PALADUGU ANKITHA

21BCE7836

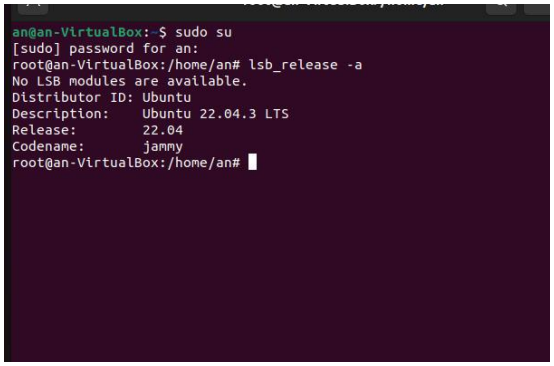
CYBER PHYSICAL SYSTEM PROJECT REPORT

Elasticsearch, Logstash, Kibana Deployment

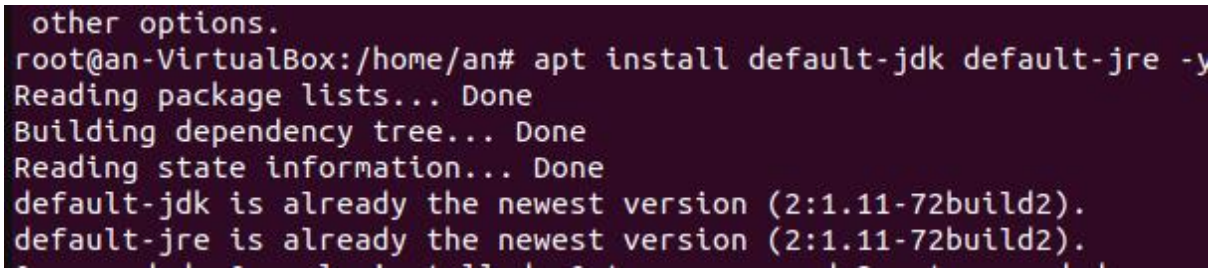
Deploying the Elasticsearch-Logstash-Kibana (ELK) stack involves setting up and configuring Elasticsearch for data storage and searching, Logstash for data processing and enrichment, and Kibana for data visualization. This stack is commonly used for log and event data analysis. Here's a high-level overview of the deployment process

Before installation of ELK do set up for dependencies required :

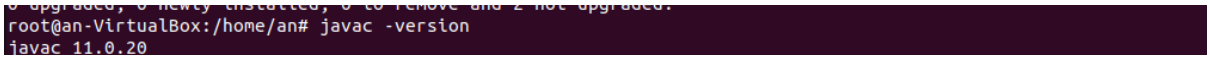
Ubuntu version



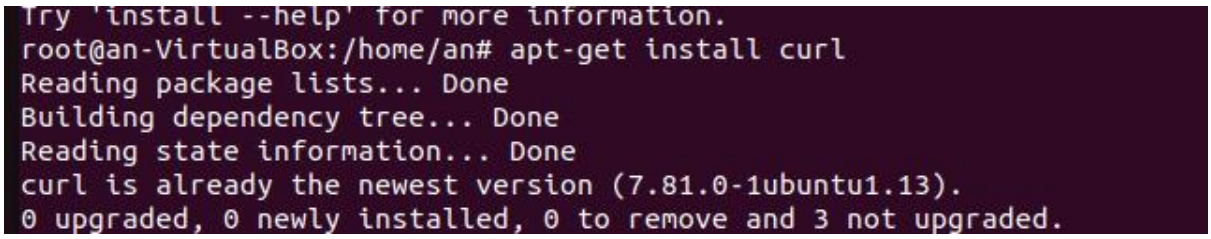
Java dependencies install



Check java version



Make sure that curl installed if not then install curl



Add the elasticsearch APT repository key by using the below command (run these commands in root privilege).

```
root@an-VirtualBox:/home/an# javac -version
javac 11.0.20
root@an-VirtualBox:/home/an# 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
```

Add the Elastic Search to the APT source List by using the below command

```
OK
root@an-VirtualBox:/home/an# 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
```

- **Installation of Elastic search:**

apt update

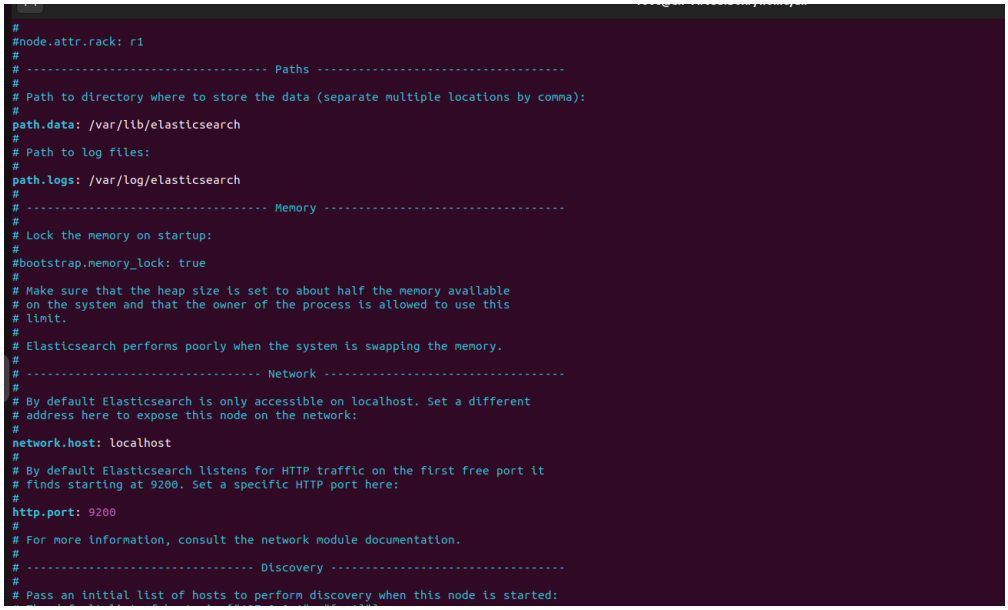
```
bash: /etc/apt/sources.list.d/: Is a directory
root@an-VirtualBox:/home/an# apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Install elastic search

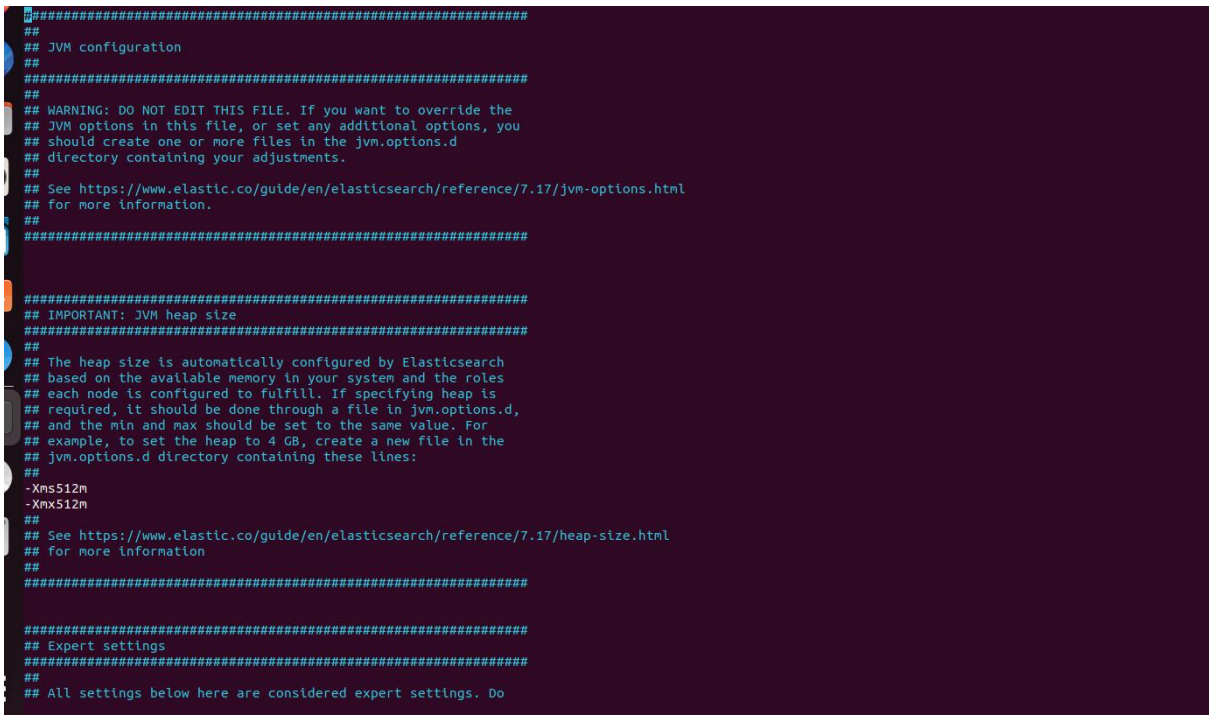
```
oot@an-VirtualBox:/home/an#  apt install elasticsearch -y
eading package lists... Done
uilding dependency tree... Done
eading state information... Done
he following NEW packages will be installed:
 elasticsearch
 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
eed to get 318 MB of archives.
fter this operation, 531 MB of additional disk space will be used.
et:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 elasticsearch amd64 7.17.12 [318 MB]
etched 318 MB in 2min 43s (1,951 kB/s)
electing previously unselected package elasticsearch.
Reading database ... 163848 files and directories currently installed.)
reparing to unpack .../elasticsearch_7.17.12_amd64.deb ...
reating elasticsearch group... OK
reating elasticsearch user... OK
npacking elasticsearch (7.17.12) ...
etting up elasticsearch (7.17.12) ...
## NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using syste
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
## You can start elasticsearch service by executing
sudo systemctl start elasticsearch.service
reated elasticsearch keystore in /etc/elasticsearch/elasticsearch.keystore
```

Configuration of elasticsearch

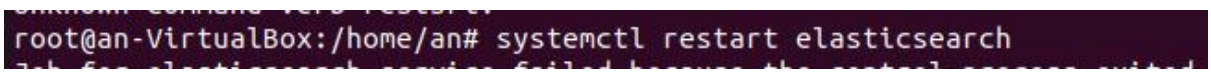
```
oot@an-VirtualBox:/home/an# nano /etc/elasticsearch/elasticsearch.yml
```



Configure the JVM heap memory by using the below command



Restart elasticsearch



Enable elastic search

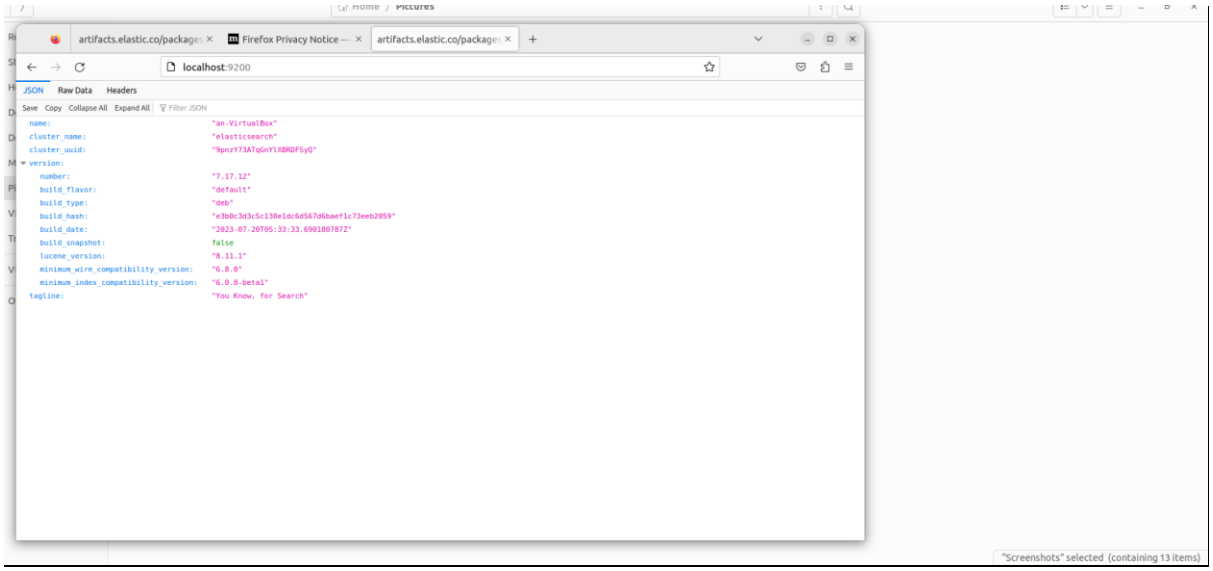
```
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
root@an-VirtualBox:/home/an#
```

Ping the Elastic Search to verify installation by using the below command

```
root@an-VirtualBox:/home/an# curl -X GET "localhost:9200"
{
  "name" : "an-VirtualBox",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "9pnzY73ATqGnYlXBRDFSyQ",
  "version" : {
    "number" : "7.17.12",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "e3b0c3d3c5c130e1dc6d567d6baef1c73eeb2059",
    "build_date" : "2023-07-20T05:33:33.690180787Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
root@an-VirtualBox:/home/an#
```

Search on browser :

localhost:9200



- **Installation of logstash**

```
root@an-VirtualBox:/home/an# apt install logstash -y
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 2 not upgraded.
Need to get 366 MB of archives.
After this operation, 623 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 logstash amd64 1:7.17.12-1 [366 MB]
Fetched 366 MB in 2min 49s (2,167 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 166886 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a7.17.12-1_amd64.deb ...
Unpacking logstash (1:7.17.12-1) ...
Setting up logstash (1:7.17.12-1) ...
Using bundled JDK: /usr/share/logstash/jdk
Using provided startup.options file: /etc/logstash/startup.options
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
/usr/share/logstash/vendor/bundle/jruby/2.5.0/gems/pleaserun-0.0.32/lib/pleaserun/platform/base.rb:112: warning: constant ::Fixnum is deprecated
Successfully created system startup script for Logstash
root@an-VirtualBox:/home/an#
```

Checking that logstash is working or not :

```
oot@an-VirtualBox:/home/an# systemctl status logstash
logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-08-23 17:07:14 IST; 11s ago
   Main PID: 16065 (java)
      Tasks: 18 (limit: 4009)
     Memory: 506.5M
        CPU: 36.453s
     CGroup: /system.slice/logstash.service
             └─16065 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.awt.headless=true -Dfile.encodi

ug 23 17:07:14 an-VirtualBox systemd[1]: Started logstash.
ug 23 17:07:14 an-VirtualBox logstash[16065]: Using bundled JDK: /usr/share/logstash/jdk
ug 23 17:07:14 an-VirtualBox logstash[16065]: OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
lines 1-13/13 (END)
```

- **Kibana Set up**

```
bash: /etc/apt/sources.list.d/: Is a directory
root@an-VirtualBox:/home/an# apt update
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:2 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
2 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Kibana Installation

```
root@an-VirtualBox:/home/an# apt install kibana -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 2 not upgraded.
Need to get 276 MB of archives.
After this operation, 673 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 kibana amd64 7.17.12 [276 MB]
Fetched 276 MB in 2min 15s (2,040 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 182259 files and directories currently installed.)
Preparing to unpack .../kibana_7.17.12_amd64.deb ...
Unpacking kibana (7.17.12) ...
Setting up kibana (7.17.12) ...
Creating kibana group... OK
Creating kibana user... OK
Created Kibana keystore in /etc/kibana/kibana.keystore
root@an-VirtualBox:/home/an#
```

Before Configuration set up make sure that you stop all services

Stop kibana

sudo systemstl stop kibana

Stop Elasticsearch

Sudo systemctl stop elasticsearch

Configuration

open to elasticsearch.yml

sudo nano /etc/elasticsearch/elasticsearch.yml

```
oot@an-VirtualBox:/home/an# nano /etc/elasticsearch/elasticsearch.yml
```

Add to elasticsearch.yml:

xpack.security.enabled: true

xpack.security.authc.api_key.enabled: true

```
GNU nano 6.2                                                    /etc/elasticsearch/elasticsearch.yml
#
# For more information, consult the network module documentation.
#
# ---------------------------------- Discovery -----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]

#
discovery.type: single node

#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
# ---------------------------------- Various -----------------------------------
#
# Require explicit names when deleting indices:
#
#action.destructive_requires_name: true
#
# ---------------------------------- Security ----------------------------------
#
#                                *** WARNING ***
#
# 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 features.
# Refer to the following documentation for instructions.
#
# https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stack-security.html
 xpack.security.enabled: true
xpack.security.authc.api_key.enabled: true

^G Help          ^O Write Out     ^W Where Is      ^K Cut           ^T Execute       ^C Location      M-U Undo         M-A Se
^X Exit          ^R Read File     ^\ Replace       ^U Paste         ^J Justify       ^/ Go To Line    M-E Redo         M-6 Co
```

Now restart elasticsearch

sudo systemctl restart elasticsearch

```
[sudo] password for an:
root@an-VirtualBox:/home/an# systemctl start elasticsearch
```

Set up default password :

cd usr/share/elasticsearch/bin

sudo ./elasticsearch-setup-passwords auto

Make sure you give elastic user name and password

```
root@an-VirtualBox:/home/an#  vim /etc/kibana/kibana.yml
root@an-VirtualBox:/home/an#
```

Give elasticsearch username and password

```
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

# 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: "elasticsearch"
elasticsearch.password: "pass"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
# If may use this token instead of a username/password.
# elasticsearch.serviceAccountToken: "my_token"
```

Configure kibana uncomment server port and host

```
root@an-VirtualBox:/home/an#  vim /etc/kibana/kibana.yml
root@an-VirtualBox:/home/an#
```

```
# 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 are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "localhost"

## Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# This setting was effectively always `false` before Kibana 6.3 and will
# default to `true` starting in Kibana 7.0.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

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

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

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these settings provide
```

