ELKStack & Wazuh

Task:01

Installation of wazuh and ELK and also integrate it on Ubuntu.

STEP 1:

Installing prerequisites in Ubuntu.

```
# apt-get install apt-transport-https zip unzip lsb-release curl
gnupg
```

STEP 2:

Install Elasticsearch on Ubuntu.

Adding the Elastic Stack repository Install

the GPG key:

```
# curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg
--no-default-keyring --keyring
gnupgring:/usr/share/keyrings/elasticsearch.gpg --import && chmod
644 /usr/share/keyrings/elasticsearch.gpg
```

Add the repository:

```
# echo "deb [signed-by=/usr/share/keyrings/elasticsearch.gpg]
https://artifacts.elastic.co/packages/7.x/apt stable main" | tee
/etc/apt/sources.list.d/elastic-7.x.list
```

Update the package information:

```
# apt-get update wget -qO - https://artifacts.elastic.co/GPG-
KEYelasticsearch | sudo gpg
--dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
```

STEP 3:

Install & Configure Elasticsearch on ubuntu.

Install the Elasticsearch package:

```
# apt-get install elasticsearch=7.17.6
```

Download the configuration file /etc/elasticsearch/elasticsearch.yml as follows:

```
# curl -so /etc/elasticsearch/elasticsearch.yml
https://packages.wazuh.com/4.3/tpl/elasticbasic/elasticsearch_all_
in_one.yml
```

STEP 4:

Certificates creation and deployment:

Download the configuration file for creating the certificates:

```
# curl -so /usr/share/elasticsearch/instances.yml
https://packages.wazuh.com/4.3/tpl/elasticbasic/instances_aio.yml
```

The certificates can be created using the elasticsearch-certutil tool:

```
# /usr/share/elasticsearch/bin/elasticsearch-certutil cert ca -
pem --in instances.yml
--keep-ca-key --out ~/certs.zip
```

Extract the generated /usr/share/elasticsearch/certs.zip file from the previous step:

```
# unzip ~/certs.zip -d ~/certs
```

The next step is to create the directory /etc/elasticsearch/certs, and then copy the CA file, the certificate and the key there:

```
# mkdir /etc/elasticsearch/certs/ca -p
# cp -R ~/certs/ca/ ~/certs/elasticsearch/* /etc/elasticsearch/certs/
# chown -R elasticsearch: /etc/elasticsearch/certs
# chmod -R 500 /etc/elasticsearch/certs
# chmod 400 /etc/elasticsearch/certs/ca/ca.*
/etc/elasticsearch/certs/elasticsearch.*
```

```
# rm -rf ~/certs/ ~/certs.zip
```

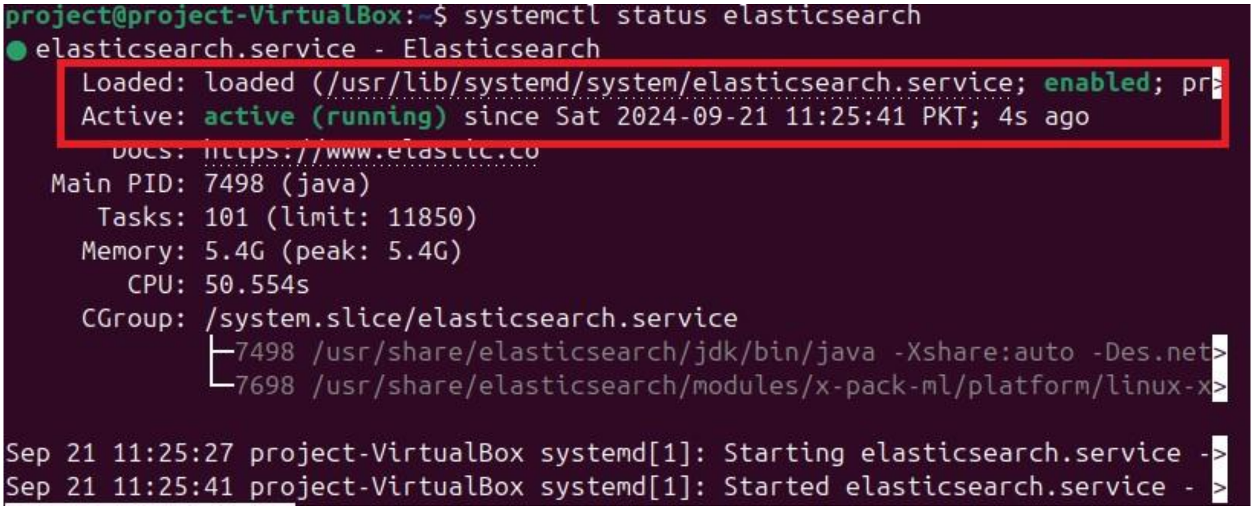
STEP 5:

Enable and start the Elasticsearch service:

```
# systemctl daemon-reload
# systemctl enable elasticsearch
# systemctl start elasticsearch
```

Check the status of elasticsearch it show active.

```
# systemctl status elasticsearch
```



```
project@project-VirtualBox:~$ systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; pr>
     Active: active (running) since Sat 2024-09-21 11:25:41 PKT; 4s ago
       Docs: https://www.elastic.co
   Main PID: 7498 (java)
      Tasks: 101 (limit: 11850)
     Memory: 5.4G (peak: 5.4G)
        CPU: 50.554s
     CGroup: /system.slice/elasticsearch.service
             ├─7498 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.net>
             └─7698 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>

Sep 21 11:25:27 project-VirtualBox systemd[1]: Starting elasticsearch.service ->
Sep 21 11:25:41 project-VirtualBox systemd[1]: Started elasticsearch.service - >
```

STEP 6:

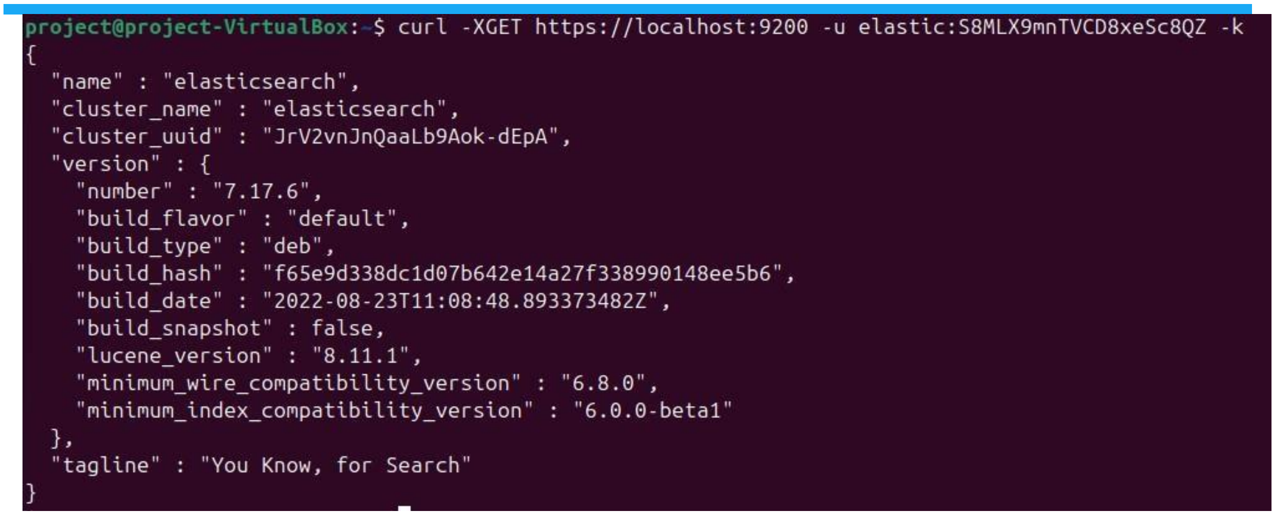
Generate credentials for all the Elastic Stack pre-built roles and users:

```
# /usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto
```

STEP 7:

To check that the installation was made successfully:

```
# curl -XGET https://localhost:9200 -u elastic:<elastic_password>
-k
```



```
project@project-VirtualBox:~$ curl -XGET https://localhost:9200 -u elastic:S8MLX9mnTVCD8xeSc8QZ -k
{
  "name" : "elasticsearch",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "JrV2vnJnQaaLb9Aok-dEpA",
  "version" : {
    "number" : "7.17.6",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "f65e9d338dc1d07b642e14a27f338990148ee5b6",
    "build_date" : "2022-08-23T11:08:48.893373482Z",
    "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"
}
```

STEP 8:

Installing Wazuh server:

Adding the Wazuh repository:

Install the GPG key:

```
# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg -no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

Add the repository:

```
# echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

Update the package information:

```
# apt-get update
```

Install the Wazuh manager package:

```
# apt-get install wazuh-manager=4.3.11-1
```

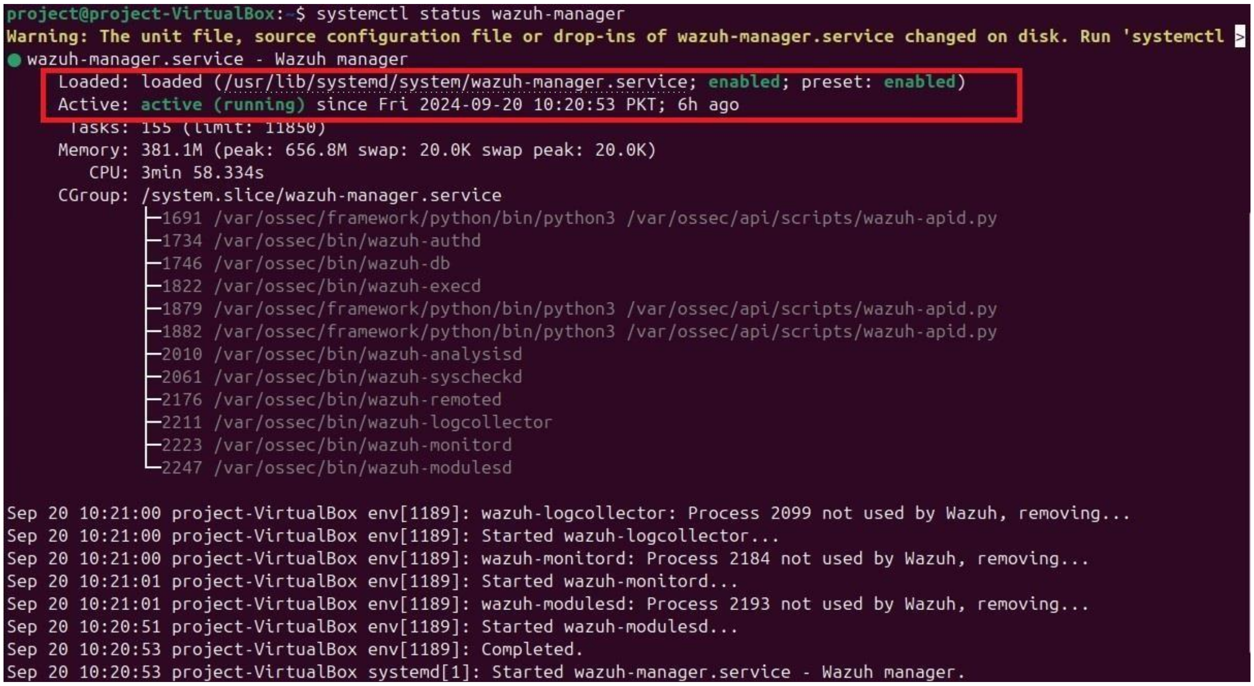
Enable and start the Wazuh manager service:

```
# systemctl daemon-reload
# systemctl enable wazuh-manager
```

```
# systemctl start wazuh-manager
```

Run the following command to check if the Wazuh manager is active:

```
# systemctl status wazuh-manager
```



```
project@project-VirtualBox:~$ systemctl status wazuh-manager
Warning: The unit file, source configuration file or drop-ins of wazuh-manager.service changed on disk. Run 'systemctl >
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: enabled)
     Active: active (running) since Fri 2024-09-20 10:20:53 PKT; 6h ago
      Tasks: 155 (limit: 11850)
     Memory: 381.1M (peak: 656.8M swap: 20.0K swap peak: 20.0K)
        CPU: 3min 58.334s
     CGroup: /system.slice/wazuh-manager.service
             ├─1691 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─1734 /var/ossec/bin/wazuh-authd
             ├─1746 /var/ossec/bin/wazuh-db
             ├─1822 /var/ossec/bin/wazuh-execd
             ├─1879 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─1882 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─2010 /var/ossec/bin/wazuh-analysisd
             ├─2061 /var/ossec/bin/wazuh-syscheckd
             ├─2176 /var/ossec/bin/wazuh-remoted
             ├─2211 /var/ossec/bin/wazuh-logcollector
             ├─2223 /var/ossec/bin/wazuh-monitord
             └─2247 /var/ossec/bin/wazuh-modulesd

Sep 20 10:21:00 project-VirtualBox env[1189]: wazuh-logcollector: Process 2099 not used by Wazuh, removing...
Sep 20 10:21:00 project-VirtualBox env[1189]: Started wazuh-logcollector...
Sep 20 10:21:00 project-VirtualBox env[1189]: wazuh-monitord: Process 2184 not used by Wazuh, removing...
Sep 20 10:21:01 project-VirtualBox env[1189]: Started wazuh-monitord...
Sep 20 10:21:01 project-VirtualBox env[1189]: wazuh-modulesd: Process 2193 not used by Wazuh, removing...
Sep 20 10:20:51 project-VirtualBox env[1189]: Started wazuh-modulesd...
Sep 20 10:20:53 project-VirtualBox env[1189]: Completed.
Sep 20 10:20:53 project-VirtualBox systemd[1]: Started wazuh-manager.service - Wazuh manager.
```

STEP 9:

Installing Filebeat:

Install the Filebeat package:

```
# apt-get install filebeat=7.17.6
```

Download the pre-configured Filebeat config file used to forward Wazuh alerts to Elasticsearch:

```
# curl -so /etc/filebeat/filebeat.yml
https://packages.wazuh.com/4.3/tpl/elasticbasic/filebeat_all_in_on
e.yml
```

Download the alerts template for Elasticsearch:

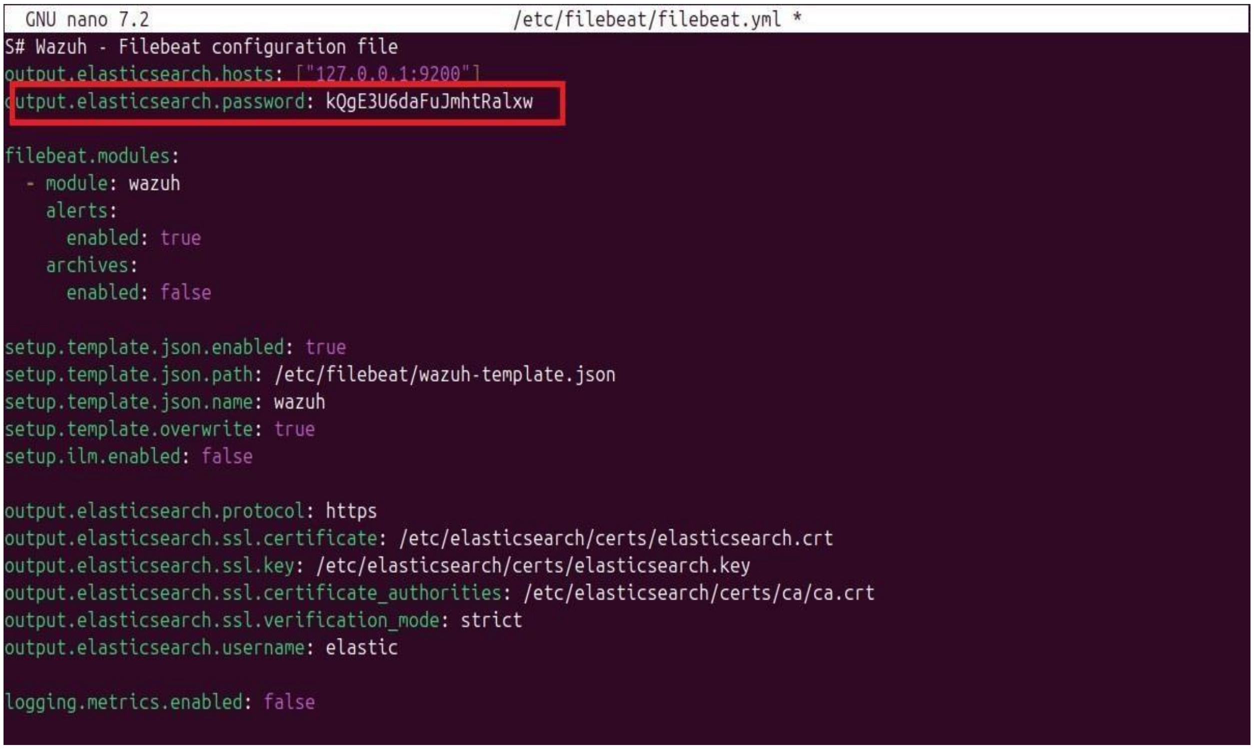
```
# curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/4.3/extensions/elasticsearch/7.x/wazuh-template.json

# chmod go+r /etc/filebeat/wazuh-template.json
```

Download the Wazuh module for Filebeat:

```
# curl -s https://packages.wazuh.com/4.x/filebeat/wazuhfilebeat-0.2.tar.gz | tar -xvz -C /usr/share/filebeat/module
```

Edit the file `/etc/filebeat/filebeat.yml` and add the following line:
`output.elasticsearch.password: <elasticsearch_password>`

Replace elasticsearch_password with the previously generated password for elastic user.



```
  GNU nano 7.2                              /etc/filebeat/filebeat.yml *
S# Wazuh - Filebeat configuration file
output.elasticsearch.hosts: ["127.0.0.1:9200"]
output.elasticsearch.password: kQgE3U6daFuJmhtRalxw

filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: false

setup.template.json.enabled: true
setup.template.json.path: /etc/filebeat/wazuh-template.json
setup.template.json.name: wazuh
setup.template.overwrite: true
setup.ilm.enabled: false

output.elasticsearch.protocol: https
output.elasticsearch.ssl.certificate: /etc/elasticsearch/certs/elasticsearch.crt
output.elasticsearch.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
output.elasticsearch.ssl.certificate_authorities: /etc/elasticsearch/certs/ca/ca.crt
output.elasticsearch.ssl.verification_mode: strict
output.elasticsearch.username: elastic

logging.metrics.enabled: false
```

Copy the certificates into /etc/filebeat/certs/

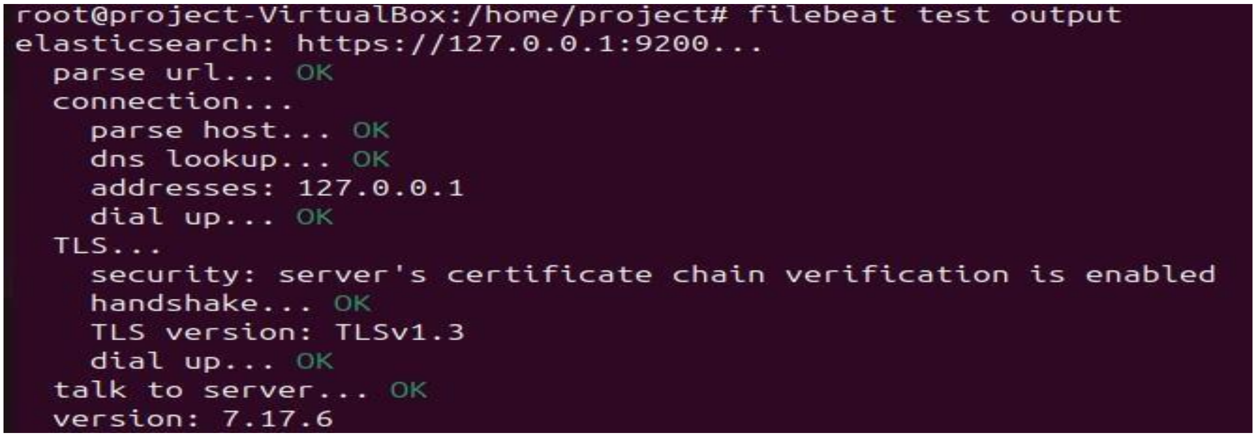
```
#cp -r /etc/elasticsearch/certs/ca/ /etc/filebeat/certs/

# cp /etc/elasticsearch/certs/elasticsearch.crt
/etc/filebeat/certs/filebeat.crt

# cp /etc/elasticsearch/certs/elasticsearch.key
/etc/filebeat/certs/filebeat.key
```

Enable and start the Filebeat service:

```
# systemctl daemon-reload

# systemctl enable filebeat

# systemctl start filebeat
```

To ensure that Filebeat has been successfully installed, run the following command:

```
# filebeat test output
```



```
root@project-VirtualBox:/home/project# filebeat test output
elasticsearch: https://127.0.0.1:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1
    dial up... OK
  TLS...
    security: server's certificate chain verification is enabled
    handshake... OK
    TLS version: TLSv1.3
    dial up... OK
  talk to server... OK
  version: 7.17.6
```

STEP 10:

Kibana installation and configuration: Install
the Kibana package:

```
# apt-get install kibana=7.17.6
```

Copy the Elasticsearch certificates into the Kibana configuration folder:

```
# mkdir /etc/kibana/certs/ca -p

# cp -R /etc/elasticsearch/certs/ca/ /etc/kibana/certs/

# cp /etc/elasticsearch/certs/elasticsearch.key
/etc/kibana/certs/kibana.key

# cp /etc/elasticsearch/certs/elasticsearch.crt
/etc/kibana/certs/kibana.crt
```

```
# chown -R kibana:kibana /etc/kibana/

# chmod -R 500 /etc/kibana/certs #

chmod 440 /etc/kibana/certs/ca/ca.

/etc/kibana/certs/kibana.
```

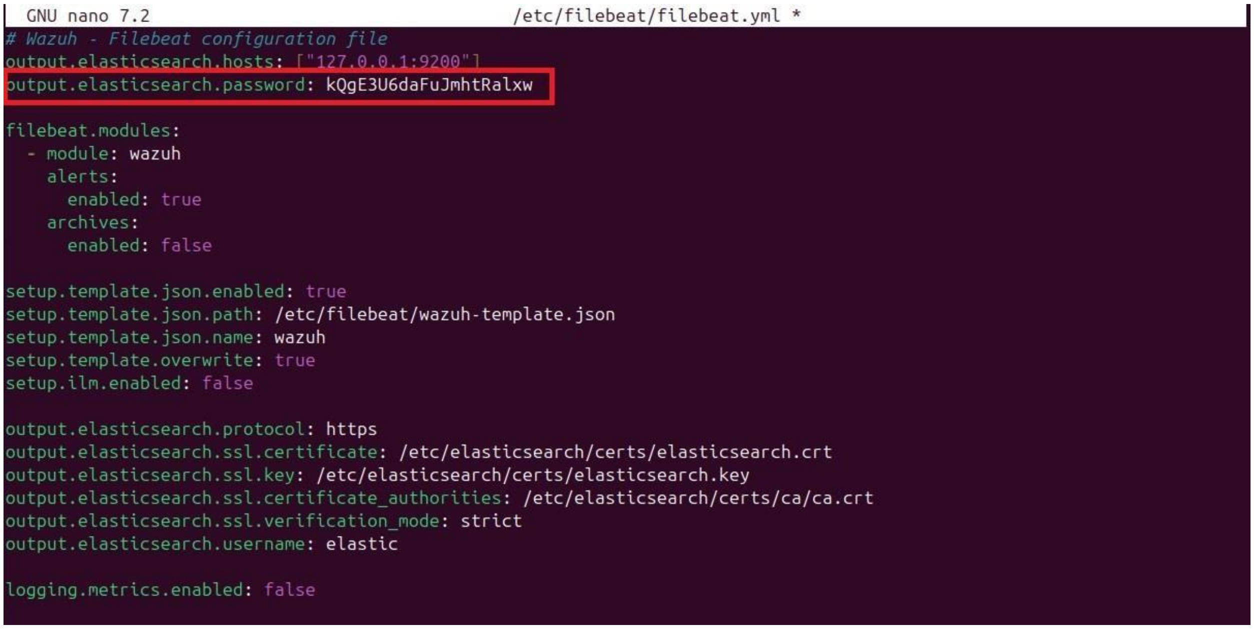
Download the Kibana configuration file:

```
# curl -so /etc/kibana/kibana.yml
https://packages.wazuh.com/4.3/tpl/elasticbasic/kibana_all_in_on
e.yml
```

