4 Install The SSH Server (Optional)

If you did not install the OpenSSH server during the system installation, you can do it now:

```
apt-get install ssh openssh-server
```

From now on you can use an SSH client such as PuTTY and connect from your workstation to your Debian Wheezy server and follow the remaining steps from this tutorial.

5 Install vim-nox (Optional)

I'll use *vi* as my text editor in this tutorial. The default *vi* program has some strange behaviour on Debian and Ubuntu; to fix this, we install *vim-nox*:

```
apt-get install vim-nox
```

(You don't have to do this if you use a different text editor such as joe or nano.)

6 Configure The Network

Because the Debian Wheezy installer has configured our system to get its network settings via DHCP, we have to change that now because a server should have a static IP addre
/etc/network/interfaces and adjust it to your needs (in this example setup I will use the IP address *192.168.0.100*) (please note that I replace *allow-hotplug eth0* with *aut*
restarting the network doesn't work, and we'd have to reboot the whole system):

```
vi /etc/network/interfaces
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#allow-hotplug eth0
#iface eth0 inet dhcp
auto eth0
iface eth0 inet static
        address 192.168.0.100
        netmask 255.255.255.0
        network 192.168.0.0
        broadcast 192.168.0.255
        gateway 192.168.0.1
```

Then restart your network:

```
/etc/init.d/networking restart
```

Then edit */etc/hosts*. Make it look like this:

```
vi /etc/hosts
```

```
127.0.0.1       localhost.localdomain   localhost
192.168.0.100   server1.example.com     server1

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Now run

```
echo server1.example.com > /etc/hostname
/etc/init.d/hostname.sh start
```

Afterwards, run

```
hostname
hostname -f
```

It is important that both show *server1.example.com* now!

7 Update Your Debian Installation

First make sure that your */etc/apt/sources.list* contains the *wheezy-updates* repository (this makes sure you always get the newest updates for the ClamAV virus scanner -
releases very often, and sometimes old versions stop working), and that the *contrib* and *non-free* repositories are enabled (some packages such as *libapache2-mod-fastcgi* a
repository).

```
vi /etc/apt/sources.list
```

```
deb http://ftp.de.debian.org/debian/ wheezy main contrib non-free
deb-src http://ftp.de.debian.org/debian/ wheezy main contrib non-free

deb http://security.debian.org/ wheezy/updates main contrib non-free
deb-src http://security.debian.org/ wheezy/updates main contrib non-free

# wheezy-updates, previously known as 'volatile'
deb http://ftp.de.debian.org/debian/ wheezy-updates main contrib non-free
deb-src http://ftp.de.debian.org/debian/ wheezy-updates main contrib non-free
```

Run

```
apt-get update
```

to update the apt package database and

```
apt-get upgrade
```

to install the latest updates (if there are any).

8 Change The Default Shell

/bin/sh is a symlink to */bin/dash*, however we need */bin/bash*, not */bin/dash*. Therefore we do this:

```
dpkg-reconfigure dash
```

Use dash as the default system shell (/bin/sh)? <-- No

If you don't do this, the ISPConfig installation will fail.

9 Synchronize the System Clock

It is a good idea to synchronize the system clock with an NTP (**n**etwork **t**ime **p**rotocol) server over the Internet. Simply run

```
apt-get install ntp ntpdate
```

and your system time will always be in sync.

10 Install Postfix, Dovecot, MySQL, phpMyAdmin, rkhunter, binutils

We can install Postfix, Dovecot, MySQL, rkhunter, and binutils with a single command:

```
apt-get install postfix postfix-mysql postfix-doc mysql-client mysql-server openssl getmail4 rkhunter binutils dovecot-imapd dovecot-pop3d dovecot-my
sudo
```

You will be asked the following questions:

General type of mail configuration: <-- Internet Site
System mail name: <-- server1.example.com
New password for the MySQL "root" user: <-- yourrootsqlpassword
Repeat password for the MySQL "root" user: <-- yourrootsqlpassword

Next open the TLS/SSL and submission ports in Postfix:

```
vi /etc/postfix/master.cf
```

Uncomment the *submission* and *smtps* sections as follows (leave *-o milter_macro_daemon_name=ORIGINATING* as we don't need it):

```
[...]
submission inet n       -       -       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
smtps     inet  n       -       -       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
[...]
```

Restart Postfix afterwards:

```
/etc/init.d/postfix restart
```

We want MySQL to listen on all interfaces, not just localhost, therefore we edit */etc/mysql/my.cnf* and comment out the line *bind-address = 127.0.0.1*:

