Installation in ubuntu 18.04 servers

1. IP plan

a. Wazuh server: 172.16.7.25
b. ELK server: 172.16.7.26
c. Agent installed on ubuntu Client : 172.16.7.24

2. Wazuh server: 172.16.7.25:

Wazuh server Installation

a. Prerequisites:
   i. `# apt-get update`
   ii. `# apt-get install curl apt-transport-https lsb-release gnupg2`
b. Install the GPG key
   i. `# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -`
c. Add the repository:
   i. `# echo "deb https://packages.wazuh.com/3.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list`
d. Update the package information:
   i. `# apt-get update`
e. Install the Wazuh manager:

i. `# apt-get install wazuh-manager`

f. Check for service status

i. `# systemctl status wazuh-manager`

g. Add official NodeJS repository:

i. `# curl -sL https://deb.nodesource.com/setup_10.x | bash -`

h. Install NodeJS

i. `# apt-get install nodejs`

i. Install the Wazuh API

i. `# apt-get install wazuh-api`

j. Check for service status

i. `# systemctl status wazuh-api`

k. Secure the wazuh API (enable https with self signed cert and set username and password for API connection)

i. `# /var/ossec/api/scripts/configure_api.sh`

l. Restart service

i. `# systemctl restart wazuh-api`

m. Test wazuh server is running properly:

i. `https://172.16.7.25:55000`

Filebeat Installation

n. Add the Elastic repository and its GPG key:

i. `# apt-get install curl apt-transport-https`

ii. `# curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -`

iii. `# echo "deb https://artifacts.elastic.co/packages/7.x/apt`

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

iv. `# apt-get update`

o. Install Filebeat:

i. `# apt-get install filebeat=7.9.1`

p. Download the Filebeat config file from the Wazuh repository. This is pre-configured to forward Wazuh alerts to Elasticsearch:

i. `# curl -so /etc/filebeat/filebeat.yml https://raw.githubusercontent.com/wazuh/wazuh/v3.13.2/extensions/filebeat/7.x/filebeat.yml`

q. Download the alerts template for Elasticsearch:

i. `# curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/v3.13.2/extensions/elasticsearch/7.x/wazuh-template.json`

r. Download the Wazuh module for Filebeat:

i. `# curl -s https://packages.wazuh.com/3.x/filebeat/wazuh-filebeat-0.1.tar.gz | sudo tar -xvz -C /usr/share/filebeat/module`

s. Edit the file /etc/filebeat/filebeat.yml and replace with the IP address or the hostname of the Elasticsearch server. For example:

i.
```
# vi /etc/filebeat/filebeat.yml
      output.elasticsearch.hosts:
      ['http://172.16.7.26:9200']
```

t. Enable and start the Filebeat service:

i. `# systemctl daemon-reload`

ii. `# systemctl enable filebeat.service`

iii. `# systemctl start filebeat.service`

u. Once Elasticsearch is up and running, load the Filebeat template by running following command on wazuh server.

i. `# filebeat setup --index-management -E setup.template.json.enabled=false`

3. ELK server: 172.16.7.26

Install Elasticsearch

a. Add the Elastic repository and its GPG key:

i. `# rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch`

ii.
```
# cat > /etc/yum.repos.d/elastic.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
```

b. Install the Elasticsearch package:

   i. `# yum install elasticsearch-7.9.1`

c. Elasticsearch will only listen on the loopback interface (localhost) by default. Configure Elasticsearch to listen to a non-loopback address by editing the file /etc/elasticsearch/elasticsearch.yml and uncommenting the setting network.host. Change the value to the IP you want to bind it to:

   i.
```
# vi /etc/elasticsearch/elasticsearch.yml
network.host: 172.16.7.26
http.port: 9200
```

d. Add or edit (if commented) the following lines in the file /etc/elasticsearch/elasticsearch.yml:

   i.
```
# vi /etc/elasticsearch/elasticsearch.yml
node.name: wazuh
cluster.initial_master_nodes: ["wazuh"]
```

e. Enable and start the Elasticsearch service:

   i. `# systemctl daemon-reload`
   ii. `# systemctl enable elasticsearch.service`
   iii. `# systemctl start elasticsearch.service`

f. Ensure elasticsearch is running

   i. `http://172.16.7.26:9200`

g. Now, in wazuh server(172.16.7.25) load the filebeat template, as mentioned earlier in filebeat installation.

Install Kibana:

h. Install the Kibana package:

   i. `# yum install kibana-7.9.1`

i. Update the optimize and plugins directories permissions:

   i. `# chown -R kibana:kibana /usr/share/kibana/optimize`

   ii. `# chown -R kibana:kibana /usr/share/kibana/plugins`

j. Install the Wazuh app plugin for Kibana from URL:

   i. `# cd /usr/share/kibana/`

   ii. `# sudo -u kibana bin/kibana-plugin install https://packages.wazuh.com/wazuhapp/wazuhapp-3.13.2_7.9.1.zip`

k. Configure Kibana to listen on its network interface IP :

   i. `# vi /etc/kibana/kibana.yml`

```
server.port: 5601
server.host: "172.16.7.26"
server.name: "wazuh kibana"
elasticsearch.hosts:
["http://172.16.7.26:9200"]
```

l. Enable and start the Kibana service:

   i. `# systemctl daemon-reload`

   ii. `# systemctl enable kibana.service`

   iii. `# systemctl start kibana.service`

4. Set up the wazuh App:

In the elk server edit the following file as per api user and password you have set and provide wazuh server ip address and port:

a. # vi /usr/share/kibana/optimize/wazuh/config/wazuh.yml

```
hosts:
  - default:
      url: https://172.16.7.25
      port: 55000
      user: wazuh
      password: eiytdvdR5?yu5
```

