Связка Postfix + Dovecot + Roundcube + Active Directory

Итак - стоит задача - настроить почтовый сервер на базе OpenSource продуктов. В качестве базы данных о пользователях, паролях, группах, электронных почтовых адресах должен использоваться Microsoft Active Directory. В качестве решения для фильтрации почтовых сообщения должно стоять решение от Лаборатории Касперского - Kaspersky for Linux Mail Servers.

Править

Введение

Для начала определимся, из каких компонент мы будем строить почтовый сервер:

- Postfix - будет использоваться в качестве SMTP-сервера и клиента. Причина - простой в настройке и мониторинге, безопасный (крайне редко находят уязвимости, архитектура, спроектированная с учетом требований по безопасности);
- Dovecot - будет использоваться в качестве серверов IMAP4/POP3, а также средства аутентификации клиентов по протоколу SASL совместно с использованием TLS туннелей от/к почтовым клиентам. Достоинства - очень гибкий, проектировался с упором на безопасность, самый популярный на текущий момент;
- RoundCube - будет использоваться в качестве WEB-интерфейса к почтовым ящикам (аналог OWA в Microsoft Exchange). Современный, многофункциональный, удобный, самый популярный;
- Apache - WEB-сервер, предоставляющий доступ к службам RoundCube, а также WEB-интерфейсу управления почтовым антивирусом и антиспамом от Лаборатории Касперского.

Править

Установка операционной системы

В качестве основной операционной системы была выбрана FreeBSD 11 x64. Причина - базовая и удобная поддержка как готовых программ, доставляемых через фреймворк pkg с официальных репозиториев, так и поддержка сборки программ из исходных текстов с уникальными опциями и возможностями (система портов). В контексте данной задачи - простой и удобный способ получить в системе нужное ПО с нужными функциями (поддержка LDAP, SASL и т.д.).

Так как данное решение устанавливается в качестве виртуальной машины в системе Hyper-V Server 2016, то на этапе создания ВМ было принято решение использовать два жестких диска VHDX:

1. первый диск - 60 Гб - под операционную систему FreeBSD, программное обеспечение, журналы, библиотеки и т.д.
2. второй диск - 300 гб - под хранение почтовых сообщений.

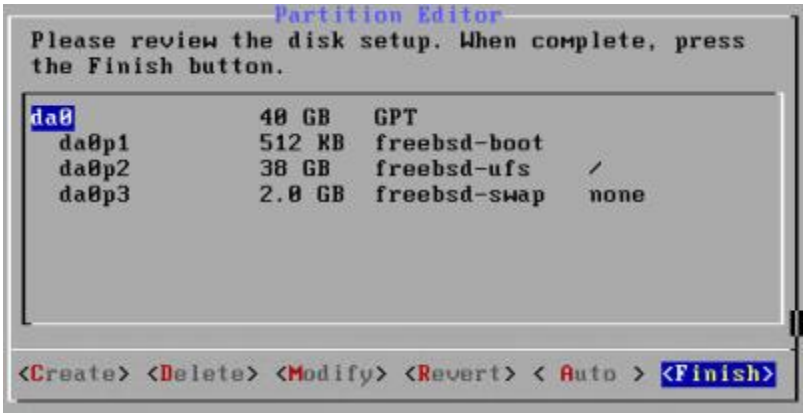
Такая комбинация дисков дает возможность гибко управлять почтовым сервером и контентом (почтой):

- Создавать резервные копии операционной системы и архива почтовых сообщений под разными расписаниями;
- Перетаскивать виртуальную машину с одного гипервизора на другой при необходимости;
- Оценивать объем использованного под почтовые сообщения дискового пространства.

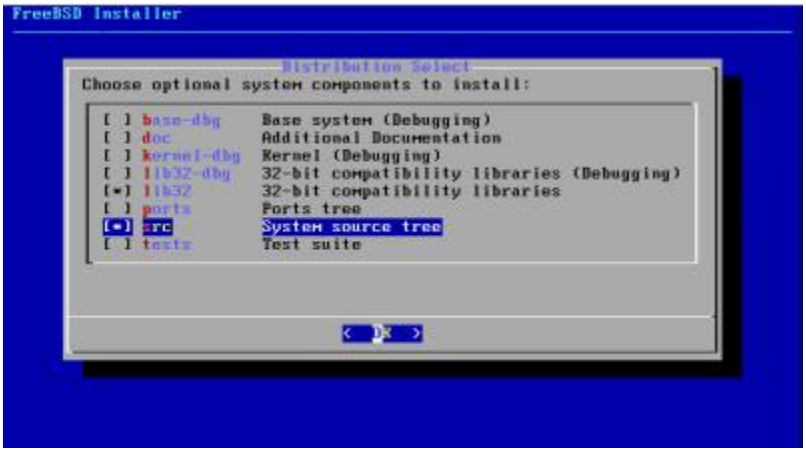
Операционная система FreeBSD устанавливается из образа: FreeBSD-11.0-RELEASE-amd64-disc1.iso со следующими значениями:

- Имя сервера: mail.mydomain.ru
- Выбор диска для установки: da0 (60 Гб)
- Выбор файловой системы: UFS

- Выбор типа разметки диска (GPT)



- Диск da0 разбивается на три партиции:
  - da0p1 - boot раздел на 512 Кб
  - da0p2 - root раздел на 52 Гб
  - da0p3 - swap раздел на 8 Гб
- Диск da1 разбивается на одну партицию на 300 Гб. Точка монтирования - /mbx.
- IP-адрес: 192.168.0.25/16, шлюз: 192.168.0.7
- Выбор distribution (помимо ядра и base): lib32 и src



- Пароли пользователей root и vershinin по желанию

Править

Установка программ и зависимостей

После установки прежде всего проверьте, что у сервера есть доступ в сеть интернет по протоколам DNS/HTTP/HTTPS/ICMP. Это условие обязательное для успешного выполнения дальнейших операций.

Для экономии времени, автор предлагает использовать следующий алгоритм работы с программным обеспечением в FreeBSD:

- Вначале вообще ВСЕ необходимое программное обеспечение устанавливается из готовых скомпилированных программ (через систему **pkg**);
- Далее удаляются три программы, опции сборки которых нас в данной задаче не устраивают (это Postfix, Dovecot и Roundcube);
- Через систему **/usr/ports** удаленные программы устанавливаются вновь - но уже с указанием необходимых для сборки опций (каких - далее по алгоритму).
- Через команду **pkg lock <имя пакета>** установленные программы «закрываются» от системы pkg - чтобы в случае выполнения команды **pkg upgrade** не произошло замещение программ с последующим изменением опций сборки.

Править

Обновление ПО в будущем

В дальнейшем, установленное ПО при необходимости, обновляется следующим образом:

- Обновление 95% программ - pkg update && pkg upgrade
- Обновление Postfix/Dovecot/Roundcube:
    - portsnap fetch update (обновляем дерево портов /usr/ports/)
    - cd /usr/ports/mail/postfix/ && make && make reinstall && make clean (обновление Postfix)
    - cd /usr/ports/mail/dovecot2/ && make && make reinstall && make clean (обновление Dovecot)
    - cd /usr/ports/mail/roundcube/ && make && make reinstall && make clean (обновление Roundcube)
    - pkg lock postfix
    - pkg lock dovecot2
    - pkg lock roundcube

Перед обновлением ПО рекомендуется сделать резервные копии сервера.

Править

Получение актуального дерева портов - /usr/ports

В консоли с правами суперпользователя root, производим запуск команды: **portsnap fetch extract**. По ее окончании в каталоге /usr/ports/ получаем свежее и актуальное дерево портов.

Править

Установка бинарных программ

Изменение репозитория для pkg

Вначале редактируем файл, указывающий системе **pkg** ветку с репозиторием пакетов для текущей операционной системы с помощью команды: ee /etc/pkg/FreeBSD.conf.

Содержимое изменяем:

```
# Было:



FreeBSD: {

  url: "pkg+http://pkg.FreeBSD.org/${ABI}/quarterly/",

  mirror_type: "srv",

  signature_type: "fingerprints",

  fingerprints: "/usr/share/keys/pkg",

  enabled: yes

}



# Стало:



FreeBSD: {

  url: "pkg+http://pkg.FreeBSD.org/${ABI}/latest",

  mirror_type: "srv",

  signature_type: "fingerprints",

  fingerprints: "/usr/share/keys/pkg",

  enabled: yes

}
```

Установка нужного ПО

Инициализируем pkg, выполняя одноименную команду - **pkg**. По завершению даем команду pkg info, чтобы убедиться в том, что pkg проинициализировался:

```
root@bsdmail:~ # pkg

The package management tool is not yet installed on your system.

Do you want to fetch and install it now? [y/N]: y

Bootstrapping pkg from pkg+http://pkg.FreeBSD.org/FreeBSD:11:amd64/latest, please wait...

Verifying signature with trusted certificate pkg.freebsd.org.2013102301... done

Installing pkg-1.10.1...

Extracting pkg-1.10.1: 100%

pkg: not enough arguments

Usage: pkg [-v] [-d] [-l] [-N] [-j <jail name or id>|-c <chroot path>|-r <rootdir>]

[-C <configuration file>] [-R <repo config dir>] [-o var=value] [-4|-6] <command> [<args>]



For more information on available commands and options see 'pkg help'.

root@bsdmail:~ # pkg info

pkg-1.10.1                     Package manager
```

Теперь установим все нужное программное обеспечение из пакетов из репозитория latest:

```
# Установка удобных и полезных программ:

pkg install htop mc wget screen nano fetchmail



# Установка SMTP-сервера Postfix:

pkg install postfix



# На вопрос об активации Postfix как основного SMTP-сервера ответьте утвердительно:

Would you like to activate Postfix in /usr/local/etc/mail/mailer.conf [n]? y

Activate Postfix in /usr/local/etc/mail/mailer.conf



# Установка POP3/IMAP4-сервера Dovecot:
```

```
pkg install dovecot2



# Установка WEB-интерфейса к почте - Roundcube:

pkg install roundcube



# Установка WEB-сервера Apache:

pkg install apache24



# Установка модуля интеграции Apache и PHP:

pkg install mod_php56



# Сразу после установки mod_php56 скопируйте в блокнот рекомендации - добавить в файл
httpd.conf строки:

You should add the following to your Apache configuration file:

<FilesMatch "\.php$">

    SetHandler application/x-httpd-php

</FilesMatch>

<FilesMatch "\.phps$">

    SetHandler application/x-httpd-php-source

</FilesMatch>



# Установка остальных модулей PHP для работы Apache и Roundcube:

pkg install php56-bz2 php56-ctype php56-gd php56-ldap php56-mcrypt php56-mysqli php56-
pdo_sqlite php56-zlib
```

Удаление бинарных Postfix, Dovecot и Roundcube

С помощью команд **pkg info postfix**, **pkg info dovecot2**, **pkg info roundcube** мы можем выяснить, что пакеты собраны без поддержки LDAP.

```
# pkg info postfix
```

```
postfix-3.2.0,1

Name           : postfix

Version        : 3.2.0,1

...

        LDAP           : off

...



# pkg info dovecot2



dovecot2-2.2.30.2

Name           : dovecot2

Version        : 2.2.30.2

...

        LDAP           : off

...



# pkg info roundcube



roundcube-1.2.5,1

Name           : roundcube

Version        : 1.2.5,1

...

        LDAP           : off

...
```

