LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CS6P05NI Final Year Project

Assessment Weightage & Type

25% FYP Interim Report

Semester

2023-24 Autumn

PROJECT TITLE: Centralized Logging Server with Network Automation

Student Name:

London Met ID:

College ID:

Internal Supervisor:

External Supervisor:

Assignment Due Date:

Assignment Submission Date:

Word Count (Where Required): 3710

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Sample 2 - BINIS.docx

Islington College,Nepal

Document Details

Submission ID
trn:oid:::3618:73855426

Submission Date
Dec 12, 2024, 2:05 PM GMT+5:45

Download Date
Dec 13, 2024, 8:54 AM GMT+5:45

File Name
Sample 2 - BINIS.docx

File Size
35.6 KB

52 Pages

5,419 Words

30,551 Characters

5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

56 Not Cited or Quoted 3%
Matches with neither in-text citation nor quotation marks

7 Missing Quotations 2%
Matches that are still very similar to source material

1 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

2% Internet sources
2% Publications
1% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **56** Not Cited or Quoted 3%
  Matches with neither in-text citation nor quotation marks
- **7** Missing Quotations 2%
  Matches that are still very similar to source material
- **1** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

2% Internet sources
2% Publications
1% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1 Submitted works
National Institute of Business Management Sri Lanka on 2024-10-31 3%

2 Internet
www.coursehero.com 3%

3 Submitted works
University of Greenwich on 2010-05-29 1%

4 Submitted works
Kingston University on 2024-01-07 1%

5 Submitted works
Ghana Technology University College on 2016-10-13 0%

Acknowledgement

I would like to extend my heartfelt appreciation to Islington College for providing me with the invaluable opportunity to explore and acquire new knowledge. Beyond just the assessments, the college has offered a platform for me to showcase my understanding, skills, and dedicated effort. I am truly grateful to our supervisors, , for their invaluable advice, constructive suggestions, and the time they dedicated to guiding me.

I also want to express my special thanks to my family for their unwavering support, encouragement, and motivation throughout this journey. Their constant belief in me has been a driving force behind my accomplishments.

Abstract

This report outlines the detailed overview of the development of the Centralized Logging Server with Network Automation System. Centralized logging is used to collect log data from multiple log files on multiple devices and transmit the data to a single centralized location which is then used for various purposes including problem detection, troubleshooting, recording user activities, track authentication attempts, and understanding user behavior. Due to increasing number of threats against networks and systems, the number of security logs increases, thus the overall objective of this project is to implement a centralized logging server with network automation. This allows real time detection and alert of all log transactions from different devices to one centralized server.

The report includes introduction, background, development, and analysis part. An overview of comparable projects used, as well as the client's information for the project, are provided in the background section. The development area includes information on the selected methodology, work break down structure, and Gantt-Chart. Analysis section of the report includes the progress of the report with task completed, and task to be done based on sprint.

Table of Contents

Table of figures

Table of tables

1. Introduction

1.1. Topic introduction

In today's rapidly evolving technological landscape, the management of network devices within IT organizations presents an array of challenges as their numbers continue to grow. These tools must be meticulously maintained to ensure that their configurations remain efficient and effective, particularly as the organization expands. However, administering a large and ever-increasing array of network devices manually, one by one, is not only highly inefficient but also prone to human error. Such errors can lead to configuration inconsistencies, which in turn, may result in critical network service disruptions. To address these complexities and streamline network management, organizations are increasingly turning to network automation with a centralized logging server.

1.2. Current scenario

In 2017, 5% of confirmed security breaches were attributed to brute force attacks, as indicated by recent data. A subsequent study by Kaspersky highlights a concerning trend during the pandemic, revealing a surge in brute force attacks. In comparison to 2020, these attacks have increased substantially from 13% to 31.6%, underscoring the heightened vulnerability brought about by the widespread adoption of remote work (Descalso, 2022).

In recent years, enterprise organizations have raised their network infrastructure standards in terms of accountability and information security. To enhance security even more, it becomes crucial to integrate Authentication, Authorization, and Accounting (AAA) servers with centralized logging. AAA servers help prevent unauthorized access, control user access to devices, and centralize the management of authentication, authorization, and accounting information.

Moreover, centralized logging contributes to enhanced security by allowing the analysis of user activity trends and the identification of unusual behavior. In the event of a system compromise, centralized logs provide forensic ability, enabling organizations to determine the events leading up to the compromise. This information is instrumental in preventing recurrences and enhancing overall cybersecurity measures. Additionally, the centralized approach facilitates the quick detection of security threats, such as brute force attacks, even when distributed across multiple systems, providing a level of visibility that would be challenging to achieve with local logs.

1.3. Problem Statement

In today's network world, organizations face an increasingly complex and multifaceted challenge in the realm of network management and security. One major problem is the traditional method for network configuration and management. This processes often rely on manual intervention, where network administrators must individually configure routers, switches, and other devices. This process is time-consuming and prone to human errors, resulting in configuration discrepancies, security vulnerabilities, and operational inefficiencies. Further, logs generated by these devices is often stored in each individual devices makes it hard to keep an eye on what's happening in the network and to quickly fix any problems.

Without centralized logging, organizations face difficulties in troubleshooting network issues. affecting the overall performance and reliability of the IT environment. Moreover, the absence of integrated Authentication, Authorization, and Accounting (AAA) servers leaves network infrastructures vulnerable to unauthorized access which exposes organizations to security threats and compromises.

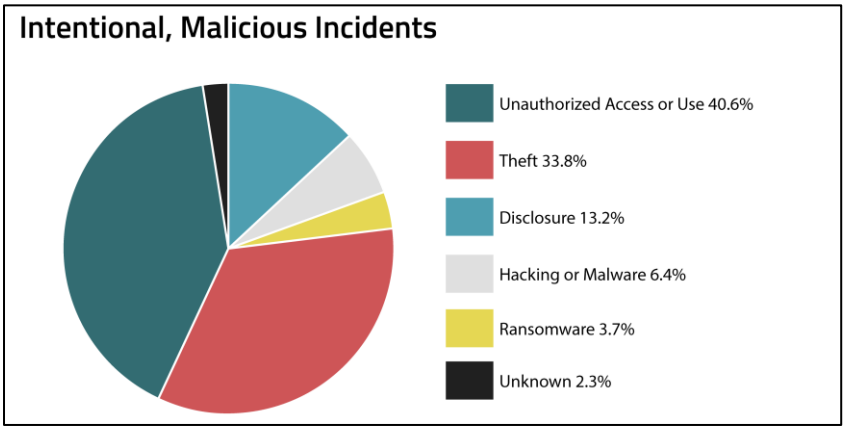


Figure 1: Ratio of unauthorized access

1.4. Project as a Solution

In response to the pressing challenges outlined in the problem statement, the "Centralized logging server with network automation" project is designed to offer comprehensive solutions that address these issues and significantly improve network management, security, and operational efficiency. This project comprises several interconnected components and key features:

Automating Basic Configuration of Network Devices using Ansible:

- Ansible, a powerful and flexible automation tool, is implemented to streamline the configuration of network devices. Ansible playbooks will be created to automate tasks such as device configuration, access control, etc. By doing so, this automation will eliminate manual errors, ensure uniformity in configurations, and drastically reduce the time and effort required for network device management.

Centralized Logging Server:

- To address the issue of decentralized logging, a centralized logging server will be established. This server will serve as a central repository for log data generated by various network devices. Key features of this centralized logging server include log aggregation, advanced search capabilities, and real-time monitoring. This will enhance visibility into network activities, streamline issue identification and resolution, and provide insights necessary for informed decision-making (Paliwal, 2023) (aws, 2023).

Security Event Detection and Response:

- The project will incorporate advanced security event detection mechanisms capable of monitoring network devices for events such as unauthorized access attempts and multiple failed login events. Upon detecting any events such as unauthorized access attempts and multiple failed login events, a log is sent to the centralized logging server such that an alert is generated to notify the event.

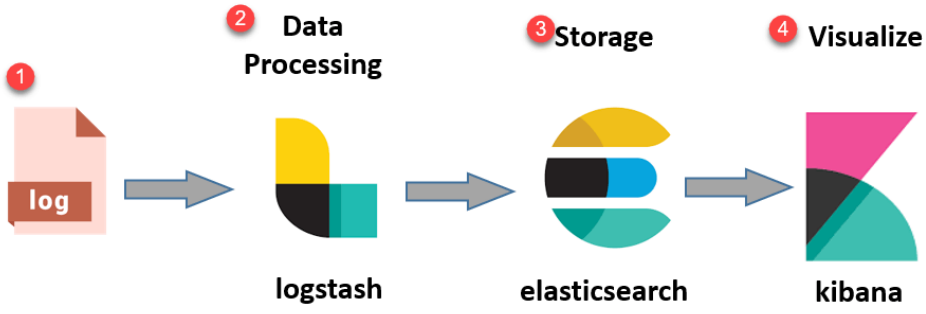


Figure 2: Log Forwarding Process.

1.5. Aim and Objectives

Aim

- The aim of this project is to design, implement, and optimize a centralized logging server as a core component of a network automation solution, enabling improved network monitoring, troubleshooting, and security analysis.

Objectives

- Develop a configuration management system to automate device configuration.
- Integrate a AAA server for authentication, authorization, and accounting within the network infrastructure.
- Implement mechanisms for controlling user access to network devices and centralizing authentication, authorization, and accounting information.
- Design and deploy a centralized logging server capable of receiving and storing log data from network devices.
- Define event criteria for security events, focusing on multiple failed logins attempts and unauthorized access.
- Configure the system to trigger automated responses based on detected security events.
- Develop automated response mechanisms using Ansible playbooks.
- Test, deploy, and maintain the system in the production network environment.

1.6. Structure of Report

1.6.1. Background

The background section of the report serves to unify the fundamental concept of the project, including the specific requirements of the client. It encompasses the essential client information and conducts a comparison analysis with similar projects.

1.6.2. Development

The development section summarizes the methods used to kick-start the development. It explains about the considered and selected methodology and analyses different phase of selected methodology. This part also includes the work breakdown and Gantt-Chart.

1.6.3. Analysis of Progress

This section explains and analyzes the progress to date. It provides the current scenario of the progress, reviews it, and shows the development progress. It includes the evidence of the progress along with a short description.

1.6.4. Future Work

The last section of the project involves the tasks and remaining work yet to be completed, outlining the steps necessary for the progression of these tasks in the future.

2. Background

2.1. Clients Description and Requirements

2.1.1. Client's Name and Description

Name of the Client:

- Vertex Special Technology

Description of the client:

- Vertex Tech is a prominent leader in the technology industry, specializing in end-to-end infrastructure services, IT automation, and cloud solutions. As a digital transformation company, Vertex is dedicated to helping businesses achieve their objectives by leveraging technology effectively. The range of services offered by Vertex includes custom software solutions and comprehensive IT consulting services, aimed at streamlining operations and improving overall business performance. The company's vision is to be at the forefront of technology solutions that drive innovation, transform businesses, and positively impact the world (Vertex, 2023).

  Mr. Suraj Neupane, Engineering and Operation Manager at Vertex, has willingly taken the role of client, believing that the project aligns with the objectives of his profession. Mr. Neupane is committed to collaborating on ideas and adhering to the established conditions for the project.

  (Client Agreement Letter: Refer to Appendix 9.4)

2.1.2. Client's Requirements

- Proper authentication and authorization are required.
- Logs should be collected and analyzed in the centralized logging server.
- Failed login should be detected and respond should be carried out automatically.
- Proper visualization.

2.2. Understanding the Project

2.2.1 Project Elaboration

Computer networks consist of interconnections between two or more devices and are under the administration of network administrators. Since network devices are under the administration of network administrators, they frequently encounter issues such as administrator errors, inadequate documentation, or unauthorized exploitation of devices by third parties. Each problem transforms into an event originating from a network device and is recorded in the system log. For example, a router might send messages about users logging on to console sessions (Leskiw, 2023). Thus, efficient device monitoring plays a crucial role in network management, providing administrators with essential information about the state or condition of the network to make informed decisions in response to events.

This network security project integrates Centralized Logging System, Network Automation, and an AAA (Authentication, Authorization, and Accounting) server. The integration with an AAA server handles authentication requests from network devices, ensuring a secure and centralized authentication, authorization, and accounting functions. These logs, in turn, are transmitted to the Centralized Logging Server for analysis. Log analysis rules defined within the Centralized Logging Server, focusing on criteria such as multiple failed logins attempts and suspicious access patterns are then tailored to respond to specific security events, including those related to authentication.

Elasticsearch serves as the repository for all logs originating from network devices, while Logstash, an open-source software, is employed for the collection and parsing of logs before storing them in Elasticsearch. Kibana, functioning as a web interface, proves valuable for presenting logs in graphical or other visualized formats.

2.2.2 Project Deliverables

The project is commonly used in organizations and projects where robust network security and access control are critical. It focusses mainly for Internet Service Providers (ISPs), telecommunications companies, Large Enterprises, Data Centers, government agencies, and other entities grappling with the challenge of securing extensive and diverse network infrastructures. By centrally managing user authentication and authorization, TACACS+ with centralized logging server facilitates a secure and efficient approach to network access, aligning seamlessly with the security requirements of modern organizations.

Implementing a Centralized Logging System, AAA server integration, and automation not only enhances security but also aids in compliance, monitoring, and incident response, making it valuable for organizations prioritizing security and centralized control over in their operations.

2.3. Similar Projects Review

Project 1- ManagaeEngine EventLog Analyzer

ManageEngine EventLog Analyzer is ‘A Single Pane of Glass for Comprehensive Log Management’, designed for businesses of all sizes and industries. ManageEngine, a division of Zoho, focuses on developing IT management and security software solutions. It is a network log monitoring software with built-in capabilities, that helps you collect and analyze log data from different types of network devices such as routers, switches, intrusion detection and prevention systems, and firewalls. It analyzes network devices' logs and presents actionable insights in the form of real-time dashboard and reports.

EventLog Analyzer provides out-of-the-box support for routers and other network devices. With EventLog Analyzer, you can track admin logons and the router configuration changes made by those admins. The router configuration reports ensure that all the changes made to your network's configuration are authorized and don't create any loopholes in your network security. It provides multiple built-in workflows for common response steps like disabling compromised computers and locking hacked or malicious users' accounts (ManageEngine, 2023).

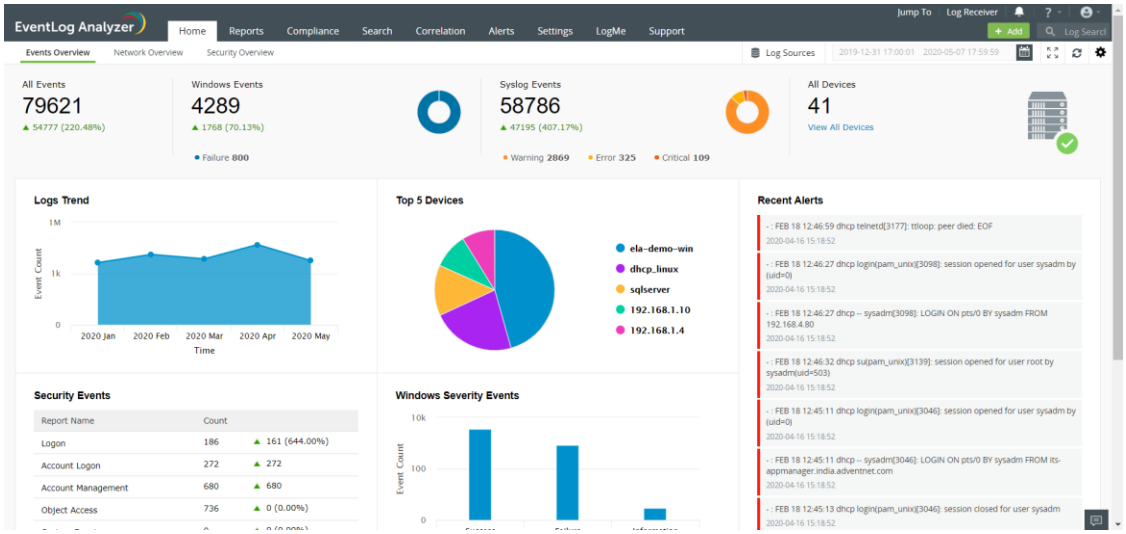


Figure 3: ManageEngine EventLog Analyzer.

Project 2- NetBox

Netbox is an open-source network infrastructure management tool that allows network administrators to effectively monitor, manage and document their infrastructure. It serves as a central repository for tracking and documenting network devices, circuits, and other components. It was developed with the objective of providing a comprehensive solution for network design and maintenance. It is a web-based application that runs on a server and allows users to access it through their web browser. The main feature is to track and manage changes to the network infrastructure (x5Servers, 2023). It is suitable for organizations of all sizes, from small businesses to large enterprises. It is commonly used by network engineers, network operators, IT departments, data centers, and telecommunications companies (Nichols, 2023).

