WAZUH

Report by: VIGNESH K.J

Abstract

Wazuh is an open-source security platform designed for threat detection, compliance monitoring, and incident response. This project focuses on the deployment of a full Wazuh setup to provide centralized security management across multiple systems. The implementation involves installing the Wazuh Manager, Indexer, and Dashboard to enable seamless monitoring and analysis of security events. Pre-installation requirements, including system specifications, software dependencies, and network configurations, were fulfilled to ensure a smooth deployment. The setup was tested to verify functionality, demonstrating its effectiveness in providing realtime security insights, compliance reporting, and streamlined incident response capabilities. This documentation outlines the installation process, configuration steps, and the overall objectives of deploying Wazuh as a robust security monitoring solution.

Acknowledgment

I would like to sincerely thank my trainer, Alex, and the entire team at the institute for their continuous support and guidance throughout this project. Their expertise and encouragement were crucial in helping me understand the process of installing and configuring Wazuh on Ubuntu. Alex’s mentorship has significantly improved my technical skills and has motivated me to approach challenges more effectively.

I would also like to thank my peers for their cooperation and teamwork, which made this project more enjoyable. The discussions we had helped me refine my ideas and improve this report.

Additionally, I am grateful for the various resources—tutorials, documentation, and online articles—that helped me gain a deeper understanding of the topic and complete this project successfully.

Lastly, I appreciate the support and contributions from everyone involved. This project would not have been possible without them.

TABLE OF CONTENT

INTRODUCTION

In today's fast-changing cybersecurity environment, organizations are exposed to a growing number of threats against their IT infrastructure. The security and compliance of the organization can be ensured only by real-time threat detection and effective monitoring and management of system logs. Wazuh is an open-source security platform that integrates log management, intrusion detection, and compliance monitoring into a single framework for solving these challenges.

This project emphasizes the installation and configuration of Wazuh for setting up a centralized security monitoring system. The core for Wazuh is a server where all data coming from agents on monitored endpoints are accumulated. These agents examine activity in the systems, report any potential vulnerabilities, and forward logs to the server for further analysis. A very intuitive interface is available to handle alerts, monitor system status, and view security data, powered by the Kibana dashboard for Wazuh.

This project aims to enhance the security posture of IT systems, simplify compliance with regulatory standards, and provide an efficient way to manage and mitigate potential threats in realtime, while implementing Wazuh.

OBJECTIVES

The main objectives of this project are:

Install Wazuh Server and Components:

Installation of the Wazuh server with necessary components like Elasticsearch and Kibana to allow easy log management, data storage, and visualization.

Configure Wazuh Agents:

Install and configure Wazuh agents on monitored systems such as endpoints and servers, gathering security logs and system events for centralized monitoring.

Integrate Elasticsearch and Kibana:

Set up Elasticsearch for data storage, indexing, and searching purposes and Kibana to visualize and manage the dashboard for Wazuh.

Create Secure Communication:

Establish the secure and reliable communication in order to collect and analyze data in real-time between Wazuh server, agent and dashboard.

Test the System:

Test the system, either by simulating the occurrence of security events or analyze the system logs, ensure that Wazuh could detect and report incidents from its dashboard.

Offer Real-Time Threat Detection and Monitoring

Allow for the real-time monitoring of IT systems in order to identify and analyze threats, with rapid response capabilities that would be developed, improving overall security posture.

Ensure Compliance:

Utilize Wazuh to monitor compliance with the security regulations such as GDPR, PCI-DSS through the monitoring of logs that are relevant to those reports.

This project shall successfully implement a fully functional Wazuh-based security monitoring system enhancing organizational security while providing an effective capability to detect threats and manage compliance.

PRE-INSTALLATION REQUIRMENTS

Before proceeding with the Wazuh full setup installation, ensure the following pre-installation requirements are met to guarantee a successful deployment :

1. **System Requirements**:

- Processor: Multi-core processor (2 GHz or higher recommended).
- Memory (RAM): Minimum 4 GB, recommended 8-16 GB for larger environments.
- Storage: At least 20 GB free disk space, with SSD recommended for better performance.
- Network: Reliable connectivity to facilitate agent-server communication.

2. **Operating System Compatibility**:

   Supported operating systems include
   Linux (Ubuntu 20.04/22.04, Debian 10/11, CentOS 7/8, RHEL 7/8), Windows (Windows 10/Server 2016/2019/2022 for agents), and macOS (10.15 or later for agents). Ensure the OS is updated with the latest patches.

3. **Software Dependencies**

   Wazuh Indexer and Manager: Java (version 11 or later), curl, wget, unzip, tar, and GCC compiler if building from source.

   Wazuh Web Interface: Node.js (latest stable version) and a web server such as Nginx or Apache for reverse proxy setup.

4. **Repository Configuration**:

   Add the Wazuh repository and update the system package manager.

5.Time Synchronization:

Use NTP or similar services to synchronize time across systems.

6. User Privileges:

Administrative (root or sudo) privileges are required on all systems.

7.**Scalability Planning**:

Plan deployment as per the scale: single-node or distributed setup.

PROCEDURE

Installing and configuring the Wazuh stack (Indexer, Server, and Dashboard) step by step:

1. Certificates Creation Generate SSL Certificates

1. Download the wazuh-certs-tool.sh and config.yml files:

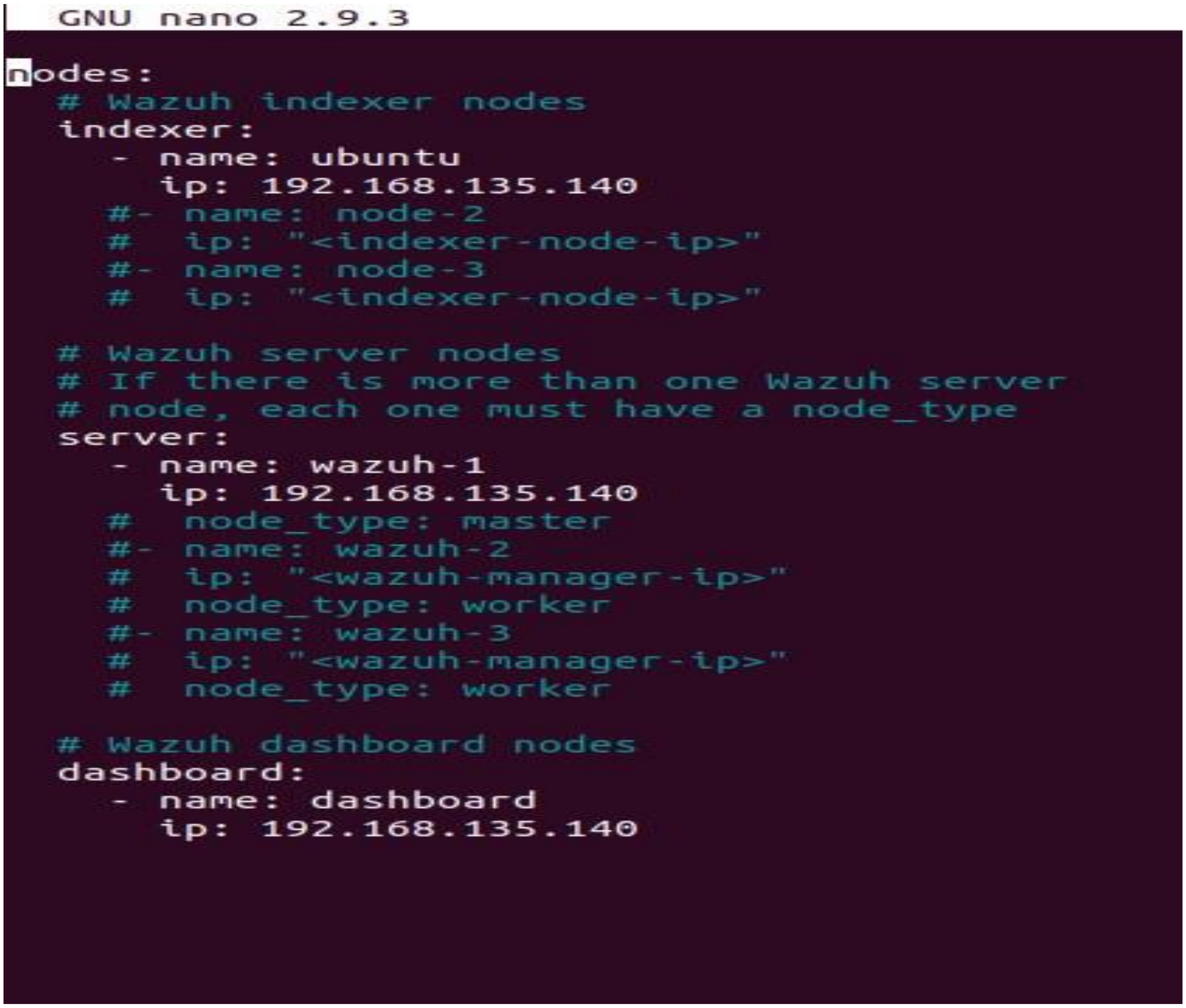
bash Copy code

```
curl -sO https://packages.wazuh.com/4.9/wazuh-certs-tool.sh

curl -sO https://packages.wazuh.com/4.9/config.yml
```

1. 2. Edit config.yml to specify node names and IP addresses:

yaml



```
  GNU nano 2.9.3

nodes:
  # Wazuh indexer nodes
  indexer:
    - name: ubuntu
      ip: 192.168.135.140
    #- 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: 192.168.135.140
    #  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: 192.168.135.140
```

2. Run the certificate creation tool:

bash Copy

code

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

3. Compress the certificates:

bash Copy code tar -cvf ./wazuh-certificates.tar -C

./wazuh-certificates/ .

