# INSTALASI ELASTIC STACK
# ASSALAMUALAIKUM WR.WB

## Langkah 1: Instal Java untuk Elastic Stack

Mulailah dengan memperbarui indeks paket sistem Anda.

$ sudo apt update

```
ilmi@DevOps-LM-ilmi:~$ sudo apt update
```

Instal paket apt-transport-https untuk mengakses repositori melalui HTTPS.

$ sudo apt install apt-transport-https

```
ilmi@DevOps-LM-ilmi:~$ sudo apt install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  apt-transport-https
0 upgraded, 1 newly installed, 0 to remove and 111 not upgraded.
Need to get 1,510 B of archives.
After this operation, 170 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 apt-transport-https all 2.4.13 [1,510 B]
Fetched 1,510 B in 2s (842 B/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 75706 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.4.13_all.deb ...
Unpacking apt-transport-https (2.4.13) ...
Setting up apt-transport-https (2.4.13) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ilmi@DevOps-LM-ilmi:~$
```

Install java OpenJDK 17

$ sudo apt install openjdk-17-jdk  -y

```
ilmi@DevOps-LM-ilmi:~$ sudo apt install openjdk-17-jdk -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  adwaita-icon-theme at-spi2-core dconf-gsettings-backend dconf-service
  fontconfig fonts-dejavu-extra gsettings-desktop-schemas
  gtk-update-icon-cache hicolor-icon-theme humanity-icon-theme
  libatk-bridge2.0-0 libatk-wrapper-java libatk-wrapper-java-jni libatk1.0-0
  libatk1.0-data libatspi2.0-0 libcairo-gobject2 libcairo2 libdatrie1
  libdconf1 libdeflate0 libdrm-amdgpu1 libdrm-intel1 libdrm-nouveau2
  libdrm-radeon1 libfontenc1 libgail-common libgail18 libgdk-pixbuf-2.0-0
  libgdk-pixbuf2.0-bin libgdk-pixbuf2.0-common libgif7 libgl1 libgl1-amber-dri
  libgl1-mesa-dri libglapi-mesa libglvnd0 libglx-mesa0 libglx0 libgtk2.0-0
  libgtk2.0-bin libgtk2.0-common libice-dev libice6 libjbig0 libllvm15
  libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpciaccess0
  libpixman-1-0 libpthread-stubs0-dev librsvg2-2 librsvg2-common
  libsensors-config libsensors5 libsm-dev libsm6 libthai-data libthai0
  libtiff5 libwebp7 libx11-dev libx11-xcb1 libxau-dev libxaw7 libxcb-dri2-0
  libxcb-dri3-0 libxcb-glx0 libxcb-present0 libxcb-randr0 libxcb-render0
  libxcb-shape0 libxcb-shm0 libxcb-sync1 libxcb-xfixes0 libxcb1-dev
  libxcomposite1 libxcursor1 libxdamage1 libxdmcp-dev libxfixes3 libxft2
  libxi6 libxinerama1 libxkbfile1 libxmu6 libxpm4 libxrandr2 libxrender1
  libxshmfence1 libxt-dev libxt6 libxtst6 libxv1 libxxf86dga1 libxxf86vm1
  openjdk-17-jre session-migration ubuntu-mono x11-common x11-utils
  x11proto-dev xorg-sgml-doctools xtrans-dev
```

Setelah instalasi, verifikasi apakah Java terinstal dengan benar dengan memeriksa versinya.

$ java -version

```
ilmi@DevOps-LM-ilmi:~$ java -version
openjdk version "17.0.14" 2025-01-21
OpenJDK Runtime Environment (build 17.0.14+7-Ubuntu-122.04.1)
OpenJDK 64-Bit Server VM (build 17.0.14+7-Ubuntu-122.04.1, mixed mode, sharing)
ilmi@DevOps-LM-ilmi:~$
```

Untuk memastikan komponen tumpukan dapat menemukan Java, kita perlu mengatur JAVA_HOMEvariabel lingkungan. Buka berkas lingkungan.

$ sudo nano /etc/environment

```
ilmi@DevOps-LM-ilmi:~$ sudo nano /etc/environment
```

Tambahkan baris berikut di akhir berkas.

JAVA_HOME="/usr/lib/jvm/java-11-openjdk-amd64"

```
  GNU nano 6.2                                                    /etc/environment
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin"
JAVA_HOME="/usr/lib/jvm/java-17-openjdk-amd64"
```

Terapkan perubahan dengan memuat ulang lingkungan.

$ source /etc/environment

```
ilmi@DevOps-LM-ilmi:~$ source /etc/environment
```

Verifikasi apakah JAVA_HOMEsudah diatur dengan benar.

