Setting up Mail Server on the Debian platform

In the following article, TipsMake.com will guide you how to set up a full-featured, secure, easy-to-expand mail server system and replace some other functions if necessary

QuanTriMang.com - In the following article, TipsMake.com will guide you how to set up a full-featured, secure, easy-to-expand mail server system and replace some other functions if needed . This model provides virtual host services for mailboxes in many different formats, quota and server-side filtering modes, alias domain, address alias, forward address and catchall address. The forwarding process is secured with STARTTLS and SMTP-AUTH protocols. Received emails are strictly controlled by virus, spam and malicious filters and quickly remove SPF policies and DNSBLs.

And the whole process will be through 3 main servers:

- 1 server MX, here will focus all security features (*faramir.middle.earth*)

- An SMTP forwarding protocol, allowing users to send email outside (*ectelion.middle.earth*)

- 1 Mailstore server used to contain all the mailbox data (*denetor.middle.earth*)

Of course, you can assign more MX records to use DNS MX to domain, round-robin DNS forwarding services, email archiving, forwarding and branching functions . will be covered in full. in the writing.

All operations are performed on the system using the Debian server operating system.

LDAP setup

All user information is stored in the LDAP directory. And this is how we install on the server as a forwarding task. The system requires the following necessary packages:

sudo apt-get install slapd ldap-utils

Here, we will use the following LDAP parameters:

- *ldapBase: dc = middle, dc = earth*

- *adminDn: cn = admin, dc = middle, dc = earth*

- *adminPwd: thirdAge*

Besides, we need to use the existing LDAP schema. Most of the properties and objects must follow the standard, noting that there are many standard properties that users should pay attention to avoid duplication of occurrences.

Pair the available schema into openldap in /etc/ldap/schema/mailMEO.schema:

attributetype (2.16.840.1.113730.3.1.13
NAME 'mailLocalAddress'
DESC 'RFC822 email address of this recipient'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 {256})
attributetype (2.16.840.1.113730.3.1.16
NAME 'mailQuota'
DESC 'Maximal s? c?a ??a trên cho m?t th? m?c trong kilobytes'
EQUALITY integerMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.27)
attributetype (2.16.840.1.113730.3.1.18
NAME 'mailHost'
DESC 'FQDN of the SMTP / MTA of this recipient'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 {256}
SINGLE-VALUE)
attributetype (2.16.840.1.113730.3.1.22
NAME 'mailCopyAddress'
DESC 'RFC822 email shadow copy address'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 {256})
attributetype (2.16.840.1.113730.3.1.47
NAME 'mailRoutingAddress'
DESC 'RFC822 routing address of this recipient'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 {256})
attributetype (2.16.840.1.113730.3.1.49
NAME 'spamassassinUserPrefs'
DESC 'SpamAssassin user preferences'
EQUALITY caseIgnoreIA5Match
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 {256})
objectclass (2.16.840.1.113730.3.2.147
NAME 'inetLocalMailRecipient'
DESC 'Internet local mail recipient'
SUP top AUXILIARY
MAY (mailLocalAddress $ mailHost $ mailRoutingAddress $ mailCopyAddress $ mailQuota $ spamassassinUserPrefs))

objectclass (2.16.840.1.113730.3.2.148
NAME 'inetMailForwarder'
DESC 'Internet mail Forward Address'

SUP top AUXILIARY
MAY (mailHost $ mailRoutingAddress))

and assign the correct schema within /etc/ldap/slapd.conf:

.
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/mailMEO.schema
.

Check the suffix (when installing slapd, debconf is pre-configured):

suffix "dc = middle, dc = earth"

Then, assign additional ACLs of the daemon to use to transfer data to LDAP. Create a readonly property to access userPassword for devecot:

access to attrs = userPassword, shadowLastChange
by dn = "cn = admin, dc = middle, dc = earth" write
by dn = "uid = dovecot, dc = middle, dc = earth" read
by anonymous auth
b?i self ghi
*by * none*

Set similar properties for exim and dovecot:

*access to **
by dn = "cn = admin, dc = middle, dc = earth" write
by dn = "uid = dovecot, dc = middle, dc = earth" read
by dn = "uid = exim, dc = middle, dc = earth" read
*by * read*
b?i anonymous none

