Wazuh Centralized Setup

LXD Container Information

```
lokesh@cybercub:~$ lxc list
+--------+---------+----------------------+-----------------------------------------------+-----------+-----------+
| NAME   |  STATE  |         IPV4         |                     IPV6                      |   TYPE    | SNAPSHOTS |
+--------+---------+----------------------+-----------------------------------------------+-----------+-----------+
| wazuh | RUNNING | 10.124.142.244 (eth0) | fd42:5307:47bf:8da3:216:3eff:fec4:6746 (eth0) | CONTAINER | 0         |
+--------+---------+----------------------+-----------------------------------------------+-----------+-----------+
```

lokesh@cybercub:~$ lxc exec wazuh /bin/bash
root@wazuh:~# su - lokesh
lokesh@wazuh:~$

Wazuh Indexer Setup

Certificate Creation

lokesh@wazuh:~$ mkdir wazuh-installer
lokesh@wazuh:~$ ls
snap wazuh-installer
lokesh@wazuh:~$ cd wazuh-installer/

Wazuh Centralized Setup in Ubuntu 22.04
lokesh@wazuh:~$ sudo apt update
[sudo] password for lokesh:
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:5 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1712 kB]
Get:6 http://archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:7 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [283 kB]

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.

```
lokesh@wazuh:~/wazuh-installer$ curl -sO https://packages.wazuh.com/4.8/wazuh-certs-tool.sh
lokesh@wazuh:~/wazuh-installer$ curl -sO https://packages.wazuh.com/4.8/config.yml

lokesh@wazuh:~/wazuh-installer$ ls
config.yml  wazuh-certs-tool.sh
```

Edit Config.yml file

```
lokesh@wazuh:~/wazuh-installer$ sudo nano config.yml
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "10.124.142.244"
    #- 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: "10.124.142.244"
    #  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: "10.124.142.244"
```

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

```
lokesh@wazuh:~/wazuh-installer$ bash ./wazuh-certs-tool.sh -A
09/08/2024 07:08:55 INFO: Generating the root certificate.
09/08/2024 07:08:55 INFO: Generating Admin certificates.
```

09/08/2024 07:08:55 INFO: Admin certificates created.
09/08/2024 07:08:55 INFO: Generating Wazuh indexer certificates.
09/08/2024 07:08:55 INFO: Wazuh indexer certificates created.
09/08/2024 07:08:55 INFO: Generating Filebeat certificates.
09/08/2024 07:08:56 INFO: Wazuh Filebeat certificates created.
09/08/2024 07:08:56 INFO: Generating Wazuh dashboard certificates.
09/08/2024 07:08:56 INFO: Wazuh dashboard certificates created.

Compress all the necessary files.

lokesh@wazuh:~/wazuh-installer$ tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
./
./admin-key.pem
./admin.pem
./wazuh-1-key.pem
./dashboard-key.pem
./node-1.pem
./root-ca.pem
./node-1-key.pem
./dashboard.pem
./wazuh-1.pem
./root-ca.key

lokesh@wazuh:~/wazuh-installer$ rm -rf ./wazuh-certificates

Node Installation

Install the following packages if missing:

lokesh@wazuh:~/wazuh-installer$ sudo apt-get install debconf adduser procps
[sudo] password for lokesh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
adduser is already the newest version (3.118ubuntu5).
adduser set to manually installed.
debconf is already the newest version (1.5.79ubuntu1).
debconf set to manually installed.
procps is already the newest version (2:3.3.17-6ubuntu2.1).
procps set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Adding the Wazuh repository

Install the following packages if missing.

```
lokesh@wazuh:~/wazuh-installer$ sudo apt-get install gnupg apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnupg is already the newest version (2.2.27-3ubuntu2.1).
apt-transport-https is already the newest version (2.4.12).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Install the GPG key