Save the changes and restart kibana

Systemctl restart kibana

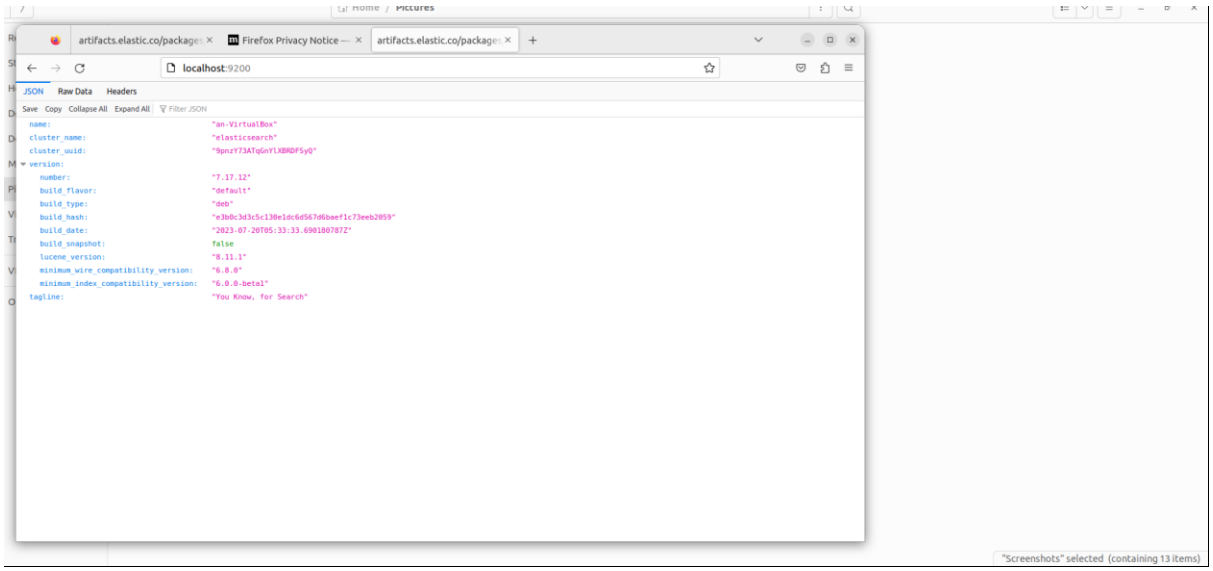
```
7:19:44 an-VirtualBox systemd[1]: Started Kibana.
12/12 (END)
opped                    systemctl status kibana
: systemstl stop kibana
```

Give a command sudo systemctl status elasticseach logstash kibana

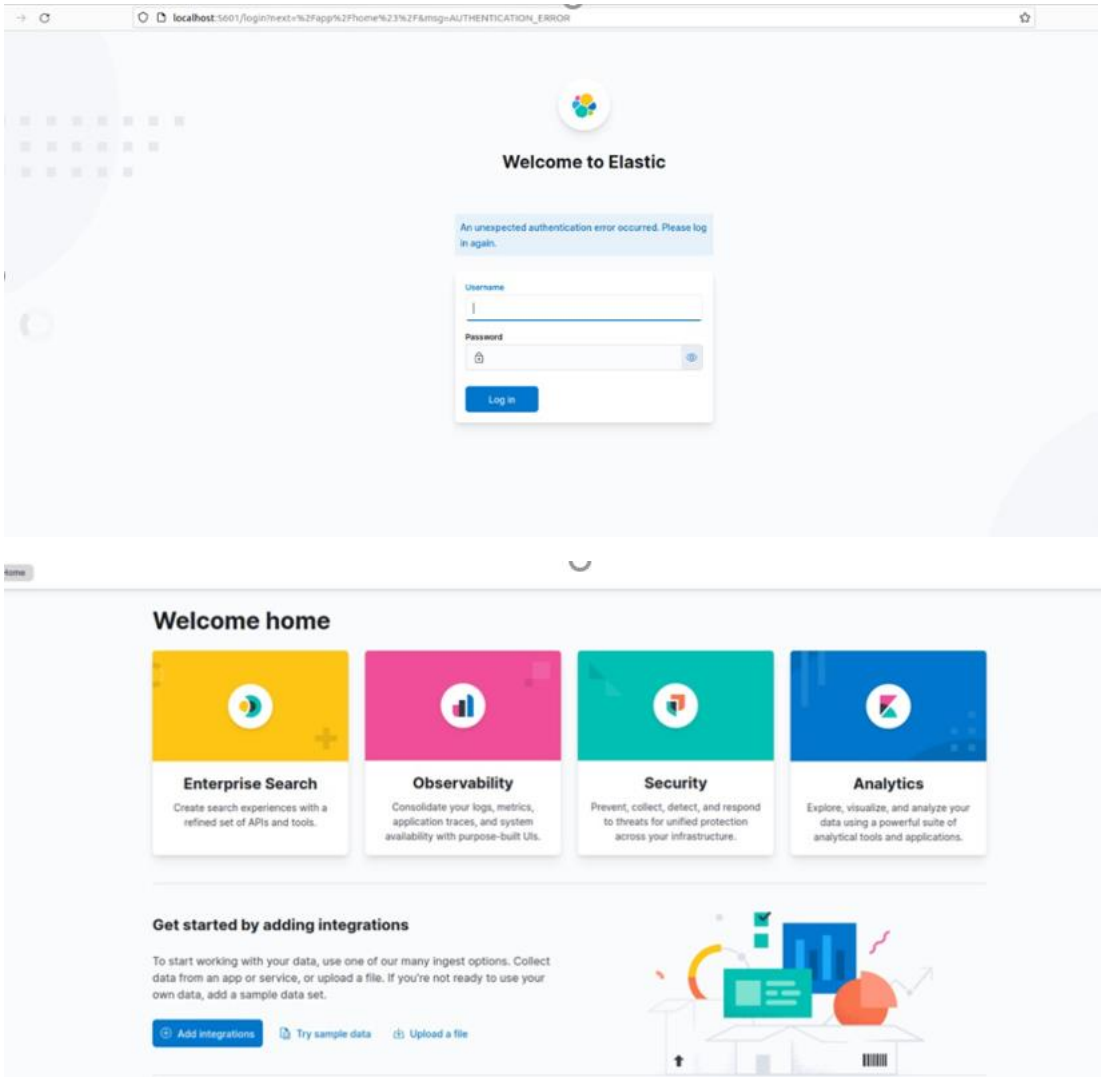
```
oot@an-VirtualBox:/home/an# systemctl status logstash
logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2023-08-23 17:07:14 IST; 11s ago
   Main PID: 16065 (java)
      Tasks: 18 (limit: 4009)
     Memory: 506.5M
        CPU: 36.453s
     CGroup: /system.slice/logstash.service
             └─16065 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.awt.headless=true -Dfile.encodi

ug 23 17:07:14 an-VirtualBox systemd[1]: Started logstash.
ug 23 17:07:14 an-VirtualBox logstash[16065]: Using bundled JDK: /usr/share/logstash/jdk
ug 23 17:07:14 an-VirtualBox logstash[16065]: OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
ines 1-13/13 (END)
```

