

1.	Настройка почтового сервера на основе exim, dovecot .....	2
	Имеется.....	2
	Задача .....	2
	Подготовка Active Directory, DNS.....	2
	Настройка Exim .....	5
	Описание настроек подключения и макросов запросов.....	5
	Конфигурация роутеров .....	7
	Конфигурация транспортов .....	8
	Настройка Dovecot .....	14
	Проверка настройки exim, dovecot .....	16
	Настройка почтового клиента (Outlook Express) .....	17
2.	Установка SQUID и настройка прозрачного проксирования.....	19
	Конфигурация системы .....	19
	Задача .....	19
	Установка SQUID и настройка прозрачного проксирования.....	19
	Установка анализатора логов прокси-сервера SARG .....	23
3.	Установка Apache, MySQL.....	23
	Установка Web сервера .....	23
	Установка MySQL .....	24
	Проверка доступности, дополнительные конфигурации .....	25
4.	Установка OpenVPN.....	27
5.	Введение Linux-сервера в домен Windows.....	30
	Задача .....	30
	Настройка DNS .....	30
	Настройка синхронизации времени .....	31
	Настройка и ввод в домен .....	31
6.	Установка webadmin .....	33
7.	Установка FTP сервера VSFTPD .....	34
8.	Установка roundcube .....	34

## 1. Настройка почтового сервера на основе exim, dovecot

Имеется

---

1. Почтовый сервер на базе Exim + Dovecot, адрес почтового сервера mailserver.intra.local (10.180.11.212).
2. Контролер домена dc01. intra.local на базе MS Windows 2003 R2 с установленным и настроенным Active Directory. Адрес сервера 10.180.11.45

Задача

---

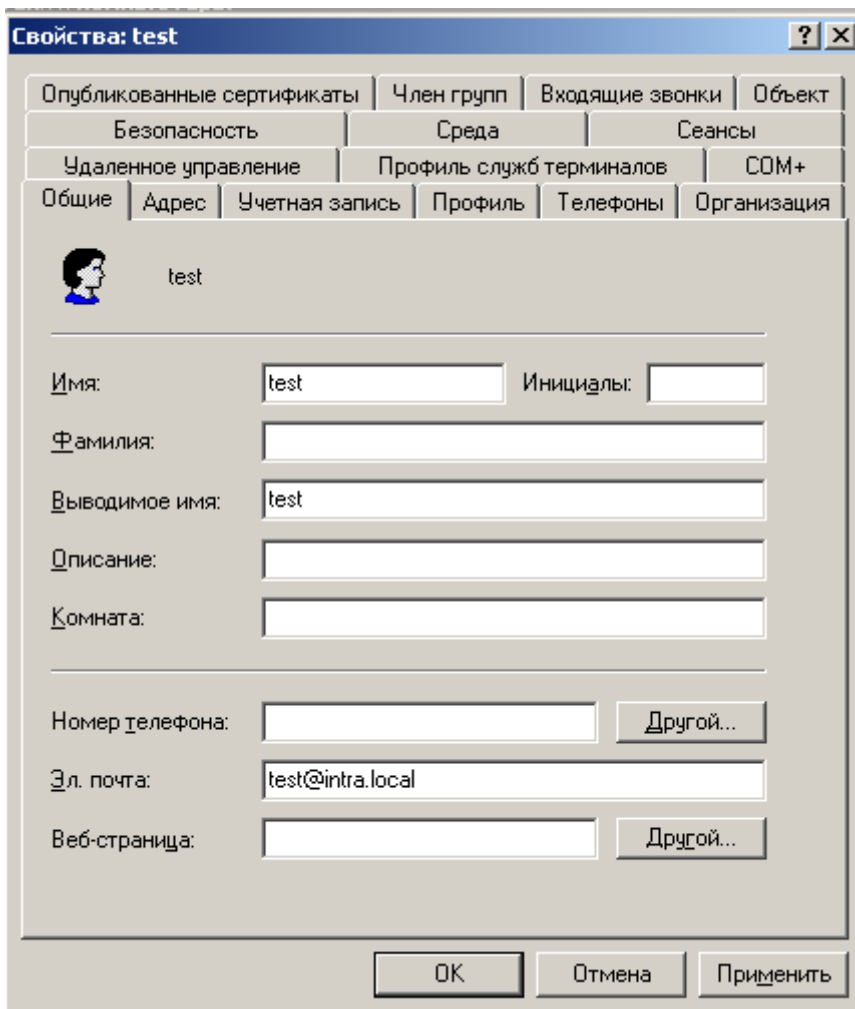
1. Для Exim организовать проверку наличия почтовых адресов в Active Directory.
2. Для Dovecot организовать авторизацию пользователей в Active Directory по логину пользователя в домене.
3. Настройка фильтрации почты.
4. Вся почта должна храниться в каталоге /home/mail, в котором:  
/home/mail/domain/<почтовый домен>/<почтовый пользователь>/.maildir/ - каталог пользователя почты

Подготовка Active Directory, DNS

---

Т.к. доступ к Active Directory у нас только авторизованный, то для его чтения в домене dc01. intra.local создайте пользователя домена, например exim. Задайте пароль пользователю exim, например P@ssword..

Запустите на контролера домена оснастку «Active Directory - пользователи и компьютеры», добавьте или найдите пользователя домена, которому нужно дать почтовый ящик на вашем сервере и откройте его свойства. В поле «Эл. почта» укажите его почтовый адрес. Примите изменения. Например: пользователь в домене test с почтовым ящиком test@intra.local.



Свойства: test

Опубликованные сертификаты | Член групп | Входящие звонки | Объект

Безопасность | Среда | Сеансы

Удаленное управление | Профиль служб терминалов | COM+

Общие | Адрес | Учетная запись | Профиль | Телефоны | Организация

test

Имя: test      Инициалы:

Фамилия:

Выводимое имя: test

Описание:

Комната:

Номер телефона:       Другой...

Эл. почта: test@intra.local

Веб-страница:       Другой...

OK      Отмена      Применить

В DNS пропишите адрес Вашего почтового сервера, а также создайте запись MX-запись для маршрутизации почты через почтовый сервер.

Почтовый обменник (MX) mailserver.intra.local

### Установка Exim и Dovecot

Для установки использовалась centos 5 x64, стандартный репозиторий (base). Предварительно отключаем firewall и selinux, в дальнейшем можно будет настроить firewall.

```
yum install exim dovecot
```

```
Dependencies Resolved
```

```
=====
=====
Package      Arch      Version      Repository    Size
-----
Installing:
dovecot      x86_64    1.0.7-7.el5_7.1  updates     1.7 M
exim         x86_64    4.63-10.el5    base         1.2 M
Installing for dependencies:
mysql        x86_64    5.0.77-4.el5_6.6  base         4.8 M
perl-DBI     x86_64    1.52-2.el5      base         600 k
```

```
[root@mailserver ~]# rpm -qa | grep dovecot
dovecot-1.0.7-7.el5_7.1
[root@mailserver ~]# rpm -qa | grep exim
exim-4.63-10.el5
```

Установим антивирус clamav. Включим собственно репозиторий из которого и установим. Создаем в папке /etc/yum.repos.d/ файл atrpms.repo следующего содержания:

```
[atrpms]
name=Red Hat Enterprise Linux 5 - x86_64 - ATrpms
baseurl=http://dl.atrpms.net/el5-x86_64/atrpms/stable
failovermethod=priority#
# requires stable
#
[atrpms-testing]
name=Red Hat Enterprise Linux 5 - x86_64 - ATrpms testing
baseurl=http://dl.atrpms.net/el5-x86_64/atrpms/testing
failovermethod=priority
enabled=0

#установим ключи
wget http://ATrpms.net/RPM-GPG-KEY.atrpms
rpm --import RPM-GPG-KEY.atrpms
```

Обновим exim:

```
yum --enablerepo=atrpms-testing update exim

rpm -qa | grep exim
exim-4.77-48.el5
```

Установка самого антивируса:

```
yum --enablerepo=atrpms install clamav

rpm -qa | grep clamav
clamav-0.97.3-61.el5
# В более ранних версиях скрипты автозапуска не создаются автоматически, поэтому лучше использовать
данную версию
#Сразу после установки доступно включение в автозагрузку
chkconfig --list | grep clamav
clamav      0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Прописываем в стартовые скрипты запуск exim, dovecot и clamav(антивирус):

```
chkconfig exim on
chkconfig dovecot on
chkconfig clamav on
```

```
service exim start
service dovecot start
service clamav start
```

Отключить стандартную почтовую службу:

```
chkconfig sendmail off
service sendmail stop
```

## Настройка Exim

### Описание настроек подключения и макросов запросов

Для хранения почты пользователей создадим каталог /home/mail, дать права доступ на чтение/запись пользователю exim и группе exim, так как службы exim и dovecot у нас будут работать от пользователя exim. Для анализа почты на вирусы добавим пользователя clamav в группу exim.

