

Contents

- 1 Current Setup & Config of Tomfmason's Fedora Server
 - ◆ 1.1 Initial Apps removed
 - ◆ 1.2 Inital Apps Installed
 - ◆ 1.3 Configs Carried out
 - ◇ 1.3.1 Shorewall Firewall Management
 - ◇ 1.3.2 Postfix
 - ◇ 1.3.3 Mutt Mail reader
 - ◇ 1.3.4 YUM - Package Management
 - ◆ 1.4 Special Apps Installed
 - ◇ 1.4.1 phpmyadmin installed from yum
 - 1.4.1.1 phpmyadmin config
 - 1.4.1.2 fail2ban on fedora
- 2 Apache, SSL, Vhost, SVN, Trac Setup and Config
 - ◆ 2.1 Typical Vhost Config
 - ◆ 2.2 SSL Config
 - ◆ 2.3 SVN Setup and Config
 - ◇ 2.3.1 SVN Account Setup Details
- 3 Runlevels in Fedora / Centos / RPM
- 4 Misc Info

Current Setup & Config of Tomfmason's Fedora Server

A few of us over at phpfreaks are planning to organise and setup a QualityCoders group. Tom (tomfmason) has kindly loaned the use of his rented server to help the cause.

I went through his fedora server, cleaning up some bits and setting up others, trying to achieve a secure and stable platform for the QualityCoders launchpad.

Initial Apps removed

Although ISPConfig can be very useful to setup multiple domains and packages, the version installed was a Dev. version. Also, as there would only be a couple of domains hosted on the server, it was decided to remove ISPConfig. With ISPConfig removed, a key selection of packages were installed and are kept up-to-date using yum.

Initial Apps Installed

- Munin-node was installed providing monitoring of the server.
- Shorewall was installed. This also cleaned/removed the old ISPConfig firewall rules.
- vim was installed and symlinked to vi
- trac was installed. etc.

Configs Carried out

Shorewall Firewall Management

Shorewall firewall was initially installed as per: http://wiki.kartbuilding.net/index.php/Shorewall_Firewall

Shorewall keeps its firewall rules in small config files, which are symlinked into place. For example, to allow HTTP, the following was done:

```
ln -s /usr/share/shorewall/macro.Web /etc/shorewall/  
vi /etc/shorewall/rules  
#add in the following at the bottom:  
Web/ACCEPT net $FW  
/etc/init.d/shorewall restart
```

Postfix

Postfix was next to be tidied up. The main file to watch for (allowing mail to be delivered to a particular domain) is: /etc/postfix/local-host-names Other tweaks were cosmetic.

Mutt Mail reader

Anyone who as a ssh/user account on the server has an email address: user@tomfmason.net To read/send emails, ssh into tomfmason.net and type "mutt", and the mail program will open. Hitting "q" will quit the current screen in mutt, and "q" again will quit the mutt program.

Note, if you are su'ing into an account from root, you need to go "su - username".

YUM - Package Management

Although there is apt-get installed on the fedora server, it doesnt easily allow you to list currently installed packages (as far as Im aware).

All packages installed should be from yum/apt as these will recieve security updates. Anyhoo, to use yum (which I recommend):

```
yum update  
yum upgrade
```

Tomfmason_Fedora_Server_Setup

```
yum list installed
yum list installed | grep nameofpackage
yum list available | grep packagetoinstall
yum install packagename
up2date yum
yum search packagetoinstall (a verbose version of list available)
```

Special Apps Installed

phpmyadmin installed from yum

As phpmyadmin is a php web app, where there are several security updates occurring, I did not want to install it from a gzip/zip file, **as it would never get updated!!**. As a result, I added in a repository to yum which would receive updates, and from which I could install phpmyadmin. More info is at:

<http://dries.ulyssis.org/rpm/packages/phpmyadmin/info.html>

```
vi /etc/yum.repos.d/dries.repo
[dries]
name=Extra Fedora rpms dries - $releasever - $basearch
baseurl=http://ftp.belnet.be/packages/dries.ulyssis.org/fedora/linux/$releasever/$basearch/dries/RPM
includepkgs=phpmyadmin

yum update
yum install phpmyadmin
```

phpmyadmin config

phpmyadmin is only installed **once** on a server. It is NOT installed everywhere it is needed.

