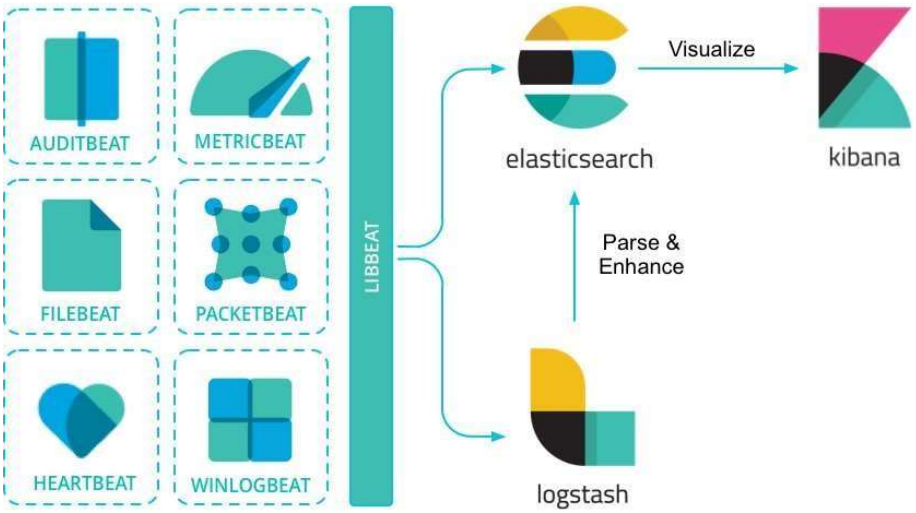
Deploying ELK Stack

Elastic Stack: Elastic Stack (formerly known as ELK Stack) is a free, open-source platform for real-time data analysis and visualisation. It includes a range of tools that can be used for UBA, including Elasticsearch, Logstash, and Kibana.

How ELK Stack?

How ELK Stack Works with Beats?



Install and Configure ELK Stack on Ubuntu

Installation Procedure:

Step 1: Check the OS version by using the below command

```
abhi@abhi:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 20.04.6 LTS
Release:        20.04
Codename:       focal
```

Step 2: Install the dependency Java environment packages by using the below command apt install default-jdk default-jre -y

```
abhi@abhi:~$ sudo apt install default-jdk default-jre -y
[sudo] password for abhi:
Reading package lists... Done
Building dependency tree
Reading state information... Done
default-jdk is already the newest version (2:1.11-72).
default-jre is already the newest version (2:1.11-72).
The following packages were automatically installed and are no longer required:
  libfwupdplugin1 libxmlb1 ubuntu-advantage-desktop-daemon
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

Step 3: Check the Installed Java Version by using the below command javac -version

```
abhi@abhi:~$ javac -version
javac 11.0.20
abhi@abhi:~$
```

Step 4: Add the elasticsearch APT repository key by using the below command

(run these commands in root privilege).

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

```
abhi@abhi:~$ sudo su
[sudo] password for abhi:
root@abhi:/home/abhi# curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
OK
root@abhi:/home/abhi#
```

Step 5: Add the Elastic Search to the APT source List by using the below command echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/ elastic-7.x.list

```
root@abhi:/home/abhi# echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list
root@abhi:/home/abhi#
```

Step 6: Update the APT source list by using the below

command apt update

```
root@abhi:/home/abhi# sudo apt update
Hit:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [632 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2,753 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [2,365 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [864 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [373 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [59.9 kB]
Get:12 http://security.ubuntu.com/ubuntu focal-security/main DEP-11 48x48 Icons [18.9 kB]
Get:13 http://security.ubuntu.com/ubuntu focal-security/main DEP-11 64x64 Icons [36.0 kB]
Get:14 http://security.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [13.0 kB]
Get:15 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [2,070 kB]
Get:16 http://in.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [456 kB]
Get:17 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [275 kB]
Get:18 http://in.archive.ubuntu.com/ubuntu focal-updates/main DEP-11 48x48 Icons [60.8 kB]
Get:19 http://in.archive.ubuntu.com/ubuntu focal-updates/main DEP-11 64x64 Icons [98.3 kB]
Get:20 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [17.0 kB]
Get:21 http://in.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [2,185 kB]
Get:22 http://security.ubuntu.com/ubuntu focal-security/restricted Translation-en [289 kB]
Get:23 http://security.ubuntu.com/ubuntu focal-security/universe i386 Packages [610 kB]
Get:24 http://security.ubuntu.com/ubuntu focal-security/universe amd64 Packages [869 kB]
Get:25 http://in.archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [306 kB]
Get:26 http://security.ubuntu.com/ubuntu focal-security/universe Translation-en [182 kB]
Get:27 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [96.5 kB]
Get:28 http://security.ubuntu.com/ubuntu focal-security/universe DEP-11 48x48 Icons [52.0 kB]
Get:29 http://security.ubuntu.com/ubuntu focal-security/universe DEP-11 64x64 Icons [101 kB]
Get:30 http://security.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [18.9 kB]
Get:31 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 Metadata [940 B]
Get:32 http://in.archive.ubuntu.com/ubuntu focal-updates/universe i386 Packages [744 kB]
Get:33 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [1,101 kB]
Get:34 http://in.archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [263 kB]
Get:35 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [410 kB]
Get:36 http://in.archive.ubuntu.com/ubuntu focal-updates/universe DEP-11 48x48 Icons [280 kB]
Get:37 http://in.archive.ubuntu.com/ubuntu focal-updates/universe DEP-11 64x64 Icons [493 kB]
Get:38 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [25.4 kB]
Get:39 http://in.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata [944 B]
Get:40 http://in.archive.ubuntu.com/ubuntu focal-backports/main amd64 DEP-11 Metadata [7,976 B]
Get:41 http://in.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Metadata [30.5 kB]
Fetched 18.5 MB in 13s (1,465 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
31 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@abhi:/home/abhi#
```

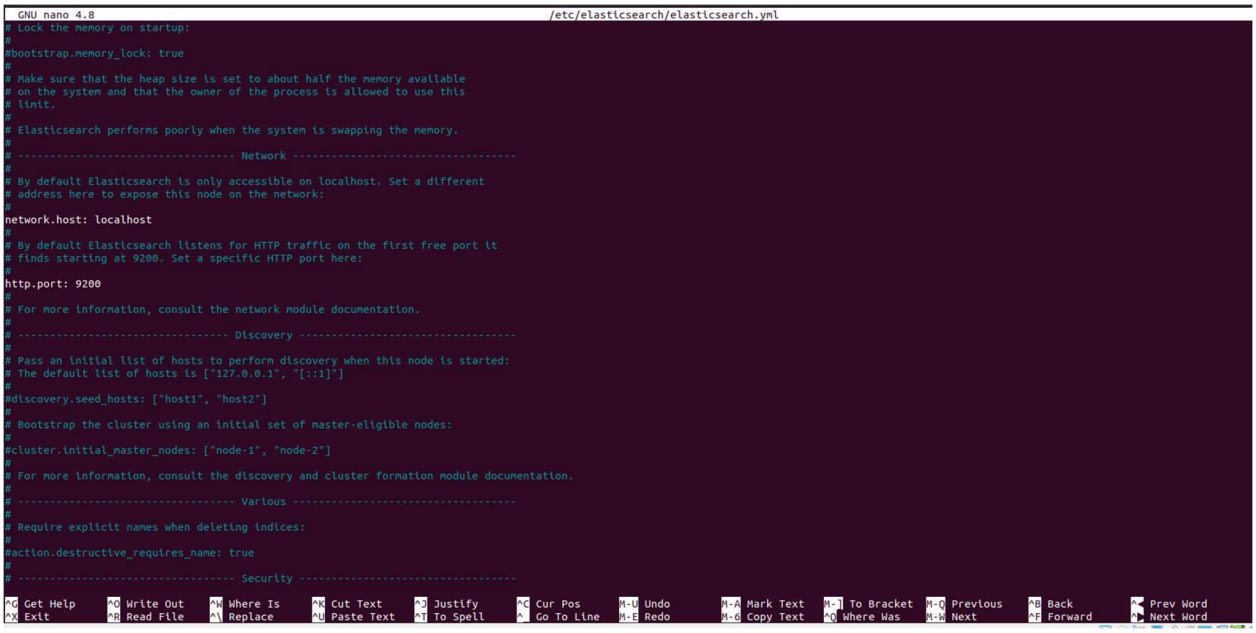
Step 7: Install the Elastic Search by using the below command
apt install elasticsearch -y

```
root@abhi:/home/abhi# sudo apt install elasticsearch -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
elasticsearch is already the newest version (7.17.12).
The following packages were automatically installed and are no longer required:
  libfwupdplugin1 libxmlb1 ubuntu-advantage-desktop-daemon
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 31 not upgraded.
root@abhi:/home/abhi#
```

Step 8: Configure the elastic search by using the below command nano /etc/elasticsearch/elasticsearch.yml

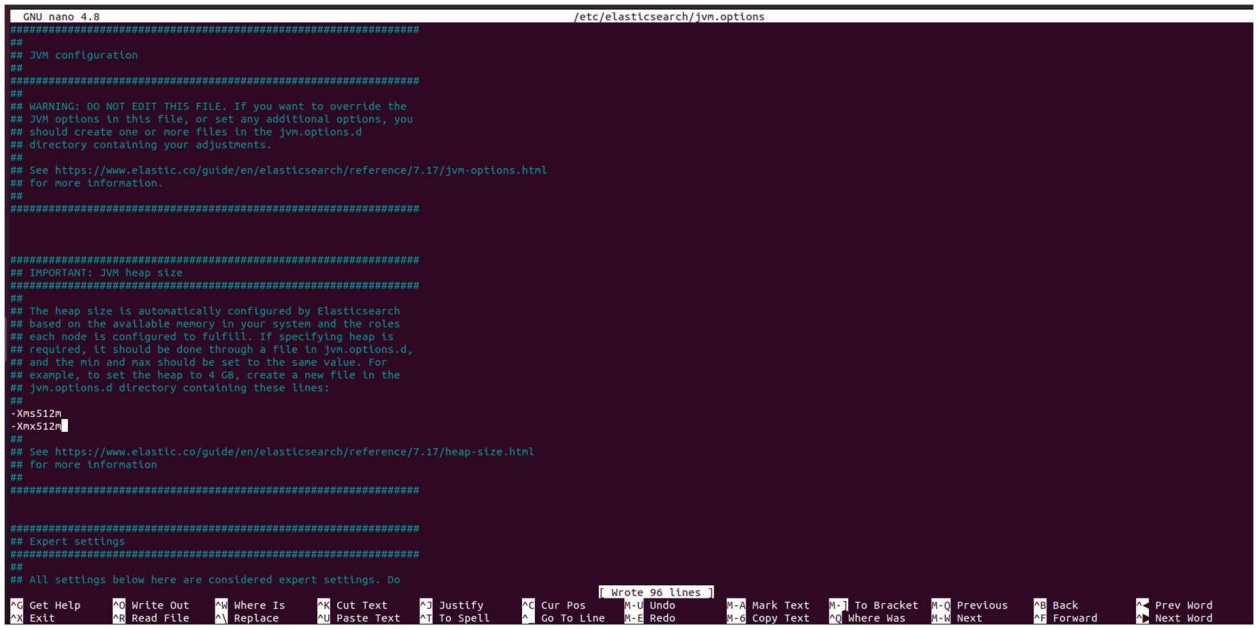
Change the network.host and http.port as per the screenshot