```
vi /etc/mysql/my.cnf
```

```
[...]
```

```
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
#bind-address           = 127.0.0.1
[...]
```

Then we restart MySQL:

```
/etc/init.d/mysql restart
```

Now check that networking is enabled. Run

```
netstat -tap | grep mysql
```

The output should look like this:

```
root@server1:~# netstat -tap | grep mysql
tcp        0      0 *:mysql                 *:*                     LISTEN      26757/mysqld
root@server1:~#
```

11 Install Amavisd-new, SpamAssassin, And Clamav

To install amavisd-new, SpamAssassin, and ClamAV, we run

```
apt-get install amavisd-new spamassassin clamav clamav-daemon zoo unzip bzip2 arj nomarch lzop cabextract apt-listchanges libnet-ldap-perl libauthen-
docs daemon libio-string-perl libio-socket-ssl-perl libnet-ident-perl zip libnet-dns-perl
```

The ISPConfig 3 setup uses amavisd which loads the SpamAssassin filter library internally, so we can stop SpamAssassin to free up some RAM:

```
/etc/init.d/spamassassin stop
update-rc.d -f spamassassin remove
```

12 Install Apache2, PHP5, phpMyAdmin, FCGI, suExec, Pear, And mcrypt

Apache2, PHP5, phpMyAdmin, FCGI, suExec, Pear, and mcrypt can be installed as follows:

```
apt-get install apache2 apache2.2-common apache2-doc apache2-mpm-prefork apache2-utils libexpat1 ssl-cert libapache2-mod-php5 php5 php5-common php5-g
imap phpmyadmin php5-cli php5-cgi libapache2-mod-fcgid apache2-suexec php-pear php-auth php5-mcrypt mcrypt php5-imagick imagemagick libapache2-mod-su
libapache2-mod-ruby libapache2-mod-python php5-curl php5-intl php5-memcache php5-memcached php5-ming php5-ps php5-pspell php5-recode php5-snmp php5-s
php5-xmlrpc php5-xsl memcached
```

You will see the following question:

```
Web server to reconfigure automatically: <-- apache2
Configure database for phpmyadmin with dbconfig-common? <-- No
```

Then run the following command to enable the Apache modules `suexec`, `rewrite`, `ssl`, `actions`, and `include` (plus `dav`, `dav_fs`, and `auth_digest` if you want to use WebDAV):

```
a2enmod suexec rewrite ssl actions include
```

```
a2enmod dav_fs dav auth_digest
```

Next open `/etc/apache2/mods-available/suphp.conf`...

```
vi /etc/apache2/mods-available/suphp.conf
```

... and comment out the `<FilesMatch "\.ph(p3?|tml)$">` section and add the line `AddType application/x-httpd-suphp .php .php3 .php4 .php5 .phtml` - otherwise all PHI SuPHP:

```
<IfModule mod_suphp.c>
    #<FilesMatch "\.ph(p3?|tml)$">
    #    SetHandler application/x-httpd-suphp
    #</FilesMatch>
        AddType application/x-httpd-suphp .php .php3 .php4 .php5 .phtml
        suPHP_AddHandler application/x-httpd-suphp

    <Directory />
        suPHP_Engine on
    </Directory>

    # By default, disable suPHP for debian packaged web applications as files
    # are owned by root and cannot be executed by suPHP because of min_uid.
    <Directory /usr/share>
        suPHP_Engine off
    </Directory>

# # Use a specific php config file (a dir which contains a php.ini file)
#       suPHP_ConfigPath /etc/php5/cgi/suphp/
# # Tells mod_suphp NOT to handle requests with the type <mime-type>.
#       suPHP_RemoveHandler <mime-type>
</IfModule>
```

Restart Apache afterwards:

```
/etc/init.d/apache2 restart
```

If you want to host Ruby files with the extension *.rb* on your web sites created through ISPConfig, you must comment out the line *application/x-ruby rb* in */etc/mime.type*

```
vi /etc/mime.types
```

```
[...]
#application/x-ruby                             rb
[...]
```

(This is needed only for *.rb* files; Ruby files with the extension *.rbx* work out of the box.)

Restart Apache afterwards:

```
/etc/init.d/apache2 restart
```

12.1 Xcache

Xcache is a free and open PHP opcode cacher for caching and optimizing PHP intermediate code. It's similar to other PHP opcode cachers, such as eAccelerator and APC. It is stron
have one of these installed to speed up your PHP page.

Xcache can be installed as follows:

```
apt-get install php5-xcache
```

Now restart Apache:

```
/etc/init.d/apache2 restart
```

12.2 PHP-FPM

Starting with ISPConfig 3.0.5, there is an additional PHP mode that you can select for usage with Apache: PHP-FPM.

To use PHP-FPM with Apache, we need the mod_fastcgi Apache module (please don't mix this up with mod_fcgid - they are very similar, but you cannot use PHP-FPM with mod_
PHP-FPM and mod_fastcgi as follows:

```
apt-get install libapache2-mod-fastcgi php5-fpm
```

Make sure you enable the module and restart Apache:

```
a2enmod actions fastcgi alias
/etc/init.d/apache2 restart
```

12.3 Additional PHP Versions

Starting with ISPConfig 3.0.5, it is possible to have multiple PHP versions on one server (selectable through ISPConfig) which can be run through FastCGI and PHP-FPM. To learn
PHP versions (PHP-FPM and FastCGI) and how to configure ISPConfig, please check this tutorial: How To Use Multiple PHP Versions (PHP-FPM & FastCGI) With ISPConfig 3 (Debia

13 Install Mailman

Since version 3.0.4, ISPConfig also allows you to manage (create/modify/delete) Mailman mailing lists. If you want to make use of this feature, install Mailman as follows:

```
apt-get install mailman
```

Select at least one language, e.g.:

```
Languages to support: <-- en (English)
Missing site list <-- Ok
```

Before we can start Mailman, a first mailing list called *mailman* must be created:

```
newlist mailman
```

```
root@server1:~# newlist mailman
Enter the email of the person running the list: <-- admin email address, e.g. listadmin@example.com
Initial mailman password: <-- admin password for the mailman list
To finish creating your mailing list, you must edit your /etc/aliases (or
equivalent) file by adding the following lines, and possibly running the
`newaliases' program:

## mailman mailing list
mailman:              "|/var/lib/mailman/mail/mailman post mailman"
mailman-admin:        "|/var/lib/mailman/mail/mailman admin mailman"
mailman-bounces:      "|/var/lib/mailman/mail/mailman bounces mailman"
mailman-confirm:      "|/var/lib/mailman/mail/mailman confirm mailman"
mailman-join:         "|/var/lib/mailman/mail/mailman join mailman"
mailman-leave:        "|/var/lib/mailman/mail/mailman leave mailman"
mailman-owner:        "|/var/lib/mailman/mail/mailman owner mailman"
mailman-request:      "|/var/lib/mailman/mail/mailman request mailman"
mailman-subscribe:    "|/var/lib/mailman/mail/mailman subscribe mailman"
mailman-unsubscribe:  "|/var/lib/mailman/mail/mailman unsubscribe mailman"
```

```
Hit enter to notify mailman owner... <-- ENTER

root@server1:~#
```

Open /etc/aliases afterwards...

```
vi /etc/aliases
```

... and add the following lines:

```
[...]
## mailman mailing list
mailman:              "|/var/lib/mailman/mail/mailman post mailman"
mailman-admin:        "|/var/lib/mailman/mail/mailman admin mailman"
mailman-bounces:      "|/var/lib/mailman/mail/mailman bounces mailman"
mailman-confirm:      "|/var/lib/mailman/mail/mailman confirm mailman"
mailman-join:         "|/var/lib/mailman/mail/mailman join mailman"
mailman-leave:        "|/var/lib/mailman/mail/mailman leave mailman"
mailman-owner:        "|/var/lib/mailman/mail/mailman owner mailman"
mailman-request:      "|/var/lib/mailman/mail/mailman request mailman"
mailman-subscribe:    "|/var/lib/mailman/mail/mailman subscribe mailman"
mailman-unsubscribe:  "|/var/lib/mailman/mail/mailman unsubscribe mailman"
```

Run

```
newaliases
```

afterwards and restart Postfix:

```
/etc/init.d/postfix restart
```

Finally we must enable the Mailman Apache configuration:

```
ln -s /etc/mailman/apache.conf /etc/apache2/conf.d/mailman.conf
```

This defines the alias /cgi-bin/mailman/ for all Apache vhosts, which means you can access the Mailman admin interface for a list at http://<vhost>/cgi-bin/mailman/admin, web page for users of a mailing list can be found at http://<vhost>/cgi-bin/mailman/listinfo/<listname>.

Under http://<vhost>/pipermail you can find the mailing list archives.

Restart Apache afterwards:

```
/etc/init.d/apache2 restart
```

Then start the Mailman daemon:

```
/etc/init.d/mailman start
```

14 Install PureFTPd And Quota

PureFTPd and quota can be installed with the following command:

```
apt-get install pure-ftpd-common pure-ftpd-mysql quota quotatool
```

Edit the file /etc/default/pure-ftpd-common...

