PROJECT : Zeek logs to ELK

Name : Vaishnavi Madhav Shinde

Roll No : MH-JM-24-07-0103

Course : Cyber Security Specialist

Guided By : Deepyesh Sir.

Zeek logs to ELK

Zeek (formerly Bro) is a powerful network analysis tool that generates detailed logs of network activity. ELK (Elasticsearch, Logstash, and Kibana) is a stack used for searching, analyzing, and visualizing log data.

Zeek Logs to ELK Workflow:

1. **Zeek Captures Traffic** → Zeek monitors network traffic and generates logs (e.g., conn.log, http.log, dns.log).

2. **Filebeat Collects Logs** → Filebeat (a lightweight log shipper) reads Zeek logs and sends them to Logstash or directly to Elasticsearch.

3. **Logstash Parses Logs** → If needed, Logstash processes and enriches the logs before forwarding them to Elasticsearch.

4. **Elasticsearch Stores Logs** → Elasticsearch indexes the logs for fast searching and analysis.

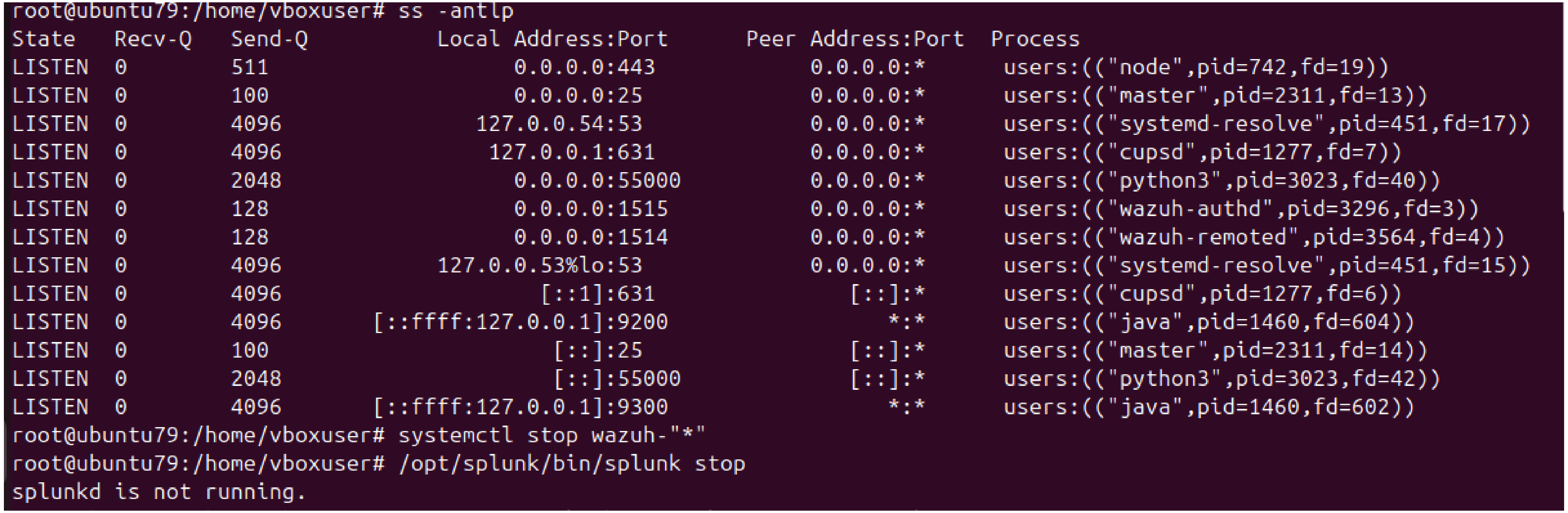
5. **Kibana Visualizes Data** → Kibana provides dashboards and search tools to analyze Zeek logs.

Let’s start commands in 1st ubuntu

>ss –antlp

>systemctl stop wazuh-”*”