Edit the /etc/kibana/kibana.yml file:

elasticsearch.password: <elasticsearch_password> Values to be replaced:

<elasticsearch_password>: the password generated during the Elasticsearch installation and configuration for the elastic user.



```
  GNU nano 7.2                              /etc/filebeat/filebeat.yml *
# Wazuh - Filebeat configuration file
output.elasticsearch.hosts: ["127.0.0.1:9200"]
output.elasticsearch.password: kQgE3U6daFuJmhtRalxw

filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: false

setup.template.json.enabled: true
setup.template.json.path: /etc/filebeat/wazuh-template.json
setup.template.json.name: wazuh
setup.template.overwrite: true
setup.ilm.enabled: false

output.elasticsearch.protocol: https
output.elasticsearch.ssl.certificate: /etc/elasticsearch/certs/elasticsearch.crt
output.elasticsearch.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
output.elasticsearch.ssl.certificate_authorities: /etc/elasticsearch/certs/ca/ca.crt
output.elasticsearch.ssl.verification_mode: strict
output.elasticsearch.username: elastic

logging.metrics.enabled: false
```

Create the /usr/share/kibana/data directory:

```
# mkdir /usr/share/kibana/data
# chown -R kibana:kibana /usr/share/kibana
```

Install the Wazuh Kibana plugin. The installation of the plugin must be done from the Kibana home directory as follows:

```
# cd /usr/share/kibana
# sudo -u kibana /usr/share/kibana/bin/kibana-plugin install
https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-
4.3.11_7.17.6-1.zip
```

Link Kibana's socket to privileged port 443:

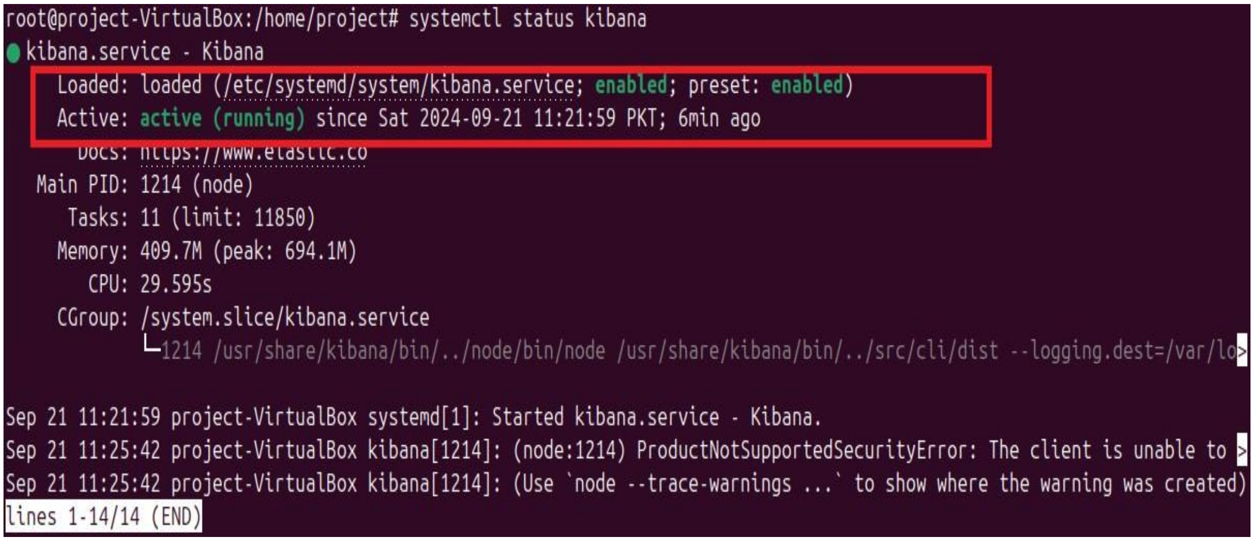
```
# setcap 'cap_net_bind_service=+ep'
/usr/share/kibana/node/bin/node
```

Enable and start the Kibana service:

```
# systemctl daemon-reload

# systemctl enable kibana

# systemctl start kibana
```

Check the status of kibana it show active.

```
# systemctl status kibana
```



```
root@project-VirtualBox:/home/project# systemctl status kibana
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-09-21 11:21:59 PKT; 6min ago
       Docs: https://www.elastic.co
   Main PID: 1214 (node)
      Tasks: 11 (limit: 11850)
     Memory: 409.7M (peak: 694.1M)
        CPU: 29.595s
     CGroup: /system.slice/kibana.service
             └─1214 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist --logging.dest=/var/lo>

Sep 21 11:21:59 project-VirtualBox systemd[1]: Started kibana.service - Kibana.
Sep 21 11:25:42 project-VirtualBox kibana[1214]: (node:1214) ProductNotSupportedSecurityError: The client is unable to >
Sep 21 11:25:42 project-VirtualBox kibana[1214]: (Use `node --trace-warnings ...` to show where the warning was created)
lines 1-14/14 (END)
```

