Nom : GARGI

Prénom : Antoine

N° Candidat : 02342374580

BTS Services Informatiques aux Organisations
(Solutions d'Infrastructure Systèmes et Réseaux)

Réalisation professionnelle n°1 : SYSLOG

Session 2024

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS	SESSION 2024
DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 1**
ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)	
Nom, prénom : GARGI ANTOINE	**N° candidat : 02342374580**
Épreuve E5 - Administration des systèmes et des réseaux (option SISR)	
Épreuve ponctuelle **X** **Contrôle en cours de formation** ☐	**Date :** ..... / ..... /.....
Organisation support de la réalisation professionnelle La réalisation professionnelle prend appuie sur une organisation fictive : le laboratoire pharmaceutique GSB	

Ecole supérieure privée Aristée – La Valette du Var

Intitulé de la réalisation professionnelle

Déploiement d'un gestionnaire de serveur de centralisation des logs Rsyslog

Période de réalisation : 02/10/2023 au 31/03/2024 **Lieu : Centre de formation Aristée**

Modalité : **X 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)

Afin de mettre en place ma réalisation professionnelle, j'ai à ma disposition au sein de l'entreprise GSB :

- Un hyperviseur de type 1 Proxmox qui héberge les services virtuels du contexte,
- Un routeur (RTROUT), un parefeu Pf (ProxSILAB)
- Plusieurs switch de niveau 3 (Cisco 3750G et 3560G)
- Un switch BDS de niveau 2 (Cisco 2960)
- Un hyperviseur de type 1 Proxmox, hébergeant entre autres la machine virtuelle Rsyslog
- Un point d'accès (GSB-DELTA)
- Plusieurs ordinateurs pour effectuer les simulations et les tests

Résultat attendu :
Solution d'infrastructure opérationnelle conforme au cahier des charges

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

Schéma infrastructure GSB
Schéma réseau Hestia-CP au sein du réseau GSB
Cahier des charges Hestia-CP
Un hyperviseur de type 1 (serveur Proxmox hebergeant entre autres ma machine virtuelle Hestia-CP)
Un hyperviseur de type 1 (serveur Proxmox Delta hebergeant les différents services GSB)
ISO Debian 12
Plusieurs Switch de niveau 3

Documentation d'installation de Rsyslog : https://neptunet.fr/rsyslog-loganalyzer/

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

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

Accès à la documentation :
Lien Owncloud : https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ?path=%2F
Mot de passe Owncloud: JURY.2024
Puis RP 1

Accès équipements RP 1 :
https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ/download?path=%2FRP1%2FAnnexes&files=GSB%20-%20Acc%C3%A8s%20Equipements.pdf
Mot de passe Owncloud: JURY.2024

Serveur Proxmox : https://192.168.110.233 :8006
Utilisateur : root
Mot de passe : Aristee.2024

Interface web LogAnalyzer : http://192.168.110.60/loganalyzer/
Utilisateur : antoine
Mot de passe : Aristee.2024

Anydesk : 1160416233
Mot de passe : Aristee.2024

[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.

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

I. Introduction

A. Contexte : GSB

Le laboratoire Galaxy Swiss Bourdin (GSB), issu de la fusion entre Galaxy et Swiss Bourdin, est devenu un leader mondial en 2009. Basé à Paris, GSB a choisi la France pour améliorer le suivi de ses activités de visite médicale, tout en ayant son siège social à Philadelphie, aux États-Unis. J'interviens en tant qu'administrateur réseau au sein de ce groupe.

B. Besoin : Mise en place d'un serveur de gestion des logs

Le laboratoire Galaxy Swiss Bourdin (GSB) a besoin de mettre en place un serveur de logs, tel que Rsyslog, pour plusieurs raisons cruciales liées à notamment à l'hebergement de ses services et applications nécessaires au bon fonctionnement de son infrastructure informatique.

Surveillance des évènements : Un serveur de logs permet à GSB de surveiller en temps réel les évènements de ses systèmes informatiques, y compris les serveurs, les bases de données et d'autres composants critiques. Cela aide à identifier rapidement les dyfsfonctionnements via les systèmes ou applications utilisateurs.

Disponibilité des Services : La remontée des logs permet de s'assurer que les services informatiques essentiels de GSB fonctionnent. En cas d'incident, le serveur de logs peut générer des alertes afin que les équipes IT puissent intervenir rapidement pour minimiser les temps d'interruption.