```
# Пользователь exim создается автоматически
id exim
uid=93(exim) gid=93(exim) groups=93(exim),12(mail)

mkdir -p /home/mail
chmod 0770 /home/mail
chown exim:exim /home/mail
# Добавляем антивирус в группу exim useradd -G {group-name} username
# Или непосредственно добавляем в группу через файл /etc/group
useradd -G exim clamav
useradd -G exim clam
id clamav
uid=102(clamav) gid=104(clamav) groups=104(clamav),93(exim)
id clam
uid=101(clam) gid=103(clam) groups=103(clam),93(exim)
service clamav restart
cd /etc/exim/
mkdir db
mkdir filters
chown exim:exim db
chown exim:exim filters
```

Добавляем в hosts имя удаленного сервера:

```
cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          mailserver.intra.local mailserver localhost.localdomain localhost
10.180.11.212     mailserver.intra.local mailserver
10.180.11.45      dc01.infra.local dc01
```

cat /etc/resolv.conf

```
domain intra.local
search intra.local
nameserver 10.180.11.45
```

Далее правим конфигурационный файл `exim.conf`. В тексте конфигурационного файла есть ряд своих значащих символов:

«!» - указывает на отрицание, его можно интерпретировать как «НЕ» или «КРОМЕ»;

«=» - присваивает значение переменным;

«+» - используется при обращении к переменным, объявленным ранее.

Сам конфигурационный файл состоит из нескольких частей:

**Главная конфигурация** – указываются общие опции сервера.

**Конфигурация ACL** - описываются списки и условия доступа. Делится, в свою очередь, на разделы, посвященные эяпу в диалоге SMTP, перед которым будет проходить проверка. Например, раздел `acl_smtp_rcpt` укажет на выполнение всех проверок после SMTP- команды RCPT TO. Принцип работы основан на директивах, указывающих, что делать с письмом, если оно удовлетворило условиям того или иного утверждения в `acl`:

**deny (drop)** – отвергнуть письмо;

**warn** – записать строку в лог, добавить заголовок и передать следующему утверждению `acl`;

**accept** – принять письмо.

**Конфигурация роутеров** – описывает все возможные маршруты для почты, например: отправить адресату в другом домене, используя DNS, или перенаправить по другому адресу и т.д. Письмо проходит роутеры в порядке их размещения в конфиге, пока не удовлетворит одному из условий, описанных в них.

**Конфигурация транспортов** - описывает типы доставки письма: отправить по smtp, положить в папку, добавить в файл, передать другому процессу и т.д. Порядок расположения не важен.

**Конфигурация повторов** – описывает, что делать с недоставленным в первый раз сообщением и через какие промежутки времени повторить отправку.

**Конфигурация аутентификации** – описывает все поддерживаемые типы аутентификации.

В данном руководстве представлены только части конфигов, измененных в стандартном конфигурационном файле.

В самом начале файла `exim.conf` в разделе «MAIN CONFIGURATION SETTINGS» разместим описание подключения и макросов проверки/поиска, к которым будем обращаться позже:

**Файл:** `exim.conf`

```
#####MAIN CONFIGURATION SETTINGS#####
# Имя хоста, как оно указано в MX-записи DNS-зоны нашего внешнего домена. Используется в командах
HELO, EHLO.
# Указываем значение, которое вернет функция hostname
primary_hostname = mailserver.intra.local
# LDAP-серверы (контроллеры домена)
ldap_default_servers = <; 10.180.11.45:3268
```

```
# Зададим BindDN
LDAP_AD_BASE_DN = "DC=intra,DC=local"
# Зададим пользователя для чтения дерева каталогов
LDAP_AD_BINDDN = "CN=exim,CN=Users,DC=intra,DC=local"
# Зададим пароль для чтения дерева каталогов
LDAP_AD_PASS = "P@ssw0rd"

# Зададим макрос проверки наличия пользователя, результатом является
# искомый адрес, если он принадлежит кому то из пользователей домена,
# иначе пустая строка
LDAP_AD_MAIL_RCPT = \
    user=LDAP_AD_BINDDN \
    pass=LDAP_AD_PASS \
    ldap:///DC=intra,DC=local?mail?sub?(&(objectClass=top)\
    (objectClass=user)(objectClass=organizationalPerson)\
    (objectClass=person)(mail=${quote_ldap:${local_part}@${domain}}))

# Изменяем существующие записи. Добавляем к локальному интерфейсу ip адрес почтового сервера
local_interfaces = <; 127.0.0.1 ; 10.180.11.212

#список доменов, для которых принимаем почту как для локальных;
domainlist local_domains = @ : localhost : localhost.localdomain
#список доменов, для которых разрешено принимать почту;
domainlist relay_to_domains = intra.local
#список адресов (IP) с которых разрешено принимать почту;
hostlist relay_from_hosts = 127.0.0.1

# Обработка спама
system_filter = /etc/exim/filters/system-filter

# Вводим названия acl`ов для проверки почты. (Это
# необязательно, если вы делаете открытый релей, или хотите
# принимать вообще всю почту с любого хоста для любых
# получателей..)Не добавляем если существует.
acl_smtp_rcpt = acl_check_rcpt
acl_smtp_data = acl_check_data

#Подключение антивируса
av_scanner = clamd:/var/run/clamav/clamd.socket
```

Таким образом мы определили макрос, который ищет E-mail адресата в атрибуте mail (Эл. Почта) у всех объектов «Пользователь» в Active Directory и возвращает содержимое этого поля на каждую найденную строку (в данном случае всегда будет адрес получателя).

## Конфигурация роутеров

Роутеры являются правилами, определяющими каким транспортом обрабатывать письмо. Выполняются они исключительно последовательно, друг за другом. Если какой либо из роутеров выявил, что обрабатываемое письмо должно быть направлено транспорту, для доставки, или отвергнуто, то все следующие роутеры уже не получают письмо для обработки. Это свойство нужно учитывать при их настройке. Последовательность для них важна, т.к. письмо будет проходить по ним сверху вниз, пока не удовлетворит одному из условий и будет передано транспорт. Все изменения вносятся в раздел ROUTERS CONFIGURATION.

**Файл:** exim.conf

```
##### ROUTERS CONFIGURATION #####
# Закомментируем стандартный способ поиска
#dnslookup:
# driver = dnslookup
# domains = ! +local_domains
# transport = remote_smtp
# ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
# no_more

# Драйвер алиасов пользователей
ldap_aliases:
  driver = redirect
  allow_fail
  allow_defer
  data = ${lookup {$local_part@$domain}|search*@{/etc/exim/db/aliases}}
  file_transport = local_LDAP_delivery
  pipe_transport = local_LDAP_delivery
  directory_transport = local_LDAP_delivery
# Теперь добавляем роутеры для проверки пользователей в Active Directory
# Проверяем есть ли такой ящик у кого то из пользователей AD
LDAP_check:
  driver = redirect
  domains = +local_domains
  allow_fail
  allow_defer
  # Проверяем наличие запрошенного ящика в Active Directory
  data = ${lookup ldapm {LDAP_AD_MAIL_RCPT}\
    {${local_part}@${domain}} {:fail: User unknown}}

# Ну и после всех проверок доставим письмо в каталог пользователя
local_LDAP_user:
  driver = accept
  transport = local_LDAP_delivery
  cannot_route_message = Unknown user
```

Обратите внимание на тот факт, что запрос в роутере LDAP\_check в случае ошибки возвращает непустое значение, блокирующее дальнейшую обработку писем, адреса которых не прошли проверку, если вам нужно дальнейшую обработку таких писем между, то в запросе просто удалите текст «{:fail: User unknown}» в описании атрибута data роутера LDAP\_check.

## Конфигурация транспортов



Транспорт отвечает за конечную доставку сообщений: отправку по smtp, запись в файл или папку. Последовательность в них не важна т.к. роутеры определяют, каким транспортом пользоваться. Все изменения вносятся в раздел TRANSPORTS CONFIGURATION.

**Файл:** exim.conf

```
##### TRANSPORTS CONFIGURATION #####
begin transports

# Доставка почты в каталоги пользователей
local_LDAP_delivery:
  driver = appendfile
  directory = /home/mail/domain/$domain/$local_part/.maildir/
  maildir_format
  delivery_date_add
  envelope_to_add
  return_path_add
  mode = 0660
  no_mode_fail_narrower
```

## Конфигурация фильтров (ACL)

В данном разделе содержатся условия фильтрации почты. Порядок расположения условий важен, т.к. письмо будет проходить их как в правилах файервола: сверху вниз, пока не удовлетворит какой либо директиве "deny" или "accept". Фильтры могут изменяться в связи с потребностями и не все являются обязательными. Фильтры можно настраивать в последнюю очередь, после того как убедись в работоспособности остальной конфигурации. Обращаем внимание, что некоторые фильтры уже существуют или требуют небольших изменений, а также обращаем внимание на разделы конфигурации.

**Файл:** exim.conf

