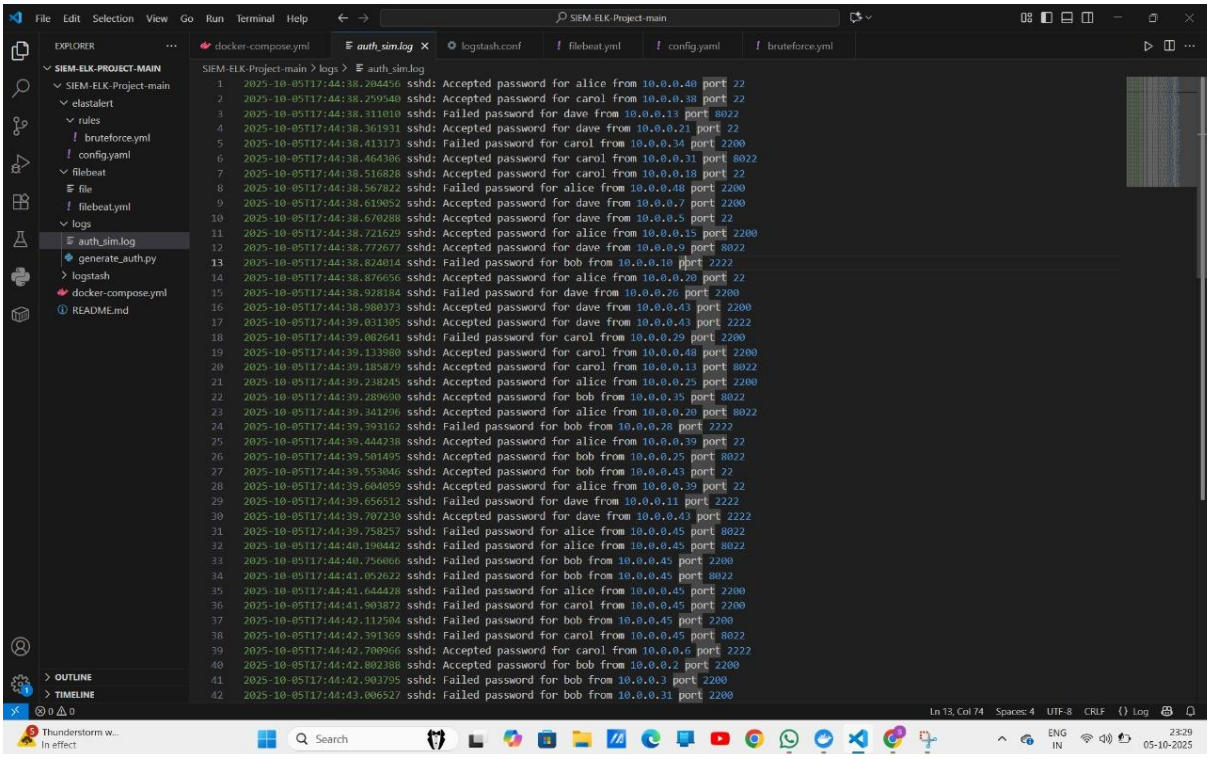
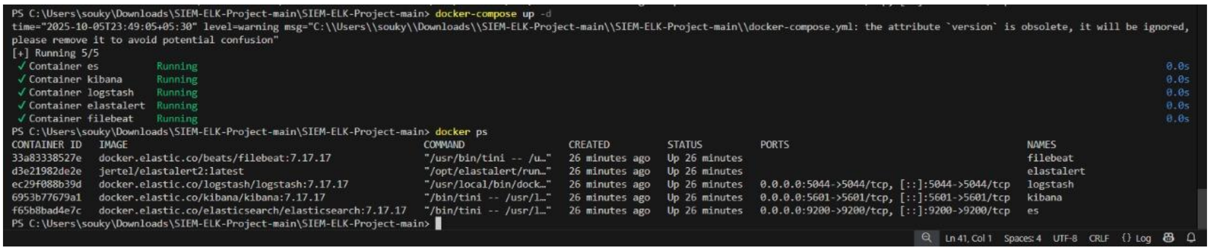
1.Log simulation using
python generate_logs.py



```
2025-10-05T17:44:38.204456 sshd: Accepted password for alice from 10.0.0.40 port 22
2025-10-05T17:44:38.259540 sshd: Accepted password for carol from 10.0.0.38 port 22
2025-10-05T17:44:38.311010 sshd: Failed password for dave from 10.0.0.13 port 8022
2025-10-05T17:44:38.361931 sshd: Accepted password for dave from 10.0.0.21 port 22
2025-10-05T17:44:38.413173 sshd: Failed password for carol from 10.0.0.34 port 2200
2025-10-05T17:44:38.464306 sshd: Accepted password for carol from 10.0.0.31 port 8022
2025-10-05T17:44:38.516828 sshd: Accepted password for carol from 10.0.0.18 port 22
2025-10-05T17:44:38.567822 sshd: Failed password for alice from 10.0.0.48 port 2200
2025-10-05T17:44:38.619052 sshd: Accepted password for dave from 10.0.0.7 port 2200
2025-10-05T17:44:38.670288 sshd: Accepted password for dave from 10.0.0.5 port 22
2025-10-05T17:44:38.721629 sshd: Accepted password for alice from 10.0.0.15 port 2200
2025-10-05T17:44:38.772677 sshd: Accepted password for dave from 10.0.0.9 port 8022
2025-10-05T17:44:38.824014 sshd: Failed password for bob from 10.0.0.10 port 2222
2025-10-05T17:44:38.876656 sshd: Accepted password for alice from 10.0.0.20 port 22
2025-10-05T17:44:38.928184 sshd: Failed password for dave from 10.0.0.26 port 2200
2025-10-05T17:44:38.980373 sshd: Accepted password for dave from 10.0.0.43 port 2200
2025-10-05T17:44:39.031305 sshd: Accepted password for dave from 10.0.0.43 port 2222
2025-10-05T17:44:39.082641 sshd: Failed password for carol from 10.0.0.29 port 2200
2025-10-05T17:44:39.133980 sshd: Accepted password for carol from 10.0.0.48 port 2200
2025-10-05T17:44:39.185879 sshd: Accepted password for carol from 10.0.0.13 port 8022
2025-10-05T17:44:39.238245 sshd: Accepted password for alice from 10.0.0.25 port 2200
2025-10-05T17:44:39.289690 sshd: Accepted password for bob from 10.0.0.35 port 8022
2025-10-05T17:44:39.341296 sshd: Accepted password for alice from 10.0.0.20 port 8022
2025-10-05T17:44:39.393162 sshd: Failed password for bob from 10.0.0.28 port 2222
2025-10-05T17:44:39.444238 sshd: Accepted password for alice from 10.0.0.39 port 22
2025-10-05T17:44:39.501495 sshd: Accepted password for bob from 10.0.0.25 port 8022
2025-10-05T17:44:39.553046 sshd: Accepted password for bob from 10.0.0.43 port 22
2025-10-05T17:44:39.604059 sshd: Accepted password for alice from 10.0.0.39 port 22
2025-10-05T17:44:39.656512 sshd: Failed password for dave from 10.0.0.11 port 2222
2025-10-05T17:44:39.707230 sshd: Accepted password for dave from 10.0.0.43 port 2222
2025-10-05T17:44:39.758257 sshd: Failed password for alice from 10.0.0.45 port 8022
2025-10-05T17:44:40.190442 sshd: Failed password for alice from 10.0.0.45 port 8022
2025-10-05T17:44:40.756066 sshd: Failed password for bob from 10.0.0.45 port 2200
2025-10-05T17:44:41.052622 sshd: Failed password for bob from 10.0.0.45 port 8022
2025-10-05T17:44:41.644428 sshd: Failed password for alice from 10.0.0.45 port 2200
2025-10-05T17:44:41.903872 sshd: Failed password for carol from 10.0.0.45 port 2200
2025-10-05T17:44:42.112504 sshd: Failed password for bob from 10.0.0.45 port 2200
2025-10-05T17:44:42.391369 sshd: Failed password for carol from 10.0.0.45 port 8022
2025-10-05T17:44:42.700966 sshd: Accepted password for carol from 10.0.0.6 port 2222
2025-10-05T17:44:42.802388 sshd: Accepted password for bob from 10.0.0.2 port 2200
2025-10-05T17:44:42.903795 sshd: Failed password for bob from 10.0.0.3 port 2200
2025-10-05T17:44:43.006527 sshd: Failed password for bob from 10.0.0.31 port 2200
```

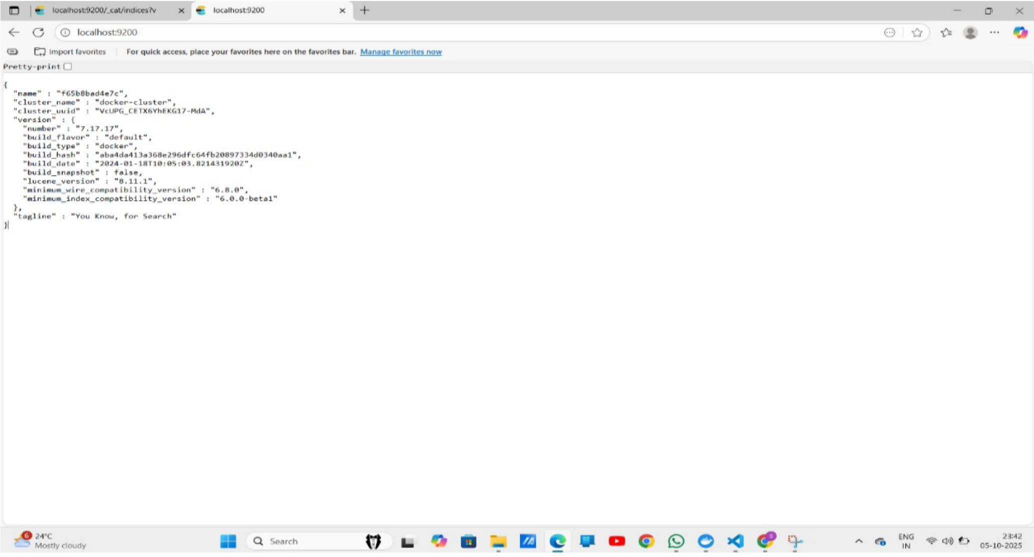
2.Running docker configuration file to pull elk stack images
docker-compose up -d

Docker ps (to test the status of images)