```
abhi@abhi:~$ sudo su
[sudo] password for abhi:
root@abhi:/home/abhi# nano /etc/elasticsearch/elasticsearch.yml
```



Step 9: Configure the JVM heap memory by using the below command nano /etc/elasticsearch/jvm.options

```
root@abhi:/home/abhi# nano /etc/elasticsearch/jvm.options
root@abhi:/home/abhi#
```



Step 10: Restart the Elastic Search by using the below command

systemctl restart elasticsearch

Step 11: Enable the Elastic Search to start on boot by using the below command

```
root@abhi:/home/abhi# systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
root@abhi:/home/abhi#
```

Step 12: Ping the Elastic Search to verify installation by using the below command

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

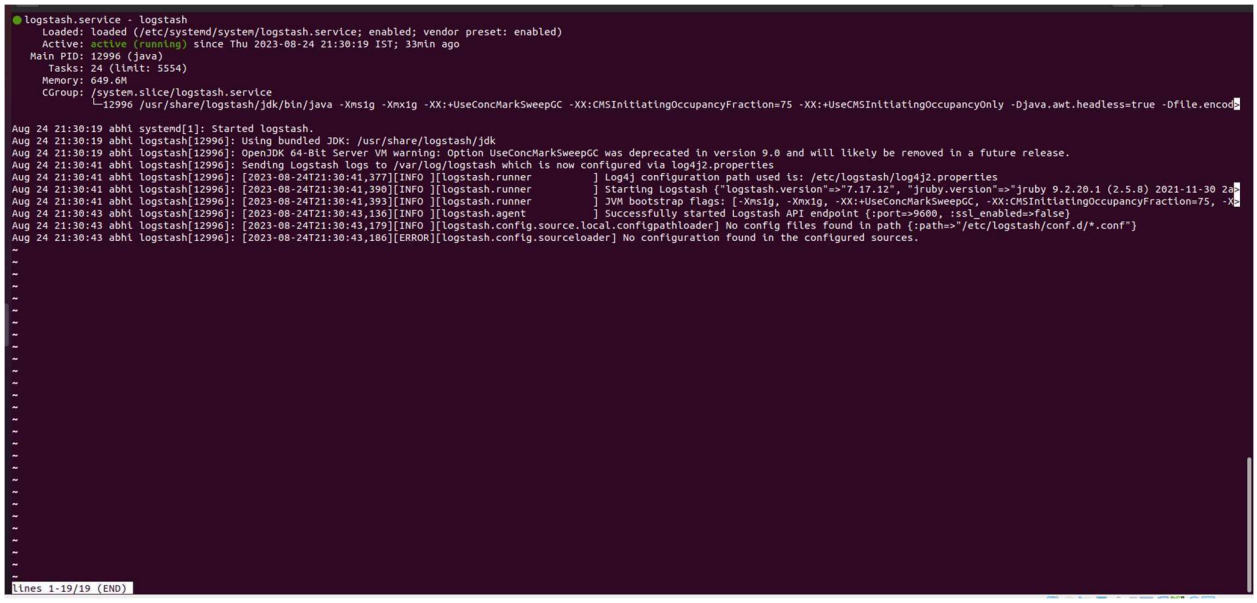
Step 13: Install the Logstash by using the below command

```
root@abhi:root@abhi:/homeroot@abhi:/home/abhi# apt install logstash -y
Reading package lists... Done
Building dependency tree
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:
  libfwupdplugin1 libxmlb1 ubuntu-advantage-desktop-daemon
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 31 not upgraded.
root@abhi:/home/abhi#
```

Step 14: Start the Logstash Service by using the below command # systemctl start logstash

Step 15: Enable the Logstash Service to start on boot by using the below command # systemctl enable logstash

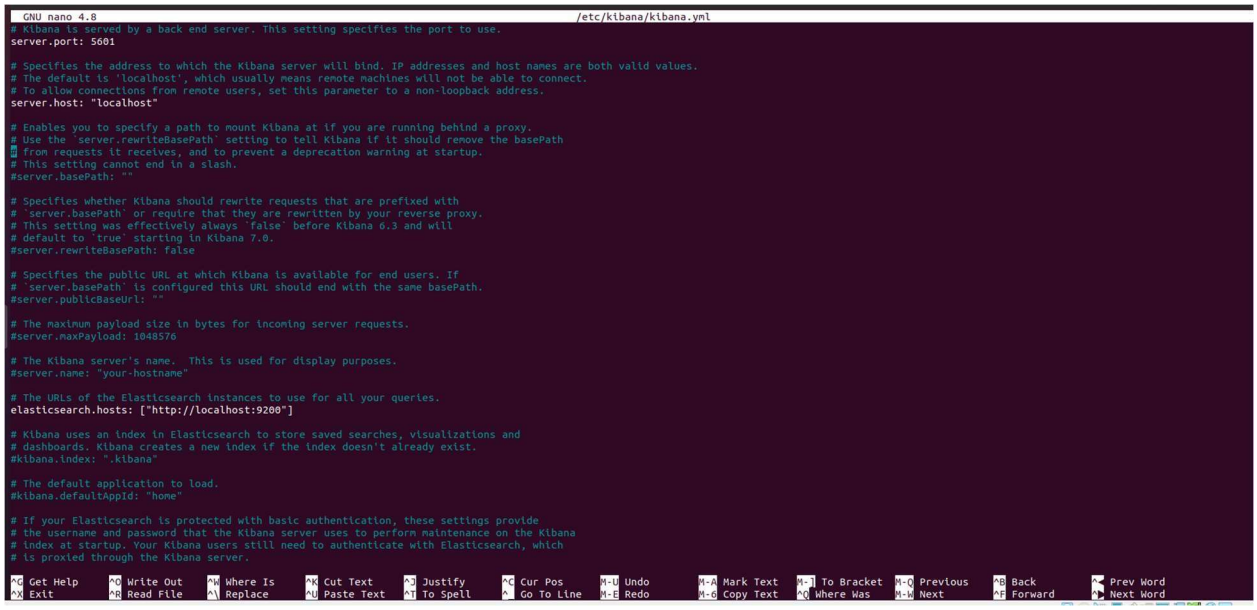
Step 16: Check the status of the Logstash Service by using the below command # systemctl status logstash



Step 17: Install the Kibana by using the below command

```
root@abhi:/home/abhi# apt install kibana -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
kibana is already the newest version (7.17.12).
The following packages were automatically installed and are no longer required:
  libfwupdplugin1 libxmlb1 ubuntu-advantage-desktop-daemon
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 31 not upgraded.
root@abhi:/home/abhi#
```

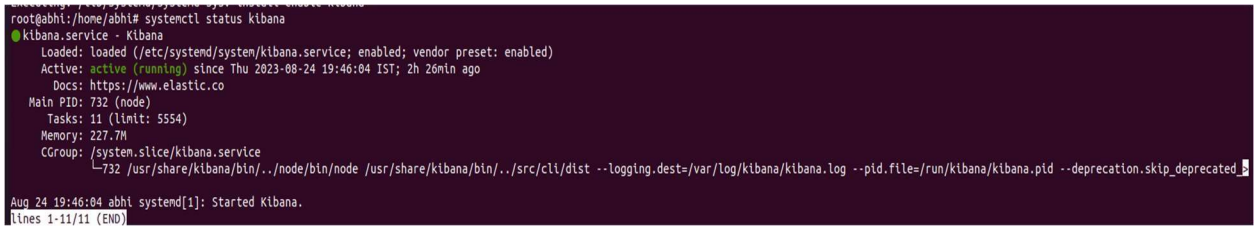
Step 18: Configure kibana in the following file by using the below command # nano/etc/kibana/kibana.yml



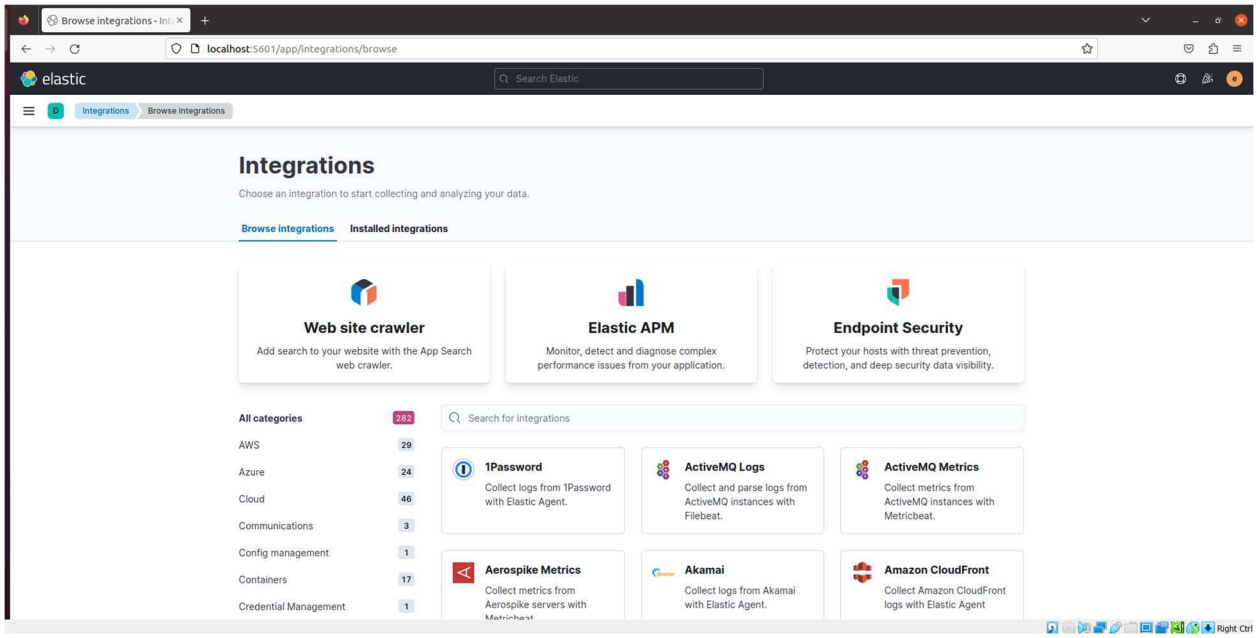
Step 19: Start the kibana Service by using the below command # systemctl start kibana

Step 20: Enable the kibana Service by using the below command # systemctl enable kibana

Step 21: Check the status of the kibana service by using the below command



Step 22: Ping the http://localhost:5601 in browser to view the Dashboard of the kibana as show in the below image



Configuring X-pack Security

Step 1: Stop the kibana by using the below command

sudo systemctl stop kibana

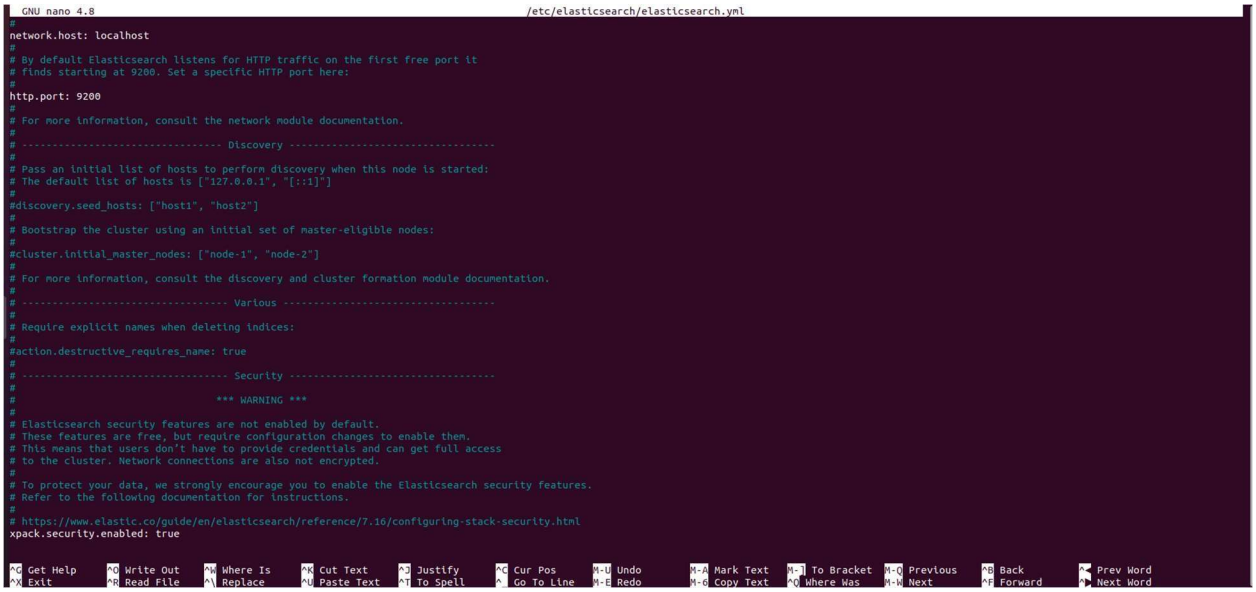
Step 2: Stop the Elastic Search by using the below command

sudo systemctl stop elasticsearch

Step 3: Enable x-pack in Elasticsearch.yml

sudo nano /etc/elasticsearch/elasticsearch.yml

add:xpack.security.enabled: true



Now restart the elasticsearch

sudo systemctl restart elasticsearch

Now start the elasticsearch

sudo systemctl start elasticsearch

Step 4: Setup default user password

cd /usr/share/elasticsearch/bin

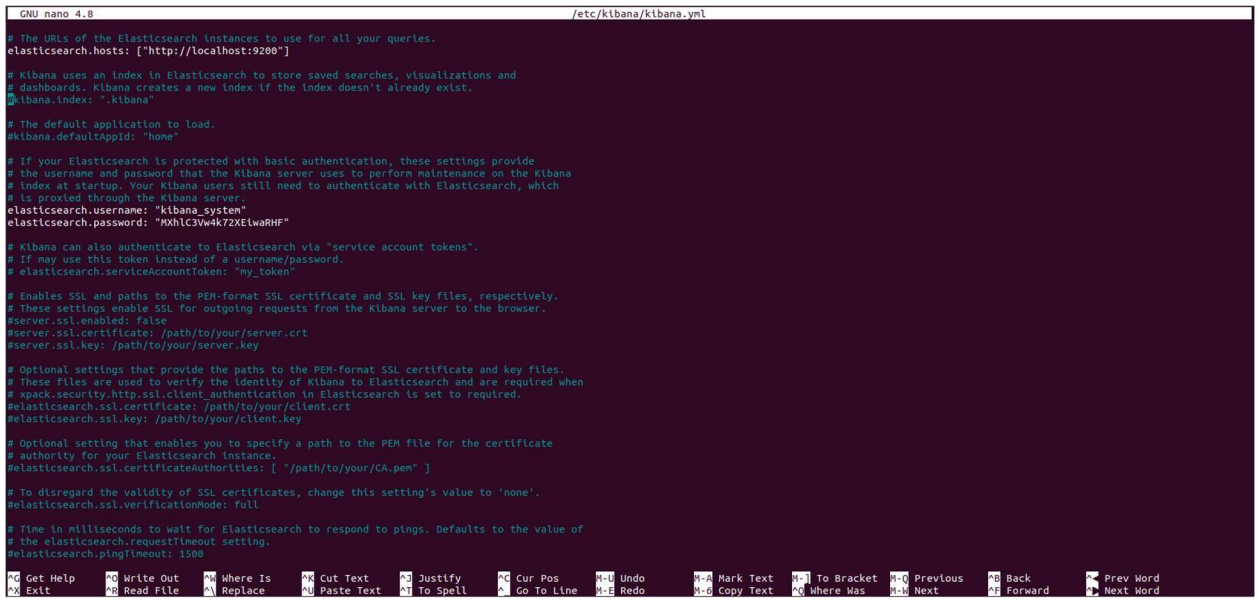
sudo ./elasticsearch-setup-passwords auto

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

Failed to authenticate user 'elastic' against http://127.0.0.1:9200/_security/_authenticate?pretty
Possible causes include:
 * The password for the 'elastic' user has already been changed on this cluster
 * Your elasticsearch node is running against a different keystore
   This tool used the keystore at /etc/elasticsearch/elasticsearch.keystore


ERROR: Failed to verify bootstrap password
root@abhi:/usr/share/elasticsearch/bin#
```

