Tutorial mengistall elasticserarch,kibana,logstash,dan filebeat di server ubuntu

1. mengistall dan configurasi Elasticsearch .

==========

elasticsearch adalah sebuah mesin pencarian dan analisis data yang terdistribusi open-source dan terintegrasi dengan berbagai jenis sumber data.

A. Mengunduh Elasticsearch GPG key dari URL yang diberikan.

==========

Perintahnya :

```
$ curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch |sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg
```

Perintah tersebut adalah untuk menambahkan Elastic's GPG key ke sistem operasi Anda. GPG (GNU Privacy Guard) key adalah kunci enkripsi yang digunakan untuk memverifikasi tanda tangan digital dari paket yang didistribusikan oleh Elastic.

B. mengambil kunci GPG untuk repository dari URL .

==========

perintahnya :

```
$ echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
```

C. melakukan update terlebih dahulu.

==========

perintahnya :

```
$ sudo apt update
```

D. install elasticsearch.

==========

perintahnya :

```
$ sudo apt install elasticsearch
```

E. setelah di install maka edit file yang yang di elasticserach.

==========

perintahnya :

```
$ sudo nano /etc/elasticsearch/elasticsearch.yml
```

Setelah masuk di file elasticserarch maka edit bagian berikut.

```
. . .
# ---------------------------------- Network
-----------------------------------
#
# Set the bind address to a specific IP (IPv4 or IPv6):
#
network.host: localhost
. . .
```

Samakan seperti file yang diatas dan silahkan ganti localhostnya jika ada domain sendiri.

F. menstart elasticsearchnya unutk memulai elasticsearchnya.

==========

perintahnya :

```
$ sudo systemctl start elasticsearch
```

G. mengenable elasticsearchnya.

==========

dunia teknologi yang berarti mengaktifkan, mengizinkan, atau memungkinkan suatu fitur, layanan, atau perangkat lunak tertentu agar dapat digunakan atau beroperasi.

Perintahnya :

```
$ sudo systemctl enable elasticsearch
```

H. untuk mengetes elasticsearch nya apakah sudah aktif apa belum.

==========

perintahnya :

```
$ curl -X GET "localhost:9200"
```

Jika sudah di enable maka akan keluar seperti di bawah ini.

```
Output
{
  "name" : "Elasticsearch",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "n8Qu5CjWSmyIXBzRXK-j4A",
  "version" : {
    "number" : "7.17.2",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "de7261de50d90919ae53b0eff9413fd7e5307301",
    "build_date" : "2022-03-28T15:12:21.446567561Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Jika sudah keluar seperti yang di atas maka anda berhasil mengistall elasticsearch nya dan berhasil configurasinya.

2.menginstall nginx untuk memjadi proxy kibananya.

==========

perintahnya :

```
$ sudo apt install nginx
```

Maka anda berhasil menginstall nginxnya

3.install dan configurasu kibana dashboard.

Kibana adalah sebuah platform open-source untuk analisis data dan visualisasi yang terintegrasi dengan Elasticsearch. Kibana memungkinkan pengguna untuk melakukan analisis data pada data yang tersimpan di Elasticsearch dan membuat visualisasi data yang interaktif dan mudah dipahami.

A. install kibana.

==========

Perintahnya :

```
$ sudo apt install kibana
```

B. mengaktifkan kibananya.

==========

```
$ sudo systemctl enable kibana
```

C. memulai kibana nya.

==========

```
$ sudo systemctl start kibana
```

D.membuat user dan kata sandi untuk kibana.

==========

```
$ echo "kibanaadmin:`openssl passwd -apr1`" | sudo tee -a /etc/nginx/htpasswd.users
```

Maka akan otomatis memberikan untuk membuat kata sandi baru di kibana dan nama usernya kibanaadmin untuk masuk ke dalam kibana nya.

E. mengedit file untuk konfigurasi kibananya.

==========

perintahnya :

```
$ sudo nano /etc/nginx/sites-available/your_domain
```

Maka tambahkan isi file nya sebagai berikut.

```
server {
    listen 80;

    server_name your_domain;

    auth_basic "Restricted Access";
```

```
    auth_basic_user_file /etc/nginx/htpasswd.users;

    location / {
        proxy_pass http://localhost:5601;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

Pada bagian your_domainnya bisa anda ganti domain anda atau ip server anda.

Untuk menjalankan atau membuka elasticsearch nya.

F. membuat symbolic link dari file konfigurasi Nginx.

==========

perintahnya :

```
$ sudo ln -s /etc/nginx/sites-available/your_domain /etc/nginx/sites-enabled/your_domain
```

Sama seperti yang di atas file nya harus sama dengan langkah yang E di atas.karna unutk membuat sysbolic link nya.

G. mengecek apakah sudah berhasil atau belum.

==========

perintahnya :

```
$ sudo nginx -t
```

Jika sudah suksessfull maka anda berhasil.jika keluarnya syntax is ok

H. mengulang membaca konfigurasinya nginxnya.

==========

perintahnya :

```
$ sudo systemctl reload nginx
```

I. memberikan izin untuk akses pada firewall nya.

==========

perintahnya :

```
$ sudo ufw allow 'Nginx Full'
```

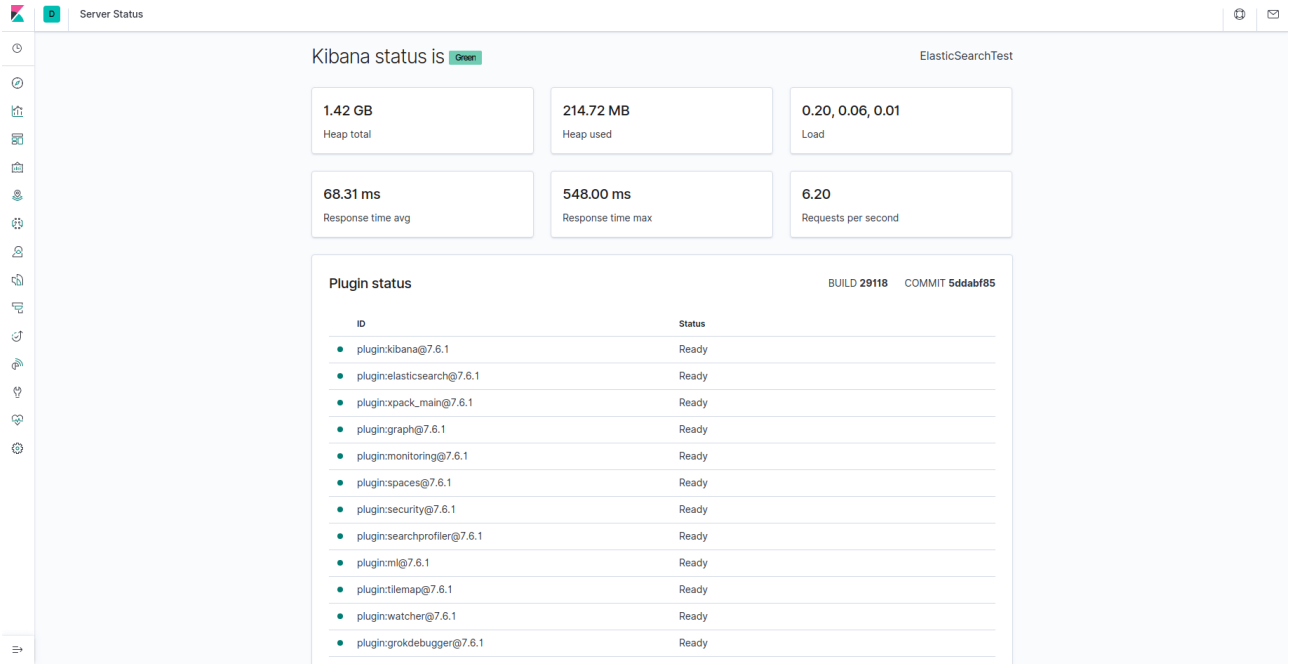
Untuk memberika izin firewall nya untuk membuka nginxnya.

J. buka di browser pencarian untuk membuka kibana anda.

==========

```
http://your_domain/status
```

your_domainnya tinggal anda ganti seperti yang anda konfigurasikan di langkah E kalo anda masukan ip a anda maka tinggal akses menggunakan ip anda.kalo domain perusahaana anda maka akses menggunakan domain perusahaan anda.



4. installing dan configurasi logstash.

Logstash adalah salah satu perangkat lunak open source yang digunakan untuk memproses, mengumpulkan, dan mengirimkan data log dari berbagai sumber ke berbagai tujuan.

A. menginstall logstash.

==========

perintahnya :

```
$ sudo apt install logstash
```

B. tambahkan isi file yang ada di logstash .

==========

perintahnya :

```
$ sudo nano /etc/logstash/conf.d/02-beats-input.conf
```

Maka tambahkan ke dalam file tersebut.

```
input {
  beats {
    port => 5044
  }
}
```

Setelah setelah itu di save.

C. kemudian buat sebuah file yang ada di logstash.

==========

perintahnya :

```
$ sudo nano /etc/logstash/conf.d/30-elasticsearch-output.conf
```

Kemudian masukan isi file tersebut.

```
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 itu di save.

D. silahkan di tes configurasi barunya.

==========

perintahnya :

```
$ sudo -u logstash /usr/share/logstash/bin/logstash --path.settings /etc/logstash -t
```

Jika keluar seperti ini maka anda berhasil `Config Validation Result: OK. Exiting Logstash`

E . memulai logstash nya .

==========

perintahnya :

```
$ sudo systemctl start logstash
```

F. mengaktifkan fitur logstash.

==========

perintahnya :

```
$ sudo systemctl enable logstash
```

Jika sudah berjalan si logstash nya maka anda sudah berhasil mengisntall logstash dan configurasinya.

5. menginstall dan configurasi filebeat.

==========

Filebeat adalah salah satu perangkat lunak open source dari Elastic Stack yang digunakan untuk memantau dan mengirimkan data log dari berbagai sumber ke Elasticsearch atau Logstash. Dengan menggunakan Filebeat, pengguna dapat memonitor file log, data log dari sistem operasi, aplikasi, atau layanan web, dan kemudian meneruskan data tersebut ke Elasticsearch atau Logstash untuk diindeks dan dianalisis.

A. menginstall filebeatnya.

==========

perintahnya :

```
$ sudo apt install filebeat
```

B. mengubah file configurasi filebeatnya.

==========

perintahnya :

```
$ sudo nano /etc/filebeat/filebeat.yml
```

Maka tinggal ubah isi file nya

yang sebelumnya gk ada tanda pagar maka tinggal tambahkan tanda pagarnya seperti berikut yang di warnai.

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

Masih di file yang sama Yang sebelumnya ada tanda pagar maka tinggal hapus tanda pagarnya.

==========

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

C. mengaktifkan modules system

==========

perintahnya :

```
$ sudo filebeat modules enable system
```

D. menampilkan daftar modul yang telah terpasang pada Filebeat.

==========

```
$ sudo filebeat modules list
```

Maka akan keluar sebagai berikut.

```
Output
Enabled:
system

Disabled:
apache2
auditd
elasticsearch
icinga
iis
kafka
```

```
kibana
logstash
mongodb
mysql
nginx
osquery
postgresql
redis
traefik
...
```

E. menginstal dan mengaktifkan pipa (pipeline) dan modul sistem.

==========

perintahnya :

```
$ sudo filebeat setup --pipelines --modules system
```

F. mengaktifkan pengelolaan indeks dan menentukan output ke Elasticsearch.

==========

perintahnya :

```
$ sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["localhost:9200"]'
```

Maka akan keluar seperti di bawah ini.

```
Output
Index setup finished.
```

G. mengatur konfigurasi filebeat dengan menentukan output elasticsearch.

==========

perintahnya :

```
$ sudo filebeat setup -E output.logstash.enabled=false -E output.elasticsearch.hosts=['localhost:9200'] -E setup.kibana.host=localhost:5601
```

Maka akan keluar sebagai berikut.

```
Output
Overwriting ILM policy is disabled. Set `setup.ilm.overwrite:true` for enabling.

Index setup finished.
Loading dashboards (Kibana must be running and reachable)
```

```
Loaded dashboards
Setting up ML using setup --machine-learning is going to be removed in 8.0.0.
Please use the ML app instead.
See more: https://www.elastic.co/guide/en/elastic-stack-overview/current/xpack-
ml.html
Loaded machine learning job configurations
```

H. memulai filebeatnya.

==========

perintahnya :

```
$ sudo systemctl start filebeat
```

I. mengaktifkan filebeatnya.

==========

perintahnya :

```
$ sudo systemctl enable filebeat
```

J. mencari data di elasticsearch

==========

perintahnya :

```
$ curl -XGET 'http://localhost:9200/filebeat-*/_search?pretty'
```

Maka akan keluar seperti di bawah ini.

```
Output
. . .
{
  "took" : 4,
  "timed_out" : false,
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 4040,
      "relation" : "eq"
    },
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "filebeat-7.17.2-2022.04.18",
        "_type" : "_doc",
```

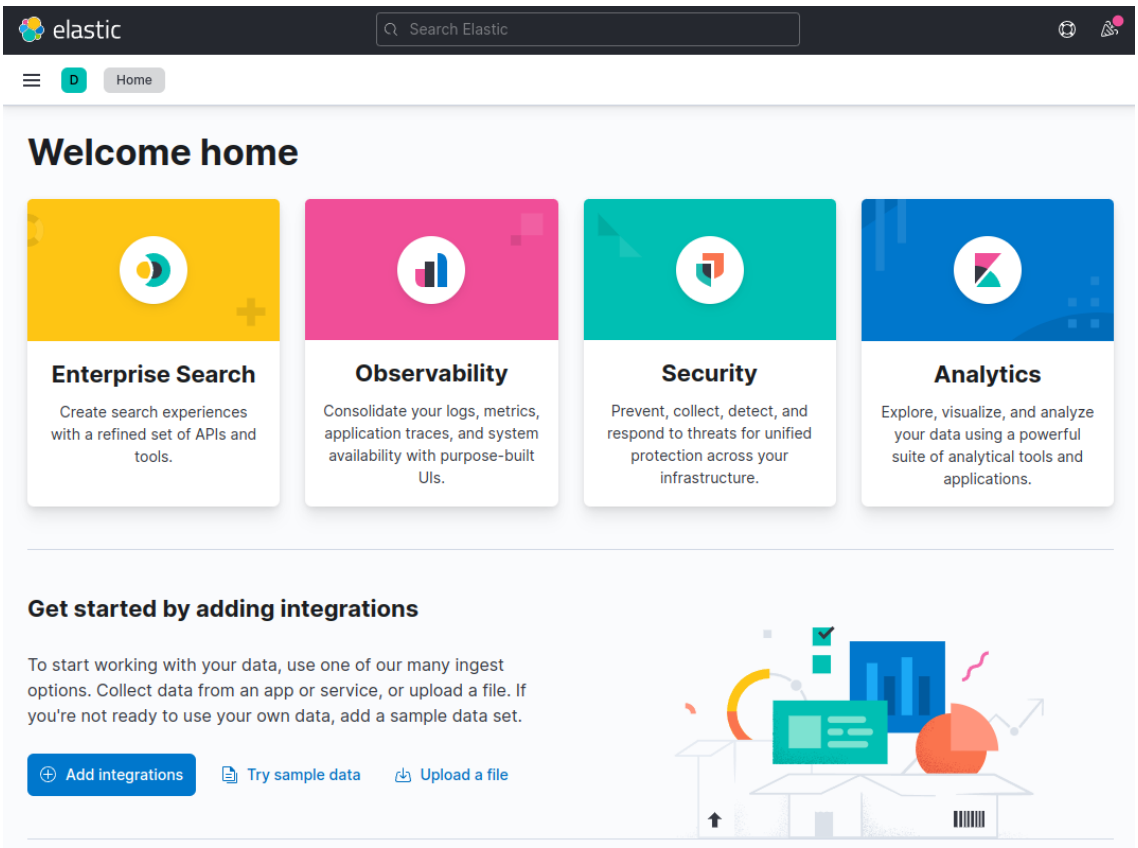
```
        "_id" : "YhwePoAB2RlwU5YB6yfP",
        "_score" : 1.0,
        "_source" : {
          "cloud" : {
            "instance" : {
              "id" : "294355569"
            },
            "provider" : "digitalocean",
            "service" : {
              "name" : "Droplets"
            },
            "region" : "tor1"
          },
          "@timestamp" : "2022-04-17T04:42:06.000Z",
          "agent" : {
            "hostname" : "elasticsearch",
            "name" : "elasticsearch",
            "id" : "b47ca399-e6ed-40fb-ae81-a2f2d36461e6",
            "ephemeral_id" : "af206986-f3e3-4b65-b058-7455434f0cac",
            "type" : "filebeat",
            "version" : "7.17.2"
          },
. . .
```


Maka akan lebih panjang lagi dari pada contoh yang di atas.

6.melihat-lihat kibana dashboard yang sudah kita buat.

==========

tampilan dashboard kibana kita yang telah berhasil di buat.



Tampilan filebeat yang berhasil kita buat.