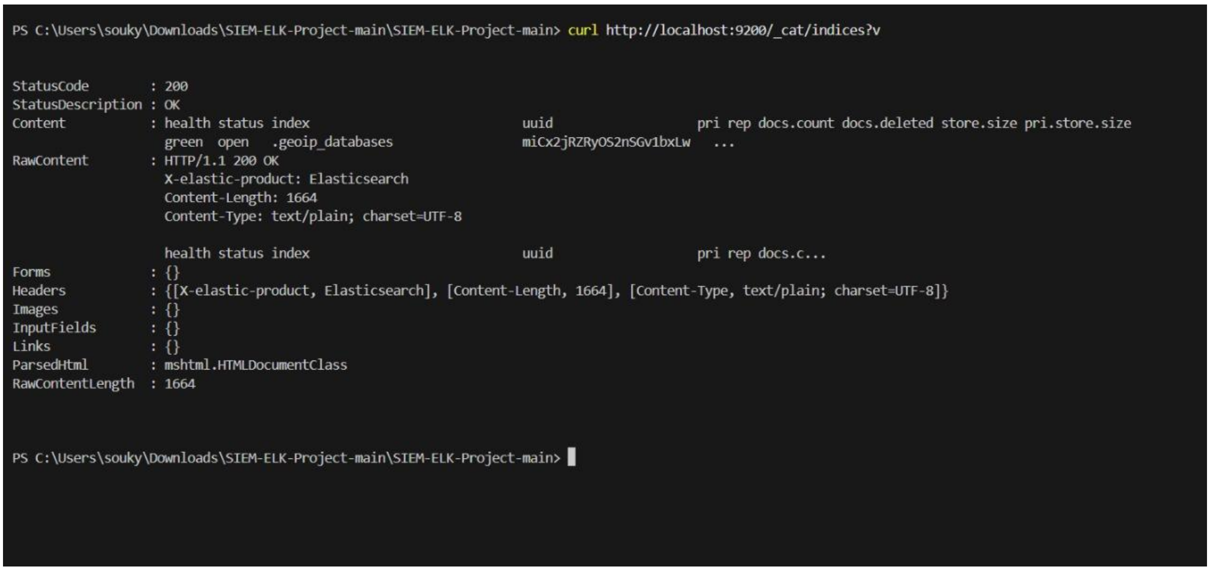


```
PS C:\Users\souky\Downloads\SIEM-ELK-Project-main\SIEM-ELK-Project-main> docker-compose up -d
time="2025-10-05T23:49:05+05:30" level=warning msg="C:\\Users\\souky\\Downloads\\SIEM-ELK-Project-main\\SIEM-ELK-Project-main\\docker-compose.yml: the attribute `version` is obsolete, it will be ignored,
please remove it to avoid potential confusion"
[+] Running 5/5
 ✓ Container es          Running                                                                                                   0.0s
 ✓ Container kibana      Running                                                                                                   0.0s
 ✓ Container logstash    Running                                                                                                   0.0s
 ✓ Container elastalert  Running                                                                                                   0.0s
 ✓ Container filebeat    Running                                                                                                   0.0s
PS C:\Users\souky\Downloads\SIEM-ELK-Project-main\SIEM-ELK-Project-main> docker ps
CONTAINER ID   IMAGE                                                  COMMAND                  CREATED          STATUS          PORTS                                        NAMES
33a83338527e   docker.elastic.co/beats/filebeat:7.17.17               "/usr/bin/tini -- /u…"   26 minutes ago   Up 26 minutes                                                filebeat
d3e21982de2e   jertel/elastalert2:latest                              "/opt/elastalert/run…"   26 minutes ago   Up 26 minutes                                                elastalert
ec29f088b39d   docker.elastic.co/logstash/logstash:7.17.17            "/usr/local/bin/dock…"   26 minutes ago   Up 26 minutes   0.0.0.0:5044->5044/tcp, [::]:5044->5044/tcp   logstash
6953b77679a1   docker.elastic.co/kibana/kibana:7.17.17                "/bin/tini -- /usr/l…"   26 minutes ago   Up 26 minutes   0.0.0.0:5601->5601/tcp, [::]:5601->5601/tcp   kibana
f65b8bad4e7c   docker.elastic.co/elasticsearch/elasticsearch:7.17.17   "/bin/tini -- /usr/l…"   26 minutes ago   Up 26 minutes   0.0.0.0:9200->9200/tcp, [::]:9200->9200/tcp   es
PS C:\Users\souky\Downloads\SIEM-ELK-Project-main\SIEM-ELK-Project-main>
```

3.sample Raw data structure collected using filebeat agent

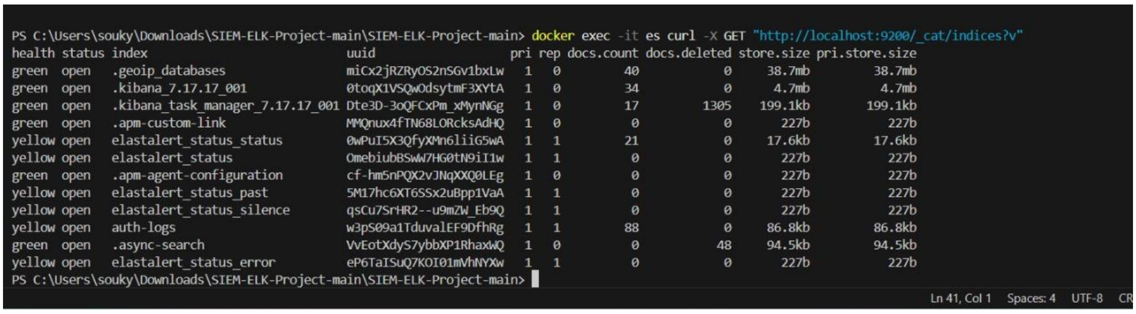

localhost:9200/_cat/indices?v
localhost:9200
localhost:9200
Import favorites
For quick access, place your favorites here on the favorites bar. Manage favorites now
Pretty-print □
24°C
Mostly cloudy
Search
ENG
IN
23:42
05-10-2025

```
{
  "name" : "f65b8bad4e7c",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "VcUPG_CETX6YhEKG17-MdA",
  "version" : {
    "number" : "7.17.17",
    "build_flavor" : "default",
    "build_type" : "docker",
    "build_hash" : "aba4da413a368e296dfc64fb20897334d0340aa1",
    "build_date" : "2024-01-18T10:05:03.821431920Z",
    "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"
}
```



