Release Notes for Dovecot Pro Minor release 2.3.2.1

Table of Contents

1. Shipped Products and Versions

Dovecot Pro 2.3.2.1
Including Object Storage Plug-in, Full Text Search and Pigeonhole Sieve Plug-in

2. Release Highlights

- Added SSL support for proxied LMTP connections.
- fs-dictmap support (e.g. Cassandra) for non-sproxyd obox storage connectors.
- Added support for IMAP FILTER=SIEVE extension (manual application of Sieve filters via IMAP commands).
- Added "doveadm mailbox cache decision" and "doveadm mailbox cache remove" commands.

3. Upgrade Instructions

- When **obox** and **stats** plugin are used, the user setting for the metacache-worker service should be commented out (or set to root). E.g.:

```
service metacache-worker {
  # Remove the setting completely or use user=root
  # user=vmail doesn't work anymore!
  user = root
}
```

This prevents metacache-worker from excessively logging errors:

```
open(/proc/self/io) failed: Permission denied
```

[See DOV-2359 change below for further information.]

- In `obox_fs` setting, **bulk_delete** and **bulk_link** settings must be removed from the URL string if they exist.

[See DOV-2393 change below for further information.]

4. Known Issues

- When "`mail_attachment_detection_options=add-flags-on-save`" is used to create attachment indicator flags on delivery, object storage using the S3 connector can stop working.

Solution: remove the configuration option.

Non-S3 object storage connectors are **not** affected.

5. Detailed Changes

5.1.   v2.3.x Specific Changes

These issues only affected earlier v2.3.x releases; they are not present in v2.2.x releases.

5.1.1.   Dovecot Pro Core

- **ISSUE DOV-1757:** mail_fsync setting's value was ignored. The default mail_fsync=optimized was always used.

- **ISSUE DOV-1984:** LUA auth: When deinitializing, Lua scripts are kept referenced even when they have been destroyed, which can lead into crash.

- **ISSUE DOV-2015:** SSL/TLS servers may have crashed if client disconnected during handshake.

- **ISSUE DOV-2043:** lda/lmtp: Unencoded UTF-8 in email address headers may cause: Panic: file smtp-address.c: line 530 (smtp_address_write): assertion failed: (smtp_char_is_qpair(*p))

- **ISSUE DOV-2043:** lda/lmtp: Unencoded UTF-8 in email address headers may cause: Panic: file smtp-address.c: line 530 (smtp_address_write): assertion failed: (smtp_char_is_qpair(*p))

- **ISSUE DOV-2072:** SSL/TLS client: Fixed assert-crash when server certificate returns subjectAltNames, but none of them matches the expected certificate: Panic: file iostream-openssl-common.c: line 177 (openssl_cert_match_name): assertion failed: (*reason_r != NULL)

- **ISSUE DOV-2081:** LMTP and Submission service have an implicit hard message size limit of 40 MB, which causes the connection to get dropped during transfer.

- **ISSUE DOV-2094:** The lda -f parameter does not allow empty/null envelope sender address.

- **ISSUE DOV-2097:** Sieve crashes with an assert panic when the Return-Path header value has no opening '<'.

- **ISSUE DOV-2124:** When ssl iostream is being destroyed before it has been handshaked, attempt to close the stream can cause handshaking which attempts to use NULL pointer resulting in a crash.

- **ISSUE DOV-2143:** Dovecot systemd unit restrictions are too strict, and prevent certain external operations, such as PAM authentication and sieve mail sending. (v2.3-only)

- **ISSUE DOV-2222:** lmtp: The login_greeting setting is ignored.

- **ISSUE DOV-2223:** The submission service ignores the rawlog_dir setting, making it impossible to record the protocol exchange between the user's client and submission service.

- **ISSUE DOV-2235:** lmtp: Segfault occurs when LMTP session has multiple recipients and delivery to a non-first recipient fails at DATA stage (e.g. out of quota)

- **ISSUE DOV-2256:** If there is lots of logs being produced, dovecot can crash with one of:
  - Fatal: master: service(imap): child ... returned error 82 (Internal logging error)
  - Panic: file http-client.c: line 705 (http_client_global_context_ioloop_switched): assertion failed: (cctx != NULL)

- **ISSUE DOV-2257:** SMTP client crashes: Panic: file ostream.c: line 394 (o_stream_send_istream): assertion failed: (!_outstream->finished)

- **ISSUE DOV-2293:** lda -f parameter didn't allow username without @domain part

- **ISSUE DOV_2296:** On unhibernation imap process always logged "Debug: Unhibernation sync" message even with mail_debug=no.

- **ISSUE DOV-2321:** doveadm-server: TCP connections are hanging when there is a lot of network output. This especially caused hangs in dsync-replication.

- **ISSUE DOV-2419:** lmtp may crash with lmtp_rcpt_check_quota=yes: Panic: file lib-event.c: line 182 (event_pop_global): assertion failed: (event != NULL)

5.2.   Other Changes (v2.2.x & v2.3.x)

5.2.1.   Dovecot Pro Core

- **CHANGE DOV-2359:** stats: Open /proc/self/io earlier to avoid a potential security hole
  - **CHANGE:** stats: Open /proc/self/io at process startup while still running as root. The previous version temporarily enabled PR_SET_DUMPABLE while opening it, which could have temporarily enabled other processes to ptrace it, causing potential security problems.

- **NEW FEATURE DOV-2065:** Added "doveadm mailbox cache decision" command for changing cache decisions in mailbox cache (dovecot.index.cache file) and "doveadm mailbox cache remove" command for removing fields from cache. See doveadm-mailbox(1) man page for details.

- **IMPROVEMENT DOV-1092:** LMTP: Add support for making raw protocol logs using the lmtp_rawlog_dir and lmtp_proxy_rawlog_dir settings. This allows recording the client/server protocol exchange and the protocol exchange between server and the proxied backend respectively.

- **IMPROVEMENT DOV-1941:** LMTP: Add support for making TLS proxy connections. Before, TLS-related fields returned from passdb were ignored and the connection was always plaintext.

- **IMPROVEMENT DOV-2095:** submission: Add submission_client_workarounds setting to implement workarounds for clients that send MAIL and RCPT commands with additional spaces before the path and for clients that omit <> brackets around the path. See example-config/conf.d/20-submission.conf.

- **IMPROVEMENT DOV-2117:** Lua auth: Add password_verify() function and additional fields in auth request.

- **IMPROVEMENT DOV-2120:** lda/lmtp: Allow omission of '<' and '>' in the Return-Path header. This is strictly a syntax violation, but this is now allowed (once more) to account for a rather wide selection of software that does not follow the standards.

- **IMPROVEMENT DOV-2262:** Added more details to error messages logged during IMAP/POP3 login. These may help with debugging performance problems during logins.

- **ISSUE DOV-1045:** "doveadm user delete" doesn't delete folders where the user doesn't have a lookup ("l") ACL right.

- **ISSUE DOV-1592:** "doveadm reload" logs empty errors if the new configuration has errors

- **ISSUE DOV-1722:** obox may have crashed with signal 11 when reading index bundles.

- **ISSUE DOV-1918:** Crash occurs at startup when multiple type=shared mdbox/obox namespaces have been configured.

- **ISSUE DOV-2013:** Dovecot sends out all certificate chains when alt cert is used, when it is supposed to send only the cert chain for the respective cert. Fix requires openssl 1.0.2 or later.

- **ISSUE DOV-2019:** imapc: Backend folder's UIDVALIDITY change wasn't detected correctly. This resulted in errors: Mailbox 'INBOX' state corrupted: Expunged message uid=... reappeared - reconnecting (delay 0 ms)

- **ISSUE DOV-2110:** imapc: Duplicate UIDs on a remote IMAP server aren't detected with imapc_features=fetch-msn-workarounds or no-msn-updates. This results in: Panic: file imapc-mailbox.c: line 533 (imapc_untagged_fetch): assertion failed: (lseq == mbox->sync_next_lseq)

- **ISSUE DOV-2113**: imapc: If SELECT INBOX fails with NO, CREATE IN-BOX is sent

- **ISSUE DOV-2116:** imapc: If a broken remote IMAP server sends untagged FETCH reply where key-value pair is missing the value, the process seg-faults.

- **ISSUE DOV-2167:** dsync: Locking fails for new users, because home direc-tory isn't created automatically: Error: Couldn't lock .../.dovecot-sync.lock: safe_mkstemp(.../.dovecot-sync.lock) failed: No such file or directory

- **ISSUE DOV-2251:** fs-posix: Directory iteration doesn't list symlinks with nonexistent destination on NFS with nordirplus mount option.

- **ISSUE DOV-2258:** Cassandra: read_consistency=quorum couldn't be used. However, it existed with empty name, i.e. "read_consistency=" enabled the quorum.

- **ISSUE DOV-2329:** IMAP COMPRESS: Connection wasn't cleanly closed by sending the "end of compressed file" marker.

- **ISSUE DOV-2358:** Obsolete dovecot.index.cache offsets are sometimes used. Trying to fetch a field that was just added to cache file may not have always found it.

5.2.2.   Object Storage Plug-in

- **IMPROVEMENT DOV-2272:** Support fs-dictmap (Cassandra) more efficiently with other object storages besides just sproxyd.
  - storage-objectid-prefix=<prefix> : Store all objects as <prefix>/<ob-jectid>. The objects can be efficiently copied within the dict. This set-ting should be used in obox_fs for storing mails under <prefix>. For example storage-objectid-prefix=%u/mails/
  - storage-passthrough-paths=full|read-only : Assume that object ID is the same as the path. Objects can't be copied within the dict. This setting should be used for obox_index_fs and fts_dovecot_fs, be-cause they don't need to support copying objects.
    - With "full" the object ID is written to dict as an empty value (because it's not used).
    - The "read-only" can be used for backwards compatibility so that the path is still written to the dict as the object ID, even though it's not used (except potentially by an older Dovecot version).
  - storage-objectid-migrate : This is expected to be used with storage-objectid-prefix when adding fs-dictmap for an existing installation. The newly created object IDs have "<storage-objectid-prefix>/<object-id>" path while the migrated object IDs have "<user>/mailboxes/<mailbox-guid>/<oid>" path. The newly created object IDs can be detected from the 0x80 bit in the object ID's extra-data. Migrated object IDs can't be copied directly within dict - they'll be first copied to a new object ID us-ing the parent fs. Note that this setting must not be removed after-wards, otherwise access to the old object IDs will fail.
    - storage-objectid-migrate-*.sh scripts are provided to perform the migration. NOTE: Make sure the user can't be accessed

during migration, not even new mail deliveries. Also be sure to run "doveadm metacache flush" for the user before calling the scripts. Otherwise a background flush might change the mailbox.

- o Example configuration with migration enabled:

```
obox_fs = fscache:1G:/var/lib/fscache:dictmap:proxy:dict-
async:cassandra ; s3:http://storage.example.com/ ; refcount-
ing-table:storage-objectid-prefix=%u/mails/:storage-ob-
jectid-migrate:bucket-size=10000:bucket-cache=%h/buck-
ets.cache:delete-timestamp=+10s:bucket-deleted-days=10

obox_index_fs = dictmap:proxy:dict-async:cassandra ;
s3:http://storage.example.com/ ; diff-table:storage-
passthrough-paths=full

plugin {
  fts_dovecot_fs = fts-cache:fscache:1G:/var/lib/ftscache:
s3:http://storage.example.com/ ; dict-prefix=%u/fts/:stor-
age-passthrough-paths=full
}
```

- **CHANGE DOV-2253:** service metacache-worker's default user was changed from $default_internal_user (dovecot) to root. This process's configuration should be similar to lmtp/doveadm, which also use root as the default.

- **ISSUE DOV-1913:** "doveadm user delete" doesn't fully finish deleting the user if
  - o folders are broken and require resyncing
  - o user's metacache root directory had subdirectories, like sieve/ or fts/

- **ISSUE DOV-2259:** fs-dictmap: If lockdir setting wasn't used and multiple copies of the same mail were being deleted in the same transaction, this caused multiple DELETEs with the same object ID to be sent to the object storage.

- **ISSUE DOV-2293**: fs-swift, fs-scality: Bulk delete/link requests fail because they have too many files

- **ISSUE DOV-2394:** obox: Moving user to another backend may wrongly cause self-bundle to be created instead of base-bundle

- **ISSUE DOV-2393:** fs-swift, fs-scality: Bulk delete/link requests fail because they have too many files
  - o bulk_delete_limit=1000 and bulk_link_limit=1000 in the URL parameters are now the default settings, which can be changed to change the limits. Setting them to 0 disables the bulk operations.
  - o bulk_delete and bulk_link settings have been removed. They are now enabled by default. Disabling can be done with bulk_delete_limit=0 and bulk_link_limit=0.

5.2.3.   Full Text Search

- **ISSUE DOV-2173:** FTS indexing may crash with: Panic: file fts-index-merge.c: line 271 (fts_index_merge_do_merge): assertion failed: (newidx > idx1 && newidx > idx2)

- **ISSUE DOV-2334:** Using fts_dovecot with compression or encryption caused "fts_dovecot: Index keeps changing under us too rapidly" errors.

5.2.4.   Pigeonhole Sieve Plug-in

- **IMPROVEMENT DOV-2312:** Pigeonhole: Implemented an IMAP plugin that adds support for manually/explicitly applying Sieve filters on messages stored in a mailbox. This is a vendor-defined Dovecot extension to the IMAP protocol.

- **ISSUE DOV-2099:** The LDA Sieve plugin attempts to execute the sieve_discard script when an error occurs. This can lead to the message being lost.

- **ISSUE DOV-2131:** Pigeonhole: The Sieve editheader extension causes an assertion panic when it is used to manipulate a message header with a very large field: Panic: file istream.c: line 197 (i_stream_read): assertion failed: ((size_t)ret+old_size == _stream->pos - _stream->skip)

- **ISSUE DOV-2160:** Pigeonhole: The subject header for a vacation response is statically truncated to 256 bytes, which is too limited for multi-byte UTF-8 characters.

- **ISSUE DOV-2218:** Pigeonhole: The Sieve address test causes and assertion panic for invalid addresses with UTF-8 codepoints in the local part. (v2.3-only)

6. Tests

The Dovecot QA team has successfully verified all issue fixes that could be reproduced within a lab environment.

To avoid side effects, the shipped packages have gone through automated regression test on both, a Continuous Integration System and a dedicated server setup for system and integration testing.

All changes have been checked for potential side-effects and effect on behavior. Unless explicitly stated within this document, we do not expect any side-effects.