獬豸日志安全审计系统

安装卸载手册

北京携推信息技术有限公司

2019 年 12 月

声明

本文档所提及的产品信息仅供参考，相关内容可能会随时更新，北京携推信息技术有限公司恕不另行通知。

1．本文档中提到的产品功能、性能、规格可能因产品具体型号、应用环境、配置方法不同而有所差异，此类差异为正常现象，相关问题请咨询北京携推信息技术有限公司。

2．本文档包含獬豸日志安全审计系统的光盘安装与卸载操作说明。手册中涉及的文档、文字、标识等信息均受版权保护，未经许可，任何部分不得复制或传播，违者必究。

3．本手册适用于獬豸日志安全审计系统的最终用户。

目　录

1 安装设备硬件及配置要求

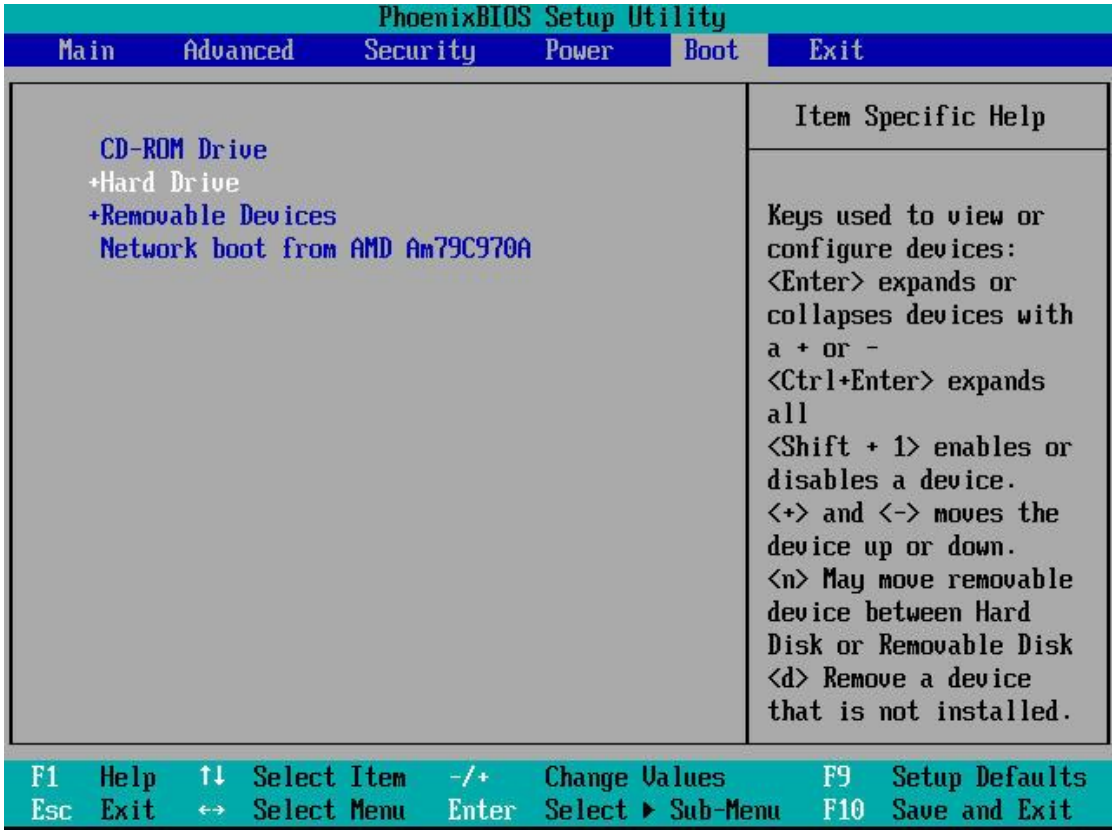
- 推荐使用 Xeon Intel 平台硬件环境。
- 最低安装要求：RAM 8GB，硬盘 50GB，网络端口 1 个。
- 软件安装时，设备必须连接显示器、键盘、光驱。
- 獬豸日志安全审计系统运行在 CentOS 系统下，自动安装光盘按标准环境定制，不保证所有环境安装成功。
- 请确保硬件驱动能被 CentOS 6.3 64 位系统正确识别，系统安装后网卡文件应识别为 ifcfg-ethx。
- 对于部分品牌服务器(如 DELL)，安装 CentOS 时网卡名称可能识别为 emx，此时推荐使用手动安装方式。
- 手动安装时，必须保证操作系统有可正常使用的 ifcfg-eth0 网口。

2 自动安装

本产品可基于 Linux CentOS 6.9 自动安装。

2.1 修改 BIOS

进入系统 BIOS，将第一启动设备设置为光驱（具体操作因主板型号而异，此处仅作示意）。



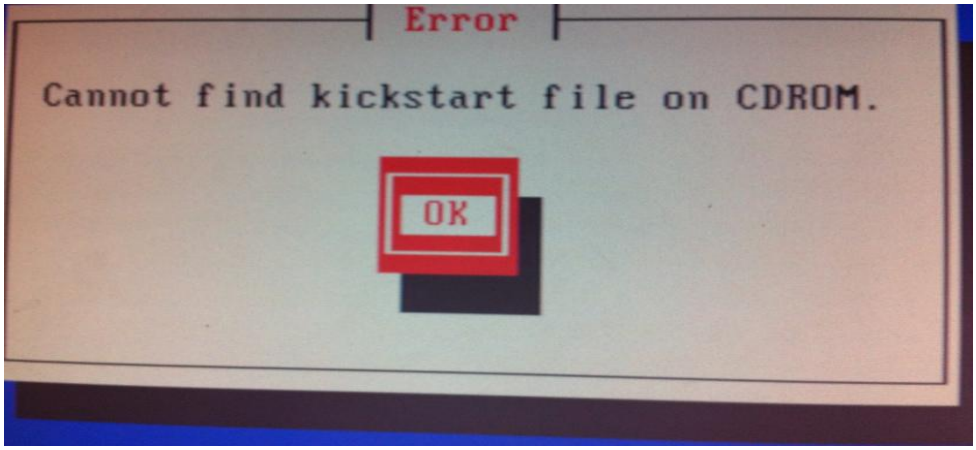
修改 BIOS 后，放入安装光盘，进入安装界面。

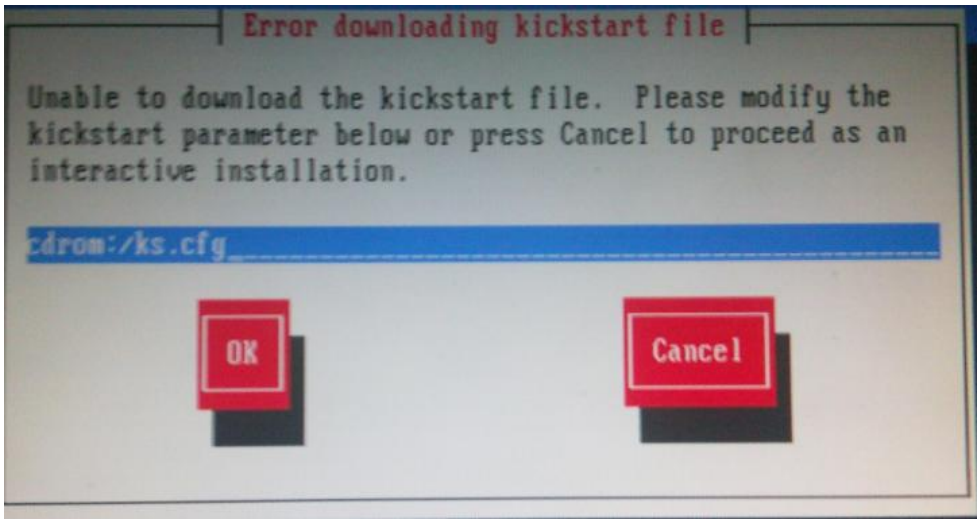
在此界面选择 LogAudit auto install 并回车，系统将开始自动安装。安装完成后会自动重启，请在重启时及时取出光盘。

2.2 开始自动安装

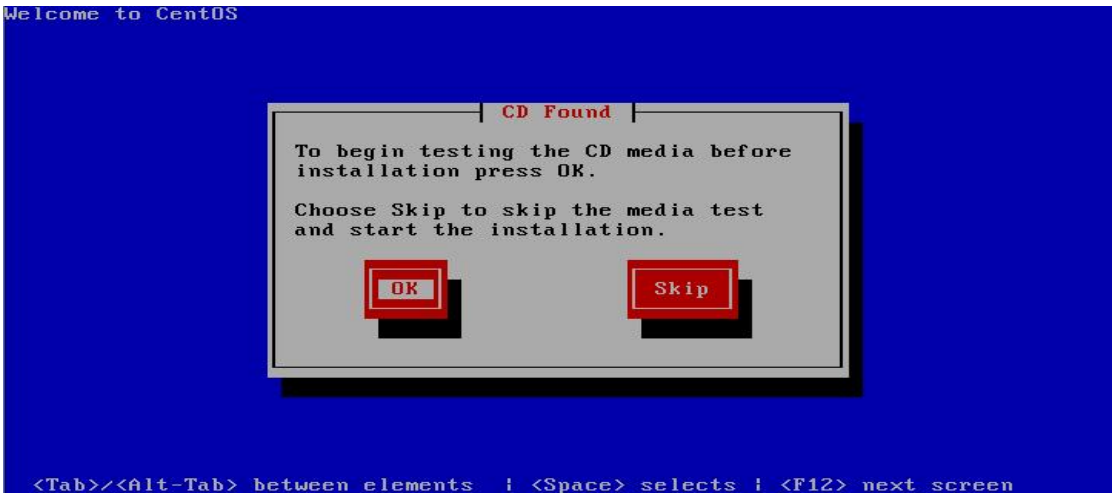
进入自动安装后，可能出现的几种特殊情况：

情况 1：若出现如下界面，先选择 OK，然后在第二个界面连续按两次回车。





情况 2：若询问是否检测光盘，选择 SKIP 回车即可。



情况 3：若提示硬盘需要格式化确认，选择 YES。

情况 4：若提示存储设备可能有数据，选择 Yes, discard any data。

如无特殊情况，系统将自动安装操作系统。安装完成后自动重启，此时请及时取出光盘。

系统再次启动后将自动安装獬豸日志安全审计系统，等待安装进度完成即可。

白色进度条完成后，等待约 3 分钟，系统再次重启，屏幕出现 NLA Login：提示，表示安装完成。

3 手动安装

手动安装分为两步：先安装操作系统（可选 CentOS 6.3 x64 至 6.9 x64 任意版本），再安装獬豸日志安全审计系统程序。

3.1 操作系统安装

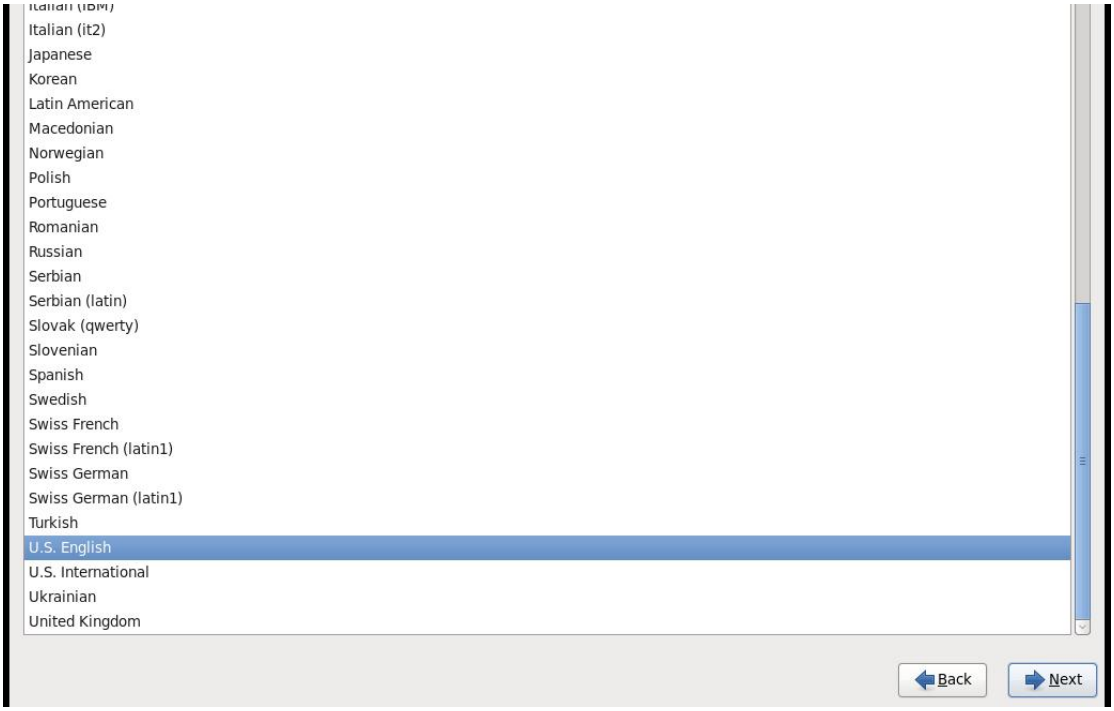
CentOS 光盘启动后，选择 Install or upgrade an existing system 并回车，或等待 60 秒自动进入。

