**Postfix & Dovecot: разгонный курс по почтовым системам. Почтовик с нуля**

(даркмайклу посвящается)

# Оглавление

[Оглавление 1](#_Toc47868657)

[**Урок 1.** Вступление. 3](#_Toc47868658)

[Исходная подготовка 5](#_Toc47868659)

[Установка, запуск, первоначальная настройка. 6](#_Toc47868660)

[Установка под Centos 8 8](#_Toc47868661)

[DNS сервер BIND 9](#_Toc47868662)

[**Урок 2. Диагностика и логгинг, настройка логгирования.** 9](#_Toc47868663)

[**Урок 3. Предварительная загрузка информацией.** 14](#_Toc47868664)

[Виды и соотношение директив userdb и passdb. 14](#_Toc47868665)

[Настройка директивы static. 15](#_Toc47868666)

[Настройка директивы **passwd-file.** 15](#_Toc47868667)

[**Настройка директивы LDAP** 16](#_Toc47868668)

[**Настройка директивы passdb – SQL (MySQL)** 16](#_Toc47868669)

[**Настройка директивы passdb – SQL (Sqlite)** 19](#_Toc47868670)

[Где и как хранится почта, форматы хранения писем 19](#_Toc47868671)

[Кооперация postfix и imap серверов и при чём тут LMTP. 21](#_Toc47868672)

[мастерпассвд 22](#_Toc47868673)

[**Урок 4. Построение минимальной рабочей конфигурации.** 22](#_Toc47868674)

[**Разбор типовых ошибок при построении минимальной конфигурации** 24](#_Toc47868675)

[Урок 5. Типовые задачи администрирования 25](#_Toc47868676)

[Восстановление писем, удалённых из корзины (аналог корзин 2-3 уровня эксченджа) 25](#_Toc47868677)

[pflogsumm – сборщик статистики из лога postfix 26](#_Toc47868678)

[logwatch – сборщик статистики вообще по всему 26](#_Toc47868679)

[imapsync – миграции,синхронизация двух ящиков на разных серверах 26](#_Toc47868680)

[Репликация между двумя серверами 27](#_Toc47868681)

[Транспортные правила. 28](#_Toc47868682)

[Пересылать письма, приходящие на несуществующие ящики на определенный 29](#_Toc47868683)

[SMTP и IMAP telent-сессии 29](#_Toc47868684)

[SMTP сессия без аутентификации или отправка первого письма 29](#_Toc47868685)

[SMTP сессия с аутентификацией PLAIN 30](#_Toc47868686)

[SMTP сессия с аутентификацией LOGIN. 30](#_Toc47868687)

[SMTP сессия с аутентификацией CRAM-MD5. 31](#_Toc47868688)

[SMTP сессия с аутентификацией NTLM. 31](#_Toc47868689)

[IMAP: чтение по через telnet 32](#_Toc47868690)

[**POP3: доступ к из командной строки через telnet (приём почты)** 33](#_Toc47868691)

[Перекодировщики бэйз 64 35](#_Toc47868692)

[gen-auth 36](#_Toc47868693)

[Команды администрирования postfix 36](#_Toc47868694)

[postfix - команда управления процессом master 36](#_Toc47868695)

[postconf – просмотр переменных настройки 37](#_Toc47868696)

[postqueue - команда управления очередями 37](#_Toc47868697)

[postsuper – управление задачами в очередях Postfix. 38](#_Toc47868698)

[postcat – посмотреть письмо 38](#_Toc47868699)

[newaliases 39](#_Toc47868700)

[postalias –создаёт cписки рассылки или запросы к ним 39](#_Toc47868701)

[postmap Команда администрирования 40](#_Toc47868702)

[Команды администрирования dovecot 40](#_Toc47868703)

[dovecot Команда администрирования 40](#_Toc47868704)

[doveadm Команда администрирования 40](#_Toc47868705)

[doveadm mailbox **list** –перечень папок 40](#_Toc47868706)

[doveadm mailbox status -размер, количество писем 41](#_Toc47868707)

[**doveadm mailbox create/delete/rename: работа с директориями внутри ящика, они же маилбоксы**. 41](#_Toc47868708)

[**doveadm mailbox subscribe/unsubscribe подписка на отображение** 41](#_Toc47868709)

[**doveadm search & fetch - поиск писем по ящикам и просмотр** 41](#_Toc47868710)

[**doveadm copy** & **move –** операции с ящиками: **копирование и перенос писем между ящиками** 43](#_Toc47868711)

[Индексы. 43](#_Toc47868712)

[doveconf – просмотр переменных настройки 43](#_Toc47868713)

[doveadm import, sync(ранее dsync), backup –экспорт/импорт, синхронизация, бэкап. 43](#_Toc47868714)

[doveadm pw – получение паролей разных видов 45](#_Toc47868715)

[doveadm user 46](#_Toc47868716)

[**doveadm auth – проверка заходов** 46](#_Toc47868717)

[**doveadm expunge – очистка папок в ящиках** 46](#_Toc47868718)

[**doveadm quota** 47](#_Toc47868719)

[**doveadm acl** 48](#_Toc47868720)

[doveadm replicator 48](#_Toc47868721)

[разгрести 48](#_Toc47868722)

[TLS, SSL, 49](#_Toc47868723)

[Проверка SMTP аутентификации через TLS. 50](#_Toc47868724)

[Отладка IMAP 51](#_Toc47868725)

[Отправка писем из командной строки 51](#_Toc47868726)

[Консольный email-клиент для windows blat 51](#_Toc47868727)

[Консольные email-отправлятор для linux mailx //доизучать 52](#_Toc47868728)

[Консольные email-просмотрщик для linux mutt 52](#_Toc47868729)

[Отправка email из Powershell 53](#_Toc47868730)

[Генератор большого количества писем 53](#_Toc47868731)

[master.cf 54](#_Toc47868732)

[Борьба со спамом: firewalld, iptables fail2ban: ловушки по логам dovecot, postfix. 55](#_Toc47868733)

[Борьба со спамом: длинные логины с точкой 56](#_Toc47868734)

[Борьба со спамом: проверки в самом Postfix 57](#_Toc47868735)

[Борьба со спамом: чёрный белый список. 57](#_Toc47868736)

[Борьба со спамом: сборка спам-фильтров Scrollout F1 58](#_Toc47868737)

[Борьба со спамом: сборка спам-фильтров Proxmox Mail Gateway 58](#_Toc47868738)

[DKIM 58](#_Toc47868739)

[SPF 59](#_Toc47868740)

[DMARC 60](#_Toc47868741)

[Готовые почтовики 60](#_Toc47868742)

[iRedMail. 60](#_Toc47868743)

[Mail-in-a-Box. 61](#_Toc47868744)

[Modoboa. 61](#_Toc47868745)

[Ubermail Stackfocus Ansible roles 61](#_Toc47868746)

[Ускорение и облегчение с помощью ViMbAdmin (vim-be-admin). 62](#_Toc47868747)

[Roundcube веб-интерфейс для лазанья по почте 64](#_Toc47868748)

[SquirrelMail веб-интерфейс для лазанья по почте 64](#_Toc47868749)

[Контакты давших хорошие ответы 64](#_Toc47868750)

[Рассмотреть: 65](#_Toc47868751)

[Разгрести: 68](#_Toc47868752)

[ACL 68](#_Toc47868753)

[Есть ли готовые докерные контейнеры 68](#_Toc47868754)

[EHLO 68](#_Toc47868755)

[DNS, MX, SPF, BIND 71](#_Toc47868756)

[postfix: замена поля from 72](#_Toc47868757)

[postfix: удаление заголовков 72](#_Toc47868758)

[Лимитирование трафика postfix 73](#_Toc47868759)

[Локальных реципиентов из базы: 76](#_Toc47868760)

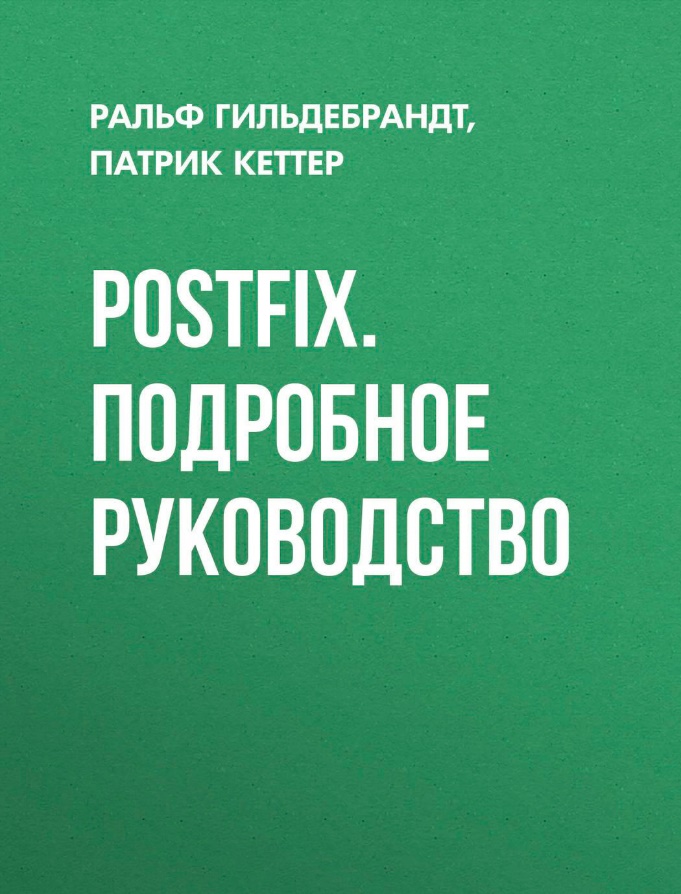
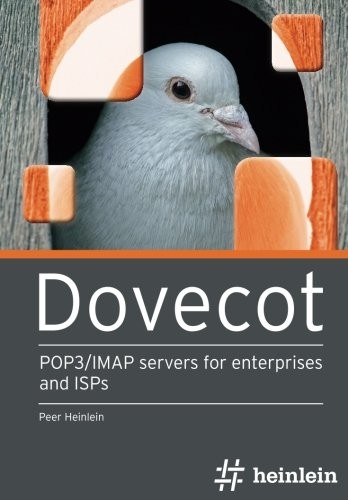
# **Урок 1.** Вступление.

Изучающих линукс надо поощрять, поэтому я и решил записать этот видеокурс. В погоне за девопсными зарплатами народ изучает, казалось бы, более важные стеки технологий забывая, что в основе основ и начале начал любой компании стоит даже не нагруженное веб приложение, а электронная почта. И я заметил, что даже к 2020 году видео по настройке почтовиков почти нету, а то что есть либо устарело, либо сложно и непонятно снято без объяснения что делается, зачем и на что влияет.

Переда нами стоит большая задача с кучей ветвящихся сложным образом параметров причем такая что я даже затрудняюсь сказать возможно ли её описать вообще полностью, начиная с азов и заканчивая антиспамами и так далее. Я хочу напомнить, что Вы можете смотреть на 1.1 -1.5 скорости если материал очередной главы вам известен. Если у вас мало опыта в работе с никс-системами, то почтовик на мой взгляд - прекрасная тема для старта, она неизбежно за собой потянет гигантский плат технологий необходимых на рынке труда. Этот курс является моим вольным переводом содержимого документации сайтов по довкоту и постфиксу которые вы наверняка уже читали, а также книг

Ральф Гильдебрандт, Патрик Кеттер **«Postfix. Подробное руководство»**

Heinlein Peer **«Dovecot: POP3/IMAP Servers for Enterprises and ISPs»**

Электронная почта исторически железобетонно встроилась в бизнес цепочки почти всех компаний. И несмотря на то что немалая часть общения людей ушла в мессенджеры, социальные сети, мессенджеры в мобильных телефонах и бог его знает ещё куда ещё сдавать позиции она не будет на долгую перспективу.

Хочу отметить что в москве, например, почти все конторы чтобы ну хоть как-то защититься от произвола госорганов диверсифицируют свою деятельность делая несколько юридических лиц. Либо занимаются перепродажей товаров производитель которых ставит обязательным условием сотрудничества –отсутствие продукции конкурентов: это например средства строительства или автомобили их производители не терпят другую продукцию даже рядом. Это приводит к тому что один человек на работе может работать с почтой нескольких доменов. Не смотря на то что, почтовики умеют обслуживать несколько доменов я бы крайне настойчиво советовал не класть все яйца в одну корзину, а сделать для каждого домена свой почтовик и спокойненько выводить их из работы на обслуживание по очереди, а не трястить над одним почтовиком где «лежит всё».

*Управляющий директор «Яндекса» Тигран Худавердян в разговоре с РБК на полях Петербургского экономического форума подтвердил, что решение по ключам шифрования, которые требует ФСБ,* ***найдено****.*

*Роскомнадзор на своем сайте объявил о разблокировке мессенджера Telegram на территории России. В ведомстве уточнили, что это произошло после согласования с Генеральной прокуратурой. Telegram был заблокирован на территории России весной 2018 года. Поводом стал отказ администрации мессенджера предоставить ФСБ ключи шифрования. С их помощью силовики могли бы получить доступ к переписке пользователей.*

[*http://www.lenty.ru/go.html?http://lenty.ru/cgi-bin/gop.cgi?https://www.svoboda.org/a/30792329.html@1842*](http://www.lenty.ru/go.html?http://lenty.ru/cgi-bin/gop.cgi?https://www.svoboda.org/a/30792329.html@1842)

*Данные с московских камер видеонаблюдения, оснащённых системой распознавания лиц, можно купить за 15 тысяч рублей, утверждают в общественной организации "Роскомсвобода". Волонтёр организации обратилась по соответствующему объявлению, опубликованному в даркнете, и получила от продавца отчёт с 79 камер с указанием всех адресов, где она была за месяц.*

*Ваши данные будут продавать.*

Есть разница когда устраиваясь на работу или рассматривая предложения мы видим у компании свой почтовый домен и другое дело когда почта на яндексе. Который к тому же явно представляет интерес и проверяющим органам и конкурентам, причём существую продажа или передача вашей информации первых вторым особенно на фоне последних новостей и рейдерских завхватов. Инфраструктуру надо держать за рубежом и иметь свою. Кроме того, почтовый сервер можно использовать для передачи крайне конфиденциальной информации, а если например настроить удаление писем с флагом просмотрено то можно получить аналог телеграма, где пришедшие сообщения со временим исчезают. Но телеграм мутная организация использующая непонятные протоколы, особенно на фоне того что к лету 2020 в рф его разблокировали а это значит что как и у Яндекса передача ключей для дешифрования всб –согласонвана. Здесь же Вы сами лично сможете контролировать процесс затирания сообщений по таймеру, надежность шифрования сообщений и затирания свободного места после них.

Показать таблицу распространенности ОС и почтовиков из вакансий чтобы обосновать выбор. Если взять несколько дней чтения вакансий по москве на зарплаты >100k и сделать греп по используемым технологиям то в разные времена у меня соотношение фронтендов плавало

|  |  |
| --- | --- |
| exim | 6 |
| postfix | 20 |

До

|  |  |  |  |
| --- | --- | --- | --- |
| exim | | 10 | |
| postfix | | 17 | |

Среди бэкэндов кроме довкота я в вакансиях приктически ничего не встречал. К слову сказать в одной из презентаций разработчиков довкот я нашел динамику в 2013 году 53% почтовиков было построено на довкот, а на 2020 уже почти 77%

<http://openemailsurvey.org/>

https://docplayer.net/9935441-Dovecot-overview-timo-sirainen-chief-architect-co-founder.html

У пира хайнлайна курс типа этого, но конечно более профессиональный указан внизу страницы как-то так:

Komplett-Paket 1.680,00 EUR zuzügl. 19% USt. (= 1.999,20 EUR brutto)

Schulung inkl. Unterrichtsmaterial/Buch; Unterbringung im Einzelzimmer, Mittag- und

Abendessen; Rahmenprogramm

Standard-Paket 1.500,00 EUR zuzügl. 19% USt. (= 1.785,00 EUR brutto)

Тема почтового сервера очень хорошо подойдёт начинающим изучать линукс как стартовая тема, которая неизбежно потянет за собой всё остальное. Можно прочесть много руководств по системе, но, когда видишь, как оно работает понимание приходит легче и быстрее. Мы в этом курсе пройдёи примерно полтора дерева настроек и параметров после чего я уверен дальше вы и сами без меня разберетёсь, а этот курс поможет Вам быстро стартануть в этом направлении увернувшись от ошибок и мест на которых я долго сам буксовал.

Кстати даже на форумах по почтовикам заметили что спама стало мало, наверное потому что рынок изменился. Раньше порнографиеских спамов много было а сейчас даже их нет, вообще не стало. Тоесть всё общение ушло в соцсети и мессенджеры и спам с рекламой ушли туда же. Я кстати и сам заметил что почти не пользуюсь почтой да и остальные знакомые похоже тоже. Тоесть все мои усилия по изучению почтовиков, как технологии уходящей в прошлое, как бы так сказать...

Что ещё хочу добавить. В процессе изучения настройки почтовиков у вас будут получаться промежуточные хорошие работающие конфигурации, потом вы зайдете в экспериментах дальше, потом запутаетесь где что правили, а где –нет и в конечном итоге станете, не зная что делать. Выход делать промежуточные копиии папок с файлами удачных конфигураций, но я, например, увлёкшись забывал это делать. Чтобы обойти эту проблему я рекомендую просмотрев этот курс потратить денек-другой на просмотр аналогичных по гит. Он позволит вам отматывать состояние конфигов назад и сэкономит дикое количество энергии и сил. Аналогично, после экспериемнтов еще неплохо делать снапшоты виртуальных машин с подробным комментарием среза времени.

Ещё одна просьба: по возможности везде персонифицировать переменные и прочие названия. Многие называют параметры словами похожими на ключевые команды конфигураций, например, внешний интерфейс называют wan учётную запись из-под которой производится чтение-запись почты – mail в результате у нового сотрудника либо новичка изучающего материал в голове получается адова каша, поэтому –персонифицируйте названия параметров конфигурации например

вместо имени файла /etc/dovecot/users лучше задавайте /etc/dovecot/ourcompanyusers,

вместо учётной записи mail делайте ourcompanymail

Очень сильно облегчит работу редактор с подсветкой синтаксиса, для последнего показать, как настраиваются цветовые схемы синтаксиса

## Исходная подготовка

Предлагается такой вариант освоения курса: не надо прям сразу за мной повторять, а сначала прослушайте его чтобы сформировалось понимание и уже после этого начинайте эксперименты.

Идём на сайт центоса, качаем исо 7 версии минимал, делаем виртуалку, задаём ей постоянный адрес, заходим по ссш, проверяем что на ней есть интернет, правильно установлено время и выключаем. Делаем снапшот, чтобы потом если потребуется не ставить ос заново.

*Отключаем SELinux*, .

***setenforce 0***

***sed -i "s/SELINUX=.\*/SELINUX=disabled/" /etc/selinux/config***

Отключаем фаерволл, его настройку сделаете потом, а сейчас он нам будет просто мешать

***chkconfig firewalld off***

здесь обязательно перегружаемся

Ставим вспомогательное ПО

***yum install -y telnet mc wget net-tools vim tree***

Объяснить два файла в одном ви.

предварительные знания,

listen= eth0,\*

первые проверки,

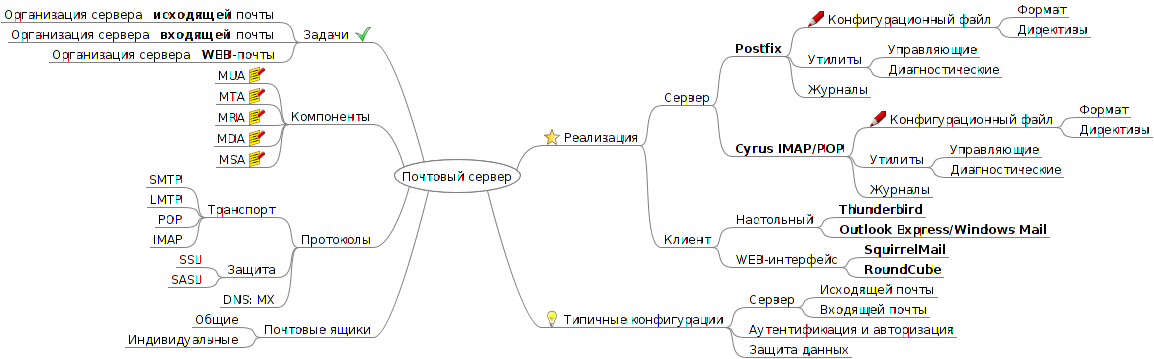
cat syslog и где смотреть логи

установка: как устроено что отдельные программы,

баннер как у эксченджа smtpd\_banner = text ($mail\_version) поискаь тут дату,

Сначала нужно чтобы A и MX, PTR, SFP записи вашего домена указывали на IP адреса ваших будущих почтовых серверов.

**hostname mail.sumare.ru**



## Установка, запуск, первоначальная настройка.

Для начала идём на сайты программ и смотрим какие там сейчас заявлены последние версии.

Смотрим сайт довекота, какая последняя версия там: 3.1

***yum repolist***

***yum info dovecot***

версии новой нет. Идём на <https://repo.dovecot.org/> читаем что там написано. Создаём файл

***vim /etc/yum.repos.d/dovecot.repo***

со следующим текстом:

[dovecot-2.3-latest]

name=Dovecot 2.3 CentOS $releasever - $basearch

baseurl=http://repo.dovecot.org/ce-2.3-latest/centos/$releasever/RPMS/$basearch

gpgkey=https://repo.dovecot.org/DOVECOT-REPO-GPG

**gpgcheck=0**

enabled=1

важно тут поменять gpgcheck=0 на 1 иначе потребуются дополнительные телодвижения, закрываем редактор, затем:

***yum install dovecot -y***

должна быть поставлена последняя версия, всё - довекот установлен, смотрим версию:

***dovecot --version***

Аналогично с postfix, в системе обычно старая версия смотрим какая есть:

***yum info postfix yum search postfix***

у меня показывает что установлена очень старая версия ещё 2.10.1 можно конечно попробовать

***yum update postfix***

идём на сайт постфикса, смотрим -там сейчас 3.2.4, 3.4.4 mail\_version = 3.5.2 удаляем старые версии:

***yum remove postfix***

yum remove ssmtp

yum remove sendmail

затем так же создаём файл описывающий репозиторий с постфиксом:

***vim /etc/yum.repos.d/gf.repo***

следующего содержания:

[gf]

name=Ghettoforge packages that won't overwrite core distro packages.

mirrorlist=http://mirrorlist.ghettoforge.org/el/7/gf/$basearch/mirrorlist

enabled=1

**gpgcheck=0**

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-gf.el7

failovermethod=priority

[gf-plus]

name=Ghettoforge packages that will overwrite core distro packages.

mirrorlist=http://mirrorlist.ghettoforge.org/el/7/plus/$basearch/mirrorlist

# Please read http://ghettoforge.org/index.php/Usage \*before\* enabling this repository!

enabled=1

**gpgcheck=0**

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-gf.el7

failovermethod=priority

gpgcheck=1 для учебного стенда не надо, оно нужно скажем так для проверки безопасности, Вам перед использованием этого репозитория надо будет скачать его ключ в виде фалй RPM-GPG-KEY-gf.el7 с Ghettoforge Key Page и сохранить по указанному выше в настройке репозитория пути /etc/pki/rpm-gpg/

**cd /etc/pki/rpm-gpg/**

**wget** [**http://mirror.ghettoforge.org/distributions/gf/RPM-GPG-KEY-gf.el7**](http://mirror.ghettoforge.org/distributions/gf/RPM-GPG-KEY-gf.el7)

В общем, теперь можно ставить последний постфикс:

***yum -y install postfix3***

yum -y install postfix3-pgsql.x86\_64

смотрим версию

**postconf -d | grep mail\_version**

rpm -ql postfix | grep bin/ посмотреть список бинарных файлов (подлежащих выполнению)

rpm -qd postfix список документации

добавляем сервисы в автозагрузку:

***systemctl enable dovecot***

***systemctl enable postfix***

Делаем резервную копию чистых конфигов:

***mkdir default\_confs && cp -R /etc/postfix/ ~/default\_confs && cp -R /etc/dovecot/ ~/default\_confs***

и запускаем:

***systemctl start dovecot***

***systemctl start postfix***

## установка из исходников

или же ставим из исходников, правда так будет дольше: идём на сайт <https://dovecot.org/> там выбираем самую верхнюю ссылку Released v2.3.5 переходим по ней там будут ссылки на исходник:

<https://www.dovecot.org/download>

***wget https://dovecot.org/releases/2.3/dovecot-2.3.5.tar.gz***

***ls***

***tar zxvf dovecot-2.3.5.tar.gz***

***ls -l***

***cd ./dovecot-2.3.5***

***ls -l***

***./configure***

***yum install gcc***

***./configure***

***make***

***mc***

***make install***

всё, довекот установлен, смотрим версию:

***dovecot --version***

2.3.5 (513208660)

2.3.10.1 (a3d0e1171)

при запуске ругнётся что нету конфигурации, её надо скопировать из примера, поставляющегося при установке, у меня он оказался в /usr/local/share/doc/dovecot, над их оттуда просто скопировать

**cp -r /usr/local/share/doc/dovecot/example-config/\* /usr/local/etc/dovecot/**

аналогично постфикс, качаем исходные тарболлы по ссылке

ftp://ftp.porcupine.org/mirrors/project-history/postfix/official/

wget <ftp://ftp.porcupine.org/mirrors/project-history/postfix/official/postfix-3.5.2.tar.gz>

***yum install gcc wget***

***tar zxvf***

читаем в каждом файл по установке, ставм

маке

## установка под Centos 8

Если сделать установку то версии пакетов у меня на 2020-07-23 получаются такие

postconf -d | grep mail\_version

mail\_version = 3.3.1

dovecot --version

2.3.8 (9df20d2db)

Однако на сайтах указано что на данный момент выпущены версии

June 27, 2020: Postfix stable release 3.5.4 and legacy releases 3.4.14, 3.3.12, 3.2.17.

