Graylog Deployment Documentation

Project Overview

As part of our project, we were tasked with deploying Graylog for centralized log management. Initially, the responsibilities were divided among the four team members to streamline the setup process. However, by Week 2, we encountered consistent and critical deployment issues, which led us to shift toward a collaborative approach, with all members jointly focusing on troubleshooting and resolving the deployment challenges.

Initial Setup and Environment Preparation

Each team member created a virtual machine (VM) on their personal computers and attempted to install and configure the core components required for Graylog:

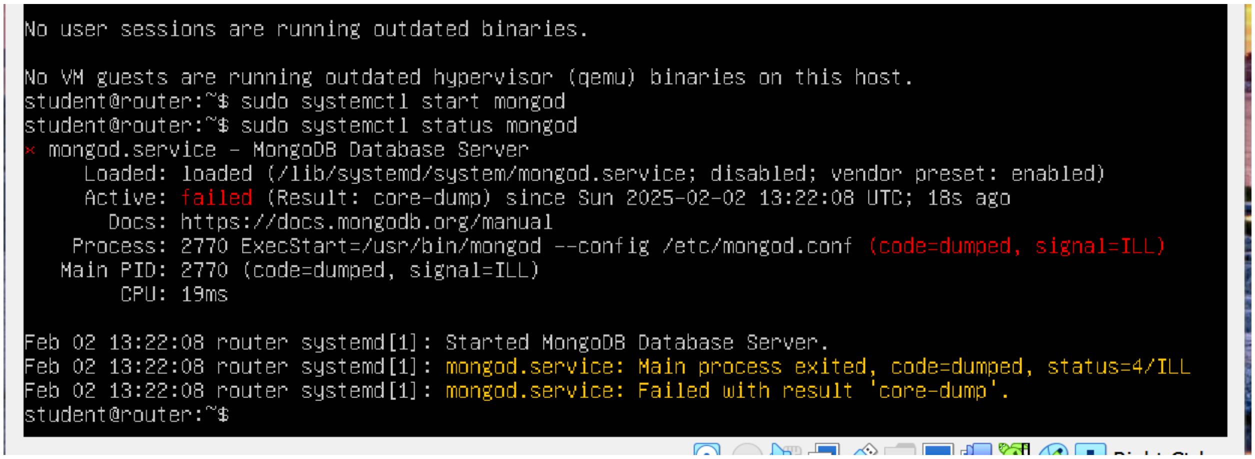
- **MongoDB** (Database backend)
- **Elasticsearch** (Search and analytics engine)
- **Graylog** (Log management platform)

Despite following standard installation steps, the environment failed to operate correctly, and Graylog could not launch due to issues related to MongoDB.

Error Encountered:

Illegal instruction (core dumped)

This recurring error, triggered when starting MongoDB, completely blocked further progress.



```
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
student@router:~$ sudo systemctl start mongod
student@router:~$ sudo systemctl status mongod
× mongod.service - MongoDB Database Server
     Loaded: loaded (/lib/systemd/system/mongod.service; disabled; vendor preset: enabled)
     Active: failed (Result: core-dump) since Sun 2025-02-02 13:22:08 UTC; 18s ago
       Docs: https://docs.mongodb.org/manual
    Process: 2770 ExecStart=/usr/bin/mongod --config /etc/mongod.conf (code=dumped, signal=ILL)
   Main PID: 2770 (code=dumped, signal=ILL)
        CPU: 19ms

Feb 02 13:22:08 router systemd[1]: Started MongoDB Database Server.
Feb 02 13:22:08 router systemd[1]: mongod.service: Main process exited, code=dumped, status=4/ILL
Feb 02 13:22:08 router systemd[1]: mongod.service: Failed with result 'core-dump'.
student@router:~$
```

Troubleshooting MongoDB Failures

I attempted several troubleshooting steps including:

- Checking MongoDB and Graylog log files
- Modifying configuration files (e.g., mongod.conf)
- Reinstalling MongoDB and removing residual files
- Verifying system compatibility and service status using commands

