Antonin
BARATEAU

2024-2025
BTS SIO SISR

Rapport de stage
DU 02/06/2025 Au 04/07/2025

Communauté de communes Mellois en Poitou

Sommaire

01 - Introduction

02 - Présentation de l’entreprise

03 - Présentation du service d'accueil

04 - Cahier des charges

05 - Présentation de la démarche

06 - Présentation de la solution technique

07 - Bilan du projet et conclusion

08 - Présentation de la solution technique

09 - Conclusion

Introduction

Afin de clôturer notre première année de **BTS S**ervices **I**nformatique aux **O**rganisations, nous avons été amenés a réalisé une période en milieu professionnel du 02/06/2025 au 04/07/2025.

Pour ma part, j'ai réalisé cette période de stage chez la Communauté de communes Mellois en Poitou, au sein de leur service **DSI** (**D**irection des **S**ystèmes d'**I**nformation), en administration réseaux. Là-bas, j'ai pu effectuer des missions de configuration de switch, répondre à des demandes utilisateur, faire une recherche de logiciel syslog et les tester .

Pour la répartition des tâches, l'entreprise utilise un outil de ticketing nommé GLPI. Ce dernier proposé une interface séparant les demandes d'assistance en 4 catégorie :

- À traiter
- En cours de traitement
- En pause
- En attente

Les tâches sont ensuite distribuées en fonction des demandes des utilisateurs, pour l'administration réseaux, il s'occupe de tout ce qui est en lien avec l'infrastructure réseaux, comme des tâches de création d'utilisateur dans Active directory ou la maintenance des serveurs.

Je remercie la DSI de m'avoir pris en stage plus particulièrement le directeur de la DSI Jérôme [redacted], mon tuteur de stage kellian [redacted] pour m'avoir accompagné tout au long de ces 5 semaines.

Présentation de l'entreprise

Information générale

- Nom de l'entreprise : Communauté de communes Mellois en Poitou
- Siège social : 2 Place de Strasbourg, 79500 Melle
- Date de création : 1er Janvier 2017

Histoire de la Communauté de communes

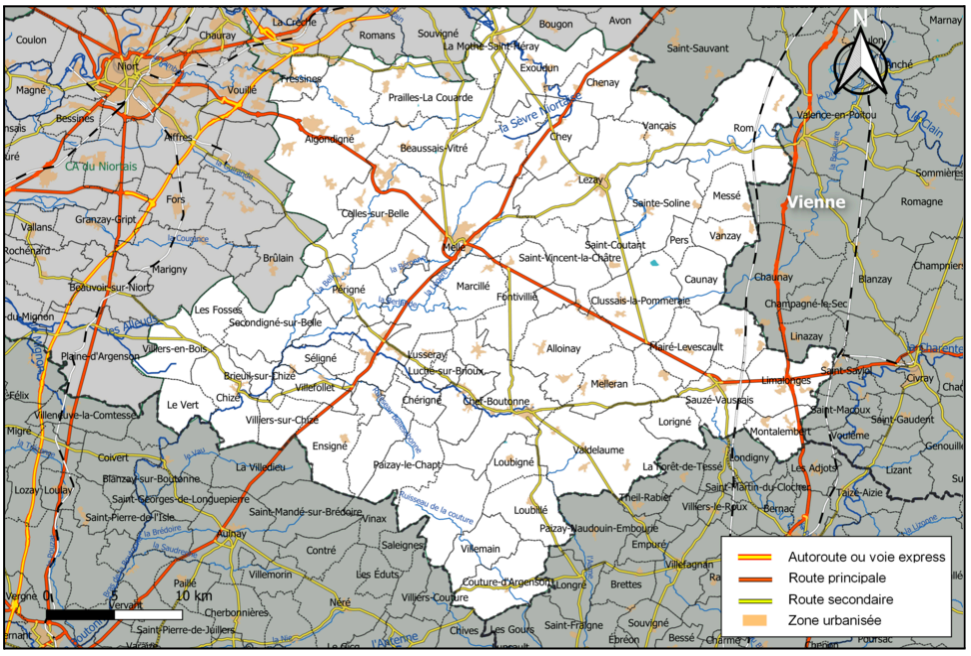
- Par arrêté préfectoral, depuis le 1er janvier 2017, a été créée la communauté de communes issue de la fusion de la communauté cantonale de Celles-sur-Belle, des communautés de communes Cœur du Poitou, du Mellois, et Val de Boutonne, du syndicat mixte du pays Mellois, du syndicat Mellois des piscines, du syndicat SICTOM de Loubeau. Le 1er janvier 2018, le syndicat d'assainissement du Mellois fusionne avec la communauté de communes.

