**MONITORING EMPLOYEE’S MACHINE WITH BEATS AND PREDICT EMPLOYEE’S MACHINE PERFORMANCE WITH ELASTIC MACHINE LEARNING**

Project Id: **2022-294**

Project Proposal Report

Mohammed Rifakathulla

BSc (Hons) in Information Technology Specializing in Information Technology

Department of computer science

Sri Lanka Institute of Information Technology

February 2022

**MONITORING EMPLOYEE’S MACHINE WITH BEATS AND PREDICT EMPLOYEE’S MACHINE PERFORMANCE WITH ELASTIC MACHINE LEARNING**

Project Id: **2022-294**

Project Proposal Report

Mohammed Rifakathulla

BSc (Hons) in Information Technology Specializing in Information Technology

Department of computer science

Sri Lanka Institute of Information Technology

February 2022

# Declaration

I hereby declare that the work contained in this proposal is our own original work, and that no material previously submitted for a degree or diploma at any other university or institution of higher learning, nor, to the best of our knowledge and belief, any material previously published or written by any other person, other than where such acknowledgment is made in the text, has been incorporated without our prior written consent.

|  |  |  |
| --- | --- | --- |
| Name | Student ID | Signature |
| Mohammed Rifakathulla | IT19033310 |  |

The above candidate is carrying out research for the undergraduate Dissertation

under my supervision

Signature of the Supervisor: Date: 21.10.2022

# Acknowledgement

I would like to express my deepest gratitude to the Sri Lanka Institute of Information Technology (SLIIT) for providing me a research project to achieve my degree with more success achievements. And also, deepest thank to **Ms. Suranjini silva and Ms Sasini Wellalage my project supervisors who helped and conducted me in right path and providing me all the guidelines with** necessary instructions **to do the project.**

Finally, I would like to thank all the people with my parents and colleagues who helped, supported and encouraged me for the research project to fulfill the all the requirements and motivating me when developing this. The achievement of this research could not have been not possible to do without the participation of so many people whose names may not all be enumerated. Their helps also sincerely appreciated and gratefully acknowledged

# Abstract

An important aspect of Employees Machine monitoring with Elasticsearch and Beats and forecast that data with Elasticsearch Machine learning is the ability to forecast machine data, such as production orders. Forecasting is a useful way of predicting future events and it helps avoid surprises by providing an early warning and increased visibility into expected outcomes. By combining monitoring data with Machine Learning, organizations can then correlate data points across time to indicate trends that may be helpful in planning strategic decisions and business operations.

This tutorial will introduce you to how these topics can be used in your company's software to help predict machine behavior based on monitored metrics like current location, production order cycle time (POCT), or the number of servers online at a given moment

# 

# Table of Content

Declaration iii

Acknowledgement iv

Abstract v

Table of Content vi

List of Tables vii

List of Abbreviations viii

1. INTRODUCTION 1

1.1 Background 1

1.2 Literature Survey 3

1.3 Research Gap 7

1.4 Research Problem 10

1.5 Research Objectives 11

1.5.1 Main objectives 11

1.5.2 Specific Objective 11

2. Methodology 12

2.1 Elasticsearch 12

2.2 Creating kibana 13

2.3 Beats Function 14

2.4 Overall Function 15

2.5 Overall Diagram 16

2.6 Elastic machinelearning 17

2.7 Commercialization 18

2.8 Testing and Implementation 19

3. Results and Discussions 26

3.1 Results 26

3.2 Discussions 26

Conclusion 28

References 29

Appendices 31

# 

# List of Tables

[Comparison of Researches 0](#_Toc85058346)9

[Test case 1 2](#_Toc85058349)1

[Test case2 2](#_Toc85058350)1

[Test case 3 23](#_Toc85058351)

[Test case 4 23](#_Toc85058352)

[Test case 5 23](#_Toc85058353)

[Test case 6 24](#_Toc85058354)

[Test case 7 24](#_Toc85058355)

[Test case 8 25](#_Toc85058356)

[Test case 9 25](#_Toc85058357)

# 

# List of Abbreviations

|  |  |
| --- | --- |
| **Abbreviation** | **Description** |
| ES | Elasticsearch |
| SVM | Support Vector Machine |
| ELK Stack | Elastic,Logstash and kibana |
| POCT | Production order cycle time |
| EML | Elasticsearch Machine Learning |

1. INTRODUCTION

1.1 Background

Employees from all over the world have to do Work From Home after the pandemic situation happened all over the world. So all company was based on this remote work concept to make their company alive in this competitive and pandemic situation world so all over the world most employees did their company work from their home

In that Pandemic situation Companies main goal was survival so they have to move on with remote working system for long days and its helped company for the survival at the same time many problems

Because employee won’t present physical company don’t know what is employee doing with their working time and if there are online on any soft-wares like (Teams & Skype) still company can’t call and monitor employees machine all time so how company can know what is employee doing with their machine on their working time

That’s why I’m using Elasticsearch and beats these beats(filebeat & metricbeat) need run in employee’s machine. Metricbeat will show machine’s metrics and CPU usage and Disk pressure and using apps. The Filebeat will get the logs from machine and send it elasticsearch and we can visualize that machine data on kibana

And also by using Elasticsearch machine learning we can predict future data these machine learning module comes with in-build algorithms like Apache Lucene ,SVM and BM25 and TermFrequency and etc.. So based on this alogrithms we can predict data set given by us

So what I’m planning to is Monitor employee’s with metric and file beats and get the data set of an employees machine use that data to Elasticsearch machine learning to forecast and predict employees machine performance and logs in future

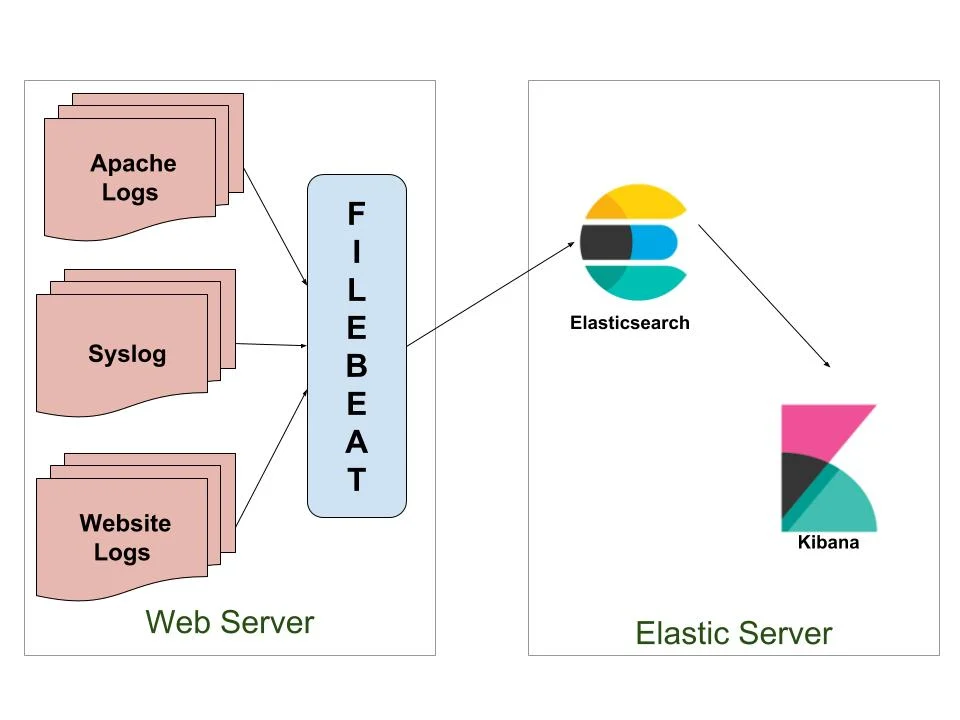


Figure 1.1: Filebeat Overview

Source: https://www.google.com/url?sa=i&url=https%3A%2F%2Fsubscription.packtpub.com%2Fbook%2Fbig\_data\_and\_business\_intelligence%2F9781788831031%2F13%2Fch13lvl1sec71%2Fconfiguring-the-beats&psig=AOvVaw1Pfe9fCIhUtsxCyEwfM\_wY&ust=1666117940522000&source=images&cd=vfe&ved=0CA8Q3YkBahcKEwjYmJaS8-f6AhUAAAAAHQAAAAAQBA

