ISPConfig 3.1 - Ubuntu 18.04 (Bionic Beaver)

Contents

[Warranty 3](#_Toc534090403)

[1. Introduction 4](#_Toc534090404)

[2. Preliminary Note 4](#_Toc534090405)

[3. Edit /etc/apt/sources.list to Update Your Linux Installation 4](#_Toc534090406)

[4. Change the Default Shell 5](#_Toc534090407)

[5. Disable AppArmor 5](#_Toc534090408)

[6. Synchronize the System Clock 6](#_Toc534090409)

[7. Required Software 6](#_Toc534090410)

[8. Install Postfix, Dovecot, MariaDB, rkhunter, and binutils 6](#_Toc534090411)

[9. Install Amavisd-new, SpamAssassin, and Clamav 9](#_Toc534090412)

[10. Install Metronome XMPP Server (optional) 10](#_Toc534090413)

[11. Install Apache, PHP, phpMyAdmin, FCGI, SuExec, Pear, and mcrypt 10](#_Toc534090414)

[12. PHP Opcode cache (optional) 11](#_Toc534090415)

[13. PHP-FPM 11](#_Toc534090416)

[14. Install HHVM (HipHop Virtual Machine), (optional) 12](#_Toc534090417)

[15. Install Let's Encrypt 12](#_Toc534090418)

[16. Install Mailman 12](#_Toc534090419)

[17. Install PureFTPd and Quota(optional) 14](#_Toc534090420)

[18. Install BIND DNS Server 16](#_Toc534090421)

[19. Install Vlogger, Webalizer, and AWStats 17](#_Toc534090422)

[20. Install Jailkit 17](#_Toc534090423)

[21. Install fail2ban 17](#_Toc534090424)

[22. Install UFW 18](#_Toc534090425)

[23. Install Roundcube Webmail 18](#_Toc534090426)

[24. Install ISPConfig 3.1 19](#_Toc534090427)

[18. Virtual machine image download of this tutorial 22](#_Toc534090428)

# Warranty

**BY USING THIS STANDARD OPERATING PROCEDURE (SOP) YOU AGREE TOTHIS WARRANTY.BEFORE USING IT, PLEASE READ THIS WARRANTY CAREFULLY. IF YOU DO NOT ACCEPT THIS WARRANTY, DO NOT USE THIS “SOP” NOR THE APPLLIANCE RETURN IT UNUSED OR DESTROY IT. YOU SHALL NOT CLAIM ANY REFUND AS IT IS PROVIDED ON “AS IS” BASIS AND PROVIDED ABSOLUTELY FREE.**

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

See https://www.ispconfig.org/warranty for more information.

This Warranty is distinct from any statutory product warrantees owed by any service provider and/or manufacturers under any national law applicable to you. It is intended to grant you specific, and as the case may be, additional rights, within the limits of what is permissible under such law, and not to restrict your rights under applicable statutory product warrantee provisions. It cannot be transferred to any third party.

**1. Warranty**

(a) For **first (15) day** from the date you downloaded appliance or plugin from us due to any defect or bug or workmanship under Normal Use Conditions you can ask for assistance. However, since this is downloaded for free we are not bound to provide any support unless and otherwise we are covered with any obligations to you.

(b) This is the only express warranty or condition we give for your purchase for support, service or plugins. We give no other guarantee, warranty, or condition. No one else may give any guarantee, warranty, or condition on our behalf.

**2. Duration**

Without prejudice to any statutory warranty to which you may be entitled under any local law applicable to You, and unless any such law provides for a longer term, We offers no Warranty, for a term from the purchase date of such appliance downloaded from our portal or an authorized service provider .

**3. Territory**

This Support Warranty is only valid under BSD License agreement if you have purchased for any support in the following countries: India, Singapore, and Australia since we operate from this countries only. You acknowledge that specific export laws and regulations may apply to you depending on your country of residence and you agree to comply with all such laws and regulations if you export your software back to us.

**Choice of Law** This Warranty will be subject to and construed in accordance with the laws of

Your country of residence where the product was originated.

# Introduction

This tutorial exhibits the installation ISPConfig hosting Server utility alike other panels e.g. cPanel on Ubuntu 18.04 (Bionic Beaver) server with Apache 2.4, Postfix, Dovecot, Bind and PureFTPD. The resulting system will also provide a Web, Mail, Mailinglist, DNS and FTP Server.

