Release Notes for Dovecot Pro Major release 2.3.1

1. Shipped Products and Versions

Dovecot Pro 2.3.1
Including Object Storage Plug-in, Full Text Search Plug-in, Pigeonhole Sieve Plug-in and Dovemon

1.1. Dovecot Pro Core

- **BUG DOV-1933: SECURITY BUG** (CVE-2017-15130): TLS SNI config lookups are inefficient and can be used for DoS. If Dovecot has been configured with local_name {...} or local {...} configuration blocks, SNI lookups can be used to fill up memory with useless config by using random servernames. This eventually reaches the imap-login/pop3-login process's VSZ limit and restarts the process.

- **BUG DOV-1702: SECURITY BUG** (CVE-2017-14461): Parsing invalid email addresses may cause a crash or leak memory contents to attacker. For example, these memory contents might contain parts of an email from another user if the same imap process is reused for multiple users. First discovered by Aleksandar Nikolic of Cisco Talos. Independently also discovered by "flxflndy" via HackerOne.
    - **FIX:** lib-mail: Fix out-of-bounds read when parsing an invalid email address
    - **FIX:** lib-mail: Make sure parsers don't accidentally go much beyond end pointer

- **BUG DOV-1695: SEURITY BUG** (CVE-2017-15132): Aborted SASL authentication leaks memory in login process
    - **FIX:** lib-auth: Fix memory leak in auth_client_request_abort()

- **BUG DOV-1471: SECURITY BUG**: Using PR_SET_DUMPABLE can bypass chroot/group restrictions
    - **FIX:** lib: Call prctl(PR_SET_DUMPABLE) only when PR_SET_DUMPABLE env variable is set
    - Dovecot enabled PR_SET_DUMPABLE for most of the processes to allow them to create core dumps. However, processes that have this enabled also allow them to ptrace() each others, as long as they're using the same UNIX UID. This can be used by attackers to bypass other security features, such as processes using different GIDs or chrooting.
        - For example a local user could ptrace() their own imap process, which has mail_access_groups set to a GID that the user normally wouldn't have access to.
    - In Linux core dumps can be safely enabled nowadays by setting sysctl fs.suid_dumpable=2

    - If the old behaviour is wanted, it can still be enabled by setting: import_environment=$import_environment PR_SET_DUMPABLE=1
    - Found by cPanel Security Team

- **NEW FEATURE DOV-1851:** Attachment indicator

  Mark email attachment presence using $HasAttachment / $HasNoAttachment keywords
  Configuration options:

    - mail_attachment_detection_options Sets various attachment detection options. Currently supported
    - add-flags-on-save — Add flags when saving mail
    - content-type=type or !type — include/exclude content type, including content types also sets limitations to what kind of inlined attachments to consider as attachments. Including a content type will only negate an exclusion.
    - exclude-inlined — exclude any attachment with disposition inline

  Behaviour:

  If turned on, all emails without $HasAttachment/$HasNoAttachment keyword will be added one when saving them.

- **IMPROVEMENT DOV-22:** Added support for the SMTP submission protocol by means of a proxy service. It includes support for the SMTP BURL and CHUNKING extensions, even when the relay MTA for which it acts as a front-end has no support.

- **IMPROVEMENT DOV-23:** Rewrite LMTP/SMTP library. Add support for submission_ssl setting to support SSL/TLS for submission_host.

- **IMPROVEMENT DOV-1816:** submission: Make the connect and command reply timeouts for the connection to MTA relay server configurable.

- **IMPROVEMENT DOV-1285:** imap: Add support for fetching body snippets using FETCH (SNIPPET) or (SNIPPET (LAZY=FUZZY)).

- **IMPROVEMENT DOV-1718:** Include hostname in doveconf output.

- **IMPROVEMENT DOV-1867:** Auth cache can now utilize auth workers to do password hash verification.

- **IMPROVEMENT DOV-1894:** Don't let users login when metacache disk space is too full.
    - Because the metacache disk space stays only approximately at metacache_max_space, this triggers only once the disk space is above metacache_max_space + metacache_max_grace. The default for grace is 1 GB, but that may be too small for some installations.
    - The logins are attempted a few times before they fail with: Metacache is out of disk space, not letting in any more users (... bytes used)

- **IMPROVEMENT DOV-25:** HTTP client connections can now be shared between different client instances. For example obox index bundle object GET and email object GET may be done with the same HTTP connection.

