**Monitoring elasticsearch logs with Graylog**

**Installing Graylog:**

Run [this](https://raw.githubusercontent.com/bedapudi6788/Python-scripts/master/es-graylog/graylog_install.sh) bash script.

Make sure you have MongoDB and ElasticSearch installed

Add the following lines to your elasticsearch.yml file

cluster.name: cluster\_name (This name should be the same here and in graylog’s config)

network.host: 0.0.0.0

discovery.zen.ping.unicast.hosts: ["ip:tcp\_port"] (keep the ip and port (tcp port) of graylog server here)

Configure admin password for graylog by running the following commands

SECRET=$(pwgen -s 96 1)

sudo -E sed -i -e 's/password\_secret =.\*/password\_secret = '$SECRET'/' /etc/graylog/server/server.conf

PASSWORD=$(echo -n YOUR\_PASSWORD | shasum -a 256 | awk '{print $1}')

sudo -E sed -i -e 's/root\_password\_sha2 =.\*/root\_password\_sha2 = '$PASSWORD'/' /etc/graylog/server/server.conf

Add the following lines to your graylog config file

is\_master = true

rest\_transport\_uri = http://127.0.0.1:12900/

elasticsearch\_shards = 1 (or number of shards you have/want)

elasticsearch\_replicas = 0

elasticsearch\_index\_prefix = graylog

elasticsearch\_cluster\_name = cluster\_name

elasticsearch\_discovery\_zen\_ping\_unicast\_hosts = ip:port ( here ip and port are of elasticsearch’s ip and tcp port)

Now, start graylog service and login with username: admin and password: YOUR\_PASSWORD and add a new user with timezone as UTC +5:30 and create a new GELF UDP input in system/inputs after logging in as the newly created user.

Run the [Python script](https://raw.githubusercontent.com/bedapudi6788/Python-scripts/master/es-graylog/es-graylog.py) and it monitors all log files and sends the messages to graylog