Elle compose en 2018 :

- 62 communes au 1er janv. 2019 par la création de communes nouvelles
- 107 conseillers communautaires
- 1 000 conseillers municipaux
- 48 168 habitants
- 1 283,4 km2
- 37,5 habitants/km

* informations au 31 décembre 2018

Carte du territoire au 1er janvier 2019

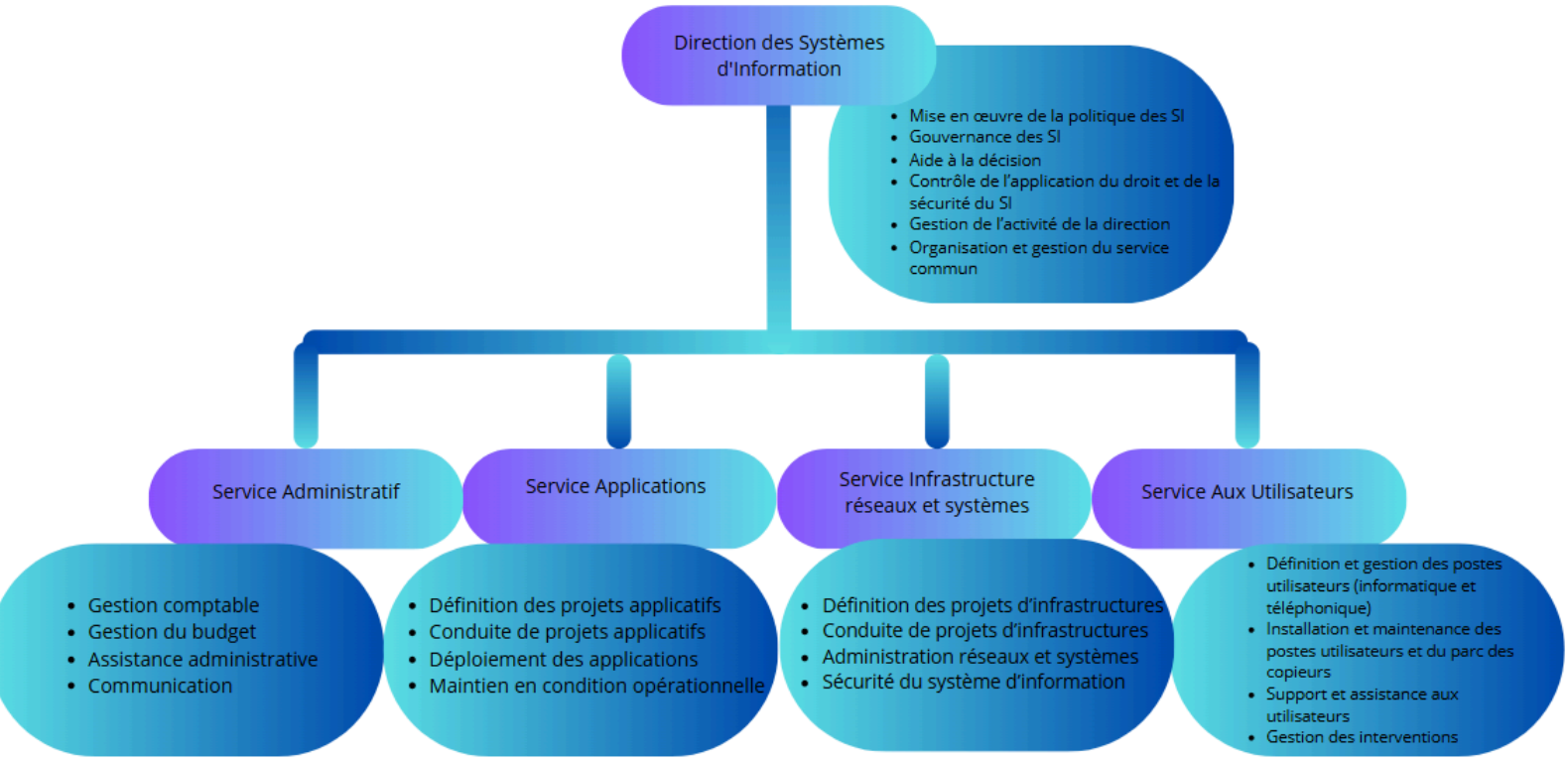


Présentation du service d'accueil

La DSI (Direction des Systèmes d'Information) a pour but de gérer

- Les tickets des utilisateurs en cas de panne ou de demande
- La maintenance des infrastructure réseau
- Coordonner les projets informatique
- Gestion du parc informatique
- La conformité au RGPD

Elle est composée de quatre services. Le service administratif, le service applications, le service infrastructure et réseaux, le service utilisateur, chaque service a un rôle spécifique à la DSI.



Cahier des charges

Présentation de la situation existante

- Avant le début du projet, l'entreprise avait des difficultés liées à la gestion et à l'exploitation des logs générés par ses différents équipements. Chaque appareil produisait ses propres logs, ce qui compliquait leur accès pour leur analyse.

  En cas d'incident de sécurité ou de dysfonctionnement, il était difficile et chronophage de retrouver les informations pertinentes.

Présentation des résultats à obtenir

- L'objectif principal du projet était de fournir à l'entreprise une solution efficace et fiable pour la centralisation des logs provenant de ses différents équipements réseau.Cette solution devait permettre à l'entreprise de mieux exploiter les données issues de son infrastructure, afin d'améliorer la supervision, la réactivité face aux incidents, ainsi que la traçabilité des événements.

