Virtual Machine

We provide a pre-built virtual machine image (OVA), you can directly import using VirtualBox (where has been built it) and other OVA compatible virtualization system as well.

> **Note**
>
> This VM only run on 64-bit systems and is not recommended to use in production environments. Instead, it can be a useful tool for proof of concepts and labs. Distributed architectures and multi-node Elastic Stack clusters are usually a better fit for production environments, where higher performance is required.

1. This virtual appliance, available at https://packages.wazuh.com/vm/wazuh2.1.1_5.6.3.ova, contains the following components:

   - CentOS 7
   - Wazuh 2.1.1-1
   - RESTful API 2.1.1-1
   - Elasticsearch 5.6.3
   - Logstash 5.6.3
   - Kibana 5.6.3 port "**5601**""
   - WazuhAPP 2.1.1_5.6.3

2. Import the OVA in your virtualization platform, and run the virtual machine. The root password is "**wazuh**" and the username/password for the Wazuh API is "**foo/bar**".

   Although you don't need to change any Elastic Stack configuration settings, feel free to explore the options. You can find Elasticsearch installed in `/usr/share/elasticsearch`. Similarly, Logstash is installed in `/usr/share/logstash` and its config directory is `/etc/logstash/conf.d/`.

3. **Wazuh Manager** and the **Elastic Stack** are configured to work out of the box. You can now deploy the Wazuh agents, on those systems that you intend to monitor, and connect them to your virtual appliance. More documentation at:

   - How to install Wazuh agents.

   > **Warning**
   >
   > Before connecting any Wazuh agent, change the VM's network interface type from NAT (the factory default) to bridge for be reachable to your network. By default, the VM will try to get an IP address from your network's DHCP server. Alternatively, you can set a static IP address by configuring the proper network files on the CentOS operating system where it's this virtual machine based on.

4. You can start and stop wazuh-manager, elasticsearch, logstash, and kibana with the 'systemctl' command. Examples:

```
$ systemctl restart wazuh-manager
$ systemctl stop elasticsearch
$ systemctl start logstash
$ systemctl status kibana
```

5. In order to connect to Kibana web user interface, you can login with `http://OVA_IP_ADRESS:5601` (where `OVA_IP_ADDRESS` is your system IP).