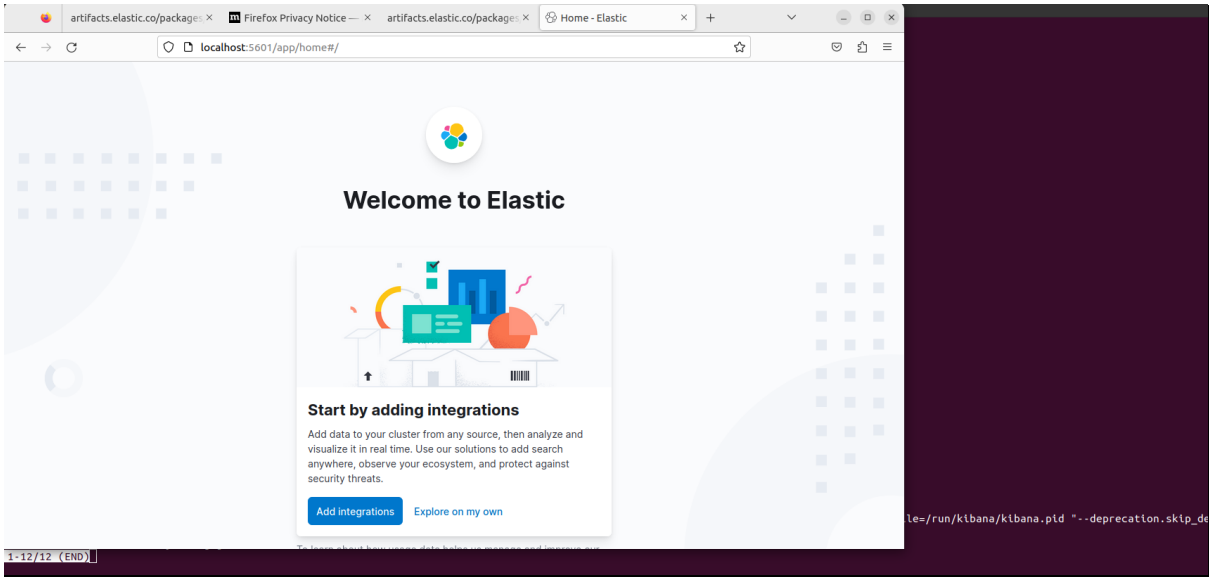
Open browser on ubuntu

Search localhost:9200

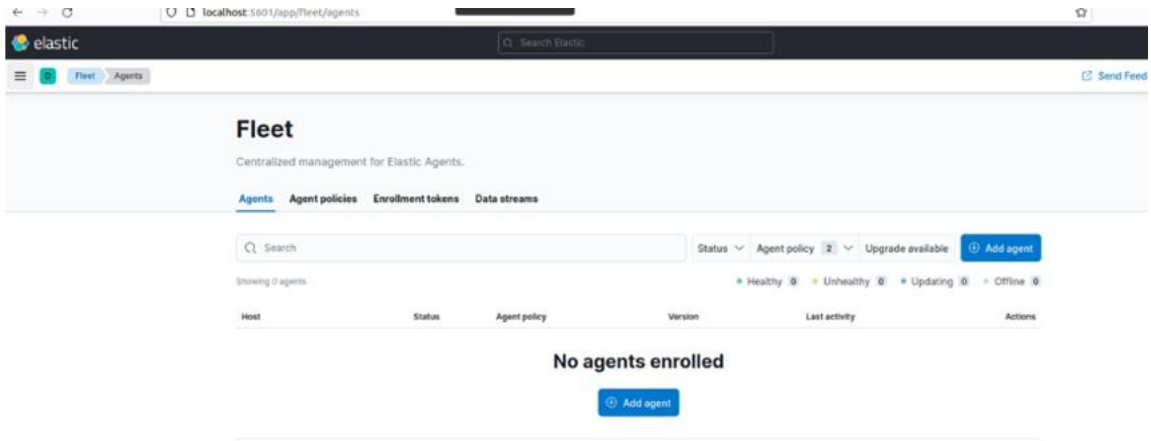


localhost:5200

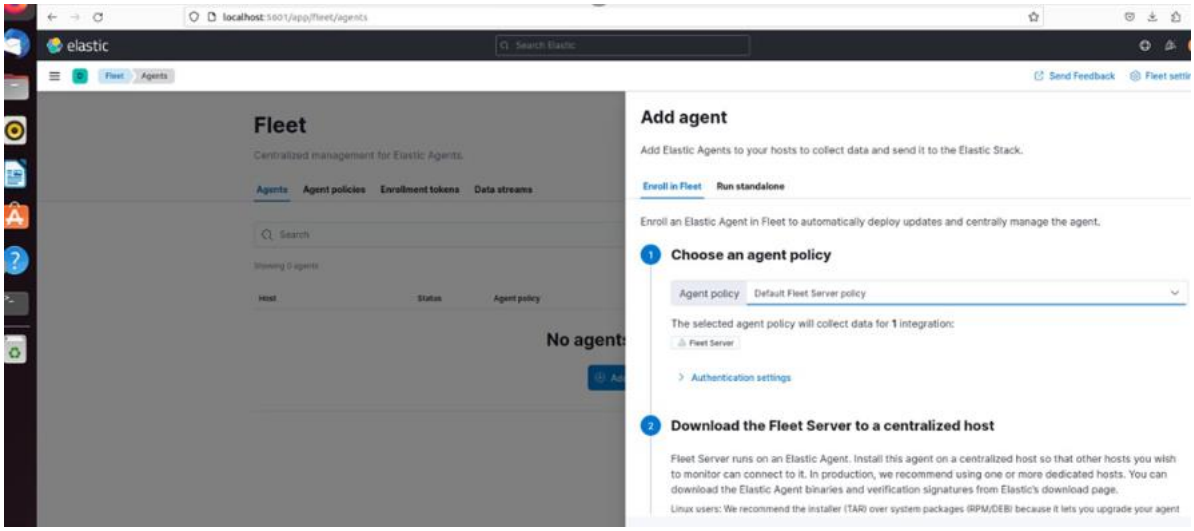




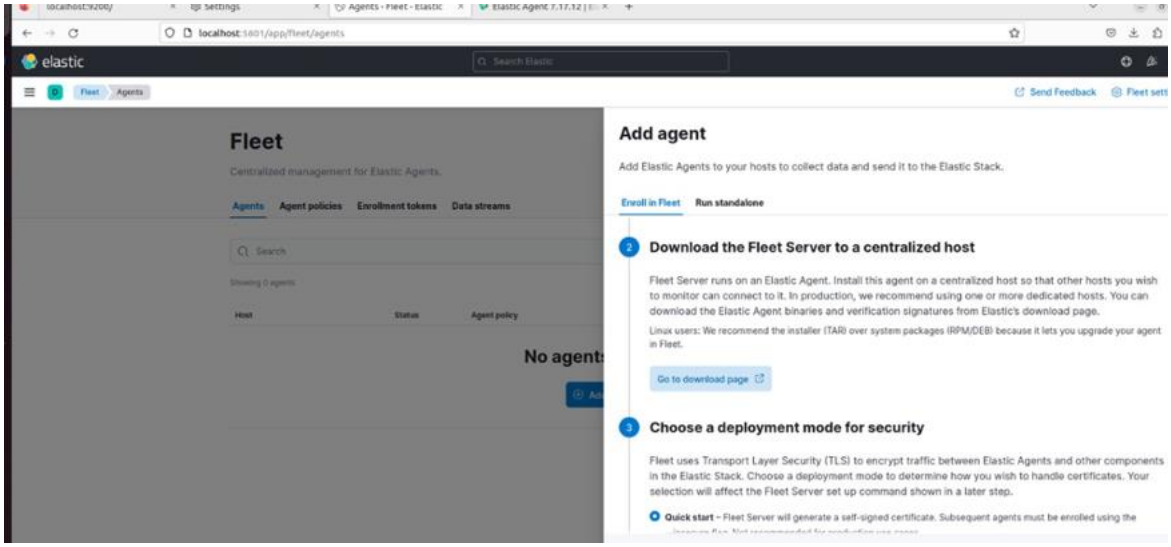
Go to management> FLEET



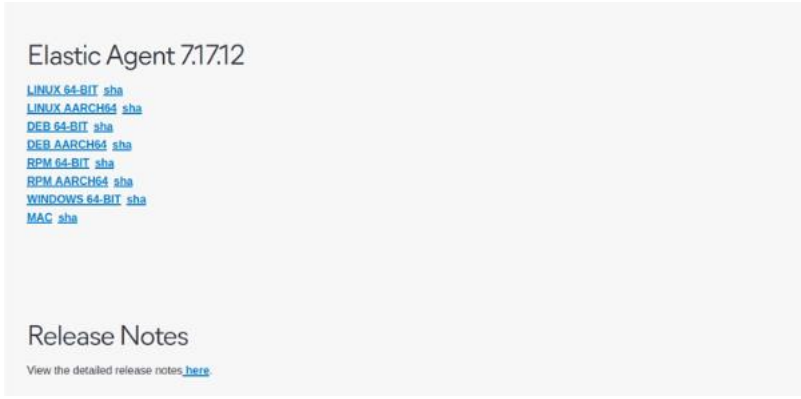
Add agent

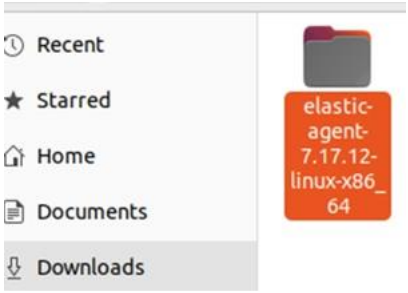


Download fleet centralised host



Click download and Download

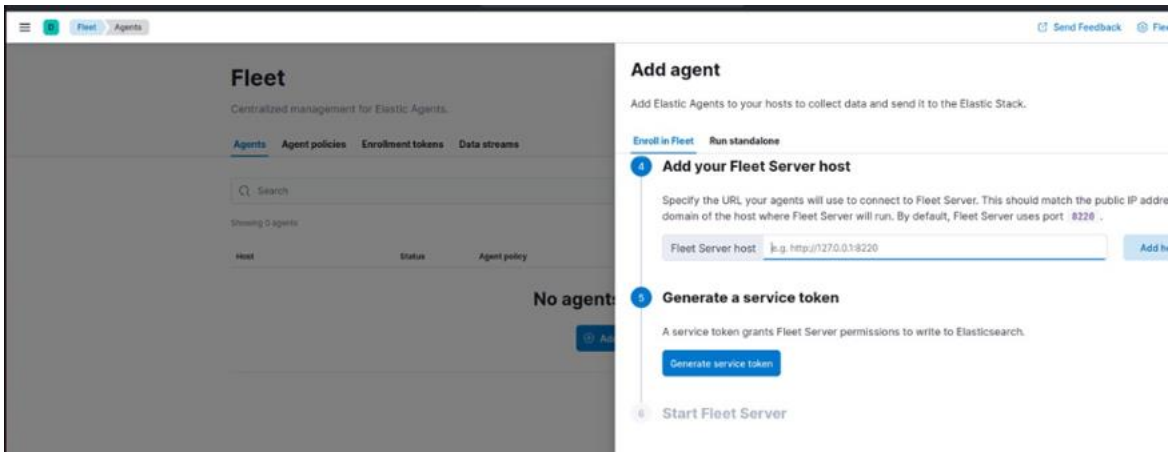


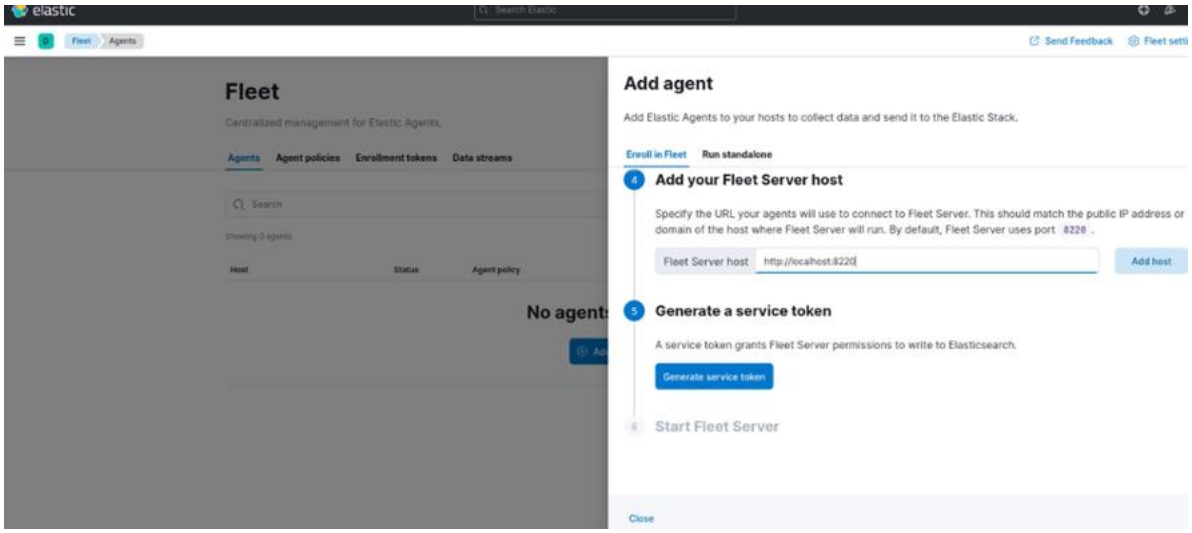


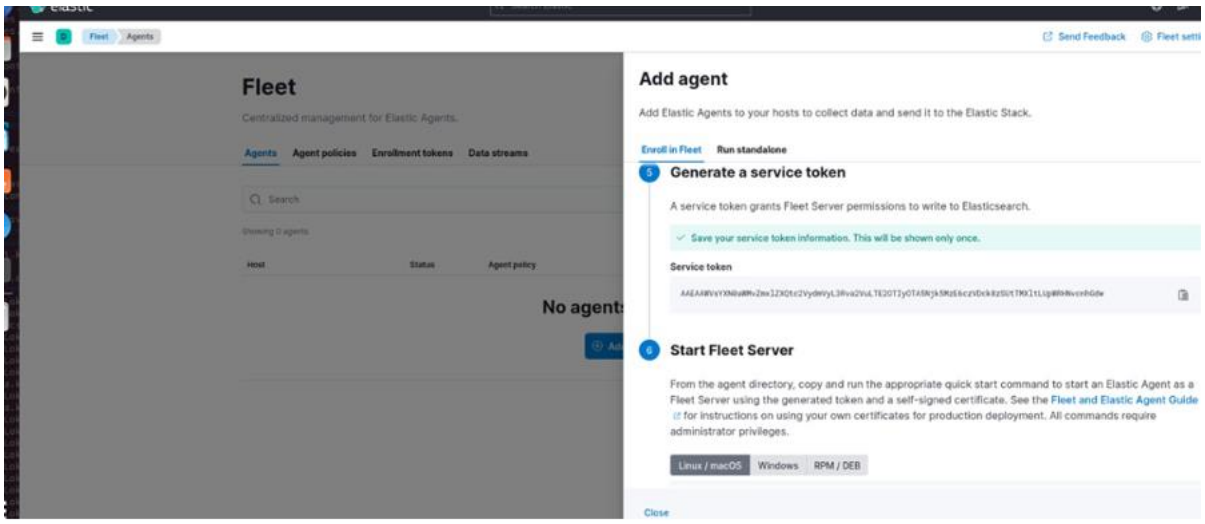
Add yours fleet host server

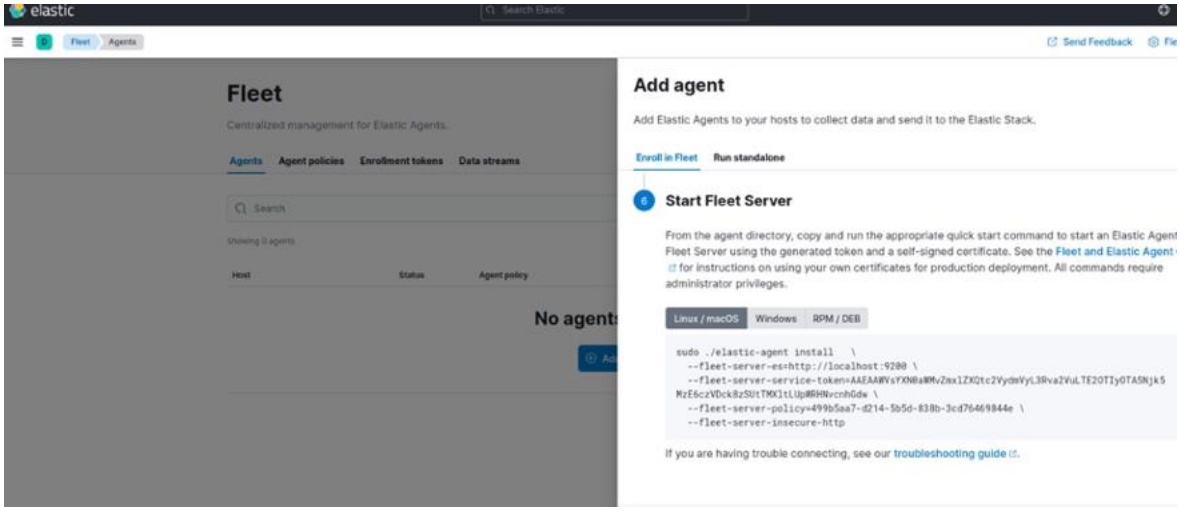
Fleet Server host : http://localhost:8220 then click on add host

Complete the following steps:


Fleet
Agents
Send Feedback
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Data streams
Search
Host
Status
Agent policy
No agents
Add agent
Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.
Enroll in Fleet
Run standalone
4 Add your Fleet Server host
Specify the URL your agents will use to connect to Fleet Server. This should match the public IP addre
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
5 Generate a service token
A service token grants Fleet Server permissions to write to Elasticsearch.
Generate service token
6 Start Fleet Server


elastic
Fleet
Agents
Send Feedback
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Data streams
Search
Host
Status
Agent policy
No agents
Add agent
Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.
Enroll in Fleet
Run standalone
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:8220
Add host
5 Generate a service token