Step 5: Configure Kibana sudo

nano /etc/kibana/kibana.yml

Uncomment elasticsearch username and password



Step 6: Restart the Kibana

sudo systemctl start kibana

```
root@abhi:/usr/share/elasticsearch/bin# sudo nano /etc/kibana/kibana.yml
root@abhi:/usr/share/elasticsearch/bin# sudo systemctl start kibana
root@abhi:/usr/share/elasticsearch/bin# sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2023-08-24 22:54:19 IST; 32s ago
       Docs: https://www.elastic.co
   Main PID: 19224 (node)
      Tasks: 11 (limit: 5554)
     Memory: 417.6M
     CGroup: /system.slice/kibana.service
             └─19224 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --logging.dest=/var/log/kibana/kibana.log --pid.file=/run/kibana/kibana.pid --deprecation.skip_deprecate>

Aug 24 22:54:19 abhi systemd[1]: Started Kibana.
lines 1-11/11 (END)
```

ZEEK installation

Step 1:

```
abhi@abhi:~$ sudo apt-get update
[sudo] password for abhi:
Hit:1 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [274 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata [410 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata [944 B]
Get:8 http://in.archive.ubuntu.com/ubuntu focal-backports/main amd64 DEP-11 Metadata [7,980 B]
Get:9 http://in.archive.ubuntu.com/ubuntu focal-backports/universe amd64 DEP-11 Metadata [30.5 kB]
Get:10 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:11 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metadata [59.9 kB]
Get:12 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-11 Metadata [96.5 kB]
Get:13 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP-11 Metadata [940 B]
Fetched 1,217 kB in 14s (86.6 kB/s)
Reading package lists... Done
```

Step 2:

```
abhi@abhi:~$ 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
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libfwupdplugin1 libxmlb1 ubuntu-advantage-desktop-daemon
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu cmake-data cpp-9 g++-9 gcc-9 gcc-9-base libasan5 libbinutils libc-dev-bin libc6-dev libcrypt-dev libctf-nobfd0 libctf0 libexpat1-dev libfl-dev
  libfl2 libgcc-9-dev libitm1 libjsoncpp1 liblsan0 libpython3-dev libpython3.8-dev libquadmath0 librhash0 libsigsegv2 libstdc++-9-dev libtsan0 libubsan1 linux-libc-dev m4 make manpages-dev
  python3-distutils python3.8-dev swig4.0
Suggested packages:
  binutils-doc bison-doc cmake-doc ninja-build gcc-9-locales build-essential flex-doc g++-multilib g++-9-multilib gcc-9-doc gcc-multilib autoconf automake libtool gcc-doc gcc-9-multilib glibc-doc
  libssl-doc libstdc++-9-doc m4-doc make-doc swig-doc swig-examples swig4.0-examples swig4.0-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bison cmake cmake-data flex g++ g++-9 gcc gcc-9 libasan5 libbinutils libc-dev-bin libc6-dev libcap-dev libcrypt-dev libctf-nobfd0 libctf0
  libexpat1-dev libfl-dev libfl2 libgcc-9-dev libitm1 libjsoncpp1 liblsan0 libpython3-dev libpython3.8-dev libquadmath0 librhash0 libsigsegv2 libssl-dev libstdc++-9-dev libtsan0 libubsan1
  linux-libc-dev m4 make manpages-dev python3-dev python3-distutils python3.8-dev swig swig4.0 zlib1g-dev
The following packages will be upgraded:
  cpp-9 gcc-9-base
2 upgraded, 45 newly installed, 0 to remove and 29 not upgraded.
Need to get 57.7 MB of archives.
```

Step 3:

```
abhi@abhi:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
```

Step 4:

```
abhi@abhi:~$ cd Downloads
abhi@abhi:~/Downloads$ ls
 ELK_Stack.pdf   zeek-6.0.0   zeek-6.0.0.tar.gz  'ZEEK Installation.docx'
abhi@abhi:~/Downloads$ cd zeek-6.0.0/
```

Step 5:

```
abhi@abhi:~/Downloads/zeek-6.0.0$ sudo apt-get install cmake make gcc g++ flex bison libpcap-dev libssl-dev python3-dev swig zlib1g-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
bison is already the newest version (2:3.5.1+dfsg-1).
flex is already the newest version (2.6.4-6.2).
g++ is already the newest version (4:9.3.0-1ubuntu2).
gcc is already the newest version (4:9.3.0-1ubuntu2).
make is already the newest version (4.2.1-1.2).
make set to manually installed.
python3-dev is already the newest version (3.8.2-0ubuntu2).
swig is already the newest version (4.0.1-5build1).
cmake is already the newest version (3.16.3-1ubuntu1.20.04.1).
libssl-dev is already the newest version (1.1.1f-1ubuntu2.19).
zlib1g-dev is already the newest version (1:1.2.11.dfsg-2ubuntu1.5).
The following packages were automatically installed and are no longer required:
  libfwupdplugin1 libxmlb1 ubuntu-advantage-desktop-daemon
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libpcap0.8-dev
The following NEW packages will be installed:
  libpcap-dev libpcap0.8-dev
0 upgraded, 2 newly installed, 0 to remove and 29 not upgraded.
Need to get 248 kB of archives.
After this operation, 852 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libpcap0.8-dev amd64 1.9.1-3 [244 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libpcap-dev amd64 1.9.1-3 [3,484 B]
Fetched 248 kB in 2s (107 kB/s)
Selecting previously unselected package libpcap0.8-dev:amd64.
(Reading database ... 256685 files and directories currently installed.)
Preparing to unpack .../libpcap0.8-dev_1.9.1-3_amd64.deb ...
Unpacking libpcap0.8-dev:amd64 (1.9.1-3) ...
Selecting previously unselected package libpcap-dev:amd64.
Preparing to unpack .../libpcap-dev_1.9.1-3_amd64.deb ...
Unpacking libpcap-dev:amd64 (1.9.1-3) ...
Setting up libpcap0.8-dev:amd64 (1.9.1-3) ...
Setting up libpcap-dev:amd64 (1.9.1-3) ...
Processing triggers for man-db (2.9.1-1) ...
```

