DEPLOYMENT METHODS

1. All-in-one deployment

In an all-in-one deployment, the Wazuh server and Elastic Stack are installed on the same host. This type of deployment is suitable for testing and small production environments. A typical use case for this type of environment supports around 100 agents.

The minimum requirements for this type of deployment are 4 GB of RAM and 2 CPU cores, and the recommendations are 16 GB of RAM and 8 CPU cores. A 64 -bit operating system is required.

Disk space requirements depend on the alerts per second (APS) generated. Expected APS varies greatly depending on the amount and type of endpoints monitored. The following table provides an estimate of storage per agent needed for 90 days of alerts based on the type of endpoint being monitored.

Table 8: Estimated storage per agent

Terminals monitored	APS	Storage (GB/90 days)
Waiters	0.25	3.8
Personal work places	0.1	1.5
Network devices	0.5	7.6

For example, for an environment with 80 workstations, 10 servers, and 10 network devices, the storage needed for 90 days of alerts would be approximately 236 GB.

2. Distributed deployment

In a distributed deployment, the Wazuh server and Elastic Stack are installed on separate hosts. This configuration is recommended for production environments because it provides high availability and scalability of services.

The Wazuh server and Elastic Stack can each be installed as a single-node or multi- node cluster. Kibana can be installed either in the same node as Elasticsearch or in a dedicated host. For each node, the hardware recommendations are:

Table 1: Hardware Recommendation Wazuh Server & Elastic Stack

	Minimum		Recommended	
Component	RAM(GB)	CPU(Cores)	RAM(GB)	CPU(Cores)
Wazuh server	2	2	8	4
Elastic stack	4	2	16	8

A 64-bit operating system is required.

Regarding disk space requirements, the amount of data depends on the alerts per second (APS) generated. The following table shows an estimate of the disk space per agent required to store 90 days of alerts on a Wazuh server as well as on an Elasticsearch server depending on the type of endpoints monitored.

Table 2: Estimated disk space per agent needed for storage

Terminals monitored	APS	Storage in Wazuh Manager (GB/90 days)	Storage in Elasticsearch (GB/90 days)
Waiters	0.25	0.1	3.7
Personal work places	0.1	0.04	1.5
Network devices	0.5	0.2	7.4

For example, for an environment with 80 workstations, 10 servers, and 10 network devices, the storage needed for 90 days of alerts would be approximately 230 GB onthe Elasticsearch server and 6 GB on the Wazuh server.

2.1. Scaling

In order to determine if a Wazuh server requires more resources, the following files can be monitored:

/var/ossec/var/run/ossec-analysisd.state and /var/ossec/var/run/ossec-remoted.sate

In the analysid.state file, the variable events_dropped indicates whether events are dropped due to a lack of resources. Similarly, ossec-remoted.state has the discarded_count variable, which indicates whether messages from agents have been discarded. These two variables must be null if the environment works correctly. If not, additional nodes can be added to the cluster.

To monitor if the Elastic Stack environment is working properly, tools such as Performance

Deployement methods

Monitor are available.

2.2. Installation method

For each type of deployment, the user can choose between two installation methods:

- Unattended: automated installation. It requires the initial entry of the necessary information to complete the installation process through scripts.
- Step by step: Manual installation. Includes a detailed description of each step of the installation process.

2.2.1 Wazuh deployment with Open Distro for Elasticsearch

2.2.1.1 All-in-one deployment

This section walks you through installing and configuring the Wazuh server and the Elastic Stack on the same host. This type of deployment is appropriate for testing and small production environments.

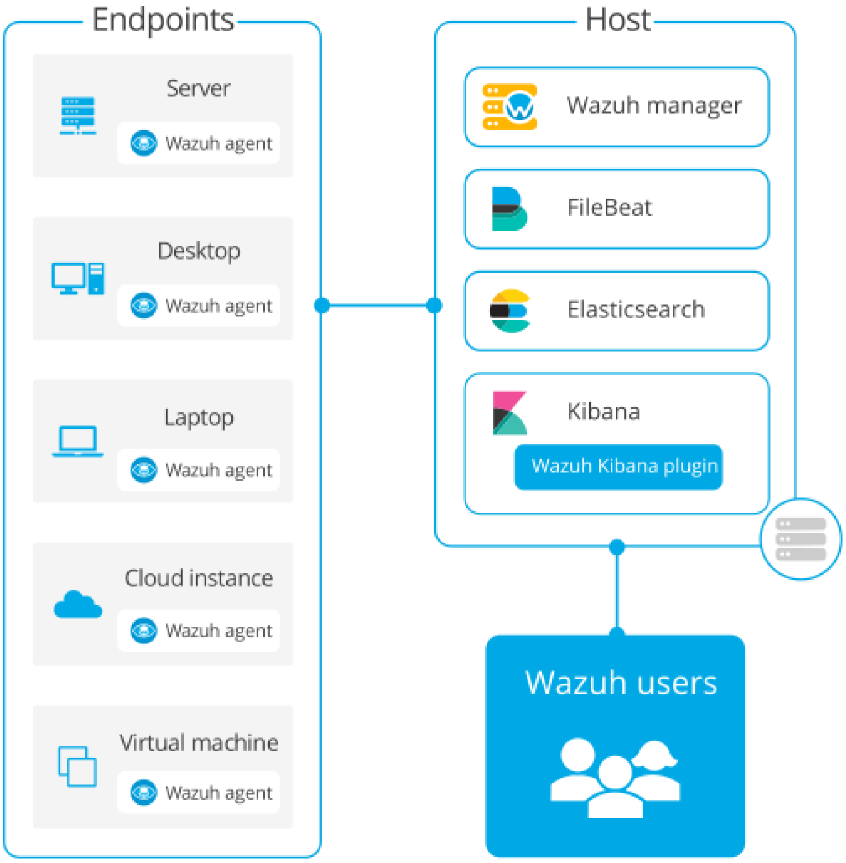


Figure1: Architecture of an all-in-one deployment of Wazuh

Deployement methods

The following components will be installed:

- The Wazuh server, including the Wazuh manager as a single node cluster and the Wazuh API.
- Elastic Stack, including Open Distro for Elasticsearch as a single-node cluster, Filebeat, and Kibana, including the Wazuh Kibana plugin.