```
lokesh@wazuh:~/wazuh-installer$ sudo curl -s
https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --no-default-keyring --keyring
/tmp/wazuh.gpg --import
gpg: keybox '/tmp/wazuh.gpg' created
gpg: directory '/root/.gnupg' created
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key 96B3EE5F29111145: public key "Wazuh.com (Wazuh Signing Key)
<support@wazuh.com>" imported
gpg: Total number processed: 1
gpg:               imported: 1
lokesh@wazuh:~/wazuh-installer$ sudo mv /tmp/wazuh.gpg /usr/share/keyrings/wazuh.gpg
lokesh@wazuh:~/wazuh-installer$ sudo chmod 644 /usr/share/keyrings/wazuh.gpg
```

Add the repository

```
lokesh@wazuh:~/wazuh-installer$ sudo -i
root@wazuh:~# 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
deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable
main
root@wazuh:~# exit
logout
```

Update Package information

```
lokesh@wazuh:~/wazuh-installer$ sudo apt-get update
Hit:1 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu jammy InRelease
Hit:3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:5 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:6 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [42.1 kB]
```

```
Fetched 59.4 kB in 6s (10.5 kB/s)
Reading package lists... Done



lokesh@wazuh:~/wazuh-installer$ sudo apt-get install wazuh-indexer -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  wazuh-indexer
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 756 MB of archives.
After this operation, 1050 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-indexer amd64 4.8.1-1
[756 MB]
Fetched 756 MB in 3min 16s (3856 kB/s)
Selecting previously unselected package wazuh-indexer.
(Reading database ... 34006 files and directories currently installed.)
Preparing to unpack .../wazuh-indexer_4.8.1-1_amd64.deb ...

Configuring the Wazuh indexer

 lokesh@wazuh:~/wazuh-installer$ sudo nano /etc/wazuh-indexer/opensearch.yml
network.host: "10.124.142.244"
node.name: "node-1"
cluster.initial_master_nodes:
- "node-1"
#- "node-2"
#- "node-3"
cluster.name: "wazuh-cluster"
discovery.seed_hosts:
  - "10.124.142.244"
#  - "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=node-1,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
```

Deploying certificates

Run the following commands replacing <indexer-node-name> with the name of the Wazuh indexer node you are configuring as defined in config.yml. For example, node-1. This deploys the SSL certificates to encrypt communications between the Wazuh central components.

```
lokesh@wazuh:~/wazuh-installer$ NODE_NAME=node-1
lokesh@wazuh:~/wazuh-installer$ sudo mkdir /etc/wazuh-indexer/certs
[sudo] password for lokesh:
lokesh@wazuh:~/wazuh-installer$ sudo 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
lokesh@wazuh:~/wazuh-installer$ sudo mv -n /etc/wazuh-indexer/certs/$NODE_NAME.pem
/etc/wazuh-indexer/certs/indexer.pem
lokesh@wazuh:~/wazuh-installer$ sudo mv -n
/etc/wazuh-indexer/certs/$NODE_NAME-key.pem /etc/wazuh-indexer/certs/indexer-key.pem
lokesh@wazuh:~/wazuh-installer$ sudo chmod 500 /etc/wazuh-indexer/certs
lokesh@wazuh:~/wazuh-installer$ sudo -i
root@wazuh:~# chmod 400 /etc/wazuh-indexer/certs/*
root@wazuh:~# chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
```

Start the Services of Wazuh Indexer

```
lokesh@wazuh:~$ sudo systemctl daemon-reload
[sudo] password for lokesh:
lokesh@wazuh:~$ sudo systemctl enable wazuh-indexer
lokesh@wazuh:~$ sudo systemctl start wazuh-indexer
lokesh@wazuh:~$ sudo systemctl status wazuh-indexer
● wazuh-indexer.service - Wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset:
enabled)
     Active: active (running) since Tue 2024-08-13 06:58:29 UTC; 11min ago
       Docs: https://documentation.wazuh.com
   Main PID: 885 (java)
      Tasks: 88 (limit: 18792)
     Memory: 1.3G
        CPU: 41.799s
     CGroup: /system.slice/wazuh-indexer.service
             └─885 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto
-Dopensearch.networkaddress.cache.ttl=60
-Dopensearch.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m
-Djava.awt.head>
```

Aug 13 06:58:20 wazuh systemd[1]: Starting Wazuh-indexer...
Aug 13 06:58:22 wazuh systemd-entrypoint[885]: WARNING: A terminally deprecated method in java.lang.System has been called

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