Mon May 18 15:03:06 EEST 2020 Dovecot Released v2.3.10.1

затем так же создаём файл описывающий репозиторий с постфиксом:

**vim /etc/yum.repos.d/gf.repo**

следующего содержания:

[gf]

name=Ghettoforge packages that won't overwrite core distro packages.

mirrorlist=http://mirrorlist.ghettoforge.org/el/8/gf/x86\_64/mirrorlist

enabled=1

gpgcheck=0

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-gf.el7

failovermethod=priority

[gf-plus]

name=Ghettoforge packages that will overwrite core distro packages.

mirrorlist= http://mirrorlist.ghettoforge.org/el/8/plus/x86\_64/mirrorlist

# Please read http://ghettoforge.org/index.php/Usage \*before\* enabling this repository!

enabled=1

gpgcheck=0

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-gf.el7

failovermethod=priority

далее ставим, не забывая что третья версия постфикса:

**dnf install -y postfix3**

смотрим что поставилась версия посвежее:

postconf -d | grep mail\_version

mail\_version = 3.5.3

с довкотом аналогично бы, но пока нету под 8, как-то по-другому её надо ставить

## установка в ubuntu

apt install postfix postfix-mysql dovecot-core dovecot-imapd dovecot-pop3d dovecot-lmtpd dovecot-mysql

mariadb-client mariadb-server

потом переконфигурировать можно так:

dpkg-reconfigure postfix

## DNS сервер BIND

Делать стенд для изучения можно двумя путями: либо взять у любого хостера самую дешевую виртуальную машину скажем за 5 долл в месяц и использовать провайдерский днс чтобы ходила почта либо сначала все можно сделать на виртуальных машинах. Для того чтобы ходила почта надо сделать чтобы между тестовыми виртуалками нормально работал днс, тоесть правильно резолвились мх записи тестовых почтовиков //добавить статью по настройке

## **Отправка первого тестового сообщения**

В конце первогоурока надо делать тестовое сообщение, н анем потом показать куда упало письмо, мутт и потом объяснить лмпт

Тут надо сделать две отправки: в первой заголовок письма английскими буквами, второй русскими чтобы увидели как оно отображается через ключево слово utf8=

Домашнее задание – взять письмо из своей почты, вычитать все заголовки и загуглить значение, обратить внимание на From (без двоеточия) и From: (с двоеточием)

# **Урок 2. Диагностика и логгинг, настройка логгирования.**

Открыть таил –фэ при работе скрипта-рассылателя. Удивительная вещь но на форумах посвящённым проблемам почтовиков посты вида не работает почтовик, конфиг не покажу, логи не дам скажите что делать как починить –ну вообще не редкость. Правильно заданный вопрос это половина решения проблемы. Чтобы починить проблемный почтовик надо глубоко залезть в его внутренности, без этого наглухо, напрочь –понимание дальнейшей настройки просто невозможно. Этим мы и займёмся в этой главе.

Показать просмотр переменных работы через постконф и довадм как посмотреть переменные работы?

Сначала смотрим состояние самих служб: как они запустились, не обнаружилось ли в конфигах ошибок помешавших нормальному запуску:

***systemctl status postfix*** выдаст ошибки при запуске постфикса а так же версию!

***systemctl status postfix –l*** выдаст тоже, но полностью, все ошибки а не только последниие

***systemctl status dovecot***

***systemctl status dovecot –l***

посмотреть дерево дочерних процессов: qmgr и другие.

***ps xaf***

покажет процессы с параметрами запуска так же в виде дерева:

**ps axjf**

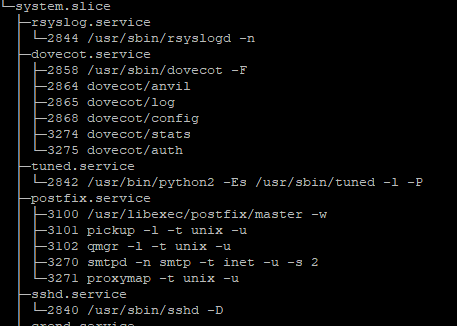
посмотреть из-под каких пользователей работают процессы постфикс

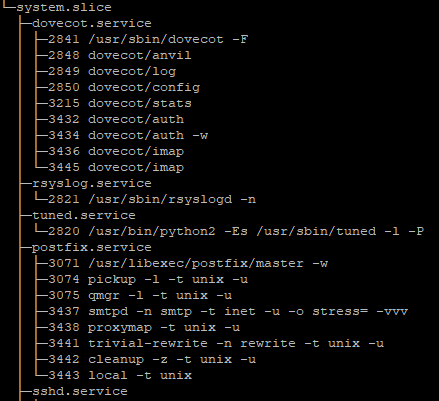
***ps axu***

а командой:

***systemd-cgls***

тоже покажет сервисы внутри самого постфикса или довекота в наглядном виде:





она тут показывает имя модуля в systemd, по которому можно смотреть журнал работы службы, например, так:

**journalctl \_SYSTEMD\_UNIT=postfix.service**

**journalctl \_SYSTEMD\_UNIT=dovecot.service**

кратенько по процессам:

dovecot

это сам основной процесс, следящий за запуском остальных

anvil

отслеживает клиентские подключения //пояснить

config

парсит файл конфигурации и передаёт настройки оттуда остальным процессам

auth

управляет всеми аутентификациями

'imap-login' and 'pop3-login

процессы пока пользователь не залогинился, управляют ссл подключений

'imap-login' and 'pop3-login

Уже занимаются польлзователем после того как он залогинился

посмотреть какой процесс на каких портах можно так (добавить команды-это все не поставлно) под убунту ставится apt install -y net-tools:

**netstat -plntu**

смотрим что процессы начали слушать порты так же и вот так:

***lsof -i4 -P –n***

возможно придётся поставить

***yum install lsof -y***

***sockstat -4 | grep dovecot***

Most daemon processes are short-lived and terminate voluntarily after serving max\_use clients, or after inactivity for max\_idle or more units of time.

Ставим телнет, ибо по умолчанию у меня в системе его не оказалось

**yum install -y telnet**

проверяем что почтовик отвечает по сети: делаем тестовое подключение телнетом-службы должны ответить:

***telnet 127.0.0.1 25***

***telnet 127.0.0.1 110***

вместо цифр 25 и 110 можно написать буквами smtp imap; для выхода для каждой набираем:

***quit***

перезапускаем оба

***systemctl restart dovecot && systemctl restart postfix***

оба процесса по дефолту пишут события в файл

/var/log/maillog

Но там этот файл не пересоздаётся при перезапуске этих служб, ибо в centos7 его ведёт отдельная служба rsyslogd:

***ps ax | grep sysl***

проверить это можно выполнив команду проверки syslog, которая добавит текст в кавычках в /var/log/maillog: это вообще хорошо делать после экспериментальной правки конфигов чтобы сразу видеть точку в логе после которой идет уже лог работы измененного конфига:

***logger -p mail.info "proverka"***

тоесть надо её перезапускать после удаления файла командой

***killall -1 rsyslogd***

**В минимал образе Centos8 вы возможно не найдете файл лога, чтобы он появился надо установить rsyslog командой перегружаемся и смотрим что файл лога появился и там начали накапливаться события работы почтового сервера // продемонстрировать** **Рсислог в 8 надо до ставить**

пока что проще делать так: удалять лог и тестовые письма и перегружать службы:

**rm -f /var/log/maillog && killall -1 rsyslogd && systemctl restart dovecot && systemctl restart postfix**

**грохнуть вместе с почтой:**

**rm -f /var/log/maillog && rm -f /var/mail/\* && killall -1 rsyslogd && systemctl restart dovecot && systemctl restart postfix**

буквально через какое-то время эта команда поломалась и что бы появилась команда killall в CentOS 7 необходимо установить psmisc.

***yum install psmisc***

После установки радуемся наличию killall. Команда killall в Linux предназначена для «убийства» всех процессов, имеющих одно и то же имя. Это удобно, так как нам не нужно знать PID процесса.

и затем:

***systemctl status postfix –l & systemctl status dovecot –l***

смотреть лог в соседней консоли лучше так (или через watch) у меня 35 строк-это почти высота экрана:

***clear && tail -F -n 35 /var/log/maillog***

Если в процессе дальнейшей настройки появятся проблемы, требующего детального понимания происходящего, то это надо отдельно донастроить в каждой программе - перевести журналирование в режим отладки:

1. Чтобы сделать компоненты Postfix SMTP server более разговорчивыми можно добавлять одну или несколько «**-v**" опций в конец конфигурационной записи демона в файле /etc/postfix/master.cf

smtp inet n - n - - smtpd -vvv

и затем выполнить

**postfix reload**

1. Если этого показалось недостаточно, то включим дебаггинг, например, именно со своим хостом, для начала узнаём с какого адреса с точки зрения почтовика мы залогинены:

w -i

получив адрес, прописываем его в файле

***vi/etc/postfix/main.cf***

в котором включаем дебаг для нашего хоста параметром  [debug\_peer\_list](http://www.postfix.org/postconf.5.html#debug_peer_list) :

debug\_peer\_list = 46.188.121.48

и задать так же уровень дебаггинга пира:

debug\_peer\_level = 2

потом понятное дело

***postfix reload***

vi /etc/postfix/master.cf

# Использовать более информативный заголовок процесса (отображается

# в команде ps). На данный момент отображаются только имя пользователя

# и IP адрес. Полезно, если вы хотите видеть кого на самом деле обслуживает

# IMAP процесс.

verbose\_proctitle = yes

Еще одним удобным способом посмотреть, что происходит во время SMTP-сессии, является директива debug\_peer\_list из файла main.cf. Глобально включать отладку всех SMTP-соединений было бы очень накладно, поэтому в нее стоит добавлять только список хостов, взаимодействие с которыми мы хотим отслеживать тщательнее, чем обычно. К примеру, для наблюдения за передачей писем между нами и yandex.ru, mail.ru, pochta.ru и 10.10.10.23 строка могла бы выглядеть вот так:

debug\_peer\_level = 2

debug\_peer\_list = yandex.ru, mail.ru pochta.ru 10.10.10.23/32 10.10.10.0/24

1. У dovecot это включается в файле

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

раскомментированием и включением директив:

auth\_verbose = yes Писать в лог о неудачных попытках входа и их причину.

auth\_verbose\_passwords = yes

auth\_debug = yes Выводить более информативные сообщения в лог. Так же пишутся запросы SQL.

auth\_debug\_passwords = yes

mail\_debug = yes

**doveadm reload**

4. Чтобы отобразить в логах процессы POP3 и IMAP в таком виде, чтобы были видны имена пользователей, IP адреса, SSL/TSL статус и выполненные команды IMAP, следует добавить в /etc/dovecot/dovecot.conf строку

verbose\_proctitle=yes

**doveadm reload**

Включите эти директивы по одной и сделайте отправку письма и перемещение по папкам ящика. Вам надо понять серию сообщений при нормальной работе. Удобно делать глядя в

**tail -F -n 35 /var/log/maillog**

В этом файле цифры в квадратных скобках –это номер процесса под которым работал конкретный экремпляр например smtpd[2364] в строке вида:

Nov 20 16:18:16 vps28780nl postfix/smtpd[2364]: resolve\_clnt: `reply@zilod.ru' -> `info@sumare.ru'

Тоесть он запустился с таким id, отработал и всю историю именно по этой smtp-сессии, именно с этим конкретным почтовиком или клиентом вы можете просто посмотреть грепом:

**cat /var/log/maillog | grep '2364'**

Здесь сделать телнетом сессию и показать, как он на это отреагировал.

В дальнейшем, чтобы понять какие данные получает почтовик и как он на них реагирует можно записать трафик приходящий на него: записывать весь трафик кроме ssh:

**tcpdump 'host 46.63.226.106 and tcp port !22' -w 0002.pcap**

полученый файл открыть wairshark-om //показать в ролике команды

В клиентах Sylpheed и Claws-mail есть детальный лог диалога с сервером. Попробуйте через них и скиньте сюда этот лог.//показать

в мастер.цф сключать разговорчивость анвил или лмтп

посмотреть куда довкот пишет логи:

**doveadm log find**

посмотреть историю версий, чейджлоги

**rpm -qa |sort**

**rpm -q --changelog dovecot-2.3.8-4.x86\_64**

**rpm -q --changelog postfix3-mysql-3.4.7-1.gf.el7.x86\_64**

Домашнее задание сделать тестовые отправки при разном уровне логирования

netstat -antp покажет что порты слушаются,

cat syslog и где смотреть логи, показать таил при отправке с внешнего почтовика

# **Урок 3. Предварительная загрузка информацией.**

Перед правкой файла-скопируй его

Для первоначальной настройки, построения минимально возможной рабочей конфигурации необходимо рассказать следующее: для самого минимального работающего полноценного почтовика надо сделать две вещи:

* + - 1. настроить между двумя программами хранение передачу писем, и
      2. настроить аутентификацию.

- аутентификация сначала заходим в довкот, делая тестовую аймап сессию, рассказать, что тег команды нужен чтобы различать их когда клиент переконнектится и передает массу оффлайн операций, показываем проверку через раздел **doveadm auth**

-где-то сюда впихнуть auth\_default\_realm = и преобразующий ДО передачи процессу аутентификации auth\_username\_format = %Lu

-делаем тестовую отправку, показываю куда письмо упало, делаю второе письмо но с темой на русской раскладке. Дать домашним заданием повторить тоже самое делая разные вербосити процессов, сказать пока что цель не разобрать вывод лога полностью а привыкнуть какая пачка сообщений соответствует нормальной отправке-получению в этой этих версих п/о;

- напоминить что если Вам не понятен тот или иной параметр настройки задайте себе мысленно вопрос: **на каком этапе SMTP сессии это должно происходить?**

-форматы хранения почтовых ящиков: блокировки, индексы, дополнительные данные Форматы файлов трее, квадратом,

- потом прикручиваем к нему постфикс через сокет аутентификации и Постфикс умеет делать аутентификацию пользователей двумя способами cyrus и dovecot:

postconf -a

-сделать второй квадрат с созданными внутри маилбоксов подпапками и папкими на уровне, среди самих маилбоксов, чтобы объяснить разделитель

## Виды и соотношение директив userdb и passdb.

В Dovecot все запросы о учётной записи пользователя разделяются на две категории (показать диаграмму захода на аймап сервер из книжки):

* passdb запросы, используются для аутентификации пользователя: логин, пароль, могут так же предоставлять дополнительную **pre-login информацию** необходимую для пользователя как например какой сервер дальше будет использоваться для проксирования (на больших бэкэндах с Dovecot director) или имеет ли пользователь право залогиниться (не выключен ли) и т.п.
* userdb запросы, выдающие **post-login информацию**, такую как где находится папка с почтой пользователя, лимит квоты, другие параметры пользователя (User database extra fields), перезаписывающие собой дефолтные на весь почтовик

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **passdb \** userdb | static | passwd | sql | ldap | prefetch | lua | nss | VPopMail |
| static | + |  |  |  |  |  |  |  |
| passwd-file |  |  |  |  |  |  |  |  |
| sql |  |  |  |  |  |  |  |  |
| ldap |  |  |  |  |  |  |  |  |
| PAM |  |  |  |  |  |  |  |  |
| BSDAuth |  |  |  |  |  |  |  |  |
| checkpassword |  |  |  |  |  |  |  |  |
| IMAP |  |  |  |  |  |  |  |  |
| shadow |  |  |  |  |  |  |  |  |
| VPopMail |  |  |  |  |  |  |  |  |
| oauth2 |  |  |  |  | dict |  |  |  |
| lua |  |  |  |  |  |  |  |  |

Так как эти директивы лежат в разных файлах, чтобы не запутаться смотрите окончательный результирующий конфиг

**doveconf -n**

или чтобы он показал и пароли то

**doveconf -nP**

userdb может содержать так же в аргс параметр acl\_groups который оторое содержит все группы, к которым принадлежит пользователь

Рассказать про выключение негативного кеширования auth\_cache\_negative\_ttl = 1 hours

### Простое использование пользоветельских учёток заводимых в саму ос

Оно включено по-умолчанию в дефолтном конфиге правда там есть нюанс: в /etc/passwd не содержатся доменная часть почтового ящика и тут нам надо знать про параметры

auth\_default\_realm = и преобразующий ДО передачи процессу аутентификации auth\_username\_format = %Lu

просьба не путать их с mydomain и myoridin postfixa. Недостатки сего метода в том что надо заводить пользователей в систему, а их можно завести всего 65тыщ штук это раз, второе то что пароли в /etc/shadow хранятся в хешированом виде что не дает использовать другие методы аутентификации типа cram-md5, если Вы не поняли что я сейчас сказал то не волнуйтесь, в следующие уроке это будет объяснено.

### Настройка директивы static.

Следующие две директивы задают, где и как Dovecot будет искать имена и пароли пользователей. Владельцем папки с почтой должен быть mail:

passdb {

driver = static

args = password=sumarepassword

}

userdb {

driver = static

args = uid=mail gid=mail #home=/var/vmail/%u

}

userdb {

driver = static

args = uid=5000 gid=5000 home=/var/vmail/%d/%n allow\_all\_users=yes

}

The “allow\_all\_users=yes” setting means that it is not necessary for Dovecot to check if a certain user exists. We can do that because Postfix has already ensured (in the virtual\_mailbox\_maps query) that the users existed before their email was handed over to Dovecot’s “deliver” agent.

### Настройка директивы **passwd-file.**

Внизу файла настроек postfix раскомментируем строку

!include auth-passwdfile.conf.ext

Он лежит в подпапочке, открываем его

**vim /etc/dovecot/conf.d/auth-passwdfile.conf.ext**

*passdb {*

*driver = passwd-file*

*args = scheme=SHA256-CRYPT username\_format=%u /etc/dovecot/users*

*}*

*userdb {*

*driver = passwd-file*

*args = username\_format=%u /etc/dovecot/users*

*}*

Мы использовали для этого файл, /etc/dovecot/users, имеющий формат стандартного файла паролей /etc/passwd. Пример файла паролей (пароль обрезан):

*zakaz@sumare.ru:{SSHA512}2YT51xuhilbvb4vYRIb1oj1EvrKFszhf2MNw=::::::*

*info@sumare.ru:{SSHA512}GdBv9GEE1rfFpd4+fzXS+UKh4x6gTpTaH4=::::::*

Для безопасности, мы не храним пароли пользователей в открытом виде, а храним их подсоленные SHA512. Для заполнения файла «/etc/dovecot/users» ручками для обучения

**echo zakaz@sumare.ru:$(doveadm pw -s CRYPT -p password):::::: >> /etc/dovecot/users**

Для безопасности, мы не храним пароли пользователей в открытом виде, а храним их подсоленные SHA512. Для заполнения файла «/etc/dovecot/users» будем использовать этот скрипт с двумя параметрами, именем пользователя и паролем пользователя.

#!/bin/sh

echo $1:$(doveadm pw -s ssha512 -p $2):::::: >> /etc/dovecot/users

Показать, что команда выдаёт каждый раз разные хеши тоесть разные пользователи, имеющие одиаковый пароль, будут иметь различающиеся хеши:

**doveadm pw -s ssha256 -p sumarepassword**

Если не указывать scheme=SHA256-CRYPT то подразумевается что пароль указан прямым текстомCRYPT

*timo@example.com:{PLAIN}hello123::::::*

*dave@example.com:{PLAIN}world234::::::*

для нескольких доменов файловую пассдб можно задать так, здесь **процент дэ** внутренняя переменная довкота означающая доменную часть имени:

*passdb {*

*driver = passwd-file*

*# Each domain has a separate passwd-file:*

*args = /etc/auth****/%d****/passwd*

перезапускаем оба

***systemctl restart dovecot && systemctl restart postfix***

Если у вас больше одного сервера то вместо копирования новой версии файла на остальные можно раздавать его сразу на все с помощью, например, ансибль

### **Настройка директивы LDAP**

Запрашивать данные пользователя из LDAP довкот может двумя путями

Password lookups (dovecot заходит в LDAP как пользователь proxy user и дальше читает данные учётной записи)

Аутентификация из LDAP

Authentication binds (dovecot сам логинится указаными логиноми паролем-это метод работы с Active Directory и допускаются только PLAIN, LOGIN)

[AuthDatabase.LDAP.txt] тут можно делать как запросы паролей, так и остальные пользовательские данные, поэтому отмечено тоже зеленым, для LDAP база проверки паролей прописывается так (сначала активируем использование конфига лдапа):

passdb {

driver = ldap

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

}

userdb {

driver = ldap

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

# Default fields can be used to specify defaults that LDAP may override

#default\_fields = home=/home/virtual/%u

}

Добавляем в павершелл модуль для работы с AD

**import-module activedirectory**

**Get-aduser -Filter \* -Properties \* | Where-Object { $\_.SamAccountName -eq "shabanov" } | FT name, enabled**

Рассказать о переборах паролей со словарем, пример выборки паролей, что через почтовик можно перебирать пароли доменных пользователей.

LdapAdmin

ASDIeditor

Ldapsearch

### **Настройка директивы passdb – SQL (MySQL)**

Для понимания работы сборок почтовиков, которые будут в курсе далее надо научиться понимать настройку получения параметров пользователей из SQL [AuthDatabase.SQL.txt]: PostgreSQL, MySQL, SQLite. для SQL форма хранящегося пароля задаётся в параметре default\_pass\_scheme = MD5 в файле конфигурации подключения к БД, указываемом произвольно после args = либо в самом файле куда указывают аргс:

passdb {

driver = sql

args = /etc/dovecot/sumare-dovecot-sql.conf

}

userdb {

driver = sql

args = /etc/dovecot/dovecot-sql.conf.ext

}

Рассказать про путаницу в файлах. Итак, при работе с сиквелом эти две директивы должны выполнить password\_query userdb\_query соотвественно. При первом понятное дело из базы извлекается пароль для дальнейшего сравнения, а вторая достаёт остальные, или «пост-логин» данные учётной записи.

***mysql -uroot –p***

***!CNSadm159!#***

***ALTER USER 'root'@'localhost' IDENTIFIED BY 'SintGi\_024';***

Создаём базу:

**create database sumare;**

**show databases;**

**use sumare;**

SQL -команды для создания таблицы, названия полей, типы данных и их длина -все это указано в файле AuthDatabase.SQL.txt (а был на digitalocean пример с автоинкрементом ):

CREATE TABLE users (

userid VARCHAR(128) NOT NULL, //унике надо

domain VARCHAR(128) NOT NULL, //а здесь –сет, для многодоменных почтовиков

password VARCHAR(128) NOT NULL, //было 64 но тогда мд2 пароли не влезут DESCRIBE users;

home VARCHAR(255) NOT NULL,

uid INTEGER NOT NULL,

gid INTEGER NOT NULL,

active char(1) DEFAULT 'Y'

);

//это всё ебала так как вызовет путаницу ибо там, в руководстве, не хватает поля что юзер активен. Тоесть надо его добавить:

**DESCRIBE users;**

**ALTER TABLE users ADD active char(1) DEFAULT 'Y';**

**ALTER TABLE users MODIFY COLUMN password varchar(128);**

**DESCRIBE users;**

чтобы вставлялась строка указывающая путь к ящику надо делать конкатенацию строк как показано тут а не писать процент эн:

**INSERT INTO users VALUES('margo', 'sumare.ru', 'sumarepassword', CONCAT('/sumarepochta/',userid), 8, 12, 'Y');**

update users SET home=CONCAT('/sumarepochta/',userid) where userid='asat'; //juntar essas duas

INSERT INTO virtual\_users (id, domain\_id, user, password) VALUES (1, 1, 'john', MD5('johnpasswd'));

update users SET active='N' where userid='asat';

select \* from users order by active;

doveadm pw -s md5 -p sumarepassword

Примеры настройки из рабочих конфигов:

driver = mysql

connect = host=localhost dbname=mail user=postfix password=password

default\_pass\_scheme = MD5

user\_query = SELECT '/var/spool/mail/%d/%n' as home, 'maildir:/var/spool/mail/%d/%n'as mail, 1150 AS uid, 12 AS gid, concat('dirsize:storage=', quota) AS quota FROM mailbox WHERE username = '%u' AND active = '1'

password\_query = SELECT username as user, password, '/var/spool/mail/%d/%n' as userdb\_home, 'maildir:/var/spool/mail/%d/%n' as userdb\_mail, 1150 as userdb\_uid, 12 asuserdb\_gid FROM mailbox WHERE username = '%u' AND active = '1'

driver = mysql

default\_pass\_scheme = CRAM-MD5

#connect = host=127.0.0.1 port=3306 dbname=sumare user=root password=gOU091HEF9bnfsf6FGV0H8tFEKL0oR

connect = host=/var/run/mysqld/mysqld.sock dbname=sumare user=root password=**!CNSadm159!#**

# Required by doveadm tools which require to list all mail users.

iterate\_query = SELECT username AS user FROM mailbox

password\_query = SELECT mailbox.password, mailbox.allow\_nets \

FROM mailbox,domain \

WHERE mailbox.username='%u' \

AND mailbox.`enable%Ls%Lc`=1 \

AND mailbox.active=1 \

AND mailbox.domain=domain.domain \

AND domain.backupmx=0 \

AND domain.active=1

user\_query = SELECT home, uid, gid FROM users WHERE userid = '%n' AND domain =

'%d'

Или вот, более правильно и сложно:

user\_query = SELECT \

LOWER('%u') AS master\_user, \

LOWER(CONCAT(mailbox.storagebasedirectory, '/', mailbox.storagenode, '/', mailbox.maildir)) AS home, \

CONCAT(mailbox.mailboxformat, ':~/', mailbox.mailboxfolder, '/') AS mail, \

CONCAT('\*:bytes=', mailbox.quota\*1048576) AS quota\_rule \

FROM mailbox,domain \

WHERE mailbox.username='%u' \

AND mailbox.`enable%Ls%Lc`=1 \

AND mailbox.active=1 \

AND mailbox.domain=domain.domain \

AND domain.backupmx=0 \

AND domain.active=1

We need to ensure that Postfix finds your domain, so we need to test it with the following command. If it is successful, it should returns 1:

**postmap -q example.com mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf**

**Prefetch Userdb**

**Эта директива означает что**

Значит тут есть один подляк: если ругается что

dovecot: auth: Fatal: sql: Unknown database driver 'mysql'

и некоторые умники советуют заменить на driver = sql и тоже будет отваливаться с той же ошибкой и даже если

dovecot --build-options

Build options: ioloop=epoll notify=inotify openssl io\_block\_size=8192

SQL driver plugins**: mysql** postgresql sqlite

Passdb: checkpassword ldap pam passwd passwd-file shadow sql

Userdb: checkpassword ldap(plugin) passwd prefetch passwd-file sql

Надо доставить

**yum install dovecot-mysql**

а так же поменять пользователю из-под которого коннектится довкот к БД схему паролей:

ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql\_native\_password BY 'SintGi\_024';

systemctl restart mysqld && systemctl restart dovecot

после этого проверяем что данные из БД довкот начал забирать:

**doveadm user margo**

**doveadm auth test -x service=smtp -x rip=127.0.0.1** [**asat@sumare.ru**](mailto:asat@sumare.ru)

### **Настройка директивы passdb – SQL (Sqlite)**

driver = sqlite

connect = /home/user-data/mail/users.sqlite

пароли должный иметь одинаковую схему хранения получаемую из "doveadm pw", если для како-то пароля используете не дефолтную то она должна быть с приставкой в фигурных скобках например "{plain}plaintext-password"

default\_pass\_scheme = SHA512-CRYPT

запрос-параметр 'password\_query' содержит SQL запрос возвращающий пароль: он должен возвращать поле с именем "password". Если оно у вас называется по-другому поменяйте её sql-директивой AS:

password\_query = SELECT email as user, password FROM users WHERE email='%u';

user\_query = SELECT email AS username, "mail" as uid, "mail" as gid, "/home/user-data/mail/mailboxes/%d/%n" as home FROM users WHERE email='%u';

iterate\_query = SELECT email AS user FROM users;

## Где и как хранится почта, форматы хранения писем

Dovecot имеет два понятия отонсящихся к месту хранения почты: сама папка с почтой и домашняя папка пользователя, которую можно потом подставлять ка ктильду ~ не путайте с домашней папкой пользователя линуск

mail\_home=/srv/mail/%Lu

mail\_location=sdbox:~/Mail

mail\_location=sdbox:%h/Mail

одно из них это непосредственно хранятся сами пиьма второе указывает место где будет храниться остальная относящаяся к почтовому ящику информация:

-файлы блокировок — это когда постфикс и довкот работают с ящиком или когда с одним ящиком рабоает группа пользователей, или один пользователь с разных устройств.

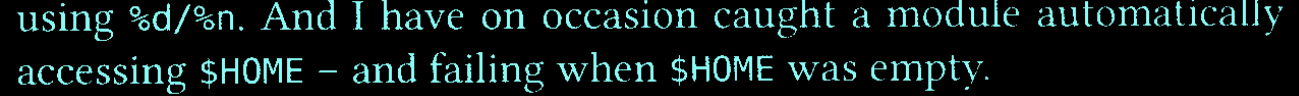
-индексы,

подписки на отображение папок,

логи состояния именно этого ящика операции

- соотношения уид –имя файла так как аймап требует чтобы каждое письмо имело свой уид

и т.п.



Рассказать про подпапки в ящиках (на одном уровне с входящими, внутри папок русскими и англ буквами показать), индексы, то где хранить индексы, что с ниьи делать при переименовании папок и т.д.

Почту dovecot ищет последовательно в трех перекрывающихся местах:

-заданое параметром mail\_location в dovecot.conf если ничего другого не задано что его перекрывает;

-mail userdb поле, которое перекрывает вышеуказанное mail\_location;

-location пареметр внутри namespaces перекрывает всё остальное. Обычно должениспользоваться только для public и shared namespaces.

Autodetection. По умолчанию mail\_location не задано и в этом случае Dovecot пытается найти автоматически где же может храниться ваша почта, он просматривает следующие расположения в следующем порядке:

~/mdbox/

~/sdbox/

~/Maildir/

~/mail/.imap/

~/mail/inbox

~/mail/mbox

~/Mail/.imap/

~/Mail/inbox

~/Mail/mbox

Когда autodetection работает, хотя бы одно из указаных расположений должно быть заполнено. Когда autodetection активно, Dovecot не будет пытаться создавать папку для почты. Внимание: .imap это папка, а inbox и mbox это файлы.

Хорошая практика явно задавать место хранения почты, даже если autodetection срабатывает, in particular to benefit from auto-creation of the folder for new users. Вторая версия делает автокриэйшн только если mail\_location задан корректно и Mail/.imap будет создана при этом. Это признак что что новый пользователь правильно настроен в довкот.

Экспериментируем с форматами хранения почты, конвертируем.

Форматы хранения писем в разных программах используются разные: dbox, maildir и поэтому, как хотелось бы вот просто взять и скопировать в файловой системе письма скажем из очереди в imap папку входящие нельзя. Для межпроцессного взаимодействия и придуман протокол LMTP, он очень прост к пониманию ибо повторяет SMTP.

LMTP = протокол межпроцесной передачи писем внутри сервера (забудьте корявое протокол локальной доставки).

Тут была идея криптед хранилища почты: надо 2 вм, одна отправлятор, вторая довекот на криптодиске

<https://bitlair.nl/Projects/Mailserver_with_Debian,_Exim,_spamassassin,_greylistd,_DKIM,_SRS,_SPF,_DMARC,_forwarding,_LDAP,_dovecot,_LMTP,_disk_crypto#MTA_.2B_Encrypted_mail_store>

**mbox**

Всё хранится одним текстовым файлом, насколько я понял если например у вас 1 ГБ ящик и вы поудаляли из середины письма то по выходу –файл перезаписывается заново целиком.

**maildir**

тут по-другому, каждое письмо — это отдельный текстовый файл, можно оперировать с отдельными письмами. Недостаток в том что в файловой системе накапливается куча папок с множеством мелких файлов

**sdbox**

свой более быстрый формат довкота, одно письмо-один файл

mail\_location = sdbox:~/dbox

**mdbox**

оно же, но несколько писем на одно письмо

mail\_location = mdbox:~/mdbox

**cydir**

ещё один формат, одно письмо-один файл с именем-уидом письма

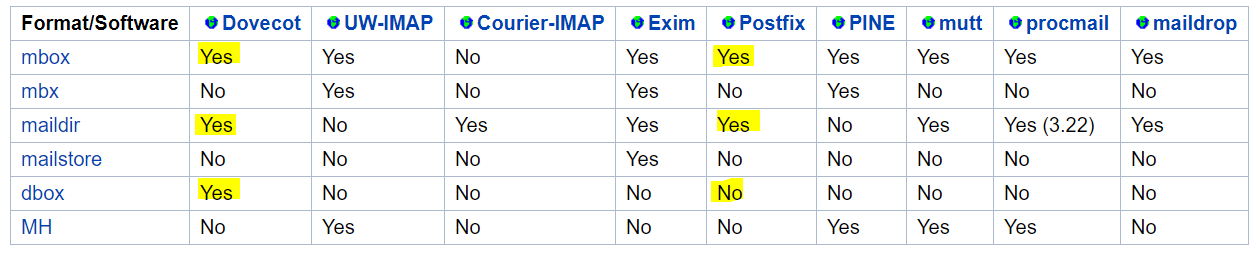
sdbox and mdbox support saving mail attachments to external files, which also allows single instance storage for them. Other backends don't suppor this for now.

**Домашнее задание:**

**В почтовом клиенте создайте новую папку и посмотреть как она выглядит в файловой системе: в ящике сверху, скопированая в папку входящие и т.д. Смените формат хранения почты на другой и повторите. Перепробуйте все форматы хранения почты. Поменяйте делимитер фс-маилдир++, посмотрите отличия, сделайте подпапки на русском, посмотрите как это выглыдит в мете хранения почты.**

## Кооперация postfix и imap серверов и при чём тут LMTP.

При взаимодействии двух разных программ перечень вопросов начинается с форматов хранения почты и блокировок при работе с ящиками и папками. В документации dovecot есть вот такая таблица поддерживаемых форматов храния почты:



объяснение работы лучше сделать

При демонстрации работы LMTP высылать пачки писем с помощью MultiMail2.exe -ибо лог пачки однотипных сообщений сообщений легко читается, сразу видны отличия.

и настройка: сначала говорим постфиксу передавать в сокет:

**vim /etc/postfix/main.cf**

раскомментируем

mailbox\_transport = lmtp:unix:private/dovecot-lmtp

затем включаем сам протокол и отслеживание сокета:

**vim /etc/dovecot/dovecot.conf**

protocols = imap pop3 **lmtp** submission

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

service lmtp {

unix\_listener /var/spool/postfix/private/dovecot-lmtp {

group = postfix

mode = 0600

user = postfix

}

}

в маил плагинс убираем сиев, оставляем только квота иначе почему-то не работало, потом разберусь:

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

protocol lmtp {

# # Space separated list of plugins to load (default is global mail\_plugins).

# #mail\_plugins = $mail\_plugins

mail\_plugins = quota

}

при настройке LMTP если получаем собщение

lmtp(4795): Error: Failed to lookup user

это значит что довкоту надо давать имя

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

вот так:

auth\_username\_format = %n

а, еще ставим права на хоум папку а то при приходе первого письма в ящик который еще не использовался довкот будет ругаться, впрочем не пугайтесь, если довкот не может создать ящик то постфикс будет держать письмо в очередях, :

**chmod 777 /home**

делаем волшебную команду:

**rm -f /var/log/maillog & rm -fR /var/mail/\* & killall -1 rsyslogd & systemctl restart dovecot & systemctl restart postfix & systemctl status postfix –l & systemctl status dovecot –l**

проверяем что, например, если задать сдбокс то постфикс не кладёт больше письма в /var/spool/mail а передает их довкоту.

в мастер.цф сключать разговорчивость анвил или лмтп

## мастерпассвд

# **Урок 4. Построение минимальной рабочей конфигурации.**

Конфигурационные файлы довкота составлены таким образом что дописывать особо и не надо – вы просто находите и раскомментируете нужный вам параметр или плагин. У довкота есть многострочные параметры и поэтому конфигурировать его как постфикс командами в отдну строку не получится.

показать отправку на несуществующий ящик

- памятка дерева параметров, которые меняют в начале.

|  |  |
| --- | --- |
| **Принимаемые домены и сетевые параметры**  **vim /etc/postfix/main.cf**  myhostname = mail.sumare.ru  mydomain = sumare.ru  myorigin = $mydomain или myorigin = sumare.ru  mydestination = $mydomain  инет интерфейсес иначе не пустит  inet\_interfaces = all  inet\_protocols = ipv4  этот параметр надо выключить потом, когда разберетесь в аутентификации.  mynetworks = 192.168.2.0/24, 127.0.0.0/8 | Аутентификация |
| Форматы хранения почты и служебной информации | передача писем и аутентификационных данных между программами  **vim /etc/postfix/main.cf**  smtpd\_sasl\_type = dovecot  smtpd\_sasl\_path = private/auth  smtpd\_sasl\_auth\_enable = yes  smtpd\_relay\_restrictions = permit\_mynetworks, permit\_sasl\_authenticated, reject\_unauth\_destination  broken\_sasl\_auth\_clients = yes  затем включаем сокет через который довкот будет отдавать постфиксу аутентификацию, приводим вот к такому виду:  ***vim /etc/dovecot/conf.d/10-master.conf***  *service auth {*  *...*  ***#unix\_listener auth-userdb*** *{*  *#mode = 0666*  *#user =*  *#group =*  ***#}***  *unix\_listener /var/spool/postfix/private/auth {*  *mode = 0660*  *# Assuming the default Postfix user and group*  *user = postfix*  *group = postfix*  *}*  *...*  *}* |

сейчас постфиск будет складывать почту в место, указанное параметром (раскомментировать)

mail\_spool\_directory = /var/spool/mail

mynetworks подразумевает под собой сети, т.е. правильно писать не просто ip, а 217.24.183.22/32

По дефолту у постфикса указан максимальный размер ящика mailbox\_size\_limit = 51200000, что означает когда ящик вырастет до 50 мегабайт у вас перестанет приниматься почта с сообщением о переполнении ящика. Выключить это можно задав mailbox\_size\_limit = 0 этот параметр надо прописать в файле, его там нет так как он дефолтный

и здесь же подключим чтобы постфикс делал аутентификацию через довекот, добавив в самый низ эти строчки:

я однажды пропустил вторую и потратил немало сил чтобы понять почему ничего не работает. Сокет там указан странно потому что он может быть задан как полным путём, так и относительным в папке очередей postconf queue\_directory

Далее в довекоте указываем что надо общаться с постфиксом через сокет, оттуда будут приходить запросы на аутентификацию пользователей:

**vim /etc/dovecot/dovecot.conf**

*login\_greeting = mailer1.sumare.ru Dovecot ready*

майлер1 здесь для того чтобы потом, когда будем делать кластер реплицирующийся мастер-мастер мы понимали на какой почтовик нас закинуло.

В нём же комментируем строку И соответствующую ей закрывающуюся скобку Кстати Postfix и Dovecot могут быть установлены вообще на разные сервера и можно настроить всё это дело через tcp/ip. далее довекот ругается что неправильно задана пассдб

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

*в нём задаём*

*disable\_plaintext\_auth = no*

*auth\_cache\_size = 0*

этот кеш надо для обучения выключить, иначе пока вы будете экспериментировать и перечитывать конфиг у вас будут кэшироваться старые неправильные результаты аутентификаций и незнание этого вас серьёзно тормознёт

*auth\_mechanisms = plain*

остальные механизмы передачи паролей добавим потом, цель обучения-научиться отлаживать аутентификацию на одном механизме, а потом, когда проясниться-можно задействовать и остальные

далее надо указать базы откуда берутся настройки пользователей, их много и это мы будем делать следующие занятия раскомментируя их все по очереди. Для начала саму базу возьмём самую простую -статик, которая пускает всех пользователей с одним и тем же паролем (она именно для целей обучения и отладки и придумана) и зададим ее в самый низ файла:

раскомментируем

!include auth-static.conf.ext

Далее открываем файл настройки этой базы, раскомментируем нижние директивы

**vim /etc/dovecot/conf.d/auth-static.conf.ext**

и донастроим к вот такому образу:

*passdb {*

*driver = static*

*args = password=sumarepassword Сменить перед выдачей курса*

*}*

*userdb {*

*driver = static*

*args = uid=mail gid=mail*

*}*

Наиболее частый вопрос а где хранится собственно почта? Хранится она там где Вы это укажите. Но перед тем как сконфигурировать место хранения почты надо знать особенности настройки этогих параметров ибо из-за этого может быть очень много непониманий почему довкот собственно ругается. Экспериментировать с расположениями почты и правами на папки начнём c раскомментирования в файле

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

строчки

You need to create group vmail and user vmail.

---%<-------------------------------------------------------------------------

mail\_home=/srv/mail/%Lu

mail\_location=sdbox:~/Mail

## this is sometimes needed

#first\_valid\_uid = uid-of-vmail-user

mail\_location = maildir:~/Maildir

Хочу обратить внимание что путь указан для пользователя который заведен в самой линуск и с домашней папкой

mail\_location = mbox:~/mail:INBOX=/var/mail/%u

Зададим в самой операционной системе пару пользователей: создать с домашней папкой, иначе не зайдет и некуда складывать будет почту

***useradd sumarepochta -m***

***mkdir /sumarepochta***

***попробовать вот такой вариант учётки чтобы не могли заходить на сам почтовик***

***useradd great -m -s /sbin/nologin***

следующие цифры доступа в папке с почтой –12 это guid группы mail

first\_valid\_uid = 8

last\_valid\_uid = 2000

first\_valid\_gid = 12

last\_valid\_gid = 2000

mail\_access\_groups = mail???

Если сейчас попытаться зайти по поп3 то доввекот будет ругаться на недостаток прав, с этим разберемся потом

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

lda\_mailbox\_autocreate = yes

smtpd\_helo\_required = yes

*и меняем права на папку с почтой:*

**chown -R mail:mail /var/mail/**

**chmod 0600 /var/mail/\***

**chown -R sumarepochta:sumarepochta /sumarepochta/sumarepublic/**

**chmod -R 777 /sumarepochta/sumarepublic/**

а на 152 странице 750 права, там же настройка прав так чтобы довкот не мог писать в несмонтированную папку

а, ещё надо добавить пользователя в группу mail, иначе будет ругаться на права, пока сделаем так, для простоты, потом будем делать правильно:

***usermod asat -G mail***

***usermod great -G mail***

***chmod -R 777 /var/ma***

Настраиваем в почтовом клиенте подключения этим пользователям: одному по pop3, второму - по imap, чтобы показать где и как хранится почта.

## **Разбор типовых ошибок при построении минимальной конфигурации**

**fatal: no SASL authentication mechanisms** //проверьте что у постфикса правильно настроена связка с довекотом

dovecot: pop3-login: Aborted login (no auth attempts in 0 secs) //

При попытке подключиться к серверу по IMAP или POP3, клиент выдаёт сообщение о неправильном имени или пароле, хотя они правильные, а в логе Dovecot пишет:

dovecot: imap-login: Disconnected (no auth attempts in 1 secs): user=<>

Как вы можете увидеть, в поле имени пользователя пусто. Это говорит о том, что соединение было завершено ещё ДО ТОГО, как Dovecot начал проверку учётных данных (имени и пароля). А значит, дело почти на 100% в SSL.

Поскольку механизм обмена именем и паролем в открытом виде (plaintext) уже давно считается небезопасным, по умолчанию в Dovecot он запрещён. По умолчанию, Dovecot будет работать только через SSL, т.е. ваш клиент, с помощью которого вы подключаетесь к Dovecot по IMAP или POP3 должен либо поддерживать STARTTLS либо TLS/SSL. Но это ещё не всё! Ваш клиент должен ПРИНЯТЬ сертификат, который ему отдаёт сервер и согласиться с ним работать! Например, в Thunderbird это как-то совсем не очевидно, что вы должны подтвердить исключение безопасности по данному сертификату, иначе будете получать вышеописанную ошибку о неверном имени и пароле!

Есть конечно в конфигурационном файле Dovecout такая опция как ***disable\_plaintext\_auth***, которая по умолчанию:

disable\_plaintext\_auth = yes

Но, если вы сделаете "no", то увидите, что мало что изменилось. В данном случае "no" позволит подключаться с plaintext только с адреса 127.0.0.1 (Что в общем-то тоже полезно, для RoundCube и других веб систем). Но что же делать, если вы хотите plaintext удалённо? Для этого надо найти в конфигурационном файле опцию ssl. По умолчанию она

ssl = required

Так вот, её надо сделать "no". Значение "yes" или "required" перекрывает значение опции ***disable\_plaintext\_auth***! Об этом почему-то нигде не написано!

# Урок 5. Типовые задачи администрирования

В этой главе рассмотрим типовый задачи администрирования почтовых серверов

## Восстановление писем, удалённых из корзины (аналог корзин 2-3 уровня эксченджа)

По идее, для этого нужна некая настройка, которая в момент логаута письма, помеченные на удаление не удаляет окончательно, а переносит в другое место (откладывает в сторону). Насколько я понял Sieve не имееет постлогаут команд, а работает только по прибытии письма. Если в эксчендже в течение retention policy которое по умлончанию, по-моему 30 дней письма хранятся в той же базе которая продолжает расти. У довкота тоже такой функионал предусмотрен, включается он через плагин (подключаемый модуль).

**vim /etc/dovecot/dovecot.conf**

namespace inbox {

mailbox .EXPUNGED {

autoexpunge = 7days

autoexpunge\_max\_mails = 100000

}

}

mail\_plugins = $mail\_plugins lazy\_expunge acl

plugin {

# Move messages to an .EXPUNGED mailbox

lazy\_expunge = .EXPUNGED

# Define ACL so that user cannot list the .EXPUNGED mailbox

acl = vfile:/etc/dovecot/dovecot.acl

# Expunged messages most likely don't want to be included in quota:

quota\_rule = .EXPUNGED:ignore

}

Перезапускаем

**systemctl restart dovecot && systemctl restart postfix**

и проверяем что он появился у пользователя:

**doveadm mailbox list -u** [**zakaz@sumare.ru**](mailto:zakaz@sumare.ru)

после удаления из корзины у меня появляется файл с очищеными письмами .EXPUNGED и аймап папка с таким же именем. Если ничего небыло удалено то если удалить 1 файл то Thrash и .EXPUNGED станут одинакового размера, потом при очистке корзины она станет начального размера а второй файл станет в 2 раза больше. Тоесть при каждом попадании в корзину он будет расти, будет расти он и при очистке корзины и переносе из неё в другие папки например во входящие. Смотрим что появилось там:

**doveadm mailbox status -u zakaz@sumare.ru "all" .EXPUNGED**

**doveadm search -u zakaz@sumare.ru mailbox .EXPUNGED**

Но это мы сделали аналог корзины 2-го уровня. Имя файл с письмами и элементраные навыки баш сделать аналог 3 уровня мне кажется очевидно, например сделать имя с %u.EXPUNGED или подобное

With v2.2+ you can set lazy\_expunge\_only\_last\_instance = yes to copy only the last instance to the expunge storage. This ensures that only a single copy of a message will appear in the expunge storage.