Communication will be encrypted using SSL certificates. These certificates will be generated using the Search Guard offline TLS tool.

Additionally, in order to properly use the Wazuh Kibana plugin, additional Elasticsearch roles and users will be added.

To ensure the expected performance of Wazuh components, the host must meet the hardware requirements described in the prerequisites section.

The user can choose between step-by-step installation, a manual way of performing the process, or unattended installation, an automated way using a script.

2.2.1.2 Unattended installation

This part will explain how to install Wazuh on a single host using a script that will automatically detect if the operating system uses rpm or deb packages. The script will perform a health check verifying that available system resources meet minimum requirements.

The script will install the Java SDK and other packages including unzip and libcap required by Open Distro for Elasticsearch. Additionally, the Search Guard offline TLS tool will be used to generate data protection certificates in the Elastic Stack.

However, let's move on to the installation:

NB: Super user privileges are required to execute all the commands described below. The curl package will be used to download the script.

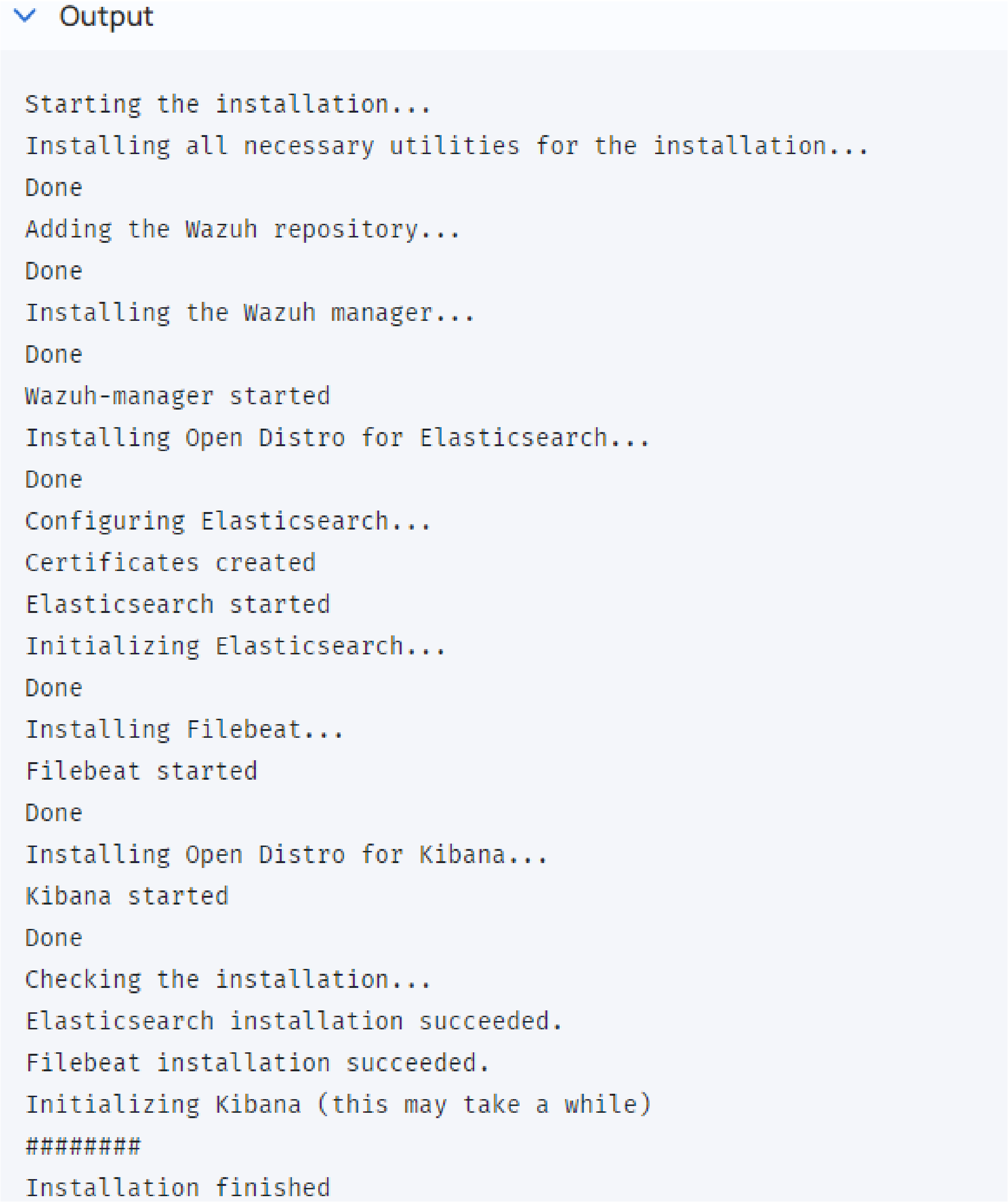
1.Download and run the script:

#curl -so ~/all-in-one-installation.sh**https://raw.githubusercontent.com/wazuh/wazuh-**

documentation/4.0/resources/open-distro/unattended-installation/all-in-one-installation.sh && bash~/all-in-one-installation.sh

The script will perform a health check to ensure that the host has enough resources to guarantee the correct performance. To skip this step, add the -i or –ignore -healthcheck option when running the script.