```
lokesh@wazuh:~/wazuh-installer$ sudo /usr/share/wazuh-indexer/bin/indexer-security-init.sh
************************************************************************
** This tool will be deprecated in the next major release of OpenSearch **
** https://github.com/opensearch-project/security/issues/1755           **
************************************************************************
Security Admin v7
Will connect to 10.124.142.244:9200 ... done
Connected as "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
OpenSearch Version: 2.10.0
Contacting opensearch cluster 'opensearch' and wait for YELLOW clusterstate ...
Clustername: wazuh-cluster
Clusterstate: GREEN
Number of nodes: 1
Number of data nodes: 1
.opendistro_security index does not exists, attempt to create it ... done (0-all replicas)
Populate config from /etc/wazuh-indexer/opensearch-security/
Will update '/config' with /etc/wazuh-indexer/opensearch-security/config.yml
   SUCC: Configuration for 'config' created or updated
Will update '/roles' with /etc/wazuh-indexer/opensearch-security/roles.yml
   SUCC: Configuration for 'roles' created or updated
Will update '/rolesmapping' with /etc/wazuh-indexer/opensearch-security/roles_mapping.yml
   SUCC: Configuration for 'rolesmapping' created or updated
Will update '/internalusers' with /etc/wazuh-indexer/opensearch-security/internal_users.yml
   SUCC: Configuration for 'internalusers' created or updated
Will update '/actiongroups' with /etc/wazuh-indexer/opensearch-security/action_groups.yml
   SUCC: Configuration for 'actiongroups' created or updated
Will update '/tenants' with /etc/wazuh-indexer/opensearch-security/tenants.yml
   SUCC: Configuration for 'tenants' created or updated
Will update '/nodesdn' with /etc/wazuh-indexer/opensearch-security/nodes_dn.yml
   SUCC: Configuration for 'nodesdn' created or updated
Will update '/whitelist' with /etc/wazuh-indexer/opensearch-security/whitelist.yml
   SUCC: Configuration for 'whitelist' created or updated
```

```
Will update '/audit' with /etc/wazuh-indexer/opensearch-security/audit.yml
   SUCC: Configuration for 'audit' created or updated
Will update '/allowlist' with /etc/wazuh-indexer/opensearch-security/allowlist.yml
   SUCC: Configuration for 'allowlist' created or updated
SUCC: Expected 10 config types for node
{"updated_config_types":["allowlist","tenants","rolesmapping","nodesdn","audit","roles","whitelist"
,"internalusers","actiongroups","config"],"updated_config_size":10,"message":null} is 10
(["allowlist","tenants","rolesmapping","nodesdn","audit","roles","whitelist","internalusers","actiong
roups","config"]) due to: null
Done with success
```

Note: You only have to initialize the cluster once, there is no need to run this command on every node.

Testing the cluster installation

Replace <WAZUH_INDEXER_IP> and run the following commands to confirm that the installation is successful. Output should look like

```
lokesh@wazuh:~/wazuh-installer$ curl -k -u admin:admin https://10.124.142.244:9200
{
  "name" : "node-1",
  "cluster_name" : "wazuh-cluster",
  "cluster_uuid" : "wJ5lJ_a6Q-Cux_qNr3bbKA",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "eee49cb340edc6c4d489bcd9324dda571fc8dc03",
    "build_date" : "2023-09-20T23:54:29.889267151Z",
    "build_snapshot" : false,
    "lucene_version" : "9.7.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

