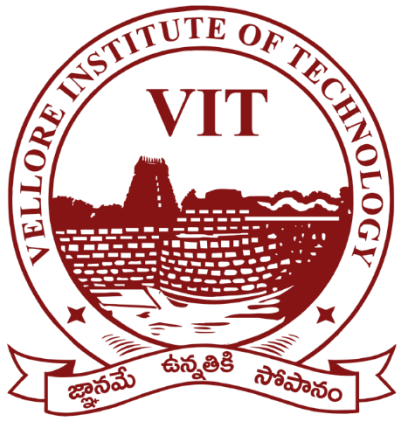


VIT-AP UNIVERSITY

NAME : POTNURI LOKESH MANIKANTA

REGISTRATION NUMBER : 21BCE9436

FACULTY : Sibi Chakkaravarthy S

SLOT : E2

PROJECT NAME : ELK

Before installation of ELK do set up for dependencies required :

Check ubuntu version you are using

```
root@Loke4884:/# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04.3 LTS
Release:        22.04
Codename:       jammy
```

Install java dependencies

apt install default-jdk default-jre -y

```
root@Loke4884:/# apt install default-jdk default-jre -y
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).
0 upgraded, 0 newly installed, 0 to remove and 14 not upgraded.
```

Check java version

javac -version

```
root@Loke4884:/# javac -version
javac 11.0.20
```

Make sure that curl installed if not then install curl

```
root@Loke4884:/# 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).
0 upgraded, 0 newly installed, 0 to remove and 14 not upgraded.
```

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 -

```
root@Loke4884:/# 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

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

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

Installation of Elastic search:

apt update

```
loke4884@Loke4884:~$ sudo su
[sudo] password for loke4884:
root@Loke4884:/home/loke4884# 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]
Ign:3 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4 InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Ign:5 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0 InRelease
Get:6 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:7 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4 Release [3,094 B]
Get:8 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0 Release [3,094 B]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [657 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:11 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4 Release.gpg [866 B]
Get:12 http://download.opensuse.org/repositories/security:/zeek/xUbuntu_22.04  InRelease [1,560 B]
Get:13 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [889 kB]
Get:14 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0 Release.gpg [866 B]
Get:15 http://download.opensuse.org/repositories/security:/zeek/xUbuntu_22.04  Packages [11.9 kB]
Get:16 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4/multiverse amd64 Packages [17.8 kB]
Get:17 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4/multiverse arm64 Packages [14.9 kB]
Get:18 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0/multiverse amd64 Packages [17.8 kB]
Get:19 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0/multiverse arm64 Packages [14.9 kB]
Get:20 http://in.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [471 kB]
Get:21 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [300 kB]
Get:22 http://in.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [214 kB]
Get:23 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [100 kB]
Get:24 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [15.6 kB]
Get:25 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [710 kB]
Get:26 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [113 kB]
Get:27 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [647 kB]
Get:28 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [965 kB]
Get:29 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [278 kB]
Get:30 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [21.5 kB]
Get:31 http://in.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:32 http://in.archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [4,924 B]
Get:33 http://in.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [15.5 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [42.8 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [11.2 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [770 kB]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [553 kB]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [39.9 kB]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [16.4 kB]
```

Install elastic search

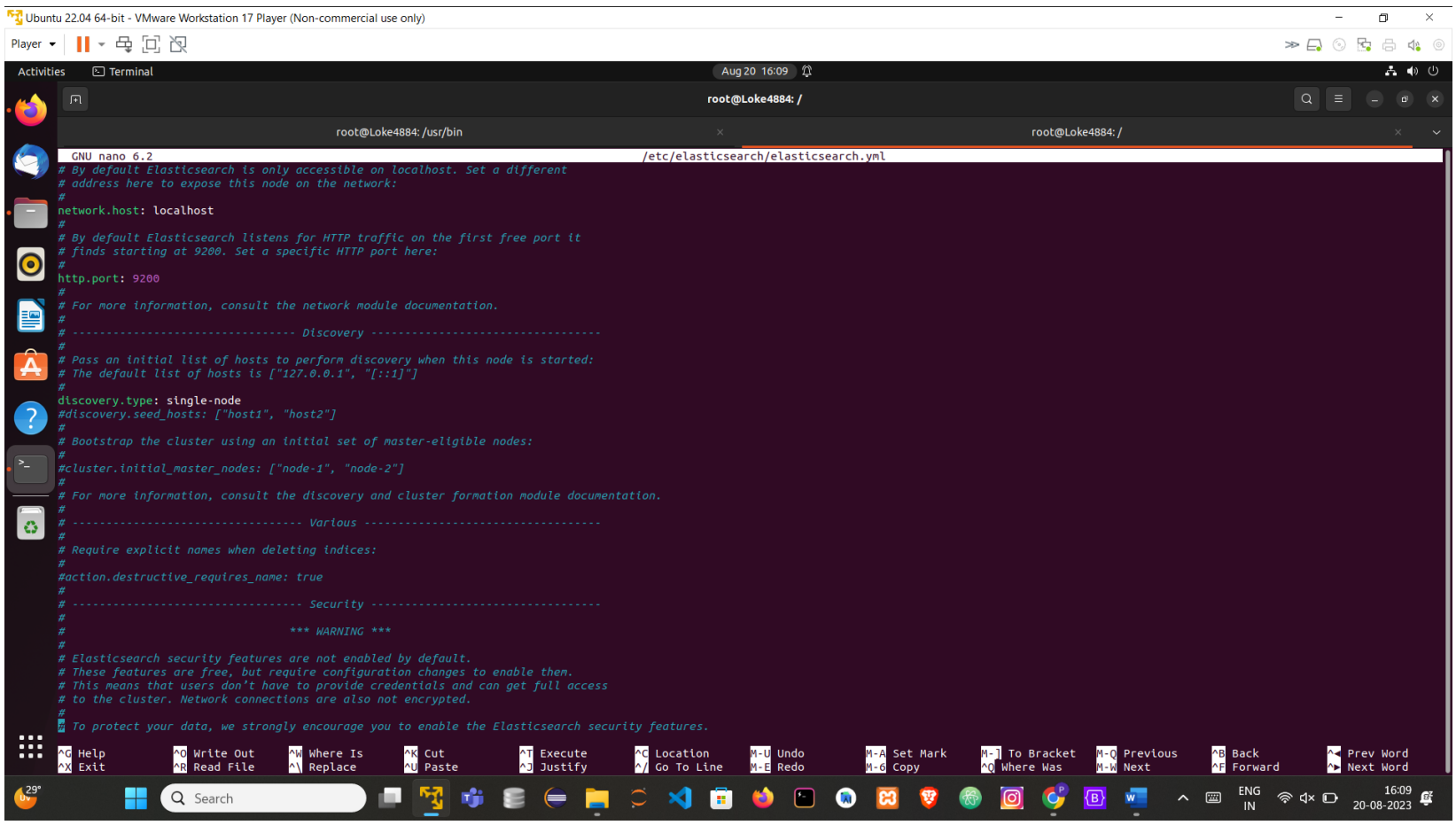
apt install elasticsearch -y

```
root@Loke4884:/# 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).
0 upgraded, 0 newly installed, 0 to remove and 14 not upgraded.
```

Configuration of elasticsearch

nano /etc/elasticsearch/elasticsearch.yml

```
root@Loke4884:/# nano /etc/elasticsearch/elasticsearch.yml
```



If you wanna speacify ip you can

```
network.host: '192.168.195.128
#
# By default Elasticsearch lis
# finds starting at 9200. Set
#
http.port: 9200
```

Configure the JVM heap memory by using the below command

nano /etc/elasticsearch/jvm.options

```
root@Loke4884:/# nano /etc/elasticsearch/jvm.options
```

```
################################################################
##
## JVM configuration
##
################################################################
##
## WARNING: DO NOT EDIT THIS FILE. If you want to override the
## JVM options in this file, or set any additional options, you
## should create one or more files in the jvm.options.d
## directory containing your adjustments.
##
## See https://www.elastic.co/guide/en/elasticsearch/reference/7.17/jvm-options.html
## for more information.
##
################################################################



################################################################
## 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
##
################################################################
```

Restart elasticsearch

systemctl restart elasticsearch

```
root@Loke4884:/# systemctl restart elasticsearch
```

Enable elastic search

```
root@Loke4884:/# sudo 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
```

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

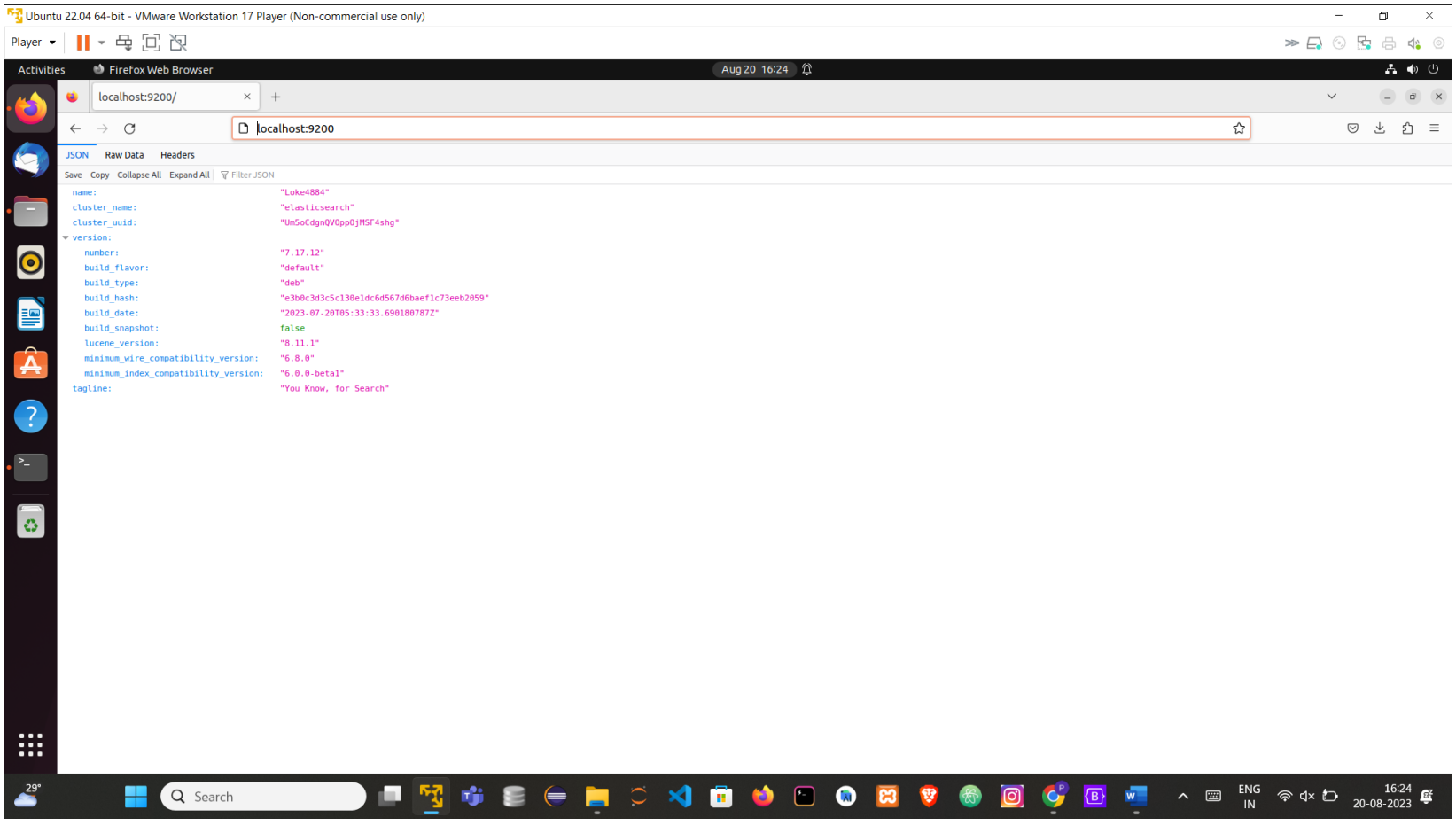
```
root@Loke4884:/# curl -X GET "localhost:9200"
```

I changed from localhost to ip

```
root@lokesh-manikanta:/# curl -X GET "192.168.195.148:9200"
{
  "name" : "lokesh-manikanta",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "k9kOW4P6RmOPF7mvL2JNyQ",
  "version" : {
    "number" : "7.17.13",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "2b211dbb8bfdecaf7f5b44d356bdfe54b1050c13",
    "build_date" : "2023-08-31T17:33:19.958690787Z",
    "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"
}
```

Search on browser :

localhost:9200



Installation of logstash

```
root@Loke4884:/home/loke4884# apt install logstash -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver intel-media-va-driver
  libaacs0 libaom3 libass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3
  libbluray2 libbs2b0 libchromaprint1 libcodec2-1.0 libdav1d5 libflashrom1 libflite1
  libftdi1-2 libgme0 libgsm1 libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0
  libllvm13 libmfx1 libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55
  librabbitmq4 librubberband2 libserd-0-0 libshine3 libsnappy1v5 libsord-0-0
  libsratom-0-0 libsrt1.4-gnutls libssh-gcrypt-4 libswresample3 libswscale5 libudfread0
  libva-drm2 libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1 libx265-199
  libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 linux-headers-5.19.0-41-generic
  linux-hwe-5.19-headers-5.19.0-41 linux-image-5.19.0-41-generic
  linux-modules-5.19.0-41-generic linux-modules-extra-5.19.0-41-generic mesa-va-drivers
  mesa-vdpau-drivers pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 141 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 4min 13s (1,449 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 286784 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@Loke4884:/home/loke4884# systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /etc/systemd/system/logstash.service.
```

systemctl enable logstash

```
root@lokesh-manikanta:/# systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /etc/systemd/system/logstash.service.
```

systemctl start logstash

```
root@lokesh-manikanta:/# systemctl start logstash
```

Checking that logstash is working or not :

```
root@lokesh-manikanta:/# systemctl status logstash
```

```
root@lokesh-manikanta:/# systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-09-23 01:03:41 IST; 18s ago
   Main PID: 11117 (java)
      Tasks: 15 (limit: 9390)
     Memory: 328.1M
        CPU: 32.516s
     CGroup: /system.slice/logstash.service
             └─11117 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.awt.headless=true -Dfile.encod>

Sep 23 01:03:41 lokesh-manikanta systemd[1]: Started logstash.
Sep 23 01:03:41 lokesh-manikanta logstash[11117]: Using bundled JDK: /usr/share/logstash/jdk
Sep 23 01:03:41 lokesh-manikanta logstash[11117]: 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)
^C
```

Kibana Set up

```
loke4884@Loke4884:~$ sudo su
[sudo] password for loke4884:
root@Loke4884:/home/loke4884# 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]
Ign:3 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4 InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Ign:5 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0 InRelease
Get:6 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:7 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4 Release [3,094 B]
Get:8 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0 Release [3,094 B]
Get:9 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [657 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:11 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4 Release.gpg [866 B]
Get:12 http://download.opensuse.org/repositories/security:/zeek/xUbuntu_22.04  InRelease [1,560 B]
Get:13 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [889 kB]
Get:14 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0 Release.gpg [866 B]
Get:15 http://download.opensuse.org/repositories/security:/zeek/xUbuntu_22.04  Packages [11.9 kB]
Get:16 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4/multiverse amd64 Packages [17.8 kB]
Get:17 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/4.4/multiverse arm64 Packages [14.9 kB]
Get:18 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0/multiverse amd64 Packages [17.8 kB]
Get:19 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/5.0/multiverse arm64 Packages [14.9 kB]
Get:20 http://in.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [471 kB]
Get:21 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [300 kB]
Get:22 http://in.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [214 kB]
Get:23 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 DEP-11 Metadata [100 kB]
Get:24 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [15.6 kB]
Get:25 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [710 kB]
Get:26 http://in.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [113 kB]
Get:27 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [647 kB]
Get:28 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [965 kB]
Get:29 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 DEP-11 Metadata [278 kB]
Get:30 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [21.5 kB]
Get:31 http://in.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 DEP-11 Metadata [940 B]
Get:32 http://in.archive.ubuntu.com/ubuntu jammy-backports/main amd64 DEP-11 Metadata [4,924 B]
Get:33 http://in.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 DEP-11 Metadata [15.5 kB]
Get:34 http://security.ubuntu.com/ubuntu jammy-security/main amd64 DEP-11 Metadata [42.8 kB]
Get:35 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [11.2 kB]
Get:36 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [770 kB]
Get:37 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [553 kB]
Get:38 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 DEP-11 Metadata [39.9 kB]
Get:39 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 c-n-f Metadata [16.4 kB]
```

Kibana Installation

apt install kibana -y

```
root@Loke4884:/home/loke4884# 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 16 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]
27% [1 kibana 93.2 MB/276 MB 34%]
224 MB in 17min 10s (217 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 268993 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
```

systemctl enable kibana

```
root@lokesh-manikanta:/# systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.
```

systemctl start kibana

```
root@lokesh-manikanta:/# systemctl start kibana
```

systemctl status kibana

```
root@lokesh-manikanta:/# systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2023-09-23 01:15:03 IST; 37s ago
       Docs: https://www.elastic.co
   Main PID: 12370 (node)
      Tasks: 11 (limit: 9390)
     Memory: 279.7M
        CPU: 24.542s
     CGroup: /system.slice/kibana.service
             └─12370 /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_deprecat>

Sep 23 01:15:03 lokesh-manikanta systemd[1]: Started Kibana.
Sep 23 01:15:04 lokesh-manikanta kibana[12370]: Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kiba>
```

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

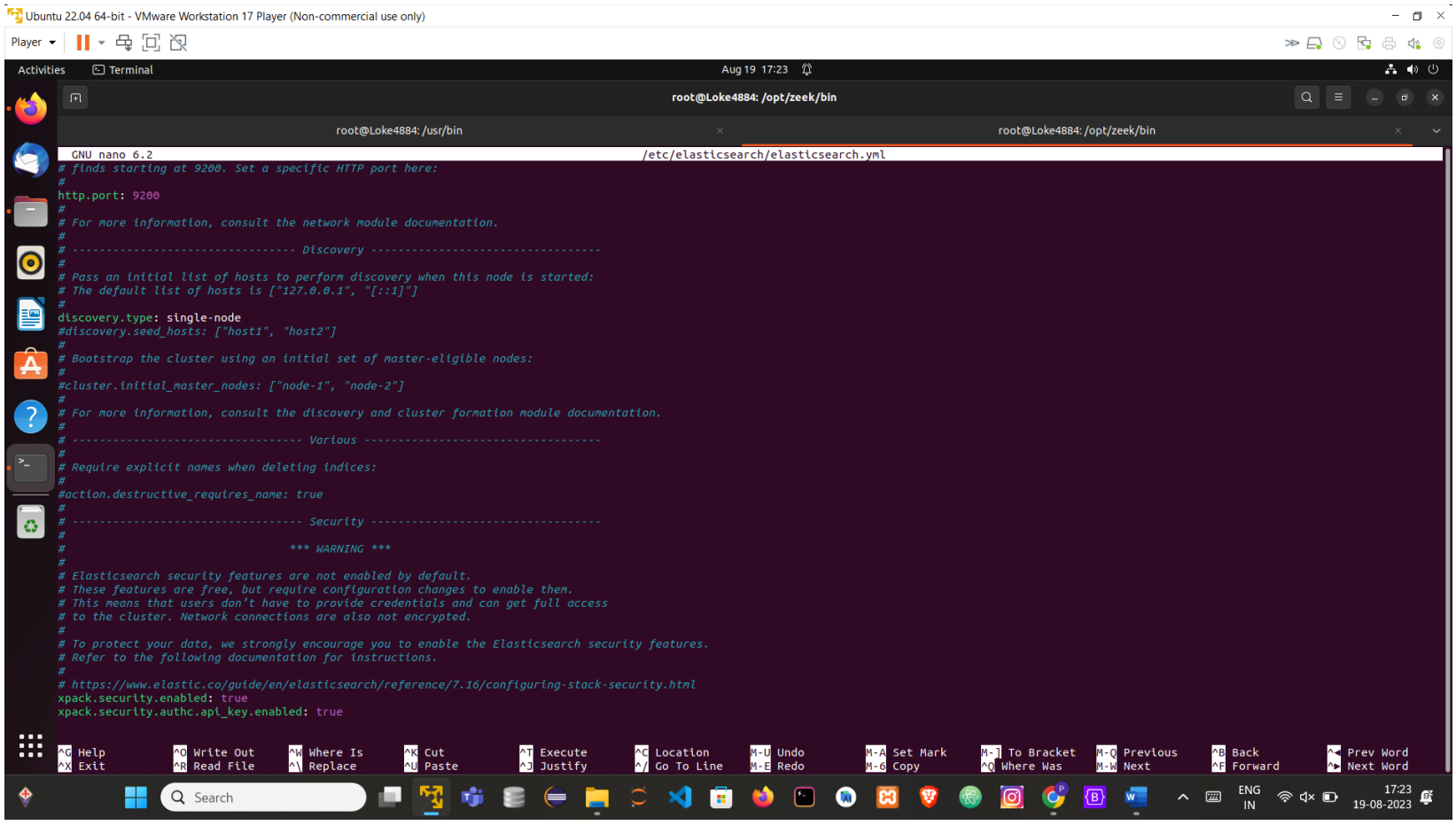
sudo nano /etc/elasticsearch/elasticsearch.yml

```
root@Loke4884:/opt/zeek/bin# nano /etc/elasticsearch/elasticsearch.yml
```

Add to elasticsearch.yml:

xpack.security.enabled: true

xpack.security.authc.api_key.enabled: true



Now restart elasticsearch

sudo systemctl restart elasticsearch

or

sudo systemctl stop elasticsearch

sudo systemctl start elasticsearch

```
root@Loke4884:/opt/zeek/bin# systemctl start elasticsearch
```

Set up default password :

Go to root by - cd /

cd usr/share/elasticsearch/bin

sudo ./elasticsearch-setup-passwords auto

Make sure you give elastic user name and password

```
root@lokesh-manikanta:/usr/share/elasticsearch/bin# ./elasticsearch-setup-passwords auto
Initiating the setup of passwords for reserved users elastic,apm_system,kibana,kibana_system,logstash_system,beats_system,remote_monitoring_user.
The passwords will be randomly generated and printed to the console.
Please confirm that you would like to continue [y/N]y
```

```
Changed password for user apm_system
PASSWORD apm_system = 34mdQ22XMqbb6iRpTdER

Changed password for user kibana_system
PASSWORD kibana_system = VXFYiFhWq3NRQadSCDvQ

Changed password for user kibana
PASSWORD kibana = VXFYiFhWq3NRQadSCDvQ

Changed password for user logstash_system
PASSWORD logstash_system = YNjmNhGLUUhUqATaCWAF

Changed password for user beats_system
PASSWORD beats_system = Zl2RNNyxr5OFAervhAA2

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = JJ4IvrCyL3QczWCf0vk6

Changed password for user elastic
PASSWORD elastic = 3c6pLbiXhKoZrvNudjgd
```

Open kibana.yml

```
root@Loke4884:/# nano /etc/kibana/kibana.yml
```

Give elasticsearch.username and elasticsearch.password as generated in

```
  GNU nano 6.2                                                                /etc/kibana/kibana.yml
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
elasticsearch.username: "elastic"
elasticsearch.password: "3c6pLbiXhKoZrvNudjgd"
```

and make sure that elasticsearch.hosts is uncommented by default it is commented to run kibana

root@Loke4884: /usr/bin × root@Loke4884: /opt/zeek/bin

GNU nano 6.2 /etc/kibana/kibana.yml

```
# 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"
```

Save kibana.yml by ctrl+O

Restart kibana

sudo systemctl restart kibana

Or

sudo systemctl stop kibana

sudo systemctl start kibana

To know elasticsearch logstash and kibana working properly

Just give command as

sudo systemctl status elasticseach logstash kibana

Ubuntu 22.04 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player

Activities Terminal Aug 20 15:46

root@Loke4884: /opt/zeek/bin

root@Loke4884: /usr/bin × root@Loke4884: /opt/zeek/bin

```
lines 1-45
You have new mail in /var/mail/root
root@Loke4884:/opt/zeek/bin# systemctl status elasticsearch logstash kibana
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2023-08-18 22:35:58 IST; 1 day 17h ago
       Docs: https://www.elastic.co
   Main PID: 43544 (java)
      Tasks: 88 (limit: 9374)
     Memory: 1.4G
        CPU: 15min 33.371s
     CGroup: /system.slice/elasticsearch.service
             ├─43544 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless=true -Dft
             └─43728 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Aug 18 22:35:40 Loke4884 systemd[1]: Starting Elasticsearch...
Aug 18 22:35:58 Loke4884 systemd[1]: Started Elasticsearch.

● logstash.service - logstash
     Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: deactivating (stop-sigterm) since Fri 2023-08-18 22:36:13 IST; 1 day 17h ago
   Main PID: 23206 (java)
      Tasks: 24 (limit: 9374)
     Memory: 592.3M
        CPU: 2min 55.605s
     CGroup: /system.slice/logstash.service
             └─23206 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.awt.headless=true -Dfile.encodi

Aug 17 22:45:36 Loke4884 logstash[23206]: OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
Aug 17 22:46:05 Loke4884 logstash[23206]: Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties
Aug 17 22:46:05 Loke4884 logstash[23206]: [2023-08-17T22:46:05,522][INFO ][logstash.runner          ] Log4j configuration path used is: /etc/logstash/log4j2.properties
Aug 17 22:46:05 Loke4884 logstash[23206]: [2023-08-17T22:46:05,545][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"7.17.12", "jruby.version"=>"jruby 9.2.20.1 (2.5.8) 2021-11-30
Aug 17 22:46:05 Loke4884 logstash[23206]: [2023-08-17T22:46:05,551][INFO ][logstash.runner          ] JVM bootstrap flags: [-Xms1g, -Xmx1g, -XX:+UseConcMarkSweepGC, -XX:CMSInitiatingOccupancyFraction=75,
Aug 17 22:46:08 Loke4884 logstash[23206]: [2023-08-17T22:46:08,279][INFO ][logstash.config.source.local.configpathloader] No config files found in path {:path=>"/etc/logstash/conf.d/*.conf"}
Aug 17 22:46:08 Loke4884 logstash[23206]: [2023-08-17T22:46:08,288][INFO ][logstash.agent           ] Successfully started Logstash API endpoint {:port=>9600, :ssl_enabled=>false}
Aug 17 22:46:08 Loke4884 logstash[23206]: [2023-08-17T22:46:08,294][ERROR][logstash.config.sourceloader] No configuration found in the configured sources.
Aug 18 22:36:13 Loke4884 systemd[1]: Stopping logstash...
Aug 18 22:36:14 Loke4884 logstash[23206]: [2023-08-18T22:36:14,192][WARN ][logstash.runner          ] SIGTERM received. Shutting down.

● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2023-08-18 22:41:23 IST; 1 day 17h ago
       Docs: https://www.elastic.co
   Main PID: 43912 (node)
      Tasks: 11 (limit: 9374)
     Memory: 281.4M
```

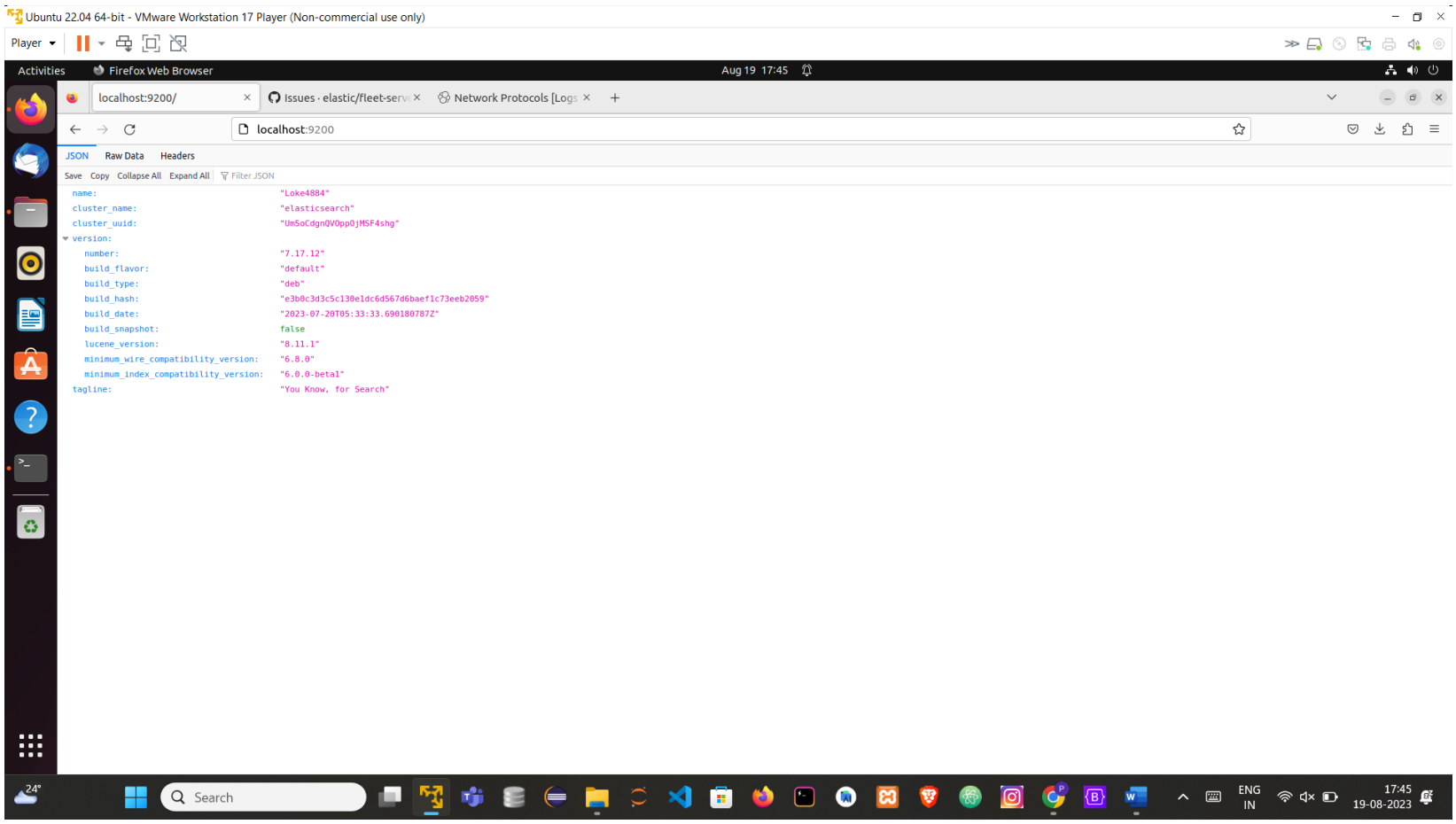
Search ENG IN 15:46 20-08-2023

Make sure to restart logstash

sudo systemctl restart logstash

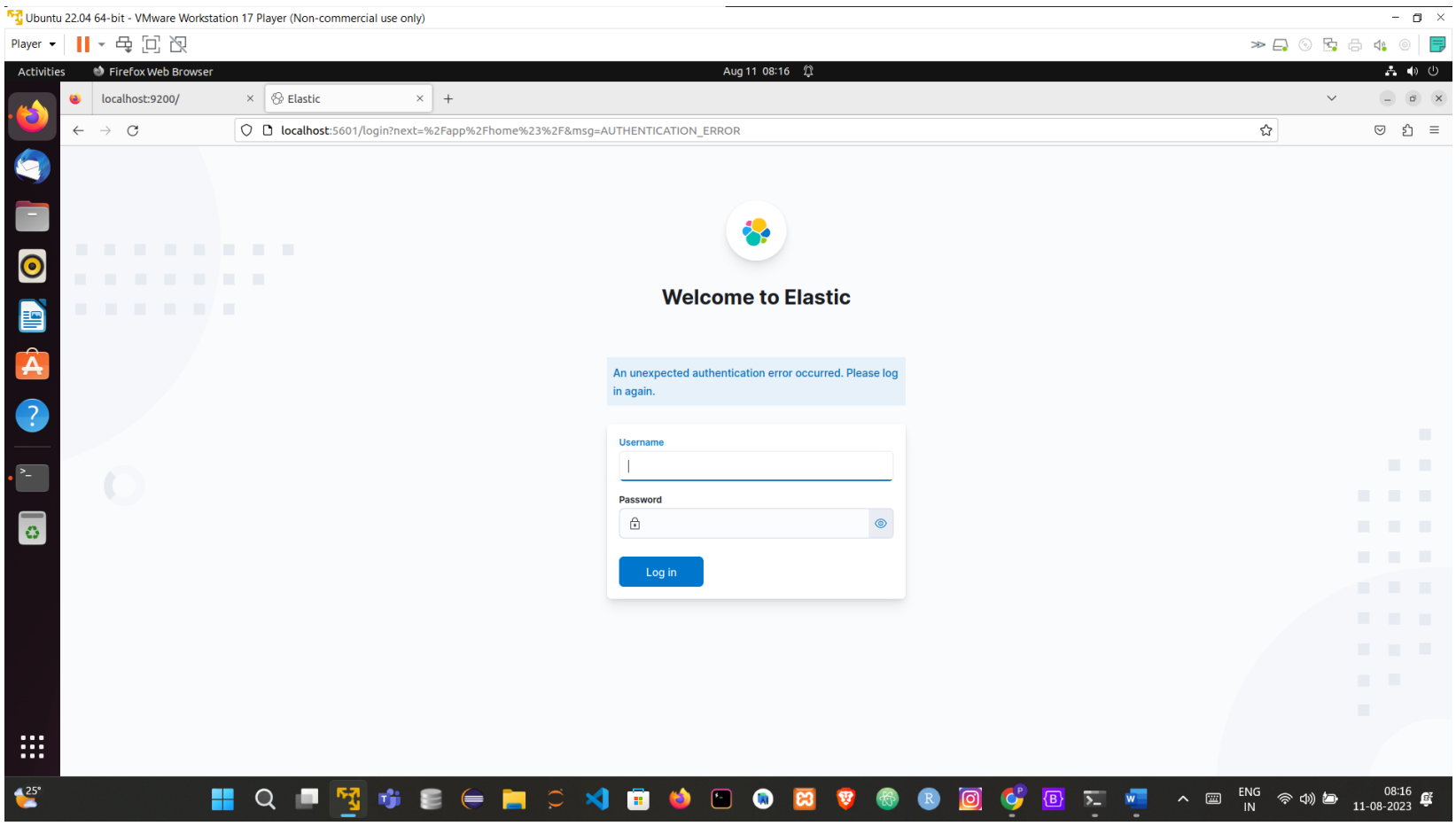
Next search browser of Ubuntu:

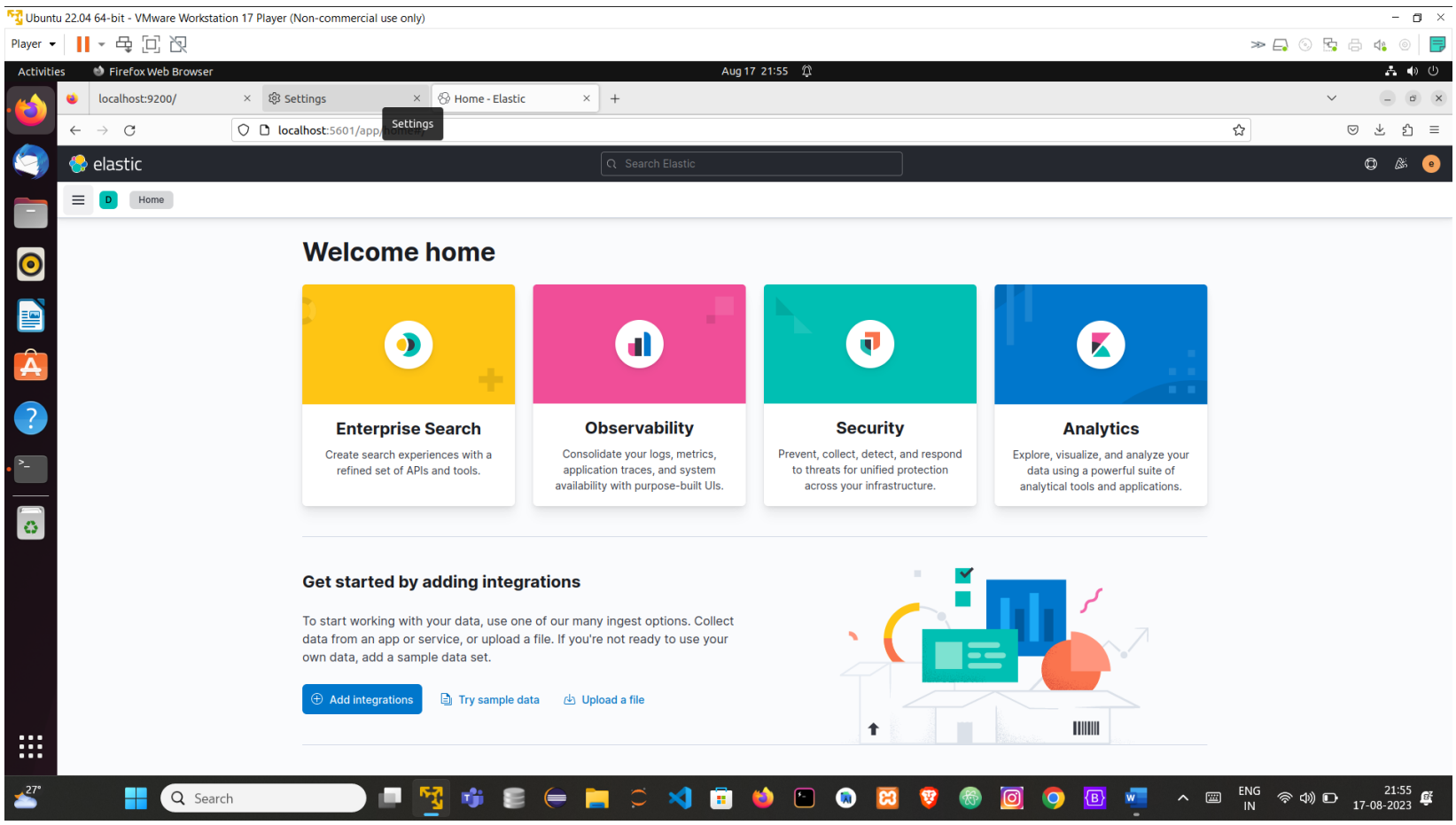
localhost:9200



Next search browser of Ubuntu :

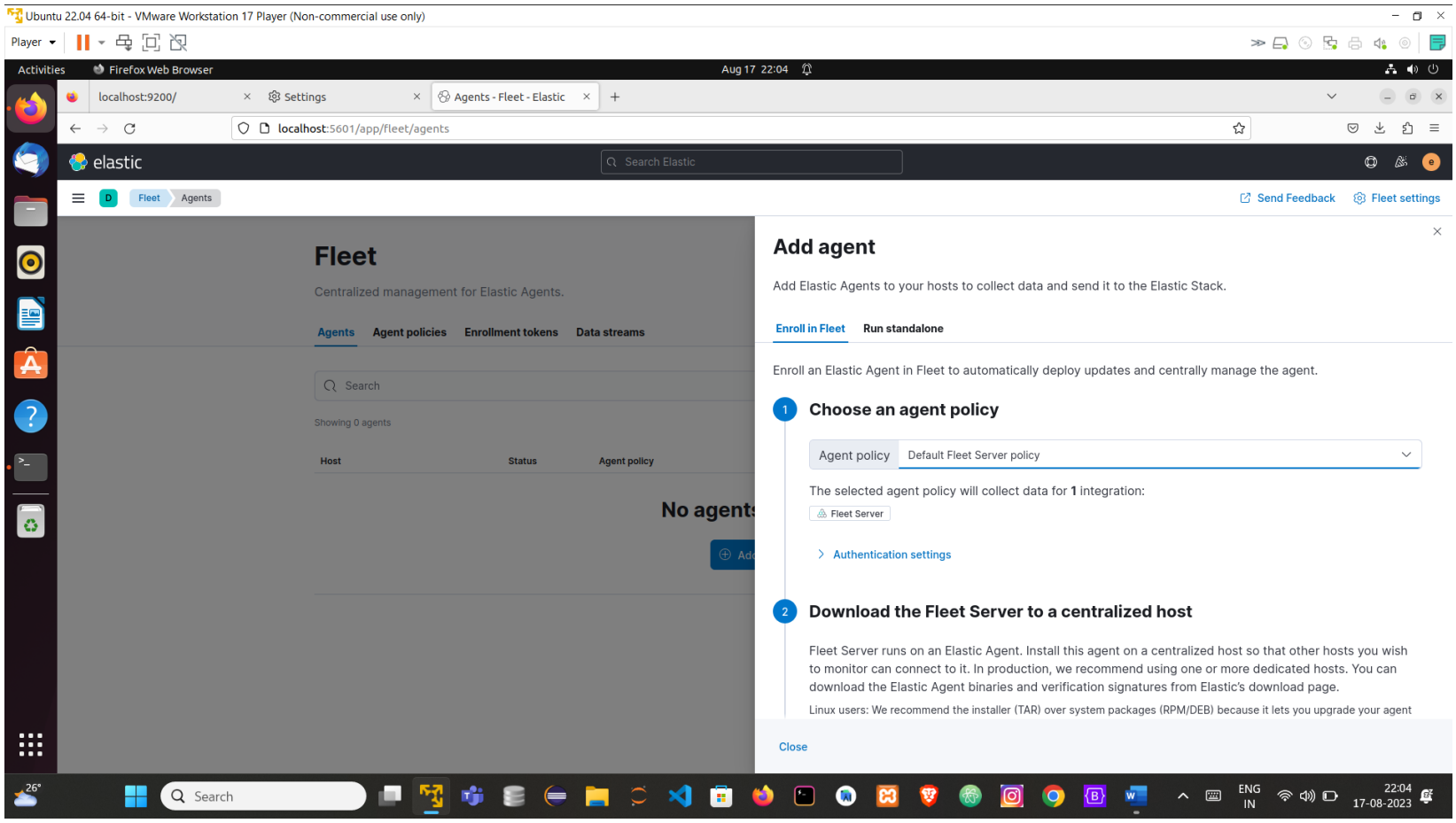
localhost:5200





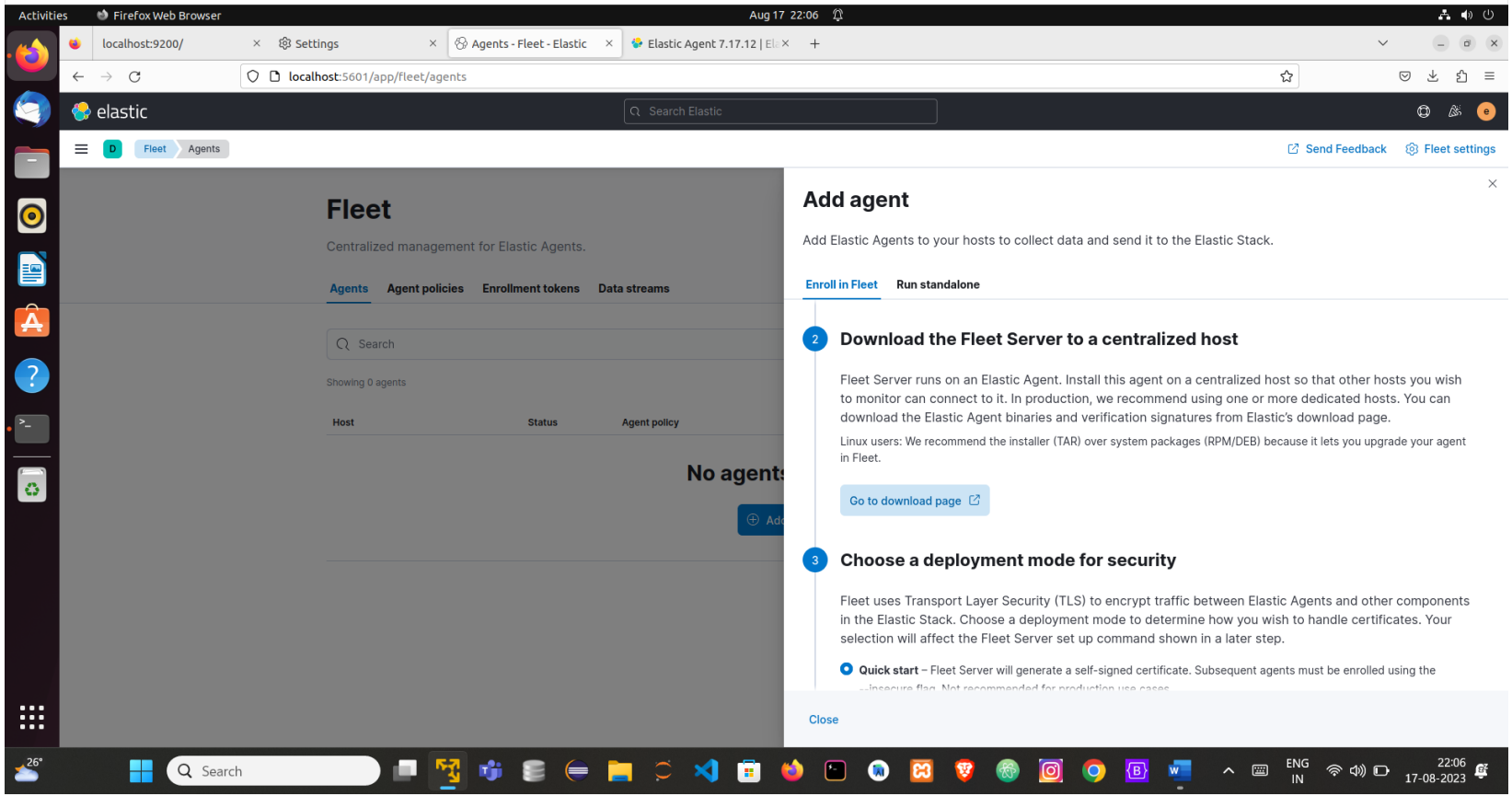
Go to management → fleet

Click on add agent

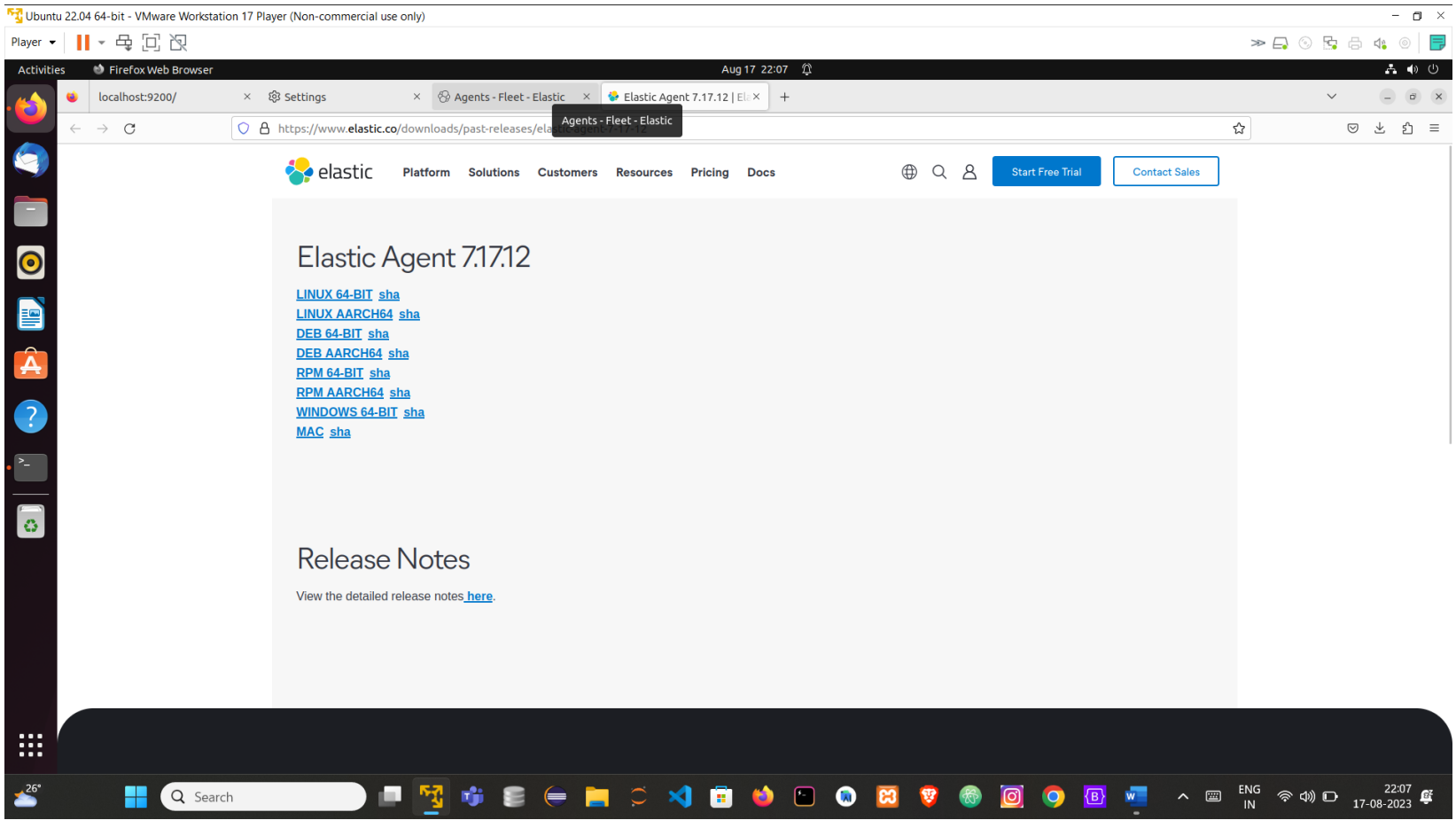


Enroll Fleet section →

Download Fleet Server to centralized host

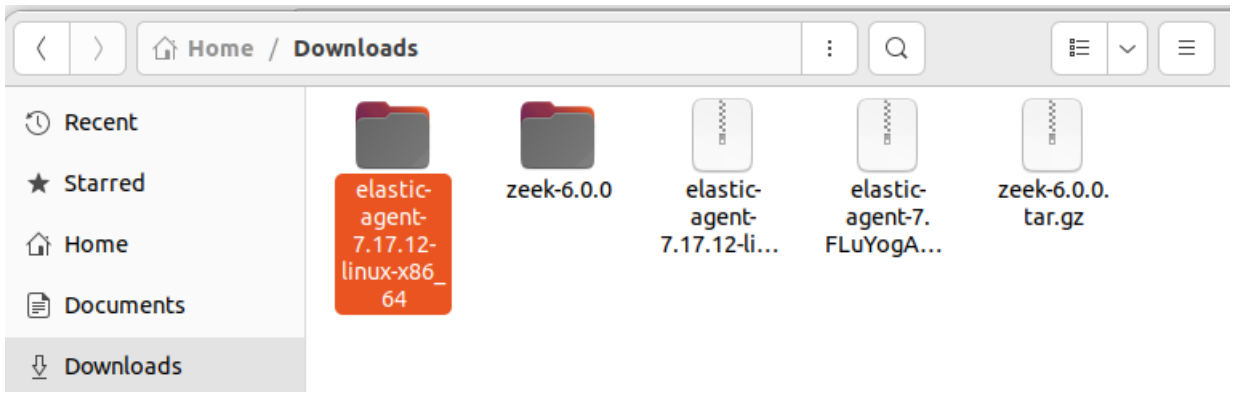


Click on download page



Download respective Elastic Agent