After the script runs, it will display the following messages to confirm that the installation was successful:



```
Starting the installation...
Installing all necessary utilities for the installation...
Done
Adding the Wazuh repository...
Done
Installing the Wazuh manager...
Done
Wazuh-manager started
Installing Open Distro for Elasticsearch...
Done
Configuring Elasticsearch...
Certificates created
Elasticsearch started
Initializing Elasticsearch...
Done
Installing Filebeat...
Filebeat started
Done
Installing Open Distro for Kibana...
Kibana started
Done
Checking the installation...
Elasticsearch installation succeeded.
Filebeat installation succeeded.
Initializing Kibana (this may take a while)
########
Installation finished
```

Deployement methods

1. Access the web interface:

URL: https://<wazuh_server_ip>
user: admin
password: admin

When accessing Kibana for the first time, the browser displays a warning message stating that the certificate was not issued by a trusted authority. It is possible to add an exception in the advanced options of the browser or, for more security, the previously generated file root-ca.pem can be imported into the certificate manager of the browser. Alternatively, it is possible to configure a certificate from a trusted authority.

NB:The Open Distro for Elasticsearch performance monitor plugin is removed during installation because it may negatively impact system resources.

2.2.1.3. Customization of the installation

The Kibana configuration found in the /etc/kibana/kibana.yml file has the server. host parameter set to 0.0.0.0 This means that Kibana is accessible externally and will accept all available IP addresses from the host. This value can be changed for a specific IP address if needed.

It is strongly recommended to change the default Elasticsearch passwords for users found in the file:

/usr/share/elasticsearch/plugins/opendistro_security/securityconfig/internal_users.yml

Now let's go through the installation step by step.

a. Installation step by step

❖ Preconditions

Open Distro for Elasticsearch requires the Java SDK as well as the installation of other packages such as wget, curl, unzip and libcap which will be used in the following steps:

1. **Installation of all packages required for installation**

#apt install curl apt-transport-https unzip wget libcap2-bin software-properties-common lsb-release gnupg2

2. **Add the Java Development Kit (JDK) repository:**

- For Debian :

```
# echo 'deb http://deb.debian.org/debian stretch-backports main' > /etc/apt/sources.list.d/backports.list
```

For Ubuntu and other Debian-based operating systems:

```
#add-apt-repository ppa:openjdk-r/ppa
```

3. **Update repository data:**

```
#aptupdate
```

4. **Install all required utilities:**

```
# export JAVA_HOME=/usr/ && apt install openjdk-11-jdk
```

❖ Installation of Wazuh

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

The first step to configure Wazuh is to add the Wazuh repository to the server.

- Added repository :

1. **Install the GPG key:**

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

2. **Add the repository:**

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

3. **Update package information:**

```
# apt-get update
```

❖ Installation of the Wazuh manager

1. **Install the Wazuh manager package:**

```
# apt-get install wazuh-manager=4.0.4-1
```

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
```

❖ Installing Elasticsearch

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

- Install Elasticsearch OSS and Open Distro for Elasticsearch:

```
# apt install elasticsearch-oss=7.9.1 opendistro-alerting=1.11.0.1-1 opendistro-anomaly-detection=1.11.0.0-1 opendistro-index-management=1.11.0.0-1 opendistro-job-scheduler=1.11.0.0- 1 opendistro-knn=1.11.0.0-1 opendistro-knnlib=1.11.0.0 opendistro-performance-analyzer=1.11.0.0-1 opendistro-security=1.11.0.0-0 opendistro-sql=1.11.0.0-1 opendistroforelasticsearch=1.11. 0-1
```

- Configuring Elasticsearch:

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

```
#curl -so /etc/elasticsearch/elasticsearch.yml https://raw.githubusercontent.com/wazuh/wazuhdocumentation/4.0/resources/op en-distro/elasticsearch/7.x/elasticsearch_all_in_one.yml
```

- elasticsearch roles and users:

In order to correctly use the Wazuh Kibana plugin, it is necessary to add the additional roles and users:

```
#curl -so/usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles.yml https://raw.githubusercontent.com/wazuh/wazuh-documentation/4.0/resources/open-distro/elasticsearch/roles/roles. yml
#curl -so/usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles_mapping.yml https://raw.githubusercontent.com/wazuh/wazuh-documentation/4.0/resources/open-distro/elasticsearch/roles/roles_mapping. yml
```

```
#curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/internal_users.yml
```

https://raw.githubusercontent.com/wazuh/wazuh-documentation/4.0/resources/open-distro/elasticsearch/roles/internal_users. yml

The above commands add the following Wazuh users to Kibana:

wazuh_user	Created for users who need read-only access to the Wazuh Kibana plugin.
wazuh_admin	Recommended user for users who need administrative privileges.

Two additional roles are added, whose function is to give the appropriate permissions to users:

wazuh_ui_user	This role provides wazuh_user permissions to read Wazuh indexes.
wazuh_ui_admin	This role allows wazuh_admin to perform read, write, manage, and index tasks on Wazuh indexes.

These users and roles are designed to work with the Wazuh Kibana plugin and they are protected so that they cannot be changed from the Kibana interface. To modify them or add new users or roles, the securityadmin script must be run.

- **Creation of certificates**

1. Delete 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

2. Generate and deploy certificates:

- Navigate to the installation location and create the certificates directory:

#mkdir /etc/elasticsearch/certs

#cd /etc/elasticsearch/certs

- Download the Search Guard offline TLS tool to create the certificates:

#curl -so ~/search-guard-tlstool-1.8.zip https://maven.search-guard.com/search- guard-tlstool/1.8/search-guard-tlstool-1.8.zip

- Extract the downloaded file. It is assumed that it was uploaded in~/ (home directory):