Replace <WAZUH_INDEXER_IP_ADDRESS> and run the following command to check if the single-node or multi-node cluster is working correctly.

```
lokesh@wazuh:~/wazuh-installer$ curl -k -u admin:admin https://10.124.142.244:9200/_cat/nodes?v
ip             heap.percent ram.percent cpu load_1m load_5m load_15m node.role node.roles                        cluster_manager name
10.124.142.244           21          54   3    0.62    0.68     0.62 dimr      cluster_manager,data,ingest,remote_cluster_client *              node-1
```

Wazuh Server Setup

The Wazuh server analyzes the data received from the Wazuh agents, triggering alerts when threats or anomalies are detected. It is also used to remotely manage the agents' configuration and monitor their status.

Scaling

To determine if a Wazuh server requires more resources, monitor these files:

- /var/ossec/var/run/wazuh-analysisd.state: the variable events_dropped indicates whether events are being dropped due to lack of resources.
- /var/ossec/var/run/wazuh-remoted.state: the variable discarded_count indicates if messages from the agents were discarded.

Wazuh server node installation.

Install the Wazuh manager package.

```
lokesh@wazuh:~/wazuh-installer$ sudo apt-get install wazuh-manager -y
[sudo] password for lokesh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  expect
The following NEW packages will be installed:
  wazuh-manager
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 310 MB of archives.
After this operation, 911 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-manager amd64 4.8.1-1
[310 MB]
```

Filebeat Setup

Install Filebeat

lokesh@wazuh:~/wazuh-installer$ sudo apt-get install filebeat -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  filebeat
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 22.1 MB of archives.
After this operation, 73.6 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 filebeat amd64 7.10.2 [22.1 MB]
Fetched 22.1 MB in 18s (1199 kB/s)

Configuring Filebeat

Download the preconfigured Filebeat configuration file.

lokesh@wazuh:~/wazuh-installer$ sudo curl -so /etc/filebeat/filebeat.yml
https://packages.wazuh.com/4.8/tpl/wazuh/filebeat/filebeat.yml

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

hosts: The list of Wazuh indexer nodes to connect to. You can use either IP addresses or hostnames. By default, the host is set to localhost hosts: ["127.0.0.1:9200"]. Replace it with your Wazuh indexer address accordingly.

lokesh@wazuh:~/wazuh-installer$ sudo nano /etc/filebeat/filebeat.yml
output.elasticsearch:
  hosts: ["10.124.142.244:9200"]
  protocol: https
  username: ${username}
  password: ${password}

Create a Filebeat keystore to securely store authentication credentials.

lokesh@wazuh:~/wazuh-installer$ sudo filebeat keystore create
Created filebeat keystore

Add the default username and password admin:admin to the secrets keystore.

```
lokesh@wazuh:~/wazuh-installer$ sudo -i
root@wazuh:~# echo admin | filebeat keystore add username --stdin --force
Successfully updated the keystore
root@wazuh:~# echo admin | filebeat keystore add password --stdin --force
Successfully updated the keystore
```

Download the alerts template for the Wazuh indexer.

```
root@wazuh:~# su - lokesh
lokesh@wazuh:~$ sudo curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v4.8.1/extensions/elasticsearch/7.x/wazuh-tem
plate.json
lokesh@wazuh:~$ cd wazuh-installer/
lokesh@wazuh:~/wazuh-installer$ sudo chmod go+r /etc/filebeat/wazuh-template.json
```

Install the Wazuh module for Filebeat.

```
lokesh@wazuh:~/wazuh-installer$ sudo -i
root@wazuh:~# curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar
-xvz -C /usr/share/filebeat/module
wazuh/
wazuh/_meta/
wazuh/_meta/docs.asciidoc
wazuh/_meta/fields.yml
wazuh/_meta/config.yml
wazuh/alerts/
wazuh/alerts/config/
wazuh/alerts/config/alerts.yml
wazuh/alerts/manifest.yml
wazuh/alerts/ingest/
wazuh/alerts/ingest/pipeline.json
wazuh/module.yml
wazuh/archives/
wazuh/archives/config/
wazuh/archives/config/archives.yml
wazuh/archives/manifest.yml
wazuh/archives/ingest/
wazuh/archives/ingest/pipeline.json
```

Deploying certificates

Note: Make sure that a copy of the wazuh-certificates.tar file, created during the initial configuration step, is placed in your working directory.

