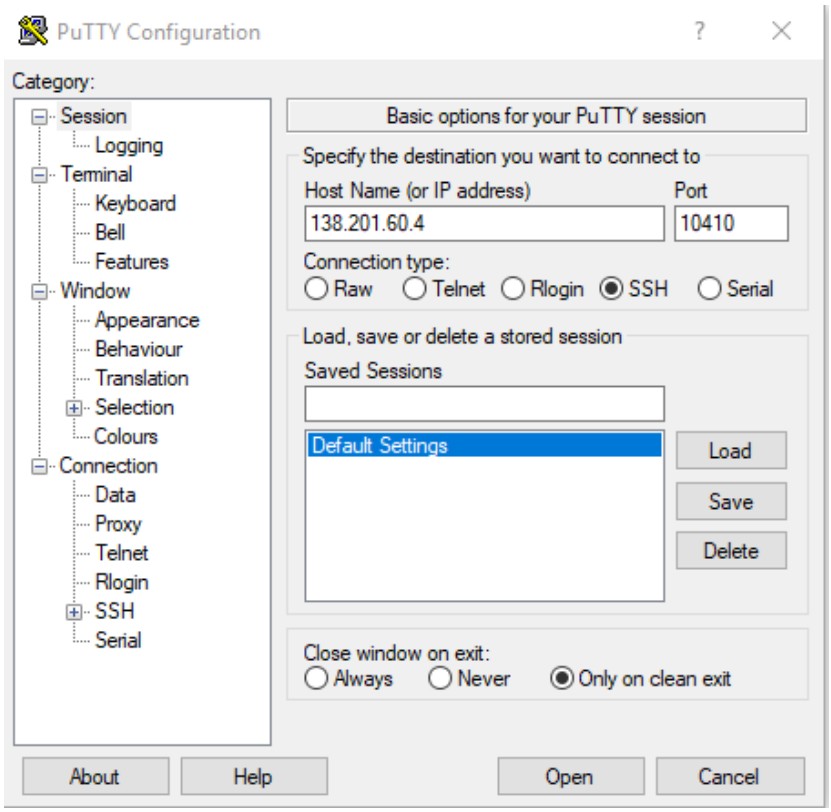
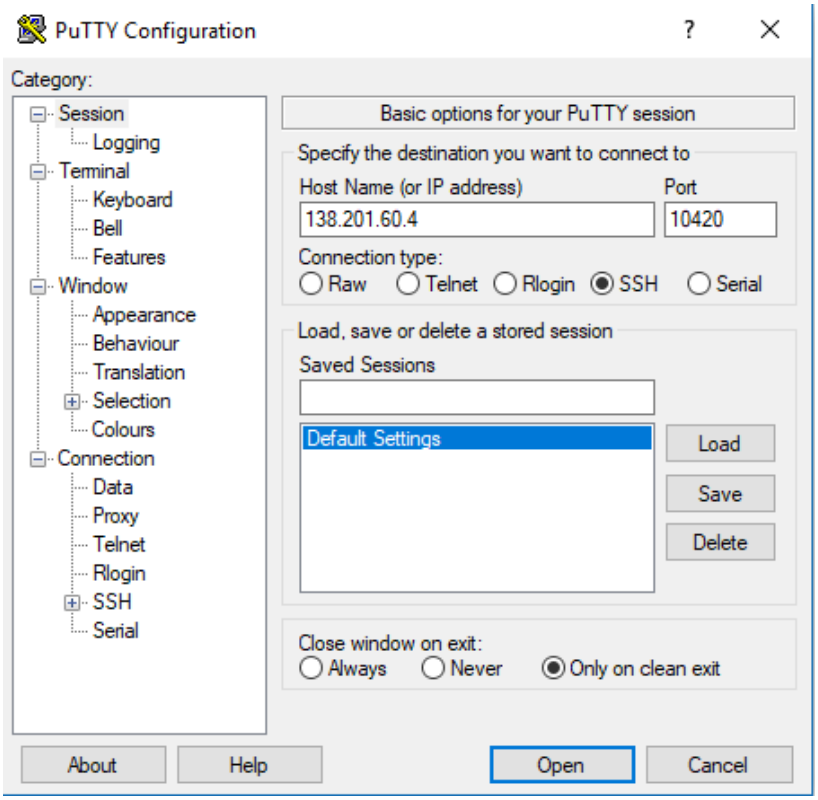
Dokumentasi *Technical Test* Konfigurasi ELK Stack

By : Erry Nur Azhari

- Menggunakan aplikasi putty untuk melakukan *remote server*



Untuk melakukan remote ke pod-elk, masukan IP 138.201.60.4 dan port 10410 seperti pada gambar di atas.