Détection Précoce des Problèmes : Un serveur de logs permet d'anticiper les problèmes potentiels en surveillant les tendances et les comportements anormaux dans les performances du système. Cela facilite la résolution proactive des problèmes avant qu'ils n'affectent sérieusement les opérations de l'entreprise.

Optimisation des Ressources : En surveillant les erreurs ou avertissements sur l'état de santé général des équipements réseaux liées aux ressources telles que la CPU, la mémoire et le stockage, GSB peut optimiser ses ressources informatiques, évitant ainsi la surutilisation ou la sous-utilisation des équipements.

Sécurité de l'Infrastructure : La supervision de logs permet de détecter et d'enregistrer des activités inhabituelles ou des comportements suspects, contribuant ainsi à renforcer la sécurité de l'infrastructure informatique de GSB. Cela inclut la détection d'attaques potentielles ou de vulnérabilités de sécurité.

Rapports et Analyse : La mise en place d'un serveur de logs permet à GSB d'obtenir des rapports détaillés sur les performances et l'utilisation des ressources. Ces rapports sont utiles pour l'analyse, la planification et la prise de décision.

Conformité Réglementaire : Certains secteurs, y compris l'industrie pharmaceutique, sont soumis à des réglementations strictes en matière de gestion des données et de sécurité informatique. Les logs générés peuvent aider à assurer la conformité aux normes réglementaires.

En résumé, un serveur de supervision comme Rsyslog serait un outil essentiel pour garantir la stabilité, la sécurité et l'efficacité des opérations informatiques de GSB, ce qui est particulièrement critique dans le domaine de l'industrie pharmaceutique où la fiabilité des systèmes informatiques est essentielle.

II. Choix de la technologie

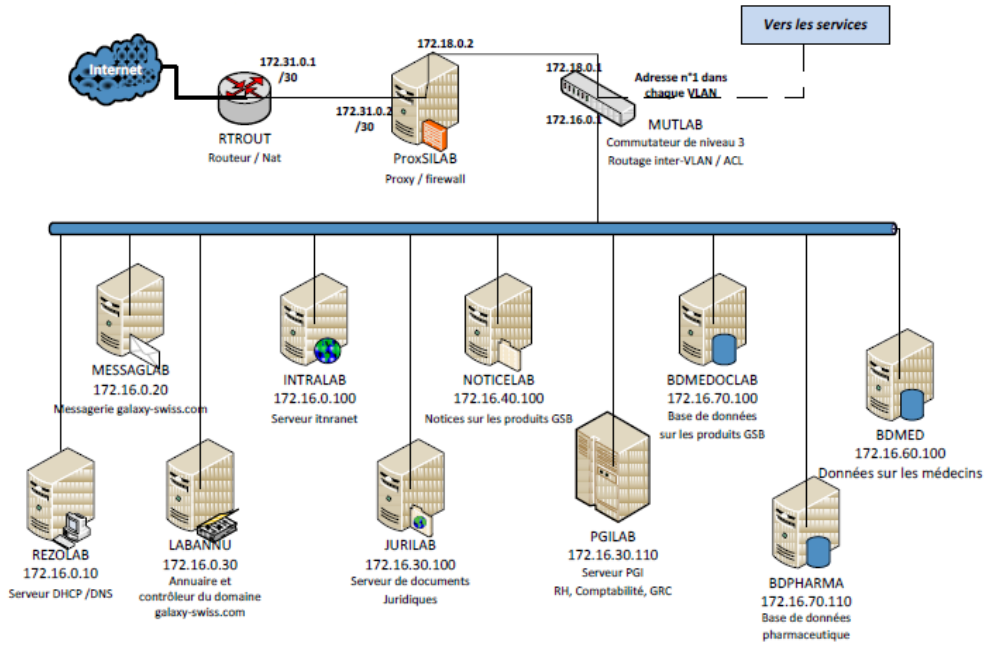
Pour pouvoir avoir une vision d'ensemble sur l'état de nos machines en temps réel, notre solution préconisée est d'installer un serveur de gestion des logs.
Le but étant d'être avertis en temps réel du fonctionnement et des pannes des différents systèmes au sein de notre réseau qui peuvent apparaitre sur les serveurs ou sur les autres équipements informatiques.
La collecte des journaux d'évènements (logs) est la méthode permettant d'obtenir des rapports détaillés sur l'activité de nos serveurs, virtualisés ou physiquement présents.