A service token grants Fleet Server permissions to write to Elasticsearch.
Generate service token
6 Start Fleet Server
Close


Fleet
Agents
Send Feedback
Fleet
Centralized management for Elastic Agents.
Agents
Agent policies
Enrollment tokens
Data streams
Search
Host
Status
Agent policy
No agents
Add agent
Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.
Enroll in Fleet
Run standalone
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
6 Start Fleet Server
From the agent directory, copy and run the appropriate quick start command to start an Elastic Agent as a
Fleet Server using the generated token and a self-signed certificate. See the Fleet and Elastic Agent Guide
for instructions on using your own certificates for production deployment. All commands require
administrator privileges.
Linux / macOS
Windows
RPM / DEB
Close



Copy commands and give those command in ubuntu terminal (give commands related to which environment based elastic agent you downloaded)

Go to the path of elastic agent and paste the fleet server commands

Fleet server hosted

Make sure zeek logs are running


```
checking configurations ...
installing ...
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/auto ...
creating policy directories ...
installing site policies ...
generating standalone-layout.zeek ...
generating local-networks.zeek ...
generating zeekctl-config.zeek ...
generating zeekctl-config.sh ...
stopping ...
stopping zeek ...
creating crash report for previously crashed nodes: zeek
starting ...
starting zeek ...
```

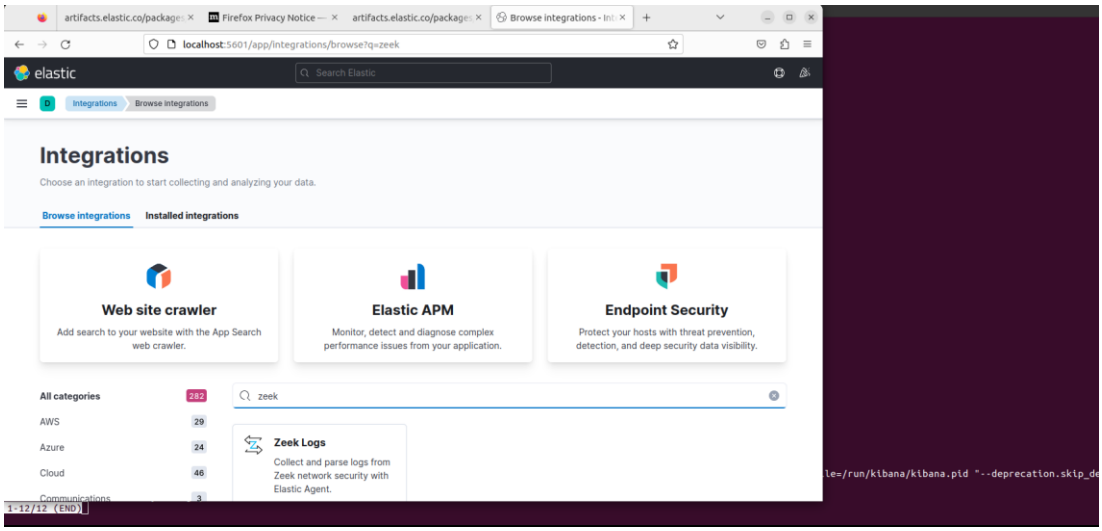
Go to local.zeek and add a line @load policy/tuning/json_logs.zeek

