راهنمای نصب ISPConfig3

برروی سیستم عامل دبیان

تابستان ۹۳

کریمی

وب سایت

وبلاگ

ISPConfig3 یک پنل کنترلی میزبانی وب است که اجازه پیکربندی سرویس های زیر را از طریق مرورگر وب می دهد:

Apache یا nginx web server، Postfix mail server، Courier یا Dovecot IMAP/POP3 Server ، MySQL ، BIND یا MyDNS nameserver، PureFTPD ، SpamAssassin، CalmAV و خیلی های دیگر .

نکته: در این نصب ما از Apache بجای nginx ، از BIND بجای MyDNS و از Dovecot بجای Courier استفاده می کنیم.

توضیح کامل هر یک از این سرویس ها در پیوست قرار دارد .

۱- احتیاجات :

- سیستم عامل دبیان (آخرین نسخه)
- ارتباط اینترنتی سریع

۲- نکته مهم:

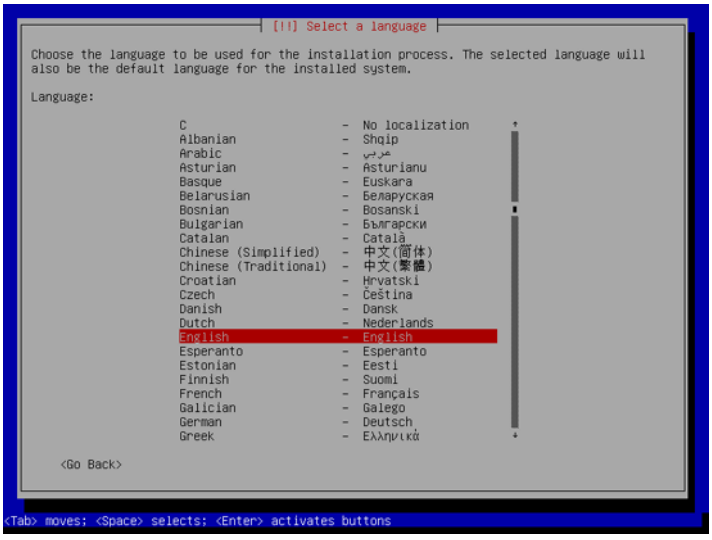
در این نوشتار ما از نام میزبان server1.example.com با آدرس IP: ۱۹۲,۱۶۸,۰,۱۰۰ و گیت وی ۱۹۲,۱۶۸,۰,۱ برای تنظیمات استفاده میکنیم .

۳- نصب سیستم عامل

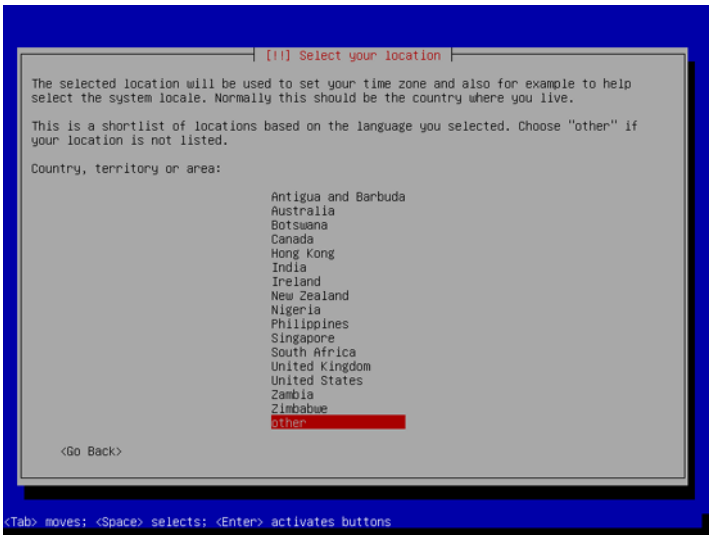
سی دی سیستم عامل را داخل درایو قرار داده و نصب را مطابق دستور پیش برید :

از بین یکی از دو گزینه Install و Graphical Install یکی را به دلخواه انتخاب کنید (اگر نصب گرافیکی را ترجیح میدهید از Graphical install بهره برید).

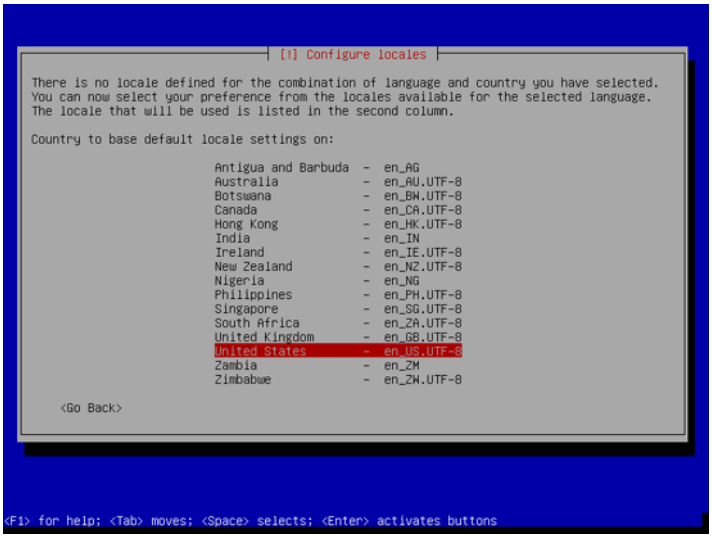
انتخاب زبان:



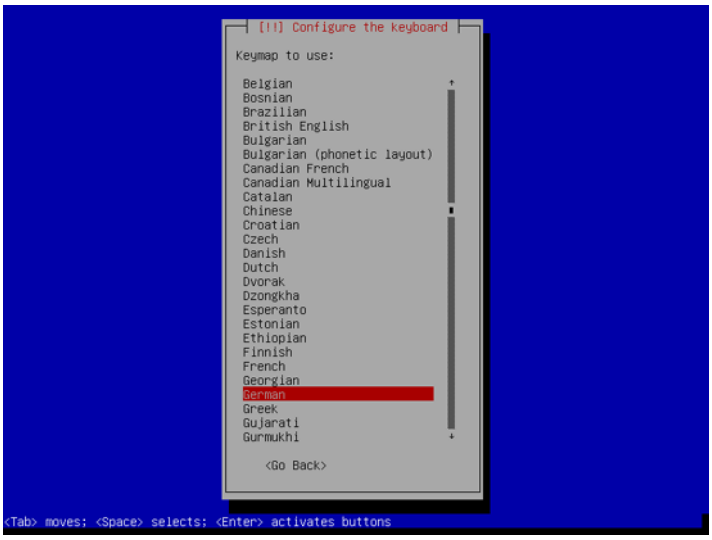
انتخاب موقعیت :



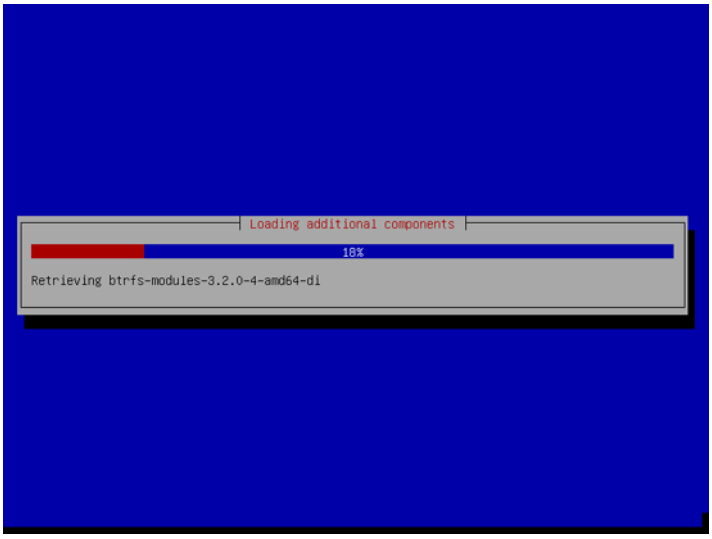
اگر زبان انتخابی و موقعیت با هم تطابق نداشته باشند (مثلا زبان انگلیسی و مکان آلمان) ، موقع نصب احتمالا با پیغامی مبنی براینکه : there is no locale defined for this combination **مواجه شوید . در این حالت مجبورید منطقه را به صورت دستی انتخاب کنید :**

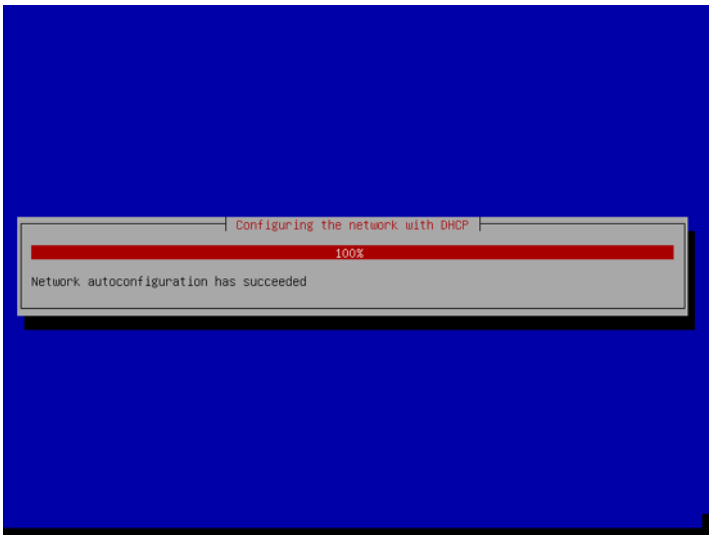


انتخاب layout **صفحه کلید :**

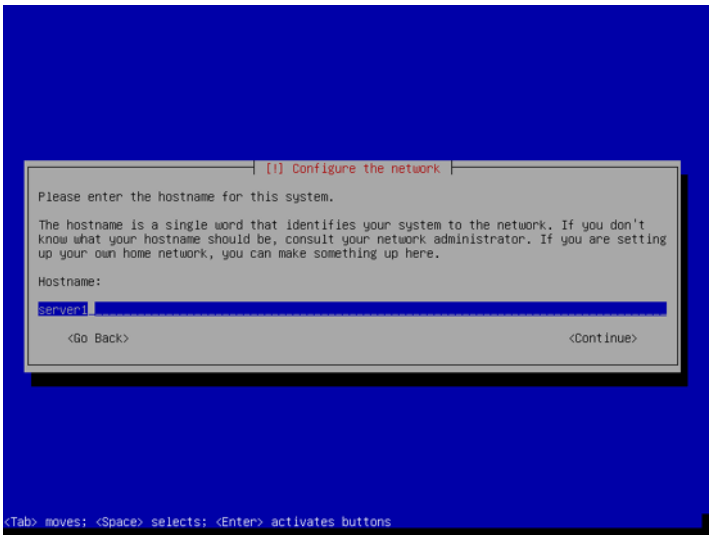


موقع نصب ، CD نصب و سخت افزارچک میشود و شبکه با DHCP پیکربندی میشود به شرط اینکه DHCP سروری در شبکه موجود باشد وگرنه باید بصورت استاتیک ثبت کنید .

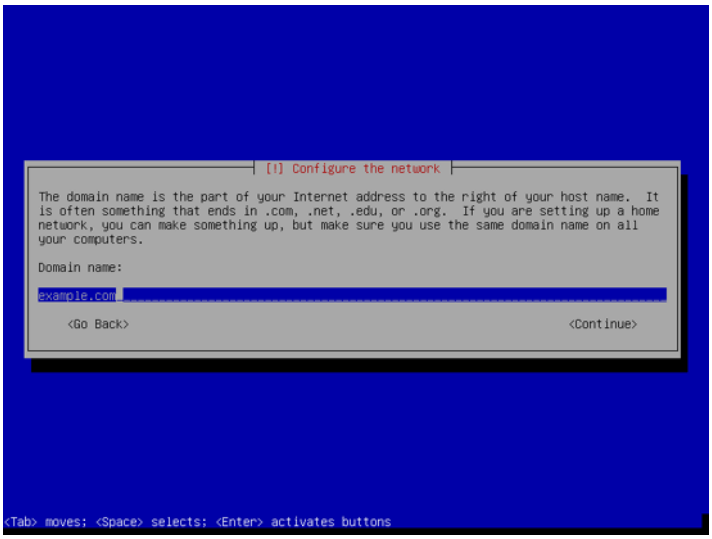




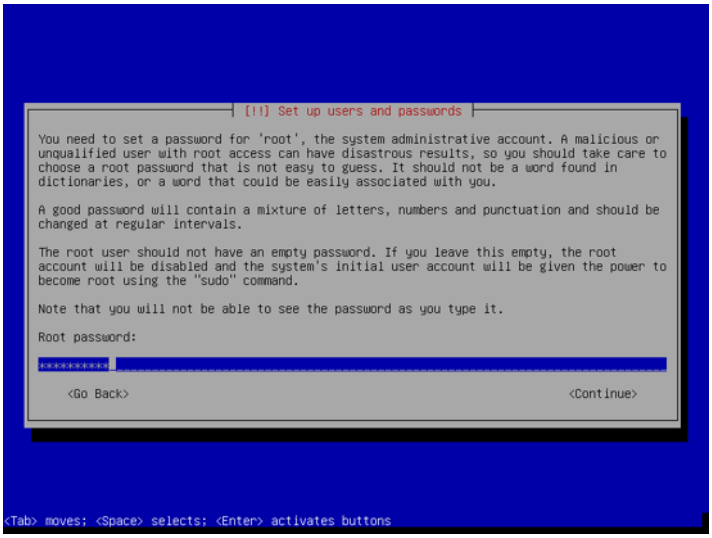
نام میزبان را وارد کنید . چون در این نوشتار ما سیستم را به نام server1.example.com **نامگذاری کردیم به همین خاطر** server1 **را وارد میکنیم .**



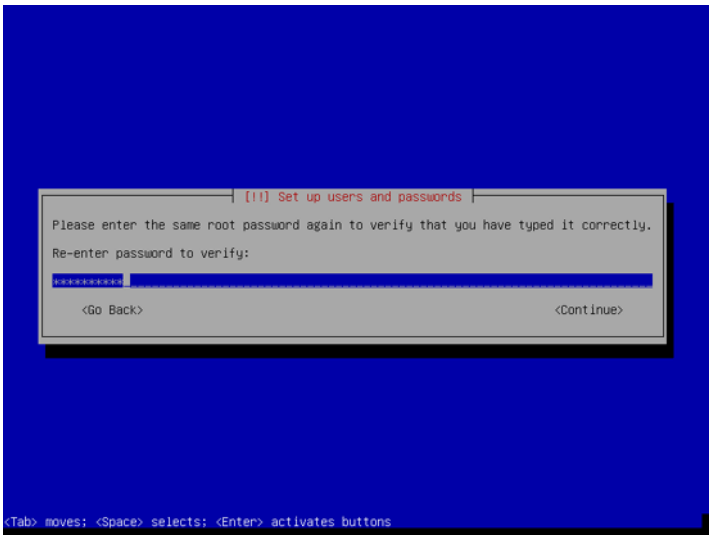
وارد کردن نام دامنه . در این نوشتار example.com



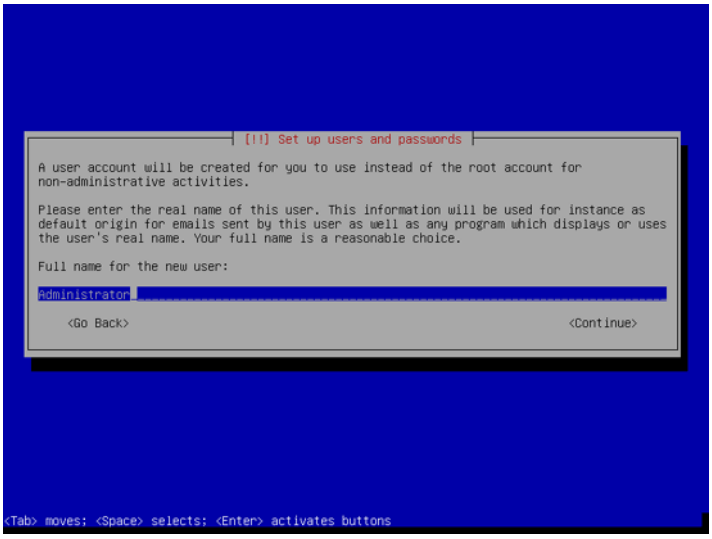
مرحله بعد ، تنظیم پسورد برای کاربر root:

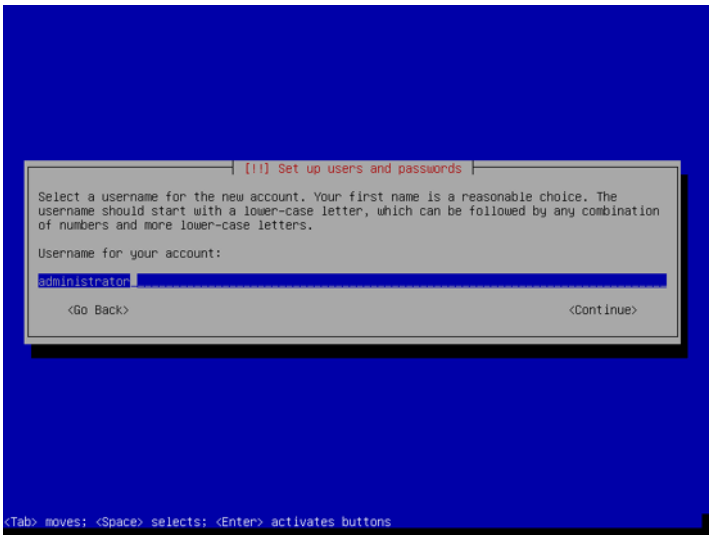


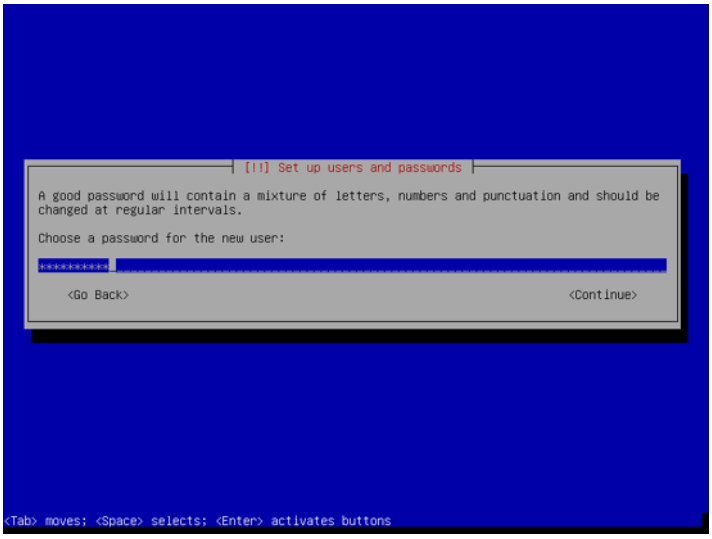
تایید رمز ورود :

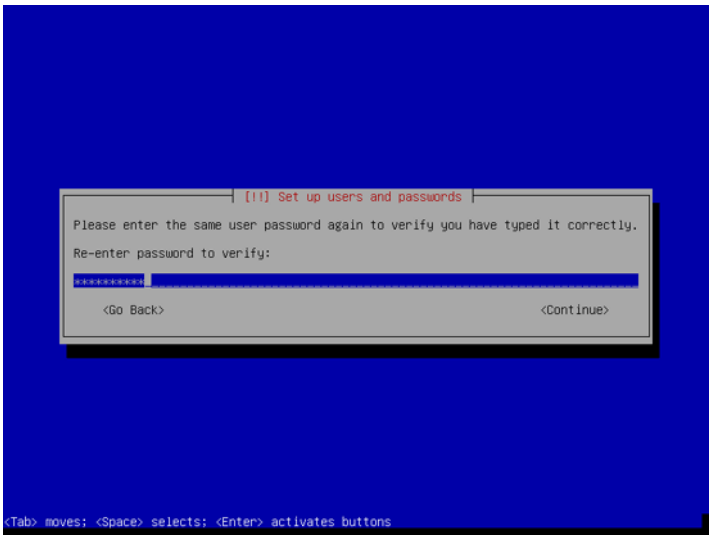


ایجاد حساب کاربری ، برای مثال میتوانید کاربری به نام administrator **ایجاد کنید فقط دقت داشته باشید نام کاربری** admin **در دیبان رزرو شده است .**

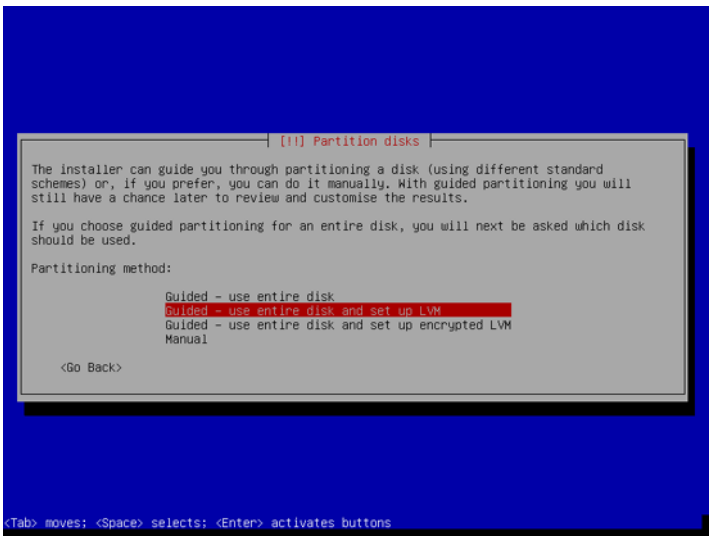



[!!] Set up users and passwords
Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.
Username for your account:
administraton
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

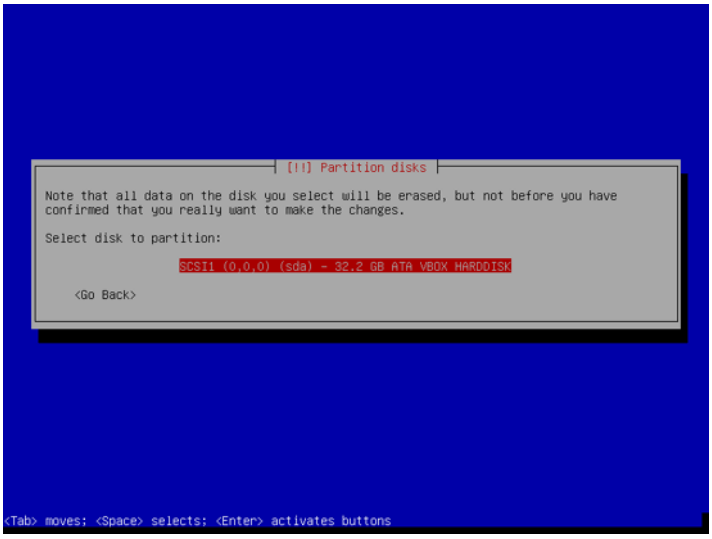

[!!] Set up users and passwords
A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.
Choose a password for the new user:
****
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons


[!!] Set up users and passwords
Please enter the same user password again to verify you have typed it correctly.
Re-enter password to verify:
****
<Go Back>
<Continue>
<Tab> moves; <Space> selects; <Enter> activates buttons

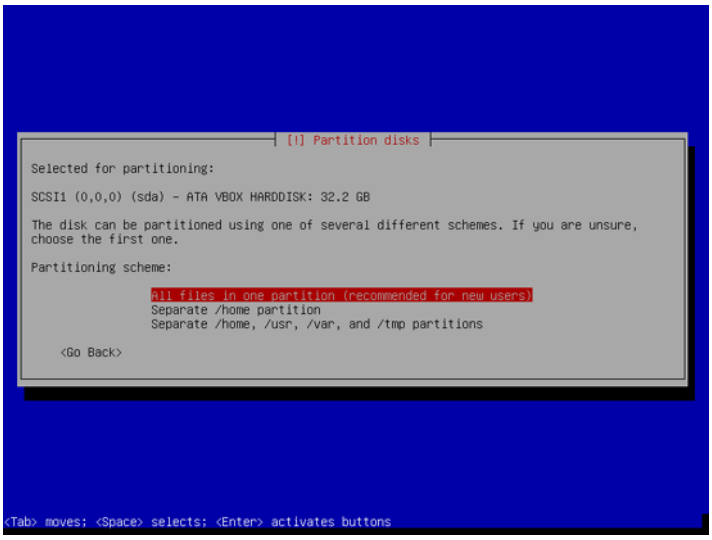
حال ، نیاز دارید تا هارددیسک را پارتیشن بندی کنید . راحت ترین روش انتخاب *Guided - use entire disk and set up LVM* میباشد که ۲ حجم منطقی ایجاد میکند یکی برای سیستم فایل / و دیگری برای swap . (البته بگم خودتون هم میتونید بنا به نیاز و دلخواهتون پارتیشن بندی رو به صورت دستی انجام دهید).



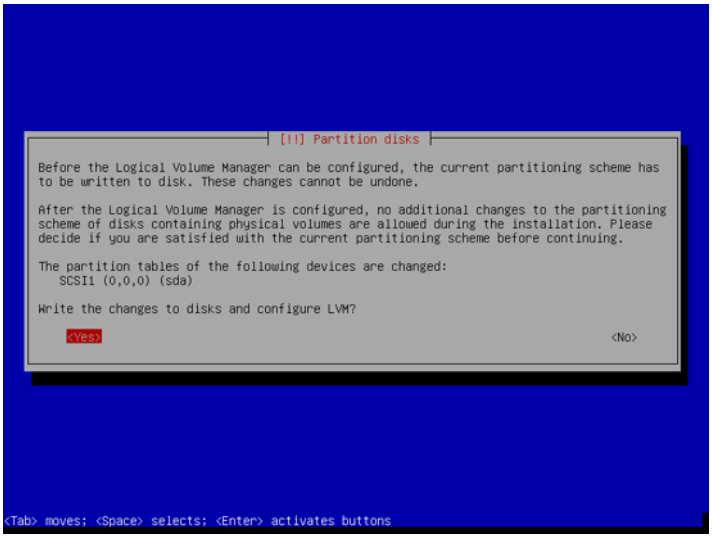
انتخاب دیسک :



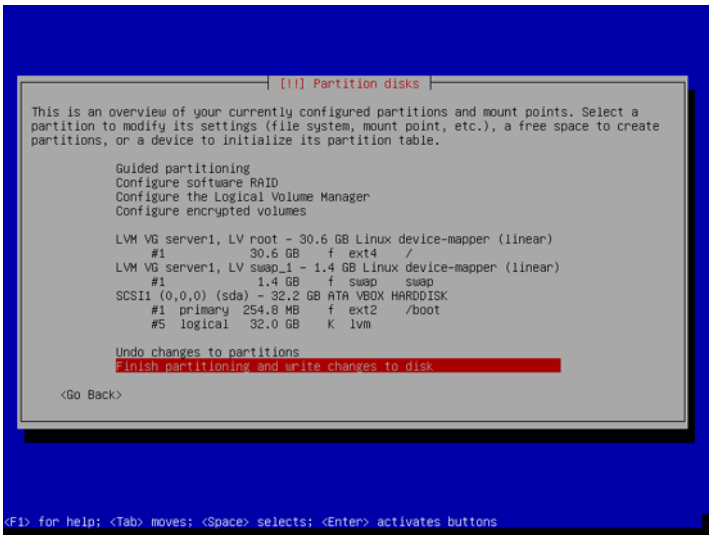
انتخاب نمای پارتیشن بندی . همانطور که قبلا اشاره شد ، ما گزینه All Files in one partition را انتخاب کردیم .



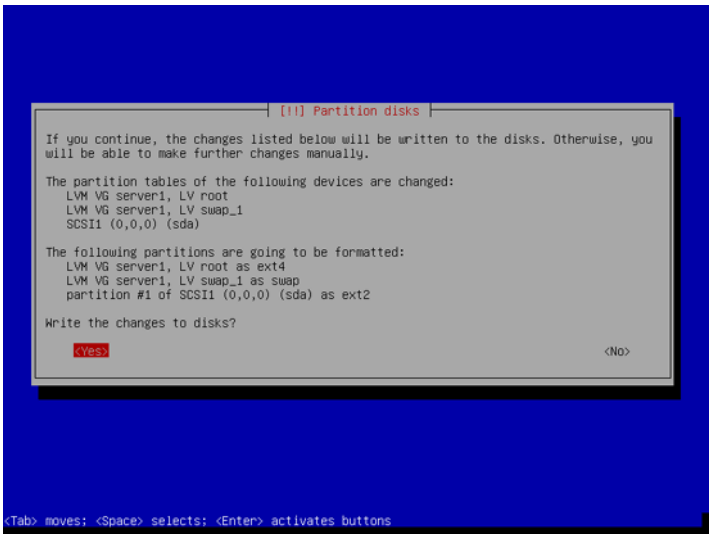
در جواب سوال *Write the changes to disks and configure LVM?* ***، گزینه Yes را انتخاب کنید.***



در انتها گزینه *Finish partitioning and write changes to disk* ***را انتخاب کنید .***



در مرحله بعدی Yes **را انتخاب میکنیم :**



در مرحله بعدی ، پارتیشن جدیدتان ایجاد و فرمت شده است . حال سیستم اصلی نصب شده است :

درمرحله بعد نیاز دارید تا apt را پیکربندی کنید .اگر از cd نصب سریع دبیان از طریق اینترنت استفاده کرده اید ، نیاز دارید از network mirror استفاده کنید . کشور network mirror را انتخاب کنید (معمولا کشوری که توزیع wheezy دبیان قرار دارد انتخاب می شود) . روش دیگر برای آپدیت کردن apt تعیین repository های دبیان در مسیر /etc/apt/sources.list می باشد.

به صورت پیش فرض شما به یک web server ، DNS server ، Mail server و یک پایگاه داده MySQL نیاز دارید اما فعلا هیچ یک را تنظیم نمی کنیم زیرا میخواهیم کنترل کاملی روی سیستم خود داشته باشیم. در واقع پکیج های مور دنیاز خود را به طور دستی بعدا نصب خواهیم کرد . در این قسمت Standard system utilities و SSH server را انتخاب می کنیم (برای اینکه بتوانیم از راه دور به سیستم وصل شویم).

بعد از نصب پکیج های انتخابی ، از شما پرسیده می شود که آیا مایل به نصب GRUB هستید که yes را انتخاب کنید :

Install the GRUB boot loader to the master boot record?

نصب سیستم عامل دبیان به پایان رسید.

۴- نصب سرور SSH

اگر در حین نصب سیستم ، سرور OpenSSH را نصب نکردید ، می توانید با دستور زیر آن را نصب کنید :

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

بعد از نصب این سرور می توانید با استفاده از نرم افزار های SSH Client همانند PuTTY از راه دور به سیستم وصل شوید و مابقی دستورات این نوشتار را ادامه دهید .

۵- نصب ویرایشگر vim

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

۶- پیکربندی شبکه :

اگر در مراحل نصب دبیان ، سیستم رو طوری تنظیم کردید که تنظیمات شبکه اش رو از طریق DHCP بگیرد ، حال باید آنرا تغییر دهید زیرا ما نیاز داریم که آدرس شبکه سرور مان استاتیک باشد . فایل رابط های شبکه را که در مسیر /etc/network/interfaces **قرار دارد ویرایش کنید و آدرس شبکه استاتیک مد نظرتان را وارد کنید .**

```
vim /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
```

حال سرویس شبکه خود را با دستور زیر دوباره بازنشانی کنید.

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

حال میزبان های سیستم خود را ثبت کنید .

```
vim /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
```

حال دستور زیر را اجرا کنید که از تنظیم میزبان ها مطمئن شوید.

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

دستورات زیر را هم می توانید اجرا کنید .

```
hostname
hostname -f
```

باید خروجی هر دو دستور *server1.example.com* ***را نشان دهند .***

۷- آپدیت کردن دبیان

اگر در فایل sources.list **، انباره** (repository) **های دبیان را** wheezy-updates **تنظیم کرده اید ، میتوانید با اجرای دستور زیر به راحتی دبیان را آپدیت کنید . سعی کنید که فایل** sources.list **شما همانند عبارات زیر تنظیم شده باشد.**

```
vim /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
```

دستور زیر را اجرا کنید .

```
apt-get update
```

برای به روز کردن پکیج های پایگاه داده ، دستور زیر را بکاربرید.

```
apt-get upgrade
```

۸- تغییر shell پیش فرض دبیان :

به صورت پیش فرض dash shell روی دبیان نصب است اما ما نیاز داریم تا bash shell را نصب کنیم به همین دلیل از دستورزیر استفاده می کنیم

```
dpkg-reconfigure dash
```

و در پاسخ سوال زیر ، no بر می گردانیم .

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

اگر این کار را انجام ندهید ، ISPConfig موقع نصب با مشکل مواجه می شود .

۹- سنکرون کردن ساعت سیستم

یه ایده خوب این است که ساعت سیستم را با پروتکل NTP سنکرون کنید .

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

در این حالت ساعت سیستم تان همواره سنکرون است .

۱۰- نصب Postfix ، Dovecot ، MySQL، phpMyAdmin ، rkhunter و binutils

همه پکیج های بالا را می توانیم با یک دستور زیر نصب کنیم :

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

پس از آن ، سوالات زیر از شما پرسیده می شود که باید به آنها پاسخ دهید .

```
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
```

در مرحله بعد ، پورت های TLS/SSl و submission را در postfix باز می کنیم :

```
vim /etc/postfix/master.cf
```

باید عبارت *milter_macro_daemon_name=ORIGINATING را غیرفعال کنید زیرا نمی خواهیم از آن استفاده کنیم:*

```
[...]
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
[...]
```

حال postfix را بازنشانی مجدد نمایید.

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

میخواهیم که MySQL به همه رابط های شبکه گوش دهد ،بنابراین فایل my.cnf که در مسیر /etc/mysql/my.cnf قرار دارد را ویرایش می کنیم و دستور *bind-address = 127.0.0.1* را غیر فعال می کنیم .

```
vim /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
[…]
```

حال MySQL را بازنشانی مجدد می کنیم .

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

برای اینکه مطمئن شویم شبکه به درستی کار می کند دستور زیر را اجرا می کنیم .

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

خروجی حاصل باید شبیه زیر باشد :

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

۱۱- نصب SpamAssassin ،Amavisd-new **و** Clamav

برای نصب پکیج های بالا ، دستور زیر را اجرا می کنیم .

```
apt-get install amavisd-new spamassassin clamav clamav-daemon zoo 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
```

فرآیند نصب ISPConfig 3 ، amavisd را که کتابخانه فیلتر SpamAssassin را بارگذاری میکند ، بکار می برد .بنابراین ما SpamAssassin را بکار می بریم تا مقداری از RAM را آزاد کنیم :

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

۱۲- نصب Apache2 ، PHP5 ، phpMyAdmin ، FCGI ، suExec ، Pear و mcrypt

نصب پکیج های بالا با دستور زیر شروع می شود :

```
apt-get install apache2 apache2.2-common apache2-doc apache2-mpm-prefork apache2-utils libexpat1 ssl-cert libapache2-mod-php5 php5 php5-common php5-gd php5-mysql php5-imap phpmyadmin php5-cli php5-cgi libapache2-mod-fcgid apache2-suexec php-pear php-auth php5-mcrypt mcrypt php5-imagick imagemagick libapache2-mod-suphp libruby 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-sqlite php5-tidy php5-xmlrpc php5-xsl memcached
```

بعد از نصب ، با دستورات زیر مواجه خواهید شد :

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

پس از آن دستور زیر را اجرا کنید تا ماژول های Apache (suexec ، rewrite ، ssl ، actions) فعال شوند و اگر میخواهید WebDAV را بکاربرید ، dev_fs، dav ، auth_digest را نیز فعال کنید :

```
a2enmod suexec rewrite ssl actions include

a2enmod dav_fs dav auth_digest
```

حال ، فایل /etc/apache2/mods-available/suphp.conf را باز کنید:

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

و بخش <FilesMatch "\.ph(p3?|tml)$"> **را غیر فعال و خط** application/x-httpd-suphp .php .php3 .phtml .php4 .php5. **را اضافه کنید تا همه فایل های** PHP **با** SuPHP **اجرا شوند :**

```
<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>
```

پس از این ، سرویس Apache **را بازنشانی کنید :**

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

اگر می خواهید فایل های Ruby **را با افزونه** rb.**روی سایت هایی که با** ISPConfig **ایجاد شده اند ، میزبانی کنید ، باید خط** application/x-ruby rb **در فایل** /etc/mime.types **غیر فعال کنید :**

```
vim /etc/mime.types
```

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

این کار فقط برای فایل های rb. **است ؛ فایل های** Ruby **با افزونه** rbx. **مشکلی ندارند.**

پس از این مرحله ، Apache را بازنشانی کنید:

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

۱۲,۱- Xcache :

Xcache **یک** opcode cache **برای بهینه سازی و ذخیره سازی فایل های** PHP **روی سرور است .**

Xcache **با دستور زیر نصب کنید :**

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

حالا ، سرویس Apache **را بازنشانی کنید:**

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

۱۲,۲- PHP-FPM :

از نسخه ۳,۰۵ به بعد ISPConfig **، یک مد اضافی** PHP **قرار داده شده است که با** Apache **استفاده می شود:** PHP-FPM

برای استفاده از PHP-FPM **به همراه** Apache **، ما نیاز به ماژول** mod_fastcgi **داریم (دقت کنید که آن را با** mod_fcgid **اشتباه نگیرید ، زیرا خیلی شبیه اند اما نمی توان** mod_fcgid **با** PHP-FPM **بکار برد.) نصب** PHP-FPM **با** Apache **با دستور زیر است :**

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

مد را فعال کنید و سرویس Apache **را بازنشانی نمایید:**

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

۱۲,۳- ورژن های اضافی PHP **:**

از نسخه ۳,۰,۵ به بعد ISPConfig ، اجازه داریم ورژن های مختلف PHP روی یک سرور (قابل انتخاب توسط ISPConfig) داشته باشیم که از طریق FastCGI و PHP-FPM می توانند اجرا شوند. می توانید مقاله زیر را برای یادگیری ساخت ورژن های دیگر PHP (PHP-FPM و FastCGI) و چگونگی پیکربندی ISPConfig مطالعه نمایید.

How To Use Multiple PHP Versions (PHP-FPM & FastCGI) With ISPConfig 3 (Debian Wheezy).

۱۳- نصب Mailman :

از نسخه ۳,۰,۴ به بعد ، ISPConfig اجازه مدیریت لیست میل Mailman(ایجاد ، تغییر ، حذف) را به کابر می دهد. اگر میخواهید از این ویژگی استفاده کنید ، Mailman را با دستور زیر نصب کنید :

```
apt-get install mailman
```

حداقل یک زبان را انتخاب کنید (fa : Farsi ، en: English) :

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

قبل از اینکه بتوانیم Mailman را راه بندازیم ، نیاز داریم یک لیست میل اولیه ایجاد کنیم :

```
newlist mailman
```

root@server1:~# newlist mailman
Enter the email of the person running the list: <--

آدرس ایمیل admin یا به عبارت دیگر listadmin@example.com

Initial mailman password: <-- admin password for the mailman list

برای اینکه ایجاد لیست میل را خاتمه دهید ، باید فایل /etc/aliases را ویرایش، دستورات زیر را اضافه و برنامه 'newaliases' را اجرا کنید :

```
## 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:~#

برای اینکار ، فایل /etc/aliases **را باز کنید:**

```
vim /etc/aliases
```

و خطوط زیر را اضافه نمایید:

```
[...]
## 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"
```

اجرا :

```
newaliases
```

حال ، Postfix **را بازنشانی نمایید:**

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

در انتها ، باید تنظیمات Apache **را برای** Mailman **فعال نمایید:**

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

با استفاده از آن ، نام مستعار /cgi-bin/mailman **برای همه میزبان های مجازی** Apache **تعریف می شود که می توانید برای دسترسی به رابط مدیریت** Mailman **یک لیست به آدرس** http://<vhost>/cgi-

http://<vhost>/cgi-bin/mailman/admin/<listname> **بروید و صفحات وب کاربران یک میل لیست در مسیر** http://<vhost>/pipermail **قرار دارند .در مسیر** bin/mailman/listinfo/<listname>. **نیز می توانید به آرشیو میل لیست ها دسترسی پیدا کنید .**

بعد از این مرحله ، سرویس Apache **را بازنشانی مجدد نمایید:**

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

دایمون Mailman **را آغاز کنید :**

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

۱۴- نصب PureFTPd و Quota

با دستور زیر PureFTPd **و** Quota **نصب می شوند :**

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

فایل /etc/default/pre-ftpd-common **را ویرایش کنید :**

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

و مطمئن شوید که مد شروع فعال شده و مقدار VIRTUALCHROOT=true **تعریف شده باشد :**

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

حالا ، PureFTPd **را پیکربندی میکنیم تا به جلسات** FTP **و** TLS **اجازه فعالیت دهیم .** FTP **یک پروتکل بسیار امن است چراکه همه رمز ها و داده ها را به صورت** clear text **انتقال می دهد . با استفاده از** TLS **، هم ارتباطات می توانند رمز نگاری شوند ، بنابراین** FTP **امن تر می شود.**

برای اینکه به FTP **و** TLS **اجازه فعالیت دهیم ، دستور زیر را اجرا کنید :**

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

برای اینکه از TLS استفاده کنیم ، باید یک مجوز SSL ایجاد کنیم . میخواهیم این مجوز در مسیر /etc/ssl/private قرار داشته باشد بنابراین ابتدا دایرکتوری مورد نظر را ایجاد می کنیم :

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

بعد از این مرحله ، مجوز SSL را می سازیم با دستور زیر :

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

نام کشور :

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

نام استان :

State or Province Name (full name) [Some-State]: <-- Enter your State or Province Name.

نام شهر :

Locality Name (eg, city) []: <-- Enter your City.

نام سازمان :

Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter your Organization Name (e.g., the name of your company).

نام مجموعه :

Organizational Unit Name (eg, section) <-- Enter your Organizational Unit Name (e.g. "IT Department").

نام خودتان :

Common Name (eg, YOUR name) <-- Enter the Fully Qualified Domain Name of the system (e.g. "server1.example.com").

آدرس ایمیل :

Email Address <-- Enter your Email Address.

در مرحله بعد ، سطح دسترسی مجوز SSL را تغییر دهید :

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

حال ،PureFTPd را دوباره بازنشانی کنید :

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

فایل /etc/fstab را همانند زیر ویرایش کنید :

```
vim /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=vfsv0 0       1
# /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
```

برای فعال سازی Quota ، دستور زیر را اجرا کنید :

```
mount -o remount /

quotacheck -avugm
quotaon -avug
```

۱۵- نصب BIND DNS Server

BIND با دستور زیر نصب می شود :

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

۱۶- نصب Vlogger ، Webalizer و AWstats

Vlogger ، Webalizer و AWstats با دستور زیر نصب می شوند :

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

فایل /etc/cron.d/awstats را باز کنید :

```
vim /etc/cron.d/awstats
```

و دستورات زیر را در آن قرار دهید :

```
#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
```

۱۷- نصب Jailkit

Jailkit زمانی استفاده می شود که شما بخواهید به کاربران chroot SSH کنید . و با دستورات زیر نصب می شود : (نکته اینکه Jailkit باید قبل از نصب ISPConfig نصب شود زیرا بعد آن نصب نمی شود.)

```
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
```

حالا نیاز دارید پکیج های دبیان Jailkit را نصب کنید :

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

۱۸- نصب fail2ban

این گزینه اختیاری است اما توصیه می شود نصب شود زیرا مانیتور ISPConfig سعی می کند لاگ ها را نشان دهد :

```
apt-get install fail2ban
```

برای اینکه fail2ban ، بتواند PureFTP و Dovecot را مانیتور کند ، فایل /etc/fail2ban/jail.local را ایجاد کنید :

```
vim /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
```

دو فایل فیلتر زیر را ایجاد کنید :

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

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

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

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

بعد از این مرحله ، fail2ban را بازنشانی مجدد نمایید:

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

۱۹- نصب SquirrelMail

برای نصب SquirrelMail ، دستور زیر را اجرا کنید :

```
apt-get install squirrelmail
```

سپس ، آن را پیکربندی کنید :

```
squirrelmail-configure
```

حال باید SquirrelMail تنظیم شود تا Dovecot-IMAP/-POP3 استفاده کند:

```
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



          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
```

حال ، ما SquirrelMail **را پیکربندی می کنیم تا بتوان از طریق وب سایت ها با استفاده از نام های مستعار** squirrelmail/ **و** webmail/ **به آن دسترسی یافت . مثلا اگر وب سایت تان** www.example.com **بود می توانید با آدرس های** www.example.com/squirrelmail **یا** www.example.com/webmail **به** SquirrelMail **دسترسی یابید .**

فایل پیکربندی Squirrelmail's Apache **در مسیر** /etc/squirrelmail/apache.conf **قرار دارد اما توسط** Apache **لود نمی شود زیرا در مسیر** /etc/apache2/conf.d **قرار ندارد . بنابراین یک** symlink **ای به نام** squirrelmail.conf **در مسیر** /etc/apache2/conf.d **ایجاد می کنیم که به** /etc/squirrelmail/apache.conf **اشاره می کند و بعد از آن** Apache **را مجددا لود می کنیم :**

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

حال ، فایل /etc/apache2/conf.d/squirrelmail.conf **راباز می کنیم :**

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

و خطوط زیر را به آن اضافه می کنیم :

```
[...]
<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>
[...]
```

دایرکتوری /var/lib/squirrelmail/tmp **را ایجاد کنید :**

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

ومالکیتش را به کاربر www-data **بدهید :**

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

حالا ، سرویس Apache را مجددا بازنشانی کنید:

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

هم اکنون ،فایل /etc/apache2/conf.d/squirrelmail.conf یک نام مستعار /squirrelmail تعریف می کند که به دایرکتوری تنظیمات SquirrelMail که در مسیر /usr/share/squirrelmail قرار دارد ، اشاره می کند :

حالا می توانید با یکی از روش های زیر به SquirrelMail دسترسی یابید :

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

بعد ازاینکه ISPConfig را نصب کردید نیز می توانید از طریق پنل کنترلی میزبان مجازی تان نیز به آن دسترسی داشته باشید :

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

اگر تمایل دارید تا از نام مستعار /webmail به جای /squirrelmail استفاده کنید ، فایل /etc/apache2/conf.d/squirrelmail.conf را باز کنید :

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

و خط Alias /webmail /usr/share/squirrelmail را به آن اضافه نمایید همانند شکل زیر :

```
Alias /squirrelmail /usr/share/squirrelmail

Alias /webmail /usr/share/squirrelmail

[...]
```

و سپس Apache را مجددا بازنشانی نمایید :

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

حالا ، می توان با یکی از روش های زیر به SquirrelMail دسترسی یافت :

http://192.168.0.100/webmail
http://www.example.com/webmail
http://server1.example.com:8080/webmail

البته راه آخر ، بعد از نصب کامل ISPCONFIG امکان پذیر می باشد.

اگر می خواهید یک میزبان مجازی همانند webmail.example.com **تعریف کنید تا کاربران بتوانند به** SquirrelMail **دسترسی داشته باشند ، باید تنظیمات میزبان مجازی زیر را به فایل** /etc/apache2/conf.d/squirrelmail.conf **اضافه نمایید :**

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

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

1.2.3.4 **را با آدرس IP سرور جایگزین کنید . این را هم در نظر داشته باشید که باید یک رکورد DNS برای** webmail.example.com **وجود داشته باشد که به آدرس IP ای که در فایل پیکربندی میزبان مجازی قرار داده اید ، اشاره کند و نکته دیگر اینکه مطمئن شوید میزبان مجازی** webmail.example.com **در** ISPConfig **وجود نداشته باشد .**

حالا ، Apache **را مجددا لود کنید :**

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

و حال می توانید به SquirrelMail **از طریق آدرس** http://webmail.example.com **دسترسی یابید :**

۲۰- **نصب** ISPConfig 3

برای نصب ISPConfig 3 **، دستور زیر را وارد کنید :**

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

قدم بعدی ، دستور زیر را اجرا کنید :

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

با این دستور ، نصاب ISPConfig 3 شروع به کار خواهد کرد و همه سرویس ها همانند Postfix ، Dovecot و غیره را پیکر بندی خواهد کرد :

```
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 Unkn
own on line 0


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


>> Initial configuration

Operating System: Debian or compatible, unknown version.
```

در زیر تعدادی سوال برای تنظیم اولیه ISPConfig پرسیده می شود . مقادیر پیش فرض در [] قرار دارد و شما فقط با زدن Enter آن را تایید کنید . برای توقف نصب عبارت "quit" را تایپ نمایید :

```
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'

سوالاتی که در زیر پرسیده می شود ، برای وارد کردن اطلاعاتی است که برای ثبت درخواست مجوز است که بهتر است کامل ودقیق و درست پر شود . بعضی فیلد ها مقدار پیش فرض دارند و بعضی دیگر نه که با وارد کردن '.' ، خالی گذاشته می شوند .

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/transfer.log -Y 1 -D -u 1000 -A -E -b -8 UTF-8 -B
Installation completed.
root@server1:/tmp/ispconfig3_install/install#
```

نصاب ، به صورت خودکار همه سرویس ها را نصب می کند و نیاز به تنظیم دستی ای نیست .

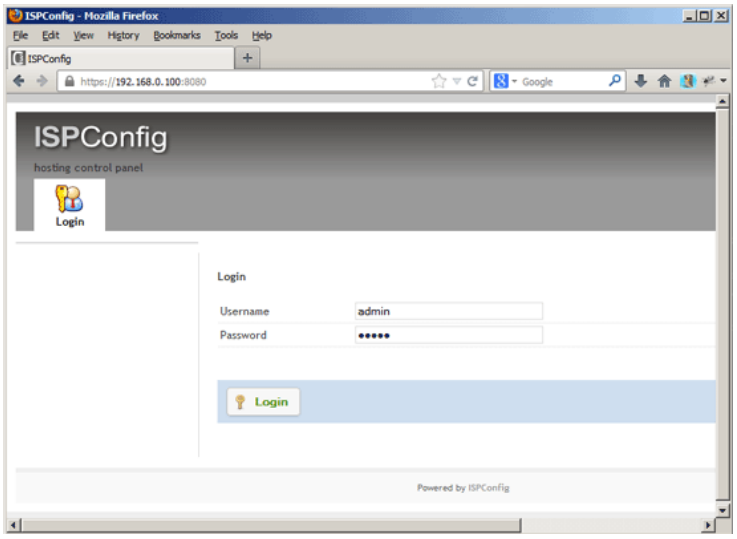
البته این امکان وجود دارد که یک SSL برای کنترل پنل ISPConfig ایجاد کنید که به جای http:// از https:// برای وارد شدن به کنترل پنل استفاده شود . برای اینکار موقع دیدن سوال Do you want a secure (SSL) connection to the ISPConfig web interface (y,n) [y] ، Enter بزنید .

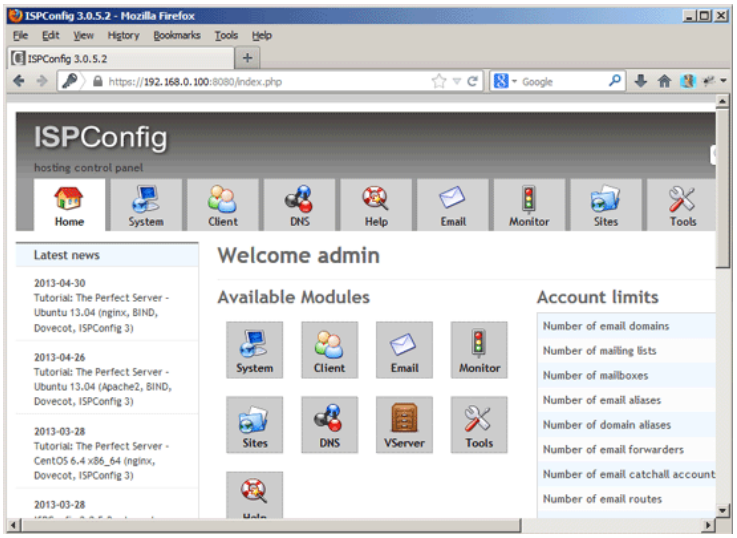
بعد از این برای دسترسی به ISPConfig 3 باید یکی از دو روش زیر را بکار برید :

https://server1.example.com:8080/

https://192.168.0.100:8080/

با نام کاربری و رمز ورود admin ، وارد کنترل پنل ISPConfig شوید :





حالا ، سیستم برای استفاده آماده است .

۲۰,۱ – راهنمای ISPConfig 3

برای یادگیری کاربا ISPConfig 3 **، توصیه می کنم که راهنمای کار با آن را از لینک زیر دریافت کنید :**

download the ISPConfig 3 Manual.

این راهنما ، مرجع کاملی برای همه مفاهیم پشت پرده ISPConfig **(مدیر ، کاربر و ...) به همراه مثال می باشد .همین طور یک بخش آن شامل افزایش امنیت سرور و بخشی از آن شامل بیان اشکالات معمول کار با** ISPConfig **می باشد .**

منابع

- Debian: http://www.debian.org/
- ISPConfig: http://www.ispconfig.org/
- Wiki : http:// Wikipedia.com/
- Howtoforge : http://www.howtoforge.com/perfect-server-debian-wheezy-apache2-bind-dovecot-ispconfig-3-p3

۲۱- پیوست

Postfix :

Postfixنرم افزاری متن باز با عنوان MTA (mail transfer agent) و یا نماینده انتقال ایمیل است که جهت حمل و مسیر یابی ایمیل استفاده می‌شود و همواره از آن به عنوان نرم افزاری سریع با مدیریت آسان و امنیت بالا یاد می‌گردد و با نام‌های VMailer و IBM Secure Mailer نیز شناخته شده است .

Dovecot :

Dovecot یک میل سرور متن باز pop3 و IMAP برای سیستم عامل های لینوکس ویونیکس است .

PhpMyAdmin :

نرم افزار PhpMyAdmin توسط زبان PHP نوشته شده است و برای مدیریت پایگاه داده MySql به کار گرفته می شود. phpMyAdmin از طیف گستره ای از عملیات های MySql پشتیبانی می کند و می‌تواند وظایفی مانند ایجاد ، تغییر و یا حذف پایگاه داده، جداول، فیلدها و یا ردیف‌ها، اجرای عبارت SQL و یا مدیریت کاربران و دسترسی‌ها را انجام دهد.

rkhunter:

RootKitها برنامه هایی هستند که از نظر ساختار کاری بسیار شبیه Trojan ها و Backdoor ها هستند ولی با این تفاوت که شناسایی RootKit بسیار مشکلتر از تروجان ها است زیرا RootKit ها علاوه بر اینکه به عنوان یک برنامه کاربردی خارجی مثل شنونده Netcat و ابزارهای درب پشتی مثل Sub7 بر روی سیستم اجرا می شوند بلکه جایگزین برنامه های اجرایی مهم سیستم عامل و در گاهی مواقع جایگزین خود هسته کرنل می شوند و به هکرها این اجازه را می دهند که از طریق درب پشتی و پنهان شدن در عمق سیستم عامل به آن نفوذ کنند و مدت زیادی با خیال راحت با نصب ردیابها ودیگر برنامه های مانیتورینگ بر روی سیستم ، اطلاعاتی را که نیاز دارند بدست آورند.

دو نرم افزار Chkrootkit و rkhunter نرم افزارهای مناسبی برای یافتن بدافزارها در لینوکس می باشند .

نکته این که این نرم افزارها به صورت realtime عمل نمی کنند و باید به صورت دوره ای دستور آن اجرا شود .می توان برای آن اسکریپتی نوشت که آن ها را در دوره معینی اجرا کند و خروجی را به صورت فایل به مدیر ارائه دهد.
برای پاکسازی هم به ازای هر کدام باید روش خاصی پی گرفت. این دو نرم افزار، نرم افزارهای قوی ای هستند که برای یافتن Malware ها و البته بیشتر rootkit ها استفاده می شوند.

BinUtils :

Binary Utilities یا به عبارت ساده تر BinUtils ، مجموعه ای از ابزارهای برنامه نویسی باینری است که برای اسمبل ، لینک و دستکاری فایل های شی و باینری بکار می رود. Binutils قابل انتقال به اکثر توزیع های یونیکس می باشد و اکثرا با یک کامپایلر و کتابخانه برای طراحی برنامه ها ، برای لینوکس بکار برده می شود.

clamav :

clamav یک آنتی ویروس رایگان برای سرورهای لینوکس می باشد که با وجود رایگان بودن ، امکانات فراوانی را در اختیار کاربر قرار میدهد. clamav قادر است اکثر ویروس ها ، فایل های جاسوسی ، تروجان و فایل های Shell را شناسایی و حذف نماید و تا حد زیادی امنیت را در سرورهای لینوکس برقرار نماید.
یکی از قابلیت مهم این آنتی ویروس به روزرسانی خودکار آن می باشد که این امکان باعث می شود که همیشه پایگاه داده آن به روز باشد و در هر لحظه جدیدترین ویروس های شناخته شده را شناسایی نماید.
از دیگر مزایای این نرم افزار ، حجم پایین و سبک بودن آن می باشد.مزیت دیگر آن ، امکان زمانبندی عملیات می باشد.

SpamAssassin :

SpamAssassin یک فیلتر ایمیل و ابزار قوی است که برای شناسایی اسپم استفاده می شود.

ابزاری که از آنها برای شناسایی اسپم استفاده می شود شامل موارد زیر می باشند :

- **تحلیلگر عنوان و متن**
- **فیلترینگ Bayesian**
- **لیستهای بلاک شده ی DNA**

- پایگاه داده فیلترینگ

AMaViS :

AMaViS (A Mail Virus Scanner) یک رابط بین Postfix ، SpamAssassian و اختیارا یک اسکنر ویروس ، می باشد که شامل بخش فیلترینگ اسپم می باشد اما اسکنر ویروس ندارد که برای این منظور می توانید از ClamAV استفاده کنید که کیفیت بالایی دارد و اسکنر ویروس آن رایگان است و به صورت دوره ای به روز رسانی می شود .

PHPsuexe :

php در سرورها می‌تواند به صورت یک ماژول برای Apache و یا به صورت CGI و کاملا مجزا اجرا شود.
در حالت اول که PHPبصورت ماژول Apache اجرا می شود با توجه به این که Apache عموما با کاربری به نام nobodyو یا apache اجرا می شود بنابراین اسکریپت های PHP نیز با مجوز های کاربر nobody اجرا می شود.
بنابراین چنانچه شما در کد PHPخودتان نیاز به نوشتن در یک فایل و یا دسترسی به یک فایل داشته باشید باید مجوز فایل را به ۷۷۷ تغییر دهید (مجوز ۷۷۷ یعنی مجوز اجرا و مشاهده و تغییر فایل برای همه کاربران). ما با این کار به همه کاربران امکان دسترسی به فایل خود را می دهیم و این یک اشکال امنیتی بزرگ است و این یعنی سرور ما NON_PHPsuexe است.
اما راه حل چیست؟
راه حل PHPsuexe است.
در این روش php را بصورت CGI و مجزا از Apache اجرا می کنیم و بااین کار ، اسکریپت‌های هر کابر با مجوزهای همان کاربر اجرا می‌شود و در نتیجه اسکریپت های اجرا شده به وسیله هر کاربر مجاز به مشاهده و ویرایش فایل های همان کاربر خواهند بود و به فایل ها و پوشه های سایر کابران دسترسی ندارند.

PEAR :

PEAR(PHP Extension and Application Repository) به معنی افزونه های PHP و انبار کاربردها است .
هدف از PEAR :
1) ایجاد کتابخانه ای ساختاری از کد های متن باز برای کاربرانphp
2) سیستمی برای توزیع کد ها و پشتیبانی از آنها
3) یک استایل استاندارد برای کدهای نوشته شده درphp

4) کتابخانه ای برای افزونه هایPHP

5) وب سایتی به همراه ایمیل و دانلود برای پشتیبانی جامعهPEAR

Mcrypt:

mcrypt یک افزونه PHP است که به عنوان رابط برای استفاده از کتابخانه mcrypt در برنامه های PHP مورد استفاده قرار می گیرد، کتابخانه mcrypt مجموعه وسیعی از الگوریتم های مدرن مانند DES, TripleDES وBlowfish را درون خود دارد.

WebDav:

WebDav یک پروتکل توسعه یافته از پروتکل HTTP می باشد که به کاربران امکان مشارکت در تغییر و مدیریت اسناد و فایل ها را بر روی وب جهانی فراهم می کند. WebDAVرسانه وب را قابل خواندن و نوشتن می کند و بستر را برای ایجاد , تغییر و جابجایی اسناد روی سرورهایی همانند Webserver و Webshare فراهم می کند. یکی از مهمترین ویژگی های WebDAVنگهداری ویژگی های نویسنده ، تاریخ تغییر , مدیریت فضای نام و مجموعه ها می باشد.

به وسیله این پروتکل ، برنامه های کاربردی می توانند با فایل های ذخیره شده به صورت آنلاین در ارتباط باشند. بسیاری از برنامه های کاربردی که شما را در گوشی های هوشمند خود استفاده می کنید به وسلیه این پروتکل اداره می شود.

Xcache :

APC ، Eaccelerator و Xcache هر سه ، Opcod Cache هستند که وظیفه ذخیره سازی فایل های PHP در وضعیت کامپایل شده روی دیسک های حافظه RAM سروررا به عهده دارند.

APC بیشترین سازگاری را دارد به خصوص اینکه در آینده نه چندان دور بخشی از PHP خواهد بود.همین پشتیبانی رسمی از APC توسط خود PHP باعث میشود که بیشترین سازگاری را داشته باشد . سرعت APC بسیار بالاست و فایل های کامپایل شده را داخل RAM سرور کش میکند .

Eaccelerator، مدت نسبتا طولانی است که نسخه جدیدی ارائه نکرده و به نظر هم نمیرسد دیگر تولید کنندگانش قصد توسعه آن را داشته باشند . Eacclereator تا php 5.4 رو پشتیبانی میکنداما به هر حال همچنان یکی از بهترین

opcode cache ها به حساب می آید به خصوص اینکه ، متد کش کردن فایل های کامپایل شده PHP روی دیسک توسط Eaccelerator بسیار رایج است و تاثیر زیادی روی کاهش لود سرور دارد .

Xcache شاید سریع ترین آپکد کش باشد ولی بیشتر برای تک سایت ها یا سرور های شخصی با تعداد سایت های کم توصیه میشود زیرا این سیستم کشینگ بیشترین آمار ناسازگاری را با سایر سرویس ها و نرم افزار های سرور دارد و در ضمن از بعضی توابع خطرناک نیز استفاده می کند . اگر توابع معروف و پر ریسک را در php.ini ببندید در فرایند نصب Xcache با خطا مواجه می شوید .

Memcache ، کاملا کارش با ۳ آپکد کش فوق متفاوت است . Memcache یک Object Cache بسیار قوی است و بهترین روش برای کش کردن کوئری های پایگاه داده است . برای داشتن حداکثر بازدهی توصیه می شود از Memcache روی یک سرور جدا (Memcache Server) استفاده شود .

PHP_FPM:

PHP-FPM یک پیاده سازی دیگر از PHP FastCGI بوده و برای سایت‌های heavy-load مناسب است. از ویژگی‌های آن در مقایسه با PHP معمولی و دیگر پیاده سازی‌های PHP FastCGI می‌توان به موارد زیر اشاره کرد:

- شروع و بارگزاری مجدد فرآیندها به صورت graceful
- خاتمه درخواست‌های موجود قبل از اتمام فرآیند.
- کنترل تعداد فرآیندها با توجه به بار سرور
- توانایی شروع workerها با uid/gid/chroot/environment و php.ini های مختلف
- سازگاری بیشتر با acceleratorها
- قابلیت کشف فرآیندهای کند SlowLog

PHP-FPM نیز همانند دیگر نرم‌افزارها باید برای محیطی که در آن کار می کند بهینه شود.

بهینه سازی یا Tunnig یعنی تعیین دقیق پارامترهای نرم‌افزار با توجه به کاربرد، کانفیگ سخت افزاری سرور شامل RAMوCPU ، تعداد درخواست‌های روی سرور و... .

Mailman :

Mailman یک برنامه کاربردی نرم افزاری برای مدیریت میل لیست ها است که به زبان پایتون نوشته شده و رایگان است .روی نسخه های مختلف لینوکس اجرا می شود و نسخه ۲,۱,۳ به بعد پایتون را نیاز دارد و با میل سرورهای یونیکسی مانند Postfix ، Sendmail و qmail کار می کند .

Bind :

وقتی شما می خواهید وارد سایتی بشوید، باید آدرس web serverخود را درمرورگروارد کنید.یک روش برای مشخص کردن سرور ، دانستن IP آدرس آن است. مثلا ۶۳,۷۲,۵۱,۸۵=www.ciwcertified.com

اما همه کاربر ها ترجیح می دهند تا به جای استفاده از این اعداد و ارقام ازنام دامنه استفاده کنند، چرا که استفاده کردن و به خاطر سپردن آنها به مراتب راحت تر است.در حقیقتDNS ، آدرس IP را به اسامی مشخص و ساده ترجمه می کند .هم نام دامنه و هم آدرس IP ، کاربر را به یک وب سرور مشخص هدایت می کند، اما نام دامنه ، هم برای استفاده و هم برای به خاطر سپردن به مراتب راحت تر است. بدون DNS کاربرها مجبور هستند برای وارد شدن به هر بخشی از اینترنت از اعداد خسته کننده آدرس IP استفاده کنند.

bind بسته نرم افزاری است که در سیستم های یونیکسی کار Domail Name Service را انجام میدهد مانند Apache که کار Web Server را انجام میدهد .

Webalizer:

یک توانمندی بسیار قوی ISPConfig که با استفاده از این توانمندی یک آمار دقیق و کامل از کلیه موارد سایت خود خواهید داشت. این آمار بصورت روزانه و هر ساعت بروزرسانی می‌شود که می‌توان به قدرت مثال نزدنی آن اشاره کرد.

AWstats:

Advanced Web Statistics سرویسی است که برخی از شرکت های میزبانی وب در کنترل پنل کاربری خودارائه می کنند . AWstats نوع متفاوتی از تحلیل ارائه میدهد و به جای دنبال کردن hit ها در یک زمان مشخص در میان کدهای سایت ، از فایل های لاگ وب سرور برای تولید گزارش های آماری استفاده می کند .

تحلیلگر لاگ های AWstats ، گزارشی از تمام آمارهای وب شما که شامل بازدیدها ، بازدیدکنندگان جدید ، صفحات ، hit ها ، ساعات پر ترافیک ، موتورهای جستجو ، کلمات کلیدی که برای پیدا کردن سایت شما استفاده شده است ، ربات ها ،لینک های شکسته شده ، کد خطاها و .. را ارائه می دهد .

Jailkit:

سیستم‌های شبیه BSD ابزاری دارند به اسم chroot که این ابزار از زمان ۴,۲ BSDوارد این سیستم عامل ها شده است. Chrootابزاری است برای تغییر دادن دایرکتوری ریشه بعضی از فرآیندها ، ساختن یک محیط امن و جدا کردن قسمتی از سیستم برای آنها. پروسه هایی که در chroot ساخته می‌شوند نمی توانند به فایل‌ها یا منابع خارج از آن دسترسی داشته باشند. به همین دلیل ، سرویس های در حال اجرا در محیط chroot نمی توانند به یک مهاجم اجازه دهند تا خطر بالقوه ای برای کل سیستم به وجود آورد. ابزار chroot برای کارهای ساده خیلی مناسب است اما در مواقعی که نیاز به انعطاف پذیری و پیچیدگی و ویژگی‌های خاص باشد جواب نمی دهد. از آنجا که با آغاز به کار مفهوم chrootاغلب راه‌های زیادی برای کنار گذاشتن محیط chroot است و اگرچه این ابزار در نسخه های مدرن هسته FreeBSDپیشرفت کرده اما نمی‌تواند یک راه حل ایده‌آل برای تأمین امنیت باشد.و این یکی از دلایل اصلی است که jail توسعه داده شد.

Jail در مسیر های مختلف از روی مفهوم سنتی محیط های chroot رشد کرده است. در محیط های سنتی ، chroot فرآیندها محدود به قسمتی از فایل سیستم که به آن دسترسی دارند ، می باشند . بقیه منابع سیستم بین پروسه های chrootو پروسه های سیستم اصلی به اشتراک گذاشته می شوند. jailها این مدل را با مجازی سازی گسترش می دهند.