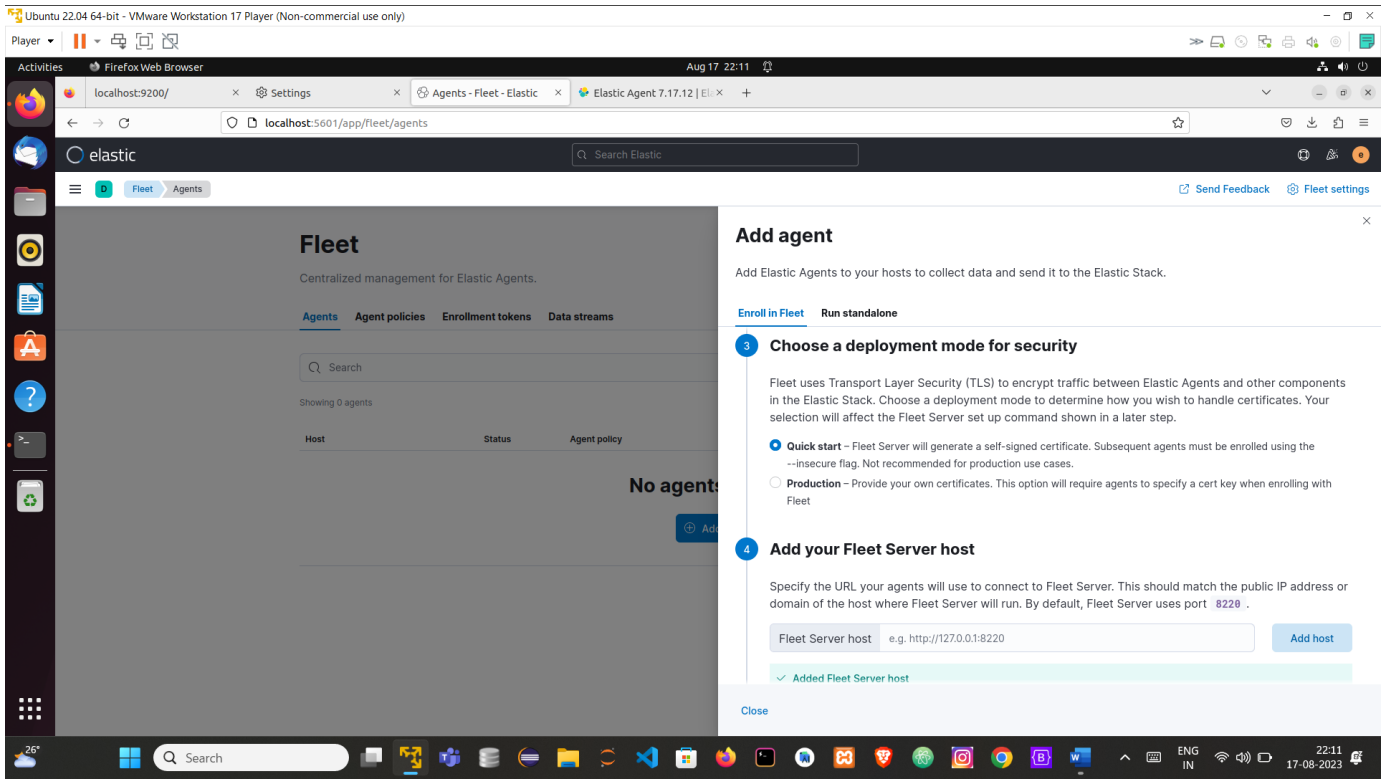
I downloaded LINUX 64-BIT sha Elastic Agent 7.17.12 just unzip that folder



Choose a deployment mode for security

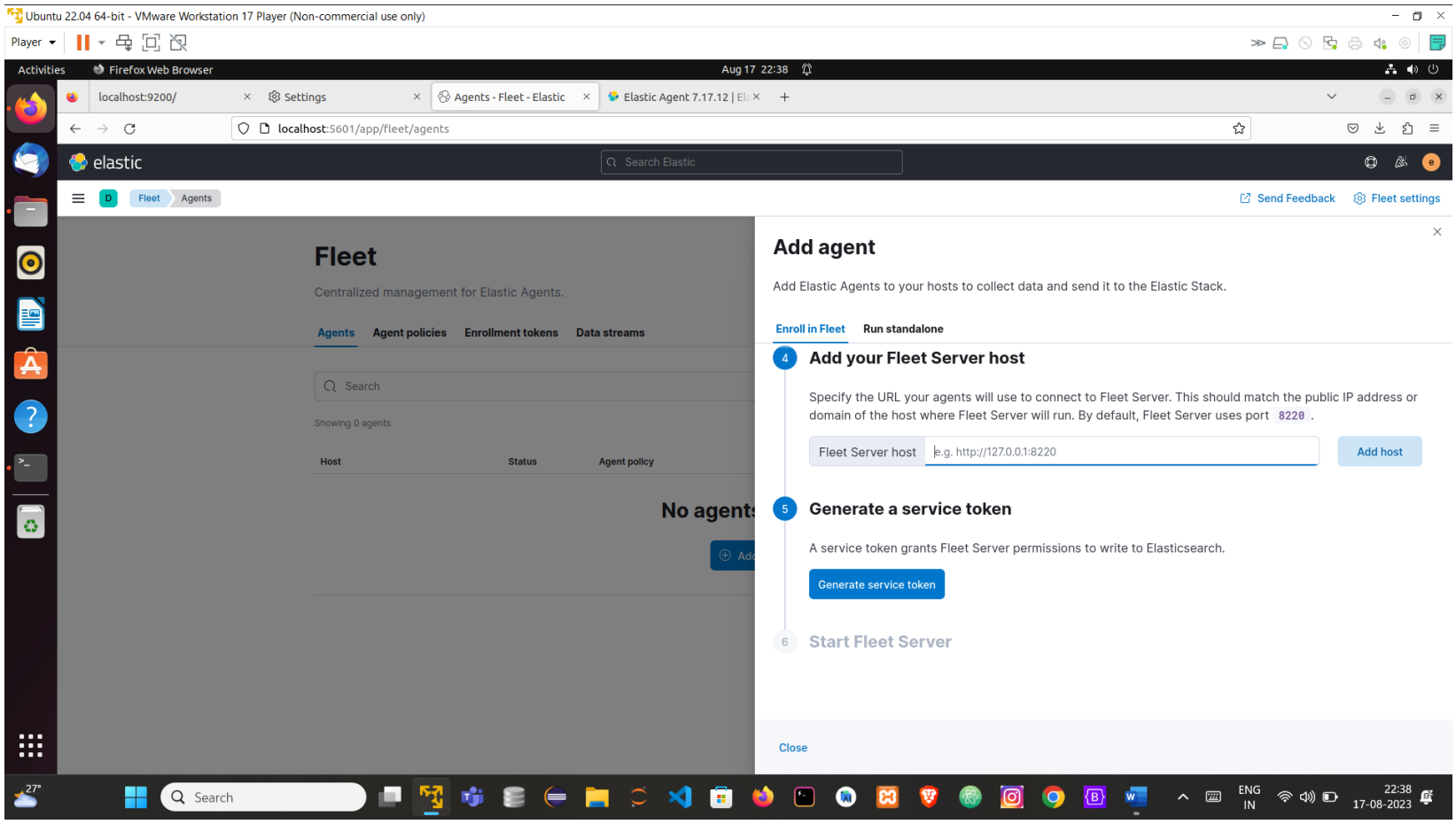
By default it is Production

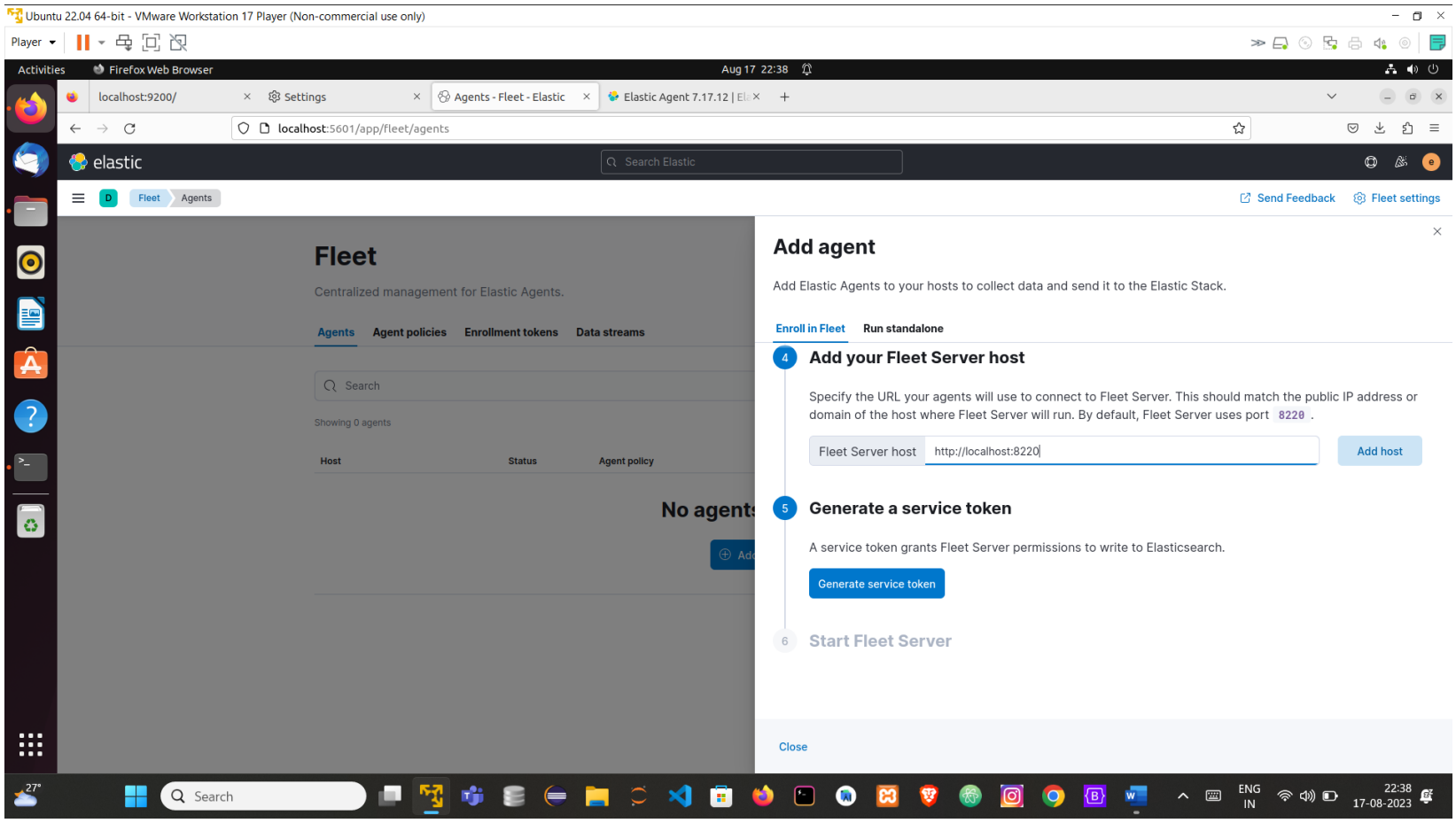
Choose Quick start



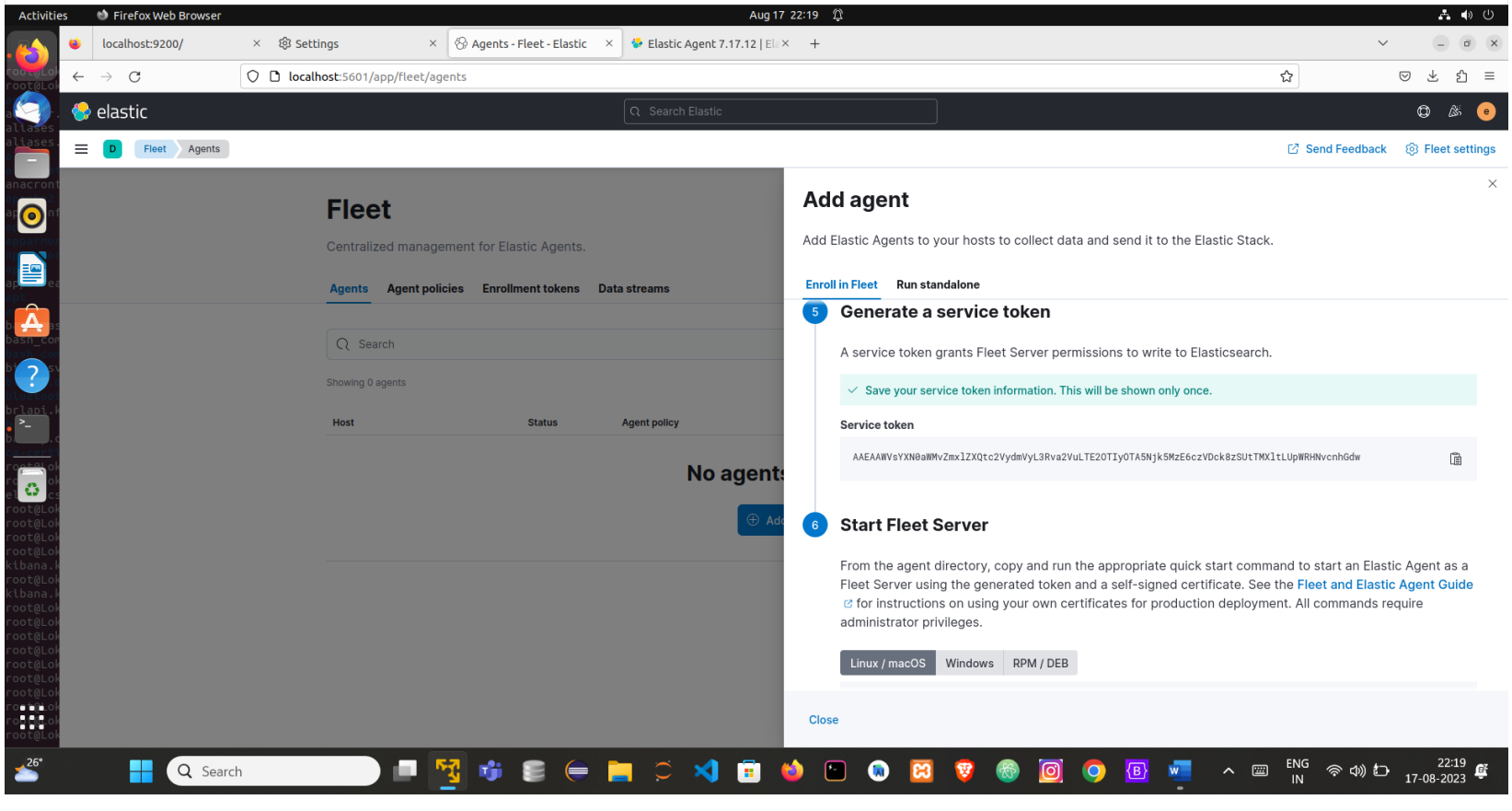
Add yours fleet host server

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



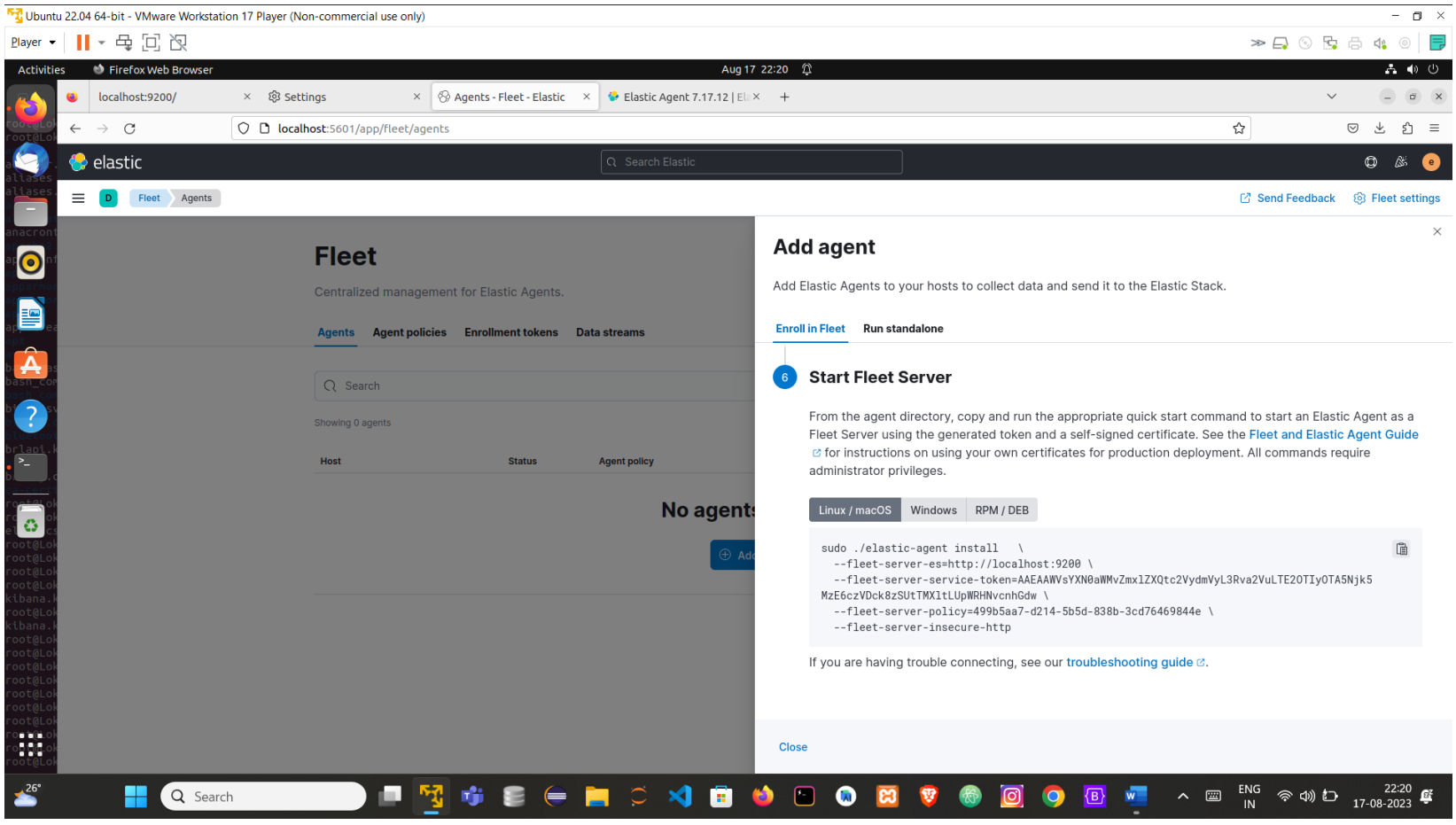


Generate a service token



Service token : AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2OTIyOTA5Njk5MzE6czVDck8zSUtTMXltLUpWRHNvcnhGdw

Start Fleet server

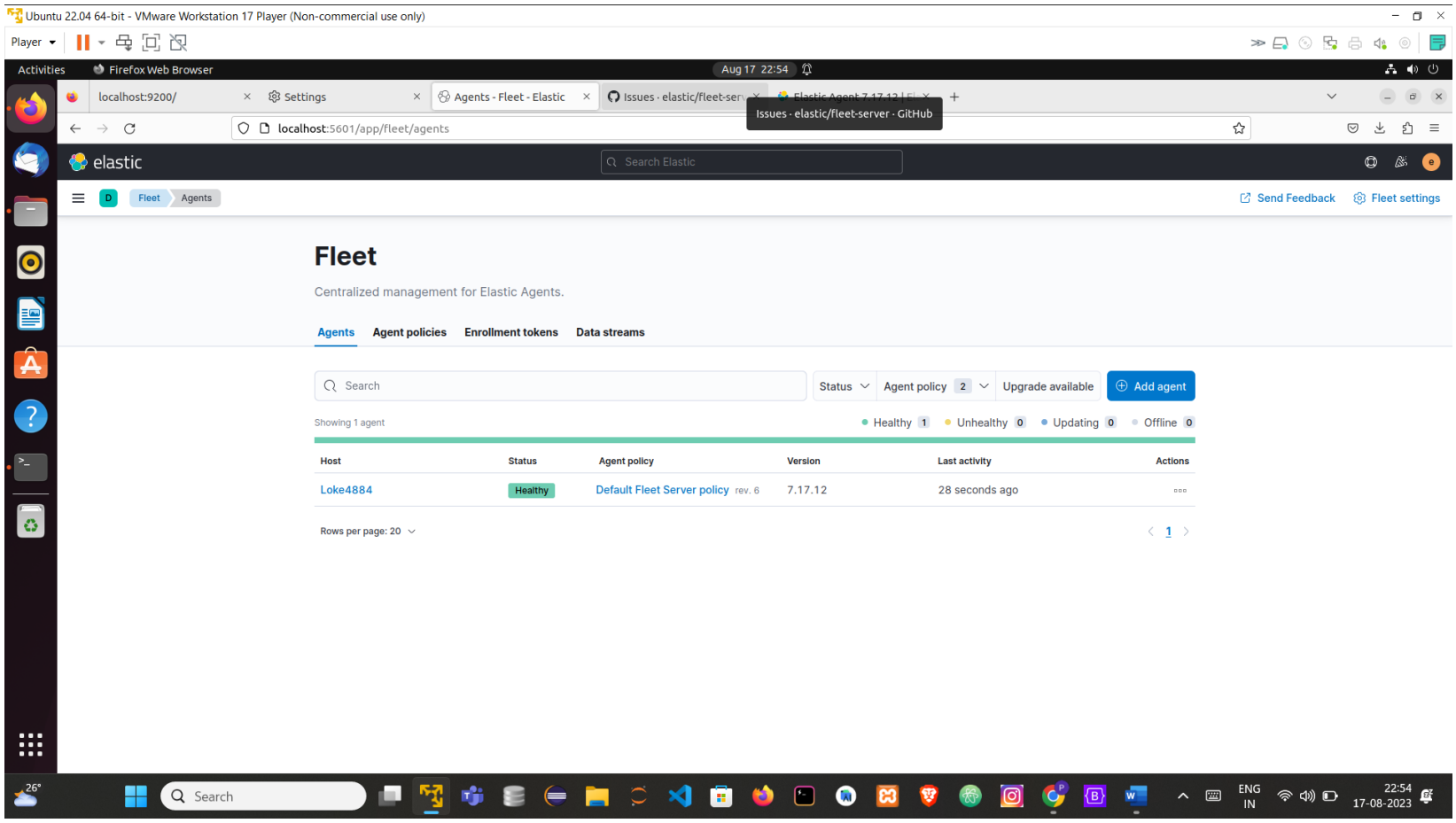


Copy commands and give those command in ubuntu terminal (give commands related to which environment based elastic agent you downloaded)

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

