Почтовый сервер

Установка и настройка postfix+dovecot

[Введение](#_c713xnuw3xem)

[Настраиваем доменные зоны](#_gm0292nw59bp)

[Postfix](#_8uyhilp8jbf4)

[Для самостоятельного изучения](#_7z9genj1oz0j)

Практическое [задание](#_3tfrjxxltv85)

[Дополнительные материалы](#_jeeoh8oz8lfe)

[Используемая литература](#_uvp6qax5r1ok)

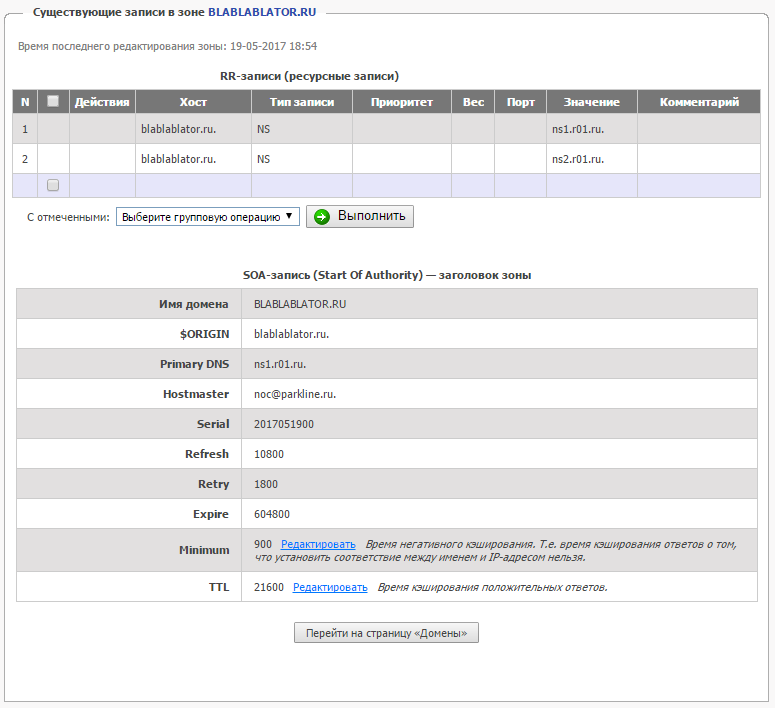
# 

# Введение

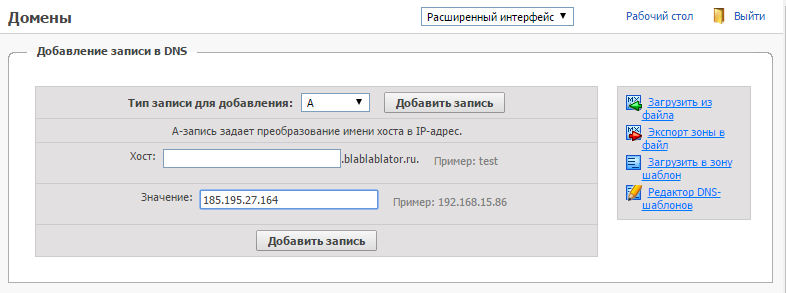
Прежде чем приступить к настройке почтового сервера, проверьте свои знания, ответив на вопросы.

1. Что такое **DNS**?
2. Сформулируйте определения.
   1. Тип ресурсной записи **NS**.
   2. Тип ресурсной записи **A**.
   3. Типа ресурсной записи **MX**.
   4. Типа ресурсной записи **PTR**.
3. Где должна быть прописана запись **PTR**? Достаточно ли прописать ее на доменном сервере? Где находится запись **A** для вашего сервера?

# Настраиваем доменные зоны

Допустим, вы купили домен blablablator.ru и решили воспользоваться DNS-хостингом у регистратора. По умолчанию настройки нашей зоны.  
  


Добавим запись **A**, чтобы на наш сервер могли заходить другие пользователи.

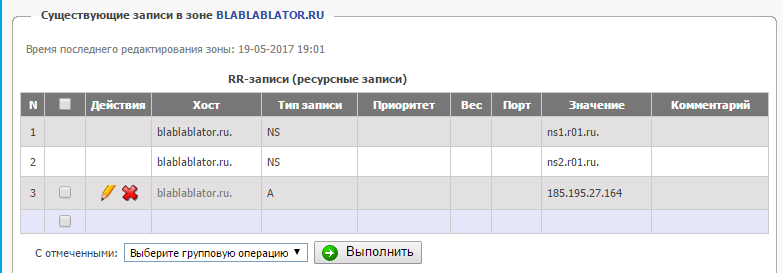


Нажимаем кнопку «Добавить запись», и система сообщает, что через 40 минут изменения вступят в силу.

