre 2025 c'est pourquoi il faut anticiper un maximum.

3.2. Le Ticketing

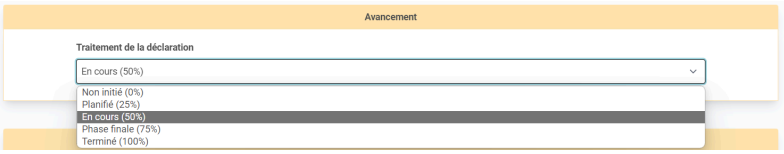
Tout d'abord le ticketing désigne un système de gestion des demandes de support et des incidents. Pour ce faire, le service informatique a mis en place l'outil **Agéval.**

Il promeut une démarche d'amélioration de la qualité et de la gestion des risques





La plateforme permet de répondre à la demande de l'utilisateur en lui permettant de lui indiquer l'avancement de son ticket.



Pendant les quatre premières semaines, j'ai effectué diverses interventions dans les différentes résidences pour répondre aux demandes des utilisateurs.

Ces interventions incluaient des :

- ☐ **Dysfonctionnements matériels** : Tablette cassée, Chargeur lent, Pile défectueuse.
- ☐ **Problèmes liés à la connectivité** : Signal borne, Perte de réseau après veille.
- ☐ **Problèmes de configuration** : Drivers Obsolète, Imprimante.
- ☐ **Dysfonctionnements Logiciels** : Document Word, Ouverture PDF.
- ☐ **Demandes nouveaux utilisateurs :** Création boite mail, répertoire, Configuration PC.

Exemple : Perte de réseau après une sortie de veille

Contexte

Lors de l'ouverture d'une session sur un PC fixe après une utilisation précédente, l'utilisateur constate une perte de connexion au réseau, le forçant à redémarrer son ordinateur. Ce problème se manifeste de manière aléatoire : certains jours, tout fonctionne sans incident, puis soudain, le problème réapparaît sans préavis.

Difficulté rencontrée

Des solutions avaient déjà été mises en place sans succès. Pour ma part, j'ai tenté plusieurs ajustements de paramètres, notamment en empêchant l'ordinateur de désactiver la carte réseau pour économiser de l'énergie. Pendant 10 jours, le problème ne s'est pas manifesté, ce qui laissait penser que la solution était efficace. Cependant, au 11e jour, la perte de connexion au réseau s'est de nouveau produite.

Solution apportée

Une solution plus radicale consistait à ajouter une carte Wi-Fi au PC pour utiliser une connexion sans fil, ce qui a permis de résoudre le problème en évitant l'utilisation du câble Ethernet. L'utilisateur ne devrait plus perdre la connexion désormais. Il reste à vérifier si cette solution est durable dans le temps.

3.3. Le déploiement d'une solution de supervision en Open Source

L'objectif est de mettre en place un outil de supervision en Open Source en récupérant les logs* des machines (serveurs, clients) afin de pouvoir les analyser et les visualiser sur une interface web.

Un "log" (ou "journal d'événements" en français) est un fichier qui enregistre de manière chronologique les actions, les événements ou les informations importantes qui se produisent dans un système informatique ou sur un réseau.

Outil	*Graylog*

Pourquoi avoir choisi Graylog ?

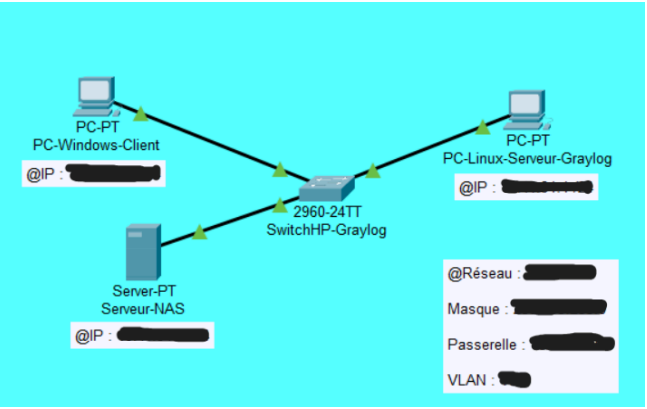
Graylog est une solution **gratuite** et **open source** qui offre des **capacités avancées** pour l'analyse et la recherche des logs. Grâce à ses fonctionnalités, il permet de **générer des tableaux de bord** personnalisés et des **visualisations graphiques**, facilitant ainsi la compréhension des tendances, la détection des anomalies et la réponse rapide aux incidents.