rm -rf ./wazuh-certificates

2. Wazuh Indexer Installation

Install Dependencies Copy

code

apt-get install debconf adduser procpsAdd Wazuh Repository

Install Wazuh Indexer

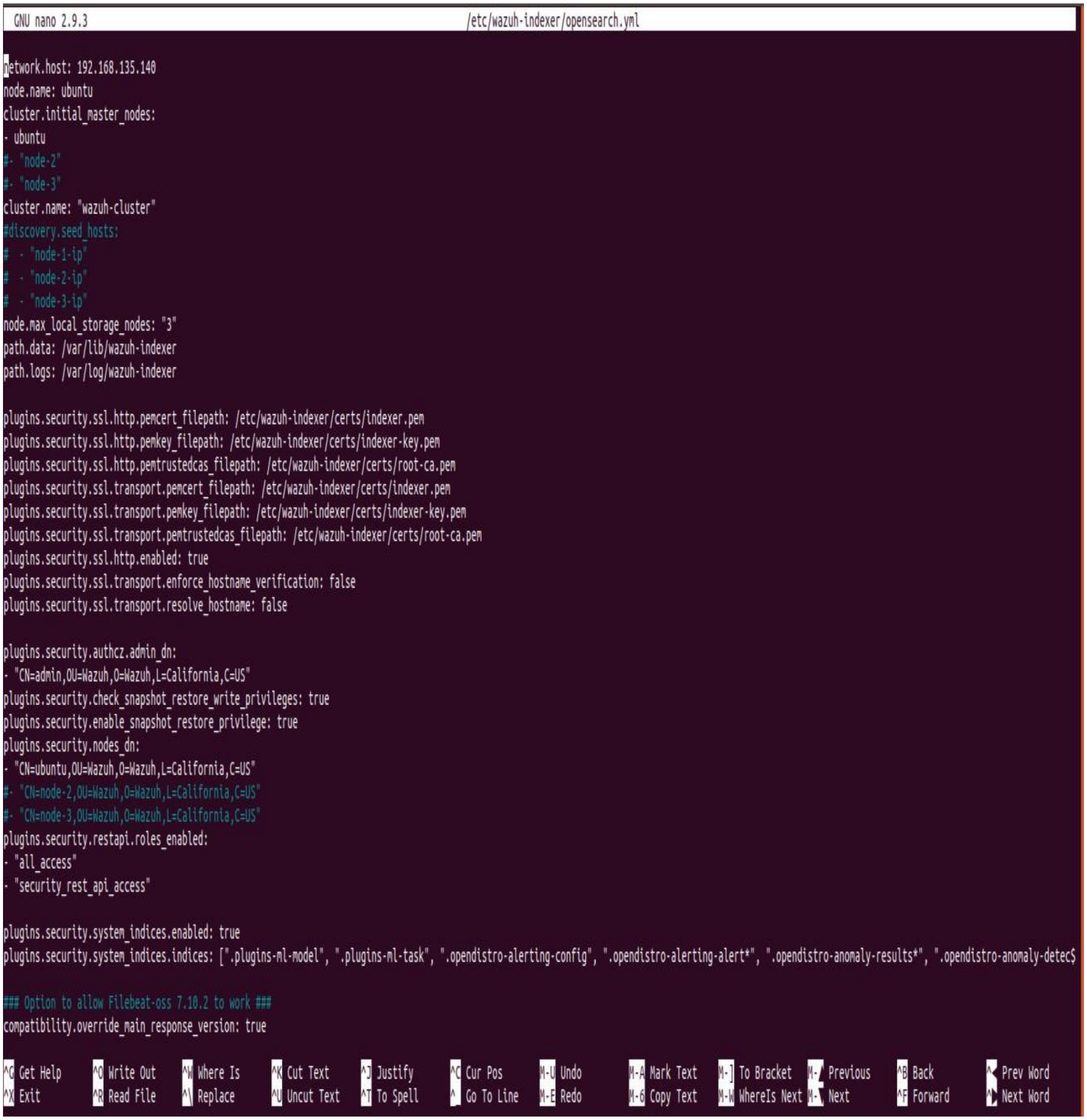
1. Install the package: Copy

code

apt-get -y install wazuh-indexerConfigure the Indexer

1. Edit /etc/wazuh-indexer/opensearch.yml:
   - Set network.host to the node IP.
   - Set node.name to the node name defined in config.yml.

- For multi-node, set cluster.initial_master_nodes and discovery.seed_hosts.



```
network.host: 192.168.135.140
node.name: ubuntu
cluster.initial_master_nodes:
- ubuntu
#- "node-2"
#- "node-3"
cluster.name: "wazuh-cluster"
#discovery.seed_hosts:
#  - "node-1-ip"
#  - "node-2-ip"
#  - "node-3-ip"
node.max_local_storage_nodes: "3"
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer

plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.http.enabled: true
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.transport.resolve_hostname: false

plugins.security.authcz.admin_dn:
- "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.check_snapshot_restore_write_privileges: true
plugins.security.enable_snapshot_restore_privilege: true
plugins.security.nodes_dn:
- "CN=ubuntu,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-2,OU=Wazuh,O=Wazuh,L=California,C=US"
#- "CN=node-3,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.restapi.roles_enabled:
- "all_access"
- "security_rest_api_access"

plugins.security.system_indices.enabled: true
plugins.security.system_indices.indices: [".plugins-ml-model", ".plugins-ml-task", ".opendistro-alerting-config", ".opendistro-alerting-alert*", ".opendistro-anomaly-results*", ".opendistro-anomaly-detec$

### Option to allow Filebeat-oss 7.10.2 to work ###
compatibility.override_main_response_version: true
```

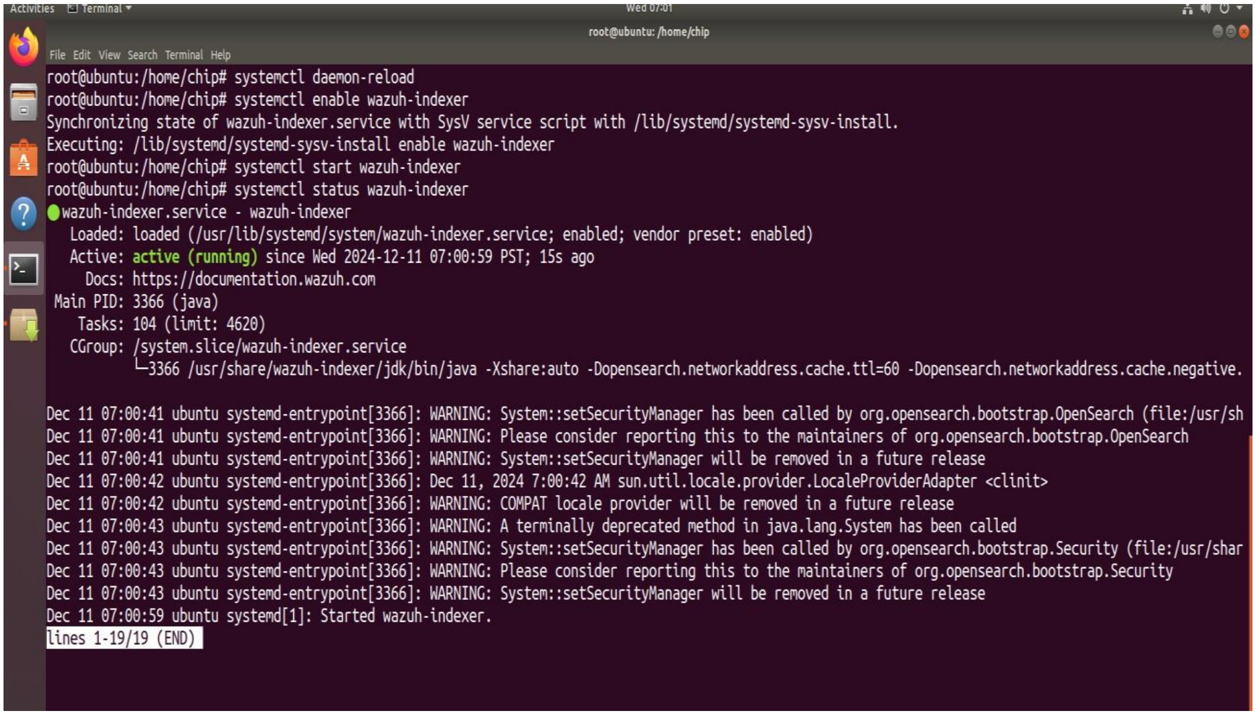
2. Deploy certificates:

Copy code

```
NODE_NAME=<indexer-node-name> mkdir
/etc/wazuh-indexer/certs
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/
./$NODE_NAME.pem ./$NODE_NAME-key.pem ./admin.pem
./admin-key.pem ./root-ca.pem
mv -n /etc/wazuh-indexer/certs/$NODE_NAME.pem
/etc/wazuh-indexer/certs/indexer.pem
mv -n /etc/wazuh-indexer/certs/$NODE_NAME-key.pem
/etc/wazuh-indexer/certs/indexer-key.pem chmod
500 /etc/wazuh-indexer/certs chmod 400
/etc/wazuh-indexer/certs/* chown -R wazuh-
indexer:wazuh-indexer /etc/wazuhindexer/certs
```

3. Start the service: Copy

```
code systemctl daemon-reload
systemctl enable wazuh-indexer
systemctl start wazuh-indexer
```



```
root@ubuntu:/home/chip# systemctl daemon-reload
root@ubuntu:/home/chip# systemctl enable wazuh-indexer
Synchronizing state of wazuh-indexer.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-indexer
root@ubuntu:/home/chip# systemctl start wazuh-indexer
root@ubuntu:/home/chip# systemctl status wazuh-indexer
●wazuh-indexer.service - wazuh-indexer
   Loaded: loaded (/usr/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-12-11 07:00:59 PST; 15s ago
     Docs: https://documentation.wazuh.com
 Main PID: 3366 (java)
    Tasks: 104 (limit: 4620)
   CGroup: /system.slice/wazuh-indexer.service
           └─3366 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.negative.

Dec 11 07:00:41 ubuntu systemd-entrypoint[3366]: WARNING: System::setSecurityManager has been called by org.opensearch.bootstrap.OpenSearch (file:/usr/sh
Dec 11 07:00:41 ubuntu systemd-entrypoint[3366]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap.OpenSearch
Dec 11 07:00:41 ubuntu systemd-entrypoint[3366]: WARNING: System::setSecurityManager will be removed in a future release
Dec 11 07:00:42 ubuntu systemd-entrypoint[3366]: Dec 11, 2024 7:00:42 AM sun.util.locale.provider.LocaleProviderAdapter <clinit>
Dec 11 07:00:42 ubuntu systemd-entrypoint[3366]: WARNING: COMPAT locale provider will be removed in a future release
Dec 11 07:00:43 ubuntu systemd-entrypoint[3366]: WARNING: A terminally deprecated method in java.lang.System has been called
Dec 11 07:00:43 ubuntu systemd-entrypoint[3366]: WARNING: System::setSecurityManager has been called by org.opensearch.bootstrap.Security (file:/usr/shar
Dec 11 07:00:43 ubuntu systemd-entrypoint[3366]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap.Security
Dec 11 07:00:43 ubuntu systemd-entrypoint[3366]: WARNING: System::setSecurityManager will be removed in a future release
Dec 11 07:00:59 ubuntu systemd[1]: Started wazuh-indexer.
lines 1-19/19 (END)
```

Cluster Initialization

1. Run the security initialization script:

Copy code

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

2. Test the installation: Copy code

curl -k -u admin:admin https://<indexer-ip>:9200

curl -k -u admin:admin https://<indexer-ip>:9200/_cat/nodes?v

3. Wazuh Server Installation Install Packages

1. Install the manager and Filebeat:

Copy code

```
apt -y install wazuh-manager apt
-y install filebeat
```

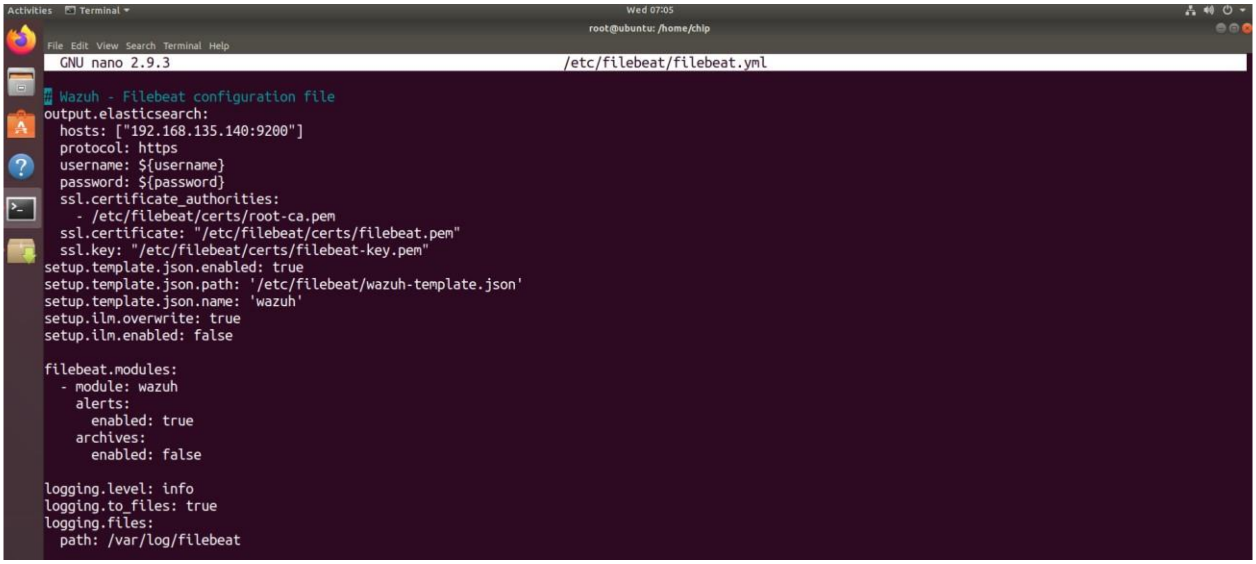
Configure Filebeat

1. Download the pre-configured filebeat.yml: Copy

code

```
curl -so /etc/filebeat/filebeat.yml
https://packages.wazuh.com/4.9/tpl/wazuh/filebeat/filebeat.y
ml
```