  L'entreprise attendait les résultats suivants :
  - Une centralisation des logs
  - Une amélioration de la visibilité

  À travers la mise en place de cette solution, l'entreprise visait donc une optimisation globale de sa supervision système, toute en assurant sa conformité au RGPD sur la conservation des données, par exemple les logs des wifi publiques

Présentation de la démarche suivie

Liste des fonctionnalités attendues

- Dans le cadre du projet de centralisation des logs, l'entreprise attendait que la solution mise en place offre les fonctionnalités suivantes :

  Collecte centralisée des logs

  - Réception des journaux système provenant de différents équipements réseau

  Filtrage et tri des logs

  - Mise en place de règles de filtrage personnalisées selon les besoins de supervision.

  Interface d'administration et de visualisation

  - Tableau de bord ergonomique permettant une visualisation claire des événements.

  Conformité RGPD

  - Respect des délais de conservation imposés par la réglementation.

Description des données

- Dans le cadre du projet, les données traitées sont essentiellement des logs générés par les équipements réseau de l'entreprise. Ces logs sont des fichiers ou messages contenant des informations sur les événements survenant au sein des systèmes.

Les logs sont générés par :

Des serveurs
Des équipements réseau
Des points d'accès Wi-Fi

Présentation de la solution technique

Choix de la solution

Afin de sélectionner la solution la plus adaptée aux besoins de l'entreprise, j'ai réalisé une étude comparative des principaux outils disponibles, puis je les ai présentés à mon tuteur, qui a choisi celui qui correspondait le mieux.

Logiciel	OS	Caractéristiques principales	Inconvénients	Log pris en charge	Lecture log	Configuration requise (recommandée)
Graylog	Debian	Interface graphique, Centralisation des logs, alertes et tableaux de bord, difficultés moyen d'installation	Nécessite plusieur composants (mongoDB, Opensearch,	Syslog(Linux, équipements réseau, pare-feu), Windows Event logs	Lecture facile	Processeur 4 cœurs, 8 Go de RAM
logAnalyzer	Debian, Ubuntu	Interface graphique, Centralisation des logs, facile d'installation, Collecte et analyse des journaux d'événemen, Recherche et filtrage	Nécessite une base de données MySQL pour stocker les logs.	Syslog(Linux, équipements réseau, pare-feu), Windows Event logs	Lecture difficiles	Processeur 4 cœurs, 16 Go de RAM
Kibana	debian	Interface graphique, filtrage des logs, Centralisation des logs	Nécessite Elasticsearch et Logstash	Syslog(Linux, équipements réseau, pare-feu), Windows Event logs	Lecture facile	Processeur 4 cœurs, 8 Go de RAM
Fluentd	debian	Interface graphique avec Fluentel, filtrage des logs, Centralisation des logs, Extensible avec des plugins, Supporte le chiffrement et compression	Nécessite une configuration initiale. Peut être gourmand en ressources selon le volume de logs	Prend en charge Syslog, fichiers journaux, API, bases de données, etc.	Lecture difficiles	Processeur 4 cœurs, 8 Go de RAM
FortiSIEM	CentOS	Interface graphique, Centralisation des logs, alertes et tableaux de bord, Analyse avencée	Complexité de configuration, cout élevé, Nécessite une infrastructure robuste pour fonctionner efficacement	Prend en charge Syslog, fichiers journaux, API, bases de données,SNMP, WMI, etc.	Lecture facile	Processeur 8 cœurs, 32 Go de RAM

Installation et configuration

j'ai donc commencé par installer graylog sous debian 12

- la première étape est d'installer debian sous une VM pour ca prendre l'ISO par exemple sur https://www.debian.org/download

- La deuxième étape est de mettre à jour le debian avec la commande
sudo apt update && sudo apt upgrade -y

Installation des différents logiciel

Étape 1 : Installer Java OpenJDK 17

Graylog nécessite Java 17 pour fonctionner.

```
sudo apt install openjdk-17-jre-headless -y
```

Vérifie la version :

```
java -version
```

Étape 2 : Installer MongoDB

MongoDB est la base de données utilisée par Graylog.

1. Ajouter la clé GPG officielle MongoDB :

```
curl -fsSL https://pgp.mongodb.com/server-6.0.asc | sudo tee
/usr/share/keyrings/mongodb-server-6.0.gpg > /dev/null
```

2. Ajouter le dépôt MongoDB pour Debian 12 :

```
echo "deb [signed-by=/usr/share/keyrings/mongodb-server-6.0.gpg]
https://repo.mongodb.org/apt/debian bookworm/mongodb-org/6.0 main" | sudo tee
/etc/apt/sources.list.d/mongodb-org-6.0.list
```

3. Mettre à jour la liste des paquets et installer MongoDB :

```
sudo apt update
sudo apt install -y mongodb-org
```

4. Démarrer et activer MongoDB :

```
sudo systemctl start mongod
sudo systemctl enable mongod
```

Étape 3 : Installer Elasticsearch

Elasticsearch est le moteur de recherche utilisé par Graylog.

1. Importer la clé GPG d'Elasticsearch :

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo tee
/usr/share/keyrings/elasticsearch-keyring.gpg > /dev/null
```

2. Ajouter le dépôt Elasticsearch :

```
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg]
https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee
/etc/apt/sources.list.d/elastic-8.x.list
```

3. Mettre à jour et installer Elasticsearch :

```
sudo apt update
sudo apt install elasticsearch -y
```

Configurer Elasticsearch (modifier le fichier/etc/elasticsearch/elasticsearch.yml)

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

Ajoute/modifie ces lignes pour permettre à Elasticsearch d'écouter en local :

```
network.host: 127.0.0.1
discovery.type: single-node
```

5. Démarrer et activer Elasticsearch :

```
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
sudo systemctl start elasticsearch.service
```

6. Vérifier qu'Elasticsearch fonctionne :

```
curl -X GET "localhost:9200"
```

Étape 4 : Installer Graylog

1. Importer la clé GPG Graylog :

```
wget https://packages.graylog2.org/repo/packages.graylog-4.4-repository_latest.deb
sudo dpkg -i packages.graylog-4.4-repository_latest.deb
sudo apt update
```

2. Installer Graylog :

```
sudo apt install graylog-server -y
```

Étape 5 : Configurer Graylog

1. Générer un secret pour le mot de passe :

```
pwgen -N 1 -s 96
```

2. Ouvrir le fichier de configuration /etc/graylog/server/server.conf :

```
sudo nano /etc/graylog/server/server.conf
```

3. Modifier et ajouter ces paramètres :

password_secret : Coller la clé générée par pwgen

root_password_sha2 : Générer le hash du mot de passe admin avec la commande : echo -n "ton_mot_de_passe_admin" | sha256sum

Et coller le hash dans root_password_sha2.

Vérifier que MongoDB et Elasticsearch sont configurés avec :

mongodb_uri = mongodb://localhost:27017/graylog

elasticsearch_hosts = http://127.0.0.1:9200

Étape 6 : Démarrer Graylog