Запись **A** означает, что если вы выполните эту команду

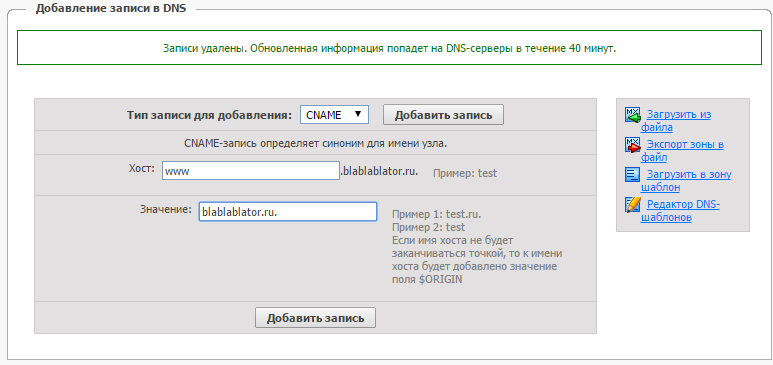
|  |
| --- |
| ping blablablator.ru |

или решите зайти на сайт blablablator.ru (где у нас уже работает Nginx или Apache2), будем обращаться на указанный адрес.



Но пользователи пока не могут зайти на [www.blablablator.ru](http://www.blablablator.ru). Нужно отдельно указать новую запись **A** для нашего домена **www** с указанием IP-адреса. Он может быть тем же или другим: записи могут вести на разные серверы. Даже одно имя может ссылаться на несколько серверов. Этот простейший механизм балансировки называется **round robin**.

В значении после домена указываем точку. Все домены заканчиваются точкой (корневым доменом), но браузеры от нас это скрывают. Если не поставить точку, считается, что это домен в локальной зоне.



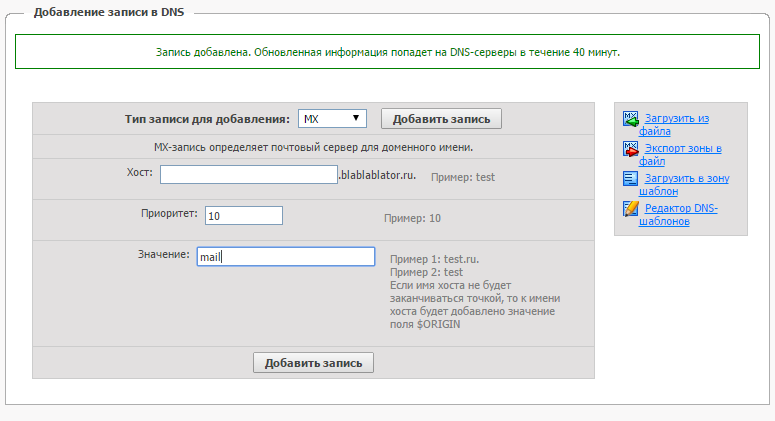
Этого достаточно, чтобы веб-сервер заработал. Осталось дождаться вступления в силу изменений на DNS-сервере регистратора, а также настроить Nginx или Apache2. Вариантов такой настройки несколько.

* Чтобы сервер отвечал и на тот, и на другой адрес.
* Чтобы сервер перекидывал с помощью кода **HTTP 302** на **www** или с **www** на основной домен.
* Можно сделать мобильный поддомен **m** и другие вплоть до микрохостинга.

Настроим домены для почты.

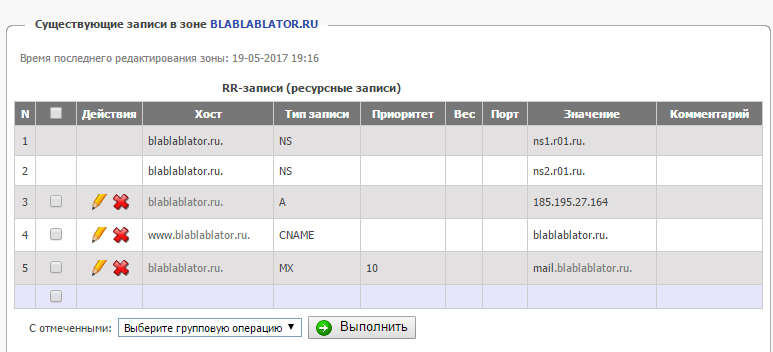
Мы настроили домен blablablator.ru так, что сайты, открываемые по этому имени, будут вести на указанный нами IP-адрес. Но это не означает, что почта, направляемая на [info@blablablator.ru](mailto:info@blablablator.ru), будет идти на тот же IP-адрес. Почтовый сервер может размещаться как на этом же сервере, так и на другом.

Поэтому придумали **MX**-записи. Необходимо указать, на какой **MX**-сервер следует отправлять почту, которая приходит на все емейлы в домене blablablator.ru



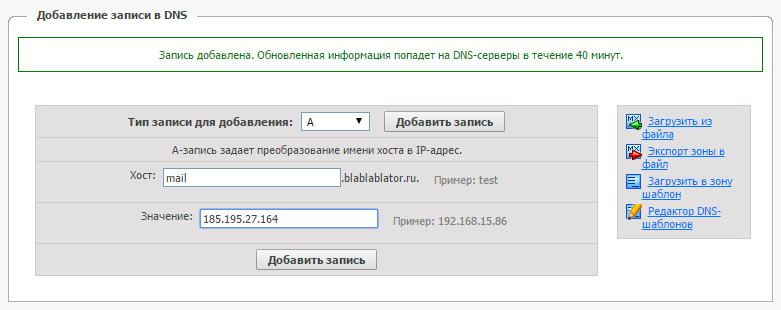
Обратите внимание: перенаправляем почту с домена blablablator.ru на почтовый сервер mail.blablablator.ru, а не наоборот!

В итоге видим такой набор записей.



