DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	N° réalisation : 1
Nom, prénom : Manguilesy Corentin	**N° candidat : 02149906117**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date : 15/04/2025**

Organisation support de la réalisation professionnelle

KaflaSoie est une entreprise réunionnaise spécialisée dans la fabrication et la vente de textiles haut de gamme, avec une attention particulière portée à la production de tissus de luxe et à l'utilisation de matières premières de qualité supérieure. Fondée à La Réunion, l'entreprise se distingue par son mélange de savoir-faire traditionnel et d'innovation, visant à offrir des produits uniques sur le marché local et international.

Avec une croissance rapide et une équipe de plus de 100 collaborateurs répartis entre les départements production, recherche et développement, administration, et marketing, KaflaSoie souhaite moderniser son infrastructure informatique pour améliorer ses opérations et soutenir son expansion. Un des aspects clés de cette modernisation est la mise en place d'un réseau Wi-Fi sécurisé, permettant à la fois de garantir une performance optimale pour les employés et de sécuriser l'accès au réseau pour les invités, tout en segmentant ces accès pour protéger les données sensibles de l'entreprise.

Intitulé de la réalisation professionnelle
Déploiement d'une infrastructure Wi-Fi sécurisée avec segmentation avec les outils Elasticsearch et Kibana.

Période de réalisation : 15/04/2025 Lieu : Lycée Marguerite Jauzelon
Modalité : ☒ Seul(e) ☐ En équipe

Compétences travaillées

☒ Concevoir une solution d'infrastructure réseau

☒ Installer, tester et déployer une solution d'infrastructure réseau

☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation[11] (ressources fournies, résultats attendus)
Ressources fournies:

Matériel Réseau :

- Switch HP ProCurve pour la gestion des VLANs, avec ports configurés en mode access et trunk.
- Points d'accès Wi-Fi (WAP121) pour permettre la connectivité sans fil pour les employés et invités.
- Serveurs pour héberger des outils de gestion, comme Elasticsearch et Kibana pour la collecte et la visualisation des logs.
- Câblage réseau (Ethernet CAT6 ou supérieur) pour connecter les équipements.
- Logiciels :
- Elasticsearch pour la collecte et l'indexation des logs des équipements réseau (switches, points d'accès, etc.).
- Kibana pour visualiser et analyser les logs en temps réel

Résultats attendus :
-Sécurisation des données sensibles: Données personnelles des employés et clients : Informations personnelles telles que les noms, adresses, numéros de téléphone, e-mails, etc.

- Isolement du réseau interne et des invités : Grâce à la segmentation du réseau en VLANs, le réseau interne des employés sera totalement isolé du réseau des invités, garantissant que les informations sensibles soient protégées contre les accès non autorisés.

[1] 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.

- Sécurisation des connexions : Le réseau des employés sera protégé par des protocoles Wi-Fi avancés comme WPA3, garantissant une sécurité renforcée pour accéder aux ressources internes de l'entreprise.

-Connexion rapide et stable pour les employés : Un réseau Wi-Fi performant améliorera l'expérience des employés, facilitant l'accès aux outils de travail et à la communication interne, ce qui contribuera à augmenter la productivité et à réduire les interruptions.

-Collecte et analyse des logs : Grâce à Elasticsearch, tous les logs générés par les points d'accès Wi-Fi, switches, routeurs et autres équipements réseau seront collectés et indexés pour une analyse rapide et efficace.

-Détection d'anomalies et incidents de sécurité : Elasticsearch et Kibana permettront de détecter rapidement toute anomalie, comme des tentatives d'intrusion ou un comportement réseau suspect. Les alertes en temps réel permettront une réponse rapide pour minimiser les risques de sécurité.

-Tableaux de bord interactifs : Kibana fournira des tableaux de bord interactifs pour visualiser en temps réel la performance du réseau Wi-Fi, la consommation de bande passante, et les événements de sécurité.

Simplification de la gestion réseau:

-Gestion centralisée : L'utilisation de VLANs pour chaque groupe d'utilisateurs (employés, invités, équipements) permet une gestion claire et centralisée du réseau, rendant l'administration plus simple et plus efficace.

-Surveillance automatisée : Elasticsearch centralisera les logs, permettant à l'équipe informatique de surveiller le réseau sans avoir à vérifier manuellement chaque appareil, ce qui réduit les risques d'erreur humaine et améliore l'efficacité opérationnelle.