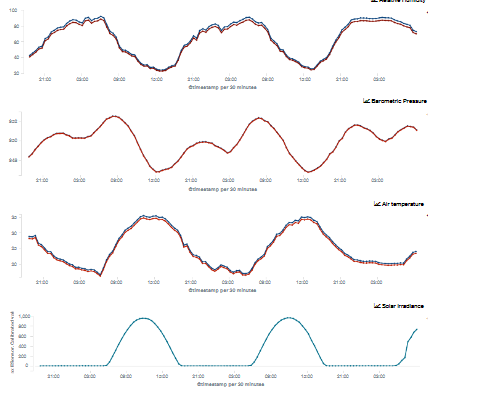
1.2 Literature Survey

In early Researches Elastic Search Machine Learning was used to read and predict some of data sets like weather, Nagios ,network logs etc..So Most of researches are used Elastic machine learning as a tool to predict their dataset and visualize it custom visualization

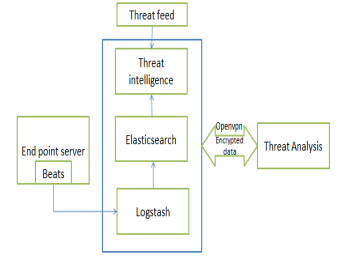
An early work by Powering Monitoring Analytics with ELK stack by “Abdelkader Lahmadi, and Fr´ed´eric Beck" used to monitor Nagios logs I Snort and suricata logs I Web server and ssh logs I Honeypots logs I Network event logs: NetFlow, IPFIX, pcap traces.

Also another early work by Application Performance Monitoring Using Log File on ELK Stack Ashwinikumar Tiwari and Dashrath Mane used logstash to get syslog and send it to ES and visualize it on kibana

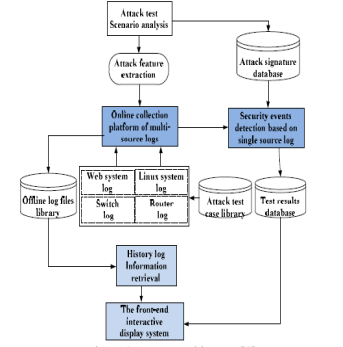
A research by Eugenio Almeida , Ivo Koga, Márcio A. A. Santana and Patricia Guimaraes was used Elastic machine learning for Predict their weather data set to predict the weather as per the image given below



And another Research by Pranita P. Bavaskar used ELK stack for “abnormality detection in log analysis “ for this they have used elasticsearch with logstash and apm server to detect that abnormality logs and over view of their system given below



Flow of the analysis for Pranita P. Bavaskar’s Abnormality log analysis



System diagram for Pranita P. Bavaskar’s Abnormality log analysis

The Elasticsearch Stack was used in this study to create clear yet comprehensive dashboards that identify system metrics, network performance measurements, user management events, and security events in Employees machine. These dashboards give security analysts a thorough understanding of security events that are occurring and aid them in conducting prompt, on-demand investigations. In such a difficult context, it was discovered to be a trustworthy tool.

And also In elastic search we have in build algorithms for machine learning so The early researches algorithms and my algorithms are same but the different is in early researches that are on my references was used elastic-search machine learning with their dataset .for my part im using elastic machine learning with a data set with that is with-in the elasticsearch

That means Employees machine data that sended Elasticsearch by Metricbeat and Filebeat with employees machine performance metrics and logs so to use these data to Elastic machine learning we need at least 1000 documents in that data sets or 1000 documents of combined employees machine.

So this elastic machine learning was already trained with Term frequency and Inverse Document Frequency models documents and Vector Space Model for multi term queries so the output will be reliable So based on this we can use this tool predict employees machine performance in future

1.3 Research Gap

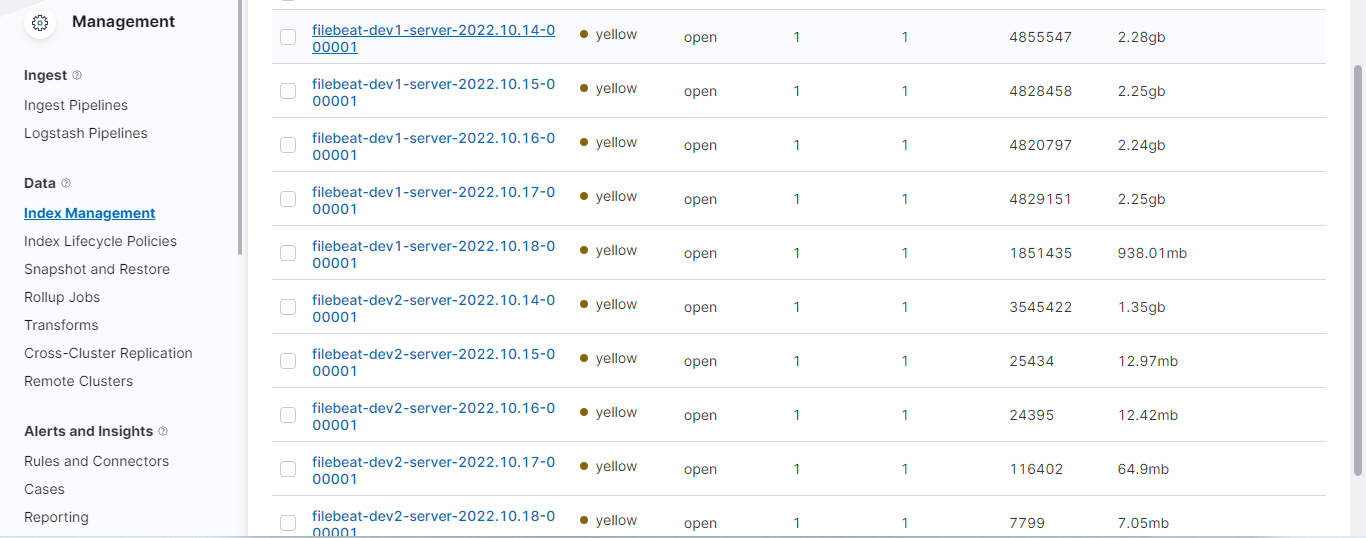
When there was remote work culture came very popular companies are still have survived in pandemic situation but as a srilankan we had a huge economic crisis so srilankan companies need to move on with remote work system even there is no pandemic

So we most companies survived but there was some major issue that’s why we decided to make a employees real time tracking system So for my part I decided to monitor employees machine I did many researches for that then I finally decided to use Elasticsearch to do that

For to do this I have to do more research so I referred many references for major of that researches are using logstash get monitor systems and use logstash as filter and elasticsearch as a anaylysis tool and so what they are doing was getting logs from logstash and evaluate analysis model with elasticsearch so the major issue in logstash was when we just run the logstash it’s got only system logs

Then I decided to go with beats and remove logstash filter in that part get beats outputs of metrics and logs directly to elasticsearch while doing this I have to do a plan how I‘m going to manage this because in one machine we can run only beat for an example if we run a metricbeat on a machine we can not run another metricbeat in that same machine but as per early researches if we run logstash in one machine we can configure many pipelines many jobs so I planning for this issue was I have to do more research and I have configured one metricbeat for all system metrics from that machine so I decided to go with metribeat modules by doing this modules can configuration metricbeat get metrics from some applications and system metrics and send it to elasticsearch

Then after the PP1 I had a problem with how I manage these beat indexes because I’m doing employees machine monitoring so I can’t get the all employee’s machine as same index so I research about this find solution with getting beats name with unique for every machine and it’s name index as per the image below



In this picture you can see filebeat same servers with date by date this how Im going to manage each and every employees machine data with unique name with date by date

But as per early researchers they used only logstash but so each every index of that are coming logstash so but for my part im getting beats data directly to elasticsearch without using logstash because my part mainly doing monitoring and using elasticsearch machine learning to analysis and prediction of data set from employees machine predict the employees machine performance

Table 1.1: Comparison of existing Researches

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Features** | **Zoe(My system)** | **LOG ANALYSIS WITH ELK STACK** | **Application Performance Monitoring Using Log File on ELK Stack** | **The Complete Guide to the ELK Stack** |
| Monitoring machine with  Logstash or beats | Yes  (With beats) | Yes | Yes | Yes |
| Using logstash for filtering | No | Yes | Yes | Yes |
| Write and store index date on beats configuration | Yes | No | No | No |
| Use elasticsearch machine learning for predict machines performance. | Yes | No | No | No |
| Integrate Elasticsearch with web application | Yes | No | No | No |
| Creating elastic index with machine name | Yes(Using specify name each machine or server) | No | No | No |