A. Comparatif de différents types de serveurs de logs

En annexe 1 RP 2, un tableau comparatif et mon choix pour la technologie choisi.
Chois et comparatif des solutions dans le dossier annexe de la RP 1 ci-dessous :
https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ/download?path=%2FRP1%2FAnnexes&files=GSB%20-%20Comparatif%20et%20choix%20solution%20serveur%20de%20logs.pdf
Mot de passe Owncloud: JURY.2024

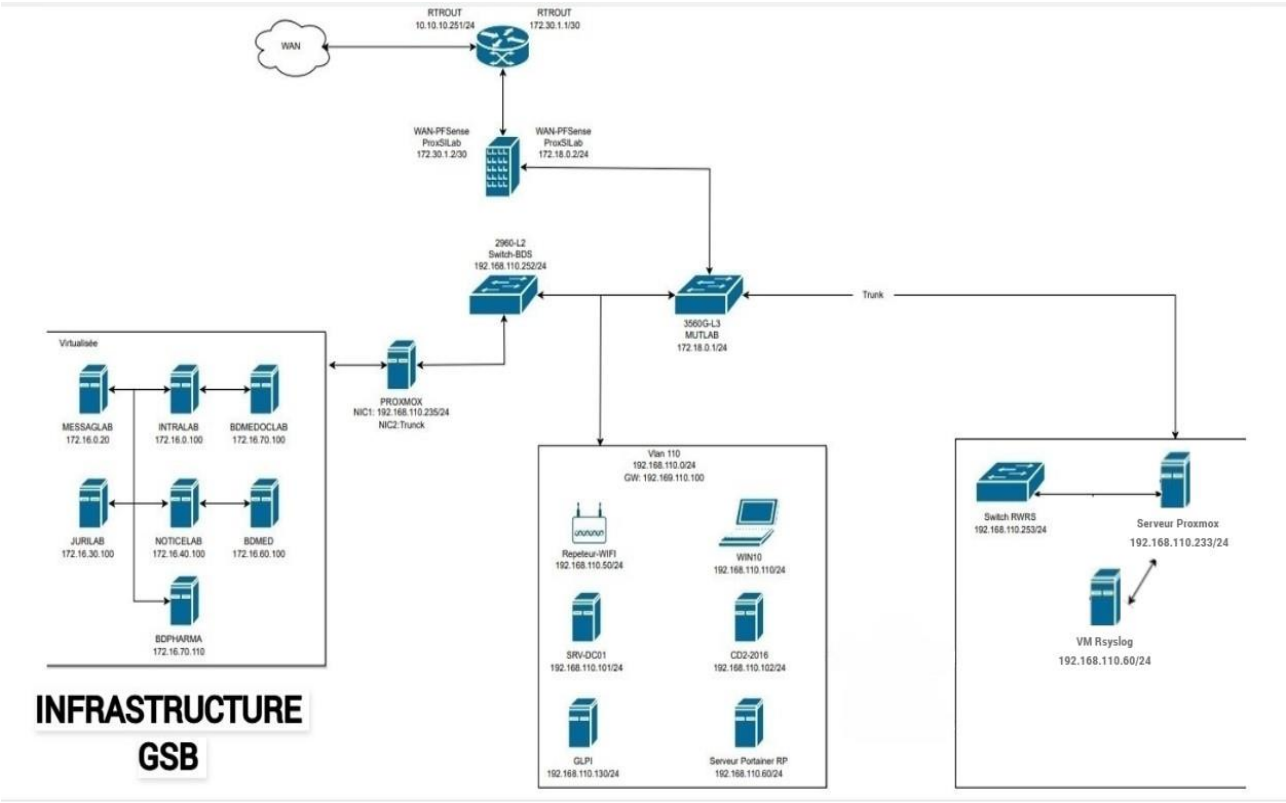
III. Schémas Réseau

A. Schéma réseau GSB existant



B. Schéma réseau de la réalisation professionnelle

J'accède au serveur Syslog en me connectant via le Switch RWRS sur le VLAN 110 (système et réseau). L'adresse de notre serveur est 192.168.110.60



IV. Matériel à Disposition

Afin de mettre en place ma réalisation professionnelle, j'ai à ma disposition au sein de l'entreprise GSB :

- Un hyperviseur de type 1 Proxmox qui héberge les services virtuels du contexte,
- Un routeur (RTROUT), un parefeu Pf (ProxSILAB)
- Plusieurs switch de niveau 3 (Cisco 3750G et 3560G)
- Un switch BDS de niveau 2 (Cisco 2960)
- Un hyperviseur de type 1 Proxmox, hébergeant entre autres la machine virtuelle Rsyslog
- Un point d'accès (GSB-DELTA)
- Plusieurs ordinateurs et vm pour effectuer les simulations et les tests

V. Tableau d'Adressage IP Services/VLAN GSB

Le serveur Rsyslog se trouve dans le VLAN 110 (Réseau et Système).

ID VLAN	Services	Passerelle VLAN
110	Réseau & Système	192.168.110.100/24
20	Direction / DSI	192.168.20.100/24
30	RH/Compta / Juridique/Secretariat	192.168.30.100/24
40	Communication / Rédaction	192.168.40.100/24
50	Développement	192.168.50.100/24
60	Commercial	192.168.60.100/24
70	Labo-Recherche	192.168.70.100/24
80	Deploiment	192.168.80.100/24
90	Salle de formation	192.168.90.100/24
100	Accueil	192.168.150.100/24
150	Visiteurs	192.168.150.100/24
200	Démonstration	192.168.200.100/24
300	Serveurs	172.16.0.100/17
400	Sorties	172.19.0.1/24

VI. Mise en Place et Installation de Rsyslog

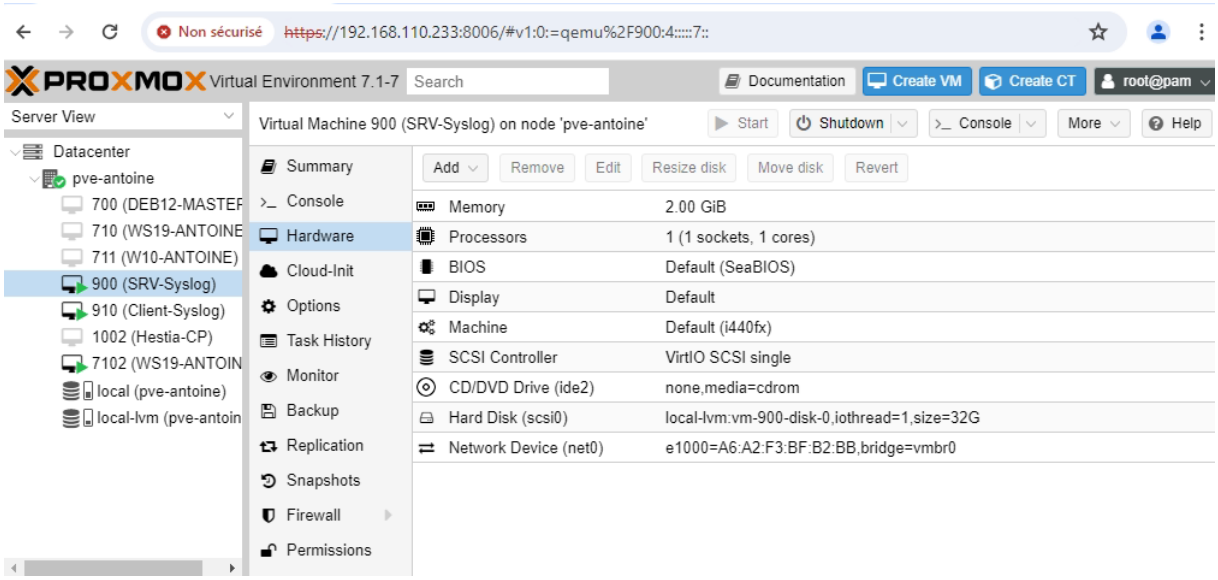
A. Création de VM + déploiement OS Debian 12

Je dispose d'un serveur Proxmox hébergé au sein d'un serveur dans notre baie de brassage Delta.
Avant l'installation, je me connecte sur mon serveur Proxmox via l'interface Web https://192.168.110.233:8006
Je rappelle que notre installation se déroule dans l'environnement virtualisé de Proxmox au sein du VLAN 110.
J'ai déployé ici une VM Debian 12 qui héberge mon serveur Syslog.
Avant son démarrage, voici ici dans un premier temps la configuration matérielle de ma VM Debian 12 en place.

