Dovecot

Fix Me!

Свободный IMAP и POP3 сервер, разрабатываемый в расчёте на безопасность, гибкость настройки и быстродействие.

http://www.dovecot.org/

Установка

```
apt-get install\
    dovecot-core\
    dovecot-imapd\
    dovecot-lmtpd\
    dovecot-ldap\
    dovecot-sieve\
    dovecot-managesieved
```

Если нужен pop3 то нужно поставить еще pop3d:

```
apt-get install dovecot-pop3d
```

Настройка

Путь к файлам настройки: /etc/dovecot, /etc/dovecot/conf.d

Fix Me!

```
service dovecot
Usage: /etc/init.d/dovecot {start|stop|restart|force-reload|status}
```

dovecot.conf

/etc/dovecot/dovecot.conf

```
!include_try /usr/share/dovecot/protocols.d/*.protocol
!include conf.d/*.conf
!include_try local.conf

protocols = imap lmtp sieve
```

10-auth.conf

/etc/dovecot/conf.d/10-auth.conf

```
disable_plaintext_auth = no
auth_username_format = %Ln
auth_master_user_separator = *
auth_mechanisms = plain

!include auth-master.conf.ext
!include auth-ldap.conf.ext
```

10-logging.conf

/etc/dovecot/conf.d/10-logging.conf

```
auth_verbose = no
auth_verbose_passwords = no
auth_debug = no
auth_debug_passwords = no
mail_debug = no
verbose_ssl = no
```

20-imap.conf

/etc/dovecot/conf.d/20-imap.conf

```
protocol imap {
  mail_plugins = $mail_plugins imap_acl imap_quota quota
}
```

15-lda.conf

/etc/dovecot/conf.d/15-lda.conf

```
postmaster_address = postmaster@domain.local
hostname = mail.domain.local
protocol lda {
  mail_plugins = $mail_plugins sieve quota
  syslog_facility = mail
}
```

10-master.conf

/etc/dovecot/conf.d/10-master.conf

```
service imap-login {
  inet_listener imap {
    port = 143
  }
}

service lmtp {
    unix_listener /var/spool/postfix/private/dovecot-lmtp {
        group = postfix
        mode = 0666
        user = postfix
    }
}

service imap {
    executable = imap imap-postlogin
}
```

```
service imap-postlogin {
    executable = script-login -d /srv/mail/vmail/postlogin.sh
    user = $default_internal_user
    unix_listener imap-postlogin {
    }
}

service pop3 {
}

service auth {
    unix_listener auth-master {
        mode = 0666
    }

    unix_listener auth-userdb {
        mode = 0666
        user = vmail
        group = mail
    }

    unix_listener /var/spool/postfix/private/auth {
        mode = 0666
    }
}

service dict {
    unix_listener dict {
        mode = 0666
        user = vmail
        group = mail
    }
}
```

15-mailboxes.conf

/etc/dovecot/conf.d/15-mailboxes.conf

```
namespace inbox {
  mailbox Drafts {
    special_use = \Drafts
    auto = create
    auto = subscribe
  }
  mailbox Junk {
    special_use = \Junk
    auto = create
    auto = subscribe
  }
  mailbox Trash {
    special_use = \Trash
    auto = create
    auto = subscribe
  }

  mailbox Sent {
    special_use = \Sent
    auto = create
    auto = subscribe
  }
  mailbox "Sent Messages" {
```

```
    special_use = \Sent
  }

  mailbox Archive {
    special_use = \Archive
    auto = create
    auto = subscribe
  }

  mailbox virtual/Flagged {
    special_use = \Flagged
  }
}
```

Администрирование с doveadm

Fix Me!

Поиск

```
doveadm search -u ПОЛЬЗОВАТЕЛЬ savedbefore 30d
```

Информация о пользователе

```
doveadm user ПОЛЬЗОВАТЕЛЬ
```

Квоты	`doveadm quota get -u ПОЛЬЗОВАТЕЛЬ`
Чистка	`doveadm expunge -u ПОЛЬЗОВАТЕЛЬ mailbox ПАПКА savedbefore 30d`

Создание пароля

```
doveadm pw -s md5
```

Сознание папки для пользователей домена

Нужно создать пользователя `vmail` и создать папку для почты данного домена, затем нужно назначить папке соответствующие права.

dovecot_mail_location_create.sh

```
#!/bin/bash

MAIL_LOCATION=/srv/mail/vmail
useradd -g mail -u 5000 vmail -d $MAIL_LOCATION
gpasswd -a vmail mail
mkdir -p $MAIL_LOCATION
```