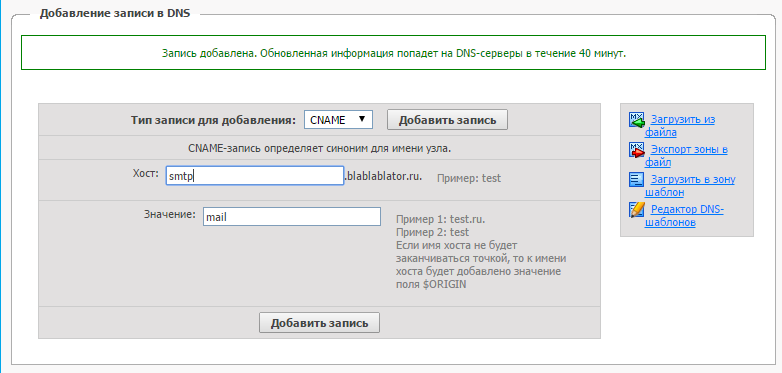
**MX**-сервер не обязан быть в нашем домене: это может быть сервер от Яндекса или Google.

Создадим A-запись для нашего веб-сервера, так как пока он не привязан к IP-адресу.

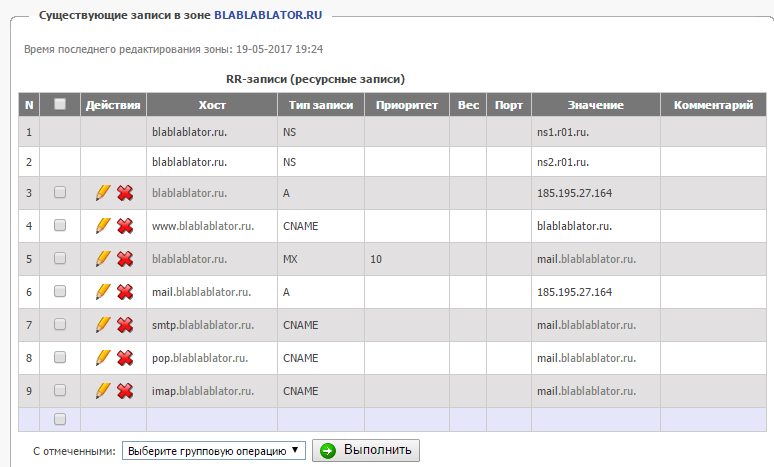


Добавляем тот же IP-адрес, что у нашего веб-сервера. Но можем указать любой другой, на котором разместим почтовый сервер. Просто в данном случае это та же машина.

Добавим поддомены **smtp**, **pop** и **imap**. Удобнее это сделать через **CNAME**.



В итоге должно получиться.

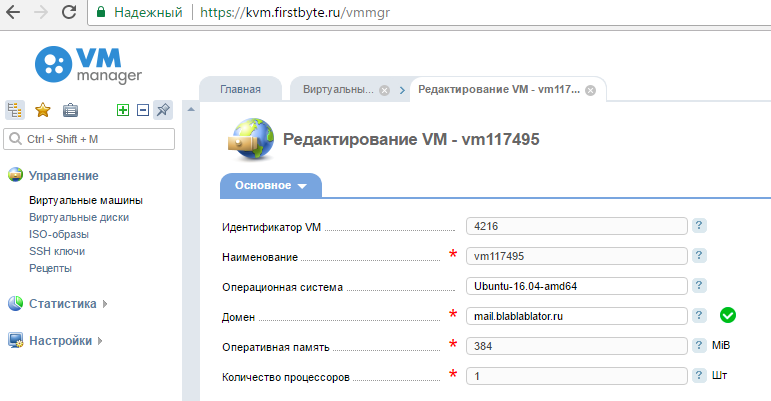


Добавим запись **PTR**, которая будет преобразовывать IP-адрес в доменное имя. Сделать это можно только на DNS-хостере провайдера. Записи имеют вид **164.27.195.185.in-addr.arpa. IN PTR mail.blablablator.ru**.

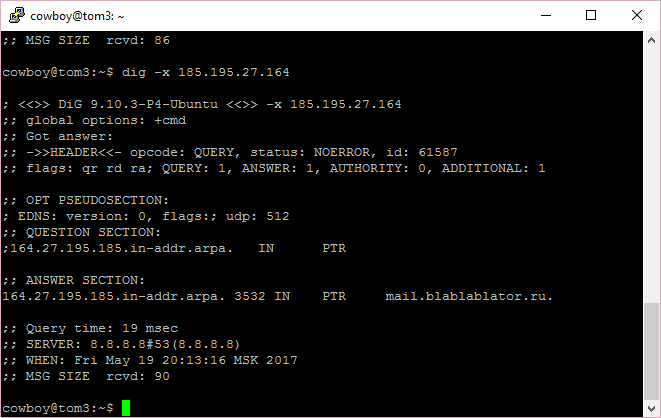
Посмотрим, что нам выдаст разрешение имени с помощью **dig**.

|  |
| --- |
| $ sudo apt -y install dnsutils  $ dig -x 185.195.27.164 |

Скорее всего, выдаст имя сервера, который был прописан при покупке **VDS**.



Прописали. Теперь все верно.



Лучше это сделать сразу и завести отдельную машину под почтовый сервер.

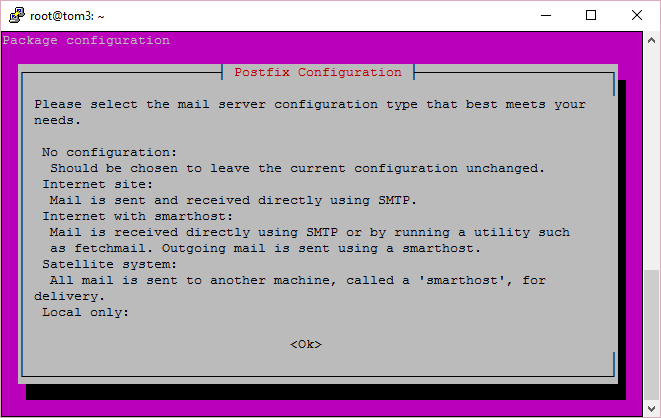
***Примечание.*** Чтобы воспользоваться собственным DNS-сервером, понадобится не менее двух серверов, доменные имена которых следует указать у регистратора. Доменные имена **NS**-серверов не обязательно должны находиться в доменной зоне, которую они будут обслуживать. Но если они находятся там же, дополнительно придется указать и IP-адреса. Для настройки собственного DNS-сервера можно использовать популярный Bind: один как **master** (на него будут вноситься все изменения), другой — как **slave** (он будет забирать изменения и отвечать вместе с первым, а также когда он на ремонте). Bind можно использовать и как кэширующий сервер, настроить для обслуживания собственной локальной сети для разрешения имен через DNS-инфраструктуру Интернета. Он может отвечать на запросы о собственной локальной зоне (например, **.mylocal**) как авторитативный сервер. Для небольших задач можно использовать готовые DNS-хостинги, которые предлагают и регистраторы доменных имен, и VDS-хостеры.

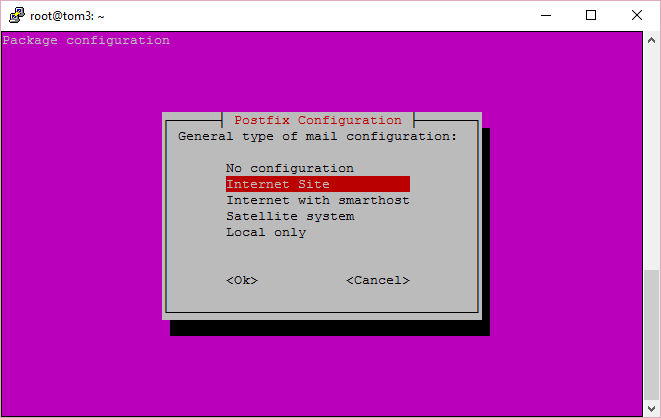
# Postfix

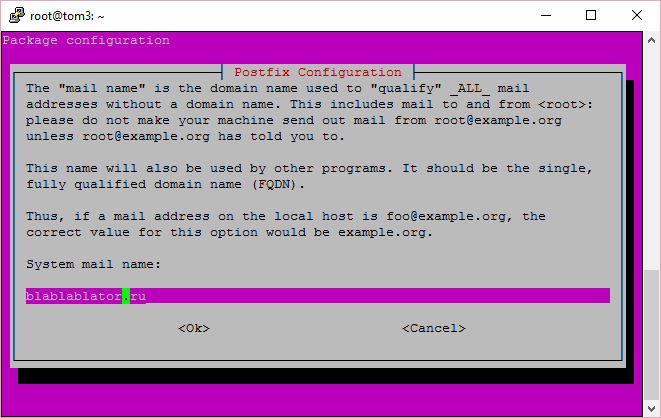
MySQL установлена, DNS-записи прописаны. Займемся Postfix.

|  |
| --- |
| # apt -y install postfix postfix-mysql postfix-doc |

Выбираем вариант настройки.





Нам хватит почты для веб-сайта. Надо указать домен почты (не путать с доменом **SMTP**-сервера).

Для **Dovecot** ставим пакеты.

|  |
| --- |
| # apt -y install dovecot-common dovecot-imapd dovecot-mysql dovecot-sieve dovecot-managesieved |

Для **SASL**.

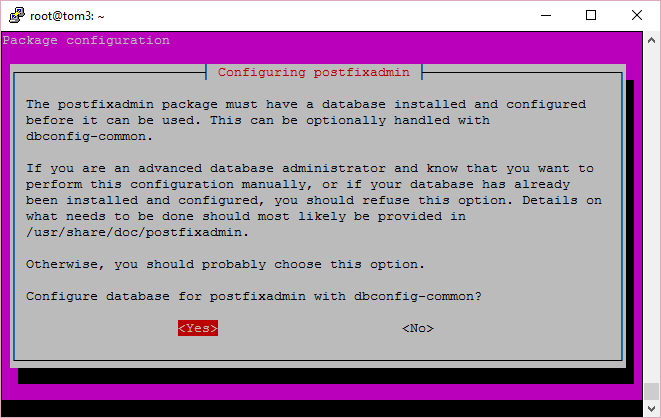
|  |
| --- |
| # apt -y install libsasl2-2 libsasl2-modules libsasl2-modules-sql sasl2-bin |

