Cara Menginstal Elastis Stack di Ubuntu 24.04 LTS

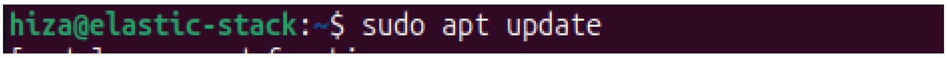
Prasyarat

- Akun AWS dengan Ubuntu 24.04 LTS EC2 Instance.
- Setidaknya 2 core CPU dan RAM 4 GB untuk kinerja yang lancar.

Langkah # 1:Install Java untuk Elastis Stack pada Ubuntu 24.04 LTS

Mulailah dengan memperbarui indeks paket sistem Anda.

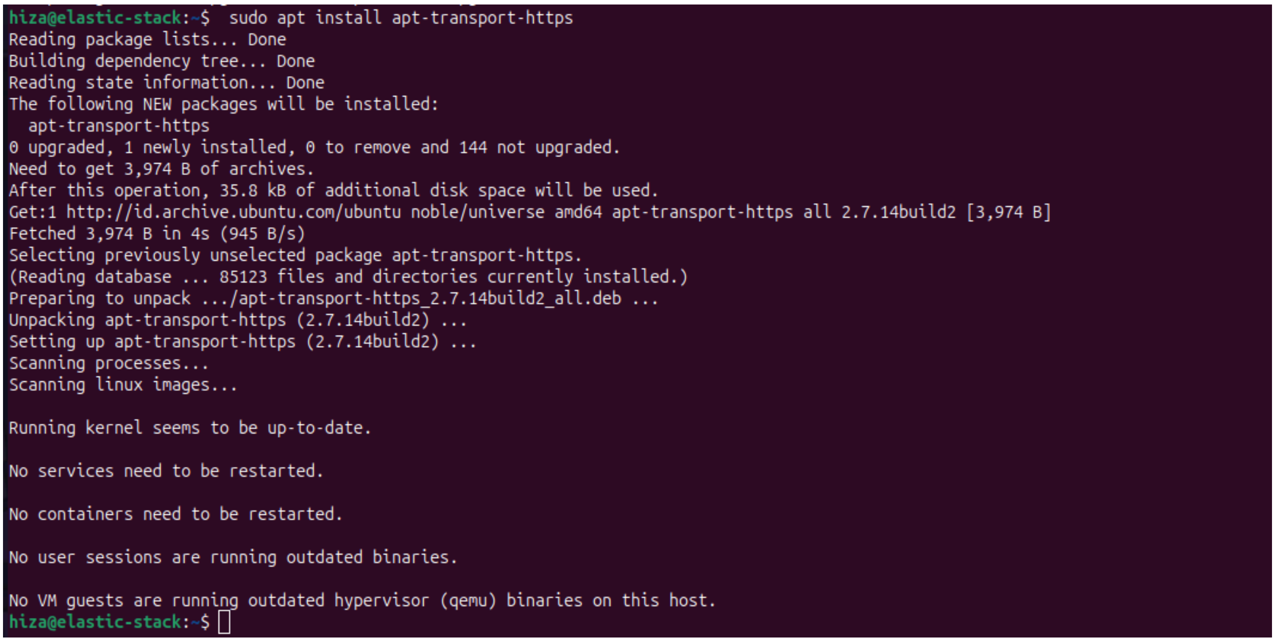
$sudo apt update



```
hiza@elastic-stack:~$ sudo apt update
```

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

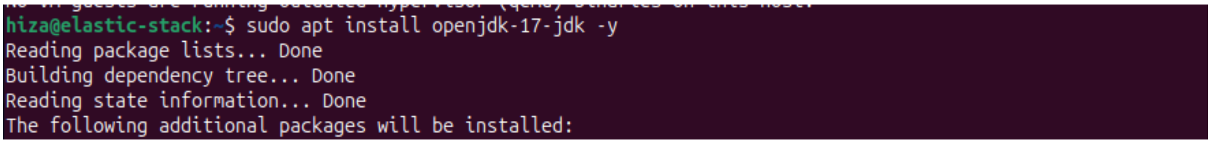
$sudo apt install apt-transport-https



```
hiza@elastic-stack:~$  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 144 not upgraded.
Need to get 3,974 B of archives.
After this operation, 35.8 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all 2.7.14build2 [3,974 B]
Fetched 3,974 B in 4s (945 B/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 85123 files and directories currently installed.)
Preparing to unpack .../apt-transport-https_2.7.14build2_all.deb ...
Unpacking apt-transport-https (2.7.14build2) ...
Setting up apt-transport-https (2.7.14build2) ...
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No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
hiza@elastic-stack:~$ 
```

Komponen-komponen Elastic Stack membutuhkan Java. Kita akan menginstal OpenJDK 17, yang merupakan implementasi sumber terbuka yang banyak digunakan dari Platform Java.

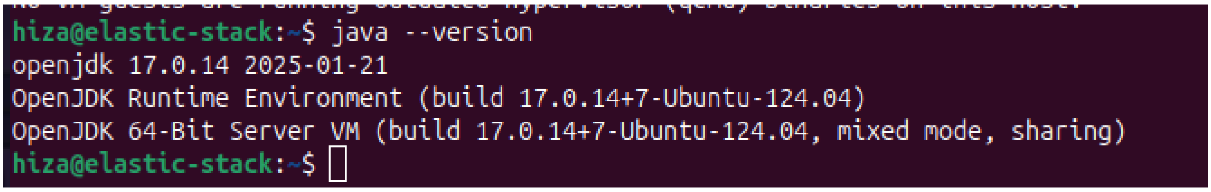
$sudo apt install openjdk-17-jdk -y



```
hiza@elastic-stack:~$ 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:
```

Setelah instalasi, pastikan bahwa Java telah terinstal dengan benar dengan memeriksa versinya.

$java –version



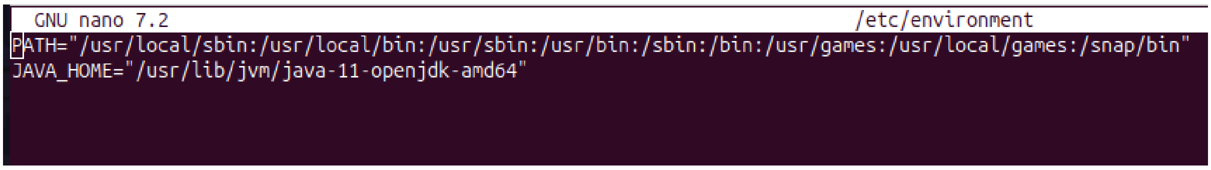
```
hiza@elastic-stack:~$ java --version
openjdk 17.0.14 2025-01-21
OpenJDK Runtime Environment (build 17.0.14+7-Ubuntu-124.04)
OpenJDK 64-Bit Server VM (build 17.0.14+7-Ubuntu-124.04, mixed mode, sharing)
hiza@elastic-stack:~$ 
```

Untuk memastikan komponen stack dapat menemukan Java, kita perlu mengatur variabel lingkungan JAVA_HOME. Buka file environment.

$sudo nano /etc/environment

Tambahkan baris berikut di akhir file.

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



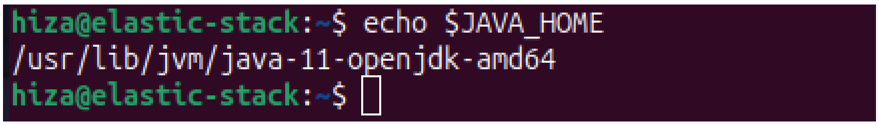
```
  GNU nano 7.2                                                    /etc/environment
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin"
JAVA_HOME="/usr/lib/jvm/java-11-openjdk-amd64"
```

Terapkan perubahan dengan memuat ulang environment.

$source /etc/environment

Verifikasi bahwa JAVA_HOME telah diatur dengan benar.

$echo $JAVA_HOME

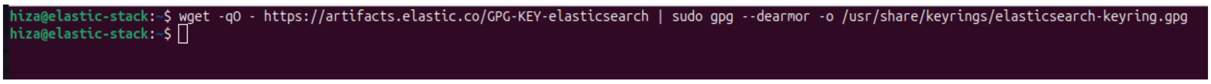


```
hiza@elastic-stack:~$ echo $JAVA_HOME
/usr/lib/jvm/java-11-openjdk-amd64
hiza@elastic-stack:~$ 
```

Langkah #2: Instal ElasticSearch di Ubuntu 24.04 LTS

Elasticsearch adalah komponen inti dari ELK Stack, yang digunakan untuk pencarian dan analisis. Kita perlu mengimpor kunci penandatanganan publik dan menambahkan repositori Elasticsearch APT ke sistem Anda.