出现是否测试 CD 媒体的提示，选择 Skip 跳过测试。

进入安装界面，点击 Next 继续。

3.1.1 语言、键盘设置

选择安装语言（默认英文，无需更改），键盘布局保持默认。



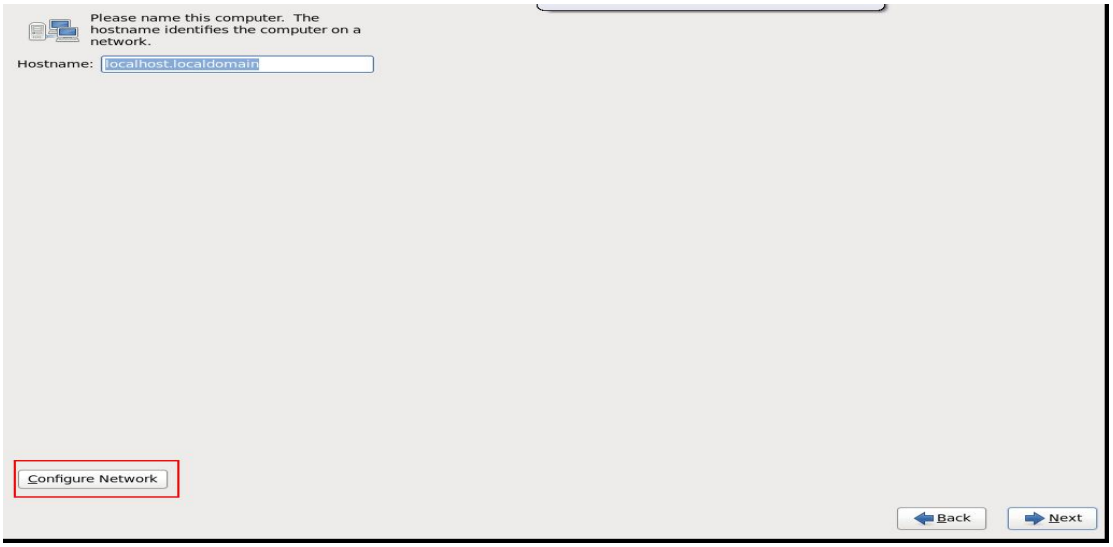
3.1.2 存储设备配置

通常选择 Basic Storage Devices，点击 Next。

若出现如下提示，点击 Yes, discard any data。

3.1.3 计算机名配置

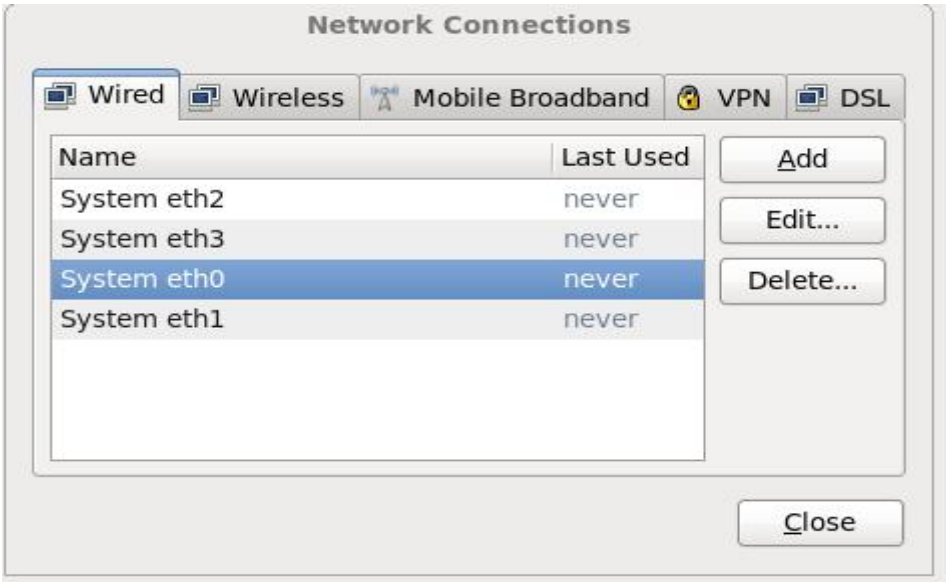
根据实际情况设置主机名。



3.1.4 网络配置

点击左下角 Configure Network，配置服务器网络。

选中 System eth0，点击 Edit。



勾选 Connect automatically，在 IPv4 Settings 中将 Method 选为 Manual，手动配置 IP 地址：

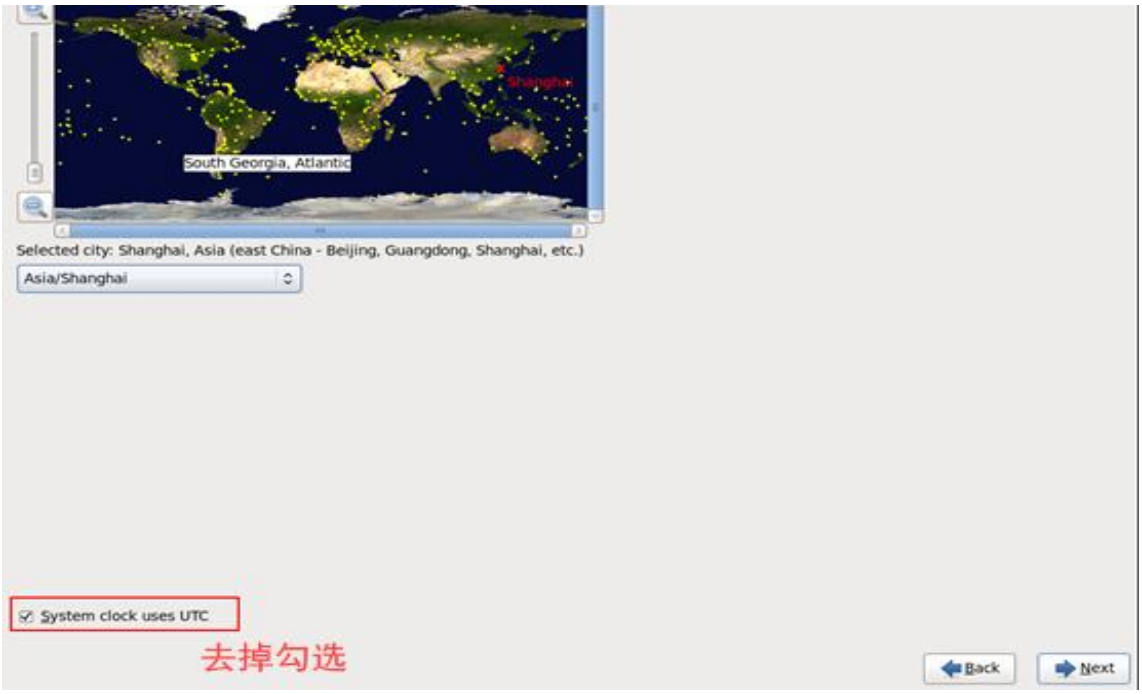
- eth0：172.19.11.24，子网掩码 255.255.255.0
- eth1（备用）：192.168.1.254，子网掩码 255.255.0.0

点击 Apply 保存配置，完成后关闭窗口。


Editing System eth1
Connection name:
System eth1
Connect automatically
Wired
802.1x Security
IPv4 Settings
IPv6 Settings
Method:
Manual
Addresses
Address
Netmask
Gateway
172.16.0.254
255.255.0.0
Add
Delete
DNS servers:
Search domains:
DHCP client ID:
Require IPv4 addressing for this connection to complete
Routes...
Available to all users
Cancel
Apply...

3.1.5 时区配置

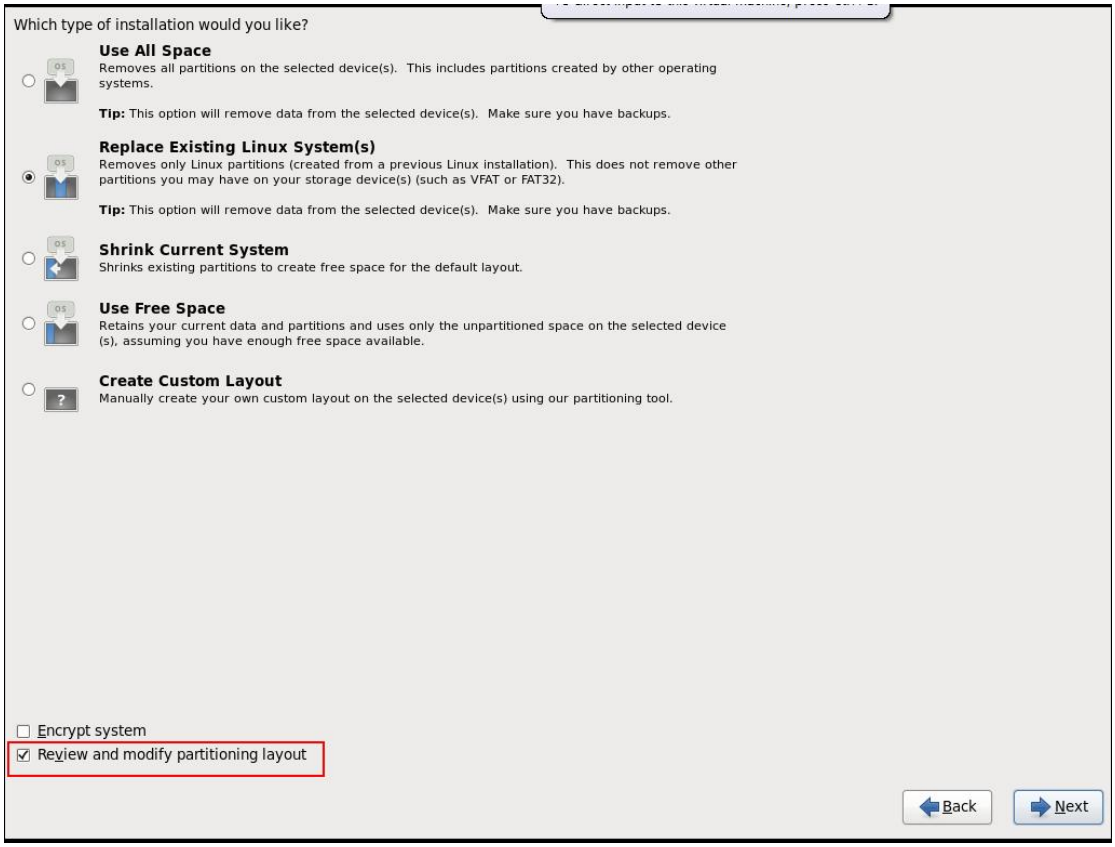
时区选择 Asia/Shanghai，并取消勾选“系统时钟使用 UTC 时间”，点击 Next。



3.1.6 ROOT 账户密码配置

设置 root 账户密码，并勾选 Review and modify partitioning layout，然后点击 Next 进入分区操作。


The root account is used for administering the system. Enter a password for the root user.
Root Password:
Confirm:
Back
Next

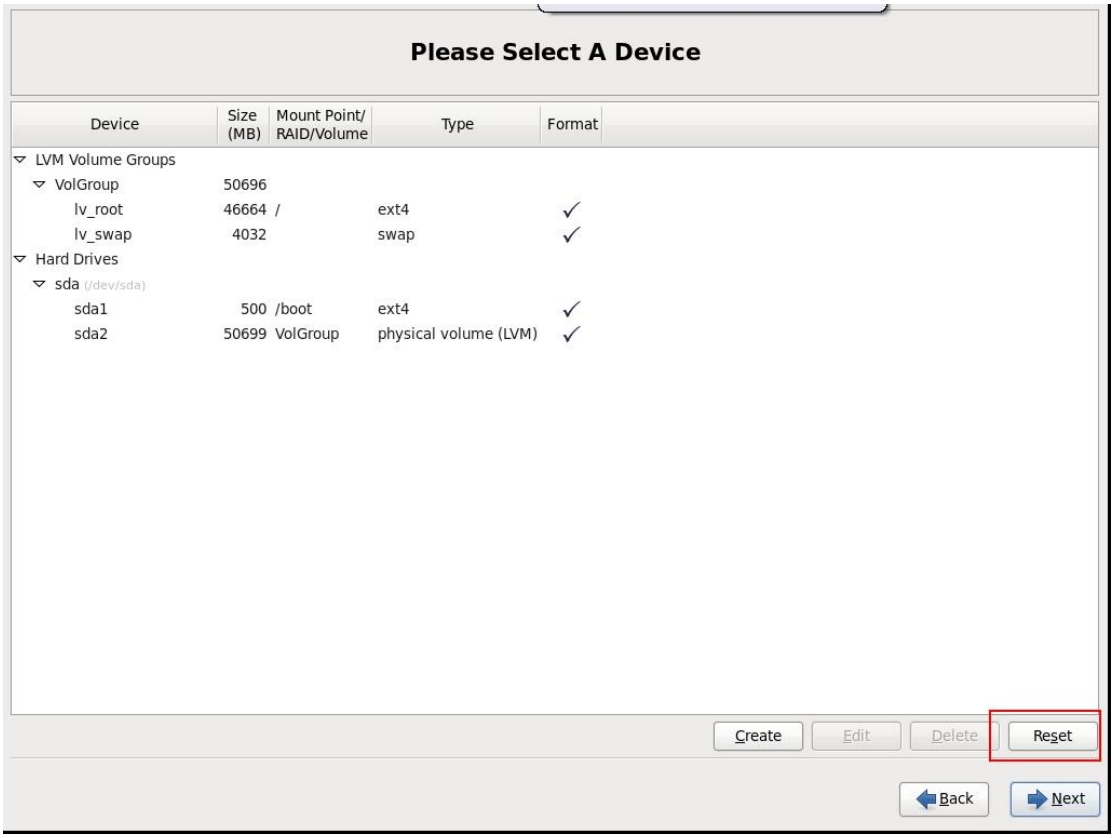

Which type of installation would you like?
Use All Space
Removes all partitions on the selected device(s). This includes partitions created by other operating systems.
Tip: This option will remove data from the selected device(s). Make sure you have backups.
Replace Existing Linux System(s)
Removes only 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
Back
Next

3.1.7 分区操作

首先确认系统硬盘数量，然后参照对应章节操作。

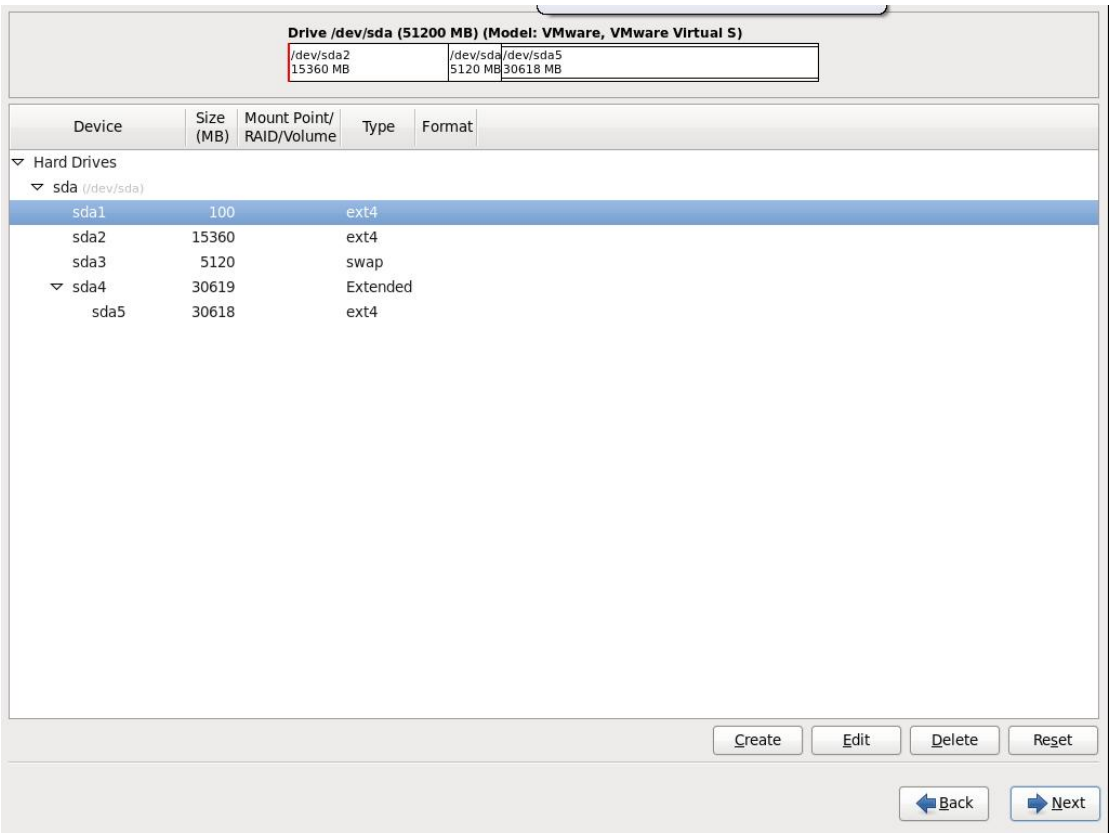
单盘分区操作

1. 硬盘已有分区，需先删除。点击 Reset 重置分区表。

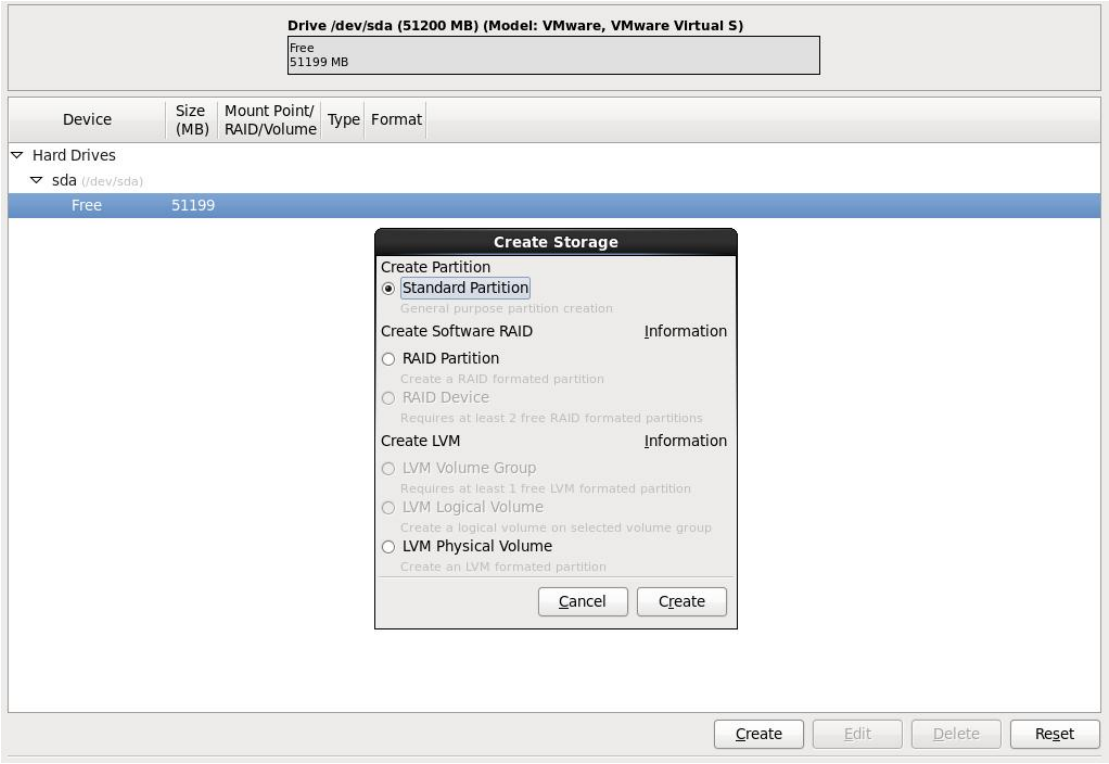


确认选择 Yes。

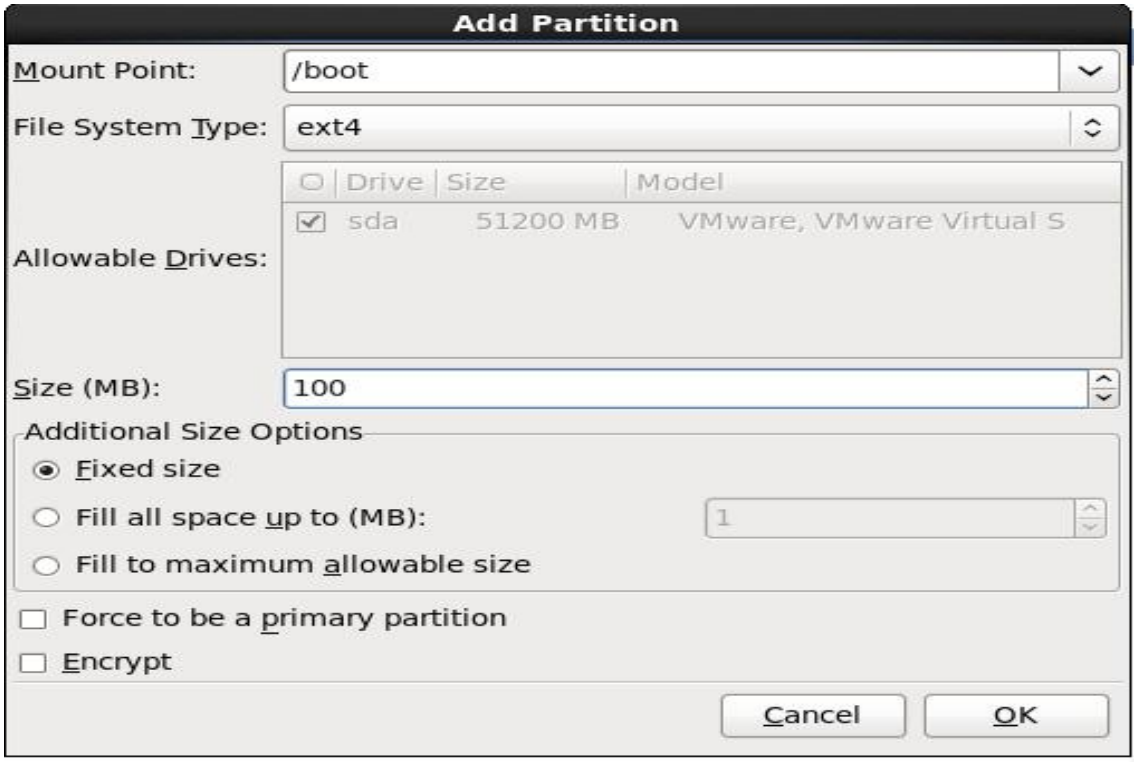
依次删除所有现有分区（如 sda1、sda2 等），直到磁盘状态显示为仅 /dev/sda 且为 Free。



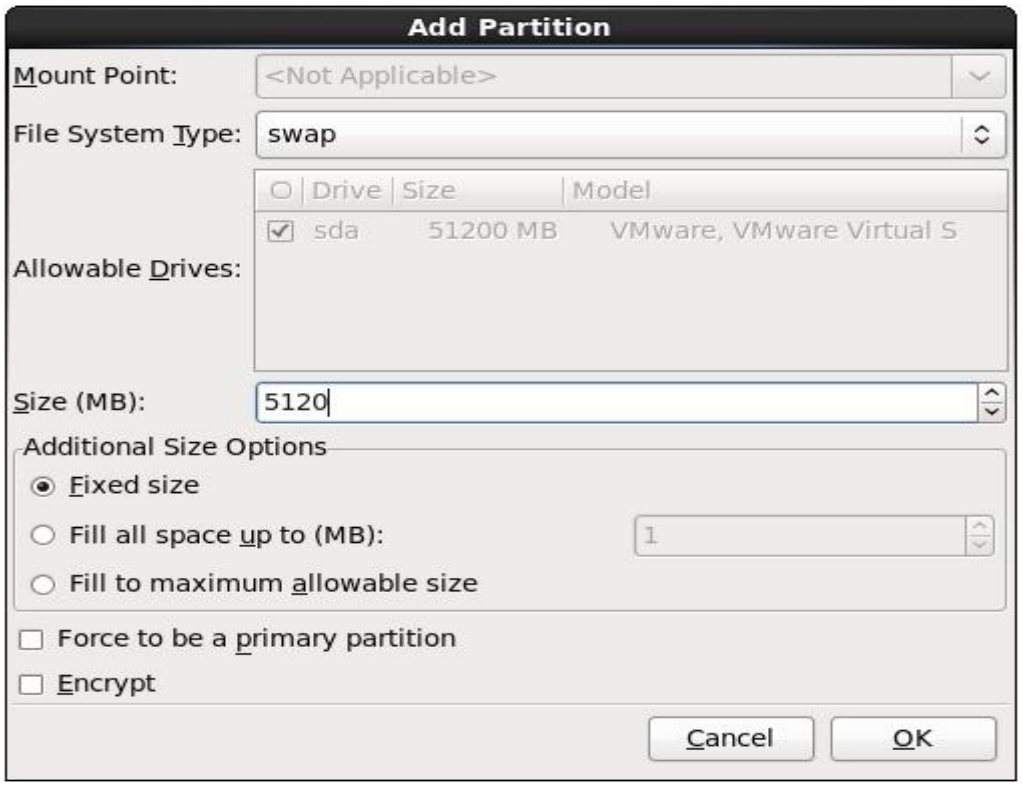
2. 选中空闲分区，点 create，选择 standard partition，再点 create



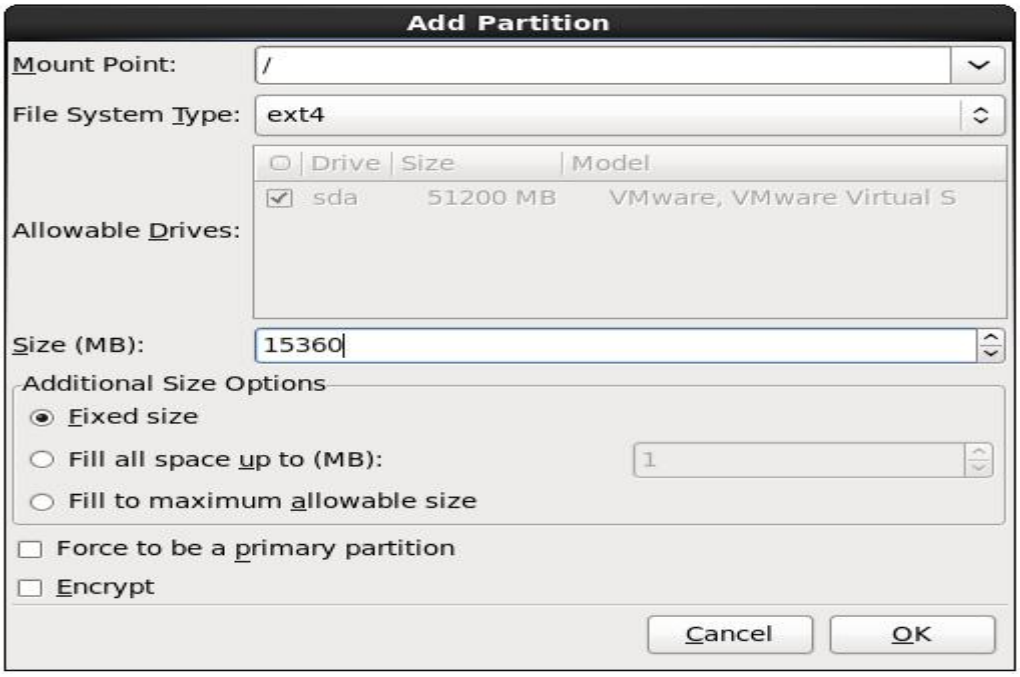
3. 在弹出的对话框中，挂载点填入 /boot，大小填 200 MB，点击 OK。



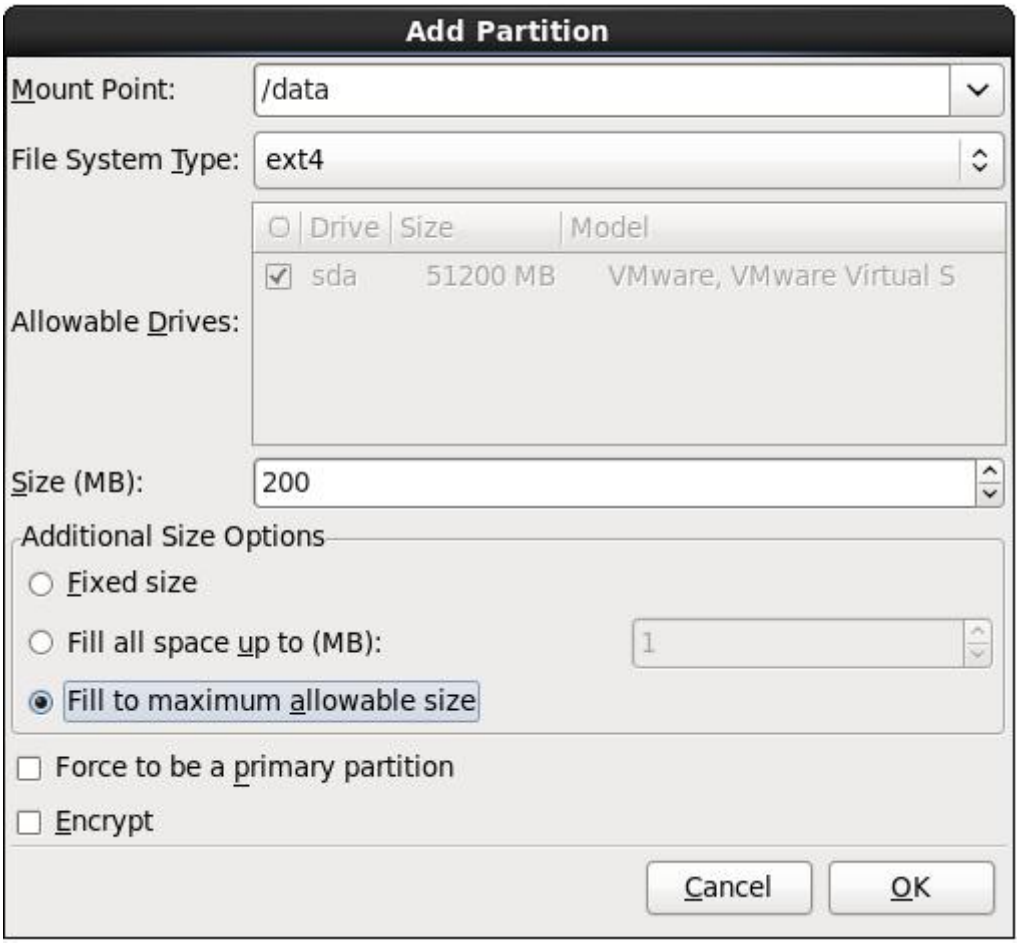
4. 再次点击 Create，文件系统类型选择 swap，大小设置为内存容量的 2 倍（例如内存 8GB，则 swap 设为 16384 MB），点击 OK。



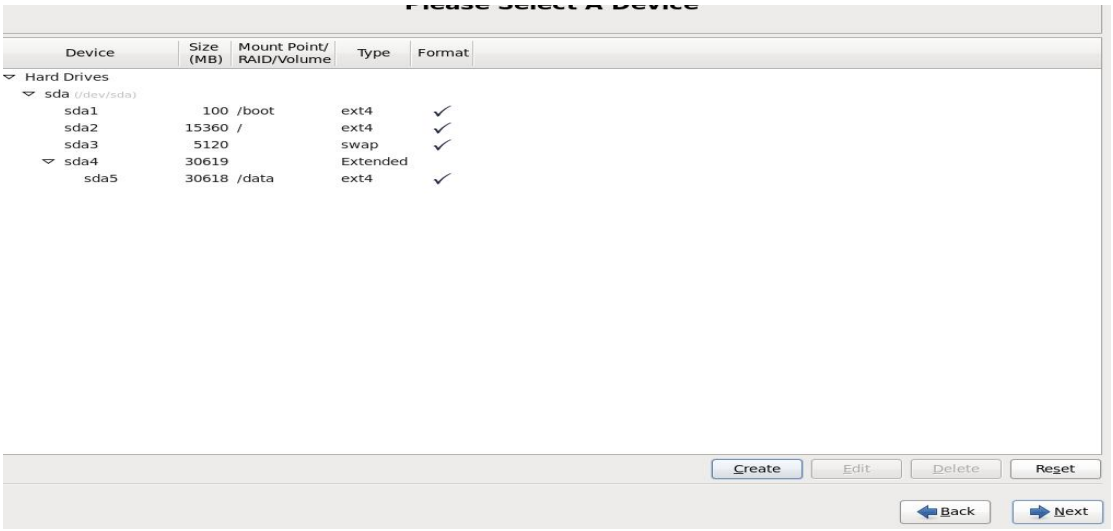
5. 再次点击 Create，挂载点填入 /，大小设为 15360 MB，点击 OK。



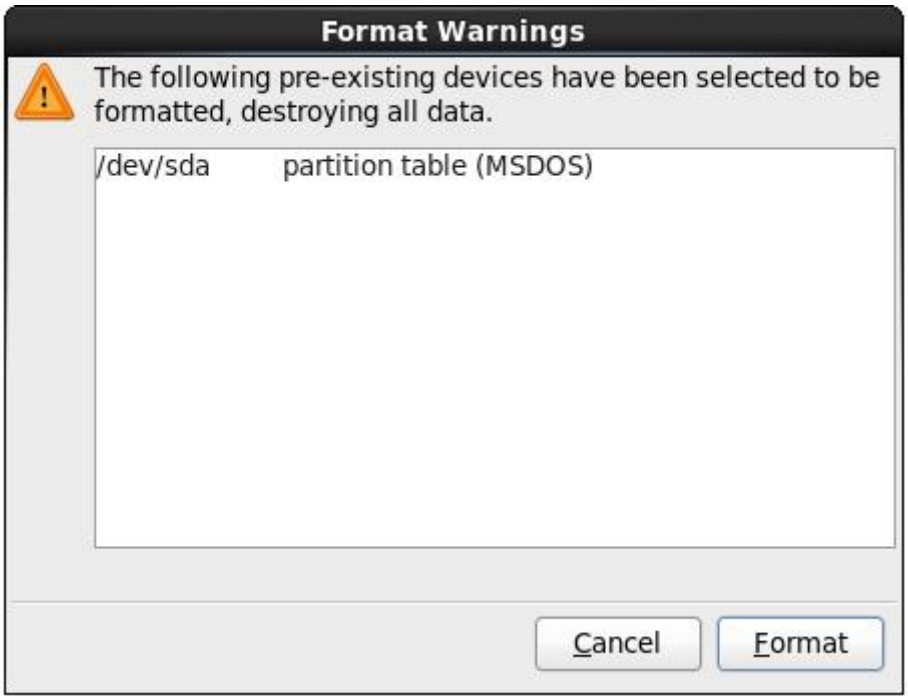
6. 最后点击 Create，挂载点填入 /data，将“Additional size options”设为 Fill to maximum allowable size，点击 OK。



