Mail

Модуль предназначен для упрощения процесса создания и управления почтовыми ящиками пользователей из интерфейса биллинга.

Возможности

- Авторизация на отправку почты (Plain Password, TLS)
- Авторизация на приём почты (Plain Password, TLS)
- Квоты на размер почтового ящика и количество писем
- Управление неограниченным количеством доменов
- Фильтры, аксеслисты, алиасы
- Антиспам
- Антивирус
- Заведение нескольких почтовых ящиков на один пользовательский акаунт
- Возможность изменять пароль на почтовый ящик пользователем

Установка

abills/libexec/config.pl

```
@MODULES = (
          'Mail'
          );
```

При использовании SpamAssasin

```
mysql -D abills < db/Mail.sql
```

$conf{MAIL_CHG_PASSWD}=1;	Разрешить пользователям изменять пароли для своих почтовых ящиков
$conf {MAIL_USER_FULL_CONTROL} =1;	Разрешить пользователям удалять и добавлять себе почтовые ящики с возможностью снятия платы за услугу
$conf {MAIL_USER_DOMAIN_MNG}=1;	Разрешить пользователю управлять своим доменом
$conf{MAIL_SPAMD} ='spamassasin';	Включить поддержку SpamAssasin

Настройка

Меню **Настройка>E-MAIL**

Domains

Список виртуальных доменов системы.

Domain	Название домена
Transport	Транспорт для данного домена. Возможные варианты: virtual: maildrop: Почтовый агент maildrop local: relay:
Backup MX	Сервер является промежуточный MX для данного домена
Disable	Блокировать
Comments	Коментарии

Access

Контроль доступа к почтовой службе.

Меню Клиенты>Логины>E-MAIL List - Список почтовых ящиков системы.

Меню Customers>Logins>Information>Services>E-MAIL - Управление почтовым ящиком пользователя.

Postfix

Используемые константы:
%user% - имя пользователя в MySQL
%password% - пароль в MySQL
%dbname% - база MySQL
%hosts% - хост MySQL

cyrus-sasl2

SASL - (**Simple Authentication and Security Layer**) служит для авторизации входящих соединений от пользователей.

Сборка

```
cd /usr/ports/security/cyrus-sasl2
make USE_MYSQL_VERSION=5 WITHOUT_OTP=yes WITHOUT_NTML=yes && make install
```

Конфигурация
Создаем файл **/usr/local/lib/sasl2/smtpd.conf**

```
pwcheck_method: saslauthd auxprop
mech_list: login plain
auxprop_plugin: sql
sql_engine: mysql
mysql_user: %dbuser%
mysql_passwd: %dbpasswd%
mysql_database: %dbname%
mysql_hostnames: %dbhost%
mysql_statement: SELECT DECODE(mb.password, 'test12345678901234567890') FROM mail_boxes mb, mail_domains
md WHERE CONCAT(mb.username, '@', md.domain)='%u@%r' and mb.domain_id=md.id and mb.status = '0' and (mb.
expire = '0000-00-00' or mb.expire > curdate())
```

Далее

```
chmod 750 /usr/local/lib/sasl2
chgrp mail /usr/local/lib/sasl2
```

Автостарт saslauthd при запуске системы FreeBSD

```
echo saslauthd_enable=\"YES\" >> /etc/rc.conf
```

проверить механизм авторизации

```
saslauthd -v
```

Postfix

Postfix При установке postfix в меню выбираем поддержку SASL2, VDA, TLS и MYSQL.

```
cd /usr/ports/mail/postfix && make install clean
```

