PROJET PERSONNALISÉ ENCADRÉ

BTS Services Informatiques aux Organisations

Option SISR – Solutions d'Infrastructure, Systèmes et Réseaux

---

Traçabilité & Supervision du SI

Entreprise JaxOLantern

Mise en place d'une architecture de supervision et de centralisation des logs

MACRET Dylan SIO26

PPE 2 – Session 2026

SOMMAIRE

1. Contexte

1.1 L'entreprise JaxOLantern

La société JaxOLantern est un acteur du marché e-commerce spécialisé dans la vente de systèmes lumineux en B to B. Disposant déjà d'une infrastructure opérationnelle (Active Directory, DNS, DHCP, serveur web) mise en place lors du PPE 1, l'entreprise souhaite désormais renforcer la sécurité et la visibilité sur son système d'information.

1.2 Problématique

À la suite d'une cyberattaque d'envergure ayant entraîné une paralysie totale de son infrastructure, la société JaxOLantern a identifié des lacunes critiques dans sa stratégie de défense. L'absence de mécanismes de traçabilité et d'outils de supervision a empêché une détection précoce et une réponse aux incidents efficace.

Afin de garantir la continuité de service et la protection de ses actifs, l'entreprise déploie une nouvelle architecture sécurisée axée sur la visibilité centralisée. Ce PPE s'inscrit dans le Thème 3 : Traçabilité et supervision de la santé et de la sécurité du système d'information.

2. Objectifs du projet

Mettre en place une infrastructure de supervision et de centralisation des logs répondant aux besoins suivants :

- Centralisation des logs : regrouper 100% des journaux d'événements (système, sécurité, application) du domaine jol.local sur la plateforme Graylog
- Monitoring de disponibilité : assurer une surveillance 24/7 des services critiques (AD, DNS, MariaDB) avec un système d'alerte en temps réel via Zabbix
- Réduction du MTTR (Mean Time To Repair) : diminuer le temps nécessaire pour identifier l'origine d'une panne ou d'une intrusion grâce à la corrélation des logs

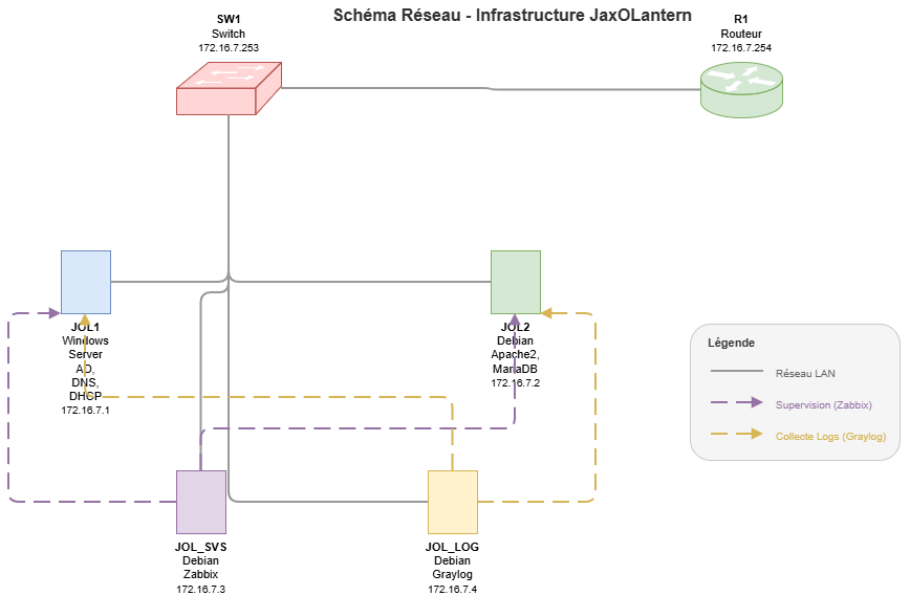
- Intégrité des logs : garantir que les journaux ne peuvent pas être modifiés localement par un attaquant en les exportant immédiatement vers le serveur sécurisé JOL_LOG
- Analyse Post-Mortem et reporting : disposer d'un historique fiable et produire des tableaux de bord mensuels sur la santé de l'infrastructure

3. Architecture et Matériels utilisés

L'infrastructure déployée repose sur les équipements suivants :

Type	Nom	IP	Système	Rôles / Services principaux
Serveur principal	JOL1	172.16.7.1	Windows Server	AD, DNS, DHCP
Serveur Web / BDD	JOL2	172.16.7.2	Debian	Apache2, MariaDB
Serveur Supervision	JOL_SVS	172.16.7.3	Debian	Zabbix
Serveur Logs	JOL_LOG	172.16.7.4	Debian	Graylog
Routeur	R1	172.16.7.254	Cisco	Routage inter-réseaux
Switch	SW1	172.16.7.253	Cisco	Commutation LAN

Le schéma réseau ci-dessous illustre l'architecture globale de l'infrastructure avec la position des serveurs de supervision JOL_SVS et de centralisation des logs JOL_LOG au cœur du système d'information :



4. Réalisation et Déploiement Technique

4.1. Préparation des serveurs JOL_SVS et JOL_LOG

Les serveurs JOL_SVS et JOL_LOG ont été déployés sous Debian avec une configuration réseau statique (IP : 172.16.7.3 pour JOL_SVS et 172.16.7.4 pour JOL_LOG). Les deux serveurs ont été intégrés au domaine jol.local via la résolution DNS pointant vers JOL1 (172.16.7.1).

