🧪 Lab Guide 4 – Installing Log Infrastructure on Lubuntu

This lab installs and configures a **Lubuntu VM** to act as the central log infrastructure. We will install **Zeek**, **Elasticsearch + Kibana**, and **Filebeat**.

Part 1 – Install Lubuntu VM

Download ISO

- Lubuntu ISO (latest LTS) (https://lubuntu.me/downloads/)

Steps

1. In VirtualBox → **New** → Name: Lubuntu-Logs, Type: *Linux*, Version: *Ubuntu (64-bit)*.
2. Assign **4-8 GB RAM**, **2 CPUs**.
3. Create a **40/60 GB VDI disk**.
4. Attach the Lubuntu ISO under **Storage**.
5. Set **Network Adapter 1** to **NAT**.

   We will need another adapter for the Zeek network log collection. We set up network in a Host Only network and logmonitor VM collects the networking logs in Zeek.
6. Start VM and run the installer with defaults.

Part 2 – Install Zeek

1. Update system:

   ```
   sudo apt update && sudo apt upgrade -y
   ```
2. Check your Lubuntu release version:

   ```
   lsb_release -rs
   ```

   (Example: 22.04, 24.04, etc.)
3. Download Zeek GPG key.

```
curl -fsSL
https://download.opensuse.org/repositories/security:zeek/xUbuntu_
25.04/Release.key | gpg --dearmor | tee
/etc/apt/trusted.gpg.d/security_zeek.gpg
```

4. Add Zeek to the APT source file

```
echo 'deb
http://download.opensuse.org/repositories/security:/zeek/xUbuntu_
25.04/ /' | tee /etc/apt/sources.list.d/security:zeek.list
```

5. Update and install zeek

   ```
   sudo apt update
   ```

   ```
   sudo apt install zeek -y
   ```

6. Add Zeek to .bashrc file

   ```
   echo "export PATH=$PATH:/opt/zeek/bin" >> ~/.bashrc
   ```

7. Reload .bashrc

   ```
   source ~/.bashrc
   ```

8. Verify installation:

   ```
   zeek -version
   ```

Note: We will configure zeek for log collection.

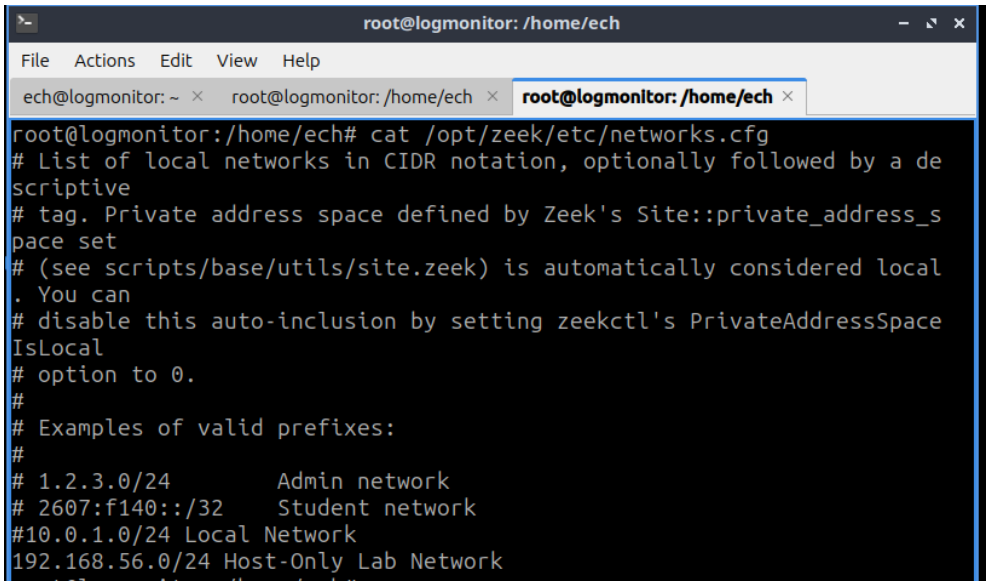
Part 3 – Configure Zeek

1. Edit Zeek networks file

   ```
   sudo nano /opt/zeek/etc/network.cfg
   ```

   Add the host-only monitored network line (exactly)

   192.168.56.0/24 Host-Only Lab Network (depends on your setup – Host-Only network IP address may be different.)



