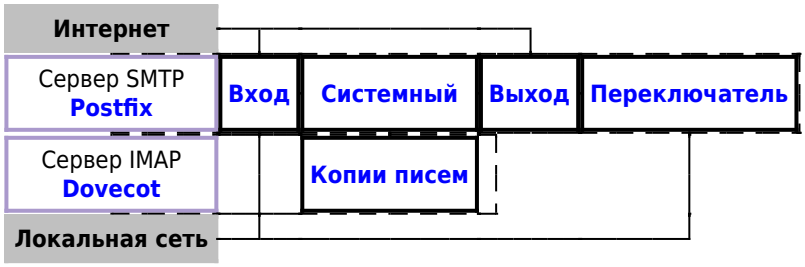
Пример почтового сервера с несколькими внутренними доменами



Postfix

Основная статья о Postfix

В данном примере использована работа с несколькими экземплярами Postfix, далее приведены команды, которые нужно выполнить для работы в этом режиме:

```
postmulti -e init

postmulti -I postfix-i -G in -e create
postmulti -i postfix-i -e enable

postmulti -I postfix-o -G out -e create
postmulti -i postfix-o -e enable

postmulti -I postfix-s -G switch -e create
postmulti -i postfix-s -e enable
```

Нужно создать символические ссылки на `/etc/postfix/dynamicmaps.cf`:

```
ln -s /etc/postfix/dynamicmaps.cf /etc/postfix-i
ln -s /etc/postfix/dynamicmaps.cf /etc/postfix-o
ln -s /etc/postfix/dynamicmaps.cf /etc/postfix-s
```

virtual_alias_maps

Fix Me!

/etc/postfix/main.cf

```
virtual_alias_maps  =  hash:/etc/postfix-i/virtual  ldap:/etc/postfix/ldap-users-1.cf
ldap:/etc/postfix/ldap-groups-1.cf         ldap:/etc/postfix/ldap-users-2.cf
ldap:/etc/postfix/ldap-groups-2.cf
```

/etc/postfix/ldap-users-1.cf

```
server_host = localhost
bind = yes
version = 3
# query_filter = (&(!(l=disabled)) (|(mail=%s)(maildrop=%s))(objectclass=mailUser))
search_base = ou=users,dc=sub1,dc=domain
query_filter = (&(|(mail=%s)(maildrop=%s))(objectclass=mailUser))
result_attribute = maildrop
```

/etc/postfix/ldap-groups-1.cf

```
server_host = localhost
search_base = ou=groups,dc=sub1,dc=domain
query_filter = (&(|(mail=%s)(mailRoutingAddress=%s))(objectclass=mailGroup))
special_result_attribute = member
result_attribute = maildrop
```

/etc/postfix/ldap-users-2.cf

```
server_host = localhost
bind = yes
version = 3
search_base = ou=users,dc=sub2,dc=domain
# query_filter = (&(!(l=disabled)) (|(mail=%s)(maildrop=%s))(objectclass=mailUser))
query_filter = (&(|(mail=%s)(maildrop=%s))(objectclass=mailUser))
result_attribute = maildrop
```

/etc/postfix/ldap-groups-2.cf

```
server_host = localhost
search_base = ou=groups,dc=sub1,dc=domain
query_filter = (&(|(mail=%s)(mailRoutingAddress=%s))(objectclass=mailGroup))
special_result_attribute = member
result_attribute = maildrop
```

Системный сервер

Папка: `/etc/postfix`

Сервер решает задачи доставки почты локальных (системный) пользователей, и копий писем всех пользователей с помощью Dovecot.

main.cf

/etc/postfix/main.cf

```
smtpd_banner = $myhostname ESMTP $mail_name
biff = no
append_dot_mydomain = no
readme_directory = no
myorigin = localhost
myhostname = localhost.localdomain
mydestination = localhost
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
relayhost =
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = 127.0.0.1
default_transport = error
relay_transport = error
multi_instance_enable = yes
multi_instance_wrapper = ${command_directory}/postmulti -p --
multi_instance_directories = /etc/postfix-i /etc/postfix-o /etc/postfix-s
```

```
virtual_mailbox_domains = localhost.localdomain
virtual_transport = lmtp:unix:private/dovecot-lmtp
```

transport

Описание транспортов.

Этот файл используются во всех экземплярах сервера

/etc/postfix/transport

```
localhost.localdomain :127.0.0.1
.localhost.localdomain :127.0.0.1
sub1.domain.ru smtp:smtp.sub1.domain.ru
sub2.domain.ru smtp:smtp.sub2.domain.ru
```

Компиляция:

```
postmap /etc/postfix/transport
```

Входной сервер

Для проверки почты используется AMaViSd-new, настройка файла `master.cf` описана в разделе AMaViSd-new