4.2. Déploiement de Graylog via Docker (Centralisation des Logs)

La pile Graylog a été déployée à l'aide de Docker, à partir d'un environnement conteneurisé fourni par le formateur. Cette approche permet un déploiement rapide et reproductible de l'ensemble des composants nécessaires : MongoDB (stockage des métadonnées), OpenSearch (indexation et recherche des logs) et Graylog Server (interface web et moteur de traitement).

Docker et Docker Compose ont été installés sur JOL_LOG. Le fichier docker-compose.yml fourni définit les trois services (mongo, opensearch et graylog) avec leurs volumes persistants et leurs ports exposés.

L'interface web de Graylog a été rendue accessible sur le port 9000 (http://172.16.7.4:9000). Un Input de type « Beats » a été créé sur le port 5044 pour recevoir les logs envoyés par les agents Winlogbeat et Filebeat déployés sur les serveurs supervisés.

4.3. Configuration de l'envoi des logs vers Graylog

Sur JOL1 (Windows Server) – Winlogbeat : L'agent Winlogbeat (solution officielle Elastic) a été installé sur JOL1 pour collecter les journaux d'événements Windows. La sortie (output) a été configurée vers 172.16.7.4:5044, correspondant à l'Input Beats créé dans Graylog.

Sur JOL2 (Debian – Apache2 / MariaDB) – Filebeat : L'agent Filebeat a été installé sur JOL2 pour collecter et transférer les logs système et applicatifs vers Graylog. La sortie a également été configurée vers 172.16.7.4:5044 (Input Beats de Graylog).

4.4. Déploiement de Zabbix (Monitoring)

Zabbix Server a été installé sur JOL_SVS depuis l'appliance Zabbix. La base de données a été créée sous MySQL local, et le schéma initial importé via les scripts fournis. Le frontend web Zabbix (PHP/Apache) a été configuré et rendu accessible sur le port 80 (http://172.16.7.3/zabbix).

L'agent Zabbix a été installé sur chaque serveur supervisé :

Sur JOL1 (Windows Server) : L'agent Zabbix pour Windows a été installé via le MSI officiel. Le fichier zabbix_agentd.conf a été configuré avec Server=172.16.7.3 et Hostname=JOL1. Le template « Windows by Zabbix agent » a été appliqué, permettant la surveillance du CPU, de la RAM, de l'espace disque et de l'état des services AD, DNS et DHCP.

Sur JOL2 (Debian) : L'agent Zabbix pour Linux a été installé via apt. Le template « Linux by Zabbix agent » a été appliqué.

4.5. Configuration des alertes et tableaux de bord

Un tableau de bord global a été créé dans Zabbix, regroupant les indicateurs clés : état de santé de chaque hôte, graphiques de consommation CPU/RAM sur 24 heures, et historique des alertes

déclenchées. Côté Graylog, un dashboard dédié à la sécurité a été mis en place, affichant les tentatives de connexion échouées sur l'AD, les erreurs HTTP 403/404/500 sur Apache2, et le volume de logs reçus par source.

5. Phase de Tests et Validation

Pour valider la robustesse de l'infrastructure de supervision et le respect du cahier des charges, plusieurs scénarios ont été simulés :

- **Test de centralisation des logs (Graylog) :** Une tentative de connexion échouée a été volontairement provoquée sur le domaine jol.local depuis un poste client.
    - *Résultat :* L'événement (Logon Failure) est apparu dans le dashboard Graylog en moins de 5 secondes, avec les détails complets (nom d'utilisateur, IP source, horodatage). La centralisation des logs est opérationnelle.
- **Test de monitoring de disponibilité (Zabbix) :** Le service Apache2 a été volontairement arrêté sur JOL2 (systemctl stop apache2).
    - *Résultat :* En moins de 60 secondes, Zabbix a déclenché une alerte « Haute » sur le dashboard, signalant l'indisponibilité du serveur. Après redémarrage du serveur, l'alerte s'est résolue automatiquement.
- **Test d'intégrité des logs :** Une suppression manuelle du journal Security a été tentée sur JOL1.
    - *Résultat :* Les événements antérieurs à la suppression étaient déjà stockés dans Graylog et restaient consultables. L'événement de purge du journal (Event ID 1102) a également été transmis, prouvant que la traçabilité est maintenue même en cas de tentative de falsification locale.

6. Conclusion

Le déploiement de l'infrastructure de supervision et de centralisation des logs de la société JaxOLantern a été réalisé avec succès et répond intégralement aux exigences du cahier des charges. L'objectif stratégique principal, à savoir la mise en place d'une visibilité centralisée sur l'ensemble du système d'information, a été atteint grâce au déploiement de Graylog sur le serveur dédié JOL_LOG et de Zabbix sur le serveur dédié JOL_SVS.

La centralisation des logs via Graylog (déployé par conteneurisation Docker) et l'envoi en temps réel depuis les agents Winlogbeat (Windows) et Filebeat (Linux) garantissent une traçabilité complète des événements, y compris en cas de tentative de falsification locale. Le monitoring proactif via Zabbix, complété par des alertes automatiques et des tableaux de bord synthétiques, permet désormais une détection rapide des pannes et des anomalies de sécurité.

Ce Projet Personnalisé Encadré m'a permis de consolider mes compétences pratiques en administration de systèmes hétérogènes (Windows Server et Linux) et de découvrir concrètement les enjeux liés à la traçabilité, à la détection d'incidents et à la supervision au sein d'un système d'information professionnel.