```
#unzip ~/search-guard-tlstool-1.8.zip -d ~/searchguard
```

- Download the search-guard.yml configuration file. This file is preconfigured to generate all necessary certificates:

```
#curl -so ~/searchguard/search-guard.yml https://raw.githubusercontent.com/wazuh/wazuh-documentation/4.0/resources/open-distro/searchguard/search-guard-aio.yml
```

- Run the Search Guard script to create the certificates:

```
#~/searchguard/tools/sgtlstool.sh -c ~/searchguard/search-guard.yml -ca -crt -t /etc/elasticsearch/certs/
```

- Once the certificates are created, delete the unnecessary files:

```
#rm /etc/elasticsearch/certs/client-certificates.readme /etc/elasticsearch/certs/elasticsearch_elasticsearch_config_snippet.yml ~/search-guard-tlstool-1.8.zip ~/searchguard -rf
```

1- Enable and start the Elasticsearch service:

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

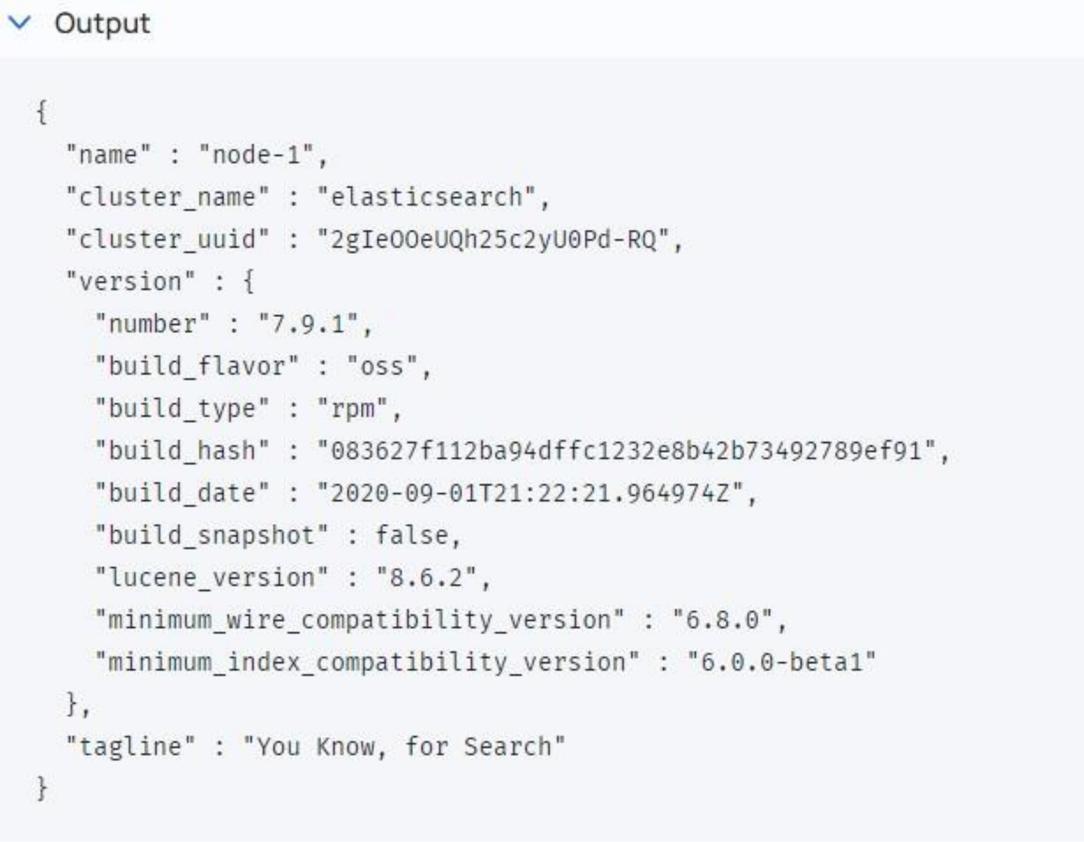
2- Run the Elasticsearch security_admin script to load the new certificate information and start the cluster:

```
#/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
```

3- Run the following command to ensure that the installation was successful:

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

An example response should look like this:



```
{
  "name" : "node-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "2gIeOOeUQh25c2yU0Pd-RQ",
  "version" : {
    "number" : "7.9.1",
    "build_flavor" : "oss",
    "build_type" : "rpm",
    "build_hash" : "083627f112ba94dffc1232e8b42b73492789ef91",
    "build_date" : "2020-09-01T21:22:21.964974Z",
    "build_snapshot" : false,
    "lucene_version" : "8.6.2",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

NB:
The Open Distro for Elasticsearch performance monitor plugin is installed by default and may negatively impact system resources. We recommend that you remove it with the following command: **/usr/share/elasticsearch/bin/elasticsearch-plugin remove opendistro_performance_analyzer**

Be sure to restart the Elasticsearch service afterwards.

