**Elastalert**

git clone https://github.com/Yelp/elastalert.git

cd elastalert

sudo pip3.8 install "setuptools>=11.3"

sudo pip3.8 install pyOpenSSL

sudo python3.8 setup.py install

sudo pip3.8 install "elasticsearch>=5.0.0"

cp config.example.yaml config.yaml

Edit config.yaml

update es\_host with IP address or dns name of the elasticsearch server

elastalert-create-index

Configure example\_rules/example\_frequency.yaml

nano example\_rules/example\_frequency.yaml

**Testing a rule**

Python3.8 -m elastalert.elastalert --verbose --rule example\_frequency.yaml