phpmyadmin's main files are stored in /usr/share/phpmyadmin/

To get this to work for a particular website, just use an alias inside a <VirtualHost>. E.g.:

```
Alias /phpmyadmin /usr/share/phpmyadmin/
<Location "/phpmyadmin">
    SSLRequireSSL
    AuthType Basic
    AuthName "phpmyadmin Access Login on tomfmason.net"
    AuthUserFile /var/www/www.tomfmason.net/.htpasswd
    Require valid-user
</Location>
```

An apache reload should suffice:

```
/etc/init.d/httpd reload
```

Just a last tweak, phpmyadmin needs a random password for cookies. It will complain when you go to it first saying a 'blowfish_secret' is needed. Simply:

```
vi /usr/share/shorewall/config.inc.php
#change the following, putting in a password (and not 123123 !!)
#$cfg['blowfish_secret'] = 'A123123'; /* YOU MUST FILL IN THIS FOR COOKIE AUTH! */
```

fail2ban on fedora

Similar to how phpmyadmin was installed, fail2ban is going to be installed from yum also.

```
vi /etc/yum.repos.d/dries.repo
[dries]
name=Extra Fedora rpms dries - $releasever - $basearch
baseurl=http://ftp.belnet.be/packages/dries.ulyssis.org/fedora/linux/\$releasever/\$basearch/dries/RPM
includepkgs=phpmyadmin,fail2ban

yum update
up2date yum
yum install fail2ban
```

Done. It works with SSH out of the box. The config is at: /etc/fail2ban.conf

As proftpd is currently running, and fail2ban only has configs for vsftpd, a special rule/config will have to be written over the next while. Also - the shorewall firewall currently blocks ftp :).

Apache, SSL, Vhost, SVN, Trac Setup and Config

Apache was already installed, however its VirtualHosts were all messed up with ISPConfig. The main details are here:

```
/etc/httpd/conf/httpd.conf - main apache config
/etc/httpd/conf/vhosts/    - files placed here, in the order ##-name are all virtual hosts. Look at
/etc/httpd/conf.d/*.conf  - files are placed here after yum installs them. E.g. ssl, php etc.
/etc/httpd/conf/ssl       - custom ssl folder where the self generated ssl certs are kept.
```

I cleaned out httpd.conf to its base config which it should be like. The last line of httpd.conf is:

```
Include /etc/httpd/conf/vhosts/
#and we take it from there.
```

Typical Vhost Config

Vhosts are named in numerical order. This is so, 01-default loads first, with NameVirtualHost settings etc.:

```
[root@server vhosts]# cat 01-default
ServerName server.net

NameVirtualHost *:80
NameVirtualHost *:443

<VirtualHost *:80>
    ServerAdmin ..
    ServerName localhost
    DocumentRoot /var/www/html/

    <Directory />
        Options Indexes FollowSymLinks
        AllowOverride Indexes AuthConfig Limit FileInfo
        AllowOverride None
```

Tomfmason_Fedora_Server_Setup

```
        Order allow,deny
        allow from all
    </Directory>

    # Possible values include: debug, info, notice, warn, error, crit, alert, emerg.
    LogLevel warn
    ErrorLog /var/log/httpd/error_log
    CustomLog /var/log/httpd/access_log combined
    ServerSignature On
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin ..
    ServerName server
    DocumentRoot /var/www/html/

    <Directory />
        Options Indexes FollowSymLinks
        AllowOverride Indexes AuthConfig Limit FileInfo
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>

    # Possible values include: debug, info, notice, warn, error, crit, alert, emerg.
    LogLevel warn
    ErrorLog /var/log/httpd/error_log
    CustomLog /var/log/httpd/access_log combined
    ServerSignature On
    SSLEngine On
    SSLCertificateFile /etc/httpd/conf/ssl/hostcert.pem
    SSLCertificateKeyFile /etc/httpd/conf/ssl/hostkey.pem
</VirtualHost>
```

SSL Config

In order to get these working: SSLEngine On SSLCertificateFile /etc/httpd/conf/ssl/hostcert.pem
SSLCertificateKeyFile /etc/httpd/conf/ssl/hostkey.pem

```
mkdir -p /etc/httpd/conf/ssl/
cd /etc/httpd/conf/ssl/
openssl req -x509 -days 365 -newkey rsa:1024 -keyout hostkey.pem -nodes -out hostcert.pem
```

Make sure to disable current ssl certs put in by default in /etc/httpd/conf.d/ssl.conf !!

Install mod_ssl:

```
yum install mod_ssl
```

See also: <http://security.ncsa.uiuc.edu/research/grid-howtos/usefulopenssl.php#taskgenself> and
<http://security.ncsa.uiuc.edu/research/wssec/gsihttps/gsiapache.php>

SVN Setup and Config

The setup was much the same as: [http://wiki.kartbuilding.net/index.php/Trac and SVN](http://wiki.kartbuilding.net/index.php/Trac_and_SVN)

The config is as follows:

```
[root@server vhosts]# cat 03-svn.server
<VirtualHost *:80>
    ServerAdmin root@server.net
    ServerName svn.server.net

    Redirect 301 / https://svn.server.net/

    # Possible values include: debug, info, notice, warn, error, crit, alert, emerg.
    LogLevel warn
    ErrorLog /var/log/httpd/error_log
    CustomLog /var/log/httpd/access_log combined
    ServerSignature On
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName svn.server.net

    DocumentRoot /var/www/www.server.net/svnwww

    <Location /svn/projectsteviedr>
    DAV svn
    SVNPath /var/www/www.server.net/svn/projectsteviedr
    AuthType Basic
    AuthName "Subversion Repository - Project Steviedr"
    AuthUserFile /var/www/www.server.net/.htpasswd
        <LimitExcept GET PROPFIND OPTIONS REPORT>
            Require valid-user
            SSLRequireSSL
        </LimitExcept>
    </Location>
    ScriptAlias /trac/projectsteviedr /var/www/cgi-bin/trac.cgi
    <Location "/trac/projectsteviedr">
        AllowOverride Indexes AuthConfig Limit FileInfo
        AllowOverride None
        SetEnv TRAC_ENV "/var/www/www.server.net/trac/tracprojectsteviedr"
    </Location>
    <Location "/trac/projectsteviedr/login">
        SSLRequireSSL
        AuthType Basic
        AuthName "Trac Login for Project Steviedr"
        AuthUserFile /var/www/www.server.net/.htpasswd
        Require valid-user
    </Location>

    # Possible values include: debug, info, notice, warn, error, crit, alert, emerg.
    LogLevel warn
    ErrorLog /var/log/httpd/error_log
    CustomLog /var/log/httpd/access_log combined
    ServerSignature On
SSLEngine On
SSLCertificateFile /etc/httpd/conf/ssl/hostcert.pem
SSLCertificateKeyFile /etc/httpd/conf/ssl/hostkey.pem
</VirtualHost>
```

SVN Account Setup Details

```
svnadmin create /var/www/www.server.net/svn/projectname --fs-type fsfs
chown -R apache:apache /var/www/www.server.net/svn/projectname
#this is needed, as the svn is accessed via apache.
```

```
htpasswd -nb newuser newpassword >> /var/www/www.server.net/.htpasswd
```

```
trac-admin /var/www/www.server.net/trac/tracprojectname initenv
//enter data for the title
//enter data for the sql-lite database (choose defaults)
//enter path to svn info ( /var/lib/svn/projectname )
//enter path to Trac template (choose default)
```

```
trac-admin /var/www/www.server.net/trac/tracprojectname/ permission add username MILESTONE_ADMIN RE
chown -R apache:apache /var/www/www.server.net/trac/tracprojectname
```

Runlevels in Fedora / Centos / RPM

```
chkconfig --list
chkconfig --del nameofservice
```

Misc Info

Extra Packages installed for php and mysql:

```
yum install php-mcrypt
yum install php-mbstring
```