**GRAYLOG Configuration**

**Graylog is an open-source log management tool that**

**helps you to collect, index and analyze any machine logs centrally.**

**Graylog is a free and open source log management tool based on Java,**

**Elasticsearch and MongoDB that can be used to collect,**

**index and analyze any server log from a centralized location.**

**You can easily monitor the SSH logins and unusual activity for**

**debugging applications and logs using Graylog. Graylog provides a powerful query language,**

**alerting abilities, a processing pipeline for data transformation and much more.**

**Components**

**(1) MongoDB – Acts as a database, stores the configurations and meta information.**

**(2) Elasticsearch – It stores the log messages and offers a searching facility.**

**It is recommended to allocate more memory and use SAS or SAN disks**

**for Elasticsearch nodes. Here, where all your searching happens.**

**(3) Graylog Server – Log Parser. It collects the logs from various inputs and**

**provides output to a built-in web interface for managing the logs.**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Configuration\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_Install Elasticsearch\_\_\_\_**

**Elasticsearch is one of the main components which requires Graylog to run, acts as a search server,**

**offers a real-time distributed search and analytics with the RESTful web interface.**

**Elasticsearch stores all the logs sent by the Graylog server and displays the messages whenever user**

**request over the built-in web interface.**

**Elasticsearch is a java based application. Install OpenJDK or Oracle JDK on your machine**

sudo apt update

sudo apt install -y apt-transport-https openjdk-8-jre-headless uuid-runtime pwgen curl dirmngr

**Download and install the GPG signing key.**

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add

**Set up Elasticsearch repository by running below command.**

echo "deb https://artifacts.elastic.co/packages/6.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-6.x.list

sudo apt update

apt install -y elasticsearch

systemctl enable elasticsearch

**The only important thing is to set a cluster name as graylog.**

**Edit the configuration file of Elasticsearch**

vi /etc/elasticsearch/elasticsearch.yml

*cluster.name: graylog (line 17)*

systemctl restart elasticsearch

**\_\_\_\_Install MongoDB\_\_\_\_**

**Download and install the latest version of MongoDB from the official website.**

**Import the public key on the terminal to begin**.

sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv 9DA31620334BD75D9DCB49F368818C72E52529D4

echo "deb [ arch=amd64 ] https://repo.mongodb.org/apt/ubuntu bionic/mongodb-org/4.0 multiverse" | sudo tee /etc/apt/sources.list.d/mongodb-org-4.0.list

apt update

apt install -y mongodb-org

systemctl start mongod

systemctl enable mongod

**\_\_\_\_Install Graylog\_\_\_**

**Graylog Server accepts and processes the log messages and then displays it for the**

**requests that come from the graylog web interface.**

**Download and Install graylog 3.x repository.**

wget https://packages.graylog2.org/repo/packages/graylog-3.0-repository\_latest.deb

sudo dpkg -i graylog-3.0-repository\_latest.deb

sudo apt update

apt install -y graylog-server

**\_\_\_\_Configure Graylog\_\_\_\_**

**You must set a secret to secure the user passwords. Use the pwgen command to the same.**

pwgen -N 1 -s 96

*fGoTI07CooB6xNy5sdPVSKSuq6QSu2QyWf6G9z3haolgwbERTQ9ZbfbF6hxRYbJMMAlEZX7CXHxJLBkNyfM0420u8aFuZy9M (output)*

vi /etc/graylog/server/server.conf

password\_secret = *fGoTI07CooB6xNy5sdPVSKSuq6QSu2QyWf6G9z3haolgwbERTQ9ZbfbF6hxRYbJMMAlEZX7CXHxJLBkNyfM0420u8aFuZy9M*

**You will need this password to login into the Graylog web interface.**

**Admin’s password can’t be changed using the web interface.**

**So, you must edit this variable to set.**

echo -n temp123 | sha256sum

*e3c652f0ba0b4801205814f8b6bc49672c4c74e25b497770bb89b22cdeb4e951 (output)*

vi /etc/graylog/server/server.conf

*root\_password\_sha2 = 0a19533d8eae0719d0e75b3cfb2d80808111b7612756418145cc7103e621f352 -*

*root\_timezone = UTC*

*http\_bind\_address = 192.168.72.91:9000*

**Restart Graylog service.**

systemctl restart graylog-server

systemctl enable graylog-server

**You can check out the server startup logs, and it will be useful for you to**

**troubleshoot Graylog in case of an issue.**

tail -f /var/log/graylog-server/server.log

*2019-02-22T10:07:49.398+05:30 INFO [ServerBootstrap] Graylog server up and running. (output)*

**\_\_\_\_Access Graylog\_\_\_\_**

**The web interface will now be listening on port 9000.**

http://192.168.72.91:9000

**Login with username admin and the password you configured at root\_password\_sha2 on server.conf.**

**\_\_\_\_Create Graylog Inputs\_\_\_\_**

Click System >> Inputs >> select Syslog UDP and then click Launch new input.

Fill with the values and then click Save.

Node: Select your Graylog Node

Title: Name your input

Bind address: 0.0.0.0 (Leave the default one)

Port: 5140

**\_\_\_\_Configure Rsyslog\_\_\_**

**Once you have created the inputs, configure Rsyslog or forward any system logs to your Graylog server.**

**Edit the Rsyslog configuration file.**

vi /etc/rsyslog.conf

**At the bottom of the file, add the following so messages will forward:**

*\*.\* @127.0.0.1:5140;RSYSLOG\_SyslogProtocol23Format*

sudo service rsyslog status

sudo service rsyslog restart

**Wait for a few minutes. You should start receiving log messages from the client**

**machine when the event is generated.**

**(Graylog console >> Search).**

**useful links**

<https://www.itzgeek.com/how-tos/linux/ubuntu-how-tos/how-to-install-graylog-on-ubuntu-16-04.html>

<https://computingforgeeks.com/manage-logs-with-graylog-server-on-ubuntu-18-04/>