So you want to do some logging. . . (PT. 1 Setup)

blog.iso365down.com/so-you-want-to-do-some-logging-pt-1-setup-ed319422d331

HanSolo71 December 3, 2023

HanSolo71

After much pestering by Reddit. I've decided to rebuild my blog series on setting up a basic Graylog server and getting some basic data ingestion started.

Without Logs Troubleshooting Can Be hard

Starting the Journey

For this project we will be using Debian. Graylog has guides built for the following OS

1. Ubuntu
2. Debian
3. SUSE
4. Red Hat

Our Debian instance has nothing installed so far and is a bare install with updates installed. Let's start by installing the prerequisites needed by Graylog.

1. Cryptographic Libraries
2. MongoDB
3. Open Search

Its time to stop planning and start building

Cryptographic Libraries

In order to import the keys need to validate various repositories we will need to ensure *gnupg* is installed.

```
sudo apt-get install gnupg
```

After we have installed *gnupg* we are ready to import any keys needed by future steps.

MongoDB

For this demo we are using Debian 12 “Bookwork” and as such we will be adding the following repository. We are using a Ubuntu Jammy repository for this install because it includes libssl1.1 which MongoDB 6.0 needs.

```
| sudo  /etc/apt/sources.list.d/mongodb-org-6.0.list
```

Run *apt update* to update the repository packages.

```
sudo apt update
```

Install MongDB

```
sudo apt install -y mongodb-org
```

Enable MongoDB to start as a service during system startup

```
sudo systemctl daemon-reloadsudo systemctl  mongod.servicesudo systemctl restart mongod.servicesudo systemctl --=service --state=active | grep mongod
```

OpenSearch

Import *OpenSearch* GPG key.

```
curl -o- https://artifacts.opensearch.org/publickeys/opensearch.pgp | sudo apt-key add -
```

Create a repository for OpenSearch

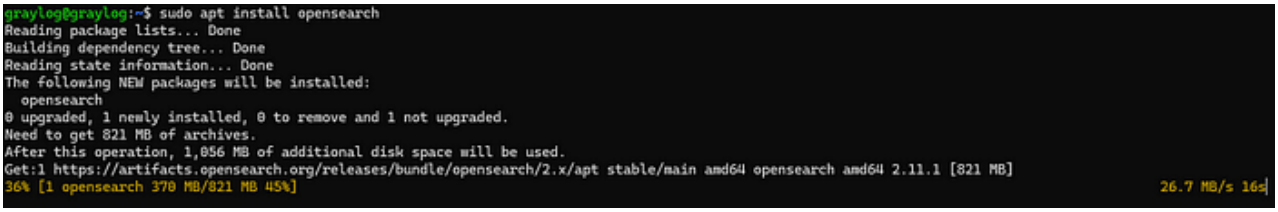
```
  | sudo  -a /etc/apt/sources.list.d/opensearch-2.x.list
```

Run *apt update* to add repository information to system

```
sudo apt update
```

Install OpenSearch

```
sudo apt install opensearch
```



Its a rather large install

Now we need to configure OpenSearch to work with our Graylog instance. Point your favorite text editor at */etc/opensearch/opensearch.yml.*

```
sudo nano /etc/opensearch/opensearch.yml
```

We will want to update the following lines in our configuration.

For my configuration I needed to add the following lines. I added them at the bottom of *opensearch.yml*

Next we need to update our JVM options for OpenSearch. Again using your favorite text editor edit */etc/opensearch/jvm.options.*

```
sudo nano /etc/opensearch/jvm.options
```

We want to update the values of *Xms* and *Xmx.* The value should be half of available memory. In our case 4GB.

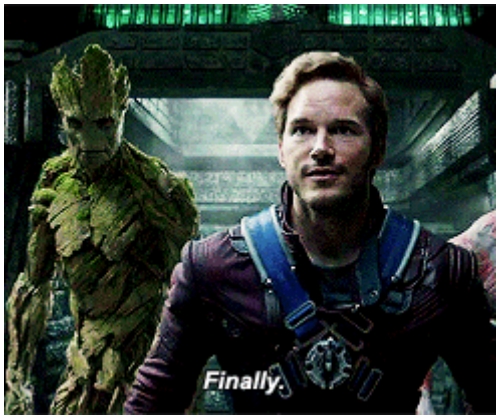
```
-Xms4g-Xmx4g
```

Update the kernel parameters for OpenSearch. This must be done as root!

```
sudo susysctl -w vm.max_map_count=262144  >> /etc/sysctl.conf
```

Enable and start the service

```
sudo systemctl daemon-reloadsudo systemctl  opensearch.servicesudo systemctl start
opensearch.service
```



Finally ready to install Graylog

Graylog

Now that we have our prerequisites installed, we can finally get to the main show. Installing Graylog.

Start by downloading the latest .deb for Graylog

```
wget https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.deb
```

Import the .deb we downloaded

```
sudo dpkg - graylog--repository_latest
```

Install Graylog

```
sudo apt   sudo apt install graylogserver
```

```
graylog@graylog:~$ wget https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.deb
--2023-12-02 21:31:33--  https://packages.graylog2.org/repo/packages/graylog-5.2-repository_latest.deb
Resolving packages.graylog2.org (packages.graylog2.org)... 104.21.88.209, 172.67.153.95, 2606:4700:3035::ac43:995f, ...
Connecting to packages.graylog2.org (packages.graylog2.org)|104.21.88.209|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://graylog-package-repository.s3.eu-west-1.amazonaws.com/packages/graylog-5.2-repository_latest.deb?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Da
te=20231203T023133Z&X-Amz-SignedHeaders=host&X-Amz-Expires=600&X-Amz-Credential=AKIAIJSI6MCSPXFVDPIA%2F20231203%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Signat
ure=33bf64f4453d05505bc88716621d37df18a95c9bcb71cbfe26195618446f5b05 [following]
--2023-12-02 21:31:33--  https://graylog-package-repository.s3.eu-west-1.amazonaws.com/packages/graylog-5.2-repository_latest.deb?X-Amz-Algorithm=AWS4-HMAC-
SHA256&X-Amz-Date=20231203T023133Z&X-Amz-SignedHeaders=host&X-Amz-Expires=600&X-Amz-Credential=AKIAIJSI6MCSPXFVDPIA%2F20231203%2Feu-west-1%2Fs3%2Faws4_reque
st&X-Amz-Signature=33bf64f4453d05505bc88716621d37df18a95c9bcb71cbfe26195618446f5b05
Resolving graylog-package-repository.s3.eu-west-1.amazonaws.com (graylog-package-repository.s3.eu-west-1.amazonaws.com)... 52.92.35.170, 52.218.36.43, 52.21
8.101.104, ...
Connecting to graylog-package-repository.s3.eu-west-1.amazonaws.com (graylog-package-repository.s3.eu-west-1.amazonaws.com)|52.92.35.170|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2088 (2.0K) [application/x-debian-package]
Saving to: 'graylog-5.2-repository_latest.deb'

graylog-5.2-repository_latest.deb      100%[===================================================================>]   2.04K  --.-KB/s    in 0s

2023-12-02 21:31:34 (218 MB/s) - 'graylog-5.2-repository_latest.deb' saved [2088/2088]

graylog@graylog:~$ sudo dpkg -i graylog-5.2-repository_latest.deb
Selecting previously unselected package graylog-5.2-repository.
dpkg: considering removing graylog-5.0-repository in favour of graylog-5.2-repository ...
dpkg: yes, will remove graylog-5.0-repository in favour of graylog-5.2-repository
(Reading database ... 30930 files and directories currently installed.)
Preparing to unpack graylog-5.2-repository_latest.deb ...
Unpacking graylog-5.2-repository (1-2) ...
Removing graylog-5.0-repository (1-2), to allow configuration of graylog-5.2-repository (1-2) ...
Setting up graylog-5.2-repository (1-2) ...
Installing new version of config file /etc/apt/sources.list.d/graylog.list ...
graylog@graylog:~$ sudo apt update
Hit:1 http://deb.debian.org/debian bookworm InRelease
Hit:2 http://deb.debian.org/debian bookworm-updates InRelease
Hit:3 https://artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt stable InRelease
Ign:4 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/6.0 InRelease
Hit:5 http://security.debian.org/debian-security bookworm-security InRelease
Hit:7 https://repo.mongodb.org/apt/ubuntu jammy/mongodb-org/6.0 Release
Hit:6 https://packages.graylog2.org/repo/debian stable InRelease
Get:9 https://packages.graylog2.org/repo/debian stable/5.2 amd64 Packages [5,417 B]
Fetched 5,417 B in 1s (4,482 B/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
W: https://artifacts.opensearch.org/releases/bundle/opensearch/2.x/apt/dists/stable/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted
.gpg), see the DEPRECATION section in apt-key(8) for details.
W: https://repo.mongodb.org/apt/ubuntu/dists/jammy/mongodb-org/6.0/Release.gpg: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the
DEPRECATION section in apt-key(8) for details.
graylog@graylog:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages will be upgraded:
  graylog-server
1 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 271 MB of archives.
After this operation, 30.4 MB disk space will be freed.
Do you want to continue? [Y/n] y
Get:1 https://packages.graylog2.org/repo/debian stable/5.2 amd64 graylog-server amd64 5.2.1-1 [271 MB]
45% [1 graylog-server 154 MB/271 MB 57%]                                                                    7,337 kB/s 15s
```

