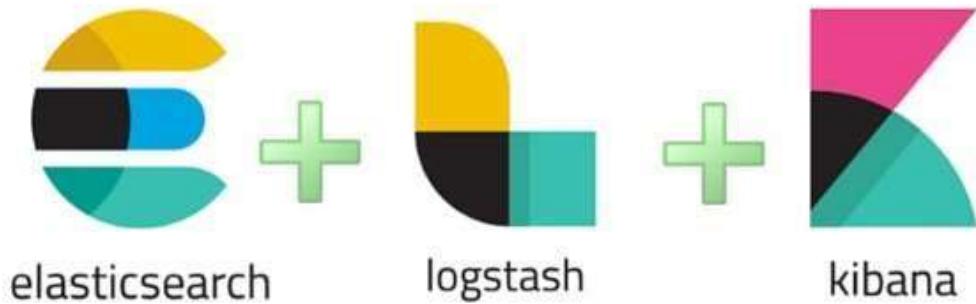


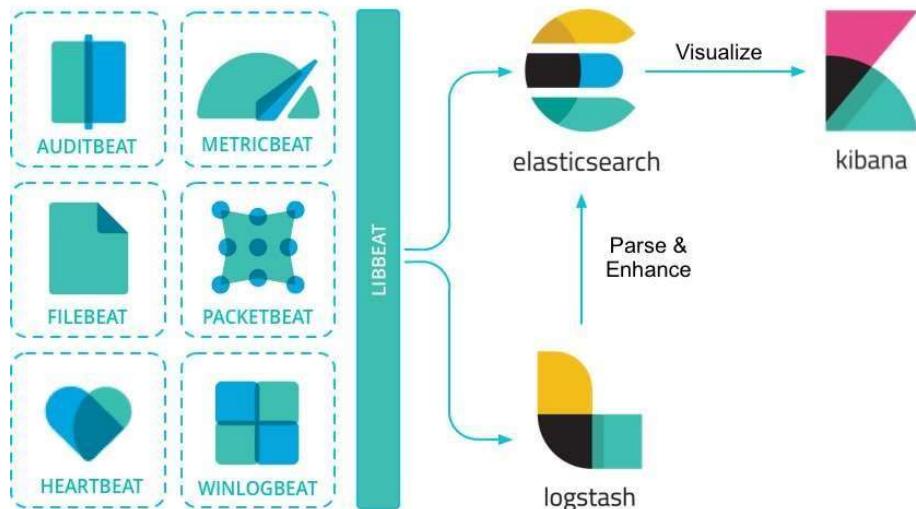
# Deploying ELK Stack

**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-adantage-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 -
```

```
java 11.0.20
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
root@abhi:/home/abhi#
```

---

```
GNU nano 4.8                               /etc/elasticsearch/elasticsearch.yml

# LOCK the Memory on startup:
#bootstrap.memory_lock: true

# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# Elasticsearch performs poorly when the system is swapping the memory.
#
# -----
# Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: localhost
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# -----
# Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
# -----
# Various -----
#
# Require explicit names when deleting indices:
#
#action.destructive_requires_name: true
#
# -----
# Security -----
#
# Get Help   W Write Out   W Where Is   C Cut Text   J Justify   Cur Pos   U Undo   A Mark Text   T To Bracket   Q Previous   B Back
# Exit      R Read File   R Replace   C Paste Text   S To Spell   G Go To Line   R Redo   C Copy Text   W Where Was   N Next   F Forward   P Prev Word   N Next Word
```

**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#
```

```

GNU nano 4.8                                     /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,
## where 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
##
#####

#####
## Expert settings
#####
## All settings below here are considered expert settings. Do
## Get Help   W Write Out   W Where Is   A Cut Text   J Justify   C Cur Pos   M-U Undo
## Exit      W Read File   R Replace    A Paste Text  J To Spell   G Go To Lne  M-E Redo
##                               A-A Mark Text  M-B To Bracket  M-Q Previous  A-B Back
##                               M-C Copy Text  M-D Where Was  M-N Next   A-F Forward  M-P Prev Word
##                               M-O Next Word
[ Wrote 96 lines ]

```

**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

```
t error: [root_cause]: [type: security_exception, reason: missing authentication credentials]
root@abhi:root@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-adantage-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

```

GNU nano 4.8                               /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"

