

首个经过教学检验的IT
培训和考试准备工具

UPDATED FOR
RED HAT
ENTERPRISE
LINUX 6

RHCSA/RHCE Red Hat Linux认证学习指南(第6版): EX200 & EX300

RHCSA/RHCETM[®]



EX200 & EX300

100%覆盖——300多道考试真题

- 经过检验的基于实验的考试准备
- 4套考试真题——两套RHCSA真题 +
两套RHCE真题
- 覆盖所有RHCSA和RHCE考试目标



[美] Michael Jang 著
吴文国
李增民
曲伟 译

清华大学出版社

RHCSA/RHCE Red Hat Linux 认证学习指南(第6版): EX200 & EX300

[美] Michael Jang 著

吴文国
李增民 译
曲 伟

清华大学出版社

北京

Michael Jang

RHCSA/RHCE Red Hat Linux Certification Study Guide(Exams EX200 & EX300), Sixth Edition

ISBN: 978-0-07-176565-7

Copyright © 2011 by The McGraw-Hill Companies, Inc.

All Rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including without limitation photocopying, recording, taping, or any database, information or retrieval system, without the prior written permission of the publisher.

This authorized Chinese translation edition is jointly published by McGraw-Hill Education (Asia) and Tsinghua University Press Limited. This edition is authorized for sale in the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan.

Copyright (c) 2013 by The McGraw-Hill Asia Holdings(Singapore)PTE.LTD and aTsinghua University Press Limited.

版权所有。未经出版人事先书面许可，对本出版物的任何部分不得以任何方式或途径复制或传播，包括但不限于复印、录制、录音，或通过任何数据库、信息或可检索的系统。

本授权中文简体字翻译版由麦格劳-希尔(亚洲)教育出版公司和清华大学出版社有限公司合作出版。此版本经授权仅限在中华人民共和国境内(不包括香港特别行政区、澳门特别行政区和台湾)销售。

版权© 2012 由麦格劳-希尔(亚洲)教育出版公司与清华大学出版社有限公司所有。

北京市版权局著作权合同登记号 图字：01-2012-4745

本书封面贴有 McGraw-Hill 公司防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

图书在版编目(CIP)数据

RHCSA/RHCE Red Hat Linux 认证学习指南(第 6 版): EX200 & EX300 / (美) 江(Jang, M.) 著;
吴文国, 李增民, 曲伟 译. —北京: 清华大学出版社, 2013.5

书名原文: RHCSA/RHCE Red Hat Linux Certification Study Guide(Exams EX200 & EX300), Sixth Edition
ISBN 978-7-302-31712-8

I . ①R… II. ①江… ②吴… ③李… ④曲… III. ①Linux 操作系统—程序设计—工程技术人员—资格考试—自学参考资料 IV. ①TP316.89

中国版本图书馆 CIP 数据核字(2013)第 048711 号

责任编辑: 王军于平

装帧设计: 牛艳敏

责任校对: 邱晓玉

责任印制:

出版发行: 清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址: 北京清华大学学研大厦 A 座 邮 编: 100084

社 总 机: 010-62770175 邮 购: 010-62786544

投稿与读者服务: 010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:

装 订 者:

经 销: 全国新华书店

开 本: 185mm×260mm 印 张: 45.25 字 数: 1158 千字

版 次: 2013 年 5 月第 1 版 印 次: 2013 年 5 月第 1 次印刷

印 数: 1~3000

定 价: 98.00 元

产品编号:

译 者 简 介

吴文国，任教于温州大学计算机科学与工程学院，副教授，中国矿业大学(北京)在读博士，从事计算机教学工作 20 多年。翻译了《交互式计算机图形——基于 OpenGL 的自顶向下的方法》(第 3 版、第 4 版)、《Unix 原理与应用》、《XML 入门》、《精通 Windows Server 2008 网络技术》等书。研究方向是计算机图形学和地球物理及探测技术。

林川，副教授，毕业于北京邮电大学，现任职于温州大学物理与电子信息工程。主要的科研方向是 Web 服务和网络应用。

作 者 简 介

Michael Jang(已通过 RHCE、LPIC-2、UCP、LCP、Linux+、MCP 等认证)目前是一位操作系统和网络领域的全职作家。他在计算机方面的经历最早可以追溯到穿孔机时代。他已出版了多本与 Linux 认证有关的图书，包括 *LPIC-1 in Depth*、*Mike Meyers' Linux + Certification Passport*、*Sair GUN/Linux Installation and Configuration Exam Cram*。他所编写的其他与 Linux 有关的图书还包括 *Linux Annoyances for Geeks*、*Linux Patch Management* 和 *Mastering Fedora Core Linux 5*。他曾编写过或合作编写过有关 Microsoft 操作系统的图书，包括 *MCSE Guide to Microsoft Windows 98* 和 *Mastering Windows XP Professional, Second Edition*。

技术编辑简介

Elizabeth Zinkann 是 Linux 领域的权威、特约技术编辑和独立的计算机咨询师。她是 *Sys Admin* 杂志的特约编辑和专栏评论作家，而且在这个职位上工作了 10 年之久。在她的编辑生涯里，一些重要的项目包括 *Mastering Fedora Core Linux 5*、*LPIC-1 in Depth*、*Linux Patch Management* 和 *Linux All-in-One Desk Reference for Dummies, Fourth Edition*。以前的职业生涯中，她曾从事过通信程序功能的设计，包括 AT &T Network Systems 的 ISDN。

致 谢

我想要特别感谢以下人员：

感谢 Nancy E. Cropley。Nancy 去世已将近 10 年了，但是你一直活在我的心里，我希望你通过我的眼睛仍然能看到这个世界的欢乐。即使在今天，你仍然是一位英雄，我希望你能看到我与 Donna 是多么幸福，我将永远记住你！

作为一位政治活动家，你为自己的信仰而战：社会公正、世界和平和人类的健康。为了支持自己的信仰，你不害怕坐牢。正是你的缘故，我找到了生活的支柱。

作为无家可归人士的庇护者，你曾帮助许多没有你幸运的同胞，你不知疲倦地穿梭在病房、庇护所、大街上。你的努力减轻了许多人的痛苦，挽救了许多生命。

作为 Internet 创业者，你向我展示了在家工作的快乐人生。正是由于你，我可以享受自由的人生，而不用在公司里受煎熬。

Nancy，你是我的搭档和知己。你帮助我在这个世界上找到欢乐。我从你那儿获益良多。感谢你为我所做的一切。

- 感谢我的妻子 Donna。你的希望和爱使我的生活有价值，你用自己的爱和支持让我的生活更加美好。
- 感谢 McGraw-Hill 出版公司所有勤奋工作的员工：Stephanie Evans、Tim Green、LeeAnn Pickrell、Robert Campbell、Susie Elkind 和 Rebecca Plunkett，没有你们的辛勤工作和团队精神，就不可能有这一系列优秀的计算机图书出版。

Michael Jang

序 言

Linux 正在茁壮成长! Red Hat 总是处于 Linux 革命的最前沿。这一切得益于 Red Hat 认证系统管理员考试(Red Hat Certified System Administrators, RHCSA)和 Red Hat 认证工程师考试(Red Hat Certified Engineers, RHCE)。

在当前经济复苏时期，商业、教育和政府等机构都怀有强烈的成本意识。他们都希望能够控制自己的操作系统。Linux——甚至 Red Hat 企业版的 Linux(Red Hat Enterprise Linux)——都可以帮助节省成本。Linux 的开源特性允许用户控制和定制自己的操作系统。虽然购买 Red Hat 企业版 Linux 只需要一次付费，但是其成本还应该包括以后的更新和支持费用。现在有了 KVM，它允许在单台物理计算机上安装多个虚拟的、相互独立的 RHEL 系统(及其他操作系统)。许多公司已经把众多的、塞满各种物理系统的房间转换为只包含有限几个系统的小机柜。在每个系统里都安装了许多虚拟机。作为 Red Hat 认证的系统管理员和工程师(RHCSA 和 RHCE)，我们也可以投身到这场变革中。

虽然 RHEL 的支持版本也需要成本，但是用户可以不需要为这个成本付费。正如后面将要指出的，可以使用学生订阅版或试用版，或者由相同源代码构建的、免费使用的 RHEL 重构版本。

实际经验

重构版本是由第三方根据相同的源代码生成得到的软件。另一方面，克隆版本(clone)是由不同源代码生成得到的软件。

安全是许多公司选择 Linux 的另一个理由。美国国家安全局已经开发出自己的 Linux 内核版本，它在名为安全增强型 Linux(Security-Enhanced Linux, SELinux)的系统里提供了基于环境的安全。RHEL 已经把 SELinux 当作分层安全策略的一个重要组成部分。

