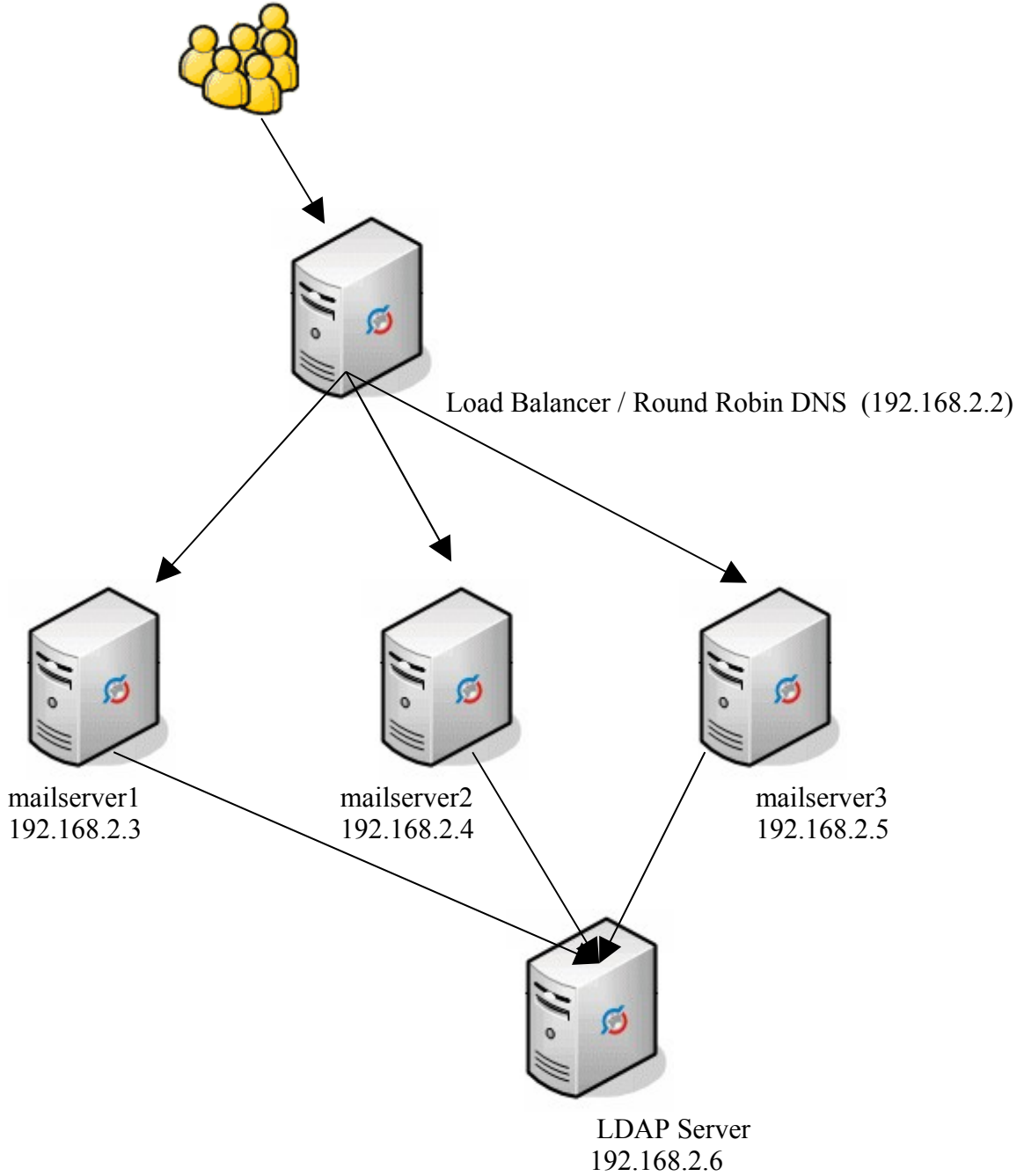


QMAIL-LDAP VE CLUSTER



Qmail kurulumlarında gördüğümüz gibi genellikle kullanıcı bilgileri cdb dosyasında ya da mysql veritabanında tutulur. Qmail, vpopmail (cdb-mysql) yapısı genellikle fazlasıyla işimizi görecektir ancak bazı karmaşık durumlarda yeterli değildir. Bu durumların başında cluster uygulamaları geliyor.

