BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :** 2
Nom, prénom : ABDOU Yousra	**N° candidat :2248198273**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 03/04/2026

Organisation support de la réalisation professionnelle

Le laboratoire pédagogique GSB (Galaxy Swiss Bourdin) est une organisation fictive utilisée dans le cadre de la formation afin de reproduire le fonctionnement d'un système d'information d'entreprise.
Les utilisateurs utilisent quotidiennement les ressources informatiques pour travailler, accéder aux données et utiliser les services réseau. L'infrastructure repose sur plusieurs serveurs et postes clients.

Cependant, les journaux d'événements sont répartis sur chaque machine, ce qui rend la supervision difficile et limite la détection rapide des incidents.

L'organisation a donc besoin d'une solution permettant de centraliser les logs afin d'améliorer la supervision et l'analyse des anomalies.

Intitulé de la réalisation professionnelle

Mise en place et déploiement d'une solution de centralisation et d'analyse des journaux d'événements avec Graylog

Période de réalisation : Janvier – Février 2026 **Lieu :** Saint-Denis

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[1] (ressources fournies, résultats attendus)

Dans le cadre de cette réalisation, l'objectif était de mettre en place une solution permettant de centraliser et analyser les journaux d'événements afin d'améliorer la supervision du système d'information.
Les ressources mises à disposition étaient :

- Environnement virtualisé sous VMware
- Serveur dédié pour Graylog
- server Windows Server (Active Directory)
- Postes clients Windows 11
- Composants nécessaires à Graylog (MongoDB, OpenSearch)
- La documentation technique Les

résultats attendus étaient :

- Mise en place d'un serveur Graylog fonctionnel
- Centralisation des journaux d'événements
- Configuration de la collecte des logs
- Vérification de la remontée des informations
- Possibilité d'analyser les événements pour détecter des anomalies

[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.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Ressources matérielles :

- Serveur virtualisé dédié à Graylog
- server Windows Server (Active Directory)
- Postes clients Windows 11

Ressources logicielles :

- Graylog (centralisation et analyse des logs)
- MongoDB (base de données)
- OpenSearch (indexation des logs)
- NXLog / Winlogbeat (collecte des journaux)
- VMware (virtualisation)
- Windows Server et Windows 11

Ressources documentaires :

- Tutoriels d'installation Graylog
- Documentation officielle Graylog
- Guides de configuration des agents de logs
- Ressources en ligne

Modalités d'accès aux productions[3] et à leur documentation[4]

Les productions sont accessibles depuis l'environnement virtualisé utilisé dans le laboratoire pédagogique. Le serveur Graylog est accessible via une interface web permettant de consulter et analyser les journaux d'événements centralisés.

Les éléments disponibles sont :

- Le serveur Graylog configuré
- Les inputs paramétrés
- Les agents de collecte installés
- Les journaux centralisés
- Les tableaux de bord de

supervision La documentation comprend :

- Les étapes d'installation et de configuration
- Les procédures de collecte des logs
- Les tests réalisés
- Des captures d'écran de l'interface Graylog

[2] Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

[3] 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.

[4] 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.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

ÉpreuveE6 - Administration des systèmes et des réseaux (option SISR)

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

Dans le cadre de cette réalisation professionnelle, j'ai mis en place une solution pour regrouper les journaux informatiques (logs) avec Graylog afin de mieux surveiller le système et améliorer la sécurité. Le but était de récupérer les informations provenant de plusieurs machines, comme un serveur Linux et un ordinateur Windows, pour repérer plus facilement les problèmes, comprendre les erreurs et suivre ce qu'il se passe sur le réseau. Pour cela, j'ai utilisé un serveur Linux sur lequel j'ai installé Graylog ainsi que les outils nécessaires pour stocker et gérer les données. Les machines envoient leurs informations vers ce serveur : les systèmes Linux utilisent un service appelé Syslog, et les machines Windows utilisent un petit programme (agent) pour transmettre leurs données.

J'ai d'abord installé et configuré le serveur Graylog, puis j'ai mis en place un point de réception (input) pour recevoir les journaux sur un port précis. Ensuite, j'ai configuré les machines pour qu'elles envoient leurs informations vers ce serveur. Une fois que les données étaient bien reçues, j'ai pu les consulter dans l'interface Graylog, faire des recherches, trier les informations et créer des tableaux de bord pour mieux visualiser l'activité.

Enfin, j'ai sécurisé l'accès à l'outil en gérant les utilisateurs et les droits. Cette solution permet aujourd'hui de regrouper toutes les informations importantes au même endroit, de mieux voir ce qui se passe sur le système et de réagir plus rapidement en cas de problème.

SCHEMA :