something old, something new, something borrowed, something blue: switching over to Dovecot 2.0

Charite Universitätsmedin Berlin

Open Source Days 2011 – Copenhagen, 05. March 2011

Why use LMTP?

- SMTP
  - all or nothing
  - successful delivery for all

Why use LMTP?

- SMTP
  - all or nothing
  - successful delivery for all
  - successful delivery for none
- LMTP
  - status per recipient

Why use LMTP?

- SMTP
  - all or nothing
  - successful delivery for all
  - successful delivery for none
- LMTP
  - status per recipient
  - successful delivery for some recipients

Why use LMTP?

- SMTP
  - all or nothing
  - successful delivery for all
  - successful delivery for none
- LMTP
  - status per recipient
  - successful delivery for some recipients

SMTP I

SMTP can only indicate successful delivery or failure for all or none of the recipients, creating the need for a separate queue to handle the failed recipients.

Example (SMTP)

```
---> MAIL FROM:<sender@example.com>
<--- 250 OK
---> RCPT TO:<recipient1@example.com>
<--- 250 OK
...
---> RCPT TO:<recipientn@example.com>
<--- 250 OK
---> DATA
<--- ok send some data
---> some text
---> .
<--- 200 OK
```

LMTP can indicate success or failure to the client for each recipient, allowing the client to handle the queueing instead.

Example (LMTP)

```
---> LHLO
<--- 250 OK
---> MAIL FROM:<address> size=messageSizeInBytes
<--- 250 OK
---> RCPT TO:<uid+folder@domain> xquota=size,number xdflg=xxx
<--- 250 OK
```

This interaction may be repeated many times, once for each recipient:

Example (DATA)

```
--->DATA
---> <the message text>
--->.
```

Possible reactions are (for each recipient):

Example (End-of-DATA responses)

```
<--- 500 message too big
```

Or:

Example

```
<--- 250 2.5.0 address OK
```

Advantages

- You can split MTA and MDA
- MDA (or rather the LMTP server) can run as a daemon

So all we need is an LMTP server. . .

Advantages

- You can split MTA and MDA
- MDA (or rather the LMTP server) can run as a daemon

So all we need is an LMTP server. . .

Enter: Dovecot I

Starting with v2.0, dovecot has an LMTP server!
In `/etc/dovecot/dovecot.conf` you say:

Example (Activating LMTP)

```
protocols = ... lmtp
```

Configuring the socket I

- LMTP uses the same settings as LDA
- The main difference is to LDA is that it starts as a binary from command line, while LMTP is another process started by Dovecot's master process.

Configuring the socket II

Example (Defining the socket)

```
service lmtp {
   unix_listener /var/spool/postfix/private/dovecot-lmtp {
      user = postfix
      group = postfix
      mode = 0660
   }
   inet_listener lmtp {
      address = 192.168.0.24 127.0.0.1 ::1
      port = 24
   }
}
```

Security I

Unfortunately LMTP process currently needs to run as root, and only temporarily drop privileges to users (or it couldn't handle mail deliveries to more than a single user with different UID). If you're using only a single global UID/GID, you can improve security by running lmtp processes as that user:

Example (Defining a uid)

```
service lmtp {
  user = vmail
}
```

Postfix config I

In Postfix you specify the corresponding socket:

Example (main.cf)

```
virtual_mailbox_domains = the.domain.com
# which domain
virtual_mailbox_maps = hash:/some/map
# which recipients,
# but you could also use reject_unverified_recipient!
virtual_transport = lmtp:unix:private/dovecot-lmtp
```

Sieve I

Pigeonhole Sieve and ManageSieve support can now be installed without patching Dovecot. But one still has to fetch and compile that source from the Pigeonhole site `http://pigeonhole.dovecot.org/download.html`

mdbox (multi-dbox) mail storage backend I

multi-dbox (`mdbox` in `mail_location`):
Multiple messages per file, but unlike `mbox` multiple files per mailbox.
(m)dbox has a feature for transparently moving message data to an alternate storage area!

Example I

```
mail_location = maildir:~/Maildir
mail_location = mdbox:~/mdbox
```

- Unlike Maildir, with dbox the message file names don’t change.
- This makes it possible to support storing files in multiple directories or mount points.

To enable this functionality, use the `ALT` parameter in the mail location. For example, specifying the mail location as:

```
mail_location = \
   mdbox:/var/vmail/%d/%n:ALT=/altstorage/vmail/%d/%n
```

- %u: Full username.
- %n: User part in `user@domain`, same as %u if there's no domain.
- %d: Domain part in `user@domain`, empty if there's no domain.

doveadm I

doveadm is a really nice tool that allows you to perform operations on some (or all) mailboxes:

- `reload`
  Force dovecot to reload the configuration
- `stop`
  Stop dovecot and all its child processes
- `search`
  Show a list of mailbox GUIDs and message UIDs matching given search query

```
% doveadm search -u dschnab mailbox INBOX subject "Dirk"
d90a12262d09ac4ced34000005ff2751 17472
d90a12262d09ac4ced34000005ff2751 18138
```

doveadm II

- `fetch`
  Fetch messages matching given search query

Example (fetch command)

```
% doveadm search -u dschnab mailbox INBOX subject "Dirk" |
while read guid uid; do
   doveadm fetch -u dschnab \
   body mailbox-guid $guid uid $uid > msg.$uid
done
```

Search queries are very flexible:

Example (search syntax)

doveadm III

```
% doveadm search ALL
% doveadm search NEW LARGER 50k
% doveadm search SAVEDON 2007-04-13 \( SEEN OR FLAGGED \)
% doveadm search mailbox Trash DELETED
```

- who
  Show who is logged in to the Dovecot server

```
% doveadm who |head
username # proto (pids)                (ips)
schrjan  1 imap  (14043)               (2.208.142.104)
sitting  3 imap  (12459 12458 12643)   (93.206.53.136)
jdschind 1 imap  (7529)                (212.23.104.60)
...
```

- expunge
  Expunge messages matching given search query

doveadm IV

- `force-resync`
  Repair broken mailboxes, in case Dovecot doesn't automatically do that

```
% doveadm force-resync -u dschnab INBOX
```

- `quota`
  Initialize/recalculate or show current quota usage:

```
% doveadm quota get -u dschnab
Quota name Type      Value   Limit  %
           STORAGE 913525 2097152 43
           MESSAGE   3114       -  0
```

- `user`
  Perform a user lookup in Dovecot's userdbs:

doveadm V

```
% doveadm user dschnab
userdb: dschnab
  cache_key : dschnab
  system_groups_user: dschnab
  uid       : 2162
  gid       : 100
  home      : /home/d/s/dschnab
```

User iteration

Example (Cleaning up after the users)

```
% doveadm expunge -A mailbox Trash savedbefore 30d
```

This can take a looong time.

User iteration

Example (Cleaning up after the users)

```
% doveadm expunge -A mailbox Trash savedbefore 30d
```

This can take a looong time.

User iteration using “-A” in LDAP

Some commands, such as `doveadm -A` need to get a list of users. With an LDAP userdb this is done with the `iterate_attrs` and `iterate_filter` settings.

Where's the beef?

A typical configuration:

Example

```
user_attrs  = homeDirectory=home, uidNumber=uid, gidNumber=gid
user_filter = (&(objectClass=posixAccount)(uid=%u))

# For using doveadm -A:
iterate_attrs = uid=user
iterate_filter = (objectClass=posixAccount)
```

User iteration in SQL

With an SQL userdb this is done with `iterate_query` setting. You can either return

- `user` field containing either `user` or `user@domain` style usernames, or
- `user` and `domain` fields

Any other fields are ignored.

Where’s the beef?

A typical configuration for mySQL:

Example

```
# The mysqld.sock socket may be in different locations in different systems
driver = mysql
# Use ''host=... pass=foo#bar'' if your password has a # character
connect = host=/var/run/mysqld/mysqld.sock dbname=mails user=admin password=pass
# Alternatively you can connect to localhost as well:
#connect = host=localhost dbname=mails user=admin password=pass

password_query = SELECT userid AS username, domain, password \
  FROM users WHERE userid = '%n' AND domain = '%d'
  user_query = SELECT home, uid, gid FROM users WHERE userid = '%n'
  AND domain = '%d'

# For using doveadm -A:
iterate_query = SELECT userid AS username, domain FROM users
```

Compression I

- The Zlib plugin can be used to **read** compressed mbox, maildir or dbox files.
- It can be also used to **write** (via IMAP, LDA and/or LMTP) compressed messages to dbox or Maildir mailboxes.
- Meaning you'll need to use maildir or dbox for both read and write access!
- zlib/gzip and bzlib/bzip2 are supported
- The compression is detected by reading the first few bytes from the file and figuring out if it's a valid gzip or bzip2 header

Compression II

Example (zlib config)

```
mail_plugins = $mail_plugins zlib

plugin {
  zlib_save_level = 6
  # 1..9
  zlib_save = gz
  # or bz2
}
```

dsync utility does a two-way mailbox synchronization I

dsync is Dovecot's mailbox synchronization utility. It can be used for several different use cases: Two-way synchronization of mailboxes in different servers (via ssh), creating backups of mails to a remote server, and convert mailboxes from/to different mailbox formats.

