Почтовый сервер Postfix Dovecot

В этой статье описывается минимальная настройка почтового сервера на основе Postfix (SMTP) и Dovecot (IMAP, POP3) с авторизаций пользователей через LDAP в Samba4 DC.
Предполагается что уже есть настройенная Samba4 в роли контроллера домена. Исходные данные:

- Домен: **test.alt**
- Контроллер домена: **dc.test.alt**
- Почтовый сервер: **mail.test.alt**
- Сгенерированные сертификаты и ключи для Dovecot и Postfix
- Пользователь для доступа к LDAP серверу: ldapbind

Как самостоятельно сгенерировать SSL сертификаты можно посмотреть тут

Содержание

Установка и предварительная настройка

Для работы почтового сервера необходимо установить следующие пакеты:

```
# apt-get install postfix-dovecot postfix-ldap postfix-tls postfix dovecot
```

Проверим работу DNS:

```
# dig +short -t A dc.test.alt
10.10.105.1
# dig +short -t A mail.test.alt
10.10.105.2
```

Проверим доступ к LDAP-серверу:

```
# ldapsearch -h dc.test.alt -p 389 -W -D "ldapbind@test.alt" -b "cn=Users,dc=test,dc=alt"
```

Если подключения не произошло и появилась ошибка связанная с безопасностью подключения:

```
ldap_bind: Strong(er) authentication required (8) <br>
        additional info: BindSimple: Transport encryption required.
```

То необходимо добавить строчку в smb.conf:

```
ldap server require strong auth = No
```

Это команда должна выдать информацию о пользователях. Все почтовые ящики пользователей будут хранится в директории `/var/vmail` и обрабатываться системным пользователем vmail с домашней директорией `/var/vmail`.

Создадим пользователя vmail и его домашнюю директорию:

```
# useradd -b /var -m -s /bin/false vmail
```

Настройка Dovecot

Создадим файл `/etc/dovecot/dovecot-ldap.conf.ext` параметров подключения Dovecot к LDAP:

```
# Контроллер домена (сервер LDAP)
hosts = dc.test.alt

# Пользователь и пароль для подключения к LDAP
dn = ldapbind@test.alt
dnpass = 'PaSSword'

# Следующая опция позволяет аутентифицировать пользователей с помощью подключения к серверу LDAP с их
аутентификационными данными
auth_bind = yes

# Преобразуем все имена пользователей в нижний регистр
auth_bind_userdn = %Lu

# Используем защищенное LDAP соединение
tls = yes

# Версия протокола LDAP
ldap_version = 3

# Где искать в LDAP
base = cn=Users,dc=test,dc=alt
deref = never

# Искать во всех вложенных объектах
scope = subtree

# Использовать фильтр для поиска пользователей - искать только пользователей (sAMAccountType=805306368),
# у которых совпадает с переданным логином IMAP или имя пользователя (userPrincipalName=%Lu) или электронная
почта (mail=%Lu)
user_filter = (&(sAMAccountType=805306368)(|(userPrincipalName=%Lu)(mail=%Lu)))

# Указываем расположение домашнего каталога подсоединенного пользователя, параметр "%$" будет заменен на
значение userPrincipalName (формата user@domain)
user_attrs = userPrincipalName=home=/var/vmail/%$

# Использовать фильтр для паролей
pass_filter = (&(sAMAccountType=805306368)(userPrincipalName=%Lu))

# Указываем имя пользователя найденное в LDAP
pass_attrs = userPrincipalName=user
```

Ссылка на этот конфигурационный файл есть в файле `/etc/dovecot/conf.d/auth-ldap.conf.ext`:

```
passdb {
  driver = ldap
  args = /etc/dovecot/dovecot-ldap.conf.ext
}
userdb {
  driver = ldap
  args = /etc/dovecot/dovecot-ldap.conf.ext
}
```

Далее настраиваем параметры аутентификации в файле /etc/dovecot/conf.d/10-auth.conf:

```
# Добавляемое к имени пользователю имя домена по умочанию (если пользователь введет имя user, то для dovecot он
будет user@test.alt)
auth_default_realm = test.alt

# Преобразуем все имена пользователей в нижний регистр
auth_username_format = %Lu

# Указываем методы аутентификации
auth_mechanisms = plain login

# Добавляем поддержку аутентификации в LDAP
!include auth-ldap.conf.ext
```

Далее настраиваем параметры работы с почтой в файле /etc/dovecot/conf.d/10-mail.conf:

```
# Настроим формат и расположение почты пользователей, %h - указывает, что почта располагается в домашнем
каталоге пользователя установленном в параметре user_attrs файла  dovecot-ldap.conf.ext
mail_location = maildir:%h

# Указываем системного пользователя, созданного реннее, для работы с почтой и минимальные/максимальные gid/uid
пользователей имеющих право работать с почтой (id vmail)
mail_uid = vmail
mail_gid = vmail
first_valid_uid = 1001
last_valid_uid = 1001
first_valid_gid = 1001
last_valid_gid = 1001

# Метод блокировок записи
mbox_write_locks = fcntl
```

