NPROBE NETFLOW

Document version:	1.0
Date:	30 November 2011
Author:	Matt Stanyon-Tall
Summary:	nProbe NetFlow
Version Changes:	Initial document

TABLE OF CONTENTS

1. SWITCH CONFIGURATION

In order to keep the flows independent, a separate switchport has been configured to correspond with each WAN interface, and two different monitoring sessions.

These ports will be dedicated to this task.

Assuming the primary CPE is connected to gi1/0/1, and the SPAN port gi1/0/2, and then secondary CPE on gi2/0/1 and its SPAN port on gi2/0/2, you will need to issue the following commands:

```
conf t
int gi1/0/2
description SPAN_PORT for <CPE ID>
speed 1000
duplex full

int gi2/0/2
description SPAN_PORT for <CPE ID>
speed 1000
duplex full

monitor session 1 source interface gi1/0/1
monitor session 1 destination interface gi1/0/2
monitor session 2 source interface gi2/0/1
monitor session 2 destination interface gi2/0/2
```

2. ESXI CONFIGURATION

Each physical SPAN port from the switch needs to be connected to a separate dedicated vSwitch, which will be connected to a dedicated vNIC on the VMs.

The switches will need to be configured to run in promiscuous mode. One physical NIC will be connected to each SPAN port on the switch.

Login to the ESXi server with the VI Client, select Host -> Configuration -> Networking

Select Add Networking…

Connection Types, select Virtual Machine

Create a virtual switch, and select the correct vmnic

Network Label: SPAN_Network_<CPE ID>

Under the new vSwitch, select Properties

On the Ports tab, select vSwitch -> Edit

On the Security tab, use the following settings:

Promiscuous Mode: Accept

MAC Address Changes: Accept

Forget Transmits: Accept

Repeat this for additional SPAN ports.

2.1.SNAPSHOT OF CURRENT CONFIGURATION

These machines are installed on the site ESXi servers.

Memory:

384 Mb assigned, and 1 vCPUs.

Create a new VM

Typical

NAME

Select DATASTORE

Select Linux -> Debian GNU/Linux 5 (64-bit)

Virtual Disk Size: 3Gb

Edit the hardware, and add an additional NIC

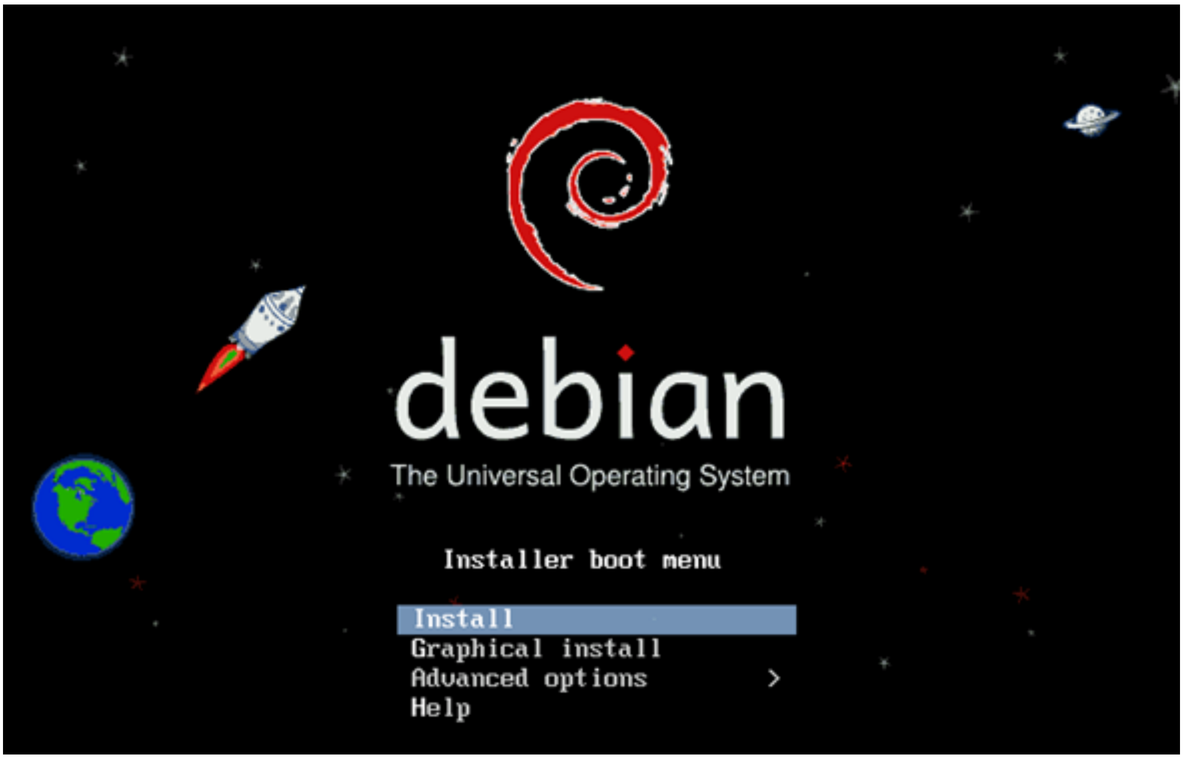
NIC1	PROD_Network
NIC2	SPAN_Network_<CPE ID>
NIC3	SPAN_Network_<CPE ID>

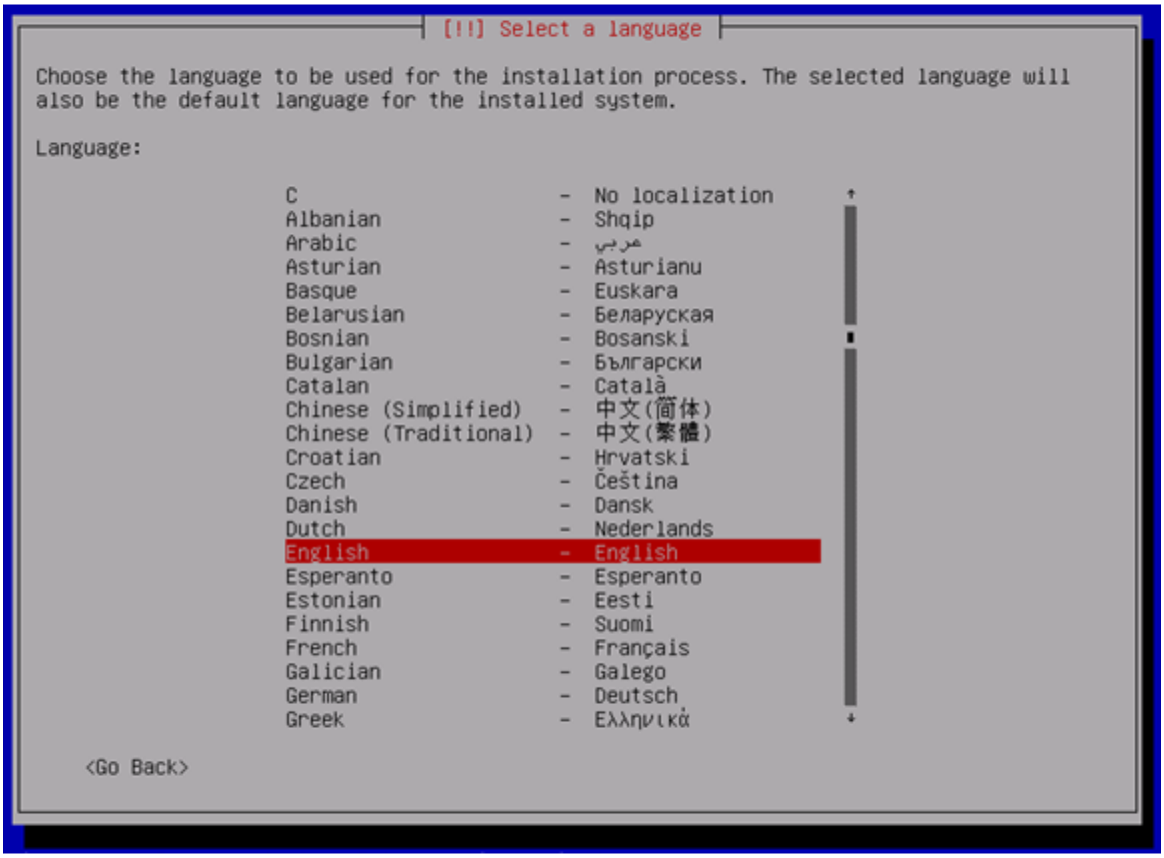
Attach the following ISO, and select the Connect at Power On

