
Network Device Log Monitoring Using ELK

Project Report

Created by: Omkar Hase , Yash Chandane

Course: PG Diploma in IT Infrastructure, Systems & Security

---

1. Introduction

This project focuses on the implementation of a network device log monitoring system using the ELK (Elasticsearch, Logstash, Kibana) stack on Fedora. The purpose is to collect logs from network devices such as routers and switches and visualize the data for better analysis and monitoring.

2. Objectives

- Install and configure the ELK stack on a Fedora system.
- Collect and parse logs from network devices (routers/switches) using Logstash.
- Store the logs in Elasticsearch and create visualizations using Kibana.
- Enable real-time monitoring of network traffic and logs.

3. Environment Setup

- **Operating System**: Fedora 38
- **Tools Used**:
    - **Elasticsearch 7.x**
    - **Logstash 7.x**
    - **Kibana 7.x**
    - Network Devices: Cisco and Juniper Routers

---

4. ELK Stack Installation

4.1 Install Java

The ELK stack requires Java, which is installed as follows:

- sudo dnf install java-11-openjdk-devel -y

4.2 Install Elasticsearch

sudo rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch

```
sudo tee /etc/yum.repos.d/elasticsearch.repo <<EOF
[elasticsearch-7.x]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF
sudo dnf install elasticsearch -y
sudo systemctl enable --now elasticsearch
```

4.3 Install Logstash

```
sudo dnf install logstash -y
sudo systemctl enable --now logstash
```

4.4 Install Kibana

```
sudo dnf install kibana -y
sudo systemctl enable --now kibana
```

6. Logstash Configuration

A Logstash configuration file was created to capture the syslogs from network devices, parse them, and send them to Elasticsearch.

6.1 Logstash Configuration File

```
sudo nano /etc/logstash/conf.d/network-device-logs.conf
```

The content of the file:

```
input {
  udp {
    port => 514
    type => "syslog"
  }
```

```
}


filter {
  if [type] == "syslog" {
    grok {
      match => { "message" => "%{SYSLOGTIMESTAMP:timestamp} %{SYSLOGHOST:hostname} %{DATA:program}: %{GREEDYDATA:log_message}" }
    }
    date {
      match => [ "timestamp", "MMM  d HH:mm:ss", "MMM dd HH:mm:ss" ]
    }
  }
}


output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "network-device-logs-%{+YYYY.MM.dd}"
  }
  stdout { codec => rubydebug }
}
```

The above configuration ensures logs are received on UDP port 514, parsed, and indexed into Elasticsearch.