ISPConfig is a web hosting control panel that allows you to configure the following services through a web browser: Apache or Nginx web server, Postfix mail server, Courier or Dovecot IMAP/POP3 server, MySQL, BIND or MyDNS nameserver, PureFTPd, SpamAssassin, ClamAV, and many more. This setup covers the installation of Apache (instead of Nginx), BIND (instead of MyDNS), and Dovecot (instead of Courier).

# Preliminary Note

In this tutorial, I use the hostname server1.example.com with the IP address 192.168.1.100 and the gateway 192.168.1.1 These settings might differ for you, so you have to replace them where appropriate. Before proceeding further you need to have a basic minimal installation of Ubuntu 18.04 as explained in the [tutorial](https://www.howtoforge.com/tutorial/ubuntu-lts-minimal-server/).

The commands in this tutorial have to be run with root permissions. To avoid adding sudo in front of each command, you'll have to become root user by running: sudo -s before you proceed.

# Edit /etc/apt/sources.list to Update Your Linux Installation

Edit /etc/apt/sources.list. Comment out or remove the installation CD from the file and make sure that the universe and multiverse repositories are enabled. It should look like this afterwards: nano /etc/apt/sources.list

# root@ispconfig3:/# cd /etc/apt

# root@ispconfig3:/etc/apt# mv sources.list sourcesold

# root@ispconfig3:/etc/apt# nano sources.list

Add Following :

# deb cdrom:[Ubuntu-Server 18.04 LTS \_Bionic Beaver\_ - Release amd64 (20180425.1)]/ bionic main restricted

#deb cdrom:[Ubuntu-Server 18.04 LTS \_Bionic Beaver\_ - Release amd64 (20180425.1)]/ bionic main restricted

# See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to

# newer versions of the distribution.

deb http://de.archive.ubuntu.com/ubuntu/ bionic main restricted

# deb-src http://de.archive.ubuntu.com/ubuntu/ bionic main restricted

## Major bug fix updates produced after the final release of the

## distribution.

deb http://de.archive.ubuntu.com/ubuntu/ bionic-updates main restricted

# deb-src http://de.archive.ubuntu.com/ubuntu/ bionic-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu

## team. Also, please note that software in universe WILL NOT receive any

## review or updates from the Ubuntu security team.

deb http://de.archive.ubuntu.com/ubuntu/ bionic universe

# deb-src http://de.archive.ubuntu.com/ubuntu/ bionic universe

deb http://de.archive.ubuntu.com/ubuntu/ bionic-updates universe

# deb-src http://de.archive.ubuntu.com/ubuntu/ bionic-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu

## team, and may not be under a free licence. Please satisfy yourself as to

## your rights to use the software. Also, please note that software in

## multiverse WILL NOT receive any review or updates from the Ubuntu

## security team.

deb http://de.archive.ubuntu.com/ubuntu/ bionic multiverse

# deb-src http://de.archive.ubuntu.com/ubuntu/ bionic multiverse

deb http://de.archive.ubuntu.com/ubuntu/ bionic-updates multiverse

# deb-src http://de.archive.ubuntu.com/ubuntu/ bionic-updates multiverse

## N.B. software from this repository may not have been tested as

## extensively as that contained in the main release, although it includes

## newer versions of some applications which may provide useful features.

## Also, please note that software in backports WILL NOT receive any review

## or updates from the Ubuntu security team.

deb http://de.archive.ubuntu.com/ubuntu/ bionic-backports main restricted universe multiverse

# deb-src http://de.archive.ubuntu.com/ubuntu/ bionic-backports main restricted universe multiverse

## Uncomment the following two lines to add software from Canonical's

## 'partner' repository.

## This software is not part of Ubuntu, but is offered by Canonical and the

## respective vendors as a service to Ubuntu users.

# deb http://archive.canonical.com/ubuntu bionic partner

# deb-src http://archive.canonical.com/ubuntu bionic partner

deb http://security.ubuntu.com/ubuntu bionic-security main restricted

# deb-src http://security.ubuntu.com/ubuntu bionic-security main restricted

deb http://security.ubuntu.com/ubuntu bionic-security universe

# deb-src http://security.ubuntu.com/ubuntu bionic-security universe

deb http://security.ubuntu.com/ubuntu bionic-security multiverse

# deb-src http://security.ubuntu.com/ubuntu bionic-security multiverse

Once, this is done, Please run the command:

# apt update

To update the apt package database and

# apt upgrade

To install the latest updates (if there are any). If you NOTICE any new kernel Packages being installed as part of the updates, it is advisable to do a reboot of system Please run the following command:

# sudo reboot

# Change the Default Shell

/bin/sh is a symlink to /bin/dash, however we need /bin/bash, not /bin/dash.