❖ Installing Filebeat

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

1- Install the Filebeat package:

#apt-get install filebeat=7.9.1

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

```
#curl -so /etc/filebeat/filebeat.yml
https://raw.githubusercontent.com/wazuh/wazuh- documentation/4.0/resources/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/4.0/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 to /etc/filebeat/certs:**

```
#mkdir /etc/filebeat/certs
#cp /etc/elasticsearch/certs/root-ca.pem /etc/filebeat/certs/
#mv /etc/elasticsearch/certs/filebeat* /etc/filebeat/certs/
```

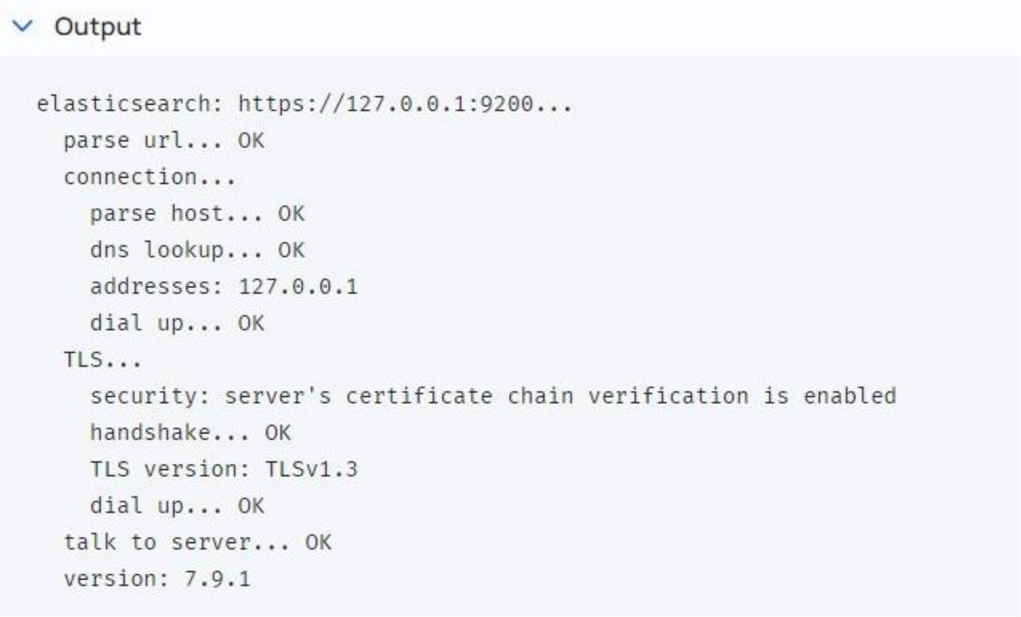
6- **Enable and start the Filebeat service:**

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

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

```
#filebeat test output
```

An example response should look like this:



```
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: 7.9.1
```

- **Installing Kibana**

Kibana is a flexible and intuitive web interface for exploring and viewing events and archives stored in Elasticsearch.

Install the Kibana package:

#apt-get install opendistroforelasticsearch-kibana=1.11.0

Download the Kibana configuration file:

#curl -so /etc/kibana/kibana.yml https://raw.githubusercontent.com/wazuh/wazuh-documentation/4.0/resources/open-distro/kibana/7.x/kibana_all_in_one.yml

In the /etc/kibana/kibana.yml file, the server.host parameter has the value 0.0.0.0. This means that Kibana is accessible from the outside and will accept all available IP addresses from the host. This value can be changed for a specific IP address if needed.

1- **Update the permissions of the optimize and: plugins directories**

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

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

2- **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-4.0.4_7.9.1-1.zip

3- **Copy the Elasticsearch certificates to /etc/kibana/certs:**

#mkdir /etc/kibana/certs

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

#mv /etc/elasticsearch/certs/kibana_http.key /etc/kibana/certs/kibana.key

#mv /etc/elasticsearch/certs/kibana_http.pem /etc/kibana/certs/kibana.pem

4- **Connect the Kibana socket to privileged port 443:**

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

5- **Enable and start the Kibana service:**

#systemctl daemon-reload

#systemctl enable kibana

#systemctl start kibana

6- **Access the web interface:**

URL: https://<wazuh_server_ip>

user: admin

password: admin

When accessing Kibana for the first time, the browser displays a warning message stating that the certificate was not issued by a trusted authority. An exception can be added in the web browser's advanced options or, for added security, the previously generated root-ca.pem file can be imported into the browser's certificate manager. Alternatively, a certificate from a trusted authority can be configured.

It is strongly recommended to change the default Elasticsearch passwords for users found in /usr/share/elasticserach/plugins/opendisro_security/securityconfig/internal_users.yml. It is also recommended to customize the /etc/elasticsearch/jvm.options file to improve

Elasticsearch performance.

❖ Installing Agents

The Wazuh agent is cross-platform and runs on the hosts the user wants to monitor. It offers the following features:

- Log and data collection
- File integrity monitoring
- Rootkit and malware detection
- Security Policy Monitoring.
- Setup Assessments
- Software inventory

The Wazuh agent communicates with the Wazuh manager, sending data in near real time through an encrypted and authenticated channel.

The agent was developed taking into account the need to monitor a wide variety of different terminals without affecting their performance. It requires an average of 35 MB of RAM. Therefore, it is supported on most popular operating systems.

There are several options for installing a Wazuh agent, depending on the operating system and whether you want to compile from source or not.
If you are deploying Wazuh in a large environment, with a large number of servers or endpoints, keep in mind that this deployment may be easier using automation tools suchas Puppet, Chef, SCCM or Ansible.
NB:
Compatibility between the Wazuh agent and the Wazuh manager is guaranteed when the Wazuh manager has a newer or equivalent version to the Wazuh agent.
In our case, we will present the installation of the Wazuh agent on the 3 most used operating systems, namely Linux (Redhat & Ubuntu), macOS, Windows.

- Installing the Wazuh agent on Linux systems:

○ REDHAT :

➢ Added repository

1- Import the GPG key:

```
#rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

2- Add the repository:

```
#cat > /etc/yum.repos.d/wazuh.repo << EOF
[wazuh]
        gpgcheck=1
        gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
        enabled=1
        name=EL-$releasever - Wazuh
        baseurl=https://packages.wazuh.com/4.x/yum/
        protect=1
        EOF
```

- **Wazuh Agent Installation**

1. Install the Wazuh agent on your terminal. You can choose between installation or deployment:

a. Facility :

```
#yum install wazuh-agent-4.0.4-1
```

Once the agent is installed, the next step is to register it and configure it to communicate with the manager. For more information on this process, let's skip the following section: Wazuh Agent Registration

- Registration of Wazuh Agents

Collecting security event data from the Wazuh agent requires enabling communication with the Wazuh manager.

The Wazuh manager needs to know which Wazuh agent sends security events and whether they are allowed. This step is called Wazuh agent registration and can be done using the . Using port 1515 and TCP protocol, the Wazuh manager will assist the registration request from the Wazuh agent using a TLS connection. The Wazuh agentwill obtain a unique key used to encrypt traffic between them. Once registered, this communication will not be used again, unless the Wazuh agent needs to be registeredin a new Wazuh manager.

After registration, the Wazuh agent must be configured to indicate the destination where the collected security events will be sent. By default, the Wazuh manager will use a communication channel on port 1514 using the TCP protocol, through which the Wazuh agent will send the collected data.

- Linux/Unix host :

Open a terminal in the Linux/Unix Wazuh agent host as the root user:

1. To register the Wazuh agent, run the agent-auth utility using the Wazuh manager IP address:

```
# /var/ossec/bin/agent-auth -m <manager_IP>
```

If the name of the new Wazuh agent is not provided, it is set automatically using the hostname. To specify the Wazuh agent name, add to the above command: -A <agent_name>

2. To enable communication with the Wazuh manager, edit the Wazuh agent configuration file located in /var/ossec/etc/ossec.conf .

In the <client><server> section, MANAGER_IP should be replaced with the Wazuh server IP address or DNS name:

```
<customer>
<server>
<address>MANAGER_IP</address>
</server>
</customer>
```

3. Restart the Wazuh agent:

```
# systemctl restart wazuh-agent
```

- macOS host:

Open a terminal in the MacOS X Wazuh agent host as root:

1- To register the Wazuh agent, run the agent-auth utility using the Wazuh manager IP address.

```
# /Library/Ossec/bin/agent-auth -m <manager_IP>
```

If the name of the new Wazuh agent is not provided, it is set automatically using the hostname. To specify the Wazuh agent name, add to the above command: -A <agent_name>

2- To enable communication with the Wazuh manager, edit the Wazuh agent configuration file located in /Library/Ossec/etc/ossec.conf

In the <client><server> section, MANAGER_IP should be replaced with the Wazuh server IP address or DNS name:

```
<customer>
<server>
<address>MANAGER_IP</address>
</server>
```

</customer>

3- Restart the Wazuh agent:

```
#/Library/Ossec/bin/ossec-control   restart
```

- Windows host:

Open Powershell or CMD session in Wazuh agent host as Administrator file
The Wazuh agent installation directory depends on the host architecture:

- C:\Program Files (x86)\ossec-agent for x86_64 hosts
- C:\Program Files\ossec-agent for x86 hosts

1. To register the Wazuh agent, run the agent-auth utility using the Wazuh manager IP address.

✓ **Powershell:**

```
# &'C:\Program Files (x86)\ossec-agent\agent-auth.exe' -m <manager_IP>
```

✓ **Windows Command Prompt:**

```
# "C:\Program Files (x86)\ossec-agent\agent-auth.exe" -m <manager_IP>
```

If the name of the new Wazuh agent is not provided, it is set automatically using the hostname. To specify the Wazuh agent name, add to the above command: -A <agent_name>

1- To enable communication with the Wazuh manager, edit the Wazuh agent configuration file located in:

C:\Program Files (x86)\ossec-agent\ossec.conf

In the <client><server> section, MANAGER_IP should be replaced with the Wazuh server IP address or DNS name:

```
<customer>
<server>
<address>MANAGER_IP</address>
</server>
</customer>
```

2- Restart the Wazuh agent:

✓ **powershell:**

```
# Restart-Service -Name wazuh
```

✓ **Windows Command Prompt**:

```
# net stop wazuh
# net start wazuh
```

a. Deployment

Agent registration and configuration can be automated using variables. At least the WAZUH_MANAGER variable must be defined. The agent will use this value to register and will be the designated manager for event forwarding.