Rufus 4.5.2180

Avant de commencer, j'ai débuté en partant de zéro en créant une clé bootable à l'aide de Rufus, un utilitaire gratuit et open source conçu pour formater et créer des médias USB démarrables à partir d'images ISO. Étant habitué à Debian 12, j'ai opté pour cet OS.

Bien sûr, avant de déployer cette solution à grande échelle, il est essentiel de la tester dans un environnement de **laboratoire**. C'est un environnement où les configurations matérielles et logicielles sont testées pour vérifier leur fonctionnement ou leur compatibilité.

Schéma réseau du lab



Après avoir installé le serveur de logs à l'aide de sources spécifiques, il était nécessaire de trouver un moyen de récupérer les logs d'une machine cliente, une tâche qui n'est pas simple à première vue.

En cherchant, l'**agent NXLog** est une bonne solution. Cet agent dispose d'un fichier de configuration (.conf) que nous pouvons configurer pour envoyer les logs au serveur de logs, en spécifiant l'IP, le port, etc.

Pour améliorer la précision des logs, notamment dans le domaine de la sécurité, nous avons combiné NXLog avec Sysmon.

```
# Collecte des journaux Sysmon
<Input sysmon>
    Module      im_msvistalog
    Query       <QueryList>\
                    <Query Id="0">\
                        <Select Path="Microsoft-Windows-Sysmon/
                        Operational">*</Select>\
                    </Query>\
                </QueryList>
</Input>
```

Il a suffi d'ajouter une section Sysmon dans le fichier de configuration de NXLog pour intégrer ces logs qui permettront de tracer les éventuelles activités malveillantes.

Après avoir déployé cet agent sur notre machine Windows cliente et vérifié que les logs remontaient correctement sur notre serveur Graylog, avec une visualisation adéquate sur l'interface web,j'ai rencontré une difficulté.

Difficulté rencontrée

Lors de la récupération des logs d'une autre machine cliente, il était compliqué de déterminer à quelle machine ces logs appartenaient.

Solution apportée

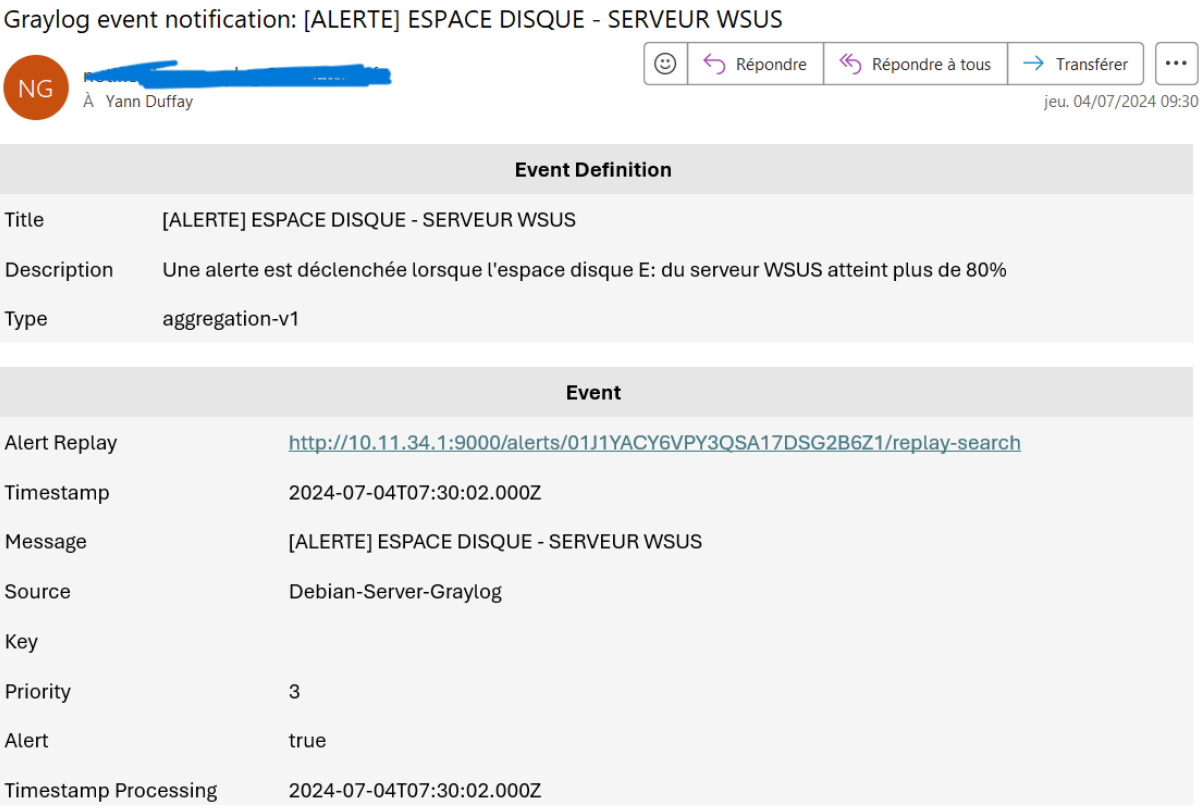
Pour résoudre ce problème, j'ai trouvé une solution : il a suffi de modifier à nouveau notre fichier de configuration NXLog en ajoutant une ligne de code permettant de récupérer le nom de la machine en tant que source.

```
Exec  $Hostname = hostname();
```