Step 6:

```
abhi@abhi:~/Downloads/zeek-6.0.0$ ./configure
Build Directory : build
Source Directory: /home/abhi/Downloads/zeek-6.0.0
Using cmake version 3.16.3

-- The C compiler identification is GNU 9.4.0
-- The CXX compiler identification is GNU 9.4.0
-- Check for working C compiler: /usr/bin/cc
-- Check for working C compiler: /usr/bin/cc -- works
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Detecting C compile features
-- Detecting C compile features - done
-- Check for working CXX compiler: /usr/bin/c++
-- Check for working CXX compiler: /usr/bin/c++ -- works
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- 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
-- Performing Test test_arch_power - Failed
-- Determined target architecture (for hashing): x86_64
-- Found sed: /usr/bin/sed
-- Found PythonInterp: /usr/bin/python3 (found version "3.8.10")
-- Found FLEX: /usr/bin/flex (found version "2.6.4")
-- Found BISON: /usr/bin/bison
-- Found PCAP: /usr/lib/x86_64-linux-gnu/libpcap.so
-- Performing Test PCAP_LINKS_SOLO
-- Performing Test PCAP_LINKS_SOLO - Success
-- Looking for pcap_get_pfring_id
-- Looking for pcap_get_pfring_id - not found
-- Looking for pcap_dump_open_append
-- Looking for pcap_dump_open_append - found
-- Found OpenSSL: /usr/lib/x86_64-linux-gnu/libcrypto.so (found version "1.1.1f")
-- Performing Test ns_initparse_works_none
-- Performing Test ns_initparse_works_none - Failed
-- Performing Test res_mkquery_works_none
-- Performing Test res_mkquery_works_none - Failed
-- Performing Test ns_initparse_works_libresolv.a
-- Performing Test ns_initparse_works_libresolv.a - Success
-- Performing Test res_mkquery_works_libresolv.a
-- Performing Test res_mkquery_works_libresolv.a - Success
```

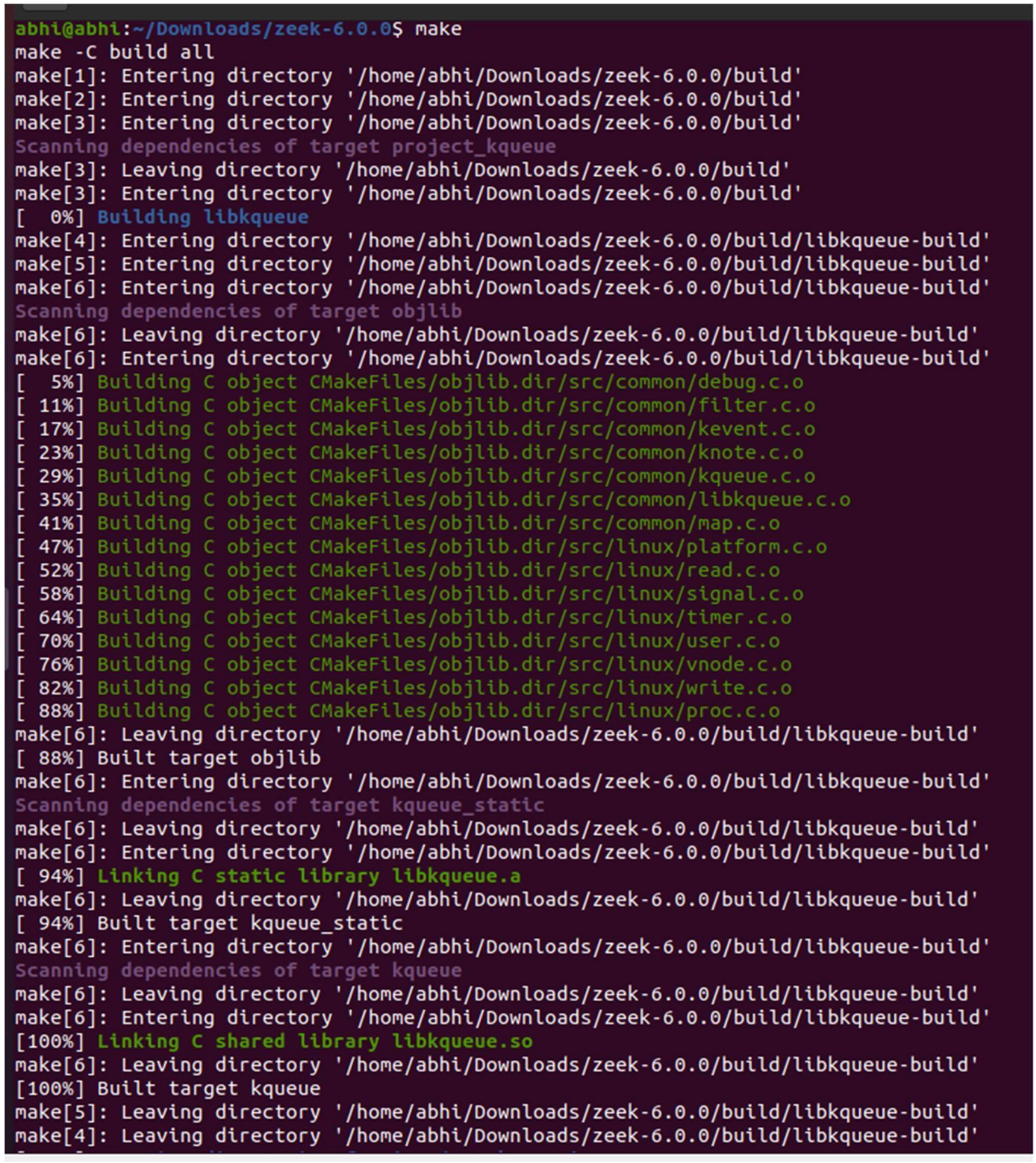
```
==================|  BinPAC Build Summary  |====================
Version:           0.61.0
SO version:        0

Build Type:        RelWithDebInfo
Debug mode:        OFF
Install prefix:    /usr/local/zeek
Shared libs:       yes
Static libs:       no

CC:                /usr/bin/cc
CFLAGS:             -Wall -Wno-unused -O2 -g -DNDEBUG
CXX:               /usr/bin/c++
CXXFLAGS:           -Wall -Wno-unused -Wno-register -Werror=vla -O2 -g -DNDEBUG
CPP:               /usr/bin/c++

================================================================

-- Found BinPAC: binpac

====================|  Bifcl Build Summary  |=====================

Build type:        RelWithDebInfo
Build dir:         /home/abhi/Downloads/zeek-6.0.0/build/auxil/bifcl
Install prefix:    /usr/local/zeek
Debug mode:        OFF

CC:                /usr/bin/cc
CFLAGS:             -Wall -Wno-unused -O2 -g -DNDEBUG
CXX:               /usr/bin/c++
CXXFLAGS:           -Wall -Wno-unused -Wno-register -Werror=vla -std=c++17 -O2 -g -DNDEBUG
CPP:               /usr/bin/c++

================================================================


====================|  Gen-ZAM Build Summary  |===================


Build type:        RelWithDebInfo
Build dir:         /home/abhi/Downloads/zeek-6.0.0/build/auxil/gen-zam
Install prefix:    /usr/local/zeek
Debug mode:        OFF

CC:                /usr/bin/cc
CFLAGS:             -Wall -Wno-unused -O2 -g -DNDEBUG
CXX:               /usr/bin/c++
```

```
==================|  Broker Config Summary  |====================
Version:         2.6.0
SO version:      4

Build Type:      RelWithDebInfo
Install prefix:  /usr/local/zeek
Library prefix:  lib
Shared libs:     yes
Static libs:     no

CC:              /usr/bin/cc
CFLAGS:           -Wall -Wno-unused -O2 -g -DNDEBUG
CXX:             /usr/bin/c++
CXXFLAGS:         -Wall -Wno-unused -Wno-register -Werror=vla  -Wall -Wno-unused -pedantic -ftemplate-depth=512 -ftemplate-backtrace-limit=0 -std=c++17 -O2 -g -DNDEBUG

CAF:             0.18.5
Python bindings: yes
Zeek:            /home/abhi/Downloads/zeek-6.0.0/build/zeek-path-dev.sh
================================================================

-- The ASM compiler identification is GNU
-- Found assembler: /usr/bin/cc
-- Found Python3: /usr/bin/python3.8 (found version "3.8.10") found components: Interpreter
-- Found BISON: /usr/bin/bison (found version "3.5.1")
-- Looking for backtrace
-- Looking for backtrace - found
-- backtrace facility detected in default set of libraries
-- Found Backtrace: /usr/include
-- Gold linker usage disabled
-- Check if compiler accepts -pthread
-- Check if compiler accepts -pthread - yes
-- Performing Test have_unused_but_set_variable
-- Performing Test have_unused_but_set_variable - Success
-- Found BISON: /usr/bin/bison
-- comp_id=GNU
-- comp_name=/usr/bin/c++
-- comp_version=9.4.0
-- Performing Test CMU_HAVE_MARCH_NATIVE
-- Performing Test CMU_HAVE_MARCH_NATIVE - Success
-- Performing Test CMU_HAVE_CF_PROTECTION
-- Performing Test CMU_HAVE_CF_PROTECTION - Success
-- Performing Test CMU_HAVE_IPA_PTA
-- Performing Test CMU_HAVE_IPA_PTA - Success
-- Performing Test CMU_HAVE_COVERAGE_FLAG
-- Performing Test CMU_HAVE_COVERAGE_FLAG - Success
-- Performing Test CMU_HAVE_FP_NO_EXCESS_PRECISION
```

```
=================|  ZeekControl Install Summary  |==================

Install prefix:    /usr/local/zeek
Zeek root:         /usr/local/zeek
Scripts Dir:       /usr/local/zeek/share/zeek
Spool Dir:         /usr/local/zeek/spool
Log Dir:           /usr/local/zeek/logs
Config File Dir:   /usr/local/zeek/etc
Python Module Dir: /usr/local/zeek/lib/zeek/python

============================================================


=================|  Zeek-Aux Build Summary  |=================

Install prefix:    /usr/local/zeek
Debug mode:        OFF

CC:                /usr/bin/cc
CFLAGS:             -Wall -Wno-unused -O2 -g -DNDEBUG
CXX:               /usr/bin/c++
CXXFLAGS:           -Wall -Wno-unused -Wno-register -Werror=vla -O2 -g -DNDEBUG
CPP:               /usr/bin/c++

============================================================


===================|  ZeekArchiver Build Summary  |====================

Build type:        RelWithDebInfo
Build dir:         /home/abhi/Downloads/zeek-6.0.0/build
Install prefix:    /usr/local/zeek

CXX:               /usr/bin/c++
CXXFLAGS (base):    -Wall -Wno-unused -Wno-register -Werror=vla -O2 -g -DNDEBUG
CXXFLAGS (extra):  -std=c++17;-Wall;-Wno-unused;-Werror=vla
============================================================


=================|  zeek-client Build Summary  |===============

Install prefix:      /usr/local/zeek
Python module path:  /usr/local/zeek/lib/zeek/python

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

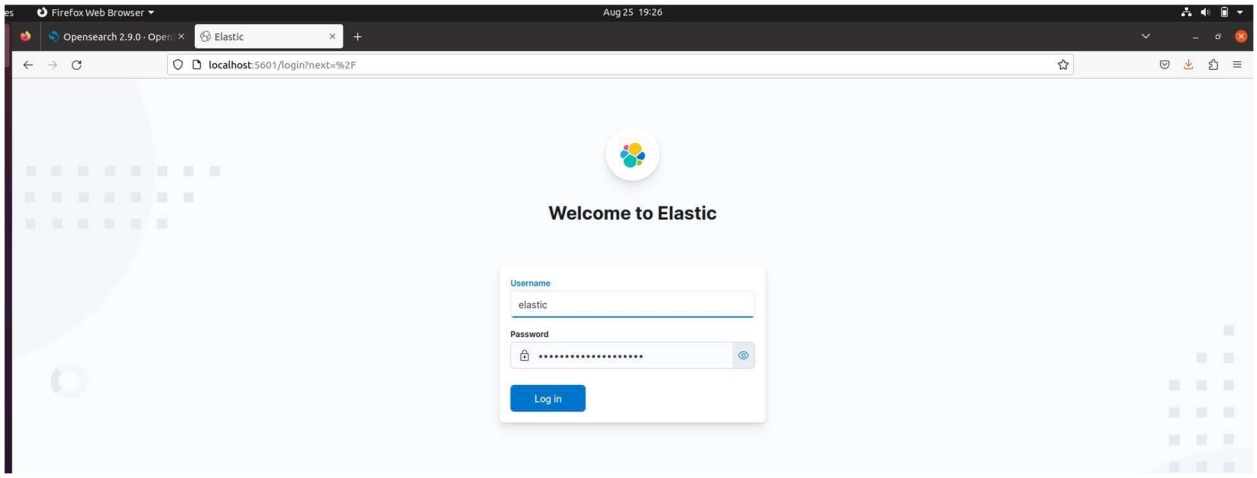
```
====================|  Zeek Build Summary  |====================