Значение переменной `MAIL_LOCATION` должно быть согласовано переменной `mail_location` в файле `/etc/dovecot/conf.d/10-mail.conf`:

/etc/dovecot/conf.d/10-mail.conf

```
mail_location = maildir:/srv/mail/vmail/%Ln
```

Установка прав на папки для пользователей домена

dovecot_mail_set_rihgts.sh

```
#!/bin/bash

MAIL_LOCATION=/srv/mail/vmail
chown vmail -R $MAIL_LOCATION
chgrp mail -R $MAIL_LOCATION
find $MAIL_LOCATION -type f -exec chmod 02600 {} \;
find $MAIL_LOCATION -type d -exec chmod 02700 {} \;
chmod 755 $MAIL_LOCATION/*.sh
```

Русские имена папок

Имена папок кодируются по спецификации UTF-7.

Вот соответствие распространенных имен:

Русское	В кодировке UTF-7	Английское
Отправленные	.&BB4EQgQ,BEAEMAQyBDsENQQ9BD0ESwQ1	.Sent
Корзина	.&BBoEPgRABDcEOAQ9BDA-	.Trash
Черновики	.&BCcENQRABD0EPgQyBDgEOgQ4-	.Drafts
СПАМ	.&BCEEHwQQBBw-	.Junk

Sieve

Язык Sieve нужен для фильтрации сообщений на стороне сервера.

После настройки необходимо выполнить действия по установке прав на папки для пользователей домена.

Установка

Для работы потребуются следующие пакеты:

```
apt-get install dovecot-sieve dovecot-managesieved
```

Настройка

1. Нужно добавить `sieve` в переменную `protocols` файла `dovecot.conf`

/etc/dovecot/dovecot.conf

```
protocols = imap lmtp sieve
```

20-lmtp.conf

Также добавляем `sieve` в следующие файлы:

/etc/dovecot/conf.d/20-lmtp.conf

```
protocol lmtp {
  mail_plugins = $mail_plugins sieve
}
```

15-lda.conf

/etc/dovecot/conf.d/15-lda.conf

```
protocol lda {
  mail_plugins = $mail_plugins sieve
}
```

90-sieve.conf

Указываем пути для размещения файлов в папке пользователя:

/etc/dovecot/conf.d/90-sieve.conf

```
plugin {
    sieve = /srv/mail/vmail/%Ln/.dovecot.sieve
    sieve_dir = /srv/mail/vmail/%Ln/sieve
    sieve_before = /srv/mail/vmail/before.sieve
}
```

before.sieve

/srv/mail/vmail/before.sieve

```
require ["fileinto"];
# rule:[SPAM]
if anyof (header :contains "X-Amavis-Alert" "BAD HEADER SECTION", header :contains "X-
Spam-Level" "*", header :contains "Subject" "***SPAM***")
{
        fileinto "Junk";
        stop;
}
# rule:[VIRUS]
if header :contains "Subject" "***INFECTED***"
{
        fileinto "Junk";
        stop;
}
```

4. Чтобы скрыть папку sieve из списка папок для подписки:

/etc/dovecot/conf.d/10-mail.conf

```
maildir_stat_dirs = yes
```

lda-dupes

Fix Me!

Ошибка:

```
lmtp Error: file_dotlock_open(/home/user/.dovecot.lda-dupes) failed: No such file or directory
```

Нужно убрать `homeDirectory=home` из файла:

```
/etc/dovecot/dovecot-ldap.conf.ext
user_attrs                                                                                =
uidNumber=unset,gidNumber=unset,homeDirectory=home,mailQuotaSize=quota_rule=*:storage=%$M
```

Общие папки

Глобальные списки контроля доступа

Fix Me!

Списки контроля доступа IMAP ACL

Путь и имя задается в файле `90-acl.conf`

90-acl.conf

/etc/dovecot/conf.d/90-acl.conf

```
plugin {
    acl_anyone = allow
    acl = vfile:/etc/dovecot/global-acls:cache_secs=300
}

plugin {
    acl_shared_dict = file:/srv/mail/vmail/shared-mailboxes
}
```

global-acls

Fix Me! Сделать скрипт для создания и примеры.

Папка `/etc/dovecot/global-acls` содержит файлы с правами по умолчанию для папок.