Qmail Ldap ve Cluster

Qmail mail sunucusunun kullanıcı bilgilerini ldap serverdan aldığı yapıdır. Qmail kurulumu sırasında ldap yaması uygulanır ve kullanıcı bilgileri ldap serverda tutulur. Qmail ldap ile ilgili cluster senaryosu eşliğinde gerekli paketlerin kurulumu ve yapılandırılmasını inceleyelim.

domain : **deneme.com**

Load Balancer / Round Robin DNS (**192.168.2.2**)

Ldap Server : **ldap.deneme.com (192.168.2.6)**

mail sunucu 1 : **mail1.deneme.com (192.168.2.3)**

mail sunucu 2 : **mail2.deneme.com (192.168.2.4)**

mail sunucu 3 : **mail3.deneme.com (192.168.2.5)**

Yapımız bu şekilde iken ilk olarak load balancer olarak hangi sistemin kurulacağına karar vermemiz gerekir. Bunu iki türlü yapabiliriz. Birincisi Round Robin DNS load balancing yöntemi diğeri ise herhangi bir Load Balancing Cluster yazılımı. Bu yazılım keepalived olabilir, www.keepalived.org adresinden Failover ve Load Balancing cluster uygulamalarını inceleyebilirsiniz. Kullanımı ve yapılandırması oldukça kolay ve zevkli bir program.

Biz Round-robin DNS tekniği ile yük dengelemesi yapacağız .

Örnek DNS Kaydı:

IN	MX	10	mail1.deneme.com.
IN	MX	10	mail2.deneme.com.
IN	MX	10	mail3.deneme.com.
mail1	IN	A	192.168.2.3
mail2	IN	A	192.168.2.4
mail3	IN	A	192.168.2.5
ldap	IN	A	192.168.2.6

Dns kayıtlarından da anlaşılacağı gibi 3 mail sunucumuz için A kaydı açıyoruz ve bu üç kayıt için de aynı öncelik değerine (10) sahip MX kayıtları yazıyoruz. deneme.com domainine gelen bir posta dns sorgusundan sonra round robin tekniğine göre 3 sunucudan birine iletilecektir.

ahmet@deneme.com adresine gönderilen bir e-posta yukarıda belirttiğimiz DNS sorgusundan sonra arkada bulunan bir mail sunucuya iletilir(örn: mail2.deneme.com).

Bu sunucu Ldap servera bağlanarak ahmet@deneme.com için bilgileri sorgular ve bu adresin hangi mail sunucuda, hangi klasörde depolandığını öğrenir (örn: mail3.deneme.com /mailkuutusu/ahmet/).

mail2.deneme.com sunucusu ahmet@deneme.com kaydının mail3.deneme.com sunucusunda olduğunu LDAP sunucudan öğrenir ve bilgileri o sunucuya iletir.

mail3.deneme.com a gelen talep alınır, işlenir ve cevap kullanıcıya geri gönderilir.

OPENLDAP KURULUMU VE YAPILANDIRILMASI

Ldap sunucu için açık kaynak kodlu OpenLdap programını kullanacağız işletim sistemi olarak FreeBSD 7.2.

Openldap 2.4 Kurulumu

```
# cd /usr/ports/net/openldap24-server
# make install clean
```

```
/etc/rc.conf dosyasına slapd_enable="YES"
# /usr/local/etc/rc.d/slapd start
```

/usr/local/etc/openldap/slapd.conf

```
include /usr/local/etc/openldap/schema/corba.schema
include /usr/local/etc/openldap/schema/core.schema
include /usr/local/etc/openldap/schema/cosine.schema
include /usr/local/etc/openldap/schema/inetorgperson.schema
include /usr/local/etc/openldap/schema/nis.schema
include /usr/local/etc/openldap/schema/openldap.schema

# qmail ldap için qmail schema eklenmelidir. qmail.schema qmailldap kurulu sistemde
/var/qmail/doc altında bulunur.
include /usr/local/etc/openldap/schema/qmail.schema

pidfile          /var/run/openldap/slapd.pid
argsfile /var/run/openldap/slapd.args
modulepath       /usr/local/libexec/openldap
moduleload       back_bdb

#erisim duzeyini tanimlayalim
access to *
    by self write
    by users read
    by anonymous auth

database         bdb

suffix dc=deneme,dc=com
rootdn cn=yonetici,dc=deneme,dc=com
rootpw deneme

directory       /var/db/openldap-data
index objectClass eq
```

deneme.com için root ldap kaydı (/root/ilk.ldif dosyası)

```
dn: dc=deneme,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
dc: deneme
o: deneme
```

Ldap kaydını Openldap servera ekleyelim

```
# ldapadd -x -D "cn=yonetici,dc=deneme,dc=com" -w deneme -f
/root/ilk.ldif
```

Qmail kullanıcılarının tutulacağı users Organisational Unit'ini oluşturalım

```
dn: ou=users,dc=deneme,dc=com
objectClass: organizationalUnit
objectClass: top
ou: users
```

```
# ldapadd -x -D "cn=yonetici,dc=deneme,dc=com" -w deneme -f
/root/users.ldif
```

qmail için ilk kullanıcıyı girelim (/root/qmailuser.ldif)

```
dn: cn=Postmaster,ou=users,dc=deneme,dc=com
cn: Postmaster
ou: users
sn: Postmaster
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: qmailUser
mailQuotaSize: 0
uid: postmaster
accountStatus: active
mail: postmaster@deneme.com
mailHost: mail1.deneme.com
mailMessageStore: /home/postmaster
userPassword: post
mailQuotaCount: 100000000
```

```
# ldapadd -x -D "cn=yonetici,dc=deneme,dc=com" -w deneme -f
/root/qmailuser.ldif
```

cn=Postmaster,ou=users,dc=deneme,dc=com : deneme.com için qmail ldap şeması kullanılarak users organisational unit içerisinde postmaster kullanıcısı eklendi.

Ldap kayıtlarını ldif dosyası şeklinde girmek zor bir iş ve zaman kaybına neden oluyor. Phpldapadmin ile bu işi kolaylıkla yapabilirsiniz.

Phpldapadmin Kurulumu

```
ldap # cd /usr/ports/net/phpldapadmin
ldap # make install clean
```

QMAIL LDAP KURULUMU

```
mail1# cd /usr/ports/mail/qmail-ldap/
mail1# make install clean
```

```
/etc/rc.conf dosyasına svscan_enable="YES"

/usr/local/etc/rc.d/svscan.sh dosyasındaki /var/service /service olarak değiştirelim.

# /usr/local/etc/rc.d/svscan.sh start
```

djbdns kurulumu (qmail-conf için gerekli)

```
# mkdir /usr/local/prog
# cd /usr/local/prog
# fetch http://cr.yip.to/djbdns/djbdns-1.05.tar.gz
# tar -zxvf djbdns-1.05.tar.gz

# cd djbdns-1.05
# make setup check
```

qmail-conf kurulumu (qmail yapılandırma scriptleri için)

```
# cd /usr/local/prog
# fetch http://www.din.or.jp/~ushijima/qmail-conf/qmail-conf-0.60.tar.gz
# tar xvfz qmail-conf-0.60.tar.gz
# cd qmail-conf-0.60

# make -f Makefile.ini djbdns=../djbdns-1.05/
# make setup check
```

