فصل پنجم

پیکربندی پیشرفته

این فصل به مسائلی همچون فیلتر کردن، نرم‌افزارهای کاربردی کاربر،qmail-users، Domainkey، DKIM، پیکربندی DNS، انواع رله کردن، SMTP AUTH، بسته‌های مختلف Courier، دسترسی از راه دور به صندوق‌های پستی کاربران از طریق پروتکل‌های IMAP و POP3، امنیت از دیدگاه پیکربندی، MailScanner، SpamAssassin، ClamAV و دامنه‌های مجازی می‌پردازد.

۵-۱ فیلترکردن ایمیل

قبل از qmail ، پشتیبانی MTA برای فضاهای نشانی مدیریت شده توسط کاربر، غیرمعمول بود، بنابراین بیشتر این تقسیم‌بندی‌ها با استفاده از فیلتر MDA هایی مانند Procmail و یا Maildrop انجام می‌شد. این MDA ها به کاربر اجازه می‌دهند تطبیق الگو را در برابر پیام‌های دریافتی انجام دهد و آنها را به صندوق‌های پستی مشخص ، هدایت کند.

خوشبختانه، فضای نشانی مدیریت شده توسط کاربر qmail، فیلتر کردن را تا حد زیادی منسوخ کرده است. به جای استفاده از یک تک آدرس و یک تک صندوق پستی، کاربران می‌توانند آدرس‌های جدید را هنگام نیاز برای اهداف جدید خود ایجاد کنند و همچنین پیام‌ها را به صندوق‌های پستی مختلف ارسال کنند.

procmail ۵-۱-۱

Procmail یک MDA محبوب می‌باشد. وظیفه MDA این است که یک پیام را از MTA برای یک کاربر یا صندوق پستی خاص، دریافت کند و پیام را با توجه به خواسته کاربر، به مقصد مناسب هدایت کند. Procmail می‌تواند برای فیلتر کردن پیام‌ها بر اساس محتوا از زمینه‌های مختلف سرآیند و یا بدنه پیام، مورد استفاده قرار گیرد. به عنوان مثال، می‌توان پیام‌ها را از یک فرد خاص و یک صندوق پستی، برای فقط آن شخص هدایت کرد.

برای اجرای Procmail با qmail، ترفندهایی وجود دارد که باید استفاده شوند.

maildrop ۲-۱-۵

Maildrop یک MDA فیلترینگ، با قابلیت‌های مشابه Procmail می‌باشد. Maildrop برای کار با qmail طراحی شده است، بنابراین preline و بسته‌بندی کدهای خروج، غیرضروری می‌باشد.

فیلتراسیون maildrop و تحویل ایمیل، توسط فایلی با نام mailfilter. تعیین می‌شود. فراخوانی maildrop، با فایل‌های qmail.، بسیار ساده و آسان می‌باشد:

|maildrop

اگر فایل /etc/maildroprc وجود داشته باشد، تحویل نامه یا دستورالعمل‌های فیلترینگ پست الکترونیکی، از آن فایل خوانده می‌شود. دستورالعمل‌های تحویل / فیلترینگ maildrop، ممکن است maildrop را به ذخیره پیام در صندوق پستی خاص، دور انداختن پیام، بازگشت پیام به فرستنده، یا به یک آدرس ایمیل متفاوت، هدایت کند.

اگر /etc/maildroprc وجود نداشته باشد و یا دستورالعمل‌های تحویل نامه به طور درست تعریف‌نشده باشند، maildrop آنگاه دستورالعمل‌های تحویل نامه را از $HOME/.mailfilter می‌خواند. اگر $HOME/.mailfilter وجود نداشته باشد و یا دستورالعمل‌های تحویل نامه، به طور درست تعریف‌نشده باشند، maildrop آنگاه پیام‌های پست الکترونیکی را در صندوق پستی پیش‌فرض، ذخیره می‌کند.