Some Commands Used for Troubleshooting:

Start MongoDB and check service status -

```
sudo systemctl start mongod
systemctl status mongod
```

View detailed MongoDB startup logs -

```
journalctl -u mongod
```

View Graylog server logs -

```
sudo tail -n 50 /var/log/graylog-server/server.log
```

View MongoDB version and check if it matches expected -

```
mongod --version
```

Removing the old MongoDB -

```
sudo apt-get purge mongodb-org*
sudo rm -r /var/log/mongodb
sudo rm -r /var/lib/mongodb
sudo apt update
```

Update and upgrade system packages -

```
sudo apt update && sudo apt upgrade
```

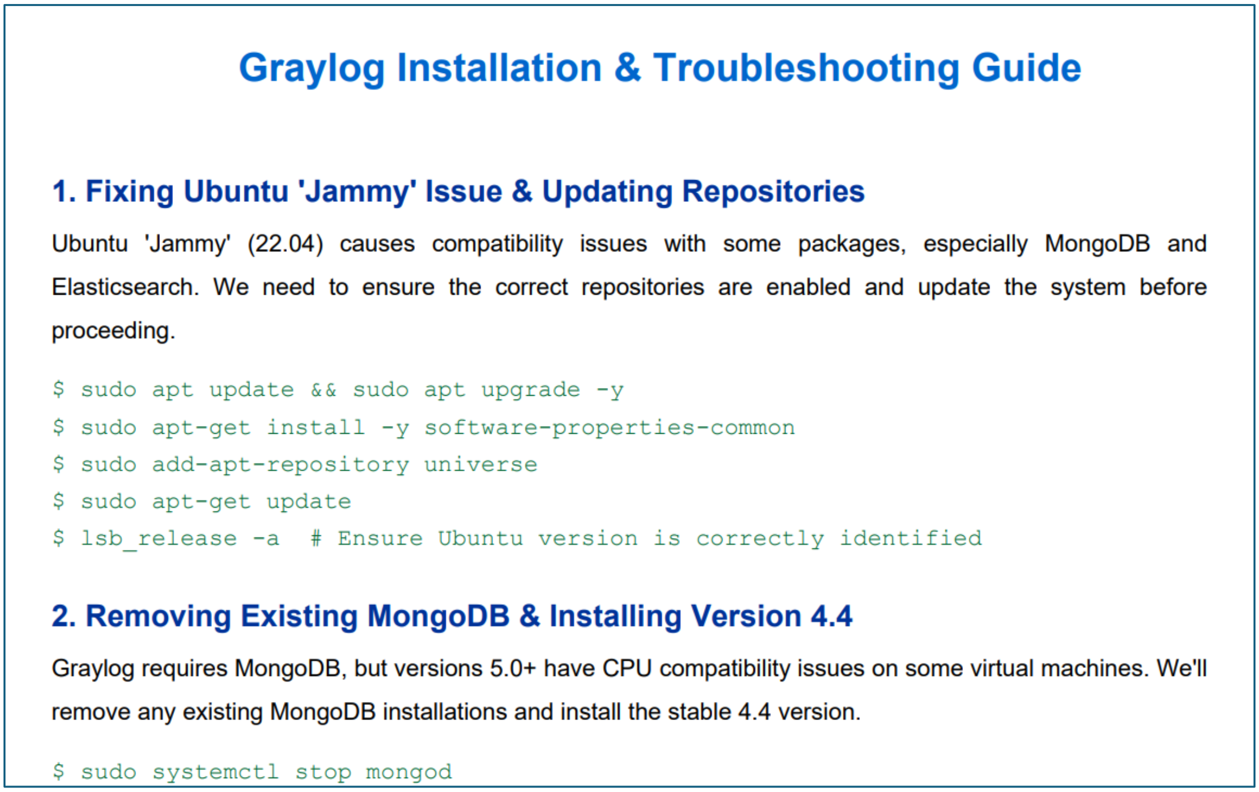
Findings:

Through research, we discovered that MongoDB versions 5 and later require AVX CPU support. Although my CPU supported AVX, the error persisted even after downgrading to MongoDB 4.0, which doesn't require AVX. This suggested a possible incompatibility with our virtualized environment.