Replace <SERVER_NODE_NAME> with your Wazuh server node certificate name, the same one used in config.yml when creating the certificates. Then, move the certificates to their corresponding location.

```
root@wazuh:~# mkdir /etc/filebeat/certs
lokesh@wazuh:~/wazuh-installer$ NODE_NAME=wazuh-1
lokesh@wazuh:~/wazuh-installer$ sudo tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/
./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem
lokesh@wazuh:~/wazuh-installer$ sudo mv -n /etc/filebeat/certs/$NODE_NAME.pem
/etc/filebeat/certs/filebeat.pem
lokesh@wazuh:~/wazuh-installer$ sudo mv -n /etc/filebeat/certs/$NODE_NAME-key.pem
/etc/filebeat/certs/filebeat-key.pem
lokesh@wazuh:~/wazuh-installer$ sudo chmod 500 /etc/filebeat/certs
lokesh@wazuh:~/wazuh-installer$ sudo chmod 400 /etc/filebeat/certs/*
chmod: cannot access '/etc/filebeat/certs/*': No such file or directory
lokesh@wazuh:~/wazuh-installer$ sudo -i
root@wazuh:~# chmod 400 /etc/filebeat/certs/*
root@wazuh:~# chown -R root:root /etc/filebeat/certs
```

Configuring the Wazuh indexer connection

To use the vulnerability detection capability.

Save the Wazuh indexer username and password into the Wazuh manager keystore using the wazuh-keystore tool:

```
root@wazuh:~# su - lokesh
lokesh@wazuh:~$ cd wazuh-installer/
lokesh@wazuh:~/wazuh-installer$ sudo /var/ossec/bin/wazuh-keystore -f indexer -k username
-v admin
lokesh@wazuh:~/wazuh-installer$ sudo /var/ossec/bin/wazuh-keystore -f indexer -k password -v
admin
```

Edit /var/ossec/etc/ossec.conf to configure the indexer connection.

```
lokesh@wazuh:~/wazuh-installer$ sudo nano /var/ossec/etc/ossec.conf
<indexer>
    <enabled>yes</enabled>
    <hosts>
      <host>https://10.124.142.244:9200</host>
    </hosts>
    <ssl>
      <certificate_authorities>
        <ca>/etc/filebeat/certs/root-ca.pem</ca>
      </certificate_authorities>
      <certificate>/etc/filebeat/certs/filebeat.pem</certificate>
      <key>/etc/filebeat/certs/filebeat-key.pem</key>
    </ssl>
  </indexer>
```

Replace <host> with your Wazuh indexer node IP address or hostname. You can find this value in the Filebeat config file /etc/filebeat/filebeat.yml.

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

```
lokesh@wazuh:~/wazuh-installer$ sudo filebeat test output
elasticsearch: https://10.124.142.244:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 10.124.142.244
    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
```

Start Wazuh Manager Services

```
lokesh@wazuh:~/wazuh-installer$ sudo systemctl daemon-reload
lokesh@wazuh:~/wazuh-installer$ sudo systemctl enable wazuh-manager
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-manager.service →
/lib/systemd/system/wazuh-manager.service.
```

lokesh@wazuh:~/wazuh-installer$ sudo systemctl start wazuh-manager

Start filebeat Services

lokesh@wazuh:~/wazuh-installer$ sudo systemctl daemon-reload
lokesh@wazuh:~/wazuh-installer$ sudo systemctl enable wazuh-indexer
lokesh@wazuh:~/wazuh-installer$ sudo 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
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/filebeat.service.
lokesh@wazuh:~/wazuh-installer$ sudo systemctl start filebeat

Wazuh dashboard Setup

Install the following packages if missing

lokesh@wazuh:~/wazuh-installer$ sudo apt-get install debhelper tar curl libcap2-bin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
curl is already the newest version (7.81.0-1ubuntu1.17).
curl set to manually installed.
libcap2-bin is already the newest version (1:2.44-1ubuntu0.22.04.1).

