frosky / **ELK-Installation** Public

Code Issues Pull requests Actions Projects Security Insights

main ▾ ···

ELK-Installation / **SIEM.md**

frosky Add files via upload

1 contributor

193 lines (118 sloc) | 4.47 KB ···

installation of ELK SIEM

1: Installing the required modules

update the system packages; sudo apt-get update

Install openjdk and other dependencies before installing elastic stack; sudo apt-get install openjdk-11-jdk sudo apt-get install wget sudo apt-get install apt-transport-https sudo apt-get install curl sudo apt-get install gnupg2

install all above listed modules in one command; sudo apt-get install openjdk-11-jdk wget apt-transport-https curl gnupg2 -y

check java version; java -version

2: Install and Configure ElasticSearch on Ubuntu

First we will have to add a signing key and will have to add repositories to our system because Elasticsearch is not pre-installed in Ubuntu, we will have to do it manually.

Follow the below command to add elasticsearch signing key; wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch --no-check-certificate | sudo apt-key add -

Next add the repository in /etc/apt/sources.list.d/elastic-7.x.list using below command; echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

after running the repo update the system package; sudo apt-get update -y

Install elasticsearch; sudo apt-get install elasticsearch -y

Do modifications on elesticsearch configuration file; sudo nano /etc/elasticsearch/elasticsearch.yml

change this; ---Network section--- network.host: localhost http.port: 9200(remove '#' here)

add this line; --- Discovery --- discovery.type: single-node

save config file and exit.

start the elacticsearch service; sudo systemctl start elasticsearch

To enable elacticsearch at system startup; sudo systemctl enable elasticsearch

To check elasticsearch service pid; sudo systemctl status elasticsearch

3: Install and Configure Kibana on Ubuntu

install kibana on Ubuntu; sudo apt-get install kibana

Do modifications on kibana configuration file; sudo nano /etc/kibana/kibana.yml

remove '#' in the below lines; server.port: 5601 server.host: "localhost" elasticsearch.hosts: ["http://localhost:9200"]

save config file and exit.

start kibana service; sudo systemctl start kibana

To enable kibana at system startup; sudo systemctl enable kibana

To check the status of kibana service; sudo systemctl status kibana

4: Install and Configure Logstash on Ubuntu

install logstash on ubuntu; sudo apt-get install logstash

Create the below config file and insert below lines to load logstash beat; sudo nano /etc/logstash/conf.d/2-beats-input.conf

input {

beats {

```
port => 5044
```

}

}

save and close the file.

sudo nano /etc/logstash/conf.d/2-elasticsearch-output.conf

output {

elasticsearch {

```
hosts => ["localhost:9200"]

manage_template => false

index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
```

}

}

save and close the editor.

start logstash service; sudo systemctl start logstash

To enable logstash at system startup; sudo systemctl enable logstash

To stop logstash service; sudo systemctl stop logstash (do not run this unless its necessary)

To check status of logstash; sudo systemctl status logstash

5: Install and Configure Filebeat on Ubuntu

install Filebeat to send logs to Logstash; sudo apt-get install filebeat

Do modifications on filebeat configuration file; sudo nano /etc/filebeat/filebeat.yml

Comment the below lines

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

Uncomment the below lines

output.logstash: hosts: ["localhost:5044"]

save & exit editor.

start filebeat service; sudo systemctl start filebeat

To enable filebeat at system startup; sudo systemctl enable filebeat

To check status of filebeat service; sudo systemctl status filebeat

Enable filebeat system module; sudo filebeat modules enable system

Enable filebeat logstash module; sudo filebeat modules enable logstash

Load the index template; filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'

start filebeat service; sudo service filebeat start

check whether elasticsearch is recieving datalog from filebeat; curl -XGET http://localhost:9200/_cat/indices?v

Access Kibana Web Interface by using the URL http://localhost:5601

execute the below command if integration check gave an error Enable filebeat kibana module; sudo filebeat modules enable kibana

Give feedback