Team Collaboration and Graylog_Installation_Guide

Throughout the deployment phase, our team communicated regularly, sharing errors and helping one another troubleshoot. If one member encountered a fix, they would relay it to the rest.

Eventually, one member, Athena, successfully deployed Graylog and shared a detailed guide titled **Graylog Installation & Troubleshooting Guide**. Although it wasn’t essential for each member to deploy the stack individually, we all chose to do so to strengthen our understanding of the system architecture.



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
```

Service Failures and Deeper Troubleshooting

Even after following the shared guide, some of us experienced:

- Graylog starting and stopping immediately
- Inaccessibility via the web interface (http://<ip>:9000)

Some Commands Used for Troubleshooting:

```
sudo systemctl status graylog-server

sudo tail -n 50 /var/log/graylog-server/server.log

sudo systemctl status mongod

sudo systemctl status elasticsearch
```

Issues Identified:

- There were missing configurations in server.conf, such as *password_secret* and *root_password_sha2*, were preventing Graylog from initialising.

  Generated a key for *password_secret* using: *pwgen -N 1 -s 96*

  Then generated an admin password for *password_secret* using: *echo -n "YourSecurePassword" | sha256sum*

- There were also network binding issues. Graylog's *http_bind_address* was initially set to *127.0.0.1*, which restricted access to the local machine only. This was corrected by updating the config to *0.0.0.0:9000*

- I also discovered disk space errors. It seemed that there was disk space exhaustion which may have been causing Graylog crashes. I fixed this by:

  Deleted unnecessary files on the system

  Increased the VM's RAM and CPU allocation in Virtualbox

  Then resized the partition in Ubuntu so it knew it had more space to use. Using Linux LVM tools (lvextend, resize2fs)

  ```
  sudo lvextend -l +100%FREE /dev/ubuntu-vg/ubuntu-lv
  sudo resize2fs /dev/mapper/ubuntu--vg-ubuntu—lv
  ```

After resolving configuration errors and resizing the virtual disk, I successfully accessed the Graylog web interface and confirmed proper log ingestion. This marked the completion of a stable deployment environment.

Parallel Tasks Completed

While dealing with deployment challenges, I worked on the following:

a. Architecture Design Diagram

- Created an architectural diagram illustrating the interaction between al the components in our environment (e.g., Graylog, MongoDB, Elasticsearch, the log sources etc)
- Used **draw.io** to visualise the system components and data flow.

b. Capacity Planning Document

- Drafted a detailed capacity planning document outlining system resource requirements (CPU, RAM, storage) based on expected log volume.
- Included calculations for estimated storage usage and scalability considerations.

c. Data Retention & Storage Configuration

- Investigated Graylog's **data retention policies** to ensure log data is stored efficiently while complying with project requirements.
- Planned configuration settings for **log rotation, data retention policy and storage optimizations** that suitable for environment and resources we working, whilst being organised.

Successful Deployment Outcome

After resolving configuration errors and resizing the virtual disk, I successfully accessed the Graylog web interface and confirmed proper log ingestion. This marked the completion of a stable deployment environment.

Lessons Learned

This deployment exercise emphasized the importance of:

- Verifying system compatibility early (e.g., AVX support)
- Thorough log analysis for resolving obscure errors
- Collaboration in overcoming complex system-level issues
- Managing VM resources proactively to avoid performance degradation

Conclusion

Deploying Graylog presented several unforeseen challenges, primarily due to hardware incompatibilities and VM resource constraints. However, through collaborative troubleshooting, persistency, and a parallel work strategy, we successfully deployed the environment while building a deeper understanding of centralised log management systems.

References

Stack Overflow. (2021, August). Illegal instruction (core dumped) MongoDB Ubuntu 20.04 LTS. Retrieved April 1, 2025, from https://stackoverflow.com/questions/68937131/illegal-instruction-core-dumped-mongodb-ubuntu-20-04-lts