Graylog Installation AWS Ubuntu 16.04

<http://docs.graylog.org/en/2.4/pages/installation/os/ubuntu.html>

First Install Oracle Java 8

**MongoDB**

**sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv 2930ADAE8CAF5059EE73BB4B58712A2291FA4AD5**

**echo "deb [ arch=amd64,arm64 ] https://repo.mongodb.org/apt/ubuntu xenial/mongodb-org/3.6 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-3.6.list**

**sudo apt-get update**

**sudo apt-get install -y mongodb-org**

**sudo systemctl daemon-reload  
sudo systemctl enable mongod.service  
sudo systemctl restart mongod.service**

**ElasticSearch**

**Graylog 2.4.x should be used with Elasticsearch 5.x.**

**wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -  
 echo "deb https://artifacts.elastic.co/packages/5.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-5.x.list  
 sudo apt-get update && sudo apt-get install elasticsearch**

**Make sure to modify the** [**Elasticsearch configuration file**](https://www.elastic.co/guide/en/elasticsearch/reference/5.6/settings.html#settings) **(/etc/elasticsearch/elasticsearch.yml) and set the cluster name to graylog additionally you need to uncomment (remove the # as first character) the line:**

**cluster.name: graylog**

**After you have modified the configuration, you can start Elasticsearch:**

**$ sudo systemctl daemon-reload  
$ sudo systemctl enable elasticsearch.service  
$ sudo systemctl restart elasticsearch.service**

**GrayLog**

**wget https://packages.graylog2.org/repo/packages/graylog-2.4-repository\_latest.deb  
 sudo dpkg -i graylog-2.4-repository\_latest.deb  
sudo apt-get update && sudo apt-get install graylog-server**

**apt-get install pwgen**

**pwgen -N 1 -s 96**

**Copy Code to the /etc/graylog/server/server.conf**

**echo -n mypassword | sha256sum**

**Find password\_secret =, copy and paste the password generated through pwgen command. Find root\_password\_sha2 =, copy and paste the converted SHA 256-bit hash of your admin password. Find #root\_email =, uncomment and provide your email address. Uncomment and set your time zone at root\_timezone.**

**Vi /etc/graylog/server/server.conf**

**rest\_listen\_uri =** [**http://17\*.3\*.2\*.1\*2:9000/api/**](http://17*.3*.2*.1*2:9000/api/) **[server private ip address]**

**rest\_transport\_uri =** [**http://5\*.1.1\*.5:9000/api/**](http://5*.1.1*.5:9000/api/) **[server public ip address]**

**web\_listen\_uri =** [**http://17\*.3\*.2\*.1\*2:9000/**](http://17*.3*.2*.1*2:9000/) **[server private ip address]**

**sudo systemctl daemon-reload  
$ sudo systemctl enable graylog-server.service  
$ sudo systemctl start graylog-server.service**