7. 分区完成后点击 Next。

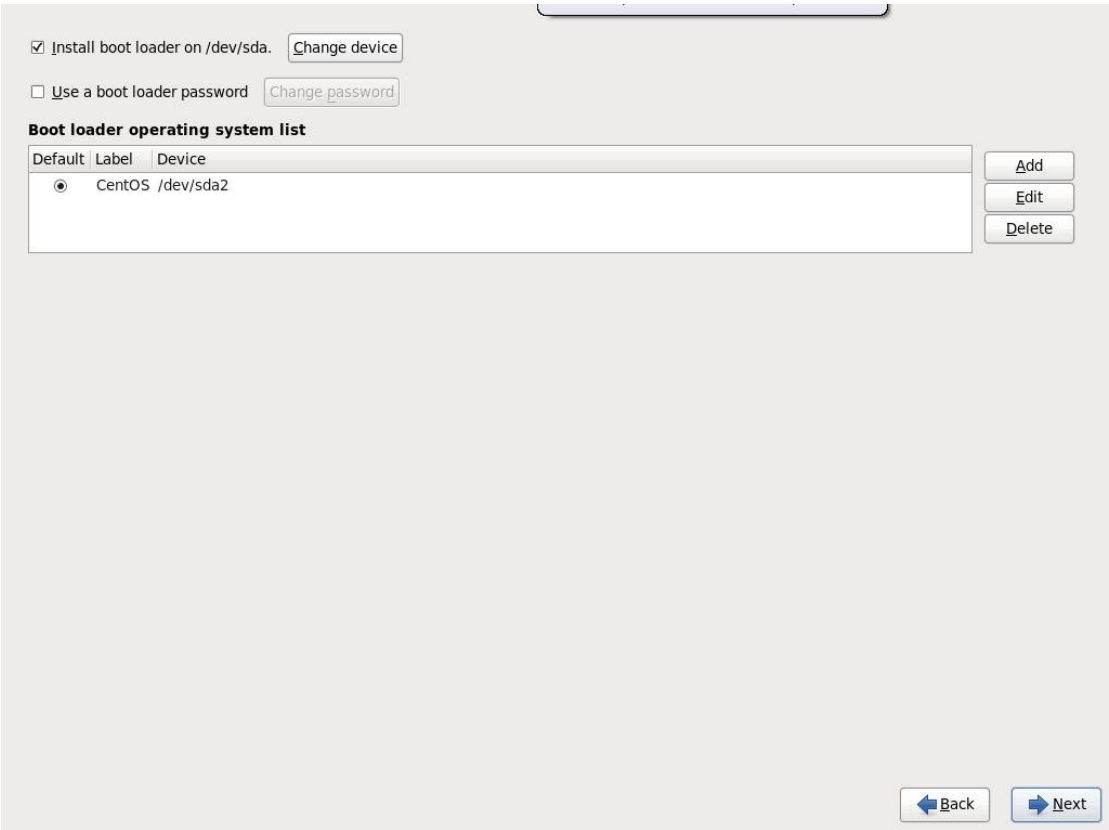


系统提示格式化，选择 format。



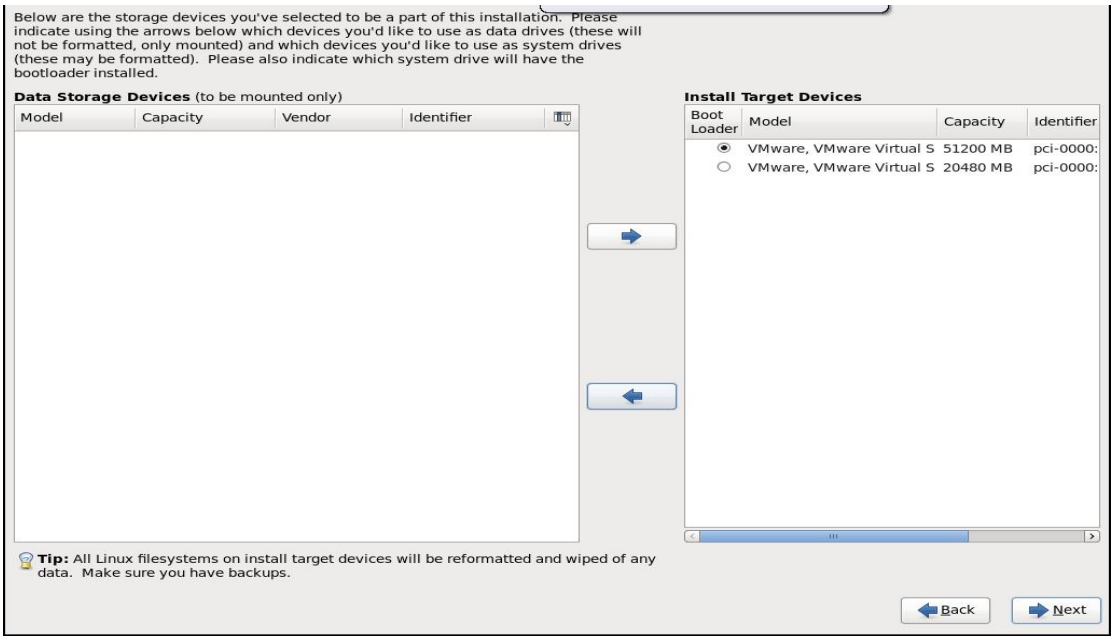
选择 Write changes to disk。

继续下一步。

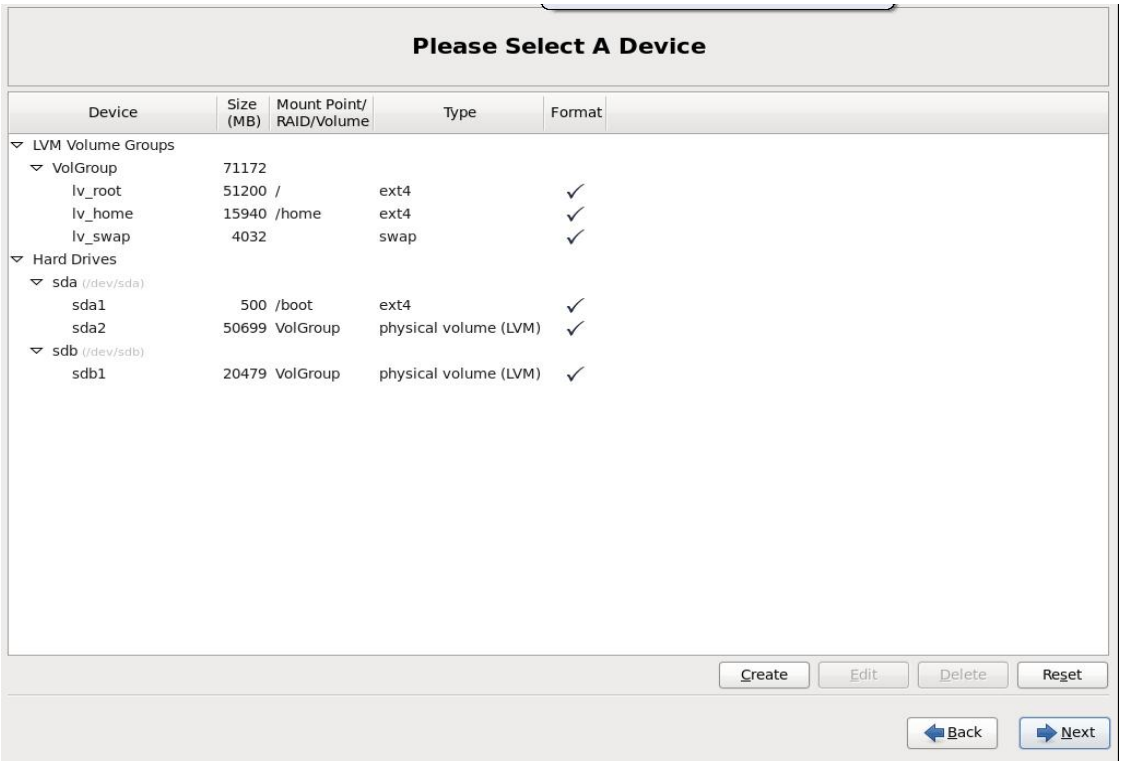


多盘分区操作

1. 将 Data Storage Devices 中的硬盘移至 Install Target Devices，点击 Next。

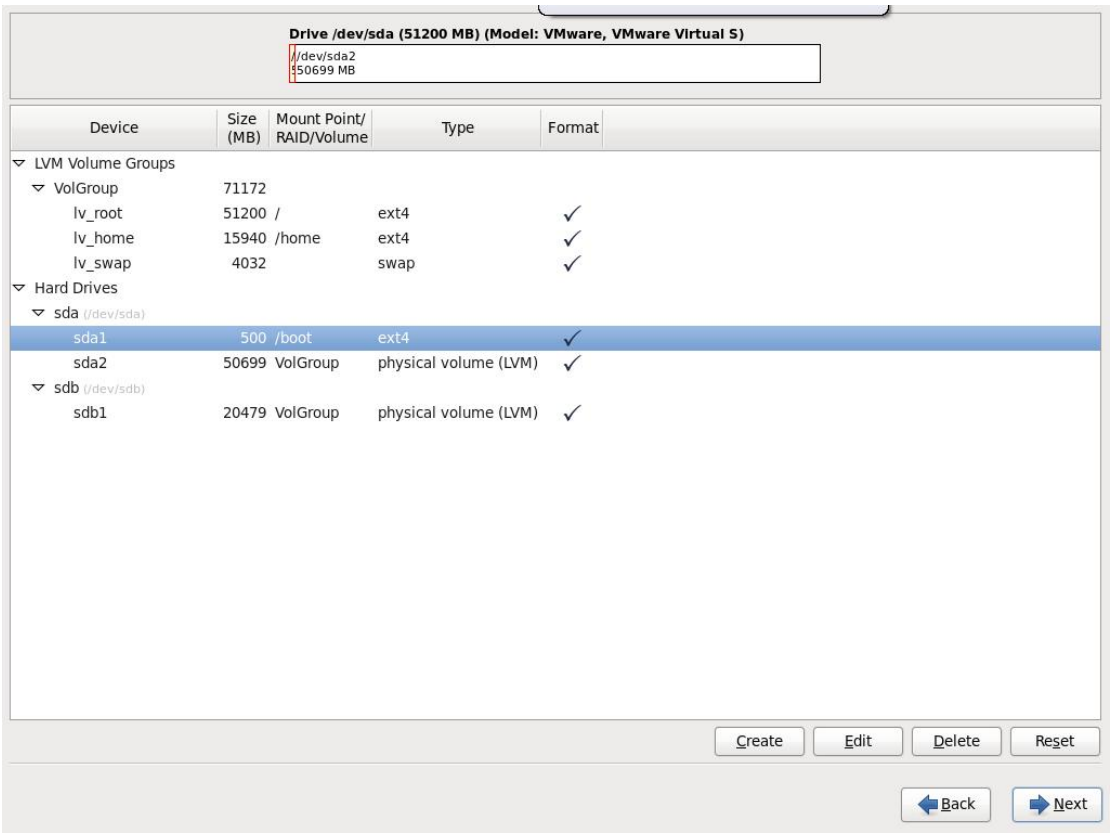


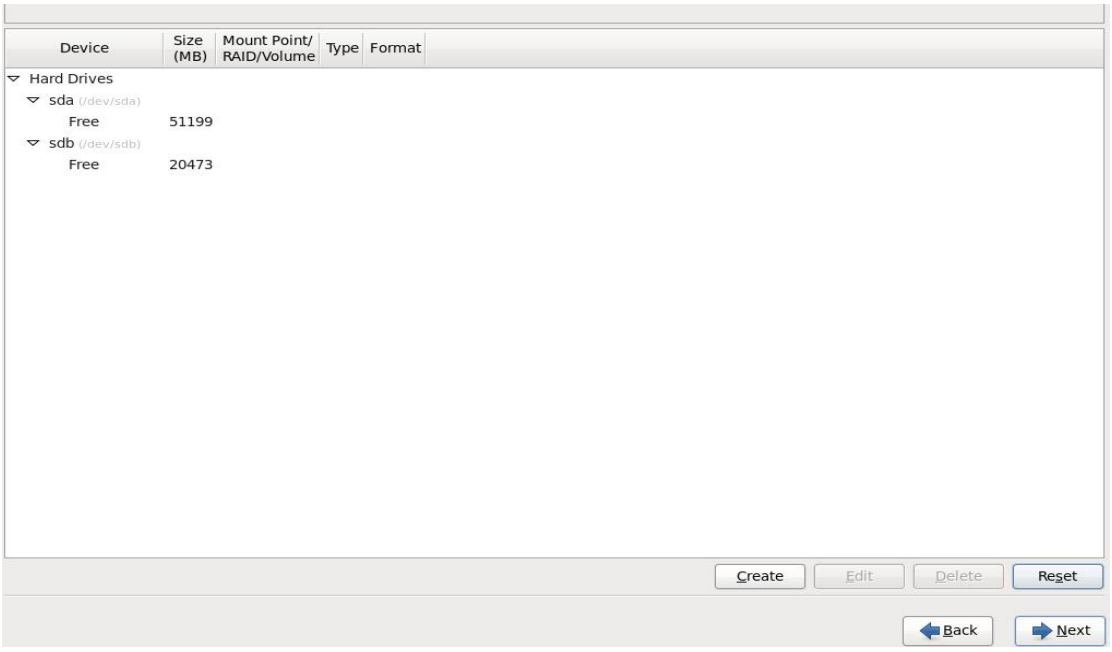
2. 点击 Reset 重置分区表。



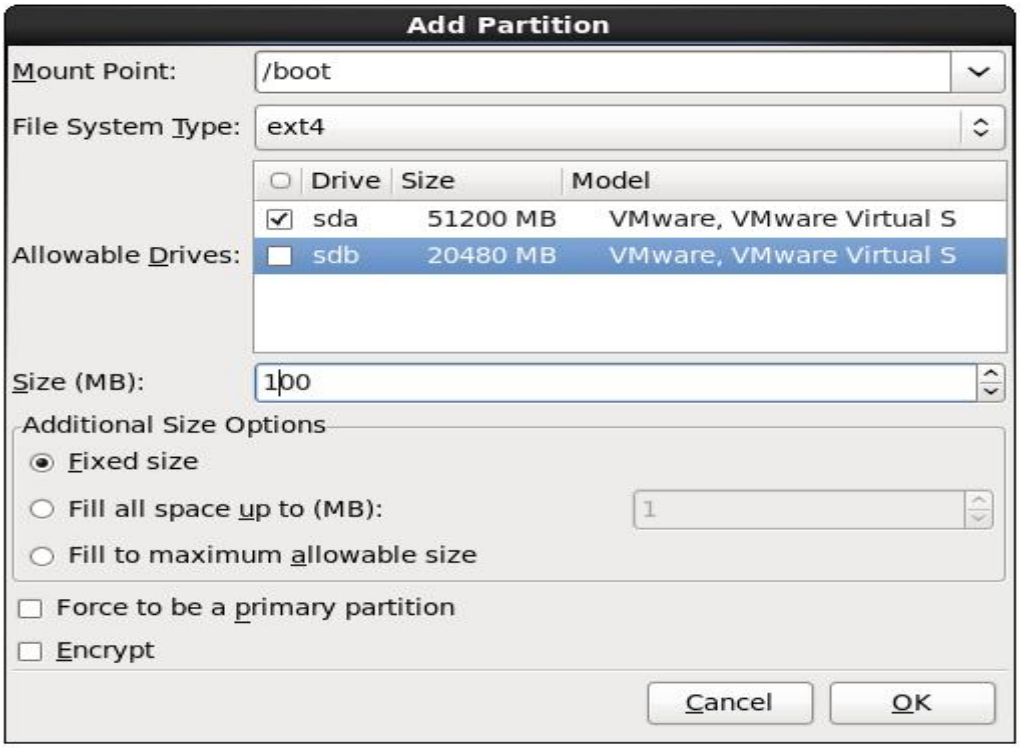
确认选择 yes。

删除所有现有分区，直到磁盘状态显示为仅 /dev/sda、/dev/sdb 且均为 Free。

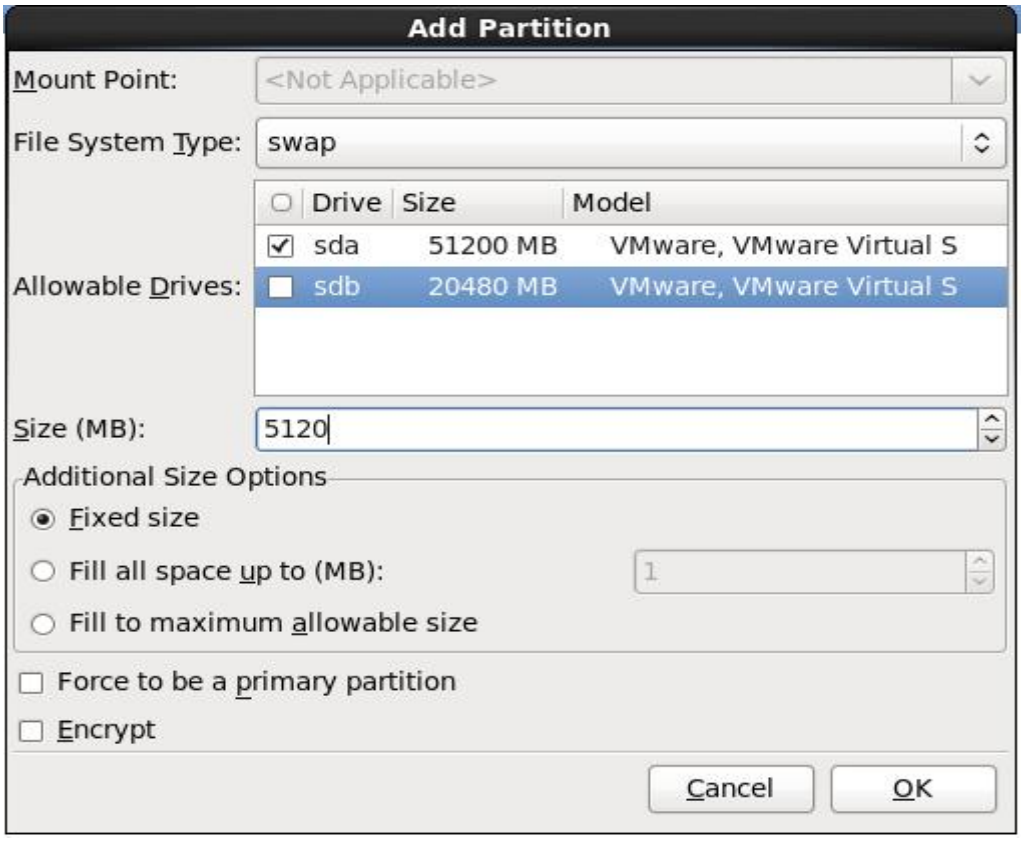




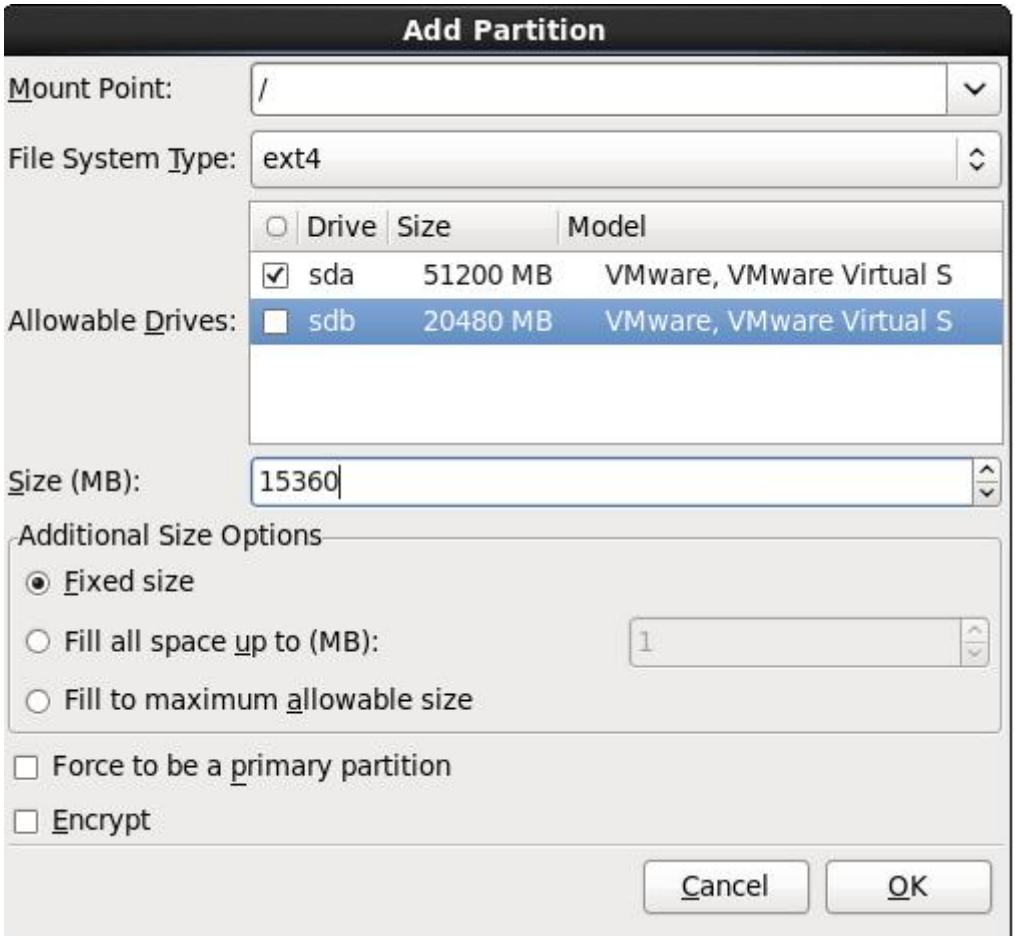
3. 点击 Create，选择 Standard Partition，再点 Create。挂载点填入 /boot，大小 200 MB，取消勾选 sdb 的允许驱动器，点击 OK。



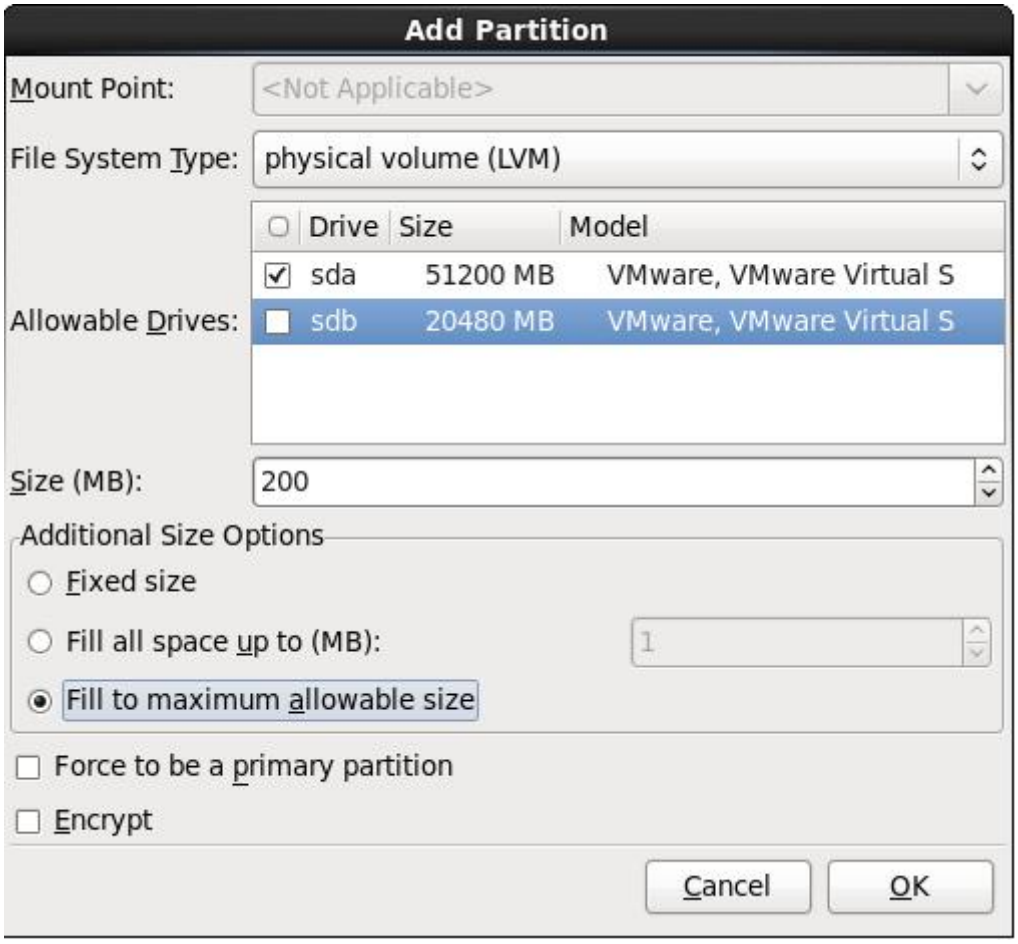
4. 再次点击 Create，文件系统类型选 swap，大小设为内存的 2 倍，取消勾选 sdb 的允许驱动器，点击 OK。



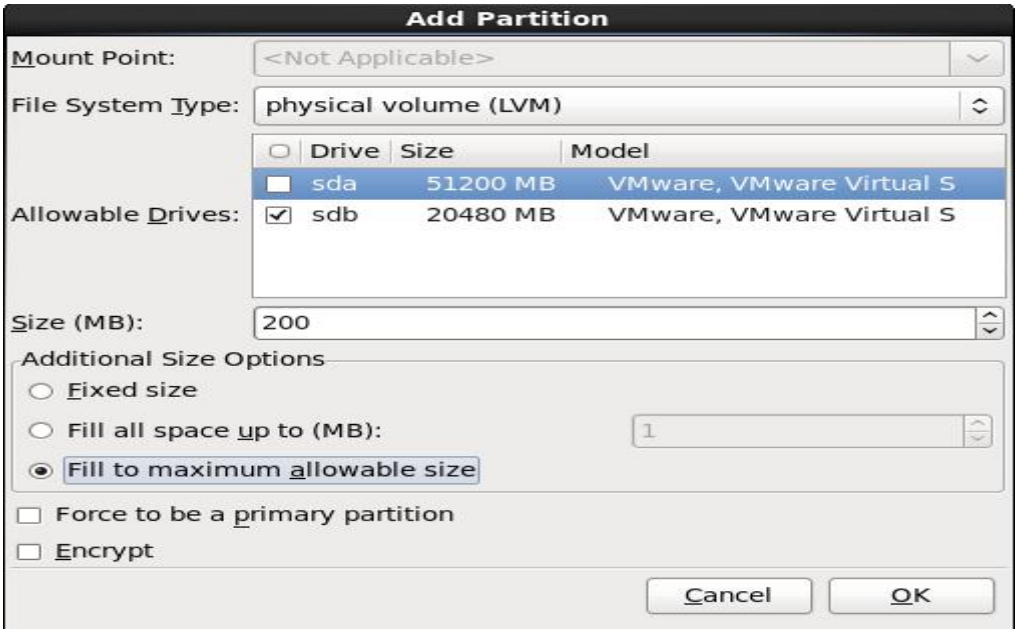
5. 再次点击 Create，挂载点填入 /，大小 15360 MB，取消勾选 sdb 的允许驱动器，点击 OK。



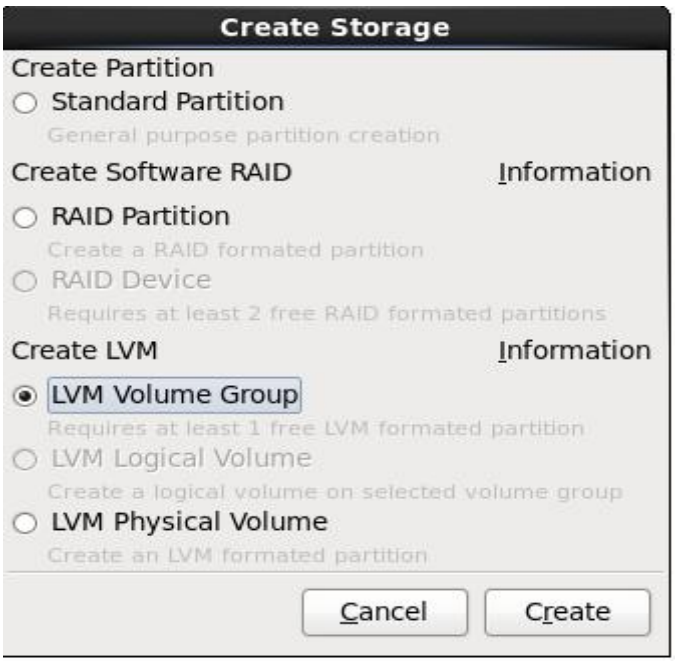
6. 点击 Create,文件系统类型选 physical volume (LVM),取消勾选 sdb 的允许驱动器，大小选 Fill to maximum allowable size，点击 OK。