После этого идем в раздел примеров довадм копи

## pflogsumm – сборщик статистики из лога postfix

Наблюдение за статистикой работы почтового сервера весьма важная вещь. На инфицированном компьютере может быть скомпрометирован пароль от почты и даже одного ящика от которого рассылался спам может стать достаточно чтобы Ваш почтовый домен попал в спам-листы. Для борьбы с этим надо вести счётчик писем от пользователя, понятное дело что скажем 100 писем от пользователя в день это уже похоже на подозрительную активность

https://sysadmins.ru/topic528243.html

Утилита анализирует mail.log файл и выводит результат. установка:

**yum install -y postfix-pflogsumm**

посмотреть статистику писем за сегодня:

**pflogsumm /var/log/maillog -d today**

посмотреть статистику писем за вчера:

**pflogsumm /var/log/maillog -d yesterday**

посмотреть статистику по всему логу вообще можно без ключей, а по предыдущим логам которые можно увидеть нажав два раза таб и выбрав нужный:

**pflogsumm /var/log/maillog-20191124**

<cnt> означает counter, но сколько и для чего надо посмотреть, не указаны диапазоны

**pflogsumm /var/log/maillog -d yesterday --bounce-detail 2**

отправка отчета pflogsumm на почту asat@sumare.ru из скрипта(от имени postmaster@sumare.ru):

pflogsumm -d yesterday /var/log/maillog | mailx -s 'sumare.ru emails daily report' -r postmaster@sumare.ru asat@sumare.ru

emerge net-mail/pflogsumm-1.1.5 -av

## logwatch – сборщик статистики вообще по всему

установка:

**yum install -y logwatch**

конфиг дефолтный у него лежит вот здесь:

**vi /usr/share/logwatch/default.conf/logwatch.conf**

себе поменял следующее вот так:

diff ./bacups-configs/logwatch.conf /usr/share/logwatch/default.conf/logwatch.conf

35c35,37

< Output = stdout

---

> #Output = stdou

> **Output = mail**

>

44c46

< MailTo = root

---

> **MailTo = asat@sumare.ru**

53c55

< MailFrom = Logwatch

---

> **MailFrom = postmaster@sumare.ru**

82a85,86

>

> **Service = "-pam\_unix"**

83a88,93

> **Service = "-sshd"**

> **Service = "-sshd2"**

> **Service = "-dovecot"**

Ну и запихнул это в crontab –e раз в сутки

## imapsync – миграции,синхронизация двух ящиков на разных серверах

установка:

**yum instal -Y imapsync**

копируем из юзер1 в юзер2

**imapsync --host1 mail.sumare.ru --user1 asat --password1 sumare1password --host2 mail.sumare.ru --user2 great --password2 sumare1password**

для джимаил добавляем ключ минус ссл1, перед этим разрешив доступ к ящику для менее безопасных почтовых приложений:

**imapsync --host1 imap.gmail.com --user1 ilhadonorte --password1 SintGi025 --host2 mail.sumare.ru --user2 great --password2 sumare1password -ssl1**

## Репликация между двумя серверами

Настраиваем второй почтовый сервер аналогично первому, делаем только разные цвета консолей чтобы не путаться, проверяем что они друг друга правильно резолсят

**ping mailer1.sumare.ru**

**ping mailer1.sumare.ru**

настраиваем в почтовом клиенте одну и туже учетную запись только смотрящую на разные севера для демонстрации репликации. Репликация работает в режиме мастер-мастер, поэтому каждая нода выступает и клиентом и сервером. Обе стороны настраиваются одинаково, за исключением айпи-адресов соседа. Делать это можно либо через ссш либо чтобы репликация шла через тср. Настроим вариант для тсп:

# cat conf.d/12-replicator.conf

mail\_plugins = $mail\_plugins notify replication

service replicator {

unix\_listener replicator-doveadm {

mode = 0660

group = vmail

}

process\_min\_avail = 3

process\_limit = 100

}

service aggregator {

fifo\_listener replication-notify-fifo {

user = vmail

}

unix\_listener replication-notify {

user = vmail

}

process\_min\_avail = 3

process\_limit = 100

}

service doveadm {

inet\_listener {

port = 4092

}

process\_min\_avail = 3

process\_limit = 100

}

service config {

unix\_listener config {

mode = 0600

user = vmail

}

}

doveadm\_password = pa$$word

dsync\_remote\_cmd = doveadm dsync-server -u%u

plugin {

mail\_replica = tcp:IP\_2:4092

replication\_full\_sync\_interval = 1 hours

}

replication\_full\_sync\_interval = 1 hours

replication\_max\_conns = 10

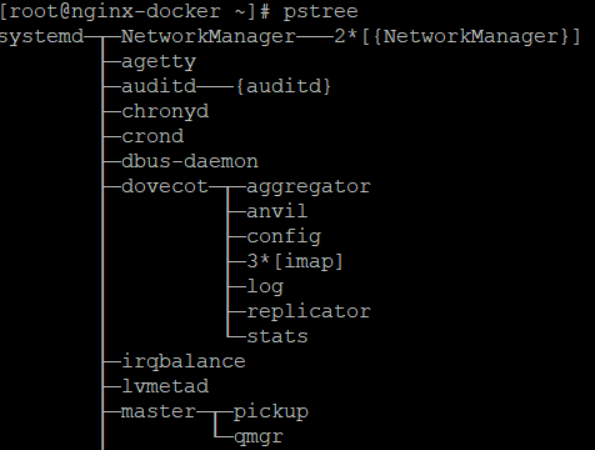
replication\_dsync\_parameters = -d -N -l 30 -U

перезапскаем довкот и смотрим статус его запуска:

**systemctl restart dovecot && systemctl status dovecot -l**

если он не ругнулся и все настройки перенесены в конфиг верно, то смотрим дерево процессов: там до aggregator replicator и еще третий процесс был

**pstree**



Отправляем тестовое письмо, проверяем статус синхронизации для пользователя по маске

**doveadm replicator status zak\***

**doveadm replicator status '\*'**

пихнуть репликацию вручную:

**doveadm replicator replicate zak\***

пихнуть репликацию вручную:

**doveadm replicator replicate `\*`**

посмотреть статус текущих процессов репликации, должны долго работать?

doveadm replicator dsync-status

Можно ключиками заставить dsync реплицировать только в одну сторону. Но тогда будет рассинхрон между мастером и слейвом. Т.е. на слейве перетащили, а на мастере файл так и будет оставаться неперетащеным.

man doveadm-deduplicate doveadm force-resync

https://www.mankier.com/1/doveadm-deduplicate

enabled optimized fsync instead

## Транспортные правила.

Надо для копирования писем в другой ящик и т.п.-было в файле

vi /etc/postfix/main.cf

Редактируем или дописываем:

transport\_maps = hash:/etc/postfix/sumare-transport

После создаем карту:

postmap hash:/etc/postfix/sumare-transport

И перезапускаем postfix:

systemctl restart postfix

## Пересылать письма, приходящие на несуществующие ящики на определенный

Добавляем строку

virtual\_alias\_maps = hash:/etc/postfix/sumare-virtual-alias-maps

в файл

**vi /etc/postfix/main.cf**

Создаем файл

**vi /etc/postfix/sumare-virtual-alias-maps**

@sumare.ru jim

Это означает что на все, не перечисленные в этом файле виртуальных алиасов адреса-пересылать на ящик джима.

После этого надо сделать из него понятную постфиксу базу, но не postalias ибо это не его формат а postmap

**postmap hash:/etc/postfix/sumare-virtual-alias-maps**

и после этого перечитываем конфигурацию постфикса:

postfix reload

проверяем отправляя на несуществующий ящик домена сумарэ-письмо должно упасть в ящик джима. Джим, естественно, должен реально существовать.

## Сбор почты с внешних аккаунтов.

https://interface31.ru/tech\_it/2013/05/zimbra-sbor-pochty-s-vneshnih-akkauntov.html

keep

Каждое сообщение, принятое fetchmail, затем обычно пересылается по SMTP на порт 25 локальной машины, на которой он запущен (localhost), как будто это сообщение было принято по обычному каналу TCP/IP. Затем почта доставляется локально системным транспортным агентом (MDA - Mail Delivery Agent, обычно это sendmail, но можно использовать smail, mmdf, exim, qmail). Все механизмы управления доставкой (например, файлы .forward), обрабатываются системным MDA, и после этого срабатвают агенты локальной доставки почты.

## Несколько почтовых доменов

Идеи: снаружи смтп позруливается поствиксом транспортными правилами на внутренние почтовики. Тут два варианта: либо напрямую в смтп либо сразу в лмтп. Аймап разруливает довкот директор либо довкот через юсердб прокси парамерт.

Ещё идея изучить маил возможности энджинкс либо просто стп сессии как он будет проксировать

# SMTP и IMAP telent-сессии

Тут рассмотрим способы передачи пароля –нам это необходимо для умения делтяь тестовые заходы когда почтовик на совсем поломался

## SMTP сессия без аутентификации или отправка первого письма

Первое письмо надо отправлять с самого хоста на 127.0.0.1 чтобы не тыкаться во всевозможные ограничения, про существование которых начинающим догадаться очень тяжело.

**telnet sumare.ru** или **smtp telnet 172.27.232.1 smtp** или **telnet 192.168.5.200 25**

**helo mail.sumare.ru**

**mail from:root@sumare.ru**

**rcpt to: root@sumare.ru** или **rcpt to: o.kostin@sky-dynamics.ru** или rcpt to: **m79586305729@yahoo.com**

Также мы можем попросить сервер отправить нам отчет о доставке или невозможности это сделать, для этого добавим в команду необязательные параметры:

**RCPT TO:<test@host31.ru> NOTIFY=success,failure**

Начинаем набирать непосредственно тело письма после команды дата

**data**

354 End data with .

Subject: message001

ok-test message001

.

quit

Обращаю внимание на точку c новой строки после test message, это означает, что передача данных завершена.

-тут показать как меняется заголовок при смене языка на русский

-показать про boundary="------------6EB656343CBFF99DA64846C2"

Как посмотреть судьбу письма

Смотрим в файле лога почовика, делая греп по адресу, каждое сообщение получает свой некий адй ди

cat /var/log/maillog | grep m79586305729@yahoo.com

узнав айди смотрим грепая уже по нему что писали о нём те или иные службы

cat /var/log/maillog | grep 88F056604339

Домашнее задание сессия на разных - vvv postfix

Домашнее задание вычитать заголовки в письме и выяснить что они означают, например чем отличаются from и фром с двоеточием from:

## SMTP сессия с аутентификацией PLAIN

14033893.ppt з38

The PLAIN mechanism's authentication format is: <authorization ID> NUL<authentication ID> NUL <password>. Authorization ID is the username who you want to log in as, and authentication ID is the username whose password you're

giving. If you're not planning on doing a <master user login> [Authentication.MasterUsers.txt], you can either set both of these fields to the same username, or leave the authorization ID empty. Аутлуки вроде с плаин работать не умеют, будут только начиная с логин аут проверить

**telnet 192.168.5.249 25** или **telnet sumare.ru smtp**

**helo mail.sumare.ru** или ehlo **mail.sumare.ru**

**AUTH PLAIN**

Сервер ответит цифрами:

334

**perl -MMIME::Base64 -e 'print encode\_base64("\0**asat**\**@sumare.ru**\000**sumarepassword**");'**

обратите внимание в начале стоит \0 (бекслеш и ноль), знак крокозяблы тоже экранирован бекслешем,а после домена .com стоят бекслеш и три ноля! пароль начинается только после трех нулей! После чего мы получим строчку в кодировке

**AGFzYXRAc3VtYXJlLnJ1AHN1bWFyZXBhc3N3b3Jk**

235 2.7.0 Authentication successful

**mail from:asat@sumare.ru**

**rcpt to:asat@sumare.ru**

**data**

**Subject: message001**

ok-test message001 //пишем произвольный текст, потом для завершения три кнопки: enter . enter

**.**

**Quit**

Всё, вышли из smtp – сессии, в папку пользователя должно добавиться письмо

проверки на этапах,

отправка через графический клиент,

генераторы е-майлов, HELO/EHLO

## SMTP сессия с аутентификацией LOGIN.

Если SMTP сервер требует SMTP-аутентификацию, то после того, как мы с ним поздоровались (ehlo lo) вводим команду AUTH LOGIN и после неё по очереди:  
USERNAME root имя-пользователя  
PASSWORD наш-пароль

**telnet 192.168.5.249 25** или **telnet sumare.ru smtp**

**helo mail.sumare.ru** или **ehlo** **mail.sumare.ru**

**auth login**

334 VXNlcm5hbWU6

**YXNhdA==** перекодированное asat (без домена) отсюда https://www.base64encode.org/

334 UGFzc3dvcmQ6

**MTFxcTIyd3c=** перекодированное 11qq22ww отсюда https://www.base64encode.org/

235 2.7.0 Authentication successful

Или прощще вот так:

***doveadm pw -p*** *11qq22ww* ***-s plain.base64 -u asat***

***doveadm pw -p*** *sumarepassword* ***-s plain.base64 -u asat***

perl -MMIME::Base64 -e 'print encode\_base64("\000asat\000 *sumarepassword* ")'

AGFzYXQAMTFxcTIyd3c= //perl -MMIME::Base64 -e 'print encode\_base64("\000asat\00011qq22ww")'

AGdyZWF0ADExcXEyMnd3 //perl -MMIME::Base64 -e 'print encode\_base64("\000great\00011qq22ww")'

235 2.7.0 Authentication successful

YXNhdAo= echo "asat" | base64 для асат YXNhdA==

YXNhdAo=

YXNhdEBvay5ydQ==

MTFRUTIyd3cK echo "11QQ22ww" | base64 для 11QQ22ww

MTFxcTIyd3cK echo "11qq22ww" | base64

mail from:postmaster@ok.ru

rcpt to:postmaster@ok.ru

data

Subject: message001

ok-test message001 //потом для завершения три кнопки: enter . enter

.

Quit

## SMTP сессия с аутентификацией CRAM-MD5.

Подробный пример:

**telnet 192.168.5.249 25** или **telnet sumare.ru smtp**

**helo mail.sumare.ru** или **ehlo** **mail.sumare.ru**

250-AUTH PLAIN LOGIN CRAM-MD5

250-AUTH=PLAIN LOGIN CRAM-MD5

250-ENHANCEDSTATUSCODES

250-8BITMIME

250-DSN

250 SMTPUTF8

**auth cram-md5**

334 PDI2MDE2OTc2NDI5OTc0MTMuMTUzOTYxMjM4NkBwZzEwY250czcub2sucnU+ //это выданный сервером разовый дайджест

YXNhdCAxY2NkZDU2MjY0MDAzYjUyOWI1NTE0M2I5OTJjZTM1MQ== //на основе логина, пароля и дайждеста генерируется вот такой респонс

235 2.7.0 Authentication successful

## SMTP сессия с аутентификацией NTLM.

Вспомнил что цветной пример тогда проебался из-за аварии. Переделать

## IMAP: чтение по через telnet

Теория хорошая тут: <https://rfc2.ru/2060.rfc> и тут https://wiki.dieg.info/imap

IMAP4rev1 включает операции создания, удаления и переименования почтовых ящиков, проверки наличия новых сообщений, удаления сообщений навсегда, установки и сброса флагов, разбора [RFC-822] и [MIME-IMB]; поиска и селективной выборки атрибутов сообщений, текста или их фрагментов. Доступ к сообщениям в IMAP4rev1 обеспечивается по номерам сообщений, которые просто присваиваются по порядку или задаются с обеспечением уникальности каждого номера.

Использование команды Telnet для проверки соединения с сервером IMAP4. Чтобы запустить сеанс Telnet, откройте командную строку, введите следующую команду и нажмите клавишу ВВОД: чтение IMAP из командной строки

**telnet 192.168.5.254 143** или **telnet sumare.ru imap** или telnet ok.ru imap

Если команда выполнена успешно, от сервера будет получен следующий ответ:

\* OK The Microsoft Exchange IMAP4 service is ready.

далее можно посмотреть перечень возможностей IMAP сервера на данном этапе, первое слово строки дальше исользуется как идентификатор транзакции и может быть любым

**qweqwe CAPABILITY**

Чтобы войти в почтовый ящик и начать обмен данными, воспользуйтесь одной из команд, приведенных ниже, да, именно с вопросительного знака:

? LOGIN <Domain\_Name>/<Log\_On\_Name> <Password>

? LOGIN <LogOnName>@<DomainName>.<Top-Level\_Domain\_Name> <Password>

У меня пока пускает так:

**? login zakaz@sumare.ru password**

Если команда выполнена успешно, от сервера будет получен следующий ответ:

+OK LOGIN completed

Чтобы просмотреть список доступных папок, введите следующую команду и нажмите клавишу ВВОД:

**? LIST "" "\*"**

Формат команды LIST приведен ниже:

LIST reference mailbox

Здесь reference — каталог, где находятся почтовые ящики. Если задается пустая строка вместо этого параметра (""), то почтовые ящики находятся в рабочем каталоге пользователя $HOME (из юзердб). Второй параметр mailbox является именем почтового ящика, который нужно просмотреть. Здесь допускается использование специальных символов, так же, как и при получении обычного списка каталогов, например, группового символа (\*). Если именем почтового ящика задана пустая строка (""), то сервер будет возвращать в качестве ответа иерархический разделитель (для Linux /) и имя корневого параметра.

Если команда выполнена успешно, от сервера будет получен следующий ответ:

? OK LIST completed

Чтобы выбрать нужный почтовый ящик (или же таки папку в своём ящике?), введите следующую команду и нажмите клавишу ВВОД:

? Select <Mailbox\_Folder\_Name>

**? SELECT INBOX**

**A142 SELECT INBOX**

Если команда будет выполнена успешна, будет получен ответ, подобный следующему (в зависимости от количества сообщений в почтовом ящике):

\* # EXISTS

\* # RECENT

\* FLAGS (\Seen \Answered \Flagged \Deleted \Draft $MDNSent)

\* OK [PERMANENTFLAGS (\Seen \Answered \Flagged \Deleted \Draft $MDNSent)]

Permanent flags

\* OK [UNSEEN #] Is the first unseen message

\* OK [UIDVALIDITY 63] UIDVALIDITY value

\* OK [UIDNEXT 7] The next unique identifier value

? OK [READ-WRITE] SELECT completed.

? EXAMINE INBOX //что делает эта команда?

Чтобы получить определенные сообщения, введите одну из следующих команд и нажмите клавишу ВВОД:

? FETCH <message number> All

<message number> – 1, 2, 3 и т. д. Например, введите ? FETCH 1 All. Алл здесь означает что письмо просим целиком, тоесть все его составляющие: и заголовки, и тело, флаги, размер, время когда оно упало. Чтобы посмотреть только тело письма используем сабкоманду с ключевым слово бади:

? FETCH <message number> Body

client: a4 FETCH 1 BODY[]

<message number> – 1, 2, 3 и т. д. Например, введите ? FETCH 1 Body.

В квадратных скобках можно уточнить что именно из письма интересует, нармер дернуть определённый заголовок

Чтобы выйти из сеанса IMAP4 с компьютером Exchange, введите следующую команду и нажмите клавишу ВВОД:

**qweqwe LOGOUT**

Если команда выполнена успешно, от сервера будет получен следующий ответ:

\* BYE Microsoft Exchange Server 2007 IMAP4 server signing off.

? OK LOGOUT completed.

Сжато для моего стенда:

telnet localhost 143

telnet 192.168.5.249

? LOGIN asat 11qq22ww //да, именно так с вопросом в начале без домена заглавными

? LOGIN asat@ok.ru secret

? login root 11QQ22ww

? LIST "" "\*"

? Select INBOX //выбрать папку «Входящие»

? LOGOUT //выйти из imap сеанса.

чтение моего ящика в скайдайнамикс:

telnet mail.cns-corp.ru imap

? LOGIN [o.kostin@sky-dynamics.ru](mailto:o.kostin@sky-dynamics.ru) Ghty789Rt#

? LOGIN [o.kostin@sky-dynamics.ru](mailto:o.kostin@sky-dynamics.ru) X253126df

Ghty789Rt#

PASS

// -ERR Invalid command; valid commands: USER PASS AUTH APOP STLS CAPA QUIT

list

retr 495

## **POP3: доступ к из командной строки через telnet (приём почты)**

Теория хорошая тут: https://rfc2.ru/1939.rfc/print

POP3 сессия состоит из нескольких стадий. После установки TCP соединения, сервер посылает приветствие, и сессия переходит в состояние AUTHORIZATION. На этом этапе клиент должен идентифицировать себя на сервере. После успешной идентификации сессия переходит в состояние TRANSACTION. В этой стадии клиент запрашивает выполнение команд на сервере. Когда клиент посылает команду QUIT, сессия переходит в состояние UPDATE. На этом этапе POP3 сервер освобождает все ресурсы, занятые в стадии TRANSACTION и заканчивает работу. TCP соединение после этого закрывается.

Тут всё просто:

***telnet 192.168.5.249 110*** или ***telnet ok.ru pop3***

***user asat*** //именно так, БОЛЬШИМИ буквами команда без доменной части

**pass parol**  
ввели пароль "parol"  
теперь мы можем узнать количество и размер почтовых сообщений:  
**stat**  
для вывода полного листинга почтовых сообщений надо использовать команду:  
**list**  
тут получим табличку вида «порядковый номер письма размер», самые новые письма -будут внизу, с самыми большими номерами, тоесть первое письмо это самое старое

для того чтобы прочитать нужное сообщение вводим:  
**retr номер письма,самое свежее-будет с максимальным номером**

**retr 1 //посмотреть первое письмо**

просмотреть только заголовок сообщения:  
**top номер письма 0 (в конце строки поставить ноль)**  
удалить письмо из ящика:  
**dele номер сообщения**  
выход:  
**quit**

**Командой user указываем серверу, почту какого пользователя мы желаем читать:**

**user tigrisha**

|  |
| --- |
| **+OK** |

Передаем наш сложнейший пароль:

**pass Sx12DF234**

|  |
| --- |
| **+OK** |

После того как нас авторизовали, посмотрим с помощью команды stat состояние нашего почтового ящика. Судя по ответу сервера, в ящике одно письмо размером 597 байт. Просмотреть содержимое письма можно с помощью команды top 1 20:

**Stat**

|  |
| --- |
| **+OK 1 597** |

Приказываем показать верхние 20 строк первого письма:

**top 1 20**

**+OK**

**Return-Path:**

**Received: (from tigrisha@test.ru)**

**for tigrisha@test.ru; Tue, 11 Feb 2003** **18:18:39** **+0300 (MSK)**

**(envelope-from tigrisha@test.ru)**

**Date: Tue, 11 Feb 2003** **18:18:39** **+0300 (MSK)**

**From: Beshkov Andrew < tigrisha@test.ru >**

**Message-Id: <200302111518.h1BFIdO44983@mail.test.ru>**

**To: tigrisha**

**testing mail for tigrisha**

помимо user pass в pop3 сервер можно авторизоваться командой APOP, которая по умолчанию отключена. Формат APOP [имя] [digest] где имя это ящик, дайджест -это MD5 от строки конкатенации временной метки выдаваемой в приветствии севером вместе с угловыми скобками и пароля к ящику как в примере ниже:

S: +OK POP3 server ready <1896.697170952@dbc.mtview.ca.us>

C: APOP mrose c4c9334bac560ecc979e58001b3e22fb

S: +OK maildrop has 1 message (369 octets)

In this example, the shared secret is the string «tan-

staaf». Hence, the MD5 algorithm is applied to the string

<1896.697170952@dbc.mtview.ca.us>tanstaaf

which produces a digest value of

c4c9334bac560ecc979e58001b3e22fb

чтение моего ящика в скайдайнамикс:

telnet mail.cns-corp.ru pop3

user o.kostin@sky-dynamics.ru

PASS Ghty789Rt#

X253126df // -ERR Invalid command; valid commands: USER PASS AUTH APOP STLS CAPA QUIT

list

retr 495

## Перекодировщики бэйз 64

В манах довкота перекодировка указана как

printf 'username\0username\0password' | mmencode

в центосе аналогичное получается как

printf 'username\0username\0password' | base64

результат обеих должен выглядеть как :

dXNlcm5hbWUAdXNlcm5hbWUAcGFzc3dvcmQ=

Есть в нотепад++ на тексте правой кнопкой-плагин командс- бэйз64 энкоде:

оно же в меню-плагины-майм //потестировать

perl -MMIME::Base64 -e 'print encode\_base64("username");'

perl -MMIME::Base64 -e 'print encode\_base64("password");'

If you have any special characters such as @ or ' or ! you must put \ in front of it to escape the character.

perl -MMIME::Base64 -e 'print encode\_base64("user\@server.ru");'

echo -en "\0username\0password"|base64

echo -ne '\0username@example.com\0password' | base64

With AUTH PLAIN, the credentials should be sent according to this grammar (from [RFC 4616](http://www.ietf.org/rfc/rfc4616.txt)):

message = [authzid] UTF8NUL authcid UTF8NUL passwd

authcid = 1\*SAFE ; MUST accept up to 255 octets

authzid = 1\*SAFE ; MUST accept up to 255 octets

passwd = 1\*SAFE ; MUST accept up to 255 octets

UTF8NUL = %x00 ; UTF-8 encoded NUL character

[...]

It seems common to have an empty authzid for SMTP servers, thus this should compute a working AUTH PLAIN message for you:

echo -ne "\0username\0password"|base64

## gen-auth

Скрипт на перле, позволяющий генерировать строки для аутентификации в почтовиках, взят отсюда

<http://www.jetmore.org/john/code/gen-auth>

**gen-auth** - generate various authentication strings

скопировать текст скрипта в файл, например /root/gen-auth, дать права на исполнение chmod +x gen-auth ,

запускать как

/usr/bin/perl /root/gen-auth

Для того чтобы заработало вычисление перлом MD5 и NTLM надо доставить Perl MD5 hashing module

yum install perl-Digest-MD5

yum install perl-NTLM

https://www.md5online.org/

# Команды администрирования postfix

Здесь мы даже не рассмотрим а набросаем себе шпаргалочку синтаксисов команд администрирования

## postfix - команда управления процессом master

запуск, останов:

***postfix start, stop***

посмотреть статус малоинформативно

**postfix status**

Проверка корректности конфигурации Postfix. Эта команда предупреждает о неправильных правах собственности и доступа для каталогов или файлов и создает недостающие каталоги. После правки конфигов надо делать вот так проверку:

***postfix check***

перечитать конфиг, обычно после правки main.cf или master.cf:

***postfix reload***

доставить застрявшую почту:

***postfix flush***

postalias

post-grohtml

postmap

postkick

posttls-finger

postlock //блокировать папку с почтой для эксклюзивного выполнения команд

postmulti //что-то для мультиинстансов

postdrop //пока не понял

postlog // Postfix-совместимая утилита логгинга для скриптов

## postconf – просмотр переменных настройки

postconf утилита изменения настроек постфикс-без ключей выдаст все параметры

postconf –d посмотреть дефолтные значения параметров

postconf -d | grep ^my вот как смотреть параметры начинающиеся на му

postconf -e "parameter=value" как то так оно конфигурируется

postconf | grep directory сначала найдем используемые Postfix каталоги при помощи такой команды:

postconf | grep queue\_directory тут вроде бы должны быть очереди.

postconf mydestination посмотреть куда Postfix доставляет почту.

postconf mail\_spool\_directory посмотреть в какую папку Postfix складывает почту.

postconf -e " mail\_spool\_directory = /var/ok-correio" задаём свою папку для хранения почты

Use "postconf readme\_directory" or "postconf html\_directory" to locate this information

postconf html\_directory readme\_directory какое-то ридми, говорит что документация лежит в /usr/share/doc/postfix3-3.2.4/README\_FILES, чуть выше кстати и по довекоту

postconf mydestination

postconf -m какие форматы карт поддерживает ваш Postfix

postconf -Mf модули постфикса??

## postqueue - команда управления очередями

начать обработку почты в очереди / очистить очередь путем форсирования отправки/доставить почту. Сымитировать наполнение очередей можно установив маленький размер ящика (mailbox\_size\_limit поставить меньше message\_size\_limit) и отправив большое количество писем-они будут накапливаться в очередях:

**postqueue -f** или **postfix flush**

посмотреть письма в очереди, посмотреть номера очередей, посмотреть почтовую очередь, после установки она пуста:

***postqueue -p или* mailq**

посмотреть тоже самое, но в JSON формате (покажет ID и имя очереди, в которой находится письмо)

**postqueue -j**

подсчитать количество писем в очередях:   

***postqueue -p | grep -c "^[A-Z0-9]"***

доставить всё для example.com

***postqueue -s example.com***

доставить конкретное письмо, -vvv уровень дебаггинга отправки:

**postqueue -i queue\_id**

Remove specific email - in case you want to remove any specific email, you can use the following command:

First search the ID of that email like below command

***postqueue -p | grep "email@example.com"***

0AB345F3D24\*    5513 Sun Feb 26 02:26:27  email@example.com

Print Postfix queue domain and age distribution

qshape, показывающую распределение сообщений между очередями. Нету такой? Таки есть

посмотреть счетчик по очередии hold:

**qshape hold**

delete-from-mailq MAILER-DAEMON

post-install исправление автоматич. конфигурации

grep /var/log/maillog F29D3562E

SEE ALSO

qmgr(8), queue manager

showq(8), list mail queue

flush(8), fast flush service

sendmail(1), Sendmail-compatible user interface

postsuper(1), privileged queue operations

README FILES

Use "postconf readme\_directory" or "postconf html\_directory" to locate this information.

