Installing Elastic Stack

This guide describes the installation of an Elastic Stack server composed by Logstash, Elasticsearch, and Kibana. We will illustrate package-based installations of these components. You can also install them from binary tarballs, however, this is not preferred or supported under Wazuh documentation.

In addition to Elastic Stack components, you will also find here the instructions to install and configure the Wazuh App (deployed as a Kibana plugin).

Depending on your operating system you can choose to install Elastic Stack from RPM or DEB packages. Consult the table below and choose how to proceed:

Type	Description
RPM packages	Install Elastic Stack on CentOS/RHEL/Fedora.
DEB packages	Install Elastic Stack on Debian/Ubuntu.