* 1. Install the mail server with mysql:

yum -y update && \  
yum -y install epel-release && \  
yum -y update && \  
yum -y install dovecot dovecot-mysql mariadb-server nginx opendkim php-fpm php-mbstring php-mysql php-xml postfix pypolicyd-spf tar wget

*来自 <*[*https://zhuanlan.zhihu.com/p/28816035*](https://zhuanlan.zhihu.com/p/28816035)*>*

* 1. Config mysql:
     1. systemctl start mariadb
     2. mysql\_secure\_installation
     3. 文本, 信件

        描述已自动生成

CREATE USER 'mail\_sys'@'localhost' IDENTIFIED BY 'mail\_sys';

CREATE DATABASE mail\_sys;

GRANT SELECT ON mail\_sys.\* TO 'mail\_sys'@'localhost' IDENTIFIED BY 'mail\_sys';

Flush privileges;

Use mail\_sys;

CREATE TABLE `domains` ( `id` int(20) NOT NULL auto\_increment, `name` varchar(100) NOT NULL, PRIMARY KEY (`id`) ) ENGINE=InnoDB DEFAULT CHARSET=utf8;

*CREATE TABLE `users` ( `id` int(20) NOT NULL auto\_increment, `domain\_id` int(20) NOT NULL, `password` varchar(200) NOT NULL, `email` varchar(200) NOT NULL, PRIMARY KEY (`id`), UNIQUE KEY `email` (`email`), FOREIGN KEY (domain\_id) REFERENCES domains(id) ON DELETE CASCADE ) ENGINE=InnoDB DEFAULT CHARSET=utf8;*

CREATE TABLE `aliases` ( `id` int(20) NOT NULL auto\_increment, `domain\_id` int(20) NOT NULL, `source` varchar(200) NOT NULL, `destination` varchar(200) NOT NULL, PRIMARY KEY (`id`), FOREIGN KEY (domain\_id) REFERENCES domains(id) ON DELETE CASCADE ) ENGINE=InnoDB DEFAULT CHARSET=utf8;

* 1. Register mail info:

|  |  |
| --- | --- |
| Insert domain name: | INSERT INTO `mail\_sys`.`domains` (`id` ,`name`) VALUES ('<域名索引号>', '<域名>'); |
| Add users | INSERT INTO `mail\_sys`.`users`(`id`, `domain\_id`, `password` , `email`) VALUES ('<用户索引号>', '<域名索引号>', ENCRYPT('<密码>', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), '<邮箱地址>'),    E.g.  INSERT INTO `mail\_sys`.`users`  (`id`, `domain\_id`, `password` , `email`) VALUES  ('1', '1', ENCRYPT('123456789', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'ceo@hepta.com'),  ('2', '1', ENCRYPT('123456789', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'hr@hepta.com'),  ('3', '1', ENCRYPT('123456789', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 'lyon@hepta.com'); |
| Alias （optional） | See the website |

* 1. Create email user group:
     1. groupadd -g 2000 mail\_sys
     2. useradd -g mail\_sys -u 2000 mail\_sys -d /var/spool/mail -s /sbin/nologin
     3. chown -R mail\_sys:mail\_sys /var/spool/mail
  2. Config postfix
     1. cp -r /etc/postfix /etc/postfix.bak
     2. Generate cert.pem + key.pem file:

[root@proxy ~]# cd /usr/local/nginx/conf #进入到目录下生成证书秘钥

[root@proxy conf]# openssl genrsa > cert.key #生成私钥,文件名必须与配置文件内相同

[root@proxy conf]# openssl req -new -x509 -key cert.key > cert.pem #生成证书,需要输入信息

Country Name (2 letter code) [XX]: china #国家

State or Province Name (full name) []:hunan #省份

Locality Name (eg, city) [Default City]:changsha #城市

Organization Name (eg, company) [Default Company Ltd]:xxx #公司名

Organizational Unit Name (eg, section) []:xxx #单位名

Common Name (eg, your name or your server's hostname) []:主机名 #主机名hostname查看

Email Address []:xx@xx.com #邮箱



* 1. Change the value of main.cf to :(remember to delete the Chinese characters or when connecting the mysql it will report error, because of the utf-8 character set)

cat > /etc/postfix/main.cf << EOF

mydomain = example.com # 您的域名，需要修改  
myhostname = mail.example.com # 您的域名前面加上 mail. 需要修改  
mydestination = localhost  
alias\_maps = hash:/etc/aliases  
alias\_database = hash:/etc/aliases  
myorigin = /etc/mailname  
mynetworks = 127.0.0.0/8  
mailbox\_size\_limit = 0  
recipient\_delimiter = +  
inet\_protocols = all  
inet\_interfaces = all  
smtp\_address\_preference = ipv4  
smtpd\_banner = ESMTP  
biff = no  
append\_dot\_mydomain = no  
readme\_directory = no  
virtual\_transport = lmtp:unix:private/dovecot-lmtp  
smtpd\_sasl\_type = dovecot  
smtpd\_sasl\_path = private/auth  
smtpd\_sasl\_auth\_enable = yes  
virtual\_mailbox\_domains = mysql:/etc/postfix/mysql\_mailbox\_domains.cf  
virtual\_mailbox\_maps = mysql:/etc/postfix/mysql\_mailbox\_maps.cf  
virtual\_alias\_maps = mysql:/etc/postfix/mysql\_alias\_maps.cf  
smtpd\_sender\_login\_maps = mysql:/etc/postfix/mysql\_mailbox\_maps.cf, mysql:/etc/postfix/mysql\_alias\_maps.cf  
disable\_vrfy\_command = yes  
strict\_rfc821\_envelopes = yes  
smtpd\_sender\_restrictions = reject\_non\_fqdn\_sender, reject\_unknown\_sender\_domain, reject\_sender\_login\_mismatch  
smtpd\_recipient\_restrictions = reject\_non\_fqdn\_recipient, reject\_unknown\_recipient\_domain, permit\_sasl\_authenticated, reject\_unauth\_destination, check\_policy\_service unix:private/policyd-spf  
virtual\_uid\_maps = static:2000  
virtual\_gid\_maps = static:2000  
message\_size\_limit = 102400000  
smtpd\_tls\_security\_level = may  
smtp\_tls\_security\_level = may  
smtpd\_tls\_cert\_file=/etc/pki/tls/certs/cert.pem # mail.example.com 证书文件位置，需要修改  
smtpd\_tls\_key\_file=/etc/pki/tls/private/key.pem # mail.example.com 证书私钥文件位置，需要修改  
smtpd\_tls\_session\_cache\_database = btree:\${data\_directory}/smtpd\_scache  
smtp\_tls\_session\_cache\_database = btree:\${data\_directory}/smtp\_scache  
smtpd\_tls\_protocols = TLSv1.2, TLSv1.1, !TLSv1, !SSLv2, !SSLv3  
smtp\_tls\_protocols = TLSv1.2, TLSv1.1, !TLSv1, !SSLv2, !SSLv3  
smtp\_tls\_ciphers = high  
smtpd\_tls\_ciphers = high  
smtpd\_tls\_mandatory\_protocols = TLSv1.2, TLSv1.1, !TLSv1, !SSLv2, !SSLv3  
smtp\_tls\_mandatory\_protocols = TLSv1.2, TLSv1.1, !TLSv1, !SSLv2, !SSLv3  
smtp\_tls\_mandatory\_ciphers = high  
smtpd\_tls\_mandatory\_ciphers = high  
smtpd\_tls\_mandatory\_exclude\_ciphers = MD5, DES, ADH, RC4, PSD, SRP, 3DES, eNULL, aNULL  
smtpd\_tls\_exclude\_ciphers = MD5, DES, ADH, RC4, PSD, SRP, 3DES, eNULL, aNULL  
smtp\_tls\_mandatory\_exclude\_ciphers = MD5, DES, ADH, RC4, PSD, SRP, 3DES, eNULL, aNULL  
smtp\_tls\_exclude\_ciphers = MD5, DES, ADH, RC4, PSD, SRP, 3DES, eNULL, aNULL  
tls\_preempt\_cipherlist = yes  
smtpd\_tls\_received\_header = yes  
policyd-spf\_time\_limit = 3600  
EOF