Debian-6.0.3-amd64-netinst.iso

3. OS INSTALLATION

Start the VM and open the console

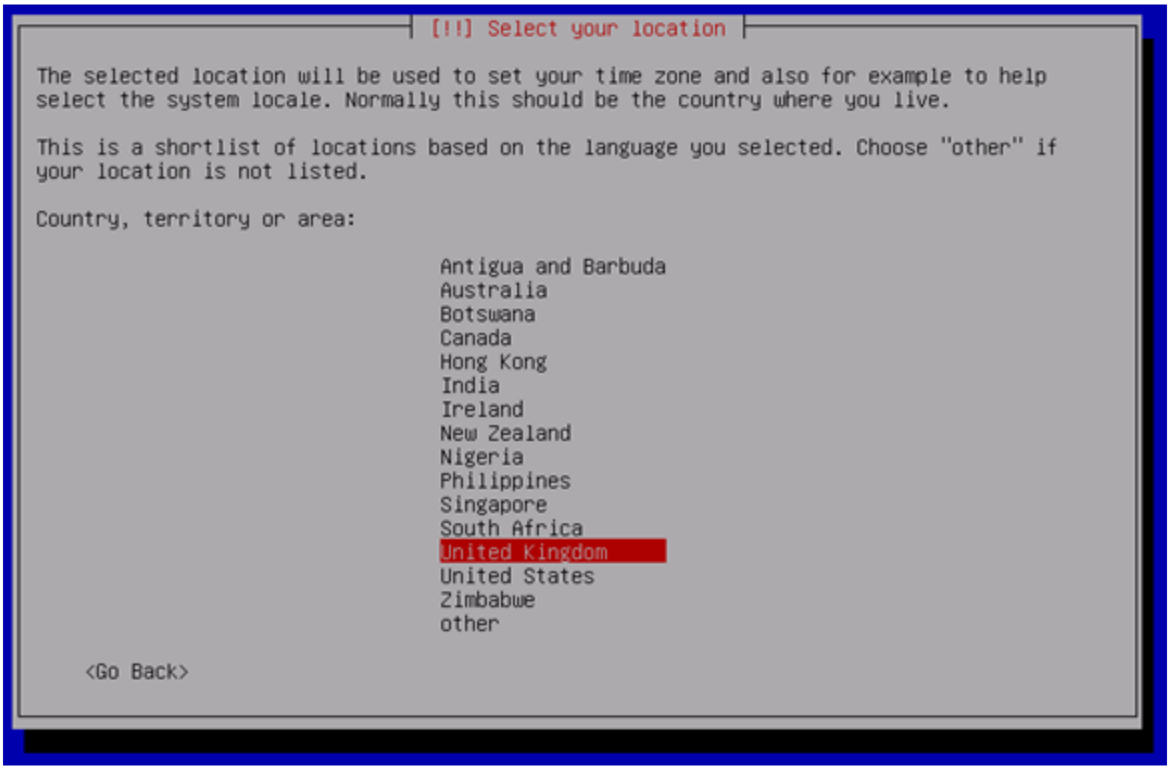




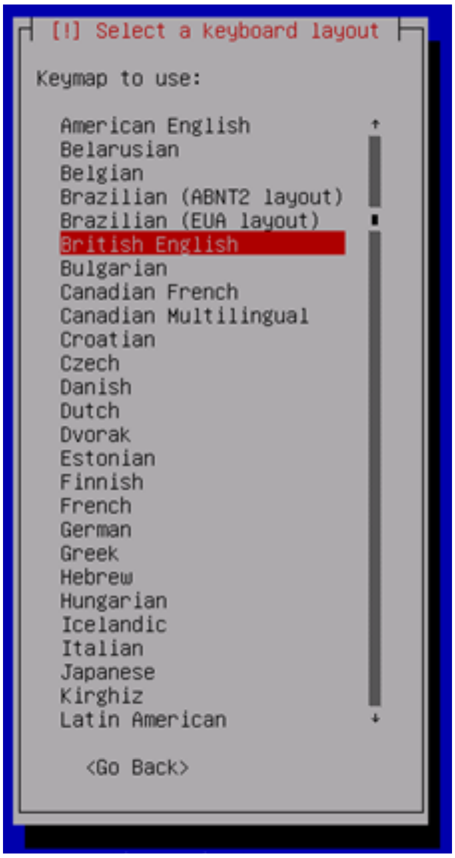
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

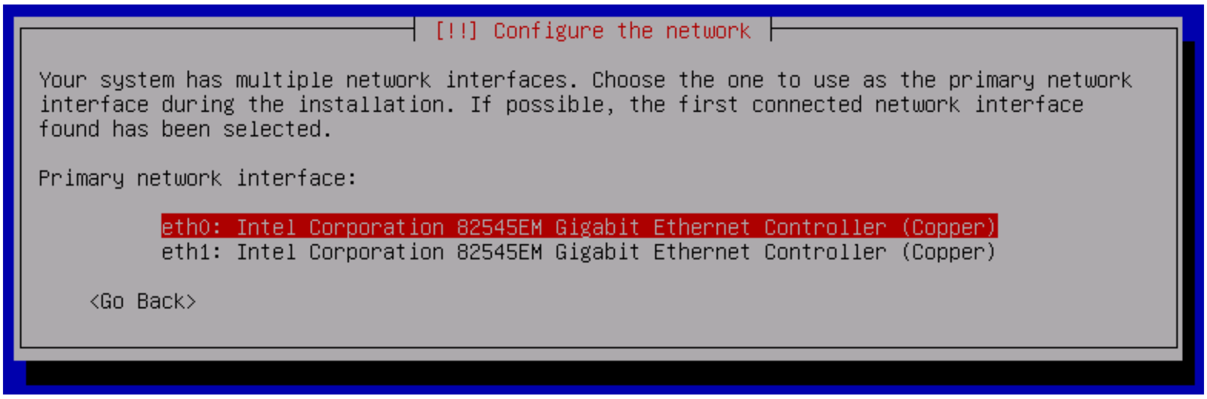
```
C                      -  No localization
Albanian               -  Shqip
Arabic                 -  عربي
Asturian               -  Asturianu
Basque                 -  Euskara
Belarusian             -  Беларуская
Bosnian                -  Bosanski
Bulgarian              -  Български
Catalan                -  Català
Chinese (Simplified)   -  中文(简体)
Chinese (Traditional)  -  中文(繁體)
Croatian               -  Hrvatski
Czech                  -  Čeština
Danish                 -  Dansk
Dutch                  -  Nederlands
English                -  English
Esperanto              -  Esperanto
Estonian               -  Eesti
Finnish                -  Suomi
French                 -  Français
Galician               -  Galego
German                 -  Deutsch
Greek                  -  Ελληνικά
```



```
[!!] 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.

This is a shortlist of locations based on the language you selected. Choose "other" if
your location is not listed.

Country, territory or area:

                                  Antigua and Barbuda
                                  Australia
                                  Botswana
                                  Canada
                                  Hong Kong
                                  India
                                  Ireland
                                  New Zealand
                                  Nigeria
                                  Philippines
                                  Singapore
                                  South Africa
                                  United Kingdom
                                  United States
                                  Zimbabwe
                                  other

    <Go Back>
```