-Audit facilité : Avec Elasticsearch et Kibana, la gestion et l'audit des activités du réseau seront considérablement améliorés. Les rapports peuvent être générés automatiquement et consultés facilement via des visualisations interactives.

Finalement ElasticSearch et Kibana permet de centraliser et d'analyser les logs des équipements réseau en temps réel, mais aussi de détecter rapidement les problèmes de sécurité et de performance, d'optimiser l'infrastructure réseau et de garantir que les accès sont contrôlés et conformes aux règles définies.

Description des ressources documentaires, matérielles et logicielles utilisées

Matériel réseau **:**

- Points d'accès Wi-Fi : Pour assurer une couverture complète et sécurisée (cisco Wap121)
- Switchs managés : Permettent la segmentation du réseau en VLANs et la gestion du trafic(2 HP Procurve 2510-24)
- 1 Serveur : Pour héberger Elasticsearch et Kibana pour l'indexation et la visualisation des logs.
- Câblage réseau : Pour relier les points d'accès, les switches et les autres équipements réseau.
- Routeurs : deux routeurs (Cisco 1941 series et 1921) a nécessaire pour effectuer le routage inter-VLAN.Ce routeur garantira que la communication entre les VLANs soit sécurisée et régulée en fonction des règles de sécurité définies.

Matériel physique:

-Ordinateur de bureau et PC portable

Services et configurations :

Services Réseau:

-Borne wifi :

- Fournir un accès Wi-Fi sécurisé et performant pour les employés et les invités.

-**Switchs managés:**

-Assurer la segmentation du réseau, gérer les VLANS et garantir une communication efficace entre les équipements réseau.

-**Routeur (pour le routage inter-VLAN)** :
-Permettre la communication sécurisée entre les VLANS.

-Création d'une IP Virtuel et HSRP par vlan pour garantir la haute disponibilité.

Services de Supervision et Sécurité:

-Elasticsearch:
-Collecte et analyse des logs pour une surveillance proactive du réseau, des performances et de la sécurité.

-Kibana:
-Visualisation des données collectées par Elasticsearch sous forme de tableaux de bord interactifs.

Modalités d'accès aux productions[22] et à leur documentation[33]
https://www.manguilesycorentin.com/ https://www.clemanet.com/hp/configuration-port.php

https://www.clemanet.com/hp/configuration-vlan.php
https://routeur.clemanet.com/routage-cisco-intervlan.php
https://routeur.clemanet.com/hsrp-cisco.php

2

1En 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.
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.

[3]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

Conception et segmentation du réseau : Le réseau a été segmenté en quatre VLANs distincts :
VLAN 10 pour les employés, avec accès complet aux ressources internes.
VLAN 20 pour les invités, avec accès limité à Internet.
VLAN 30 pour les équipements, accessibles uniquement depuis le réseau des employés.
VLAN 999 pour l'administration, dédié aux équipements critiques du réseau.

• Configuration des sous-réseaux et des adresses IP : Chaque VLAN a une plage d'adresses IP dédiée pour éviter les conflits. Par exemple, VLAN 10 utilise l'adresse réseau 192.168.1.0/27 pour les employés.

• Mise en place du Wi-Fi sécurisé avec WAP121 : La borne WAP121 offre deux SSID :
Un pour les employés(personnel) avec sécurité renforcée (WPA3).
Un pour les invités(visiteur), limité à l'accès Internet uniquement.

• Routage entre les VLANs et sécurité : Le routage inter-VLAN est configuré pour permettre un contrôle strict des communications et empêcher les invités d'accéder aux ressources internes.

• Supervision et gestion des logs : Les logs sont collectés dans Elasticsearch et visualisés avec Kibana pour surveiller la performance du réseau et détecter des anomalies ou tentatives d'intrusion.

La segmentation du réseau en plusieurs VLANs permet d'assurer une sécurité renforcée, une gestion efficace des ressources et une optimisation des performances. Chaque groupe d'utilisateurs, qu'ils soient employés, invités ou équipements, bénéficie d'un accès adapté et sécurisé, garantissant ainsi l'isolation des données sensibles. Le Wi-Fi sécurisé avec des SSID distincts pour chaque groupe d'utilisateurs assure une connexion fiable et contrôlée.

Le routage inter-VLAN a été soigneusement configuré pour garantir que seules les communications autorisées soient possibles entre les VLANs, tout en empêchant les accès non souhaités

Schéma de l'infrastructure :

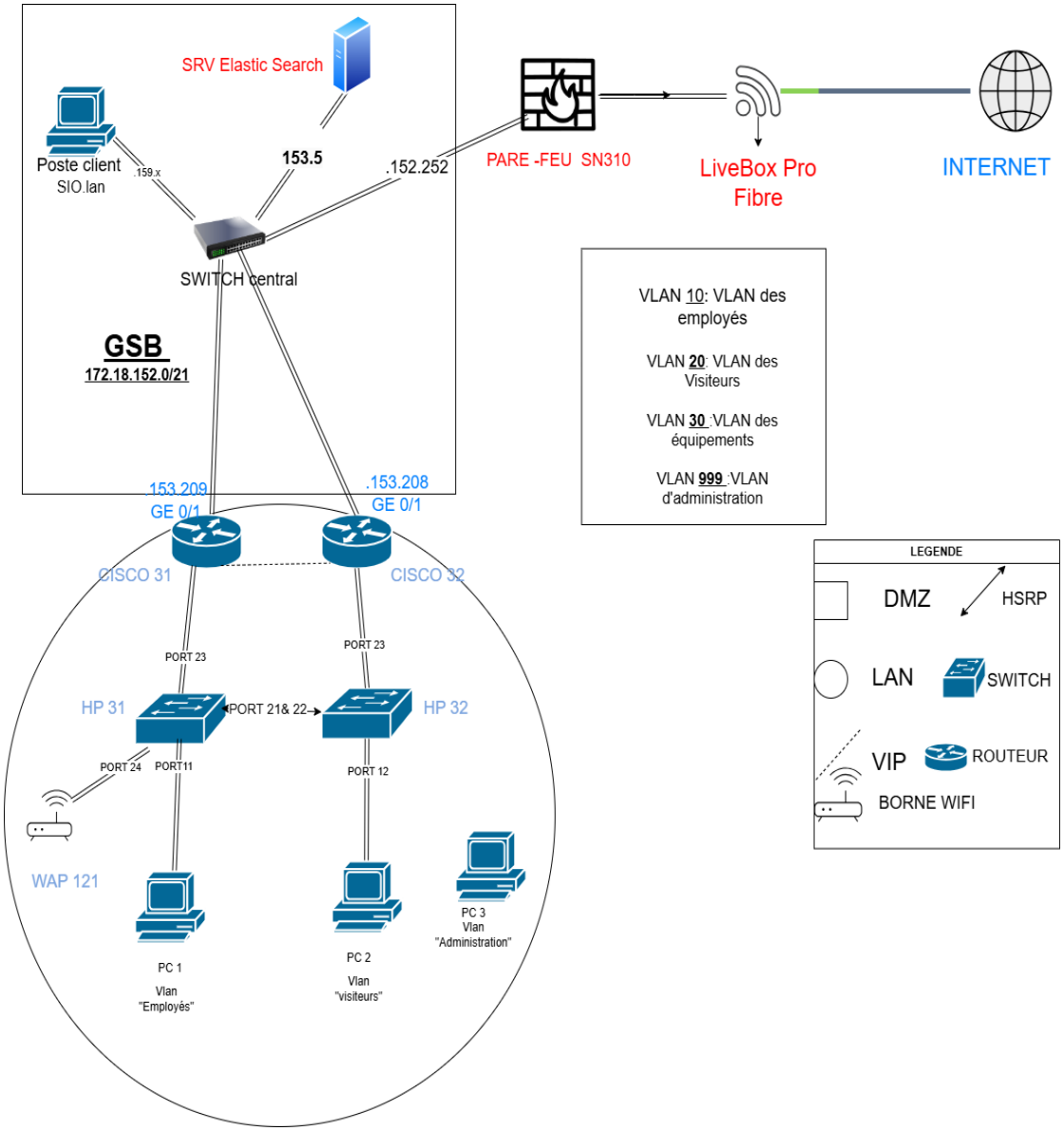
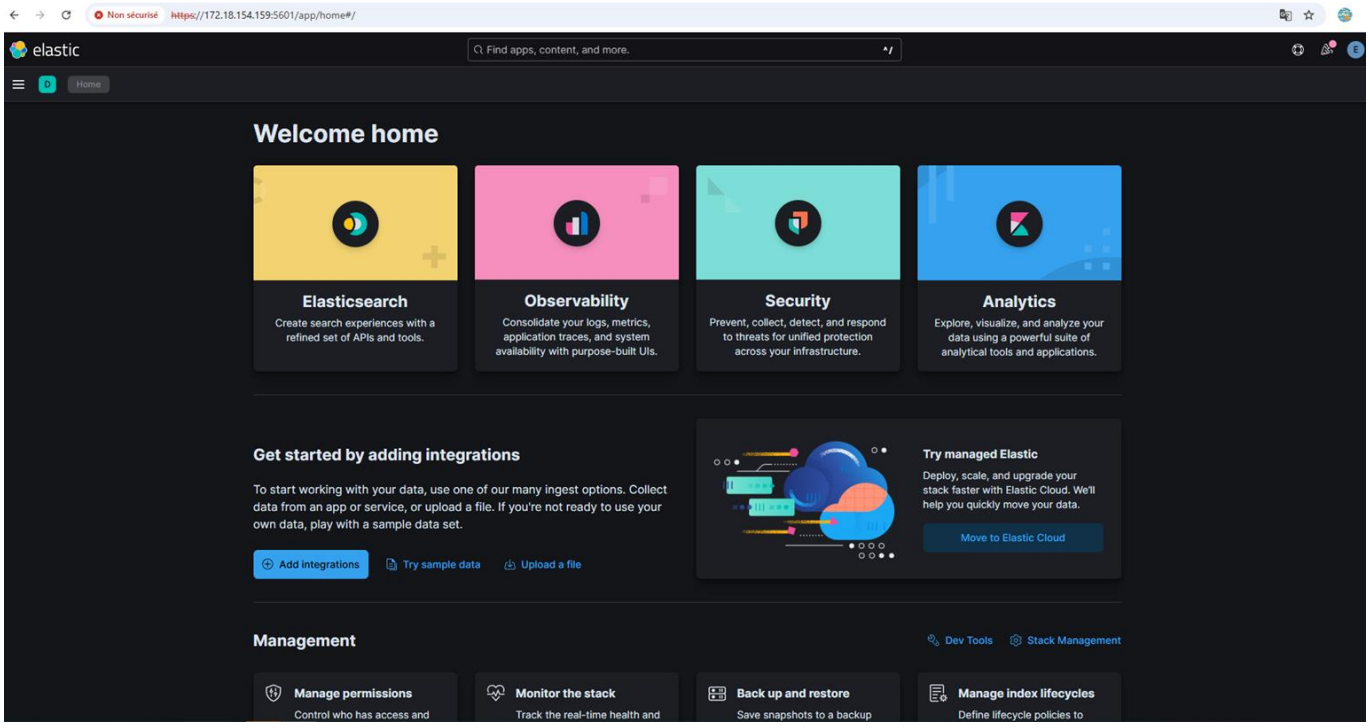


