Running Secure & Reliable Web/Mail/other Services from Home

Part-II: Setting Up A SOHO Linux Web and Email Server

About Me

- Robert Taylor (A.K.A. Robot Terror)
  Linux Admin II
  Rackspace Managed Hosting
- BS Info Sys, SCJP, RHCT
- Father of three, husband of one

Part-II: Setting Up A SOHO Linux Web and Email Server

- Choices, choices, choices
  - Distro
  - Web Server
  - MTA
  - Other Services

Choice 1: Distro

- Mainstream
  - Debian line - Ubuntu Server
  - Red Hat line - RHEL / CentOS
- Specialty
  - Devil-Linux, etc.
- Bonus choices

Choice 2: Web Server

- LAMP
  Linux Apache MySQL Perl|PHP
- JAML
  Java Apache MySQL Linux
- Proprietary stacks
  IIS, re-branded Apache (websphere, stronghold, etc.)
- Specialty
  lighttpd, mongrel, boa, thttpd

Choice 3: Mail

- Sendmail - granddady
- Postfix - sendmail-compatible but simpler
- QMail - love it / hate it
- Exim - debian standard

My Choices

- CentOS 5
- LAMP: Linux, Apache, MySQL, PHP|Perl
- Sendmail / Dovecot / Squirrelmail

Platform Setup

- Installing CentOS 5
  - Get the ISO
    http://isoredirect.centos.org/centos/5/isos/i386/
  - Boot, Click, Use
- Man, this is simple (*Caveats*)
  - selinux and RHEL5/CentOS5
  - yum, yum (A.K.A., Repo Man)

SELinux-fu

<caveat implementor!>

The following one-liners are *hacks* to quickly get past SELinux policy limits that prevent commonly used web service configurations. Using audit2allow bypasses the limitations by force. Use only when initially configuring your server within a secure environment.

- PGM='httpd'; grep $PGM /var/log/audit/audit.log | audit2allow -M $PGM && semodule -i $PGM.pp

  (NB: change 'httpd' to the name of the command violating SELinux policies)

Do you feel LUCKY?? :-)
This one-liner bypasses ALL SELinux policy restrictions logged to date.

- cat /var/log/audit/audit.log | audit2allow -M all && semodule -i all.pp

Installing Services

- Using yum
  - yum check-update
  - yum search <package>
  - yum update <existing package>
  - yum install <new package>

Web Server Setup

- Configuring Apache
  - Listen up! (Listen <port>)
  - How may I direct your call? (VirtualHost)

/etc/httpd/conf/httpd.conf

```
Listen 80
ServerAdmin webmaster@robotterror.com
ServerName home.robotterror.com
CustomLog logs/access_log combined
ServerSignature Off
NameVirtualHost *:80
<VirtualHost *:80>
  ServerName default
  DocumentRoot /var/www/html
</VirtualHost>
<VirtualHost *:80>
  ServerName riceyes.com
  ServerAlias www.riceyes.com
  ErrorLog logs/riceyes.com-error_log
  CustomLog logs/riceyes.com-access_log combined
</VirtualHost>
```

Sendmail

- /etc/mail/sendmail.mc

```
DAEMON_OPTIONS(`Port=smtp, Name=MTA')dnl
MASQUERADE_AS(`robotterror.com')dnl
FEATURE(masquerade_envelope)dnl
FEATURE(masquerade_entire_domain)dnl
# service sendmail restart
```

- /etc/mail/virtusertable

```
@riceyes.com rtaylor
#  makemap hash /etc/mail/virtusertable \
   < /etc/mail/virtusertable
# service sendmail restart
```

Squirrelmail

- Squirrelmail install steps:
  yum install squirrelmail
  yum install php-pear
  yum install php-mysql
  pear channel-update pear.php.net
  pear install DB
  service httpd restart
  /usr/share/squirrelmail/config/config.pl
- http://riceyes.com/webmail/src/configtest.php

squirrelmail, cont'd

MySQL:

```
# mysql -u root -p
create database hrt_sqm;
CREATE USER 'hrt_sqm'@'localhost' IDENTIFIED BY ‘password’;
grant all on hrt_sqm.* to 'hrt_sqm'@'localhost';
flush privileges;
 CREATE TABLE address (
     owner varchar(128) DEFAULT '' NOT NULL,
     nickname varchar(16) DEFAULT '' NOT NULL,
     firstname varchar(128) DEFAULT '' NOT NULL,
     lastname varchar(128) DEFAULT '' NOT NULL,
     email varchar(128) DEFAULT '' NOT NULL,
     label varchar(255),
     PRIMARY KEY (owner,nickname),
     KEY firstname (firstname,lastname)
   );
 CREATE TABLE userprefs (
    user varchar(128) DEFAULT '' NOT NULL,
    prefkey varchar(64) DEFAULT '' NOT NULL,
    prefval BLOB DEFAULT '' NOT NULL,
    PRIMARY KEY (user,prefkey)
  );
```

Mail Alternative

To have virtual users with virtual domains (that is, not using system accounts) there are several How-Tos available that walk one through the steps necessary to set everything up.
A future version of this presentation will incorporate this step-by-step for CentOS5. In the meantime, review these resources:

- http://www.opensourcehowto.org/how-to/mysql/mysql-users-postfixadmin-postfix-dovecot--squirrelmail-with-userprefs-stored-in-mysql.html
- http://www.howtoforge.com/virtual_users_postfix_courier_mailscanner_clamav_centos
- http://www.google.com/search?q=postfix+imap+mysql+virtual

Web Apps

- Portals
  All-in-one content management systems
- Galleries
  Image and Video galleries for family pics & more
- Blogs
  Host your own journal and spin-zone

http://OpenSourceCMS.org
Live demos of Free PHP web apps

Bonuses

- poor man's GoToMyPC.com
  - vnc
  - ssh -fY rtaylor@riceyes.com /usr/bin/startxfce4
- Other servers!
  - IIS? Sure!
  - NFS / FTP
  - ... the possibilities are endless