

凝思安全操作系统

V6.0.60

安装手册

北京凝思科技有限公司
Linx Technology Co.,Ltd.

2014.5

ChangeLog

- 2012.2 增加“China GRID needed packages”软件集。
- 2012.7 根据6.0.3版系统修改。
- 2013.3 根据6.0.4版系统修改。
- 2014.1 根据最新版6.0.4系统修改。
- 2014.4 根据6.0.60.4-2014-04-10版系统修改。
- 2014.5 根据6.0.60.4-2014-05-05版系统修改。

目 录

产品概述	1
关于本书	6
文档约定	6
术语简介	8
如何使用本书	10
第 1 章 准备工作	11
1.1 备份资料	11
1.2 系统兼容性	11
1.2.1 硬件兼容	11
1.2.2 软件兼容	11
1.3 系统需求	12
第 2 章 本地安装	14
2.1 安装程序用户界面	14
2.1.1 图形界面	14
2.1.2 字符界面	14
2.1.2.1 界面构件	14
2.1.2.2 使用键盘来导航	15
2.2 启动安装程序	16
2.3 图形界面安装	19
2.3.1 选择语言（专家模式）	19
2.3.2 配置键盘	21
2.3.3 探测并挂载光盘（专家模式）	23
2.3.4 加载安装程序组件（专家模式）	25
2.3.5 配置网络	27
2.3.5.1 指定 DHCP 服务器	30
2.3.5.2 手动设置网络	31
2.3.5.3 确认网络参数	35
2.3.5.4 设置主机名	36
2.3.5.5 设置域名	37

2.3.6	输入序列号	38
2.3.7	设置用户和密码	39
2.3.8	时钟设置（专家模式）	45
2.3.9	磁盘分区	48
2.3.9.1	选择磁盘	49
2.3.9.2	选择分区方案	50
2.3.9.3	修改分区设置	52
2.3.9.4	复制分区	60
2.3.9.5	删除分区	60
2.3.9.6	撤销修改	60
2.3.9.7	确认分区	61
2.3.9.8	配置 LVM	62
2.3.9.9	配置加密的 LVM	64
2.3.9.10	手动分区	66
2.3.9.11	配置软 Raid	70
2.3.10	安装基本系统	83
2.3.11	配置软件包管理器	86
2.3.12	选择应用软件包	93
2.3.13	配置服务器参数	97
2.3.13.1	设置 MySQL 管理员口令	97
2.3.13.2	配置 Samba 服务	99
2.3.13.3	配置 FTP 服务	100
2.3.13.4	配置 Postfix 服务	101
2.3.14	安装 GRUB	103
2.3.15	安装完成	106
2.3.16	中止安装	108
2.4	字符界面安装	110
2.4.1	配置网络	111
2.4.1.1	使用DHCP主机名重试网络自动设置	113
2.4.1.2	手动设置网络	114
2.4.1.3	设置主机名	118
2.4.1.4	设置域名	119
2.4.2	输入序列号	120
2.4.3	设置用户和密码	121
2.4.4	磁盘分区	127
2.4.4.1	分区向导	127
2.4.4.2	选择分区方案	130
2.4.4.3	修改分区设置	132
2.4.4.4	复制分区	139
2.4.4.5	删除分区	140

2.4.4.6	撤销修改	140
2.4.4.7	确认分区	141
2.4.4.8	配置 LVM	142
2.4.4.9	配置加密的 LVM	144
2.4.4.10	手动分区	147
2.4.4.11	配置软Raid	153
2.4.5	安装基本系统	163
2.4.6	配置软件包管理器	164
2.4.7	选择应用软件包	171
2.4.8	配置服务器参数	173
2.4.8.1	设置 MySQL 管理员口令	173
2.4.8.2	配置 Samba 服务	175
2.4.8.3	配置 FTP 服务	176
2.4.8.4	配置 Postfix 服务	177
2.4.9	安装 GRUB	179
2.4.10	安装完成	181
2.4.11	中止安装	182
2.5	自动安装	184
2.6	电网定制安装	184
第 3 章	网络部署	185
3.1	原理	185
3.2	环境配置	186
3.2.1	PXE 客户端与 PXE 服务器端的配置	186
3.2.1.1	待安装操作系统的计算机系统的配置 (PXE 客户端)	186
3.2.1.2	DHCP 服务器的设置 (PXE 服务器端)	186
3.2.1.3	高级 TFTP 服务器的配置 (PXE 服务器端)	188
3.2.2	与 NBP 相关的配置	188
3.2.2.1	NBP 的配置	188
3.2.3	与操作系统安装过程相关的配置	189
3.2.3.1	apache 服务器的配置	189
3.2.3.2	操作系统安装程序的释放	190
3.2.3.3	操作系统安装过程自动化的配置	190
3.3	实施过程	192
3.3.1	DHCP、TFTP 和 apache 服务器的启动	192
3.3.2	网络安装过程的启动	192
第 4 章	常见问题解答	194
附录 A	文件和目录	199
A.1	/	200

目 录

A.2 /etc	201
A.3 /dev	202
A.4 /usr	202
A.5 /var	203
A.6 /proc	204

表 格

2.1 Raid 级别比较 71

插图

2.1	安装界面	16
2.2	Advanced options	17
2.3	Choose language	19
2.4	安装程序主菜单	20
2.5	选择键盘布局区	21
2.6	从光盘加载安全程序组件	22
2.7	PCMCIA资源范围选项	23
2.8	探测并挂载光盘	24
2.9	可选的安装程序组件	25
2.10	安装程序组件主界面	26
2.11	选择网络配置方式	27
2.12	网络自动设置失败	28
2.13	配置网络	29
2.14	指定 DHCP 主机名	30
2.15	设置 IP 地址	31
2.16	设置网络掩码	32
2.17	设置网关	33
2.18	域名服务器地址	34
2.19	确认网络参数	35
2.20	设置主机名	36
2.21	设置域名	37
2.22	输入序列号	38
2.23	激活序列号	38
2.24	启用影子口令	39
2.25	设置系统管理员密码	40
2.26	创建普通用户	41
2.27	设置普通用户全名	42
2.28	设置用户名	43
2.29	设置用户密码	44
2.30	使用 NTP 设置时钟	45

2.31 输入 NTP 服务器	46
2.32 选择时区	47
2.33 磁盘分区	48
2.34 选择磁盘	49
2.35 分区方案	50
2.36 分区结果	51
2.37 分区设置	52
2.38 分区类型	54
2.39 挂载点	55
2.40 挂载选项	56
2.41 分区标识	57
2.42 磁盘保留块	58
2.43 典型用途	59
2.44 复制分区	60
2.45 确认分区	61
2.46 配置LVM	62
2.47 LVM 分区	63
2.48 加密分区	64
2.49 加密的 LVM 分区	65
2.50 创建分区	66
2.51 输入分区大小	67
2.52 选择分区类型	68
2.53 选择新分区的位置	69
2.54 软件 RAID 设置	72
2.55 确认配置 Raid	73
2.56 盘组配置	74
2.57 盘组设备类型	75
2.58 Raid阵列中活跃设备的个数	76
2.59 Raid阵列中备用设备的个数	77
2.60 选择活跃的 RAID 分区	78
2.61 选择备用的 RAID 分区	79
2.62 删除 MD 设备	80
2.63 确认删除 MD 设备	81
2.64 完成 RAID 配置	82
2.65 安装基本系统	83
2.66 安装内核	84
2.67 选择驱动程序	85
2.68 扫描CD或DVD	86
2.69 网络镜像	87
2.70 选择文件下载的协议	88

2.71 选择镜像	89
2.72 输入镜像的主机名和目录	90
2.73 输入 HTTP 代理信息	91
2.74 加载软件选择组件	92
2.75 选择应用软件包	93
2.76 安装应用软件包	96
2.77 设置MYSQL管理员口令	97
2.78 重复MYSQL管理员口令	98
2.79 配置 Samba 服务	99
2.80 配置 FTP 服务	100
2.81 配置 Postfix 服务	101
2.82 配置系统邮件名称	102
2.83 安装 GRUB	103
2.84 手动设置引导分区	104
2.85 安装 GRUB	105
2.86 结束安装进程	106
2.87 安装完成	107
2.88 中止安装	108
2.89 确认退出	109
2.90 扫描CD-ROM	110
2.91 加载安装组件	110
2.92 使用DHCP配置网络	111
2.93 网络自动设置成功	111
2.94 选择网络配置方式	112
2.95 设置DHCP主机名	113
2.96 设置 IP 地址	114
2.97 设置网络掩码	115
2.98 设置网关	116
2.99 域名服务器地址	117
2.100设置主机名	118
2.101设置域名	119
2.102输入序列号	120
2.103设置系统管理员密码	121
2.104验证密码正确性	122
2.105设置普通用户全名	123
2.106设置用户名	124
2.107设置用户密码	125
2.108验证密码正确性	126
2.109磁盘分区	127
2.110分区方法	128

2.111选择磁盘	129
2.112分区方案	130
2.113分区结果	131
2.114分区设置	132
2.115文件系统	133
2.116挂载点	134
2.117挂载选项	135
2.118标识	136
2.119保留块	137
2.120典型用途	138
2.121复制分区	139
2.122选择要复制的分区	140
2.123确认分区	141
2.124配置LVM	142
2.125LVM分区	143
2.126加密分区	144
2.127确认加密口令	145
2.128加密的LVM分区	146
2.129创建分区表	147
2.130选择磁盘空闲空间	148
2.131创建新分区	149
2.132输入分区大小	150
2.133选择分区类型	151
2.134选择新分区的位置	152
2.135选择新分区的位置	153
2.136确认配置Raid	154
2.137盘组配置	155
2.138盘组设备类型	156
2.139Raid阵列中活跃设备的个数	157
2.140Raid阵列中备用设备的个数	158
2.141选择RAID分区	159
2.142删除MD设备	160
2.143确认删除MD设备	161
2.144完成RAID配置	162
2.145安装基本系统	163
2.146扫描CD或DVD	164
2.147网络镜像	165
2.148设置网络镜像	166
2.149设置镜像的主机名	167
2.150设置镜像所在目录	168

2.151输入 HTTP 代理信息	169
2.152加载软件选择组件	170
2.153选择应用软件包	171
2.154安装应用软件包	172
2.155设置MYSQL管理员口令	173
2.156重复MYSQL管理员口令	174
2.157配置 Samba 服务	175
2.158配置 FTP 服务	176
2.159配置 Postfix 服务	177
2.160配置系统邮件名称	178
2.161安装 GRUB	179
2.162手动设置引导分区	180
2.163结束安装进程	181
2.164中止安装	182
2.165确认退出	183
2.166Loading additional components	184
3.1 引导程序选择界面	192
3.2 PXE 运行界面	193
4.1 系统安装首界面死机	194
4.2 安装过程中界面无响应	195
4.3 切换至终端登录系统	196

产品概述

凝思安全操作系统是北京凝思科技有限公司自主研发、拥有完全自主知识产权、具备等保四级要求、并且达到军 B 级安全级别的操作系统，是国内首家达到安全服务器保护轮廓 EAL3 级别的安全产品。

凝思科技经过多年的研究，开发出的凝思安全操作系统具有以下主要特点：

- 高可用性

凝思安全操作系统发布前进行了长时间的压力测试，能够保证在高内存和 CPU 负载环境下稳定运行，为各类应用提供稳定的运行平台。

为进一步提高操作系统稳定性，凝思安全操作系统还提供多种冗余容错机制，降低部件故障引起的整机失效。这些机制包括：

- 磁盘冗余技术

提供软 RAID 技术，通过磁盘冗余降低磁盘故障引起的系统风险。支持在线重建，减少系统恢复时间，提高系统稳定性。

- 网卡冗余技术

提供网卡的负载均衡和冗余备份，当两块网卡自身及其链路正常时，可提供网卡负载均衡功能，提高网络传输效率；当一块网卡或其链路发生故障时，另一网卡仍可继续提供服务，提高网络的整体可靠性。

- 磁盘阵列卡冗余技术

支持磁盘阵列卡的主备机制，当主卡或其通信链路发生故障时，凝思安全操作系统将自动切换至备份卡进行设备访问，保证磁盘阵列数据的连续性。

- 软件固化技术

支持关键操作系统数据以只读形式存储于电子盘中，防止恶意或偶然操作破坏系统数据。支持无硬盘工作模式，系统运行在基于电子盘的环境中，进一步提高系统稳定性。

- 双机热备和服务热切换机制

支持分布式双机数据热备份和服务热切换机制，当主服务器当机时服务将自动漂移至辅服务器，由于数据实现实时同步，在服务器单点故障时，服务仍不会终止，系统的整体稳定性得以充分保障。

– 资源控制机制

支持对系统中应用程序进程使用服务器软硬件资源的控制，有效解决了应用程序对资源的无限制申请和占用问题。通过对服务器软硬件资源在应用服务程序之间合理的配置和使用，可以有力保证系统的长期稳定运行，大大提高系统的可用性和健壮性，为用户业务的长期不间断运行提供保障。

● 高兼容性

凝思安全操作系统适用于从大型计算到桌面办公等各种环境，支持各类通用和专业应用，具有良好的软硬件兼容性。

凝思安全操作系统的 API 接口和实用工具完全遵循 POSIX 标准，并支持 LSB 和 FHB 等 Linux 相关标准，能够二进制兼容各类为 Linux 系统开发的应用软件，并可在二进制保持与其它 Linux 发行版的兼容。支持基于 Java 的跨平台软件，可实现基于多款中间件软件的 Web 应用系统。支持 32 位和 64 位应用程序，使用户在 32 位系统上开发的软件可直接运行于 64 系统，缩短用户应用系统的研发周期。

凝思安全操作系统提供丰富的驱动程序，支持各类主流磁盘驱动器、网卡驱动器和显示控制器等硬件设备。兼容国内外各大主流厂商的多款服务器和桌面计算机。凝思科技还可协助第三方硬件厂商完成驱动程序的研发和移植，实现加密卡等专用硬件设备支持。

● 高效性

凝思安全操作系统可针对服务器、工作站、专用设备和桌面环境进行特别优化，获得比通用操作系统更高的运行效率。

在特定项目的应用环境中，凝思可以还可针对应用系统的特性对操作系统做进一步的优化，使系统的运行效率最大化。各个操作系统内核组件的定制和优化，可充分发挥硬件平台的性能，对应用程序提供最佳支持，构建稳定、高效的计算环境。定制的内容包括：

- 定制和剪裁最小应用软件运行环境，保证系统组件的可控性，提高系统的运行效率和可用性。
- 定制进程调度策略，减少调度开销，提高操作系统和应用程序的响应速度和运行效率。
- 定制文件系统类型和存储模式，提供可靠和有效的文件系统支持，使应用程序能够快速访问文件数据。
- 定制驱动程序，实现用户程序对设备数据的快速访问，降低设备访问的系统资源

开销，提高应用系统的数据处理能力。

- 易维护性

凝思安全操作系统的配置、使用和维护方法与传统 UNIX 和 Linux 保持一致，提供丰富的管理和维护软件，既可通过命令行工具完成系统配置和维护，又可通过图形界面完成相关操作，简化用户操作步骤，减少管理员的维护工作量。支持键盘/显示器、串口和网络等多种接入方式，便于管理员的本地和远程管理。基于网络的远程管理支持加密通道的远程登录，可使用命令行方式管理远程系统；同时支持远程图形化管理和远程桌面重定向，为管理员和用户提供了图形界面的系统维护和操作。服务自启动功能使系统无须人工干预即可自动进入服务提供状态，减少系统故障恢复时间，提高系统可获得性。丰富的审计日志使管理员能够准确分析并定位各类系统故障，为快速排除问题，恢复系统正常运行提供支持。凝思安全操作系统还提供状态显示、声音报警、邮件和短信通知等多种报警机制，使管理员能够及时掌握系统的运行状态，第一时间获取系统紧急故障和安全性信息。

目前，以凝思安全操作系统为核心的安全服务器系统平台已广泛应用在国家部委、军队系统及电信、电力等行业关键部门，并获得了用户的一致好评。

凝思安全操作系统 V6.0.60 基于凝思安全操作系统 V4.x，并在以下方面对系统进行了改进和完善：

- 硬件兼容性

凝思安全操作系统 V6.0.60 分为32位和64位，支持 x86_64、i386、PPC、IA、MIPS、龙芯、SPARC 的 CPU，IDE、RAID、USB 和 SCSI 控制器，HBA 控制器，nVIDIA、ATI 显卡，能在主流厂商的服务器、PC、公共机及笔记本上正常运行。

经测试，凝思安全操作系统 V6.0.60 能在下列服务器上稳定运行：曙光专用并行机、曙光专用并行机-Z、曙光专用并行机-Y、曙光专用并行机-Z2、曙光专用并行机-H、曙光 A830r-fx、曙光 A620r-F、联想 R525G3 机架服务器、联想 R680G7 机架服务器、联想 E710R 刀片服务器、浪潮 NF5220 机架服务器、浪潮 NF5280M2 机架服务器、华为 E6000 刀片服务器、华为 RH2285V1R1 机架服务器、华为 RH2488 机架服务器。

- 软件兼容性

凝思安全操作系统 V6.0.60 上可运行多种应用软件。

经测试，达梦数据库 V6.0.60、金仓数据库 V6.1.3、神州通用数据库 V7.0、IBM DB2 数据库 V9.7、Oracle 10g 数据库、Oracle 11g 数据库、中创 InforSuite 中间件 V8.2.0、OpenLDAP V2.4.26、曙光、哈工大、计算所、启明星辰和北航等单位

的前端和后端软件都能够在凝思安全操作系统 V6.0.60 上稳定运行。

- 软件包管理机制

凝思安全操作系统 V6.0.60 采用 deb 包管理方式，能够更好地处理软件依赖关系，便于本地管理以及远程升级软件包。

- 网络部署

网络部署模块采用客户端/服务器的网络模式，利用 DHCP/BOOTP 协议从服务器端获得客户端计算机系统的 IP 地址，然后客户端再利用 TFTP 协议从服务器端下载引导程序。这个引导程序为 Network Bootstrap Program (NBP)，引导程序加载凝思安全操作系统 V6.0.60 的安装程序，执行安装程序。安装程序到已经搭建好的凝思安全操作系统 V6.0.60 的安装源中取得各个需要的组件，安装到硬盘，实现通过网络进行部署。支持全自动网络安装，提高大规模部署的工作效率，降低安装出错几率。

- 能量控制

在能量控制研究方面，经过仔细分析计算机中 cpu、硬盘、显卡等硬件的耗电情况，根据实际应用要求，最终确定以控制 cpu 频率、内核节电配置和用内存盘缓存硬盘读写的方案实现能耗的降低。通过方案的实施，达到了相对原有系统能耗降低0.5%的目标。

- 速率优化

在速率优化方面，分别针对 AMD 和 Intel 的体系结构进行了研究。主要在内核中针对不同体系结构的选项进行筛选，在编译系统的过程中，为不同的体系结构配置了不同的编译选项。

- 凝思安全机制

凝思安全操作系统V6.0.60的安全机制继承了原4.2系统安全的优点，并不断创新和完善：

- 强制访问控制 (Mandatory Access Control, 简称MAC)

在4.2系统实现的强制访问控制功能中，强制访问控制策略中的规则是固定的，数据流动需同时满足BLP策略和BIBA 策略。规则固定，主体和客体标签的含义也是固定的，分别代表BLP级别 (category)、BLP类别 (class) 以及BIBA 的完整性级别 (integrity)。而6.0.60系统中实现的强制访问控制的规则是可以配置的，标签的含义也是可以配置的，并且可以配置为完全覆盖4.2系统的强制访问控制机制。另外，与4.2不同的是，6.0.60的标签是全系统的，每个主体或客体都带有标签。

- 强制行为控制 (Mandatory Behavior Control, 简称MBC)

MBC是4.2系统中MEC (Mandatory Execution Control, 强制运行控制) 的增强。MEC是对进程执行系统调用execve进行控制，允许或拒绝进程execve某些

程序文件。MBC在MEC的基础上将控制的行为从执行扩展到读、写、和执行。

– 强制能力控制（Mandatory Capability Control，简称MCC）

MCC利用能力，针对传统UNIX模型进行优化，将特权细分成不同的能力，从而可以避免因挟持特权进程而产生的安全威胁。这和4.2系统的目的是一致的，但是我们采用了完全不一样的实现方式。

关于本书

本书将向您详细介绍使用凝思安全操作系统 V6.0.60 光盘的安装方法，从安装准备之类的基本概念，到步骤分明的安装过程。当您按照本书介绍的步骤安装完毕后，您将会拥有一个功能完全的安全系统。

文档约定

本手册中会有某些字词使用了不一样的字体、样式，规律如下：

- `command`

命令，表示您可以在命令行中输入单词或短语，然后按 `Enter` 键来启用命令。

例如：使用 `cat testfile` 命令来查看当前目录中一个叫 `testfile` 的文件。

- `file name`

文件名、目录名、路径，表示系统中存在着一个叫这个名称的文件或目录。

例如：

- 您的主目录中的 `.bashrc` 文件包括您自用的 `bash shell` 定义和别名。
- `/etc/fstab` 文件包括关于不同系统设备和文件系统的信息。

- `parameter value`

参数及其设定值。

例如：

```
ServerType standalone
```

`ServerType` 定义服务器的启动方式，缺省值为独立方式 `standalone`。

- `script`

脚本。

例如：

```
<Directory />
  Options FollowSymLinks
  AllowOverride None
</Directory>

<Directory "/var/www/htdocs">
```

- **key**

键盘上的按键。

例如：要使用 **Tab** 键补全，输入一个字符然后按 **Tab** 键，您的终端上就会显示目录中起首为那个字符的文件列表。

- **key - combination**

击键的组合方式。

例如：**Ctrl - Alt - Backspace** 击键组合会退出您的图形会话，把您返回到图形登录屏幕或控制台。

- **[Button] 或 <Button>**

这种方式表明它是字符界面窗口中可用的按钮。例如：

移动到 **[Edit]** 上并按 **Enter** 键进入编辑状态。

移动到 **< Yes >** 上并按 **Enter** 键继续。

- **按钮**

这种方式表明它是对话框窗口中可点击的按钮。例如：

点击 **返回** 后退至上一界面。

除此之外，我们还使用几种不同的方式来强调某些信息。按照信息对您的系统的重要程度，它们被标为注意、提示、重要、小心或警告。例如：



注意

切记，凝思安全操作系统区分大小写。换一句话说，rose 不是 ROSE 或 Rose。

**提示**

目录 `/usr/share/doc` 包括了关于您的系统上安装的软件包的附加信息。

**重要**

如果您修改了 DHCP 配置文件，这些改变在您重启 DHCP 守护进程之后才会生效。

**小心**

管理员帐号是用来执行系统管理任务的，执行日常任务请使用一个常规的用户帐号。

**警告**

删除分区操作没有确认过程，会直接将已有分区删除。如果您想撤销该删除操作，只能不将分区结果写入磁盘而直接退出分区界面，然后再重新进入分区界面，但之前的所有分区操作都将丢失。慎用！

术语简介

您会在凝思安全操作系统的文档中经常看到以下这些术语：

- shell

登录 Linux 系统时，系统会为登录用户启动一个程序。通过这个程序，可以和 Linux 进行交互。这个程序就是通常所说的 Linux shell，它的作用就是执行通过键盘输入的命令。

- 命令（Command）

给计算机的命令，多数使用键盘或鼠标输入。

- 命令行（Command line）

在 shell 提示中输入命令的地方。

- shell 提示（shell prompt）

用户和操作系统的命令行界面。shell 解释用户输入的命令，并把它们传递给操作系统。

shell 运行的时候会在屏幕上显示一个提示符，这表示它在等待用户的命令。当输入了命令并按下 `Enter` 键，shell 就开始解释命令并且执行这个命令。如果输入了一个并不存在的命令，shell 也会提示您，并且重新显示提示符，等待输入下一个命令。

- 手册页 (Man page) 和信息页 (Info page)

手册 (Man 是 manual 的简写) 页和信息页提供了关于命令或文件的详细信息 (手册页比信息页提供的解释要简略)。例如，要阅读 `su` 命令的手册页，在 shell 提示下输入 `man su` (或输入 `info su` 来阅读信息页)。要关闭手册页或信息页，按 `q`。

- 根 (Root)

根是在安装中创建的超级用户账号，除非您设置了强制访问控制，否则它对您的系统有完全的访问权。在一般 UNIX/Linux 系统中，您必须登录为根用户来完成某些系统管理任务，如改变管理口令和运行系统配置工具。用户账号的创建目的是使您不必使用根账号来完成普通的用户任务，从而减少永久性损坏您的操作系统或应用程序的机会。

- 终端

终端是一种字符型设备，它有多种类型，通常使用 `tty` 来简称各种类型的终端设备。`tty` 一词源于 Teletypes，或者 teletypewriters，原来指的是电传打字机，是通过串行线用打印机键盘通过阅读和发送信息的东西，后来这东西被键盘与显示器取代，所以现在叫终端比较合适。

- 控制台

控制台是与操作系统交互的设备，系统将一些信息直接输出到控制台上。

在 Linux 系统中，计算机显示器通常被称为控制台终端 (Console)。它仿真了类型为 Linux 的一种终端，并且有一些设备特殊文件与之相关联：`tty0`、`tty1`、`tty2` 等。当您在控制台上登录时，使用的是 `tty1`。使用 `Alt - F1 ~ F6` 组合键时，我们就可以切换到 `tty2`、`tty3` 等上面去。`tty1 ~ tty6` 等称为虚拟终端，而 `tty0` 则是当前所使用虚拟终端的一个别名，系统所产生的信息会发送到该终端上 (这时也叫控制台终端)。因此不管当前正在使用哪个虚拟终端，系统信息都会发送到控制台终端上。您可以登录到不同的虚拟终端上去，因而可以让系统同时有几个不同的会话存在。

- 图形化用户界面 (Graphical User Interface, GUI)

图形化用户界面是指用图形方式显示的计算机操作环境用户接口，包括互动窗口、图标、菜单等，并且允许用户使用鼠标和键盘来启动程序和打开文件等。

- 挂载

linux 操作系统将所有的设备都看作文件，它将整个计算机的资源都整合成一个大

的文件目录。我们要访问存储设备中的文件，必须将文件所在的分区挂载到一个已存在的目录上，然后通过访问这个目录来访问存储设备。

在 linux 操作系统中，挂载是一个非常重要的功能，使用非常频繁。它指将一个设备（通常是存储设备）挂接到一个已存在的目录上。这个目录可以不为空，但挂载后这个目录下以前的内容将不可用。

如何使用本书

本书旨在指导用户安装凝思安全操作系统 V6.0.60，您可以遵循下面的步骤完成凝思安全操作系统 V6.0.60 的安装。

第 1 章 准备工作

本章将向用户介绍在安装凝思安全操作系统 V6.0.60 之前需要的准备工作。

1.1 备份资料

首先建议您将硬盘上的重要数据备份到光盘/磁带上，以免发生意外时给您造成不必要的损失。

1.2 系统兼容性

凝思安全操作系统 V6.0.60 具有良好的软硬件兼容性。

1.2.1 硬件兼容

硬件兼容性在某些情况下很重要。凝思安全操作系统支持主流硬件平台。

凝思安全操作系统 V6.0.60 分为32位和64位，用户可自己选择安装。

凝思安全操作系统 V6.0.60 支持 x86_64、i386、Itanium、PowerPC、SPARC、MIPS等架构的 CPU，IDE、RAID、USB 和 SCSI 控制器，HBA 控制器，nVIDIA、ATI 显卡，能在主流厂商（如曙光、浪潮、联想、华为、宝德等品牌）的服务器、工作站、PC、公共机及笔记本上正常运行。

1.2.2 软件兼容

凝思安全操作系统 V6.0.60 支持人大金仓、达梦、神舟通用等数据库软件，支持永中office、openoffice、WPS等主流办公软件。

1.3 系统需求

凝思安全操作系统 V6.0.60 的最低硬件要求如下：

- CPU

凝思安全操作系统 V6.0.60 可运行于Pentium 4、1GHz以上的计算机上。

- 内存空间

无图形的凝思安全操作系统 V6.0.60 需要64MB以上的内存，推荐使用256MB以上；图形环境需要128MB以上的内存，推荐使用512MB以上。内存空间无上限要求。

- 磁盘空间

几乎每一个现代操作系统（OS）都使用磁盘分区（disk partitions），凝思安全操作系统也不例外。当您安装凝思安全操作系统时，您也得使用磁盘分区。

如果凝思安全操作系统将会与另一个 OS 共享您的系统，您将需要确定在这次安装中您的硬盘驱动器上有足够的可用磁盘空间。

凝思安全操作系统使用的磁盘空间必须和在您的系统上可能安装的其它 OS 所用的磁盘空间分离，如 Windows、OS/2、甚至于不同版本的 Linux。

至少两个分区（/ 和 swap）必须要专用于凝思安全操作系统。

在您开始安装进程之前，必须要满足以下条件之一：

1. 您的计算机必须有足够的未分区¹的磁盘空间来安装凝思安全操作系统。
2. 您必须有一个或多个可以删除的分区，因此能够空出足够的空间来安装凝思安全操作系统。

您可以定制安装凝思安全操作系统，选择安装应用软件包，但基本系统是必需的。

- 基本系统

最基本的没有图形化环境的最小系统，可以独立运行各种不依靠图形界面的程序，不包括各种网络服务，至少需要 500M 空闲空间。

- 应用软件包

您可以根据需要安装所需的软件包，如开发环境、桌面环境及各种服务，完全安装需要 6G 空闲空间。

¹未分区的磁盘空间意味着在您要安装的硬盘驱动器上的可用磁盘空间还没有为数据而划分成块。当您为一个磁盘分区时，每个分区都如同一个独立的磁盘驱动器。



以上数据不包含 swap 分区大小，并且没有把您的用户数据考虑在内。如果您打算在系统上保存用户数据（个人文件），您必须要有额外的可用空间。

现在，您已为安装凝思安全操作系统做好了准备。

第2章 本地安装

本章将指导用户安装凝思安全操作系统。

2.1 安装程序用户界面

凝思安全操作系统 V6.0.60 的安装程序支持两种用户界面：图形界面和字符界面。

2.1.1 图形界面

如果您从前使用过图形化用户界面（graphical user interface, GUI），您对此一进程会比较熟悉；您只需使用鼠标在屏幕间翻阅，点击 **按钮**，或者输入文本字段。您还可以使用 **Tab** 和 **Enter** 键在安装中浏览各屏幕。

2.1.2 字符界面

如果不想或无法使用图形界面的安装程序，您可以使用字符界面的安装程序。

凝思安全操作系统 V6.0.60 字符界面的安装程序使用一个基于屏幕的界面，包括多数通常在图形化用户界面中能够看到的屏幕“构件”。

2.1.2.1 界面构件

下面是一些在字符界面中会显示的最重要的构件：

- 窗口

在整个安装进程中，您会不时地在屏幕上看到窗口（本书中通常把它称为对话框）。有时，一个窗口会重叠在另一个窗口之上；在这种情况下，您只能与最上面的窗口交流。当该窗口使用完毕，它就会消失，允许您继续使用下面的窗口。

- 复选框

复选框允许您选择或取消选择某项功能。框内要么显示一个“*”（已选），要么是一个空格（未选）。当光标位于复选框内，按 **Space** 键来选择一个未选的功能或取消一个已选的功能。

- 文本输入行

文本输入行是您可以输入安装程序所要求信息的区域。当光标停在文本输入行时，您可以在那一行中输入并（或）编辑信息。

- 文本

文本构件是屏幕上用于显示文本的区域。有时，文本构件可能还会含有其它构件，如复选框。如果文本构件所含的信息超出为它保留的空间所能显示的，您可以使用 **↑** 和 **↓** 箭头键来在所有信息中上下滚动。您在文本上的当前位置被显示为一个百分比数字，它会随着您上下滚动文本而变化。

- 滚动条

滚动条出现在窗口的侧面或底部，它用来控制窗框内显示的文档或列表部分。滚动条使您能够轻而易举地查看文件的任意部分。

- 按钮

按钮构件是与安装程序交流的主要方法。通过 **Tab** 键和 **Enter** 键使用这些按钮，您可在安装程序的屏幕中逐步推进。当按钮被突出显示时，它们可以被选择。

另外，光标虽然不是一个构件，但它被用来选择（并联络）某个构件。当光标从一个构件移至另一个构件后，它可能会导致构件改变颜色，或者您可能只会看到光标本身定位在构件内或构件旁。

2.1.2.2 使用键盘来导航

在安装对话框之间的切换是通过一组简单的击键来达到的。要移动光标，使用 **←**、**→**、**↑** 和 **↓** 箭头键。使用 **Tab**、**Shift** - **Tab** 和 **Alt** - **Tab** 键来在屏幕上的每个构件间向前或向后循环。多数屏幕在底部显示了一个可用光标定位键的摘要。

要“按”一个按钮，将光标定位在按钮之上（例如，使用 **Tab** 键），然后按 **Enter** 键。要从一系列项目中选择一项，将光标移至您要选择的项目，然后按 **Space** 键。要选择带复选框的项目，将光标移至复选框内，然后按 **Space** 键来选择这个项目。要取消选择，再按一次 **Space** 键。

**小心**

除非一个对话框在等待您的输入，在安装过程中不要随意按键（这么做可能会导致无法预料的行为）。

2.2 启动安装程序

要开始安装，请确定您已具备安装中将会用到的所有资料，已经一切就绪。

在 BIOS 中设置光盘为第一启动盘，将凝思安全操作系统 V6.0.60 安装光盘放入光驱内，重新启动，将会看到安装界面如图 2.1 所示。



图 2.1: 安装界面

- Install

字符界面安装，详见 2.4。

- Automated install

字符界面的自动安装，将采用默认设置安装凝思安全操作系统 V6.0.60，详见 2.5。

- Graphical install

图形界面安装，详见 2.3。

- Boot harddisk

从硬盘启动，用于已经安装好系统的情况。

- Test memory

内存检测。

Install和Graphical install仅用于默认安装，您也可以使用专家模式进行一些详细设置。选择“Advanced options”，按 `Enter` 进入如图 2.2 所示。