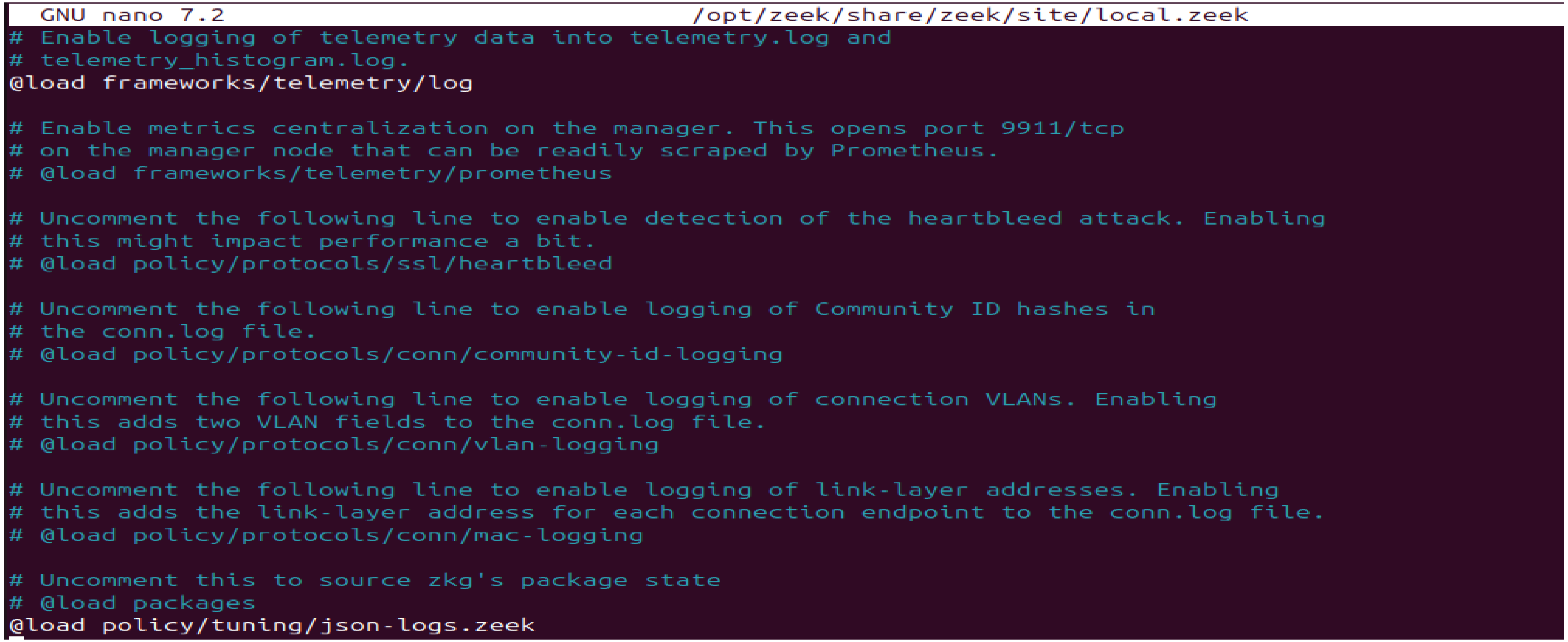
>/opt/splunk/bin/splunk stop



```
root@ubuntu79:/home/vboxuser# ss -antlp
State   Recv-Q   Send-Q          Local Address:Port      Peer Address:Port  Process
LISTEN  0        511                   0.0.0.0:443            0.0.0.0:*      users:(("node",pid=742,fd=19))
LISTEN  0        100                   0.0.0.0:25             0.0.0.0:*      users:(("master",pid=2311,fd=13))
LISTEN  0        4096               127.0.0.54:53             0.0.0.0:*      users:(("systemd-resolve",pid=451,fd=17))
LISTEN  0        4096                127.0.0.1:631            0.0.0.0:*      users:(("cupsd",pid=1277,fd=7))
LISTEN  0        2048                  0.0.0.0:55000          0.0.0.0:*      users:(("python3",pid=3023,fd=40))
LISTEN  0        128                   0.0.0.0:1515           0.0.0.0:*      users:(("wazuh-authd",pid=3296,fd=3))
LISTEN  0        128                   0.0.0.0:1514           0.0.0.0:*      users:(("wazuh-remoted",pid=3564,fd=4))
LISTEN  0        4096          127.0.0.53%lo:53               0.0.0.0:*      users:(("systemd-resolve",pid=451,fd=15))
LISTEN  0        4096                    [::1]:631               [::]:*      users:(("cupsd",pid=1277,fd=6))
LISTEN  0        4096       [::ffff:127.0.0.1]:9200                 *:*      users:(("java",pid=1460,fd=604))
LISTEN  0        100                      [::]:25                [::]:*      users:(("master",pid=2311,fd=14))
LISTEN  0        2048                     [::]:55000             [::]:*      users:(("python3",pid=3023,fd=42))
LISTEN  0        4096       [::ffff:127.0.0.1]:9300                 *:*      users:(("java",pid=1460,fd=602))
root@ubuntu79:/home/vboxuser# systemctl stop wazuh-"*"
root@ubuntu79:/home/vboxuser# /opt/splunk/bin/splunk stop
splunkd is not running.
```

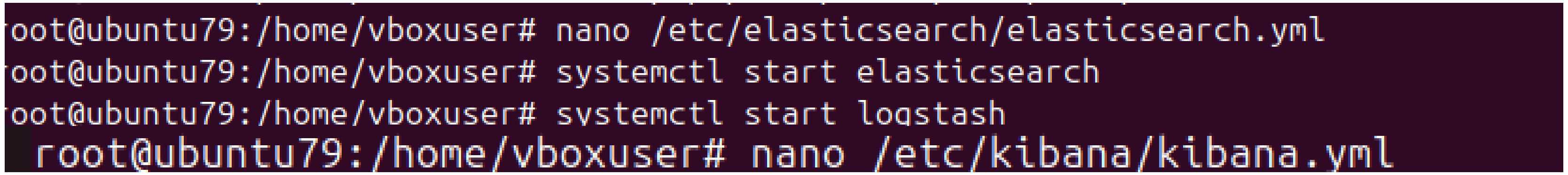
Make changes in **[nano /opt/zeek/share/zeek/site/local.zeek]** file add following command at the end of the line

>@load policy/tuning/json-logs.zeek



```
  GNU nano 7.2                                        /opt/zeek/share/zeek/site/local.zeek
# 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
```

