Graylog Installation & Troubleshooting Guide

1. Fixing Ubuntu 'Jammy' Issue & Updating Repositories

Ubuntu 'Jammy' (22.04) causes compatibility issues with some packages, especially MongoDB and Elasticsearch. We need to ensure the correct repositories are enabled and update the system before proceeding.

```
$ sudo apt update && sudo apt upgrade -y
$ sudo apt-get install -y software-properties-common
$ sudo add-apt-repository universe
$ sudo apt-get update
$ lsb_release -a  # Ensure Ubuntu version is correctly identified
```

2. Removing Existing MongoDB & Installing Version 4.4

Graylog requires MongoDB, but versions 5.0+ have CPU compatibility issues on some virtual machines. We'll remove any existing MongoDB installations and install the stable 4.4 version.

```
$ sudo systemctl stop mongod
$ sudo apt-get purge mongodb-org*
$ sudo apt-get autoremove
$ sudo rm -rf /var/log/mongodb
$ sudo rm -rf /var/lib/mongodb
$ sudo rm -rf /etc/apt/sources.list.d/mongodb*.list
$ curl -fsSL https://pgp.mongodb.com/server-4.4.asc | sudo gpg -o
/usr/share/keyrings/mongodb-server-4.4.gpg --dearmor
$ echo "deb [arch=amd64,arm64
signed-by=/usr/share/keyrings/mongodb-server-4.4.gpg]
https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/4.4 multiverse" | sudo tee
/etc/apt/sources.list.d/mongodb-org-4.4.list
$ sudo apt-get update
$ sudo apt-get install -y mongodb-org
$ sudo systemctl start mongod
$ sudo systemctl enable mongod
$ sudo systemctl status mongod
```

3. Installing and Configuring Elasticsearch 7.x

Elasticsearch is required for Graylog to function. We install version 7.x and configure it to allow Graylog indexing.

```
$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key
add -
$ echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo
```

```
tee /etc/apt/sources.list.d/elastic-7.x.list
$ sudo apt-get update
$ sudo apt-get install -y elasticsearch
$ sudo tee /etc/elasticsearch/elasticsearch.yml > /dev/null <<EOT
$ cluster.name: graylog
$ network.host: 0.0.0.0
$ http.port: 9200
$ action.auto_create_index: false
$ discovery.type: single-node
$ EOT
$ sudo systemctl restart elasticsearch
$ sudo systemctl enable elasticsearch
$ sudo systemctl status elasticsearch
```

4. Installing Graylog 4.3.11-1 (Compatible with MongoDB 4.4)

Graylog 5.x requires MongoDB 5.0, which does not work on some CPUs, so we downgrade to Graylog 4.3.11-1.

```
$ sudo systemctl stop graylog-server
$ sudo apt-get remove graylog-server
$ wget
https://packages.graylog2.org/repo/packages/graylog-4.3-repository_latest.deb
$ sudo dpkg -i graylog-4.3-repository_latest.deb
$ sudo apt-get update
$ sudo apt-cache madison graylog-server  # Check available versions
$ sudo apt-get install -y --allow-downgrades graylog-server=4.3.11-1
$ sudo systemctl daemon-reload
$ sudo systemctl enable graylog-server
$ sudo systemctl start graylog-server
$ sudo systemctl status graylog-server
```

5. Final Checks & Troubleshooting

Ensure that MongoDB, Elasticsearch, and Graylog are running properly before trying to access the web interface.

```
$ sudo systemctl start mongod
$ sudo systemctl start elasticsearch
$ sudo systemctl start graylog-server
$ sudo systemctl status mongod
$ sudo systemctl status elasticsearch
$ sudo systemctl status graylog-server
$ sudo tail -n 50 /var/log/graylog-server/server.log  # Check for errors
$ echo 'Ensure all services are running and logs do not contain errors.'
$ echo 'Access Graylog Web Interface at: http://your-server-ip:9000'
```