图 2.2: Advanced options

Advanced options 中包含以下安装模式：

- Expert install

字符界面专家安装模式。

- State Grid automated install

电网定制自动安装模式，详见 2.6。

- Rescue mode

救援模式，用于修复系统。

- Dmraid install

如果在主板Bios中设置了Raid，则需要选择此安装模式。

- Graphical expert install
图形界面专家安装模式，详见 2.3。
- Graphical rescue mode
图形界面救援模式。

选择好安装方式，按 键继续。

接下来，您会开始安装系统。字符界面安装步骤与图形界面安装步骤基本一致。

2.3 图形界面安装

本章节包括图形界面普通模式和专家模式的所有步骤，某些步骤只有专家模式才会出现，普通模式安装时可忽略。

专家模式安装从 2.3.1 开始，普通模式安装从 2.3.2 开始。

2.3.1 选择语言（专家模式）

专家模式中，启动安装后，进入画面如图 2.3 所示。选择“Choose language”，然后点击 **Continue** 继续。



图 2.3: Choose language

安装系统将默认使用中文及其时区，然后进入安装程序主菜单。

选择“配置键盘”，然后点击 **继续** 将继续手动安装。



图 2.4: 安装程序主菜单

2.3.2 配置键盘

在进入安装程序前，您还需要手动配置键盘和挂载光盘。选择您想使用的键盘布局，如“美国英语”，点击 **继续**，如图 2.5 所示。



图 2.5: 选择键盘布局区

普通模式中，等待程序探测并挂载光驱等设备，进行下一步安装，详见 2.3.5。专家模式中，还需要手动探测并挂载光盘，详见 2.3.3。



图 2.6: 从光盘加载安全程序组件

2.3.3 探测并挂载光盘（专家模式）

某些PCMCIA硬件需要使用特殊的资源配置选项以正常工作，否则会导致计算机冻结。这些选项将会被添加到 `/etc/pcmcia/config.opts` 中。对于大多数的硬件，您并不需要在此设定任何数值。输入需要的资源配置选项，然后点击 **继续**。



图 2.7: PCMCIA资源范围选项

安装系统将探测并挂载光盘，如图 2.8 所示，点击 **继续**。



图 2.8: 探测并挂载光盘

2.3.4 加载安装程序组件（专家模式）

挂载光盘后，选择“从光盘加载安装程序组件”，然后点击 **继续**。

所有完成安装所必需的组件都将被自动加载，系统将列出可选的安装程序组件，如图 2.9 所示。它们不是必需的，如果您想自己设置某些选项，可以选中对应的组件前的复选框，然后点击 **继续**。



图 2.9: 可选的安装程序组件

安装程序将进入加载的安装程序组件主界面，如图 2.10 所示。



图 2.10: 安装程序组件主界面

之后的安装与普通模式大体一致，安装步骤详见 2.3.5，区别在于更多地方需要手动设置参数，并且每个组件设置完毕后都会返回到安装程序组件主界面。另外，在安装基本系统时可选择要安装的内核，详见 2.3.10。

2.3.5 配置网络

您可以使用 DHCP 对网络进行配置，或者手动输入所有信息，如图 2.11 所示。



图 2.11: 选择网络配置方式

选择“是”并点击 **继续**，安装程序将开始搜索 DHCP 服务器。

如果搜索到了 DHCP 服务器，将自动配置网络参数，并直接进入下一步设置主机名和域名，详见 2.3.5.4。如果未搜索到 DHCP 服务器，将出现提示画面如图 2.12 所示，你可以手动进行网络配置。



图 2.12: 网络自动设置失败

点击 **继续**，进入网络配置界面，如图 2.13 所示。



图 2.13: 配置网络

您可以选择“重新尝试网络自动设置”并点击 **继续**，如果搜索到了 DHCP 服务器，将自动配置网络参数，并直接进入下一步设置主机名和域名。如果未搜索到 DHCP 服务器，仍将出现提示画面如图 ?? 所示。

选择“现在不进行网络设置”，然后点击 **继续** 可以跳过网络设置，并直接进入下一步设置主机名和域名。您可以安装完成后再进入系统设置网路参数。

除此之外，您还可以指定某个 DHCP 服务器来自动配置网络参数，或者手动设置网络参数。

2.3.5.1 指定 DHCP 服务器

选择“使用 DHCP 主机名重试网络自动设置”并点击 **继续**，可以指定使用某个 DHCP 服务器，如图 2.14 所示。



图 2.14: 指定 DHCP 主机名

输入 DHCP 主机名，然后点击 **继续**，如果该 DHCP 服务器可用，将自动配置网络参数，并直接进入下一步设置主机名和域名。如果无法使用该 DHCP 服务器，仍将出现提示画面如图 ?? 所示。

2.3.5.2 手动设置网络

选择“手动进行网络设置”并点击 **继续**，可自行配置 IP 地址、网络掩码、网关、域名服务器地址。

如图 2.15 所示，输入本机 IP 地址，如 192.168.0.1，然后点击 **继续**。



图 2.15: 设置 IP 地址

如图 2.16 所示，输入网络掩码，如 255.255.255.0，然后点击 **继续**。



图 2.16: 设置网络掩码

如图 2.17 所示，输入网关，如 192.168.0.254，然后点击 **继续**。



图 2.17: 设置网关

如图 2.18 所示，输入域名服务器地址，如 192.168.0.254，然后点击 **继续**。



图 2.18: 域名服务器地址

2.3.5.3 确认网络参数

确认当前配置的网络参数是否正确，如图 2.19 所示。如果正确，选择“是”，然后点击 **继续**，进入下一步设置主机名。如果有误，选择“否”，然后点击 **继续**，返回重新设置网络参数。



图 2.19: 确认网络参数



提示

请根据具体情况输入网络参数，如有不明，请咨询您公司的网络管理人员。

网络设置完成，进入下一步设置主机名和域名。

2.3.5.4 设置主机名

输入主机名，点击 **继续**，如图 2.20 所示。



图 2.20: 设置主机名



提示

即便您的计算机不属于任何网络，您也必须为您的系统输入一个主机名！主机名默认为 Linux。

2.3.5.5 设置域名

输入域名，点击 **继续**，如图 2.21 所示。



图 2.21: 设置域名

2.3.6 输入序列号

序列号是凝思用户的服务凭证，如果不输入序列号则在安全内核下不能使用网络相关的功能。请输入16个字符的序列号¹，然后点击 **继续**。



图 2.22: 输入序列号

您也可以在安装时跳过此步骤，登录系统后再输入序列号，如图 ?? 所示。

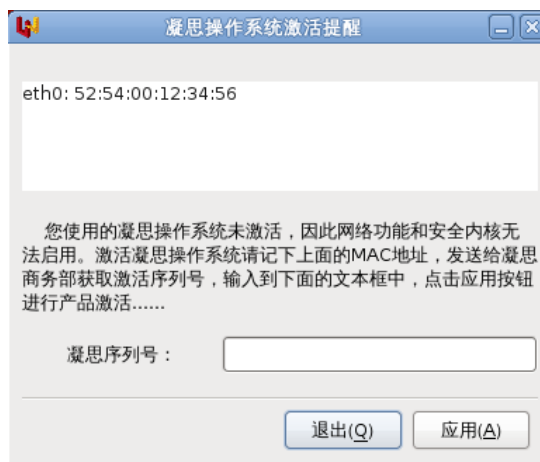


图 2.23: 激活序列号

¹序列号需由北京凝思科技有限公司提供，如有问题，请向技术人员咨询。

2.3.7 设置用户和密码

基本系统安装完毕后，需要设置系统管理员密码。

在专家模式中，您可以选择启用“影子口令”，还可以将系统设置成不允许 root 用户登录，从而使系统更加安全，如图 2.24 所示。

在普通模式中，是默认启用“影子口令”和允许 root 用户登录的。



图 2.24: 启用影子口令

做好选择后，点击 **继续**，设置系统管理员密码，如图 2.25 所示。



图 2.25: 设置系统管理员密码

输入 root 用户密码, 然后点击 **继续**。

在专家模式中，你可以选择是否创建一个普通用户帐号用来执行日常操作，如图 2.26 所示。



图 2.26: 创建普通用户

选择“是”，点击 **继续**，创建普通用户帐号。

在普通模式中会默认需要创建，直接进入下一步。

输入普通用户全名，然后点击 **继续**，如图 2.27 所示。



图 2.27: 设置普通用户全名

输入用户名，然后点击 **继续**，如图 2.28 所示。



图 2.28: 设置用户名

输入用户密码，然后点击 **继续**，如图 2.29 所示。



图 2.29: 设置用户密码

专家模式还需要进行时钟设置，详见 2.3.8，普通模式直接进入磁盘分区设置，详见 2.3.9。

2.3.8 时钟设置（专家模式）

在专家模式中，您可以通过 NTP 来设置系统时钟，选择“是”，点击 **继续**，如图 2.30 所示。



图 2.30: 使用 NTP 设置时钟

输入要使用的 NTP 服务器，如“0.debian.pool.ntp.org”，点击 **继续**，如图 2.31 所示。



图 2.31: 输入 NTP 服务器

安装程序将从 NTP 服务器读取时间，并列出可选的时区，如图 2.32 所示。你可以选择一个时区，点击 **继续**。



图 2.32: 选择时区

2.3.9 磁盘分区

您可以使用向导指导您进行分区操作，也可以手动操作。选择分区方法，点击 **继续**，如图 2.33 所示。



图 2.33: 磁盘分区



提示

即使选择了向导分区，您也可以对分区结果进行修改；选择手动分区也会在每一步给出建议。

根据向导提示进行分区操作如下：

2.3.9.1 选择磁盘

选择要分区的磁盘，点击 **继续**，如图 2.34 所示。



图 2.34: 选择磁盘

2.3.9.2 选择分区方案

选择分区方案，点击 **继续**，如图 2.35 所示。



图 2.35: 分区方案

用户可根据场景、应用的需要定制合适的分区方案。关于凝思安全操作系统的文件和目录结构的说明，详见附录 A。如果您不知道该采取哪种分区方案，可按照向导提供的第一方案进行分区。

- 一个交换分区

交换分区用来支持虚拟内存。换一句话说，当没有足够的内存来贮存您的系统正在处理的数据时，这些数据就被写入交换区。一般来说，您的交换分区的最小值应该相当于您的计算机内存的两倍和 1G 中较大的一个值。

例如，如果您的内存小于等于 1 GB，您的交换分区应是您的系统内存的两倍和 1G 中较大的一个值。如果内存大于 1 GB，建议使用 2 GB 交换区。创建一个有大量空间的交换分区将会在您未来升级内存的时候特别有用。

★ 重要

如果您需要使用休眠功能，则交换分区的大小必须为系统内存的两倍或两倍以上。

• 一个 / 分区

这是“/”（根目录）将被挂载的位置。在这个设置中，所有文件都位于根分区上。对大多数用户来说，只使用这一个分区就可以了。一个大小为 500M 的根分区可以容纳最小的基本系统的安装（只剩极少空闲空间），而一个大小为 6 的根分区将会允许您安装所有软件包。

📌 注意

最小空闲空间没有把您的用户数据考虑在内。如果您打算在系统上保存用户数据（个人文件），您必须要有额外的可用空间。

选择好分区方案后，分区向导将列出分区结果，如图 2.36 所示。



图 2.36: 分区结果

2.3.9.3 修改分区设置

如果对分区结果不满意，可以选择某个分区，然后点击 **继续**，进入该分区设置界面进行修改，如图 2.37 所示。



图 2.37: 分区设置

可修改的分区设置如下：

1. 文件系统

要使分区后的磁盘可用，必须在其上构建文件系统。实际上，可以将这些文件系统看作是文件管理系统，这是因为该称呼正体现了它们的功能：它们通过维护文件上的元数据，使系统上的文件保持状态一致。下面是可选的文件系统及其简要描述：

- Ext2 文件系统

ext2 文件系统支持标准 Unix 文件类型（常规文件，目录，符号链接等）。它还支持长至255个字符的文件名。

- Ext3 日志文件系统

ext3 文件系统是基于 ext2 文件系统之上的，它有一个主要优点——日志。使

用日志文件系统减少了崩溃后恢复文件系统所花费的时间，因为它没有必要运行 fsck² 来检查文件系统。

- Ext4 日志文件系统

ext4 是一种针对 ext3 系统的扩展日志式文件系统，是专门为 Linux 开发的原始的扩展文件系统（ext 或 extfs）的第四版。Linux kernel 自 2.6.28 开始正式支持新的文件系统 Ext4。Ext4 修改了 Ext3 中部分重要的数据结构，可以提供更佳的性能和可靠性，还有更为丰富的功能。

- btrfs 日志文件系统

Btrfs (Butter FS) 是由 Oracle 于 2007 年宣布并进行中的 COW (copy-on-write 式) 文件系统。目标在取代 Linux 的 ext3 文件系统，改善 ext3 的限制，特别是单一文件的大小，总文件系统大小及加入文件校验和。加入目前 ext3/4 未支持的功能，例如可写的磁盘快照 (snapshots)，以及支持递归的快照 (snapshots of snapshots)，内建磁盘阵列 (RAID) 支持，支持子卷 (Subvolumes) 的概念，支持在线调整文件系统大小。

- JFS 日志文件系统

JFS 是 IBM 公司为 linux 系统开发的日志文件系统。如果发生系统崩溃，JFS 提供了快速文件系统重启。通过使用数据库日志技术，JFS 能在几秒或几分钟之内把文件系统恢复到一致状态，而非日志文件系统却要花上几小时甚至几天才能完成。

- XFS 日志文件系统

XFS 是 SGI 开发的高级日志文件系统，XFS 极具伸缩性，非常健壮。所幸的是 SGI 将其移植到了 Linux 系统中。

- FAT16 文件系统

FAT16 使用了 16 位的空间来表示每个扇区 (Sector) 配置文件的情形，故称之为 FAT16。FAT16 支持的分区最大为 2GB。

- FAT32 文件系统

FAT32 是 Windows 系统硬盘分区格式的一种。这种格式采用 32 位的文件分配表，使其对磁盘的管理能力大大增强，突破了 FAT16 对每一个分区的容量只有 2GB 的限制。

- RAID 物理卷

Raid (Redundant Array of Inexpensive Disks) 的用途是将多个硬盘分区合并成一个大的虚拟硬盘，以便优化性能和/或数据安全性。软件 Raid 具有 Raid 系统

²fsck 程序被用来检查文件系统元数据统一性，还可以选用它修复一个或多个 Linux 文件系统。

的优势，并且没有硬件 Raid 控制器的额外成本，但是需要一些 CPU 时间以及内存。

- LVM 物理卷

LVM（Logical Volume Manager）是逻辑盘卷管理，它是 Linux 环境下对磁盘分区进行管理的一种机制。LVM 是在磁盘分区和文件系统之间添加的一个逻辑层，来为文件系统屏蔽下层磁盘分区布局，提供一个抽象的盘卷，在盘卷上建立文件系统。物理卷（physical volume）就是指硬盘分区或从逻辑上与磁盘分区具有同样功能的设备（如 RAID），是 LVM 的基本存储逻辑块，但和基本的物理存储介质（如分区、磁盘等）比较，却包含有与 LVM 相关的管理参数。

- 交换空间

交换分区（swap）被用于支持虚拟内存。换一句话说，如果存放您的系统正在处理的数据所需的内存不够时，这些数据就会被写到您的交换分区上。

除此之外，您还可以选择“要加密的物理卷”。加密分区可像普通分区一样被使用，如建立文件系统，建立物理卷等。

如图 2.38 所示，选择好分区类型，然后点击 **继续**，返回上一界面。



图 2.38: 分区类型

2. 挂载点

您可以选择列出的挂载点，如图 2.39 所示，或者手动输入一个挂载点，然后点击 **继续**，返回上一界面。



图 2.39: 挂载点

3. 挂载选项

挂载选项可以调节文件系统的行为。如图 2.40 所示，点击各选项前的复选框，选择挂载选项，然后点击 **继续**，返回上一界面。



图 2.40: 挂载选项

4. 标识

输入该分区文件系统的标识，如图 2.41 所示，然后点击 **继续**，返回上一界面。



图 2.41: 分区标识

5. 保留块

设置文件系统保留给超级用户的磁盘容量百分比，以免磁盘空间被占满了系统无法正常运行。

输入百分比，如图 2.42 所示，然后点击 **继续**，返回上一界面。



图 2.42: 磁盘保留块

6. 典型用途

指定文件系统的用途，安装程序将根据用途指定优化的文件系统参数。

- 标准：标准参数
- news：每4KB block分配一个inode
- largefile：每1M分配一个inode
- largefile4：每4M分配一个inode

如图 2.43 所示，选择文件系统用途，然后点击 **继续**，返回上一界面。



图 2.43: 典型用途

7. 可启动标志

选择“可启动标志”，然后点击 **继续**，该参数将在“开”和“关”之间进行切换。“可启动标志”设置为“开”，则该分区为启动分区。

2.3.9.4 复制分区

选择“将另一分区的数据复制到此处”，然后点击 **继续**，可以复制分区，如图 2.44 所示。



图 2.44: 复制分区

选择“是”，然后点击 **继续** 确认进行复制操作；选择“否”，然后点击 **继续** 撤销复制操作并返回上一界面。

2.3.9.5 删除分区

选择“删除此分区”，然后点击 **继续**，可删除该分区并返回上一界面。

设置结束后，选择“分区设定结束”，然后点击 **继续**，返回上一界面。

2.3.9.6 撤销修改

要恢复修改之前的分区设置，选择“撤销对分区设置的修改”，然后点击 **继续** 撤销修改。

2.3.9.7 确认分区

确认分区结果后，选择“分区设定结束并将修改写入磁盘”，然后点击 **继续**，确认将分区结果写入磁盘，如图 2.45 所示，选择“是”，点击 **继续**，分区结果将写入磁盘。



图 2.45: 确认分区

**注意**

分区结果要写入磁盘才会生效！没有执行写入操作而直接退出将丢失分区结果。

2.3.9.8 配置 LVM

Linux 用户安装 Linux 操作系统时遇到的一个最常见的难以决定的问题就是如何正确地给评估各分区大小，以分配合适的硬盘空间。而遇到出现某个分区空间耗尽时，解决的方法通常是使用符号链接，或者使用调整分区大小的工具（如 PartitionMagic），但这都只是暂时解决办法，没有根本解决问题。LVM 技术使得用户在无需停机的情况下方便地调整各个分区大小。

通过 LVM，系统管理员可以轻松管理磁盘分区，如：将若干个磁盘分区连接为一个整块的卷组（volume group），形成一个存储池。管理员可以在卷组上随意创建逻辑卷组（logical volumes），并进一步在逻辑卷组上创建文件系统。管理员通过 LVM 可以方便的调整存储卷组的大小，并且可以对磁盘存储按照组的方式进行命名、管理和分配，例如按照使用用途进行定义：“development”和“sales”，而不是使用物理磁盘名“sda”和“sdb”。而且当系统添加了新的磁盘，通过 LVM 管理员就不必将磁盘的文件移动到新的磁盘上以充分利用新的存储空间，而是直接扩展文件系统跨越磁盘即可。

分区操作与 2.3.9.1 相似，只是选择分区方案后需要确认配置 LVM，如图 2.46 所示。



图 2.46: 配置LVM

选择“是”，然后点击 **继续** 确认配置 LVM，分区向导将列出分区结果，如图 2.47 所示。



图 2.47: LVM 分区

2.3.9.9 配置加密的 LVM

使用此分区向导进行分区，分区操作与 2.3.9.8 相似，但在确认配置 LVM 后，将会要求用户输入加密口令，如图 2.48 所示。



图 2.48: 加密分区

输入加密口令后，点击 **继续** 确认，分区向导将列出分区结果，如图 2.49 所示。



图 2.49: 加密的 LVM 分区

2.3.9.10 手动分区

除此之外，你还可以选择手动分区。

选择要分区的磁盘，然后点击 **继续** 开始分区。

1. 创建分区您可以选择“显示柱面/磁头/扇区信息”查看磁盘信息，然后再进行分区，或者选择“对空闲空间进行自动分区”，与向导分区一样自动分区。如果想手动输入参数，请选择“创建新分区”，然后点击 **继续**，如图 2.50 所示。



图 2.50: 创建分区

- 2. 设置分区大小您需要指定分区大小，有多种表示方式可以选择，如容量、最大空间的百分比、最大空间。

输入分区大小，然后点击 **继续**，如图 2.51 所示。



图 2.51: 输入分区大小

3. 设置分区类型选择“主分区”或“逻辑分区”，然后点击 **继续**，如图 2.52 所示。

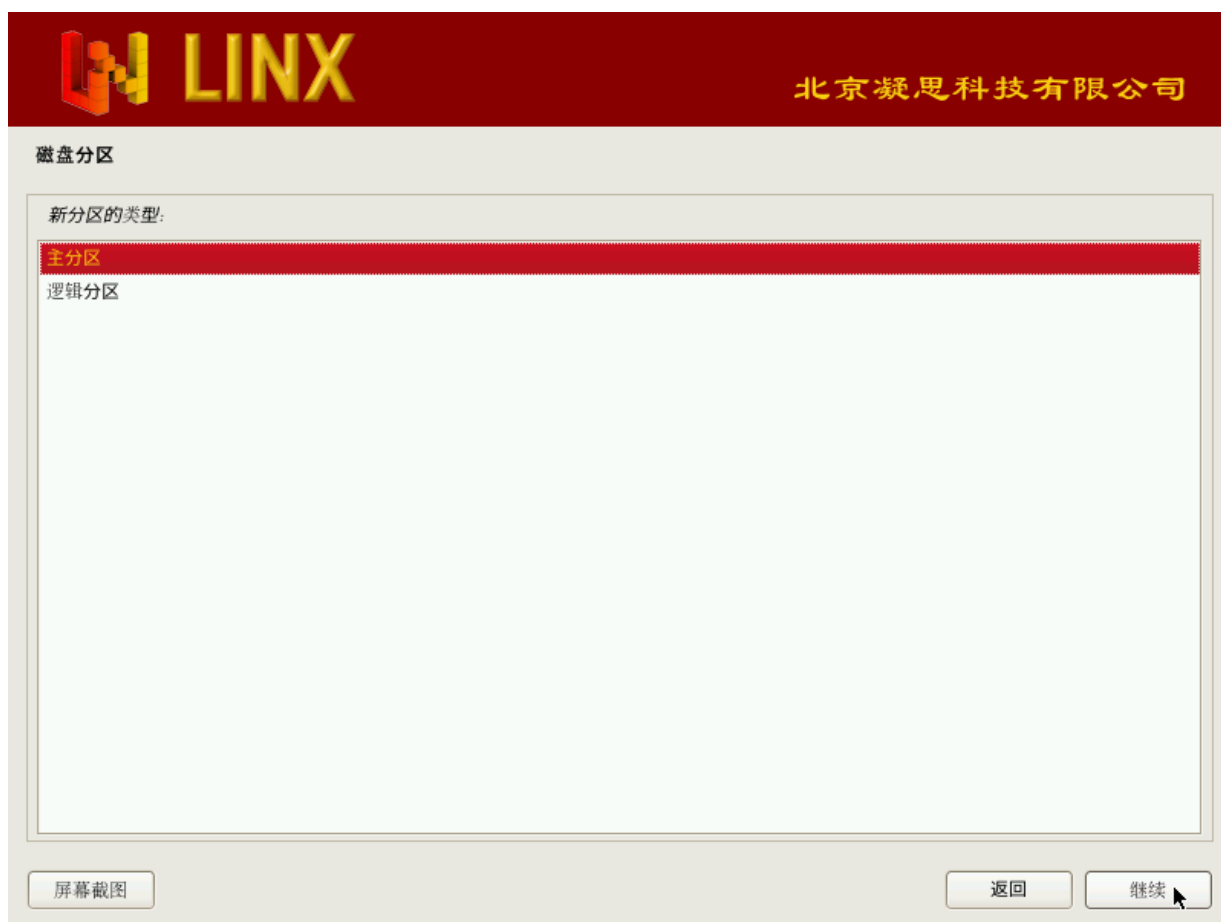


图 2.52: 选择分区类型

4. 新分区的位置选择从磁盘的“开始”或“结束”来划分此分区，然后点击 **继续**，如图 2.53 所示。



图 2.53: 选择新分区的位置

5. 分区设置安装程序已给出默认设置，您可以修改分区设置，操作与 2.3.9.3 相同。

2.3.9.11 配置软 Raid

Raid (Redundant Array of Inexpensive Disks) 的用途是将多个硬盘分区合并成一个大的虚拟硬盘, 以便优化性能和/或数据安全性。软件 Raid 具有 Raid 系统的优势, 并且没有硬件 Raid 控制器的额外成本, 但是需要一些 CPU 时间以及内存。

Raid 具有将多块硬盘合成一个 Raid 系统的多种策略, 这些策略的目标、优点及特点各不相同。这些变化形式通常称作 Raid 级别。

凝思安全操作系统 V6.0.60 中可采用的 Raid 级别如下:

- RAID 0

此级别通过将每个文件按块分放到多个磁盘驱动器上, 提高了数据访问性能。这实际上并不是真正的 RAID, 因为它未提供数据备份, 但 RAID 0 已成为这种类型的系统的标准名称。使用 RAID 0 可以将两块或多块硬盘组合在一起。这样性能固然很好, 但如果有任何一块硬盘出现故障, 都将损坏 RAID 系统并丢失数据。

- RAID 1

此级别为数据提供了充分的安全性, 因为它将数据按 1:1 复制到另一块硬盘上。这种方法称为硬盘镜像。如果一块磁盘损坏, 则可以使用另一块磁盘上的内容副本。在所有这些硬盘上, 只要有一块硬盘没有损坏, 您的数据就不会丢失。但是, 如果没有检测到损坏, 已损坏的数据镜像到正确的磁盘仍有可能发生, 从而导致数据损坏。与使用单个磁盘访问时相比, 写性能在复制进程中稍有损失 (慢 10% 到 20%), 但读访问的速度要大大快于任何一块普通物理硬盘, 原因是数据进行了复制, 从而可以并行扫描它们。一般来讲, 使用级别 1 读的速率几乎是使用单个磁盘时的两倍, 而写的速率与使用单个磁盘时相差无几。

- RAID 5

RAID 5 是级别 0 和级别 1 在性能和冗余方面经优化后的折衷方案。可以采用的最大硬盘空间等于使用的磁盘数减 1 乘以容量最小的磁盘容量。数据分布在这些硬盘上, 这一点与 RAID 0 相同。但出于安全原因, 在其中一个分区上创建了奇偶校验块。这些块通过 XOR 相互链接, 并在系统出现故障时, 通过启用相同的校验块重构造内容。对于 RAID 5, 在同一时间只能有一块硬盘出现故障。如果一块硬盘出现故障, 则必须尽快将其更换, 以防止丢失数据。

- RAID 6

RAID 6 技术是在 RAID 5 基础上, 为了进一步加强数据保护而设计的一种 RAID 方式, 实际上是一种扩展 RAID 5 等级。与 RAID 5 的不同之处在于除了每个硬盘上都有同级数据 XOR 校验区外, 还有一个针对每个数据块的 XOR 校验区, 因此 RAID 6 的数据冗余性能相当好。但是, 由于增加了一个校验, 所以写入的效率较 RAID 5 还差, 而且控制系统的设计也更为复杂, 第二块的校验区也减少了有效存储空间。

- RAID 10

Raid 0 的高速+ Raid 1 的安全。复数的外部存储装置 (harddisk) 作为一台装置使用。首先理解一下 Raid 0, 所有数据分成两部分存在多个硬盘上, I/O 符合分散导致读写 (I/O) 变快, 所以高速。然后, 这多个硬盘采用 Raid 1 (镜像), 也就是说上面说的每个硬盘都可以看成一个 set, 每个 set 包含复数个硬盘, 里面存的相同的内容, 是谓镜像。

常用的 Raid 级别是0、1、5这三个, 表 2.1 是对这三个 Raid 级别的比较。

表 2.1: Raid 级别比较

Raid 级别	Raid 0	Raid 1	Raid 5
别名	条带	镜像	分布奇偶位条带
容错性	没有	有	有
冗余类型	没有	复制	奇偶校验
热备盘选项	没有	有	有
读性能	高	低	高
随机写性能	高	低	高
连续写性能	高	低	低
需要的磁盘数	一个或多个	只需2个或 $2 \times N$ 个	三个或更多
可用容量	总的磁盘的容量	只能用磁盘容量的50%	$(n - 1)/n$ 的总磁盘容量, 其中 n 为磁盘数
典型应用	无故障的迅速读写, 要求安全性不高, 如图形工作站等。	随机数据写入, 要求安全性高, 如服务器、数据库存储领域。	随机数据传输要求安全性高, 如金融、数据库、存储等。

当划分了 Raid 分区后，分区信息上将出现“软件 RAID 设置”，如图 2.54 所示。



图 2.54: 软件 RAID 设置

选择“软件 RAID 设置”，然后点击 **继续** 至确认界面，选择“是”并点击 **继续** 确认配置 Raid，如图 2.55 所示。



图 2.55: 确认配置 Raid

1. 创建 MD 设备

选择“创建 MD 设备”，然后点击 **继续**，如图 2.56 所示。



图 2.56: 盘组配置

选择 RAID 级别，然后点击 **继续**，如图 2.57 所示。



图 2.57: 盘组设备类型

不同 Raid 级别代表着不同的存储性能、数据安全性和存储成本。Raid 级别的选择有三个主要因素：可用性（数据冗余）、性能和成本。如果不要求可用性，选择 Raid 0 以获得最佳性能。如果可用性和性能是重要的而成本不是一个主要因素，则根据硬盘数量选择 Raid 1。如果可用性、成本和性能都同样重要，则根据一般的数据传输和硬盘的数量选择 Raid 5，参见表 2.1。

除Raid 0之外，其它几个级别要使用不止一个分区，Raid 1和Raid 10是2个及以上（需双数），Raid 5是3个及以上，Raid 6是4个及以上。

输入活跃设备的个数，然后按 键，如图 2.58 所示。



图 2.58: Raid阵列中活跃设备的个数

当活跃设备出故障时，将启用备用设备。

输入备用设备的个数，然后按 `Enter` 键，如图 2.59 所示。



图 2.59: Raid阵列中备用设备的个数

根据设置的设备个数，选择活跃的 RAID 分区，然后点击 **继续**，如图 2.60 所示。



图 2.60: 选择活跃的 RAID 分区

根据设置的设备个数，选择备用的 RAID 分区，然后点击 **继续**，如图 2.61 所示。



图 2.61: 选择备用的 RAID 分区

创建完成后返回盘组配置界面。

2. 删除 MD 设备

选择“删除 MD 设备”，然后点击 **继续** 至选择界面，如图 2.62 所示，选择要删除的 MD 设备，然后点击 **继续**。



图 2.62: 删除 MD 设备

确认界面如图 2.63 所示，选择“是”，然后点击 **继续** 确认删除。



图 2.63: 确认删除 MD 设备

删除完成后返回盘组配置界面。

3. 配置完成

配置完成后，在盘组配置界面选择“完成”，然后点击 **继续** 完成 RAID 配置并返回分区列表，如图 2.64 所示。



图 2.64: 完成 RAID 配置

您还可以修改这个 RAID 设备的分区设置，详见 2.3.9.3。

2.3.10 安装基本系统

确认分区操作完成后，分区结果将被写入磁盘并格式化分区，然后开始安装基本系统，安装的快慢要依据您的计算机的运行速度而定，如图 2.65 所示。



图 2.65: 安装基本系统

普通模式直接进入 2.3.11，专家模式还要进行下面的设置。

如果选择了专家模式进行安装，在安装基本系统的时候会让用户选择所要安装的内核，如图 2.66 所示。



图 2.66: 安装内核

可选择的内核如下

- linux-image-2.6-amd64
默认安装的内核，即 linux-image-2.6.32.5-linx-amd64
- linux-image-2.6.32.5-linx-amd64
凝思安全内核，具有凝思安全功能。
- linux-image-2.6.32.5-linxcompute-amd64
不包含 cgroup 的凝思安全内核。

选择要安装的内核，然后点击 **继续**。

您还需要选择将包含在 initrd 里的驱动程序，如图 2.67 所示。



图 2.67: 选择驱动程序

您可以选择包含所有的驱动程序，或者只包含此系统需要的驱动程序，然后点击 **继续**。

2.3.11 配置软件包管理器

配置软件包源，可用于安装或升级软件包，您可以插入CD或DVD并选择“是”进行扫描，作为配置软件包源，如图 2.68 所示。



图 2.68: 扫描CD或DVD

或者使用网络镜像，如图 2.69 所示。



图 2.69: 网络镜像

选择“否”，然后点击 **继续**，转至下一步；选择“是”，然后点击 **继续**，配置网络镜像。

选择文件下载的协议，选择“http”或“ftp”，然后点击 **继续**，如图2.70 所示。



图 2.70: 选择文件下载的协议

安装程序将列出可用的网络镜像，您可以选择一个网络镜像或者选择“手动输入信息”，然后手动输入某个镜像的主机名和镜像所在的目录，如图2.71所示。



图 2.71: 选择镜像

输入镜像的主机名和目录，然后点击 **继续**，如图2.72 所示。



图 2.72: 输入镜像的主机名和目录

如果需要使用代理来连接外部网络，输入 HTTP 代理信息，否则请空置，如图 2.73 所示，然后点击 **继续**。



图 2.73: 输入 HTTP 代理信息

设置了正确的网络镜像后，即可使用该网络镜像进行软件包的安装、升级，否则需要重新设置或选择不使用网络镜像。



图 2.74: 加载软件选择组件

安装程序将加载软件选择组件，进入软件包选择界面。

2.3.12 选择应用软件包

在之前的安装过程中，已安装了基本系统，这里可以定制安装应用软件包，如桌面环境和各种服务。



图 2.75: 选择应用软件包

可供选择的软件集如下：

- 服务器运行环境

包括Web 服务器、打印服务器、DNS 服务器、文件服务器、邮件服务器、SQL 数据库、SSH 服务器所需软件。

- Web 服务器

WEB 服务器也称为 WWW (WORLD WIDE WEB) 服务器，主要功能是提供网上信息浏览服务。WWW 是 Internet 的多媒体信息查询工具，是 Internet 上近年才发展起来的服务，也是发展最快和目前用的最广泛的服务。正是因为有了 WWW 工具，才使得近年来 Internet 迅速发展，且用户数量飞速增长。

凝思安全操作系统 V6.0.60 提供了 Apache 等软件。

- 打印服务器

打印服务器提供简单而高效的网络打印解决方案。一端连接打印机，一端连接网络(交换机)，打印机在网络中的任何位置，都能够很容易地为局域网内所有用户提供打印。

凝思安全操作系统 V6.0.60 提供了 cups 等软件。

– DNS 服务器

DNS 服务器是 (Domain Name System 或者 Domain Name Service) 域名系统或者域名服务,域名系统为 Internet 上的主机分配域名地址和 IP 地址。用户使用域名地址,该系统就会自动把域名地址转为 IP 地址。域名服务是运行域名系统的 Internet 工具。执行域名服务的服务器称之为 DNS 服务器,通过 DNS 服务器来应答域名服务的查询。

凝思安全操作系统 V6.0.60 提供了 bind9 等软件。

– 文件服务器

文件服务器的功能就是向服务器提供文件。它加强了存储器的功能,简化了网络数据的管理。它一则改善了系统的性能,提高了数据的可用性,二则减少了管理的复杂程度,降低了运营费用。

凝思安全操作系统 V6.0.60 提供了 nfs、samba 等软件。

NFS 是 Network File System 的简写,即网络文件系统。网络文件系统是 FreeBSD 支持的文件系统中的一种。NFS 允许一个系统在网络上与他人共享目录和文件。通过使用 NFS,用户和程序可以像访问本地文件一样访问远端系统上的文件。

