Infrastructure Operations, Package Management, and Centralized Logging

This body of work demonstrates hands-on Linux system administration across application and web servers, with a focus on filesystem management, system maintenance, and centralized logging for operational visibility. Tasks were performed in a multi-host environment and reflect real-world responsibilities commonly handled by Linux and infrastructure administrators.

The work includes creating and validating symbolic links to securely reference web application files without duplicating data, reinforcing proper filesystem organization and access practices. System maintenance activities are also represented through controlled package upgrades, where critical components such as GNU C Library (glibc) and MariaDB services were updated and verified to ensure stability, compatibility, and security on CentOS Stream 9 systems.

In addition to host-level operations, centralized logging was leveraged using Graylog to monitor system and application activity across multiple servers. Log searches were executed over defined time windows, using histograms and indexed results to identify trends, spikes, and anomalies in log volume. Detailed message views were analyzed to track authentication events, service state changes, Filebeat log shipping behavior, and application-level errors, supporting troubleshooting and auditability.

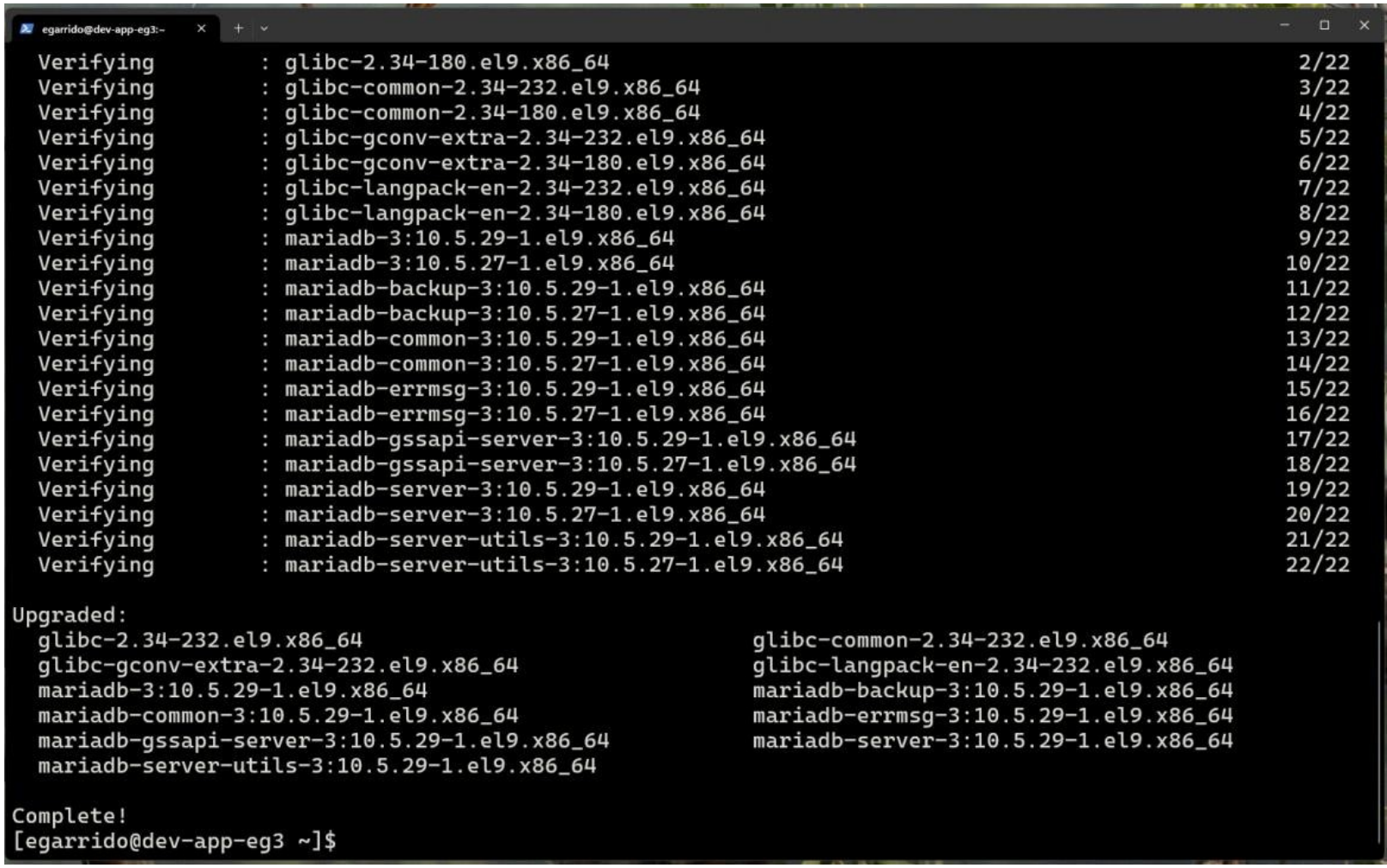
Collectively, these tasks highlight practical experience with Linux command-line operations, system updates, service awareness, and log analysis in a production-like environment. The work reflects a strong emphasis on verification, visibility, and operational reliability—core skills required for systems administration, production support, and infrastructure roles.

The terminal output captures the verification and completion of a system package upgrade on a CentOS Stream 9 server.

During the process, core system libraries such as glibc, glibc-common, glibc-gconv-extra, and language packs are verified alongside multiple MariaDB components, including the server, common files, backup utilities, error messages, GSSAPI server support, and server utilities.

Each package is checked sequentially, showing progress through the verification stage, followed by an Upgraded summary that lists the successfully updated package versions.

The process concludes with a Complete! message and returns to the shell prompt, confirming that the system and database-related packages were upgraded successfully with no reported errors.



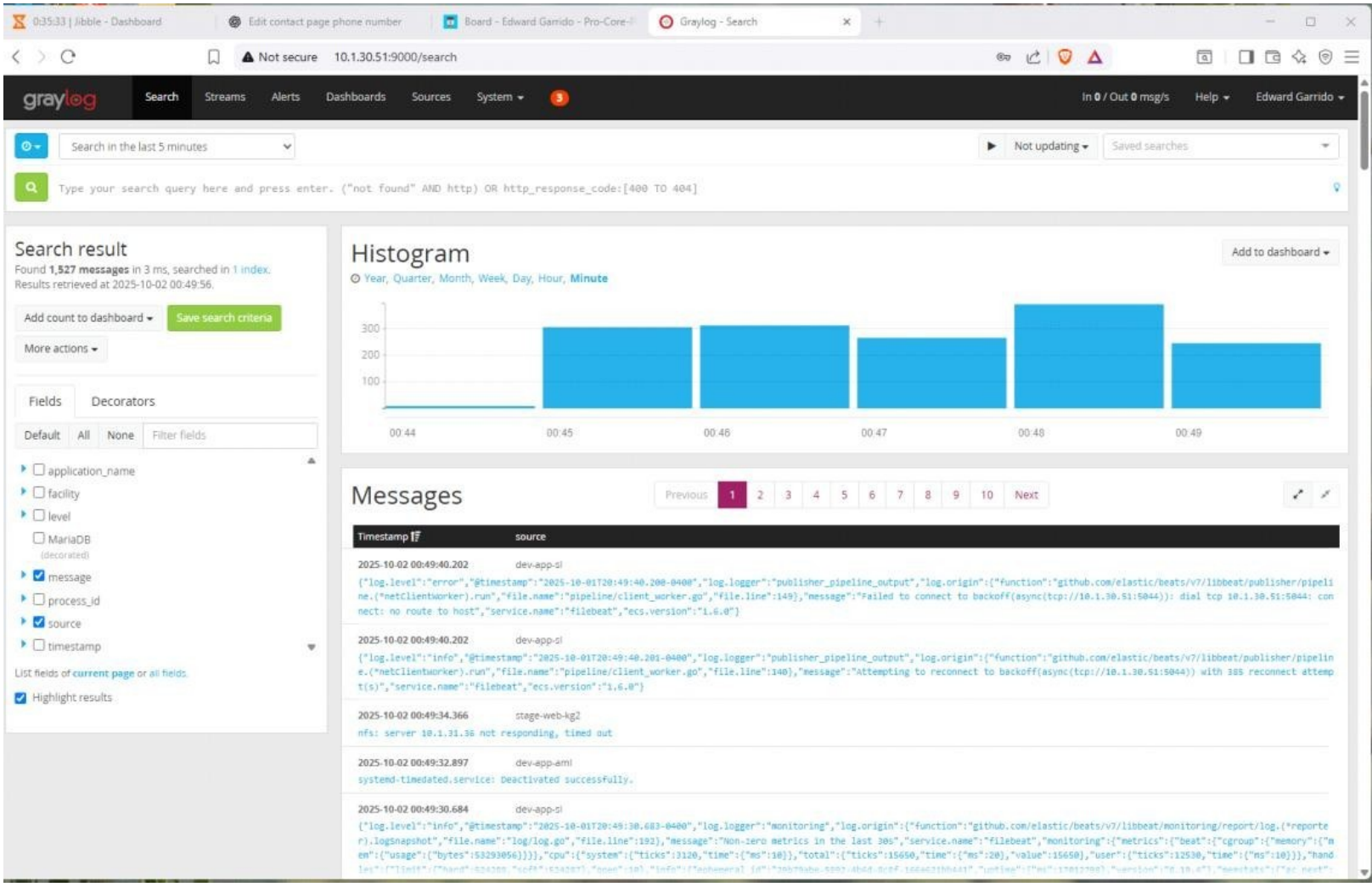
The Graylog web interface is displaying centralized log search results from a recent time window.

A histogram at the top visualizes log volume over time, showing fluctuations in message counts at minute-level intervals.

The messages pane lists individual log entries collected from multiple servers, including application and web hosts. Each entry includes a timestamp, source system, log level, and detailed message content. Several logs reference Filebeat activity, connection retries, backoff behavior, and network-related errors, along with system-level events such as service state changes.

A fields panel on the left provides selectable metadata—such as source, process ID, facility, and severity—to filter and refine searches.

This view confirms that log ingestion is active and provides visibility into system health, application behavior, and connectivity issues across the environment in near real time.



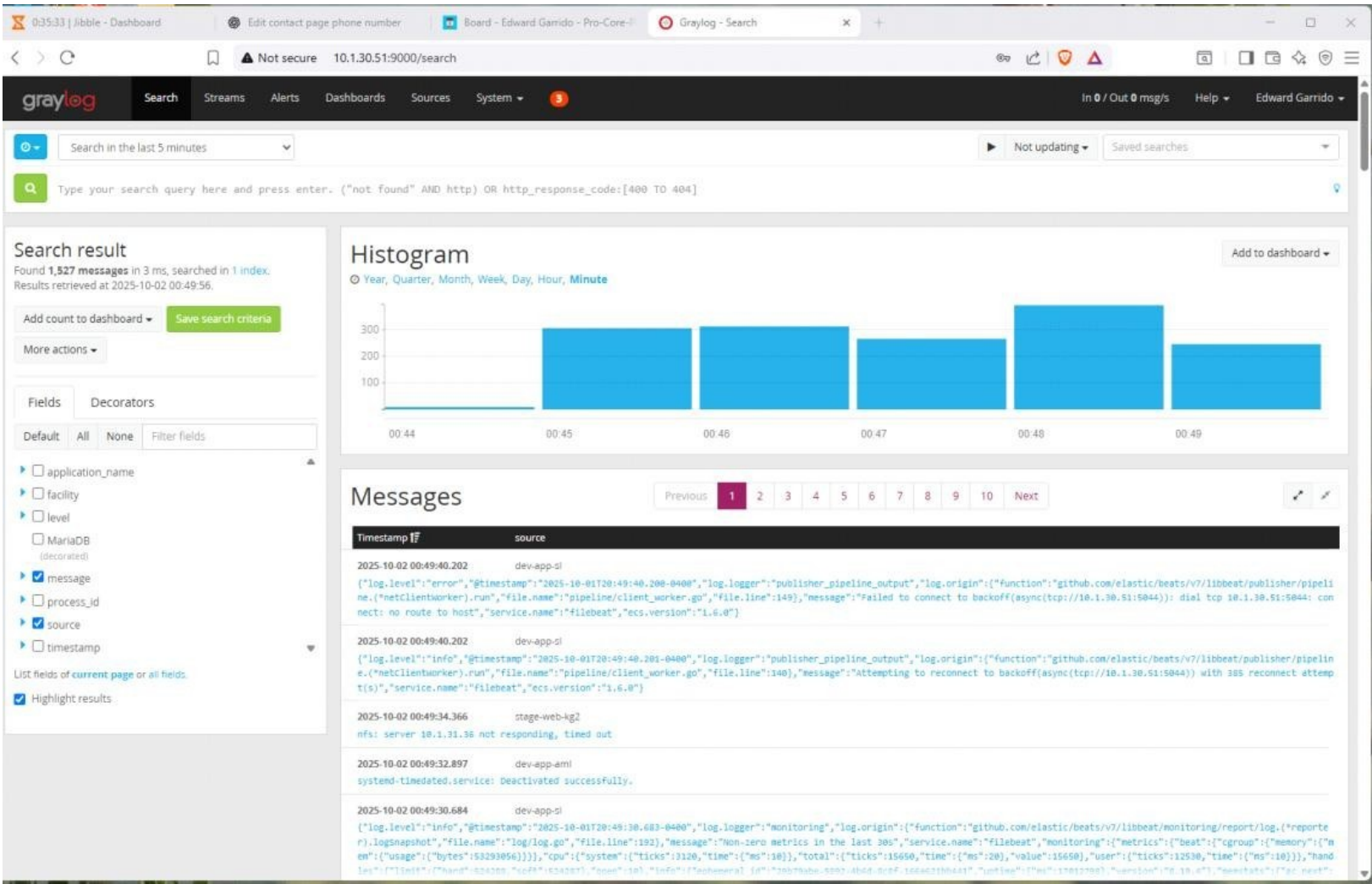
The Graylog web interface is displaying centralized log data collected from multiple servers within the environment.

A search query scoped to the last few minutes returns over a thousand messages from a single index, with a histogram visualizing message volume by minute to highlight activity trends and spikes.

The messages panel lists detailed log entries from application and web hosts, including timestamps, source systems, log levels, and full message payloads. Several entries reference Filebeat operations such as connection retries, backoff behavior, and network connectivity errors, alongside system-level events like service deactivation and application status updates.

On the left, available log fields—such as source, process ID, facility, severity level, and application name—are displayed to support filtering and deeper analysis.

This view provides real-time visibility into application behavior, service health, and log ingestion status across the infrastructure.



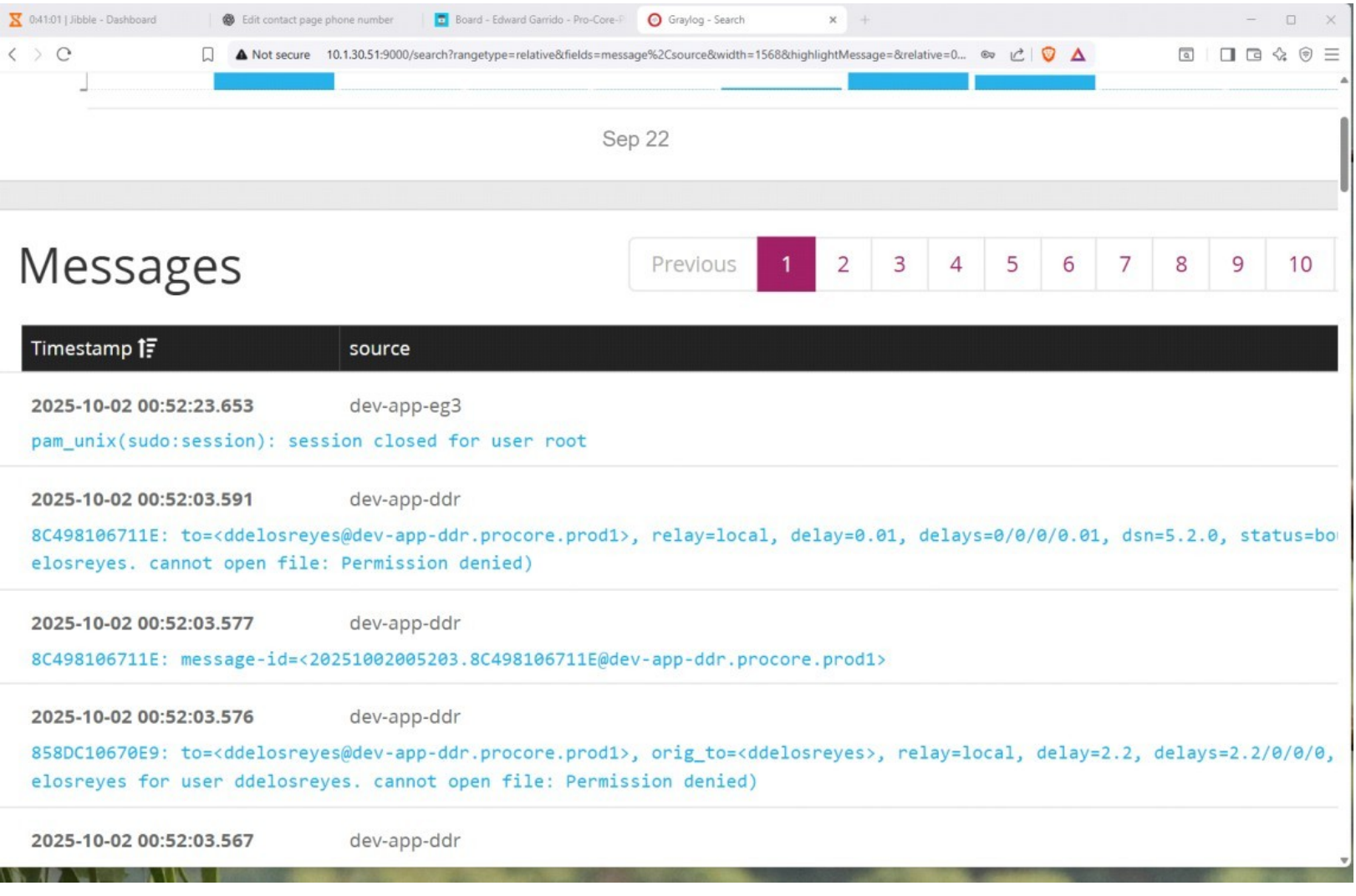
The Graylog messages view is displaying individual log entries from multiple hosts within the environment, sorted by timestamp.

Each entry shows the exact time of the event, the source system, and the associated log message, allowing precise tracking of activity across servers.

Several messages indicate authentication and session activity, including a pam_unix event confirming that a sudo session for the root user was closed on a development application server. Other entries originate from a separate application host and show mail-related events, including message IDs, relay information, delivery delays, and repeated permission denied errors when attempting to access user mail files.

The pagination controls at the top of the messages panel indicate multiple pages of results, enabling navigation through historical log data.

This view highlights how Graylog centralizes authentication, system, and application logs to support auditing, troubleshooting, and root-cause analysis across distributed systems.



Summary

The recent work covers core Linux system administration tasks across application and web servers, focusing on filesystem management, system updates, and centralized log monitoring. Activities include creating and validating symbolic links to provide controlled access to web application files, ensuring proper path resolution without duplicating data.

System maintenance was performed through verified package upgrades involving critical components such as glibc and MariaDB, confirming successful updates and service readiness on CentOS Stream 9 systems. Upgrade verification outputs were reviewed to ensure consistency and completion without errors.

Centralized logging was utilized through Graylog to monitor real-time and historical system activity across multiple hosts. Log searches and message analysis captured authentication events, service lifecycle changes, Filebeat log shipping behavior, and application-level permission errors, supporting troubleshooting and audit visibility.

Together, these tasks demonstrate practical experience in Linux operations, system reliability, and observability within a production-like environment.