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

^G Get Help   ^Q Write Out  ^W Where Is   ^X Cut Text   ^J Justify   ^C Cur Pos   ^U Undo
^R Read File  ^P Replace    ^V Paste Text  ^T To Spell   ^A Mark Text  ^I To Bracket ^O Previous
^F Find        ^L Go To Line ^M-E Redo    ^G Copy Text  ^O Where Was  ^N Next     ^B Back
^D Delete     ^H Go To Word ^M-A Undo    ^P Paste     ^O Where Was  ^K Next     ^F Forward
^S Save        ^Z Exit      ^M-C Copy   ^M-Z Paste   ^O Where Was  ^L Next     ^P Prev Word
^X Exit        ^M-R Read File ^M-P Replace ^M-V Paste Text ^M-T To Spell ^M-U Undo ^M-G Copy Text ^M-I To Bracket ^M-O Previous ^M-B Back ^M-F Forward ^M-P Prev Word ^M-N Next Word

```

**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

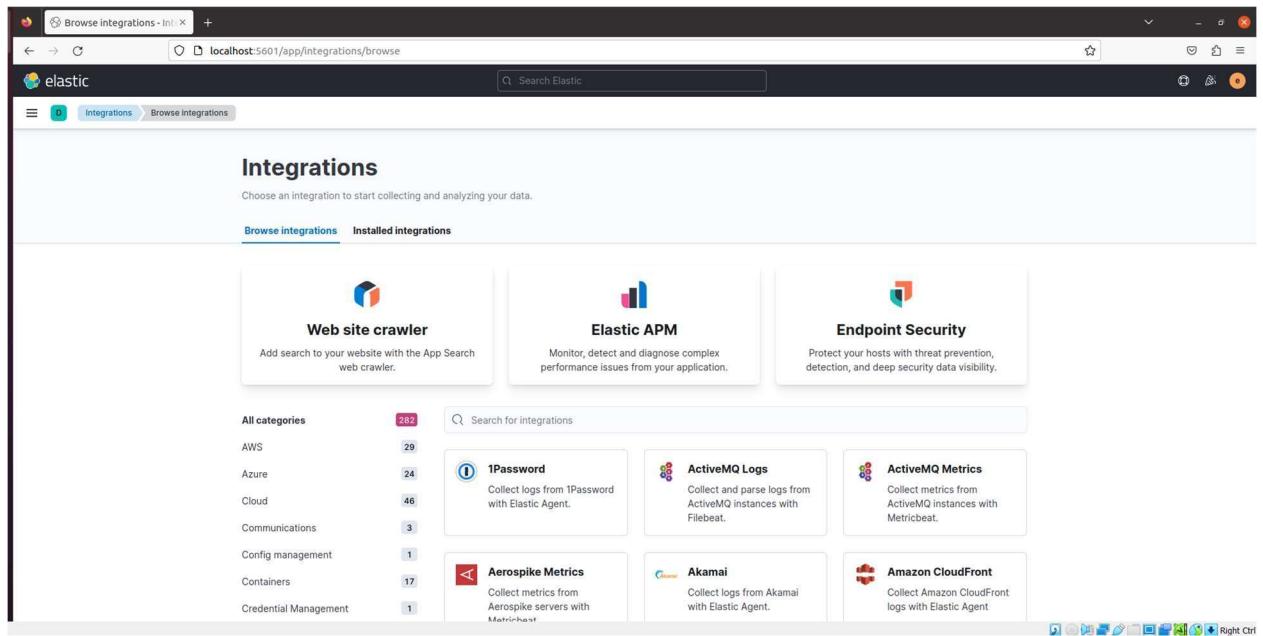
```

root@abhi:/home/abhi# 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 19:46:04 IST; 2h 26min ago
     Docs: https://www.elastic.co
 Main PID: 732 (node)
    Tasks: 11 (limit: 5554)
   Memory: 227.7M
      Group: /system.slice/kibana.service
             └─732 /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_deprecated

Aug 24 19:46:04 abhi systemd[1]: Started Kibana.
lines 1-11/11 (END)

```

**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
```