Samba 是在 Linux 和 UNIX 系统上实现 SMB 协议的一个免费软件,由服务器及客户端程序构成。SMB(Server Message Block)协议,或者称之为 NETBIOS/LanManager 协议,通常是用来实现磁盘和打印机共享。

– 邮件服务器

邮件服务器提供邮件系统服务,包括邮件发送和接收。

凝思安全操作系统 V6.0.60 提供了 exim4、procmail 等软件。

– SQL 数据库

数据库 (Database) 是按照数据结构来组织、存储和管理数据的仓库,它产生于距今五十年前,随着信息技术和市场的发展,特别是二十世纪九十年代以后,数据管理不再仅仅是存储和管理数据,而转变成用户所需要的各种数据管理的方式。数据库有很多种类型,从最简单的存储有各种数据的表格到能够进行海量数据存储的大型数据库系统都在各个方面得到了广泛的应用。

SQL (Structured Query Language) 结构化查询语言,是一种数据库查询和程序设计语言,用于存取数据以及查询、更新和管理关系数据库系统。

凝思安全操作系统 V6.0.60 提供了 postgresql 软件。

– SSH 服务器

SSH (Secure Shell) 是以远程联机服务方式操作服务器时的较为安全的解决方案。SSH 是一个用来替代 TELNET、FTP 以及 R 命令的工具包，主要是想解决口令在网上明文传输的问题。

凝思安全操作系统 V6.0.60 提供了 openssh 软件。

• 图形工作站

包括 GNOME 桌面环境和 KDE 桌面环境。

GNOME 是 The GNU Network Object Model Environment 的缩写，意思是 GNU 网络对象模型环境。GNOME 桌面是一个基于非 Qt 库的桌面系统，目标是基于自由软件，为 Unix 或者类 Unix 操作系统构造一个功能完善、操作简单以及界面友好的桌面环境。

KDE 是 K 桌面环境 (Kool Desktop Environment) 的缩写。一种著名的运行于 Linux、Unix 以及 FreeBSD 等操作系统上面自由图形工作环境，整个系统采用的都是 TrollTech 公司所开发的 Qt 程序库。KDE 包含许多应用程序用于协助您的日常工作。

GNOME 和 KDE 都是 Linux 操作系统上最流行的桌面环境系统。

• 办公套件

包括 OpenOffice.org 等办公软件。

• 开发环境

包括基本的系统工具，建议安装。

选中软件集前的复选框，然后点击 **继续**，开始安装应用软件包，安装的快慢要依据您所选择的软件包数量和您的计算机的运行速度而定，如图 2.76 所示。



图 2.76: 安装应用软件包

在安装软件的过程中，您还需要手动配置一些参数。

2.3.13 配置服务器参数

如果您选择了安装“服务器运行环境”，将安装 MySQL、Samba、ProFTPd、Postfix 等服务，安装过程中还需要进行一些设置。

2.3.13.1 设置 MySQL 管理员口令

如果您选择了安装“服务器运行环境”，将安装 MySQL 数据库软件，建议您在安装过程中设置 MySQL 管理员口令，如图 2.77 所示。



图 2.77: 设置MySQL管理员口令

再次输入 MySQL 管理员口令，点击 **继续**。



图 2.78: 重复MYSQl管理员口令

2.3.13.2 配置 Samba 服务

如果您选择了安装“服务器运行环境”，安装文件服务器软件，需要配置 Samba 服务，如图 2.79 所示。



图 2.79: 配置 Samba 服务

输入工作组名称，然后点击 **继续**。

2.3.13.3 配置 FTP 服务

如果您选择了安装“服务器运行环境”，安装文件服务器软件，需要配置 ProFTPd 服务，如图 2.80 所示。



图 2.80: 配置 FTP 服务

选择ftp工作方式，然后点击 **继续**。

2.3.13.4 配置 Postfix 服务

如果您选择了安装“服务器运行环境”，将安装 Postfix 邮件服务器，需要配置 Postfix 服务，如图 2.81 所示。



图 2.81: 配置 Postfix 服务

选择默认的邮件类型，然后点击 **继续**。



图 2.82: 配置系统邮件名称

输入系统邮件名称，，然后点击 **继续**。

2.3.14 安装 GRUB

软件包安装完毕后，还将安装 GRUB。



图 2.83: 安装 GRUB

您可以选择将GRUB安装到主引导记录（MBR）上，选择“是”，然后点击 **继续**，如图 2.83 所示。

或者选择“否”，然后手动设置引导分区，如图 2.84 所示。



图 2.84: 手动设置引导分区

输入要安装GRUB的分区，然后点击 **继续**。



小心

如果该计算机上存在其它操作系统，安装 GRUB 可能会影响到其它操作系统的启动。

然后将开始安装 GRUB，安装的快慢要依据您的计算机的运行速度而定，如图 2.85 所示。



图 2.85: 安装 GRUB

2.3.15 安装完成

安装程序将保存设置，结束安装进程，如图 2.86 所示。



图 2.86: 结束安装进程

等待安装程序自动调整一些设置后，安装完成，如图 2.87 所示，点击 **继续** 将重启计算机。请取出光盘，并确认从硬盘启动系统。关于系统如何使用请阅读《凝思安全操作系统 V6.0.60 用户手册》。



图 2.87: 安装完成

2.3.16 中止安装

安装过程中，如果您想退出安装，可以按 **ESC** 退出当前界面到安装程序主菜单，如图 2.88 所示。



图 2.88: 中止安装

下拉滚动条，选择“中止安装”，然后点击 **继续**，转至中止安装确认界面，如图 2.89 所示。



图 2.89: 确认退出

选择“是”，然后点击 **继续** 即可退出安装；选择“否”，然后点击 **继续** 可返回安装程序主菜单，然后选择某个安装步骤，再点击 **继续** 继续安装系统。

2.4 字符界面安装

在启动界面选择“Install”，按 键，将进入字符界面安装模式，安装程序将读取光盘，加载安装组件，如图 2.90、2.91 所示。

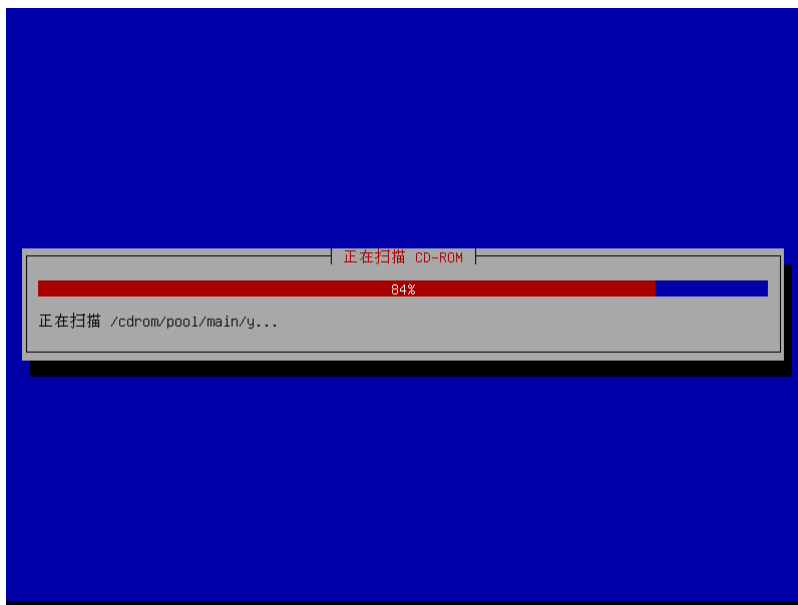


图 2.90: 扫描CD-ROM



图 2.91: 加载安装组件

加载完毕后，将进入网络配置界面。

2.4.1 配置网络

安装程序将默认使用DHCP自动配置网络，如图 2.92、2.93 所示。

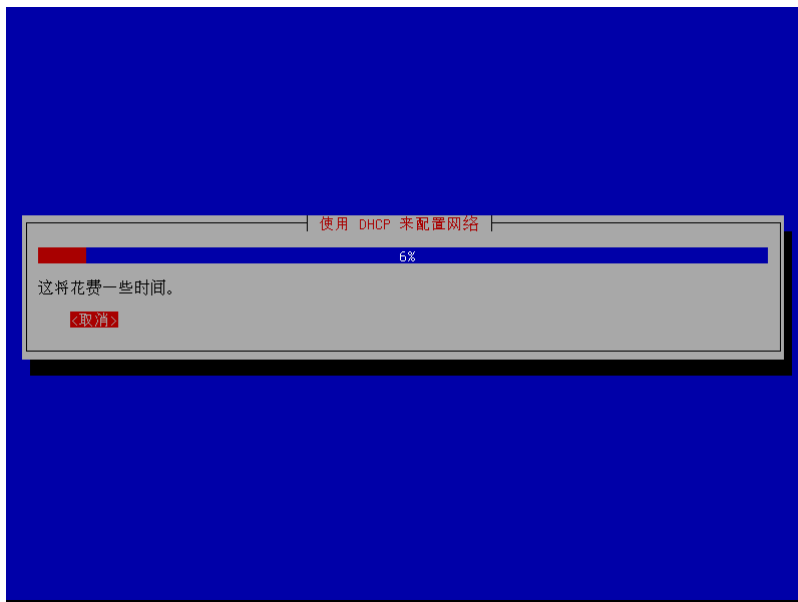


图 2.92: 使用DHCP配置网络

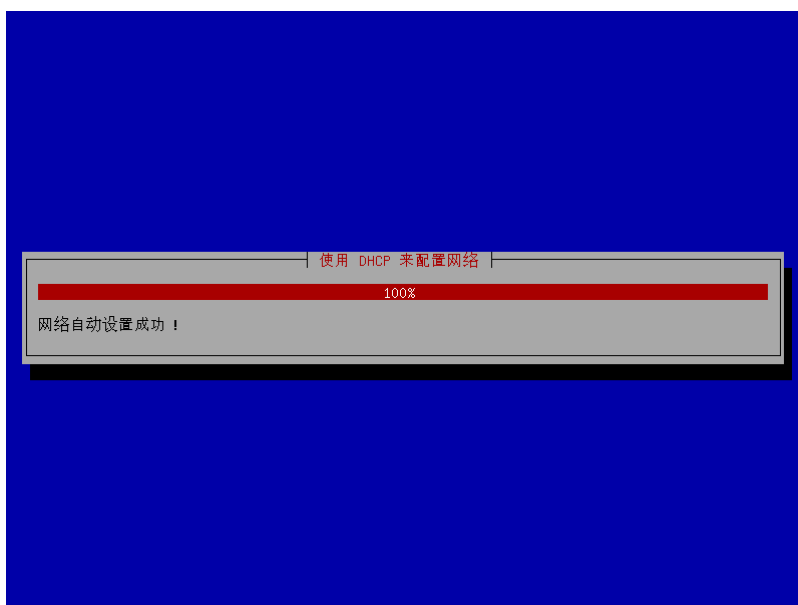


图 2.93: 网络自动设置成功

如果自动设置失败，您可以尝试重新设置，或者手动输入所有信息，如图 2.94 所示。

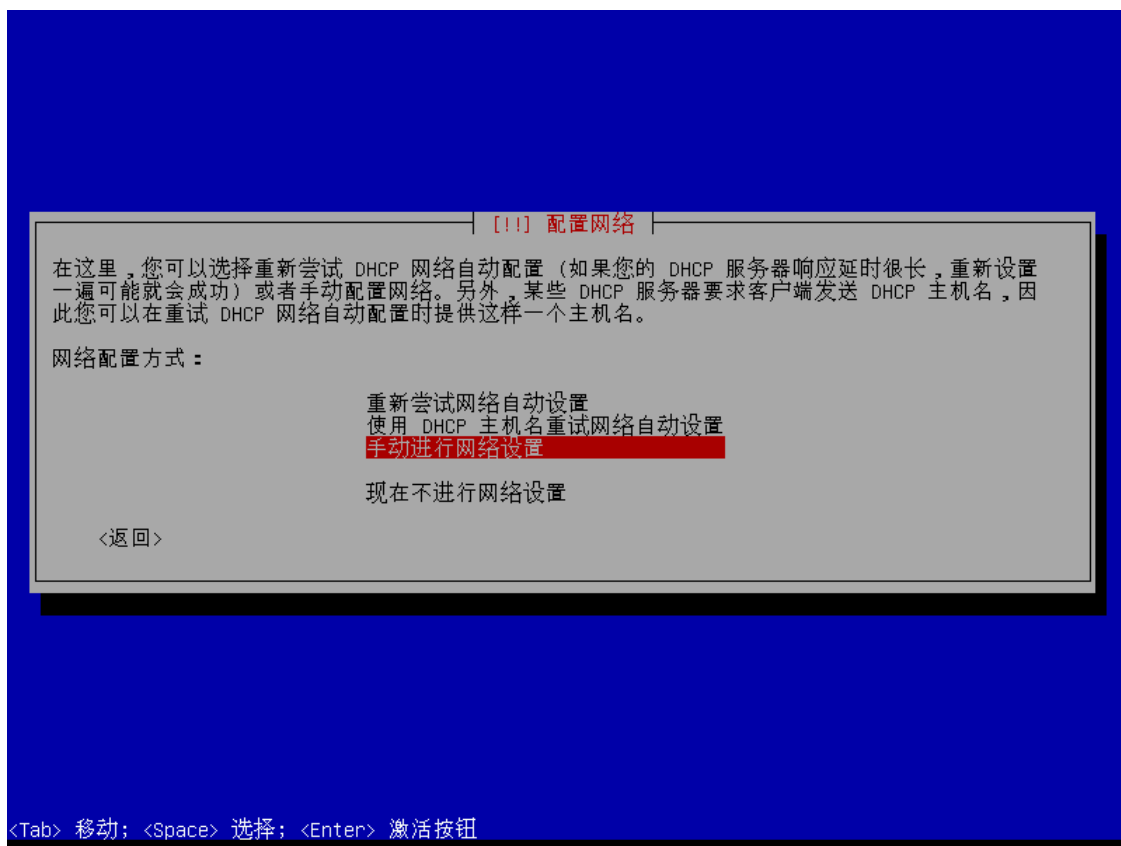


图 2.94: 选择网络配置方式

您可以选择“重新尝试网络自动设置”，如果搜索到了 DHCP 服务器，将自动配置网络参数，并直接进入下一步设置主机名和域名。如果未搜索到 DHCP 服务器，将出现提示画面。

您也可以选择“使用 DHCP 主机名重试网络自动设置”，然后指定某个 DHCP 服务器来自动配置网络参数，或者手动设置网络参数。

除此之外，选择“现在不进行网络设置”，可以跳过网络设置，并直接进入下一步设置主机名和域名。您可以安装完成后再进入系统设置网路参数。

2.4.1.1 使用DHCP主机名重试网络自动设置

某些DHCP服务器要求客户端发送DHCP主机名，您可以尝试设置DHCP主机名，完成网络自动配置，如图 2.95 所示。



图 2.95: 设置DHCP主机名

输入DHCP主机名，选择“继续”并按 `Enter` 键，安装程序将开始搜索 DHCP 服务器。

如果搜索到了 DHCP 服务器，将自动配置网络参数，并直接进入下一步设置主机名和域名，详见 2.4.1.3。如果未搜索到 DHCP 服务器，您还可以手动网络配置。

2.4.1.2 手动设置网络

选择“手动进行网络设置”并按 键，可自行配置 IP 地址、网络掩码、网关、域名服务器地址。

如图 2.96 所示，输入本机 IP 地址，如 192.168.0.1，然后按 键。



图 2.96: 设置 IP 地址

如图 2.97 所示，输入网络掩码，如 255.255.255.0，然后按 **Enter** 键。

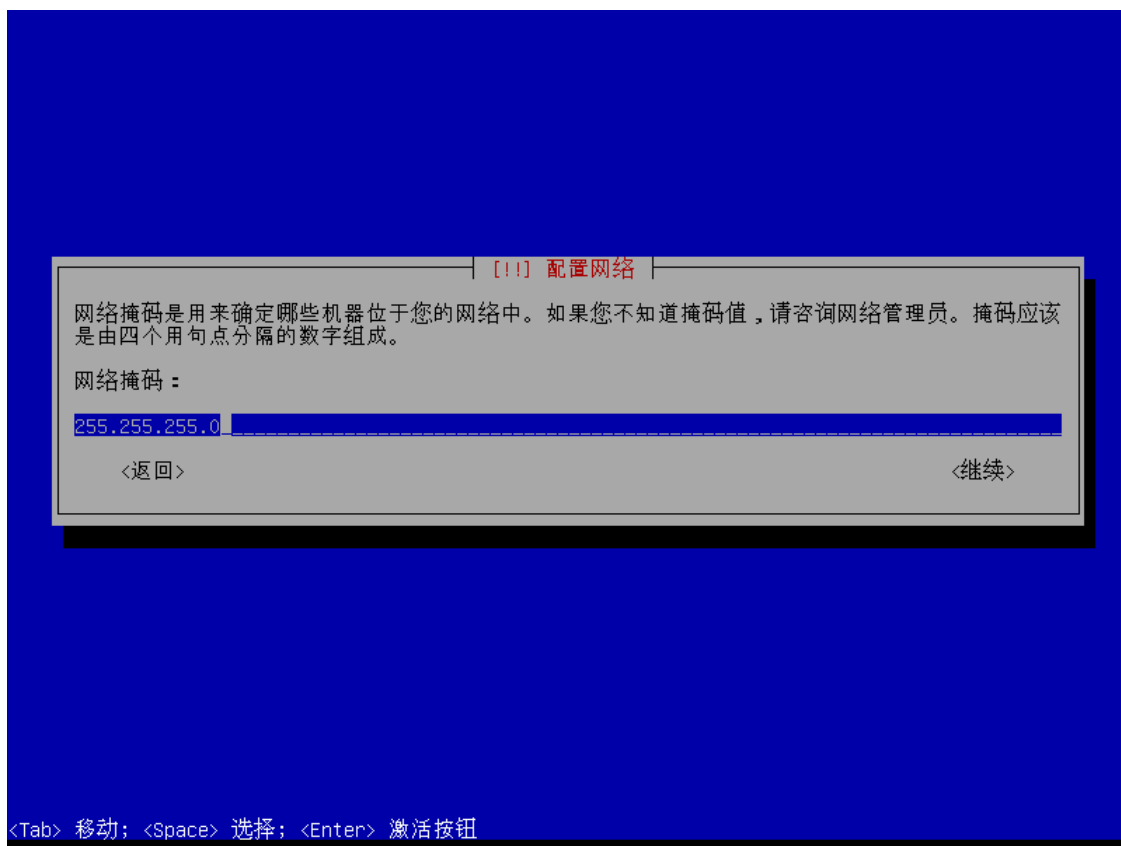


图 2.97: 设置网络掩码

如图 2.98 所示，输入网关，如 192.168.0.254，然后按 **Enter** 键。

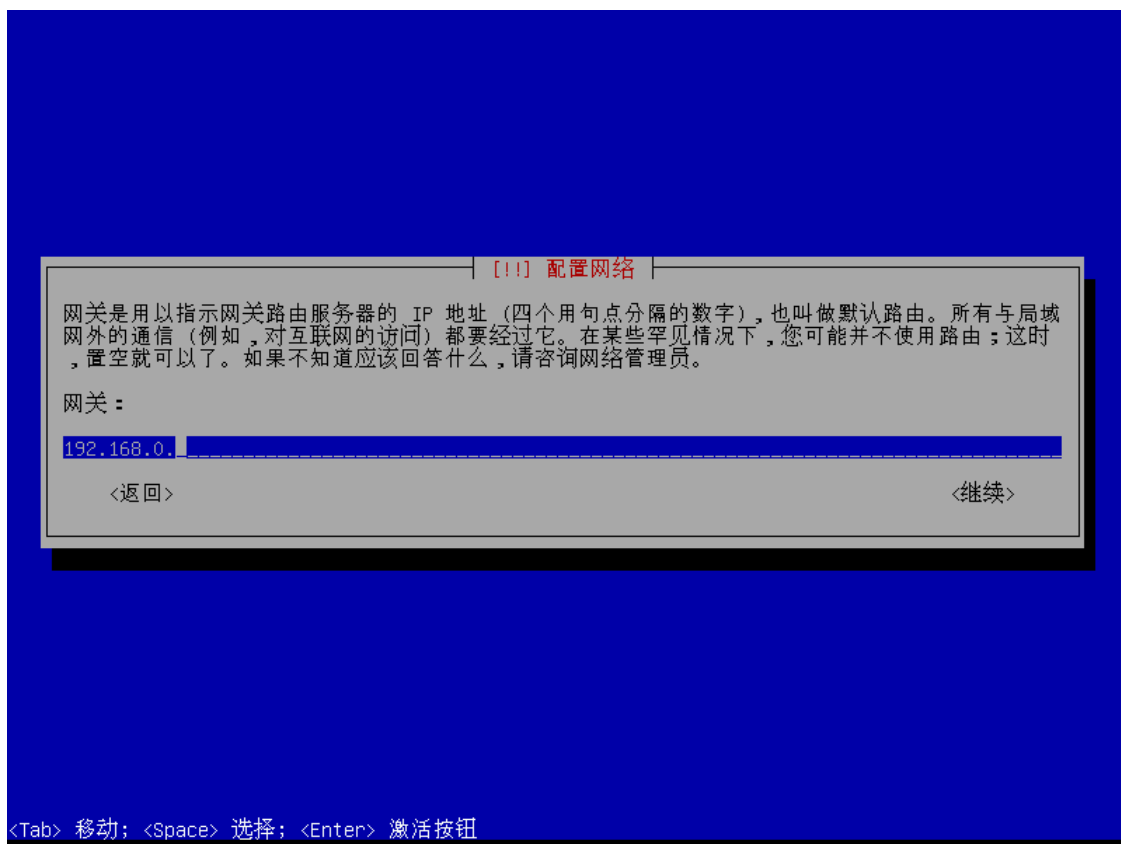


图 2.98: 设置网关

如图 2.99 所示，输入域名服务器地址，如 192.168.0.254，然后按 **Enter** 键。

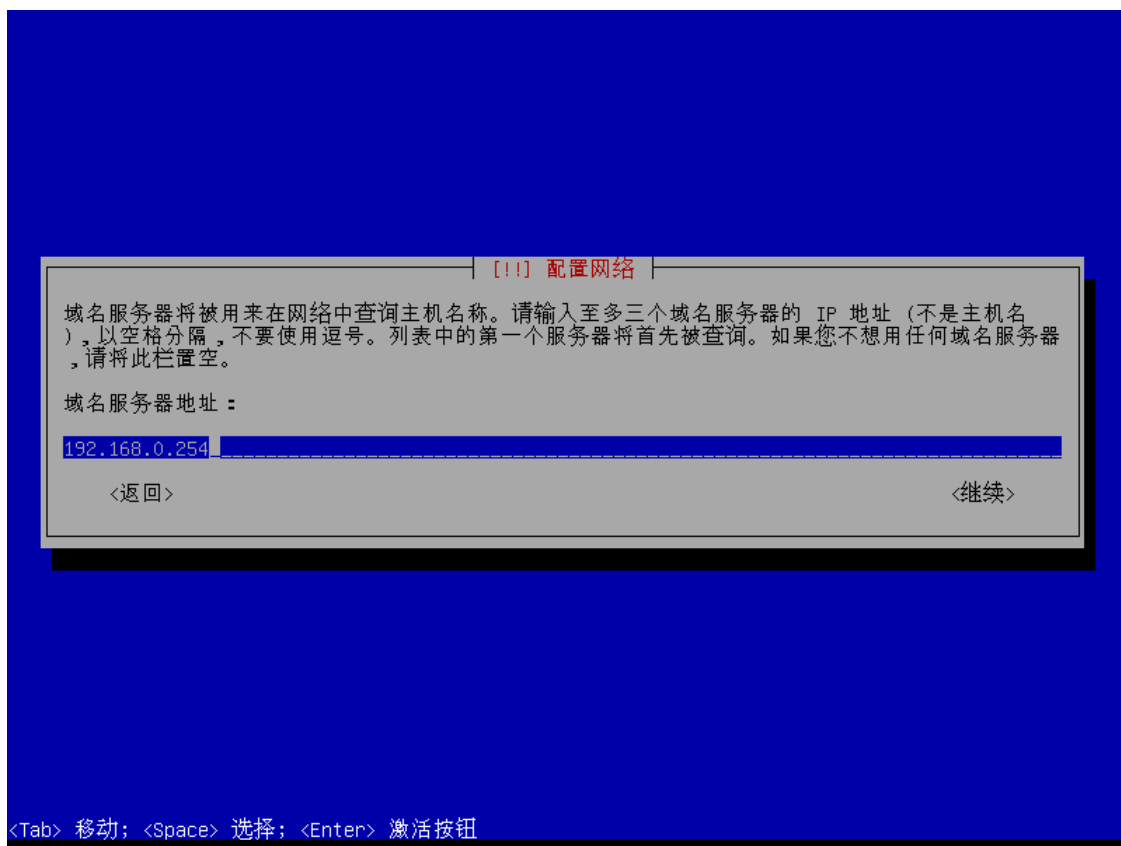


图 2.99: 域名服务器地址



提示

请根据具体情况输入网络参数，如有不明，请咨询您公司的网络管理人员。

网络设置完成，进入下一步设置主机名和域名。

2.4.1.3 设置主机名

输入主机名，然后按 **Enter** 键，如图 2.100 所示。

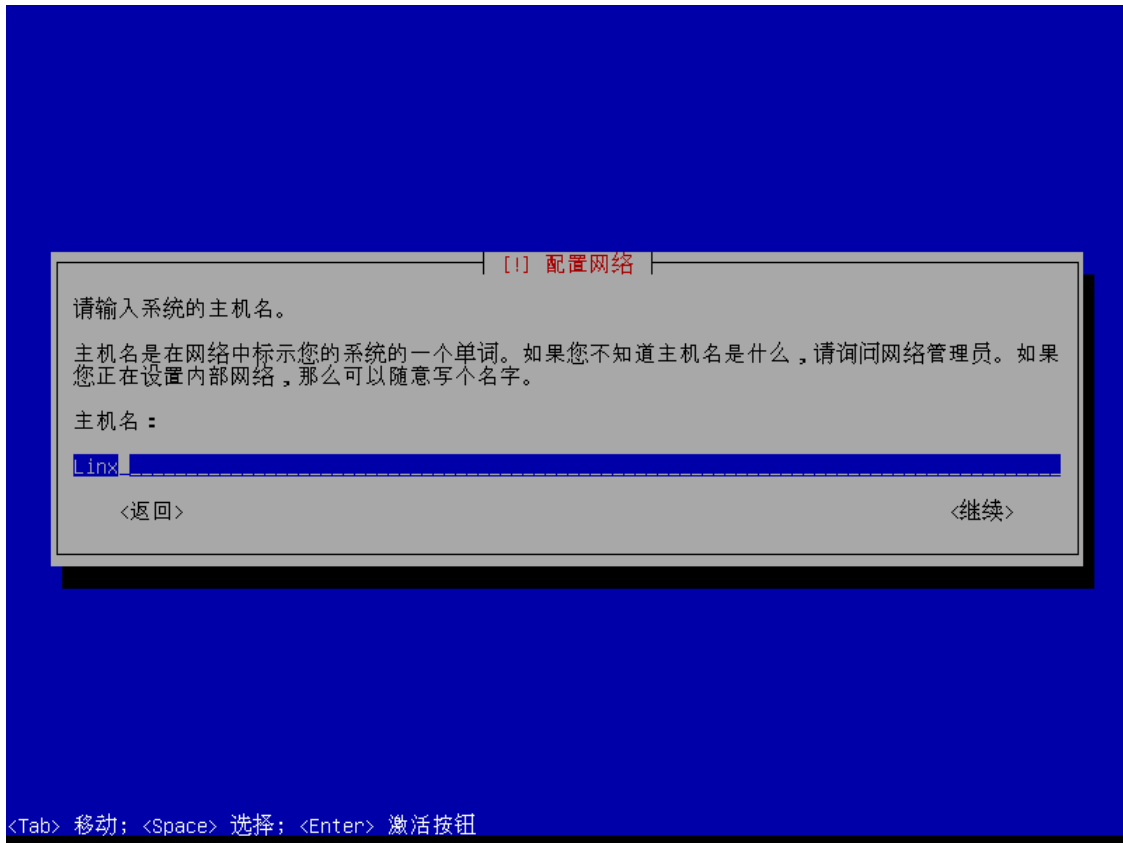


图 2.100: 设置主机名



提示

即便您的计算机不属于任何网络，您也必须为您的系统输入一个主机名！主机名默认为 Linux。

2.4.1.4 设置域名

输入域名，然后按 **Enter** 键，如图 2.101 所示。

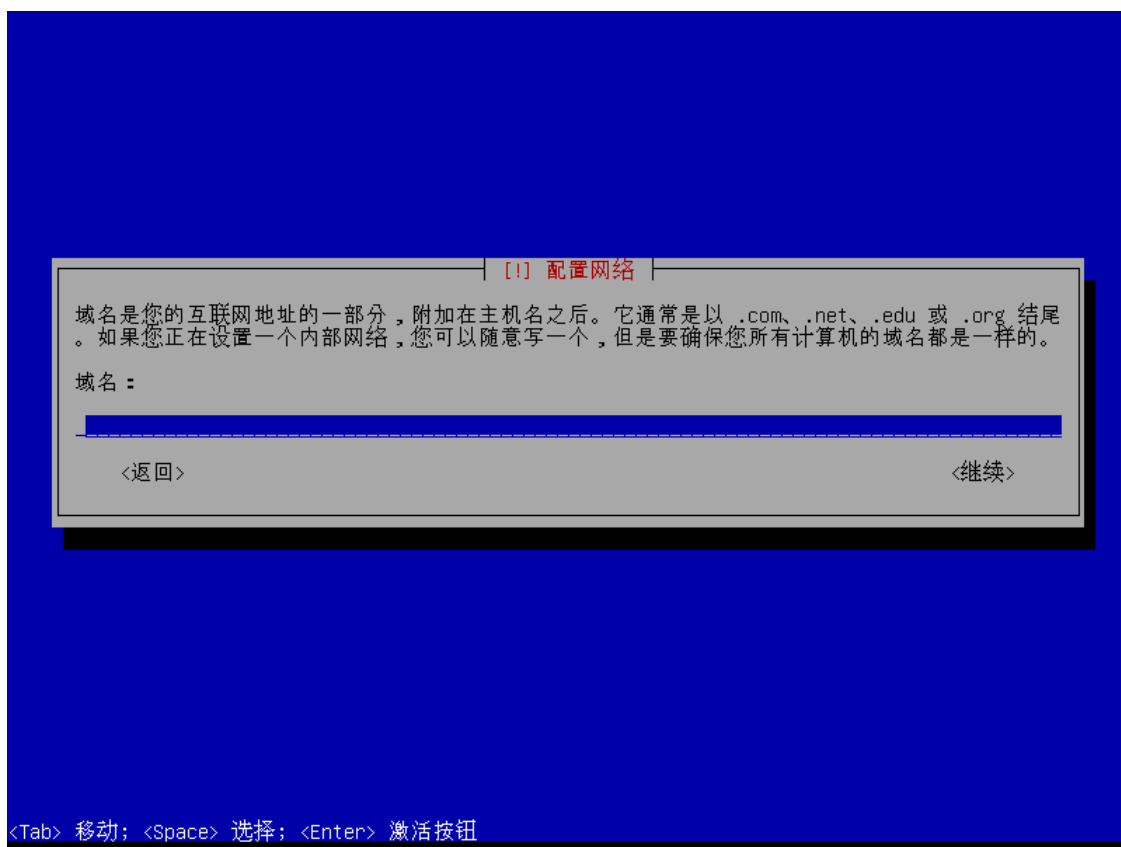


图 2.101: 设置域名

2.4.2 输入序列号

序列号是凝思用户的服务凭证，如果不输入序列号则在安全内核下不能使用网络相关的功能。请输入16个字符的序列号³，然后按 键。

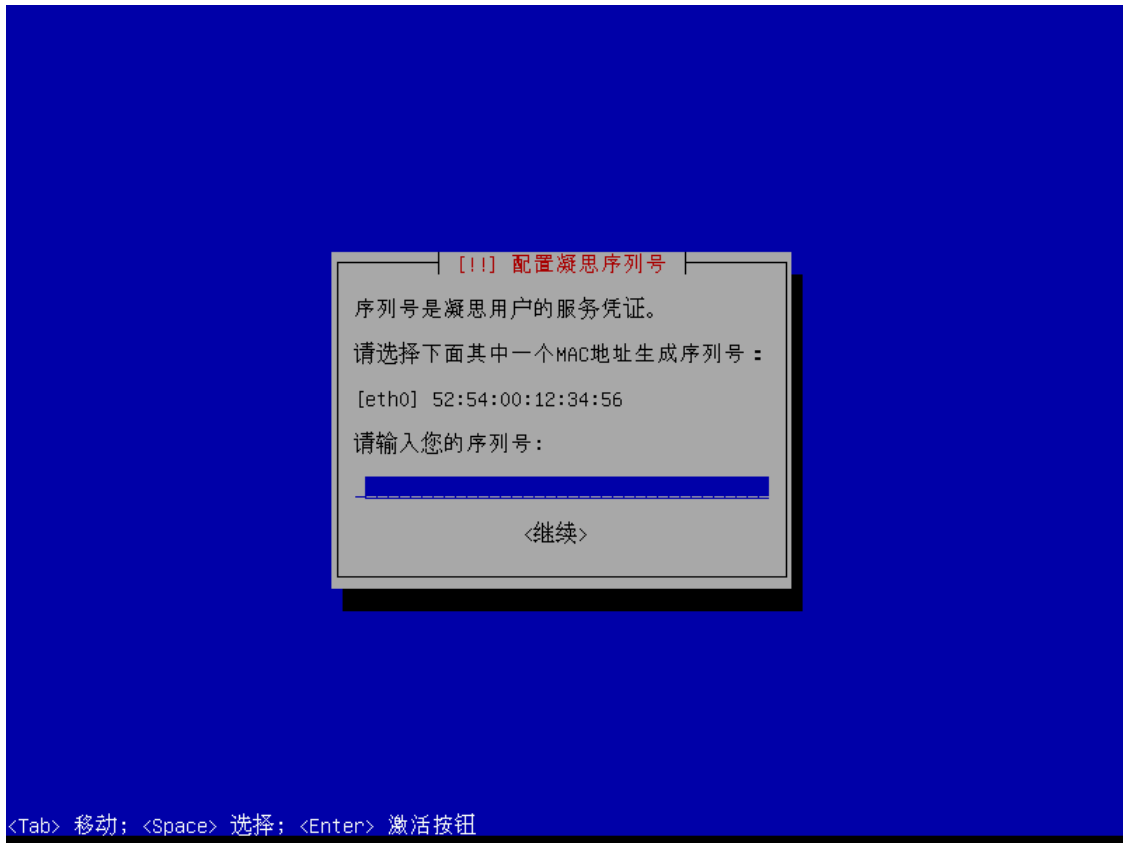


图 2.102: 输入序列号

³序列号需由北京凝思科技有限公司提供，如有问题，请向技术人员咨询。

2.4.3 设置用户和密码

基本系统安装完毕后，需要设置系统管理员密码，如图 2.103 所示。



图 2.103: 设置系统管理员密码

输入 root 用户密码，然后按 键。

再次输入密码，然后按 **Enter** 键，如图 2.104 所示。

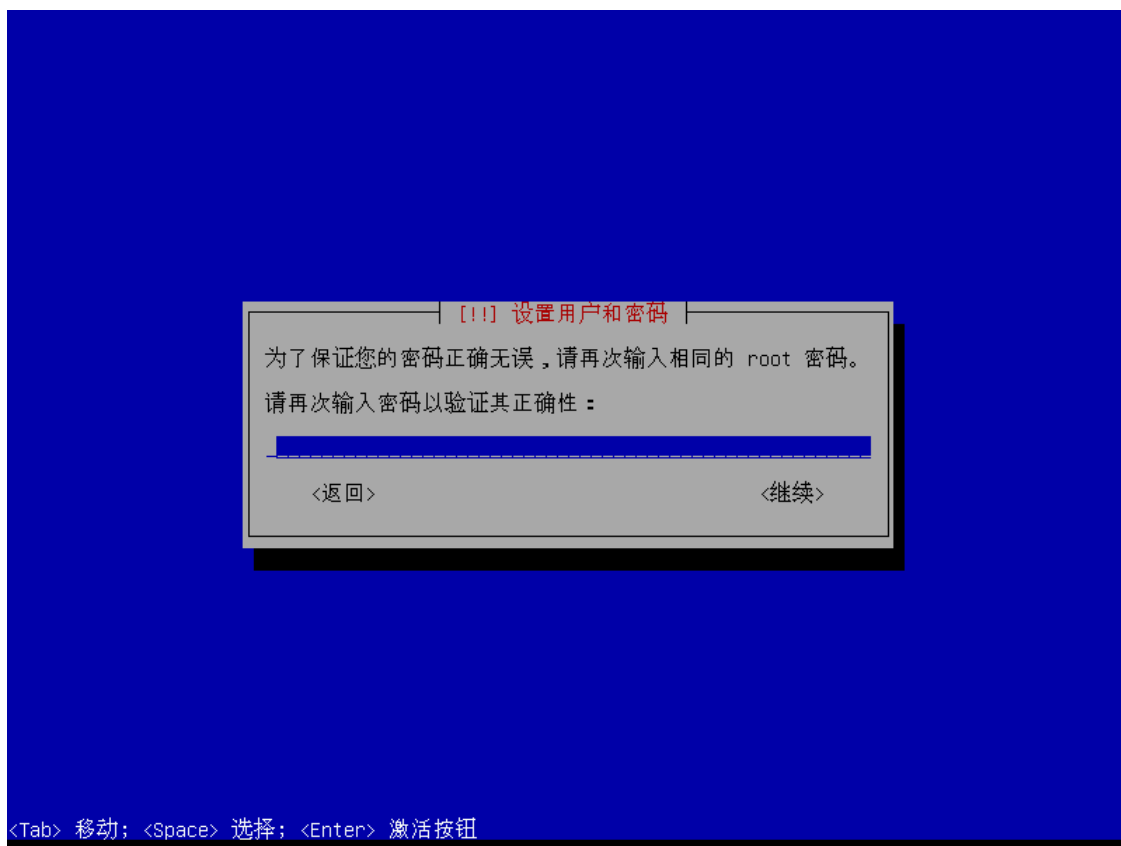


图 2.104: 验证密码正确性

普通模式会默认创建一个普通用户帐号用来执行日常操作，输入普通用户全名，然后按 Enter 键，如图 2.105 所示。



图 2.105: 设置普通用户全名

输入普通帐号的用户名，然后按 `Enter` 键，如图 2.106 所示。



图 2.106: 设置用户名

输入用户密码，然后按 **Enter** 键，如图 2.107 所示。

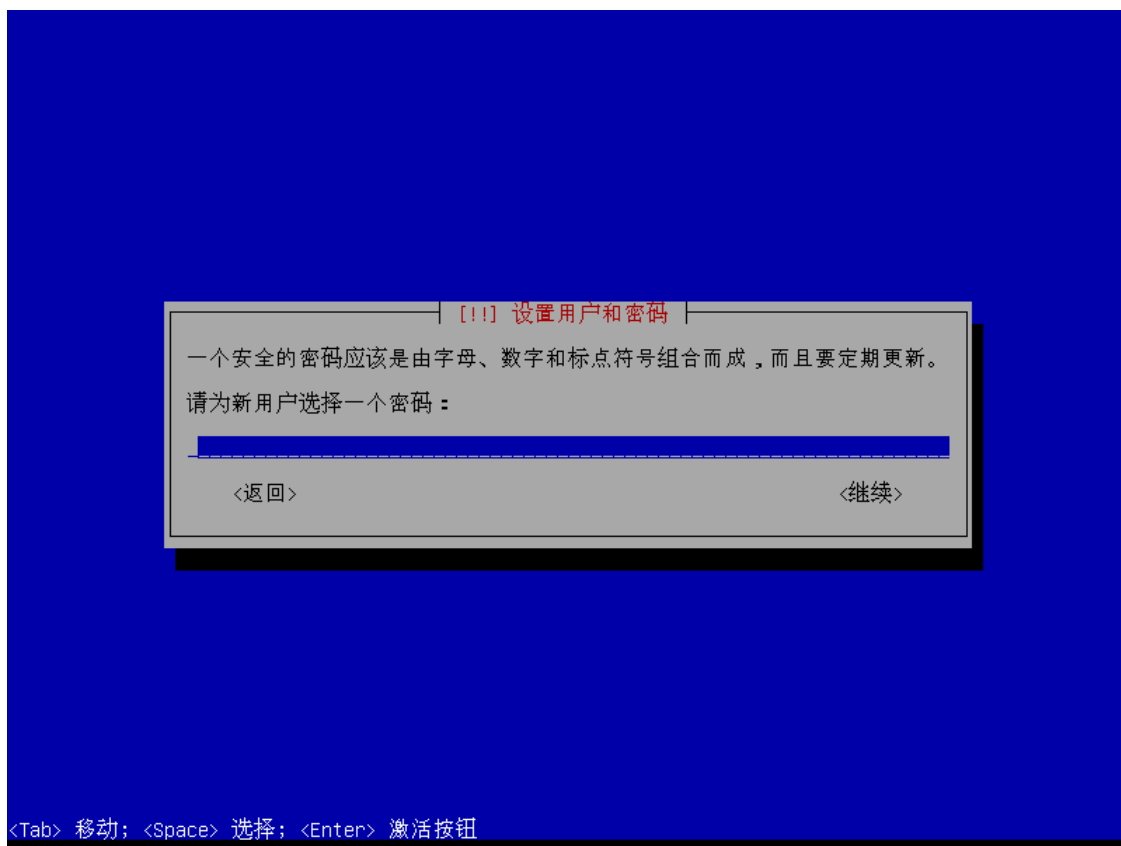


图 2.107: 设置用户密码

再次输入密码，然后按 **Enter** 键，如图 2.108 所示。

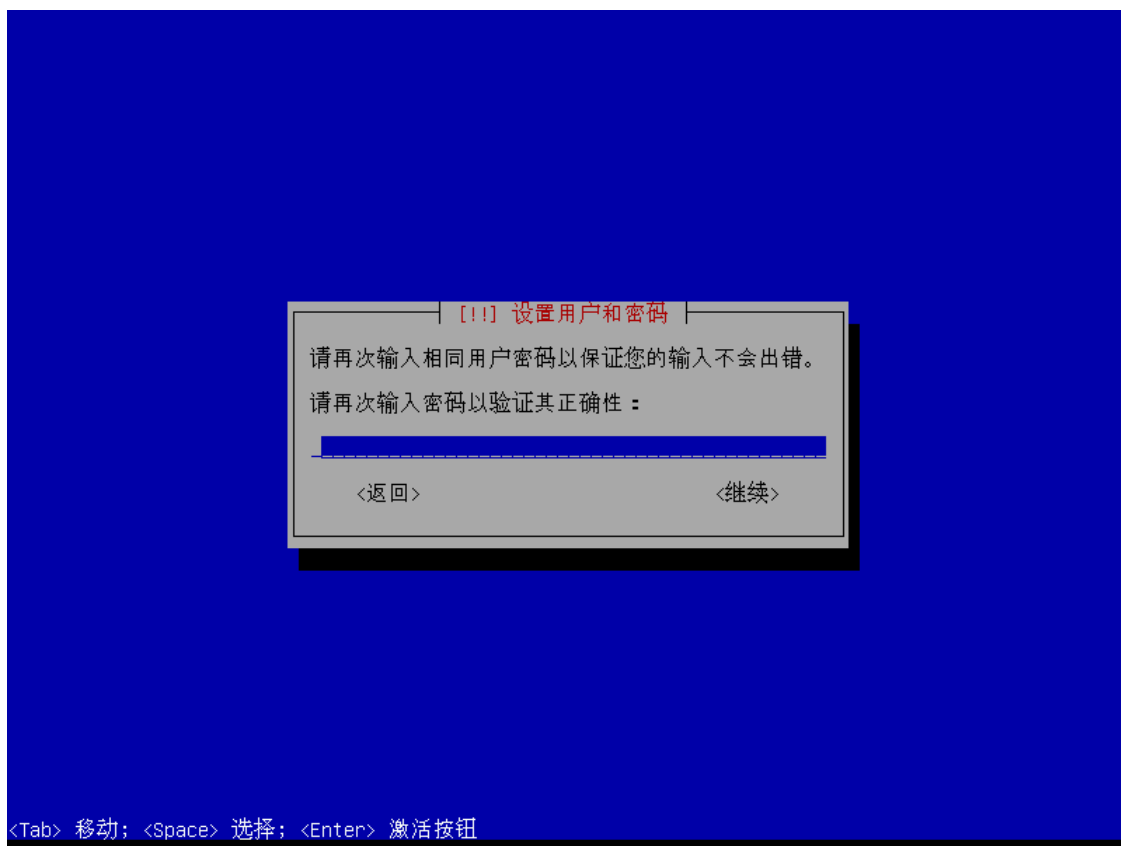


图 2.108: 验证密码正确性

下面将进入磁盘分区设置。

2.4.4 磁盘分区

您可以使用向导指导您进行分区操作，也可以选择磁盘进行手动分区。

2.4.4.1 分区向导

选择“分区向导”，按 `Enter` 键继续，如图 2.109 所示。

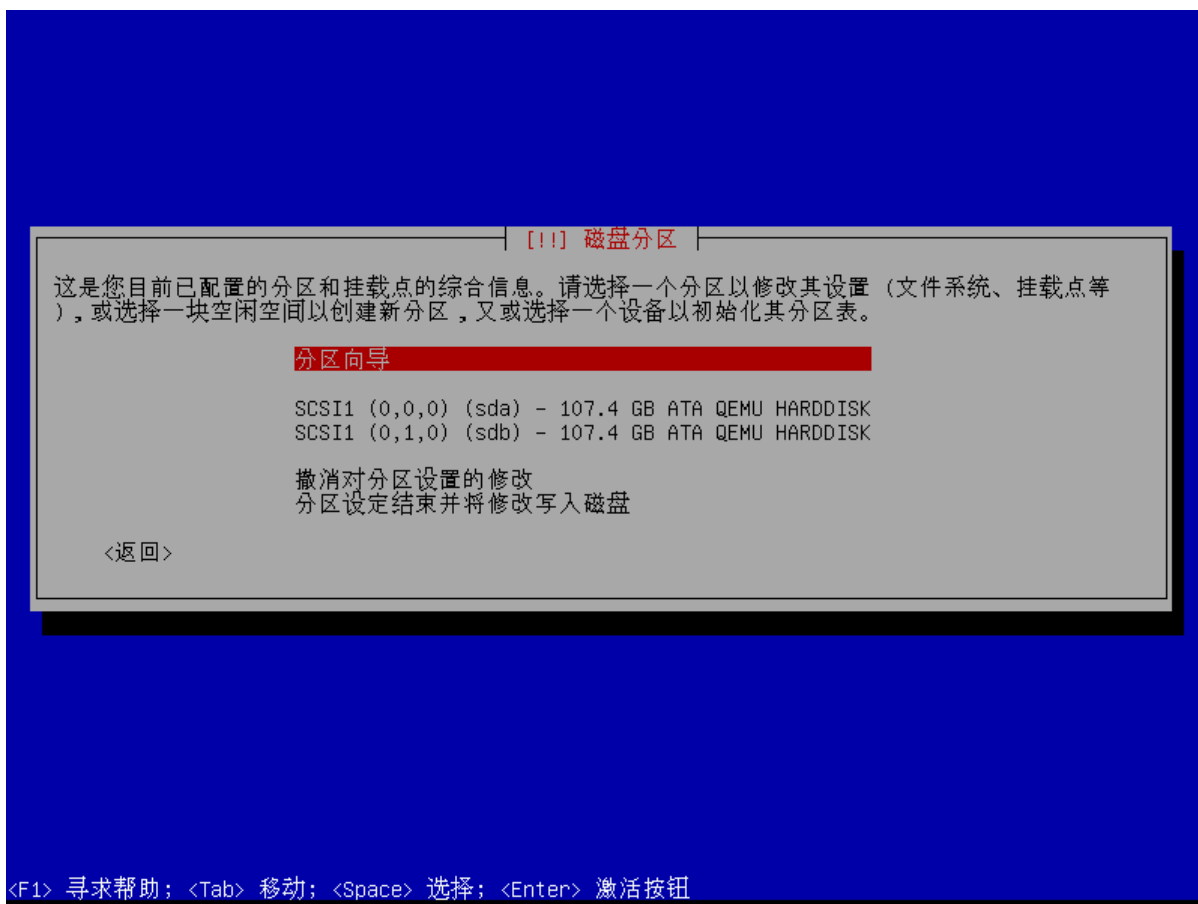


图 2.109: 磁盘分区

根据向导提示进行分区操作如下：

选择分区方法，按 **Enter** 键继续，如图 2.110 所示。

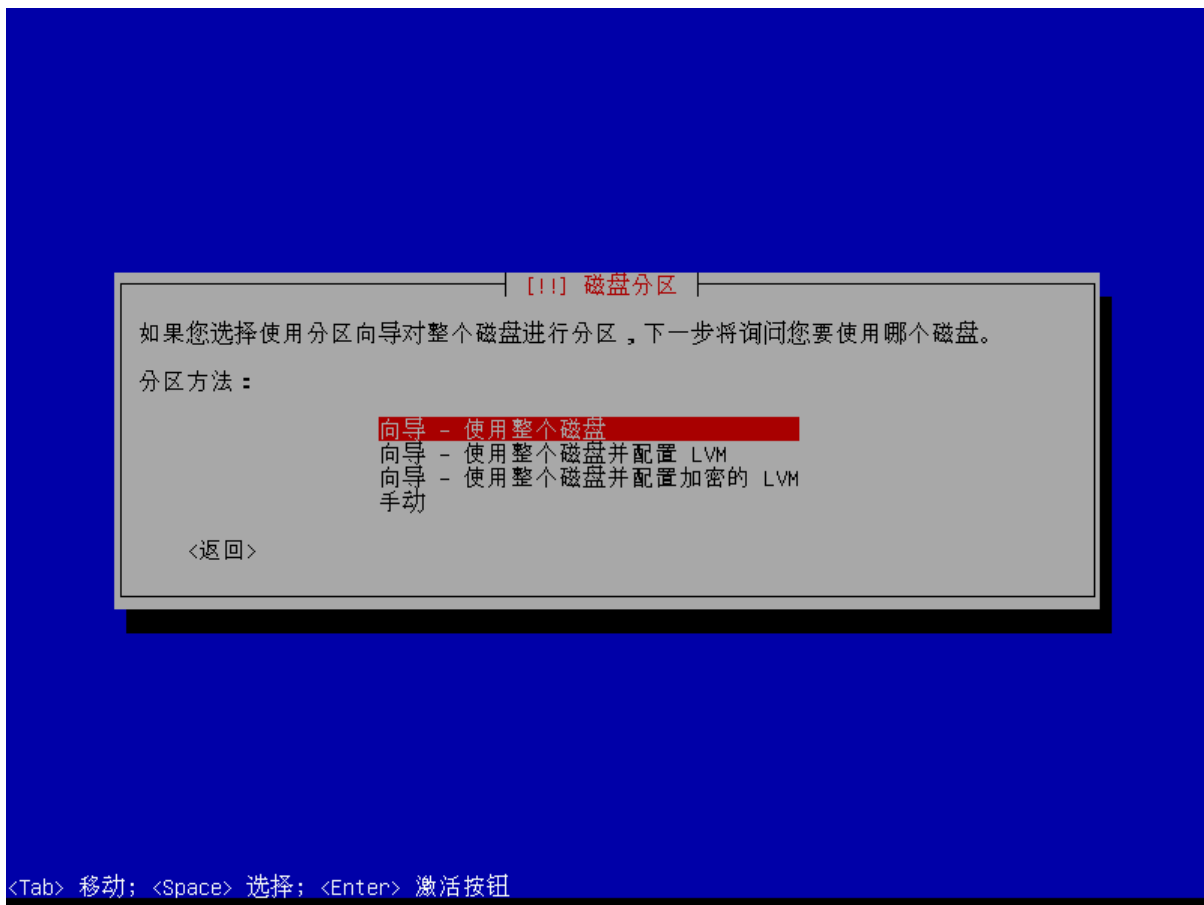


图 2.110: 分区方法

选择要分区的磁盘，按 **Enter** 键继续，如图 2.111 所示。

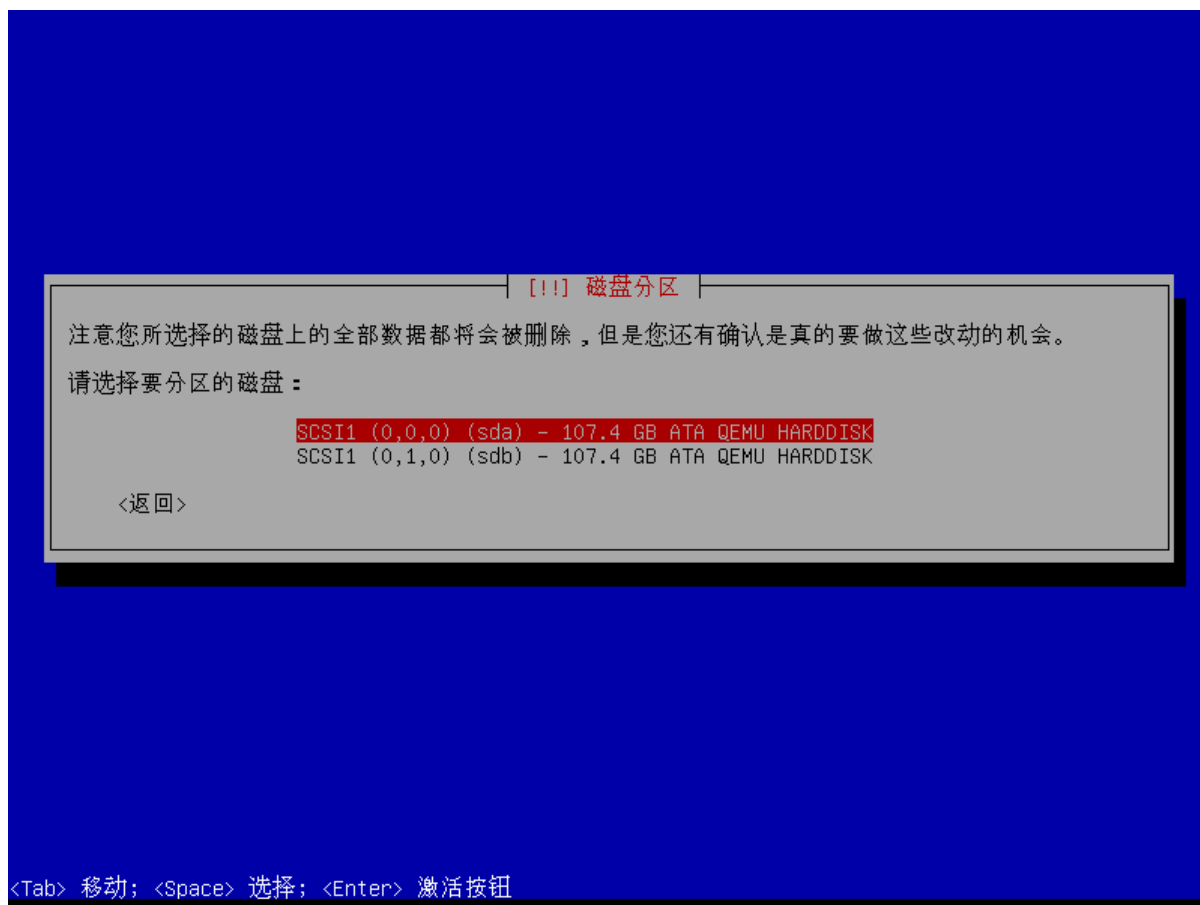


图 2.111: 选择磁盘

2.4.4.2 选择分区方案

选择分区方案，按 **Enter** 键继续，如图 2.112 所示。

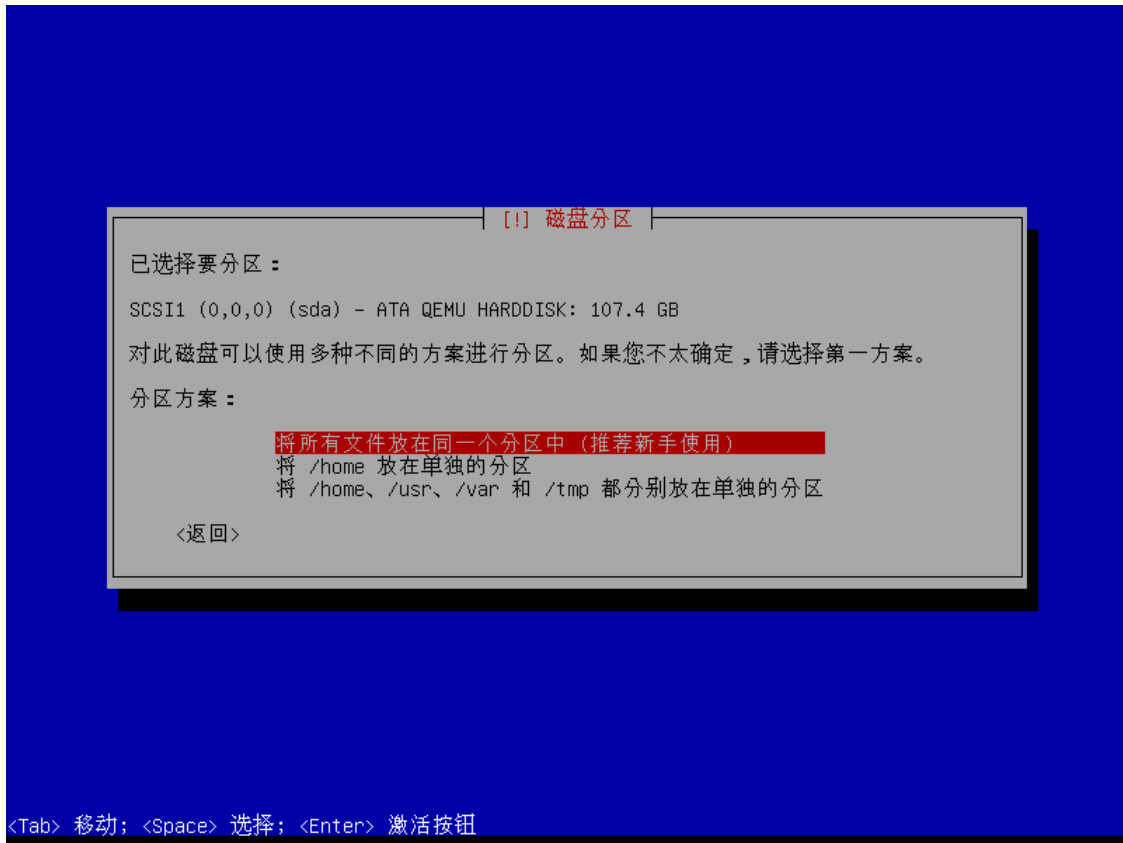


图 2.112: 分区方案

用户可根据场景、应用的需要定制合适的分区方案。如果您不知道该采取哪种分区方案，可按照向导提供的第一方案进行分区。

分区向导将列出分区结果，如图 2.113 所示。



图 2.113: 分区结果

2.4.4.3 修改分区设置

如果对分区结果不满意，可以选择某个分区，按 **Enter** 键继续，进入该分区设置界面进行修改，如图 2.114 所示。



图 2.114: 分区设置

可修改的分区设置如下：

1. 文件系统

要使分区后的磁盘可用，必须在其上构建文件系统。实际上，可以将这些文件系统看作是文件管理系统，这是因为该称呼正体现了它们的功能：它们通过维护文件上的元数据，使系统上的文件保持状态一致。

选项中的各文件系统介绍详见 2.3.9.3，选择好文件系统，按 **Enter** 键返回上一界面。

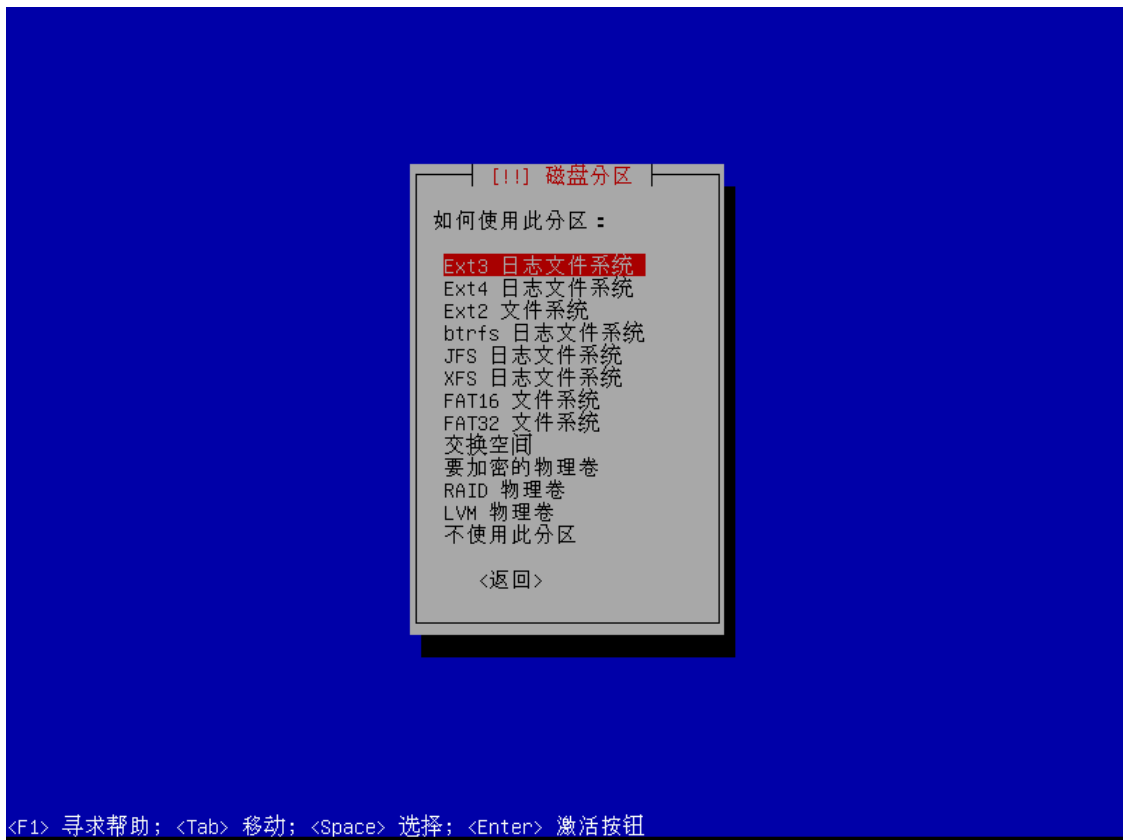


图 2.115: 文件系统

2. 挂载点

您可以选择列出的挂载点，如图 2.116 所示，或者手动输入一个挂载点，然后按 **Enter** 键返回上一界面。

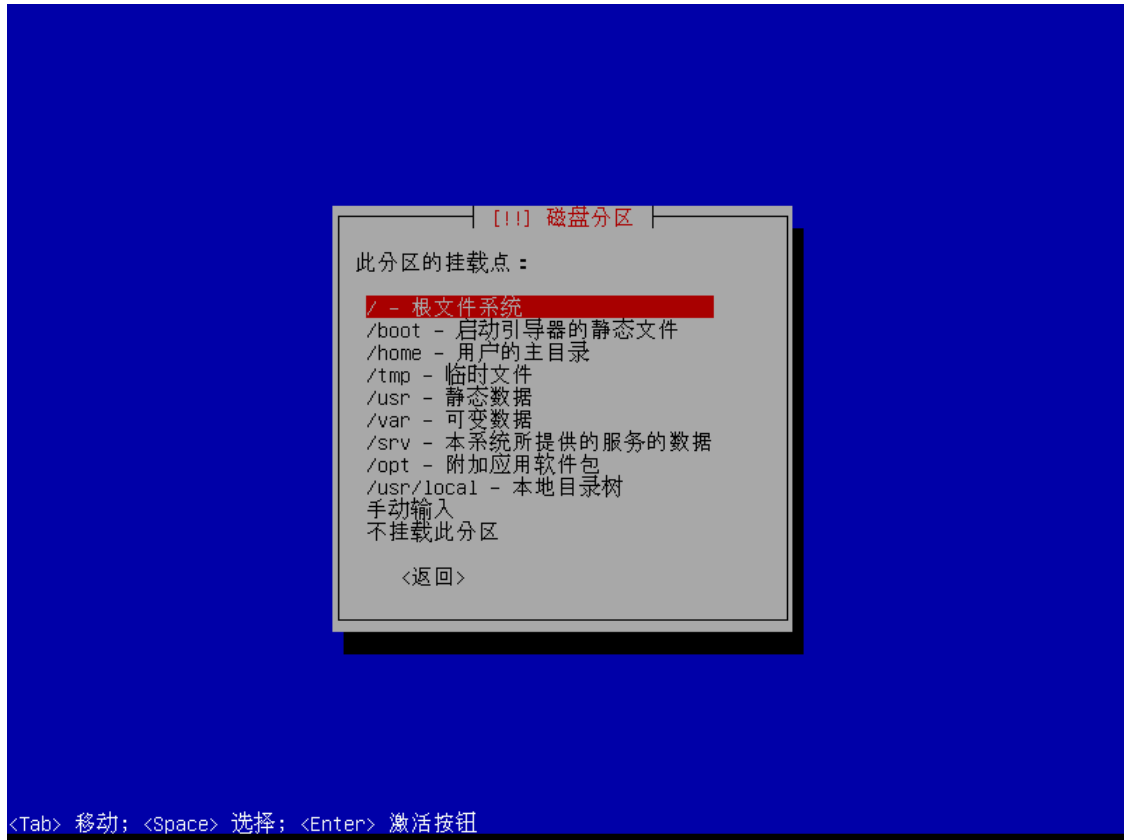


图 2.116: 挂载点

3. 挂载选项

挂载选项可以调节文件系统的行为。如图 2.117 所示，按 `space` 键选中各选项前的复选框，选择挂载选项，然后按 `Enter` 键返回上一界面。

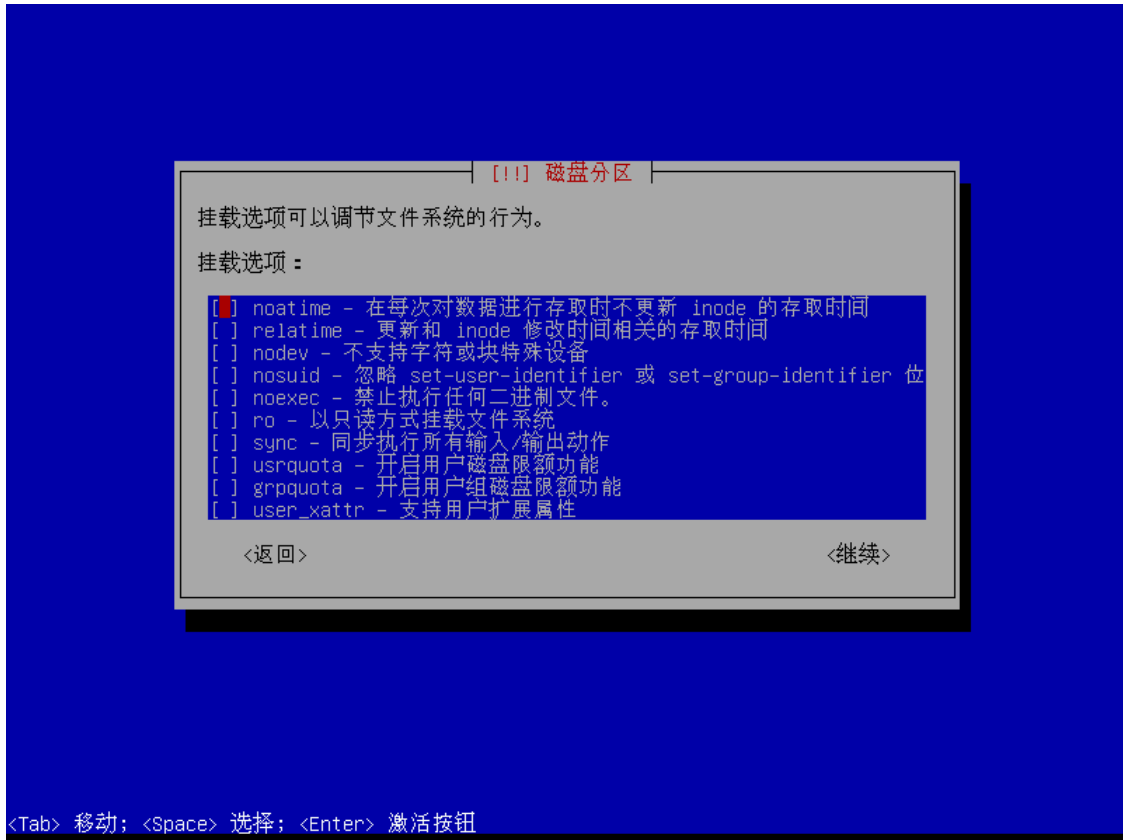


图 2.117: 挂载选项

4. 标识

输入该分区文件系统的标识，如图 2.118 所示，然后按 键返回上一界面。



图 2.118: 标识

5. 保留块

设置文件系统保留给超级用户的磁盘容量百分比，以免磁盘空间被占满了系统无法正常运行。输入百分比，如图 2.119 所示，然后按 **Enter** 键返回上一界面。