.DEFAULT	для любой папки

Пример:

```
anyone lr
owner lrwstipekxa
```

```
authenticated lrwstipekxa
```

Список доступа к папке

Папка для которой задаются права содержит файл `dovecot-acl` Пример:

dovecot-acl

```
user=ИМЯ_ПОЛЬЗОВАТЕЛЯ ПРАВА
```

Пространство имён

⚠ Чтобы не слетала подписка при совместном использовании нужно указать `subscriptions = no`

10-mail.conf

/etc/dovecot/conf.d/10-mail.conf

```
mail_location = maildir:/srv/mail/vmail/%Ln
mail_home=/srv/mail/%Ln

namespace inbox {
  # Namespace type: private, shared or public
  type = private
  separator = /
  prefix =
  inbox = yes
  hidden = no
  list = yes
  subscriptions = yes
}

namespace {
# Чтобы скрыть shared/common/
  type = private
  separator = /
  prefix = shared/common/
  inbox = no
  hidden = yes
  list = no
  subscriptions = no
}

namespace {
    type = public
    separator = /
    prefix = common/
    location = maildir:/srv/mail/vmail/common
    inbox = no
    hidden = no
    list = yes
    subscriptions = no
}

namespace {
  type = shared
  separator = /
```

```
  prefix = shared/%%n/
  location = maildir:/srv/mail/vmail/%%n:INDEXPVT=/srv/mail/%n/shared/%%n
  subscriptions = no
  inbox = no
  list = children
}

mail_uid = vmail
mail_gid = mail
mail_privileged_group = mail
mail_access_groups = mail

mail_plugins = $mail_plugins acl quota
maildir_stat_dirs = yes
maildir_very_dirty_syncs = no
```

Общие папки пользователей

Пользователи могут задать права к своей папке

Fix Me!

Готовые настройки приведены в главе: Пример почтового сервера для внутреннего домена

Пространство имен

10-mail.conf

```
namespace {
  type = shared
  separator = /
  prefix = shared/%%n/
  location = maildir:/srv/mail/vmail/%%n:INDEX=/srv/mail/vmail/%n/shared/%%n
  inbox = no
  list = children
  subscriptions = no
}
```

Словарь

shared-mailboxes

```
90-acl.conf
plugin {
acl_shared_dict = file:/srv/mail/vmail/shared-mailboxes
}
```

в файле shared-mailboxes только список доступных папок, права определяются в ACL файлах. Этот файл нужен для того, чтобы в пространстве имен появились Общие папки.

Пример:

ПОЛЬЗОВАТЕЛЬ_1 предоставляет доступ к своим папкам (включая вложенные) для пользователей: ПОЛЬЗОВАТЕЛЬ_2 и ПОЛЬЗОВАТЕЛЬ_3

```
shared/shared-boxes/anyone/ПОЛЬЗОВАТЕЛЬ_1
1
shared/shared-boxes/user/ПОЛЬЗОВАТЕЛЬ_2/ПОЛЬЗОВАТЕЛЬ_1
1
shared/shared-boxes/user/ПОЛЬЗОВАТЕЛЬ_3/ПОЛЬЗОВАТЕЛЬ_1
1
```

Квоты

Fix Me!

Нужно добавить значение `quota` в переменную `mail_plugins` в эти файлы:

/etc/dovecot/conf.d/10-mail.conf

```
mail_plugins = $mail_plugins quota
```

/etc/dovecot/conf.d/15-lda.conf

```
protocol lda {
  mail_plugins = $mail_plugins quota
}
```

/etc/dovecot/conf.d/20-lmtp.conf

```
protocol lmtp {
  mail_plugins = $mail_plugins sieve quota
}
```

90-quota.conf

/etc/dovecot/conf.d/90-quota.conf

```
plugin {
  quota = maildir:User quota
  quota_rule = *:storage=100MB
  quota_rule2 = Trash:storage=+100M
  quota_exceeded_message = Quota exceeded (mailbox for user is full)
  quota_grace = 10%%
  quota_grace = 50M
}
```

mailQuotaSize

Имя поля в LDAP: `mailQuotaSize`, размер квоты задан в Мбайтах

Fix Me! заменить на dovecot-ldap.conf.ext

dovecot-ldap.conf.ext

```
user_attrs                                                                =
uidNumber=unset,gidNumber=unset,homeDirectory=home,mailQuotaSize=quota_rule=*:storage=%$M
```

Файл квот: `maildirsize`

Показать размер квоты для пользователя

```
doveadm -f tab quota get -u ПОЛЬЗОВАТЕЛЬ
```

