GNU/Linux Administration - Support #435

Installing Graylog2 on Debian 7

08/12/2014 07:28 AM - Daniel Curtis

Status:	Suspended	**Start date:**	07/17/2014
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	10%
Category:	Logging Server	**Estimated time:**	4.00 hours
Target version:		**Spent time:**	0.00 hour

Description

Prerequisites

You will need the following environment:

- Debian Linux
- 2GB RAM (I ran into issues using less)
- 80GB HD

You will need to have the following services installed on either the host you are running graylog2-server on or on dedicated machines:

1. ElasticSearch v0.90.10
2. MongoDB (as recent stable version as possible, at least v2.0)

Vagrant Box available

- https://github.com/hggh/graylog2-vagrant

Install Graylog2

- Install Debian a few dependencies

```
apt-get install mongodb-server openjdk-7-jre-headless uuid-runtime adduser pwgen
```

- Install Elasticsearch from Upstream

```
wget https://download.elasticsearch.org/elasticsearch/elasticsearch/elasticsearch-0.90.10.deb
dpkg -i elasticsearch-0.90.10.deb
```

  - Configure of Elasticsearch:

```
vi /etc/elasticsearch/elasticsearch.yml
```

  - Add to configuration:

cluster.name: graylog2

Install Graylog2 Packages

- Install GPG Key from Jonas Genannt GPG Stats:

```
apt-key adv --keyserver pgp.surfnet.nl --recv-keys 016CFFD0
```

- Add Graylog2 Apt Repro:

```
echo 'deb http://finja.brachium-system.net/~jonas/packages/graylog2_repro/ wheezy main' > /etc
/apt/sources.list.d/graylog2.list
```

- Install Graylog2 Packages:

```
apt-get update && apt-get install graylog2-server graylog2-web
```

- Install Graylog2 Stream Dashboard:

```
apt-get install graylog2-stream-dashboard
```

- OR: manually download deb files: http://finja.brachium-system.net/~jonas/packages/graylog2/

Enable Graylog2 init script

- Graylog2 Server

```
sed -i 's@no@yes@' /etc/default/graylog2-server
```

- Graylog2 Webinterface

```
sed -i 's@no@yes@' /etc/default/graylog2-web
```

Configuration of Graylog2

- Edit the Graylog2 server parameters, see configuration:

```
vi /etc/graylog2/server/server.conf
```

password_secret
root_password_sha2

- To generate the "password_secret", run:

```
pwgen -s 96
```

- To generate the "root_password_sha2", run:
echo -n SuperSecretPassword | shasum -a 256

Edit the Graylog2 web server parameters:

```
vi /etc/graylog2/web/graylog2-web-interface.conf
```

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

- To generate the "application.secret", run:

```
pwgen -s 96
```

Start the Graylog2 services

- Graylog2 Server
  service graylog2-server start
- Graylog2 Webinterface

```
service graylog2-web start
```

- Elasticsearch

```
service elasticsearch
```

- Now its time to access the web interface, open a web browser and navigate to: http://localhost:9000/
  - Username: admin
  - Password: (see /etc/graylog2/server/server.conf)

Graylog2 official documentation

http://support.torch.sh/help/kb/graylog2-web-interface/installing-graylog2-web-interface-v0200-previewx-on-nix-systems

Resources

- https://gist.github.com/hggh/7492598
- http://support.torch.sh/help/kb/graylog2-server/installing-graylog2-server-v020x-on-nix-systems
- https://wiki.joyent.com/wiki/display/jpc2/Installing+Elasticsearch+From+Source+on+SmartOS
- http://www.elasticsearch.org/downloads/0-90-10/

Related issues:

Copied from GNU/Linux Administration - Support #426: Installing Graylog2 on A...	**Suspended**	**07/17/2014**

History

#1 - 08/12/2014 07:28 AM - Daniel Curtis

- Copied from Support #426: Installing Graylog2 on Arch Linux added

#2 - 08/12/2014 08:41 AM - Daniel Curtis

- Description updated

#3 - 02/15/2015 08:37 PM - Daniel Curtis

- Project changed from 94 to GNU/Linux Administration

- Category set to Logging Server

#4 - 06/04/2017 08:24 PM - Daniel Curtis

- Status changed from New to Suspended