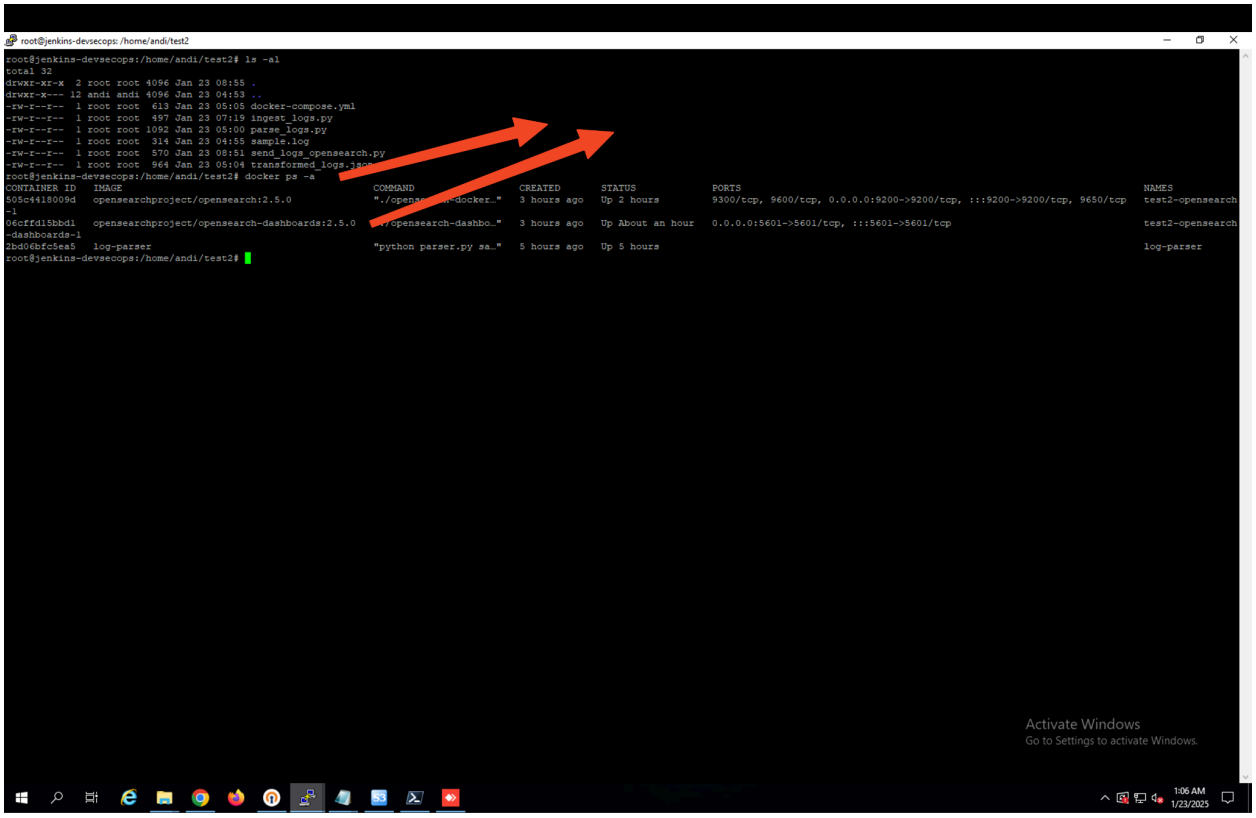
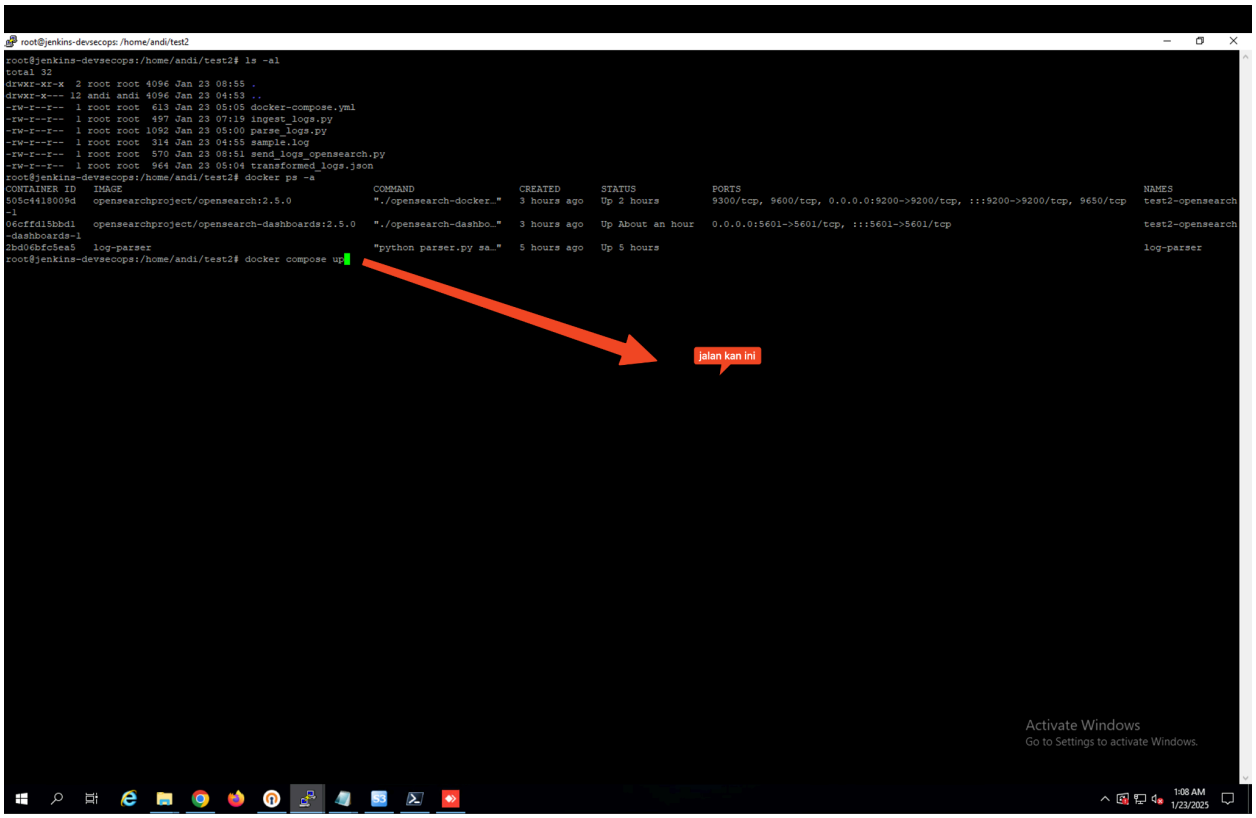
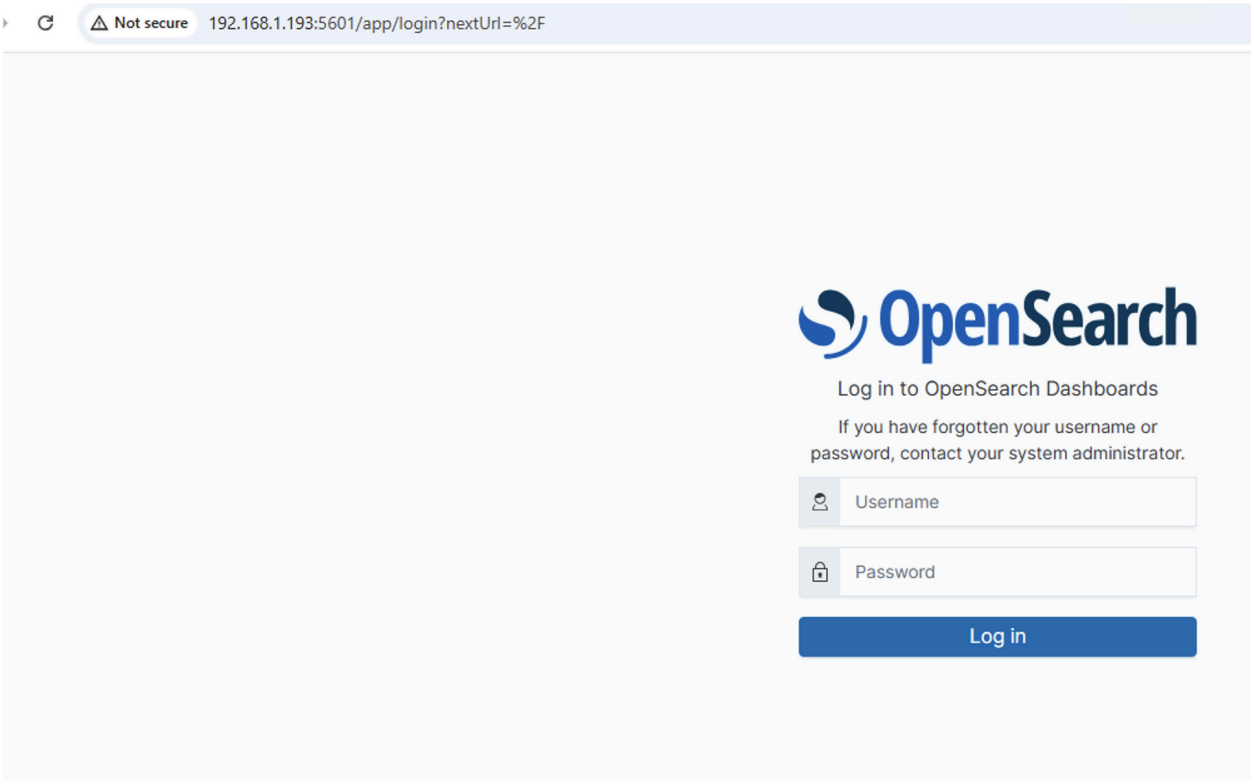
