

# **Centralized Logging with Rsyslog & Graylog (CentOS Stream 9)**

This project demonstrates the implementation of centralized system logging using rsyslog clients forwarding logs to a Graylog server in a multi-node CentOS Stream 9 environment. The objective was to ensure reliable, centralized visibility into system activity across web, application, and performance hosts while following security and operational best practices.

## **Overview**

Configured rsyslog on multiple CentOS Stream 9 servers to forward all system logs to a centralized Graylog instance using the Syslog Protocol (TCP/514).

Created a dedicated rsyslog configuration file (/etc/rsyslog.d/90-graylog.conf) to ensure clean, modular, and maintainable logging rules.

Restarted and enabled rsyslog to persist across reboots and validated service health using systemctl.

Verified log ingestion end-to-end by generating test events and confirming successful indexing and visibility in the Graylog web interface.

## **Key Tasks Performed**

Installed and updated rsyslog packages

Enabled and validated rsyslog as an active system service

Configured centralized log forwarding to Graylog

Restarted services and confirmed runtime status

Generated test logs using logger

Validated ingestion, indexing, and searchability in Graylog

Confirmed host-specific log visibility using Graylog search filters

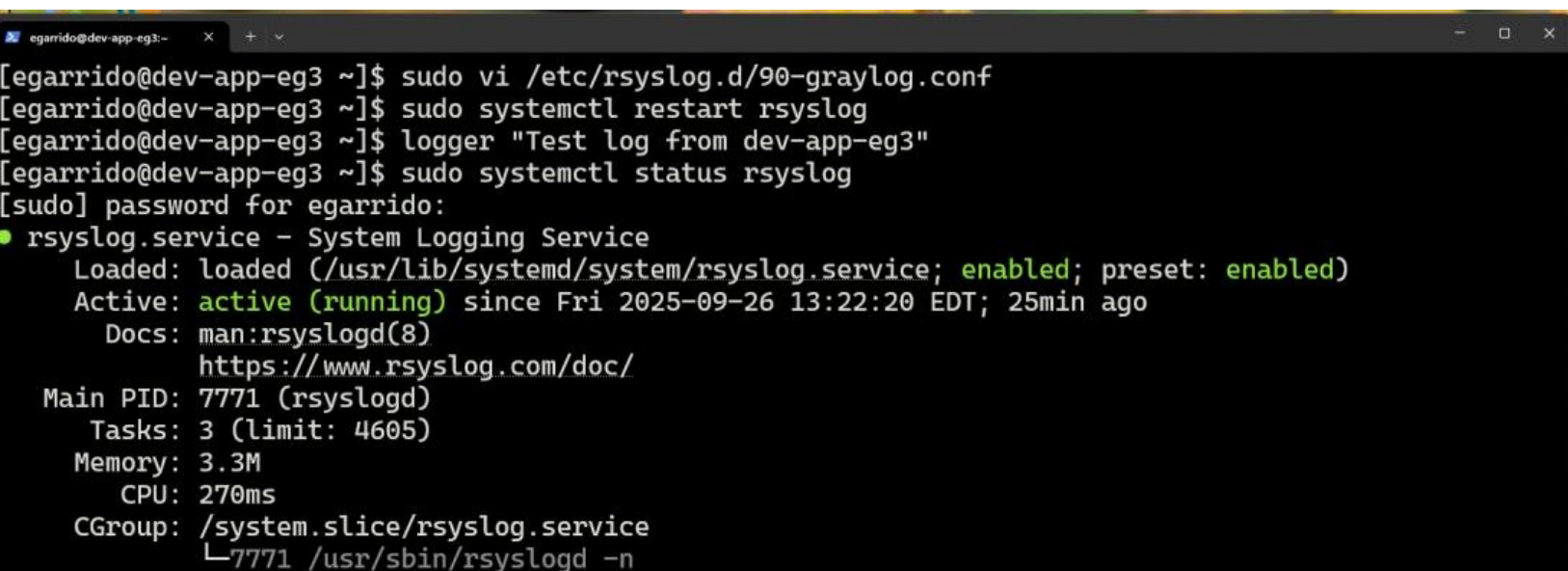
## **Validation**

Graylog dashboards and search results confirm logs are being received in real time.

System events such as service restarts, sudo activity, and journal reloads are visible and correctly attributed to their source hosts.

```
-- INSERT --
```

The screenshot shows the rsyslog service being restarted and verified on a Linux system after configuring a custom Graylog forwarding rule. A test log message is generated using the logger command, and the systemctl status rsyslog output confirms that the rsyslog service is enabled, actively running, and processing logs as expected.

A terminal window with a dark background and light text. The window title is 'egarrido@dev-app-eg3:~'. The terminal shows a series of commands and their outputs. The commands are: 'sudo vi /etc/rsyslog.d/90-graylog.conf', 'sudo systemctl restart rsyslog', 'logger "Test log from dev-app-eg3"', and 'sudo systemctl status rsyslog'. The output of the last command shows the status of the rsyslog service, indicating it is loaded, active (running), and has been running since Fri 2025-09-26 13:22:20 EDT. The output also shows the main PID, tasks, memory, CPU, and CGroup for the service.

```
egarrido@dev-app-eg3 ~]$ sudo vi /etc/rsyslog.d/90-graylog.conf
egarrido@dev-app-eg3 ~]$ sudo systemctl restart rsyslog
egarrido@dev-app-eg3 ~]$ logger "Test log from dev-app-eg3"
egarrido@dev-app-eg3 ~]$ sudo systemctl status rsyslog
[sudo] password for egarrido:
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Fri 2025-09-26 13:22:20 EDT; 25min ago
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
  Main PID: 7771 (rsyslogd)
    Tasks: 3 (limit: 4605)
   Memory: 3.3M
      CPU: 270ms
   CGroup: /system.slice/rsyslog.service
           └─7771 /usr/sbin/rsyslogd -n
```

The screenshot shows the Graylog System → Overview page displaying system messages and operational events. It confirms that the Graylog server is running normally, with logs indicating index rotation, retention strategy execution, index optimization, and Syslog UDP inputs transitioning to a RUNNING state. The timestamps and messages demonstrate that log ingestion and backend maintenance tasks are functioning as expected, verifying successful log flow into Graylog after rsyslog configuration and testing

4:27:09 | Jibble - Dashboard

Board - Edward Garrido - Pro-Core-IP

Graylog - System overview

10.1.30.51:9000/system/overview

graylog

Search Streams Alerts Dashboards Sources System / Overview

In 0 / Out 0 msg/s Help Edward Garrido

time configuration

Dealing with timezones can be confusing. Here you can see the timezone applied to different components of your system. You can check timezone settings of specific graylog-server nodes on their respective detail page.

User egarrido:

2025-09-26 18:01:12 +00:00

Your web browser:

2025-09-26 14:01:12 -04:00

Graylog server:

2025-09-26 14:01:12 -04:00

The screenshot shows the rsyslog service being restarted and verified on a Linux system after configuring a custom Graylog forwarding rule. A test log message is generated using the logger command, and the systemctl status rsyslog output confirms that the rsyslog service is enabled, actively running, and processing logs as expected.

system messages

Nodes on certain events that may be interesting for the Graylog administrators. You don't need to actively act upon any message in here because notifications will be raised for any events that required action.

Timestamp	Node	Message
2025-09-25T20:05:06-04:00	9313d1ac / stage-graylog-procore.dev	Running retention strategy [org.graylog2.indexer.retention.strategies.DeletionRetentionStrategy] for index <graylog_254>
2025-09-25T20:05:06-04:00	9313d1ac / stage-graylog-procore.dev	Number of indices (15) higher than limit (14). Running retention for 1 indices.
2025-09-25T20:01:03-04:00	9313d1ac / stage-graylog-procore.dev	SystemJob <d518b5f0-9a6b-11f0-9489-005056b43d7f> [org.graylog2.indexer.indices.jobs.OptimizeIndexJob] finished in 26209ms.
2025-09-25T20:00:38-04:00	9313d1ac / stage-graylog-procore.dev	SystemJob <c2f7c000-9a6b-11f0-9489-005056b43d7f> [org.graylog2.indexer.indices.jobs.SetIndexReadOnlyAndCalculateRangeJob] finished in 1051ms.
2025-09-25T20:00:37-04:00	9313d1ac / stage-graylog-procore.dev	Optimizing index <graylog_267>.
2025-09-25T20:00:37-04:00	9313d1ac / stage-graylog-procore.dev	Flushed and set <graylog_267> to read-only.
2025-09-25T20:00:07-04:00	9313d1ac / stage-graylog-procore.dev	Cycled index alias <graylog_deflector> from <graylog_267> to <graylog_268>.
2025-09-25T14:45:32-04:00	9313d1ac / stage-graylog-procore.dev	Input [Syslog UDP/68d0d62bb466d53a05232e25] is now STARTING
2025-09-25T14:45:32-04:00	9313d1ac / stage-graylog-procore.dev	Input [Syslog UDP/68d0d62bb466d53a05232e25] is now RUNNING
2025-09-25T14:45:32-04:00	9313d1ac / stage-graylog-procore.dev	Input [Syslog UDP/66759fd0b466d523ea074924] is now RUNNING
2025-09-25T14:45:31-04:00	9313d1ac / stage-graylog-procore.dev	Input [Syslog UDP/66759fd0b466d523ea074924] is now STARTING
2025-09-25T14:45:31-04:00	9313d1ac / stage-graylog-procore.dev	Started up.
2025-09-25T14:42:31-04:00	9313d1ac / stage-graylog-procore.dev	Notification condition [NO_MASTER] has been fixed.
2025-09-25T14:42:25-04:00	9313d1ac / stage-graylog-procore.dev	Notification condition [NO_MASTER] has been fixed.
2025-09-25T14:42:00-04:00	9313d1ac / stage-graylog-procore.dev	Graceful shutdown initiated.
2025-09-25T14:41:54-04:00	9313d1ac / stage-graylog-procore.dev	SIGNAL received. Shutting down.
2025-09-25T14:41:47-04:00	9313d1ac / stage-graylog-procore.dev	Notification condition [NO_MASTER] has been fixed.
2025-09-25T14:41:10-04:00	9313d1ac / stage-graylog-procore.dev	Notification condition [NO_MASTER] has been fixed.

