Release Notes for OX Dovecot Pro Minor Release v2.3.11

Table of Contents

1. Shipped Products and Versions 2
2. Release Highlights 2
3. Upgrade Information 3
4. Known Issues 4
5. Detailed Changes 4
5.1. OX Dovecot Pro Core 4
5.2. Object Storage (obox) Plug-in 10
5.3. Full Text Search (fts) Plug-in 11
5.4. Pigeonhole (sieve) Plug-in 11
5.5. OX Engage (imap-injection) Plug-in 11
5.6. Chat Over Imap (coi) Plug-in [beta] 11
5.7. Intercept (intercept) Plug-in 12
6. Tests 12
7. Repository Information 12

1. Shipped Products and Versions

OX Dovecot Pro v2.3.11
Built on Dovecot Community Edition Core v2.3.11
Including Object Storage (obox) and Full Text Search (FTS) Plug-ins

Supported OS Distributions:

- Amazon Linux 2
- CentOS 6.9, 7.8, 8.2
- RHEL 6.9, 7.4, 8.2
- Debian stretch (9.12), buster (10)
- Ubuntu 16.04 LTS (xenial), 18.04 LTS (bionic)

Apache Cassandra Driver: v2.13

2. Release Highlights

SECURITY FIX

This release fixes a security issue. It is urged that all installations of OX Dovecot Pro running v2.3.x upgrade to apply the fix. 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 15 July 2020.

Note: this release also fixes two additional authentication related CVE's contained in Dovecot Community Edition Core, CVE-2020-12673 and CVE-2020-12674. Neither of these affect OX Dovecot Pro as the authentication methods affected (NTLM, RPA) are not supported in Pro.

Deeply Nested MIME Structures

Parsing mails with many MIME parts could have resulted in excessive CPU usage or a crash due to running out of stack memory.

This issue is present in Dovecot since it was first released.

Fix: MIME nesting limits have been added.

CVE-2020-12100; CVSS Score: 7.5 (CVSS3.1:AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

OTHER HIGHLIGHTS

- OpenMetrics Exporter for Statistics
    - OX Dovecot Pro now natively supports metrics export via theOpenMetrics format, which allows for e.g. Prometheus ingestion. For information how to use this feature, see documentation at https://doc.dovecot.org/configuration_manual/stats/
- OAUTH: Support local validation/decoding of JWT Tokens

    - Users can now be authenticated to Dovecot using OAUTH without the need to contact a remote OAUTH2 server. See: https://doc.dovecot.org/configuration_manual/authentication/oauth2/#local-validation
- Events Improvements
    - This release continues to add additional events for monitoring, metrics, and debugging. Specifically, events for Dictionary and Metacache (obox) have been added. For more information, see: https://doc.dovecot.org/admin_manual/list_of_events/
- Auto-truncation of large index cache files
    - Added auto-truncation of large index cache files instead of requiring admin to manually delete these files. This may occur for users that have 100,000s of messages in a mailbox.
- RHEL 8/CentOS 8
    - RHEL 8/CentOS 8 support has been added. Note: support for RHEL6/CentOS 6 will be dropped in a future release

3. Upgrade Information

This section includes changes that may change Dovecot's behavior when compared to prior versions.

- Due to fixes in packaging, customers using mail-crypt need to ensure dovecot-ee-mail-crypt-plugin is installed. (Previously, mail-crypt would have worked if only the base dovecot-ee package was installed.)
- Event changes (https://doc.dovecot.org/admin_manual/list_of_events/):
    - imap_command_finished event's cmd_name field now contains "unknown" for unknown commands, rather than the command name that was sent. (The "cmd_input_name" field now contains the command name exactly as it was sent.)
    - smtp_server_command_started/finished event's cmd_name field now contains "unknown" for unknown commands, rather than the command name that was sent. (The "cmd_input_name" field now contains the command name exactly as it was sent.)
    - Renamed push_notification category to push-notification
    - sieve-* categories now have "sieve" as the parent category
    - Removed auth-master-client and auth-master-client-login categories. Their events now use "auth-client" category.
    - auth_request_finished event changes:
        - Removed "mechanism" field in favor of already existing "mech" field.
        - Renamed "original_username" to "orig_user"
        - Renamed "translated_username" to "translated_user"
    - Renamed auth_client_request_continue event to auth_client_request_continued.
    - Renamed "index" event category to "mail-index".
    - dns_client service renamed to dns-client
    - service:<name> category is now using the name from configuration file.
        - Most importantly this means that auth-worker process now uses "service:auth-worker" instead of "service:auth".
- session_id added to the default auth_policy_request_attributes setting.
- Log prefixes now use the service name from configuration file. For example, dict-async service will now use "dict-async(pid): " log prefix instead of "dict(pid): "