```
### конфигурация ACL для входящей почты
begin acl

# Эти правила срабатывают для каждого получателя
acl_check_rcpt:

# принимать сообщения которые пришли с локалхоста,
# не по TCP/IP
accept hosts = :

# Это правило блокирует адреса, локальные части которых начинаются или содержат знаки @ % ! / or |.
deny message = Restricted characters in address
  domains = +relay_to_domains
  local_parts = ^[.] : ^.*[!%/|]

# Проверяем недопустимые символы для нелокальных получателей
deny message = Restricted characters in address
  domains = !+relay_to_domains
  local_parts = ^[./|] : ^.*[!%!] : ^.*[\\.\.\/]
```

```
# Запрещаем пользователей с хостами, попадающими под список ip-адресов blacklist
deny    message = This ip-address in our blacklist
        hosts = net32-lsearch;/etc/exim/db/blacklist

# Запрещаем тех, кто не обменивается приветственными сообщениями (HELO/EHLO)
deny message    = "HELO/EHLO require by SMTP RFC"
condition      = ${if eq{$sender_helo_name}{}}{yes}{no}}

# Запрещаем тех, кто подставляет свой IP в HELO
deny    message    = We don't allow domain literals, sorry - many spam...
        hosts      = !+relay_from_hosts:*
        condition  = ${if isip{$sender_helo_name}{yes}{no}}

# Правило разрешающее указанные в списке хосты
accept hosts = net32-lsearch;/etc/exim/db/whitelist

# Запрещаем, если невозможно проверить отправителя
require verify    = sender

# Устанавливаем в 0 переменную acl_c1. По ее значению дальше в системном фильтре будет установлено,
# по какому правилу письмо было определено как SPAM. Краткая информация об этом будет помещена в
исходник
# письма, дабы помочь нам сразу понять, какое правило сработало на искомом письме
warn    set acl_c1    = 0

# Начисляем очки за SPAM тем, кто подставляет имя нашего сервера в команде HELO
warn    hosts        = !+relay_from_hosts : !localhost
        condition    = ${if eq{$acl_c1}{0}{yes}{no}}
        condition    = ${if match_domain{$sender_helo_name}{$primary_hostname : +local_domains :
+relay_to_domains}{yes}{no}}
        logwrite     = SPAM. In HELO a name of our server
        set acl_c1   = ${eval:$acl_c1+1}

# Проверяем совпадение PTR и A записей DNS для хостов
warn    hosts        = !+relay_from_hosts : !localhost
        condition    = ${if eq{$acl_c1}{0}{yes}{no}}
        condition    = ${if eq{$host_lookup_failed}{1}{yes}{no}}
        logwrite     = SPAM. Yours PTR and A records DNS do not conform
        set acl_c1   = ${eval:$acl_c1+2}

# Проверяем хост-отправитель в общедоступных «черных» списках RBL и DNSBL
warn    hosts        = !+relay_from_hosts : !localhost
        condition    = ${if eq{$acl_c1}{0}{yes}{no}}
        dnslists     = cbl.abuseat.org : sbl-xbl.spamhaus.org : bl.spamcop.net
        logwrite     = SPAM. You in blacklist - $dnslist_domain --> $dnslist_text; $dnslist_value
```

```
set acl_c1 = ${eval:$acl_c1+3}
```

```
# Callback или «обратный вызов». Попытка проверить на существование адрес отправителя в процессе получения
```

```
# сообщения. Как правило, помогает от несуществующих почтовых адресов
```

```
warn hosts      = !+relay_from_hosts : !localhost
  condition     = ${if eq{$acl_c1}{0}{yes}{no}}
    !senders    = : verify@*
  !authenticated = *
  !verify       = sender/callout=15s
  logwrite      = SPAM. $acl_verify_message: $sender_address - does not exist
  set acl_c1    = ${eval:$acl_c1+4}
```

#### **acl\_check\_data:**

```
# В блоке проверки содержимого письма (acl_check_data) добавляем правило,
```

```
# блокирующее письма с потенциально опасным содержимым
```

```
deny message = Contains ".$found_extension" file (blacklisted).
```

```
demime = exe:com:vbs:bat:pif:scr:js:cab:wsh:msi:hta:\
```

```
vb:vbe:jse:cpl:reg:misp:msi:mst
```

```
# Проверяем письмо на вирусы
```

```
deny malware = *
```

```
message = This message contains a virus ($malware_name).
```

```
# блокируем письма с китайскими символами
```

```
deny message = "this is spam - denied"
```

```
condition = ${if match{$message_body} \
  {105[-_]*51[-_]*86|778[-_]*98[-_]*94} \
  {yes}{no}}
```

```
# проверяем MIME
```

```
deny message = This message contains a MIME error ($demime_reason)
```

```
demime = *
```

```
condition = ${if >{$demime_errorlevel}{2}{1}{0}}
```

```
# Сообщения с NUL-символами
```

```
deny message = This message contains NUL characters
```

```
log_message = NUL characters!
```

```
condition = ${if >{$body_zerocount}{0}{1}{0}}
```

```
# Синтаксис заголовков
```

```
deny message = Incorrect headers syntax
```

```
hosts = !+relay_from_hosts:*
```

```
!verify = header_syntax
```

```
# Пропускаем остальное
```

```
accept
```

Чтобы пометить заголовком **\*\*\*SPAM\*\*\*** сомнительные письма, попавшие под правило acl, составляем системный фильтр. Он добавляет в тему письма слово **\*\*\*SPAM\*\*\***, а также добавляет заголовки внутри с меткой "X-Spam\_FM:yes", "X-Spam\_Report" с описанием причины, по которой письмо попало в спам. Файл system-filter создаем вручную, устанавливаем владельцем exim.

## Конфигурация аутентификации

**Файл:** exim.conf

```
begin authenticators

dovecot_login:
  driver = dovecot
  public_name = LOGIN
  server_socket = /var/run/dovecot/auth-client
# setting server_set_id might break several headers in mails sent by authenticated smtp. So be careful.
  server_set_id = $auth1

dovecot_plain:
  driver = dovecot
  public_name = PLAIN
  server_socket = /var/run/dovecot/auth-client
  server_set_id = $auth1
```

**Файл:** /etc/exim/filters/system-filter

```
# # Add second subject line with ***SPAM*** if message
# detected as spam
if $acl_c1 contains "1"
then
  headers add "Old-Subject: $rh_subject:"
  headers remove "Subject"
  headers add "Subject: ***SPAM*** $rh_old-subject:"
  headers add "X-Spam-FM: YES"
  headers add "X-Spam-Report: Forbidden to use IP-address instead of the host name in HELO"
  headers remove "Old-Subject"
endif
if $acl_c1 contains "2"
then
  headers add "Old-Subject: $rh_subject:"
  headers remove "Subject"
  headers add "Subject: ***SPAM*** $rh_old-subject:"
  headers add "X-Spam-FM: YES"
  headers add "X-Spam-Report: Yours PTR and A records DNS do not conform"
  headers remove "Old-Subject"
endif
if $acl_c1 contains "3"
then
```

```
headers add "Old-Subject: $rh_subject:"
headers remove "Subject"
headers add "Subject: ***SPAM*** $rh_old-subject:"
headers add "X-Spam-FM: YES"
headers add "X-Spam-Report: You in blacklist"
headers remove "Old-Subject"
endif
if $acl_c1 contains "4"
then
headers add "Old-Subject: $rh_subject:"
headers remove "Subject"
headers add "Subject: ***SPAM*** $rh_old-subject:"
headers add "X-Spam-FM: YES"
headers add "X-Spam-Report: Sender address - does not exist"
headers remove "Old-Subject"
endif
```

## Содержимое каталога db

Рассмотрим содержимое списков, на которые есть ссылки в конфигурации exim: blacklist, whitelist и dealup\_host. В данные списки можем добавлять нужные нам хосты после чего необходимо перезапустить службу exim. Все файлы создаем вручную, устанавливаем владельца exim. Названия файлов и путь к ним может быть любым, главное условие, чтобы путь к файлу был прописан в конфигурационном файле.