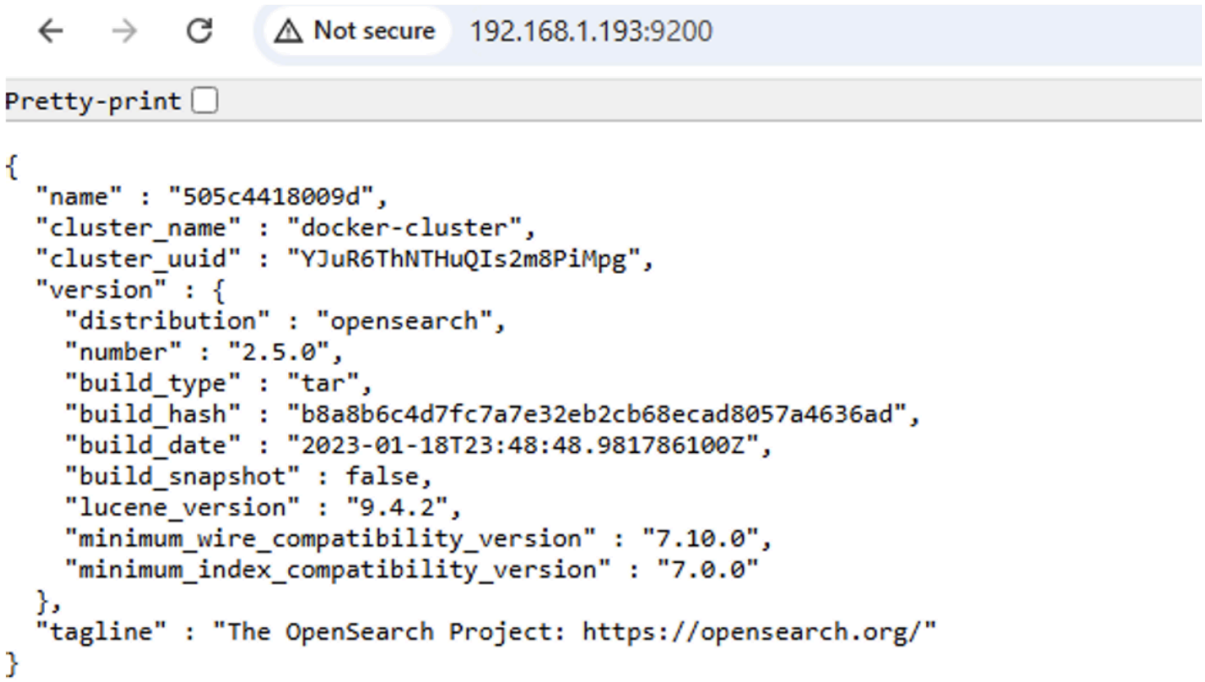
Opensearch menggunakan Docker, seperti contoh dibawah, berjalan



