Интеграция iRedMail с Microsoft Active Directory

Обновлено: 10.02.2024 Опубликовано: 10.10.2022
Используемые термины: iRedMail, Active Directory.

Из коробки iRedMail умеет работать с OpenLDAP, но можно перенастроить его для работы с активным каталогом от компании Microsoft. Управление почтовыми ящиками после этого должно будет выполняться в AD DS.

В итоге, мы получим:

- Аутентификацию пользователей в iRedMail через Active Directory.
- Почтовые ящики и группы рассылки из активного каталога.
- Глобальную адресную книгу LDAP.
- Возможность быстрого отключения ящика путем отключения учетной записи пользователя в AD.

В официальной документации предоставлен материал для настройки Интеграции iRedMail с Microsoft Active Directory. Наша инструкция делает упор на официальное руководство с адаптацией на русский язык.

Прежде чем начать

1. Установленные сервисы

Предполагается, что у нас уже установлены и настроены:

- Почтовая система iRedMail (желательно, с хранением почтовых аккаунтов в OpenLDAP).
- Роль контроллера домена (Windows 2000 и выше).

Соответствующие инструкции по настройке данных систем будут приведены ниже.

Если у нас iRedMail уже установлен без использования ldap в качестве хранения пользователей, то устанавливаем дополнительные пакеты.

а) На Linux Deb (Ubuntu / Debian / Astra Linux):

apt update

apt install postfix-ldap dovecot-ldap ldap-utils

б) На Linux RPM (Rocky Linux / РЕД ОС / CentOS):

yum install openldap-clients

2. Используемые домен, имена и пути

В нашем примере будет использоваться домен **dmosk.ru**. Это соответствует формату записи BASE_DN **dc=dmosk,dc=ru**. Все пользователи у меня будут храниться в контейнере **users**, что соответствует формату записи **cn=Users,dc=dmosk,dc=ru**.

У вас будут другие записи, что нужно учитывать при настройке. Также нужно учитывать тип каталога в AD: если это контейнер, запись будет **cn=**, а если организационный юнит — **ou=**.

3. Сетевые настройки на сервере iRedMail

Для корректного взаимодействия с Active Directory, лучше всего, чтобы сервер iRedMail использовал DNS, на которых регистрирует свои запись AD DS. Как правило, это и есть сам контроллер домена.

Если мы не можем использовать данные серверы имен, то можно в файле hosts прописать адреса контроллеров домена, например:

vi /etc/hosts

192.168.0.15 dmosk.ru
192.168.0.16 dmosk.ru

** в данном примере мы указали, что для доменного имени **dmosk.ru** соответствуют два адреса **192.168.0.15** и **192.168.0.16**. Это наши предполагаемые контроллеры домена.*

4. Служебная учетная запись в AD

Необходимо создать учетную запись в Active Directory со стандартными правами. Она будет использоваться для привязки к AD по LDAP и получения списка всех пользователей и групп. Пароль данной записи не должен содержать символа **#**, так как он используется в Dovecot в качестве комментария и неправильно интерпретируется при проверке подлинности.

В нашем примере мы создадим пользователя с именем **vmail** во встроенном контейнере **users**. Таким образом, формат обращения к данной записи будет **cn=vmail,cn=users,dc=dmosk,dc=ru**. Вам нужно будет заменить данные значения в инструкции своими.

После создания пользователя, проверяем возможность подключения к LDAP с сервера iRedMail:

ldapsearch -x -H ldap://dmosk.ru -D 'vmail' -W -b 'cn=users,dc=dmosk,dc=ru'

* где:

- **-H ldap://dmosk.ru —** контроллер домена, к которому нужно подключиться. В данном примере мы подключаемся по доменному имени, который разрешится в IP-адрес одного из серверов AD.
- **-D 'vmail' —** имя учетной записи для BIND DN.
- **-b 'cn=users,dc=dmosk,dc=ru' —** путь контейнера, где нужно выполнить поиск пользователей.

Система попросит ввести пароль от учетной записи vmail:

Enter LDAP Password:

В итоге, мы должны получить список пользователей.

Postfix + Active Directory

Для удобства, разобьем процесс на несколько блоков — внесем изменения в конфигурационный файл Postfix, создадим дополнительные конфигурационные файлы с картами и выполним тестирование с последующим применением сделанных настроек.

Настройка Postfix

Отключаем настройки iRedMail. которые больше не будут использоваться:

```
postconf -e virtual_alias_maps='' ; \
postconf -e sender_bcc_maps='' ; \
postconf -e recipient_bcc_maps='' ; \
postconf -e relay_domains='' ; \
postconf -e relay_recipient_maps='' ; \
postconf -e sender_dependent_relayhost_maps=''
```

* где:

- **virtual_alias_maps** — формат и путь хранения алиасов для виртуальных пользователей.
- **sender_bcc_maps —** правила для копирования исходящих писем.
- **recipient_bcc_maps —** правила для копирования входящих писем.
- **relay_domains —** список доменов, на которые разрешена пересылка почты.
- **relay_recipient_maps —** список разрешенных адресов.
- **sender_dependent_relayhost_maps —** указание на список адресов и почтовых серверов, через которые нужно отправлять письма на эти адреса.

