1. *Graylog is an open-source log management tool that helps you to collect, index and analyze any machine logs centrally.*
2. *Graylog is a free and open source log management tool based on Java, Elastic search and MongoDB that can be used to collect, index and analyze any server log from a centralized location.*
3. *You can easily monitor the SSH logins and unusual activity for debugging applications and logs using Graylog.*

***Components used in graylog,***

**Mongo DB – Acts as a database, stores the configurations and meta information.**

**Elastic search – It stores the log messages and offers a searching facility. It is recommended to allocate more memory and use SAS or SAN disks Elastic search nodes. Here, where all your searching happens.**

**Gray log Server – Log Parser. It collects the logs from various inputs and provides output to a built-in web interface for managing the logs.**

***Now Install Elastic search***

Elastic search stores all the logs sent by the Gray log server and display the messages whenever user request over the built-in web interface.

Elastic search is a java based application. Install Open JDK or Oracle JDK on your machine.

apt update

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

***Now install the GPG 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

apt update

apt install -y elasticsearch

systemctl start elasticsearch

systemctl enable elasticsearch

***Now edit the configuration file of Elastic search***

vi /etc/elasticsearch/elasticsearch.yml

*cluster.name: graylog (uncomment and change at line no. 17)*

systemctl restart elasticsearch

***Now Install MongoDB***

***Download MongoDB and 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*

***Now Install Graylog-Server***

Graylog Server processes the log and then displays it for the requests that come from the graylog web interface.

***Install graylog 3.x repository***

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

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

*apt update*

*apt install -y graylog-server*

***Now set a secret to secure the user passwords.***

*pwgen -N 1 -s 96*

*QlRyHh8VIoqiFnS3giJEM6bE1v6ZWvtq04d7TeVvGcRp5QuOfI67h6sTogqxWAubsjumdo5ehNyJd5P1lwB8JJSmaMPnFv6A*

***Now open graylog-server configuration file and put password inside it,***

vi /etc/graylog/server/server.conf

password\_secret = a6864eb339b0e1f6e00d75293a8840abf069a2c0fe82e6e53af6ac099793c1d5

**You will need this password to login into the Gray log web interface. Admin password can’t be changed using the web interface. So, you must edit this variable to set.**

echo -n temp123 | sha256sum (password is temp123)

*e3c652f0ba0b4801205814f8b6bc49672c4c74e25b497770bb89b22cdeb4e951 (output)*

***And open the graylog-server configuration file,***

vi /etc/graylog/server/server.conf

*root\_password\_sha2 = 0a19533d8eae0719d0e75b3cfb2d80808111b7612756418145cc7103e621f352*

*root\_timezone = UTC*

*http\_bind\_address = 192.168.72.91:9000*

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***

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

***Now access graylog at any....***

*http://192.168.72.80:9000*

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

***Now create Graylog Inputs***

*Now click on System > Inputs > select Syslog UDP and then click Launch new input then click on Global.*

*Select your Graylog Node*

*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.*

***Now Edit the Rsyslog configuration file***

vi /etc/rsyslog.conf

*At the end , add the following for which messages will forward and save file.*

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

*service rsyslog restart*

*You should start receiving log messages from the client machine when the event is generated.*