```
touch blacklist
touch whitelist
touch dealup_host
touch aliases
chown exim:exim <имя файла>
```

Первый список – это ручной black-лист, в котором могут указываться целые зоны (при условии, что у вас нет адресатов в этих зонах):

**Файл:** /etc/exim/db/blacklist

```
# spammers domains
*.pl
*.it
*.nl
*.cl
*.br
```

Следующий список содержит регулярные выражения – шаблоны для поиска типовых DNS-имен хостов, принадлежащих провайдерам домашнего Интернета. Таким образом, защищаемся от домашних ПК, зараженных вирусами-спамботами:

**Файл:** /etc/exim/db/dialup\_hosts

```
# dialup hosts
^\.*dsl\.*
^\.*dialup\.*
^\.*dialin\.*
^\.*pool\.*
^\.*peer\.*
^\.*dhcp\.*
^\.*dynamic\.*
^\.*cable\.*
^\.*ppp\.*
```

Список ниже содержит ручной список white list доменов, письма из которых помечаются как спам из-за неверно настроенных почтовых серверов (либо не прописана обратная зона, либо в команде HELO указывается неверное имя и т.п.)

**Файл:** /etc/exim/db/whitelist

```
# white list, любой хост
111.com
```

Следующий файл содержит список алиасов для существующих почтовых ящиков. Поступающая корреспонденция на алиас автоматически перенаправляется в существующий почтовый ящик, описанный в этом файле.

**Файл:** /etc/exim/db/aliases

```
#В начале алиас затем реальный адрес через пробел.
tttt@intra.local test@intra.local
```

## Настройка Dovecot

Настраиваем Dovecot на свой вкус и цвет. Т.к. Все пользователи у меня виртуальные, и каталог с почтовыми папками принадлежит пользователю exim, то аутентификация и работа с каталогами почты была настроена на пользователя exim, таким образом в секции общих настроек были установлены следующие опции:

**Файл:** /etc/dovecot.conf

```
mail_location = maildir:/home/mail/domain/%d/%n/.maildir
mail_access_groups = exim
mail_full_filesystem_access = no
mail_drop_priv_before_exec = yes
first_valid_uid = 93
last_valid_uid = 93
first_valid_gid = 93
last_valid_gid = 93
```

```
#Далее ищем в конфигурационном файле записи связанные с пользователями и меняем на пользователя  
exim  
mail_privileged_group = exim  
mail_access_groups = exim  
log_path = /var/log/dovecot/dovecot.log
```

В строках указаны uid пользователя exim, и gid группы exim из файла /etc/passwd.

```
mkdir -p /var/log/dovecot
```

Секция auth default была приведена к следующему виду (удаляем существующий раздел и заменяем):

**Файл:** /etc/dovecot.conf

```
auth default {  
mechanisms = plain login  
passdb ldap {  
  args = /etc/dovecot/dovecot-ldap.conf  
}  
userdb ldap {  
  args = /etc/dovecot/dovecot-ldap.conf  
}  
user = exim  
socket listen {  
  client {  
    path = /var/run/dovecot/auth-client  
    mode = 0666  
  }  
}  
}
```

Создаем файл dovecot-ldap.conf:

```
cd /etc  
mkdir dovecot  
touch dovecot-ldap.conf  
chown -R exim:exim dovecot
```

Файл /etc/dovecot/dovecot-ldap.conf имеет следующее содержимое, где uid можно посмотреть id exim:

**Файл:** /etc/dovecot/dovecot-ldap.conf

```
hosts = 10.180.11.45:3268  
dn = CN=exim,CN=Users,DC=intra,DC=local
```

```
dnpass = P@ssw0rd
auth_bind = yes
ldap_version = 3
base = dc=intra, dc=local

# Поиск в поддеревьях
#
deref=searching
scope=subtree
#mail - это ldap запрос к AD, uid gid пользователя exim
user_attrs = mail=user, uid=93, gid=93

user_filter= (&(objectClass=user)(objectClass=person)(sAMAccountName=%n))

# Параметры пароля
#pass_attrs=sAMAccountName=user
pass_filter = (&(objectClass=user)(objectClass=person)(sAMAccountName=%n))

user_global_uid = 93
user_global_gid = 93

# Заменяем имя текущего пользователя на его E-mail
pass_attrs = mail=user
```

## Проверка настройки exim, dovecot

---

Перезапускаем службы

```
service exim restart
service dovecot restart
```

Проверяем логи на ошибки, при отсутствии ошибок проверяем работоспособность. Добавляем разрешения на папки:

```
chown -R exim:exim /var/spool/exim/scan/
chmod -R 777 /var/spool/exim/
service clamav restart
```

Для начала проверьте доступность Вашего домена для почтового сервера. Чтобы проверить все ли мы правильно настроили, попытаемся подключиться к нашему серверу.

```
[root@mailserver ~]# telnet mailserver 110
```



```
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
+OK Dovecot ready.
user test      --пользователь который есть у нас в домене
+OK
pass P@ssw0rd
+OK Logged in.
```

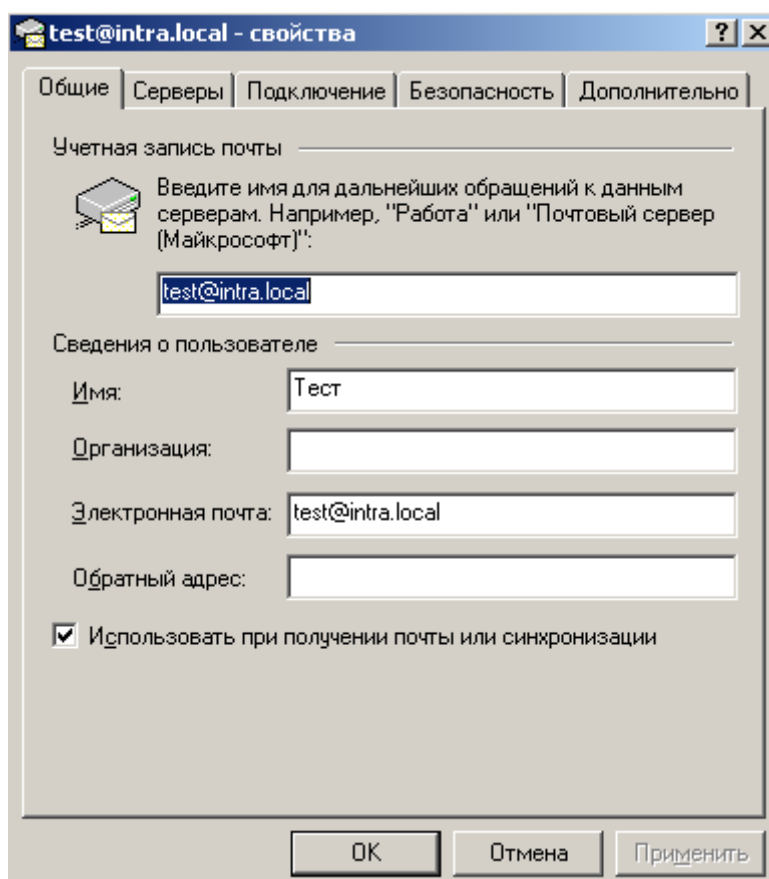
Если возникнут проблемы, более подробную информацию об ошибке смотрим в логе maillog или в файле указанном в переменной log\_path в файле dovecot.conf

```
[root@mailserver ~]# telnet mailserver 25
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 mailserver.intra.local ESMTP Exim 4.63 Fri, 13 Jan 2012 15:16:37 +0200
ehlo HELLO
250-mailserver.intra.local Hello localhost [127.0.0.1]
250-SIZE 52428800
250-PIPELINING
250-STARTTLS
250 HELP
mail from: test@intra.local
250 OK
rcpt to: test@intra.local
250 Accepted
data
354 Enter message, ending with "." on a line by itself
test
.
250 OK id=1RIh0S-0003Jd-W2
quit
```

Новое письмо сразу попадет в папку пользователя например:  
/home/mail/domain/intra.local/test/.maildir/new/, после получения письма на стороне клиента, письмо из этой папки исчезнет.

## Настройка почтового клиента (Outlook Express)

Для тестирования отправки получения почты будем использовать, стандартный почтовый клиент Outlook Express. Outlook Ex Сервис -> учетные записи ->Добавить -> почта -> Имя пользователя -> Почта(например ivan@domain.ru)-> сервер входящей и исходящей почты(указываем наш почтовый сервер) -> Учетная запись (ivan@domain.ru) и пароль этого пользователя в АД (учетная запись для входа в домен).



test@intra.local - свойства

Общие Серверы Подключение Безопасность Дополнительно

Учетная запись почты

Введите имя для дальнейших обращений к данным серверам. Например, "Работа" или "Почтовый сервер (Майкрософт)":

test@intra.local

Сведения о пользователе

Имя: Тест

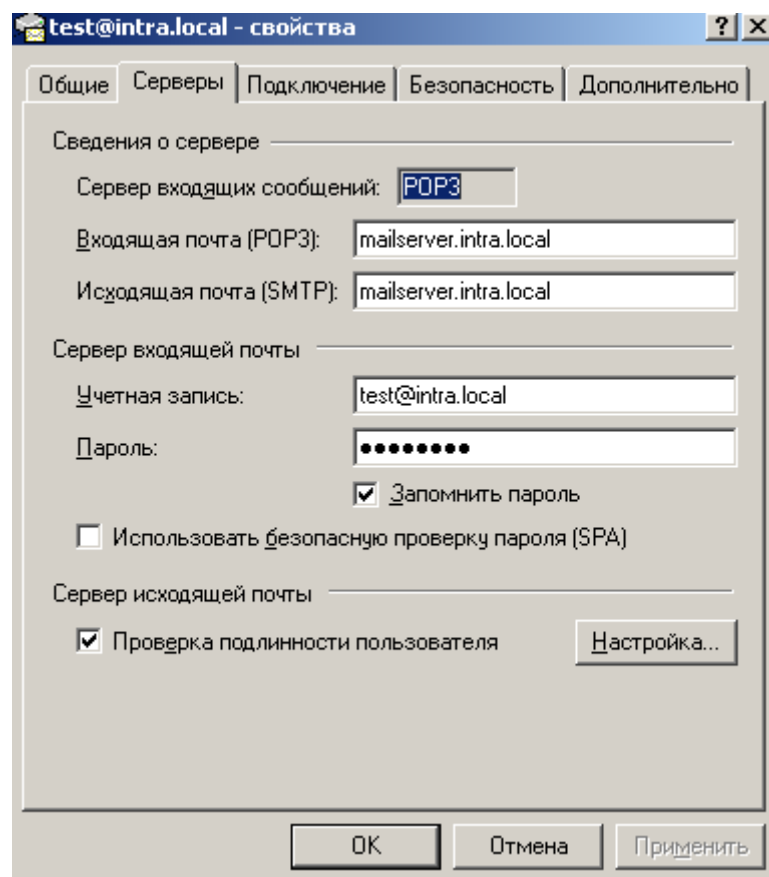
Организация:

Электронная почта: test@intra.local

Обратный адрес:

Использовать при получении почты или синхронизации

OK Отмена Применить



test@intra.local - свойства

Общие Серверы Подключение Безопасность Дополнительно

Сведения о сервере

Сервер входящих сообщений: POP3

Входящая почта (POP3): mailserver.intra.local

Исходящая почта (SMTP): mailserver.intra.local

Сервер входящей почты

Учетная запись: test@intra.local

Пароль: .....

Запомнить пароль

Использовать безопасную проверку пароля (SPA)

Сервер исходящей почты

Проверка подлинности пользователя Настройка...

OK Отмена Применить

После настройки клиента можем зайти и получить почту.

## 2. Установка SQUID и настройка прозрачного проксирования

### Конфигурация системы

1. Интерфейс eth0 – с доступом к интернету
2. Интерфейс eth1 – с доступом только в локальную сеть

### Задача

1. Настроить прозрачное проксирование, используя прокси сервер SQUID
2. Настроить правила

### Установка SQUID и настройка прозрачного проксирования

Обновим ОС до последней версии

```
yum update -y
```

Устанавливаем прокси сервер

```
yum install squid
```

После установки, добавляем его в автозагрузку

```
chkconfig squid on
```

Теперь приступаем к редактированию конфигурационного файла SQUID. Выполнив следующую команду, мы получим стандартный файл конфигурации без комментариев и лишних пробелов:

```
grep -v "^#" /etc/squid/squid.conf | sed -e '/^$/d'
```

Копируем получившийся вывод.  
Очищаем конфигурационный файл

```
/dev/null > /etc/squid/squid.conf
```

Вставляем в файл, скопированный нами, вывод. Для первого запуска, нам будет достаточно внести только некоторые изменения в настройки сервера.

Добавляем в файл /etc/squid/squid.conf параметр `visible_hostname` и через пробел пишем полное имя нашего сервера.

**Файл:** /etc/squid/squid.conf

```
visible_hostname <имя сервера>
```

Теперь, находим параметр `http_port 3128` и через пробел дописываем слово `transparent`. Эта опция включает режим прозрачного проксирования запросов.

Так же необходимо разрешить доступ к серверу из нашей локальной сети, для этого добавляем в файл `squid.conf` еще 2 строки:

**Файл:** /etc/squid/squid.conf

```
acl lan src 10.180.0.0/16
```

```
http_access allow lan
```

Адрес сети нужно заменить на свой.

В итоге, должен получиться файл с таким содержимым:

**Файл:** /etc/squid/squid.conf

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80      # http
acl Safe_ports port 21     # ftp
acl Safe_ports port 443   # https
acl Safe_ports port 70    # gopher
acl Safe_ports port 210   # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280   # http-mgmt
acl Safe_ports port 488   # gss-http
acl Safe_ports port 591   # filemaker
acl Safe_ports port 777   # multiling http
acl CONNECT method CONNECT

acl lan src 10.180.0.0/16

http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access allow localhost
http_access allow lan
http_access deny all
icp_access allow all

http_port 3128 transparent

visible_hostname proxy
hierarchy_stoplist cgi-bin ?
access_log /var/log/squid/access.log squid
acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY
refresh_pattern ^ftp:      1440 20% 10080
refresh_pattern ^gopher:  1440 0% 1440
refresh_pattern .         0 20% 4320
```

```
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
coredump_dir /var/spool/squid
```

Для фильтрации пользователей по их IP адресам необходимо добавлять правила на основе такой конструкции:

```
acl <имя правила> src <адрес компьютера или сети>
http_access allow <имя правила>
Например:
acl user1 src 10.180.11.11/32
http_access allow user1
```

Теперь необходимо внести кое-какие изменения в настройки самой ОС. Открываем файл `/etc/sysctl.conf`, находим параметр `net.ipv4.ip_forward` и меняем значение с 0 на 1. Далее нам необходимо настроить фаервол. Для облегчения задачи есть скрипт, который внесет все необходимые начальные настройки автоматически. Создаем файл `firewall.sh` с таким содержанием

**Файл:** `firewall.sh`

```
#!/bin/sh
# squid server IP
SQUID_SERVER="10.180.11.225"
# Interface connected to Internet
INTERNET="eth0"
# Interface connected to LAN
LAN_IN="eth1"
# Squid port
SQUID_PORT="3128"
# DO NOT MODIFY BELOW
# Clean old firewall
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
# Load IPTABLES modules for NAT and IP conntrack support
modprobe ip_conntrack
modprobe ip_conntrack_ftp
# For win xp ftp client
#modprobe ip_nat_ftp
echo 1 > /proc/sys/net/ipv4/ip_forward
# Setting default filter policy
iptables -P INPUT DROP
```

```
iptables -P OUTPUT ACCEPT
# Unlimited access to loop back
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A INPUT -i $INTERNET -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 21 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 20 -j ACCEPT
#Если на сервере установлена почтовая служба SMTP, разрешаем к ней доступ
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
#Разрешаем доступ к серверу по протоколу SSH
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
#Разрешаем доступ к портам веб сервера
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
#Разрешаем доступ к серверу баз данных MySQL
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
#Разрешаем доступ к прокси серверу SQUID
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 3128 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 3128 -j ACCEPT
#Если на сервере используется служба DNS, разрешаем к ней доступ
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT
#Открываем порты которые мы используем для пассивного режима FTP сервера
iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 1500:1550 -j ACCEPT
iptables -A INPUT -m state --state NEW -m udp -p udp --dport 1500:1550 -j ACCEPT
# set this system as a router for Rest of LAN
iptables --table nat --append POSTROUTING --out-interface $INTERNET -j MASQUERADE
iptables --append FORWARD --in-interface $LAN_IN -j ACCEPT
# unlimited access to LAN
iptables -A INPUT -i $LAN_IN -j ACCEPT
iptables -A OUTPUT -o $LAN_IN -j ACCEPT
# DNAT port 80 request coming from LAN systems to squid 3128 ($SQUID_PORT) aka transparent proxy
iptables -t nat -A PREROUTING -i $LAN_IN -p tcp --dport 80 -j DNAT --to $SQUID_SERVER:$SQUID_PORT
# if it is same system
iptables -t nat -A PREROUTING -i $INTERNET -p tcp --dport 80 -j REDIRECT --to-port $SQUID_PORT
# ACCEPT everything
iptables -A INPUT -j ACCEPT
```

Разрешим его исполнение командой

```
chmod +x firewall.sh
```

Теперь запустив этот файл, все настроится автоматически, останется только сохранить изменения командой

```
service iptables save
```

В завершении всего включаем автозагрузку iptables командой

```
service iptables on
```

Отключаем SELinux, изменив параметр SELINUX в файле /etc/sysconfig/selinux со значения enforcing на disabled

Перезапускаем сервер и после перезагрузки все службы запустятся автоматически, остается только на клиентских компьютерах поставить в качестве шлюза наш сервер и проверить его работоспособность.

### Установка анализатора логов прокси-сервера SARG

Перед установкой этого пакета в системе уже должен быть установлен веб-сервер Apache (пакет httpd).

Устанавливаем пакет sarg из репозитория rpmforge командой:

```
yum --enablerepo=rpmforge install sarg
```

После установки в системе будут созданы ежедневное, еженедельное и месячное задания по генерации отчетов о работе пользователей в интернет. Отчеты генерируются в директорию /var/www/sarg и доступны для просмотра по ссылке <http://<имя сервера>/sarg>

## 3. Установка Apache, MySQL

### Установка Web сервера

Зайдем под пользователем root

```
su -
```

Установим Apache (httpd) Web server и PHP

```
yum install httpd php
```

Запустим Apache HTTP server (httpd) и добавим его в автозагрузку

```
/etc/init.d/httpd start  
## или ##  
service httpd start  
chkconfig --levels 235 httpd on
```

*Если вы обновляете Apache или устанавливаете новые модули к php не забывайте его перезагрузить (service httpd restart)*

Создадим тестовый файл для проверки работоспособности сервера  
Добавим функцию php — phpinfo() в файл «/var/www/html/test.php».