   Save and exit

2. Find the host-only interface name (on Lubuntu)

   ```
   Ip a
   ```

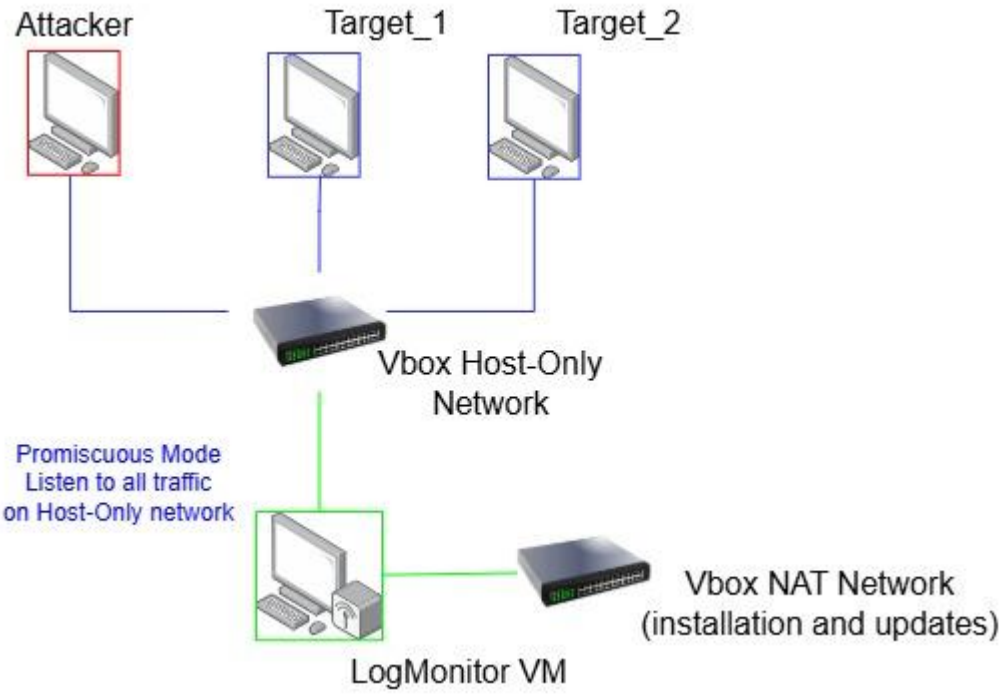
   Look for the interface that has IP 192.168.56.[4]. Typical names: **enp0s8**, enp0s3, eth1.

   Note the interface name (we'll call it IFACE below)

Part 4 – Make Zeek Listen to (and capture) Host-Only Traffic

1. Configure VM setup following steps:
   - *Shutdown all VMs.*
   - *Change network adapters of Kali, Metasploitable 2, Windows and configure as Host-Only adapter.*
   - *Lubuntu is the LogMonitoring VM. Add another network adapter and set one as Host-Only (promiscuous mode/All).*

     Configure the second adapter as either NAT or Bridged.



2. Ensure that all inter-VM traffic goes through the Host-Only network and visible to LogMonitor VM.
3. Ping each host and see the echo requests/replies.
4. Check the configuration of Zeek. Zeek should listen on the Host-Only NIC. At this point check the node.cfg to listen on the Host-Only network