Проверяем собран ли Postfix с поддержкой Cyrus-SASL

```
postconf -a
```

Если включён должна присутствовать строка:

```
cyrus
```

Проверяем собран ли Postfix с поддержкой Mysql

```
postconf -m
```

Если включён должна присутствовать строка:

```
mysql
```

После установки

```
newaliases
```

main.cf должен содержать:

```
debug_peer_level = 2
command_directory = /usr/local/sbin
daemon_directory = /usr/local/libexec/postfix
#mydestination = $myhostname

disable_vrfy_command = yes
smtpd_helo_required = yes

smtpd_helo_restrictions =       permit_mynetworks,
                    reject_invalid_hostname,
                    reject_unknown_hostname,
                    reject_non_fqdn_hostname

smtpd_recipient_restrictions =  permit_mynetworks,
                    permit_sasl_authenticated,
                    reject_unauth_destination,
                    reject_unknown_recipient_domain,
                    reject_non_fqdn_recipient,
                    reject_unauth_destination



smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sender_restrictions =     permit_mynetworks,
                    permit_sasl_authenticated,
                    reject_unknown_sender_domain,
                    check_sender_access mysql:/usr/local/etc/postfix/sql/access.cf
#                      reject_rhsbl_sender dsn.rfc-ignorant.org

transport_maps = mysql:/usr/local/etc/postfix/sql/transport.cf
virtual_alias_maps = mysql:/usr/local/etc/postfix/sql/aliases.cf
virtual_gid_maps = static:1005
virtual_mailbox_base = /var/spool/virtual
virtual_mailbox_domains = mysql:/usr/local/etc/postfix/sql/virtual_domains.cf
virtual_mailbox_maps = mysql:/usr/local/etc/postfix/sql/virtual_mailbox.cf
virtual_mailbox_limit = 51200000
virtual_minimum_uid = 1005
virtual_uid_maps = static:1005
# Additional for quota support for virtual transport
#virtual_create_maildirsize = yes
#virtual_mailbox_extended = yes
#virtual_mailbox_limit_maps = mysql:/usr/local/etc/postfix/sql/virtual_mailbox_limits.cf
#virtual_mailbox_limit_override = yes
#virtual_maildir_limit_message = Sorry, the user's maildir has overdrawn his diskspace quota, please try
again later.
#virtual_overquota_bounce = yes

maildrop_destination_recipient_limit=1

readme_directory = no
sample_directory = /usr/local/etc/postfix
sendmail_path = /usr/local/sbin/sendmail
html_directory = no
setgid_group = maildrop
manpage_directory = /usr/local/man
newaliases_path = /usr/local/bin/newaliases
mailq_path = /usr/local/bin/mailq
queue_directory = /var/spool/postfix
mail_owner = postfix
```

Для TLS авторизации создаём сертификат x509 добавляем в конфиг **main.cf**:

```
# tls config
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls_offer = yes
smtpd_tls_key_file = /usr/abills/Certs/smtpd.key
smtpd_tls_cert_file = /usr/abills/Certs/smtpd.cert
smtpd_tls_CAfile = /usr/abills/Certs/smtpd.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
```

Создание сертификата

```
/usr/abills/misc/certs_create.sh postfix_tls
```

Обратите внимание! Что virtual uid и gid имеют статическую привязку и эти значения следует изменить на uid и gid юзера, от которого будет работать maildrop. В моем случае, это юзер vmail с uid 1005 и gid 1005. Транспорт virtual не поддерживает квоты, в отличии от maildrop, поэтому, если вы хотите включить поддержку квот для virtual, установите патч VDA

Создайте пользователя vmail с UID 1005 и GID 1005

Каталог для виртуальных хостов

```
# mkdir /var/spool/virtual
# chown -R vmail:vmail /var/spool/virtual
# chmod -R 771 /var/spool/virtual
```

transport.cf

```
user = %dbuser%
password = %dbpasswd%
dbname = %dbname%
hosts = %dbhost%
query = SELECT transport FROM mail_domains WHERE domain='%d'
```

access.cf

```
user = %dbuser%
password = %dbpasswd%
dbname = %dbname%
hosts = %dbhost%
query = SELECT action FROM mail_access WHERE pattern='%s'
```

aliases.cf

```
user = %dbuser%
password = %dbpasswd%
dbname = %dbname%
hosts = %dbhost%
query = SELECT goto FROM mail_aliases WHERE address='%s'
```

virtual_domains.cf

```
user = %dbuser%
password = %dbpasswd%
hosts = %dbhost%
dbname = %dbname%
query = SELECT domain FROM mail_domains WHERE domain='%s' AND backup_mx='0' AND status='0'
```

virtual_mailbox.cf

```
user = %dbuser%
password = %dbpasswd%
dbname = %dbname%
hosts = %dbhost%
query = SELECT CONCAT(md.domain,'/',mb.username,'/') FROM mail_boxes mb, mail_domains md WHERE CONCAT(mb.
username, '@', md.domain)='%s' and mb.domain_id=md.id and mb.status = '0' and (mb.expire = '0000-00-00'
or mb.expire > curdate())
```

virtual_mailbox_limits.cf

```
user = %dbuser%
password = %dbpasswd%
hosts = %dbhost%
dbname = %dbname%
query = SELECT box_size * 1048576 FROM mail_boxes mb, mail_domains md WHERE CONCAT(mb.username, '@', md.
domain)='%s' and mb.domain_id=md.id and mb.status = '0'
```

