Linux
ISPConfig3 and Wheezy

These are my personal notes for installing ISPConfig3 on our servers. This is a "recipe" type of howto, with very little information on what is going on and why. Since most of it is taken from the excellent articles by Falko on howtofoge, I recommend reading his documents if you want more information. This is definitely modified from his work to fit our requirements. This works for us, but if you do not understand what we're doing or why, I recommend going to Falko's instruction sets and following his well commented howto. Following are direct links to his original works:

- http://www.howtoforge.com/perfect-server-debian-wheezy-apache2-bind-dovecot-ispconfig-3
- http://www.howtoforge.com/using-roundcube-webmail-with-ispconfig-3-on-debian-wheezy-apache2

Our modifications are:

- use mariadb instead of mysql
- no install of ntp or ntpdate as we are working on a Xen DOMU, whose clock is controlled by the DOM0 (which has ntp on it)
- no information on how to create a Debian Install. If you can't do that on your own, read Falko's work. Assumes a base image of Debian Wheezy already installed
- unlike Falko, I want to install everything first, then configure it all.
- I HATE vim. joe is used throughout.
- all web sites and e-mail will be stored in /home/hosting

Preliminary Instructions:

- Do a base setup of the server, including any special packages you need. Create a 10G root partition, and set the remaining space to LVM
- Create a Logical Volume for /home to store the web site, e-mail and ssh access. Be mildly conservative; with minimal downtime, it can be increased.

```
# ensure hostname set correctly. Use FQDN for /etc/hostname. Edit file
s
joe /etc/hosts /etc/hostname /etc/mailname
# reload hostname for session (prompt does not change)
hostname -F /etc/hostname
# add contrib non-free as repositories for apt. This assumes if main i
s at the end of the line, it is the only one listed
# saves original file as /etc/apt/sources.list.bak
sed -i'.bak' 's/main$/main contrib non-free/' /etc/apt/sources.list
# create an apt entry for mariadb (or download mariadb.list to /etc/ap
t/sources.list.d/maria.list)
echo deb http://mirror.jmu.edu/pub/mariadb/repo/5.5/debian wheezy main
 > /etc/apt/sources.list.d/maria.list
echo deb-src http://mirror.jmu.edu/pub/mariadb/repo/5.5/debian wheezy
main >> /etc/apt/sources.list.d/maria.list
```

```
# and get the key for the mariadb repository
sudo apt-key adv --recv-
keys --keyserver keyserver.ubuntu.com 0xcbcb082a1bb943db
# Add Daily Data repository (if you are using that)
echo '#' > /etc/apt/sources.list.d/dailydata.list
echo '# Daily Data Repository' >> /etc/apt/sources.list.d/dailydata.li
st
echo '#' >> /etc/apt/sources.list.d/dailydata.list
echo 'deb http://debian.dailydata.net/debian_repository /' >> /etc/apt
/sources.list.d/dailydata.list
# add list of all servers in the cluster to /etc/hosts. Example follow
s, but make sure you
# change the IP's and names to match your own setup
cp /etc/hosts /etc/hosts.bak
cat '192.168.1.5 mail.example.com mail' >> /etc/hosts
cat '192.168.1.6 web.example.com web' >> /etc/hosts
cat '192.168.1.5 ns.example.com ns' >> /etc/hosts

#
# Install common packages for all of servers. NOTE: be sure to remembe
r the mySQL database root password
apt-get --purge install bzip2 debsums dnsutils fail2ban mariadb-client
 mariadb-server mcrypt openssh-
server php5-cli php5-mcrypt php5-mysql postfix postfix-doc \
                         rkhunter ssh ssl-cert sudo wget zip
## 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
# Edit /etc/mysql/my.cnf and comment out the line
# bind-address = 127.0.0.1
# by placing a pound sign in front of it. You can secure mariadb via i
ptables
sed -i'.bak' 's/^bind-address/# bind-address/' /etc/mysql/my.cnf
# secure mysql. This is interactive. Remove all the unneeded gunk inst
alled by default.
mysql_secure_installation

# If you are using DHCP on an internal connection and do NOT want it t
o update resolv.conf,
# run the following. You should then restart the DHCP server and manua
lly set your resolv.conf
echo '#! /bin/bash' < /etc/dhcp3/dhclient-enter-hooks.d/nodnsupdate
echo 'make_resolv_conf(){' << /etc/dhcp3/dhclient-enter-
hooks.d/nodnsupdate
echo ' :' << /etc/dhcp3/dhclient-enter-hooks.d/nodnsupdate
echo '}' << /etc/dhcp3/dhclient-enter-hooks.d/nodnsupdate
chmod +x /etc/dhcp3/dhclient-enter-hooks.d/nodnsupdate
ln -s /etc/dhcp3/dhclient-enter-hooks.d/nodnsupdate /etc/dhcp/dhclient-
```

```
enter-hooks.d/nodnsupdate
# kill dash. It really messes up a lot of stuff
dpkg-reconfigure dash
## Use dash as the default system shell (/bin/sh)? <-- No
```

Server Specific installation and instructions

NOTE: Items marked with double pound signs at the beginning are instructions on what to answer to package installation questions

Choose which type of server you are installing, and choose only the ones below. ie, if you are installing a stand alone mail server, do the "for mail server", but if it will be a mail and DNS server, do both installs

DNS Server Installation and Configuration

```
apt-get --purge install bind9 geoip-database zip
# there is no configuration needed at this time
```

Web Server Install and Configuration

```
apt-get --purge install apache2 apache2-doc apache2-mpm-prefork apache
2-suexec apache2-utils apache2.2-common autoconf automake1.9 awstats b
ison \
                        build-essential debhelper flex imagemagick lib
apache2-mod-fastcgi libapache2-mod-fcgid libapache2-mod-
php5 libapache2-mod-python \
                        libapache2-mod-ruby libapache2-mod-suphp libex
pat1 libruby libtool php-auth php-
pear php5 php5-cgi php5-common php5-curl php5-gd \
                        php5-imagick php5-imap phpmyadmin pure-ftpd-co
mmon pure-ftpd-mysql quota quotatool roundcube roundcube-
plugins roundcube-plugins-extra \
                        squirrelmail ssl-cert vlogger webalizer zip li
bapache2-mod-perl2 libapache2-reload-perl libbsd-resource-
perl libdevel-symdump-perl

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

```
## Configure database for roundcube with dbconfig-common? <-- Yes
## Database type to be used by roundcube: <-- mysql
## Password of the database's administrative user: <-- yourrootsqlpass
word (the password of the MySQL root user)
## MySQL application password for roundcube: <-- roundcubesqlpassword
## Password confirmation: <-- roundcubesqlpassword


# install jailkit from source
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
cd ..
dpkg -i jailkit_2.15-1_*.deb
rm -rf jailkit-2.15*

# fix pure-ftp
joe /etc/default/pure-ftpd-
common # ensure these two lines set correctly
STANDALONE_OR_INETD=standalone
VIRTUALCHROOT=true
# set up TLS for pure-ftpd
echo 1 > /etc/pure-ftpd/conf/TLS
mkdir -p /etc/ssl/private/
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]: <-- Ent
er your Organization Name (e.g., the name of your company).
## Organizational Unit Name (eg, section) []: <-- Enter your Organizat
ional Unit Name (e.g. "IT Department").
## Common Name (eg, YOUR name) []: <-- Enter the Fully Qualified Domai
n Name of the system (e.g. "server1.example.com").
## Email Address []: <-- Enter your Email Address.
chmod 600 /etc/ssl/private/pure-ftpd.pem

# kill awstats cron job, let ISPConfig do it
joe /etc/cron.d/awstats # comment out everything, every single line in
 the file

# configure squirrelmail
squirrelmail-configure # Configure Squirrelmail
 ## set Predefined (Option D) to dovecot, SAVE your work then quit
```

```
# configure roundcube. Also, add webmail aliase for all domains
joe /etc/apache2/conf.d/roundcube # replace the top four lines with th
ese five, then replace the  sec

# 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/program/js/tiny_mce/ /usr/share/tinymce/www/
Alias /roundcube /var/lib/roundcube
Alias /webmail /var/lib/roundcube

# DO NOT SAVE. Now, replace the <Directory /var/lib/roundcube/> sectio
n with this
<Directory /var/lib/roundcube/>
  Options +FollowSymLinks
  DirectoryIndex index.php

  <IfModule mod_php5.c>
    AddType application/x-httpd-php .php

    php_flag magic_quotes_gpc Off
    php_flag track_vars On
    php_flag register_globals Off
    php_value include_path .:/usr/share/php
  </IfModule>

  # This is needed to parse /var/lib/roundcube/.htaccess. See its
  # content before setting AllowOverride to None.
  AllowOverride All
  order allow,deny
  allow from all
</Directory>


joe /etc/roundcube/main.inc.php # find and edit the following line
$rcmail_config['default_host'] = 'localhost';

# set up fail2ban. NOTE: files are stored here as attachments also
# create main fail2ban conf file
echo '[pureftpd]' > /etc/fail2ban/jail.local
echo 'enabled = true' >> /etc/fail2ban/jail.local
echo 'port = ftp' >> /etc/fail2ban/jail.local
echo 'filter = pureftpd' >> /etc/fail2ban/jail.local
echo 'logpath = /var/log/syslog' >> /etc/fail2ban/jail.local
echo 'maxretry = 3' >> /etc/fail2ban/jail.local
echo '' >> /etc/fail2ban/jail.local
echo '[dovecot-pop3imap]' >> /etc/fail2ban/jail.local
echo 'enabled = true' >> /etc/fail2ban/jail.local
```

```
echo 'filter = dovecot-pop3imap' >> /etc/fail2ban/jail.local
echo 'action = iptables-multiport[name=dovecot-pop3imap, port="pop3,po
p3s,imap,imaps", protocol=tcp]' >> /etc/fail2ban/jail.local
echo 'logpath = /var/log/mail.log' >> /etc/fail2ban/jail.local
echo 'maxretry = 5' >> /etc/fail2ban/jail.local
echo '' >> /etc/fail2ban/jail.local
echo '[sasl]' >> /etc/fail2ban/jail.local
echo 'enabled = true' >> /etc/fail2ban/jail.local
echo 'port = smtp' >> /etc/fail2ban/jail.local
echo 'filter = sasl' >> /etc/fail2ban/jail.local
echo 'logpath = /var/log/mail.log' >> /etc/fail2ban/jail.local
echo 'maxretry = 3' >> /etc/fail2ban/jail.local
# create pureftpd fail2ban
echo '[Definition]' > /etc/fail2ban/filter.d/pureftpd.conf
echo 'failregex = .*pure-ftpd: \(.*@\) \[WARNING\] Authentication fail
ed for user.*' >> /etc/fail2ban/filter.d/pureftpd.conf
echo 'ignoreregex =' >> /etc/fail2ban/filter.d/pureftpd.conf
# create dovcot fail2ban
echo '[Definition]' > /etc/fail2ban/filter.d/dovecot-pop3imap.conf
echo 'failregex = (?: pop3-login|imap-login): .*(?:Authentication fail
ure|Aborted login \(auth failed|Aborted login \(tried to use disabled|
Disconnected \(auth failed|Aborted login \(\d+ authentication attempts
).*rip=(?P\S*),.*' >> /etc/fail2ban/filter.d/dovecot-pop3imap.conf
echo 'ignoreregex = '>> /etc/fail2ban/filter.d/dovecot-pop3imap.conf

# enable mods on Apache2
a2enmod suexec rewrite ssl actions include dav_fs dav auth_digest acti
ons fastcgi alias

# add squirrelmail link
ln -s /etc/squirrelmail/apache.conf /etc/apache2/conf.d/squirrelmail.c
onf
joe /etc/apache2/conf.d/squirrelmail.conf # change the following block
<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/squirrelm
ail:/var/lib/squirrelmail:/etc/hostname:/etc/mailname
   php_flag register_globals off
</IfModule>

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

joe /etc/apache2/mods-available/suphp.conf # replace lines to explicit
```

```
ly choose files for SuPHP
#    <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

joe /etc/mime.types # disable .rb extension
#application/x-ruby rb

# restart modified services
/etc/init.d/apache2 restart
/etc/init.d/pure-ftpd-mysql restart
/etc/init.d/fail2ban restart
/etc/init.d/mysql restart

# IF you will have another partition for web sites, prepare it and mou
nt it on /var/www
mkfs.ext4 -m0 -L somename /dev/path/to/partition
mount /dev/path/to/partition /mnt
/etc/init.d/apache2 stop
mv /var/www/* /mnt
umount /mnt
blkid # get the UUID of the partition
joe /etc/fstab
# assuming the UUID is the thing below, create this entry. Be sure and
 put a blank line at the end of the file
UUID=1b341475-b591-4dd4-bbac-372e7516dfac /var/www ext4 defaults,usrjq
uota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0 2
mount /var/www # mount the file system
# now, set up quota on /var/www
quotacheck -avugm
quotaon -avug
/etc/init.d/apache2 start
```

Mail Server Install and Configuration

```
apt-get --purge install amavisd-new apt-listchanges arj binutils cabex
tract clamav clamav-daemon clamav-docs daemon dovecot-imapd dovecot-
mysql dovecot-pop3d \
                        dovecot-sieve getmail4 libauthen-sasl-perl lib
io-socket-ssl-perl libio-string-perl libnet-dns-perl libnet-ident-
perl libnet-ldap-perl \
                        lzop mailman nomarch openssl postfix-
```

```
mysql quota quotatool spamassassin unzip zip zoo
## Languages to support: <-- en (English)
## Missing site list <-- Ok


# kill spamassassin since it is run through amavisd (probably already
stopped)
/etc/init.d/spamassassin stop
update-rc.d -f spamassassin remove



joe /etc/postfix/master.cf # replace the following lines, ie uncomment
 them
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

# mailman config
newlist mailman # Set up mailmain
## Enter the email of the person running the list: <-- admin email add
ress, e.g. listadmin@example.com
## Initial mailman password: <-- admin password for the mailman list
# copy output and paste into /etc/aliases
newaliases # update aliases database
# enable mailmain

ln -s /etc/mailman/apache.conf /etc/apache2/conf.d/mailman.conf
# This defines the alias /cgi-bin/mailman/ for all Apache vhosts, whic
h means you can access the Mailman admin interface for a list at
# http:///cgi-bin/mailman/admin/, and the web page for users of a mail
ing list can be found at
# http:///cgi-bin/mailman/listinfo/. Under http:///pipermail you can f
ind the mailing list archives.

# IF you will have another partition for email, prepare it and mount i
t on /var/vmail
# ispconfig will create a /var/vmail directory
mkfs.ext4 -m0 -L somename /dev/path/to/partition
mkdir /var/vmail
```

```
blkid # get the UUID of the partition
joe /etc/fstab
# assuming the UUID is the thing below, create this entry. Be sure and
 put a blank line at the end of the file
UUID=1b341475-b591-4dd4-bbac-372e7516dfac /var/vmail ext4 defaults,usr
jquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0 2
mount /var/vmail # mount the file system
# now, set up quota on /var/vmail
quotacheck -avugm
quotaon -avug
```

Unique solution ID: #1178
Author: Rod
Last update: 2013-10-30 03:08