Name: Muhammad Faiq
Project: Growth Arbor SOC

Installing the Wazuh 4.2 server step by step

Step 1 # Installing Wazuh:

1. Install the necessary packages for the installation:

- # yum install curl unzip wget libcap

2. Import the GPG key:

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

3. 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

Step 2 # Installing the Wazuh manager:

1. Install the Wazuh manager package:

- apt-get install wazuh-manager=4.2.6-1

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

Step 3 # Installing Elasticsearch:

1. Install Elasticsearch OSS and Open Distro for Elasticsearch:

- apt install elasticsearch-oss opendistroforelasticsearch

Step 4 # Configuring Elasticsearch:

1. /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

Step 4 # Elasticsearch users and roles:

1. 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://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/roles.yml
- curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/roles_mapping.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/roles_mapping.yml
- curl -so /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/internal_users.yml https://packages.wazuh.com/resources/4.2/open-distro/elasticsearch/roles/internal_users.yml

Name: Muhammad Faiq
Project: Growth Arbor SOC

Step 5 # 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

2. 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/

3. Enable and start the Elasticsearch service:

- mkdir -p /etc/elasticsearch/jvm.options.d
- echo '-Dlog4j2.formatMsgNoLookups=true' > /etc/elasticsearch/jvm.options.d/disabledlog4j.options
- chmod 2750 /etc/elasticsearch/jvm.options.d/disabledlog4j.options
- chown root:elasticsearch /etc/elasticsearch/jvm.options.d/disabledlog4j.options
- systemctl daemon-reload
- systemctl enable elasticsearch

- systemctl start elasticsearch

4. 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

The Open Distro for Elasticsearch performance analyzer plugin is installed by default and can have a negative impact on system resources. We recommend removing it with the following command **/usr/share/elasticsearch/bin/elasticsearch-plugin remove opendistro-performance-analyzer.** Please be sure to restart the Elasticsearch service afterwards.

Step 6 # Installing Filebeat:

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

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

- filebeat test output

Step 7 # 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 address 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

- cd /usr/share/kibana
- sudo -u kibana /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.2.6_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