Wazuh Installation

Wazuh Components:

Wazuh Indexer

Wazuh Manager (Server)

Wazuh Dashboard

Filebeat

Wazuh Agent

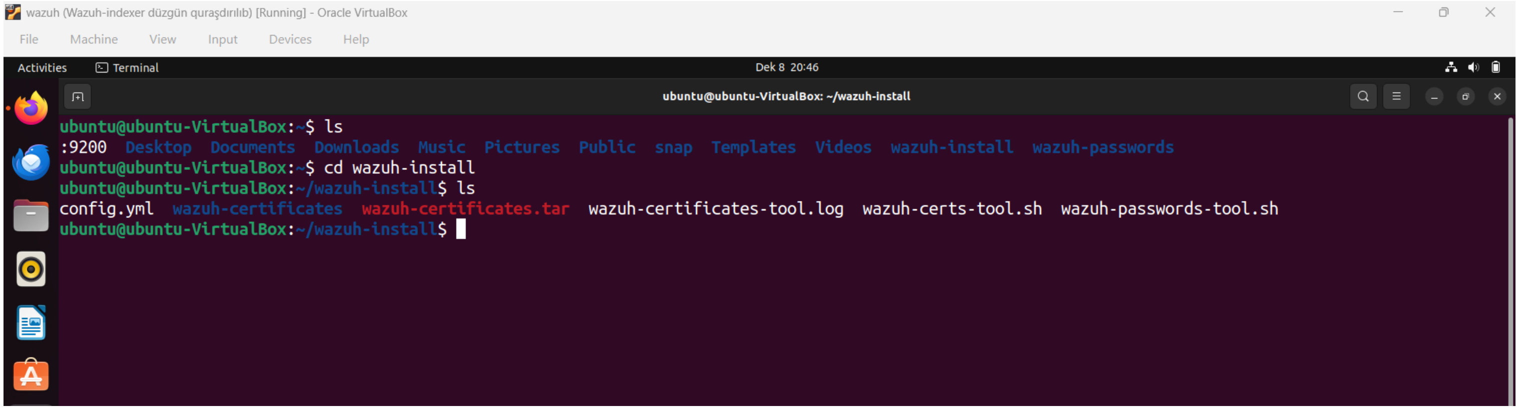
Certificate Creation

1)First we make direction for installation certificates and install certificates to the directory:

```
mkdir wazuh-install
```

Download the wazuh-certs-tool.sh script and the config.yml configuration file. This creates the certificates that encrypt communications between the Wazuh central components.

```
cd wazuh-install

curl -sO https://packages.wazuh.com/4.14/wazuh-certs-tool.sh

curl -sO https://packages.wazuh.com/4.14/config.yml
```

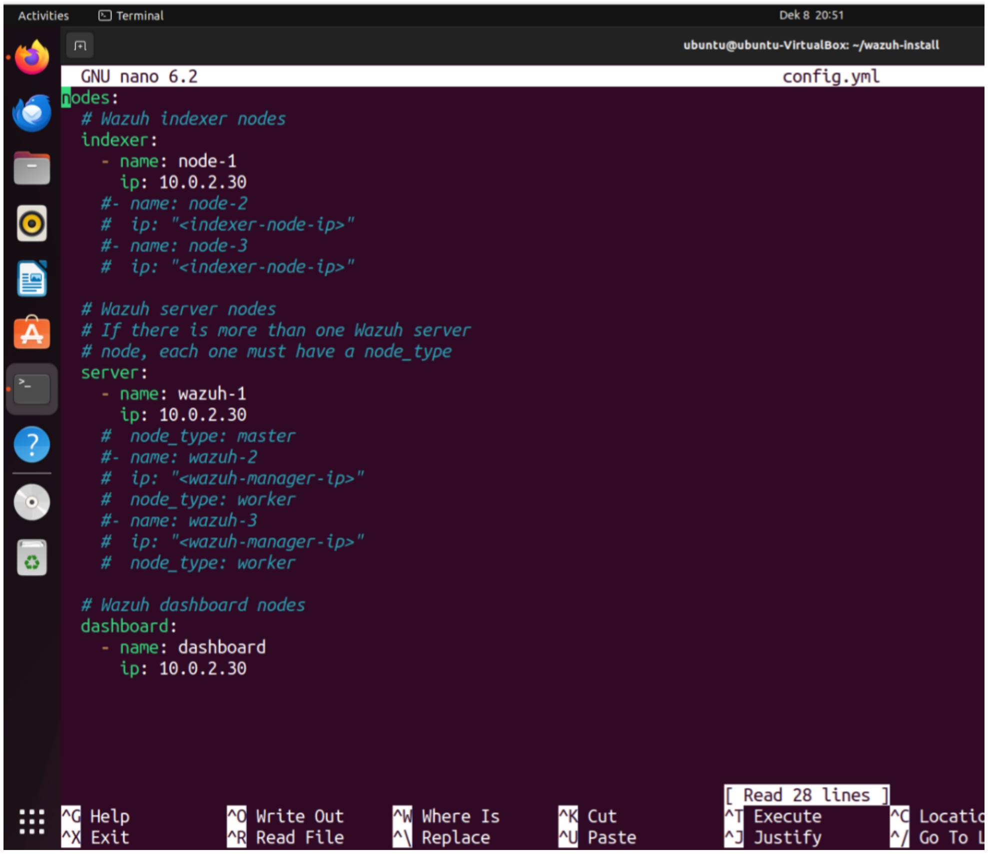

wazuh (Wazuh-indexer düzgün quraşdırılıb) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Dek 8 20:46
ubuntu@ubuntu-VirtualBox: ~/wazuh-install

```
ubuntu@ubuntu-VirtualBox:~$ ls
:9200  Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos  wazuh-install  wazuh-passwords
ubuntu@ubuntu-VirtualBox:~$ cd wazuh-install
ubuntu@ubuntu-VirtualBox:~/wazuh-install$ ls
config.yml  wazuh-certificates  wazuh-certificates.tar  wazuh-certificates-tool.log  wazuh-certs-tool.sh  wazuh-passwords-tool.sh
ubuntu@ubuntu-VirtualBox:~/wazuh-install$ 
```

2) Configure config.yml

```
nano config.yml
```

10.0.2.30 is our Ubunutu machine ipv4 which we install wazuh all-in-one



```
  GNU nano 6.2                                          config.yml
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: 10.0.2.30
    #- name: node-2
    #  ip: "<indexer-node-ip>"
    #- name: node-3
    #  ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: 10.0.2.30
    #  node_type: master
    #- name: wazuh-2
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: 10.0.2.30




                                                    [ Read 28 lines ]
^G Help         ^O Write Out    ^W Where Is     ^K Cut          ^T Execute      ^C Locatio
^X Exit         ^R Read File    ^\ Replace      ^U Paste        ^J Justify      ^/ Go To L
```