1.4 Research Problem

As I mentioned earlier we don’t what is employees are doing with their machine while on their working time so I decided implement a employees machine monitoring system for ZOE employee real time tracker since we planned to make our application as I application I needed to do employee machine monitoring as a web application

My main research problems was can we monitor employee’s machine in real time and also can we know if there was issue or error in employee’s machine before they are telling to us. Can we predict employee’s machine performance in future these are my research problems for this research

So I Research more about how can I make a solution for all of these problems and I found some researches with Elastic search that using logstash to get logs from machine and visualize and analyse those logs to predict the status of that machine. But that was researches not a solution for my research problems so I decided to do more research with ELK stack

Then I found options call beats that are running on machine and send machine usage and logs in real time to make custom visualization. So I decided move with beats without logstash then I found we can use any data sets Elastic search machine learning so I used beats data sets to elastic search and predict it regression training model and this part gave me the solution for all of my research problems it can monitor employee’s machine in real time and also we can employees machine errors by seeing employees machine logs and also we can predict the machine performance by using beats data set so I trained my data set and got 80% reliable output by Elasticsearch machine learning

1.5.1 Main objectives

The main objective is Monitor employees machine with Elasticsearch and beats and Visualize it on Kibana and Predict employee’s machine performance from the data set from beat configuration with Elastic machine learning

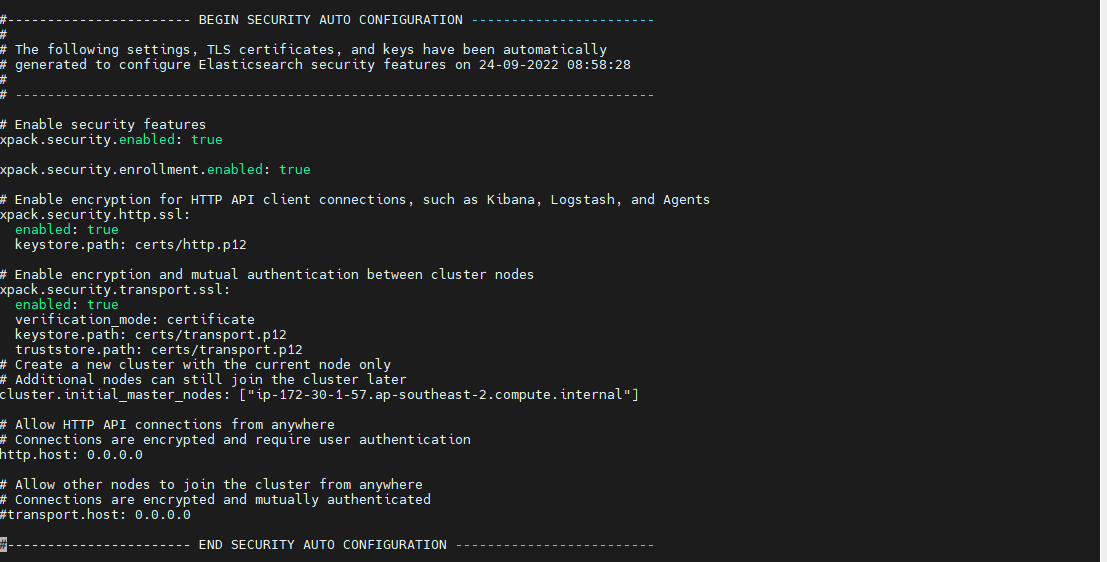
1.5.2 Specific Objective

* Research Configured needed beats to get employees machine usage and logs
* Keep monitor employees network and cpu usage in real time.
* Secure those data with X pack security.
* Train Elastic search Regression data set to read machine logs and predict performance of the machine
* Sent notifications to companies about monitoring state of employee’s machine.

1. Methodology

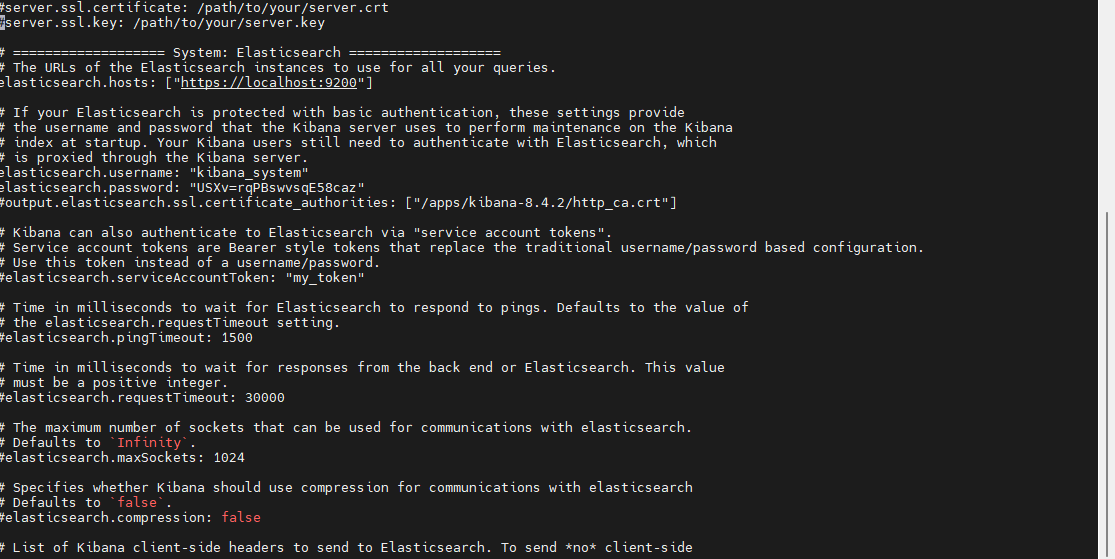
2.1 Configure Elasticsearch as single node

The elastic search need to configure before use that tool to monitoring in elastic search im using x pack security to protect it and it’s having separate certificate to connect to that elasticsearch while connecting beat otherwise you can’t connect to that elastisearch and while configure elasticsearch we have to provide a host for elasticsearch and we have to give a name that elasticearch node for my part I have configured elasticsearch as single node but it can be change in future 3 node Elasticsearch cluster to manage the indexes from employee’s machine a image of elasticearch configuration is given below



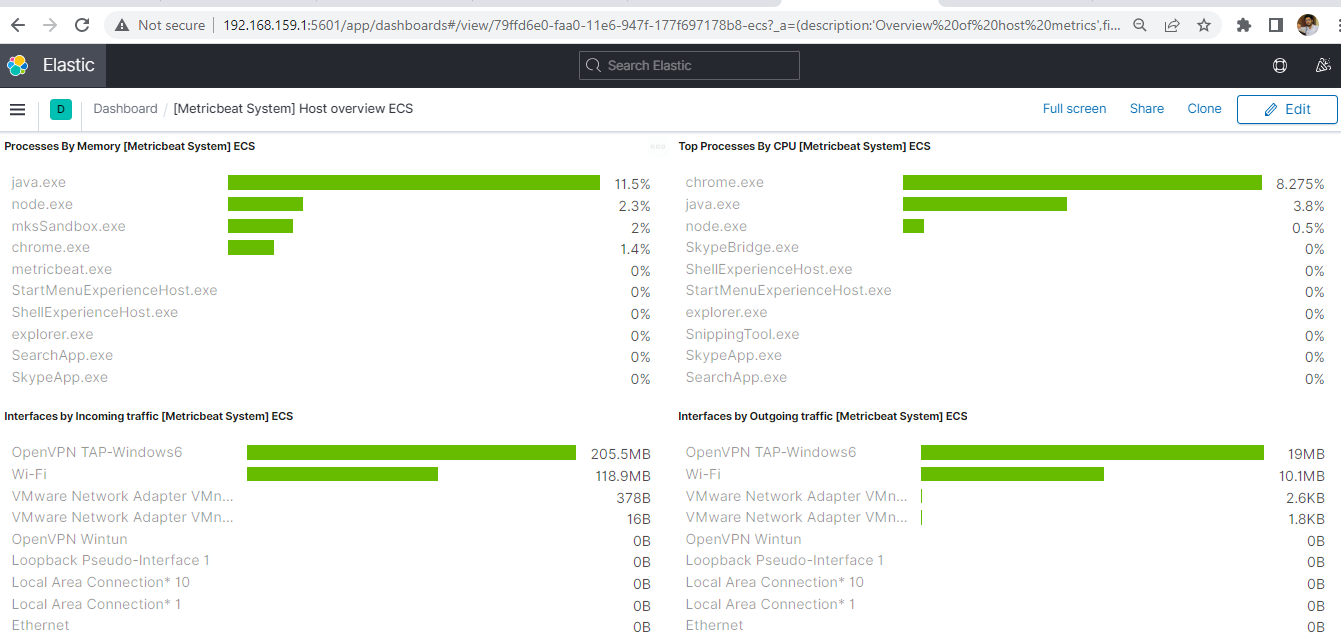
**2.2 Kibana configuration visualization**