Добавляем имя своего почтового домена в smtpd_sasl_local_domainи virtual_mailbox_domains:

postconf -e smtpd_sasl_local_domain='dmosk.ru'

postconf -e virtual_mailbox_domains='dmosk.ru'

* где:

- **smtpd_sasl_local_domain —** домен для клиентов, которые проходят smtp-аутентификацию.
- **virtual_mailbox_domains —** формат и путь хранения доменов виртуальных почтовых аккаунтов.

Изменяем настройки транспортной карты:

postconf -e transport_maps='hash:/etc/postfix/transport'

Файл для получения списка отправителей SMTP:

postconf -e smtpd_sender_login_maps='proxy:ldap:/etc/postfix/ad_sender_login_maps.cf'

Проверка локальных почтовых пользователей и получение пути хранения почтового ящика:

postconf -e virtual_mailbox_maps='proxy:ldap:/etc/postfix/ad_virtual_mailbox_maps.cf'

Файл для получения адресов списков рассылки:

postconf -e virtual_alias_maps='proxy:ldap:/etc/postfix/ad_virtual_group_maps.cf'

Открываем файл:

vi /etc/postfix/main.cf

Комментируем строку **check_policy_service inet:127.0.0.1:7777**:

```
smtpd_recipient_restrictions =
   ...
#check_policy_service inet:127.0.0.1:7777

   smtpd_end_of_data_restrictions =
   #check_policy_service inet:127.0.0.1:7777
```

С внесением изменений в конфигурацию Postfix закончили. Идем дальше.

Создание карт

Создаем файл для транспортной карты:

vi /etc/postfix/transport

dmosk.ru dovecot

** в данном примере мы указываем, что для домена **dmosk.ru** в качестве транспортной службы будет использоваться **dovecot**.*

Создаем транспортную карты из файла:

postmap hash:/etc/postfix/transport

Создаем файл с настройками получения списка электронных адресов:

vi /etc/postfix/ad_sender_login_maps.cf

```
server_host      = dmosk.ru
server_port      = 389
version          = 3
bind             = yes
start_tls        = no
bind_dn          = vmail
bind_pw          = vmail_password
search_base      = cn=users,dc=dmosk,dc=ru
scope            = sub
```

```
query_filter     = (&(objectClass=person)(mail=%s))
result_attribute = mail
debuglevel       = 0
```

* обратите особое внимание на опции:

- **server_host —** адрес контроллера домена. Мы указали домен, который разрешается в один из активных контроллеров, который обслуживает данный домен.
- **bind_dn —** учетная запись для привязки к ldap.
- **bind_pw —** пароль для учетной записи привязки к ldap.
- **search_base —** адрес организационного подразделения в ldap, откуда будет вестись поиск.

Создаем следующий файл, в котором будут настройки пути до почтовых ящиков:

vi /etc/postfix/ad_virtual_mailbox_maps.cf

```
server_host      = dmosk.ru
server_port      = 389
version          = 3
bind             = yes
start_tls        = no
bind_dn          = vmail
bind_pw          = vmail_password
search_base      = cn=users,dc=dmosk,dc=ru
scope            = sub
query_filter     = (&(|(mail=%s)(otherMailbox=%u@%d))(objectClass=person))
result_attribute = mail
result_format    = %d/%u/Maildir/
debuglevel       = 0
```

* обратите особое внимание на опции:

- **server_host —** адрес контроллера домена. Мы указали домен, который разрешается в один из активных контроллеров, который обслуживает данный домен.
- **bind_dn —** учетная запись для привязки к ldap.
- **bind_pw —** пароль для учетной записи привязки к ldap.
- **search_base —** адрес организационного подразделения в ldap, откуда будет вестись поиск.
- **query_filter —** ldap-фильтр, по которому мы ищем пользователей. В нашем примере мы рассматриваем только objectClass=person (очетные записи пользоватлей), а также ищем по значениям атрибутов **mail** или **otherMailbox**. При этом,, атрибут mail является основным, а otherMailbox можно рассматривать как альтернативные почтовые адреса.

