

Лабораторная работа № 10

Расширенные настройки SMTP-сервера

Сахно Никита НФИбд-02-23

Содержание

1	Цель работы	1
2	Задание	1
3	Выполнение лабораторной работы.....	1
3.1	Настройка LMTP в Dovecote	1
3.2	Настройка SMTP-аутентификации	3
3.3	Настройка SMTP over TLS.....	5
3.4	Внесение изменений в настройки внутреннего окружения виртуальной машины	6
4	Выводы.....	7
5	Контрольные вопросы.....	7

1 Цель работы

Приобрести практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

2 Задание

1. Настроить Dovecot для работы с LMTP.
2. Настроить аутентификацию посредством SASL на SMTP-сервере.
3. Настроить работу SMTP-сервера поверх TLS.
4. Скорректировать скрипт для Vagrant, фиксирующий действия расширенной настройки SMTP-сервера во внутреннем окружении виртуальной машины server.

3 Выполнение лабораторной работы

3.1 Настройка LMTP в Dovecote

На виртуальной машине server войдем под своим пользователем и откроем терминал. Перейдем в режим суперпользователя: `sudo -i`

В дополнительном терминале запустим мониторинг работы почтовой службы: `tail -f /var/log/maillog`

```
Dec 9 13:18:55 server postfix/master[7816]: terminating on signal 15
Dec 9 13:18:55 server postfix/postfix-script[8378]: starting the Postfix mail system
Dec 9 13:18:55 server postfix/master[8380]: daemon started -- version 3.5.9, configuration /etc/postfix
Dec 9 13:29:26 server dovecot[1389]: imap-login: Disconnected: Connection closed (no auth attempts in 0 secs): user=<>, rip=192.168.1.30, lip=192.168.1.1, TLS, session=<Se+NsBMMAJPAqAEe>
Dec 9 13:29:29 server dovecot[1389]: imap-login: Disconnected: Connection closed (no auth attempts in 0 secs): user=<>, rip=192.168.1.30, lip=192.168.1.1, TLS, session=<TW6sBMN8KfAqAEe>
Dec 9 13:29:43 server dovecot[1389]: imap-login: Login: user=<dmbelicheva>, method=PLAIN, rip=192.168.1.30, lip=192.168.1.1, mpid=8558, TLS, session=<ZZWtsRMM8qrAqAEe>
Dec 9 13:30:57 server dovecot[1389]: imap(dmbelicheva)<8558><ZZWtsRMM8qrAqAEe>: Disconnected: Connection closed (IDLE finished 67.800 secs ago) in=674 out=4791 deleted=0 expunged=0 trashed=0 hdr_count=3 hdr_bytes=1854 body_count=1 body_bytes=689
Dec 9 15:42:49 server postfix/postfix-script[1074]: starting the Postfix mail system
Dec 9 15:42:49 server postfix/master[1078]: daemon started -- version 3.5.9, configuration /etc/postfix
Dec 9 15:42:50 server dovecot[1179]: master: Dovecot v2.3.16 (7e2e908c1a) starting up for imap, pop3 (core dumps disabled)
```

Мониторинг работы почтовой службы

Добавим в список протоколов, с которыми может работать Dovecot, протокол LMTP. Для этого в файле `/etc/dovecot/dovecot.conf` укажем `protocols = imap pop3 lmtp`

```
GNU nano 5.6.1 dovecot.conf
# Default values are shown for each setting, it's not required to uncomment
# those. These are exceptions to this though: No sections (e.g. namespace {})
# or plugin settings are added by default, they're listed only as examples.
# Paths are also just examples with the real defaults being based on configure
# options. The paths listed here are for configure --prefix=/usr
# --sysconfdir=/etc --localstatedir=/var

# Protocols we want to be serving.
#protocols = imap pop3 lmtp submission
protocols = imap pop3 lmtp
```

Редактирование файла

Настроим в Dovecot сервис lmtp для связи с Postfix. Для этого в файле `/etc/dovecot/conf.d/10-master.conf` заменим определение сервиса lmtp на следующую запись:

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

```
GNU nano 5.6.1 10-master.conf
}
}

service submission-login {
  inet_listener submission {
    #port = 587
  }
}

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

  # 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 =
  }
}

service imap {
```