Tableau de bord elasticsearch :



Elastic Search comprend des modules intégrés :

Module intégré	Rôle
xpack.monitoring	Supervision du cluster, état des nœuds, index, performances
xpack.alerting	Création d'alertes automatiques sur erreurs ou seuils
xpack.ml (machine learning)	Détection d'anomalies réseau (flux inhabituels, pics d'erreurs)

En plus de cela j'ai installé Packetbeat qui permet de :
-Superviser le trafic réseau en temps réel, protocole par protocole.

-Identifier les communications entre hôtes (IP source/destination, ports, protocoles).

- Analyser en profondeur les échanges applicatifs (HTTP, DNS, MySQL, etc.).

- Diagnostiquer les dysfonctionnements réseau ou comportements suspects.

- Déclencher des alertes en cas d'anomalies (requêtes excessives, erreurs, pics d'activité).

Les Différents Vlans ainsi que leurs configurations :

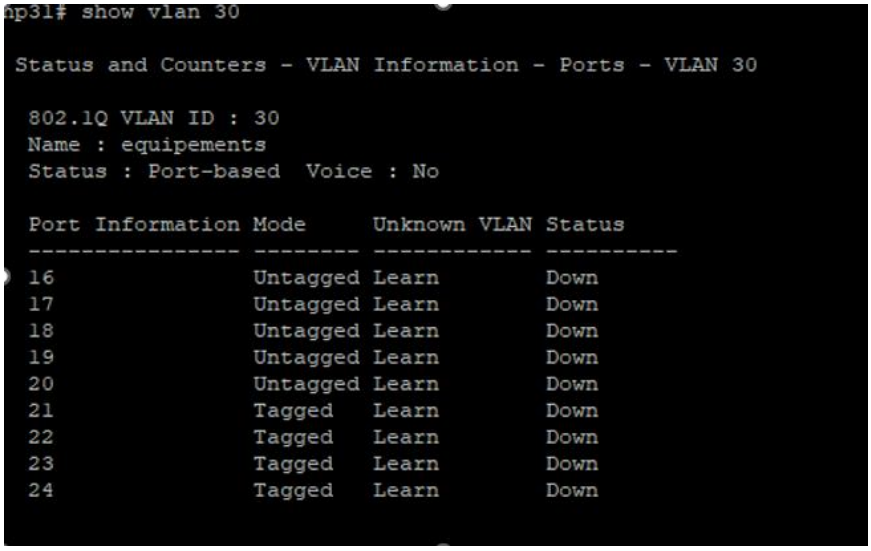
```
hp31# sh vlan

 Status and Counters - VLAN Information

  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  Management VLAN :

  802.1Q VLAN ID Name         Status       Voice
  -------------- ------------ ------------ -----
  1              DEFAULT_VLAN Port-based   No
  10             employes     Port-based   No
  20             visiteur     Port-based   No
  30             equipements  Port-based   No
  999            admin        Port-based   No
```

Le VLAN 10 sera utilisé pour les employés. Les ports 2 à 10 seront non taggés (access port) pour les PC des employés, et les ports 21 à 24 seront taggés pour permettre à d'autres équipements (comme les serveurs) de communiquer avec ce VLAN.

```
hp31# sh vlan 10

 Status and Counters - VLAN Information - Ports - VLAN 10

  802.1Q VLAN ID : 10
  Name : employes
  Status : Port-based  Voice : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  2                Untagged Learn        Down
  3                Untagged Learn        Down
  4                Untagged Learn        Down
  5                Untagged Learn        Down
  6                Untagged Learn        Down
  7                Untagged Learn        Down
  8                Untagged Learn        Down
  9                Untagged Learn        Down
  10               Untagged Learn        Down
  21               Tagged   Learn        Down
  22               Tagged   Learn        Down
  23               Tagged   Learn        Down
  24               Tagged   Learn        Down
```

Le VLAN 20 est pour les invités, qui auront un accès à Internet seulement. Les ports 11 à 15 seront non taggés pour connecter les appareils des invités (comme les PC ou téléphones), tandis que les ports 21-24 seront taggés pour assurer la connectivité avec des équipements partagés (comme les points d'accès Wi-Fi).

Le **VLAN 30** est pour les équipements (comme les imprimantes, les caméras, etc.). **Les ports 16 à 20** seront **non taggés** pour connecter ces équipements, tandis que les **ports 21-24** seront **taggés** pour assurer la communication avec d'autres VLANs si nécessaire.



```
hp31# show vlan 30

Status and Counters - VLAN Information - Ports - VLAN 30

 802.1Q VLAN ID : 30
 Name : equipements
 Status : Port-based  Voice : No

 Port Information Mode     Unknown VLAN Status
 ---------------- -------- ------------ ----------
 16               Untagged Learn        Down
 17               Untagged Learn        Down
 18               Untagged Learn        Down
 19               Untagged Learn        Down
 20               Untagged Learn        Down
 21               Tagged   Learn        Down
 22               Tagged   Learn        Down
 23               Tagged   Learn        Down
 24               Tagged   Learn        Down
```

Le VLAN 999 est réservé à l'administration. Le port 21 sera non taggé pour un accès administratif direct, tandis que les ports 22-24 seront taggés pour assurer la communication avec les équipements d'administration réseau.

Ports taggés sur les VLANs communs (ports 21-24)

Les ports 21-24 seront taggés pour permettre la communication entre les VLANs. Cela est utile pour les équipements partagés, tels que les serveurs, points d'accès Wi-Fi ou switches intermédiaires qui doivent être capables de communiquer avec plusieurs VLANs.

Port 21 : Associé à VLAN 10 (employés) pour l'accès aux équipements internes.

Ports 22-24 : Associés aux autres VLANs, tels que VLAN 20 (invités) et VLAN 30 (équipements) pour faciliter l'interconnexion entre ces VLAN.