نمونه پیکربندی فایل maildroprc، در زیر آمده است:

```
import HOME
import MAILDIRQUOTA
#XBOUNCE="| bouncesaying 'Sorry, no mailbox here by that name.'"
if ( $SIZE < 262144 )
{
exception {
```

```
        xfilter "/usr/bin/spamc"
}
}
if (/^X-Spam-Status: Yes/)
{
        #cc "|/usr/bin/sa-learn --single --spam"
    to "$HOME/Maildir/.Spam/"
}
#else
#{
#       cc "|/usr/bin/sa-learn --single --ham"
#}
exception {
        include "$HOME/.mailfilter"
}
exception {
        to "$HOME/Maildir"
}
to "Maildir"
```

۵-۲ نرم‌افزارهای کاربردی کاربر

Qmail چندین ابزار کاربردی دارد که درون فایل‌های qmail. بکار می روند و برای مدیریت صندوق‌های پستی، مفید می‌باشند. در ادامه برخی از این ابزارها معرفی می‌شوند:

bouncesaying ۵-۲-۱

دستور bouncesaying یک پیغام خطا و فرمان اختیاری را می‌پذیرد تا آن را اجرا کند. اگر یک دستور، ارائه شده باشد، آن را با پیام فعلی، در ورودی استاندارد اجرا می‌کند. اگر دستور، با یک کد موفق (صفر) خارج شود، یا دستوری ارائه نشده باشد، bouncesaying پیغام خطا را چاپ کرده و با کد ۱۰۰ (خطای سخت) خارج می‌شود. در نهایت باعث می‌شود که یک پیام واگشت تولید شده و پردازش فایل qmail. متوقف شود.

اگر دستور با کد ۱۱۱ (خطای نرم) خارج شود، bouncesaying نیز با کد ۱۱۱ خارج می‌شود و تحویل به زمانی دیگر معوق خواهد شد. اگر دستور، با هر کد دیگری خارج شود، bouncesaying با کد ۰ (صفر)، بدون چاپ هیچ پیغام خطایی، خارج می‌شود.

نحوه استفاده از bouncesaying در زیر ارائه شده است:

bouncesaying *error-message [command]*

|bouncesaying "This mailbox has been deactivated."

پیام bounce تولیدشده، به عنوان یک نتیجه از تحویل فایلqmail. ، شبیه خروجی زیر خواهد شد:

From MAILER-DAEMON Sun Apr 22 17:55:27 2001

Date: 22 Apr 2001 17:55:27 -0000

From: MAILER-DAEMON@sparge.example.com

To: debbie@example.net

Subject: failure notice

Hi. This is the qmail-send program at sparge.example.com.

I'm afraid I wasn't able to deliver your message to the following addresses.

This is a permanent error; I've given up. Sorry it didn't work out.

<bounce@sparge.example.com>:

This address has been deactivated.

—- Below this line is a copy of the message.

Return-Path: <debbie@example.net>

Received: (qmail 6863 invoked by uid 500); 22 Apr 2001 17:55:27 -0000

Message-ID: <20010422175527.6862.qmail@example.net>

Date: Sun, 22 Apr 2001 13:55:27 -0400

From: debbie@example.net

To: bounce@sparge.example.com

برای واگشت کردن پیام‌هایی که شامل عبارت Subject: MAKE MONEY FAST هستند و تحویل دیگر پیام‌ها به $HOME/Maildir، از bouncesaying زیر استفاده می‌کنیم:

|bouncesaying "Go away." grep "^Subject: MAKE MONEY FAST"

./Maildir/

condredirect ۲-۲-۵

دستور condredirect، یک آدرس ایمیل و فرمان را می‌پذیرد تا آن را اجرا کند. دستور با پیام فعلی، در ورودی استاندارد اجرا می‌شود. اگر دستور با یک کد موفق (صفر) خارج شود، condredirect پیام را به آدرس ارائه‌شده، هدایت می‌کند و با کد ۹۹ خارج می‌شود. در نهایت، پردازش فایل qmail. متوقف می‌شود.

اگر دستور با کد ۱۱۱ (خطای نرم) خارج شود، condredirect نیز با کد ۱۱۱ خارج می‌شود و تحویل، به زمانی دیگر معوق خواهد شد. اگر دستور، با هر کد دیگری خارج شود یا خارج نشود، bouncesaying با کد ۰ (صفر)، بدون هدایت پیام خارج می‌شود.

نحوه استفاده از condredirect در زیر ارائه شده است:

condredirect *address command*

برای هدایت کردن پیام‌هایی که شامل عبارت Project X هستند به project-x@example.com و تحویل دیگر پیام‌ها، به $HOME/Maildir از condredirect زیر، استفاده می‌کنیم:

[hossein@linuxcent ~]$ cat .qmail-project

|condredirect project-x@example.com grep -i "project x"

./Maildir/

datemail ۳-۲-۵

datemail یک پوشش اسکریپت پوسته ساده، در اطراف فرمان sendmail از qmail می‌باشد. datemail از predate استفاده می‌کند تا یک فیلد سرآیند تاریخ در منطقه به وقت محلی وارد کند. این مسئله وقتی مفید است که تزریق پیام از طریق sendmail با MUA، یک تاریخ درست را شامل نمی‌شود. Qmail-inject می‌تواند تاریخ را به پیام‌ها اضافه کند، اما این کار را با استفاده از زمان گرینویچ (GMT) به جای منطقه به وقت محلی، انجام می‌دهد که می‌تواند گیج کننده باشد. به عنوان مثال خروجی دو دستور زیر را باهم مقایسه کنید:

[root@linuxcent ~]# echo to: hossein | /var/qmail/bin/sendmail –t

[hossein@linuxcent cur]$ cat 1340792568.27593.linuxcent.raja.com:2,S

Return-Path: <root@linuxcent.raja.com>

Delivered-To: hossein@linuxcent.raja.com

Received: (qmail 27590 invoked by uid 0); 27 Jun 2012 10:22:48 -0000

Date: 27 Jun 2012 10:22:48 -0000

Message-ID: <20120627102248.27589.qmail@linuxcent.raja.com>

From: root@linuxcent.raja.com

to: hossein@linuxcent.raja.com

[root@linuxcent ~]# echo to: hossein | /var/qmail/bin/datemail –t

[hossein@linuxcent new]$ ls

1340792788.27804.linuxcent.raja.com

[hossein@linuxcent new]$ cat 1340792788.27804.linuxcent.raja.com

Return-Path: <root@linuxcent.raja.com>

Delivered-To: hossein@linuxcent.raja.com

Received: (qmail 27801 invoked by uid 0); 27 Jun 2012 10:26:28 -0000

Message-ID: <20120627102628.27800.qmail@linuxcent.raja.com>

From: root@linuxcent.raja.com

Date: 27 Jun 2012 14:56:28 +0430

to: hossein@linuxcent.raja.com

توجه داشته باشید که عدد **0430+** درون تاریخ پیام آزمون دوم، به معنی منطقه به وقت محلی می‌باشد که چهار ساعت و نیم، جلوی GMT را نشان می‌دهد.

forward ۴-۲-۵

Forward، یک پیام در قالب ورودی استاندارد را می‌خواند و یک کپی از پیام را به هر یک از نشانی‌های جلوی دستور، هدایت می‌کند. forward سودمند است چرا که نشانی‌های مشخص‌شده را می‌توان در زمان تحویل ایجاد کرد، درحالی‌که forward در فایل‌های qmail. استاتیک می‌باشد.

لیست زیر، نحوه کار با forward را نشان می‌دهد:

forward *addresses*

|forward $LOCAL@mailhub.example.com

maildir2mbox ۵-۲-۵

maildir2mbox پیام‌های ایمیل را از maildir مشخص‌شده به MBOX مشخص‌شده، با استفاده از فایل‌های موقت مشخص‌شده منتقل می‌کند. توجه داشته باشید که سه آرگومان به maildir2mbox از طریق متغیرهای محیطی و نه آرگومان‌های خط فرمان منتقل می‌شوند.

در مثال زیر کاربر maryjane می‌خواهد پیام‌های موجود در $HOME/Maildir به $HOME/Mailbox منتقل کند:

$ **MAILDIR=~/Maildir**

$ **MAIL=~/Mailbox**

$ **MAILTMP=~/mailtemp**

$ **export MAILDIR MAIL MAILTMP**

$ **ls Mailbox**

ls: Mailbox: No such file or directory

$ **maildir2mbox**

$ **ls -l Mailbox**

-rw------- 1 maryjane maryjane 18719 Apr 22 22:45 Mailbox

$

maildirmake ۶-۲-۵

maildirmake صندوق پستی maildir خالی، در پوشه مشخص‌شده ایجاد می‌کند. maildirmake باید با کاربری اجرا شود که مالک صندوق پستی می‌باشد. در مثال زیر، کاربر Dixie می‌خواهد maildir ی درون $HOME/Maildir بسازد:

$ **maildirmake ~/Maildir**

$ **ls -ld ~/Maildir**

```
drwx------  5 dixie  dixie     4096 May  9 19:54 Maildir
$ ls -l ~/Maildir
total 12
drwx------  2 dixie  dixie     4096 May  9 19:54 cur
drwx------  2 dixie  dixie     4096 May  9 19:54 new
drwx------  2 dixie  dixie     4096 May  9 19:54 tmp
$
```

predate ۵-۲-۷

predate یک فیلد سرآیند تاریخ، به خروجی استاندارد ارسال می‌کند، استاندارد ورودی را به خروجی استاندارد کپی کرده و فرمان را اجرا می‌کند. predate برای پیاده‌سازی فرمان datemail، استفاده می‌شود.

در مثال زیر، predate با ورودی تهی اجرا می‌شود و برنامه‌ای که اجرا می‌کند cat می‌باشد که به سادگی ورودی‌اش را منعکس می‌کند(تاریخی که توسط predate تولید می‌شود).

```
[root@linuxcent bin]# /var/qmail/bin/predate  cat < /dev/null
Date: 27 Jun 2012 16:15:24 +0430
```

qmail-users مکانیسم ۵-۳

Qmail-users یک سیستم برای اختصاص آدرس به کاربران می‌باشد. به طور معمول، تحویل‌های محلی با qmail-lspawn مدیریت می‌شوند که qmail-getpw را برای تعیین اینکه آدرس به کدام کاربر تعلق دارد، مسیر خانگی کاربر کجاست، UID و GID آن کجاست، اجرا می‌کنند.

با این حال، در صورتی که فایل var/qmail/users/cdb وجود داشته باشد، qmail-lspawn تلاش می‌کند در ابتدا جزئیات تحویل را جستجو کند. فایل users/cdb پایگاه داده باینری تولیدشده از users/assign، با استفاده از دستور qmail-newu می‌باشد.

فایل assign، جدولی از تخصیصات می‌باشد. دو نوع از تخصیصات وجود دارد: ساده و الگوی عام.

۵-۳-۱ تخصیص ساده

تخصیص ساده، مشابه عبارت زیر می‌باشد:

=address:user:uid:gid:directory:dash:extension:

این بدان معنی است که پیام‌های دریافتی به آدرس به عنوان کاربر user، با uid و gid مشخص‌شده و دایرکتوری فایل qmail*dashextension*./ اجرا خواهد شد و مشخص می‌شود که چگونه پیام‌ها تحویل داده می‌شوند.

به عنوان مثال، اگر بخواهید گیرنده محلی info توسط کاربر اندی، با مشخصات زیر مدیریت شود از تخصیص ساده زیر باید استفاده کنید:

(UID=35, GID=20, directory=/home/andy , file /home/andy/.qmail-info)

=info:andy:35:20:/home/andy:-:info:

۵-۳-۲ تخصیص الگوی عام

تخصیص الگوی عام، مشابه عبارت زیر می‌باشد:

+prefix:user:uid:gid:directory:dash:prepend:

این بدان معنی است که پیام‌های دریافتی به آدرس به فرمت *prefixrest*، با کاربر user، با uid و gid مشخص‌شده و دایرکتوری فایل qmail*dashextension*./ اجرا خواهد شد و مشخص می‌شود که چگونه پیام‌ها تحویل داده می‌شوند.

به عنوان مثال اگر بخواهید پیام‌های برای کاربر andy-info توسط کاربر اندی با مشخصات زیر مدیریت شود از تخصیص الگوی عام زیر، باید استفاده کنید:

(UID=35, GID=20, directory=/home/andy , file /home/andy/.qmail-info)

+andy-:andy:35:20:/home/andy:-::

۵-۳-۳ برنامه‌های qmail-users

qmail-users دو برنامه کمک‌کننده دارد: qmail-newu و qmail-pw2u. qmail-newu فایل assign را پردازش کرده و پایگاه داده‌ای بنام CDB درون مسیر /var/qmail/users/ ایجاد می‌کند. CDB یک فایل باینری است که توسط qmail-lspawn قابل خواندن می‌باشد.

qmail-pw2u پایگاه داده کاربر سیستمی /etc/passwd/ را به تخصیصات مناسب برای assign تبدیل می‌کند.

۵-۴ پیکربندی DNS

در این قسمت، پیکربندی نمونه‌ای برای سرور DNS ارائه داده‌ایم که در ادامه می‌آید. لازم به ذکر است که در اینجا ۳ سرور مختلف DNS، وب و MTA داریم که از آدرس‌های زیر برای آنها استفاده کرده‌ایم:

- سرور DNS: x.x.x.x
- سرور وب: z.z.z.z
- سرور MTA: y.y.y.y

البته می‌توان تمامی سرورها را بر روی یک تک آدرس IP قرار داد ولی برای افزایش امنیت و کارایی، ما برای ۳ سرور مختلفمان، ۳ آدرس IP مجزا در نظر گرفته‌ایم و آنها را بر روی سیستم‌های مجزا، قرار داده‌ایم.

در ابتدا تنظیمات فایل /etc/resolv.conf/ را مشاهده می‌کنید. ما سه دامنه raja.org، raja.ir و raja.com را که هر سه بر روی یک آدرس IP قرار دارند، در این فایل تعریف کرده‌ایم.

```
[root@ns1 ~]#  vim /etc/named.conf

zone "raja.org" IN {

        type master;

        file "raja.org.zone";

        allow-update { none; };

        allow-transfer { none; };
```

```
};
zone "raja.ir" IN {
        type master;
        file "raja.ir.zone";
        allow-update { none; };
        allow-transfer { none; };
};
zone "raja.com" IN {
        type master;
        file "raja.com.zone";
        allow-update { none; };
        allow-transfer { none; };
};
include "/etc/rndc.key";
include "/etc/named.rfc1912.zones";
include "/etc/named.rfc1912.zones";
```

مطابق با هر دامنه، باید یک فایل zone در مسیر var/named/ وجود داشته باشد. تنظیمات فایل zone دامنه raja.com را در زیر مشاهده می‌کنید.

```
[root@ns1 ~]#  vim /var/named/raja.com.zone
$TTL    86400
@               IN SOA  ns1.raja.com.          netadmin.raja.com. (
                                2011010901      ; serial (d. adams)
                                2H              ; refresh
                                5M              ; retry
```

```
                        2H          ; expiry
                        1H )        ; minimum
;Nameservers
        IN NS       ns1.raja.com.
;MailServers
        IN MX  10    mx1.raja.com.
;Hosts
ns1         IN A        x.x.x.x
mailserver  IN A        y.y.y.y
mx1         IN CNAME    mailserver
imap        IN CNAME    mailserver
smtp        IN CNAME    mailserver
mail        IN A        z.z.z.z
;@          IN A        z.z.z.z
@           IN TXT      "v=spf1 mx ~all"
_domainkey  IN TXT      "o=-"
@           IN TXT      "v=spf1 mx ~all"
_domainkey  IN TXT      "o=-"
default._domainkey  IN TXT  "k=rsa;
p=CIGfMA8GCSqGSIb3DQUJKIYGFAA4GNADDBiQKBgQDAZbSzYb
e+gCGpkVJXGPcKwEan910aVYkYTGeBz7PIEw8mj3iEp3GH+iNwRObT
1CSSPuHewGVTzKEDWj9E9JxfP2M67XGB8caMXfash0i0VC3I7Qb08Q
xEwYldYWwGjit1w2ZkLnhgb5675674kUf7w4w9fc8kgh00nHx5sskzF45dl
QI567WAC;"
```

همچنین name server، باید درون فایل resolve.conf قرار بگیرد.

]root@mx1 ~]# cat /etc/resolv.conf

nameserver x.x.x.x

nameserver 8.8.8.8

nameserver 4.2.2.4

با دستور nslookup می‌توانیم درستی nameserver و تعاریف DNS را بررسی کنیم و در صورت وجود خطا، آن را رفع کنیم.

] root@linuxcent named]# nslookup

<server x.x.x.x

Default server: x.x.x.x

Address: x.x.x.x#53

<mail.raja.com

Server: x.x.x.x

Address: x.x.x.x#53

Non-authoritative answer:

Name: mail.raja.com

Address: z.z.z.z

<

نکته: اگر بخواهیم ایمیل‌های دامنه‌ای مانند mail.raja.external را داشته باشیم باید در فایل rcpthosts، این دامنه را اضافه کنیم.

]root@linuxcent control]# cat rcpthosts

linuxcent.raja.com

linuxcent.raja.external

همچنین MX loolup ها را برای تحویل ایمیل‌ها باید bypass کنیم و مسیری برای آن، درون smtproutes تعریف کنیم:

[root@linuxcent control]# cat smtproutes

linuxcent.raja.external:linuxcent.raja.com

[root@linuxcent control]#

با این کار پیام‌های به مقصد linuxcent.raja.external از طریق linuxcent.raja.com رله می‌شوند.

۵-۵ پیکربندی DomainKeys و DKIM

DomainKeys و جانشین آن، ایمیل شناسایی (DKIM)، فن آوری‌هایی می‌باشند که اجازه می‌دهند سازمان‌ها، مسئولیت یک پیام را بعهده گیرند. این امر، با امضای رمزنگاری شده یک ایمیل، با عنوان یک سازمان در مسیر به مقصد، انجام می‌شود. امضاء می‌تواند با استفاده از سیستم DNS، برای ایجاد اعتماد تأیید شده، صورت پذیرد. استفاده از سیستم domainkeys، برای کاهش ایمیل‌های spam، توسط هویت سنجی DNS، که مشخص می‌کند یک دامنه همانی است که می‌گوید، بسیار موثر است.

وصله DomainKeys، یک برنامه واحد بنام qmail-dk ایجاد می‌کند که قبل از qmail-queue فراخوانی می‌شود. این برنامه، تمامی پیام‌های ورودی را بر اساس متغیرهای DKSIGN و DKVERIFY امضاء کرده یا اعتبارسنجی می‌نماید.

برای استفاده و نصب DomainKeys و DKIM، دستورات زیر را گام به گام دنبال کنید:

کتابخانه libdomainkeys، برای امضا و بررسی امضاهای DomainKeys استفاده می‌شود. برای نصب libdomainkeys دستورات زیر را اجرا کنید:

$ wget http://downloads.sourceforge.net/domainkeys/libdomainkeys-0.69.tar.gz

$ tar -xzf libdomainkeys-0.69.tar.gz

$ cd libdomainkeys-0.69

$ make

(If you get errors during make, edit the Makefile and add -lresolv to the end of the LIBS line)

$ sudo install -m 644 libdomainkeys.a /usr/local/lib