ETRN\_README, Postfix ETRN howto

## postsuper – управление задачами в очередях Postfix.

У Postfix есть много разных очередей которые по дефолту лежат в папке /var/spool/postfix и являются её подпапками, различающихся назначением, и содержимым. Содержимое может быть самими почтовыми сообщениями, это очереди:

incoming, active and deferred (отложенные)

либо логами работы:

bounce, defer, trace and flush

Очистить все очереди из Postfix:

***postsuper -d ALL***

Очистить: удалить из очереди отложенных писем(deferred):

***postsuper -d ALL deferred***

поставить доставку конкретного письма на паузу (–Н отпустит)

**postsuper -h queue-id**

postsuper вручную поместить сообщения в очередь hold или вернуть их оттуда, переместив в очередь deferred.

postsuper -r достать более старые и перемещения их в очередь maildrop.

postsuper -d queue id удаление сообщения из очереди

Delete mail from mail queue with id 0AB345F3D24.

***postsuper -d  0AB345F3D24***

## postcat – посмотреть письмо

Команда администрирования postcat позволяет посмотреть в текстовом режиме письмо: исследовать повреждённые письма, смотреть письмо в очереди, идентификатор очереди даст mailq

смотрим сообщение с ИД таким-то

**postcat -q F2B9715C0B3**

посмотреть письмо по идентификатору

**postcat -vq messageid**

сохранить сообщение в файл:  

***postcat -vq  messageid  > message.txt***

## newaliases

## postalias –создаёт cписки рассылки или запросы к ним

Алиас - это то что перед знаком "@" в адресе почты. в aliases пишется сначала алиас, двоеточие а потом юзер линукс

Как пример, сделаем алиас наподобие all@sumare.ru, чтобы письма пересылались бы на всех существующих юзеров этого домена. Пользователей у нас только двое, поэтому создаём текстовый файл без расширения

**vi /etc/postfix/sumare-aliases**

с одной строкой следующего содержания (алиас all разворачивающийся в great и asat):

all: great, asat

в конфиге постфикс прописываем его адрес и механизм создания, но постфикс потом будет обращаться не к нему а базе которая создастся потом а том же месте, с таким же именем но расширением .db

**vi /etc/postfix/main.cf**

alias\_maps = hash:/etc/postfix/sumare-aliases

сохраняем конфиг и теперь из того текстового файла генерируем понимаемую postfix-ом базу (это наследие плюс делалось под очень большие продакшены где не два а тысячи пользователей и много правил)

**postalias hash:/etc/postfix/sumare-aliases**

и не забываем после этого сказать постфиксу чтобы перечитал всё это дело, да, получившемуся файлу sumare-aliases.db дайте владельцем postfix и права, иначе посктфикс ругнётся при перечитывании конфига.

**postfix reload**

проверяем что олл у нас начало резолвиться в грит и асат:

**postmap -q all hash:/etc/postfix/sumare-aliases**

Пару минут как раз в паре постов от этого оставил комент по этому поводу

/etc/postfix/alluserslist в котором прописаны необходимы юзеры и в

/etc/postfix/aliases

allusers: :include:/etc/postfix/alluserslist

отсылается письмо на адрес allusers@mydomain.net

Чтоб ручками не приходилось добавлять, то можно в скрипт на создание нового пользователя добавить строчку, которая дописывает нового пользователя в лист

если реализовать то, что вы пытаетесь сделать, то почта для user@любой\_домен будет переадресована на admin@тот\_же\_домен, а это в общем случае совершенно неправильно.

Изначально все группы рассылки будут заблокированы на прием почты снаружи, т.е. в них можно будет отправить письмо только сотрудникам нашей организации

man transport

man smtp

man lmtp

## postmap Команда администрирования

в отличие от предыдущей postmap не может работать с форматом файла, где ключ и значение разделены двоеточием

At this moment we are going to ensure Postfix finds your first email address with the following command. It should return 1 if it's successful:

postmap -q email1@example.com mysql:/etc/postfix/mysql-virtual-mailbox-maps.cf

postmap -q "example.com" mysql:/etc/postfix/sql/virtual\_mailbox\_domains.cf протестировать запрос к БД, база должна быть заранее прописана, устанлен ее поддерживающий постфикс, на запрос должна отвечать тем что запрашивается либо если запрошеного нет-ничем не отвечать

postmap -q "asat" mysql:/etc/postfix/sumare-local-recipient-maps.cf

asat

postmap -q sender@example.com hash:/etc/postfix/sender\_access посмотреть есть ли такая-то запись в карте

postmap -q "all@example.com" ldap:/etc/postfix/ldap/virtual\_aliases.cf

для того чтобы создать карту /etc/postfix/virtual.db на основе /etc/postfix/virtual, выполните такую команду:

postmap hash:/etc/postfix/virtual //для алиасов-посталиас

# Команды администрирования dovecot

Здесь мы даже не рассмотрим а набросаем себе шпаргалочку синтаксисов команд администрирования

## dovecot Команда администрирования

Справка говорит что у нас есть следующие утилиты администрирования: doveadm(1), doveconf(1), dovecot-lda(1), dsync(1)

dovecot – Собственно сам запускаемый с ключами файл Dovecot .

dovecot stop && dovecot

Просмотр всех настроек Dovecot

**dovecot -a**

Просмотр настроек отличных от дефолтных и N

**dovecot -n**

## doveadm Команда администрирования

утилита администрирования, выдаёт перечень команд управления довекотом

**doveadm**

Ну и само собой: перечитать конфигурацию

**doveadm reload**

Просмотр активных подключений

**doveadm who**

Размещение LOG-файлов Dovecot

**doveadm log find**

Просмотр последних 1000 ошибок и предупреждений с момента последнего запуска Dovecot

**doveadm log errors**

Переоткрытие всех логов Dovecot(полезно выполнять после ручной ротации логов)

doveadm log reopen

doveadm user asat2 проверить, есть ли вообще с точки зрения довекота пользователь асат2

doveadm auth test asat2 проверить заход пользователем асат2 с паролем-спросит потом

doveadm log find

doveadm quota get -A посмотреть табличку с квотами на размеры ящиков

## doveadm mailbox **list** –перечень папок

Позволяет посмотреть какие папки есть у пользователя:

**doveadm mailbox list -u zakaz@sumare.ru**

**doveadm mailbox list --user asat**

с ключами -7 и -8 в конце строки выдаст соотвественно в 7 и 8 битной кодировке, английские слова при этом естественно не меняются.

## doveadm mailbox status -размер, количество писем

Посмотреть количество писем в ящике, размер, количество непрочитанных и т.п.

посмотреть папку входящие пользователя заказ –все поля

**doveadm mailbox status -u zakaz@sumare.ru "all" INBOX**

**doveadm mailbox status -u zakaz@sumare.ru "all" .EXPUNGED**

определённые поля:

**doveadm mailbox status -u zakaz@sumare.ru "messages vsize" INBOX**

посмотреть количество писем и размер входящие пользователя асат:

**doveadm -f table mailbox status -u asat "messages vsize" INBOX**

тоже самое, но посмотреть всё о письмах в подпапке:

**doveadm -f table mailbox status -u asat all INBOX/pastanova**

посмотреть информацию о письмах по всем папкам пользователя асат:

**doveadm -f table mailbox status -u asat all '\*'**

ключом –t вводится слово всего или total, вот размер ящика и число писем в нём:

**doveadm -f table mailbox status -u asat -t all '\*'**

посмотреть состояние папок входящие у всех пользователей:

**doveadm -f table mailbox status -A all INBOX**

тоже, только по сообщениям и размеру

**doveadm -f table mailbox status -A "messages vsize" INBOX**

doveadm -f table mailbox status -u asat all INBOX

doveadm -f table mailbox status -u asat all Trash

doveadm mailbox status -u asat -t all INBOX

doveadm -Dv mailbox subscribe -u great INBOX/old/INBOX

## **doveadm mailbox create/delete/rename: работа с директориями внутри ящика, они же маилбоксы**.

Тут всё просто, смотрим какие маилбоксы есть у пользователя:

**doveadm mailbox list -u zakaz@sumare.ru**

и создаём у него две папки: одну без подписки на отображение, вторую – с подпиской

**doveadm mailbox create -u zakaz@sumare.ru INBOX/withsubscribe**

**doveadm mailbox create -u zakaz@sumare.ru -s withoutsubscribe**

перезапускаем почтовый клиент, показываем что вторая папка появилась, а вторая нет но существует в меню сабкрайб и на неё можно подписаться. Чтобы наглухо запретить пользователю видеть папки внутри его ящика например для административных целей типа временного хранения удалённых уже из корзины писем –надо на неё вешать аксес-лист.

## **doveadm mailbox subscribe/unsubscribe подписка на отображение**

создаём папку, выключаем подписку на отображение ранее созданной папки

**doveadm mailbox unsubscribe -u zakaz@sumare.ru subscribe-demo**

перезапускаем почтовый клиент, показываем что папка пропала, переподключаем её обратно:

**doveadm mailbox subscribe -u zakaz@sumare.ru subscribe-demo**

## **doveadm search & fetch - поиск писем по ящикам и просмотр**

команда doveadm searchиспользуется для поиска сообщений по почтовым ящикам, она может возвращать: username, mailbox-GUID / -UID and message-GUIDs / -UIDs. В общем случае использует файлы индексов и кэши поэтому работает намного быстрее грепа по файловым системам.

doveadm fetch: Fetch mail contents or metadata.

doveadm search does the same as doveadm fetch ‘mailbox-guid did’. It’s useful for quick checks where you don’t want to write the full fetch command.

Для начала посмотрим существующие папки в почтовых ящиках, надо посмотреть и pop3 ящик и imap: содержимое их будет отображаться по-разному: у второго будет Sent, Trash, INBOX, у первого только INBOX:

**doveadm mailbox list -u great**

посмотреть у пользователя great перечень писем папки входящие:

**doveadm search -u zakaz@sumare.ru mailbox .EXPUNGED**

**doveadm search -u great mailbox INBOX**

**doveadm search -u great mailbox Sent**

**doveadm search -u great mailbox Trash**

ищем у пользователя great перечень писем папки входящие со словами в теме '7 секретов' у меня нормально работало и в одинарных и в двойных кавычках:

**doveadm search -u great mailbox INBOX Subject '7 секретов'**

**doveadm search -u great mailbox INBOX Subject "7 секретов"**

**doveadm search -u asat@sumare.ru mailbox inbox\\* subject 'Logwatch for vps28780nl (Linux)' unseen**

здесь мы видим guid папки в почтовом ящике и порядковый uid письма в ней: их потом используем, например при просмотре писем в ящике:

**doveadm fetch -u great body mailbox-guid** 5461fe272354025d2f0f000099e495d9 **uid** 1

подсчитать количество писем в папке входящие пользователя делается штатными командами linux:

**doveadm search -u great mailbox INBOX | awk '{print $1}' | sort | uniq -c**

doveadm search -A mailbox 'Trash' | awk '{print $1}' | sort | uniq -c

посмотреть у пользователя great в папке входящие перечень писем размером более 50 килобайт:

**doveadm search -u great mailbox INBOX LARGER 50k**

найти у пользователя great в папке входящие и по всем папкам письма за 10 октября 2019 года:

**doveadm search -u great mailbox INBOX ON 2019-10-10**

**doveadm search -u great mailbox '\*' ON 2019-10-10**

поиск по двум критериям:

**doveadm search -u great mailbox '\*' ON 2019-10-10 OR Subject '7 секретов'**

найти у пользователя great в папке входящие перечень писем с текстом «test-great»

**doveadm search -u great mailbox INBOX TEXT test-great**

**doveadm search -u great mailbox INBOX BEFORE 2019-06-14**

Посмотреть все письма у пользователя в **inbox** старше 90 дней:

doveadm search -u 'great@sumare.ru' mailbox 'INBOX' savedbefore 90d

Show **all messages** in **any folder** that are **older** then 30 days for mailbox@example.org:

doveadm search -u 'mailbox@example.org' mailbox "\*" savedbefore 30d

## **doveadm copy** & **move –** операции с ящиками: **копирование и перенос писем между ящиками**

Скопировать во входящие пользователю great письма из входящих пользователя info что пришли до 7 февраля 2020:

doveadm -Dv copy -u great INBOX user info BEFORE 2020-02-07

Скопировать пользователю great во входящие, в подпапку mail2 (должна быть создана заранее иначе ошибка, ибо автоматически не создаётся) письма из входящих пользователя info что пришли до 8 февраля 2020:

doveadm -Dv copy -u great INBOX/mail2 user info BEFORE 2020-02-08

скопировать все письма пользователю great во входящие, в подпапку mail2 (должна быть создана заранее иначе ошибка, ибо автоматически не создаётся) ВСЕ письма из всех папок пользователя info:

doveadm -Dv copy -u great INBOX/mail2 user info ALL

Скопировать пользователю great во входящие, в подпапку mail3 (должна быть создана заранее иначе ошибка, ибо автоматически не создаётся) письма из входящих пользователя info что пришли до 8 февраля 2020:

doveadm -Dv copy -u great mail3 user info BEFORE 2020-02-08

doveadm move Trash mailbox INBOX from [great@sumare.ru](mailto:great@sumare.ru) //отладить, должно у грита переностить ввесь инокс в трэш

## Индексы.

Есть IMAP команда поиска писем по тем или иным критериям. Совместить с командами поиска самого довкот и показать аутентификацию вот отсюда, есть в прочитаных:

https://wiki.dieg.info/imap

## doveconf – просмотр переменных настройки

doveconf - показывает действующую конфигурацию, состоящую из значений в конфиг. файлах и дефолтных значение

doveconf -n - показывает все параметры текущей конфигурации, которые отличаются от дефолтных

doveconf -N - показывает все параметры текущей конфигурации, даже если они установлены по умолчанию

doveconf -d - показывает дефолтные значения всех параметров (игнорируя текущую конфигурацию)

## doveadm import, sync(ранее dsync), backup –экспорт/импорт, синхронизация, бэкап.

sync это дерево команд для синхронизации почтовых ящиков, для бэкапа и конвертации между различными форматами mailbox<->maildir

Делаем копию почты great в папку бэкап в разные форматы: sdbox именно так - без слеша в конце:

**doveadm sync -u great sdbox:/home/great/2019-11-03-backup-sdbox-great**

или в mdbox:

**doveadm sync -u asat mdbox:/home/asat/2019-11-03-backup-mdbox-asat**

**doveadm sync -u asat tcp:mailer2.sumare.ru //проверить это на миррор импорт должно работать после настройки репликации**

после этого делаем импорт всех писем оттуда в подпапку old папки Входящие, если её нет то создастся автоматически как и у эксченджа:

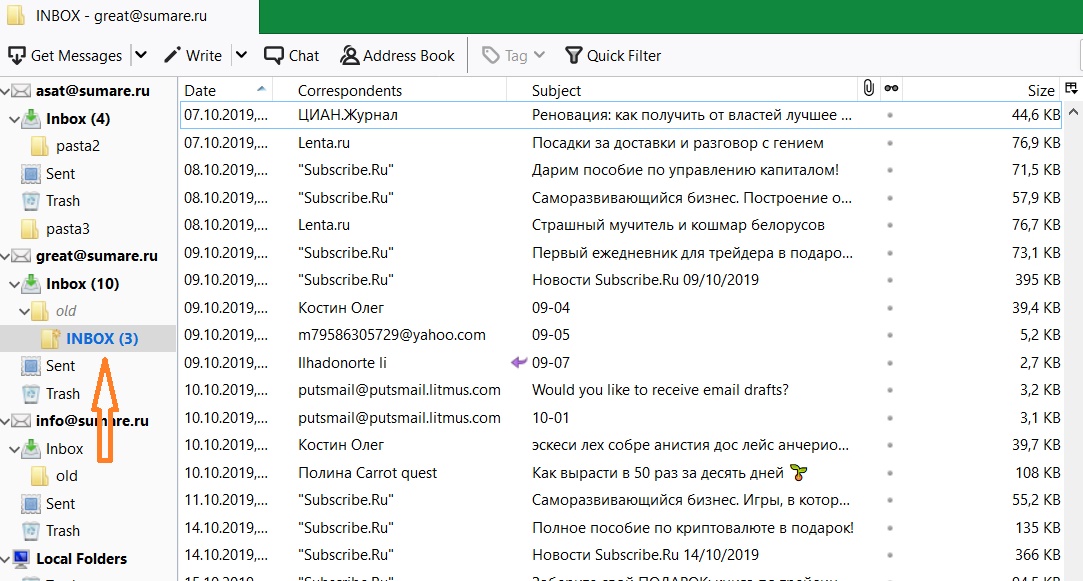
**doveadm -Dv import -u great mdbox:/home/great/2019-11-03-backup-mdbox-great/ Inbox/old al**l

но после этого там ничего не отобразится и вот почему: дело в том, что мало просто создать папку, надо ещё и подписаться на её отображение. Сейчас в почтовом клиенте она не видна и письма в ней тоже, но если посмотреть управлялкой, то можно увидеть что в INBOX появилась подпапка old со всей структурой состояния ящика на момент импорта

**doveadm mailbox list --user great**

подписываемся на неё и после перезапуска она появится в почтовом клиенте:

**doveadm -Dv mailbox subscribe -u great INBOX/old/INBOX**

****

**doveadm -Dv backup –u asat@sumare.ru maildir:/home/asat/ //доделать команду –Rделает обратно папку в ящик пользователю, пир, 232**

**doveadm import -u info sdbox:/home/info/2019-11-03-backup-mdbox-info/ INBOX/old all //не работает пока заработала 2019-11-13**

dovecot-lda(1),

maildir -> dbox migration

Set

mail\_location=sdbox:~/sdbox

and run

**dsync -u username mirror maildir:~/Maildir**

dsync SYNOPSIS

dsync [options] mirror location2

dsync [options] backup location2

mirror

Does a two-way synchronization between two mail locations. Changes in

both locations are synchronized to the other one, without losing any

changes made by either of them. Any potential UID conflicts are

resolved by giving them new UIDs.

backup

Backup mails from default mail location to location2 (or vice versa, if

-R parameter is given). No changes are ever done to the source

location. Any changes done in destination are discarded.

Two-way synchronization of mailboxes in different servers (via ssh)

(dsync will merge the changes without losing any changes done on either side.)

(Dovecot's index logs that keep track of changes.)

creating backups of mails to a remote server

dsync can be run completely standalone.

opts:

-u parameter to do a userdb lookup from auth process.

-v Makes dsync more verbose.

-R Reverse backup direction, so mails in location2 are backed up to default mail location.

i.e.

**dsync -u username mirror ssh -i id\_dsa.dovecot mailuser@example.com dsync -u username**

https://www.heinlein-support.de/howto/backups-und-snapshots-von-linux-servern-mit-rsync-und-ssh

## doveadm pw – получение паролей разных видов

doveadm pw -l посмотреть поддерживаемые механизмы передачи пароля, вот названия:

|  |  |  |
| --- | --- | --- |
| BLF-CRYPT | MD5-CRYPT | SHA1 |
| CLEAR | NTLM | SHA256 |
| CLEARTEXT | OTP | SHA256-CRYPT |
| CRAM-MD5 | PBKDF2 | SHA512 |
| CRYPT | PLAIN | SHA512-CRYPT |
| DES-CRYPT | PLAIN-MD4 | SKEY |
| DIGEST-MD5 | PLAIN-MD5 | SMD5 |
| HMAC-MD5 | PLAIN-TRUNC | SSHA |
| LANMAN | RPA | SSHA256 |
| LDAP-MD5 | SCRAM-SHA-1 | SSHA512 |
| MD5 | SHA |  |

посмотреть как в том или ином методе хранения пароля он будет выглядеть

**doveadm pw -s SHA512-CRYPT**

Эти механизмы можно указывать как напрямую, так и через точку указав в какой кодировке хотим получить результат

.b64, .base64 and .hex.

Например для аутентификации LOGIN имя пользователя и пароль надо передавать в бэйз64:

**doveadm pw -s CLEAR.base64 -p asat**

тоесть строке asat соответствует YXNhdA==

**doveadm pw -s cram-md5 -p sumarepassword**

-t hash посмотреть соответствует ли хэш указанному паролю:

doveadm [-Dv] pw -t hash [-p password] [-u user]

doveadm pw -s sha512 -r 100

## doveadm user

посмотреть всех заведенных пользователей

**doveadm user '\*'**

сделать userdb запрос:

**doveadm user** [**zakaz@sumare.ru**](mailto:zakaz@sumare.ru)

## **doveadm auth – проверка заходов**

Просто проверить заход пользователем асат-проверить правильный ли пароль, покажет uid, папку и проч.

**doveadm auth login asat**

Проверить заход имеющимися логином и паролем password (где rip-remote ip) конкретно на imap,pop3 или smtp:

**doveadm auth test -x service=imap -x rip=127.0.0.1 zakaz@sumare.ru password**

**doveadm auth test -x service=pop3 -x rip=127.0.0.1 asat@ok.ru**

**doveadm auth test -x service=smtp -x rip=127.0.0.1 asat@ok.ru**

сделать проверку passdb запроса (без аутентификации) instead of a userdb lookup.

**doveadm auth lookup username@example.com**

Просмотр информации о пользователе (покажет в каких папках лежит почта пользователя)

**doveadm user asat**

дефолтная подстановка перед поиском в базе пользователей:

dovecot -a | grep auth\_username\_format

auth\_username\_format = %Lu

# %u - username full username (e.g. user@domain

# %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

# %h - home directory

## **doveadm expunge – очистка папок в ящиках**

Это подсемейство команд очистки почтовых ящиков, обычно используется для подчистки папок Trash или Spam у пользователей, тут тоже просто и не интересно (нагенерировать писем генератором и удалить циклом): doveadm expunge: Expunge mails (without moving to Trash).

Вычищаем пользователю все письма из папки удаленные:

**doveadm expunge -u username@example.com mailbox Trash all**

Удаление писем с каталога Trash, которые были помещены туда более 2 недель назад

**doveadm expunge -u username@example.com mailbox Trash savedbefore 2w**

удалить у пользователя письма старше одной недели, по-моему, за исключением Inbox – проэкспериментируйте:

**doveadm expunge -u user@example.com mailbox '\*' before 1w**

Remove all messages from 'Drafts' folder on all example.com domain mailboxes:

for i in $(plesk bin mail -l | tr '\t' ' ' | cut -d' ' -f 3- | grep example.com); do doveadm expunge -u "$i" mailbox INBOX.Drafts all; done

Delete all messages from the particular mailbox user@example.com:

doveadm expunge -u user@example.com mailbox 'INBOX' all

doveadm expunge -u user@example.com mailbox 'INBOX.\*' all

Remove all messages from 'Spam' and 'Trash' folders from all mailboxes on all domains:

for i in $(plesk bin mail -l | tr '\t' ' ' | cut -d' ' -f 3-); do doveadm expunge -u "$i" mailbox INBOX.Spam all; done

for i in $(plesk bin mail -l | tr '\t' ' ' | cut -d' ' -f 3-); do doveadm expunge -u "$i" mailbox INBOX.Trash all; done

## **doveadm quota**

The quota get and quota recalc[1](https://mailcow.github.io/mailcow-dockerized-docs/u_e-dovecot-more/#fn:1) commands are used to display or recalculate the current user's quota usage. The reported values are in kilobytes.

To list the current quota status for a user / mailbox, do:

doveadm quota get -u 'mailbox@example.org'

To list the quota storage value for **all** users, do:

doveadm quota get -A |grep "STORAGE"

Recalculate a single user's quota usage:

doveadm quota recalc -u 'mailbox@example.org'

Просмотр квоты пользователя

# doveadm quota get -u username@example.com

1

# doveadm quota get -u username@example.com

Аналогично,но для всех пользователей (например,список пользователей берется из таблицы postfix.mailbox )

# for user in `mysql -Bse "select username from postfix.mailbox"`; do doveadm quota get -u $user; done

Альтернативно можно попробовать использовать команду

# doveadm quota get -A

Пересчет квоты пользователя

# doveadm quota recalc -u username@example.com

Аналогично,но для всех пользователей (например,список пользователей берется из таблицы postfix.mailbox )

# for user in `mysql -Bse "select username from postfix.mailbox"`; do doveadm quota recalc -u $user; done

Альтернативно можно попробовать использовать команду

# doveadm quota recalc -A

## **doveadm acl**

Надо в тандерберд добавить плагин аймап-ацл, глючное говно, надо смотреть версию плагина и с какими версиями тандербёрда он совместим иначе виснет. еще включить плагин ацл в протоколах, задать пути к словарям, выставить на них права…

Посмотреть свои права на определённый маилбокс:1

doveadm acl MYRIGHTS <mailbox>

глянуть все аклы выставленные на маилбоксе

doveadm acl GETACL <mailbox>

Give <id> the specified rights to the mailbox.

doveadm acl SETACL <mailbox> <id> [+|-]<rights>

doveadm acl DELETEACL <mailbox> [-]<id>: Delete <id>'s ACL from the mailbox.

где <id> может быть:

anyone: все пользователи включая анонимных Matches all users, including anonymous users.

authenticated: все пользователино без анонимныхLike "anyone", but doesn't match anonymous users.

$group: Matches all users belonging to the group ($ is not part of the group name).