# WAZUH_MANAGER="10.0.0.2" yum install wazuh-agent-4.0.4-1

1- Activate the service:

# systemctl daemon-reload

#systemctl enable wazuh-agent

#systemctl start wazuh-agent

2- Disable Wazuh updates:

It is recommended that the version of the Wazuh manager be greater than or equal to that of the Wazuh agents. Therefore, we recommend disabling the Wazuh repository to avoid accidental upgrades. To do this, use the following command:

# sed -i "s/^enabled=1/enabled=0/" /etc/yum.repos.d/wazuh.repo

✓ Uninstall the agent:

To uninstall the agent:

# yum remove wazuh-agent

Some files are marked as configuration files. Because of this designation, the package manager does not remove these files from the file system. The complete file removal action is the responsibility of the user and can be performed by deleting the /var/ossec folder.

- UBUNTU

✓ Added repository:

1- Install the GPG key:

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

2- Add the repository:

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

3- Update package information:

#apt-get update

➢ **Wazuh agent installation:**

1. As we can see previously it is possible to choose between installation and deployment:

a. Facility :

# apt-get install wazuh-agent=4.0.4-1

Once the agent is installed, the next step is to register it and configure it to communicate with the manager. For more information on this process, visit the Registration of wazuh agents section seen above.

b. Deployment :

Agent registration and configuration can be automated using variables. At least the WAZUH_MANAGER variable must be defined. The agent will use this value to register and will be the designated manager for event forwarding.

# WAZUH_MANAGER="10.0.0.2" apt-get install wazuh-agent=4.0.4-1

2. Activate the service:

# systemctl daemon-reload

#systemctl enable wazuh-agent

#systemctl start wazuh-agent

3. Disable updates:

# sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list

#apt-get update

➢ Uninstall the agent:

To uninstall the agent, type the following command:

# apt-get remove wazuh-agent

Some files are marked as configuration files. Because of this designation, the package manager does not remove these files from the file system. A complete deletion of the file can be performed using the following command:

# apt-get remove --purge wazuh-agent

- **MacOS:**

You can install it using the command line or by following the GUI steps:

a. Using the command line, you can choose between installing or deploying:

- **Facility :**

# install -pkg wazuh-agent-4.0.4-1.pkg -target/

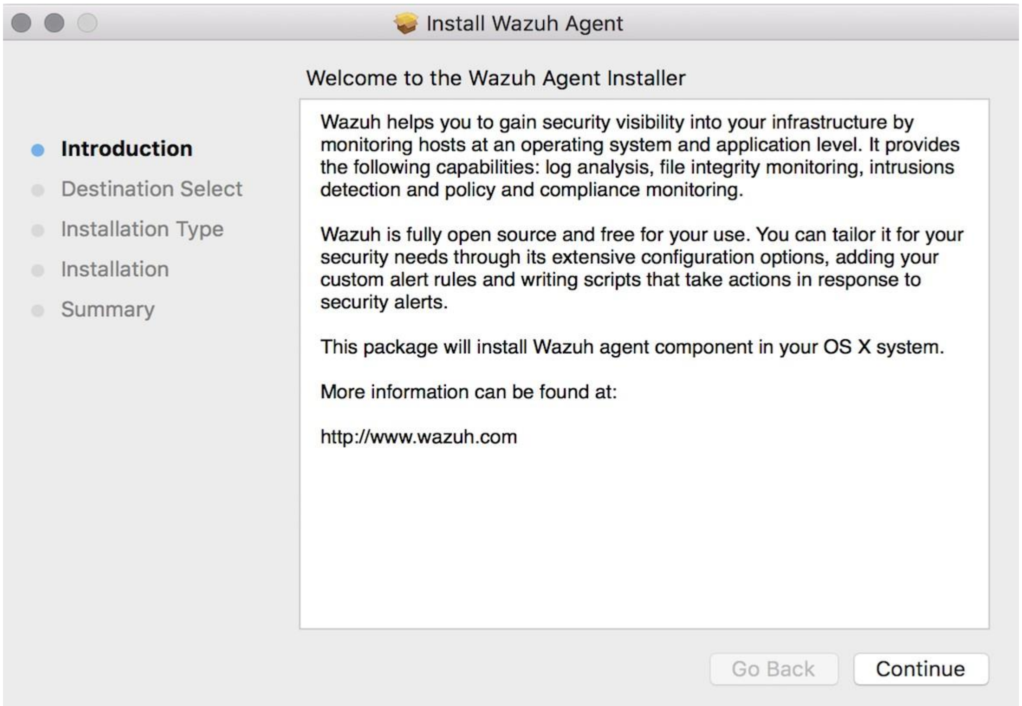
- **Deployment:**

You can automate agent registration and configuration using variables. At least the WAZUH_MANAGER variable must be defined. The agent will use this value to register and will be the designated manager for event forwarding.

# launchctl setenv WAZUH_MANAGER "MANAGER_IP" && install -pkg wazuh-agent-4.0.4-1.pkg -target /

b. Using the GUI:

Using the GUI, you can perform a simple installation without registering or configuringthe agent. Double click on the downloaded file and follow the wizard. If you don't know how to answer certain prompts, just use the default answers.



Install Wazuh Agent

Welcome to the Wazuh Agent Installer

Wazuh helps you to gain security visibility into your infrastructure by monitoring hosts at an operating system and application level. It provides the following capabilities: log analysis, file integrity monitoring, intrusions detection and policy and compliance monitoring.

Wazuh is fully open source and free for your use. You can tailor it for your security needs through its extensive configuration options, adding your custom alert rules and writing scripts that take actions in response to security alerts.

This package will install Wazuh agent component in your OS X system.

More information can be found at:

http://www.wazuh.com

By default, all agent files are located in the following location: /Library/Ossec/

Now that the agent is installed, if you have not used the deployment method, you will need to register and configure the agent to communicate with the handler (Confer session Registration Wazuh agents) seen earlier!