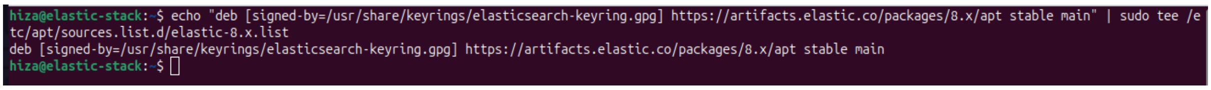
$wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg



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

Tambahkan definisi repositori.

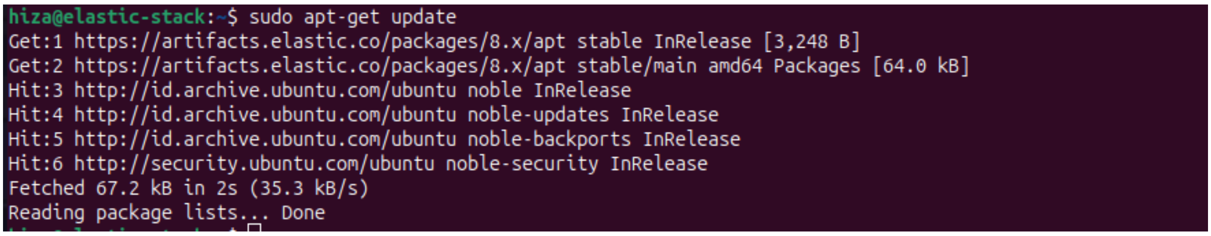
$echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list



```
hiza@elastic-stack:~$ echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /e
tc/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
hiza@elastic-stack:~$ 
```

Perbarui lagi daftar paket untuk menyertakan repositori Elasticsearch yang baru.

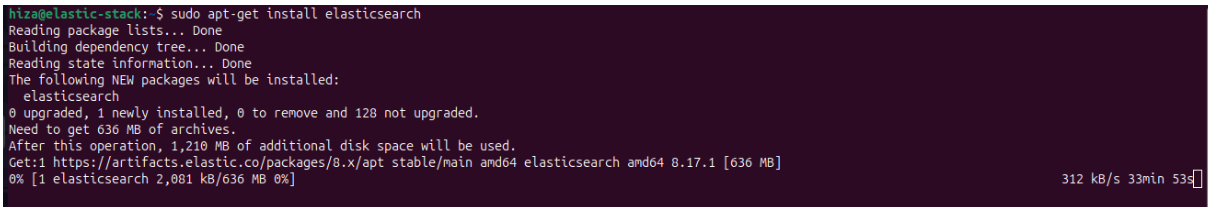
$sudo apt-get update



```
hiza@elastic-stack:~$ 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 noble InRelease
Hit:4 http://id.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:5 http://id.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:6 http://security.ubuntu.com/ubuntu noble-security InRelease
Fetched 67.2 kB in 2s (35.3 kB/s)
Reading package lists... Done
```

Install Elasticsearch.

$sudo apt-get install elasticsearch



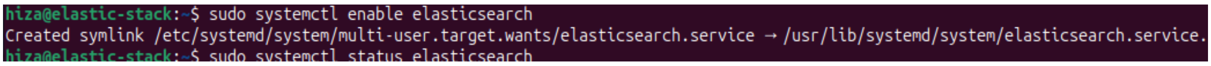
```
hiza@elastic-stack:~$ sudo apt-get install elasticsearch
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 128 not upgraded.
Need to get 636 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]
0% [1 elasticsearch 2,081 kB/636 MB 0%]                                                       312 kB/s 33min 53s
```

**Tunggu proses install memungkinkan membutuhkan waktu yang cukup lama*

Setelah Terinstall , Mulai Elasticsearch dan konfigurasikan untuk dijalankan pada saat pengaktifan sistem.

$sudo systemctl start elasticsearch

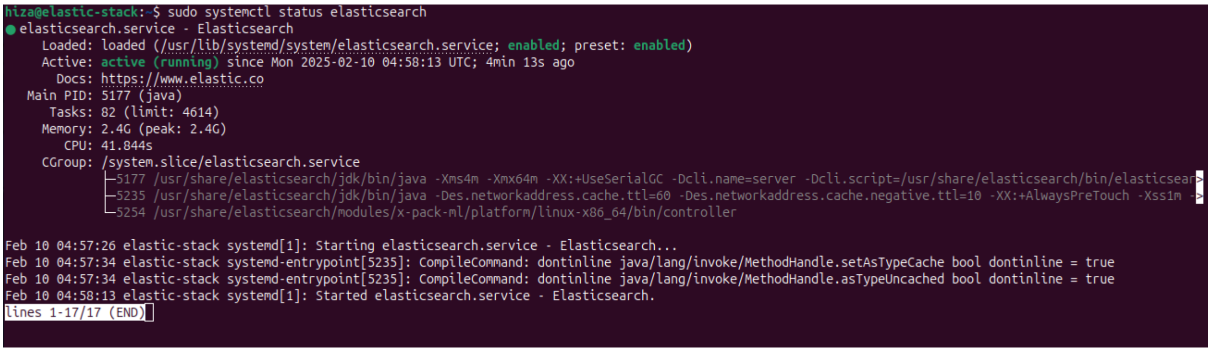
$sudo systemctl enable elasticsearch



```
hiza@elastic-stack:~$ sudo systemctl enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd/system/elasticsearch.service.
hiza@elastic-stack:~$ sudo systemctl status elasticsearch
```

Verifikasi bahwa Elasticsearch sedang berjalan.

$sudo systemctl status elasticsearch



```
hiza@elastic-stack:~$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-02-10 04:58:13 UTC; 4min 13s ago
       Docs: https://www.elastic.co
   Main PID: 5177 (java)
      Tasks: 82 (limit: 4614)
     Memory: 2.4G (peak: 2.4G)
        CPU: 41.844s
     CGroup: /system.slice/elasticsearch.service
             ├─5177 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsear>
             ├─5235 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m ->
             └─5254 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Feb 10 04:57:26 elastic-stack systemd[1]: Starting elasticsearch.service - Elasticsearch...
Feb 10 04:57:34 elastic-stack systemd-entrypoint[5235]: CompileCommand: dontinline java/lang/invoke/MethodHandle.setAsTypeCache bool dontinline = true
Feb 10 04:57:34 elastic-stack systemd-entrypoint[5235]: CompileCommand: dontinline java/lang/invoke/MethodHandle.asTypeUncached bool dontinline = true
Feb 10 04:58:13 elastic-stack systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-17/17 (END)
```

Langkah #3: Konfigurasikan Elasticsearch di Ubuntu 24.04 LTS

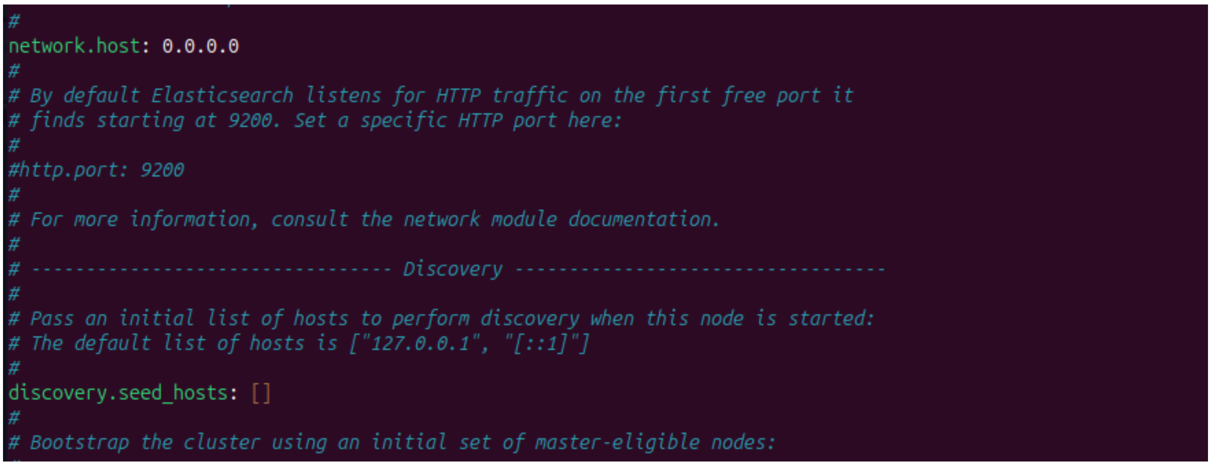
Untuk mengizinkan akses eksternal ke Elasticsearch, ubah file konfigurasi.