Configure Graylog to start on system boot

```
sudo systemctl  graylog-server.servicesudo systemctl start graylog-server.service
```

Edit the Graylog configuration file located at */etc/graylog/server/server.conf.*

In particular pay attention to the following areas.

```
password_secret =root_password_sha2 =http_bind_address =
```

To create *password_secret* run the following command

```
< /dev/urandom  -dc A-Z-a-z-0-9 |  -c;;
```

To create *root_password_sha2*

```
 -n  &&  -1 </dev/stdin |  -d  |  |  -d -f1
```

Restart the Graylog service

```
sudo systemctl restart graylog-server
```

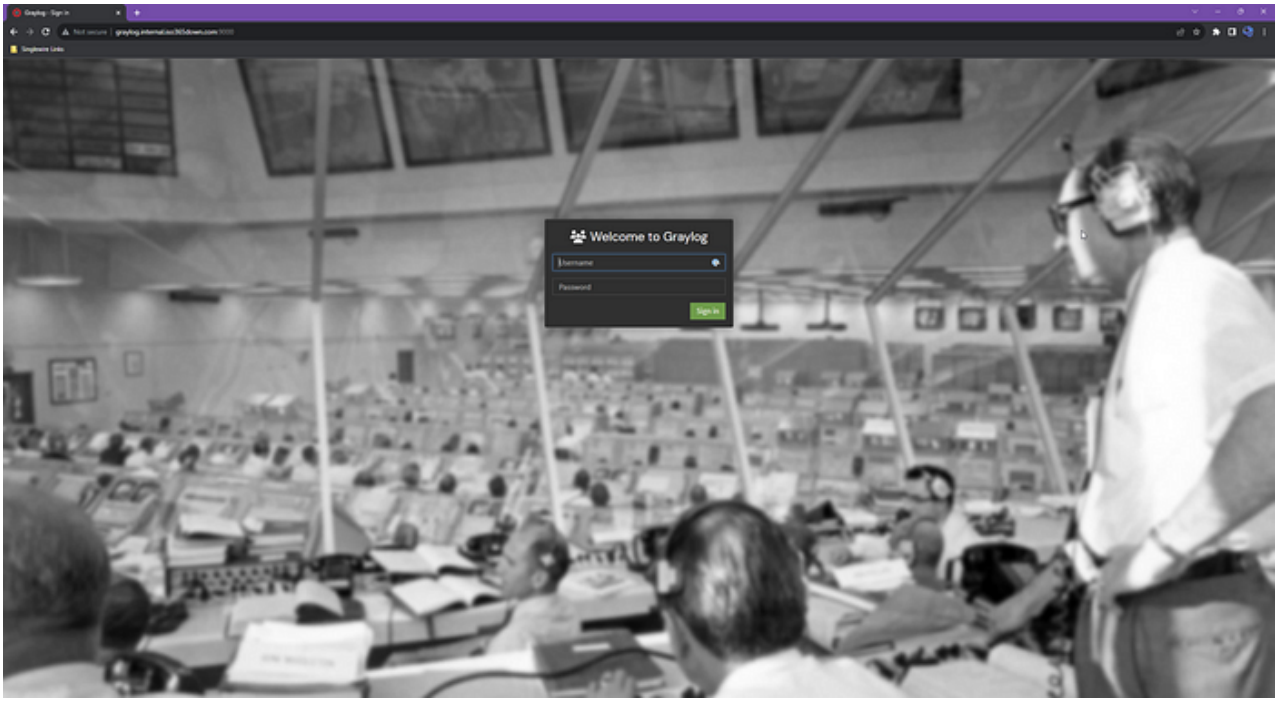
Validate we have no errors and the Graylog starts by tailing the logs located at

```
sudo  -f /var/log/graylog-server/server.log
```