图 2.119: 保留块

6. 典型用途

指定文件系统的用途，安装程序将根据用途指定优化的文件系统参数。如图 2.120 所示，选择文件系统用途，然后按 **Enter** 键返回上一界面。



图 2.120: 典型用途

7. 可启动标志

选择“可启动标志”，然后按 **Enter** 键，该参数将在“开”和“关”之间进行切换。“可启动标志”设置为“开”，则该分区为启动分区。

设置好分区后，选择“分区设定结束”，按 **Enter** 键返回磁盘分区界面。

2.4.4.4 复制分区

选择“将另一分区的数据复制到此处”，然后按 **Enter** 键，可以复制分区。

复制操作需要将之前的分区结果写入磁盘后再进行，如图 2.121 所示，选择“是”，然后按 **Enter** 键确认分区结果；选择“否”，然后按 **Enter** 键撤销复制操作并返回上一界面。

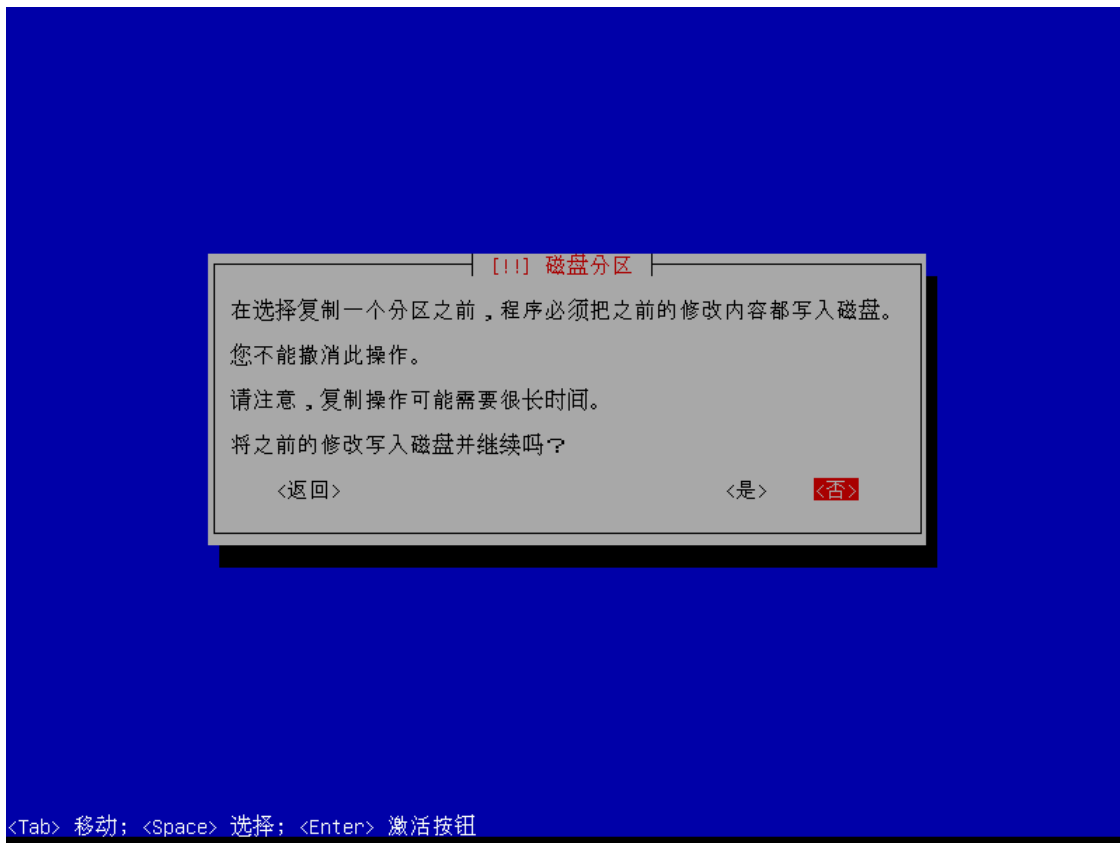


图 2.121: 复制分区

选择要复制的分区，然后按 **Enter** 键继续，如图 2.122 所示。



图 2.122: 选择要复制的分区

2.4.4.5 删除分区

选择“删除此分区”，然后按 **Enter** 键，可删除该分区并返回上一界面。

设置结束后，选择“分区设定结束”，然后按 **Enter** 键返回上一界面。

2.4.4.6 撤销修改

要恢复修改之前的分区设置，选择“撤销对分区设置的修改”，然后按 **Enter** 键撤销修改。

2.4.4.7 确认分区

确认分区结果后，选择“分区设定结束并将修改写入磁盘”，按 **Enter** 键继续，确认将分区结果写入磁盘，如图 2.123 所示，选择“是”，按 **Enter** 键继续，分区结果将写入磁盘。



图 2.123: 确认分区

**注意**

分区结果要写入磁盘才会生效！没有执行写入操作而直接退出将丢失分区结果。

2.4.4.8 配置 LVM

LVM 介绍详见 2.3.9.8。

分区操作与 2.4.4.1 相似，只是选择分区磁盘后需要确认配置 LVM，如图 2.124 所示。

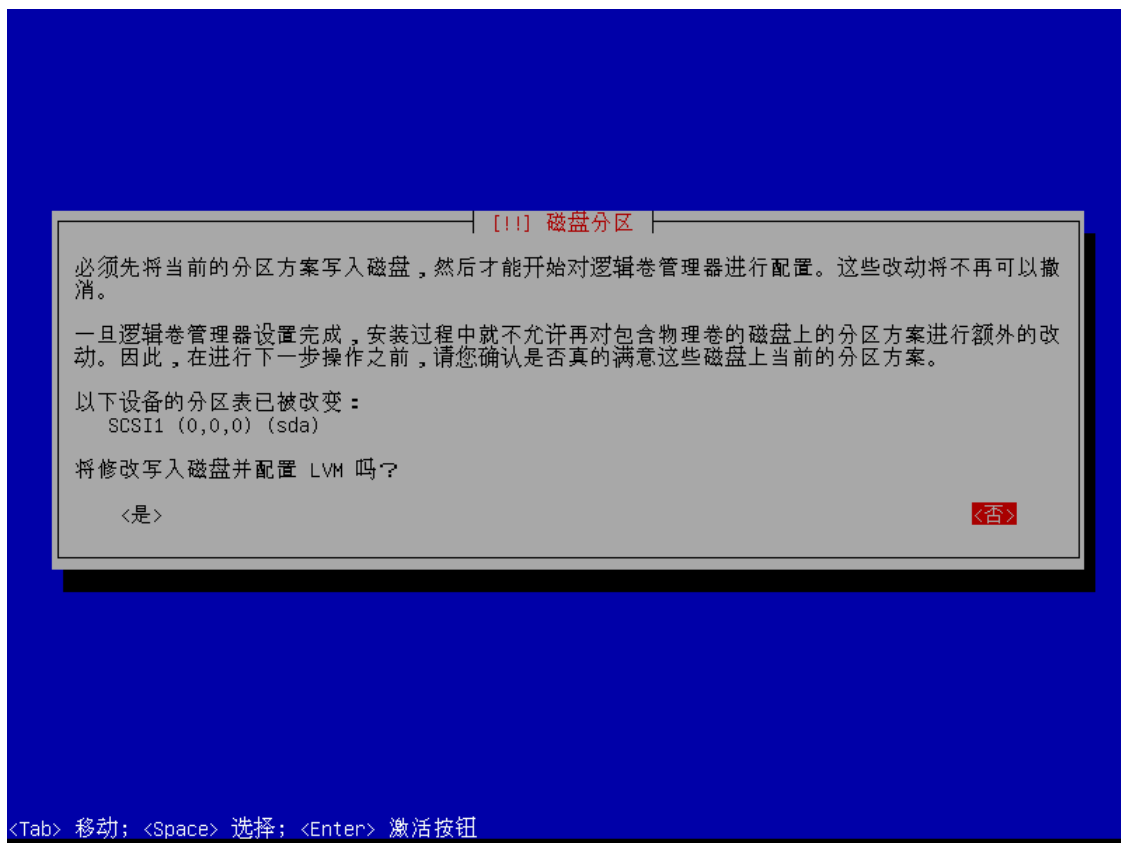


图 2.124: 配置LVM

选择“是”，然后按 **Enter** 键确认配置 LVM，分区向导将列出分区结果，如图 2.125 所示。

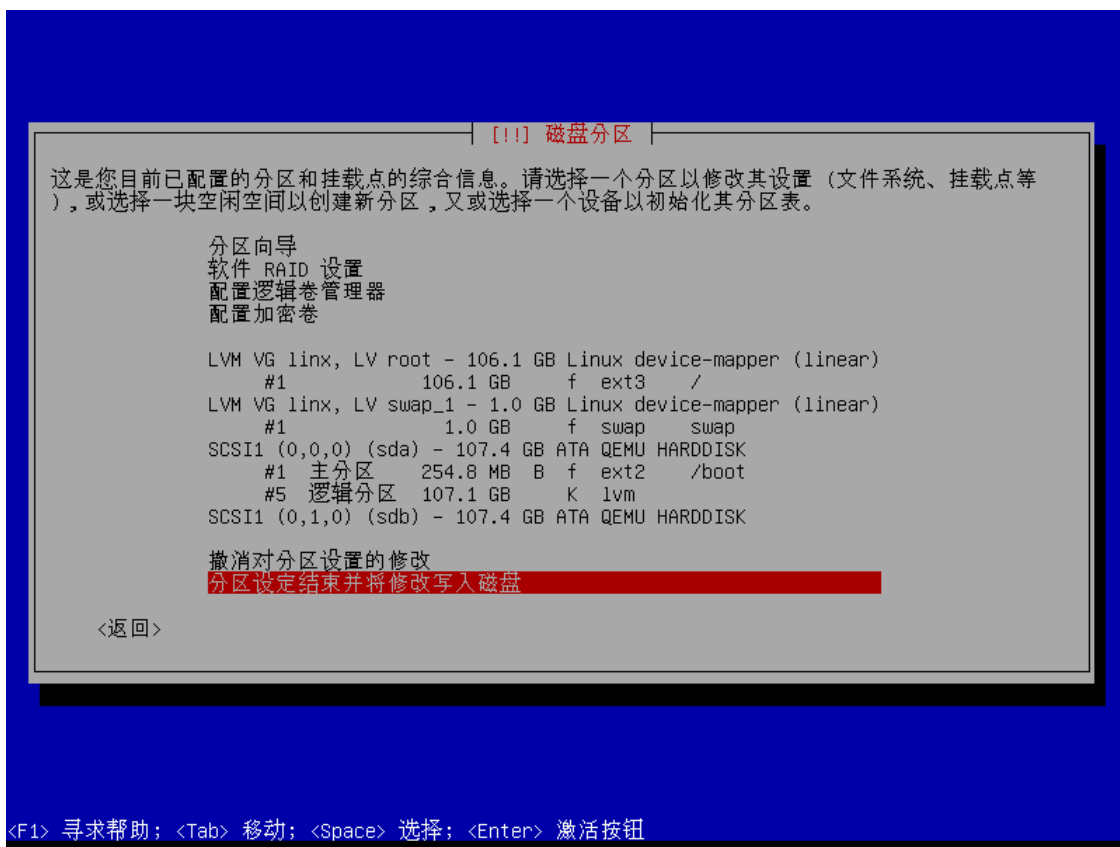


图 2.125: LVM 分区

2.4.4.9 配置加密的 LVM

使用此分区向导进行分区，分区操作与 2.4.4.8 相似，但在确认配置 LVM 后，将会要求用户输入加密口令。输入加密口令后，按 键确认，如图 2.126 所示。

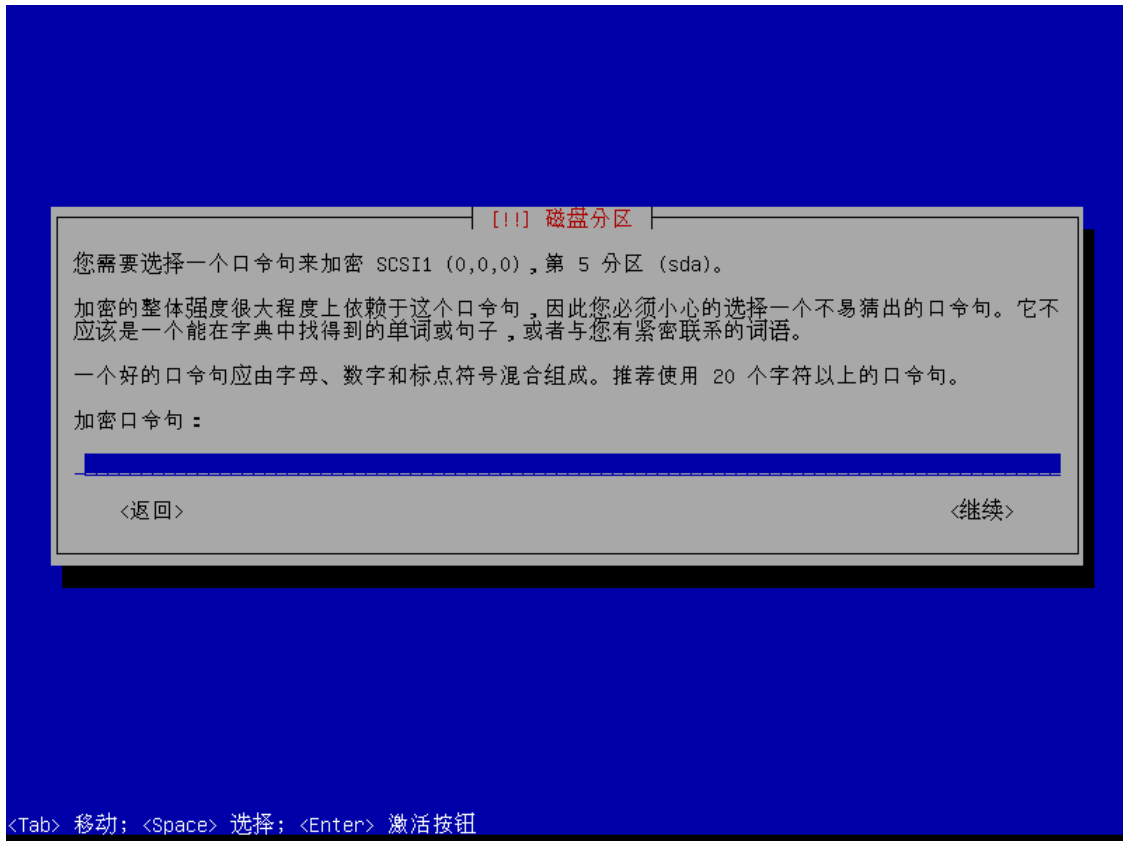


图 2.126: 加密分区

再次输入加密口令，按 **Enter** 键确认，如图 2.127 所示。

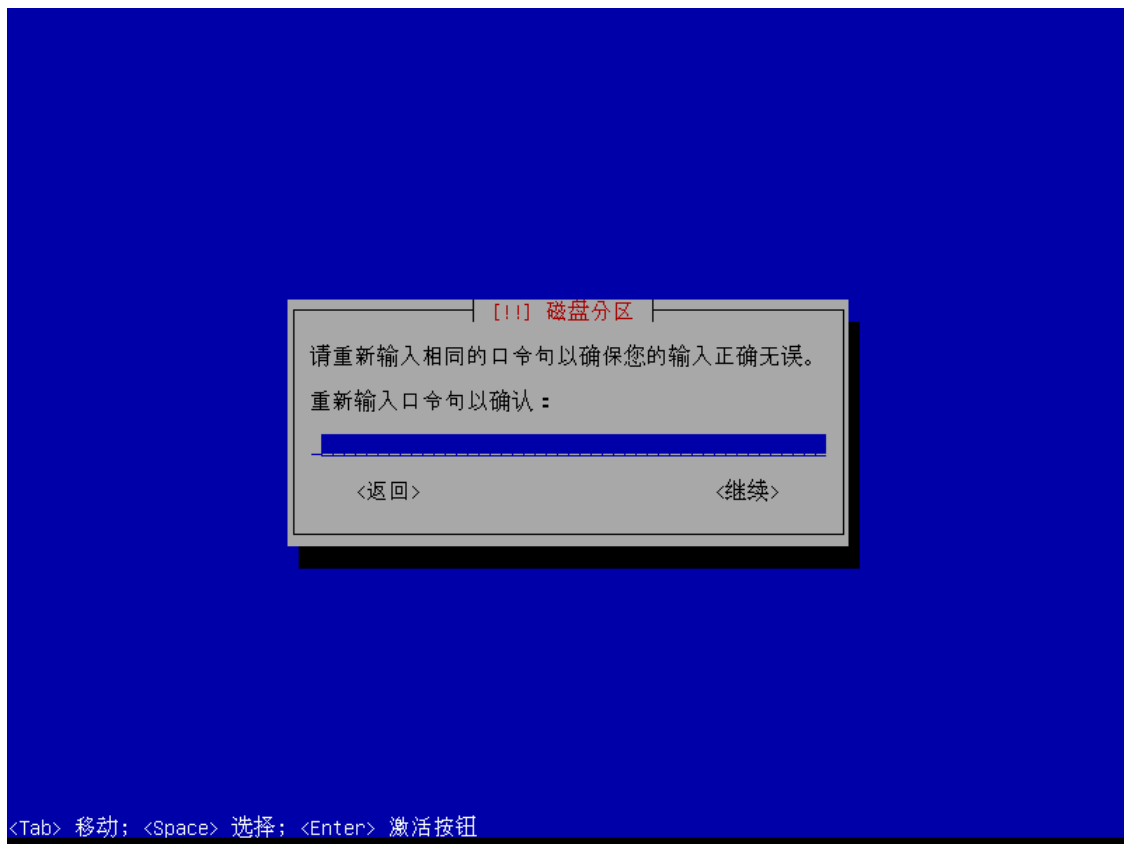


图 2.127: 确认加密口令

分区向导将列出分区结果，如图 2.128 所示。

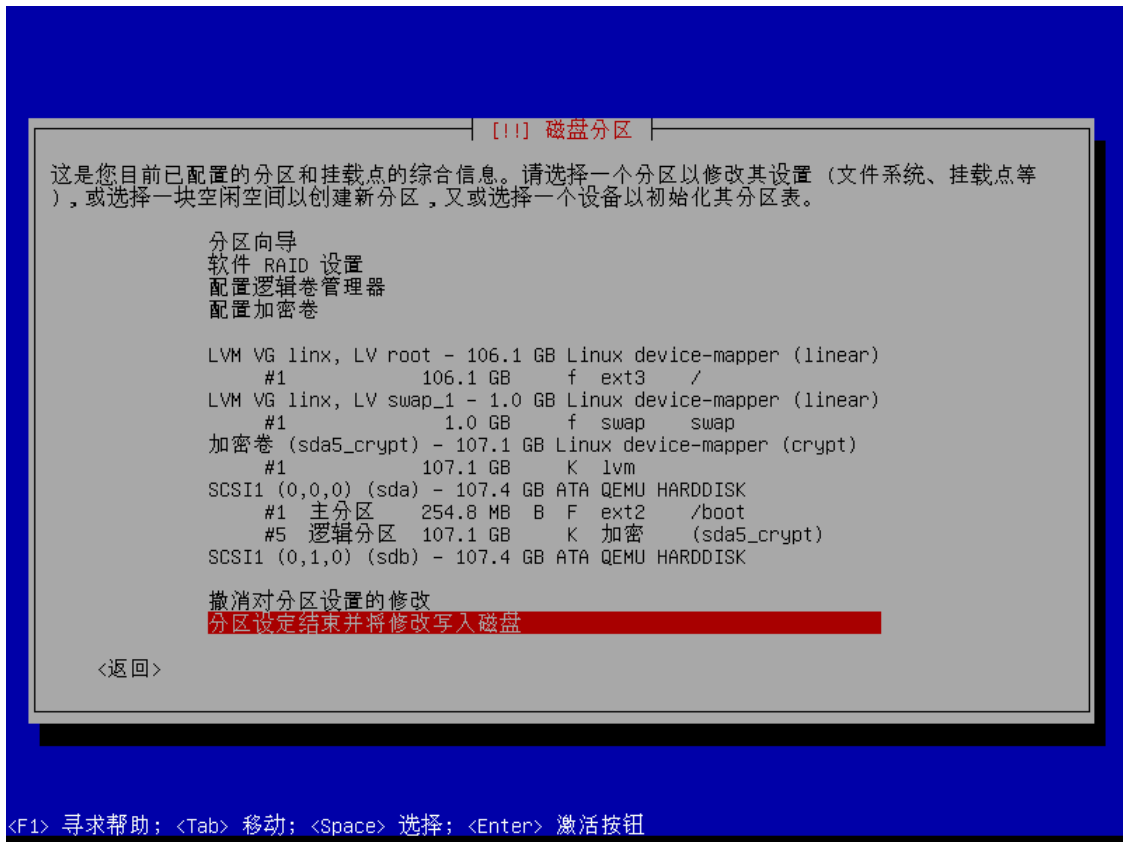


图 2.128: 加密的 LVM 分区

2.4.4.10 手动分区

除了使用分区向导，您还可以选择手动分区。选择要分区的磁盘，然后按 键继续。

1. 创建分区表

默认对整个磁盘进行分区，创建新的分区表，现有的所有分区都将删除，确定创建新的空分区表，选择“是”，按 键继续，如图 2.129 所示。



图 2.129: 创建分区表

2. 选择磁盘空间

选择要分区的磁盘空闲空间，按 `Enter` 键继续，如图 2.130 所示。

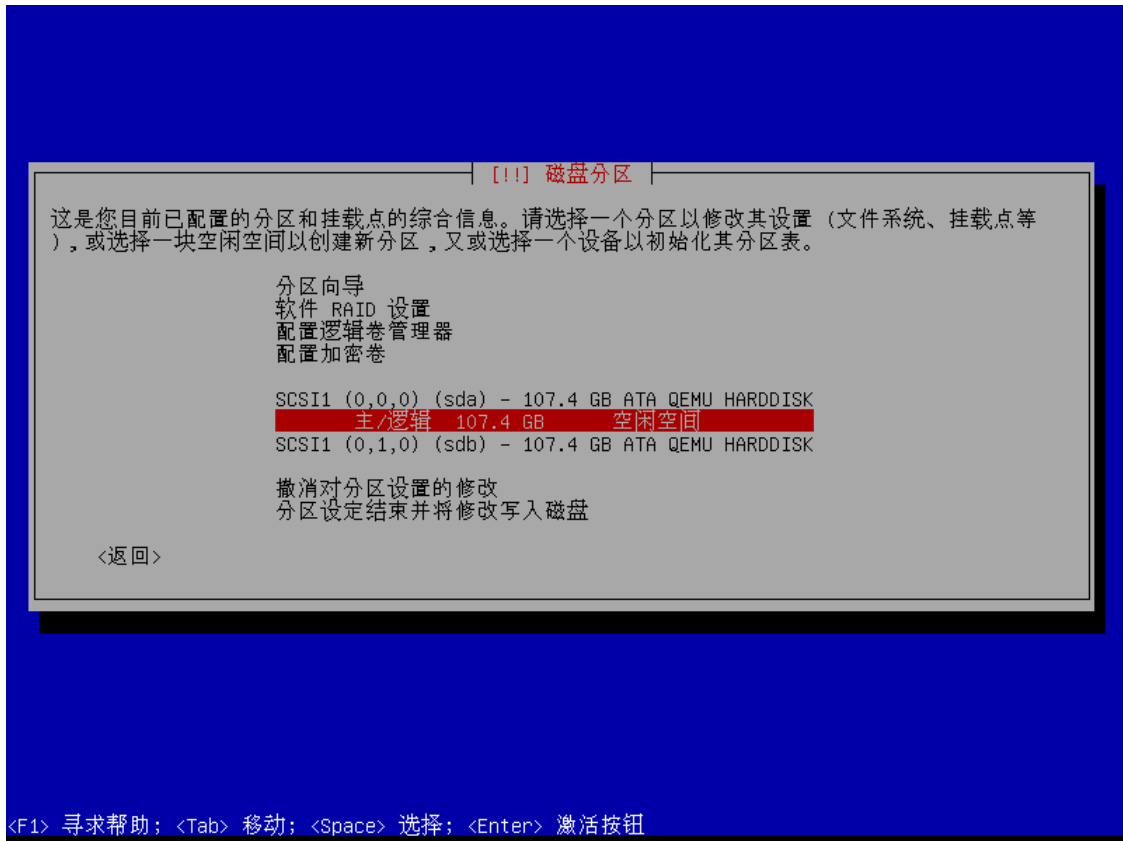


图 2.130: 选择磁盘空闲空间

3. 创建新分区

选择“创建新分区”，按 **Enter** 键继续，如图 ?? 所示。

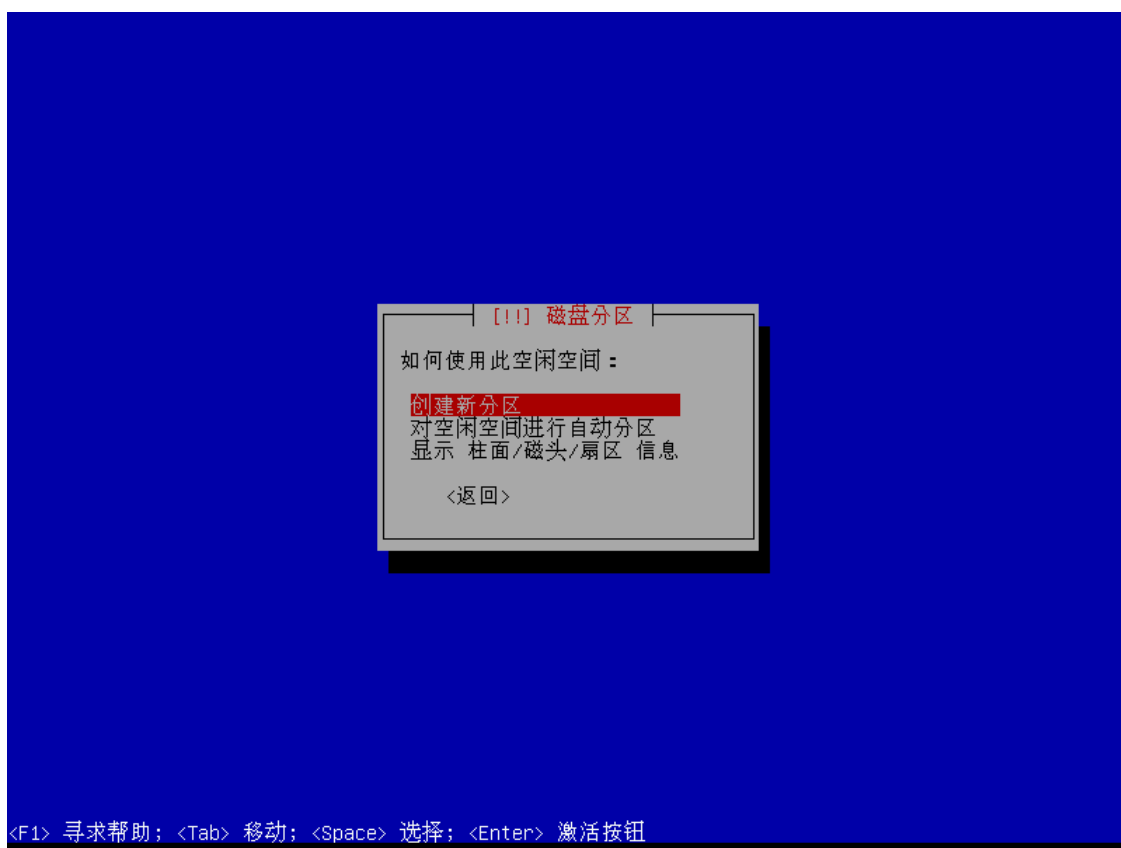


图 2.131: 创建新分区

4. 设置分区大小您需要指定分区大小，有多种表示方式可以选择，如容量、最大空间的百分比、最大空间。

输入分区大小，然后按 键继续，如图 2.132 所示。



图 2.132: 输入分区大小

5. 设置分区类型选择“主分区”或“逻辑分区”，然后按 **Enter** 键继续，如图 2.133 所示。

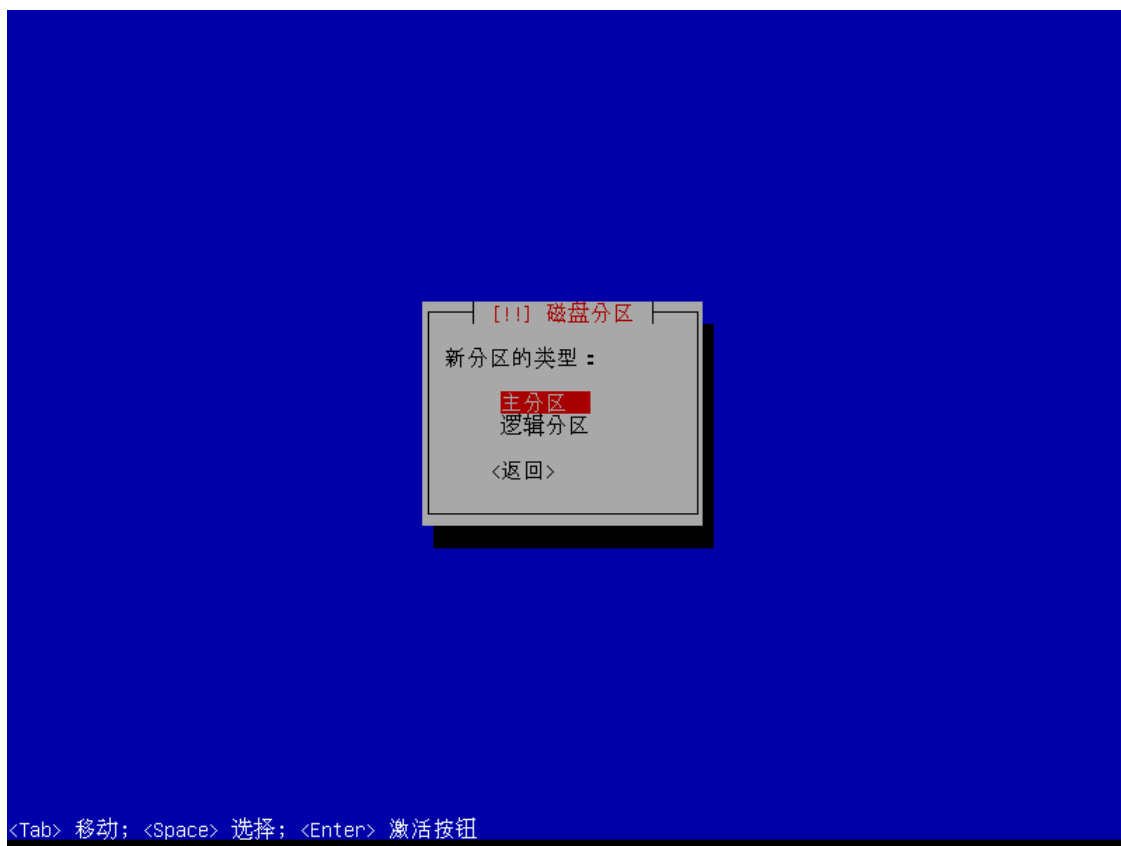


图 2.133: 选择分区类型

6. 新分区的位置选择从磁盘的“开始”或“结束”来划分此分区，然后按 **Enter** 键继续，如图 2.134 所示。



图 2.134: 选择新分区的位置

7. 分区设置安装程序已给出默认设置，您可以修改分区设置，操作与 2.4.4.3 相同。

2.4.4.11 配置软Raid

关于软Raid的介绍，详见 2.3.9.11，本节仅描述操作步骤。

将分区的文件系统设置为“RAID物理卷”，该分区将可用来制作软RAID，如图 2.135 所示。



图 2.135: 选择新分区的位置

选择“软件 RAID 设置”，然后按 **Enter** 键至确认界面，选择“是”并按 **Enter** 键确认将分区设定写入磁盘并配置 Raid，如图 2.136 所示。

