Le serveur parfait - Debian 12 (Bookworm) avec Apache, BIND, Dovecot, PureFTPD et ISPConfig 3.2

This tutorial shows how to prepare a Debian 12 server (with Apache2, BIND, Dovecot) for the installation of ISPConfig 3.2, and how to install ISPConfig. The web hosting control panel ISPConfig 3 allows you to configure the following services through a web browser: Apache or nginx web server, Postfix mail server, Dovecot IMAP/POP3 server, MySQL, BIND nameserver, PureFTPd, Rspamd or Amavis, ClamAV, and many more. This setup covers Apache (instead of nginx), BIND, and Dovecot with Rspamd spam scanner.

1 Preliminary Note

In this tutorial, I will use the hostname *server1.example.com* with the IP address *192.168.0.100* and the gateway *192.168.0.1*. These settings might differ for you, so you have to replace them where appropriate. Before proceeding further, you need to have a minimal installation of Debian 12. This might be a Debian minimal image from your Hosting provider or you use the Minimal Debian Server tutorial to set up the base system.

All commands below are run as root user. Either login as the root user directly or log in as your regular user and then use the command

```
su -
```

to become the root user on your server before you proceed. **IMPORTANT**: You must use 'su -' and not just 'su', otherwise, your PATH variable is set wrong by su.

Ensure that your */etc/apt/sources.list* contains the bookworm-updates repository (this ensures you always get the newest updates), and that the *contrib*, *non-free* and *non-free-firmware* repositories are enabled.

```
nano /etc/apt/sources.list
```

```
#deb cdrom:[Debian GNU/Linux 12.1.0 _Bookworm_ - Official amd64 NETINST with firmware 20230722-10:48]/ bookworm main non-free-firmware

deb http://deb.debian.org/debian/ bookworm main contrib non-free non-free-firmware
deb-src http://deb.debian.org/debian/ bookworm main contrib non-free non-free-firmware

deb http://security.debian.org/debian-security bookworm-security main contrib non-free non-free-firmware
deb-src http://security.debian.org/debian-security bookworm-security main contrib non-free non-free-firmware

# bookworm-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates_and_backports
deb http://deb.debian.org/debian/ bookworm-updates main contrib non-free non-free-firmware
deb-src http://deb.debian.org/debian/ bookworm-updates main contrib non-free non-free-firmware

# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
```

Save the file.

2 Install the SSH server (Optional)

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

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

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

3 Install a shell text editor (Optional)

We will use *nano* text editor in this tutorial. Some users prefer the classic vi editor, therefore, we will install both editors here. The default *vi* program has some strange behavior on Debian and Ubuntu; to fix this, we install *vim-nox*:

```
apt install nano vim-nox
```

If vi is your favorite editor, replace nano with vi in the following commands to edit files.

4 Configure the Hostname

The hostname of your server should be a subdomain like "server1.example.com". Do not use a domain name without subdomain part like "example.com" as hostname as this will cause problems later with your mail setup. First, you should check the hostname in */etc/hosts* and change it when necessary. The line should be: "IP Address - space - full hostname incl. domain - space - subdomain part". For our hostname server1.example.com, the file shall look like this:

```
nano /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
```

Then edit the /etc/hostname file:

```
nano /etc/hostname
```

It shall contain only the subdomain part, in our case:

```
server1
```

Finally, reboot the server to apply the change:

```
systemctl reboot
```

Log in again and check if the hostname is correct now with these commands:

```
hostname
hostname -f
```

The output shall be like this:

```
root@server1:/tmp# hostname
server1
root@server1:/tmp# hostname -f
server1.example.com
```