$!group: See group-override in <ACL.txt> (Dovecot-specific feature).

user: только определенный пользовтель

owner tambem

**doveadm acl get [-u user|-A|-F file] [-S socket\_path] [-m] mailbox**

Посмотреть ACLs для маилбокса: посмотреть кому и как asat расшарил свою подпапку toshare:

**doveadm acl get -u zakaz@sumare.ru newfolder**

**doveadm acl get -u asat INBOX/toshare**

Установить или добавить ACL права на mailbox/id, если каке-то права уже есть **они сохраняются**. Добавим пользователю [office@sumare.ru](mailto:office@sumare.ru) право на отображение подпапки newfolder пользователя zakaz@sumare.ru

**doveadm acl add -u zakaz@sumare.ru newfolder user=office@sumare.ru lookup [right ...]**

Расписать айди подробнее, про группу, евривану и так дале

Установить определенные ACL права на mailbox/id, если какие-то права были то они **будут заменены**. Установить права пользователю great на подпапку toshare пользователя asat:

**doveadm acl set -u asat INBOX/toshare user=great write**

**doveadm acl set -u asat INBOX/toshare user=great expunge insert lookup read write write-deleted write-seen**

doveadm acl set [zakaz@donainone.ru](mailto:zakaz@donainone.ru) INBOX owner all

doveadm acl set zakaz@donainone.ru INBOX authenticated lookup read write-seen

Убрать определенные ACL права из mailbox/id. Если удалены все права, то будет оставаться без каких-либо прав.

**doveadm acl remove [-u user|-A|-F file] [-S socket\_path] mailbox id right [right ...]**

Удалить ACL целиком для mailbox/id.

**doveadm acl delete [-u user|-A|-F file] [-S socket\_path] mailbox id**

Команда дебаггинга почему shared mailbox не доступен пользователю, покажет какие есть проблемы

**doveadm acl debug [-u user|-A|-F file] [-S socket\_path] mailbox**

посмотреть доступ к подпапке, с разделителями / и . соответственно:

**doveadm acl debug -u asat@sumare.ru INBOX/toshare**

**doveadm acl debug -u asat@sumare.ru INBOX.toshare**

**doveadm acl debug -u zakaz@sumare.ru Public/zakaz@sumare.ru**

Убедиться что пользовательский shared mailboxes корректно заведён в acl\_shared\_dict.

**doveadm acl recalc [-u user|-A|-F file] [-S socket\_path]**

Посмотреть текущие права ACL на mailbox.

**doveadm acl rights [-u user|-A|-F file] [-S socket\_path] mailbox**

**doveadm [-Dv] [-f formatter] acl command [OPTIONS] [ARGUMENTS]**

посмотреть права асата на собственный инбокс

**doveadm acl rights -u asat INBOX**

## doveadm replicator

doveadm replicator

doveadm -Dv replicator status

## разгрести

doveadm reduplicate: Deduplicate mails either by their GUID or by Message-Id: header.

doveadm flags add/remove/replace: Update IMAP flags for a mail

doveadm force-rsync: Try to fix a broken mailbox (or verify that all is ok) Перестроить индексы:

**doveadm force-resync -u great '\*'**

doveadm index: Index any mails that aren’t indexed yet. Mainly useful if full text search indexing is enabled.

страница 153

doveadm mount list

doveadm mount remove

For easily testing authentication, use: doveadm auth test user@domain password

For looking up userdb information for a user, use: doveadm user user@domain

For simulating a full login with both passdb and userdb lookup, use: doveadm auth login user@domain password

doveadm sis

управление релеем

postmap /etc/postfix/sumare\_transport &&postfix reload

# TLS, SSL,

ssl, tls, pops, imaps показать табличку чтобы не путались, проверка секьюрных сессий Чтобы не путаться в портах где что работает есть вот такая табличка:

|  |  |  |  |
| --- | --- | --- | --- |
| Protocol | IANA port (Explicit TLS) | Protocol | IANA Port (Implicit TLS) |
| E-SMTP | 25 | SMTPS | 465\*\* |
| POP3 | 110 | POPS | 995 |
| IMAP4 | 143 | IMAPS | 993 |
| HTTP | 80\* | HTTPS | 443 |

\* HTTP doesn’t implement explicit TLS, because it is stateless and the overhead would not be worth it.  
\*\* Exchange specifically does not support SMTPS (implicit TLS).

Но в этой почему-то не сказали, что 25 порт может быть закрыт и вместо него могут использоватся 587 или 465.

Правильная схема такая:

25: от чужих с/без tls — как у них получится, пусть так и шлют

25: от своих (с аутентификацией) обязательный tls

465: deprecated in RFC 2487

587: tls

Let’s Encrypt 14 -дают ли биесплатные

**vi /etc/postfix/main.cf**

В файле находим секцию, относящуюся к настройкам TLS и добавляем туда несколько строк или раскомментируем их

# TLS parameters

smtpd\_tls\_cert\_file=/etc/dovecot/dovecot.crt

smtpd\_tls\_key\_file=/etc/dovecot/private/dovecot.key

smtpd\_use\_tls = yes

smtp\_use\_tls = yes

Тем не менее, этого недостаточно — дополнительно требуется добиться того, чтобы Postfix работал на портах, поддерживающих шифрование — это 587 и 465 порты.

vi /etc/postfix/master,cf

В файле находим и раскомментируем 2 строки:

#submission inet n — — — — smtpd

Отвечает за работу службы на порту 587

#smtps inet n — — — — smtpd

Отвечает за работу службы на порту 465

Перезапускаем почтовую службу

**postfix restart**

Проверяем какие порты использует Postfix сейчас

**netstat -nltp | grep master**

tcp 0 0 0.0.0.0:465 0.0.0.0:\* LISTEN 1264/master

tcp 0 0 0.0.0.0:25 0.0.0.0:\* LISTEN 1264/master

tcp 0 0 0.0.0.0:587 0.0.0.0:\* LISTEN 1264/master

Цель достигнута, используются в том числе порты 587 и 465. Чтобы теперь отправлять с сервера почту с шифрованием достаточно указывать в настройках почтового клиента SSL/TLS и один из открытых только что портов. //показать что в smtp сессии появилась опция 250-STARTTLS и что на яху почта теперь не попадает в bulk mail/

SSL подключение к IMAP из командной строки

openssl s\_client -connect sumare.ru:143 -starttls imap

TLS/STARTTLS (sometimes called Explicit TLS): uses port 587

SSL (sometimes called Implicit TLS): uses port 465

Determine if the server supports Explicit SSL. Telnet to the server at port 25 Type “starttls” and hit enter. If Explicit SSL is supported, you should see “220 2.0.0 Ready to start TLS”.

## Проверка SMTP аутентификации через TLS.

Надо поставить OpenSSL клиент:

sudo apt-get install openssl

**sudo yum install openssl**

**openssl s\_client -connect sumare.ru:25 -starttls smtp**

When the connection is made, you’ll notice an SMTP 250 code:

250 DSN

Это значит что можно начинать SMTP транзакцию.

Bonus: verify StartTLS for SMTP-, POP3- or IMAP servers – Check HTTPS TLS/SSL certificates.To verify whether your (SMTP-, POP3-, or IMAP) mail server supports StartTLS, use the following OpenSSL command:

openssl s\_client -connect imap.example.com:143 -starttls imap

openssl s\_client -connect imap.mail.ru:993 -starttls imap

TAG1 CAPABILITY

tag1 LOGIN oplblitz@mail.ru pioneer

TAG4 STATUS INBOX (MESSAGES)

\* STATUS "INBOX" (MESSAGES 259)

TAG4 OK Status completed.

TAG5 STATUS INBOX (RECENT)

\* STATUS "INBOX" (RECENT 0)

TAG5 OK Status completed.

TAG6 STATUS INBOX (UNSEEN)

\* STATUS "INBOX" (UNSEEN 0)

TAG6 OK Status completed.

openssl s\_client -connect pop.example.com:110 -starttls pop3

openssl s\_client -connect smtp.example.com:25 -starttls smtp

было понятно в файле IMAP Telnet at PHP Gangsta – Der PHP Blog mit Praxisbezug

curl --connect-timeout 59 -v --insecure "smtps://smtp.live.com:25" -u "\*\*\*\*\*@outlook.com:\*\*\*\*\*\*\*" --mail-from "\*\*\*\*\*\*\*\*@outlook.com" --mail-rcpt "\*\*\*\*\*@yahoo.de" -T mail.txt –ssl

curl smtp://smtp.gmail.com:587 -v --mail-from "my.mail@gmail.com" --mail-rcpt "your.mail@x.com" --ssl -u my.mail@gmail.com:password -T "c:\test.txt" -k –anyauth

curl smtp://smtp.gmail.com:465 -v --mail-from "my.mail@gmail.com" --mail-rcpt "your.mail@x.com" --ssl -u my.mail@gmail.com:password -T "c:\test.txt" -k --anyauth

Use smtps:// for SMTPS (i.e. SMTP on top of an existing SSL/TLS connection).

This works:

curl smtps://smtp.gmail.com:465 -v

I would also use --ssl-reqd for the explicit STARTTLS connection to make sure SSL/TLS is used when you expect it to be (downgrade attacks would be possible otherwise).

curl --url "smtps://smtp.gmail.com:465" --ssl-reqd --mail-from "sender@gmail.com" --mail-rcpt "recepient@gmail.com" --upload-file /var/scripts/mail.txt --user [sender@gmail.com:senderGmailPassword](mailto:sender@gmail.com:senderGmailPassword)

## Отладка IMAP

openssl s\_client -crlf -connect imap.mail.yahoo.com:993

123 login m79586305729@yahoo.com sintgi024

# openssl s\_client -crlf -connect test.alt:993

...

tag login petrov@test.alt Pa$$word

Примечание: выход по Ctrl+D

# Отправка писем из командной строки

## Консольный email-клиент для windows blat

-распаковываем скачанное в папку c:\Windows\ чтобы не набирать полный путь к файлу

- указываются E-Mail отправителя и получателя (postmaster должен быть по-умолчанию на каждом почтовике, адрес получателя-тоже, для простоты отправляем ему же), IP SMTP сервера, тело и заголовок E-Mail, и указываем куда писать лог файл отправки:

del e:\blat-smtp-log.txt

blat -f postmaster@ok.ru -to postmaster@ok.ru -server 192.168.5.249 -body "Ando estudando o postfix" -subject " E-mail do teste do blat do windows " -debug -timestamp -log e:\blat-smtp-log.txt

blat -f postmaster@ok.ru -to administrator@sumare.ru -server 10.77.7.17 -body "E-mail do teste do blat do windows" -subject "tema um do blat do windows" -debug -timestamp -log d:\blat\_SMTP\_log.txt

if %errorlevel%==0 goto end

blat.exe -charset windows-1251 -hdrencb -f "357538@mail.ru" -to 357538@gmail.com -server smtp.mail.ru:2525 -subject "Backup storage connection fail!" -body "Backup storage drive connection fail!" -u 357538 -pw TimeForMail -base64

:end

## Консольные email-отправлятор для linux mailx //доизучать

Установка:

**yum install mailx -y**

под убунту

**sudo apt install mailutils**

тест отправки вставляя дату в заголовок и тело письма:

**date | mailx -s "`date --rfc-3339='date'` test e-mail" -r postmaster@sumare.ru m79586305729@yahoo.com**

Отправка из командной строки поправив днс так как нельзя тут сервер задать делается как-то так:

***date | mailx -s "correio do relay centos" root@ok.ru***

***date | mailx -s "SERVIDOR DE CORREIO OK.RU" asat@ok.ru***

в консоль будет выдано сообщение с указание куда руту упадёт почта: You have mail in /var/spool/mail/root

Это помещает текущую дату в теме Записки backtics вокруг команды date.

**mailx -s "Test the date `date`" TestUser123**

вставить в заголовок дату в нормальном формате: сам текст в двойных кавычках, команда ос с ключом-в обратных

**mailx -s "`date --rfc-3339='date'` connections semanal report" -r postmaster@sumare.ru asat@sumare.ru**

Дату в тело письма чтобы различать потом и аттачи чтобы наполнить:

**date | mailx -s "correio do relay centos" -a /root/attaches/doshirak.mp3 -a /root/attaches/linux.docx -a /root/attaches/ssh.pdf administrator@sumare.ru**

date | mailx -s "correio do relay centos" great@ok.ru

echo "E-mail do teste do linux" | mailx -s "correio do centos" [postmaster@ok.ru](mailto:postmaster@ok.ru)

echo "E-mail do teste do linux" | mailx -s "correio do relay centos" [administrator@sumare.ru](mailto:administrator@sumare.ru)

echo "E-mail do teste do linux" | mailx -s "correio do relay centos" ok@sumare.ru

date | mailx -s "correio do relay centos" [administrator@sumare.ru](mailto:administrator@sumare.ru)

mailx -s "Test e-mail" root@359831-ca13528.tmweb.ru

## Консольные email-просмотрщик для linux mutt

Зайдя в систему, вы иногда видите сообщение You have mail in /var/spool/mail/root. Можно просто посмотреть что там лежит но удобнее приход писем лучше смотреть через mutt чтобы каждый раз в папку не лазить. Ставится так:

**yum install mutt -y**

After it connect to the mail box by hitting

**mutt -f imaps://sabi@localhost**

Для отправки файла из командной строки можно воспользоваться несколькими способами:

Отправка текстового файла:

cat text.txt | mail -s TEST email@address

Отправка бинарного файла:

cat text.exe | uuencode text.txt | mail -s TEST email@address

Отправка файла с архивированием на лету:

gzip -c text | uuencode text.gz | mail -s TEST email@address

Отправка с помощью утилиты mpack:

mpack -s “Attached file” file.jpg test@example.com

Отправка с помощью утилиты nail:

nail -s "Let's send file" -a file\_to\_send.rar recepient@email.adr<Enter>

Look at this funny file<Enter>

.<Enter>

<Ctrl-D>

echo "Eu sou fodinha." | mail -s "Own! Meu primeiro email: local <3" -r "root@exemplo.com" eumesmo@exemplo.com

## Отправка email из Powershell

запустить PowerShell от имени администратора. Ввести команду set-executionpolicy unrestricted (или bypass) и согласиться на изменение режима запуска скриптов. это позволит запускать любые скрипты PowerShell далее копируем на сервер в папку c:\Scripts\ (которую надо предварительно создать) файл **send\_backup\_mail.ps1** такого содержания:

# Add-PSSnapin Windows.Serverbackup

$EmailFrom = "support@sky-dynamics.ru"

$EmailTo = "backup@sky-dynamics.ru"

$Username = "backup@sky-dynamics.ru"

$Password = "X253126df"

$Subject = "Backup ZVVZ\_M Server [PDC.zvvz.local]"

$Body = Get-WBSummary | Out-String

$SMTPServer = "mail.cns-corp.ru"

$SMTPClient = New-Object Net.Mail.SmtpClient($SmtpServer, 587)

$SMTPClient.Credentials = New-Object System.Net.NetworkCredential($Username, $Password);

$SMTPClient.Send($EmailFrom, $EmailTo, $Subject, $Body)

Так же если выскакивает подтверждение выполнения скрипта pic1.jpg, то необходимо передавать powershell.exe следущую строку:

Get-Content c:\scripts\send\_backup\_mail.ps1 | PowerShell.exe -noprofile -

Иначе на подтверждении скрипт будет зависать.

## Генератор большого количества писем

smtp-source - parallelized SMTP/LMTP test generator

smtp-source -m 10 -s 10 -f sender@example.com –t [recipient@example.com](mailto:recipient@example.com) 127.0.0.1:25

-f от кого

-m количество сообщений, по дефолту одно

-s в 10 параллельных сессиях

smtp-source -m 10 -s 10 -f postmaster@ok.ru –t [ok@sumare.ru](mailto:ok@sumare.ru) 192.168.5.249:25

/етц/пассвд редактируется через випв

висудо

pwgen 16 вроде генератор паролей

Далее у Вас появится много вопросов, вот чт оя нашёл на форумах:

-Последние проблемы были лет 6-7 назад, когда система стала затыкаться на больших mailbox'ах и пришлось всё сконвертить в Maildir.

- в каком формате лучше хранить скажем 2 ТБ почты, как её бэкапить и так далле.

# master.cf

The -o ... options override the settings that are taken from defaults or define in the config, which we'll set later.

ВОПРОС допустим у меня несколько серверов и все они отсылают письма на logs@yandex.ru, так вот как я пойму какой из серверов прислал мне письмо. В поле отправитель буде же везде logs@yandex.ru ? может как то тему можно настроить ? Нашел решение, может кому будет полезно: Добавим в файл /etc/postfix/main.cf одну строчку:

header\_checks = pcre:/etc/postfix/rewrite\_subject

Теперь нужно создать файл /etc/postfix/rewrite\_subject и поместить в него правило, которое будет добавлять в тему письма дополнительный текст с именем сервера

/^Subject: (.\*)$/ REPLACE Subject: $1 (from server.domain.tld)

systemctl restart postfix

При отправке писем с другого SMTP-сервера нужно чтобы адрес отправителя в письме совпадал с реальным адресом отправителя (в частности, чтобы письма приходили на серверы mail.ru) нужно в фале /etc/posstfix/main.cf добавить строку

smtp\_generic\_maps = hash:/etc/postfix/generic

в самом файле /etc/postfix/generic добавить строку

root@server.mydomain.ru [реальное\_имя\_отправителя@mydomain.ru](mailto:реальное_имя_отправителя@mydomain.ru)

и создать хэш

postmap /etc/postfix/generic

перезапустить postfix

systemctl restart postfix

Добрый день, мы предлагаем вам в качестве дополнительной услуги настроить для вашего почтового сервера записи DKIM, SPF и DMARC. Что это такое и зачем это надо?

Корректно настроенные SPF, DKIM и DMARC уменьшают вероятность попадания отправленных вами писем в спам на стороне клиента и защищают от интернет-мошенничества.

Если вы отправляете рассылки, то могли заметить, что с помощью нехитрых манипуляций можно отправить письмо с любым обратным адресом, от имени любого отправителя.

Это используют мошенники. Выдав себя за приличную компанию (например, вашу), они крадут личные данные и деньги пользователей — занимаются фишингом.

# Борьба со спамом и начальная безопасность:

Напомню что в начале уровок мы выключили селинукс и фаерволл. Сейчас самое время вернуть всё обратно: настройку селинукс в этот курс включать смысла нету, а вот небольшой тюниг фаервольных правил и настроек упомянуть обязательно надо

Сравнить два спамореза в уроке рспамд и спамасасин паралелько скриптом рассылщиком. Прям скриптом генератором на два домена

postfix mail fow12682018.ppt 51 страница рестрикшены

## firewalld, iptables fail2ban: ловушки по логам dovecot, postfix.

Test your (inbound mail) spamfilter with https://www.emailsecuritycheck.net/

Test your (outbound mail) spammyness with https://www.mail-tester.com/

Перед началом настройки всего остального-или после, подумать, как лучше. Надо не забыть, что первый способ защиты почтового сервера это фаервольные правила. Не только на самом почтовике но и на входящем маршрутизаторе. Правила должны быть настроены так чтобы изнутри сети отправлять можно было только на ваш почтовик и никак иначе. Если рабочие станции будут иметь возможность коннектиться к другим почтовикам то в случае заражения вирусами рассылающими спам ваш внешний адрес и домен попадут во все возможные блеклисты и переписываться на анлгийском с их администрациями придется Вам. Поэтому изнутри наружу соединения на 25 порт должен делать только почтовик и никто больше.

Остаётся открытым вопрос после чего начинает ломиться спам на почтовый домен. У меня есть предположение что сначала спаммеры пробуют подключиться перебирая имена из словаря по imap и если получают пассворд мисматч а не юзер не найден –то ваш ящик попадает в базу рассылающих спам. Этот перебор можно сильно смягчить при помощи файл2бан. //обсудить

файил ту бан защитит от подборов и изнутри от инфицированных узлов

Напоминаю, что fail2ban имеет ловушки не только для ssh, но так же для dovecot, postfix. Надо научиться их применять и прикинуть как проверить эффективность. Тут надо привести цитату с хабра от человека, у которого подобрали пароль к учётке:

Первый его вопрос был: как подобрали — у меня же fail2ban там. И вот здесь как раз засада: не все представляют себе, что подбором паролей сегодня занимаются уже не отдельные компьютеры, а целые бот-сети, кстати поумневшие донельзя. Так вот по логам выяснили, что тут как раз такой случай: перебирала бот-сеть, причем на практике выяснившая его настройки в fail2ban (maxRetry=5, findTime=600 и banTime=600). Т.е. чтобы избежать бана, сеть делала 4 попытки в течении 10 минут с каждого IP. На минуточку в сети порядка 10 тысяч уникальных IP = что-то более 5 с половиной миллионов паролей в сутки. Кроме того, его почтовик делал большую глупость — а именно паузу до 10 секунд, при логине с неправильным именем. Т.е. выяснить, что некоторые имена, в том числе admin, реально имеются, этой сетке не составило труда.

Поэтому просто включаем её чуть ниже ловушки для ssh в конфиге fail2ban:

[sshd]

enabled = true

[dovecot]

enabled = true

а по postfix есть аж три джаила:

[postfix-rbl]

enabled = true

[postfix-sasl]

enabled = true

[postfix]

enabled = true

Включить надо аналогично, должно сильно сократить скорость роста файла /var/log/maillog от хостов выплняющих подбор паролей, перебор учётных записей разных почтовых ящиков по словарю-у меня это резко увеличилось под конец второго менсяца жизни сервера, до этого пока он был новый и никто в нитернете про него не знал-в логе было тихо а потом после подписки на ряд рассылок и последующей отписки- как попёрло. Ну, ещё можно для

[mysqld-auth]

enabled = true

[recidive]

enabled = true

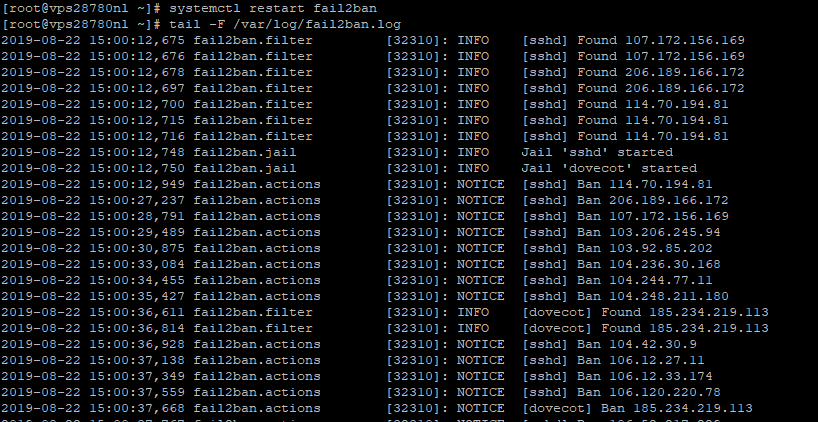
туда же надо добавлять правила, регеэкспы например на такое, это пассворд в бэйс 64, тоесть если эта строка появляется в логе-ее источник надо банить:

SASL LOGIN authentication failed: UGFzc3dvcmQ6

SASL LOGIN authentication failed: VXNlcm5hbWU6

Первое означает Password второе означает Username.

Но даже с fail2ban ботнеты в несколько тысяч узлов вычисляют параметры с которыми работает fail2ban и начинают щипать почтовик по чуть-чуть то с одного адреса, то с другого. Это ведет росту лог файла и тому что в fail2ban накопится скажем 2-3 тысячи уже забаненых узлов. Мне помогало в этом случае просто остановить почтовик на какое-то время, например на сутки и потом запустить. Атаки сильно падали //2020-03-28



**systemctl restart fail2ban**

**tail -F /var/log/fail2ban.log**

После запуска спустя какое-то время посматриваем результаты:

**fail2ban-client status dovecot**

**fail2ban-client status sshd**

у меня статистика эффектривности получилась такой: до включения было так:

--------------------- Postfix Begin ------------------------

3012 SASL authentication failed

2840 Miscellaneous warnings

После включения оно упало вот так:

--------------------- Postfix Begin ------------------------

36 SASL authentication failed

23 Miscellaneous warnings

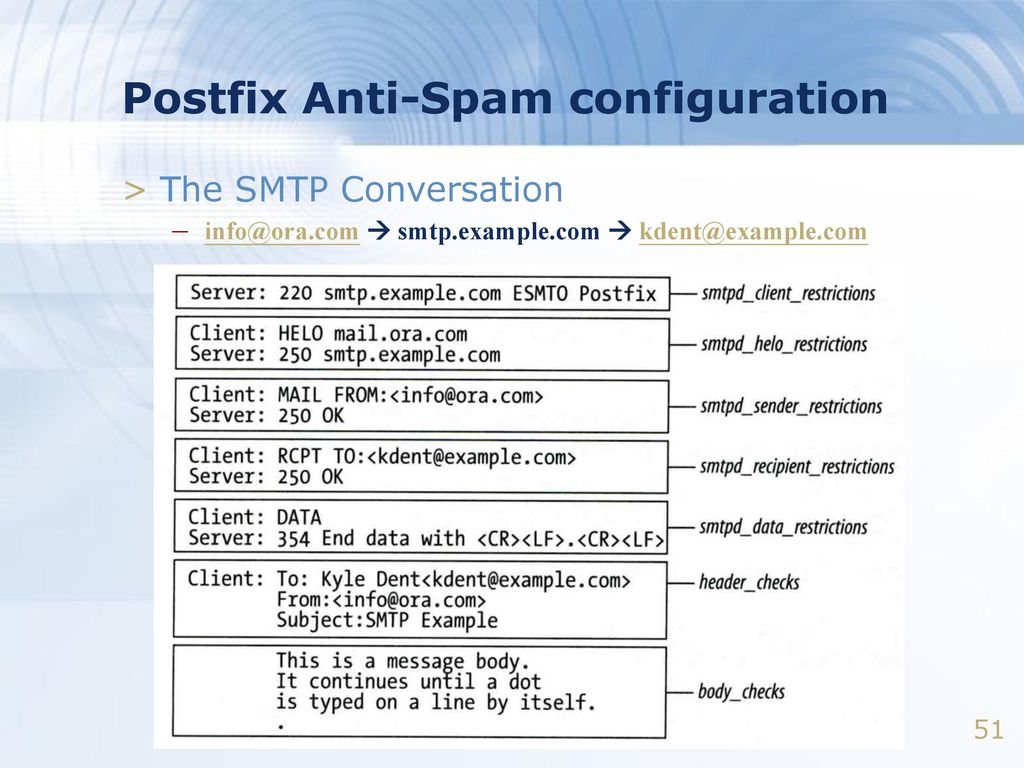
## длинные логины с точкой

Вот прямо сходу спам пошёл на ящики инфо и заказ.

