VIT-AP UNIVERSITY

CYBER PHYSICAL SYSTEM SECURITY

COURCE CODE: CSE1018

PROJECT REPORT

Deploying ELK Stack and File Beats in Cloud and Local

NAME: Anguluri Pavani Anvitha

REG: 21BCE7498

SLOT: E2+TE2

FACULTY: Prof. Sibi Chakkaravarthy

ELK

Elasticsearch Logstash Kibana

Elasticsearch:

Elasticsearch is a highly scalable and open-source search and analytics engine built on top of Apache Lucene. It's designed to store, search, and analyze large volumes of data quickly and in near real-time. Elasticsearch uses a distributed architecture, enabling it to horizontally scale across multiple servers or nodes. It supports various data types, text analysis, full-text search, and complex queries. It's commonly used for log and event data analysis, monitoring, and powering search functionality in applications. Elasticsearch provides RESTful APIs for interaction, making it accessible from various programming languages. Its ecosystem includes tools like Kibana for data visualization and management, and Logstash for data collection and processing.

Logstash:

Logstash operates by creating data pipelines that consist of multiple stages. It can pull data from various sources like logs, databases, or APIs, process and enrich the data using filters, and then send it to various destinations such as Elasticsearch, other databases, or message queues. This makes it versatile for tasks like log aggregation, data normalization, and real-time analytics.

Kibana:

Kibana is an open-source data visualization and exploration platform developed by Elastic. It is designed to work seamlessly with the Elasticsearch database, forming part of the Elastic Stack. Kibana enables users to interact with their data stored in Elasticsearch through dynamic and customizable visualizations, dashboards, and searches. It offers a user-friendly interface to create and share visual representations of data trends, patterns,

and insights, making it a valuable tool for data analysis, monitoring, and business intelligence. Kibana supports various chart types, data filtering, and aggregation options, allowing users to gain actionable insights from their data quickly and efficiently.

Using these steps, we can installation ELK

Step-1

Use command

lsb_release -a

```
vboxuser@ubuntu:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04.3 LTS
Release:        22.04
Codename:       jammy
```

Step-2

Sudo apt install default-jdk default-jre -y

```
vboxuser@ubuntu:~$ sudo apt install default-jdk default-jre -y
[sudo] password for vboxuser:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
default-jdk is already the newest version (2:1.11-72build2).
default-jre is already the newest version (2:1.11-72build2).
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 28 not upgraded.
```

Step-3

Javac -version

```
vboxuser@ubuntu:~$ javac -version
javac 11.0.20
```

Step-4

Sudo apt-get install curl

```
root@ubuntu:/home/vboxuser# sudo apt-get install curl
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (7.81.0-1ubuntu1.13).
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 28 not upgraded.
```

Step-5

Curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -

```
root@ubuntu:/home/vboxuser# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
```

Step-6

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/ elastic-7.x.list

```
root@ubuntu:/home/vboxuser# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources
.list.d/
elastic-7.x.list
bash: /etc/apt/sources.list.d/: Is a directory
elastic-7.x.list: command not found
```

Step-7

apt update

```
root@ubuntu:/home/vboxuser# apt update
Hit:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [305 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [894 kB]
Get:8 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [680 kB]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [155 kB]
Get:10 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [43.0 kB]
Get:11 http://security.ubuntu.com/ubuntu jammy-security/main DEP-11 48x48 Icons [16.9 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/main DEP-11 64x64 Icons [26.5 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [11.2 kB]
Get:14 http://security.ubuntu.com/ubuntu jammy-security/restricted amd64 Packages [694 kB]
Get:15 http://in.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [471 kB]
Get:16 http://in.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [214 kB]
Get:17 http://security.ubuntu.com/ubuntu jammy-security/restricted Translation-en [110 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [101 kB]
Get:19 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [772 kB]
Get:20 http://in.archive.ubuntu.com/ubuntu jammy-updates/main DEP-11 48x48 Icons [36.1 kB]
Get:21 http://in.archive.ubuntu.com/ubuntu jammy-updates/main DEP-11 64x64 Icons [55.1 kB]
Get:22 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [15.6 kB]
Get:23 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [714 kB]
Get:24 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [114 kB]
Get:25 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [555 kB]
Get:26 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [650 kB]
Get:27 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [971 kB]
Get:28 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [141 kB]
Get:29 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [212 kB]
Get:30 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [288 kB]
Get:31 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe DEP-11 48x48 Icons [192 kB]
Get:32 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe DEP-11 64x64 Icons [295 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [40.0 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/universe DEP-11 48x48 Icons [21.4 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/universe DEP-11 64x64 Icons [33.9 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [16.5 kB]
Get:37 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [21.6 kB]
Get:38 http://in.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [944 B]
Get:39 http://in.archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [4,916 B]
Get:40 http://in.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [15.5 kB]
Fetched 9,227 kB in 14s (663 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
44 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg
e DEPRECATION section in apt-key(8) for details.
```

Step-8

apt install elasticsearch -y

```
root@ubuntu:/home/vboxuser# apt install elasticsearch -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
elasticsearch is already the newest version (7.17.12).
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 44 not upgraded.
```

Step-9

Configure elasticsearch

nano /etc/elasticsearch/elasticsearch.yml

```
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: localhost
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
```

Step-10

nano /etc/elasticsearch/jvm.options

```
################################################################
## IMPORTANT: JVM heap size
################################################################
##
## The heap size is automatically configured by Elasticsearch
## based on the available memory in your system and the roles
## each node is configured to fulfill. If specifying heap is
## required, it should be done through a file in jvm.options.d,
## and the min and max should be set to the same value. For
## example, to set the heap to 4 GB, create a new file in the
## jvm.options.d directory containing these lines:
##
-Xms512m
-Xmx512m
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/heap-size.html
## for more information
##
################################################################
```