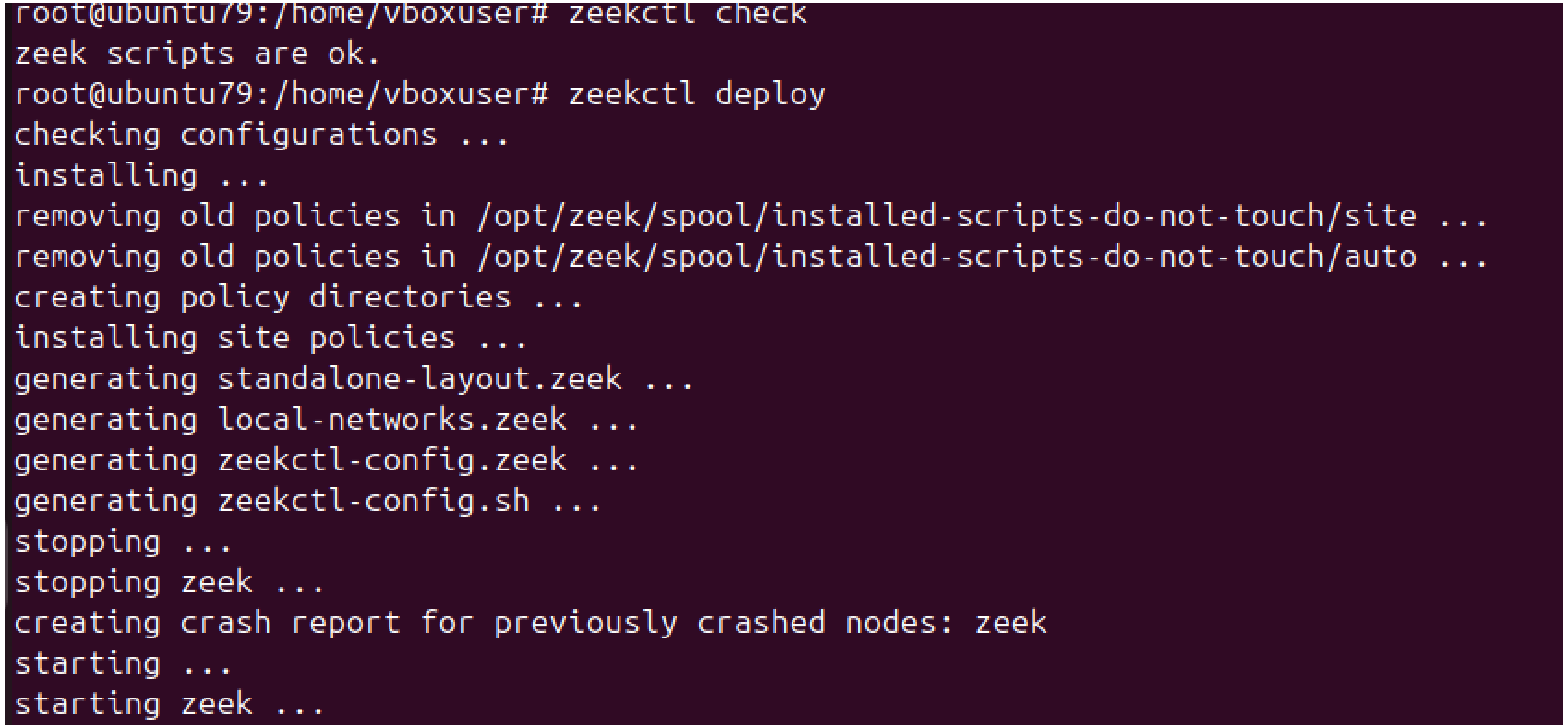
Change ip address in >**[nano /etc/elasticsearch/elasticsearch.yml]** and in **>[nano /etc/kibana/kibana.yml]** file



```
oot@ubuntu79:/home/vboxuser# nano /etc/elasticsearch/elasticsearch.yml
oot@ubuntu79:/home/vboxuser# systemctl start elasticsearch
oot@ubuntu79:/home/vboxuser# systemctl start logstash
 root@ubuntu79:/home/vboxuser# nano /etc/kibana/kibana.yml
```

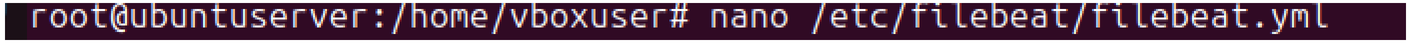
>zeekctl check

>zeekctl deploy



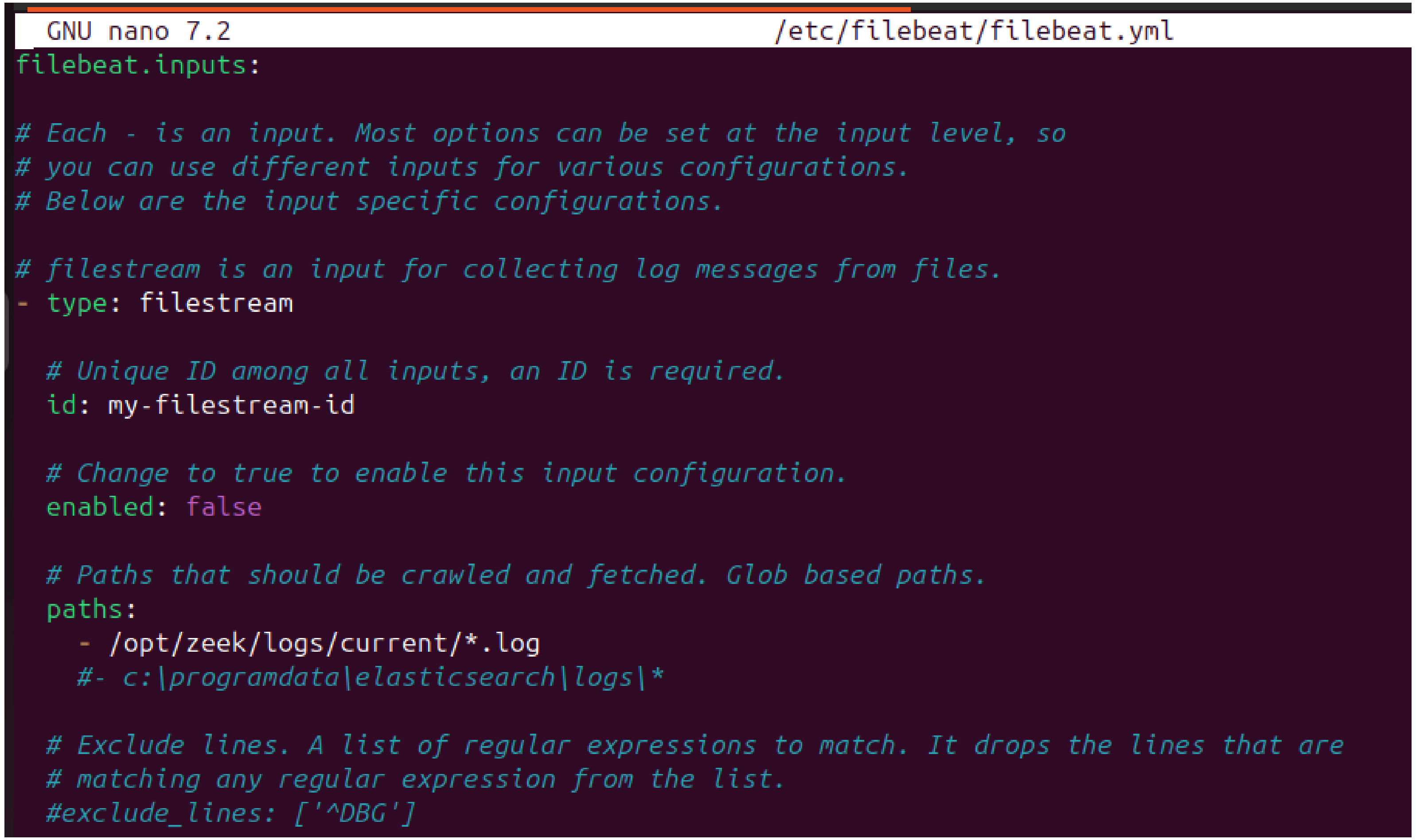
```
root@ubuntu79:/home/vboxuser# zeekctl check
zeek scripts are ok.
root@ubuntu79:/home/vboxuser# zeekctl deploy
checking configurations ...
installing ...
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/site ...
removing old policies in /opt/zeek/spool/installed-scripts-do-not-touch/auto ...
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 ...
```