$ echo $JAVA_HOME

```
ilmi@DevOps-LM-ilmi:~$ echo $JAVA_HOME
/usr/lib/jvm/java-17-openjdk-amd64
ilmi@DevOps-LM-ilmi:~$
```

## Langkah 2: Instal ElasticSearch

Mengimpor kunci penandatanganan publik dan menambahkan repositori Elasticsearch APT ke sistem.

$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

```
ilmi@DevOps-LM-ilmi:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.g
pg
ilmi@DevOps-LM-ilmi:~$
```

Tambahkan definisi repositori.

$ echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

```
ilmi@DevOps-LM-ilmi:~$ echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" |
sudo tee /etc/apt/sources.list.d/elastic-8.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main
ilmi@DevOps-LM-ilmi:~$
```

Perbarui lagi daftar paket untuk menyertakan repositori Elasticsearch baru.

$ sudo apt update

```
ilmi@DevOps-LM-ilmi:~$ sudo apt-get update
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [3,248 B]
Get:2 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [
64.0 kB]
Hit:3 http://id.archive.ubuntu.com/ubuntu jammy InRelease
Hit:4 http://id.archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:5 http://id.archive.ubuntu.com/ubuntu jammy-backports InRelease
Hit:6 http://id.archive.ubuntu.com/ubuntu jammy-security InRelease
Fetched 67.2 kB in 3s (20.8 kB/s)
Reading package lists... Done
ilmi@DevOps-LM-ilmi:~$
```

Instal Elasticsearch.

$ sudo apt-get install elasticsearch

```
ilmi@DevOps-LM-ilmi:~$ sudo apt-get install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 111 not upgraded.
Need to get 636 MB of archives.
After this operation, 1,210 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.17.1 [636 MB]
Ign:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.17.1
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.17.1 [636 MB]
Fetched 99.4 MB in 24min 34s (67.4 kB/s)
Selecting previously unselected package elasticsearch.
(Reading database ... 90850 files and directories currently installed.)
Preparing to unpack .../elasticsearch_8.17.1_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.17.1) ...
Setting up elasticsearch (8.17.1) ...
```

Mulai Elasticsearch dan konfigurasikan untuk berjalan saat sistem dimulai.

$ sudo systemctl start elasticsearch

$ sudo systemctl enable elasticsearch

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl start elasticsearch
[sudo] password for ilmi:
```

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/system/elasticsearch.service.
```

Verifikasi bahwa Elasticsearch sedang berjalan.

```
$ sudo sistemctl status elasticsearch
```

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor>
     Active: active (running) since Mon 2025-02-10 04:02:13 UTC; 22s ago
       Docs: https://www.elastic.co
   Main PID: 4353 (java)
      Tasks: 80 (limit: 4564)
     Memory: 2.4G
        CPU: 46.701s
     CGroup: /system.slice/elasticsearch.service
             ├─4353 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+U>
             ├─4411 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.c>
             └─4430 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>

Feb 10 04:01:26 DevOps-LM-ilmi systemd[1]: Starting Elasticsearch...
Feb 10 04:01:30 DevOps-LM-ilmi systemd-entrypoint[4411]: CompileCommand: dontin>
Feb 10 04:01:30 DevOps-LM-ilmi systemd-entrypoint[4411]: CompileCommand: dontin>
Feb 10 04:02:13 DevOps-LM-ilmi systemd[1]: Started Elasticsearch.
lines 1-17/17 (END)
ilmi@DevOps-LM-ilmi:~$
```

## Langkah 3: Konfigurasikan Elasticsearch

Untuk mengizinkan akses eksternal ke Elasticsearch, ubah berkas konfigurasi.

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

```
ilmi@DevOps-LM-ilmi:~$ sudo nano /etc/elasticsearch/elasticsearch.yml
```

Temukan network.hostpengaturannya, hapus komentarnya, dan atur ke `0.0.0.0` untuk mengikat ke semua alamat IP yang tersedia dan hapus komentar pada discoverybagian tersebut untuk menentukan node awal untuk pembentukan kluster `discovery.seed_hosts: []`

```
# ---------------------------------- Network -----------------------------------
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 0.0.0.0
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
#http.port: 9200
#
# For more information, consult the network module documentation.
#
# --------------------------------- Discovery ----------------------------------
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
discovery.seed_hosts: []
#
```

Untuk pengaturan dasar (tidak disarankan untuk produksi), nonaktifkan fitur keamanan, xpack.security.enable: false

```
#----------------------- BEGIN SECURITY AUTO CONFIGURATION -----------------------
#
# The following settings, TLS certificates, and keys have been automatically
# generated to configure Elasticsearch security features on 10-02-2025 04:00:07
#
# ----------------------------------------------------------------------------

