

3. ELK stack Install

ELK Stack Install

ELK Stack [1001](#) [1002](#) - ELK[1003](#) [1004](#)

1. repository [1001](#)

```
$ vi /etc/yum.repos.d/elk.repo

[logstash-7.x]
name=Elastic repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=0
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

2. java [1001](#) (java [1002](#) [1003](#) 1.8 [1004](#) [1005](#) [1006](#))

```
$ yum install java -y
$ java -version
openjdk version "1.8.0_282"
OpenJDK Runtime Environment (build 1.8.0_282-b08)
OpenJDK 64-Bit Server VM (build 25.282-b08, mixed mode)
```

3. Logstash / Elasticsearch / Kibana [1001](#)

```
$ yum install logstash elasticsearch kibana -y
```

ELK Stack Config - ELK[1001](#) [1002](#)

1. kibana

```
$ vi /etc/kibana/kibana.yml
...
server.host: "0.0.0.0" (webui 0.0.0.0 )
...
elasticsearch.hosts: ["http://localhost:9200"] (Elasticsearch ip)
...
i18n.locale: "ko-KR"
```

2. Cluster Elasticsearch

```
$ vi /etc/elasticsearch/elasticsearch.yml
...
cluster.name: es-cluster # cluster.name
node.name: ${HOSTNAME} # (unique )
path.data: /data/elasticsearch # Elasticsearch Data
path.logs: /var/log/elasticsearch # Elasticsearch
network.host: 0.0.0.0 #
discovery.seed_hosts: ["192.168.0.10", "192.168.0.11", "192.168.0.12"] #Elasticsearch Discovery
cluster.initial_master_nodes: ["192.168.0.10", "192.168.0.11", "192.168.0.12"] #
...
http.port: 9200 # http
transport.tcp.port: 9300 #
...
node.master: true # master true
node.data: true # data true
...
index.number_of_replicase: 1 # 3 replicaset
index.number_of_shards: 2 #
...
node.attr.box_type: hot # (hot / warm / cold )
```

3. logstash config

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

```
input {
  beats {
    port => 5044
    host => "0.0.0.0"
  }
}

output {
  elasticsearch {
    hosts => ["http://localhost:9200"]
    index => "nginx-%{+YYYY.MM.dd}"
    #user => "elastic"
    #password => "changeme"
  }
}
```

```
#config 1111 logstash 1111 11 (11 11 11 1 1111 11 )
```

```
$ vi /etc/systemd/system/logstash.service
```

```
...
```

```
ExecStart=/usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/nginx.conf
```

```
...
```

```
$ systemctl daemon-reload
```

4. filebeat 11 - log 111 111 11

1. repository 11

```
$ vi /etc/yum.repos.d/elk.repo
```

```
[logstash-7.x]
```

```
name=Elastic repository for 7.x packages
```

```
baseurl=https://artifacts.elastic.co/packages/7.x/yum
```

```
gpgcheck=0
```

```
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

```
enabled=1
```

```
autorefresh=1
type=rpm-md
```

2. 安装 filebeat

```
$ yum install filebeat -y
```

3. filebeat 配置

```
$ vi /etc/filebeat/filebeat.yml
...
filebeat.inputs:
- type: log
  enabled: true #true 是否启用
  paths: #Logstash 采集的路径 可以是单个也可以是多个
    - /svc/stg/web/logs/access.log
    - /var/log/cmd.log
    - /var/log/kibana/*
...
setup.kibana:
  host: "192.168.0.11:5601" #Kibana IP
...
#output.elasticsearch: #filebeat -> logstash 输出到 elasticsearch
# hosts: ["localhost:9200"]
...
output.logstash: #输出
  hosts: ["192.168.0.11:5044"] #logstash ip
```

安装 kibana 和 elasticsearch

1. kibana / elasticsearch 安装 - ELK 安装

```
$ systemctl enable kibana --now
$ systemctl enable elasticsearch --now
$ systemctl enable logstash --now
```

2. filebeat - Log








```
$ systemctl enable filebeat --now
```

1. logstash









```
#logstash  LISTEN   
$ netstat -antp | grep 5044 | grep LISTEN  
tcp6      0      0 :::5044          :::*              LISTEN      6730/java  
  
#filebeat → logstash     (logstash )  
$ tcpdump -nn port 5044 -i bond0  
14:11:35.759481 IP 192.168.0.11.5044 > 192.168.10.2.34160: Flags [P.], seq 379:385, ack 87143,  
win 1432, options [nop,nop,TS val 341934898 ecr 464702009], length 6  
14:11:35.760109 IP 192.168.10.2.34160 > 192.168.0.11.5044: Flags [.], ack 385, win 115, options  
[nop,nop,TS val 464702013 ecr 341934898], length 0
```

2. Elasticsearch

```
#Elasticsearch  LISTEN   
$ netstat -antp | grep 9200 | grep LISTEN  
tcp6      0      0 :::9200          :::*              LISTEN      11324/java  
  
#logstash   elasticsearch index   
$ curl --connect-timeout 2 -XGET http://127.0.0.1:9200/_cat/indices?v  
health status index                uuid                pri rep docs.count docs.deleted store.size  
pri.store.size  
green open   .kibana_task_manager_7.12.0_001 jNMZ2LZcRtqYkwCrQqCsdQ 1 1      9  
10 92.6kb    73.7kb  
green open   .apm-custom-link          MmzSDfLtSXuQCYwqXoYbFg 1 1      0      0  
416b      208b  
green open   .apm-agent-configuration  xbHoMaQ0QUS2WAsOy3Uspw 1 1      0      0  
416b      208b  
green open   .async-search            pMPoD_2OQzue0gJH-vSdig 1 1      1      0
```

90.9kb	46.9kb						
green	open	.kibana_7.12.0_001	Qmo4u9gjTOmihGVWJlguqQ	1	1	22	0
6.3mb	4.2mb						
green	open	.kibana-event-log-7.12.0-000001	VykSos0vR1W_I5F2E5G2pg	1	1	2	0
21.9kb	10.9kb						
green	open	.elastichq	7sr4ATTsSnasGRH4tjhCBA	1	1	1	0
13.7kb	6.8kb						
green	open	.tasks	X2B8PyG5SMCV0dPAo6eH4g	1	1	2	0
15.5kb	7.7kb						

3.

```
$ curl --connect-timeout 2 -XGET http://127.0.0.1:9200/_cluster/health?pretty=true
{
  "cluster_name" : "es-cluster", #  
  "status" : "green", #  
  "timed_out" : false,
  "number_of_nodes" : 3, #   
  "number_of_data_nodes" : 3, #   
  "active_primary_shards" : 9,
  "active_shards" : 18,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```
























4. Kibana

```
#kibana  LISTEN 
$ netstat -antp | grep 5601 | grep LISTEN
tcp      0      0 0.0.0.0:5601          0.0.0.0:*             LISTEN   13513/node

#kibana  
$ curl -IL -XGET http://192.158.0.11:5601/app/home/
```

```
HTTP/1.1 200 OK
content-type: text/html; charset=utf-8
content-security-policy: script-src 'unsafe-eval' 'self'; worker-src blob: 'self'; style-src 'unsafe-inline' 'self'
kbn-name: SKB-DJK-ELK1
kbn-license-sig: 0f6943d9f4b6625724a0d78fe647bbe2f284a6e24fb46f587b17b1b0bec18e34
cache-control: private, no-cache, no-store, must-revalidate
content-length: 127971
vary: accept-encoding
accept-ranges: bytes
Date: Fri, 09 Apr 2021 05:52:47 GMT
Connection: keep-alive
Keep-Alive: timeout=120
```

Kibana Index Pattern

1. WebUI : <http://kibanaIP:5601>
image-1658595831958.png
2. Management → Stack Management → Kibana → Index patterns
image-1658595840322.png
3. {{ index name }}-YYYY.mm.DD    elasticsearch   
   .
4. Search   index   Create index pattern 
5. Time filed  @timestamp   Create index pattern 
image-1658595851071.png
6. Analytics → discover     
image-1658595858282.png

WEB UI Elasticsearch

- docker   cerebro container 

```
$ docker container run -d --name cerebro --restart always -p 9000:9000 -m 512m
lmenezes/cerebro:latest
```

8d691f585fa8: Pull complete


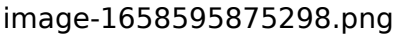
3da6fe7ff2ef: Pull complete

e22147996cc0: Pull complete





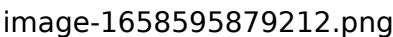
8df48a2d4467: Pull complete








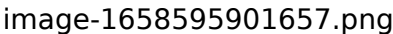
45e578fea430: Pull complete

Digest: sha256:1cd0765418f1737de3533648d549655437eb550ee0cfad27488c19e620028f2f

- WEB UI  : <http://elk:ip:9200>


- Node address  ELK  IP 

-  (Overview) : Elastic  &  


- Nodes :    (   master )


Site

- *logstash input* : <https://www.elastic.co/guide/en/logstash/current/input-plugins.html>
- *filebeat log* : <https://www.elastic.co/guide/en/beats/filebeat/current/configuration-filebeat-options.html#filebeat-input-types>
- *elk intall*: <https://www.elastic.co/guide/en/beats/filebeat/current/setup-repositories.html>
- *elk stack*  : <https://medium.com/naver-cloud-platform/%EB%84%A4%EC%9D%B4%EB%B2%84-%ED%81%B4%EB%9D%BC%EC%9A%B0%EB%93%9C-%ED%94%8C%EB%9E%AB%ED%8F%BC%EC%9D%84-%ED%99%9C%EC%9A%A9%ED%95%B4-elk-elasticsearch-logstash-kibana-%EC%8A%A4%ED%83%9D-%EA%B5%AC%EC%B6%95%ED%95%98%EA%B8%B0-4cbaf5dd4305>
- *logstash / filebeat*  : <https://velog.io/@deet1107/logstash-filebeat>
- *ElasticSearch*  : <https://nesoy.github.io/articles/2019-01/ElasticSearch-System-Architecture>
- *elasticsearch data*  : <https://koocci-dev.tistory.com/13>

Revision #5

Created 17 July 2022 18:34:21 by artop0420

Updated 11 November 2024 10:33:23 by artop0420