Более подробно параметры безопасности описаны в главе Безопасность

Папка: `/etc/postfix/postfix-i`

main.cf

/etc/postfix/postfix-i/main.cf

```
unknown_local_recipient_reject_code = 550
readme_directory = no
inet_protocols = ipv4
recipient_delimiter = +

multi_instance_enable = yes
multi_instance_group = in
multi_instance_name = postfix-i
data_directory=/var/lib/postfix-i
queue_directory = /var/spool/postfix-i
mynetworks = 127.0.0.0/8
myhostname = ИМЯ_ХОСТА
smtpd_proxy_ehlo = ИМЯ_СЕРВЕРА
smtpd_banner = $myhostname ESMTP
inet_interfaces = ВНЕШНИЙ_АДРЕС ВНУТРЕННИЙ_АДРЕС
mydestination = ПОЧТОВЫЙ_ДОМЕН_1 ПОЧТОВЫЙ_ДОМЕН_2
content_filter=smtp-amavis:[127.0.0.1]:10024
virtual_alias_maps = hash:/etc/postfix-i/virtual
relayhost =
disable_vrfy_command = yes
show_user_unknown_table_name = no
smtpd_helo_required = yes
smtpd_helo_restrictions=
    permit_mynetworks,
```

```
    permit_sasl_authenticated,
    reject_invalid_hostname,
    reject_non_fqdn_hostname,
    reject_invalid_helo_hostname,
    reject_unknown_helo_hostname
smtpd_sender_restrictions=
    reject_non_fqdn_sender,
    reject_unknown_sender_domain,
    reject_unlisted_sender,
    permit_mynetworks,
    permit_sasl_authenticated
smtpd_recipient_restrictions=
    reject_non_fqdn_recipient,
    reject_unknown_recipient_domain,
    reject_unlisted_recipient,
    permit_mynetworks,
    permit_sasl_authenticated,
    reject_unauth_destination
    reject_invalid_hostname
smtpd_data_restrictions=
    reject_unauth_pipelining,
    reject_multi_recipient_bounce
smtpd_etrn_restrictions=
    permit_mynetworks,
    permit_sasl_authenticated,
    reject

message_size_limit = 30720000

virtual_alias_maps  =  hash:/etc/postfix-i/virtual  ldap:/etc/postfix/ldap-users-1.cf
ldap:/etc/postfix/ldap-groups-1.cf         ldap:/etc/postfix/ldap-users-2.cf
ldap:/etc/postfix/ldap-groups-2.cf

always_bcc = bcc@localhost.localdomain
receive_override_options = no_address_mappings
transport_maps = hash:/etc/postfix/transport
```

Имя заданное в `smtpd_proxy_ehlo` должно разрешаться внешними DNS серверами

В строке `inet_interfaces = ВНЕШНИЙ_АДРЕС ВНУТРЕННИЙ_АДРЕС` нужно указать специальный `ВНУТРЕННИЙ_АДРЕС` с которого входящая почта будет отправятся в локальную сеть. Например можно использовать адрес `127.0.0.2`, вот пример его описания для `/etc/network/interfaces`:

```
auto lo:0
        iface lo:0 inet static
        address 127.0.0.2
```

Добавление псевдонима «на ходу»:

```
ifconfig lo:0 127.0.0.2 up
```

В переменой `virtual_alias_maps` определен список источников для разрешение почтовых адресов (т.е. для получения соответствия адреса пользователя во внешних доменах с адресом во внутренних)

В качестве LDAP сервера специально указан `localhost`, т.к. хорошо иметь на одном компьютере с почтовым сервером и LDAP сервер, на котором находятся реплики внутренних серверов. Сделано это для того, чтобы при временном отсутствии связи разрешение почтовых адресов происходило правильно.
Пример настройки: Подчиненный сервер для нескольких доменов

virtual

Список соответствия пользователей

Поскольку существует два внутренних домена, почта внешнего пользователя должна доставляться пользователю в нужный внутренний домен.

/etc/postfix/postfix-i/virtual

```
test: test@domain.ru
test1: test1@sub1.domain.ru
test2: test2@sub2.domain.ru
```

Компиляция:

```
postalias /etc/postfix-i/virtual
```

Выходной сервер

Маскарад домена

Папка: `/etc/postfix/postfix-o`

main.cf

/etc/postfix/postfix-o/main.cf

```
unknown_local_recipient_reject_code = 550
smtpd_banner = $myhostname ESMTP
readme_directory = no
inet_protocols = ipv4
recipient_delimiter = +
multi_instance_enable = yes
multi_instance_group = out
multi_instance_name = postfix-o
queue_directory = /var/spool/postfix-o
data_directory = /var/lib/postfix-o
relayhost =
mydestination = ПОЧТОВЫЙ_ДОМЕН_1 ПОЧТОВЫЙ_ДОМЕН_2
myhostname = ИМЯ_СЕРВЕРА
mynetworks = ВНУТРЕННЯЯ_СЕТЬ_1, ВНУТРЕННЯЯ_СЕТЬ_2
inet_interfaces = ВНУТРЕННИЙ_АДРЕС
smtp_bind_address = ВНЕШНИЙ_АДРЕС
smtp_helo_name = $myhostname
smtp_generic_maps = hash:/etc/postfix-o/generic
receive_override_options = no_address_mappings
always_bcc = bcc@localhost.localdomain
transport_maps = hash:/etc/postfix/transport
receive_override_options =
delay_warning_time = 4h
```

master.cf

Меняем стандартный порт `smtp` на 587

/etc/postfix/postfix-o/master.cf

```
587       inet  n       -       -       -       -       smtpd
```

generic

Маскарад адресов

/etc/postfix/postfix-o/generic

```
@sub2.domain.ru @domain.ru
@sub2.domain.ru @domain.ru
```