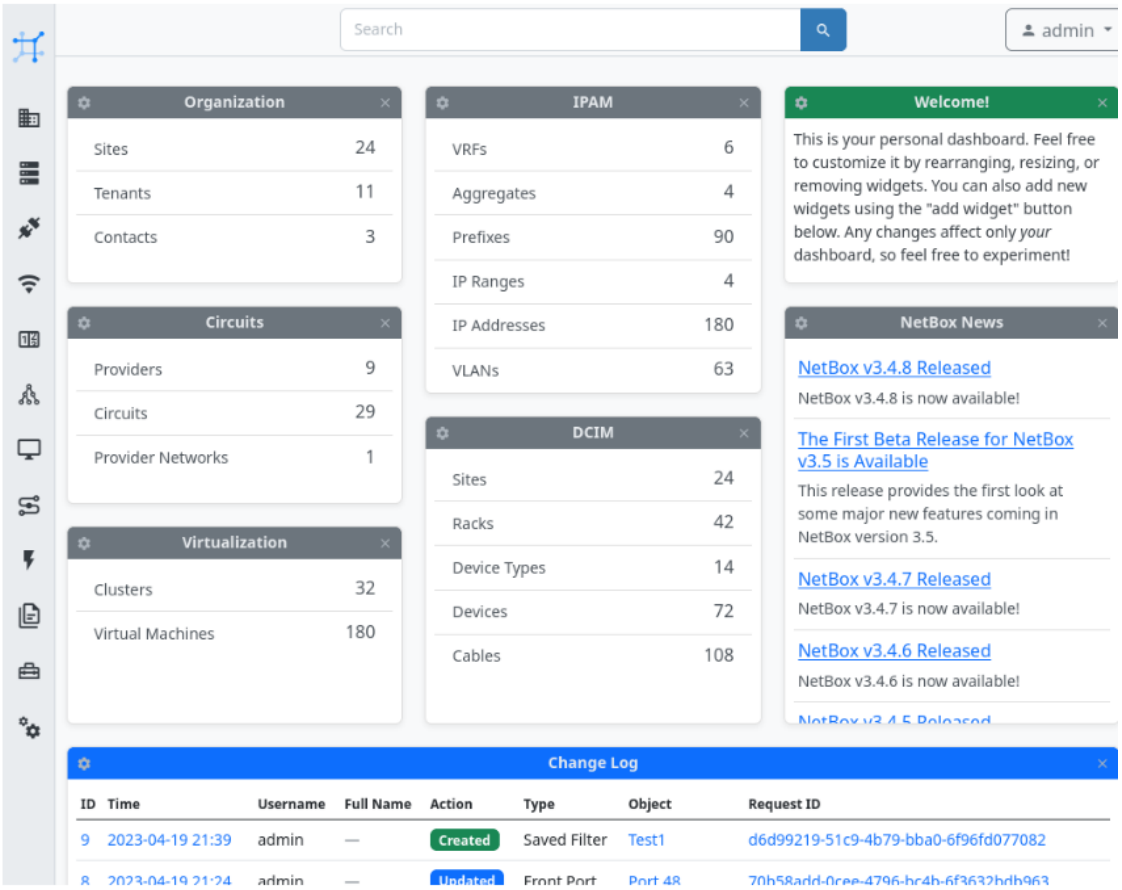


Figure 4: NetBox.

Project 3 – Graylog

Graylog delivers a better user experience by making analysis fast and efficient. Thousands of IT professionals rely on Graylog's scalability, flexibility, and exceptional user experience to solve daily security, compliance, operational, and DevOps issues. It centrally captures, stores, and enables real-time search and log analysis. It is a powerful tool for logs management that analyzes incoming logs from different servers and allows you to create any alert condition based on the data you are collecting (graylog, 2023).

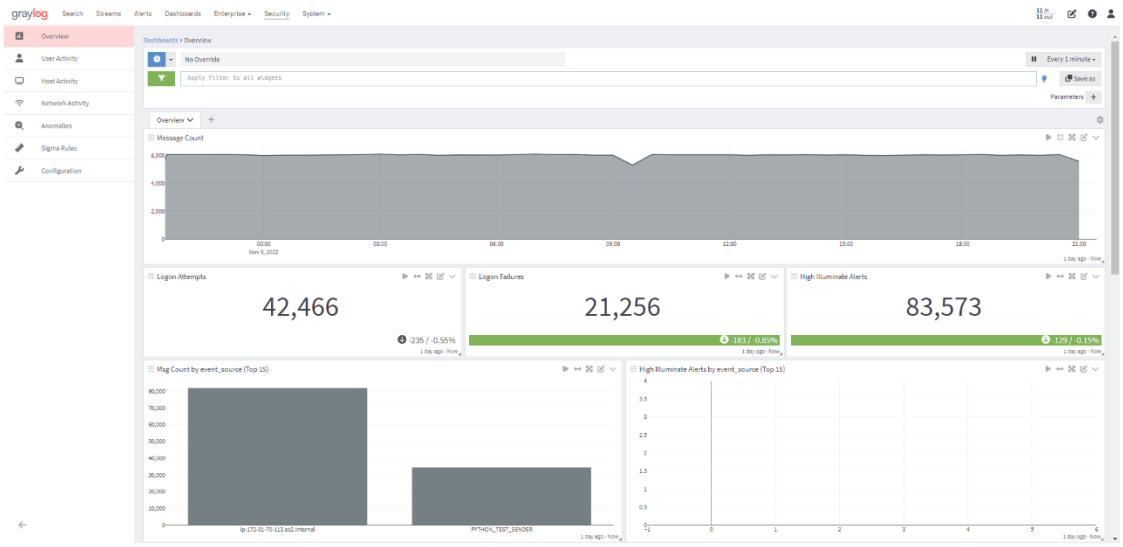


Figure 5: Graylog

2.4. Comparison Table

Features	Project 1	Project 2	Project 3	My Project
Collects and analyze the logs centrally	✓	✓	✓	✓
Monitor privileged users (Users logons.)	✓	✗	✓	✓
Real-time notification and graphical visualization	✓	✗	✓	✓
Incident Response	✓	✗	✗	✓
Open source	Limited	✓	✓	✓

Table 1: Comparison Table.

2.5. Analysis and Conclusion of the Comparison

After analyzing and comparing the features from the similar projects, this project delivers all the fundamental functions in an open-source system. Project 1 has a significant influence on this project as it aligns with the project goals. The idea of the centralized logging to track the network device was taken mainly from the project 2 and 3.

3. Development

3.1. Considered Methodology

Software development life cycle is a systematic process of developing any software, tracking the progress of software development, managing the changes appeared in the system, and minimizing the risks of system failure. The different Software Development Models are:

- Waterfall model
- Prototype model
- Spiral model

3.1.1. Waterfall model

Waterfall model is a traditional software development method that follows a sequential approach. It requires completing each stage before moving on, which makes it inflexible for projects with changing requirements (Badkar, 2023).

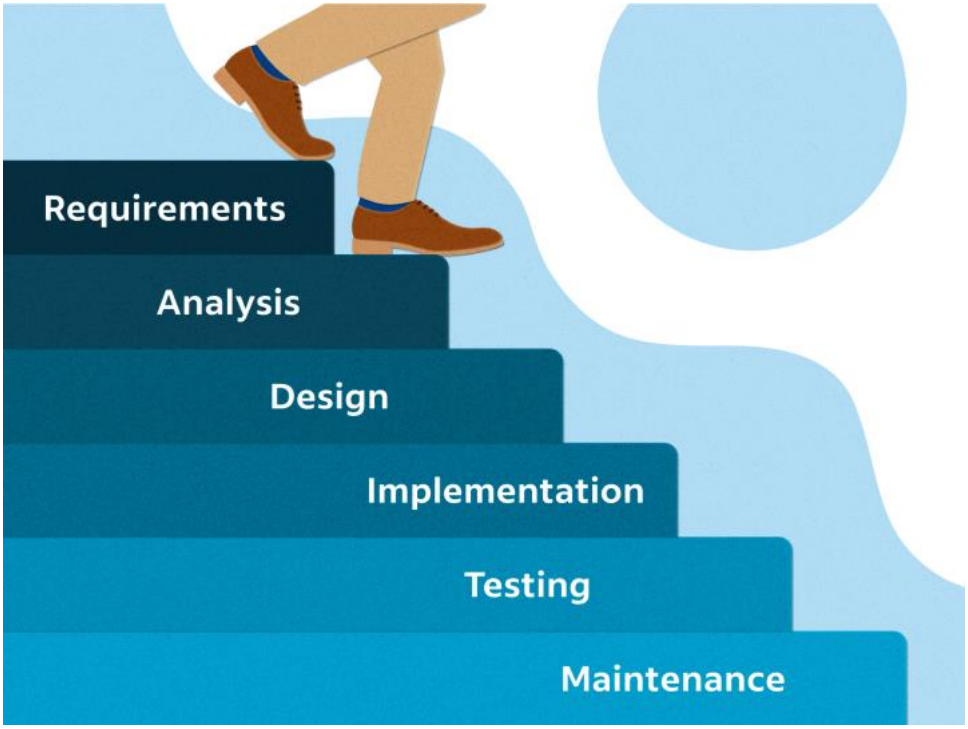


Figure 6: Waterfall Methodology (Indeed Editorial Team, 2023)

3.1.2. Prototype methodology

The Prototype Methodology is a software development process that enables developers to produce a prototype to show its functioning to clients before using this process to construct the actual application (RKEI, 2022).

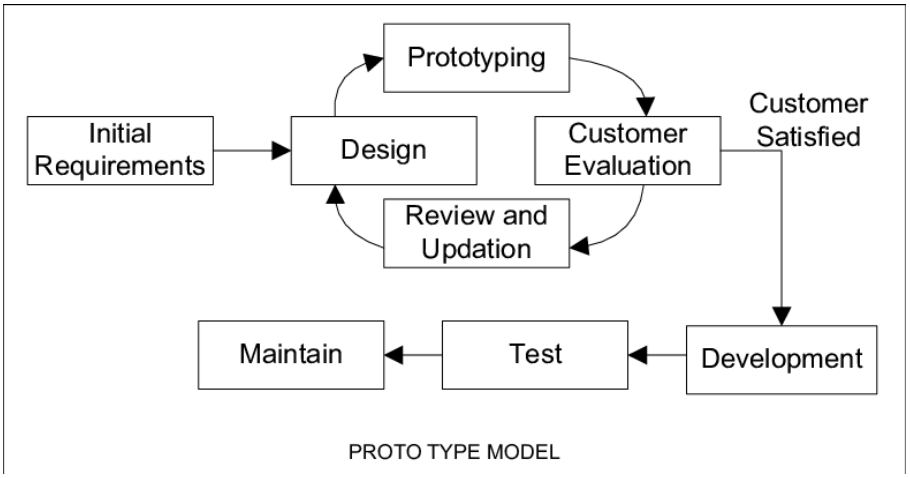


Figure 7:Prototype methodology

3.1.3. Spiral methodology

Spiral methodology is a systematic approach to managing risks that involves multiple iterations. It combines the idea of iterative development with the systematic, controlled aspects of the waterfall model (totorials point, 2023).

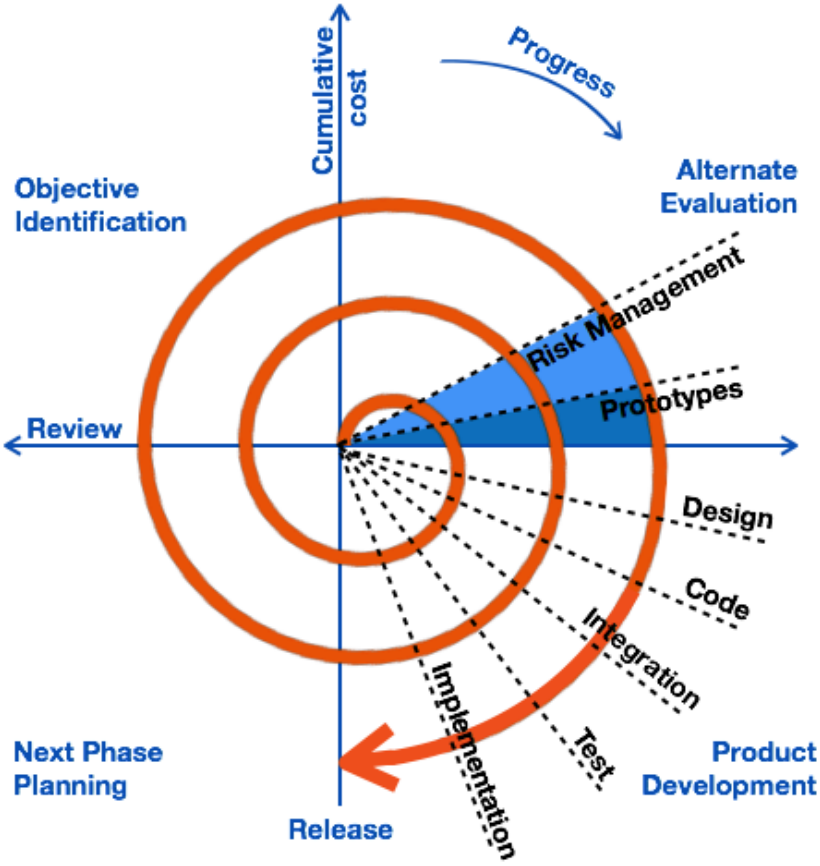


Figure 8:Spiral methodology

3.2. Selected Methodology

Scrum Methodology

Scrum is an Agile project management methodology that is widely used in software development and in is increasingly being adopted in various other fields. It is characterized by its iterative, continuous improvement and increment approach to project management.

Scrum being an Agile framework places a strong emphasis on collaboration, adaptability, and delivering value to stakeholders. It is based on the principles of transparency, inspection, and adaptation. Scrum organizes work into a series of fixed-length iterations called "sprints," which typically last two to four weeks. Each sprint aims to produce a potentially shippable product increment.

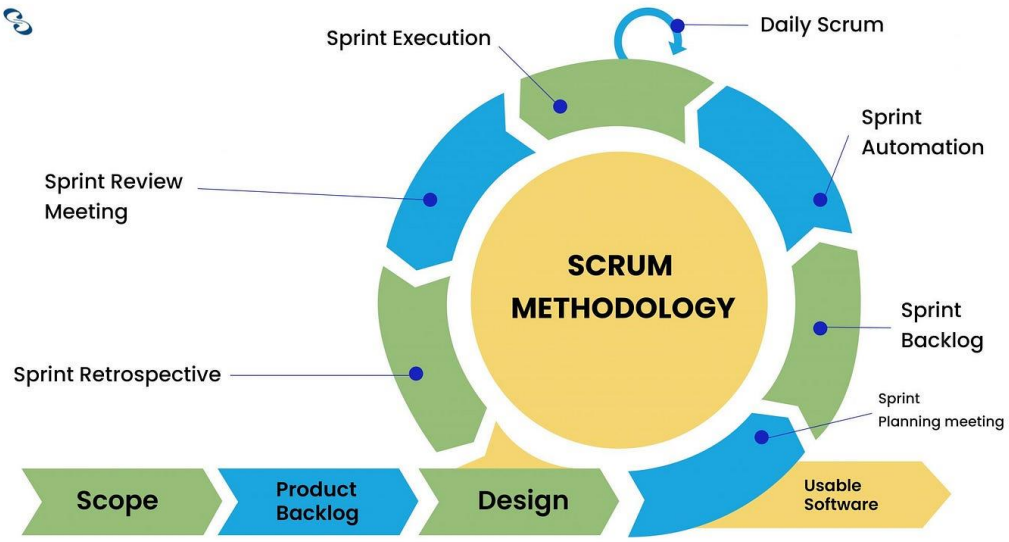


Figure 9: Scrum methodology.

For the centralized logging server project using Scrum, the approach would involve the following Scrum elements:

Product Backlog and User Stories:

- The project requirements, represented as user stories, will be maintained in a product backlog. User stories will define features from the perspective of end-users and stakeholders, such as administrators, developers, or other relevant roles.

Sprint Planning:

- Before each sprint, a sprint planning session will be held to select and prioritize user stories from the product backlog. The team will break down selected user stories into tasks, estimate the effort required, and establish a sprint goal.

Scrum Team:

- The development team will be cross-functional and self-organizing, with members having the necessary skills to complete the tasks. Roles may include a Scrum Master, responsible for facilitating the Scrum process, and a Product Owner, representing the stakeholders and ensuring the product backlog is prioritized.

Sprint Execution:

- During the sprint, the team will work on the tasks and user stories identified during sprint planning.
  Daily stand-up meetings will be held for quick updates, and the Scrum Master will address any impediments.

Incremental Development:

- The logging server will be developed incrementally, with each sprint delivering a potentially shippable product increment.
  At the end of each sprint, there will be a potentially releasable product increment.

Time management

- Scrum enforces time management through its time-boxed iteration (sprints). Each sprint represents a cycle of planning, execution, review, and adaptation which ensures continuous improvement providing a clear structure for managing the project.

Sprint Review and Retrospective:

- At the end of each sprint, a sprint review will be conducted to demonstrate the completed work to stakeholders. A sprint retrospective will follow, allowing the team to reflect on the sprint and identify areas for improvement.

Continuous Integration and Testing:

- Continuous integration practices will be followed to integrate code frequently, and automated testing will be implemented to ensure the quality of the logging server.

3.3. Work Break Down Structure

Work breakdown structure (WBS) is basically a technique for dividing work into smaller task so that the work can be more approachable and manageable. It frames out all the task that need to be completed from beginning to end, starting with the larger activities, and breaking down into more granular detail (Project.co, 2023).

