Documentation › Installation guide › Installing Wazuh server › Install Wazuh server with DEB packages

Install Wazuh server with DEB packages

For Debian/Ubuntu 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 Wazuh Repositories

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.

1. In order to perform this procedure properly, packages `curl`, `apt-transport-https` and `lsb-release` must be installed into your system. If they are not, install them:

```
$ apt-get update
$ apt-get install curl apt-transport-https lsb-release
```

2. Install the GPG key:

```
$ curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
```

3. Getting the distribution codename and adding the repository:

```
$ CODENAME=$(lsb_release -cs)
$ echo "deb https://packages.wazuh.com/apt $CODENAME main" | tee /etc/apt/sources.list.d/wazuh.list
```

These are the supported codename values:

- For Debian: wheezy, jessie, stretch and sid
- For Ubuntu: trusty, vivid, wily, xenial and yakkety

4. Update the package information:

```
$ apt-get update
```

Installing Wazuh Manager

On your terminal, install the Wazuh manager:

```
$ apt-get 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 -sL https://deb.nodesource.com/setup_6.x | sudo -E bash -
```

and then, install nodejs:

```
$ apt-get install nodejs
```

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

```
$ apt-get 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 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"
    }
];
```

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 DEB package is suitable for Debian, Ubuntu, and other Debian-based systems.

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

```
$ curl -s https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
$ echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | tee
/etc/apt/sources.list.d/elastic-5.x.list
$ apt-get update
```

2. Install Filebeat:

```
$ apt-get 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:

```
$ update-rc.d filebeat defaults 95 10
$ 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.