Therefore, we need this change :

# dpkg-reconfigure dash

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

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

# Disable AppArmor

AppArmor is a security extension (similar to SELinux) that should provide extended security. In my opinion, you don't need it to configure a secure system, and it usually causes more problems than advantages (think of it after you have done a week of trouble-shooting because some service wasn't working as expected, and then you find out that everything was ok, only AppArmor was causing the problem). Therefore, I disable it (this is a must if you want to install ISPConfig later on).

We can disable it like this:

# service apparmor stop

# update-rc.d -f apparmor remove

# apt remove apparmor apparmor-utils

# 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 when you run a physical server.

# apt install ntp

Just in case you run a virtual server then you can skip this step.

# Required Software

It is mostly required to have this software for most of your work while you install ISPConfig.

# apt install –y nano ( Just incase you are using minimal this is not pre-installed.)

# apt install –y ping (-do-)

# apt install –y tmux

#

# Install Postfix, Dovecot, MariaDB, rkhunter, and binutils

Whilst installing postfix, we need to make sure that sendmail(another mail transfer agent) is not installed and running. To check that run this command:

#service sendmail stop;

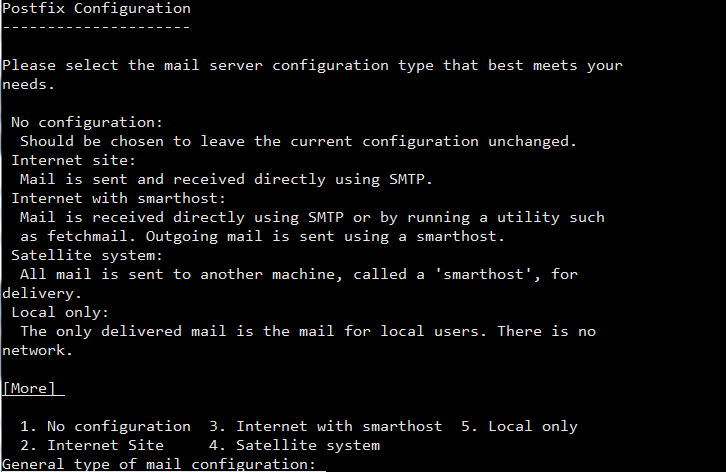
#update-rc.d -f sendmail remove

You should get the error message like (Ignore it):

Failed to stop sendmail.service: Unit sendmail.service not loaded.

Now we can install Postfix, Dovecot, MariaDB (as MySQL replacement), rkhunter, and binutils with a single command:

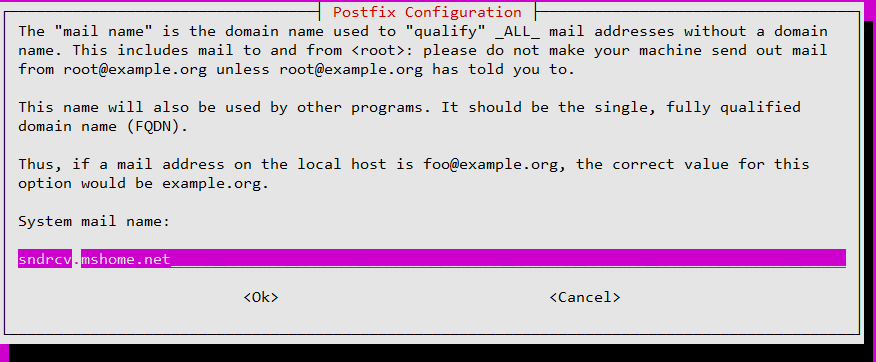
#apt -y install gettext postfix postfix-mysql postfix-doc mariadb-client mariadb-server openssl getmail4 rkhunter binutils dovecot-imapd dovecot-pop3d dovecot-mysql dovecot-sieve dovecot-lmtpd sudo



You will be asked the above questions:

General type of mail configuration: <-- Internet Site

System mail name: <-- sendrecv.mshome.net



Use an appropriate name of the server that you want to use it for sending and receiving mails.

System mail name: This is the base domain used to construct a valid email address when only the account portion of the address is given. For instance, the hostname of our server is mail.mshome.net, but we probably want to set the system mail name to mshome.net so that given the username user1, Postfix will use the address user1@ mshome.net

It is important that you use a subdomain as "system mail name" like server1.mshome.net or server1.yourdomain.com and not a domain that you want to use as email domain (e.g. yourdomain.tld) later.

