Wazuh

Wazuh is used to collect, aggregate, index and analyze security data, helping organizations detect intrusions, threats and behavioral anomalies.

As cyber threats are becoming more sophisticated, real-time monitoring and security analysis are needed for fast threat detection and remediation. That is why our light-weight agent provides the necessary monitoring and response capabilities, while our server component provides the security intelligence and performs data analysis.

Step-by-step installation :

Install Wazuh and Open Distro for Elasticsearch components in an all-in-one deployment. Follow the instructions to configure the official repositories to perform installations.

## Installing Wazuh :

The Wazuh server collects and analyzes data from the deployed Wazuh agents. It runs the Wazuh manager, the Wazuh API and Filebeat.

To start setting up Wazuh, add the Wazuh repository to the server.

1 - Adding the Wazuh repository

1. Install the necessary packages for the installation:

# apt install curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gnupg

1. Install the GPG key:

# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -

1. Add the repository:

# echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list

1. Update the package information:

# apt-get update

### 1.2 - Installing the Wazuh manager

1. Install the Wazuh manager package:

# apt-get install wazuh-manager

2 . Enable and start the Wazuh manager service:

systemctl daemon-reload

systemctl enable wazuh-manager

systemctl start wazuh-manager

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

systemctl status wazuh-manager

## Elasticsearch :

Elasticsearch is a distributed, free and open search and analytics engine for all types of data, including textual, numerical, geospatial, structured, and unstructured. Elasticsearch is built on Apache Lucene and was first released in 2010 by Elasticsearch N.V. (now known as Elastic). Known for its simple REST APIs, distributed nature, speed, and scalability, Elasticsearch is the central component of the Elastic Stack, a set of free and open tools for data ingestion, enrichment, storage, analysis, and visualization. Commonly referred to as the ELK Stack (after Elasticsearch, Logstash, and Kibana), the Elastic Stack now includes a rich collection of lightweight shipping agents known as Beats for sending data to Elasticsearch.

Installing Elasticsearch :

Open Distro for Elasticsearch is an open source distribution of Elasticsearch, a highly scalable full-text search engine. It offers advanced security, alerting, index management, deep performance analysis, and several other additional features.

apt install elasticsearch-oss opendistroforelasticsearch

### Configuring Elasticsearch :

Run the following command to download the configuration file /etc/elasticsearch/elasticsearch.yml:

curl -so /etc/elasticsearch/elasticsearch.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/7.x/elasticsearch\_all\_in\_one.yml

### Elasticsearch users and roles :

You need to add users and roles in order to use the Wazuh Kibana properly.

Run the following commands to add the Wazuh users and additional roles in Kibana:

curl -so /usr/share/elasticsearch/plugins/opendistro\_security/securityconfig/roles.yml https://github.com/Opentech-helper/OpechtechTechhelper/blob/main/roles.yml

curl -so /usr/share/elasticsearch/plugins/opendistro\_security/securityconfig/roles\_mapping.yml https://github.com/Opentech-helper/OpechtechTechhelper/blob/main/roles\_mapping.yml

curl -so /usr/share/elasticsearch/plugins/opendistro\_security/securityconfig/internal\_users.yml https://github.com/Opentech-helper/OpechtechTechhelper/blob/main/internal\_users.yml

Wazuh users added in Kibana by running the commands above

|  |  |
| --- | --- |
| wazuh\_user | It is created for users who need read-only access to the Wazuh Kibana plugin. |
| wazuh\_admin | It is recommended for users who need administrative privileges. |

Wazuh additional roles added in Kibana to give the appropriate permissions to users:

|  |  |
| --- | --- |
| wazuh\_ui\_user | It provides wazuh\_user with permissions to read the Wazuh indices. |
| wazuh\_ui\_admin | It allows wazuh\_admin to perform reading, writing, management, and indexing tasks on the Wazuh indices. |

These users and roles are designed to operate along with the Wazuh Kibana plugin, but they are protected and cannot be modified from the Kibana interface. To modify them or add new users or roles, the securityadmin script has to be run.