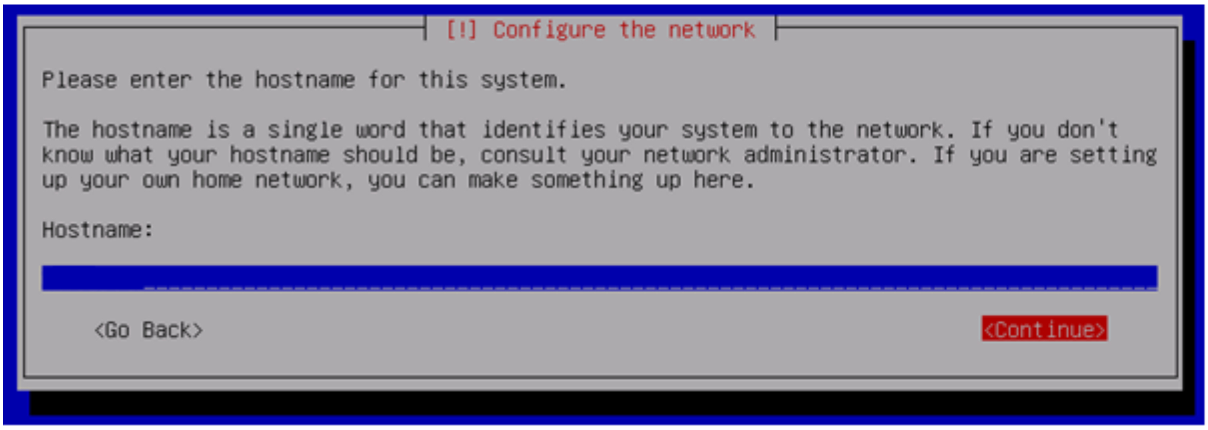


```
[!] Select a keyboard layout

Keymap to use:

  American English
  Belarusian
  Belgian
  Brazilian (ABNT2 layout)
  Brazilian (EUA layout)
  British English
  Bulgarian
  Canadian French
  Canadian Multilingual
  Croatian
  Czech
  Danish
  Dutch
  Dvorak
  Estonian
  Finnish
  French
  German
  Greek
  Hebrew
  Hungarian
  Icelandic
  Italian
  Japanese
  Kirghiz
  Latin American

    <Go Back>
```

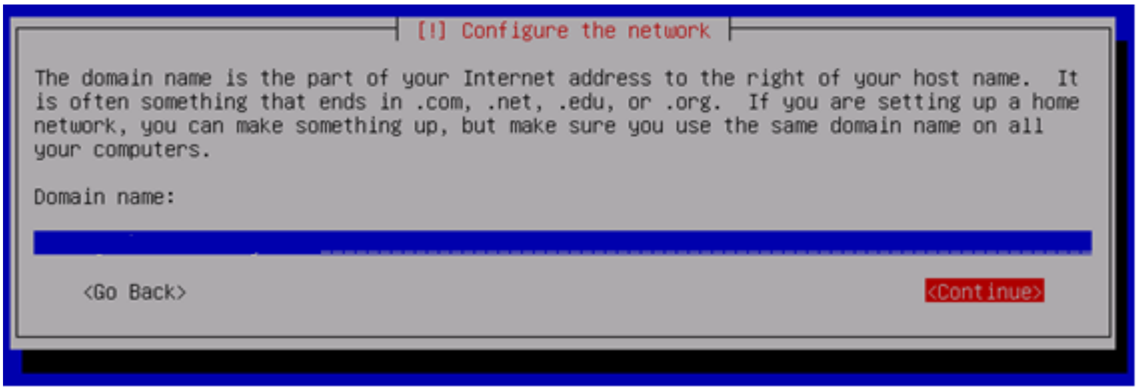


```
[!!] Configure the network

Your system has multiple network interfaces. Choose the one to use as the primary network
interface during the installation. If possible, the first connected network interface
found has been selected.

Primary network interface:

          eth0: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)
          eth1: Intel Corporation 82545EM Gigabit Ethernet Controller (Copper)

    <Go Back>
```

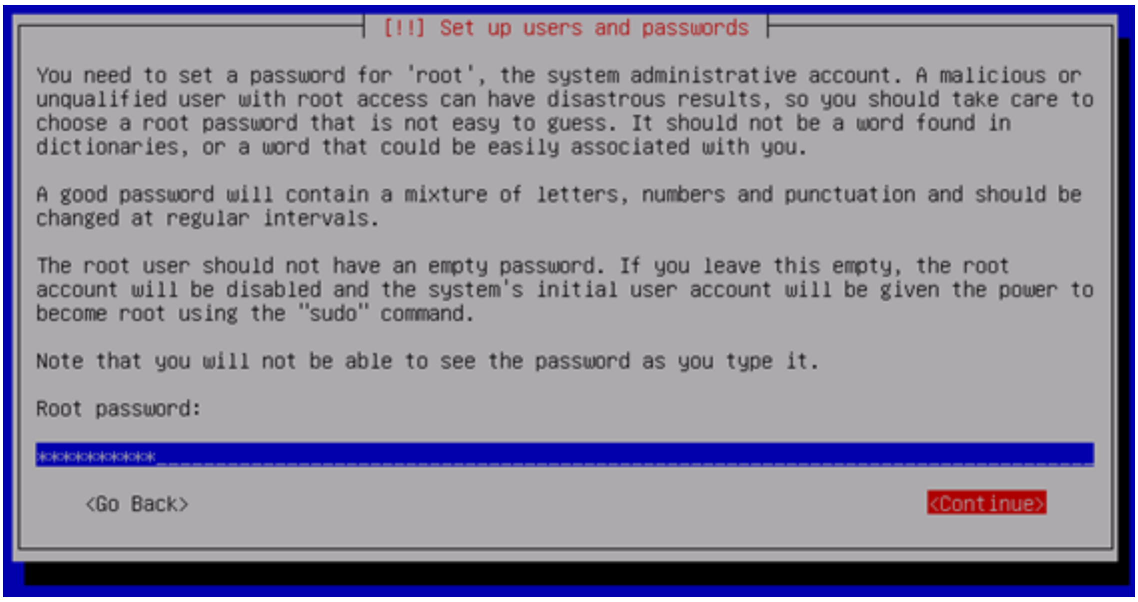
Always select eth0.



```
[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't
know what your hostname should be, consult your network administrator. If you are setting
up your own home network, you can make something up here.

Hostname:

    <Go Back>                                                            <Continue>
```

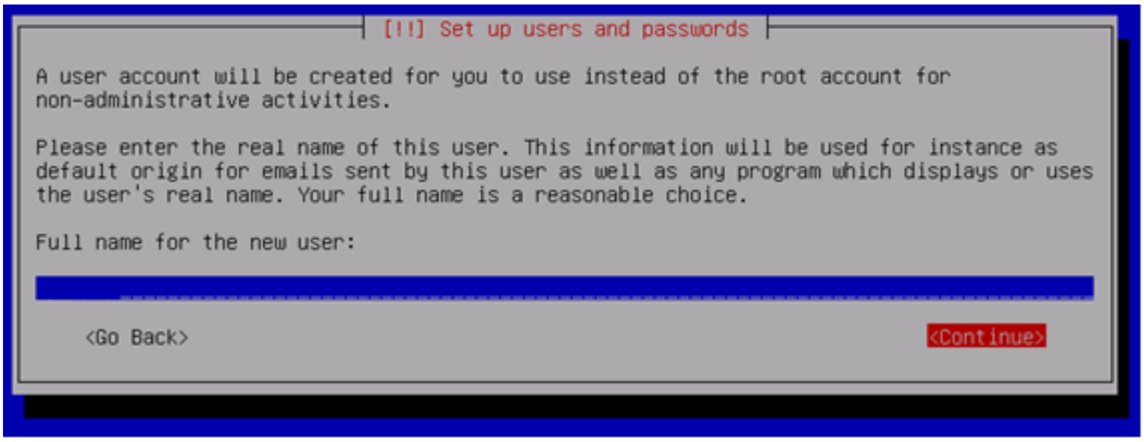


```
[!] Configure the network

The domain name is the part of your Internet address to the right of your host name.  It
is often something that ends in .com, .net, .edu, or .org.  If you are setting up a home
network, you can make something up, but make sure you use the same domain name on all
your computers.

Domain name:

    <Go Back>                                                        <Continue>
```