```
root@Loke4884:/home/loke4884/Downloads/elastic-agent-7.17.12-linux-x86_64# ls
data  elastic-agent  elastic-agent.reference.yml  elastic-agent.yml  LICENSE.txt  NOTICE.txt  README.md
root@Loke4884:/home/loke4884/Downloads/elastic-agent-7.17.12-linux-x86_64# sudo ./elastic-agent install   \
  --fleet-server-es=http://localhost:9200 \
  --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE2OTIyOTI1MzQ4MDQ6RTQyTEFxS01TTUc4RjNpdWFqSUI1Zw \
  --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
2023-08-17T22:51:54.451+0530    INFO    cmd/enroll_cmd.go:776   Fleet Server - Starting
2023-08-17T22:51:58.455+0530    INFO    cmd/enroll_cmd.go:757   Fleet Server - Running on policy with Fleet Server integration: 499b5aa7-d214-5b5d-838b-3cd76469844e; missing config fleet.agent.id (expecte
d during bootstrap process)
2023-08-17T22:51:58.456+0530    WARN    [tls]   tlscommon/tls_config.go:101     SSL/TLS verifications disabled.
2023-08-17T22:51:58.533+0530    INFO    cmd/enroll_cmd.go:454   Starting enrollment to URL: http://localhost:8220/
2023-08-17T22:51:59.543+0530    INFO    cmd/enroll_cmd.go:254   Successfully triggered restart on running Elastic Agent.
Successfully enrolled the Elastic Agent.
Elastic Agent has been successfully installed.
```

Fleet server hosted



Make sure that zeek logs are running :