Emailaddress to Username Aliasing

Problem: I want compression, but that means I have to switch to dovecot for all services!

Example (config snippet)

```
# passwd-style File
passdb {
   args = username_format=%Ln /etc/dovecot/dovecot.aliases
   driver = passwd-file
   # Format should look like this:
   # firstname.lastname::::::user=realloginname
}
```

The actual conversion process

- I recompiled and installed dovecot with a different `prefix` setting
- I converted the old dovecot-1.2 config

```
% doveconf -n -c dovecot-1.conf > dovecot-2.conf
```

The actual conversion process

- I recompiled and installed dovecot with a different `prefix` setting
- I converted the old dovecot-1.2 config

```
% doveconf -n -c dovecot-1.conf > dovecot-2.conf
```

- It wouldn't work at all!

The actual conversion process

- I recompiled and installed dovecot with a different `prefix` setting
- I converted the old dovecot-1.2 config

```
% doveconf -n -c dovecot-1.conf > dovecot-2.conf
```

- It wouldn't work at all!
- The conversion would change the config, but not the filenames within the config, which were different due to the different `prefix` setting!

The actual conversion process

- I recompiled and installed dovecot with a different `prefix` setting
- I converted the old dovecot-1.2 config

```
% doveconf -n -c dovecot-1.conf > dovecot-2.conf
```

- It wouldn't work at all!
- The conversion would change the config, but not the filenames within the config, which were different due to the different `prefix` setting!

Recompiling Dovecot I

- use a “new” `prefix`
  because recompiling into the same paths will break some plugins and logging in!
- then rename paths
- Alternative: stop the old version, start new version
- explicitly specify the configuration file (otherwise `prefix` will bite you)

Quota warnings – are configured differently I

You can configure Dovecot to run an external command when user's quota exceeds a specified limit.
Note that the warning is **only** executed at the exact time the limit is being crossed!

Example (Quota)

```
plugin {
  quota = maildir
  quota_rule = INBOX.Trash:storage=+2048M
  quota_warning  = storage=99%% quota-warning 99 %u
  quota_warning2 = storage=95%% quota-warning 95 %u
  quota_warning3 = storage=90%% quota-warning 90 %u
  quota_warning4 = storage=85%% quota-warning 85 %u
}
```

Quota warnings – are configured differently II

Example (Quota Warning)

```
service quota-warning {
  executable = script /usr/local/scripts/quota-warning
  user = root
  unix_listener quota-warning {
    mode = 0666
    user = vmail
    group = users
  }
}
```

So the script `/usr/local/scripts/quota-warning` is executed as user root, but the socket that being used to communicate with it is owned by `vmail:users` and is mode 666.

The `quota-warning` script can be very simple:

Example

```
cat << EOF | dovecot-lda -d $MAIL_TO -o "plugin/quota=maildir::noenforcing"
Clean up your mailbox!
EOF
```

The quota enforcing is disabled to avoid looping! You'll of course need to change the `plugin/quota` value to match the quota backend and other configuration you use. Basically preserve your original `quota` setting and just insert `:noenforcing` to proper location in it.

The quota enforcing is disabled to avoid looping! You'll of course need to change the `plugin/quota` value to match the quota backend and other configuration you use. Basically preserve your original `quota` setting and just insert `:noenforcing` to proper location in it.

The CAPABILITY announcement changed

Pre-login and post-login CAPABILITY reply is now different.

Dovecot expects clients to recognize new automatically sent capabilities. This should work with all commonly used clients, but some rarely used clients might have problems. Either get the client fixed, or set `imap_capability` manually.

The CAPABILITY announcement changed

Pre-login and post-login CAPABILITY reply is now different. Dovecot expects clients to recognize new automatically sent capabilities. This should work with all commonly used clients, but some rarely used clients might have problems. Either get the client fixed, or set `imap_capability` manually.