   ```
   sudo nano /opt/zeek/etc/node.cfg
   ```

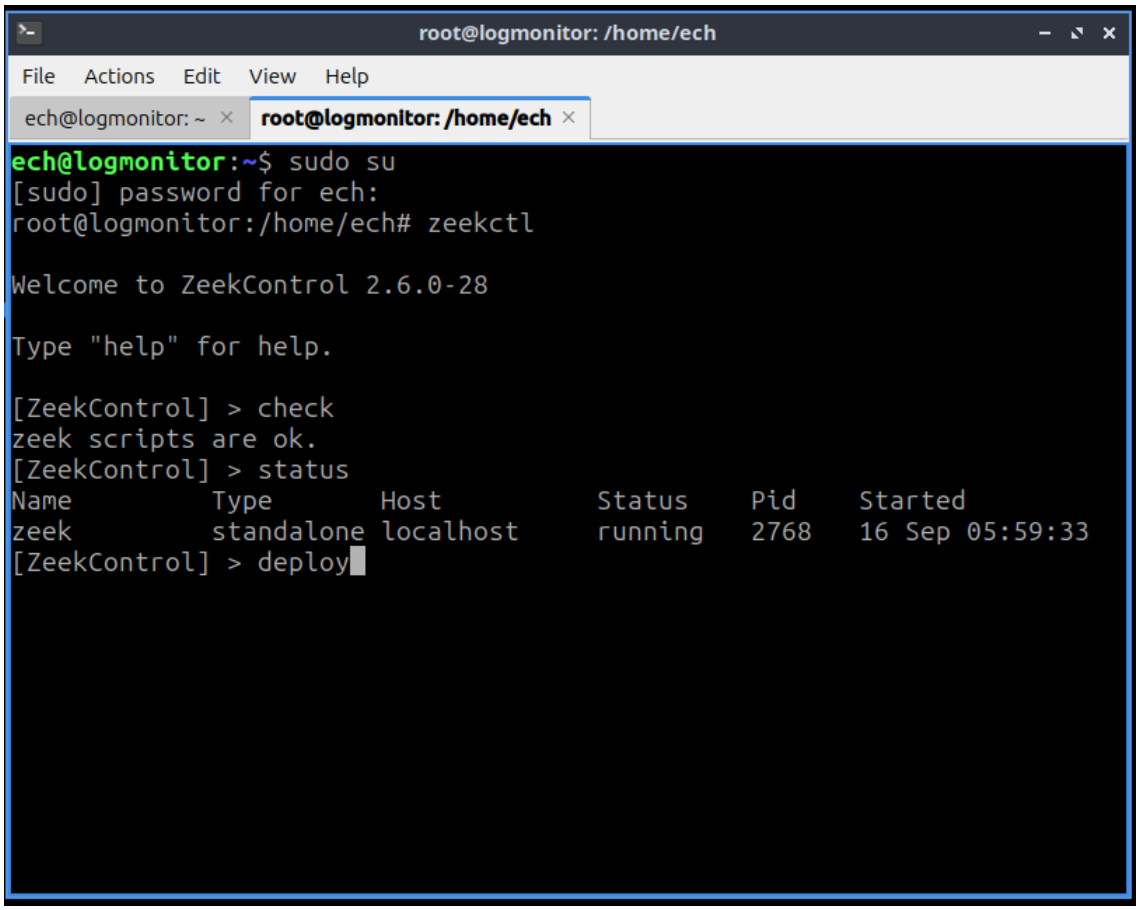
[zeek]

type=standalone

host=localhost

interface=enp0s8 [← this is the interface of your VM. You can get the interface name using “ip a” command.

`zeekctl – check – status – deploy`



5. Start Zeek in capture mode

   `sudo zeek -i enp0s8 -C`

6. Generate some lab traffic

Windows → open a website or connect to Metasploitable

Kali → run a quick scan “namp -sS <host only network>

7. Inspect Zeek logs

ls /opt/zeek/logs/current

Common files:

- conn.log → connection summaries
- dns.log → DNS queries

- http.log → web requests

Part 5 – Install Elasticsearch & Kibana (Elastic Stack)

Step 1 Install Elasticsearch

Elasticsearch and Kibana installation requires additional configuration, and steps here should be followed accordingly.

1. Update packages and install prerequisites:

```
sudo apt update && sudo apt install -y apt-transport-https wget gnupg
```

2. Import Elastic GPG key:

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg
```

3. Add Elastic repository:

```
echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
```

4. Install Elasticsearch:

```
sudo apt update

sudo apt install -y elasticsearch
```

5. Enable and start Elasticsearch:

```
sudo systemctl daemon-reload

sudo systemctl enable elasticsearch.service

sudo systemctl start elasticsearch.service
```

Step 2 Initial Security Configuration

After installation, Elastic 8.x enables security **by default**.

- A bootstrap password is generated for the built-in elastic user.
- To reset it manually:

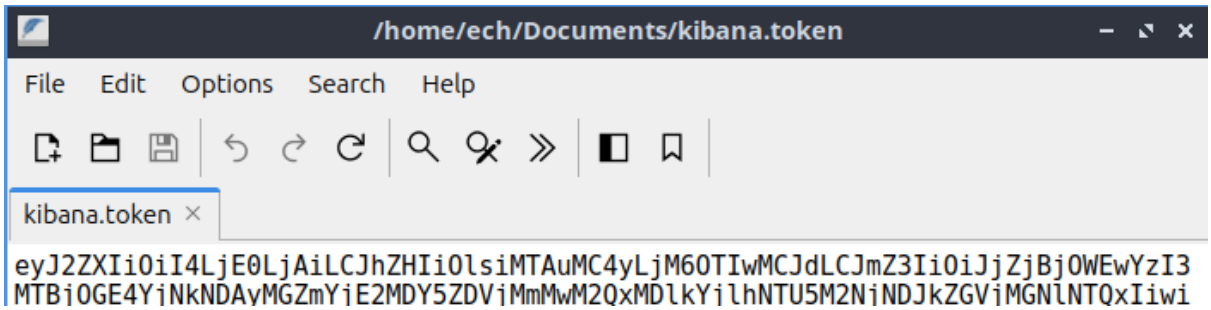
```
sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic -i
```

Step 3 Create Enrollment Token for Kibana

Generate a new token to link Kibana with Elasticsearch:

```
sudo /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana
```

Copy the token string.



Step 4 Install Kibana

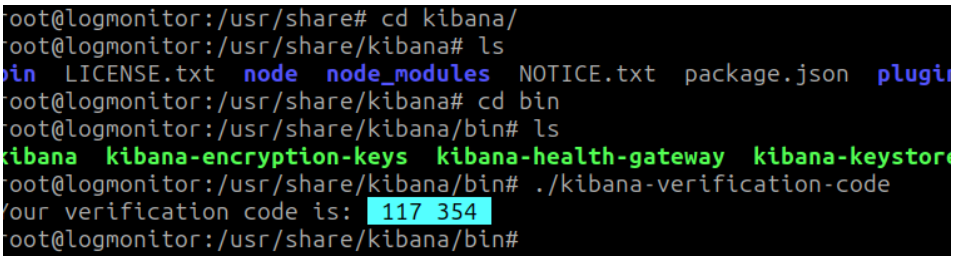
1. Install Kibana via APT:
   ```
   sudo apt install -y kibana
   ```
2. Enable and start Kibana:
   ```
   sudo systemctl enable kibana --now
   sudo systemctl status kibana
   ```

Step 5 Enroll Kibana with Elasticsearch

1. /usr/share/kibana/bin/kibana-verification-code

   Get the Kibana verification code (needed for browser login).

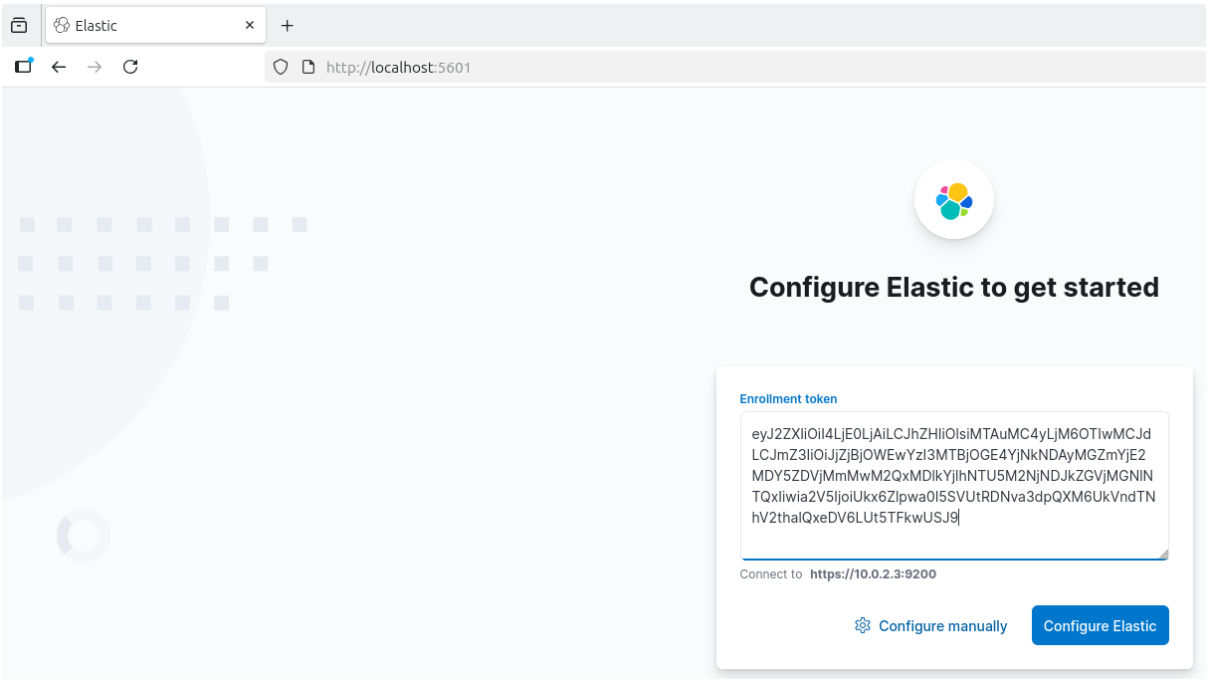
   Copy the 6-digit code (an example code, below)



Step 6 Access Kibana Web UI

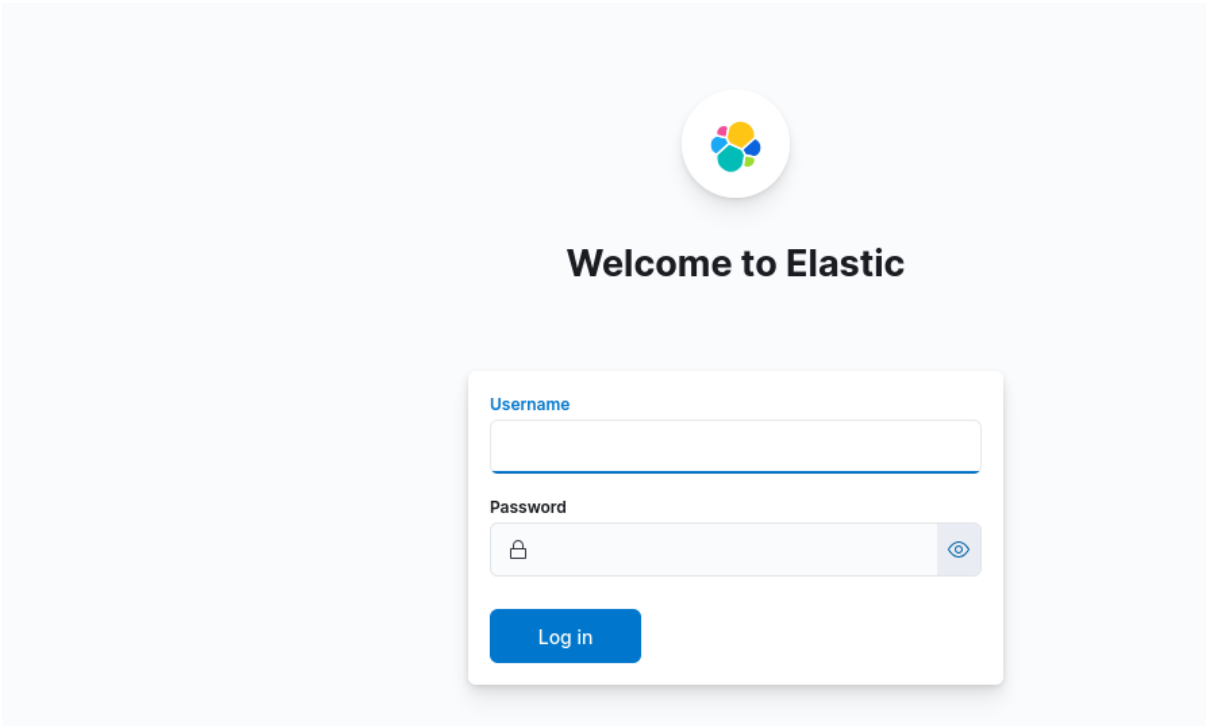
Open in browser:

- From Lubuntu: http://localhost:5601



Enter username and password (username: elastic and password is the one you set before).

This is the screen you should access if every step is run as expected. (The dashboard below is sign in, https://www.elastic.co/elasticsearch for extra information.)



Part 6 Ingest Zeek logs into Elasticsearch/Kibana with Filebeat

Step 1 Lab topology & assumptions

- OS: Ubuntu/Debian (sudo available)
- Elasticsearch: https://10.0.2.3:9200 (TLS enabled, http_ca.crt exists) [this is the NAT/Bridge Network Interface. This can be different for your setup. If it does not works try localhost, Host-Only interface and troubleshoot using online resources, LLM support]
- Kibana: http://localhost:5601 (no TLS in this lab) [In production and real-life use, Kibana should communicate with elasticsearch via encrypted channel.]
- Zeek logs: **/opt/zeek/logs/current/*** [default location where Zeek logs are. You can see additional directories in the /opt/zeek/logs/ path. These are rotated logs when you ran zeekctl deploy command or normally every 24 hrs.]
- You'll use **Filebeat's Zeek module** (not Fleet)
- You have either a **service account token** or **elastic** username/password

---

Step 2 Install Filebeat

Elastic apt repo (8.x) [We add this repo while installing elasticsearch]