Build type:        RelWithDebInfo
Build dir:         /home/abhi/Downloads/zeek-6.0.0/build

Install prefix:    /usr/local/zeek
Config file dir:   /usr/local/zeek/etc
Log dir:           /usr/local/zeek/logs
Plugin dir:        /usr/local/zeek/lib/zeek/plugins
Python module dir: /usr/local/zeek/lib/zeek/python
Script dir:        /usr/local/zeek/share/zeek
Spool dir:         /usr/local/zeek/spool
State dir:         /usr/local/zeek/var/lib
Spicy modules dir: /usr/local/zeek/lib/zeek/spicy

Debug mode:        OFF
Unit tests:        ON
Builtin Plugins:   zeek-af_packet-plugin

CC:                /usr/bin/cc
CFLAGS:             -Wall -Wno-unused -O2 -g -DNDEBUG
CXX:               /usr/bin/c++
CXXFLAGS:           -Wall -Wno-unused -Wno-register -Werror=vla -O2 -g -DNDEBUG
CPP:               /usr/bin/c++

zeek-client:       ON
ZeekControl:       ON
Aux. Tools:        ON
BifCL:             included
BinPAC:            /home/abhi/Downloads/zeek-6.0.0/build/auxil/binpac/src/binpac
BTest:             ON
BTest tooling:     all
Gen-ZAM:           included
zkg:               ON
Spicy:             included
Spicy analyzers:   yes
JavaScript:        no

libmaxminddb:      false
Kerberos:          false
gperftools found:  false
        tcmalloc:  false
       debugging:  false
jemalloc:          OFF

Fuzz Targets:
```

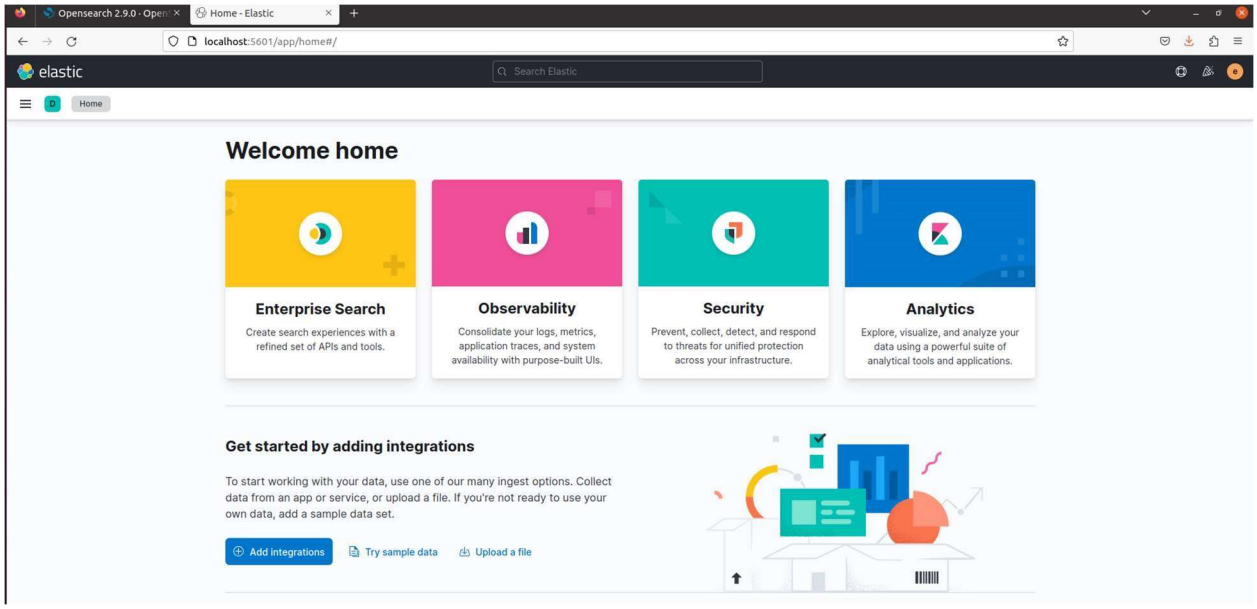
Step 7:


abhi@abhi:~/Downloads/zeek-6.0.0$ make
make -C build all
make[1]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build'
make[2]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build'
make[3]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build'
Scanning dependencies of target project_kqueue
make[3]: Leaving directory '/home/abhi/Downloads/zeek-6.0.0/build'
make[3]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build'
[0%] Building libkqueue
make[4]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
make[5]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
make[6]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
Scanning dependencies of target objlib
make[6]: Leaving directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
make[6]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
[5%] Building C object CMakeFiles/objlib.dir/src/common/debug.c.o
[11%] Building C object CMakeFiles/objlib.dir/src/common/filter.c.o
[17%] Building C object CMakeFiles/objlib.dir/src/common/kevent.c.o
[23%] Building C object CMakeFiles/objlib.dir/src/common/knote.c.o
[29%] Building C object CMakeFiles/objlib.dir/src/common/kqueue.c.o
[35%] Building C object CMakeFiles/objlib.dir/src/common/libkqueue.c.o
[41%] Building C object CMakeFiles/objlib.dir/src/common/map.c.o
[47%] Building C object CMakeFiles/objlib.dir/src/linux/platform.c.o
[52%] Building C object CMakeFiles/objlib.dir/src/linux/read.c.o
[58%] Building C object CMakeFiles/objlib.dir/src/linux/signal.c.o
[64%] Building C object CMakeFiles/objlib.dir/src/linux/timer.c.o
[70%] Building C object CMakeFiles/objlib.dir/src/linux/user.c.o
[76%] Building C object CMakeFiles/objlib.dir/src/linux/vnode.c.o
[82%] Building C object CMakeFiles/objlib.dir/src/linux/write.c.o
[88%] Building C object CMakeFiles/objlib.dir/src/linux/proc.c.o
make[6]: Leaving directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
[88%] Built target objlib
make[6]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
Scanning dependencies of target kqueue_static
make[6]: Leaving directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
make[6]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
[94%] Linking C static library libkqueue.a
make[6]: Leaving directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
[94%] Built target kqueue_static
make[6]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
Scanning dependencies of target kqueue
make[6]: Leaving directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
make[6]: Entering directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
[100%] Linking C shared library libkqueue.so
make[6]: Leaving directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
[100%] Built target kqueue
make[5]: Leaving directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'
make[4]: Leaving directory '/home/abhi/Downloads/zeek-6.0.0/build/libkqueue-build'

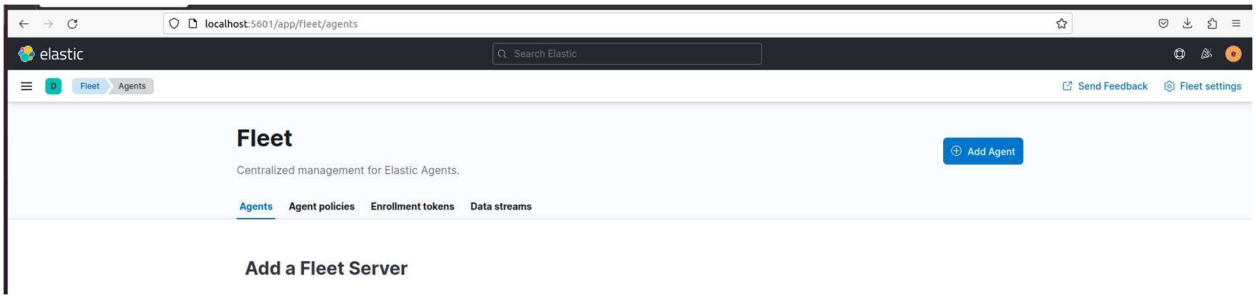
Configuring Fleet

Search for the localhost:5200 in browser

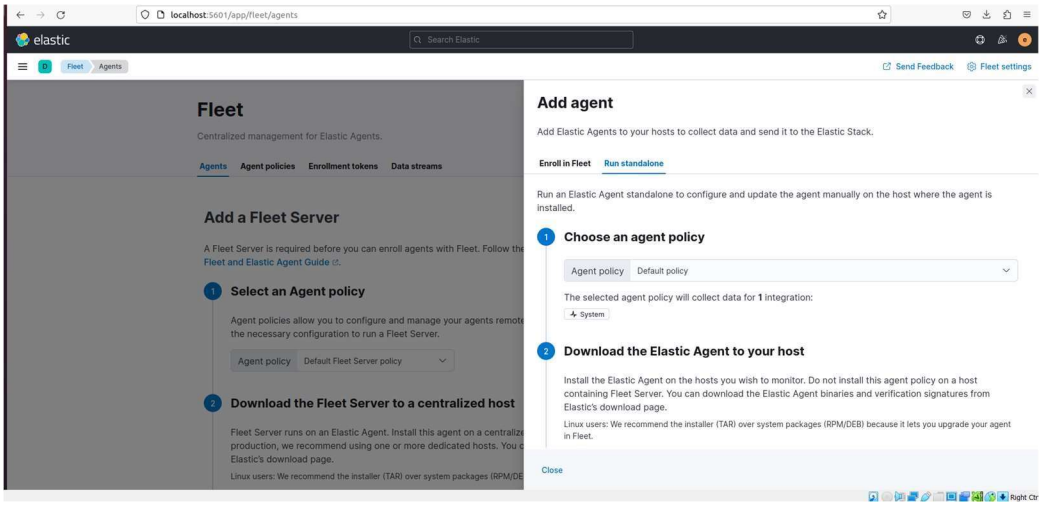




Go to mangement → Fleet

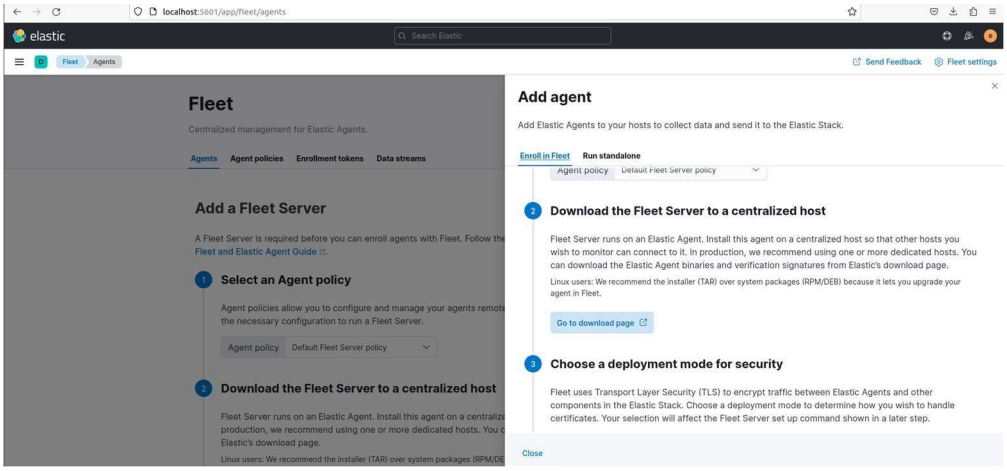


Click on add agent

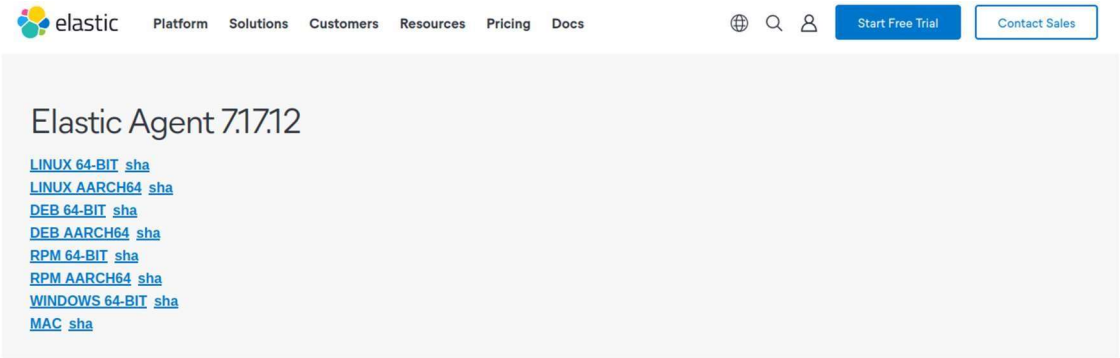


Enroll Fleet section →

Download Fleet Server to centralized host



Click on download page



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 | 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