Step-11

systemctl restart elasticsearch

```
root@ubuntu:/home/vboxuser# systemctl restart elasticsearch
root@ubuntu:/home/vboxuser#
```

Step-12

systemctl status elasticsearch

```
root@ubuntu:/home/vboxuser# systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-08-23 23:41:38 IST; 7min ago
       Docs: https://www.elastic.co
   Main PID: 16868 (java)
      Tasks: 76 (limit: 14281)
     Memory: 997.0M
        CPU: 1min 32.302s
     CGroup: /system.slice/elasticsearch.service
             ├─16868 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.ca>
             └─17073 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Aug 23 23:41:07 ubuntu systemd[1]: Starting Elasticsearch...
Aug 23 23:41:38 ubuntu systemd[1]: Started Elasticsearch.
```

Step-13

curl -X GET “localhost:9200”

```
root@ubuntu:/home/vboxuser# curl -X GET "localhost:9200"
```

Step-14

installation of logstash

apt install logstash -y

```
root@ubuntu:/home/vboxuser# apt install logstash -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
logstash is already the newest version (1:7.17.12-1).
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 27 not upgraded.
```

Step-15

systemctl start logstash

systemctl enable logstash

systemctl status logstash

```
root@ubuntu:/home/vboxuser# systemctl start logstash
root@ubuntu:/home/vboxuser# systemctl enable logstash
root@ubuntu:/home/vboxuser# systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-08-24 00:05:58 IST; 5s ago
   Main PID: 45555 (java)
      Tasks: 18 (limit: 14281)
     Memory: 432.3M
        CPU: 15.159s
     CGroup: /system.slice/logstash.service
             └─45555 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -
XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.awt.headless=t
rue -Dfile.encodi>

Aug 24 00:05:58 ubuntu systemd[1]: Started logstash.
Aug 24 00:05:58 ubuntu logstash[45555]: Using bundled JDK: /usr/share/logstash/jdk
Aug 24 00:05:59 ubuntu logstash[45555]: OpenJDK 64-Bit Server VM warning: Option UseConcMarkS
weepGC was deprecated in version 9.0 and will likely be removed in a future release.
lines 1-13/13 (END)
```

Step-16

apt update

```
root@ubuntu:/home/vboxuser# apt update
Hit:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:5 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
27 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in leg
acy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for
 details.
```

Step-17

apt install kibana -y

```
root@ubuntu:/home/vboxuser# apt install kibana -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
kibana is already the newest version (7.17.12).
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 27 not upgraded.
```

Un command these lines and change them

```
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names ar>
# The default is 'localhost', which usually means remote machines will not be able to connec>
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "localhost"
```

```
# The Kibana server's name.  This is used for display purposes.
server.name: "your-hostname"
```

systemctl start kibana

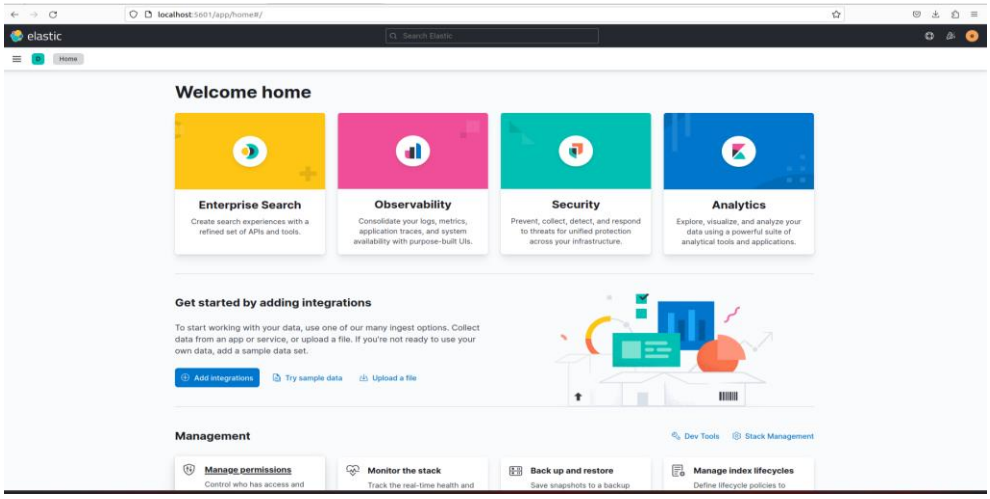
systemctl enable kibana

systemctl status kibana

```
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-08-23 22:56:21 IST; 1h 37min ago
       Docs: https://www.elastic.co
   Main PID: 832 (node)
      Tasks: 11 (limit: 14281)
     Memory: 634.0M
        CPU: 2min 21.132s
     CGroup: /system.slice/kibana.service
             └─832 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/d>

Aug 23 22:56:21 ubuntu systemd[1]: Started Kibana.
```

http://localhost:5601 in browser to view the Dashboard of the kibana as show in the below image



XPACK

Before we configure use this all commands one by one

systemctl stop kibana

systemctl stop elasticsearch

nano /etc/elasticsearch/elasticsearch.yml

on this .yml file add xpack security

xpack.security.enabled: true

xpack.security.authc.api_key.enabled: true

```
# Elasticsearch security features are not enabled by default.
# These features are free, but require configuration changes to enable them.
# This means that users don't have to provide credentials and can get full access
# to the cluster. Network connections are also not encrypted.
#
# To protect your data, we strongly encourage you to enable the Elasticsearch security featu>
# Refer to the following documentation for instructions.
#
# https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stack-security.ht>
xpack.security.enabled: true
xpack.security.authc.api_key.enabled: true
```

systemctl restart elasticsearch

systemctl stop elasticsearch

systemctl start elasticsearch

cd /usr/share/elasticsearch/bin

```
root@ubuntu:/home/vboxuser# cd /usr/share/elasticsearch/bin
root@ubuntu:/usr/share/elasticsearch/bin#
```

sudo ./elasticsearch-setup-passwords auto

By using these commands some user names passwords will be generated

```
root@ubuntu:/usr/share/elasticsearch/bin# sudo ./elasticsearch-setup-passwords auto
```