Поэтому, на следующем шаге, мы удаляем эти пакеты из системы, оставляя тем не менее их зависимости (для ускорения пересборки из исходных текстов.

```
# pkg remove postfix dovecot2 roundcube
```

```
Checking integrity... done (0 conflicting)

Deinstallation has been requested for the following 3 packages (of 0 packages in the
universe):



Installed packages to be REMOVED:

        postfix-3.2.0,1

        dovecot2-2.2.30.2

        roundcube-1.2.5,1



Number of packages to be removed: 3



The operation will free 39 MiB.



Proceed with deinstalling packages? [y/N]: y

[1/3] Deinstalling postfix-3.2.0,1...

[1/3] Deleting files for postfix-3.2.0,1: 100%

==> You should manually remove the "postfix" user.

==> You should manually remove the "maildrop" group

==> You should manually remove the "postfix" group

[2/3] Deinstalling dovecot2-2.2.30.2...

[2/3] Deleting files for dovecot2-2.2.30.2: 100%

==> You should manually remove the "dovecot" user.

==> You should manually remove the "dovenull" user.

==> You should manually remove the "dovecot" group

==> You should manually remove the "dovenull" group

If you are removing dovecot2 permanently, you should 'rm -rf /var/db/dovecot' to clear out
any remaining data.
```

```
[3/3] Deinstalling roundcube-1.2.5,1...

[3/3] Deleting files for roundcube-1.2.5,1: 100%
```

Править

Компиляция из исходных текстов

Теперь устанавливаем те же самые пакеты, но с помощью дерева портов. Сборка осуществляется по следующему алгоритму:

- Смотрим где в портах находится программа - команда **whereis <имя>**
- Переходим в каталог с программой **cd </path>**
- Смотрим опции сборки и выставляем необходимые (далее по тексту) с помощью команды **make config**
- После выставления сборки смотрим, что в системе еще не хватает: **make missing**
- Собираем с помощью команды: **make**
- Устанавливаем в систему и очищаем каталог сборки (**work/**) внутри папки с портом - команда: **make install clean**
- С помощью **pkg info <имя>** проверяем, что у установленной программы появились нужные опции и библиотеки.

Сборка Postfix

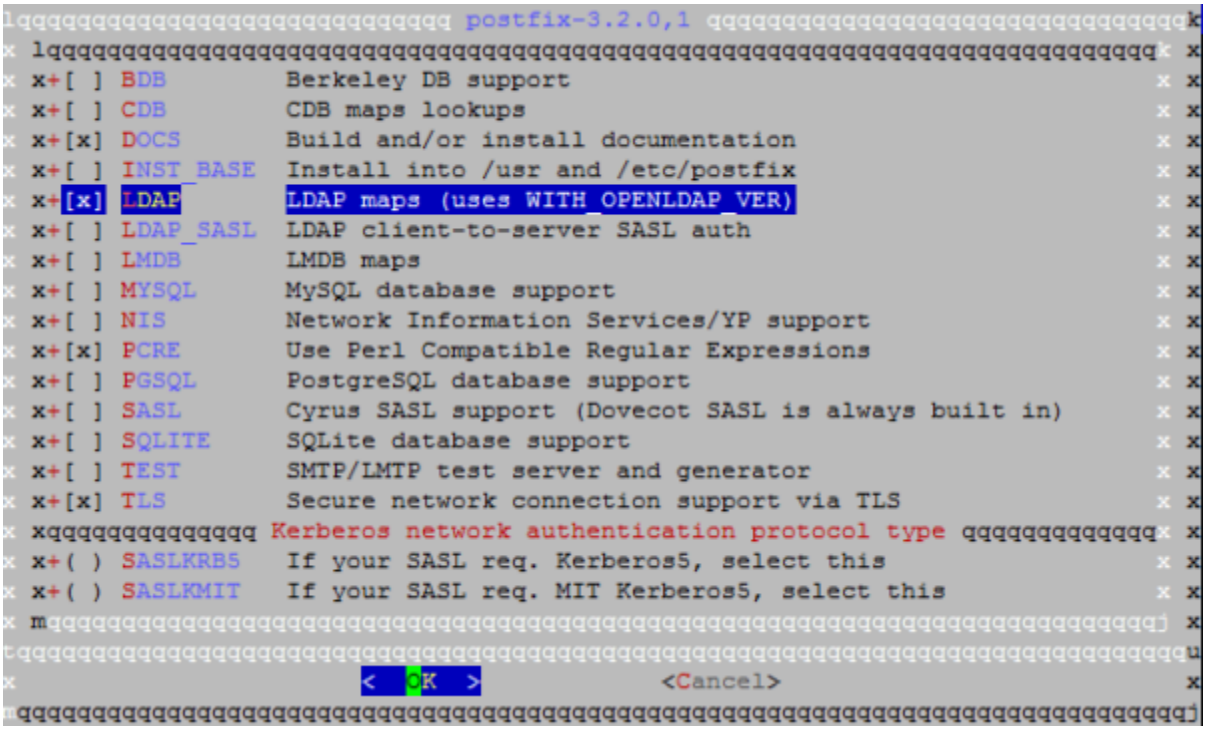
Нужные опции:

```
OPTIONS_FILE_SET+=DOCS

OPTIONS_FILE_SET+=LDAP

OPTIONS_FILE_SET+=PCRE

OPTIONS_FILE_SET+=TLS
```



Сборка Компиляция Dovecot2

Нужные опции:

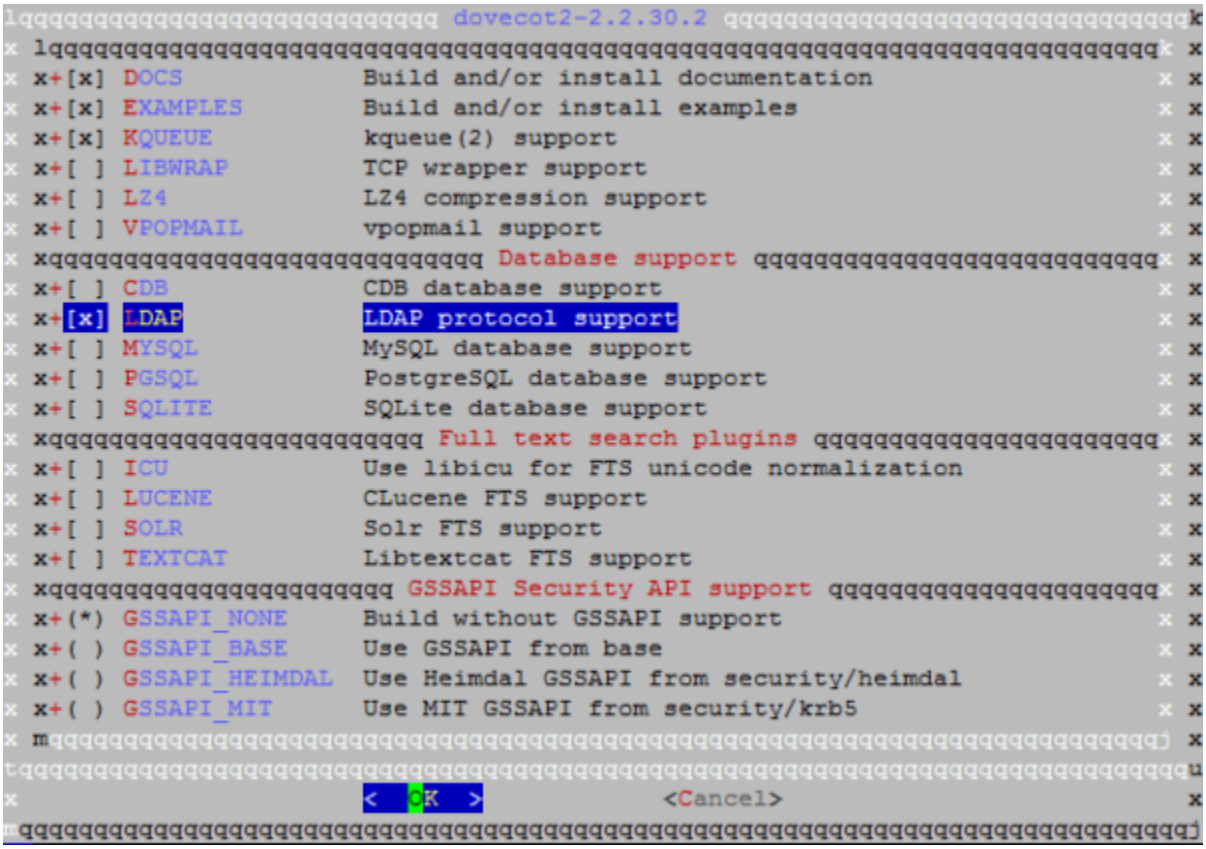
```
OPTIONS_FILE_SET+=DOCS

OPTIONS_FILE_SET+=EXAMPLES

OPTIONS_FILE_SET+=KQUEUE

OPTIONS_FILE_SET+=GSSAPI_NONE

OPTIONS_FILE_SET+=LDAP
```



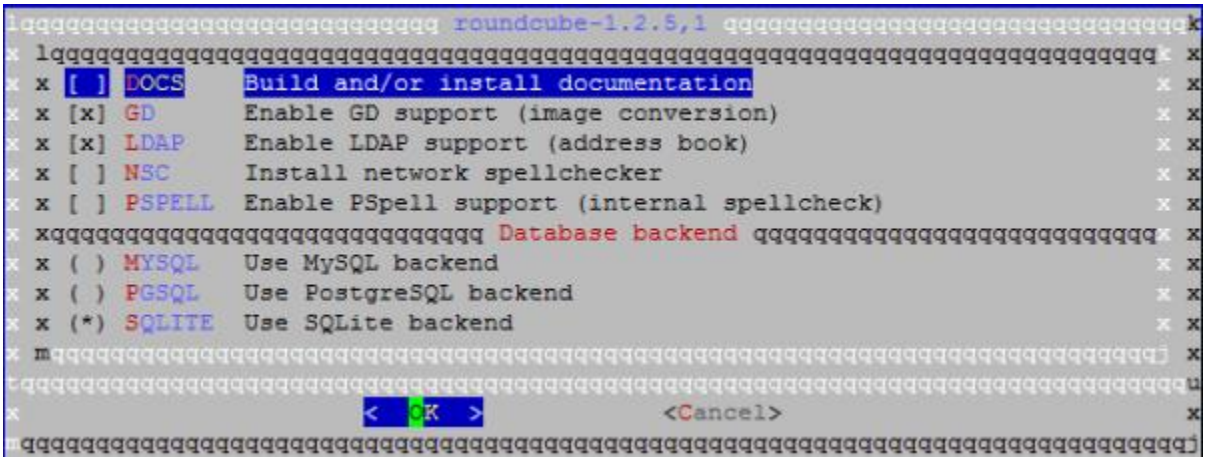
Сборка RoundCube

Нужные опции:

```
OPTIONS_FILE_SET+=GD

OPTIONS_FILE_SET+=LDAP

OPTIONS_FILE_SET+=SQLITE
```



Защита собранных программ от автоматического обновления через систему pkg

Чтобы в будущем не потерять сделанные изменение в ПО, с помощью pkg lock закрываем обновление собранных программ:

```
# pkg lock postfix

postfix-3.2.0,1: lock this package? [y/N]: y

Locking postfix-3.2.0,1



# pkg lock dovecot2

dovecot2-2.2.30.2: lock this package? [y/N]: y

Locking dovecot2-2.2.30.2



# pkg lock roundcube

roundcube-1.2.5,1: lock this package? [y/N]: y

Locking roundcube-1.2.5,1



# pkg lock -l

Currently locked packages:

dovecot2-2.2.30.2

postfix-3.2.0,1

roundcube-1.2.5,1
```