The final ACL parameter takes care of preventing the ability to read data from anonymous accounts but is allowed to edit with verified accounts. Restart slapd to apply the changes above:

sudo /etc/init.d/slapd restart

After that, we have to create user accounts with previous ACLs. To do this, we must use the following user.ldif file:

dn: uid = exim, dc = middle, dc = earth
objectClass: account
objectClass: simpleSecurityObject
objectClass: top

uid: exim
userPassword :: e01ENX1hOElTeXAwV2hnVzFSVnhHd0hCNDF3PT0 =
dn: uid = dovecot, dc = middle, dc = earth
objectClass: account
objectClass: simpleSecurityObject
objectClass: top
uid: dovecot
userPassword :: e01ENX1yZGp2Q1lPNmtDRm1scXAyVWQwa0xBPT0 =

This account will have user / pass: dovecot / dovecotpopper and exim4 / eximmta

To provide information and data for the root directory, use the following command:

ldapadd -x -D cn = admin, dc = middle, dc = earth -W

Below is a sample ldif file containing other data:

dn: ou = domains, dc = middle, dc = earth
objectClass: organizationalUnit
objectClass: top
ou: domains
dn: dc = middle.earth, ou = domains, dc = middle, dc = earth
dc: middle.earth
objectClass: dNSDomain
objectClass: top
objectClass: inetLocalMailRecipient
objectClass: domainRelatedObject
objectClass: posixAccount
mailLocalAddress: catchall@middle.earth
cn: catchall
gidNumber: 8
homeDirectory: /var/mail/middle.earth/c/catchall
uid: catchall
uidNumber: 8
userPassword :: e01ENX1EV3RteGErOFROanJKNUFXZWt1Z0tBPT0 =
mailQuota: 102400
mailHost: denetor.middle.earth
associatedDomain: middle.earth
associatedDomain: lotr.middle.earth
dn: uid = sam, dc = middle.earth, ou = domains, dc = middle, dc = earth
cn: sam
displayName: Sam Gamji
gidNumber: 8
homeDirectory: /var/mail/middle.earth/s/sam
mail: sam@middle.earth
mailHost: 172.16.16.23
mailQuota: 102400

objectClass: inetLocalMailRecipient
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
sn: Gamji
uidNumber: 8
uid: sam
userPassword :: e01ENX1NeVV5M1BxaHkvWWVLaVpyMXlOaExBPT0 =
mailLocalAddress: sam@middle.earth
mailLocalAddress: gamji@middle.earth
mailLocalAddress: shire@middle.earth
dn: uid = frodo, dc = middle.earth, ou = domains, dc = middle, dc = earth
cn: frodo
displayName: Frodo Baggins
gidNumber: 8
givenName: Frodo
homeDirectory: /var/mail/middle.earth/f/frodo
mail: frodo@middle.earth
mailHost: 172.16.16.23
mailQuota: 102400
objectClass: inetLocalMailRecipient
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
sn: Baggins
uidNumber: 8
uid: frodo
userPassword :: e01ENX04UGlDRHVnWEdCMmNhRktnbDljTmpRPT0 =
mailLocalAddress: frodo@middle.earth
mailLocalAddress: baggins@middle.earth
mailLocalAddress: shire@middle.earth
dn: uid = gmail, dc = middle.earth, ou = domains, dc = middle, dc = earth
cn: gmail
mail: alxgomz@gmail.com
mailHost: 172.16.16.23
mailRoutingAddress: alxgomz@gmail.com
objectClass: inetMailForwarder
objectClass: inetOrgPerson
objectClass: top
sn: alias to Gmail address
uid: gmail

Set up MTAs

Here, we will use the MTA Exim4 on the MX system, server for forwarding and archiving email.

With forwarding server:

First, we need to add volatile repository in the file /etc/apt/source.list.d/volatile.list:

deb http://volatile.debian.org/debian-volatile lenny / volatile main

and update apt database:

sudo apt-get update

Then there is the step to install exim4, remember to select Yes to split the configuration files:

sudo apt-get install exim4-daemon-heavy clamav-clamav-freshclam daemon openssl

In order, to use TLS through SMTP sessions, the system needs a certificate - certificate. It can be a certificate provided by organizations, businesses or just created by the system itself. Here, we will use the second case - the self-created certificate, when using the workstation, will display warning information about these certificates.

Create RSA key:

openssl genrsa 2048

chmod 640 exim.key

Certificate request:

openssl req -new -key exim.key -out exim.csr

Certificate confirmation:

openssl x509 -req -signkey exim.key -in exim.csr -days 9999 -out exim.c

Copy file:

chown Debian-exim exim.key

sudo cp exim.key exim.crt / etc / exim4

Enable TLS in the file /etc/exim4/update-exim4.conf.conf:

.
MAIN_TLS_ENABLE = 'true'

.