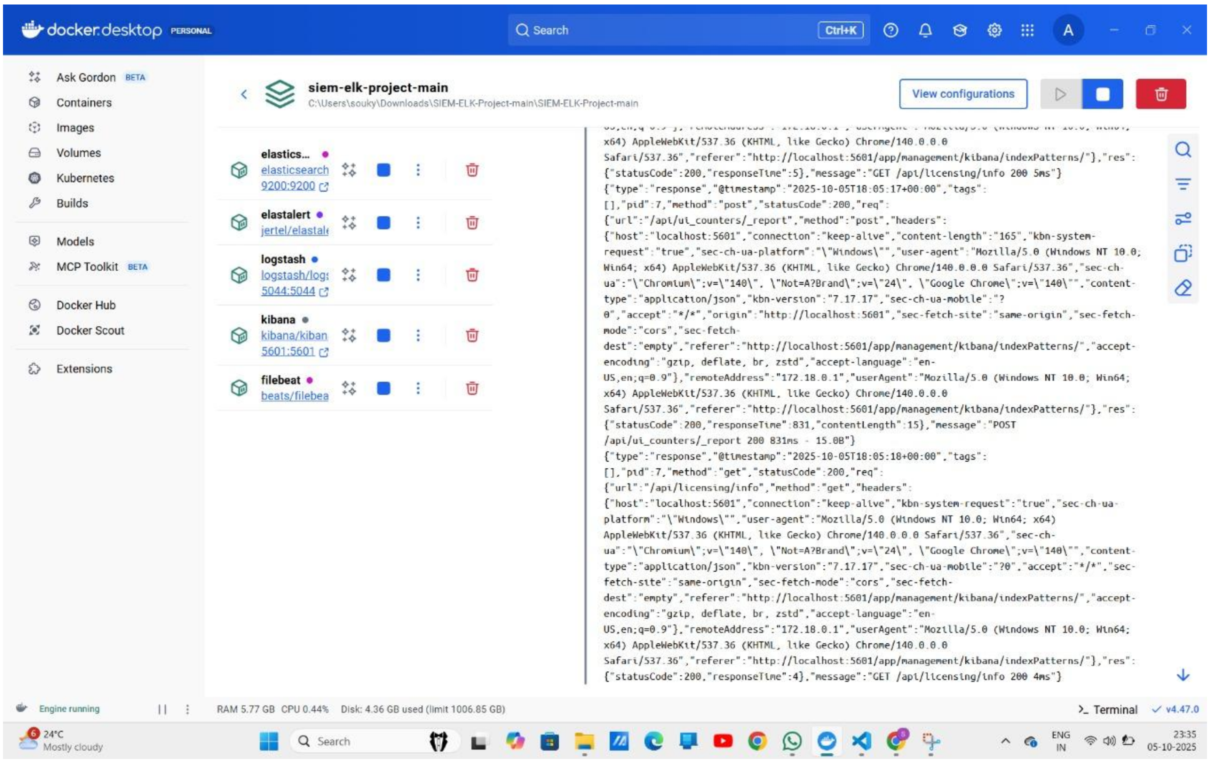
```
PS C:\Users\souky\Downloads\SIEM-ELK-Project-main\SIEM-ELK-Project-main> curl http://localhost:9200/_cat/indices?v


StatusCode        : 200
StatusDescription : OK
Content           : health status index                      uuid                   pri rep docs.count docs.deleted store.size pri.store.size
                    green  open   .geoip_databases           miCx2jRZRyOS2nSGv1bxLw   ...
RawContent        : HTTP/1.1 200 OK
                    X-elastic-product: Elasticsearch
                    Content-Length: 1664
                    Content-Type: text/plain; charset=UTF-8

                    health status index                      uuid                   pri rep docs.c...
Forms             : {}
Headers           : {[X-elastic-product, Elasticsearch], [Content-Length, 1664], [Content-Type, text/plain; charset=UTF-8]}
Images            : {}
InputFields       : {}
Links             : {}
ParsedHtml        : mshtml.HTMLDocumentClass
RawContentLength  : 1664



PS C:\Users\souky\Downloads\SIEM-ELK-Project-main\SIEM-ELK-Project-main> 
```

4.Health status index



```
PS C:\Users\souky\Downloads\SIEM-ELK-Project-main\SIEM-ELK-Project-main> docker exec -it es curl -X GET "http://localhost:9200/_cat/indices?v"
health status index                            uuid                   pri rep docs.count docs.deleted store.size pri.store.size
green  open   .geoip_databases                 miCx2jRZRyOS2nSGv1bxLw   1   0         40            0     38.7mb         38.7mb
green  open   .kibana_7.17.17_001              0toqX1VSQwOdsytmF3XYtA   1   0         34            0      4.7mb          4.7mb
green  open   .kibana_task_manager_7.17.17_001 Dte3D-3oQFCxPm_xMynNGg   1   0         17         1305    199.1kb        199.1kb
green  open   .apm-custom-link                 MMQnux4fTN68LORcksAdHQ   1   0          0            0       227b           227b
yellow open   elastalert_status_status         0wPuI5X3QfyXMn6liiG5wA   1   1         21            0     17.6kb         17.6kb
yellow open   elastalert_status                OmebiubBSwW7HG0tN9iI1w   1   1          0            0       227b           227b
green  open   .apm-agent-configuration         cf-hm5nPQX2vJNqXXQ0LEg   1   0          0            0       227b           227b
yellow open   elastalert_status_past           5M17hc6XT6SSx2uBpp1VaA   1   1          0            0       227b           227b
yellow open   elastalert_status_silence        qsCu7SrHR2--u9mZW_Eb9Q   1   1          0            0       227b           227b
yellow open   auth-logs                        w3pS09a1TduvalEF9DfhRg   1   1         88            0     86.8kb         86.8kb
green  open   .async-search                    VvEotXdyS7ybbXP1RhaxWQ   1   0          0           48     94.5kb         94.5kb
yellow open   elastalert_status_error          eP6TaISuQ7KOI01mVhNYXw   1   1          0            0       227b           227b
PS C:\Users\souky\Downloads\SIEM-ELK-Project-main\SIEM-ELK-Project-main> 
```

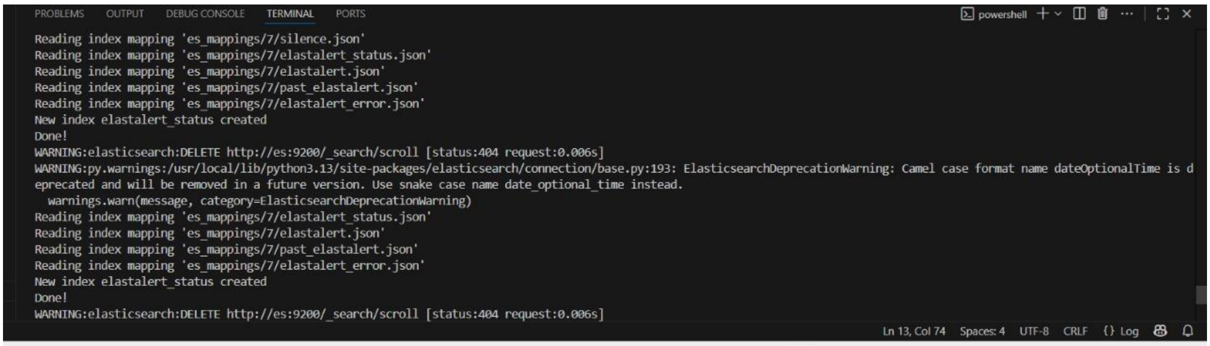
5.Images running in containerised environment in docker



```
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36","referer":"http://localhost:5601/app/management/kibana/indexPatterns/"},"res":
{"statusCode":200,"responseTime":5},"message":"GET /api/licensing/info 200 5ms"}
{"type":"response","@timestamp":"2025-10-05T18:05:17+00:00","tags":
[],"pid":7,"method":"post","statusCode":200,"req":
{"url":"/api/ui_counters/_report","method":"post","headers":
{"host":"localhost:5601","connection":"keep-alive","content-length":"165","kbn-system-
request":"true","sec-ch-ua-platform":"\"Windows\"","user-agent":"Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36","sec-ch-
ua":"\"Chromium\";v=\"140\", \"Not=A?Brand\";v=\"24\", \"Google Chrome\";v=\"140\"","content-
type":"application/json","kbn-version":"7.17.17","sec-ch-ua-mobile":"?
0","accept":"*/*","origin":"http://localhost:5601","sec-fetch-site":"same-origin","sec-fetch-
mode":"cors","sec-fetch-
dest":"empty","referer":"http://localhost:5601/app/management/kibana/indexPatterns/","accept-
encoding":"gzip, deflate, br, zstd","accept-language":"en-
US,en;q=0.9"},"remoteAddress":"172.18.0.1","userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36","referer":"http://localhost:5601/app/management/kibana/indexPatterns/"},"res":
{"statusCode":200,"responseTime":831,"contentLength":15},"message":"POST
/api/ui_counters/_report 200 831ms - 15.0B"}
{"type":"response","@timestamp":"2025-10-05T18:05:18+00:00","tags":
[],"pid":7,"method":"get","statusCode":200,"req":
{"url":"/api/licensing/info","method":"get","headers":
{"host":"localhost:5601","connection":"keep-alive","kbn-system-request":"true","sec-ch-ua-
platform":"\"Windows\"","user-agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36","sec-ch-
ua":"\"Chromium\";v=\"140\", \"Not=A?Brand\";v=\"24\", \"Google Chrome\";v=\"140\"","content-
type":"application/json","kbn-version":"7.17.17","sec-ch-ua-mobile":"?0","accept":"*/*","sec-
fetch-site":"same-origin","sec-fetch-mode":"cors","sec-fetch-
dest":"empty","referer":"http://localhost:5601/app/management/kibana/indexPatterns/","accept-
encoding":"gzip, deflate, br, zstd","accept-language":"en-
US,en;q=0.9"},"remoteAddress":"172.18.0.1","userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0
Safari/537.36","referer":"http://localhost:5601/app/management/kibana/indexPatterns/"},"res":
{"statusCode":200,"responseTime":4},"message":"GET /api/licensing/info 200 4ms"}
```

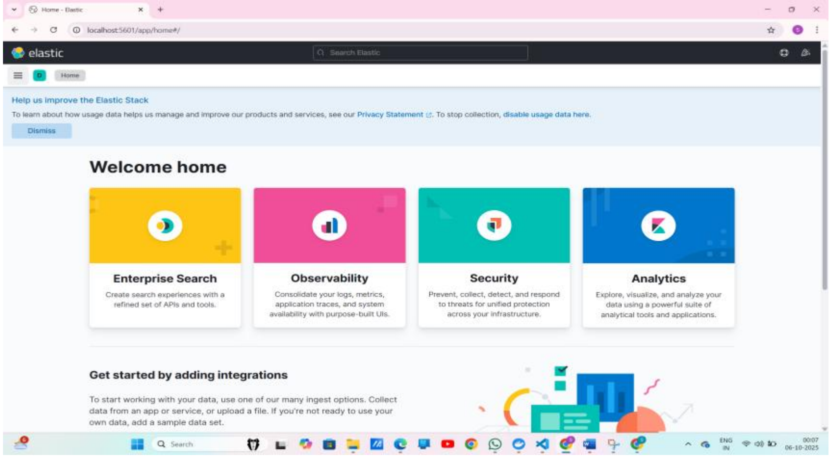
6.Elast alert test

>>>docker logs elastalert



```
Reading index mapping 'es_mappings/7/silence.json'
Reading index mapping 'es_mappings/7/elastalert_status.json'
Reading index mapping 'es_mappings/7/elastalert.json'
Reading index mapping 'es_mappings/7/past_elastalert.json'
Reading index mapping 'es_mappings/7/elastalert_error.json'
New index elastalert_status created
Done!
WARNING:elasticsearch:DELETE http://es:9200/_search/scroll [status:404 request:0.006s]
WARNING:py.warnings:/usr/local/lib/python3.13/site-packages/elasticsearch/connection/base.py:193: ElasticsearchDeprecationWarning: Camel case format name dateOptionalTime is d
eprecated and will be removed in a future version. Use snake case name date_optional_time instead.
  warnings.warn(message, category=ElasticsearchDeprecationWarning)
Reading index mapping 'es_mappings/7/elastalert_status.json'
Reading index mapping 'es_mappings/7/elastalert.json'
Reading index mapping 'es_mappings/7/past_elastalert.json'
Reading index mapping 'es_mappings/7/elastalert_error.json'
New index elastalert_status created
Done!
WARNING:elasticsearch:DELETE http://es:9200/_search/scroll [status:404 request:0.006s]
```

7.Kibana (Visualization and analysis tool) --http://localhost:5601/



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Welcome home

Enterprise Search

Create search experiences with a refined set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics

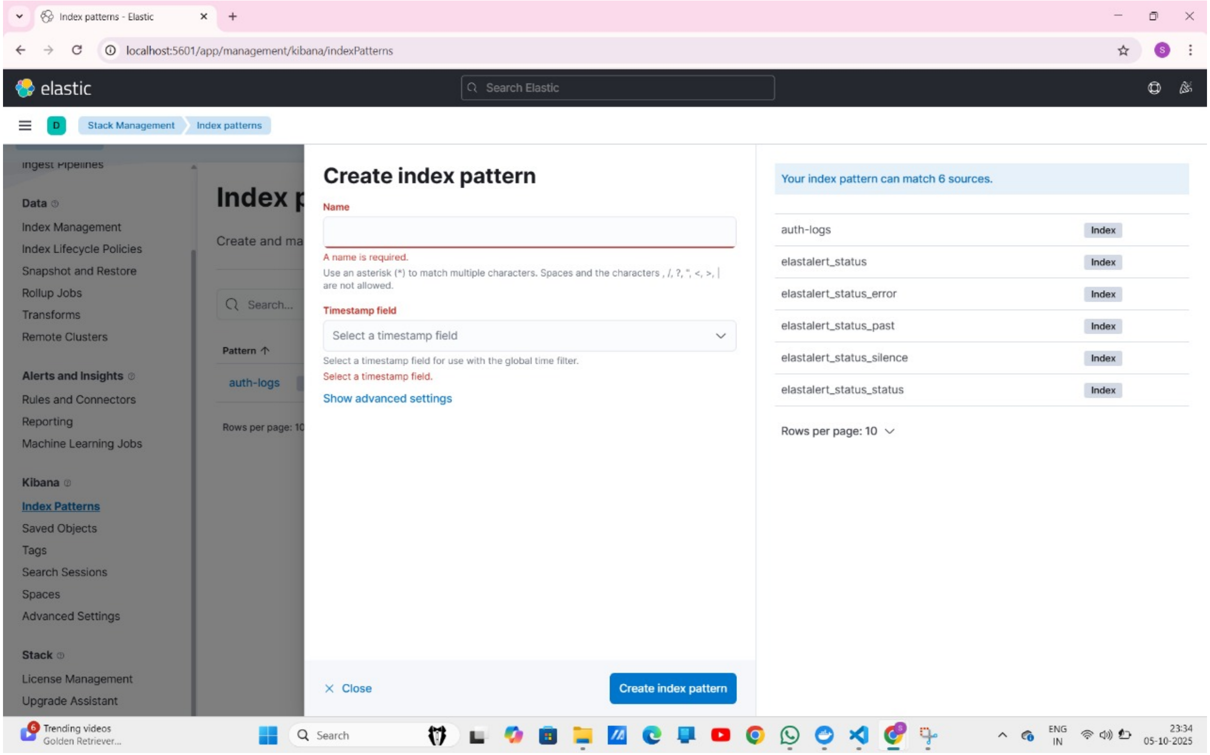
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, add a sample data set.

8. Create index

Discover>>Index management



Create index pattern

Name

A name is required.

Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed.

Timestamp field

Select a timestamp field

Select a timestamp field for use with the global time filter.

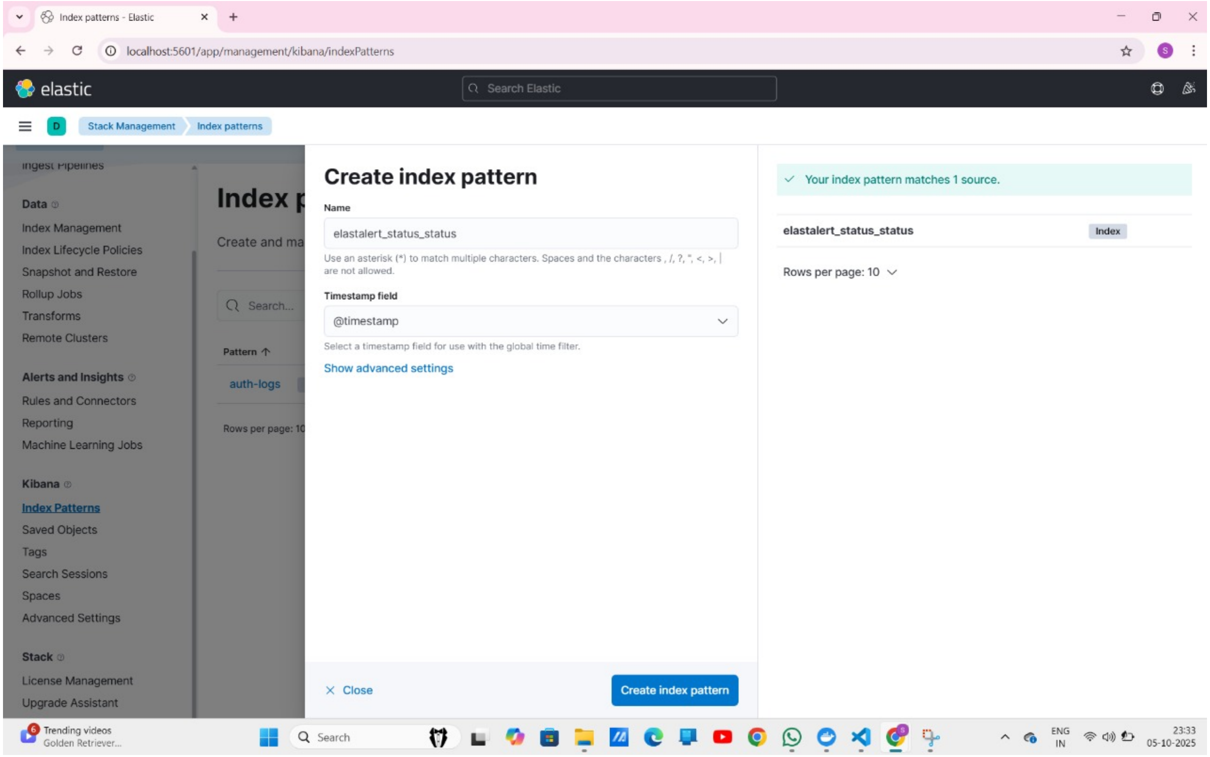
Select a timestamp field.

Show advanced settings

Your index pattern can match 6 sources.

auth-logs	Index
elastalert_status	Index
elastalert_status_error	Index
elastalert_status_past	Index
elastalert_status_silence	Index
elastalert_status_status	Index

Rows per page: 10



Create index pattern

Name

elastalert_status_status

Use an asterisk (*) to match multiple characters. Spaces and the characters , /, ?, ", <, >, | are not allowed.