Далее настраваем параметра SSL Dovecot в файле /etc/dovecot/conf.d/10-ssl.conf:

```
ssl = required
ssl_cert = </etc/dovecot/imap.test.alt.crt
ssl_key = </etc/dovecot/imap.test.alt.key
```

Далее настраиваем сокет авторизации для postfix. Он настраивается в файле /etc/dovecot/conf.d/10-master.conf секция service auth:

```
service auth {
  unix_listener auth-userdb {
    mode = 0660
    user = vmail
  }
  unix_listener /var/spool/postfix/private/auth {
    mode = 0660
    user = postfix
    group = postfix
  }
}
```

В этом же файле настроим сокет для приема писем из postfix-а - секция service lmtp:

```
service lmtp {
  unix_listener /var/spool/postfix/private/dovecot-lmtp {
    group = postfix
    mode = 0600
    user = postfix
  }
```

```
  user = vmail
}
```

В файле `/etc/dovecot/dovecot.conf` можно все оставить по умолчанию, например он может выглядеть так:

```
protocols = imap pop3 lmtp
listen = *
base_dir = /var/run/dovecot/
login_greeting = Dovecot ready.
dict {
}
!include conf.d/*.conf
```

Теперь можно запускать и добавлять в автозагрузку сервис dovecot:

```
# systemctl enable dovecot
# systemctl start dovecot
```

Настройка Postfix

Настраиваем параметры postfix в файле `/etc/postfix/main.cf`:

```
# Использовать ipv4 и слушать на всех интерфейсах
inet_protocols = ipv4
inet_interfaces = all

# Следующие параметры оставляем без изменения
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
data_directory = /var/lib/postfix
mail_owner = postfix

# Задаем полное имя сервера, которым postfix будет представляться при отправке/получении почты
myhostname = mail.test.alt

# Задаем имя нашего домена
mydomain = test.alt

# Имя от которого будут посылаться письма с локальной машины
myorigin = mail.test.alt

# Параметр указывает для каких доменов почта будет доставляться локально без пересылки на другие сервера
mydestination = $myhostname, localhost.$mydomain, localhost

# Указываем как доставляется локальная почта
local_transport = virtual

# Указываем как определять локальных пользователей
local_recipient_maps = $virtual_mailbox_maps

# Номер ошибки посылаемый оправителю при отказе
unknown_local_recipient_reject_code = 550

# Задаем список виртуальных доменов
virtual_mailbox_domains =  test.alt

virtual_mailbox_base = /var/mail/vhosts

# Список разрешенных пользователей
virtual_mailbox_maps = ldap:/etc/postfix/ldap/local_recipients.cf

# Указываем сокет для доставки писем в dovecot
virtual_transport = lmtp:unix:private/dovecot-lmtp

# Указываем сертификаты, ключи SSL и включаем безопасные соединения и аутентификацию
```

```
smtpd_tls_cert_file = /etc/postfix/smtp.test.alt.crt
smtpd_tls_key_file = /etc/postfix/smtp.test.alt.key
smtpd_use_tls = yes
smtpd_tls_auth_only = yes

# Настраиваем правила фильтрации писем
smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination,
reject_non_fqdn_sender, reject_unknown_sender_domain, reject_invalid_helo_hostname,
reject_non_fqdn_helo_hostname, check_helo_access

# Указываем опции SASL аутентификации через dovecot
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
smtpd_sasl_local_domain =  $myorigin
```

Для работы smtps раскоментируем следующие строки в файле `/etc/postfix/master.cf`:

```
smtps     inet  n       -       -       -       -       smtpd
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
```

Далее создадим каталог ldap и добавим файлы с правилами, указанные выше:

```
# mkdir /etc/postfix/ldap
```

В этом каталоге создадим файл `local_recipients.cf`, который проверяет считать ли пользователя локальным:

```
debuglevel = 0
version = 3
server_host = dc.test.alt
bind_dn = ldapbind@test.alt
bind_pw = PaSSword
search_base = dc=test,dc=alt
search_scope = subtree
query_filter = (&(|(userPrincipalName=%u@%d)(mail=%u@%d)(otherMailbox=%u@%d))(sAMAccountType=805306368))
result_attribute = userPrincipalName
cache = no
```

Запускаем и добавляем в автозагрузку сервис postfix:

```
# systemctl enable postfix
# systemctl start postfix
```

Проверка работоспособности

Создадим в домене двух пользователей u01test (u01test@test.alt) и u02test (u02test@test.alt). Настроим почтовый клиент и попробуем посылать письма от одного пользователя другому.