/var/qmail/control/ dosyaları (mail1.deneme.com)

```
/var/qmail/control/me
mail1.deneme.com
```

```
/var/qmail/control/ldapserver
192.168.2.6
```

```
/var/qmail/control/ldapbasedn
ou=users ,dc=deneme ,dc=com
```

```
/var/qmail/control/ldappassword
deneme
```

```
/var/qmail/control/ldaplogin
cn=yonetici ,dc=deneme ,dc=com
```

```
>/var/qmail/control/ldapobjectclass
qmailUser
```

```
/var/qmail/control/ldaplocaldelivery
0
```

```
/var/qmail/control/ldapcluster
1
```

```
/var/qmail/control/ldapmailhost
mail1.deneme.com
mail2.deneme.com
mail3.deneme.com
```

```
/var/qmail/control/defaultquotasize
10000000
```

```
/var/qmail/control/defaultquotacount
1000
```

```
/var/qmail/control/quotawarning
Kota sınırını aştınız.
```

```
/var/qmail/control/ldapdefaultdotmode
ldaponly
```

```
/var/qmail/control/ldapmessagestore (postalardan saklanacağı klasör)
/mailkutusu/
```

```
/var/qmail/control/ldapuid (qmail kullanıcısının id değeri)
82
```

```
/var/qmail/control/ldapgid (qmail grubunun id değeri)
82
```

```
/var/qmail/control/ldaptimeout  
30
```

```
/var/qmail/control/defaultdelivery  
./Maildir/
```

```
/var/qmail/control/locals  
deneme.com  
sirket.com
```

```
/var/qmail/control/rcpthosts  
deneme.com  
sirket.com
```

```
/var/qmail/control/defaultdomain  
deneme.com
```

```
/var/qmail/control/rbllist  
zen.spamhaus.org
```

```
/var/qmail/control/dirmaker  
/var/qmail/bin/dirmaker.sh
```

Dirmaker

/var/qmail/bin/dirmaker.sh (otomatik /Maildir oluşturmak için)

```
#!/bin/sh  
/bin/mkdir -m 700 -p $1/Maildir  
/bin/mkdir -m 700 -p $1/Maildir/new  
/bin/mkdir -m 700 -p $1/Maildir/cur  
/bin/mkdir -m 700 -p $1/Maildir/tmp
```

```
# chmod +x /var/qmail/bin/dirmaker.sh
```

MailStore Dizini (epostaların saklanacağı dizin ve yetkileri)

```
# mkdir /mailkutusu  
# chown qmaild:qmail /mailkutusu
```

/var/qmail/rc

```
#!/bin/sh
exec env - PATH="/usr/local/bin:/var/qmail/bin:/bin" \
    qmail-start ./Maildir/
```

```
#chmod 755 /var/qmail/rc
```

qmail-delivery

```
#!/var/qmail/bin/qmail-delivery-conf qmail /var/qmail/service/qmail
#ln -s /var/qmail/service/qmail /service
```

qmail-smtpd

```
#!/var/qmail/bin/qmail-smtpd-conf qmaild qmail /var/qmail/service/smtpd
#ln -s /var/qmail/service/smtpd /service/smtpd
```

Hafıza Limiti

```
#echo "80000000" > /var/qmail/service/smtpd/env/DATALIMIT
```

/service/smtpd/tcp (Relay izni verilen ip adresleri)

```
127.:allow,RELAYCLIENT=""
192.168.2.:allow,RELAYCLIENT=""
:allow
```

tcp dosyasını aktiveleştirelim.

```
#cd /service/smtpd
#make
```

gelişmiş log seviyesi (3)

```
#echo "3"> /service/smtpd/env/LOGLEVEL
```

qmail pop3d

```
#!/var/qmail/bin/qmail-pop3d-conf /var/qmail/bin/auth_pop qmail1  
/var/qmail/service/pop3d  
  
#ln -s /var/qmail/service/pop3d /service
```

/var/qmail/service/pop3d/tcp(pop3 erişimi için sınırlama koymadık. Default değeri :deny)

```
:allow
```

```
# cd /var/qmail/service/pop3d  
# make  
  
# echo "3"> /service/pop3d/env/POP3_LOGLEVEL
```

qmail-qmqpd (cluster üyeleri arasında iletişim için)

```
# /var/qmail/bin/qmail-qmqpd-conf qmaild qmail1 /var/qmail/service/qmqpd  
# ln -s /var/qmail/service/qmqpd /service/qmqpd
```