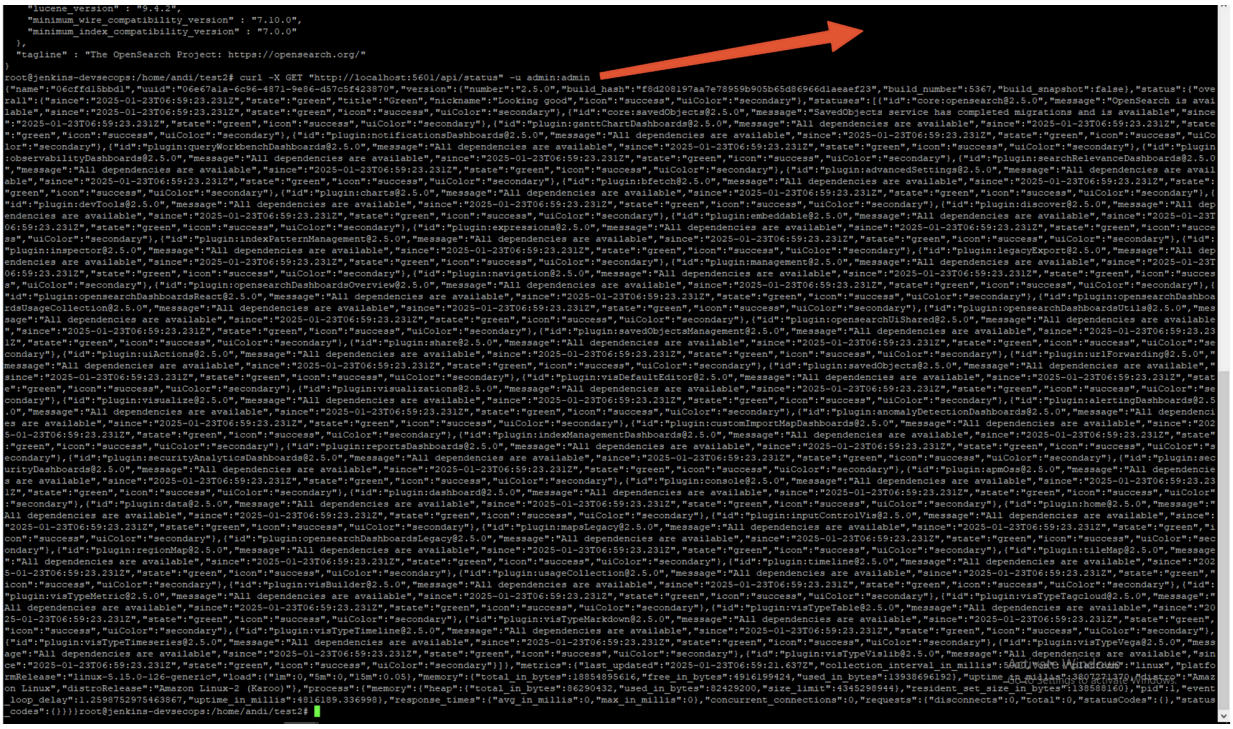


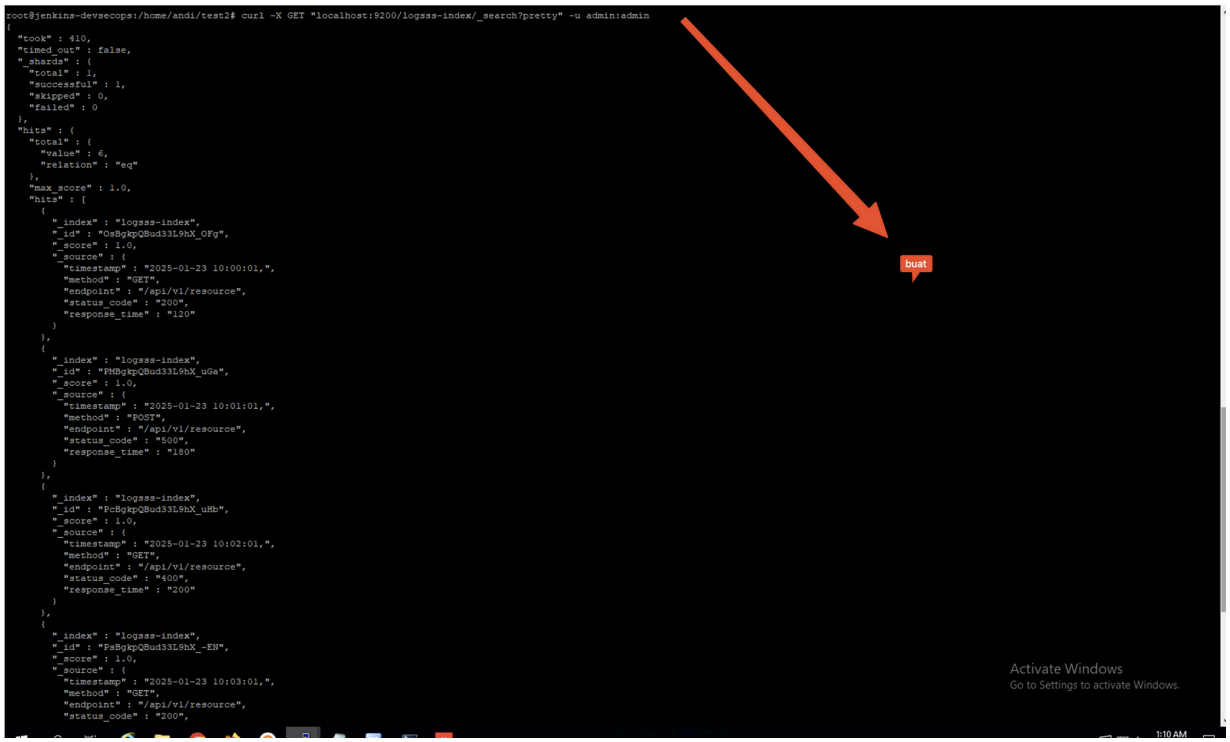
Terliat Dashboard opensearch

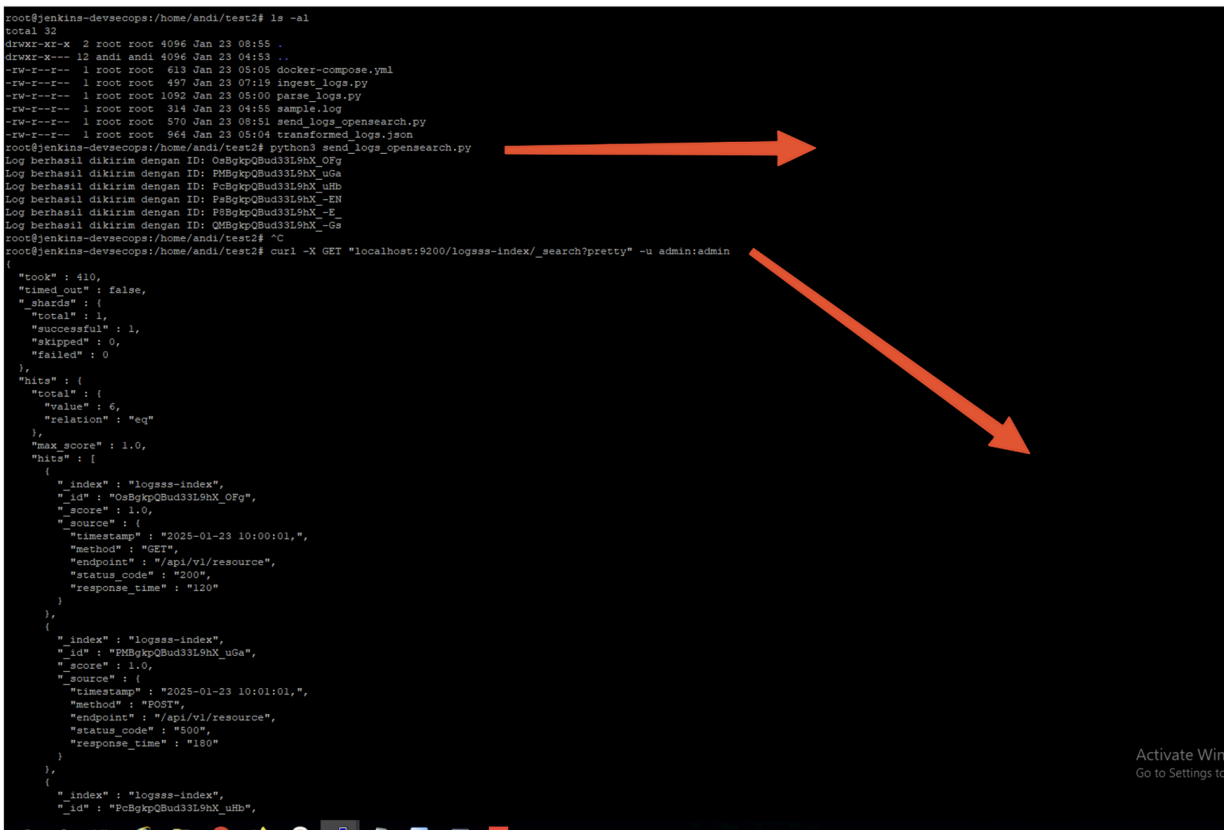


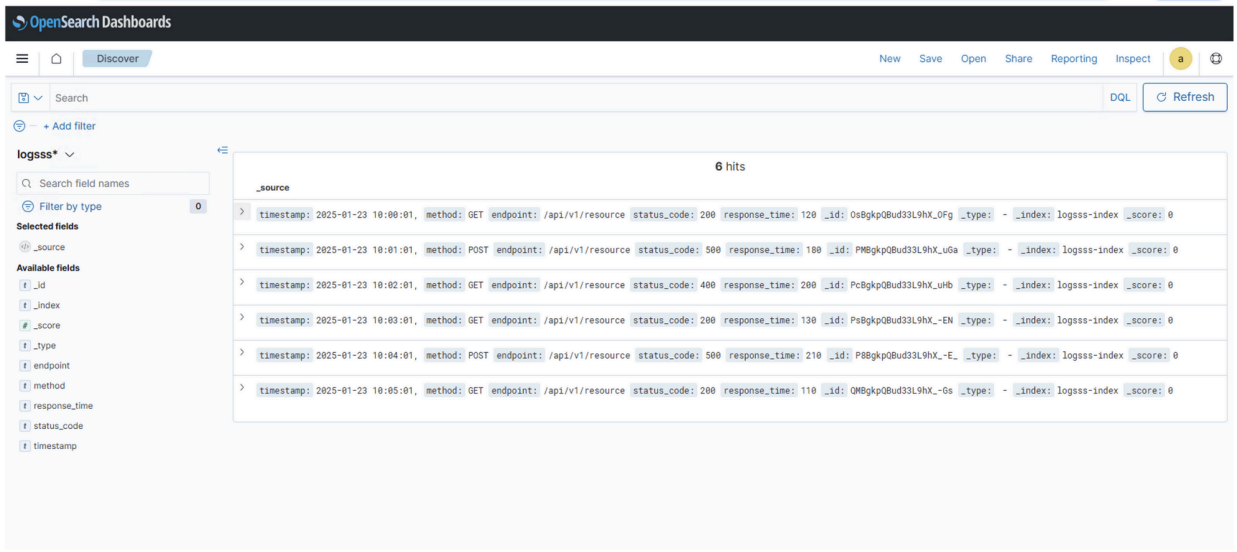


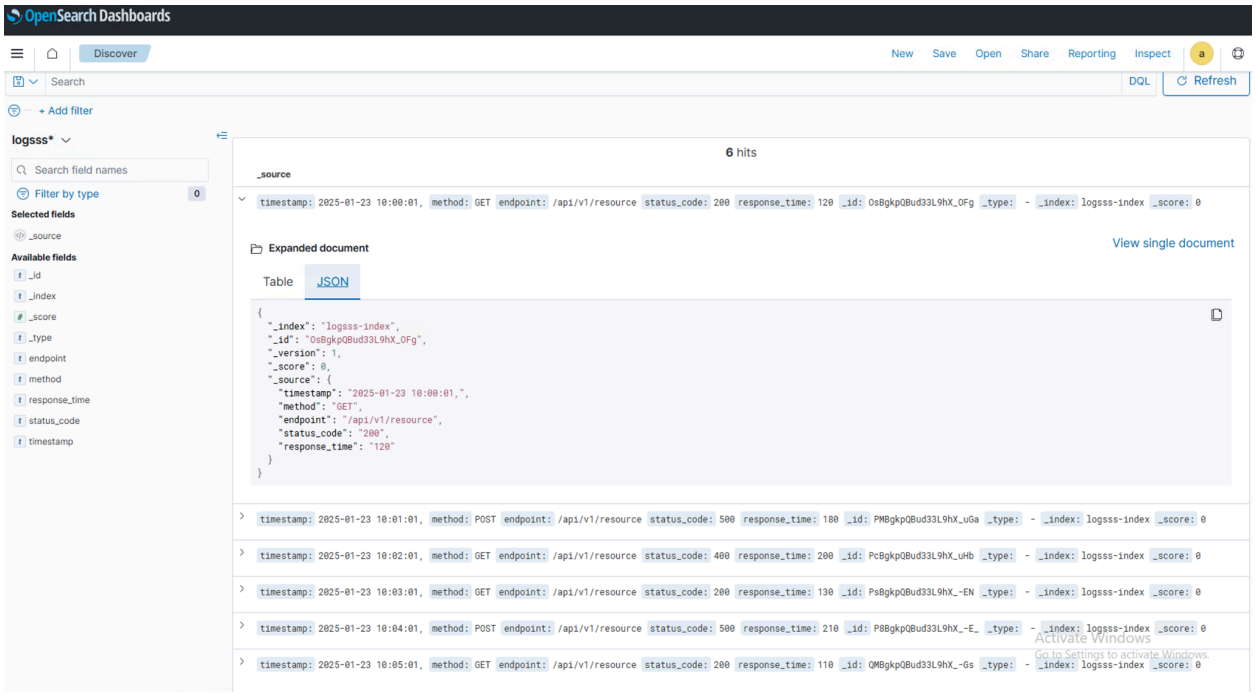

curl: (6) Could not resolve host: elasticsearch
root@jenkins-devsecops:/home/andi/test2# curl -X GET "http://localhost:9200/" -u admin:admin
{
"name" : "505c4418009d",
"cluster_name" : "docker-cluster",
"cluster_uuid" : "YJuR6ThNTHuQIs2m8PiMpg",
"version" : {
"distribution" : "opensearch",
"number" : "2.5.0",
"build_type" : "tar",
"build_hash" : "b8a8b6c4d7fc7a7e32eb2cb68ecad8057a4636ad",
"build_date" : "2023-01-18T23:48:48.981786100Z",
"build_snapshot" : false,
"lucene_version" : "9.4.2",
"minimum_wire_compatibility_version" : "7.10.0",
"minimum_index_compatibility_version" : "7.0.0"
},
"tagline" : "The OpenSearch Project: https://opensearch.org/"
}
root@jenkins-devsecops:/home/andi/test2#


"lucene_version" : "9.4.2",
"minimum_wire_compatibility_version" : "7.10.0",
"minimum_index_compatibility_version" : "7.0.0"
},
"tagline" : "The OpenSearch Project: https://opensearch.org/"
}
root@jenkins-devsecops:/home/andi/test2# curl -X GET "http://localhost:5601/api/status" -u admin:admin

