System Logs

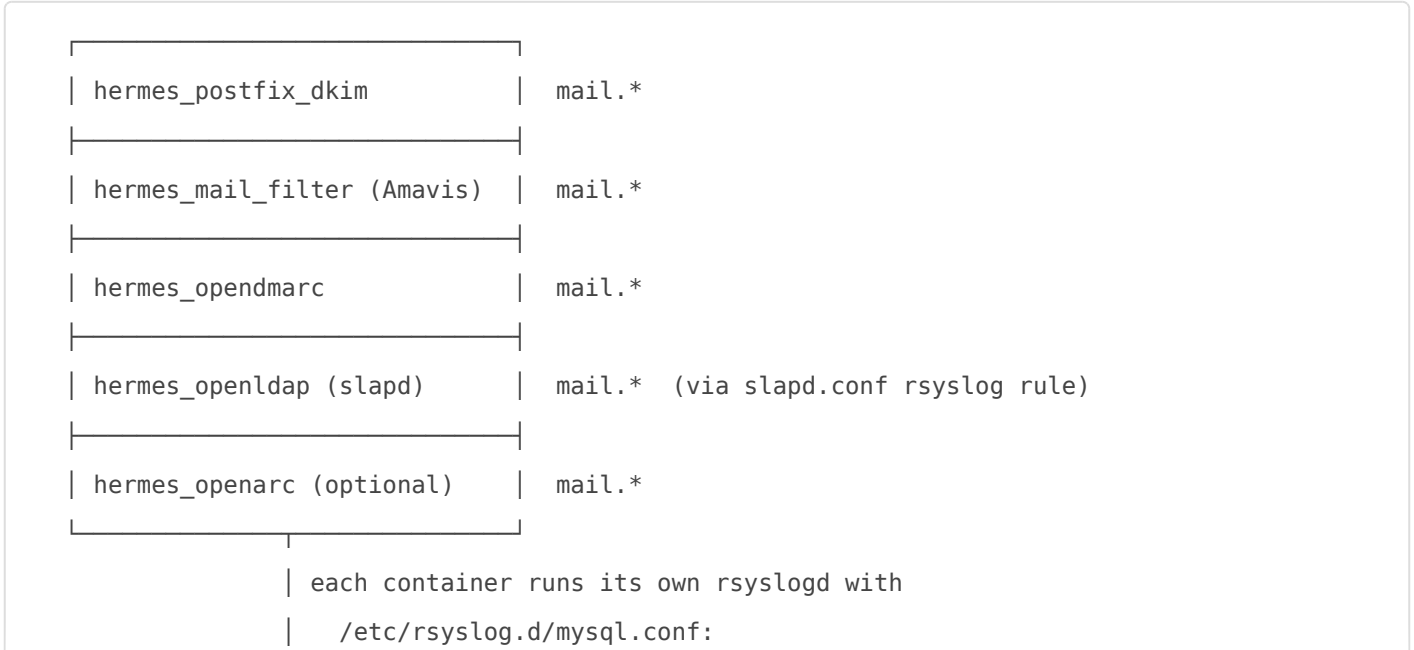
System Logs

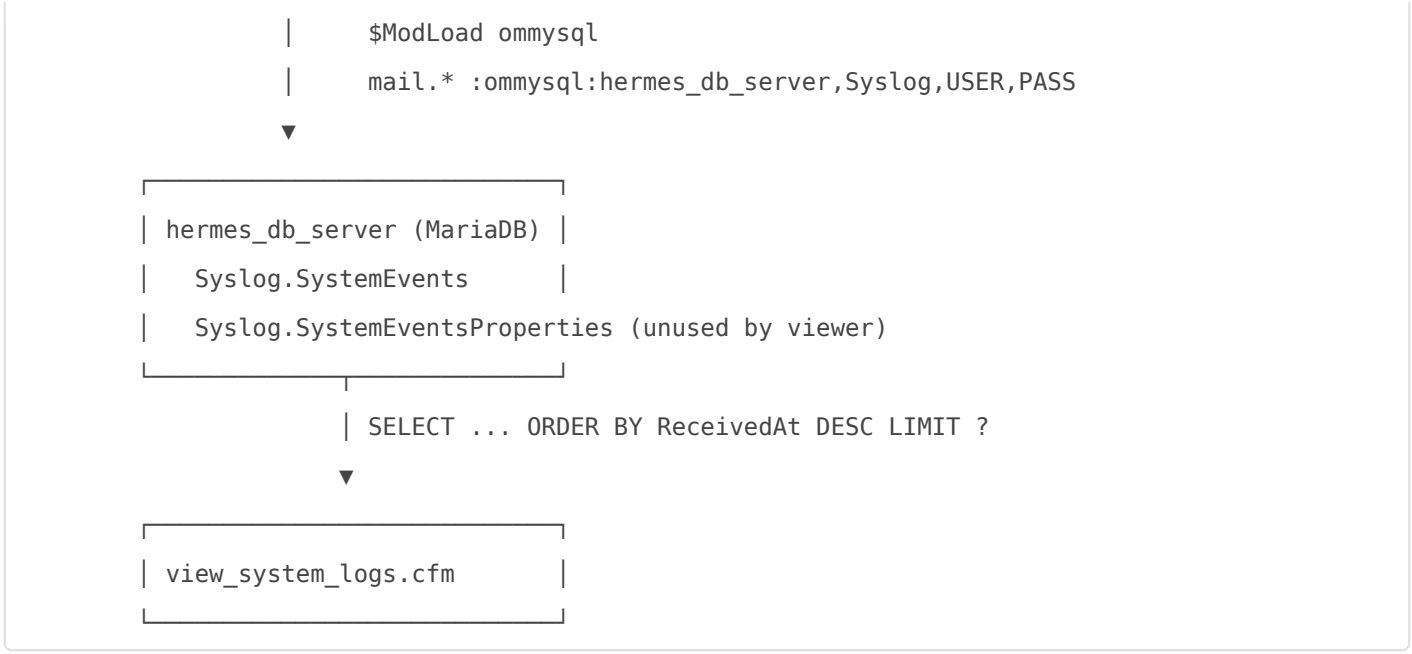
Admin path: **System > System Logs** (`view_system_logs.cfm`, `schedule/message_cleanup.cfm`).

This page is a SQL-backed log viewer over **rsyslog's `SystemEvents` table** in the `Syslog` database. Every mail-side container in the stack ships its `mail.*` syslog stream to MariaDB via the `ommysql` rsyslog output module; this page reads from that table with a date range, optional facility filter, and a row limit, and renders the result in a sortable DataTable.

Pairs with Mail Queue: the Mail Queue viewer shows what Postfix is currently holding; this page shows the historical log trail — connection negotiation, milter results, content-filter verdicts, delivery outcomes, bounce generation — that explains *why* a message did or did not make it through.

The log pipeline — container `mail.*` to `SystemEvents`





The MySQL output config that wires each container into the pipeline is templated at install time. Each service gets a per-container template under `config/<service>/etc/rsyslog.d/mysql.conf.template` with `__SYSLOG_USER__` / `__SYSLOG_PASS__` placeholders; the install script substitutes the generated credentials and bind-mounts the rendered file into the container at `/etc/rsyslog.d/mysql.conf`. There is no container-side aggregator — every container talks to MariaDB directly.

> **Operational consequence.** If MariaDB is down or unreachable from a container, that container's `mail.*` log entries are buffered by rsyslog and then dropped when the buffer fills. Log gaps during a database outage are expected and are not a bug in the viewer.

What lands in `SystemEvents` — and what doesn't

The `mail.*` selector covers everything that uses syslog facility 2 (`mail`) on the source containers. That is:

- All Postfix smtpd / cleanup / qmgr / smtp / lmtp / bounce / pickup output (connection logs, milter verdicts, `status=sent|deferred| bounced`, queue lifecycle events)
- All Amavis content-filter output (verdict, score, virus name, per-policy bank decisions)
- All OpenDMARC verdict lines (`policy=`, `disposition=`)
- All OpenDKIM signing and verifying output

- slapd's syslog output (only because `slapd.conf` is explicitly configured to use the `mail` facility — see LDAP & RemoteAuth)
- OpenARC output if the optional service is enabled

What is **not** here:

- **nginx access / error logs** — not configured to ship to syslog; read them with `docker exec hermes_nginx tail -f /var/log/nginx/...` or via Admin Console Firewall / Intrusion Prevention for the security view.
- **Authelia auth logs** — written to `/remotelogs/authelia/ authelia.log` for fail2ban consumption; see Authentication Settings and Intrusion Prevention.
- **Dovecot login / IMAP logs** — written to `/remotelogs/dovecot/dovecot-info.log` for fail2ban; the LMTP delivery side that Postfix talks to is visible here because Postfix logs the LMTP handoff result.
- **CommandBox / Lucee application logs** — Lucee internal logs live under the Lucee server home on the data tier, not in `SystemEvents`.
- **Container stdout/stderr** — `docker logs <name>` only.

This page is the operator's one-stop view for *mail-flow* questions. Auth and HTTP-side concerns have their own log surfaces.

The `SystemEvents` schema

`config/database/syslog_schema.sql` defines the table (MyISAM, `latin1_swedish_ci` — rsyslog's canonical schema, kept verbatim for compatibility). The viewer touches only four columns:

Column	Type	Used for
`ReceivedAt`	`datetime`	Date-range filter, sort order, displayed timestamp
`Message`	`text`	The log line body
`SysLogTag`	`varchar(60)`	Facility filter; rendered as a badge per row. Format is typically `<program>[<pid>]:` (e.g. `postfix/smtpd[12345]:`)
`Facility`	`smallint`	Present but not read by the viewer

Two indexes ship in the baseline schema:

```
KEY `idx_systemevents_receivedat` (`ReceivedAt`),
KEY `idx_systemevents_tag_receivedat` (`SysLogTag`, `ReceivedAt`)
```

The composite covers both the bare date-range query and the facility-filtered date-range query (which uses `SysLogTag LIKE '<facility>%'` and an `ORDER BY ReceivedAt DESC`). Issue #184, which tracked the missing indexes, was closed when these were added to `syslog_schema.sql`; existing installs pick them up via the `schema_updates.sql` path.

The Facility dropdown is populated by a separate query that pulls distinct values of `SUBSTRING_INDEX(SysLogTag, '[', 1)` over the current date range — so the available facilities reflect what actually logged during the window, not a static enum.

Fields on the page

Log Retention

Stored in `parameters2` with `parameter = 'system_log_retention'` and `module = 'systemlog'`. The dropdown offers 7 / 15 / 30 / 60 / 90 / 120 / 180 days; the seed value is 30. Saving the form just updates the row — it does not run the cleanup immediately.

The actual deletion runs in `schedule/message_cleanup.cfm`, scheduled by Ofelia (the in-stack cron container) once per night. The cleanup job reads the retention value, computes `today - N days`, and runs:

```
DELETE FROM SystemEvents WHERE ReceivedAt < '<cutoff-date>'
```

This is the same cleanup job that prunes the Amavis quarantine on the data tier — log retention and quarantine retention share the schedule but have independent thresholds. See Scheduled Tasks for the full Ofelia job list and how to run the cleanup on demand.

> **Operational consequence.** Changing the retention value does not shrink the table until the next nightly cleanup runs. To force an immediate prune after dialing the value down, trigger the cleanup job from the Scheduled Tasks page.

Start Date / Time and End Date / Time

Tempus Dominus datetime pickers with second-level resolution. Defaults are the last 24 hours (midnight-to-midnight on today rounded back). Both go into the query as `cf_sql_timestamp` parameters via `cfqueryparam` — there is no string concatenation in the SQL.

Facility

A Tom Select multi-select. Empty (no chips) means "all facilities". Selecting one or more populates a `SysLogTag LIKE '<facility>%'` clause per chip, OR'd together. The facility list is recomputed every time the page loads against the current date range — there is no cached enum.

Limit

One of `1000 / 1500 / 2500 / 5000 / 10000 / 15000`. The viewer validates against this exact list and falls back to `1000` if an out-of-range value is passed. A yellow callout appears when the selected limit is 10000 or higher.

> **Why the cap and not unlimited.** The DataTable widget needs to render every row into the DOM up front (it does not use server-side pagination). A 10,000-row table is already heavy in the browser; an unbounded fetch on a multi-month-deep `SystemEvents` table would lock the page.

Reading the badges

The Facility badge contains the raw `SysLogTag` value, which Postfix and friends format as `<program>[<pid>]:`. A few high-frequency tags worth recognising:

Tag (prefix match)	Meaning
`postfix/smtpd`	Inbound SMTP — connection, EHLO, helo, rcpt, milter results
`postfix/cleanup`	Header normalisation, header_checks, milter signing
`postfix/qmgr`	Queue manager — message scheduling, expiry
`postfix/smtp`	Outbound delivery to remote MX
`postfix/lmtp`	Local delivery to Dovecot
`postfix/bounce`	Bounce message generation
`amavis`	Content-filter verdicts (`Passed CLEAN`, `Blocked SPAM`, virus names)
`opendkim`	DKIM signing on outbound, verifying on inbound
`opendmarc`	DMARC alignment verdicts
`openarc`	ARC seal verdicts (if enabled)

Tag (prefix match)	Meaning
`slapd`	LDAP — bind / search / modify operations

A row's badge is exact-match for sort but prefix-match for the filter — selecting `postfix/smtpd` in the Facility dropdown matches `postfix/smtpd[12345]`, `postfix/smtpd[12346]`, and so on.

Performance notes

With the two baseline indexes the common query shapes are O(log n) on `ReceivedAt`:

- Last-24-hour, all facilities, limit 1000 — fast on any table size.
- Last-24-hour, one facility, limit 1000 — covered by the composite index, also fast.
- Multi-month window, all facilities, limit 10000 — slow on large tables; the index narrows the range but 10000 rows of `text` data is the bottleneck. Pull a tighter window.
- `SELECT DISTINCT SUBSTRING_INDEX(SysLogTag, '[', 1)` for the facility dropdown — fast on a 24-hour window, noticeably slower on weeks-deep windows because the index does not help with the expression.

If the table has grown into the tens of millions of rows because retention was left at 180 days on a high-traffic gateway, dial retention down and let the next nightly cleanup prune, or run the cleanup job manually from Scheduled Tasks.

Related pages

- Mail Queue — live view of what Postfix is holding; pair with this page to trace a stuck message from queue to log.
- Scheduled Tasks — the Ofelia job that runs the retention cleanup.
- LDAP & RemoteAuth — context on why slapd appears in `mail.*` (it is configured to use the `mail` facility).
- Intrusion Prevention and Admin Console Firewall — auth-side and HTTP-side log surfaces that do not land in `SystemEvents`.
- Authentication Settings — Authelia log location and what auth events look like on disk.

Revision #48
Created 2026-05-31 12:52:04 UTC by Dino Edwards
Updated 2026-06-20 13:33:02 UTC by Dino Edwards