Редактирование файла

Переопределим в Postfix с помощью postconf передачу сообщений не на прямую, а через заданный unix-сокеты: postconf -e 'mailbox_transport = lmtp:unix:private/dovecot-lmtp'

В файле /etc/dovecot/conf.d/10-auth.conf зададим формат имени пользователя для аутентификации в форме логина пользователя без указания домена:
auth_username_format = %Ln

```
root@server:/etc/dovecot/conf.d
GNU nano 5.6.1 10-auth.conf
# the standard variables here, eg. %Lu would lowercase the username, %n would
# drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
# "-AT-". This translation is done after auth_username_translation changes.
auth_username_format = %Ln
```

Редактирование файла

Перезапустим Postfix и Dovecot.

Из-под учётной записи своего пользователя отправим письмо с клиента: echo . | mail -s "LMTP test" nvsakhno@dmbelicheva.net

На сервере посмотрим почтовый ящик пользователя: MAIL=~/.Maildir/ mail

Там оказалось пусто, потому что письмо не было доставлено в связи с какими-то проблемами.

3.2 Настройка SMTP-аутентификации

В файле /etc/dovecot/conf.d/10-master.conf определим службу аутентификации пользователей:

```
GNU nano 5.6.1 10-master.conf
service auth {
  # auth_socket_path points to this userdb socket by default. It's typically
  # used by dovecot-lda, doveadm, possibly imap process, etc. Users that have
  # full permissions to this socket are able to get a list of all usernames and
  # get the results of everyone's userdb lookups.
  #
  # The default 0666 mode allows anyone to connect to the socket, but the
  # userdb lookups will succeed only if the userdb returns an "uid" field that
  # matches the caller process's UID. Also if caller's uid or gid matches the
  # socket's uid or gid the lookup succeeds. Anything else causes a failure.
  #
  # To give the caller full permissions to lookup all users, set the mode to
  # something else than 0666 and Dovecot lets the kernel enforce the
  # permissions (e.g. 0777 allows everyone full permissions).
  unix_listener /var/spool/postfix/private/auth {
    group = postfix
    user = postfix
    mode = 0660
  }
  unix_listener auth-userdb {
    mode = 0666
    user = dovecot
    #group =
  }
}
```

Редактирование файла

Для Postfix зададим тип аутентификации SASL для smtpd и путь к соответствующему unix-сокеты:

```
postconf -e 'smtpd_sasl_type = dovecot'
postconf -e 'smtpd_sasl_path = private/auth'
```

Настроим Postfix для приёма почты из Интернета только для обслуживаемых нашим сервером пользователей или для произвольных пользователей локальной машины

(имеется в виду локальных пользователей сервера), обеспечивая тем самым запрет на использование почтового сервера в качестве SMTP relay для спам-рассылок (порядок указания опций имеет значение):

```
postconf -e 'smtpd_recipient_restrictions =  
reject_unknown_recipient_domain,  
permit_mynetworks, reject_non_fqdn_recipient,  
reject_unauth_destination, reject_unverified_recipient, permit'
```

В настройках Postfix ограничим приём почты только локальным адресом SMTP-сервера сети: `postconf -e 'mynetworks = 127.0.0.0/8'`

```
# 'smtpd_sasl_type = dovecot'  
# 'smtpd_sasl_path = private/auth'  
# 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, pe  
# 'smtpd_recipient_restrictions = reject_unknown_recipient_domain, pe  
# 'mynetworks = 127.0.0.0/8'
```