Rsyslog fonctionne dans notre cas sous Debian 12.
Intallation de debian dans le dossier annexe de la RP 1 ci-dessous :
LienOwncloud:
https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ/download?path=%2FRP1%2FAnnexes&files=GSB%20-%20Installation%20OS%20Debian%2012.pdf
Mot de passe Owncloud: JURY.2024

A. Installation de Rsyslog (procédure)

Je dispose d'un serveur Proxmox dans notre baie de brassage GSB Delta.
Avant l'installation, je me connecte à l'hyperviseur Proxmox à l'adresse :
https://192.168.110.233:8006
Je rappelle que notre installation se déroule dans l'environnement virtualisé de Proxmox au sein du VLAN 110.
J'ai déployé ici une VM Debian 12 qui hébergera mon serveur web Rsyslog.
Avant son démarrage, voici ici dans un premier temps la configuration matérielle de ma VM Debian 12 en place.



a. Pré-requis de notre serveur Rsyslog

En suivant le plan d'adressage, il faudra configurer l'adresse IP 192.168.110.38 pour ce serveur.
Je fixe donc l'adresse sur le système Debian et je réserve l'IP dans le serveur dhcp -Windows 2019).
Je mets à jour aussi la résolution DNS ; hestia.gsb.lan sera joiganble à l'adresse IP 192.168.110.38
Configuration des pré requis IP dans le dossier annexe de la RP 1 ci-dessous :
https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ/download?path=%2FRP1%2FAnnexes&files=GSB%20-%20Pre%20requis%20IP.pdf
Mot de passe Owncloud: JURY.2024

b. Installer et configurer Rsyslog pour notre plateforme

https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ/download?path=%2FRP1%2FAnnexes&files=GSB%20-%20Installation%20Rsyslog.pdf
Mot de passe Owncloud: JURY.2024

c. Paramétrage du fichier de configuration Rsyslog

La configuration du fichier rsyslog.conf est nécessaire afin de personnaliser et optimiser la réception des logs.
Configuration du fichier *rsyslog.conf* dans le dossier annexe de la RP 1 ci-dessous :
https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ/download?path=%2FRP1%2FAnnexes&files=GSB%20-%20Param%C3%A9trage%20du%20fichier%20de%20configuration%20Rsyslog.pdf
Mot de passe Owncloud: JURY.2024

d. Installation outil de centralisation des logs : LogAnalyzer

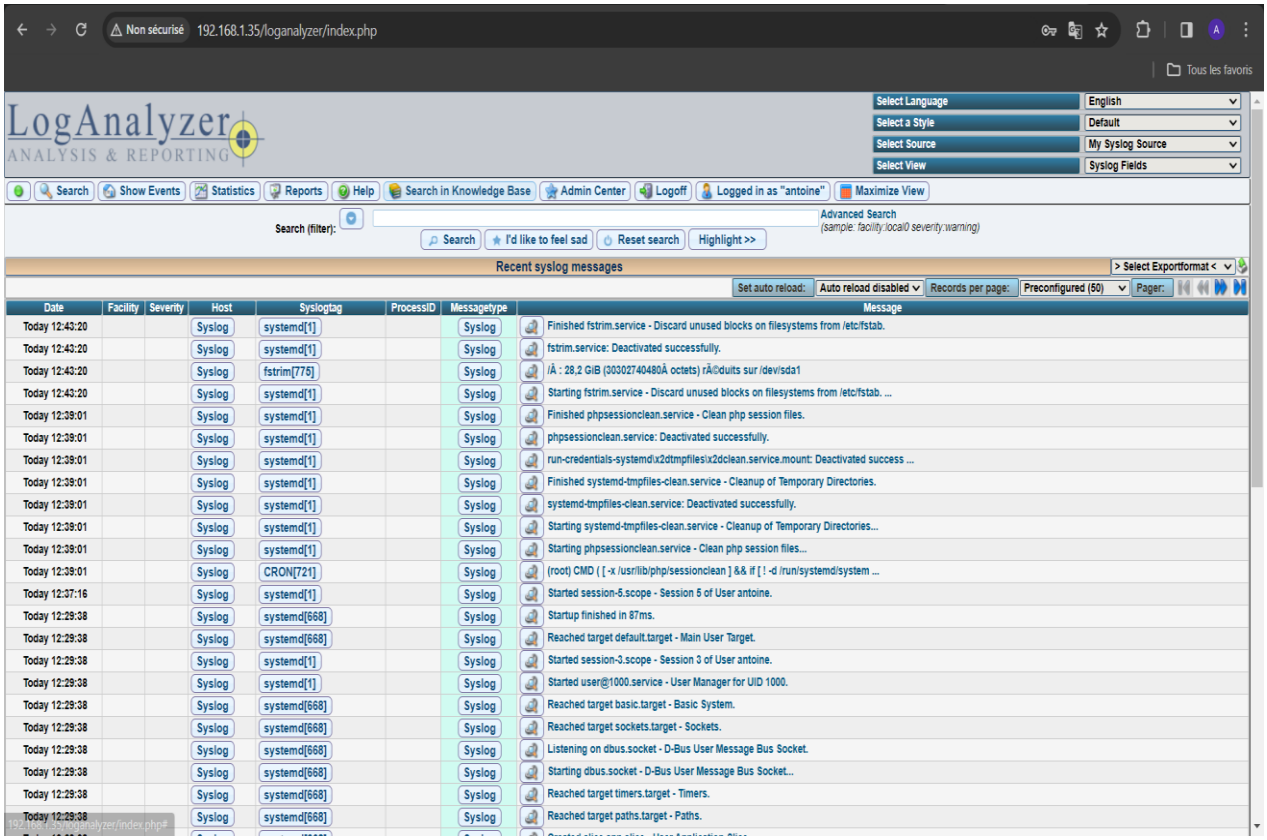
L'outil LogAnalyzer me permets une meilleure gestion des logs.
L'installation de l'application LogAnalyzer le dossier annexe de la RP 1 ci-dessous :
https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ/download?path=%2FRP1%2FAnnexes&files=GSB%20-%20Installation%20LogAnalyzer.pdf
Mot de passe Owncloud: JURY.2024

e. Tests (Client – Serveur)

La remontée des logs depuis une machine cliente Debian 12 vers notre serveur Rsyslog se trouve dans le dossier annexe de la RP 1 ci-dessous :

https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ/download?path=%2FRP1%2FAnnexes&files=GSB%20-%20Remont%C3%A9e%20de%20logs.pdf
Mot de passe Owncloud: JURY.2024

Je vois l'utilisateur antoine se connecter à 12 :37 :16, cela confirme la remontée de logs du client Debian 12 vers le serveur syslog.



f. Paramétrage rotation des logs (logrotate)

Je configure également la rotation des logs pour une meilleure gestion du stockage des logs.

La configuration de *logrotate* se trouve dans le dossier annexe de la RP 1 ci-dessous :

https://cloud.aristeecampus.org/index.php/s/hzDr59qOlXJOEaZ/download?path=%2FRP1%2FAnnexes&files=GSB%20-%20Rotation%20des%20logs%20(rsyslog).pdf
Mot de passe Owncloud: JURY.2024

VII. Évolution

Les évolutions possibles sont les suivantes :

Filtres à appliquer pour la remontée des logs

Il serait intéressant d'adapter le besoin souhaité en appliquant des filtres, en choisissant des alertes ou messages spécifiques qui remonteraient dans notre serveur collecteur de logs.

Déploiement sondes clients via GPO

Aussi, il est possible d'activer la remontée des logs sur différents équipements de l'infrastructure réseau GSB en rentrant dans les systèmes directement ou via des GPO.

VII. Conclusion

RSYSLOG en tant que journal de logs est efficace pour surveiller l'état des systèmes informatiques, des applications et des réseaux.

Bien que la configuration initiale puisse être complexe, RSYSLOG est très flexible et peut être adapté aux besoins spécifiques de l'organisation GSB.

Je mets ici en avant l'importance de comprendre les principes de base de la surveillance informatique et de mettre en place une stratégie de surveillance appropriée pour tirer le meilleur parti de mon serveur de logs.

Dans l'ensemble, ce type de serveur de logs est un outil précieux et essentiel pour garantir une fonctionnalité optimale des systèmes et des applications. Tout au long de ma présentation j'ai tenté de démontrer son rôle d'analyse favorisant la vue d'ensemble sur l'infrastructure que je dois avoir en tant qu'administrateur réseau.

Enfin, la récolte des logs permet une meilleure prise d'initiative dans le but d'aider à éviter les erreurs logicielles ou matérielles couteuses pour l'ensemble des services de GSB.