Let’s start commands in 2nd ubuntu



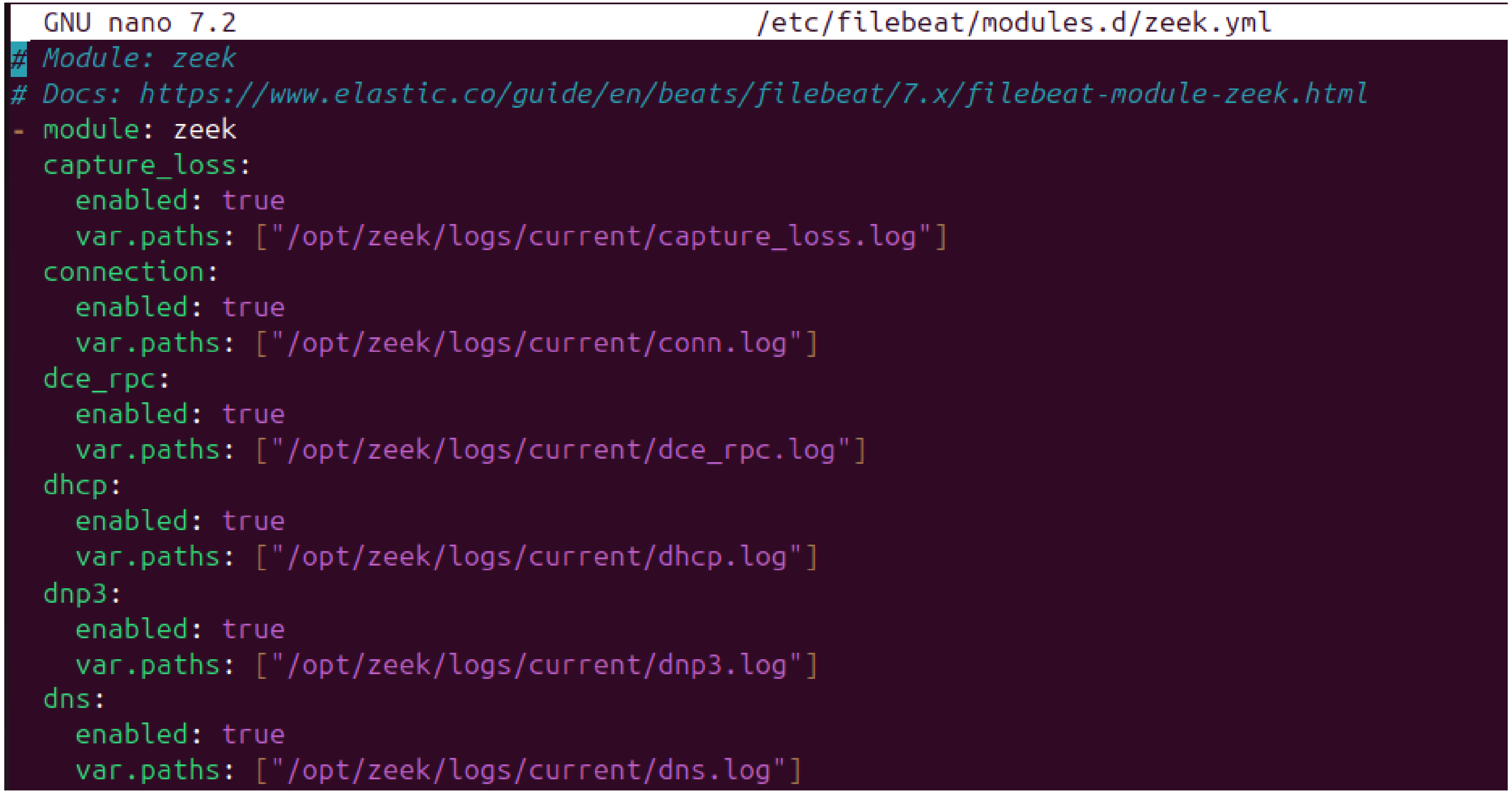
```
root@ubuntuserver:/home/vboxuser# nano /etc/filebeat/filebeat.yml
```

