Wazuh container

Requirements

Increase max_map_count on your host (Linux)

You need to increase `max_map_count` on your Docker host:

```
$ sudo sysctl -w vm.max_map_count=262144
```

To set this value permanently, update the vm.max_map_count setting in `/etc/sysctl.conf`. To verify after rebooting, run “sysctl vm.max_map_count”.

⚠ Warning

If you don’t set the **max_map_count** on your host, Elasticsearch will probably don’t work.

Increase max_map_count on your host (Windows)

You need to increase `max_map_count` on your Docker host:

```
$ docker-machine ssh default
$ sudo sysctl -w vm.max_map_count=262144
$ exit
```

To set this value permanently, update the vm.max_map_count setting in `/var/lib/boot2docker/profile`:

```
$ docker-machine ssh default
$ sudo vi /var/lib/boot2docker/bootlocal.sh
```

Add the following line into the profile file:

```
sysctl -w vm.max_map_count=262144
```

Make the script runneable:

```
$ sudo chmod +x /var/lib/boot2docker/bootlocal.sh
```

To verify after rebooting, run “sysctl vm.max_map_count”.

⚠ Warning

If you don’t set the **max_map_count** on your host, Elasticsearch will probably don’t work.

SELinux

On distributions which have SELinux enabled out-of-the-box, you will need to either re-context the files or put SELinux into Permissive mode for docker-elk to start properly. For example, on Red Hat and CentOS the following command will apply the proper context

```
# chcon -R system_u:object_r:admin_home_t:s0 docker-elk/
```

Docker for OSX

In Docker for OSX, there is a default memory limit of 2GB, in order to run *docker-compose up* successfully you have to change default memory settings from 2GB to at least 4 or 5GB. To do so, click on the Docker icon in the menu bar, then “Preferences...”, go to “Advanced” tab and set 5GB of memory, then click on “Apply & Restart” and run *docker-compose up*.

Usage

1. Copy the *docker-compose* file to your system:

```
$ curl -so docker-compose.yml https://raw.githubusercontent.com/wazuh/wazuh-docker/master/docker-compose.yml
```

2. Start Wazuh and Elastic Stack using *docker-compose*:

a. Foreground:

```
$ docker-compose up
```

b. Background:

```
$ docker-compose up -d
```

Then access the Kibana UI by hitting http://localhost:5601 with a web browser.

By default, the stack exposes the following ports:

1514	Wazuh UDP
1515	Wazuh TCP
514	Wazuh UDP
55000	Wazuh API
5000	Logstash TCP input
9200	Elasticsearch HTTP
9300	Elasticsearch TCP transport
5601	Kibana

Note

Configuration is not dynamically reloaded, so you will need to restart the stack after any change in the configuration of a component.