/service/qmqpd/tcp (cluster üyelerinin ip adresleri :deny satırını silmeyiniz aksi takdirde mail sunucusu relay'a açık olabilir)

```
192.168.2.3:allow  
192.168.2.4:allow  
192.168.2.5:allow  
:deny
```

```
# cd /service/qmqpd/  
# make
```

Courier-imap

Sunucumuzu imap destekli kurmaya ihtiyaç duyabiliriz. Bu ihtiyaçların başında bazı webmail yazılımlarını kullanmak var. FreeBSD port ağacından courier-imap yazılımını kurdum ve fakat bazı sorunlarla karşılaştım. Bu nedenle aşağıdaki adımları uygularsanız bir sorun yaşamazsınız.

İlk olarak courier-imap yazılımını indirelim

```
fetch http://200.4.48.8/pub/mail-tools/qmail/imap/courier-imap-3.0.8.tar.bz2
```

root olmayan bir kullanıcı ile oturumu açalım

```
# su ahmet
$ ./configure --without-authdaemon
$ make
$ make check
```

derleme işlemini yaptıktan sonra kurulum için root kullanıcı hakkına ihtiyacımız var.

```
$ su -
# gmake install
# gmake install-configure
```

Şimdi can alıcı noktaya geldik.

Courier-imap authentication için /var/qmail/bin/auth_imap kullanır.

/usr/lib/courier-imap/libexec/imapd.rc dosyasındaki LIBAUTHMODULE kısmını aşağıdaki gibi yapalım

```
LIBAUTHMODULES="/var/qmail/bin/auth_imap"
```

Imap sunucumuzu başlatalım ve test edelim

```
#!/usr/lib/courier-imap/libexec/imapd.rc start
# telnet 127.0.0.1 143
.....
a1 login postmaster@deneme.com postit
login ok :)
```

Simscan , Spamassassin ve Clamav

qmail ldap sunucusu spam ve virus korumasını simscan ile verebiliriz.
Bunun için qmail-ldap Qmailqueue desteği ile derlenmelidir.

Kurulum

```
#cd /usr/ports/mail/p5-MailSpamassassin
#make install clean

#cd /usr/ports/security/clamav
#make install clean

#cd /usr/ports/mail/simscan
#make install clean
```

Simscan, make config sırasında **clamav, ripmime, spamd, user, domain, passthru** seçenekleri ile kurulmuştur.

simscan izinleri

```
#chgrp clamav /var/qmail/simscan
#chmod g+s /var/qmail/simscan
```

/var/qmail/control/simcontrol

```
:clam=yes,spam=yes,spam_passthru=yes
```

simcontrol aktivasyonu için

```
#!/var/qmail/bin/simscanmk
```

Simscan Aktivasyonu

/service/smtpd/tcp:

```
127.:allow,RELAYCLIENT=""
:allow,QMAILQUEUE="/var/qmail/bin/simscan"
```

```
# cd /service/smtpd
# make
```

Testler

qmail test

```
#svstat /service/qmail/  
/service/qmail/: up (pid 7126) 699 seconds  
  
#svstat /service/smtpd/  
/service/smtpd/: up (pid 7127) 725 seconds  
  
#svstat /service/pop3d/  
/service/pop3d: up (pid 7128) 732 seconds
```

Ldap test

```
#!/var/qmail/bin/qmail-ldaplookup -d 255 -m postmaster@deneme.com -p post
```