Certificates creation :

1. Remove the demo certificates:

# rm /etc/elasticsearch/esnode-key.pem /etc/elasticsearch/esnode.pem /etc/elasticsearch/kirk-key.pem /etc/elasticsearch/kirk.pem /etc/elasticsearch/root-ca.pem -f

1. Generate and deploy the certificates:
   * Download the wazuh-cert-tool.sh:
   * # curl -so ~/wazuh-cert-tool.sh https://packages.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/wazuh-cert-tool.sh
   * # curl -so ~/instances.yml https://packages.wazuh.com/resources/4.2/open-distro/tools/certificate-utility/instances\_aio.yml
   * Run the wazuh-cert-tool.sh to create the certificates:
   * # bash ~/wazuh-cert-tool.sh
   * Move the Elasticsearch certificates to their corresponding location:
   * # mkdir /etc/elasticsearch/certs/
   * # mv ~/certs/elasticsearch\* /etc/elasticsearch/certs/
   * # mv ~/certs/admin\* /etc/elasticsearch/certs/
   * # cp ~/certs/root-ca\* /etc/elasticsearch/certs/
2. Enable and start the Elasticsearch service:

Systemd

# systemctl daemon-reload

# systemctl enable elasticsearch

# systemctl start elasticsearch

1. Run the Elasticsearch securityadmin script to load the new certificates information and start the cluster:

# export JAVA\_HOME**=**/usr/share/elasticsearch/jdk/ **&&** /usr/share/elasticsearch/plugins/opendistro\_security/tools/securityadmin.sh -cd /usr/share/elasticsearch/plugins/opendistro\_security/securityconfig/ -nhnv -cacert /etc/elasticsearch/certs/root-ca.pem -cert /etc/elasticsearch/certs/admin.pem -key /etc/elasticsearch/certs/admin-key.pem

Run the following command to ensure that the installation is successful:

# curl -XGET https://localhost:9200 -u admin:admin -k

Filebeat :

Filebeat is a lightweight shipper for forwarding and centralizing log data. Installed as an agent on your servers, Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to [Elasticsearch](https://www.elastic.co/products/elasticsearch) or [Logstash](https://www.elastic.co/products/logstash) for indexing.

## Installing Filebeat

Filebeat is the tool on the Wazuh server that securely forwards alerts and archived events to Elasticsearch.

1 - Install the Filebeat package:

apt-get install filebeat

2 - Download the preconfigured Filebeat configuration file used to forward the Wazuh alerts to Elasticsearch:

curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/resources/4.2/open-distro/filebeat/7.x/filebeat\_all\_in\_one.yml

3 - Download the alerts template for Elasticsearch:

curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/4.2/extensions/elasticsearch/7.x/wazuh-template.json

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

4 - Download the Wazuh module for Filebeat:

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.1.tar.gz | tar -xvz -C /usr/share/filebeat/module

5 - Copy the Elasticsearch certificates into /etc/filebeat/certs:

mkdir /etc/filebeat/certs

# cp ~/certs/root-ca.pem /etc/filebeat/certs/

# mv ~/certs/filebeat\* /etc/filebeat/certs/

6 - Enable and start the Filebeat service:

systemctl daemon-reload

# systemctl enable filebeat

# systemctl start filebeat

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

filebeat test output

## **Kibana**

ibana is an free and open frontend application that sits on top of the Elastic Stack, providing search and data visualization capabilities for data indexed in Elasticsearch. Commonly known as the charting tool for the Elastic Stack (previously referred to as the ELK Stack after Elasticsearch, Logstash, and Kibana), Kibana also acts as the user interface for monitoring, managing, and securing an Elastic Stack cluster — as well as the centralized hub for built-in solutions developed on the Elastic Stack. Developed in 2013 from within the Elasticsearch community, Kibana has grown to become the window into the Elastic Stack itself, offering a portal for users and companies.

Installing Kibana:

Kibana is a flexible and intuitive web interface for mining and visualizing the events and archives stored in Elasticsearch.

1 - Install the Kibana package:

apt-get install opendistroforelasticsearch-kibana

2 - Download the Kibana configuration file:

curl -so /etc/kibana/kibana.yml https://packages.wazuh.com/resources/4.2/open-distro/kibana/7.x/kibana\_all\_in\_one.yml

In the /etc/kibana/kibana.yml file, the setting server.host has the value 0.0.0.0. It means that Kibana can be accessed from the outside and accepts all the available IPs of the host. This value can be changed for a specific IP if needed.

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

# mkdir /usr/share/kibana/data

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

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

1. cd /usr/share/kibana
2. # sudo -u kibana /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh\_kibana-4.2.3\_7.10.2-1.zip

5 - Copy the Elasticsearch certificates into /etc/kibana/certs:

# mkdir /etc/kibana/certs

# cp ~/certs/root-ca.pem /etc/kibana/certs/

# mv ~/certs/kibana\* /etc/kibana/certs/

# chown kibana:kibana /etc/kibana/certs/\*

6 - Link Kibana socket to privileged port 443:

setcap 'cap\_net\_bind\_service=+ep' /usr/share/kibana/node/bin/node

7 - Enable and start the Kibana service:

# systemctl daemon-reload

# systemctl enable kibana

# systemctl start kibana

8 - Access the web interface:

URL: https://<wazuh\_server\_ip>

user: admin

password: admin