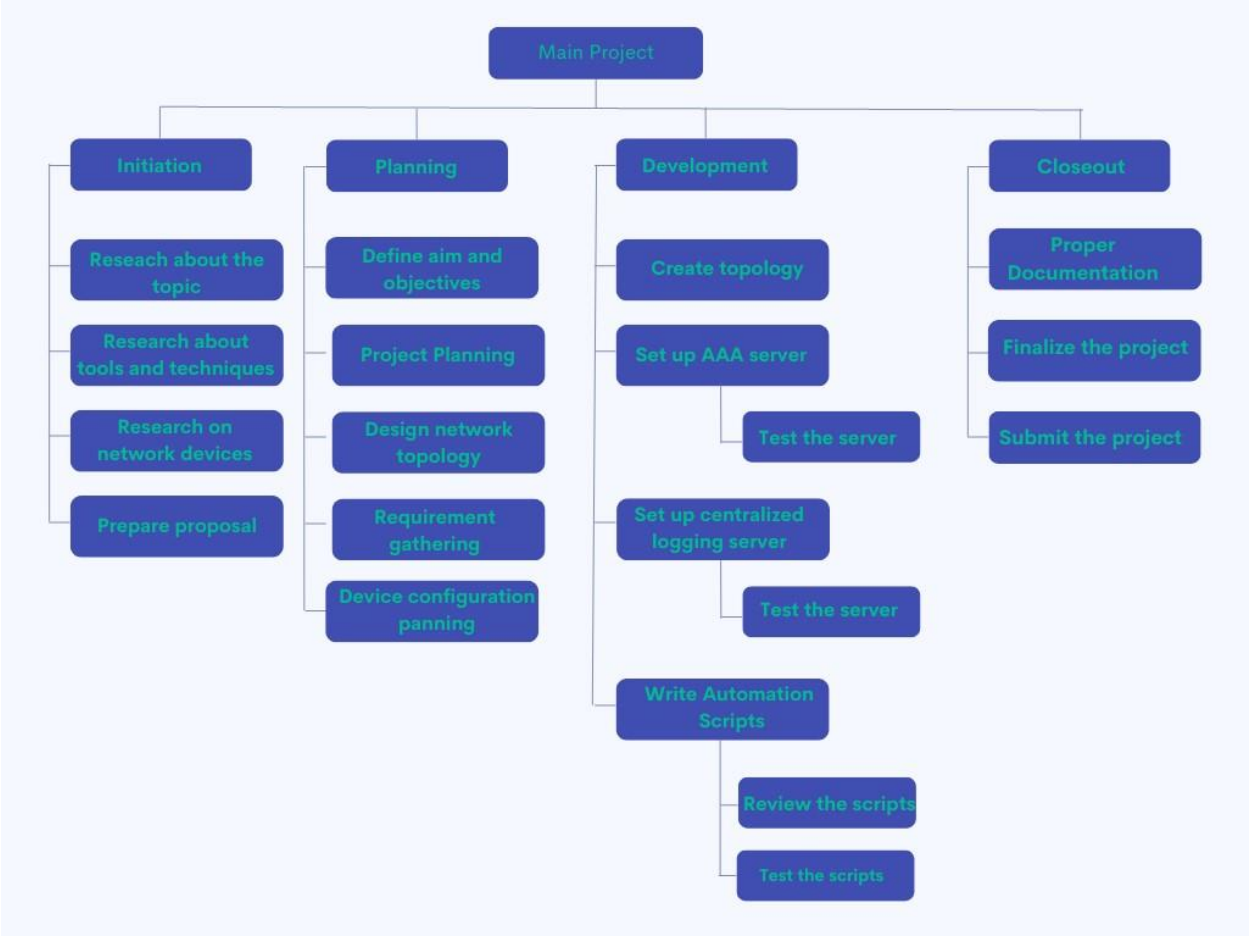
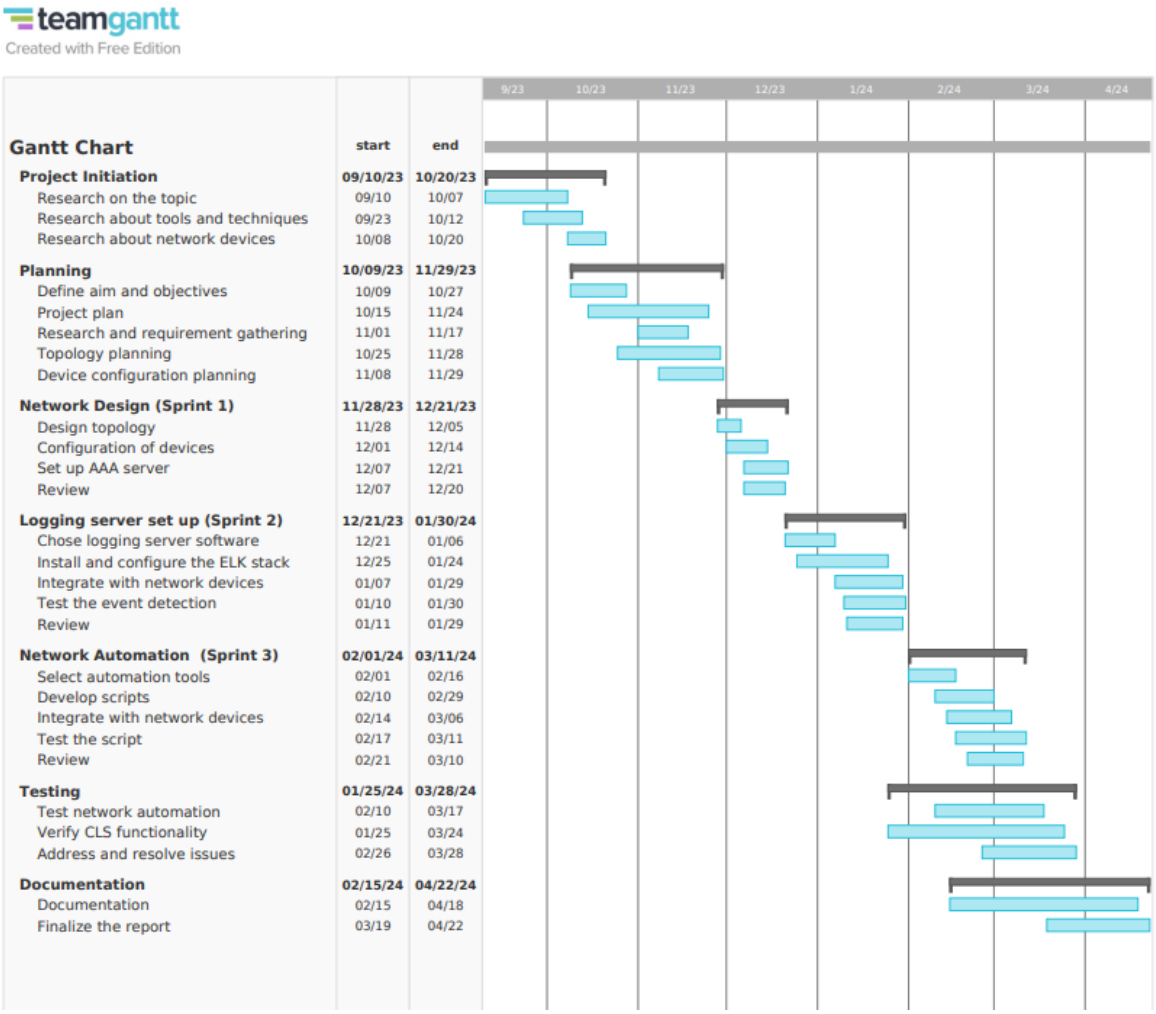


Figure 10: Work Breakdown Structure.

3.4. Gantt Chart

Gantt chart is a project management tool for graphical visualization of a project schedule. These charts are useful in planning a project and defining the sequence of tasks that require completion (GRANT, 2022).



Gantt Chart	start	end
Project Initiation	**09/10/23**	**10/20/23**
Research on the topic	09/10	10/07
Research about tools and techniques	09/23	10/12
Research about network devices	10/08	10/20
Planning	**10/09/23**	**11/29/23**
Define aim and objectives	10/09	10/27
Project plan	10/15	11/24
Research and requirement gathering	11/01	11/17
Topology planning	10/25	11/28
Device configuration planning	11/08	11/29
Network Design (Sprint 1)	**11/28/23**	**12/21/23**
Design topology	11/28	12/05
Configuration of devices	12/01	12/14
Set up AAA server	12/07	12/21
Review	12/07	12/20
Logging server set up (Sprint 2)	**12/21/23**	**01/30/24**
Chose logging server software	12/21	01/06
Install and configure the ELK stack	12/25	01/24
Integrate with network devices	01/07	01/29
Test the event detection	01/10	01/30
Review	01/11	01/29
Network Automation (Sprint 3)	**02/01/24**	**03/11/24**
Select automation tools	02/01	02/16
Develop scripts	02/10	02/29
Integrate with network devices	02/14	03/06
Test the script	02/17	03/11
Review	02/21	03/10
Testing	**01/25/24**	**03/28/24**
Test network automation	02/10	03/17
Verify CLS functionality	01/25	03/24
Address and resolve issues	02/26	03/28
Documentation	**02/15/24**	**04/22/24**
Documentation	02/15	04/18
Finalize the report	03/19	04/22

Figure 11: Gantt chart

3.5. SRS Document

SRS Document: Refer to Appendix 9.1

3.6. System Architecture

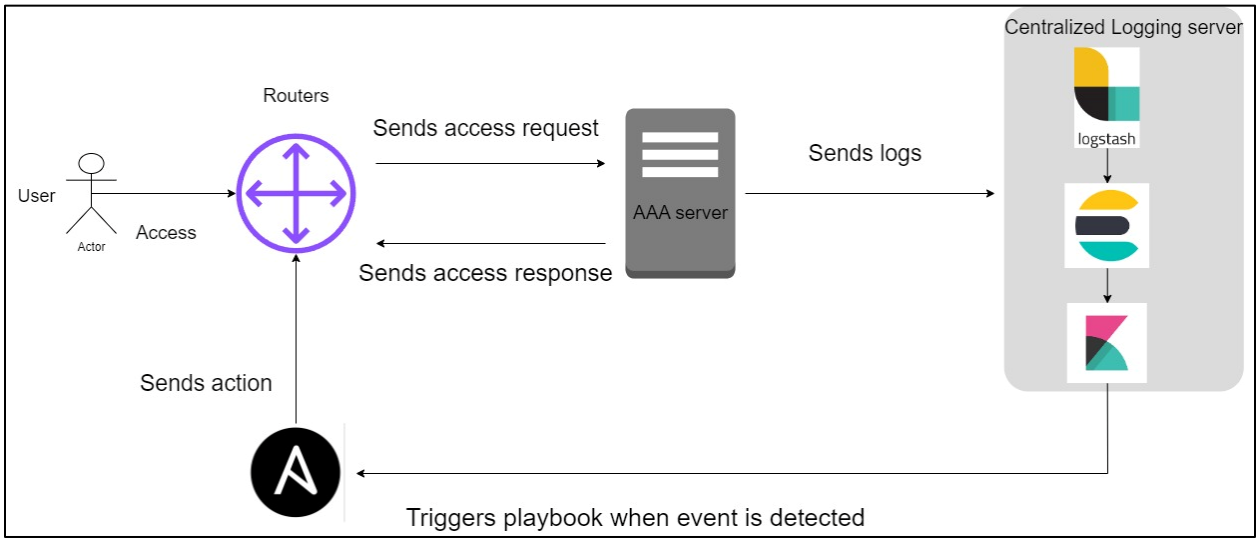


Figure 12: System Architecture.

4. Analysis of Progress

4.1. Progress Table

S.N.	Tasks	Status	Progress(%)
1	Project Initiation	Completed	100
2	Research on the topic	Completed	80
3	Research about tools and techniques	Completed	80
4	Research about network devices	Completed	80
5	Planning	Completed	90
6	Define aim and objectives	Completed	100
7	Project plan	Completed	90
8	Research and requirement gathering	Completed	80
9	Topology planning	Completed	90
10	Device configuration planning	Completed	90
11	Network Design	In Progress	90
12	Design topology	In Progress	80
13	Configuration of devices	Completed	100
14	Set up AAA server	In Progress	100
15	Review	Completed	100
16	Chose logging server software	Completed	100
17	Install and configure the logging server	In Progress	60
18	Integrate with network device	In Progress	0
19	Test the event Detection	In Progress	0
20	Review	In Progress	0
21	Network Automation	Incomplete	0
22	Select automation tools	Incomplete	0
23	Develop scripts	Incomplete	0
24	Integrate with network device	Incomplete	0
25	Test the script	Incomplete	0
26	Review	Incomplete	0
27	Testing	Incomplete	0
28	Test network automation	Incomplete	0
29	Verify CLS functionality	Incomplete	0

30	Address and resolve the issues	Incomplete	0
31	Documentation	Incomplete	0
32	Finalize the report	Incomplete	0

Table 2: Progress Table.

The project progress table serves as a detailed report form, systematically capturing the status of various tasks and milestones. It provides a comprehensive overview of each item, indicating whether it has been completed or is still pending. This reporting format enables a clear understanding of the project's status, facilitating effective tracking of progress and ensuring that the project adheres to its schedule for timely completion.

4.2. Progress Review

4.2.1. Project Plan, Design and Requirements

The progression of activities within the project aligns with the predefined timeline outlined in the Gantt chart. The Gantt chart served as a guiding framework, ensuring a systematic approach to each task. In the initial phase, the process of topic selection and feasibility study was carried out following the resource requirements. For the project a pre survey was conducted through online google form and then a client was also selected. A survey was conducted among IT industry professionals to get their opinions on logging and automation.

After the completion of the initiation phase, planning phase was performed which involved defining aim and objectives, designing network topology along with its configuration.

4.2.2. Progress Timeline

The project has been continued and is progressing according to the scrum methodology. The tasks are being executed in accordance with the defined work breakdown structure within the time outlined in the Gantt Chart. In the initiation phase, the research related to the project was carried out including the tools and techniques used for developing the system. With the research phase still carrying on, the planning of the project was carried out which included the network topology planning with the device configuration. The project's goals and objectives were clearly defined in this phase, and expected outcomes and deliverables were identified.

Then, the development phase was started with the first sprint being carried out. The GNS3 was set up and the images for network devices, virtual machine and network automation was added. Based on the initial topology design, the network was created in the GNS3. The network device i.e., routers was configured, and the network connectivity were verified. For AAA server, TACACS+ was installed and configured in the Ubuntu 16.04 LTS on virtual machine. Then, the connectivity among the network devices in GNS3 and AAA server in ubuntu was checked and verified. After which AAA was configured in the network device as well. The working of TACACS+ for authentication was verified by accessing through telnet using the username and password configured in the AAA server. The authentication log was also successfully generated when both authorized and unauthorized attempt was recorded.

For the next phase of the project, ELK stack (Elasticsearch, Logstash and Kibana) had been selected for the centralized logging server and was installed and configured in ubuntu server.

(Screenshots of Development work: Refer to Appendix 9.3)

4.2.3. Action Plan

The project is divided into different section and is tracked to analyze the progress. The project initial tasks have been completed as per the Gantt chart and work breakdown structure. The remaining section such as logging server setup, network automation, testing and documentation will also be completed according to the Gantt chart.

4.2.4. Survey Findings

A survey was conducted among IT industry professionals to get their opinions on logging and automation.

(Screenshots of Survey Response: Refer to Appendix 9.2)

5. Future Work

5.1. Phases-to-complete

5.1.1. Logging server set-up

In this phase, initially Ubuntu 22.04 LTS will be set up in virtual machine where the chosen centralized logging server would be installed. Elastic search will be installed at first followed by Logstash and then Kibana. The necessary changes would be carried out in each YAML file so that they will be able to communicate and have proper connectivity for carrying out the further task. After the completion of installation of ELK stack, the Ubuntu server is then connected with the network device in the GNS3. Then the devices are configured accordingly to send the logs to the centralized logging server for proper analysis and visualization.

5.1.2. Network Automation

Different tools and technologies will be evaluated to determine the most suitable to have integrated them with automation tool. Scripts will be created, and a test will then be run to see the functioning after being integrated with network device.

5.1.3. Testing

In this phase, the overall system will be checked and verified. For the effectiveness of network and to maintain stability issues will be monitored and necessary changes will be made accordingly. The survey form related to the project will be created and surveyed among people as the feedback from the people can improve our system.

5.1.4. Documentation

This is the final phase of the project's development. All the tests will be documented and the final report with detailed process will be created which marks the completion of the project.

6. Conclusion

As logs play a critical role in the proper functioning and management of any system, it is required to monitor and analyse in real time for the smooth operation and success of the organization. By collecting and analysing log data, organizations can identify and address problems, monitor performance, and gather valuable data.

Moreover, the integration of an AAA (Authentication, Authorization, and Accounting) server with the Centralized Logging and Network Automation system represents a robust approach to enhancing network security.

Thus, the project ensures proactive security practices, aligning with industry standards, and provides organizations with the tools to effectively manage and respond to evolving cybersecurity challenges.

7. References

Abreu, J. T. A., 2020. *Development of a Centralized Log Management System,* s.l.: Universidade da maderia.

aws, 2023. *Benefits of centralized logs.* [Online]
Available at: https://docs.aws.amazon.com/whitepapers/latest/establishing-your-cloud-foundation-on-aws/benefits-of-centralized-logs.html

Badkar, A., 2023. *simplilearn.* [Online]
Available at: https://www.simplilearn.com/software-development-methodologies-article

Descalso, A., 2022. *How to Prevent Brute Force Attacks in 8 Easy Steps [Updated].* [Online]
Available at: https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks

GRANT, M., 2022. *Gantt Charting: Definition, Benefits, and How They're Used.* [Online]
Available at: https://www.investopedia.com/terms/g/gantt-chart.asp#:~:text=A%20Gantt%20chart%20is%20a,engineer%2C%20designed%20the%20Gantt%20chart.

Gratas, B., 2022. *15 Top Network Automation Tools and Must-Have Features.* [Online]
Available at: https://blog.invgate.com/network-automation-tools

graylog, 2023. *THE GRAYLOG BLOG.* [Online]
Available at: https://graylog.org/

Indeed Editorial Team, 2023. *indeed.* [Online]
Available at: https://www.indeed.com/career-advice/career-development/waterfall-methodology

info-finder, 2023. *What Is AAA?.* [Online]
Available at: https://info.support.huawei.com/info-finder/encyclopedia/en/AAA.html

KINUTHIA, K. P., 2016. *IMPLEMENTATION OF CENTRALIZED INFORMATION SYSTEMS LOGS SERVER,* s.l.: s.n.

Leskiw, A., 2023. *Syslog: Servers, Messages & Security – Tutorial & Guide to this System Logs!.* [Online]
Available at: https://www.networkmanagementsoftware.com/what-is-syslog/

ManageEngine, 2023. *Router log auditing.* [Online]
Available at: https://www.manageengine.com/products/eventlog/monitor-router-logs.html

Nichols, K., 2023. *5 Great Network Automation Tools.* [Online]
Available at: https://netboxlabs.com/blog/great-network-automation-tools/

Paliwal, M., 2023. *Centralized Logging with Open Source Tools - OpenTelemetry and SigNoz.* [Online]
Available at: https://signoz.io/blog/centralized-logging/

Project.co, 2023. *Work Breakdown Structure (WBS): The Complete Guide.* [Online]
Available at: https://www.project.co/work-breakdown-structure/#:~:text=A%20work%20breakdown%20structure%20is,well%20as%20identify%20potential%20issues.

RKEI, 2022. [Online]
Available at: https://rikkeisoft.com/blog/methodologies-in-software-development/

Rochim, A. f., Aziz, M. A. & Fauzi, A., 2019. *Design Log Management System of Computer Network Devices Infrastructures Based on ELK Stack.* Indonesia, IEEE.

Saranya, 2021. *The key to centralized log aggregation and easy troubleshooting.* [Online]
Available at: https://www.site24x7.com/blog/log-management-the-key-to-centralized-log-aggregation-and-easy-troubleshooting-4-5-2020-1

Sharif, A., 2022. *WHAT IS CENTRALIZED LOGGING?.* [Online]
Available at: https://www.crowdstrike.com/cybersecurity-101/observability/centralized-logging/

totorials point, 2023. [Online]
Available at: https://www.tutorialspoint.com/sdlc/sdlc_spiral_model.htm

Vertex, 2023. *Vertex.* [Online]
Available at: https://vertexspecial.com/about

x5Servers, 2023. *What is Netbox and How Does It Work?.* [Online]
Available at: https://x5servers.com/en/What-is-netbox-and-how-does-it-work%3F/

8. Bibliography

Abreu, J. T. A., 2020. *Development of a Centralized Log Management System,* s.l.: Universidade da maderia.

Gratas, B., 2022. *15 Top Network Automation Tools and Must-Have Features.* [Online]
Available at: https://blog.invgate.com/network-automation-tools

KINUTHIA, K. P., 2016. *IMPLEMENTATION OF CENTRALIZED INFORMATION SYSTEMS LOGS SERVER,* s.l.: s.n.

Rochim, A. f., Aziz, M. A. & Fauzi, A., 2019. *Design Log Management System of Computer Network Devices Infrastructures Based on ELK Stack.* Indonesia, IEEE.

Saranya, 2021. *The key to centralized log aggregation and easy troubleshooting.* [Online]
Available at: https://www.site24x7.com/blog/log-management-the-key-to-centralized-log-aggregation-and-easy-troubleshooting-4-5-2020-1

Sharif, A., 2022. *WHAT IS CENTRALIZED LOGGING?.* [Online]
Available at: https://www.crowdstrike.com/cybersecurity-101/observability/centralized-logging/

9. Appendix

9.1. System/Software Requirement Specification (SRS)

9.1.1. Introduction

9.1.1.1. Purpose

Software Requirements Specification (SRS) document is developed to provide the detail information about system functionalities and non-functionalities. This document provides the detail description of the functionalities of Centralized Logging Server with Network Automation. This system aims to address the challenges associated with the management of network devices by implementing automated network automation and a centralized logging server.

9.1.1.2. Indented Audiences and Reading Suggestions.

This document is specifically tailored for the development team involved in the creation of the "Centralized Logging Server with Network Automation" system. It serves as a central reference point, providing developers with detailed insights into the architectural design, functionalities, and essential requirements of the system.

9.1.1.3. Project Scope

The proposed system aims to enhance security by employing TACACS for user authentication and authorization, logging unauthorized access attempts, and leveraging the ELK (Elasticsearch, Logstash, Kibana) stack for log analysis. Additionally, the system will utilize Ansible for network automation to respond to detected security incidents. It focuses to enhance network security, streamline troubleshooting, and facilitate log analysis.

9.1.2. Overall Description

9.1.2.1. System Perspective

The "Centralized Logging Server with Network Automation" system will function as a standalone application integrated with existing enterprise network infrastructures. It will interact with network devices, AAA servers, and a centralized logging server to automate network management tasks and enhance overall security.

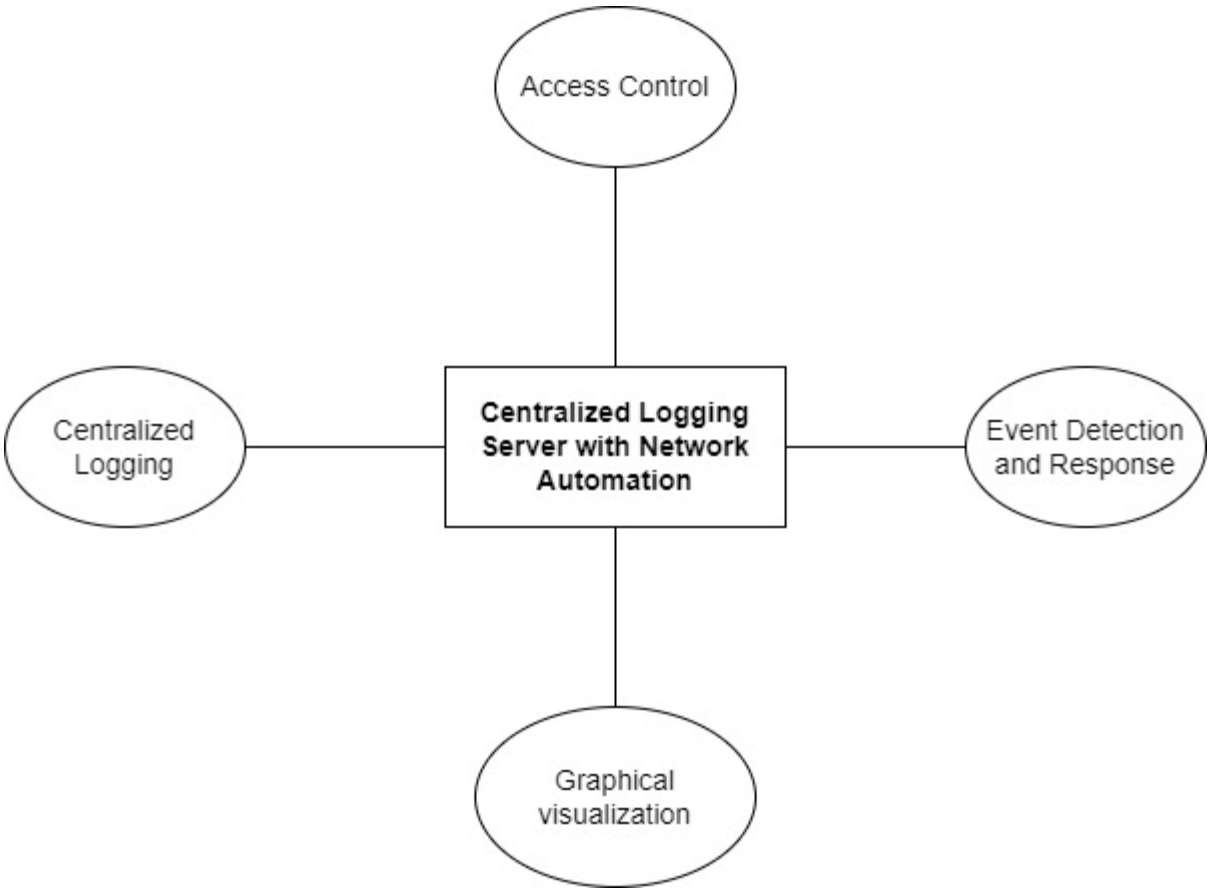


Figure 13: System Perspective Diagram

The Application provides an application-based interface to:

SP1: Targeted Vision 1

SP2: Targeted Vision 1

SP3: Targeted Vision 1

SP4: Targeted Vision 1

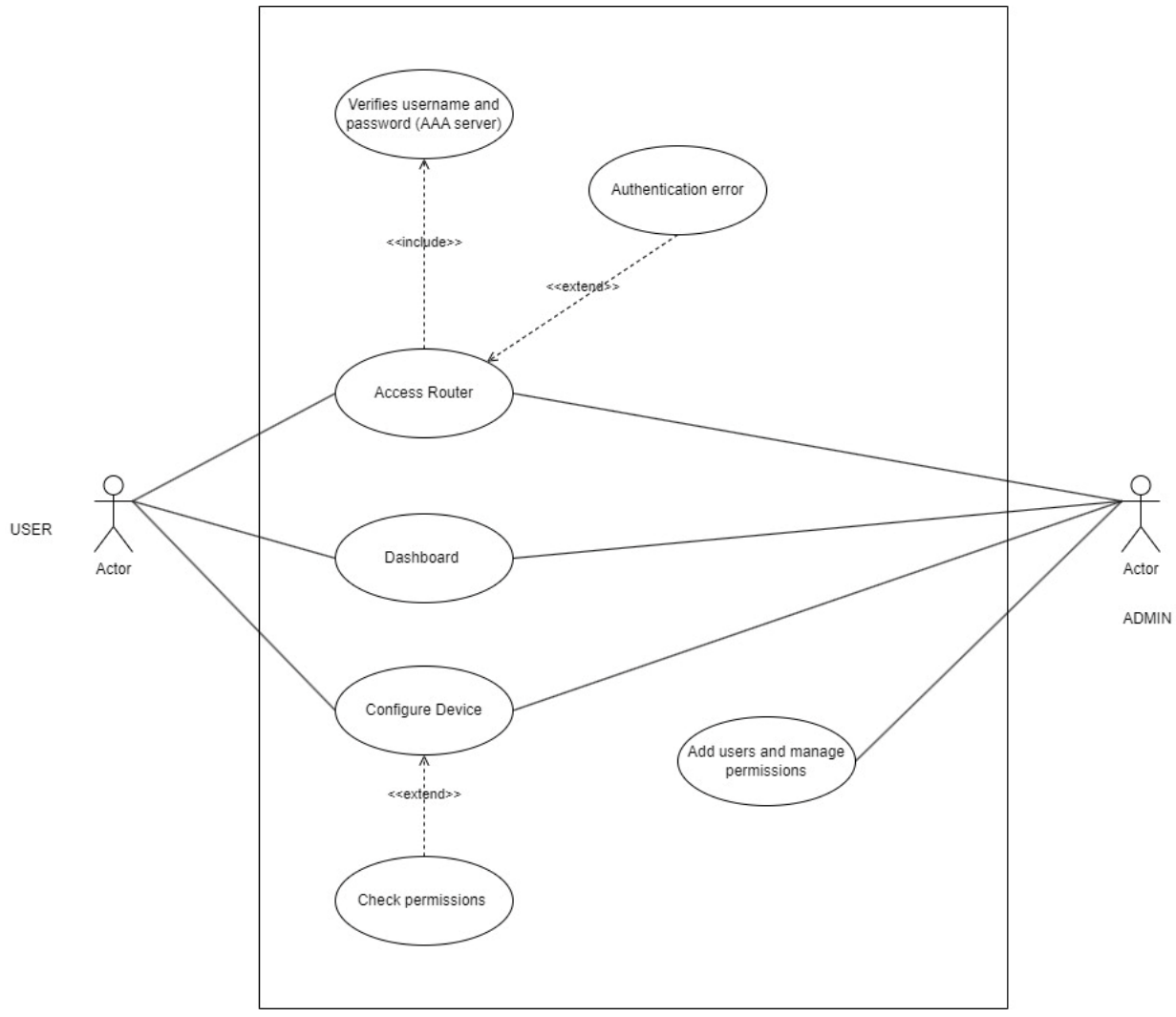


Figure 14: Use Case Diagram.

9.1.2.2. System Features

The following are the primary features of the Application.

SF1: AAA Integration

The system will integrate with AAA servers for user authentication and enforces access control policies defined on AAA servers.

SF2: Centralized Logging

The system will collect log data from all connected network devices and store logs centrally with proper indexing for quick retrieval.

SF3: Real-time Log Analysis

The system will provide real-time graphing and visualization of log data. It will generate alerts for predefined security events.

SP4: Automated Network Automation:

The system will facilitate to discover and manage network devices efficiently ensuring consistency and effective configurations.

9.1.2.3. User class and characteristics

The following are the classes of users who will have specific roles of operation with Application and its reports:

UC1: Normal User

UC1.1

A user access and carry out the task based on the authorization level they are given.

UC1.2

A user interacts with the Kibana interface for visualizing the logs.

UC3: Admin/Developer

UC3.1

An admin/developer is responsible for overseeing the functionality of the system and has the authority to manage the roles of user, and their permissions.

UC3.2

Admin is responsible for configuring and maintaining the system.

9.1.2.4. Operating Environment

The system will operate in a typical enterprise network environment with a mix of network devices and AAA servers. In current context, the system has been designed to be used on GNS3 and Ubuntu machine.

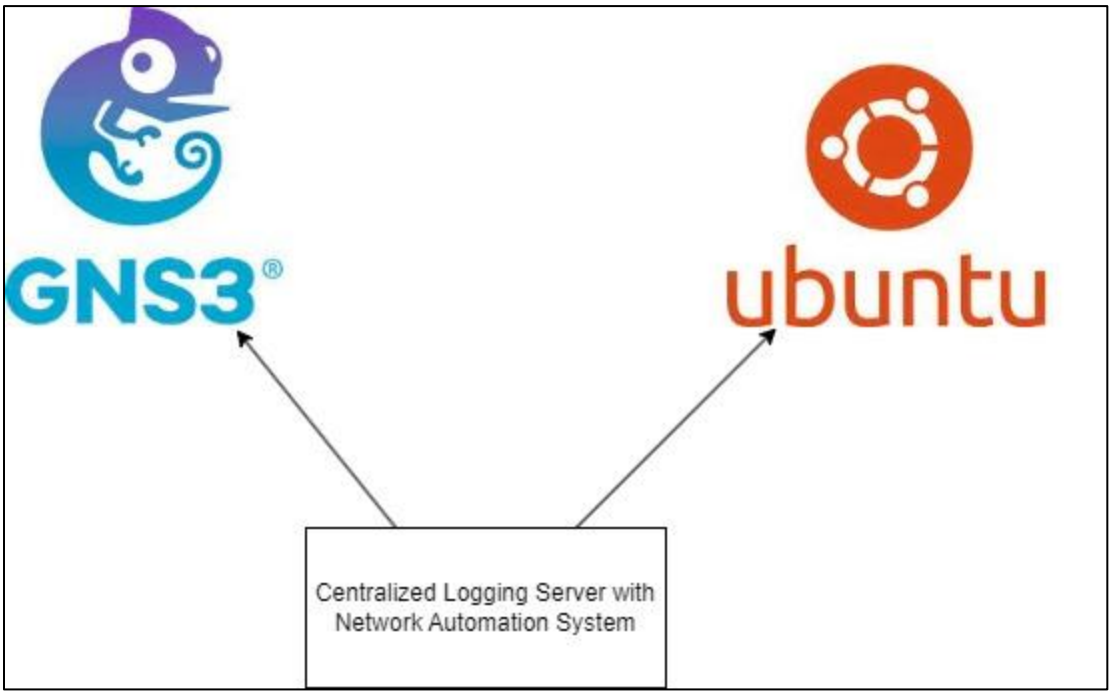


Figure 15: Operating Environment.

9.1.2.5. Design and Implementation Constraints

CO1: The system relies on routers supporting TACACS for authentication.

CO2: ELK server must meet hardware and software specifications recommended by Elastic.

CO3: Potential delays in log analysis during peak usage times.

CO4: Compatibility with legacy network devices may be limited**.**

.

9.1.2.6. Assumptions and Dependencies

AS1: The documentation and reports will only be accessible to admin, client, and supervisors.

AS2: The application is targeted for typical enterprise network environment.

9.1.3. Functional Requirements

9.1.3.1. User authentication and authorization

<table>
<tr><th>Req.ID</th><th colspan="2">Requirement Description</th><th>Priority</th><th>Complexity</th></tr>
<tr><td>FR.01</td><td colspan="2">All users will be required to authenticate themselves with username and password.

<table><tr><th colspan="2">System Requirement</th></tr><tr><td>SR.01</td><td>On opening the network device, users will be prompted with username and password.</td></tr><tr><td>SR.02</td><td>User enters the credentials.</td></tr><tr><td>SR.03</td><td>The system establishes integration with AAA servers to authenticate users.</td></tr><tr><td>SR.04</td><td>The system verifies if the submitted username and password corresponds to the data in the TACACS server.</td></tr><tr><td>SR.05</td><td>Access control policies defined on AAA servers are enforced by the system, restricting unauthorized access to network devices.</td></tr></table></td><td>Most</td><td>High</td></tr>
</table>

Table 3: Function requirement 1.

9.1.3.2. Log Collection and Transmission

<table>
<tr><th>Req.ID</th><th>Requirement Description</th><th>Priority</th><th>Complexity</th></tr>
<tr><td>FR.02</td><td>The system must collect log data from network devices and securely transmit it to the centralized logging server.

<table><tr><th colspan="2">System Requirement</th></tr><tr><td>SR.01</td><td>The system should be connected and integrated with the devices.</td></tr><tr><td>SR.02</td><td>The system shall collect log data from all connected network devices.</td></tr><tr><td>SR.03</td><td>Logs must be stored centrally with proper indexing.</td></tr><tr><td>SR.04</td><td>Logs must be visualized in the Kibana interface.</td></tr></table></td><td>Most</td><td>High</td></tr>
</table>

Table 4: Function requirement 2.

9.1.3.3. Real-time Log Analysis

<table>
<tr><th>Req.ID</th><th>Requirement Description</th><th>Priority</th><th>Complexity</th></tr>
<tr><td>FR.03</td><td>The system shall provide real-time graphing and visualization of log data, support filtering based on various criteria, and generate alerts for predefined security events.

<table><tr><th colspan="2">System Requirement</th></tr><tr><td>SR.01</td><td>Real-time graphing and visualization tools are implemented for efficient log data analysis.</td></tr><tr><td>SR.02</td><td>Filtering options based on various criteria, such as time and type of events, are integrated into the system.</td></tr><tr><td>SR.03</td><td>The system is configured to generate alerts for predefined security events, ensuring quick detection and response.</td></tr></table></td><td>Most</td><td>High</td></tr>
</table>

Table 5: Function requirement 3.

9.1.3.4. Network Automation

<table>
<tr><th>Req.ID</th><th>Requirement Description</th><th>Priority</th><th>Complexity</th></tr>
<tr><td>FR.04</td><td>The automaton server needs to be integrated with centralized logging server and network device.

<table><tr><th colspan="2">System Requirement</th></tr><tr><td>SR.01</td><td>The system must have connectivity with the network devices.</td></tr><tr><td>SR.02</td><td>The system must trigger the appropriate play book according to the event detection</td></tr><tr><td>SR.03</td><td>The system must integrate with devices to run the script.</td></tr></table></td><td>Most</td><td>Normal</td></tr>
</table>

Table 6:Function requirement 4.