Править

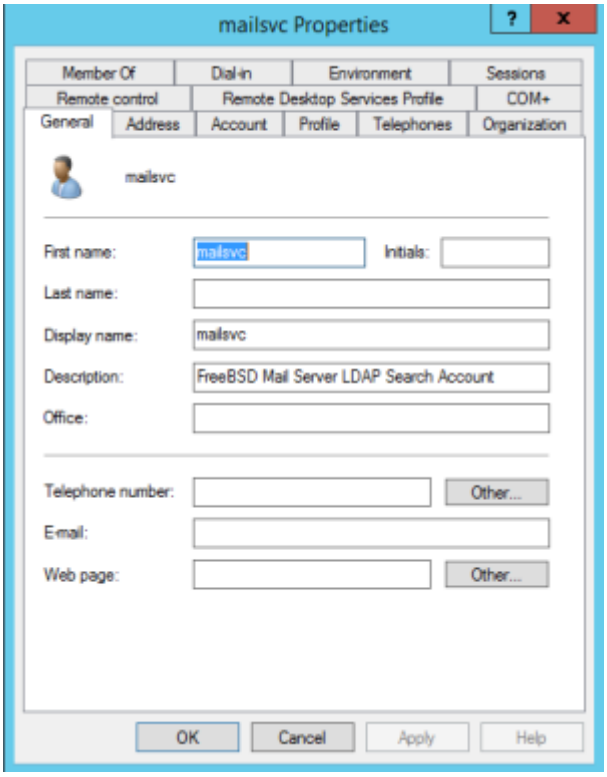
Настройки каталога Active Directory

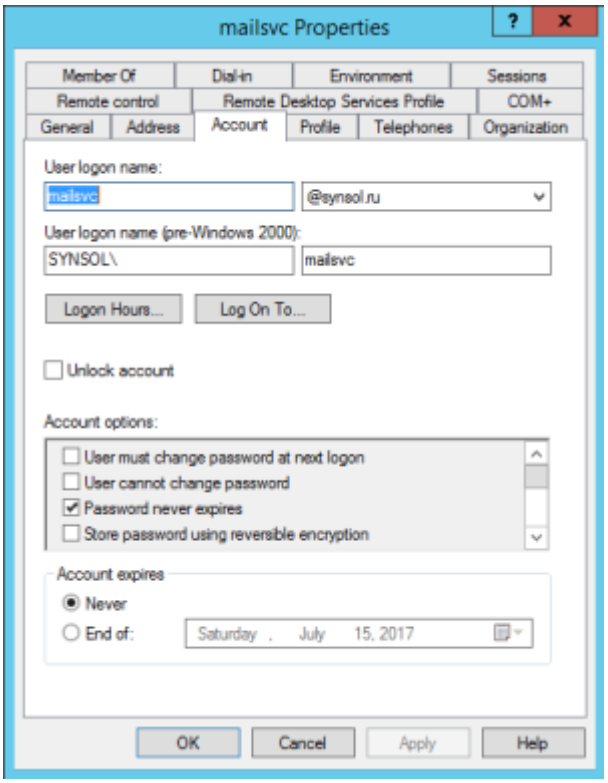
Всем трем программам (Postfix, Dovecot, Roundcube) для интеграции с LDAP нужна известная учетная запись с паролем. Права минимальные - пользователь домена AD. Также желательно создавать учетку с контейнере с английским названием (например, CN=Users). Пароль учетной записи не должен устаревать и меняться со временем (иначе сломается интеграция).

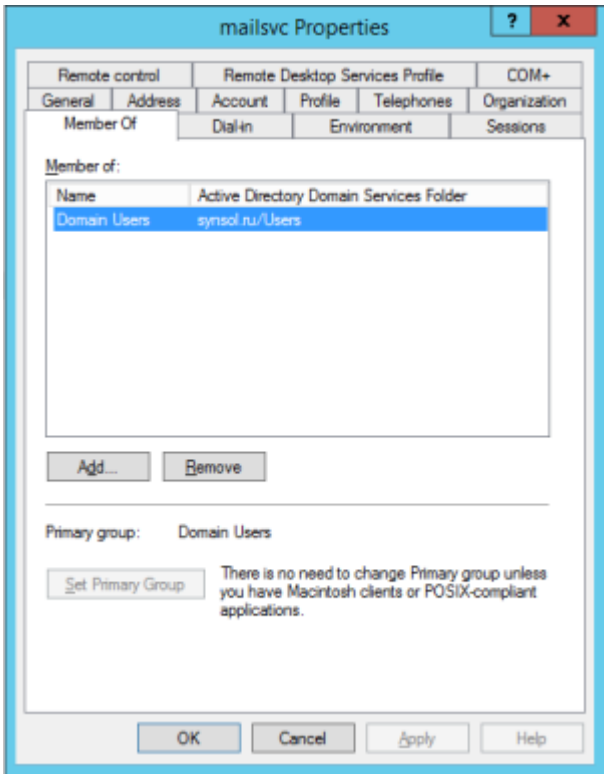
Править

Создание учетной записи для поиска в LDAP

Создадим учетку mydomain\mailsvc:







Править

Проверка работы поиска в LDAP

С помощью команды ldapsearch, которая входит в пакет openldap-client, делаем тестовый запрос в каталог с помощью только что созданной учетной записи:

```
ldapsearch -x -h 192.168.0.2 -D "CN=mailsvc,CN=Users,DC=mydomain,DC=ru" -W -b
"OU=mydomain,DC=mydomain,DC=ru" "(sAMAccountName=*)" mail | grep -i "mail"
```

После ввода пароля и успешной авторизации, получаем вывод почтовых адресов пользователей, найденных в контейнере **OU=mydomain**

```
# requesting: mail

mail: vershinin@mydomain.ru

mail: vasya@mydomain.ru

...
```

LDAPTLS_REQCERT=never ldapsearch -LLL - в ситуации, когда обязательно по SSL/TLS соединяться

Править

Генерация SSL-сертификата для почтовых служб с помощью AD CS

Если у Вас на контроллерах домена Active Directory нет центра сертификации (Certificate Authority), то на каком то одном установите и настройте роль AD CS.

Далее - алгоритм генерации сертификата и ключа для Postfix/Dovecot/Apache следующий:

Создание нужного шаблона для WEB-сервера:

1. Откройте mmc консоль Certificate Authority
2. Зайдите в раздел Certificate Templates и в контекстном меню выберите пункт - Manage (откроется отдельная mmc консоль)
3. В новой консоли найдите шаблон - Web Server - выполните на нем пункт: Duplicate Template
4. В открывшемся окне настроек копии шаблона сертификата укажите:
    a. Закладка General - имя шаблона: Web Server Custom;
    b. Закладка General - Validity Period: 5 лет;
    c. Закладка Request Handling - параметр: Allow private key to be exported - установить;
    d. Закладка Security - находим группу Authenticated Users - дать право: Enroll.
    e. Apply и OK. Применить и закрыть параметры шаблона.
5. Закрыть mmc консоль Certificate Templates Console.
6. В консоли Cenrificate Authority добавить новый шаблон в список доступных для выбора (Certificate Template → New → Certificate Templates to Issue → Web Server Custom.

Запрос сертификата на Windows-компьютере:

1. Нужен любой Windows-компьютер, включенный в данный домен Active Directory.
2. Запускаем MMC, добавляем оснастку Certificates (в раздел - Local Computer), заходим в раздел Personal.
3. Выполняем запрос нового сертификата по шаблону Web Server Custom: Certificates → All Tasks → Request New Certificate.
4. В разделе дополнительных опций указываем:
    a. Subject Name → Common Name → mail.mydomain.ru
    b. Alternate Name → DNS → mail.mydomain.ru и mail

c. В разделе Private Key → Key Options нужно убедиться, что приватный ключ доступен для экспорта (параметр влючен).

Экспортируем сертификат и приватный ключ в .PFX контейнер:

1. В контекстном меню сертификата раздел All Tasks → Export
2. Указать экспорт приватного ключа (по умолчанию не предлагает)
3. Указать экспорт ключа CA тоже
4. Указать пароль для .PFX контейнера
5. Сохранить файл с именем mail.mydomain.ru.pfx
6. С помощью SSH протокола и программ pscp/WinSCP перекачать данный файл на FreeBSD-сервер

Конвертация .PFX-контейнера в .PEM-файл:

```
# openssl pkcs12 -in mail.mydomain.ru.pfx -out mail.mydomain.ru.pem -nodes



Enter Import Password:

MAC verified OK
```

Править

Установка TLS сертфикатов в службы Postfix/Dovecot/Apache

Создаем необходимые каталоги:

```
# mkdir -pv /usr/local/etc/postfix/ssl /usr/local/etc/dovecot/ssl



/usr/local/etc/postfix/ssl

/usr/local/etc/dovecot/ssl
```

Копируем .pem файл, в котором есть закрытый ключ и сертификат сервера mail.mydomain.ru, а также сертификат CA, в каталоги к службам:

```
# cp -v mail.mydomain.ru.pem /usr/local/etc/postfix/ssl/

mail.mydomain.ru.pem -> /usr/local/etc/postfix/ssl/mail.mydomain.ru.pem



# cp -v mail.mydomain.ru.pem /usr/local/etc/dovecot/ssl/

mail.mydomain.ru.pem -> /usr/local/etc/dovecot/ssl/mail.mydomain.ru.pem



# cp -v mail.mydomain.ru.pem /usr/local/etc/apache24/Includes/
```

```
mail.mydomain.ru.pem -> /usr/local/etc/apache24/Includes/mail.mydomain.ru.pem
```

Править

Создание почтового хранилища

Почтовые сообщения будут храниться на отдельном виртуальном диске.

Необходимо создать каталог для хранения почты и назначить его владельцем службу Postfix (uid 125, gid 125):

```
mkdir -vp /mbx/mydomain.ru

chown postfix:postfix /mbx/mydomain.ru

chmod 770 /mbx/mydomain.ru
```

Править

Настройка Postfix

Прежде всего объявим службу Postfix на автоматическую загрузку при старте FreeBSD:

```
echo 'postfix_enable="YES"' >> /etc/rc.conf.local
```

Далее переходим в каталог с конфигурацией Postfix: **cd /usr/local/etc/postfix**.

Делаем копию оригинального конфигурационного файла main.cf:

```
cp main.cf main.cf.original
```

Приводим конфигурацию к итоговому виду (см. ниже).

Править

Интеграция Postfix и Active Directory

Осуществляется за счет создания отдельного файла (users.cf), в котором описывается LDAP-запрос в каталог Active Directory:

```
mkdir -vp /usr/local/etc/postfix/ldap

touch /usr/local/etc/postfix/ldap/users.cf
```

Его содержимое зависит от того, какого пользователя мы создали в AD для поиска и где мы хотим искать учетные записи с аттрибутом mail:

```
                # LDAP сервер

server_host = ldap://192.168.0.2
```

```
                # От какой базы искать пользователей
search_base = DC=mydomain,DC=ru

                # Версия LDAP каталога
version = 3

                # Поиск объектов по аттрибуту
query_filter = (mail=%s)

                # Какой аттрибут получать
result_attribute = mail

                # В каком формате выводить (domen/login)
result_format = %D/%U/

                # Уровень отладки
verbose=1

                # Учетная запись для аутентификации
bind = yes

                # Учетка
bind_dn = CN=mailsvc,CN=Users,DC=mydomain,DC=ru

                # Пароль
```

```
bind_pw = XXXXXXXX
```

Если у Вас ситуация, когда поле mail в AD у некоторых пользователей указано с использованием букв в Верхнем регистре - на файловой системе Postfix в почтовой базе будет создавать каталоги по именам пользователей - тоже с использованием букв в Верхнем регистре. Для того, чтобы Postfix так не делал - в параметре result_format замените %u на %U, а %d на %D (result_format = %D/%U/). И тогда все создаваемые каталоги будут в нижнем регистре - что как раз нужно Dovecot-y)

Править

Интеграция Postfix и SASL Dovecot

В современных версиях Postfix уже встроена поддержка SASL службы, которую может предоставлять Dovecot. Поэтому, логично для Postfix не собирать и не настраивать отдельный сервис - а довериться единой на две службы SASL реализации.