While configure kibana first we have make the configuration in kibana.yml this yml file is giving instructions to machine so we have to provide it as per our configuration to work with kibana configuration our pre requirement was an elasticsearch node we have to give elasticsearch node host and user name to that kibana configuration after that we have to provide password of that kibana username so based on this kibana will connect to elasticsearch and able to give the visualization of that cluster and read the logs and metrics from elasticsearch indexes able to send them to relevant dashboards by reading logs metrics with fields name and we will able to visualize all of our elasticsearch cluster details in kibana



2.3 Monitoring employees machine application usage with beats

The employees machine application monitoring is can be done with metricbeat that collect metrics from the system and send that to ES so the company can monitor employee’s machine performance in real time this metricbeat configuration is need to be done on employee’s machine with the needed modules that need to be monitor with metricbeat so when employee’s turn on their machine they will able turn on the beat so metricbeat will capture that machine metrics in realtime and it’s will send that metrics to elasticsearch so company will able monitor employees machine in real time while they are doing their work and filebeat configuration is also done in the same way but we have to provide logs path as per that machine OS for an example if that system is running on Linux os we have to provide var path as var/log like wise it’s different as per OS so when I did this filebeat configuration I have tested with windows and linux machines and got those machine logs to kibana a sample pic of a windows machine application monitoring is given in below image in that image you can see what are applications now running on that machine and how much cpu usage consumed by them ,how much processor is consumed by that applications like wise you can visualize it as per you custom visualization



**2.4 Over all Process**

Elasticsearch is a distributed, open-source search and analytics engine for textual, numerical, geographical, structured, and unstructured data. Elasticsearch was initially released by Elasticsearch in 2010. It is based on Apache Lucene. Elasticsearch is the heart of the Elastic Stack, a collection of free and open tools for data intake, enrichment, storage, analysis, and visualization. It is known for its easy REST APIs, distributed nature, speed, and scalability. The Elastic Stack now contains a comprehensive collection of lightweight shipping agents known as Beats for sending data to Elasticsearch, which is sometimes referred to as the ELK Stack Logs, system metrics, and web applications all feed raw data into Elasticsearch. The act of parsing, normalizing, and enriching this raw data before it is indexed in Elasticsearch is known as data ingestion. Users may conduct complicated queries against their data and use aggregations to receive elaborate summaries of their data once their data has been indexed in Elasticsearch. Kibana is a free and open-source frontend tool that sits atop the Elastic Stack, allowing users to search and see data stored in Elasticsearch. Kibana also serves as a user interface for monitoring, administering, and protecting an Elastic Stack cluster, as well as a central center for Elastic Stack-based built-in solutions. In 2013, it was created. Beats is a collection of lightweight, open source log shippers that act as agents installed on various servers in your infrastructure to collect logs or metrics.  This could be log files (Filebeat), network data (Packetbeat), server metrics (Metricbeat), or  other types of data that can be collected from the growing number of Beats being developed by both Elastic and the community

Elastic Beats is a very useful tool for moving data from servers to Elasticsearch

and  can be used to investigate and improve quality of  service. Beats uses very little

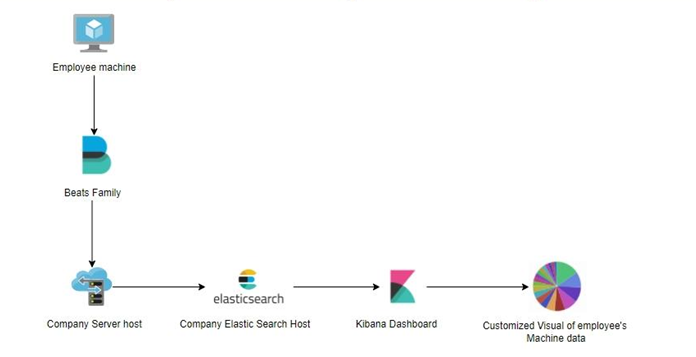
resources, so having little overhead has many advantages. There are many different

beats out there, and there may be beats for  use cases already created by the

community

.

**2.5 Overall Diagram**



System overall diagram

2.6 Elasticsearch Machine Learning

Your data is analysed using machine learning features, which create models of its patterns of activity. The questions or issues you wish to address and the kind of data you have available will determine the style of analysis you pick we can use supervised and unsupervised machine learning with elasticsearch and also we have forecast option to predict the data output so for configure some jobs option with our data set or we can use any data set to these jobs we forecast it on elasticsearch machine learning.For this work I have used a sample of machine performance datasets to check the forecast option and it’s gave the exactly predicted ouputs graph



Data set before forecast



Data set after forecast

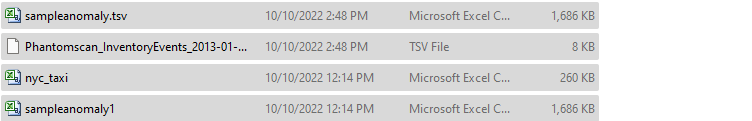
2.7 Commercialization

* We provide elasticearch monitoring with our web app. ​
* Specially for the Remote work companie, we are trying to give them a web application that provides a realtime employee;s machine monitoring, and predict employees machine performance. ​
* By using this companies can make employees work efficient and they can know what is happening with employee’s machine and what are they doing with their machine and it’s will help identify employee’s machine performance and provide some tasks as per their machine performance

2.8 Testing and Implementation

2.8.1 Implementation

After setup elasticsearch node and Kibana I setup Filebeat and metric beat on companies server and my friends machine got the data from their machine monitor their machine metrics and logs and for the machine learning part I have used some data sets from internet and also some data sets from my beats configuration and trained and tested them elasticsearch machine learning



Sample datasets used elasticsearch machine learning

2.8.2 Testing

Following the implementation phase, the system must be tested to determine whether or not it meets the requirements. As a result, the system must be tested. These tests ensure that the system was developed in accordance with industry standards. If we do not test the system, it will fail and fail to meet the expected goal.

There are some core testing methods such as,

* Unit Testing
* Integration Testing
* System Testing
  + Performance testing
  + Security testing
  + Functionality testing

Some core testing methods that using to test system are discussed in below,

**Unit Testing**

There are subcomponents or subunits in every system. We must ensure that the developed system works properly while developing it. Unit testing entails testing individual system subcomponents (subunits). Testing each and every unit was identifying all minor flaws in each unit. By doing this testing it helps to understand which subunits or which sub functions contains errors and bugs.

**Integration Testing**

Another testing called integration testing also used for testing the system to analyze errors and other issues. In unit testing it tested only units separately but in integration testing it test the system after the functions were combined. Purpose of this type of testing is to expose issues happened after integrated.

**System Testing**

Another type of core testing is system testing, which is used to test the entire system. It tested integration testing after testing subcomponents, which are combined functions. This system identifies the problems and errors in the final system. Subtesting methods include functionality testing, performance testing, and security testing.

Some test cases were created to test the system based on the functions and components. It tested the system as shown below using these test cases.

