

Лабораторная работа № 10. Расширенные настройки SMTP-сервера

Студент: Яссин оуледсалем

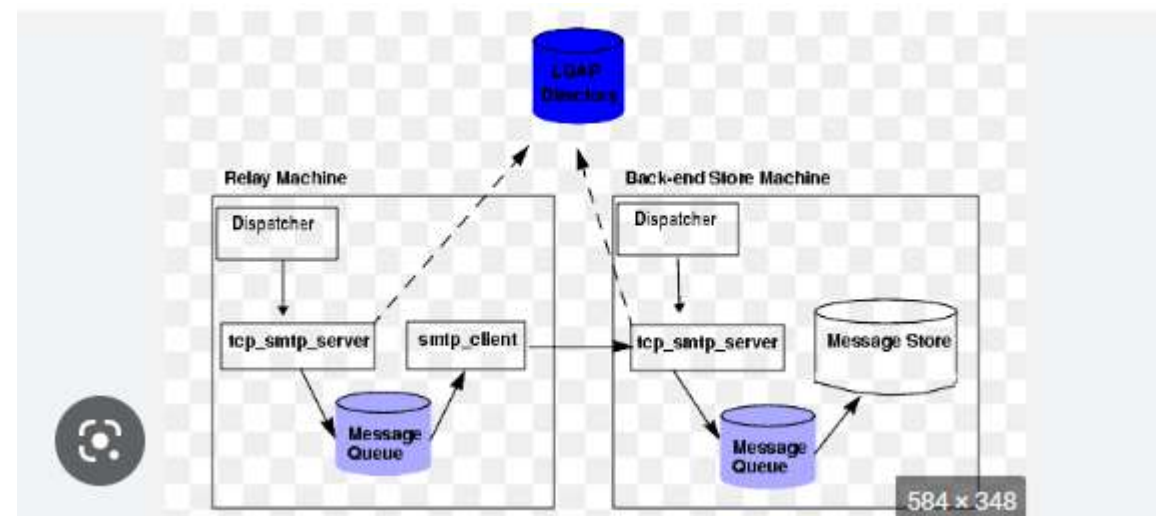
НПИбд-02-20

Цель работы

- Приобретение практических навыков по конфигурированию SMTP-сервера в части настройки аутентификации.

Протокол LMTP

Local Mail Transfer Protocol (LMTP) — протокол локальной пересылки почты. По сути, Dovecot с включённым в него функционалом LMTP выступает в качестве локального агента доставки почты, т.е. является службой приёма почтовых сообщений от SMTP-сервера для последующей их пересылки клиентам локальной сети. Использование Dovecot и протокола LMTP позволяет организовать фильтрацию почты на стороне сервера в момент размещения письма в почтовый ящик, а не на стороне клиента.



Задание

1. Настройте Dovecot для работы с LMTP (см. раздел 10.4.1).
2. Настройте аутентификацию посредством SASL на SMTP-сервере (см. раздел 10.4.2).
3. Настройте работу SMTP-сервера поверх TLS (см. раздел 10.4.3).
4. Скорректируйте скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины server (см. раздел 10.4.4).

Настройка LMTP в Dovecot

```
root@server:~ * root@server:~ * root@server:~ * yassine@serv... *
# Password database is used to verify user's password (and nothing more).
# You can have multiple passwdbs and userdbs. This is useful if you want to
# allow both system users (/etc/passwd) and virtual users to login without
# duplicating the system users into virtual database.
#
# <doc/wiki/PasswordDatabase.txt>
#
# User database specifies where mails are located and what user/group IDs
# own them. For single-UID configuration use "static" userdb.
#
# <doc/wiki/UserDatabase.txt>
#
#!include auth-deny.conf.ext
#!include auth-master.conf.ext

!include auth-system.conf.ext
#!include auth-sql.conf.ext
#!include auth-ldap.conf.ext
#!include auth-passwdfile.conf.ext
#!include auth-checkpassword.conf.ext
#!include auth-static.conf.ext
auth_username_format = %Ln
```

```
[root@server.yassine.net ~]# postconf -e 'mailbox_transport = lmtp:unixprivate/dovecot-lmtp'
[root@server.yassine.net ~]#
```

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

    # Create inet listener only if you can't use the above UNIX socket
    #inet_listener lmtp {
        # Avoid making LMTP visible for the entire internet
        #address =
        #port =
    #}
```

2. Настройка SMTP-аутентификации

