ElastiFlow

2-step Installation

View latest version

---

1. Execute installation script

```
sudo bash -c "$(wget -qLO -
https://raw.githubusercontent.com/elastiflow/ElastiFlow-Tools/m
ain/docker_install/install.sh)"
```

2. Install dashboards

1. Download this dashboards file to your local machine.
2. Log in to `Kibana`.
3. Click menu, "`Stack Management`", then under the heading "`Kibana`", click "`Saved Objects`"
4. Browse for and upload the `ndjson` file you downloaded. Choose "`import`" and "`overwrite`".

Prerequisites:

- Internet connected, clean Ubuntu 22 (or greater) Linux server with admin access
- Ubuntu VM should have access to 16 GB of RAM, 8 CPU cores, and 500 GB of disk space. This will allow you to store roughly 1 month of flow data at 500 FPS

Optional Enrichments:

ElastiFlow is able to enrich flow records with many different pieces of data, making those records even more valuable, from app id, to threat information, geolocation, DNS hostnames, and more. Please click here for information on how to enable various enrichments. More enrichments and functionality are available with a free basic license. You can also request a 30-day premium license which unlocks even more.