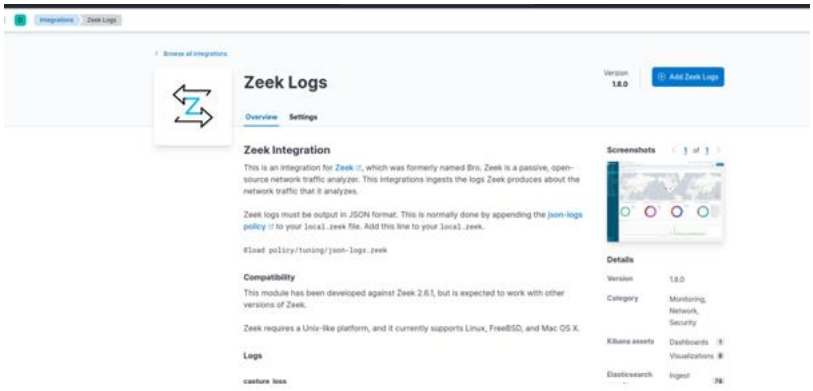
Add at the end of the file @load policy/tuning/json-logs.zeek → to solve error of getting zeek logs

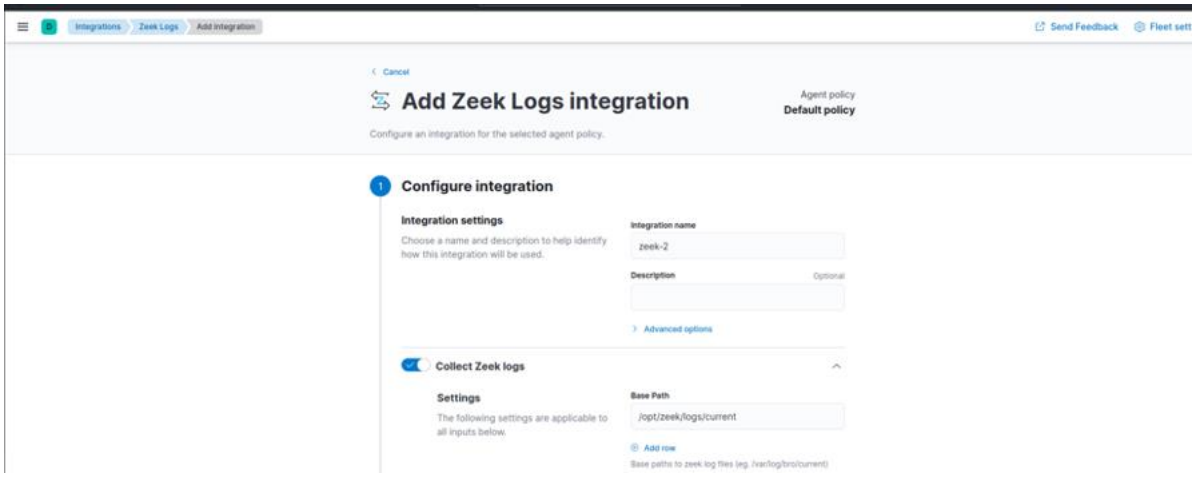
```
@load protocols/http/detect-sqli

#### Network File Handling ####

# Enable MD5 and SHA1 hashing for all files.
@load frameworks/files/hash-all-files

# Detect SHA1 sums in Team Cymru's Malware Hash Registry.
@load frameworks/files/detect-MHR

# Extend email alerting to include hostnames
@load policy/frameworks/notice/extend-email/hostnames

# Extend the notice.log with Community ID hashes
# @load policy/frameworks/notice/community-id

# Enable logging of telemetry data into telemetry.log and
# telemetry_histogram.log.
@load frameworks/telemetry/log

# Enable metrics centralization on the manager. This opens port 9911/tcp
# on the manager node that can be readily scraped by Prometheus.
# @load frameworks/telemetry/prometheus

# Uncomment the following line to enable detection of the heartbleed attack. Enabling
# this might impact performance a bit.
# @load policy/protocols/ssl/heartbleed

# Uncomment the following line to enable logging of Community ID hashes in
# the conn.log file.
# @load policy/protocols/conn/community-id-logging

# Uncomment the following line to enable logging of connection VLANs. Enabling
# this adds two VLAN fields to the conn.log file.
# @load policy/protocols/conn/vlan-logging

# Uncomment the following line to enable logging of link-layer addresses. Enabling
# this adds the link-layer address for each connection endpoint to the conn.log file.
# @load policy/protocols/conn/mac-logging

# Uncomment this to source zkg's package state
# @load packages
```