5 Update your Debian Installation

First, ensure that your /etc/apt/sources.list contains the bookworm/updates repository (this ensures you always get the newest security updates), and that the *contrib, non-free* and *non-free-firmware* repositories are enabled, as some required packages are not in the main repository.

```
nano /etc/apt/sources.list
```

```
#deb cdrom:[Debian GNU/Linux 12.1.0 _Bookworm_ - Official amd64 NETINST with firmware 20230722-10:48]/ bookworm main non-free-firmware

deb http://deb.debian.org/debian/ bookworm main contrib non-free non-free-firmware
deb-src http://deb.debian.org/debian/ bookworm main contrib non-free non-free-firmware

deb http://security.debian.org/debian-security bookworm-security main contrib non-free non-free-firmware
deb-src http://security.debian.org/debian-security bookworm-security main contrib non-free non-free-firmware

# bookworm-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates_and_backports
deb http://deb.debian.org/debian/ bookworm-updates main contrib non-free non-free-firmware
deb-src http://deb.debian.org/debian/ bookworm-updates main contrib non-free non-free-firmware

# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
# For information about how to configure apt package sources,
# see the sources.list(5) manual.
```

Run:

```
apt update
```

To update the apt package database

```
apt upgrade
```

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

6 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 -y install ntp
```

and your system time will always be in sync.

7 Install Postfix, Dovecot, MariaDB, rkhunter, and Binutils

We can install Postfix, Dovecot, MariaDB as a MySQL alternative, rkhunter, and Binutils with a single command:

```
apt -y install postfix postfix-mysql postfix-doc mariadb-client mariadb-server openssl getmail6 rkhunter binutils dovecot-imapd dovecot-pop3d dovecot-mysql dovecot-sieve dovecot-lmtpd sudo curl rsyslog wget gnupg2 lsb-release ufw
```

You will be asked the following questions:

```
General type of mail configuration: <-- Internet Site
System mail name: <-- server1.example.com
```

To secure the MariaDB installation and to disable the test database, run this command:

```
mysql_secure_installation
```

Answer the questions as follows:

```
Switch to unix_socket authentication [Y/n] <-- n
Change the root password? [Y/n] <-- y
New password: <-- Enter new password
Re-enter new password: <-- Repeat new password
Remove anonymous users? [Y/n] <-- y
Disallow root login remotely? [Y/n] <-- y
Remove test database and access to it? [Y/n] <-- y
Reload privilege tables now? [Y/n] <-- y
```

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

```
nano /etc/postfix/master.cf
```

Uncomment the *submission* and *submissions* sections as follows and add lines where necessary so that this section of the master.cf file looks exactly like the one below. **IMPORTANT:** Remove the # in front of the lines that start with submissions and submission too and not just from the -o lines after these lines!

```
[...]
#127.0.0.1:submission inet n -   y       -       -       smtpd
submission inet n       -       y       -       -       smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_tls_auth_only=yes
#  -o smtpd_reject_unlisted_recipient=no
#     Instead of specifying complex smtpd__restrictions here,
#     specify "smtpd__restrictions=$mua__restrictions"
#     here, and specify mua__restrictions in main.cf (where
#     "" is "client", "helo", "sender", "relay", or "recipient").
#  -o smtpd_client_restrictions=
#  -o smtpd_helo_restrictions=
#  -o smtpd_sender_restrictions=
#  -o smtpd_relay_restrictions=
#  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
# Choose one: enable submissions for loopback clients only, or for any client.
#127.0.0.1:submissions inet n  -       y       -       -       smtpd
submissions     inet  n       -       y       -       -       smtpd
  -o syslog_name=postfix/submissions
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_reject_unlisted_recipient=no
#     Instead of specifying complex smtpd__restrictions here,
#     specify "smtpd__restrictions=$mua__restrictions"
#     here, and specify mua__restrictions in main.cf (where
#     "" is "client", "helo", "sender", "relay", or "recipient").
#  -o smtpd_client_restrictions=
#  -o smtpd_helo_restrictions=
#  -o smtpd_sender_restrictions=
#  -o smtpd_relay_restrictions=
#  -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#628       inet  n       -       y       -       -       qmqpd
[...]
```

Restart Postfix afterward:

```
systemctl restart postfix
```

If you want MySQL to listen on all interfaces, not just localhost, to allow access to MySQL from desktop tools, then edit */etc/mysql/mariadb.conf.d/50-server.cnf* and comment out the line *bind-address = 127.0.0.1* by adding a # in front of it.

