Release Notes for OX Dovecot Pro Minor Release v2.3.10.1 (Revised)

Table of Contents

1. Shipped Products and Versions

OX Dovecot Pro v2.3.10.1
Built on Dovecot Community Edition Core v2.3.10
Including Object Storage (obox) and Full Text Search (FTS) Plug-ins

Supported OS Distributions:

- Amazon Linux 2
- CentOS 6.9, 7.7
- RHEL 6.9, 7.4
- Debian stretch (9.12), buster (10)
- Ubuntu 16.04 LTS (xenial), 18.04 LTS (bionic)

Apache Cassandra Driver: v2.13

2. Release Highlights

SECURITY FIXES

This release fixes three security issues. It is urged that all installations of Dovecot newer than 2.3.0 are upgraded to apply the fixes. The issues are summarized below. Further details will be made available, when the issues are disclosed to the public.

These vulnerabilities were discovered by a responsible third party. Open-Xchange has no knowledge of these exploits being used as targeted attacks in the wild.

The release notes are CONFIDENTIAL and restricted to OX Dovecot Pro customers only. Public disclosure of the CVE issues will occur on or after 18 May 2020.

LMTP/Submission crash on empty local part

The LMTP and Submission services crash when the local-part of an address is "" (double quotes). For LMTP, this can only happen if the MTA passes through all mail deliveries to Dovecot and lets Dovecot determine if a user exists.

This issue is present in Dovecot since version 2.3.0.

Workaround:

For submission there is no workaround, but triggering the bug requires valid credentials.

For LMTP, one can implement sufficient filtering on MTA level to prevent mails with such addresses from ending up in LMTP delivery.

CVE-2020-10967; CVSS Score: 5.3 (CVSS3.1:AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

LMTP/Submission crash on malformed NOOP

Sending a malformed NOOP command causes a crash in submission, submission-login, or LMTP service. For LMTP, this can only occur if the LMTP service is open to the public (NOT RECOMMENDED) or the local MTA is malicious.

This issue is present in in Dovecot since version 2.3.0.

CVE-2020-10957; CVSS: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Possible LMTP/submission crash on invalid commands

Sending many invalid or unknown commands can cause the server to access freed memory, which can lead to a server crash. This happens when the server closes the connection with a "`421 Too many invalid commands`" error. The bad command limit depends on the service (LMTP or submission) and varies between 10 to 20 bad commands.

This issue is present in in Dovecot since version 2.3.0.

CVE-2020-10958; CVSS: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)

AWS S3 IAM

Dovecot now supports AWS Identity and Access Management (IAM) for authenticating requests to AWS S3 using the AWS EC2 Instance Metadata Service (IMDS). Version 2 of IMDS (IMDSv2) is supported.

To use this feature, Dovecot must be running on an AWS EC2 instance which supports the service. Additionally, an IAM role must be configured which allows trusted entities, EC2 in this case, to assume that role.

Full details on how to configure can be found at:
https://doc.dovecot.org/configuration_manual/mail_location/obox/amazon_s3/.

Maximum Parallel Iterations Setting (Obox)

This new setting allows configuration on how many dict iterations can be used internally in parallel (i.e. retrieving information from Cassandra). Parallel iterations can potentially speed up opening huge folders when they're not yet in metacache.

Transaction Batching Improvements

IMAP MOVE, autoexpunge, and expunges now commits transactions in batches of 1000 mails.

For autoexpunge, this helps with the lazy_expunge feature when expunging many messages (10,000s) to make sure that the progress always moves forward even if the process is killed.

For IMAP MOVE, this helps to avoid situations where multiple IMAP sessions are running the same MOVE command and duplicating the mails in the lazy_expunge folder. With this change there can still be some duplication, but the MOVE always progresses forward.

Summary of Highlights

- Fix security issues CVE-2020-10967, CVE-2020-10957, and CVE-2020-10958
- AWS S3 IAM support
- Obox maximum parallel iterations setting (for use with Scality sproxyd+Cassandra)
- Transaction batching improvements (autoexpunge, IMAP MOVE)
- S3 batch/bulk delete
- Sysreport tool (see https://doc.dovecot.org/admin_manual/troubleshooting/)

- Disable all retpoline mitigations, due to severe performance regressions.
- Add support for IMAP features:
  - \Important SPECIAL-USE flag (RFC 8457)
  - STATUS=SIZE (RFC 8438)

3. Upgrade Instructions

- `max-parallel-iter` parameter [obox; see DOV-3517]
  - See https://doc.dovecot.org/configuration_manual/mail_location/obox/dictmap/
- S3 max parallel deletes [obox; see DOV-3577]
  - See https://doc.dovecot.org/configuration_manual/mail_location/obox/amazon_s3/#deleting-multiple-objects-per-request
- Webpush proxy support [COI; see DOV-3656]
  - See https://doc.dovecot.org/configuration_manual/coi/
- Add `fs_dictmap_object_lost` event [core; see DOV-3663]
  - See https://doc.dovecot.org/admin_manual/list_of_events/#fs-dictmap-object-lost
- Add SASL SCRAM-SHA-256 mechanism [core; see DOV-3664]
- Add `metric { group_by }` setting [core; see DOV-3671]
  - See https://doc.dovecot.org/configuration_manual/stats/#group-by
- Add `loghdr` parameter for obox drivers [obox; see DOV-3675]
  - These headers are included in the http_request_finished event as fields prefixed with `http_hdr_`.
  - Configuring `loghdr` for `x-amz-request-id` and `x-amz-id-2` tells Dovecot to include this information in any error, debug or warning message. This additional information helps when Troubleshooting Amazon S3 (see https://docs.aws.amazon.com/AmazonS3/latest/API/RESTCommonResponseHeaders.html). You can add multiple other `loghdr` parameters, if needed.
- AWS IAM tokens supported [obox; see DOV-3734, DOV-3761, DOV-3764]
  - See https://doc.dovecot.org/configuration_manual/mail_location/obox/amazon_s3/
- For Debian packages, this release changes the `dovecot-ee-submissiond` from a dependency to a suggestion. In OX Dovecot Pro v2.3.9, this package was split from `dovecot-ee-core` and made a hard dependency. With this change, Dovecot Submission has now completed its transition to an independent package.

Recommendations and Configuration Review Hints:

- Recommendation: DOV-3714 improves performance of the `lazy_expunge_only_last_instance` option. A reminder that this option should ONLY be set if you are using fs-dictmap (e.g. Cassandra/sproxyd). With other drivers, this setting causes unnecessary extra object storage operations.
- Warning: `ssl_client_ca_file` reads certs into memory. In a standard CentOS 7 CA bundle it uses about 800 kB of memory. This gets multiplied by

thousands of imap processes leading to a lot of wasted memory. See https://doc.dovecot.org/settings/core/#ssl-client-ca-file for alternatives.

4. Known Issues

- Not all Dovecot 2.2.x logging has been converted to Dovecot 2.3.x events, so newer logging/metrics configuration will not work on these older log entries.

5. Detailed Changes

5.1. Dovecot Pro Core

- **SECURITY DOV-3846**: lmtp/submission: Issuing the RCPT command with an address that has the empty quoted string as local-part causes the lmtp service to crash. (CVE-2020-10967)

- **SECURITY DOV-3874**: lmtp/submission: A client can crash the server by sending a NOOP command with an invalid string parameter. This occurs particularly for a parameter that doesn't start with a double quote. This applies to all SMTP services, including submission-login, which makes it possible to crash the submission service without authentication. (CVE-2020-10957)

- **SECURITY DOV-3875**: lmtp/submission: Sending many invalid or unknown commands can cause the server to access freed memory, which can lead to a server crash. This happens when the server closes the connection with a "421 Too many invalid commands" error. The bad command limit depends on the service (lmtp or submission) and varies between 10 to 20 bad commands. (CVE-2020-10958)

- **ISSUE DOV-3594**: Fixed auth lookup privilege problem when imap process is reused and user is un-hibernated: Error: net_connect_unix(/run/dovecot/auth-master) failed: Permission denied.

- **ISSUE DOV-3598**: Mailbox synchronization may have assert-crashed in some rare situations: Panic: file mail-transaction-log.c: line 25 (mail_transaction_log_set_head): assertion failed: (log->files != NULL).

- **ISSUE DOV-3600**: lib-smtp client could have assert-crashed if STARTTLS handshake finished earlier than usually: Panic: file smtp-client-connection.c: line 1212 (smtp_client_connection_established): assertion failed: (!conn->connect_succeeded).

- **ISSUE DOV-3617**: Fix potential crash when copying/moving mails within the same folder. This happened only when there were a lot of fields in dovecot.index.cache.

- **IMPROVEMENT DOV-3628**: Add tool for generating sysreport. This generates a bundle of information usually needed for support requests.

- **ISSUE DOV-3629**: Recreating dovecot.index.cache file could have crashed when merging bitmask fields: Panic: file array.c: line 10 (array_idx_modifiable_i): assertion failed: (idx < array->buffer->used / array->element_size).

- **IMPROVEMENT DOV-3636**: Use TCP_QUICKACK to reduce latency for some TCP connections.
  - Fixes v2.3 regression with SMTP client connections.

- **IMPROVEMENT DOV-3647**: Autoexpunging now expunges mails in batches of 1000 mails. This helps especially with lazy_expunge when expunging a lot of mails (e.g. millions) to make sure that the progress always moves forward even if the process is killed.

- **ISSUE DOV-3649**: v2.3.9.2 regression: imap-hibernate process crashed if unhibernation for a user fails because imap-master communication times out or gets disconnected too early.

- **IMPROVEMENT DOV-3651**: Made the quota-status service more robust against erroneous use with Postfix ACL policies other than smtpd_recipient_restrictions.

- **ISSUE DOV-3652**: quota: Addresses with special characters in the local part caused problems in the interaction between Postfix and Dovecot through the quota-status service. Postfix sent its own internal representation in the recipient field, while Dovecot expected a valid RFC5321 mailbox address.

- **ISSUE DOV-3653**: Some services could respawn unthrottled if they crash during startup.

- **ISSUE DOV-3663**: Add fs_dictmap_object_lost named event for "Object exists in dict, but not in storage".

- **IMPROVEMENT DOV-3664**: Support SCRAM-SHA-256 authentication mechanism.

- **IMPROVEMENT DOV-3665**: Add support for the IMAP \Important SPECIAL-USE flag (RFC 8457).

- **ISSUE DOV-3666**: mdbox didn't preserve date.saved with dsync.

- **IMPROVEMENT DOV-3671**: Add `metric { group_by }` setting. This allows automatically creating new metrics based on the fields you want to group statistics by.

- **IMPROVEMENT DOV-3672**: IMAP MOVE now commits transactions in batches of 1000 mails. This helps especially with lazy_expunge when moving a lot of mails. It mainly avoids situations where multiple IMAP sessions are running the same MOVE command and duplicating the mails in the lazy_expunge folder. With this change there can still be some duplication, but the MOVE always progresses forward. Also, if the MOVE fails at some point, the changes up to the last 1000 mails are still committed instead of rolled back. Note that the COPY command behavior hasn't changed, because it is required by IMAP standard to be an atomic operation.

- **ISSUE DOV-3710**: cassandra: CASS_ERROR_SERVER_WRITE_FAILURE error should also be treated as "uncertain write failure".

- **IMPROVEMENT DOV-3712**: Implement `lazy_expunge_only_last_instance=yes` in a bit more reliable way, which tracks the files/objects rather than GUIDs. This also improves performance in case GUIDs weren't already indexed/cached.
  - Only obox with fs-dictmap has ever supported `lazy_expunge_only_last_instance=yes`.

- **ISSUE DOV-3718**: Regression introduced in dovemon 2.3 release where backend update scripts (`beupdatescript` in dovemon configs) were not executed when marking a host down or bringing it back up.

- **ISSUE DOV-3721**: v2.3.8 regression: Using public/shared folders with INDEXPVT configured to use private \Seen flags, trying to search seen/unseen in an empty folder crashes with segfault.

- **ISSUE DOV-3722**: Trusted connections crash in second connection's EHLO if `submission-login { service_count }` is something else than 1 (which is the default).

- **ISSUE DOV-3723**: submission-login does not properly encode the SESSION field of the XCLIENT command. Particularly, a '+' character introduced by the session ID's Base64 encoding causes problems.

- **ISSUE DOV-3726**: INBOX ACLs shouldn't apply for IMAP GETMETADATA/SETMETADATA commands.

- **ISSUE DOV-3731**: FTS Solr: The XML response parser fails to parse large/chunked responses correctly. This leads to spurious parse errors, most notably: "Error: fts_solr: received invalid uid '0'".

- **ISSUE DOV-3732**: Add "revision" field support to `imap_id_send` setting. Using "`revision *`" will send in IMAP ID command response the short commit hash of the Dovecot git source tree HEAD (same as in “`dovecot --version`”). This is not intended for production use.

- **CHANGE DOV-3733**: IMAP ENVELOPE includes now all addresses when there are multiple headers (From, To, Cc, etc.) The standard way of having multiple addresses is to just list them all in a single header. It's non-standard to have multiple headers. However, since MTAs allow these mails to pass through and different software may handle them in different ways, it's better from security point of view to show all the addresses.

- **IMPROVEMENT DOV-3736**: IMAP EXPUNGE and CLOSE now expunges mails in batches of 1000 mails. This helps especially with lazy_expunge when expunging a lot of mails (e.g. millions) to make sure that the progress always moves forward even if the process is killed.

- **IMPROVEMENT DOV-3741**: Include mailbox name in `push_notification_finished` event.

- **ISSUE DOV-3741**: Do not send push notification event if nothing was done. This happens when mail transaction is started and ended with no changes.

- **IMPROVEMENT DOV-3753**: Event filters now support using "`field_name=`" to match a field that doesn't exist or has an empty value.
  - For example, use "`error=`" to match only events that didn't fail.

- **IMPROVEMENT DOV-3754**: Using quota_clone configured with dict-redis can crash when Redis responds slowly: Panic: file quota-clone-plugin.c: line 240 (quota_clone_mail_user_deinit_pre): assertion failed: (!quser->quota_flushing).

- **IMPROVEMENT DOV-3756**: Support the new IMAP STATUS=SIZE capability.

- **ISSUE DOV-3758**: Submission: XCLIENT command is never used in the protocol exchange with the relay MTA when `submission_backend_capabilities` is configured, even when the relay MTA is properly configured to accept the XCLIENT command.

- **IMPROVEMENT DOV-3782**: Disable all retpoline mitigations, due to severe performance regressions.

- **ISSUE DOV-3794**: v2.3.8 regression: Large base64-encoded mails weren't decoded properly. This could have affected searching/indexing mails and message snippet generation. Note: previously indexed messages will not be automatically fixed.

- **ISSUE DOV-3811**: Message with only quoted text could have caused message snippet to ignore its 200-character limit and return the entire message. This was added also to dovecot.index.cache file, which increased disk space and memory usage unnecessarily. v2.3.9.2 regression (previous versions cached the quoted snippet as empty).

- **ISSUE DOV-3811**: In a large mail, quoted text could have become wrongly added to the snippet, possibly mixed with non-quoted text.

5.2. Object Storage (obox) Plug-in

- **IMPROVEMENT DOV-3517**: fs-dictmap (obox/Cassandra): Add the `max-parallel-iter` setting. This new setting allows to configure how many dict-iterations can be used internally in parallel. The default value is 1. Parallel iterations can especially help speed up opening huge folders when they're not yet in metacache.

- **IMPROVEMENT DOV-3577**: fs-s3: Implement bulk-deletion for up to 1000 objects per request.

- **ISSUE DOV-3598**: New index merging might assert-crash if dovecot.index.log rotation also happens at the same time: Panic: file mail-transaction-log.c: line 229 (mail_transaction_logs_clean): assertion failed: (!file->locked || file->refcount > 0).

- **ISSUE DOV-3634**: obox: Moving mails inside a mailbox now updates the save-date.

- **ISSUE DOV-3668**: If there are queued metacache-worker commands (i.e. all workers were busy) while the metacache process is shutting down, it crashes:

Panic: file userdb.c: line 123 (user_free): assertion failed: (user_can_free(user)).

- **IMPROVEMENT DOV-3675**: Added "`loghdr`" parameter for obox drivers. These headers in HTTP responses are logged as part of any error, debug or warning messages related to the HTTP request. These headers are included in the http_request_finished event as fields prefixed with "`http_hdr_`".

- **IMPROVEMENT DOV-3675**: fs-scality, fs-azure: Use exponential backoff for retrying 5xx errors (instead of hardcoded 1 second).

- **IMPROVEMENT DOV-3675**: fs-s3, fs-scality: Retry 5xx errors for iteration requests.

- **IMPROVEMENT DOV-3709**: Support using x-amz-* headers in "`addhdr`" parameter. These are now properly included as part of the AWS4 signature. This is especially useful with x-amz-security-token header.

- **ISSUE DOV-3713**: fs-dictmap: Prevent a panic that could occur when an inner fs-dictmap ioloop hits a specific codepath. Panic: file ioloop.c: line 673 (io_loop_handle_timeouts_real): assertion failed: (ioloop == current_ioloop)

- **IMPROVEMENT DOV-3714**: obox: Perform reference count lookups from Cassandra asynchronously with `lazy_expunge_only_last_instance=yes`. This allows doing multiple lookups in parallel and make the expunging finish faster.

- **IMPROVEMENT DOV-3734**: fs-aws-s3: Add the `aws-s3` scheme for using AWS S3 storage with default URL parameters.
    - Currently this is the same as using the s3 scheme with parameters: `auth_protocol=iam&addhdrvar=x-amz-security-token:%%{auth:token}&loghdr=x-amz-request-id&loghdr=x-amz-id-2`

- **IMPROVEMENT DOV-3737**: Fix a potential hang with fts_dovecot+S3 when doveadm obox user delete is deleting FTS indexes.

- **IMPROVEMENT DOV-3761**: S3 supports now AWS IAM tokens. The easiest way to configure this is to use the new "aws-s3" scheme.
    - See https://doc.dovecot.org/configuration_manual/mail_location/obox/amazon_s3/ for details.

5.3. Full Text Search (fts) Plug-in

No Changes

5.4. Pigeonhole (sieve) Plug-in

- **ISSUE DOV-3481**: Sieve trace debugging (`sieve_trace_dir=` setting) causes runtime errors when enabled for IMAPSieve on a mailbox that has a name containing slashes. This erroneously attempts to access a subdirectory in the trace log directory because the mailbox name including the slashes is part of the log file name.

- **ISSUE DOV-3655**: The Sieve "vacation" action compares the local part of addresses listed in the ":addresses" argument case-sensitively. This used to be performed case-insensitively for Dovecot v2.2.

- **ISSUE DOV-3717**: The administrator scripts defined for the IMAPSieve capability are not always executed in the numeric order used for the mailbox rules in the configuration. This problem can occur when several rules match at the same time for a mailbox event.

- **ISSUE DOV-3729**: Avoid logging info log messages for each message acted upon by the IMAPSieve and IMAP FILTER=SIEVE features. This can quickly fill administrator log files with often useless log messages. If enabled, debug messages are logged instead.

5.5. OX Engage (imap-injection) Plug-in

No Changes

5.6. Chat Over Imap (coi) Plug-in [beta]

- **IMPROVEMENT DOV-3656**: Support proxying for webpush driver. This allows specifying HTTP proxy with optional authentication for outgoing HTTP pushes.

- **IMPROVEMENT DOV-3667**: Webpush no longer sends push notifications for message delivery notifications.

5.7. Intercept (intercept) Plug-in

No Changes

6. Tests

The 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.

7. Repository Information

For details of how to install and update OX Dovecot Pro, please refer to the instructions at:

https://doc.dovecot.org/installation_guide/dovecot_pro_releases/repository_guide/.

8. Release Notes Revisions

- 27 April 2020: Added changelog entry for DOV-3649.