EBRYX X AKHUWAT

SECURITY PROJECT #02

REPORT NO.1

Submitted By: Khalid Hussain
Muhammad Usama

Date of Submission: 22 Sep, 2024

Installing Wazuh with Elastic Stack

All-in-one deployment

This document guides through an installation of the Wazuh server and Elastic Stack components in an all-in-one configuration

Note: It need root user privileges to run all the commands described below.

Installing prerequisites

Install all the necessary packages:

```
# apt-get install apt-transport-https zip unzip lsb-release curl gnupg
```

Installing Elasticsearch

Elasticsearch is a highly scalable full-text search and analytics engine.

Adding the Elastic Stack repository

1. Install the GPG key:

```
# curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch | gpg --
nodefault-keyring --keyring
gnupgring:/usr/share/keyrings/elasticsearch.gpg --import && chmod 644
/usr/share/keyrings/elasticsearch.gpg
```

2. Add the repository:

```
# echo "deb [signed-by=/usr/share/keyrings/elasticsearch.gpg]
https://artifacts.elastic.co/packages/7.x/apt stable main" | tee
/etc/apt/sources.list.d/elastic-7.x.list
```

3. Update the package information:

```
# apt-get update
```

Elasticsearch installation and configuration

1. Install the Elasticsearch package:

```
# apt-get install elasticsearch=7.17.6
```

.

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

```
# curl -so /etc/elasticsearch/elasticsearch.yml
 https://packages.wazuh.com/4.3/tpl/elastic-basic/elasticsearch_all_in_one.yml
```

Certificates creation and deployment

---

1. Download the configuration file for creating the certificates:

> ```
> # curl -so /usr/share/elasticsearch/instances.yml
> https://packages.wazuh.com/4.3/tpl/elastic-basic/instances_aio.yml
> ```
>
> In the following steps, a file that contains a folder named after the instance defined here will be created. This folder will contain the certificates and the keys necessary to communicate with the Elasticsearch node using SSL.

2. The certificates can be created using the elasticsearch-certutil tool:

> ```
> # /usr/share/elasticsearch/bin/elasticsearch-certutil cert ca --pem --in
> instances.yml --keep-ca-key --out ~/certs.zip
> ```

3. Extract the generated `/usr/share/elasticsearch/certs.zip` file from the previous step.

> ```
> # unzip ~/certs.zip -d ~/certs
> ```

4. The next step is to create the directory `/etc/elasticsearch/certs`, and then copy the CA file, the certificate and the key there:

> ```
> # mkdir /etc/elasticsearch/certs/ca -p
> # cp -R ~/certs/ca/ ~/certs/elasticsearch/* /etc/elasticsearch/certs/
> # chown -R elasticsearch: /etc/elasticsearch/certs
> # chmod -R 500 /etc/elasticsearch/certs
> # chmod 400 /etc/elasticsearch/certs/ca/ca.*
> /etc/elasticsearch/certs/elasticsearch.*
> # rm -rf ~/certs/ ~/certs.zip
> ```

5. Enable and start the Elasticsearch service:

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

6 Generate credentials for all the Elastic Stack pre-built roles and users:

> ```
> # /usr/share/elasticsearch/bin/elasticsearch-setup-passwords auto
> ```
>
> The command above will prompt an output like this. Save the password of the `elastic` user for further steps:
>
> Output
>
> ```
> Changed password for user apm_system
> PASSWORD apm_system = lLPZhZkB6oUOzzCrkLSF
>
> Changed password for user kibana_system
> PASSWORD kibana_system = TaLqVOnSoqKTYLIU0vDn
>
> Changed password for user kibana
> PASSWORD kibana = TaLqVOvXoqKTYLIU0vDn
>
> Changed password for user logstash_system
> PASSWORD logstash_system = UtuDv2tWkXGYL83v9kWA
>
> Changed password for user beats_system
> PASSWORD beats_system = qZcbvCslafMpoEOrE9Ob
>
> Changed password for user remote_monitoring_user
> PASSWORD remote_monitoring_user = LzJpQiSylncmCU2GLBTS
>
> Changed password for user elastic
> PASSWORD elastic = AN4UeQGA7HGl5iHpMla7
> ```