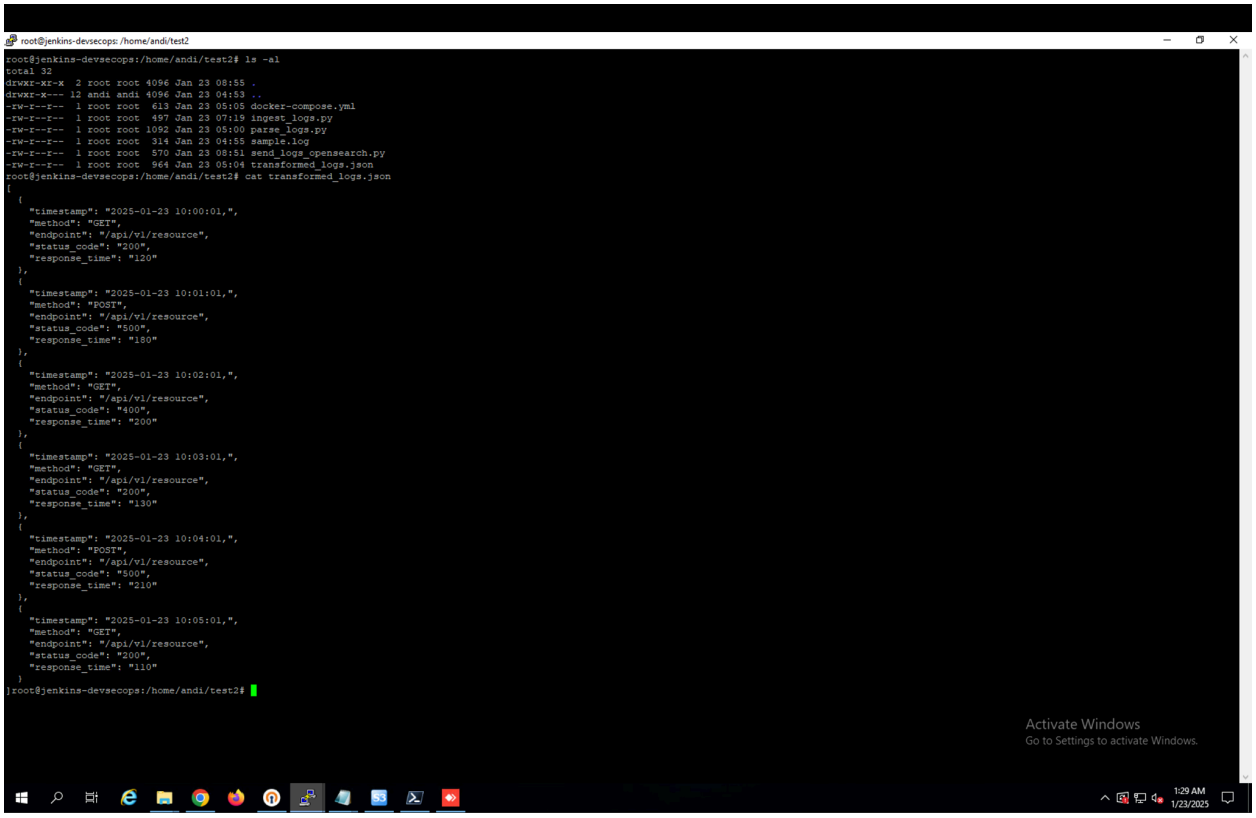

root@jenkins-devsecops:/home/andi/test2# curl -X GET "localhost:9200/logsss-index/_search?pretty" -u admin:admin
{
"took" : 410,
"timed_out" : false,
"_shards" : {
"total" : 1,
"successful" : 1,
"skipped" : 0,
"failed" : 0
},
"hits" : {
"total" : {
"value" : 6,
"relation" : "eq"
},
"max_score" : 1.0,
"hits" : [
{
"_index" : "logsss-index",
"_id" : "OsBgkpQBud33L9hX_OFg",
"_score" : 1.0,
"_source" : {
"timestamp" : "2025-01-23 10:00:01,",
"method" : "GET",
"endpoint" : "/api/v1/resource",
"status_code" : "200",
"response_time" : "120"
}
},
{
"_index" : "logsss-index",
"_id" : "PMBgkpQBud33L9hX_uGa",
"_score" : 1.0,
"_source" : {
"timestamp" : "2025-01-23 10:01:01,",
"method" : "POST",
"endpoint" : "/api/v1/resource",
"status_code" : "500",
"response_time" : "180"
}
},
{
"_index" : "logsss-index",
"_id" : "PcBgkpQBud33L9hX_uHb",
"_score" : 1.0,
"_source" : {
"timestamp" : "2025-01-23 10:02:01,",
"method" : "GET",
"endpoint" : "/api/v1/resource",
"status_code" : "400",
"response_time" : "200"
}
},
{
"_index" : "logsss-index",
"_id" : "PsBgkpQBud33L9hX_-EN",
"_score" : 1.0,
"_source" : {
"timestamp" : "2025-01-23 10:03:01,",
"method" : "GET",
"endpoint" : "/api/v1/resource",
"status_code" : "200",
buat
Activate Windows
Go to Settings to activate Windows.
1:10 AM

