

# How to Install a Debian 12 (Bookworm) Minimal Server

This tutorial shows how to install a Debian 12 - Bookworm - minimal server in detail with many screenshots. The purpose of this guide is to provide a minimal setup that can be used as the basis for our other Debian 12 tutorials here at howtoforge.com.

## 1 Requirements

To install a Debian 12 server system, you will need the following:

- The Debian Bookworm network installation CD is available here:  
64Bit: <https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-12.1.0-amd64-netinst.iso> (x86\_64 / amd64)
- A fast Internet connection.

I will use the Debian 12.1.0 64Bit (amd64) installation media.

The Debian Download links change regularly. If the above links do not work anymore, then go here to fetch the latest Debian netinst image: <https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/>.

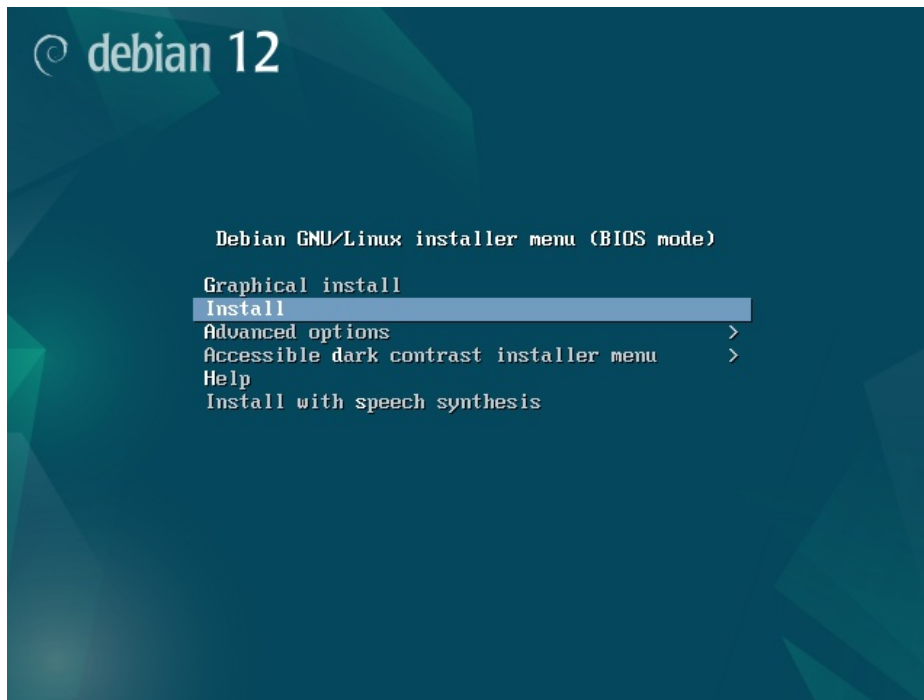
## 2 Preliminary Note

In this tutorial, I will use the hostname *server1.example.com* with the IP address *192.168.0.100* and the gateway *192.168.0.1*. These settings might differ for you, so you have to replace them where appropriate.

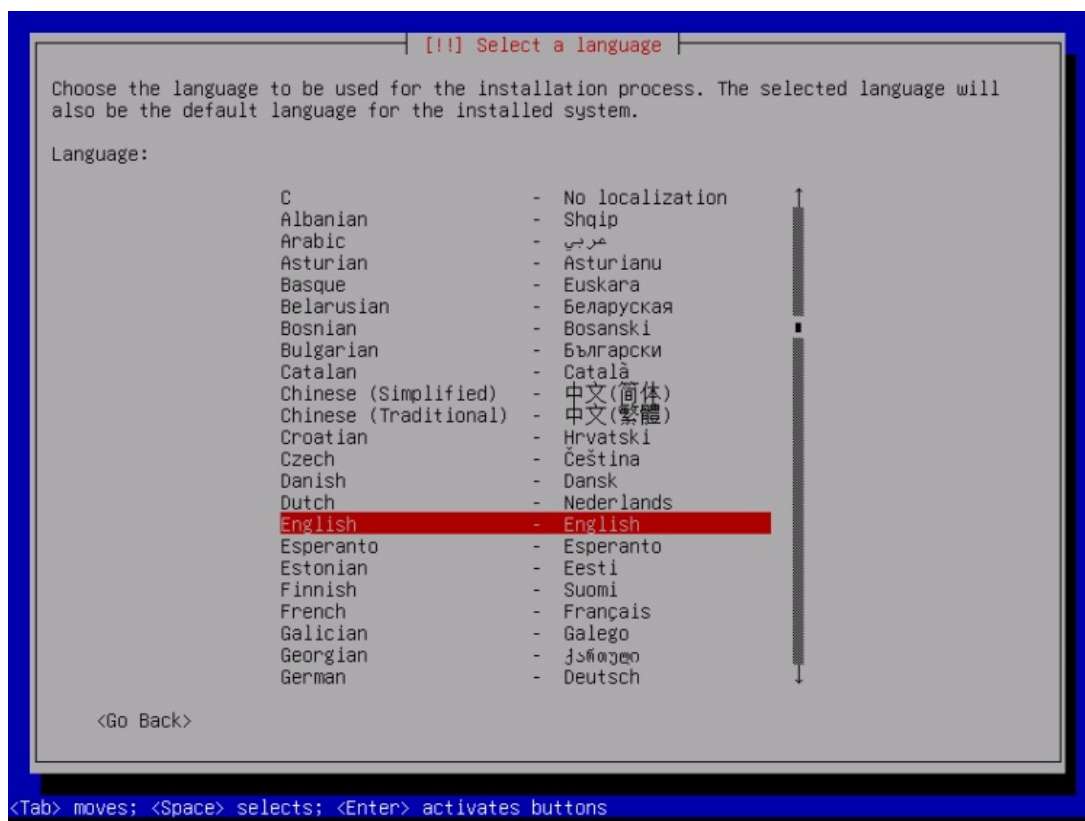
## 3 The Debian Base System

Insert your Debian 12 (Bookworm) network installation CD into your system (or a USB drive where you installed the iso file) and boot from it. When you use virtualization software like VMware or Virtualbox, then select the Debian 12 minimal iso file as the source file for the DVD drive of the VM. You don't have to burn it to a CD or DVD for that first.

Select *Install* (this will start the text installer - if you prefer a graphical installer, select *Graphical install*):

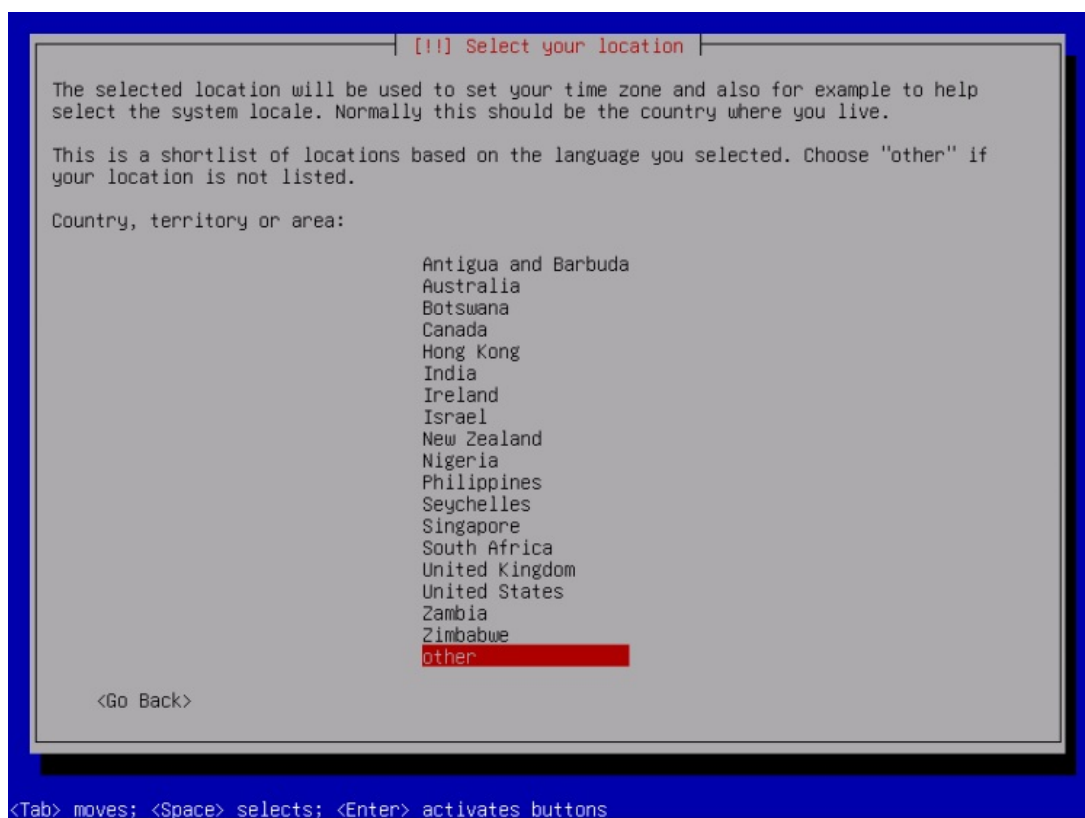


Select your language:



Then choose your location and select the keyboard layout. the next screens will differ depending on your choices. Just select which country and keyboard layout are the right ones for you as they define the language that your Debian system will use on the shell and which keyboard layout is used. In my case, I'll have a german keyboard layout but prefer English as the language on the shell.

Select Country, territory, or area:



Select your location, territory again, and locale and keyboard:

!!! Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

Select the continent or region to which your location belongs.

Continent or region:

Africa

Antarctica

Asia

Atlantic Ocean

Caribbean

Central America

Europe

Indian Ocean

North America

Oceania

South America

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

!!! Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

Listed are locations for: Europe. Use the <Go Back> option to select a different continent or region if your location is not listed.

Country, territory or area:

Armenia

Austria

Azerbaijan

Belarus

Belgium

Bosnia and Herzegovina

Bulgaria

Croatia

Cyprus

Czechia

Denmark

Estonia

Faroe Islands

Finland

France

Georgia

Germany

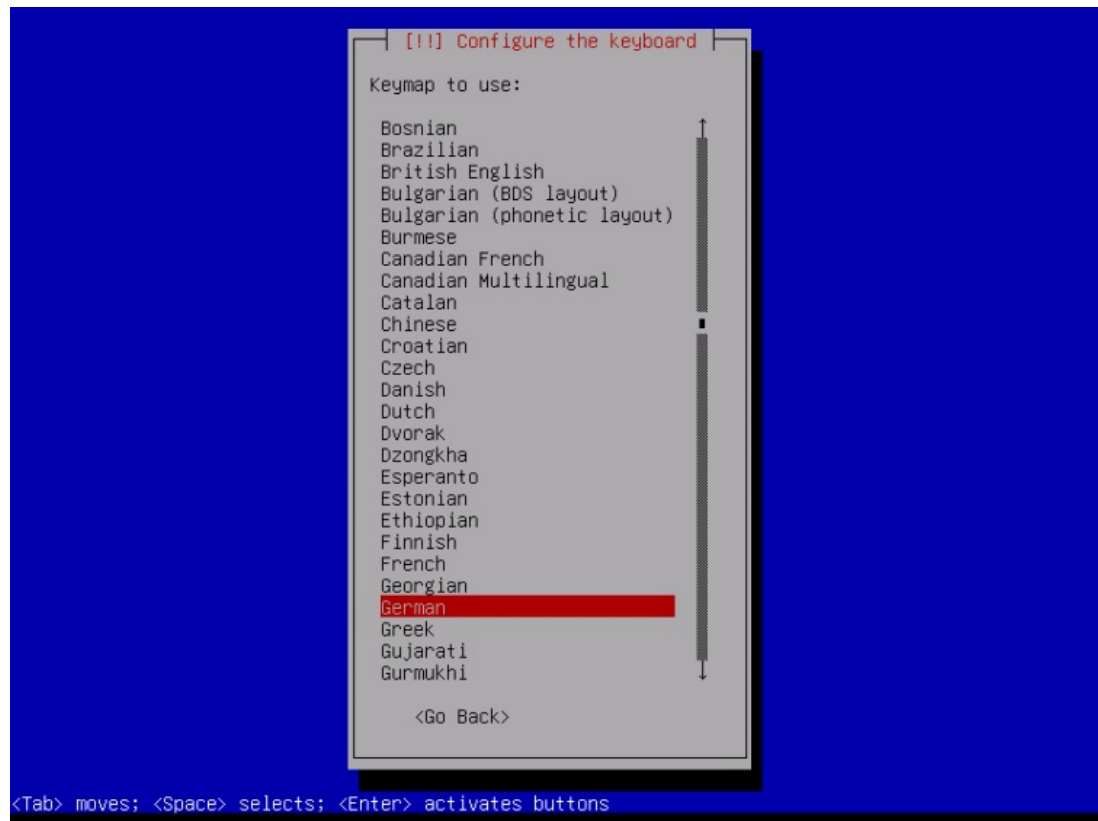
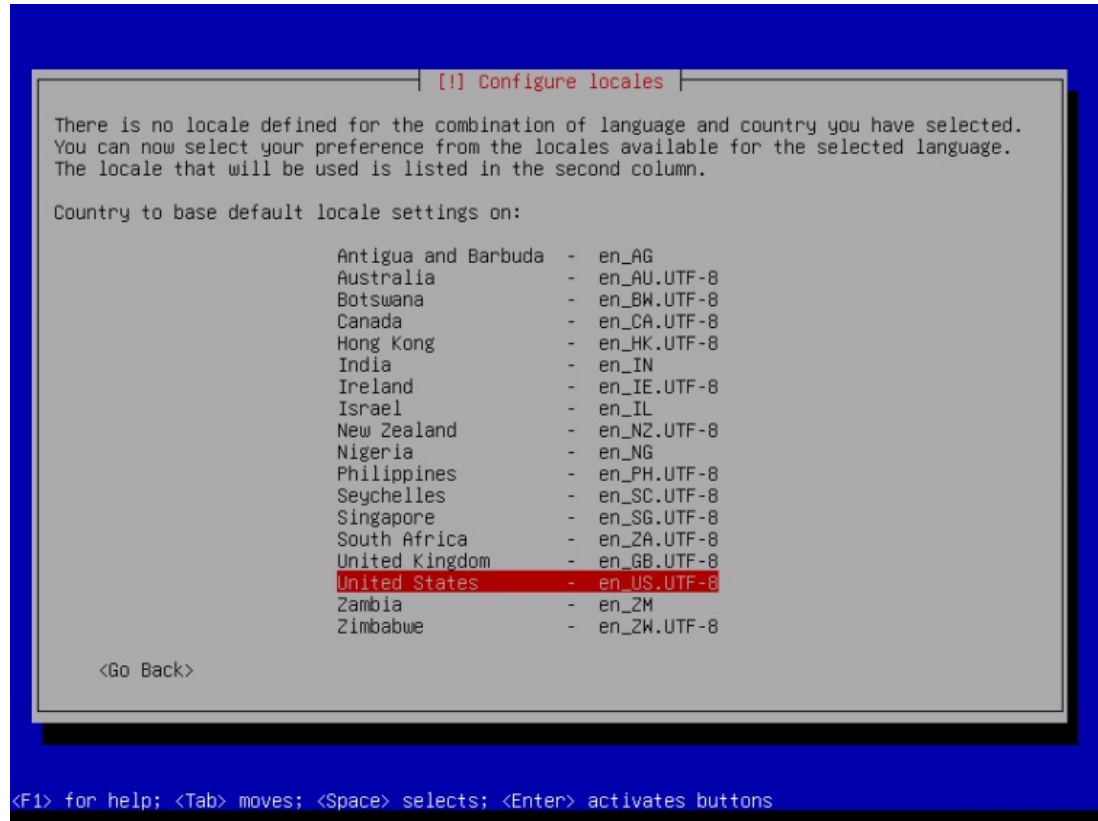
Gibraltar

