第 1 章

搭建服务器前的准备工作

很多朋友因为自身或所服务单位的需求，总会遇到搭建各种网络服务器的问题，这个时候大多数前辈都会推荐他们使用 Linux 作为搭建服务器的操作系统。然而，许多朋友并没有接受过 Linux 操作系统使用方面的训练，因此他们总觉得反正都是操作系统，Linux 应该跟 Windows 差不多，就硬着头皮使用图形界面来配置众多的服务器，也有可能参考网络上的一些文章，通过文字界面进行配置，也能够很轻松地做好服务器的搭建。问题是，这样的一台服务器其实是很容易被绑架的。而且，如果网络不通，你又该如何自行进行故障诊断（Trouble Shooting）呢？难道出问题只能无语问苍天吗？所以，除非你只是暂时需要搭建网络服务器，可以请朋友或其他信息公司帮忙，如果你本身就是信息方面的服务提供商，那么鸟哥建议在正式部署服务器之前，不妨阅读一下本篇的内容，看看你是否具备了配置网络服务器的基本技能。

1.1　Linux 的功能

很多刚接触 Linux 的朋友常常会问的一句话就是：“我学 Linux 就是为了搭建服务器，既然只是为了搭建服务器，为什么我还要学习 Linux 的其他功能？例如计划任务、Bash Shell，又为什么去认识所有的登录文件，等等，我又用不到啊！此外，既然有好用的 Web 接口的 Server 配置软件，可以简单地将网站搭建起来，为什么我还要去学习用 vim 手动编辑一些配置文件？为什么还需要去理解服务器的工作原理？”上面这些话对于刚刚学会搭建网站的人来说，确实道出了他们作为**一个新手的心声**。不过，对于任何一个曾经搭建网站并把网站发布到 Internet 上的朋友来说，上面这些话，**真的会害死人**！为什么呢？下面我们就来分析一下。

1.1.1　用 Linux 搭建服务器需要的能力

如果有人问你：**“Linux 最强大的功能是什么？”**大概大家都会回答：**“是网络功能”**，如果对方再问：**“学 Linux 就是为了搭建服务器吗？”**这个问题可就见仁见智了！说穿了，Linux 其实就是一套非常稳定的操作系统，任何工作只要能在 Linux 这个操作系统上运行，那它就是 Linux 可以实现的功能之一！所以 Linux 的作用远不止于提供网络服务器功能这么简单。

举例来说，在 Linux 上开发跨平台的数值计算模型（Model），例如大型的大气仿真计算模型，由于 Linux 的稳定性与完善的资源分配功能，使得在 Linux 上开发的程序在运行方面既快又稳定。此外，诸如 KDE、GNOME 等漂亮的图形界面，搭配 Open Office 等办公室软件，使 Linux 立刻摇身一变而成为优秀的桌面计算机（Desktop）。此外，Google 开发的专门用于手机系统的 Android 操作系统也是以 Linux 为基础的。所以说，千万不要小看了 Linux 在功能多样性方面的表现。

不过，无论怎么说，Linux 的强大网络功能确实是使得它在服务器领域内占有一席之地的重要因素。既然如此，我们就来探索一下 Linux 的网络世界吧。首先，Linux 到底可以实现哪些网络功能呢？这可就多了！不论是 WWW、Mail、FTP、DNS，还是 DHCP、NAT 与 Router 等，Linux 系统都可以实现，而且只需要一台 Linux 主机就能够实现上述所有功能。当然，在不考虑网络安全与效率的情况下，你可以使用一台 Linux 主机来实现所有的网络功能。

但是，对于一个服务器而言，**“搭建容易，维护难”**！更深一层来说，**维护还好，而故障诊断与排除更难！**搭建一个服务器难吗？即使你完全没有摸过 Linux，只要参考鸟哥的书籍或者是网站，而且一步一步照着做，保准你一个下午就可以搭建完成 5 个以上的网络服务器。所以说，搭建服务器没什么难的。但是，这样的一个网络服务器，多则三天，少则数小时，很快就会入侵了！此外，被入侵之后，或许可以利用一些工具来帮你将 root 的密码救回来，可惜的是，这样的一个服务器还是有可能作为一个中继站被入侵而危害网络中其他主机的安全。

另外，如果你使用工具（例如 Webmin）却怎么也搭建不起来某个网络服务，要怎么解决？如果你不懂该**服务器（Server）的工作原理与 Linux 系统的故障诊断信息**，那么难道只能无语问苍天吗？不要怀疑这种情况的可能性，只需参考一下各大论坛上面的留言，你就会明显地看到这种情况越来越普遍。

所以说，在搭建服务器之前还需要学会一些基本的技能！而且一旦**学会了这些技能，我们可以终身受用！**只要花一个学期（3~6 个月）的时间就能学会一辈子可以使用的技能，真的非常值得。

举例来说，鸟哥在 2003—2005 年期间去当兵了，当兵期间很少接触 Linux。等到退伍后，带的第一个学习班就是帮助班里的同学通过 Linux 国际认证，那时我几乎对 Linux 的所有命令都感到很陌生。不过，懂得学习方法的鸟哥，通过 man、百度以及以前学习累积的一些知识和概念，几乎都可以在一分钟内解决所遇到的问题，班里的同学也不会有突然不知鸟哥所云的困扰。

Linux 不是很好学。根据鸟哥过去教学的经验，很多同学在学习 Linux 时真的感到非常痛苦，不过学完之后，以前在 Windows 中遇到的困难却会迎刃而解！因为学习 Linux 时，要求我们解决每一个发现的问题，这个过程会让我们学到很多基础知识，所以学完之后，你会觉得很多事情都变得很简单了。但如果使用 Windows 的懒人方案，很多问题就不可能了解为什么会发生以及为什么可以这样处理。在下一节中，我们将分析搭建服务器的流程，并提供相对应的应该掌握的 Linux 技能。

1.1.2 搭建服务器难不难

无论是 Windows 还是 Linux，要搭建一台堪称完美的服务器，基本功课还是需要做的，这包括：

- 了解网络的基本概念，以方便进行联网与配置及故障诊断与排除。
- 熟悉操作系统的基本操作，包括登录控制、账号管理、文本编辑器的使用等技巧。
- 信息安全方面，包括防火墙与软件更新方面的相关知识等。
- 该服务器协议所需软件的基本安装、配置、故障诊断与排除等。

掌握这些基本功课后，才能进行实际部署，而且，每个项目中都有许多需要学习的技巧。不要以为信息管理人员整天闲着没事干，大家可是天天在应用技术，同时还得天天应付随时可能会发生的各种漏洞与网络攻击方法！想干好这份工作，真的会非常辛苦。

这样看来，搭建服务器真的是挺难的。事实上，搭建服务器其实又是挺简单的。为什么这样说呢？其实“搭建服务器很难”是由于我们学习的角度有偏差。还记得当初进入理工学院的时候，天天在念的东西是基础物理、基础化学、工程数学与流体力学等基础课程，这些课程花了我们 1~2 学期的时间，而且内容还很难，都是一大堆的理论。我们进理工学院是为

了学习更高深的知识，那么这些基础知识学了有什么用呢？当然有用，因为更高深的知识都是建构在这些基本课程的理论之上的，如果**基础课程没有学好，那么专业课程中提到的基本理论就不可能听懂**。

这样说应该就比较容易理解了，认识操作系统与该操作系统的基本操作，还有网络基础知识，就是我们在搭建服务器前的“基础课程”。所以说，在进入 Linux 的服务器世界之前，不能够略过网络基础的相关知识，同时，也必须掌握使用 Linux 系统的基本技能。

或许，你对于 Linux 系统中的“**重要知识**”还不太了解，果真如此的话，那么我们就举个简单的例子来说明。下一节将列出一般的搭建服务器流程，让我们在这个流程中看看哪些是重要的 Linux 相关技能。

