# ELK Stack Report

Software Service Construction: CS468  
Antoine Gaton

November 24, 2024

## Introduction

This report explores the use of the Elastic Cloud ELK stack (Elasticsearch, Logstash, Kibana) as a Software-as-a-Service (SaaS) solution for centralized logging. Elastic Cloud provides an efficient alternative to self-hosted ELK deployments, addressing challenges such as patching and maintenance. This proof of concept demonstrates the deployment, data ingestion, and visualization capabilities of Elastic Cloud.

## Process

### 1. Deployment

The Elastic Cloud deployment was configured with the following settings:  
- Deployment Name: AntoineGaton ELKCluster  
- Node Capacity: 4GB/96GB storage  
- Platform: Amazon Web Services (AWS)  
- Region: U.S. East  
- Elasticsearch Version: 6.3.0  
- Plugins: ingest-geoip, ingest-user-agent  
- Additional Settings: Automated index creation and Restore from Snapshot enabled.

A screenshot of a computer

Description automatically generated

### 2. Data Ingestion

Thirteen log messages were ingested into Elasticsearch. The data included fields such as timestamp, message, and user. The following steps were followed:  
1. Accessed Kibana Dev Tools.  
2. Used the `POST` API to index 13 documents into the 'my-index'.  
3. Verified the successful ingestion using a `\_search` query in Dev Tools.

A screenshot of a computer screen

Description automatically generated

### 3. Visualizations and Dashboard

Three visualizations were created in Kibana to analyze the indexed data:  
- A bar chart showing record counts over time.  
- A table displaying key details such as user and description.  
- A word cloud summarizing user activity.

These visualizations were combined into a dashboard named 'Record Count Over Time', which provides a comprehensive view of the log data.

## A screenshot of a computer Description automatically generated

## Conclusion

Elastic Cloud's SaaS model simplifies ELK stack deployment and management, making it a practical solution for centralized logging. The dashboard created demonstrates the platform's ability to visualize and analyze log data effectively. This proof of concept confirms the feasibility of transitioning to Elastic Cloud for enhanced scalability and reduced maintenance overhead.