Documentation › Docker › FAQ

FAQ

How can I tune the Kibana configuration?

The Kibana default configuration is stored in `kibana/config/kibana.yml`.:

```
kibana:
  image: wazuh/wazuh-kibana
  hostname: kibana
  restart: always
  ports:
    - "5601:5601"
  networks:
    - docker_elk
  depends_on:
    - elasticsearch
  environment:
    - "WAZUH_KIBANA_PLUGIN_URL=http://your.repo/wazuhapp-2.0_5.3.0.zip"
  entrypoint: sh wait-for-it.sh elasticsearch
```

How can I tune the Logstash configuration?

The logstash configuration is stored in `logstash/config/logstash.conf`.

The `logstash/config` folder is mapped onto the `/etc/logstash/conf.d` container so that you can create more than one file in that folder if you'd like to. However, you must be aware that config files will be read from that directory in alphabetical order.

How can I specify the amount of memory used by Logstash?

The Logstash container uses the *LS_HEAP_SIZE* environment variable to determine how much memory should be allocated as JVM heap memory (defaults to 2048m).

If you want to override the default configuration, edit the *LS_HEAP_SIZE* environment variable defined in the logstash section of `docker-compose.yml`:

```
logstash:
  image: wazun/wazuh-logstash:latest
  command: -f /etc/logstash/conf.d/
  volumes:
    - ./logstash/config:/etc/logstash/conf.d
  ports:
    - "5000:5000"
  networks:
    - docker_elk
  depends_on:
    - elasticsearch
  environment:
    - LS_HEAP_SIZE=2048m
```

How can I tune the Elasticsearch configuration?

The Elasticsearch container uses the default configuration and it is not exposed by default.

If you want to override the default configuration, create a file `elasticsearch/config/elasticsearch.yml` and put your custom version of the configuration in it.

Then map your configuration file inside the container in the `docker-compose.yml`. Update the elasticsearch container declaration to:

```
elasticsearch:
 image: wazuh/wazuh-elasticsearch:latest
 ports:
   - "9200:9200"
   - "9300:9300"
 environment:
   ES_JAVA_OPTS: "-Xms1g -Xmx1g"
 networks:
   - docker_elk
```

How can I store Wazuh data?

The data stored in Wazuh will persist after container reboots but not after container removal.

In order to preserve Wazuh data even after removing the Wazuh container, you'll have to mount a volume on your Docker host. Update the Wazuh container declaration in the `docker-compose.yml` to look like this:

```
elasticsearch:
  image: wazuh/wazuh:latest
  hostname: wazuh-manager
  ports:
    - "1514:1514/udp"
    - "1515:1515"
    - "514:514"
    - "55000:55000"
  networks:
    - docker_elk
  volumes:
    - /path/to/storage:/var/ossec/data
```

This will store Wazuh data inside */path/to/storage* in the Docker host's local file system.

How can I store Elasticsearch data?

The data stored in Elasticsearch will persist after container reboots but not after container removal.

In order to preserve Elasticsearch data even after removing the Elasticsearch container, you'll have to mount a volume on your Docker host. Update the elasticsearch container declaration in the `docker-compose.yml` file to look like this:

```
elasticsearch:
  image: wazuh/wazuh-elasticsearch:latest
  hostname: elasticsearch
  command: elasticsearch -Des.network.host=_non_loopback_ -Des.cluster.name: my-cluster
  ports:
    - "9200:9200"
    - "9300:9300"
  environment:
    ES_JAVA_OPTS: "-Xms1g -Xmx1g"
  networks:
    - docker_elk
  volumes:
    - /path/to/storage:/usr/share/elasticsearch/data
```

This will store elasticsearch data inside `/path/to/storage` in the Docker host's local file system.