Install Elasticsearch:

Elasticsearch is an open source search server, it offers a real-time distributed search and analytics with Restful web interface. Elasticsearch stores all the logs sent by the Gray log server and displays the messages when the gray log web interface requests for full filling user request over the web interface.

Import the GPG key.

rpm --import https://packages.elastic.co/GPG-KEY-elasticsearch

Add Elasticsearch repository:

1. vi /etc/yum.repos.d/elasticsearch.repo

[elasticsearch-1.7]

name=Elasticsearch repository for 1.7.x packages

baseurl=http://packages.elastic.co/elasticsearch/1.7/centos

gpgcheck=1

gpgkey=http://packages.elastic.co/GPG-KEY-elasticsearch

enabled=1

Install the latest version using yum command

1. yum –y install elasticsearch

Configure Elasticseach to start during system startup.

1. systemctl daemon-reload
2. systemctl enable elasticsearch.service

The only important thing is to set a cluster name as “**graylog2**“, that is being used by graylog. Now edit the configuration file of Elasticsearch.

1. vi /etc/elasticsearch/elasticsearch.yml

cluster.name: graylog2

Disable dynamic scripts to avoid remote execution, that can be done by adding the following line at the end of above file.

script.disable\_dynamic: true

Once it is done, we are good to go. Before that, restart the Elasticsearch services to load the modified configuration.

1. systemctl restart elasticsearch.service

Wait at least a minute to let the Elasticsearch get fully restarted, otherwise testing will fail. Elastisearch should be now listen on 9200 for processing HTTP request, we can use CURL to get the response. Ensure that it returns with cluster name as “**graylog2**”

1. curl -X GET <http://localhost:9200>

{

"status" : 200,

"name" : "Silver Fox",

"cluster\_name" : "graylog2",

"version" : {

"number" : "1.7.2",

"build\_hash" : "e43676b1385b8125d647f593f7202acbd816e8ec",

"build\_timestamp" : "2015-09-14T09:49:53Z",

"build\_snapshot" : false,

"lucene\_version" : "4.10.4"

},

"tagline" : "You Know, for Search"

}

**Optional:** Use the following command to check the Elasticsearch cluster health, you must get a cluster status as “green” for graylog to work.

1. curl -XGET 'http://localhost:9200/\_cluster/health?pretty=true'

{

"cluster\_name" : "graylog2",

"status" : "green",

"timed\_out" : false,

"number\_of\_nodes" : 1,

"number\_of\_data\_nodes" : 1,

"active\_primary\_shards" : 0,

"active\_shards" : 0,

"relocating\_shards" : 0,

"initializing\_shards" : 0,

"unassigned\_shards" : 0,

"delayed\_unassigned\_shards" : 0,

"number\_of\_pending\_tasks" : 0,

"number\_of\_in\_flight\_fetch" : 0

}

## Install MongoDB:

MongoDB is available in RPM format and same can be downloaded from the [official website](http://www.mongodb.org/downloads). Add the following repository information on the system to install MongoDB using yum.

1. vi /etc/yum.repos.d/mongodb-org-3.0.repo

[mongodb-org-3.0]

name=MongoDB Repository

baseurl=http://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/3.0/x86\_64/

gpgcheck=0

enabled=1

1. yum -y install mongodb-org

If you use SELinux, you must install below package to configure certain elements of SELinux policy.

1. yum -y install policycoreutils-python

Run the following command to configure SELinux to allow MongoDB to start.

1. semanage port -a -t mongod\_port\_t -p tcp 27017

Or, if you do not wish to use SELinux on the system, consider [disabling of SELinux](https://www.itzgeek.com/how-tos/linux/centos-how-tos/disable-selinux-on-centos-6-disable-selinux-on-rhel-6.html).

1. systemctl start mogod
2. systemctl status mongod

Start the MongoDB service and enable it to start automatically during the system start-up.

service mongod start

chkconfig mongod on

## Install Graylog2:

Graylog-server accepts and process the log messages, also spawns the RESTAPI for the requests that comes from graylog-web-interface. Download the latest version of graylog from [graylog.org.](https://www.graylog.org/download/)

Use the following command to install graylog2 repository.

rpm -Uvh <https://packages.graylog2.org/repo/packages/graylog-1.2-repository-el7_latest.rpm>

Install the latest graylog server.

1. yum -y install graylog-server

Edit the server.conf file.

1. # vi /etc/graylog/server/server.conf

Configure the following variables in the above file.

Set a secret to secure the user passwords, use the following command to generate a secret, use at least 64 character’s.

1. pwgen -N 1 -s 96

5uxJaeL4vgP9uKQ1VFdbS5hpAXMXLq0KDvRgARmlI7oxKWQbH9tElSSKTzxmj4PUGlHIpOkoMMwjICYZubUGc9we5tY1FjLB

If you get a “pwgen: command not found“, use the following command to install pwgen.

Note: Do not forget to configure EPEL respoitory on CentOS 7 / RHEL 7.

1. yum -y install pwgen

password\_secret = 5uxJaeL4vgP9uKQ1VFdbS5hpAXMXLq0KDvRgARmlI7oxKWQbH9tElSSKTzxmj4PUGlHIpOkoMMwjICYZubUGc9we5tY1FjLB

Next is to set a hash password for the root user (not to be confused with system user, root user of graylog is admin). You will use this password for login into the web interface, admin’s password can not be changed using web interface, must edit this variable to set.

Replace “yourpassword” with the choice of your’s.

1. echo -n yourpassword | sha256sum

e3c652f0ba0b4801205814f8b6bc49672c4c74e25b497770bb89b22cdeb4e951

Place the hash password.

root\_password\_sha2 = e3c652f0ba0b4801205814f8b6bc49672c4c74e25b497770bb89b22cdeb4e951

You can setup email address root (admin) user.

root\_email = "kranthi@gmail.com"

Set timezone of root (admin) user.

root\_timezone = UTC

Graylog will try to find the Elasticsearch nodes automatically, it uses multicast mode for the same. But when it comes to larger network, it is recommended to use unicast mode which is best suited one for production setups. So add the following two entries to graylog server.conf file, replace ipaddress with live hostname or ipaddress, multiple hosts can be added with comma separated.

elasticsearch\_http\_enabled = false

elasticsearch\_discovery\_zen\_ping\_unicast\_hosts = ipaddress:9300

Set only one master node by defining the below variable, default setting is true, you must set it as a false to make the particular node as a slave. Master node performs some periodic tasks that slave won’t perform.

is\_master = true

The following variable sets the number of log messages to keep per index, it is recommended to have several smaller indices instead of larger ones.

elasticsearch\_max\_docs\_per\_index = 20000000

The following parameter defines to have total number of indices, if the this number is reached old index will be deleted.

elasticsearch\_max\_number\_of\_indices = 20

Shards setting is really depends on the number of nodes in the Elasticsearch cluster, if you have only one node, set it as 1.

elasticsearch\_shards = 1

The number of replicas for your indices, if you have only one node in Elasticsearch cluster; set it as 0.

elasticsearch\_replicas = 0

Add MongoDB authentication information.

mongodb\_useauth = false

Start the graylog server using the following command.

1. systemctl restart graylog-server

You can check out the server startup logs, it will be useful for you to troubleshoot graylog in case of any issue.

1. tailf /var/log/graylog-server/server.log

On successful start of graylog-server, you should get the following message in the log file.

2015-09-16T21:26:05.689-04:00 INFO [ServerBootstrap] Graylog server up and running.

**Install Graylog web interface:**

To configure graylog-web-interface, you must have at least one graylog-server node. Install web interface using below command.

1. yum -y install graylog-web

Edit the configuration file and set the following parameters.

1. vi /etc/graylog/web/web.conf

This is the list of graylog-server nodes, you can add multiple nodes, separate by commas.

graylog2-server.uris="http://127.0.0.1:12900/"

Set the application scret, you can generate it using pwgen -N 1 -s 96.

application.secret="sNXyFf6B4Au3GqSlZwq7En86xp10JimdxxYiLtpptOejX6tIUpUE4DGRJOrcMj07wcK0wugPaapvzEzCYinEWj7BOtHXVl5Z"

Restart the gralog-web-interface using following command,

1. systemctl restart graylog-web

Access Graylog web interface:

The web interface will listen on port 9000, configure the firewall to allow traffic on port 9000.

1. # firewall-cmd --permanent --zone=public --add-port=9000/tcp
2. # firewall-cmd --reload

Point your browser to http://ip-add-ress:9000. Log in with username “admin” and the password you configured at root\_password\_sha2 on server.conf.