Then, create the macro file that initializes /etc/exim4/conf.d/main/04_mailMEOmacrodefs:

ldap_default_servers = ldap.middle.earth
.ifndef MAILMEO_DOMAINROOT
MAILMEO_DOMAINROOT = ou = domains, dc = middle, dc = earth
.endif

MAILMEO_DOMAINROOT defines and initializes the LDAP root dn value, which stores information about domain and user. For servers that are transitioning, the user accounts will be verified before the email is sent, this model is SMTP-AUTH. And to do this, we have to create another configuration file /etc/exim4/conf.d/auth/50_mailMEO_authsmtp:

plain_server:
driver = plaintext
public_name = PLAIN
{user = "uid = $ {quote_ldap_dn: $ {extract {1} {@} {$ 2} {$ value} fail}},
dc = $ {quote_ldap_dn: $ {extract {2} {@} {$ 2} {$ value} fail}},
MAILMEO_DOMAINROOT "
pass = $ {quote: $ 3}
ldap: ///} {yes} {no}}
server_set_id = $ auth2
server_prompts =:
.ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
server_advertise_condition = $ {if eq {$ tls_cipher} {} {} {}}*
.endif
login_server:
driver = plaintext
public_name = LOGIN
{user = "uid = $ {quote_ldap_dn: $ {extract {1} {@} {$ 1} {$ value} fail}},
dc = $ {quote_ldap_dn: $ {extract {2} {@} {$ 1} {$ value} fail}},
MAILMEO_DOMAINROOT "
pass = $ {quote: $ 2}
ldap: ///} {yes} {no}}
server_set_id = $ auth1
server_prompts = "Username ::: Password ::"
.ifndef AUTH_SERVER_ALLOW_NOTLS_PASSWORDS
server_advertise_condition = $ {if eq {$ tls_cipher} {} {} {}}*
.endif

Since we store passwords in encrypted form, it is imperative to use a password authentication mechanism explicitly based on PLAIN or LOGIN (or both). On the other hand, administrators should only use the AUTH standard to 'hide' SMTP sessions. And if you want to use the AUTH function to delete all sessions, initialize AUTH_SERVER_ALLOW_NOTLS_PASSWORDS parameter (eg set to true) in the file /etc/exim4/conf.d/main/04_mailMEOmacrodefs. In addition, we will require exim to transfer all data through port 587 - which is more commonly used than MUA to upload email, and to inform TLS standards. In the configuration file /etc/exim4/update-exim4.conf.conf, modify the dc_local_interfaces parameter according to the following value:

dc_local_interfaces = '0.0.0.0: 0.0.0.0.587'

The security function of Antivirus programs - clamav here is guaranteed, this application is closely linked to exim4. All you need to do is activate the option in the file /etc/exim4/conf.d/main/02_exim4-config_options:

av_scanner = clamd: /var/run/clamav/clamd.ctl

Uncomment 3 lines in the file /etc/exim4/conf.d/acl/40_exim4-config_check_data:

deny
*malware = **
message = Thông báo này ???c tìm th?y có th? malware ($ malware_name).

Assign clamav accounts to the Debian-exim group:

sudo adduser clamav Debian-exim

After that, restart clamav and exim4, and we have completed the basic steps with the forwarding server:

sudo /etc/init.d/clamav-daemon restart

sudo /etc/init.d/exim4 restart

With storage server - Mailstore

This server is responsible for storing all the email data on the system, the process of checking and sorting spam is also done here. In fact, this process will consume a lot of system resources, so most people just want to do this step after each filtering process (DNSBL or similar). To make the most of dovecot's effectiveness, we should use 1.2.x version. Unfortunately, version 1.0 for Debian lacks many important functions, typically quotawarning. To overcome this situation, we need to add repository backport by file /etc/apt/sources.list.d/backports.list:

deb http://backports.debian.org/debian-backports lenny-main backports

and run the following commands:

sudo apt-get update

sudo apt-get install spamassassin exim4-daemon-heavy

sudo apt-get -t lenny-backports install dovecot-imapd dovecot-pop3d

Exim definitions in the file /etc/exim4/conf.d/main/04_mailMEOmacrodefs:

ldap_default_servers = ldap.middle.earth
 # mailMEO macros definitions
.ifndef MAILMEO_DOMAINROOT
MAILMEO_DOMAINROOT = ou = domains, dc = middle, dc = earth
.endif
.ifndef MAILMEO_MAINDOMAIN
MAILMEO_MAINDOMAIN = $ {lookup ldap {USER = userid = exim, dc = middle, dc = earth PASS = eximmta ldap: /// MAILMEO_DOMAINROOT? Dc? One? (AssociatedDomain = $ domain)}}
.endif
domainlist mailMEO_domains = USER = userid = exim, dc = middle, dc = earth PASS = eximmta ldap: /// MAILMEO_DOMAINROOT? associatedDomain? one?
kup dnsdb {a = $ primary_hostname} {$ value} fail}))}}} {,} {n}}

where the mailMEO_domains value will return the result as a list of domains hosted in LDAP, and to enable management features with domains in LDAP, we simply need to create additional entry entries based on the template. later (please change the specifications according to your system):

dn: dc =% MYDOMAIN.TLD%, ou = domains, dc = middle, dc = earth
dc: middle.earth
objectClass: dNSDomain
objectClass: top
objectClass: inetLocalMailRecipient
objectClass: domainRelatedObject
mailHost:% IPADDR_OF_MAILSTORE%
associatedDomain:% MYDOMAIN%

On the other hand, we must explicitly specify exim to accept those domains by adding the domainlist to the rcpt acl file: /etc/exim4/conf.d/acl/30_exim4-config_check_rcpt, please change the following parameters:

require
message = relay không có quy?n
domains = + local_domains: + relay_to_domains
into:

require
message = relay không có quy?n
domains = + local_domains: + relay_to_domains: + mailMEO_domains

Here, MAILMEO_MAINDOMAIN refers to a function that we often call domain aliasing, which allows email addresses of this domain to exist in another domain as well. In the sample data lotr.middle.earth is a domain alias of middle.earth, so the frodo mailbox can be accessed from frodo@middle.earth or frodo@lotr.middle.earth. In which middle.earth is the main domain, with a certain level of authorization, for example, authentication via POP / IMAP / SMTP can only be used through this main domain.

Aliases:
This is the second address for the mailbox, they must belong to the same domain as the destination address. 1

Alias ??can be assigned to multiple mailboxes, in case all mailboxes receive email to send to available addresses. In the sample data item, baggins@middle.earth is an alias of frodo@middle.earth and shire@middle.earth is alias of both 2, frodo@middle.earth and sam@middle.earth.

To assign aliases to an existing mailbox, you just need to add the mailLocalAddress attribute to the alias mail address. The file /etc/exim4/conf.d/router/070_mailMEO_alias is responsible for routing for addresses like mailMEO_alias:

mailMEO_alias:
driver = redirect
debug_print = "R: locally aliased from $ local_part @ $ domain"
domains = + mailMEO_domains
qualify_domain = MAILMEO_MAINDOMAIN
check_ancestor = true

(& (objectClass = inetLocalMailRecipient) (objectClass = inetOrgPerson) (mailLocalAddress = $ local_part @ $ domain))}
}}{([w-.]+)@([w-]+.)([w-]+)}{$1}}
} {,} {n}}
(& (objectClass = inetLocalMailRecipient) (objectClass = inetOrgPerson) (mailLocalAddress = $ local_part @ $ domain))}}
} {([w -.] +)} {$ 1 @ $ domain}
}

Forwarding - Forwarder

This transition is quite similar to alias except that they can transfer emails to non-domain addresses or even remote addresses. To create a mail forward, create an LDAP entry below the domain entry in the following form:

dn: uid = gmail, dc = middle.earth, ou = domains, dc = middle, dc = earth
cn:% FWD_LOCALPART%
mail:% DEST_MAILADDR%
mailHost:% IPADDR_OF_MAILSTORE%
mailRoutingAddress:% DEST_MAILADDR%
objectClass: inetMailForwarder
objectClass: inetOrgPerson
objectClass: top
sn: Alias ??address
uid:% FWD_LOCALPART%
The file /etc/exim4/conf.d/router/071_mailMEO_fwd also belongs to this address:

mailMEO_fwd_routes:
driver = redirect
debug_print = "R: Forwarded from $ local_part @ $ domain"
domains = + mailMEO_domains
qualify_domain = MAILMEO_MAINDOMAIN
check_ancestor = true

forbid_pipe = true
forbid_file = true
forbid_exim_filter = true
(& (uid = $ local_part) (objectClass = inetOrgPerson) (objectClass = inetMailForwarder))}
}
(& (uid = $ local_part) (objectClass = inetOrgPerson) (objectClass = inetMailForwarder))}
}

