

# 毕方数据库安全审计系统

安装卸载手册



北京携推信息技术有限公司

2019年12月

## 声明

1. **信息变更：**本文档所含信息仅供参考，如有更新，恕不另行通知。如需了解最新信息，请咨询北京携推信息技术有限公司或访问官方网站。
2. **性能差异：**文中所描述的产品功能、性能及规格可能因具体型号、应用环境和配置方法的不同而有所差异，此为正常现象。
3. **版权声明：**本文档及相关内容受版权保护，未经北京携推信息技术有限公司书面许可，任何单位或个人不得以任何形式复制或传播本文档的任何部分。
4. **适用对象：**本手册主要面向毕方数据库审计系统的最终用户及安装维护人员。

**权利归属：**与本文档内容相关的权利归北京携推信息技术有限公司所有。文档将定期更新，最新版本请访问：[www.xie-tui.com](http://www.xie-tui.com)

## 目 录

1 安装环境与配置要求 .....	4
2 自动安装 .....	5
2.1 修改 BIOS 启动顺序 .....	5
2.2 执行自动安装 .....	6
3 手动安装 .....	11
3.1 操作系统安装 .....	11
3.1.1 语言、键盘设置 .....	13
3.1.2 存储设备配置 .....	14
3.1.3 计算机名配置 .....	15
3.1.4 网络配置 .....	15
3.1.5 时区配置 .....	17
3.1.6 root 账户密码配置 .....	18
3.1.7 分区操作 .....	19
3.1.8 软件包安装 .....	38
3.2 安装审计产品 .....	40
4 卸载 .....	42
4.1 卸载探针 .....	42
4.2 卸载审计中心 .....	42

# 1 安装环境与配置要求

为确保毕方数据库安全审计系统的顺利安装与稳定运行，请确保硬件环境满足以下要求：

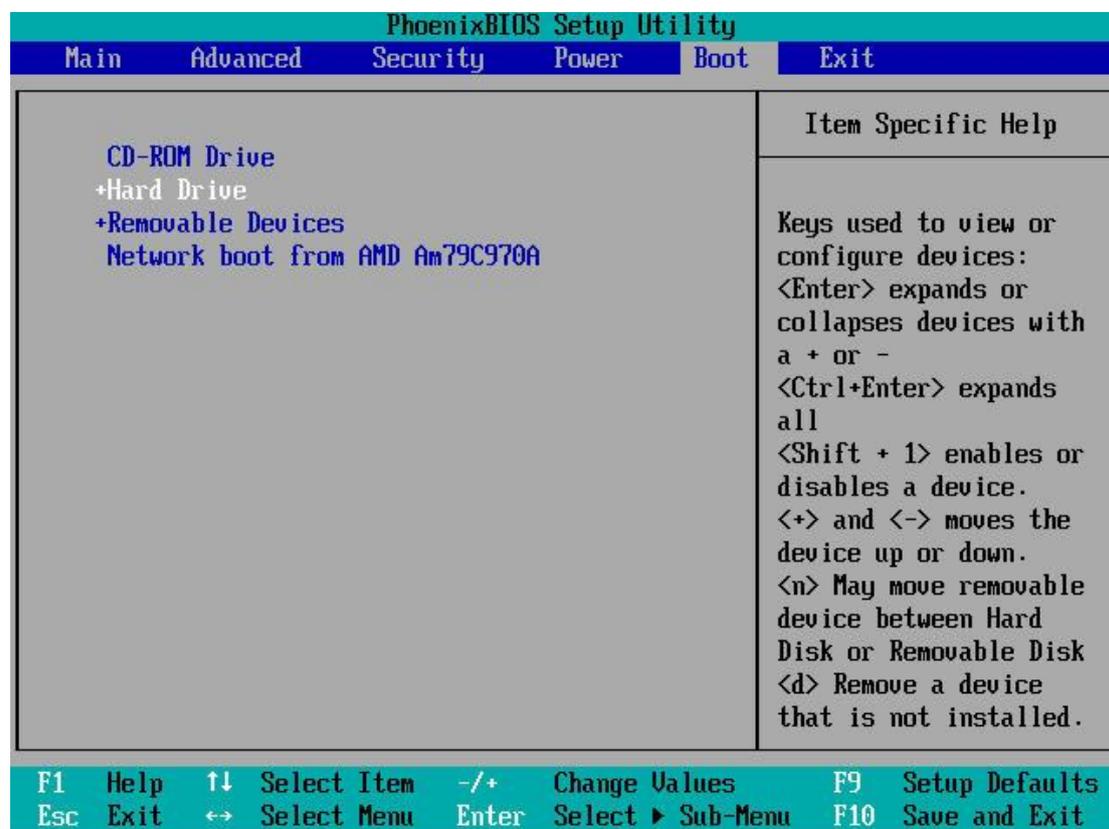
- **硬件平台：**推荐使用 Intel Xeon 系列处理器。
- **最低配置：**内存 (RAM) 8GB, 硬盘 (HD) 50GB, 网络端口 3 个。
- **安装准备：**安装过程中，设备必须连接显示器、键盘，并配有光驱。
- **系统环境：**毕方审计系统基于 CentOS 运行。
  - ◇ **自动安装：**安装光盘已针对标准环境定制，但不保证在所有硬件上均能成功安装。请确认您的硬件驱动可被 CentOS 6.9 64 位系统识别，且安装后网卡设备名识别为 ifcfg-ethx 格式。
  - ◇ **手动安装：**对于部分品牌服务器（如 DELL），网卡名称可能被识别为 emx 格式，此时推荐使用手动安装方式。手动安装必须确保操作系统至少有一个可用的 ifcfg-eth0 网口。

## 2 自动安装

本章节介绍如何使用安装光盘进行全自动安装。系统将自动安装 CentOS 6.9 及毕方审计产品。

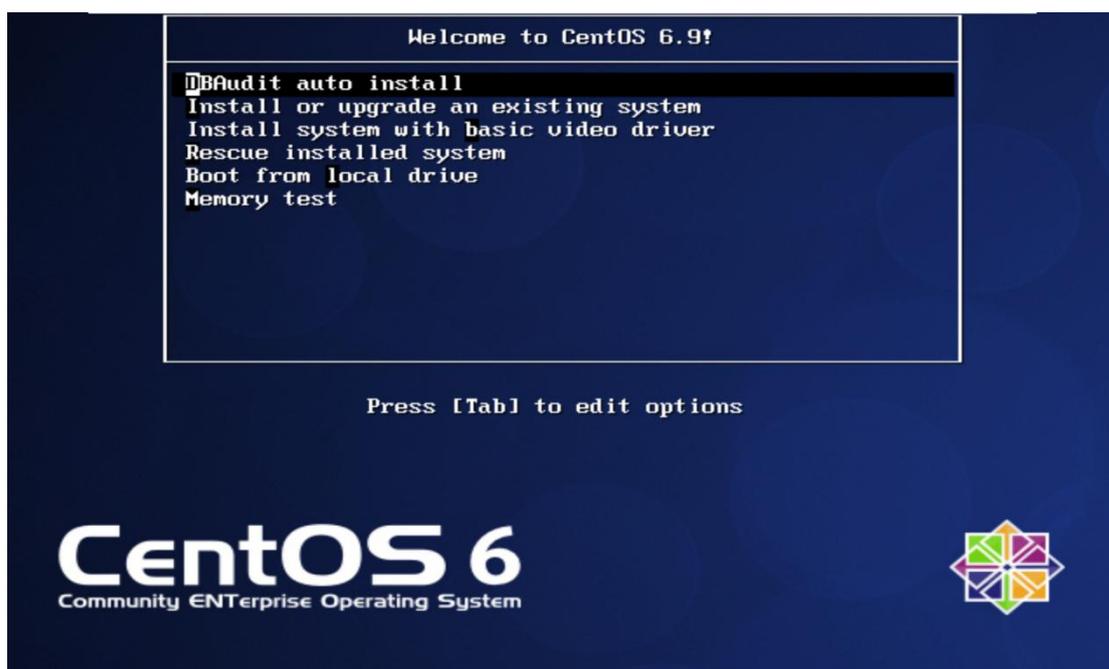
### 2.1 修改 BIOS 启动顺序

- 1 启动服务器，进入 BIOS 设置界面。
- 2 将 第一启动设备 设置为光驱 (CD/DVD-ROM)。不同品牌服务器 BIOS 界面不同，请参考下图示例。



## 2.2 执行自动安装

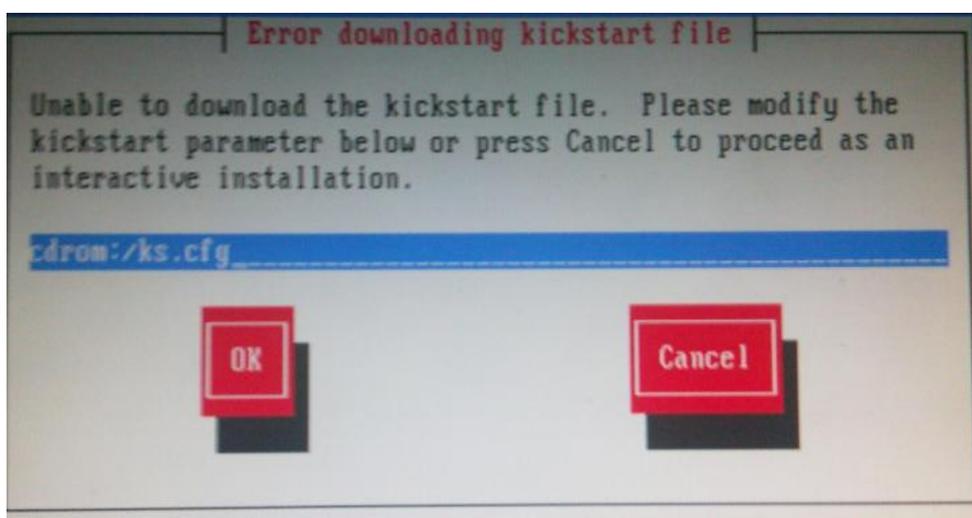
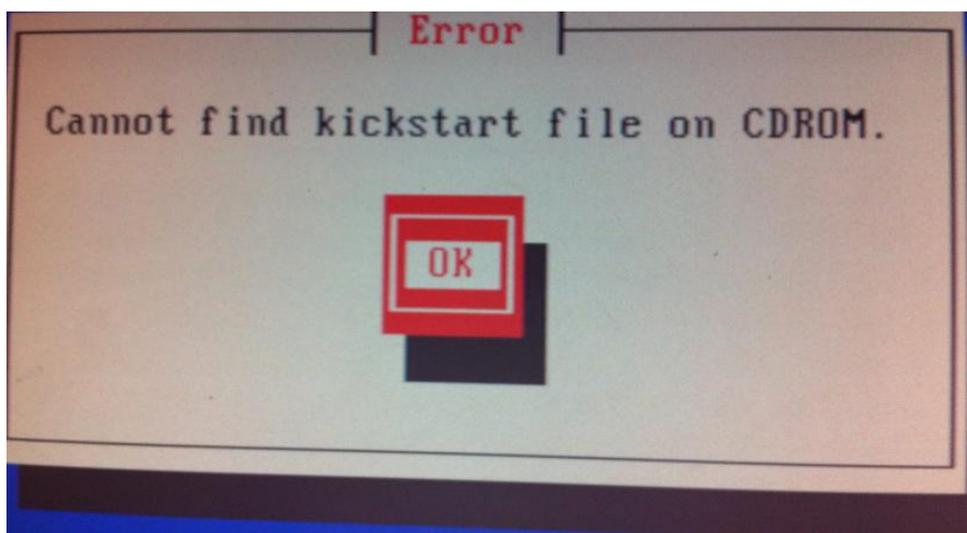
- 1 将安装光盘放入光驱，保存 BIOS 设置并重启。
- 2 系统从光盘启动后，出现安装选项界面。通过上下键选择 NuoLi u audit auto Install，然后按回车键确认。



- 3 系统将开始自动化安装流程。在此过程中，可能会遇到以下几种特殊情况，请根据提示操作：

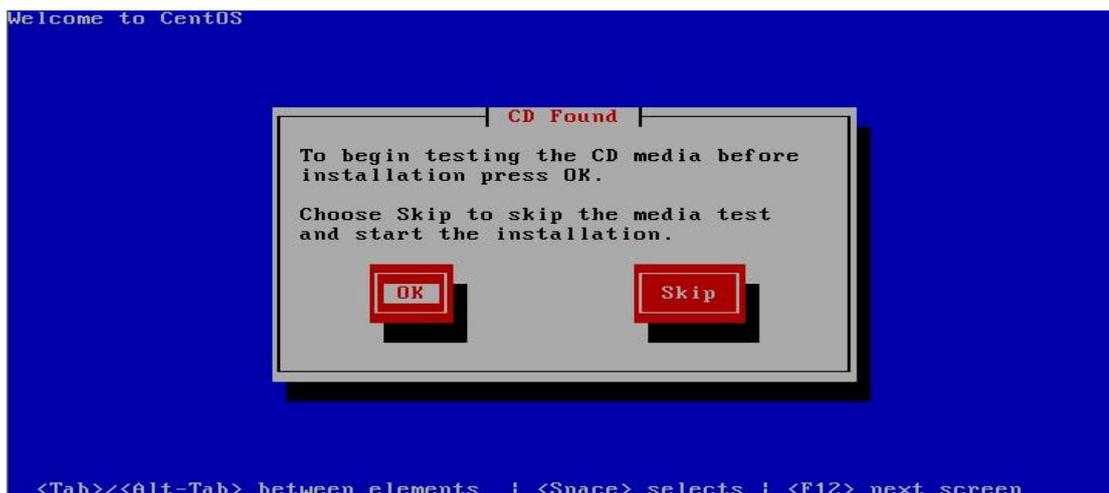
- 情况 1：硬盘数据确认

如果出现如下图所示提示，直接按 OK 继续，并在后续提示中按两次回车键即可。



- 情况 2: 光盘介质检查

如果提示是否检查安装光盘, 请使用 `Tab` 键选择 `Skip` 并回车, 以跳过检查, 加快安装速度。



- 情况 3: 硬盘格式化确认

如果出现如下提示，表示需要对硬盘进行格式化，请选择 Yes 确认。

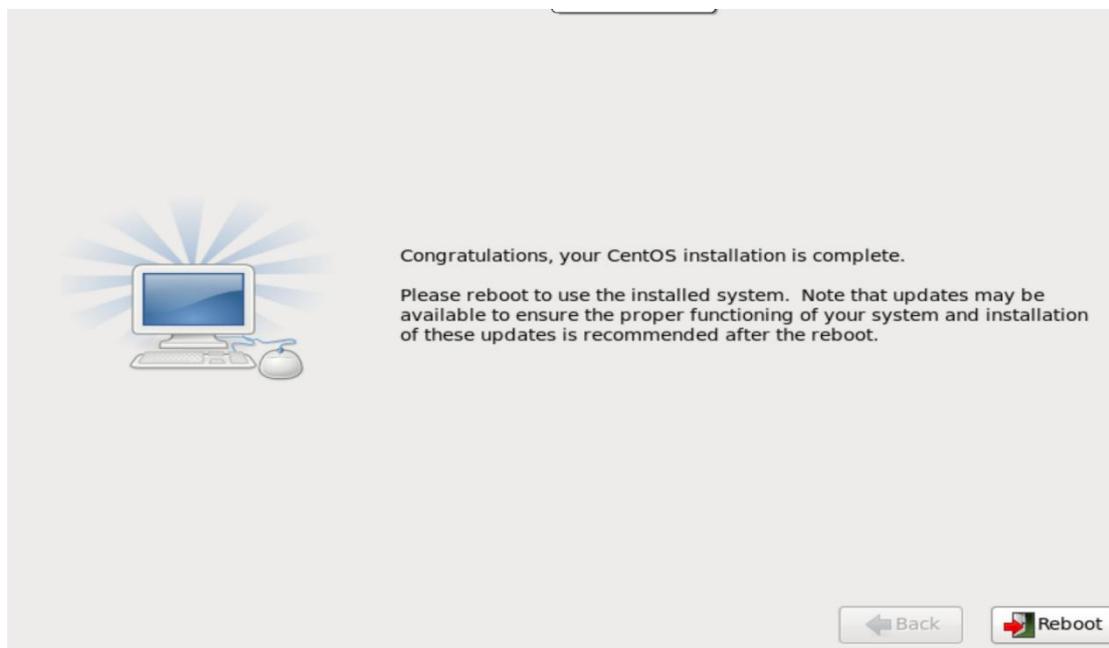


- 情况 4: 存储设备数据警告

如果检测到存储设备上存在已有数据，提示警告信息，请选择 Yes, discard any data 以继续安装。



- 若无特殊情况，系统将自动完成操作系统的安装。安装完成后会自动重启，此时请务必取出安装光盘。



- 重启后，系统将自动继续安装毕方审计系统核心程序，请耐心等待，界面如下图所示。



- 6 安装过程全部完成后，系统将再次自动重启。当屏幕出现 Login: 提示符时，表示安装已全部完成。

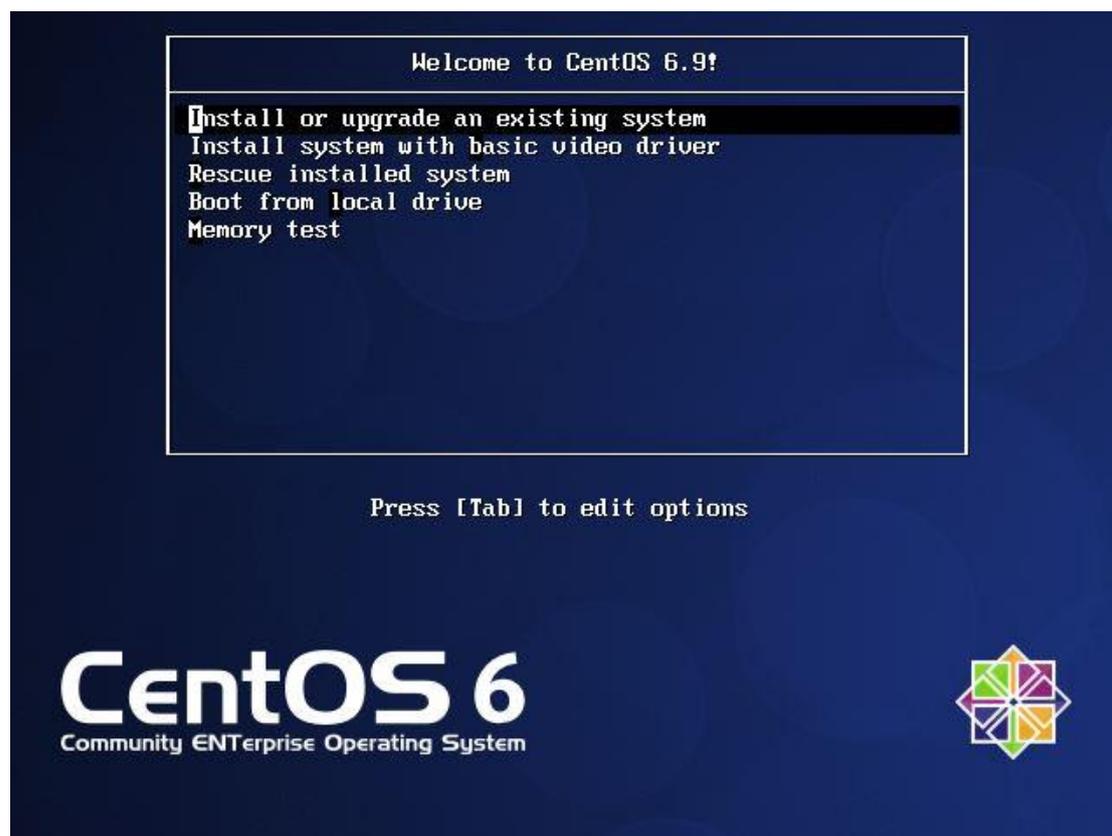
```
CentOS release 6.9 (Final)
Kernel 2.6.32-754.30.2.el6.x86_64 on an x86_64
dbaudit login: _
```

## 3 手动安装

手动安装分为两个阶段：首先安装 CentOS 6.9 x64 操作系统，然后再安装毕方审计系统程序。

### 3.1 操作系统安装

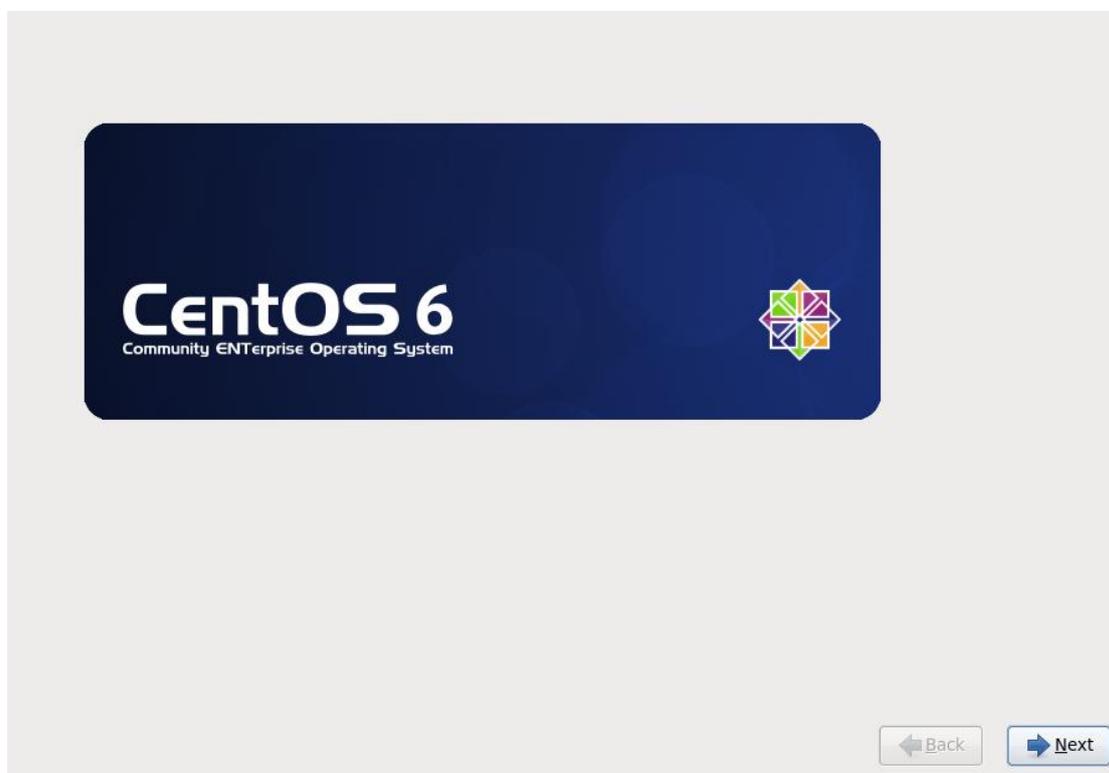
- 1 光盘启动后出现安装选择，选择 Install or upgrade an existing system 回车，或等待 60 秒后自动进入。