9.1.4. External Interfaces Requirements

9.1.4.1. User Interfaces.

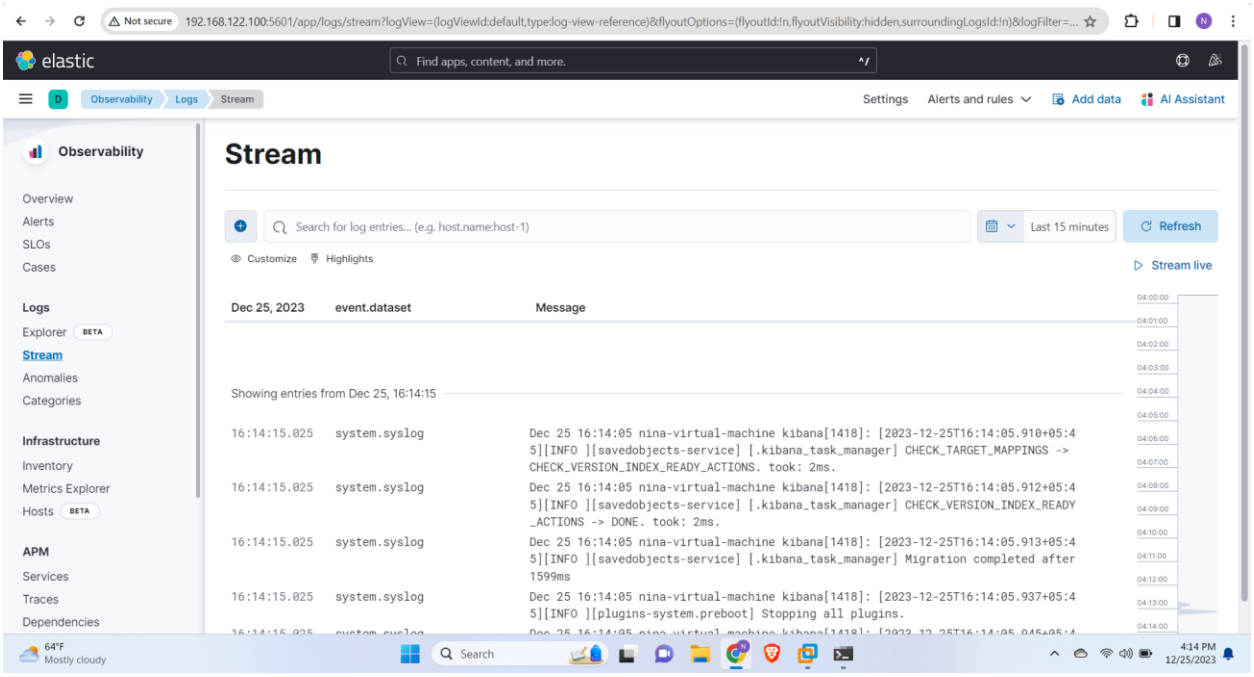


Figure 16: Kibana Interface

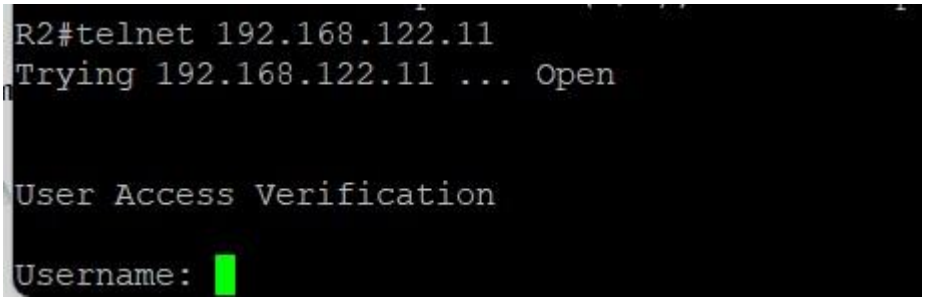


Figure 17: Router interface.

9.1.4.2. Hardware Interfaces

The project has minimal hardware prerequisites as its primary functionality centers around software components. It requires the uses of a standard computer system to host and execute the application. The system needs to have sufficient computing power, like CPU, RAM and storage.

9.1.4.3. Software Interfaces

- Integration with AAA servers will utilize standard AAA protocols.
- The system shall communicate with network devices and the centralized logging server using standard networking protocols.
- Ansible, consisting of playbooks written in YAML configuration will be used as network automation.

9.1.4.4. Communication Interfaces

Secure communication protocols shall be implemented for interactions between the system and network devices.

- ELK utilizes various protocols for log collection, storage, and analysis, including syslog, HTTP/HTTPS, and Beats.
- TACACS+ uses TCP for communication, establishing connections with TACACS+ servers.
- Ansible communicates with network devices using SSH, ensuring secure and encrypted connections for network automation tasks.

9.1.4.5. Other Non-Functional Requirements

- Log retrieval and analysis should have a response time of less than 5 seconds.
- The system should be scalable to accommodate the growth of network devices.
- All communications between the system and network devices must be encrypted.
- Access to the system shall be secured using multi-factor authentication.
- AAA server integration must follow industry-standard security practices.
- The system may experience delays in log analysis during peak usage times.

9.1.4.5.1. Performance Requirements

Req.ID	Requirement Description	Priority	Complexity
PR.01	The system should maintain stability and not crash upon the opening of the application.	Should	High
PR.02	Log retrieval and analysis response time should be normal.	Could	Normal
PR.03	The system should verify the user and authorize accordingly.	Should	High

Table 7: Performance requirement.

9.1.4.5.2. Safety and Security Requirements

Safety Requirements

Req.ID	Requirement Description	Priority	Complexity
SR.01	The user authentication mechanisms should be robust to avoid any unauthorized access to the system's data and functionality.	Should	High
SR.02	Secure connection should be established among devices and server.	Should	High

Table 8: Safety requirement.

Other Software Quality Attributes

Req.ID	Requirement Description	Priority	Complexity
SQA.01	The application should be responsive and easy to operate.	Should	High
SQA.02	The application should demonstrate high availability and have minimal downtime.	Should	High

Table 9: Other Software Quality Attributes.

9.2. Survey Findings

The pre-survey was completed and got a good response from 24 participants. The findings of this project are shown in the figures below.

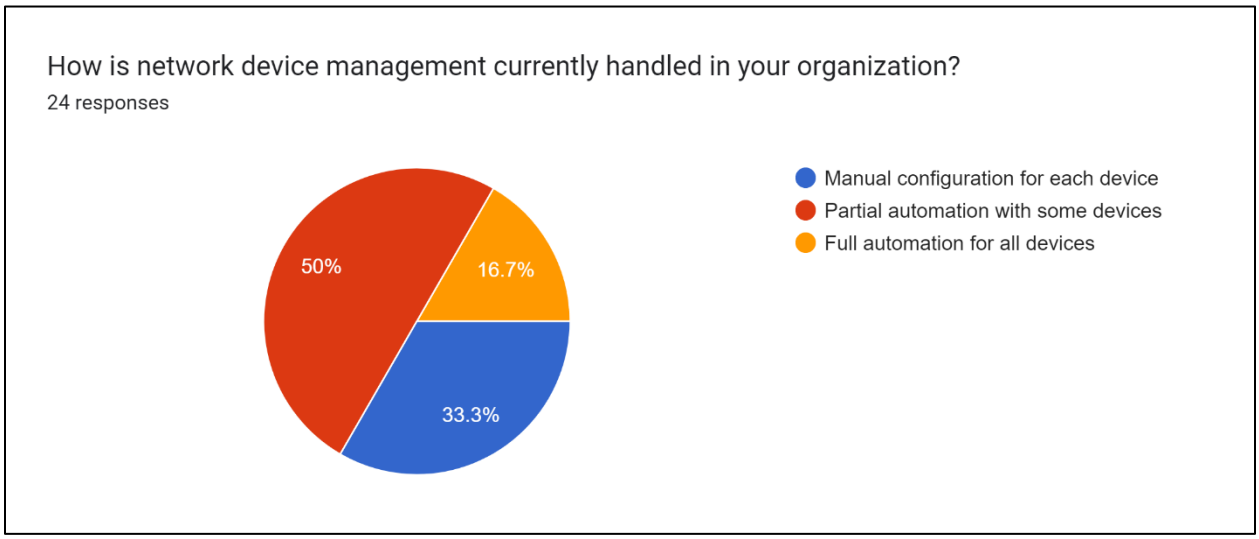


Figure 18: Survey question 1.

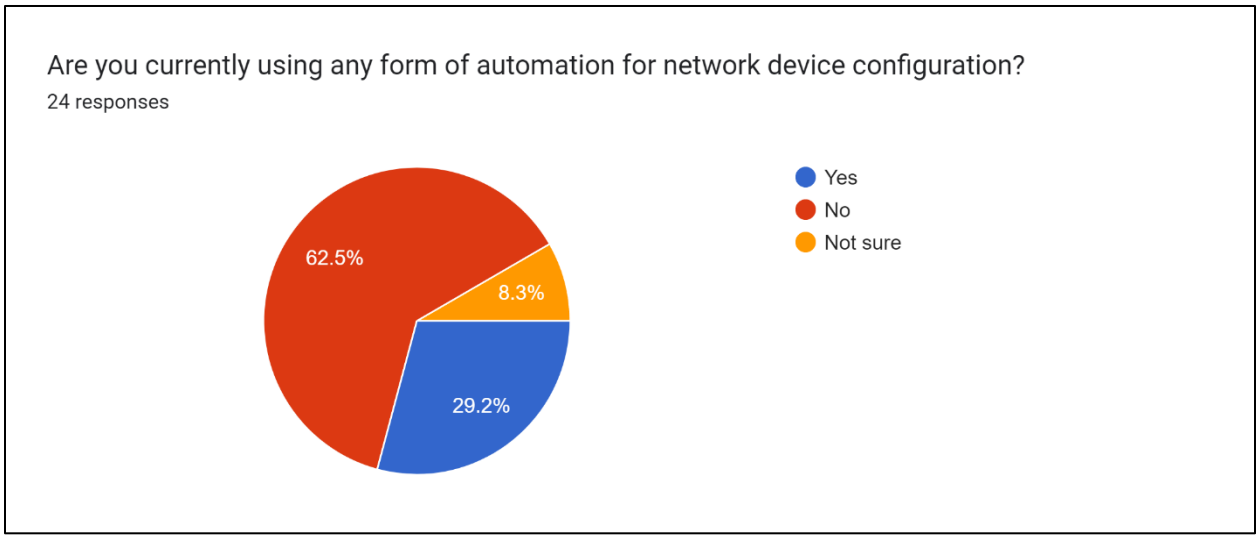


Figure 19: Survey question 2.

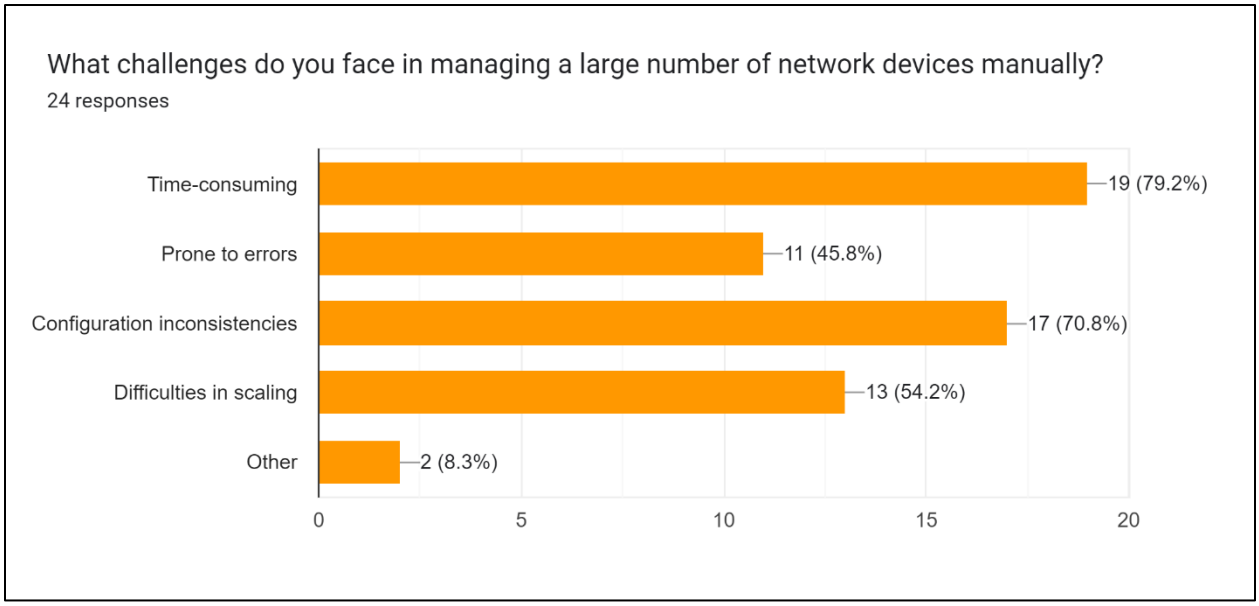


Figure 20: Survey question 3.

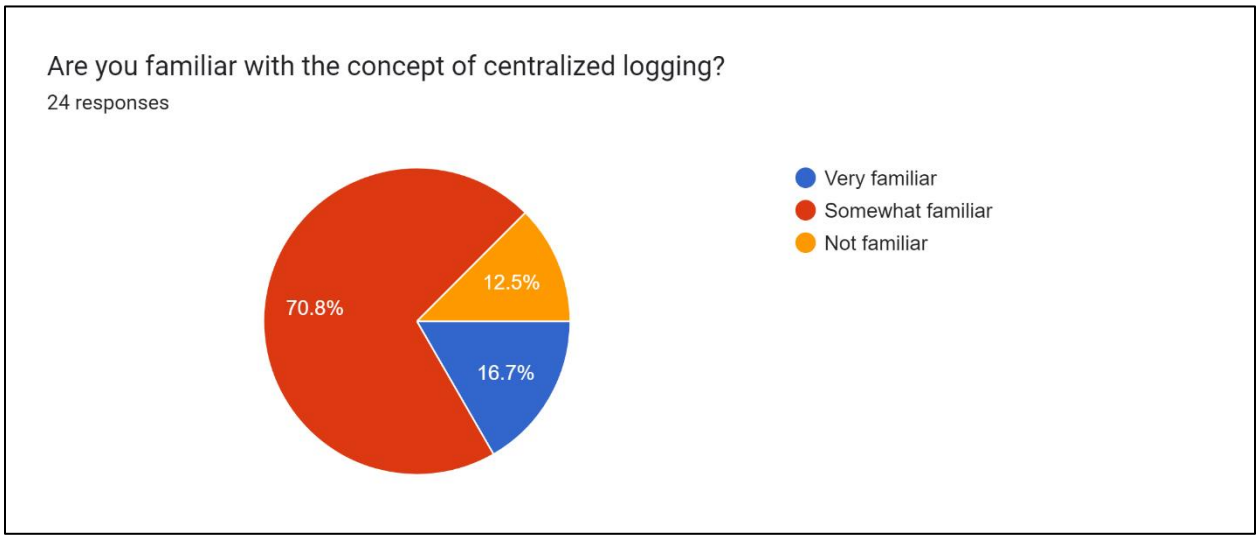


Figure 21: Survey question 4.

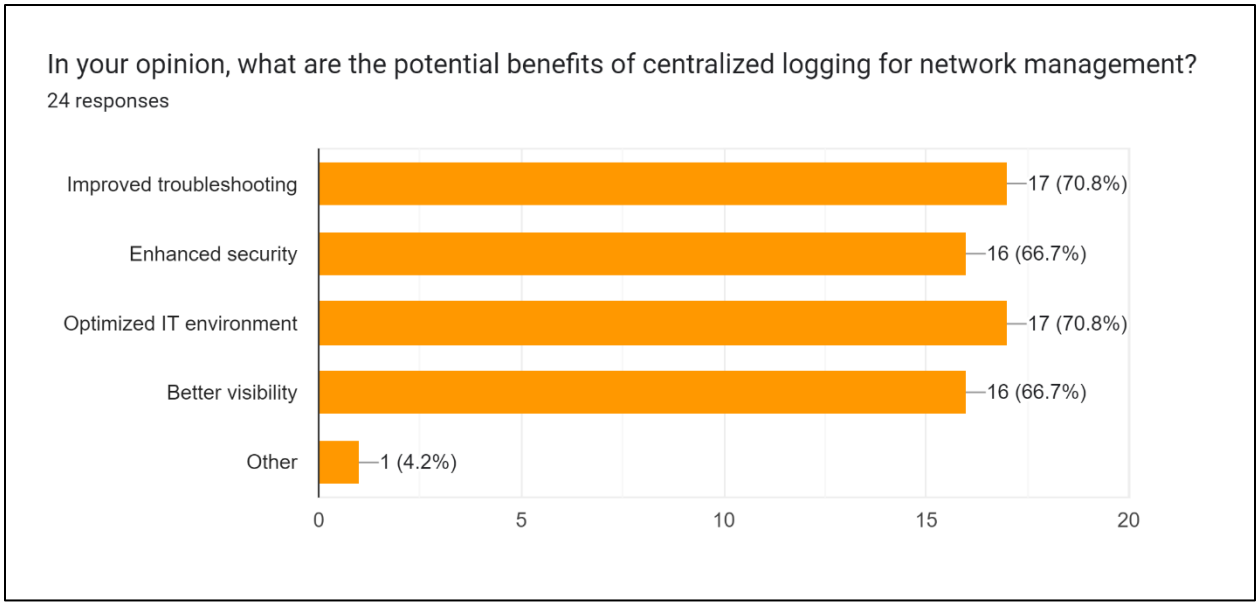


Figure 22: Survey question 5.

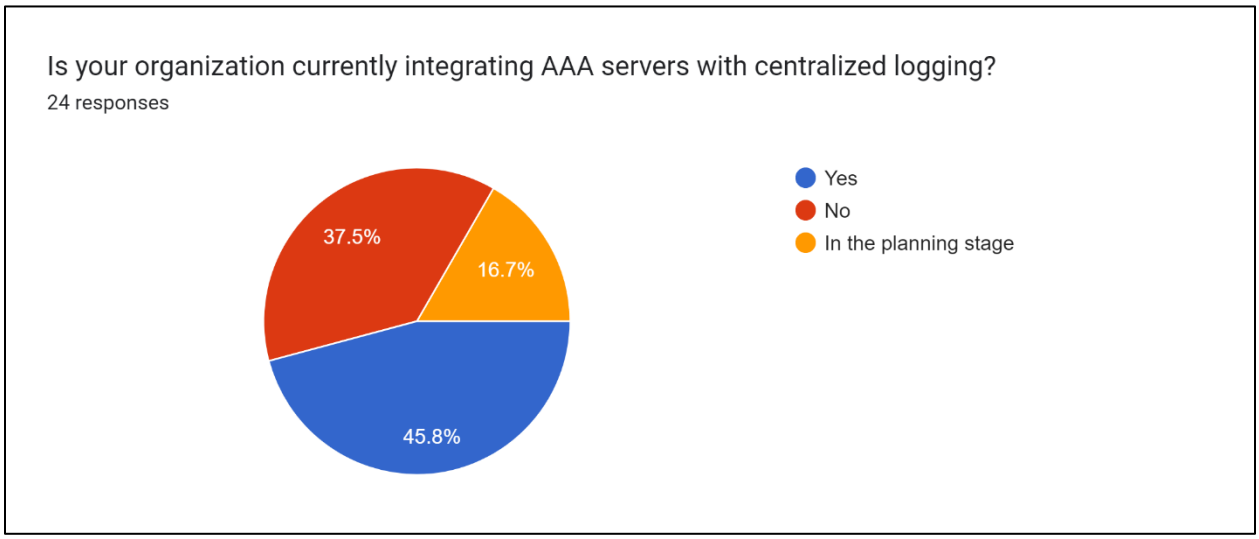


Figure 23:Survey question 6.