```
root@Loke4884:/opt/zeek/bin# ./zeekctl deploy
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

```
root@Loke4884:/# cd home/
root@Loke4884:/home# cd loke4884/
root@Loke4884:/home/loke4884# cd Downloads/
root@Loke4884:/home/loke4884/Downloads# cd zeek-6.0.0
root@Loke4884:/home/loke4884/Downloads/zeek-6.0.0# ls
auxil    cl            configure         doc                       INSTALL   NEWS       repo-info.json  src      zeek-config.h.in        zeek-path-dev.bat.in  zkg-config.in
build    cmake         COPYING           docker                    Makefile  README     scripts         testing  zeek-config.in          zeek-path-dev.in
CHANGES  CMakeLists.txt  COPYING-3rdparty  hilti-cxx-include-dirs.in  man       README.md  spicy-path.in   VERSION  zeek-config-paths.h.in  zeek-version.h.in
root@Loke4884:/home/loke4884/Downloads/zeek-6.0.0# cd scripts/
root@Loke4884:/home/loke4884/Downloads/zeek-6.0.0/scripts# ls
base  CMakeLists.txt  policy  site  spicy  test-all-policy.zeek  zeekygen
root@Loke4884:/home/loke4884/Downloads/zeek-6.0.0/scripts# cd site/
root@Loke4884:/home/loke4884/Downloads/zeek-6.0.0/scripts/site# ls
local.zeek
```

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

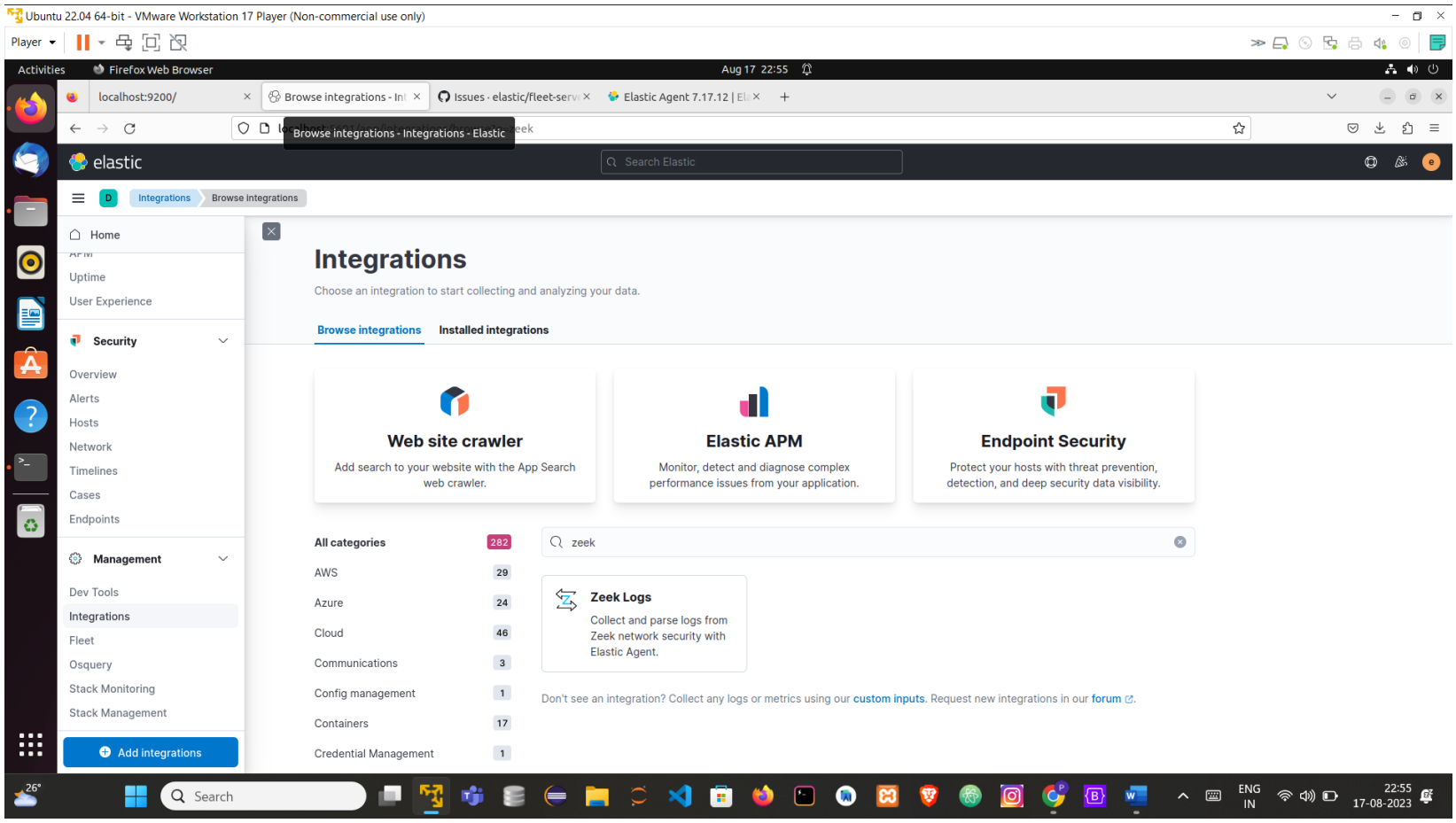
```
  GNU nano 6.2                                                                local.zeek *
@load protocols/http/detect-sqli

#### 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
@load policy/tuning/json-logs.zeek
```

Then save the file by ctrl+o ,ctrl+x to exit

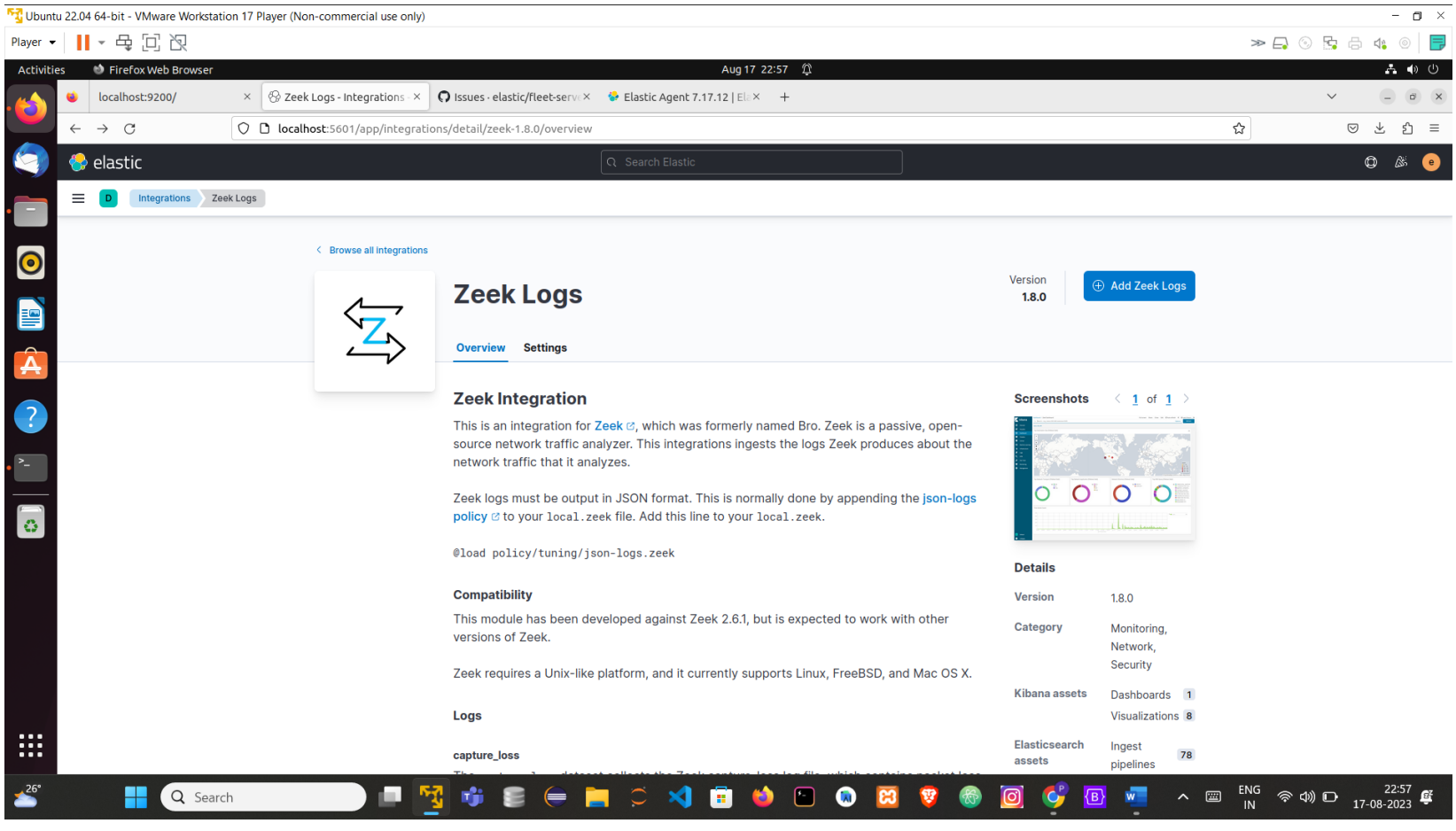
After saving the file restart zeek again

```
root@Loke4884:/opt/zeek/bin# ./zeekctl deploy
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 ...
starting ...
starting zeek ...
```

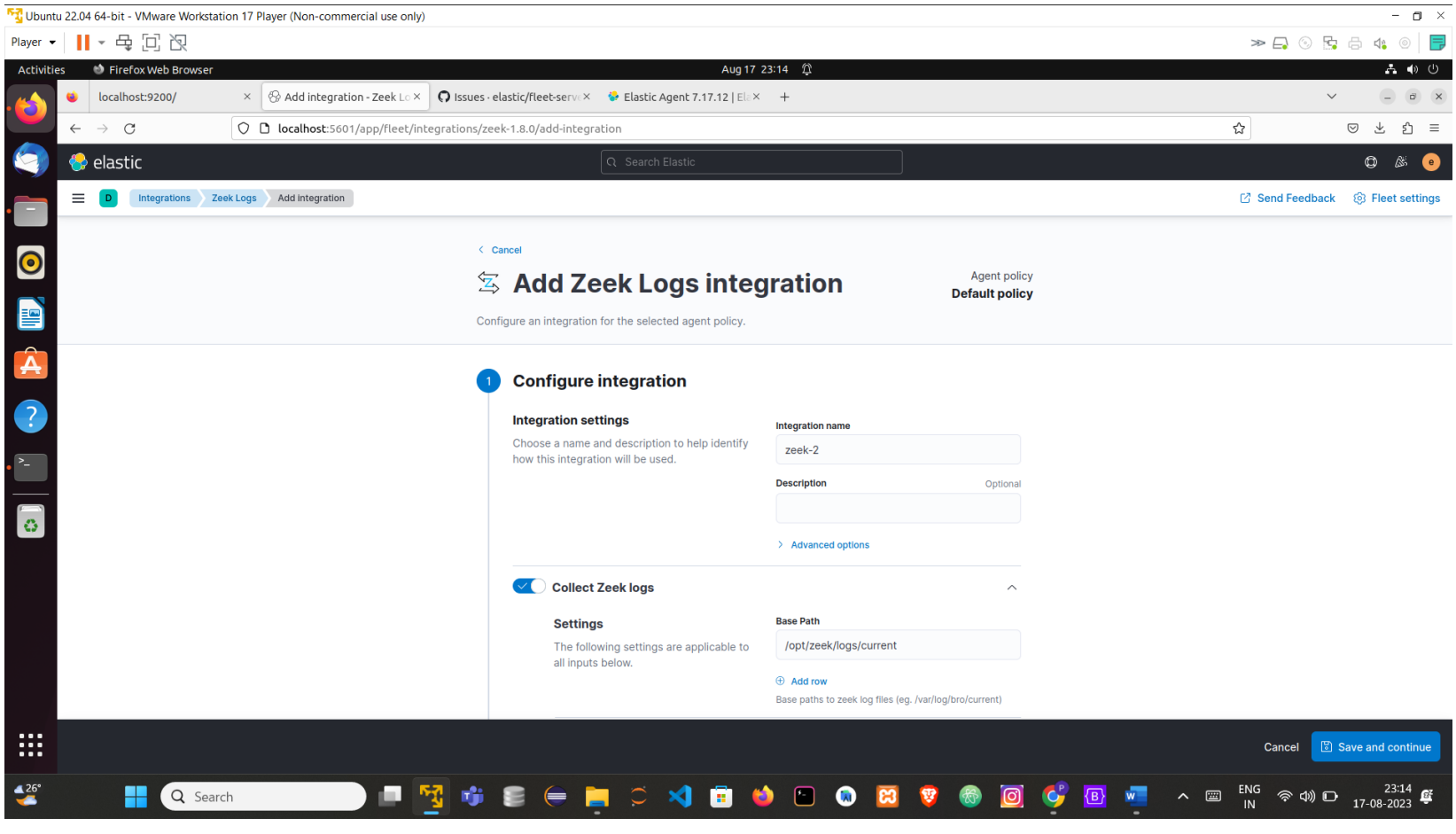
Go to Integrations → search Zeek logs



Click on add zeek logs



Give as bellow



Give the path where zeek logs stored

```
root@Loke4884:/opt/zeek/logs/current# ls
capture_loss.log  conn.log  dhcp.log  dns.log  notice.log  stats.log  stderr.log  stdout.log  telemetry.log  weird.log
```

```
root@Loke4884:/opt/zeek/logs/current# cat conn.log
#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      miss
ed_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       CvHrt72jIcRCoeBBAk      192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109800.594809       COkkuUDxTHWHoWOmd       192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       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       0       -
1692109794.563978       CJDKkC1zKeagrxVFYb      192.168.128.129 59382   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109794.564078       Ceovc44fI8WaiKHhB2      192.168.128.129 58498   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       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       0       -
1692109802.608777       CtUaMs4FYaxaBybKCi      192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109806.703519       CrgE9r3feTHKpbOtHk      192.168.128.129 33630   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       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       0       -
1692109815.655527       CJBEZ12TpaKDYDZrc7      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109809.599495       Cpa6ld48FuFoiKOwD3      192.168.128.129 34987   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109809.599699       CztbKY1mVWHdxSGGPk      192.168.128.129 33829   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109809.599948       C7KoAS12GjkayjyZg4      192.168.128.129 34753   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       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       0       -
1692109809.600497       CwR6ru47hLZ3mX9Hhf      192.168.128.129 38296   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109809.600932       CA24qL36IrV8eVqsud      192.168.128.129 41801   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       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       0       -
1692109817.717870       CQAfJM39saLgh8UEEf      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109821.817420       C89OK126MYoPiLDy27      192.168.128.129 49770   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109829.632272       CdD18z4OA35tjyrDzi      192.168.128.129 40510   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109830.639696       ClN3iX1ahoIZPeG0S3      192.168.128.129 40510   192.168.128.1   53      tcp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109824.617310       CvXOu52uVyRseU6tog      192.168.128.129 43988   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       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       0       -
1692109824.618129       CNui7TCyia58nJPsg       192.168.128.129 44948   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109824.618473       CUK8s32qk8IkircFci      192.168.128.129 36646   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       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       0       -
1692109824.619235       CYzfj52530amZBHvr       192.168.128.129 53275   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       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       0       -
1692109824.619573       CI4EGw1p6uEayGHwH8      192.168.128.129 48442   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
1692109824.619703       Ck6dIWVRTpOCMKcX7       192.168.128.129 35050   192.168.128.1   53      udp     -       -       -       -       OTH     T       T       0       C       0       0       0       0       -
```

Ubuntu 22.04 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player

Activities Firefox Web Browser Aug 17 23:17

localhost:9200/ | Add integration - Zeek Lo | Issues · elastic/fleet-serv | Elastic Agent 7.17.12 | El

localhost:5601/app/fleet/integrations/zeek-1.8.0/add-integration

elastic Search Elastic

D 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

26° Search ENG IN 23:17 17-08-2023

Ubuntu 22.04 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player

Activities Firefox Web Browser Aug 17 23:17

localhost:9200/ | Add integration - Zeek Lo | Issues · elastic/fleet-serv | Elastic Agent 7.17.12 | El

localhost:5601/app/fleet/integrations/zeek-1.8.0/add-integration

elastic Search Elastic

D 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

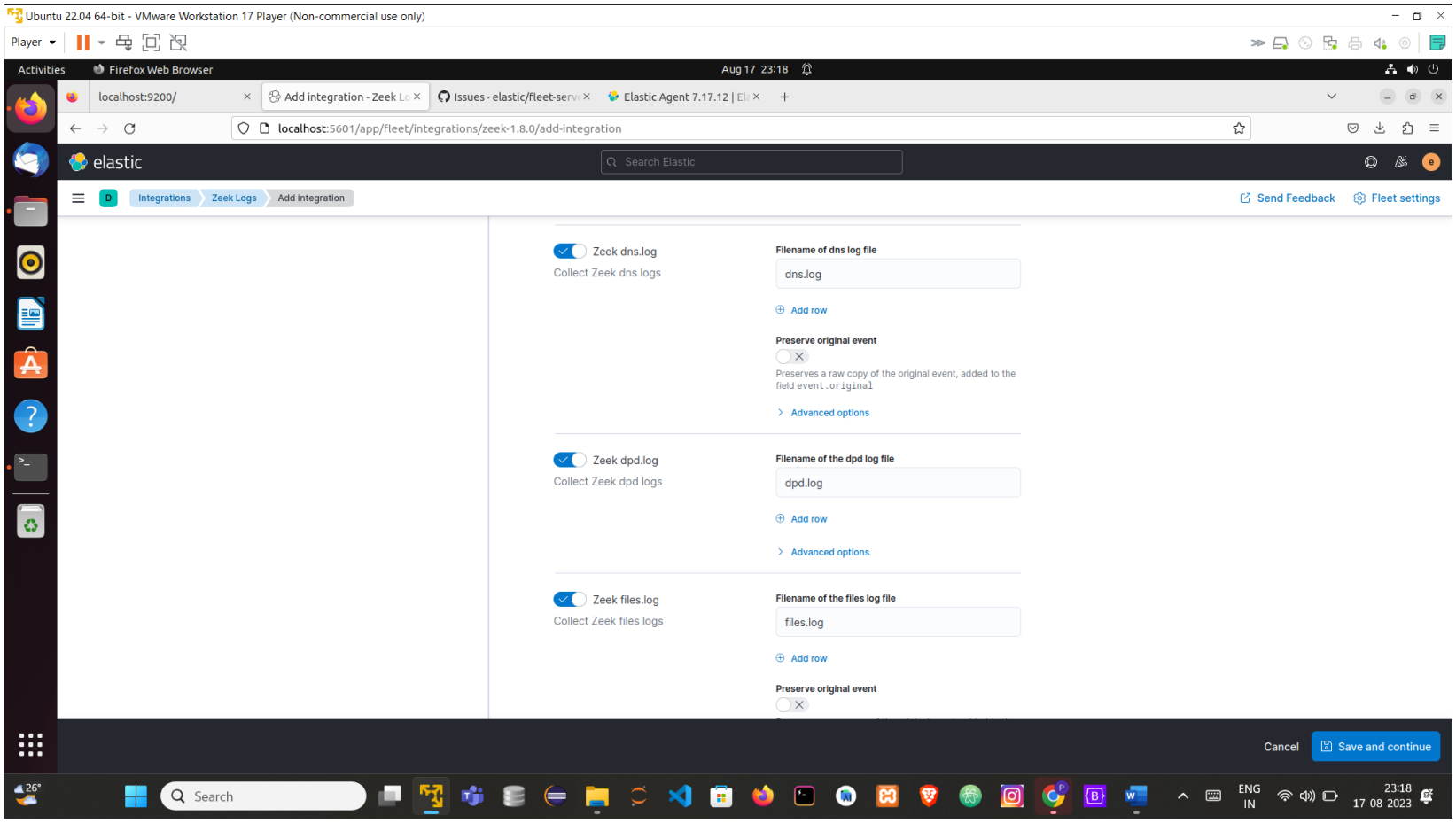
Filename of dnp3 log file

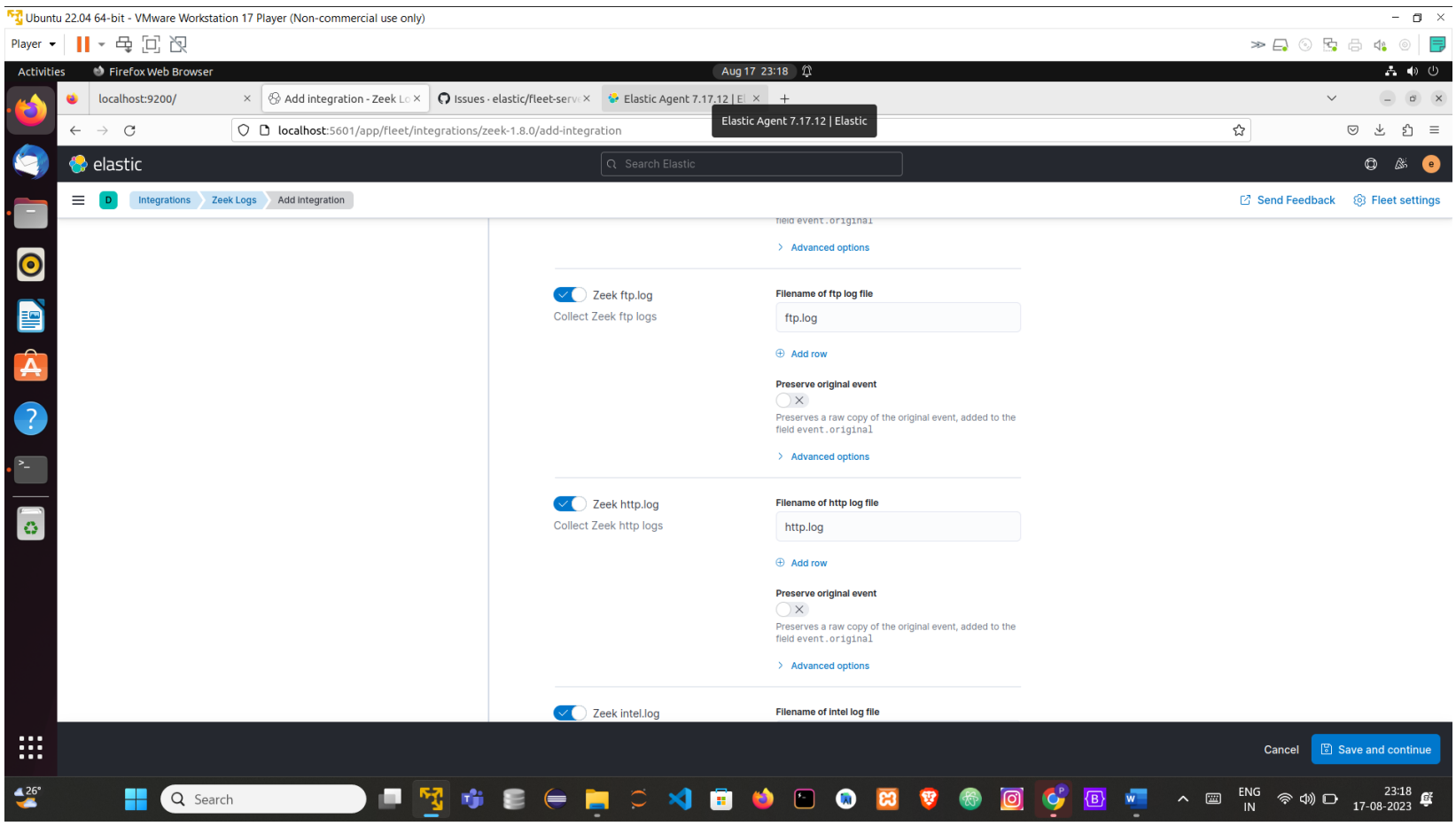
dnp3.log

Add row

Cancel Save and continue

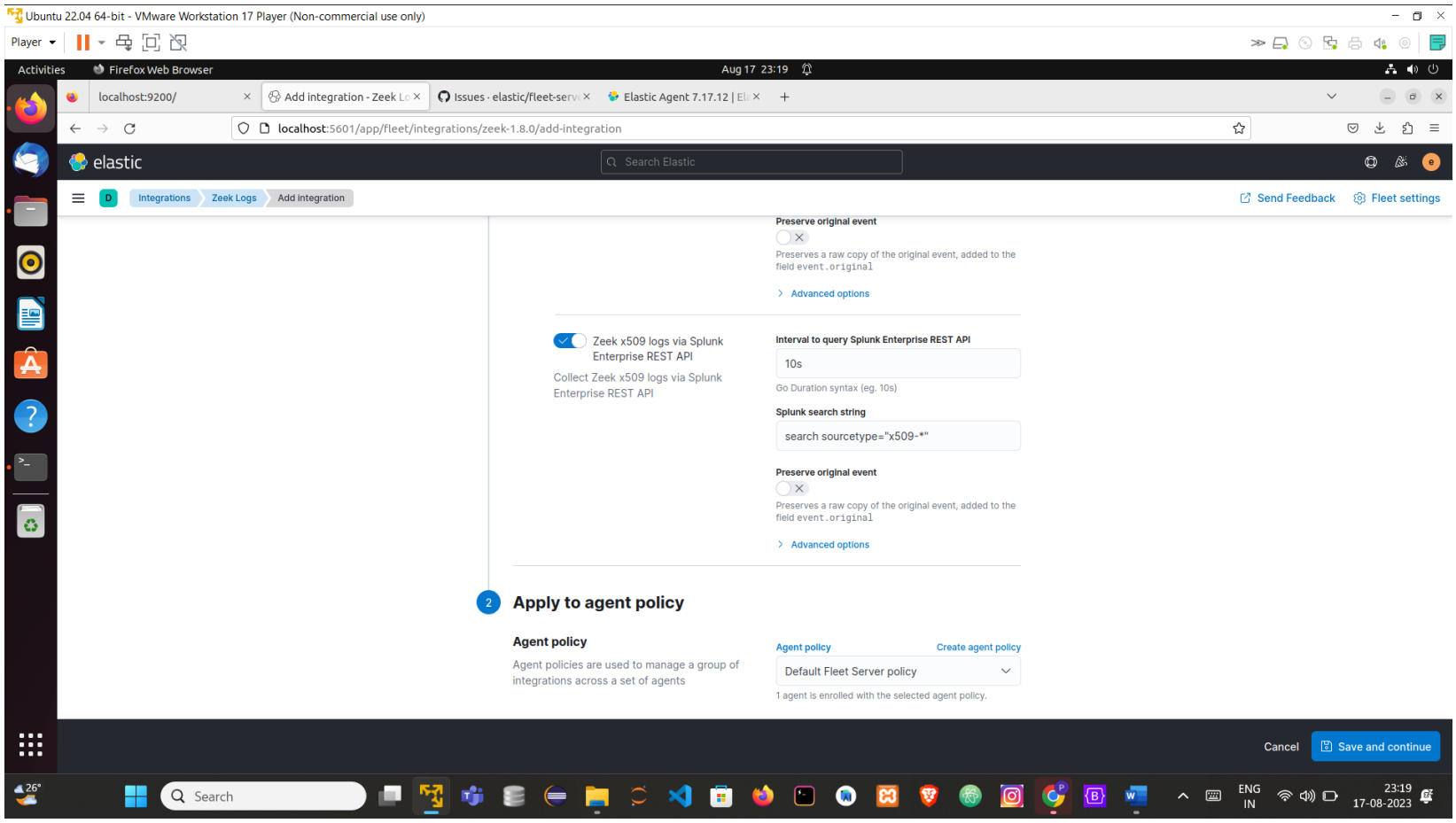
26° Search ENG IN 23:17 17-08-2023

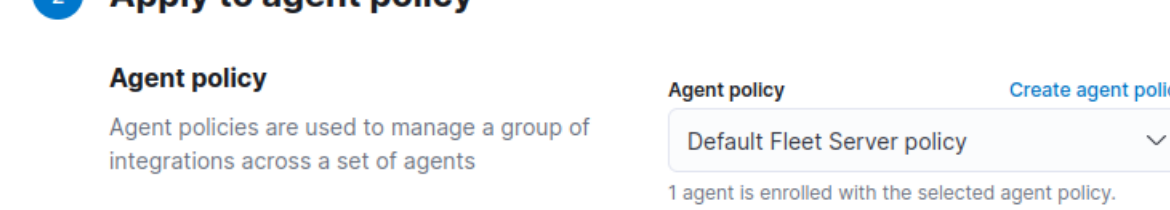




Leave all by default

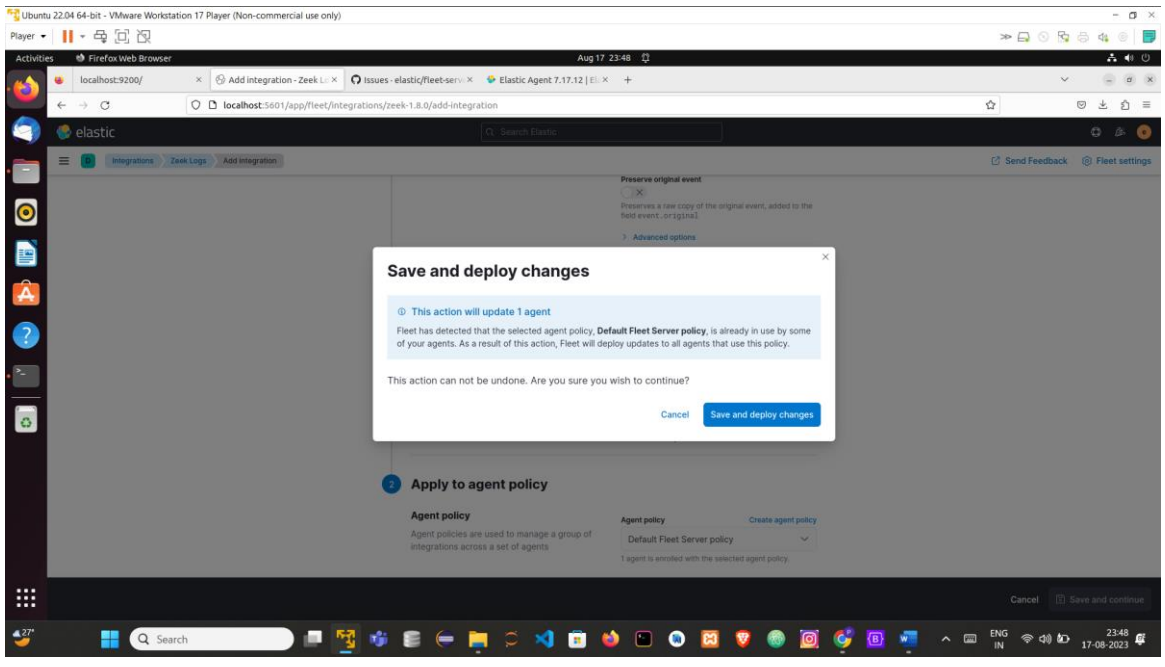
Change Agent policy to Default fleet Server policy



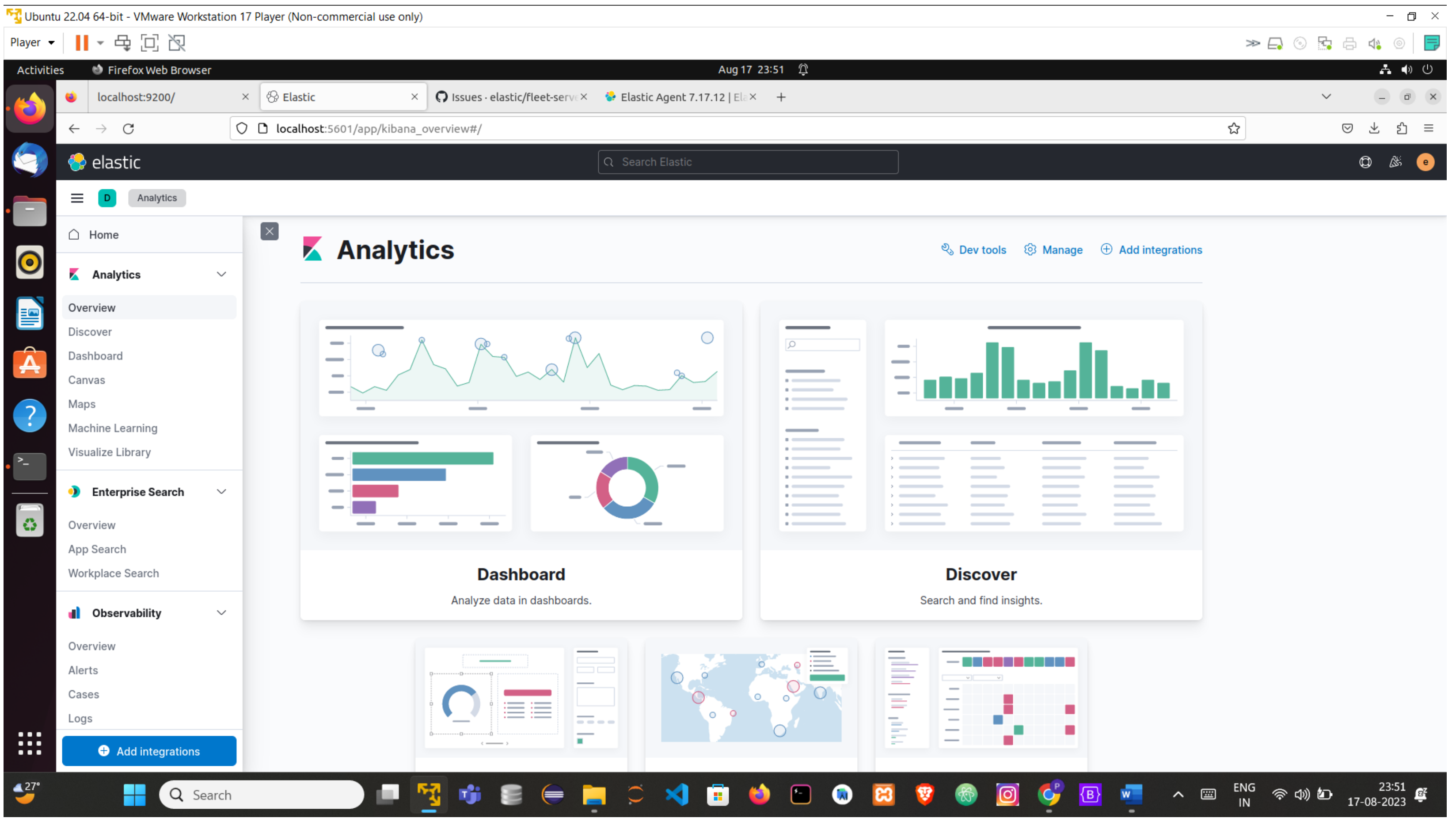


Make sure the 1 agent is enrolled with the selected policy

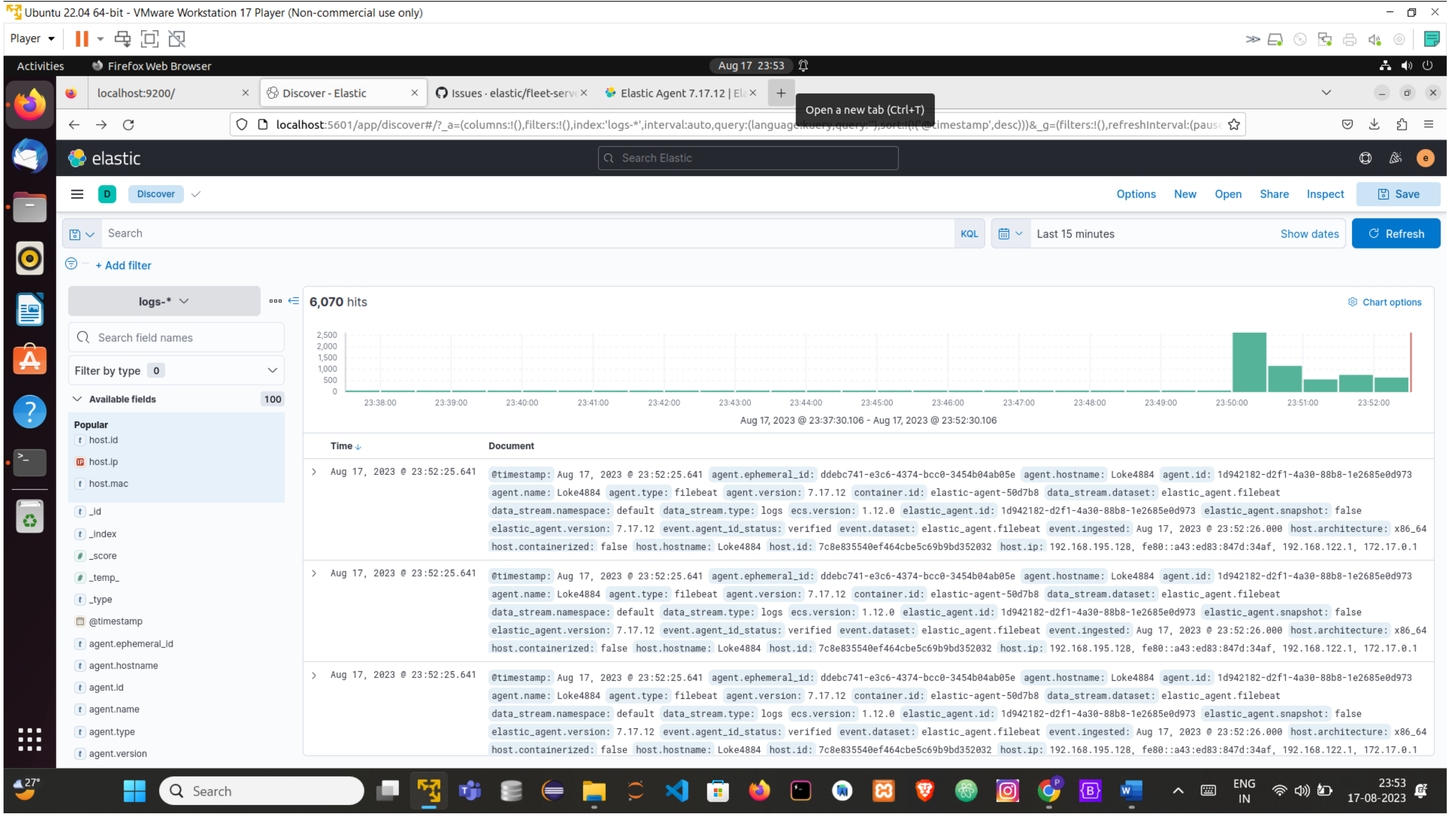
Click on save and deploy changes

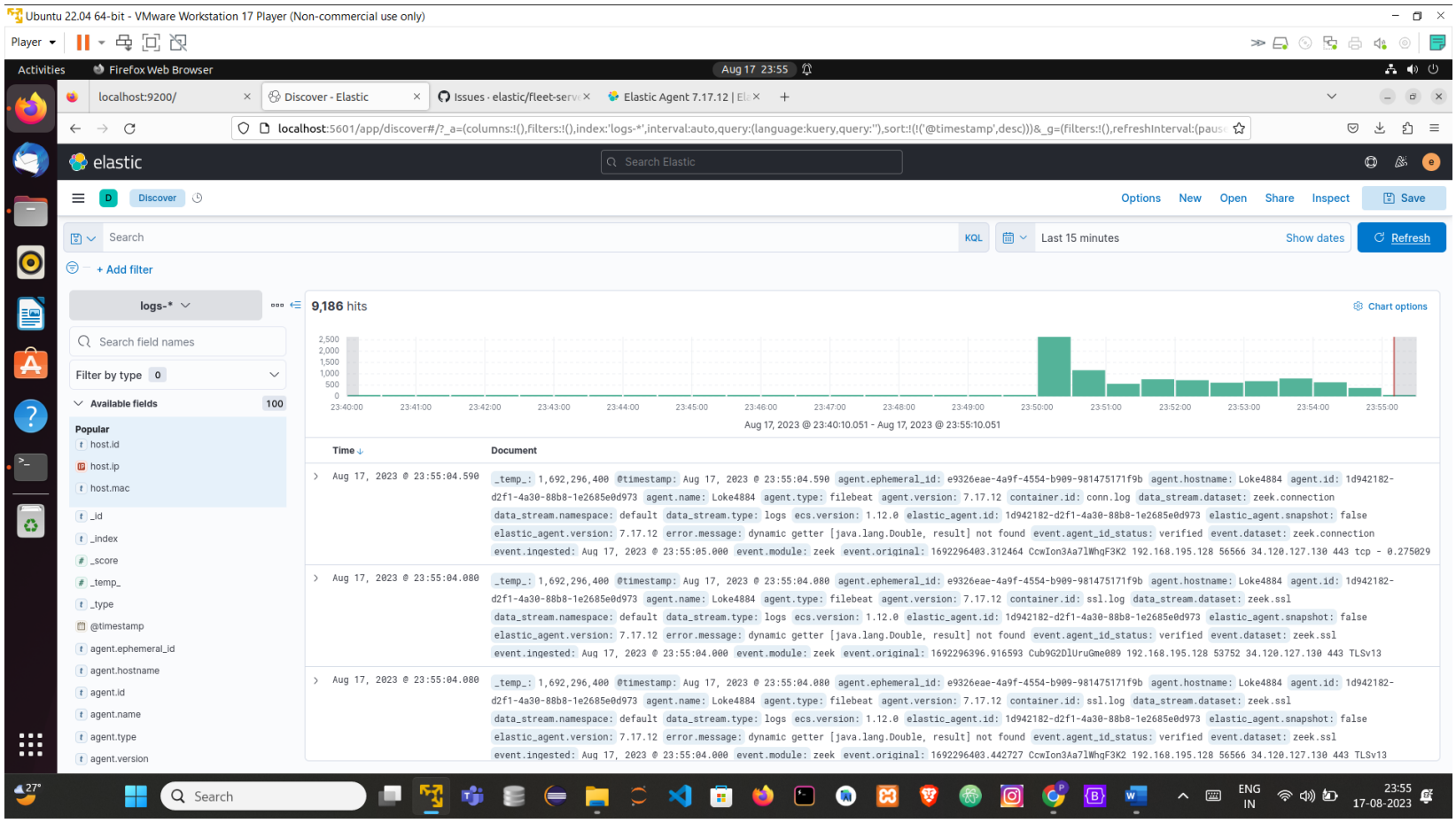


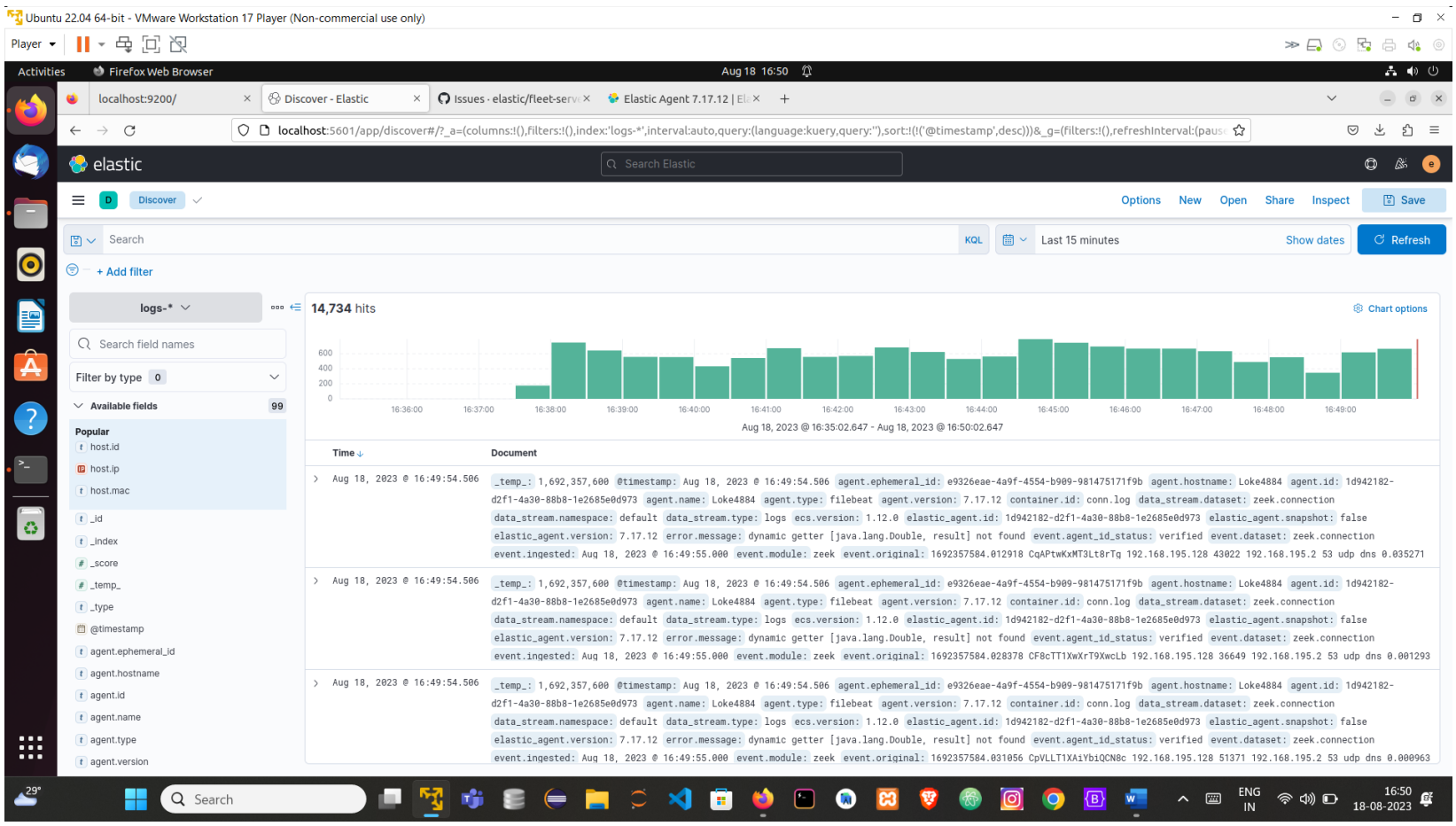
Go to Discover



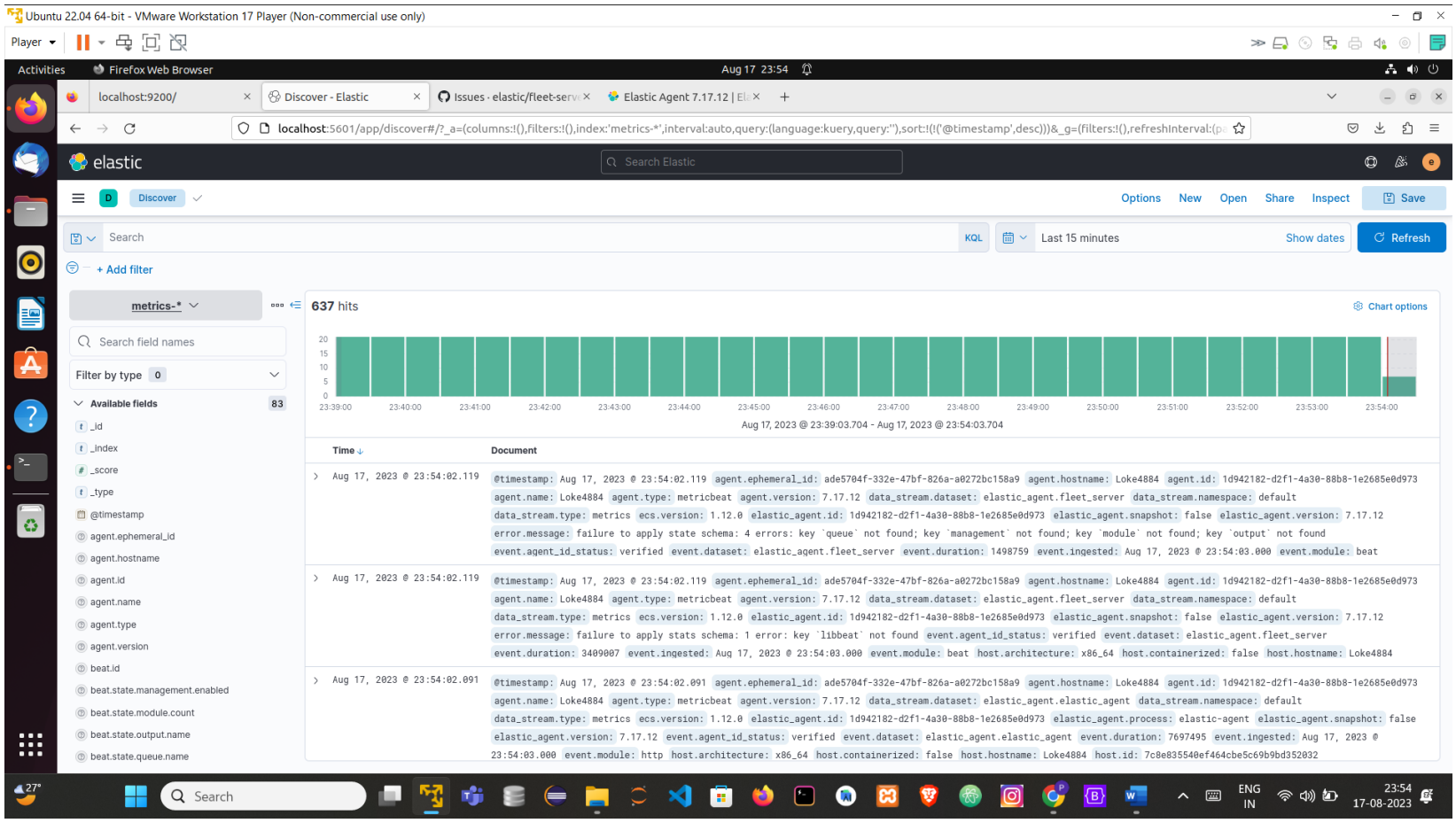
In logs

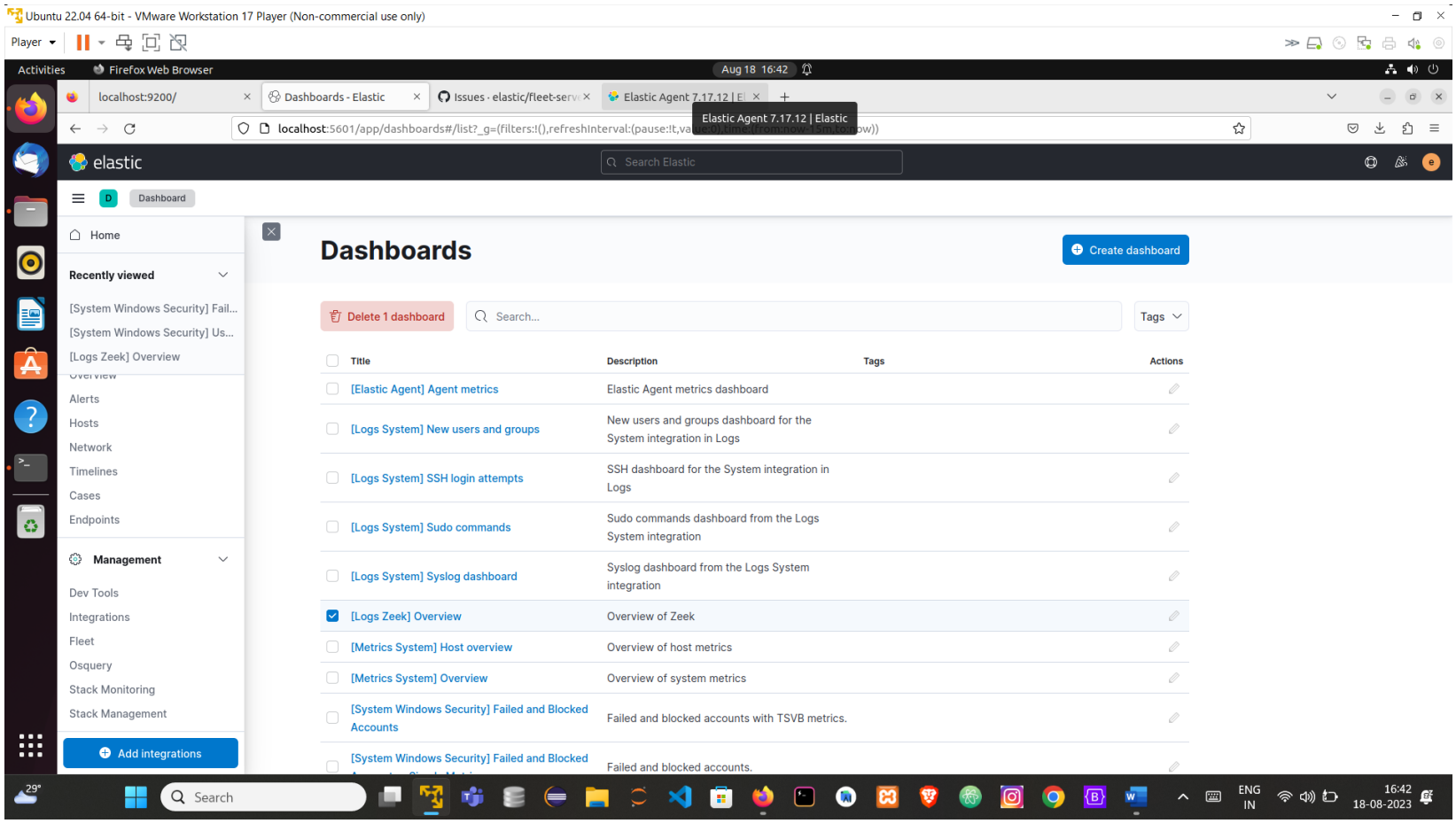



Ubuntu 22.04 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Firefox Web Browser
Aug 17 23:55
localhost:9200/
Discover - Elastic
Issues · elastic/fleet-serv
Elastic Agent 7.17.12 | El
localhost:5601/app/discover#/?_a=(columns:!(),filters:!(),index:'logs-*',interval:auto,query:(language:kuery,query:''),sort:!(!('@timestamp',desc)))&_g=(filters:!(),refreshInterval:(paus
elastic
Search Elastic
Discover
Options
New
Open
Share
Inspect
Save
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
logs-*
9,186 hits
Chart options
Search field names
Filter by type 0
Available fields 100
Popular
host.id
host.ip
host.mac
_id
_index
_score
temp
_type
@timestamp
agent.ephemeral_id
agent.hostname
agent.id
agent.name
agent.type
agent.version
2,500
2,000
1,500
1,000
500
0
23:40:00
23:41:00
23:42:00
23:43:00
23:44:00
23:45:00
23:46:00
23:47:00
23:48:00
23:49:00
23:50:00
23:51:00
23:52:00
23:53:00
23:54:00
23:55:00
Aug 17, 2023 @ 23:40:10.051 - Aug 17, 2023 @ 23:55:10.051
Time
Document
Aug 17, 2023 @ 23:55:04.590
temp: 1,692,296,400 @timestamp: Aug 17, 2023 @ 23:55:04.590 agent.ephemeral_id: e9326eae-4a9f-4554-b909-981475171f9b agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 container.id: conn.log data_stream.dataset: zeek.connection data_stream.namespace: default data_stream.type: logs ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false elastic_agent.version: 7.17.12 error.message: dynamic getter [java.lang.Double, result] not found event.agent_id_status: verified event.dataset: zeek.connection event.ingested: Aug 17, 2023 @ 23:55:05.000 event.module: zeek event.original: 1692296403.312464 CcwIon3Aa7lWhqF3K2 192.168.195.128 56566 34.120.127.130 443 tcp - 0.275029
Aug 17, 2023 @ 23:55:04.080
temp: 1,692,296,400 @timestamp: Aug 17, 2023 @ 23:55:04.080 agent.ephemeral_id: e9326eae-4a9f-4554-b909-981475171f9b agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 container.id: ssl.log data_stream.dataset: zeek.ssl data_stream.namespace: default data_stream.type: logs ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false elastic_agent.version: 7.17.12 error.message: dynamic getter [java.lang.Double, result] not found event.agent_id_status: verified event.dataset: zeek.ssl event.ingested: Aug 17, 2023 @ 23:55:04.000 event.module: zeek event.original: 1692296396.916593 Cub9G2DlUruGme089 192.168.195.128 53752 34.120.127.130 443 TLSv13
Aug 17, 2023 @ 23:55:04.080
temp: 1,692,296,400 @timestamp: Aug 17, 2023 @ 23:55:04.080 agent.ephemeral_id: e9326eae-4a9f-4554-b909-981475171f9b agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 container.id: ssl.log data_stream.dataset: zeek.ssl data_stream.namespace: default data_stream.type: logs ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false elastic_agent.version: 7.17.12 error.message: dynamic getter [java.lang.Double, result] not found event.agent_id_status: verified event.dataset: zeek.ssl event.ingested: Aug 17, 2023 @ 23:55:04.000 event.module: zeek event.original: 1692296403.442727 CcwIon3Aa7lWhqF3K2 192.168.195.128 56566 34.120.127.130 443 TLSv13
27°
Search
ENG
IN
23:55
17-08-2023


Ubuntu 22.04 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Firefox Web Browser
Aug 18 16:50
localhost:9200/
Discover - Elastic
Issues · elastic/fleet-serv
Elastic Agent 7.17.12 | El
localhost:5601/app/discover#/?_a=(columns:!(),filters:!(),index:'logs-*',interval:auto,query:(language:kuery,query:''),sort:!(!('@timestamp',desc)))&_g=(filters:!(),refreshInterval:(paus
elastic
Search Elastic
Discover
Options
New
Open
Share
Inspect
Save
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
logs-*
14,734 hits
Chart options
Search field names
Filter by type 0
Available fields 99
Popular
host.id
host.ip
host.mac
_id
_index
_score
temp
_type
@timestamp
agent.ephemeral_id
agent.hostname
agent.id
agent.name
agent.type
agent.version
600
400
200
0
16:36:00
16:37:00
16:38:00
16:39:00
16:40:00
16:41:00
16:42:00
16:43:00
16:44:00
16:45:00
16:46:00
16:47:00
16:48:00
16:49:00
Aug 18, 2023 @ 16:35:02.647 - Aug 18, 2023 @ 16:50:02.647
Time
Document
Aug 18, 2023 @ 16:49:54.506
temp: 1,692,357,600 @timestamp: Aug 18, 2023 @ 16:49:54.506 agent.ephemeral_id: e9326eae-4a9f-4554-b909-981475171f9b agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 container.id: conn.log data_stream.dataset: zeek.connection data_stream.namespace: default data_stream.type: logs ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false elastic_agent.version: 7.17.12 error.message: dynamic getter [java.lang.Double, result] not found event.agent_id_status: verified event.dataset: zeek.connection event.ingested: Aug 18, 2023 @ 16:49:55.000 event.module: zeek event.original: 1692357584.012918 CqAPtwKxMT3Lt8rTq 192.168.195.128 43022 192.168.195.2 53 udp dns 0.035271
Aug 18, 2023 @ 16:49:54.506
temp: 1,692,357,600 @timestamp: Aug 18, 2023 @ 16:49:54.506 agent.ephemeral_id: e9326eae-4a9f-4554-b909-981475171f9b agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 container.id: conn.log data_stream.dataset: zeek.connection data_stream.namespace: default data_stream.type: logs ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false elastic_agent.version: 7.17.12 error.message: dynamic getter [java.lang.Double, result] not found event.agent_id_status: verified event.dataset: zeek.connection event.ingested: Aug 18, 2023 @ 16:49:55.000 event.module: zeek event.original: 1692357584.028378 CF8cTT1XwXrT9XwcLb 192.168.195.128 36649 192.168.195.2 53 udp dns 0.001293
Aug 18, 2023 @ 16:49:54.506
temp: 1,692,357,600 @timestamp: Aug 18, 2023 @ 16:49:54.506 agent.ephemeral_id: e9326eae-4a9f-4554-b909-981475171f9b agent.hostname: Loke4884 agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 agent.name: Loke4884 agent.type: filebeat agent.version: 7.17.12 container.id: conn.log data_stream.dataset: zeek.connection data_stream.namespace: default data_stream.type: logs ecs.version: 1.12.0 elastic_agent.id: 1d942182-d2f1-4a30-88b8-1e2685e0d973 elastic_agent.snapshot: false elastic_agent.version: 7.17.12 error.message: dynamic getter [java.lang.Double, result] not found event.agent_id_status: verified event.dataset: zeek.connection event.ingested: Aug 18, 2023 @ 16:49:55.000 event.module: zeek event.original: 1692357584.031056 CpVLLT1XAiYbiQCN8c 192.168.195.128 51371 192.168.195.2 53 udp dns 0.000963
29°
Search
ENG
IN
16:50
18-08-2023

In metric





Click on Create Visualization

Ubuntu 22.04 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player

Activities Firefox Web Browser Aug 18 16:44

localhost:9200/ | New Dashboard - Elastic | Issues · elastic/fleet-serv | Elastic Agent 7.17.12 | El

localhost:5601/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-15m,to:now))

elastic Search Elastic

D Dashboard Editing New Dashboard Options Share Switch to view mode Save

Search KQL Last 15 minutes Show dates Refresh

+ Add filter

Create visualization All types Add from library

Add your first visualization

Create content that tells a story about your data.

29° Search ENG IN 16:44 18-08-2023

Ubuntu 22.04 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player

Activities Firefox Web Browser Aug 18 21:47

localhost:9200/ | New Dashb | Issues · elasti | Elastic Agent | vitap - Google | sundhar picha | sundhar picha | vitap - Google | armaan malik | Thehackersnews | Thehackersne | Kubernates

sundhar pichai - Google Search

localhost:5601/app/dashboards#/create?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2023-08-18T14:08:06.962Z',to:'2023-08-18T12:00:00.000Z'))

elastic Search Elastic

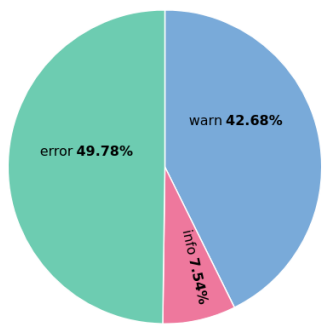
D Dashboard Editing New Dashboard Unsaved changes Options Share Switch to view mode Save

Search KQL Aug 18, 2023 @ 17:08:06.96 → Aug 18, 2023 @ 17:30:00.00 Refresh

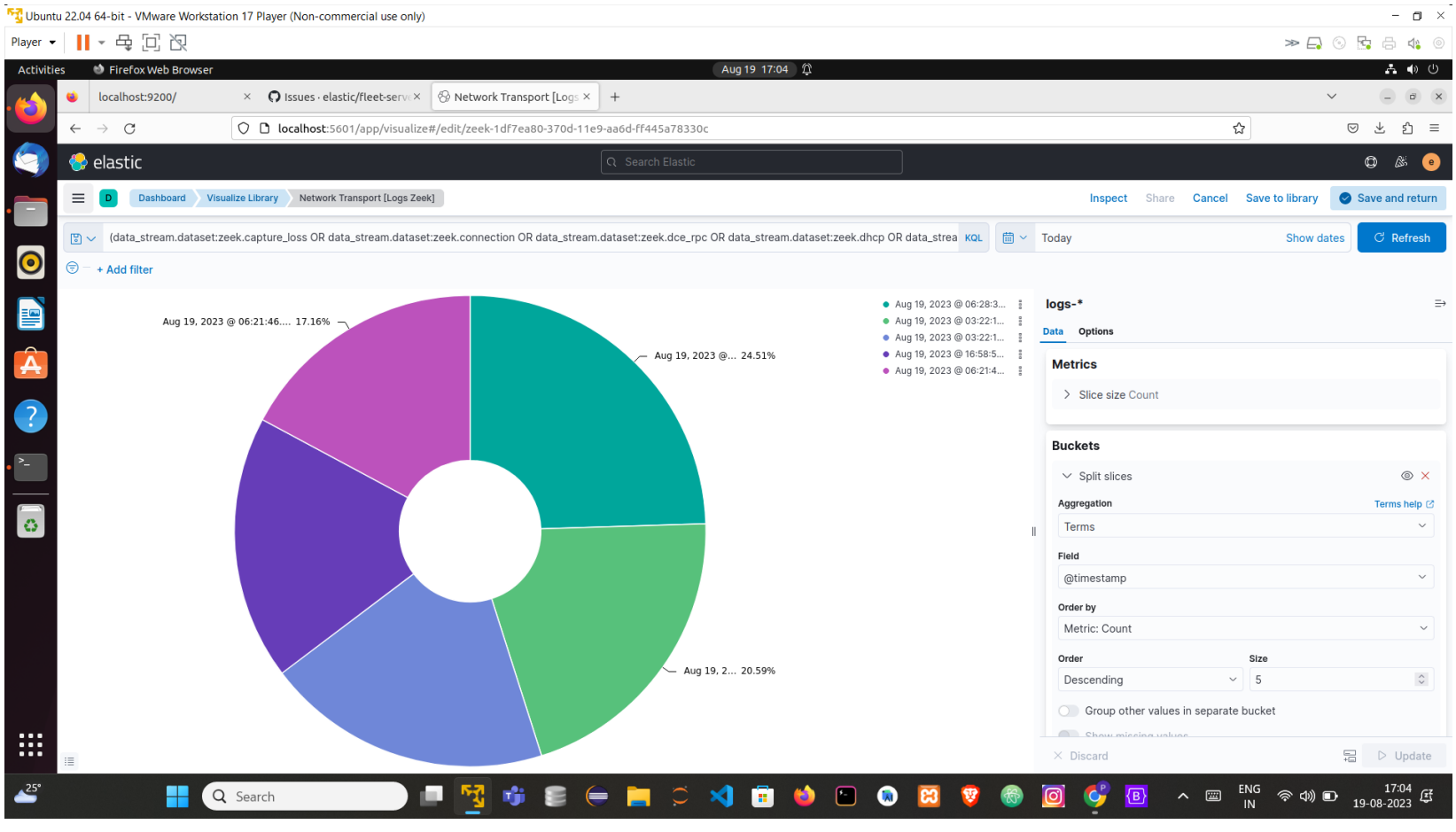
+ Add filter

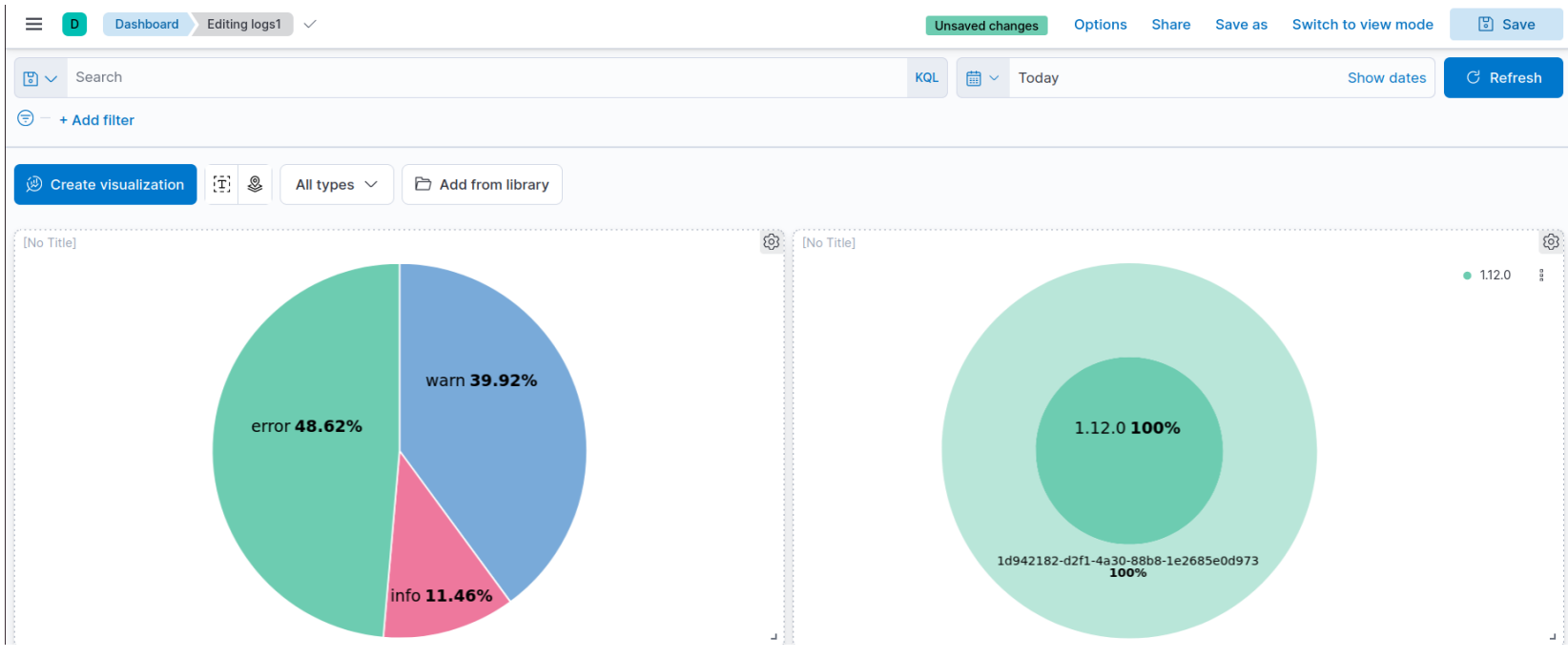
Create visualization All types Add from library

[No Title]



24° Search ENG IN 21:47 18-08-2023


Ubuntu 22.04 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Firefox Web Browser
Aug 19 17:04
localhost:9200/
Issues · elastic/fleet-serv
Network Transport [Logs
localhost:5601/app/visualize#/edit/zeek-1df7ea80-370d-11e9-aa6d-ff445a78330c
elastic
Search Elastic
Dashboard
Visualize Library
Network Transport [Logs Zeek]
Inspect
Share
Cancel
Save to library
Save and return
(data_stream.dataset:zeek.capture_loss OR data_stream.dataset:zeek.connection OR data_stream.dataset:zeek.dce_rpc OR data_stream.dataset:zeek.dhcp OR data_strea
KQL
Today
Show dates
Refresh
+ Add filter
Aug 19, 2023 @ 06:21:46.... 17.16%
Aug 19, 2023 @... 24.51%
Aug 19, 2... 20.59%
Aug 19, 2023 @ 06:28:3...
Aug 19, 2023 @ 03:22:1...
Aug 19, 2023 @ 03:22:1...
Aug 19, 2023 @ 16:58:5...
Aug 19, 2023 @ 06:21:4...
logs-*
Data
Options
Metrics
Slice size Count
Buckets
Split slices
Aggregation
Terms help
Terms
Field
@timestamp
Order by
Metric: Count
Order
Descending
Size
5
Group other values in separate bucket
Discard
Update
Search
ENG
IN
17:04
19-08-2023


Dashboard
Editing logs1
Unsaved changes
Options
Share
Save as
Switch to view mode
Save
Search
KQL
Today
Show dates
Refresh
+ Add filter
Create visualization
All types
Add from library
[No Title]
warn 39.92%
error 48.62%
info 11.46%
[No Title]
1.12.0
1.12.0 100%
1d942182-d2f1-4a30-88b8-1e2685e0d973
100%