

The Perfect Linux CentOS Web Server

The Perfect Linux CentOS Web Server – CentOS 6.3 x86_64 (Apache2, Dovecot, ISPConfig 3)

This tutorial shows how to prepare a CentOS 6.3 x86_64 server for the installation of ISPConfig 3, and how to install ISPConfig 3. ISPConfig 3 is a webhosting control panel that allows you to configure the following services through a web browser: Apache web server, Postfix mail server, MySQL, BIND nameserver, PureFTPd, SpamAssassin, ClamAV, Mailman, and many more. Since version 3.0.4, ISPConfig comes with full support for the nginx web server in addition to Apache; this tutorial covers the setup of a server that uses Apache, not nginx.

Please note that this setup does not work for ISPConfig 2! It is valid for ISPConfig 3 only!

I do not issue any guarantee that this will work for you!

ISPConfig 3 Manual

In order to learn how to use ISPConfig 3, I strongly recommend to [download 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 lines out how to make your server more secure and comes with a troubleshooting section at the end.

1 Requirements

To install such a system you will need the following:

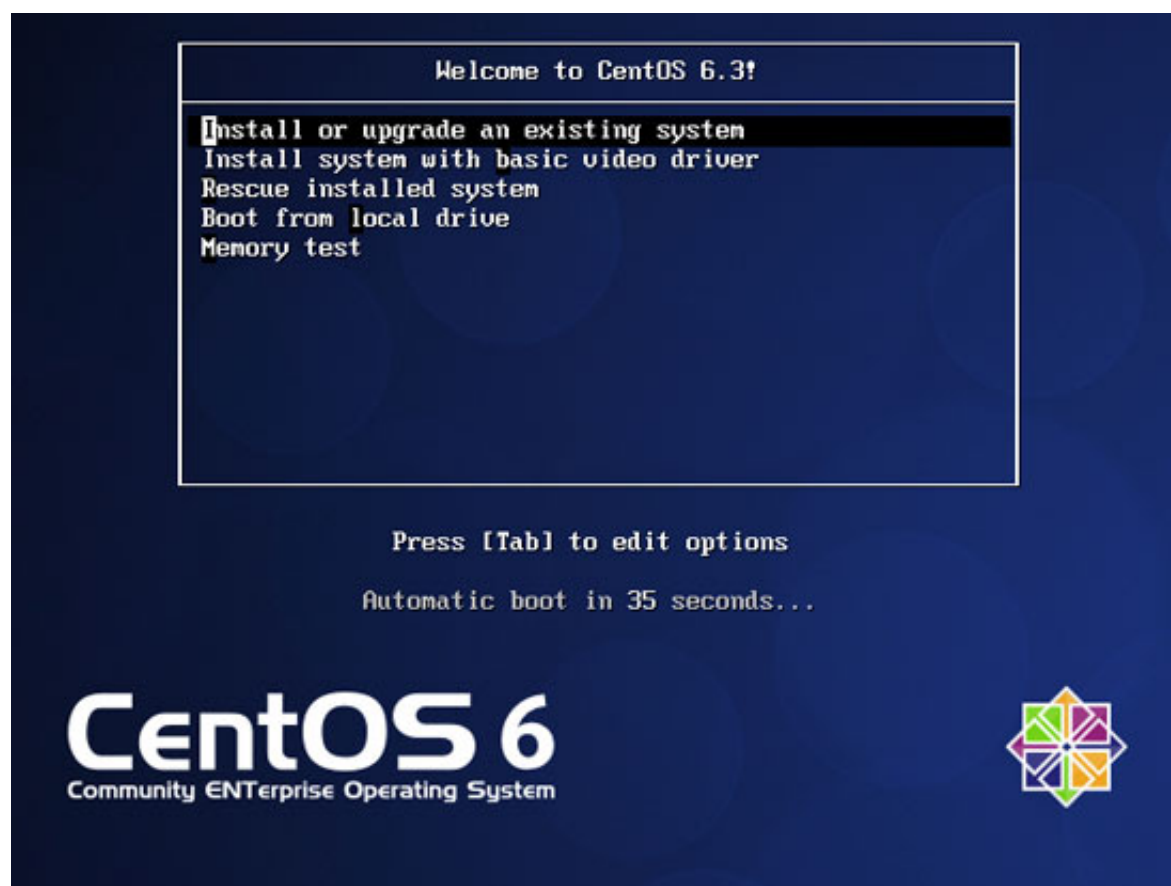
- Download the two CentOS 6.3 DVDs from a mirror next to you (the list of mirrors can be found here: http://isoredirect.centos.org/centos/6/isos/x86_64/).
- a fast Internet connection.

2 Preliminary Note

In this tutorial I 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 Install The Base System

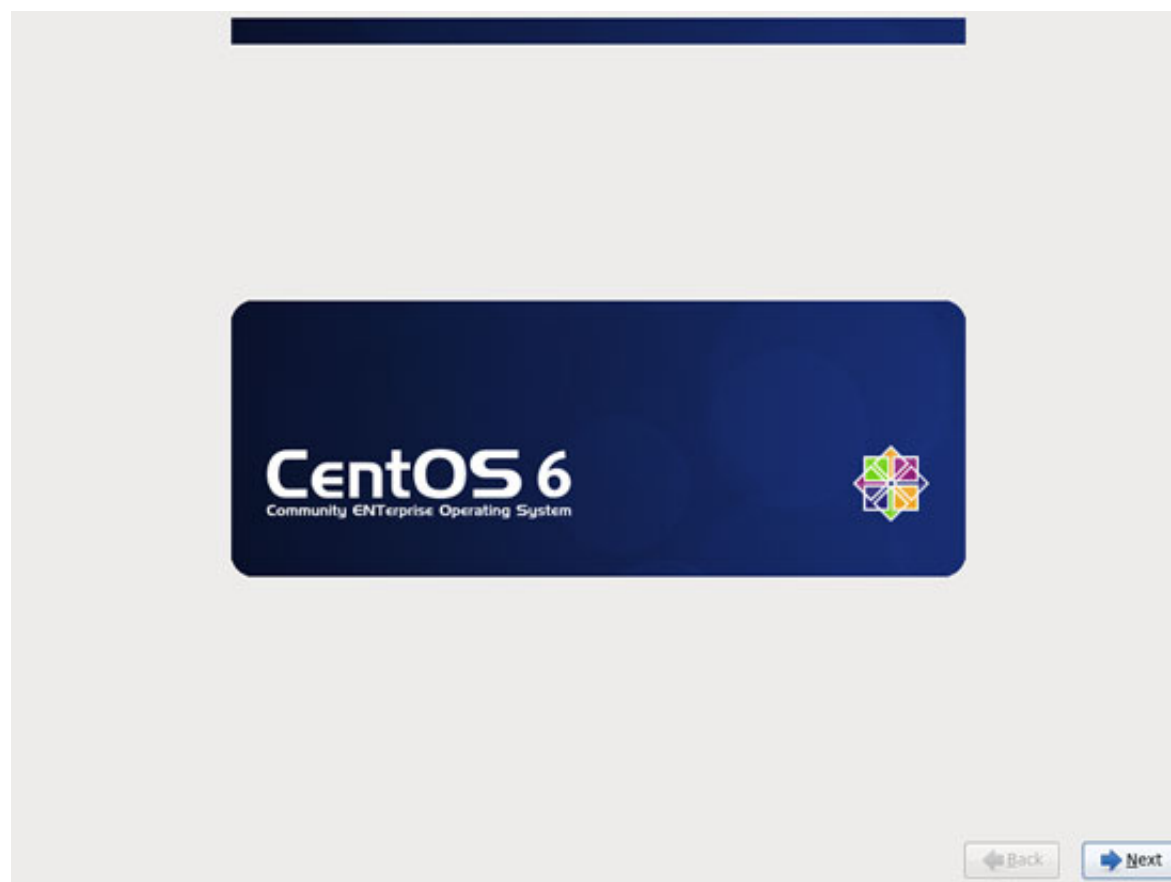
Boot from your first CentOS 6.3 DVD (DVD 1). Select Install or upgrade an existing system:



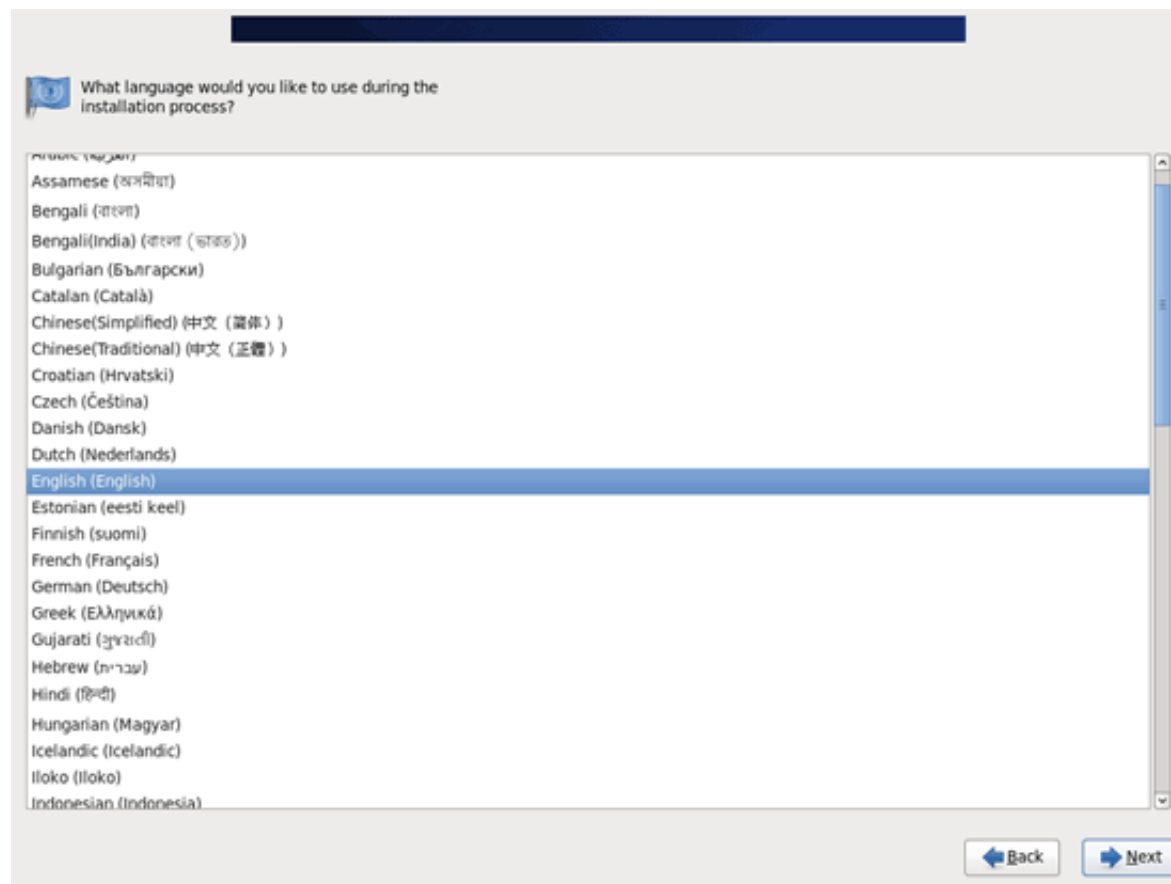
It can take a long time to test the installation media so we skip this test here:



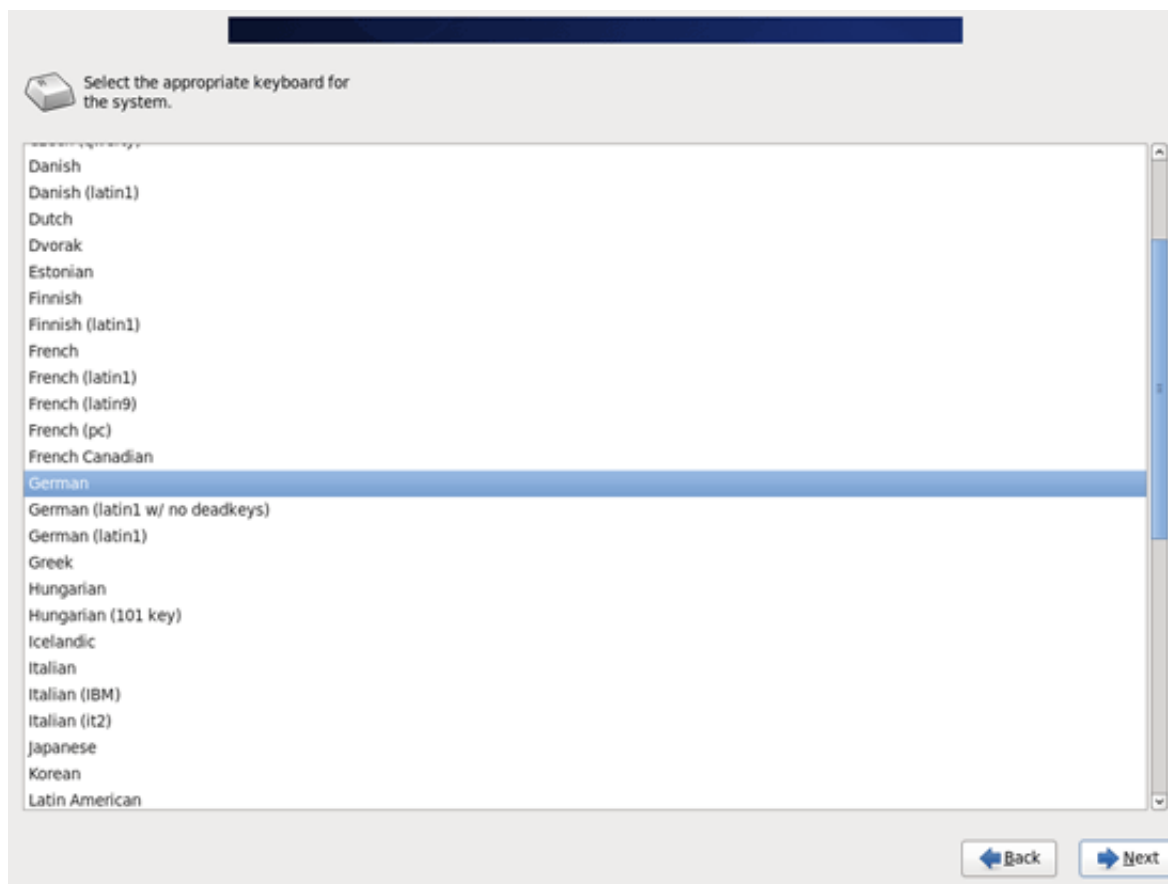
The welcome screen of the CentOS installer appears. Click on Next:



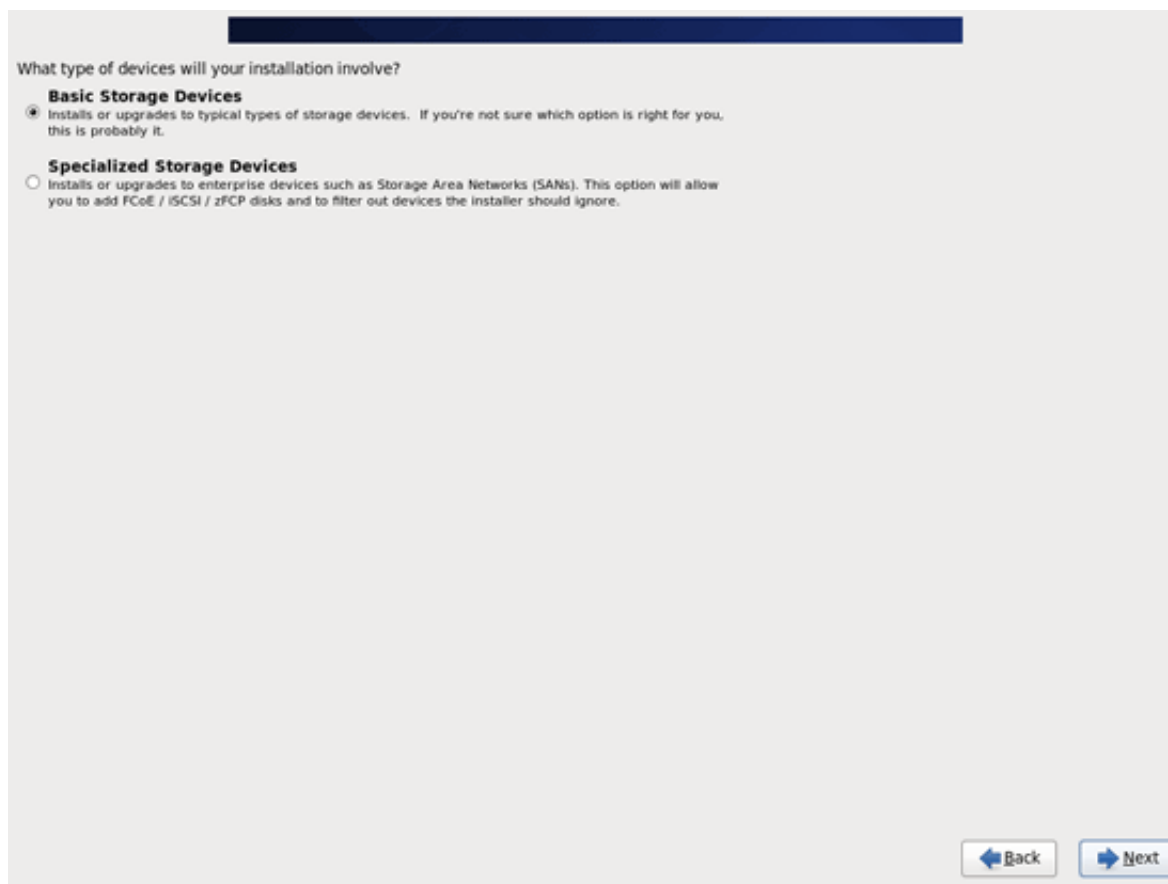
Choose your language next:



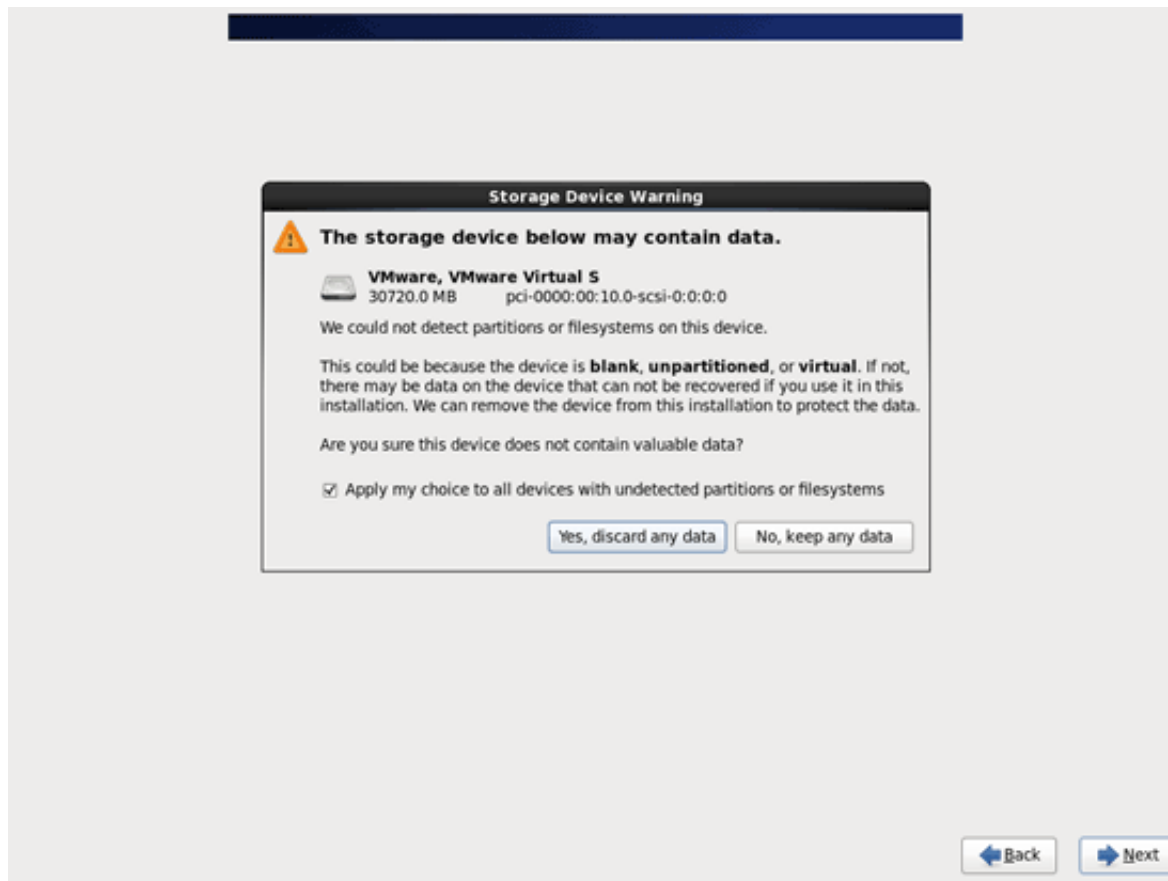
Select your keyboard layout:



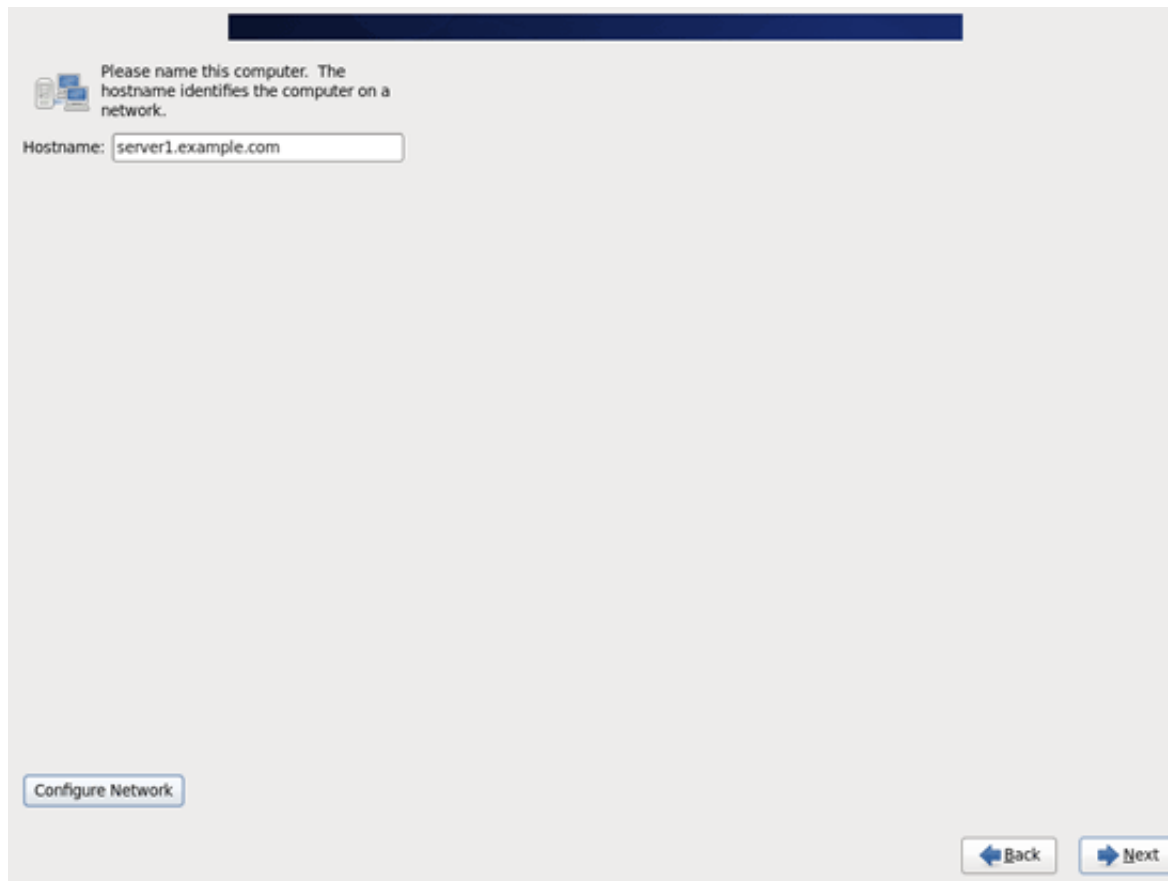
I assume that you use a locally attached hard drive, so you should select Basic Storage Devices here:



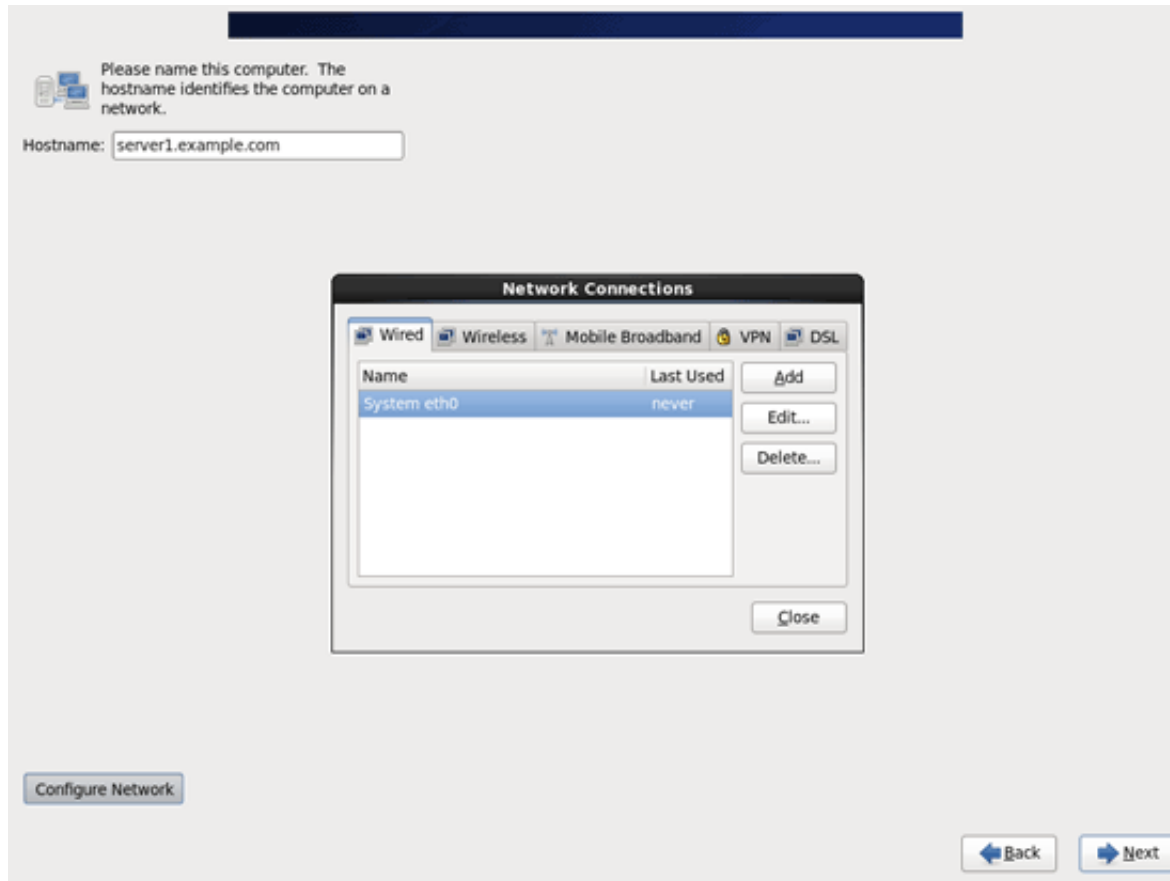
You might see the following warning - Error processing drive. If you see this click on the Re-initialize all button to proceed:



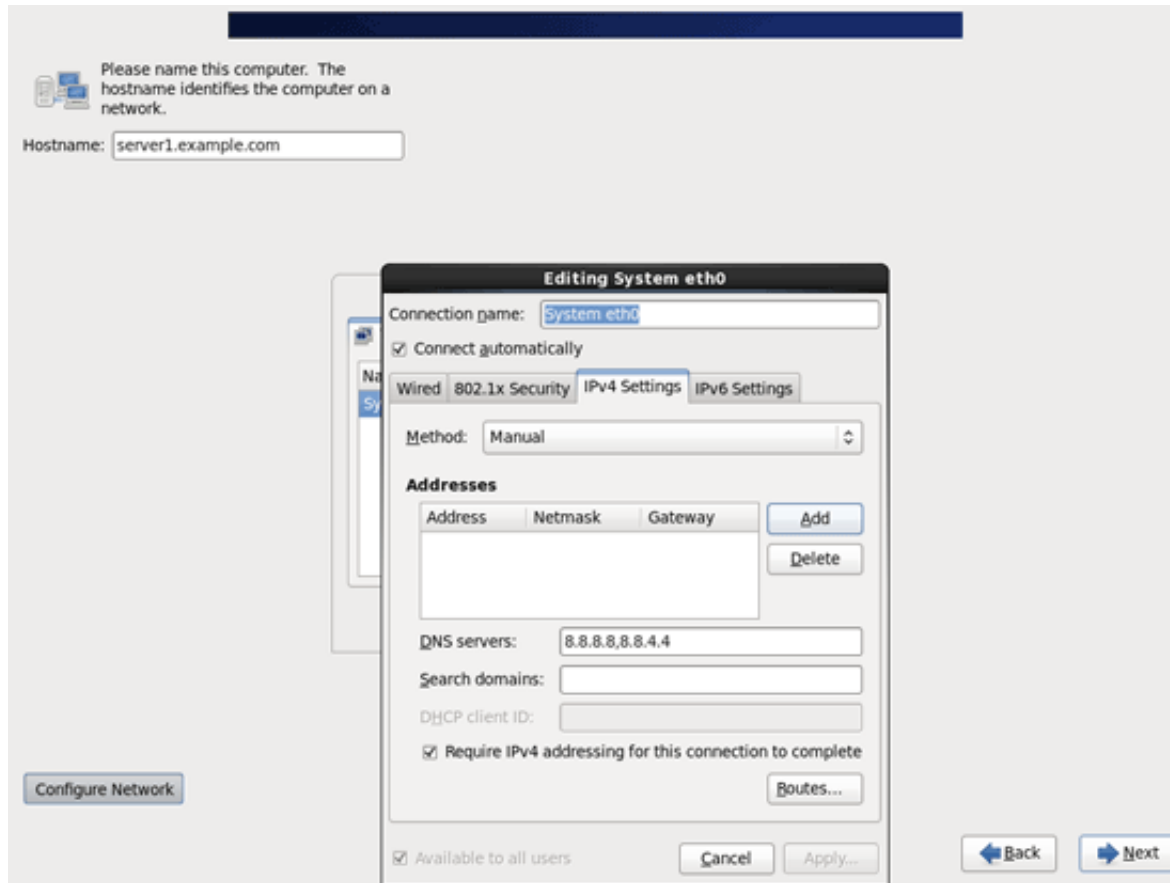
Fill in the hostname of the server (e.g. server1.example.com), then click on the Configure Network button:



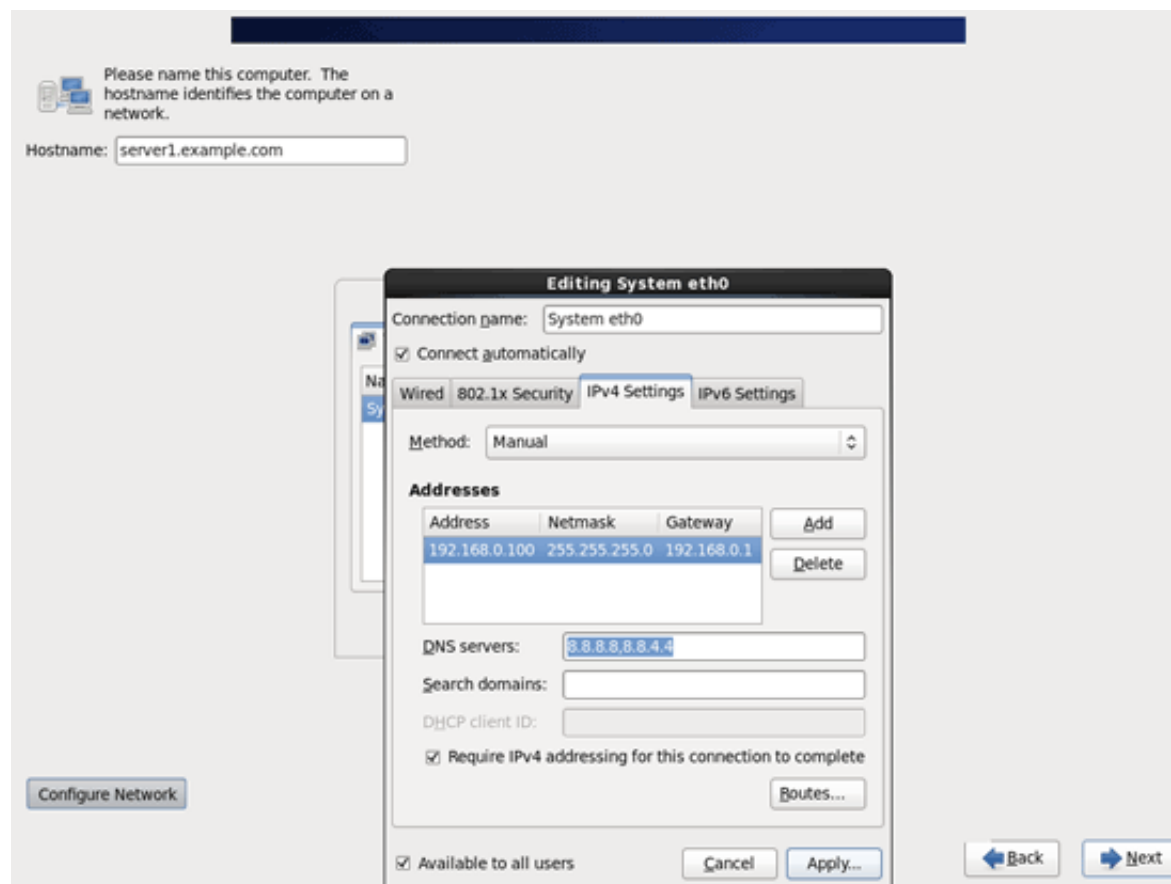
Go to the Wired tab, select the network interface (probably eth0) and click on Edit...:



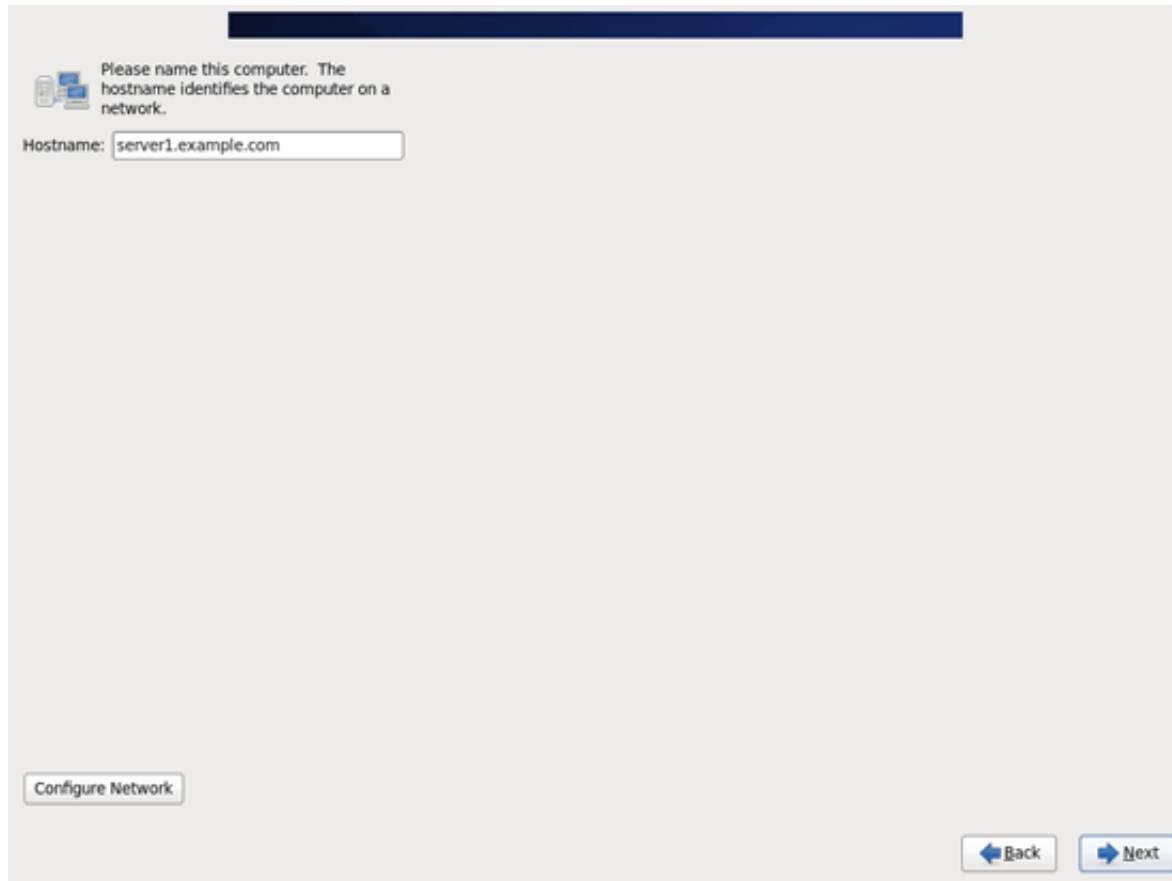
Mark the Connect automatically checkbox and go to the IPv4 Settings tab and select Manual in the Method drop-down menu. Fill in one, two, or three nameservers (separated by comma) in the DNS servers field (e.g. 8.8.8.8,8.8.4.4), then click on the Add button next to the Addresses area:



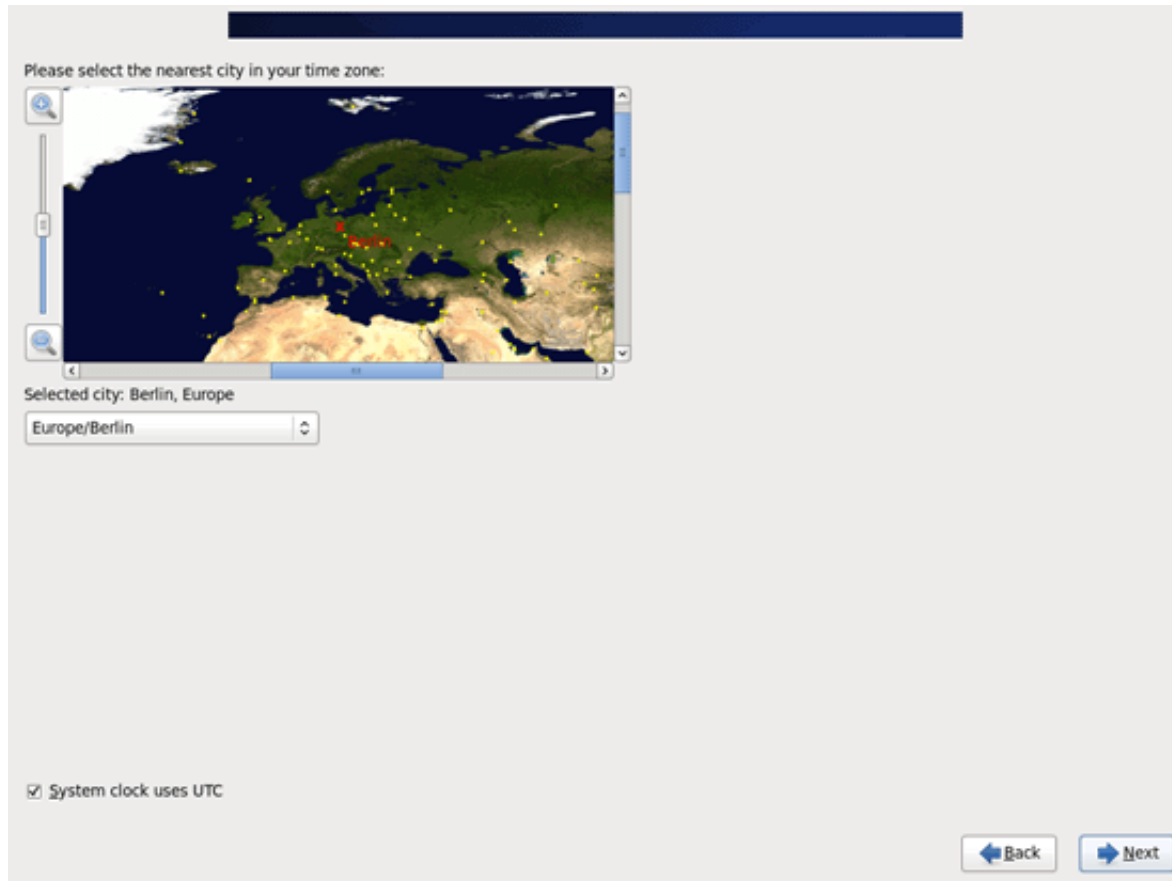
Now give your network card a static IP address and netmask (in this tutorial I'm using the IP address 192.168.0.100 and netmask 255.255.255.0 for demonstration purposes; if you are not sure about the right values, <http://www.subnetmask.info> might help you). Also fill in your gateway (e.g. 192.168.0.1) and click on the Apply... button:



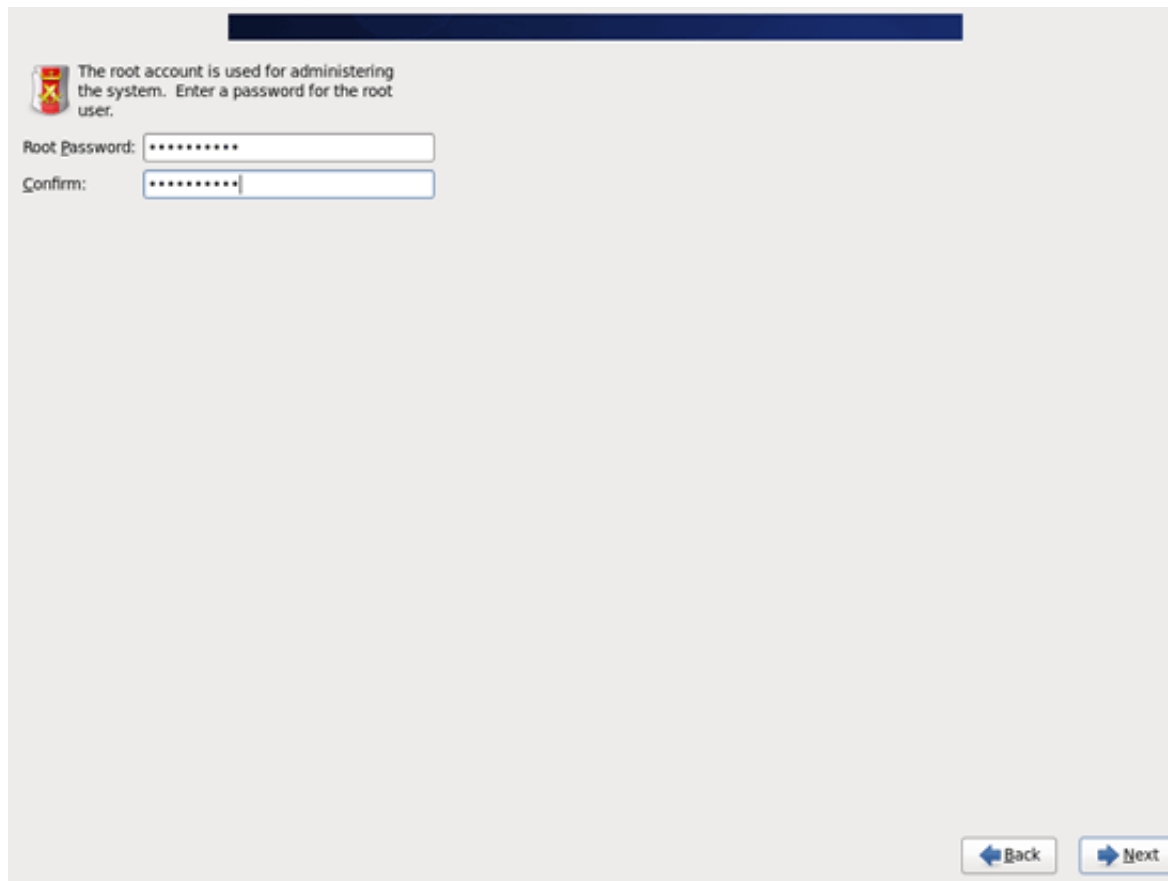
The network configuration is now finished. Click on the Next button:



Choose your time zone:



Give root a password:



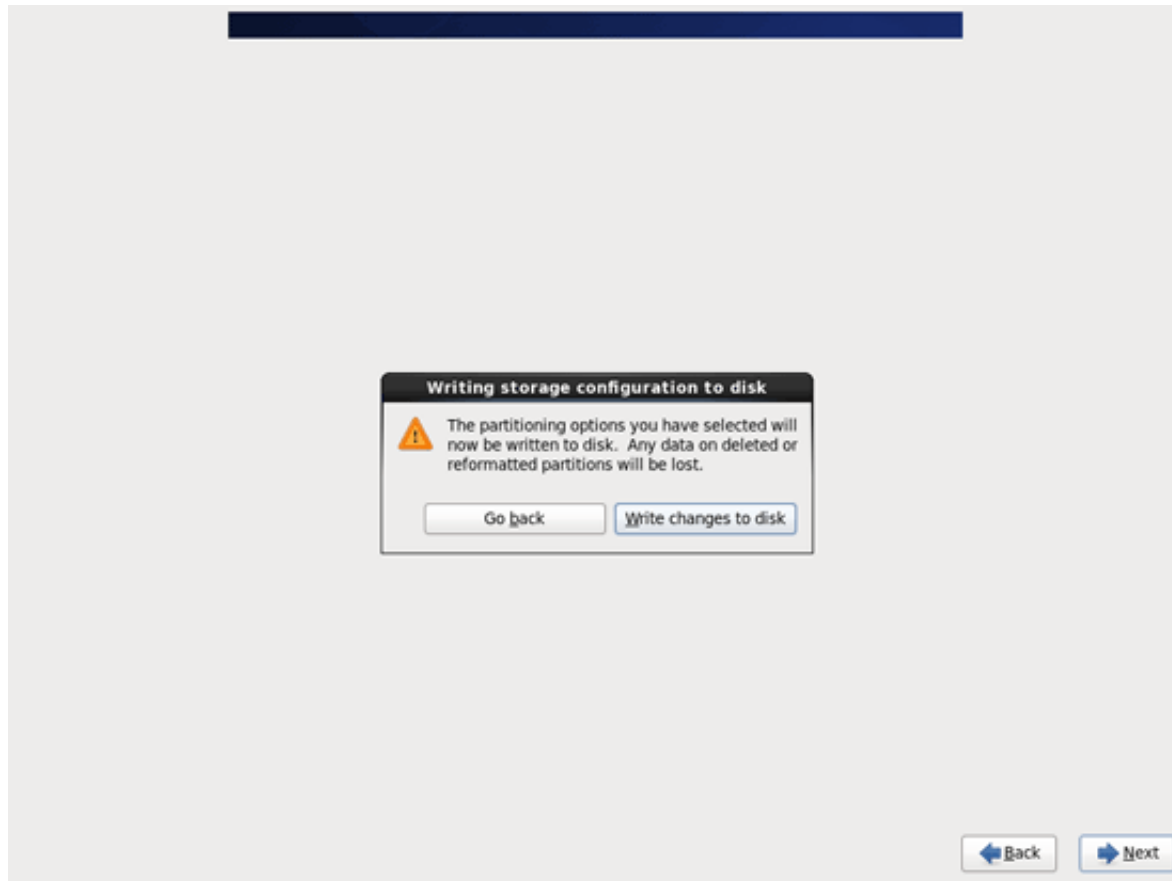
Next we do the partitioning. Select Replace Existing Linux System(s). This will give you a small /boot partition and a large / partition which is fine for our purposes:

Which type of installation would you like?

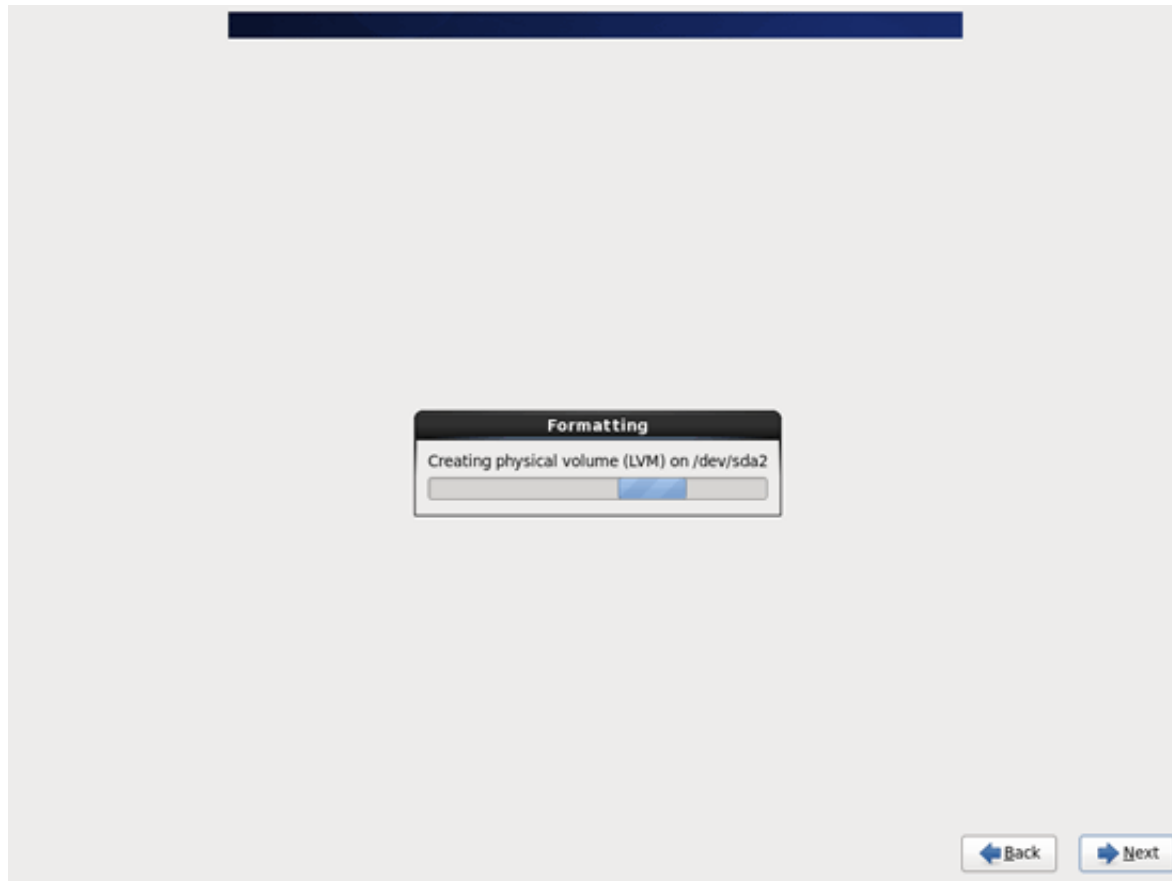
- Use All Space**
Removes all partitions on the selected device(s). This includes partitions created by other operating systems.
Tip: This option will remove data from the selected device(s). Make sure you have backups.
- Replace Existing Linux System(s)**
Removes only Linux partitions (created from a previous Linux installation). This does not remove other partitions you may have on your storage device(s) (such as VFAT or FAT32).
Tip: This option will remove data from the selected device(s). Make sure you have backups.
- Shrink Current System**
Shrinks existing partitions to create free space for the default layout.
- Use Free Space**
Retains your current data and partitions and uses only the unpartitioned space on the selected device(s), assuming you have enough free space available.
- Create Custom Layout**
Manually create your own custom layout on the selected device(s) using our partitioning tool.

Encrypt system
 Review and modify partitioning layout

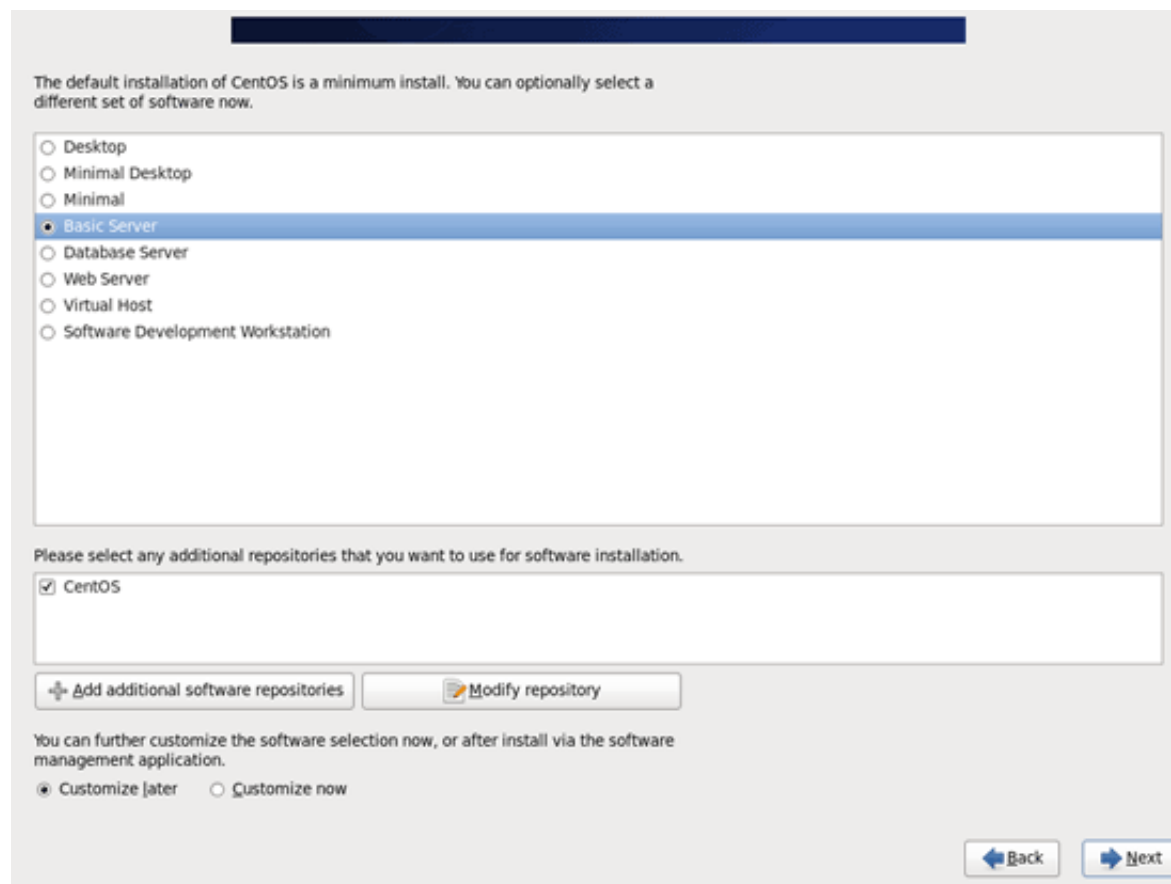
Select Write changes to disk:



The hard drive is being formatted:



Now we select the software we want to install. Select Basic Server, then check CentOS in the additional repositories field, choose Customize later and click on Next:



The default installation of CentOS is a minimum install. You can optionally select a different set of software now.

- Desktop
- Minimal Desktop
- Minimal
- Basic Server
- Database Server
- Web Server
- Virtual Host
- Software Development Workstation

Please select any additional repositories that you want to use for software installation.

- CentOS

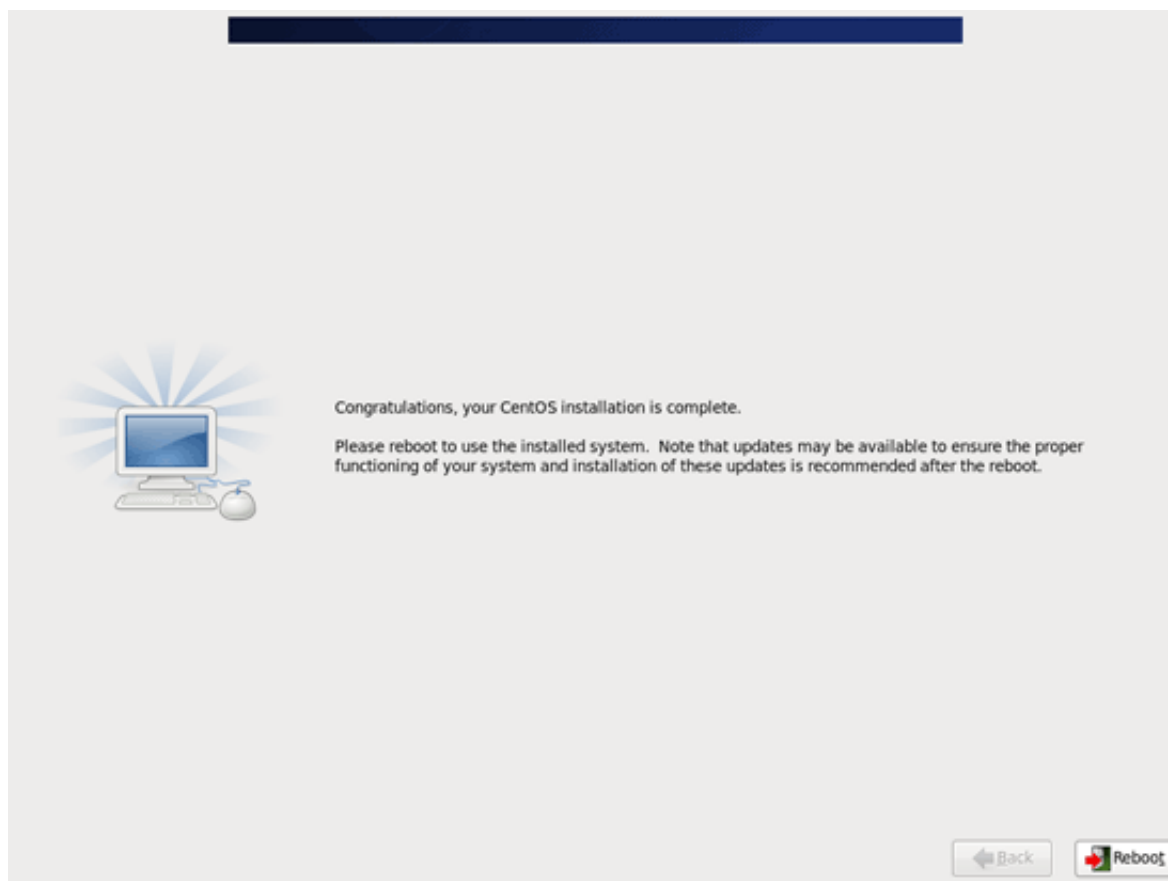
You can further customize the software selection now, or after install via the software management application.

- Customize later
- Customize now

The installation begins. This will take a few minutes:



Finally, the installation is complete, and you can remove your DVD from the computer and reboot it:



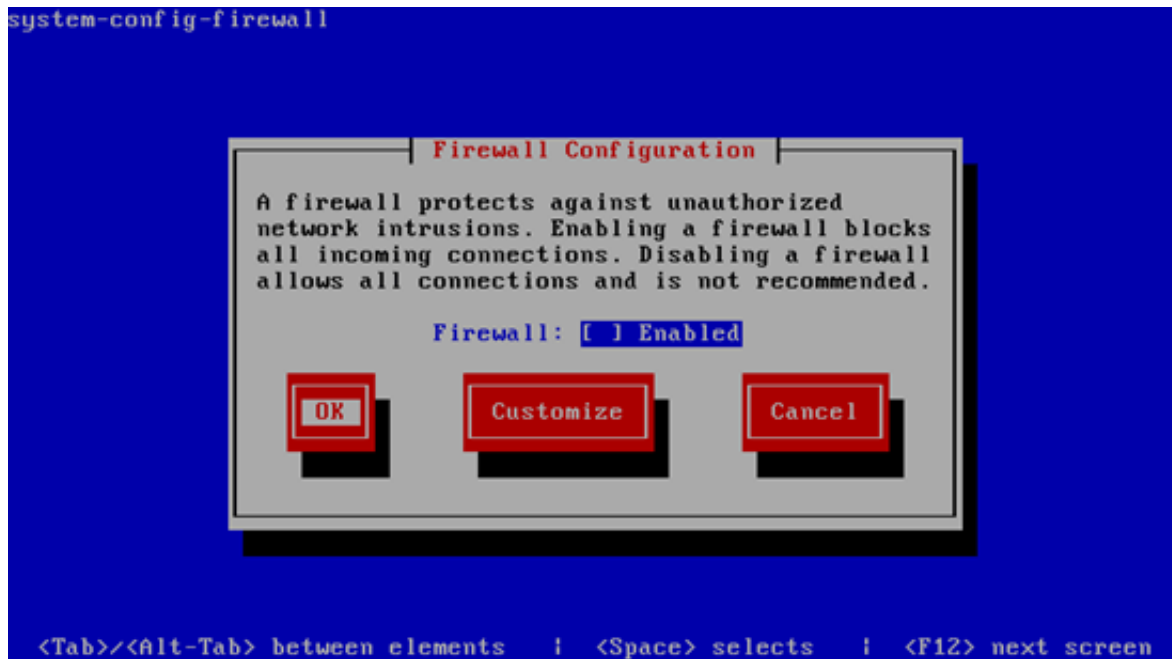
After the reboot, log in as root.

I want to install ISPConfig at the end of this tutorial which comes with its own firewall. That's why I disable the default CentOS firewall now. Of course, you are free to leave it on and configure it to your needs (but then you shouldn't use any other firewall later on as it will most probably interfere with the CentOS firewall).

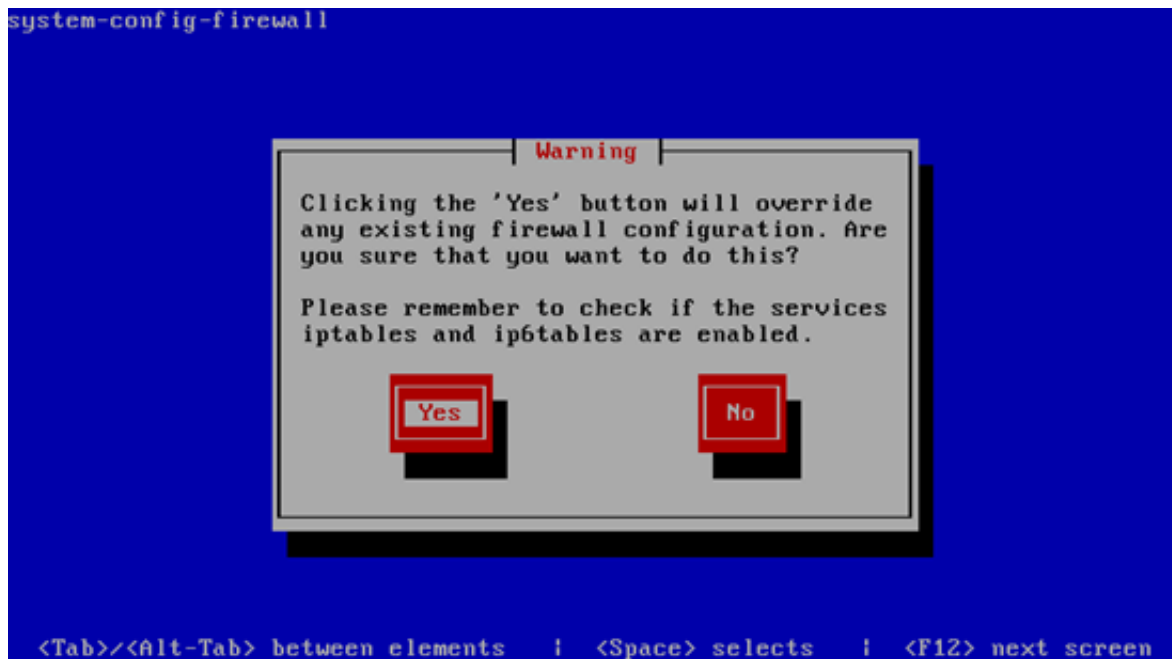
Run...

```
system-config-firewall-tui
```

... and disable the firewall. Hit OK afterwards:



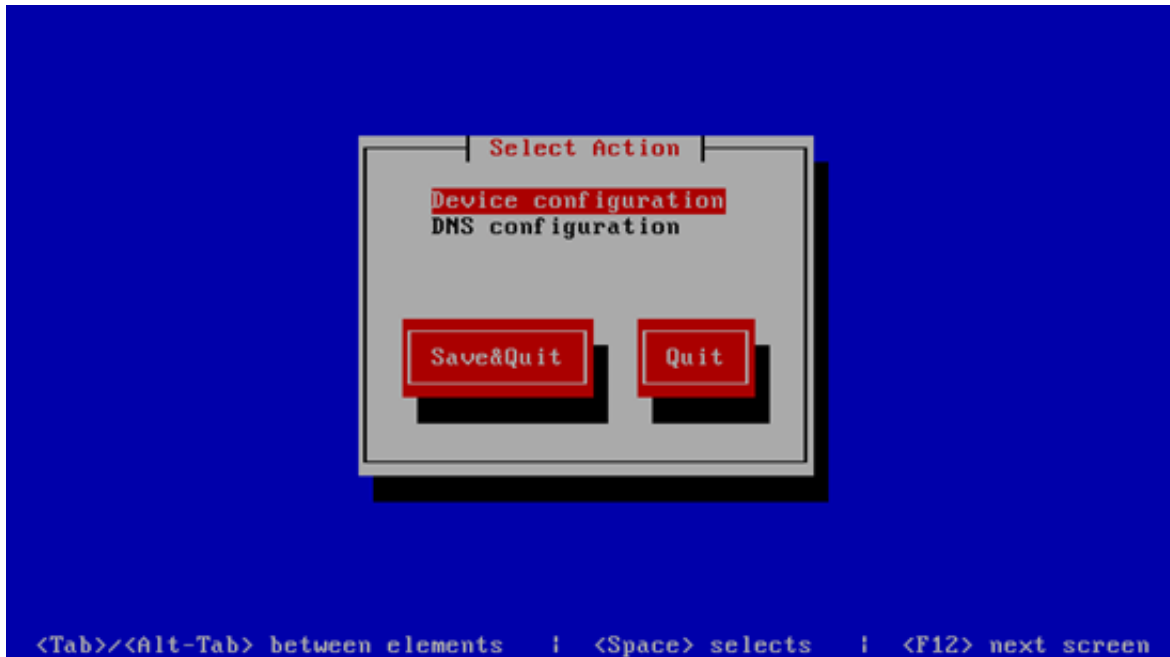
Confirm your choice by selecting Yes:



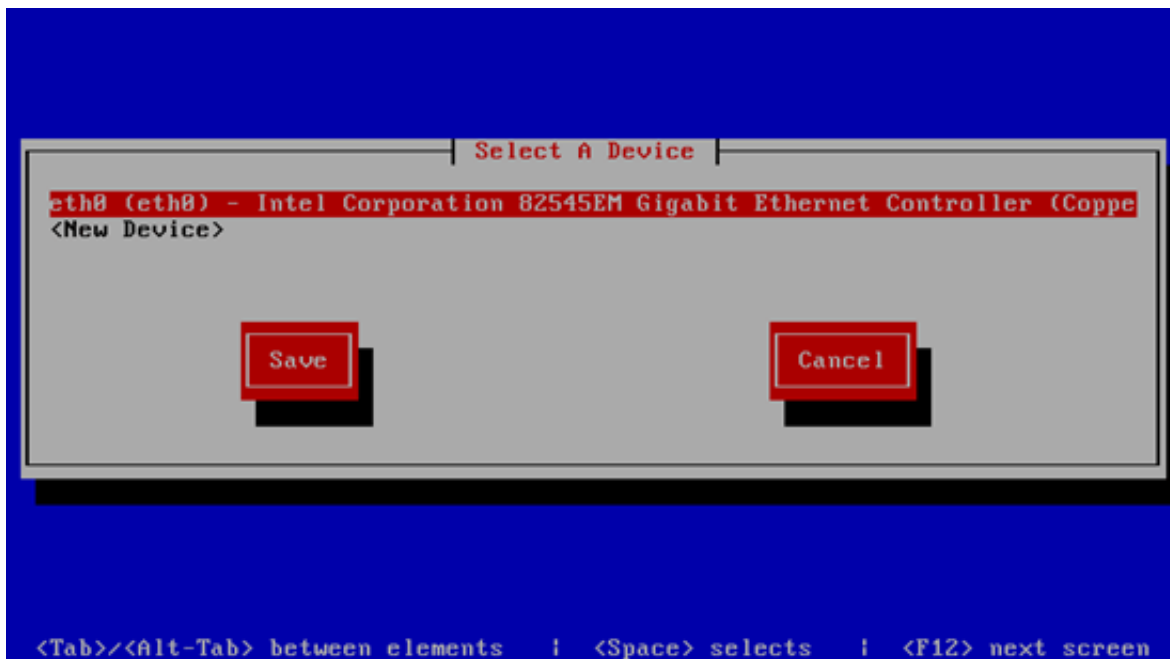
If you did not configure your network card during the installation, you can do that now. Run...

system-config-network

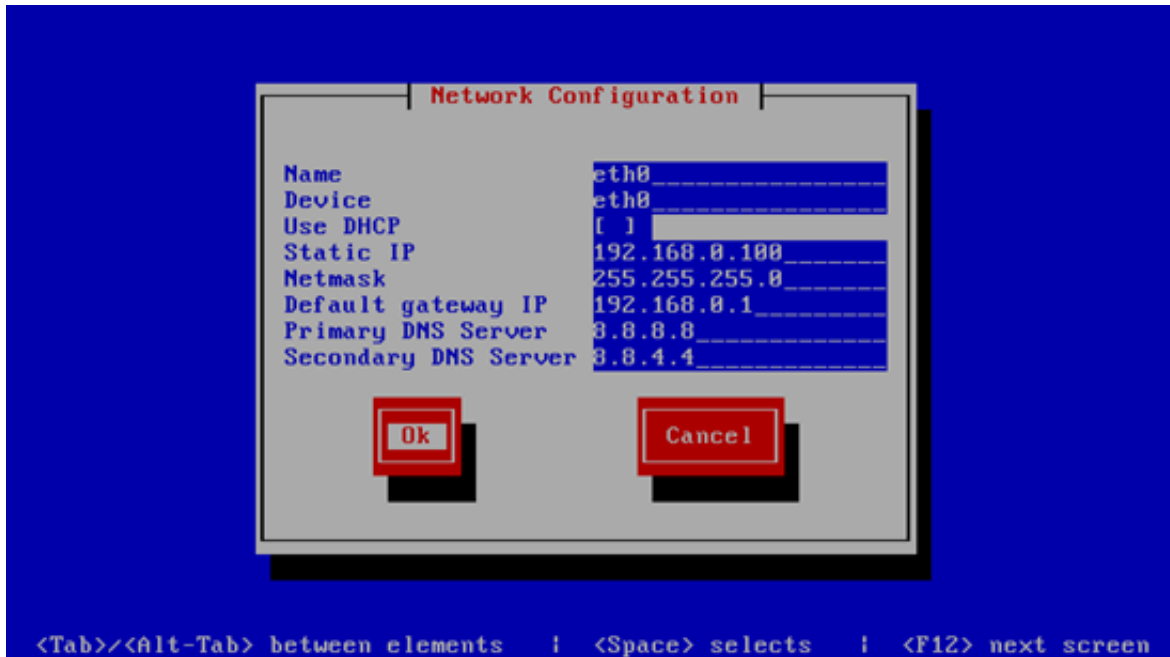
... and go to Device configuration:



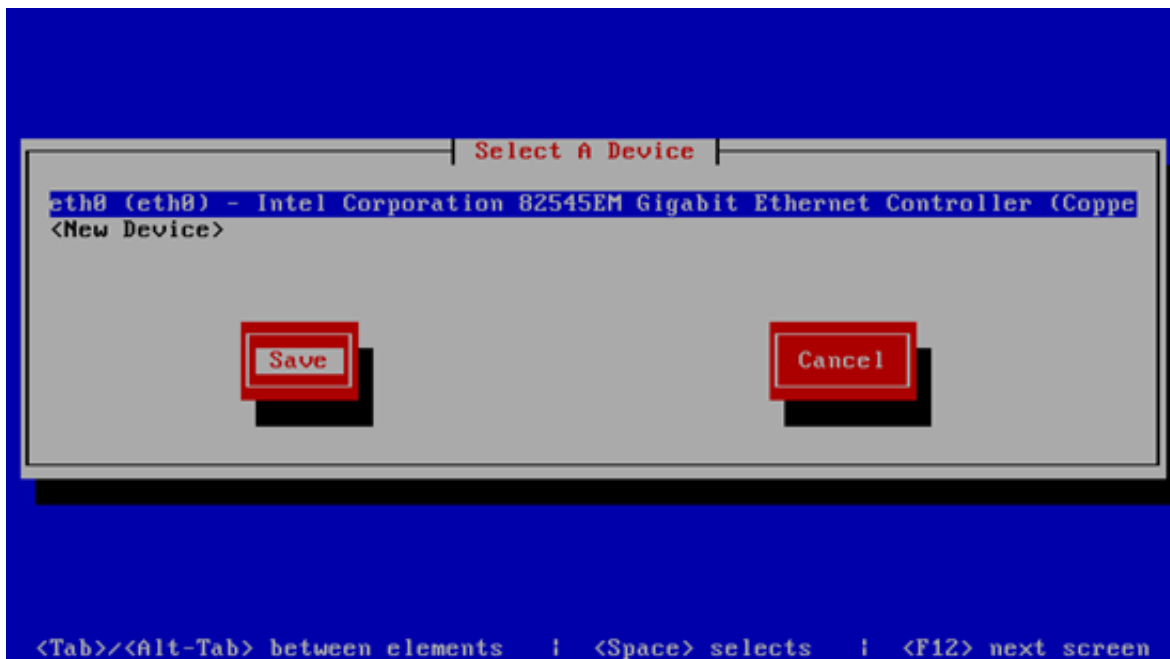
Select your network interface:



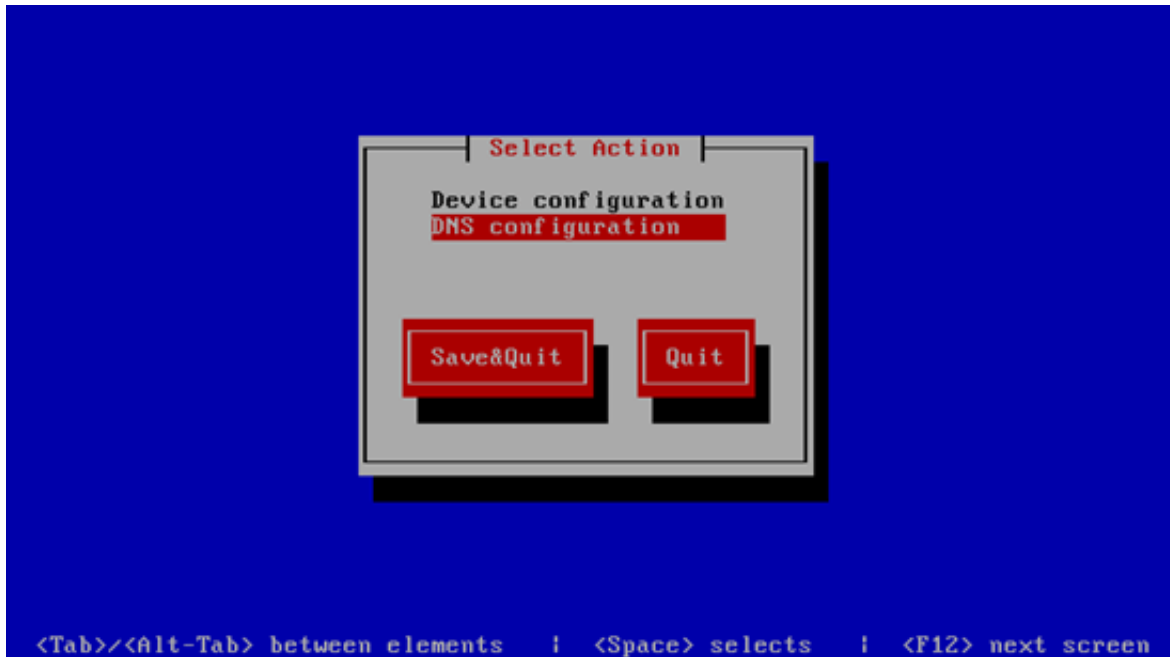
Then fill in your network details - disable DHCP and fill in a static IP address, a netmask, your gateway, and one or two nameservers, then hit Ok:



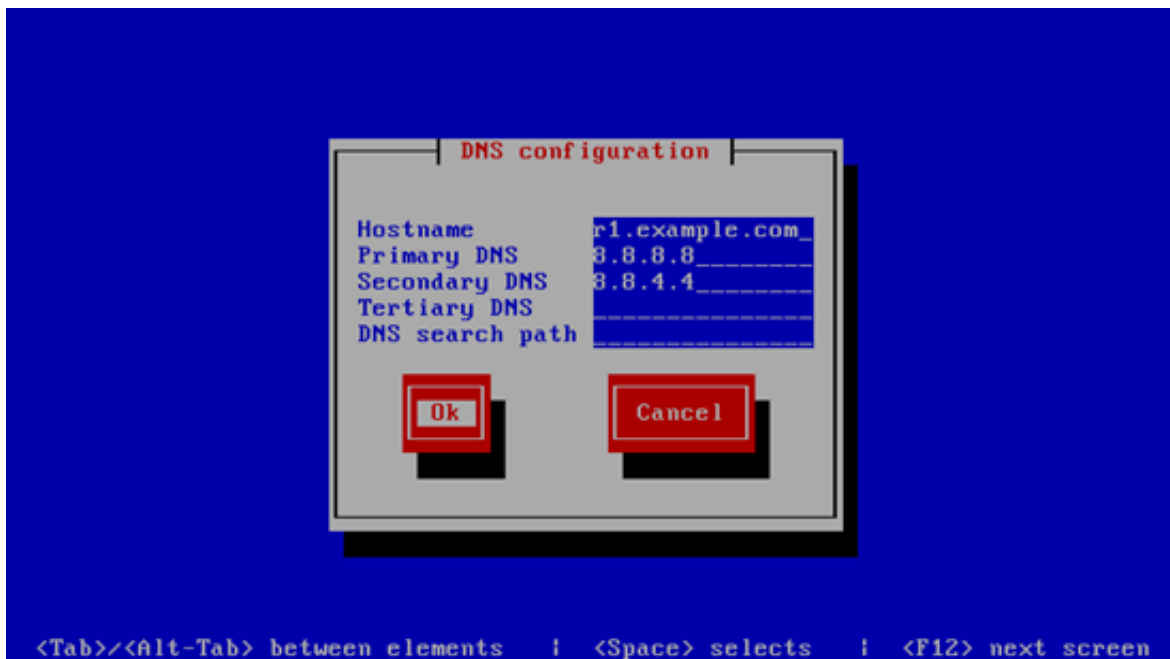
Next select Save:



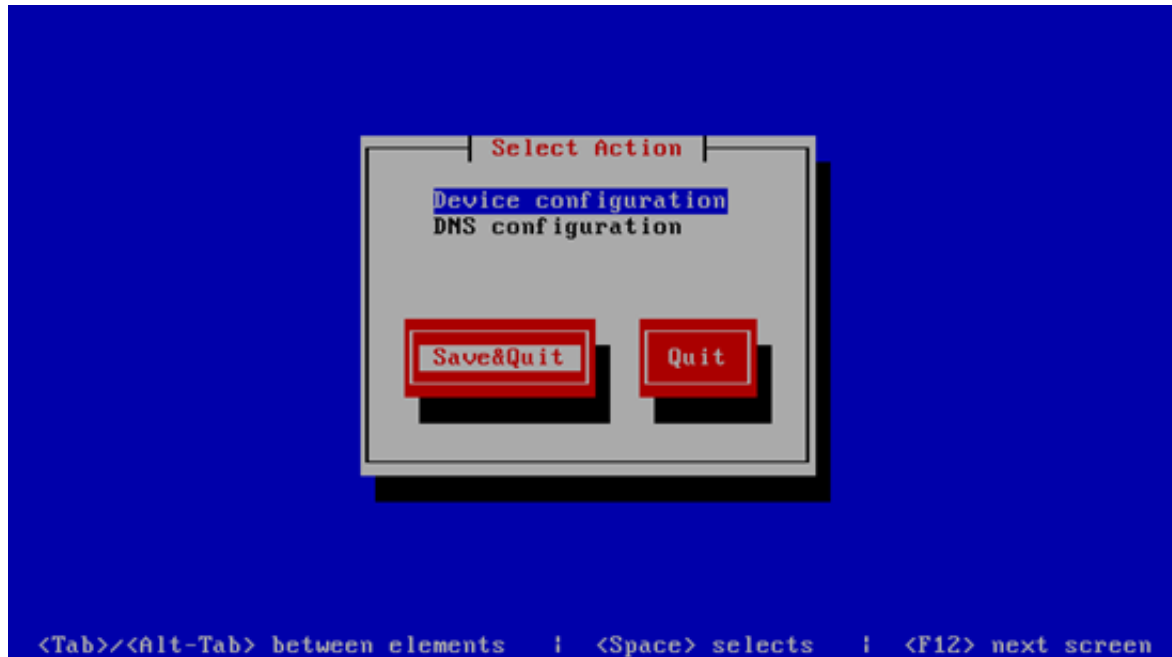
You can also specify additional nameservers. Select DNS configuration:



Now you can fill in additional nameservers and hit Ok:



Hit Save&Quit afterwards:



You should run

```
ifconfig
```

now to check if the installer got your IP address right:

```
[root@server1 ~]# ifconfig
eth0  Link encap:Ethernet  HWaddr 00:0C:29:00:85:AC
inet addr:192.168.0.100 Bcast:192.168.0.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe00:85ac/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:278 errors:0 dropped:0 overruns:0 frame:0
TX packets:86 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:28503 (27.8 KiB) TX bytes:16360 (15.9 KiB)
```

```
lo    Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING  MTU:16436  Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
```

```
[root@server1 ~]#
```

Check your `/etc/resolv.conf` if it lists all nameservers that you've previously configured:

```
cat /etc/resolv.conf
```

If nameservers are missing, run

```
system-config-network
```

and add the missing nameservers again.

Now, on to the configuration...

4 Adjust `/etc/hosts`

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

```
vi /etc/hosts
```

```
127.0.0.1    localhost localhost.localdomain localhost4 localhost
t4.localdomain4 192.168.0.100  server1.example.com  server
1      ::1      localhost localhost.localdomain localhost6 loc
alhost6.localdomain6
```

5 Configure The Firewall

(You can skip this chapter if you have already disabled the firewall at the end of the basic system installation.)

I want to install ISPCConfig at the end of this tutorial which comes with its own firewall. That's why I disable the default CentOS firewall now. Of course, you are free to leave it on and configure it to your needs (but then you shouldn't use any other firewall later on as it will most probably interfere with the CentOS firewall).

Run

```
system-config-firewall
```

and disable the firewall.

To check that the firewall has really been disabled, you can run

```
iptables -L
```

afterwards. The output should look like this:

```
[root@server1 ~]# iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source          destination

Chain FORWARD (policy ACCEPT)
target    prot opt source          destination

Chain OUTPUT (policy ACCEPT)
target    prot opt source          destination
[root@server1 ~]#
```

6 Disable SELinux

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

Edit /etc/selinux/config and set SELINUX=disabled:

```
vi /etc/selinux/config
```

```
# This file controls the state of SELinux on the system. # SEL
INUX= can take one of these three values: #      enforcing - SE
Linux security policy is enforced. #      permissive - SELinux
prints warnings instead of enforcing. #      disabled - No SELi
nux policy is loaded. SELINUX=disabled # SELINUXTYPE= can tak
e one of these two values: #      targeted - Targeted processes
are protected, #      mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Afterwards we must reboot the system:

```
reboot
```

7 Enable Additional Repositories And Install Some Software

First we import the GPG keys for software packages:

```
rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY*
```

Then we enable the RPMforge and EPEL repositories on our CentOS system as lots of the packages that we are going to install in the course of this tutorial are not available in the official CentOS 6.3 repositories:

```
rpm --import http://dag.wieers.com/rpm/packages/RPM-GPG-KEY.dag.txt
```

```
cd /tmp
```

```
wget http://pkgs.repoforge.org/rpmforge-release/rpmforge-release-0.5.2-2.el6.rf.x86_64.rpm
```

```
rpm -ivh rpmforge-release-0.5.2-2.el6.rf.x86_64.rpm
```

(If the above link doesn't work anymore, you can find the current version of rpmforge-release here: <http://packages.sw.be/rpmforge-release/>)

```
rpm --import https://fedoraproject.org/static/0608B895.txt
```

```
wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-7.noarch.rpm
```

```
rpm -ivh epel-release-6-7.noarch.rpm
```

```
yum install yum-priorities
```

```
Edit /etc/yum.repos.d/epel.repo...
```

```
vi /etc/yum.repos.d/epel.repo
```

... and add the line `priority=10` to the `[epel]` section:

```
[epel] name=Extra Packages for Enterprise Linux 6 - $basearch
#baseurl=http://download.fedoraproject.org/pub/epel/6/$basearc
h mirrorlist=https://mirrors.fedoraproject.org/metalink?repo=e
pel-6&arch=$basearch failovermethod=priority enabled=1 prior
ity=10 gpgcheck=1 gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-
EPEL-6 [...]
```

Then we update our existing packages on the system:

```
yum update
```

Now we install some software packages that are needed later on:

```
yum groupinstall 'Development Tools'
```

8 Quota

(If you have chosen a different partitioning scheme than I did, you must adjust this chapter so that quota applies to the partitions where you need it.)

To install quota, we run this command:

```
yum install quota
```

Edit `/etc/fstab` and add `,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0` to the / partition (`/dev/mapper/vg_server1-lv_root`):

```
vi /etc/fstab
```

```
# # /etc/fstab # Created by anaconda on Wed Jul 11 17:52:57 2
012 # # Accessible filesystems, by reference, are maintained
under '/dev/disk' # See man pages fstab(5), findfs(8), mount(8
) and/or blkid(8) for more info # /dev/mapper/vg_server1-lv_r
oot /                               ext4      defaults,usrjquota=aquota.u
ser,grpjquota=aquota.group,jqfmt=vfsv0      1 1  UID=806910a
1-dbdf-4746-bd94-cbe73ce81493 /boot          ext4      d
efaults          1 2  /dev/mapper/vg_server1-lv_swap swap
swap          defaults          0 0  tmpfs
/dev/shm          tmpfs          defaults          0 0  devpts
/dev/pts          devpts          gid=5,mode=620
0 0  sysfs          /sys          sysfs      d
efaults          0 0  proc          /proc
proc          defaults          0 0
```

Then run

```
mount -o remount /
```

```
quotacheck -avugm
```

```
quotaon -avug
```

to enable quota.

9 Install Apache, MySQL, phpMyAdmin

We can install the needed packages with one single command:

```
yum install ntp httpd mod_ssl mysql-server php php-mysql php-mbstring phpmyadmin
```

10 Install Dovecot

Dovecot can be installed as follows:

```
yum install dovecot dovecot-mysql
```

Now create the system startup links and start Dovecot:

```
chkconfig --levels 235 dovecot on
```

```
/etc/init.d/dovecot start
```

11 Install Postfix

Postfix can be installed as follows:

```
yum install postfix
```

Then turn off Sendmail and start Postfix and MySQL:

```
chkconfig --levels 235 mysqld on
```

```
/etc/init.d/mysqld start
```

```
chkconfig --levels 235 sendmail off
```

```
chkconfig --levels 235 postfix on
```

```
/etc/init.d/sendmail stop
```

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

12 Install Getmail

Getmail can be installed as follows:

```
yum install getmail
```

13 Set MySQL Passwords And Configure phpMyAdmin

Set passwords for the MySQL root account:

```
mysql_secure_installation
```

```
[root@server1 tmp]# mysql_secure_installation
```

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MySQL to secure it, we'll need the current password for the root user. If you've just installed MySQL, and you haven't set the root password yet, the password will be blank, so you should just press enter here.

Enter current password for root (enter for none):

OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MySQL root user without the proper authorisation.

Set root password? [Y/n] /etc/named.conf

```
vi /etc/named.conf
```

```
// // named.conf // // Provided by Red Hat bind package to c
onfigure the ISC BIND named(8) DNS // server as a caching only
nameserver (as a localhost DNS resolver only). // // See /us
r/share/doc/bind*/sample/ for example named configuration files
. // options {          listen-on port 53 { any; };
listen-on-v6 port 53 { any; };          directory          "/var/n
amed";          dump-file          "/var/named/data/cache_dump.db"
```

```
;       statistics-file "/var/named/data/named_stats.txt";
       memstatistics-file "/var/named/data/named_mem_stats.txt"
";       allow-query      { any; };           recursion yes;
}; logging {           channel default_debug {
file "data/named.run";           severity dynamic;
}; }; zone "." IN {           type hint;           file "n
amed.ca"; }; include "/etc/named.conf.local";
```

Create the file `/etc/named.conf.local` that is included at the end of `/etc/named.conf` (`/etc/named.conf.local` will later on get populated by ISPConfig if you create DNS zones in ISPConfig):

```
touch /etc/named.conf.local
```

Then we create the startup links and start BIND:

```
chkconfig --levels 235 named on
/etc/init.d/named start
```

18 Install Vlogger, Webalizer, And AWStats

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

```
yum install webalizer awstats perl-DateTime-Format-HTTP perl-DateTime-Format-Builder
```

```
cd /tmp
wget http://n0rp.chemlab.org/vlogger/vlogger-1.3.tar.gz
tar xvfz vlogger-1.3.tar.gz
mv vlogger-1.3/vlogger /usr/sbin/
rm -rf vlogger*
```

19 Install Jailkit

Jailkit is needed only if you want to chroot SSH users. It can be installed as follows (important: Jailkit must be installed before ISPConfig - it cannot be installed afterwards!):

```
cd /tmp
wget http://olivier.sessink.nl/jailkit/jailkit-2.15.tar.gz
tar xvfz jailkit-2.15.tar.gz
cd jailkit-2.15
./configure
```



```
make
make install
cd ..
rm -rf jailkit-2.15*
```

20 Install fail2ban

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

```
yum install fail2ban
```

We must configure fail2ban to log to the log file `/var/log/fail2ban.log` because this is the log file that is monitored by the ISPConfig Monitor module. Open `/etc/fail2ban/fail2ban.conf...`

```
vi /etc/fail2ban/fail2ban.conf
```

... and comment out the `logtarget = SYSLOG` line and add `logtarget = /var/log/fail2ban.log`:

```
[...] # Option: logtarget # Notes.: Set the log target. This
s could be a file, SYSLOG, STDERR or STDOUT. #           Only o
ne log target can be specified. # Values:  STDOUT STDERR SYSLO
G file Default:  /var/log/fail2ban.log # #logtarget = SYSLOG
          logtarget = /var/log/fail2ban.log [...]
```

Then create the system startup links for fail2ban and start it:

```
chkconfig --levels 235 fail2ban on
/etc/init.d/fail2ban start
```

21 Install rkhunter

rkhunter can be installed as follows:

```
yum install rkhunter
```

22 Install Mailman

Since version 3.0.4, ISPConfig also allows you to manage (create/modify/delete) Mailman mailing lists. If you want to make use of this feature, install Mailman as follows:

```
yum install mailman
```

Before we can start Mailman, a first mailing list called mailman must be created:

```
/usr/lib/mailman/bin/newlist mailman
```

```
[root@server1 tmp]# /usr/lib/mailman/bin/newlist mailman
```

Enter the email of the person running the list: