

qmail ile üniversite mail sistemi yönetimi

Devrim Sipahi
Dokuz Eylül Üniversitesi
devrim.sipahi@deu.edu.tr

Üniversitelerde kullanılan mail sisteminin iki belirgin özelliği vardır.

1. Çok sayıda kullanıcı (örneğin 8000)

2. Yoğun kullanım

- a. Normal kullanım (Toplu mail gönderimi)
- b. İstenmeyen trafik (spam virüs)

Sistem yapısı

Solaris 8

qmail-vpopmail-mysql

Sanal kullanıcılar (vpopmail:vchkpw)

posta kutusu türü: maildir

Ekli dosya tipi kontrolü

Log analizi (isoqlog)

Alınış sayısız kontrolü

Uzunluk kontrolü

Genel ve özel duyurulara yönelik çözüm

Yerel olarak mail gönderimi bir dosya kopyalama işlemidir.

Aynı dosyayı binlerce farklı dizine kopyalamak yerine aynı dosyaya farklı dizinlerden erişimi sağlamak gerekir.

Unix sistemlerde “ln” komutu ile yapılır.

Dosya sahibinin aynı olması gerekir.

Programın çalışma mantığı

Duyuru maili sunucu üzerindeki farklı bir domaindeki adrese atılır.

(Bu adres Bcc kısmına yazılır.)

Bu adresteki .qmail dosyasına programın adı yazılır.

.qmail dosyasının gelen maili bir programa yönlendirme yeteneğinden yararlanır.

`#!/usr/local/bin/program_adi`

Bu sayede program sadece mail geldiğinde çalışır.

Programın yapısı

Önce yetkili kişilerden gelip gelmediği kontrol edilir.
cat mail | grep Received | grep from |grep IP | wc -l
Sonuç 1 ise gönderen yetkili kişidir.

Gönderilen adres mailden çıkarılır. Bu adres BCC kısmına yazıldığı için Delivered-To ile başlayan satırda gözüktür. Bu satır kırıldıktan sonra kalan kısım gecici bir dosyaya yazılır. Bu dosya, kullanıcıların postakutularına linklenir.

Kullanıcıların maildir'lerinin bulunduğu dosya bir sql promramcıği ile istenilen sıklıkta güncellenir.

Program örneği

```
#####program başlıyor #####  
#!/bin/bash  
KISI=`grep -l "IP_ADRESİ" /duyuru/Maildir/new/* | wc -l`  
echo $KISI  
if [ $KISI -eq 0 ]  
    then  
        ##### Duyuru gonderiliyorsa bekle ###  
        COUNTER=0  
        while [ -r /usr/local/vpopmail/domains/duyuru/calisiyor ];  
            do  
                echo $COUNTER  
                sleep 1  
                let COUNTER=COUNTER+1  
            done  
        ##### Artık bir önceki duyuru gonderilmistir #####
```

Program örneği

```
##### Yeni duyurunun baslatildiginin isareti #####  
echo >/usr/local/vpopmail/domains/duyuru/calisiyor
```

```
##### Duyurunun gonderildigi adres gizleniyor  
##### ve ilgili yere kopyalaniyor #####  
cat `grep -l "IP" /duyuru/Maildir/new/* | head -n 1` |grep -v \  
"Delivered-To:" > /duyuru-`date +%s`
```

```
cd /usr/local/vpopmail/domains/duyuru/  
DuyuruDosya=`ls duyuru*|head -n 1`  
echo "duyurudosya : $DuyuruDosya" ;
```

Program örneği

```
# Duyurunun gonderilecegi adresler veritabindan okunuyor #
cd /usr/local/vpopmail
while read INLINE
do
echo $n ;
echo "ln $DuyuruDosya $INLINE/Maildir/new/"

##### Duyuru dosyasi kullanicilara linkleniyor #####
ln $DuyuruDosya $INLINE/Maildir/new/
let "n += 1"
done < /usr/local/vpopmail/domains/PERSDIR

##### Gonderilen duyuru siliniyor #####
rm $DuyuruMail
```

Program örneği

```
##### Linklenen duyuru baska dizine tasiniyor #####  
mv $DuyuruDosya /usr/local/vpopmail/domains/duyurulmus/  
  
##### Duyurunun calistigini gosteren isaret siliniyor #####  
rm /usr/local/vpopmail/domains/duyuru/calisiyor  
    else  
    echo "yanlis kisi"  
    fi  
  
### program sonu #####
```

SPAM yapan adreslerin engellenmesi

3 yöntemle yapılabilmektedir:

Firewall, tcpserver programı ve badmailfrom dosyası

1. Firewall spam yapan IP ve IP gruplarının mail sunucuların 25. portuna bağlanmasını engelleyerek sistemin yükünü azaltır.
2. tcp.smtp dosyasına `IP_ADRESİ:deny,RELAYCLIENT=""` satırı ekleyerek o ip adresinin mail göndermesi engellenir.
3. `/var/qmail/control/badmailfrom` dosyasına mail adresi veya domain yazılarak o adresin veya domainin mail göndermesi engellenir.

Mail büyüklüğünün sınırlandırılması

`/var/qmail/control/databytes`

dosyasına en fazla mail büyüklüğü yazılarak daha büyük mail gönderilmesi engellenir.

İstisnalar için `tcp.smtp` dosyasında IP adresinin yanına

`IP:allow,RELAYCLIENT="",DATABYTES="1000000"`
yazılarak o ip için sınır değiştirilebilir.

`# qmail cdb`
komutunu unutmamak gerekir.

Virus Kontrolü

Bunun en basit yolu ekli dosya tiplerine bakılarak karar verilmesidir.

Dosya tipi virüslü dosyaların kullandığı dosya tipine benziyorsa reddedilir.

Bu sistemin yan etkisi virüslü olmayan dosyalarında engellenmesidir.

Bunun çözümü de göndericinin veya alıcının bilgilendirilmesidir.

Bu kontrol bir kabuk programcığı veya C ile derlenmiş program ile yapılabilir.

C ile derlenmiş program daha hızlı çalışır.

Dosya tipi kontrolü programı

```
#!/bin/sh
printmsg () {
    echo "--- dosya tipi virüslü dosyalara benzediğinden engellenmiştir.
dosya tipi =$ATTYPE"
}
checktype () {
    case $ATTYPE in
        VBS | ZIP | PIF | SCR | JSE | EXE | COM | BAT | SHS )
            printmsg $ATTYPE
            exit 100;;
# gönderene cevap vermemesi istenirse 100 yerine 99 yazılır.
        *)
            ;;
    esac
}
ATTACHTYPE=`grep "name=" | awk 'BEGIN {FS="."}; {print toupper
($NF)}' | cut -c -3`
for ATTTYPE in $ATTACHTYPE
do
    checktype $ATTTYPE
done
exit 0
```

Alıcı sayısını kısıtlamak

Bunun için “tarpit” yaması uygulanır.

<http://www.palomine.net/qmail/tarpit.patch>

adresindeki yama qmail-smtpd.c dosyasına uygulanır.

Bu yama programın akışını değiştirmez.

İ

ki kontrol dosyasında yazılı iki değişken kullanılır.

Tarpit sayısı ---> control/tarpitcount

Tarpit süresi ---> control/tarpitdelay

Bir mesajdaki alıcı sayısı (To,Cc, Bcc toplanımı) tarpit sayısına ulaştığında tarpit süresi kadar bekletilir.

Böylelikle toplu maillerde istemci program zaman aşımına uğrar.

Kuyruktaki belirli maillerin silinmesi

Kuyrukta içinde \$1 de yazılı sözcüğü bulan komut

```
find /var/qmail/queue -exec grep -l "$1" {} \; -print|uniq
```

Bulunan maili silmek için

```
find /var/qmail/queue -exec grep -l "$1" {} \; -print|uniq|xargs rm
```

Bozulan kuruk yapısını düzeltmek için (Tek satır)

```
qmail queue|grep trouble|awk -F" " '{ print $4}'|awk 'FS="#"  
{print $2}'|awk 'FS=":" {print $1}'|nl -s"find /var/qmail/queue/  
-name "|cut -c7-80 | sh |xargs rm
```

Kaynaklar

1. <http://cr.yip.to> qmail resmi sitesi
2. <http://www.qmail.org>
3. <http://www.lifewithqmail.org/lwq.html>

Mail listesinde aramayapmak için

4. <http://www-archive.ornl.gov:8000/>

Türkçe kurulum belgesi

5. <http://www.enderunix.org/documents/qmail.html>

İngilizce Kurulum belgesi

6. <http://www.flounder.net/qmail/qmail-howto.html>

Tarpit yaması

7. <http://www.palomine.net/qmail/tarpit.patch>

Bu belgenin adresi:

8. <http://izmirunix.deu.edu.tr/seminer/deumail.sxi>