Example

```
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR
      LOGIN-REFERRALS ID ENABLE IDLE STARTTLS
      AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
. LOGIN dschnab password
. OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR
      LOGIN-REFERRALS ID ENABLE IDLE SORT
      SORT=DISPLAY THREAD=REFERENCES
      THREAD=REFS MULTIAPPEND UNSELECT
      CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED
      I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH
      ESORT SEARCHRES WITHIN CONTEXT=SEARCH
      LIST-STATUS QUOTA] Logged in
. LOGOUT
```

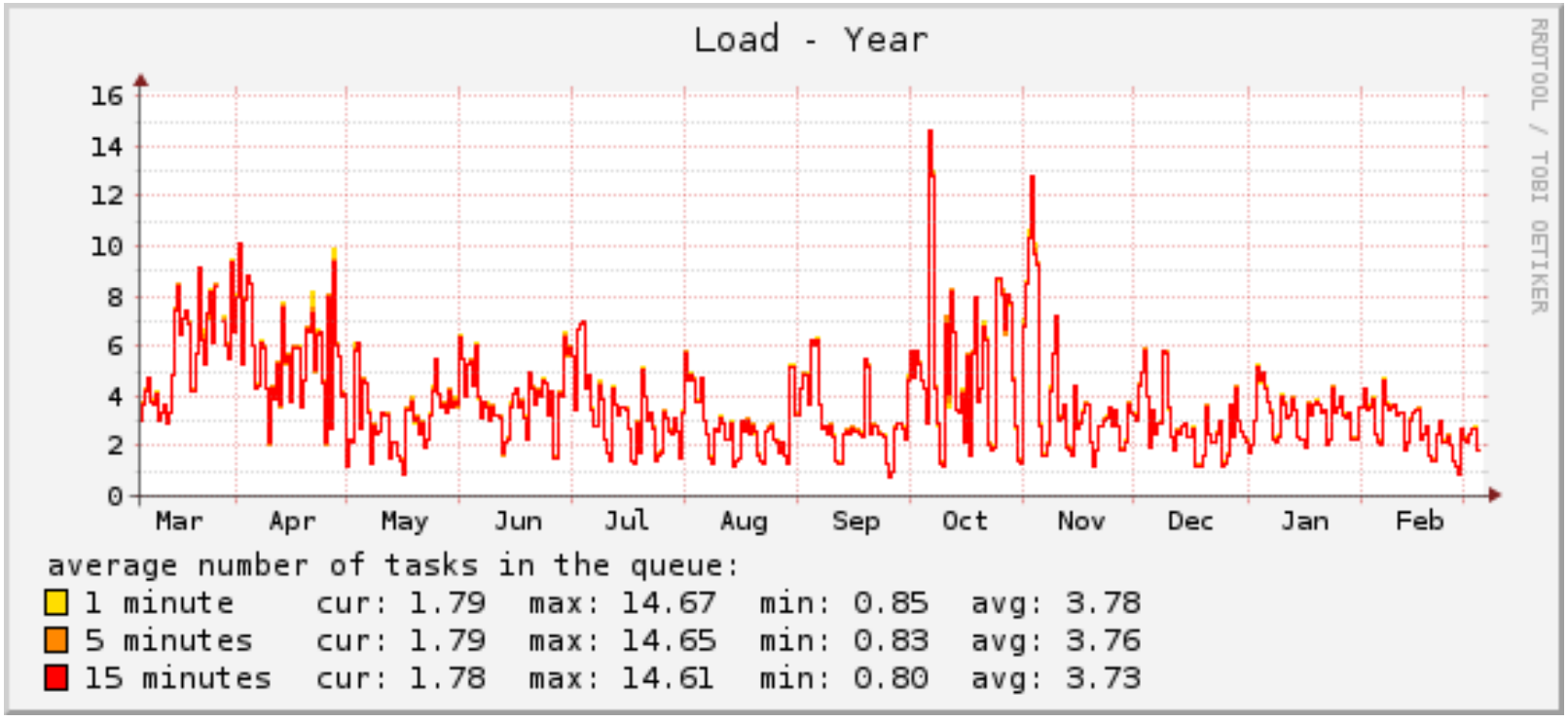
The CAPABILITY announcement changed

Pre-login and post-login CAPABILITY reply is now different. Dovecot expects clients to recognize new automatically sent capabilities. This should work with all commonly used clients, but some rarely used clients might have problems. Either get the client fixed, or set `imap_capability` manually.