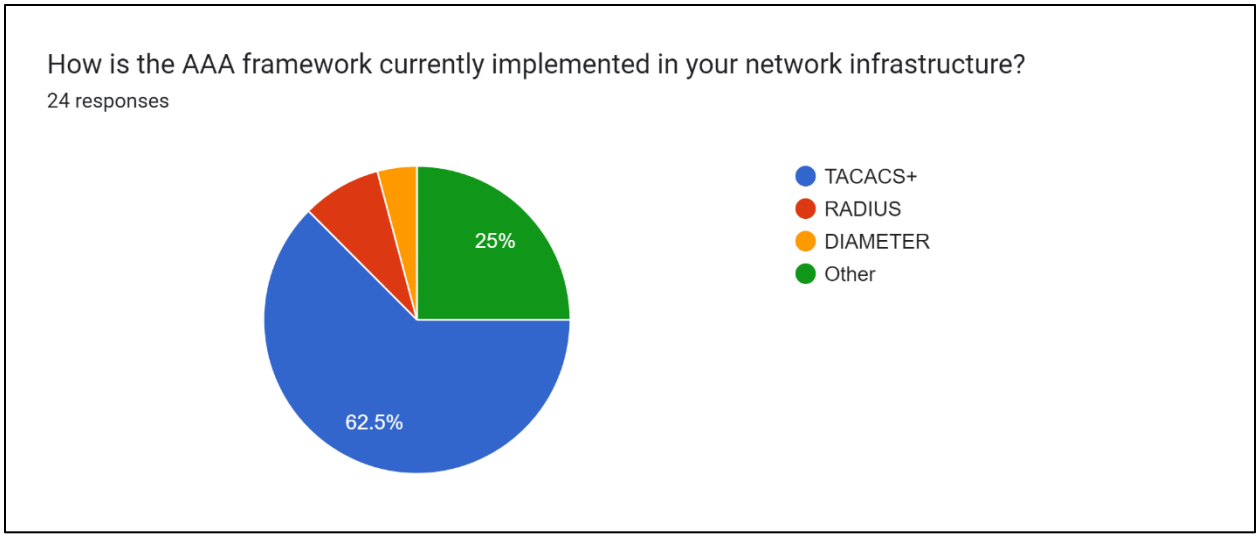


Figure 24: Survey question 7.

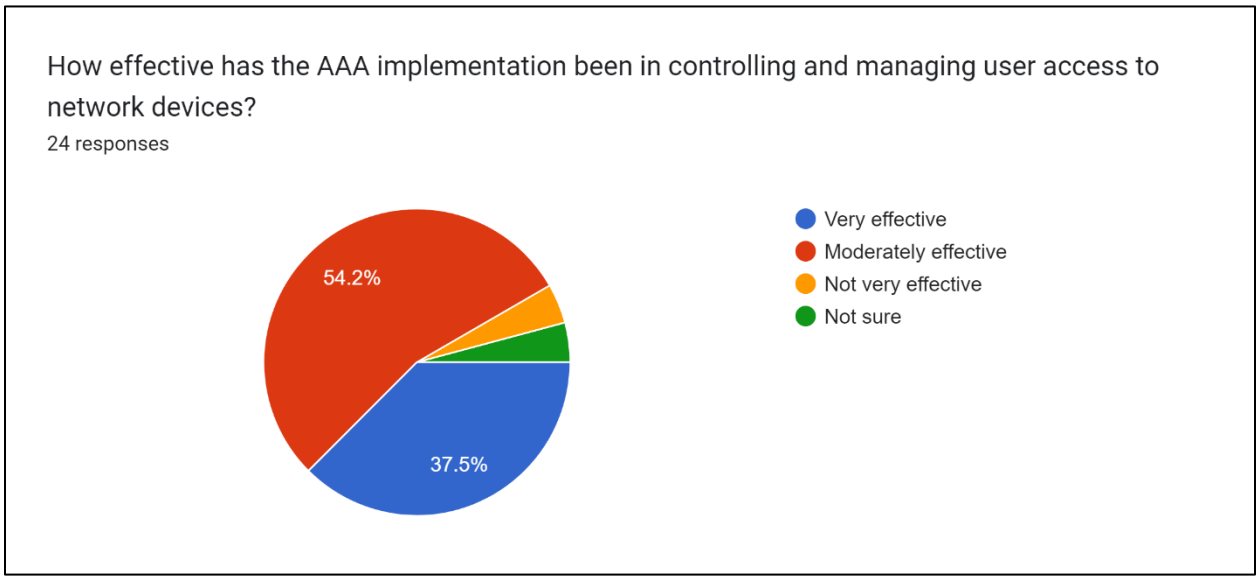


Figure 25: Survey question 8.

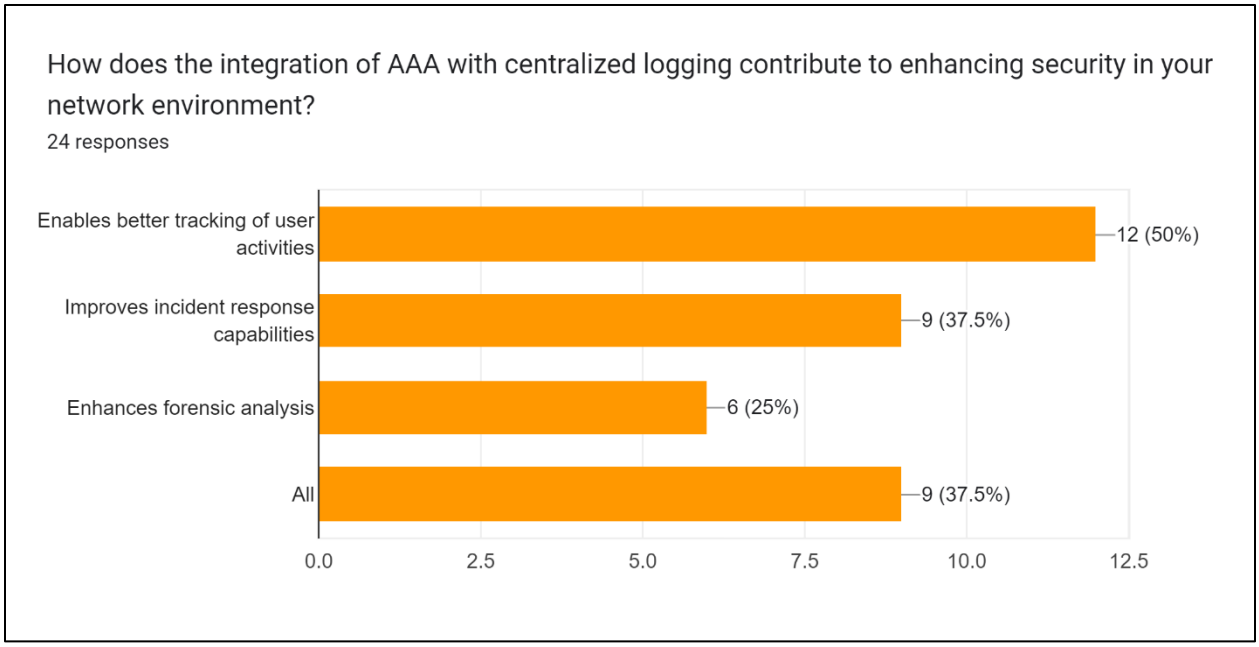


Figure 26: Survey question 9.

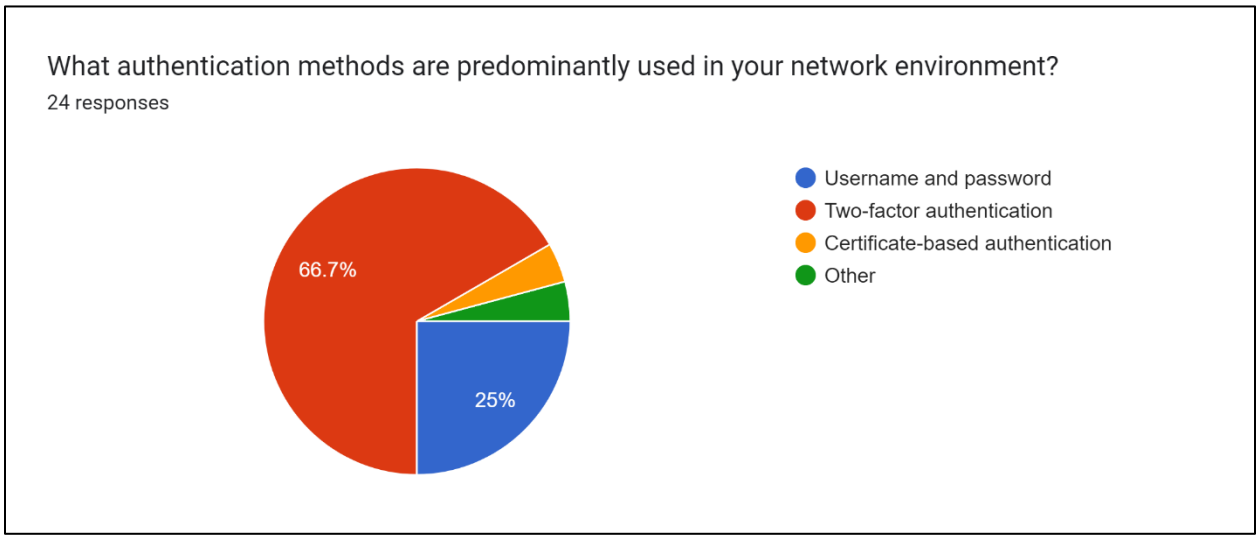


Figure 27: Survey question 10.

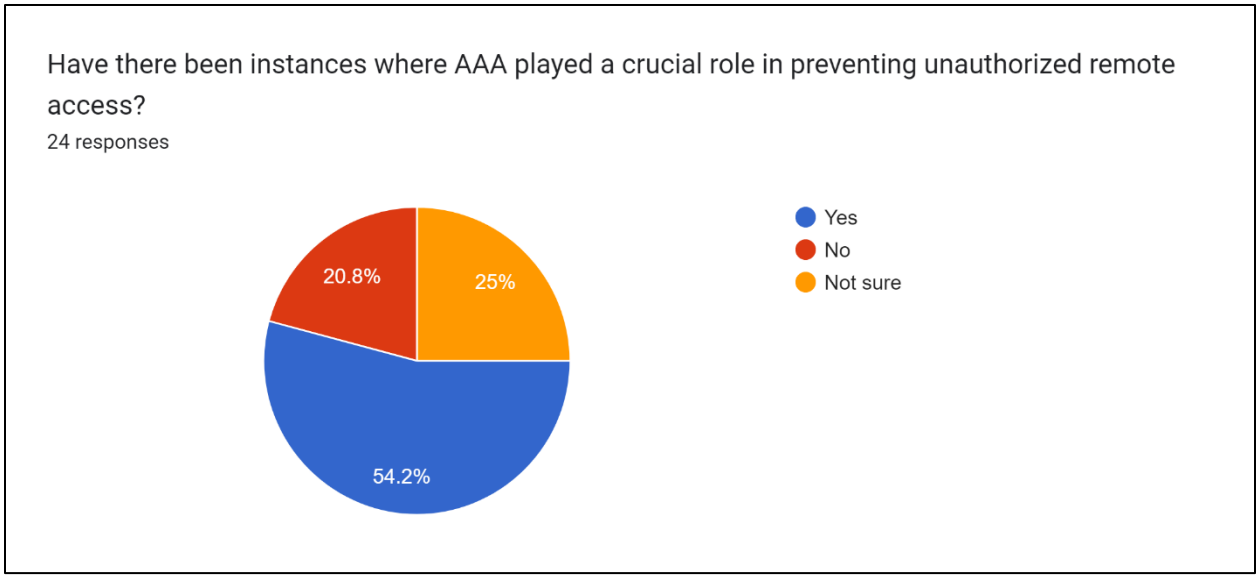


Figure 28: Survey question 11.

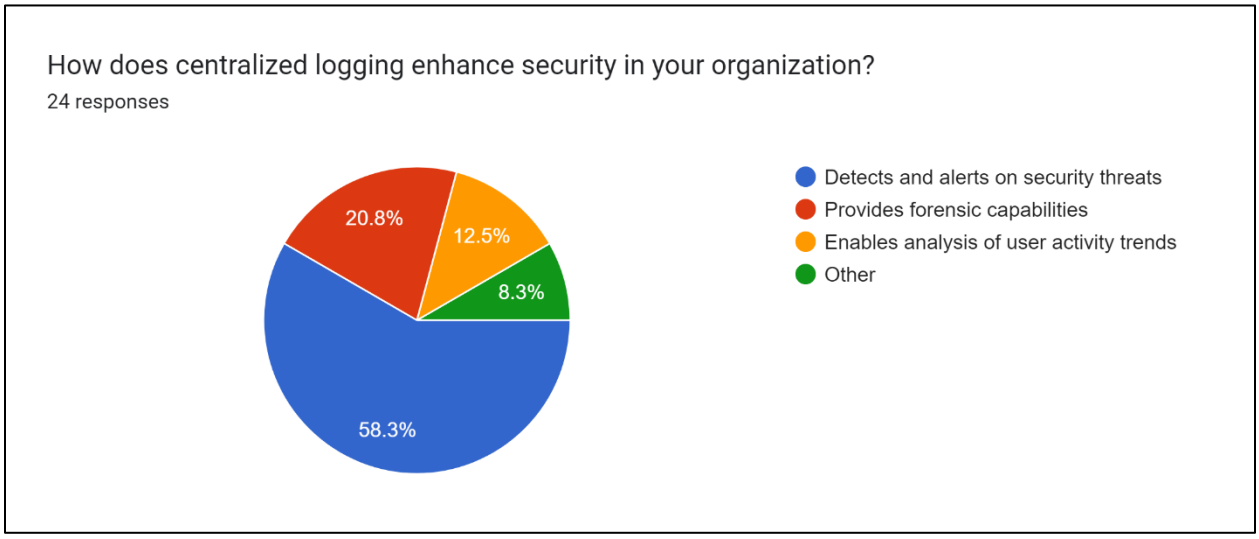


Figure 29: Survey question 12.

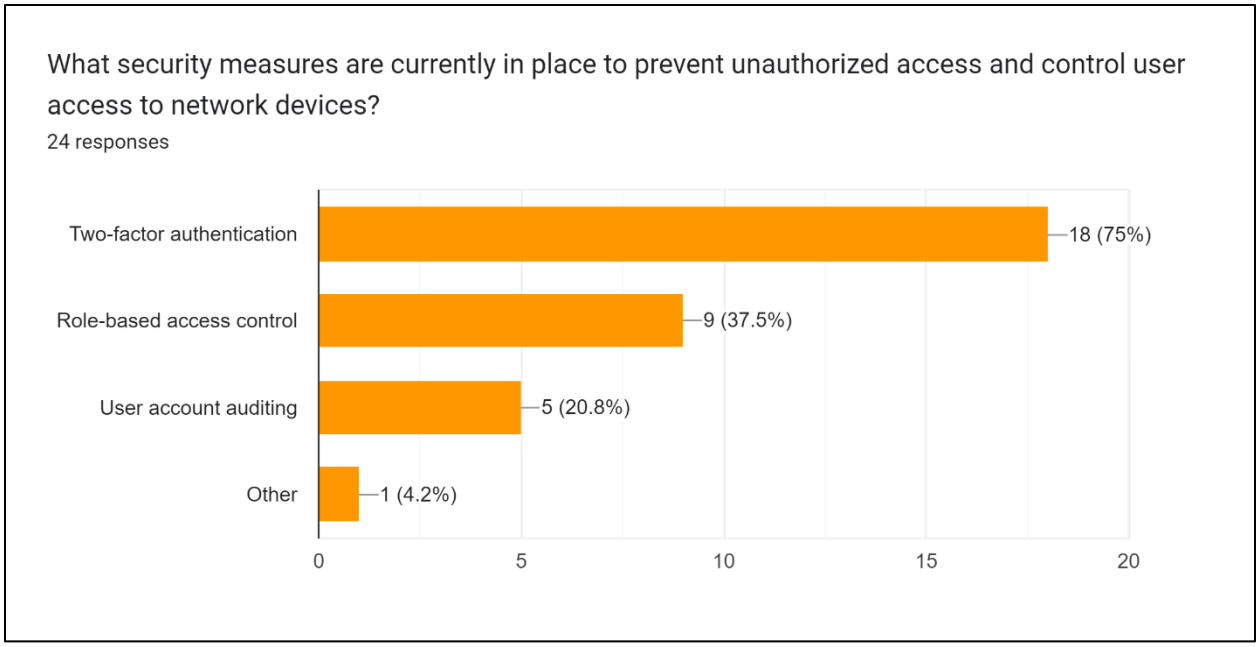


Figure 30: Survey question 13.

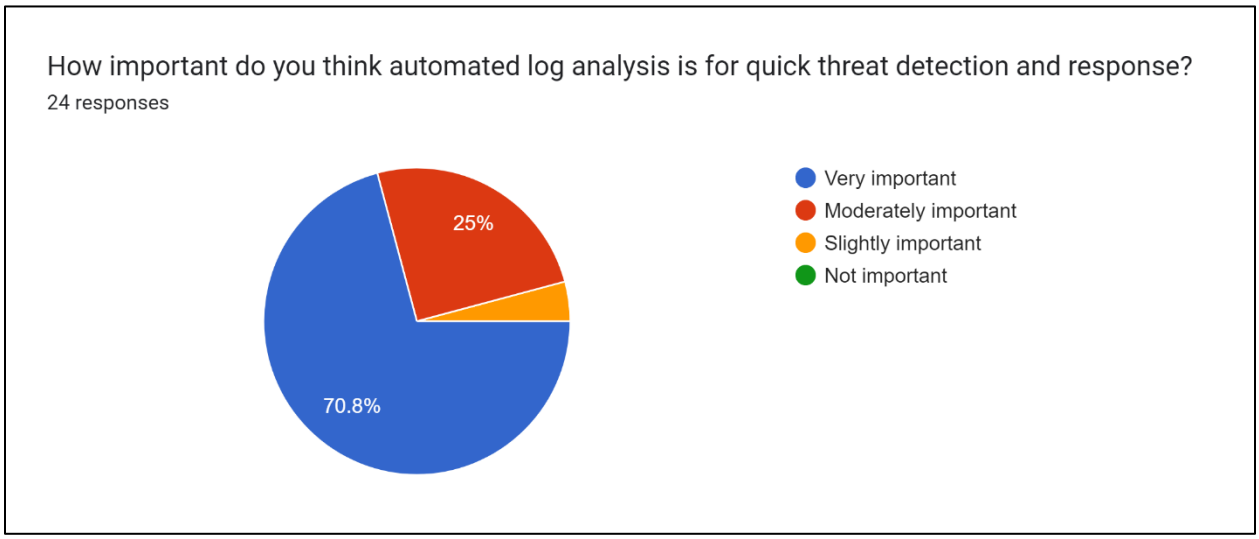


Figure 31: Survey question 14.