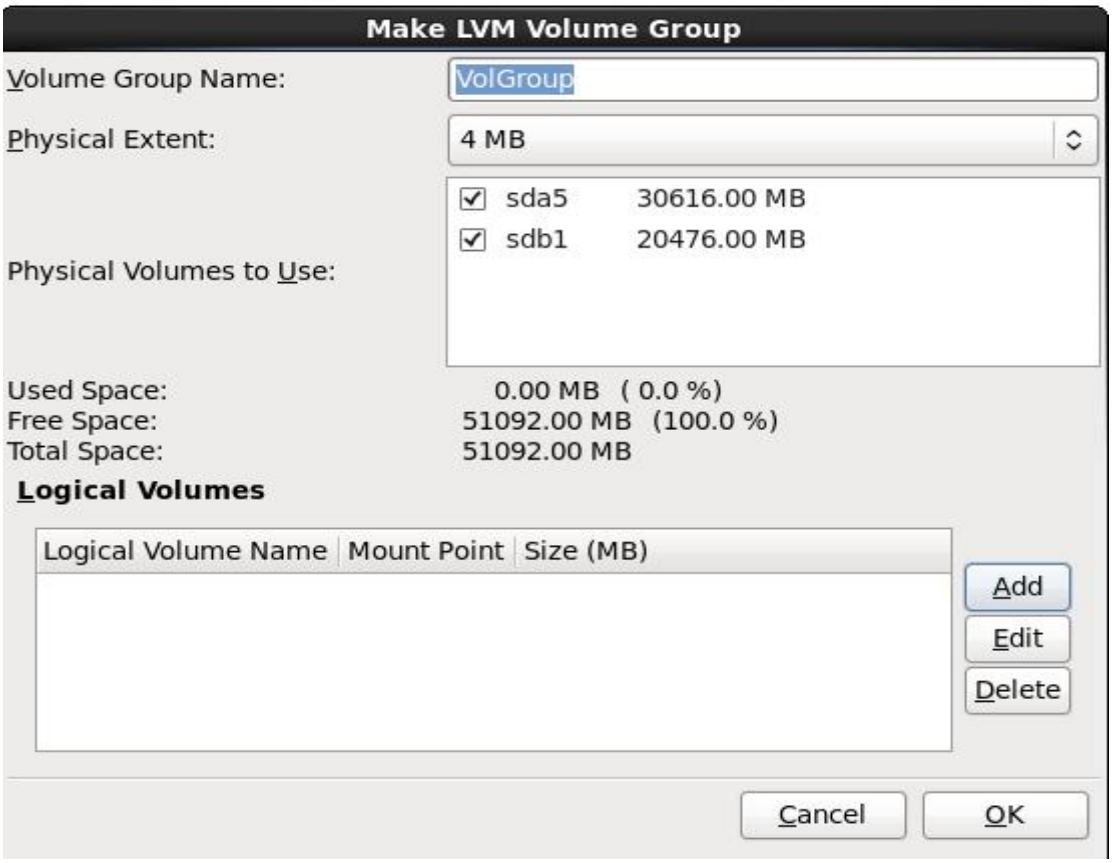
7. 同样操作，创建另一个 PV，取消勾选 sda 的允许驱动器，大小填满，点击 OK。