```
nano /etc/mysql/mariadb.conf.d/50-server.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

[...]
```

Edit the file /etc/mysql/debian.cnf and set the MYSQL / MariaDB root password there twice in the rows that start with the word password.

```
nano /etc/mysql/debian.cnf
```

The MySQL root password that needs to be added is shown in red. In this example, the password is "mickaelangel".

```
# Automatically generated for Debian scripts. DO NOT TOUCH!
[client]
host = localhost
user = root
password = "mickaelangel"
[mysql_upgrade]
host = localhost
user = root
password = "mickaelangel"
```

To prevent the error '***Error in accept: Too many open files***' we will set higher open file limits for MariaDB now.

Open the file /etc/security/limits.conf with an editor:

```
nano /etc/security/limits.conf
```

and add these lines at the end of the file.

```
mysql soft nofile 65535
mysql hard nofile 65535
```

Next, create a new directory /etc/systemd/system/mysql.service.d/ with the mkdir command.

```
mkdir -p /etc/systemd/system/mysql.service.d/
```

and add a new file inside:

```
nano /etc/systemd/system/mysql.service.d/limits.conf
```

paste the following lines into that file:

```
[Service]
LimitNOFILE=infinity
```

Save the file and close the nano editor.

Then we reload systemd and restart MariaDB:

```
systemctl daemon-reload
systemctl restart mariadb
```

Now check that networking is enabled. Run

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

The output should look like this:

```
root@server1:/home/administrator# netstat -tap | grep mysql
tcp6 0 0 [::]:mysql [::]:* LISTEN 16623/mysqld
```

8 Install Email filter and signing software Rspamd and ClamAV

Add the Rspamd repository:

```
CODENAME=`lsb_release -c -s`
wget -qO- https://rspamd.com/apt-stable/gpg.key | tee /etc/apt/trusted.gpg.d/rspamd.asc > /dev/null
echo "deb [arch=amd64] http://rspamd.com/apt-stable/ $CODENAME main" > /etc/apt/sources.list.d/rspamd.list
```

```
echo "deb-src [arch=amd64] http://rspamd.com/apt-stable/ $CODENAME main" >> /etc/apt/sources.list.d/rspamd.list
```

To install Rspamd and ClamAV, we run

```
apt install rspamd redis clamav clamav-daemon unzip bzip2 arj nomarch lzop cabextract p7zip p7zip-full unrar lrzip apt-listchanges libnet-ldap-perl libauthen-sasl-perl clamav-docs daemon libio-string-perl libio-socket-ssl-perl libnet-ident-perl zip libnet-dns-perl libdbd-mysql-perl postgrey -y
```

Activate Redis in Rspamd configuration.

```
echo 'servers = "127.0.0.1";' > /etc/rspamd/local.d/redis.conf
```

Increase the Rspamd history, enable compression and show the subject in the history. This step is optional.

```
echo "nrows = 2500;" > /etc/rspamd/local.d/history_redis.conf
echo "compress = true;" >> /etc/rspamd/local.d/history_redis.conf
echo "subject_privacy = true;" >> /etc/rspamd/local.d/history_redis.conf
```

Then restart Rspamd.

```
systemctl restart rspamd
```

9 Install Apache Web Server and PHP

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

```
apt -y install apache2 apache2-utils php8.2 php8.2-fpm php8.2-common php8.2-gd php8.2-mysql php8.2-imap php8.2-cli php8.2-cgi libapache2-mod-fcgid apache2-suexec-pristine php-pear mcrypt imagemagick libruby libapache2-mod-python php8.2-curl php8.2-intl php8.2-pspell php8.2-sqlite3 php8.2-tidy php8.2-xmlrpc php8.2-xsl memcached php-memcache php-imagick php8.2-zip php8.2-mbstring memcached libapache2-mod-passenger php8.2-soap php8.2-opcache php-apcu libapache2-reload-perl php8.2-mcrypt
```

Now enable php-fpm in Apache:

```
a2enmod proxy_fcgi setenvif
a2enconf php8.2-fpm
```

Then run the following command to enable the additional 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 dav_fs dav auth_digest cgi headers actions alias
```

To ensure that the server cannot be attacked through the HTTPOXY vulnerability, we will disable the HTTP_PROXY header in apache globally by adding the configuration file /etc/apache2/conf-available/httpoxy.conf.

Note: *The vulnerability is named httpoxy (without 'r') and therefore the file where we add the config to prevent it is named httpoxy.conf and not httproxy.conf, so there is no 'r' missing in the filename.*

```
nano /etc/apache2/conf-available/httpoxy.conf
```

Paste the following content to the file:

```
<IfModule mod_headers.c>
    RequestHeader unset Proxy early
</IfModule>
```

And enable the module by running:

```
a2enconf httpoxy
systemctl restart apache2
```

10 Install Let's Encrypt

ISPConfig is using acme.sh now as Let's Encrypt client. Install acme.sh using the following command:

```
curl https://get.acme.sh | sh -s
```

11 Install PureFTPd and Quota

PureFTPd and quota can be installed with the following command:

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

Create the dhparam file for pure-ftpd:

```
openssl dhparam -out /etc/ssl/private/pure-ftpd-dhparams.pem 2048
```

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

```
nano /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 communication can be encrypted, thus making FTP much more secure.

If you want to allow FTP and TLS sessions, run

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

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:

```
systemctl restart pure-ftpd-mysql
```

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

```
nano /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>
# / was on /dev/sda1 during installation
UUID=45576b38-39e8-4994-b8c1-ea4870e2e614 / ext4 errors=remount-ro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0 1
# swap was on /dev/sda5 during installation
UUID=8bea0d1e-ec37-4b20-9976-4b7daaa3eb69 none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
```

To enable quota, run these commands:

```
mount -o remount /
systemctl daemon-reload
```

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

You will get the message "*quotaon: Your kernel probably supports ext4 quota feature but you are using external quota files. Please switch your filesystem to use ext4 quota feature as external quota files on ext4 are deprecated.*" which is ok and can be ignored.

12 Install BIND DNS Server

BIND can be installed as follows:

```
apt install bind9 dnsutils
```

If your server is a virtual machine, then it is highly recommended to install the haveged daemon to get a higher entropy for DNSSEC signing. You can install haveged on nonvirtual servers as well, it should not hurt.

```
apt install haveged
```

An explanation on that topic can be found here.

13 Install Webalizer replacement awffull, AWStats and GoAccess

Webalizer and AWStats can be installed as follows:

```
apt install awffull awstats geoip-database libclass-dbi-mysql-perl libtimedate-perl
```

Create webalizer directory and symlink so awffull is recognized as webalizer:

```
mkdir /etc/webalizer
chmod 0755 /etc/webalizer
ln -s /etc/awffull/awffull.conf /etc/webalizer/webalizer.conf
ln -s /usr/bin/awffull /usr/bin/webalizer
```

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

```
nano /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
```

Installing the latest GoAccess version directly from the GoAccess repository:

```
echo "deb https://deb.goaccess.io/ $(lsb_release -cs) main" | tee -a /etc/apt/sources.list.d/goaccess.list
wget -O - https://deb.goaccess.io/gnugpg.key | tee /etc/apt/trusted.gpg.d/goaccess.asc >/dev/null
apt update
apt install goaccess
```

14 Install Jailkit

Jailkit is needed only if you want to chroot SSH users. It can be installed as follows:

```
apt install jailkit
```

15 Install fail2ban and UFW Firewall

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

```
apt install fail2ban
```

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

```
nano /etc/fail2ban/jail.local
```

And add the following configuration to it.

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

[dovecot]
enabled = true
filter = dovecot
```

```
logpath = /var/log/mail.log
maxretry = 5

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

Restart fail2ban afterwards:

```
systemctl restart fail2ban
```

To install the UFW firewall, run this apt command:

```
apt install ufw
```

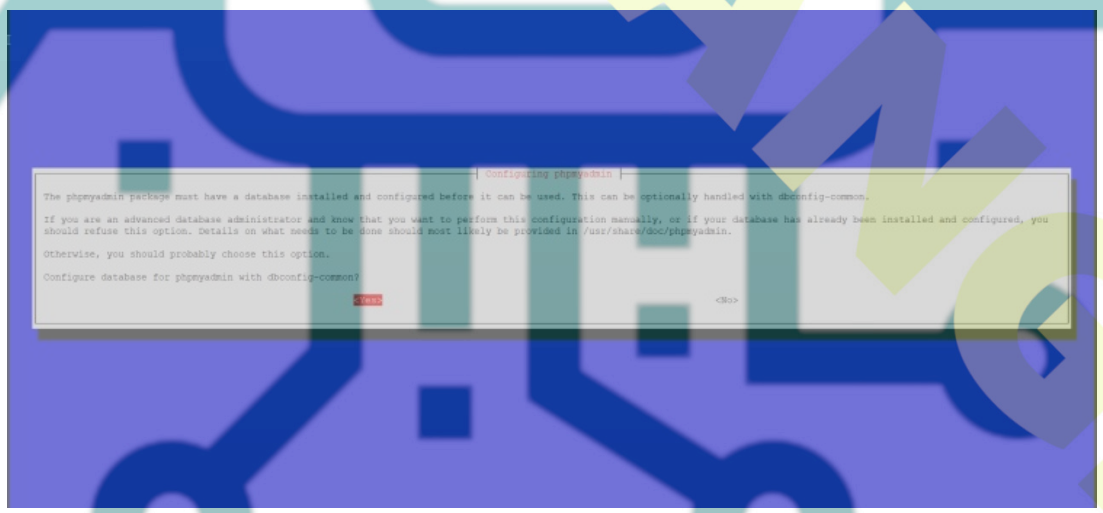
16 Install PHPMyAdmin Database Administration Tool

Install phpMyAdmin with apt:

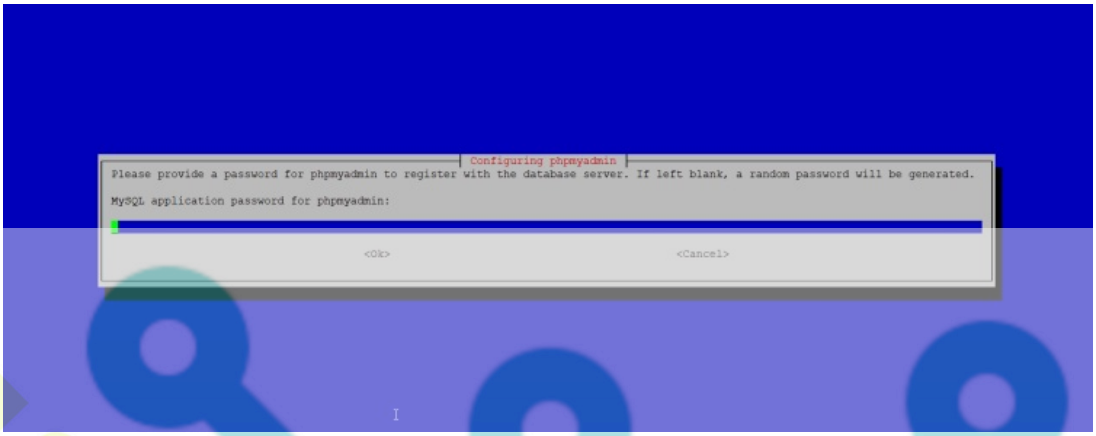
```
apt install phpmyadmin
```

Chose to enable phpMyAdmin in Apache:

Configure PHPMyAdmin using dbconfig common.



Leave the application password field empty and press return. Apt will create a secure random password automatically, and you do not need to know this password to access PHPMyAdmin later.



17 Install RoundCube Webmail (optional)

In this chapter, we will install the RoundCube webmail client.

Then install RoundCube with this command:

```
apt install roundcube roundcube-core roundcube-mysql roundcube-plugins
```

The installer will ask the following questions:

```
Configure database for roundcube with dbconfig.common? <-- yes
MySQL application password for roundcube: <-- press enter
```

Then edit the Apache RoundCube configuration file /etc/apache2/conf-enabled/roundcube.conf:

```
nano /etc/apache2/conf-enabled/roundcube.conf
```

And add an alias line for the apache /webmail alias and one for /roundcube, you can add the line right at the beginning of the file. NOTE: Do not use /mail as alias or the ispconfig email module will stop working!

```
Alias /roundcube /var/lib/roundcube/public_html
Alias /webmail /var/lib/roundcube/public_html
```

Then reload Apache:

```
systemctl reload apache2
```

Now edit the RoundCube Configuration file:

```
nano /etc/roundcube/config.inc.php
```

And change the line:

```
$config['smtp_host'] = 'localhost:587';
```

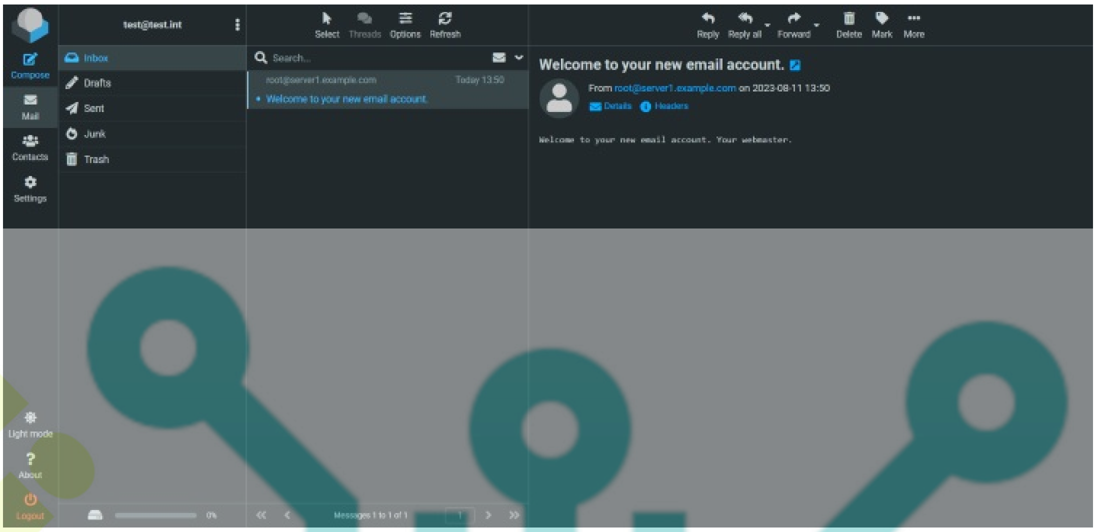
to:

```
$config['smtp_host'] = 'localhost:25';
```

Now you can access RoundCube as follows:

```
https://192.168.0.100:8081/webmail
https://www.example.com:8081/webmail
```

After you have installed ISPConfig, see the next chapter.



Some plugins exist to integrate RoundCube Webmail with ISPConfig, have a look here for the [ISPConfig RoundCube plugin installation instructions](#).

18 Download ISPConfig 3.2

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/
```

19 Install ISPConfig

The next step is to run the ISPConfig installer.

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

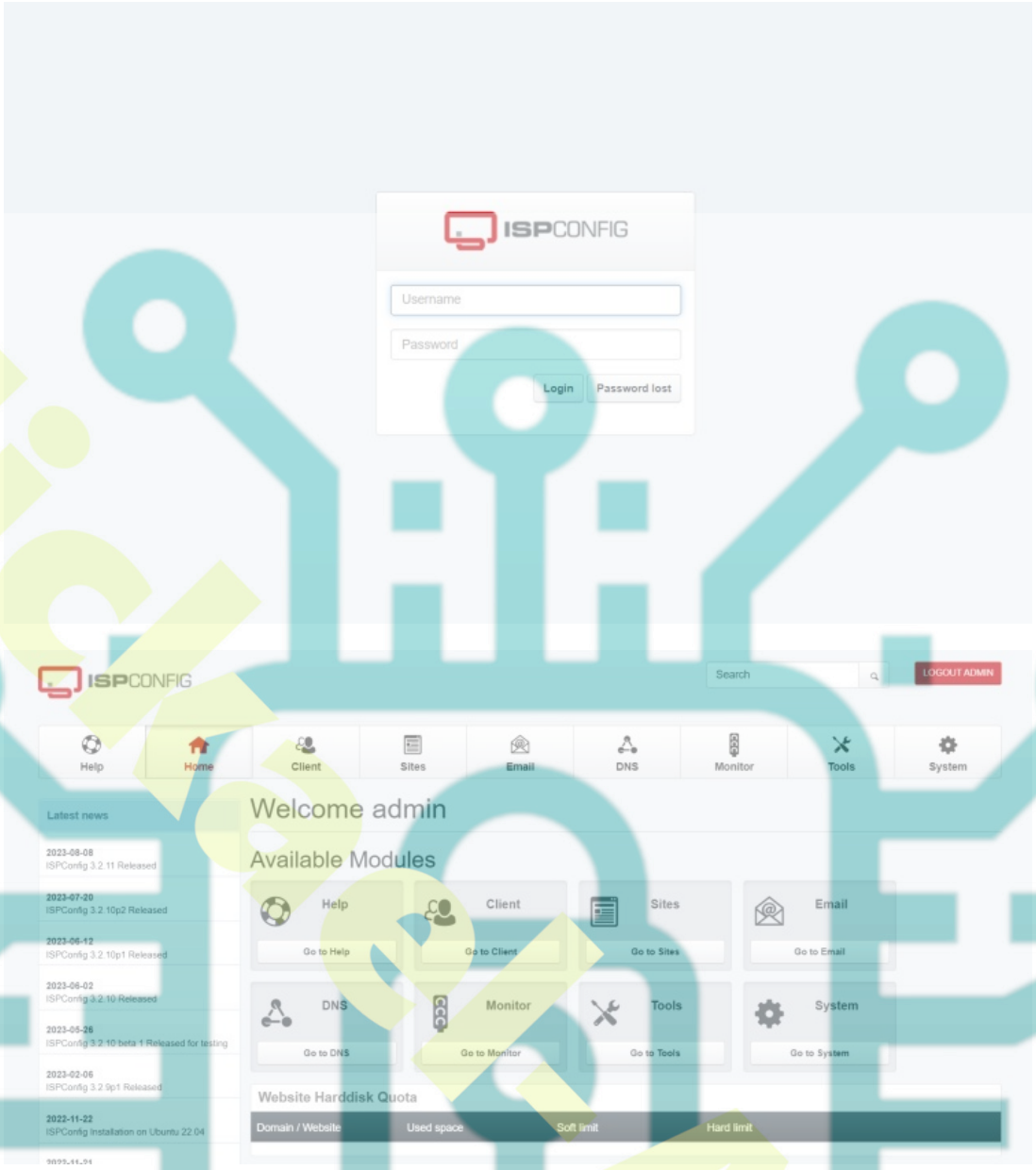
This will start the ISPConfig 3 installer. The installer will configure all services, like Postfix, Dovecot, etc., for you.

```
php -q install.php

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

>> Initial configuration

Operating System: Debian 12.0 (Bookworm) or compatible

    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]: <-- press enter

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

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

MySQL server hostname [localhost]: <-- press enter

MySQL server port [3306]: <-- press enter

MySQL root username [root]: <-- press enter

MySQL root password []: <-- enter the MySQL root password

MySQL database to create [dbispconfig]: <-- press enter

MySQL charset [utf8]:

Checking MariaDB version 10.11.3 .. OK
Configuring Postgrey
Configuring Postfix
[....]
-----
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 country code
State or Province Name (full name) [Some-State]: <-- Enter state
Locality Name (eg, city) []: <-- Enter City
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter company name
Organizational Unit Name (eg, section) []: <-- press enter
Common Name (e.g. server FQDN or YOUR name) []: <-- Enter server hostname
Email Address []: <-- Enter email address
[INFO] service Mailman not detected
Configuring Dovecot
Creating new DHParams file, this takes several minutes. Do not interrupt the script.
Generating DH parameters, 2048 bit long safe prime
[.....]
[INFO] service Spamassassin not detected
[INFO] service Amavisd not detected
Configuring Rspamd
Configuring Getmail
Configuring Jailkit
Configuring Pureftpd
Configuring BIND
Configuring Apache
Configuring vlogger
[INFO] service OpenVZ not detected
Configuring AppArmor
Configuring Ubuntu Firewall
[INFO] service Metronome XMPP Server not detected
Configuring Fail2ban
Installing ISPConfig
ISPConfig Port [8080]: <-- press enter

Admin password [8563a921]: <-- Enter your ISPConfig admin password, or press enter to accept the one that is shown

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

Checking / creating certificate for server1.example.com
Using certificate path /etc/letsencrypt/live/server1.example.com
Server's public ip(s) (91.38.138.191, 2003:e1:bf42:2500:20c:29ff:fe32:617f) not found in A/AAAA records for server1.example.com:
Ignore DNS check and continue to request certificate? (y,n) [n]: <-- press enter

Could not issue letsencrypt certificate, falling back to self-signed.
[....]
-----
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 country code
State or Province Name (full name) [Some-State]: <-- Enter state
Locality Name (eg, city) []: <-- Enter City
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter company name
Organizational Unit Name (eg, section) []: <-- press enter
Common Name (e.g. server FQDN or YOUR name) []: <-- Enter server hostname
Email Address []: <-- Enter email address
Symlink ISPConfig SSL certs to Postfix? (y,n) [y]: <-- press Enter

Symlink ISPConfig SSL certs to Pure-FTPd? Creating dhparam file may take some time. (y,n) [y]: <-- press Enter

Configuring Apps vhost
Configuring DBServer
Installing ISPConfig crontab
no crontab for getmail
Detect IP addresses
Restarting services ...
Installation completed.
```

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

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 installation). Log in with the username *admin* and the password *admin* (you should change the default password after your first login):



The system is now ready to be used.

20 ISPConfig 3 Manual

To learn how to use ISPConfig 3, I strongly recommend downloading the ISPConfig 3 Manual.

On more than 300 pages, it covers the concept behind ISPConfig (admin, resellers, clients), explains how to install and update ISPConfig 3, includes a reference for all forms and form fields in ISPConfig together with examples of valid inputs, and provides tutorials for the most common tasks in ISPConfig 3. It also outlines how to make your server more secure and has a troubleshooting section.

21 Virtual Machine Image Download of this Tutorial

This tutorial is available as ready to-use virtual machine image in ovf/ova format that is compatible with VMWare and Virtualbox. The virtual machine image uses the following login details:

SSH / Shell Login

Username: administrator
Password: mickaelangel

Username: root
Password: mickaelangel

ISPConfig Login

Username: admin
Password: mickaelangel

MySQL Login

Username: root
Password: I7DFg3!cpHfw3bxZj6Fg

The IP of the VM is 192.168.0.100. It can be changed in the file /etc/network/interfaces. Please change all the above passwords to secure the virtual machine.

23 Links

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