LDAP

dovecot-ldap.conf.ext

/etc/dovecot/dovecot-ldap.conf.ext

```
hosts = localhost ldap directory
uris = ldap://localhost ldap://ldap ldap://directory
dn = cn=admin,dc=domain,dc=local
dnpass = ПАРОЛЬ
auth_bind = no
ldap_version = 3
base = ou=users,dc=domain,dc=local
deref = never
scope = subtree
user_attrs = uidNumber=unset,gidNumber=unset,mailQuotaSize=quota_rule=*:storage=%$M
user_filter = (&(objectClass=mailUser)(uid=%u))
pass_attrs = uid=user,userPassword=password
pass_filter = (&(objectClass=mailUser)(uid=%u))
default_pass_scheme = MD5
```

Мастер-пользователи

Под именем мастер-пользователя можно войти в систему от любого обычного пользователя, процедура входа выглядит так:

Имя	ПОЛЬЗОВАТЕЛЬ*МАСТЕР_ПОЛЬЗОВАТЕЛЬ
Пароль	ПАРОЛЬ_МАСТЕР_ПОЛЬЗОВАТЕЛЯ

Для работы рекомендуется RoundCube

После настройки необходимо выполнить действия по установке прав на папки для пользователей домена.

Настройка

1. Определяем базу мастер паролей auth-master.conf.ext

auth-master.conf.ext

/etc/dovecot/conf.d/auth-master.conf.ext

```
passdb {
  driver = passwd-file
  master = yes
  args = /etc/dovecot/master-users
}
```

2. Включаем `auth-master.conf.ext` в `10-auth.conf`:

```
!include auth-master.conf.ext
```

3. Создаем файл с паролями master-users:

master-users

Получение хеша пароля описано в главе Создание пароля

Пример (пароль `master`):

/etc/dovecot/master-users

```
master:{MD5}$1$T2nnJqr7$mbv9te4mQOn4INFyoUs7k.
```

Пункты 4 и 5 нужны для обеспечения работы с списками доступа `ACL`

4. Настройка процедуры `postlogin`

В файл `10-master.conf` вносим следущие изменения:

```
service imap {
  executable = imap imap-postlogin
}

service imap-postlogin {
  executable = script-login -d /srv/mail/vmail/postlogin.sh
  user = $default_internal_user
  unix_listener imap-postlogin {
  }
}
```

5. Создание файла `postlogin.sh`

/srv/mail/vmail/postlogin.sh

```
#!/bin/bash
MASTER_USER=$USER
exec "$@"
```

systemd

Fix Me!

Пример настройки: IMAP только `localhost`

/lib/systemd/system/dovecot.socket

```
[Unit]
Description=Dovecot IMAP/POP3 email server activation socket

[Socket]
#dovecot expects separate IPv4 and IPv6 sockets
BindIPv6Only=ipv6-only
ListenStream=127.0.0.1:143
ListenStream=[::1]:143
```

```
ListenStream=0.0.0.0:993
ListenStream=[::]:993
KeepAlive=true

[Install]
WantedBy=sockets.target
```

SSL

Пример настройки работы по IMAPS(порт 993), с использованием сертификатов Let's Encrypt:

/etc/dovecot/conf.d/10-ssl.conf

```
ssl = yes

ssl_cert = </etc/letsencrypt/live/domain.ru/fullchain.pem
ssl_key = </etc/letsencrypt/live/domain.ru/privkey.pem

ssl_prefer_server_ciphers = yes

ssl_min_protocol = TLSv1
ssl_cipher_list                                                                 =
ALL:!LOW:!SSLv2:!EXP:!aNULL:!RC4::!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS
```

Также нужно добавить в секцию «service imap-login» настройку для `imaps`

/etc/dovecot/conf.d/10-master.conf

```
service imap-login {
    inet_listener imaps {
        port = 993
        ssl = yes
    }
}
```

logrotate

Fix Me!

Настройка ротации протокола с помощью logrotate:

/etc/logrotate.d/dovecot

```
/var/log/dovecot*.log {
  missingok
  notifempty
  delaycompress
  sharedscripts
  postrotate
    doveadm log reopen
  endscript
}
```

http://wiki2.dovecot.org/Logging

Ссылки

Русский перевод dovecot.conf v.1.2.17

Dovecot 2 по шагам

Dovecot 2 - описание настроек, в контексте рассматриваемой конфигурации

Dovecot 2 - ACL

Migrating from any IMAP/POP3 server to Dovecot via dsync

http://wiki2.dovecot.org/HowTo/PostfixAndDovecotSASL

https://sysadminmosaic.ru/dovecot/dovecot

2020-11-02 11:41