NFSU

विद्या अमृतं अश्नुते

National Forensic Sciences University

Knowledge | Wisdom | Fulfilment

An Institution of National Importance
(Ministry of Home Affairs, Government of India)

BTECH MTECH COMPUTER SCIENCE AND ENGINEERING

(CYBERSECURITY)

INCIDENT RESPONSE MANAGEMENT

PRACTICAL FILE

SUBMITTED BY:

VISHNULAL N

102CTBMCS2122025

SEMESTER -8

SUBMITTED TO:

Dr.Indrajeet Singh

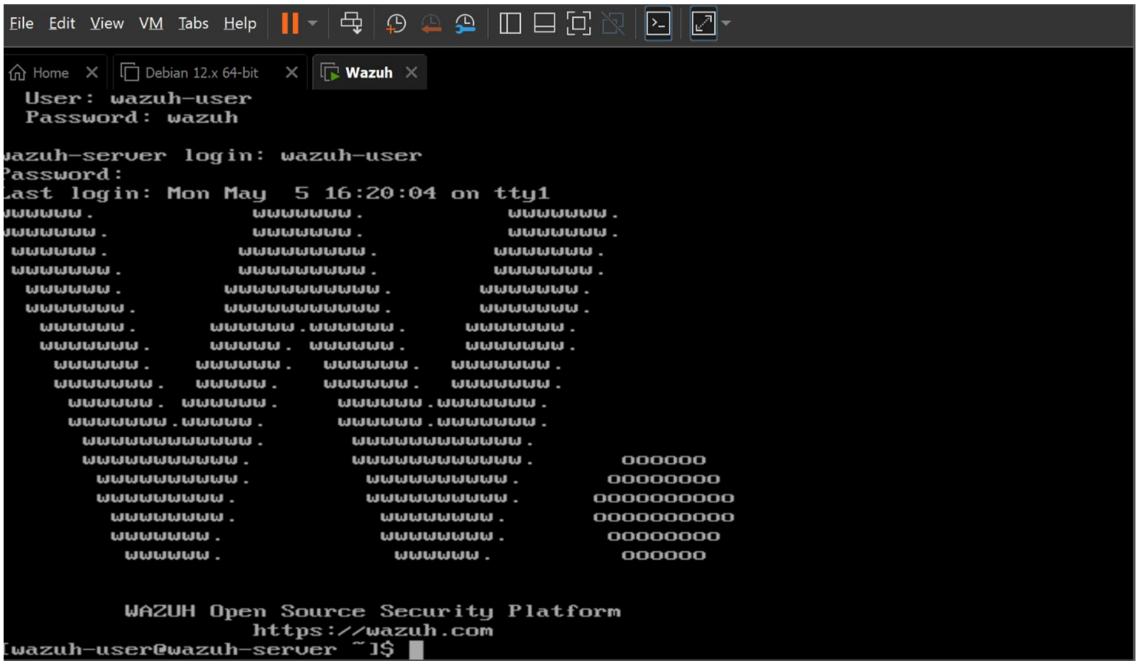
Practical 1: Wazuh

Objective:

To deploy, configure, and verify the working of a Wazuh agent on a Windows endpoint and connect it to the Wazuh server for centralized monitoring and threat detection.

Steps:

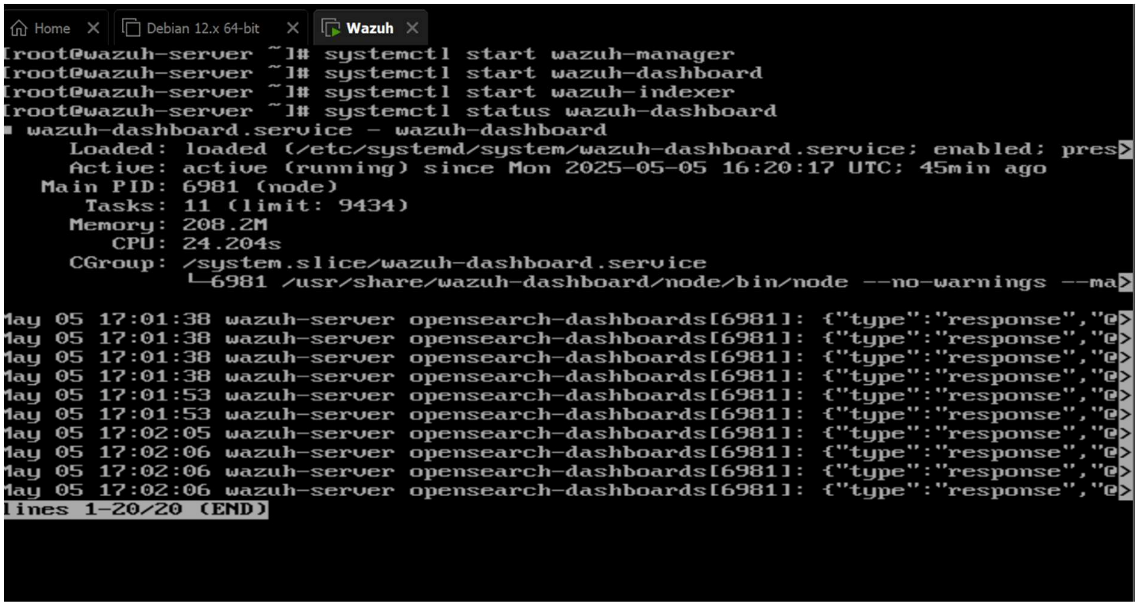
1. Launching Wazuh Server



```
  User: wazuh-user
  Password: wazuh

azuh-server login: wazuh-user
assword:
ast login: Mon May  5 16:20:04 on tty1
wwwww.            wwwwwww.            wwwwwww.
wwwwww.           wwwwwww.            wwwwwww.
 wwwwww.         wwwwwwwww.          wwwwwww.
 wwwwwww.        wwwwwwwww.          wwwwwww.
  wwwwww.       wwwwwwwwwww.        wwwwwww.
  wwwwwww.      wwwwwwwwwww.        wwwwwww.
   wwwwww.     wwwwww.wwwwww.      wwwwwww.
   wwwwwww.    wwwww. wwwwww.      wwwwwww.
    wwwwww.   wwwwww.  wwwwww.   wwwwwww.
    wwwwwww.  wwwww.   wwwwww.   wwwwwww.
     wwwwww. wwwwww.    wwwwww.wwwwwww.
     wwwwwww.wwwww.     wwwwww.wwwwwww.
      wwwwwwwwwwww.      wwwwwwwwwwwww.
      wwwwwwwwwww.       wwwwwwwwwwwww.      oooooo
       wwwwwwwwww.        wwwwwwwwwww.      oooooooo
       wwwwwwwww.         wwwwwwwwwww.     oooooooooo
        wwwwwwww.          wwwwwwwww.      oooooooooo
        wwwwwww.           wwwwwwwww.       oooooooo
         wwwwww.            wwwwwww.         oooooo


         WAZUH Open Source Security Platform
                  https://wazuh.com
[wazuh-user@wazuh-server ~]$
```

2. Starting Wazuh Services:

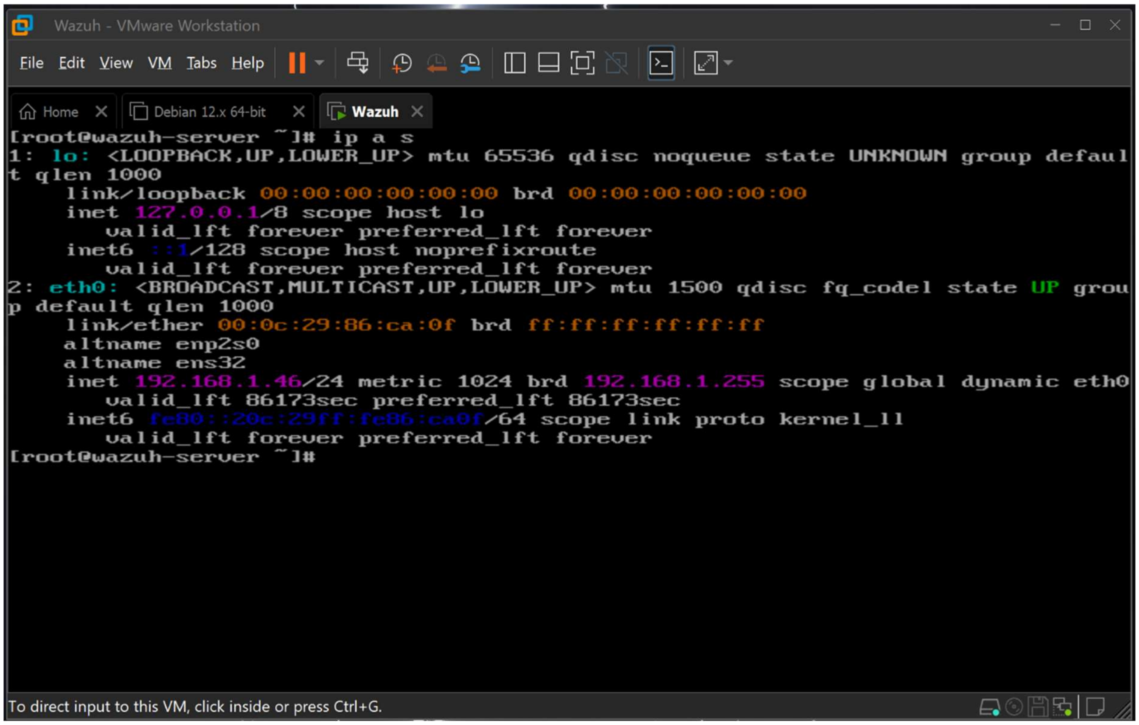
- The following services were started using systemctl:
    - wazuh-manager
    - wazuh-dashboard
    - wazuh-indexer
- All services were confirmed to be running actively.



```
[root@wazuh-server ~]# systemctl start wazuh-manager
[root@wazuh-server ~]# systemctl start wazuh-dashboard
[root@wazuh-server ~]# systemctl start wazuh-indexer
[root@wazuh-server ~]# systemctl status wazuh-dashboard
■ wazuh-dashboard.service - wazuh-dashboard
     Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; pres>
     Active: active (running) since Mon 2025-05-05 16:20:17 UTC; 45min ago
   Main PID: 6981 (node)
      Tasks: 11 (limit: 9434)
     Memory: 208.2M
        CPU: 24.204s
     CGroup: /system.slice/wazuh-dashboard.service
             └─6981 /usr/share/wazuh-dashboard/node/bin/node --no-warnings --ma>

May 05 17:01:38 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
May 05 17:01:38 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
May 05 17:01:38 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
May 05 17:01:38 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
May 05 17:01:53 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
May 05 17:01:53 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
May 05 17:02:05 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
May 05 17:02:06 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
May 05 17:02:06 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
May 05 17:02:06 wazuh-server opensearch-dashboards[6981]: {"type":"response","@>
lines 1-20/20 (END)
```

3.Find IP address

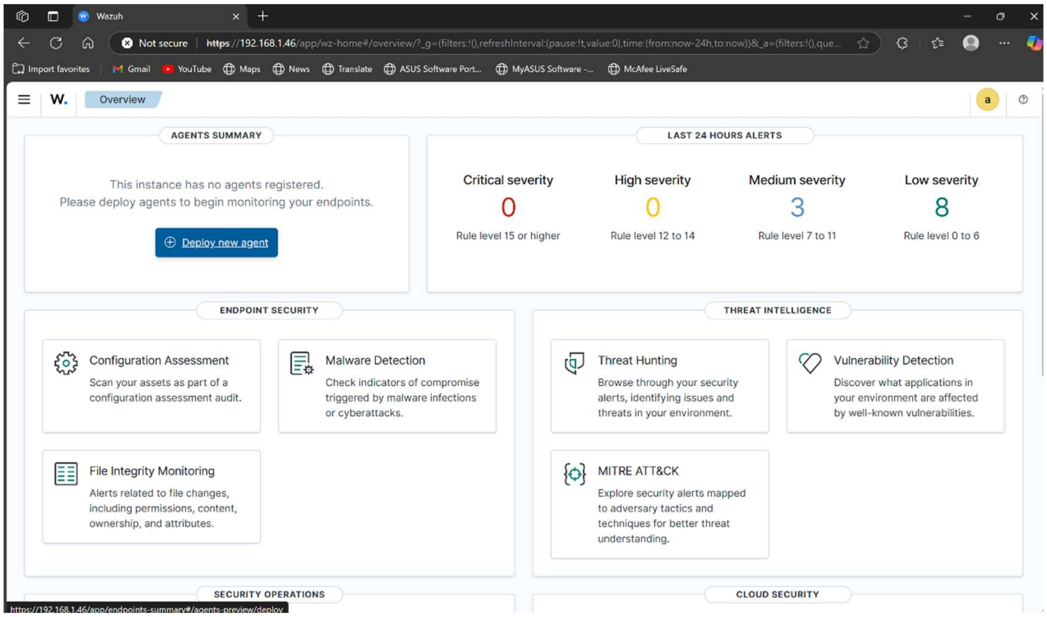
On checking the IP configuration using ip a, the server IP was found to be 192.168.1.46.


Wazuh - VMware Workstation
File
Edit
View
VM
Tabs
Help
Home
Debian 12.x 64-bit
Wazuh
To direct input to this VM, click inside or press Ctrl+G.

```
[root@wazuh-server ~]# ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 00:0c:29:86:ca:0f brd ff:ff:ff:ff:ff:ff
    altname enp2s0
    altname ens32
    inet 192.168.1.46/24 metric 1024 brd 192.168.1.255 scope global dynamic eth0
       valid_lft 86173sec preferred_lft 86173sec
    inet6 fe80::20c:29ff:fe86:ca0f/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@wazuh-server ~]#
```

4. Accessing Wazuh Dashboard:

- The Wazuh dashboard was accessed via browser using the server IP: https://192.168.1.46.
- The overview section initially showed **no registered agents**.



Wazuh
Not secure
https://192.168.1.46/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(filters:!(),que...
Import favorites
Gmail
YouTube
Maps
News
Translate
ASUS Software Port...
MyASUS Software -...
McAfee LiveSafe
W.
Overview
a

AGENTS SUMMARY

This instance has no agents registered.
Please deploy agents to begin monitoring your endpoints.

Deploy new agent

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	3	8
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring
Alerts related to file changes, including permissions, content, ownership, and attributes.

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

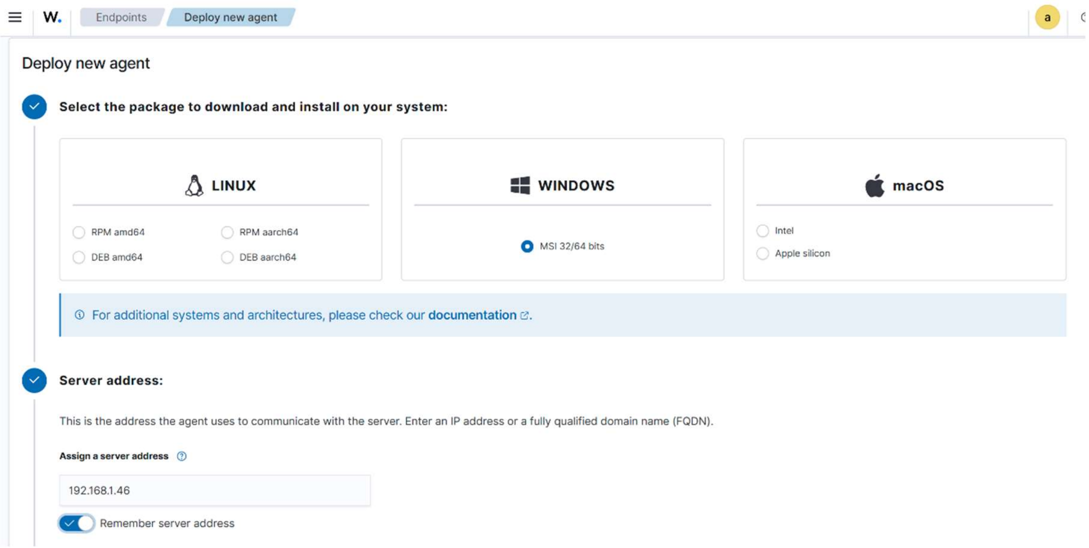
Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK
Explore security alerts mapped to adversary tactics and techniques for better threat understanding.

SECURITY OPERATIONS
CLOUD SECURITY
https://192.168.1.46/app/endpoints-summary#/agents-preview/deploy

5. Deploying the Agent:

- From the dashboard, under “Deploy new agent”, **Windows (MSI 32/64 bits)** was selected as the target platform.
- The server address 192.168.1.46 was specified to ensure agent-server communication.



Deploy new agent

Select the package to download and install on your system:

LINUX
○ RPM amd64 ○ RPM aarch64
○ DEB amd64 ○ DEB aarch64

WINDOWS
● MSI 32/64 bits

macOS
○ Intel
○ Apple silicon

For additional systems and architectures, please check our documentation.

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

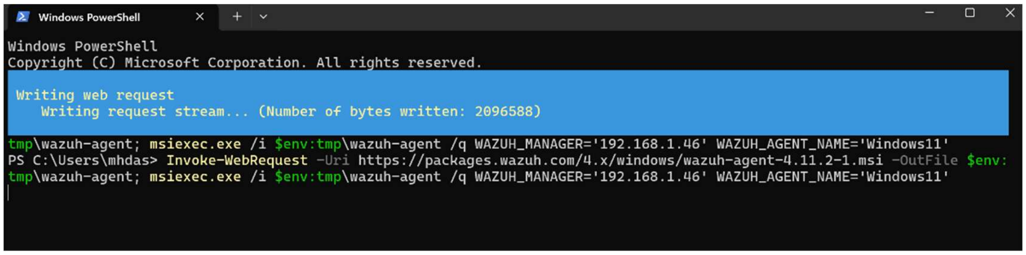
Assign a server address

192.168.1.46

Remember server address

6. Installing Agent on Windows Machine:

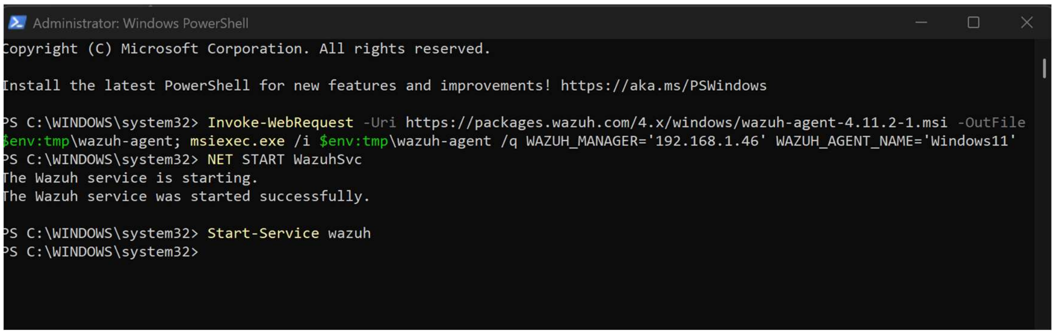
A PowerShell command was used to download and install the Wazuh agent:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

 Writing web request
    Writing request stream... (Number of bytes written: 2096588)

tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.1.46' WAZUH_AGENT_NAME='Windows11'
PS C:\Users\mhdas> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.2-1.msi -OutFile $env:
tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.1.46' WAZUH_AGENT_NAME='Windows11'
```

7. Starting the Agent Service:

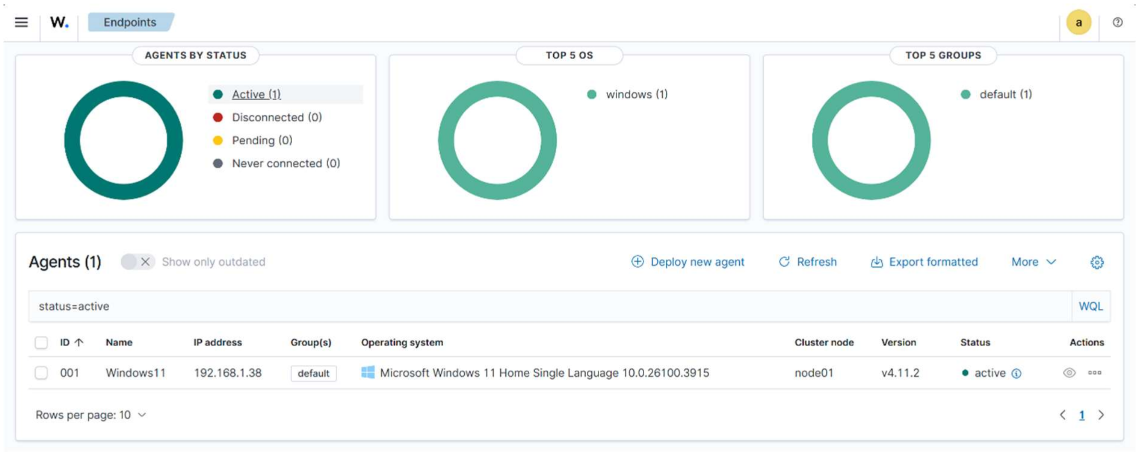
The Wazuh agent service was started using the commands:



```
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.2-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.1.46' WAZUH_AGENT_NAME='Windows11'
PS C:\WINDOWS\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\WINDOWS\system32> Start-Service wazuh
PS C:\WINDOWS\system32>
```

8. Verifying Agent Registration:

- After successful installation and service startup, the agent appeared in the Wazuh dashboard.
- Details like agent ID, name (Windows11), IP address (192.168.1.38), OS, status (active), and version were visible.



status=active

ID ↑	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	Windows11	192.168.1.38	default	Microsoft Windows 11 Home Single Language 10.0.26100.3915	node01	v4.11.2	● active	

Practical 2: ELK (Elasticsearch, Logstash, Kibana)

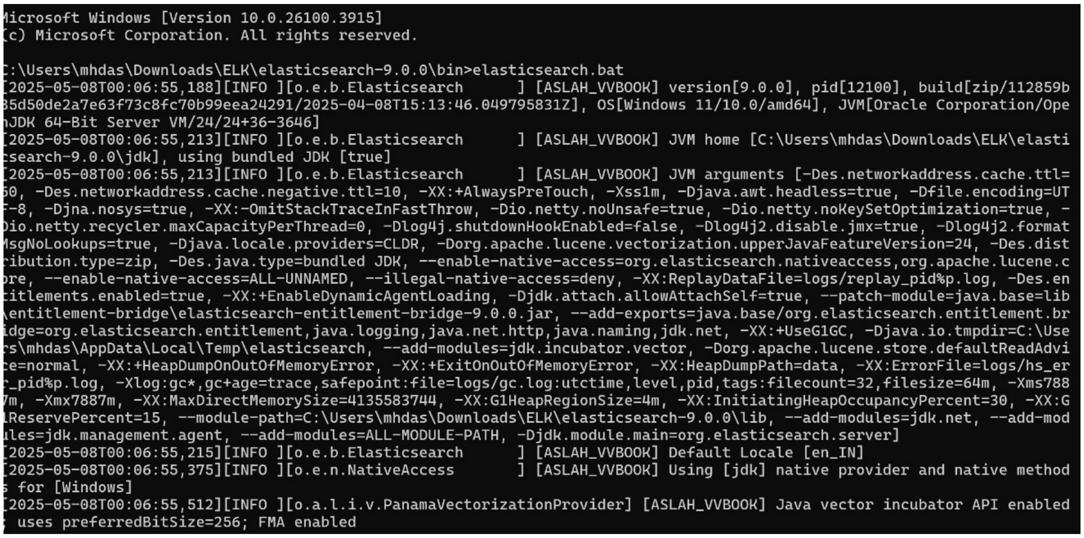
Objective:

To install and configure the ELK stack components — **Elasticsearch** and **Kibana** — on a local machine, and verify that the services are running and connected properly for data visualization and search.

Steps:

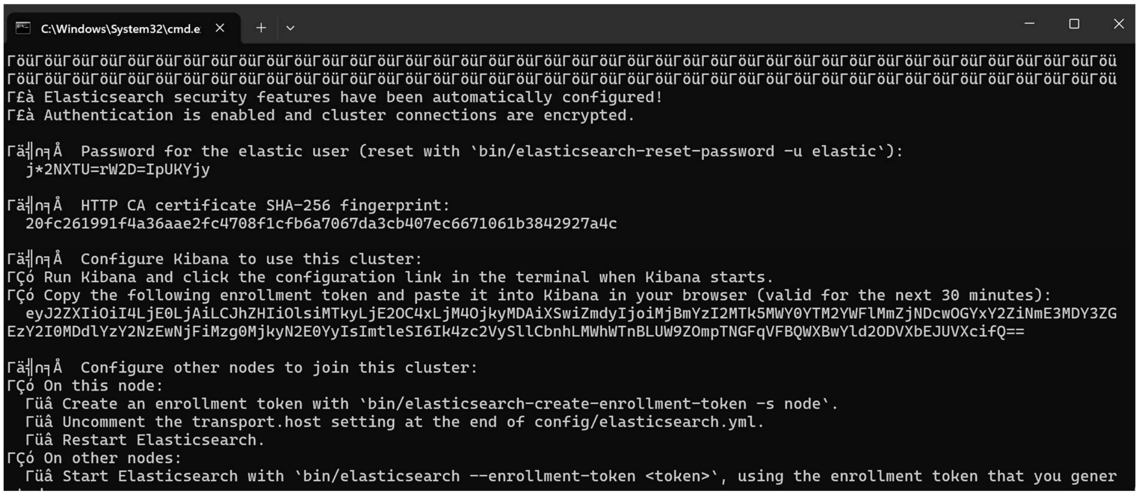
1. Started Elasticsearch using the elasticsearch.bat file from the command line.

Waited for Elasticsearch to finish its startup. The terminal displayed logs confirming successful initialization and cluster details.



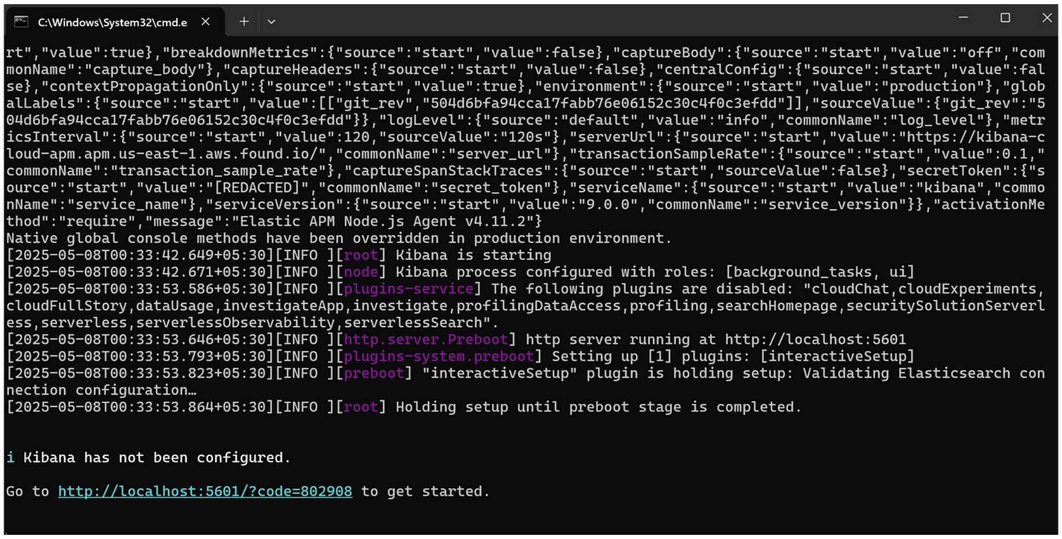
```
licrosoft Windows [Version 10.0.26100.3915]
(c) Microsoft Corporation. All rights reserved.

:\Users\mhdas\Downloads\ELK\elasticsearch-9.0.0\bin>elasticsearch.bat
[2025-05-08T00:06:55,188][INFO ][o.e.b.Elasticsearch      ] [ASLAH_VVBOOK] version[9.0.0], pid[12100], build[zip/112859b
35d50de2a7e63f73c8fc70b99eea24291/2025-04-08T15:13:46.049795831Z], OS[Windows 11/10.0/amd64], JVM[Oracle Corporation/Ope
nJDK 64-Bit Server VM/24/24+36-3646]
[2025-05-08T00:06:55,213][INFO ][o.e.b.Elasticsearch      ] [ASLAH_VVBOOK] JVM home [C:\Users\mhdas\Downloads\ELK\elasti
csearch-9.0.0\jdk], using bundled JDK [true]
[2025-05-08T00:06:55,213][INFO ][o.e.b.Elasticsearch      ] [ASLAH_VVBOOK] JVM arguments [-Des.networkaddress.cache.ttl=
60, -Des.networkaddress.cache.negative.ttl=10, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UT
F-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -
Dio.netty.recycler.maxCapacityPerThread=0, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Dlog4j2.format
MsgNoLookups=true, -Djava.locale.providers=CLDR, -Dorg.apache.lucene.vectorization.upperJavaFeatureVersion=24, -Des.dist
ribution.type=zip, -Des.java.type=bundled JDK, --enable-native-access=org.elasticsearch.nativeaccess,org.apache.lucene.c
ore, --enable-native-access=ALL-UNNAMED, --illegal-native-access=deny, -XX:ReplayDataFile=logs/replay_pid%p.log, -Des.en
titlements.enabled=true, -XX:+EnableDynamicAgentLoading, -Djdk.attach.allowAttachSelf=true, --patch-module=java.base=lib
\entitlement-bridge\elasticsearch-entitlement-bridge-9.0.0.jar, --add-exports=java.base/org.elasticsearch.entitlement.br
idge=org.elasticsearch.entitlement,java.logging,java.net.http,java.naming,jdk.net, -XX:+UseG1GC, -Djava.io.tmpdir=C:\Use
rs\mhdas\AppData\Local\Temp\elasticsearch, --add-modules=jdk.incubator.vector, -Dorg.apache.lucene.store.defaultReadAdvi
ce=normal, -XX:+HeapDumpOnOutOfMemoryError, -XX:+ExitOnOutOfMemoryError, -XX:HeapDumpPath=data, -XX:ErrorFile=logs/hs_er
r_pid%p.log, -Xlog:gc*,gc+age=trace,safepoint:file=logs/gc.log:utctime,level,pid,tags:filecount=32,filesize=64m, -Xms788
7m, -Xmx7887m, -XX:MaxDirectMemorySize=4135583744, -XX:G1HeapRegionSize=4m, -XX:InitiatingHeapOccupancyPercent=30, -XX:G
1ReservePercent=15, --module-path=C:\Users\mhdas\Downloads\ELK\elasticsearch-9.0.0\lib, --add-modules=jdk.net, --add-mod
ules=jdk.management.agent, --add-modules=ALL-MODULE-PATH, -Djdk.module.main=org.elasticsearch.server]
[2025-05-08T00:06:55,215][INFO ][o.e.b.Elasticsearch      ] [ASLAH_VVBOOK] Default Locale [en_IN]
[2025-05-08T00:06:55,375][INFO ][o.e.n.NativeAccess       ] [ASLAH_VVBOOK] Using [jdk] native provider and native method
s for [Windows]
[2025-05-08T00:06:55,512][INFO ][o.a.l.i.v.PanamaVectorizationProvider] [ASLAH_VVBOOK] Java vector incubator API enabled
; uses preferredBitSize=256; FMA enabled
```

2. Noted the auto-generated enrollment token and password for the elastic user from the console logs.



```
ΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöü
ΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöüΓöü
Γ£à Elasticsearch security features have been automatically configured!
Γ£à Authentication is enabled and cluster connections are encrypted.

Γä╣n┬Å  Password for the elastic user (reset with `bin/elasticsearch-reset-password -u elastic`):
  j*2NXTU=rW2D=IpUKYjy

Γä╣n┬Å  HTTP CA certificate SHA-256 fingerprint:
  20fc261991f4a36aae2fc4708f1cfb6a7067da3cb407ec6671061b3842927a4c

Γä╣n┬Å  Configure Kibana to use this cluster:
ΓÇó Run Kibana and click the configuration link in the terminal when Kibana starts.
ΓÇó Copy the following enrollment token and paste it into Kibana in your browser (valid for the next 30 minutes):
  eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMTkyLjE2OC4xLjM4OjkyMDAiXSwiZmdyIjoiMjBmYzI2MTk5MWY0YTM2YWFlMmZjNDcwOGYxY2ZiNmE3MDY3ZG
EzY2I0MDdlYzY2NzEwNjFiMzg0MjkyN2E0YyIsImtleSI6Ik4zc2VySllCbnhLMWhWTnBLUW9ZOmpTNGFqVFBQWXBwYld2ODVXbEJUVXcifQ==

Γä╣n┬Å  Configure other nodes to join this cluster:
ΓÇó On this node:
  Γüâ Create an enrollment token with `bin/elasticsearch-create-enrollment-token -s node`.
  Γüâ Uncomment the transport.host setting at the end of config/elasticsearch.yml.
  Γüâ Restart Elasticsearch.
ΓÇó On other nodes:
  Γüâ Start Elasticsearch with `bin/elasticsearch --enrollment-token <token>`, using the enrollment token that you gener
```

3. Started Kibana by executing kibana.bat from the Kibana directory.

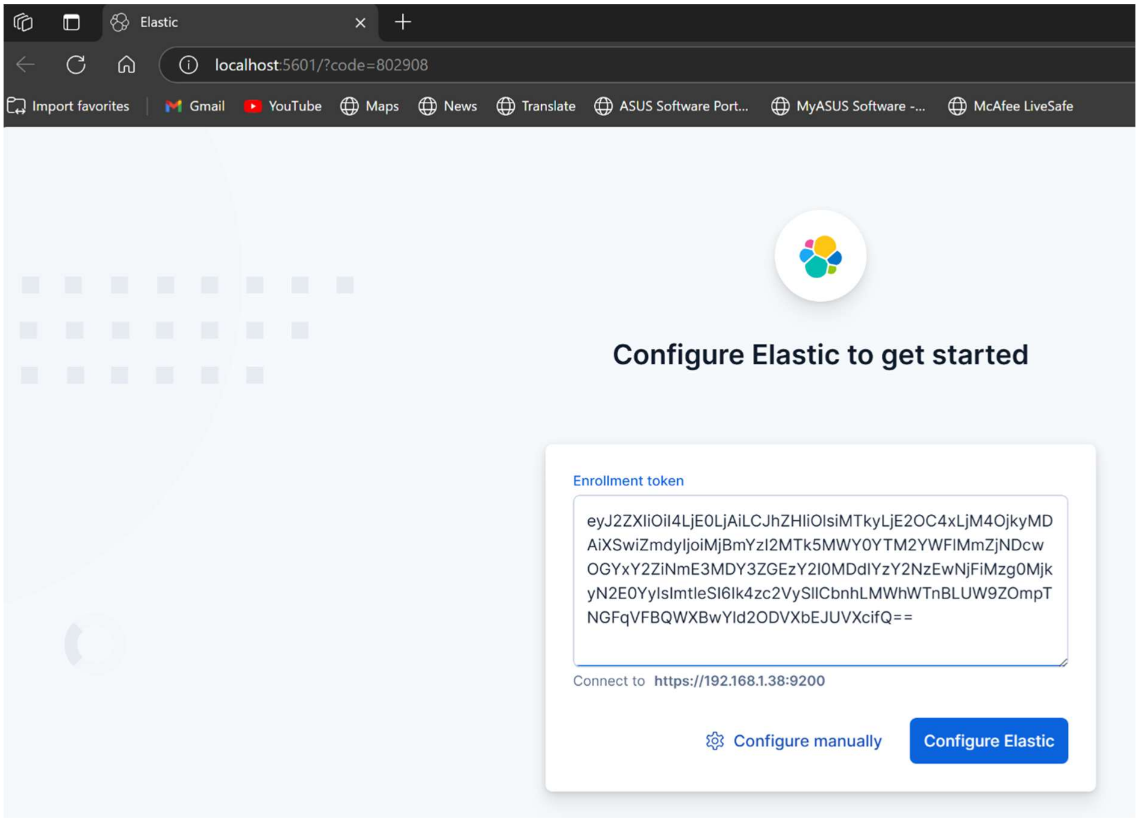


```
rt","value":true},"breakdownMetrics":{"source":"start","value":false},"captureBody":{"source":"start","value":"off","com
monName":"capture_body"},"captureHeaders":{"source":"start","value":false},"centralConfig":{"source":"start","value":fal
se},"contextPropagationOnly":{"source":"start","value":true},"environment":{"source":"start","value":"production"},"glob
alLabels":{"source":"start","value":[["git_rev","504d6bfa94cca17fabb76e06152c30c4f0c3efdd"]],"sourceValue":{"git_rev":"5
04d6bfa94cca17fabb76e06152c30c4f0c3efdd"}},"logLevel":{"source":"default","value":"info","commonName":"log_level"},"metr
icsInterval":{"source":"start","value":120,"sourceValue":"120s"},"serverUrl":{"source":"start","value":"https://kibana-c
loud-apm.apm.us-east-1.aws.found.io/","commonName":"server_url"},"transactionSampleRate":{"source":"start","value":0.1,"
commonName":"transaction_sample_rate"},"captureSpanStackTraces":{"source":"start","sourceValue":false},"secretToken":{"s
ource":"start","value":"[REDACTED]","commonName":"secret_token"},"serviceName":{"source":"start","value":"kibana","commo
nName":"service_name"},"serviceVersion":{"source":"start","value":"9.0.0","commonName":"service_version"}},"activationMe
thod":"require","message":"Elastic APM Node.js Agent v4.11.2"}
Native global console methods have been overridden in production environment.
[2025-05-08T00:33:42.649+05:30][INFO ][root] Kibana is starting
[2025-05-08T00:33:42.671+05:30][INFO ][node] Kibana process configured with roles: [background_tasks, ui]
[2025-05-08T00:33:53.586+05:30][INFO ][plugins-service] The following plugins are disabled: "cloudChat,cloudExperiments,
cloudFullStory,dataUsage,investigateApp,investigate,profilingDataAccess,profiling,searchHomepage,securitySolutionServerl
ess,serverless,serverlessObservability,serverlessSearch".
[2025-05-08T00:33:53.646+05:30][INFO ][http.server.Preboot] http server running at http://localhost:5601
[2025-05-08T00:33:53.793+05:30][INFO ][plugins-system.preboot] Setting up [1] plugins: [interactiveSetup]
[2025-05-08T00:33:53.823+05:30][INFO ][preboot] "interactiveSetup" plugin is holding setup: Validating Elasticsearch con
nection configuration…
[2025-05-08T00:33:53.864+05:30][INFO ][root] Holding setup until preboot stage is completed.


i Kibana has not been configured.

Go to http://localhost:5601/?code=802908 to get started.
```

5. Accessed Kibana setup via browser using the link:

http://localhost:5601/?code=802908.

Pasted the enrollment token copied from the Elasticsearch console into the Kibana web UI to begin the setup.



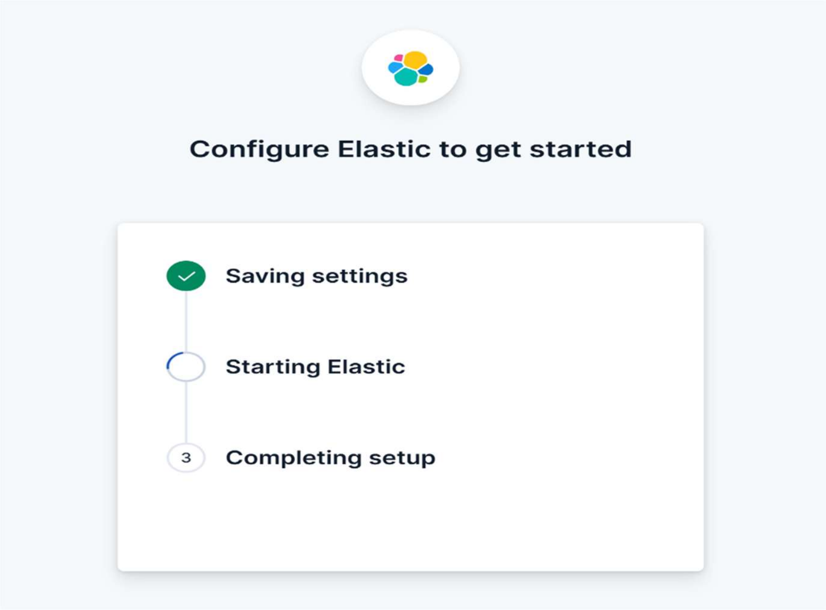
Configure Elastic to get started

Enrollment token