Test case 1

|  |  |
| --- | --- |
| Test Case Id | TC01 |
| Test Case Name | Running elasticearch. |
| Test Input Data | localhost9200 |
| Expected Output | Elastic search ui should be displayed |
| Actual Output | Elasticsearch ui displayed with cluter details |
| Pass/Fail Status | Pass |

Test case 2

|  |  |
| --- | --- |
| Test Case Id | TC02 |
| Test Case Name | Kibana |
| Test Input Data | Localhost:5601 |
| Expected Output | Kibana Ui should be displayed |
| Actual Output | Kibana ui with log in page |
| Pass/Fail Status | Pass |

Test case 3

|  |  |
| --- | --- |
| Test Case Id | TC03 |
| Test Case Name | Metricbeat bin file configuration directly to ES & Kibana |
| Test Input Data | Output.elasticsearch  Kibana host |
| Expected Output | Metricbeat index should be displayed on <http://localhost:9200/_cat/indices> and kibana index management page |
| Actual Output | Displayed the index on both pages |
| Pass/Fail Status | Pass |

Test case 4

|  |  |
| --- | --- |
| Test Case Id | TC04 |
| Test Case Name | Filebeat bin file configuration directly to ES & Kibana |
| Test Input Data | Output.elasticsearch and Kibana host |
| Expected Output | index should be displayed on <http://localhost:9200/_cat/indices> and kibana index management page |
| Actual Output | Displayed the index on both pages |
| Pass/Fail Status | Pass |

Test case 5

|  |  |
| --- | --- |
| Test Case Id | TC05 |
| Test Case Name | Show metricbeat index with date |
| Test Input Data | Index name yyyymmdd |
| Expected Output | Show machine index with date by date |
| Actual Output | Displaying index date by date |
| Pass/Fail Status | Pass |

Test case 6

|  |  |
| --- | --- |
| Test Case Id | TC06 |
| Test Case Name | Show filebeat index with date |
| Test Input Data | Index name yyyymmdd |
| Expected Output | Show machine index with date by date |
| Actual Output | Displaying index date by date area. |
| Pass/Fail Status | Pass |

Test case 7

|  |  |
| --- | --- |
| Test Case Id | TC07 |
| Test Case Name | Metricbeat system and other enabled metrics can viewed on kibana dashboard |
| Test Input Data | Kibana Dashboards for metricbeat |
| Expected Output | Metrics can be visualize |
| Actual Output | Showed metricbeat metrics as custom visualization in kibana dashboard |
| Pass/Fail Status | Pass |

Test case 8

|  |  |
| --- | --- |
| Test Case Id | TC08 |
| Test Case Name | Filebeat system and other enabled logs can viewed on kibana dashboard |
| Test Input Data | Kibana Dashboards |
| Expected Output | Logs can be visualize |
| Actual Output | Showed filebeat logs as custom visualization in kibana dashboard |
| Pass/Fail Status | Pass |

Test case 9

|  |  |
| --- | --- |
| Test Case Id | TC09 |
| Test Case Name | Predict employees machine performance with Elastic Machine Learning |
| Test Input Data | Employee machine’s metrics |
| Expected Output | Able to predict employee’s machine performance with metricbeat dataset. |
| Actual Output | Calculate and display metrics for given time period |
| Pass/Fail Status | Pass |

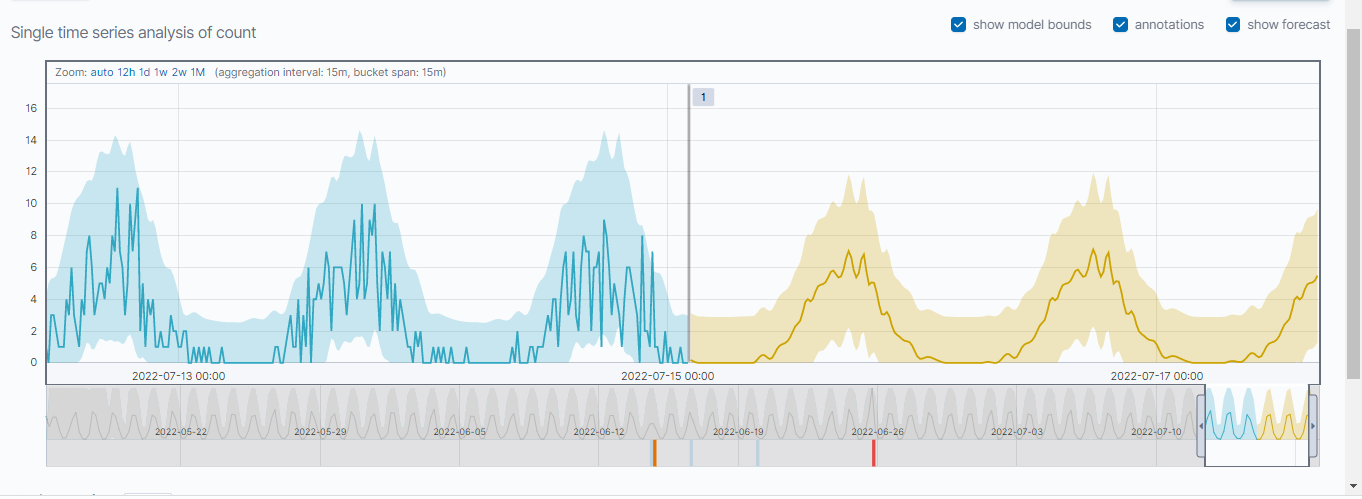
Test case 10

|  |  |
| --- | --- |
| Test Case Id | TC10 |
| Test Case Name | Predict employees machine logs with Elastic Machine Learning |
| Test Input Data | Employee machine’s logs |
| Expected Output | Able to predict employee’s machine performance with filebeat dataset |
| Actual Output | Calculate and display logs for given time period |
| Pass/Fail Status | Pass |

1. Results and Discussions

3.1 Results

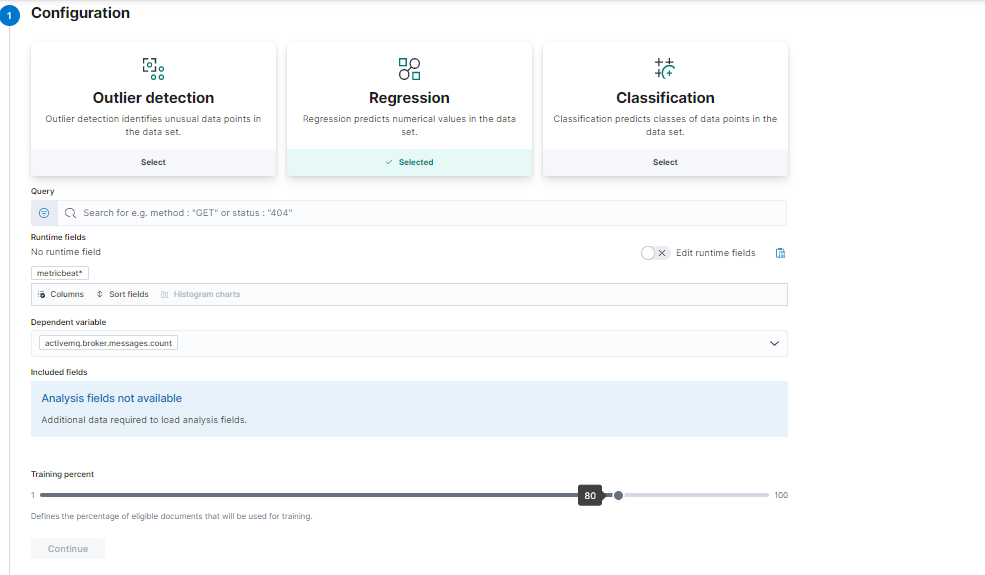
To predict the performance I have trained sample data sets of metribeats on Elasticsearch it and also with the inbuild algorithms of ES it predict exactly 80 percentage of given data set



3.2 Discussions

Many issues and faults may arise during the implementation of a system. Many drawbacks and failures can occur during the research phase. This section discussed the issues that arose during the system's implementation as well as the technologies that were used in the system. The component's main research component is Machine monitoring. CPU and Other usage of machine will shown in this scenario. Because there are so many different types of machines with many os, so have to run the beat with as per the os configuration. The All OS part was done first with the researches and . However, that beat outcome was failure. Mertics were not detected for that beat. Another issue was the incompleteness of the elastic server. Because it was not secured so have to make cerficate and user roles and password for elasticsearch and without them we can’t connect our beats so after that elastic update I have configured beats with enable elastic security.Then when we think about elastic machine learning we have to enable elastic machine learning with premium license of elastic search. There have to activate trail elastic search license for 30 days.

With all these issues it improved the system by using some solutions. From researches and asking ideas from ES experts With these kibana ouput and elastic machine learning results it improved this system .