* 1. Change the value of master.cf:

cat > /etc/postfix/master.cf << EOF

smtp inet n - n - - smtpd  
submission inet n - n - - smtpd  
 -o smtpd\_tls\_security\_level=encrypt  
smtps inet n - n - - smtpd  
 -o smtpd\_tls\_wrappermode=yes  
pickup unix n - n 60 1 pickup  
cleanup unix n - n - 0 cleanup  
qmgr unix n - n 300 1 qmgr  
tlsmgr unix - - n 1000? 1 tlsmgr  
rewrite unix - - n - - trivial-rewrite  
bounce unix - - n - 0 bounce  
defer unix - - n - 0 bounce  
trace unix - - n - 0 bounce  
verify unix - - n - 1 verify  
flush unix n - n 1000? 0 flush  
proxymap unix - - n - - proxymap  
proxywrite unix - - n - 1 proxymap  
smtp unix - - n - - smtp  
relay unix - - n - - smtp  
 -o smtp\_helo\_timeout=120 -o smtp\_connect\_timeout=120  
showq unix n - n - - showq  
error unix - - n - - error  
retry unix - - n - - error  
discard unix - - n - - discard  
local unix - n n - - local  
virtual unix - n n - - virtual  
lmtp unix - - n - - lmtp  
anvil unix - - n - 1 anvil  
scache unix - - n - 1 scache  
policyd-spf unix - n n - 0 spawn  
 user=mail\_sys argv=/usr/libexec/postfix/policyd-spf  
EOF

* 1. Config Dovecot
     1. Bake up the file:

cp -r /etc/dovecot /etc/dovecot.bak

* 1. cat > /etc/dovecot/dovecot.conf << EOF

protocols = imap lmtp  
dict {  
}  
!include conf.d/\*.conf  
!include\_try local.conf  
EOF

* 1. cat > /etc/dovecot/conf.d/10-mail.conf << EOF

namespace inbox {  
 inbox = yes  
}  
first\_valid\_uid = 1000  
mbox\_write\_locks = fcntl  
mail\_location = maildir:/var/spool/mail/%d/%n  
mail\_privileged\_group = mail  
EOF

* 1. cat > /etc/dovecot/conf.d/15-mailboxes.conf << EOF

namespace inbox {  
 mailbox Drafts {  
 auto = create  
 special\_use = \Drafts  
 }  
 mailbox Trash {  
 auto = create  
 special\_use = \Trash  
 }  
 mailbox Sent {  
 auto = create  
 special\_use = \Sent  
 }  
}  
EOF

* 1. cat > /etc/dovecot/conf.d/10-auth.conf << EOF

auth\_mechanisms = plain login

!include auth-sql.conf.ext

EOF

* 1. cat > /etc/dovecot/conf.d/auth-sql.conf.ext << EOF

passdb {

driver = sql

args = /etc/dovecot/dovecot-sql.conf.ext

}

userdb {

driver = static

args = uid=mail\_sys gid=mail\_sys home=/var/spool/mail/%d/%n

}

EOF

* 1. cat > /etc/dovecot/dovecot-sql.conf.ext << EOF

driver = mysql

connect = host=localhost dbname=mail\_sys user=mail\_sys password=mail\_sys

default\_pass\_scheme = SHA512-CRYPT

password\_query = SELECT email as user, password FROM users WHERE email='%u';

EOF

* 1. cat > /etc/dovecot/conf.d/10-ssl.conf << EOF

ssl = required  
ssl\_cert = </etc/pki/tls/certs/cert.pem # mail.example.com 证书文件位置，需要修改  
ssl\_key = </etc/pki/tls/private/key.pem # mail.example.com 证书私钥文件位置，需要修改  
ssl\_protocols = TLSv1.2 TLSv1.1 !TLSv1 !SSLv2 !SSLv3  
ssl\_cipher\_list = ALL:!MD5:!DES:!ADH:!RC4:!PSD:!SRP:!3DES:!eNULL:!aNULL  
EOF

* 1. cat > /etc/dovecot/conf.d/10-master.conf << EOF

service imap-login {  
 inet\_listener imap {  
 port = 143  
 }  
 inet\_listener imaps {  
 port = 993  
 ssl = yes  
 }  
}

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

service imap {

}

service auth {  
 unix\_listener /var/spool/postfix/private/auth {  
 mode = 0666  
 user = postfix  
 group = postfix  
 }

unix\_listener auth-userdb {  
 mode = 0600  
 user = mail\_sys  
 }  
 user = dovecot  
}

service auth-worker {  
 user = mail\_sys  
}  
EOF

* 1. cat > /etc/dovecot/conf.d/15-lda.conf << EOF

postmaster\_address = postmaster@%d

protocol lda {  
}  
EOF

* 1. Config OpenDKIM(and record the domain name)