Install Elastic Stack with RPM packages

The RPM packages are suitable for installation on Red Hat, CentOS and other RPM-based systems.

Note

Many of the commands described below need to be executed with root user privileges.

Preparation

1. Oracle Java JRE is required by Logstash and Elasticsearch.

Note

The following command accepts the necessary cookies to download Oracle Java JRE. Please, visit Oracle Java 8 JRE Download Page for more information.

```
$ curl -Lo jre-8-linux-x64.rpm --header "Cookie: oraclelicense=accept-securebackup-cookie"
"https://download.oracle.com/otn-pub/java/jdk/8u191-b12/2787e4a523244c269598db4e85c51e0c/jre-8u191-linux-
x64.rpm"
```

Now check if the package was download successfully:

```
$ rpm -qlp jre-8-linux-x64.rpm > /dev/null 2>&1 && echo "Java package downloaded successfully" || echo
"Java package did not download successfully"
```

Finally, install the RPM package using yum:

```
$ yum install jre-8-linux-x64.rpm
$ rm jre-8-linux-x64.rpm
```

2. Install the Elastic repository and its GPG key:

```
$ rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch

$ cat > /etc/yum.repos.d/elastic.repo << EOF
[elastic-5.x]
name=Elastic repository for 5.x packages
baseurl=https://artifacts.elastic.co/packages/5.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
EOF
```

Elasticsearch

Elasticsearch is a highly scalable full-text search and analytics engine. For more info please see Elasticsearch.

1. Install the Elasticsearch package:

```
$ yum install elasticsearch-5.6.5
```

2. Enable and start the Elasticsearch service:

a. For Systemd:

```
$ systemctl daemon-reload
$ systemctl enable elasticsearch.service
$ systemctl start elasticsearch.service
```

b. For SysV Init:

```
$ chkconfig --add elasticsearch
$ service elasticsearch start
```

3. Load Wazuh Elasticsearch template:

```
$ curl https://raw.githubusercontent.com/wazuh/wazuh-kibana-
app/2.1/server/startup/integration_files/template_file.json | curl -XPUT
'http://localhost:9200/_template/wazuh' -H 'Content-Type: application/json' -d @-
```

4. Insert sample alert:

```
$ curl https://raw.githubusercontent.com/wazuh/wazuh-kibana-
app/2.1/server/startup/integration_files/alert_sample.json | curl -XPUT "http://localhost:9200/wazuh-
alerts-"`date +%Y.%m.%d`"/wazuh/sample" -H 'Content-Type: application/json' -d @-
```

Note

It is recommended to edit the default configuration to improve the Elasticsearch performance. To do so, please see Elasticsearch tuning.

Logstash

Logstash is the tool that will collect, parse, and forward to Elasticsearch for indexing and storage all logs generated by Wazuh server. For more info please see Logstash.

1. Install the Logstash package:

```
$ yum install logstash-5.6.5
```

2. Download the Wazuh config for Logstash:

```
$ curl -so /etc/logstash/conf.d/01-wazuh.conf
https://raw.githubusercontent.com/wazuh/wazuh/2.1/extensions/logstash/01-wazuh.conf
```

3. Download the Wazuh Logstash template:

```
$ curl -so /etc/logstash/wazuh-elastic5-template.json
https://raw.githubusercontent.com/wazuh/wazuh/2.1/extensions/elasticsearch/wazuh-elastic5-template.json
```

4. **Follow this step only if you are using a single-host architecture**:

a. Edit `/etc/logstash/conf.d/01-wazuh.conf`, commenting out the entire input section titled “Remote Wazuh Manager - Filebeat input” and uncommenting the entire input section titled “Local Wazuh Manager - JSON file input”. This will set up Logstash to read the Wazuh `alerts.json` file directly from the local filesystem rather than expecting Filebeat on a separate server to forward the information in that file to Logstash.

b. Because the Logstash user needs to read alerts.json file, please add it to OSSEC group by running:

```
$ usermod -a -G ossec logstash
```

Note

Follow the next steps if you use CentOS-6/RHEL-6 or Amazon AMI (logstash uses Upstart like service manager and need to be fixed, see bug)

```
1) Edit the file /etc/logstash/startup.options and in the line 30 change the LS_GROUP=logstash to
LS_GROUP=ossec.
2) Update the service with the new parameters run the command /usr/share/logstash/bin/system-install
3) Start Logstash again.
```

5. Enable and start the Logstash service:

a. For Systemd:

```
$ systemctl daemon-reload
$ systemctl enable logstash.service
$ systemctl start logstash.service
```

b. For SysV Init:

```
$ chkconfig --add logstash
$ service logstash start
```

Note

If you are running Wazuh server and the Elastic Stack server on separate systems (**distributed architecture**), then it is important to configure encryption between Filebeat and Logstash. To do so, please see Setting up SSL for Filebeat and Logstash.

Kibana

Kibana is a flexible and intuitive web interface for mining and visualizing the events and archives stored in Elasticsearch. More info at Kibana.

1. Install the Kibana package:

```
$ yum install kibana-5.6.5
```

2. Install the Wazuh App plugin for Kibana:

```
$ /usr/share/kibana/bin/kibana-plugin install https://packages.wazuh.com/wazuhapp/wazuhapp-
2.1.1_5.6.5.zip
```

Warning

The Kibana plugin installation process may take several minutes. Please wait patiently.

3. **Optional.** Kibana will listen only on the loopback interface (localhost) by default. To set up Kibana to listen on all interfaces, edit the file `/etc/kibana/kibana.yml`. Uncomment the setting `server.host` and change the value to:

```
server.host: "0.0.0.0"
```

Note

It is recommended to set up an Nginx proxy for Kibana in order to use SSL encryption and to enable authentication. Instructions to set the proxy up can be found at Setting up SSL and authentication for Kibana.

4. Enable and start the Kibana service:

a. For Systemd:

```
$ systemctl daemon-reload
$ systemctl enable kibana.service
$ systemctl start kibana.service
```

b. For SysV Init:

```
$ chkconfig --add kibana
$ service kibana start
```

5. Disable the Elasticsearch repository:

We recommend to disable the Elasticsearch repository in order to prevent an upgrade to a newer Elastic Stack version due to possible breaking changes with our App, so you should do it as follow:

```
$ sed -i "s/^enabled=1/enabled=0/" /etc/yum.repos.d/elastic.repo
```

Connecting the Wazuh App with the API

Follow the next guide in order to connect the Wazuh App with the API:

- Connect the Wazuh App with the API