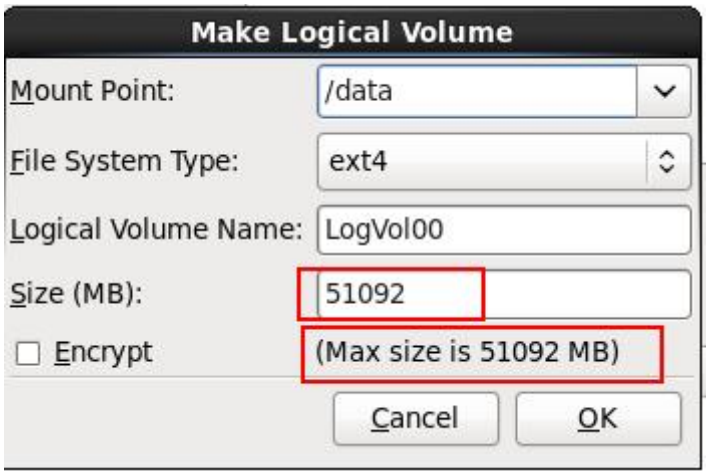
8. 最后点击 Create，选择 Create LVM，点击 Create。



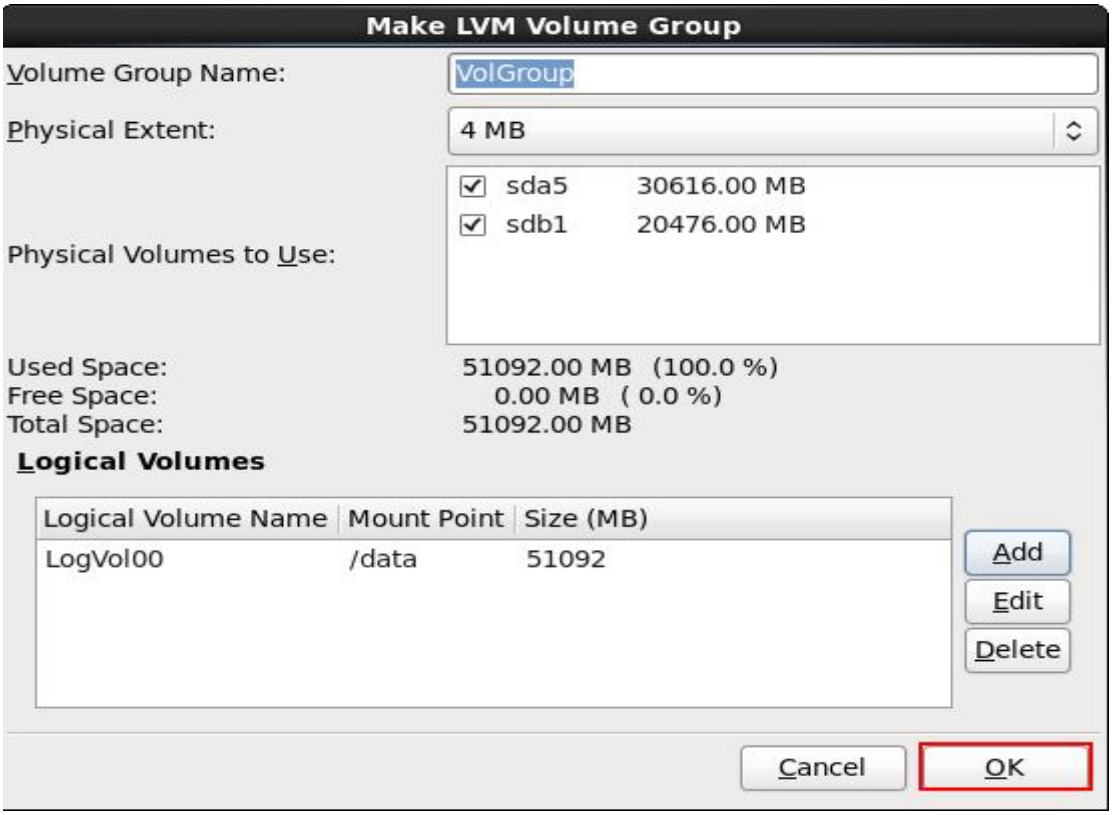
在 LVM 配置界面点击 Add。



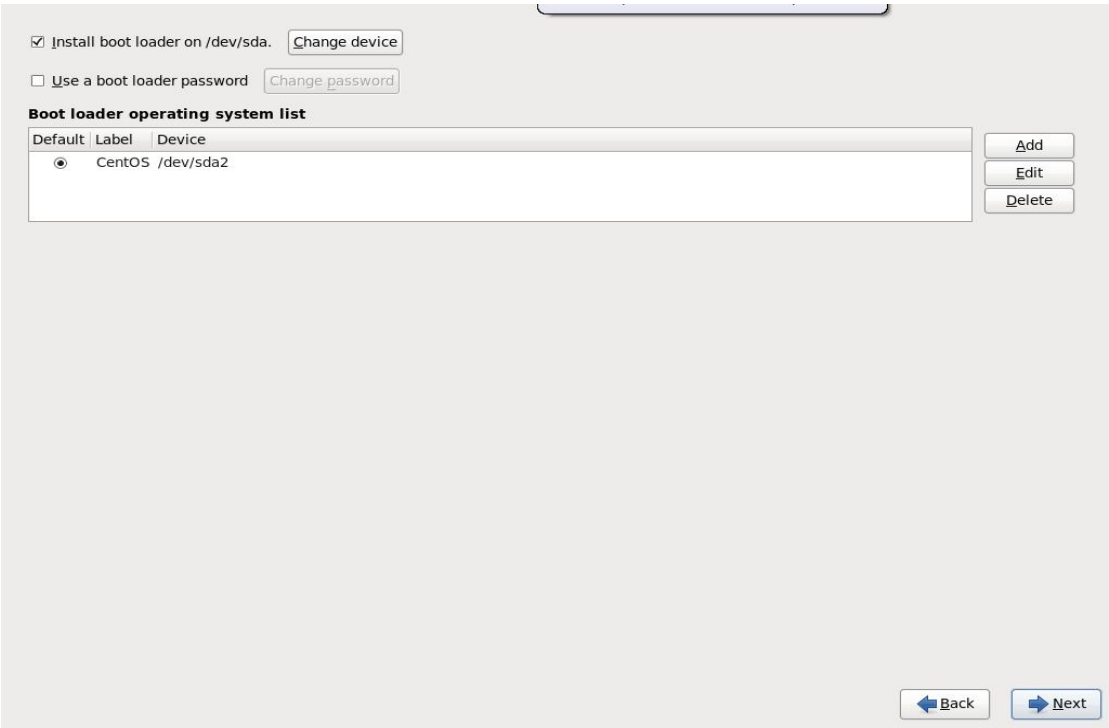
挂载点填入 /data，大小填入与提示的最大值一致，点击 OK。



点击 OK 完成分区。

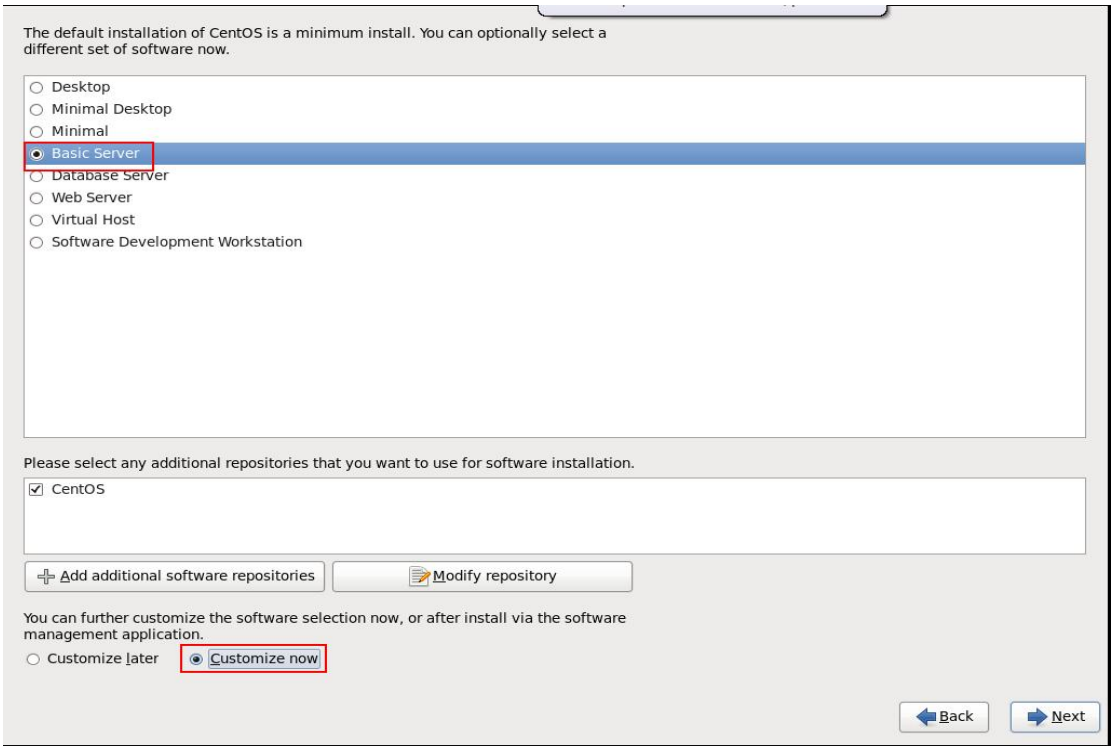


下一步。

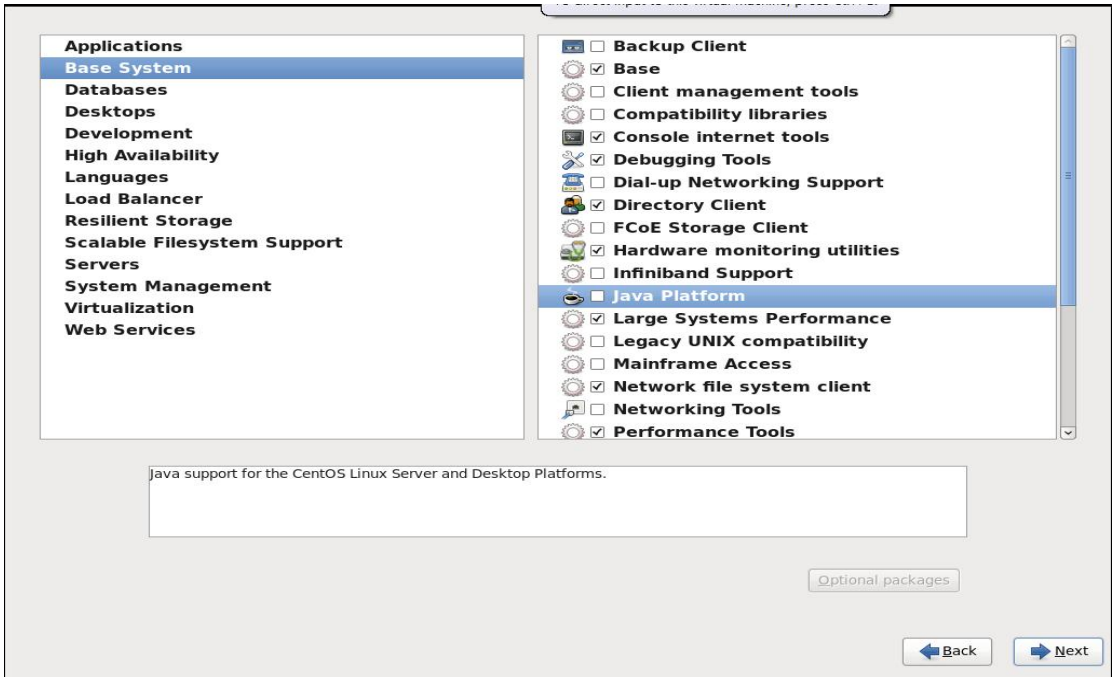


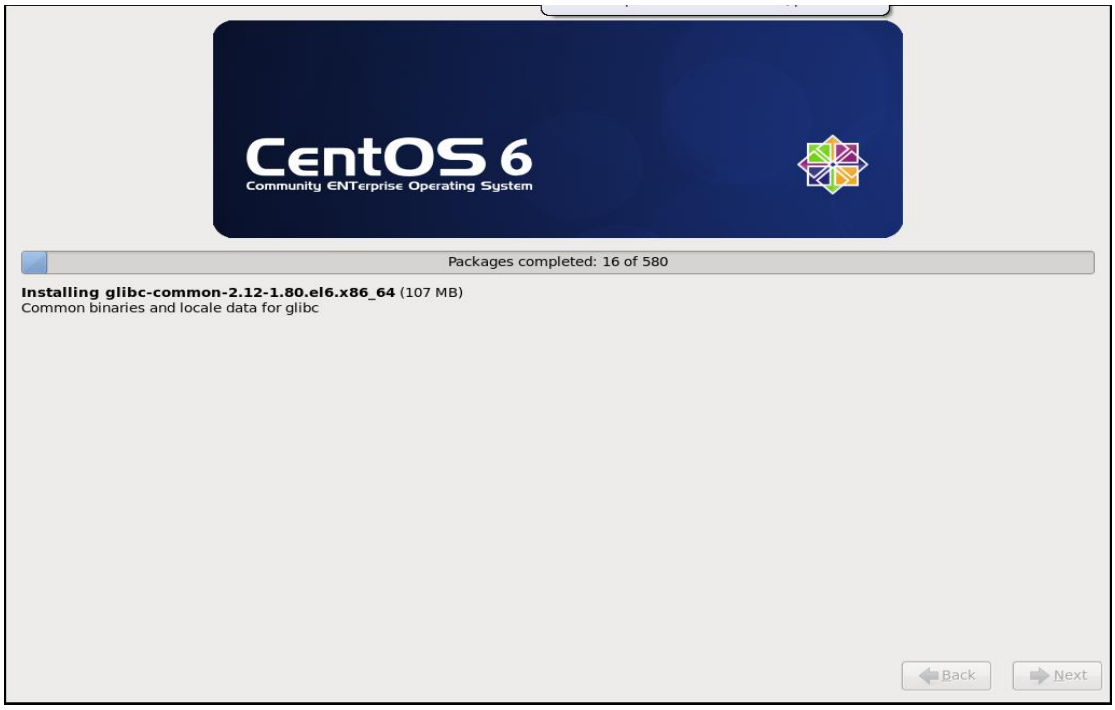
3.1.8 安装组件

进入组件选择界面，选择 Basic Server，再勾选 Customize now，点击 Next。

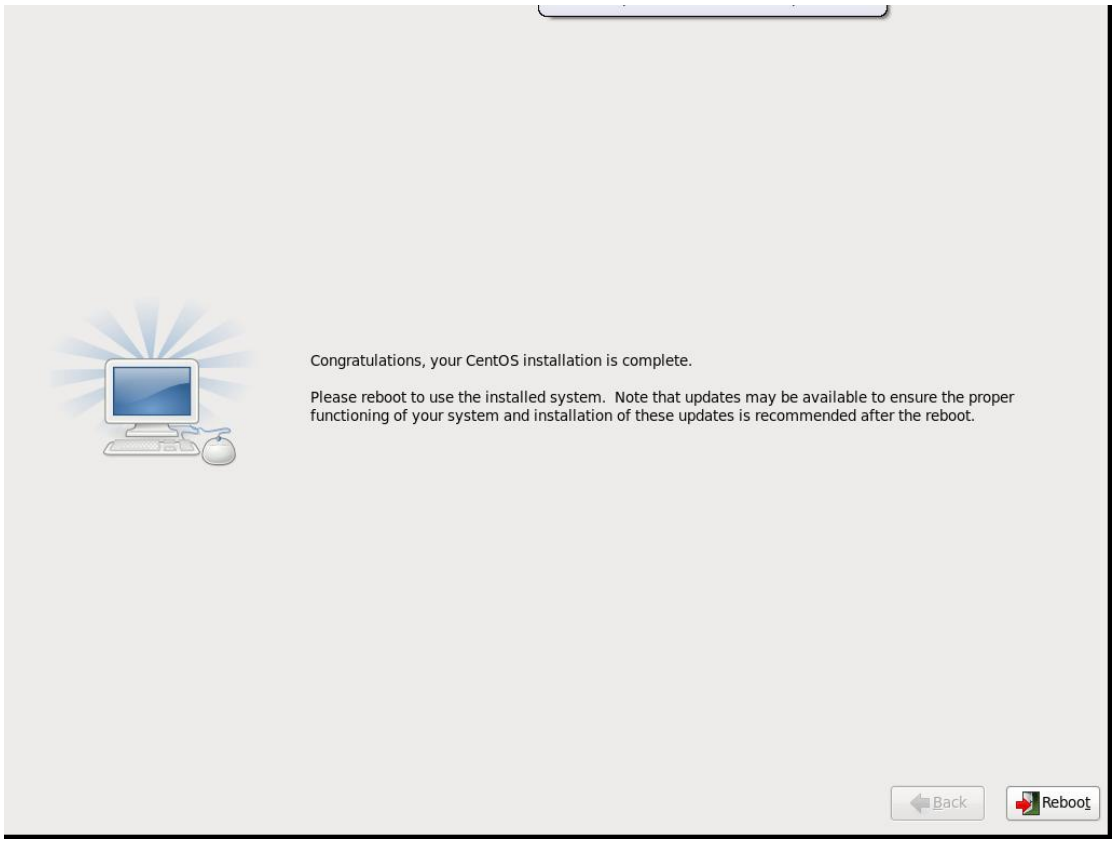


在 Base System 中，取消勾选 Java Platform，点击 Next。





安装完成后点击 Reboot 重启系统。



3.2 安装审计产品

使用 SSH 工具登录系统，上传獬豸日志安全审计系统安装包至 /root 目录，执行以下命令赋予执行权限并运行安装程序：

chmod +x xxx.bin

./xxx.bin

进入安装菜单：

[1] 安装全部

[2] 重启系统

[q] 退出

Please Input[1-2，q]，and Enter：

输入 1 并回车，开始安装。

安装过程中依次出现以下交互提示，请根据实际情况选择：

- 安装 rpm 依赖包：输入 y 开始安装，n 跳过。

```
Verifying archive integrity... All good.
Uncompressing RPM Install.............................
Sure you want to Install rpm? [y/n]?
```

- 安装 MySQL 数据库：首次安装输入 y；若保留原有数据库则输入 n。

```
Mysql has already installed, Sure you want to cover mysql? [y/n]?
```

- 安装数据处理相关程序：输入 y。

```
Sure you want to install esm-dbprocess package[Y/N]?
```

- 安装采集探针：输入 y。

```
Sure you want to install esm-probe package[Y/N]?
```

- 安装关联分析模块：输入 y。

```
Sure you want to install esm-analyzer package[Y/N]?
```

- 安装表现层和服务层模块：输入 y。

```
Sure you want to Install app? [y/n]?
```

- 安装知识库程序：输入 y。

```
Sure you want to install esm-KB package[Y/N]?
```

- 所有组件安装完成后，按回车键返回主菜单。

```
esm-KB install success!
--------
ESM Product Installation Completed!
Press any key and Enter to return
```

在主菜单输入 2 重启系统（安装完成后必须重启），或输入 q 退出。

注意：

- 安装完成后必须重启系统。
- 安装程序会自动将 SSH 端口修改为 2222。

```
==============================================
      ESM Product Install Main Menu
==============================================
[1] Install all
[2] Reboot system
[q] Quit
Please Input[1-2,q],and Enter:
```

3.3 卸载审计系统

在命令行执行卸载脚本：

uninstall-esm.sh

```
[root@localhost ~]# uninstall-esm.sh
Sure you want to Uninstall ESM Product[y/n]?
```

输入 y 确认卸载，n 退出。

依次出现以下交互提示：

- 卸载表现层和服务层模块：输入 y。

```
Sure you want to Uninstall app?[y/n]?
```

- 卸载关联分析模块：输入 y。

```
Sure you want to uninstall esm-analyzer[y/n]?
```

- 卸载采集探针：输入 y。

```
Sure you want to uninstall esm-probe[y/n]?
```

- 卸载数据处理相关：输入 y。

```
Sure you want to uninstall esm-dbprocess[y/n]?
```

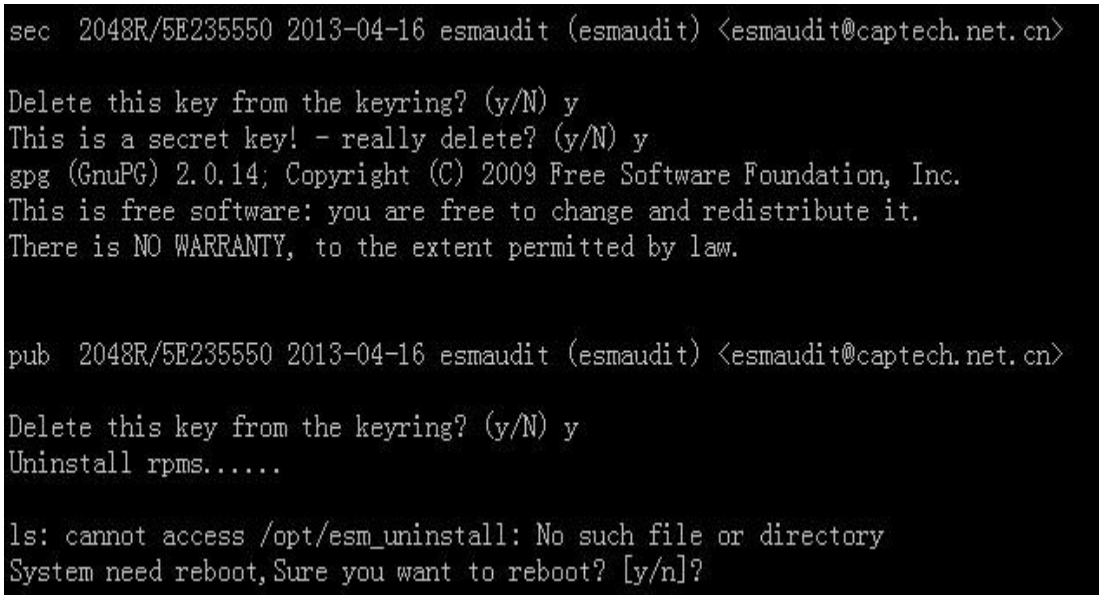
- 卸载知识库相关：输入 y。

```
Sure you want to uninstall esm-KB[y/n]?
```

- 卸载 rpm 依赖包：输入 y。

```
Sure you want to Unstall rpm?[y/n]?
```

- 删除授权文件：输入 y 删除，n 保留。



最后提示是否立即重启系统，选择 y 重启。

注意：从 sec 2048R... 开始的四个选项必须同时选择 y 或同时选择 n。卸载完成后必须重启服务器才能进行再次安装。