Catchall

It is understandable that this is a classified spam box, can receive all emails sent to different domains regardless of the local path. Users can merge this normal mailbox or catchall mailbox together (of course only one catchall can be used on one domain). And to assign catchall addresses to the domain, join posixAccount to the domain entry (and all necessary attributes) such as mailLocalAddress and mailQuota:

objectClass: posixAccount
mailLocalAddress:% CATCHALL_ADDR%
gidNumber:% gID%
homeDirectory:% MAILDIR_PATH%
uid:% CATCHALL_LOCALPART%
uidNumber:% UID%
userPassword ::% HASH_PASS_STR%
mailQuota:% KB%
The file /etc/exim4/conf.d/router/079_mailMEO_catchall will initialize the routing value for catchall:

mailMEO_catchall:
driver = redirect
debug_print = "R: domain catchall for $ domain domains = USER = userid = exim, dc = middle, dc = earth PASS = eximmta
ldap: /// ou = domains, dc = middle, dc = earth? associatedDomain? one?
(& (objectClass = inetLocalMailRecipient) (objectClass = posixAccount) (objectClass = dNSDomain) (mailHost = $ primary_hostname))}}} {,} {n}}
qualify_domain = MAILMEO_MAINDOMAIN
ldap: /// dc = MAILMEO_MAINDOMAIN, MAILMEO_DOMAINROOT? uid? base?}
}

Virtual user accounts

To create this account, please join the LDAP entry below the domain in the following form:

dn: uid =% LOCALPART%, dc =% DOMAIN%, ou = domains, dc = middle, dc = earth
cn:% SOMETHING_DESCRIPTIVE%
displayName:% SOMETHING_DESCRIPTIVE%
gidNumber:% GID%
givenName:% SOMETHING_DESCRIPTIVE%
homeDirectory:% MAILDIR_PATH%

mail:% EMAIL_ADDR%
mailHost:% IPADDR_OF_MAILSTORE%
mailQuota:% KB%
objectClass: inetLocalMailRecipient
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
sn:% SOMETHING_DESCRIPTIVE%
uidNumber:% UID
uid:% LOCALPART%
userPassword ::% HASH_PASS_STR%
mailLocalAddress:% EMAIL_ADDR%

But please note that the main email addresses must be set up according to the mailLocalAddress feature like that of alias. The routing process is based on the file /etc/exim4/conf.d/router/077_mailMEO_users:

mailMEO_virtual:
driver = accept
debug_print = "R: mailMEO virtual for $ local_part @ $ domain"
domains = + mailMEO_domains
(& (objectClass = inetLocalMailRecipient) (uid = $ local_part))}
}
transport = mailMEO_virtual_delivery

Spamassassin

This function is used to check email, prevent spam by spamassassin daemon:

spamcheck_router:
no_verify
condition = $ {if and {{{$ message_size} {90K}} {! def: header_X-Spam-Flag:} {! eq {$ received_protocol} {spam-scanned}}} {1} {0}}
driver = accept
transport = spamcheck

This test is applied to all emails identified in spamassassin daemon. And the SA transport is set up in the file /etc/exim4/conf.d/transport/50_mailMEO_spamcheck:

spamcheck:
driver = pipe
command = / usr / sbin / exim4 -oMr spam-scanned -bS
use_bsmtp = true
transport_filter = / usr / bin / spamc -u $ local_part @ $ domain
home_directory = "/ dev / shm"
current_directory = "/ dev / shm"
 # ph?i s? d?ng m?t quy?n h?n ng??i dùng ?? ??t $ received_protocol on the way back in!

user = mail
group = mail
log_output = true
return_fail_output = true
return_path_add = false
message_prefix =
message_suffix =

And now the SpamAssassin tuning operations, most configuration files are stored in /etc/spamassassin/local.cf:

user_scores_dsn ldap: //ldap.middle.earth/ou=domains,dc=middle,dc=earth? spamassassinUserPrefs? sub? (& (mailLocalAddress = __ USERNAME__) (objectClass = inetLocalMailRecipient))
user_scores_ldap_username uid = exim, dc = middle, dc = earth
user_scores_ldap_password eximmta
clear_headers
*add_header all Flag _YESNO_*
add_header spam Result _SCORE _ / _ REQD_ (_TESTS_)

By changing this setting, you can sort it out for each account, just apply the spamassassinUserPrefs attribute to the form value item value. Besides, we need to enable more spamd in / etc / default / spamassassin:

ENABLED = 1
OPTIONS = "- x --ldap-config -u nobody - max-children 5"

and start this feature:

sudo /etc/init.d/spamassassin restart

Restart exim:

sudo /etc/init.d/exim4 restart

At this point, the entire email cannot be sent to the mailstore (dovecot needs to be adjusted), and most security functions have not been activated yet.