Komutunun çıktısı aşağıdakine benzer ise qmail, ldap sunucu ile sorunsuz iletişim kuruyor demektir.

```
Searching ldap for: (&(objectClass=qmailUser)(  
(mail=postmaster@deneme.com)  
(mailAlternateAddress=postmaster@deneme.com)))  
under dn: ou=users,dc=deneme,dc=com  
Found 1 entry:
```

```
dn: cn=Postmaster,ou=users,dc=deneme,dc=com
```

```
-----  
objectClass: top  
objectClass: person  
objectClass: inetOrgPerson  
objectClass: qmailUser  
mail: postmaster@deneme.com  
uid: postmaster  
accountStatus: active  
mailHost: mail1.deneme.com  
homeDirectory: /home/postmaster  
aliasEmpty: using default  
qmailDotMode: ldaponly  
qmailUID: 82  
qmailGID: 82  
mailQuotaSize: 0 (unlimited)  
....
```

simscan test

```
# echo "deneme postasi buradan gecer" > /root/simscan.txt
```

```
# env QMAILQUEUE=/var/qmail/bin/simscan SIMSCAN_DEBUG=2  
/var/qmail/bin/qmail-inject postmaster@deneme.com < /root/simscan.txt
```

```
simsan: cdb looking up
simsan: cdb for found clam=yes,spam=yes,spam_passthru=yes
simsan: pelookup clam = yes
simsan: pelookup spam = yes
simsan: pelookup spam_passthru = yes
simsan: spampassthru = yes/1
simsan: starting: work dir: /var/qmail/simsan/1241708736.758946.3647
simsan: pelookup: called with root@mail1.deneme.com
simsan: pelookup: domain is mail1.deneme.com
simsan: cdb looking up mail1.deneme.com
simsan: pelookup: local part is root
simsan: cdb looking up root@mail1.deneme.com
simsan: pelookup: called with postmaster@deneme.com
simsan: pelookup: domain is deneme.com
simsan: cdb looking up deneme.com
simsan: pelookup: local part is postmaster
simsan: cdb looking up postmaster@deneme.com
simsan: calling clamdscan
simsan: normal clamdscan return code: 0
simsan: calling spamc
simsan: calling /usr/local/bin/spamc spamc -u postmaster@deneme.com
simsan: delivering spam because spam-passthru is defined in this domain
simsan:[3646]:PASSTHRU (5.80/5.00):6.9533s:*****SPAM***** :
(null):root@mail1.deneme.com: postmaster@deneme.com
simsan: done, execing qmail-queue
simsan: qmail-queue exited 0
```

Cluster mimarisiyle kurulum yapıldıysa tüm cluster üyelerinin ldapmailhost , rcpthosts ve locals dosyaları aynı olmalıdır.

Ldap sunucudan mailhost değeri öğrenilip mail sunucuya iletim yapıldığında qmail önce me dosyasına bakar ve ldap sunucudan gelen mailhost değeri ile karşılaştırır eğer me dosyasındaki domain ile ldapdan gelen mailhost aynı ise işlemin yerel sunucuda yapılacağını anlar. me ile mailhost değeri farklı ise ldapmailhost dosyasındaki sunucularla karşılaştırma yapar ve mail hangi sunucuya aitse qmqp ile iletişimi gerçekleştirir.

Bu nedenle sunucunun tam domain adı ne ise me dosyasında aynısı olmalıdır ve ldapmailhost değerleri her üyede aynı olmalıdır.

Ldap sunucuda kullanıcı parolalarını clear text olarak kaydetmeniz durumunda outlook hata verecektir. phpldapadmin ile md5 parolalar tanımlayabilirsiniz.

mail2.deneme.com için

```
/var/qmail/control/me
```

```
mail2.deneme.com
```

```
/var/qmail/control/ldapmailhost
```

```
mail1.deneme.com
```

```
mail2.deneme.com
```

```
mail3.deneme.com
```

mail3.deneme.com için

```
/var/qmail/control/me
```

```
mail3.deneme.com
```

```
/var/qmail/control/ldapmailhost
```

```
mail1.deneme.com
```

```
mail2.deneme.com
```

```
mail3.deneme.com
```

Gelen maillerin kabulü açısından da , rcpthosts ve locals dosyaları aynı olmalıdır.

Eğer qmail-ldap cluster yapısından kurulmayacaksa

/var/qmail/control/ldapcluster değeri 0 yapılmalıdır.

/control/ldapmailhost boş olmalı

qmqpd servisinin kurulmasına gerek yoktur.

AHMET ORHAN

ahmetorhan@yahoo.com