Example

```
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR
      LOGIN-REFERRALS ID ENABLE IDLE STARTTLS
      AUTH=PLAIN AUTH=LOGIN] Dovecot ready.
. LOGIN dschnab password
. OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR
      LOGIN-REFERRALS ID ENABLE IDLE SORT
      SORT=DISPLAY THREAD=REFERENCES
      THREAD=REFS MULTIAPPEND UNSELECT
      CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED
      I18NLEVEL=1 CONDSTORE QRESYNC ESEARCH
      ESORT SEARCHRES WITHIN CONTEXT=SEARCH
      LIST-STATUS QUOTA] Logged in
. LOGOUT
```

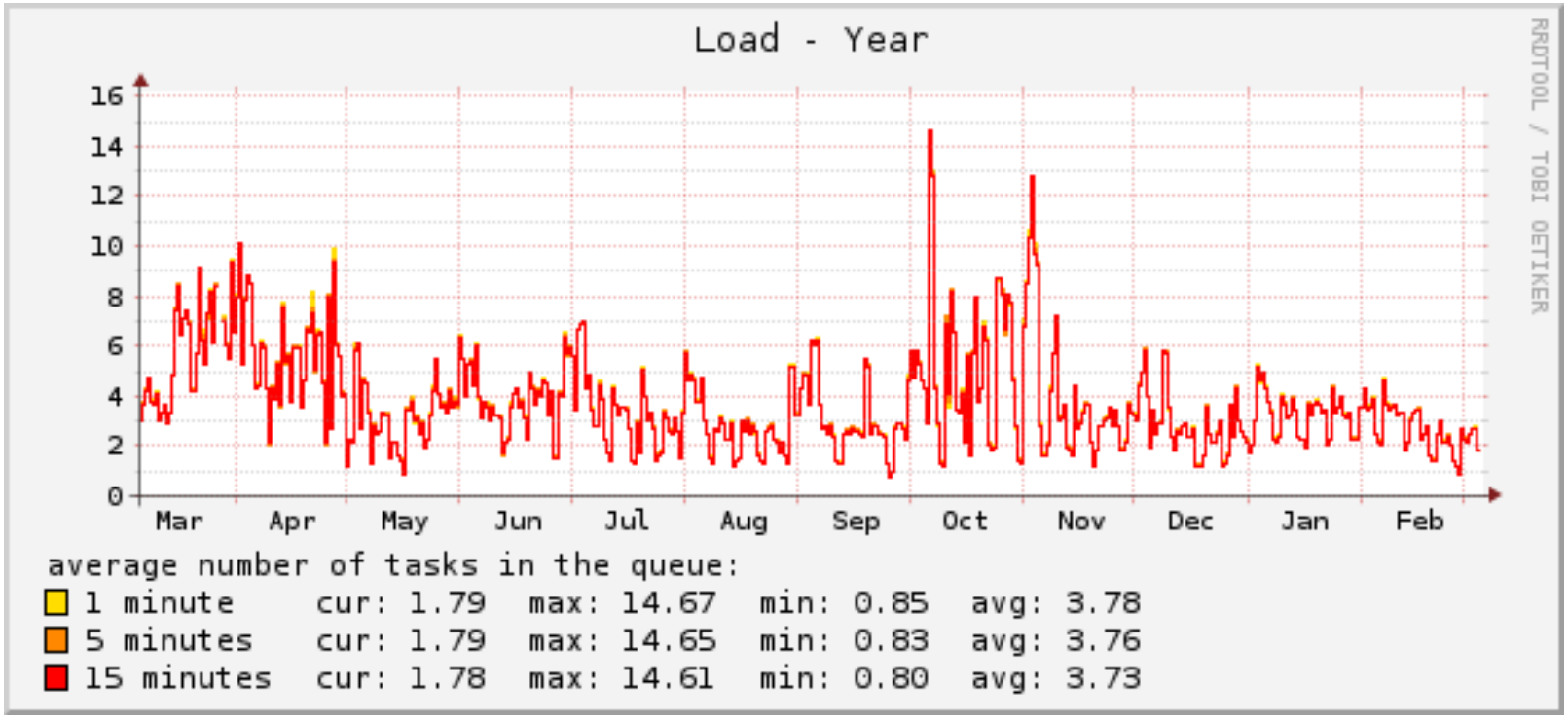
dovecot-2.0 didn’t scale



But that was fixed in 2.0.9:

- Linux: Fixed a high system CPU usage / high context switch count performance problem

dovecot-2.0 didn’t scale



But that was fixed in 2.0.9:

- Linux: Fixed a high system CPU usage / high context switch count performance problem

Masteruser I

Example

```
auth_master_user_separator = *
passdb {
  driver = passwd-file
  args = /etc/dovecot/passwd.masterusers
  master = yes
  pass = yes
}
passdb {
  driver = shadow
}
userdb {
  driver = passwd
}
```

Where the `passwd.masterusers` file would contain the master usernames and passwords:

Masteruser II

Example

```
admin:{SHA1}nU4eI71bcnBGqeO0t9tXvY1u5oQ=
admin2:{SHA1}i+UhJqb95FCnFio2UdWJu1HpV50=
```