# Enable security features
xpack.security.enabled: false

xpack.security.enrollment.enabled: true

# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and
xpack.security.http.ssl:
  enabled: true
  keystore.path: certs/http.p12
```

Mulai ulang Elasticsearch untuk menerapkan perubahan.

$ sudo systemctl restart elasticsearch

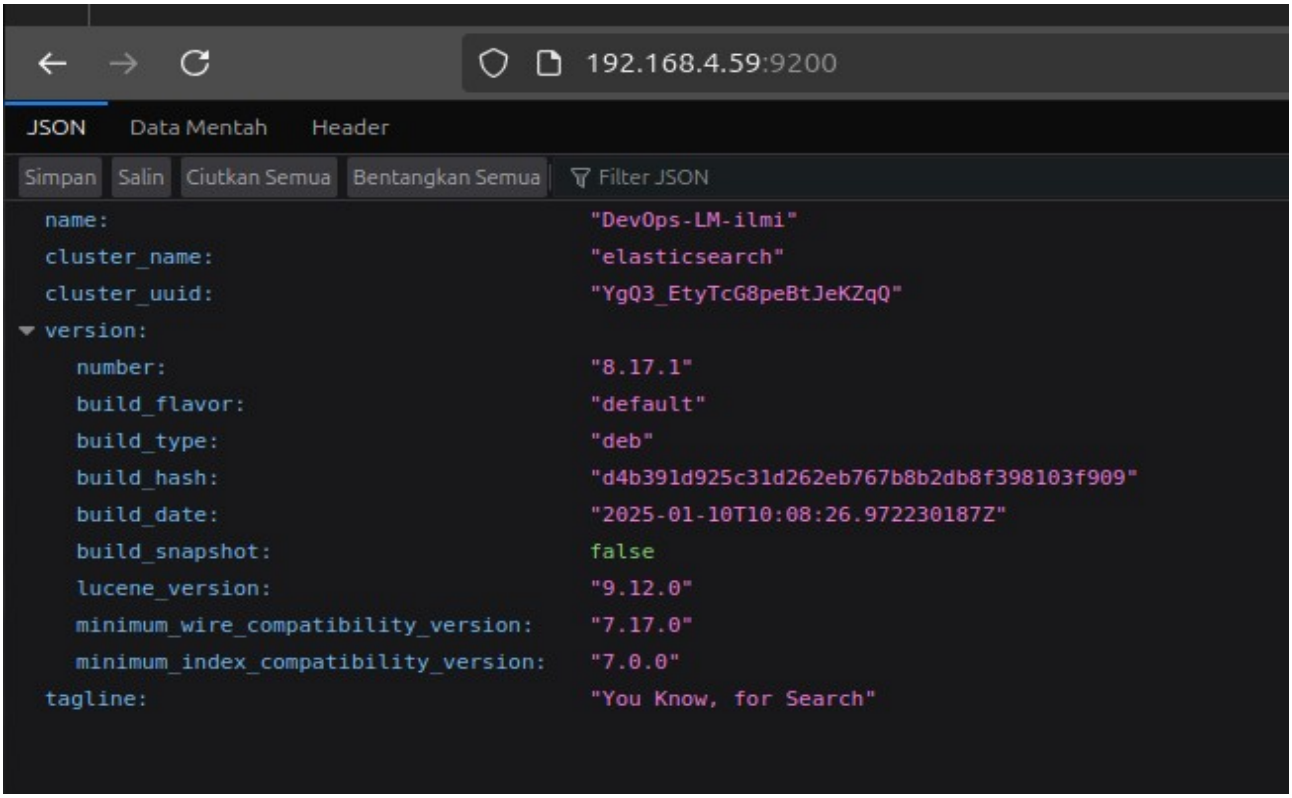
```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl restart elasticsearch
ilmi@DevOps-LM-ilmi:~$
```

Untuk mengonfirmasi bahwa Elasticsearch telah disiapkan dengan benar, kirimkan permintaan HTTP uji menggunakan curl.

```
$ curl -X GET "host lokal:9200"
```

```
ilmi@DevOps-LM-ilmi:~$ curl -X GET "localhost:9200"
{
  "name" : "DevOps-LM-ilmi",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "YgQ3_EtyTcG8peBtJeKZqQ",
  "version" : {
    "number" : "8.17.1",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "d4b391d925c31d262eb767b8b2db8f398103f909",
    "build_date" : "2025-01-10T10:08:26.972230187Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
ilmi@DevOps-LM-ilmi:~$
```

Aksesnya menggunakan browser dengan alamat IP Publik Anda: port 9200 yang merupakan port default untuk Elasticksearch.



## Langkah 4: Instal Logstash

Logstash digunakan untuk memproses dan meneruskan data log ke Elasticsearch. Instal Logstash menggunakan perintah berikut.

```
$ sudo apt-get install logstash -y
```

```
ilmi@DevOps-LM-ilmi:~$ sudo apt-get install logstash -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  logstash
0 upgraded, 1 newly installed, 0 to remove and 111 not upgraded.
Need to get 436 MB of archives.
After this operation, 715 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 logstash amd64 1:8.17.1-1 [436 MB]
Fetched 436 MB in 17min 35s (413 kB/s)
Selecting previously unselected package logstash.
(Reading database ... 92327 files and directories currently installed.)
Preparing to unpack .../logstash_1%3a8.17.1-1_amd64.deb ...
Unpacking logstash (1:8.17.1-1) ...
Setting up logstash (1:8.17.1-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ilmi@DevOps-LM-ilmi:~$
```

Start dan aktifkan Logstash.

```
$ sudo systemctl start logstash
```

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl start logstash
[sudo] password for ilmi:
ilmi@DevOps-LM-ilmi:~$
```

```
$ sudo systemctl enable logstash
```

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /lib/systemd/system/logstash.service
ilmi@DevOps-LM-ilmi:~$
```

Cek status layanan.

```
$ sudo systemctl status logstash
```

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/lib/systemd/system/logstash.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2025-02-10 04:42:29 UTC; 863ms ago
   Main PID: 5288 (java)
      Tasks: 13 (limit: 4564)
     Memory: 56.3M
        CPU: 839ms
     CGroup: /system.slice/logstash.service
             └5288 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djruby.compile.invokedynamic=true -X>

Feb 10 04:42:29 DevOps-LM-ilmi systemd[1]: Started logstash.
Feb 10 04:42:29 DevOps-LM-ilmi logstash[5288]: Using bundled JDK: /usr/share/logstash/jdk
lines 1-12/12 (END)
ilmi@DevOps-LM-ilmi:~$
```

## Langkah 5: Instal Kibana

Instal Kibana menggunakan perintah berikut.

$ sudo apt-get install kibana

```
ilmi@DevOps-LM-ilmi:~$ sudo apt-get install kibana
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  kibana
0 upgraded, 1 newly installed, 0 to remove and 111 not upgraded.
Need to get 347 MB of archives.
After this operation, 1,073 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 kibana amd64 8.17.1 [347 MB]
Fetched 347 MB in 14min 43s (393 kB/s)
Selecting previously unselected package kibana.
(Reading database ... 106848 files and directories currently installed.)
Preparing to unpack .../kibana_8.17.1_amd64.deb ...
Unpacking kibana (8.17.1) ...
Setting up kibana (8.17.1) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/ki
bana/8.17/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
Scanning processes...

Scanning linux images...


Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ilmi@DevOps-LM-ilmi:~$
```

Start dan aktifkan layanan Kibana.

$ sudo systemctl start kibana

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl start kibana
[sudo] password for ilmi:
ilmi@DevOps-LM-ilmi:~$
```

$ sudo systemctl enable kibana

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /lib/systemd/system/kibana.service.
ilmi@DevOps-LM-ilmi:~$
```

Periksa status Kibana:

$ sudo systemctl status kibana

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/lib/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2025-02-10 08:50:48 UTC; 54s ago
       Docs: https://www.elastic.co
   Main PID: 33965 (node)
      Tasks: 11 (limit: 4564)
     Memory: 491.5M
        CPU: 13.469s
     CGroup: /system.slice/kibana.service
             └─33965 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

Feb 10 08:51:37 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:37.252+00:00][INFO ][plugins.security.config] Hash
Feb 10 08:51:37 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:37.260+00:00][WARN ][plugins.security.config] Sess
Feb 10 08:51:37 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:37.333+00:00][WARN ][plugins.security.config] Gene
Feb 10 08:51:37 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:37.334+00:00][INFO ][plugins.security.config] Hash
Feb 10 08:51:37 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:37.334+00:00][WARN ][plugins.security.config] Sess
Feb 10 08:51:38 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:38.037+00:00][WARN ][plugins.encryptedSavedObjects
Feb 10 08:51:38 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:38.435+00:00][WARN ][plugins.actions] APIs are dis
Feb 10 08:51:38 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:38.647+00:00][INFO ][plugins.notifications] Email
Feb 10 08:51:39 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:39.802+00:00][WARN ][plugins.alerting] APIs are d
Feb 10 08:51:39 DevOps-LM-ilmi kibana[33965]: [2025-02-10T08:51:39.803+00:00][INFO ][plugins.alerting] using index
lines 1-21/21 (END)
ilmi@DevOps-LM-ilmi:~$
```

## Langkah 6:Konfigurasi Kibana

Untuk mengonfigurasi Kibana untuk akses eksternal, edit berkas konfigurasi.

$ sudo nano /etc/kibana/kibana.yml

```
ilmi@DevOps-LM-ilmi:~$ sudo nano /etc/kibana/kibana.yml
```

Hapus komentar dan sesuaikan baris berikut untuk mengikat Kibana ke semua alamat IP dan menghubungkannya ke Elasticsearch.

server.port: 5601

server.host: "0.0.0.0"

elasticsearch.hosts: ["http://localhost:9200"]

```
# ================== System: Kibana Server ==================
# 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 host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"
```

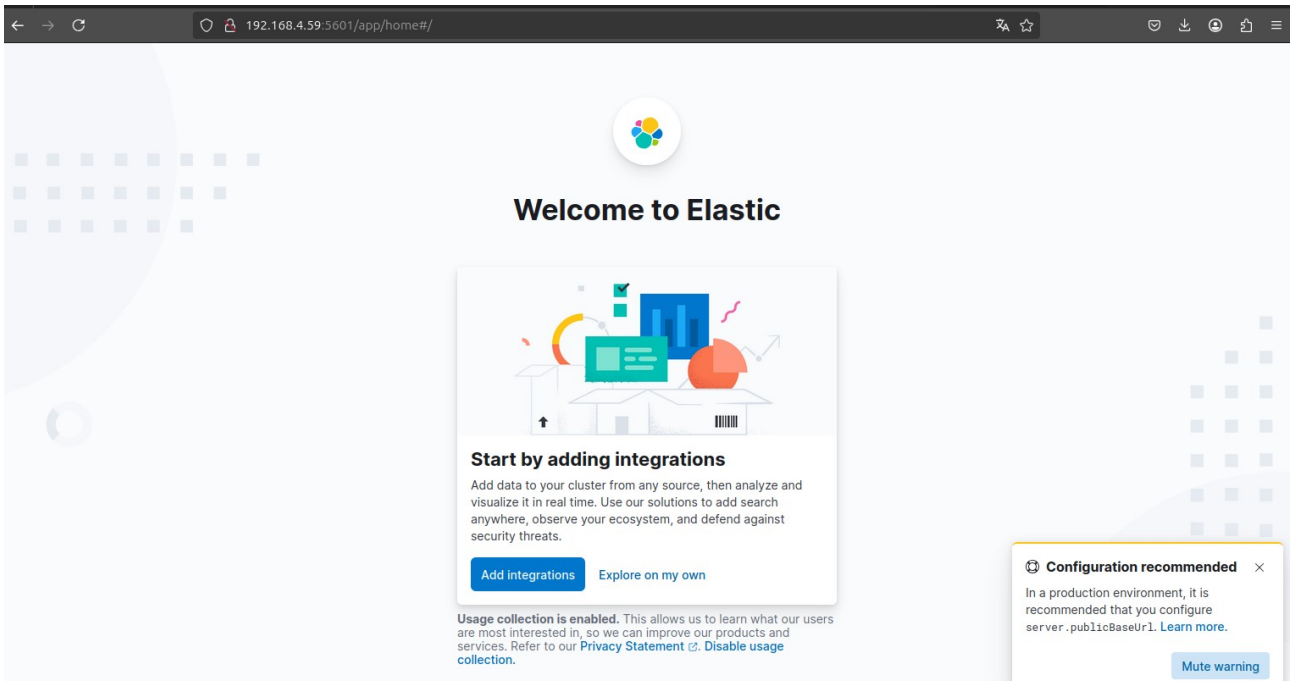
```
# ==================== System: Elasticsearch ====================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana
# index at startup. Your Kibana users still need to authenticate with Elasticsearch, which
# is proxied through the Kibana server.
#elasticsearch.username: "kibana_system"
#elasticsearch.password: "pass"
```

Mulai ulang Kibana untuk menerapkan perubahan.

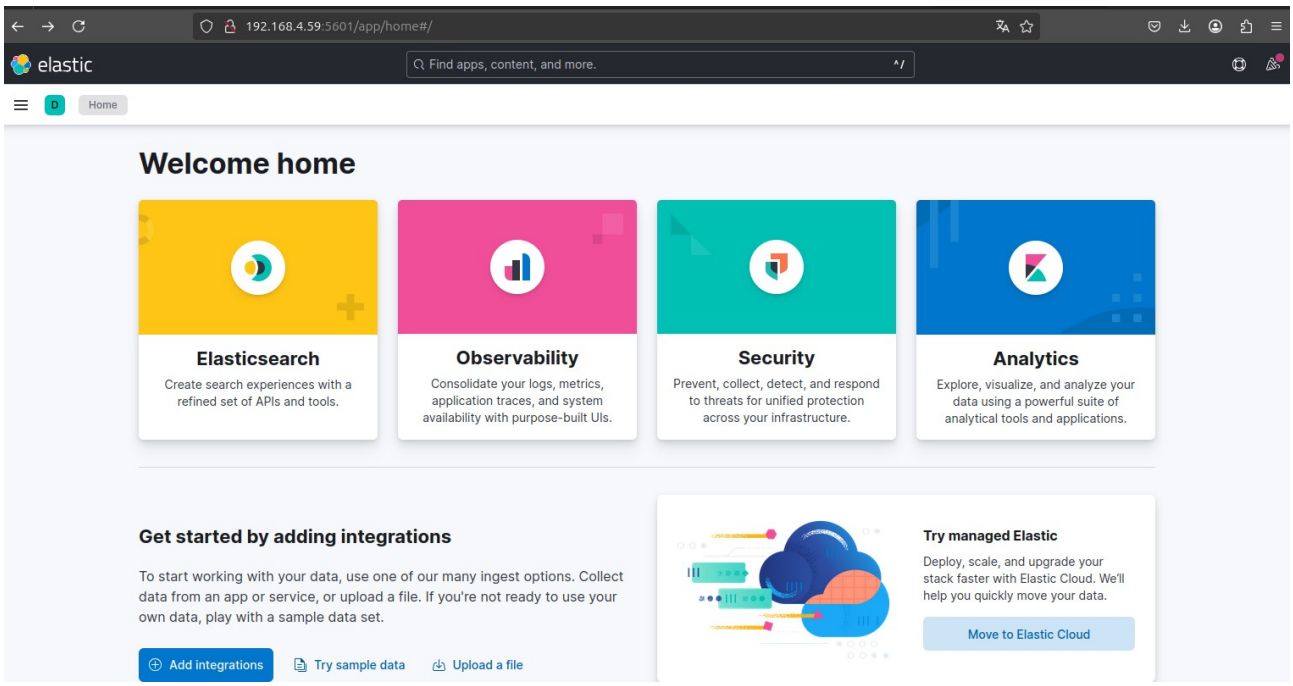
$ sudo systemctl restart kibana

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl restart kibana
ilmi@DevOps-LM-ilmi:~$
```

Akses antarmuka Kibana dengan menavigasi ke http://<ip-server>:5601di peramban web. Ini akan membuka dasbor Kibana tempat Anda dapat mulai menjelajahi data.




Anda dapat menekan adding integrations atau Explore on my own.




## Langkah 7: Instal Filebeat

Instal Filebeat menggunakan perintah berikut.

```
$ sudo apt-get install filebeat
```

```
ilmi@DevOps-LM-ilmi:~$ sudo apt-get install filebeat
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  filebeat
0 upgraded, 1 newly installed, 0 to remove and 111 not upgraded.
Need to get 56.0 MB of archives.
After this operation, 206 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 filebeat amd64 8.17.1 [56.0 MB]
Fetched 56.0 MB in 24s (2,302 kB/s)
Selecting previously unselected package filebeat.
(Reading database ... 209761 files and directories currently installed.)
Preparing to unpack .../filebeat_8.17.1_amd64.deb ...
Unpacking filebeat (8.17.1) ...
Setting up filebeat (8.17.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ilmi@DevOps-LM-ilmi:~$
```

Buka file konfigurasi Filebeat untuk mengirim log ke logstash

$ sudo nano /etc/filebeat/filebeat.yml

```
ilmi@DevOps-LM-ilmi:~$ sudo nano /etc/filebeat/filebeat.yml
```

Berikan pagar pada bagian output Elasticsearch .
Hapus pagar dan konfigurasikan bagian outputLogstash.

# output.elasticsearch:

# hosts: ["localhost:9200"]

output.logstash:

hosts: ["localhost:5044"]

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

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  preset: balanced

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"

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

Aktifkan modul sistem, yang mengumpulkan data log dari sistem lokal.

$ sudo filebeat modules enable system

```
ilmi@DevOps-LM-ilmi:~$ sudo filebeat modules enable system
Enabled system
ilmi@DevOps-LM-ilmi:~$
```

Siapkan Filebeat untuk memuat templat indeks ke dalam Elasticsearch.

$ sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["0.0.0.0:9200"]'

```
ilmi@DevOps-LM-ilmi:~$ sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["0.0.0.0:9200"]'
Overwriting lifecycle policy is disabled. Set `setup.ilm.overwrite: true` to overwrite.
Index setup finished.
ilmi@DevOps-LM-ilmi:~$
```

Start dan aktifkan layanan Filebeat.

```
$ sudo systemctl start filebeat
$ sudo systemctl enable filebeat
```

```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl start filebeat
[sudo] password for ilmi:
ilmi@DevOps-LM-ilmi:~$
```

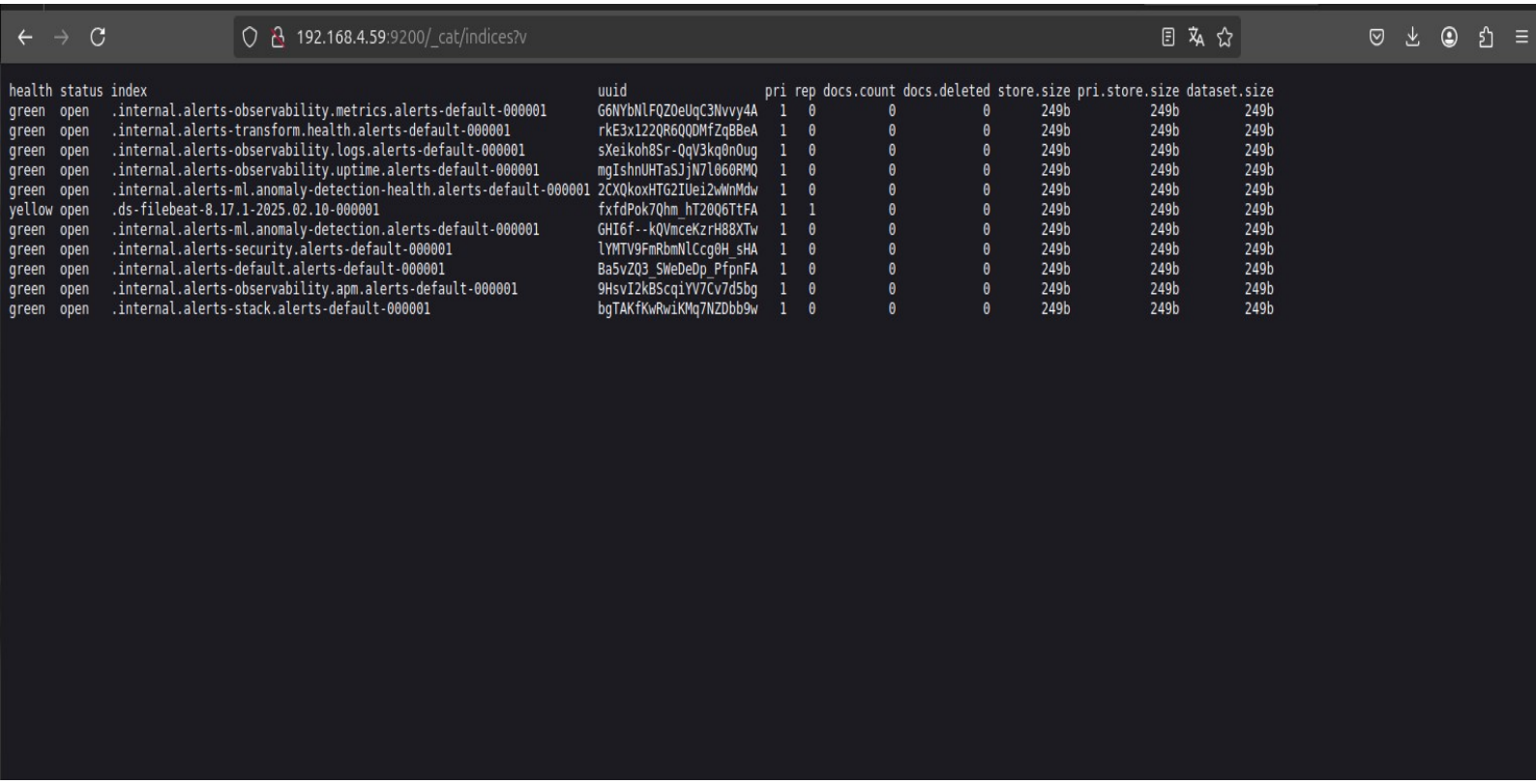
```
ilmi@DevOps-LM-ilmi:~$ sudo systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/filebeat.service.
ilmi@DevOps-LM-ilmi:~$
```

Pastikan Elasticsearch menerima data dari Filebeat dengan memeriksa indeks.

```
$ curl -XGET "localhost:9200/_cat/indices?v"
```

```
ilmi@DevOps-LM-ilmi:~$ curl -XGET "localhost:9200/_cat/indices?v"
health status index                                                                uuid                   pri rep docs.count docs.deleted store.size pri.s
tore.size dataset.size
green  open   .internal.alerts-observability.metrics.alerts-default-000001       G6NYbNlFQZOeUqC3Nvvy4A   1   0          0            0       249b
     249b         249b
green  open   .internal.alerts-transform.health.alerts-default-000001            rkE3x122QR6QQDMfZqBBeA   1   0          0            0       249b
     249b         249b
green  open   .internal.alerts-observability.logs.alerts-default-000001          sXeikoh8Sr-QqV3kq0nOug   1   0          0            0       249b
     249b         249b
green  open   .internal.alerts-observability.uptime.alerts-default-000001        mgIshnUHTaSJjN7l060RMQ   1   0          0            0       249b
     249b         249b
green  open   .internal.alerts-ml.anomaly-detection-health.alerts-default-000001 2CXQkoxHTG2IUei2wWnMdw   1   0          0            0       249b
     249b         249b
yellow open   .ds-filebeat-8.17.1-2025.02.10-000001                               fxfdPok7Qhm_hT20Q6TtFA   1   1          0            0       249b
     249b         249b
green  open   .internal.alerts-ml.anomaly-detection.alerts-default-000001        GHI6f--kQVmceKzrH88XTw   1   0          0            0       249b
     249b         249b
green  open   .internal.alerts-security.alerts-default-000001                     lYMTV9FmRbmNlCcg0H_sHA   1   0          0            0       249b
     249b         249b
green  open   .internal.alerts-default.alerts-default-000001                      Ba5vZQ3_SWeDeDp_PfpnFA   1   0          0            0       249b
     249b         249b
green  open   .internal.alerts-observability.apm.alerts-default-000001           9HsvI2kBScqiYV7Cv7d5bg   1   0          0            0       249b
     249b         249b
green  open   .internal.alerts-stack.alerts-default-000001                        bgTAKfKwRwiKMq7NZDbb9w   1   0          0            0       249b
     249b         249b
ilmi@DevOps-LM-ilmi:~$
```

Akses menggunakan browser menggunakan http://<ip-server>:9200/_cat/indices?v



192.168.4.59:9200/_cat/indices?v

| health | status | index | uuid | pri | rep | docs.count | docs.deleted | store.size | pri.store.size | dataset.size |
|---|---|---|---|---|---|---|---|---|---|---|
| green | open | .internal.alerts-observability.metrics.alerts-default-000001 | G6NYbNlFQZOeUqC3Nvvy4A | 1 | 0 | 0 | 0 | 249b | 249b | 249b |
| green | open | .internal.alerts-transform.health.alerts-default-000001 | rkE3x122QR6QQDMfZqBBeA | 1 | 0 | 0 | 0 | 249b | 249b | 249b |
| green | open | .internal.alerts-observability.logs.alerts-default-000001 | sXeikoh8Sr-QqV3kq0nOug | 1 | 0 | 0 | 0 | 249b | 249b | 249b |
| green | open | .internal.alerts-observability.uptime.alerts-default-000001 | mgIshnUHTaSJjN7l060RMQ | 1 | 0 | 0 | 0 | 249b | 249b | 249b |
| green | open | .internal.alerts-ml.anomaly-detection-health.alerts-default-000001 | 2CXQkoxHTG2IUei2wWnMdw | 1 | 0 | 0 | 0 | 249b | 249b | 249b |
| yellow | open | .ds-filebeat-8.17.1-2025.02.10-000001 | fxfdPok7Qhm_hT20Q6TtFA | 1 | 1 | 0 | 0 | 249b | 249b | 249b |
| green | open | .internal.alerts-ml.anomaly-detection.alerts-default-000001 | GHI6f--kQVmceKzrH88XTw | 1 | 0 | 0 | 0 | 249b | 249b | 249b |
| green | open | .internal.alerts-security.alerts-default-000001 | lYMTV9FmRbmNlCcg0H_sHA | 1 | 0 | 0 | 0 | 249b | 249b | 249b |
| green | open | .internal.alerts-default.alerts-default-000001 | Ba5vZQ3_SWeDeDp_PfpnFA | 1 | 0 | 0 | 0 | 249b | 249b | 249b |
| green | open | .internal.alerts-observability.apm.alerts-default-000001 | 9HsvI2kBScqiYV7Cv7d5bg | 1 | 0 | 0 | 0 | 249b | 249b | 249b |
| green | open | .internal.alerts-stack.alerts-default-000001 | bgTAKfKwRwiKMq7NZDbb9w | 1 | 0 | 0 | 0 | 249b | 249b | 249b |

SEKIAN DAN TERIMAKASIH

WASSALAMUALAIKUM WR.WB