Open kibana.yml

nano /etc/kibana/kibana.yml

```
root@ubuntu:~# nano /etc/kibana/kibana.yml
root@ubuntu:~#
```

Un command this line also

```
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]
```

elasticsearch. Username = “kibana_system”

elasticsearch. Password = “**********”

```
# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
elasticsearch.username: "kibana_system"
elasticsearch.password: "aLQTjFUSPJNYpHC8XfF5"
```

systemctl restart kibana

systemctl stop kibana

systemctl start kibana

```
root@ubuntu:~# systemctl restart kibana
root@ubuntu:~# systemctl stop kibana
root@ubuntu:~# systemctl start kibana
root@ubuntu:~#
```

systemctl status elasticsearch logstash kibana

```
root@ubuntu:~# systemctl status elasticsearch logstash kibana
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enab>
     Active: active (running) since Thu 2023-08-24 00:39:45 IST; 19min ago
       Docs: https://www.elastic.co
   Main PID: 52371 (java)
      Tasks: 77 (limit: 14281)
     Memory: 1020.0M
        CPU: 2min 17.291s
     CGroup: /system.slice/elasticsearch.service
             ├─52371 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.>
             └─52560 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/co>

Aug 24 00:39:21 ubuntu systemd[1]: Starting Elasticsearch...
Aug 24 00:39:45 ubuntu systemd[1]: Started Elasticsearch.

● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-08-24 00:58:42 IST; 16s ago
   Main PID: 55773 (java)
      Tasks: 18 (limit: 14281)
     Memory: 657.1M
        CPU: 46.963s
     CGroup: /system.slice/logstash.service
             └─55773 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC >

Aug 24 00:58:42 ubuntu systemd[1]: Started logstash.
Aug 24 00:58:42 ubuntu logstash[55773]: Using bundled JDK: /usr/share/logstash/jdk
Aug 24 00:58:42 ubuntu logstash[55773]: OpenJDK 64-Bit Server VM warning: Option UseConcMark>

● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-08-24 00:56:53 IST; 2min 5s ago
       Docs: https://www.elastic.co
   Main PID: 55534 (node)
      Tasks: 11 (limit: 14281)
     Memory: 275.3M
        CPU: 27.650s
     CGroup: /system.slice/kibana.service
             └─55534 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli>

Aug 24 00:56:53 ubuntu systemd[1]: Started Kibana.
lines 1-41/41 (END)
```

ZEEK installation

```
vboxuser@ubuntu:~$ sudo apt-get update
[sudo] password for vboxuser:
Hit:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [101 kB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [43.0 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [289 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:10 http://in.archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [4,920 B]
Get:11 http://in.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [15.5 kB]
Get:12 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [40.0 kB]
Fetched 832 kB in 4s (188 kB/s)
Reading package lists... Done
W: https://artifacts.elastic.co/packages/7.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/e
tc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
```

```
vboxuser@ubuntu:~$ sudo apt-get install cmake gcc g++ flex bison libcap-dev libssl-dev python3-dev swig zlib1g-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bison is already the newest version (2:3.8.2+dfsg-1build1).
flex is already the newest version (2.6.4-8build2).
g++ is already the newest version (4:11.2.0-1ubuntu1).
gcc is already the newest version (4:11.2.0-1ubuntu1).
swig is already the newest version (4.0.2-1ubuntu1).
cmake is already the newest version (3.22.1-1ubuntu1.22.04.1).
libcap-dev is already the newest version (1:2.44-1ubuntu0.22.04.1).
libssl-dev is already the newest version (3.0.2-0ubuntu1.10).
python3-dev is already the newest version (3.10.6-1~22.04).
zlib1g-dev is already the newest version (1:1.2.11.dfsg-2ubuntu9.2).
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 27 not upgraded.
```

```
vboxuser@ubuntu:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
vboxuser@ubuntu:~$ cd Downloads
vboxuser@ubuntu:~/Downloads$ cd zeek-6.0.0/
vboxuser@ubuntu:~/Downloads/zeek-6.0.0$ s
```

```
vboxuser@ubuntu:~/Downloads/zeek-6.0.0$ sudo apt-get install cmake gcc g++ flex bison libcap-dev libssl-dev python3-dev
swig zlib1g-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
bison is already the newest version (2:3.8.2+dfsg-1build1).
flex is already the newest version (2.6.4-8build2).
g++ is already the newest version (4:11.2.0-1ubuntu1).
gcc is already the newest version (4:11.2.0-1ubuntu1).
swig is already the newest version (4.0.2-1ubuntu1).
cmake is already the newest version (3.22.1-1ubuntu1.22.04.1).
libcap-dev is already the newest version (1:2.44-1ubuntu0.22.04.1).
libssl-dev is already the newest version (3.0.2-0ubuntu1.10).
python3-dev is already the newest version (3.10.6-1~22.04).
zlib1g-dev is already the newest version (1:1.2.11.dfsg-2ubuntu9.2).
The following packages were automatically installed and are no longer required:
  libflashrom1 libftdi1-2
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 27 not upgraded.
```

```
vboxuser@ubuntu:~/Downloads/zeek-6.0.0$ ./configure
Build Directory : build
Source Directory: /home/vboxuser/Downloads/zeek-6.0.0
Using cmake version 3.22.1

-- The C compiler identification is GNU 11.4.0
-- The CXX compiler identification is GNU 11.4.0
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Check for working C compiler: /usr/bin/cc - skipped
-- Detecting C compile features
-- Detecting C compile features - done
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Check for working CXX compiler: /usr/bin/c++ - skipped
-- Detecting CXX compile features
-- Detecting CXX compile features - done
-- Performing Test test_arch_x64
-- Performing Test test_arch_x64 - Success
-- Performing Test test_arch_aarch64
-- Performing Test test_arch_aarch64 - Failed
-- Performing Test test_arch_arm
-- Performing Test test_arch_arm - Failed
-- Performing Test test_arch_power
```

```
================================================================

-- Configuring done
-- Generating done
-- Build files have been written to: /home/vboxuser/Downloads/zeek-6.0.0/build
vboxuser@ubuntu:~/Downloads/zeek-6.0.0$
```

