**Step 1: Installs: (java, ES, Kibana, Logstash, NGINX,File beat) all in one Debian Box**

**1.1 Java :**

sudo apt update

sudo apt upgrade

sudo apt update

sudo apt install default-jdk

java –version –to make sure java installed with latest version

**apt install curl**

**1.2 Elastic Search/logstash/Kibana/filebeat/NGINX:**

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

sudo apt-get install apt-transport-https

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

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

sudo apt-get update && sudo apt-get install logstash

sudo apt-get update && sudo apt-get install kibana

sudo apt-get update && sudo apt-get install filebeat

***## if you are going to have NGINX then follow the below steps: ##***

sudo apt-get update && sudo apt-get install nginx

apt-get install apache2-utils

htpasswd -c /etc/nginx/conf.d/kibana.htpasswd **<user> # Type the username you wanted in <user>** **it will prompt for password, retype the password and user is added to NGINX**

***Install your SSL certificate and private key:***

***If you have a valid signed certificate, copy your key file <ssl\_key> and your certificate file <ssl\_pem> to their proper locations:***

# mkdir -p /etc/ssl/certs /etc/ssl/private

# cp <ssl\_pem> /etc/ssl/certs/kibana-access.pem

# cp <ssl\_key> /etc/ssl/private/kibana-access.key

***If you do not have a valid signed certificate, create a self-signed certificate as follows:***

# mkdir -p /etc/ssl/certs /etc/ssl/private

# openssl req -x509 -batch -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/kibana-access.key -out /etc/ssl/certs/kibana-access.pem

**STEP 2: Enable al these in Service**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

TO Start ES to start automatically after the computer boots up

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

To check what is running: SystemD or sysV

ps -p 1

Use the update-rc.d command to configure Elasticsearch to start automatically when the system boots up:

if sysV

sudo update-rc.d elasticsearch defaults 95 10

sudo update-rc.d kibana defaults 95 10

To start |stop|status

sudo -i service elasticsearch start |stop|status

sudo -i service kibana start |stop|status

df

if systemD

To create as service

sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable elasticsearch.service

sudo /bin/systemctl enable kibana.service

sudo /bin/systemctl enable logstash.service

sudo /bin/systemctl enable nginx.service

sudo /bin/systemctl enable filebeat.service

**STEP 3: Configuration:**

**/etc/elasticsearch/ElasticSearch.yml**  
  
path.data: /var/lib/elasticsearch  
path.logs: /var/log/elasticsearch  
network.host: 127.0.0.1  
http.port: 9200

**/etc/kibana/Kibana.YML Contents**  
  
server.port: 5601  
server.host: “localhost” #### put "<the box's static IP address>" if NGINX is not used”  
[server.name](http://server.name/): "DeeBuntu ELK"  
elasticsearch.hosts: "[http://127.0.0.1:9200](http://127.0.0.1:9200/)"

**/etc/logstash/logstash.yml**  
  
path.data: /var/lib/logstash  
path.logs: /var/log/ logstash  
pipeline.ordered: auto

**/etc/logstash/conf.d/<<Anyfilename>>.conf**

input {

beats {

port => 5044

#type => syslog

}

}

output {

elasticsearch {

hosts => ["192.168.198.132:9200"] ## if it is not cluster put the Local host

manage\_template => true

index => "logstash-%{+YYYY.MM.dd}"

user => "elastic"

password => "changeme"

}

}

To test: ./logstash first-pipeline.conf --config.test\_and\_exit

**/etc/filebeats/filebeats.yml**

filebeat.inputs:

- type: log

enabled: true

paths:

- /var/log/\*.log

- /var/log/logstash/\*.log

- /var/log/elasticsearch/\*.log

- /var/log/kibana/\*.log

- /var/log/nginx/\*.log

output.logstash:

hosts: ["localhost:5044"]

//NGINX

**/etc/nginx/sites-available/default**

server {

listen 80;

listen [::]:80;

return 301 https://$host$request\_uri;

}

server {

listen 443 default\_server;

listen [::]:443;

ssl on;

ssl\_certificate /etc/ssl/certs/kibana-access.pem;

ssl\_certificate\_key /etc/ssl/private/kibana-access.key;

access\_log /var/log/nginx/nginx.access.log;

error\_log /var/log/nginx/nginx.error.log;

location / {

auth\_basic "Restricted";

auth\_basic\_user\_file /etc/nginx/conf.d/kibana.htpasswd;

proxy\_pass http://localhost:5601/;

}

}

**STEP 4: Test Running**

To start|stop|status as service

sudo systemctl start|stop|status elasticsearch.service

sudo systemctl start|stop|status kibana.service

sudo systemctl start|stop|status logstash.service

apt install curl

apt install ufw

sudo ufw disable

//it allows all port

//if you want any specific ports then use the following comments:

sudo ufw allow 22

sudo ufw allow 9200

sudo ufw allow 9300

sudo ufw allow 9400

sudo ufw allow 5601

sudo ufw allow 5044

sudo ufw allow 5600

https://<<Static IPADddress>>/app/kibana#/home

ES Cluster:

cluster.name: PD-Cluster  
node.name: ES-Node2  
node.master: true  
node.data: true  
path.data: /var/lib/elasticsearch  
path.logs: /var/log/elasticsearch

network.host: 192.168.10.105  
http.port: 9200  
discovery.seed\_hosts: ["192.168.10.104", "192.168.10.105","192.168.10.106"]  
cluster.initial\_master\_nodes: ["192.168.10.104", "192.168.10.105"]

**Trouble shoot**

**Whenever you add new node or when data is full:**

#### Always stop elasticsearch

rm -rf /var/log/elasticsearch/\*

rm -rf /var/lib/elasticsearch/\*

``````` restart elasticsearch

**Winlog/Filebeats debug**

To debug winlogbeats:

.\winlogbeat -e -c winlogbeat.yml

To debug filebeats:

.\filebeat.exe -e test config

To start as service

Start-Service filebeat

To stop

STop-Service filebeat

**When any VM is not able to reach from outside:**

1. Check the network is set as follows:
   1. Address: IP Address
   2. NetMask: 24
   3. Gateway: <<XX:XX:XX:1>>
   4. DNS: 8.8.8.8