If Graylog starts successfully you should see a message similar to the following

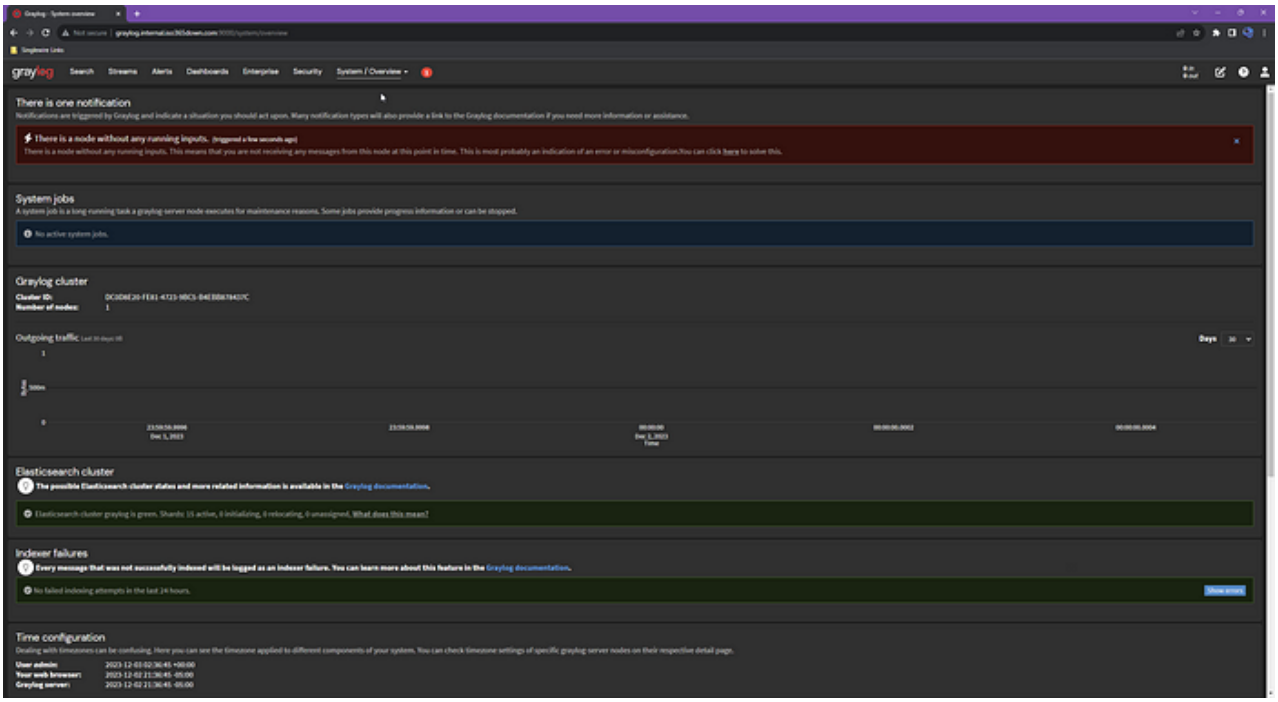
```
2023-12-02T21:24:57.926-05:00 INFO  [NetworkListener] Started listener bound to
[192.168.127.77:9000]2023-12-02T21:24:57.927-05:00 INFO  [HttpServer] [HttpServer]
Started.2023-12-02T21:24:57.927-05:00 INFO  [JerseyService] Started REST API at
<192.168.127.77:9000>2023-12-02T21:24:57.927-05:00 INFO  [ServiceManagerListener]
Services are healthy....2023-12-02T21:24:57.932-05:00 INFO  [ServerBootstrap]
Graylog server up and running.2023-12-02T21:25:07.015-05:00 INFO  [connection]
Opened connection [connectionId{localValue:11, serverValue:41}] to localhost:27017
```

Browsing to http://servername:9000 or http://serverIP:9000 should now show the Graylog login page



Finally ready to login

Using the password we set for *root_password_sha2* we can login and see our system is running but unconfigured.



Its a blank slate

Whats next?

For the next part in this series we will be putting Graylog behind a NGINX reverse proxy and adding LetsEncrypt certificates to our web interface along adding Active Directory authentication to Graylog.