7. Kibana Setup and Visualization

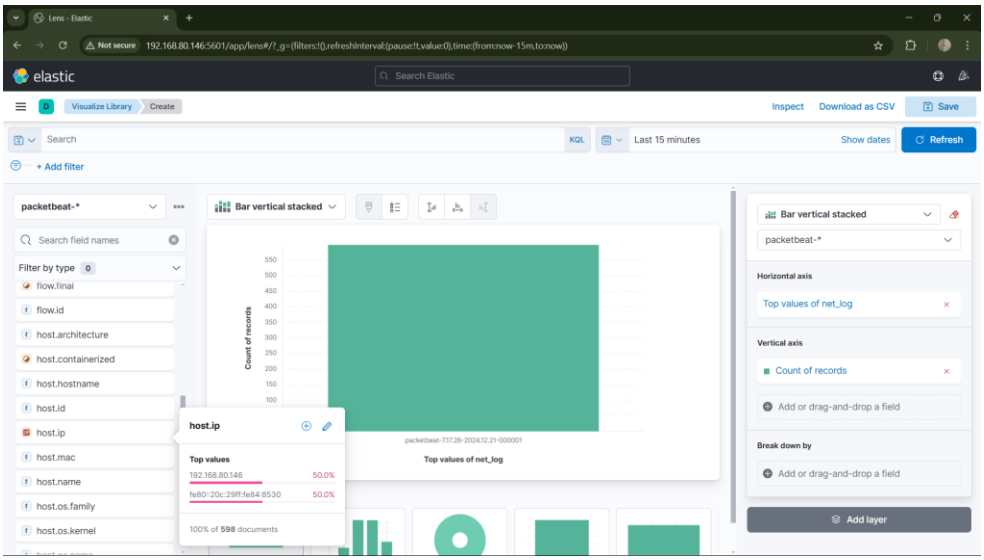
7.1 Access Kibana

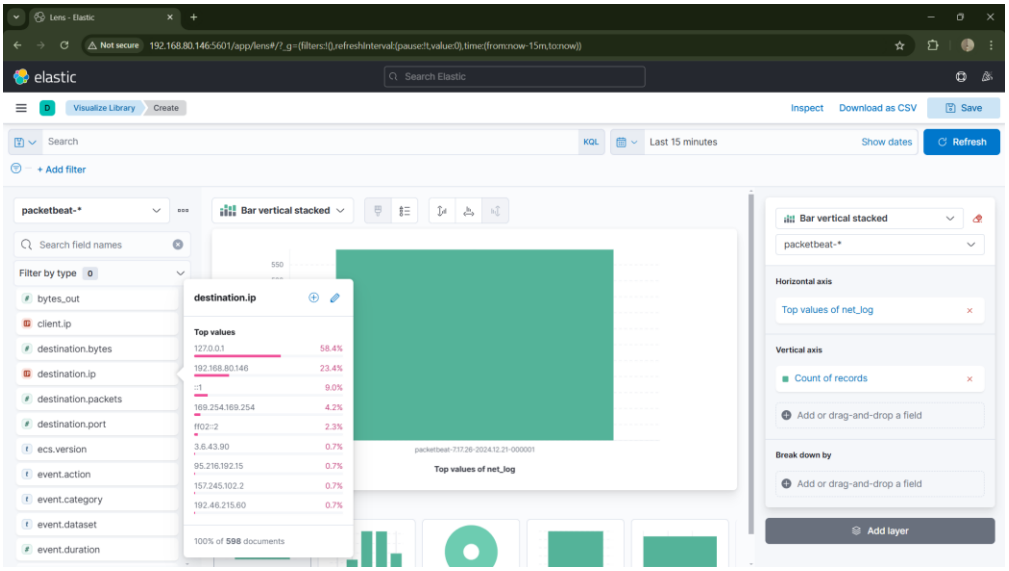
Kibana was accessed via http://192.168.80.146:5601 and the following steps were performed:

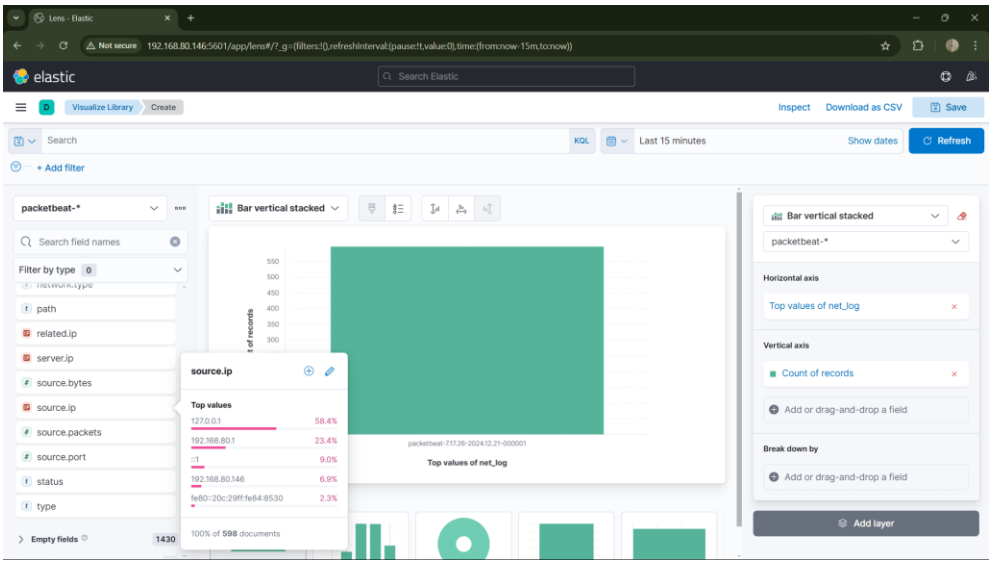
1. **Create Index Pattern**:
    - Navigate to **Management** > **Index Patterns** and create a pattern for network-device-logs-*.
    - Set the timestamp field to @timestamp.

2. **Visualizations**:

    - Visualizations such as bar charts and pie charts were created based on fields like hostname, program, and log message.







8. Troubleshooting

8.1 Logstash Not Processing Logs

- Ensure that the correct path to the logs is provided and that Logstash has the appropriate permissions.

8.2 Elasticsearch Not Running

- Restart Elasticsearch if needed:
- sudo systemctl restart elasticsearch

8.3 Kibana Visualization Issues

- Ensure the index pattern in Kibana is correctly pointing to network-device-logs-*.

9. Conclusion

The project successfully implemented a network device log monitoring system using ELK on Fedora. Logs were captured from network devices, processed, and visualized using Kibana. This solution provides real-time insights into network activity, helping in proactive monitoring and troubleshooting.