Final Year Documentation
Everything about GrayLog:

Definition:

Graylog is an open-source log management platform designed to help organizations centralize, index, and analyze large volumes of machine data in real-time. It is widely used by IT operations, security teams, and developers to troubleshoot systems, monitor security events, and ensure compliance.

In simple terms (Computers, apps, and networks) write messages that are called logs that record what happens (like a diary). Graylog gathers all of them in one place so we can look through them easily.

Core Functions: Basically, what does Graylog do?

Graylog, Organize data, collect data, Help us search and alerting, and Dashboard.

- Collect Data: It takes the logs from various sources like servers applications or network devices.
- Graylog cleans up and organize: messages and put them in order so it's to search and find the important details.
- Helps You Search: You can search through all the logs and find what you need much like looking for a word in a story
- Alerting and Dashboards: Graylog can alert when something unusual happens and shows data on simple screens called dashboards.

Why Use Graylog (Benefits) ?

- Quick Problem Finding: Logs show what happened and Graylog helps to see the problems or mistakes as soon as they happen.

- Works in Real Time: You see the events as soon as they happen therefore, we can react to them quickly
- Scalability: If we need to add more computers later as we process Graylog can extend and add more sources

- There’s an open-source version of Graylog that many small or big organizations use and its free

- Integration: Gray log can easily integrate with other devices and sources without much extra work

Limitation of Graylog:

- Can be complex in setup: When we have a lot of data or computers sending logs, setting up Graylog can get complicated.
- Learning New Tools: For none technical users it takes some time to figure out and get used to how it works.
- Extra Features Cost More: Some advanced features are not free and may cost extra if needed.
- Resource Needs: Graylog needs strong computers with a good processor to run and for many companies, this means buying special servers with strong processors.

Key Terms and Simple definitions:

Logs: A small record or diary entry that a computer writes down. It tells use what the computer did in a certain time.

Log Management: Log management is the process of collecting, storing, and analyzing logs to understand what happened.

Ingestion: This means collecting logs from different places

Indexing: Organizing and put the logs in order so they’d be easy to search when we need to find something.

Dashboard: A simple screen with charts and numbers basically visualizes information that shows important information at a glance.

Alert: A notification that informs us when something new and important accrues

Extractor /Pipelines: These are cleaning up or filter steps that help to clean up messy logs and turn them into easy-to-read and cleaned-up information.

Streams: Groups of logs that are stored into Categories (by names or level of importance) .

Retention Policy: Rules that decide how long old logs will be kept before they get deleted.

How Graylog Works :

Elastic Search: It stores and Organize the logs so they can easily and quickly be found upon searching

MongoDB: Stores all the important information that Graylogs needs to run including settings and user information.