Elk stack

ELK

install java

```
Add the following line to /etc/apt/sources.list:

deb http://debian.opennms.org/ stable main

wget -O - http://debian.opennms.org/OPENNMS-GPG-KEY | sudo apt-key add -

sudo apt-get update

sudo apt-get install oracle-java8-installer
```

- .

. .

Install Elasticsearch

```
sudo 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/6.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d
/elastic-6.x.list
sudo apt-get update
sudo apt-get install elasticsearch
```

- .

```
cd /usr/share/elasticsearch/bin/
./elasticsearch-setup-passwords auto
```

- .

```
Changed password for user apm_system
PASSWORD apm_system = PCj10gOqouXsjJucfjVDx

Changed password for user kibana_system
PASSWORD kibana_system = Mg7hGEyPcAdgE42l8jnxx

Changed password for user kibana
PASSWORD kibana = Mg7hGEyPcAdgE42l8jnxx

Changed password for user logstash_system
PASSWORD logstash_system = c8vL705G717E8lf3S8Hsx

Changed password for user beats_system
PASSWORD beats_system = BLyXYkabW8XyVYg1jnhFx

Changed password for user remote_monitoring_user
PASSWORD remote_monitoring_user = vD9ca95aHj5wCIkOWglUxx

Changed password for user elastic
PASSWORD elastic = WhqSZGDhbiEZcdHpVGgCx
```

.

/etc/elasticsearch/elasticsearch.yml

```
vi /etc/elasticsearch/elasticsearch.yml

xpack.security.enabled: true
```

```
Mount –o remount,exec /tmp

sudo systemctl enable elasticsearch.service

sudo systemctl start elasticsearch.service
```

```
sudo curl -XGET 'localhost:9200/?pretty'

{

"name" : "UHR2XBB",

"cluster_name" : "elasticsearch",

"cluster_uuid" : "Ranc0Jh9QAuuMYhALcZIRA",

"version" : {

"number" : "6.2.4",

"build_hash" : "ccec39f",

"build_date" : "2018-04-12T20:37:28.497551Z",

"build_snapshot" : false,

"lucene_version" : "7.2.1",

"minimum_wire_compatibility_version" : "5.6.0",

"minimum_index_compatibility_version" : "5.0.0"

},

"tagline" : "You Know, for Search"

}
```

.

install kibana:

```
sudo apt-get install kibana


sudo vim /etc/kibana/kibana.yml
```

```
server.port: 5601

server.host: "192.168.110.174"

elasticsearch.username: "elastic"
elasticsearch.password: "WhqSZGDhbiEZcdHpVGgC"
```

.

```
sudo systemctl enable kibana.service


sudo systemctl start kibana.service
```

```
sudo apt-get install logstash

vi /etc/logstash/conf.d/logstash.conf
```

```
input {

beats {

port => 5044

type => syslog

ssl => true

ssl_certificate => "/etc/ssl/logstash-forwarder.crt"

ssl_key => "/etc/ssl/logstash-forwarder.key.pem"

}

}

filter {

if [type] == "syslog" {

grok {

match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp} %{SYSLOGHOST:syslog_hostname} %{DATA:
syslog_program}(?:\[%{POSINT:syslog_pid}\])?: %{GREEDYDATA:syslog_message}" }

add_field => [ "received_at", "%{@timestamp}" ]

add_field => [ "received_from", "%{host}" ]

}

date {

match => [ "syslog_timestamp", "MMM d HH:mm:ss", "MMM dd HH:mm:ss" ]

}

}

}


output {

elasticsearch { hosts => ["localhost:9200"]

hosts => "localhost:9200"

user => "elastic"

password => "WhqSZGDhbiEZcdHpVGgC"

manage_template => false

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

document_type => "%{[@metadata][type]}"

}

}
```

```
vi /etc/logstash/pipelines.yml# This file is where you define your pipelines. You can define multiple.
# For more information on multiple pipelines, see the documentation:
# https://www.elastic.co/guide/en/logstash/current/multiple-pipelines.html

- pipeline.id: syslog-pipeline
path.config: "/etc/logstash/conf.d/syslog.conf"
- pipeline.id: apache-access-pipeline
path.config: "/etc/logstash/conf.d/apache-access.conf"
```

```
sudo systemctl enable logstash.service


sudo systemctl start logstash.service
```

install filebeat

```
sudo vim /etc/hosts
```

```
192.168.110.174 elk-server
```

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


sudo apt-get install apt-transport-https


sudo echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d
/elastic-6.x.list


sudo apt-get update


sudo apt-get install filebeat
```

```
sudo vim /etc/filebeat/filebeat.yml

enabled: true


paths:

- /var/log/*.log

output.logstash:

# The Logstash hosts

hosts: ["elk-server:5044"]

#output.elasticsearch:

# Array of hosts to connect to.

# hosts: [“localhost:9200”]
```

```
sudo systemctl enable filebeat.service


sudo systemctl start filebeat.service
```

. . . .

```
cd /etc/logstash/conf.d/
vi container.conf
```

.

```
input {
  beats {
    port => 6050
    ssl => false
  }
}
#filter {
#  if "syslog" in [tags] {
#    grok {
#      match => { "message" => "%{SYSLOGLINE}" }
#    }

#    date {
#match => [ "timestamp", "MMM  d HH:mm:ss", "MMM dd HH:mm:ss" ]
#}

#  }
#}
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    user => "elastic"
    password => "Db4Ts567MMQod54Ettym"
    index => "k8s-logs-%{+YYYY.MM.dd}"
  }
  stdout {
    codec => rubydebug
  }
}
```

```
cd /etc/logstash
vi pipelines.yml
```

```
.
.
.
- pipeline.id: container-pipeline
  path.config: "/etc/logstash/conf.d/container.conf"
```

```
systemctl restart logstash
```