2. Update the hosts field with the Indexer IP(s).



```
  GNU nano 2.9.3                                    /etc/filebeat/filebeat.yml

# Wazuh - Filebeat configuration file
output.elasticsearch:
  hosts: ["192.168.135.140:9200"]
  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: false

logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
```

3. Secure credentials in the keystore: Copy code

```
filebeat keystore create
echo admin | filebeat keystore add username --stdin --force
echo admin | filebeat keystore add password --stdin –force
```

4. Deploy certificates for Filebeat:

Copy code

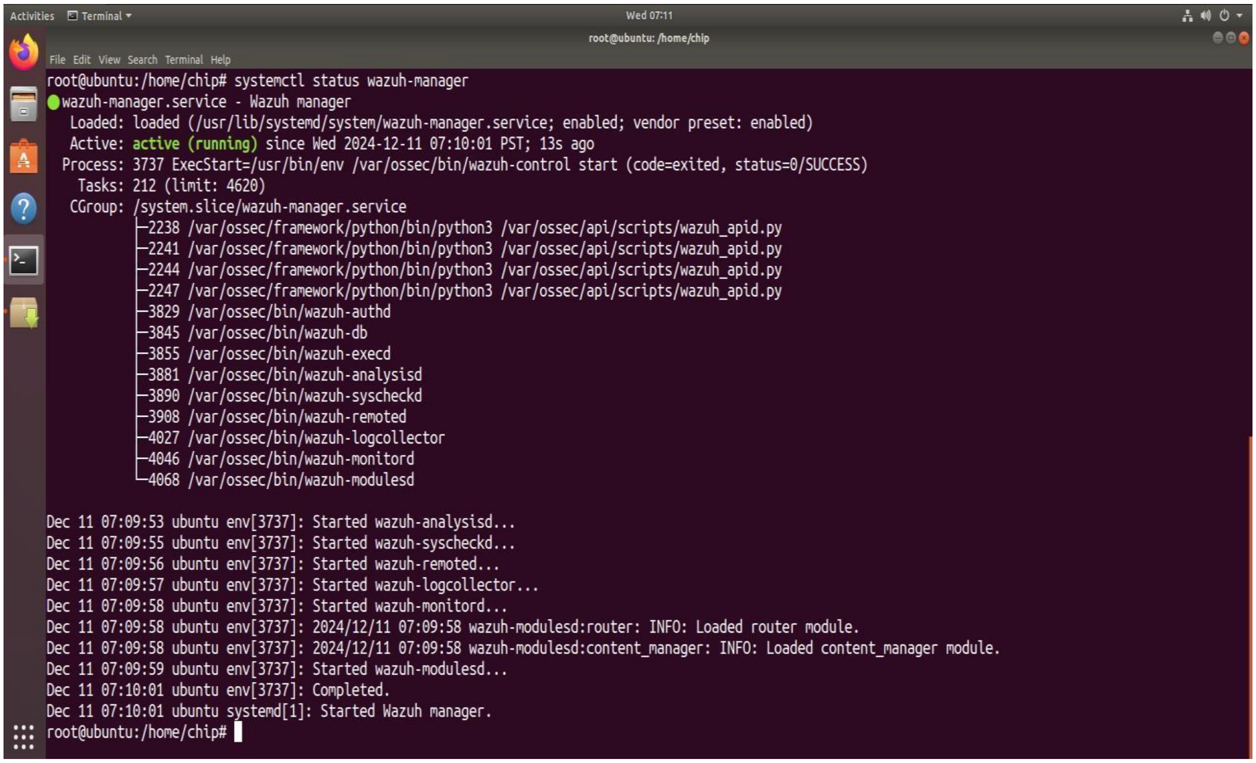
```
NODE_NAME=<server-node-name>
mkdir /etc/filebeat/certs
tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem
mv -n /etc/filebeat/certs/$NODE_NAME.pem /etc/filebeat/certs/filebeat.pem
mv -n /etc/filebeat/certs/$NODE_NAME-key.pem /etc/filebeat/certs/filebeat-key.pem
chmod 500 /etc/filebeat/certs chmod
400 /etc/filebeat/certs/* chown -R
root:root /etc/filebeat/certs
```

Start Services

1. Start the Wazuh

manager: Copy code

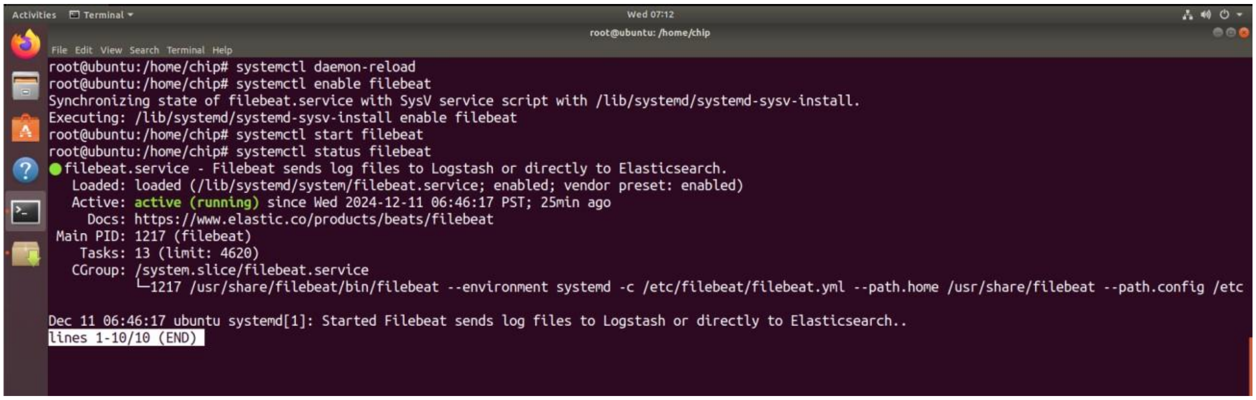
```
systemctl daemon-reload
systemctl enable wazuh-
manager systemctl start
wazuh-manager
```



```
root@ubuntu:/home/chip# systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-12-11 07:10:01 PST; 13s ago
  Process: 3737 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
    Tasks: 212 (limit: 4620)
   CGroup: /system.slice/wazuh-manager.service
           ├─2238 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
           ├─2241 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
           ├─2244 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
           ├─2247 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
           ├─3829 /var/ossec/bin/wazuh-authd
           ├─3845 /var/ossec/bin/wazuh-db
           ├─3855 /var/ossec/bin/wazuh-execd
           ├─3881 /var/ossec/bin/wazuh-analysisd
           ├─3890 /var/ossec/bin/wazuh-syscheckd
           ├─3908 /var/ossec/bin/wazuh-remoted
           ├─4027 /var/ossec/bin/wazuh-logcollector
           ├─4046 /var/ossec/bin/wazuh-monitord
           └─4068 /var/ossec/bin/wazuh-modulesd

Dec 11 07:09:53 ubuntu env[3737]: Started wazuh-analysisd...
Dec 11 07:09:55 ubuntu env[3737]: Started wazuh-syscheckd...
Dec 11 07:09:56 ubuntu env[3737]: Started wazuh-remoted...
Dec 11 07:09:57 ubuntu env[3737]: Started wazuh-logcollector...
Dec 11 07:09:58 ubuntu env[3737]: Started wazuh-monitord...
Dec 11 07:09:58 ubuntu env[3737]: 2024/12/11 07:09:58 wazuh-modulesd:router: INFO: Loaded router module.
Dec 11 07:09:58 ubuntu env[3737]: 2024/12/11 07:09:58 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Dec 11 07:09:59 ubuntu env[3737]: Started wazuh-modulesd...
Dec 11 07:10:01 ubuntu env[3737]: Completed.
Dec 11 07:10:01 ubuntu systemd[1]: Started Wazuh manager.
root@ubuntu:/home/chip#
```

2. Start Filebeat: Copy code systemctl daemon-reload systemctl enable filebeat systemctl start filebeat



```
root@ubuntu:/home/chip# systemctl daemon-reload
root@ubuntu:/home/chip# systemctl enable filebeat
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
root@ubuntu:/home/chip# systemctl start filebeat
root@ubuntu:/home/chip# systemctl status filebeat
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
   Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-12-11 06:46:17 PST; 25min ago
     Docs: https://www.elastic.co/products/beats/filebeat
 Main PID: 1217 (filebeat)
    Tasks: 13 (limit: 4620)
   CGroup: /system.slice/filebeat.service
           └─1217 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home /usr/share/filebeat --path.config /etc

Dec 11 06:46:17 ubuntu systemd[1]: Started Filebeat sends log files to Logstash or directly to Elasticsearch..
lines 1-10/10 (END)
```

4. Wazuh Dashboard Installation Install Dashboard

1. Install the package: Copy

code

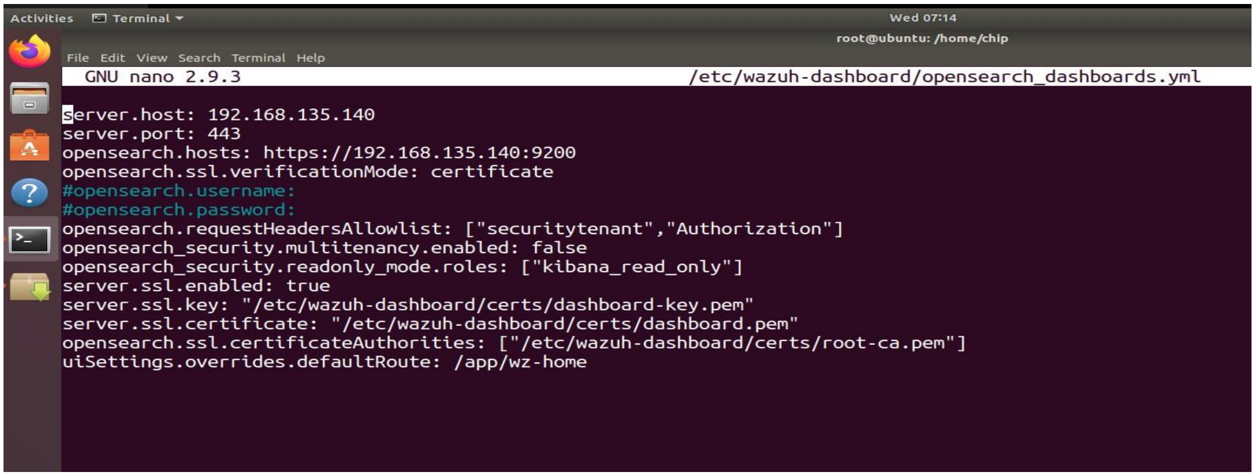
apt -y install wazuh-dashboard

Configure the Dashboard

1. Edit /etc/wazuh-dashboard/opensearch_dashboards.yml:

    ○ Set server.host to 0.0.0.0. ○ Configure

    opensearch.hosts with Indexer IPs.


Activities
Terminal ▾
Wed 07:14
root@ubuntu: /home/chip
File Edit View Search Terminal Help
GNU nano 2.9.3
/etc/wazuh-dashboard/opensearch_dashboards.yml

```
server.host: 192.168.135.140
server.port: 443
opensearch.hosts: https://192.168.135.140:9200
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
```

2. Deploy certificates for the Dashboard:

Copy code

NODE_NAME=<dashboard-node-name> mkdir

/etc/wazuh-dashboard/certs

tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/

./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem mv -n /etc/wazuh-dashboard/certs/$NODE_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem

mv -n /etc/wazuh-dashboard/certs/$NODE_NAME-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/wazuhdashboard/certs

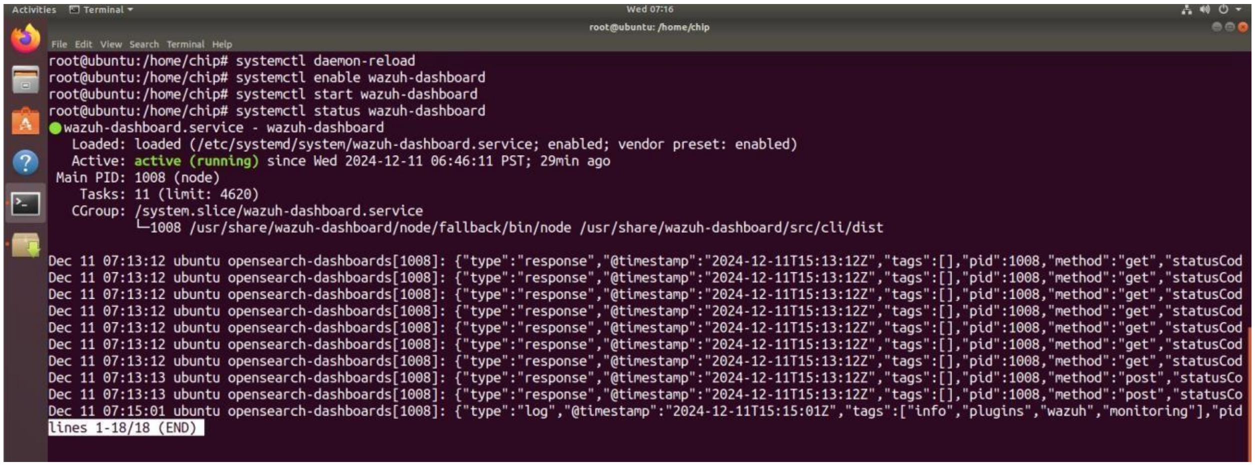
3. Start the Dashboard service:

Copy code systemctl daemon-

reload systemctl enable wazuh-

dashboard systemctl start wazuh-

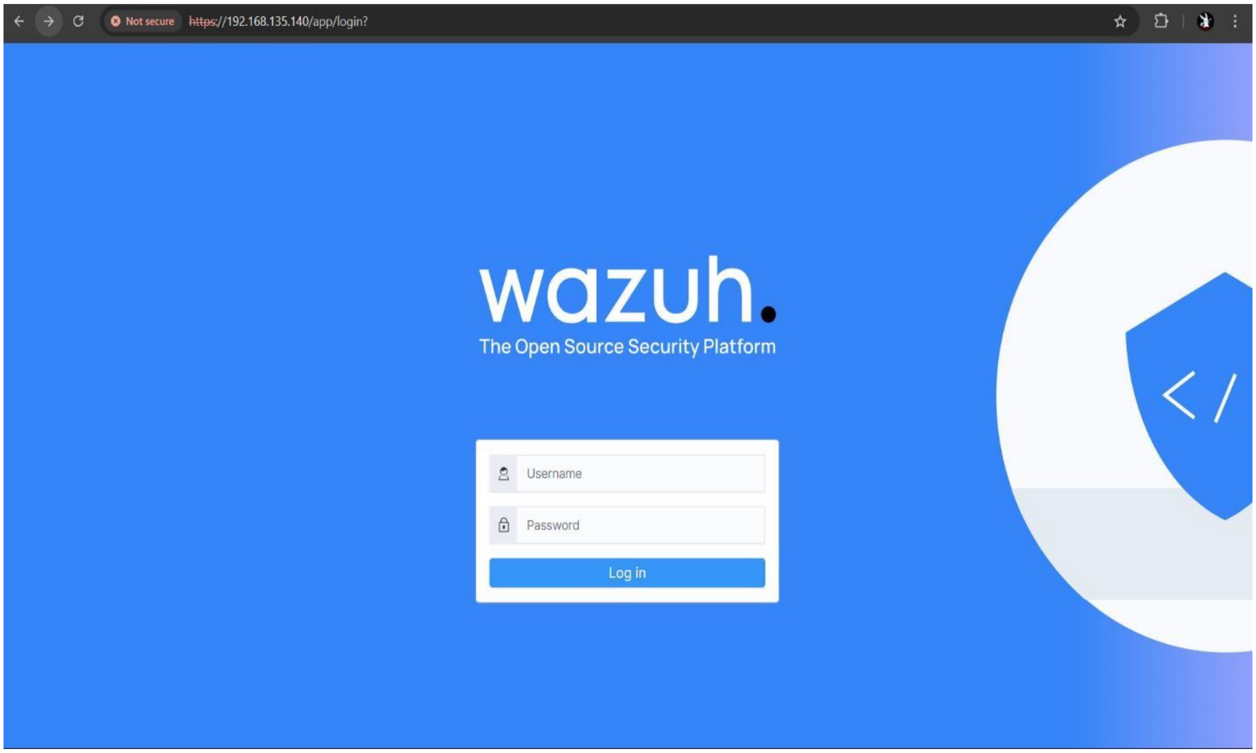
dashboard

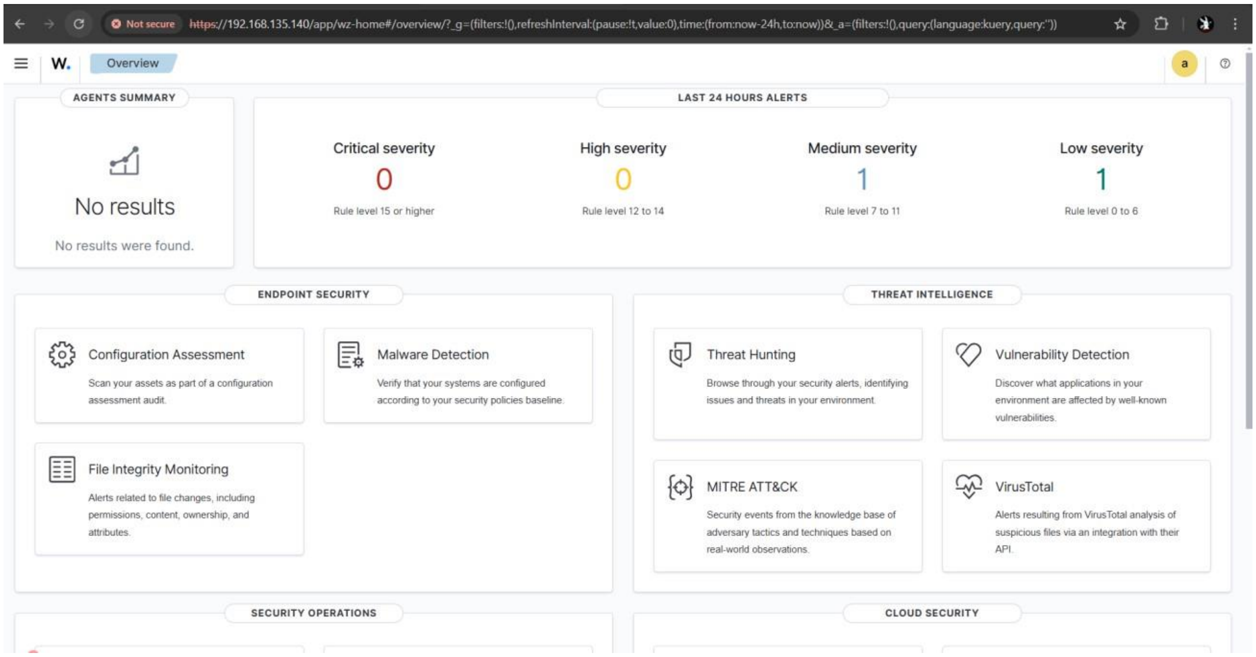


```
root@ubuntu:/home/chip# systemctl daemon-reload
root@ubuntu:/home/chip# systemctl enable wazuh-dashboard
root@ubuntu:/home/chip# systemctl start wazuh-dashboard
root@ubuntu:/home/chip# systemctl status wazuh-dashboard
●wazuh-dashboard.service - wazuh-dashboard
   Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-12-11 06:46:11 PST; 29min ago
 Main PID: 1008 (node)
    Tasks: 11 (limit: 4620)
   CGroup: /system.slice/wazuh-dashboard.service
           └─1008 /usr/share/wazuh-dashboard/node/fallback/bin/node /usr/share/wazuh-dashboard/src/cli/dist

Dec 11 07:13:12 ubuntu opensearch-dashboards[1008]: {"type":"response","@timestamp":"2024-12-11T15:13:12Z","tags":[],"pid":1008,"method":"get","statusCod
Dec 11 07:13:12 ubuntu opensearch-dashboards[1008]: {"type":"response","@timestamp":"2024-12-11T15:13:12Z","tags":[],"pid":1008,"method":"get","statusCod
Dec 11 07:13:12 ubuntu opensearch-dashboards[1008]: {"type":"response","@timestamp":"2024-12-11T15:13:12Z","tags":[],"pid":1008,"method":"get","statusCod
Dec 11 07:13:12 ubuntu opensearch-dashboards[1008]: {"type":"response","@timestamp":"2024-12-11T15:13:12Z","tags":[],"pid":1008,"method":"get","statusCod
Dec 11 07:13:12 ubuntu opensearch-dashboards[1008]: {"type":"response","@timestamp":"2024-12-11T15:13:12Z","tags":[],"pid":1008,"method":"get","statusCod
Dec 11 07:13:12 ubuntu opensearch-dashboards[1008]: {"type":"response","@timestamp":"2024-12-11T15:13:12Z","tags":[],"pid":1008,"method":"get","statusCod
Dec 11 07:13:12 ubuntu opensearch-dashboards[1008]: {"type":"response","@timestamp":"2024-12-11T15:13:12Z","tags":[],"pid":1008,"method":"get","statusCod
Dec 11 07:13:13 ubuntu opensearch-dashboards[1008]: {"type":"response","@timestamp":"2024-12-11T15:13:12Z","tags":[],"pid":1008,"method":"post","statusCo
Dec 11 07:13:13 ubuntu opensearch-dashboards[1008]: {"type":"response","@timestamp":"2024-12-11T15:13:12Z","tags":[],"pid":1008,"method":"post","statusCo
Dec 11 07:15:01 ubuntu opensearch-dashboards[1008]: {"type":"log","@timestamp":"2024-12-11T15:15:01Z","tags":["info","plugins","wazuh","monitoring"],"pid
lines 1-18/18 (END)
```

Now, you can access the Wazuh Dashboard through the browser using https://<dashboard-ip>.


Not secure
https://192.168.135.140/app/login?
wazuh.
The Open Source Security Platform
Username
Password
Log in



https://192.168.135.140/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(filters:!(),query:(language:kuery,query:''))

AGENTS SUMMARY

No results

No results were found.

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	1	1
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
Verify that your systems are configured according to your security policies baseline.

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
Security events from the knowledge base of adversary tactics and techniques based on real-world observations.

VirusTotal
Alerts resulting from VirusTotal analysis of suspicious files via an integration with their API.

SECURITY OPERATIONS

CLOUD SECURITY

CONCLUSION

The Wazuh full setup installation provides a centralized security monitoring system, enabling efficient threat detection and incident response. The successful deployment of Wazuh ensures enhanced security compliance and operational insights, proving its value in diverse IT environments.

APPENDIX

Configuration Files

- /var/ossec/etc/ossec.conf: Main configuration file for the Wazuh Manager.
- /etc/elasticsearch/elasticsearch.yml: Configuration file for the Wazuh Indexer.

Useful Commands

- Restarting Wazuh Manager:

```
sudo systemctl restart wazuh-manager
```

- Checking service status:

```
sudo systemctl status wazuh-manager
```

BIBLIOGRAPHY

1.OfficialWazuhDocumentation:
https://documentation.wazuh.com

2. OpenSearch Documentation: https://opensearch.org