在这一章中，鸟哥不再就 Linux 基础命令进行解析，因为在《鸟哥的 Linux 私房菜 基础学习篇（第四版）》一书中已经详细介绍过了！所以下一节仅对 Linux 基础学习的重要性进行分析。

1.2　搭建服务器的基本流程

虽然不同的服务器提供的服务并不相同，而且每种服务的原理也不见得都一样，不过，每种服务器由规划、搭建到后续的安全维护，其实整个流程是大同小异的。下面我们将逐项进行分析。

1.2.1　网络服务器成功连接的分析

下面我们针对整个服务器的简易搭建流程来做一个分析，以明确**为什么了解操作系统的基础对于服务器的维护是相当重要的**。首先，让我们来看看是如何连接到服务器的？ 连接到服务器要获取什么资源？我们先通过图 1–1 进行简单说明。

先来理解一下，到底我们连接到服务器想要得到什么？举例来说，当你连接到抖音想要观看视频时，抖音的服务器会将视频数据流传输给你；当你连接到新浪网站想要看新闻时，新浪的服务器会将新闻的文本文件通过网页的方式提供给你；当你连接到无名小站想要浏览图片时，对方的服务器会将图片文件发送给你；当你连接到游戏网站想要去偷菜时，游戏网站的服务器会参考你之前留下来的记录，从数据库中将你的记录检索出来传送给你。可以看到，**当你连接到服务器时，重点是获取服务器上的数据，而这些数据通常以文件的形式存在！**那么，你有没有权限获取这些文件或者文件中的数据呢？最终取决于对应网站服务器中文件系统的设置。

图 1–1 显示的是客户端到服务器的网络连接必须连通。一旦客户端成功访问服务器，服务器的防火墙会先判断该连接请求能否放行，等到连接请求被放行之后，才能使用服务器上

软件的功能。然而，该功能又需要通过 SELinux 这个细粒度存取权限配置，才能够读取文件系统。但能不能读到具体文件呢？又取决于文件系统的权限设置（r、w、x）。上述的每个部分都要满足系统的要求，否则将无法顺利读取数据。

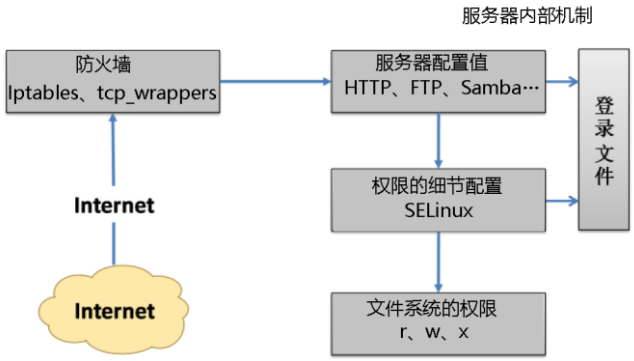

图 1-1　通过网络连接至服务器所需经过的各项环节

所以，根据上面的流程，我们可以将整个连接分为几个关键部分，包括网络连接、服务器本身、内部防火墙软件的设置、各项服务的配置文件、细粒度存取权限的 SELinux 配置以及最重要的文件权限。接下来，我们将分别讨论每个部分的相关内容。

1. 网络：了解网络基础知识与所需服务的通信协议

既然要搭建服务器，首先需要了解一下因特网。因为无论使用哪种操作系统，要与因特网连接，首先要求掌握网络基础知识。举例来说，“子网”是一个经常被提及的概念，当你遇到一个配置为 192.168.1.0/255.255.255.0 的设置项时，知道这是什么吗？ 如果不知道的话，那么你绝对无法正确配置网络服务，另外，为何你需要服务器？当然是为了实现某种网络服务。举例来说，传输文件可以用 FTP，那 WWW 可以传输文件吗？“网上邻居”功能可以传输文件吗？每个网络服务的用途是什么？哪个网络服务在传输文件方面更方便？ 对于客户或公司领导来说，我们所搭建的服务能否满足他们的需求等，这些都需要了解，否则你将会一头雾水！因此，在这部分你需要了解的内容如下：

- 网络基础知识，包括以太网络硬件与协议、TCP/IP、网络连接所需参数等。
- 各网络服务所对应的通信协议的工作原理，以及实现各通信协议的具体应用程序。

2. 服务器本身：了解搭建网络服务器的目的以配合主机的安装规划

想要搭建服务器吗？那么，你要搭建什么样的服务器？这个服务器要不要对 Internet 开放？这个服务是否需要为客户提供访问账号？是否需要针对不同的访问账号进行限制，例如磁盘容量、可用空间与可用系统资源等方面的限制？如果需要进行各项资源的限制，那么服务器操作系统应该要如何安装与设置呢？问题很多吧？所以，只有在明确了解你所需搭建的服务器的各项预期功能之后，后续的规划才能陆续出炉。不过，如果你配置服务器只是为了“练功”，那就不需要考虑太多了。

3. 服务器本身：了解操作系统的基本操作

网络服务软件是需要在操作系统上运行的，所以需要掌握操作系统基本的管理与操作技术！这包括如何安装和删除软件、如何管理系统的计划任务、如何根据服务器的服务目的规划文件系统、如何使文件系统具有可扩展性（LVM 之类）、系统如何管理各项服务的启动、系统的开机流程是什么，以及系统出错时如何进行快速恢复等。这些都是需要了解的内容。

4. 内部防火墙设置：管理系统的可共享资源

一台主机可以允许多种服务器软件同时运行在其中，而许多 Linux 发行版的默认设置已经开放了很多服务供 Internet 使用，不过这些服务可能并不是你想要开放的。在了解网络基础知识和所需服务的预期目的之后，接下来通过防火墙来限制可以使用本服务器服务的用户，以确保系统在使用上拥有较佳的可控环境。此外，**无论你的防火墙系统设置得多么严格，只要是你要开放的服务，防火墙对该服务就没有保护作用**。因此，在线更新软件机制一定要定期进行，否则你的系统将非常容易受到安全威胁。

5. 服务器软件设置：学习设置技巧以及设置开机是否自动执行

在第一点中已经提到，我们需要知道每种服务所能实现的功能，这样才能够搭建你所需要的服务站点。那么你所需要的服务是由哪个软件来实现的呢？同一个服务可否由不同的软件实现？每种软件可以实现的目的是否相同？根据所需的功能，如何设置你的服务器软件？在搭建过程中，如果出现错误，你应该如何观察与进行故障诊断与排除？可否定期地分析服务器相关的登录信息，以便了解服务器的使用情况与错误发生的原因？能否通知多个用户进行连接测试，以获取较佳的服务器配置值？因此，在这里你可能需要知道以下内容：

- 软件如何安装，如何查询相关配置文件所在的位置？
- 服务器软件如何设置？
- 服务器软件如何启动，如何设置自动开机启动，如何观察启动的端口？
- 服务器软件激活失败如何进行故障诊断与排除，如何查看日志，如何通过日志进行故障诊断与排除？
- 通过客户端进行连接测试，如果失败该如何处理？连接失败的原因是服务器还是防火墙？
- 服务器的设置修改是否有相关的日志，相关日志是否要定期分析？
- 服务器所提供或共享的数据有无定期备份，如何定期自动备份或远程备份？

6. 细粒度存取权限设置：包括 SELinux 与文件权限

等到你的服务器全部设置妥当，而你将文件数据的存取权限设置为 000，那么鸟哥可以确定地告诉你，其他人将无法读到你所提供的数据！此外，新的 Linux 发行版都建议启动 SELinux。那么 SELinux 是什么呢？如果你的数据存放在非正规的目录中，应该如何处理 SELinux 的问题？又如何让文件具有保密性或共享性（如文件权限概念与 ACL）？我们要厘

清所有这些相关概念。

在上述的服务器搭建流程中，除第 5 点外，其他步骤在各种服务器的设置过程中都是需要了解的，而且内容都是相似的。因此，如果掌握了这些基础知识，最终只需要了解第 5 点中具体软件的基本设置，你就能够快速完成服务器的设置。所以说，基础学习非常重要。

1.2.2 一个常见的服务器设置案例分析

上述内容讲完后，或许你还不太清楚这些技能如何串联起来？在这里，鸟哥提供一个简单的案例来进行分析，这样更容易理解为何需要学习这些内容。

- **网络环境**：假设你的环境中有 5 台计算机（无论是在家里还是在宿舍里），这 5 台计算机需要通过网络连接在一起，并且都可以对外提供访问服务。
- **对外网络**：你的环境只有一个对外的连接，假设是 ADSL 或更快的的光纤，即通过电话线或者光纤连接。
- **额外服务**：你希望这 5 台计算机都能上网，而且其中有一台主机还可以作为文件服务器，用于同学或家人的数据备份与共享。
- **服务器管理**：由于可能需要进行远程管理，因此你的服务器需要开放连接机制，以让远程计算机可以连接到该主机进行维护。
- **防火墙管理**：出于对文件共享服务器系统被攻击的担忧，你需要根据源 IP 进行登录控制。
- **账号管理**：由于同学们的数据有隐秘与共享之分，因此你还需要为每个同学提供专门的访问账号，并对每个账号设置磁盘容量使用限制。
- **后台分析**：出于对系统问题的担心，你需要让系统定期自动分析磁盘使用量、日志文件参数等信息。

在上述环境中，你需要考虑哪些事项呢？根据本节一开始提到的 6 个步骤来分析的话，你可能需要掌握下面的内容。

1. 了解网络基础

1）硬件规划

我们想要将 5 台计算机连接在一起，但只有一个可以对外提供连接。在这种情况下，就需要购买集线器（Hub）或者交换机（Switch）来连接所有的计算机。但是这两者有何不同？为何交换机比较贵？另外，我们所用的网线有不同等级，如何区分这些等级？不同等级的网线的速度有没有差异？只有在了解了这些硬件基础知识之后，你才能根据环境进行连接的设计。这部分内容将在下一章介绍。

2）连接规划

由于只有一条对外连接的线路，因此通常建议你用如图 1–2 所示的方式来连接网络。

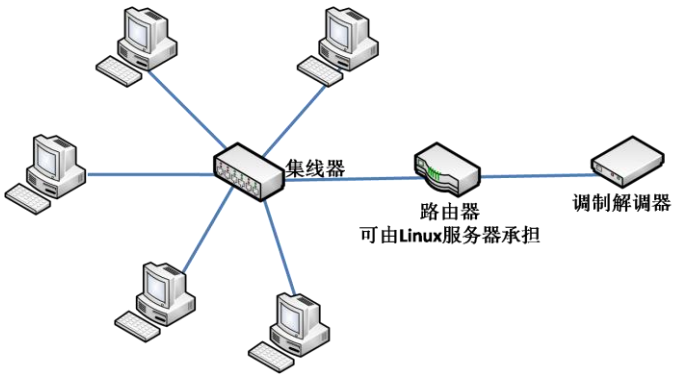

图 1-2　硬件的网络连接示意图

通过路由器，我们的 5 台计算机就可以连接到 Internet 了。需要注意的是，能否上网与 Internet 有关，其核心是著名的 TCP/IP 通信协议。要了解网络，就需要知道什么是 OSI 七层协议。我们知道能否连上 Internet 与 IP 有关，那么我们内部这 5 台计算机所获得的 IP 能否用来作为服务器的 IP 地址呢？也就是说，IP 地址有没有不同种类？如果路由器突然宕机了，那么这 5 台计算机能否继续互连进行网络游戏？这涉及网络参数配置问题。

2. 网络基础

如果你的同学或家人跑来告诉你：网络不通了！你的第一反应会是什么？是硬件问题，软件问题，还是某未知的或一些莫名其妙的问题？如果你不了解网络基础的 IP 相关参数，包括路由设置和域名系统（Domain Name System，DNS），那么肯定不知道如何进行连接测试。因此，你可能会被指责：“你什么都不懂还想管理我们家的网络……”那时候是不是很糗呢？所以要将一些基础知识学好。这部分内容就比较复杂了，包括 TCP/IP、网络 IP、子网掩码（Netmask IP）、广播 IP、网关、DNS IP 等。

了解了这些原理之后，你才能够进行故障诊断和排除的工作。最常见的错误之一，例如，你的主机明明可以使用 ping 命令连接到远程主机（ping IP），但无法使用 ping hostname 连接到远程主机。那么，这个问题的原因是什么呢？对于了解网络基础知识的人来说，他们会知道这很可能是 DNS 出了问题。一旦知道问题出在哪里，就能够有针对性地解决该问题。

是否掌握网络基础知识对于进行正确的网络设置至关重要。因为即使你成功搭建了服务器，如果你的网络不通，别人也无法访问你的服务器。所以，如果要搭建服务器，就必须努力学好网络基础知识。关于网络基础知识的内容，我们将在第 2 章中进行详细说明。

3. 服务器本身的安装规划与服务器目的的搭配

如图 1–2 所示，服务器端位于那 5 台计算机之中，而且服务器必须要针对不同的账号分配磁盘空间。在这里，我们会提供共享（SAMBA）这个服务，因为它可以在 Linux/Windows 之间通用。由于需要为用户提供账号，并考虑到未来的磁盘扩展情况，因此我们希望将 /home

独立出来，并使用逻辑卷管理（Logical Volume Manager，LVM）模式，同时搭配 Quota 机制来控制每个账号的磁盘使用情况。

所以说，你需要了解 Linux 目录结构下的文件系统层次结构标准（Filesystem Hierarchy Standard，FHS）规范，否则错误的目录与磁盘分区配置可能导致无法启动系统！那么为什么要将 /home 单独放在一个分区中呢？这是因为 Quota 仅支持文件系统（Filesystem），而不支持单个目录！好了，如果给你一台全新的主机，该如何安装你自己的系统呢？

例题

全新安装：请到 CentOS 官方网站下载最新的 Linux 镜像文件，并根据自己的需求安装好 Linux 系统（其中最重要的是磁盘分区问题，其他工作可以在安装完成后进行）。

答：由于本书系列中的《鸟哥的 Linux 私房菜 基础学习篇（第四版）》一书中的第 4 章已经介绍了 Linux 的安装过程，这里不再使用图形界面进行说明，只使用文字说明来介绍在每个项目中应完成的操作。此外，根据之前版本的读者反馈，学习者通常只有一台主机，因此我们建议使用 VirtualBox 虚拟机系统来模拟出一台实体主机，以便安装和测试环境。请注意，这台主机将在本书的各个章节中使用。

VirtualBox 的安装和配置请参考其官网上的文档（Documentation）介绍，这里不再赘述。但需要注意的是，（1）如果需要搭建服务器进行上网，建议使用桥接模式（Bridge）进行网络设置，网卡类型选择 Intel 的桌面计算机类型即可；（2）由于我们将引入 NAT 服务器，因此最好有两张网卡，一张使用桥接模式，另一张使用内网（Internet）较为合适；（3）对于磁盘配置，建议使用 SATA 类型，并选择容量在 25GB 以上；（4）内存建议至少 512MB，最好有 1GB 来进行测试。其他的可以参考官网文档，或者使用默认配置。当然，如果你有独立的实体机器来进行安装，那就更好了，就不需要考虑上述说明了。

默认配置如下：

- 分区表请按如下方式进行：
  - /：2GB。
  - /boot：200MB。
  - /usr：4GB。
  - /var：2GB。
  - /tmp：1GB。
  - swap：1GB。
  - /home：5GB，并且使用 LVM 模式进行构建。
  - 其他容量请保留，以后再进行额外练习。
- 挑选软件时，选择 basic server 项目即可。
- 信息安全部分，防火墙选择“启动”，SELinux 选择“强制（Enforce）”。