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

# nano /etc/postfix/master.cf

Uncomment the submission and smtps sections as follows - add the line -o smtpd\_client\_restrictions=permit\_sasl\_authenticated,reject to both sections and leave everything thereafter commented:

[...] submission inet n - y - - 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 smtpd\_reject\_unlisted\_recipient=no

# -o smtpd\_client\_restrictions=$mua\_client\_restrictions # -o smtpd\_helo\_restrictions=$mua\_helo\_restrictions

# -o smtpd\_sender\_restrictions=$mua\_sender\_restrictions

# -o smtpd\_recipient\_restrictions=permit\_sasl\_authenticated,reject

# -o milter\_macro\_daemon\_name=ORIGINATING smtps inet n - y - - 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 smtpd\_reject\_unlisted\_recipient=no

# -o smtpd\_client\_restrictions=$mua\_client\_restrictions # -o smtpd\_helo\_restrictions=$mua\_helo\_restrictions

# -o smtpd\_sender\_restrictions=$mua\_sender\_restrictions

# -o smtpd\_recipient\_restrictions=permit\_sasl\_authenticated,reject

# -o milter\_macro\_daemon\_name=ORIGINATING

[...]

**NOTE:** The whitespaces in front of the "-o ....” lines are important!

We want MySQL to listen on all interfaces, not just localhost. Therefore, we edit /etc/mysql/mariadb.conf.d/50-server.cnf and comment out the line bind-address = 127.0.0.1:

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

[...]

Restart Postfix afterward:

service postfix restart

Please set a root password in MariaDB. Run:

# mysql\_secure\_installation

You will be asked these questions:

Enter current password for root (enter for none): <-- press enter

Set root password? [Y/n] <-- y

New password: <-- Enter the new MariaDB root password here

Re-enter new password: <-- Repeat the password Remove anonymous users? [Y/n] <-- y

Disallow root login remotely? [Y/n] <-- y Reload privilege tables now? [Y/n] <-- y

Set the password authentication method in MariaDB to native so we can use PHPMyAdmin later to connect as root user:

echo "update mysql.user set plugin = 'mysql\_native\_password' where user='root';" | mysql -u root

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

# nano /etc/mysql/debian.cnf

The MySQL root password that needs to be added is shown in read, in this example the password is

" 93$3m>ZJc&YVD+FEd#fS ".

# Automatically generated for Debian scripts. DO NOT TOUCH!

[client]

host = localhost

user = root

password = 93$3m>ZJc&YVD+FEd#fS

socket = /var/run/mysqld/mysqld.sock

[mysql\_upgrade]

host = localhost

user = root

password = 93$3m>ZJc&YVD+FEd#fS

socket = /var/run/mysqld/mysqld.sock basedir = /usr

Post to that restart MariaDB:

# service 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 tcp6 0 0 [::]:mysql [::]:\* LISTEN 30591/mysqld root@server1:~#

# Install Amavisd-new, SpamAssassin, and Clamav

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

# apt -y install amavisd-new spamassassin clamav clamav-daemon unzip bzip2 arj nomarch lzop cabextract 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 postgrey

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

# service spamassassin stop

# update-rc.d -f spamassassin remove

To start ClamAV use:

freshclam

service clamav-daemon start

The following error can be ignored on the first run of freshclam.

ERROR: /var/log/clamav/freshclam.log is locked by another process

ERROR: Problem with internal logger (UpdateLogFile = /var/log/clamav/freshclam.log).

The amavisd-new program has currently a bug in Ubuntu 18.04 which prevents that emails get signed with Dkim correctly. Run the following commands to patch amavisd-new.

cd /tmp

wget https://git.ispconfig.org/ispconfig/ispconfig3/raw/stable-3.1/helper\_scripts/ubuntu-amavisd-new-2.11.patch

cd /usr/sbin

cp -pf amavisd-new amavisd-new\_bak

patch < /tmp/ubuntu-amavisd-new-2.11.patch

Result :

patching file amavisd-new

Hunk #2 succeeded at 34363 (offset 1 line).

In case you get an error for thelast 'patch' command, then Ubuntu has probably fixed the issue in the meantime, so it should be safe to ignore that error then.

# Install Metronome XMPP Server (optional)

The Metronome XMPP Server provides an XMPP chat server. This step is optional, if you do not need a chat server, then you can skip this step. No other ISPConfig functions depend on this software.

Install the following packages with apt.

# apt -y install git lua5.1 liblua5.1-0-dev lua-filesystem libidn11-dev libssl-dev lua-zlib lua-expat lua-event lua-bitop lua-socket lua-sec luarocks luarocks

# luarocks install lpc

Add a shell user for Metronome.