$sudo nano /etc/elasticsearch/elasticsearch.yml

Temukan pengaturan network.host, hapus koma, dan atur ke 0.0.0.0 untuk mengikat semua alamat IP yang tersedia dan hapus koma pada bagian discovery untuk menentukan simpul awal untuk pembentukan klaster discovery.seed_hosts: [ ]

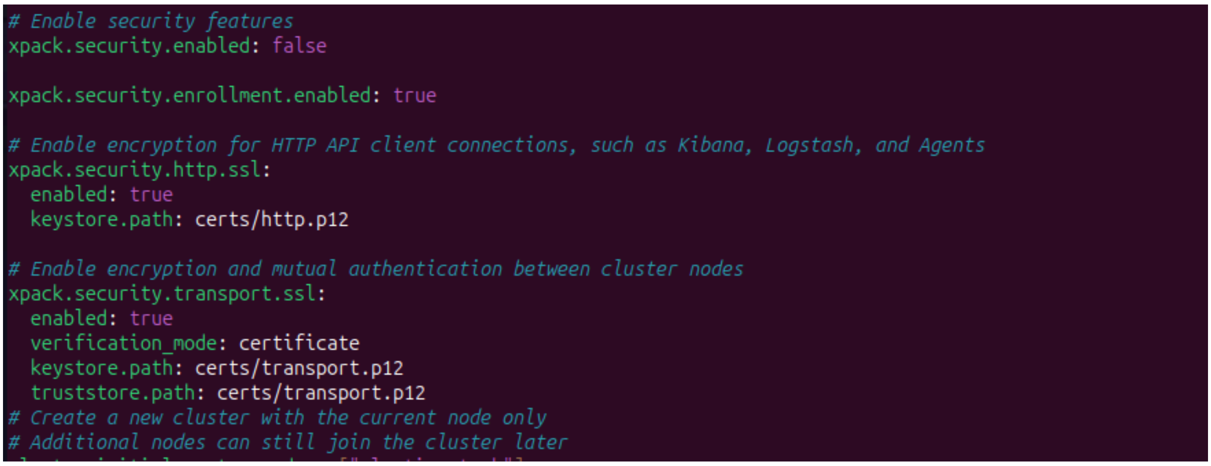
- Network.host: 0.0.0.0

- discovery.seed_hosts: []



```
#
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: []
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
```

untuk pengaturan dasar (tidak disarankan untuk produksi), nonaktifkan fitur keamanan.



```
# Enable security features
xpack.security.enabled: false

xpack.security.enrollment.enabled: true

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

# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  keystore.path: certs/transport.p12
  truststore.path: certs/transport.p12
# Create a new cluster with the current node only
# Additional nodes can still join the cluster later
```

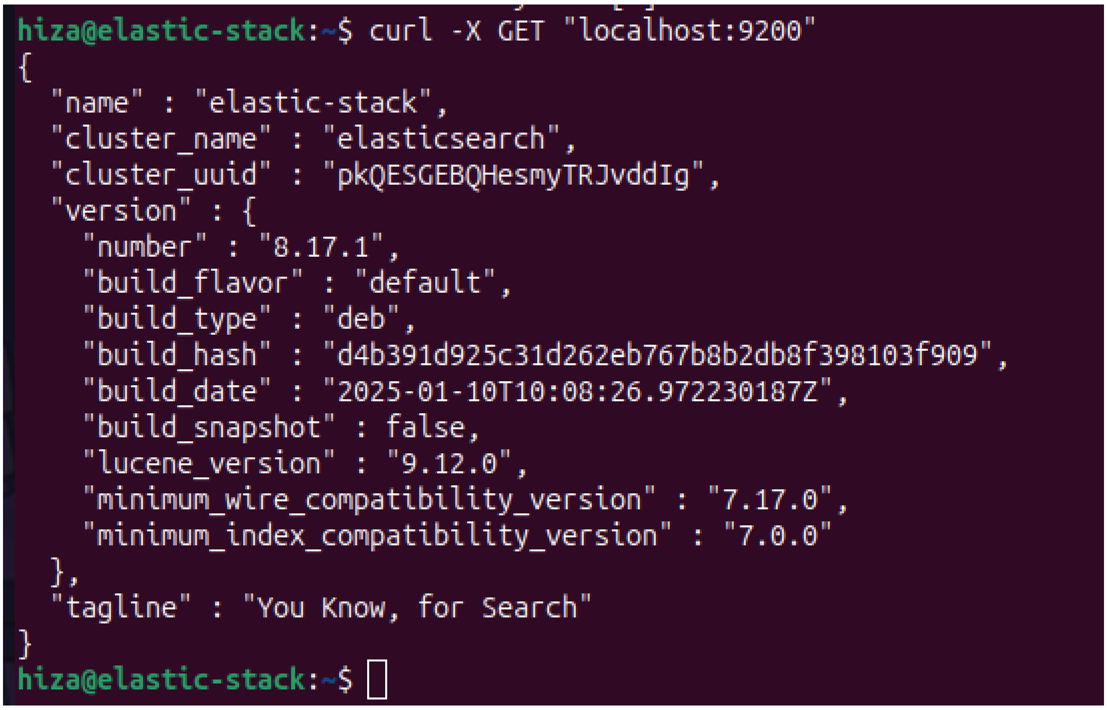
Mulai ulang Elasticsearch untuk menerapkan perubahan.

$sudo systemctl restart elasticsearch

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

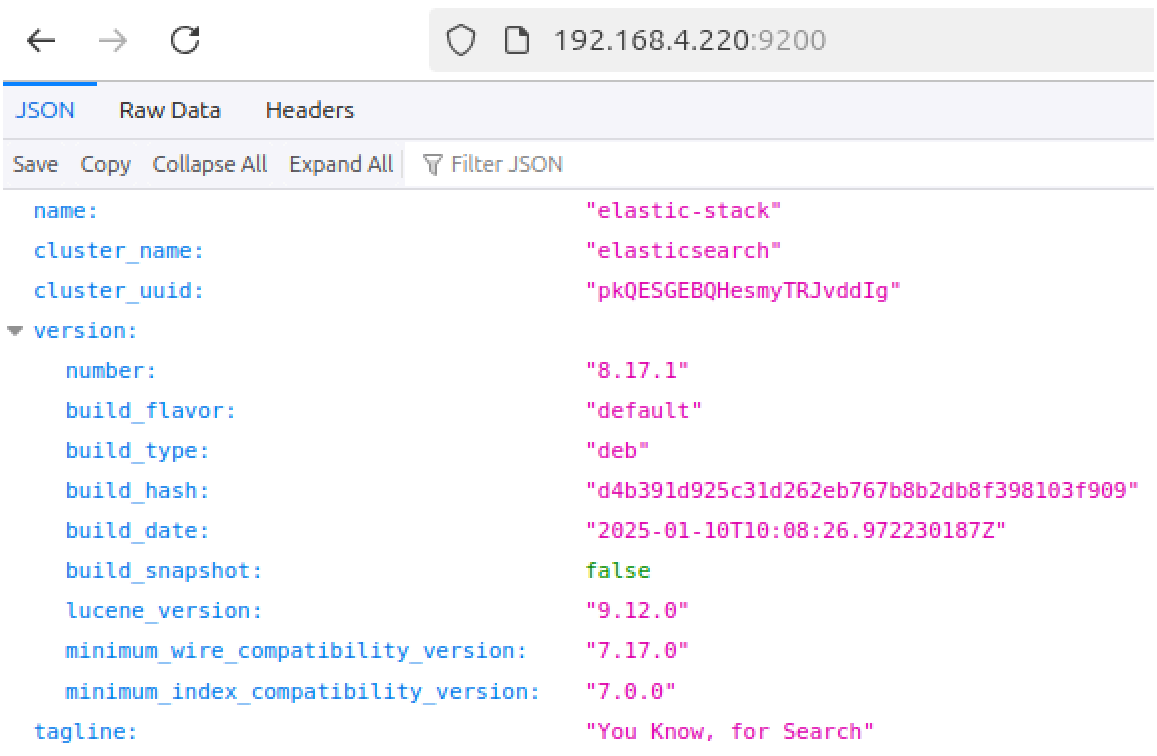
$curl -X GET "localhost:9200"

Anda akan melihat respons JSON.



```
hiza@elastic-stack:~$ curl -X GET "localhost:9200"
{
  "name" : "elastic-stack",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "pkQESGEBQHesmyTRJvddIg",
  "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"
}
hiza@elastic-stack:~$ 
```

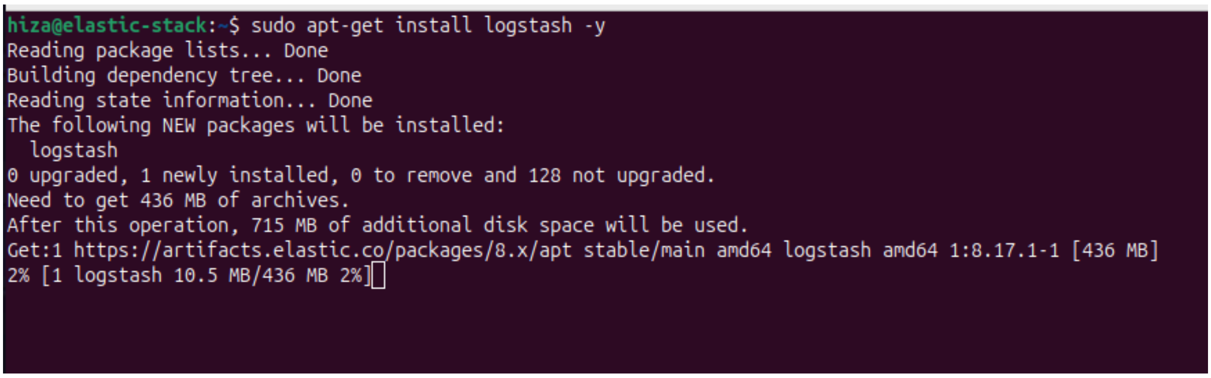
Anda dapat mengaksesnya menggunakan browser dengan alamat IP Publik Anda: port 9200 yang merupakan port default untuk Elasticksearch.



```
name:                                   "elastic-stack"
cluster_name:                           "elasticsearch"
cluster_uuid:                           "pkQESGEBQHesmyTRJvddIg"
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"
```

Langkah #4: Instal Logstash di Ubuntu 24.04 LTS

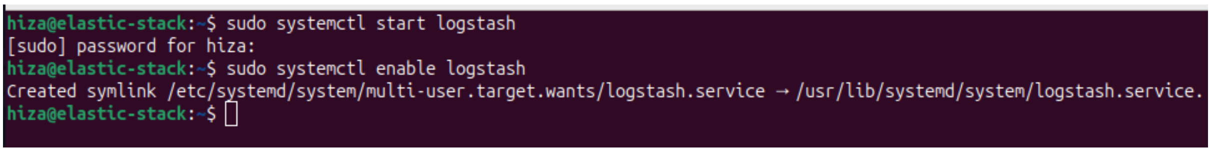
Logstash digunakan untuk memproses dan meneruskan data log ke Elasticsearch.
Instal Logstash menggunakan perintah berikut.
$sudo apt-get install logstash -y



```
hiza@elastic-stack:~$ 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 128 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]
2% [1 logstash 10.5 MB/436 MB 2%]
```

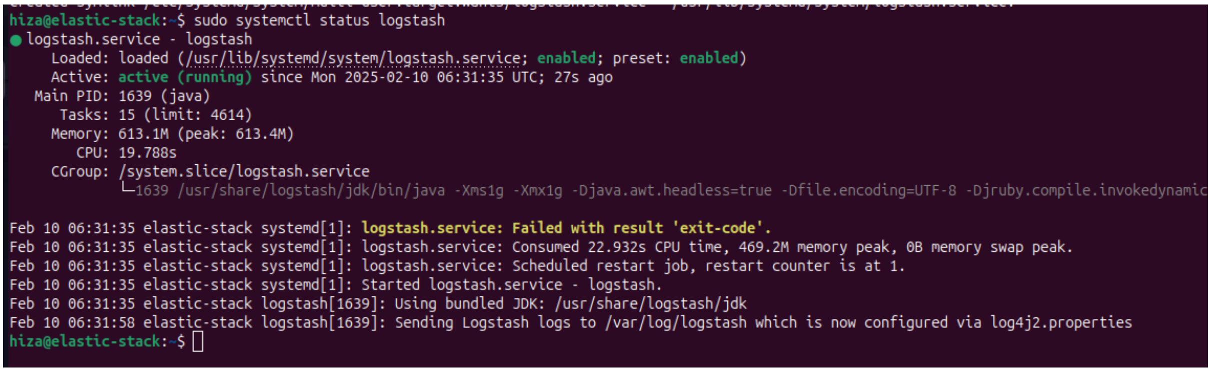
**tunggu sampai proses installasi selesai.*

Mulai dan aktifkan Logstash.
$sudo systemctl start logstash
$sudo systemctl enable logstash



```
hiza@elastic-stack:~$ sudo systemctl start logstash
[sudo] password for hiza:
hiza@elastic-stack:~$ sudo systemctl enable logstash
Created symlink /etc/systemd/system/multi-user.target.wants/logstash.service → /usr/lib/systemd/system/logstash.service.
hiza@elastic-stack:~$
```

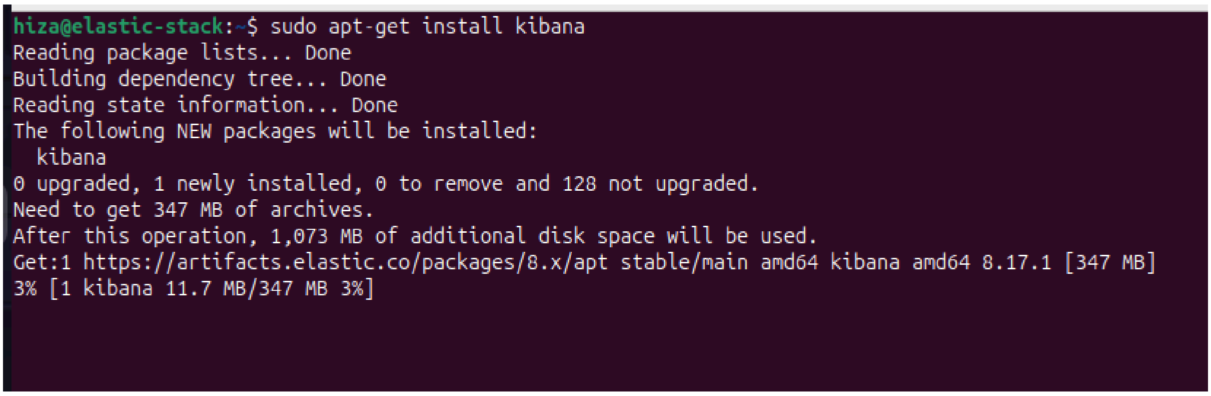
Verifikasi status layanan.
$sudo systemctl status logstash



```
hiza@elastic-stack:~$ sudo systemctl status logstash
● logstash.service - logstash
     Loaded: loaded (/usr/lib/systemd/system/logstash.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-02-10 06:31:35 UTC; 27s ago
   Main PID: 1639 (java)
      Tasks: 15 (limit: 4614)
     Memory: 613.1M (peak: 613.4M)
        CPU: 19.788s
     CGroup: /system.slice/logstash.service
             └─1639 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djruby.compile.invokedynamic

Feb 10 06:31:35 elastic-stack systemd[1]: logstash.service: Failed with result 'exit-code'.
Feb 10 06:31:35 elastic-stack systemd[1]: logstash.service: Consumed 22.932s CPU time, 469.2M memory peak, 0B memory swap peak.
Feb 10 06:31:35 elastic-stack systemd[1]: logstash.service: Scheduled restart job, restart counter is at 1.
Feb 10 06:31:35 elastic-stack systemd[1]: Started logstash.service - logstash.
Feb 10 06:31:35 elastic-stack logstash[1639]: Using bundled JDK: /usr/share/logstash/jdk
Feb 10 06:31:58 elastic-stack logstash[1639]: Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties
hiza@elastic-stack:~$
```

Langkah #5: Instal Kibana di Ubuntu 24.04 LTS

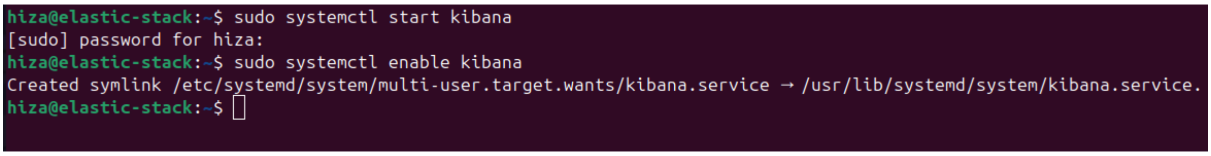
Kibana menyediakan antarmuka web untuk memvisualisasikan data dari Elasticsearch.
Instal Kibana menggunakan perintah berikut.
$sudo apt-get install kibana



```
hiza@elastic-stack:~$ 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 128 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]
3% [1 kibana 11.7 MB/347 MB 3%]
```

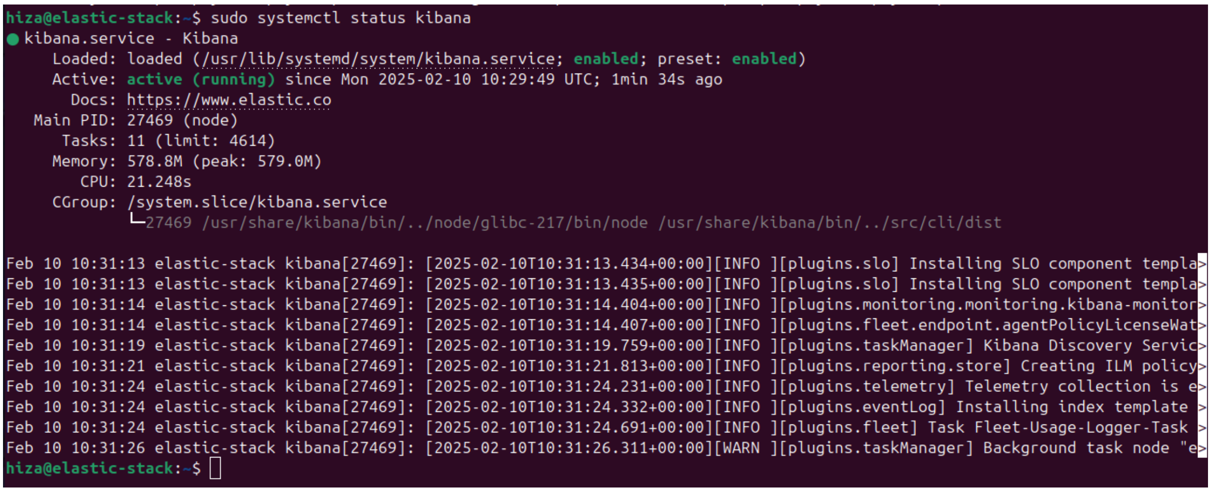
**tunngu sampai proses installasi Selesai*

setelah selesai, Mulai dan aktifkan layanan Kibana.
$sudo systemctl start kibana
$sudo systemctl enable kibana



```
hiza@elastic-stack:~$ sudo systemctl start kibana
[sudo] password for hiza:
hiza@elastic-stack:~$ sudo systemctl enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /usr/lib/systemd/system/kibana.service.
hiza@elastic-stack:~$ 
```

Verivikasi status layanan.
$ sudo systemctl status kibana

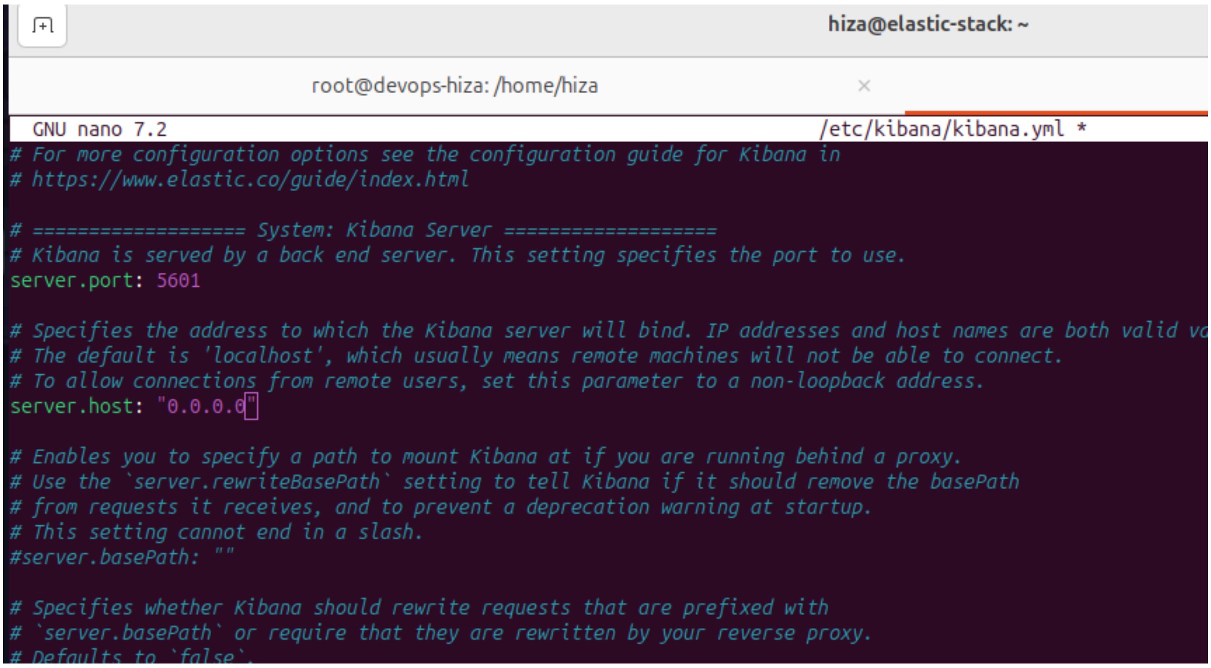


```
hiza@elastic-stack:~$ sudo systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-02-10 10:29:49 UTC; 1min 34s ago
       Docs: https://www.elastic.co
   Main PID: 27469 (node)
      Tasks: 11 (limit: 4614)
     Memory: 578.8M (peak: 579.0M)
        CPU: 21.248s
     CGroup: /system.slice/kibana.service
             └─27469 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

Feb 10 10:31:13 elastic-stack kibana[27469]: [2025-02-10T10:31:13.434+00:00][INFO ][plugins.slo] Installing SLO component templa>
Feb 10 10:31:13 elastic-stack kibana[27469]: [2025-02-10T10:31:13.435+00:00][INFO ][plugins.slo] Installing SLO component templa>
Feb 10 10:31:14 elastic-stack kibana[27469]: [2025-02-10T10:31:14.404+00:00][INFO ][plugins.monitoring.monitoring.kibana-monitor>
Feb 10 10:31:14 elastic-stack kibana[27469]: [2025-02-10T10:31:14.407+00:00][INFO ][plugins.fleet.endpoint.agentPolicyLicenseWat>
Feb 10 10:31:19 elastic-stack kibana[27469]: [2025-02-10T10:31:19.759+00:00][INFO ][plugins.taskManager] Kibana Discovery Servic>
Feb 10 10:31:21 elastic-stack kibana[27469]: [2025-02-10T10:31:21.813+00:00][INFO ][plugins.reporting.store] Creating ILM policy>
Feb 10 10:31:24 elastic-stack kibana[27469]: [2025-02-10T10:31:24.231+00:00][INFO ][plugins.telemetry] Telemetry collection is e>
Feb 10 10:31:24 elastic-stack kibana[27469]: [2025-02-10T10:31:24.332+00:00][INFO ][plugins.eventLog] Installing index template >
Feb 10 10:31:24 elastic-stack kibana[27469]: [2025-02-10T10:31:24.691+00:00][INFO ][plugins.fleet] Task Fleet-Usage-Logger-Task >
Feb 10 10:31:26 elastic-stack kibana[27469]: [2025-02-10T10:31:26.311+00:00][WARN ][plugins.taskManager] Background task node "e>
hiza@elastic-stack:~$ 
```

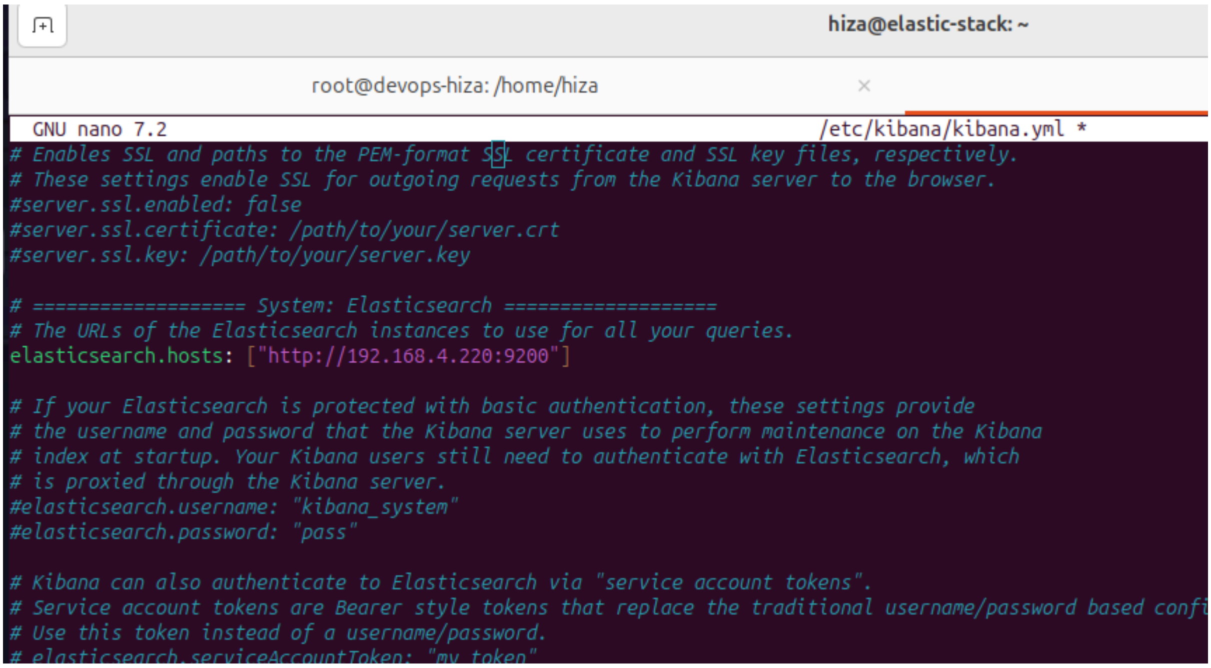
Langkah #6: Konfigurasi Kibana di Ubuntu 24.04 LTS

Untuk mengonfigurasi Kibana untuk akses eksternal, edit file konfigurasi.
$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"]



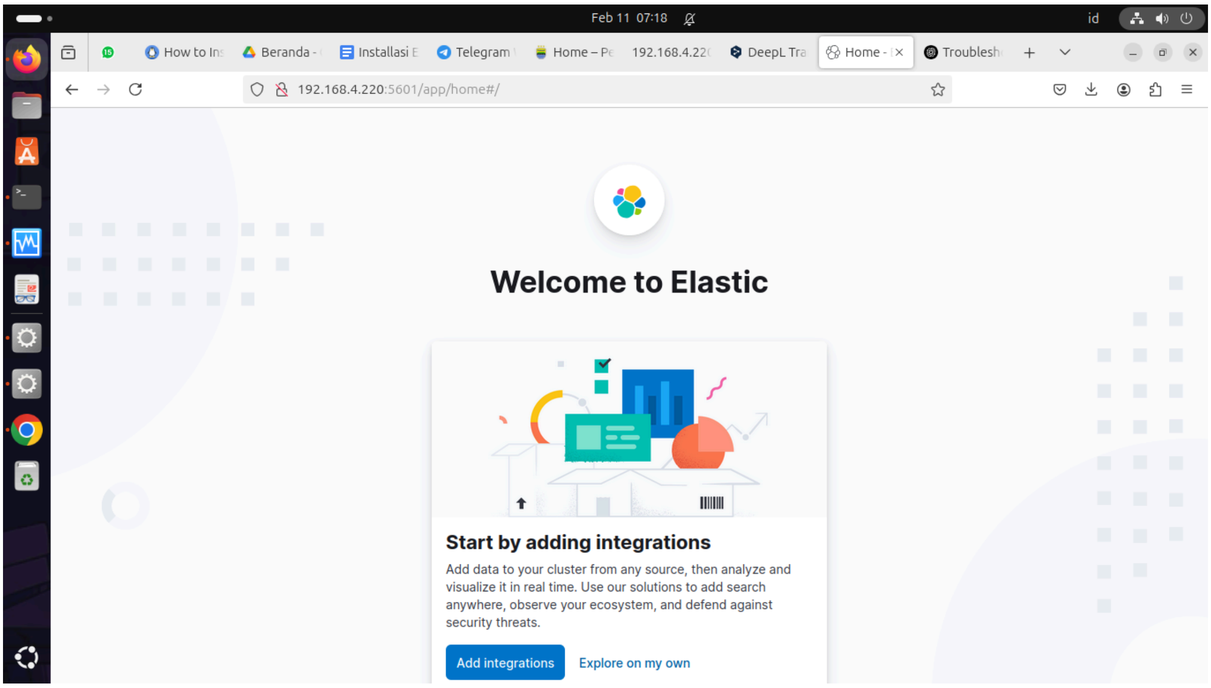
```
  GNU nano 7.2                                            /etc/kibana/kibana.yml *
# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# =================== 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 va
# 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"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#server.basePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# `server.basePath` or require that they are rewritten by your reverse proxy.
# Defaults to `false`.
```



```
  GNU nano 7.2                                            /etc/kibana/kibana.yml *
# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.
# These settings enable SSL for outgoing requests from the Kibana server to the browser.
#server.ssl.enabled: false
#server.ssl.certificate: /path/to/your/server.crt
#server.ssl.key: /path/to/your/server.key

# =================== System: Elasticsearch ===================
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://192.168.4.220:9200"]

# 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"

# Kibana can also authenticate to Elasticsearch via "service account tokens".
# Service account tokens are Bearer style tokens that replace the traditional username/password based confi
# Use this token instead of a username/password.
# elasticsearch.serviceAccountToken: "my_token"
```

Mulai ulang Kibana untuk menerapkan perubahan.
$sudo systemctl restart kibana

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

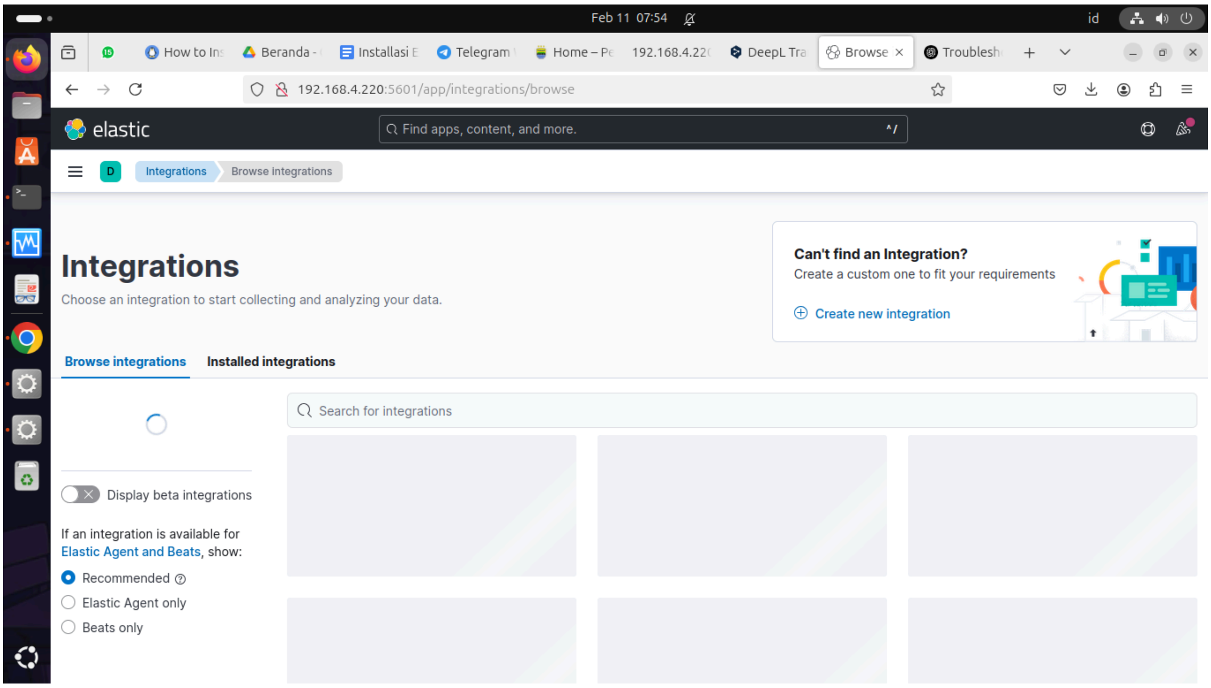


Welcome to Elastic

Start by adding integrations

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.

Anda bisa mulai dengan menambahkan integrasi atau Jelajahi sendiri.



Integrations

Choose an integration to start collecting and analyzing your data.