- 假设路由器有自动分配 IP 地址的功能，则网络参数先选择 DHCP 即可，以后再根据需要进行修改。

实际流程大致如下：

（1）由于我们使用 U 盘启动来安装系统，因此要先进入计算机的 BIOS 界面，选择从 U 盘启动，并且将制作好的 CentOS 安装 U 盘插入计算机的 USB 口（最好是计算机后面的 USB 口，有些计算机的前置 USB 口不支持 U 盘启动）。重新启动系统。

（2）在启动安装的界面中，选择 Install or upgrade an existing system 选项来安装新系统。

（3）出现 Disc Found 字样，可以选择 Skip 跳过。

（4）在“欢迎”界面单击 Next 按钮。

（5）语系选项可以选择“Chinese（简体）（中文（简体））”。

（6）键盘格式保留“美式英文”。

（7）安装使用的设备类型，直接选择默认的“基本存储设备”即可。

（8）因为是全新的硬盘，因此会出现一个找不到分区表的错误，此时选择“重新初始化”。

（9）进入网络主机名的设置，先保留 localhost.localdomain，同界面中还有一个“配置网络”的选项，我们先不要动它，等以后涉及网络设置时再来处理。

（10）进入时区选择，选择“亚洲/上海”。

（11）出现 root 密码设置，这里我们先设置为 centos；这个密码太简单，系统会出现警告，选择“无论如何都使用”即可，另外，也可以将密码设置为复杂密码。

（12）出现哪种类型的安装，因为我们有自己的分区考虑，所以，请选择“创建自定义布局”来处理。

（13）在分区界面中，选择 sda 项目，然后单击“创建”按钮，在出现的窗口中，再选择“标准分区”选项，然后单击“生成”按钮。在最后的窗口中填写挂载点、容量等信息后，最后单击“确定”按钮即可。最终界面如图 1–3 所示。

（14）根据前面的分区规划，重复执行上述操作，将所有的分区都处理好，/home 除外。

（15）由于 /home 要使用 LVM 的方式来建立文件系统，因此单击“创建”按钮后，选择“LVM 物理卷”选项，再单击“生成”按钮，在出现的分区窗口中，容量填写“5000MB”，如图 1–4 所示。

接下来回到原来的分区界面，单击“创建”按钮并选择“**LVM 卷组**”选项，在出现的界面中，卷组名称填写 server，并且在右下方的逻辑卷部分单击“添加”按钮，又会额外出现一个窗口，此时填入 /home 的相关参数。注意，逻辑卷标名称设置为 myhome，如图 1–5 所示。

图 1-3 分区参数设置窗口

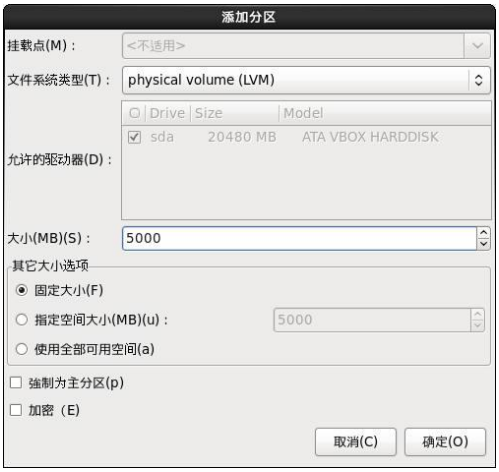

图 1-4 划分 LVM 分区

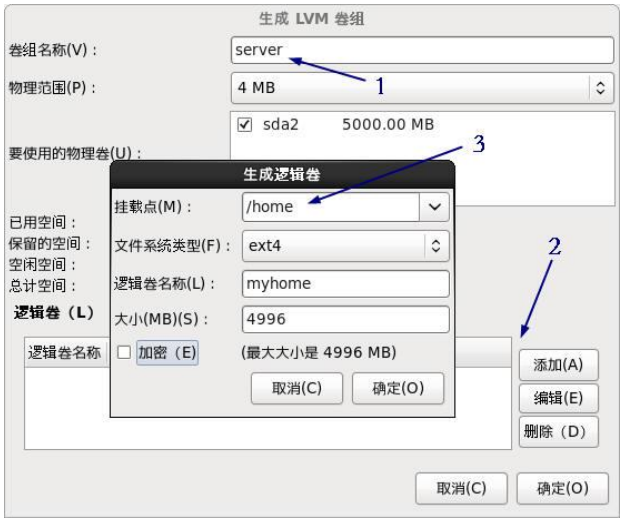

图 1-5 建立最终的 LVM 的逻辑卷与 /home

回到原来的分区界面，最终的显示如图 1–6 所示，然后单击“下一步”按钮。由于新建分区需要格式化，因此又会出现一个警告窗口，选择“**格式化**”以及“**将修改写入磁盘**”。

（16）出现装载引导程序的操作，都使用默认设置即可，单击“**下一步**”按钮。

（17）出现安装类型，因为我们主机的角色为服务器，因此选择 Basic Server 选项。其他各项保留默认设置，然后单击“下一步”按钮开始执行安装程序。

（18）经过一段时间的等待，出现重新启动提示后，就可以重新启动系统了，启动前要记得将 U 盘拔出来。鸟哥在第一次安装时，竟然发现电源管理有问题，要在 kernel 处增加 noapic 才能顺利启动系统。

图 1-6　分区的最终结果

（19）安装好系统并重新启动，就会进入 runlevel 3 的纯文本界面。

4. 服务器操作系统的基本使用

既然我们的主机需要为不同的账号提供独立的网络驱动器，因此还需要创建账号、配置磁盘配额（Quota）等。那么你会不会创建账号？是否知道如何配置共享目录？能否处理每个账号的磁盘配额？如果 /home 的容量不足，你是否知道如何扩充 /home 的容量？是否知道如何定期将系统的磁盘使用情况通过邮件发送给管理员？这些都是基本的维护操作。接下来，我们将通过几个实际的例子来练习一下，看看你的基本能力。

例题

批量创建账号：假设我有 5 个朋友的账号分别是 vbirduser{1,2,3,4,5}。这 5 个朋友未来想要共享一个目录，因此应该加入同一个用户组，假设这个用户组为 vbirdgroup，并且这 5 个账号的密码均为 password。那么如何创建这 5 个账号？

答：你可以编写一个脚本程序来完成上述任务。

```
[root@localhost ~]# mkdir bin
[root@localhost ~]# cd /root/bin
[root@localhost bin]# vim useradd.sh
#!/bin/bash
groupadd vbirdgroup
for username in vbirduser1 vbirduser2 vbirduser3 vbirduser4 vbirduser5
do
        useradd -G vbirdgroup $username
        echo "password" | passwd --stdin $username
done
[root@localhost bin]# sh useradd.sh
```

```
[root@localhost bin]# id vbirduser1
uid=501(vbirduser1)gid=502(vbirduser1)groups=502(vbirduser1),501(vbirdgroup)
context=root:system_r:unconfined_t:SystemLow-SystemHigh
```

最后使用 id 命令来查询组的支持是否正确。

例题

共享目录的权限：这 5 个朋友的共享目录位于 /home/vbirdgroup 目录，这个目录只能供这 5 个人使用，且每个人都可以在该目录内进行任何操作，而其他人则无权使用（没有权限）该目录，那么如何设置这个目录的权限呢？

答：考虑到共享目录的特性，目录需要具有 SGID 权限，否则个别组的数据可能会导致这 5 个人无法修改别人的数据。因此，需要执行以下操作：

```
[root@localhost ~]# mkdir /home/vbirdgroup
[root@localhost ~]# chgrp vbirdgroup /home/vbirdgroup
[root@localhost ~]# chmod 2770 /home/vbirdgroup
[root@localhost ~]# ll -d /home/vbirdgroup
drwxrws---. 2 root vbirdgroup 4096 2011-07-14 14:49 /home/vbirdgroup/
# 上面加粗体字的部分就是需要注意的部分！特别要注意权限中的 s 功能
```