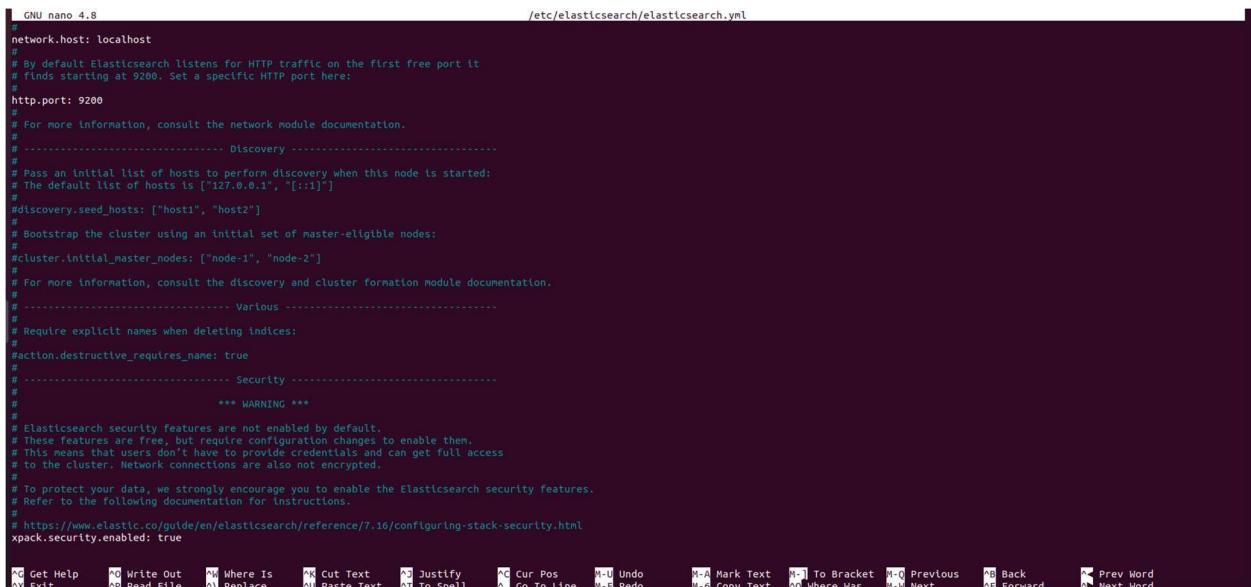
**Step 2:** Stop the Elastic Search by using the below command

```
# sudo systemctl stop elasticsearch
```

**Step 3:** Enable x-pack in Elasticsearch.yml

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

```
add:xpack.security.enabled: true
```



```
GNU nano 4.8                               /etc/elasticsearch/elasticsearch.yml

#network.host: localhost
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
#----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
#discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
#
#cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
#----- Various -----
#
# Require explicit names when deleting indices:
#
#action.destructive_requires_name: true
#
#----- Security -----
#
# *** WARNING ***
#
# Elasticsearch security features are not enabled by default.
# These features are free, but require configuration changes to enable them.
# This means that users don't have to provide credentials and can get full access
# to the cluster. Network connections are also not encrypted.
#
# To protect your data, we strongly encourage you to enable the Elasticsearch security features.
# Refer to the following documentation for instructions.
#
# https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stack-security.html
xpack.security.enabled: true

[Get Help] [Write Out] [Where Is] [Cut Text] [Justify] [Cur Pos] [Undo] [Mark Text] [To Bracket] [Previous] [Back]
[Exit] [Read File] [Replace] [Paste Text] [To Spell] [Go To Line] [Redo] [Copy Text] [Where Was] [Next] [Forward]
[Prev Word] [Next Word]
```

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

```
GNU nano 4.8                               /etc/kibana/kibana.yml

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

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

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

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
elasticsearch.username: "kibana_system"
elasticsearch.password: "MWhlC3Vw4k72xEIwARHF"

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

# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.
# These settings enable SSL for outgoing requests from the Kibana server to the browser.
#server.ssl.enabled: false
#server.ssl.certificate: /path/to/your/server.crt
#server.ssl.key: /path/to/your/server.key

# Optional settings that provide the paths to the PEM-format SSL certificate and key files.
# These files are used to verify the identity of Kibana to Elasticsearch and are required when
# xpack.security.http.ssl.client authentication in Elasticsearch is set to required.
#elasticsearch.ssl.certificate: /path/to/your/client.crt
#elasticsearch.ssl.key: /path/to/your/client.key

# Optional setting that enables you to specify a path to the PEM file for the certificate
# authority for your Elasticsearch instance.
#elasticsearch.ssl.certificateAuthorities: [ "/path/to/your/CA.pem" ]

# To disregard the validity of SSL certificates, change this setting's value to 'none'.
#elasticsearch.ssl.verifyMode: full

# Time in milliseconds to wait for Elasticsearch to respond to pings. Defaults to the value of
# the elasticsearch.requestTimeout setting.
#elasticsearch.pingTimeout: 1500

^D Get Help      ^A Write Out    ^W Where Is     ^X Cut Text      ^Z Justify      ^C Cur Pos      M-U Undo      M-A Mark Text  M-[ To Bracket M-Q Previous  ^B Back
^Q Exit          ^R Read File    ^X Replace      ^U Paste Text    ^T To Spell      ^G Go To Line   M-E Redo      M-G Copy Text M-Q Where Was  M-W Next     ^F Forward
^S Prev Word    ^P Next Word
```

## 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 zlib-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
libfwupdplugin liblxqt ubuntu-adantage-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 gcc-9-base libasan5 libbinutils libc-dev-bin libc6-dev libcrypt-dev libctf-nobfd0 libctf0 libexpat1-dev libfl-dev
libfl2 libgcc-9-dev libitm1 libjsonecppi liblsan libpythont3.8-dev libquadmath0 librhash0 libsigsegv2 libstdc++-9-dev libtsan0 libubsani 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 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-doc
The following NEW packages will be installed:
binutils binutils-common binutils-x86-64-linux-gnu bison cmake cmake-data Flex g++-9 gcc-9-base libasan5 libbinutils libc-dev-bin libc6-dev libcrypt-dev libctf-nobfd0 libctf0
libexpat1-dev libfl libfl2 libgcc-9-dev libitm1 libjsonecppi liblsan libpythont3.8-dev libquadmath0 librhash0 libsigsegv2 libssl-dev libstdc++-9-dev libtsan0 libubsani
linux-libc-dev m4 make manpages-dev python3-dev python3-distutils python3.8-dev swig swig4.0 zlib-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
abhi@abhi:~$ cd Downloads
```

## 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_librresolv
-- Performing Test ns_initparse_works_librresolv.a - Success
-- Performing Test res_mkquery_works_librresolv.a
-- Performing Test res_mkquery_works_librresolv.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 -fthread - 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

The screenshot shows two browser windows. The top window is a Firefox session titled 'Elastic' with the URL 'localhost:5601/login?next=%2F'. It displays a 'Welcome to Elastic' page with a login form. The form has 'Username' set to 'elastic' and 'Password' obscured by dots. A 'Log in' button is at the bottom. The bottom window is also titled 'Elastic' with the URL 'localhost:5601/app/home#/'. It shows a 'Welcome home' dashboard with four main sections: 'Enterprise Search' (yellow), 'Observability' (pink), 'Security' (teal), and 'Analytics' (blue). Each section has a small icon and a brief description. Below the dashboard is a 'Get started by adding integrations' section with three buttons: '+ Add integrations', 'Try sample data', and 'Upload a file'. To the right of this text is a colorful illustration of data flowing through various components.

Go to management → Fleet

The screenshot shows a browser window titled 'localhost:5601/app/fleet/agents'. The title bar includes the Elastic logo and tabs for 'Fleet' and 'Agents'. The main content area is titled 'Fleet' with the subtitle 'Centralized management for Elastic Agents.' Below this is a navigation bar with links for 'Agents', 'Agent policies', 'Enrollment tokens', and 'Data streams'. At the bottom of the page is a large blue button labeled 'Add a Fleet Server'.

## Click on add agent

The screenshot shows the Fleet interface on a web browser. The main navigation bar has 'Fleet' selected. Below it, there are tabs for 'Agents', 'Agent policies', 'Enrollment tokens', and 'Data streams'. A modal window titled 'Add agent' is open. At the top of the modal, it says 'Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.' There are two tabs: 'Enroll in Fleet' (selected) and 'Run standalone'. Below this, a note says 'Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.' The main content area is divided into three numbered steps:

- 1 Choose an agent policy**  
A dropdown menu shows 'Agent policy' and 'Default policy'. A note below says 'The selected agent policy will collect data for 1 integration: System'.
- 2 Download the Elastic Agent to your host**  
A note says 'Install the Elastic Agent on the hosts you wish to monitor. Do not install this agent policy on a host containing Fleet Server. You can download the Elastic Agent binaries and verification signatures from Elastic's download page.' It also notes 'Linux users: We recommend the installer (TAR) over system packages (RPM/DEB)' and 'Windows users: We recommend the installer (TAR) over system packages (RPM/DEB)'.
- 3 Choose a deployment mode for security**  
A note says '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.'

At the bottom right of the modal is a 'Close' button, and at the bottom right of the browser window are various icons.

Enroll Fleet section →

Download Fleet Server to centralized host

This screenshot is similar to the previous one but with a key difference: the 'Run standalone' tab is now selected instead of 'Enroll in Fleet'. The rest of the content and steps remain the same, detailing the process of choosing an agent policy, downloading the agent, and selecting a deployment mode for security.

Click on download page

The screenshot shows the 'Elastic Agent 7.17.12' download page. At the top, there is a navigation bar with links for 'Platform', 'Solutions', 'Customers', 'Resources', 'Pricing', 'Docs', and user icons for 'Start Free Trial' and 'Contact Sales'. Below this is a large heading 'Elastic Agent 7.17.12'. Underneath the heading, there is a list of download links for different operating systems and architectures, each with a corresponding 'sha' link for the checksum:

- LINUX 64-BIT [sha](#)
- LINUX AARCH64 [sha](#)
- DEB 64-BIT [sha](#)
- DEB AARCH64 [sha](#)
- RPM 64-BIT [sha](#)
- RPM AARCH64 [sha](#)
- WINDOWS 64-BIT [sha](#)
- MAC [sha](#)

### 3 Choose a deployment mode for security

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

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

### 4 Add your Fleet Server host

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

Fleet Server host 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

AAEAAWVsYXN0aWMvZmx1ZXQtc2VydmyL3Rva2VuLTE20TI5MDc4NzkyMTU6Q1NIT1AtaE9UWUNvQzZLRHYxekR5QQ



## Fleet sever connected

AAEAAWVsYXN0aWMvZmx1ZXQtc2VydmyL3Rva2VuLTE20TI5MDc4NzkyMTU6Q1NIT1AtaE9UWUNvQzZLRHYxekR5QQ



### 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=AAEAAWVsYXN0aWMvZmx1ZXQtc2VydmyL3Rva2VuLTE20TI5MDc4NzkyMTU6Q1NIT1AtaE9UWUNvQzZLRHYxekR5QQ \
--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

### Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Data streams

Search		Status	Agent policy	Upgrade available	Add agent
Showing 1 agent					
Host	Status	Agent policy	Version	Last activity	Actions
abhi	Healthy	Default Fleet Server policy rev. 3	7.17.12	20 seconds ago	...
Rows per page: 20 < 1 >					

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 ▾

Opensearch 2.9.0 - Open Add integration - Zeek Log +

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

elastic Search Elastic

Send Feedback Fleet settings

Integrations Zeek Logs Add integration

Collect Zeek logs

Settings Base Path /opt/zeek/logs/current

The following settings are applicable to all inputs below.

① Add row Base paths to zeek log files (e.g. /var/log/bro/current)

Zeek capture\_loss.log Collect Zeek capture\_loss logs

Filename of capture loss log file capture\_loss.log

② Add now

Preserve original event

Preserves a raw copy of the original event, added to the field event.event.original

③ Advanced options

Zeek conn.log Collect Zeek connection logs

Filename of connection log conn.log

④ Add now

Preserve original event

Cancel Save and continue

Activities Firefox Web Browser ▾

Opensearch 2.9.0 - Open Add integration - Zeek Log +

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

elastic Search Elastic

Send Feedback Fleet settings

Integrations Zeek Logs Add integration

field event.event.original

④ Advanced options

Zeek dce\_rpc.log Collect Zeek dce\_rpc logs

Filename of dce\_rpc log file dce\_rpc.log

⑤ Add now

Preserve original event

Preserves a raw copy of the original event, added to the field event.event.original

⑥ Advanced options

Zeek dhcp.log Collect Zeek dhcp logs

Filename of dhcp log file dhcp.log

⑦ Add now

⑧ Advanced options

Zeek dnp3.log Collect Zeek dnp3 logs

Filename of dnp3 log file dnp3.log

⑨ Add now

Cancel Save and continue

Activities Firefox Web Browser ▾

Opensearch 2.9.0 - Open Add integration - Zeek Log +

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

elastic Search Elastic

Send Feedback Fleet settings

Integrations Zeek Logs Add integration

Zeek dns.log Collect Zeek dns logs

Filename of dns log file dns.log

⑩ Add now

Preserve original event

Preserves a raw copy of the original event, added to the field event.event.original

⑪ Advanced options

Zeek dpd.log Collect Zeek dpd logs

Filename of the dpd log file dpd.log

⑫ Add now

⑬ Advanced options

Zeek files.log Collect Zeek files logs

Filename of the files log file files.log

⑭ Add now

Preserve original event

Cancel Save and continue

The screenshot shows the 'Add integration - Zeek Logs' configuration page. It lists three log types: 'Zeek ftp.log', 'Zeek http.log', and 'Zeek intel.log'. Each entry includes a 'Filename of log file' field (set to 'ftp.log', 'http.log', and 'intel.log' respectively) and a 'Preserve original event' checkbox. Below each entry is a 'Save and continue' button.

Leave all by default

## Change Agent policy to Default fleet Server policy

The screenshot shows the 'Configure integration' step of the 'Add integration - Zeek Logs' process. It includes sections for 'Integration settings' (with 'Integration name' set to 'zeek-2') and 'Agent policy' (with 'Default Fleet Server policy' selected). A 'Save and continue' button is at the bottom right.

Make sure the 1 agent is enrolled with the selected policy

The screenshot shows the 'Zeek Logs' integration details page. It displays the 'Integration policies' tab, which shows one policy named 'zeek' assigned to version 1.8.0. The 'Agent policies' section shows 2 policies assigned to 1 agent. A 'Save and continue' button is at the bottom right.

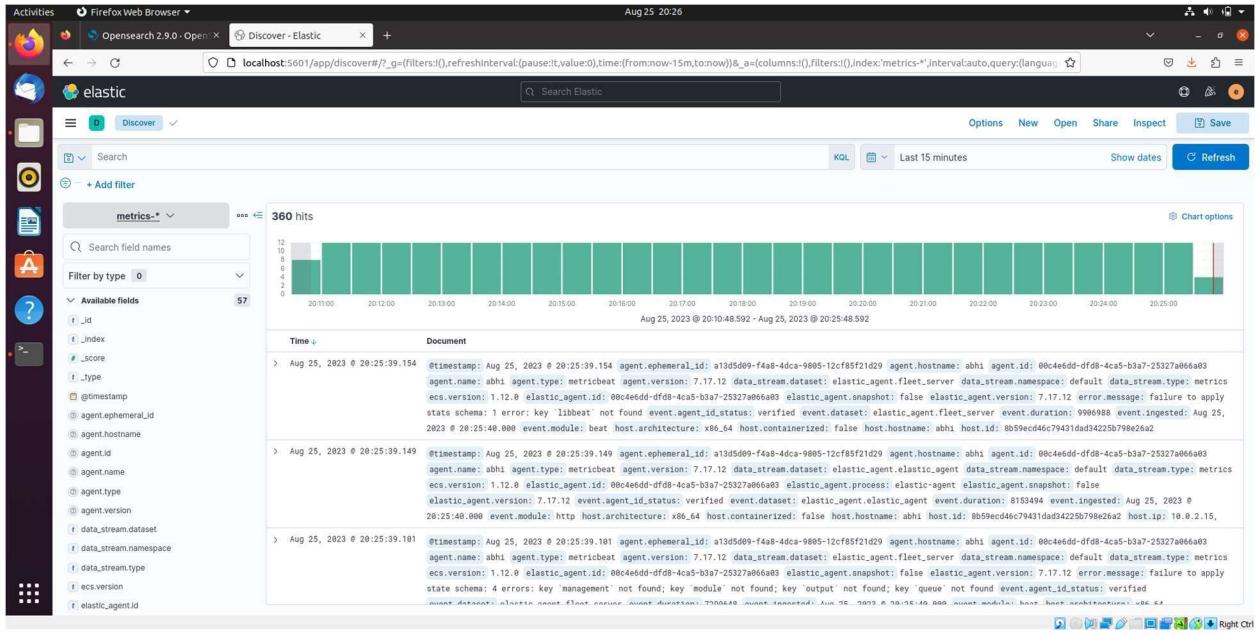
## Go to Discover

The screenshot shows the Kibana Analytics interface. On the left, a sidebar navigation includes sections like Overview, Discover, Dashboard, Canvas, Maps, Machine Learning, Visualize Library, Enterprise Search, Observability, and a section for Add integrations. The main area features two main sections: 'Dashboard' and 'Discover'. The 'Dashboard' section contains a line chart, a bar chart, and a donut chart. The 'Discover' section contains a histogram and a list of search results. At the top right, there are links for Dev tools, Manage, and Add integrations.

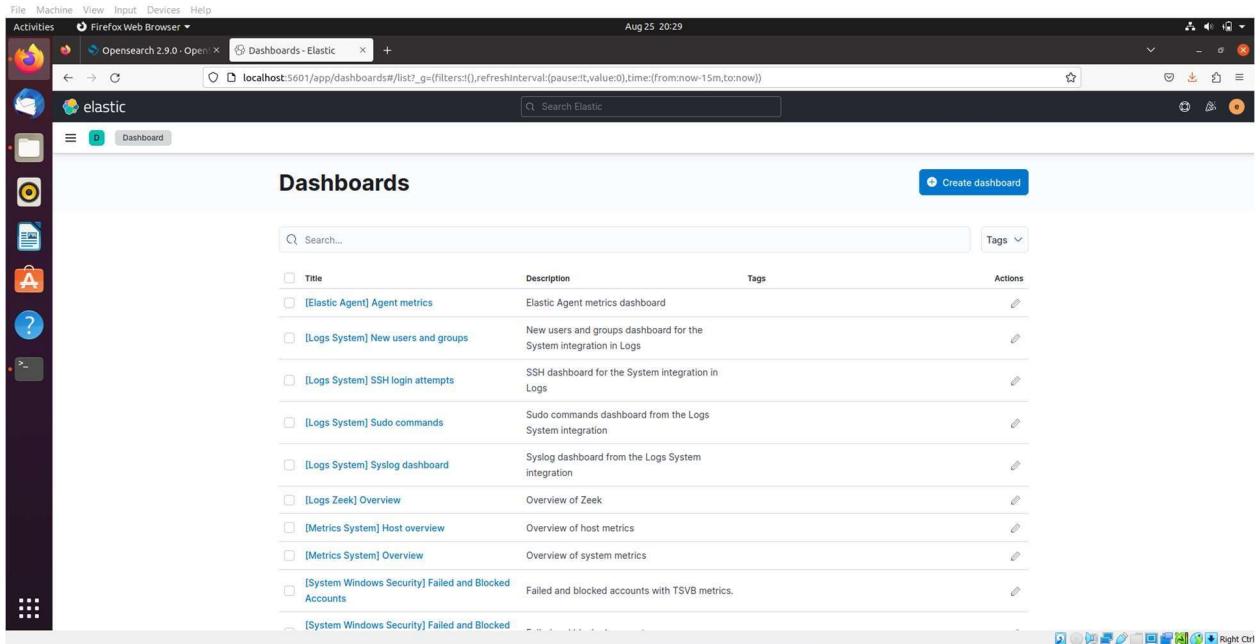
## In logs

The screenshot shows the Kibana Discover interface. The top navigation bar includes links for Options, New, Open, Share, Inspect, Save, Last 15 minutes, Show dates, Refresh, and a KQL button. The main search bar has a placeholder 'Search field names' and a 'Filter by type' dropdown set to 'logs-\*'. Below the search bar, a table displays search results with columns for 'Time' and 'Document'. The table shows three log entries from August 25, 2023, at 20:04:42.370, 20:04:42.273, and 20:03:37.029. Each entry includes detailed log data such as timestamp, agent ID, host information, and event details. A sidebar on the left lists available fields including \_id, \_index, \_score, \_type, @timestamp, @agent.ephemeral\_id, @agent.hostname, @agent.id, @agent.name, @agent.type, @agent.version, @coordinator\_idx, @ctx, @data\_stream.dataset, @data\_stream.namespace, and @data\_stream.type. A 'Chart options' button is located at the top right of the results table.

## In metrics



## Dashboard



## Click on Create Visualization