Править

Настройка Postfix и групп распространения Active Directory

Осуществляется аналогично за счет создания отдельного файла (aliases.cf), в котором описывается LDAP-запрос в каталог Active Directory:

```
touch /usr/local/etc/postfix/ldap/aliases.cf
```

Его содержимое уже другое - нам нужно искать в контейнерах AD группы распространения и явно сказать об этом Postfix (чтобы, найдя группу, он по вложенным в нее пользователям сделал дополнительные LDAP-запросы и для каждого вытащил из AD значение аттрибута mail):

```
                # LDAP сервер

server_host = ldap://192.168.0.2



                # От какой базы искать пользователей

search_base = DC=mydomain,DC=ru



                # Версия LDAP каталога

version = 3



query_filter = (&(objectClass=group)(mail=%s))

leaf_result_attribute = mail

special_result_attribute = member
```

```
                # Уровень отладки

verbose=1



                # Учетная запись для аутентификации

bind = yes



                # Учетка

bind_dn = CN=mailsvc,CN=Users,DC=mydomain,DC=ru



                # Пароль

bind_pw = XXXXXXXXX
```

Править

Указание обслуживаемого домена для транспорта Virtual

Так как мы используем для доставки почты транспорт Virtual (пользователи то не локальные - сам FreeBSD о них ничего не знает), нужно явно указать в файле transport.cf, какой почтовый домен мы обслуживаем транспортом.

```
echo 'mydomain.ru virtual:' > /usr/local/etc/postfix/transport.cf
```

Postfix работает с такими файлами в специальном формате - поэтому еще нужно выполнить команду:

```
postmap /usr/local/etc/postfix/transport.cf



# и убедиться, что теперь есть transport.cf и transport.cf.db:

ls -l /usr/local/etc/postfix/

total 244

-rw-r--r--  1 root  wheel    3547 15 июня  15:22 bounce.cf.default

drwxr-xr-x  2 root  wheel     512 15 июня  17:14 ldap

-rw-r--r--  1 root  wheel   11942 15 июня  15:22 LICENSE

-rw-r--r--  1 root  wheel    5064 15 июня  17:15 main.cf
```

```
-rw-r--r--  1 root  wheel   35394 15 июня  15:22 main.cf.default
-rw-r--r--  1 root  wheel   27109 15 июня  17:04 main.cf.original
-rw-r--r--  1 root  wheel   27109 15 июня  15:22 main.cf.sample
-rw-r--r--  1 root  wheel    6230 15 июня  15:22 master.cf
-rw-r--r--  1 root  wheel    6230 15 июня  15:22 master.cf.sample
drwxr-xr-x  2 root  wheel     512 15 июня  16:44 ssl
-rw-r--r--  1 root  wheel    1629 15 июня  15:22 TLS_LICENSE
-rw-r--r--  1 root  wheel      19 15 июня  17:18 transport.cf
-rw-r--r--  1 root  wheel  131072 15 июня  17:21 transport.cf.db
```

Править

Итоговая конфигурация Postfix

Итоговый конфиг получается следующий:

```
                # Уровень совместимости для SMTP транспорта
compatibility_level = 2



                # Рабочий каталог с очередями
queue_directory = /var/spool/postfix



                # Каталог с бинарными программами
command_directory = /usr/local/sbin
daemon_directory = /usr/local/libexec/postfix



                # Служебные базы данных
data_directory = /var/db/postfix



                # Владелец службы
mail_owner = postfix
```

```
                # Имя почтового сервера
myhostname = mail.mydomain.ru

                # Обслуживаемый домен
mydomain = mydomain.ru
myorigin = $mydomain

                # Интерфейс для работы с TCP/25
inet_interfaces = all

                # Обслуживаемые варианты доменов
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

                # Код возврата для неизвестного клиента
unknown_local_recipient_reject_code = 550

                # Сети с открытым Relay
mynetworks = 127.0.0.0/8

                # HELO/EHLO при коннекте на TCP/25
smtpd_banner = $myhostname ESMTP

                # Уровень отладочных сообщений в /var/log/maillog
debug_peer_level = 2
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
```

```
          ddd $daemon_directory/$process_name $process_id & sleep 5


                # Backend в виде SendMail для скриптов и устаревших программ
sendmail_path = /usr/local/sbin/sendmail


                # Default PATHs
newaliases_path = /usr/local/bin/newaliases
mailq_path = /usr/local/bin/mailq
setgid_group = maildrop
html_directory = /usr/local/share/doc/postfix
manpage_directory = /usr/local/man
sample_directory = /usr/local/etc/postfix
readme_directory = /usr/local/share/doc/postfix
inet_protocols = ipv4
meta_directory = /usr/local/libexec/postfix
shlib_directory = /usr/local/lib/postfix


                # Обслуживаемые виртуальные домены
transport_maps = hash:/usr/local/etc/postfix/transport.cf


                # Общий путь до почтовых ящиков
virtual_mailbox_base = /mbx


                # Описание LDAP-коннектора к Active Directory
virtual_mailbox_maps = ldap:/usr/local/etc/postfix/ldap/users.cf
virtual_alias_maps = ldap:/usr/local/etc/postfix/ldap/aliases.cf
```

```
                # Default UID/GID for mail users
virtual_uid_maps = static:125
virtual_gid_maps = static:125

                # Relay для обслуживаемых виртуальных доменов
relay_domains = $transport_maps

                # Описание локальных получателей почты
local_recipient_maps = $virtual_mailbox_maps, $virtual_maps

                # Интеграция аутентификации SASL от Dovecot с Postfix
smtpd_sasl_auth_enable = yes
broken_sasl_auth_clients = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth

                # В заголовок письма вставлять информацию об аутентификации
smtpd_sasl_authenticated_header = yes

                # Для каких доменов производить аутентификацию
smtpd_sasl_local_domain = $mydomain

                # Разрешить Relay авторизовавшимся клиентам
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination

                # Разрешения для клиентов
```

```
smtpd_client_restrictions = permit_mynetworks, permit_sasl_authenticated


                # Разрешения для отправителей
smtpd_sender_restrictions = permit_mynetworks, permit_sasl_authenticated


                # Отключить анонимный вход
smtpd_sasl_security_options = noanonymous


                # Настройки TLS/STARTTLS для SMTP-клиентов
smtpd_tls_security_level = may


                # Не разрешать пересылать пакеты с аутентификацией без TLS
smtpd_tls_auth_only = yes


                # Включаем TLS для SMTP-клиента и сервера
smtp_use_tls = yes
smtpd_use_tls = yes


                # Логировать информацию по инициализации TLS-соединения
smtp_tls_note_starttls_offer = yes


                # Ключ и сертификат X.509 для TLS
smtpd_tls_key_file = /usr/local/etc/postfix/ssl/mail.mydomain.ru.pem
smtpd_tls_cert_file = /usr/local/etc/postfix/ssl/mail.mydomain.ru.pem
smtpd_tls_CAfile = /usr/local/etc/postfix/ssl/mail.mydomain.ru.pem


                # Уровень логирования
```

```
smtpd_tls_loglevel = 1



                # Отражать информацию о TLS в заголовках письма

smtpd_tls_received_header = yes



                # Кэшировать TLS-сессии 1 час

smtpd_tls_session_cache_timeout = 3600s



                # Как SMTP клиент проверяет TLS сертификаты удаленной стороны

smtp_tls_verify_cert_match = hostname, nexthop, dot-nexthop



                # Объем почтового ящика - 500 Мб

mailbox_size_limit = 512000000

virtual_mailbox_limit = 512000000



                # Лимит на размер сообщения - 50 Мб

message_size_limit = 52428800
```

Править

Проверка работы Postfix и LDAP Lookup

На данном этапе настройки Postfix мы можем проверить следующие настройки:

1. Работу службы (запуск)
2. Работу транспорта SMTP
3. Проверку получателей в LDAP-каталоге AD

Произвести проверку аутентификации через Dovecot SASL пока мы не можем (так как не настроен Dovecot).

Запускаем службу Postfix и смотрим вывод в журнале /var/log/maillog:

```
/usr/local/etc/rc.d/postfix start



tail -n 10 /var/log/maillog
```

```
# В случае успешного запуска имеем:

Jun 15 18:40:52 bsdmail postfix/postfix-script[73005]: starting the Postfix mail system

Jun 15 18:40:52 bsdmail postfix/master[73007]: daemon started -- version 3.2.0,
configuration /usr/local/etc/postfix
```

Проверяем SMTP-транспорт и проверку получателей в каталоге - с помощью коннекта на 127.0.0.1:25

```
root@bsdmail:~ # telnet 127.0.0.1 25

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^]'.

220 mail.mydomain.ru ESMTP

HELO mail.mydomain.ru

250 mail.mydomain.ru

MAIL FROM: root@mydomain.ru

250 2.1.0 Ok

RCPT TO: vershinin@mydomain.ru

250 2.1.5 Ok

DATA

354 End data with <CR><LF>.<CR><LF>

To: vershinin@mydomain.ru

Subject: hello world!

.

250 2.0.0 Ok: queued as A8A1E27439

quit

221 2.0.0 Bye

Connection closed by foreign host.
```

В почтовом журнале /var/log/maillog во время SMTP-диалога мы видим:

```
Jun 15 18:41:46 mail postfix/smtpd[73011]: connect from localhost[127.0.0.1]

Jun 15 18:42:04 mail postfix/smtpd[73011]: A8A1E27439: client=localhost[127.0.0.1]

Jun 15 18:42:17 mail postfix/cleanup[73014]: A8A1E27439: message-
id=<20170615134204.A8A1E27439@mail.mydomain.ru>

Jun 15 18:42:17 mail postfix/qmgr[73009]: A8A1E27439: from=<root@mydomain.ru>, size=358,
nrcpt=1 (queue active)

Jun 15 18:42:17 mail postfix/virtual[73015]: A8A1E27439: to=<vershinin@mydomain.ru>,
relay=virtual, delay=19, delays=19/0.02/0/0, dsn=2.0.0, status=sent (delivered to maildir)

Jun 15 18:42:17 mail postfix/qmgr[73009]: A8A1E27439: removed

Jun 15 18:42:19 mail postfix/smtpd[73011]: disconnect from localhost[127.0.0.1] helo=1
mail=1 rcpt=1 data=1 quit=1 commands=5
```