The screenshot shows the `dnf install rsyslog -y` command being executed on a CentOS Stream 9 system. The output confirms that `rsyslog` was already installed and successfully upgraded, along with the `rsyslog-logrotate` package, from the AppStream repository. Dependency checks, transaction tests, and post-install cleanup all completed without errors, verifying that the `rsyslog` logging service and its log rotation components are properly installed and up to date.

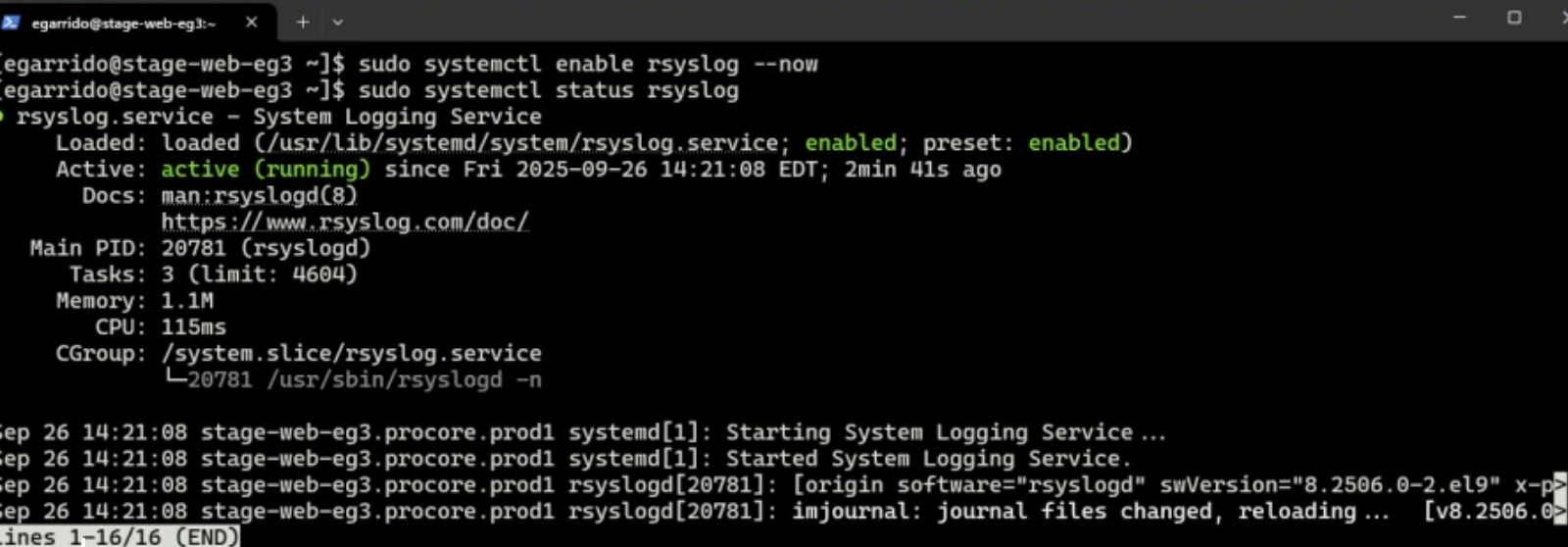
```
egarrido@stage-web-eg3:~$ sudo dnf install rsyslog -y
[sudo] password for egarrido:
Last metadata expiration check: 2:25:18 ago on Fri 26 Sep 2025 11:55:44 AM EDT.
Package rsyslog-8.2412.0-1.el9.x86_64 is already installed.
Dependencies resolved.
```

Package	Architecture	Version	Repository	Size
Upgrading:				
rsyslog	x86_64	8.2506.0-2.el9	appstream	817 k
rsyslog-logrotate	x86_64	8.2506.0-2.el9	appstream	8.5 k

```
Transaction Summary
Upgrade 2 Packages

Total download size: 825 k
Downloading Packages:
(1/2): rsyslog-logrotate-8.2506.0-2.el9.x86_64.rpm 71 kB/s | 8.5 kB 00:00
(2/2): rsyslog-8.2506.0-2.el9.x86_64.rpm 1.6 MB/s | 817 kB 00:00
Total 1.1 MB/s | 825 kB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Upgrading : rsyslog-logrotate-8.2506.0-2.el9.x86_64 1/4
Upgrading : rsyslog-8.2506.0-2.el9.x86_64 2/4
Running scriptlet: rsyslog-8.2506.0-2.el9.x86_64 2/4
Running scriptlet: rsyslog-8.2412.0-1.el9.x86_64 3/4
Cleanup : rsyslog-8.2412.0-1.el9.x86_64 3/4
Running scriptlet: rsyslog-8.2412.0-1.el9.x86_64 3/4
Cleanup : rsyslog-logrotate-8.2412.0-1.el9.x86_64 4/4
Running scriptlet: rsyslog-logrotate-8.2412.0-1.el9.x86_64 4/4
```

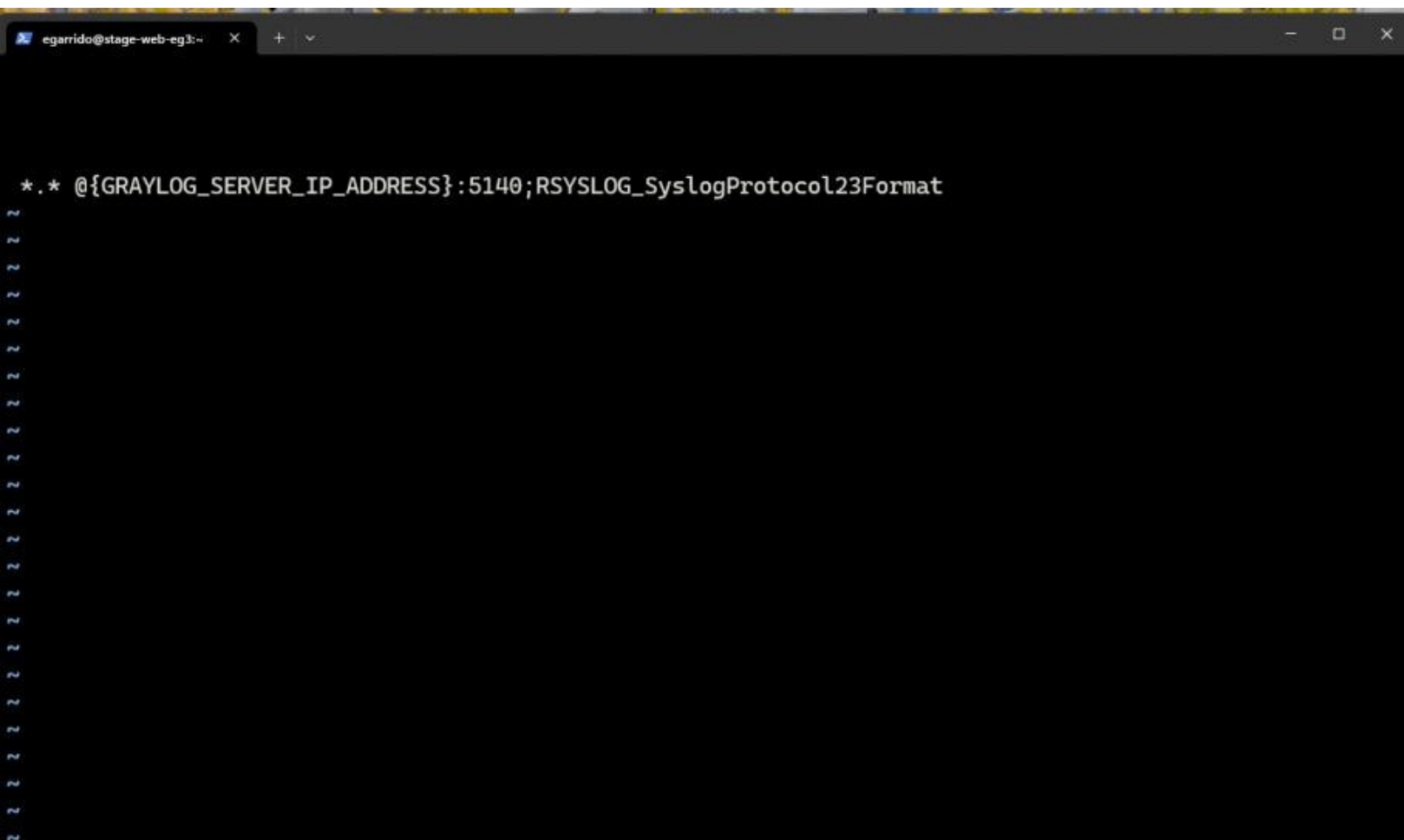
The screenshot shows the rsyslog service being enabled and started using `systemctl enable rsyslog --now` on a CentOS Stream 9 system. The `systemctl status rsyslog` output confirms that the System Logging Service is enabled at boot and actively running. Service details, including the main process ID and recent startup log messages, indicate that rsyslog initialized successfully and is ready to process system logs.

A terminal window with a dark background and light text. The window title is 'egarrido@stage-web-eg3:~'. The user has entered two commands: 'sudo systemctl enable rsyslog --now' and 'sudo systemctl status rsyslog'. The output of the second command shows the service is 'active (running)' with a PID of 20781. Below this, there are several log lines from 'systemd[1]' and 'rsyslogd[20781]' showing the service starting and reloading journal files. The terminal text is as follows:

```
egarrido@stage-web-eg3 ~]$ sudo systemctl enable rsyslog --now
egarrido@stage-web-eg3 ~]$ sudo systemctl status rsyslog
rsyslog.service - System Logging Service
  Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
  Active: active (running) since Fri 2025-09-26 14:21:08 EDT; 2min 41s ago
  Docs: man:rsyslogd(8)
        https://www.rsyslog.com/doc/
  Main PID: 20781 (rsyslogd)
  Tasks: 3 (limit: 4604)
  Memory: 1.1M
  CPU: 115ms
  CGroup: /system.slice/rsyslog.service
          └─20781 /usr/sbin/rsyslogd -n

Sep 26 14:21:08 stage-web-eg3.procore.prod1 systemd[1]: Starting System Logging Service ...
Sep 26 14:21:08 stage-web-eg3.procore.prod1 systemd[1]: Started System Logging Service.
Sep 26 14:21:08 stage-web-eg3.procore.prod1 rsyslogd[20781]: [origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-p>
Sep 26 14:21:08 stage-web-eg3.procore.prod1 rsyslogd[20781]: imjournal: journal files changed, reloading ... [v8.2506.0>
lines 1-16/16 (END)
```

The screenshot shows the `/etc/rsyslog.d/90-graylog.conf` configuration file open in a text editor. It contains a single rsyslog rule that forwards all system logs (`*.*`) to a Graylog server over UDP port 5140, using the Syslog Protocol 23 format. The Graylog server address is referenced via a variable (`@{GRAYLOG_SERVER_IP_ADDRESS}`), indicating a centralized logging setup that standardizes log forwarding while keeping the configuration clean and reusable.



```
egarrido@stage-web-eg3:~$ cat /etc/rsyslog.d/90-graylog.conf
*. * @{{GRAYLOG_SERVER_IP_ADDRESS}}:5140;RSYSLOG_SyslogProtocol23Format
```



The screenshot displays the Graylog System → Overview page confirming the health and operational status of the logging platform. It shows no failed indexing attempts in the last 24 hours, indicating stable log ingestion. The Time configuration section confirms consistent timestamps across the user session, browser, and Graylog server.

Below, the System messages panel lists normal Graylog activities such as index rotation, retention strategy execution, index optimization, and Syslog UDP inputs starting and running successfully. Together, these details verify that Graylog is functioning correctly and actively receiving and managing logs from connected systems.

4:58:34 | Jibble - Dashboard

Board - Edward Garrido - Pro-Core-P

Graylog - System overview

< > ↺

Not secure 10.1.30.51:9000/system/overview

graylog

Search Streams Alerts Dashboards Sources System / Overview 1

In 4 / Out 4 msg/s Help Edward Garrido

No failed indexing attempts in the last 24 hours.

Show errors

### Time configuration

Dealing with timezones can be confusing. Here you can see the timezone applied to different components of your system. You can check timezone settings of specific graylog-server nodes on their respective detail page.

User egarrido:	2025-09-26 18:32:37 +00:00
Your web browser:	2025-09-26 14:32:37 -04:00
Graylog server:	2025-09-26 14:32:37 -04:00

### System messages

System messages are generated by graylog-server nodes on certain events that may be interesting for the Graylog administrators. You don't need to actively act upon any message in here because notifications will be raised for any events that required action.

Timestamp	Node	Message
2025-09-25T20:05:06-04:00	9313d1ac / stage-graylog-procore.dev	Running retention strategy [org.graylog2.indexer.retention.strategies.DeletionRetentionStrategy] for index <graylog_254>
2025-09-25T20:05:06-04:00	9313d1ac / stage-graylog-procore.dev	Number of indices (15) higher than limit (14). Running retention for 1 indices.
2025-09-25T20:01:03-04:00	9313d1ac / stage-graylog-procore.dev	SystemJob <d518b5f0-9a6b-11f0-9489-005056b43d7f> [org.graylog2.indexer.indices.jobs.OptimizeIndexJob] finished in 26209ms.
2025-09-25T20:00:38-04:00	9313d1ac / stage-graylog-procore.dev	SystemJob <c2f7c000-9a6b-11f0-9489-005056b43d7f> [org.graylog2.indexer.indices.jobs.SetIndexReadOnlyAndCalculateRangeJob] finished in 1051ms.
2025-09-25T20:00:37-04:00	9313d1ac / stage-graylog-procore.dev	Optimizing index <graylog_267>.
2025-09-25T20:00:37-04:00	9313d1ac / stage-graylog-procore.dev	Flushed and set <graylog_267> to read-only.
2025-09-25T20:00:07-04:00	9313d1ac / stage-graylog-procore.dev	Cycled index alias <graylog_deflector> from <graylog_267> to <graylog_268>.
2025-09-25T14:45:32-04:00	9313d1ac / stage-graylog-procore.dev	Input [Syslog UDP/68d0d62bb466d53a05232e25] is now STARTING
2025-09-25T14:45:32-04:00	9313d1ac / stage-graylog-procore.dev	Input [Syslog UDP/68d0d62bb466d53a05232e25] is now RUNNING
2025-09-25T14:45:32-04:00	9313d1ac / stage-graylog-procore.dev	Input [Syslog UDP/66759fd0b466d523ea074924] is now RUNNING
2025-09-25T14:45:31-04:00	9313d1ac / stage-graylog-procore.dev	Input [Syslog UDP/66759fd0b466d523ea074924] is now STARTING
2025-09-25T14:45:31-04:00	9313d1ac / stage-graylog-procore.dev	Started up.
2025-09-25T14:42:31-04:00	9313d1ac / stage-graylog-procore.dev	Notification condition [NO_MASTER] has been fixed.
2025-09-25T14:42:25-04:00	9313d1ac / stage-graylog-procore.dev	Notification condition [NO_MASTER] has been fixed.



The screenshot shows the installation of required editor packages (including vim-enhanced) followed by configuration and validation of rsyslog on a CentOS Stream 9 system. After editing the Graylog configuration file (/etc/rsyslog.d/90-graylog.conf), the rsyslog service is restarted and its status is checked. The output confirms that rsyslog is enabled, actively running, and restarted successfully, with system logs indicating proper initialization and readiness to forward logs to the centralized Graylog server.

```
Total 5.2 MB/s | 8.8 MB 00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing      : 1/1
  Installing     : gpm-libs-1.20.7-29.el9.x86_64 1/4
  Installing     : vim-filesystem-2:8.2.2637-22.el9.noarch 2/4
  Installing     : vim-common-2:8.2.2637-22.el9.x86_64 3/4
  Installing     : vim-enhanced-2:8.2.2637-22.el9.x86_64 4/4
Running scriptlet: vim-enhanced-2:8.2.2637-22.el9.x86_64 4/4
  Verifying      : vim-filesystem-2:8.2.2637-22.el9.noarch 1/4
  Verifying      : gpm-libs-1.20.7-29.el9.x86_64 2/4
  Verifying      : vim-common-2:8.2.2637-22.el9.x86_64 3/4
  Verifying      : vim-enhanced-2:8.2.2637-22.el9.x86_64 4/4

Installed:
gpm-libs-1.20.7-29.el9.x86_64 vim-common-2:8.2.2637-22.el9.x86_64
vim-enhanced-2:8.2.2637-22.el9.x86_64 vim-filesystem-2:8.2.2637-22.el9.noarch

Complete!
[egarrido@dev-app-eg3 ~]$ sudo vim /etc/rsyslog.d/90-graylog.conf
[egarrido@dev-app-eg3 ~]$ sudo systemctl restart rsyslog
[egarrido@dev-app-eg3 ~]$ sudo systemctl status rsyslog
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Fri 2025-09-26 18:22:49 EDT; 15s ago
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
  Main PID: 8445 (rsyslogd)
    Tasks: 3 (limit: 4605)
   Memory: 1.3M
      CPU: 105ms
  CGroup: /system.slice/rsyslog.service
          └─8445 /usr/sbin/rsyslogd -n

Sep 26 18:22:49 dev-app-eg3.procore.prod1 systemd[1]: Starting System Logging Service ...
Sep 26 18:22:49 dev-app-eg3.procore.prod1 systemd[1]: Started System Logging Service.
Sep 26 18:22:49 dev-app-eg3.procore.prod1 rsyslogd[8445]: [origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-pid="8445" x-
Sep 26 18:22:49 dev-app-eg3.procore.prod1 rsyslogd[8445]: imjournal: journal files changed, reloading... [v8.2506.0-2.el9 try h
[egarrido@dev-app-eg3 ~]$
```

The screenshot shows the Graylog Search interface confirming successful log ingestion from the host dev-app-eg3. A filtered search (source:dev-app-eg3) returns multiple messages across recent timestamps, visualized in the histogram at the top and detailed in the message list below.

10.1.30.51

Join from Zoom Workplace app - Z...

Join from Zoom Workplace app - Z...

Board - Edward Garrido - Pro-Core-F

Graylog - Search

< > ↺

⚠ Not secure

10.1.30.51:9000/search?rangetype=relative&fields=message%2Csource&width=1718&highlightMessage=&relative=0&q=source%3Adev-app-eg3

🔖 🔔 🔒 🔗 📄

graylog

Search

Streams

Alerts

Dashboards

Sources

System

1

In 97 / Out 97 msg/s

Help

Edward Garrido

🔍 Search in all messages

▶ Not updating

📄 Saved searches

🔍 source:dev-app-eg3

📍

Search result

Found 153 messages in 21 ms, searched in 14 indices.  
Results retrieved at 2025-09-26 23:23:16.

Add count to dashboard

Save search criteria

More actions

Fields

Decorators

Default

All

None

Filter fields

☐ application\_name

☐ facility

☐ level

☐ MariaDB (decorated)

☒ message

☐ process\_id

☒ source

☐ timestamp


List fields of current page or all fields.

☒ Highlight results

Histogram

Add to dashboard

🕒 Year, Quarter, Month, Week, Day, Hour, Minute



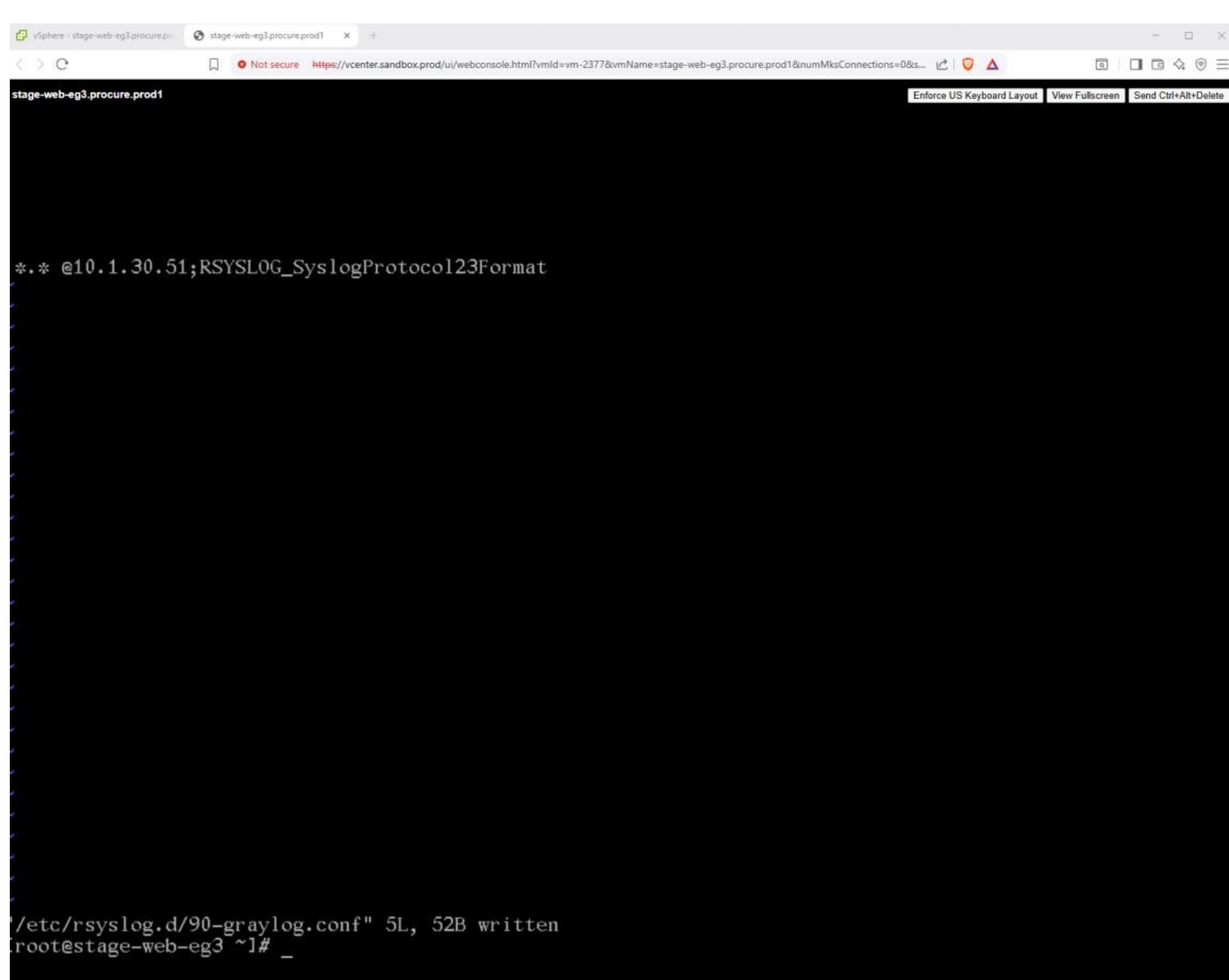
Messages

Previous 1 2 Next

🔗 📄

Timestamp	source
2025-09-26 23:20:11.628	dev-app-eg3
pam_unix(sudo:session): session closed for user root	
2025-09-26 23:20:07.871	dev-app-eg3
pam_unix(sudo:session): session opened for user root(uid=0) by root(uid=770000476)	
2025-09-26 23:20:07.862	dev-app-eg3
egarrido : TTY=pts/0 ; PWD=/home/egarrido ; USER=root ; COMMAND=/bin/systemctl status rsyslog	
2025-09-26 23:19:54.610	dev-app-eg3
ImJournal: Journal files changed, reloading... [v8.2506.0-2.el9 try https://www.rsyslog.com/e/0 ]	
2025-09-26 23:19:54.594	dev-app-eg3
[origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-pid="8587" x-info="https://www.rsyslog.com"] start	
2025-09-26 23:19:54.593	dev-app-eg3
pam_unix(sudo:session): session closed for user root	
2025-09-26 23:19:54.585	dev-app-eg3
Started System Logging Service.	
2025-09-26 23:19:54.492	dev-app-eg3
Starting System Logging Service...	
2025-09-26 23:19:54.469	dev-app-eg3
Stopped System Logging Service.	
2025-09-26 23:19:54.467	dev-app-eg3
rsyslog.service: Deactivated successfully.	
2025-09-26 23:19:54.461	dev-app-eg3
[origin software="rsyslogd" swVersion="8.2506.0-2.el9" x-pid="8445" x-info="https://www.rsyslog.com"] exiting on signal 15.	

The screenshot shows the `/etc/rsyslog.d/90-graylog.conf` file open on the stage-web-eg3 server after being edited and saved. The configuration contains a rule that forwards all system logs (\*.\*) to a centralized Graylog server using the RSYSLOG Syslog Protocol 23 format. The file save confirmation at the bottom indicates the configuration was successfully written, preparing the system for centralized log forwarding via rsyslog.



The screenshot displays a web browser window with a single tab titled "stage-web-eg3.prod1". The address bar shows a "Not secure" warning and the URL `https://vcenter.sandbox.prod/ui/webconsole.html?vmId=vm-2377&vmName=stage-web-eg3.prod1&numMksConnections=0&is...`. The browser interface includes standard navigation buttons (back, forward, refresh) and a menu icon. The main content area is a dark-themed terminal window titled "stage-web-eg3.prod1". At the top right of the terminal, there are three buttons: "Enforce US Keyboard Layout", "View Fullscreen", and "Send Ctrl+Alt+Delete". The terminal shows the command `.* @10.1.30.51;RSYSLOG_SyslogProtocol23Format` entered. At the bottom of the terminal, a confirmation message reads `"/etc/rsyslog.d/90-graylog.conf" 5L, 52B written`, followed by the prompt `root@stage-web-eg3 ~1#` and a cursor.

```
stage-web-eg3.prod1
```

```
.* @10.1.30.51;RSYSLOG_SyslogProtocol23Format
```

```
"/etc/rsyslog.d/90-graylog.conf" 5L, 52B written
root@stage-web-eg3 ~1#
```