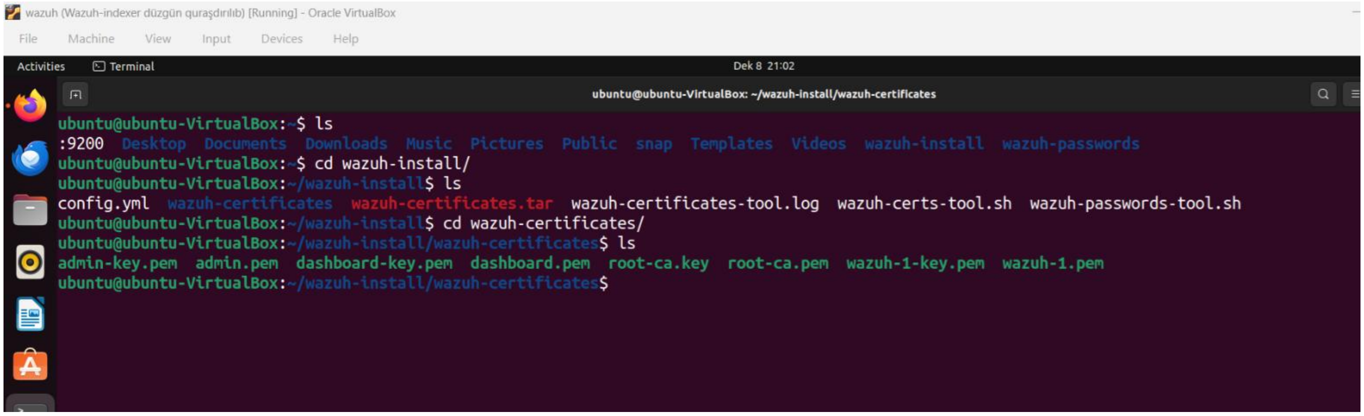
Note: Təhlükəsizlik Sertifikatlarının Yaradılması

Ən vacib hissə budur. Wazuh komponentləri bir-biri ilə şifrələnmiş (SSL/TLS) əlaqə qurur. Quraşdırma skripti bu config.yml faylını oxuyur və oradakı IP ünvanlarına uyğun **sertifikatlar (certificates)** yaradır.

Əgər bu faylda IP-ni səhv yazsan, sertifikatlar səhv yaranacaq və sistem işləməyəcək.

3) Run ./wazuh-certs-tool.sh to create the certificates

```
bash ./wazuh-certs-tool.sh -A
```



wazuh (Wazuh-indexer düzgün quraşdırılıb) [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Terminal
Dek 8 21:02
ubuntu@ubuntu-VirtualBox: ~/wazuh-install/wazuh-certificates

```
ubuntu@ubuntu-VirtualBox:~$ ls
:9200  Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos  wazuh-install  wazuh-passwords
ubuntu@ubuntu-VirtualBox:~$ cd wazuh-install/
ubuntu@ubuntu-VirtualBox:~/wazuh-install$ ls
config.yml  wazuh-certificates  wazuh-certificates.tar  wazuh-certificates-tool.log  wazuh-certs-tool.sh  wazuh-passwords-tool.sh
ubuntu@ubuntu-VirtualBox:~/wazuh-install$ cd wazuh-certificates/
ubuntu@ubuntu-VirtualBox:~/wazuh-install/wazuh-certificates$ ls
admin-key.pem  admin.pem  dashboard-key.pem  dashboard.pem  root-ca.key  root-ca.pem  wazuh-1-key.pem  wazuh-1.pem
ubuntu@ubuntu-VirtualBox:~/wazuh-install/wazuh-certificates$
```

Wazuh indexer nodes installation

1) Installing package dependencies

```
apt-get install debconf adduser procps
```

2) Adding the Wazuh repository

1. Install the following packages if missing.

   ```
   apt-get install gnupg apt-transport-https
   ```

2. 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
   ```

3. 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
   ```

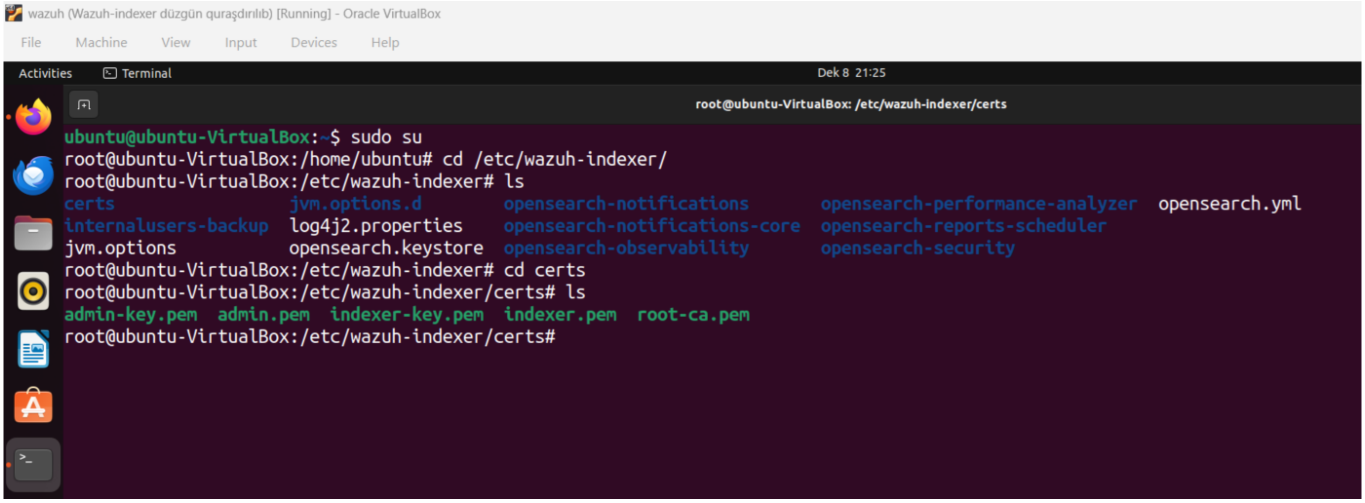
4. Update the packages information.

   ```
   apt-get update
   ```

Deploying certificates

```
1) mkdir /etc/wazuh-indexer/certs

2) tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./wazuh-1.pem ./wazuh-1-key.pem ./admin.pem ./admin-key.pem ./root-ca.pem

3) mv -n /etc/wazuh-indexer/certs/wazuh-1.pem /etc/wazuh-indexer/certs/indexer.pem

4) mv -n /etc/wazuh-indexer/certs/wazuh-1-key.pem /etc/wazuh-indexer/certs/indexer-key.pem

5) chmod 500 /etc/wazuh-indexer/certs

6) chmod 400 /etc/wazuh-indexer/certs/*

7) chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
```

Result:

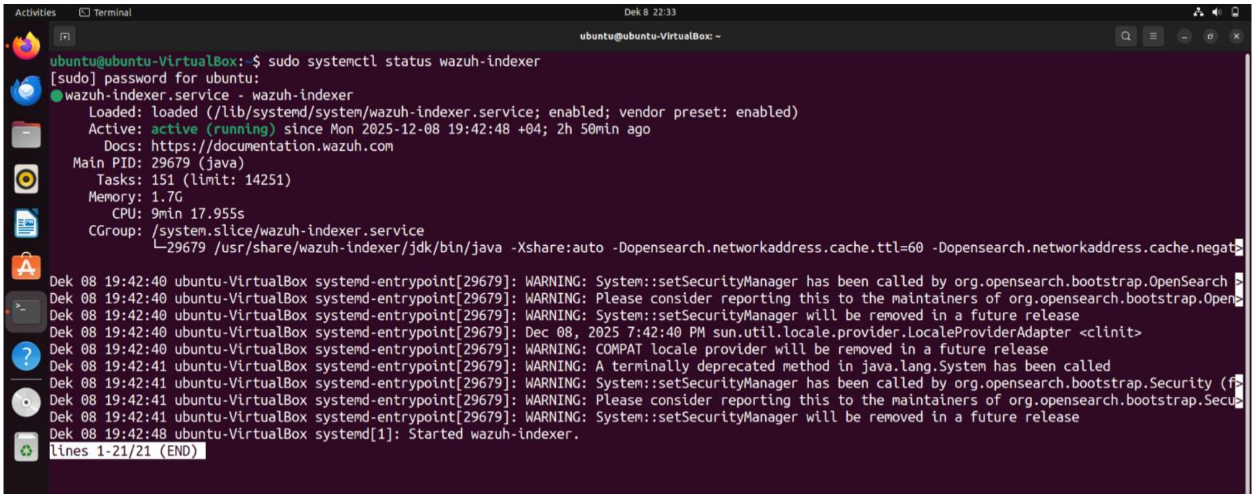

wazuh (Wazuh-indexer düzgün quraşdırılıb) [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Activities
Terminal
Dek 8 21:25
root@ubuntu-VirtualBox: /etc/wazuh-indexer/certs

```
ubuntu@ubuntu-VirtualBox:~$ sudo su
root@ubuntu-VirtualBox:/home/ubuntu# cd /etc/wazuh-indexer/
root@ubuntu-VirtualBox:/etc/wazuh-indexer# ls
certs                jvm.options.d        opensearch-notifications       opensearch-performance-analyzer  opensearch.yml
internalusers-backup log4j2.properties    opensearch-notifications-core  opensearch-reports-scheduler
jvm.options          opensearch.keystore  opensearch-observability       opensearch-security
root@ubuntu-VirtualBox:/etc/wazuh-indexer# cd certs
root@ubuntu-VirtualBox:/etc/wazuh-indexer/certs# ls
admin-key.pem  admin.pem  indexer-key.pem  indexer.pem  root-ca.pem
root@ubuntu-VirtualBox:/etc/wazuh-indexer/certs#
```

Starting the service

Enable and start the Wazuh indexer service

```
systemctl daemon-reload

systemctl enable wazuh-indexer

systemctl start wazuh-indexer
```



```
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl status wazuh-indexer
[sudo] password for ubuntu:
● wazuh-indexer.service - wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2025-12-08 19:42:48 +04; 2h 50min ago
       Docs: https://documentation.wazuh.com
   Main PID: 29679 (java)
      Tasks: 151 (limit: 14251)
     Memory: 1.7G
        CPU: 9min 17.955s
     CGroup: /system.slice/wazuh-indexer.service
             └─29679 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.negat>

Dek 08 19:42:40 ubuntu-VirtualBox systemd-entrypoint[29679]: WARNING: System::setSecurityManager has been called by org.opensearch.bootstrap.OpenSearch >
Dek 08 19:42:40 ubuntu-VirtualBox systemd-entrypoint[29679]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap.Open>
Dek 08 19:42:40 ubuntu-VirtualBox systemd-entrypoint[29679]: WARNING: System::setSecurityManager will be removed in a future release
Dek 08 19:42:40 ubuntu-VirtualBox systemd-entrypoint[29679]: Dec 08, 2025 7:42:40 PM sun.util.locale.provider.LocaleProviderAdapter <clinit>
Dek 08 19:42:40 ubuntu-VirtualBox systemd-entrypoint[29679]: WARNING: COMPAT locale provider will be removed in a future release
Dek 08 19:42:41 ubuntu-VirtualBox systemd-entrypoint[29679]: WARNING: A terminally deprecated method in java.lang.System has been called
Dek 08 19:42:41 ubuntu-VirtualBox systemd-entrypoint[29679]: WARNING: System::setSecurityManager has been called by org.opensearch.bootstrap.Security (f>
Dek 08 19:42:41 ubuntu-VirtualBox systemd-entrypoint[29679]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap.Secu>
Dek 08 19:42:41 ubuntu-VirtualBox systemd-entrypoint[29679]: WARNING: System::setSecurityManager will be removed in a future release
Dek 08 19:42:48 ubuntu-VirtualBox systemd[1]: Started wazuh-indexer.
lines 1-21/21 (END)
```

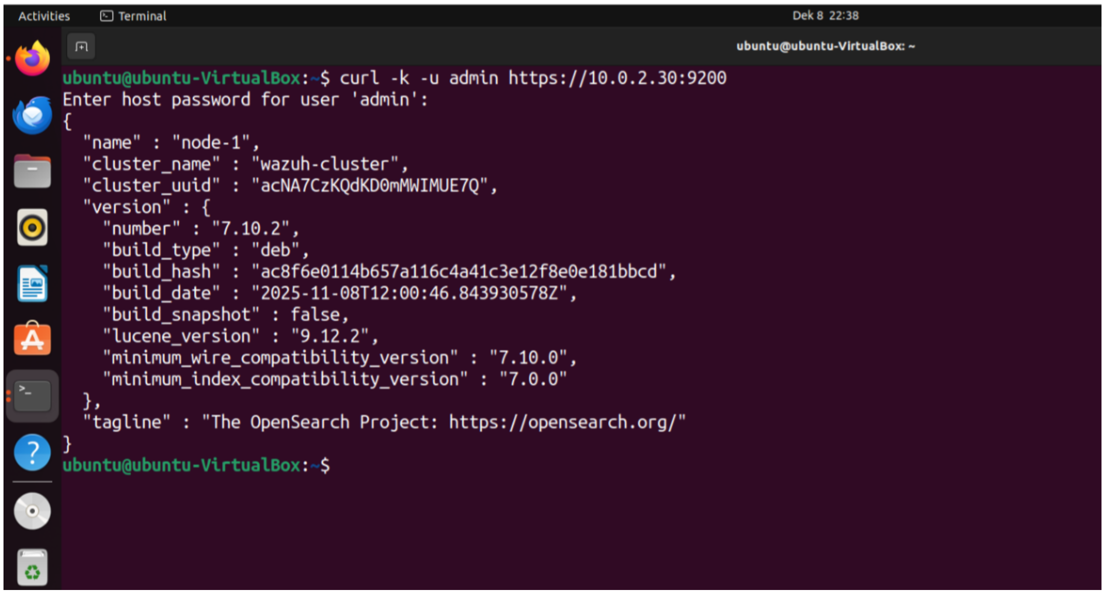
Cluster initialization

Run the Wazuh indexer indexer-security-init.sh script on *any* Wazuh indexer node to load the new certificates information and start the single-node or multi-node cluster

```
/usr/share/wazuh-indexer/bin/indexer-security-init.sh
```

Testing the cluster installation:

```
curl -k -u admin https://10.0.2.30:9200
```



```
ubuntu@ubuntu-VirtualBox:~$ curl -k -u admin https://10.0.2.30:9200
Enter host password for user 'admin':
{
  "name" : "node-1",
  "cluster_name" : "wazuh-cluster",
  "cluster_uuid" : "acNA7CzKQdKD0mMWIMUE7Q",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "deb",
    "build_hash" : "ac8f6e0114b657a116c4a41c3e12f8e0e181bbcd",
    "build_date" : "2025-11-08T12:00:46.843930578Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.2",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
ubuntu@ubuntu-VirtualBox:~$
```

Installing the Wazuh manager

Install the Wazuh manager package.

```
apt-get -y install wazuh-manager
```

Installing Filebeat

Install the Filebeat package.

```
apt-get -y install filebeat
```

Configuring Filebeat

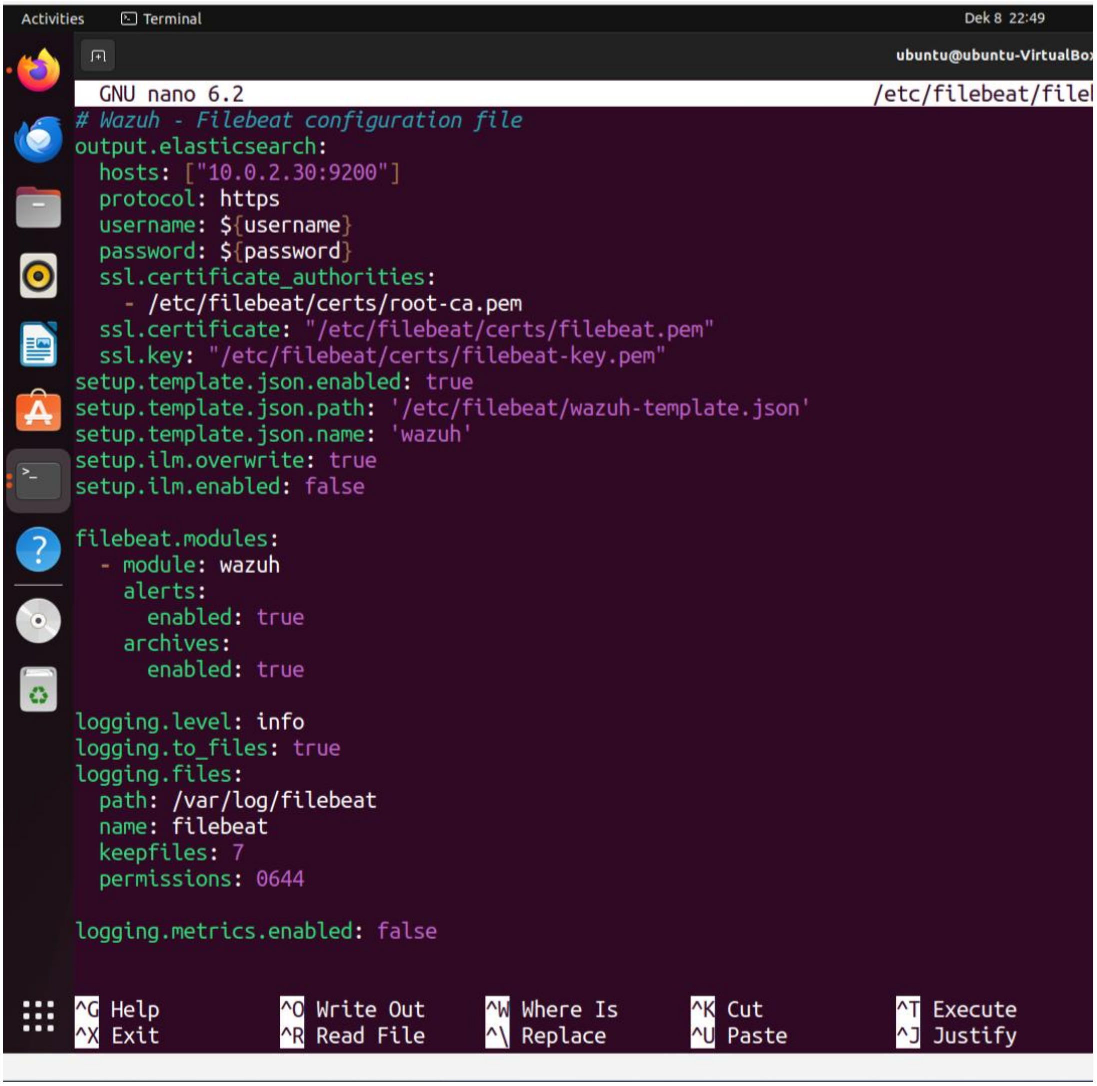
1) Download the preconfigured Filebeat configuration file

curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.14/tpl/wazuh/filebeat/filebeat.yml

2) Edit the /etc/filebeat/filebeat.yml configuration file and replace the following value:

```
nano /etc/filebeat/filebeat.yml
```

Note: archives:enabled:true



```
# Wazuh - Filebeat configuration file
output.elasticsearch:
  hosts: ["10.0.2.30:9200"]
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/filebeat.pem"
  ssl.key: "/etc/filebeat/certs/filebeat-key.pem"
setup.template.json.enabled: true
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: false

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

logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat
  keepfiles: 7
  permissions: 0644

logging.metrics.enabled: false
```

3) Create a Filebeat keystore to securely store authentication credentials.

```
filebeat keystore create
```

4) Add the default username and password admin:admin

```
filebeat keystore add username

filebeat keystore add password
```

5) Download the alerts template for the Wazuh indexer.

```
curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v4.14.1/extensions/elasticsearc
h/7.x/wazuh-template.json

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

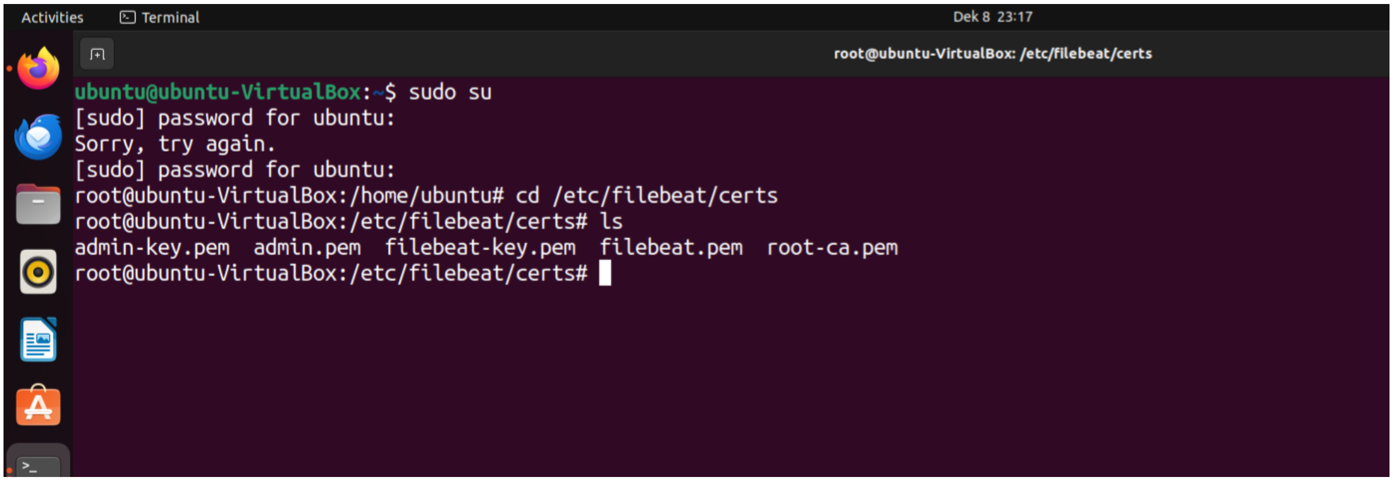
6) Install the Wazuh module for Filebeat

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar -xvz -C /usr/share/filebeat/module

Deploying certificates

Deploy certificates for filebeat

```
mkdir /etc/filebeat/certs

tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./wazuh-1.pem ./
wazuh-1-key.pem ./root-ca.pem

mv -n /etc/filebeat/certs/wazuh-1.pem /etc/filebeat/certs/filebeat.pem

mv -n /etc/filebeat/certs/wazuh-1-key.pem /etc/filebeat/certs/filebeat-
key.pem

chmod 500 /etc/filebeat/certs

chmod 400 /etc/filebeat/certs/*

chown -R root:root /etc/filebeat/certs
```



```
ubuntu@ubuntu-VirtualBox:~$ sudo su
[sudo] password for ubuntu:
Sorry, try again.
[sudo] password for ubuntu:
root@ubuntu-VirtualBox:/home/ubuntu# cd /etc/filebeat/certs
root@ubuntu-VirtualBox:/etc/filebeat/certs# ls
admin-key.pem  admin.pem  filebeat-key.pem  filebeat.pem  root-ca.pem
root@ubuntu-VirtualBox:/etc/filebeat/certs# 
```

Starting the Wazuh manager

1) Starting the Wazuh manager:

```
systemctl daemon-reload

systemctl enable wazuh-manager

systemctl start wazuh-manager
```

2) Run the following command to verify the Wazuh manager status.

```
systemctl status wazuh-manager
```

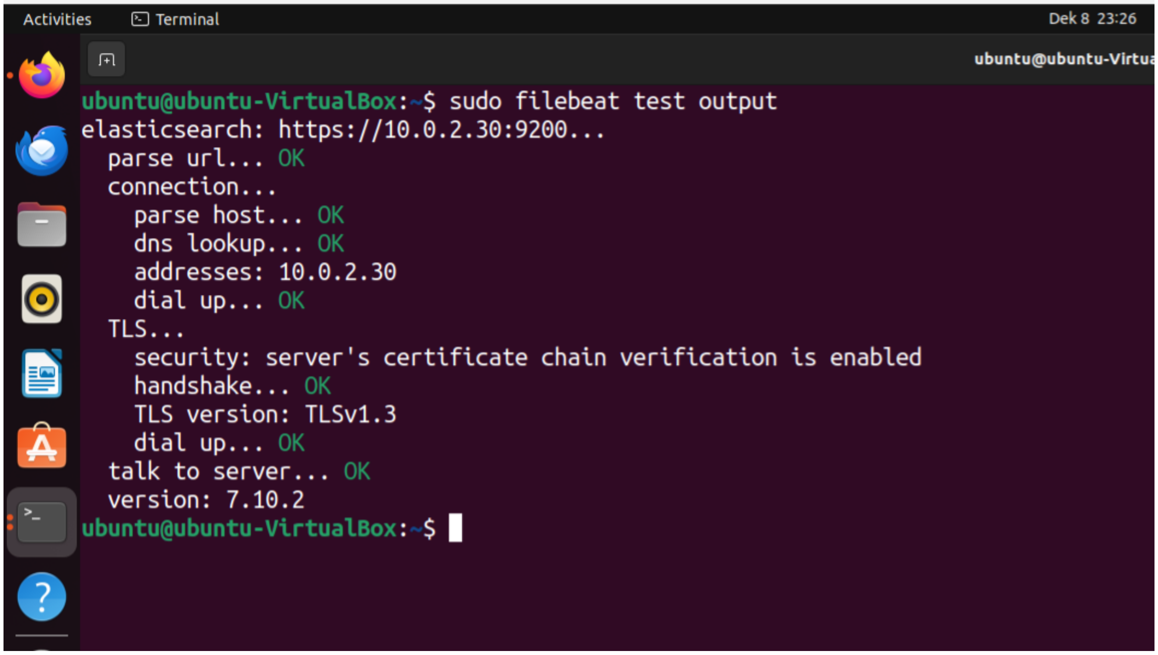
Starting the Filebeat service

1) Enable and start the Filebeat service

```
systemctl daemon-reload

systemctl enable filebeat

systemctl start filebeat
```

2) Run the following command to verify that Filebeat is successfully installed.

```
filebeat test output
```



```
ubuntu@ubuntu-VirtualBox:~$ sudo filebeat test output
elasticsearch: https://10.0.2.30:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 10.0.2.30
    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: 7.10.2
ubuntu@ubuntu-VirtualBox:~$
```

Wazuh dashboard installation

Install the following packages if missing

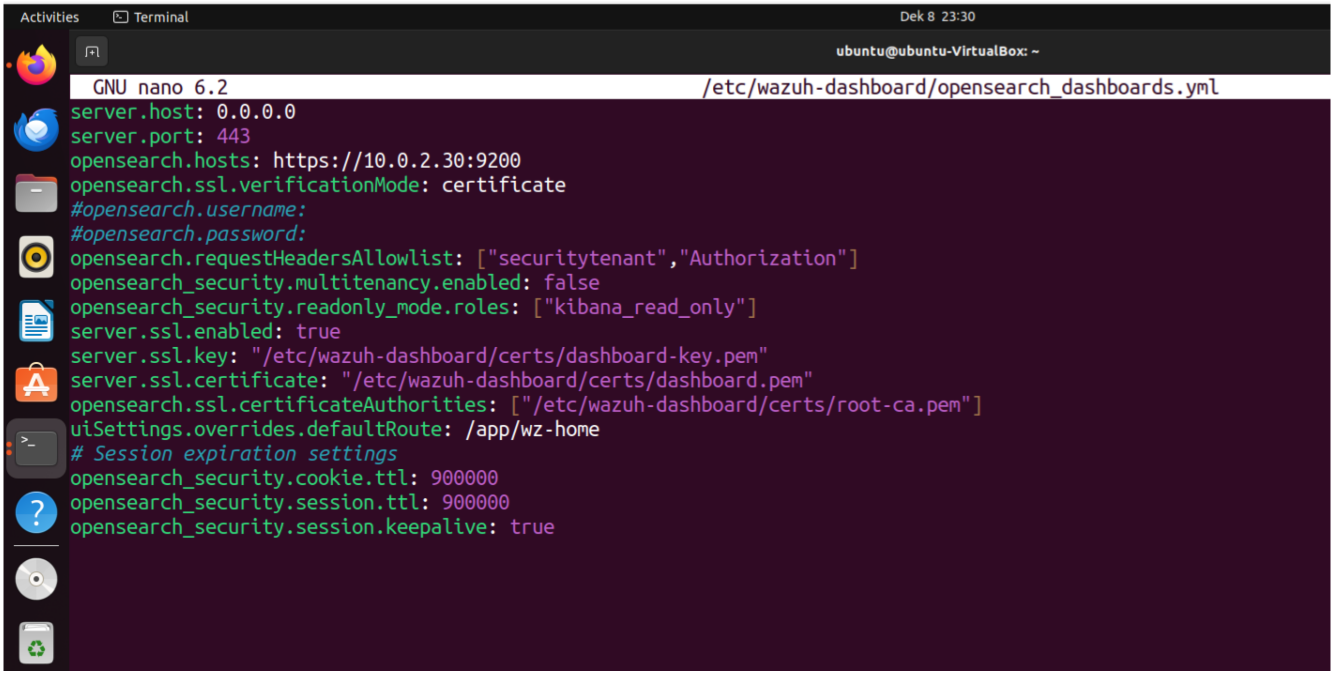
```
apt-get install debhelper tar curl libcap2-bin
```

Install the Wazuh dashboard package

```
apt-get -y install wazuh-dashboard
```

Configuring the Wazuh dashboard:

sudo nano /etc/wazuh-dashboard/opensearch_dashboards.yml



```
  GNU nano 6.2                                /etc/wazuh-dashboard/opensearch_dashboards.yml
server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://10.0.2.30:9200
opensearch.ssl.verificationMode: certificate
#opensearch.username:
#opensearch.password:
opensearch.requestHeadersAllowlist: ["securitytenant","Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wz-home
# Session expiration settings
opensearch_security.cookie.ttl: 900000
opensearch_security.session.ttl: 900000
opensearch_security.session.keepalive: true
```

Deploying certificates:

```
mkdir /etc/wazuh-dashboard/certs
```

```
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./wazuh-1.pem ./wazuh-1-key.pem ./root-ca.pem
```

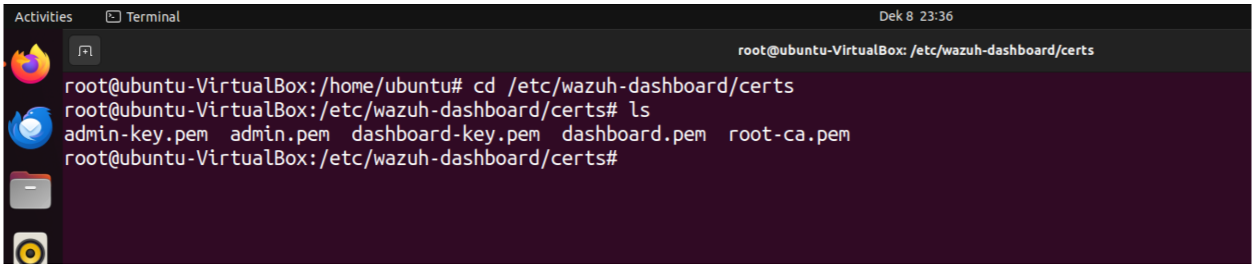
```
mv -n /etc/wazuh-dashboard/certs/wazuh-1.pem /etc/wazuh-dashboard/certs/dashboard.pem
```

```
mv -n /etc/wazuh-dashboard/certs/wazuh-1-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
```

```
chmod 500 /etc/wazuh-dashboard/certs
```

```
chmod 400 /etc/wazuh-dashboard/certs/*
```

```
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```



```
root@ubuntu-VirtualBox:/home/ubuntu# cd /etc/wazuh-dashboard/certs
root@ubuntu-VirtualBox:/etc/wazuh-dashboard/certs# ls
admin-key.pem  admin.pem  dashboard-key.pem  dashboard.pem  root-ca.pem
root@ubuntu-VirtualBox:/etc/wazuh-dashboard/certs#
```

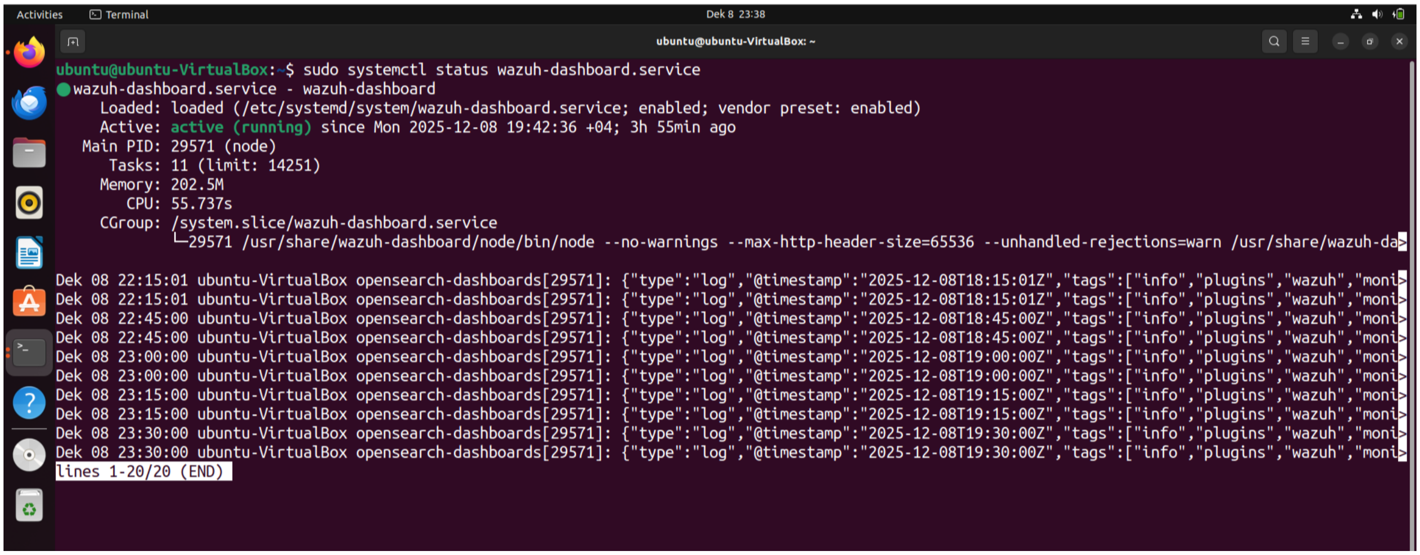
Starting the Wazuh dashboard service:

```
systemctl daemon-reload
```

```
systemctl enable wazuh-dashboard
```

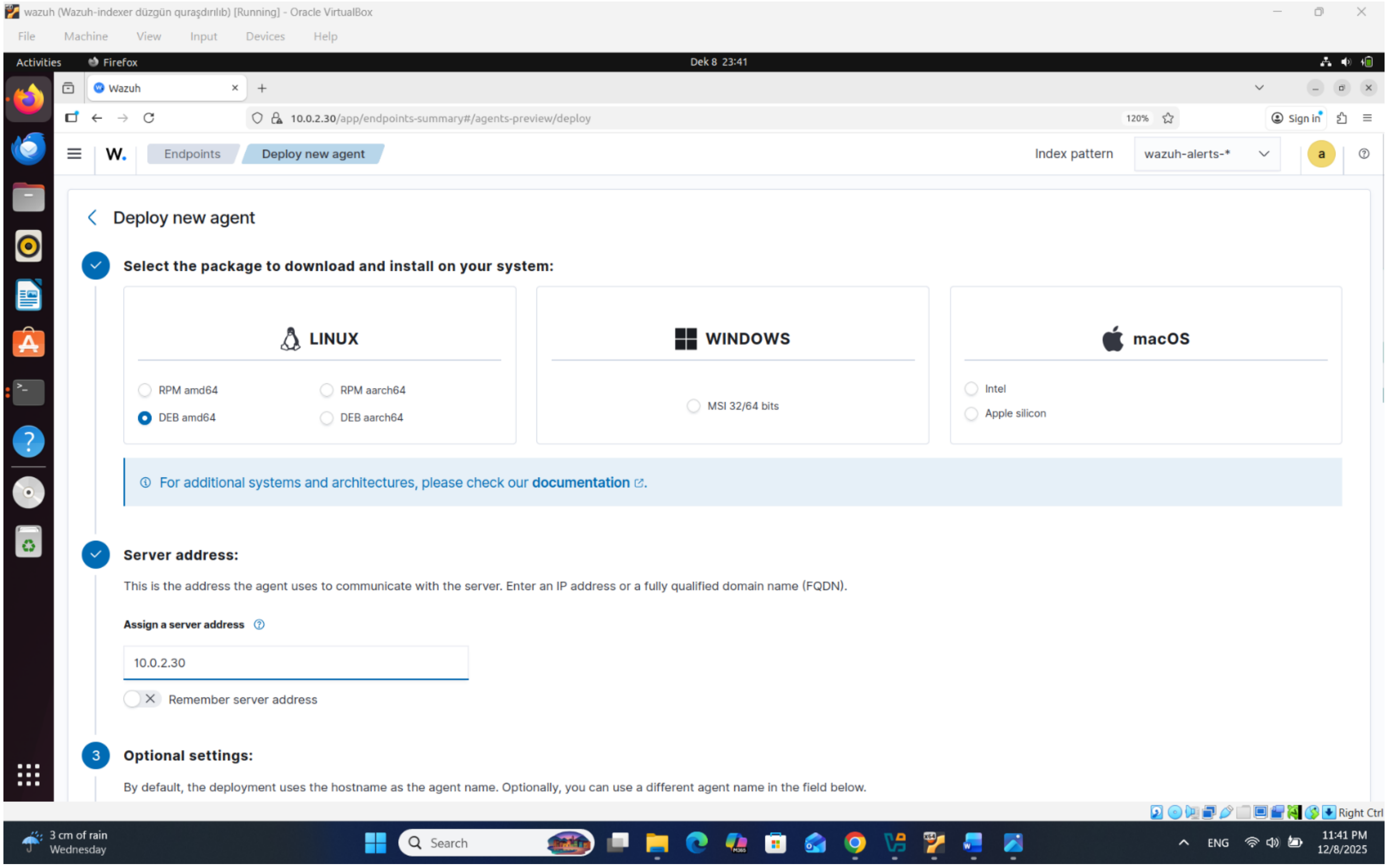
```
systemctl start wazuh-dashboard
```

```
systemctl status wazuh-dashboard
```



```
ubuntu@ubuntu-VirtualBox:~$ sudo systemctl status wazuh-dashboard.service
● wazuh-dashboard.service - wazuh-dashboard
     Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2025-12-08 19:42:36 +04; 3h 55min ago
   Main PID: 29571 (node)
      Tasks: 11 (limit: 14251)
     Memory: 202.5M
        CPU: 55.737s
     CGroup: /system.slice/wazuh-dashboard.service
             └─29571 /usr/share/wazuh-dashboard/node/bin/node --no-warnings --max-http-header-size=65536 --unhandled-rejections=warn /usr/share/wazuh-da>

Dek 08 22:15:01 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T18:15:01Z","tags":["info","plugins","wazuh","moni>
Dek 08 22:15:01 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T18:15:01Z","tags":["info","plugins","wazuh","moni>
Dek 08 22:45:00 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T18:45:00Z","tags":["info","plugins","wazuh","moni>
Dek 08 22:45:00 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T18:45:00Z","tags":["info","plugins","wazuh","moni>
Dek 08 23:00:00 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T19:00:00Z","tags":["info","plugins","wazuh","moni>
Dek 08 23:00:00 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T19:00:00Z","tags":["info","plugins","wazuh","moni>
Dek 08 23:15:00 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T19:15:00Z","tags":["info","plugins","wazuh","moni>
Dek 08 23:15:00 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T19:15:00Z","tags":["info","plugins","wazuh","moni>
Dek 08 23:30:00 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T19:30:00Z","tags":["info","plugins","wazuh","moni>
Dek 08 23:30:00 ubuntu-VirtualBox opensearch-dashboards[29571]: {"type":"log","@timestamp":"2025-12-08T19:30:00Z","tags":["info","plugins","wazuh","moni>
lines 1-20/20 (END)
```

Download agent to kali linux


wazuh (Wazuh-indexer düzgün quraşdırılıb) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Firefox Dek 8 23:41
Wazuh
10.0.2.30/app/endpoints-summary#/agents-preview/deploy
120%
Sign in
W.
Endpoints
Deploy new agent
Index pattern
wazuh-alerts-*
3 cm of rain
Wednesday
Search
ENG
11:41 PM
12/8/2025
Right Ctrl

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

10.0.2.30

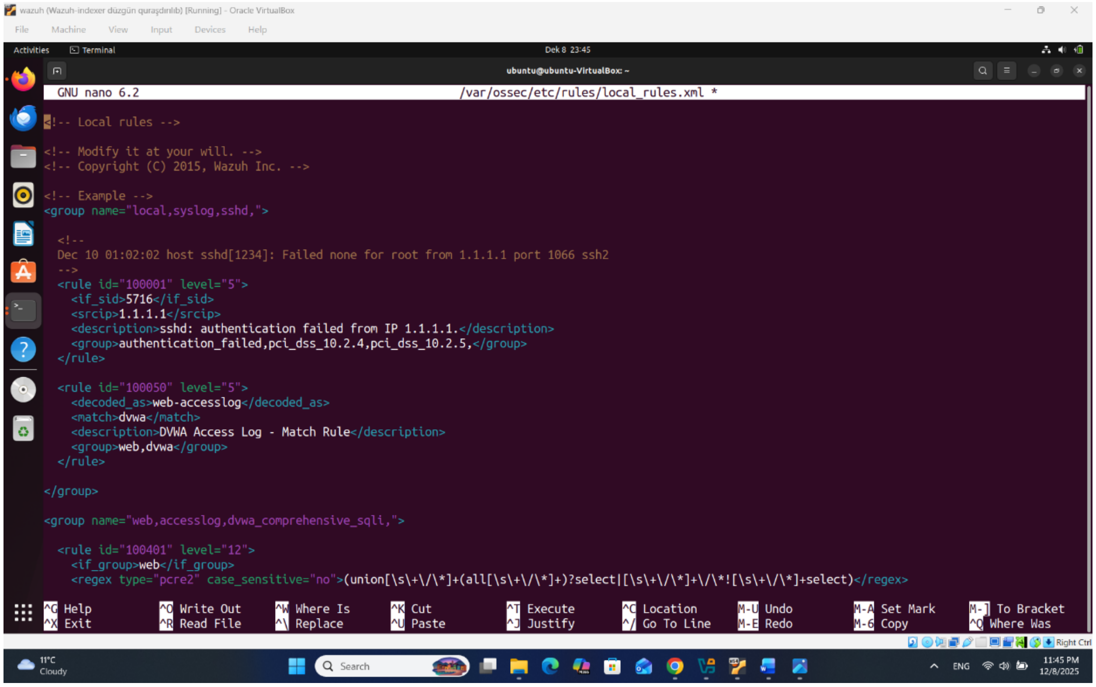
☒ Remember server address

3 **Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

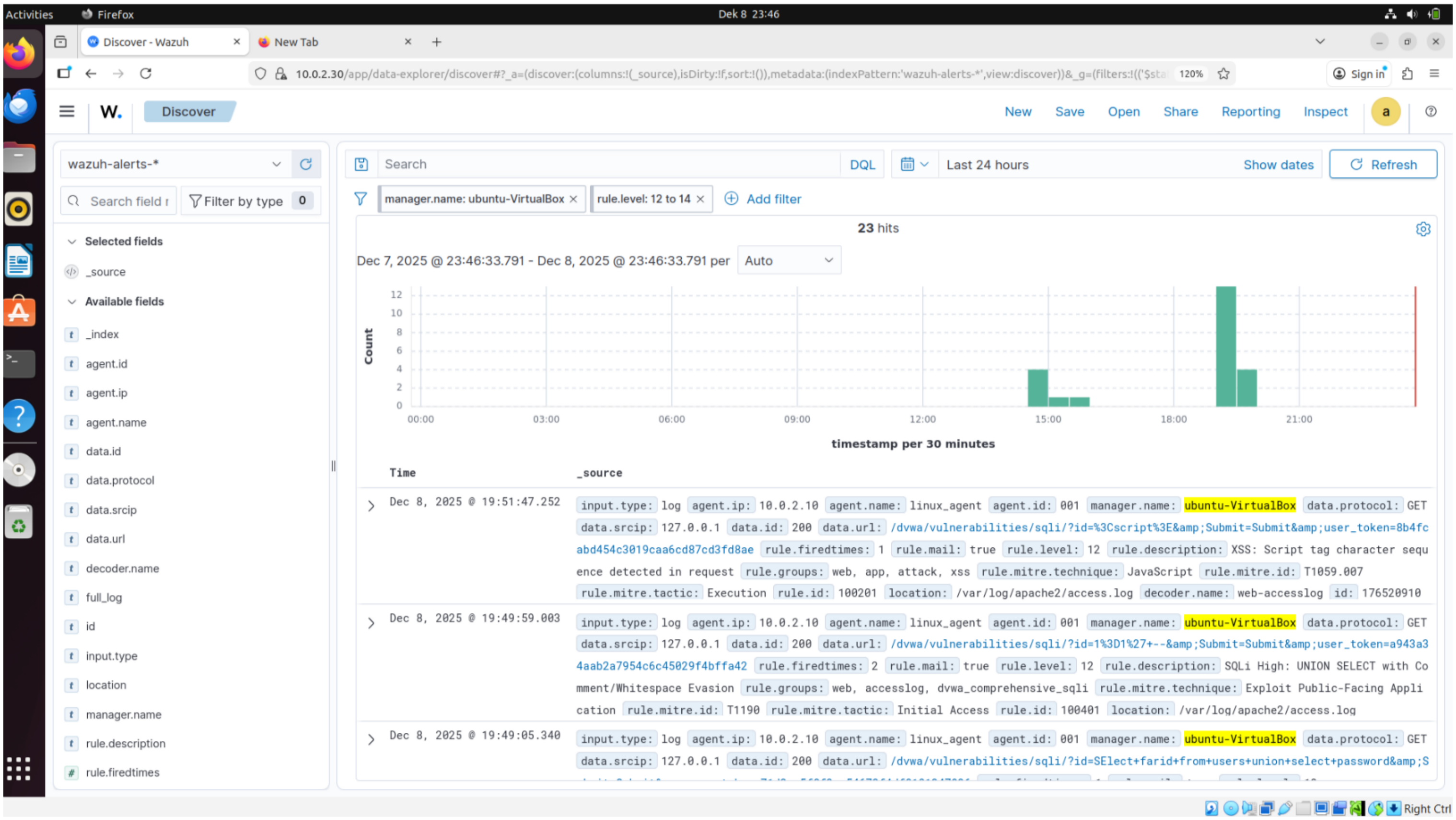
Rules for detection of attacks:

sudo nano /var/ossec/etc/rules/local_rules.xml


wazuh (Wazuh-indexer düzgün quraşdırılıb) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Activities Terminal Dek 8 23:45
ubuntu@ubuntu-VirtualBox: ~
11°C
Cloudy
Search
ENG
11:45 PM
12/8/2025
Right Ctrl

```
 GNU nano 6.2                                /var/ossec/etc/rules/local_rules.xml *

<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

  <rule id="100050" level="5">
    <decoded_as>web-accesslog</decoded_as>
    <match>dvwa</match>
    <description>DVWA Access Log - Match Rule</description>
    <group>web,dvwa</group>
  </rule>

</group>

<group name="web,accesslog,dvwa_comprehensive_sqli,">

  <rule id="100401" level="12">
    <if_group>web</if_group>
    <regex type="pcre2" case_sensitive="no">(union[\s\+\/\*]+(all[\s\+\/\*]+)?select|[\s\+\/\*]+\/\*![\s\+\/\*]+select)</regex>

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was
```

Result



manager.name: ubuntu-VirtualBox × rule.level: 12 to 14 ×

23 hits

Dec 7, 2025 @ 23:46:33.791 - Dec 8, 2025 @ 23:46:33.791 per Auto

```
Time                          _source
Dec 8, 2025 @ 19:51:47.252    input.type: log agent.ip: 10.0.2.10 agent.name: linux_agent agent.id: 001 manager.name: ubuntu-VirtualBox data.protocol: GET
                              data.srcip: 127.0.0.1 data.id: 200 data.url: /dvwa/vulnerabilities/sqli/?id=%3Cscript%3E&amp;Submit=Submit&amp;user_token=8b4fc
                              abd454c3019caa6cd87cd3fd8ae rule.firedtimes: 1 rule.mail: true rule.level: 12 rule.description: XSS: Script tag character sequ
                              ence detected in request rule.groups: web, app, attack, xss rule.mitre.technique: JavaScript rule.mitre.id: T1059.007
                              rule.mitre.tactic: Execution rule.id: 100201 location: /var/log/apache2/access.log decoder.name: web-accesslog id: 176520910
Dec 8, 2025 @ 19:49:59.003    input.type: log agent.ip: 10.0.2.10 agent.name: linux_agent agent.id: 001 manager.name: ubuntu-VirtualBox data.protocol: GET
                              data.srcip: 127.0.0.1 data.id: 200 data.url: /dvwa/vulnerabilities/sqli/?id=1%3D1%27+--&amp;Submit=Submit&amp;user_token=a943a3
                              4aab2a7954c6c45029f4bffa42 rule.firedtimes: 2 rule.mail: true rule.level: 12 rule.description: SQLi High: UNION SELECT with Co
                              mment/Whitespace Evasion rule.groups: web, accesslog, dvwa_comprehensive_sqli rule.mitre.technique: Exploit Public-Facing Appli
                              cation rule.mitre.id: T1190 rule.mitre.tactic: Initial Access rule.id: 100401 location: /var/log/apache2/access.log
Dec 8, 2025 @ 19:49:05.340    input.type: log agent.ip: 10.0.2.10 agent.name: linux_agent agent.id: 001 manager.name: ubuntu-VirtualBox data.protocol: GET
                              data.srcip: 127.0.0.1 data.id: 200 data.url: /dvwa/vulnerabilities/sqli/?id=SElect+farid+from+users+union+select+password&amp;S
```