```
curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg
```

```
echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
```

```
sudo apt-get update
```

```
sudo apt-get install -y filebeat
```

```
filebeat version
```

Step 3 Point Filebeat to Elasticsearch (TLS) and Kibana

Find the CA:

```
sudo find /etc/elasticsearch -name http_ca.crt
```

```
# example: /etc/elasticsearch/certs/http_ca.crt
```

Edit /etc/filebeat/filebeat.yml and set **one** of these,

A. Service account token (recommended for labs)

output.elasticsearch:

hosts: ["https://10.0.2.3:9200"]

service_account_token: "<SERVICE_ACCOUNT_TOKEN>" #[same token used for kibana integration.]

ssl.certificate_authorities: ["/etc/elasticsearch/certs/http_ca.crt"]

B. Username/password

output.elasticsearch:

hosts: ["https://10.0.2.3:9200"]

username: "elastic"

password: "<ELASTIC_PASSWORD>"

ssl.certificate_authorities: ["/etc/elasticsearch/certs/http_ca.crt"]

C. Continue editing the filebeat.yml file with Kibana service details.

Kibana (dashboards setup):

setup.kibana:

host: "http://localhost:5601"

Sanity checks:

```
sudo filebeat test config -e
sudo filebeat test output -e
```

You should see TLS handshake **OK** and ES version detected.

Step 4 Make Zeek write JSON (strongly recommended)

Backup and edit the active Zeek site config

```
sudo cp -a /opt/zeek/share/zeek/site/local.zeek /opt/zeek/share/zeek/site/local.zeek.bak.$(date +%F)
sudo nano /opt/zeek/share/zeek/site/local.zeek
```

Add:

```
@load policy/tuning/json-logs
redef LogAscii::use_json = T;
```

Apply & verify:

```
sudo zeekctl deploy
head -n1 /opt/zeek/logs/current/conn.log | jq .
```

(If it prints JSON, you're good.)

Step 5 Enable the Zeek module & configure paths

Enable:

```
sudo filebeat modules enable zeek
sudo filebeat modules list   # should show [*] zeek
```

Create a **clean** /etc/filebeat/modules.d/zeek.yml (keep only logs you actually have):

```
- module: zeek

  connection:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/conn.log"]

  dns:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/dns.log"]

  http:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/http.log"]

  ssl:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/ssl.log"]

  x509:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/x509.log"]

  notice:
```

```
    enabled: true
    var.paths: ["/opt/zeek/logs/current/notice.log"]

  weird:
    enabled: true
    var.paths: ["/opt/zeek/logs/current/weird.log"]
```

YAML rules: two spaces before fileset keys, four spaces before enabled and var.paths. **No tabs**.

Validate:

```
sudo filebeat test config -e
```

Step 6 Load ingest pipelines & dashboards

```
sudo filebeat setup --pipelines --dashboards -e
```

(Should say “Loaded dashboards” and “Loaded Ingest pipelines”.)

Step 7 Start Filebeat

```
sudo systemctl enable --now filebeat
sudo journalctl -u filebeat -e
```

Look for messages like **“harvester started for file: …/dns.log”**.

If you see “permission denied” on /opt/zeek/logs/current/*.log:

```
sudo setfacl -m u:filebeat:r /opt/zeek/logs/current/*.log
sudo systemctl restart filebeat
```

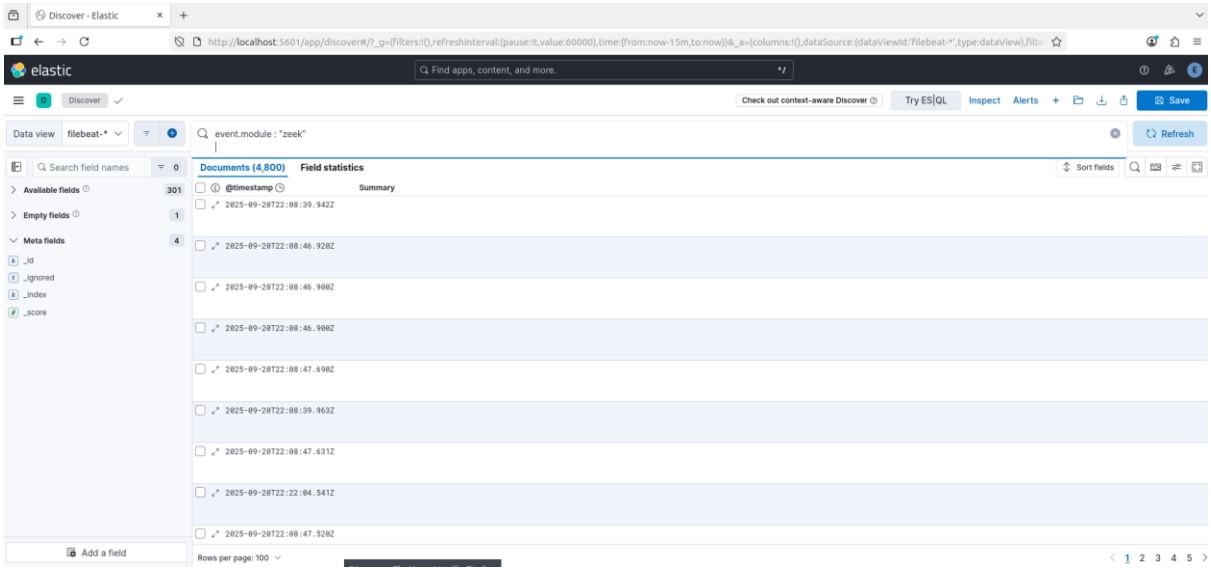
Step 8 Validate in Kibana

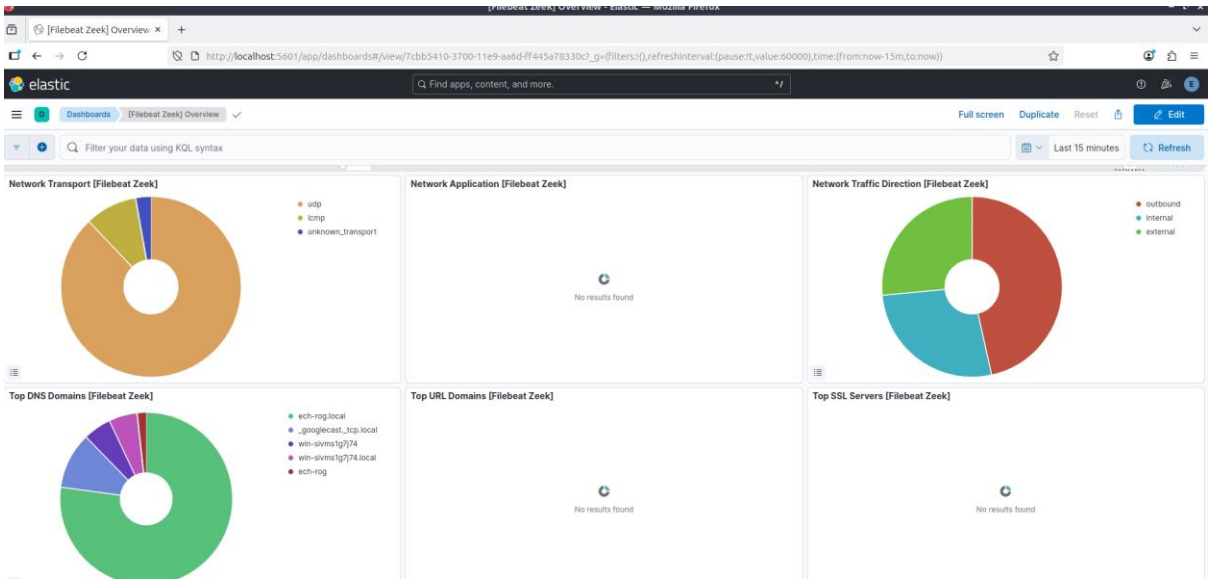
Open **Discover**:

- KQL quick filters:
- event.module : "zeek"
- data_stream.dataset : "zeek.connection"
- data_stream.dataset : "zeek.dns"

Open the Zeek dashboards that ship with the module:

- Dashboards → search “Zeek”





Step 9 Useful KQL searches for the lab

- High DNS volume by host:
- data_stream.dataset:"zeek.dns"

Then aggregate by source.ip (or zeek.orig_h if present).

- Long-lived connections:
- data_stream.dataset:"zeek.connection" and zeek.connection.duration > 300
- Self-signed / weak TLS:
- (data_stream.dataset:"zeek.ssl" or data_stream.dataset:"zeek.x509") and tls.established:true

- Zeek weirds (anomaly hints):
- data_stream.dataset:"zeek.weird"

Step 10 Quick troubleshooting (copy/paste fixes)

- *YAML error (e.g., "did not find expected '-' indicator")*
  Your /etc/filebeat/modules.d/zeek.yml indentation is off. Replace with the known-good block above. Remove tabs/CRLF:

  ```
  sudo apt-get -y install dos2unix

  sudo dos2unix /etc/filebeat/modules.d/zeek.yml
  ```

- *No events in Kibana*
  - Confirm Zeek logs exist & grow:

    ```
    ls -lh /opt/zeek/logs/current/*.log
    ```

  - Confirm JSON:

    ```
    head -n1 /opt/zeek/logs/current/conn.log | jq .
    ```

  - Check Filebeat status/logs:

    ```
    sudo systemctl status filebeat

    sudo journalctl -u filebeat -e
    ```

  - Verify ES index creation:

    ```
    curl -k https://10.0.2.3:9200/_cat/indices/filebeat*?v
    ```

- *TLS/CA errors*
  Point Filebeat to the correct CA:

  ```
  ssl.certificate_authorities:
  ["/etc/elasticsearch/certs/http_ca.crt"]
  ```

- *401/403 unauthorized*
  Wrong creds/token. Re-enter elastic password or use a fresh service account token with write privileges.
- *Module enabled but still no parsing*
  Make sure the module file name is exactly /etc/filebeat/modules.d/zeek.yml and sudo filebeat test config -e passes.

Step 11 (Optional) Make Kibana reachable remotely

In /etc/kibana/kibana.yml:

```
server.host: "0.0.0.0"
```

```
server.publicBaseUrl: "http://<kibana-ip>:5601"
```

Then:

```
sudo systemctl restart kibana
```

Step 12 (Optional) Performance tips for busy labs

- Keep only the filesets you need in zeek.yml.
- Consider faster Zeek rotation and let Filebeat catch up.
- Filebeat queue tuning (only if necessary; defaults are fine for most labs):

/etc/filebeat/filebeat.yml

queue.mem.events: 4096

queue.mem.flush.min_events: 2048

queue.mem.flush.timeout: 10s

Restart Filebeat after changes.