# adduser --no-create-home --disabled-login --gecos 'Metronome' metronome

Download Metronome to the /opt directory and compile it.

# cd /opt; git clone https://github.com/maranda/metronome.git metronome

# cd ./metronome; ./configure --ostype=debian --prefix=/usr

# make

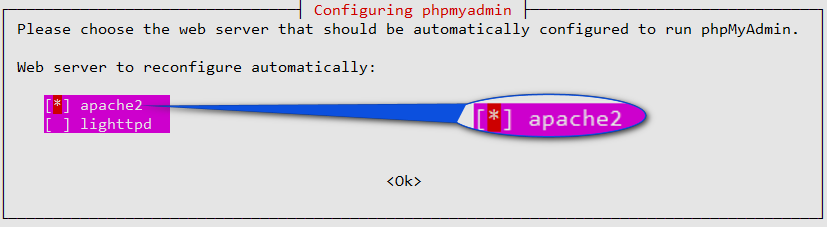
# make install

Metronome has now be installed to /opt/metronome.

# Install Apache, PHP, phpMyAdmin, FCGI, SuExec, Pear, and mcrypt

Apache 2.4, PHP 7.2, phpMyAdmin, FCGI, suExec, and Pear can be installed as follows:

# apt -y install apache2 apache2-doc apache2-utils libapache2-mod-php php7.2 php7.2-common php7.2-gd php7.2-mysql php7.2-imap phpmyadmin php7.2-cli php7.2-cgi libapache2-mod-fcgid apache2-suexec-pristine php-pear mcrypt  imagemagick libruby libapache2-mod-python php7.2-curl php7.2-intl php7.2-pspell php7.2-recode php7.2-sqlite3 php7.2-tidy php7.2-xmlrpc php7.2-xsl memcached php-memcache php-imagick php-gettext php7.2-zip php7.2-mbstring php-soap php7.2-soap

You will see the following question:

Web server to reconfigure automatically: <-- apache2

Configure database for phpmyadmin with dbconfig-common? <-- NO

MySQL application password for phpmyadmin: <-- Press enter

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 cgi

# a2enmod dav\_fs dav auth\_digest headers

To ensure that the server cannot be attacked through the [HTTPOXY](https://www.howtoforge.com/tutorial/httpoxy-protect-your-server/) vulnerability, I will disable the HTTP\_PROXY header in apache globally.

Create a new httpoxy.conf file with nano:

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

Paste this content into the file:

<IfModule mod\_headers.c>

RequestHeader unset Proxy early

</IfModule>

Enable the config file by running:

a2enconf httpoxy

Restart Apache afterward:

service apache2 restart

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

nano /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: service apache2 restart

# PHP Opcode cache (optional)

OPcache improves PHP performance by storing precompiled script bytecode in shared memory, thereby removing the need for PHP to load and parse scripts on each request.Opcache is a free PHP opcode cacher for caching and optimizing PHP intermediate code.

APCU can be installed as follows:

# apt -y install php7.2-opcache php-apcu

Again restart Apache:

service apache2 restart

# PHP-FPM

To use PHP-FPM with Apache, we need the mod\_proxy\_fcgi Apache module, which is installed by default and needs just be enabled. We can install PHP-FPM and as follows:

apt -y install php7.2-fpm

Make sure you enable the modules and restart Apache:

a2enmod actions proxy\_fcgi alias

service apache2 restart

# Install HHVM (HipHop Virtual Machine), (optional)

In this step, we will install HHVM with apt. HHVM is a fast PHP engine developed by Facebook.

apt -y install hhvm

# Install Let's Encrypt

ISPConfig 3.1 has built-in support for the free SSL Certificate Authority Let's encrypt. The Let's Encrypt function allows you to create free SSL Certificates for your website in ISPConfig.