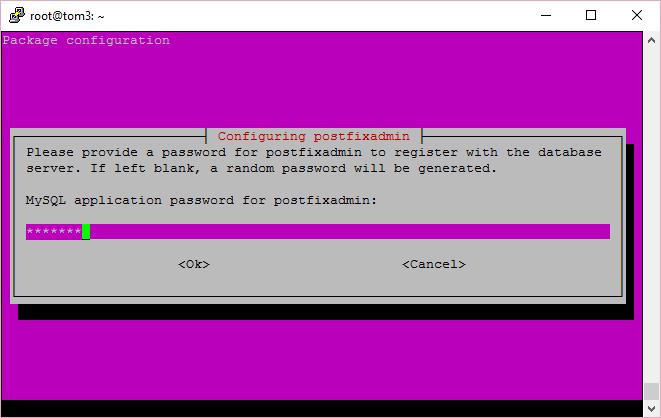
Еще поставим.

|  |
| --- |
| # apt -y install libpam-mysql openssl telnet bsd-mailx  # Установка и конфигурирования пакета Postfixadmin |

И для **Postfixadmin.**

|  |
| --- |
| # apt -y install postfixadmin |





Этот пароль пригодится многократно.

|  |
| --- |
| # nano /etc/postfixadmin/config.inc.php |

Меняем параметры.

* **$CONF['emailcheck\_resolve\_domain']='YES'** на '**NO**'.
* **$CONF['default\_language'] = 'en'** на '**ru**'.

Заходим на <http://blablablator.ru/postfixadmin/setup.php>.



Видим ошибки. Ключевой момент заключается в строке.

|  |
| --- |
| DEBUG INFORMATION:  MySQL 3.x / 4.0 functions not available! (php5-mysql installed?)  database\_type = 'mysql' in config.inc.php, are you using a different database? |

Поправим файл.

|  |
| --- |
| # nano /etc/postfixadmin/dbconfig.inc.php |

Заменим **$database\_type='mysql'**; на **$database\_type='mysqli'**.

Устраняем вторую ошибку (что **php7.0** не установлен, можно видеть через **phpinfo()**). Обязательно надо рестартовать сервер.

|  |
| --- |
| # apt install php7.0-mbstring  # systemctl restart apache2 |

Следующая ошибка.

|  |
| --- |
| DEBUG INFORMATION:  Invalid query: Invalid default value for 'created' |

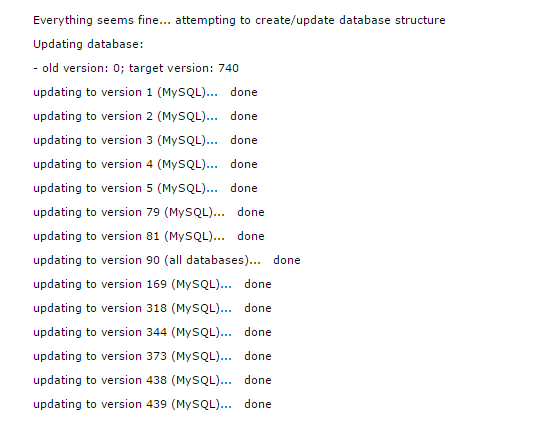
Проблема снова связана с MySQL. Исправляем.

|  |
| --- |
| # cd /usr/share/postfixadmin  # sed 's/0000-00-00 00:00:00/1970-01-01 08:00:00/g' upgrade.php |

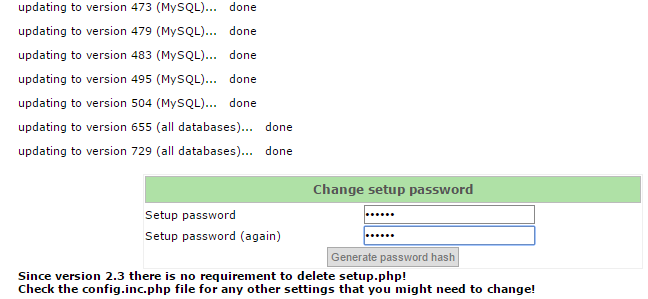
Если все верно.

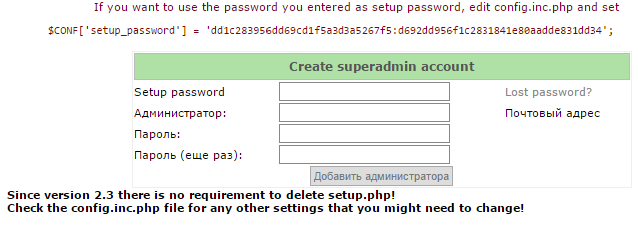
|  |
| --- |
| # cd /usr/share/postfixadmin  # sed 's/0000-00-00 00:00:00/1970-01-01 08:00:00/g' upgrade.php -i |

Процесс пошел.



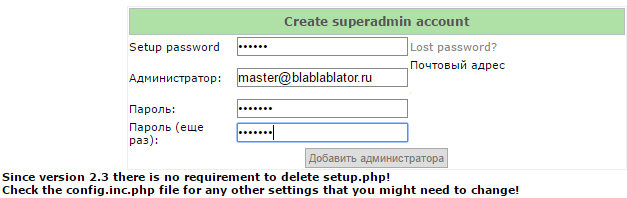
Создаем установочный пароль.

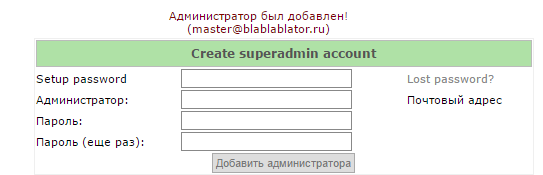




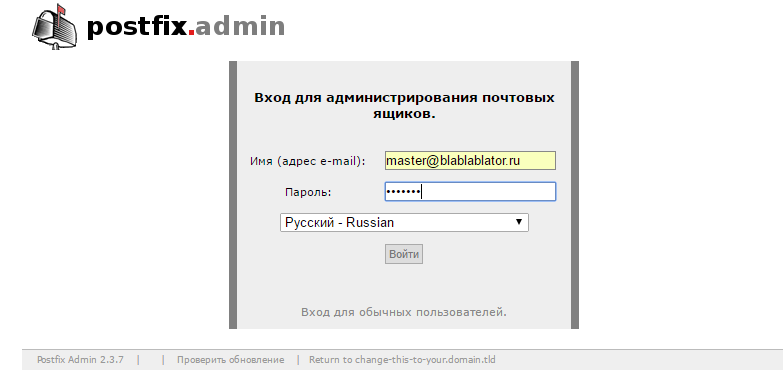
Надо последовать совету и заменить в файле строку **$CONF['setup\_password'] = 'changeme';** на указанную.

После этого вводим установочный пароль, почтовый адрес администратора и его пароль.





Теперь можем перейти в панель администрирования <http://blablablator.ru/postfixadmin/login.php> и добавить почтовые ящики (в том числе для себя).





Правим **/etc/postfix/virtual-mailbox-domains.cf.**

|  |
| --- |
| user = postfixadmin  password = password  hosts = 127.0.0.1  dbname = postfixadmin  query = select 1 from `domain` where `domain` = '%s' |

**/etc/postfix/virtual-mailbox-maps.cf**.

|  |
| --- |
| user = postfixadmin  password = password  hosts = 127.0.0.1  dbname = postfixadmin  query = select 1 from `mailbox` where `username` = '%s' |

**/etc/postfix/virtual-alias-maps.cf**.

|  |
| --- |
| user = postfixadmin  password = password  hosts = 127.0.0.1  dbname = postfixadmin  query = select goto from `alias` where `address` = '%s' |

Осторожно, названия полей в БД старых версий могут отличаться!

Добавим группу с пользователем для хранения и передачи почты.

|  |
| --- |
| groupadd -g 5000 vmail  useradd -g vmail -u 5000 vmail -d /home/vmail -m |

Проверим параметры (в особенности имена доменов) в **/etc/postfix/main.cf**.

|  |
| --- |
| myhostname = mail.blablablator.ru  mydestination = $myhostname, mail.blablablator.ru, localhost.localdomain, , localhost |

Делаем копию.

|  |
| --- |
| cp /etc/postfix/main.cf /etc/postfix/main.cf.bak |

Правим. **TLS-**конфигурация**.**

|  |
| --- |
| smtpd\_use\_tls = yes  smtpd\_tls\_cert\_file=/etc/postfix/certificate/smtpd.pem  smtpd\_tls\_key\_file=/etc/postfix/certificate/smtpd.key  smtpd\_tls\_session\_cache\_database = btree:${data\_directory}/smtpd\_scache  smtp\_tls\_session\_cache\_database = btree:${data\_directory}/smtp\_scache  smtpd\_tls\_loglevel = 0  smtpd\_tls\_received\_header = yes |

**MySQL**-конфигурация.

|  |
| --- |
| # MySQL конфигурация  virtual\_mailbox\_domains = mysql:/etc/postfix/virtual-mailbox-domains.cf  virtual\_mailbox\_maps = mysql:/etc/postfix/virtual-mailbox-maps.cf  virtual\_alias\_maps = mysql:/etc/postfix/virtual-alias-maps.cf  virtual\_mailbox\_base = /home/vmail  virtual\_uid\_maps = static:5000  virtual\_gid\_maps = static:5000 |

Настроим ограничения **SMTP**, чтобы защитить себя от спама.

|  |
| --- |
| # Настройка ограничений SMTPD  smtpd\_delay\_reject = yes  smtpd\_client\_restrictions =  permit\_mynetworks,  permit\_sasl\_authenticated,  permit  smtpd\_helo\_restrictions =  permit\_mynetworks,  permit\_sasl\_authenticated,  reject\_invalid\_helo\_hostname,  reject\_non\_fqdn\_helo\_hostname,  reject\_unknown\_helo\_hostname,  permit  smtpd\_sender\_restrictions =  permit\_mynetworks,  reject\_non\_fqdn\_sender,  permit\_sasl\_authenticated,  permit  smtpd\_recipient\_restrictions =  reject\_non\_fqdn\_recipient,  reject\_unknown\_recipient\_domain,  reject\_unlisted\_recipient,  permit\_mynetworks,  permit\_sasl\_authenticated,  reject\_unknown\_sender\_domain,  reject\_rbl\_client sbl.spamhaus.org,  reject\_rbl\_client dnsbl-1.uceprotect.net,  reject\_rbl\_client dnsbl.sorbs.net,  reject\_rbl\_client ix.dnsbl.manitu.net,  reject\_rbl\_client bl.spamcop.net,  reject\_rbl\_client access.redhawk.org,  reject\_rbl\_client bl.deadbeef.com,  reject\_rbl\_client dnsbl.cyberlogic.net,  reject\_rbl\_client dul.ru,  reject\_rbl\_client korea.services.net,  reject\_unknown\_client\_hostname,  reject\_unauth\_pipelining,  reject\_unauth\_destination,  permit  smtpd\_data\_restrictions =  permit\_mynetworks,  permit\_sasl\_authenticated,  reject\_unauth\_pipelining,  permit  smtpd\_end\_of\_data\_restrictions =  permit\_mynetworks,  permit\_sasl\_authenticated,  reject\_multi\_recipient\_bounce,  permit  #  proxy\_read\_maps = $local\_recipient\_maps $mydestination $virtual\_alias\_maps $virtual\_alias\_domains $virtual\_mailbox\_maps $virtual\_mailbox\_domains $relay\_recipient\_maps $relay\_domains $canonical\_maps $sender\_canonical\_maps $recipient\_canonical\_maps $relocated\_maps $transport\_maps $mynetworks $virtual\_mailbox\_limit\_maps  virtual\_transport = dovecot  # Алиасы  alias\_maps = hash:/etc/aliases  alias\_database = hash:/etc/aliases |

Генерируем **SSL**-сертификаты для **Postfix**.

|  |
| --- |
| mkdir /etc/postfix/certificate  cd /etc/postfix/certificate  openssl req -new -outform PEM -out smtpd.pem -newkey rsa:2048 -nodes -keyout smtpd.key -keyform PEM -days 365 -x509 |

На вопрос отвечаем.

|  |
| --- |
| Common Name (e.g. server FQDN or YOUR name) []:mail.blablablator.ru |

Устанавливаем права доступа для созданного файла-ключа.

|  |
| --- |
| chmod o= /etc/postfix/certificate/smtpd.key |

Необходимо перезапустить сервисы **postfix** и **saslauthd**.

|  |
| --- |
| #systemctl restart postfix |

Настроим **Dovecot**. Создадим резервную копию конфигурационного файла.

|  |
| --- |
| cp /etc/postfix/master.cf /etc/postfix/master.cf.bak |

Правим **master.cf,** добавляя в конце конфига.

|  |
| --- |
| mcedit /etc/postfix/master.cf |

|  |
| --- |
| dovecot unix - n n - - pipe  flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/deliver -d ${recipient} |

Делаем резервную копию **dovecot.conf**.

|  |
| --- |
| cp /etc/dovecot/dovecot.conf /etc/dovecot/dovecot.conf.bak |

Заменяем все содержимое файла конфига на код, приведенный ниже.

|  |
| --- |
| mcedit /etc/dovecot/dovecot.conf |

|  |
| --- |
| # Dovecote configuration file  protocols = imap  listen = \*  shutdown\_clients = yes  mail\_uid = vmail  mail\_gid = vmail  first\_valid\_uid = 5000  last\_valid\_uid = 5000  # Log files  log\_path = /var/log/dovecot.log  log\_timestamp = "%Y-%m-%d %H:%M:%S "  # SSL  ssl\_cert = </etc/dovecot/certificate/dovecot.pem  ssl\_key = </etc/dovecot/certificate/dovecot.key  # Расположение и формат файлов почты (%d — домен, %n — имя пользователя)  mail\_location = maildir:/home/vmail/%d/%n  protocol lda {  auth\_socket\_path = /var/run/dovecot/auth-master  log\_path = /home/vmail/dovecot-deliver.log  mail\_plugins = sieve  postmaster\_address = admin@blablablator.ru  }  namespace {  inbox = yes  location =  prefix = INBOX.  separator = .  }  passdb {  args = /etc/dovecot/dovecot-sql.conf  driver = sql  }  service auth {  unix\_listener /var/spool/postfix/private/auth {  group = postfix  mode = 0660  user = postfix  }  unix\_listener auth-master {  mode = 0600  user = vmail  }  user = root  }  userdb {  args = uid=5000 gid=5000 home=/home/vmail/%d/%n allow\_all\_users=yes  driver = static  } |

Создаем **dovecot-sql.conf** из файла **dovecot-sql.conf.ext**.

|  |
| --- |
| cp /etc/dovecot/dovecot-sql.conf.ext /etc/dovecot/dovecot-sql.conf |

Файл полностью состоит из комментариев. Добавляем.

|  |
| --- |
| mcedit /etc/dovecot/dovecot-sql.conf |

|  |
| --- |
| driver = mysql  connect = host=127.0.0.1 dbname=postfixadmin user=postfixadmin password=парольдляпользователя  default\_pass\_scheme = CRYPT  password\_query = SELECT username as user, password FROM mailbox WHERE username = '%u' |

Создадим каталог для сертификатов **Dovecot**.

|  |
| --- |
| mkdir /etc/dovecot/certificate  cd /etc/dovecot/certificate |

Далее приступаем к генерированию SSL-сертификатов для **Dovecot**.

|  |
| --- |
| openssl req -new -outform PEM -out dovecot.pem -newkey rsa:2048 -nodes -keyout dovecot.key -keyform PEM -days 365 -x509 |

Не забудьте также заполнить все поля (особенно **FQDN**!).