- **IMPROVEMENT DOV-41:** CHANGE: More secure default ssl settings

  ssl_cipher_list = ALL:!kRSA:!SRP:!kDHd:!DSS:!aNULL:!eNULL:!EXPORT:!DES:!3DES:!MD5:!PSK:!RC4:!ADH:!LOW@STRENGTH

ssl_options = no_compression is deprecated, as it's the default now. ssl_options = compression is now needed if you want compression enabled.

- **IMPROVEMENT DOV-106:** fts-parser API change + fts-tika should retry once if server gives 500 error
    - CHANGE: Retry once if fts-tika server gives 500 error
- **IMPROVEMENT DOV-122:** login processes: Rewrite SSL proxying to use lib-ssl-iostream instead of duplicating the same code in a different way.´
- **IMPROVEMENT DOV-1174:** IMPROVEMENT: imapc: Send ID command, including x-session-ext-id parameter, if imapc_features contains "send-id".
- **IMPROVEMENT DOV-1330:** auth: Avoid DNS lookup for "host" passdb extra field if "hostip" is specified
- **IMPROVEMENT DOV-1383:** Changed the default mail_log_prefix setting to include PID and session ID.
- **IMPROVEMENT DOV-1462:** Add support for ARGON2I and ARGON2ID password schemes (when available)
    - BLF-CRYPT is now available on all supported platforms
- **IMPROVEMENT DOV-1563:** Explicitly ask XML format from Solr server. This is required to work with Solr v7.0 default configuration.
- **IMPROVEMENT DOV-1569:** auth: Remove userdb nss. There's no benefit anymore to using it over userdb passwd.
- **IMPROVEMENT DOV-1611:** login-proxy: Log connection errors using IP, not hostname
- **IMPROVEMENT DOV-55:** IPv6 support is no longer optional, but a requirement to build Dovecot
- **IMPROVEMENT DOV-57:** CHANGE: Log headers as utf8 in mail_log plugin
- **IMPROVEMENT DOV-58:** CHANGE: doveadm table formatter: print to stdout instead of stderr
- **IMPROVEMENT DOV-60:** CHANGE: Remove forced duplicate session ID logging on mail delivery.
- **IMPROVEMENT DOV-61:** CHANGE: auth: Make logging of ldap unknown user and password mismatch with different auth_bind values uniform.
- **IMPROVEMENT DOV-65:** CHANGE: IMAP FETCH BINARY - Return [PARSE] instead of [UNKNOWN-CTE] for mails with invalid MIME parts
- **IMPROVEMENT DOV-115:** CHANGE: fs-posix: prefix=path parameter no longer automatically appends '/' to the path if it's not there. This allows using it properly as a prefix, instead of only a directory prefix. Make sure you have the '/' appended to the prefix, or the "dir/filename" will be accessed just as "dirnamename".
- **IMPROVEMENT DOV-1648:** CHANGE: Provide more secure defaults for password generation. Use blowfish in CRYPT by default.

- **IMPROVEMENT DOV-1842:** Added imapc_features=no-msn-updates
  - This is a stricter version of fetch-msn-workarounds. The MSNs aren't trusted at all. This means any new untagged EXISTS and EXPUNGE replies are ignored, as well as untagged FETCH replies that don't include UID.
  - A potential downside with this feature is that UID FETCH/STORE commands sent to expunged messages will likely fail without the IMAP client being notified of the EXPUNGEs. New mails are also not noticed, so this should be used only when it's known that the clients don't keep the connection open for long.

- **IMPROVEMENT DOV-1848:** CHANGE: "ipc" socket's owner was changed to $default_internal_user
  - This is mainly used by director process, which runs as $default_internal_user. This setting change was always required for director installations.

- **IMPROVEMENT DOV-42:** ssl DH parameters are no longer automatically generated, but require ssl_dh setting with admin generated parameters.

- **IMPROVEMENT DOV-1136:** doveadm service status shows doveadm_stop field to indicate whether service is stopped or not.

- **IMPROVEMENT DOV-1168**: Improve auth process efficiency when using non-hashed password.

- **IMPROVEMENT DOV-1194:** Add new environment variable CORE_IO_LEAK. When turned on, dovecot will panic when IO or timeout leak occurs. For debug use only.

- **IMPROVEMENT DOV-1319:** Do not log password mismatch twice when using auth cache.

- **IMPROVEMENT DOV-1323:** Log early startup warnings

- **IMPROVEMENT DOV-1373:** Require unique listindex name for all namespaces with different mailbox paths

- **IMPROVEMENT DOV-1378:** Indicate in process title if logging is blocked

- **IMPROVEMENT DOV-1288:** Add debug logging when quota is recalculated in dict quota

- **BUG DOV-1049/53037:** DSYNC fails with unmatched special characters
  - **FIX:** imapc: Don't disconnect on broken untagged IMAP replies. Try to skip over the line and continue. This may allow imapc to work around broken input sent by some IMAP servers.

- **BUG DOV-1204:** imapc: Reconnection may cause crashes and other errors.
  - Panic: file imapc-sync.c: line 373 (imapc_initial_sync_check): assertion failed: (mail_index_is_expunged(view, lseq) || seq_range_exists(&ctx->mbox->delayed_expunged_uids, luid))
  - Panic: Leaked view for index (in-memory index): Opened in imapc-mailbox.c:47
  - **FIX:** Mailbox state should be fetched immediately after a folder is SELECTed. This should happen before any other commands are re-sent that were waiting for an answer before reconnection

- **BUG DOV-1283:** imapc: Crash with mailbox_list_index=yes if index path is specified
  - **FIX:** Fix assert-crash on imapc with mailbox_list_index=yes if index path is specified

- **BUG DOV-1898/56430:** dovecot uses master username in before authentication policy lookup
  - **FIX:** auth: Use correct username in auth policy requests
  - **CHANGE:** Add auth_policy_check_before_auth, auth_policy_check_after_auth, and auth_policy_report_after_auth tunables to control which auth policy requests are enabled

- **BUG DOV-713/52399:** dict-cdb driver not compatible with new API
  - **FIX:** cdb driver has been fixed to compile against 2.3 dovecot

- **BUG DOV-831/49212:** ostream-zlib and ostream-encrypt don't verify whether the footer is successfully written
  - **FIX:** c Add o_stream_finish() call to ostream API
  - **FIX**: ostream-zlib, ostream-crypt: Write footer in o_stream_finish(). Require it to be called before stream is closed.

- **BUG DOV-843/53083:** quota_vsizes not handled correctly
  - **FIX:** Count with virtual sizes on both append and expunge with quota_vsizes=yes

- **BUG DOV-891:** OAuth2 token validation does not accept empty responses
  - **FIX:** lib-oauth2: Accept empty responses

- **BUG DOV-929:** SEARCH MIME may crash with: Panic: file index-mail-headers.c: line 296 (index_mail_parse_header): assertion failed: (part != NULL)
  - **FIX:** lib-storage: Fix assert-crash when searching header and MIMEPART

- **BUG DOV-1013/53350:** SEARCH MIME FILENAME is case-sensitive
  - **FIX:** Made MIME FILENAME search criterion match case-insensitively.

- **BUG DOV-1021/52325:** "Password mismatch" casing inconsistent
  - **FIX:** Use consistent log message

- **BUG DOV-1197:** replicator: dsync triggers an unnecessary replication when UIDs are renumbered. The remote side should have done the same renumbering without the extra replication.
  - **FIX:** dsync: Add missing transaction flags when performing UID renumbering

- **BUG DOV-1320:** auth: Fix original_username rename
  - **FIX:** Fix using %{orig_username} in auth-worker var-expand.

- **BUG DOV-1549:** quota-fs: mount= parameter doesn't work
  - **FIX:** Fix mount= parameter parsing in quota-fs

- **BUG DOV-1551:** quota: doveadm quota get exit value is 0 even on internal error
  - **FIX:** Return EX_TEMPFAIL on doveadm quota get error

- **BUG DOV-1608:** mdbox rebuild repeatedly fails with: Error: mdbox map .../dovecot.map.index corrupted: missing map extension
  - **FIX:** mdbox: Fix rebuilding when dovecot.map.index is missing map/ref extension

- **BUG DOV-1625: r**eplicator process crashes if "doveadm replicator remove" is run while user is dsynced
  - **FIX:** replicator: Keep user referenced while dsync is running

- **BUG DOV-1627:** LMTP proxy doesn't share any backend connections for RCPT TOs when passdb returns "hostip"

    - **FIX:** lmtp: proxy: Fix connection settings comparison in lmtp_proxy_get_connection() when hostip field is set.