Проверяем ситуацию, когда пользователя в AD нет:

```
root@bsdmail:~ # telnet 127.0.0.1 25

Trying 127.0.0.1...

Connected to localhost.

Escape character is '^]'.

220 mail.mydomain.ru ESMTP

HELO mail.mydomain.ru

250 mail.mydomain.ru

MAIL FROM: root@mydomain.ru

250 2.1.0 Ok

RCPT TO: vershinin666@mydomain.ru

550 5.1.1 <vershinin666@mydomain.ru>: Recipient address rejected: User unknown in local
recipient table

quit

221 2.0.0 Bye

Connection closed by foreign host.
```

```
# В журнале /var/log/maillog:

Jun 15 18:43:28 bsdmail postfix/smtpd[73011]: connect from localhost[127.0.0.1]

Jun 15 18:43:45 bsdmail postfix/smtpd[73011]: NOQUEUE: reject: RCPT from
localhost[127.0.0.1]: 550 5.1.1 <vershinin666@mydomain.ru>: Recipient address rejected:
User unknown in local recipient table; from=<root@mydomain.ru>
to=<vershinin666@mydomain.ru> proto=SMTP helo=<mail.mydomain.ru>

Jun 15 18:43:52 bsdmail postfix/smtpd[73011]: disconnect from localhost[127.0.0.1] helo=1
mail=1 rcpt=0/1 quit=1 commands=3/4
```

Если необходимо - включить debug для Postfix:

```
postconf debug_peer_level=4

postconf debug_peer_list=127.0.0.1
```

Править

Настройка Dovecot

В комплекте с пакетом Dovecot идут некие шаблоны конфигураций со значениями по умолчанию. Расположены они в каталоге: **/usr/local/etc/dovecot/example-config**. Перетаскиваем нужные нам файлы в каталог программы:

```
cp -v /usr/local/etc/dovecot/example-config/dovecot.conf  /usr/local/etc/dovecot/

cp -R -v /usr/local/etc/dovecot/example-config/conf.d /usr/local/etc/dovecot/
```

Править

Интеграция Dovecot и Active Directory LDAP

Для интеграции Dovecot и LDAP-каталога AD создаем отдельный тектовый конфиг:

```
touch /usr/local/etc/dovecot/dovecot-ldap.conf.ext
```

Его содержимое:

```
                # адреса серверов Active Directory

hosts = 192.168.0.2:3268 192.168.0.4:3268



                # Учетная запись для поиска в AD

dn = CN=mailsvc,CN=Users,DC=mydomain,DC=ru
```

```
                # Пароль учетной записи

dnpass = XXXXXXXXXXX



                # Уровень отладочных сообщений

debug_level = 0



                # Аутентифицироваться от имени пользователя

auth_bind = yes



                # Подключаться к LDAP без TLS

tls = no



                # Версия LDAP каталога

ldap_version = 3



                # База поиска пользователей в AD. ВАЖНО: Не указывать корень домена -
только контейнер внутри!!!

base = OU=mydomain,DC=mydomain,DC=ru



                # Альтернативные псевдонимы

deref = searching



                # Искать в указанном OU и в подкаталогах

scope = subtree



                # Как интерпретировать получаемые данные

user_filter = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))
```

```
user_attrs = =uid=125,=gid=125,=home=/mbx/mydomain.ru/%Ln,=quota_rule=*:bytes=%{ldap:st}

pass_filter = (&(objectClass=user)(|(mail=%Lu)(sAMAccountName=%Lu)))

pass_attrs = mail=user
```

Есть неприятная фича/бага - если в base указать корень домена AD - то не работает. Указывайте только какой нибудь контейнер внутри домена

Параметр =quota_rule=*:bytes=%{ldap:st} в user_attrs явно говорит Dovecot-у, что нужно у каждого пользователя из AD считывать аттрибут st и заданное в нем значение интерпретировать как значение квоты для ящика пользователя. Значение нужно указывать в байтах. ВАЖНО: если аттрибут st у пользователя пустой - то Dovecot в ящик не пустит!!!

Примеры PowerShell команд, которые позволят всем или одному пользователю в Active Directory, прописать аттрибут st (для работы квот):

```
# Выставляем всем пользователям из контейнера UO=mydomain аттрибут st в 1 Гб:

Get-ADUser -Filter * -SearchBase "OU=mydomain,DC=mydomain,DC=ru" | set-aduser -state
"1073741824"



# Выставляем конкретному пользователю квоту в 4 Гб:

Get-ADUser -Filter 'samAccountName -like "*vershinin*"' -SearchBase
"OU=mydomain,DC=mydomain,DC=ru" | set-aduser -state "4294967296"
```

На текущий момент квоты отображаются:

- В WEB-интерфейсе Roundcube
- В почтовом клиенте Mozilla Thunderbird при условии, что установлен плагин: Display Quota

Править

Файл конфигурации dovecot.conf

Можно оставить без изменения. Либо отключить, например, протокол POP3 (оставить только IMAP4):

```
protocols = imap pop3 lmtp
```

Править

Файл конфигурации 10-auth.conf

Нужно поправить следующие параметры:

```
# Перечень поддерживаемых протоколов:

auth_mechanisms = plain login



# Домен авторизации
```

```
auth_realms = mydomain.ru



# Разрешаем протоколы аутентификации открытым текстом (защищать от перехвата будем с
помощью TLS):

disable_plaintext_auth = no



# Подключаем авторизацию по LDAP:

!include auth-ldap.conf.ext



# Отключаем системную аутентификацию:

#!include auth-system.conf.ext
```

Править

Файл конфигурации 10-logging.conf

Включаем дополнительное журнализирование аутентификации в отдельный файл:

```
# Логируем неуспешные авторизации и причины:

auth_verbose = yes



# Путь до журнала:

debug_log_path = /var/log/dovecot_debug.log
```

Также в случае больших и непонятных проблем - включайте в журнале еще ряд параметров:

```
auth_debug = yes

auth_debug_passwords = yes

mail_debug = yes
```

После выявления причины - последние три опции обязательно отключите - чтобы не переполнять журнал

Править

Файл конфигурации 10-mail.conf

Правим следующие опции:

```
# Минимальный UID, с которым Dovecot разрешит входить в Maildir. У Postfix 125 - а
значение first_valid_uid по умолчанию 500.

first_valid_uid = 1



# Аналогично предыдущей опции но для групп:

first_valid_gid = 1



# Права на Maildir для пользователя

mail_uid = 125



# Права на Maildir для группы

mail_gid = 125



# Местонахождение почты:

mail_location = maildir:/mbx/mydomain.ru/%Ln/



# Подключаемые плагины:

mail_plugins = $mail_plugins quota imap_quota
```

Опять аккуратнее с регистром! Если стоит %Ln - тогда IMAP будет создавать каталоги пользователей по короткому имени в нижнем регистре. А если стоит %n - то будет учитываться регистр значения аттрибута mail в AD. Например у пользователя почта: VaSyA666@mydomain.ru. Каталог будет: /mbx/mydomain.ru/VaSyA666

Править

Файл конфигурации 10-master.conf

Правим следующие параметры:

```
# Для службы IMAP4 раскомментировать:

     port = 143

     port = 993

     ssl = yes
```

```
# Для настроек количества процессов:
   service_count = 0
   process_min_avail = 5

# Для службы POP3 раскомментировать:
     port = 110
     port = 995
     ssl = yes

# Для SASL аутентификации для Postfix поправить:
  # Postfix smtp-auth
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    user = postfix
    group = postfix
  }
```

Править

Файл конфигурации 10-ssl.conf

Правим следующие параметры:

```
# Включение SSL
ssl = yes

# Путь до общего .PEM-файла с сертификатом сервера
ssl_cert = </usr/local/etc/dovecot/ssl/mail.mydomain.ru.pem

# Путь до общего .PEM-файла с ключом
```

```
ssl_key = </usr/local/etc/dovecot/ssl/mail.mydomain.ru.pem



# Путь до общего .PEM-файла с CA

ssl_ca = </usr/local/etc/dovecot/ssl/mail.mydomain.ru.pem



# Не проверять CRL Distribution Point в сертификатах (файл отзыва)

ssl_require_crl = no



# Не требовать и не проверять клиентский сертификат

ssl_verify_client_cert = no
```

Править

Файл конфигурации 20-imap.conf

Изменения - включаем плагины квот для IMAP4:

```
mail_plugins = $mail_plugins quota imap_quota
```

Править

Файл конфигурации 90-quota.conf

Настраиваем общие параметры квот:

```
# Общие правила для ящиков и писем:

 plugin {

   quota_rule = *:storage=500MB



   quota_grace = 10%%



   quota_max_mail_size = 50M

 }



# Генерирование уведомлений:
```

```
 plugin {

   quota_warning = storage=95%% quota-warning 95 %u

 }



# Алгоритм оценки ящика пользователя:

plugin {

   quota = maildir:User quota

 }
```

Править

Файл конфигурации auth-ldap.conf.ext

Изменения:

```
# Указываем общие значения для полей при LDAP запросе (т.е. Dovecot через LDAP не будет выяснять эти поля в AD):

default_fields = home=/mbx/mydomain.ru/%n uid=125 gid=125
```

Если нужно пользователей выдергивать из нескольких OU - тогда под каждый OU создается в файле auth-ldap.conf.ext описание - новый раздел userdb + новый файл описывающий LDAP запрос

Править

Проверка работы Dovecot

Добавляем Dovecot на автозапуск:

```
echo 'dovecot_enable="YES"' >> /etc/rc.conf.local
```

Запускаем: **/usr/local/etc/rc.d/dovecot start**.

Если все хорошо - то в журнале /var/log/maillog видим:

```
Jun 15 20:04:50 bsdmail dovecot: master: Dovecot v2.2.30.2 (c0c463e) starting up for imap, pop3, lmtp

Jun 15 20:04:50 bsdmail dovecot: ssl-params: Generating SSL parameters

Jun 15 20:05:07 bsdmail dovecot: ssl-params: SSL parameters regeneration completed
```

Список открытых сокетов от Dovecot:

```
dovecot  auth       73251 20 tcp4   192.168.0.25:22455    192.168.0.10:3268
```

```
dovenull imap-login 73248 7  tcp4   *:143                *:*

dovenull imap-login 73248 9  tcp4   *:993                *:*

dovenull imap-login 73247 7  tcp4   *:143                *:*

dovenull imap-login 73247 9  tcp4   *:993                *:*

dovenull imap-login 73246 7  tcp4   *:143                *:*

dovenull imap-login 73246 9  tcp4   *:993                *:*

dovenull imap-login 73245 7  tcp4   *:143                *:*

dovenull imap-login 73245 9  tcp4   *:993                *:*

dovenull imap-login 73241 7  tcp4   *:143                *:*

dovenull imap-login 73241 9  tcp4   *:993                *:*

root     dovecot    73240 25 tcp4   *:110                *:*

root     dovecot    73240 27 tcp4   *:995                *:*

root     dovecot    73240 40 tcp4   *:143                *:*

root     dovecot    73240 42 tcp4   *:993                *:*
```

Настраиваем почтовый клиент и видим в логах:

```
Jun 15 20:08:15 bsdmail dovecot: imap-login: Login: user=<vershinin@mydomain.ru>,
method=PLAIN, rip=192.168.10.220, lip=192.168.10.3, mpid=73264, TLS,
session=<fRTECQFS3eTAqArc>

Jun 15 20:08:16 bsdmail dovecot: imap(vershinin@mydomain.ru): Logged out in=8 out=410

Jun 15 20:08:19 bsdmail dovecot: imap-login: Login: user=<vershinin@mydomain.ru>,
method=PLAIN, rip=192.168.10.220, lip=192.168.10.3, mpid=73265, TLS,
session=<Wsf+CQFS3uTAqArc>
```

