Logo

Description automatically generated with medium confidence

Sri Lanka Institute of Information Technology

**Information Security Project**

**Logo, icon

Description automatically generated**

**Open-Source SoC Platform**

**Implementation Guide**

Submitted by:

|  |  |
| --- | --- |
| Student Registration Number | Student Name |
| IT20077624 | P.A Daham Thameera |
| IT20021870 | Dilshan K. N |

Date of submission

5th December 2022

Table of Contents

[Installation Requirements 3](#_Toc121441347)

[Environment 3](#_Toc121441348)

[Ports and Network 3](#_Toc121441349)

[ELK Stack 5](#_Toc121441350)

[Elastic Search 6](#_Toc121441351)

[7](#_Toc121441352)

[Logstash 10](#_Toc121441353)

[Kibana 10](#_Toc121441354)

[The Cassandra Database 12](#_Toc121441355)

[The Hive Project 13](#_Toc121441356)

[Implementation Process 13](#_Toc121441357)

# **Installation Requirements**

## Environment

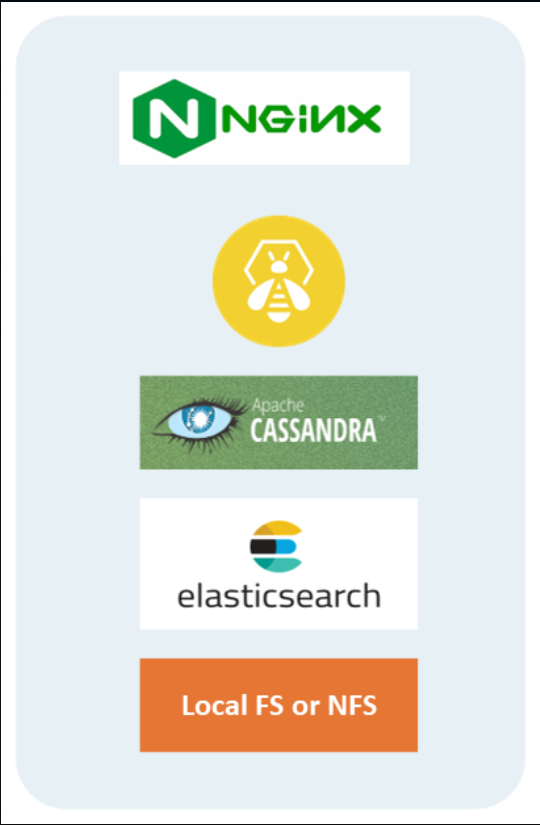
* Ubuntu VM version 20.04 as standalone server
* Cassandra DB
* MISP- Ubuntu20- t3.micro
* Elastic SIEM- Ubuntu20- t2.medium (Best performance can be achieved on t2.large)
* Cortex- Ubuntu20- t3a.medium (Can work on t2.medium as well)
* TheHive- Ubuntu20- t2.medium

## Ports and Network

|  |  |  |
| --- | --- | --- |
| Ports | IP Ranges | Comments |
| 22 | Host IP | SSH to the VMs |
| 443 | Host IP | Accessing MISP UI on browser |
| 9200 | Host IP | Accessing ElasticSearch |
| 5601 | Host IP | Accessing Kibana UI |
| 9001 | Host IP | Accessing Cortex UI |
| 9000 | Your IP | Accessing TheHive UI |
| All TCP | Cortex VM IP | Accssing inbound API |
| All TCP | MISP VM IP | Accssing inbound API |
| All TCP | TheHive VM IP | Accssing inbound API |

All applications are installed on the same server.

* Cassandra
* Elasticsearch
* Files are store on the filesystem (or MinIO if desired)
* TheHive
* NGINX (optional): to manage HTTPS communications



Before any of the installation or configurations, need to update the relevant ubuntu system to latest version using “sudo apt update” command.

# **ELK Stack**

"ELK" is the acronym for three open source projects: Elasticsearch, Logstash, and Kibana. Elasticsearch is a search and analytics engine. Logstash is a server‑side data processing pipeline that ingests data from multiple sources simultaneously, transforms it, and then sends it to a "stash" like Elasticsearch. Kibana lets users visualize data with charts and graphs in Elasticsearch. The Elastic Stack is the next evolution of the ELK Stack.

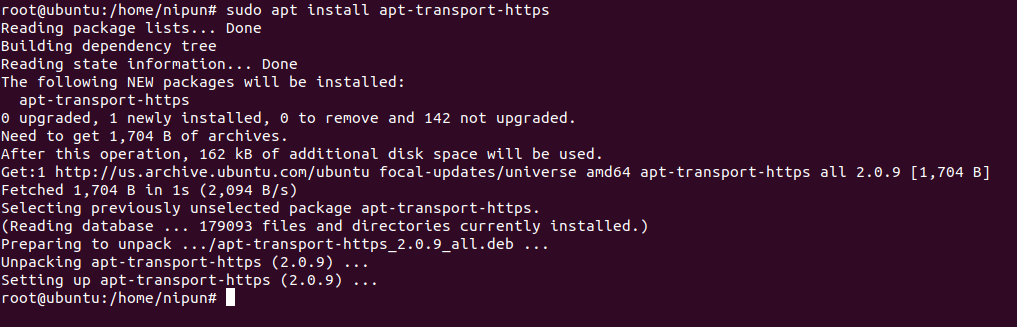
# ElasticSearch

Elasticsearch is a distributed, free and open search and analytics engine for all types of data, including textual, numerical, geospatial, structured, and unstructured. Elasticsearch is built on Apache Lucene and was first released in 2010 by Elasticsearch N.V. (now known as Elastic). Known for its simple REST APIs, distributed nature, speed, and scalability, Elasticsearch is the central component of the Elastic Stack, a set of free and open tools for data ingestion, enrichment, storage, analysis, and visualization. Commonly referred to as the ELK Stack (after Elasticsearch, Logstash, and Kibana), the Elastic Stack now includes a rich collection of lightweight shipping agents known as Beats for sending data to Elasticsearch.

Raw data flows into Elasticsearch from a variety of sources, including logs, system metrics, and web applications. Data ingestion is the process by which this raw data is parsed, normalized, and enriched before it is indexed in Elasticsearch. Once indexed in Elasticsearch, users can run complex queries against their data and use aggregations to retrieve complex summaries of their data. From Kibana, users can create powerful visualizations of their data, share dashboards, and manage the Elastic Stack.

* Before installation of ELK stack, we have to fulfill the following requirements.
* Initially have to install the compatible jdk version and transport https.

A picture containing text

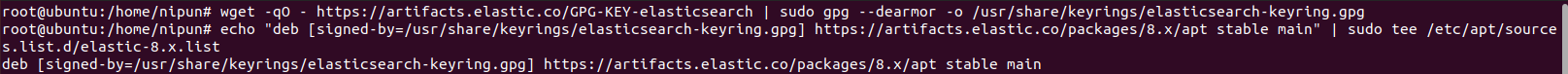
Description automatically generated

* Text

  Description automatically generatedCheck whether the jdk installation and environment variable setup are correct.

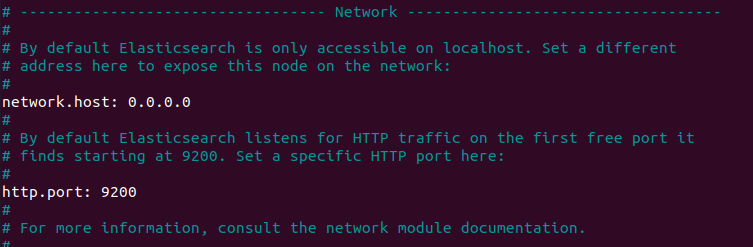
# 

* Get the relevant GPG key



* Text

  Description automatically generatedInstall the Elastic Search
* Generated super user password need to store securely.
* The following configuration needs to be done in etc/elasticsearch/elasticsearch.yml to establish the host and port connections for the Elasticsearch.



Text

Description automatically generated

* Text

  Description automatically generatedVerify the ElasticSearch status.

Text

Description automatically generated

# Logstash

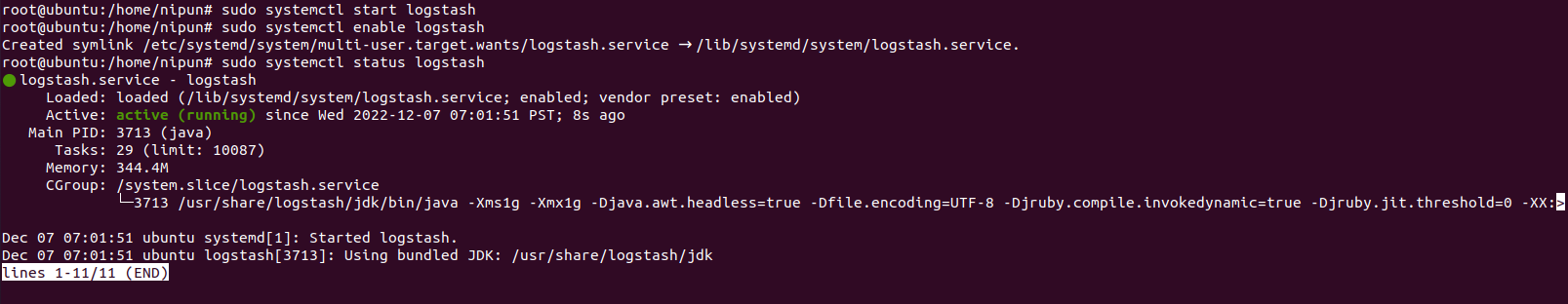
Logstash, one of the core products of the Elastic Stack, is used to aggregate and process data and send it to Elasticsearch. Logstash is an open source, server-side data processing pipeline that enables you to ingest data from multiple sources simultaneously and enrich and transform it before it is indexed into Elasticsearch.

* Install Logstash using APT store

Text

Description automatically generated

* Check the Logstash status



# Kibana

Kibana is a data visualization and management tool for Elasticsearch that provides real-time histograms, line graphs, pie charts, and maps. Kibana also includes advanced applications such as Canvas, which allows users to create custom dynamic infographics based on their data, and Elastic Maps for visualizing geospatial data.

* Install the Kibana Dashboard

Text

Description automatically generated

* Edit the etc/kibana/kibana.yml file.

Text

Description automatically generatedText

Description automatically generated

* Check the Kibana Status

Text

Description automatically generated

* Enable the relevant ports to Listen in order to communicate.

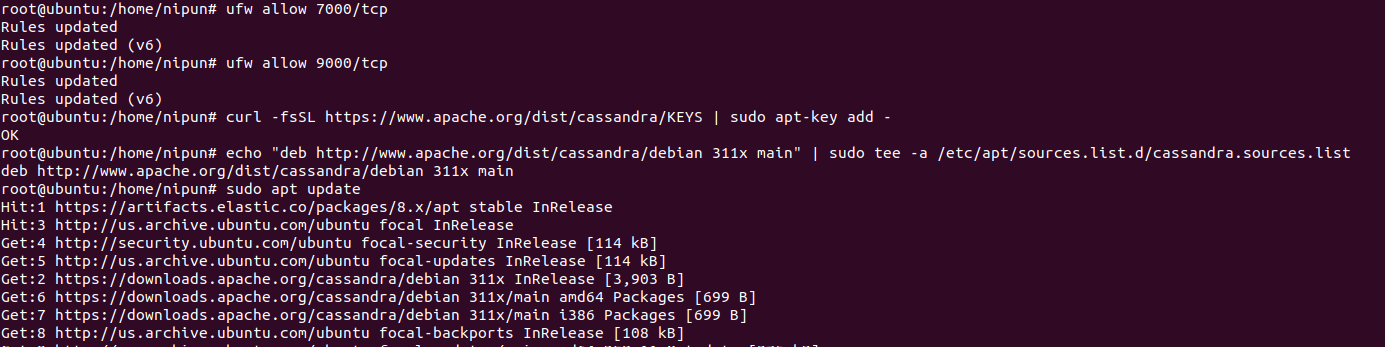
Text

Description automatically generated

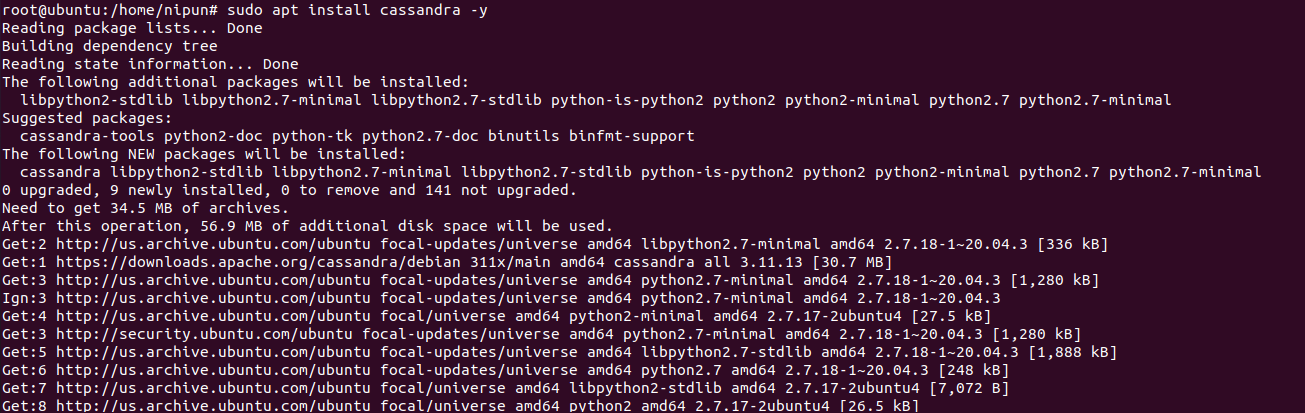
# **The Cassandra Database**

Apache Cassandra is an open source NoSQL distributed database trusted by thousands of companies for scalability and high availability without compromising performance. Linear scalability and proven fault-tolerance on commodity hardware or cloud infrastructure make it the perfect platform for mission-critical data.

* Initial dependency fulfillment



* Installing Cassandra DB using APT store



* Check the Cassandra status

Text

Description automatically generated

# **The Hive Project**



A scalable, open source, free Security Incident Response Platform that is tightly integrated with MISP (Malware Information Sharing Platform) is created to make life easier for SOCs, CSIRTs, CERTs, and any other information security professional dealing with security incidents that must be quickly investigated and addressed.

The Hive is a fully open-source platform but if we use TheHive Cloud platform it will be managed by the Hive group and it occurs the cost of the product. So, in this project, we use an open-source platform, and because of that, we need to customize and manage the product also this is an On-Prem solution.

## Implementation Process