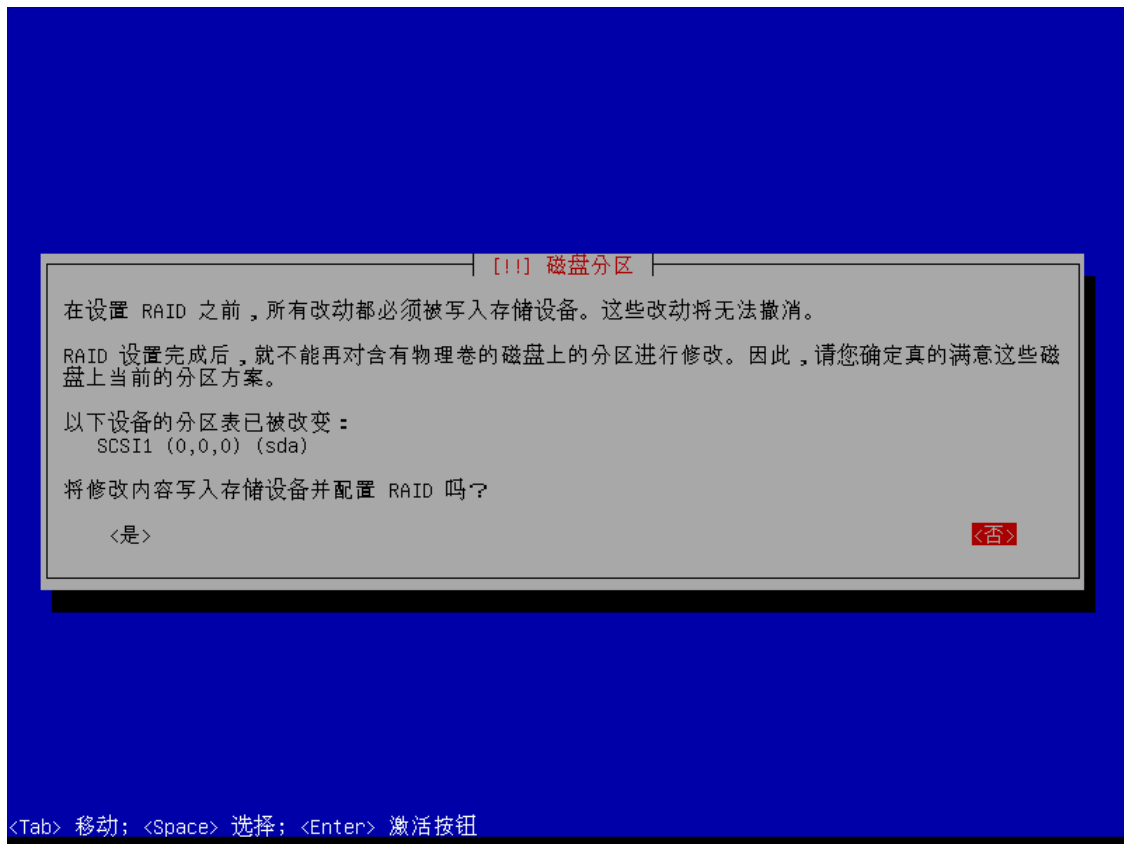


图 2.136: 确认配置 Raid

1. 创建 MD 设备

选择“创建 MD 设备”，然后按 **Enter** 键，如图 2.137 所示。

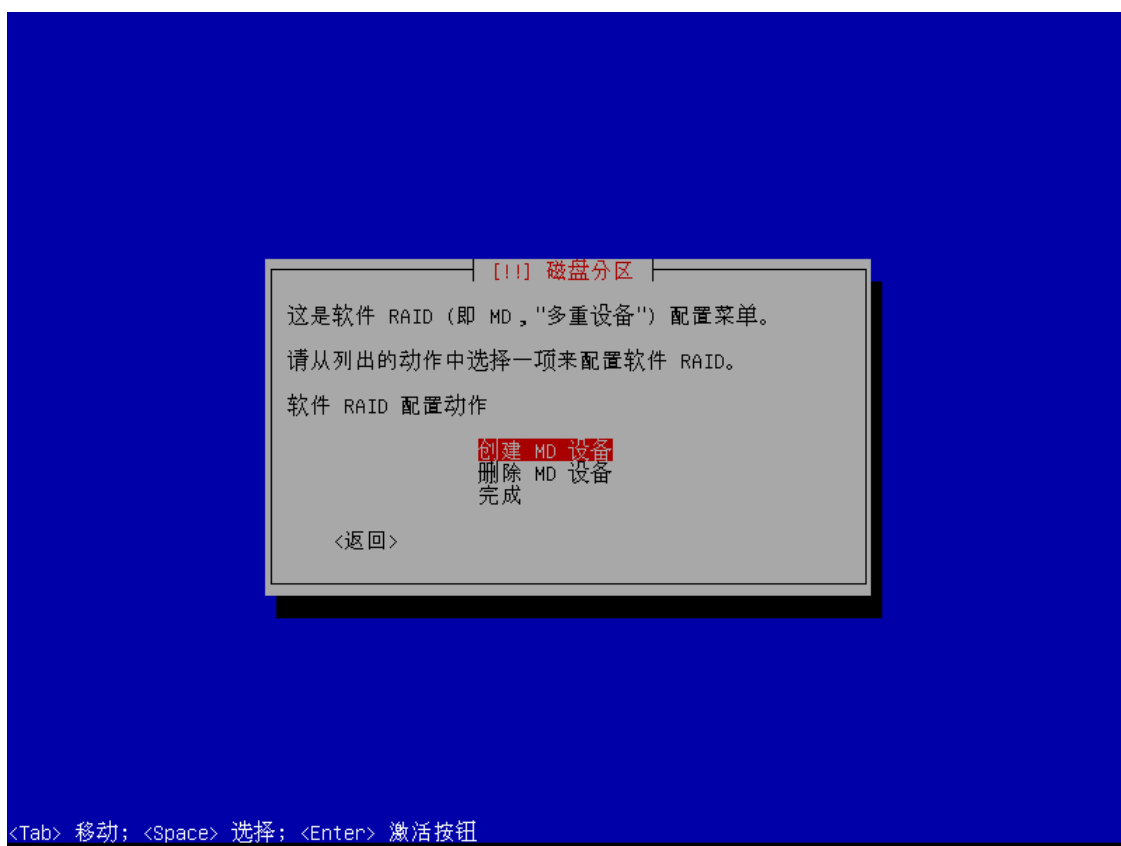


图 2.137: 盘组配置

选择 RAID 级别，然后按 **Enter** 键，如图 2.138 所示。

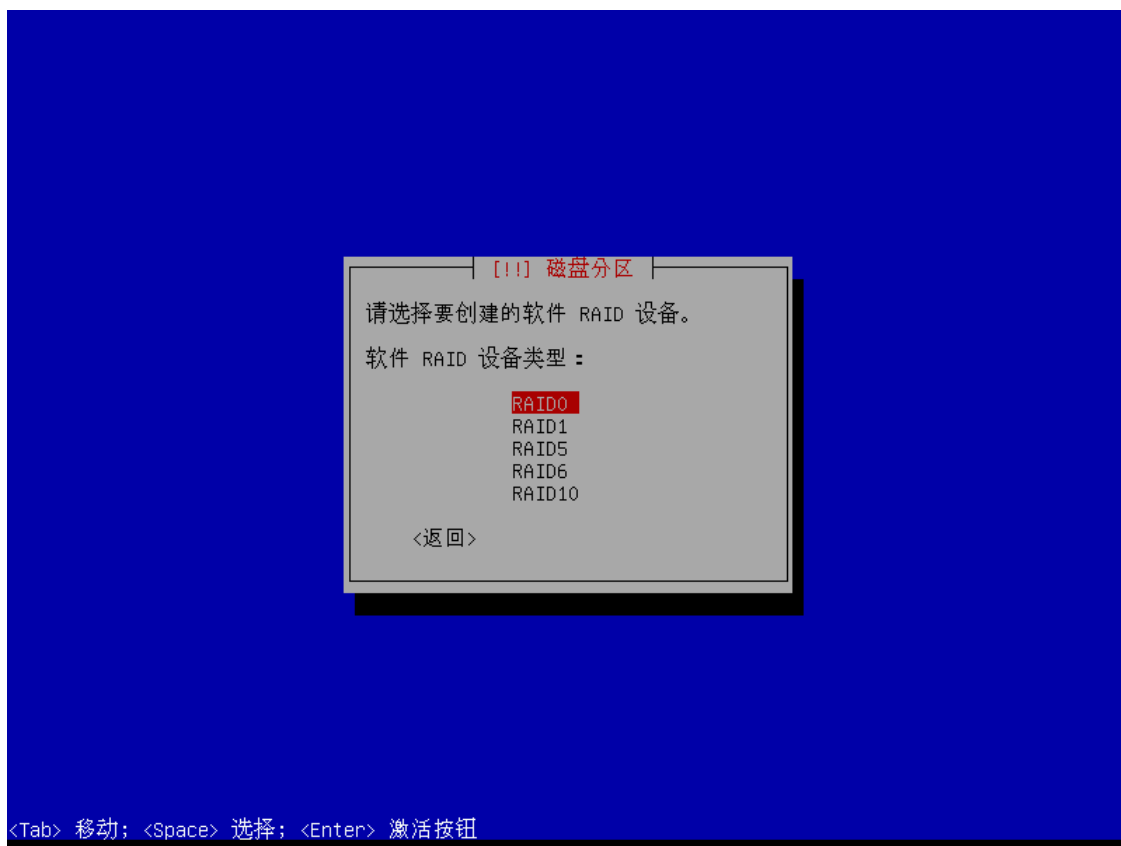


图 2.138: 盘组设备类型

关于Raid级别如何选择，详见 2.3.9.11。

除Raid 0之外，其它几个级别要使用不止一个分区，Raid 1和Raid 10是2个及以上（需双数），Raid 5是3个及以上，Raid 6是4个及以上。

输入活跃设备的个数，然后按 键，如图 2.139 所示。

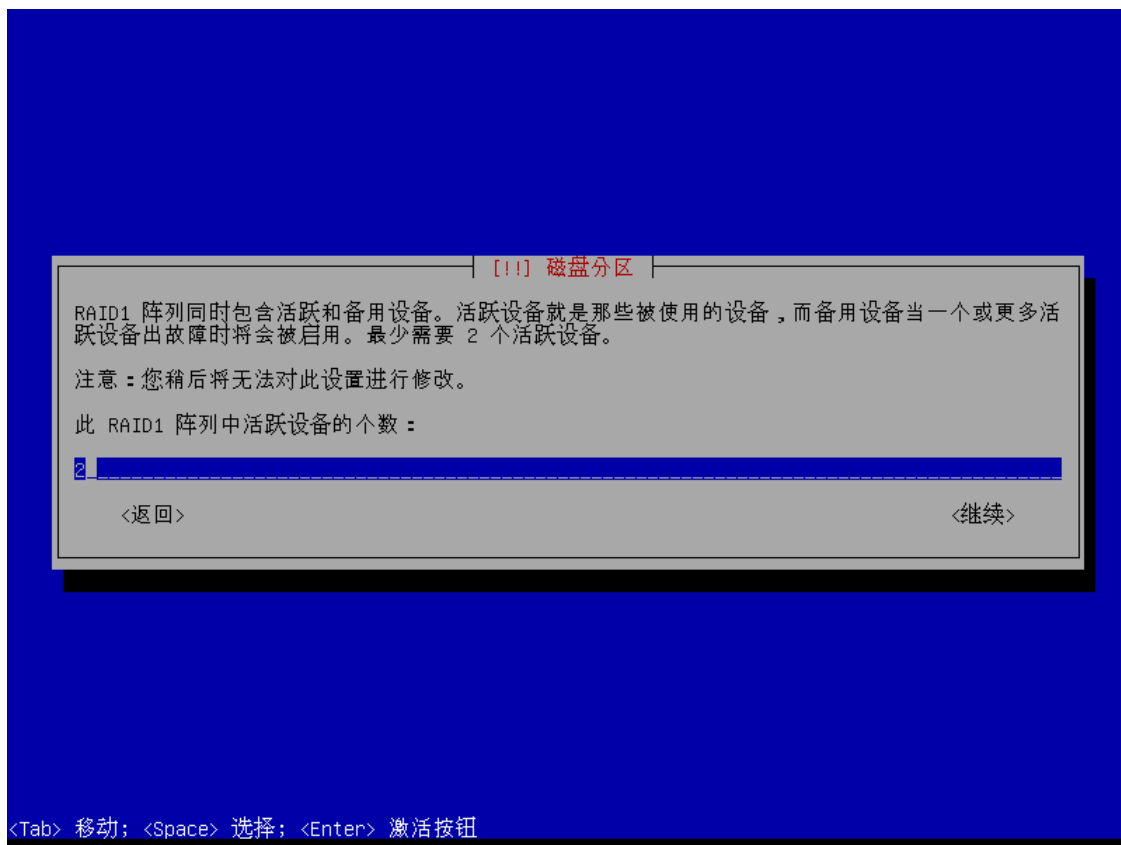


图 2.139: Raid阵列中活跃设备的个数

当活跃设备出故障时，将启用备用设备。

输入备用设备的个数，然后按 **Enter** 键，如图 2.140 所示。



图 2.140: Raid阵列中备用设备的个数

选择制作 RAID 的分区，然后按 键，如图 2.141 所示。



图 2.141: 选择 RAID 分区

创建完成后返回盘组配置界面。

2. 删除 MD 设备

选择“删除 MD 设备”，然后按 `Enter` 键至选择界面，如图 2.142 所示，选择要删除的 MD 设备，然后按 `Enter` 键。

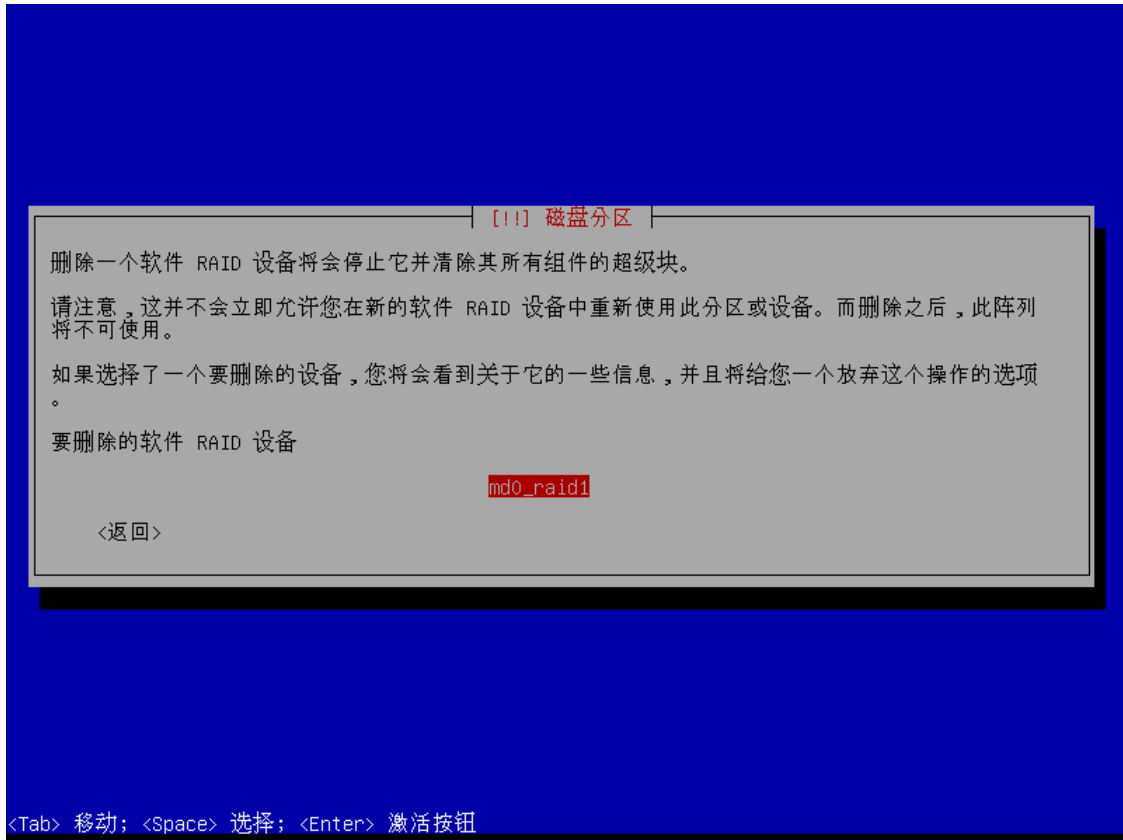


图 2.142: 删除 MD 设备

确认界面如图 2.143 所示，选择“是”，然后按 键确认删除。

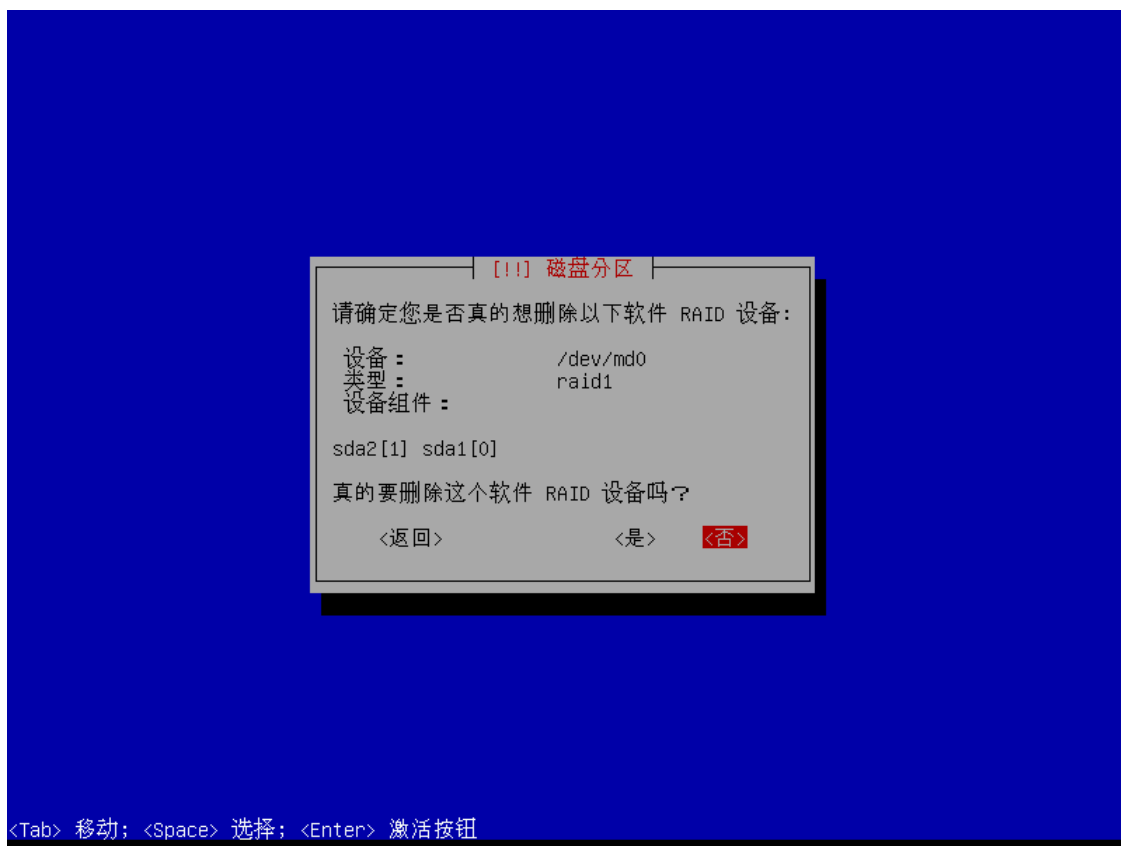


图 2.143: 确认删除 MD 设备

删除完成后返回盘组配置界面。

3. 配置完成

配置完成后，在盘组配置界面选择“完成”，然后按 **Enter** 键完成 RAID 配置并返回分区列表，如图 2.144 所示。



图 2.144: 完成 RAID 配置

您还可以修改这个 RAID 设备的分区设置，详见 2.4.4.3。

2.4.5 安装基本系统

确认分区操作完成后，分区结果将被写入磁盘并格式化分区，然后开始安装基本系统，安装的快慢要依据您的计算机的运行速度而定，如图 2.145 所示。



图 2.145: 安装基本系统

2.4.6 配置软件包管理器

配置软件包源，可用于安装或升级软件包，您可以插入CD或DVD并选择“是”进行扫描，作为配置软件包源，如图 2.146 所示。

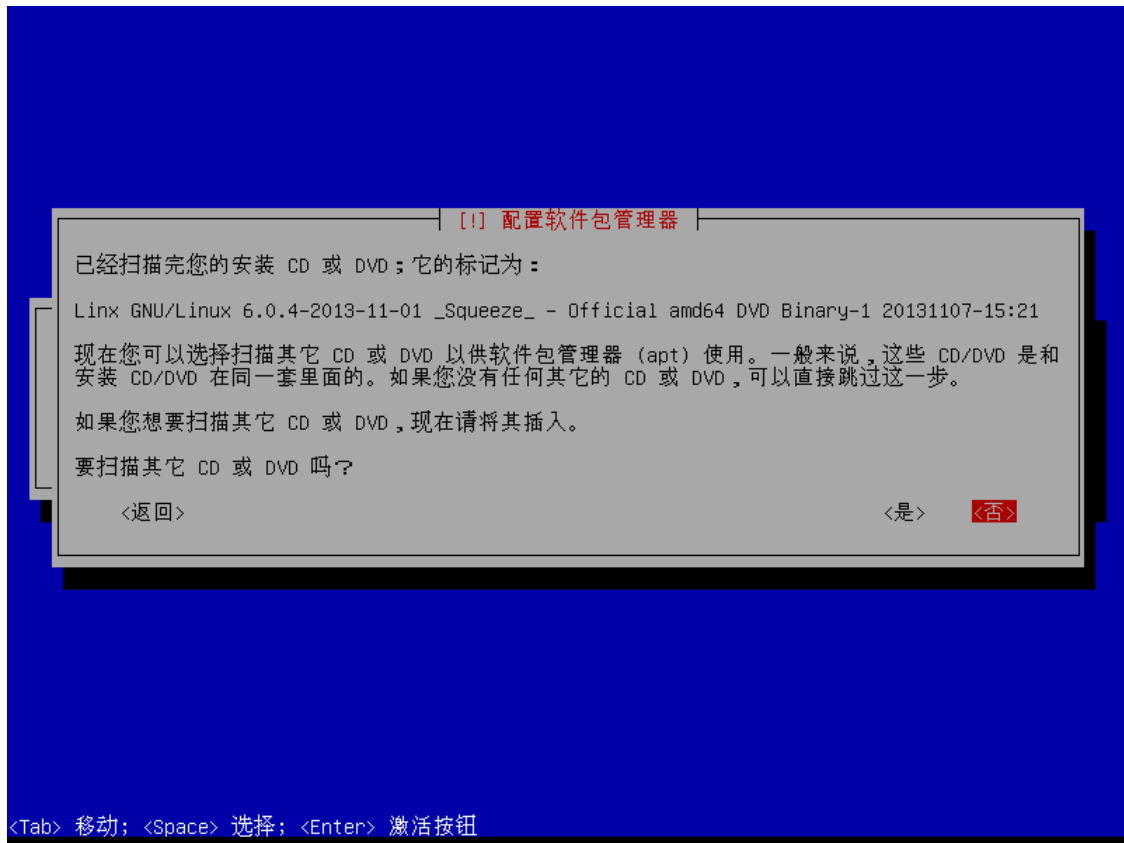


图 2.146: 扫描CD或DVD

或者使用网络镜像，如图 2.147 所示。

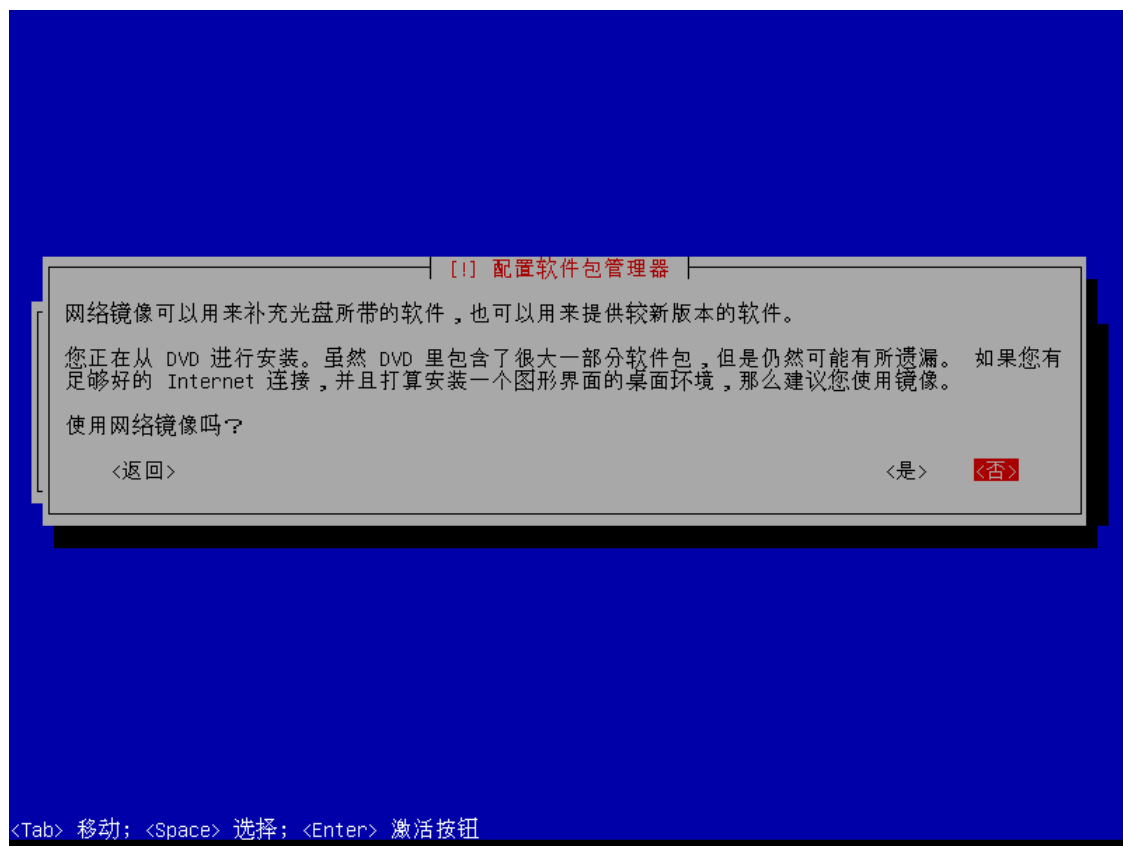


图 2.147: 网络镜像

选择“否”，然后按 **Enter** 键，转至下一步；选择“是”，然后点按 **Enter** 键，配置网络镜像。

安装程序将列出可用的网络镜像，您可以选择一个网络镜像或者选择“手动输入信息”，然后手动输入某个镜像的主机名和镜像所在的目录，如图 2.148 所示。



图 2.148: 设置网络镜像

输入将要使用的镜像的主机名，然后按 **Enter** 键，如图 2.149 所示。

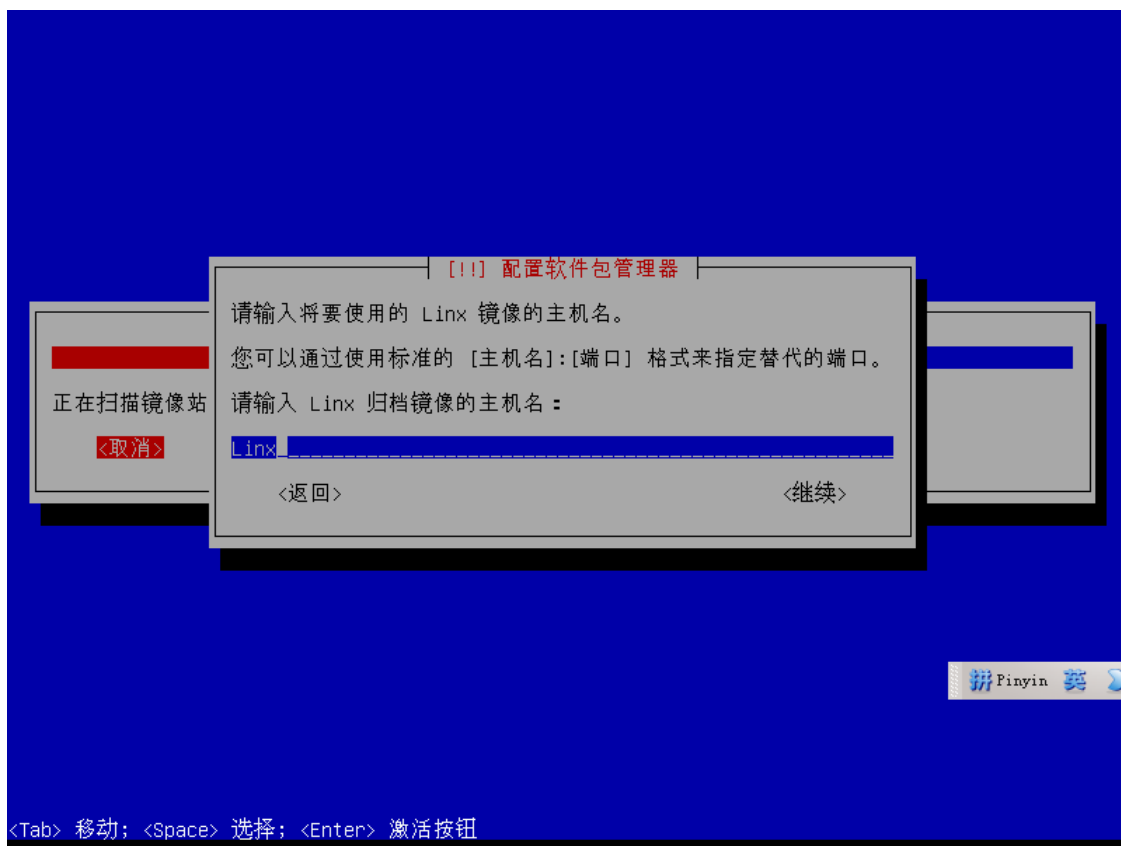


图 2.149: 设置镜像的主机名

输入镜像所在的目录，然后按 **Enter** 键，如图 2.150 所示。



图 2.150: 设置镜像所在目录

如果需要使用代理来连接外部网络，输入 HTTP 代理信息，否则请空置，如图 2.151 所示，然后按 **Enter** 键。



图 2.151: 输入 HTTP 代理信息

设置了正确的网络镜像后，即可使用该网络镜像进行软件包的安装、升级，否则需要重新设置或选择不使用网络镜像。

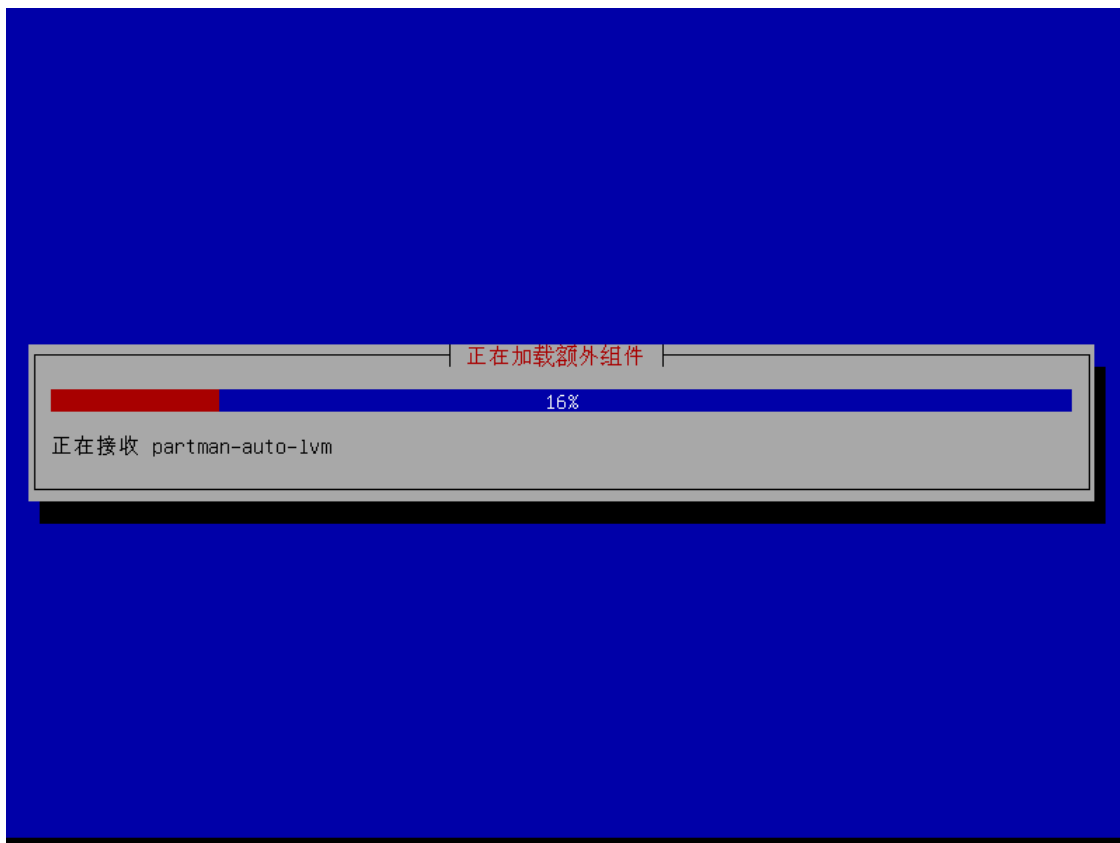


图 2.152: 加载软件选择组件

安装程序将加载软件选择组件，进入软件包选择界面。

2.4.7 选择应用软件包

在之前的安装过程中，已安装了基本系统，这里可以定制安装应用软件包，如桌面环境和各种服务。



图 2.153: 选择应用软件包

可供选择的软件集如下：

- 服务器运行环境
- 图形工作站
- 办公套件
- 开发环境

关于软件集的介绍详见 2.3.12。

选中软件集前的复选框，然后按 `Enter` 键，开始安装应用软件包，安装的快慢要依据您所选择的软件包数量和您的计算机的运行速度而定，如图 2.154 所示。

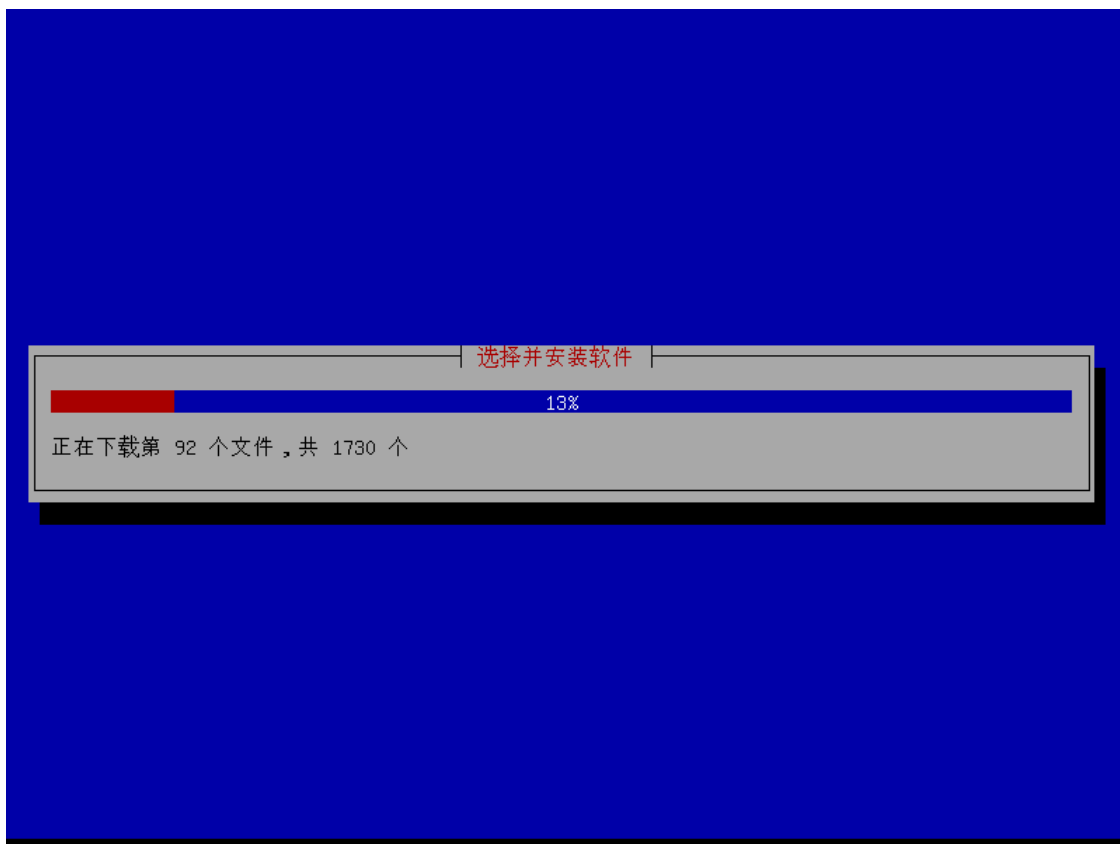


图 2.154: 安装应用软件包

在安装软件的过程中，您还需要手动配置一些参数。

