Installing ELK With Ubuntu and Nginx WIth Filebeat
Intro

The ELK stack is a set of three open-source technologies that are commonly used together for managing large amounts of data. It's an acronym that stands for Elasticsearch, Logstash, and Kibana.

Elasticsearch is a powerful search engine that can store, search, and analyze large volumes of data. Logstash is a tool that can process data from different sources and prepare it for Elasticsearch. Finally, Kibana is a data visualization platform that helps users explore and analyze data stored in Elasticsearch.

The ELK stack is used in a variety of applications, such as analyzing logs, monitoring system performance, and tracking user behavior. By combining these three tools, users can quickly identify and troubleshoot problems and gain valuable insights into their data.

#Elasticsearch: A distributed, open-source search and analytics engine that is used to store, search, and analyze large volumes of data.

#Logstash: A data processing pipeline that collects, filters, and transforms data from multiple sources, such as logs, metrics, and other data sources, and sends it to Elasticsearch.

#Kibana: A data visualization and exploration platform that allows users to analyze and visualize the data stored in Elasticsearch, including dashboards, charts, and graphs.

##Nginx

NGINX is a type of software that helps serve websites and applications on the internet. It's like a traffic cop that directs visitors to the right place. NGINX can handle a lot of visitors at once and is really good at delivering web pages and other content quickly and reliably.

It's used by many popular websites and applications that need to handle a lot of traffic and deliver content quickly, like online marketplaces, social networks, and media sites. It's also flexible and can be customized to do a lot of different things, like load balancing (making sure requests are distributed evenly across multiple servers) and caching (storing frequently accessed content for faster delivery).

##Filebeat

Filebeat is a tool that helps collect and manage log data from different sources in a distributed system. It's like a courier that picks up log data from different sources, such as servers or applications, and delivers it to a central location for analysis and visualization.

Filebeat is designed to be easy to use and doesn't take up a lot of resources, so it won't slow down the system it's running on. It can monitor log files, metrics, and other types of data, and supports a variety of popular log formats.

Filebeat is often used by developers and IT teams to monitor and analyze log data, which can help them identify issues, track performance, and gain insights into their applications and systems.

###Lets Get Into The Job

```
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/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
```

```
sudo apt update
```

```
sudo apt install elasticsearch
```

## Edit config file of elastic search

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

Change the value of
Uncomment network.host and replace existing value with localhost or 127.0.0.1

```
. . .
# ---------------------------------- Network
-----------------------------------
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
network.host: localhost

. . .
```

```
sudo systemctl start elasticsearch

sudo systemctl enable elasticsearch
```

##Now Time To Install KIbana

```
sudo apt install kibana

sudo systemctl enable kibana

sudo systemctl start kibana
```

#We will be Using Nginx Webserver this project Optional

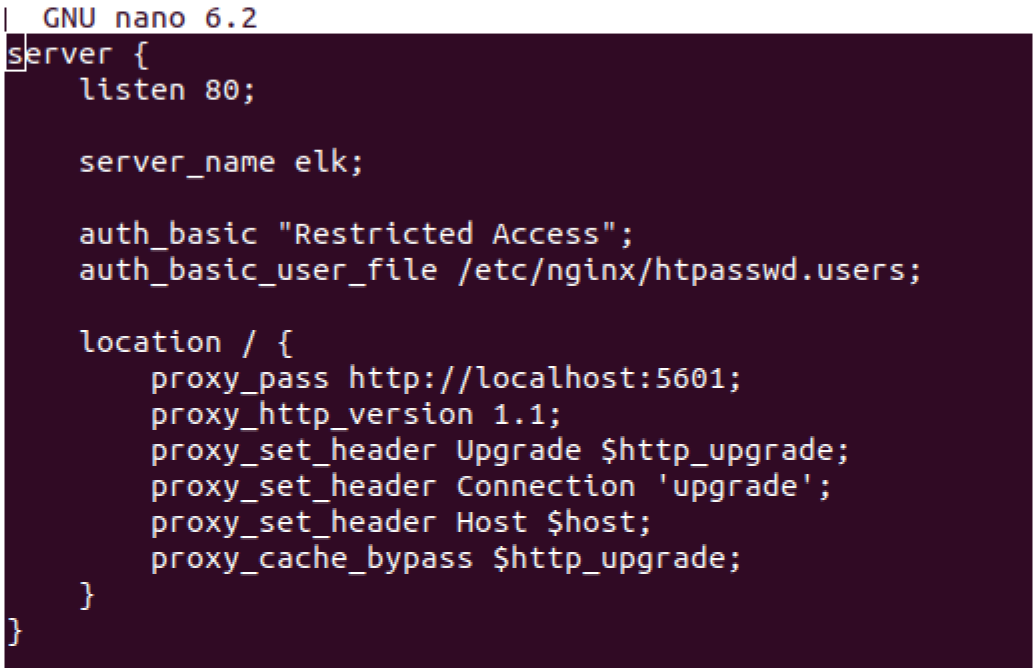
```
sudo apt update

sudo apt-get install nginx

echo "kibanaadmin:`openssl passwd -apr1`" | sudo tee -a
/etc/nginx/htpasswd.users

sudo nano /etc/nginx/sites-available/elk
```

```
server {
    listen 80;
    server_name elk;
    auth_basic "Restricted Access";
    auth_basic_user_file /etc/nginx/htpasswd.users;
    location / {
        proxy_pass http://localhost:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```



