BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

Fiche descriptive de réalisation professionnelle (recto)

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

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation :**
Nom, prénom : Metreau Nicolas **Lien du Portfolio : https://metreau-nicolas.fr/**	**N° candidat :**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** ..... / ..... /.....

Organisation support de la réalisation professionnelle
WiFi public). Suite à la mise en place de l'infrastructure sécurisée et hautement disponible, aucun outil ne permettait de surveiller en temps réel l'état des équipements réseau et serveurs. Le directeur des systèmes d'information souhaite désormais assurer une supervision continue de l'ensemble de l'infrastructure, détecter rapidement toute anomalie ou panne, et centraliser les journaux d'événements afin de faciliter le diagnostic et la traçabilité des incidents.

Intitulé de la réalisation professionnelle
Mise en place d'une solution de supervision réseau avec Zabbix et d'une centralisation des logs via Rsyslog et Graylog au sein du port de Cherbourg

Période de réalisation : ..... **Lieu :** .....
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 (ressources fournies, résultats attendus)
Ressources fournies :
Schéma réseau existant, Accès à l'environnement virtualisé, Cahier des charges DSI, Liste des équipements à superviser

Résultats attendus :
Tableau de bord de supervision opérationnel, Alertes automatiques configurées, Centralisation des logs, Documentation technique

Description des ressources documentaires, matérielles et logicielles utilisées
Serveurs virtualisés, Équipements réseau (pare-feux pfSense, switches)

Logicielles :
Zabbix Server & Agent, Rsyslog, Graylog, Linux Debian, SNMP

Documentaires :
Documentation officielle Zabbix, Documentation Rsyslog, Documentation Graylog, Documentation SNMP

Modalités d'accès aux productions et à leur documentation
Tableau de bord Zabbix, Interface web Graylog, Fichiers de configuration, Procédures d'installation, Documentation technique numérique.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

Fiche descriptive de réalisation professionnelle (verso)

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

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

Partie 1 - Besoins spécifiques de l'entreprise

Le port de Cherbourg gère une infrastructure réseau critique utilisée par plusieurs services. Suite au déploiement de l'infrastructure sécurisée et hautement disponible, aucun outil ne permettait de surveiller en temps réel l'état des équipements. Le DSI souhaitait être alerté automatiquement en cas de panne ou de comportement anormal, disposer d'une vue centralisée sur la disponibilité des services, et conserver une trace structurée des événements système pour faciliter le diagnostic en cas d'incident.

Partie 2 - Solutions envisageables

Plusieurs solutions ont été étudiées. Un monitoring manuel via des scripts bash a été envisagé, mais il ne permettait pas une surveillance en temps réel ni une centralisation efficace. Des solutions commerciales comme PRTG ont été analysées, mais leur coût de licence était incompatible avec le budget disponible. Nagios a également été étudié, mais sa configuration complexe et son interface vieillissante le rendaient moins adapté. Zabbix, solution open source, s'est imposé comme le meilleur compromis entre richesse fonctionnelle, facilité de déploiement et coût nul. Pour la centralisation des logs, Rsyslog associé à Graylog a été retenu pour sa capacité à collecter, acheminer et visualiser les journaux de manière structurée.

Partie 3 - Solutions retenues

La solution retenue repose sur un serveur Zabbix déployé sous Linux, assurant la supervision en temps réel de l'ensemble des équipements réseau et serveurs via des agents Zabbix et le protocole SNMP pour les équipements ne pouvant accueillir d'agent. Un serveur Rsyslog a été mis en place pour collecter et acheminer les journaux d'événements vers Graylog, qui assure leur indexation, leur analyse et leur visualisation via une interface web. Des alertes automatiques par email ont été configurées pour notifier l'équipe technique en cas d'anomalie détectée.

Partie 4 - Mise en oeuvre des solutions

La mise en oeuvre a débuté par l'installation et la configuration du serveur Zabbix sur une machine virtuelle Linux Debian. Les agents Zabbix ont ensuite été déployés sur l'ensemble des serveurs Windows et Linux de l'infrastructure. Les équipements réseau (pfSense, switches) ont été intégrés via SNMP pour permettre leur supervision sans installation d'agent. Des tableaux de bord personnalisés ont été créés pour offrir une vue globale de l'état du réseau. En parallèle, un serveur Rsyslog centralisé a été configuré pour collecter les journaux de tous les équipements et les transmettre à Graylog. Des seuils d'alerte ont été définis pour les indicateurs critiques (CPU, mémoire, disponibilité des services) et des notifications automatiques ont été paramétrées. Des règles de filtrage et de rétention des logs ont également été configurées dans Graylog.

Partie 5 - Améliorations futures

Plusieurs améliorations pourraient être envisagées, notamment l'intégration de Grafana pour enrichir les tableaux de bord Zabbix avec des visualisations graphiques avancées. La mise en place de règles de corrélation d'alertes dans Graylog permettrait une analyse plus fine et automatisée des incidents. L'ajout de sondes de supervision réseau externes garantirait une détection plus rapide des coupures de connectivité. L'automatisation des rapports de supervision hebdomadaires pourrait également être mise en oeuvre pour faciliter le suivi de l'infrastructure.

Partie 6 - Conclusion

La mise en place de Zabbix, Rsyslog et Graylog au sein du port de Cherbourg offre désormais une visibilité complète sur l'état de l'infrastructure réseau et système. La supervision en temps réel, les alertes automatiques et la centralisation des journaux permettent à l'équipe technique d'anticiper les pannes, de réagir rapidement aux incidents et d'assurer une traçabilité complète des événements. Cette solution complète et renforce naturellement l'infrastructure sécurisée et hautement disponible déployée précédemment, en apportant la couche de monitoring indispensable à une administration efficace du système d'information du port de Cherbourg.