2.4.8 配置服务器参数

如果您选择了安装“服务器运行环境”，将安装 MySQL、Samba、ProFTPd、Postfix 等服务，安装过程中还需要进行一些设置。

2.4.8.1 设置 MySQL 管理员口令

如果您选择了安装“服务器运行环境”，将安装 MySQL 数据库软件，建议您在安装过程中设置 MySQL 管理员口令，如图 2.155 所示。

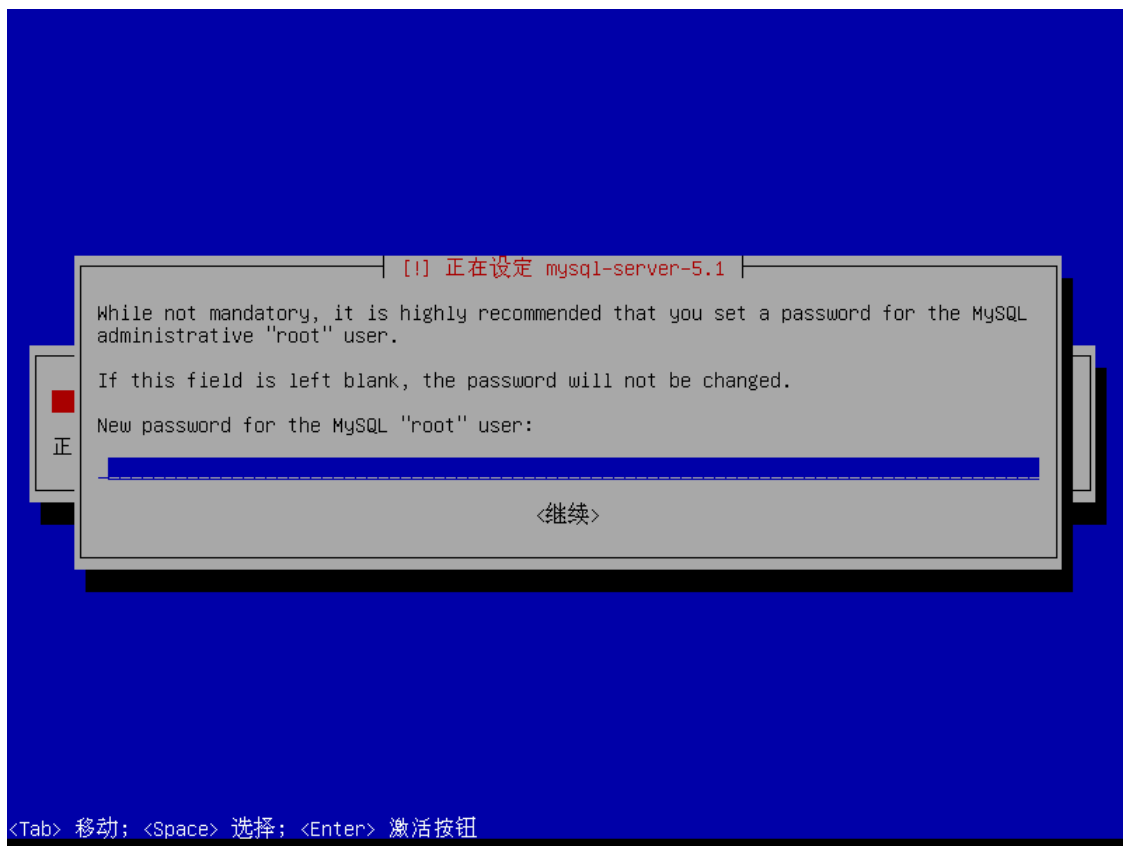


图 2.155: 设置MySQL管理员口令

再次输入 MySQL 管理员口令，然后按 键。



图 2.156: 重复MYSQL管理员口令

2.4.8.2 配置 Samba 服务

如果您选择了安装“服务器运行环境”，安装文件服务器软件，需要配置 Samba 服务，如图 2.157 所示。

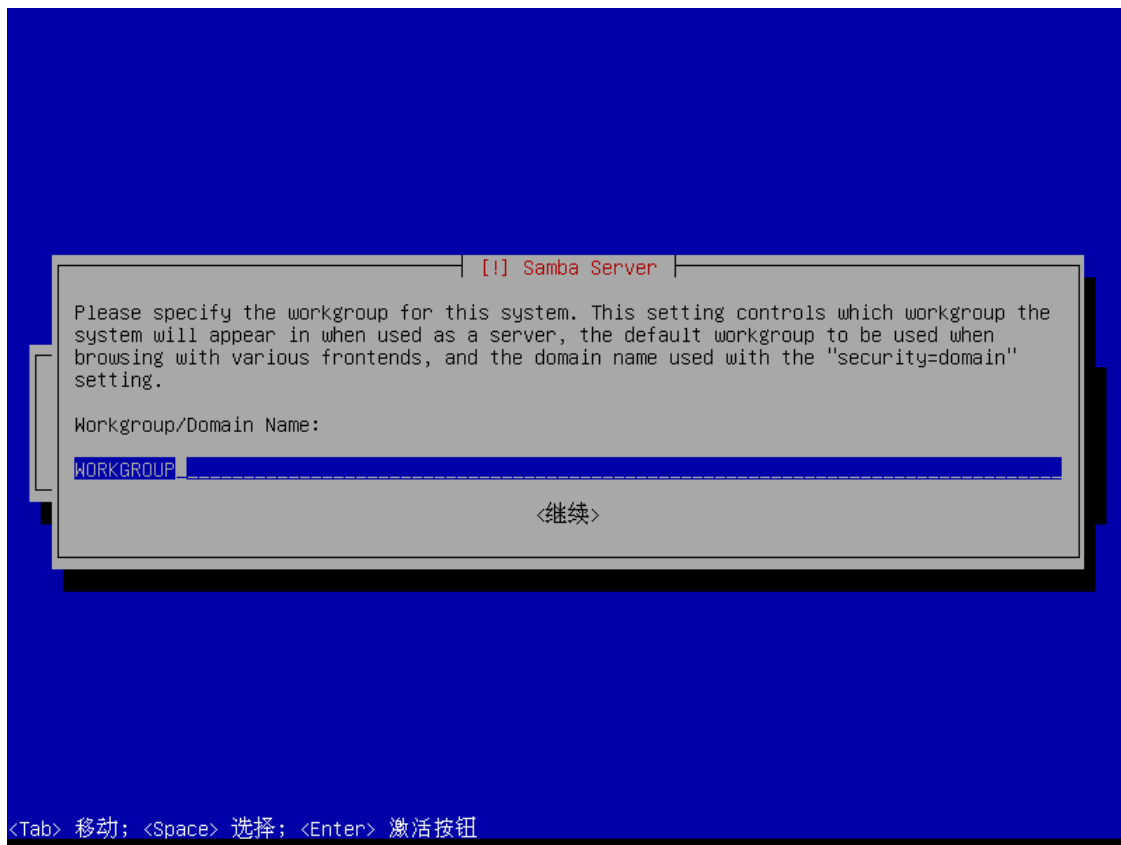


图 2.157: 配置 Samba 服务

输入工作组名称，然后按 键。

2.4.8.3 配置 FTP 服务

如果您选择了安装“服务器运行环境”，安装文件服务器软件，需要配置 ProFTPD 服务，如图 2.158 所示。

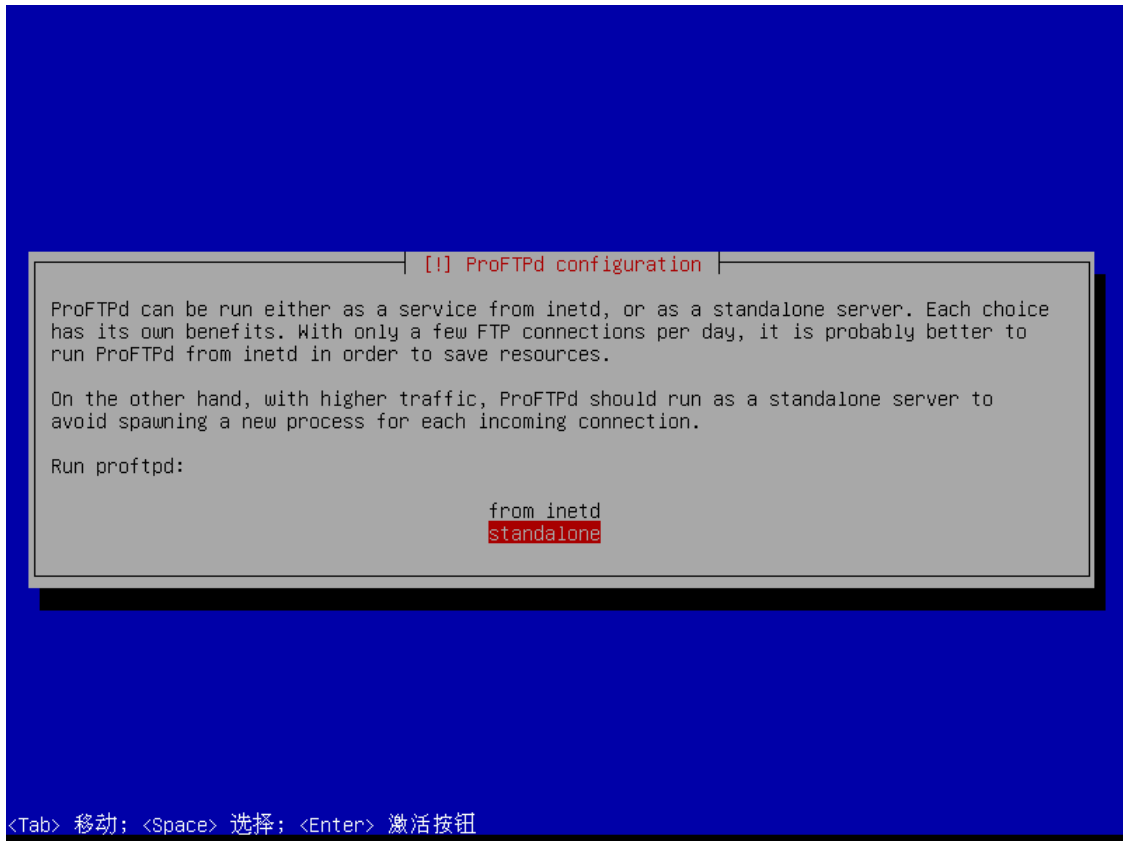


图 2.158: 配置 FTP 服务

选择ftp工作方式，然后按 键。

2.4.8.4 配置 Postfix 服务

如果您选择了安装“服务器运行环境”，将安装 Postfix 邮件服务器，需要配置 Postfix 服务，如图 2.159 所示。

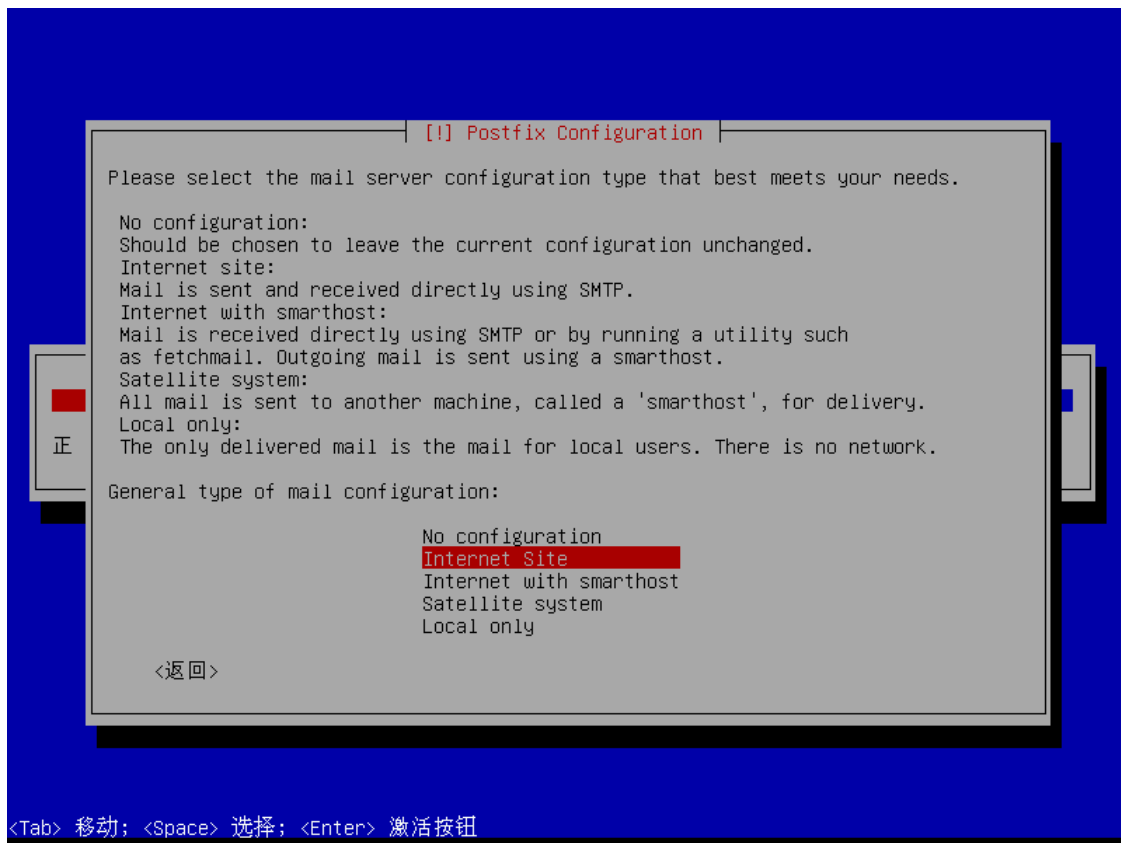


图 2.159: 配置 Postfix 服务

选择默认的邮件类型，然后按 键。

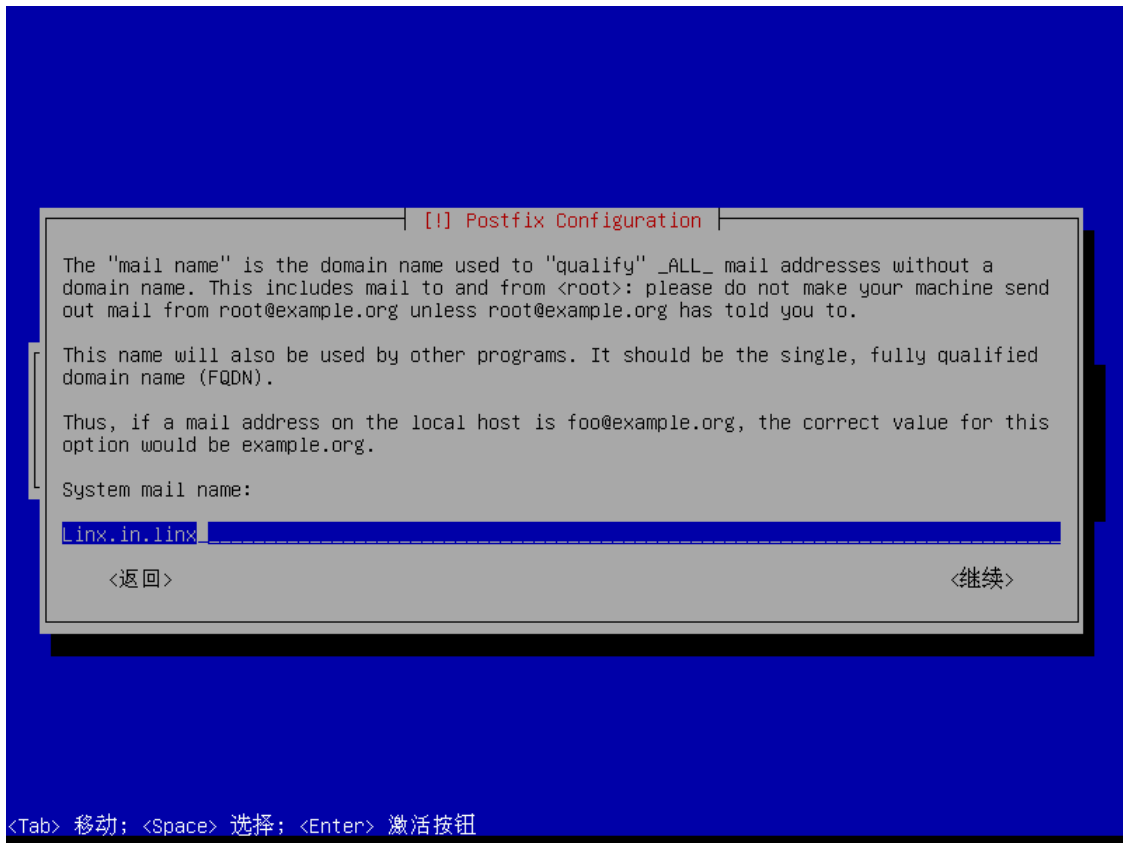


图 2.160: 配置系统邮件名称

输入系统邮件名称，然后按 键。

2.4.9 安装 GRUB

软件包安装完毕后，还将安装 GRUB。

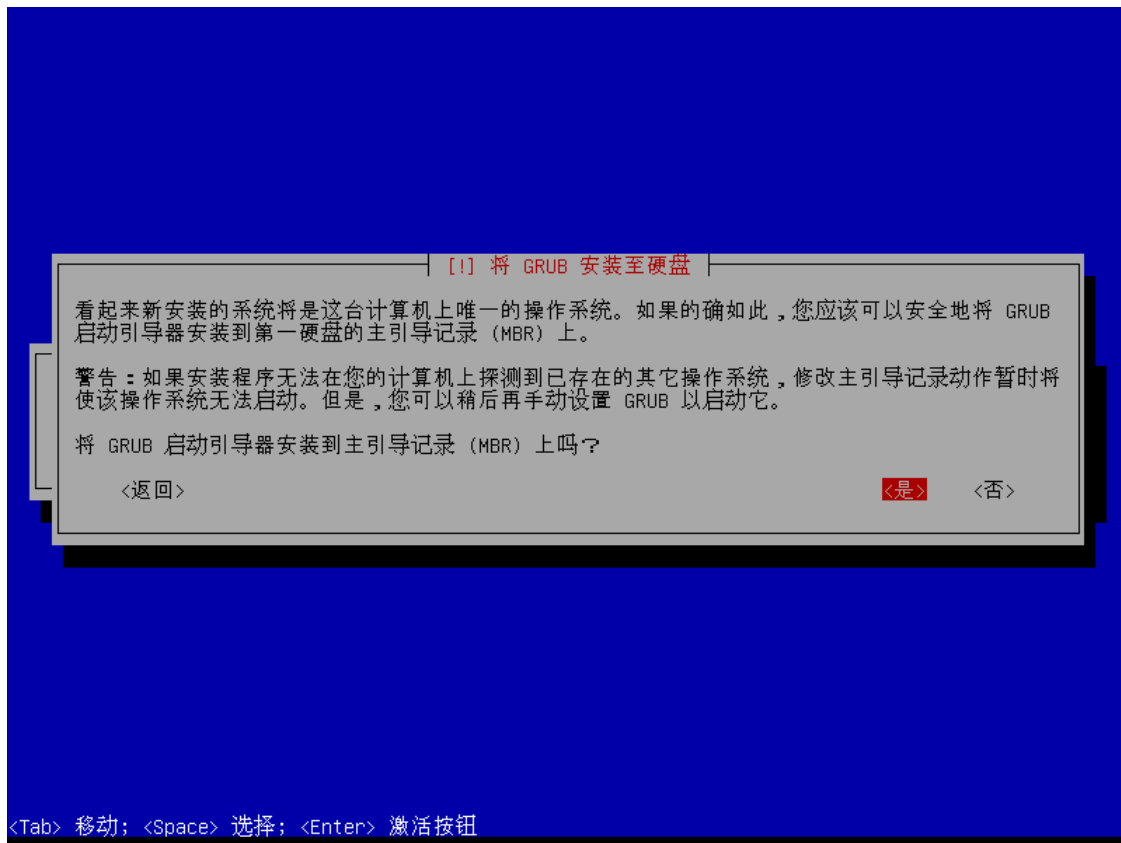


图 2.161: 安装 GRUB

您可以选择将GRUB安装到主引导记录 (MBR) 上，选择“是”，然后按 **Enter** 键。

或者选择“否”，然后手动设置引导分区，如图 2.162 所示。

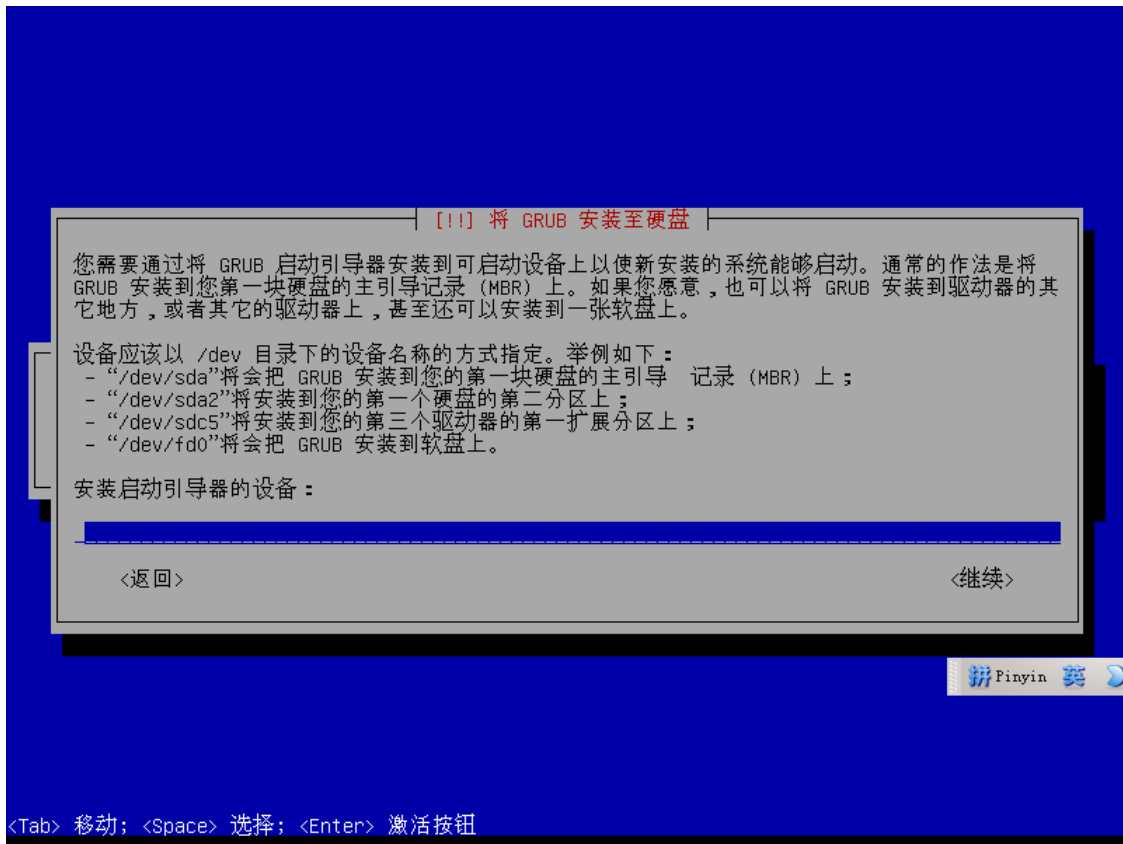


图 2.162: 手动设置引导分区

输入要安装GRUB的分区, 然后按 **Enter** 键。

小心

如果该计算机上存在其它操作系统, 安装 GRUB 可能会影响到其它操作系统的启动。

2.4.10 安装完成

安装程序将保存设置，结束安装进程，如图 2.163 所示。

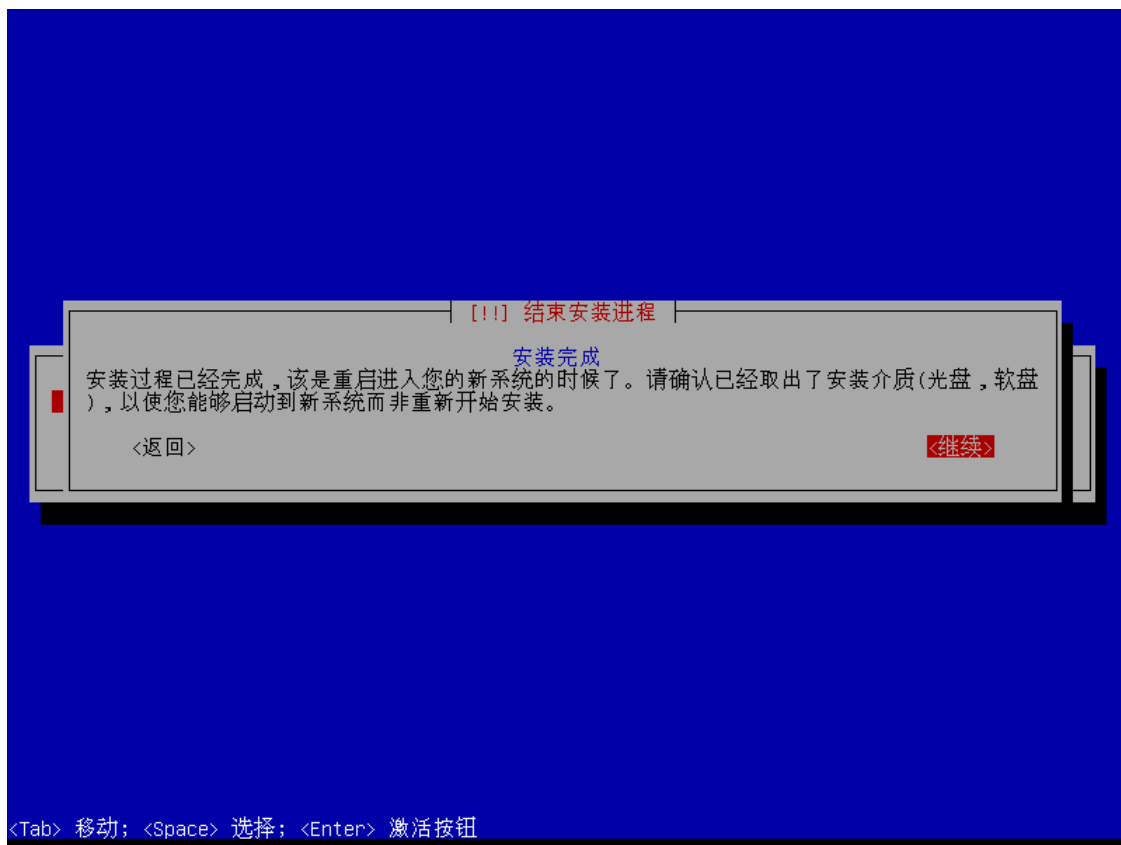


图 2.163: 结束安装进程

安装完成后，选择“继续”，然后按 键将重启计算机。

2.4.11 中止安装

安装过程中，如果您想退出安装，可以按 **ESC** 退出当前界面到安装程序主菜单，如图 2.164 所示。

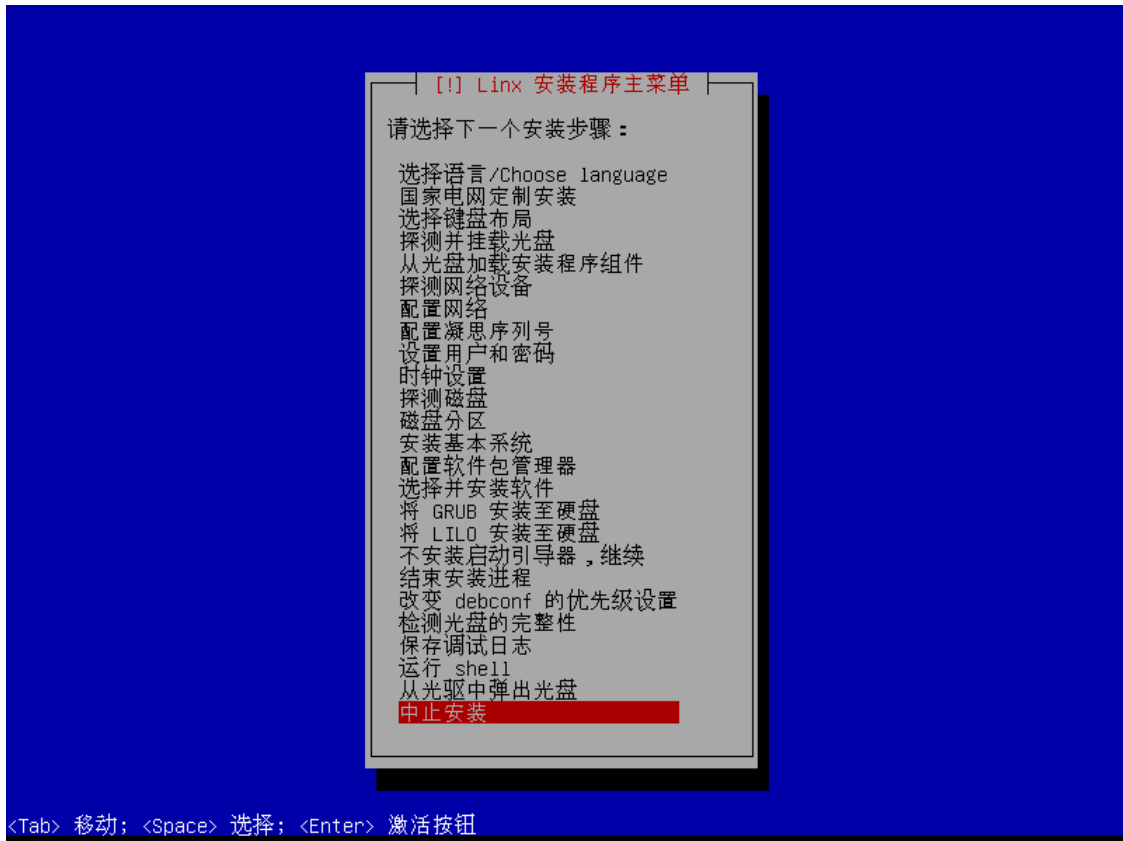


图 2.164: 中止安装

选择“中止安装”，然后按 **Enter** 键，转至中止安装确认界面，如图 2.165 所示。



图 2.165: 确认退出

选择“是”，然后按 **Enter** 键即可退出安装；选择“否”，然后点击 **继续** 可返回安装程序主菜单，然后选择某个安装步骤，再按 **Enter** 键继续安装系统。

2.5 自动安装

上面两节分别介绍了图形界面和字符界面的安装步骤，除此之外，您还可以选择自动安装，只需要执行很少的步骤即可完成安装。

在启动界面中选择“Automated install”，将进入字符界面的自动安装模式，自动加载及设置参数，如图 2.166 所示。

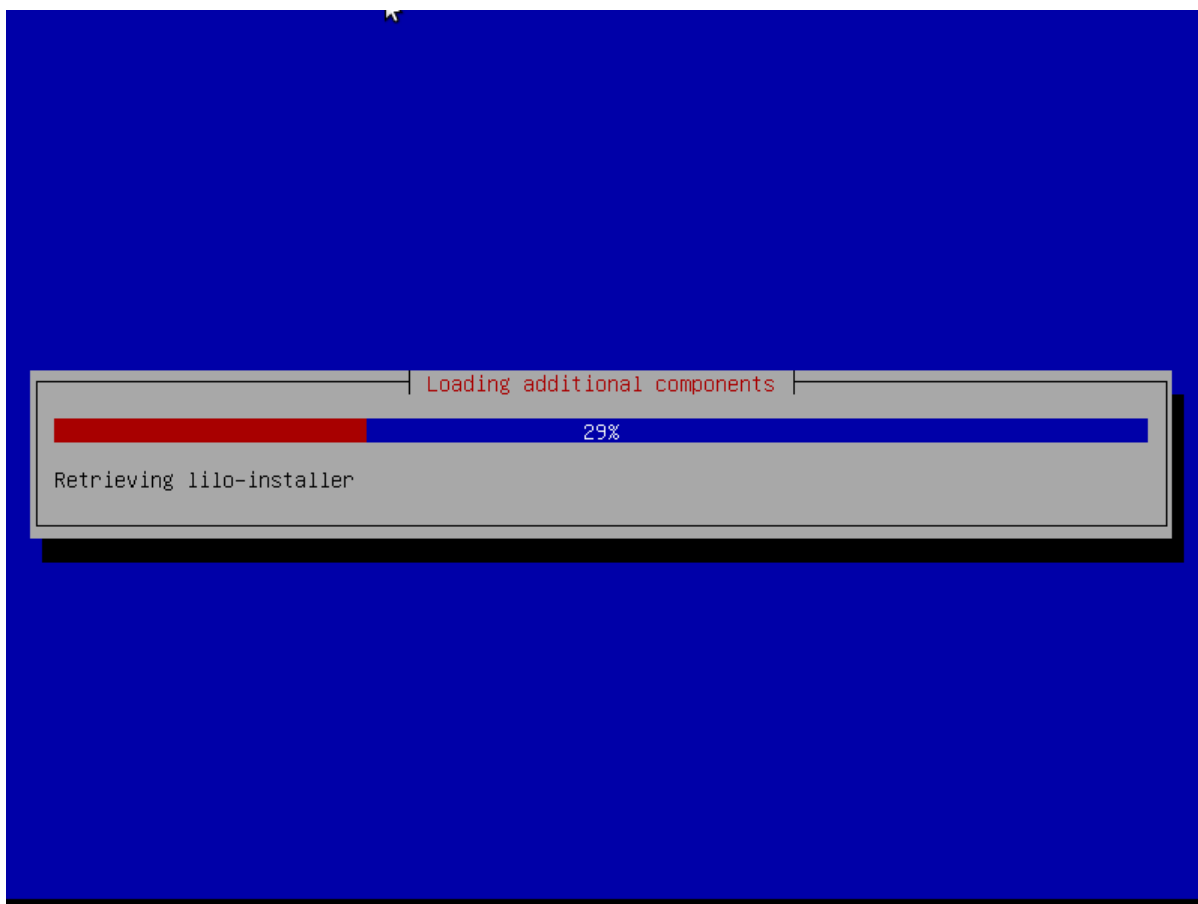


图 2.166: Loading additional components

除了磁盘分区操作外您不需要进行任何设置，关于磁盘分区，详见 2.4.4。

2.6 电网定制安装

在启动界面选择“Advanced options”，然后选择“State Grid automated install”，即可进入电网定制安装模式，安装程序将根据定制方案进行自动安装，同样，您需要进行磁盘分区操作，详见 2.4.4。

第3章 网络部署

凝思安全操作系统 V6.0.60 支持大规模网络部署。本章将具体介绍凝思操作系统 V6.0.60 网络部署的原理、配置与实施过程。

3.1 原理

计算机系统加电后的启动过程可以大致分为三个阶段：引导程序（bootloader）的加载、操作系统内核（kernel）的加载和操作系统的启动运行。其中，“引导程序的加载”这一功能一般由 BIOS 实现，“操作系统内核的加载”这一功能由引导程序实现，“操作系统的启动运行”这一功能由操作系统内核实现。