Untuk melakukan remote ke pod-clietnt, masukan IP 138.201.60.4 dan port 10420 seperti pada gambar di atas. Beda dengan gambar pertama terletak pada port nya.

- Install JDK, Elasticsearch, Kibana, Logstash

```
student@pod04-elk:~$ sudo apt install openjdk-8-jdk
```

Install java, saya menggunakan open jdk 8 seperti pada gambar di atas

```
student@pod04-elk:~$ echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" |
 sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
deb https://artifacts.elastic.co/packages/7.x/apt stable main
```

Simpan definisi direktori package elasticsearch dari repository debian dengan perintah :
“`echo “deb https://artifacts.elastic.co/packages/7.x/apt stable main” | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list`”

```
student@pod04-elk:~$ sudo apt install elasticsearch
```

Install elasticsaearch seperti pada gambar di atas

```
student@pod04-elk:~$ sudo apt install kibana
```

Install kibana seperti pada gambar di atas

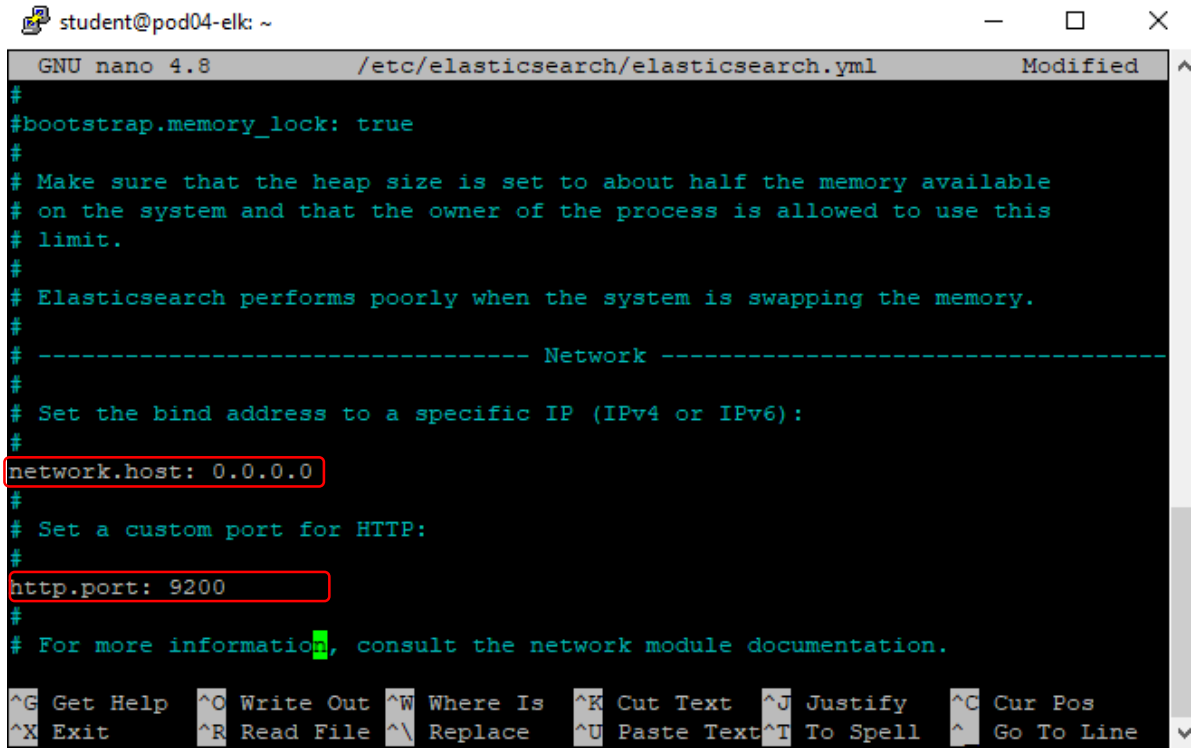
```
student@pod04-elk:~$ sudo apt install logstash
```