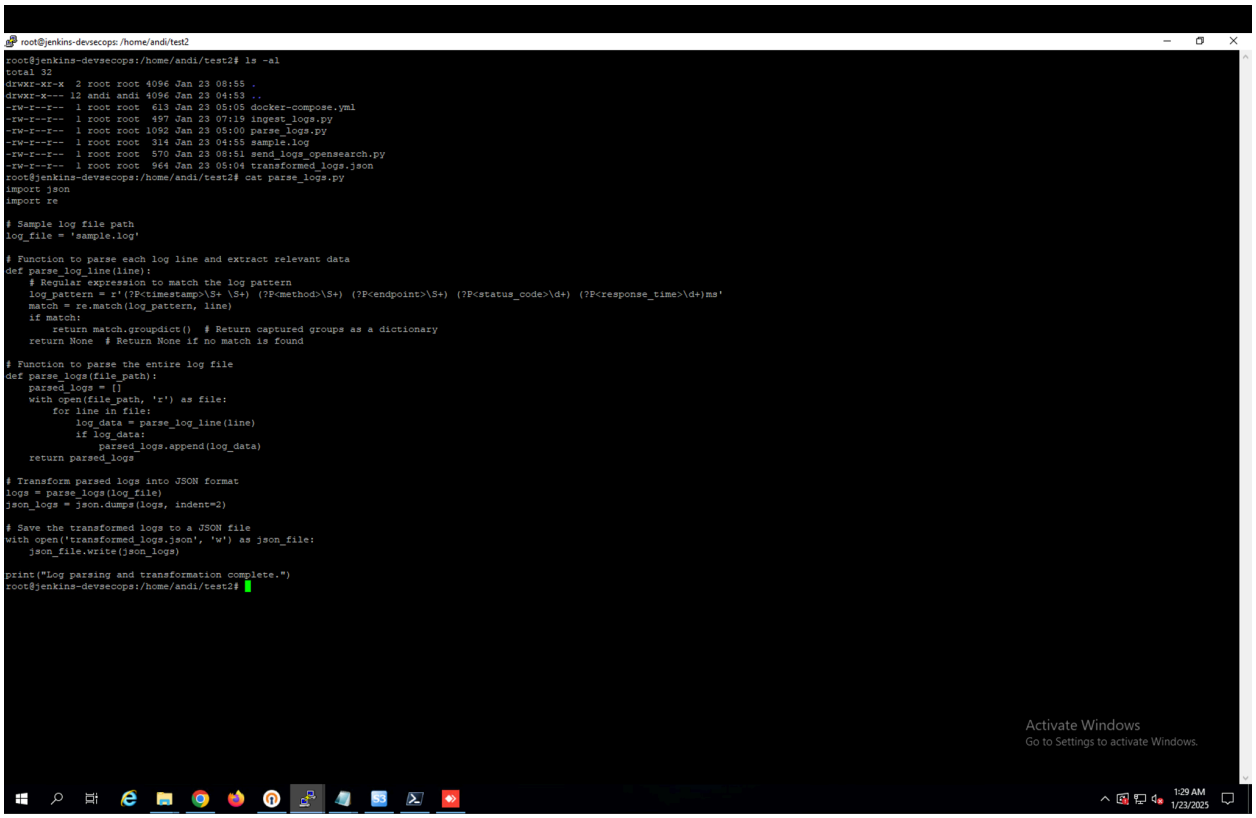

root@jenkins-devsecops:/home/andi/test2# ls -al
total 32
drwxr-xr-x 2 root root 4096 Jan 23 08:55 .
drwxr-x--- 12 andi andi 4096 Jan 23 04:53 ..
-rw-r--r-- 1 root root 613 Jan 23 05:05 docker-compose.yml
-rw-r--r-- 1 root root 497 Jan 23 07:19 ingest_logs.py
-rw-r--r-- 1 root root 1092 Jan 23 05:00 parse_logs.py
-rw-r--r-- 1 root root 314 Jan 23 04:55 sample.log
-rw-r--r-- 1 root root 570 Jan 23 08:51 send_logs_opensearch.py
-rw-r--r-- 1 root root 964 Jan 23 05:04 transformed_logs.json
root@jenkins-devsecops:/home/andi/test2# python3 send_logs_opensearch.py
Log berhasil dikirim dengan ID: OsBgkpQBud33L9hX_OFg
Log berhasil dikirim dengan ID: PMBgkpQBud33L9hX_uGa
Log berhasil dikirim dengan ID: PcBgkpQBud33L9hX_uHb
Log berhasil dikirim dengan ID: PsBgkpQBud33L9hX_-EN
Log berhasil dikirim dengan ID: P8BgkpQBud33L9hX_-E_
Log berhasil dikirim dengan ID: QMBgkpQBud33L9hX_-Gs
root@jenkins-devsecops:/home/andi/test2# ^C
root@jenkins-devsecops:/home/andi/test2# curl -X GET "localhost:9200/logsss-index/_search?pretty" -u admin:admin
{
"took" : 410,
"timed_out" : false,
"_shards" : {
"total" : 1,
"successful" : 1,
"skipped" : 0,
"failed" : 0
},
"hits" : {
"total" : {
"value" : 6,
"relation" : "eq"
},
"max_score" : 1.0,
"hits" : [
{
"_index" : "logsss-index",
"_id" : "OsBgkpQBud33L9hX_OFg",
"_score" : 1.0,
"_source" : {
"timestamp" : "2025-01-23 10:00:01,",
"method" : "GET",
"endpoint" : "/api/v1/resource",
"status_code" : "200",
"response_time" : "120"
}
},
{
"_index" : "logsss-index",
"_id" : "PMBgkpQBud33L9hX_uGa",
"_score" : 1.0,
"_source" : {
"timestamp" : "2025-01-23 10:01:01,",
"method" : "POST",
"endpoint" : "/api/v1/resource",
"status_code" : "500",
"response_time" : "180"
}
},
{
"_index" : "logsss-index",
"_id" : "PcBgkpQBud33L9hX_uHb",
Activate Win
Go to Settings to


OpenSearch Dashboards
Discover
New Save Open Share Reporting Inspect
Search
DQL
Refresh
+ Add filter
logsss*
Search field names
Filter by type 0
Selected fields
_source
Available fields
_id
_index
_score
_type
endpoint
method
response_time
status_code
timestamp
6 hits
_source
timestamp: 2025-01-23 10:00:01, method: GET endpoint: /api/v1/resource status_code: 200 response_time: 120 _id: OsBgkpQBud33L9hX_OFg _type: - _index: logsss-index _score: 0
timestamp: 2025-01-23 10:01:01, method: POST endpoint: /api/v1/resource status_code: 500 response_time: 180 _id: PMBgkpQBud33L9hX_uGa _type: - _index: logsss-index _score: 0
timestamp: 2025-01-23 10:02:01, method: GET endpoint: /api/v1/resource status_code: 400 response_time: 200 _id: PcBgkpQBud33L9hX_uHb _type: - _index: logsss-index _score: 0
timestamp: 2025-01-23 10:03:01, method: GET endpoint: /api/v1/resource status_code: 200 response_time: 130 _id: PsBgkpQBud33L9hX_-EN _type: - _index: logsss-index _score: 0
timestamp: 2025-01-23 10:04:01, method: POST endpoint: /api/v1/resource status_code: 500 response_time: 210 _id: P8BgkpQBud33L9hX_-E_ _type: - _index: logsss-index _score: 0
timestamp: 2025-01-23 10:05:01, method: GET endpoint: /api/v1/resource status_code: 200 response_time: 110 _id: QMBgkpQBud33L9hX_-Gs _type: - _index: logsss-index _score: 0