Править

Итоговый конфиг Dovecot - когда все в одном файле

С помощью команды **dovecot** с ключом **-n** можно сгенерировать единый текстовый конфиг. Используйте для максимально быстрой инсталляции и для верификации опций, отличных от настроек по умолчанию:

```
root@bsdmail:~ # dovecot -n

# 2.2.30.2 (c0c463e): /usr/local/etc/dovecot/dovecot.conf

# OS: FreeBSD 11.0-RELEASE-p1 amd64  zfs
```

```
auth_mechanisms = plain login

auth_realms = mydomain.ru

auth_verbose = yes

debug_log_path = /var/log/dovecot_debug.log

disable_plaintext_auth = no

first_valid_uid = 1

mail_gid = 125

mail_location = maildir:/mbx/mydomain.ru/%Ln/

mail_plugins = " quota imap_quota"

mail_uid = 125

namespace inbox {

  inbox = yes

  location =

  mailbox Drafts {

    special_use = \Drafts

  }

  mailbox Junk {

    special_use = \Junk

  }

  mailbox Sent {

    special_use = \Sent

  }

  mailbox "Sent Messages" {

    special_use = \Sent

  }

  mailbox Trash {

    special_use = \Trash
```

```
  }
  prefix =
}
passdb {
  args = /usr/local/etc/dovecot/dovecot-ldap.conf.ext
  driver = ldap
}
plugin {
  quota = maildir:User quota
  quota_grace = 10%%
  quota_max_mail_size = 50M
  quota_rule = *:storage=1G
  quota_warning = storage=95%% quota-warning 95 %u
}
service auth {
  unix_listener /var/spool/postfix/private/auth {
    group = postfix
    mode = 0666
    user = postfix
  }
}
service imap-login {
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    port = 993
```

```
    ssl = yes
  }
  process_min_avail = 5
  service_count = 0
}
service pop3-login {
  inet_listener pop3 {
    port = 110
  }
  inet_listener pop3s {
    port = 995
    ssl = yes
  }
}
ssl_ca = </usr/local/etc/dovecot/ssl/mail.mydomain.ru.pem
ssl_cert = </usr/local/etc/dovecot/ssl/mail.mydomain.ru.pem
ssl_key =  # hidden, use -P to show it
ssl_require_crl = no
userdb {
  args = /usr/local/etc/dovecot/dovecot-ldap.conf.ext
  default_fields = home=/mbx/mydomain.ru/%n uid=125 gid=125
  driver = ldap
}
protocol imap {
  mail_plugins = " quota imap_quota quota imap_quota"
}
```

Править

Настройка WEB-сервера Apache

В файле **/usr/local/etc/apache24/httpd.conf** включаем следующие разделы и модули:

```
# Включаем модули:

LoadModule socache_shmcb_module libexec/apache24/mod_socache_shmcb.so

LoadModule include_module libexec/apache24/mod_include.so

LoadModule expires_module libexec/apache24/mod_expires.so

LoadModule ssl_module libexec/apache24/mod_ssl.so

LoadModule rewrite_module libexec/apache24/mod_rewrite.so

LoadModule php5_module        libexec/apache24/libphp5.so



# Включаем обработку PHP-файлов

<FilesMatch "\.php$">

    SetHandler application/x-httpd-php

</FilesMatch>

<FilesMatch "\.phps$">

    SetHandler application/x-httpd-php-source

</FilesMatch>



# Вынесем корневой каталог выше:

DocumentRoot "/usr/local/www/"

<Directory "/usr/local/www/">

    Options Indexes FollowSymLinks

    AllowOverride All

    Require all granted

</Directory>
```

```
# Включаем SSL:

Include etc/apache24/extra/httpd-ssl.conf
```

Править

Конфигурация доступа к RoundCube через HTTP/HTTPS

Создаем файл конфигурации для RoundCube:

```
touch /usr/local/etc/apache24/Includes/roundcube.conf



# его содержимое:

Alias /owa "/usr/local/www/roundcube/"

Alias /roundcube "/usr/local/www/roundcube/"



<Directory "/usr/local/www/roundcube/">

        RewriteEngine on

        Options +FollowSymLinks

        DirectoryIndex index.php

        AllowOverride All

        Order Deny,Allow

        Allow from all

</Directory>
```

Конфигурация SSL:

```
# Открываем файл /usr/local/etc/apache24/extra/httpd-ssl.conf

# Исправляем:

DocumentRoot "/usr/local/www/"

ServerName mail.mydomain.ru:443

ServerAdmin vershinin@mydomain.ru
```

```
SSLCertificateFile "/usr/local/etc/apache24/Includes/mail.mydomain.ru.pem"

SSLCertificateKeyFile "/usr/local/etc/apache24/Includes/mail.mydomain.ru.pem"
```

Править

Проверка работы Apache

Определяем автозапуск службы, правим /etc/hosts и запускаем:

```
echo 'apache24_enable="YES"' >> /etc/rc.conf.local



# в файл /etc/hosts вносим информацию о hostname:

::1                     localhost

127.0.0.1               localhost

192.168.0.25            mail.mydomain.ru mail



# Запускаем службу:

service apache24 start
```

Править

Настройка Roundcube

Минимальная настройка:

```
# Переходим в каталог с конфигурацией Roundcube:

cd /usr/local/www/roundcube/config/



# копируем файл с конфигурацией:

config.inc.php.sample config.inc.php



# правим следующие параметры:



# База данных для локальных адресов (персональная адресная книга):

$config['db_dsnw'] = 'sqlite:////usr/local/www/roundcube/db/sqlite.db?mode=0646';
```

```
# Адрес SMTP-службы для отправки:

# Через 127.0.0.1 разрешен Open Relay - а значит Roundcube не нужно будет использовать аутентификацию и SASL

$config['smtp_server'] = '127.0.0.1';
```

Править

Добавление от 14-09-2021

В конфиг Roundcube необходимо:

```
$config['default_host'] = '%n';

$config['smtp_server'] = 'tls://%n';

$config['smtp_port'] = 25;
```

Также при использовании приватных сертификатов из приватного CA добавить сертификат CA в /etc/ssl/certs/ согласно статье: https://blog.socruel.nu/freebsd/how-to-install-private-CA-on-freebsd.html

Править

Добавление от 27-09-2022

Чтобы отправлять письма из интерфейса Roundcube через SMTP сервер по адресу 127.0.0.1 без авторизации, уберите все указанные по умолчанию настройки в параметрах юзера:

```
$config['default_host'] = '127.0.0.1';

$config['smtp_server'] = '127.0.0.1';

$config['smtp_port'] = 25;

$config['smtp_user'] = '';

$config['smtp_pass'] = '';
```

Править

Настройка локальной базы SQLite3 для персональных адресов

Для работы RoundCube с SQLite3 нужно выполнить следующие шаги:

```
# Перейти в каталог Roundcube:

cd /usr/local/www/roundcube/



# создать каталог для SQLite базы:
```

```
mkdir db



# проинициализировать базу

sqlite3 -init SQL/sqlite.initial.sql db/sqlite.db



# Далее выйти из базы с помощью команды .quit

# sqlite3 -init SQL/sqlite.initial.sql db/roundcube.sqlite

 -- Loading resources from SQL/sqlite.initial.sql



 SQLite version 3.7.13 2012-06-11 02:05:22

 Enter ".help" for instructions

 Enter SQL statements terminated with a ";"

 sqlite> .quit



# выставить права на каталог и базу:

chown -R www:www temp logs db

chmod -R 775 db
```

Важно - хоть для аутентификации Roundcube использует Dovecot/SASL, тем не менее в своей локальной базе он создает пользователей тоже! Учитывайте это!

Дополнительные параметры в файл config.inc.php:

```
# Автоматически создавать пользователя в SQL-базе (в нашем случае SQLite3):

$config['auto_create_user'] = true;



# Нормализировать имя в нижний регистр:

$config['login_lc'] = 2;



# В случае входа по короткому имени - подставлять почтовый домен в профиль.
```

```
# Если имя входа в AD отличается от почтового адреса - в WEB-профиле roundcube нужно
руками поправить нужный email

$config['mail_domain'] = 'mydomain.ru';
```

Править

Интеграция RoundCube и LDAP Address Book

Добавляем в файл **config.inc.php** следующий раздел:

```
$config['ldap_public'] = array(

    'MyAdLdap' =>array (

        'name' => 'mydomain',

        'hosts' => array('192.168.0.2'),

        'sizelimit' => 6000,

        'port' => 389,

        'use_tls' => false,

        'user_specific' => false,

        'base_dn' => 'OU=mydomain,DC=mydomain,DC=ru',

        'bind_dn' => 'CN=mailsvc,CN=Users,DC=mydomain,DC=ru',

        'bind_pass' => 'XXXXXXXXX',

        'writable' => false,

        'ldap_version' => 3,

        'search_fields' => array(

           'mail',

           'cn',

        ),

      'fieldmap'                    => array(

             'name'                 => 'cn',

             'firstname'            => 'givenName',

             'surname'              => 'sn',
```

```
            'jobtitle'              => 'title',
            'businessCategory'      => 'businessCategory',
            'email'                 => 'mail:*',
            'phone:work'            => 'telephoneNumber',
            'phone:mobile'          => 'mobile',
            'phone:home'            => 'homePhone',
            'phone:workfax'         => 'facsimileTelephoneNumber',
            'street'                => 'street',
            'zipcode'               => 'postalCode',
            'region'                => 'st',
            'locality'              => 'l',
            'country'               => 'c',
            'organization'          => 'o',
            'department'            => 'businessCategory',
            'notes'                 => 'description',
    ),
      'name_field' => 'cn',
      'email_field' => 'mail',
      'surname_field' => 'sn',
      'firstname_field' => 'givenName',
      'sort' => 'sn',
      'scope' => 'sub',
      'filter' => '(mail=*)',
      'global_search' => true,
      'fuzzy_search' => true
  ),
```

```
);
```

Теперь у нас в адресной книге в WEB-интерфейсе отображаются персональные учетки и из каталога LDAP. Группы распространения тоже работают.

Править

Поддержка отображения квот

Квоты в WEB-интерфейсе Roundcube автоматически отображаются в случае, если они были правильно включены через Dovecot (что было уже ранее сделано).