```
sudo systemctl daemon-reload
sudo systemctl enable graylog-server.service
sudo systemctl start graylog-server.service
```

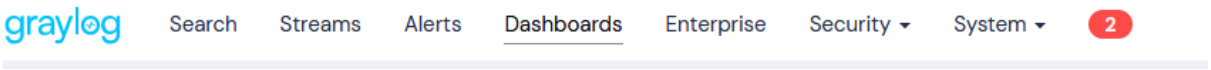
Étape 7 : Accéder à l'interface Web

- Ouvrire un navigateur et va à :

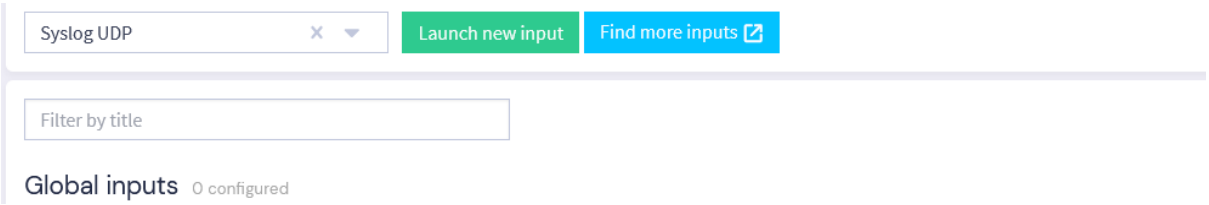
http://IpDuServeur:9000/

Configuration de graylog

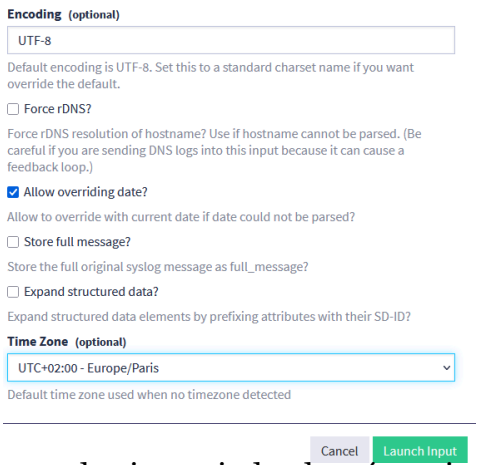
- Une fois Graylog installé, il est nécessaire de le configurer pour qu'il puisse recevoir les logs, nous allons configurer les input en haut aller dans system puis input.



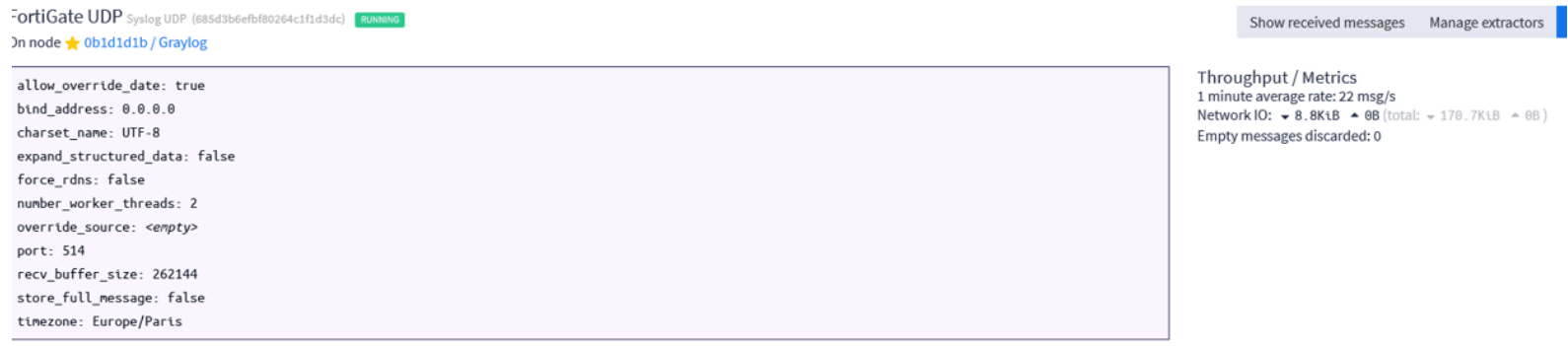
- Ensuite dans la barre de recherche, rechercher Syslog UDP puis cliquez sur launch new input



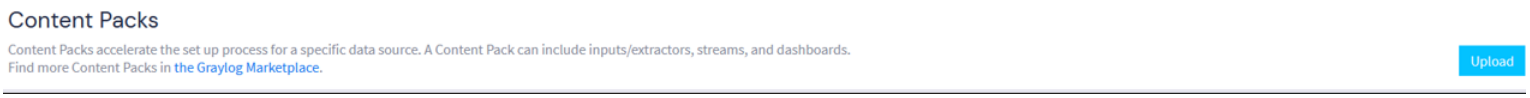
- Dans les paramètres title : FortiGate UDP, Bind address : 0.0.0.0, Port : 514

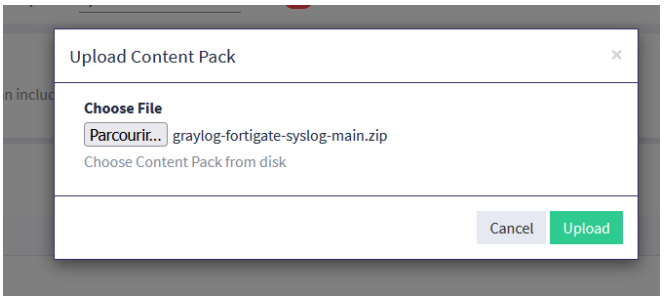


- Une fois cela fait vous devriez avoir des données qui transite dans Network IO si votre pare-feu est bien configurer

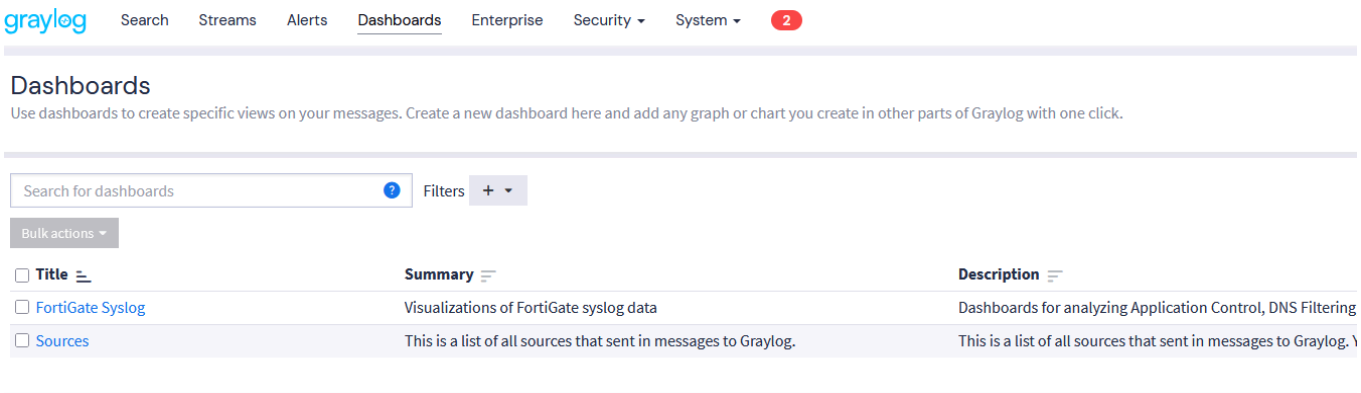


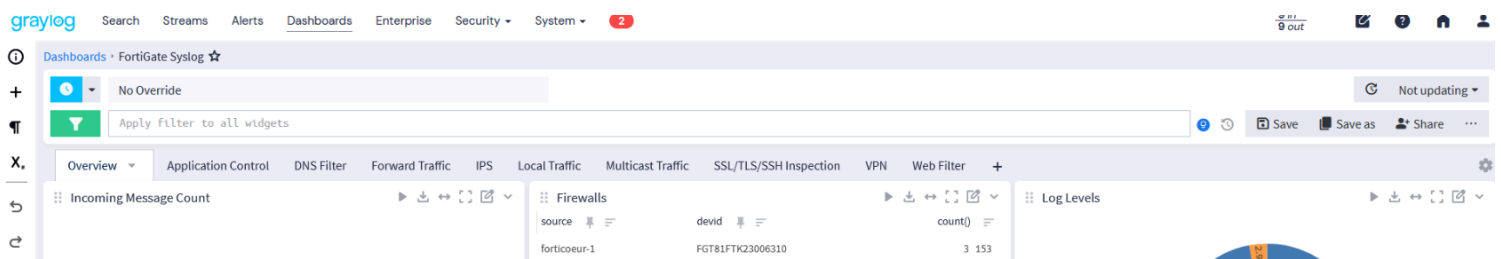
- Ensuite nous allons importer un dashboard pour une meilleur visibilité des logs, pour cela aller dans system puis content pack upload, parcourir et sélectionner le fichier installer sur [github](#) et Upload





- Ensuite aller dans dashboard et vous devriez voire le dashboard apparaître cliquez dessus et vous verrez les logs du pare-feu





Conclusion

Ce stage m'a permis de découvrir concrètement le fonctionnement des logs systèmes et des solutions de centralisation comme Syslog. En participant à la mise en place d'un serveur de collecte des logs, j'ai pu appliquer et mettre en pratique des connaissances théoriques acquises au cours de ma formation, notamment en réseau, en administration système et en sécurité.

Ce projet m'a aidé à mieux comprendre l'importance de la supervision dans une infrastructure informatique, ainsi que les enjeux liés à la traçabilité et à la conformité (notamment vis-à-vis du RGPD). Ce fut une expérience enrichissante qui a renforcé mon intérêt pour les métiers techniques liés aux systèmes et réseaux.