2 出现是否对 CD 媒体进行测试的提问，这里选择“Skip”跳过测试



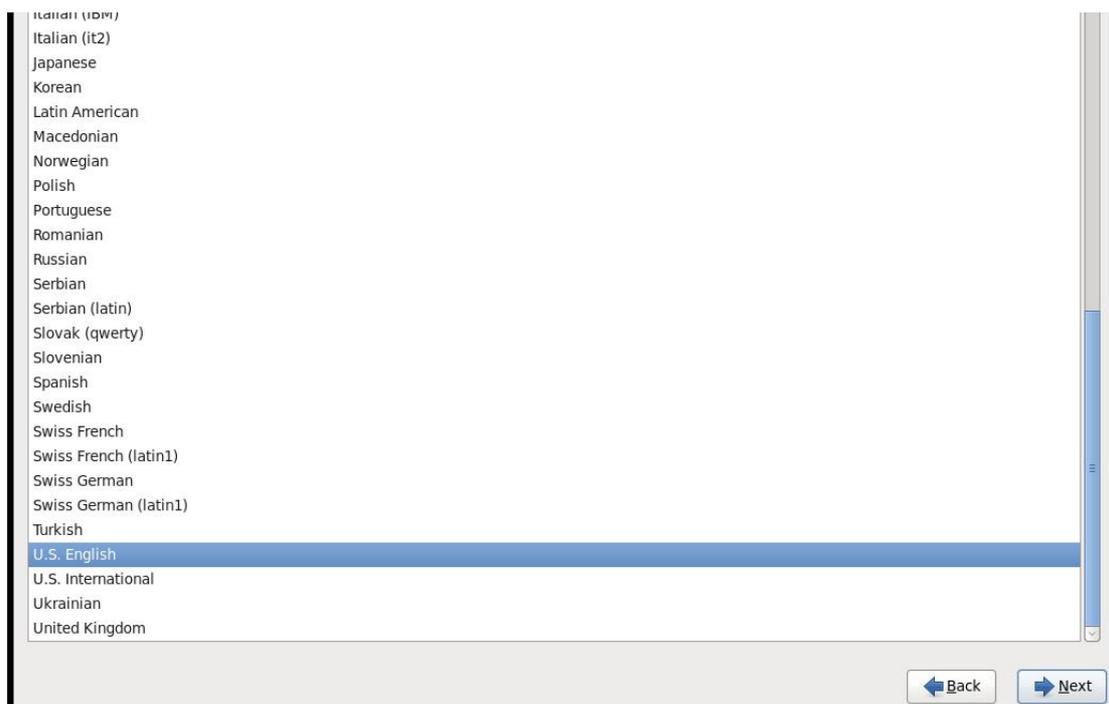
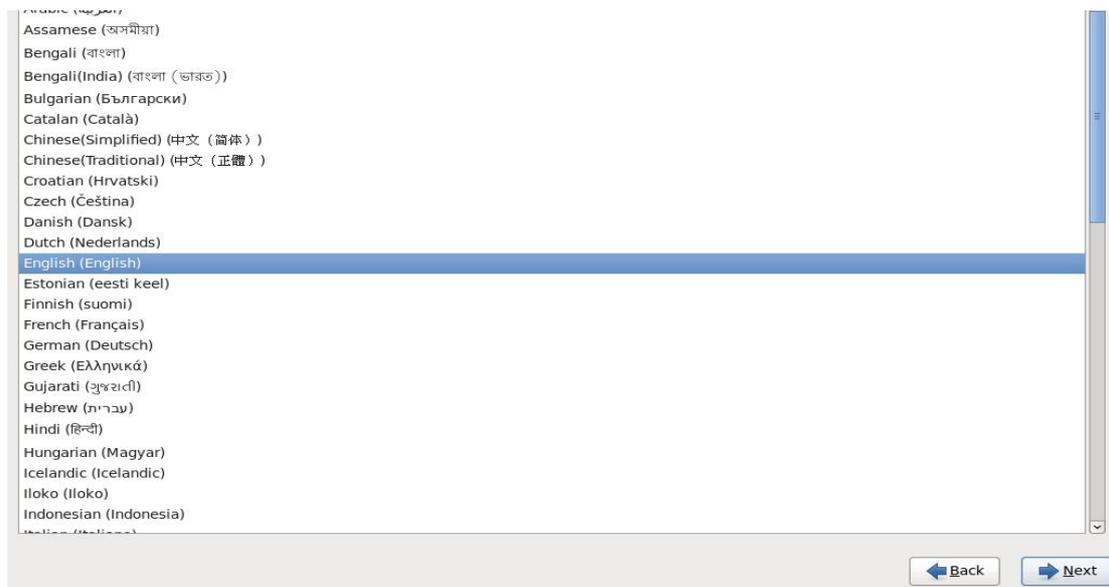
3 进入安装界面，选择“NEXT”继续安装。



### 3.1.1 语言、键盘设置

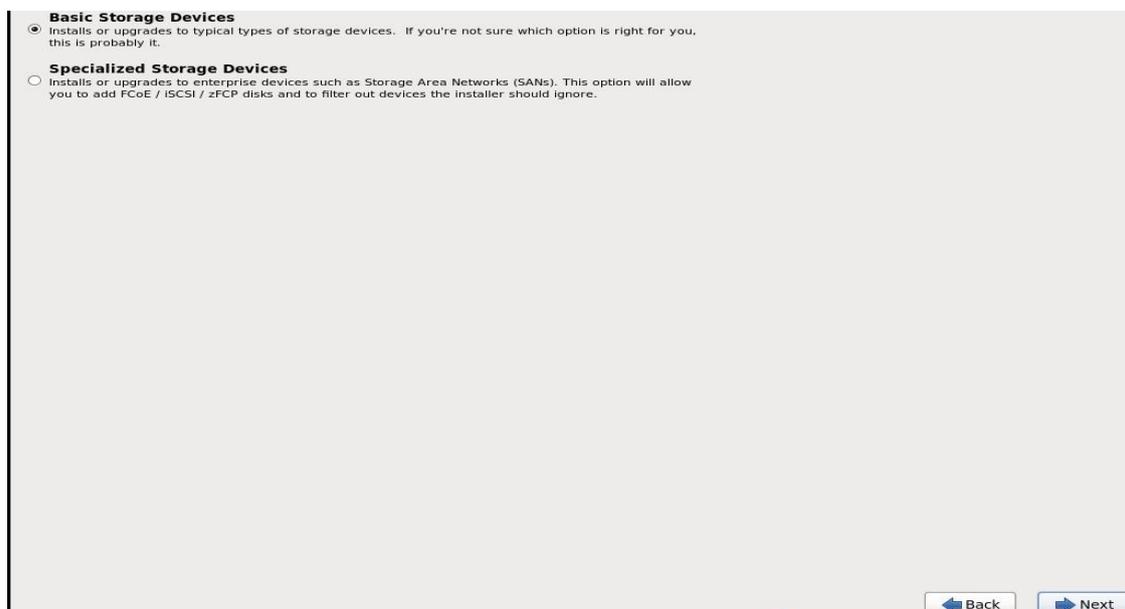
- **Language:** 选择安装过程中使用的语言，保持默认 **English** 即可。
- **Keyboard:** 选择键盘类型，保持默认的 **U.S. English** 即可。

依次点击 **Next** 继续。



## 3.1.2 存储设备配置

一般情况，均默认选择“basic storage devices”，点“next”

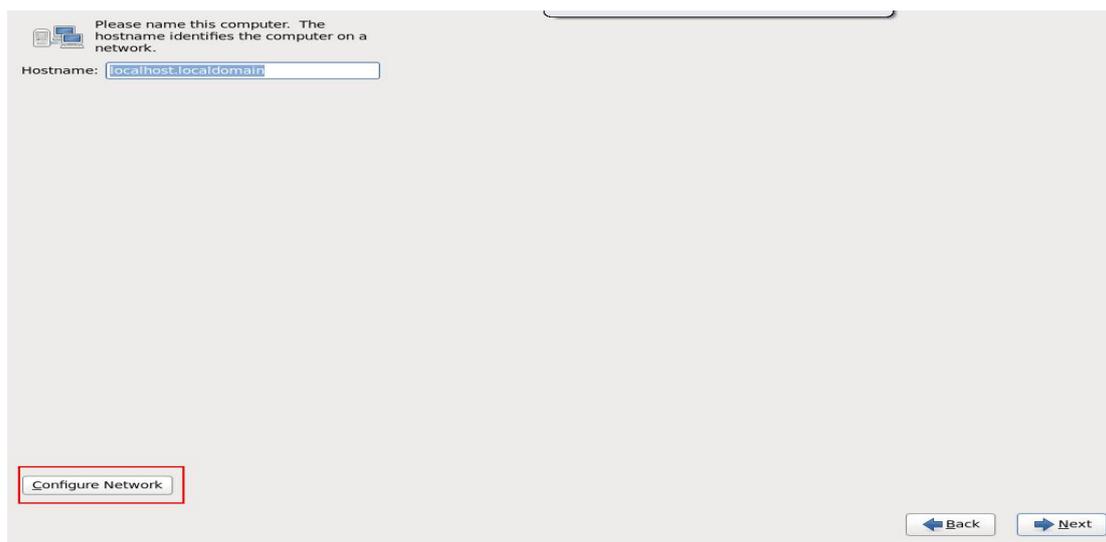


如果系统提示存储设备可能包含数据，请选择 Yes, discard any data 以继续。



### 3.1.3 计算机名配置

在 Hostname 输入框中，根据实际规划为服务器设置一个主机名，例如 audit-server。点击 Next。



### 3.1.4 网络配置

- 1 点击界面左下角的 Configure Network，打开网络配置对话框。



- 2 选中网卡 System eth0，点击 Edit。



### 3 在网卡配置窗口中：

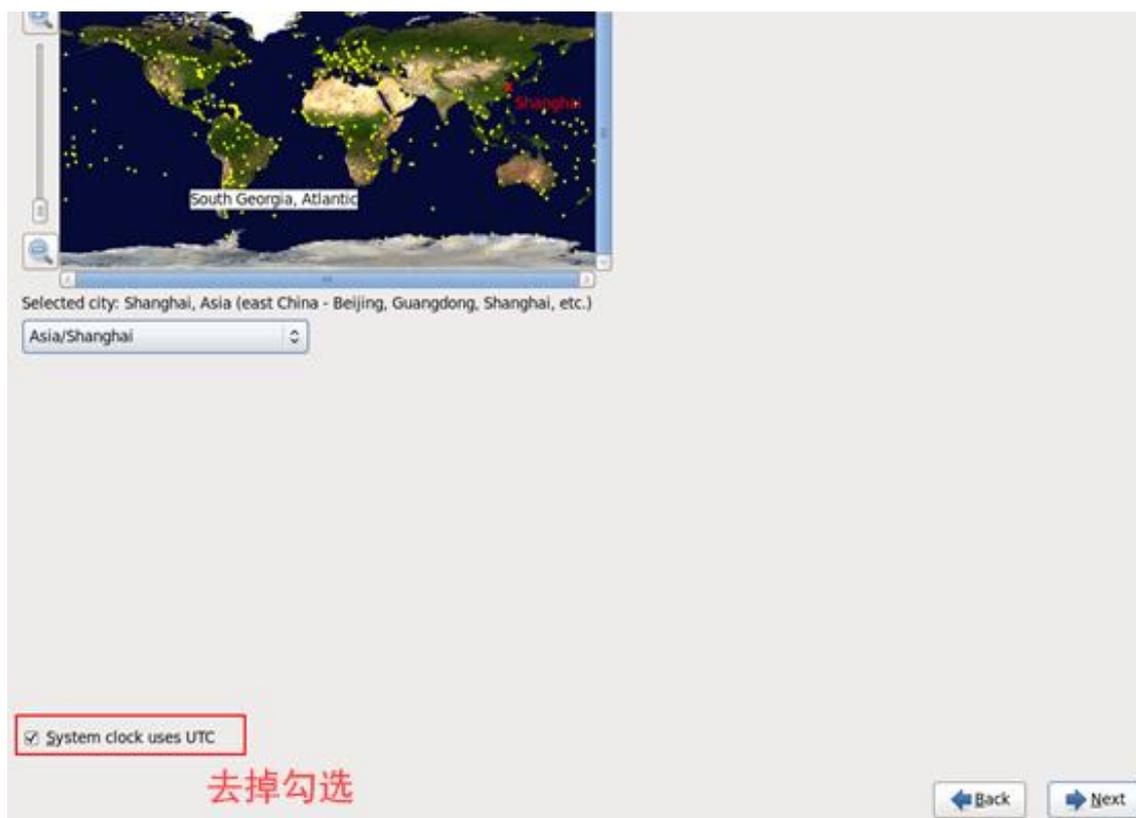
- 勾选 Connect automatically。
- 切换到 IPv4 Settings 选项卡，将 Method 设置为 Manual。
- 点击 Add，填入 IP 地址信息。例如，可将 eth0 的地址设为 192.168.1.254，子网掩码 255.255.255.0。点击 Apply 保存。



- 4 按照同样的方法配置备用网口 eth1, 例如设置 IP 为 172.19.11.26, 子网掩码 255.255.255.0。
- 5 配置完成后, 点击 Close 关闭网络配置窗口, 返回主机名配置界面。

### 3.1.5 时区配置

在时区选择界面, 选择 Asia/Shanghai。注意: 请务必取消勾选 System clock uses UTC (系统时钟使用 UTC 时间), 然后点击 Next。

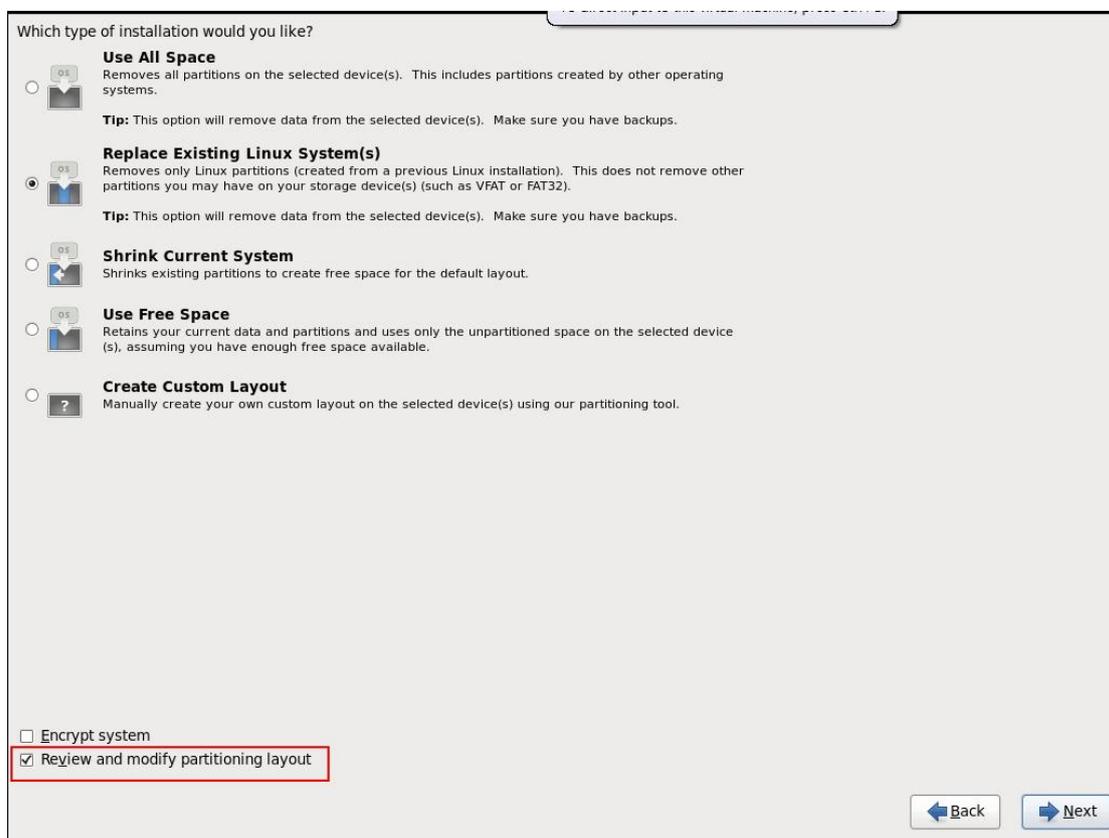


### 3.1.6 ROOT 账户密码配置

为系统超级管理员 root 账户设置一个强密码，并牢记。然后点击 Next。



在后续界面中，勾选 Review and modify partitioning layout（查看并修改分区布局），然后点击 Next 进入磁盘分区设置。



### 3.1.7 分区操作

根据服务器硬盘数量，参考以下对应章节进行分区。请谨慎操作，避免数据丢失。

#### 单盘分区操作

1. 清理旧分区：如果硬盘上已有分区，点击界面下方的 Reset 按钮，并在确认窗口中选择 Yes，以清除所有现有分区，使硬盘空间变为 Free 状态。

### Please Select A Device

Device	Size (MB)	Mount Point/ RAID/Volume	Type	Format
LVM Volume Groups				
VolGroup	50696			
lv_root	46664 /		ext4	✓
lv_swap	4032		swap	✓
Hard Drives				
sda (dev/sda)				
sda1	500 /boot		ext4	✓
sda2	50699 VolGroup		physical volume (LVM)	✓

### Confirm Reset

 Are you sure you want to reset the partition table to its original state?

**Drive /dev/sda (51200 MB) (Model: VMware, VMware Virtual S)**

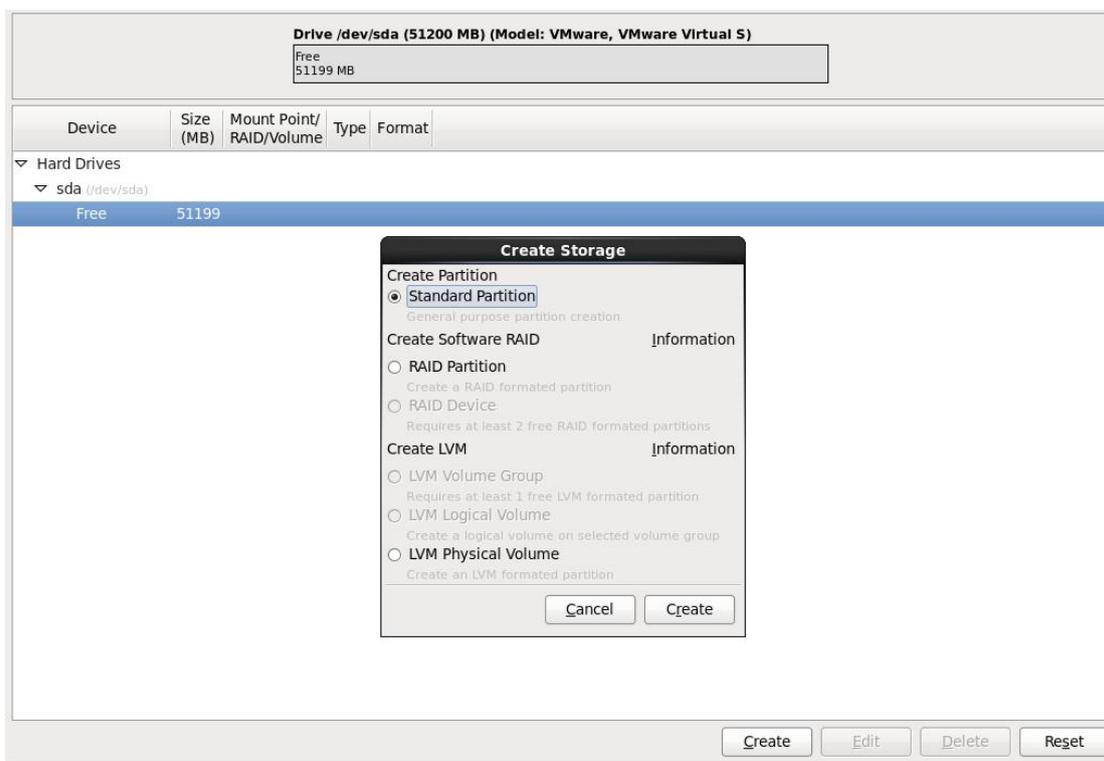
/dev/sda2 15360 MB	/dev/sda4 5120 MB	/dev/sda5 30618 MB
-----------------------	----------------------	-----------------------

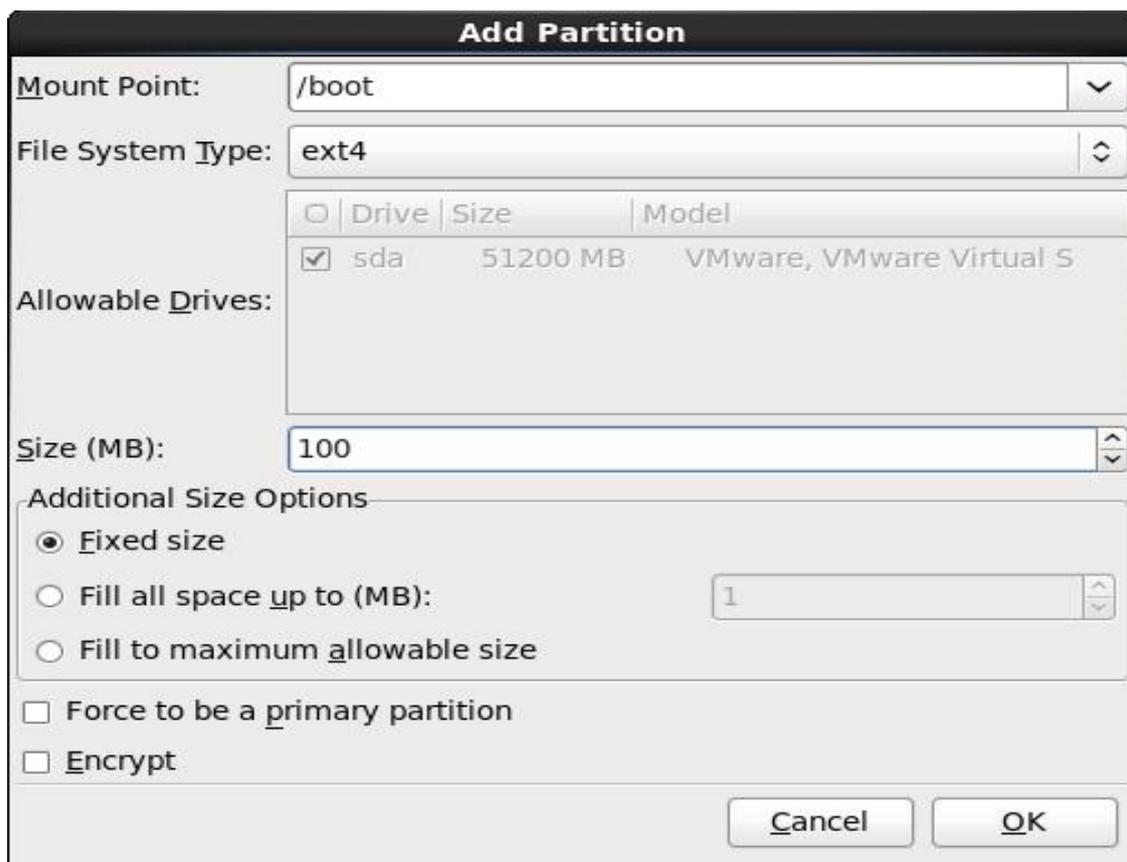
Device	Size (MB)	Mount Point/ RAID/Volume	Type	Format
▼ Hard Drives				
▼ sda (/dev/sda)				
sda1	100		ext4	
sda2	15360		ext4	
sda3	5120		swap	
▼ sda4				
sda5	30618		ext4	

**Please Select A Device**

Device	Size (MB)	Mount Point/ RAID/Volume	Type	Format
▼ Hard Drives				
▼ sda (/dev/sda)				
Free	51199			

2. 创建 /boot 分区：选中空闲空间 Free，点击 Create。在弹出的对话框中，依次选择 Standard Partition -> Create。在 Mount Point 中输入 /boot，Size 输入 200 (MB)，点击 OK。





**Add Partition**

Mount Point: /boot

File System Type: ext4

Drive	Size	Model
<input checked="" type="checkbox"/> sda	51200 MB	VMware, VMware Virtual S

Size (MB): 100

Additional Size Options

Fixed size

Fill all space up to (MB): 1

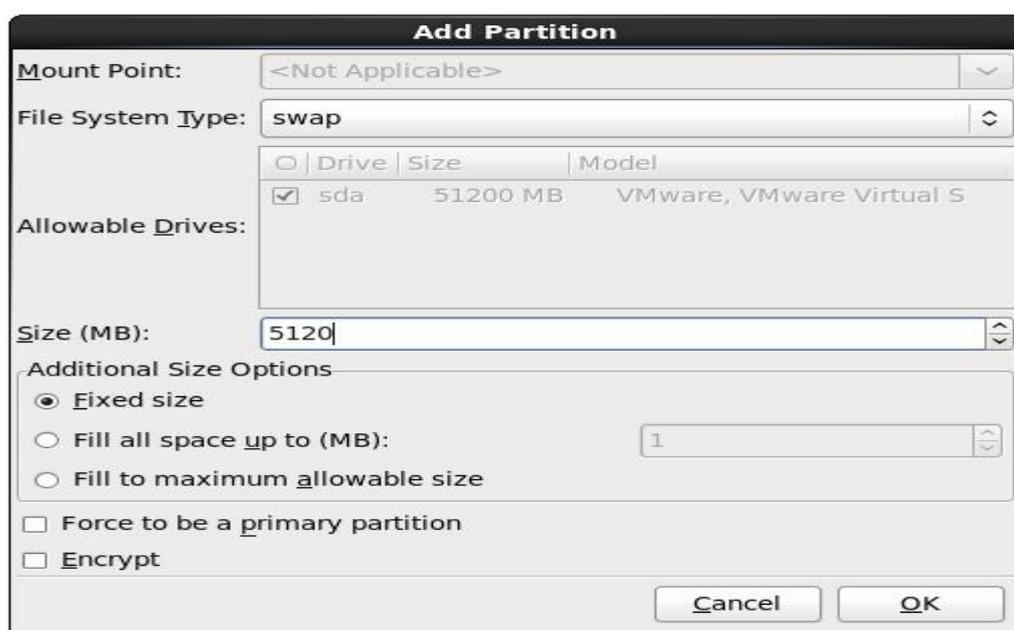
Fill to maximum allowable size

Force to be a primary partition

Encrypt

Cancel OK

3. 创建 Swap 分区: 再次点击 Create, Mount Point 留空, File System Type 选择 swap, Size 设置为物理内存大小的 2 倍 (例如内存 8GB, 则输入 16384) , 点击 OK。



**Add Partition**

Mount Point: <Not Applicable>

File System Type: swap

Drive	Size	Model
<input checked="" type="checkbox"/> sda	51200 MB	VMware, VMware Virtual S

Size (MB): 5120

Additional Size Options

Fixed size

Fill all space up to (MB): 1

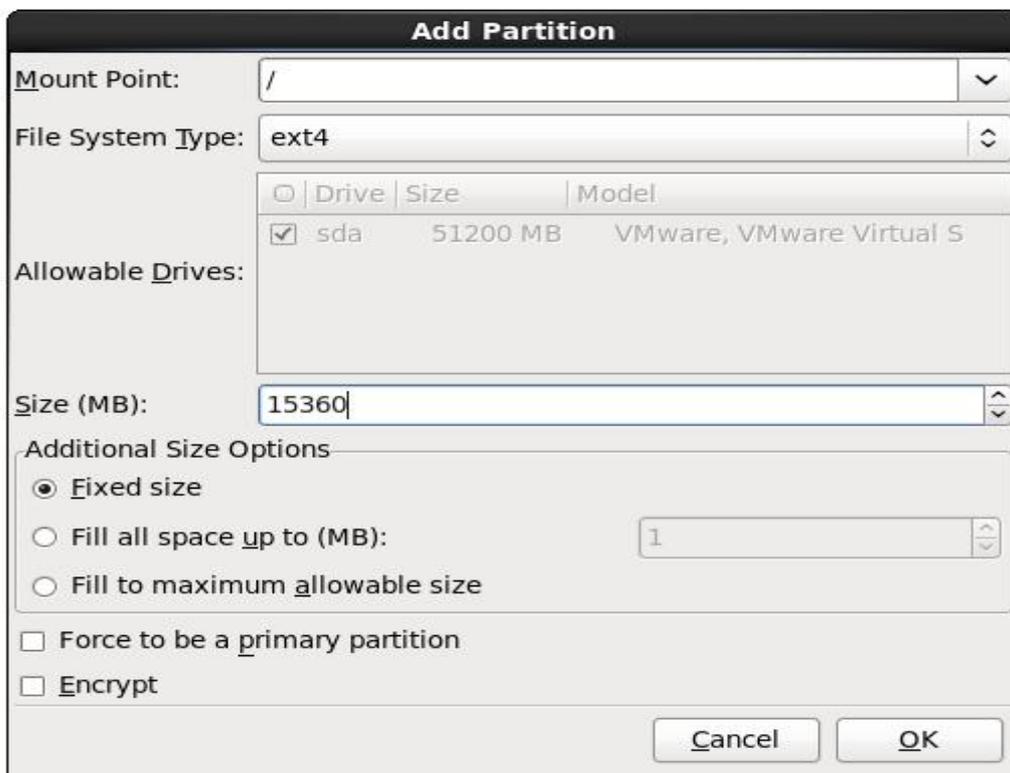
Fill to maximum allowable size

Force to be a primary partition

Encrypt

Cancel OK

4. 创建根分区 /: 再次点击 Create, Mount Point 输入 /, Size 输入 15360 (即 15GB) , 点击 OK。



Drive	Size	Model
<input checked="" type="checkbox"/> sda	51200 MB	VMware, VMware Virtual S

5. 创建 /data 分区: 再次点击 Create, Mount Point 输入 /data, 在 Additional Size Options 中选择 Fill to maximum allowable size (使用剩余全部空间) , 点击 OK。

### Add Partition

**Mount Point:** /data

**File System Type:** ext4

**Allowable Drives:**

<input type="checkbox"/>	Drive	Size	Model
<input checked="" type="checkbox"/>	sda	51200 MB	VMware, VMware Virtual S

**Size (MB):** 200

**Additional Size Options**

Fixed size

Fill all space up to (MB): 1

Fill to maximum allowable size

Force to be a primary partition

Encrypt

6. 完成分区：确认分区信息无误后，点击 Next。

### Please select a device

Device	Size (MB)	Mount Point/ RAID/Volume	Type	Format
▼ Hard Drives				
▼ sda (/dev/sda)				
sda1	100	/boot	ext4	✓
sda2	15360	/	ext4	✓
sda3	5120		swap	✓
▼ sda4				
sda4	30619		Extended	
sda5	30618	/data	ext4	✓

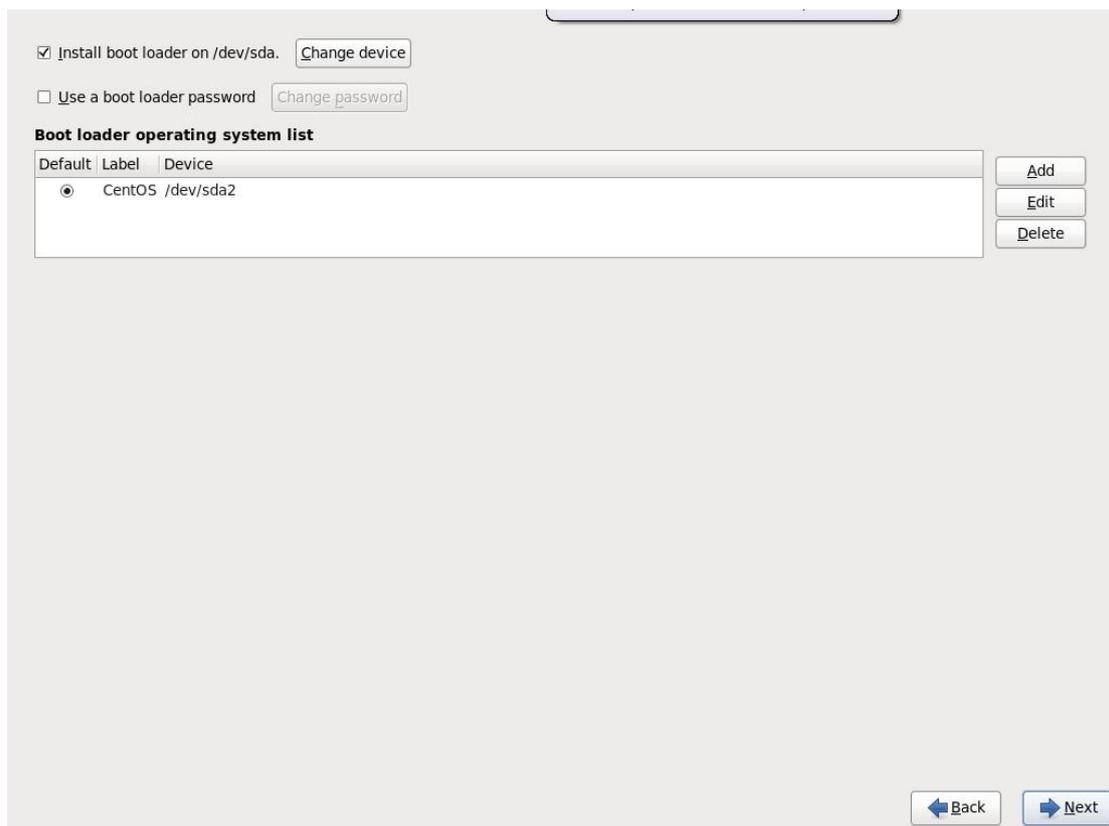
7. 格式化确认：系统提示需要格式化分区，选择 Format。



8. 写入磁盘：系统再次提示将修改写入磁盘，选择 Write changes to disk。



9. 点击 Next 继续后续安装。



## 多盘分区操作

本示例以两块硬盘 (sda, sdb) 为例, 目标是使用 sda 安装系统, sdb 全部用作数据盘 /data。

1. 选择安装目标: 在 Select the drive(s) to use for this installation 界面, 将需要安装系统的硬盘 (如 sda, sdb) 从左侧 Data storage devices 移至右侧 Install target devices, 点击 Next。

Below are the storage devices you've selected to be a part of this installation. Please indicate using the arrows below which devices you'd like to use as data drives (these will not be formatted, only mounted) and which devices you'd like to use as system drives (these may be formatted). Please also indicate which system drive will have the bootloader installed.

**Data Storage Devices** (to be mounted only)

Model	Capacity	Vendor	Identifier

**Install Target Devices**

Boot Loader	Model	Capacity	Identifier
<input checked="" type="radio"/>	VMware, VMware Virtual S	51200 MB	pci-0000:
<input type="radio"/>	VMware, VMware Virtual S	20480 MB	pci-0000:

**Tip:** All Linux filesystems on install target devices will be reformatted and wiped of any data. Make sure you have backups.

2. 清理所有分区：点击 Reset 按钮，并在确认窗口中选择 Yes，清除所有硬盘上的现有分区，使每块硬盘都变为 Free 状态。

**Please Select A Device**

Device	Size (MB)	Mount Point/ RAID/Volume	Type	Format
LVM Volume Groups				
VolGroup	71172			
lv_root	51200	/	ext4	✓
lv_home	15940	/home	ext4	✓
lv_swap	4032		swap	✓
Hard Drives				
sda (/dev/sda)				
sda1	500	/boot	ext4	✓
sda2	50699	VolGroup	physical volume (LVM)	✓
sdb (/dev/sdb)				
sdb1	20479	VolGroup	physical volume (LVM)	✓



Drive /dev/sda (51200 MB) (Model: VMware, VMware Virtual S)

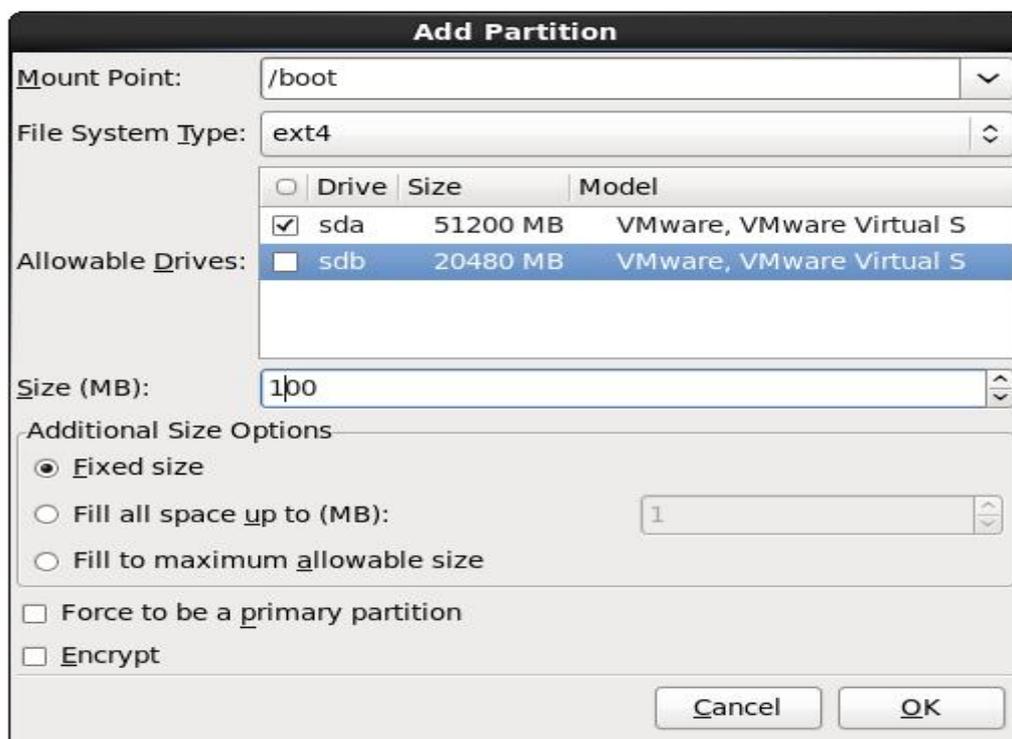
/dev/sda2  
50699 MB

Device	Size (MB)	Mount Point/ RAID/Volume	Type	Format
LVM Volume Groups				
VolGroup 71172				
lv_root	51200	/	ext4	✓
lv_home	15940	/home	ext4	✓
lv_swap	4032		swap	✓
Hard Drives				
sda (/dev/sda)				
sda1	500	/boot	ext4	✓
sda2	50699	VolGroup	physical volume (LVM)	✓
sdb (/dev/sdb)				
sdb1	20479	VolGroup	physical volume (LVM)	✓

Device	Size (MB)	Mount Point/ RAID/Volume	Type	Format
Hard Drives				
sda (/dev/sda)				
Free	51199			
sdb (/dev/sdb)				
Free	20473			

3. 在 sda 上创建 /boot 分区：选中 sda 的空闲空间，点击 Create -> Standard Partition -> Create。配置如下：

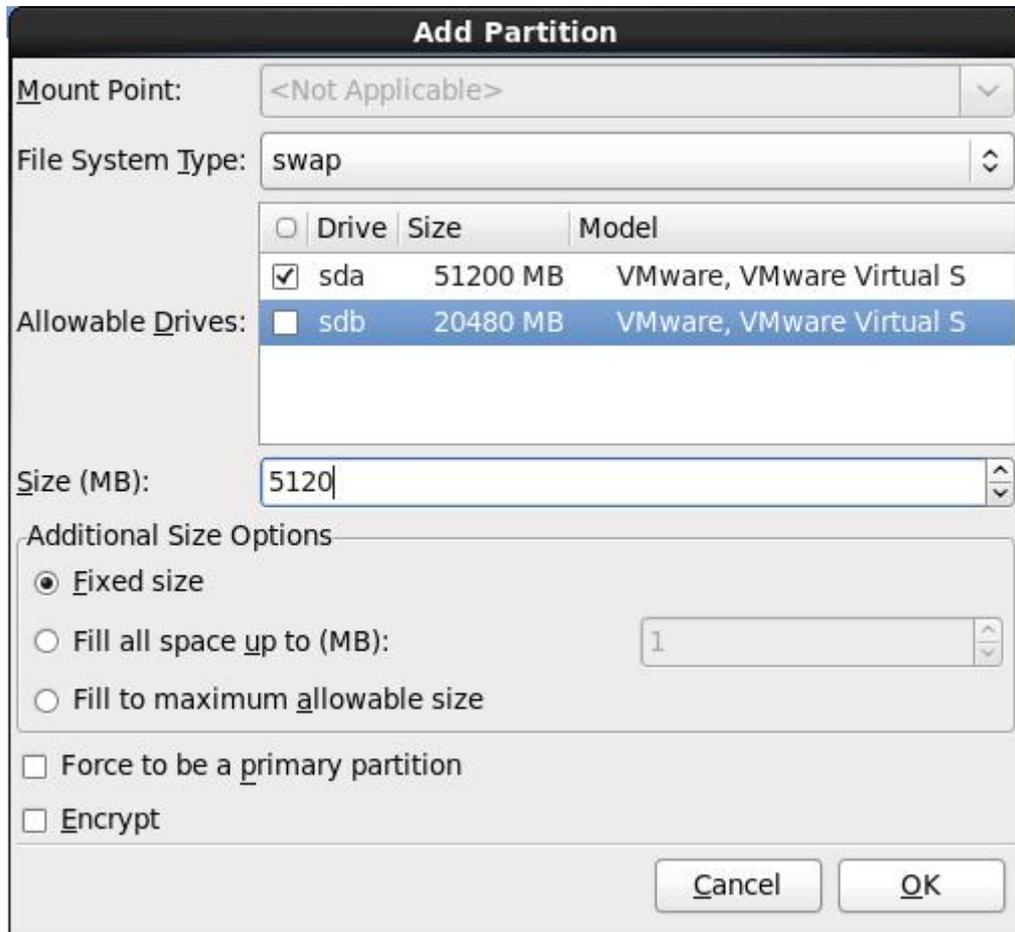
- Mount Point: /boot
- File System Type: ext4 (默认)
- Allowable Drives: 仅勾选 sda, 取消勾选 sdb
- Size: 200 MB
- 点击 OK



4. 在 sda 上创建 Swap 分区：再次点击 Create, 配置如下：

- File System Type: swap
- Allowable Drives: 仅勾选 sda
- Size: 内存大小的 2 倍 (如 16384)

- 点击 OK



**Add Partition**

Mount Point: <Not Applicable>

File System Type: swap

Allowable Drives:

<input type="checkbox"/>	Drive	Size	Model
<input checked="" type="checkbox"/>	sda	51200 MB	VMware, VMware Virtual S
<input type="checkbox"/>	sdb	20480 MB	VMware, VMware Virtual S

Size (MB): 5120

Additional Size Options

Fixed size

Fill all space up to (MB): 1

Fill to maximum allowable size

Force to be a primary partition

Encrypt

Cancel OK

5. 在 sda 上创建根分区 /: 再次点击 Create, 配置如下:

- Mount Point: /
- Allowable Drives: 仅勾选 sda
- Size: 15360 MB
- 点击 OK

**Add Partition**

Mount Point: /

File System Type: ext4

<input type="checkbox"/>	Drive	Size	Model
<input checked="" type="checkbox"/>	sda	51200 MB	VMware, VMware Virtual S
<input type="checkbox"/>	sdb	20480 MB	VMware, VMware Virtual S

Allowable Drives:

Size (MB): 15360

Additional Size Options

Fixed size

Fill all space up to (MB): 1

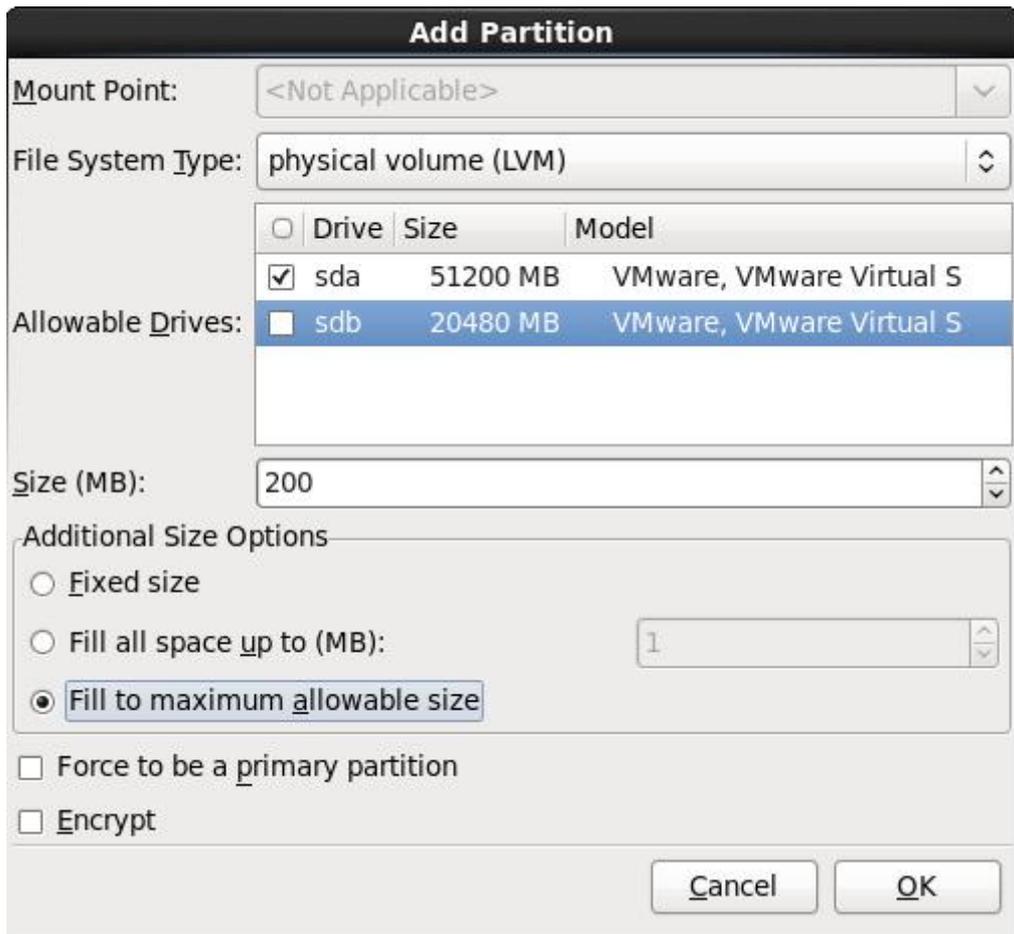
Fill to maximum allowable size

Force to be a primary partition

Encrypt

6. 在 sda 上创建物理卷 (PV): 再次点击 Create, 配置如下:

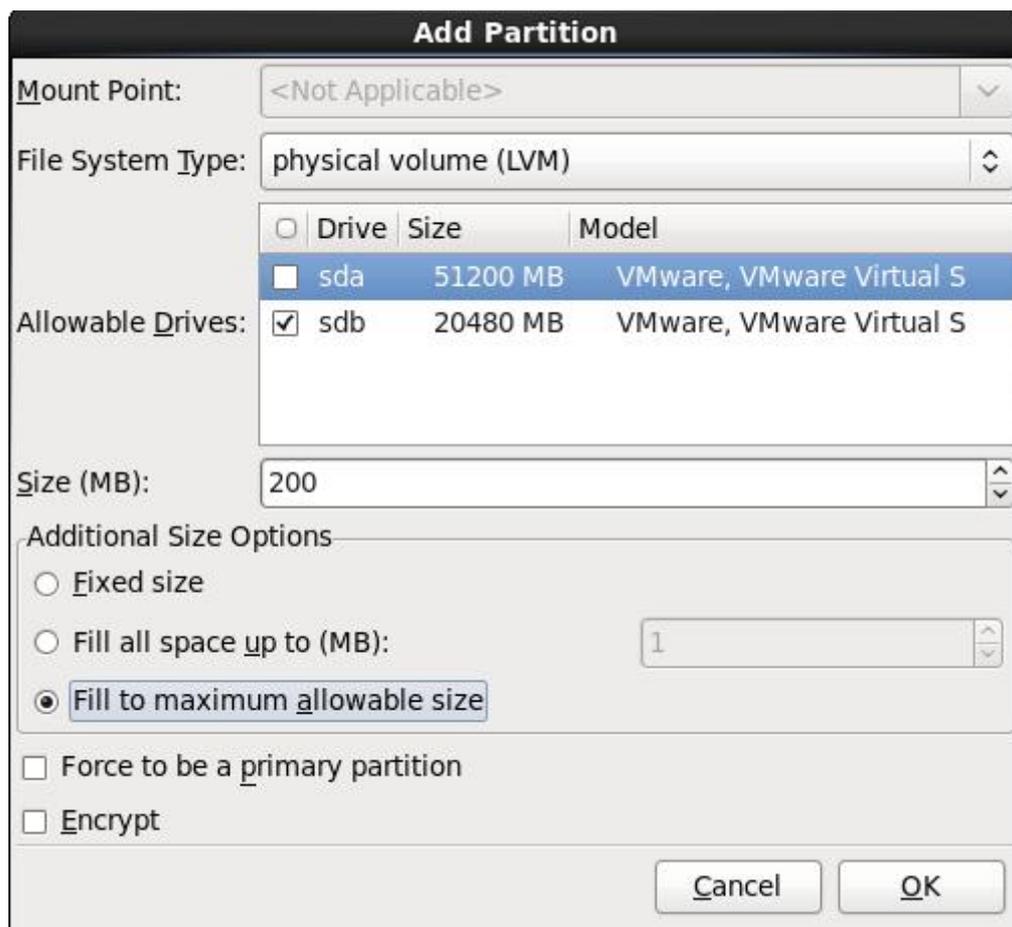
- File System Type: physical volume (LVM)
- Allowable Drives: 仅勾选 sda
- Additional Size Options: Fill to maximum allowable size (使用 sda 剩余空间)
- 点击 OK



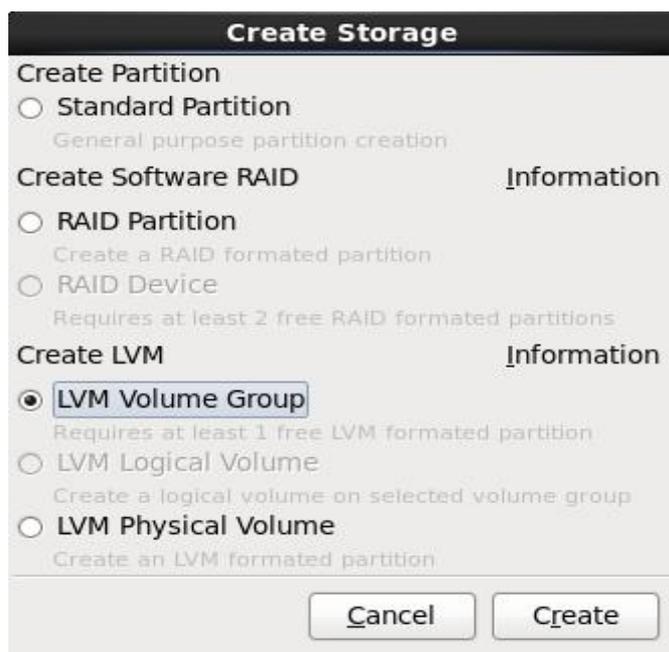
Drive	Size	Model
<input checked="" type="checkbox"/> sda	51200 MB	VMware, VMware Virtual S
<input type="checkbox"/> sdb	20480 MB	VMware, VMware Virtual S

7. 在 sdb 上创建物理卷 (PV): 再次点击 Create, 配置如下:

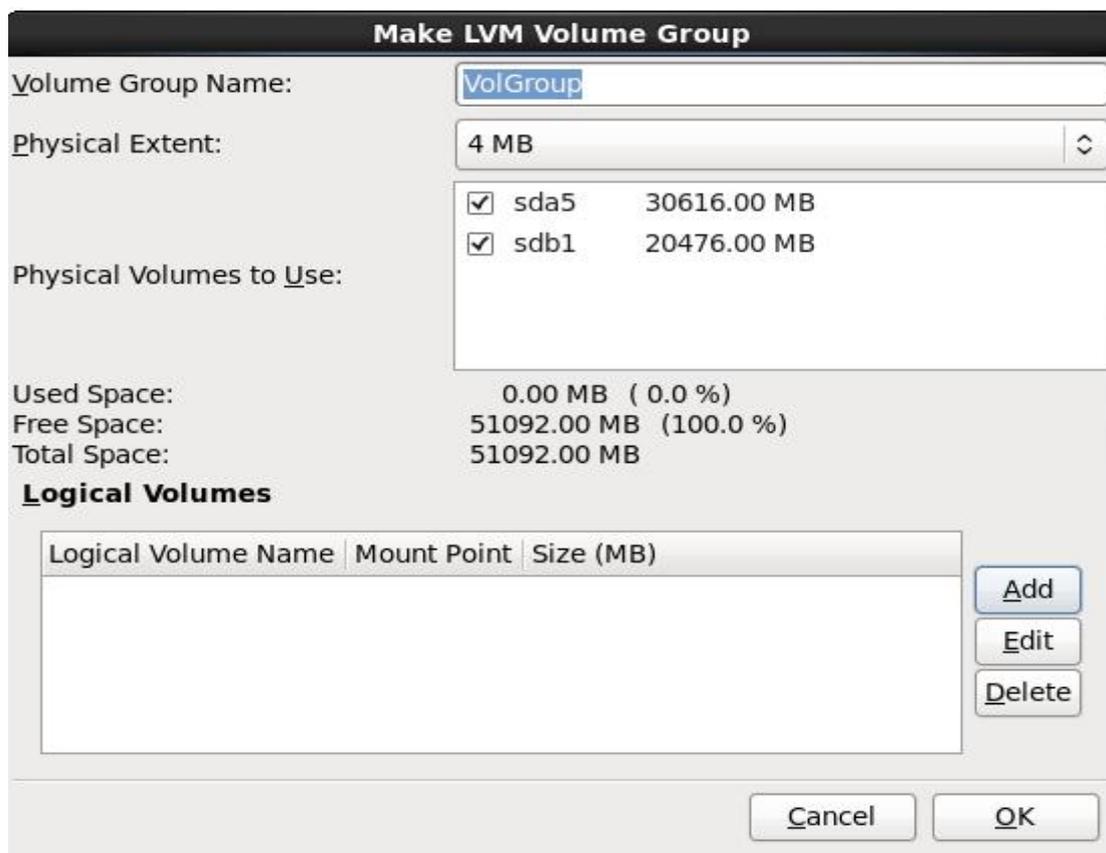
- File System Type: physical volume (LVM)
- Allowable Drives: 仅勾选 sdb
- Additional Size Options: Fill to maximum allowable size (使用 sdb 全部空间)
- 点击 OK



8. 创建 LVM 卷组 (VG): 最后, 点击 Create, 在弹出的窗口中选择 Create LVM, 然后点击 Create。

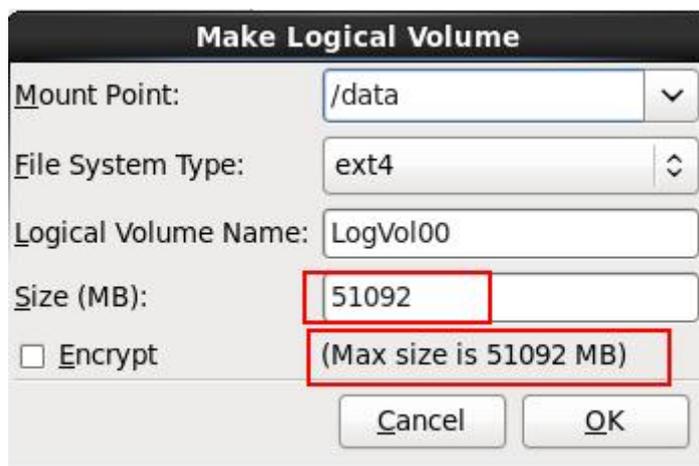


9. 在 LVM 中创建逻辑卷 (LV): 在 Create LVM 界面, 点击 Add 添加逻辑卷。



10. 配置 /data 逻辑卷：在弹出的 Make Logical Volume 窗口中，配置如下：

- Mount Point: /data
- File System Type: ext4 (默认)
- Size: 输入与 (Max size is xxxx MB) 中提示的最大值相同的数值 (通常界面已自动填入) , 即将所有可用空间分配给 /data。
- 点击 OK。



11. 完成 LVM 创建：确认信息无误后，点击 OK 完成 LVM 创建。

### Make LVM Volume Group

Volume Group Name:

Physical Extent:

Physical Volumes to Use:

<input checked="" type="checkbox"/>	sda5	30616.00 MB
<input checked="" type="checkbox"/>	sdb1	20476.00 MB

Used Space: 51092.00 MB (100.0 %)  
Free Space: 0.00 MB (0.0 %)  
Total Space: 51092.00 MB

#### Logical Volumes

Logical Volume Name	Mount Point	Size (MB)
LogVol00	/data	51092

12. 分区完成后，点击 Next 继续。

Install boot loader on /dev/sda.