```
vi /etc/default/pure-ftpd-common
```

... and make sure that the start mode is set to standalone and set VIRTUALCHROOT=true:

```
[...]
STANDALONE_OR_INETD=standalone
[...]
VIRTUALCHROOT=true
[...]
```

Now we configure PureFTPd to allow FTP and TLS sessions. FTP is a very insecure protocol because all passwords and all data are transferred in clear text. By using TLS, the whole encrypted, thus making FTP much more secure.

If you want to allow FTP and TLS sessions, run

```
echo 1 > /etc/pure-ftpd/conf/TLS
```

In order to use TLS, we must create an SSL certificate. I create it in /etc/ssl/private/, therefore I create that directory first:

```
mkdir -p /etc/ssl/private/
```

Afterwards, we can generate the SSL certificate as follows:

```
openssl req -x509 -nodes -days 7300 -newkey rsa:2048 -keyout /etc/ssl/private/pure-ftpd.pem -out /etc/ssl/private/pure-ftpd.pem
```

```
Country Name (2 letter code) [AU]: <-- Enter your Country Name (e.g., "DE").
```

```
State or Province Name (full name) [Some-State]: <-- Enter your State or Province Name.
Locality Name (eg, city) []: <-- Enter your City.
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter your Organization Name (e.g., the name of your company).
Organizational Unit Name (eg, section) []: <-- Enter your Organizational Unit Name (e.g. "IT Department").
Common Name (eg, YOUR name) []: <-- Enter the Fully Qualified Domain Name of the system (e.g. "server1.example.com").
Email Address []: <-- Enter your Email Address.
```

Change the permissions of the SSL certificate:

```
chmod 600 /etc/ssl/private/pure-ftpd.pem
```

Then restart PureFTPd:

```
/etc/init.d/pure-ftpd-mysql restart
```

Edit */etc/fstab*. Mine looks like this (I added *,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0* to the partition with the mount point */*):

```
vi /etc/fstab
```

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point>   <type>  <options>       <dump>  <pass>
/dev/mapper/server1-root /               ext4    errors=remount-ro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=v
# /boot was on /dev/sda1 during installation
UUID=46d1bd79-d761-4b23-80b8-ad20cb18e049 /boot           ext2    defaults        0       2
/dev/mapper/server1-swap_1 none            swap    sw              0       0
/dev/sr0        /media/cdrom0   udf,iso9660 user,noauto     0       0
```

To enable quota, run these commands:

```
mount -o remount /
```

```
quotacheck -avugm
quotaon -avug
```

15 Install BIND DNS Server

BIND can be installed as follows:

```
apt-get install bind9 dnsutils
```

16 Install Vlogger, Webalizer, And AWstats

Vlogger, webalizer, and AWstats can be installed as follows:

```
apt-get install vlogger webalizer awstats geoip-database libclass-dbi-mysql-perl
```

Open */etc/cron.d/awstats* afterwards...

```
vi /etc/cron.d/awstats
```

... and comment out everything in that file:

```
#MAILTO=root

#*/10 * * * * www-data [ -x /usr/share/awstats/tools/update.sh ] && /usr/share/awstats/tools/update.sh

# Generate static reports:
#10 03 * * * www-data [ -x /usr/share/awstats/tools/buildstatic.sh ] && /usr/share/awstats/tools/buildstatic.sh
```

17 Install Jailkit

Jailkit is needed only if you want to chroot SSH users. It can be installed as follows (important: Jailkit must be installed before ISPConfig - it cannot be installed afterwards!):

```
apt-get install build-essential autoconf automake1.9 libtool flex bison debhelper binutils-gold
```

```
cd /tmp
wget http://olivier.sessink.nl/jailkit/jailkit-2.15.tar.gz
tar xvfz jailkit-2.15.tar.gz
cd jailkit-2.15
./debian/rules binary
```

You can now install the Jailkit *.deb* package as follows:

```
cd ..
dpkg -i jailkit_2.15-1_*.deb
rm -rf jailkit-2.15*
```

18 Install fail2ban

This is optional but recommended, because the ISPConfig monitor tries to show the log:

```
apt-get install fail2ban
```