MX server

At this step, we will proceed to pair security features. Also here, MX server will take the virus scanning function, on the other hand need to have volatile repository in the file /etc/apt/sources.list.d/volatile.list:

deb http://volatile.debian.org/debian-volatile lenny / volatile main

and backport for newer versions of dovecot in the file /etc/apt/sources.list.d/backports.list:

deb http://backports.debian.org/debian-backports lenny-main backports

Update the database for apt:

sudo apt-get update

and install the required packages as usual:

sudo apt-get install clamav -clamav-freshclam exim4 daemon-heavy libmail-spf-query-perl

sudo apt-get -t lenny-backports install dovecot-imapd dovecot-pop3d

Continue with the exim4 installation process similar to the relay server. The file /etc/exim4/conf.d/main/04_mailMEOmacrodefs initializes the macros for us to use in other config files:

ldap_default_servers = ldap.middle.earth
 # mailMEO macros definitions
.ifndef MAILMEO_DOMAINROOT
MAILMEO_DOMAINROOT = ou = domains, dc = middle, dc = earth
.endif
.ifndef MAILMEO_MAINDOMAIN
MAILMEO_MAINDOMAIN = $ {lookup ldap {USER = userid = exim, dc = middle, dc = earth PASS = eximmta ldap: /// MAILMEO_DOMAINROOT? Dc? One? (AssociatedDomain = $ domain)}}
.endif
domainlist mailMEO_domains = USER = userid = exim, dc = middle, dc = earth PASS = eximmta ldap: /// MAILMEO_DOMAINROOT? associatedDomain? one? (& (objectClass = inetLocalMailRecipient) (objectClass = dNSDomain))}}} {,} {n}}
.ifndef CHECK_RCPT_IP_DNSBLS
CHECK_RCPT_IP_DNSBLS = cbl.abuseat.org:dnsbl.njabl.org:sbl.spamhaus.org
.endif
.ifndef CHECK_RCPT_SPF
CHECK_RCPT_SPF = true
.endif

CHECK_RCPT_SPF activates SPF to check in the SMTP session, rejecting mail to check mail if spf fails. On the other hand, CHECK_RCPT_IP_DNSBL also activates the DNSBL lookup function. Open the file /etc/exim4/conf.d/acl/30_exim4-config_check_rcpt and change the following parameters:

.ifdef CHECK_RCPT_IP_DNSBLS
warn
message = X-Warning: $ sender_host_address is listed at $ dnslist_domain ($ dnslist_value: $ dnslist_text)
log_message = $ sender_host_address is listed at $ dnslist_domain ($ dnslist_value: $ dnslist_text)
dnslists = CHECK_RCPT_IP_DNSBLS
.endif

into:

.ifdef CHECK_RCPT_IP_DNSBLS
deny
message = Access denied: $ sender_host_address is listed at $ dnslist_domain ($ dnslist_value: $ dnslist_text)
dnslists = CHECK_RCPT_IP_DNSBLS
.endif

And specify exim to accept domain values ??initialized by mailMEO_domains in the file /etc/exim4/conf.d/acl/30_exim4-config_check_rcpt. Please change:

require
message = relay không có quy?n
domains = + local_domains: + relay_to_domains

into:

require
message = relay không có quy?n
domains = + local_domains: + relay_to_domains: + mailMEO_domains

Enable the same antivirus function with server relay in the file /etc/exim4/conf.d/main/02_exim4-config_options:

av_scanner = clamd: /var/run/clamav/clamd.ctl

Uncomment 3 lines in the file /etc/exim4/conf.d/acl/40_exim4-config_check_data:

deny
*malware = **
message = Thông báo này ???c tìm th?y có th? malware ($ malware_name).

And assign user accounts clamav to the Debian-exim group:

sudo adduser clamav Debian-exim
sudo /etc/init.d/clamav-daemon restart

The main purpose of MX server is to orient the whole email to the mailstore server MX - where the mailbox is stored. In Exim, this orientation can be done using manual driver routing, capable of sending email through remote SMTP hosts. Here, we need two drivers - drivers to manage, hold user accounts, aliases and forwarders on one side and all catchall accounts on the other side.