To check that the installation was made successfully, run the following command replacing `<elastic_password>` with the password generated in the previous step for `elastic` user:

`# curl -XGET https://localhost:9200 -u elastic:<elastic_password> -k` This command should have an output like this:

Output

```
{
  "name" : "elasticsearch",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "BgdIyCXxSPGeRusvb6-_Qw",
  "version" : {
    "number" : "7.17.6",
    "build_flavor" : "default",
    "build_type" : "rpm",
    "build_hash" : "f65e9d338dc1d07b642e14a27f338990148ee5b6",
    "build_date" : "2022-08-23T11:08:48.893373482Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
```

```
    .
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Installing Wazuh server

The Wazuh server collects and analyzes data from deployed agents. It runs the Wazuh manager, the Wazuh API and Filebeat. The first step in setting up Wazuh is to add the Wazuh repository to the server.

Adding the Wazuh repository

1. Install the GPG key:

```
# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --nodefault-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg -import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

2. Add the repository:

```
# 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
```

3. Update the package information:

```
# apt-get update
```

Installing the Wazuh manager

1. Install the Wazuh manager package:

```
# apt-get install wazuh-manager=4.3.11-1
```

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 Filebeat

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

Filebeat installation and configuration

1. Install the Filebeat package:

   ```
   # apt-get install filebeat=7.17.6
   ```

2. Download the pre-configured Filebeat config file used to forward Wazuh alerts to Elasticsearch:

   ```
   # curl -so /etc/filebeat/filebeat.yml
   https://packages.wazuh.com/4.3/tpl/elastic-basic/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/4.3/extensions/elasticsear
   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-
   0.2.tar.gz | tar -xvz -C /usr/share/filebeat/module
   ```

5. Edit the file `/etc/filebeat/filebeat.yml` and add the following line:

   ```
   output.elasticsearch.password: <elasticsearch_password>
   ```

   Replace `elasticsearch_password` with the previously generated password for `elastic` user.

6. Copy the certificates into `/etc/filebeat/certs/`

   ```
   # cp -r /etc/elasticsearch/certs/ca/ /etc/filebeat/certs/
   # cp /etc/elasticsearch/certs/elasticsearch.crt
   /etc/filebeat/certs/filebeat.crt
   # cp /etc/elasticsearch/certs/elasticsearch.key
   /etc/filebeat/certs/filebeat.key
   ```

.

7 Enable and start the Filebeat service:

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

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

```
# filebeat test output
```

This command should have an output like this:

Output

```
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: 7.17.6
```

Kibana installation and configuration

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 kibana=7.17.6
```

2. Copy the Elasticsearch certificates into the Kibana configuration folder:

```
# mkdir /etc/kibana/certs/ca -p
# cp -R /etc/elasticsearch/certs/ca/ /etc/kibana/certs/
# cp /etc/elasticsearch/certs/elasticsearch.key
/etc/kibana/certs/kibana.key
# cp /etc/elasticsearch/certs/elasticsearch.crt
/etc/kibana/certs/kibana.crt
# chown -R kibana:kibana /etc/kibana/
# chmod -R 500 /etc/kibana/certs
# chmod 440 /etc/kibana/certs/ca/ca.* /etc/kibana/certs/kibana.*
```

.

3. Download the Kibana configuration file:

```
# curl -so /etc/kibana/kibana.yml
https://packages.wazuh.com/4.3/tpl/elastic-basic/kibana_all_in_one.yml
```

Edit the `/etc/kibana/kibana.yml` file:

`elasticsearch.password:`

`<elasticsearch_password>` Values to be replaced:

`<elasticsearch_password>`: the password generated during the Elasticsearch installation and configuration for the `elastic` user.

4. Create the `/usr/share/kibana/data` directory:

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

5. 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-4.3.11_7.17.6-
1.zip
```

6. Link Kibana's 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 using the password generated during the Elasticsearch installation process:

```
URL: https://<wazuh_server_ip> user:
elastic
password: <PASSWORD_elastic>
```