```
AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2OTI5MDc4NzkyMTU6QlNIT1AtaE9UWUNvQzZLRHYxekR5QQ
```

Fleet sever connected


```
AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2OTI5MDc4NzkyMTU6QlNIT1AtaE9UWUNvQzZLRHYxekR5QQ
```


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

```
sudo ./elastic-agent install   \
  --fleet-server-es=http://localhost:9200 \
  --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2OTI5MDc4NzkyMTU6QlNIT1AtaE9UWUNvQzZLRHYxekR5
QQ \
  --fleet-server-policy=499b5aa7-d214-5b5d-838b-3cd76469844e \
  --fleet-server-insecure-http
```

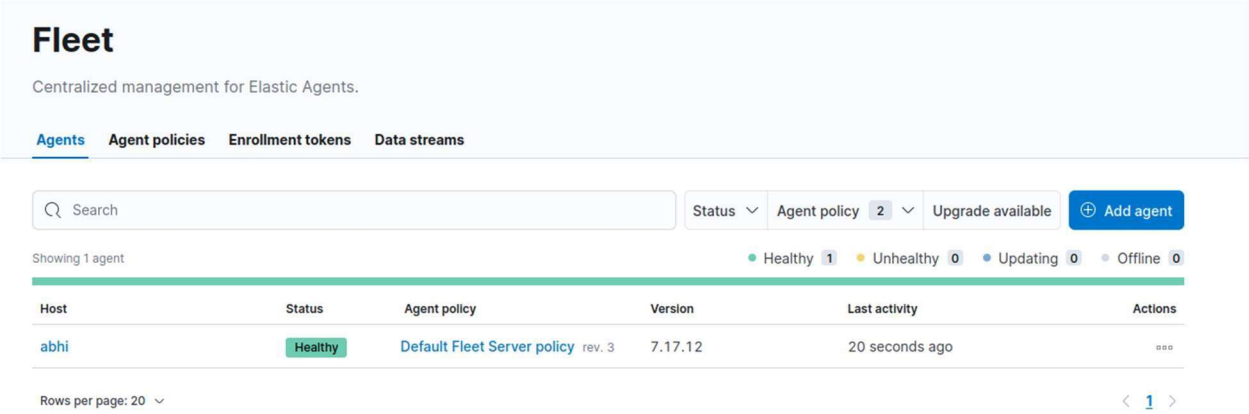
If you are having trouble connecting, see our troubleshooting guide.

Fleet Server connected

You can now enroll agents with Fleet.

Continue

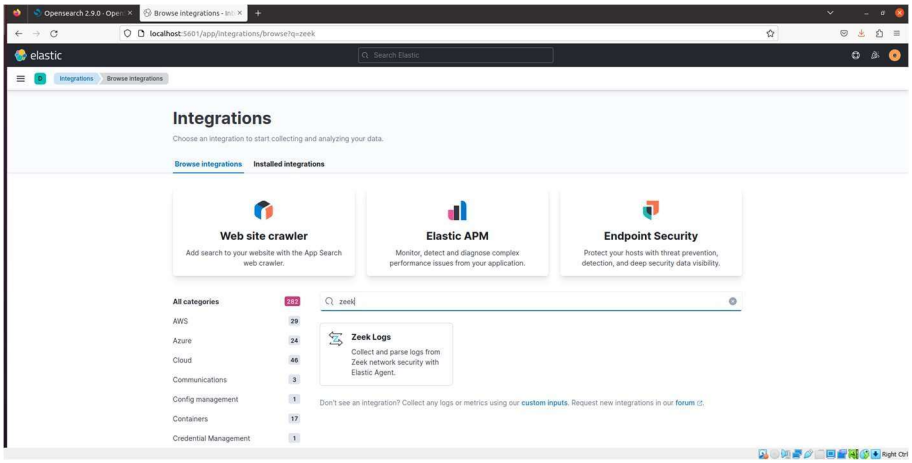
Centralized management for Elastic Agents



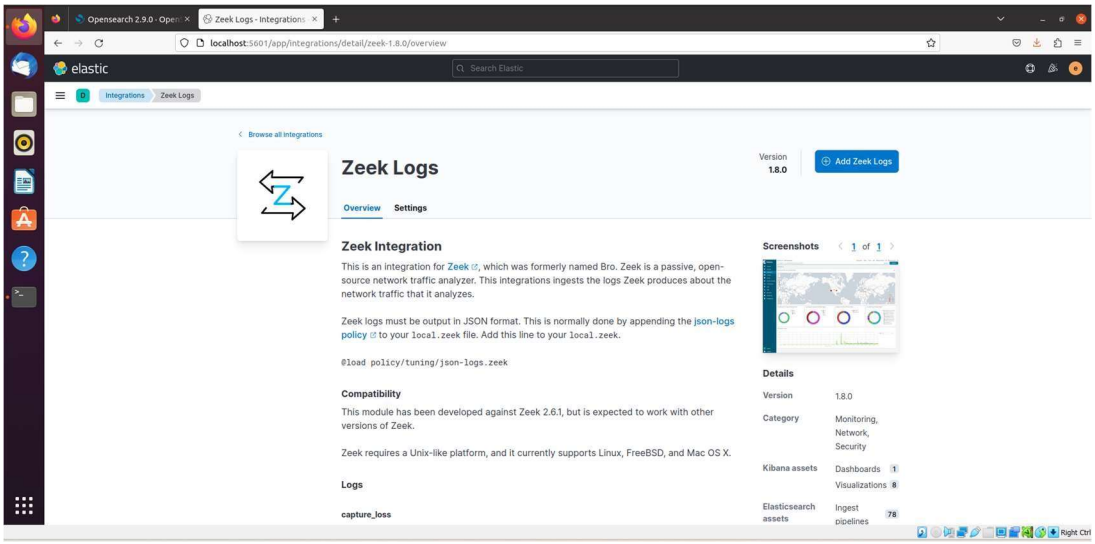
Go to local.zeek and add a line @load policy/tuning/json_logs.zeek

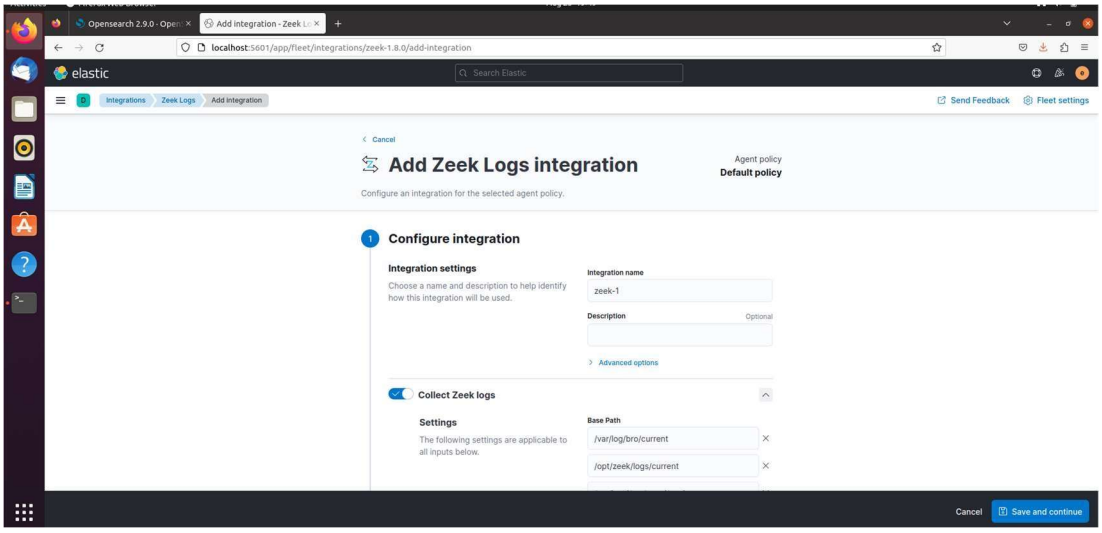
```
abhi@abhi:~$ sudo su
[sudo] password for abhi:
root@abhi:/home/abhi# cd Downloads
root@abhi:/home/abhi/Downloads# ls
 elastic-agent-7.17.12-linux-x86_64          zeek-6.0.0
 elastic-agent-7.17.12-linux-x86_64.tar.gz   zeek-6.0.0.tar.gz
 ELK_Stack.pdf                              'ZEEK Installation.docx'
 opensearch-2.9.0-linux-x64.deb
root@abhi:/home/abhi/Downloads# zeek-6.0.0
zeek-6.0.0: command not found
root@abhi:/home/abhi/Downloads# cd zeek-6.0.0
root@abhi:/home/abhi/Downloads/zeek-6.0.0# ls
auxil             hilti-cxx-include-dirs.in  testing
build             INSTALL                    VERSION
CHANGES           Makefile                   zeek-config.h.in
ci                man                        zeek-config.in
cmake             NEWS                       zeek-config-paths.h.in
CMakeLists.txt    README                     zeek-path-dev.bat.in
configure         README.md                  zeek-path-dev.in
COPYING           repo-info.json             zeek-version.h.in
COPYING-3rdparty  scripts                    zkg-config.in
doc               spicy-path.in
docker            src
root@abhi:/home/abhi/Downloads/zeek-6.0.0# scripts