All are in the file /etc/exim4/conf.d/router/075_mailMEOroutes:

mailMEO_routes:
debug_print = "R: $ local_part @ $ domain routed with mailMEO_routes to $ 0"
driver = manualroute
domains = + mailMEO_domains
transport = remote_smtp
(& (objectClass = inetLocalMailRecipient) (mailLocalAddress = $ local_part @ $ domain))}
}}{([w-.]+)@([w-]+.)([w-]+)}{$1}}
(uid = $ local_part)}}
} {,} {n}}
ldap: /// dc = MAILMEO_MAINDOMAIN, MAILMEO_DOMAINROOT? mailHost? base?}}
host_find_failed = defer
same_domain_copy_routing = yes
mailMEO_catchall_routes:
debug_print = "R: $ local_part @ $ domain routed with mailMEO_catchall_route to $ 0"
driver = manualroute
(& (objectClass = inetLocalMailRecipient) (objectClass = posixAccount) (objectClass = dNSDomain))}}
} {,} {n}}
transport = remote_smtp
ldap: /// dc = MAILMEO_MAINDOMAIN, MAILMEO_DOMAINROOT? mailHost? base?}}
host_find_failed = defer
same_domain_copy_routing = yes

This process can be briefly explained as follows: this router will perform the task of checking and confirming that the domain is first stored on ldap, then check to see if those email addresses are available, and request the hostname of the mail server where the mailbox is located.

Then restart exim and continue with dovecot in the following section:

sudo /etc/init.d/exim4 restart

Adjust and set up Dovecot

Dovecot is used to receive email via POP3 or IMAP. Of course, Dovecot must be installed on the mailstore, but for systems with multiple mailstore, we need POP / IMAP proxy to locate all connections to the mailstore to store mailboxes to receive emails. Dovecot is now a popular POP / IMAP server and is widely used.

With Dovecot on the mailstore :

Here, we will proceed to set up dovecot on the mailstore. There are two configuration files to adjust, file /etc/dovecot/dovecot.conf:

protocols = imap imaps pop3 pop3s managesi ve
disable_plaintext_auth = no
log_timestamp = "% Y-% m-% d% H:% M:% S"
mail_location = maildir:% h / MailDir

```
mail_privileged_group = mail
#mail_debug = yes
first_valid_uid = 8
last_valid_uid = 8
first_valid_gid = 8
last_valid_gid = 8
protocol imap {
mail_plugins = imap_quota quota
}
protocol pop3 {
pop3_uidl_format =% 08Xu% 08Xv
mail_plugins = quota
}
protocol managesieve {
login_executable = / usr / lib / dovecot / managesieve-login
mail_executable = / usr / lib / dovecot / managesieve
}
protocol lda {
postmaster_address = postmaster@denetor.middle.earth
hostname = denetor@middle.earth
mail_plugins = quota sieve
auth_socket_path = / var / run / dovecot / auth-master
sieve_global_path = / var / sieve / global
sieve = ~ / .dovecot.sieve
}
auth default {
mechanisms = plain login
passdb ldap {
args = /etc/dovecot/dovecot-ldap.conf
}
userdb ldap {
args = /etc/dovecot/dovecot-ldap.conf
}
userdb prefetch {
}
user = root
socket listen {
master {
path = /var/run/dovecot/auth-master
mode = 0660
group = mail
}
client {
path = /var/run/dovecot/auth-client
mode = 0660
group = mail
}
}
```

}
dict {
}
plugin {
quota = maildir:User quota
quota_warning = storage=90%% /usr/local/bin/quota-warning.sh 90
sieve_before = /var/sieve/global
}

và file /etc/dovecot/dovecot-ldap.conf:

uris = ldap://ldap.middle.earth
dn = uid=dovecot,dc=middle,dc=earth
dnpass = dovecotpopper
ldap_version = 3
base = dc=%d,ou=domains,dc=middle,dc=earth
scope = subtree
user_attrs =
homeDirectory=home,uidNumber=uid,gidNumber=gid,mailQuota=quota_rule=:storage=%$*
user_filter = (&(objectClass=inetLocalMailRecipient)(objectClass=posixAccount)(uid=%n))
pass_attrs =
mailRoutingAddress=user,userPassword=password,homeDirectory=userdb_home,uidNumber
=userdb_uid,gidNumber=userdb_gid,mailQuota=userdb_quota_rule=:storage=%$*
pass_filter = (&(objectClass=inetLocalMailRecipient)(objectClass=posixAccount)(uid=%n))
default_pass_scheme = LDAP-MD5