例题

配额操作：假设这 5 个用户都需要进行磁盘配额限制（存储容量的限制），每个用户的配额为 2GB（hard）和 1.8GB（soft），该如何处理？

答：该操作实现起来比较复杂，因为它涉及文件系统的支持、Quota 数据文件的设置、Quota 的启动、建立用户 Quota 信息等步骤。整个过程在《鸟哥的 Linux 私房菜 基础学习篇（第四版）》一书已经讲过了，这里快速地带领大家操作一次。

```
# 1. 启动 filesystem 的 Quota 支持
[root@localhost ~]# vim /etc/fstab
UUID=01acf085-69e5-4474-bbc6-dc366646b5c8 /      ext4  defaults  1 1
UUID=eb5986d8-2179-4952-bffd-eba31fb063ed /boot  ext4  defaults  1 2
/dev/mapper/server-myhome /home     ext4  defaults,usrquota,grpquota  1 2
UUID=605e815f-2740-4c0e-9ad9-14e069417226 /tmp   ext4  defaults  1 2
...(以下省略)...
# 因为是要处理用户的磁盘，所以采用的是/home 这个目录来进行限额
# 另外，CentOS 6.x 以后，默认使用 UUID 的磁盘代号而非使用文件名
# 不过，你还是能使用类似/dev/sda1 的文件名
[root@localhost ~]# umount /home; mount -a
[root@localhost ~]# mount | grep home
/dev/mapper/server-myhome on /home type ext4 (rw,usrquota,grpquota)
# 完成后使用 mount 检查一下 /home 所在的文件系统有没有上述的挂载属性
```

```
# 2. 制作配额（Quota）文件，并启动文件系统的配合支持
[root@localhost ~]# quotacheck -avug
quotacheck: Scanning /dev/mapper/server-myhome [/home] done
...(以下省略)...
# 会出现一些错误的警告信息，但那是正常的！出现上述的提示信息就对了
[root@localhost ~]# quotaon -avug
/dev/mapper/server-myhome [/home]: group quotas turned on
/dev/mapper/server-myhome [/home]: user quotas turned on

# 3. 为用户定义配额（Quota）
[root@localhost ~]# edquota -u vbirduser1
Disk quotas for user vbirduser1 (uid 500):

  Filesystem                   blocks   soft     hard    inodes  soft  hard
  /dev/mapper/server-myhome      20   1800000  2000000      5     0     0
# 因为配额使用的单位是 KB，所以这里要补上好多 0，看得眼都花了

[root@localhost ~]# edquota -p vbirduser1 vbirduser2
# 持续操作几次，将 vbirduser{3,4,5} 全部添加上去

[root@localhost ~]# repquota -au
*** Report for user quotas on device /dev/mapper/server-myhome
Block grace time: 7days; Inode grace time: 7days
                        Block limits                File limits
User            used    soft    hard  grace    used  soft  hard  grace
----------------------------------------------------------------------
root       --      24       0       0              3     0     0
vbirduser1 --      20 1800000 2000000              5     0     0
vbirduser2 --      20 1800000 2000000              5     0     0
vbirduser3 --      20 1800000 2000000              5     0     0
vbirduser4 --      20 1800000 2000000              5     0     0
vbirduser5 --      20 1800000 2000000              5     0     0
# 看到了吗？上述的结果就是发现了设置好的配额值！整个流程就是这样的
```

例题

文件系统的扩充（LVM）：假设我们的 /home 容量不够用了，想要将 /home 扩充到 7GB 是否可行？

答：因为我们当初就担心这个问题，所以 /home 目录定义为使用 LVM 的方式进行管理。此时我们要来瞧瞧检查卷组（Volume Group，VG）的容量是否够。如果够用，就可以继续进行；如果不够用，就需要从物理卷（Physical Volume，PV）着手了！整个流程可以按照下面的步骤来进行。

```
# 1. 先看看 VG 的容量够不够用
[root@localhost ~]# vgdisplay
  --- Volume group ---
  VG Name               server
```

```
  System ID
  Format                lvm2
...(中间省略)...
  VG Size               4.88 GiB  <==只有区区 5GB 左右
  PE Size               4.00 MiB
  Total PE              1249
  Alloc PE / Size       1249 / 4.88 GiB
  Free  PE / Size       0 / 0     <==完全没有剩余的容量了
  VG UUID               SvAEou-2quf-Z1Tr-Wsdz-2UY8-Cmfm-Ni0Oaf
# 真惨！已经没有多余的 VG 容量可以使用了，因此，我们需要增加 PV 才行

# 2. 开始制作出 PV 用的分区
[root@localhost ~]# fdisk /dev/sda  <==详细流程我不写了，自己瞧吧

Command (m for help): p
   Device Boot      Start    End      Blocks   Id  System
...(中间省略)...
/dev/sda8            1812   1939     1024000   83  Linux <==最后一个柱面

Command (m for help): n
First cylinder (1173-3264, default 1173): 1940  <==上面查到的柱面值加 1
Last cylinder, +cylinders or +size{K,M,G} (1940-3264, default 3264): +2G

Command (m for help): t
Partition number (1-9): 9
Hex code (type L to list codes): 8e

Command (m for help): p
   Device Boot  Start    End   Blocks  Id  System
/dev/sda9        1940   2201  2104515  8e  Linux LVM <==得到 /dev/sda9

Command (m for help): w

[root@localhost ~]# partprobe <==在虚拟机上面需要重新引导（reboot）才行

# 3. 将 /dev/sda9 加入 PV，并将该 PV 加入服务器这个 VG
[root@localhost ~]# pvcreate /dev/sda9
[root@localhost ~]# vgextend server /dev/sda9
[root@localhost ~]# vgdisplay
...(前面省略)...
  VG Size               6.88 GiB       <==这个 VG 最大就是 6.88GB
...(中间省略)...
  Free  PE / Size       513 / 2.00 GiB <==多出 2GB 的容量可用了

# 4. 准备扩充 /home，开始前，还是先观察一下，再增加 LV 容量较好
[root@localhost ~]# lvdisplay
  --- Logical volume ---
  LV Name                /dev/server/myhome <==这是 LV 的名字
  VG Name                server
...(中间省略)...
  LV Size                4.88 GiB  <==只有 5GB 左右，需要增加 2GB
...(下面省略)...
# 看起来，是需要增加容量了！我们使用 lvresize 来扩大容量吧

[root@localhost ~]# lvresize -L 6.88G /dev/server/myhome
```

```
  Rounding up size to full physical extent 6.88 GiB

  Extending logical volume myhome to 6.88 GiB  <==处理完毕了。
  Logical volume myhome successfully resized
# 看来确实是扩大到 6.88GB 了，开始处理文件系统吧

# 5. 扩充文件系统
[root@localhost ~]# resize2fs /dev/server/myhome
resize2fs 1.41.12 (17-May-2010)
Filesystem at /dev/server/myhome is mounted on /home; on-line resizing required
old desc blocks = 1, new desc blocks = 1
Performing an on-line resize of /dev/server/myhome to 1804288 (4k) blocks.
The filesystem on /dev/server/myhome is now 1804288 blocks long.

[root@localhost ~]# df -h
文件系统              Size  Used Avail Use% 挂载点
/dev/mapper/server-myhome
                      6.8G  140M  6.4G   3% /home
...(其他省略)...
# 可以看到文件系统确实扩充到 6.8GB 了
```

执行完上面的操作之后，现在你知道为什么在《鸟哥的 Linux 私房菜 基础学习篇（第四版）》一书中，鸟哥一直强调一些有用的内容，因为那些内容在这里都用得上！如果本章这些内容你都不会，甚至连为什么要这么操作都不明白的话，建议你赶紧回去阅读《鸟哥的 Linux 私房菜 基础学习篇（第四版）》一书。

5. 服务器内部的资源管理与防火墙规划

你可知道本章的第一个例子安装好了 Linux 之后，系统到底开放了多少服务？这些服务有没有对外面的世界开放监听？这些服务有没有漏洞或者能不能进行网络在线更新？这些服务如果没有用到，能不能关闭？此外，这些服务能不能仅开放给部分的原用户而不是对整个 Internet 开放？这都是需要了解的。接下来我们就以几个小案例来了解一下，到底哪些数据是必须要熟悉的。