Greece

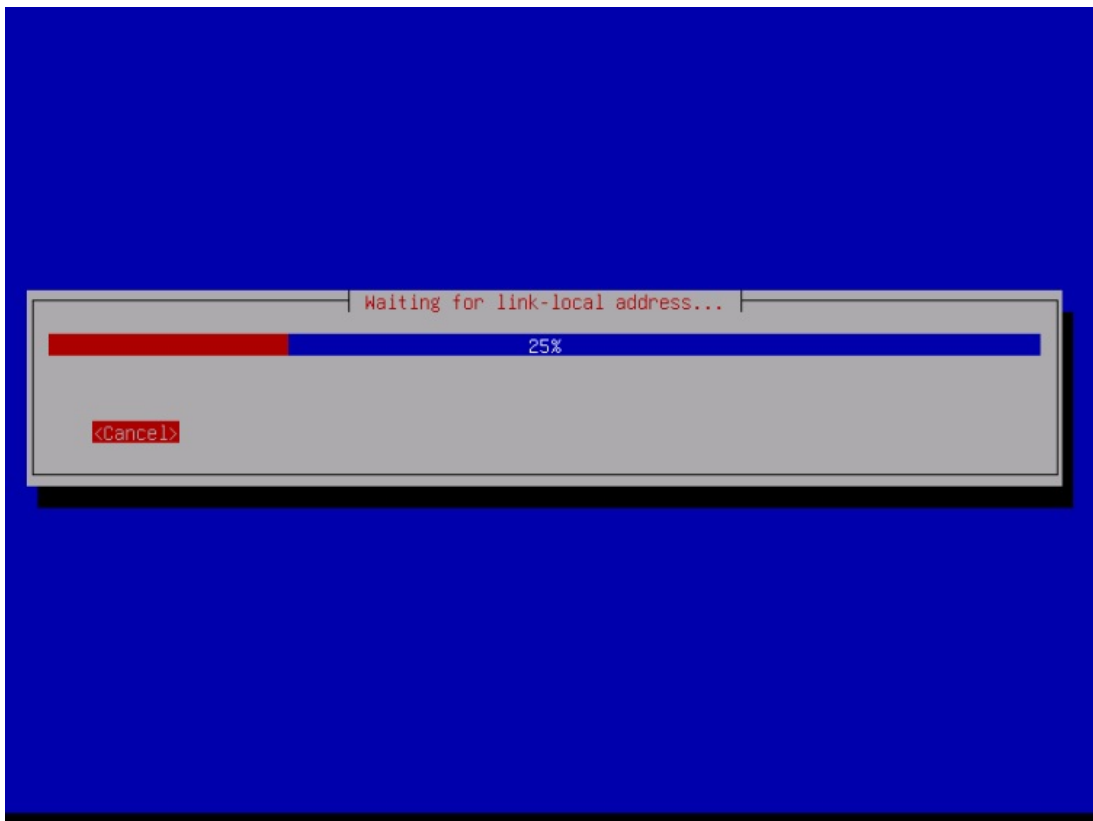
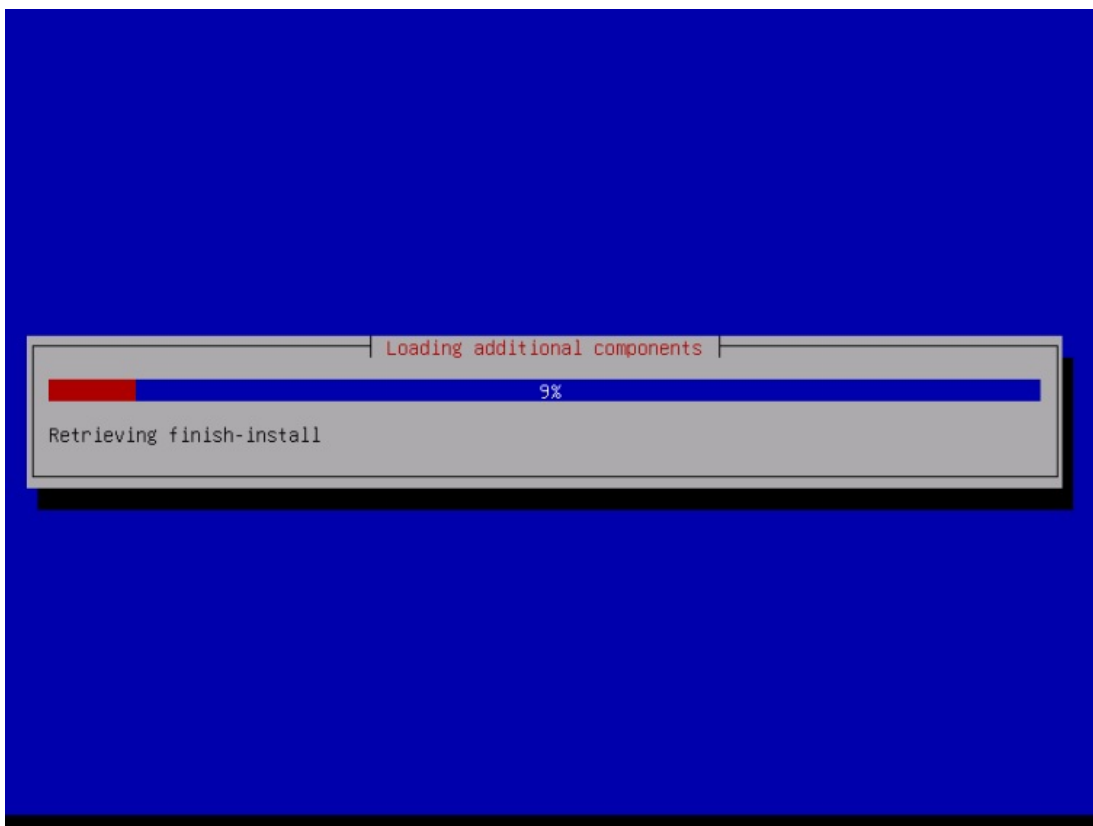
Greenland

<Go Back>

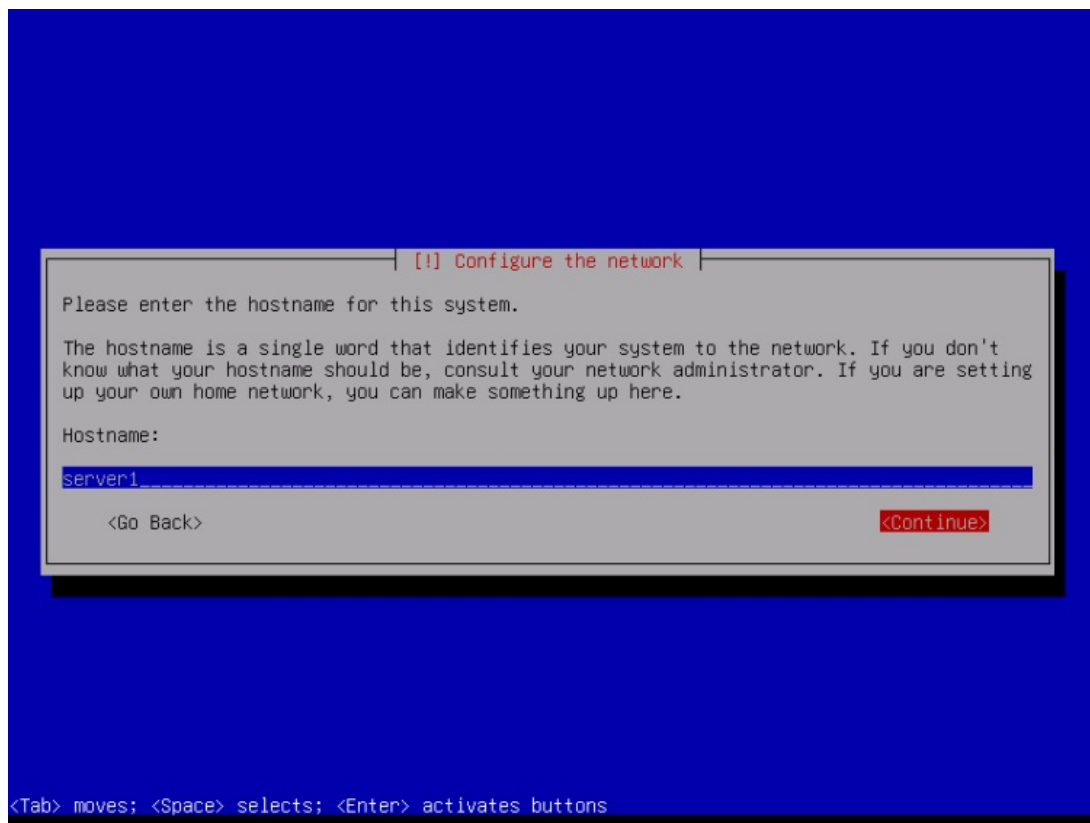
<Tab> moves; <Space> selects; <Enter> activates buttons



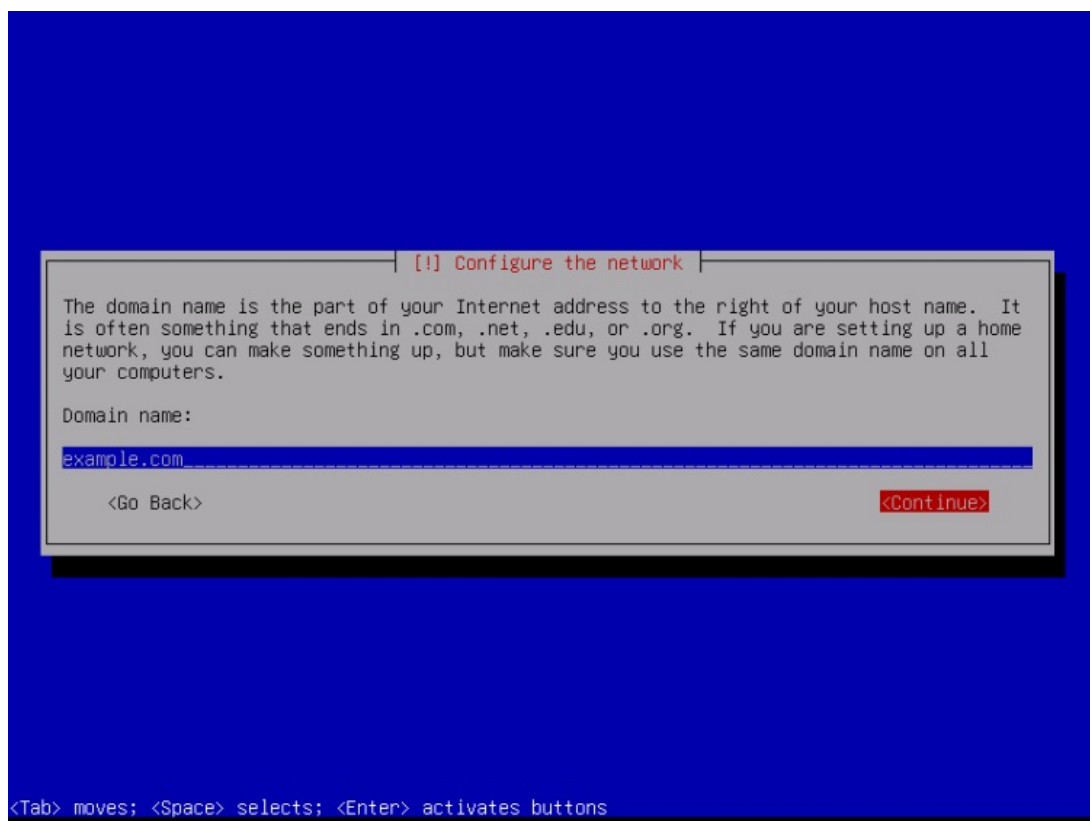
The installer checks the installation CD and your hardware and configures the network with DHCP if there is a DHCP server in the network:



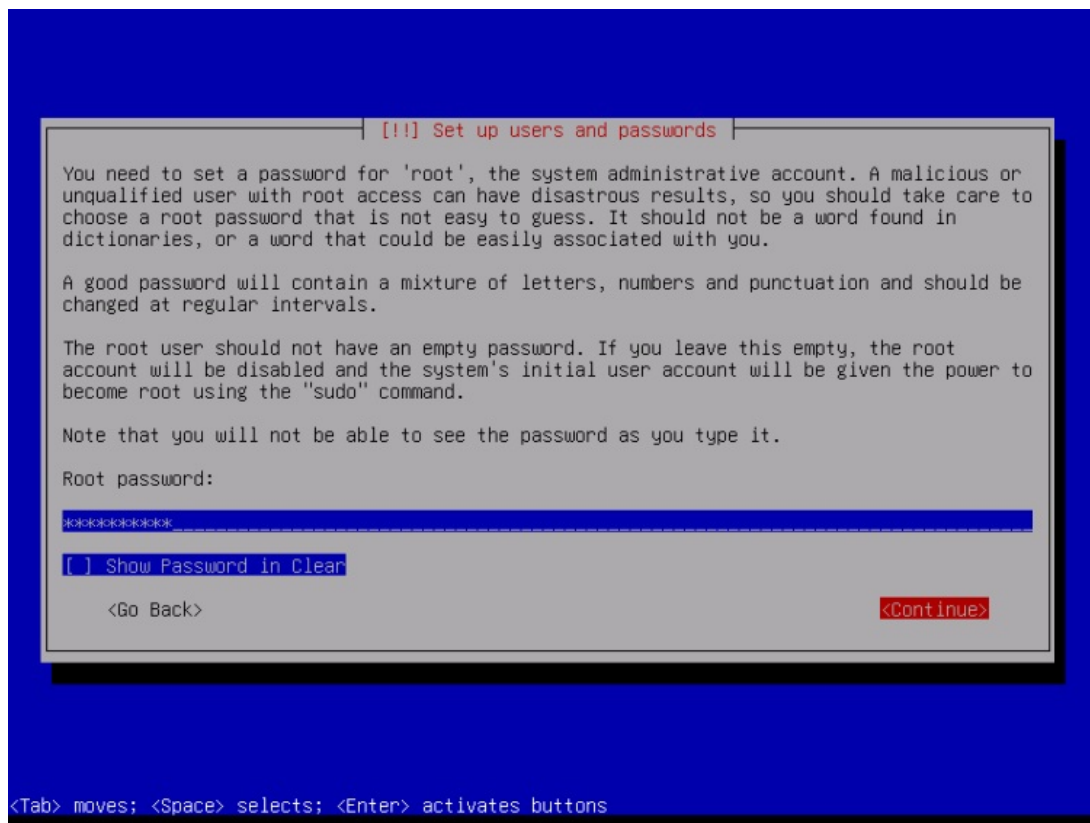
Enter hostname. In this example, my system is called *server1.example.com*, so I enter *server1*:



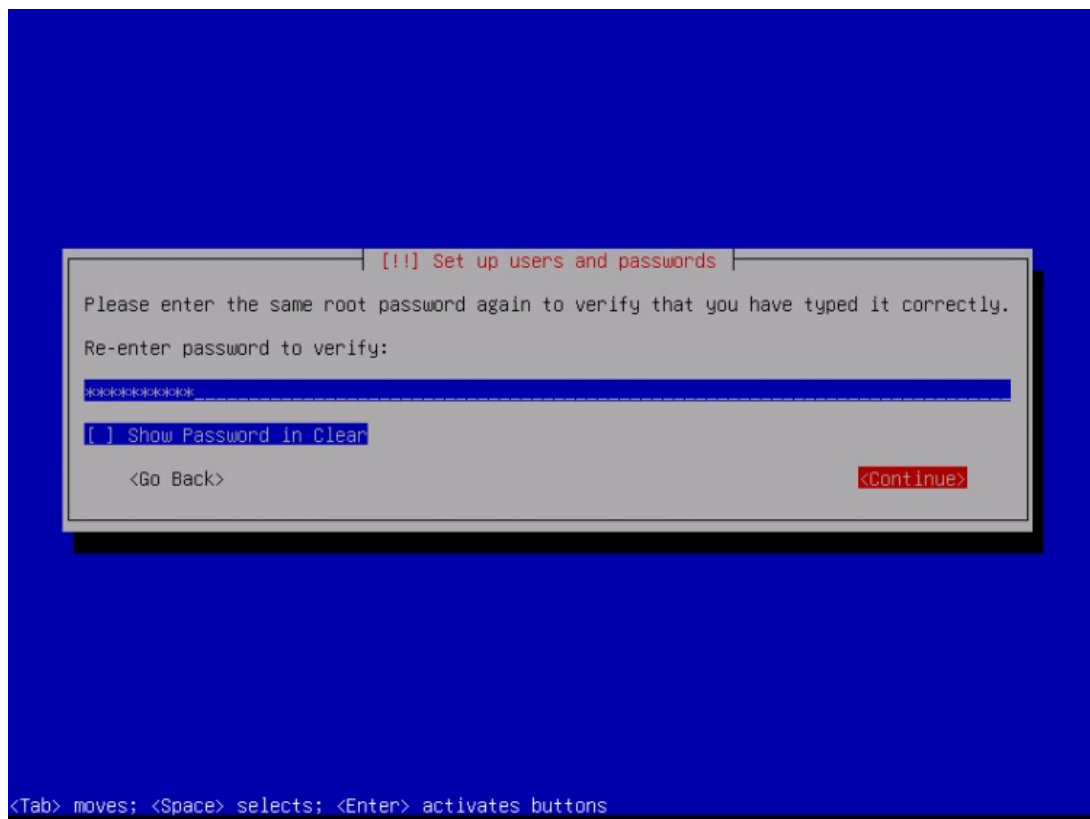
Enter your domain name. In this example, this is *example.com*:



Afterward, give the root user a password:



Confirm that password to avoid typos:



Create a Linux user account, use e.g. your name or nickname. For this example installation, I will choose the name "administrator" with the user name *administrator* (don't use the user name *admin* as it is a reserved name on Debian Linux):

[!!] Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

Administrator\_\_\_\_\_

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

[!!] 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.

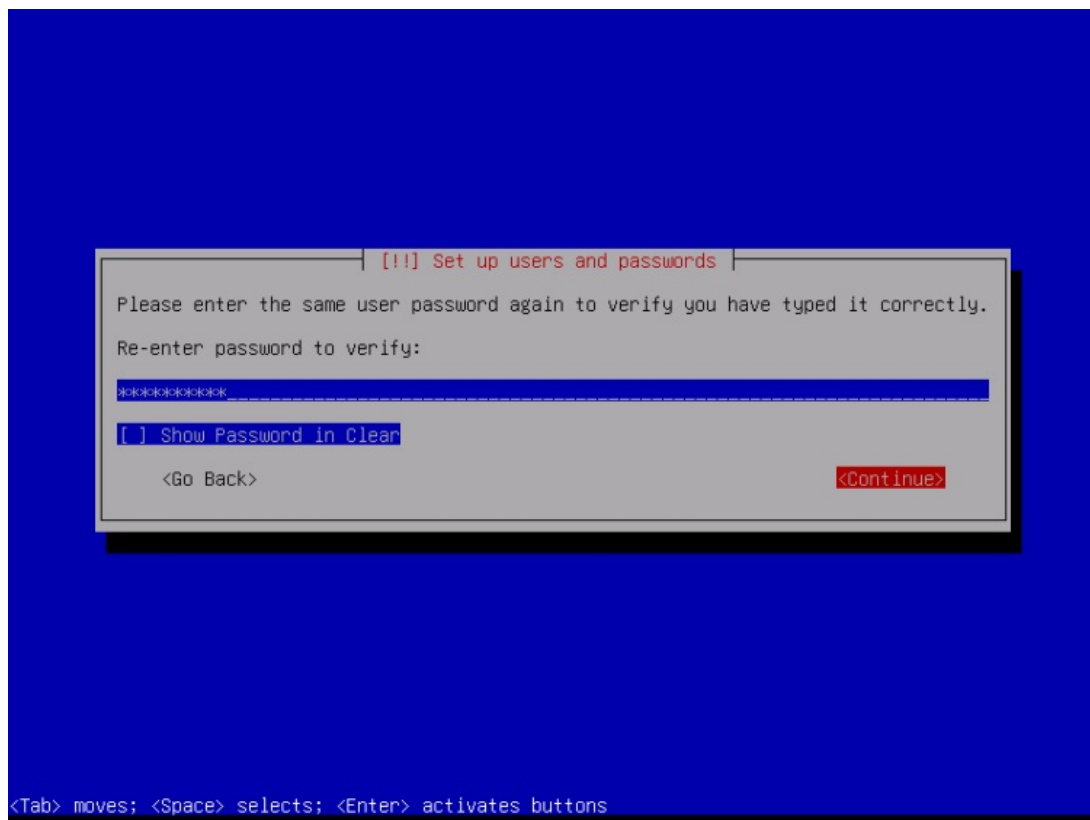
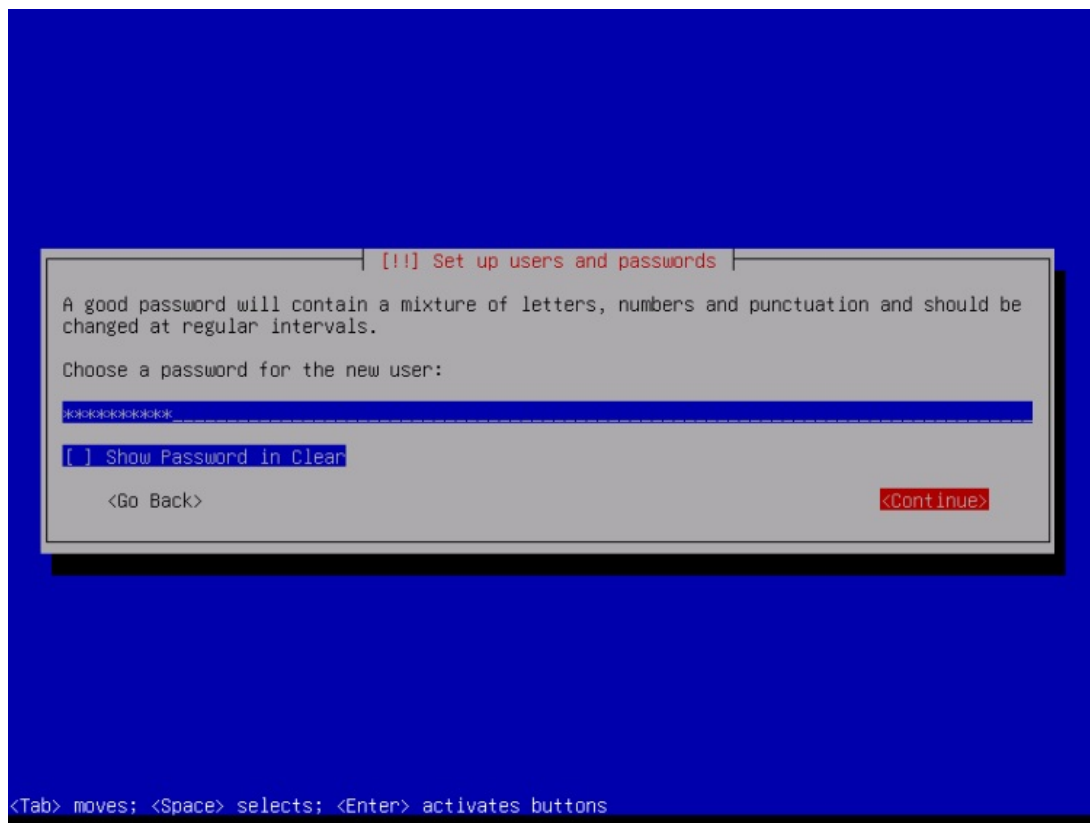
Username for your account:

administrator\_\_\_\_\_

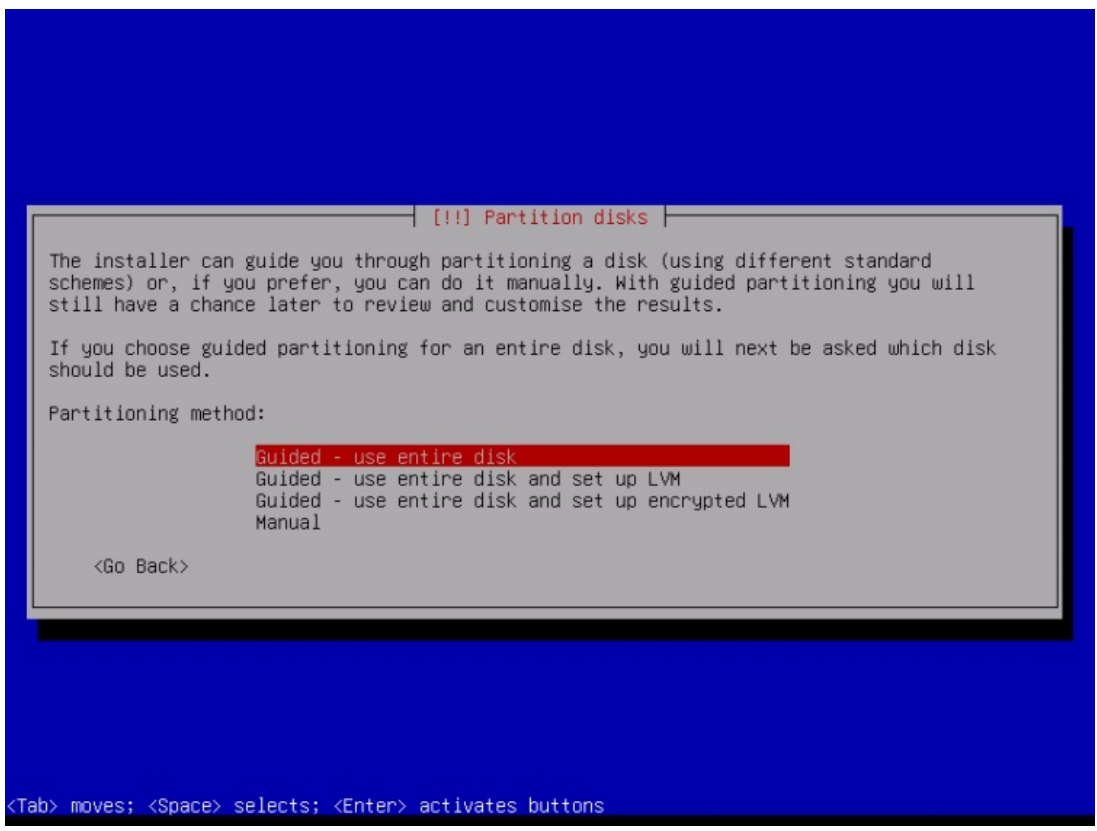
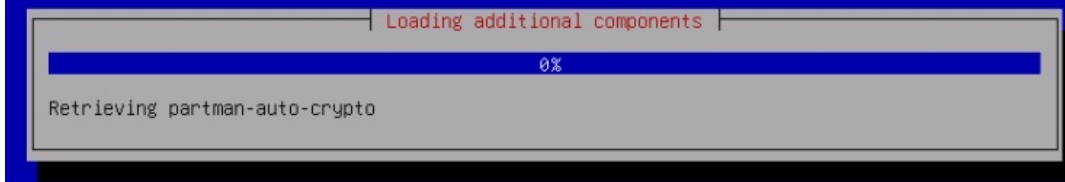
<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

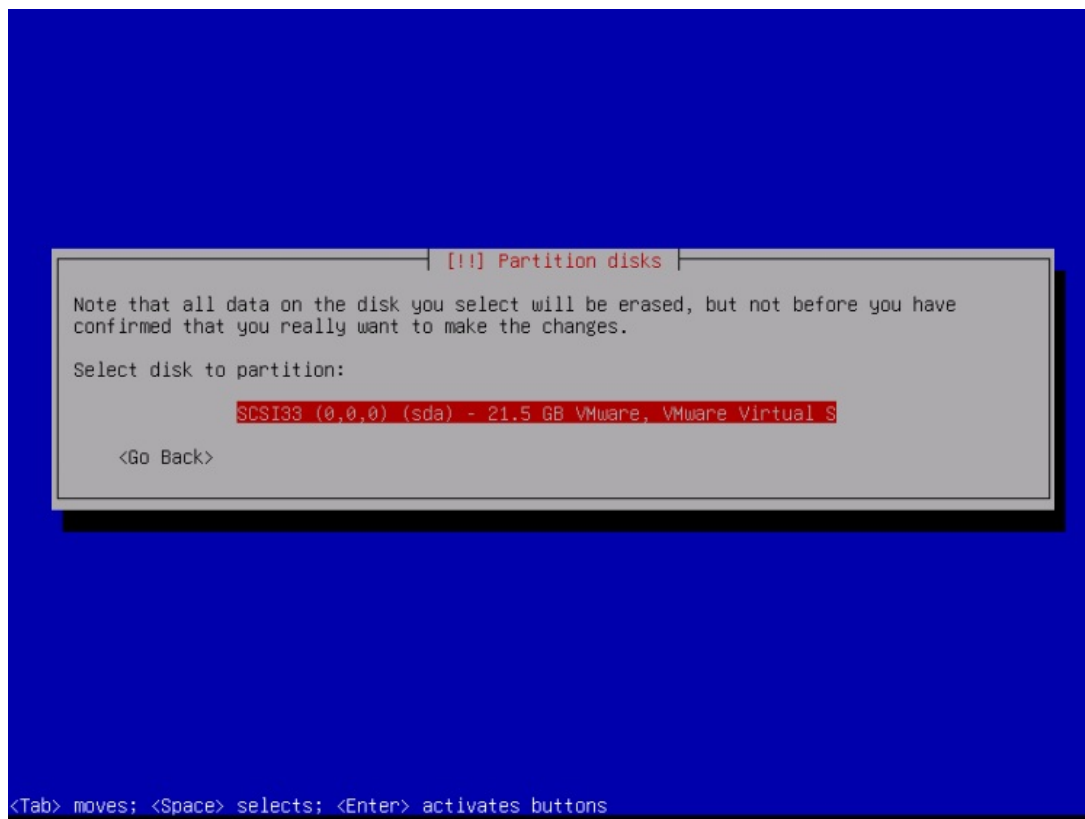




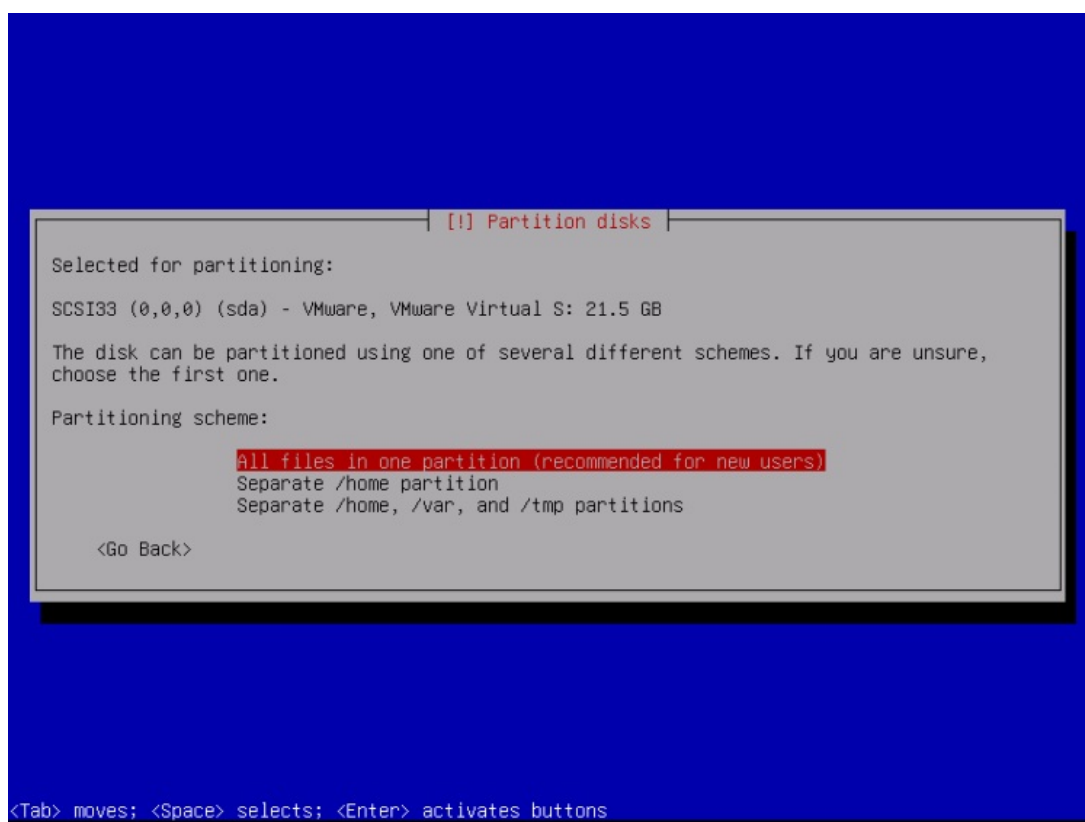
Now you have to partition your hard disk. For simplicity's sake, I select *Guided - use entire disk* - this will create a large partition for the `/` file system and another one for swap (of course, the partitioning is totally up to you - if you know what you're doing, you can also set up your partitions manually). For hosting systems like the ISPConfig 3 perfect server tutorials, you might want to choose e.g., 60GB for `/` and a large `/var` partition, as all website and email data is stored in subdirectories of `/var`.



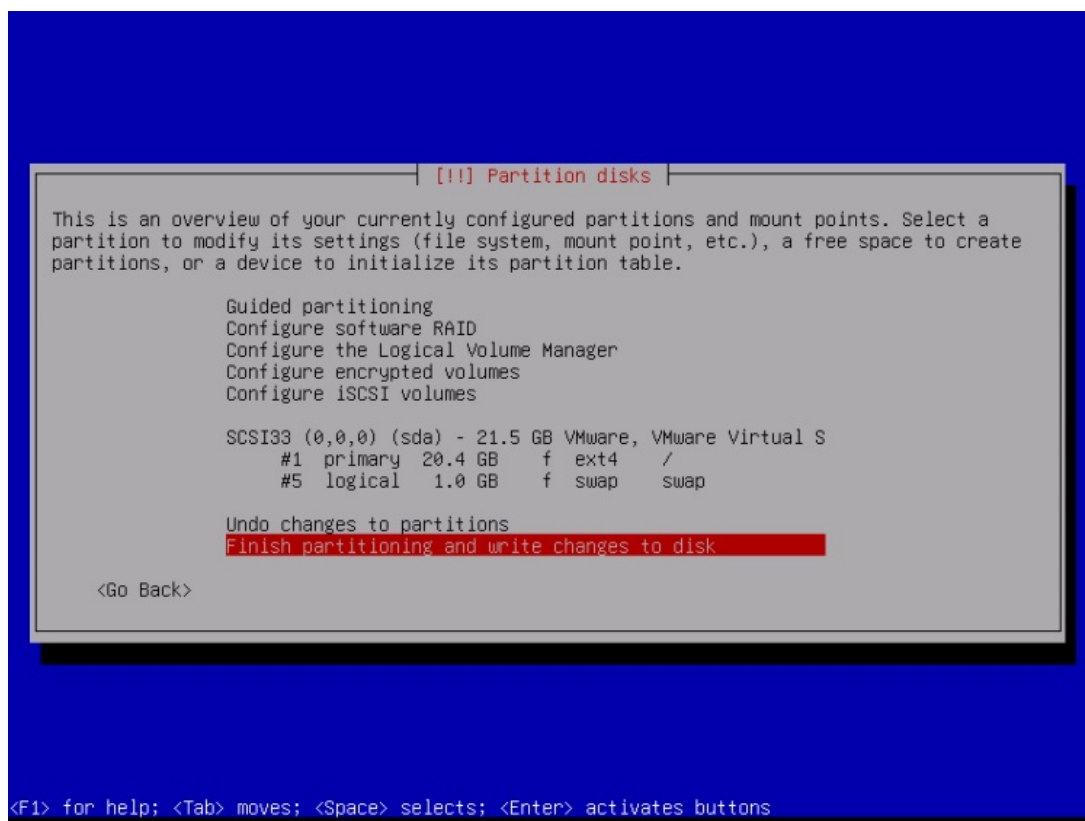
Select the disk that you want to partition:



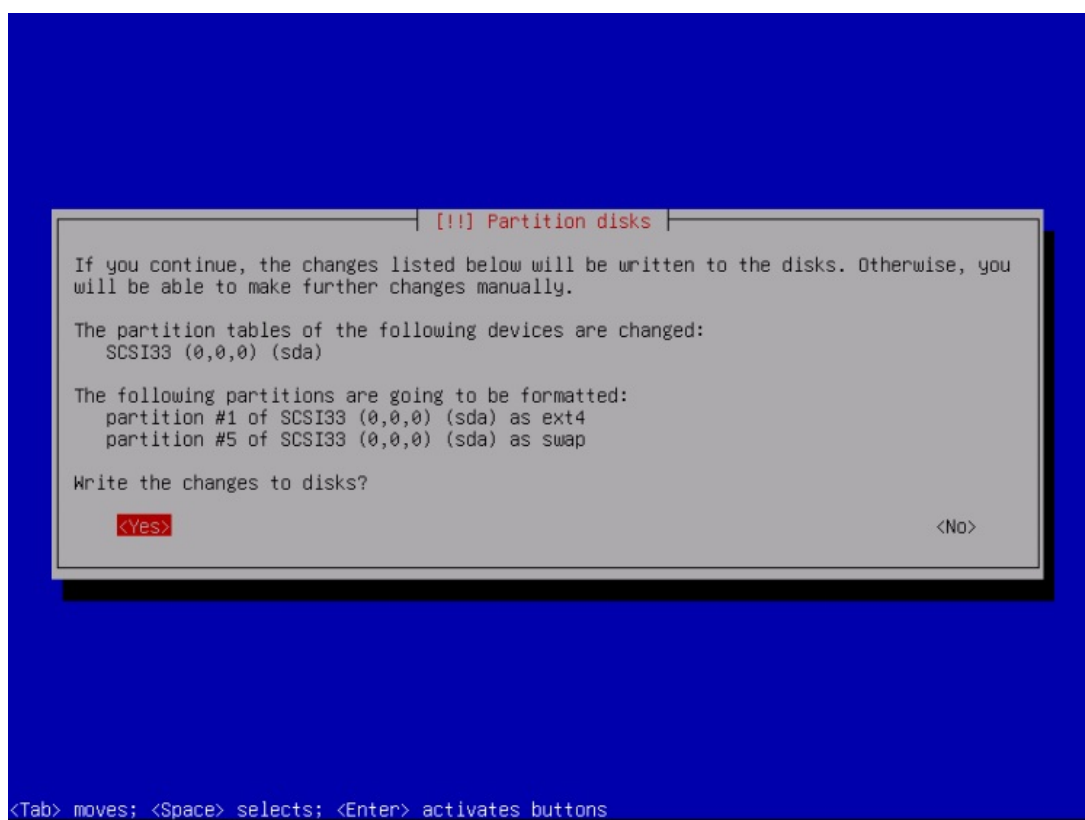
Then select the partitioning scheme. As mentioned before, I select *All files in one partition (recommended for new users)* for simplicity's sake - it's up to your liking what you choose here:



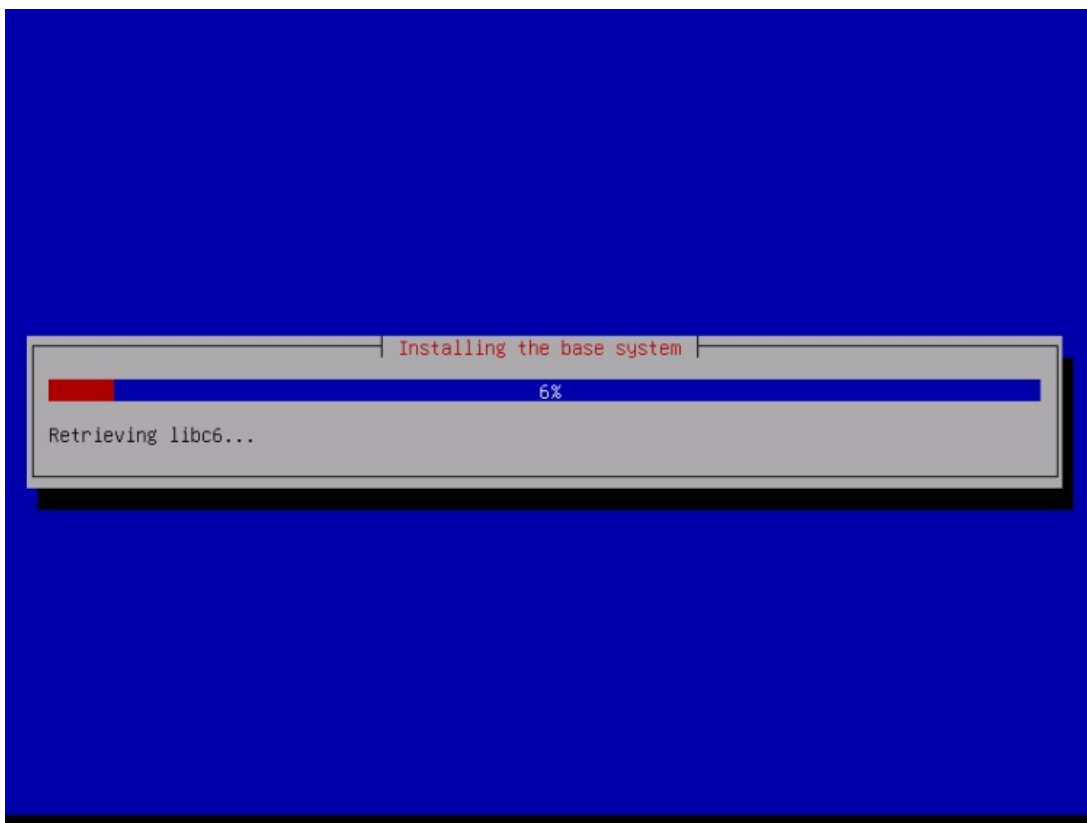
When you're finished, select *Finish partitioning and write changes to disk*:



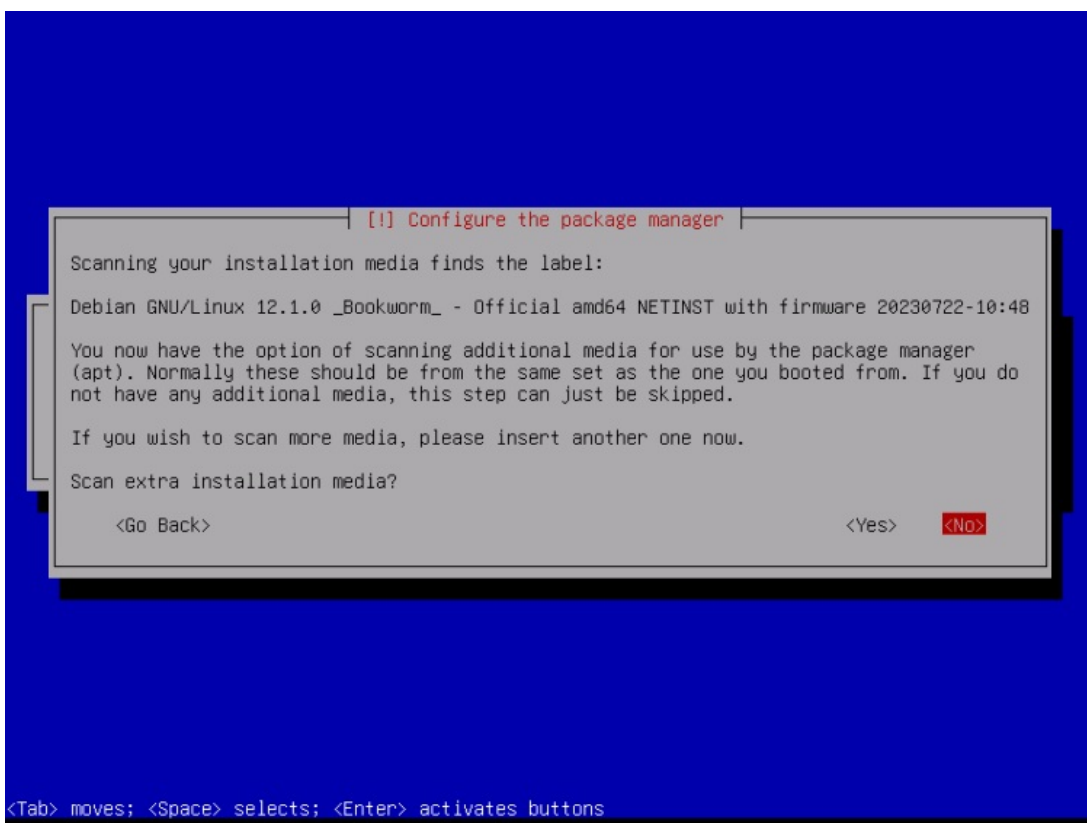
Select *yes* when you're asked: "*Write changes to disk?*":



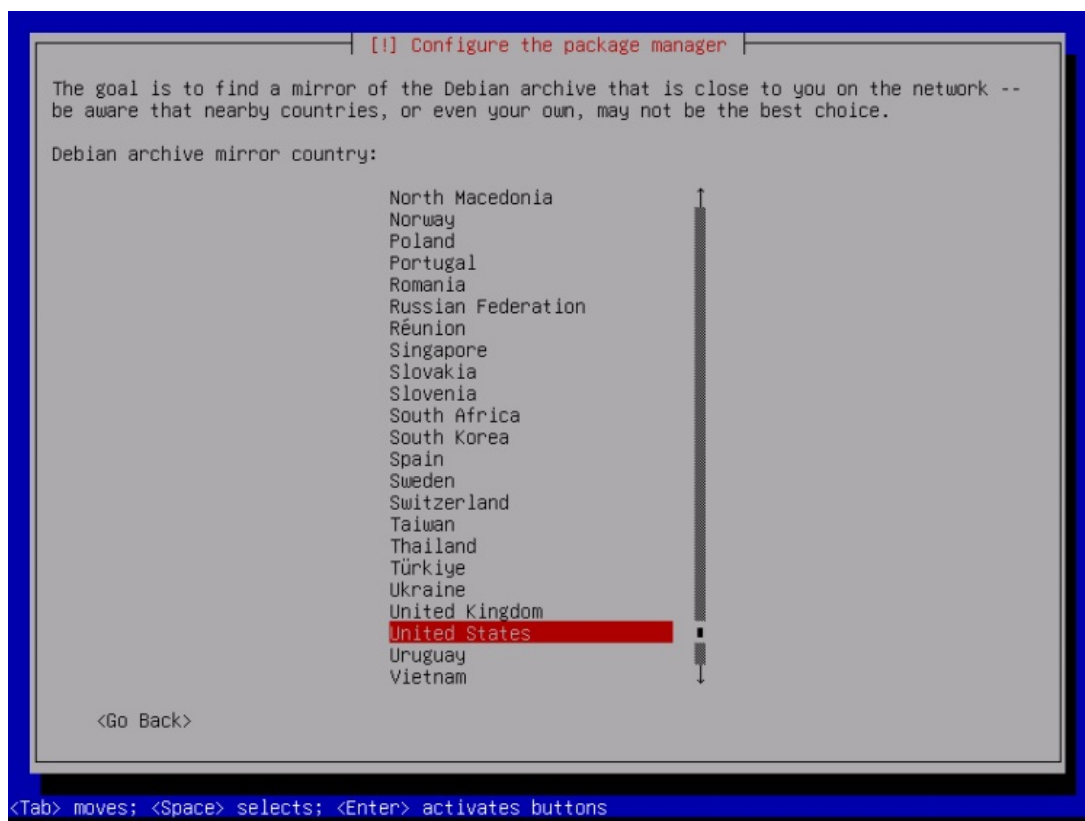
Afterward, your new partitions are created and formatted. Now the partitions are created, and the base system is installed:



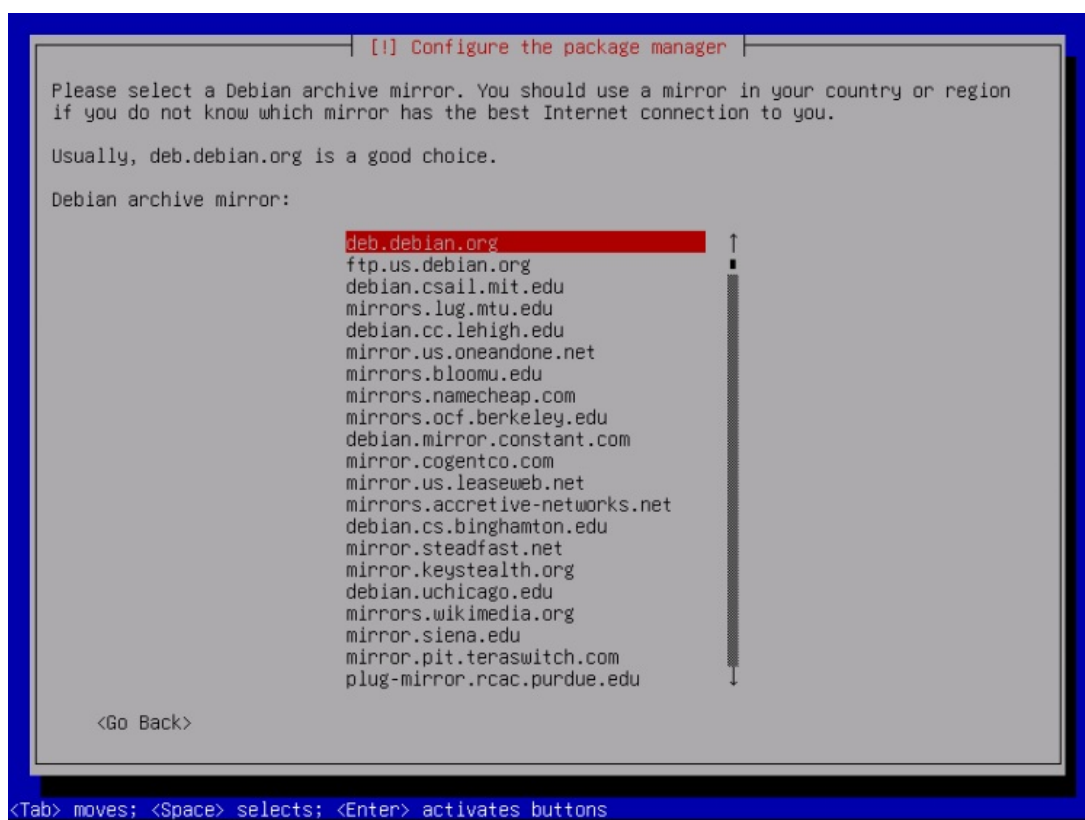
It might be that the following screen pop's up, depending on your install media. I will do a network-based installation (all additional installation packages get downloaded from the internet), so I choose here not to scan any additional install disks.



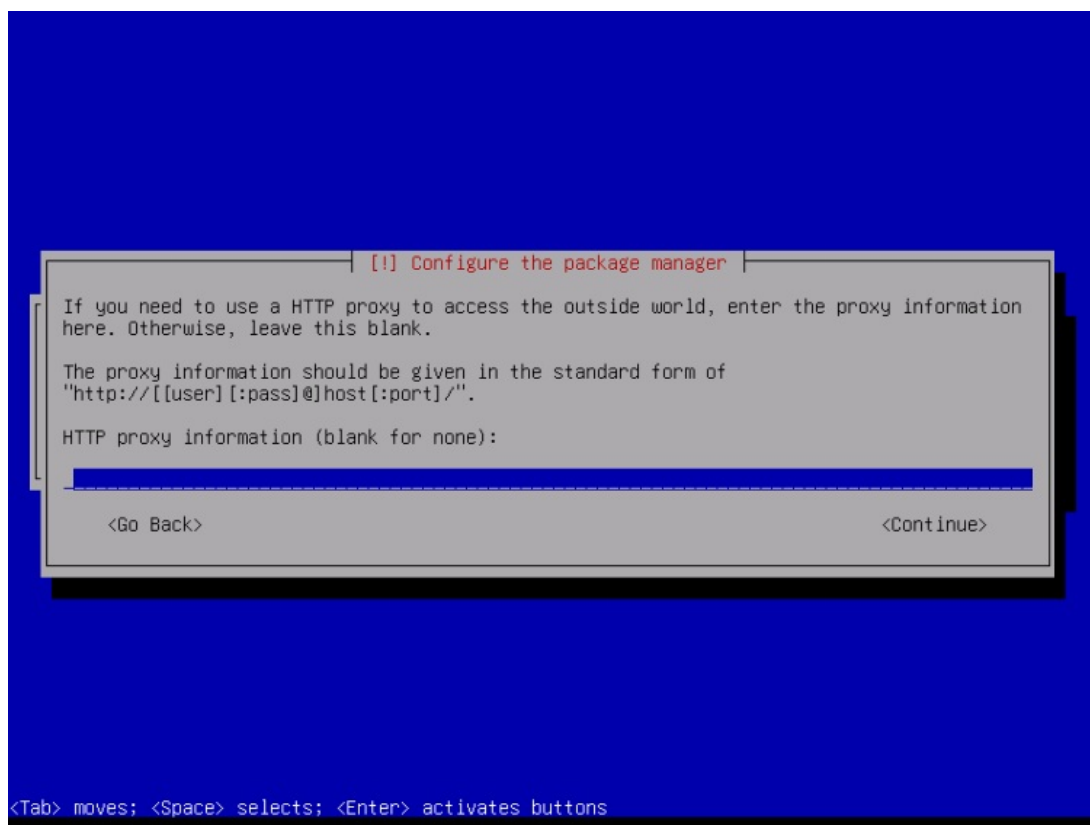
Next, you must configure apt. Because we are using the Debian Netinstall CD, which contains only a minimal set of packages, we must use a network mirror. Select the country where the network mirror that you want to use is located (usually, this is the country where your Server system is located):



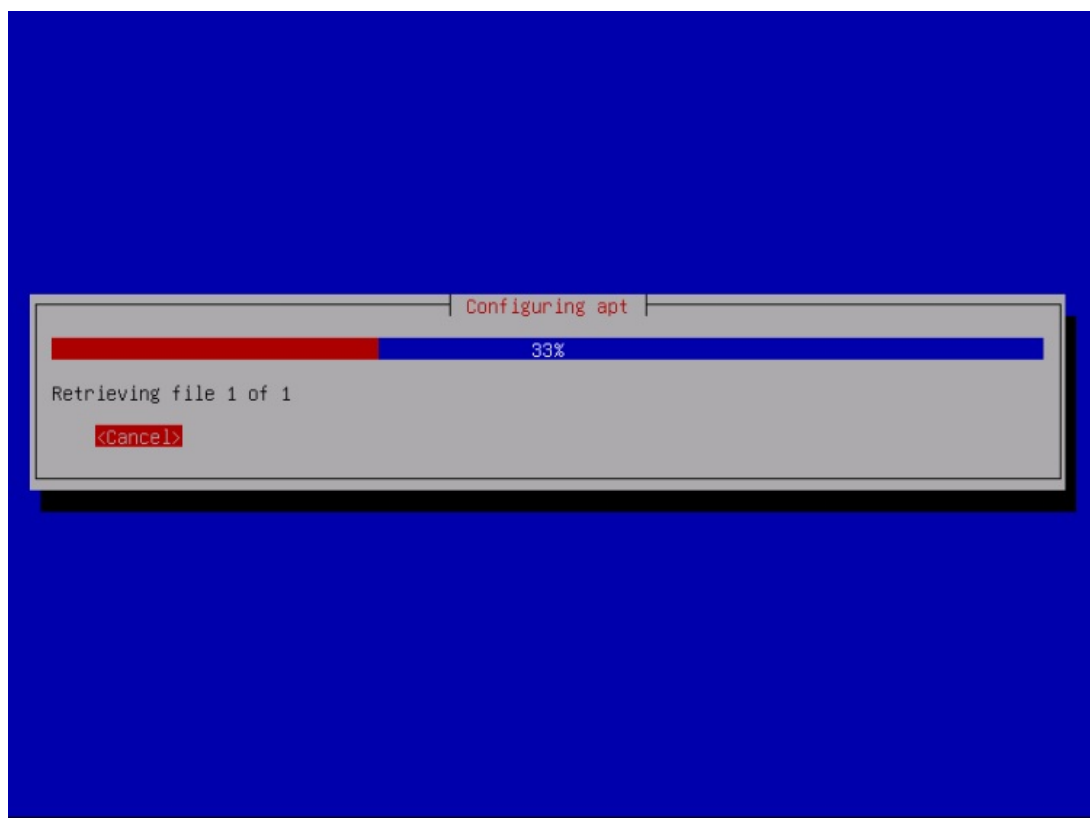
Then select the mirror you wish to use (e.g. *deb.debian.org*):



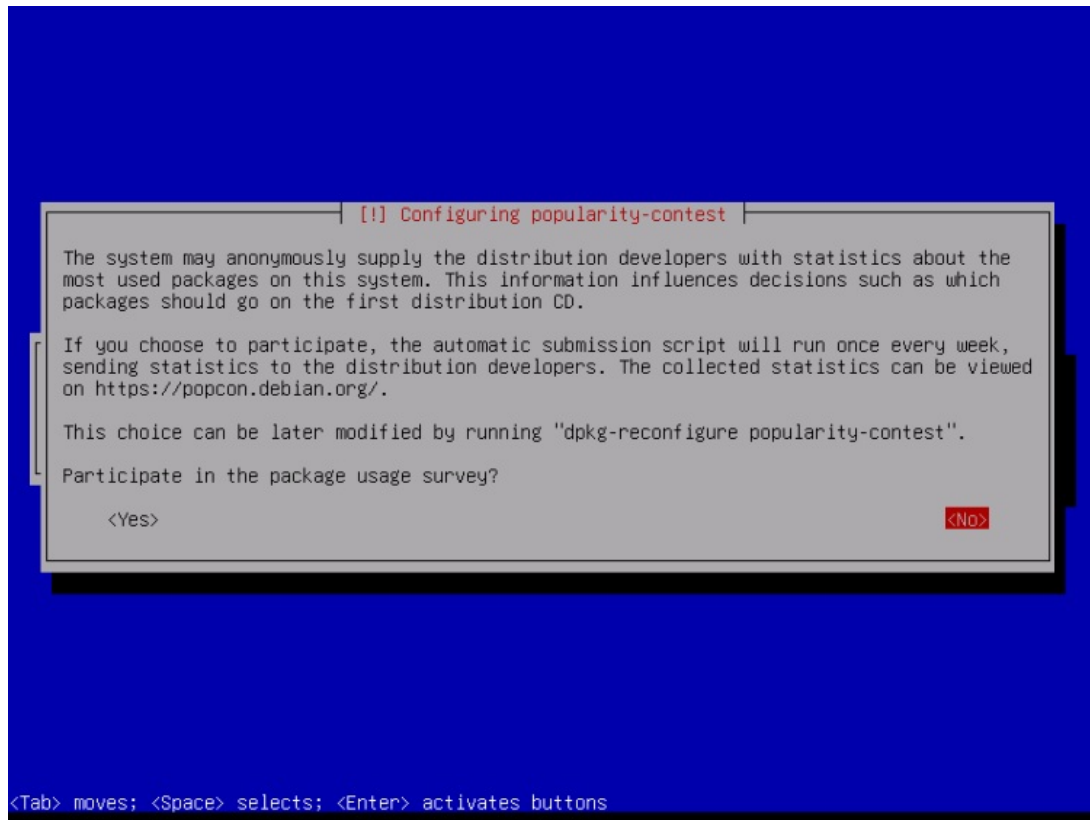
Unless you use an HTTP proxy, leave the following field empty and hit *Continue*:



Apt is now updating its packages database:

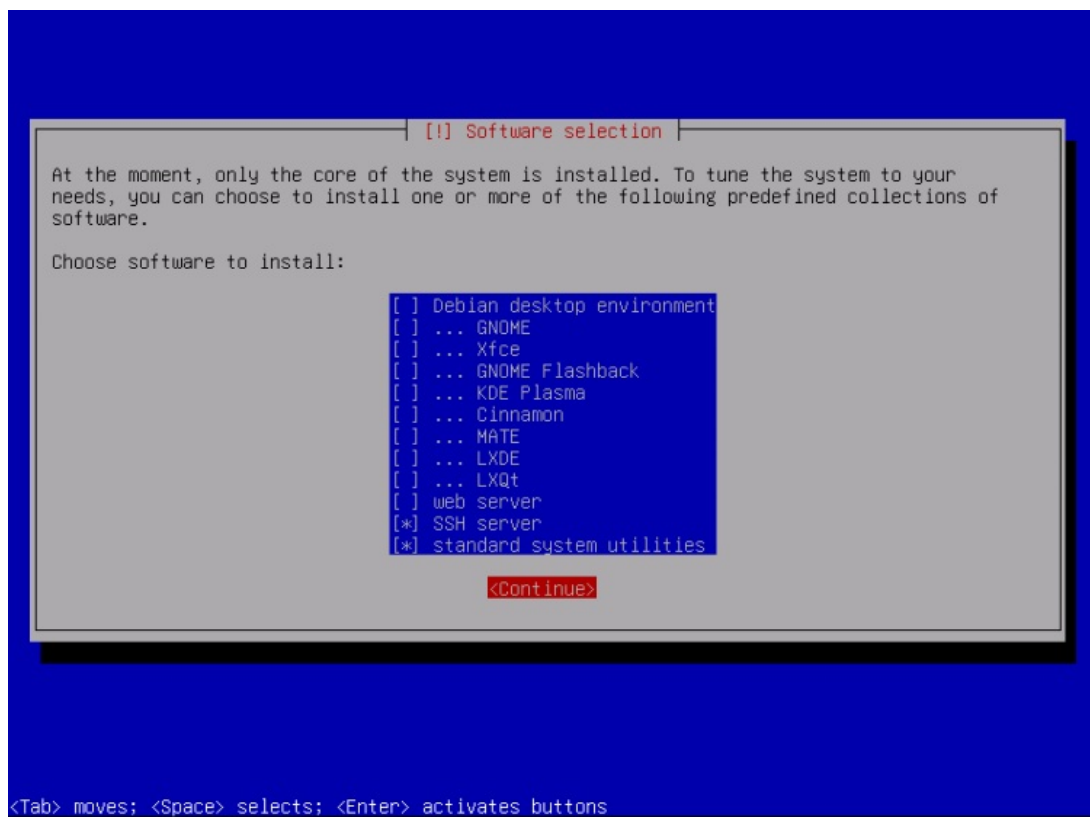


You can skip the package usage survey by selecting *No*:



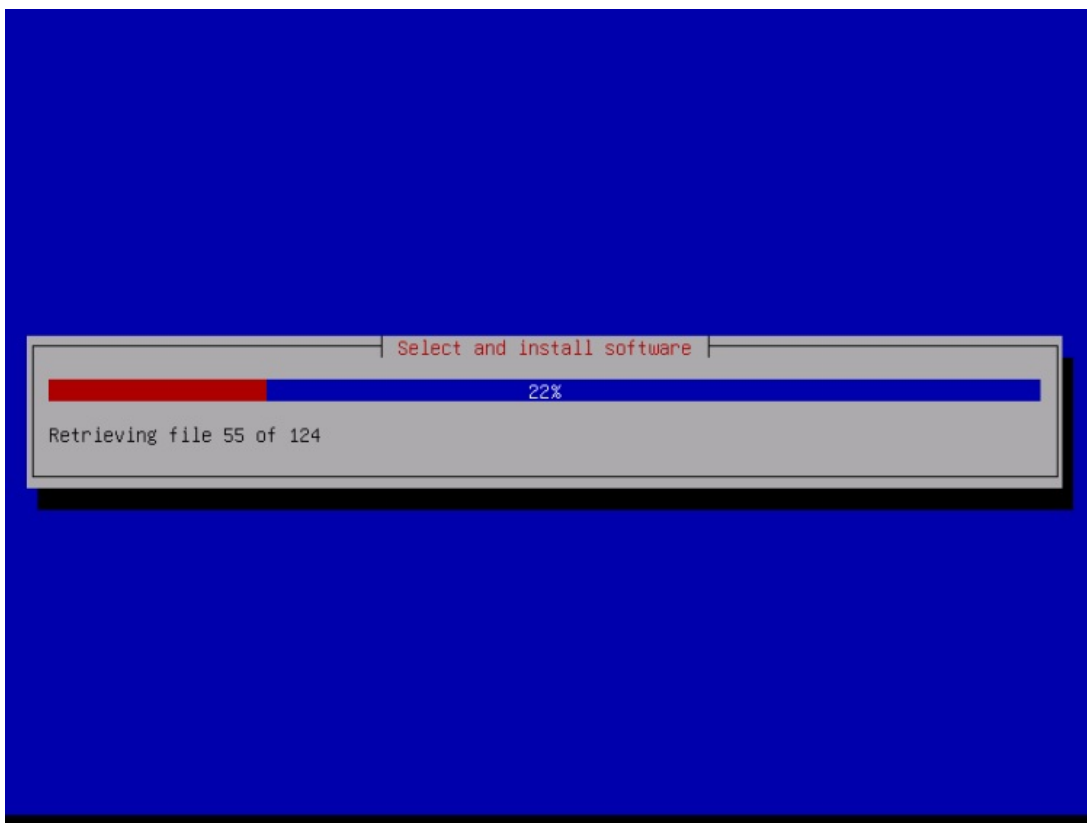
We select Standard system utilities and *SSH server* (so that I can immediately connect to the system with an SSH client such as [PuTTY](#) after the installation has finished) and hit *Continue*.

Some might argue that one should not install Standard System Utilities on a minimal server. Still, in my opinion, you will need most of the standard utilities later anyway, so I will install them on this server as part of the base setup.

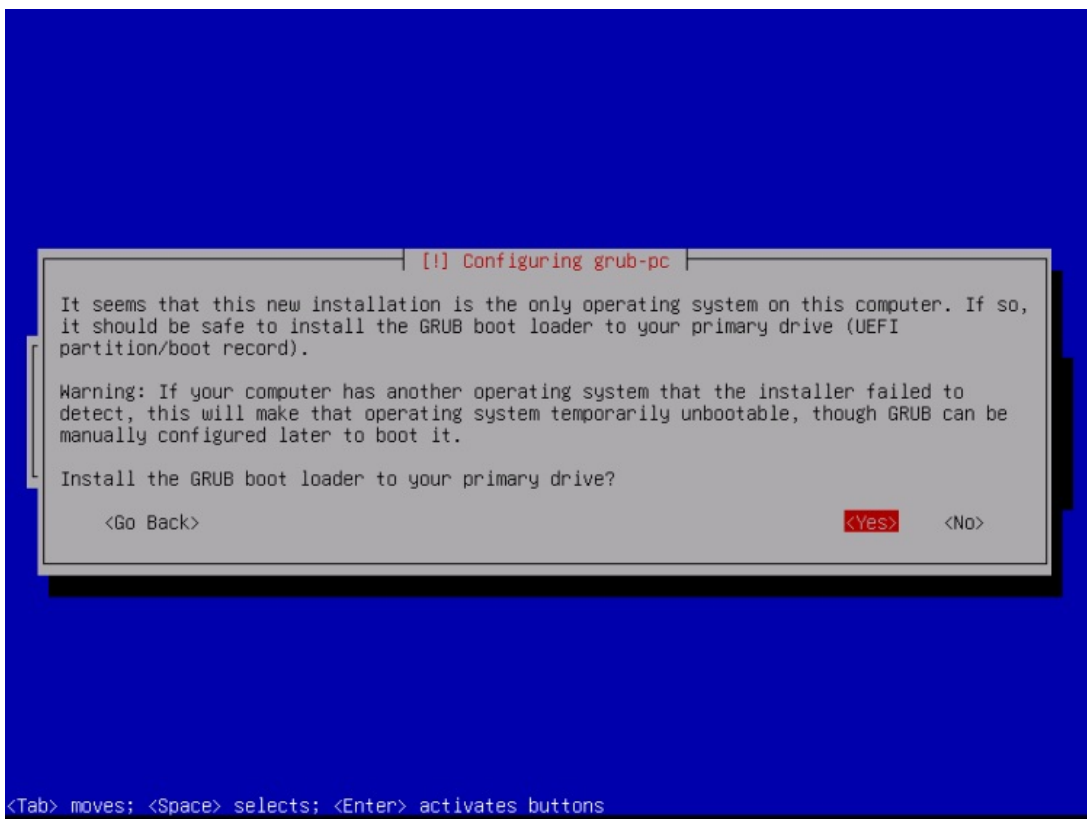


The required packages are downloaded and installed on the system:

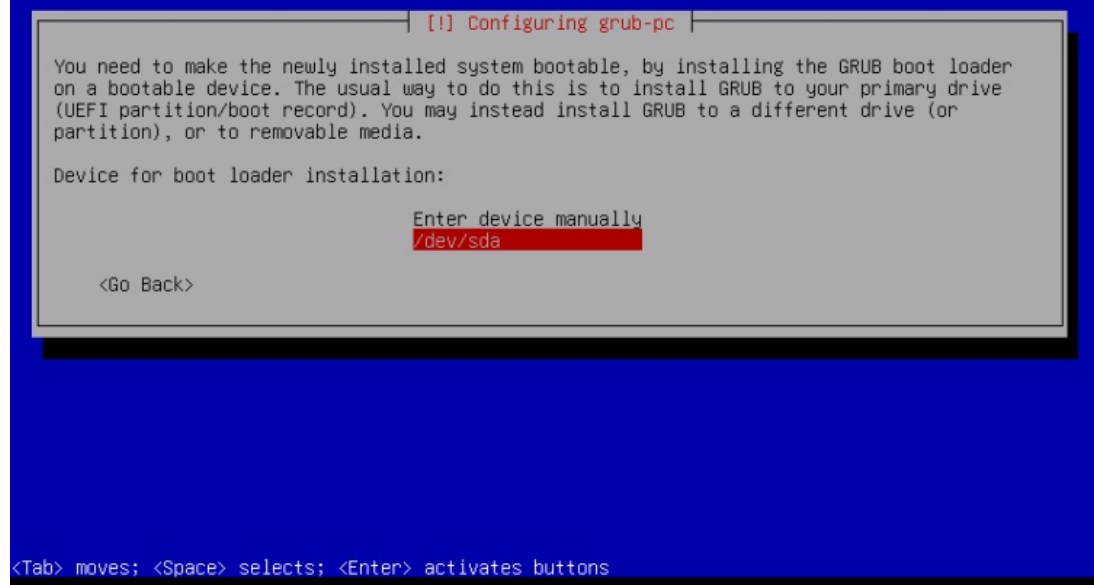




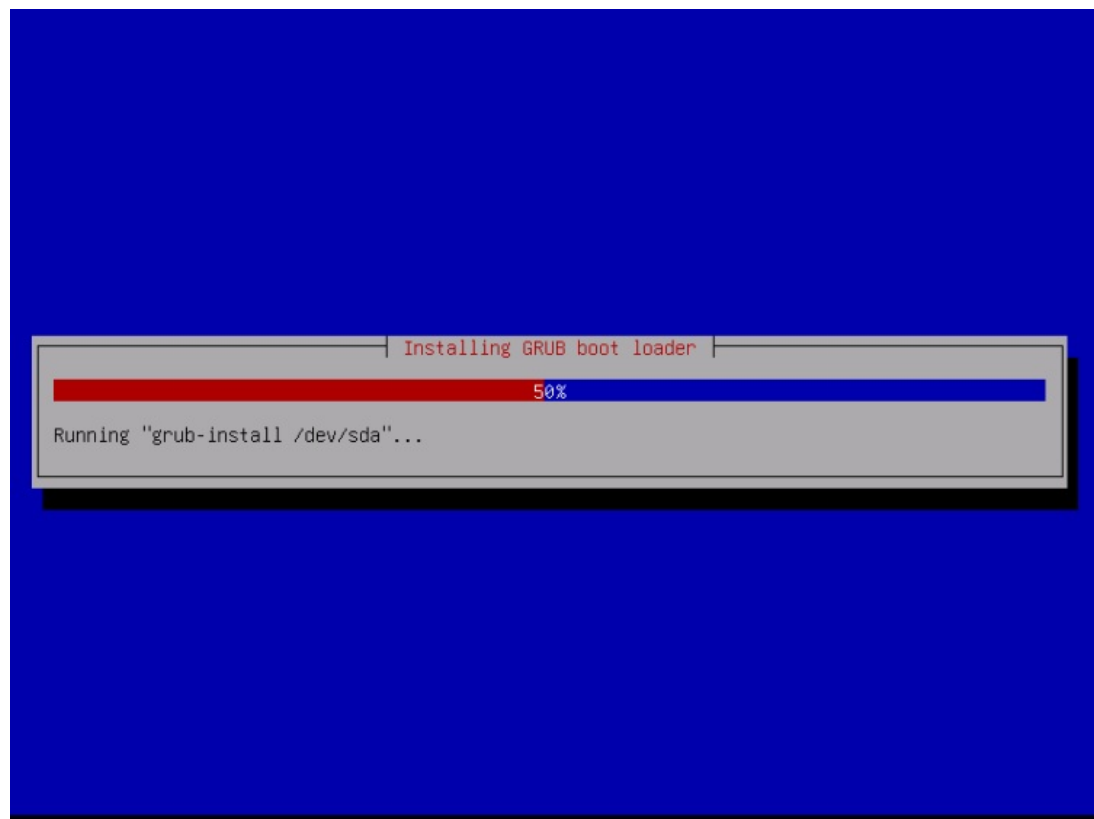
When you're asked to *Install the GRUB boot loader to the master boot record?*, select *Yes*:

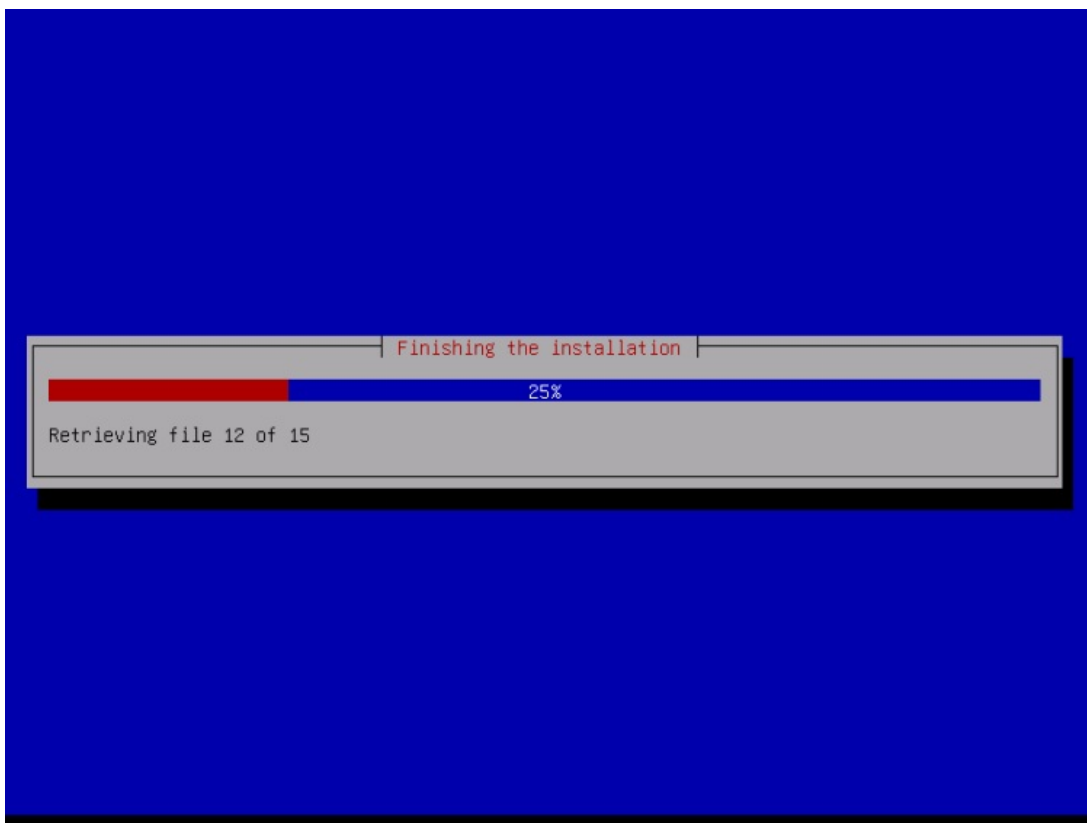


The installer might ask you which partition Grub shall be installed to. This server has just one hard disk, so I choose `/dev/sda` here.

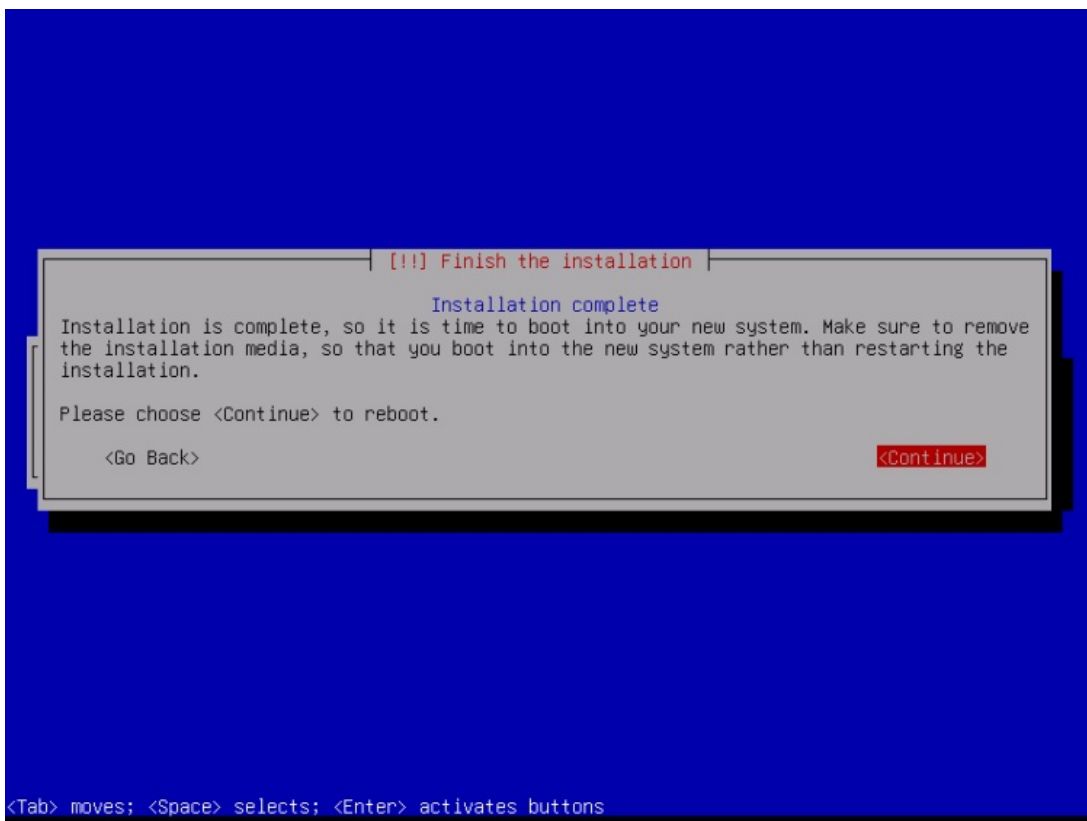


Press enter, and the Installer will install Grub and finishes the installation.

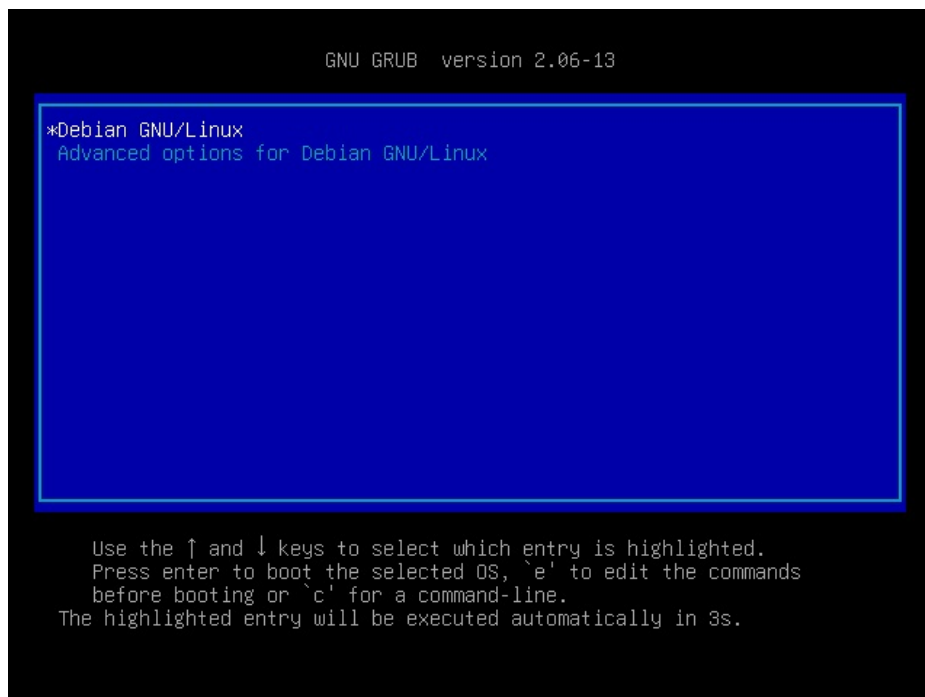




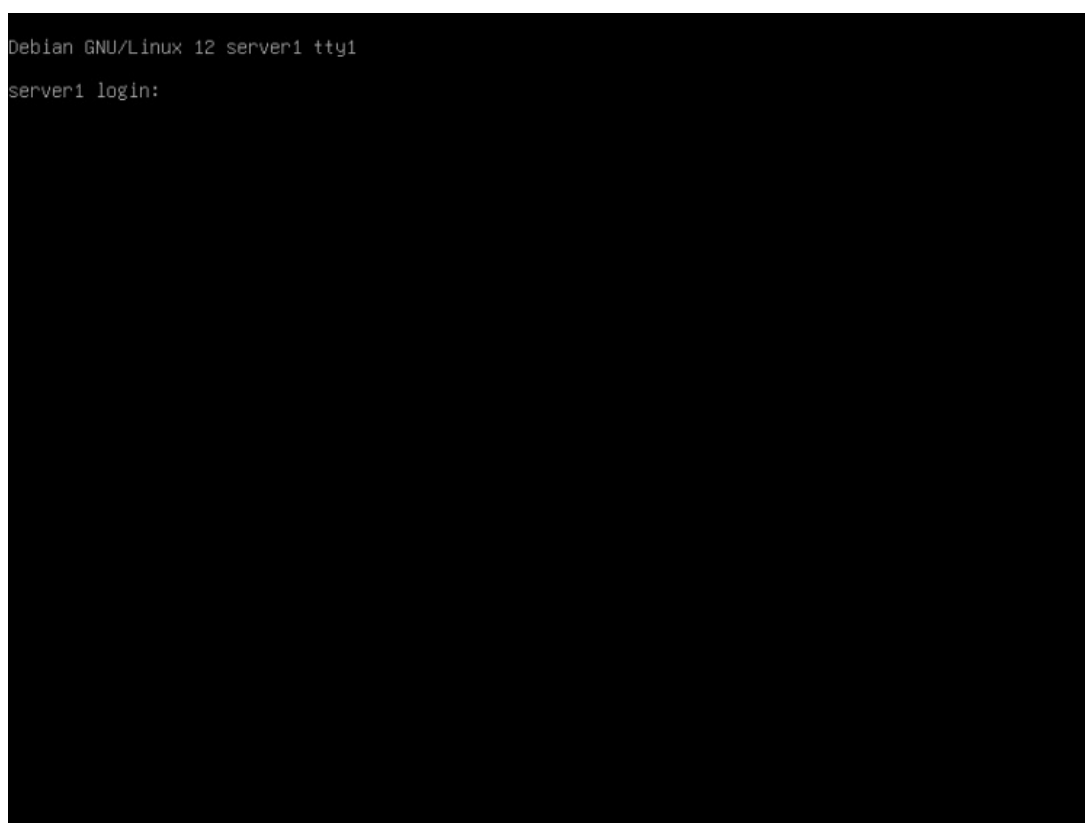
The base system installation is now finished. Remove the Debian Netinstall CD from the CD drive and hit *Continue* to reboot the system:



The first boot of the newly installed Debian 10 server: first, you will see the boot screen of the Grub Boot Loader, press enter or wait a few seconds, and the boot process will continue automatically.



A few seconds later, the login prompt should show up.



Log in with the username "root" and the root password that you have chosen during installation. When you log in by SSH, then use the username "administrator" as the root user is disabled for remote logins. Then run the command "su -":

```
su -
```

To become the root user. It is important that you use the command su with '-' or use 'su --login' as this is required to initialize the PATH variable correctly for the root user.

On to the next step...

## 4 Install The SSH Server (Optional)

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

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

From now on you can use an SSH client such as [PuTTY](#) and connect from your workstation to your Debian Jessie server and follow the remaining steps from this tutorial.

## 5 Install a shell editor (Optional)

I'll use *nano* as my favorite shell text editor. Others prefer *vi*, which is not that easy to use for beginners. With the following command, I will install both editors:

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

(You don't have to do this if you use a different text editor such as *joe* or the built-in editor from *mc*).

## 6 Configure The Network

You can get your current IP address with the command:

```
ip a
```

By default, some network tools might not be available. Install the package with the following command:

```
apt install net-tools
```

Because the Debian 12 installer has configured our system to get its network settings via DHCP, we have to change that now because a server should have a static IP address. Edit */etc/network/interfaces* and adjust it to your needs (in this example setup, I will use the IP address *192.168.0.100*) (please note that I replace *allow-hotplug ens33* with *auto ens33*; otherwise, restarting the network doesn't work, and we'd have to reboot the whole system):

```
nano /etc/network/interfaces
```

The interfaces file with DHCP enabled as created by the apt installer:

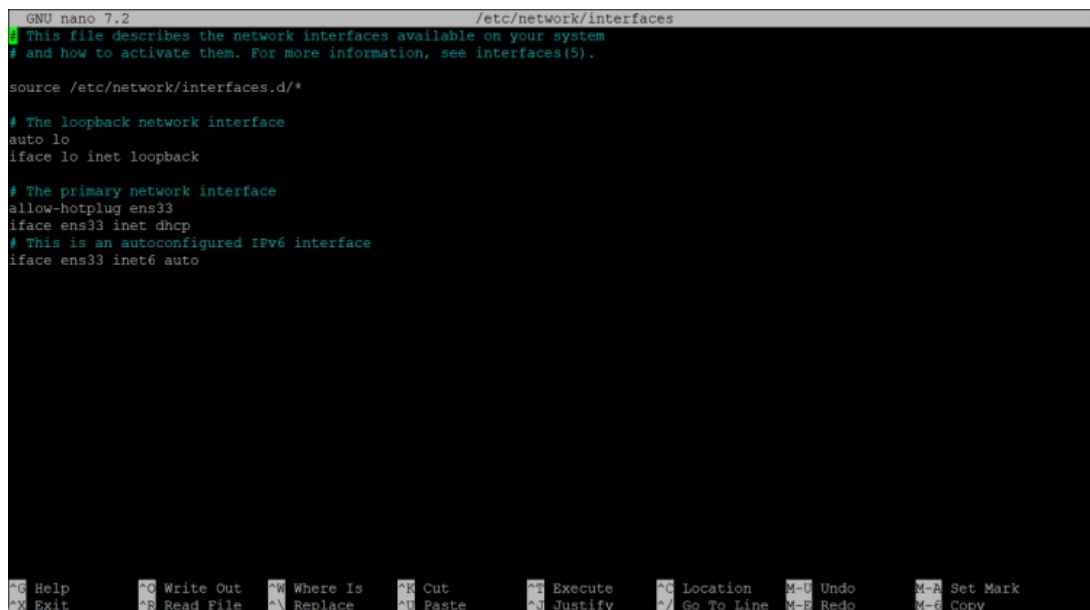
```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
```

```
source /etc/network/interfaces.d/*
```

```
# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp
# This is an autoconfigured IPv6 interface
iface ens33 inet6 auto
```

Or as a screenshot:



And here is the edited interfaces file with the static IP 192.168.0.100 configured.

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

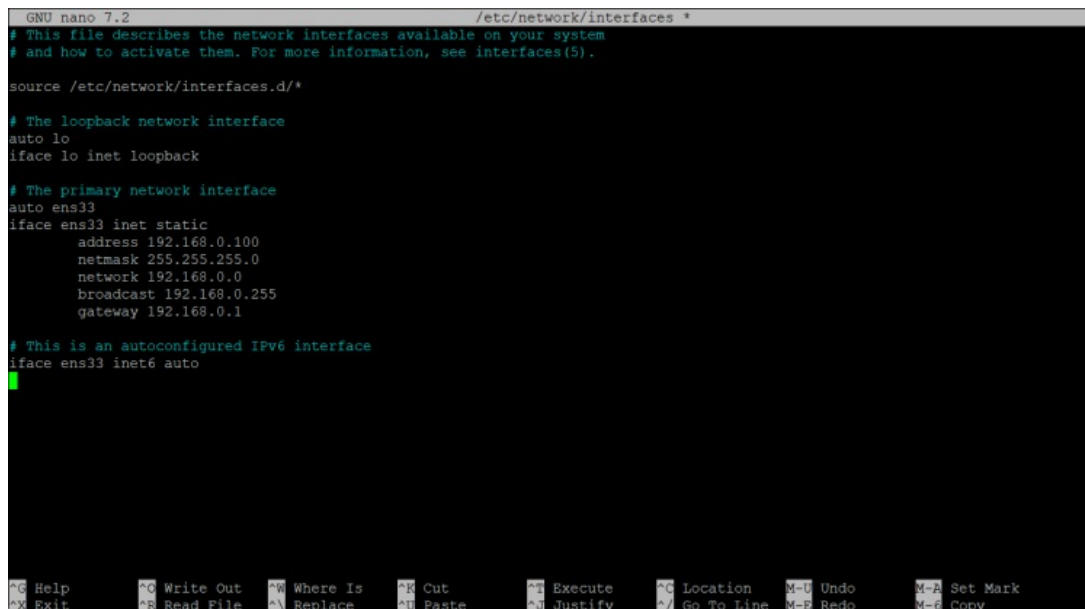
```
source /etc/network/interfaces.d/*
```

```
# The loopback network interface
auto lo
iface lo inet loopback
```

```
# The primary network interface
auto ens33
iface ens33 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

# This is an autoconfigured IPv6 interface
iface ens33 inet6 auto
```

The edited file should look like this:



```
GNU nano 7.2 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens33
iface ens33 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

# This is an autoconfigured IPv6 interface
iface ens33 inet6 auto
```

Then restart your network:

```
systemctl restart networking
```

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

```
nano /etc/hosts
```

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

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

Now edit the hostname in case you did not select the final hostname in the installer

```
nano /etc/hostname
```

The `/etc/hostname` file contains the hostname without the domain part, so in our case just "server1".

Then reboot the server to apply the hostname change:

```
systemctl reboot
```

After you log in again, run the following command:

```
hostname
hostname -f
```

To verify that the new hostname is set correctly. The output should be:

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

## 7 Update Your Debian Installation

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

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

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

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

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

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

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

Run

```
apt update
```

to update the apt package database and

```
apt upgrade
```

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

## 8 Debian 12 VMWare Server Image

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

### SSH / Shell Login

Username: administrator  
Password: howtoforge

Username: root  
Password: howtoforge

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

## 9 Links

- Debian: <http://www.debian.org/>

---

This PDF file is provided by howtoforge.com <https://www.howtoforge.com>. (c) projektfarm GmbH - republishing not permitted.

# The Perfect Server - Debian 12 (Bookworm) with Apache, BIND, Dovecot, PureFTPD and ISPConfig 3.2

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

This tutorial shows the manual installation procedure for ISPConfig, which takes some time but gives you full control over all installation steps. The fast and easy installation method (which we highly recommend!) is to use the ISPConfig auto-installer instead. You can find the ISPConfig installation tutorial for the auto-installer here: <https://www.howtoforge.com/ispconfig-autoinstall-debian-ubuntu/>

## 1 Preliminary Note

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

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

```
su -
```

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

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

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

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

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

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

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

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

Save the file.

## 2 Install the SSH server (Optional)

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

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

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

## 3 Install a shell text editor (Optional)

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

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

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



## 4 Configure the Hostname

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

```
nano /etc/hosts
```

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

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

Then edit the */etc/hostname* file:

```
nano /etc/hostname
```

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

```
server1
```

Finally, reboot the server to apply the change:

```
systemctl reboot
```

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

```
hostname
hostname -f
```

The output shall be like this:

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

## 5 Update your Debian Installation

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

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

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

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

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

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

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

Run:

```
apt update
```

To update the apt package database

```
apt upgrade
```

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

## 6 Synchronize the System Clock

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

```
apt -y install ntp
```

and your system time will always be in sync.

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

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

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

You will be asked the following questions:

General type of mail configuration: <-- [Internet Site](#)  
System mail name: <-- [server1.example.com](#)

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

```
mysql_secure_installation
```

Answer the questions as follows:

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

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

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

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

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

Restart Postfix afterward:

```
systemctl restart postfix
```

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

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

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

```
[...]
```

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

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

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

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

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

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

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

and add these lines at the end of the file.

```
mysql soft nfile 65535
mysql hard nfile 65535
```

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

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

and add a new file inside:

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

paste the following lines into that file:

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

Save the file and close the nano editor.

Then we reload systemd and restart MariaDB:

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

Now check that networking is enabled. Run

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

The output should look like this:

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

## 8 Install Email filter and signing software Rspamd and ClamAV

Add the Rspamd repository:

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

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

To install Rspamd and ClamAV, we run

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

Activate Redis in Rspamd configuration.

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

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

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

Then restart Rspamd.

```
systemctl restart rspamd
```

## 9 Install Apache Web Server and PHP

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

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

Now enable php-fpm in Apache:

```
a2enmod proxy fcgi setenvif
a2enconf php8.2-fpm
```

Then run the following command to enable the additional Apache modules *suexec*, *rewrite*, *ssl*, *actions*, and *include* (plus *dav*, *dav\_fs*, and *auth\_digest* if you want to use WebDAV):

```
a2enmod suexec rewrite ssl actions include dav_fs dav auth_digest cgi headers actions alias
```

To ensure that the server cannot be attacked through the [HTTPOXY vulnerability](#), we will disable the HTTP\_PROXY header in apache globally by adding the configuration file /etc/apache2/conf-available/httpoxy.conf.

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

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

Paste the following content to the file:

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

And enable the module by running:

```
a2enconf httpoxy
systemctl restart apache2
```

## 10 Install Let's Encrypt

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

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

## 11 Install PureFTPd and Quota

PureFTPd and quota can be installed with the following command:

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



Create the dhparam file for pure-ftpd:

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

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

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

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

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

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

If you want to allow FTP and TLS sessions, run

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

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

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

Afterwards, we can generate the SSL certificate as follows:

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

```
Country Name (2 letter code) [AU]: <-- Enter your Country Name (e.g., "DE").
State or Province Name (full name) [Some-State]: <-- Enter your State or Province Name.
Locality Name (eg, city) []: <-- Enter your City.
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter your Organization Name (e.g., the name of your company).
Organizational Unit Name (eg, section) []: <-- Enter your Organizational Unit Name (e.g., "IT Department").
Common Name (eg, YOUR name) []: <-- Enter the Fully Qualified Domain Name of the system (e.g. "server1.example.com").
Email Address []: <-- Enter your Email Address.
```

Change the permissions of the SSL certificate:

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

Then restart PureFTPD:

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

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

```
nano /etc/fstab
```

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=45576b38-39e8-4994-b8c1-ea4870e2e614 / ext4 errors=remount-ro,usrjquota=quota.user,grpjquota=quota.group,jqfmt=vfsv0 0 1
# swap was on /dev/sda5 during installation
UUID=8bea0d1e-ec37-4b20-9976-4b7daaa3eb69 none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
```

To enable quota, run these commands:

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

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

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

## 12 Install BIND DNS Server

BIND can be installed as follows:

```
apt install bind9 dnsutils
```

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

```
apt install haveged
```

An explanation on that topic can be found [here](#).

## 13 Install Webalizer replacement awffull, AWStats and GoAccess

Webalizer and AWStats can be installed as follows:

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

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

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

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

```
nano /etc/cron.d/awstats
```

... and comment out everything in that file:

```
#MAILTO=root
```

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

```
# Generate static reports:
```

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

Installing the latest GoAccess version directly from the GoAccess repository:

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

## 14 Install Jailkit

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

```
apt install jailkit
```

## 15 Install fail2ban and UFW Firewall

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

```
apt install fail2ban
```

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

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

And add the following configuration to it.

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

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

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

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

Restart fail2ban afterwards:

```
systemctl restart fail2ban
```

To install the UFW firewall, run this apt command:

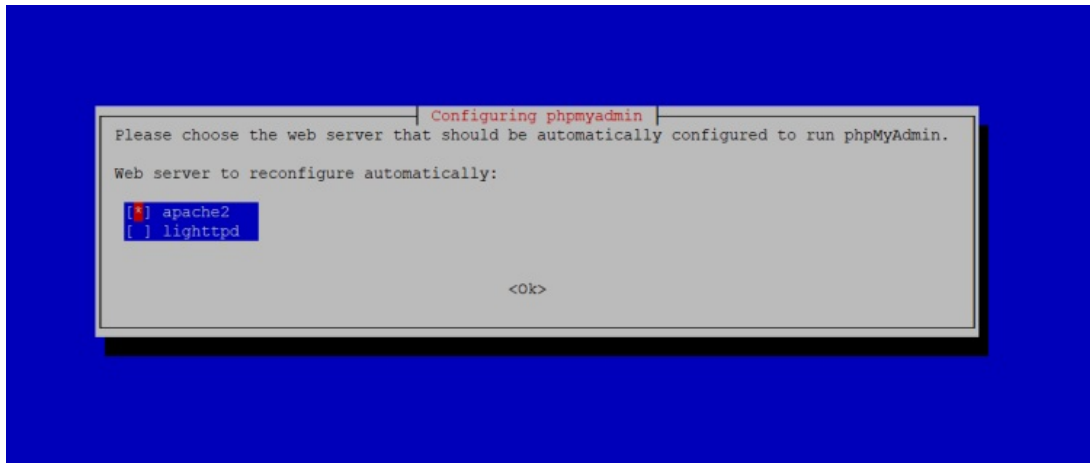
```
apt install ufw
```

## 16 Install PHPMyAdmin Database Administration Tool

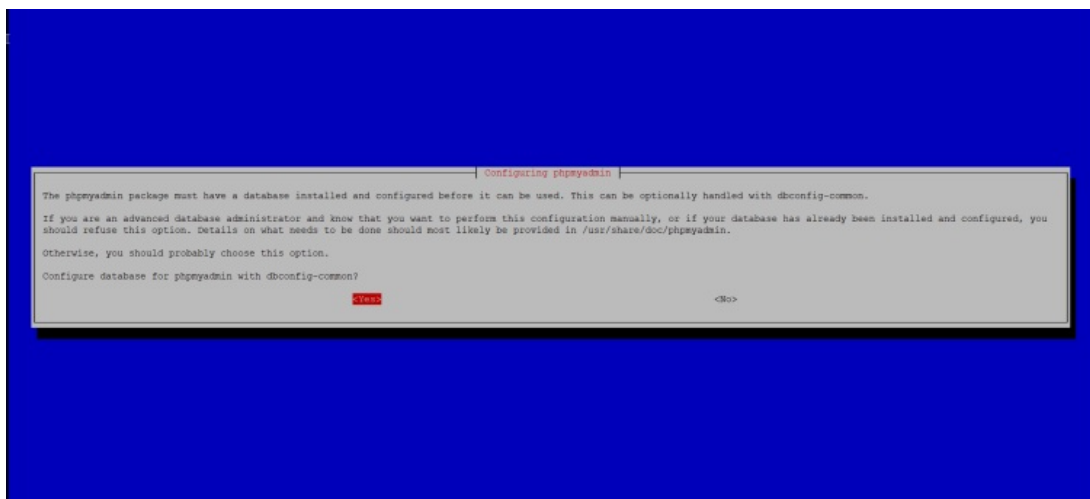
Install phpMyAdmin with apt:

```
apt install phpmyadmin
```

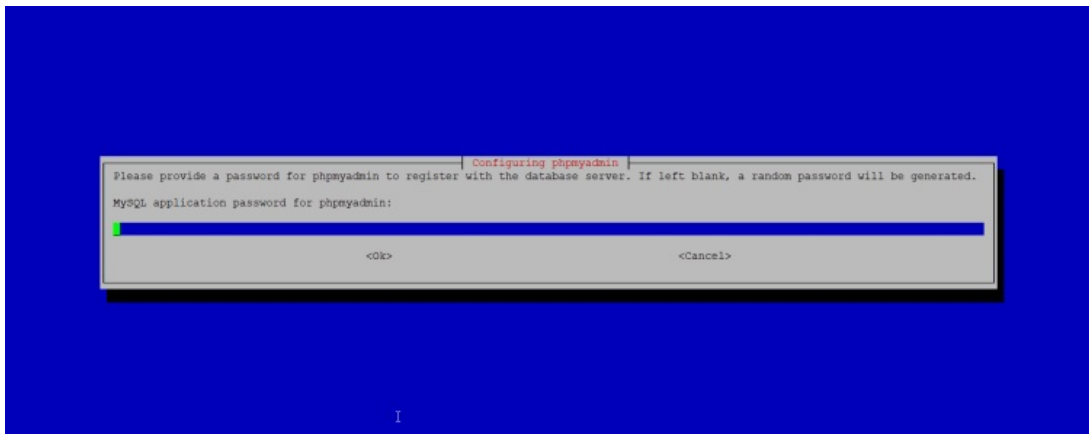
Chose to enable phpMyAdmin in Apache:



Configure PHPMyAdmin using dbconfig common.



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



## 17 Install RoundCube Webmail (optional)

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

Then install RoundCube with this command:

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

The installer will ask the following questions:

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

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

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

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

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

Then reload Apache:

```
systemctl reload apache2
```

Now edit the RoundCube Configuration file:

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

And change the line:

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

to:

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

Now you can access RoundCube as follows:

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

After you have installed `ISPConfig`, see the next chapter.



*What you are about to enter is what is called a Distinguished Name or a DN.*

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----  
Country Name (2 letter code) [AU]: <-- Enter country code  
State or Province Name (full name) [Some-State]: <-- Enter state  
Locality Name (eg, city) []: <-- Enter City  
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter company name  
Organizational Unit Name (eg, section) []: <-- press enter  
Common Name (e.g. server FQDN or YOUR name) []: <-- Enter server hostname  
Email Address []: <-- Enter email address  
[INFO] service Mailman not detected  
Configuring Dovecot  
Creating new DHParams file, this takes several minutes. Do not interrupt the script.  
Generating DH parameters, 2048 bit long safe prime  
[.....]  
[INFO] service Spamassassin not detected  
[INFO] service Amavisd not detected  
Configuring Rspamd  
Configuring Getmail  
Configuring Jailkit  
Configuring Pureftpd  
Configuring BIND  
Configuring Apache  
Configuring vlogger  
[INFO] service OpenVZ not detected  
Configuring AppArmor  
Configuring Ubuntu Firewall  
[INFO] service Metronome XMPP Server not detected  
Configuring Fail2ban  
Installing ISPConfig  
ISPConfig Port [8080]: <-- press enter

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

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

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

Could not issue letsencrypt certificate, falling back to self-signed.  
[....]  
-----

You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----

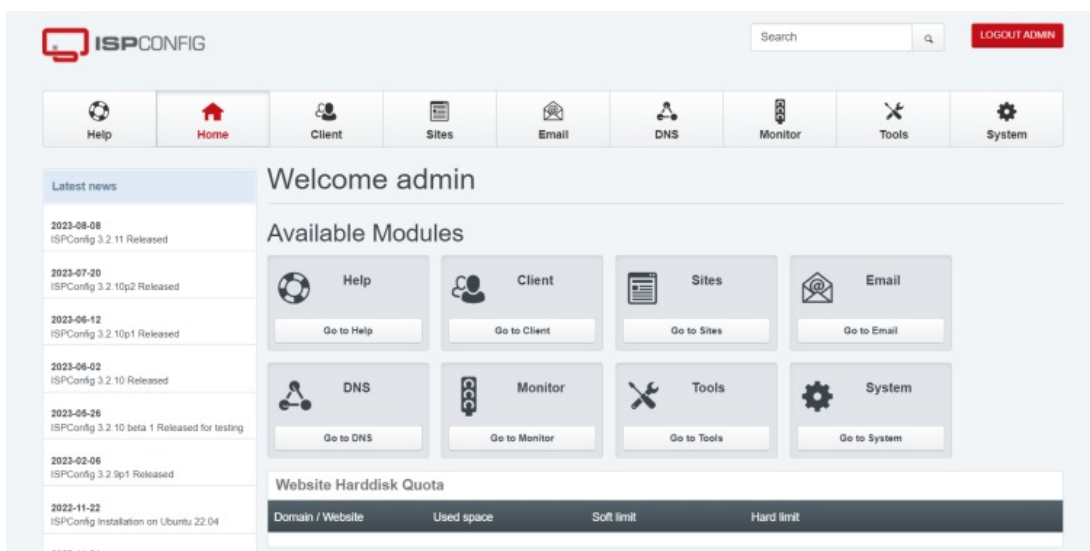
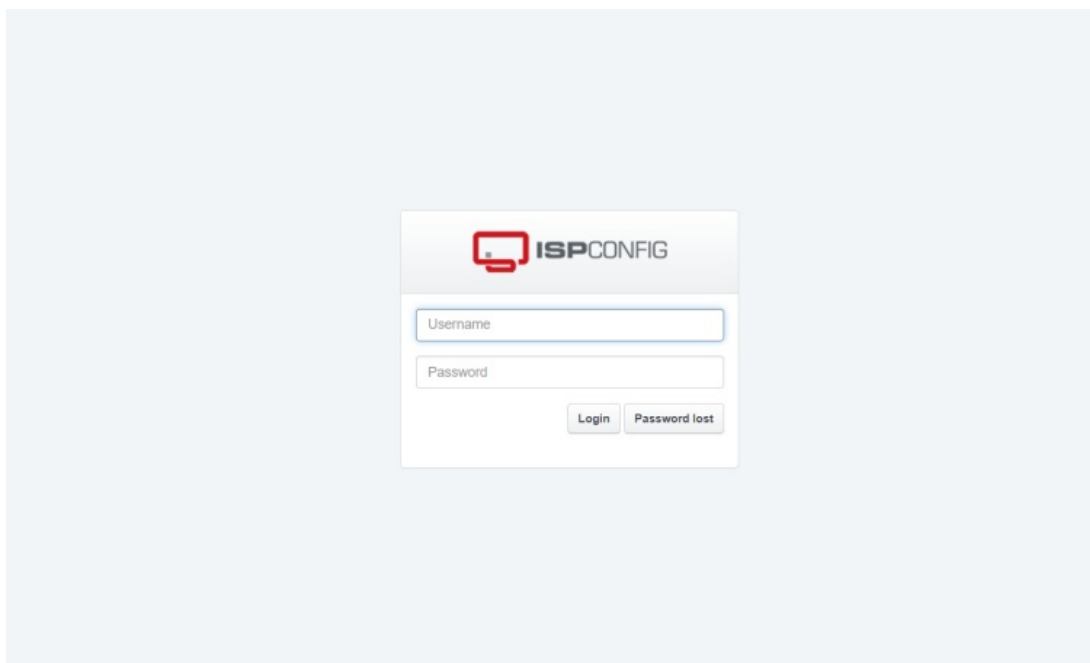
Country Name (2 letter code) [AU]: <-- Enter country code  
State or Province Name (full name) [Some-State]: <-- Enter state  
Locality Name (eg, city) []: <-- Enter City  
Organization Name (eg, company) [Internet Widgits Pty Ltd]: <-- Enter company name  
Organizational Unit Name (eg, section) []: <-- press enter  
Common Name (e.g. server FQDN or YOUR name) []: <-- Enter server hostname  
Email Address []: <-- Enter email address  
SymLink ISPConfig SSL certs to Postfix? (y,n) [y]: <-- press Enter

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

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

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

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



The system is now ready to be used.

## 20 ISPConfig 3 Manual

To learn how to use ISPConfig 3, I strongly recommend downloading [the ISPConfig 3 Manual](#).

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

## 21 Virtual Machine Image Download of this Tutorial

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

### SSH / Shell Login

Username: administrator  
Password: howtoforge

Username: root  
Password: howtoforge

### ISPConfig Login

Username: admin  
Password: howtoforge

### MySQL Login

Username: root  
Password: I7DFg3!cpHfw3bxZj6Fg

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

## 23 Links

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

---

This PDF file is provided by howtoforge.com <https://www.howtoforge.com>. (c) projektfarm GmbH - republishing not permitted.