Править

Настройка PHP и Roundcube

Так как Roundcube использует PHP, необходимо будет настроить ряд параметров:

```
# Переходим в каталог, где должен находиться конфигурационный файл php.ini:

cd /usr/local/etc/



# Копируем пример конфига для Production:

cp php.ini-production php.ini



# Открываем в редакторе и исправляем следующие параметры:

# Максимальный размер файла, отправляемого через POST:

post_max_size = 64M



# Аналогично. Все это нужно для отправки вложений через WEB-интерфейс RoundCube:

upload_max_filesize = 64M



# чтобы в Roundcube корректно отображались метки времени - выставляем временную зону:

date.timezone = "Asia/Yekaterinburg"
```

Так как WEB-интерфейс RoundCube содержив в корне сайта файл .htaccess - и в нем определены свои параметры post_max_size и upload_max_filesize - то придется этот файл изменить тоже

```
# Редактируем файл /usr/local/www/roundcube/.htaccess

# Изменяем параметры:
```

```
php_value   upload_max_filesize   64M

php_value   post_max_size         64M

php_value   memory_limit          128M
```

Править

Установка и настройка Kaspersky for Linux Mail Servers

Так как пакеты KLMS под FreeBSD 9-й версии - установите пакеты совместимости:

```
pkg install compat9x-amd64



The following 2 package(s) will be affected (of 0 checked):



New packages to be INSTALLED:

        compat9x-amd64: 9.3.903000.20170608

        compat10x-amd64: 10.3.1003000.20170608



Number of packages to be installed: 2



The process will require 18 MiB more space.

5 MiB to be downloaded.



Proceed with this action? [y/N]: y

[1/2] Fetching compat9x-amd64-9.3.903000.20170608.txz: 100%    3 MiB   2.9MB/s    00:01

[2/2] Fetching compat10x-amd64-10.3.1003000.20170608.txz: 100%    2 MiB   2.4MB/s    00:01

Checking integrity... done (0 conflicting)

[1/2] Installing compat10x-amd64-10.3.1003000.20170608...

[1/2] Extracting compat10x-amd64-10.3.1003000.20170608: 100%

[2/2] Installing compat9x-amd64-9.3.903000.20170608...
```

```
Extracting compat9x-amd64-9.3.903000.20170608: 100%
```

Скачайте в сайта ЛК пакеты: KLMS - Пакеты установки FreeBSD 9.3/10.1 (txz). Версия 8.0.1.721

```
http://products.s.kaspersky-
labs.com/multilanguage/email_gateways/kavlinuxfreebsdmailserver/freebsd9/klms-
8.0.1_721.txz

http://products.kaspersky-
labs.com/products/multilanguage/email_gateways/kavlinuxfreebsdmailserver/freebsd9/ui-
64/klmsui-8.0.1_721.txz
```

Устанавливать пакеты придется с помощью pkg add с ключом -f - так как не совпадают архитектура и версия ветки BSD:

```
pkg add -f klms-8.0.1_721.txz



Installing klms-8.0.1-721...

pkg: wrong architecture: FreeBSD:9:x86:32 instead of FreeBSD:11:amd64

Extracting klms-8.0.1-721: 100%

Kaspersky Security 8.0 for Linux Mail Server has been installed

successfully, but it must be properly configured before using.

Please run /usr/local/bin/klms-setup.pl script manually to configure it.
```

Запускаем конфигурирование KLMS:

```
/usr/local/bin/klms-setup.pl
```

По окончании работы мастера определяем автоматический запуск KLMS и перезагружаем Postfix:

```
echo 'klms_enable="YES"' >> /etc/rc.conf.local

echo 'klmsdb_enable="YES"' >> /etc/rc.conf.local



/usr/local/etc/rc.d/postfix restart
```

Для управления KLMS через WEB-интерфейс установим второй пакет:

```
pkg add -f klmsui-8.0.1_721.txz



Installing klmsui-8.0.1-721...

pkg: wrong architecture: FreeBSD:9:x86:64 instead of FreeBSD:11:amd64

Extracting klmsui-8.0.1-721: 100%

Kaspersky Security 8.0 for Linux Mail Server UI has been installed

successfully, but it must be properly configured before using.

Please run /usr/local/bin/klmsui-setup.pl script manually to configure it.
```

Запускаем конфигурацию:

```
/usr/local/bin/klmsui-setup.pl
```

В процессе конфигурирования возникет ошибка - не найдена библиотека:

```
httpd: Syntax error on line 541 of /usr/local/etc/apache24/httpd.conf: Syntax error on
line 1 of /usr/local/etc/apache24/Includes/klmsui.conf:

Cannot load /usr/local/libexec/kaspersky/klmsui/mod_klwi5_2.4.so into server:

Shared object "libapr-1.so.0.5.1" not found, required by "mod_klwi5_2.4.so"
```

Делаем символическую ссылку:

```
ln -s /usr/local/lib/libapr-1.so.0.5.2 /usr/local/lib/libapr-1.so.0.5.1
```

Определяем автозапуск KLMS UI и перегружаем Apache:

```
service apache24 restart
```

Править

Адаптация настроек в Debian 11

Править

Установка пакетов

```
apt install htop dstat net-tools dnsutils mc wget screen nano fetchmail mlocate tree lsof

apt install postfix postfix-ldap
```

```
apt install dovecot-ldap

apt install dovecot-pop3d/stable dovecot-imapd/stable dovecot-lmtpd/stable

apt install roundcube/stable roundcube-sqlite3/stable roundcube-plugins-extra/stable
roundcube-plugins/stable php-net-ldap3

apt install ldap-utils
```

Править

Установка корневого сертификата CA в доверенное хранилище

```
root@linuxmailserver:/usr/local/share/ca-certificates# ls -la

итого 12

drwxr-xr-x 2 root root 4096 сен 21 12:52 .

drwxr-xr-x 5 root root 4096 сен 21 11:31 ..

-rw-r--r-- 1 root root 1968 сен 21 12:52 synsol-DC01-CA

root@linuxmailserver:/usr/local/share/ca-certificates# mv synsol-DC01-CA synsol-DC01-
CA.crt

root@linuxmailserver:/usr/local/share/ca-certificates# update-ca-certificates

Updating certificates in /etc/ssl/certs...

1 added, 0 removed; done.

Running hooks in /etc/ca-certificates/update.d...

done.
```

Настройка Postfix и Dovecot практически идентична, за исключением значений UID и GID. В Linux будут другие цифры, смотрите пристально в /etc/passwd и /etc/group

Править

Настройка Postfix - 27-09-2022

Основной конфиг:

main.cf файл

```
compatibility_level = 2

command_directory = /usr/sbin

daemon_directory = /usr/lib/postfix/sbin

data_directory = /var/lib/postfix
```

```
myhostname = icinga3.synsol.ru

mydomain = synsol.ru

myorigin = $mydomain

inet_interfaces = all

mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

unknown_local_recipient_reject_code = 550

mynetworks = 127.0.0.0/8, 192.168.10.40




smtpd_banner = $myhostname ESMTP

debugger_command =

         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin

         ddd $daemon_directory/$process_name $process_id & sleep 5

sendmail_path = /usr/sbin/sendmail

newaliases_path = /usr/bin/newaliases

mailq_path = /usr/bin/mailq

html_directory = /usr/share/doc/postfix

manpage_directory = /usr/local/man/

inet_protocols = ipv4

                # Обслуживаемые виртуальные домены

transport_maps = hash:/etc/postfix/transport.cf

                # Общий путь до почтовых ящиков

virtual_mailbox_base = /mbx

                # Описание LDAP-коннектора к Active Directory

virtual_mailbox_maps = ldap:/etc/postfix/ldap/users.cf

virtual_alias_maps = ldap:/etc/postfix/ldap/aliases.cf

                # Default UID/GID for mail users
```

```
virtual_uid_maps = static:107

virtual_gid_maps = static:114

                # Relay для обслуживаемых виртуальных доменов

relay_domains = $transport_maps

                # Описание локальных получателей почты

local_recipient_maps = $virtual_mailbox_maps, $virtual_maps

                # Интеграция аутентификации SASL от Dovecot с Postfix

smtpd_sasl_auth_enable = yes

broken_sasl_auth_clients = yes

smtpd_sasl_type = dovecot

smtpd_sasl_path = private/auth

                # В заголовок письма вставлять информацию об аутентификации

smtpd_sasl_authenticated_header = yes

                # Для каких доменов производить аутентификацию

smtpd_sasl_local_domain = $mydomain

                # Разрешить Relay авторизовавшимся клиентам

smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination

                # Разрешения для клиентов

smtpd_client_restrictions = permit_mynetworks, permit_sasl_authenticated

                # Разрешения для отправителей

smtpd_sender_restrictions = permit_mynetworks, permit_sasl_authenticated

                # Отключить анонимный вход

smtpd_sasl_security_options = noanonymous

                # Настройки TLS/STARTTLS для SMTP-клиентов

smtpd_tls_security_level = may

                # Не разрешать пересылать пакеты с аутентификацией без TLS
```

```
smtpd_tls_auth_only = yes

                # Включаем TLS для SMTP-клиента и сервера

smtp_use_tls = yes

smtpd_use_tls = yes

                # Логировать информацию по инициализации TLS-соединения

smtp_tls_note_starttls_offer = yes

                # Ключ и сертификат X.509 для TLS

smtpd_tls_key_file = /etc/postfix/ssl/synsol.pem

smtpd_tls_cert_file = /etc/postfix/ssl/synsol.pem

                # Уровень логирования

smtpd_tls_loglevel = 1

                # Отражать информацию о TLS в заголовках письма

smtpd_tls_received_header = yes

                # Кэшировать TLS-сессии 1 час

smtpd_tls_session_cache_timeout = 3600s

                # Как SMTP клиент проверяет TLS сертификаты удаленной стороны

smtp_tls_verify_cert_match = hostname, nexthop, dot-nexthop

                # Объем почтового ящика - 500 Мб

mailbox_size_limit = 512000000

virtual_mailbox_limit = 512000000

                # Лимит на размер сообщения - 50 Мб

message_size_limit = 52428800
```

Настройки почтового домена:

transport.cf файл

```
synsol.ru virtual:
```

Конфиги LDAP-коннекторов:

users.cf и aliases.cf файлы

```
# users.cf


server_host = ldap://192.168.10.9

search_base = OU=SYNSOL,DC=synsol,DC=ru

version = 3

query_filter = (mail=%s)

result_attribute = mail

result_format = %D/%U/

verbose=1

bind = yes

bind_dn = CN=mailsvc,CN=Users,DC=synsol,DC=ru

bind_pw = XXXXXXXXXXXXXXX



# aliases.cf


server_host = ldap://192.168.10.9

search_base = DC=synsol,DC=ru

version = 3

query_filter = (&(objectClass=group)(mail=%s))

leaf_result_attribute = mail

special_result_attribute = member

verbose=1

bind = yes

bind_dn = CN=mailsvc,CN=Users,DC=synsol,DC=ru
```

```
bind_pw = XXXXXXXXXXXXXXX
```

LDAP-проверка:

```
 ldapsearch -x -h 192.168.10.9 -D "CN=mailsvc,CN=Users,DC=synsol,DC=ru" -W -b
"OU=SYNSOL,DC=synsol,DC=ru" "(sAMAccountName=*)" mail | grep -i "mail"
```

Каталог для хранения почты:

```
mkdir -pv /mbx/synsol.ru

chown -R 107:114 mbx/
```

Править

Настройка Dovecot - 27-09-2022

вывод dovecot -n

```
root@icinga3:/etc/dovecot# dovecot -n

# 2.3.13 (89f716dc2): /etc/dovecot/dovecot.conf

# Pigeonhole version 0.5.13 (cdd19fe3)

# OS: Linux 5.10.0-18-amd64 x86_64 Debian 11.5 ext4

# Hostname: icinga3.synsol.ru

auth_mechanisms = plain login

auth_realms = synsol.ru

auth_verbose = yes

debug_log_path = /var/log/dovecot_debug.log

disable_plaintext_auth = no

first_valid_uid = 1

mail_gid = 114

mail_location = maildir:/mbx/synsol.ru/%Ln/

mail_plugins = " quota imap_quota"

mail_privileged_group = mail

mail_uid = 107
```

```
namespace inbox {
  inbox = yes
  location =
  mailbox Drafts {
    special_use = \Drafts
  }
  mailbox Junk {
    special_use = \Junk
  }
  mailbox Sent {
    special_use = \Sent
  }
  mailbox "Sent Messages" {
    special_use = \Sent
  }
  mailbox Trash {
    special_use = \Trash
  }
  prefix =
}
passdb {
  args = /etc/dovecot/dovecot-ldap.conf.ext
  driver = ldap
}
plugin {
  quota = maildir:User quota
  quota_grace = 10%%
```

```
  quota_max_mail_size = 100M
  quota_rule = *:storage=1G
  quota_warning = storage=95%% quota-warning 95 %u
}
protocols = " imap lmtp pop3"
service auth {
  unix_listener /var/spool/postfix/private/auth {
    group = postfix
    mode = 0666
    user = postfix
  }
}
service imap-login {
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    port = 993
    ssl = yes
  }
  process_min_avail = 5
  service_count = 0
}
service pop3-login {
  inet_listener pop3 {
    port = 110
  }
```

```
  inet_listener pop3s {
    port = 995
    ssl = yes
  }
}
ssl_cert = </etc/dovecot/ssl/synsol.pem
ssl_client_ca_dir = /etc/ssl/certs
ssl_dh = # hidden, use -P to show it
ssl_key = # hidden, use -P to show it
ssl_require_crl = no
userdb {
  args = /etc/dovecot/dovecot-ldap.conf.ext
  default_fields = home=/mbx/synsol.ru/%n uid=107 gid=114
  driver = ldap
}
protocol imap {
  mail_plugins = " quota imap_quota quota imap_quota"
}
```