例题

不同运行级别（Runlevel）下服务的管理：在当前的运行级别之下，有哪些服务是默认启动的呢？此外，如果我的系统当前不想启动自动网络挂载（Autofs）机制，则如何让该服务在系统启动时不被自动加载启动呢？

答：默认的运行级别可以使用 runlevel 这个命令来设置，如果默认使用运行级别 3，那么可以执行如下的命令：

```
[root@localhost ~]# LANG=C chkconfig --list | grep '3:on'
```

在上面命令的输出信息中，有 autofs 服务处于启动状态，如果想要关闭它，可以执行如

下命令：

```
[root@localhost ~]# chkconfig autofs off
[root@localhost ~]# /etc/init.d/autofs stop
```

上面提到的只是已经启动的服务，如果想要了解已启动的网络监听服务，那该如何处理？可以参考下面的练习题。

例题

查询已启动的网络监听服务：想要检查当前这台主机启动的所有网络监听服务有哪些，并且关闭不需要的网络监听程序，该如何进行？

答：网络监听服务及其所使用的端口情况，可以使用如下方式查询到：

```
[root@localhost ~]# netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address   Foreign Address   State  PID/Program name
tcp        0      0 0.0.0.0:111     0.0.0.0:*     LISTEN 1005/rpcbind
tcp        0      0 0.0.0.0:22      0.0.0.0:*     LISTEN 1224/sshd
tcp        0      0 127.0.0.1:25    0.0.0.0:*     LISTEN 1300/master
tcp        0      0 0.0.0.0:35363   0.0.0.0:*     LISTEN 1023/rpc.statd
tcp        0      0 :::111          :::*          LISTEN 1005/rpcbind
tcp        0      0 :::22           :::*          LISTEN 1224/sshd
tcp        0      0 ::1:25          :::*          LISTEN 1300/master
tcp        0      0 :::36985        :::*          LISTEN 1023/rpc.statd
udp        0      0 0.0.0.0:5353    0.0.0.0:*     1108/avahi-daemon:
udp        0      0 0.0.0.0:58474   0.0.0.0:*     1108/avahi-daemon:
...(以下省略)...
```

现在假设想要关闭 avahi-daemon 这个服务以删除该服务所使用的端口，该操作应该如同上题一样，利用 /etc/init.d/xxx stop 关闭，再使用 chkconfig 来处理开机不启动的服务。不过，因为启动的服务名称与实际命令可能不一样，我们在 netstat 命令执行结果中看到的 program 项目是实际程序的执行文件，可能与 /etc/init.d/ 下面的服务脚本文件名不同，因此可能需要使用 grep 命令来摘取数据，或者通过 Tab 按键来取得相关的服务文件名。

```
[root@localhost ~]# /etc/init.d/avahi-daemon stop
[root@localhost ~]# chkconfig avahi-daemon off
```

我们常常会开玩笑说，如果对外开放的软件没有更新，那么防火墙形同虚设。所以，软件更新是相当重要的。在 CentOS 内，我们已经有 yum 来进行在线更新了，你当然可以自己利用更改配置文件来指定 yum 要查询的镜像站点（Mirror Site），不过这里鸟哥建议

使用默认的设定值即可，因为系统会主动判断较近的镜像站点（虽然常常会误判），不需要人工微调。

例题

利用 yum 进行系统更新：假设你的网络已经通了，目前想要进行整个系统的更新，同时希望每天凌晨 2:15 自动进行整个系统的更新，该怎样做？

答：整个系统更新使用 yum update 即可。但是由于 yum update 需要用户手动输入 y 来确认所要进行的安装，因此在 crontab 中定义相关的任务时，就需要使用 yum –y update 了。

```
[root@localhost ~]# yum -y update
# 第一次进行该操作会有较长的等待时间！因为系统有些数据要更新

[root@localhost ~]# vim /etc/crontab
15 2 * * * root /usr/bin/yum -y update
```

不过这里还是要额外提醒一下，如果你的系统曾经更新过内核（Kernel），务必重新启动，因为内核是在开机时加载的，一经载入就无法在这次的操作中更改版本。

对于 crontab 文件的处理，以及 crontab –e 命令的应用、内容的写法、字段值的定义，请读者自行参考《鸟哥的 Linux 私房菜 基础学习篇（第四版）》一书的说明。

在完成上述各项设置后，我们的 Linux 系统应该变得相对稳定了。接下来，开始配置资源的保护。例如，ssh 这个远程登录服务需要限制可登录的源 IP，以及制定防火墙规则等。这部分内容将在本书的后续章节中详细介绍。

程序设计师所编写的程序并非十全十美，总是可能有些地方没有设计好，这就导致了所谓的“程序漏洞”。程序漏洞带来的问题有大有小，小问题可能导致主机宕机，大问题则可能导致主机的敏感数据泄露，或者主机的控制权被黑客窃取。在当前网络发达的时代，程序漏洞已成为主机遭受攻击和入侵的主要因素之一。因此，快速、有效地修补程序漏洞是一项非常重要的维护任务。

6. 服务器软件设置：学习设置技巧以及如何配置开机自动执行

这部分内容是本书的重要内容。前面我们已经提到，你需要熟悉这部分内容，否则未来的维护工作可能会变得很棘手。以本章提到的大前提为例，如果想要搭建一个网络文件服务器，那么网络文件服务器使用的机制有哪些呢？除常见的基于网页形式的共享磁盘外，还有一些其他常见的方式，比如网上邻居以及 Linux 的 NFS 方式（后续章节将逐一介绍）。注意：在较新的 Windows 版本中，“网上邻居”功能已由文件资源管理器中的“网络”取代。

假设局域网内的大部分操作系统是 Windows，使用网上邻居实现磁盘共享机制应该是比较合理的。那么，网上邻居究竟启用了几个端口？它是如何持续提供网上邻居数据的？访问的账号有没有限制？访问的权限该如何设置？是否可以指定谁可以登录某些特定目录？针对网上邻居服务的端口该如何设置防火墙？如果系统出错，该如何查询错误信息？这个网上邻居在 Linux 下，我们该使用什么服务来实现类似的功能？这些都是需要学习的内容。

事实上，网上邻居的实现在 Linux 环境中是由 Samba 这套软件来完成的。关于 Samba 的详细设置，我们会在后续章节介绍。在这里，我想告诉你的是，要搭建一个网上邻居服务器，你需要掌握哪些基础知识。此外，你可以把搭建流程中理论上要经过的步骤与过程背下来，这对你未来处理服务器的设置时可能会有所帮助。

1）**软件安装与查询**

从前面的内容可知，网上邻居需要安装的是 Samba 这个软件。那么，该如何查询是否安装了 Samba？如果没有安装，又该如何安装呢？可参照下面的步骤。

例题

查询你的系统中有没有 Samba 这个软件，若无，请安装该软件。

答：若已安装，可以使用 rpm 查询。若未安装，则可以使用 yum 来安装，具体操作如下：

```
[root@localhost ~]# rpm -qa | grep -i samba
samba-common-3.5.4-68.el6_0.2.x86_64
samba-client-3.5.4-68.el6_0.2.x86_64
samba-winbind-clients-3.5.4-68.el6_0.2.x86_64
# 看起来 Samba 主程序尚未被安装，此时就要这样操作

[root@localhost ~]# yum search samba  <==先查一下有没有相关的软件
[root@localhost ~]# yum install samba <==找到之后，那就安装吧

# 那么如何找出配置文件呢？因为我们经常需要修改配置文件，可以这样做
[root@localhost ~]# rpm -qc samba samba-common
/etc/logrotate.d/samba
/etc/pam.d/samba
/etc/samba/smbusers
/etc/samba/lmhosts
/etc/samba/smb.conf
/etc/sysconfig/samba
```

2）**服务器的基本配置与相关配置**

这部分有点麻烦，因为你要清楚地知道你所需的服务是什么，以及针对该服务需要设置的项目有哪些，这些设置需要用到什么命令或配置文件等。一般来说，你需要先查看这个服务使用的通信协议是什么，然后了解该如何设置，接下来编辑主配置文件，并根据主配置文

件的数据执行相对应的命令来取得正确的环境设置。以这里的网上邻居为例，我们需要设置工作组，并将网上邻居的身份设置为非匿名。然后，我们可以开始处理主配置文件。因此，你需要：

（1）先使用 vim 编辑 /etc/samba/smb.conf 配置文件。

（2）利用 useradd 建立所需要的网上邻居实体用户。

（3）利用 smbpasswd 建立可用网上邻居的实体账户。

（4）利用 testparm 测试一下所有数据语法是否正确。

（5）检查在网上邻居内共享的目录权限是否正确。

这些设置都完成之后，才能够继续进行启动与观察的操作！若想要了解更多关于 Samba 的相关配置技巧和应用，除使用搜索引擎外，还可查阅位于 /usr/share/doc 目录下的文件，以及 man 页的文档。man 页是一个非常实用的工具，也值得一读。

3）**服务器的启动与观察**

在设置妥当之后，接下来当然就是启动该服务器了。一般服务器的启动大多采用 stand alone 模式，如果是不经常使用的服务，例如 Telnet，可能会使用到 super daemon 的服务启动类型。在这里我们仍以 Samba 为例，来看看如何启动它。

例题

如何启动 Samba 这个服务，并且设置好开机就启动它？

答：想要了解如何启动，需要使用 rpm 去找一下软件的启动方式，然后再去处理启动的操作。

```
# 先查询一下启动的方式是什么
[root@localhost ~]# rpm -ql samba | grep '/etc'
/etc/logrotate.d/samba
/etc/openldap/schema
/etc/openldap/schema/samba.schema
/etc/pam.d/samba
/etc/rc.d/init.d/nmb
/etc/rc.d/init.d/smb  <==所以说是 stand alone 且文件名为 smb、nmb 两个
/etc/samba/smbusers

# 开始启动它，且设置为开机就启动
[root@localhost ~]# /etc/init.d/smb start
[root@localhost ~]# /etc/init.d/nmb start
[root@localhost ~]# chkconfig smb on
[root@localhost ~]# chkconfig nmb on
# 接下来，让我们观察一下有没有启动相关的端口
[root@localhost ~]# netstat -tlunp | grep '[sn]mbd'
tcp    0    0 :::139                  :::*         LISTEN   1484/smbd
tcp    0    0 :::445                  :::*         LISTEN   1484/smbd
```

```
udp    0    0 0.0.0.0:137          0.0.0.0:*              1492/nmbd
udp    0    0 0.0.0.0:138          0.0.0.0:*              1492/nmbd
```

最终我们可以看到启动的端口为 137、138、139、445。

4）**客户端的连接测试**

接下来需要找一台机器作为客户端，然后尝试使用该机器提供的网上邻居功能，这样才能够判断配置是否正确。客户端的连接方式与服务器提供的服务有关。例如，如果是 WWW 服务器，需要使用浏览器进行测试；而对于网上邻居功能，则需要使用相应的网上邻居客户端程序。这也是本书将要介绍的基本内容之一。

但是很多时刻，客户端连接测试不成功并不是服务器配置的问题，很多情况下是由于客户端的使用方式不正确，例如客户端的防火墙未开启、客户端的账号权限或密码错误等。总体来说：**“教育你的客户端用户掌握基础的 Linux 账号、组和文件权限等概念，才是一个彻底解决问题的方法”**，但这也是最难的部分。

5）**错误的解决与查看日志文件**

一般来说，如果 Linux 中的服务出现问题，通常会在屏幕上面直接提示错误的原因，所以你要注意屏幕信息。屏幕信息通常包含该如何处理的信息。如果还不能处理，可以参考下面的方法来发现错误的原因：

- 先看看相关日志文件有没有错误信息，举例来说，Samba 除会在 /var/log/messages 中列出相关信息外，大部分的日志信息应该存放在 /var/log/samba/ 这个目录下，因此我们需要先查阅这些文件。通常情况下，在日志文件中的信息比在屏幕上显示的信息还要详细。
- 如果查阅日志后仍无法解决问题，可以将相关信息输入搜索引擎。通常情况下，能够解决日志中出现的问题，成功率在 95% 以上。
- 如果仍然没有成功解决问题，可以到各大讨论区去发问，建议到 Linux 中国区提问（https://linux.cn/tech/）。
- 最常出现的问题实际上是 SELinux 错误。此时就需要使用 SELinux 的方法来尝试处理，这也是本书后续章节会提到的内容。

经过上面的流程可知，搭建好一台主机需要知道：①**各个进程（Process）与信号（Signal）的概念**；②**账号与组的概念与相关性**；③**文件与目录的权限，其中包含与账号相关的特性**；④**软件管理的学习**；⑤**Bash 语法与 Shell 脚本语法以及重要的 vim 编辑器**；⑥**启动流程分析以及日志文件的设置与分析**；⑦**还需要了解类似 Quota 和文件系统连接等的概念**。需要了解的内容很多，而且这些步骤是不能省略的。

7. 详细权限与 SELinux

在特殊的使用情况下，权限配置就成为一个很重要的因素。举例来说，在我们的系统中，现在有 vbirduser{1,2,3,4,5} 以及 student 等账号，而共享目录为 /home/vbirdgroup。现在，vbirdgroup 组希望让 student 这个用户可以进入该共享目录查阅内容，但不能修改他们原本的数据。在这种情况下，你可以考虑以下解决办法：

- 让 student 加入 vbirdgroup 群组。但如此一来，student 将具有 vbirdgroup 的读、写和执行（r、w、x）权限，也就可以写入与修改，因此这个方案行不通。
- 将 /home/vbirdgroup 的权限改为 2775。如此一来，student 将拥有其他用户的读和执行（r、x）权限，但其他所有任何人均拥有 r、x 权限，因此这个方案也行不通。

传统的身份与权限概念确实只有上面两种解决方案，无法针对 student 进行特定的权限设置。在这种情况下，我们需要使用访问控制列表（Access Control List，ACL）。

例题

对于单个用户或组的权限设置，我们可以使用 ACL。如果想要让 student 能够进入 /home/vbirdgroup 进行查询，但不可写入，同时 vbirduser5 在 /home/vbirdgroup 内不具有任何权限，要怎么办？

答：只能使用 ACL。由于安装时默认启用了支持 ACL 的文件系统功能，因此可以直接执行以下各项指令。如果你使用的是后来新添加的分区或文件系统，或许需要在/etc/fstab 内额外添加 ACL 控制参数。

```
[root@localhost ~]# useradd student
[root@localhost ~]# passwd student
[root@localhost ~]# setfacl -m u:student:rx /home/vbirdgroup
[root@localhost ~]# setfacl -m u:vbirduser5:- /home/vbirdgroup
[root@localhost ~]# getfacl /home/vbirdgroup
# file: home/vbirdgroup
# owner: root
# group: vbirdgroup
# flags: -s-
user::rwx

user:vbirduser5:---
user:student:r-x      <==就是这两行，额外的权限参数
group::rwx
mask::rwx
other::---

[root@localhost ~]# ll -d /home/vbirdgroup

drwxrws---+ 2 root vbirdgroup 4096 2011-07-14 14:49 /home/vbirdgroup
```

上面说的是正确的权限控制操作。然而，如果系统管理员并不了解权限的重要性，常常会因为某些特殊需求而将整个目录设定为 777 的情况！举例来说，如果是一位不太负责的网络管理人员为了方便自己和其他人，将 /home/vbirdgroup 设置为 777，认为这样大家都会喜欢。此时，如果没有加上任何管理机制，这个组成员工作的成果就很容易被其他人窃取，这真的非常危险。