Paths: **> /opt/zeek/logs/current/*.log**



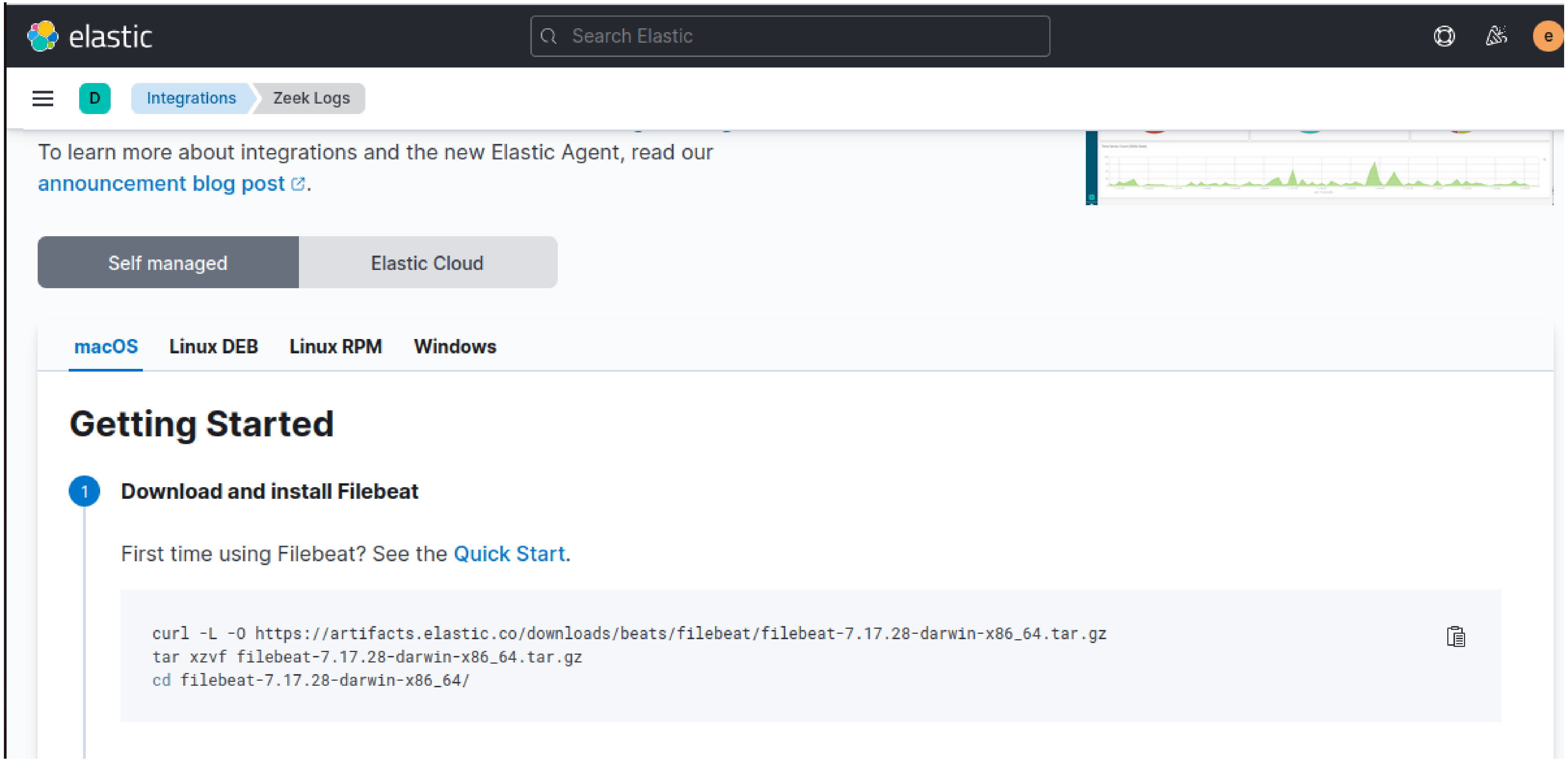
```
  GNU nano 7.2                                   /etc/filebeat/filebeat.yml
filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.

# filestream is an input for collecting log messages from files.
- type: filestream

  # Unique ID among all inputs, an ID is required.
  id: my-filestream-id

  # Change to true to enable this input configuration.
  enabled: false

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - /opt/zeek/logs/current/*.log
    #- c:\programdata\elasticsearch\logs\*

  # Exclude lines. A list of regular expressions to match. It drops the lines that are
  # matching any regular expression from the list.
  #exclude_lines: ['^DBG']
```

Make changes in **[etc/filebeat/modules.d/zeek.yml] file**
paths: **>[“/opt/zeek/logs/current”]** in the file



```
  GNU nano 7.2                              /etc/filebeat/modules.d/zeek.yml
# Module: zeek
# Docs: https://www.elastic.co/guide/en/beats/filebeat/7.x/filebeat-module-zeek.html
- module: zeek
  capture_loss:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/capture_loss.log"]
  connection:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/conn.log"]
  dce_rpc:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/dce_rpc.log"]
  dhcp:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/dhcp.log"]
  dnp3:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/dnp3.log"]
  dns:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/dns.log"]
```

On firefox when we search http://ubuntu-ip:5601 than we login as username and password than we search zeek logs after login and copy this commands on 2nd ubuntu to get the data from another 1st ubuntu



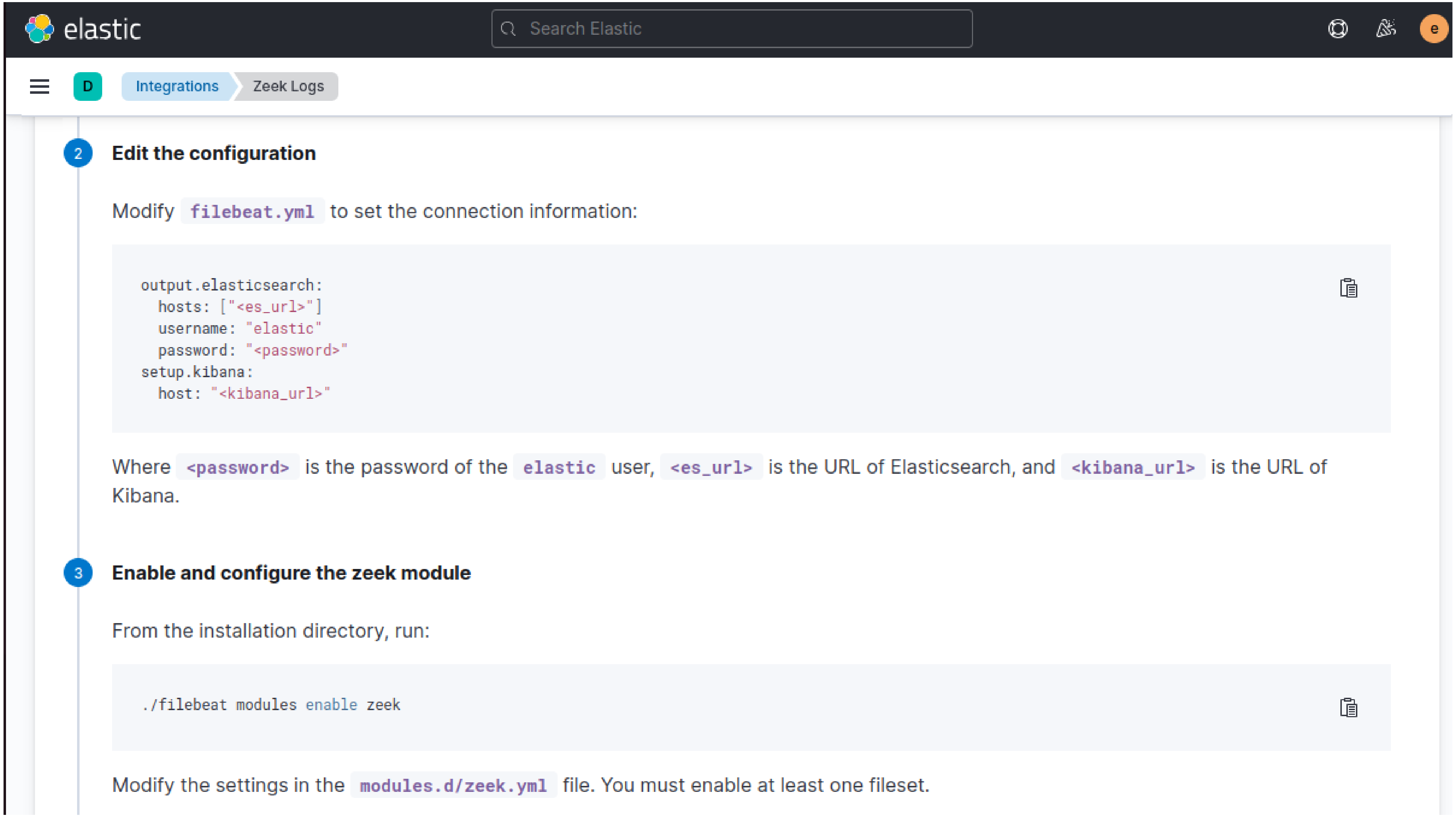
To learn more about integrations and the new Elastic Agent, read our announcement blog post.

Getting Started

1 **Download and install Filebeat**

First time using Filebeat? See the Quick Start.

```
curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.17.28-darwin-x86_64.tar.gz
tar xzvf filebeat-7.17.28-darwin-x86_64.tar.gz
cd filebeat-7.17.28-darwin-x86_64/
```



2 **Edit the configuration**

Modify `filebeat.yml` to set the connection information:

```
output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
  password: "<password>"
setup.kibana:
  host: "<kibana_url>"
```

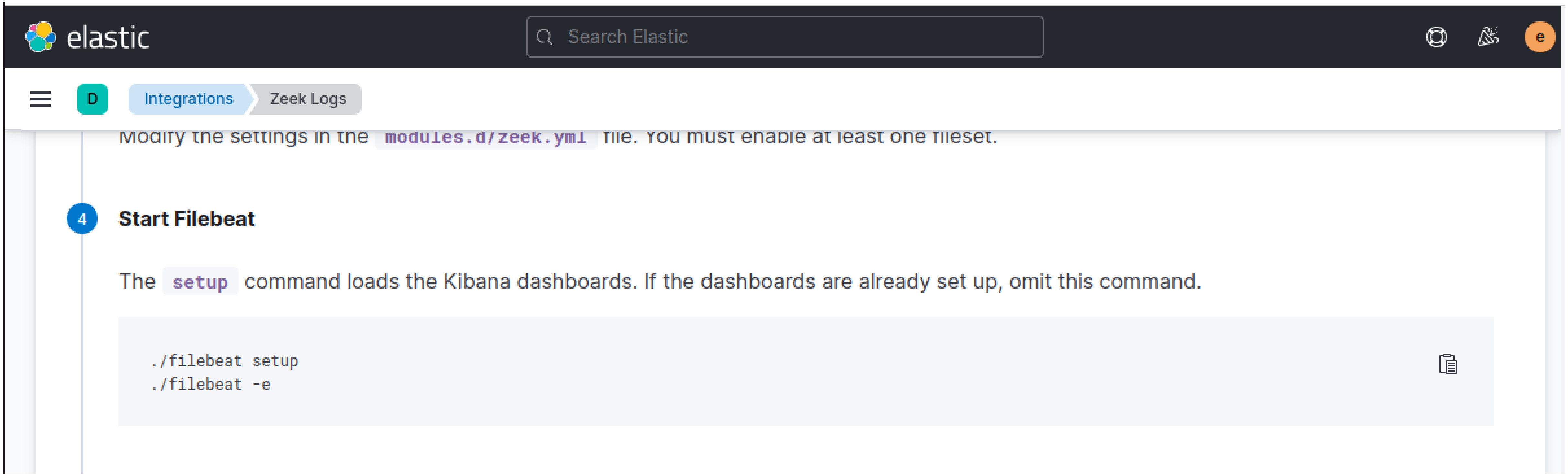
Where `<password>` is the password of the `elastic` user, `<es_url>` is the URL of Elasticsearch, and `<kibana_url>` is the URL of Kibana.

3 **Enable and configure the zeek module**

From the installation directory, run:

```
./filebeat modules enable zeek
```

Modify the settings in the `modules.d/zeek.yml` file. You must enable at least one fileset.