- **BUG DOV-1700:** Lua auth cannot see password field in table response
    - **FIX:** Lua auth cannot see password field in table response

- **BUG DOV-1708:** SMTP client: When rawlog is enabled, the TLS handshake sometimes fails.
    - **FIX:** Properly update rawlog streams after the TLS handshake.

- **BUG DOV-1719:** dsync replication duplicates mails if there are multiple dsync processes running concurrently.
    - This was especially problematic when using dsync-replication in public namespaces, because there was no locking.
    - **FIX:** dsync: Add per-mailbox sync lock that is always used

- **BUG DOV-1727:** auth: SASL with Exim fails for AUTH commands without an initial response
    - **FIX:** auth: SASL with Exim fails for AUTH commands without an initial response

- **BUG DOV-1728:** Dovecot html2text conversion does not validate UCS4 code points in HTML text, causing assert-crash when converting to UTF-8.
    - **FIX:** Check and discard any invalid code points.

- **BUG DOV-1739:** IMAP capabilities haven't automatically contained SPECIAL-USE since v2.2.30.
    - **FIX:** imap: Iterate over ns settings when deciding to add SPECIAL-USE capability

- **BUG DOV-1754:** lmtp: Segfault when user is over quota
    - **FIX:** lmtp: local: Fix segfault occurring when quota is exceeded.

- **BUG DOV-1796:** mail_always/never_cache_fields changes weren't applied for existing dovecot.index.cache files
    - **FIX:** lib-index: Fix adding forced cache decisions to existing cache files
        - f a field already existed in the cache file, the cache decision from the file was always used. This caused force-decisions to be ignored.
    - **FIX:** lib-index: Fix removal of forced cache decisions from existing cache files
        - The forced-flags are written to the cache file when the file is created. They were also read back, and the force-flag was preserved even when the configuration was removed.
    - **FIX:** lib-index: Write forced cache decision changes immediately to cache file
        - When mail_always/never_cache_fields doesn't match the current caching decisions in the cache file, write the updated decisions to the file.

- **BUG DOV-1805:** program-client sometimes truncated output. This was visible with e.g. Sieve extprograms plugin sometimes truncated output from external programs. This applies to the "vnd.dovecot.filter" and "vnd.dovecot.execute" Sieve extensions. Applies to both forked programs and programs invoked through the script socket service.
    - **FIX:** Fix bugs in program-client I/O stream handling.

- **BUG DOV-1807:** .vsize.lock filename conflicts with "vsize/lock" folder name with Maildir. It may also show up in the list of folders (e.g. with NFS).
    - **FIX:** lib-storage: Rename .vsize.lock file to dovecot-vsize.lock

- **BUG DOV-1822:** lib-lda: Parsing Return-Path header address fails when it contains CFWS
  - **FIX:** lib-lda: Parse Return-Path header using RFC5322 (IMF) "path" syntax, rather than RFC5321 (SMTP) "Path" syntax.

- **BUG DOV-1865:** fs-posix: Directory iteration is broken on NFS with nordirplus mount option
  - **FIX:** fs-posix: Fix iterating directories when readdir() returns DT_UNKNOWN

- **BUG DOV-1893:** SSL connections may have been hanging with imapc or doveadm client .
  - **FIX:** lib-imap-client: Fix IO after enabling SSL
  - **FIX:** doveadm: client: Set IO only after enabling SSL

- **BUG DOV-1895:** Too many parallel metacache requests cause HTTP timeouts
  - **FIX:** Throttle parallel metacache requests and add meta-cache_max_parallel_requests to tune it

- **BUG DOV-1920:** connection.c attempts to switch iostreams to ioloop on connection, but the streams are not always created.
  - **FIX:** Only move iostreams that are created the connection ioloop.

- **BUG DOV-1942:** LMTP proxy crashes if remote endpoint shuts down after RCPT TO
  - **FIX:** lib-smtp: client: transaction: Don't call the DATA callbacks upon failure until the transaction is complete.

- **BUG DOV-1979:** UTF-8 code points in From header can cause an assert-crash
  - **FIX:** lib-lda: Do not convert "From:" message address to STMP address, just to make a string for logging.

- **BUG DOV-1994:** lmtp ORCPT parameter support in RCPT TO was missing in 2.3.0
  - **FIX:** lmtp: Provide hidden support for ORCPT RCPT parameter.

- **BUG DOV-2022:** sdbox: Temporary files aren't deleted if COPY fails due to user being over quota
  - **FIX:** sdbox: Delete .temp* files on when save/copy transaction is rolled back

- **BUG DOV-2026:** When reading encrypted data, more data would not be read if buffer was consumed causing panic.
  - **FIX:** Decrypt more data when buffer becomes empty.

- **BUG DOV-2040:** Multiple space-separated local_names were treated as one
  - **FIX:** Properly handle space-separated local_names in config parser

- **BUG DOV-2047:** imapc: If email is modified, cached mail size isn't updated
  - **FIX:** Recalculate mail size even if istream_opened() hook is called.
  - **FIX:** imapc: Update mail size also when RFC822.SIZE is smaller than fetched header size

- **BUG DOV-1959:** dsync overrides BROKENCHAR, which prevents migrating invalid mUTF-7 mailbox names.
  - **FIX:** doveadm sync/backup: Don't override BROKENCHAR if it's already set

1.2. Object Storage Plug-in

- **IMPROVEMENT DOV-856:** obox: metacache_delay_uploads=yes should be default and remove config knob
  - CHANGE: Removed metacache_delay_uploads setting. It's now always enabled.

- **IMPROVEMENT DOV-1382:** Remove _msecs suffix from timeout parameters in a backwards compatible way.

- **IMPROVEMENT DOV-1636:** obox: If mailbox list index is empty on login, try to rebuild the list

- **BUG DOV-1866:** Dovecot might choose wrong object-store endpoint in swift if region is used.
  - **FIX:** Consider region and interface together when choosing object-store endpoint

- **BUG DOV-1876:** fs-s3: Failed multi-request iteration accesses freed memory
  - **FIX:** fs-s3: Make sure iteration doesn't double-free XML parser

1.3. Full Text Search Plug-in

- **BUG DOV-1862:** fts_dovecot was logging debug lines that couldn't be disabled: "Debug: FTS: bubble merge"
  - **FIX:** lib-fts-index: Make debug-logging bubble merges optional.

- **BUG DOV-1864/54383:** FTS reindexes mails unnecessarily after loss of .cache file
  - **FIX:** fts: Don't reindex FTS mails if .cache file is deleted

- **BUG DOV-1958/56066:** fs-fts-cache: Stale cache.log may cause errors: fts_dovecot: Index keeps changing under us too rapidly
  - **FIX:** plugin: Refresh fs-fts-cache if FTS_INDEX_READ_ERROR_RETRY is returned

- **BUG DOV-2023:** fs-fts-cache leaks memory whenever trying to access FTS objects that don't exist in cache.
  - **FIX:** fs-fts-cache: Fix memory leak when reading fts object that doesn't exist in cache

- **BUG DOV-2044:** fs-fts-cache: cache.log could become corrupt when there were more than 32 files
  - **FIX:** fs-fts-cache: Fix corruption in cache.log when there are more than 32 files

1.4. Pigeonhole Sieve Plug-in

- **BUG DOV-1671:** dovecot-lda always substituted a default envelope sender when -f was omitted or "<>".
  - **FIX:** Remove the substitution, so that the NULL sender is properly used.

- **BUG DOV-1922:** Pigeonhole/Sieve: Large output from Sieve exprograms "execute" command crashed LMTP.
  - **FIX:** Resolved buffering issue in code that handles output from external program.

- **BUG DOV-2041:** Pigeonhole Sieve crashes in LMTP with an assertion panic when the Sieve editheader extension is used before the message is redirected. Experiments indicate that the problem occurs only with LMTP and that LDA is not affected.
    - **FIX:** Corrected the stream position calculations performed while making the modified message available as a stream.

1.5. Dovemon

- **BUG DOV-1508:** Dovemon: settings not set in configuration file are lost
    - **FIX:** update modified settings according to config file and use default values for settings not present in config file.
    - **IMPROVEMENT:** Dovemon: Use an in-memory logger at startup and flush messages to syslog after initialization is complete to prevent pre-initialization logs from being lost.
    - **IMPROVEMENT:** Dovemon: use pyyaml's safe_load when reading configuration file to improve security.
    - **IMPROVEMENT:** Dovemon: log current configuration options being used upon receiving SIGUSR1.

1.6. Tests

The Dovecot QA team has successfully verified all bug 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.