This screenshot verifies that the rsyslog service on the stage-web-eg3 server was successfully restarted, enabled at boot, and is actively running. The output confirms the service is loaded, enabled, and operational, with recent log entries showing the system logging service starting and reloading journal files—indicating the updated logging configuration has been applied correctly.

```
Stage-Web-Eg3.ProcCore.Prod1 | Enforce US Keyboard Layout | View Fullscreen | Send Ctrl+Alt+Delete

[root@stage-web-eg3 ~]# systemctl restart rsyslog
[root@stage-web-eg3 ~]# systemctl enable rsyslog
[116798.906179] systemd-rc-local-generator[21018]: /etc/rc.d/rc.local is not marked executable, skipping.
[root@stage-web-eg3 ~]# systemctl status rsyslog
■ rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: active (running) since Fri 2025-09-26 18:45:04 EDT; 16s ago
     Docs: man:rsyslogd(8)
           https://www.rsyslog.com/doc/
  Main PID: 20998 (rsyslogd)
    Tasks: 3 (limit: 4604)
   Memory: 1.1M
      CPU: 107ms
   CGroup: /system.slice/rsyslog.service
           └─20998 /usr/sbin/rsyslogd -n

Sep 26 18:45:04 stage-web-eg3.procCore.prod1 systemd[1]: Starting System Logging Service...
Sep 26 18:45:04 stage-web-eg3.procCore.prod1 systemd[1]: Started System Logging Service.
Sep 26 18:45:04 stage-web-eg3.procCore.prod1 rsyslogd[20998]: [origin software="rsyslogd" swVersion="8.250
Sep 26 18:45:05 stage-web-eg3.procCore.prod1 rsyslogd[20998]: imjournal: journal files changed, reloading.
[root@stage-web-eg3 ~]# _
```

This screenshot confirms that logs from the stage-web-eg3 host are successfully being ingested and indexed in Graylog. The search filter is scoped to source:stage-web-eg3, and the results show recent system and rsyslog events, including service restarts, journal reloads, and sudo session activity. The populated histogram and message list verify end-to-end log forwarding from the server to Graylog and successful processing by the logging pipeline.

10.1.30.51

Join from Zoom Workplace app - Z...

Join from Zoom Workplace app - Z...

Board - Edward Garrido - Pro-Core-F

Graylog - Search

Not secure

10.1.30.51:9000/search?rangetype=relative&fields=message%2Csource&width=1718&highlightMessage=&relative=0&q=source%...

graylog

Search

Streams

Alerts

Dashboards

Sources

System

1

In 0 / Out 0 msg/s

Help

Edward Garrido

Search in all messages

▶ Not updating

Saved searches

source:stage-web-eg3

Search result

Found 14 messages in 14 ms, searched in 14 indices.  
Results retrieved at 2025-09-26 23:42:37.

Add count to dashboard

Save search criteria

More actions

Fields

Decorators

Default

All

None

Filter fields

☐ application\_name

☐ facility

☐ level

☐ MariaDB (decorated)

☒ message

☐ process\_id

☒ source

☐ timestamp

List fields of current page or all fields.

☒ Highlight results

Histogram

Add to dashboard

Year, Quarter, Month, Week, Day, Hour, Minute

Messages

Previous1Next

Timestamp	TF	source
2025-09-26 23:40:20.046		stage-web-eg3 pam_unix(sudo:session): session closed for user root
2025-09-26 23:40:18.234		stage-web-eg3 pam_unix(sudo:session): session opened for user root(uid=0) by egarrido(uid=770000476)
2025-09-26 23:40:18.226		stage-web-eg3 egarrido : TTYpts/0 ; PWD=/home/egarrido ; USER=root ; COMMAND=/bin/systemctl status rsyslog
2025-09-26 23:40:11.748		stage-web-eg3 injournal: journal files changed, reloading... [v8.2506.0-2.el9 try https://www.rsyslog.com/e/0 ]
2025-09-26 23:40:11.735		stage-web-eg3 pam_unix(sudo:session): session closed for user root
2025-09-26 23:40:11.733		stage-web-eg3 [origin software="rsyslogd" swversion="8.2506.0-2.el9" x-pid="21126" x-info="https://www.rsyslog.com"] start
2025-09-26 23:40:11.725		stage-web-eg3 Started System Logging Service.
2025-09-26 23:40:11.636		stage-web-eg3 Starting System Logging Service...
2025-09-26 23:40:11.612		stage-web-eg3 Stopped System Logging Service.
2025-09-26 23:40:11.611		stage-web-eg3 rsyslog.service: Deactivated successfully.
2025-09-26 23:40:11.605		stage-web-eg3 [origin software="rsyslogd" swversion="8.2506.0-2.el9" x-pid="21107" x-info="https://www.rsyslog.com"] exiting on signal 15.

PCP Tickets Page 9

## Summary

Centralized logging was implemented using rsyslog to forward system logs from multiple CentOS Stream 9 servers to a Graylog server. Logging services were installed, enabled, and validated on each host, with log forwarding configured through a dedicated rsyslog configuration file. End-to-end functionality was confirmed by generating test events and verifying successful ingestion, indexing, and searchability within the Graylog interface. All environment details and IP addresses shown are sanitized for security.