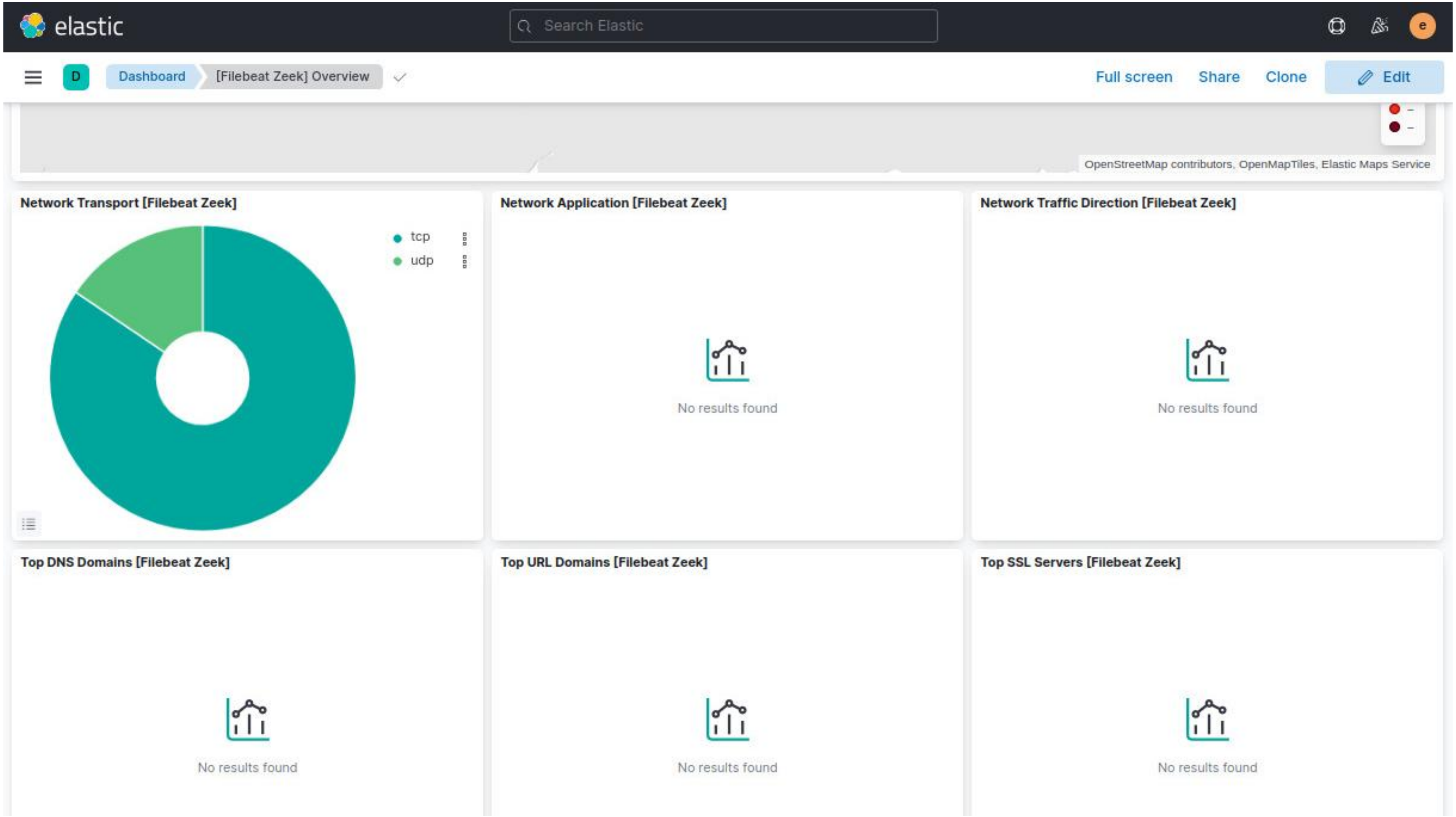
Modify the settings in the `modules.d/zeek.yml` file. You must enable at least one fileset.

4 **Start Filebeat**

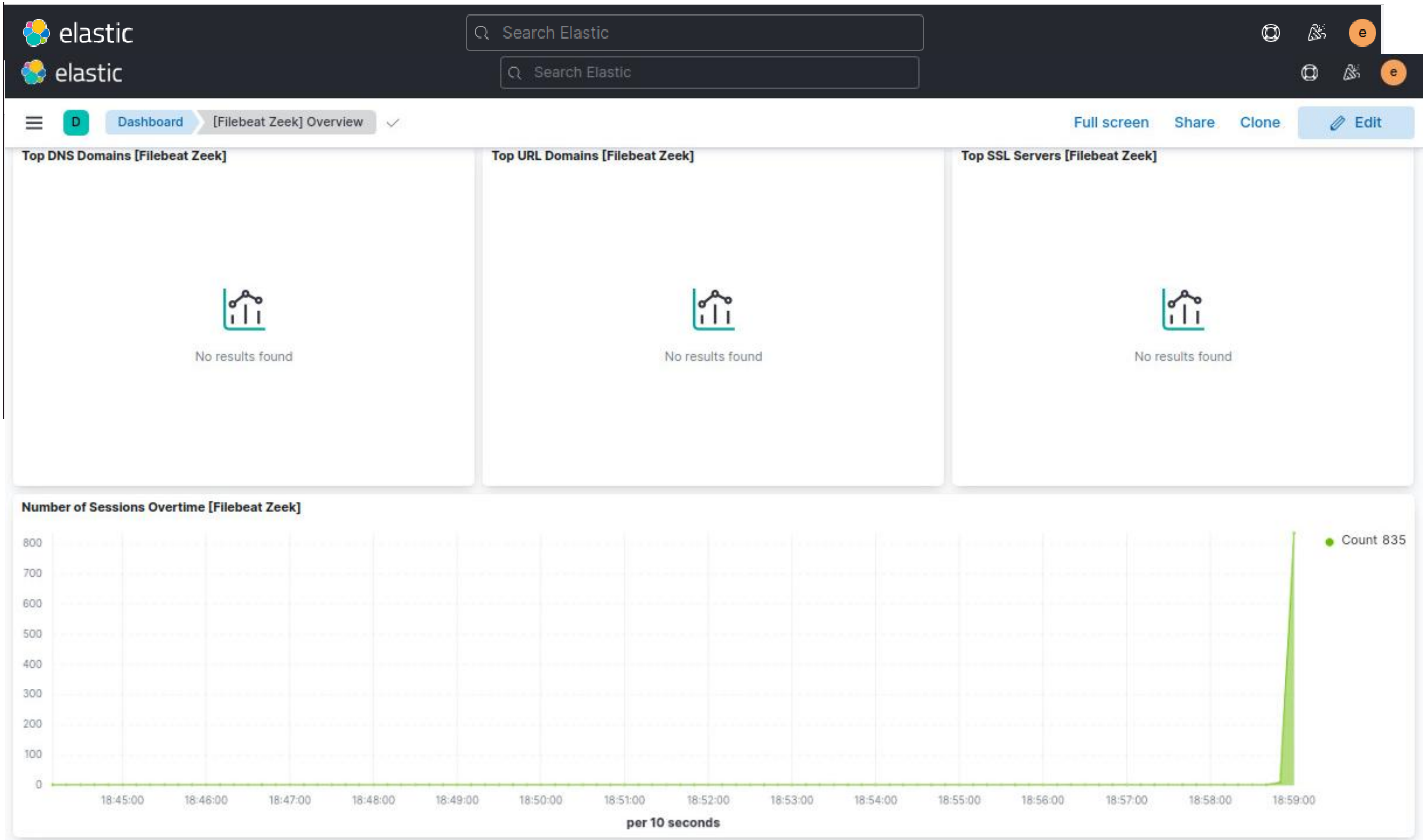
The `setup` command loads the Kibana dashboards. If the dashboards are already set up, omit this command.

```
./filebeat setup
./filebeat -e
```

After this [**./filebeat –e]** command we will get the data on this interface



elastic
Search Elastic
Dashboard
[Filebeat Zeek] Overview
Full screen
Share
Clone
Edit
OpenStreetMap contributors, OpenMapTiles, Elastic Maps Service
Network Transport [Filebeat Zeek]
tcp
udp
Network Application [Filebeat Zeek]
No results found
Network Traffic Direction [Filebeat Zeek]
No results found
Top DNS Domains [Filebeat Zeek]
No results found
Top URL Domains [Filebeat Zeek]
No results found
Top SSL Servers [Filebeat Zeek]
No results found



Top DNS Domains [Filebeat Zeek]

No results found

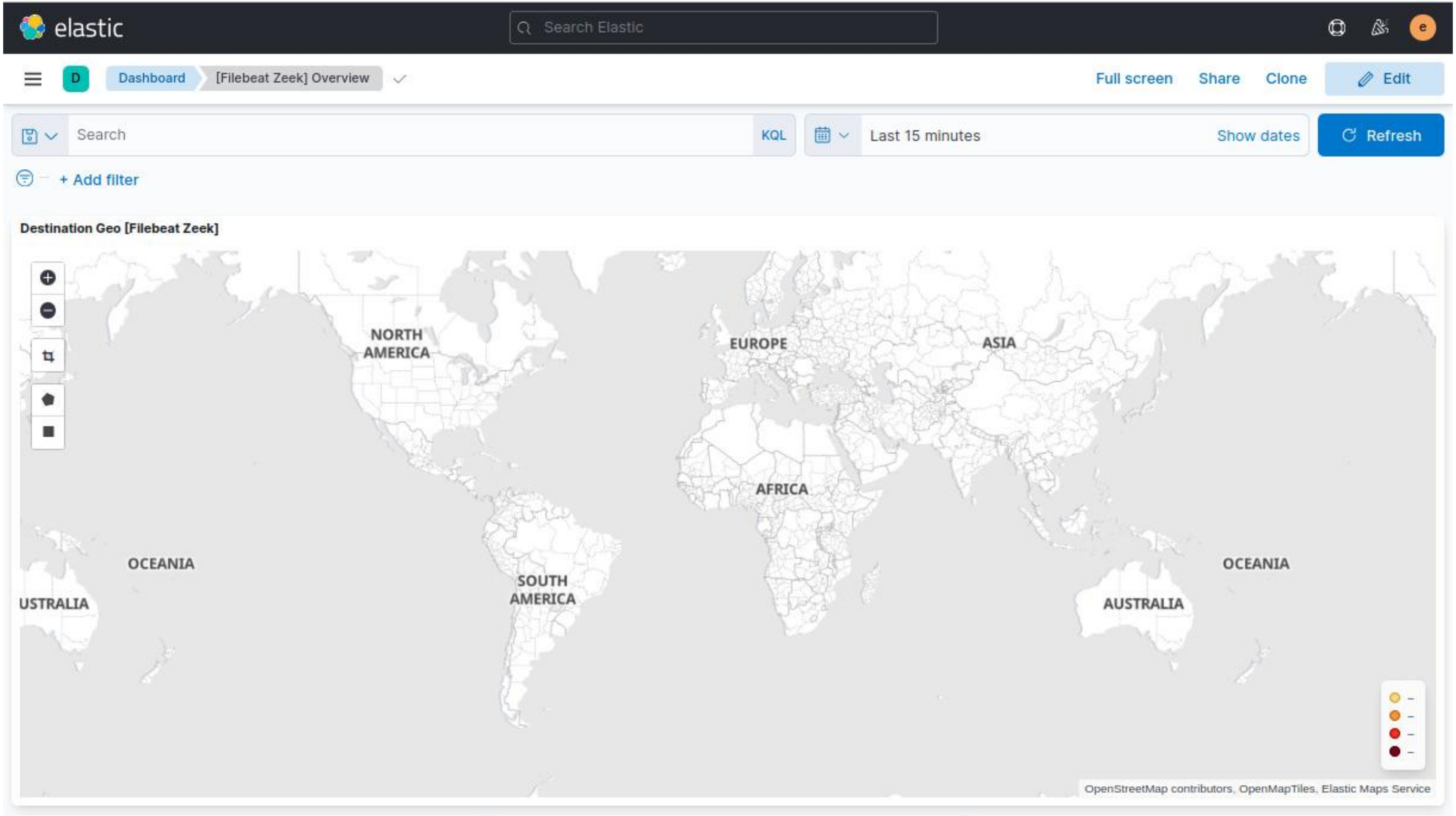
Top URL Domains [Filebeat Zeek]

No results found

Top SSL Servers [Filebeat Zeek]

No results found

Number of Sessions Overtime [Filebeat Zeek]



elastic
Search Elastic
e
D
Dashboard
[Filebeat Zeek] Overview
Full screen
Share
Clone
Edit
Search
KQL
Last 15 minutes
Show dates
Refresh
+ Add filter
Destination Geo [Filebeat Zeek]
NORTH AMERICA
EUROPE
ASIA
AFRICA
OCEANIA
SOUTH AMERICA
USTRALIA
OCEANIA
AUSTRALIA
● –
● –
● –
● –
OpenStreetMap contributors, OpenMapTiles, Elastic Maps Service