

<b>DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE</b>		<b>N° réalisation :2</b>
<b>Nom, prénom :</b> FRELAUT Raphaël		<b>N° candidat :</b> 02441695738
<b>Épreuve ponctuelle</b>		<b>Date :</b> ..... / ..... / .....
<b>Organisation support de la réalisation professionnelle</b>		
<b>Intitulé de la réalisation professionnelle</b> Mise en place d'une solution de centralisation de logs		
<b>Période de réalisation :</b> 2024 - 2025 <b>Lieu :</b> Lycée Elie Vinet - Barbezieux Saint Hilaire <b>Modalité :</b> Seul		
<b>Compétences travaillées</b> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau</li> <li><input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau</li> <li><input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau</li> </ul>		
<b>Conditions de réalisation<sup>1</sup> (ressources fournies, résultats attendus)</b> <ul style="list-style-type: none"> <li>• Mise en place d'un serveur GrayLog</li> <li>• Analyse et réception des logs des machines clientes</li> <li>• filtres des logs pour analyse</li> <li>• Envoi d'alertes sur discord</li> </ul>		
<b>Description des ressources documentaires, matérielles et logicielles utilisées<sup>2</sup></b> <ul style="list-style-type: none"> <li>• Machine virtuelles sous Proxmox/VmWare</li> <li>• Maquettage sous Packet Tracer</li> <li>• Un switch reliant les hyperviseurs</li> <li>• Poste client sous Windows 10</li> </ul>		
<b>Modalités d'accès aux productions<sup>3</sup> et à leur documentation<sup>4</sup></b> <ul style="list-style-type: none"> <li>• Accès aux maquettes via VPN sur le routeur PfSense</li> <li>• Documentation accessible depuis l'onglet projet sur le portfolio et sur le classroom <ul style="list-style-type: none"> <li>○ <a href="https://drive.google.com/drive/folders/1cHvN-synAVMzsUgp6trw08n9-66vkYvF?usp=sharing">https://drive.google.com/drive/folders/1cHvN-synAVMzsUgp6trw08n9-66vkYvF?usp=sharing</a></li> </ul> </li> </ul>		

<sup>1</sup> En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

<sup>2</sup> Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

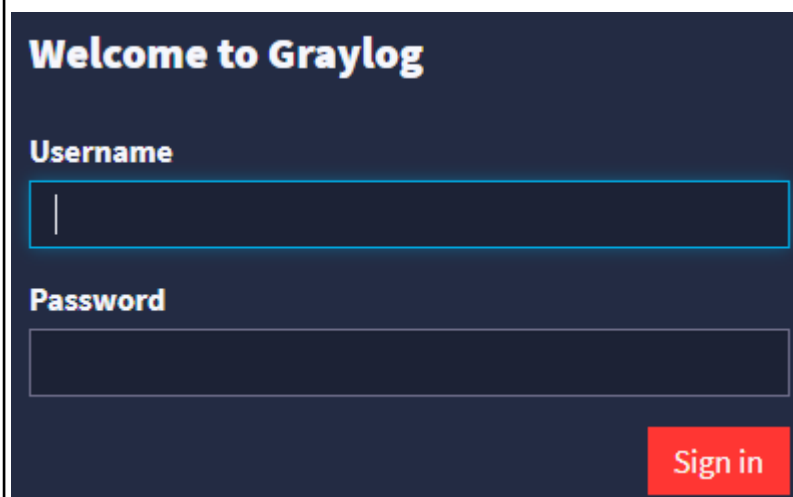
<sup>3</sup> Conformément au référentiel du BTS SIO « Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve. ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

<sup>4</sup> Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

## Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

1. Préparation de la machine
  - a. Installation des paquets Graylog
  - b. Emplacement dans le réseau
  - c. Choix des logs à recevoir
2. Configuration des logs
  - a. Installation des redirections de logs sur les machines cibles
  - b. Configuration du serveur Graylog
3. Mise en place des alertes
  - a. Création d'un serveur discord
  - b. Configuration des événements
    - i. Connexion à l'AD
    - ii. Connexion ssh sur un serveur
    - iii. Connexion VPN
    - iv. Connexion à l'interface web pfSense
  - c. Configuration des alertes en fonction des événements
4. Supervision et dépannage
  - a. Vérification de la bonne exécution des alertes
  - b. Ajout de paramètres supplémentaires dans les alertes
  - c. vérification au bon fonctionnement de la machine Debian

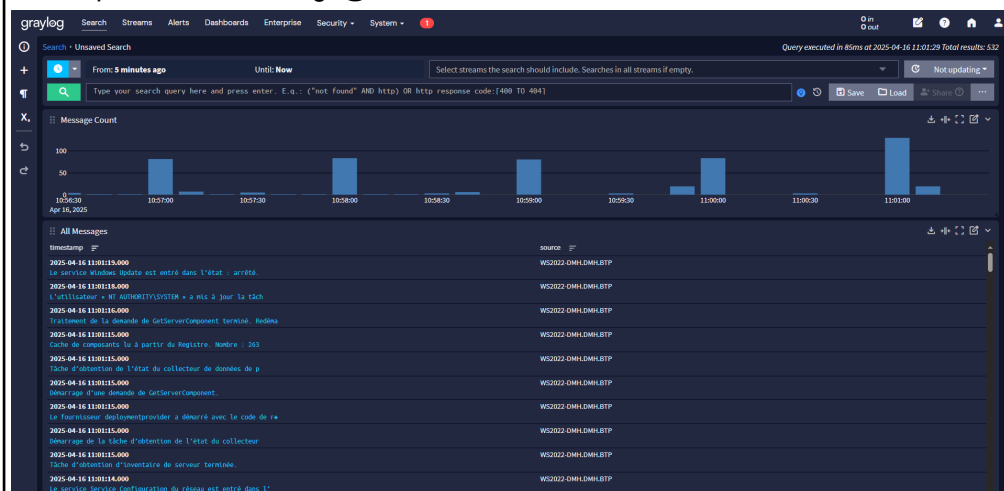
Menu d'interface :



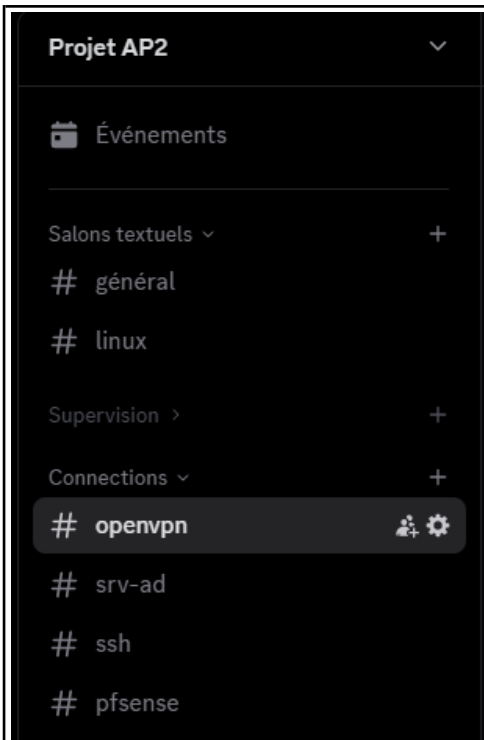
The image shows the Graylog login interface. It has a dark blue background with the text 'Welcome to Graylog' in a large, white, sans-serif font. Below this, there are two input fields: 'Username' and 'Password', both with white text and a light blue border. To the right of the 'Password' field is a red button with the text 'Sign in' in white. The interface is clean and modern.

login : admin

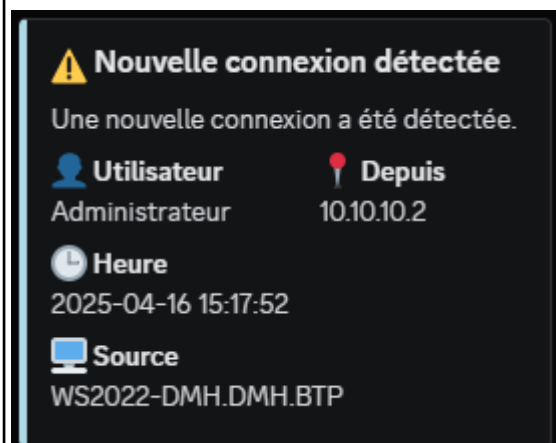
mot de passe : PuitsDeLogs@



Les alertes sont envoyées dans un serveur discord :



Les channels permettent le trie des logs pour une meilleure lisibilité.



Les inputs sont configurés en UDP :

- port 12222 → toutes les machines windows via NXLOG
- port 12514 → toutes les machines Linux via RSYSLOG
- port 5555 → spécialement pour Suricata

Graylog\_UDP\_NXLogs\_Windows
GELF UDP (87e4104198ac3d251908dca3)
RUNNING

Show received messages
Manage extractors
Stop input
More actions

On node ★ bc53f8d8 / Graylog

```

bind_address: 0.0.0.0
charset_name: UTF-8
decompress_size_limit: 8388608
number_worker_threads: 1
override_source: <empty>
port: 12222
recv_buffer_size: 262144

```

Throughput / Metrics

1 minute average rate: 2 msg/s
Network IO: ▼ 0B ▲ 0B (total: ▼ 93.4MiB ▲ 0B)
Empty messages discarded: 0

---

Graylog\_UDP\_RAW\_suricata
Raw/Plaintext UDP (67f9ef8a36ce5b4c45709c50)
RUNNING

Show received messages
Manage extractors
Stop input
More actions

On node ★ bc53f8d8 / Graylog

```

bind_address: 0.0.0.0
charset_name: UTF-8
number_worker_threads: 1
override_source: <empty>
port: 5555
recv_buffer_size: 1048576

```

Throughput / Metrics

1 minute average rate: 0 msg/s
Network IO: ▼ 0B ▲ 0B (total: ▼ 148.9KiB ▲ 0B)
Empty messages discarded: 0

---

Graylog\_UDP\_Rsyslog\_Linux
Syslog UDP (87dbdfdf1686b44324688e83)
RUNNING

Show received messages
Manage extractors
Stop input
More actions

On node ★ bc53f8d8 / Graylog

```

allow_override_date: true
bind_address: 0.0.0.0
charset_name: UTF-8
expand_structured_data: false

```

Throughput / Metrics

1 minute average rate: 0 msg/s
Network IO: ▼ 0B ▲ 0B (total: ▼ 1.5MiB ▲ 0B)
Empty messages discarded: 0