Устанавливаем права доступа для созданного файла-ключа.

|  |
| --- |
| chmod o= /etc/dovecot/certificate/dovecot.key |

Перезапускаем сервис **dovecot**.

|  |
| --- |
| systemctl restart dovecot |

Устанавливаем права и владельца на созданные файлы конфигурации.

|  |
| --- |
| chgrp vmail /etc/dovecot/dovecot.conf  chmod g+r /etc/dovecot/dovecot.conf |

Настраиваем почтовые алиасы.

|  |
| --- |
| mcedit /etc/aliases |

|  |
| --- |
| postmaster: root  root: admin@blablablator.ru  newaliases |

Перезагружаем сервисы **Postfix**, **Dovecot**.

|  |
| --- |
| systemctl restart postfix dovecot |

Проверяем.

|  |
| --- |
| systemctl status postfix dovecot  journalctl -u postfix  journalctl -u dovecot |

Теперь нужно поставить веб-интерфейс.

|  |
| --- |
| apt -y install roundcube |

Настраиваем.

|  |
| --- |
| mcedit /etc/roundcube/main.inc.php |

|  |
| --- |
| $rcmail\_config['default\_host']= 'localhost';  $rcmail\_config['default\_port'] = 143;  $rcmail\_config['smtp\_server'] = 'localhost';  $rcmail\_config['smtp\_port'] = 25; |

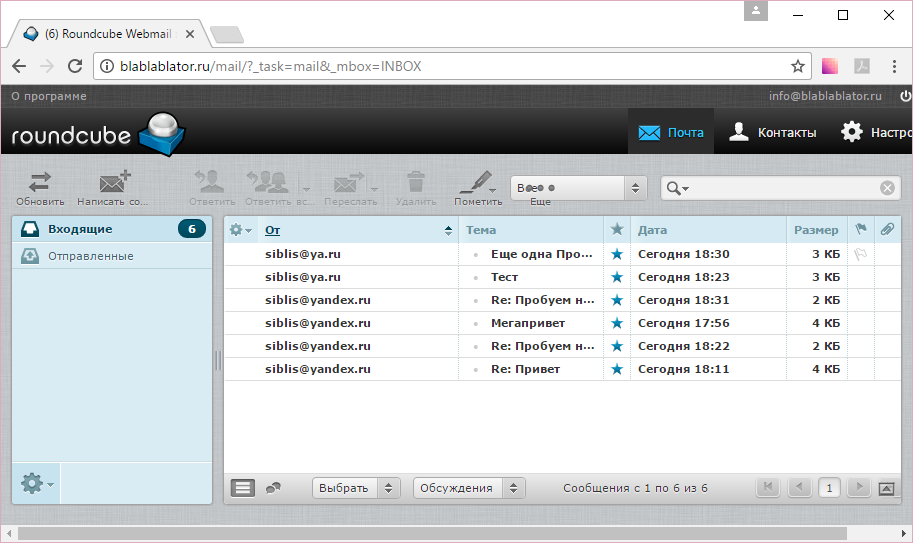
|  |
| --- |
| mcedit /etc/roundcube/apache.conf |

|  |
| --- |
| #Alias /roundcube /var/lib/roundcube  Alias /mail /var/lib/roundcube |

Перезагружаем Apache2.

|  |
| --- |
| systemctl restart apache2 |

Заходим на <http://mail.blablablator.ru/mail>. Логинимся, проверяем.



# Для самостоятельного изучения

* **SpamAssassin**.
* **DKIM**, **SPF**.

# Практическое задание

К 7 уроку.

1. Установить и настроить Postfix.
2. \* Постараться установить Dovecot и Roundcube.
3. Даже если вы не успели доделать к 8 уроку, обязательно приложите практическое задание. чтобы преподаватель смог разобрать и подсказать.

К 8 уроку: полностью сдать отчет о настроенном почтовом сервере.

# Дополнительные материалы

1. <https://ru.wikipedia.org/wiki/DNSBL>

# Используемая литература

Для подготовки данного методического пособия были использованы следующие ресурсы.

1. <https://interface31.ru/tech_it/2010/10/pochtovyj-server-dlya-nachinayushhix-nastraivaem-dns-zonu.html>
2. <https://losst.ru/ustanovka-postfix-ubuntu-s-dovecot>
3. <https://www.8host.com/blog/ustanovka-i-nastrojka-postfix-v-ubuntu-16-04/>
4. <http://forum.ubuntu-fr.org/viewtopic.php?id=1992106>
5. <http://stackoverflow.com/questions/168736/how-do-you-set-a-default-value-for-a-mysql-datetime-column>
6. <http://stackoverflow.com/questions/35565128/mysql-incorrect-datetime-value-0000-00-00-000000>.
7. <https://www.digitalocean.com/community/tutorials/how-to-configure-a-mail-server-using-postfix-dovecot-mysql-and-spamassassin>
8. <https://bozza.ru/art-169.html>
9. <https://mnorin.com/dovecot-sieve-sortirovka-pochty-na-servere.html>
10. <http://itzx.ru/linux/derektiva-nginx-location-s-primerami>