OpenSearch Dashboards
Discover
New Save Open Share Reporting Inspect
Search
DQL
Refresh
+ Add filter
logsss*
Search field names
Filter by type 0
Selected fields
_source
Available fields
_id
_index
_score
_type
endpoint
method
response_time
status_code
timestamp
6 hits
_source
timestamp: 2025-01-23 10:00:01, method: GET endpoint: /api/v1/resource status_code: 200 response_time: 120 _id: OsBgkpQBud33L9hX_OFg _type: - _index: logsss-index _score: 0
Expanded document
View single document
Table
JSON
{
"_index": "logsss-index",
"_id": "OsBgkpQBud33L9hX_OFg",
"_version": 1,
"_score": 0,
"_source": {
"timestamp": "2025-01-23 10:00:01,",
"method": "GET",
"endpoint": "/api/v1/resource",
"status_code": "200",
"response_time": "120"
}
}
timestamp: 2025-01-23 10:01:01, method: POST endpoint: /api/v1/resource status_code: 500 response_time: 180 _id: PMBgkpQBud33L9hX_uGa _type: - _index: logsss-index _score: 0
timestamp: 2025-01-23 10:02:01, method: GET endpoint: /api/v1/resource status_code: 400 response_time: 200 _id: PcBgkpQBud33L9hX_uHb _type: - _index: logsss-index _score: 0
timestamp: 2025-01-23 10:03:01, method: GET endpoint: /api/v1/resource status_code: 200 response_time: 130 _id: PsBgkpQBud33L9hX_-EN _type: - _index: logsss-index _score: 0
timestamp: 2025-01-23 10:04:01, method: POST endpoint: /api/v1/resource status_code: 500 response_time: 210 _id: P8BgkpQBud33L9hX_-E_ _type: - _index: logsss-index _score: 0
timestamp: 2025-01-23 10:05:01, method: GET endpoint: /api/v1/resource status_code: 200 response_time: 110 _id: QMBgkpQBud33L9hX_-Gs _type: - _index: logsss-index _score: 0
Activate Windows
Go to Settings to activate Windows.

Tambahan


root@jenkins-devsecops: /home/andi/test2
root@jenkins-devsecops:/home/andi/test2# ls -al
total 32
drwxr-xr-x 2 root root 4096 Jan 23 08:55 .
drwxr-x--- 12 andi andi 4096 Jan 23 04:53 ..
-rw-r--r-- 1 root root 613 Jan 23 05:05 docker-compose.yml
-rw-r--r-- 1 root root 497 Jan 23 07:19 ingest_logs.py
-rw-r--r-- 1 root root 1092 Jan 23 05:00 parse_logs.py
-rw-r--r-- 1 root root 314 Jan 23 04:55 sample.log
-rw-r--r-- 1 root root 570 Jan 23 08:51 send_logs_opensearch.py
-rw-r--r-- 1 root root 964 Jan 23 05:04 transformed_logs.json
root@jenkins-devsecops:/home/andi/test2# cat transformed_logs.json
[
  {
    "timestamp": "2025-01-23 10:00:01,",
    "method": "GET",
    "endpoint": "/api/v1/resource",
    "status_code": "200",
    "response_time": "120"
  },
  {
    "timestamp": "2025-01-23 10:01:01,",
    "method": "POST",
    "endpoint": "/api/v1/resource",
    "status_code": "500",
    "response_time": "180"
  },
  {
    "timestamp": "2025-01-23 10:02:01,",
    "method": "GET",
    "endpoint": "/api/v1/resource",
    "status_code": "400",
    "response_time": "200"
  },
  {
    "timestamp": "2025-01-23 10:03:01,",
    "method": "GET",
    "endpoint": "/api/v1/resource",
    "status_code": "200",
    "response_time": "130"
  },
  {
    "timestamp": "2025-01-23 10:04:01,",
    "method": "POST",
    "endpoint": "/api/v1/resource",
    "status_code": "500",
    "response_time": "210"
  },
  {
    "timestamp": "2025-01-23 10:05:01,",
    "method": "GET",
    "endpoint": "/api/v1/resource",
    "status_code": "200",
    "response_time": "110"
  }
]root@jenkins-devsecops:/home/andi/test2#
Activate Windows
Go to Settings to activate Windows.
1:29 AM
1/23/2025


root@jenkins-devsecops: /home/andi/test2
root@jenkins-devsecops:/home/andi/test2# ls -al
total 32
drwxr-xr-x 2 root root 4096 Jan 23 08:55 .
drwxr-x--- 12 andi andi 4096 Jan 23 04:53 ..
-rw-r--r-- 1 root root 613 Jan 23 05:05 docker-compose.yml
-rw-r--r-- 1 root root 497 Jan 23 07:19 ingest_logs.py
-rw-r--r-- 1 root root 1092 Jan 23 05:00 parse_logs.py
-rw-r--r-- 1 root root 314 Jan 23 04:55 sample.log
-rw-r--r-- 1 root root 570 Jan 23 08:51 send_logs_opensearch.py
-rw-r--r-- 1 root root 964 Jan 23 05:04 transformed_logs.json
root@jenkins-devsecops:/home/andi/test2# cat parse_logs.py
import json
import re

# Sample log file path
log_file = 'sample.log'

# Function to parse each log line and extract relevant data
def parse_log_line(line):
    # Regular expression to match the log pattern
    log_pattern = r'(?P<timestamp>\S+ \S+) (?P<method>\S+) (?P<endpoint>\S+) (?P<status_code>\d+) (?P<response_time>\d+)ms'
    match = re.match(log_pattern, line)
    if match:
        return match.groupdict() # Return captured groups as a dictionary
    return None # Return None if no match is found

# Function to parse the entire log file
def parse_logs(file_path):
    parsed_logs = []
    with open(file_path, 'r') as file:
        for line in file:
            log_data = parse_log_line(line)
            if log_data:
                parsed_logs.append(log_data)
    return parsed_logs

# Transform parsed logs into JSON format
logs = parse_logs(log_file)
json_logs = json.dumps(logs, indent=2)

Save the transformed logs to a JSON file
with open('transformed_logs.json', 'w') as json_file:
    json_file.write(json_logs)

print("Log parsing and transformation complete.")
root@jenkins-devsecops:/home/andi/test2#
Activate Windows
Go to Settings to activate Windows.
1:29 AM
1/23/2025