Nh? là 1 ph?n c?a b? l?c t?ng h?p chúng ta ?ã ??nh ngh?a và kh?i t?o bên trên, và ???c s? d?ng ?? l?u tr? d? li?u trong m?c Junk – b? spamassassin ng?n ch?n và báo cáo v?i phân lo?i spam:

sudo mkdir /var/sieve

B? l?c ???c s? d?ng ? ?ây là /var/sieve/global:

require "fileinto";
if header :contains ["X-Spam-Flag"] ["Yes"] {
fileinto "Junk";
stop;
}
sudo chown mail -R /var/sieve

và c?ng nh? 1 ph?n c?a plugin quota, chúng ta c?n t?o ra 1 ?o?n mã ng?n ?? c?nh báo ng??i s? d?ng r?ng h? ?ã g ?n s? d?ng h?t l?u l??ng cho phép, thông tin này ???c l?u tr? t?i /usr/local/bin/quota-warning.sh:

#! / bin / sh
PERCENT=$1
FROM="postmaster@denetor.middle.earth"

qwf="/tmp/quota.warning.$$"
echo "From: $FROM
To: $USER
To: postmaster@domain.org
Subject: Your email quota is $PERCENT% full
Content-Type: text/plain; charset='UTF-8'
This message is automatically created
by mail delivery software.
The size of your mailbox has exceeded
a warning threshold that is
set by the system administrator.
*You *must* delete mails or empty some folders*
or you may loose emails in the future.">> $qwf
cat $qwf | /usr/sbin/sendmail -f $FROM "$USER"
rm -f $qwf
exit 0
sudo chmod +x /usr/local/bin/quota-warning.sh

Thi?t l?p Dovecot trên MX

Trên h? th?ng l?u tr? này, chúng ta s? ?i?u ch?nh và thi?t l?p l?i Dovecot ?? ho?t ??ng nh? 1 proxy. T?t c? thông tin thi?t l?p ??u n?m trong file /etc/dovecot/dovecot.conf:

protocols = imap imaps pop3 pop3s managesieve
disable_plaintext_auth = no
log_timestamp = "%Y-%m-%d %H:%M:%S "
login_process_per_connection = no
login_processes_count = 8
mail_uid = 8
mail_gid = 8
mail_privileged_group = mail
first_valid_uid = 8
last_valid_uid = 8
first_valid_gid = 8
last_valid_gid = 8
protocol imap {
}
protocol pop3 {
pop3_uidl_format = %08Xu%08Xv
}
protocol managesieve {
}
auth default {
mechanisms = plain login
passdb ldap {
args = /etc/dovecot/dovecot-ldap.conf
}

userdb passwd {
}
userdb static {
}
user = nobody
}
dict {
}
plugin {
}

và /etc/dovecot/dovecot-ldap.conf:

uris = ldap://ldap.middle.earth
dn = uid=dovecot,dc=middle,dc=earth
dnpass = dovecotpopper
base = dc=%d,ou=domains,dc=middle,dc=earth
pass_attrs==nopassword=1,=password=,=proxy=y,mailHost=host,=destuser=%u
pass_filter = (&(objectClass=inetLocalMailRecipient)(objectClass=posixAccount)(uid=%n))

Các l?u ý c?n quan tâm

N?u mu?n dùng nhi?u mailstore, ban có th? áp d?ng c? s? d? li?u sql ?? l?u tr? d? li?u bayesian và chia s? trên t?t c? các mailstore (nh?ng hi?n t?i thì tính n?ng l?u tr? bayesian trong ldap ch?a có s?n)

?? qu?n lý các tài kho?n ng??i s? d?ng, domain và t?t c? các thành ph?n liên quan thì ng??i dùng có th? áp d?ng b?t c? mô hình ldap client nào, ví d? nh? PHPLDAPAdmin

Trong bài h??ng d?n trên, t?t c? các ho?t ??ng ??u ???c th?c hi?n trên tài kho?n mail, tùy t?ng h? th?ng c?a ng??i dùng mà các b?n nên có nh?ng thay ??i c?n thi?t và thích h?p

Trên ?ây là 1 s? b??c h??ng d?n ?? thi?t l?p h? th?ng Mail Server s? d?ng Exim4, Clamav, Dovecot, SpamAssassin … trên n?n t?ng Debian. Good luck!