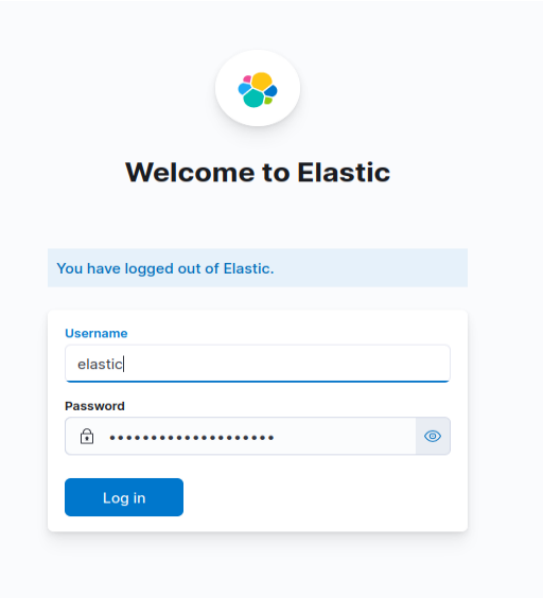
```
vboxuser@ubuntu:~/Downloads/zeek-6.0.0$ make
make -C build all
make[1]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
make[2]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
make[3]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
Consolidate compiler generated dependencies of target bifcl
make[3]: Leaving directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
[ 57%] Built target bifcl
make[3]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
make[3]: Leaving directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
[ 57%] Built target bif-plugin-Zeek_AF_Packet-af_packet.bif
make[3]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
make[3]: Leaving directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
[ 57%] Built target zeek_bison_outputs
make[3]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
make[3]: Leaving directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
[ 57%] Built target bif-std-zeek.bif
make[3]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
make[3]: Leaving directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
[ 57%] Built target bif-std-communityid.bif
make[3]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
make[3]: Leaving directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
[ 57%] Built target bif-std-stats.bif
make[3]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
make[3]: Leaving directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
[ 57%] Built target bif-std-event.bif
make[3]: Entering directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
make[3]: Leaving directory '/home/vboxuser/Downloads/zeek-6.0.0/build'
```

After generating passwords in previous step in that use

Login in the web page

username: elastic

password: ********(in there it will be there)



Fleet

Fleet

Centralized management for Elastic Agents.

Add Agent

Agents | Agent policies | Enrollment tokens | Data streams

Add a Fleet Server

A Fleet Server is required before you can enroll agents with Fleet. Follow the instructions below to set up a Fleet Server. For more information, see the Fleet and Elastic Agent Guide.

1 Select an Agent policy

Agent policies allow you to configure and manage your agents remotely. We recommend using the "Default Fleet Server policy" which includes the necessary configuration to run a Fleet Server.

Agent policy: Default Fleet Server policy

2 Download the Fleet Server to a centralized host

Fleet Server runs on an Elastic Agent. Install this agent on a centralized host so that other hosts you wish to monitor can connect to it. In production, we recommend using one or more dedicated hosts. You can download the Elastic Agent binaries and verification signatures from Elastic's download page.

Linux users: We recommend the installer (TAR) over system packages (RPM/DEB) because it lets you upgrade your agent in Fleet.

Go to download page

3 Choose a deployment mode for security

1 Select an Agent policy

Agent policies allow you to configure and manage your agents remotely
the necessary configuration to run a Fleet Server.

Agent policy: Default Fleet Server policy

2 Download the Fleet Server to a centralized host

Fleet Server runs on an Elastic Agent. Install this agent on a centralized host so that other hosts you wish to monitor can connect to it. In production, we recommend using one or more dedicated hosts. You can download the Elastic Agent binaries and verification signatures from Elastic's download page.

Linux users: We recommend the installer (TAR) over system packages (RPM/DEB) because it lets you upgrade your agent in Fleet.

Go to download page

elastic | Platform | Solutions | Customers | Resources | Pricing | Docs

Elastic Agent 7.17.12

LINUX 64-BIT sha
LINUX AARCH64 sha
DEB 64-BIT sha
DEB AARCH64 sha
RPM 64-BIT sha
RPM AARCH64 sha
WINDOWS 64-BIT sha
MAC sha

3 Choose a deployment mode for security

Fleet uses Transport Layer Security (TLS) to encrypt traffic between Elastic Agents and other components in the Elastic Stack. Choose a deployment mode to determine how you wish to handle certificates. Your selection will affect the Fleet Server set up command shown in a later step.

- (●) **Quick start** – Fleet Server will generate a self-signed certificate. Subsequent agents must be enrolled using the --insecure flag. Not recommended for production use cases.
- ( ) **Production** – Provide your own certificates. This option will require agents to specify a cert key when enrolling with Fleet

4 Add your Fleet Server host

Specify the URL your agents will use to connect to Fleet Server. This should match the public IP address or domain of the host where Fleet Server will run. By default, Fleet Server uses port `8220`.