Command 'scripts' not found, but can be installed with:

apt install gitlab-runner

root@abhi:/home/abhi/Downloads/zeek-6.0.0# cd scripts
root@abhi:/home/abhi/Downloads/zeek-6.0.0/scripts# ls
base  CMakeLists.txt  policy  site  spicy  test-all-policy.zeek  zeekygen
root@abhi:/home/abhi/Downloads/zeek-6.0.0/scripts# cd site
root@abhi:/home/abhi/Downloads/zeek-6.0.0/scripts/site# ls
local.zeek
```

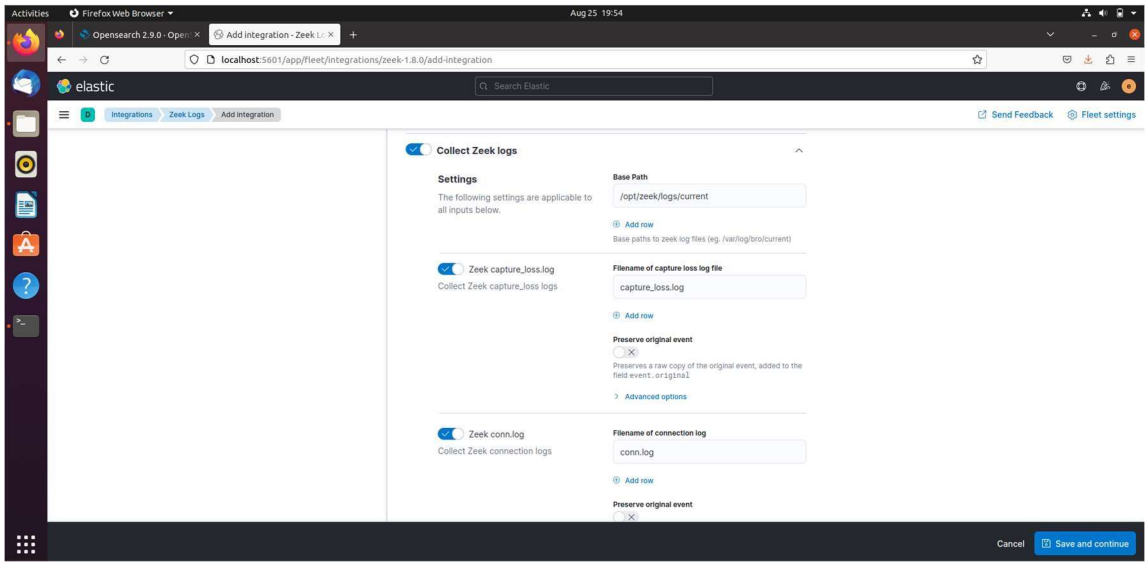
Go to Integrations → search Zeek logs

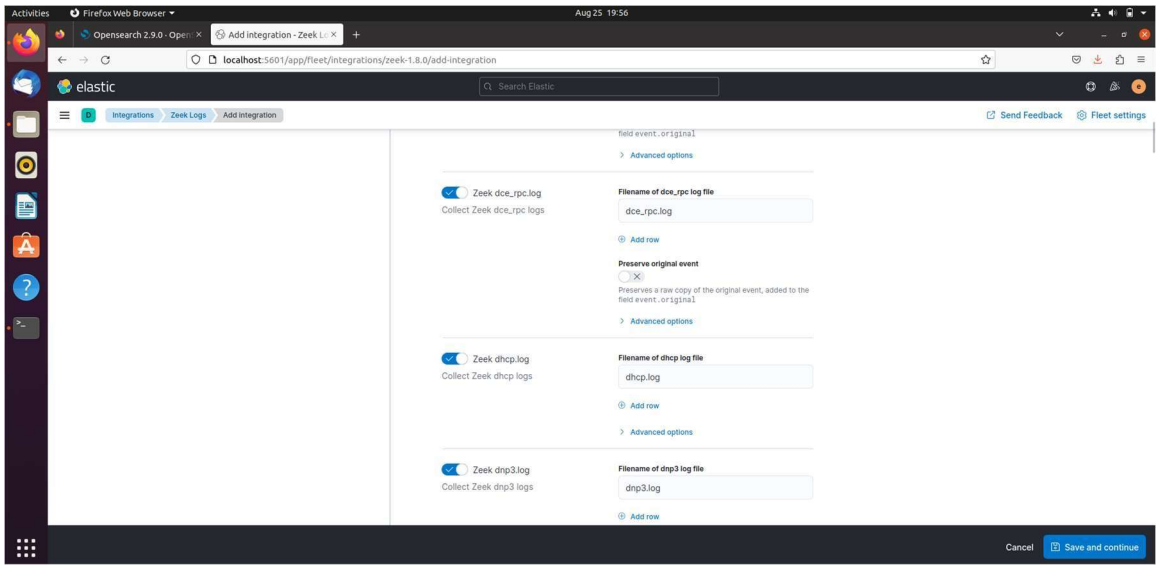


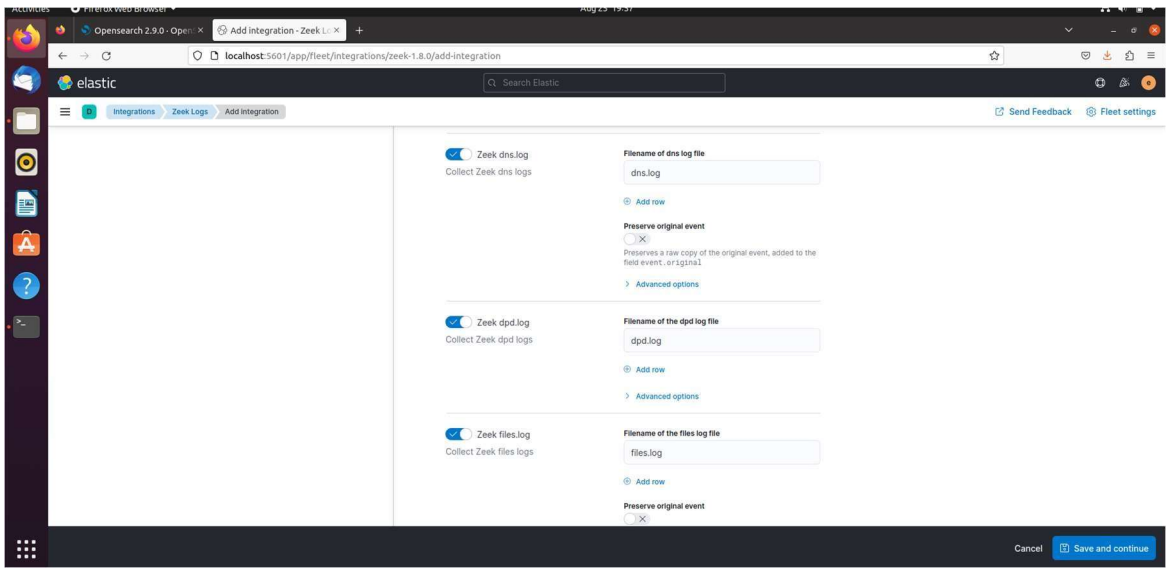
Click on add zeek logs

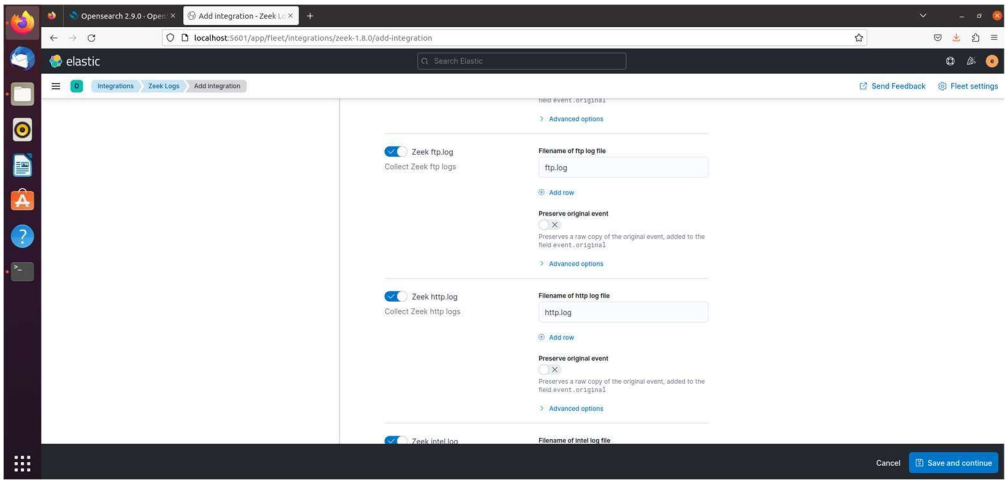





Activities
Firefox Web Browser
Aug 25 19:54
Opensearch 2.9.0 - Open
Add integration - Zeek Lo
localhost:5601/app/fleet/integrations/zeek-1.8.0/add-integration
elastic
Search Elastic
Integrations
Zeek Logs
Add integration
Send Feedback
Fleet settings
Collect Zeek logs
Settings
The following settings are 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
Cancel
Save and continue

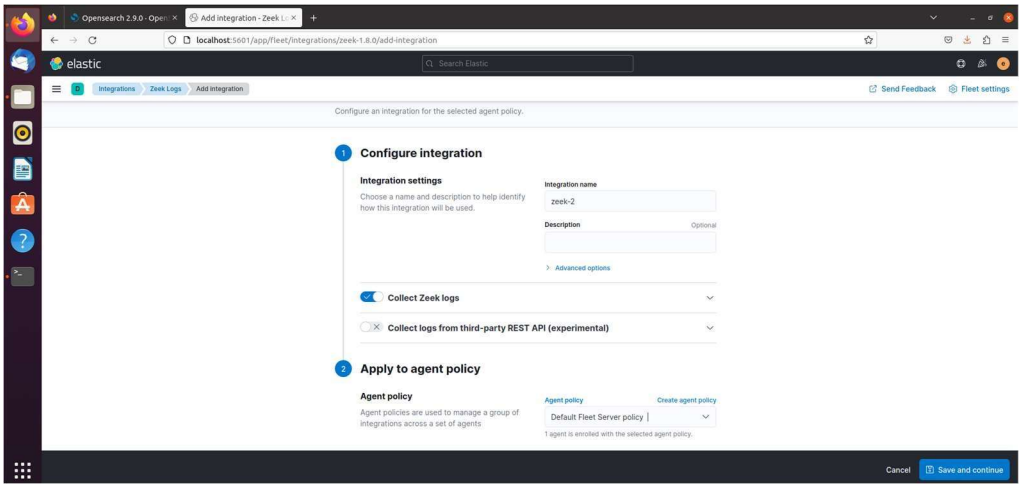

Activities