Автозагрузка при старте /etc/rc.conf

```
#   sendmail
sendmail_enable="NONE"
mta_start_script=""
sendmail_outbound_enable="NO"
sendmail_submit_enable="NO"
sendmail_msp_queue_enable="NO"

#  postfix
postfix_enable="YES"
```

maildrop

http://www.courier-mta.org/maildrop
maildrop является альтернативой широко используемому procmail и имеет гораздо большие возможности - поддержка mysql и ldap, поддержка квот, более мощный язык фильтрации, повышенная безопасность, поддержка формата Maildir++. Более подробная документации в директории **/usr/local/share/doc/maildrop**

```
cd /usr/ports/mail/maildrop
make WITH_AUTHLIB=yes MAILDROP_TRUSTED_USERS=vmail MAILDROP_SUID=1005 MAILDROP_SGID=1005
make install
```

```
#    AUTHLIB multi, select at least one option,   :
make WITH="AUTHLIB" WITH="AUTH_MYSQL" MAILDROP_TRUSTED_USERS=vmail MAILDROP_SUID=1005
MAILDROP_SGID=1005
make install
```

После сборки запустите maildrop -v. Должны быть следующие строки
Courier Authentication Library extension enabled.
Maildir quota extension enabled.

В **/usr/local/etc/postfix/master.cf** измените конфиг maildrop на

```
maildrop  unix  -       n       n       -       -       pipe
    flags=Rhu user=vmail argv=/usr/local/bin/maildrop -w 90 -d ${recipient}
```

Создаем файл **/var/spool/virtual/.mailfilter** со следующим содержанием

```
SHELL=/bin/sh
UMASK=077
mail=tolower($mail)
LOGNAME=tolower($LOGNAME)
VERBOSE=7
user=`echo $LOGNAME|sed s/\@/\ /| awk '{print $1}'`
domain=`echo $LOGNAME|sed s/\@/\ /| awk '{print $2}'`
MAILDIR="$HOME/$domain/$user/"

#Make maildir if not exists
`test -d $MAILDIR`
if ($RETURNCODE!=0)
 {
  `test -d $HOME/$domain/`
   if ($RETURNCODE!=0)
    {
     `mkdir "$HOME/$domain/"`
    }

  `/usr/local/bin/maildirmake $MAILDIR`
  #Make spam dir
  `/usr/local/bin/maildirmake -f Spam $MAILDIR`
  }
#Filter check system
# Check user filter if exist use filter
FILTERDIR="$HOME/.mailfilters/$LOGNAME"

`test -d $FILTERDIR`
 if ($RETURNCODE!=0)
  {
   to "$MAILDIR"
   }
 else
  {
   include "$HOME/.mailfilters/$LOGNAME"
   }
```

Ставим права на запись и чтение только пользователю иначе maildrop откажется работать.

```
chmod 600 /var/spool/virtual/.mailfilter
chown vmail:vmail /var/spool/virtual/.mailfilter
```

Создаем директорию **/var/spool/virtual/.mailfilters**

```
mkdir -m 700 /var/spool/virtual/.mailfilters
chown vmail:vmail /var/spool/virtual/.mailfilters
```

Для включения пользовательского фильтра, который будет раскладывать почту по дополнительным ящикам, создаем include файл в формате user@domain соответствующему переменной $LOGNAME **/var/spool/virtual/.mailfilters/user@test.local.net** со следующим содержанием

```
user=`echo $LOGNAME|sed s/\@/\ /| awk '{print $1}'`
domain=`echo $LOGNAME|sed s/\@/\ /| awk '{print $2}'`
MAILDIR="$HOME/$domain/$user/"

if ( /^X-Spam-Status: Yes/:h )
 {
  to "$MAILDIR/.Spam"
  #    /dev/null
  # to "| cat - >/dev/null"
 }
to $MAILDIR
```

Файл **/var/spool/virtual/.mailfilters/user@test.local.net** - предоставляет возможность maildrop выбрать нужный конфиг для пользователя, используя его логин, который берется из переменной $LOGNAME (user@domain). В директории .mailfilters хранятся конфиги для каждого виртуального юзера. Maildrop будет искать конфиг в формате user@domain и использовать его.
Можно написать скрипт, который при создании maildir, автоматически создает нужный конфиг с дефолтными опциями в .mailfilters.
В данном примере maildrop отбирает почту с заголовком X-Spam-Status: Yes, который генерирует spamassassin, установка которого будет рассмотрена ниже, и кладет ее в папку Spam. Остальная почта направляется в INBOX. Примеры фильтров для maildrop можно найти на mdropspammailfilter

Создаем файл **/usr/local/etc/quotawarnmsg**

courier-authlib

Демон авторизации для dropmail, courier-imap, courier-pop3d

```
cd  /usr/ports/security/courier-authlib && make && make install
```

Для доступа к спулу почты /var/spool/virtual courier работает от юзера vmail (uid 1005,gid 1005)

```
pw group mod vmail -m courier
```

Правим конфигурационный файл для courier-authlib **/usr/local/etc/authlib/authmysqlrc**

```
MYSQL_CLEAR_PWFIELD     DECODE(mb.password, '%secretkey%')
MYSQL_DATABASE          %dbname%
MYSQL_PASSWORD          %dbpasswd%
MYSQL_USERNAME          %dbuser%
MYSQL_SERVER            %dbhost%
MYSQL_GID_FIELD         '1005'
MYSQL_HOME_FIELD        CONCAT('/var/spool/virtual/')
MYSQL_LOGIN_FIELD       CONCAT(mb.username, '@', md.domain)
MYSQL_MAILDIR_FIELD     CONCAT('/var/spool/virtual/', md.domain,'/',mb.username,'/')
MYSQL_NAME_FIELD        CONCAT(mb.username, '@', md.domain)
MYSQL_OPT               0
MYSQL_PORT              3306
MYSQL_QUOTA_FIELD       CONCAT(mb.box_size * 1048576,'S')
MYSQL_UID_FIELD         '1005'
MYSQL_USER_TABLE        mail_boxes mb, mail_domains md
MYSQL_WHERE_CLAUSE      mb.status='0' AND mb.domain_id=md.id
```

Убедитесь что использована табуляция, а не пробелы, иначе конфиг не будет работать.
Делаем возможность доступа пользователя vmail к сокету авторизации

```
chown vmail /var/run/authdaemond/
```

Автозагрузка при старте системы **/etc/rc.conf**

```
courier_authdaemond_enable="YES"
```

Установка Courier-imap

Courier-imap
Courier Authentication Library

```
cd /usr/ports/mail/courier-imap && make WITH_CRAM=yes WITH_MYSQL=yes install clean
chmod 700 /usr/local/etc/courier-imap/
chown vmail:vmail /var/run/authdaemond/
```

Создаем SSL сертификат (для работы в защищённом режиме)

```
cd /usr/local/etc/courier-imap/
cp /usr/local/etc/courier-imap/imapd.cnf.dist /usr/local/etc/courier-imap/imapd.cnf
mkimapdcert
cp /usr/local/etc/courier-imap/pop3d.cnf.dist /usr/local/etc/courier-imap/pop3d.cnf
mkpop3dcert
cp /usr/local/etc/courier-imap/imapd.dist /usr/local/etc/courier-imap/imapd
cp /usr/local/etc/courier-imap/pop3d-ssl.dist /usr/local/etc/courier-imap/pop3d-ssl
```

В **/usr/local/etc/courier-imap/imapd** меняем

```
TCPDOPTS="-nodnslookup -noidentlookup"
```

на

```
TCPDOPTS="-nodnslookup -noidentlookup -user=vmail"
```

Для автозагрузки при старте систему прописываем в /etc/rc.conf
Для IMAP сервера:

```
courier_imap_imapd_enable="YES"
```

Для POP3 сервера

```
courier_imap_pop3d_enable="YES"
```

Данная установка рассчитана на мультидоменные почтовые системы, по этому в качестве логина для авторизации при получении почты нужно использовать связку логин@домен.

/etc/rc.conf

```
courier_imap_pop3d_ssl_enable="YES"
courier_imap_imapd_ssl_enable="YES"
```

SpamAssassin

SpamAssassin

Настройка Спамфильра

Установка

```
cd /usr/ports/mail/spamassassin && make install clean
```

Обязательно отмечаем MySQL. После установки внимательно смотрим на вывод пост-инсталл информации.

Возможно уведомление о том что отсутствуют некоторые Perl модули. Их необходимо доустановить вручную.

/usr/local/etc/mail/spamassassin/local.cf

```
user_scores_dsn                                 DBI:mysql:%dbname%:%dbhost%
user_scores_sql_username        %dbuser%
user_scores_sql_password        %dbpasswd%
user_scores_sql_custom_query     SELECT preference, value FROM mail_spamassassin
  WHERE username = _USERNAME_ OR username = '$GLOBAL' OR username = CONCAT('%',_DOMAIN_)
  ORDER BY username ASC

# Autowhite list
auto_whitelist_factory Mail::SpamAssassin::SQLBasedAddrList
user_awl_dsn                DBI:mysql:%dbname%:%dbhost%
user_awl_sql_username       %dbuser%
user_awl_sql_password       %dbpasswd%
user_awl_sql_table          mail_awl
```

SpamAssassin не понимает переноса строк в конфигурационном файле, поэтому пишите запрос в одной строке.

Автозапуск в FreeBSD

```
echo spamd_enable=\"YES\" >> /etc/rc.conf
```

После установки и конфигурации запускаем :

```
sa-update
sa-compile
```

sasql - Плагин для SquirrelMail для управления спам фильтром

Настройка милтера для связи фильтра с почтовым сервером:

AMaViS

AMaViS

Собираем Антивирус clamav

```
cd /usr/ports/security/clamav && make install clean
```

Собираем AMaViS

```
cd /usr/ports/security/amavisd-new && make install clean
```

Автозапуск сервисов: **/etc/rc.conf**

```
clamav_clamd_enable="YES"
clamav_freshclam_enable="YES"

amavisd_enable="YES"
amavisd_ram="512m"
```

Изменяем параметры **/usr/local/etc/amavisd.conf**

```
$mydomain
$myhostname
```

для связки с **Clamav** нужно раскомментировать

```
# ### http://www.clamav.net/
 ['ClamAV-clamd',
   \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd"],
   qr/\bOK$/, qr/\bFOUND$/,
   qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

и потом добавить пользователя под которым работает Clamav в группу Amavis-new (по умолчанию vscan)

/etc/group

```
vscan:*:110:clamav
```

Запускаем

```
/usr/local/etc/rc.d/clamav-freshclam start
/usr/local/etc/rc.d/clamav-clamd start
/usr/local/etc/rc.d/amavisd start
```

Правка конфигов **Postfix**
/usr/local/etc/postfix/main.cf

```
content_filter = smtp-amavis:[127.0.0.1]:10024
max_use = 10
```

/usr/local/etc/postfix/master.cf

```
# AMaVIs interface
smtp-amavis unix -      -       n       -       2       smtp
    -o smtp_data_done_timeout=1200
    -o disable_dns_lookups=yes

127.0.0.1:10025 inet n  -       n       -       -       smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_client_restrictions=
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o mynetworks=127.0.0.0/8
    -o strict_rfc821_envelopes=yes
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
```

Управление антиспамом

Можно осуществлять через админ. форму или через веб-интерфейс почтового клиента Squirellmail.

(System configuration>E-MAIL> SpamAssassin>All)

ID:	Номер правила в системе
Пользователь ($GLOBAL - Все):	E-mail пользователя. При параметре $GLOBAL применяется всем пользователям
Настройки:	Настройки. blacklist_from blacklist_to
Значение:	Адрес для блокировки. Пример: *@advertisingbymail.com test@advertisingbymail.com
Комментарии:	Комментарии

Ошибки

Postfix: Ошибка групп

```
postfix/postfix-script: warning: not set-gid or not owner+group+world executable: /usr/sbin/postqueue
postfix/postfix-script: warning: not set-gid or not owner+group+world executable: /usr/sbin/postdrop
```

Установка корректных прав

```
chmod 2555 /usr/sbin/postqueue
chmod 2555 /usr/sbin/postdrop
postfix set-permissions
```

Postfix: Ошибка окружения

```
fatal: unknown service: smtp/tcp
```

решение

```
cp /etc/services  /var/spool/postfix/etc/
```

Проверка работоспособности maildrop

```
/usr/local/bin/maildrop -V 3  -w 90 -d test@test.domain maildrop
```

imapd-ssl: maximum connection limit reached for

```
imapd-ssl: maximum connection limit reached for 1.45.55.6
```

Возможен такой вариант:

```
imapd: maximum connection limit reached for 1.45.55.6
```

Посмотрел – в конфигах **/usr/local/etc/courier-imap/imapd** и **/usr/local/etc/courier-imap/imapd-ssl** есть переменная MAXPERIP по дефолту равная четырём. То есть imap принимает только по четыре соединения с одного айпишника (судя по всему, по соображениям безопасности для контроля расхода ресурсов), что конечно очень мало, если к примеру по имапу к серверу обращаются клиенты из-за ната. Меняем на большее значение:

```
MAXPERIP=40
```

и перезапускаем сервис:

```
cd /usr/local/etc/rc.d
./courier-imap-imapd-ssl restart
./courier-imap-imapd restart
```

Дополнительно

Очередь отправки

```
postqueue -p
```

почистить очередь

```
postsuper -d ALL
```

- Pflogsumm
- AWStats

Настройка почтового клиента

- Thunderbird
- The Bat
- Outlook Express
- Pine

1. **local send**

   ```
   mail -v
   ```

   !check port
   !check mailoy
2. **send to gmail**

   ```
   mail -v
   ```

   !check maillog

3. **reply know ymail**

   !check maillog