Fleet Server host: http://localhost:8200 | Add host

4 Add your Fleet Server host

Specify the URL your agents will use to connect to Fleet Server. This should match the public IP address or domain of the host where Fleet Server will run. By default, Fleet Server uses port `8220`.

Fleet Server host: e.g. http://127.0.0.1:8220 | Add host

✓ Added Fleet Server host

Added http://localhost:8200. You can edit your Fleet Server hosts in Fleet Settings.

5 Generate a service token

A service token grants Fleet Server permissions to write to Elasticsearch.

✓ Save your service token information. This will be shown only once.

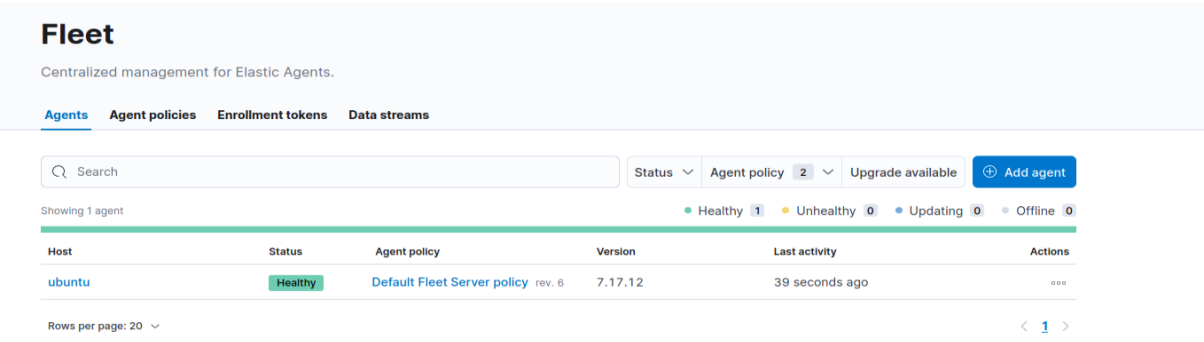
Service token

AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2OTI4MjAxOTM5ODA6dnRjUkNnd1ZUdHl1S0x1VEpFTlJsZw

```
root@ubuntu:~# cd /home/vboxuser/Downloads/elastic-agent-7.17.12-linux-x86_64
root@ubuntu:/home/vboxuser/Downloads/elastic-agent-7.17.12-linux-x86_64#
```

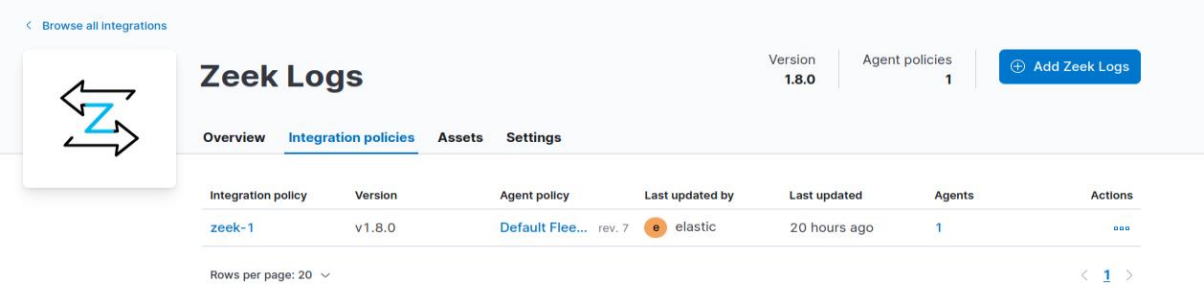
```
root@ubuntu:~# cd /home/vboxuser/Downloads/elastic-agent-7.17.12-linux-x86_64
root@ubuntu:/home/vboxuser/Downloads/elastic-agent-7.17.12-linux-x86_64# sudo ./elastic-agent
 install   \
  --fleet-server-es=http://localhost:9200 \
  --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2OTI4MjAxOTM5ODA6dn
RjUkNnd1ZUdHl1S0x1VEpFTlJsZw \
  --fleet-server-policy=499b5aa7-d214-5b5d-838b-3cd76469844e \
  --fleet-server-insecure-http
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want
to continue? [Y/n]:Y
```

```
Elastic Agent will be installed at /opt/Elastic/Agent and will run as a service. Do you want
to continue? [Y/n]:Y
2023-08-24T01:30:47.321+0530    INFO    cmd/enroll_cmd.go:743   Waiting for Elastic Agent to
start Fleet Server
2023-08-24T01:30:49.330+0530    INFO    cmd/enroll_cmd.go:776   Fleet Server - Starting
2023-08-24T01:30:53.337+0530    INFO    cmd/enroll_cmd.go:757   Fleet Server - Running on pol
icy with Fleet Server integration: 499b5aa7-d214-5b5d-838b-3cd76469844e; missing config fleet
.agent.id (expected during bootstrap process)
2023-08-24T01:30:53.338+0530    WARN    [tls]   tlscommon/tls_config.go:101     SSL/TLS verif
ications disabled.
2023-08-24T01:30:54.165+0530    INFO    cmd/enroll_cmd.go:454   Starting enrollment to URL: h
ttp://localhost:8220/
2023-08-24T01:30:56.864+0530    INFO    cmd/enroll_cmd.go:254   Successfully triggered restar
t on running Elastic Agent.
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
root@ubuntu:/home/vboxuser/Downloads/elastic-agent-7.17.12-linux-x86_64# S
```

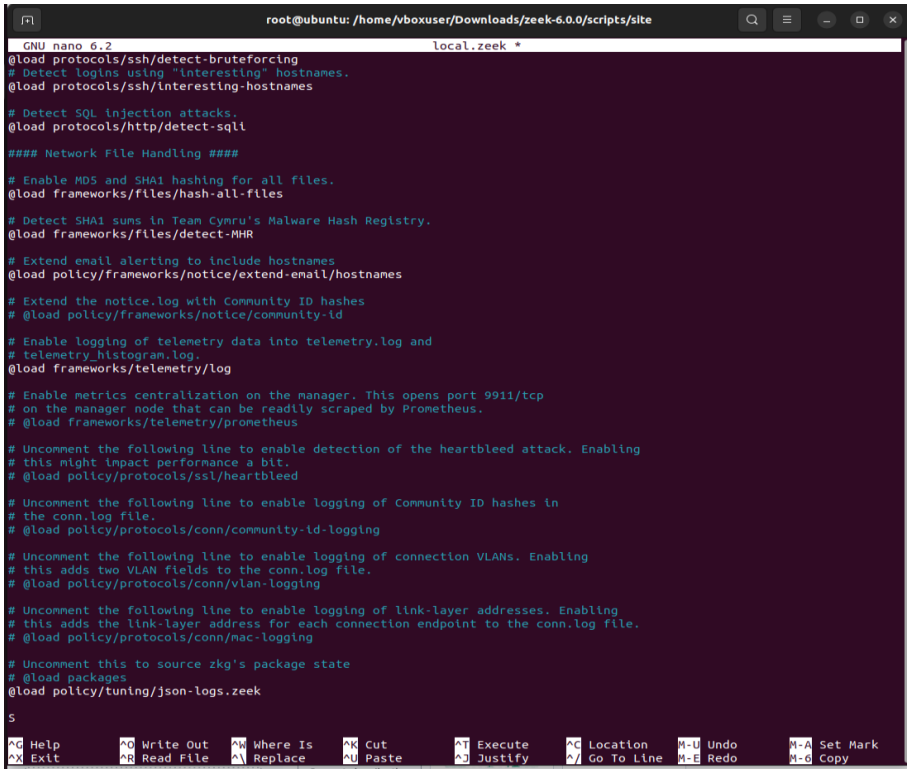


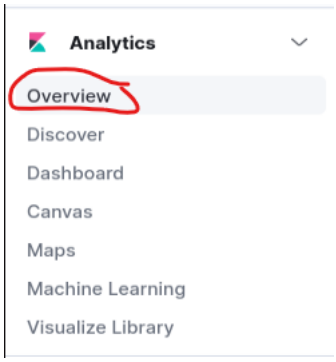
Add Zeek Logs

Integrations ➡️ search Zeek logs

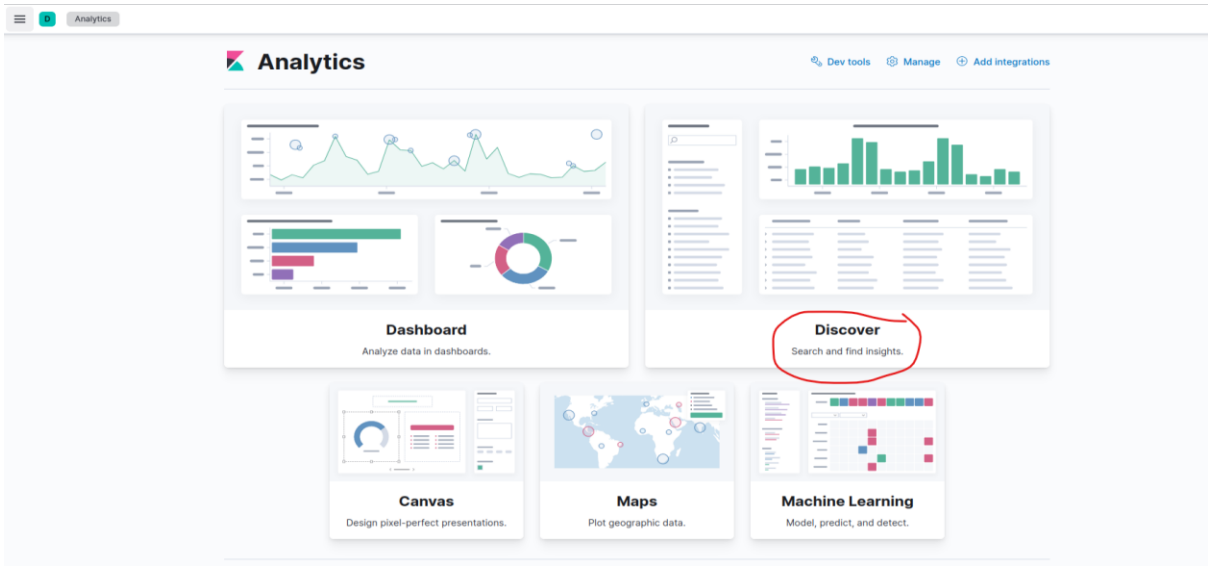



```
root@ubuntu:/home/vboxuser# cd Downloads/
root@ubuntu:/home/vboxuser/Downloads# cd zeek-6.0.0/
root@ubuntu:/home/vboxuser/Downloads/zeek-6.0.0# cd scripts
root@ubuntu:/home/vboxuser/Downloads/zeek-6.0.0/scripts# cd site/
root@ubuntu:/home/vboxuser/Downloads/zeek-6.0.0/scripts/site# nano local.zeek
```



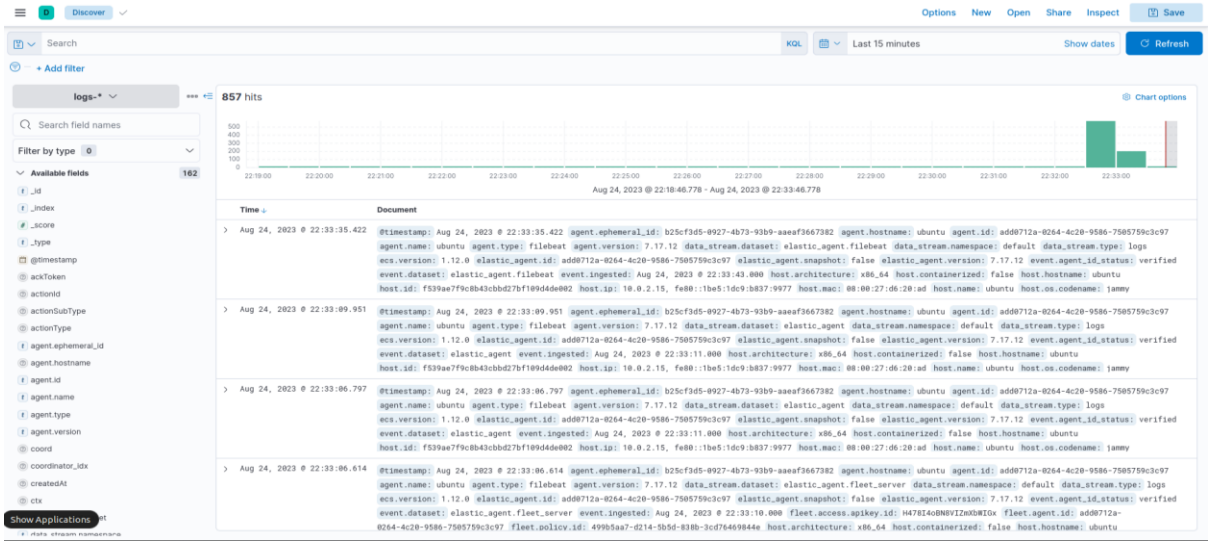


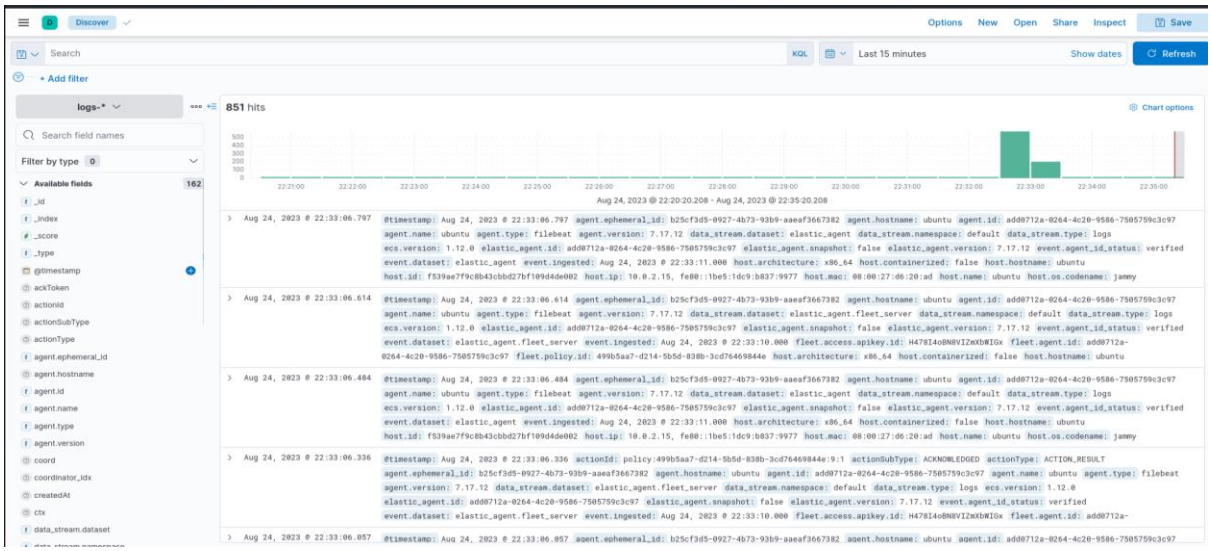
U get display like this



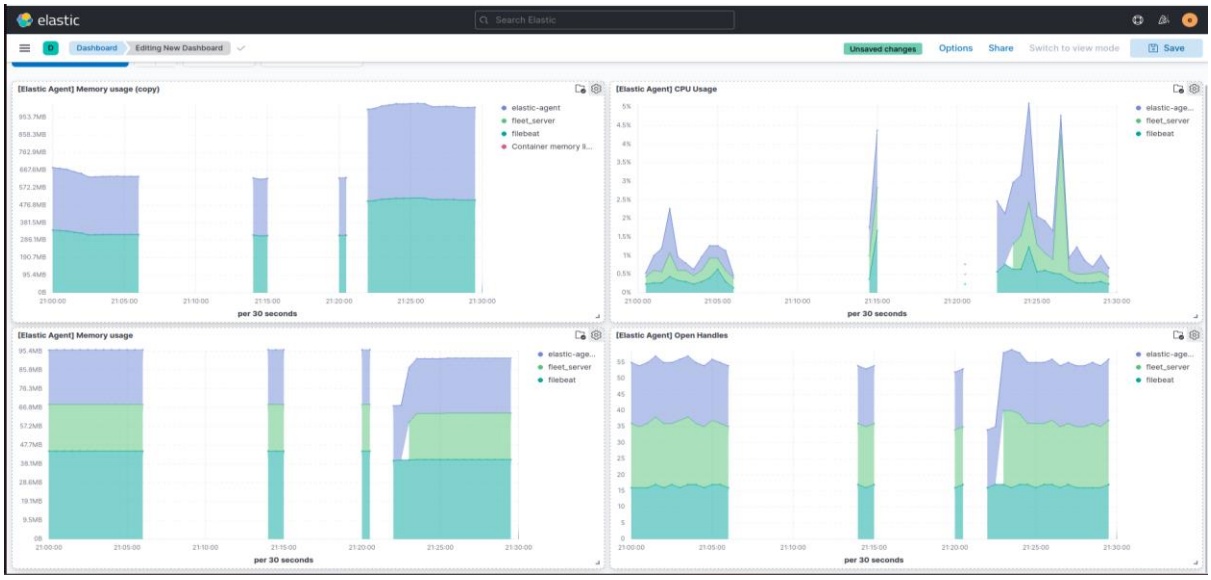
On clicking Discover

U can see the system logs



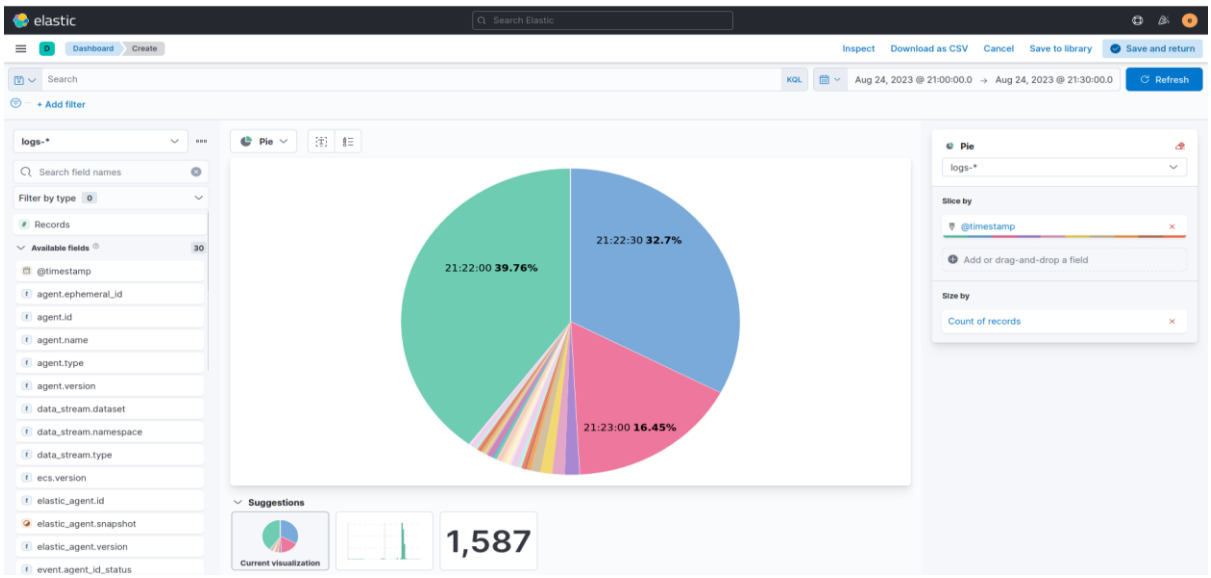


Dashboard

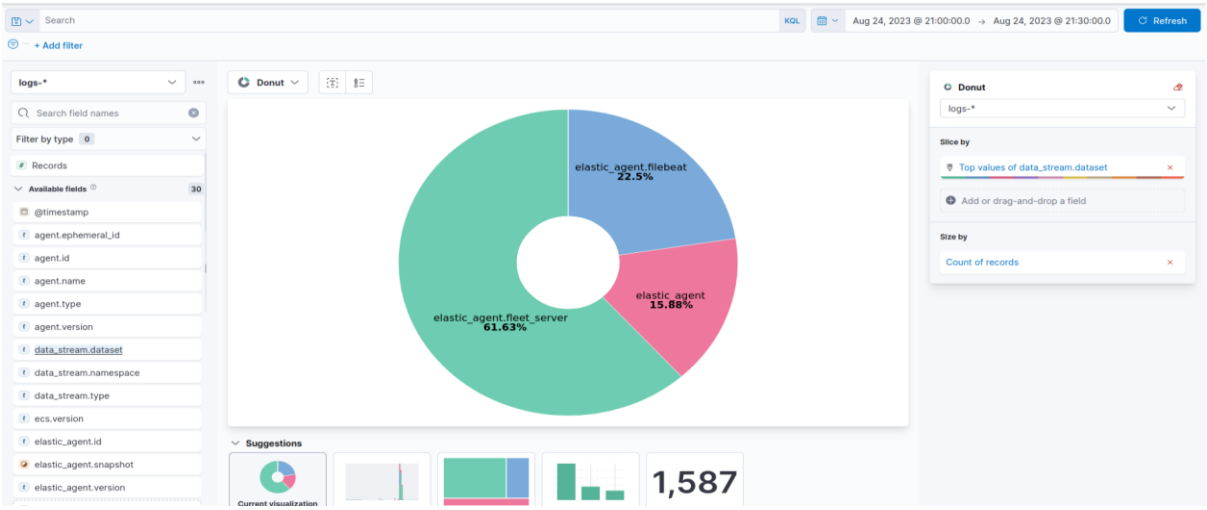


Pie charts

@timestamp



data_stream.dataset


Search
KQL
Aug 24, 2023 @ 21:00:00.0 → Aug 24, 2023 @ 21:30:00.0
Refresh
+ Add filter
logs-*
Donut
Search field names
Filter by type 0
Records
Available fields 30
@timestamp
agent.ephemeral_id
agent.id
agent.name
agent.type
agent.version
data_stream.dataset
data_stream.namespace
data_stream.type
ecs.version
elastic_agent.id
elastic_agent.snapshot
elastic_agent.version
elastic_agent.filebeat
22.5%
elastic_agent
15.88%
elastic_agent.fleet_server
61.63%
Suggestions
Current visualization
1,587
Donut
logs-*
Slice by
Top values of data_stream.dataset
Add or drag-and-drop a field
Size by
Count of records