为了预防这种心不在焉的管理员，于是就有了 SELinux。SELinux 的主要作用是控制特殊权限，它可以为某些程序要读取的文件设计 SELinux 类别或标签，只有当程序与文件的标签相匹配时，文件才能被读取。如此一来，当我们将文件的权限设置为 777，由于程序和文件的 SELinux 标签不匹配，因此该程序仍然无法读取该文件。这就是我们将 SELinux 的图示绘制到守护程序（Daemon）与文件权限（File Permission）之间的原因。

事实上，SELinux 确实相当复杂，但是如果我们只是想要应用它，那么处理 SELinux 问题完全可以通过日志来解决！因此，SELinux 出现问题的概率非常大，但解决方法却很简单，只需根据日志中的说明进行操作即可。关于具体的操作方法，我们将在后续章节中进行详细讲解。

1.2.3 系统安全与备份处理

老实说，根据鸟哥在服务器管理方面的经验，硬件问题往往比操作系统和软件问题更为严重，而人为问题又比硬件问题更为严重。举例来说，如果你的老板跟你说：“我想要一个账号，名为 eric，密码也要是 eric ！这样比较好记嘛！”那么你应该如何处理呢？你需要说服老板不要这样设置。

因此，在系统安全方面，首要的工作是通过日常生活的社交活动逐渐揭示一些安全方面的困扰，并向老板提供一些制订安全规则的信息，以便未来更容易推动安全条件的制定。建议采取严格的密码策略。

“猜密码”仍是一个不可忽视的入侵手段。例如，如果将 SSH 对 Internet 开放，我们又没有禁用 root 登录权限，那么攻击者可能会尝试使用 root 账户登录你的 Linux 主机，此时他们最重要的一步就是猜出 root 密码。如果你将 root 密码设置成 1234567 这样简单的密码，想不被入侵都很难！因此，当然需要采用严格的用户密码策略。那么如何制定严格的密码规则呢？可以采取以下措施：①修改 /etc/login.defs 文件中的规则，要求用户每半年更改一次密码，且密码长度需要大于 8 个字符；②利用 /etc/security/limits.conf 来规范每个用户的权限，以增加 Linux 的安全性；③利用 PAM 模块进行额外的密码验证工作。

另外，虽然“防火墙无用论”常常被提及，但实际上 netfilter（Linux 的核心内置防火墙）仍然具有存在的必要性。因此，你仍然需要根据自己的主机环境来设计专属于自己的防火墙规则。例如，在上面提到的 SSH 服务中，你可以只针对某个局域网络或某个特定的 IP 开放连接功能。

最后，备份是不可忽略的一环。正如本节开头讲到的，鸟哥经历过系统常常莫名其妙地

自动重启或不稳定的情况，这通常不是因为遭受到了攻击，而是由于硬件内部电子元件老化导致的系统不稳定。在这种情况下，冗余备份和备用机器的接管等就显得非常重要。

例题

系统中一些重要的目录有 /etc、/home、/root、/var/spool/mail 等。如果我们想要在每天 2:45am 进行备份，并将备份数据存储到 /backup 目录中，同时使用 tar 命令将备份数据打包，那么该如何处理呢？

答：鸟哥通常使用 Shell 脚本进行数据备份的汇总，范例如下：

```
[root@localhost ~]# mkdir /root/bin; vim /root/bin/backup.sh
#!/bin/bash
backdir="/etc /home /root /var/spool/mail"
basedir=/backup
[ ! -d "$basedir" ] && mkdir $basedir
backfile=$basedir/backup.tar.gz
tar -zcvf $backfile $backdir

[root@localhost ~]# vim /etc/crontab
45 2 * * * root sh /root/bin/backup.sh
```

无论如何，从现今的网络功能和维护角度来看，**搭建一个“功能强大”的主机并不如搭建一个“稳定且安全”的主机好！**因此，对于主机的安全要求需要严格。根据鸟哥的观点，如果你的主机是用来赚钱的，例如某些研究单位的大型集群计算主机，即使架设一个可能让你觉得很不方便的防火墙系统也是合理的手段。因为主机被入侵固然不好，倘若数据被窃取，那可不是闹着玩的。

从上面整个服务搭建流程来看，由规划到安装、主机设置、账号与文件权限的管理、后续安全性维护与管理，以及重要的备份工作，等等，每个环节都必须清楚明了，才能够配置出一个稳定且正常工作的服务器。而每个环节都涉及相当多的 Linux 基础操作与相关的概念。因此，**想要学服务器配置，绝对不能省略 Linux 基础知识的学习，这也是为什么我们一再强调 Linux 新手不要一头扎入单纯搭建服务器的迷思之中！**如果你对上面谈到的几个基础概念不太清楚，那么建议你从一些 Linux 学习网站开始学习。

1.3　自我评估是否已经具备服务器搭建的能力

网络管理人员需要什么样的能力？我认为，搭建几个服务器与成为一名称职的网络管理人员之间相差很大。搭建服务器只是一件很简单的事情，按照书本上的步骤进行操作，一定能够成功。但是，很多人只知道“**如何搭建服务器**”，却不知道“**如何维护一个站点的安全**”。事实上，维护一个已经搭建好的站点正常运行要比搭建站点难多了。你需要随时了解系统的状态，及时修补可能存在的软件漏洞，关注各种服务的日志文件（Logfile）以了解系统的运

行情况。当出现问题时，知道问题发生在哪里。比如，如果系统宕机了，那么你知道宕机的原因吗？即使不知道，也要能大致猜测出问题所在。如果系统安全出了问题，被人侵了，除重新格式化（Format）和重装系统外，你能够在不删除系统的情况下修补漏洞吗？这些都是网络管理人员需要学习的内容。而且，通常需要积累经验才能知道问题所在。此外，还要保持身心的活力，随时关注在线公布的安全防护信息等。

网络管理人员最需要的是“**道德感与责任感**”。要知道，机器上所有人的隐私都在你的监控之下，如果你本身有偷窥欲望，那就非常可怕了。此外，作为网络管理人员，还要有耐心，否则可能会疯掉，因为不论何时何地，只要你所监控的主机出了问题，你都会成为被怀疑的第一个人。所以，你必须随时随地准备好被召唤回到主机面前。更可笑的是，如果你服务的人群中有几个连启动系统都弄错了，还会跟你抱怨说“**嘿！你经手的计算机怎么这么烂，动不动就不能启动**”，此时，你需要有容人的雅量，说点冷笑话来缓解尴尬。总之，网络管理人员并不是只要会搭建服务器，还需要有道德感、责任感和耐心，这些都是必不可少的。

好了，如果你了解了鸟哥上述想要表达的想法，接下来请认真评估一下，看看你是否适合成为一名称职的网络管理人员！

1. 是否具有 Linux 的基础概念

这应当包含很多部分，例如账号管理、BASH、权限的概念、进程与信号的概念、简易的硬件与 Linux 相关性（如 mount）的认识、日志文件的解析、对守护进程（Daemon）的认识等。所有这些都需要有一定程度的了解。

2. 是否具备基础网络知识

如果没有网络知识，想要管理服务器，那简直是天方夜谭。请确认你已经熟悉 IP、子网掩码（Netmask）、路由（Route）、DNS、守护进程与端口（Port）、TCP 数据包的概念等基础知识。

3. 是否能全身心投入

网络管理人员必须时刻关注网站的相关信息，包括网站软件的漏洞修补、网络上公告的网络安全通报等。此外，还需要每天分析主机的登录文件。你是否已经具备了随时关注这些信息的“耐心”呢？

4. 是否具有道德感与责任感

如果你还有一点点偷窥欲望，努力克服吧。另外，如果老板想要请你“偷窥”时，请尽一切努力让他明白这么做是多么的可笑。

最后，再强调一次，搭建一个 Linux 服务器是很简单的，但维护的工作除全身心投入外，还需要具备高标准的道德感，否则网站倒塌是可以预见的后果。