Now we will add support for Let's encrypt.

apt -y install certbot

# certbot –version

Result : certbot 0.23.0

# Install Mailman

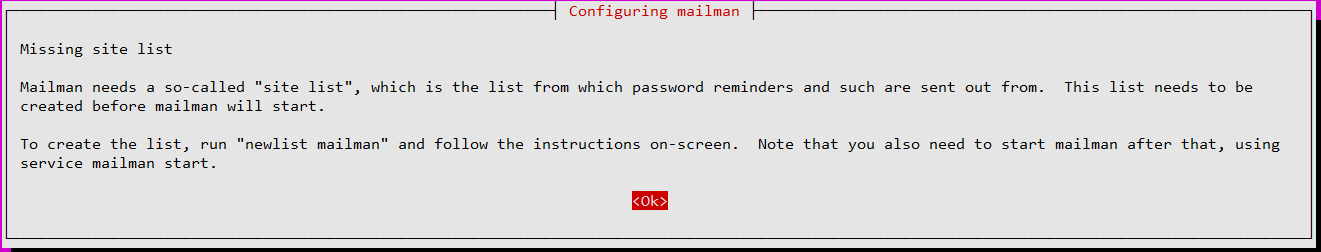
Within ISPConfig you can use GNU Mailing List Manager as an integrated feature to manage (create/modify/delete) mailing lists. Install Mailman as follows:

apt -y install mailman

Select the language of your Choice:

Languages to Chosen: en (English)

Missing site list <-- Ok





The above errors can be ignored for the time being as we need to create a mailing list.

Can be done through following command :

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...

nano /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 command :

newaliases

Afterward and restart Postfix:

service postfix restart

Finally, we must enable the Mailman Apache configuration:

ln -s /etc/mailman/apache.conf /etc/apache2/conf-available/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>/cgibin/mailman/admin/<listname>, and the 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.

Activate the configuration with:

a2enconf mailman

Restart Apache afterward:

service apache2 restart

Then start the Mailman daemon:

service mailman start

You might notice that the error below is gone now ☺ .



# Install PureFTPd and Quota(optional)

PureFTPd and quota can be installed with the following command:

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

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

[...]

File specified for transfer logs, in Apache format:

# cat /etc/pure-ftpd/conf/AltLog

clf:/var/log/pure-ftpd/transfer.log

Specified configuration file for MySQL:

# cat /etc/pure-ftpd/conf/MySQLConfigFile

/etc/pure-ftpd/db/mysql.conf

Anonymous users are denied access:

# cat /etc/pure-ftpd/conf/NoAnonymous

yes

Now you need to complete the configuration. To begin with, we prohibit UNIX authentication:

# echo no > /etc/pure-ftpd/conf/UnixAuthentication

Then disable PAM authentication:

# echo no > /etc/pure-ftpd/conf/PAMAuthentication

Restrict the user to their home directory:

# echo "yes" > /etc/pure-ftpd/conf/ChrootEveryone

# cat /etc/pure-ftpd/conf/ChrootEveryone

yes

We indicate the range of ports for passive connections:

# echo "40110 40210" > /etc/pure-ftpd/conf/PassivePortRange

# cat /etc/pure-ftpd/conf/PassivePortRange

40110 40210

P.S. : Do not forget to open the necessary ports in the firewall later.

Now We will configure WebUI (Optional):

Go to the web server file directory:

# cd /var/www/sitename OR

#cd /var/www/clients/client1/web1/web

( incase using ISPConfig you need to use an appropriate directory for each customer.)

Download the web interface files from the githab:

git clone <https://github.com/mazay/pure-ftpd-webui.git>

Go to the downloaded directory pure-ftpd-webui :

# cd pure-ftpd-webui

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

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

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

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

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

Now restart PureFTPd:

service 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 /):

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> /dev/mapper/server1--vg-root / ext4 errors=remountro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0 1 /dev/mapper/server1--vg-swap\_1 none swap sw 0 0

/dev/fd0 /media/floppy0 auto rw,user,noauto,exec,utf8 0 0 To enable quota, run these commands:

mount -o remount /

quotacheck -avugm quotaon -avug

Which will show the following output:

root@server1:/opt/metronome# quotacheck -avugm quotacheck: Scanning /dev/mapper/server1--vg-root [/] done quotacheck: Cannot stat old user quota file //quota.user: No such file or directory.

Usage will not be subtracted. quotacheck: Cannot stat old group quota file //quota.group: No such file or directory. Usage will not be subtracted.

quotacheck: Cannot stat old user quota file //quota.user: No such file or directory.