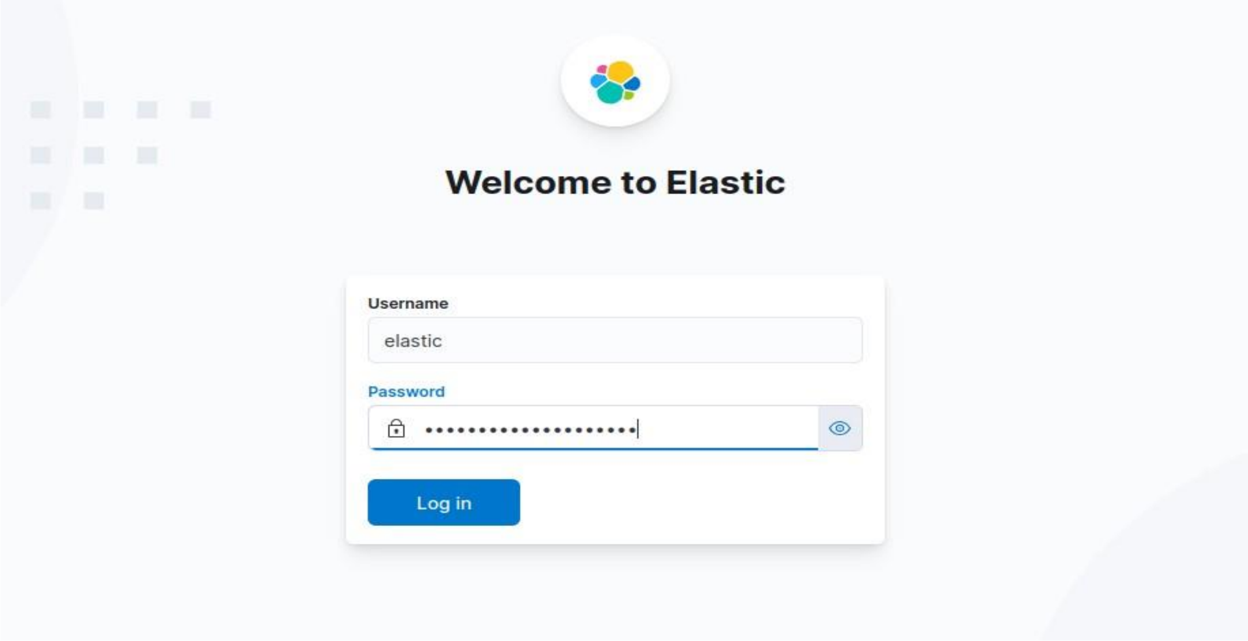
STEP 11:

Access the web interface using the password generated during the Elasticsearch installation process:

URL: https://<wazuh_server_ip> user:

elastic

Password: <Your Etastic Password>



Welcome to Elastic

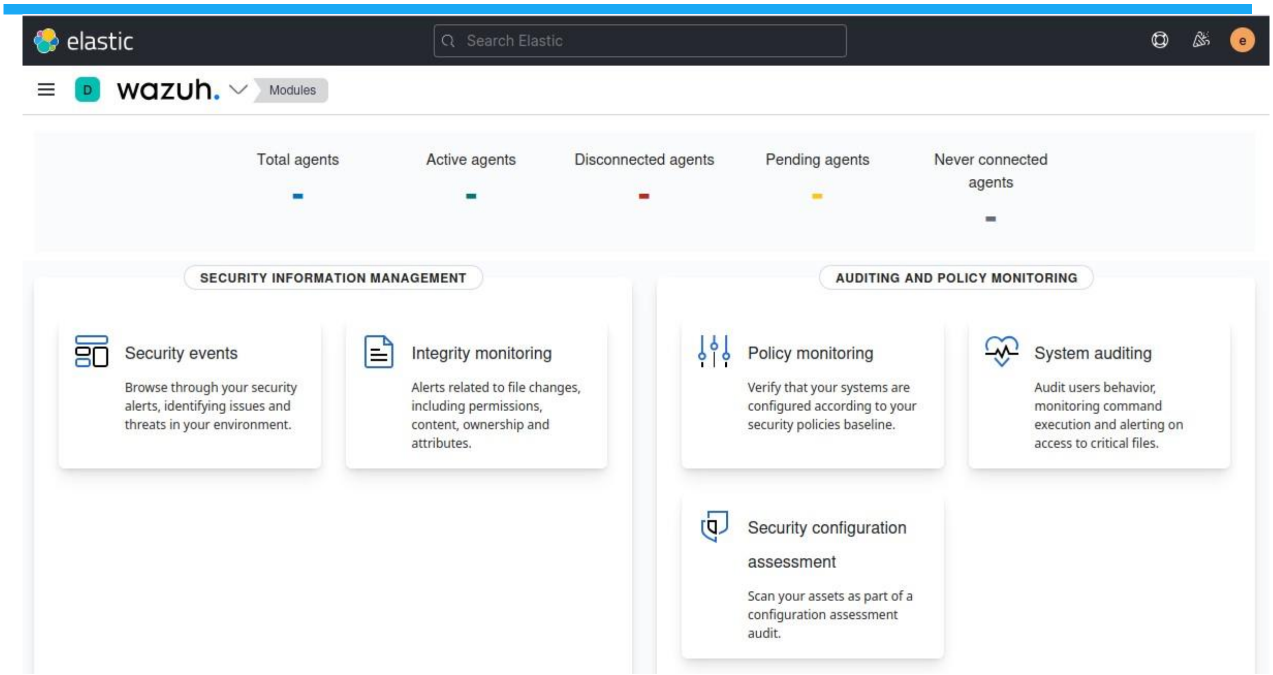
Username

elastic

Password

••••••••••••••••••••

After adding username & Password it show the wazuh within elasticsearch:



Total agents -

Active agents -

Disconnected agents -

Pending agents -

Never connected agents -

SECURITY INFORMATION MANAGEMENT

Security events

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

Integrity monitoring

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

AUDITING AND POLICY MONITORING

Policy monitoring

Verify that your systems are configured according to your security policies baseline.

System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.

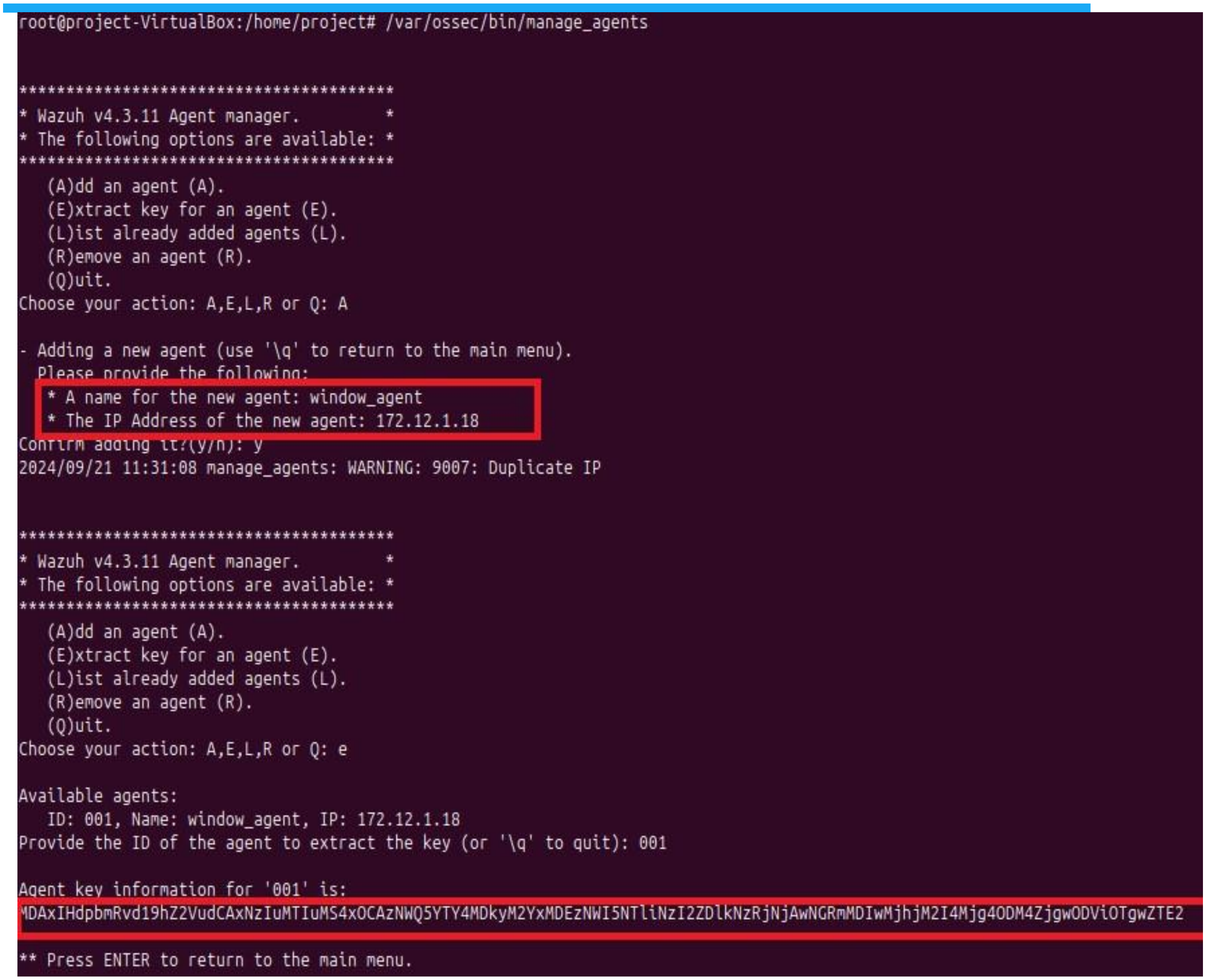
Security configuration assessment

Scan your assets as part of a configuration assessment audit.

Task 2
Adding the agent on wazuh.

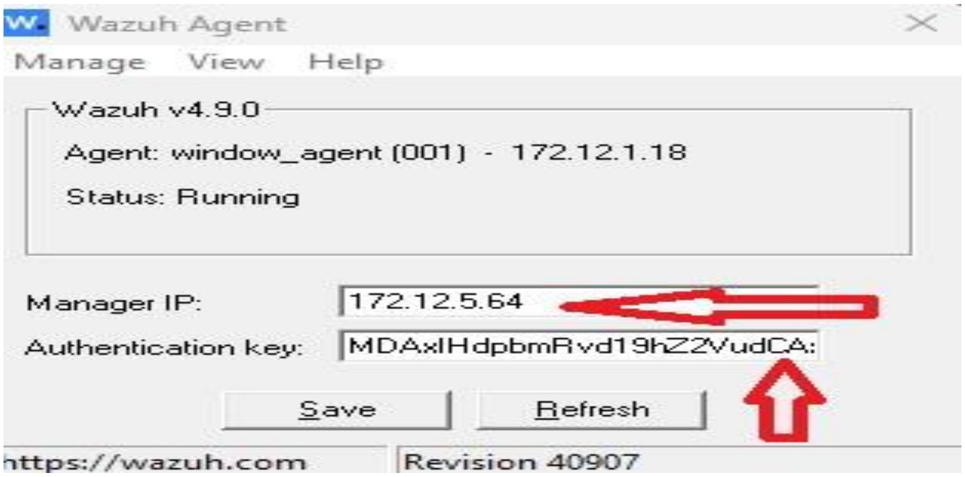
```
# /var/ossec/bin/manage_agents
```

Add the agent name and IP address of the agent machine and generate the key for agent.



```
root@project-VirtualBox:/home/project# /var/ossec/bin/manage_agents


****************************************
* Wazuh v4.3.11 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: window_agent
   * The IP Address of the new agent: 172.12.1.18
Confirm adding it?(y/n): y
2024/09/21 11:31:08 manage_agents: WARNING: 9007: Duplicate IP


****************************************
* Wazuh v4.3.11 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: e

Available agents:
   ID: 001, Name: window_agent, IP: 172.12.1.18
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIHdpbmRvd19hZ2VudCAxNzIuMTIuMS4xOCAzNWQ5YTY4MDkyM2YxMDEzNWI5NTliNzI2ZDlkNzRjNjAwNGRmMDIwMjhjM2I4Mjg4ODM4ZjgwODViOTgwZTE2

** Press ENTER to return to the main menu.
```

Install the agent on other system that you want to monitor it. I install the agent on window. Add the wazuh manger IP and agent key.



Wazuh v4.9.0

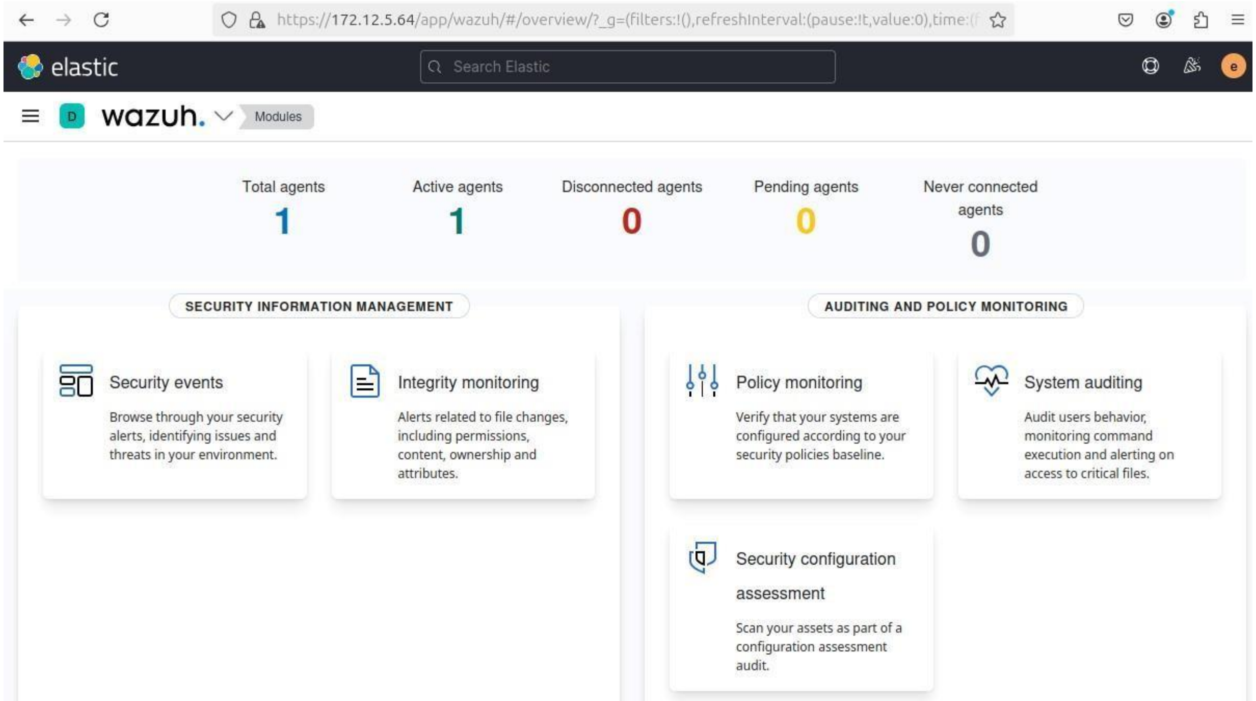
Agent: window_agent (001) - 172.12.1.18

Status: Running

Manager IP: 172.12.5.64

Authentication key: MDAxIHdpbmRvd19hZ2VudCA:

After adding the running the agent on window open the refresh the wazuh dashboard and it show agent was active.



https://172.12.5.64/app/wazuh/#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(
elastic
Search Elastic
wazuh.
Modules

Total agents	Active agents	Disconnected agents	Pending agents	Never connected agents
1	1	0	0	0

SECURITY INFORMATION MANAGEMENT

Security events

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

Integrity monitoring

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

AUDITING AND POLICY MONITORING

Policy monitoring

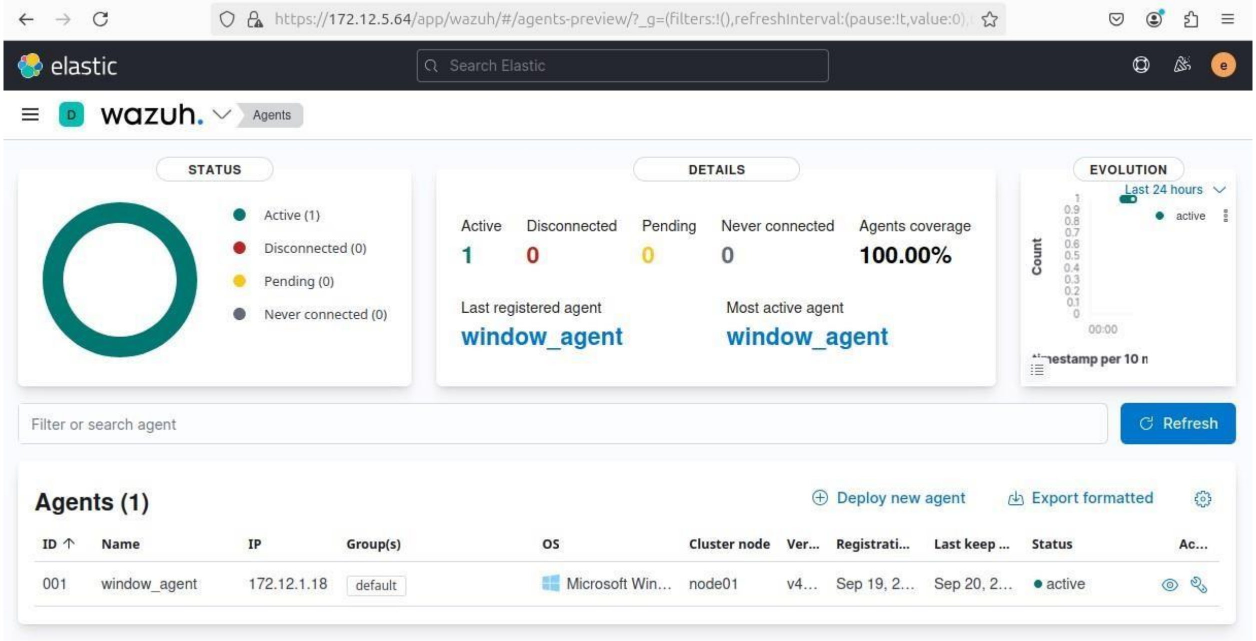
Verify that your systems are configured according to your security policies baseline.

System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.

Security configuration assessment

Scan your assets as part of a configuration assessment audit.



STATUS

- Active (1)
- Disconnected (0)
- Pending (0)
- Never connected (0)

DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

Last registered agent: window_agent

Most active agent: window_agent

Agents (1)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Ver...	Registrati...	Last keep ...	Status	Ac...
001	window_agent	172.12.1.18	default	Microsoft Win...	node01	v4...	Sep 19, 2...	Sep 20, 2...	● active	