# **Building a Home Network Monitoring Lab with Zeek and ELK Stack Using VMs**

This tutorial will guide you through setting up a network monitoring lab using Zeek, Elastic Stack, and virtualization. The lab will utilize virtual machines (VMs) for ease of deployment and scalability.

## **Step 1: Prepare the Environment**

### **Hardware and Software Requirements**

* **Physical Hardware**: A laptop or desktop with at least 8GB of RAM and 100GB of storage.
* **Virtualization Platform**:
  + Oracle VirtualBox or VMware Workstation.
* **VM Configurations**:
  + Ubuntu Server 24.0.1 LTS (or other compatible Linux distributions).
* **Network Access**:
  + Internet connection and access to your home router.

### **Create Virtual Machine**

1. **Install Virtualization Software**:
   * Download and install VirtualBox or VMware.
2. **Set Up the VM**:
   * **Zeek + ELK VM**:
     + 4 CPUs, 8GB RAM, 100 GB disk.
3. **Networking Configuration**:
   * Set the VMs to "Bridged Networking" to allow direct communication with your home network. Set the VMs to "Bridged Networking" to allow direct communication with your home network. Bridged networking ensures the VMs behave as separate devices on your network, simplifying traffic analysis.
   * Disable DHCP and set a static address

## 

## **Step 2: Install Ubuntu Server on Each VM**

1. **Download Ubuntu Server ISO**:
   * Get the ISO from [Ubuntu’s website](https://ubuntu.com/download/server).
2. **Install Ubuntu Server**:
   * Boot the VM using the ISO.

* Follow the on-screen instructions.
* Use the entire disk as an LVM group.
* Assign a static IP address during setup or configure it post-installation.

1. **Post-Installation Configuration**:
   * Update the system:  
      sudo apt update && sudo apt upgrade -y
   * Install essential tools:  
      sudo apt install net-tools curl wget -y
   * Verify SSH is running:  
      sudo systemctl status ssh

## **Step 3: Install and Configure Zeek**

### **Download Zeek**

* wget “<https://download.zeek.org/zeek-7.0.5.tar.gz>”

**Install Dependencies**

* sudo apt-get install cmake make gcc g++ flex libfl-dev bison libpcap-dev libssl-dev python3 python3-dev swig zlib1g-dev

**Build and Install Zeek**

tar -xzvf zeek-7.0.5.tar.gz

cd zeek-7.0.5.tar.gz

./configure

make

make install

**Add Zeek to PATH** (to use Zeek as a service)

echo “export PATH=/usr/local/zeek/bin:$PATH” >> ~/.bashrc

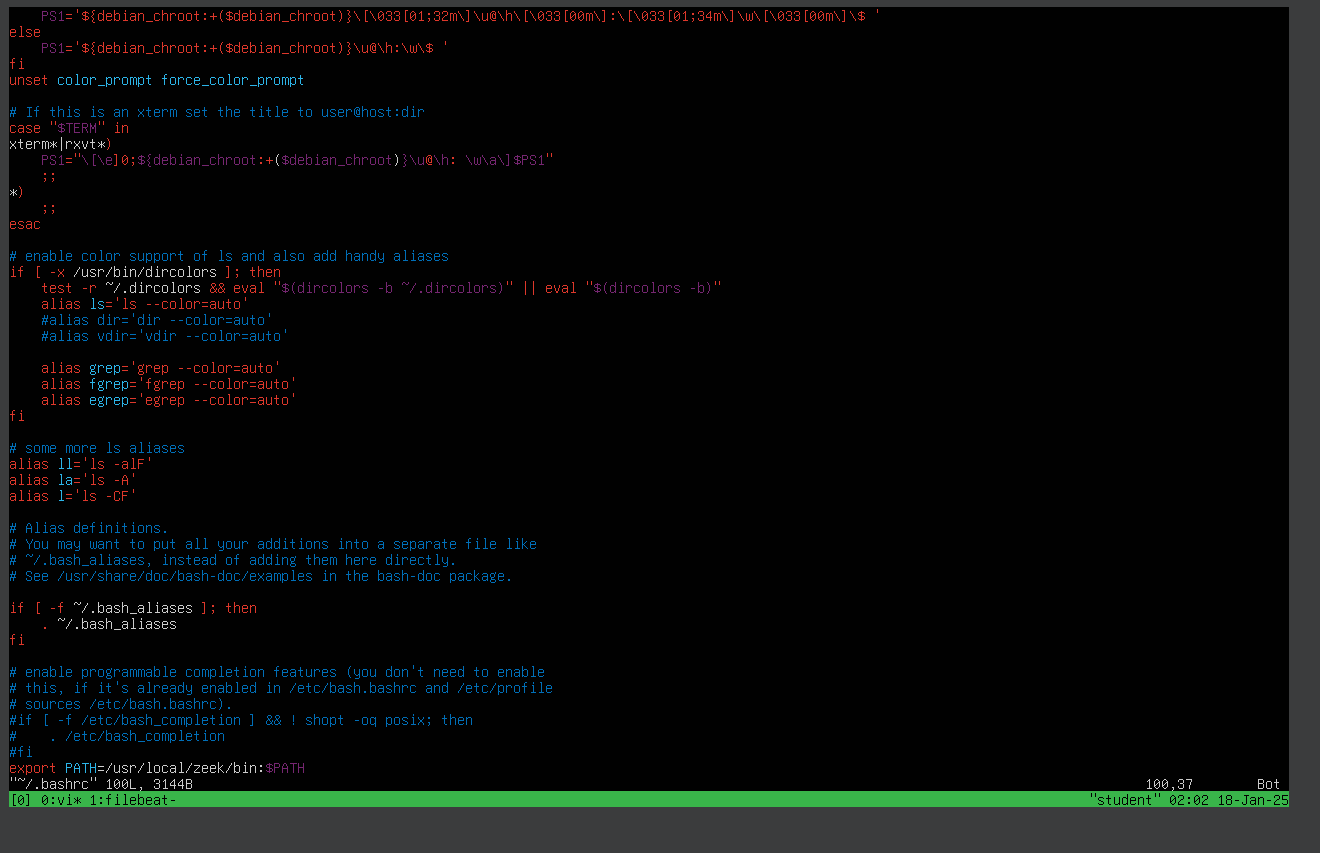
source ~/.bashrc

which zeek

zeek –version

cd /usr/local/zeek/etc

ls



### **Configure Zeek**

* + Identify the network interface:  
     ip a



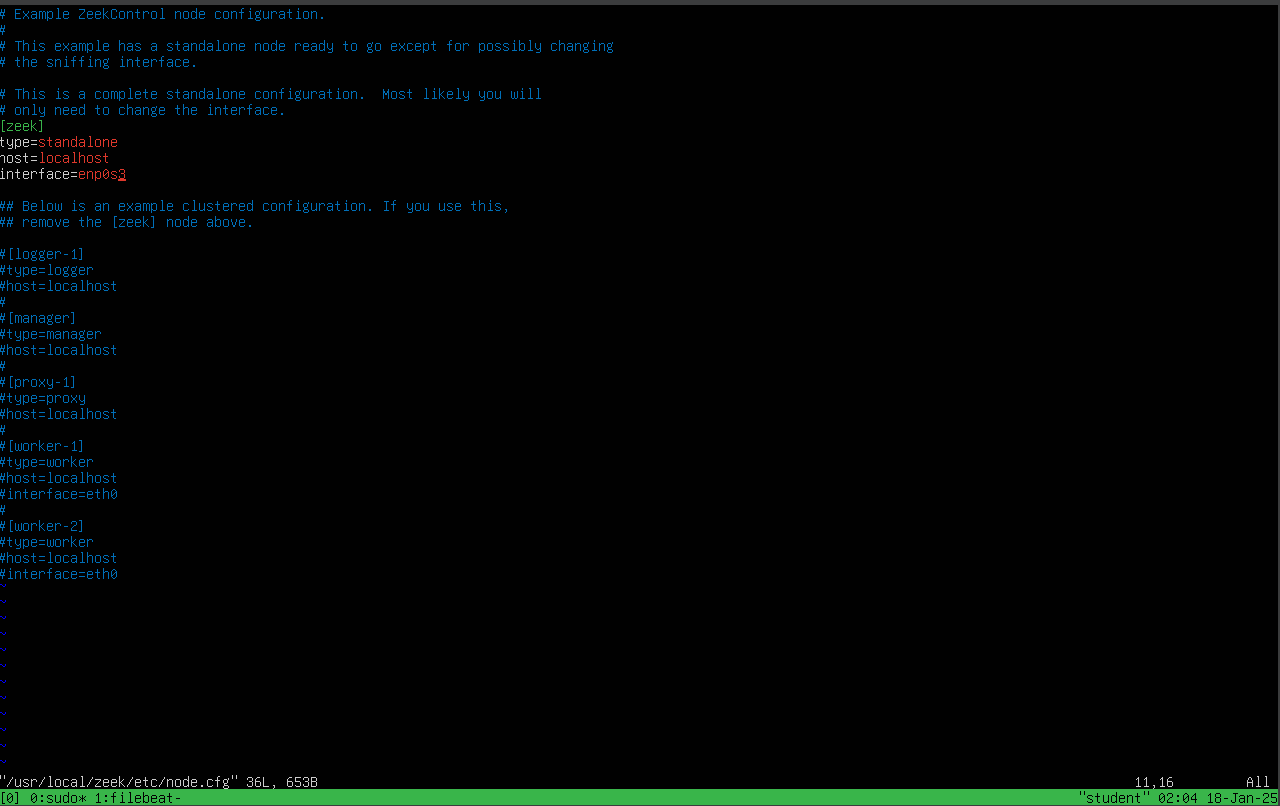
* + Edit Zeek’s configuration:  
     sudo vi /usr/local/zeek/etc/node.cfg
  + Update the interface line:

[zeek]s

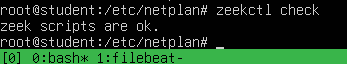
type=standalone

host=localhost

interface=<your-interface>



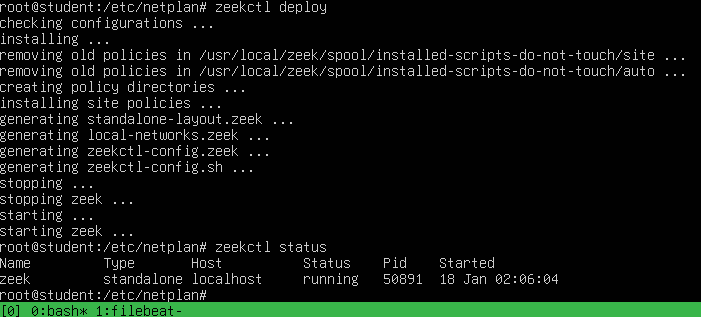
* + Verify the Setup:  
     zeekctl check



* + Deploy and start Zeek:

sudo zeekctl deploy

sudo zeekctl status

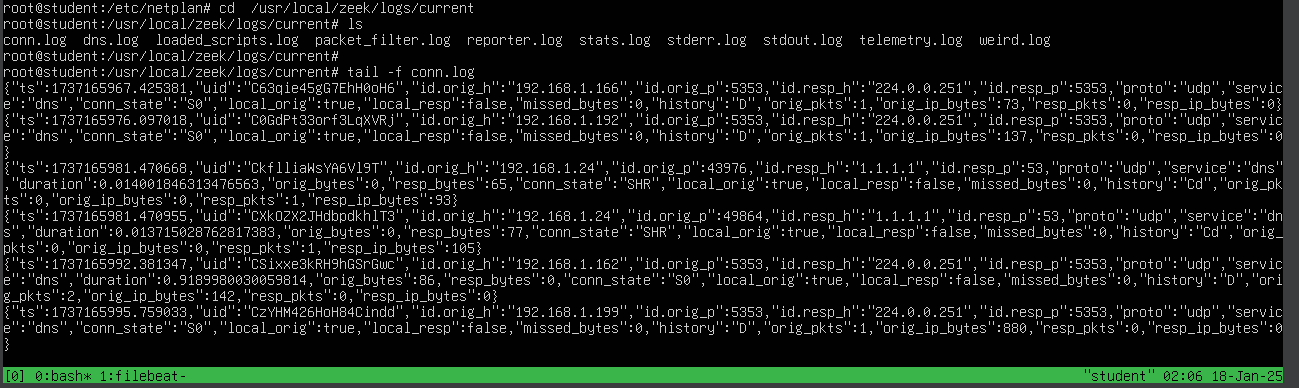


View the logs:

Change directory to /usr/local/zeek/logs/current: cd /usr/local/zeek/logs/current

List all log files: ls

View conn.log: tail -f conn.log



## **Step 4: Set Up the ELK Stack**

### **Install Elasticsearch**

* + Add the PGP key used to sign elastic packages

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

* + Add the apt-transport-https package

sudo apt-get install apt-transport-https

* + Add elastic repository to your source list

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

* + Install the ElasticSearch package

sudo apt-get update && sudo apt-get install elasticsearch

* + Once installed - make this change to the ES config file:  
    vi /etc/elasticsearch/elasticsearch.yml

Set the bind address as “0.0.0.0” so any host on the network can access ES (not advisable in production environments)



* + Start the ES service

sudo systemctl start elasticsearch

sudo systemctl enable elasticsearch

* + Reset the credentials:  
    sudo /usr/share/elasticsearch/bin/elasticsearch-setup-passwords interactive

^If it states the password has already been set or mismatched keystore, we will go ahead and reset it

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

Note down the password: keEYWndS28PZMm8CGs+k

* + Verify Elasticsearch:  
     curl -k -u elastic:[password] "http://localhost:9200/?pretty"

### **Install Kibana**

* + Install Kibana:

sudo apt install kibana -y

* + Configure Kibana:

sudo nano /etc/kibana/kibana.yml

* + Update server.host:

server.host: "0.0.0.0"

* + Start Kibana:

sudo systemctl start kibana

sudo systemctl enable kibana

* + Access Kibana in a browser:  
     http://<server\_ip>:5601

### **Install Filebeat**

* + Download and Install Filebeat:

curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.17.0-darwin-x86\_64.tar.gz

tar xzvf filebeat-8.17.0-darwin-x86\_64.tar.gz

cd filebeat-8.17.0-darwin-x86\_64/

* + Modify filebeat.yml to set the connection information:

filebeat.inputs:

- type: log

paths:

- /usr/local/zeek/logs/current/\*.log

fields:

log\_type: zeek

fields\_under\_root: true

output.elasticsearch:

hosts: ["<es\_url>"]

username: "elastic"

password: "<password>"

# If using Elasticsearch's default certificate

ssl.ca\_trusted\_fingerprint: "<es cert fingerprint>"

setup.kibana:

host: "<kibana\_url>"

* + Configure Zeek to convert the Zeek logs into JSON format:

zeekctl stop

add the following to /opt/zeek/share/zeek/site/local.zeek:

@load policy/tuning/json-logs.zeek

zeekctl deploy

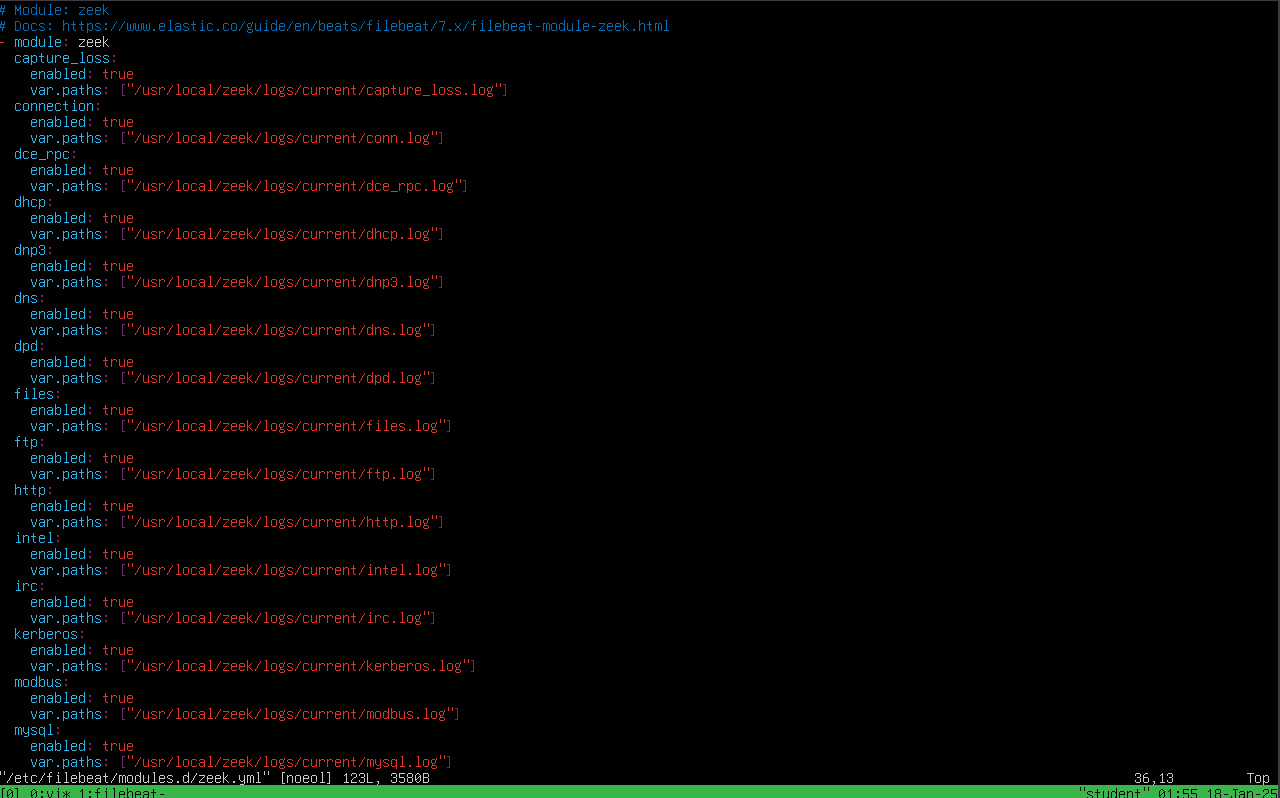
* + Check that the logs are in JSON format

tail -f /opt/zeek/logs/current/dns.log

* + Enable and configure the zeek module

filebeat modules enable zeek

* + Edit the config file in /etc/filebeat/modules.d/zeek.yml:

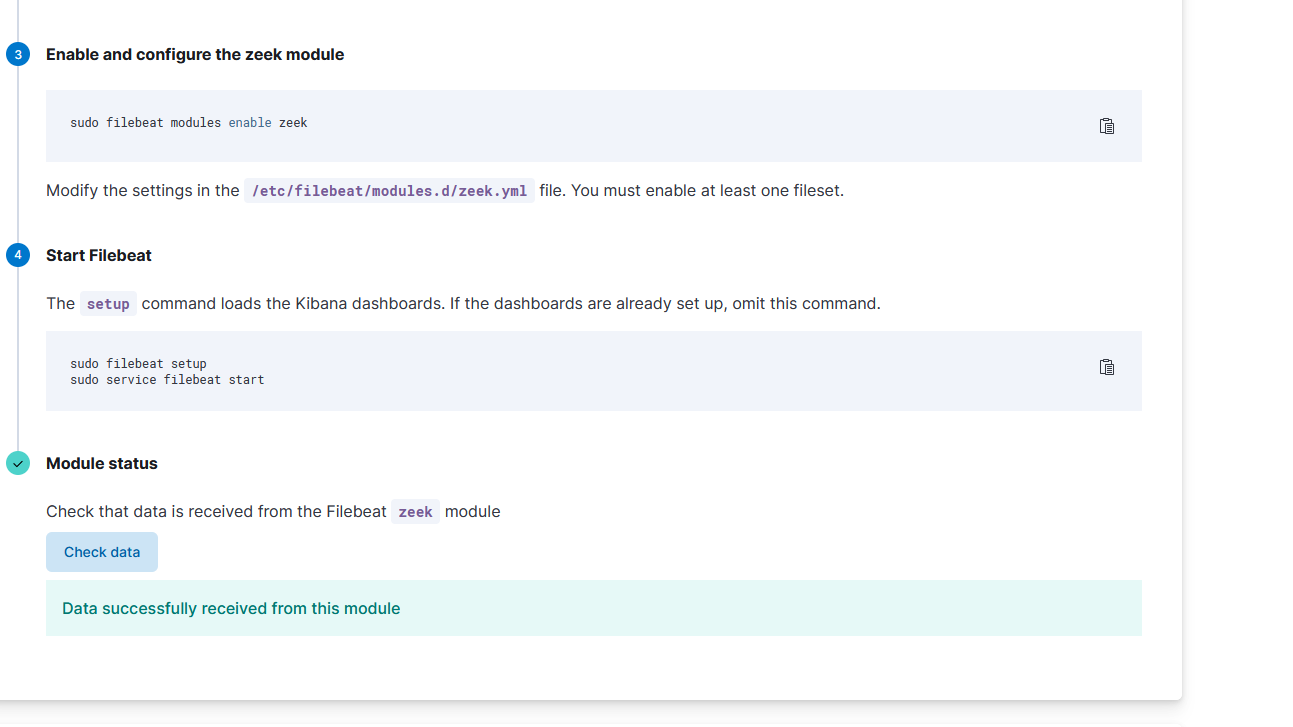


* + Start Filebeat

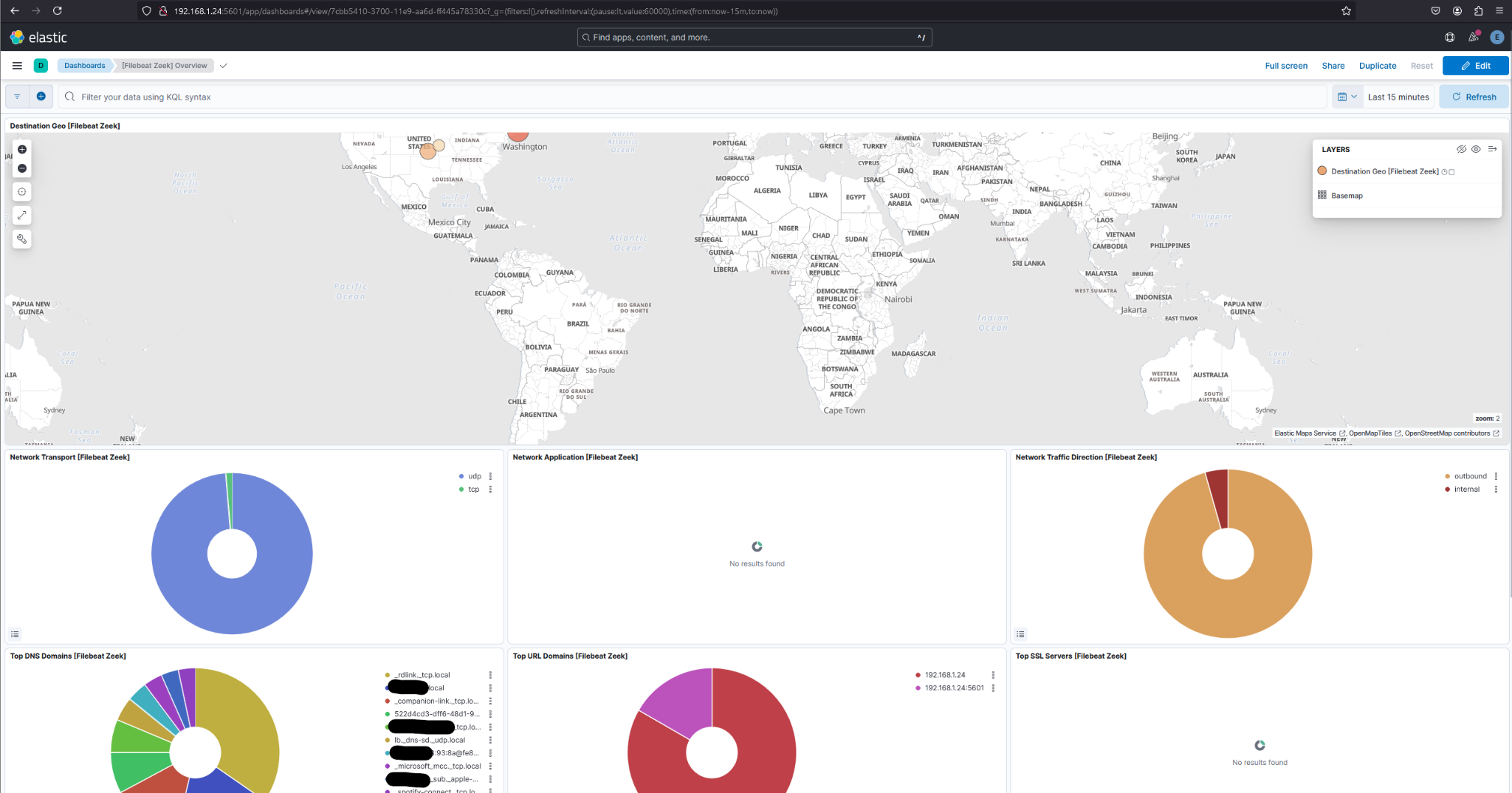
filebeat setup

service filebeat start

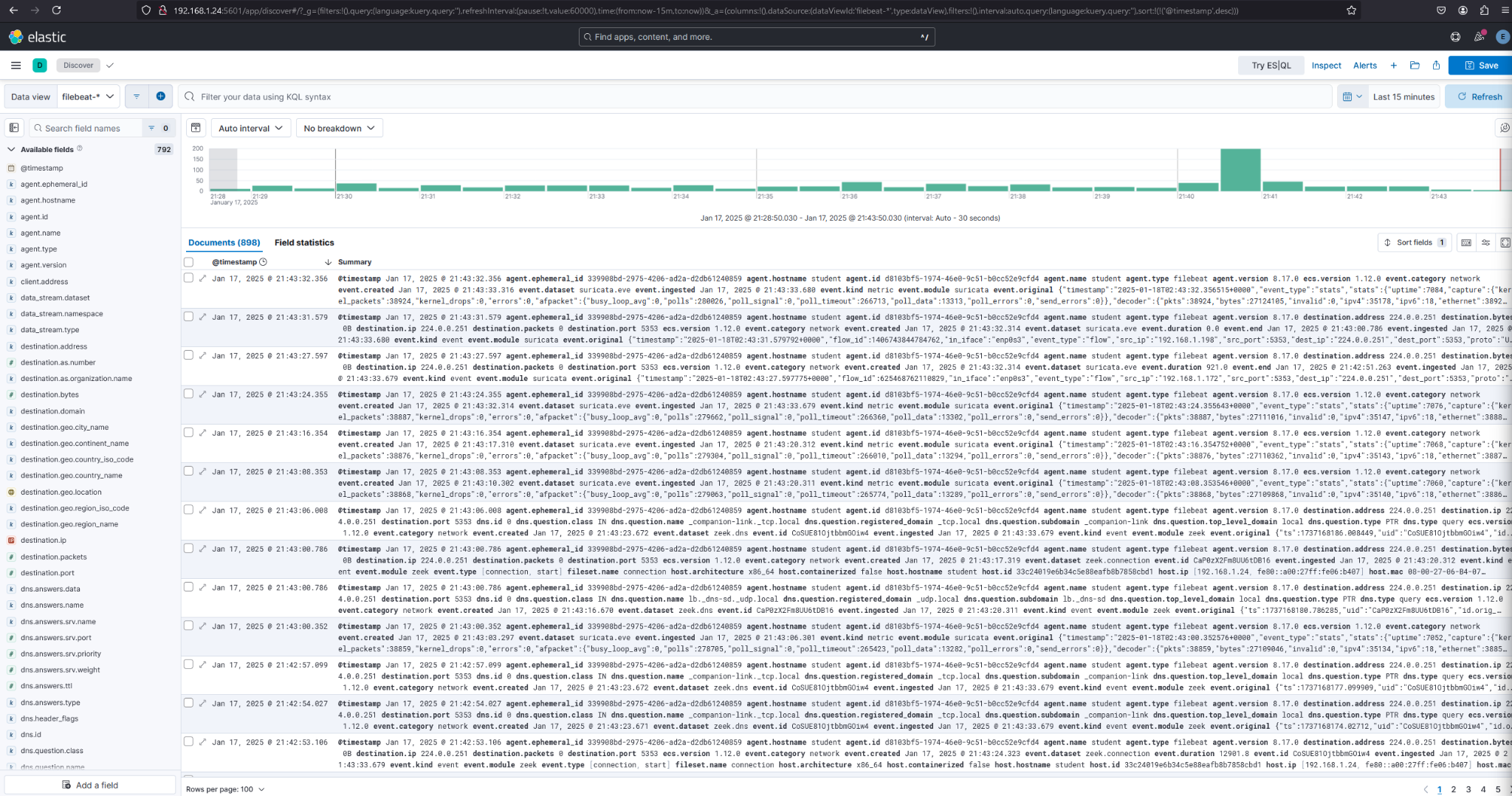
* + Check on Kibana that data is received from the Filebeat zeek module:

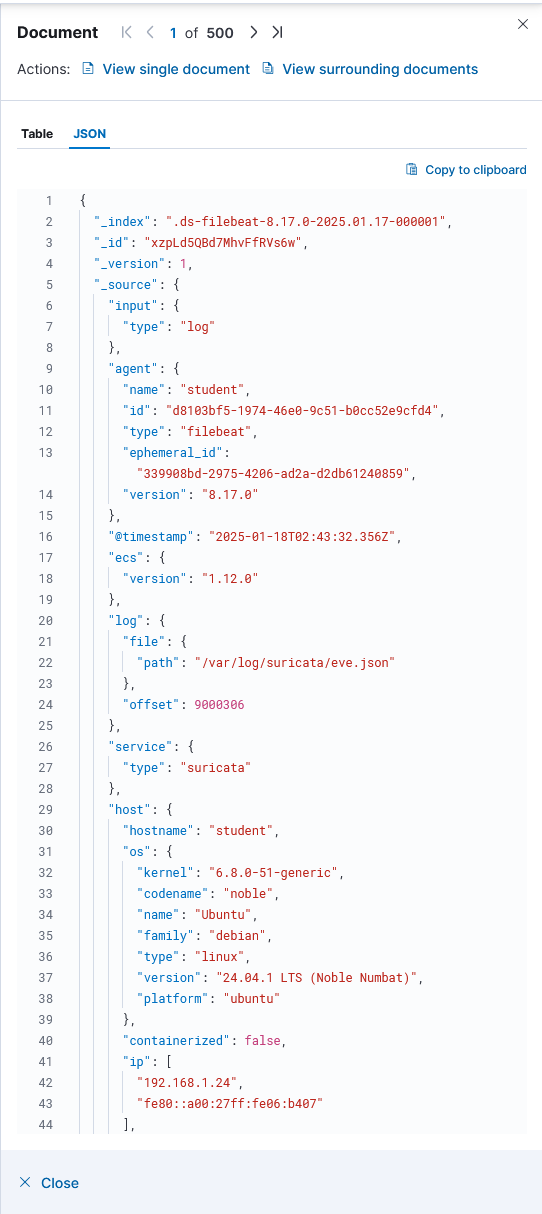
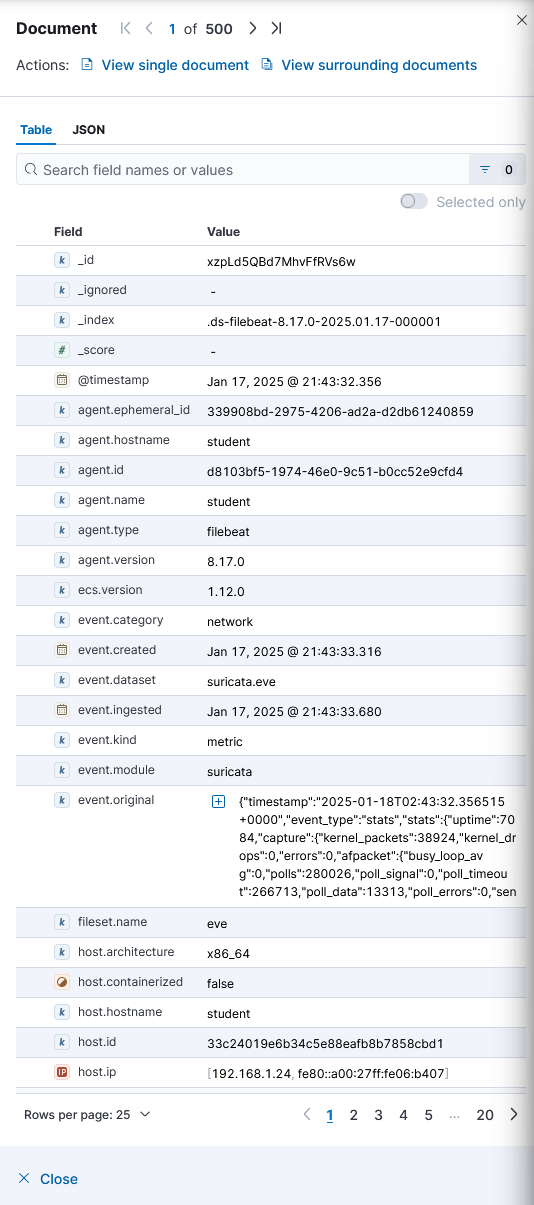


Let’s explore our data on the dashboard:



Let’s take a deeper dive and look at the logs:

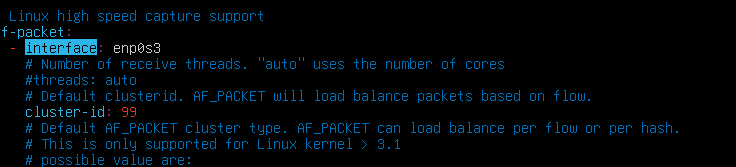
Click on the hamburger icon on the top left and navigate to “Discover” under “Analytics”:  
  


Here is a sample log, we can view this data in Table format or JSON:  
  


You can build your own queries using KQL syntax, I encourage you to play around and explore, happy hunting!

## **Step 5: Install and Configure Suricata (Optional)**

* + Install Suricata:  
     sudo apt install suricata -y
  + Configure Suricata to monitor traffic on your interface:  
     sudo vi /etc/suricata/suricata.yaml



* + Enable event log in JSON format + collect all event types:



* + Start Suricata:  
    sudo systemctl start suricata

sudo systemctl enable suricata