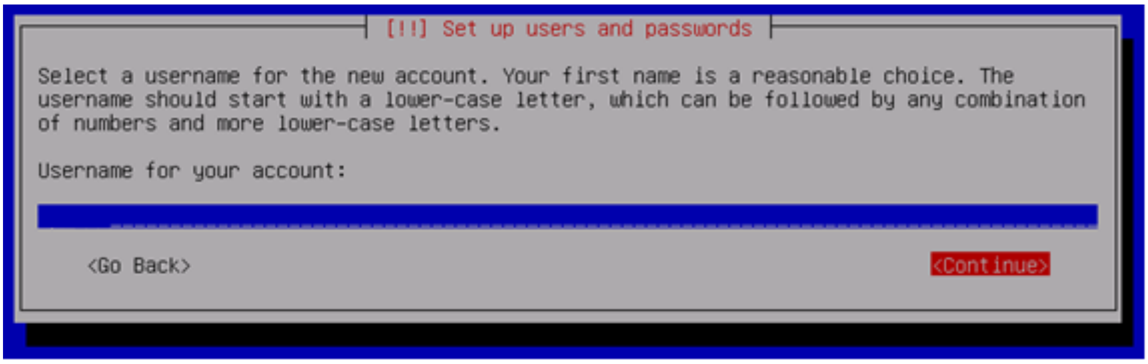
```
[!!] Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or
unqualified user with root access can have disastrous results, so you should take care to
choose a root password that is not easy to guess. It should not be a word found in
dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be
changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root
account will be disabled and the system's initial user account will be given the power to
become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

**********

     <Go Back>                                                       <Continue>
```

Enter a temporary root password (we will change this later)

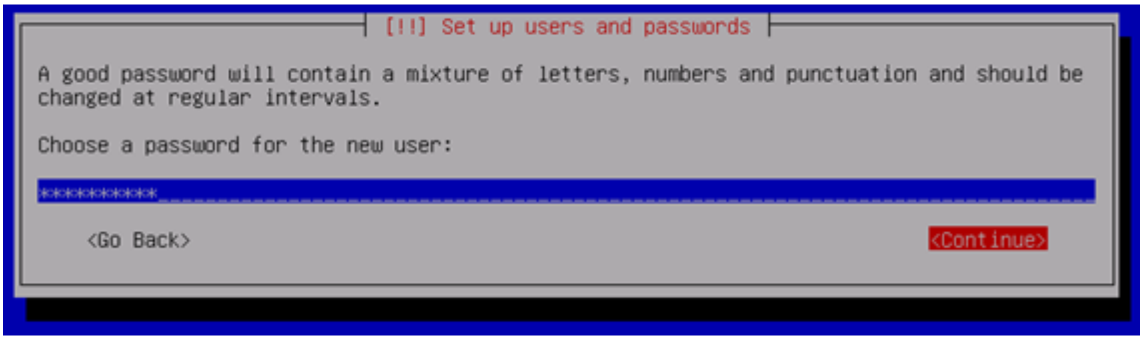


```
[!!] Set up users and passwords

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:

     <Go Back>                                                       <Continue>
```

Create a standard user account



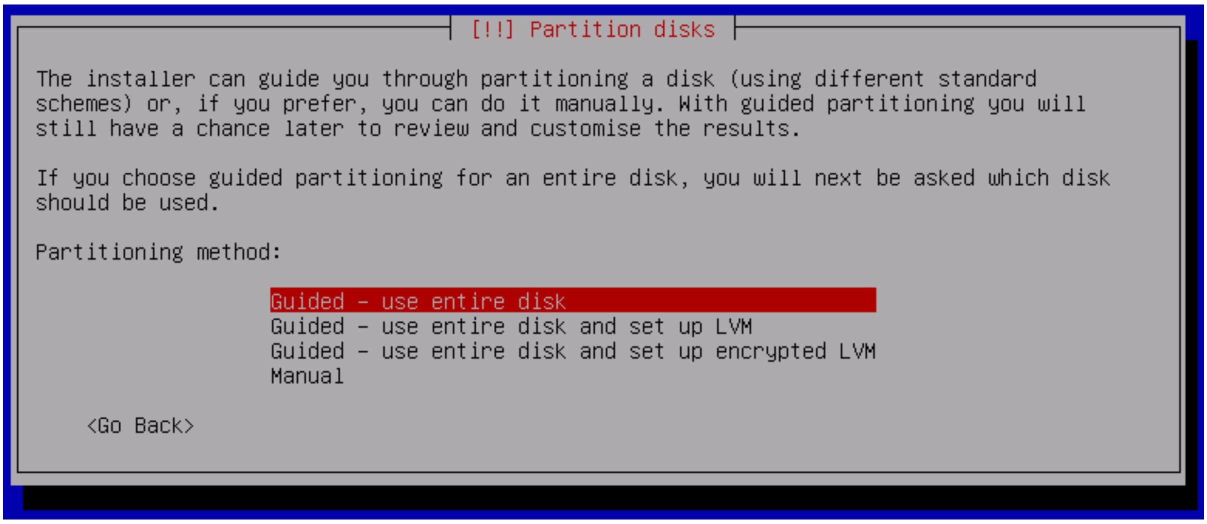
```
[!!] Set up users and passwords

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:

     <Go Back>                                                       <Continue>
```



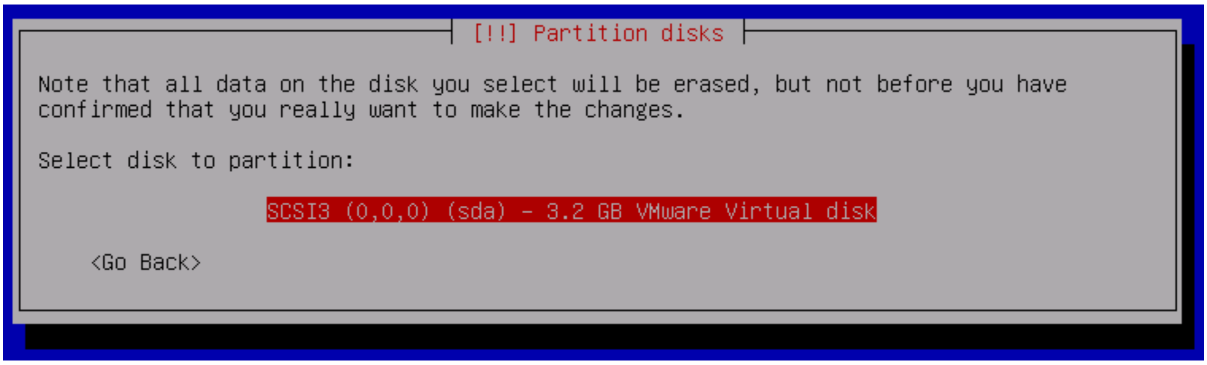
```
[!!] Set up users and passwords

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>
```

Enter a temporary ops password (we will change this later)