Firefox Web Browser
Aug 25 19:56
Opensearch 2.9.0 - Open
Add integration - Zeek Lo
localhost:5601/app/fleet/integrations/zeek-1.8.0/add-integration
elastic
Search Elastic
Integrations
Zeek Logs
Add integration
Send Feedback
Fleet settings
field event.original
Advanced options
Zeek dce_rpc.log
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
Cancel
Save and continue


Opensearch 2.9.0 - Open
Add integration - Zeek Lo
localhost:5601/app/fleet/integrations/zeek-1.8.0/add-integration
elastic
Search Elastic
Integrations
Zeek Logs
Add integration
Send Feedback
Fleet settings
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
Cancel
Save and continue

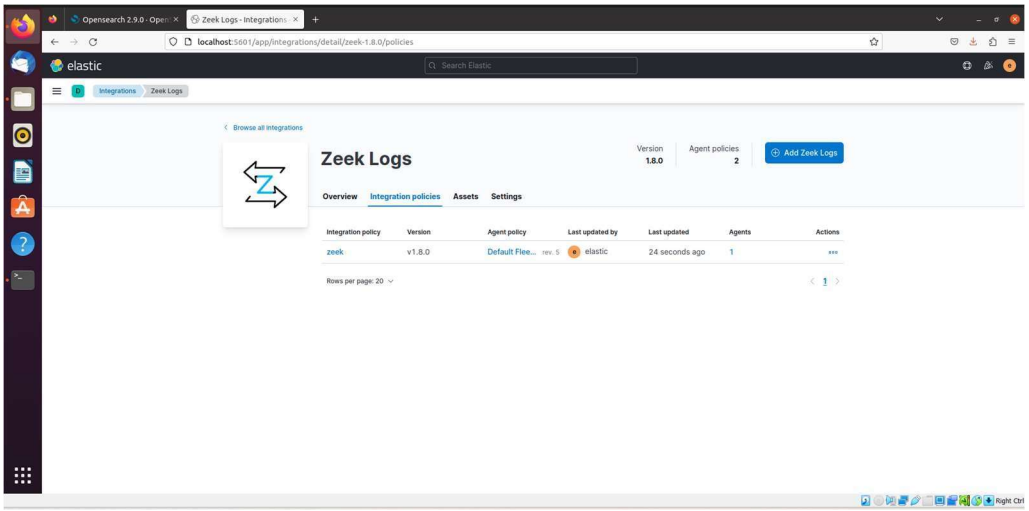


Leave all by default

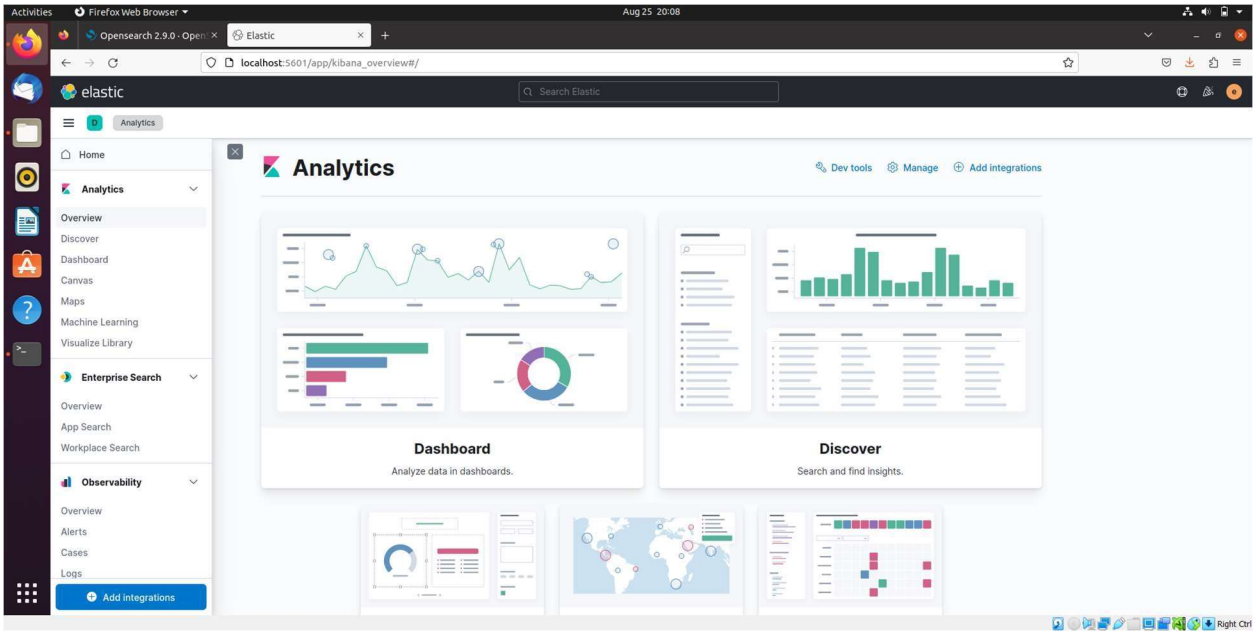
Change Agent policy to Default fleet Server policy



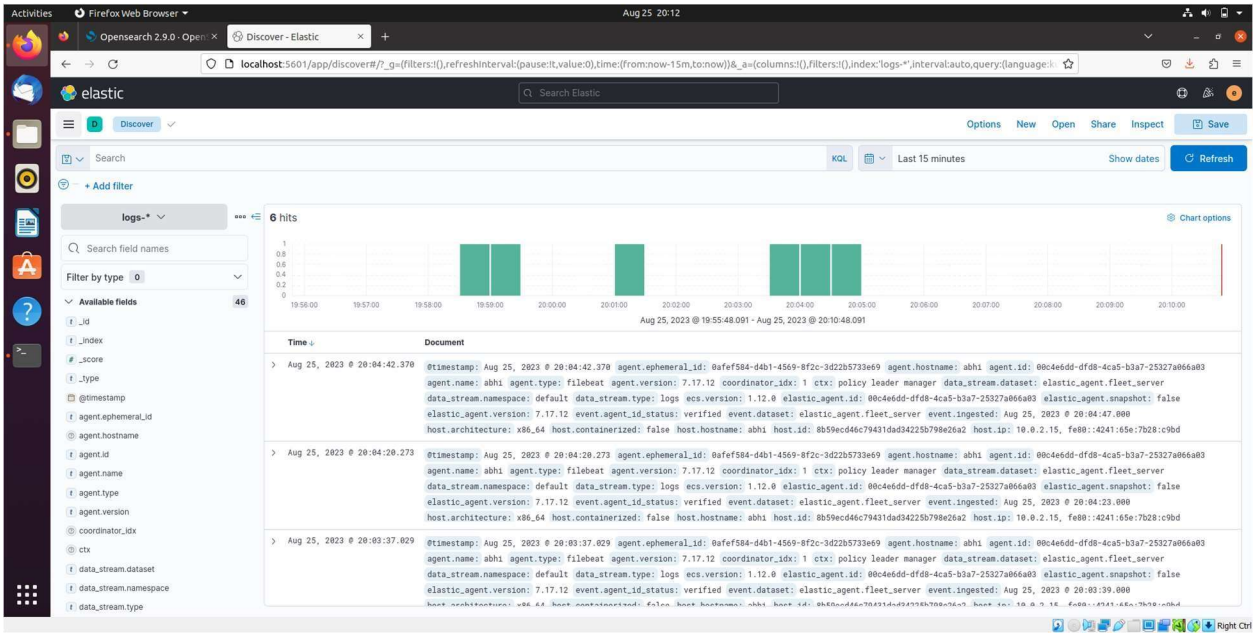
Make sure the 1 agent is enrolled with the selected policy



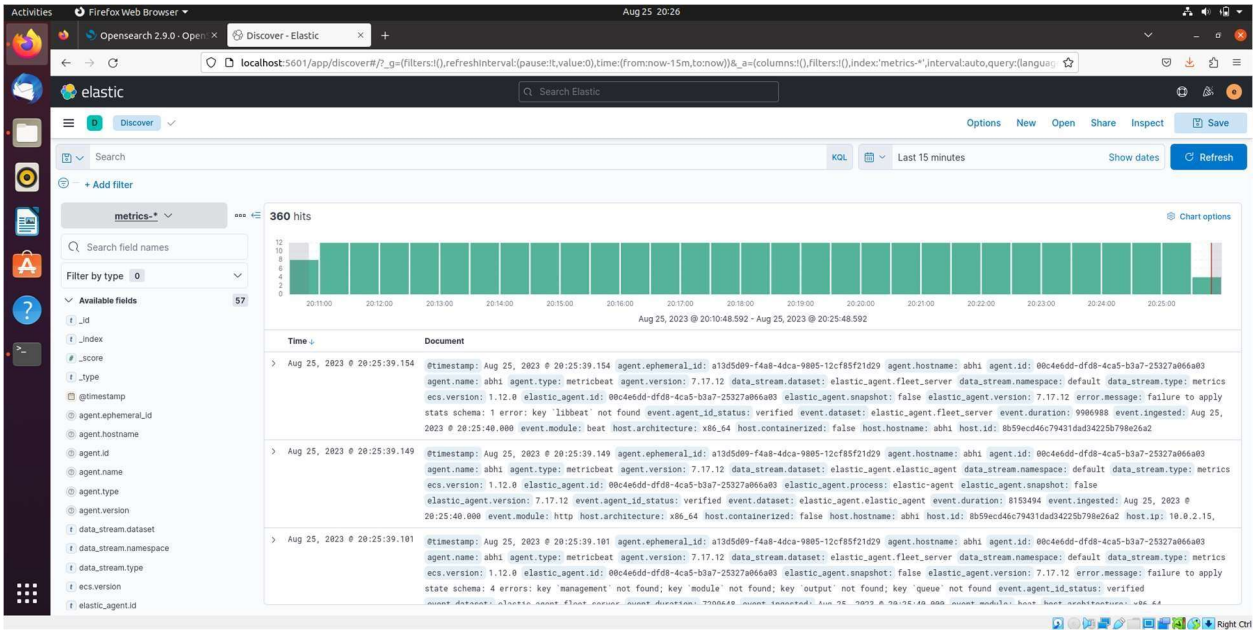
Go to Discover



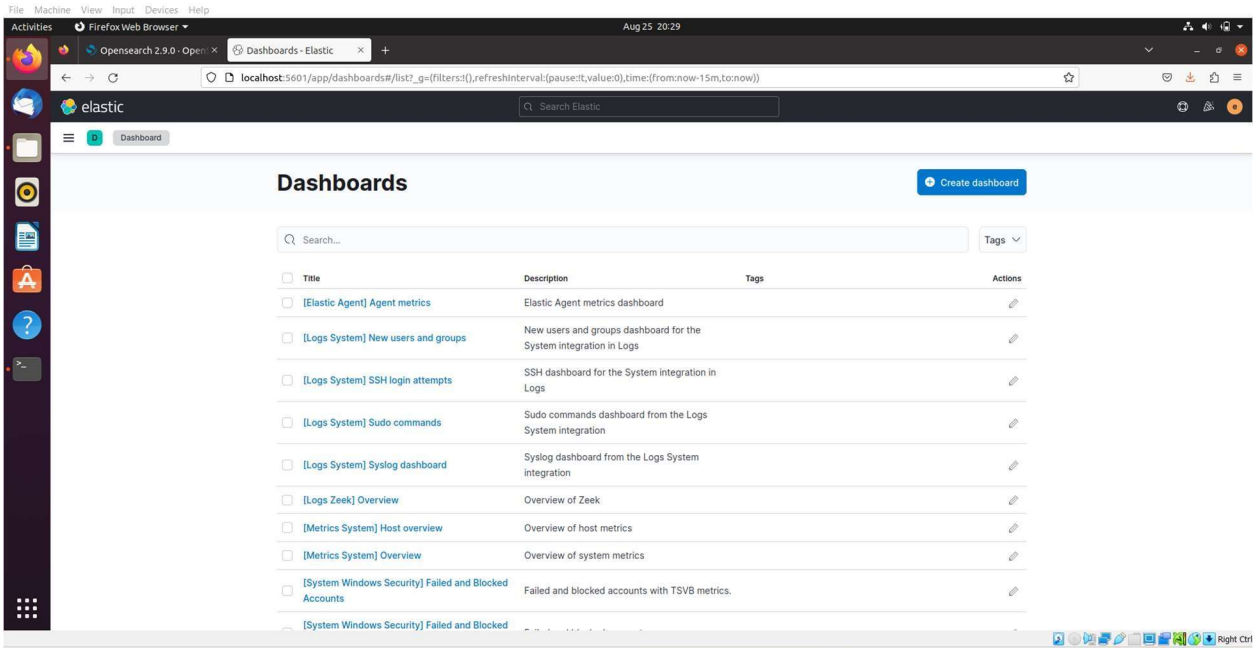
In logs



In metrics



Dashboard



Click on Create Visualization