To make fail2ban monitor PureFTPd and Dovecot, create the file */etc/fail2ban/jail.local*:

```
vi /etc/fail2ban/jail.local
```

```
[pureftpd]
enabled  = true
port     = ftp
filter   = pureftpd
logpath  = /var/log/syslog
maxretry = 3

[dovecot-pop3imap]
enabled = true
filter = dovecot-pop3imap
action = iptables-multiport[name=dovecot-pop3imap, port="pop3,pop3s,imap,imaps", protocol=tcp]
logpath = /var/log/mail.log
maxretry = 5

[sasl]
enabled  = true
port     = smtp
filter   = sasl
logpath  = /var/log/mail.log
maxretry = 3
```

Then create the following two filter files:

```
vi /etc/fail2ban/filter.d/pureftpd.conf
```

```
[Definition]
failregex = .*pure-ftpd: \(.*@<HOST>\) \[WARNING\] Authentication failed for user.*
ignoreregex =
```

```
vi /etc/fail2ban/filter.d/dovecot-pop3imap.conf
```

```
[Definition]
failregex = (?: pop3-login|imap-login): .*(?:Authentication failure|Aborted login \(auth failed|Aborted login   \(trie
bled|Disconnected \(auth failed|Aborted login \(\d+ authentication attempts).*rip=(?P<host>\S*),.*
ignoreregex =
```

Restart fail2ban afterwards:

```
/etc/init.d/fail2ban restart
```

19 Install SquirrelMail

To install the SquirrelMail webmail client, run

```
apt-get install squirrelmail
```

Then configure SquirrelMail:

```
squirrelmail-configure
```

We must tell SquirrelMail that we are using Dovecot-IMAP/-POP3:

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages
```

```
D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> <-- D


SquirrelMail Configuration : Read: config.php
---------------------------------------------------------
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others.  If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct.  This does not change everything.  There are
only a few settings that this will change.

Please select your IMAP server:
    bincimap    = Binc IMAP server
    courier     = Courier IMAP server
    cyrus       = Cyrus IMAP server
    dovecot     = Dovecot Secure IMAP server
    exchange    = Microsoft Exchange IMAP server
    hmailserver = hMailServer
    macosx      = Mac OS X Mailserver
    mercury32   = Mercury/32
    uw          = University of Washington's IMAP server
    gmail       = IMAP access to Google mail (Gmail) accounts

    quit        = Do not change anything
Command >> <-- dovecot


SquirrelMail Configuration : Read: config.php
---------------------------------------------------------
While we have been building SquirrelMail, we have discovered some
preferences that work better with some servers that don't work so
well with others.  If you select your IMAP server, this option will
set some pre-defined settings for that server.

Please note that you will still need to go through and make sure
everything is correct.  This does not change everything.  There are
only a few settings that this will change.

Please select your IMAP server:
    bincimap    = Binc IMAP server
    courier     = Courier IMAP server
    cyrus       = Cyrus IMAP server
    dovecot     = Dovecot Secure IMAP server
    exchange    = Microsoft Exchange IMAP server
    hmailserver = hMailServer
    macosx      = Mac OS X Mailserver
    mercury32   = Mercury/32
    uw          = University of Washington's IMAP server
    gmail       = IMAP access to Google mail (Gmail) accounts

    quit        = Do not change anything
Command >> dovecot

             imap_server_type = dovecot
        default_folder_prefix = <none>
                 trash_folder = Trash
                  sent_folder = Sent
                 draft_folder = Drafts
           show_prefix_option = false
         default_sub_of_inbox = false
show_contain_subfolders_option = false
            optional_delimiter = detect
                 delete_folder = false

Press any key to continue... <-- press a key


SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
```

```
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> <-- S


SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> <-- Q
```

Now we will configure SquirrelMail so that you can use it from within your web sites (created through ISPConfig) by using the */squirrelmail* or */webmail* aliases. So if your we *www.example.com*, you will be able to access SquirrelMail using *www.example.com/squirrelmail* or *www.example.com/webmail*.

SquirrelMail's Apache configuration is in the file */etc/squirrelmail/apache.conf*, but this file isn't loaded by Apache because it is not in the */etc/apache2/conf.d/* directory. symlink called *squirrelmail.conf* in the */etc/apache2/conf.d/* directory that points to */etc/squirrelmail/apache.conf* and reload Apache afterwards:

```
cd /etc/apache2/conf.d/
ln -s ../../squirrelmail/apache.conf squirrelmail.conf
/etc/init.d/apache2 reload
```

Now open */etc/apache2/conf.d/squirrelmail.conf*...

```
vi /etc/apache2/conf.d/squirrelmail.conf
```

... and add the following lines to the *<Directory /usr/share/squirrelmail></Directory>* container that make sure that mod_php is used for accessing SquirrelMail, regardles you select for your website in ISPConfig:

```
[...]
<Directory /usr/share/squirrelmail>
  Options FollowSymLinks
  <IfModule mod_php5.c>
    AddType application/x-httpd-php .php
    php_flag magic_quotes_gpc Off
    php_flag track_vars On
    php_admin_flag allow_url_fopen Off
    php_value include_path .
    php_admin_value upload_tmp_dir /var/lib/squirrelmail/tmp
    php_admin_value open_basedir /usr/share/squirrelmail:/etc/squirrelmail:/var/lib/squirrelmail:/etc/hostname:/etc/mailname
    php_flag register_globals off
  </IfModule>
  <IfModule mod_dir.c>
    DirectoryIndex index.php
  </IfModule>

  # access to configtest is limited by default to prevent information leak
  <Files configtest.php>
    order deny,allow
    deny from all
    allow from 127.0.0.1
  </Files>
</Directory>
[...]
```

Create the directory */var/lib/squirrelmail/tmp*...

```
mkdir /var/lib/squirrelmail/tmp
```

... and make it owned by the user *www-data*:

```
chown www-data /var/lib/squirrelmail/tmp
```

Reload Apache again:

```
/etc/init.d/apache2 reload
```

That's it already - */etc/apache2/conf.d/squirrelmail.conf* defines an alias called */squirrelmail* that points to SquirrelMail's installation directory */usr/share/squirrelmail*

You can now access SquirrelMail from your web site as follows:

http://192.168.0.100/squirrelmail
http://www.example.com/squirrelmail

You can also access it from the ISPConfig control panel vhost (after you have installed ISPConfig, see the next chapter) as follows (this doesn't need any configuration in ISPCon

http://server1.example.com:8080/squirrelmail

If you'd like to use the alias */webmail* instead of */squirrelmail*, simply open */etc/apache2/conf.d/squirrelmail.conf*...

```
vi /etc/apache2/conf.d/squirrelmail.conf
```

... and add the line *Alias /webmail /usr/share/squirrelmail*:

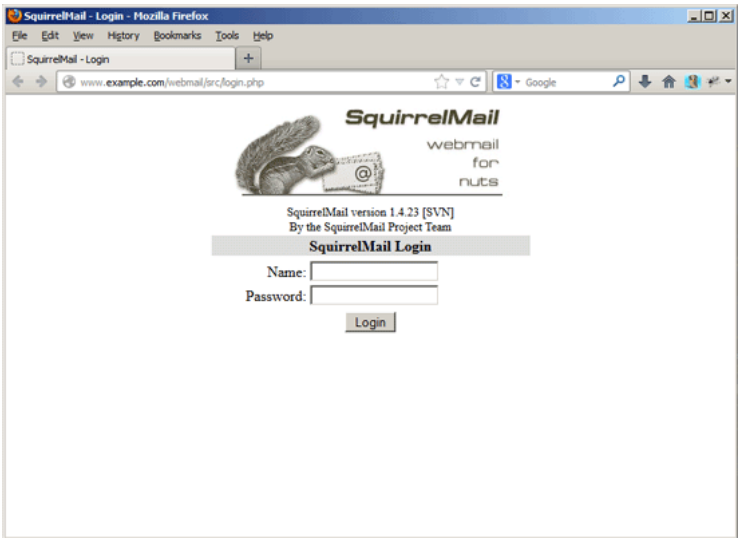
```
Alias /squirrelmail /usr/share/squirrelmail
Alias /webmail /usr/share/squirrelmail
[...]
```

Then reload Apache:

```
/etc/init.d/apache2 reload
```

Now you can access Squirrelmail as follows:

http://192.168.0.100/webmail
http://www.example.com/webmail
http://server1.example.com:8080/webmail (after you have installed ISPConfig, see the next chapter)



Click to enlarge

If you'd like to define a vhost like *webmail.example.com* where your users can access SquirrelMail, you'd have to add the following vhost configuration to */etc/apache2/conf.d*

```
vi /etc/apache2/conf.d/squirrelmail.conf
```

```
[...]
<VirtualHost 1.2.3.4:80>
  DocumentRoot /usr/share/squirrelmail
  ServerName webmail.example.com
</VirtualHost>
```

Make sure you replace *1.2.3.4* with the correct IP address of your server. Of course, there must be a DNS record for *webmail.example.com* that points to the IP address that y configuration. Also make sure that the vhost *webmail.example.com* does not exist in ISPConfig (otherwise both vhosts will interfere with each other!).

Now reload Apache...

```
/etc/init.d/apache2 reload
```

... and you can access SquirrelMail under *http://webmail.example.com*!

20 Install ISPConfig 3

To install ISPConfig 3 from the latest released version, do this:

```
cd /tmp
wget http://www.ispconfig.org/downloads/ISPConfig-3-stable.tar.gz
tar xfz ISPConfig-3-stable.tar.gz
cd ispconfig3_install/install/
```

The next step is to run

```
php -q install.php
```

This will start the ISPConfig 3 installer. The installer will configure all services like Postfix, Dovecot, etc. for you. A manual setup as required for ISPConfig 2 (perfect setup guides

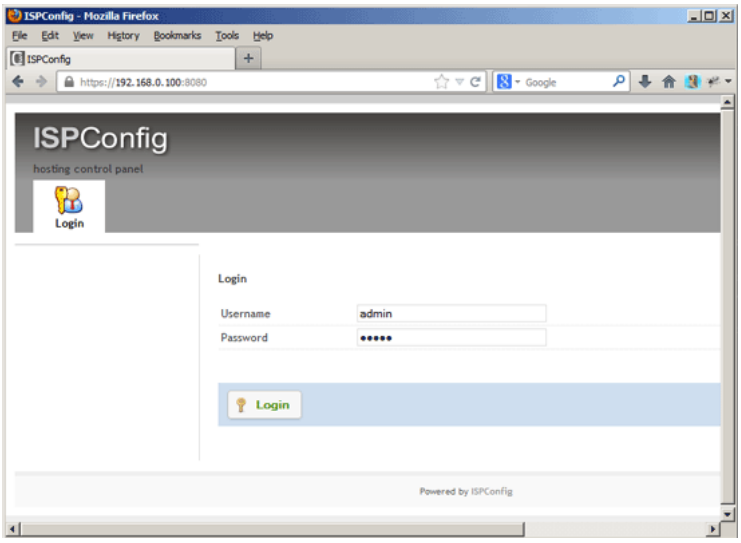
```
root@server1:/tmp/ispconfig3_install/install# php -q install.php
PHP Deprecated:  Comments starting with '#' are deprecated in /etc/php5/cli/conf.d/ming.ini on line 1 in Unknown on line 0


--------------------------------------------------------------------------------
 _____ _____________   _____                 __ _                 ____
|_   _/  ___| ___ \ /  __ \               / _(_)               /__  \
  | | \ `--.| |_/ / | /  \/ ___  _ __  | |_ _  __ _    _/ /
  | |  `--. \  __/  | |    / _ \| '_ \|  _| |/ _` |  |_ |
 _| |_/\__/ / |     | \__/\ (_) | | | | | | | (_| | ___\ \
 \___/\____/\_|      \____/\___/|_| |_|_| |_|\__, | \____/
                                              __/ |
                                             |___/
--------------------------------------------------------------------------------


>> Initial configuration

Operating System: Debian or compatible, unknown version.

    Following will be a few questions for primary configuration so be careful.
    Default values are in [brackets] and can be accepted with <ENTER>.
    Tap in "quit" (without the quotes) to stop the installer.


Select language (en,de) [en]: <-- ENTER

Installation mode (standard,expert) [standard]: <-- ENTER

Full qualified hostname (FQDN) of the server, eg server1.domain.tld  [server1.example.com]: <-- ENTER

MySQL server hostname [localhost]: <-- ENTER

MySQL root username [root]: <-- ENTER

MySQL root password []: <-- yourrootsqlpassword

MySQL database to create [dbispconfig]: <-- ENTER

MySQL charset [utf8]: <-- ENTER

Generating a 4096 bit RSA private key
.....................................................++
.....................................................................................................................++
writing new private key to 'smtpd.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: <-- ENTER
State or Province Name (full name) [Some-State]: <-- ENTER
Locality Name (eg, city) []: <-- ENTER
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- ENTER
Organizational Unit Name (eg, section) []: <-- ENTER
Common Name (e.g. server FQDN or YOUR name) []: <-- ENTER
Email Address []: <-- ENTER
Configuring Jailkit
Configuring Dovecot
Configuring Spamassassin
Configuring Amavisd
Configuring Getmail
Configuring Pureftpd
Configuring BIND
Configuring Apache
Configuring Vlogger
Configuring Apps vhost
```

```
Configuring Bastille Firewall
Configuring Fail2ban
Installing ISPConfig
ISPConfig Port [8080]: <-- ENTER

Do you want a secure (SSL) connection to the ISPConfig web interface (y,n) [y]: <-- ENTER