Install logstash seperti pada gambar di atas

- Konfigurasi Elasticsearch

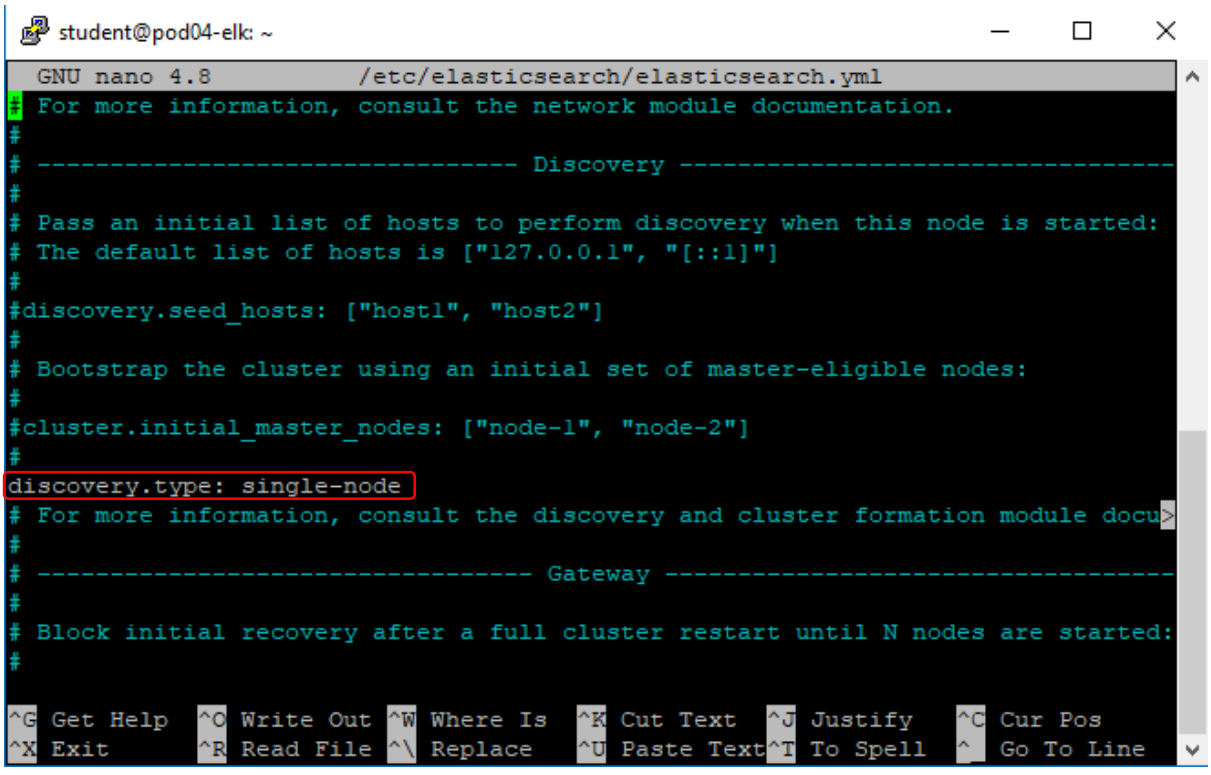
```
student@pod04-elk:~$ sudo nano /etc/elasticsearch/elasticsearch.yml
```

Lakukan konfigurasi pada file “elasticsearch.yml” dengan script seperti pada gambar di atas



-Ganti alamat dan hapus komen menjadi network.host: 0.0.0.0 supaya bisa diakses lewat internet.

-Hapus komen pada http.port: 9200, kali ini port dibiarkan sesuai settingan default



Tambahkan “discovery.type: single-node” karena menggunakan mode single node

```
student@pod04-elk:~$ sudo systemctl daemon-reload
student@pod04-elk:~$ sudo systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /lib/
systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
student@pod04-elk:~$ sudo systemctl start elasticsearch
```

Gunakan script seperti pada gambar di atas untuk melakukan restart dan mengaktifkan service elasticsearch

```
student@pod04-elk:~$ curl -XGET http://localhost:9200/_cluster/health?pretty
{
  "cluster_name" : "elasticsearch",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 1,
  "number_of_data_nodes" : 1,
  "active_primary_shards" : 6,
  "active_shards" : 6,
  "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
}
```

Validasi elasticsearch dengan perintah :

“curl -XGET http://localhost:9200/_cluster/health?pretty”

- Konfigurasi Kibana

```
student@pod04-elk:~$ sudo nano /etc/kibana/kibana.yml
```

Konfigurasi file kibana.yml dengan perintah seperti pada gambar di atas

```
  GNU nano 4.8                  /etc/kibana/kibana.yml
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and >
# The default is 'localhost', which usually means remote machines will not be a>
# To allow connections from remote users, set this parameter to a non-loopback >
server.host: "0.0.0.0"
```

-Hilangkan komen pada bagian server.port, pada bagian ini port tidak diubah

-Hilangkan komen pada bagian server.host, isi IP 0.0.0.0 supaya bisa diakses lewat internet

```
# The Kibana server's name.  This is used for display purposes.
server.name: "test-kibana"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]
```

-Hilangkan komen pada bagian server.name, saya memberi nama “test-kibana”

-Hilangkan komen pada bagian elasticsearch.hosts, url tidak diubah

```
student@pod04-elk:~$ sudo systemctl start kibana
```

Aktifkan service kibana dengan perintah seperti pada gambar di atas

- Konfigurasi Logstash

```
student@pod04-elk:~$ sudo nano /etc/logstash/conf.d/02-beats-input.conf
```

Konfigurasi input port pada logstash

```
  GNU nano 4.8          /etc/logstash/conf.d/02-beats-input.conf
input {
  beats {
   port => 5044
  }
}
```

Script seperti pada gambar di atas lalu save and exit

```
student@pod04-elk:~$ sudo nano /etc/logstash/conf.d/30-elasticsearch-output.conf
```

Masukan perintah seperti pada gambar di atas untuk melakukan konfigurasi logstash

```
  GNU nano 4.8   /etc/logstash/conf.d/30-elasticsearch-output.conf    Modified
output {
  if [@metadata][pipeline] {
    elasticsearch {
    hosts => ["localhost:9200"]
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
    pipeline => "%{[@metadata][pipeline]}"
    }
  } else {
    elasticsearch {
    hosts => ["localhost:9200"]
    manage_template => false
    index => "%{[@metadata][beat]}-%{[@metadata][version]}-%{+YYYY.MM.dd}"
    }
  }
}
```

Setelah file diisi dengan script seperti pada gambar di atas save & exit

```
student@pod04-elk:~$ sudo -u logstash /usr/share/logstash/bin/logstash --path.setting
s /etc/logstash -t
```

```
Config Validation Result: OK. Exiting Logstash
```

Validasi logstash seperti pada gambar di atas

```
student@pod04-elk:~$ sudo systemctl start logstash
student@pod04-elk:~$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /etc/systemd/system/logstas
h.service.
```

Aktifkan service logstash seperti pada gambar di atas

- Konfigurasi Filebeat

```
student@pod04-elk:~$ sudo nano /etc/filebeat/filebeat.yml
```

Konfigurasi filebeat dengan perintah seperti pada gambar di atas

```
# ---------------------------- Elasticsearch Output ----------------------------
#output.elasticsearch:
  # Array of hosts to connect to.
 # hosts: ["localhost:9200"]
```

```
# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5044"]
```

-Pada bagian elasticsearch output, beri komen “#” pada bagian output & hosts

```
student@pod04-elk:~$ sudo filebeat modules enable system
Enabled system
```

Aktifkan filebeat modules dengan perintah seperti gambar di atas

```
student@pod04-elk:~$ sudo filebeat setup --pipelines --modules system
```

Set up the Filebeat untuk parse data dari logstash ke elasticsearch

```
student@pod04-elk:~$ sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.el
asticsearch.hosts=["localhost:9200"]'
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite: true` for enabling.

Index setup finished.
```

Setelah set up berhasil maka akan seperti pada gambar di atas

```
student@pod04-elk:~$ sudo systemctl start filebeat
student@pod04-elk:~$ sudo systemctl enable filebeat
```

Aktifkan service filebeat seperti pada gambar di atas

```
student@pod04-elk:~$ curl -XGET 'http://localhost:9200/filebeat-*/_search?pretty'
{
  "took" : 3,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 0,
      "relation" : "eq"
    },
    "max_score" : null,
    "hits" : [ ]
  }
}
```

Verifikasi bahwa elasticsearch telah menerima data dengan perintah se[erti pada gambar di atas.

Untuk visualisasi pada resource pod-client dan hasil dari parsing dari file raw yg terlampir belum bisa saya dokumentasikan karena saya belum berhasil menampilkan laman web nya via IP Public yang telah diberikan. Jika saya diberi kesempatan bergabung dengan Btech, insya Allah saya akan berusaha mengejar kebutuhan skill pada bidang pekerjaan saya dengan banyak belajar kepada Cloud Engineer senior di sana, terima kasih atas technical test yang diberikan karena telah banyak memberi saya ilmu baru.