Timestamp field

@timestamp

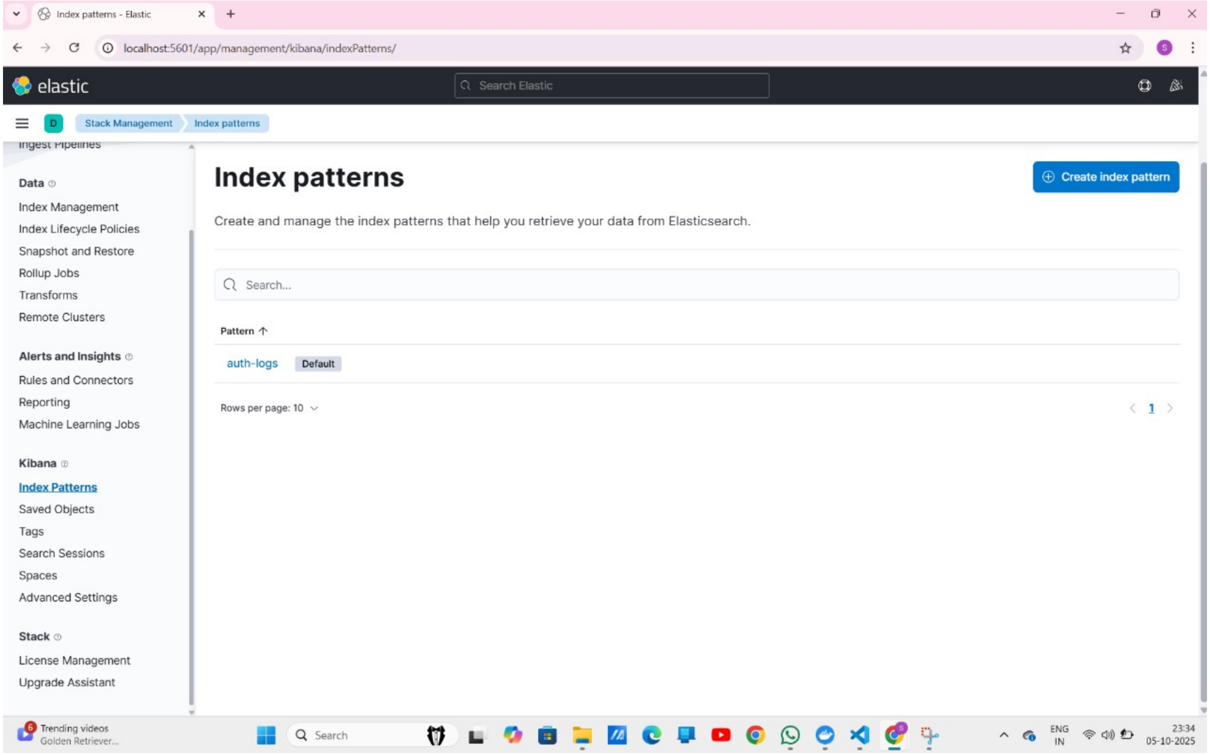
Select a timestamp field for use with the global time filter.

Show advanced settings

✓ Your index pattern matches 1 source.

elastalert_status_status	Index

Rows per page: 10

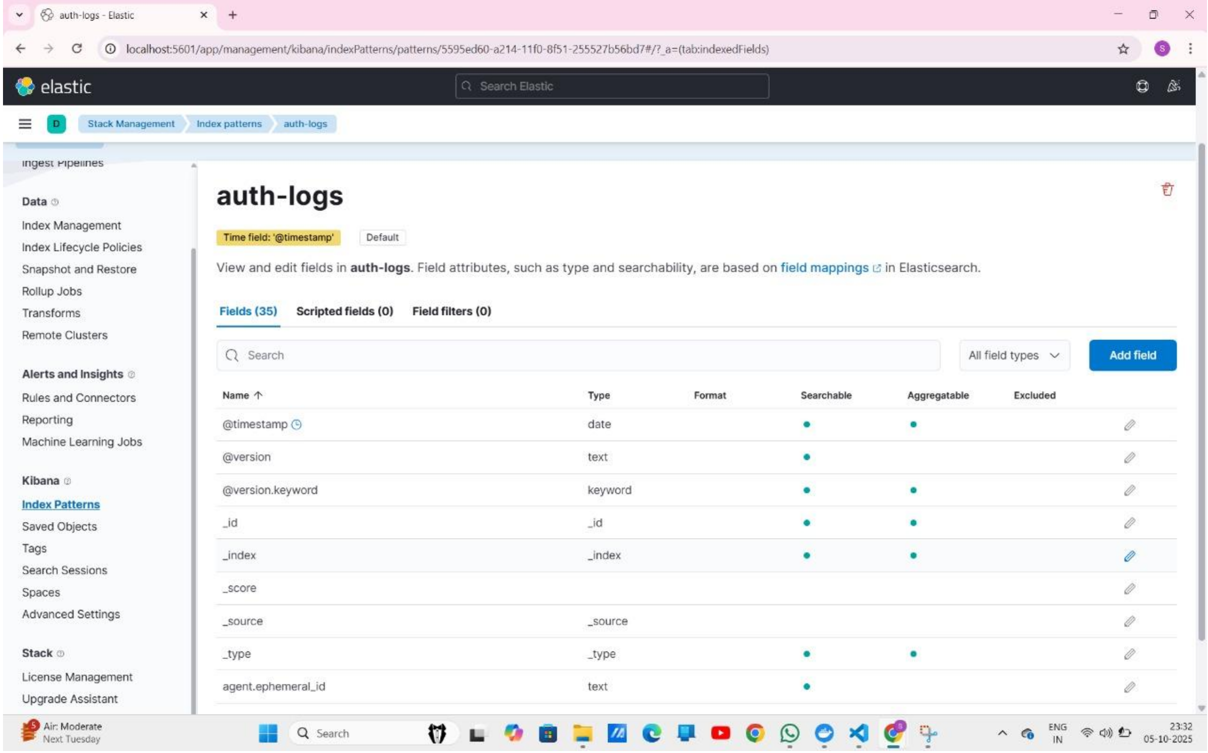


Index patterns

Create and manage the index patterns that help you retrieve your data from Elasticsearch.