Компиляция:

```
postmap /etc/postfix-o/generic
```

Переключающий сервер

Принимает почту от из внутренней сети и перенаправляет ее на другие внутренние серверы или отравляет на внешние серверы через Выходной сервер, фактически это режим Smart host

Папка: /etc/postfix/postfix-s

main.cf

/etc/postfix/postfix-s/main.cf

```
unknown_local_recipient_reject_code = 550
smtpd_banner = $myhostname ESMTP (s)
readme_directory = no
inet_protocols = ipv4
recipient_delimiter = +
multi_instance_enable = yes
multi_instance_group = switch
multi_instance_name = postfix-s
queue_directory = /var/spool/postfix-s
data_directory = /var/lib/postfix-s
relayhost = ВНУТРЕННИЙ_АДРЕС:587
mydestination = ПОЧТОВЫЙ_ДОМЕН_1 ПОЧТОВЫЙ_ДОМЕН_2
myhostname = ИМЯ_СЕРВЕРА
mynetworks = ВНУТРЕННЯЯ_СЕТЬ_1, ВНУТРЕННЯЯ_СЕТЬ_2
inet_interfaces = ВНУТРЕННИЙ_АДРЕС
smtp_helo_name = $myhostname
receive_override_options = no_address_mappings
transport_maps = hash:/etc/postfix/transport
receive_override_options =
```

Dovecot

Fix Me!

Основная статья о Dovecot

Ящик для хранения копий писем

В примере используется адрес: `bcc@localhost.localdomain`

Postfix: Копирование всей почты

dovecot.conf

/etc/dovecot/dovecot.conf

```
!include_try /usr/share/dovecot/protocols.d/*.protocol
!include conf.d/*.conf
!include_try local.conf

protocols = imap pop3 lmtp
```

users

Файл с описанием пользователей

Создание пароля

/etc/dovecot/users

```
bcc:{PLAIN}PASSWORD..:3000:3000::/home/dovecot/BCC::userdb_mail=maildir:~/
```

10-auth.conf

/etc/dovecot/conf.d/10-auth.conf

```
disable_plaintext_auth = no
auth_username_format = %Ln
auth_mechanisms = plain
!include auth-passwdfile.conf.ext
```

10-director.conf

/etc/dovecot/conf.d/10-director.conf

```
service director {
  unix_listener login/director {
  }
  fifo_listener login/proxy-notify {
  }
  unix_listener director-userdb {
  }
  inet_listener {
  }
}
```

```
service imap-login {
}
service pop3-login {
}

protocol lmtp {
}
```

10-master.conf

/etc/dovecot/conf.d/10-master.conf

```
service imap-login {
  service_count = 1
  inet_listener imap {
    port = 143
  }
}

service pop3-login {
  service_count = 1
  inet_listener pop3 {
    port = 110
  }
}

service lmtp {
   unix_listener /var/spool/postfix/private/dovecot-lmtp {
   group = postfix
   mode = 0666
   user = postfix
  }
}

service imap {
  process_limit = 10
}

service pop3 {
  process_limit = 10
}

service auth {
  unix_listener auth-master {
    mode = 0666
  }

 unix_listener auth-userdb {
    mode = 0666
    user = vmail
    group = mail
  }

  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
  }

service auth-worker {
}
```

```
service dict {
  unix_listener dict {
  }
}
```

15-lda.conf

/etc/dovecot/conf.d/15-lda.conf

```
postmaster_address = root@localhost.localdomain
hostname = mail.domain.ru

protocol lda {
}
```

15-mailboxes.conf

/etc/dovecot/conf.d/15-mailboxes.conf

```
namespace inbox {

  mailbox Drafts {
    special_use = \Drafts
    auto = create
  }
  mailbox Junk {
    special_use = \Junk
    auto = create
  }
  mailbox Trash {
    special_use = \Trash
    auto = create
  }

  mailbox Sent {
    special_use = \Sent
    auto = create
  }
  mailbox "Sent Messages" {
    special_use = \Sent
  }
}
```

20-lmtp.conf

/etc/dovecot/conf.d/20-lmtp.conf

```
protocol lmtp {
  mail_plugins = $mail_plugins sieve
}
```

auth-passwdfile.conf.ext

/etc/dovecot/conf.d/auth-passwdfile.conf.ext

```
passdb {
  driver = passwd-file
  args = scheme=CRYPT username_format=%u /etc/dovecot/users
}

userdb {
  driver = passwd-file
  args = username_format=%u /etc/dovecot/users
}
```

Ссылки

Postfix Standard Configuration Examples

Managing multiple Postfix instances on a single host

Системное и сетевое администрирование: postfix - повышаем безопасность

http://sysadminmosaic.ru/examples/email_server_several_subdomain

2019-05-11 00:05