Installing the Wazuh dashboard

lokesh@wazuh:~/wazuh-installer$ sudo apt-get install wazuh-dashboard -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  wazuh-dashboard
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 186 MB of archives.
After this operation, 998 MB of additional disk space will be used.
Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-dashboard amd64 4.8.1-1 [186 MB]

Configuring the Wazuh dashboard

- server.host: This setting specifies the host of the Wazuh dashboard server. To allow remote users to connect, set the value to the IP address or DNS name of the Wazuh dashboard server. The value 0.0.0.0 will accept all the available IP addresses of the host.
- opensearch.hosts: The URLs of the Wazuh indexer instances to use for all your queries

lokesh@wazuh:~/wazuh-installer$ sudo nano /etc/wazuh-dashboard/opensearch_dashboards.yml
server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://10.124.142.244:9200
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

Deploying certificates

Note: Make sure that a copy of the wazuh-certificates.tar file, created during the initial configuration step, is placed in your working directory.

Replace <DASHBOARD_NODE_NAME> with your Wazuh dashboard node name, the same one used in config.yml to create the certificates, and move the certificates to their corresponding location.

```
lokesh@wazuh:~/wazuh-installer$ NODE_NAME=dashboard
lokesh@wazuh:~/wazuh-installer$ sudo mkdir /etc/wazuh-dashboard/certs
lokesh@wazuh:~/wazuh-installer$ sudo tar -xf ./wazuh-certificates.tar -C
/etc/wazuh-dashboard/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem
lokesh@wazuh:~/wazuh-installer$ sudo mv -n /etc/wazuh-dashboard/certs/$NODE_NAME.pem
/etc/wazuh-dashboard/certs/dashboard.pem
lokesh@wazuh:~/wazuh-installer$ sudo mv -n
/etc/wazuh-dashboard/certs/$NODE_NAME-key.pem
/etc/wazuh-dashboard/certs/dashboard-key.pem
lokesh@wazuh:~/wazuh-installer$ sudo chmod 500 /etc/wazuh-dashboard/certs
lokesh@wazuh:~/wazuh-installer$ sudo -i
root@wazuh:~# chmod 400 /etc/wazuh-dashboard/certs/*
root@wazuh:~# chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

Starting the Wazuh dashboard service

```
lokesh@wazuh:~/wazuh-installer$ sudo systemctl daemon-reload
lokesh@wazuh:~/wazuh-installer$ sudo systemctl enable wazuh-dashboard
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-dashboard.service →
/etc/systemd/system/wazuh-dashboard.service.
lokesh@wazuh:~/wazuh-installer$ sudo systemctl start wazuh-dashboard
```

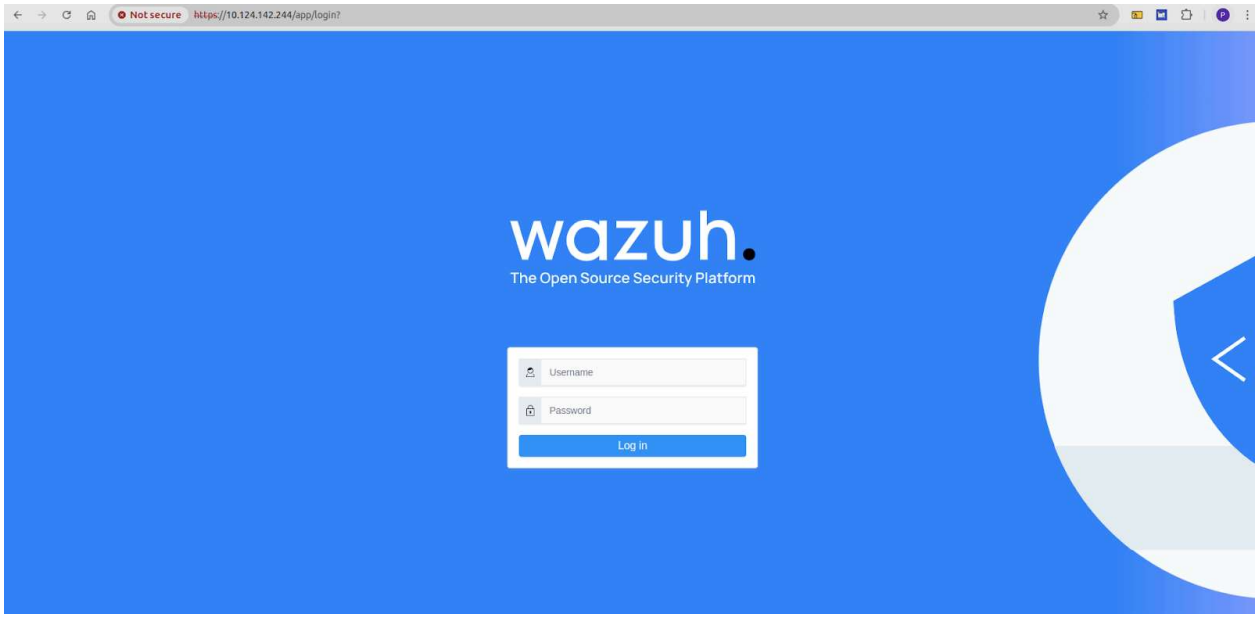
Edit /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml file and replace the url value with the IP address or hostname of the Wazuh server master node.

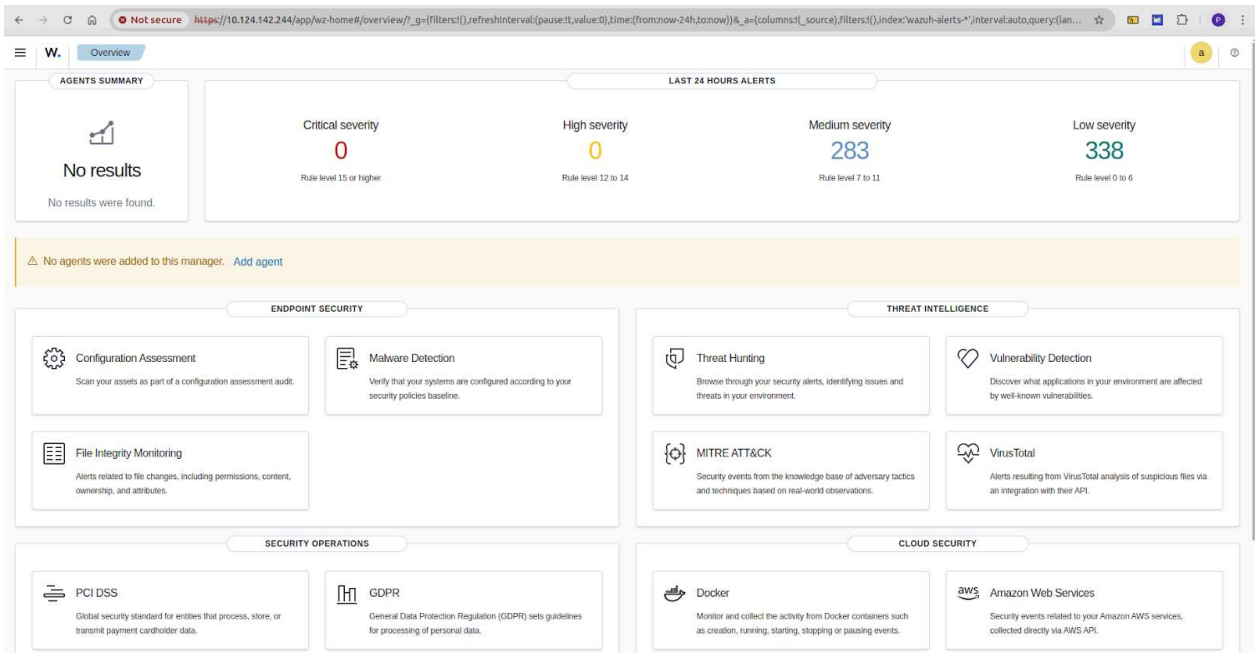
```
hosts:
  - default:
      url: https://10.124.142.244
      port: 55000
      username: wazuh-wui
      password: wazuh-wui
      run_as: false
```

Access the Wazuh web interface with your credentials

URL: https://<WAZUH_DASHBOARD_IP>
Username: admin
Password: admin

URL: https://10.124.142.244/





When you access the Wazuh dashboard for the first time, the browser shows a warning message stating that the certificate was not issued by a trusted authority. An exception can be added in the advanced options of the web browser. For increased security, the root-ca.pem file previously generated can be imported to the certificate manager of the browser. Alternatively, a certificate from a trusted authority can be configured.

Issues Faced and Debugged

At Wazuh Indexer :