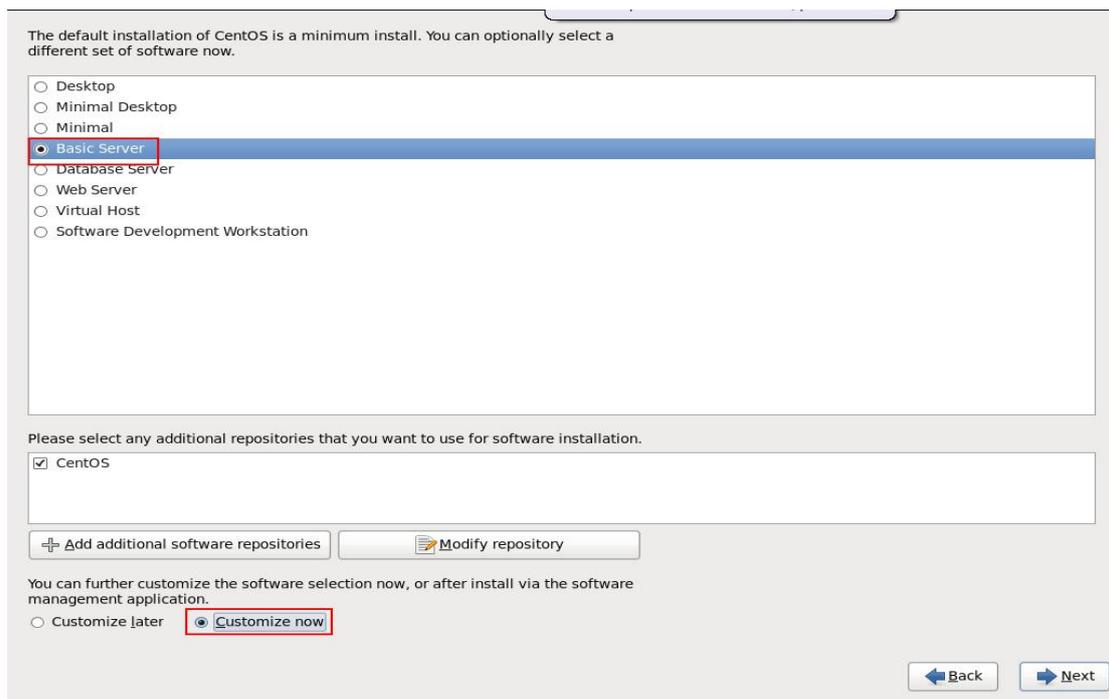
Use a boot loader password

#### Boot loader operating system list

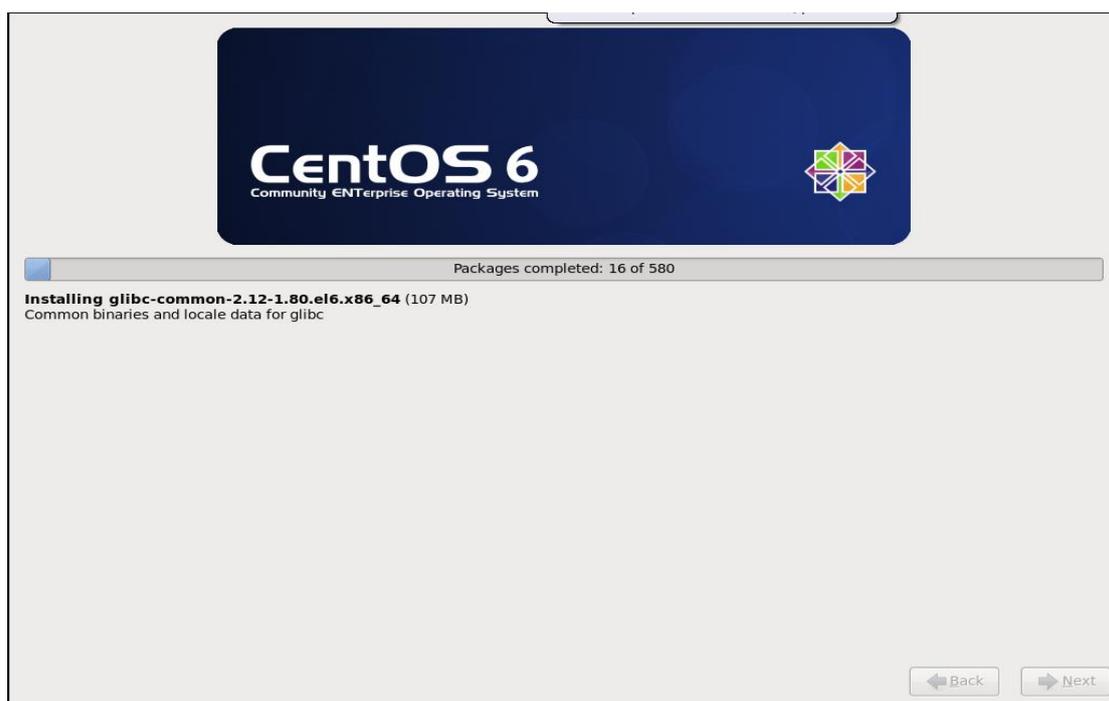
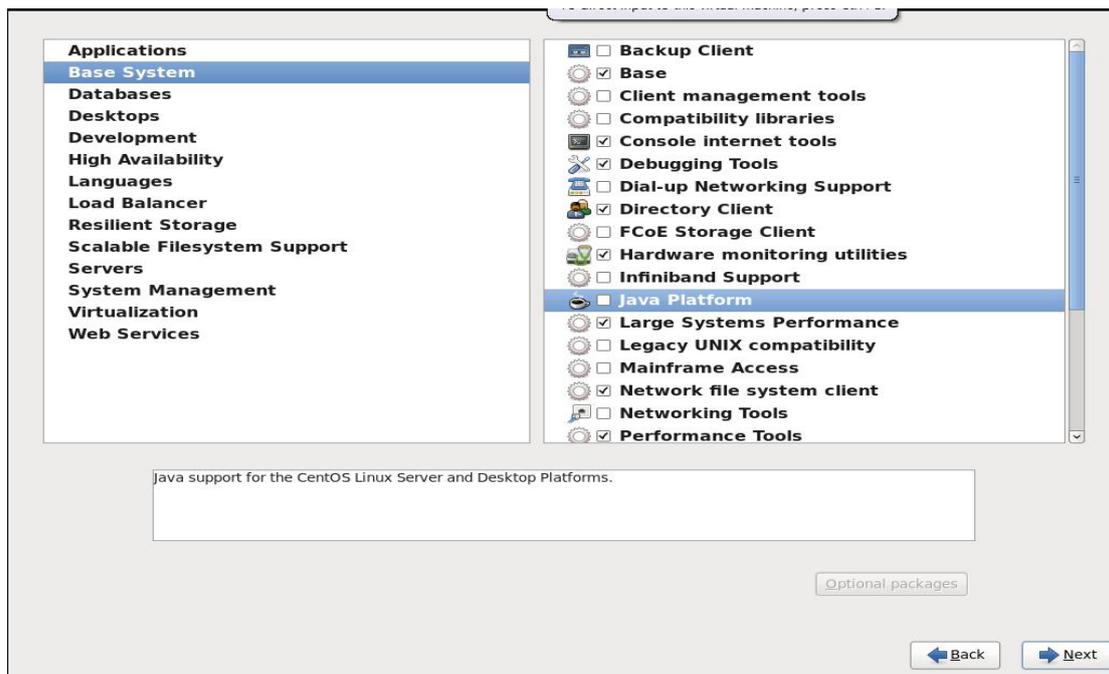
Default	Label	Device
<input checked="" type="radio"/>	CentOS	/dev/sda2

### 3.1.8 软件包安装

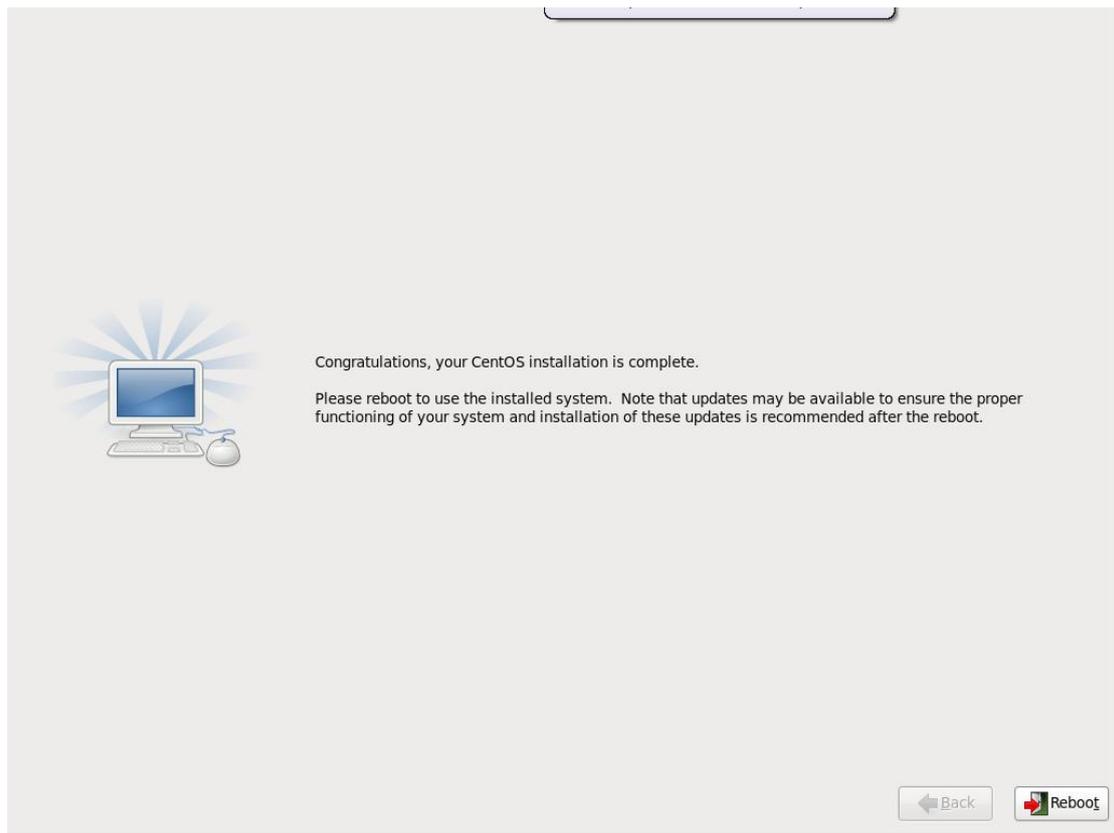
- 1 在软件包安装选项界面，选择 Basic Server，然后勾选 Customize now（现在自定义），点击 Next。



- 2 在组件选择窗口左侧选择 Base System，在右侧找到 Java Platform，取消勾选，然后点击 Next。



- 3 系统开始安装所选组件，此过程可能需要几分钟。安装完成后，点击 Reboot 重启系统。至此，操作系统安装完成。



## 3.2 安装审计产品

- 1 使用 SSH 工具登录已安装好的 CentOS 系统。由于系统进行了安全加固，推荐使用 SecureCRT 工具，其他工具可能无法正常连接。
- 2 将毕方审计系统安装包（例如 `cnnl_DBAuditInstall_1.0E_b260_r63518.bin`）上传至 `/root` 目录。
- 3 执行以下命令，赋予安装包执行权限并运行安装程序。

**针对 E 版本：**

```
cd /root
```

```
chmod +x cnnl_DBAuditInstall_1.0E_b260_r63518.bin
```

```
./cnnl_DBAuditInstall_1.0E_b260_r63518.bin
```

**针对 U 版本:**

```
cd /root
```

```
chmod +x cnnl_DBAuditInstall_1.0U_b260_r63518.bin
```

```
./cnnl_DBAuditInstall_1.0U_b260_r63518.bin
```

4 安装脚本执行完成后, 请注意以下默认变更:

- 操作系统 root 密码会被修改为: cnnl@1126
- SSH 服务端口会被修改为: 2222

## 4 卸载

重要：卸载时，请务必遵循先卸载探针、再卸载审计中心的顺序。知识库模块无需单独卸载。

### 4.1 卸载探针

- 1 使用 root 账户登录系统，执行以下命令启动卸载程序：

```
python /var/aoc/probe/bin/tools/uninstall-probe.py
```

- 2 系统提示确认：uninstall Probe: (y/n)

- 3 输入 y 并回车，卸载程序将自动运行，输出类似如下信息：

```
stopping dba-collection-process-manager... [ OK ]remove probe
success!Begin to uninstall Database IDS PackageShutting down dbidsmon:
[ OK ]Shutting down dbidsprobe: [ OK ]Database table be
dropped+++++uninstall
ok+++++
```

- 4 在卸载过程中，如果出现任何二次确认提示（如删除数据等），请全部输入 y 并按回车继续，直至卸载完成。

### 4.2 卸载审计中心

- 1 执行以下命令启动卸载程序：

1.

```
python /var/aoc/analyzer/bin/tools/uninstall-dba.py
```

2 系统提示确认: uninstall AMC: (y/n)

3 输入 y 并回车, 卸载程序将自动运行, 输出类似如下信息:

```
stopping dba-business-process-manager... [ OK ]Stopping automount_smb  
[FAILED]Stopping httpd: [ OK ]Stopping tomcatd:  
[ OK ]...+++++rpm  
uninstall+++++Success: Usage count is  
0...+++++uninstall ok+++++
```

4 在卸载过程中, 如果出现任何二次确认提示, 请全部输入 y 并按回车继续, 直至卸载完成。

5 卸载程序执行完毕后, 建议重启设备以完成所有清理工作。