Архив: dovecot-27-09-2022.tar

Править

Основные настройки Roundcube

config.inc.php файл

```
root@icinga3:/etc/roundcube# cat config.inc.php
<?php

/*
+-----------------------------------------------------------------------+
```

```
| Local configuration for the Roundcube Webmail installation.           |
|                                                                       |
| This is a sample configuration file only containing the minimum       |
| setup required for a functional installation. Copy more options       |
| from defaults.inc.php to this file to override the defaults.          |
|                                                                       |
| This file is part of the Roundcube Webmail client                     |
| Copyright (C) The Roundcube Dev Team                                  |
|                                                                       |
| Licensed under the GNU General Public License version 3 or            |
| any later version with exceptions for skins & plugins.                |
| See the README file for a full license statement.                     |
+-----------------------------------------------------------------------+
*/


$config = array();


// Do not set db_dsnw here, use dpkg-reconfigure roundcube-core to configure
database!
include_once("/etc/roundcube/debian-db-roundcube.php");


// The IMAP host chosen to perform the log-in.
// Leave blank to show a textbox at login, give a list of hosts
// to display a pulldown menu or set one host as string.
// Enter hostname with prefix ssl:// to use Implicit TLS, or use
// prefix tls:// to use STARTTLS.
// Supported replacement variables:
```

```
// %n - hostname ($_SERVER['SERVER_NAME'])

// %t - hostname without the first part

// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)

// %s - domain name after the '@' from e-mail address provided at login screen

// For example %n = mail.domain.tld, %t = domain.tld

$config['default_host'] = '127.0.0.1';



// SMTP server host (for sending mails).

// Enter hostname with prefix ssl:// to use Implicit TLS, or use

// prefix tls:// to use STARTTLS.

// Supported replacement variables:

// %h - user's IMAP hostname

// %n - hostname ($_SERVER['SERVER_NAME'])

// %t - hostname without the first part

// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)

// %z - IMAP domain (IMAP hostname without the first part)

// For example %n = mail.domain.tld, %t = domain.tld

$config['smtp_server'] = '127.0.0.1';



// SMTP port. Use 25 for cleartext, 465 for Implicit TLS, or 587 for STARTTLS
(default)

$config['smtp_port'] = 25;



// SMTP username (if required) if you use %u as the username Roundcube

// will use the current username for login

$config['smtp_user'] = '';
```

```
// SMTP password (if required) if you use %p as the password Roundcube

// will use the current user's password for login

$config['smtp_pass'] = '';



// provide an URL where a user can get support for this Roundcube installation

// PLEASE DO NOT LINK TO THE ROUNDCUBE.NET WEBSITE HERE!

$config['support_url'] = '';



// Name your service. This is displayed on the login screen and in the window title

$config['product_name'] = 'Roundcube Webmail';



// This key is used to encrypt the users imap password which is stored

// in the session record. For the default cipher method it must be

// exactly 24 characters long.

// YOUR KEY MUST BE DIFFERENT THAN THE SAMPLE VALUE FOR SECURITY REASONS

$config['des_key'] = 'P3qHHhORDDGnyaDaU0SNrzHe';



// List of active plugins (in plugins/ directory)

// Debian: install roundcube-plugins first to have any

$config['plugins'] = array(

);



// skin name: folder from skins/

$config['skin'] = 'elastic';



// Disable spellchecking
```

```
// Debian: spellchecking needs additional packages to be installed, or calling
external APIs

//         see defaults.inc.php for additional informations

$config['enable_spellcheck'] = false;



$config['auto_create_user'] = true;

$config['login_lc'] = 2;

$config['mail_domain'] = 'synsol.ru';



$config['ldap_public'] = array(

    'MyAdLdap' =>array (

        'name' => 'SYNSOL',

        'hosts' => array('192.168.10.9'),

        'sizelimit' => 6000,

        'port' => 389,

        'use_tls' => false,

        'user_specific' => false,

        'base_dn' => 'OU=SYNSOL,DC=synsol,DC=ru',

        'bind_dn' => 'CN=mailsvc,CN=Users,DC=synsol,DC=ru',

        'bind_pass' => 'XXXXXXXXXXXXXXXX',

        'writable' => false,

        'ldap_version' => 3,

        'search_fields' => array(

           'mail',

           'cn',

        ),

      'fieldmap'                      => array(
```

```
            'name'                  => 'cn',
            'firstname'             => 'givenName',
            'surname'               => 'sn',
            'jobtitle'              => 'title',
            'businessCategory'      => 'businessCategory',
            'email'                 => 'mail:*',
            'phone:work'            => 'telephoneNumber',
            'phone:mobile'          => 'mobile',
            'phone:home'            => 'homePhone',
            'phone:workfax'         => 'facsimileTelephoneNumber',
            'street'                => 'street',
            'zipcode'               => 'postalCode',
            'region'                => 'st',
            'locality'              => 'l',
            'country'               => 'c',
            'organization'          => 'o',
            'department'            => 'businessCategory',
            'notes'                 => 'description',
    ),
      'name_field' => 'cn',
      'email_field' => 'mail',
      'surname_field' => 'sn',
      'firstname_field' => 'givenName',
      'sort' => 'sn',
      'scope' => 'sub',
      'filter' => '(mail=*)',
      'global_search' => true,
```

```
        'fuzzy_search' => true

    ),

);
```

Править

Установка и настройка на Debian 11 с помощью Ansible Playbook

postfix.yml код

```
- hosts: debian

  vars:

    apt_env:

      DEBIAN_FRONTEND: noninteractive   # Устанавливать пакеты без ответов на
вопросы

  tasks:

    - name: Install MailServer Software

      apt:

        pkg:

          - htop                        # Диспетчер процессов

          - dstat                       # Анализ производительности сети и дисков

          - net-tools                   # сетевые утилиты ifconfig и route

          - dnsutils                    # DNS-утилиты nslookup и dig

          - mc                          # Файловый менеджер Midnight Commander

          - wget                        # Загрузка файлов

          - screen                      # Виртуальный терминар

          - nano                        # Редактор файлов

          - fetchmail                   # Сборщик почты с внешних POP3/IMAP4 ящиков

          - mlocate                     # Поиск файлов

          - tree                        # Просмотр файлов в виде дерева
```

```
            - lsof                          # Просмотр открытых сокетов
            - postfix                       # SMTP-сервер
            - postfix-ldap                  # Интеграция Postfix и LDAP-каталога
            - dovecot-ldap                  # Установка Dovecot и интеграции с LDAP-
каталога
            - dovecot-pop3d                 # POP3 сервер Dovecot
            - dovecot-imapd                 # IMAP4 сервер Dovecot
            - dovecot-lmtpd                 # LMTP сервер Dovecot
            - roundcube                     # WEB-интерфейс к почте (Apache и PHP как
зависимости)
            - roundcube-sqlite3             # СУБД для локальных контактов
            - roundcube-plugins-extra       # Плагины
            - roundcube-plugins             # Плагины
            - php-net-ldap3                 # Интеграция Apache+PHP с LDAP для адресной
книги
            - ldap-utils                    # утилиты ldapsearch для проверки работы с
LDAP
          state: present
          update_cache: true
        become: yes
        environment: "{{ apt_env }}"
```

Полная версия playbook и файлов от 02-10-2022: ansible-02-20-2022v4.tar

Добавил template с сертификатом - от 27-03-2023: ansible-27-03-2023v2.tar

Исправил баги, сократил количество переменных - от 11-04-2023: ansible-11-04-2023.tar

Debian12: ansible-debian12-02-11-2023-v5.tar

Перед запуском Ansible Playbook важно убедиться, что ряд условий выполнен на сервере предварительно

условия успешного запуска

```
1. Имя сервера соответствует FQDN в домене и сертификате - например,
mailserver.test.ru

2. В DNS-сервере в Active Directory мы прописали адрес и имя сервера
```

```
3. В начале файла postfix.yml мы изменили все нужные переменные

4. В AD у нас есть нужный контейнер и юзер mailsvc с паролем (см. postfix.yml)
```

Править

Установка и настройка на ALT Linux Server 10.1 с помощью Ansible Playbook

Заметки по адаптации Playbook-а на ALT Linux Server (версия 10.1).

- в самом начале в секции **apt** нужно указать **apt_rpm**, так как в ALT немного другой APT
- из каталога **/etc/control.d/facilities** нужно убрать все файлы, которые контролируют службы Postfix/Dovecot
- в файле main.cf службы Postfix (SMTP) нужно добавить: **compatibility_level = 3.6** и **virtual_minimum_uid = 1**
- в файле master.cf службы Postfix (SMTP) нужно раскомментировать строчку **smtp inet n - y - - smtpd**
- В настройки Ansible в файле ansible.cfg нужно явно указать версию Python 3.x: **interpreter_python = /usr/bin/python3**
- Настройки WEB-сайта с RoundCube находятся по другому пути: **/etc/httpd2/conf/extra-available/roundcube.conf**
- **uid** и **gid** от Postfix в ALT Server не совпадают с Debian (а они в множестве файлов используются). Исправляем
- Если у нас LDAP-сервер не Active Directory - а, например, ALT Linux Domain на Samba - отключите LDAPS в /etc/samba/smb.conf (параметр **ldap server require strong auth = no**).

Адаптированный архив с Ansible Playbook и Templates под ALT Linux Server 10.1: ansible-alt-server-01-10-2023.tar

Чтобы починить LDAP-адресную книжку: https://forum.altlinux.org/index.php?topic=37284.0

Вторая версия - добавил файлы и пути для починки LDAP адресной книги: ansible-alt-server-01-10-2023-v2.tar

Третья версия - интегрировал LDAP3.php и замену всех нужных файлов: ansible-alt-server-02-10-2023-v3.tar

Править

Установка и настройка на Astra Linux Special Edition с помощью Ansible Playbook

Для начала в ansible.cfg вносим изменения:

```
root@astra:~/Ansible# cat ansible.cfg

[defaults]

inventory = /root/Ansible/hosts

remote_user = user

private_key_file = /root/Ansible/id_rsa

host_key_checking = False
```

```
[privilege_escalation]

become                  = true

become_method           = sudo

become_user             = root

become_ask_pass         = false

default_become          = true
```

Для пользователя user команда sudo должна выполняться без подтверждения пароля.

Немного не доделанный до конца Playbook (Roundcube не инициализирован): astra-mailserver-02-11-2023.tar

Каталог installer удалите руками в каталоге /var/www/html/roundcubemail/

Править

Установка и настройка на RedOS Server с помощью Ansible Playbook

Заметки:

- Отключить SELinux (в Playbook есть)
- Пакетный менеджер - dnf (не apt и не apt_rpm)