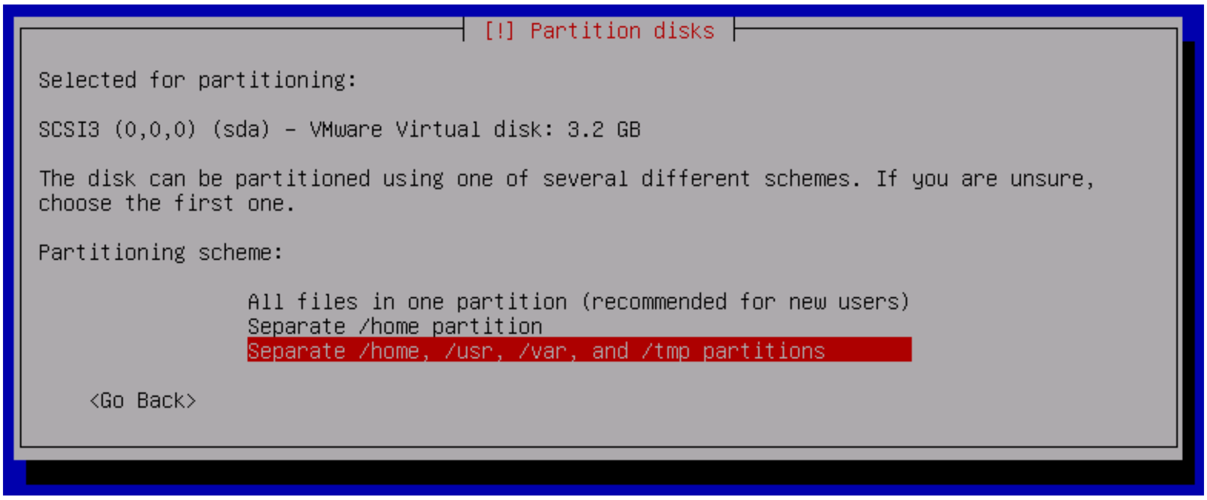
As this machine runs one small app, which is processing, then proxying NetFlow data to the central collector, we really don’t need to manually configure the partitions, so we will accept the defaults:



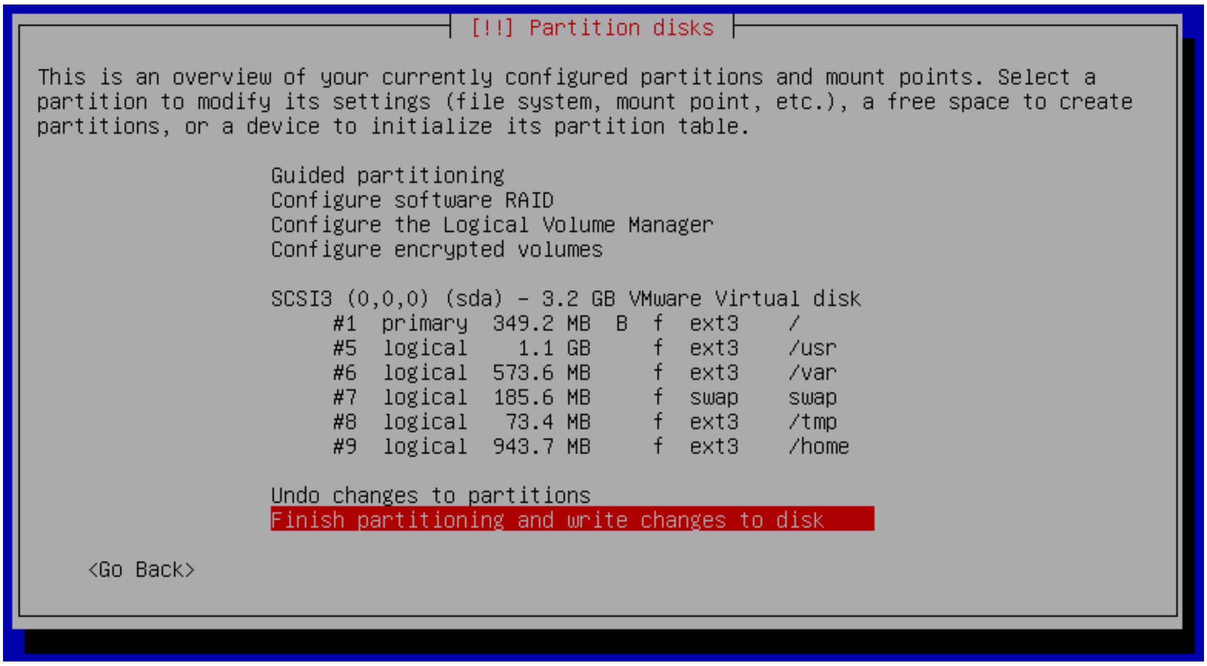
```
[!!] Partition disks

The installer can guide you through partitioning a disk (using different standard
schemes) or, if you prefer, you can do it manually. With guided partitioning you will
still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk
should be used.

Partitioning method:

                    Guided - use entire disk
                    Guided - use entire disk and set up LVM
                    Guided - use entire disk and set up encrypted LVM
                    Manual

    <Go Back>
```



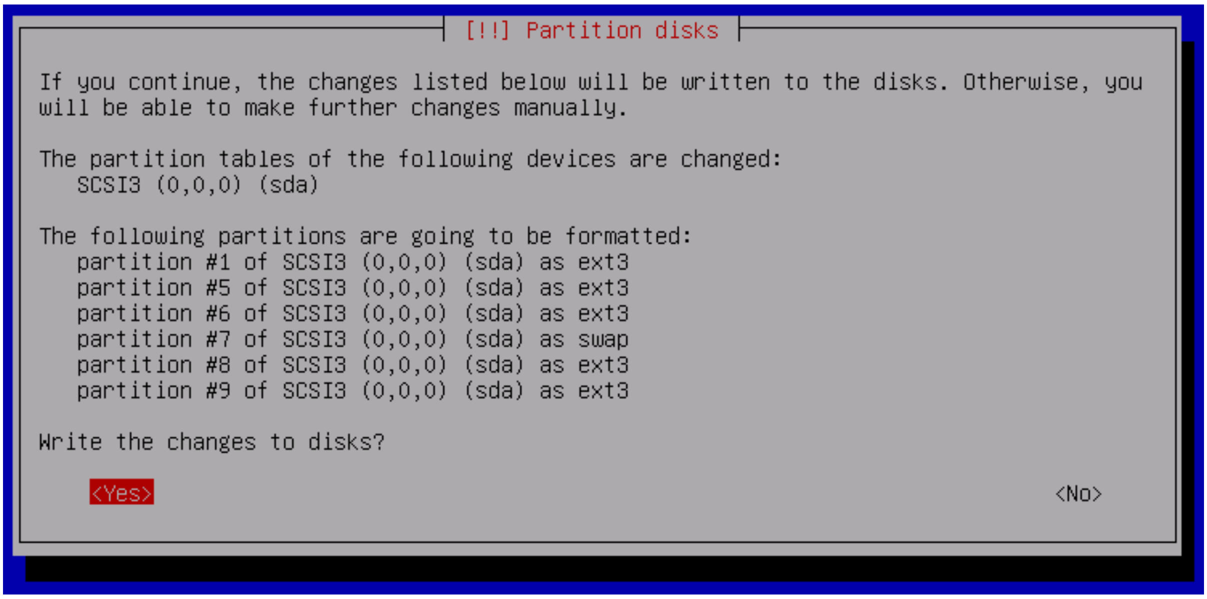
```
[!!] Partition disks

Note that all data on the disk you select will be erased, but not before you have
confirmed that you really want to make the changes.

Select disk to partition:

                    SCSI3 (0,0,0) (sda) - 3.2 GB VMware Virtual disk

    <Go Back>
```



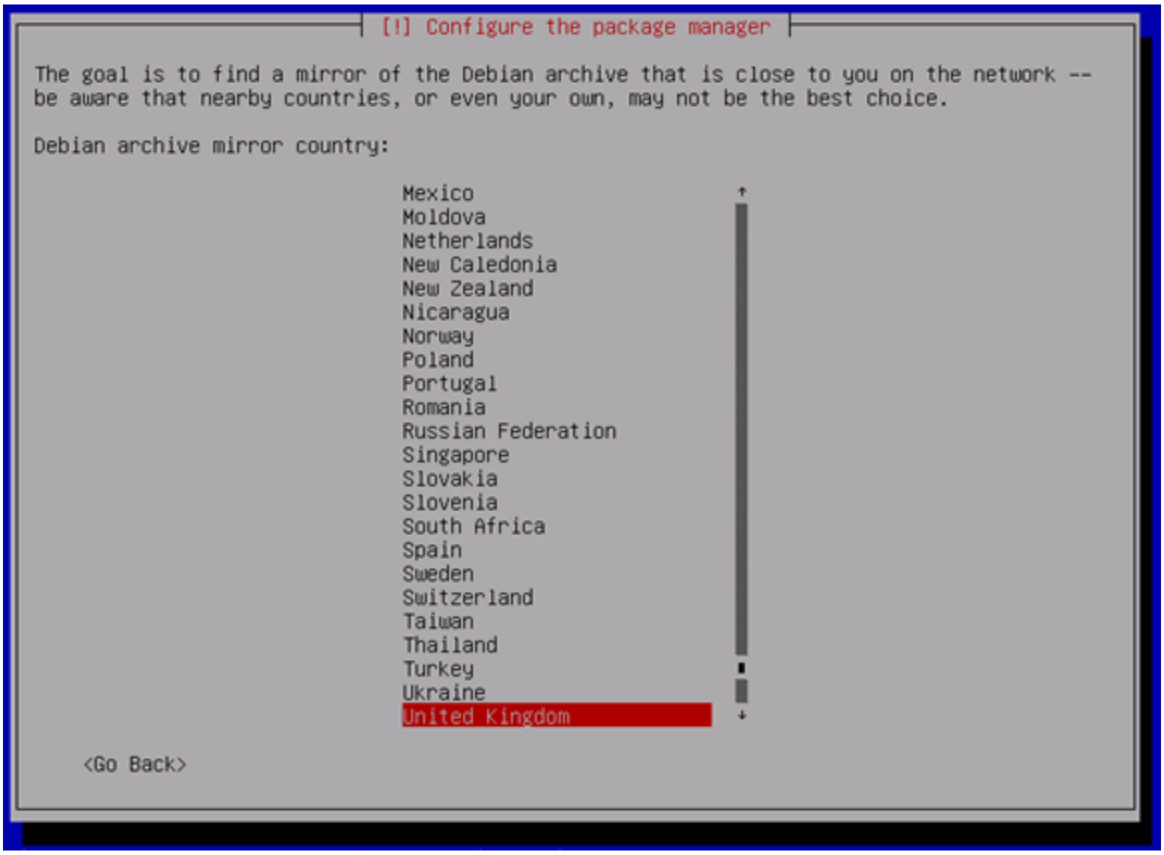
```
                         [!] Partition disks

Selected for partitioning:

SCSI3 (0,0,0) (sda) - VMware Virtual disk: 3.2 GB

The disk can be partitioned using one of several different schemes. If you are unsure,
choose the first one.

Partitioning scheme:

                 All files in one partition (recommended for new users)
                 Separate /home partition
                 Separate /home, /usr, /var, and /tmp partitions

    <Go Back>
```



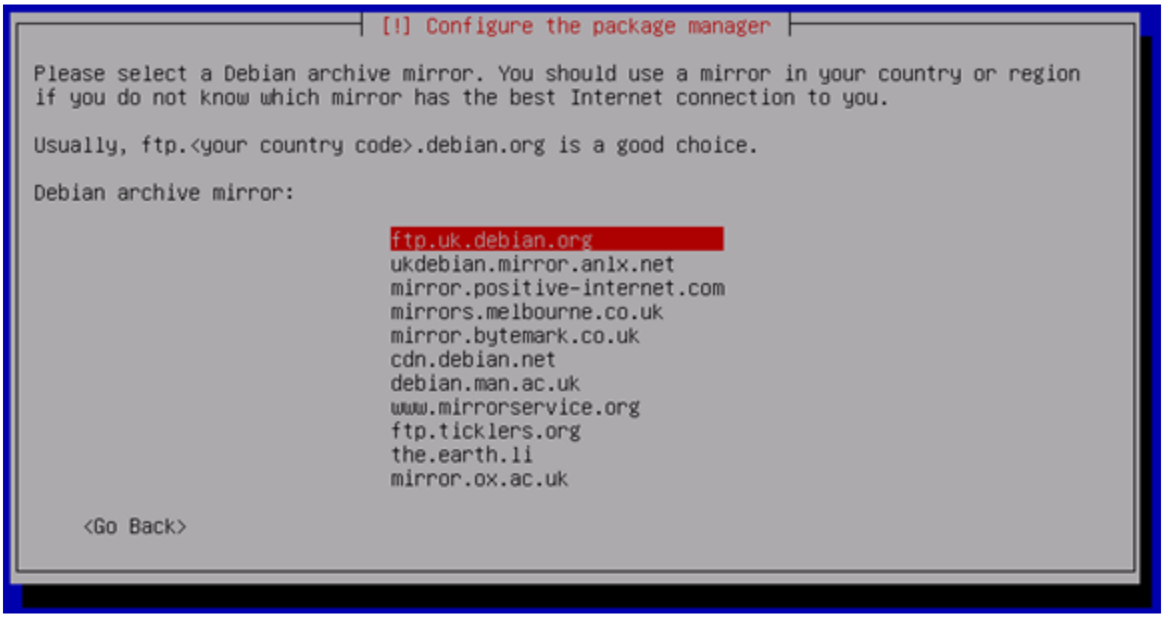
```
                         [!!] Partition disks

This is an overview of your currently configured partitions and mount points. Select a
partition to modify its settings (file system, mount point, etc.), a free space to create
partitions, or a device to initialize its partition table.

                   Guided partitioning
                   Configure software RAID
                   Configure the Logical Volume Manager
                   Configure encrypted volumes

                   SCSI3 (0,0,0) (sda) - 3.2 GB VMware Virtual disk
                        #1  primary  349.2 MB  B  f  ext3    /
                        #5  logical    1.1 GB     f  ext3    /usr
                        #6  logical  573.6 MB     f  ext3    /var
                        #7  logical  185.6 MB     f  swap    swap
                        #8  logical   73.4 MB     f  ext3    /tmp
                        #9  logical  943.7 MB     f  ext3    /home

                   Undo changes to partitions
                   Finish partitioning and write changes to disk

    <Go Back>
```



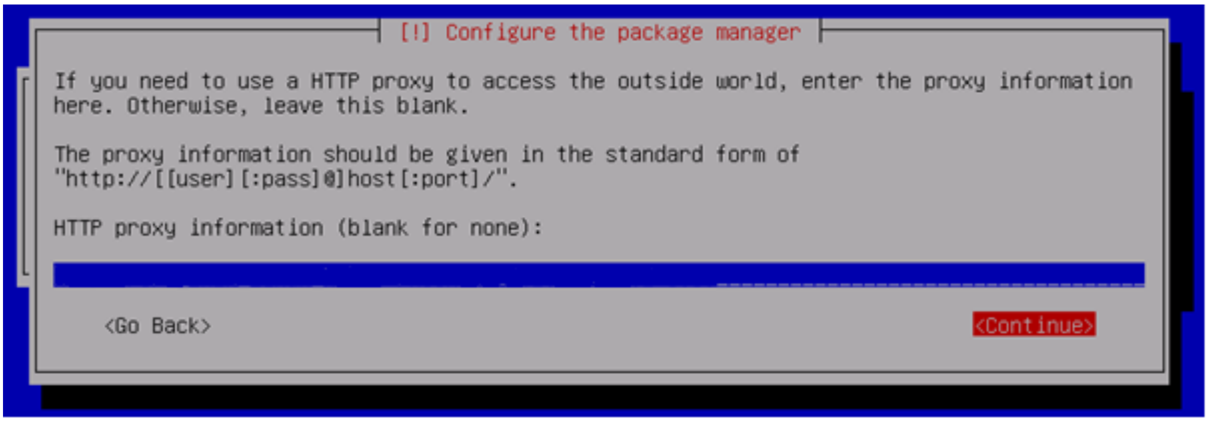
```
                        [!!] Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you
will be able to make further changes manually.

The partition tables of the following devices are changed:
   SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
   partition #1 of SCSI3 (0,0,0) (sda) as ext3
   partition #5 of SCSI3 (0,0,0) (sda) as ext3
   partition #6 of SCSI3 (0,0,0) (sda) as ext3
   partition #7 of SCSI3 (0,0,0) (sda) as swap
   partition #8 of SCSI3 (0,0,0) (sda) as ext3
   partition #9 of SCSI3 (0,0,0) (sda) as ext3

Write the changes to disks?

    <Yes>                                                                      <No>
```



```
[!] Configure the package manager

The goal is to find a mirror of the Debian archive that is close to you on the network --
be aware that nearby countries, or even your own, may not be the best choice.

Debian archive mirror country:

                         Mexico
                         Moldova
                         Netherlands
                         New Caledonia
                         New Zealand
                         Nicaragua
                         Norway
                         Poland
                         Portugal
                         Romania
                         Russian Federation
                         Singapore
                         Slovakia
                         Slovenia
                         South Africa
                         Spain
                         Sweden
                         Switzerland
                         Taiwan
                         Thailand
                         Turkey
                         Ukraine
                         United Kingdom

    <Go Back>
```



```
[!] Configure the package manager

Please select a Debian archive mirror. You should use a mirror in your country or region
if you do not know which mirror has the best Internet connection to you.

Usually, ftp.<your country code>.debian.org is a good choice.

Debian archive mirror:

                        ftp.uk.debian.org
                        ukdebian.mirror.anlx.net
                        mirror.positive-internet.com
                        mirrors.melbourne.co.uk
                        mirror.bytemark.co.uk
                        cdn.debian.net
                        debian.man.ac.uk
                        www.mirrorservice.org
                        ftp.ticklers.org
                        the.earth.li
                        mirror.ox.ac.uk

    <Go Back>
```

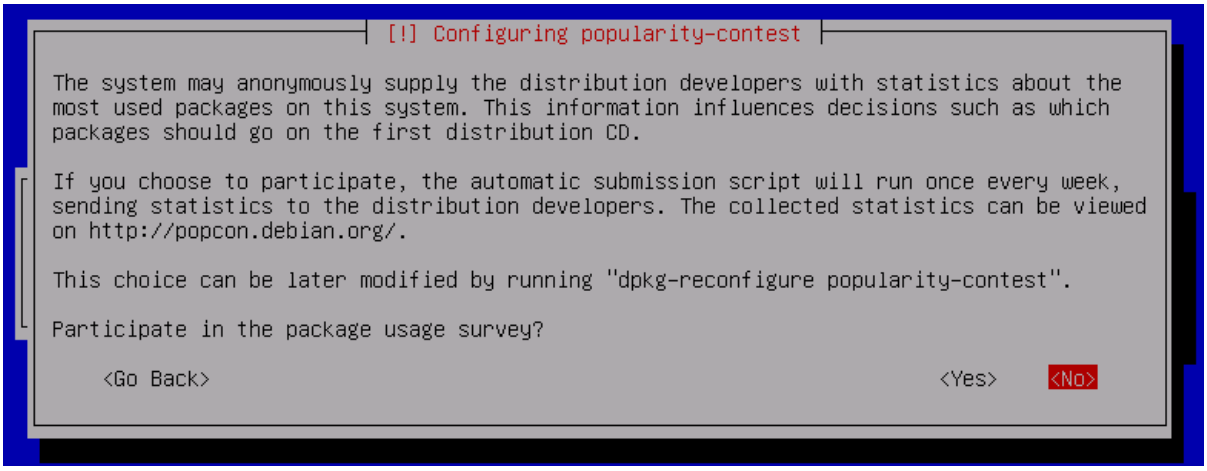


[!] Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".

HTTP proxy information (blank for none):



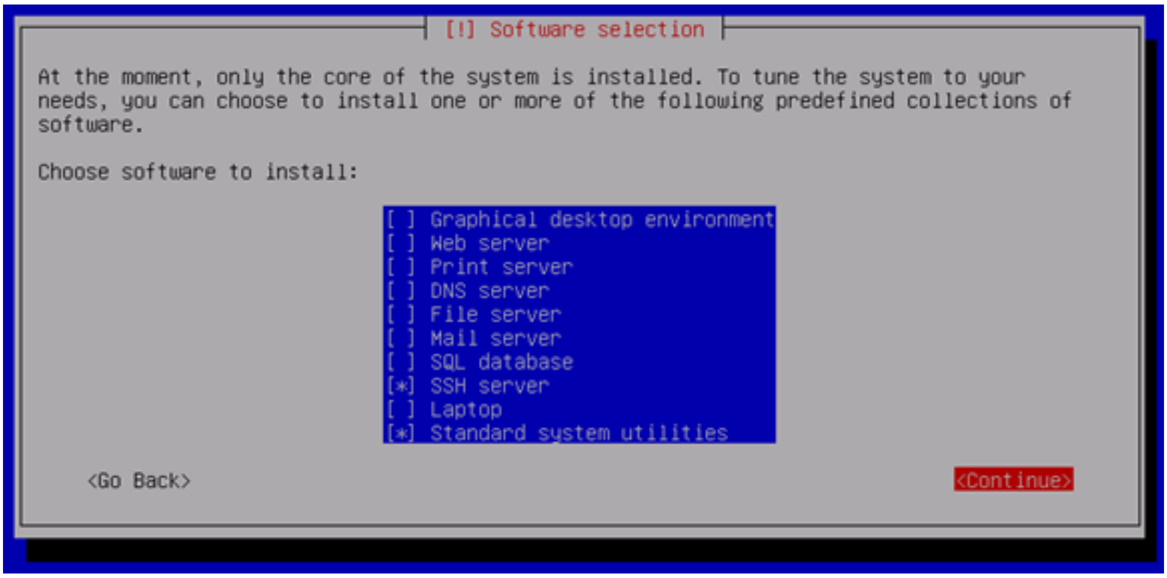
[!] Configuring popularity-contest

The system may anonymously supply the distribution developers with statistics about the most used packages on this system. This information influences decisions such as which packages should go on the first distribution CD.

If you choose to participate, the automatic submission script will run once every week, sending statistics to the distribution developers. The collected statistics can be viewed on http://popcon.debian.org/.

This choice can be later modified by running "dpkg-reconfigure popularity-contest".

Participate in the package usage survey?



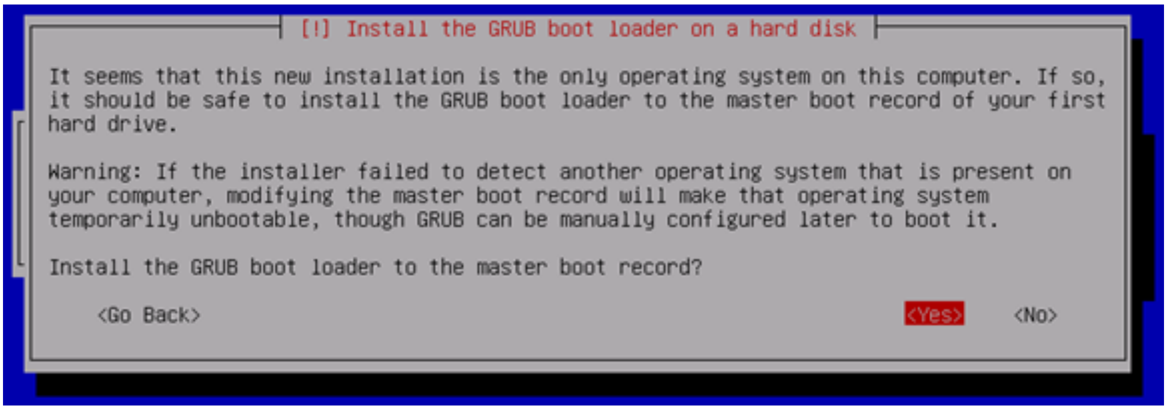
[!] Software selection

At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.

Choose software to install:

```
[ ] Graphical desktop environment
[ ] Web server
[ ] Print server
[ ] DNS server
[ ] File server
[ ] Mail server
[ ] SQL database
[*] SSH server
[ ] Laptop
[*] Standard system utilities
```

Select SSH Server and Standard system utilities.

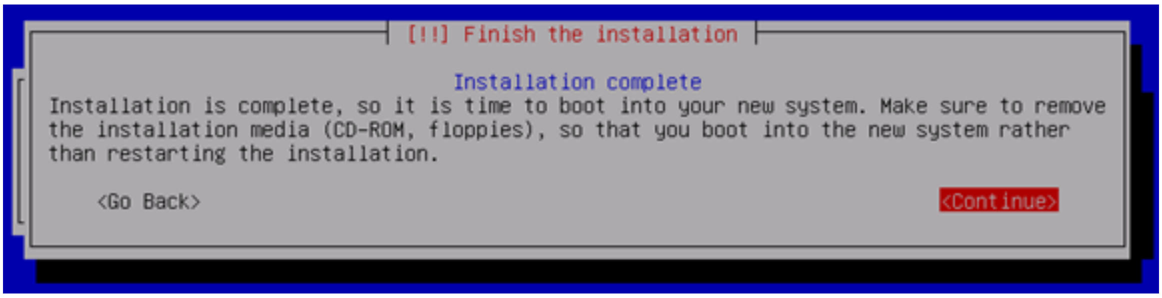


[!] Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?



[!!] Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.

Once the server has rebooted, login with root from the console of the ESXi server.

3.1.SET IP ADDRESS AND ADD DNS ENTRY

Edit the network configuration file, depending on how many NICs you have attached:

```
vi /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 static
address xxx.xxx.xxx.xxx
netmask xxx.xxx.xxx.xxx
network xxx.xxx.xxx.xxx
broadcast xxx.xxx.xxx.xxx
gateway xxx.xxx.xxx.xxx

auto eth1
iface eth1 inet dhcp

auto eth2
iface eth2 inet dhcp


:wq

reboot
```

While the server is rebooting, add a DNS A record (including PTR record)

You can now login to the server via SSH as root

3.2.CONFIGURE DNS

```
vi /etc/resolv.conf
      domain my.domain.com
      search my.domain.com
      nameserver xxx.xxx.xxx.xxx
      nameserver xxx.xxx.xxx.xxx
      nameserver xxx.xxx.xxx.xxx
      nameserver xxx.xxx.xxx.xxx
      nameserver xxx.xxx.xxx.xxx

:wq
```

3.3.INSTALL NTP

```
apt-get install ntp
Do you want to continue [Y/n]? Y

vi /etc/ntp.conf
```

Find the section where the servers are listed, delete the four existing entries, and add:

```
server xxx.xxx.xxx.xxx
:wq

/etc/init.d/ntp restart
dpkg-reconfigure ntp
ntpq -p
```

3.4.INSTALL VMWARE TOOLS

```
apt-get install build-essential linux-headers-`uname -r`
Do you want to continue [Y/n]? Y
```

While this is installing, return to the VI Client, right-click on the host -> Guest -> Install/Upgrade VMware Tools

When the installation has completed, enter the following commands:

```
mount /media/cdrom0
cp /media/cdrom/VMware<tab> /home/ops
cd /home/ops
tar xvf VMwareTools<tab>
cd vmware-tools-distrib/
./vmware-install.pl --default
rm VMwareTools<tab>
rm -r /home/ops/vmware-tools-distrib
```

3.5.DISABLE ROOT LOGIN DIRECTLY FROM SSH AND RESET PASSWORDS

```
vi /etc/ssh/sshd_config
```

Find the line “PermitRootLogin yes” and change it to:

```
PermitRootLogin no

:wq
```

Restart the SSH service:

```
/etc/init.d/ssh restart


passwd root
```

Enter a strong password

```
passwd ops
```

Enter a strong password

4. INSTALL NPROBE

4.1.PREREQUISITES

You will need to login with the "ops" user, and then SU – (as we disabled root from being able to login directly)

```
      apt-get install libtool automake autoconf subversion python-dev libpcap-dev
```

Add proxy details to subversion

```
vi /root/.subversion/servers
```

Fine the [global] section, and edit as follows:

```
[global]

http-proxy-host = xxx.xxx.xxx.xxx

http-proxy-port = xxxx

http-proxy-username = Username

http-proxy-password = Password

:wq
```

4.2.INSTALLATION

The file nprobe_6.7.0_111911.tgz has been downloaded from:

http://www.nmon.net/nprobe

Transfer this to the server (/home/ops) using WinSCP.

SSH to the server, login as Ops, and SU –, then run the following commands:

```
cd /home/ops
tar xvf nprobe_<tab>
cd nprobe_<tab>
./autogen.sh

8. Downloading OpenDPI-ntop...
Error validating server certificate for 'https://svn.ntop.org:443':
 - The certificate hostname does not match.
Certificate information:
 - Hostname: ntop.org
 - Valid: from Sat, 15 Oct 2011 09:19:36 GMT until Thu, 16 Aug 2012
16:56:46 GMT
 - Issuer: 07969287, http://certificates.godaddy.com/repository,
GoDaddy.com, Inc., Scottsdale, Arizona, US
```

```
    - Fingerprint: 6a:52:49:4c:76:fb:27:cb:2f:
32:33:f6:c8:51:00:26:f5:99:f7:5a
(R)eject, accept (t)emporarily or accept (p)ermanently?

Press P

Make
Make install
rm nprobe-<tab>.tgz
rm -r nprobe-<tab>
```

4.3.CONFIGURATION

You will now need to configure the options, these are detailed in the nProbe documentation.

For example

OPTIONS="-u 432 -1 11:01:F5:B3:12:D5@432 -q 192.168.1.11:2055 -V 5 -i eth1 -n 192.168.52.10:9996 ${PID_FILE}"

This is using an Interface Index of 432 which has the MAC address 11:01:F5:B3:12:D5, with an IP address of 192.168.1.11 on port 2055. Then the collector server is 192.168.1.11 port 9996.

4.4.LINK THE LIBRARY

```
vi /etc/ld.so.conf
```

add the line:

```
include /usr/local/lib

:wq

ldconfig
```

4.5.CREATING THE SERVICES

Once we have all this data, we can create the required services (one per monitored interface). To do this, we first need to create a file for each of the services.

```
    vi /etc/init.d/nprobe.sh

#! /bin/bash

#

# (C) 2003-10 - Luca Deri <deri@ntop.org>

#

### BEGIN INIT INFO
```

```
# Provides:          nprobe
# Required-Start:    $local_fs $remote_fs $network $syslog
# Required-Stop:     $local_fs $remote_fs $network $syslog
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Start/stop nprobe web
### END INIT INFO
#
# nprobe          This init.d script is used to start nprobe.
#

NPROBE=/usr/local/bin/nprobe
INTERFACE="eth1"
PID_FILE="/var/run/nprobe.pid"
OPTIONS="-u 432 -1 11:01:F5:B3:12:D5@432 -q 192.168.1.11:2055 -V 5 -i eth1 -n 192.168.52.10:9996 ${PID_FILE}"
start_nprobe() {
    ${NPROBE} ${OPTIONS} > /dev/null &
    return 1
}
stop_nprobe() {
    if [ -f ${PID_FILE} ]; then
      kill `cat ${PID_FILE}`  2>1 /dev/null
      \rm ${PID_FILE}
    fi
}
########
if [ -z "$2" ]; then
    interface="all";
else
    interface=$2;
fi
case "$1" in
  start)
      echo -n "Starting nProbe"
      start_nprobe $interface;
      echo " Done."
      ;;
  force-start)
```

```
      echo -n "Starting nProbe"
      start_nprobe $interface;
      echo "Done."
      ;;
  stop)
        echo -n "Stopping nProbe"
            stop_nprobe $interface;
      echo " Done."
      ;;
  restart)
        echo -n "Restarting nProbe"
        stop_nprobe $interface;
      sleep 1
      start_nprobe $interface 0;
      echo " Done."
      ;;
  *)
      echo "Usage: /etc/init.d/nprobe {start|force-start|stop|restart}"
      exit 1
esac
exit 0

:wq
```

```
      chmod +x /etc/init.d/nprobe.sh
      insserv /etc/init.d/nprobe.sh
      /etc/init.d/nprobe.sh start
```