Steps to deploy Wazuh on Rhel

Note: These scripts have been tested for Wazuh 3.8.2 and ELK 6.5.4 on rhel 7.6

Step 1:

Install wazuh manager and wauh-api by running wazuh.sh script on server machine. The script will ask for configuration related inputs**. Refer Step 4** under https://documentation.wazuh.com/current/installation-guide/installing-wazuh-server/sources_installation.html#installing-wazuh-manager for further details.

```
$ bash wazuh.sh          #manager/agent
```

The script will prompt for which component you want to install, run the script twice for manager and api:

```
1-  What kind of installation do you want (manager, agent, local, hybrid or help)? manager
```

After successful installation

```
- To start Wazuh:       /var/ossec/bin/ossec-control start

- To stop Wazuh:       /var/ossec/bin/ossec-control stop

- The configuration can be viewed or modified at /var/ossec/etc/ossec.conf
```

```
$ bash wazuh_api.sh   #api
```

Step 2:

Install ELT stack by running elasticsearch.sh, logstash.sh and kibana.sh scripts. All the 3 scripts require one command line argument stating the directory of installation. Check this link for wazuh version and ELK version compatibility.

```
$ bash elasticsearch.sh /root/elk-stack
$ bash logstash.sh /root/elk-stack
$ bash kibana.sh /root/elk-stack
$ sudo -u elasticsearch /usr/share/elasticsearch/bin/elasticsearch &
$ cd /root/elk-stack/kibana/bin/kibana &
$ /root/elk-stack/logstash/bin/logstash -e 'input { stdin { } } output { stdout {} }' &
```

Step 3:

Install wazuh-agent by running wazuh.sh script on the client machine.

```
$ bash wazuh.sh
```

The script will prompt for which component you want to install, type agent. You will also need to enter the IP address of machine where wazuh-manager is installed:

```
1-  What kind of installation do you want (manager, agent, local, hybrid or help)? agent

3- Configuring Wazuh.
```

```
  3.1- What's the IP Address or hostname of the Wazuh server?: X.X.X.X
```

Register agent with server using steps mentioned here https://documentation.wazuh.com/current/user-manual/registering/cli/using-command-line-linux.html

Step 4:

Load kibana's dashboard through browser at http://localhost:5601. You will be able to see wazuh app in the left hand side menu.

Common Issues:

Issue 1:

Checking active connection between wazuh manager and agent showing Never Connected.

Solution:

Restart both wazuh manager and agent using following commands.

```
$ /var/ossec/bin/ossec-control stop
$ /var/ossec/bin/ossec-control start
```

Issue 2:

Not able to access kibana through browser.

Solution:

Edit **config/kibana.yml** file to uncomment and change line **server.host: "localhost"** to **server.host: "0.0.0.0".**

Issue 3:

Connect logstash with elasticsearch

Solution:

To connect logstash to filebeat and elasticsearch we need to pass **logstash.conf** file to the binary using the **-f** option present here. https://github.com/wazuh/wazuh/blob/v3.8.2/extensions/logstash/01-wazuh-local.conf

```
$./bin/logstash -f logstash.conf
```

For installing filebeat run the filebeat.sh script.