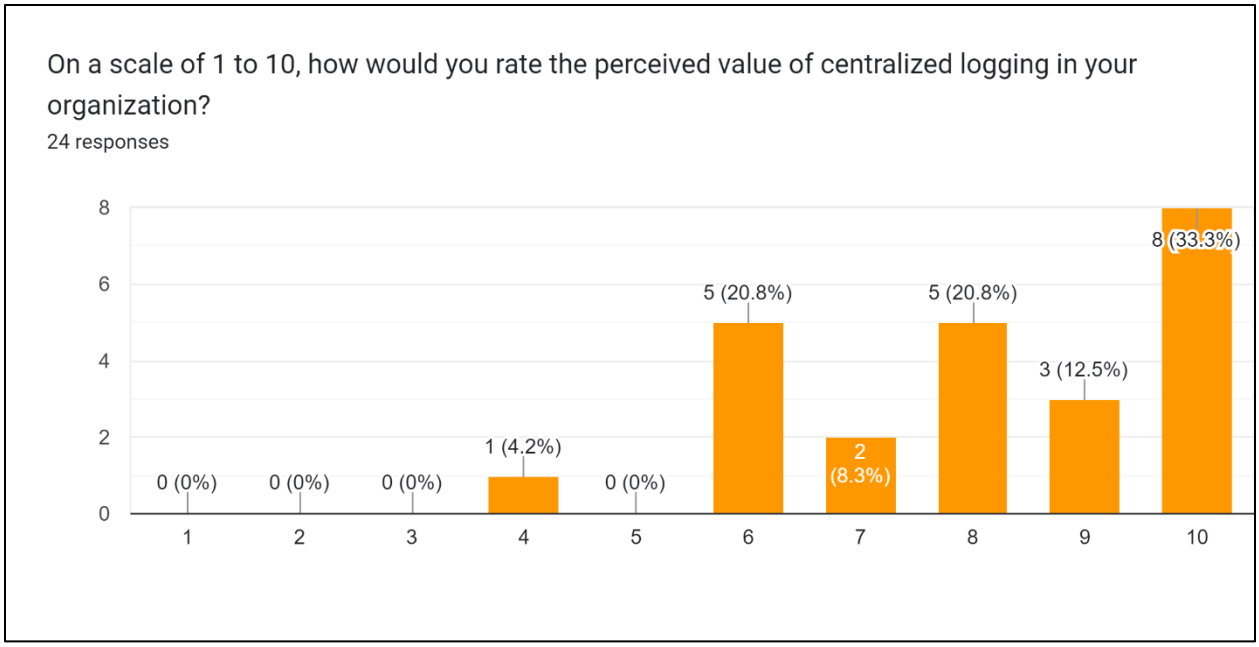


Figure 32: Survey question 15.

9.3. Development Work

Initially, network topology was designed and then created in GNS3. Then the devices were given static IP and configured.

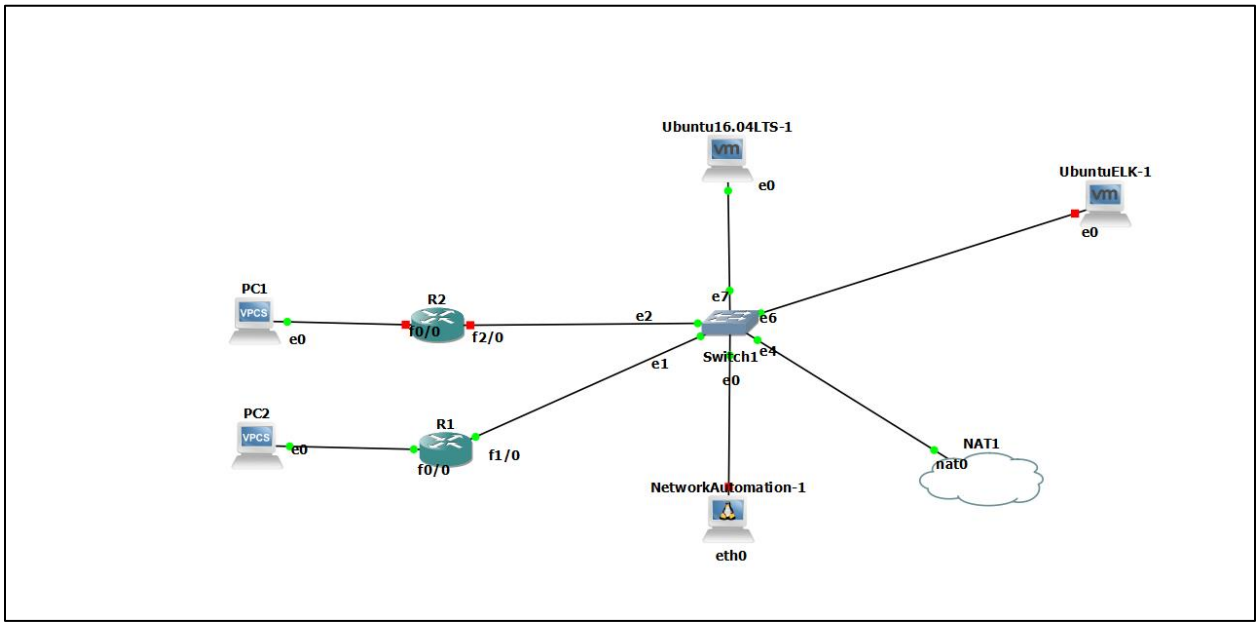


Figure 33: Network Architecture set up on GNS3.

```
R1#
R1#ping 192.168.122.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/44 ms
R1#
```

```
R1#ping 192.168.122.22
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/31/48 ms
R1#
```

```
R2#
R2#ping 192.168.122.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/32/48 ms
R2#
```

Figure 34: Checking network connectivity.

```
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated
aaa accounting send stop-record authentication failure
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 0 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
```

Figure 35: AAA configuration on router

```
!
tacacs-server host 192.168.122.5
tacacs-server key testing123
```

Figure 36: Setting up the host and the key on router.

```
ninal@ninal-virtual-machine:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
00
    link/ether 00:0c:29:7c:93:28 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.5/24 brd 192.168.122.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::e1ee:86e3:b982:140a/64 scope link
       valid_lft forever preferred_lft forever
ninal@ninal-virtual-machine:~$
```

Figure 37: Setting the static IP on AAA server.

```
  GNU nano 2.5.3                File: /etc/tacacs+/tac_plus.conf

# Created by Henry-Nicolas Tourneur(henry.nicolas@tourneur.be)
# See man(5) tac_plus.conf for more details

# Define where to log accounting data, this is the default.

accounting file = /var/log/tac_plus.log

# This is the key that clients have to use to access Tacacs+

key = testing123

# Use /etc/passwd file to do authentication

#default authentication = file /etc/passwd


# You can use feature like per host key with different enable passwords
#host = 127.0.0.1 {
#        key = test
#        type = cisco
#        enable = <des|cleartext> enablepass
#        prompt = "Welcome XXX ISP Access Router \n\nUsername:"
#}
```

Figure 38: Configuring tac_plus file, setting the location of accounting log and key as testing123.

```
user = Administrator {
     login = cleartext "Cisco"
     member = "admin"
}

user = nina_{
     login = cleartext "cisco"
     enable = cleartext "cisco"
     member = readonly
}

group = admin {
     default service = permit
     service = exec {
            default attribute = permit
            priv-lvl = 15
  }
}
```

Figure 39: Setting up user and permission.

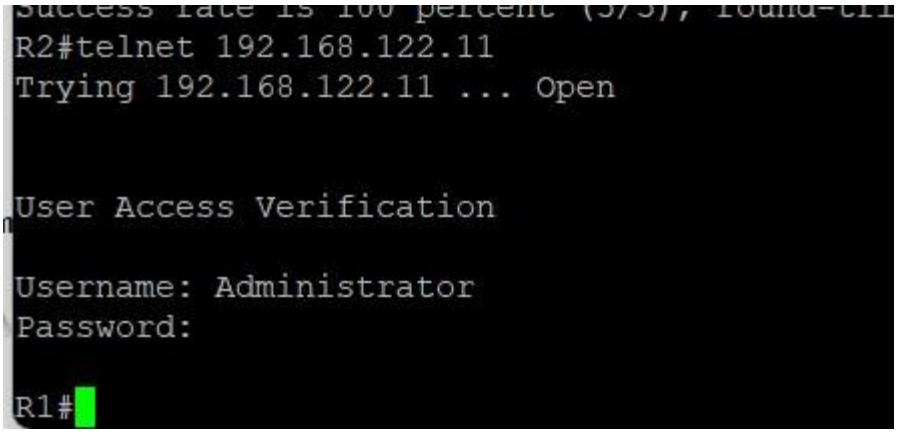


Figure 40: Screenshot of successful authentication via SSH.

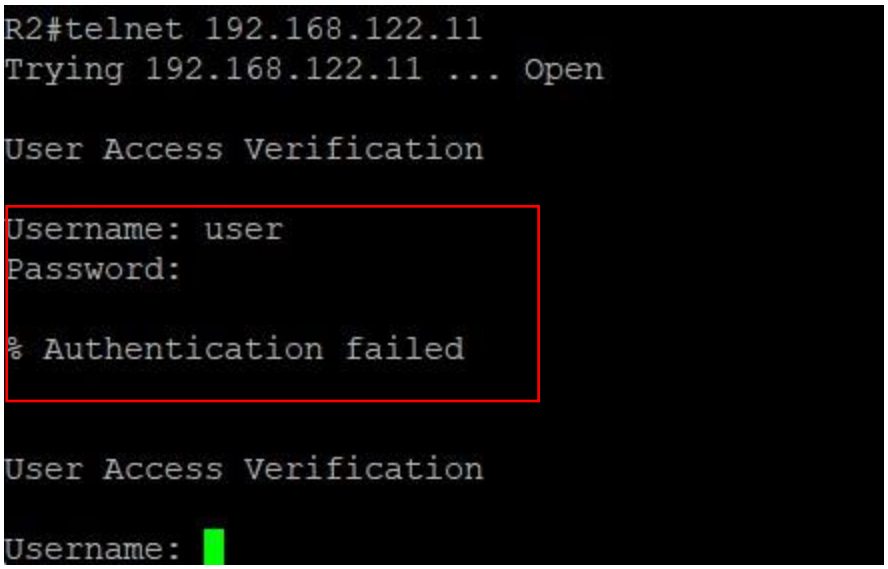


Figure 41: Screenshot of Authentication error while accessing from unknown user.

```
ninal@ninal-virtual-machine:~$ cat /var/log/tac_plus.log
Jan  2 11:32:48 192.168.122.11  unknown unknown unknown start   task_id=1       timezone=UTC    serv
ice=system      event=sys_acct  reason=reload   reload-reason=unknown reload cause - suspect boot_da
ta[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19   ios-version=Cisco IOS Software, 7200 Software (C7200
-ADVENTERPRISEK9-M), Version 15.2(4)S3, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Fri 19-Apr-13 05:11 by prod_
Jan  2 11:33:19 192.168.122.11  unknown tty0    async   stop    task_id=7       timezone=UTC    serv
ice=shell       pre-session-time=35     elapsed_time=0  stop_time=1704195127    stop_time=1704195127
disc-cause=4    disc-cause-ext=47
Jan  2 11:33:48 192.168.122.11  Administrator   tty0    async   start   task_id=8       timezone=UTC
service=shell
Jan  2 11:34:05 192.168.122.11  Administrator   tty0    async   stop    task_id=8       timezone=UTC
service=shell   priv-lvl=15     cmd=show running-config <cr>
Jan  2 11:36:35 192.168.122.11  Administrator   tty0    async   stop    task_id=9       timezone=UTC
service=shell   priv-lvl=15     cmd=ping 192.168.122.5 <cr>
Jan  2 11:36:50 192.168.122.11  Administrator   tty0    async   stop    task_id=10      timezone=UTC
service=shell   priv-lvl=15     cmd=ping 192.168.122.2 <cr>
Jan  2 11:37:02 192.168.122.11  Administrator   tty0    async   stop    task_id=11      timezone=UTC
service=shell   priv-lvl=15     cmd=ping 192.168.122.22 <cr>
Jan  2 11:37:07 192.168.122.11  Administrator   tty0    async   stop    task_id=12      timezone=UTC
service=shell   priv-lvl=15     cmd=ping 192.168.122.22 <cr>
Jan  2 11:38:17 192.168.122.11  Administrator   tty2    192.168.122.22  start   task_id=14      time
zone=UTC        service=shell
Jan  2 11:38:30 192.168.122.11  Administrator   tty2    192.168.122.22  stop    task_id=14      time
zone=UTC        service=shell   priv-lvl=0      cmd=exit <cr>
Jan  2 11:38:30 192.168.122.11  Administrator   tty2    192.168.122.22  stop    task_id=14      time
zone=UTC        service=shell   disc-cause=1    disc-cause-ext=9        pre-session-time=28     elap
sed_time=13     stop_time=1704195440
Jan  2 11:39:37 192.168.122.11  unknown tty2    192.168.122.22  stop    task_id=16      timezone=UTC
service=shell   pre-session-time=62     elapsed_time=0  stop_time=1704195507    stop_time=1704195507
disc-cause=4    disc-cause-ext=47
ninal@ninal-virtual-machine:~$ _
```

```
Dec 12 16:07:33 192.168.122.11  Administrator   tty2    192.168.122.22  start   task_id=7       time
zone=UTC        service=shell
Dec 12 16:07:38 192.168.122.11  Administrator   tty2    192.168.122.22  stop    task_id=7       time
zone=UTC        service=shell   disc-cause=1    disc-cause-ext=9        pre-session-time=10     elap
sed_time=5      stop_time=1702397258
Dec 12 16:07:52 192.168.122.11  Administrator   tty0    async   start   task_id=8       timezone=UTC
service=shell
Dec 15 12:43:36 192.168.122.11  Administrator   tty2    192.168.122.22  start   task_id=1       time
zone=UTC        service=shell
Dec 15 12:53:19 192.168.122.11  Administrator   tty2    192.168.122.22  stop    task_id=1       time
zone=UTC        service=shell   disc-cause=1    disc-cause-ext=9        pre-session-time=15     elap
sed_time=584    stop_time=1702645891
Dec 15 12:53:37 192.168.122.11  Administrator   tty2    192.168.122.22  start   task_id=2       time
zone=UTC        service=shell
Dec 15 12:54:06 192.168.122.11  Administrator   tty2    192.168.122.22  stop    task_id=2       time
zone=UTC        service=shell   disc-cause=1    disc-cause-ext=9        pre-session-time=16     elap
sed_time=30     stop_time=1702645938
Dec 15 12:54:18 192.168.122.11  Administrator   tty2    192.168.122.22  start   task_id=3       time
zone=UTC        service=shell
Dec 15 16:46:12 192.168.122.11  Administrator   tty2    192.168.122.22  start   task_id=2       time
zone=UTC        service=shell
Dec 15 16:46:29 192.168.122.11  Administrator   tty2    192.168.122.22  stop    task_id=2       time
zone=UTC        service=shell   disc-cause=1    disc-cause-ext=9        pre-session-time=21     elap
sed_time=16     stop_time=1702658749
```

Figure 42: Authentication logs

```
nina@nina-virtual-machine:~/Downloads/ELK$ curl -X GET "localhost:9200"
{
  "name" : "nina-virtual-machine",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "DLi19o_hRKi3DkbMwfToSQ",
  "version" : {
    "number" : "8.11.1",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "6f9ff581fbcde658e6f69d6ce03050f060d1fd0c",
    "build_date" : "2023-11-11T10:05:59.421038163Z",
    "build_snapshot" : false,
    "lucene_version" : "9.8.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Figure 43: Screenshot of Elasticsearch installation.

```
nina@nina-virtual-machine:~/Downloads/ELK$ sudo apt-get install logstash
[sudo] password for nina:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 117 not upgraded.
Need to get 350 MB of archives.
After this operation, 607 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 logstash amd64 1:8.11.1-1 [350 MB]
Fetched 350 MB in 45s (7,704 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 202041 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a8.11.1-1_amd64.deb ...
Unpacking logstash (1:8.11.1-1) ...
Setting up logstash (1:8.11.1-1) ...
nina@nina-virtual-machine:~/Downloads/ELK$ sudo systemctl start logstash
nina@nina-virtual-machine:~/Downloads/ELK$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /lib/systemd/system/logstash.service.
nina@nina-virtual-machine:~/Downloads/ELK$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/lib/systemd/system/logstash.service; enabled; vendo>
     Active: active (running) since Sun 2023-12-03 14:04:03 +0545; 26s ago
   Main PID: 2988 (java)
      Tasks: 22 (limit: 4556)
     Memory: 556.7M
        CPU: 39.985s
     CGroup: /system.slice/logstash.service
             └─2988 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava>

दि सम्बर 03 14:04:03 nina-virtual-machine systemd[1]: Started logstash.
दि सम्बर 03 14:04:04 nina-virtual-machine logstash[2988]: Using bundled JDK>
 ^X
[1]+  Stopped                 sudo systemctl status logstash
nina@nina-virtual-machine:~/Downloads/ELK$ sudo nano /etc/logstash/logstash.yml
```

Figure 44: Screenshot of Logstash installation.

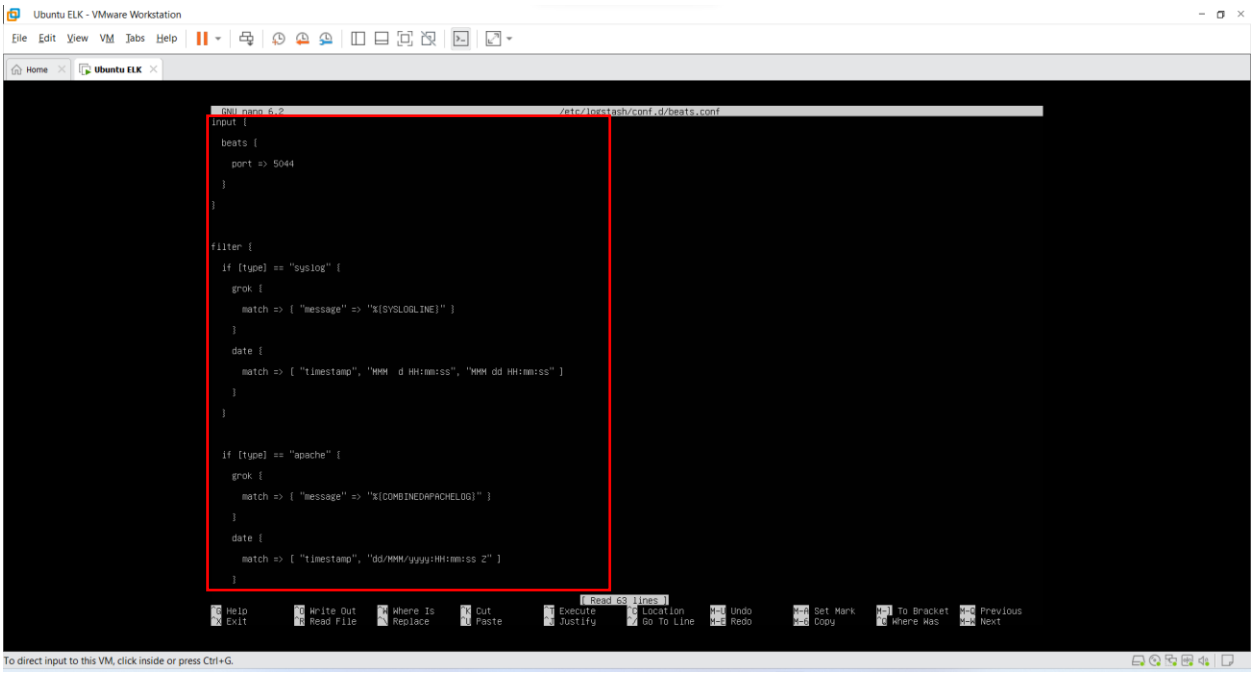


Figure 45: Configuring Logstash.

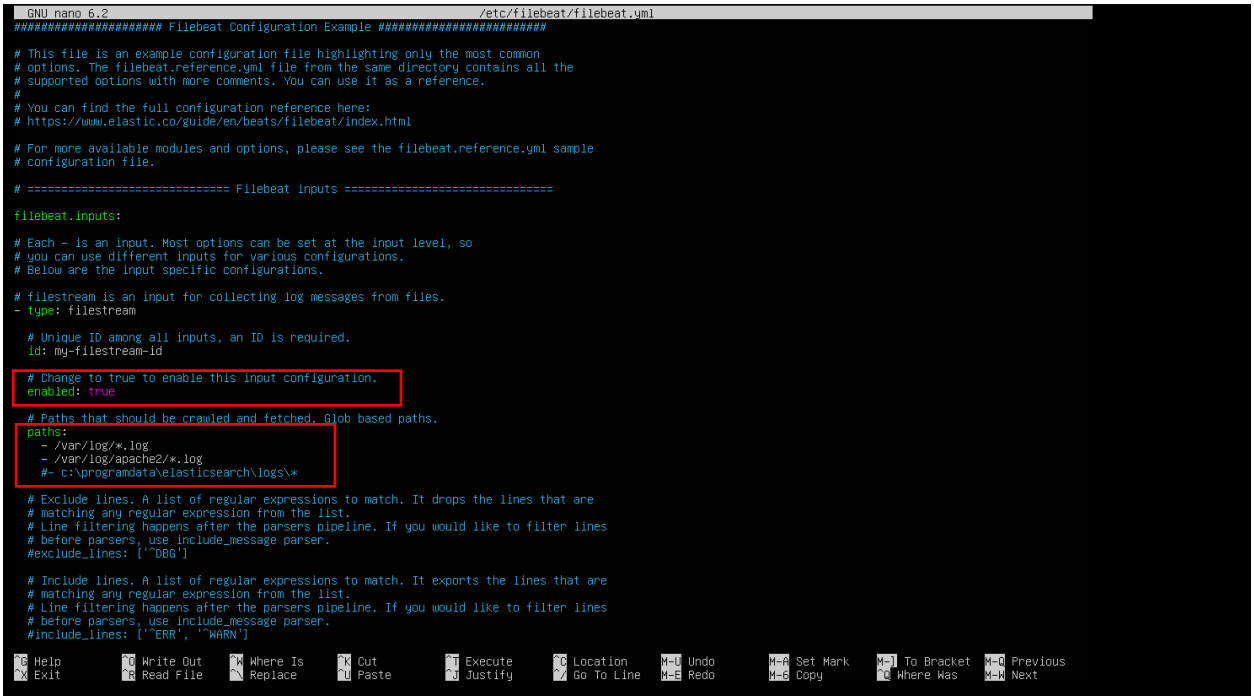


Figure 46: Configuring FileBeat setting enabled as true.

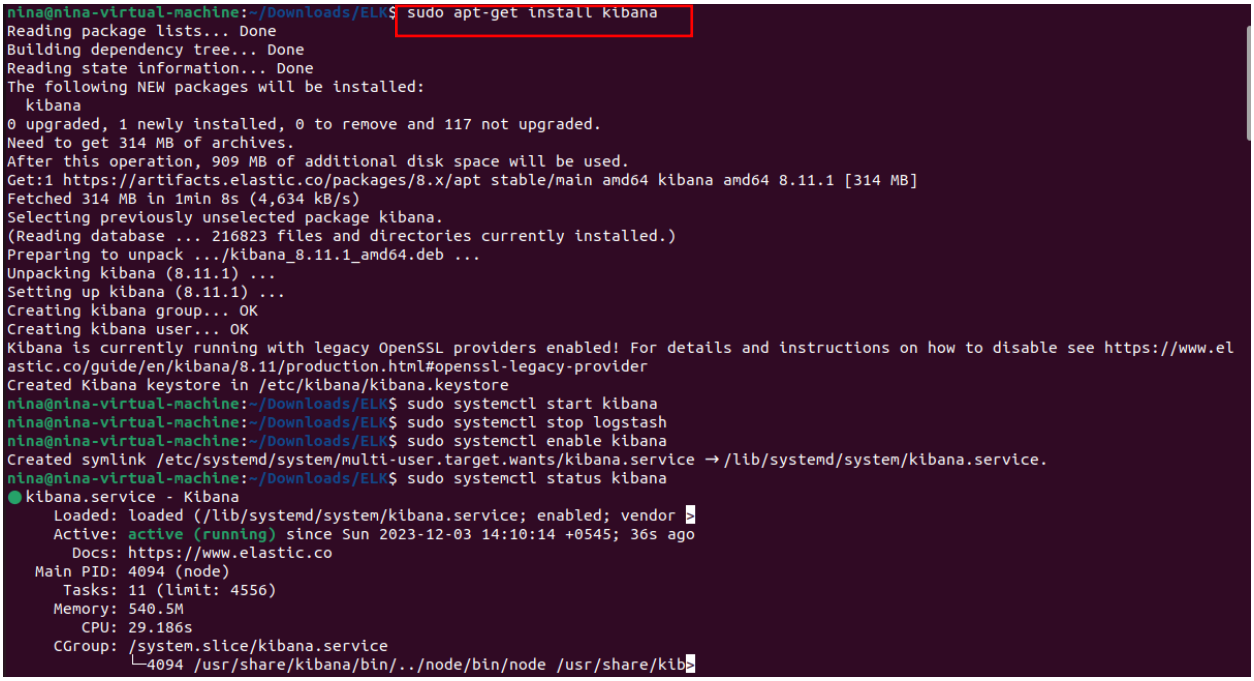


Figure 47: Screenshot of Kibana installation.

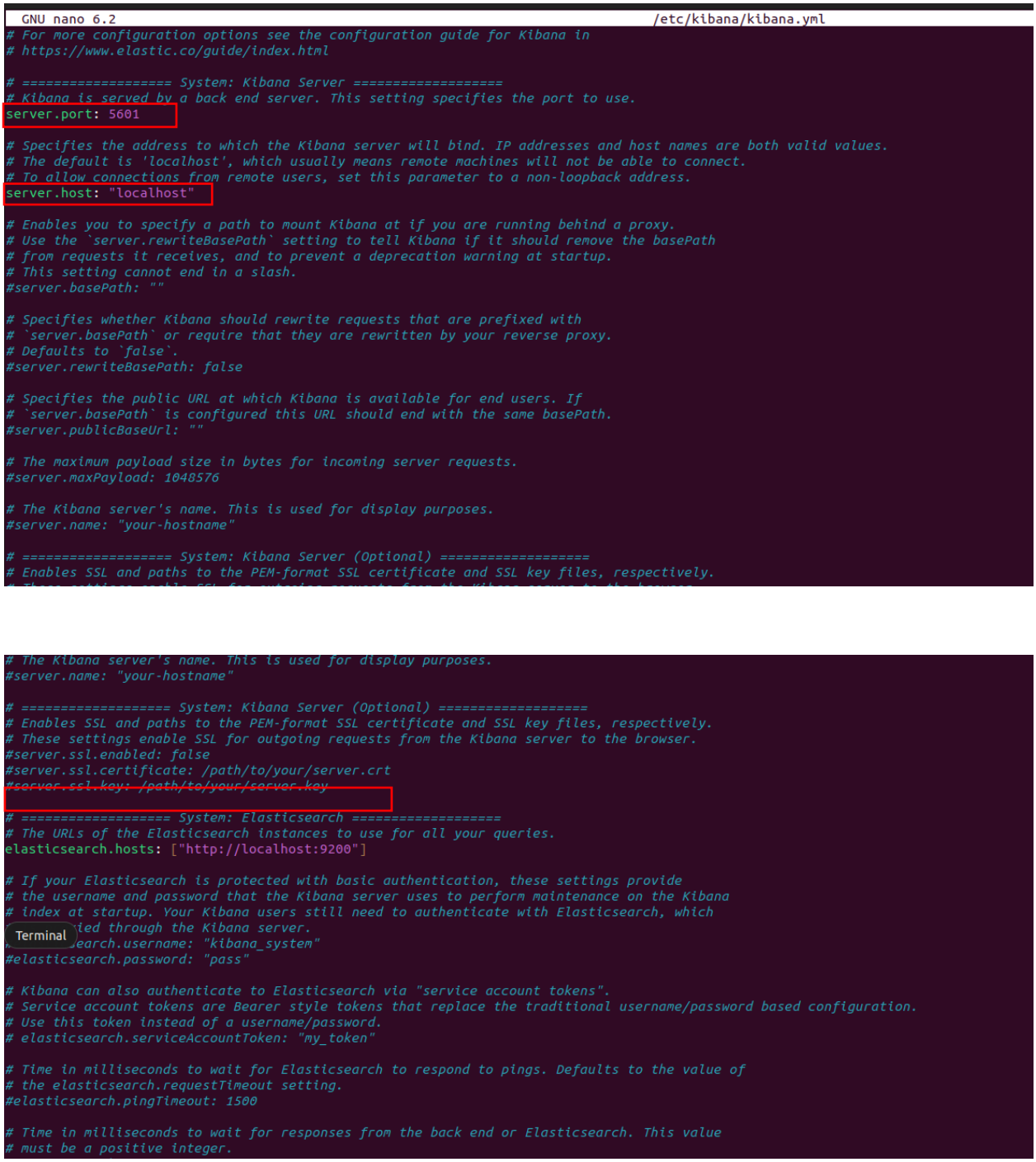


Figure 48: Configuring Kibana setting the port and localhost.

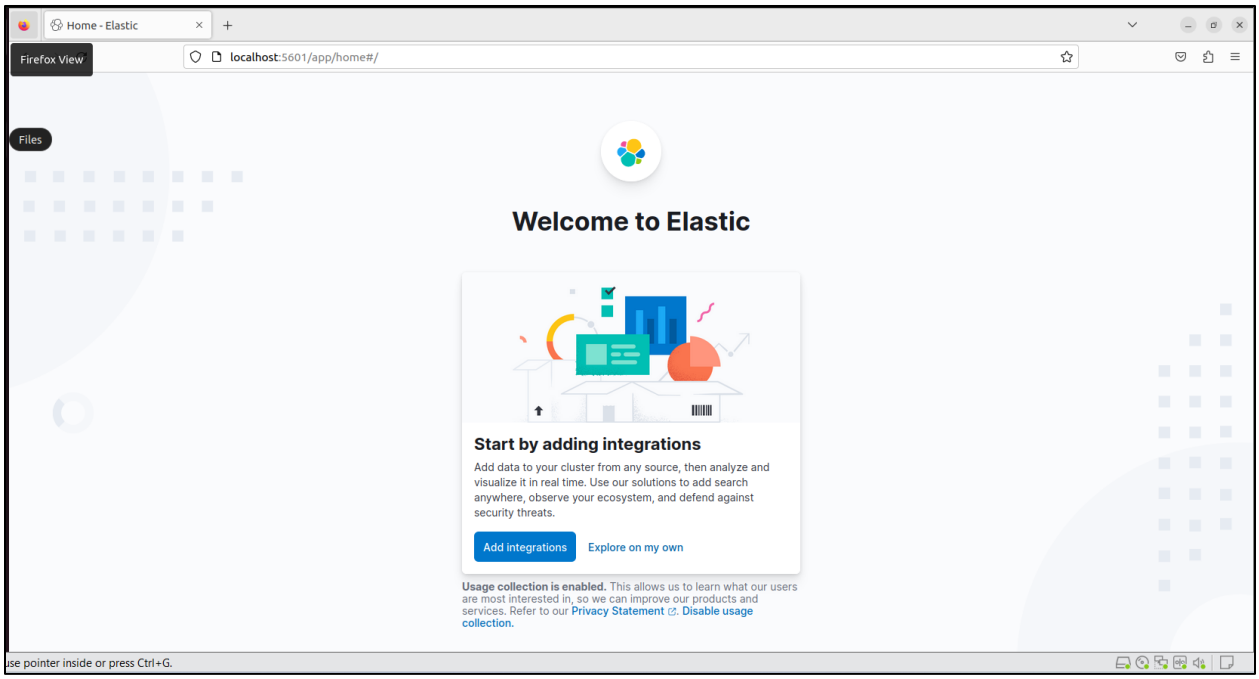


Figure 49: Successfully accessed Kibana from web interface.

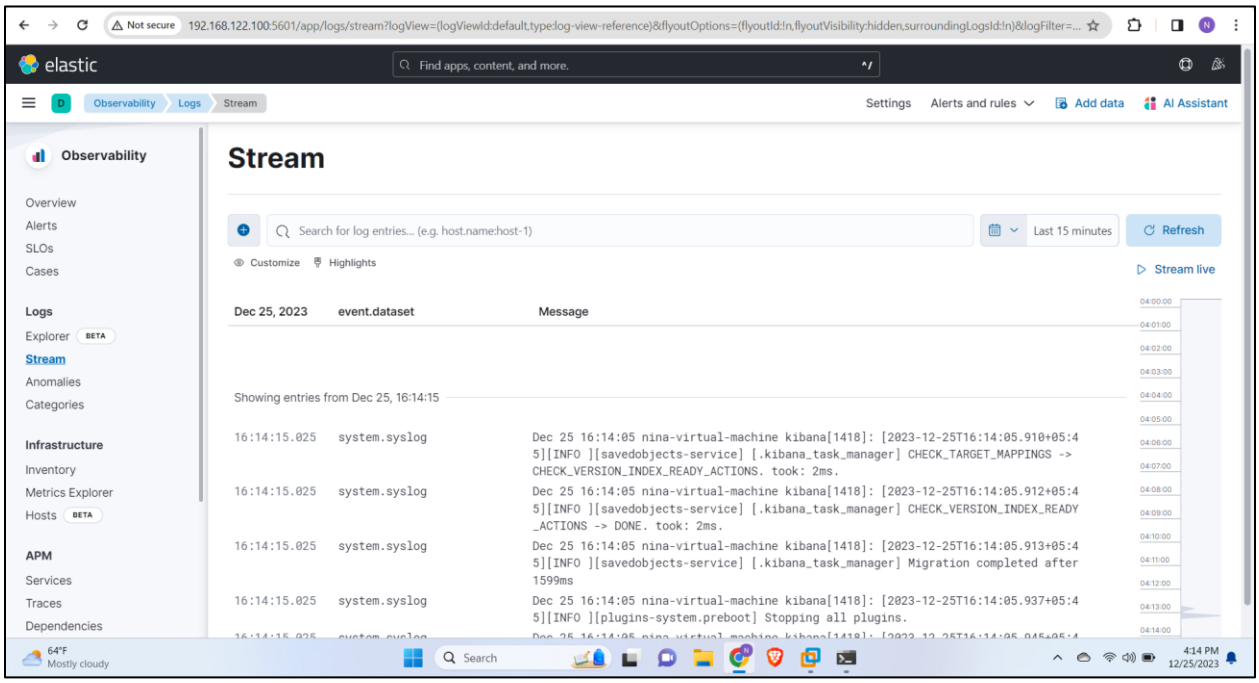


Figure 50: Screenshot of System logs.

9.4. Client Agreement Letter

Vertex Special Technology (P.) Ltd.
Lalitpur, Bagmati Province, Nepal
Phone: +977-01-5912720
Email: info@vertexspecial.com
Website: vertexspecial.com

Reg No: 291736/78/079
VAT No: 610293762

VERTEX

Vertex Special Technology Pvt. Ltd
Mahalaxmisthan
Lalitpur, Nepal

Date: December 28, 2023

Ms. Nina Lageju
Islington College Pvt. Ltd
Kamalpokhari
Kathmandu

TO WHOM IT MAY CONCERN

Dear Nina,

I am writing this letter on behalf of Vertex Special Technology Pvt. I am writing to confirm my acceptance for the Final Year Project of your student [redacted], I and [redacted] reached an agreement and our company will be her client in the "Centralized Logging Server with Network Automation System." project.

Understanding the importance and critical aspects of the project that impact her graduation, we will allow her to conduct the research and collect the required information for this project. With your assurance that the information provided here will only be used for academic purposes and kept confidential, I am approving it. I and [redacted] have already discussed the project in the past and will coordinate with her till the successful completion of the project.

I look forward to working with [redacted]

Should there be any queries regarding this matter, please do not hesitate to contact me at suraj@vertexspecial.com.

Best regards

Suraj Neupane
Engineering and Operation Manager
Vertex Special Technology Pvt. Ltd

Where Technology Works Automagically

Remember us for any kinds of IT & Software Development works.

Figure 51: Client Approval Letter.