Can't find an Integration?
Create a custom one to fit your requirements

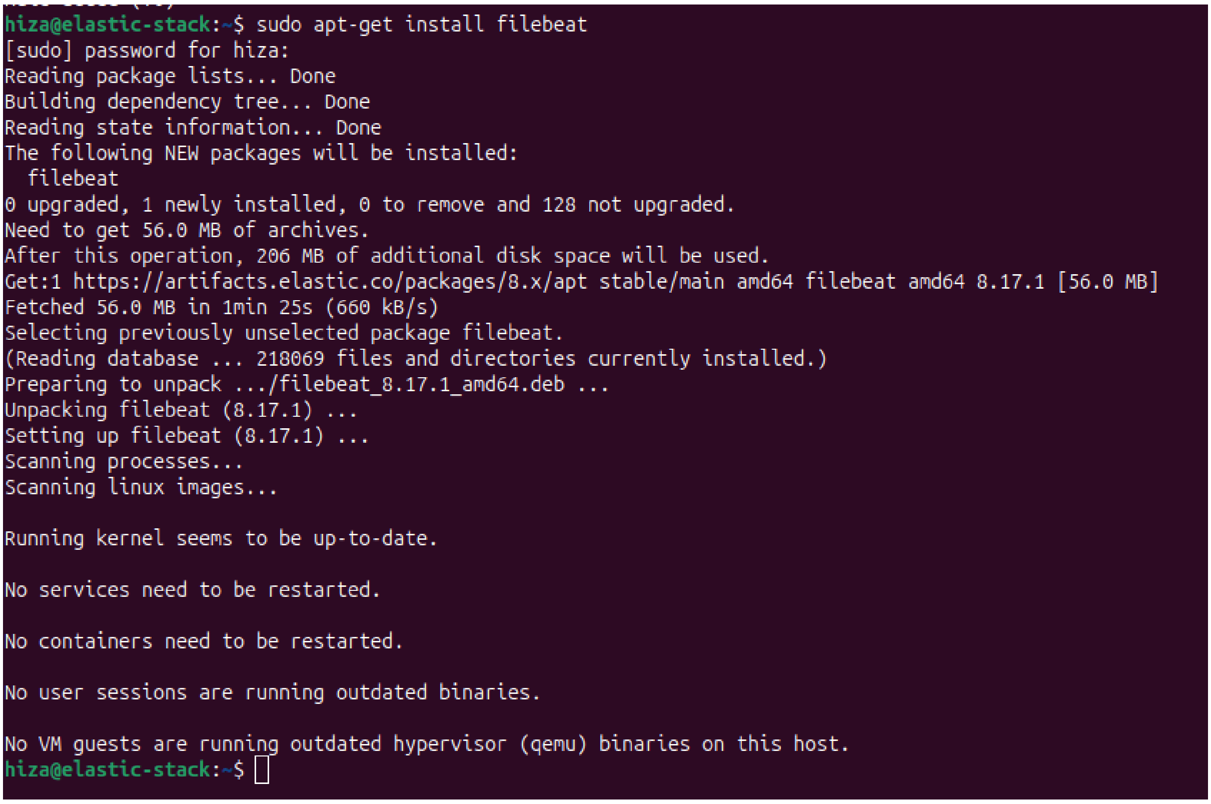
If an integration is available for Elastic Agent and Beats, show:

● Recommended
○ Elastic Agent only
○ Beats only

Langkah #7: Instal Filebeat di Ubuntu 24.04 LTS

Filebeat adalah pengirim ringan yang digunakan untuk meneruskan dan memusatkan data log. Instal Filebeat menggunakan perintah berikut.

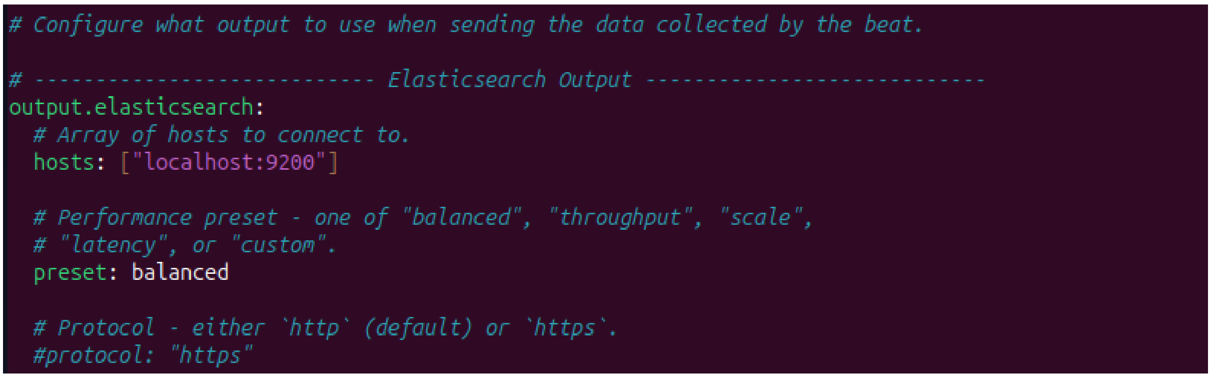
$sudo apt-get install filebeat



```
hiza@elastic-stack:~$ sudo apt-get install filebeat
[sudo] password for hiza:
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 128 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 1min 25s (660 kB/s)
Selecting previously unselected package filebeat.
(Reading database ... 218069 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.
hiza@elastic-stack:~$
```

Buka file konfigurasi Filebeat untuk mengirim log ke Logstash.

$sudo nano /etc/filebeat/filebeat.yml



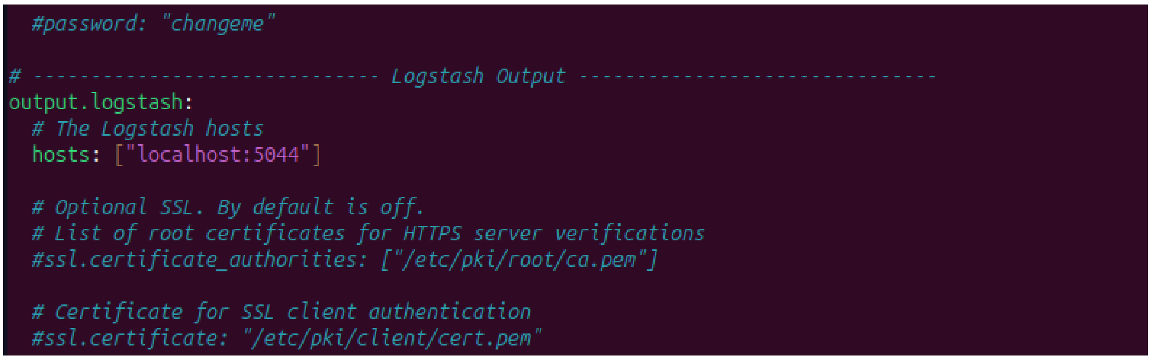
```
# Configure what output to use when sending the data collected by the beat.

# ---------------------------- 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"
```

Beri komentar (#) pada bagian :

#output.elasticsearch:

  #hosts: ["localhost:9200"]

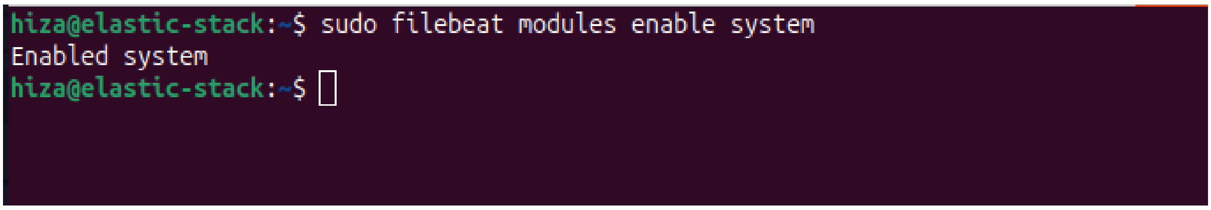
Hapus komentar dan konfigurasikan bagian outputLogstash.



```
  #password: "changeme"

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

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"
```

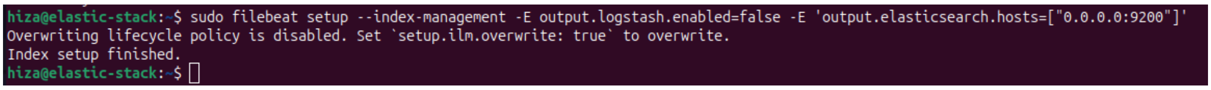
Aktifkan modul sistem, yang mengumpulkan data log dari sistem lokal.

$sudo filebeat modules enable system



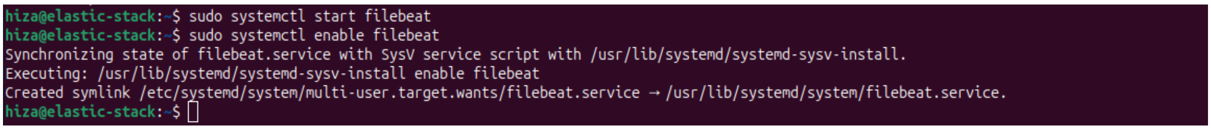
```
hiza@elastic-stack:~$ sudo filebeat modules enable system
Enabled system
hiza@elastic-stack:~$ 
```

Set Up 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"]'



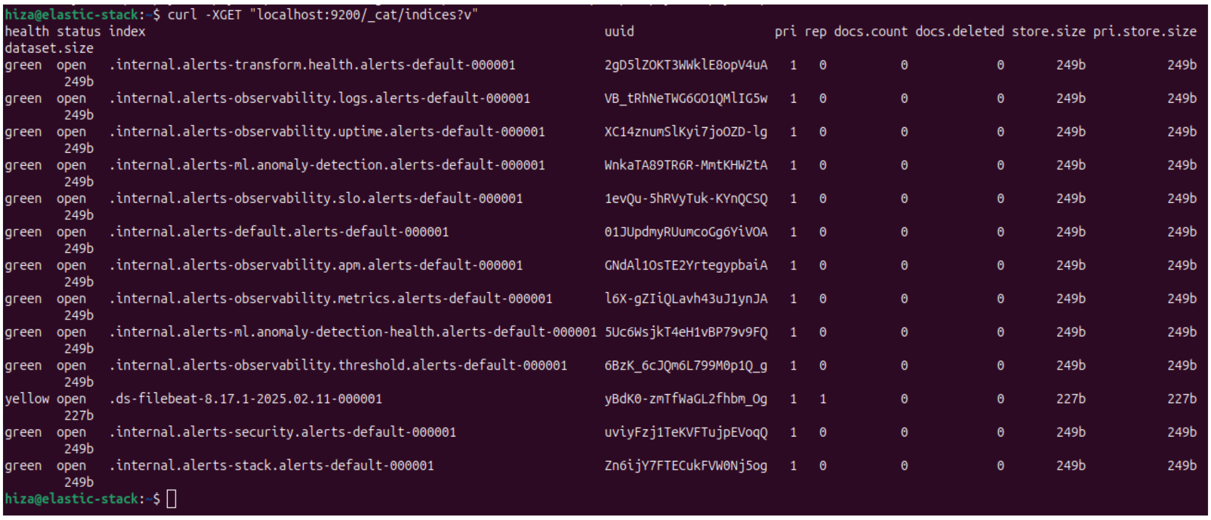
```
hiza@elastic-stack:~$ sudo filebeat setup --index-management -E output.logstash.enabled=false -E 'output.elasticsearch.hosts=["0.0.0.0:9200"]'
Overwriting lifecycle policy is disabled. Set `setup.ilm.overwrite: true` to overwrite.
Index setup finished.
hiza@elastic-stack:~$ 
```

Mulai dan aktifkan layanan Filebeat.
$sudo systemctl start filebeat
$sudo systemctl enable filebeat



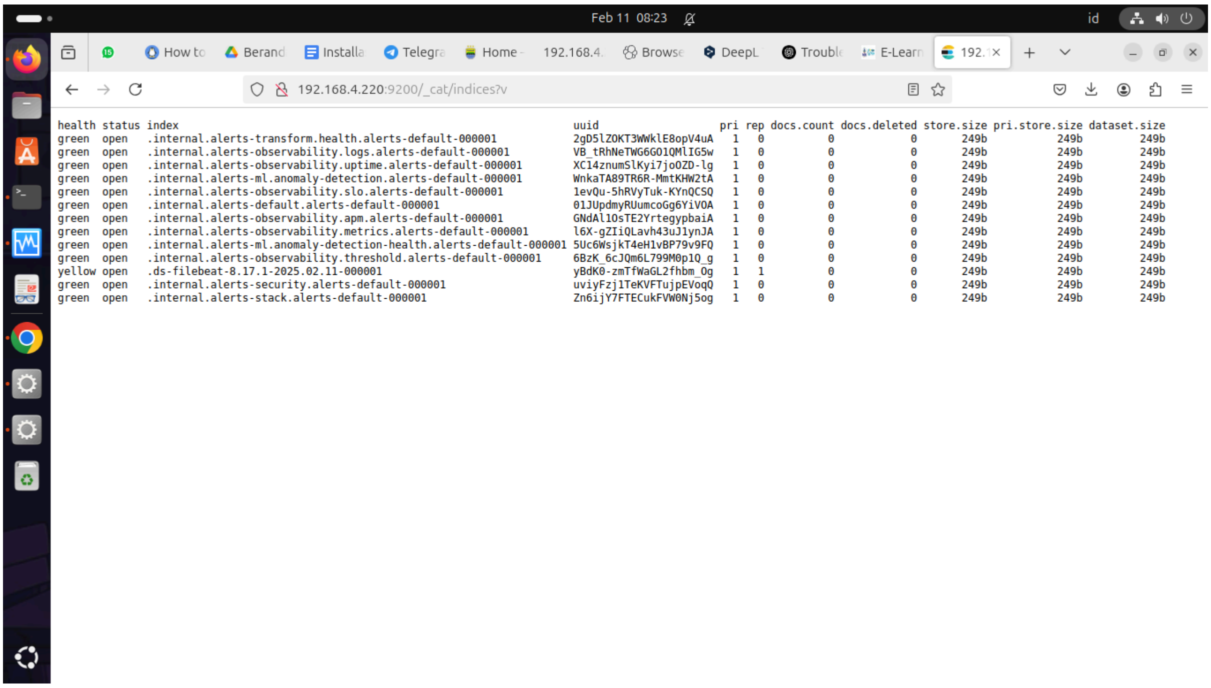
```
hiza@elastic-stack:~$ sudo systemctl start filebeat
hiza@elastic-stack:~$ sudo systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service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

Pastikan Elasticsearch menerima data dari Filebeat dengan memeriksa indeks.
$curl -XGET "localhost:9200/_cat/indices?v"
Anda akan melihat output yang menunjukkan adanya indeks yang dibuat oleh Filebeat.



```
hiza@elastic-stack:~$ curl -XGET "localhost: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-transform.health.alerts-default-000001            2gD5lZOKT3WWklE8opV4uA   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-observability.logs.alerts-default-000001          VB_tRhNeTWG6GO1QMlIG5w   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-observability.uptime.alerts-default-000001        XC14znumSlKyi7joOZD-lg   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-ml.anomaly-detection.alerts-default-000001        WnkaTA89TR6R-MmtKHW2tA   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-observability.slo.alerts-default-000001           1evQu-5hRVyTuk-KYnQCSQ   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-default.alerts-default-000001                     01JUpdmyRUumcoGg6YiVOA   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-observability.apm.alerts-default-000001           GNdAl1OsTE2YrtegypbaiA   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-observability.metrics.alerts-default-000001       l6X-gZIiQLavh43uJ1ynJA   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-ml.anomaly-detection-health.alerts-default-000001 5Uc6WsjkT4eH1vBP79v9FQ   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-observability.threshold.alerts-default-000001     6BzK_6cJQm6L799M0p1Q_g   1   0          0            0       249b           249b
        249b
yellow open   .ds-filebeat-8.17.1-2025.02.11-000001                              yBdK0-zmTfWaGL2fhbm_Og   1   1          0            0       227b           227b
        227b
green  open   .internal.alerts-security.alerts-default-000001                    uviyFzj1TeKVFTujpEVoqQ   1   0          0            0       249b           249b
        249b
green  open   .internal.alerts-stack.alerts-default-000001                       Zn6ijY7FTECukFVW0Nj5og   1   0          0            0       249b           249b
        249b
hiza@elastic-stack:~$ 
```

Anda dapat mengaksesnya menggunakan browser dengan menggunakan
http://<your-server-ip>: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-transform.health.alerts-default-000001            2gD5lZOKT3WWklE8opV4uA   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-observability.logs.alerts-default-000001          VB_tRhNeTWG6GO1QMlIG5w   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-observability.uptime.alerts-default-000001        XC14znumSlKyi7joOZD-lg   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-ml.anomaly-detection.alerts-default-000001        WnkaTA89TR6R-MmtKHW2tA   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-observability.slo.alerts-default-000001           1evQu-5hRVyTuk-KYnQCSQ   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-default.alerts-default-000001                     01JUpdmyRUumcoGg6YiVOA   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-observability.apm.alerts-default-000001           GNdAl1OsTE2YrtegypbaiA   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-observability.metrics.alerts-default-000001       l6X-gZIiQLavh43uJ1ynJA   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-ml.anomaly-detection-health.alerts-default-000001 5Uc6WsjkT4eH1vBP79v9FQ   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-observability.threshold.alerts-default-000001     6BzK_6cJQm6L799M0p1Q_g   1   0          0            0       249b           249b         249b
yellow open   .ds-filebeat-8.17.1-2025.02.11-000001                              yBdK0-zmTfWaGL2fhbm_Og   1   1          0            0       249b           249b         249b
green  open   .internal.alerts-security.alerts-default-000001                    uviyFzj1TeKVFTujpEVoqQ   1   0          0            0       249b           249b         249b
green  open   .internal.alerts-stack.alerts-default-000001                       Zn6ijY7FTECukFVW0Nj5og   1   0          0            0       249b           249b         249b
```

Kesimpulan:

Kesimpulannya, saya telah berhasil menginstal dan mengonfigurasi Elastic Stack di Ubuntu 24.04 LTS. Ini termasuk menyiapkan Elasticsearch untuk pencarian dan analisis, Logstash untuk pemrosesan data, Kibana untuk visualisasi data, dan Filebeat untuk pengiriman log. Elastic Stack menyediakan solusi yang kuat untuk pencatatan dan analisis data terpusat, sehingga sangat berharga untuk memantau dan menganalisis kinerja sistem dan log aplikasi.

sumber : https://www.fosstechnix.com/how-to-install-elastic-stack-on-ubuntu-24-04/

Pemilik Tutorial:

Arbabil Hiza