```
root@server:~  
root@server:~  
yassine@server:~  
service auth {  
    unix_listener /var/spool/postfix/private/auth {  
        mode = 0666  
        user = postfix  
        group = postfix  
    }  
  
    unix_listener auth-userdb {  
mode = 0600  
user= dovecot  
}  
}  
  
service auth-worker {  
    # Auth worker process is run as root by default, so that it can access  
    # /etc/shadow. If this isn't necessary, the user should be changed to  
    # $default_internal_user.  
    #user = root  
}  
  
service dict {  
-- INSERT --  
100,3 91%
```

```
root@server:~  
root@server:~  
yassine@server:~  
#  
# Postfix master process configuration file. For details on the format  
# of the file, see the master(5) manual page (command: "man 5 master" or  
# on-line: http://www.postfix.org/master.5.html).  
#  
# Do not forget to execute "postfix reload" after editing this file.  
#  
# =====  
# service type private unpriv chroot wakeup maxproc command + args  
# (yes) (yes) (no) (never) (100)  
# =====  
smtp inet n - n - - smtpd  
-o smtpd_sasl_auth_enable=yes  
-o smtpd_recipient_restrictions=reject_non_fqdn_recipient, reject_unknown_recipient_domain, permit_sasl_authenticated, reject  
#smtp inet n - n - 1 postscreen  
#smtpd pass - - n - - smtpd  
#dnsblog unix - - n - 0 dnsblog  
#tlsproxy unix - - n - 0 tlsproxy  
#submission inet n - n - - smtpd  
# -o syslog_name=postfix/submission  
# -o smtpd_tls_security_level=encrypt  
#-o smtpd_sasl_auth_enable=yes  
-- INSERT --  
14 124 Top
```

```
[root@server.yassine.net ~]# cat /etc/dovecot/conf/10-master.conf  
[root@server.yassine.net ~]# postconf -e 'smtpd_sasl_type = dovecot'  
[root@server.yassine.net ~]# postconf -e 'smtpd_sasl_path = private/auth'  
[root@server.yassine.net ~]#  
[root@server.yassine.net ~]# postconf -e 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, permit_mynetworks, reject_non_fqdn_recipient, reject_unauth_destination, reject_unverified_recipient, permit'  
[root@server.yassine.net ~]#
```

```
[root@client.yassine.net client]# printf 'yassine\x00yassine\x00123456' base64
yassineyassine123456[root@client.yassine.net client]# telnet server.yassine.net 25
Trying 192.168.1.1...
Connected to server.yassine.net.
Escape character is '^]'.
220 server.yassine.net ESMTP Postfix
EHLO test
250-server.yassine.net
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
AUTH PLAIN <CNHJRF DLYA AUTHENTICATION >
```

Account Editor

Identity

Receiving Email

Receiving Options

Sending Email

Defaults

Composing Messages

Security

Server Type: **SMTP**

Description: For delivering mail by connecting to a remote mailhub using SMTP.

Configuration

Server: Port:

☐ Server requires authentication

Security

Encryption method:

Authentication

Type:

Username:

Cancel OK

```
[root@client.yassine.net client]# openssl s_client -starttls smtp -crlf -connect server.yassine.net:587
CONNECTED(00000003)
EH809B8066A37F0000:error:0A00010B:SSL routines:ssl3_get_record:wrong version number:ssl/record/ssl3_record.c:354:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 262 bytes and written 355 bytes
Verification: OK
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
```

```
# =====
smtp inet n - n - - smtpd
submission inet n - n - - smtpd
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
#smtp      inet  n       -       n       -       1       postscreen
#smtpd     pass  -       -       n       -       -       smtpd
#dnsblog   unix  -       -       n       -       0       dnsblog
#tlsproxy  unix  -       -       n       -       0       tlsproxy
#submission inet n       -       n       -       -       smtpd
```

3. Настройка SMTP over TLS


```
root@server:/vagrant/provision/server

firewall-cmd --add-service=imap --permanent
firewall-cmd --add-service=smtp --permanent
firewall-cmd --reload

restprecon -vR /etc
echo "Start postfix service"
systemctl enable postfix
systemctl start postfix
systemctl enable dovecot
systemctl start dovecot
echo "Configure postfix"
postconf -e 'mydomain = yassine.net'
postconf -e 'myorigin = $mydomain'
postconf -e 'inet_protocols = ipv4'
postconf -e 'inet_interfaces = all'
postconf -e 'mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain'
postconf -e 'mynetworks = 127.0.0.0/8, 192.168.0.0/16'
echo "Configure postfix for SMTP over TLS"
cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
postconf -e 'smtpd_tls_session_cache_database =
htree:/var/lib/postfix/smtpd_scache'
postconf -e 'smtpd_tls_security_level = may'
postconf -e 'smtp_tls_security_level = may'
echo "Configure postfix for SMTP over TLS"

postconf -e 'smtpd_tls_cert_file=/etc/pki/tls/certs/dovecot.pem'
postconf -e 'smtpd_tls_key_file=/etc/pki/tls/private/dovecot.pem'
postconf -e 'smtpd_tls_session_cache_database = htree:/var/lib/postfix/smtpd_scache'
postconf -e 'smtpd_tls_security_level = may'
postconf -e 'smtp_tls_security_level = may'
postfix set-permissions
doveadm mailbox list -u yassine
restorecon -vR /etc

systemctl stop postfix
systemctl start postfix
systemctl restart dovecot

-- INSERT --
```

ВЫВОД

- Получил практических навыков по конфигурированию SMTP-сервера в части настройки аутентификации.