Pattern ↑
auth-logs Default

Analyse

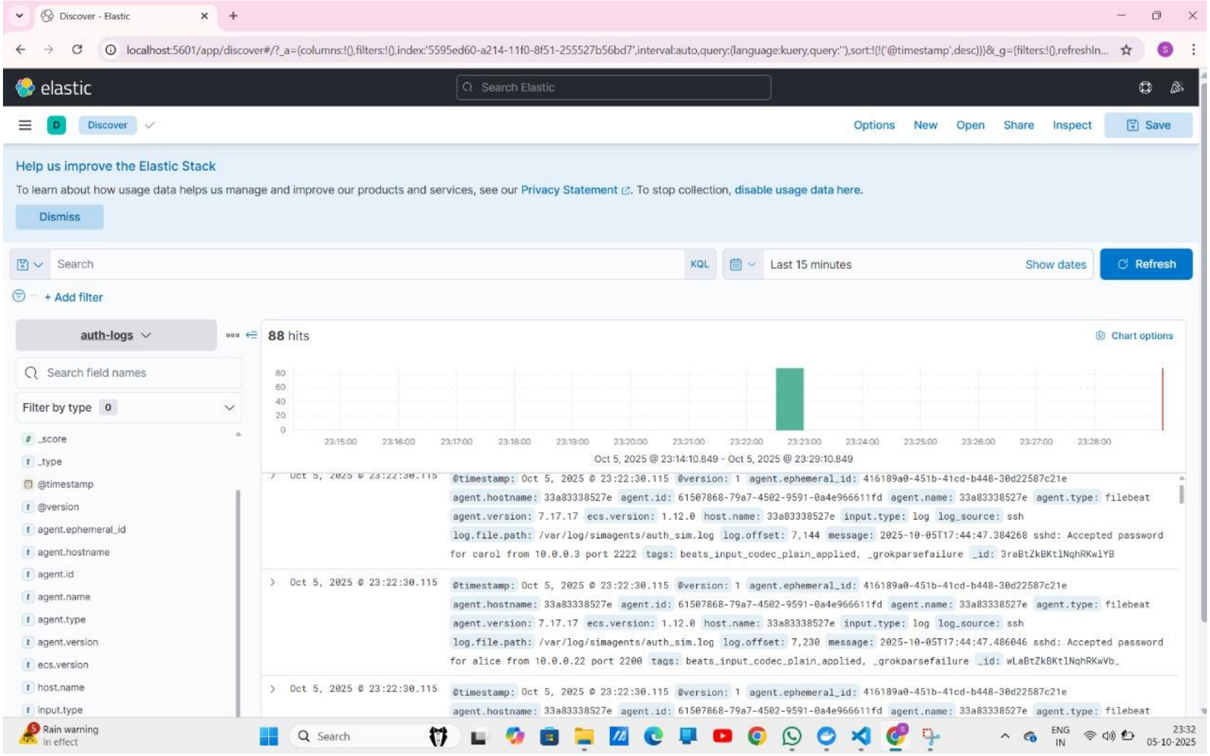


auth-logs

Time field: '@timestamp' Default

View and edit fields in **auth-logs**. Field attributes, such as type and searchability, are based on field mappings in Elasticsearch.

Name ↑	Type	Format	Searchable	Aggregatable	Excluded
@timestamp	date		●	●	
@version	text		●		
@version.keyword	keyword		●	●	
_id	_id		●	●	
_index	_index		●	●	
_score					
_source	_source				
_type	_type		●	●	
agent.ephemeral_id	text		●		


Discover - Elastic
localhost:5601/app/discover#/?_a=(columns:!(),filters:!(),index:'5595ed60-a214-11f0-8f51-255527b56bd7',interval:auto,query:(language:kuery,query:''),sort:!(!('@timestamp',desc)))&_g=(filters:!(),refreshIn...
elastic
Search Elastic
D
Discover
Options
New
Open
Share
Inspect
Save

Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

```
> Oct 5, 2025 @ 23:22:30.115  @timestamp: Oct 5, 2025 @ 23:22:30.115 @version: 1 agent.ephemeral_id: 416189a0-451b-41cd-b448-30d22587c21e
                              agent.hostname: 33a83338527e agent.id: 61507868-79a7-4502-9591-0a4e966611fd agent.name: 33a83338527e agent.type: filebeat
                              agent.version: 7.17.17 ecs.version: 1.12.0 host.name: 33a83338527e input.type: log log_source: ssh
                              log.file.path: /var/log/simagents/auth_sim.log log.offset: 7,144 message: 2025-10-05T17:44:47.384268 sshd: Accepted password
                              for carol from 10.0.0.3 port 2222 tags: beats_input_codec_plain_applied, _grokparsefailure _id: 3raBtZkBKtlNqhRKwlYB

> Oct 5, 2025 @ 23:22:30.115  @timestamp: Oct 5, 2025 @ 23:22:30.115 @version: 1 agent.ephemeral_id: 416189a0-451b-41cd-b448-30d22587c21e
                              agent.hostname: 33a83338527e agent.id: 61507868-79a7-4502-9591-0a4e966611fd agent.name: 33a83338527e agent.type: filebeat
                              agent.version: 7.17.17 ecs.version: 1.12.0 host.name: 33a83338527e input.type: log log_source: ssh
                              log.file.path: /var/log/simagents/auth_sim.log log.offset: 7,230 message: 2025-10-05T17:44:47.486046 sshd: Accepted password
                              for alice from 10.0.0.22 port 2200 tags: beats_input_codec_plain_applied, _grokparsefailure _id: wLaBtZkBKtlNqhRKwVb_

> Oct 5, 2025 @ 23:22:30.115  @timestamp: Oct 5, 2025 @ 23:22:30.115 @version: 1 agent.ephemeral_id: 416189a0-451b-41cd-b448-30d22587c21e
                              agent.hostname: 33a83338527e agent.id: 61507868-79a7-4502-9591-0a4e966611fd agent.name: 33a83338527e agent.type: filebeat
```