Restart zeek

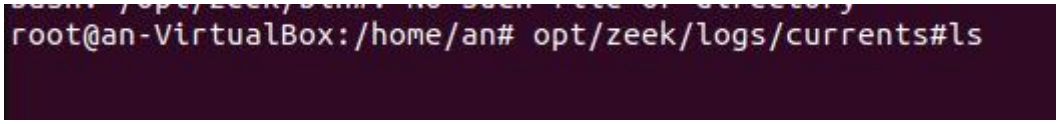
Go to integrations>> search zeek logs



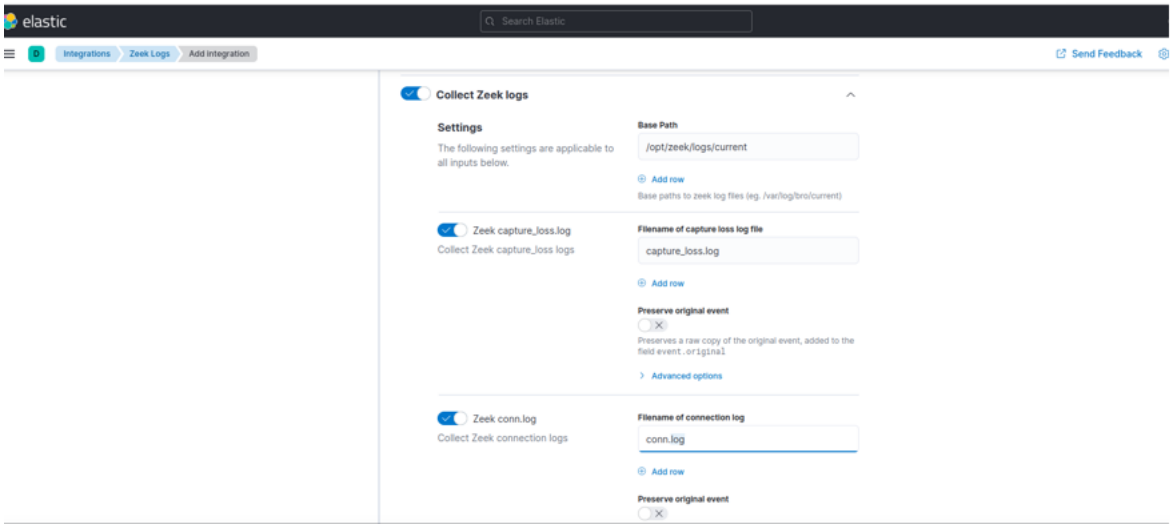


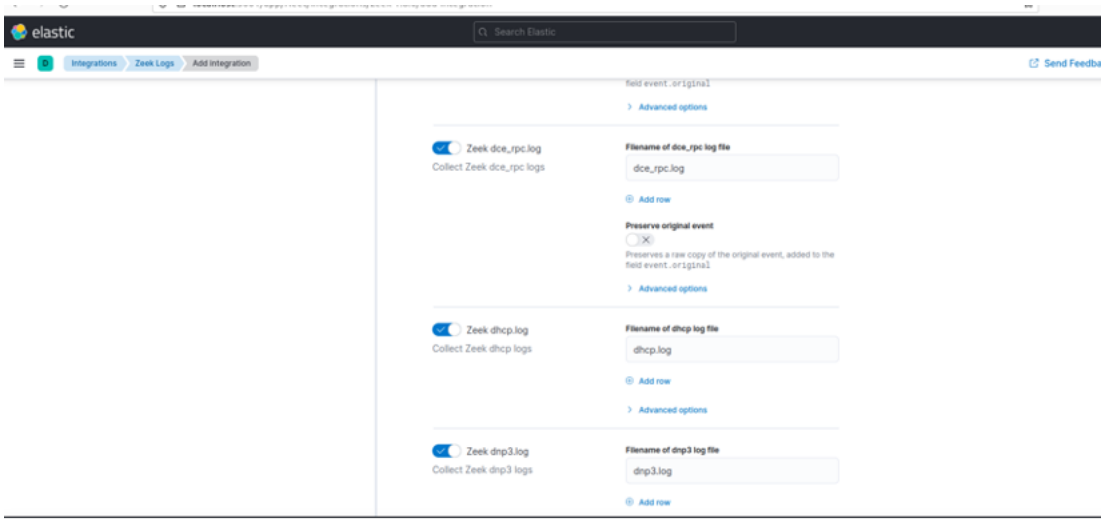


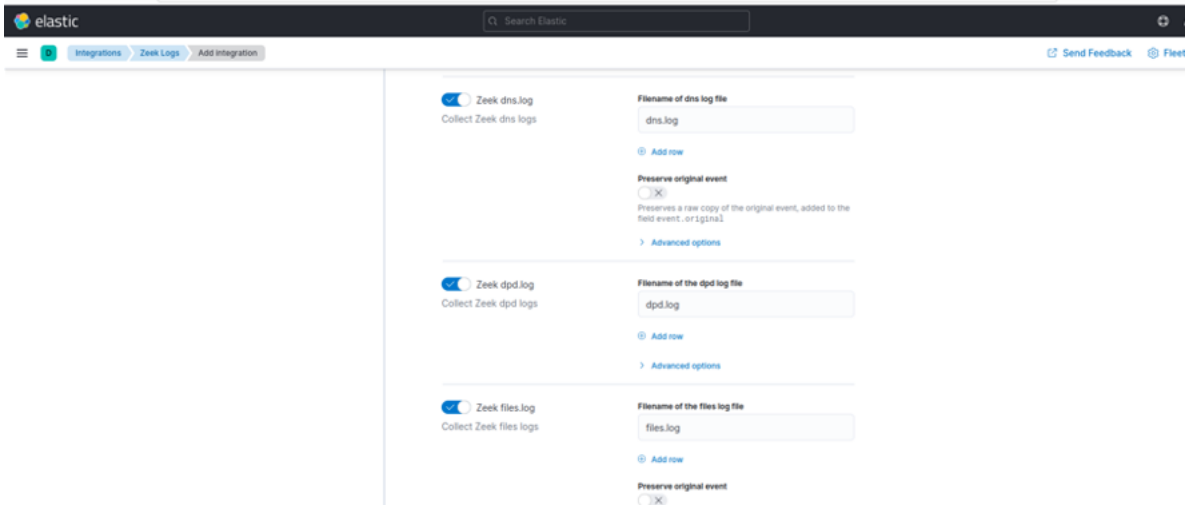
Give the path where zeek logs stored

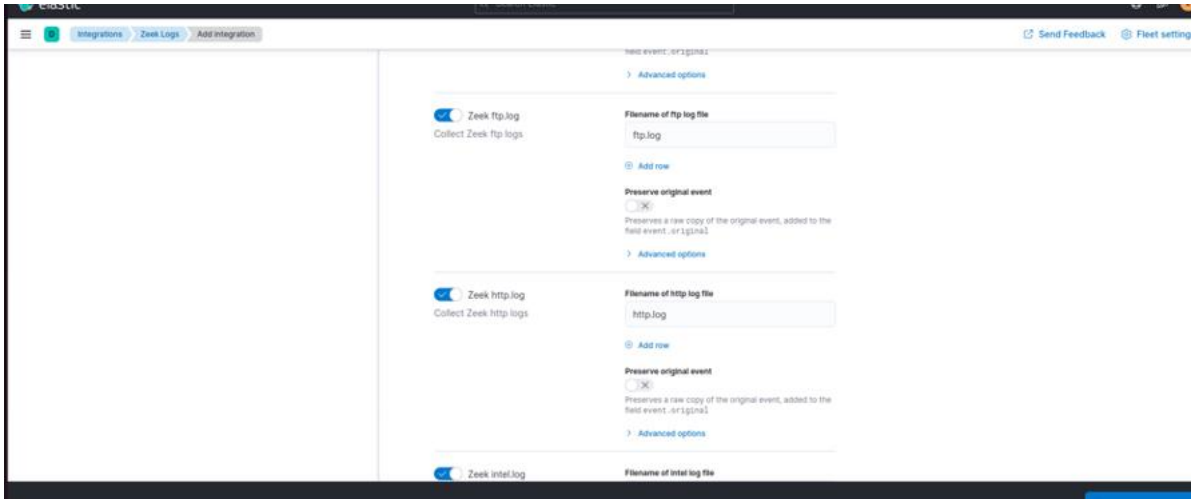


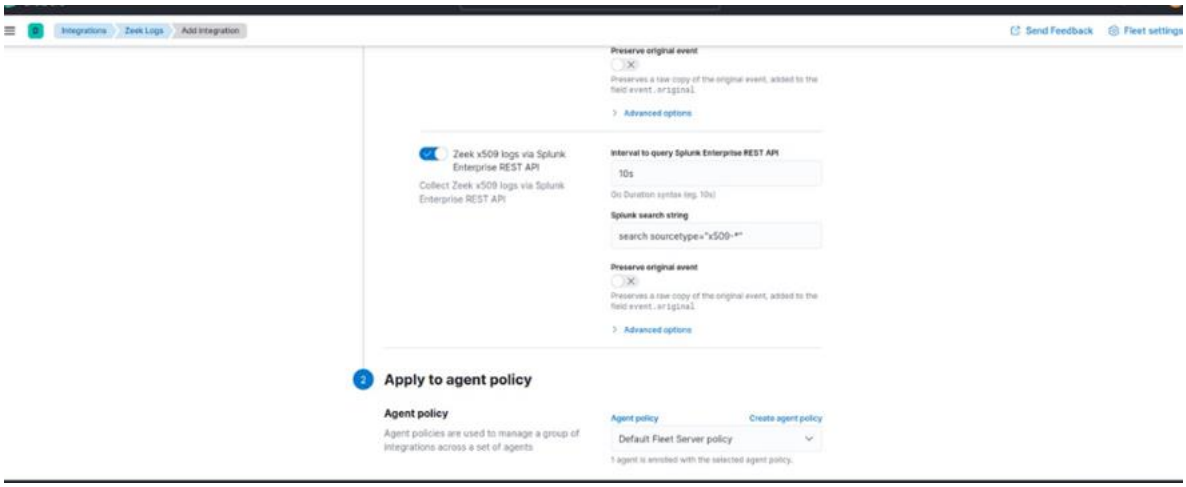

```
separator \x09
set_separator   ,
empty_field     (empty)
unset_field     -
path    conn
open    2023-08-15-20-00-01
fields ts       uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duration        orig_bytes      resp_bytes      conn_state      local_orig      local_resp      missed_bytes    history orig_pkts       orig_ip_bytes   resp_pkts       resp_ip_bytes   tunnel_parents
types   time    string  addr    port    addr    port    enum    string  interval        count   count   string  bool    bool    count   string  count   count   count   count   set[string]
1692109799.569452       CvHrt72jIcRCoeB8Ak      192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109800.594809       COkkuUDxTHkHoWOmd       192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109794.563787       CHUtSK1EkzpBpn1Fj7      192.168.128.129 54915   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109794.563978       CJDkkC1rKeagrxVFYb      192.168.128.129 59382   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109794.564078       Ceovc44fI8WalKHh82      192.168.128.129 58498   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109794.564351       CQhD9Y2nIXeFgW3a        192.168.128.129 48331   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109802.668777       CtUaMs4FYaxaBybKCl      192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109806.783519       CrgE9r3feTHKpbOtHk      192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109814.612171       CSVgSf3OXfkJZFOnt2      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109815.655527       CJBEZz2TpaKDYOZrc7      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.599495       Cpa6id48FuFotKOwD3      192.168.128.129 34987   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.599699       CztbKY1mVWHdx5GGPk      192.168.128.129 33829   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.599948       C7KoAS12Gjkayjy2g4      192.168.128.129 34753   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.600290       Cu0ozr1GfhagdQyGxl      192.168.128.129 42859   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.600497       CwR6ru47hLZ3mX9Hhf      192.168.128.129 38296   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109809.600932       CA24qL36IrVBeVqsud      192.168.128.129 41801   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109810.490462       CgsKfm43Ps7t8yTzD5      192.168.128.129 53672   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109817.717070       CQAfJM39salgh8UEEf      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109821.817420       CB9OKI26MYoPLLDy27      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109829.632272       CdD18z4OA35tjyrDzl      192.168.128.129 40510   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109830.639696       ClN3lX1ahoIZPeG053      192.168.128.129 40510   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.617310       CvXOuSZuVyRseU6tog      192.168.128.129 43988   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.617713       C02c9xuVWhCzEKsU1       192.168.128.129 59767   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.618129       CNul7TCyla58mJPsg       192.168.128.129 44948   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.618473       CUK8s32qk0IkIrcFcl      192.168.128.129 36646   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.619017       CnapGt3AKcWAD6r38b      192.168.128.129 38310   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.619235       CYzfj5Z530amZBHvr       192.168.128.129 53275   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
1692109824.619438       C0enSq3tOBpy7qzYIa      192.168.128.129 51916   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0
```