Команды *postconf*

Для проверки работы аутентификации временно запустим SMTP-сервер (порт 25) с возможностью аутентификации. Для этого необходимо в файле `/etc/postfix/master.cf` изменить строки

```
#####  
smtp      inet  n       -       n       -       1       smtpd  
#smtp     inet  n       -       n       -       1       postscreen  
#smtpd    pass  -       -       n       -       -       smtpd  
#dnsblog  unix  -       -       n       -       0       dnsblog  
#tlspolicy unix  -       -       n       -       0       tlspolicy  
#submission inet  n       -       n       -       -       smtpd  
#  -o syslog_name=postfix/submission  
#  -o smtpd_tls_security_level=encrypt  
#  -o smtpd_sasl_auth_enable=yes  
#  -o smtpd_tls_auth_only=yes  
#  -o smtpd_reject_unlisted_recipient=no  
#  -o smtpd_client_restrictions=$mua_client_restrictions  
#  -o smtpd_helo_restrictions=$mua_helo_restrictions  
#  -o smtpd_sender_restrictions=$mua_sender_restrictions  
#  -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject  
#  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject  
#  -o milter_macro_daemon_name=ORIGINATING  
#smtps    inet  n       -       n       -       -       smtpd
```

Редактирование файла

Перезапустим Postfix и Dovecot:

```
systemctl restart postfix  
systemctl restart dovecot
```

На клиенте установим telnet: `dnf -y install telnet`

На клиенте получим строку для аутентификации, вместо username указав логин вашего пользователя, а вместо password указав пароль этого пользователя: `printf 'username\x00username\x00password' | base64`

Подключимся на клиенте к SMTP-серверу посредством telnet: `telnet server.nvsakhno.net 25`

```
Last metadata expiration check: 1:43:48 ago on Sat 09 Dec 2023 02:58:02 PM UTC.  
Package telnet-1:0.17-85.el9.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!
```

Получение строки для аутентификации и подключение через telnet

Подключение не удалось.

3.3 Настройка SMTP over TLS

Настроим на сервере TLS, воспользовавшись временным сертификатом Dovecot. Предварительно скопируем необходимые файлы сертификата и ключа из каталога /etc/pki/dovecot в каталог /etc/pki/tls/ в соответствующие подкаталоги (чтобы не было проблем с SELinux):

```
cp /etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
cp /etc/pki/dovecot/private/dovecot.pem /etc/pki/tls/private
```

Сконфигурируем Postfix, указав пути к сертификату и ключу, а также к каталогу для хранения TLS-сессий и уровень безопасности:

```
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 = btree:/var/lib/postfix/smtpd_scache'
postconf -e 'smtpd_tls_security_level = may'
postconf -e 'smtp_tls_security_level = may'
```

```

/etc/pki/dovecot/certs/dovecot.pem /etc/pki/tls/certs
/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 = btree:/var/lib/postfix/smtpd_scache'
postconf -e 'smtpd_tls_security_level = may'
postconf -e 'smtp_tls_security_level = may'
```

Настройка SMTP over TLS

Для того чтобы запустить SMTP-сервер на 587-м порту, в файле /etc/postfix/master.cf изменим строки

```
# 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
#smtp     inet  n       -       n       -       1       postscreen
#smtpd    pass  -       -       n       -       -       smtpd
#dnsblog  unix  -       -       n       -       -       dnsblog
#tlsproxy unix  -       -       n       -       -       tlsproxy
submission inet n       -       n       -       -       smtpd
# -o syslog_name=postfix/submission
# -o smtpd_tls_security_level=encrypt
# -o smtpd_sasl_auth_enable=yes
# -o smtpd_tls_auth_only=yes
# -o smtpd_reject_unlisted_recipient=no
# -o smtpd_client_restrictions=$mua_client_restrictions
# -o smtpd_helo_restrictions=$mua_helo_restrictions
# -o smtpd_sender_restrictions=$mua_sender_restrictions
# -o smtpd_recipient_restrictions=reject_non_fqdn_recipient,reject_unknown_recipient_domain,permit_sasl_authenticated,reject
# -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
# -o milter_macro_daemon_name=ORIGINATING
```

Редактирование файла

Настроим межсетевой экран, разрешив работать службе smtp-submission:

```

RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-ks-client amqp amqps apcupsd audit ausweisapp2 bacula bacu
la-client bb bpp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-mon cfsengine checkmk-ag
ent cockpit collectd condor-collector cratedb etdb dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-registry dock
er-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeip
a-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gssd grafana gre high-availability
http https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdeconnect
kerberos kibana klogon kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-c
ontroller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker
kubectx kubectx-readonly kubectx-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-tcp llmnr-udp manage
sieve matrix mdns memcached minidlna mongod mongodb mosh mountd ngtt ngtt-tls ms-abt mssq murmur mysql nbd netbios-ns netdata-da
shboard nfs nfs3 nmap-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmpoxy pmwe
bapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dhcp ps3netsrv ptp pulseaudio pupp
etmaster quassel radius rdp redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc
sane sip sips sip smtp smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssd
ssh ssh-custom steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38
tinc tor-socks transmission-client upnp-client vdom vnc-server wbee-http wbee-https wireguard ws-discovery ws-discovery-c
lient ws-discovery-tcp ws-discovery-udp wsman wsman5 xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabb
ix-server zerotier

```

Настройка межсетевого экрана

Перезапустим Postfix: `systemctl restart postfix`

На клиенте подключимся к SMTP-серверу через 587-й порт посредством openssl:

```
openssl s_client -starttls smtp -crlf -connect server.dmbelicheva.net:587
```

```

80AB28FA507F0000:error:10080002:BIO routines:libcrypto/bio/bio_addr.c:738:Name or service not known
connect:errno=0

```

openssl

Подключение не удалось.

3.4 Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/`. В соответствующие подкаталоги поместим конфигурационные файлы Dovecot и Postfix:

```

$ /vagrant/provision/server
-R /etc/dovecot/dovecot.conf /vagrant/provision/server/mail/etc/dovecot/
/mail/etc/dovecot/dovecot.conf? y
-R /etc/dovecot/conf.d/10-master.conf /vagrant/provision/server/mail/etc/dovecot
-R /etc/dovecot/conf.d/10-auth.conf /vagrant/provision/server/mail/etc/dovecot/c
/mail/etc/dovecot/conf.d/10-auth.conf? y
-R /etc/postfix/master.cf /vagrant/provision/server/mail/etc/postfix/
/server/mail/etc/postfix/: Not a directory
-R /etc/postfix/master.cf /vagrant/provision/server/mail/etc/postfix
/mail/etc/postfix? y

```

Внесение изменений в настройки внутреннего окружения виртуальной машины

Внесем соответствующие изменения по расширенной конфигурации SMTP-сервера в файл `/vagrant/provision/server/mail.sh`:

```
root@server:/vagrant/provision/server
GNU nano 5.6.1 mail.sh
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install postfix
dnf -y install dovecot
dnf -y install telnet

echo "Copy configuration files"
cp -R /vagrant/provision/server/mail/etc/* /etc

chown -R root:root /etc/postfix
restorecon -vR /etc

echo "Configure firewall"
firewall-cmd --add-service smtp --permanent

firewall-cmd --add-service pop3 --permanent
firewall-cmd --add-service pop3s --permanent
firewall-cmd --add-service imap --permanent
firewall-cmd --add-service imaps --permanent

firewall-cmd --add-service smtp-submission --permanent

firewall-cmd --reload

echo "Start postfix service"
systemctl enable postfix
systemctl start postfix

echo "Configure postfix"
```

Редактирование файла

Внесем изменения в файл /vagrant/provision/client/mail.sh, добавив установку telnet.

```
root@client:/vagrant/provision/client
GNU nano 5.6.1 mail.sh
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install postfix
dnf -y install s-nail
dnf -y install evolution
dnf -y install telnet

echo "Configure postfix"
postconf -e 'inet_protocols = ipv4'

echo "Start postfix service"
systemctl enable postfix
systemctl start postfix
```

Редактирование файла

4 Выводы

В процессе выполнения данной лабораторной работы я приобрел практические навыки по конфигурированию SMTP-сервера в части настройки аутентификации.

5 Контрольные вопросы

1. Приведите пример задания формата аутентификации пользователя в Dovecot в форме логина с указанием домена.

auth_username_format = %Lu%d

2. Какие функции выполняет почтовый Relay-сервер?

обеспечивает приём сообщения, временное хранение (часто не больше нескольких минут в случае мгновенных сообщений, до недели в случае электронной почты), пересылку сообщения узлу-получателю (или следующему релю)

3. Какие угрозы безопасности могут возникнуть в случае настройки почтового сервера как Relay-сервера?

спам, перехват и изменение электронных сообщений.