```
server {
    listen 80;

    server_name elk;

    auth_basic "Restricted Access";
    auth_basic_user_file /etc/nginx/htpasswd.users;

    location / {
        proxy_pass http://localhost:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

```
sudo ln -s /etc/nginx/sites-available/elk /etc/nginx/sites-enabled/elk
```

```
sudo nginx -t
```

```
sudo systemctl reload nginx
```

##Now You can access status of Kibana

http://localhost:5601/status

#Lets Install Logstash

sudo apt install logstash

```
sudo nano /etc/logstash/conf.d/02-beats-input.conf
```

##Paste This Configuaration

input {

```
  beats {
    port => 5044
  }
}
```

```
sudo nano
/etc/logstash/conf.d/30-elasticsearch-output.conf
```

```
##Paste This
```

```
output {
  if [@metadata][pipeline] {
      elasticsearch {
      hosts => ["localhost:9200"]
      manage_template => false
      index =>
"%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
      pipeline => "%{[@metadata][pipeline]}"
      }
  } else {
      elasticsearch {
      hosts => ["localhost:9200"]
      manage_template => false
      index =>
"%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
      }
  }
}
```

#Test your Logstash configuration with this command

```
sudo -u logstash /usr/share/logstash/bin/logstash
--path.settings /etc/logstash -t
```

```
sudo systemctl start logstash
sudo systemctl enable logstash
```

##Installing Filebeat

```
sudo apt install filebeat
```

##Edit Filebeat Configuration

```
sudo nano /etc/filebeat/filebeat.yml
```

##Comment This

```
...
#output.elasticsearch:
  # Array of hosts to connect to.
  #hosts: ["localhost:9200"]
...
```

##Then FInd `output.logstash and Uncomment`

```
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]
```

```
sudo filebeat modules enable system
```

```
Enabled system
```

```
sudo filebeat modules list
```

```
sudo filebeat setup --pipelines --modules system
```

```
Output
```

```
Index setup finished.
```

```
sudo filebeat setup -E output.logstash.enabled=false -E output.elasticsearch.hosts=['localhost:9200'] -E setup.kibana.host=localhost:5601
```

```
sudo systemctl start filebeat
```

```
sudo systemctl enable filebeat
```

##To verify that Elasticsearch is indeed receiving this data, query the Filebeat index with this command:

```
curl -XGET 'http://localhost:9200/filebeat-*/_search?pretty'
```

http://localhost:5601/

http://localhost:5601/status

If Kibana Dashboard is loading then Congratulation
Welcome To The Kibana

FOR REMOTE ACCEESS

First of all you have to edit "elasticsearch.yml" file.

```
nano /etc/elasticsearch/elasticsearch.yml
```

It should look like this:

"network.host" line must be "0.0.0.0" to allow remote access. You must restart the service to make configuration work.

```
sudo systemctl restart elasticsearch
```

And then you have to edit Kibana's config file which names as "kibana.yml"

```
nano /etc/kibana/kibana.yml
```

```
server.port: 5601
server.host: 0.0.0.0
```

```
sudo systemctl restart kibana
```

After that editing part, then you will be able to access Kibana's Dashboard on a web browser with this

Please replace x.x.x.x with your ELK machine IP address. And if You are using VM then make sure You are in bridge mode in network setting.

```
http://X.X.X.X:5601
```

```
transport.host: localhost

transport.tcp.port: 9300

http.port: 9200

network.host: 0.0.0.0
```

By Yamu Poudel

Lecturer. Herald College Kathmandu

DevOps Chief/Project Manager / Data Engineer #Hello World Corp

Application Architect / Inventor / Founder #TradEngine