随着计算机应用的发展，引导程序可以放置在各种硬件存储设备上，也就是说，操作系统目前可以有多种引导方式，如从硬盘引导、从光盘引导、从 USB 设备引导、以及从网络引导等。PXE 技术规范就是基于网络引导的解决方案。PXE 的全称为 Preboot eXecute Environment，是由 Intel 公司开发的技术规范，支持工作站通过网络从远端服务器加载引导程序。它采用客户端/服务器的网络模式，利用 DHCP/BOOTP 协议从服务器端获得客户端计算机系统的 IP 地址，然后客户端再利用 TFTP 协议从服务器端下载引导程序。在 PXE 技术规范中，这个引导程序称为 Network Bootstrap Program（NBP）。PXE 技术只负责解决计算机系统如何通过网络加载引导程序的问题，而 NBP 运行后的行为，PXE 规范中并没有定义。也就是说，如果 NBP 运行后加载的是正常的操作系统的内核程序，那么该计算机系统将会成为无盘工作站；如果 NBP 运行后加载的是操作系统的安装程序（installer），那么该计算机系统就进入操作系统的安装模式，并将操作系统安装到其本地的硬盘中。操作系统网络部署即是指后者这种情况。

综上所述，操作系统网络部署的原理为：计算机系统加电后，指定“从网络加载引导程序”，然后计算机系统利用 PXE 技术从服务器端下载引导程序，引导程序运行后从服务器端下载操作系统安装程序并运行该安装程序开始操作系统的安装过程。操作系统将被安装到计算机系统本地的硬盘当中，安装结束后，计算机系统将可以从本地硬盘引导启动操作系统。

3.2 环境配置

操作系统的网络安装需要作如下配置：

1. PXE 客户端与 PXE 服务器端的配置。
2. 与 NBP 相关的配置。
3. 与操作系统安装过程相关的配置

3.2.1 PXE 客户端与 PXE 服务器端的配置

由于 PXE 技术使用客户端/服务器的方式实现，为了使用 PXE 技术进行操作系统的网络部署，需要在待安装操作系统的计算机系统上，以及该计算机系统所处的网络中的服务器进行相关的配置。

3.2.1.1 待安装操作系统的计算机系统的配置（PXE 客户端）

目前，PXE 客户端程序已经预置在网卡当中。如果计算机系统使用的是独立网卡，那么不需要做任何配置。如果网卡被集成在计算机系统的主板上，那么需要通过 BIOS 将其打开。具体操作如下：进入 BIOS，找到“LAN Option ROM”选项，将其设置为“Enabled”。

3.2.1.2 DHCP 服务器的设置（PXE 服务器端）

在实际应用中，PXE 客户端启动后，会首先向网络中广播 DHCP 请求，从而获得自己的 IP 地址。所以，服务器端必须能够响应该 DHCP 请求，也就是说，服务器端必须首先配置 DHCP 服务。这里只描述 DHCP 服务与 PXE 客户端处于同一网段内的情况。

在凝思操作系统中，DHCP 服务可以配置为随操作系统一同启动。启动脚本为：`dhcp3-server`，位于目录 `/etc/init.d` 下（如果没有该文件，说明还没有安装该服务器，安装命令为 `apt-get install dhcp3`）。您还可以修改 DHCP 服务的配置文件使其满足各种不同应用的需求。DHCP 服务的配置文件为：`dhcpd.conf`，位于目录 `/etc/dhcp3/` 下。

一个可能的 `dhcpd.conf` 文件内容如下：

```
#Start of dhcpd.conf
option domain-name-servers 172.16.0.254;
default-lease-time 86400;           # 默认租约时间为1天
max-lease-time 604800;             # 默认最大租约时间7天
allow booting;
allow bootp;
authoritative;

subnet 172.16.0.0 netmask 255.255.255.0 {
    range 172.16.0.212 172.16.0.215; # IP地址范围
    next-server 172.16.0.100;        # 为PXE客户端提供TFTP服务的
                                     # 服务器IP地址。
    filename "/tftpboot/pxelinux.0"; # NBP的路径及文件名。
    option subnet-mask 255.255.255.0;
    option broadcast-address 172.16.0.255;
    option routers 172.16.0.254;
}

host rd53 {                          # 将IP地址与MAC地址绑定。
    hardware ethernet 00:21:85:06:8a:66;
    fixed-address 172.16.0.153;
}

ddns-update-style none;
#End of dhcpd.conf
```

关于 DHCP 服务的更详细的配置介绍可以参考 `dhcpd.conf` 的手册页 (`man dhcpd.conf`)，以及位于目录 `/usr/share/doc/dhcp3-server/examples` 下的一个配置文件的例子 `dhcpd.conf`。

由 DHCP 服务的配置文件可知，PXE 客户端除获得 IP 地址信息外，还将获得 TFTP 服务器的 IP 地址，以及网络引导程序 NBP 的存放位置。PXE 客户端根据这些信息，便可以利用 TFTP 协议开始下载引导程序并安装操作系统了。

**注意**

TFTP 服务器的地址、客户机的网卡 MAC 地址和 IP 地址均需根据真实的实施场景进行设置。

3.2.1.3 高级 TFTP 服务器的配置 (PXE 服务器端)

服务器端可以使用 `atftpd` (advanced TFTP server) 提供 TFTP 服务, 该服务通过 `inetd` 启动 (后文所说的 TFTP 服务均指 `atftpd` 提供的 TFTP 服务)。为了符合 PXE 客户端的需求, 需要在 TFTP 服务器上, 以 `root` 用户身份创建目录 `/tftpboot`。该目录必须与 DHCP 服务中的配置信息

```
filename "/tftpboot/pxelinux.0";
```

保持一致。

通常情况下, TFTP 服务的启动配置信息包含在 `inetd` 的配置文件中。例如, 在 `/etc/inetd.conf` 文件中加入如下信息:

```
tftp dgram udp4 wait nobody /usr/sbin/tcpd /usr/sbin/in.tftpd
--tftpd-timeout 300 --retry-timeout 5 --mcast-port 1758
--mcast-addr 239.239.239.0-255 --mcast-ttl 1 --maxthread 100
--verbose=5 /tftpboot
```



注意

`/tftpboot` 表示 TFTP 只对该目录下的内容提供下载服务。

TFTP 服务可以通过命令 `/etc/init.d/inetutils-inetd restart` 启动。



提示

其它的 TFTP 服务器 (`tftpd`) 可能不能正常工作, 为确保能正常工作请使用 `atftpd` 来提供 TFTP 服务

3.2.2 与 NBP 相关的配置

3.2.2.1 NBP 的配置

凝思操作系统的网络部署软件模块提供了 `pxelinux.0` 程序、`pxelinux.cfg` 目录、一个默认的配置文件的 `default`、安装程序的内核文件和根文件系统镜像文件。负责网络部署的人员只需将凝思操作系统的网络部署软件模块解压到 `/tftpboot` 目录下即可。

下面对 NBP 的工作原理做一简要介绍。

在 Linux 操作系统的引导程序中, `SYSLINUX` 是一款非常成熟稳定的引导程序, 而 `PXELINUX` 则从 `SYSLINUX` 演化出来, 用于通过网络引导 Linux 操作系统。这里使用

PXELINUX 作为 NBP。

首先，将引导程序 `pxelinux.0` 放到上节提到的目录 `/tftpboot` 下，从而保证安装过程的接续运行。然后，在该目录下创建目录 `pxelinux.cfg`，将 `pxelinux.0` 运行时需要加载的配置文件放到该目录下。一个默认的配置文件的内容为：

```
default install
label install
menu label ^Install
menu default
kernel linux
append vga=normal initrd=initrd.gz -- quiet
```

配置文件中主要指定了要加载的操作系统内核和根文件系统镜像文件的名称和存放路径，该路径为相对 `/tftpboot` 的路径。

配置文件的名称可以为 PXE 客户端的 UUID 名称，PXE 客户端的网卡 MAC 地址，PXE 客户端 IP 地址16进制值（如：192.0.2.91 对应C000025B）的全部或部分，或者为 `default`。假设引导程序在 TFTP 服务器上存放的路径为 `/tftpboot/pxelinux.0`，PXE 客户端的 UUID 为 `b8945908-d6a6-41a9-611d-74a6ab80b83d`，网卡 MAC 地址为 `88:99:AA:BB:CC:DD`，IP 地址为 `192.0.2.91`，则 PXE 客户端会严格按照如下顺序寻找并下载配置文件：

```
/tftpboot/pxelinux.cfg/b8945908-d6a6-41a9-611d-74a6ab80b83d
/tftpboot/pxelinux.cfg/01-88-99-aa-bb-cc-dd
/tftpboot/pxelinux.cfg/C000025B
/tftpboot/pxelinux.cfg/C000025
/tftpboot/pxelinux.cfg/C00002
/tftpboot/pxelinux.cfg/C0000
/tftpboot/pxelinux.cfg/C000
/tftpboot/pxelinux.cfg/C00
/tftpboot/pxelinux.cfg/C0
/tftpboot/pxelinux.cfg/C
/tftpboot/pxelinux.cfg/default
```

3.2.3 与操作系统安装过程相关的配置

3.2.3.1 apache 服务器的配置

当使用光盘来安装操作系统时，操作系统的软件包都存放在光盘上，而当通过网络安装时，操作系统的软件包必须通过网络获得。也就是说，此时操作系统的软件包必须放置在网

络中的某台服务器上。为了满足凝思操作系统网络部署的需求，需要在网络中配置 apache 服务器，为网络中的客户端提供文件下载服务。

apache 服务器对外提供文件下载服务时，缺省的文件存放目录为 `/var/www`。负责网络部署的人员需要在该目录下，以 root 用户身份创建一个新目录，如 `rocky`。然后，将凝思操作系统网络安装光盘中的内容复制到目录 `/var/www/rocky` 下。这样，凝思操作系统在网络部署过程中，就可以利用 apache 服务从该服务器上下载所需的软件包并安装。

apache 服务器一般随计算机系统的启动而启动。apache 服务器的配置信息在文件 `/etc/apache2/apache2.conf` 中，启动脚本为 `/etc/init.d/apache2`。

3.2.3.2 操作系统安装程序的释放

将凝思操作系统的网络部署软件模块 `net-installer.tar.gz`¹ 释放到 TFTP 服务器的 `/tftpboot` 目录下即可。如果不希望配置操作系统通过网络自动化安装的功能，则可以开始实施操作系统的网络安装过程了。

3.2.3.3 操作系统安装过程自动化的配置

为了满足操作系统大规模网络部署的要求，实现操作系统安装过程自动化是非常必要的。操作系统在安装过程中需要得到很多配置信息，如：使用的语言环境，网络配置，硬盘分区等。为了实现操作系统安装过程的自动化，可以将这些信息放置在指定的配置文件当中，操作系统在安装过程中将从这个配置文件中得到相关信息，从而实现安装过程的自动化。

凝思操作系统的网络部署软件模块中已经内置了该配置文件。具体操作如下：

1. 将凝思操作系统网络安装光盘中的网络部署软件模块 `net-installer.tar.gz` 释放到 TFTP 服务器的 `/tftpboot` 目录下。
2. 将文件 `/tftpboot/preseed.cfg` 放置在 apache 服务器上软件包源的根目录下，如目录 `/var/www/rocky` 下。并修改 `preseed.cfg` 文件中的如下内容：

```
d-i mirror/http/hostname string rocky.mirror.server
d-i mirror/http/directory string /rocky
```

使其指向真实的 apache 服务器的地址（hostname）和目录（directory）。

修改

```
d-i passwd/root-password-crypted password
$1$SzpUqgPG$X3c6DBG6ytQUNUvO6kU/d.
```

¹网络部署软件模块未包含在凝思安全操作系统 V6.0.60 的安装光盘中，如需使用，请联系北京凝思科技有限公司技术支持部。

将“\$1\$SZpUqgPG\$X3c6DBG6ytQUNUv06kU/d.”替换为真实的 root 口令的 MD5 hash 值。
该 MD5 hash 值可以用命令：

```
echo "your_root_password"|mkpasswd -s -H MD5
```

获得。

修改其他配置信息，如硬盘分区信息等。

3. 修改安装程序相关的配置信息。

将文件 /tftpboot/pxelinux.cfg/default 中的

```
timeout 0
```

修改为

```
timeout 1
```

这样修改后，安装程序将会直接按缺省安装选项启动安装程序。

4. 修改安装程序启动时的命令行参数。

将文件/tftpboot/rocky-installer/amd64/boot-screens/txt.cfg 中的

```
append vga=normal initrd=initrd.gz -- quiet
```

修改为

```
append vga=normal auto=true initrd=initrd.gz locale=en_US  
preseed/url=http://your.apache.server/rocky/preseed.cfg  
netcfg/get_hostname=seen netcfg/get_domain=seen -- quiet
```

- 参数“auto=true”表示设置安装程序进入自动安装状态。
- 参数“locale=en_US”用于设置操作系统的语言信息。
- 参数“preseed/url=http://your.apache.server/rocky/preseed.cfg”用于指定 preseed.cfg 文件的位置。注意：“your.apache.server”即为 apache 服务器的真实地址。
- 参数“netcfg/get_hostname=seen netcfg/get_domain=seen”表示计算机使用从域名服务器上得到的主机名和域名。

经过上面的配置后，就可以开始实施操作系统的网络自动安装过程了。

3.3 实施过程

3.3.1 DHCP、TFTP 和 apache 服务器的启动

当与操作系统网络安装相关的所有配置均完成后，就可以启动 DHCP、TFTP 和 apache 服务，为网络中的计算机提供操作系统的网络安装服务了。各服务的启动命令如下：

- DHCP 服务

```
/etc/init.d/dhcp3-server restart
```

- TFTP 服务

```
/etc/init.d/inetutils-inetd restart
```

- apache 服务

```
/etc/init.d/apache2 restart
```

3.3.2 网络安装过程的启动

当 DHCP、TFTP 和 apache 服务启动后，就可以启动 PXE 客户端，开始操作系统的安装了。当操作系统开始安装后，与通过其它介质安装操作系统的过程没有区别。如果设置了操作系统的网络自动化安装功能，那么整个安装过程不需要人工参与。这里仅叙述如何启动 PXE 客户端。

当计算机加电后，按 **F11** 键（某些主板要按 **F8** 键，如华硕的主板），在 BIOS 加载后，会弹出类似下面的界面：

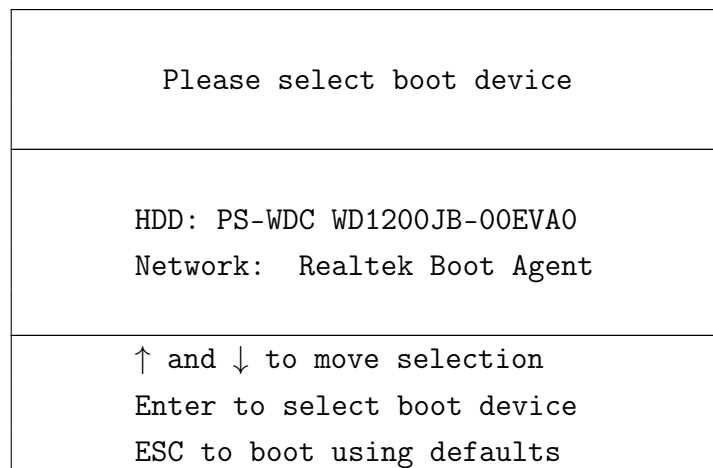


图 3.1: 引导程序选择界面

选择从网络启动后，PXE 客户端便会启动，显示类似下面的界面。

```
Intel UNDI, PXE-2.1 (build082)
Copyright(c) 1997-2000 Intel Corporation

For Reltek RTL8111B/8111C Gigabit Ethernet Controller
V2.11 (071127)

CLIENT MAC ADDR: 00 21 85 06 8A 66 GUID: 00000000-
0000-0000-0000-002185068A66
DHCP....
```

图 3.2: PXE 运行界面

进入该界面，表示 PXE 客户端开始通过 DHCP 服务获得 IP。一旦 PXE 客户端获得 IP 地址，便会通过 TFTP 加载网络引导程序 NBP，然后就会进入正常的操作系统安装界面了。

第4章 常见问题解答

本章用于解答凝思安全操作系统 V6.0.60 安装过程中或安装完毕后可能出现的一些问题，并建议了相应的解决方法。

当您无法解决该问题或者遇到文档中未提及的问题时，请详细记录该问题并联系北京凝思科技有限公司技术支持部。

1. 系统安装过程中死机

在系统安装过程中，由于硬件设备过新或硬件设备过旧都会出现兼容性问题，如果在安装过程中出现“卡死”现象。

1) 在系统安装首界面死机

如图 4.1 所示，当选择Install后回车，系统无任何响应死机。

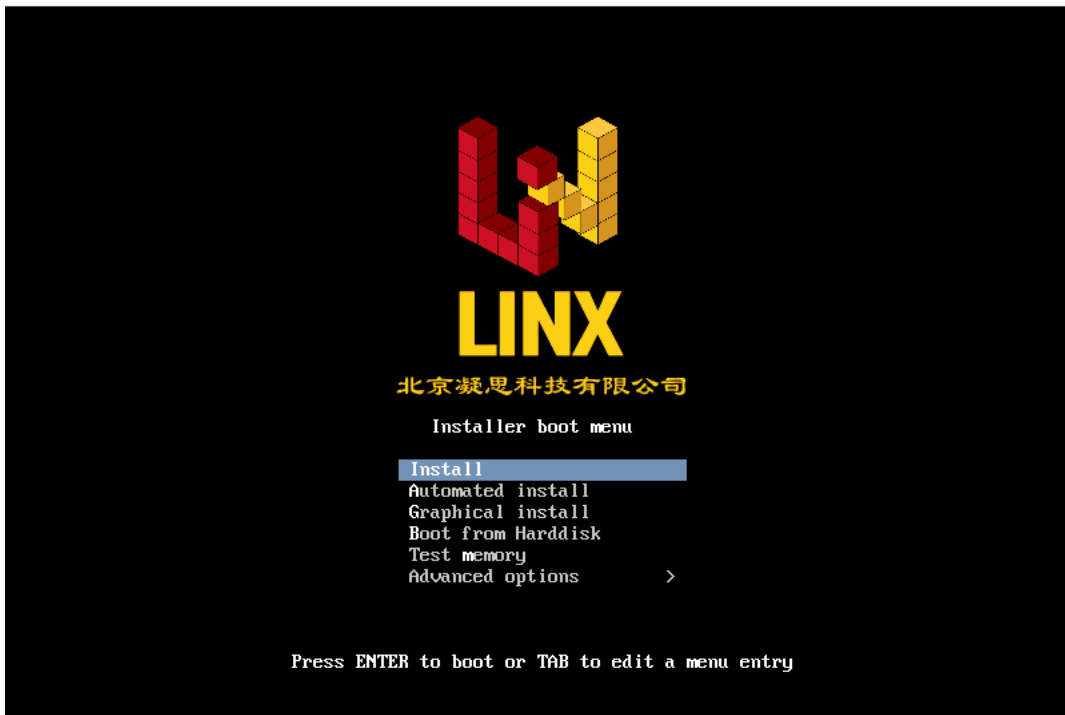


图 4.1: 系统安装首界面死机

此现象很有可能是因为使用了与目标硬件不相符的体系结构的操作系统版本。请与技术支持部门联系，确认安装介质中操作系统的版本。

2) 安装过程中界面无响应

如图 4.2 所示，安装过程中长时间停留在某一界面上并且无响应。



图 4.2: 安装过程中界面无响应

- 诊断方法一：切换至有安装信息的终端检查安装信息，Ctrl+Alt+F4切换至安装日志终端。
- 诊断方法二：通过切换到另一个空闲终端登入安装程序后台，检查响应配置文件或安装介质的挂载情况，或者通过检查相关日志文件的内容判断系统安装过程中出现什么问题。

使用快捷键Ctrl+Alt+F2切换至终端，按回车键登录系统，如图 4.3 所示。

```
Please press Enter to activate this console.

BusyBox v1.17.1 (Linux 1:1.17.1-8linux2) built-in shell (ash)
Enter 'help' for a list of built-in commands.

~ # _
```

图 4.3: 切换至终端登录系统

输入以下命令查看系统安装完整日志信息，判断是何种原因导致安装过程“卡死”。

```
less /var/log/syslog
```

如果需要使用网络将安装日志信息传到另一台机器中可以安装scp程序，再使用scp将日志文件传送之，命令如下：

```
anna-install openssh-client-udeb
ifconfig eth0 192.168.123.12 netmask 255.255.255.0
scp /var/log/syslog 192.168.123.11
```



提示

以上命令中涉及的IP地址应该根据实际情况配置。

2. 重启

安装完毕后重新启动计算机，仍然从光盘启动。

解决方法：

- 1) 将光盘从光驱中取出。
- 2) 在 BIOS 中，将硬盘设置为第一启动盘。

3. 挂载

用户定制了某分区方案，但某分区未按照预期挂载到某目录（挂载点）上。

解决方法：

使用系统管理员 `sysadmin` 登录到系统，修改 `/etc/fstab` 文件。

文件 `/etc/fstab` 存放的是系统中的文件系统信息。当正确的设置了该文件，则可以通过 `mount /directoryname` 命令来加载一个文件系统，每种文件系统都对应一个独立的行，每行中的字段由空格隔开。同时 `fsck`、`mount`、`umount` 等命令都利用该程序。

参数设置: `<device>` `<mount>` `<fstype>` `<option>` `<dump>` `<check>`

- `<device>`

该字段定义希望加载的文件系统所在的设备或远程文件系统，对于一般的本地块设备情况来说：IDE 设备一般描述为 `/dev/hdXN`，X 是 IDE 设备通道（a, b, or c），N 代表分区号；SCSI 设备一描述为 `/dev/sdXN`。对于 NFS 情况，格式一般为 `<host>:<dir>`，例如：`knuth.aeb.nl:/`。对于 procfs，使用 `proc` 来定义。

- `<mount>`

该字段描述希望的文件系统加载的目录点，对于 swap 设备，该字段为 `none`；对于加载目录名包含空格的情况，用 `40` 来表示空格。

- `<fstype>`

该字段定义该设备上的文件系统，一般常见的文件类型为 `ext2`、`ext3`、`vfat`（Windows 系统的 `fat32` 格式）、`NTFS`、`iso9600` 等。

- `<option>`

该字段指定加载该设备的文件系统时需要使用的特定参数选项，多个参数由逗号隔开。对于大多数系统使用 `defaults` 就可以满足需要。其它常见的选项包括：

- `ro`

以只读模式加载该文件系统。

- `sync`

不对该设备的写操作进行缓冲处理，这可以防止在非正常关机情况下破坏文件系统，但是会降低计算机的速度。

- `user`

允许普通用户加载该文件系统。

- `quota`

强制在该文件系统上进行磁盘定额限制。

- `noauto`

不再使用 `mount -a` 命令（例如系统启动时）加载该文件系统。

- <dump>

该选项被 `dump` 命令使用来检查一个文件系统应该以多快频率进行转储，若不需要转储就设置该字段为0。

- <check>

该字段被 `fsck` 命令用来决定在启动时需要被扫描的文件系统的顺序，根文件系统 / 对应该字段的值应该为 1，其它文件系统应该为 2。若该文件系统无需在启动时扫描则设置该字段为 0。

例样：

```
# /etc/fstab
/dev/hda9 swap swap defaults 0 0
/dev/hda1 / ext2 defaults 1 1
/dev/hda5 /home ext2 defaults 1 1
/dev/hda6 /usr ext2 defaults 1 1
/dev/hda7 /usr/local ext2 defaults 1 1
/dev/hda8 /var ext2 defaults 1 1
/dev/hdb /cdrom iso9660 noauto,user 0 0
proc /proc proc defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
```

附录 A 文件和目录

本章从目录的角度出发，总览整个系统，有关各个文件的详情，请参考手册页。

完整的目录树分为若干部分，如果将各部分挂载到不同的分区，将更易于进行备份和系统管理。目录树中，主要的几个部分是 `/`、`/usr`、`/var` 和 `/home`，各部分用途不同。具体描述如下：

`/` 目录是每台机器特有的（它一般保存在本地磁盘上，但也可保存在 RAM 磁盘或网络驱动器上），其中包含启动系统和引导装入文件系统所需的文件。因此，对单用户模式来说，只使用一个分区挂载 `/` 目录就足够了。另外，该目录内还包含一些工具，用于修复损坏的系统和从备份中恢复丢失的文件。

`/usr` 目录内包含所有的命令库，手册页和其他没有变动过的文件（这些文件是普通操作期间所需要的）。`/usr` 目录内没有专门针对哪台机器的文件，也没有普通用户操作期间应该修改的文件。这样一来，便可以通过网络实现文件共享，从而有效地节约成本，因为这样可节省磁盘空间（要知道 `/usr` 文件系统起码也有几百个 MB），使管理工作更容易（在更新应用程序时，只有 `master/usr` 需要改动，而不是逐一在每台机器上改动）。即使文件系统是在本地磁盘上，也可以采用只读方式装入它，减小系统崩溃时文件系统受损的可能性。

`/var` 目录中包含有变动的文件，比如假脱机目录（用于邮件、新闻、打印机等）、日志文件、格式化的手册页和临时文件。

`/home` 目录中包含用户的家目录，一般是系统保存用户数据的地方。把家目录和其它目录区分开是为了方便备份；其它部分通常是不需要备份的，或者说至少不需要经常备份（因为它们几乎没有变动）。一个大型的 `/home` 目录可能必须分为若干个小型的目录，这就需要在 `/home` 下面加一个额外的命名级别，比如 `/home/students` 和 `/home/staff`。

上述各个目录可以分别挂载到不同的分区。如果是一个小型的单用户系统，而且用户想一切简单明了的话，可以只挂载一个 `/` 目录。

不同用途的目录所需空间大小不同，可根据需要挂载到不同的分区。如果要使两个目录在同一个分区，例如 `/var` 和 `/usr`，可以将 `/var` 挂载到 `/usr/var` 目录，然后在 `/` 中建立一个链接到 `/usr/var` 的符号链接 `/var`。

A.1 /

一般说来，/ 应该较小，因为其中包含非常关键的文件和一个小型的，非频繁变动的文件系统。受损的 / 目录一般意味着系统不能启动，除非借助于特殊的启动设备（比如说软盘），所以一般不要轻易更改它。

/ 目录一般不包含任何文件，系统的标准启动镜像除外，这个镜像通常称为 /vmlinuz。其他的所有文件都保存在 / 目录的子目录下：

1. /bin

启动期间，可供普通用户使用的命令（也可能在启动之后）。

2. /sbin

和 /bin 一样，但不是供普通用户使用的，虽然在必要或经过允许的情况下，普通用户也可使用它们。

3. /etc

某台机器专用的配置文件。

4. /root

用户 root 的家目录。

5. /lib、/lib32

/ 目录上的程序所需的共享库。

6. /lib/modules

可装载的内核模块，特别是从灾难中恢复时，启动系统所需的那些模块（比如，网络和文件系统驱动程序）。

7. /dev

设备文件。

8. /tmp

临时文件。

9. /boot

启动装载程序所用文件，比如 LILO。内核镜像通常保存在这里，而不是 / 目录中。如果有多个内核镜像，这个目录就可能增长得很快，所以最好把它单独保存在一个文件系统内。这样做的另一个原因是确保内核镜像在 IDE 磁盘的前1024个磁道内。

10. /mnt

系统管理员临时装入的装入点。程序不会自行装入 /mnt。/mnt 也可以分为若干个子目录（比如 /mnt/dosa 可能是使用 MS-DOS 文件系统的软驱，而 /mnt/extra 则可能和 ext2 文件系统如出一辙）。

11. /proc、/usr、/var 和 /home

其它目录的装入点。

A.2 /etc

/etc 目录中包含许多文件。下面将讨论其中的一部分。另外的文件，则应该由你决定它们属于哪个程序，并参考该程序的手册页。许多网络配置文件也被包含在 /etc 内。

1. /etc/rc 或 /etc/rc.d 或 /etc/rc?.d

启动时或运行级别发生变化时运行的脚本或脚本的目录。

2. /etc/passwd

用户数据库，其中有一些字段指定用户名，用户真名，根目录，加密密码以及该用户的其他信息。

3. /etc/fstab

列出启动时由 `mount -a` 命令（在 /etc/rc 或等同的启动文件内）自动装入的文件系统。Linux 系统中，这个文件还包含一些信息，这些信息和 `swapon -a` 自动采用的交换区有关。

4. /etc/group

类似于 /etc/passwd，但它描述的不是用户，而是组。更多详情，请参考 group 手册页。

5. /etc/inittab

init 配置文件。

6. /etc/issue

登录提示出现之前的 getty 输出。通常包含对系统的简短说明或欢迎消息。其内容由系统管理员决定。

7. /etc/motd

日期消息，是在成功登录之后自动输出的。其内容由系统管理员决定。通常用来提示每个用户，比如既定的系统关闭警告等。

8. /etc/mtab

列出当前已装入的文件系统。最初是由启动脚本设置，由 `mount` 命令自动更新的。用于需要已装入文件系统列表时（比如说在运行 `df` 命令时）。

9. /etc/shadow

在已安装影子密码软件的系统上的影子密码文件。影子密码把已加密的密码从 `/etc/passwd` 移入 `/etc/shadow`；后者只有 `root` 才能读取。这样可进一步保证密码的安全性。

10. /etc/login.defs

`login` 命令的配置文件。

11. /etc/profile、/etc/csh.login 和 /etc/csh.cshrc

登录或启动时，由 Bourne 或 C 外壳执行的文件。这些文件允许系统管理员为所有的用户设置全局默认设置。各外壳的详情，请参考手册页。

12. /etc/securetty

标识安全终端，也就是允许 `root` 通过哪些终端登录。一般说来，只列出了虚拟控制台，如此一来，恶意用户不可能通过 `modem` 或网络攻击系统，从而获得超级用户特权（至少说很难）。

13. /etc/shells

列出受托（信得过的）外壳。`chsh` 命令允许用户把他们自己的登录外壳改成这个文件内列出的受托外壳。为计算机提供 FTP 服务的 `ftpd` 服务器进程，将复查用户的外壳是否在 `/etc/shells` 内，如果在，将允许用户登录，如果不在，就不会让用户登录。

A.3 /dev

`/dev` 目录下包含所有设备的特定设备文件。设备文件的命名有特殊的约定；对这些约定的描述包括在 `Device` 列表中。

A.4 /usr

`/usr` 通常较大，因为所有的程序都是保存在这个文件系统中的。`/usr` 内的文件通常是系统文件；本地安装的程序和其他东西都保存在 `/usr/local` 下面。这样一来，就能够通过安装该目录的新版本来升级系统，而不需要再次安装所有的程序。下面列出了部分 `/usr` 子目录。

1. /usr/bin

几乎包含所有的用户命令。有些命令在 `/bin` 或 `/usr/local/bin` 内。

2. `/usr/sbin`

`root` 文件系统上不需要的系统管理命令，例如，大多数服务器程序。

3. `/usr/share/man`, `/usr/share/info` 和 `/usr/share/doc`

分别包含手册页，GNU 信息文档和名目繁多的其他文档文件。

4. `/usr/include`

C 编程语言的头文件。实际上，为了保持数据的一致，这个文件应该保存在 `/usr/lib` 下面，但过去一直都采用这个名称。

5. `/usr/lib`、`/usr/lib32`

程序和子系统所用的未变动过的数据文件，其中包括一些和站点有关的配置文件。`lib` 这个名称源于库（library）；最初用来编写子例程的库都保存在 `/usr/lib` 和 `/usr/lib32` 内。

A.5 /var

`/var` 内包含系统正常运行时所改动的数据。它是各个系统专有的，也就是说，不能通过网络和其他计算机共享。

1. `/var/lib`

系统正常运行期间发生变化的文件。

2. `/var/lock`

锁文件。许多程序都习惯在 `/var/lock` 内建立一个锁文件，借以表明它们正在使用某个特定的设备或文件。其他程序将注意到这个锁文件，并不再尝试使用这个特定的设备或文件。

3. `/var/log`

日志文件，它源于各个程序，特别是 `login`（`/var/log/wtmp`，记录所有的系统登录和注销活动）和 `syslog`（`/var/log/messages`，通常保存所有的内核和系统程序消息）。`/var/log` 内的文件通常增长较快，需要定期清空。

4. `/var/run`

系统信息文件，其中包含系统相关信息，在系统下一次启动之前，都是有效的。例如，`/var/run/utmp` 内包含和当前登录用户有关的信息。

5. `/var/spool`

用于邮件，新闻，打印机队列和其他队列作业的目录。对每个不同的假脱机来说，在 /var/spool 下面都有其自己的子目录，比如用户信箱就在 /var/spool/mail 内。

6. /var/tmp

临时文件，通常存放较大或需要保存的时间比 /tmp 长的文件。

A.6 /proc

/proc 内包含一个伪文件系统，用于提供和系统相关的信息（最初是进程相关信息，并由此得名）。下面将对有些比较重要的文件和目录进行解释。/proc 文件系统的更多详情，请参考 proc 手册页。

1. /proc/1

目录，其中有1号进程的相关信息。每个进程在 /proc 下面都有一个子目录，这个子目录名就是该进程的编号。

2. /proc/cpuinfo

其中保存关于中央处理器的信息，比如型号，制造商，模型和性能等。

3. /proc/devices

其中列出了已经配置到当前正在运行的内核之中的设备驱动程序。

4. /proc/dma

展示当前正在使用的 DMA 通道。

5. /proc/filesystems

已配置到内核中的文件系统。

6. /proc/interrupts

展示哪些中断号正在使用中，以及各中断号使用了多少次。

7. /proc/ioports

展示此时哪些 I/O 端口正在使用中。

8. /proc/kcore

系统物理内存的镜像。其大小完全和你的物理内存一样，但事实上占不了多少内存；它是在程序访问它时，即时生成的（记住，除非你把它复制到别的地方，否则，/proc 根本就不占用任何磁盘空间）。

9. /proc/loadavg

系统的“负载均衡”；无意义的三个识别符，表示此时系统应该做多少操作。

10. /proc/meminfo

包含和内存使用相关的信息，其中既包括物理内存，又有交换空间。

11. /proc/modules

表明此时正在装载哪些内核模块。

12. /proc/net

目录，其中包含和网络协议相关的状态信息。

13. /proc/self

指向一个程序进程目录的符号链接，这个程序此刻正在查看 /proc。如果有两个程序都在查看 /proc，它们就会得到两个不同的符号链接。这主要是为了方便程序更容易得到自己的进程目录。

14. /proc/stat

关于系统的各种统计数据，比如自系统启动以来出现的页故障次数统计。

15. /proc/uptime

表明系统已启用多久。

16. /proc/version

内核版本号。

注意，上面的文件越来越发展成为易于理解的文本化文件，但有时，它们采用的格式却是难以理解的。所以，目前有许多命令将上面的文件转换为更便于理解的格式。比如，有个自由软件读取 /proc/meminfo，并将指定的字节转换为千字节（同时，还增加了少许信息）。