Показать базу логинов на которые чаще всего ломятся. Этих ящиков быть не должно, инфо заменить ну хотя бы на информ, админ на админс и т.п.

Почти нету логинов с точкой вида петров.вс и

## Борьба со спамом: проверки в самом Postfix

## чёрный белый список.

Создаём файл

touch /etc/postfix/whitelist

Добавляем в него записи, можно конкретный ящик, можно все ящики домена, можно домен с под доменами.

user@examlpe.com OK

@examlpe.com OK

.example.ru OK

@mail.ru reject

@yandex.ru reject

Теперь преобразим наш файл whitelist в индексированную базу данных, выполнив команду:

postmap /etc/postfix/whitelist

Теперь смотрим каком типом БД пользуется наш postfix

postconf | grep database\_type

Возможные варианты ответа hash, btree или dbm

В зависимости от этого в секцию

smtpd\_sender\_restrictions

Добавляем строку

check\_sender\_access hash:/etc/postfix/whitelist

Вот как это выглядит у меня (не забываем про запятые после переменных) (вместо hash пишем свой тип БД)

smtpd\_sender\_restrictions =

check\_sender\_access hash:/etc/postfix/whitelist,

permit\_sasl\_authenticated,

permit\_mynetworks,

reject\_non\_fqdn\_sender,

reject\_unknown\_sender\_domain,

permit

## Борьба со спамом: сборка спам-фильтров Scrollout F1

Набор некоторых способов фильтрования спама объединен в различные сборки, которые можно выставлять наружу, например Scrollout F1 (Spam фильтр)

## Борьба со спамом: сборка спам-фильтров [Proxmox Mail Gateway](https://www.proxmox.com/en/downloads/category/proxmox-mail-gateway)

Сделано похоже на postfix, можно посмотреть нюансы настройки:

<https://www.proxmox.com/en/downloads/category/iso-images-pmg>

# DKIM

DKIM (DomainKeys Identified Mail - идентификация почты по доменным ключам) - метод, позволяющий связать идентичность доменного имени с отправляемым сообщением,

а также проверить идентичность доменного имени, связанного с входящим сообщением, с помощью криптографической аутентификации. Он позволяет организациям брать

на себя ответственность за отправляемые письма путём присоединения к ним автоматически сгенерированной цифровой подписи, а также использует криптографические

средства, чтобы проверять входящие письма на наличие такой подписи.

**yum install -y opendkim opendkim-tools**

**opendkim-genkey -D /etc/opendkim/keys/sumare.ru/ -d sumare.ru -s default**

**chown -R opendkim:opendkim /etc/opendkim/keys**

**vi /etc/opendkim/KeyTable**

default.\_domainkey.sumare.ru sumare.ru:default:/etc/opendkim/keys/sumare.ru/default

**vi /etc/opendkim/SigningTable**

\*@sumare.ru default.\_domainkey.sumare.ru

**vi /etc/opendkim/TrustedHosts**

91.235.129.43

mail.sumare.ru

**vi /etc/postfix/main.cf**

smtpd\_milters = inet:127.0.0.1:8891

non\_smtpd\_milters = $smtpd\_milters

milter\_default\_action = accept

milter\_protocol = 2

chkconfig opendkim on

systemctl start opendkim

systemctl status opendkim

vi /etc/opendkim.conf

и собственно в свой dns надо добавить TXT запись

default.\_domainkey

вот так, все в кавычках, без скобок, одной строкой:

"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCWQvsyiIna/SVcOSyxAkYPugx7qChsVrclMitI5krK1UTWNL2BamnfJAnK6qiTYEZJ0+g5oCPMwfvzw8hB3M0/XsyN/ENEX1rxbolNCHYkMeJXLfIEVtIgYWcu+tiHsE7VVxrI78H8UGex7ighEyUVXGbJ/yEU7EPtUWmOaAWlZQIDAQAB"

# SPF

(Sender Policy Framework - инфраструктура политики отправителя) - метод, используемый для предотвращения подделки адреса отправителя письма, то есть использования

фальшивого адреса отправителя. Он позволяет проверить, что входящая почта от определённого домена приходит с хоста, уполномоченного администратором этого домена.

Вот требовался однажды такой проверятор: This is **tumgreyspf**, an external policy checker for the postfix mail server. It can optionally greylist and/or use spfquery to check SPF records to determine if email should be accepted by your server.

# DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance - идентификация сообщений, создание отчётов и определение соответствия по доменному имени)

- это технология, расширяющая возможности методов SPF и DKIM. Политика DMARC определяет, что получатель должен делать с электронными сообщениями в зависимости

от результатов проверки DKIM и SPF.

# Готовые почтовики

Рассмотрим несколько мне кажется наиболее популярных сборок почтовиков в интернете. В них можно подсмотреть довольно интересные идеи конфигурирования. В принцыпе ничего не мешает их просто брать и использовать у себя в компании: пройденный ранее материал поможет Вам в дальнейшем обслуживании почтовика.

## iRedMail.

Для тех же, кому надо что бы работало «в два клика», dovecod+postfix+mysql с веб-доступом подымаются скриптом iRedMail.

<https://iredmail.org/download.html>

документацию смотрим тут:

<https://docs.iredmail.org/install.iredmail.on.rhel.html>

**yum install wget -y**

**wget https://bitbucket.org/zhb/iredmail/downloads/iRedMail-0.9.9.tar.bz2**

**tar xjf iRedMail-0.9.9.tar.bz2**

если не распакуется то у меня например просто небыло архиватора, его надо поставить ибо в минимал образе его нету:

**yum install bzip2**

переходим в распаковавшуюся папку

**cd /root/iRedMail-x.y.z/**

и запускаем установщик:

# **bash iRedMail.sh**

Эта и другие сборки ставятся долго с полчаса, наверное, ибо там качаются антивирусные базы и т.п так что запаситесь терпением. Когда установка завершится все настройки посмотрите в файле:

**cat iredmail.tips**

кстати пробежитесь глазами по содержимому самой исходной папки

\iRedMail-0.9.9.tar\iRedMail-0.9.9\ там есть скрипты, примеры конфигов и прочие полезные на потом вещи.

Для создания учётных записей и прочего администрирования почтовика переходим по адресу (iRedAdmin):

<https://192.168.109.249/iredadmin>

и вводим логин

[postmaster@sumare.ru](mailto:postmaster@sumare.ru)

11QQ22ww

Для чтения почтовых ящиков есть на выбор пару веб-клиентов:

Roundcube webmail: https:// 192.168.109.249/mail/

SOGo Groupware: https://192.168.109.249/SOGo/

Awstats: httpS:// 192.168.109.249/awstats/awstats.pl?config=web (or ?config=smtp for SMTP traffic log)

У меня эта статистика не работала.

## Mail-in-a-Box.

как ускорить и облегчить внедрение клиентам для аутсорсеров проект <https://mailinabox.email/> показать развёртывание и схему той картинкой, подсказать что там можно подсмотреть непонятные нюансы конфигурирования. Эта сборка заточена под установку на убунту сервер а не на центос, поэтому качаем образ отсюда:

https://ubuntu.com/#download

You must choose the Ubuntu 18.04 x64 (server edition) operating system and a machine with at least 512 MB of RAM.

Для тестового стенда чтобы установщик не ругался добавим чтобы резолвилось:

**vi /etc/hosts**

box.sumare.ru 127.0.0.1

затем запускаем скрипт-установщик всего:

**curl -s https://mailinabox.email/setup.sh | sudo -E bash**

Эта и другие сборки ставятся долго с полчаса, наверное, ибо там качаются антивирусные базы и т.п так что запаситесь терпением. Чтобы потом перенастроить ответы, или если отвалилось по разным причинам как у меня пару раз просто перезапустите его заново, выполненные шаги он проверит, пропустит и доделает остающееся

**sudo mailinabox**

у меня ставилось, наверное, час. После установки пробуем заходить на веб-интерфейс, меня пустило раза с третьего через час.

<https://ip-вашей-виртуалки/admin>

<https://192.168.109.57/admin>

[postmaster@sumare.ru](mailto:postmaster@sumare.ru)

11QQ22ww

Читать почту можно через раундкуб вот тут

<https://192.168.109.57/mail/>

## Modoboa.

Ещё одна довольно серьёзная сборка почтовика. Документация по установке и всё остальное тут

[https://modoboa.readthedocs.io/en/latest/index.html#](https://modoboa.readthedocs.io/en/latest/index.html)

Установка сжато на минимал центосе:

**yum install git**

**git clone https://github.com/modoboa/modoboa-installer**

у Вас после этого в текущей папке появится папка modoboa-installer, переходим в неё:

**cd modoboa-installer**

и запускаем через точку лежащий в ней установщик указав свой домен почты:

**sudo или # ./run.py <your domain>**

Эта и другие сборки ставятся долго с полчаса, наверное, ибо там качаются антивирусные базы и т.п так что запаситесь терпением. По завершении установщика пробуем зайти на

https://192.168.109.248/

дефолтные учётные данные почтовика:

admin/password

## Ubermail Stackfocus Ansible roles

Следующие два готовых почтовика делаются как роли ансибл из сообщества ансибл-галакси

Есть ещё много вариантов, посмотреть можно тут:

<https://github.com/search?p=4&q=dovecot&type=Repositories>

https://mailu.io/1.7/faq.html

https://gitlab.com/simple-nixos-mailserver/nixos-mailserver

<https://mailcow.email/>

https://mailu.io/1.7/ Mailu is a simple yet full-featured mail server as a set of Docker images.

## Ускорение и облегчение с помощью ViMbAdmin (vim-be-admin).

Ещё один из веб-интерфейсов управления связкой postfix dovecot (vim-be-admin) можно поизучать тут:

<https://www.vimbadmin.net/>

инструкция по установке

<https://github.com/opensolutions/ViMbAdmin/wiki/Installation>

sudo apt-add-repository ppa:ondrej/php

sudo apt-get update

sudo apt-get install php7.0-cgi php7.0-mcrypt php-memcache php7.0-json php7.0-mysql php-gettext libapache2-mod-php7.0

export INSTALL\_PATH=/srv/vimbadmin

sudo git clone https://github.com/opensolutions/ViMbAdmin.git $INSTALL\_PATH

sudo apt install composer

sudo composer install –dev

sudo wget <https://dev.mysql.com/get/mysql-apt-config_0.8.14-1_all.deb>

sudo dpkg -i mysql-apt-config\_0.8.14-1\_all.deb

sudo apt-get update

sudo apt-get install mysql-server

sudo service mysql status

sudo mysql -p

**11qq22ww**

CREATE DATABASE `vimbadmin`;

CREATE USER 'vimbadmin'@'localhost' IDENTIFIED BY 'password';

GRANT ALL ON `vimbadmin`.\* TO `vimbadmin`@`localhost`;

FLUSH PRIVILEGES;

<https://ubuntu.com/#download>

php -r "copy('https://getcomposer.org/installer', 'composer-setup.php');"

php -r "if (hash\_file('sha384', 'composer-setup.php') === 'a5c698ffe4b8e849a443b120cd5ba38043260d5c4023dbf93e1558871f1f07f58274fc6f4c93bcfd858c6bd0775cd8d1') { echo 'Installer verified'; } else { echo 'Installer corrupt'; unlink('composer-setup.php'); } echo PHP\_EOL;"

php composer-setup.php

php -r "unlink('composer-setup.php');"

apt-get update

apt-get install libapache2-mod-php7.0 php7.0-curl php7.0-cli php-memcache php-memcached php7.0-mysql php7.0-pgsql php7.0-gd php7.0-imagick php7.0-intl php7.0-mcrypt

sudo apt-get -y install memcached

sudo apt install php-mysql

sudo ./bin/doctrine2-cli.php orm:schema-tool:create

проверяем что таблицы-создались:

mysql -uvimbadmin –p

password

use vimbadmin;

show tables;

Антиспамы

Чаще всего с самого начала щимились на эти адреса:

[demo@sumare.ru](mailto:demo@sumare.ru) UGFzc3dvcmQ6 is base64 for 'Password:'

[ftp@sumare.ru](mailto:ftp@sumare.ru)

spam@sumare.ru

[library@sumare.ru](mailto:library@sumare.ru)

[staff@sumare.ru](mailto:staff@sumare.ru)

[postletter@sumare.ru](mailto:postletter@sumare.ru)

[webmaster@sumare.ru](mailto:webmaster@sumare.ru)

[news@sumare.ru](mailto:news@sumare.ru)

[sales@sumare.ru](mailto:sales@sumare.ru)

[office@sumare.ru](mailto:office@sumare.ru)

[admin@sumare.ru](mailto:admin@sumare.ru)

[lab@sumare.ru](mailto:lab@sumare.ru)

(lp@sumare

[nagios@sumare.ru](mailto:nagios@sumare.ru)

[com@sumare.ru](mailto:com@sumare.ru)

[scan@sumare.ru](mailto:scan@sumare.ru)

[test2@sumare.ru](mailto:test2@sumare.ru)

test1@sumare.ru

[test@sumare.ru](mailto:test@sumare.ru)

[guest@sumare.ru](mailto:guest@sumare.ru)

[orders@sumare.ru](mailto:orders@sumare.ru)

[claims@sumare.ru](mailto:claims@sumare.ru)

[help@sumare.ru](mailto:help@sumare.ru)

[tech@sumare.ru](mailto:tech@sumare.ru)

[operator@sumare.ru](mailto:operator@sumare.ru)

[shop@sumare.ru](mailto:shop@sumare.ru)

newsletter@sumare.ru

добавим их чтобы принимать больше спама для тренировки спамфильтров. А, кстати, такие ящики-у себя не создавать.

useradd admin -m -s /sbin/nologin

useradd office -m -s /sbin/nologin

useradd sales -m -s /sbin/nologin

useradd news -m -s /sbin/nologin

useradd webmaster -m -s /sbin/nologin

useradd postletter -m -s /sbin/nologin

useradd staff -m -s /sbin/nologin

useradd library -m -s /sbin/nologin

useradd spam -m -s /sbin/nologin

useradd ftp -m -s /sbin/nologin

useradd demo -m -s /sbin/nologin

useradd lab -m -s /sbin/nologin

useradd -m -s /sbin/nologin

useradd -m -s /sbin/nologin

useradd -m -s /sbin/nologin

# Roundcube веб-интерфейс для лазанья по почте

Roundcube понадобится не сколько как аналог OWA эксченджа, с него проще раздавать права пользователям на свои папки другим пользователям.

Для раундкуба надо чтобы почтовик **уже работал**, ибо на одном из этаопв настройки он попросит проверку захода по аймап и смтп, причем на последний не просто на 25 порт на на субмишн порт который надо включить.

**vim /etc/postfix/master.cf**

раскомментируем строку

*submission inet n - n - - smtpd*

перезапускаем почтовик и проверяем что порт начал слушаться

**systemctl restart postfix**

**telnet 192.168.5.250 587**

Далее делал по статье моска, сохранил у себя

Идём в раздел загрузок раундкуба и качаем оттуда последнюю Complete версию:

**wget https://github.com/roundcube/roundcubemail/releases/download/1.4.6/roundcubemail-1.4.6-complete.tar.gz**

**tar zxvf roundcubemail-1.4.6-complete.tar.gz**

**/etc/nginx/nginx.conf**

**listen 192.168.5.250:80**

**nginx -s reload**

# SquirrelMail веб-интерфейс для лазанья по почте

# Контакты давших хорошие ответы

После отправки первой версии курса курс-в чат телеграм линуск чаты, потом повторно типа не забыл ли

https://www.linux.org.ru/forum/general/14041429

Twissell@fex.net

DeadLoco

<https://www.opennet.ru/openforum/vsluhforumID1/95287.html>

Mavrikii

<http://forum.ru-board.com/topic.cgi?forum=8&topic=81497>

casperonius

https://sysadmins.ru/topic434679.html

<https://www.dmosk.ru/kontakti.php>

Телефон: +7(906)250-48-69

Эл. почта: master@dmosk.ru

Мессенджеры: Viber WhatsApp

Skype: dmosk.ru

E-mail: ilya.evseev@gmail.com

Дал хороший ответ на <https://toster.ru/q/61150>

E.Vasilyev [bq@bissquit.ru](mailto:bq@bissquit.ru) Егор Васильев

<https://github.com/bissquit/postfix-dovecot-maildir>

https://notessysadmin.com/about

admin@notessysadmin.com

# История правок:

2016-11-30

2017-01-

2018-04-08

2018-08-21..2018-08-28

2018-09-08, 10,

2018-10-09 составить план слайд курса по постфиксу и довекоту на основе глав шпаргалки:

2018-10-25

2019-01-04

2019-03-18

2019-06-11

2020-05-26 цветовой редактор [Visual Studio Code](https://code.visualstudio.com/)и гит цветной консольный редактор джое или вим

2020-06-03 прикрутил бинд чтобы сделать 2 виртуалки, причём как-то легко. Теперь эксперименты пойдут быстрее, а когда-то уже на этом стопорился

2020-06-13 у тандерберда экстеншн ацл не работает с новой версией, надо искать старую

2020-08-15 без хоум иогут крашиться модули

2020-08-16 первая заглавная страница

# Рассмотреть:

Установка из исходников //поставлено 2020-08-27./configure --help dovcot

Тсп дамп плаина от тандера в диагностику, рвутся сессии//поставлено 2020-08-27

В благодарность ссемаеву

curl  is  a  tool  to transfer data from or to a server, using one of the supported protocols (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPS,

       TELNET and TFTP). The command is designed to work without user interaction.

DOVECOT

yum install epel-release

В рсислог должно высыпать пользователю в консоль

mail.debug asat

<https://workaround.org/ispmail/buster/whats-new-in-the-buster-guide/>

добавить

cat <<EOF >index.html

daleee mnongo

rasnogo texta

openssl  s\_client -tls1\_2 -connect mx1.mydomain.ru:587

openssl  s\_client -tls2\_3 -connect mx1.mydomain.ru:587

EOF

2017-01-17 16:30:28 2.1.1.12.

2.1.5.

2.1.6.

update-exim4.conf --keepcomments --output /etc/exim4/exim4.conf

тяжко идет. все подорожало. безденежное вермя

2.3.2.

**2017-01-19** 17:31:45

[http://**wiki2.dovecot.org**/FindMailLocation](http://wiki2.dovecot.org/FindMailLocation)

<http://wiki2.dovecot.org/BasicConfiguration>

<http://wiki2.dovecot.org/RunningDovecot>

Давно уже взял за правило - при поднятии любого почтосервера, который будет работать с внешним миром:

1. Проверить, что mail.domain.com указывает на адрес сервера, убедиться, что PTR адреса сервера указывает на mail.domain.com

2. primary\_hostname = mail.domain.com (в Exim. Так мы представляемся собой остальным)

3. domainlist relay\_to\_domains = domain.com (так мы разрешаем релей почты для основного домена

4. SPF-запись в DNS - "v=spf1 a mx ip4:1.2.3.4 ~all"

5. Генерация DKIM-сертификатов для domain.com, конфигурация DNS и Exim на работу с этой подписью.

5а. В запущеных случаях - настройка SPF и DKIM для домена mail.domain.com, для писем, генерируемых самим сервером.

6. Тестовое письмо на ящик в яндексе, чтобы увидеть зеленый шильдик о том, что DKIM настроен верно.

7. Чуть не забыл - в /etc/aliases строку "root: [vasya.pupkin@gmail.com](mailto:vasya.pupkin@gmail.com)" (вкупе с "webmaster: root"), затем newaliases чтобы получать отчеты об отлупах.

Смпт руками поможет разобраться когда рвутся сессии, на каких этапах.

В рсислог должно высыпать пользователю в консоль

mail.debug asat

информация о пакетах в указанном репозитории

yum repo-pkgs gf list

https://github.com/LukeSmithxyz/emailwiz

под контролем имею ввиду, например:

- скрытая перенаправление всех входящих

- скрытая перенаправление всех исходящих

- групповая настройка УЗ (например, открючить, перенаправить и т.д.)

- фильтрация по ключевым словам в теме\ в писме

- фильтрация по вложенным файлам (doc, pdf, bat, exe......)

echo "0JDQtNC80LjQvdC40YHRgtGA0LDRgtC+0YDRiyDQtNC+0LzQtdC90LA=" | base64 -d

Администраторы домена

# echo "0JDQtNC80LjQvdC40YHRgtGA0LDRgtC+0YDRiw==" | base64 -d

Администраторы

curl --url "imap://lira.msk.vbrr.loc/" --user "boddy:tables"

• imap: 143, 993

• pop3: 110, 995

• smtp: 25, 587, 465

По умолчанию этот модуль не собирается, его сборку необходимо разрешить с помощью конфигурационного параметра --with-mail.

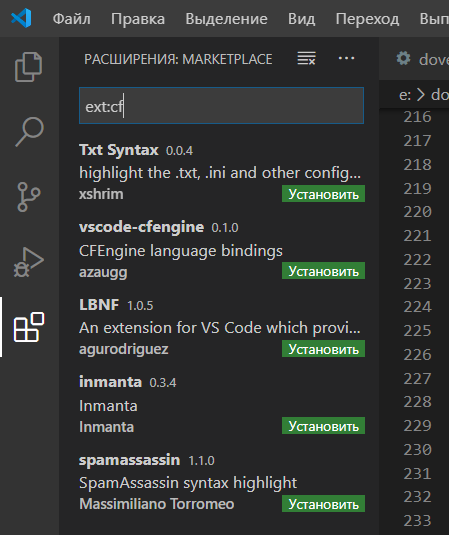
По сравнению с Docker Swarm, Kubernetes функционально богаче, но обладает более высоким порогом вхождения в технологию.

Gropware: календари, адресные книги, если силы остануться

Настраивать только в 2файлах чтобы люди не путались

Эксчендж довкот адэ автодискаверинг.

Редактор с подсветкой синтаксисаVisual Studio Codehttps://code.visualstudio.com/ показать что там есть даже спамассасин синтаксис



Разбить параметры цветами на секции Em verde e amarelo и слайд на каждую

Сделать цветами [asat@sumare.ru](mailto:asat@sumare.ru) соответственно%d %n

~~Где узнавать возможные и дефолтные значения параметров?~~

аутентификация, база проверок паролей и база параметров пользователя,

-чёрно голубая тема как в рива бернер для оформления слайдов

Вывести может версии ос и довкотов

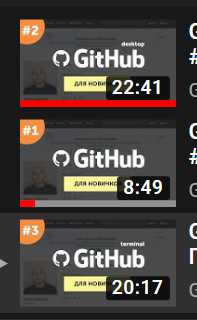
Если чего-то нет это надо создать чтобы не от меня отвязалось

Позиции ансибля я глянул по новому на задачи ская, например гашение вм по добавочномк

Ссмартхост приёма нескольких доменов, пассдб адишионал параметр прокси мэйби-форвардит на другой бэкэнд!

визио сервер с эмблемой постфикс, нджинкс

белый фон черные буквы легче читаются



простейшие проверки аутентификации, кодировки, на чем подкололся с кодировками http://winitpro.ru/index.php/2017/08/11/otpravka-pisma-iz-telnet-s-smtp-avtorizaciej/

~~аутентификация pop3, imap4 по шагам~~

~~дебаггинг аутентификации~~,

коды отлупов довекота

smtp сессия с аутентификацией, виды механизмов аутентификации, кто-то где-то упомянул что Единственное — я не стал отключать плэйнтекстовые логины, т.к. почту у нас используют в т.ч. принтеры, а они через SSL работать не умеют.

~~её величество smtp сессия без аутентификации, проверки на этапах,~~ отправка через графический клиент,

рассмотреть поля емайла, прям расписать что каждое значит: конвертный адрес, майм-адрес.: в мозилла more-view source.

виды почтовых форматов с картинкой маилхоум папка инбокс с картинкой из dovecot-intro

Письмо, которое я ждал, не пришло, как разобраться?

утилиты администрирования с примерами на типовые возникавшие задачи:

~~операции по ящикам типа поиск и удаление писем~~,

отключение/включение ящика,

Перенос ящика в другой сторидж альт, конвертация

Сиев, автоответы отпуска

Нджинкс плюс довкот аналог ддимайла

лун-кусок сториджа только для одного инициатора?

айскази –монтировать как раздел для почты, мультипасинг, как клонировать лун?

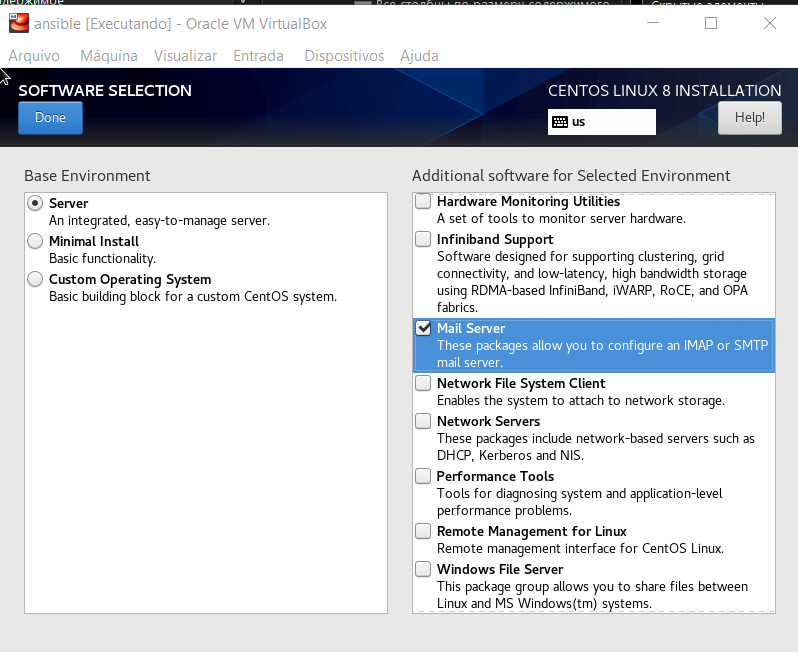
Алиас-акела парчи антиш ахоба

коннект нового пользователя к старому ящику

пастас компарчильядас.

Глобальный каталог адресов.

При установке центос был выбор установки маил сервер-посмотреть что это такое



Коллеги, добрый день.

У некоторых пользователей в старой почтовой системе были заведены дополнительные почтовые ящики, например с номером телефона. Есть два варианта как реализовать такую схему на новом почтовом сервере.

1. Создать alias, т.е. дополнительный адрес электронной почты к вашему существующему почтовому ящику.

2. Создать отдельный почтовый ящик и подключить его в Outlook.

При первом варианте вы не сможете отправлять письма от имени дополнительного адреса, но зато у вас будет один ящик в который будут приходить письма со всех ваших адресов.

При втором варианте вы сможете отправлять письма с дополнительного почтового ящика, но два ящика - это двойная работа. В случае вашего отсутствия переадресацию надо включать на обоих ящиках. Этот ящик надо отдельно подключать в Outlook и еще не известно как он себя поведет на мобильном телефоне.

При формировании заявки пожалуйста сообщайте как вам надо подключить дополнительный адрес, в виде дополнительного почтового адреса или отдельного ящика.

выдача прав второму пользователю,

общие ящики,

перенос ящиков,

экспорт почтового ящика в/из .pst

разобраться почему черновик в аквамаил можно редактировать а в аутлуке уже нет.

веб-интерфейсы управления почтовиком postfixadmin (Postfixadmin-CLI can be used to create mailbox users or aliases by command line.)

Вычитать статьи на https://github.com/opensolutions/ViMbAdmin/wiki/Full-setup-installation-%28ViMbAdmin-postfix-dovecot%29

веб-интерфейсы для лазанья по почте horde/imp: A web based webmail system

антиспамы какие антиспамы чаще требуются, Почтовый фильтр Procmail,

spamassasin

postgrey

Вместо костыльного spamassassin имеется приятный и технологичный rspamd

Вместо SpamAssassin можно использовать dspam. попробуйте dspam

rf по пунктам антиспам,

простой релей для эксченджа

антивирусы Антивирусы drweb ClamAV и прочие антивирусные проверки почты

Postgrey + Postscreen + Sieve

интеграция с AD

обслуживание, мониторинг zabbix

бэкапы, аварийное восстановление Отработать восстановление письма и ящика

спаять всё это с той схемой курсов по постфиксу.

показать про плюс между ящиками,

автоответчик по отпускам, а после, как выяснилось, и пересылка писем по правилам sieve, если таковые устанавливал пользователь в roundcube или thundebird через managesieve.

генераторы е-майлов Mail2 из папки эксченджа

транспортные правила, берклидибишная база

Объемы спама в общем трафике вообще радуют конечно — сделал ящик на своем домене, куда все письма складываются пришедшие на несуществующие адреса (моего домена)

разбор параметров конфигурации по примеру

|  |  |
| --- | --- |
| Синтаксис: | **ignore\_invalid\_headers** on | off; |
| Умолчание: | ignore\_invalid\_headers on; |
| Контекст: | http, server |

DKIM: OpenDKIM, OpenDMARC Интересно, а поддержка DKIM у него входящяя или исходящяя (в смысле отправленные имейлы подписаны сертификатами)?

почта для нескольких доменов

кластеризация lsyncd не пробовали для синхронизации стораджей? isync: free IMAP and MailDir mailbox synchronizer

Install Webmin if you want a web-based interface to manage your mail accounts.

Лулу 1:40 в заставку или полисия пара кем пресиза ди полисия начало

Сделать дизайн заглавной страницы как письмо, эмблемы сделать как марки с зубчатой линией вокруг.

спам-фильтров ORF\GFI

The Anti-Spam SMTP Proxy (ASSP)

SOGo supports standard groupware capabilities including CalDAV, CalDAV auto-scheduling, CardDAV, WebDAV Sync, WebDAV ACLs, and iCalendar.

Peer Heinlein: Dovecot - POP3/IMAP-Server für Unternehmen und ISPs

Бесплатный днс домен \*.prohoster.biz 0 $

Заставка сэмпл из полисиа пара кей пресиза джи полисия инисио 13 MLADEK IVAN - Side By Side. Фим 08. Šuškavý víno.mp3

Ou Linda Fazenda em Tocantins

Laid Back - Sunshine Reggae

prosy\_pass

https://iaas-blog.it-grad.ru/funkcionalnost/perenos-microsoft-exchange-v-oblako-pyat-prakticheskix-rekomendacij/

Оделл приводит пример, в котором компания переносит в облако 12 Тб данных, которые используют 8 тыс. пользователей. Ограничивающим фактором здесь выступает то, насколько быстро возможно осуществить перенос. Учитывая, что в среднем за час переносится 20 Гб данных, мы получаем 614 часов, необходимых для завершения процесса, или 50 дней при условии, что каждый день на миграцию уходит 12 часов. Такие сроки для миграции приемлемы. Если же за час удается скопировать 2 Гб данных, на их перенос с учетом затраченных 12 часов в сутки уйдет минимум 500 дней, а это не очень хороший показатель.

Что мониторить в почтовике? Ну, наверное свободное место, частоту отправки от пользователей, явно что 100 писем в час говорит о заломаном пароле, а, ещё длину очередей

# Рассмотрено

-вывести дату и город, +

Даркмайклу благодарность. +

Если возможно, в других Ваших видео-уроках , добавляйте пожалуйста подсвечивание положения курсора+

Git+

# Разгрести:

Плаин ваиршарком от тандерберда снять

dovecot-pigeonhole последнее это что такое?? взято из https://habr.com/post/166487/

## ACL

Тема вызывает, наверное, наибольшее количество непонимания судя по вопросам на форумах. Ну, первое с чего можно начать диагностику это вывод прав на папку при попытке выбрать её в аймап сессии командой селект:

aa1 SELECT INBOX.testfolder

там внизу MYRIGHTS покажет имеющиеся права на папку

<https://addons.thunderbird.net/ru/thunderbird/search/?q=acl&appver=&platform>=

у тандерберда экстеншн ацл не работает с новой версией, надо искать старуюThere is a Version pending (since 5 Months currently) which fixed TB 60, use github Download until Mozilla releases the new Version.

https://github.com/dasTor/imap-acl/releases

Перед правкой файла-скопируй его

## Есть ли готовые докерные контейнеры

Ставим докер и просто делаем поиск по названию программ:

docker search dovecot

docker search postfix

читаем описания, ставим например вот этот:

docker pull marooou/postfix-roundcube

останавливаем все

docker run marooou/postfix-roundcube

## EHLO

telnet mail.itband.ru 25

ehlo

mail from:[1@2.ru](mailto:1@2.ru)

rcpt to:[1@3.ru](mailto:1@3.ru)

data

Subject:test-spam

some text

.

ограничения в postfix

smtpd\_client\_restrictions =

permit\_mynetworks,

permit\_sasl\_authenticated,

check\_client\_access hash:/etc/postfix/whitelist,

**check\_sender\_access hash:/etc/postfix/whitelist,**

# reject\_unknown\_client

reject\_rbl\_client bl.spamcop.net

# reject\_rbl\_client zen.spamhaus.org

permit

на основе этого объяснить все эти хэш и прочие dict.

AMaViS

Что поддерживает iRedMail для защиты почты:

1. Поддержка SPF (Sender Policy Framework).

2. Поддержка DKIM (DomainKeys Identified Mail).

3. Поддержка Greylist.

4. Поддержка «Белых списков» ( на основании DNS имени и IP адреса)

5. Поддержка «Черных списков» ( на основании DNS имени и IP адреса)

6. Поддержка «Черного списка» HELO запросов.

7. Поддержка HPR (HELO Randomization Prevention)

8. Поддержка Spamtrap.

9. Интерграция SpamAssassin

10. Интеграция ClamAV, автообновление вирусных баз.

In /etc/dovecot:

1. /etc/dovecot/10-mail.conf (line 10) I set:

mail\_location = maildir:~/Maildir:LAYOUT=fs

2. /etc/dovecot/20-imap.conf (line 57) I set:

imap\_client\_workarounds = tb-extra-mailbox-sep

Добавить исправление известнх ошибок почтовых

Климентов:

imap client workarounds = outlook-idle

Создадим символическую ссылку для того, чтобы вся почта хранилась в /var/mail/company:

#ln -s /var/mail/company /home/company/Maildir

Маппинги User<‐>password

hosts

10.77.7.89 pg10cnts7.ok.ru pg10cnts7

Теперь у вас есть FQDN, который будет использоваться почтовым сервером.  
4down vote

You need to know the differences between smtpd and smtp in Postfix. In short, [smtpd](http://www.postfix.org/smtpd.8.html) is the SMTP server that **receive** the email and [smtp](http://www.postfix.org/smtp.8.html) is the SMTP client that **send** the email.

|  |
| --- |
| Шпаргалка Postfix  Автор: |
| Вывод количества сообщений в очереди. **# postqueue -p | grep -v "^[^0-9A-Z]\|^$" | wc -l**    Вывод списка сообщений в очереди  **# postqueue -p**    Пример:  C67B97A0E42     2128 Sun Jun  8 17:00:41  support@domain.com                                           gusso79@domain.net    где:  **C67B97A0E42** - ID сообщения **2128** - размер сообщения **support@domain.com** - email отправителя **gusso79@domain.ne**t - email получателя    Просмотр сообщения в очереди: **# postcat -q ID\_сообщения**    Отправить сообщение вне очереди по ID сообщению  **# postqueue -i ID\_сообщения**    Отправить сообщение вне очереди по домену **# postqueue -s damain.com** Повторная отправка всех сообщений в очереди  **# postsuper -r ALL**    Скрипт для поиска спамера в очереди. Формирование списка сообщений по количеству писем от отправителя:  **# postqueue -p | grep -v "^[^0-9A-Z]\|^$" | awk '{print $7}' | sort -rn | uniq -c | sort -rn**    **Удаление сообщения из очереди:**  **#  postsuper -d ID\_сообщения**    Удаление сообщений из очереди от email  **# postqueue -p | grep support@doamin.com | awk '{print $1}' | xargs -n1 postsuper -d**   Удаление всех сообщений из очереди **# postsuper -d ALL** |

При обновлении системы или постфикса или довкота ваши настройки в /etc могут быть утрачены.

\етц.рассвд \* значит что пользовательне может входить в системы

Метод фильтрации До Получения срабатывает, когда сервер отправителя только что указал адрес получателя (RCPT TO command) и ждет подтверждение от вашего сервера. На этом этапе содержимое письма пока не передано, но ORF уже может принять решение относительно письма: например, если сервер отправителя был замечен в распространении спама, ORF отклонит запрос.

Немного погодя в действие вступает метод фильтрации После Получения, когда сервер отправителя передает письмо и ждет подтверждения. Поскольку содержимое письма становится доступным, ORF может осуществить более глубокий его анализ и произвести больше действий, чем при методе фильтрации До Получения, например, перенаправить письмо или отправить его в ящик для спама пользователя.

отчеты об отклонении (известные как NDRs или DSNs) и забрасывать ими невиновных псевдо-отправителей. Этот феномен и называется обратным рассеянием. Чтобы избежать этого, мы рекомендуем использовать присваивание ярлыков письмам вместо отклонения.

## DNS, MX, SPF, BIND

Перед правкой файла-скопируй его

Для начала надо чтобы у нас правильно резолвилась зона ok.ru только в наш почтовик как можно посмотреть на любом другом:

***host -t mx sky-dynamics.ru***

***host -t a mail3.sky-dynamics.ru***

чтобы эта сетевая утилита заработала, необходимо установить пакет bind-utils:

***yum -y install bind-utils***

appliance@zabbix:~$ telnet 172.25.30.2 25

Trying 172.25.30.2...

Connected to 172.25.30.2.

Escape character is '^]'.

220 mail.nawinia.com Microsoft ESMTP MAIL Service ready at Fri, 30 Aug 2019 11:07:46 +0300

451 4.7.0 Timeout waiting for client input

doveadm log find

pwgen 16 вроде генератор паролей

Если вы используете Ubuntu в качестве ОС для Zimbra, то установить программу можно при помощи команды sudo apt-get install imapsync -y, в CentOS и RHEL установка будет осуществляться при помощи команды sudo yum install imapsync -y.

yum install dnsmasq dnsmasq-utils

## [postfix: замена поля from](https://it-e.ru/blogs/administrirovanie/postfix-zamena-polya-from)

Разместил авг 27, 2013 | Метки: [nix](https://it-e.ru/blogs/administrirovanie?tag=nix&key=tags), [mail](https://it-e.ru/blogs/administrirovanie?tag=mail&key=tags), [postfix](https://it-e.ru/blogs/administrirovanie?tag=postfix&key=tags), [rewrite](https://it-e.ru/blogs/administrirovanie?tag=rewrite&key=tags) | [Комментарии (0)](https://it-e.ru/blogs/administrirovanie/postfix-zamena-polya-from#comments)

Изменим поле "From" при отравке письма с помощью MTA Postfix

Иногда при отправке необходимо заменить отправителя письма. Такое бывает нужно, например, для конфигурации отправки писем с хоста от некоего локального пользователя, потому что программист пользовался функцией mail - знакомо?

Итак, vi /etc/postfix/main.cf

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1  2  3 | mydomain = it-e.ru  inet\_interfaces = all  smtp\_generic\_maps = hash:/etc/postfix/generic |

Теперь vi /etc/postfix/generic

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1  2 | root@it-e.ru no-reply@it-e.ru  @it-e.ru no-reply@it-e.ru |

Собираем хеш:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1 | postmap /etc/postfix/generic |

Перезапускаем:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1 | /etc/init.d/postfix restart |

В версия младше 2 (вряд ли у вас такая будет), эта опция называлась sender\_canonical\_maps. В остальном все так же.

## [postfix: удаление заголовков](https://it-e.ru/blogs/administrirovanie/postfix-rewrite)

Разместил авг 27, 2013 | Метки: [nix](https://it-e.ru/blogs/administrirovanie?tag=nix&key=tags), [mail](https://it-e.ru/blogs/administrirovanie?tag=mail&key=tags), [postfix](https://it-e.ru/blogs/administrirovanie?tag=postfix&key=tags), [headers](https://it-e.ru/blogs/administrirovanie?tag=headers&key=tags) | [Комментарии (0)](https://it-e.ru/blogs/administrirovanie/postfix-rewrite#comments)

Для повышения безопасности системы часто необходимо скрыть некую техническую информацию о ней, которая доступна в заголовках писем, получаемых из этой системы.

Рассмотрим способ удаления лишных информационных записей в заголовках писем. Это необходимо для удаления информации о релее, ид локального пользователя или сокрытия информации о обработчиках сообщения.

редактируем конфиг main.cf:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1 | header\_checks = regexp:/etc/postfix/header\_checks |

Теперь сделаем файл /etc/postfix/header\_checks:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1  2  3  4  5 | /^Header: IfContains/ IGNORE  /^Received: from 127.0.0.1/ IGNORE  /^User-Agent:/ IGNORE  /^X-Mailer:/ IGNORE  /^X-Originating-IP:/ IGNORE |

Каждая строка, помеченная IGNORE, содержащая текст между "/^" и "/", будет удалена. Приведу пример очищения заголовков от результатов работы SpamAssassin:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11 | /^Header: IfContains/  IGNORE  /^Received:/    IGNORE  /^User-Agent:/  IGNORE  /^Message-ID:/  IGNORE  /^X-Mailer:/    IGNORE  /^X-MimeOLE:/   IGNORE  /^X-MSMail-Priority:/   IGNORE  /^X-Spam-Status:/   IGNORE  /^X-Spam-Level:/    IGNORE  /^X-Sanitizer:/     IGNORE  /^X-Originating-IP:/    IGNORE |

Уверен, что теперь вы легко приведете заголовки своих писем в порядок.

## [Лимитирование трафика postfix](https://it-e.ru/blogs/administrirovanie/limitirovanie-trafika-postfix)

Разместил сен 27, 2015 | Метки: | [Комментарии (0)](https://it-e.ru/blogs/administrirovanie/limitirovanie-trafika-postfix#comments)

Лимитирование трафика postfix поможет несколько угомонить локальных и внешних спамеров, не терять сообщения при работе через смтп-провайдера и многое другое.

Для ограничения трафика в postfix можно использовать следующие переменные:

* **initial\_destination\_concurrency** = количество одновременных доставок возможно первоначально. (по умолчанию 5 )
* **smtpd\_client\_event\_limit\_exceptions** = клиенты, которые исключены из подсчёта (по умолчанию: $mynetworks)
* **anvil\_rate\_time\_unit** =период времени, в течение которого рассчитываются показатели. (default: 60s)
* **anvil\_status\_update\_time** = как часто писать в лог статистику. (default: 600s)
* **default\_client\_message\_rate\_limit** = максимальное количество сообщений, которое клиент имеет право отправить в период времени. (default: 0)
* **smtpd\_destination\_concurrency\_limit** = сколько одновременных доставок. (по умолчанию: 100)
* **smtpd\_destination\_rate\_delay** = задержка между отдельными доставками на один и тот же домен
* **smtpd\_destination\_recipient\_limit** = максимальное количество получателей письма (по умолчанию: 50)
* **smtpd\_error\_sleep\_time** = время задержки ответов клиенту. Значение должно быть больше smtpd\_soft\_error\_limit и меньше smtpd\_hard\_error\_limit
* **smtpd\_soft\_error\_limit** = количество ошибок в смтп-сессии перед замедлением сессии на smtpd\_error\_sleep\_time. (по умолчанию: 10)
* **smtpd\_hard\_error\_limit** = количество ошибок в смтп-сессии перед отключением клиента. (по умолчанию: 20)
* **smtpd\_client\_connection\_count\_limit** = колическо одновременных соединений (default: 50)
* **smtpd\_client\_connection\_rate\_limit** = количество соединений в anvil\_rate\_time\_unit период (по умолчанию anvil\_rate\_time\_unit: 60s, а smtpd\_client\_connection\_rate\_limit: 0)
* **smtpd\_process\_limit** = количество процессов postfix. (по умолчанию 100)

.

* **smtp\_mx\_session\_limit** = количество попыток отправки письма перед сбросом на fallback и удалением письма
* **maximal\_backoff\_time** = максимальное время между попытка отправить задержанное письмо (по умолчанию: 4000s)
* **minimal\_backoff\_time** = минимальное время между попытка отправить задержанное письмо (по умолчанию: 300s)
* **queue\_run\_delay** = время опроса очереди задержаных писем. Должно быть меньше minimal\_backoff\_time (по умолчанию: 300s)

Таким образом можно добавить примерно следущее в my main.cf:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21 | anvil\_status\_update\_time = 600s  anvil\_rate\_time\_unit = 60s  initial\_destination\_concurrency=1  default\_destination\_concurrency\_limit=50  default\_destination\_recipient\_limit=50  default\_destination\_rate\_delay = 1s  default\_process\_limit=200  smtp\_mx\_session\_limit=100  smtpd\_client\_connection\_rate\_limit = 60  smtpd\_client\_connection\_count\_limit = 25  smtpd\_client\_message\_rate\_limit = 50  smtpd\_client\_recipient\_rate\_limit = 100  smtpd\_destination\_concurrency\_limit=100  smtpd\_destination\_recipient\_limit = 2  smtpd\_destination\_rate\_delay = 1s  maximal\_backoff\_time = 1000s  minimal\_backoff\_time = 300s  queue\_run\_delay = 300s  smtpd\_error\_sleep\_time = 1s  smtpd\_soft\_error\_limit = 10  smtpd\_hard\_error\_limit = 20 |

В postfix возможно задавать индивидуальные параметры доставок для доменов. Для этого необходимо задать файл транспортов, которые расскажут postfix по каким правилам работать с определенными доменами, и создать набор правил.  
Добавил ограничение 10/5/2 одновременных доставок для домена с задержками:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8 | transport\_maps = hash:/etc/postfix/transport  smtp\_rate10\_destination\_concurrency\_limit = 10  policy5\_destination\_concurrency\_limit = 2  policy5\_destination\_rate\_delay = 0  policy5\_destination\_recipient\_limit = 5  policy2\_destination\_concurrency\_limit = 1  policy2\_destination\_rate\_delay = 3s  policy2\_destination\_recipient\_limit = 2 |

/etc/postfix/transport:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1  2  3 | domain.ru  smtp\_rate10:somedomain.ru  domain5.ru policy5:  domain2.ru policy2: |

/etc/postfix/master.cf:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1  2  3 | smtp\_rate10     unix - - n - - smtp  policy5         unix - - n - - smtp  policy2         unix - - n - - smtp |

Тестирование:

[?](https://it-e.ru/)

|  |  |
| --- | --- |
| 1  2  3  4  5  6 | #!/bin/bash  i=0  while [ $i != 2500 ]; do  echo test | /bin/mail -s "test message$i" "user@test.com"  i=$(( $i + 1 ))  done; |

Пожалуйста, уважайте труд автора, при копировании материалов сохраняйте ссылку на источник!

*где:*

* ***virtual\_mailbox\_base****— базовый путь хранения почтовых ящиков в системе UNIX.*
* ***virtual\_alias\_maps****— формат и путь хранения алиасов для виртуальных пользователей.*
* ***virtual\_mailbox\_domains****— формат и путь хранения доменов виртуальных пользователей.*
* ***virtual\_mailbox\_maps****— формат и путь хранения почтовых ящиков для виртуальных пользователей.*
* ***virtual\_minimum\_uid****— с какого номера присваивать идентификаторы пользователям.*
* ***virtual\_uid\_maps****— идентификатор пользователя, от которого записываются сообщения.*
* ***virtual\_gid\_maps****— идентификатор группы, от которой записываются сообщения.*
* ***virtual\_transport****— задает доставщика сообщений.*
* ***dovecot\_destination\_recipient\_limit****— передача сообщений от Postfix в Dovecot выполняется по заданному количеству (в нашем примере, по 1 шт.).*
* ***smtpd\_sasl\_auth\_enable****— разрешает sasl аутентификацию.*
* ***smtpd\_sasl\_exceptions\_networks****— исключение сетей от использования шифрования.*
* ***smtpd\_sasl\_security\_options****— дополнительные опции настройки sasl.*
* ***broken\_sasl\_auth\_clients****— эту опцию прописываем для клиентов MS Outlook.*
* ***smtpd\_sasl\_type****— указывает тип аутентификации.*
* ***smtpd\_sasl\_path****— путь до временных файлов обмена информацией с Dovecot. Указывается либо абсолютный путь, либо относительный queue\_directory.*
* ***smtpd\_tls\_cert\_file****— полный путь до публичного сертификата.*
* ***smtpd\_tls\_key\_file****— полный путь до приватного сертификата.*
* ***smtpd\_use\_tls****— указывает клиентам на наличие поддержки TLS.*
* ***smtpd\_tls\_auth\_only****— использовать только TLS.*
* ***smtpd\_helo\_required****— требовать начинать сессию с приветствия.*

## Локальных реципиентов из базы:

cat /etc/postfix/sumare-local-recipient-maps.cf

hosts = 127.0.0.1

dbname = sumare

user = root

password = SintGi\_024

query = SELECT userid FROM users WHERE userid ='%s' AND active='Y'

cat /etc/postfix/main.cf

local\_recipient\_maps = mysql:/etc/postfix/sumare-local-recipient-maps.cf

postfix reload

postconf | grep local

postmap -q "asat" mysql:/etc/postfix/sumare-local-recipient-maps.cf

если выдаст ошибку postmap: fatal: unsupported dictionary type: mysql

надо посмотреть а поддерживается ли она вообще:

postconf –m

в выводе не будет майэскуель, а это значит что надо доустановить умеющий в мускул третий постфикс:

yum install –y postfix3-mysql

и снова смотрим postconf –m

на сей раз поддержка должна установиться, чтобы заработало надо перезапустить постфикс целиком

systemctl restart postfix

systemctl status postfix –l

протестировать запрос к БД, база должна быть заранее прописана, устанлен ее поддерживающий постфикс, на запрос должна отвечать тем что запрашивается либо если запрошеного нет-ничем не отвечать

postmap -q "asat" mysql:/etc/postfix/sumare-local-recipient-maps.cf

asat

после этого пользователи, заведенные в базе тоже станут принимать почту а не только заведенные в сам линукс.