Nous souhaitions également surveiller l'espace de stockage du disque du serveur WSUS, qui distribue les mises à jour des produits Microsoft sur les postes de travail et les serveurs. Après avoir consulté les logs, j'ai constaté qu'aucun d'entre eux ne fournissait cette information.

Pour résoudre ce problème, j'ai créé un script PowerShell qui mesure l'espace disque et génère un log lorsque celui-ci dépasse 80% de sa capacité. Grâce à Graylog, nous pouvons créer des alertes basées sur ces logs. Ainsi, lorsque ce log spécifique est reçu par Graylog, une alerte est déclenchée et nous recevons un email pour nous avertir que l'espace disque de notre serveur WSUS a dépassé les 80%.

Pour automatiser l'exécution du script PowerShell, j'ai créé une tâche planifiée qui exécute le script à une heure définie.



Graylog event notification: [ALERTE] ESPACE DISQUE - SERVEUR WSUS

NG [redacted]

À Yann Duffay

Répondre | Répondre à tous | Transférer | ...

jeu. 04/07/2024 09:30

Event Definition	
Title	[ALERTE] ESPACE DISQUE - SERVEUR WSUS
Description	Une alerte est déclenchée lorsque l'espace disque E: du serveur WSUS atteint plus de 80%
Type	aggregation-v1

Event	
Alert Replay	http://10.11.34.1:9000/alerts/01J1YACY6VPY3QSA17DSG2B6Z1/replay-search
Timestamp	2024-07-04T07:30:02.000Z
Message	[ALERTE] ESPACE DISQUE - SERVEUR WSUS
Source	Debian-Server-Graylog
Key	
Priority	3
Alert	true
Timestamp Processing	2024-07-04T07:30:02.000Z

IV. Bilan global Stage

Points forts

En ce qui concerne mes points forts, je suis autonome lorsqu'il s'agit de mener à bien des missions. Je me sens à l'aise pour aller voir les utilisateurs sur place et résoudre les problèmes techniques qu'ils rencontrent. Je fais de mon mieux pour persévérer face aux difficultés.

Ce que j'aurais dû faire différemment

En rétrospective, j'aurais pu améliorer ma gestion du temps pour être plus efficace sur certaines tâches, en établissant des priorités de manière plus stratégique. De plus, il aurait été essentiel d'assurer une sauvegarde systématique des configurations avant toute modification ,afin de pouvoir revenir en arrière si nécessaire et ainsi être prêt à réagir rapidement en cas de problème après une modification.

Ce que je peux améliorer pour le prochain stage

Pour mon prochain stage, je souhaite développer mes compétences en cybersécurité afin d'apporter une perspective innovante et de proposer de nouvelles solutions en explorant les possibilités disponibles dans ce domaine.

Ce qu'il reste à faire

Il reste à approfondir le projet de supervision en Open Source, Graylog, qui est encore incomplet. Je suis particulièrement intéressé par les nombreuses fonctionnalités que je n'ai pas encore eu l'occasion d'explorer et que je souhaite développer davantage.