Install Wazuh server with RPM packages

For CentOS/RHEL/Fedora platforms, installing Wazuh server components is just install relevant packages by previously adding the appropriate repositories.

Note

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

Adding the Wazuh repository

The first thing you need is to add the Wazuh repository to your server. Alternatively, if you prefer to download the wazuh-manager package directly, you can find it here.

To set up the repository, run the command that corresponds to your specific RPM-based Linux distribution:

a. For CentOS:

```
$ cat > /etc/yum.repos.d/wazuh.repo <<\EOF
[wazuh_repo]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=CentOS-$releasever - Wazuh
baseurl=https://packages.wazuh.com/yum/el/$releasever/$basearch
protect=1
EOF
```

b. For RHEL:

```
$ cat > /etc/yum.repos.d/wazuh.repo <<\EOF
[wazuh_repo]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=RHEL-$releasever - Wazuh
baseurl=https://packages.wazuh.com/yum/rhel/$releasever/$basearch
protect=1
EOF
```

c. For Fedora:

```
$ cat > /etc/yum.repos.d/wazuh.repo <<\EOF
[wazuh_repo]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
name=Fedora-$releasever - Wazuh
enabled=1
baseurl=https://packages.wazuh.com/yum/fc/$releasever/$basearch
protect=1
EOF
```

d. For Amazon Linux:

```
$ cat > /etc/yum.repos.d/wazuh.repo <<\EOF
[wazuh_repo]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=Amazon Linux - Wazuh
baseurl=https://packages.wazuh.com/yum/el/7/$basearch
protect=1
EOF
```

Installing Wazuh manager

The next will install Wazuh manager on your system:

```
$ yum install wazuh-manager
```

Once the process is completed, you can check the service status with:

a. For Systemd:

```
$ systemctl status wazuh-manager
```

b. For SysV Init:

```
$ service wazuh-manager status
```

Installing Wazuh API

1. NodeJS >= 4.6.1 is required in order to run the Wazuh API. If you do not have NodeJS installed, or your version is older than 4.6.1, we recommend you add the official NodeJS repository like this:

```
$ curl --silent --location https://rpm.nodesource.com/setup_6.x | bash -
```

and then, install nodejs:

```
$ yum install nodejs
```

2. Install the Wazuh API. It will update NodeJS if it is required:

```
$ yum install wazuh-api
```

3. Once the process is completed, you can check the service status with:

a. For Systemd:

```
$ systemctl status wazuh-api
```

b. For SysV Init:

```
$ service wazuh-api status
```

4. Python >= 2.7 is required in order to run the Wazuh API. It is installed by default or included in the official repositories in most Linux distributions.

   It is possible to set a custom Python path for the API in `/var/ossec/api/configuration/config.js`, in case the stock version of Python in your distro is too old:

```
config.python = [
    // Default installation
    {
        bin: "python",
        lib: ""
    },
    // Package 'python27' for CentOS 6
    {
        bin: "/opt/rh/python27/root/usr/bin/python",
        lib: "/opt/rh/python27/root/usr/lib64"
    }
];
```

CentOS 6 and Red Hat 6 come with Python 2.6, you can install Python 2.7 in parallel maintaining older version:

a. For CentOS 6:

```
$ yum install -y centos-release-scl
$ yum install -y python27
```

b. For RHEL 6:

```
$ yum install python27

# You may need to first enable a repository in order to get python27, with a command like this:
#   yum-config-manager --enable rhui-REGION-rhel-server-rhscl
#   yum-config-manager --enable rhel-server-rhscl-6-rpms
```

Installing Filebeat

Filebeat is the tool on the Wazuh server that will securely forward the alerts and archived events to the Logstash service on the Elastic Stack server(s).

⚠ Warning

In a single-host architecture (where Wazuh server and Elastic Stack are installed in the same system), you may entirely skip installing Filebeat, since Logstash will be able to read the event/alert data directly from the local filesystem without the assistance of a forwarder.

The RPM package is suitable for installation on Red Hat, CentOS and other modern RPM-based systems.

1. Install the GPG keys from Elastic, and the Elastic repository:

```
$ 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
```

2. Install Filebeat:

```
$ yum install filebeat-5.6.5
```

3. Download the Filebeat config file from the Wazuh repository, which is preconfigured to forward Wazuh alerts to Logstash:

```
$ curl -so /etc/filebeat/filebeat.yml
https://raw.githubusercontent.com/wazuh/wazuh/2.1/extensions/filebeat/filebeat.yml
```

4. Edit the file `/etc/filebeat/filebeat.yml` and replace `ELASTIC_SERVER_IP` with the IP address or the hostname of the Elastic Stack server. For example:

```
output:
  logstash:
    hosts: ["ELASTIC_SERVER_IP:5000"]
```

5. Enable and start the Filebeat service:

   a. For Systemd:

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

   b. For SysV Init:

```
$ chkconfig --add filebeat
$ service filebeat start
```

Next steps

Once you have installed the manager, API and Filebeat (only needed for distributed architectures), you are ready to install Elastic Stack.