```
lokesh@wazuh:~$ sudo systemctl status wazuh-indexer.service
× wazuh-indexer.service - Wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset:
enabled)
     Active: failed (Result: exit-code) since Tue 2024-08-13 03:02:36 UTC; 22s ago
       Docs: https://documentation.wazuh.com
    Process: 619 ExecStart=/usr/share/wazuh-indexer/bin/systemd-entrypoint -p
${PID_DIR}/wazuh-indexer.pid --quiet (code=exited, status=78)
   Main PID: 619 (code=exited, status=78)
        CPU: 28.410s

Aug 13 03:02:30 wazuh systemd-entrypoint[619]: WARNING: System::setSecurityManager has
been called by org.opensearch.bootstrap.Security
(file:/usr/share/wazuh-indexer/lib/opensearch-2.10.0.jar)
Aug 13 03:02:30 wazuh systemd-entrypoint[619]: WARNING: Please consider reporting this to
the maintainers of org.opensearch.bootstrap.Security
Aug 13 03:02:30 wazuh systemd-entrypoint[619]: WARNING: System::setSecurityManager will
be removed in a future release
Aug 13 03:02:36 wazuh systemd-entrypoint[619]: ERROR: [1] bootstrap checks failed
Aug 13 03:02:36 wazuh systemd-entrypoint[619]: [1]: max virtual memory areas
vm.max_map_count [65530] is too low, increase to at least [262144]
Aug 13 03:02:36 wazuh systemd-entrypoint[619]: ERROR: OpenSearch did not exit normally -
check the logs at /var/log/wazuh-indexer/wazuh-cluster.log
Aug 13 03:02:36 wazuh systemd[1]: wazuh-indexer.service: Main process exited, code=exited,
status=78/CONFIG
Aug 13 03:02:36 wazuh systemd[1]: wazuh-indexer.service: Failed with result 'exit-code'.
Aug 13 03:02:36 wazuh systemd[1]: Failed to start Wazuh-indexer.
Aug 13 03:02:36 wazuh systemd[1]: wazuh-indexer.service: Consumed 28.410s CPU time.
```

Go to host system

```
lokesh@cybercub:~$ sysctl vm.max_map_count
vm.max_map_count = 65530
lokesh@cybercub:~$ sudo sysctl -w vm.max_map_count=262144
[sudo] password for lokesh:
vm.max_map_count = 262144
```

To Apply that change while booting
lokesh@cybercub:~$ sudo nano /etc/sysctl.conf
vm.max_map_count = 262144
lokesh@cybercub:~$ sudo sysctl -p
vm.max_map_count = 262144