Finally, start the Wazuh agent:

# sudo /Library/Ossec/bin/ossec-control start

- Uninstallation:

To uninstall the agent on MacOs:

1. Stop the Wazuh agent service:

# /Library/Ossec/bin/ossec-control stop

Delete the /Library/Ossec/ folder and ossec-init.conf file:

```
# /bin/rm -r /Library/Ossec
#/bin/rm /etc/ossec-init.conf
```

2. Stop and unload the dispatcher:

```
# /bin/launchctl unload /Library/LaunchDaemons/com.wazuh.agent.plist
```

3. Remove launchdaemons and StartupItems:

```
#/bin/rm -f /Library/LaunchDaemons/com.wazuh.agent.plist
#/bin/rm -rf /Library/StartupItems/WAZUH
```

4. Delete user and groups:

```
#/usr/bin/dscl . -delete "/Users/ossec"
#/usr/bin/dscl . -delete "/Groups/ossec"
```

5. Remove Pkgutil:

```
# /usr/sbin/pkgutil --forget com.wazuh.pkg.wazuh-agent
```

- **WINDOWS**

NB: To perform this installation, administrator privileges are required.

The first step to install the Wazuh agent on a Windows machine is to download the Windows installer from the list of packages that can be found at the following address: (https://documentation.wazuh. com/4.0/installation-guide/packages-list.html#packages). Once downloaded, it can be installed using the command line orby following the GUI steps:

a. Using the command line, installation or deployment can be chosen:

➢ Facility :

To install the Windows Agent from the command line, the installer must be run using the following command (the /g argument is used for unattended installations):

- Using CMDs:

```
wazuh-agent-4.0.4-1.msi /q
```

- Using PowerShell:

```
.\wazuh-agent-4.0.4-1.msi /q
```

➢ **Deployment :**

Agent registration and configuration can be automated using variables. It is necess ary to define at least the WAZUH_REGISTRATION_SERVER or AUTHD_SERVER variable. The agent will use these values to register and assign a Wazuh handler to forward events

- **Using CMDs:**

wazuh-agent-4.0.4-1.msi /q WAZUH_MANAGER="MANAGER_IP" WAZUH_REGISTRATION_SERVER="MANAGER_IP"

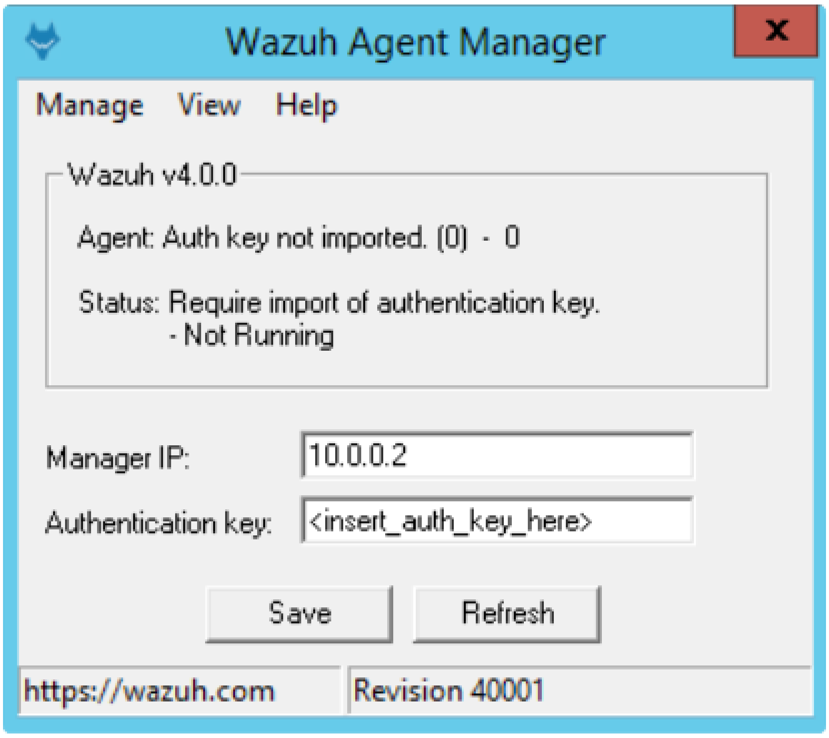
- **Using PowerShell:**

.\wazuh-agent-4.0.4-1.msi /q WAZUH_MANAGER=" MANAGER_IP " WAZUH_REGISTRATION_SERVER=" MANAGER_IP "

b. Using the GUI:

To install the Windows agent from the GUI, run the downloaded file and follow thesteps in the installation wizard. If you don't know how to answer some of the prompts, just use the default answers.

Once installed, the agent uses a graphical user interface for configuration, opening the log file, or starting and stopping the service.



Wazuh Agent Manager

Wazuh v4.0.0

Agent: Auth key not imported. (0) - 0

Status: Require import of authentication key.
- Not Running

Manager IP: 10.0.0.2

Authentication key: <insert_auth_key_here>

https://wazuh.com

Revision 40001

By default, all agent files will be located in C:\Program Files (x86)\ossec-agent.

Now that the agent is installed, the next step is to register it and configure it to communicate with the manager. For more information on this process, visit the previous Wazuh Agent Records section.

- Uninstallation:

In order to uninstall the agent, the original MSI file will be needed to perform the process unattended:

```
msiexec.exe  /x  wazuh-agent-4.0.4-1.msi  /qn
```

However, we are coming to the end of the installation of our solution! Now let's move on to the use case.