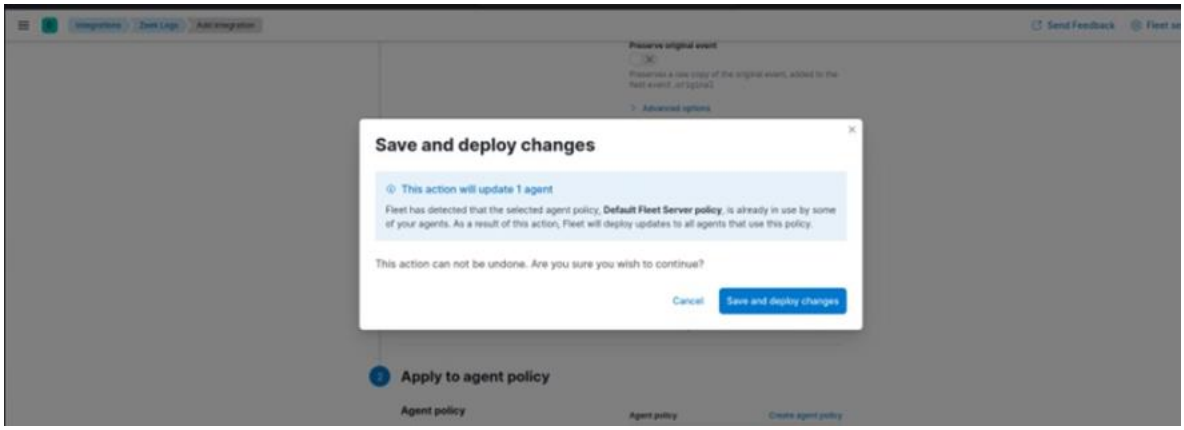

elastic
Search Elastic
Integrations
Zeek Logs
Add integration
Send Feedback
Collect Zeek logs
Settings
The following settings are applicable to all inputs below.
Base Path
/opt/zeek/logs/current
Add row
Base paths to zeek log files (eg. /var/log/bro/current)
Zeek capture_loss.log
Collect Zeek capture_loss logs
Filename of capture loss log file
capture_loss.log
Add row
Preserve original event
Preserves a raw copy of the original event, added to the field event.original
Advanced options
Zeek conn.log
Collect Zeek connection logs
Filename of connection log
conn.log
Add row
Preserve original event


elastic
Search Elastic
Integrations
Zeek Logs
Add integration
Send Feedba
field event.original
Advanced options
Zeek dce_rpc.log
Collect Zeek dce_rpc logs
Filename of dce_rpc log file
dce_rpc.log
Add row
Preserve original event
Preserves a raw copy of the original event, added to the field event.original
Advanced options
Zeek dhcp.log
Collect Zeek dhcp logs
Filename of dhcp log file
dhcp.log
Add row
Advanced options
Zeek dnp3.log
Collect Zeek dnp3 logs
Filename of dnp3 log file
dnp3.log
Add row

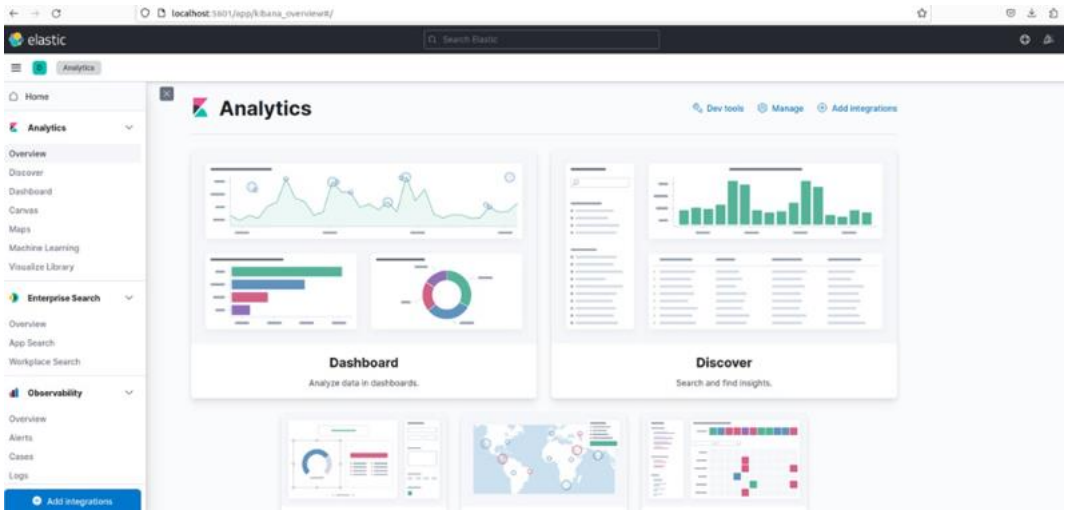

elastic
Search Elastic
Integrations
Zeek Logs
Add integration
Send Feedback
Fleet
Zeek dns.log
Collect Zeek dns logs
Filename of dns log file
dns.log
Add row
Preserve original event
Preserves a raw copy of the original event, added to the field event.original
Advanced options
Zeek dpd.log
Collect Zeek dpd logs
Filename of the dpd log file
dpd.log
Add row
Advanced options
Zeek files.log
Collect Zeek files logs
Filename of the files log file
files.log
Add row
Preserve original event

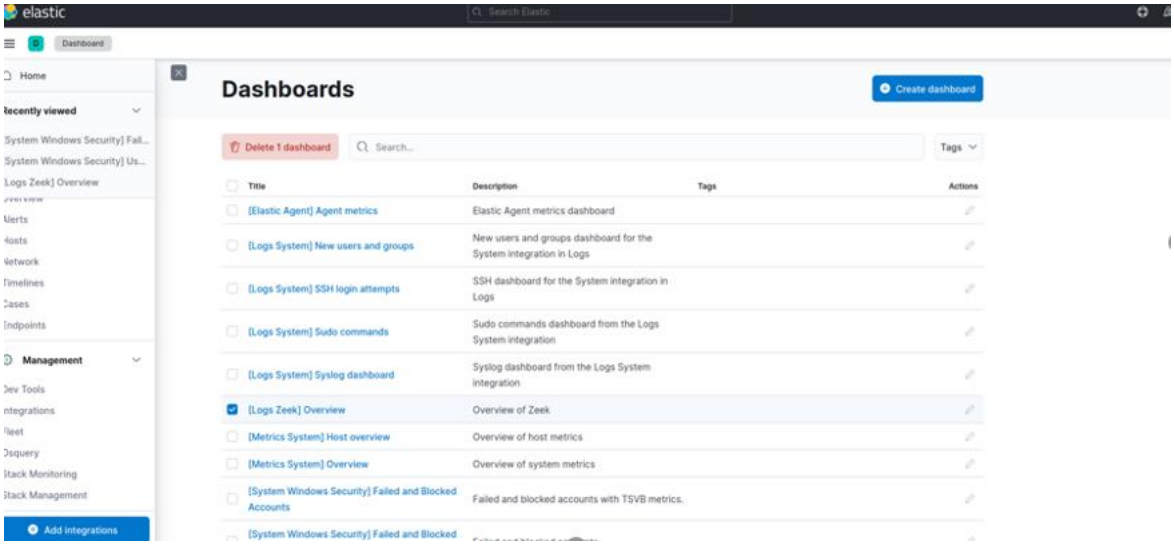

Integrations
Zeek Logs
Add integration
Send Feedback
Fleet setting
Advanced options
Zeek ftp.log
Collect Zeek ftp logs
Filename of ftp log file
ftp.log
Add row
Preserve original event
Preserves a raw copy of the original event, added to the field event.original
Advanced options
Zeek http.log
Collect Zeek http logs
Filename of http log file
http.log
Add row
Preserve original event
Preserves a raw copy of the original event, added to the field event.original
Advanced options
Zeek intel.log
Filename of intel log file

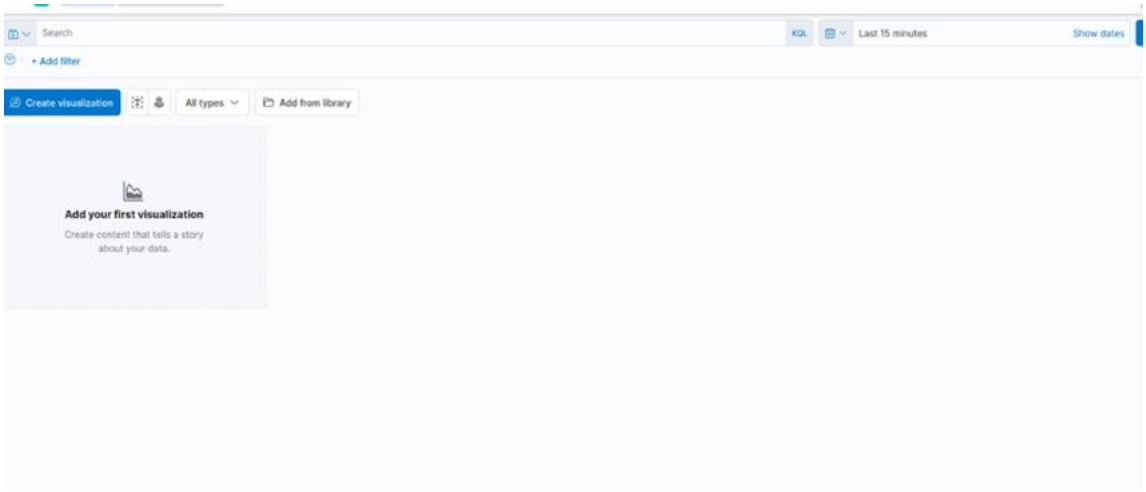

Integrations
Zeek Logs
Add integration
Send Feedback
Fleet settings
Preserve original event
Preserves a raw copy of the original event, added to the field event.original
Advanced options
Zeek x509 logs via Splunk Enterprise REST API
Collect Zeek x509 logs via Splunk Enterprise REST API
Interval to query Splunk Enterprise REST API
10s
Splunk search string
search sourcetype="x509-*"
Preserve original event
Preserves a raw copy of the original event, added to the field event.original
Advanced options
2
Apply to agent policy
Agent policy
Agent policies are used to manage a group of integrations across a set of agents
Agent policy
Create agent policy
Default Fleet Server policy
1 agent is enrolled with the selected agent policy.


Save and deploy changes
This action will update 1 agent
Fleet has detected that the selected agent policy, Default Fleet Server policy, is already in use by some of your agents. As a result of this action, Fleet will deploy updates to all agents that use this policy.
This action can not be undone. Are you sure you wish to continue?
Cancel
Save and deploy changes
2
Apply to agent policy
Agent policy

Go to discover








+ Add filter
Create visualization
All types
Add from library
warn 42.68%
error 49.78%
info 7.54%