

Требуется: несложный мейлер с поддержкой виртуальных доменов + локальная доставка. SMTP, IMAP, POP3 с авторизацией. Без всякой антиустойчивой ереси вроде MySQL :)
Система : FreeBSD 5.x, CentOS 5.x

Оригинал: http://pentarh.googlepages.com/postfix-sasl-cyrus-mta Отличие от оригинальной статьи: Прикручена SASL авторизация (с теми же данными что и POP3) к SMTP, запрещен рилей для world. Исправлено несколько подводных камней, с которыми я мучался пару дней. Прикручена доставка локальной почты (root©localhost)
Решение: Postfix MTA, Авторизация Cyrus SASL 2, POP3/IMAP - Cyrus IMAPd 2.2 Ставим из портов. Если на каком-либо этапе что-либо отказывается работать, смотрите логи и делайте выводы. Полезные логи: /var/log/auth.log - SASL, imapd /var/log/maillog - Postfix /var/log/messages - все подряд :)
Berkeley DB # cd /usr/ports/databases/db4 # make install clean
Используется имеено 4я версия беркли, т.к. с ней у меня было меньше всего глюков при установке из портов.

Cyrus SASL Этот порт будет обрабатывать авторизацию по POP3/IMAP (Cyrus) и SMTP (Postfix). Работает как универсальный модуль авторизации.
cd /usr/ports/security/cyrus-sasl2 # make WITHOUT_OTP=YES WITHOUT_NTLM=YES WITHOUT_GSSAPI=YES WITH_BDB_VER=4 # make install clean && rehash
Здесь отключены "ненужные" механизмы авторизации. Проверяем установку. Создадим юзера "admin", зададим пароль и просмотрим базу данных авторизации:

saslpasswd2 -c admin # sasldblistusers2 admin ©
yourhostname.com: userPassword
Запомните пароль на юзера admin, он еще понадобится. Изменить пароль всегда можно командой "saslpasswd2 admin". При добавлении юзеров в логах иногда появляются странные вещи вроде:
saslpasswd2: setpass succeeded for admin saslpasswd2: error deleting entry from sasldb: DB_NOTFOUND: No matching key/data pair found
Я устал с ними бороться и уже не обращаю внимания :) Авторизация не смотря ни на что работает. Необходимо убедиться что база данных SASL (/usr/local/etc/sasldb2) имеет аттрибут chmod 640 и принадлежит юзеру cyrus и группе mail (чтобы и postfix и cyrus могли ее читать). В добавок теперь надо сделать симлинк /usr/lib/sasl2 -> /usr/local/lib/sasl2. Это требуется для нормальной работы Postfix SMTP авторизации через SASL.
Cyrus IMAPd Этот порт будет отвечать за локальную доставку в локальные и

виртуальные мейлбоксы. Взаимодействует с постфиксом через LMTP unix сокет /var/imap/socket/lmtp. Ставим из портов, в диалоге сразу жмем "окей".

cd /usr/ports/mail/cyrus-imapd22 # make USE_BDB_VER=4 # mail install clean

Инициализируем каталоги

mkdir /var/imap # mkdir /var/imap/spool # chown -R cyrus:mail /var/imap # chmod -R 751 /var/imap

Чобы imap успешно поднялся, надо прописать в /etc/rc.conf:

cyrus_imapd_enable="YES"

Postfix и Cyrus взаимодействуют между собой через сокет, его имя и размещение указано в /usr/local/etc/cyrus.conf. Закомментируйте строку, содержащую lmtp и добавльте:

lmtpunix cmd="lmtpd" listen="/var/imap/socket/lmtp" prefork=0

Главным файлом конфигурации Cyrus является /usr/local/etc/imapd.conf. Его краткое содержание представлено ниже, обратите внимание на комментарии:

[root@lockdoc etc]# cat ./imapd.conf reject8bit: no autocreatequota: 102400 hashimapspool: 1 sasl_pwcheck_method: auxprop sasl_auxprop_plugin: sasldb sasl_sasldb_path: /etc/sasldb2 sasl_mech_list: plain login cram-md5 digest-md5 sievedir: /var/lib/imap/sieve configdirectory: /var/lib/imap admins: admin lmtp_overquota_perm_failure: no dracinterval: 0 poptimeoute: 10 autocreatequota_units: 1048576 sendmail: /usr/sbin/sendmail aloowanonymouslogin: no partition-default: /var/spool/imap loginrealms: d1.com d2.com quotawarn: 90 timeoute: 30 drachost: localhost unixhierarchysep: no virtdomains: userid defaultdomain: yourhostname.com tls_cert_file: /var/imap/server.pem tls_key_file: /var/imap/server.pem tls_ca_file: /var/imap/server.pem

где

yourhostname.com - хостнейм сервера d1.com d2.com - обслуживаемые виртуальные домены

Создаем сертификаты:

mkdir /var/imap openssl req -new -x509 -nodes -out /var/imap/server.pem -keyout /var/imap/server.pem -days 720 chown cyrus:mail /var/imap/server.pem chmod 600 /var/imap/server.pem # Your key should be protected echo tls_ca_file: /var/imap/server.pem >> /etc/imapd.conf echo tls_cert_file: /var/imap/server.pem >> /etc/imapd.conf echo tls_key_file: /var/imap/server.pem >> /etc/imapd.conf

Теперь нам необходимо создать несколько каталогов, необходимых для подготовки Cyrus к работе:

su cyrus % /usr/local/cyrus/bin/mkimap % exit

С правами рута:

/usr/local/etc/rc.d/imapd.sh start

Смотрим в /var/log/messages на матюки :) Подобные следующим матюкам можно пропустить мимо глаз:

ctl_cyrusdb[63797]: checkpointing cyrus databases ctl_cyrusdb[63797]: DBERROR: error listing log files: DB_NOTFOUND: No matching key/data pair found ctl_cyrusdb[63797]: DBERROR: archive /var/imap/db: cyrusdb error ctl_cyrusdb[63797]: DBERROR: error listing log files: DB_NOTFOUND: No matching key/data pair found ctl_cyrusdb[63797]: DBERROR: archive /var/imap/db: cyrusdb error

Главное чтобы команда "sockstat | grep ':143'" выдавала строку слушающего демона цирруса. Проверяем работу IMAPd:

telnet localhost 143 Trying ::1... Connected to localhost. Escape character is '^]'. * OK yourhostname.com Cyrus IMAP4 v2.2.12 server ready . logout * BYE LOGOUT received . OK Completed Connection closed by foreign host.

Для каждого почтового ящика необходимо создать и SASL2 и Cyrus ID. Для примера, создадим пользователя test в домене d1.com:

Создаем SASL2 ID: # saslpasswd2 -c test©d1.com Password: Again (for verification): # sasldblistusers2 test
©
d1.com: userPassword

Создаем Cyrus ID, учтите, что вам понадобится пароль пользователя admin, изменить его можно командой 'saslpasswd2 admin'. Вообще, чтобы создать почтовый язик в циррусе из-под админа, надо выполнить две команды. Для создания почтового ящика, не забудьте добавить префикс 'user.' к нему. 1. cm user.mailbox©domain - создаст почтовый ящик 2. Чтобы из-под админа можно было его удалить, надо гарантировать админу CREATE привилегию на этот ящик тут же: sam user.mailbox©domain admin c Итак: #cyradm --user admin localhost Password: youhostname.com> cm user.test
©
d1.com youhostname.com> lm user.test
©
d1.com (HasNoChildren) youhostname.com> sam user.test
©
d1.com admin c youhostname.com> quit

Для тех, кого интересует автоматизация процесса, все эти команды доступны при коннекте к IMAP серверу (по расширенному IMAP протоколу RFC 4314,RFC 1730,RFC 2087). В особенности cyrrus входит что при создании мейлбокса надо делать префикс "user.".

Postfix Прежде всего, киляем процесс sendmail (или текущий MTA). Далее, ставим Postfix из порта. В открывающемся диалоге выбираем Cyrus SASL v2 и Berkely DB 4. При вопросе, добавить ли postfix в группу mail, отвечаем "yes" # cd /usr/ports/mail/postfix # make install clean # rehash

Смотрим, чего насоветовал нам make, делаем выводы. Редактируем /etc/rc/conf:

sendmail_enable="NONE" sendmail_flags="-bd" sendmail_pidfile="/var/spool/postfix/pid/master.pid" sendmail_outbound_enable="NO" sendmail_submit_enable="NO" sendmail_msp_queue_enable="NO"

Создадим символическую ссылку, необходимую для запуска во время начальной загрузки:

cd /usr/local/etc/rc.d # ln -s /usr/local/sbin/postfix postfix.sh

Также необходимо отключить спечифичные для Sendmail инструкции в файле

/etc/periodic.conf. Если этого файла нет, создайте его.

daily_clean_hoststat_enable="NO" daily_status_mail_rejects_enable="NO" daily_status_include_submit_mailq="NO" daily_submit_queuerun="NO"

Когда Postfix уже сконфигурирован, необходимо создать базу данных псевдонимов alias.db и запустить Postfix. Так как /etc/aliases.db имеет формат отличный от Berkeley 4, вместо команды newaliases используейте postalias:

postalias /etc/aliases # ls -l /etc/aliases.db # postmap /usr/local/etc/postfix/virtual # postfix start

Проверим что postfix работает:

telnet localhost 25 Trying 127.0.0.1... Connected to localhost. Escape character is '^]'. 220 server.pentarh.com ESMTP Postfix quit 221 Bye Connection closed by foreign host.

Отредактируем /usr/local/etc/postfix/main.cf Обратите внимание на выделенное жирным шрифтом:

command_directory = /usr/local/sbin daemon_directory = /usr/local/libexec/postfix mailq_path = /usr/local/bin/mailq manpage_directory = /usr/local/man newaliases_path = /usr/local/bin/newaliases queue_directory = /var/spool/postfix sample_directory = /usr/local/etc/postfix sendmail_path = /usr/local/sbin/sendmail mail_owner = postfix soft_bounce = no myhostname = yourhostname.com myorigin = $mydomain relay_domains = $mydestination local_recipient_maps = $virtual_mailbox_maps recipient_delimiter = + debug_peer_level = 2 mynetworks_style = host smtpd_sasl_application_name = smtpd smtpd_sasl_auth_enable = yes smtpd_sasl_local_domain = $myhostname smtpd_sasl_security_options = noanonymous unknown_local_recipient_reject_code = 550 setgid_group = maildrop html_directory = no readme_directory = no masquerade_domains = $mydomain smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated, permit_auth_destination, reject smtpd_helo_restrictions = reject_invalid_hostname smtpd_require_helo = yes mailbox_transport = lmtp:unix:/var/imap/socket/lmtp virtual_transport = lmtp:unix:/var/imap/socket/lmtp virtual_mailbox_domains = d1.com d2.com virtual_alias_maps = hash:/usr/local/etc/postfix/virtual

где

yourhostname.com - хостнейм сервера d1.com d2.com - обслуживаемые виртуальные домены

Для того, чтобы SMTP авторизация работала, создадим файл /usr/lib/sasl2/smtpd.conf:

pwcheck_method: auxprop auxprop_plugin: sasldb mech_list: plain login cram-md5 digest-md5

Также надо убедиться, что демон smtpd работает не в chroot (дабы иметь доступ к sasldb2). Для этого посмотрите файл /usr/local/etc/postfix/master.cf и убедитесь что в поле "chroot" против демона "smtp" стоит значение "n". Так же поле unpriv должно иметь значение "y". Можно конечно и запустить его в chroot, при этом создав жесткую ссылку на sasldb2, но мне лично мучаться пока не хо. Перезапустим postfix:

postfix reload

Теперь попытайтесь извне послать мыло по нашему SMTP с любым юзером из

sasldb2. Надеюсь, у вас все получится :)

Управление почтой

Управление почтой сводится к следующему. 1. При добавлении нового домена или его удалении, необходимо внести изменения в

- /usr/local/etc/imapd.conf (переменная loginrealms) - /usr/local/etc/postfix/main.cf (переменная virtual_mailbox_domains) - Соответственно, перезапустить postfix и imapd.

2. При добавлении мыла user©domain.com с форвардом на fwd©somewhere.com, добавить строку "user©domain.com fwd©somewhere.com" в файл /usr/local/etc/postfix/virtual и выполнить команду

postmap /usr/local/etc/postfix/virtual

3. При добавлении регулярного почтового ящика user©domain.com : - Создать этот почтовый ящик в Cyrus используя команду cyradm (как описано выше). Либо автоматизируя процесс, создать скриптом по IMAP этот ящик на сервере, подсоединившись на localhost:143 (что собсно и делает cyradm).

- Создать для него логин в SASL, используя команду "saslpasswd2 -c user©domain.com" - Указать postfix на локальную доставку этого мейлбокса, создав строку "user©domain.com user©domain.com" в /usr/local/etc/postfix/virtual и выполнив postmap как описано выше. - POP3/IMAP логин будет user©domain.com, пароль - который вы задали в SASL - автоматически "раздуплится" аналогичный логин и пароль для SMTP авторизации

4. Для создания отдельного SMTP логина/пароля, просто добавьте соотв. юзера в sasldb2 используя вышеописанную команду saslpasswd2. Для работы локальной доставки мыл на root©yourhostname, добавьте по п.3 соотв. почтовый ящик. При большом желании можно написать пару скриптов, автоматизирующих эти действия :)

Замечание: Если вы настраиваете реальный MX, то весьма желательно, чтобы ваш хостнейм был реальным доменом и откликался на примари IP вашего MX. Еще весьма желательно чтобы reverse-DNS примари IP вашего сервера указывала на ваш хостнейм. Таким образом, почта будет ходить довольно неплохо.