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. OX Dovecot Pro Core

- **SECURITY DOV-3963**: Parsing mails with a large number of MIME parts could have resulted in excessive CPU usage or a crash due to running out of stack memory. (CVE-2020-12100)
  - Nested MIME part count is now limited to 100. When the limit is reached, the innermost MIME part's body contains all the rest of the inner bodies until a parent MIME part is reached.
  - Total number of MIME parts is now limited to 10000. When it's reached, no more MIME boundary lines will be recognized, so the rest of the mail belongs to the last added MIME part.

- **IMPROVEMENT DOV-3670**: Add support for quantized sub-metrics. See https://doc.dovecot.org/configuration_manual/stats/ for details.

- **IMPROVEMENT DOV-3751**: Added mail_cache_max_size setting, which now defaults to 1 GB. If the cache file reaches this size, it becomes truncated to empty size.

- **IMPROVEMENT DOV-3783**: Support local validation and decoding of JWT tokens. This allows authenticating users with JWT tokens without contacting OAUTH2 server.

- **IMPROVEMENT DOV-3787**: Support the new IMAP SAVEDATE extension (RFC 8514).

- **IMPROVEMENT DOV-3799**: Add events for dictionaries. See https://doc.dovecot.org/admin_manual/list_of_events/#dictionaries

- **IMPROVEMENT DOV-3822**: dovecot.index.cache changes:
  - Renamed mail_cache_compress_* settings to mail_cache_purge_*. Note that these settings are mainly intended for testing and usually shouldn't be changed.
  - Renamed "index" event category to "mail-index".
  - Created a new "mail-cache" category and new events related to dovecot.index.cache handling. See https://doc.dovecot.org/admin_manual/list_of_events/#mail-cache for details.
    - mail_cache_decision_changed
    - mail_cache_purge_started
    - mail_cache_purge_drop_field
    - mail_cache_purge_finished
    - mail_cache_corrupted
    - mail_cache_record_corrupted

- **IMPROVEMENT DOV-3843**: Add session_id to the default auth_policy_request_attributes setting.

- **IMPROVEMENT DOV-3872**: Support disabling stats-writer socket by setting stats_writer_socket_path="".

- **IMPROVEMENT DOV-3873**: If a long-running transaction (e.g. SORT/FETCH on a huge folder) adds a lot of data to dovecot.index.cache file, commit those changes periodically to make them visible to other concurrent sessions as well. Previously it committed only at the end of the whole operation, which in some situations might even have lost all the changes if the cache file was purged during it.

- **IMPROVEMENT DOV-3894**: Add more consistency to events.
  - Changed event categories to make them more consistent:
    - Renamed push_notification category to push-notification
    - sieve-* categories now have "sieve" as the parent category
    - Removed auth-master-client and auth-master-client-login categories. Their events now use "auth-client" category.
  - Changed event fields to make them more consistent with %\{variable\} names:
    - auth_request_finished: Removed "mechanism" field in favor of already existing "mech" field.
    - auth_request_finished: Renamed "original_username" to "orig_user"
    - auth_request_finished: Renamed "translated_username" to "translated_user"
  - Renamed auth_client_request_continue event to auth_client_request_continued.

- **IMPROVEMENT DOV-3917**: Add consistency to service naming.
  - dns_client service renamed to dns-client
  - service:<name> category is now using the name from configuration file.
    - Most importantly this means that auth-worker process now uses "service:auth-worker" instead of "service:auth".
  - Log prefixes now use the service name from configuration file. For example, dict-async service will now use "dict-async(pid): " log prefix instead of "dict(pid): "

- **IMPROVEMENT DOV-3921**: Login processes log now via events.
  - Changed logging done by proxying to use a consistent prefix containing the IP address and port.
  - Changed disconnection log messages to be slightly clearer.

- **IMPROVEMENT DOV-3931**: Add OpenMetrics exporter for statistics. All metrics and sub-metrics are automatically exported. For information how to use this feature, see documentation at https://doc.dovecot.org/configuration_manual/stats/openmetrics/

- **ISSUE DOV-3740**: The mail_delivery_finished event has no "error" field that allows determining whether the delivery was successful.

- **ISSUE DOV-3751**: Writing to >=1 GB dovecot.index.cache files may cause assert-crashes: Panic: file mail-index-util.c: line 37 (mail_index_uint32_to_offset): assertion failed: (offset < 0x40000000).

- **ISSUE DOV-3755**: v2.3 regression: lmtp process title wasn't showing recipient username at DATA stage.

- **ISSUE DOV-3778**: Fix buggy OpenSSL error handling without assert-crashing. If there is no error available, log it as an error instead of crashing: Panic: file iostream-openssl.c: line 599 (openssl_iostream_handle_error): assertion failed: (errno != 0).

- **ISSUE DOV-3779**: v2.3.7 regression: If DNS lookup times out, lib-dns can cause crash in calling process.

- **ISSUE DOV-3780**: v2.3.4 regression: dict process title no longer shows decimals for the "average" value.

- **ISSUE DOV-3784**: auth: If a username gets changed and auth cache is in use, auth-workers did not update the username in cache.

- **ISSUE DOV-3785**: imap_command_finished event's cmd_name field now contains "unknown" for unknown commands. A new "cmd_input_name" field contains the command name exactly as it was sent.

- **ISSUE DOV-3796**: When specifying multiple scopes in oauth2 config file, it would become impossible to match the response value. After the fix, it is possible to match against multiple possible scopes, like RFC6749 demands.

- **ISSUE DOV-3797**: Minor performance optimization: Multiple processes could have recreated dovecot.index at the same time, instead of only one process recreating it and other processes reopening it. This was unlikely to happen outside stress testing.

- **ISSUE DOV-3808**: Auth process crash when auth_policy_server_url is set to an invalid URL.

- **ISSUE DOV-3815**: Auth-worker process keeps slowly increasing its memory usage and eventually dies with "out of memory" due to reaching vsz_limit.

- **ISSUE DOV-3816**: Fixed various bugs with IMAP SEARCHRES:
    - SEARCH $ or SEARCH UID $ didn't return any results
    - SEARCH returning BAD tagged reply shouldn't clear $ results
    - $ wasn't cleared when changing folders
    - Using $ in the SEARCH RETURN (SAVE) query itself always expanded to empty set
    - PARTIAL should have included only the partial results in $ instead of everything

- **ISSUE DOV-3816**: Using SEARCH RELEVANCY option with MIN/MAX/PARTIAL did not work correctly. All the relevancies were returned instead of only the returned MIN/MAX/PARTIAL relevancies.

- **ISSUE DOV-3822**: Fixed several bugs in dovecot.index.cache handling that could have caused cached data to be lost. There is still one known situation (expected to be rare) when it can lose data, but now it logs a warning if that happens.

- **ISSUE DOV-3830**: dict-ldap crashes if %variable expansion fails.

- **ISSUE DOV-3832**: Using an unknown CHARSET parameter with IMAP SEARCH returned BAD tagged response instead of NO, as required by the IMAP RFC.

- **ISSUE DOV-3833**: smtp_server_command_started/finished event's cmd_name field now contains "unknown" for unknown commands. A new "cmd_input_name" field contains the command name exactly as it was sent.

- **ISSUE DOV-3835**: lib-smtp did not try all the IP addresses returned by DNS lookup when connection failed. This affected for example connecting to submission_host.

- **ISSUE DOV-3836**: Reading a mail could have resulted in an infinite loop in some broken configurations, e.g. reading encrypted or compressed mail without the crypt/compress plugin enabled.

- **ISSUE DOV-3836**: auth: Several auth-mechanisms allowed input to be truncated by NUL which can lead to unintentional issues or even successful logins which should have failed.
    - This was mainly a problem if webmail (or other authentication proxy) forwards NULs in a master user authenticated login username using SASL PLAIN mechanism, which results in invalid PLAIN input that should have been rejected. Instead, this could have resulted in being able to overwrite the login or master username that was provided by the webmail/proxy and possibly login as another user or bypass IP address-based restrictions (allow_nets). However, the authentication still could not have succeeded without knowing the master's password.
    - For example: Webmail normally uses "login-user\0master-user\0master-password" as the PLAIN authentication string. Attacker sends "different-user\0master-user\0master-password" as the

webmail login username. This results in the webmail sending "different-user\0master-user\0master-password\0master-user\0master-password" to Dovecot as the PLAIN authentication string. The user is now logged in as "different-user" without knowing its password. However, the attacker must have a valid master-password for this attack to succeed. It also requires that the webmail forwards the NULs, which is also a bug. If the attacker knows the master-password, they may be able to do the same attack via regular IMAP authentication. However, many installations restrict master user logins only from internal IP addresses, like the webmail IPs. The allow_nets would normally prevent this attack, but not when doing it via webmail.

- **ISSUE DOV-3849**: Prevent potential timing attacks in authentication secret comparisons: OAUTH2 JWT-token HMAC, imap-urlauth token, crypt() result.

- **ISSUE DOV-3855**: Using modifiers with unknown %variables (e.g. %2M{asdf}) should return "UNKNOWN_VARIABLE_*" string rather than returning the string through the modifiers (e.g. 00..ff).

- **ISSUE DOV-3856**: Using a single letter %x variable should return "UNKNOWN_VARIABLE_x" string instead of an empty string.

- **ISSUE DOV-3861**: submission: A segfault crash may occur when the client or server disconnects while a non-transaction command like NOOP or VRFY is still being processed. This is normally difficult to reproduce, but the same problem occurs readily when submission_backend_capabilities setting is configured (mainly for VRFY) and the relay server is unavailable completely.

- **ISSUE DOV-3879**: Flags in gz compressed files' headers weren't parsed correctly. This could have resulted in out-of-bounds reads, which could potentially have caused crashes. However, untrusted gz input isn't normally read anywhere. Only using IMAP COMPRESS extension the client could use gz compression and potentially crash the user's own IMAP session.

- **ISSUE DOV-3881**: Using passdb delay_until extra field caused a crash when used with auth policy and auth_policy_check_after_auth=no: Panic: file auth-request.c: line 292 (auth_request_success_continue): assertion failed: (request->state == AUTH_REQUEST_STATE_MECH_CONTINUE).

- **ISSUE DOV-3887**: v2.3 regression: ssl_key_password setting did not work.

- **ISSUE DOV-3891**: dovecot.index.cache caching decisions sometimes changed too early from "cache field for all mails" to "cache field only for the last 1 week's mails". This happened when the cache file was recreated (purged) twice without the IMAP client fetching those fields between the recreates. This could have happened for example if a lot of mails were expunged just after the previous recreate. This didn't affect the fields listed by mail_always_cache_fields setting, which has been recommended as a workaround. The new behavior is to preserve the caching decision always for at least 30 days. See https://doc.dovecot.org/configuration_manual/mail_cache_settings/ for details.

- **ISSUE DOV-3918**: Running doveadm commands via proxying may hang, especially when doveadm is printing a lot of output.

- **ISSUE DOV-3929**: lmtp, submission: smtp_server_* events didn't have "protocol" field even though it was documented.

- **ISSUE DOV-3942**: When auth policy returned a delay, auth_request_finished event had policy_result=ok field instead of policy_result=delayed.

- **ISSUE DOV-3965**: Dovecot's NTLM implementation does not correctly check message buffer size, which leads to reading past allocation which can lead to crash. (CVE-2020-12673) (Not supported in OX Dovecot Pro)

- **ISSUE DOV-3966**: Dovecot's RPA mechanism implementation accepts zero-length message, which leads to assert-crash later on. (CVE-2020-12674) (Not supported in OX Dovecot Pro)

- **ISSUE DOV-3978**: If dict client disconnected while iteration was still running, dict process could have started using 100% CPU, although it was still handling clients.

- **ISSUE DOV-3985**: v2.3.10 regression: Running "UID MOVE 1:* Trash" on an empty folder goes to infinite loop.

- **ISSUE DOV-3990**: v2.3.10 regression: "MOVE * destfolder" goes to a loop copying the last mail to the destination until the imap process dies due to running out of memory.

- **ISSUE DOV-4014**: v2.3.10 regression: Copying/moving mails with IMAP into a virtual folder assert-crashes: Panic: file cmd-copy.c: line 152 (fetch_and_copy): assertion failed: (copy_ctx->copy_count == seq_range_count(&copy_ctx->saved_uids)).

5.2. Object Storage (obox) Plug-in

- **IMPROVEMENT DOV-3586**: Added new events for obox and metacache - see https://doc.dovecot.org/admin_manual/list_of_events/ for additional details.
  - metacache_user_refresh_started
  - metacache_user_refresh_finished
  - metacache_mailbox_refresh_started
  - metacache_mailbox_refresh_finished
  - metacache_upload_started
  - metacache_upload_finished
  - metacache_user_bundle_upload_started
  - metacache_user_bundle_upload_finished
  - metacache_mailbox_bundle_upload_started
  - metacache_mailbox_bundle_upload_finished
  - metacache_user_bundle_download_started
  - metacache_user_bundle_download_finished
  - metacache_mailbox_bundle_download_started
  - metacache_mailbox_bundle_download_finished
  - obox_mailbox_rescan_started
  - obox_mailbox_rescan_finished
  - obox_mailbox_rebuild_started
  - obox_mailbox_rebuild_finished

- **ISSUE DOV-3730**: Fix a crash that could occur when using fs-compress or fs-mail-crypt without fscache while also having configured mail_prefetch_count >= 9: Panic: BUG: No IOs or timeouts set. Not waiting for infinity.

- **ISSUE DOV-3801**: Root index bundles in metacache were flushed unnecessarily often. When flushing >0 priority indexes the root bundle should not be uploaded.

- **ISSUE DOV-3817**: obox_size_missing_action=warn_read (default) or "read" did not properly calculate the message size. This caused errors when reading some very old broken mails.

- **ISSUE DOV-3916**: fs-auth service logged an error if ssl=yes but ssl_cert was not set globally, even though it didn't use it for anything.

- **ISSUE DOV-3938**: v2.3.10 regression: fs-dictmap (obox/Cassandra): It was possible that max-parallel-iter limit was exceeded when there were iteration errors.

- **ISSUE DOV-3949**: fs-dictmap (obox/Cassandra): Under high load iterations could cause a Panic: file dict.c: line 323 (dict_iterate_init_multiple): assertion failed: (paths[0] != NULL).

- **ISSUE DOV-3950**: buckets.cache became corrupted when there was a folder with a huge number of buckets. This also caused the cache to become excessively large and log a huge number of errors about buckets.cache corruption.

- **ISSUE DOV-3955**: v2.3.9 regression: fs-dictmap/Cassandra: Number of email buckets in a folder could have kept increasing up to thousands in some situations when Cassandra had problems iterating mails in buckets. If >=50% of existing buckets' sizes are unknown in buckets.cache, try to refresh them first, and if they still can't be iterated, fail saving the mail.

- **ISSUE DOV-3956**: v2.3.10 regression: fs-dictmap/Cassandra: pop3 session could have assert-crashed at QUIT if lazy_expunge was used, only some of the messages were DELEted and index was missing Scality object IDs for some of the messages.

- **ISSUE DOV-3956**: v2.3.10 regression: fs-dictmap/Cassandra: pop3 with lazy_expunge_only_last_instance=yes was doing unnecessary refcount lookups at QUIT for mails that weren't deleted. This was mainly visible as unnecessary Cassandra lookups with fs-dictmap.

- **ISSUE DOV-3993**: fs-s3/fs-aws-s3: When using IAM for authentication, request retries after key-rotation could fail because of not matching signatures.

- **ISSUE DOV-4003**: Bulk deletion does not work with S3 if the URL contains a non-empty prefix (i.e. http://s3.example.com/prefix/). This mainly happened in the fts_dovecot_fs setting and caused FTS objects not to be deleted. For now bulk deletion is automatically disabled in this case - a proper fix will be in v2.3.12.

5.3. Full Text Search (fts) Plug-in

No Changes

5.4. Pigeonhole (sieve) Plug-in

- **IMPROVEMENT DOV-3862**: managesieve_max_line_length setting is now a "size" type instead of just number of bytes. This allows using e.g. "64k" as the value.

- **ISSUE DOV-3884**: Zimbra compatibility plugin: Invalid UTF-8 in email address when doing addressbook lookup crashes: Panic: file smtp-address.c: line 684 (smtp_address_write): assertion failed: (smtp_char_is_qpair(*p)).

- **ISSUE DOV-3906**: When folding white space is used in the Message-ID header, it is not stripped away correctly before the message ID value is used, causing e.g. garbled log lines at delivery.

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

No Changes

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

- **IMPROVEMENT DOV-3762**: webpush: Allow specifying a list of From: addresses to *not* be notified if any match the message's from address. The list can be set via an optional "exclude_from" : ["address1", "address2", ...] field in the subscription.

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/.