Training metricbeat data set to predict machine performance

Above picture shows elastic search machine learning job configuration we can configure jobs with Outlier Detection detect structural data points , Regression can be used for predicts numerical value data set and classification can be use predicts the class of data so when we predict machine performance we should use classification configuration type

# Conclusion

This individual component was primarily used for monitoring employees machine with beats and get the data for on elasticsearch and visualize it on kibana and predict employees machine performance

By visualizing employee’s machine metrics data company can understand what going on with employees machine and what are the apps they are using.By visualizing employees machine logs with filebeat company and get application’s logs that are using by employees machine for an example if employees has a apache server on their machine we can monitor it by filebeat and get Apache access and error log

So since we are getting every employees machine data as separate index and with date we can pull that data set Elasticsearch machine learning and we can predict employees machine performance metrics and we can also predict employees machine logs

So I hope this solution will really helpful company and employees because we are monitoring employees machine with beats and use it to predict the machine data company and employee will know if there was issue on their machines or something going to happened with employees machine

# References

M Harikanth, Rajarajeswari

## Malicious Event Detection Using ELK Stack through Cyber Threat Intelligence

International Journal of Innovative Technology and Exploring Engineering (IJITEE)

Posted: 2019

Sikender Mohammad, Mohsienuddin

## Cloud Computing in IT and How It's Going to Help United States Specifically

International Journal of Computer Trends and Technology, volume 67

Posted: 2019-10-04

[Crossref](https://doi.org/10.14445/22312803/ijctt-v67i10p118)

Youngmi Sung Jun Son, Kwon

## Performance of ELK Stack and Commercial System in Security Log Analysis

IEEE 13th Malaysia International Conference on Communications (MICC)

Posted: 2017

Ibrahim Yahya Mohammed Al-Mahbashi, Dr M B Potdar, Mr Prashant Chauhan

## Network Security Enhancement through Effective Log Analysis Using ELK

IEEE 2017 International Conference on Computing Methodologies and Communication (ICCMC)

Posted: 2017

Jia Zhanpei, Y I Shen Chao, Chen Xiao, Yufei, Yu Tianwen, Xiaohong

## Big-Data Analysis of Multi-Source Logs for Anomaly Detection on Network-based System

13th IEEE Conference on Automation Science and Engineering

Posted: 2017

Siwoon Son, Myeong-Seon, Yang-Sae Gil, Moon

Anomaly Detection for Big Log Data Using a Hadoop Ecosystem

Juan Pablo Gila, Johnny Revecoa, Tzu-Chiang Shena

Operational logs analysis at ALMA observatory based on ELK stack

Posted: 2016

OnlineOpen Source Search & Analytics" elastic

ELK to Monitor Performance [Online] Available: [https://logz.io/blog/elk-monitor-platformperformance[Accessed:15-June-2020](https://logz.io/blog/elk-monitor-platformperformance%5bAccessed:15-June-2020)].

C. Preneur, “ELK (ElasticSearch, Logstash, Kibana),” 2020.[Online].https://medium.com/elkelasticsearch - Logstash-kibaa-a48c12612b16. [Accessed: 7-June-2020].

S. Alspaugh et al., “Analyzing Log Analysis: An Empirical Study of User Log Mining This paper is Included in the Proceedings of the Analyzing Log Analysis: An Empirical Study of User Log Mining User surveys,” 2014.

Chen-Kun Tsung, Member, IEEE, Chao-Tung Yang, Member, IEEE Visualizing Potential Transportation Demand from ETC Log Analysis Using ELK Stack

Tarun Prakash, Ms. Misha Kakkar, Kritika Patel, GeoIdentification of Web Users through Logs using ELK Stack

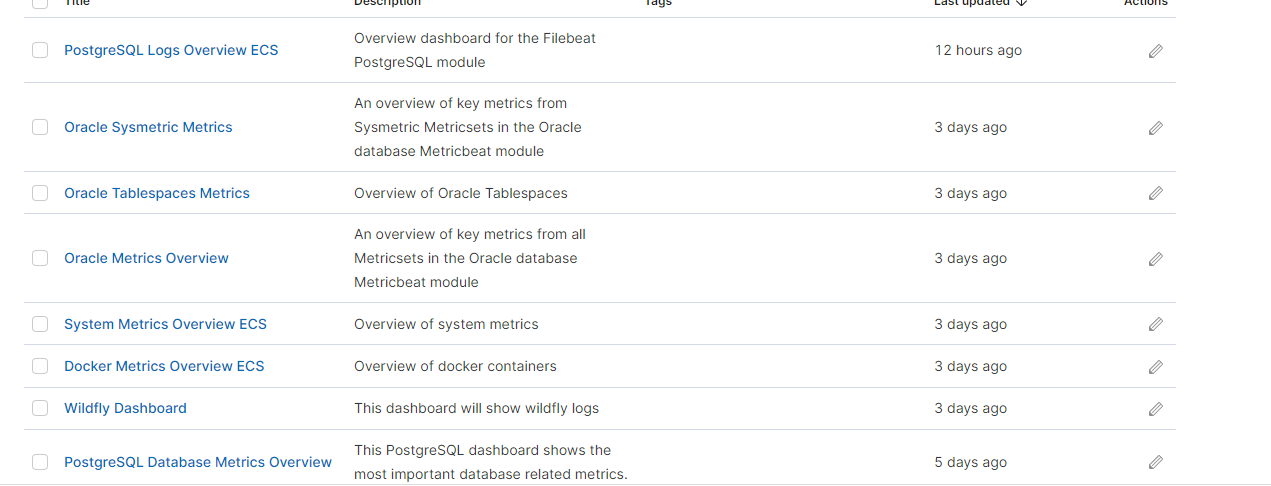
Júlia Murínová, Application Log Analysis

[ APM Server Reference [Online] Available: https://www.elastic.co/guide/en/apm/server/cureNt/i ndex.html [Accessed: 20-June-2020].

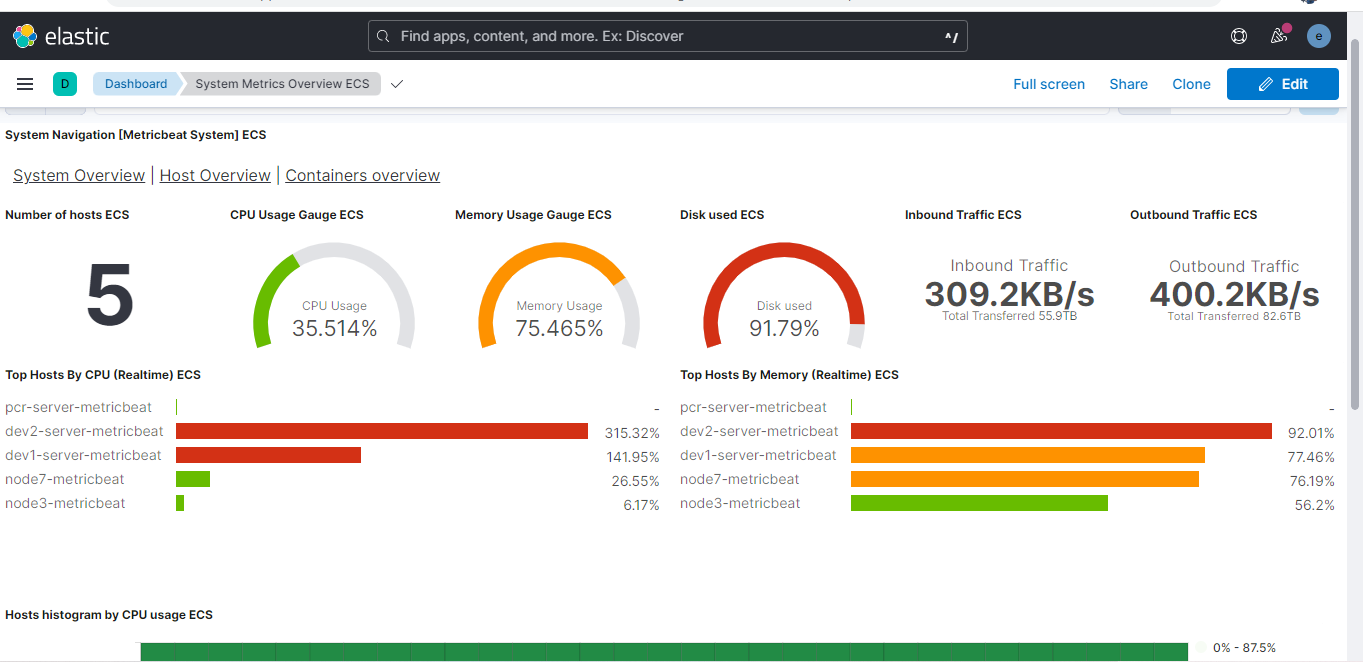
ELK Stack: Elasticsearch, Logstash, Kibana | Elastic [Online] Available: https://www.elastic.co/what-is/elkstack[Accessed:21-June-2020]. [9] Adian F. Rochim, Mukhlish A. Aziz, Adnan Fauzi. "Design Log management System of Computer Network Devices Infrastructures Based on ELK Stack", 2019 International Conference on Electrical Engineering and Computer Science (ICECOS), 2019

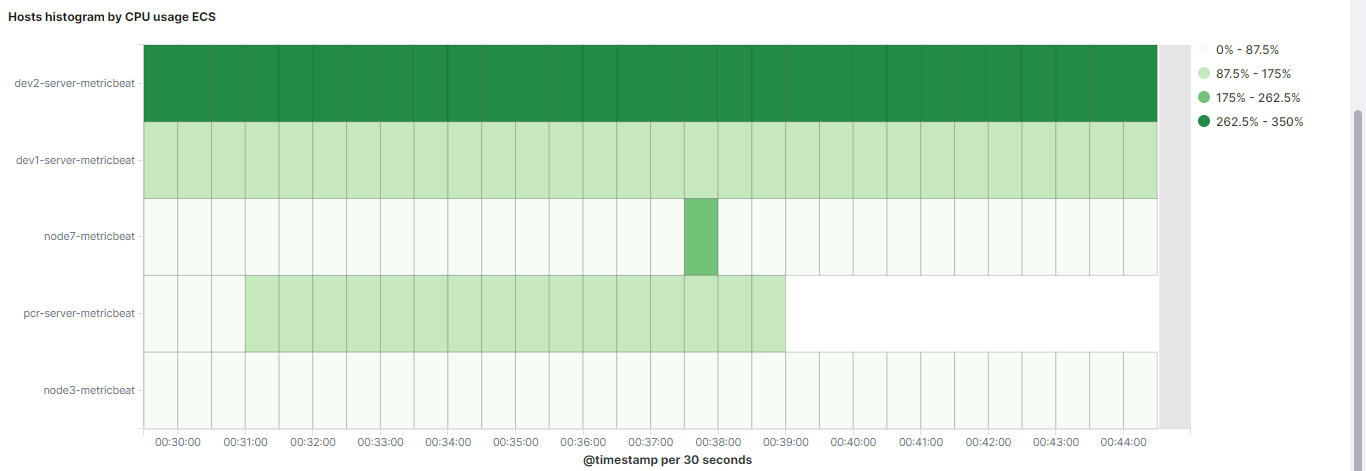
Appendices

Appendix A: Interfaces



Sample Dashboards

average all server metrics



Histogram cpu usage for all servers

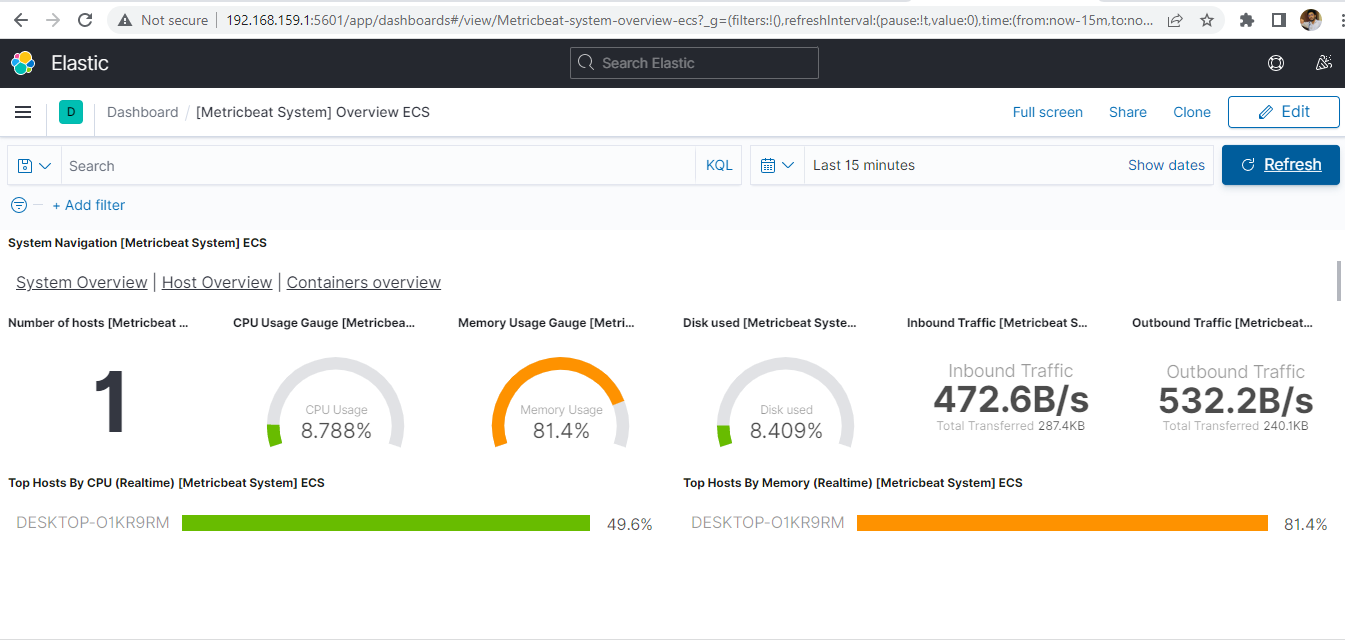
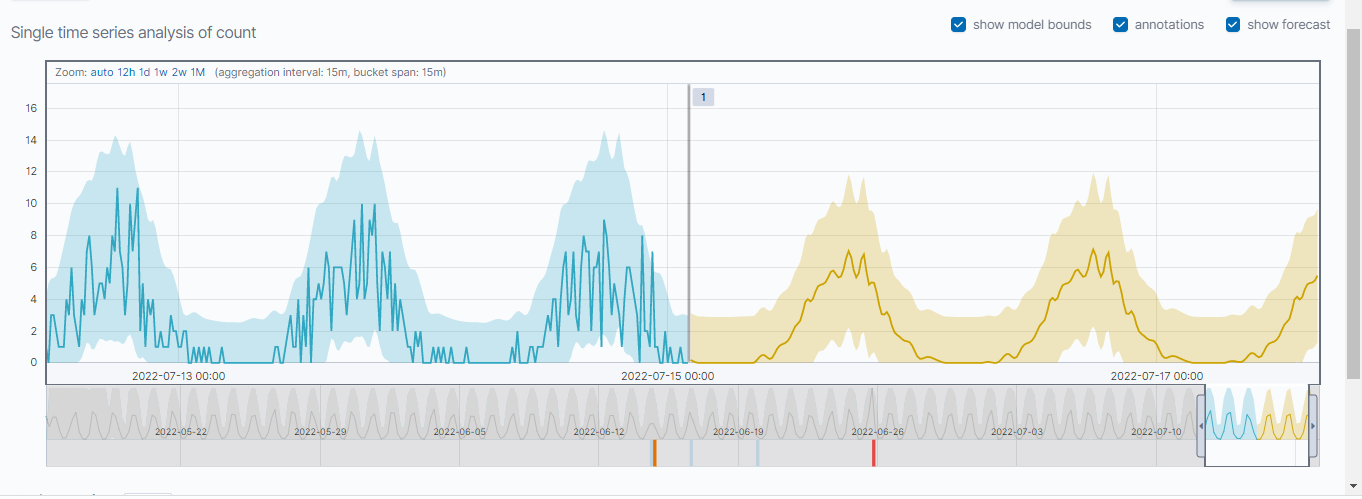
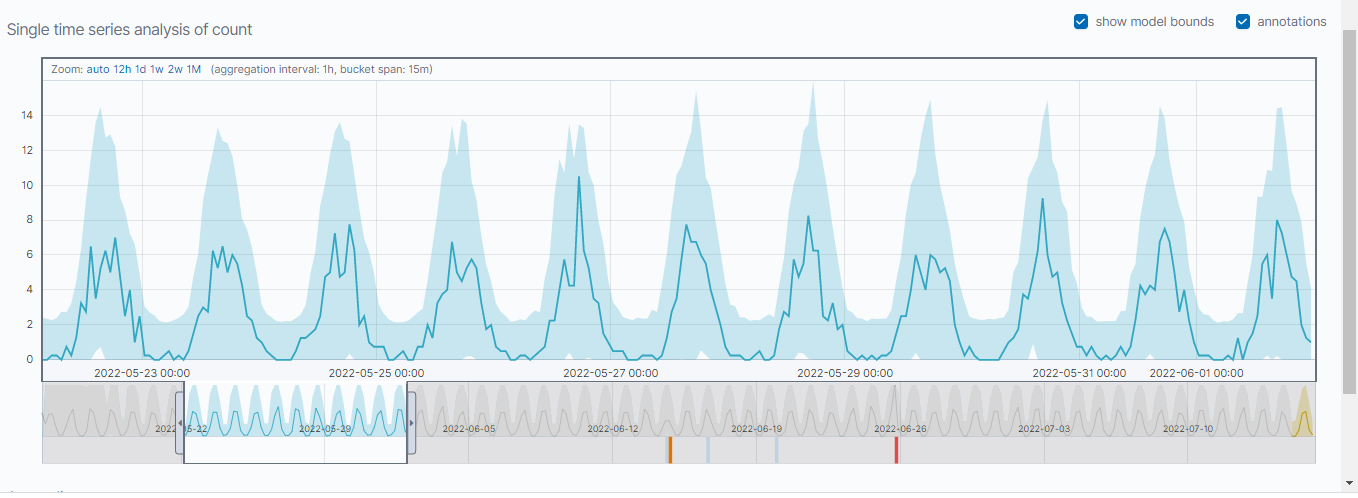


Figure .2 Drawer (Multi Language Supported)

Figure 21 Homepage

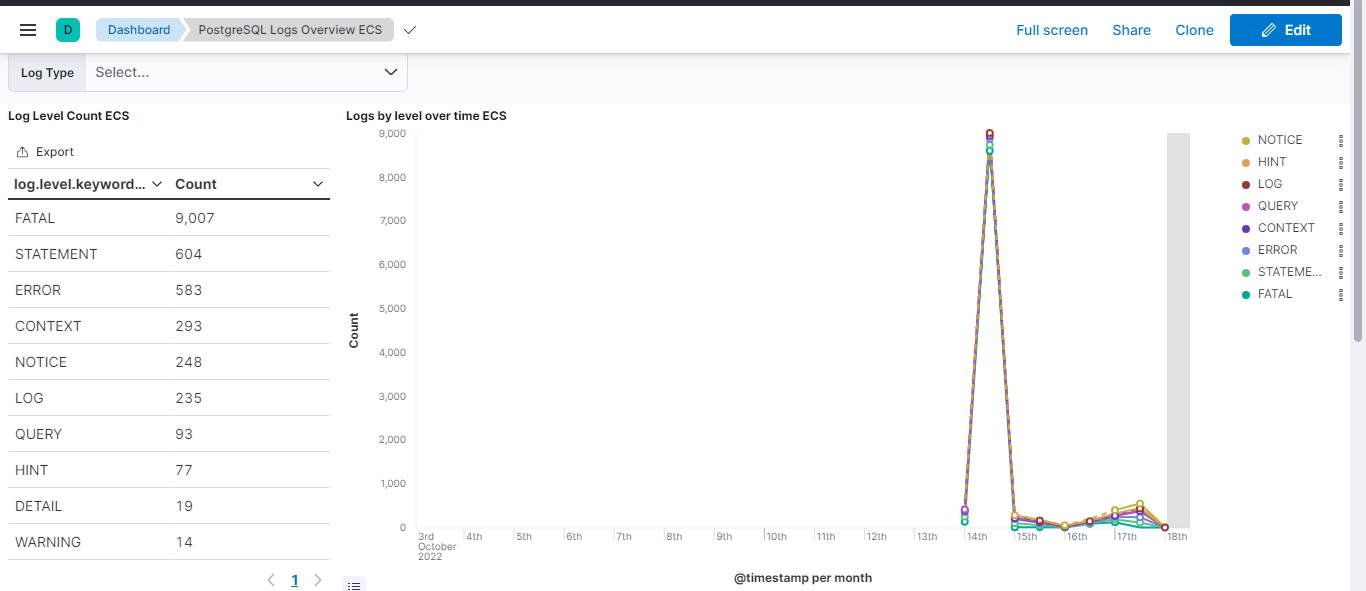
Figure Homepage

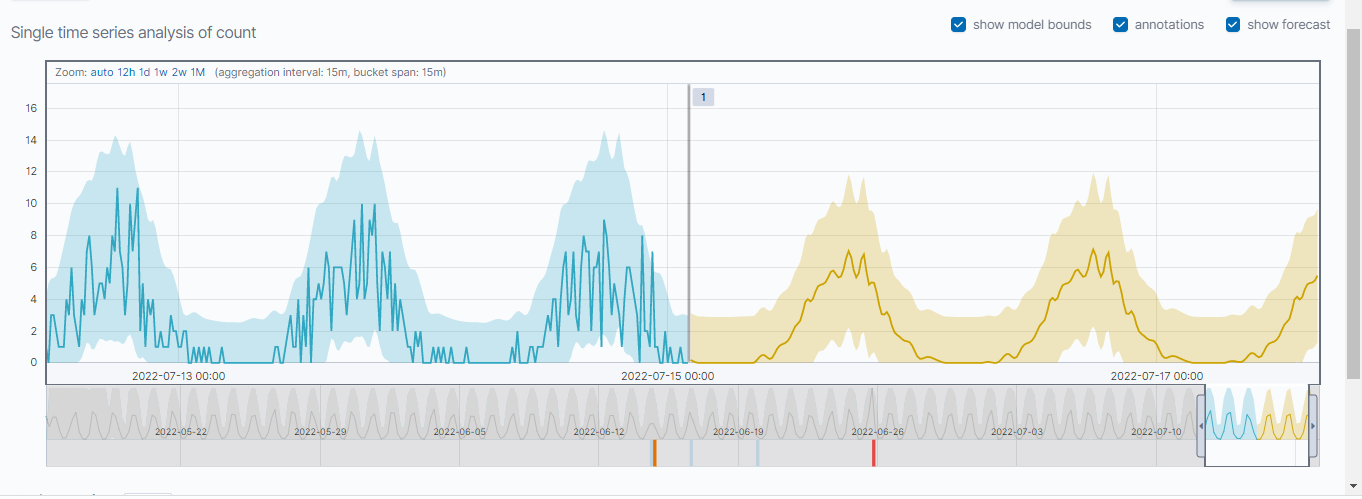
Machine learinig anaylysis count with machine data

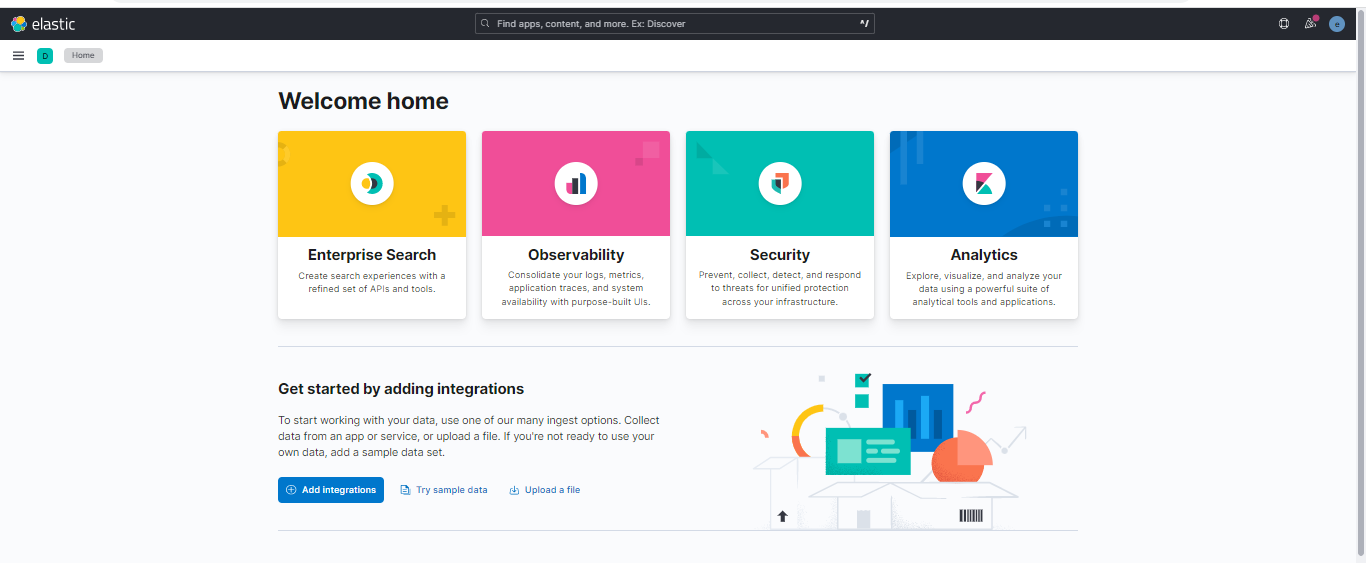


Predicted machine data

Filebeat logs for Postgres logs





Kibana ui