Syslog Server with Elastic Stack and Kibana Setup Guide

This document provides a step-by-step guide to setting up a Syslog Server on an Ubuntu Server with the Elastic Stack (Elasticsearch, Logstash, Kibana) for centralized log collection and visualization. Logs from various devices, such as firewalls and Active Directory servers, will be forwarded to the syslog server for further processing and visualized in Kibana.

Features

- Syslog collection from network devices, firewalls, and servers.
- Centralized storage of logs using **Elasticsearch**.
- Log visualization in real-time using **Kibana**.
- Step-by-step guide for setting up the server and connecting devices.

1. Install and Configure Syslog Server

- Update the system:

    $ sudo apt update

    $ sudo apt upgrade

- Install rsyslog:

    $ sudo apt install rsyslog

- Configure rsyslog to receive remote logs by editing /etc/rsyslog.conf file:

    $ sudo nano /etc/rsyslog.conf

Uncomment the following lines:

$ModLoad imudp

$UDPServerRun 514

$ModLoad imtcp

$InputTCPServerRun 514

- Restart rsyslog service:

$ sudo systemctl restart rsyslog

$ sudo systemctl enable rsyslog

2. Install and Configure Elasticsearch

- Install Elasticsearch:

$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -

$ sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.list'

$ sudo apt update

$ sudo apt install elasticsearch

- Configure Elasticsearch (set network.host):

$ sudo nano /etc/elasticsearch/elasticsearch.yml

Add: network.host: 0.0.0.0

- Start and enable Elasticsearch:

$ sudo systemctl start elasticsearch

$ sudo systemctl enable elasticsearch

- Test Elasticsearch by accessing:

  http://<your-ubuntu-server-ip>:9200

3. Install and Configure Logstash

- Install Logstash:

  $ sudo apt install logstash

- Create Logstash configuration file:

  $ sudo nano /etc/logstash/conf.d/syslog.conf

  Add the following:

```
input {
  udp { port => 514 type => syslog }
  tcp { port => 514 type => syslog }
}
output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "syslog-%{+YYYY.MM.dd}"
  }
}
```

- Start and enable Logstash:

  $ sudo systemctl start logstash

  $ sudo systemctl enable logstash

4. Install and Configure Kibana

- Install Kibana:

    $ sudo apt install kibana

- Configure Kibana (set server.host):

    $ sudo nano /etc/kibana/kibana.yml

    Add: server.host: "0.0.0.0"

- Start and enable Kibana:

    $ sudo systemctl start kibana

    $ sudo systemctl enable kibana

- Access Kibana by navigating to:

    http://<your-ubuntu-server-ip>:5601

5. Configure Firewalls to Forward Logs to Syslog Server

- For Ubuntu (using UFW):

    $ sudo ufw allow 514/udp

    $ sudo ufw allow 514/tcp

    $ sudo ufw reload

- For FortiGate Firewalls:

  Set up remote logging to the syslog server IP on port 514.

- For Active Directory Servers:

  Use NXLog or Winlogbeat to forward Windows Event Logs:

    Example NXLog Configuration:

      <Output syslog>

        Module om_udp

        Host <syslog_server_ip>

        Port 514

        Exec $Message = to_syslog_ietf();

      </Output>

6. Visualize Logs in Kibana

- In Kibana, go to Management > Index Patterns.
- Create an index pattern for syslog logs (e.g., syslog-*).
- After creating the index pattern, use Discover to view logs in real-time.

Conclusion

By following this guide, you can successfully set up a Syslog Server with Elastic Stack and Kibana to collect, store, and visualize logs from various network devices and servers. This setup is crucial for monitoring and troubleshooting network infrastructure.

License

For any questions or further assistance, reach out to:

nithyananthannagarajan092@gmail.com