```
eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMTkyLjE2OC4xLjM4OjkyMD
AiXSwiZmdyIjoiMjBmYzI2MTk5MWY0YTM2YWFlMmZjNDcw
OGYxY2ZiNmE3MDY3ZGEzY2I0MDdlYzY2NzEwNjFiMzg0Mjk
yN2E0YyIsImtleSI6Ik4zc2VySllCbnhLMWhWTnBLUW9ZOmpT
NGFqVFBQWXBwYld2ODVXbEJUVXcifQ==
```

Connect to https://192.168.1.38:9200

6. After successful verification, Kibana proceeded to the **"Saving settings" → "Starting Elastic" → "Completing setup"** stages.



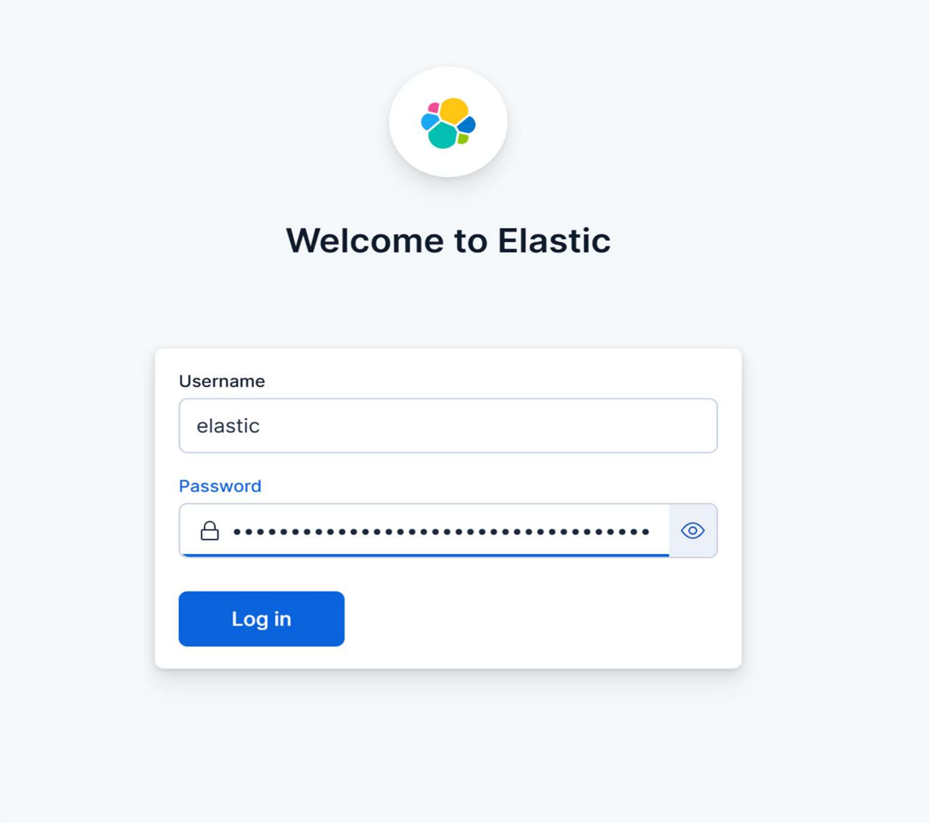
Configure Elastic to get started

✓ Saving settings

○ Starting Elastic

3 Completing setup

7. Logged in with the default username elastic and the password shown during Elasticsearch startup.

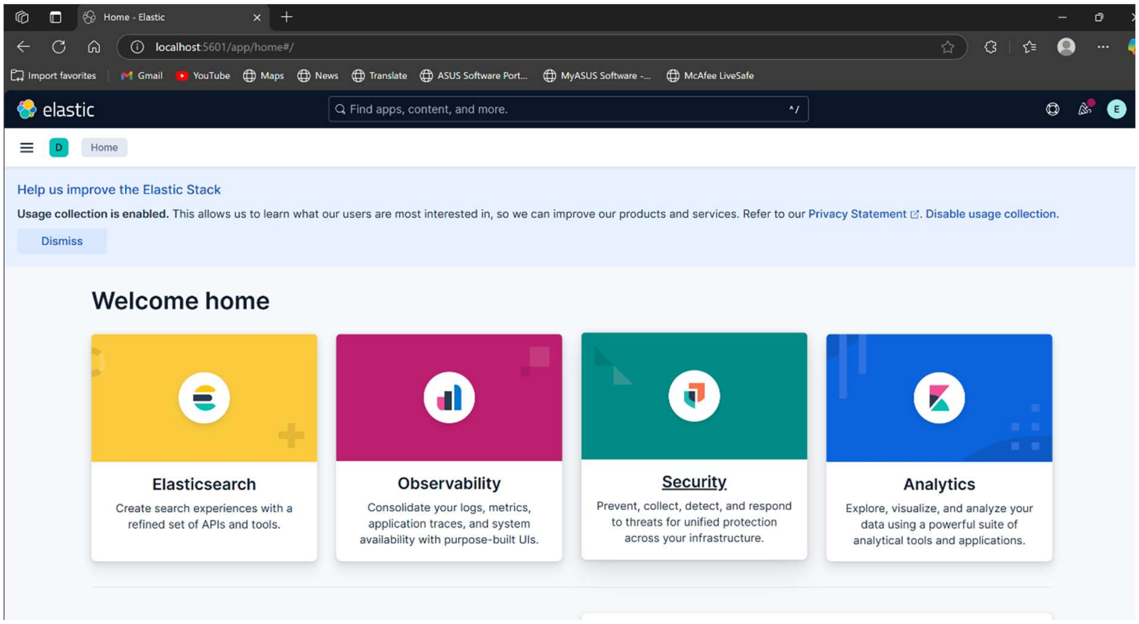


Welcome to Elastic

Username: elastic

Password: ••••••••••••••••••••••••••••••••••••

8. Accessed the **Kibana Dashboard**, which displayed available modules like *Elasticsearch*, *Observability*, *Security*, and *Analytics*.



Help us improve the Elastic Stack

Usage collection is enabled. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our Privacy Statement. Disable usage collection.

Welcome home

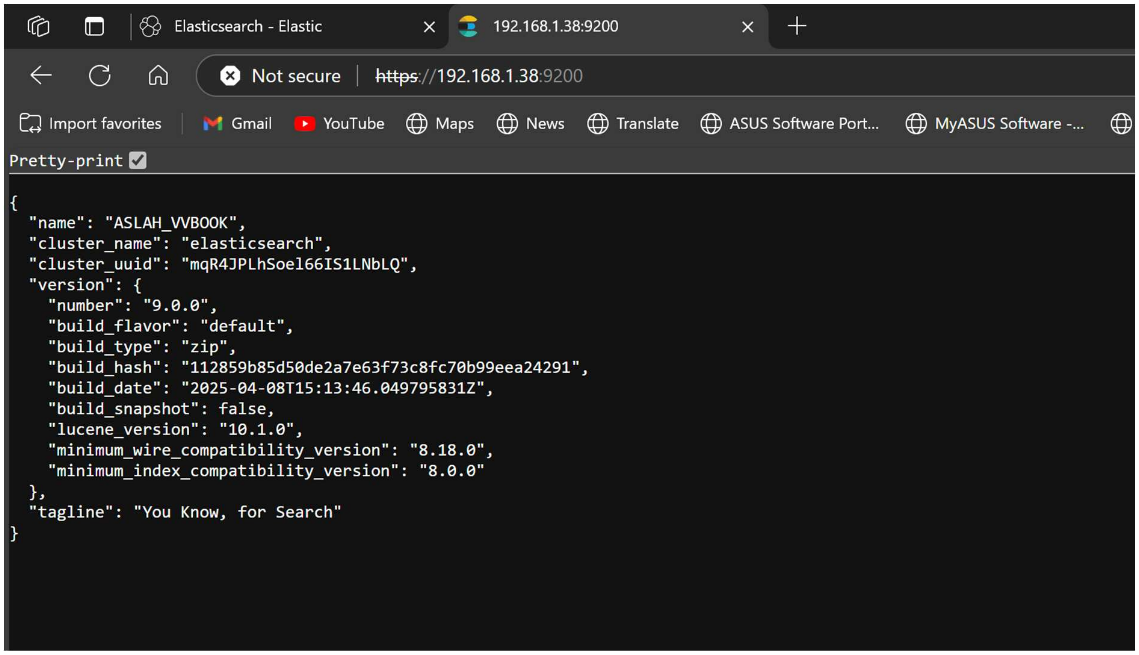
Elasticsearch
Create search experiences with a refined set of APIs and tools.

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.

9.Verified Elasticsearch was running by visiting https://192.168.1.38:9200, where the node details, version, and cluster metadata were shown in JSON format.



```
{
  "name": "ASLAH_VVBOOK",
  "cluster_name": "elasticsearch",
  "cluster_uuid": "mqR4JPLhSoel66IS1LNbLQ",
  "version": {
    "number": "9.0.0",
    "build_flavor": "default",
    "build_type": "zip",
    "build_hash": "112859b85d50de2a7e63f73c8fc70b99eea24291",
    "build_date": "2025-04-08T15:13:46.049795831Z",
    "build_snapshot": false,
    "lucene_version": "10.1.0",
    "minimum_wire_compatibility_version": "8.18.0",
    "minimum_index_compatibility_version": "8.0.0"
  },
  "tagline": "You Know, for Search"
}
```