5. Secure ELK using X-Pack

Configure the instance you want to secure:

a. # vi /usr/share/elasticsearch/instances.yml

```
instances:
    - name: "wazuh"
      ip:
        - "172.16.7.25"
    - name: "elasticsearch"
      ip:
        - "172.16.7.26"
    - name: "kibana"
      ip:
        - "172.16.7.26"
```

b. Generate the Certificates:

i. # /usr/share/elasticsearch/bin/elasticsearch-certutil cert --pem --in instances.yml --out certs.zip --keep-ca-key

c. Extract the certificates:

i. # unzip /usr/share/elasticsearch/certs.zip -d /usr/share/elasticsearch/

d. Configure elastic search instance

i. # mkdir /etc/elasticsearch/certs/ca -p
ii. # cp ca/ca.crt /etc/elasticsearch/certs/ca
iii. # cp elasticsearch/elasticsearch.crt /etc/elasticsearch/certs

iv. `# cp elasticsearch/elasticsearch.key /etc/elasticsearch/certs`

v. `# chown -R elasticsearch: /etc/elasticsearch/certs`

vi. `# chmod -R 770 /etc/elasticsearch/certs`

vii. Add following to end of `/etc/elasticsearch/elasticsearch.yml`

```
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mo
de: certificate
xpack.security.transport.ssl.key:
/etc/elasticsearch/certs/elasticsearch.key
xpack.security.transport.ssl.certificate:
/etc/elasticsearch/certs/elasticsearch.crt
xpack.security.transport.ssl.certificate_aut
horities: [
"/etc/elasticsearch/certs/ca/ca.crt" ]

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.verification_mode:
certificate
xpack.security.http.ssl.key:
/etc/elasticsearch/certs/elasticsearch.key
xpack.security.http.ssl.certificate:
/etc/elasticsearch/certs/elasticsearch.crt
xpack.security.http.ssl.certificate_authorit
ies: [ "/etc/elasticsearch/certs/ca/ca.crt"
]
```

viii. Restart the service

```
# systemctl restart elasticsearch
```

e. Configure Kibana Instance:

i. `# mkdir /etc/kibana/certs/ca -p`

ii. `# cd /usr/share/elasticsearch/`

iii. `# cp ca/ca.crt /etc/kibana/certs/ca`

iv. `# cp kibana/kibana.crt /etc/kibana/certs`

v. `# cp kibana/kibana.key /etc/kibana/certs`

vi. `# chown -R kibana: /etc/kibana/certs`

vii. `# chmod -R 770 /etc/kibana/certs`

viii. Make following changes to /etc/kibana/kibana.yml

```
elasticsearch.hosts:
["https://172.16.7.26:9200"]
elasticsearch.ssl.certificateAuthorities:
["/etc/kibana/certs/ca/ca.crt"]
elasticsearch.ssl.certificate:
"/etc/kibana/certs/kibana.crt"
elasticsearch.ssl.key:
"/etc/kibana/certs/kibana.key"

server.ssl.enabled: true
server.ssl.certificate:
"/etc/kibana/certs/kibana.crt"
server.ssl.key:
"/etc/kibana/certs/kibana.key"
```

ix. Restart the service

```
# systemctl restart kibana
```

f. Configure Filebeat installed on wazuh server

Copy certificates and keys from elk server to wazuh server

```
# cd /usr/share/elasticsearch
# scp -r ca  wazuh  wazuh@172.16.7.25:/home/wazuh
```

g. Configure the filebeat

i. `# mkdir /etc/filebeat/certs/ca -p`
ii. `# cd /home/wazuh`
iii. `# cp ca/ca.crt /etc/filebeat/certs/ca`
iv. `# cp wazuh-manager/wazuh.crt /etc/filebeat/certs`
v. `# cp wazuh-manager/wazuh.key /etc/filebeat/certs`
vi. `# chmod 770 -R /etc/filebeat/certs`

vii. Make the following changes to /etc/filebeat/filebeat.yml:

```
output.elasticsearch.hosts:
['172.16.7.26:9200']
output.elasticsearch.protocol: https
output.elasticsearch.ssl.certificate:
"/etc/filebeat/certs/wazuh.crt"
output.elasticsearch.ssl.key:
"/etc/filebeat/certs/wazuh.key"
output.elasticsearch.ssl.certificate_authori
ties: ["/etc/filebeat/certs/ca/ca.crt"]
```

h. Restart the service:

```
# systemctl restart filebeat
```

i. Add Authentication for Elastic Stack:

i. `# vi /etc/elasticsearch/elasticsearch.yml`

```
xpack.security.enabled: true
```

j. Restart Elasticsearch
   i. `# systemctl restart elasticsearch`

k. Auto generate credentials for all prebuilt users and roles

```
# /usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto
```

Changed password for user elastic

PASSWORD elastic = He7FY50syQ4dI9oWRIqA

**** Note down the passwords*******

l. Setup the credentials for filebeat and Kibana
   i. `# vi /etc/filebeat/filebeat.yml`

```
output.elasticsearch.username: "elastic"
output.elasticsearch.password:
"He7FY50syQ4dI9oWRIqA"
```

   ii. Restart filebeat

```
# systemctl restart filebeat
```

   iii. `# vi /etc/kibana/kibana.yml`

```
xpack.security.enabled: true
elasticsearch.username: "elastic"
elasticsearch.password:
"He7FY50syQ4dI9oWRIqA"
```

   iv. Restart Kibana

```
# systemctl restart kibana
```