Generating RSA private key, 4096 bit long modulus
.....................................................................................++
........++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: <-- ENTER
State or Province Name (full name) [Some-State]: <-- ENTER
Locality Name (eg, city) []: <-- ENTER
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- ENTER
Organizational Unit Name (eg, section) []: <-- ENTER
Common Name (e.g. server FQDN or YOUR name) []: <-- ENTER
Email Address []: <-- ENTER

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []: <-- ENTER
An optional company name []: <-- ENTER
writing RSA key
Configuring DBServer
Installing ISPConfig crontab
no crontab for root
no crontab for getmail
Restarting services ...
Stopping MySQL database server: mysqld.
Starting MySQL database server: mysqld ..
Checking for tables which need an upgrade, are corrupt or were
not closed cleanly..
Stopping Postfix Mail Transport Agent: postfix.
Starting Postfix Mail Transport Agent: postfix.
Stopping amavisd: amavisd-new.
Starting amavisd: amavisd-new.
Stopping ClamAV daemon: clamd.
Starting ClamAV daemon: clamd .
Restarting IMAP/POP3 mail server: dovecot.
[Tue May 07 02:36:22 2013] [warn] NameVirtualHost *:443 has no VirtualHosts
[Tue May 07 02:36:22 2013] [warn] NameVirtualHost *:80 has no VirtualHosts
[Tue May 07 02:36:23 2013] [warn] NameVirtualHost *:443 has no VirtualHosts
[Tue May 07 02:36:23 2013] [warn] NameVirtualHost *:80 has no VirtualHosts
Restarting web server: apache2 ... waiting .
Restarting ftp server: Running: /usr/sbin/pure-ftpd-mysql-virtualchroot -l mysql:/etc/pure-ftpd/db/mysql.conf -l pam -H -O clf:/var/log/pure-ftpd/trar
u 1000 -A -E -b -8 UTF-8 -B
Installation completed.
root@server1:/tmp/ispconfig3_install/install#
```

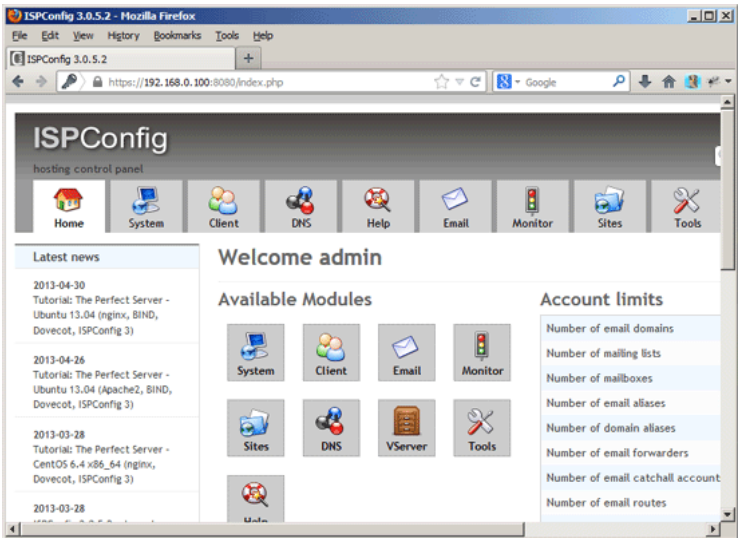
The installer automatically configures all underlying services, so no manual configuration is needed.

You now also have the possibility to let the installer create an SSL vhost for the ISPConfig control panel, so that ISPConfig can be accessed using *https://* instead of *http://*. To press *ENTER* when you see this question: *Do you want a secure (SSL) connection to the ISPConfig web interface (y,n) [y]:*.

Afterwards you can access ISPConfig 3 under *http(s)://server1.example.com:8080/* or *http(s)://192.168.0.100:8080/* (http or https depends on what you chose during i the username *admin* and the password *admin* (you should change the default password after your first login):



Click to enlarge



Click to enlarge

The system is now ready to be used.

21 Additional Notes

21.1 OpenVZ

If the Debian server that you've just set up in this tutorial is an OpenVZ container (virtual machine), you should do this on the host system (I'm assuming that the ID of the Ope
replace it with the correct *VPSID* on your system):

```
VPSID=101
for CAP in CHOWN DAC_READ_SEARCH SETGID SETUID NET_BIND_SERVICE NET_ADMIN SYS_CHROOT SYS_NICE CHOWN DAC_READ_SEARCH SETGID SETUID NET_BIND_SERVICE N
SYS_CHROOT SYS_NICE
do
  vzctl set $VPSID --capability ${CAP}:on --save
done
```

22 Links

- Debian: http://www.debian.org/
- ISPConfig: http://www.ispconfig.org/