Usage will not be subtracted. quotacheck: Cannot stat old group quota file //quota.group: No such file or directory. Usage will not be subtracted.

quotacheck: Checked 13602 directories and 96597 files quotacheck: Old file not found. quotacheck: Old file not found.

root@server1:/opt/metronome# quotaon -avug

/dev/mapper/server1--vg-root [/]: group quotas turned on /dev/mapper/server1--vg-root [/]: user quotas turned on

# Install BIND DNS Server

BIND can be installed as follows:

apt -y install bind9 dnsutils haveged

Enable and start the haveged Daemon:

systemctl enable haveged

systemctl start haveged

# Install Vlogger, Webalizer, and AWStats

Vlogger, Webalizer, and AWStats can be installed as follows:

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

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

# 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 -y install build-essential autoconf automake1.11 libtool flex bison debhelper binutils

cd /tmp

wget http://olivier.sessink.nl/jailkit/jailkit-2.20.tar.gz

tar xvfz jailkit-2.20.tar.gz

cd jailkit-2.20

echo 5 > debian/compat

Then build the jailkit package by running this command:

./debian/rules binary

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

cd ..  
dpkg -i jailkit\_2.20-1\_amd64.deb

rm -rf jailkit-2.19\*

# Install fail2ban

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

apt -y install fail2ban

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

nano /etc/fail2ban/jail.local

[pure-ftpd]

enabled = true

port = ftp

filter = pure-ftpd

logpath = /var/log/syslog

maxretry = 3

[dovecot]

enabled = true

filter = dovecot

action = iptables-multiport[name=dovecot-pop3imap, port="pop3,pop3s,imap,imaps", protocol=tcp]

logpath = /var/log/mail.log

maxretry = 5

[postfix]

enabled = true

port = smtp

filter = postfix

logpath = /var/log/mail.log

maxretry = 3

Restart fail2ban afterwards:

service fail2ban restart

# Install UFW

To install the UFW firewall, run this apt command:

apt install ufw

# Install Roundcube Webmail

To install Roundcube Webmail, run:

apt-get -y install roundcube roundcube-core roundcube-mysql roundcube-plugins javascript-common libjs-jquery-mousewheel php-net-sieve tinymce

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 RoundCube apache configuration file.

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

and remove the # in front of the Alias line, then add the second Alias line for /webmail and add the line "AddType application/x-httpd- php .php" right after the "<Directory /var/lib/roundcube>" line:

# Those aliases do not work properly with several hosts on your apache server  
# Uncomment them to use it or adapt them to your configuration  
Alias /roundcube /var/lib/roundcube  
Alias /webmail /var/lib/roundcube

[...]

<Directory /var/lib/roundcube>

AddType application/x-httpd-php .php

[...]

Post to that restart apache :

service apache2 restart

Then edit the RoundCube config.inc.php configuration file:

nano /etc/roundcube/config.inc.php

Now change the default host to localhost:

$config['default\_host'] = 'localhost';

This prevents that Roundcube will show server name input field in the login form.

# Install ISPConfig 3.1

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

cd /tmp   
wget -O ispconfig.tar.gz https://git.ispconfig.org/ispconfig/ispconfig3/repository/archive.tar.gz?ref=stable-3.1  
q  
cd ispconfig3\*/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.

# php -q install.php

--------------------------------------------------------------------------------  
\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_ \_\_ \_ \_\_\_\_  
|\_ \_/ \_\_\_| \_\_\_ \ / \_\_ \ / \_(\_) /\_\_ \  
| | \ `--.| |\_/ / | / \/ \_\_\_ \_ \_\_ | |\_ \_ \_\_ \_ \_/ /  
| | `--. \ \_\_/ | | / \_ \| '\_ \| \_| |/ \_` | |\_ |  
\_| |\_/\\_\_/ / | | \\_\_/\ (\_) | | | | | | | (\_| | \_\_\_\ \  
\\_\_\_/\\_\_\_\_/\\_| \\_\_\_\_/\\_\_\_/|\_| |\_|\_| |\_|\\_\_, | \\_\_\_\_/  
\_\_/ |  
|\_\_\_/  
--------------------------------------------------------------------------------

>> Initial configuration

Operating System: Ubuntu 18.04 (Bionic Beaver)

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]: <-- Hit Enter

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

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

MySQL server hostname [localhost]:  <-- Hit Enter

MySQL server port [3306]:  <-- Hit Enter

MySQL root username [root]:  <-- Hit Enter

MySQL root password []:  <-- Enter your MySQL root password

MySQL database to create [dbispconfig]:   <-- Hit Enter

MySQL charset [utf8]:  <-- Hit Enter

Configuring Postgrey  
Configuring Postfix  
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 2 letter country code  
State or Province Name (full name) [Some-State]: <-- Enter the name of the  state  
Locality Name (eg, city) []: <-- Enter your city  
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter company name   
Organizational Unit Name (eg, section) []:  <-- Hit Enter  
Common Name (e.g. server FQDN or YOUR name) []: <-- Enter the server hostname,

in my case: sndrcv.mshome.net  
Email Address []:  <-- Hit Enter  
Configuring Mailman  
Configuring Dovecot  
Configuring Spamassassin  
Configuring Amavisd  
Configuring Getmail  
Configuring BIND  
Configuring Jailkit  
Configuring Pureftpd  
Configuring Apache  
Configuring vlogger  
Configuring Metronome XMPP Server  
writing new private key to 'localhost.key'  
-----  
Country Name (2 letter code) [AU]:  <-- Enter 2 letter country code  
Locality Name (eg, city) []:  <-- Enter your city  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:  <-- Enter company name   
Organizational Unit Name (eg, section) []:  <-- Hit Enter  
Common Name (e.g. server FQDN or YOUR name) [sndrcv.mshome.net]: <-- Enter the server hostname,

in my case: sndrcv.mshome.net  
Email Address []:  <-- Hit Enter

Configuring Ubuntu Firewall  
Configuring Fail2ban  
[INFO] service OpenVZ not detected  
Configuring Apps vhost  
Installing ISPConfig  
ISPConfig Port [8080]:

Admin password [admin]:

Do you want a secure (SSL) connection to the ISPConfig web interface (y,n) [y]: <-- Hit 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 2 letter country code  
State or Province Name (full name) [Some-State]: <-- Enter the name of the  state  
Locality Name (eg, city) []: <-- Enter your city  
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter company name or press enter  
Organizational Unit Name (eg, section) []: <-- Hit Enter  
Common Name (e.g. server FQDN or YOUR name) []: <-- Enter the server hostname, in my case: server1.example.com  
Email Address []: <-- Hit Enter

Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []: <-- Hit Enter  
An optional company name []: <-- Hit Enter  
writing RSA key

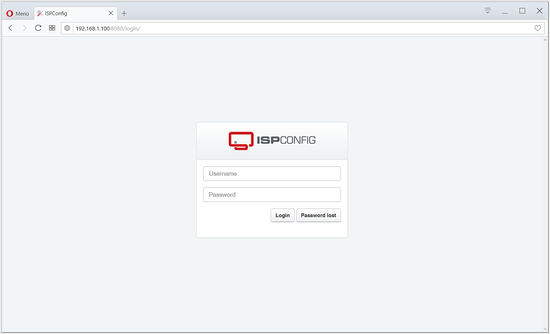
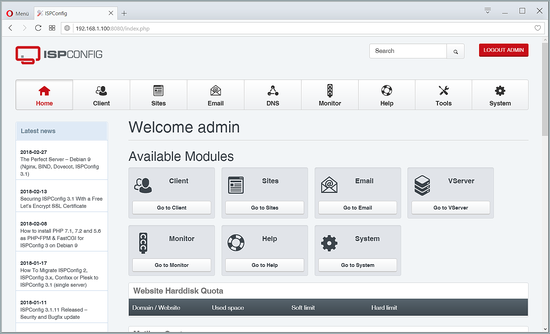
Configuring DBServer  
Installing ISPConfig crontab  
no crontab for root  
no crontab for getmail  
Detect IP addresses  
Restarting services ...  
Installation completed.

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

Cheers, you can access ISPConfig3.1 with hostname url :

https://server1.example.com:8080/ OR https://192.168.1.x:8080/

Log in with the username admin and the password admin

[](https://www.howtoforge.com/images/ubuntu_18.04_perfect_server_apache/big/ubuntu-1804-ispconfig-login.png)  
  
[](https://www.howtoforge.com/images/ubuntu_18.04_perfect_server_apache/big/ispconfig-ubuntu-dashboard.png)

The system is now ready for use.

# 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: root /vishal  
Password: Passw0rd

This user has sudo rights.

**ISPConfig Login**

Username: admin  
Password: $GvY?eLPHqrxCk2j~+5d

**MySQL Login**

Username: root  
Password: 93$3m>ZJc&YVD+FEd#fS

Roundcube Login

Username: root

Password : ebt2m#KW^uW#dZQ>c7xd

Certificate Chellenge Password : ~W28S3$b4cVAL#NKqE#B

Mailman credentials : X~v7%mYF4B8f9Hd@G?SK

Phpmyadmin

User: phpmyadmin (non-root)

Password: 93$3m>ZJc&YVD+FEd#fS

User: sqladm (root=)

Password : ~fk5r#z$4+?A&^JZ9ZK3

The IP of the VM is DHCP based and can be allocated by dhcp else you can keep a statice one.It can be changed in the file /etc/netplan/50-cloud-init.yaml. Please change all the above passwords to secure the virtual machine.