**Файл:** test.php

```
<?php  
  
phpinfo();
```

Следует заметить, что директория «/var/www/html/» является директорией по умолчанию для файлов веб-сервера. Ее можно сменить в конфигурационном файле Apache «/etc/httpd/conf/httpd.conf». В нем же, впоследствии, можно и настроить виртуальные хосты и указать необходимые модули для Apache.

Еще один важный момент заключается в том, что при использовании прозрачного проксирования, все запросы, которые приходят на 80 порт переадресовываются на порт 3128 (SQUID). Поэтому для того чтобы получить доступ к веб-серверу необходимо в файле httpd.conf изменить параметр listen 80 на любой другой свободный порт. Например, 81.

## Установка MySQL

```
yum install mysql mysql-server
```

Для установки более новой версии mysql можно использовать репозиторий.

```
wget http://rpms.famillecollet.com/enterprise/remi-release-5.rpm  
rpm -ivh remi-release-5.rpm  
vi /etc/yum.repos.d/remi.repo  
Изменить значение:  
enable=0
```

После подключения репозитория

```
yum install --enablerepo=remi mysql mysql-server
```

Если у Вас ранее была установлена mysql, то после обновления необходимо запустить скрипт миграции уже существующих БД.

Запустим mysql и добавим в автозагрузку

```
chkconfig --levels 235 mysqld on
```

И не забудьте, что чтобы поставить новый пароль пользователю root, необходимо выполнить вот такие команды

```
/usr/bin/mysqladmin -u root password 'new-password'
```



```
/usr/bin/mysqladmin -u root -h localhost.localdomain password 'new-password'
```

Основной файл конфигурации /etc/my.cnf

При инсталляции формируются файлы примеров конфигурационных файлов для различных систем /usr/share/mysql/:

my-small.cnf	Пример конфигурационного файла MySQL для небольших систем. Для системы с небольшим объемом памяти (<= 64М), где MySQL используется только время от времени и очень важно, что демон не требует много ресурсов.
my-medium.cnf	Пример конфигурационного файла MySQL для средних систем. Для системы с небольшим объемом памяти ( 64М-128М,), где MySQL играет важную часть, и используется совместно с другими программами (таких, как веб-сервер).
my-large.cnf	Пример конфигурационного файла MySQL для больших систем. Для большой системы с памятью = 512, где система MySQL является главной.
my-huge.cnf	Пример конфигурационного файла MySQL для очень больших систем. Для большой системы с памятью 1G-2G, где система MySQL является главной.

Определяем какая у нас система и копируем нужный конфигурационный файл, после чего перезагружаем сервер БД.

```
cp /usr/local/share/mysql/my-*****.cnf /etc/my.cnf  
service mysqld restart
```

Переходим к созданию необходимой базы данных и пользователя:

```
$ mysql -u root -p  
mysql> CREATE DATABASE ИмяБазы;  
mysql> USE ИмяБазы;  
mysql> GRANT ALL PRIVILEGES ON *.* TO Юзер@localhost IDENTIFIED BY 'ПАРОЛЬ' WITH GRANT OPTION;  
mysql> FLUSH PRIVILEGES;
```

## Проверка доступности, дополнительные конфигурации

Проверим доступность нашего сервера

Откроем браузер и попробуем перейти по адресу <http://<адрес сервера>/test.php>, если информация о php появилась, то все работает как надо. Если страница не открылась, то:

1. Проверьте, верно ли вы выполнили все шаги
2. Открыть доступ в iptables для 80 порта (если iptables установлен)

Настройка iptables

Далее откройте следующий файл «/etc/sysconfig/iptables»

**Файл:** /etc/sysconfig/iptables

```
# добавьте следующую строчку до слова COMMIT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
```

И перезагрузите iptables

```
service iptables restart
## Или ##
/etc/init.d/iptables restart
```

Для графического управления сервером базы данных mysql, установим phpMyadmin

Установка репозитория для системы CentOS 5 i386:

```
rpm -Uvh http://download.fedora.redhat.com/pub/epel/5/i386/epel-release-5-4.noarch.rpm
```

Отключаем репозиторий в конфигурационном файле. В файле /etc/yum.repos.d/epel.repo устанавливаем:

```
enable=0
```

Устанавливаем программу.

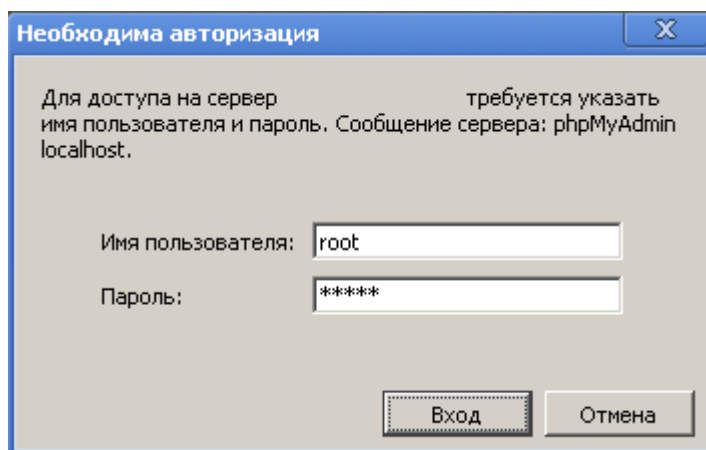
```
yum --enablerepo=epel install phpmyadmin
```

**Файл:** /etc/httpd/conf.d/phpMyAdmin.conf

```
#Добавляем IP адрес для разрешения подключения с удаленной машины.
Allow from 127.0.0.1, IP
#Перезапускаем Web сервер
service httpd restart
```

Откроем браузер и попробуем перейти по адресу <http://<адрес сервера>/phpmyadmin>

В появившемся окне вводим имя пользователя Базы данных MySQL и пароль.



Далее открывается страница управления Базами данных mysql нашего сервера.

#### 4. Установка OpenVPN

Для установки OpenVPN в CentOS 5 необходимо добавить в систему сторонний репозиторий. Подробный процесс добавления репозитория рассмотрен по ссылке <http://fedoraproject.org/wiki/EPEL>. Нам необходимо скачать RPM пакет и установить его в системе, делается это командами:

```
wget http://download.fedoraproject.org/pub/epel/5/i386/epel-release-5-4.noarch.rpm
yum --nogpgcheck install epel-release-5-4.noarch.rpm -y
```

Теперь необходимо отключить автоматическую установку пакетов и обновлений из этого репозитория, делается это для того, что бы при обновлении системы не устанавливались пакеты (ядро в том числе) из сторонних репозиториев. Для этого переходим в каталог `/etc/yum.repos.d` и правим файл `epel.repo`. Заменяем в нем строку `enabled=1` на `enabled=0`.

Можно приступать к установке OpenVPN. Для этого выполним команду:

```
yum --enablerepo=epel install openvpn -y
```

После установки переходим в каталог `/usr/share/doc/openvpn-2.2.0` (путь можем измениться в зависимости от версии пакета) и копируем каталог `easy-rsa` в `/etc/openvpn` командой:

```
cp -r easy-rsa /etc/openvpn
```

Далее, переходим в скопированный только что каталог по адресу `/etc/openvpn/easy-rsa/2.0`, в этом каталоге выполняем следующие команды:

```
chmod +x clean-all
chmod +x build*
chmod +x whichopensslcnf
chmod +x pkitool
```

После, отредактируем /etc/openvpn/easy-rsa/2.0/vars. В этом файле необходимо заменить параметры, с которыми будут генерироваться сертификаты, на свои:

```
export KEY_COUNTRY="RU"  
export KEY_PROVINCE="MSK"  
export KEY_CITY="MOSCOW"  
export KEY_ORG="OpenVPN-TEST-INSTALLATION"  
export KEY_EMAIL="admin@example.com"
```

Теперь, создадим ключи:

```
source ./vars  
./clean-all  
./build-ca  
./build-key-server vpnserver  
./build-dh
```

Скопируем полученные ключи в каталог /etc/openvpn/keys:

```
cp keys/ca.crt /etc/openvpn/keys/ca.crt  
cp keys/vpnserver.crt /etc/openvpn/keys/vpnserver.crt  
cp keys/vpnserver.key /etc/openvpn/keys/vpnserver.key  
cp keys/dh1024.pem /etc/openvpn/keys/dh1024.pem
```

Отредактируем конфигурационный файл /etc/openvpn/openvpn.conf:

**Файл:** /etc/openvpn/openvpn.conf

```
# Порт для подключений  
port 1194  
proto tcp  
# Устройство  
dev tun  
# Расположение сертификатов и ключей  
ca /etc/openvpn/keys/ca.crt  
cert /etc/openvpn/keys/vpnserver.crt  
key /etc/openvpn/keys/vpnserver.key  
dh /etc/openvpn/keys/dh1024.pem  
# Параметры для виртуального туннеля сервера VPN  
server 10.10.10.0 255.255.255.0  
ifconfig-pool-persist ipp.txt  
# Прописываем маршруты  
push "route 10.10.10.0 255.255.255.0"  
# Разрешаем клиентам обмениваться пакетами  
client-to-client
```



```
# Проверяем соединение каждые 10 секунд, если его нет то через 120 секунд переподключаем
keepalive 10 120
# Используем компрессию
comp-lzo
# Назначаем пользователя и группу для работы с OpenVPN
user nobody
group nobody
# Не перечитывать ключи после получения SIGUSR1 или ping-restart
persist-key
# Не закрывать или переоткрывать TUN\TAP устройство, после получения SIGUSR1 или ping-restart
persist-tun
# Записывать статус сервера OpenVPN
status openvpn-status.log
# Логи
log /var/log/openvpn.log
# Уровень отладки
verb 3
mute 10
```

Проверяем, включена ли маршрутизация:

```
grep net.ipv4.ip_forward /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

Если net.ipv4.ip\_forward = 0, то меняем на 1 в файле /etc/sysctl.conf, если же строки вообще нет, ее нужно добавить.

Основная настройка сервера закончена.

Сгенерируем клиентские ключи:

```
cd /etc/openvpn/easy-rsa/2.0
./build-key client01 (в секции Common Name указать client01)
```

Теперь клиенту следует отдать файлы ca.crt, client01.crt, client01.key (все находятся в /etc/openvpn/easy-rsa/2.0/keys) и конфигурационный файл server.ovpn с таким содержанием:

```
client
dev tun
proto tcp
remote <ip адрес vpn сервера> 1194
resolv-retry infinite
nobind
persist-key
persist-tun
```

```
ca ca.crt  
cert client01.crt  
key client01.key  
comp-lzo  
verb 3
```

Сертификаты необходимо скопировать в ту же папку, что и конфигурационный файл (C:\Program Files\OpenVPN\config).

Такую процедуру необходимо проделывать для каждого нового клиента.

Клиент для Windows можно загрузить на сайте: <http://openvpn.se/download.html>

## 5. Введение Linux-сервера в домен Windows

### Задача

Зачастую возникает необходимость ввести Linux-машину в существующий домен Windows. Например, чтобы сделать файловый сервер с помощью Samba. Сделать это очень просто, для этого вам понадобятся клиент Kerberos, Samba и Winbind.

Установить всё можно командой:

```
yum install samba3x samba3x-common samba3x-client samba3x-winbind krb5-workstation
```

Далее вам потребуется настроить все вышеперечисленные инструменты для работы с вашим доменом. Допустим, вы хотите войти в домен INTRA.LOCAL, доменконтроллером которого является сервер dc01.intra.local с IP адресом 10.180.1.45. Этот же сервер является и первичным DNS сервером домена. Вводить в домен будем сервер meilserver.intra.local.

### Настройка DNS

Для начала необходимо изменить настройки DNS на вашей машине, прописав в качестве DNS сервера доменконтроллер2) и в качестве домена поиска - нужный домен.

Если у вас статический IP-адрес, то необходимо изменить содержимое файла/etc/resolv.conf на примерно такое:

```
domain intra.local  
search intra.local  
nameserver 10.180.11.45
```

Для применения изменений остается перезапустить службу:

```
service network restart
```

Кроме того необходимо отредактировать файл /etc/hosts так, чтобы в нём была запись с полным доменным именем компьютера и обязательно коротким именем хоста, ссылающаяся на один из внутренних IP:

```
# Имена этого компьютера
127.0.0.1      mailserver.intra.local mailserver localhost.localdomain localhost
10.180.11.212 mailserver.intra.local mailserver
10.180.11.45   dc01.intra.local      dc01
```

Не обязательно, но если вы что-то поменяете - перезагрузите компьютер для применения изменений.

## Настройка синхронизации времени

---

Далее необходимо настроить синхронизацию времени с доменконтроллером. Если разница будет более 5 минут мы не сможем получить лист от Kerberos.

Если в сети существует сервер точного времени, то можно воспользоваться им или любым публичным:

```
ntpdate ua.pool.ntp.org
```

Автоматическая же синхронизация настраивается с помощью ntpd, это демон будет периодически выполнять синхронизацию. Для начала его необходимо установить:

```
yum install ntp
```

Теперь исправьте файл /etc/ntp.conf, добавив в него информацию о вашем сервере времени:

```
server dc01.intra.local
```

После чего перезапустите демон ntpd:

```
sudo /etc/init.d/ntp restart
```

## Настройка и ввод в домен

---

Теперь пора настраивать непосредственно взаимодействие с доменом.

Запускаем нижеследующую команду одной строкой либо с обратными слешами:

```
authconfig --update --kickstart \  
--enablewinbind \  
--enablewinbindauth \  
--smbsecurity=ads \  
--smbworkgroup=INTRA \  
--smbrealm=INTRA.LOCAL \  
--smbservers=DC01.INTRA.LOCAL \  
--smbidmapuid=10000-20000 \  

```

```
--smbidmapgid=10000-20000 \  
--winbindtemplatehomedir=/home/%U \  
--enablemkhomedir \  
--winbindtemplateshell=/bin/bash \  
--enablewinbindusedefaultdomain \  
--enablelocauthorize \  
--enablekrb5 \  
--krb5realm INTRA.LOCAL \  
--krb5kdc DC01.INTRA.LOCAL \  
--krb5adminserver DC01.INTRA.LOCAL
```

Эта команда вносит все необходимые изменения в конфигурационные файлы системы:

- \* настраивает клиент Kerberos /etc/krb5.conf
- \* добавляет службу winbind в /etc/nsswitch.conf для passwd, shadow и group
- \* изменяет должным образом /etc/samba/smb.conf на работу в домене
- \* стартует службу winbind позволяет которая обмениваться информацией с NT системами

```
[root@mailserver ~]# kinit admin  
Password for admin@INTRA.LOCAL:
```

Если всё прошло без ошибок, то закешированный Kerberos-тикет можно просмотреть командой

```
[root@mailserver ~]# klist  
Ticket cache: FILE:/tmp/krb5cc_0  
Default principal: admin@INTRA.LOCAL  
Valid starting Expires Service principal  
01/30/12 10:47:48 01/30/12 20:47:53 krbtgt/INTRA.LOCAL@INTRA.LOCAL  
renew until 01/31/12 10:47:48  
Kerberos 4 ticket cache: /tmp/tkt0  
klist: You have no tickets cached
```

Вот теперь настал момент добавления нашего сервера в домен:

```
[root@mailserver ~]# net ads join -U admin
```

Должно появиться поле ввода пароля для администратора домена admin  
После ввода которого и при корректной настройке система сообщит об успешном завершении операции

```
[root@mailserver ~]# net ads join -U admin
```



Enter admin's password:

Using short domain name -- INTRA

Joined 'MAILSERVER' to realm 'intra.local'

# и стартуем winbind

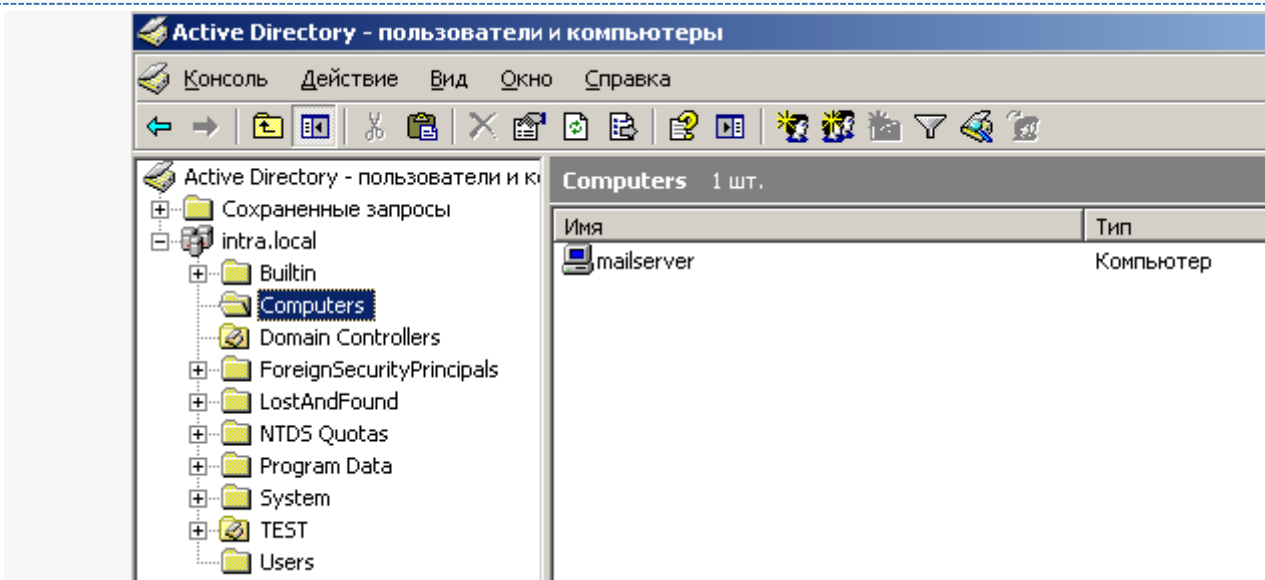
```
[root@mailserver ~]# service winbind restart
```

Если что-то не получается, для начала надо проверять подключение к DNS и логи winbind.

На этом настройка завершена. В Active Directory появилась учетная запись mailserver в "Computers", можно подключаться по SSH, используя учетные записи пользователей домена.

login as: test

test@10.180.11.212's password:



## 6. Установка webadmin

На сайте выбрать необходимую версию пакета <http://www.webmin.com/download.html>

Установить необходимые пакеты:

```
yum install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions
```

Скачать пакет

```
wget http://prdownloads.sourceforge.net/webadmin/webmin-1.580.tar.g
```

Распаковать и установить

```
tar xzvf webmin-1.580.tar.gz
```

```
cd webmin-1.580  
./setup.sh
```

Ответить на заданные вопросы. В конце установки получите строку для доступа к сервису через браузер.

## 7. Установка FTP сервера VSFTPD

Устанавливаем сервер VSFTPD командой:

```
yum install vsftpd
```

Правим конфигурационный файл `/etc/vsftpd/vsftpd.conf`. Добавляем в него следующие строки (если они уже есть правим их значение на указанное ниже):

```
tcp_wrappers=YES  
chroot_local_user=YES  
force_dot_files=YES  
background=YES  
anonymous_enable=NO  
pasv_enable=YES  
pasv_min_port=1500  
pasv_max_port=1550
```

Этими параметрами мы запрещаем пользователям выходить за рамки своего домашнего каталога; отключаем анонимный вход на сервер; разрешаем использование пассивного режима и указываем диапазон портов, которые сервер может использовать.

Добавляем службу в автозагрузку:

```
chkconfig vsftpd on
```

Запускаем:

```
service vsftpd start
```

Для подключения к серверу используются внутренние учетные записи, которые созданы на сервере. Т.е. для добавления нового FTP аккаунта нужно создать нового пользователя в ОС и задать ему домашнюю директорию, в которую он будет попадать, подключаясь к FTP.

## 8. Установка roundcube

Установим последнюю доступную версию roundcube <http://roundcube.net/download>. Для её установки на потребуется php-5.2.1 и выше. Для этого подключим репозиторий и обновим php.

```
wget http://rpms.famillecollet.com/enterprise/remi-release-5.rpm
rpm -ivh remi-release-5.rpm
vi /etc/yum.repos.d/remi.repo
Изменить значение:
enable=0
```

Установим php и дополнительные модули

```
yum install gcc
yum --enablerepo=remi install php php-pear php-devel
pear channel-update pear.php.net
pear install MDB2
pear install Mail_MIME
pear install Net_SMTP
pear install Auth_SASL
```

Загрузим пакет roundcube

```
wget wget http://sourceforge.net/projects/roundcubemail/files/roundcubemail/0.7.2/roundcubemail-0.7.2.tar.gz/download

tar zxvf roundcubemail-0.7.2.tar.gz
mv roundcubemail-0.7.2 /var/www/rcmail/
cd /var/www/rcmail/
chown -R apache:apache .
chmod 777 temp logs
```

Настроим apache, для этого создадим файл

**/etc/httpd/conf.d/roundcubemail.conf:**

```
# for roundcube mail
Alias /rcmail/ /var/www/rcmail/
<Location /rcmail>
    Order Deny,Allow
    Deny from None
    Allow from All
</Location>
```

Создадим БД

```
service mysqld restart
mysql>
```



```
#Создаем БД с именем rcmail
create database rcmail CHARACTER SET utf8 COLLATE utf8_general_ci;
grant all privileges on rcmail.* to 'rcmail'@'localhost' identified by 'rcmail';
#где
#grant all privileges on имя_ БД.* to 'имя пользователя'@'localhost' identified by 'пароль';
```

Перезапустим apache и зайдем через браузер

```
service httpd restart
http://hostname/rcmail/installer/index.php
```

После start installation проверяется наличие необходимых пакетов. При проверке не должно быть **“NOT OK”**, чтобы исправить данную ситуацию, необходимо доставить недостающие пакеты и перезапустить установку. Недостающие модули php устанавливаются, так же как и php. Для поиска пакета можно использовать команду search

```
yum search --enablerepo=remi название недостающего расширения (например dom)
```

## Roundcube Webmail Installer

1. Check environment    2. Create config    3. Test config

### Checking PHP version

Version: **OK** (PHP 5.3.10 detected)

### Checking PHP extensions

The following modules/extensions are *required* to run Roundcube:

PCRE: **OK**  
DOM: **OK**  
Session: **OK**  
XML: **OK**  
JSON: **OK**

The next couple of extensions are *optional* and recommended to get the best performance:

FileInfo: **OK**  
Libiconv: **OK**  
Multibyte: **OK**  
OpenSSL: **OK**  
Mcrypt: **OK**  
Intl: **OK**

### Checking available databases

Check which of the supported extensions are installed. At least one of them is required.

MySQL: **OK**  
MySQLi: **OK**  
PostgreSQL: **NOT AVAILABLE** (Not installed)  
SQLite (v2): **NOT AVAILABLE** (Not installed)

### Check for required 3rd party libs

This also checks if the include path is set correctly.

PEAR: **OK**  
MDB2: **OK**  
Net\_SMTP: **OK**  
Net\_IDNA2: **OK**  
Mail\_mime: **OK**

### Checking php.ini/.htaccess settings

The following settings are *required* to run Roundcube:

file\_uploads: **OK**  
session.auto\_start: **OK**  
zend.ze1\_compatibility\_mode: **OK**  
mbstring.func\_overload: **OK**  
suhosin.session.encrypt: **OK**

The following settings are *optional* and recommended:

date.timezone: **NOT OK** (Could be set)

На следующей вкладке необходимо внести корректные данные в разделы:

### IMAP Settings

default\_host

The IMAP host(s) chosen to perform the log-in

 add

Leave blank to show a textbox at login. To use SSL/IMAPS connection, type ssl://hostname

### SMTP Settings

smtp\_server

Use this host for sending mails

To use SSL connection, set ssl://smtp.host.com. If left blank, the PHP mail() function is used

### Database setup

db\_dsnw

Database settings for read/write operations:

Database type

Database server (omit for sqlite)

Database name (use absolute path and filename for sqlite)

Database user name (needs write permissions)(omit for sqlite)

Database password (omit for sqlite)

После этого будет сформировано 2 конфигурационных файла, которые должны быть скопированы в /var/www/rcmail/config/

## Roundcube Webmail Installer

1. Check environment    2. **Create config**    3. Test config

Copy or download the following configurations and save them in two files (names above the text box) within the `/var/www/rmail/config` directory of your Roundcube installation. Make sure that there are no characters outside the `<?php ?>` brackets when saving the files.

`main.inc.php` [\(download\)](#)

```
<?php
/*
+-----+
| Main configuration file                               |
| |                                                    |
| This file is part of the Roundcube Webmail client   |
| Copyright (C) 2005-2011, The Roundcube Dev Team    |
| Licensed under the GNU GPL                         |
+-----+
*/

$rmail_config = array();

// -----
// LOGGING/DEBUGGING
// -----

// system error reporting: 1 = log; 2 = report (not implemented yet), 4 = show, 8 = trace
$rmail_config['debug_level'] = 1;
```

`db.inc.php` [\(download\)](#)

```
<?php
/*
+-----+
| Configuration file for database access              |
| |                                                    |
| This file is part of the Roundcube Webmail client   |
| Copyright (C) 2005-2009, The Roundcube Dev Team    |
| Licensed under the GNU GPL                         |
+-----+
*/
```

На последнем шаге необходимо проинициализировать БД, и проверить настройки пользователя и отправку сообщений.



## Roundcube Webmail Installer

1. Check environment
2. Create config
3. Test config

### Check config files

main.inc.php: **OK**

db.inc.php: **OK**

### Check if directories are writable

Roundcube may need to write/save files into these directories

temp/: **OK**

logs/: **OK**

### Check DB config

DSN (write): **OK**

DB Schema: **NOT OK** (Database not initialized)

### Test SMTP config

Server: 10.180.11.212

Port: 25

User: (none)

Password: (none)

Sender

Recipient

### Test IMAP config

Server

Port 143

Username

Password