И последний файл, с помощью которого мы будем получать адресатов группы:

vi /etc/postfix/ad_virtual_group_maps.cf

```
server_host             = dmosk.ru
server_port             = 389
version                 = 3
bind                    = yes
start_tls               = no
bind_dn                 = vmail
bind_pw                 = vmail_password
search_base             = cn=users,dc=dmosk,dc=ru
scope                   = sub
query_filter            = (&(objectClass=group)(mail=%s))
special_result_attribute = member
leaf_result_attribute    = mail
result_attribute        = mail
debuglevel              = 0
```

* обратите особое внимание на опции:

- **server_host —** адрес контроллера домена. Мы указали домен, который разрешается в один из активных контроллеров, который обслуживает данный домен.

- **bind_dn —** учетная запись для привязки к ldap.
- **bind_pw —** пароль для учетной записи привязки к ldap.
- **search_base —** адрес организационного подразделения в ldap, откуда будет вестись поиск.

В последних трех файлах хранятся настройки обработки данных, которые мы получаем по LDAP. В качестве основного атрибута поиска пользователя или группы мы выбрали **mail** — адрес электронной почты.

Проверка и применение настроек

Создаем тестовых пользователя и группу в AD. Например, user@dmosk.ru и group@dmosk.ru. Обязательно, заполняем для них поле с почтовым адресом. В группу добавим созданного тестового пользователя.

Проверяем получение адреса для пользователя:

postmap -q user@dmosk.ru ldap:/etc/postfix/ad_sender_login_maps.cf

В итоге, мы должны получить в качестве результата свой email:

user@dmosk.ru

Проверяем, что система вернет путь для хранения почтовых сообщений:

postmap -q user@dmosk.ru ldap:/etc/postfix/ad_virtual_mailbox_maps.cf

dmosk.ru/user/Maildir/

Проверяем списки пользователей в группах:

postmap -q group@dmosk.ru ldap:/etc/postfix/ad_virtual_group_maps.cf

user@dmosk.ru

Если все команды вернули нам результаты, мы на правильном пути. В противном случае, в настроенных картах меняем значение опций **debuglevel** на **1** и смотрим лог в файле **/var/log/maillog**.

При успешном тестировании, перезапускаем postfix для применения настроек:

systemctl restart postfix

Dovecot + Active Directory

Открываем файл:

vi /etc/dovecot/dovecot.conf

Проверяем, чтобы у нас были следующие строки:

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

Откроем/создадим файл с настройками подключения Dovecot к Active Directory:

vi /etc/dovecot/dovecot-ldap.conf

Заменяем его содержимое на:

```
hosts          = dmosk.ru:389
ldap_version    = 3
auth_bind       = yes
dn              = vmail
dnpass          = vmail_password
```

```
base           = cn=users,dc=dmosk,dc=ru
scope          = subtree
deref          = never

iterate_attrs   = mail=user
iterate_filter  = (&(objectClass=person)(mail=*))

user_filter         = (&(objectClass=person)(|(mail=%u)(otherMailbox=%u)))
pass_filter         = (&(objectClass=person)(mail=%u))
pass_attrs          = userPassword=password
default_pass_scheme  = CRYPT
user_attrs          = mail=master_user,mail=user,=home=/var/vmail/vmail1/%Ld/%Ln/,=mail=maildir:~/Maildir/
```
* обратите особое внимание на опции:

- **hosts —** адрес контроллера домена. Мы указали домен, который разрешается в один из активных контроллеров, который обслуживает данный домен.
- **dnpass —** учетная запись для привязки к ldap.
- **bind_pw —** пароль для учетной записи привязки к ldap.
- **base —** адрес организационного подразделения в ldap, откуда будет вестись поиск. Есть ограничение по значению — оно не должно вести только на домен (например, **dc=dmosk,dc=ru** работать не будет).

Перезапускаем dovecot:

```
systemctl restart dovecot
```

Проверим наши настройки. Подключимся к нашему SMTP телнетом:

```
telnet localhost 143
```

> Если система пришлет ошибку, устанавливаем telnet.
>
> а) на системы DEB:
>
> ```
> apt install telnet
> ```
>
> б) на системы RPM:
>
> ```
> yum install telnet
> ```

Мы должны увидеть что-то на подобие:

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
* OK ... ready.
```

После вводим команду для аутентификации (точка в начале обязательна):

```
. login user@dmosk.ru user_password
```

** где **user@dmosk.ru —** созданный в AD пользователь для теста; **user_password —** его пароль.*

Если все корректно работает, мы должны увидеть:

```
. OK ... Logged in
```

Диагностика проблем

Если мы получим ошибку, то необходимо обратиться к логу, чтобы понять причину проблемы. Открываем файл:

```
vi /etc/dovecot/dovecot.conf
```

Добавляем:

```
auth_verbose = yes
auth_debug = yes
auth_debug_passwords = yes
```

Перезапускаем dovecot:

systemctl restart dovecot

Пробуем авторизоваться и после получения ошибки смотрим лог:

journalctl -e -u dovecot

Roundcube + Active Directory

Последнее, что мы рассмотрим в данной инструкции — настройка адресной книги в Roundcube, которая будет формироваться из AD.

Открываем конфигурационный файл:

vi /opt/www/roundcubemail/config/config.inc.php

Находим строки:

// Global LDAP address book.

После них должен идти блок настроек $config['ldap_public']["global_ldap_abook"]. Удаляем его и вставляем новые настройки:

```
$config['ldap_public']["ldap"] = array(
   'name'          => 'Global Address Book',
'hosts'         => array("dmosk.ru"),
   'port'          => 389,
   'use_tls'       => false,
   'ldap_version'  => '3',
   'network_timeout' => 10,
   'user_specific' => false,



'base_dn'       => "cn=users,dc=dmosk,dc=ru",
'bind_dn'       => "vmail",
'bind_pass'     => "vmail_password",
   'writable'      => false,



   'search_fields' => array('mail', 'cn', 'sAMAccountName', 'displayname', 'sn', 'givenName'),

   // mapping of contact fields to directory attributes
   'fieldmap' => array(
      'name'          => 'cn',
      'displayname'   => 'displayName',
      'surname'       => 'sn',
      'firstname'     => 'givenName',
      'jobtitle'      => 'title',
      'department'    => 'department',
      'company'       => 'company',
      'email'         => 'mail:*',
      'phone:work'    => 'telephoneNumber',
      'phone:home'    => 'homePhone',
      'phone:mobile'  => 'mobile',
      'phone:workfax' => 'facsimileTelephoneNumber',
      'phone:pager'   => 'pager',
      'phone:other'   => 'ipPhone',
      'street:work'   => 'streetAddress',
      'zipcode:work'  => 'postalCode',
      'locality:work' => 'l',
      'region:work'   => 'st',
      'country:work'  => 'c',
      'notes'         => 'description',
      'photo'         => 'jpegPhoto',   // Might be 'thumbnailPhoto' for
```

```
                                // compatibility with some other
                                // Microsoft software
        'website'       => 'wWWHomePage',
    ),
    'sort'          => 'cn',
    'scope'         => 'sub',
    'filter'        => "(&(|(objectclass=person)(objectclass=group)))",
    'fuzzy_search'  => true,
    'vlv'           => false,   // Enable Virtual List View to more
                                // efficiently fetch paginated data
                                // (if server supports it)
    'sizelimit'     => '0',     // Enables you to limit the count of
                                // entries fetched. Setting this to 0
                                // means no limit.
    'timelimit'     => '0',     // Sets the number of seconds how long
                                // is spend on the search. Setting this
                                // to 0 means no limit.
    'referrals'     => false,   // Sets the LDAP_OPT_REFERRALS option.
                                // Mostly used in multi-domain Active
                                // Directory setups
);
```

** желтым выделены опции, значения которых нужно заменить своими данными.*

Открываем Roundcube и создаем новое письмо для отправки. В списке получателей мы должны иметь возможность увидеть пользователей Active Directory.

Настройка квот

Если мы хотим включить квотирование для почтовых адресов, созданных в ldap, открываем файл:

vi /etc/dovecot/dovecot-ldap.conf

К директиве **user_attrs** нужно добавить строку **,postOfficeBox=quota_rule=*:storage=%{ldap:postOfficeBox}G**, итого мы получим:

user_attrs = mail=master_user,mail=user,=home=/var/vmail/vmail1/%Ld/%Ln/,=mail=maildir:~/Maildir/,postOfficeBox=quota_rule=*:storage=%{ldap:postOfficeBox}G

Перезапустим dovecot:

systemctl restart dovecot

Теперь в Active Directory заполняем атрибут пользователя **postOfficeBox**, в котором должен быть указан объем квоты в гигабайтах.

Готово.

Читайте также

1. Полноценный почтовый сервер с iRedMail на Ubuntu или Debian.

2. Установка и настройка iRedMail на CentOS.

3. Как установить роль контроллера домена на Windows Server.

4. Настройка Postfix + Dovecot + LDAP.

5. Установка и настройка Proxmox Mail Gateway.

Active Directory # Linux # Почта # Серверы

Дмитрий Моск — IT-специалист.
Настройка серверов, услуги DevOps.
Заказать настройку почты

Нужна бесплатная консультация?

Написать в телеграм-чат

Мини-инструкции

Как настроить автоматический запуск конвейера CI/CD в Jenkins при коммитах в Subversion

Развертывание OpenStack для тестовых целей с помощью DevStack

Как настроить возможность виртуализации внутри виртуализации Proxmox

Как настроить связку почтовой системы iRedMail с MS Active Directory

Настройка отказоустойчивого кластера Postgres + Patroni на Linux CentOS

Как обновить версию СУБД PostgreSQL на CentOS

Как установить программный брокер Kafka на Linux и выполнить базовые команды

Другие инструкции

Все статьи

Нужна помощь? Пишите: