

# Enabling Docker Listener in Wazuh

## To Enable Docker Listener in Wazuh

To maintain the security and compliance of your Docker environment, it is crucial to proactively monitor both your Docker server and containers. The Docker server is the backbone of your container infrastructure and manages the deployment of containers and resource allocation. By monitoring the Docker server, you can keep track of resource usage, unauthorized access attempts, performance issues, and other security concerns.

However, it is not enough to monitor only the Docker server, you also need to monitor the containers themselves. Container monitoring provides insight into the activities of your containers, such as network connections, file system changes, and process executions. Monitoring these activities helps to detect suspicious behavior, identify malware or malicious processes, and respond to security incidents in real-time.

By monitoring both the Docker server and the containers, you can proactively detect and respond to security threats, ensuring the security and compliance of your Docker environment to regulatory standards.

## Wazuh agent configuration

### 1. Install the dependencies on the docker server :

**Run each line Separately**

```
sudo apt-get update && sudo apt-get install python3 -y  
sudo apt-get install python3-pip -y  
pip3 install docker==4.2.0 urllib3==1.26.18
```

## 2. Edit the File using `sudo nano /var/ossec/etc/ossec.conf` and add the following:

```
<!-- Docker Container Runtime configuration -->
<wodle name="docker-listener">
  <interval>10m</interval>
  <attempts>5</attempts>
  <run_on_start>yes</run_on_start>
  <disabled>no</disabled>
</wodle>
```

## 3. To monitor the logs of the container add the text below to the `"<!-- Log analysis -->"` section:

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/lib/docker/containers/*/*-json.log</location>
</localfile>
```

## 4. Restart the wazuh-agent service:

```
sudo systemctl restart wazuh-agent
```

# Wazuh server configuration

## 1. Edit the Decoder File in `/var/ossec/etc/decoders/local_decoder.xml` on the Wazuh Server and add:

```
<decoder name="web-accesslog-docker">
  <parent>json</parent>
  <type>web-log</type>
  <use_own_name>true</use_own_name>
  <prematch offset="after_parent">^log:"\S+ \S+ \S+ \. *[\S+ \S\d+] \. *"\w+ \S+ HTTP\S+"
\d+</prematch>
  <regex offset="after_parent">^log:"(\S+) \S+ \S+ \. *[\S+ \S\d+] \. *"( \w+) ( \S+) HTTP\S+"
```

```
(\d+)</regex>
  <order>srcip,protocol,url,id</order>
</decoder>

<decoder name="json">
  <parent>json</parent>
  <use_own_name>true</use_own_name>
  <plugin_decoder>JSON_Decoder</plugin_decoder>
</decoder>
```

## 2.Restart the Wazuh-Manager:

```
sudo systemctl restart wazuh-manager
```

# Wazuh Docker listener dashboard

The Wazuh Docker listener dashboard offers a centralized and user-friendly interface that allows you to monitor the security of your Dockerized infrastructure. With real-time insights and actionable information, the Wazuh Docker listener dashboard empowers system administrators and security teams to detect and respond to potential threats, ensuring the integrity and reliability of containerized applications. From monitoring container events to analyzing logs and implementing custom rules, this dashboard streamlines the security management process, enhancing the overall protection of your Docker environment.

Take the following steps to enable the Wazuh Docker listener dashboard:

1. Click on the **Wazuh** menu icon, and select **Settings > Modules**.
2. Scroll down to the **Threat Detection and Response** section and enable **Docker listener**.
3. Click on the **Wazuh** menu icon, and select **Modules > Docker listener** to view the Docker listener dashboard.

The animation below is a graphical representation of the steps you need to take to enable the Wazuh Docker listener dashboard.

# Wazuh Docker listener configuration options

In this section, we provide more information about the Wazuh Docker listener and all possible configuration options. The Docker listener has the main options and the scheduling options.

## Main options

The main options allow you to enable or disable the Docker listener, and to configure the number of attempts to rerun the listener in case it fails. The two main options are `disabled` and `attempts`.

### disabled

The `disabled` option allows you to enable or disable the Docker listener.

Default value	no
Allowed values	yes, no

### attempts

The `attempts` option specifies the number of attempts to execute the listener in case it fails.

Default value	5
Allowed values	A positive number

## Scheduling options

The scheduling options allow you to configure when the Docker listener should execute. The available scheduling options are `run_on_start`, `interval`, `day`, `wday`, and `time`. The Docker listener runs on start by default when enabled without any scheduling options.

## run\_on\_start

Run the Docker listener immediately when the Wazuh agent starts.

Default value	yes
Allowed values	yes, no

## interval

Waiting time to rerun the Docker listener in case it fails.

Default value	1m
Allowed values	A positive number that should contain a suffix character indicating a time unit, such as s (seconds), m (minutes), h (hours), d (days), M (months).

## day

Day of the month to run the scan.

Default value	n/a
Allowed values	Day of the month [1..31]

### Note

When the `day` option is set, the interval value must be a multiple of months. By default, the interval is set to a month.

## wday

Day of the week to run the scan. This option is *not compatible* with the `day` option.

Default value	n/a
---------------	-----

Allowed values	Day of the week: <ul style="list-style-type: none"><li>• sunday/sun</li><li>• monday/mon</li><li>• tuesday/tue</li><li>• wednesday/wed</li><li>• thursday/thu</li><li>• friday/fri</li><li>• saturday/sat</li></ul>
----------------	---

Note

When the `wday` option is set, the interval value must be a multiple of weeks. By default, the interval is set to a week.

time

Time of the day to run the scan. It has to be represented in the format hh:mm.

Default value	n/a
Allowed values	Time of day <i>[hh:mm]</i>

Note

When only the `time` option is set, the interval value must be a multiple of days or weeks. By default, the interval is set to a day.

# Example configuration

The example configuration below shows an enabled Docker listener. The listener attempts to execute five times at ten-minute intervals if it fails

```
<wodle name="docker-listener">
  <interval>10m</interval>
  <attempts>5</attempts>
  <run_on_start>no</run_on_start>
  <disabled>no</disabled>
</wodle>
```