通过 RHCSA 和 RHCE 认证考试不容易。根据现有的数据，只有 50% 的考生第一次通过 RHCE 考试。但是读者不要被这个统计数字吓跑。虽然无法保证，但是本书可以帮助读者准备并通过 RHCSA 和 RHCE 认证考试。本书介绍的技术同样可以应用到读者日常的系统管理工作中。需要记住的是，本书无意取代后面将要介绍的 Red Hat 培训课程(Red Hat Prep Courses)。

为了准备 Red Hat 认证考试，需要准备一个至少由 3 台 Linux 计算机组成的网络。由于 RHCSA 考试的重点是虚拟机，因此建议读者把其中两台 Linux 计算机用作 KVM 系统。配置了网络服务后，可以通过另一台计算机检查操作结果。

如何获得 Red Hat 企业版 Linux 操作系统

Red Hat 考试测验考生对 Red Hat 企业版 Linux 操作系统的知识。但是现在有一个重要的变化，RHCSA 认证目标规定了几个与虚拟机有关的考试目标。默认的 RHEL 6 解决方案使用

基于内核的虚拟机(Kernel-based Virtual Machine, KVM)。Red Hat 只支持 64 位 CPU 物理计算机上的 KVM 虚拟主机。因此,为了掌握 RHCSA 认证中与 KVM 有关的内容,读者需要一个能够处理 RHEL 6 64 位版本的硬件系统(但是,实际上可能并不需要真正的 64 位系统;在 Scientific Linux 上 32 位的 KVM(基于相同的 Red Hat 源代码)也可以使用,后面将介绍 Scientific Linux)。

读者可能需要在此 64 位硬件系统上安装两个或两个以上的虚拟机。虚拟机在多 CPU 系统或者多核 CPU 系统上运行起来可能会更好。因此,为了避免因硬件缘故而影响读者的学习,建议读者的 64 位硬件系统至少要有 2GB 的 RAM, 4GB 的 RAM 也许会更好(我是在 8GB RAM 的 64 位硬件系统上编写本书的)。如果读者使用便携式计算机,则建议读者阅读 https://bugzilla.redhat.com/show_bug.cgi?id=667485 网页上的有关说明。如果这个网页上列出的 bug 在你阅读本书的时候还没有解决,则硬盘驱动器的默认寿命可能会与这个 bug 有关。在 Red Hat 培训课程指南里,也没有明确把 Red Hat 网络更新当作一个考试要求,因此使用试用订阅版或重构版就足够了。如果读者希望获得一个完整的订阅版(它可以帮助读者测试与 Red Hat 网络有关的功能),则它的价格取决于硬件技术和技术支持的级别。需要强调,Red Hat 只要求使用 Red Hat 源代码的任何发行版本,包括本节提到的重构版本(及其他版本)。

对于 Red Hat 企业版 Linux 6, Red Hat 修改为以下 3 个不同的版本:

- RHEL 服务器版本(Linux Server)提供了不同级别的技术支持,它又分为 3 个基本类型:
 - 普通的基于 AMD 和 Intel CPU 的 32 位和 64 位系统。其价格取决于 CPU 插槽数和支持虚拟访客的数量。
 - IBM POWER 系统(IBM POWER Systems), 其价格取决于 CPU 插槽数。
 - IBM z 系统(IBM System z)。
- RHEL 桌面(RHEL Desktop)系统,它为工作站提供了各个级别的技术支持。
- RHEL Add-ons 系统可用于高可用性、弹性存储和负载均衡及其他领域中。

本书是我在 RHEL 6 服务器上完成的。RHEL 6 工作站也有 RHCSA 和/或 RHCE 认证考试所需要的服务器程序包。虽然 RHEL 是根据开源许可协议发布的,但这只是指开源代码而已。访问这个二进制程序包需要购买一个订阅服务,这可能比较昂贵。

企业级操作系统的一个优点是它的稳定性。当一个企业把自己的操作系统升级到 RHEL 6 时,就是利用了这种稳定性,只需要一次性更新整个系统的配置。之后的安全升级和 bug 修正都可以自动完成。为此,Red Hat 采取各种措施,避免强制出现这样的情形:企业只是为了一个修改版本(如 RHEL 6.1)而更新自己的系统。如果一个企业对每个修改版本都要修订自己的配置文件,则 Red Hat 企业版操作系统的成本会大大增加。

出于同样的理由,修改版本也不会影响 Red Hat 考试目标。虽然 RHEL 6.1 改进了操作系统的性能,嵌入了 bug 修改程序,集成了安全的更新程序,但是并没有改变配置文件的任何默认参数(本书后面将要介绍)。

即使在未来的几个月里,Red Hat 不断地推出 RHEL 6.2、RHEL 6.3 等修改版本,但我可以预料,情况还是一样。否则,Red Hat 可能会失去它的客户,因为系统升级会给企业带来计划外的成本。我在近 10 年里一直监测 RHEL 版本,发现没有迹象表明认证目标因修改版本而发生变化。如果读者对此还有怀疑,则可以仔细分析 www.redhat.com/certification/rhcsa/objectives/ 和 www.redhat.com/certification/rhce/objectives/ 网页上的考试目标。

如果读者学习本书只是为了参加 Red Hat 认证考试，则 Linux 的产品网站上提供了试用版的订阅服务。例如在 www.redhat.com/rhel/server 网页里有一个“Free Evaluation Software”(免费评估软件)链接。但是，它要求用户必须使用 Red Hat 网络(Red Hat Network, RHN)账户。个人电子邮件地址(如某些搜索引擎里的那些电子邮件地址)不可用作 RHN 账户。虽然试用订阅版只支持 30 天的更新，但是利用重构发行版本的镜像储存库也可以测试更新内容。从这里还可以像付费 Red Hat 用户那样下载由相同源代码生成的操作系统。

如果读者是学生或教育机构的成员，也就是使用.edu 电子邮件地址的用户，则可以使用学术订阅版本。在编写本书的时候，RHEL Server 的学术订阅版本只需要 60 美元，这相对于最便宜的标准 REHL Server 订阅费用(349 美元)也是很大的优惠。

但是，即使读者没有.edu 或商业的电子邮件地址，也可以不用为准备 RHCE 认证考试支付完整版或试用版的费用。有几个项目专门重构(Rebuild)Red Hat 企业版 Linux。它们使用的源代码几乎全部是以 Linux 通用公共许可证(Linux General Public License, GPL)或其他相关开源许可证发布的 RHEL RPM 程序包。这给任何用户提供了从 Red Hat 发布的源代码重构 Red Hat 企业版 Linux 的权利。

Linux 的源代码是以 Source RPM 程序包格式发布的。这意味着，RPM 程序包可以用 `rmpbuild` 命令生成(这个命令将在第 12 章中介绍)。重构版本的所有开发人员都会修改源代码，删除其中的 Red Hat 商标。有些发行版本，如 Scientific Linux 6，免费供大众使用。另一些发行版本，如 Oracle Linux，需要先注册，并且必须遵从美国出口控制法律等规定。

读者可以选择并下载最符合自己需要的重构版本。我曾试用过好几个重构版本，包括 Scientific Linux 版本和社区企业版本(Community Enterprise Linux, CentOS)。在本书将要印刷时，Microsoft 宣布在自己的虚拟机软件里支持 CentOS。

RHEL 的重构版本可以免费使用；但是，读者必须有一个高速的 Internet 连接。虽然这些重构版本总是对 RHEL 源代码做微小的修改(主要是删除 Red Hat 商标，用自己的商标取而代之)，但是我并没有发现这些修改可能会影响读者学习 Red Hat 认证考试。

- **Scientific Linux** 以前曾称为费米 Linux(Fermi Linux)，它集中了费米国家加速器实验室、欧洲粒子物理研究所(CERN)的许多知识分子精英。万维网最重要的发明人之一，即 Tim Berners-Lee，就是欧洲粒子物理研究所的成员之一。
- **社区企业版 Linux** 由 www.centos.org 小组开发的社区企业操作系统(Community Enterprise Operating System, CentOS)重构版本，在我看来，它是一个比较可靠的版本。这个小组拥有重构版本里最庞大的社区。CentOS 开发人员提供的一些消息显示，CentOS-6 将在本书出版时发布。

对于以 Red Hat 企业版 Linux 6 为基础的 Red Hat 认证考试，建议读者不要使用 Fedora Linux。尽管 RHEL 6 基本上是建立在 Fedora 12、Fedora 13 甚至 Fedora 14 之上的，但是这 3 个发行版本在形式上的明显差别会引起考试内容的混乱。因此，强烈建议读者不要使用 Linux 的其他发行版本，因为 Red Hat 认证考试是以 Red Hat 企业版 Linux 为基础的。在许多情形下，即使在 Linux 发行版里只属于一个标准的修改，也可能会给 RHEL 6 带来麻烦。

给使用本书的培训老师及其他人的建议

我希望每位读者仔细阅读本节内容。本书的组织形式便于一次只参加一个考试的读者学习。

为了方便培训老师的使用而对本书组织形式所做的修改也许是本书最大的特点。RHCSA 和 RHCE 是两个不同的认证考试，本书的结构反映了这一点。如果读者只是想参加 RHCSA 认证考试，则只需要阅读第 1~9 章的内容。如果读者只想准备 RHCE 考试，则只需要阅读第 1 章和第 10~17 章的内容。这样安排也方便了使用本书的认证候选人，他们知道针对其中一个认证考试需要掌握哪些技能。

许多考生，也许是绝大多数考生，要在规定的时间内完成 RHCSA 和 RHCE 考试操作可能会有困难。节省考试时间的方法之一是把事情简单化。虽然认真阅读考试题目是非常有必要的，但是也不要做得太过头。例如，在 RHCSA 考试里不需要配置虚拟服务器。RHCE 考试的一个目标是这样要求的：“只需要能够配置完成基本操作的服务”。

每一章都至少提供 12 道自测题。虽然 Red Hat 考试没有选择题或填空题，但是这些题目可以测验读者对本章内容的掌握程度。这些自测题强调读者的实践操作经验，因为这就是 RHCSA 考试所要求的。

同理，对于 RHCE 考试，也要尽量把事情简单化，除非有特殊要求。例如，RHCE 考试没有要求在防火墙里添加受怀疑的 IP 地址列表。只要求配置一个防火墙，允许某个指定的服务通过。简单的防火墙很快就能配置完毕。许多安全专家认为，越是简单的防火墙就越可靠。

有几个服务既属于 RHCSA 考试目标，也在 RHCE 目标里提到，因此这几个服务需要在多个章节里进行论述。例如，第 1 章讨论 RHCSA 与 HTTP 和 FTP 有关的考试目标，同时在第 14 章和第 16 章中也分别讨论这两个服务的 RHCE 认证目标。

第 1 章专门为读者建立一个学习 RHCSA 和 RHCE 认证考试所需要的基本系统。本章也会比较详细地介绍有关这两个认证考试的经验。一方面，本章介绍 RHCSA 在配置 FTP 服务器和 HTTP 服务器方面的认证目标；另一方面，它也提供如何从作为安装服务器的 RHEL 6 DVD 配置文件的指令。利用第 7 章提供的操作指示，读者应该能够把这个安装服务器设置为基于 yum 的储存库。后者可用于 RHCE 考试的服务器服务。

如果读者正在准备 RHCE 认证考试，那么可能需要了解 RHCSA 某些方面的内容。事实上，RHCE 部分的内容假定读者已按照第 2 章的操作指示建立起基于 KVM 的虚拟机，按第 1 章中自测中实验题 2 的要求建立起网络上的网络储存库。

考试之前的准备

对于 Red Hat 考试，没有办法临时抱佛脚。但是正如运动员在比赛之前需要做热身活动一样，读者也可以在考试之前做“热身”活动。重温选定考试的每一个认证考试目标。复习每一章末尾的“故障情景与解决方案”表。思考哪些软件需要安装，哪些文件需要配置，哪些命令比较难记。

记住，Red Hat 的 RHCSA 和 RHCE 考试专门用来测试考生是否具有 Linux 系统管理员和工程师的能力。如果读者通过了其中一门考试，这并不是因为你死记硬背了一组答案，而是因

为你具有 Linux 系统管理员的一套技能，以及在压力下(不管是考试压力还是现实世界的压力)知道如何使用这些技能。

本书内容简介

本书的某些重要组成部分只出现在随附光盘上。从第 2 章(实验题 2)开始，实验题内容只能在光盘上找到，而且实验题的存储格式允许读者在测试系统上读取它们。实验题的答案仍然出现在每章的末尾。假设读者已把 CD 挂载到 Linux 系统的/media 目录上，则在光盘上的/media/Chapter2、/media/Chapter3 和/media/Chapter4 等目录中可以找到这些实验题。此光盘也包含了本书内容的电子版。它采用了 PDF 文件的格式，保存在与实验题相同的 Chapter 文件夹里。PDF 文件并没有包括实验题的电子版。

术语表(Glossary)只出现在光盘上。假设光盘挂载在同一个目录上，则在/media/Glossary 目录里可以找到术语表。有关光盘的更多信息，以及如何在 Linux 里安装 Adobe Reader，读者可以参考附录 E。

RHCSA 和 RHCE 是两个不同的认证考试。如果读者打算同时参加这两个考试，则本书可以帮助读者掌握这两个考试之间的差别。例如，在第 2 章里会看到，作为客户端的安全 shell (SSH) 是 RHCSA 的一个认证目标。另一方面，在第 11 章里我们会看到，作为服务端的安全 shell 属于 RHCE 考试的一个目标。

虽然本书的组织方便了有经验的 Linux 和 Unix 专业人士深入学习 RHCSA 和 RHCE 考试内容，但是本书无意取代 Red Hat 培训课程。需要指出的是，本书无法取代实际的操作实践。尽管如此，本书的每一章讨论考试的某个重要专题，既强调系统管理员使用和维护 RHEL 的“原因”，也强调管理和维护的过程。由于 RHCSA 和 RHCE 目标(www.redhat.com/certification/rhcsa/objectives 和 www.redhat.com/certification/rhce/objectives)随 RHEL 新版本的推出(甚至有时在两个版本之间)而变化，因此读者要想了解最新信息，可以访问前面提到的 URL。

Red Hat 认为，要通过他们的考试，必须具有实际的操作经验，这种说法很正确！但是，对于 RHCSA 和 RHCE 考试，他们确实把重点放在 Linux 系统管理员的一套技能上，这可以由相应的认证目标看出。本书的目的是帮助读者充分发挥自己已掌握的技能——更重要的是，帮助读者掌握某些不熟悉的技能。

本书包括有关 Red Hat 企业版 Linux 6(RHEL 6)的内容。RHEL 6 在某些方面与 RHEL 5 相比有明显的改进。两者之间的主要区别有：

- RHEL 6 更好地支持“大规模、集中式管理的企业部署方案”；
- RHEL 6 默认支持 KVM 虚拟机，并且重视系统的性能、可伸缩性和安全性；
- RHEL 6 改进了电源管理功能；
- RHEL 6 使用 ext4 文件系统，后者现在是默认文件系统，而且最多可以支持 16TB 的文件；
- 比较容易配置 SELinux。

还有更多的重要功能。本书也包括一些我认为与 RHCSA 和 RHCE 考试有关的内容，这些内容也出现在 Red Hat 公开的教程或考试培训课程里。

在考试期间，以超级系统管理员身份登录到系统是一个非常危险的做法，但它确实是管理

RHEL 的最快捷方法。命令提示和 PATH 环境变量假定用户使用系统管理员的账户。当登录到根账户时，则会看到如下所示的命令行提示：

```
[root@server1 root]#
```

由于这个提示的长度可能会导致本书里的代码换行或断行，因此本书把这个根账户的提示简化为

```
#
```

特别需要注意的是，哈希标记(#)在 Linux 脚本和程序里用作注释字符。例如，下面是来自 /etc/inittab 的一段脚本：

```
# Default runlevel. The runlevels used are:
```

当我们以普通用户登录到 Linux 系统时，就会看到稍微不同的提示。假设采用 michael 用户登录到系统，则通常情形下系统的提示如下所示：

```
[michael@server1 michael]$
```

同样，我把上面的提示简化为

```
$
```

在每一章里都有很多命令行和代码段。正文中的命令，如 ls -l，都用黑体表示。正文中的用户条目以及某些变量也用黑体表示。

书中有些命令会超出一行的长度，例如：

```
# virt-install -n outsider1.example.org -r 768 --disk
path=/var/lib/libvirt/images/outsider1.example.org.img -1
ftp://192.168.122.1/pub/inst -x "ks=ftp://192.168.122.1/pub/ks1.
cfg"
```

除非这个命令经过精心排列，否则换行符可能会出现在错误的位置，如出现在—disk 开关前面的两个短划线之间。解决这个问题的方法之一是使用反斜杠符号(\)，它转义表示其后的回车符(反斜杠也可以转义空格，因此可以方便地使用长文件名)。这样，虽然下面的内容看起来在 4 个不同的行里，但是根据反斜杠符号的作用，Linux 会把它当作一个命令来处理。

```
# virt-install -n outsider1.example.org -r 768 --disk \
path=/var/lib/libvirt/images/outsider1.example.org.img \
-1 ftp://192.168.122.1/pub/inst \
-x "ks=ftp://192.168.122.1/pub/ks1.cfg"
```

有时区别是很微妙的。有时需要实际输入一个命令，或者在命令行里响应一个请求。在这种情形中，会看到“type y”这样的指示。或者，有些菜单要求按下一个键。例如，为了进入到密码提示，需要按下 P 键。在这种情形中，当我们按下这个键时，屏幕上不会出现字母 p。此外，A 尽管外表看起来是大写，但实际上还是小写。相反，A 表示大写的 A。

令有些出版商感到麻烦的是双短划线。有些排版软件把双短划线改为破折号(em dash)。但

是这会带来问题。两短划线经常出现在 Linux 的许多命令里。例如，下面的命令列出所有已安装在本地系统上的程序包：

```
# rpm --query --all
```

当我在自己的 RHEL 6 系统上执行这个命令时，它列出了 1300 个程序包。

相反，下面的命令列出本地系统上所有程序包里的文件：

```
# rpm --query -all
```

当我在自己的 RHEL 6 系统里执行上述命令时，它列出 133 000 个文件。这个结果完全不同于前一个命令的结果。因此，读者必须注意书中的短划线。希望本书的出版商在排版本书时特别注意双短划线。

考试知识点检查表

在本引言的末尾是考试知识点检查表(Exam Readiness Checklist)。这些表是为了方便读者交叉参考官方的考试目标而设计的。同时，这些检查表也可以帮助读者评估自己在开始学习时的专业水平。这样有利于读者检查自己的学习进展，确保在某些不熟悉或比较难的方面花较多的时间。检查表列出官方的考试目标、本书介绍这些考试目标的学习专题以及相关内容所在的章和页码。

每章内容简介

为了编好本书，我专门建立了一套章节组成部分，目的是引起读者对书中重要内容的注意，强化重要的知识点，提供有用的考试提示。读者在每章里都会遇到以下符号：

- 每一章都以认证目标(Certification Objectives)开始——即读者为了通过认证考试而需要在本章掌握的技能。在“目标”标题下确定本章的主要目标。因此只要读者看到这个标题，就知道它是一个考试目标。
- 考试提示(Exam Watch)用于引起读者对考试有关的信息以及可能存在的陷阱的注意。这些有用的提示信息都是由参加考试并获得认证的作者提供的——还有谁比他们更适合告诉你们考试的注意事项？他们经历了读者将要经历的一切过程。
- 每章都有实践操作题(Practice Exercises)。这些逐个步骤的练习让读者获得考试所需的实际操作经验。它们也有助于读者掌握考试要点。不要只是看看这些题目而已，而是要动手完成这些操作题。实践是提高技能掌握水平最好的方法。记住，Red Hat 考试完全是实践型考试，这些考试没有多选题。
- 实际经验(On the Job)栏说明了在实际情形中经常遇到的问题。“实际经验”栏提供了与认证考试和实际产品有关的、十分有用的经验，它们指出了常见的错误和工作中经常讨论和经历的问题。

- 考试内幕(Inside the Exam)栏突出了在实际考试过程中经常遇到的和最容易混淆的问题。这个栏目是专为预测未来考试的重点内容而设计的，它帮助读者切实理解通过考试需要掌握的要点。如果读者多注意这些栏目里的内容，并且完成那些比较难理解的实验题，就会比其他考生更有优势。
- 故障情景与解决方案(Scenario & Solution)栏以便于阅读的表形式列出可能存在的问题及解决方案。
- 认证小结(Certification Summary)总结了本章的内容，复习本章中与考试有关的重要技能。
- 每章末尾的小练习(Two-minute Drill)是本章重要知识点的检查表。可以在考试前的最后时刻做这些练习。
- 自测题(Self test)帮助读者测评自己对与认证考试有关的实用知识的掌握程度。这些自测题的答案以及说明都在每章的末尾给出。在阅读每章之后做这些自测题可以巩固你在每章学到的知识。本书并不打算提供多选题，因为 Red Hat 考试并没有这样的题目。
- 自测题之后的实验题(Lab Question)提供了独一无二的和具有挑战性的操作练习。要回答这些题目，读者需要综合利用本章的知识。这些问题比较复杂，而且综合性较强，它们用来测试读者对本章全部内容的掌握程度以及把它们应用于复杂的真实情形的能力。从第 2 章的实验题 2 开始，所有实验题都只出现在本书的光盘上，采用与 Red Hat 考试相一致的电子格式。记住，Red Hat 考试只有实验题！如果读者能够完成这些实验题，则说明读者已经掌握相关主题。

附加资源

有些读者可能还想深入研究 Linux。深入研究 Linux 的最佳方法是阅读 Red Hat 的帮助文档。我有关 RHEL 6 的很多知识都来自于 http://docs.redhat.com/docs/en-US/Red_Hat_Enterprise_Linux/ 上的帮助文档。对于读者，以下也许是比較有用的指南：

- 安装指南 由于 Red Hat 考试使用预先配置好的系统，因此这个安装指南相对来说不是很重要，但是它包含了有关 Kickstart 的重要内容。
- 部署指南 部署指南也许是与如下内容有关的最重要的指南：Red Hat 给出的如何为完成基本操作配置服务的建议。
- 安全增强型 Linux 安全增强型 Linux 指南详细介绍了帮助进一步提高系统安全的各种选项。

几点建议

当读者读完本书之后，最好花点时间对本书内容做一个全面的总结。读者可能以后经常需要翻看本书，应用本书提供的很多方法：

- 重读书中的全部“考试提示” 记住由那些参加并通过考试的考生提供的注意事项。
他们知道你们所需要的知识——以及应该注意哪些问题。
- 复习所有的故障情景与解决方案 找到快速解决问题的方法。

-
- **重做自测题** 重点是操作题，因为 Red Hat 考试没有多选题(或填空题)。本书提供的自测题只是为了测验读者是否掌握了每一章的实践性知识。
 - **完成练习** 读者是否读完每章后就立刻做后面的练习呢？如果没有，则必须这样做。这些练习包括了考试的主要内容。掌握这些内容的最好方法莫过于实践操作。对于每个练习里的每一步操作，都要问为什么。如果发现自己对某个问题还没有弄清楚，则重读本章相应的内容。

前　　言

Red Hat 考试具有挑战性

前言论述获得一个行业公认的证书的理由，并说明 RHCSA 和 RHCE 认证的重要性，以及如何准备考试。此外，前言还介绍在考试当天的准备工作和相关事宜。

本书包括了在编写时所有公开的认证目标。有关最新的认证目标，可以参阅 www.redhat.com/certification/rhcsa/objectives/ 和 www.redhat.com/certification/rhce/objectives/ 这两个网站。Red Hat 也公开发布了考试培训课程(后面将要介绍)的教学大纲。虽然公开发布的考试目标都十分准确，但是培训课程的教学大纲会提供更详细、更有用的信息。Red Hat 的每个培训课程都在系统管理、网络管理、安全等技术方面提供了坚实的基础。为此，本书也提到 RH124、RH134 和 RH254 等 Red Hat 课程的大纲。这些课程后面还会谈到。

尽管如此，本书无意取代任何 Red Hat 培训课程。

在竞争中胜人一筹

Red Hat 的 RHCSA 和 RHCE 认证考试属于实践操作型考试。因此，它们被整个行业认为是具有真正实践操作能力的标志。如果读者通过这些考试，则会比那些只通过“标准”选择题型认证考试的考生更胜一筹。

从 1999 年开始，Red Hat 就已开始提供实践操作型考试，在过去几年里，这些考试不断得到完善。正如第 1 章将要详细介绍的，现在的 RHCSA 考试时间为 2.5 小时，RHCE 考试时间为 2 小时。考试内容及要求在本前言后面的考试知识点检查表里有详细介绍。虽然这些考试的合格分数目前并没有公开，但是针对 RHEL 5 的 Red Hat 考试，在某个时期的合格分数是 70 分，这里假设满分为 100 分。公开发布的第三方报告认为，这个合格分数并没有改变。

采用实践型操作考试的原因

当今大多数认证考试都是采用选择题形式。对于这些类型的考试，其成本相对较低，而且监考容易。但是，许多没有真正技能的人却擅长这些类型的考试。在某些情形中，这些选择题型考试的答案在网络中早已存在。这导致了这样一种现象：那些通过认证的工程师相当于一个“纸老虎”，他们并没有掌握真正的技能。

针对这种情形，Red Hat 希望设计一个具有实际价值的认证考试项目。在我们看来，他们

已经在 RHCSA 考试、RHCE 考试以及其他高级考试中取得了很大的成功。

Linux 系统管理员有时需要在一台计算机或一个虚拟机上安装 Linux 系统。事实上，RHCSA 也包含几个与此问题有关的目标。系统管理员可能需要通过网格从一个中央储存库安装 Linux 系统，这取决于系统的配置。仅仅会安装 Linux 是不够的，更重要的是会使用 Linux。管理员需要知道如何配置 Linux：添加用户、安装和配置服务、建立防火墙以及其他操作。

考试提示

RHCSA 和 RHCE 认证考试是 Red Hat 考试。掌握 Ubuntu 等 Linux 或 Unix 发行版的知识以及 Apache、SMB、NFS、DNS、iptables 和 SSH 等服务的使用经验当然是有帮助的。但更重要的是如何在 Red Hat 企业版 Linux(或使用相同源代码的重构版，如 Scientific Linux、CentOS 或 Oracle Linux)下掌握这些服务的建立、配置、安装和调试方法。

为 RHCSA 和 RHCE 考试做好准备

随着 RHEL 6 的发布，Red Hat 引入了 RHCSA 考试以取代 RHCT。RHCSA 考试独立于 RHCE 考试。当然，两者确实存在一定的重叠。例如，SELinux 同时出现在这两个考试里，但是这两个考试的要求范围却不相同。RHCSA 和 RHCE 认证根据不同考试的结果进行评测。

RHCSA 属于初级 Red Hat 认证。虽然可以先考 RHCE，但是 Red Hat 不会授予 RHCE 证书给考生，除非他们已经通过了 RHCSA 考试。有些考生可能会在同一天参加这两个考试。正如第 1 章将要提到的，Red Hat 已公开发表声明，Red Hat 考试现在采用电子形式，本书提供的光盘也以电子形式向读者提供(绝大部分)实验题和考试模拟卷。

读者必须使用 Red Hat 企业版 Linux，并在一台没有其他用途的计算机上安装 Linux 系统，配置本书介绍的服务，找出保护这些服务安全的各种不同方法，从网络内部和网络外部测试这个系统。

在读者阅读本书的过程中，有好几个情况需要安装 RHEL。如果读者的计算机不止一台，可以通过网络安装 RHEL，然后测试各个网络服务。测试每个配置的服务，最好从网络上的另一台计算机进行测试。当需要验证考试中或生产网络中用到的安全功能时，测试是非常重要的。

Red Hat 认证项目

Red Hat 提供多个课程，帮助读者准备 RHCSA 和 RHCE 认证。这些课程的绝大多数需要 4~5 天的时间。在某些情形下，一些课程也以电子形式提供。

Red Hat 提供的培训课程不仅限于上述这些。它还提供其他培训课程，如 Red Hat 认证构架师(Red Hat Certified Architect, RHCA)、Red Hat 认证虚拟化管理专家(Red Hat Certified Virtualization Administrator, RHCVA)、Red Hat 认证数据中心专家(Red Hat Certified Datacenter Specialist, RHCDS)和 Red Hat 认证安全专家(Red Hat Certified Security Specialist, RHCSS)。但是必须先通过 RHCSA 和 RHCE 认证，它们是 Red Hat 其他认证的先决条件，例外情形是 RHCVA 认证。

是否必须参加 RHCSA/RHCE 培训课程

本书无意取代任何 Red Hat RHCSA 或 RHCE 培训课程。但是，本书讨论的主题内容部分来源于www.redhat.com/courses 网站上培训课程的教学大纲。根据最初的设计愿望，这些内容可以帮助 Linux 用户成为一名真正合格的系统管理员，这一点已得到证实。读者只需要记住，Red Hat 随时会改变这些考试内容和培训课程的教学大纲，因此要掌握最新的内容，读者需要经常访问 www.redhat.com 网站。表 1 介绍了与 RHCSA 和 RHCE 考试有关的课程。

表 1 与 Red Hat RHCSA/RHCE 认证考试有关的课程

课　程	说　明
RH124	系统管理 I 级：核心系统管理技能
RH134	系统管理 II 级：Linux 系统管理员的命令行技能(RH135 中不包括 RHCSA 内容)
RH135	系统管理 II 级：包含 RHCSA 内容
RH199	为有经验的系统管理员提供的快速培训课程
RH200	RH199+RHCSA 考试
EX200	只包括 RHCSA 考试
RH254	系统管理 III 级：高级安全与服务器技能
RH299	系统管理IV级：针对有经验的系统管理员的 Red Hat 快速课程
RH300	RH299+RHCSA 考试+RHCE 考试
EX300	RHCE 考试

Red Hat 提供的课程都是很不错的。教授这些课程的老师都具有高超的技能。如果读者已经拥有这些技能，则这是准备参加 RHCSA 和 RHCE 考试的最佳方式。如果读者觉得需要得到这些老师的指导，则先阅读本书，然后参加这些培训课程。

如果读者还没有确定是参加培训课程还是使用本书，则可以阅读本书的第 1 章。这一章概括介绍与 RHCSA 和 RHCE 认证考试相关的要求及相应内容。如果读者觉得第 1 章的内容太难，无法接受，则可以考虑使用本章开头介绍的参考书之一或者其他 Red Hat 较低级的课程。此外，第 1 章里提供了一个实验题，目的是让读者了解 Linux 职业学院对第一级认证(LPIC-1)的要求。一些与你一样也准备参加 Red Hat 考试的计算机高手总是先参加 LPIC-1 考试。

或者，读者可能已经熟悉了本书的内容，而且具有通过 RHCSA 和 RHCE 考试所需的知识深度和广度。在这种情形下，读者可以使用本书，它可以让读者快速熟悉这两个考试所需的技术和技能。

RHCSA/RHCE 课程和/或考试的注册

Red Hat 为培训课程和测试提供了方便的、基于 Web 的注册系统。要注册 Red Hat 的某门课程或考试，需要先导航到 www.redhat.com 网站，单击 Training | Courses 链接，然后选择想要参加的培训课程或考试。如表 1 所示，有些考试有专门的培训课程。例如，RHCSA 和 RHCE 考试有相应的专门课程 EX200 和 EX300。考试可以作为在线培训课程或者有指导老师负责的培

训课程的一部分。或者，联系 Red Hat 入学注册中心，它的 email 地址是 training@redhat.com，联系电话是(866)626-2994。

对于已经通过 RHCE 或 RHCE 认证的考生，Red Hat 提供了优惠措施。关于当前的优惠信息可以阅读 <https://www.redhat.com/training/specials/> 网站上的内容。在缴付考试费时，不要忘记提供优惠代码(offer code)。

在注册之前，仔细阅读当前的 Red Hat 政策，www.redhat.com/training/policy/ 网站上有这方面的信息。注意，Red Hat 也可能由于参加考试的人数比较少而取消考试。

最后的准备

Red Hat 考试是很累人的。对于拥有相关技能的考生，最重要的是考试时保持清醒的头脑。如果考生感觉到疲劳或者恐慌，则可能会想不起经常使用的、十分容易的解决方法。在考试前一个晚上，要保证充足的睡眠。早餐要吃饱，可以带一些点心，想办法让自己处于巅峰状态。

RHCSA 考试需要 2.5 个小时，RHCE 考试需要 2 个小时。在很多时候，Red Hat 尽量会安排让一个考生在同一天参加两个考试。虽然这对于那些需要跑很长路的考生来说可以带来旅途方便(在北美有超过 40 个城市设有考点)，但是在同一天参加这两个考试就像是参加两次马拉松赛跑。本书属于高级教程，不是为 Linux 或 Unix 入门者设计的。原来的“必备技能”已经合并到 RHCSA 要求里，因此本书只是简单地介绍与这些必备技能有关的工具——主要在第 1 章和第 3 章。如果读者想进一步了解这些必备技能，Red Hat 提供了其他培训课程(浏览 www.redhat.com/apps/training/)，或者可以阅读第 1 章介绍的参考书。

考试内幕

RHCSA 和 RHCE 认证对应于两个不同的考试。然而，RHCE 考试要求考生掌握比 RHCSA 更高级的技能。由于它们是两个不同的考试，因此本书分开介绍它们的目标。读者可以注意 www.redhat.com/certification/rhcsa/objectives/ 和 www.redhat.com/certification/rhce/objectives/ 上的最新内容。

RHCSA 考试

表 2 RHCSA 考试知识点检查表

认 证 目 标	学 习 主 题	章
分类：基本工具的认识和使用		
用正确的语法访问 shell 提示和执行命令	shell，标准命令行工具	3
用 grep 和正则表达式分析文本流和文件	文本文件的管理	3
使用输入/输出重定向	shell	3
用 SSH 访问远程系统	用安全 shell 管理系统	2
用 VNC 访问远程系统	用 VNC 配置访问	9
在多用户运行级别中登录和切换用户	用户和 shell 配置	8

(续表)

认 证 目 标	学 习 主 题	章
用 tar、star、gzip 和 bzip2 命令存档、压缩、解包、解压缩文件	基本的系统管理命令	9
创建和编辑文本文件	文本文件的管理	3
建立、删除、复制、移动文件和目录	标准的命令行工具	3
建立硬链接和软链接	标准的命令行工具	3
列出、设置和修改 ugo/rwx 权限	基本的文件权限	4
定位、读取、使用系统文档，包括 man、info 命令和/usr/share/doc 目录里的文件	本地在线文档	3
分类：操作运行的系统		
正常的启动、重新启动和关闭系统过程	引导程序与 GRUB；在 GRUB 和登录之间	5
在系统引导时，用手动方法把系统引导到不同的运行级别	引导程序与 GRUB	5
用单用户模式访问系统	引导程序与 GRUB	5
识别 CPU/内存密集型进程，用 renice 和 kill 进程调整进程优先级	基本的系统管理命令	9
定位和解释系统的日志文件	本地日志文件分析	9
访问虚拟机的控制台	配置 KVM 上的一个虚拟机	2
启动和停止虚拟机	配置 KVM 上的一个虚拟机	2
启动、停止网络服务、检查网络服务的当前状态	联网入门	2
分类：建立、配置文件系统		
建立、挂载、卸载和使用 ext2、ext3 和 ext4 文件系统	卷管理与分区、文件系统格式化、文件系统管理	6
建立、挂载、使用 LUKS 加密的文件系统	用 LUKS 方法加密卷	6
挂载、卸载 CIFS 和 NFS 网络文件系统	文件系统管理	6
配置系统，它可以自动挂载 ext4 文件系统、LUKS 加密的文件系统和网络文件系统	文件系统管理	6
扩展现有的未加密的 ext4 格式逻辑卷	逻辑卷管理(LVM)	6
配置用于协作的 GID 目录	特殊组	8
建立和管理访问控制列表(ACL)	访问控制列表及其他	4
诊断和修正文件权限问题	基本文件权限	4
分类：系统的部署、配置和维护		
配置网络连接以及主机名静态和动态解析	网络配置与故障排查	3
用 cron 实现任务调度	系统管理的自动化：cron 和 at 命令	9
系统配置：自动启动到某个运行级别	在 GRUB 和登录之间	5
用 Kickstart 自动安装 Red Hat 企业版 Linux	自动安装的选项	2
在一个物理机器上配置以托管虚拟访客	为 Red Hat 配置 KVM	2
以虚拟访客的身份安装 Red Hat 企业版 Linux	在 KVM 上配置一个虚拟机	2
配置系统，使它在引导时启动虚拟机	在 KVM 上配置一个虚拟机	2
配置网络服务，使服务在引导时自动启动	运行级别的控制	5
配置一个系统，它可以运行一个默认配置的 HTTP 服务器	配置默认文件共享服务	1
配置一个系统，它可以运行一个默认配置的 FTP 服务器	配置默认文件共享服务	1
通过 Red Hat 网络、远程储存库或本地文件系统安装和更新软件程序包	Red Hat 程序包管理器、依赖关系和 yum 命令、其他程序包管理工具	7

(续表)

认 证 目 标	学 习 主 题	章
适当更新内核程序包, 确保可引导系统的安全	Red Hat 程序包管理器	7
修改系统的引导程序	引导程序与 GRUB	5
分类: 用户和组的管理		
建立、删除、修改本地用户账户	用户账户的管理	8
修改密码, 解决本地用户账户的密码过期问题	用户账户的管理	8
建立、删除和修改本地组和组成员关系	用户账户的管理	8
配置一个系统, 它用现有的 LDAP 目录服务保存用户和组的信息	用户与网络认证	8
分类: 安全管理		
用 system-config-firewall 或 iptables 命令配置防火墙设置	防火墙的基本控制	4
给 SELinux 设置强制模式和许可模式	安全增强型 Linux 入门	4
显示和识别 SELinux 文件和进程上下文	安全增强型 Linux 入门	4
恢复默认的文件上下文	安全增强型 Linux 入门	4
用二进制参数修改系统的 SELinux 配置	安全增强型 Linux 入门	4
诊断和处理日常的 SELinux 策略违反问题	安全增强型 Linux 入门	4

表 3 RHCE 考试目标检查表

RHCE 考试知识检查表		
认 证 目 标	专 题	章
分类: 系统配置与管理		
路由 IP 流量, 建立静态的路由	特殊网络选项	12
用 iptables 实现数据包过滤和配置网络地址转换(NAT)	防火墙和网络地址转换	10
用 /proc/sys 和 sysctl 修改和设置内核运行时参数	内核运行时参数	12
配置一个使用 Kerberos 认证的系统	特殊网络选项	12
建立一个简单的 RPM, 它对一个文件进行打包	建立一个 RPM 程序包	12
把一个系统配置为 iSCSI 启动, 它可以持久挂载一个 iSCSI 目标	特殊的网络选项	12
生成并发布利用报告(处理器、内存、磁盘和网络)	建立系统利用报告	17
用 shell 脚本功能自动实现系统的维护	系统维护的自动化	12
配置一个系统, 它可以记录到一个远程系统	配置一个系统日志记录服务器	17
配置一个系统, 它可以接受来自远程系统的记录	配置一个系统日志记录服务器	17
分类: 网络服务(以下 5 个目标都针对网络服务)		
安装提供网络服务所需要的程序包	全部 RHCE 章节	10-17
配置 SELinux, 支持网络服务	安全增强型 Linux, 以及每个服务的其他章节	10-17
配置网络服务, 使得它在系统启动时自动启动	安全和配置检查表	11
配置完成基本操作的服务	所有 RHCE 章节	10-17
为服务配置基于主机的安全和基于用户的安全	所有 RHCE 章节	10-17
子分类: HTTP/HTTPS		
配置一个虚拟主机	一般的和安全的虚拟主机	14

(续表)

RHCE 考试知识检查表		
认 证 目 标	专 题	章
配置专用目录	专用的 Apache 目录	14
部署一个基本的 CGI 应用程序	部署一个基本的 CGI 应用程序	14
配置组托管的内容	专用的 Apache 目录	14
子分类: DNS(不要求考生配置主名称服务器和从名称服务器)		
配置一个仅缓存的名称服务器	最少的 DNS 服务器配置	17
配置一个仅缓存的名称服务器, 它可以转发 DNS 请求	最少的 DNS 服务器配置	17
子分类: FTP		
配置只允许匿名访问的下载功能	非常安全的 FTP 服务器	16
子分类: NFS		
给特定的客户端提供网络共享服务	网络文件系统(NFS)服务器	15
为组协作提供合适的网络共享	网络文件系统(NFS)服务器	16
子分类: SMB		
给特定的客户端提供网络共享服务	Samba 服务、Samba 故障排查	15
为组协作提供合适的网络共享	Samba 服务、Samba 故障排查	15
子分类: SMTP		
配置一个邮件转发代理(MTA), 它可以接受由其他系统传入的电子邮件	Postfix 的配置, 其他 STMP 服务: sendmail	13
配置一个 MTA 代理, 它通过一个智能主机转发(中继)电子邮件	Postfix 的配置, 其他 STMP 服务: sendmail	13
子分类: SSH		
配置基于键的认证	安全 shell 服务器	11
配置文档里介绍的其他选项	安全 shell 服务器	11
子分类: NTP		
使用其他 NTP 对等体同步时间	网络时间服务器服务	17

目 录

第 1 章 准备 Red Hat 操作型认证考试 1	
认证目标 1.01 RHCSA 和 RHCE 认证考试 3	
1.1.1 考试体验 4	
1.1.2 RHCSA 认证考试 4	
1.1.3 RHCE 认证考试 5	
1.1.4 如果只准备参加 RHCSA 考试 5	
1.1.5 不断演变的要求 5	
认证目标 1.02 基本的硬件要求 5	
1.2.1 硬件兼容性 5	
1.2.2 体系结构 6	
1.2.3 内存要求 7	
1.2.4 硬盘选项 7	
1.2.5 网络连接 8	
1.2.6 虚拟机选项 8	
认证目标 1.03 获得 Red Hat 企业版 Linux 9	
1.3.1 购买预订版本(subscription) 9	
1.3.2 获得评估版本 9	
1.3.3 第三方重构版本 10	
1.3.4 检查下载的文件 10	
认证目标 1.04 安装要求 11	
1.4.1 不需要从零开始 11	
1.4.2 网络安装的优点 11	
1.4.3 Red Hat 与虚拟机 12	
1.4.4 虚拟系统与物理系统 12	
1.4.5 练习使用的预安装环境 12	
1.4.6 系统角色(System Role) 13	
认证目标 1.05 安装选项 14	
1.5.1 引导媒介 14	
1.5.2 用 CD/DVD 或引导 USB 启动安装 15	
1.5.3 基本的安装步骤 15	
1.5.4 准备在分区上安装 21	
1.5.5 分区创建练习 23	
1.5.6 练习 1-1：在安装过程中进行分区 24	
1.5.7 配置引导加载程序 25	
1.5.8 RHEL 6 中的所有程序包 26	
1.5.9 基线程序包 28	
1.5.10 程序包组 28	
1.5.11 系统重启 30	
认证目标 1.06 系统设置选项 31	
1.6.1 第一引导进程 31	
1.6.2 默认的安全设置 32	
1.6.3 虚拟机的特殊设置选项 33	
认证目标 1.07 配置默认的文件共享服务 34	
1.7.1 挂载和复制安装 DVD 盘 34	
1.7.2 设置一个默认配置的 Apache 服务器 35	
1.7.3 练习 1-2：把 Apache 服务器配置为安装服务器 36	
1.7.4 通过 FTP 服务器共享复制文件 37	
1.8 认证小结 38	
1.9 小练习 39	
1.10 自测题 40	
1.11 实验题 41	
1.12 自测题答案 43	
1.13 实验题答案 44	
第 2 章 虚拟机与自动安装 47	
认证目标 2.01 配置 Red Hat KVM 48	
2.1.1 选择虚拟机的理由 49	

2.1.2 假设必须安装 KVM 49 2.1.3 选择正确的 KVM 模块 51 2.1.4 配置虚拟机管理程序 51 2.1.5 练习 2-1: 创建第二个虚拟 网络 54 认证目标 2.02 在 KVM 上配置 虚拟机 56 2.2.1 在 KVM 上配置虚拟机 57 2.2.2 练习 2-2: 添加虚拟硬盘 驱动器 61 2.2.3 KVM 配置文件 62 2.2.4 从命令行控制虚拟机 62 认证目标 2.03 自动安装选项 66 2.3.1 Kickstart 基本原理 67 2.3.2 设置对 Kickstart 的本地 访问 67 2.3.3 建立 Kickstart 的网络 访问 68 2.3.4 示例 Kickstart 文件 69 2.3.5 练习 2-3: 创建和使用示例 Kickstart 文件 73 2.3.6 Kickstart 配置程序 74 认证目标 2.04 用 SSH 管理系统 77 2.4.1 配置 SSH 客户端 78 2.4.2 命令行访问 78 2.4.3 SSH 的其他命令行工具 79 2.4.4 SSH 图形化访问 79 认证目标 2.05 考虑添加命令行 工具 80 2.5.1 用 telnet 检查端口 80 2.5.2 用 nmap 检查端口 81 2.5.3 配置 e-mail 客户端 82 2.5.4 命令行电子邮件 82 2.5.5 阅读邮件信息 82 2.5.6 文本和图形浏览器的 使用 83 2.5.7 用 lftp 访问 URL 84 2.6 认证小结 85 2.7 小练习 86	2.8 自测题 87 2.9 实验题 88 2.10 自测题答案 89 2.11 实验题答案 90 第 3 章 基本的命令行技术 93 认证目标 3.01 shell 96 3.1.1 其他 shell 96 3.1.2 终端控制台 96 3.1.3 GUI shell 接口 97 3.1.4 普通用户与管理员用户的 区别 97 3.1.5 文本流与命令重定向 98 认证目标 3.02 标准命令行工具 99 3.2.1 文件与目录的概念 99 3.2.2 文件列表和 ls 命令 101 3.2.3 文件创建命令 102 3.2.4 通配符 104 3.2.5 文件搜索 104 认证目标 3.03 文本文件的管理 105 3.3.1 文本流的读命令 105 3.3.2 处理文本流的命令 107 3.3.3 在控制台编辑文本文件 108 3.3.4 练习 3-1: 用 vi 创建一个 新用户 110 3.3.5 如果不喜欢 vi 111 3.3.6 用 GUI 工具编辑文本 文件 112 认证目标 3.04 本地在线文档 112 3.4.1 何时需要帮助文档 113 3.4.2 各种 man 页面 113 3.4.3 info 手册 115 3.4.4 /usr/share/doc 目录中的文档 细节 115 认证目标 3.05 网络入门 115 3.5.1 IPv4 数字与地址类 116 3.5.2 基本的 IPv6 寻址 116 3.5.3 如何用 IP 地址定义一个 网络 117
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3.5.4 工具、命令和网关 118 认证目标 3.06 网络配置与故障排除 3.6.1 网络配置文件 122 3.6.2 网络配置工具 124 3.6.3 练习 3-2：配置一个网卡 126 3.6.4 主机名配置文件 128 3.6.5 主机名配置选项 129 3.6.6 网络管理器小程序 130 3.7 认证小结 131 3.8 小练习 131 3.9 自测题 133 3.10 实验题 134 3.11 自测题答案 134 3.12 实验题答案 135 第 4 章 RHCSA 级的安全选项 137 认证目标 4.01 文件的基本权限 139 4.1.1 文件权限和所有权 139 4.1.2 用户与组的基本概念 141 4.1.3 umask 141 4.1.4 默认的 umask 值 142 4.1.5 修改权限和所有权的命令 142 4.1.6 特殊文件的属性 144 认证目标 4.02 访问控制列表及其他 145 4.2.1 每个文件都有一个 ACL 145 4.2.2 使文件系统成为 ACL 友好的系统 145 4.2.3 控制文件的 ACL 146 4.2.4 配置 ACL 的目录 147 4.2.5 用 ACL 实现特殊限制 148 4.2.6 ACL 和屏蔽位 149 4.2.7 练习 4-1：用 ACL 拒绝一个用户的访问 149 4.2.8 NFS 共享与 ACL 150 认证目标 4.03 基本的防火墙控制 151	4.3.1 标准端口 152 4.3.2 重点介绍 iptables 命令 152 4.3.3 确保防火墙在运行中 154 4.3.4 RHEL 6 默认防火墙 154 4.3.5 防火墙配置工具 156 4.3.6 练习 4-2：调整防火墙配置 160 认证目标 4.04 安全增强型 Linux 入门 161 4.4.1 SELinux 的基本功能 161 4.4.2 SELinux 的状态 161 4.4.3 在命令行配置 SELinux 162 4.4.4 配置基本的 SELinux 设置 163 4.4.5 为 SELinux 配置普通用户 163 4.4.6 管理 SELinux 布尔型设置 164 4.4.7 显示和识别 SELinux 文件上下文 165 4.4.8 恢复 SELinux 文件上下文 166 4.4.9 识别 SELinux 进程上下文 166 4.4.10 诊断和处理违反 SELinux 策略的事件 167 4.4.11 GUI SELinux 管理工具 169 4.4.12 SELinux 故障排除浏览器 172 4.4.13 练习 4-3：测试 SELinux 用户类型 172 4.5 认证小结 173 4.6 小练习 174 4.7 自测题 175 4.8 实验题 176 4.9 自测题答案 176 4.10 实验题答案 177
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

第 5 章 引导过程 181 认证目标 5.01 BIOS 与 UEFI 182 <ul style="list-style-type: none"> 5.1.1 系统的基本配置 183 5.1.2 启动菜单 183 5.1.3 访问 Linux 引导程序 184 认证目标 5.02 引导程序与 GRUB 程序 185 <ul style="list-style-type: none"> 5.2.1 GRand 统一引导加载 程序——GRUB 185 5.2.2 引导到不同的运行级 185 5.2.3 练习 5-1: 将系统引导到 不同的运行级 186 5.2.4 修改系统的引导程序 187 5.2.5 更多的选项 189 5.2.6 GRUB 安全与口令保护 190 5.2.7 如何更新 GRUB 190 5.2.8 GRUB 错误的影响 190 5.2.9 GRUB 命令行 191 5.2.10 练习 5-2: 使用 GRUB 命令行 192 5.2.11 创建自己的 GRUB 配置 文件 193 5.2.12 从 GRUB 引导的一个选项: 急救模式 193 证书目标 5.03 GRUB 与登录 196 <ul style="list-style-type: none"> 5.3.1 内核与初始 RAM 磁盘 196 5.3.2 第一个进程、运行级和 服务 197 5.3.3 运行级之间的切换 198 5.3.4 重新启动和正常关闭 系统 198 5.3.5 用 Upstart 取代 SysVInit 199 5.3.6 Upstart 配置文件 199 5.3.7 终端与登录界面 201 认证目标 5.04 运行级的控制 202 <ul style="list-style-type: none"> 5.4.1 按运行级定义功能 202 5.4.2 运行级脚本的内部 构造 203 5.4.3 命令行服务配置 204 	5.4.4 文本控制台服务配置 工具 205 <ul style="list-style-type: none"> 5.4.5 GUI 服务配置工具 206 认证目标 5.05 网络配置 207 <ul style="list-style-type: none"> 5.5.1 网络配置命令 207 5.5.2 网络配置文件 211 5.5.3 etc/sysconfig/network-scripts 文件 211 5.5.4 Red Hat 配置工具 212 5.5.5 练习 5-3: 用网络连接工具 修改网络接口 213 5.5.6 配置名称解析 214 5.5.7 练习 5-4: 修改克隆系统的 网络接口 215 认证目标 5.06 时间同步 217 <ul style="list-style-type: none"> 5.6.1 NTP 客户端 217 5.6.2 日期/时间属性 217 5.7 认证小结 218 5.8 小练习 219 5.9 自测题 220 5.10 实验题 222 5.11 自测题答案 222 5.12 实验题答案 223
第 6 章 Linux 文件系统管理 229	
认证目标 6.01 存储管理与分区 231 <ul style="list-style-type: none"> 6.1.1 系统的当前状态 231 6.1.2 fdisk 实用工具 232 6.1.3 parted 实用工具 237 6.1.4 图形选项 242 6.1.5 练习 6-1: fdisk 和 parted 命令的使用 243 认证目标 6.02 文件系统的格式 244 <ul style="list-style-type: none"> 6.2.1 标准的格式化文件系统 244 6.2.2 日志式文件系统 245 6.2.3 文件系统格式化命令 246 6.2.4 交换卷 246 6.2.5 文件系统的检查命令 247 6.2.6 文件系统的相互转换 247 	

6.2.7 练习 6-2: 格式化、检查和挂载不同的文件系统 248 认证目标 6.03 基本的 Linux 文件系统和目录 248 6.3.1 Linux 的各个文件系统 248 6.3.2 可以单独挂载的目录 250 认证目标 6.04 逻辑卷管理器 (LVM) 250 6.4.1 与 LVM 有关的定义 250 6.4.2 建立物理卷 251 6.4.3 建立卷组 251 6.4.4 建立逻辑卷 251 6.4.5 逻辑卷的使用 252 6.4.6 其他 LVM 命令 252 6.4.7 删除逻辑卷 254 6.4.8 调整逻辑卷的大小 255 6.4.9 GUI 逻辑卷管理工具 256 认证目标 6.05 用 Linux 统一密钥设定方法实现卷加密 260 6.5.1 口令、密码短语及其他 260 6.5.2 安装过程中的加密 261 6.5.3 加密的准备工作和初始化 261 6.5.4 准备好新的文件系统 262 6.5.5 创建新文件系统 262 认证目标 6.06 文件系统的管理 264 6.6.1 /etc/fstab 文件 264 6.6.2 /etc/fstab 文件中的通用唯一标识符 266 6.6.3 挂载命令 266 6.6.4 文件系统挂载的其他选项 267 6.6.5 虚拟文件系统 268 6.6.6 在/etc/fstab 文件中添加自己的文件系统 268 6.6.7 可移动媒介和/etc/fstab 文件 268 6.6.8 联网的文件系统 269 认证目标 6.07 自动挂载程序 270	6.7.1 通过自动挂载程序进行挂载 270 6.7.2 练习 6-3: 配置自动挂载程序 274 6.8 认证小结 275 6.9 小练习 276 6.10 自测题 277 6.11 实验题 278 6.12 自测题答案 279 6.13 实验题答案 280 第 7 章 程序包管理 283 认证目标 7.01 Red Hat 程序包管理器 284 7.1.1 程序包的含义 284 7.1.2 Red Hat 程序包的含义 285 7.1.3 库的含义 285 7.1.4 安装 RPM 程序包 286 7.1.5 卸载 RPM 程序包 287 7.1.6 从远程系统安装 RPM 287 7.1.7 RPM 安装的安全性 288 7.1.8 带内核的特殊 RPM 过程 289 认证目标 7.02 更多 RPM 命令 290 7.2.1 程序包查询 291 7.2.2 程序包签名 291 7.2.3 文件校验 291 7.2.4 所安装程序包的不同数据库 293 认证目标 7.03 依赖和 yum 命令 293 7.3.1 依赖地狱示例 293 7.3.2 从依赖地狱解脱 295 7.3.3 yum 基本配置 295 7.3.4 基本 yum 配置文件: yum.conf 296 7.3.5 /etc/yum/pluginconf.d 目录中的配置文件 297 7.3.6 /etc/yum.repos.d 目录中的配置文件 297
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.3.7 创建自己的/etc/yum.repos.d 配置文件 299 7.3.8 练习 7-1: 从 RHEL 6 DVD 创建 yum 库 302 7.3.9 第三方库 303 7.3.10 基本 yum 命令 303 7.3.11 安装模式 303 7.3.12 安全性和 yum 304 7.3.13 更新和安全修复 305 7.3.14 程序包组和 yum 305 7.3.15 更多 yum 命令 307 认证目标 7.04 更多程序包管理 工具 308 7.4.1 GNOME 软件更新工具 309 7.4.2 自动更新 310 7.4.3 GNOME Add/Remove Software 工具 310 7.4.4 练习 7-2: 使用 yum 和 Add/ Remove Software 工具安装多 个程序包或程序包组 311 7.4.5 Red Hat 网络 312 7.5 认证小结 313 7.6 小练习 313 7.7 自测题 314 7.8 实验题 315 7.9 自测题答案 315 7.10 实验题答案 317 第 8 章 用户管理 321 认证目标 8.01 用户账户管理 322 8.1.1 用户类型 323 8.1.2 阴影口令套组 323 8.1.3 命令行工具 327 8.1.4 练习 8-1: 使用 Red Hat User Manager 添加用户 329 8.1.5 练习 8-2: 真假 Shell 330 8.1.6 删除用户 330 8.1.7 修改账户 330 8.1.8 更多用户和组管理命令 331	认证目标 8.02 管理控制 332 8.2.1 作为根管理用户登录 333 8.2.2 练习 8-3: 限制根管理用户 登录 333 8.2.3 登录 333 8.2.4 su 命令的正确用法 334 8.2.5 限制访问 su 334 8.2.6 sg 命令的正确用法 335 8.2.7 使用 sudo 命令自定义 管理员 335 8.2.8 其他管理用户 336 认证目标 8.03 用户和 Shell 配置 336 8.3.1 主目录和/etc/skel 336 8.3.2 /etc/bashrc 337 8.3.3 /etc/profile 和/etc/ profile.d 337 8.3.4 /etc/profile.d 338 8.3.5 练习 8-4: 保护系统的另一种 方法 338 8.3.6 用户主目录中的 Shell 配置 文件 339 8.3.7 登录、登出和用户转换 339 认证目标 8.04 用户和网络身份 验证 339 8.4.1 LDAP 客户配置 340 8.4.2 Name Service Switch 文件 341 8.4.3 Red Hat 网络验证工具 342 认证目标 8.05 特定组 344 8.5.1 标准组和 Red Hat 组 344 8.5.2 共享目录 344 8.5.3 练习 8-5: 使用 SGID 位 控制组所有权 345 8.6 认证小结 347 8.7 小练习 347 8.8 自测题 348 8.9 实验题 349 8.10 自测题答案 350 8.11 实验题答案 350
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

第 9 章 RHCSA 级系统管理任务	353	9.4.5 练习 9-2: 学习日志文件	379
认证目标 9.01 通过 VNC 配置		9.5 认证小结	379
访问	354	9.6 小练习	380
9.1.1 安装和配置 TigerVNC 服务器	355	9.7 自测题	381
服务器	355	9.8 实验题	382
9.1.2 基于 GNOME 的 vino 服务器	356	9.9 自测题答案	382
服务器	356	9.10 实验题答案	383
9.1.3 安装和配置 VNC 客户	357		
9.1.4 防火墙选项	358		
9.1.5 确认访问 VNC 服务器	359		
9.1.6 通过安全 Shell 选择			
路由	360		
9.1.7 更多 VNC 配置	360		
9.1.8 用户 VNC 配置文件	361		
认证目标 9.02 基本的系统管理			
命令	361		
9.2.1 系统资源管理命令	361		
9.2.2 存档文件和压缩	368		
9.2.3 通过守护进程控制			
服务	369		
认证目标 9.03 系统管理自动化:			
cron 和 at	369		
9.3.1 系统 crontab 和组件	370		
9.3.2 按小时执行的 cron 任务	371		
9.3.3 定期的 Anacron 工作			
任务	372		
9.3.4 为用户建立 cron 工作			
任务	373		
9.3.5 练习 9-1: 创建 cron 工作			
任务	373		
9.3.6 使用 at 系统运行工作			
任务	374		
9.3.7 安全的 cron 和 at	374		
认证目标 9.04 本地日志文件分析	375		
9.4.1 系统日志配置文件	376		
9.4.2 日志文件管理	376		
9.4.3 各种日志文件	377		
9.4.4 服务专用日志	378		
第 10 章 安全入门	385		
认证目标 10.01 Linux 安全层	386		
10.1.1 Bastion 系统	387		
10.1.2 使用安全更新的最佳防御	387		
10.1.3 服务特有的安全	387		
10.1.4 基于主机的安全	389		
10.1.5 基于用户的安全	389		
10.1.6 控制台安全	390		
10.1.7 美国国家安全局的建议	390		
10.1.8 PolicyKit	390		
认证目标 10.02 防火墙和网络地址转换			
10.2.1 定义	392		
10.2.2 iptables 命令的结构	392		
10.2.3 默认防火墙	394		
10.2.4 NSA 的建议	394		
10.2.5 确保防火墙始终运行	396		
10.2.6 IP 伪装	396		
10.2.7 IP 转发	397		
10.2.8 Red Hat Firewall Configuration 工具	398		
认证目标 10.03 扩充的 Internet 超级服务器			
10.3.1 通用 xinetd 配置	404		
10.3.2 服务特有的 xinetd 配置	405		
10.3.3 练习 10-1: 配置 xinetd	406		
认证目标 10.04 TCP 包装器	407		

10.4.1 服务由 TCP 包装器 保护吗 407 10.4.2 TCP 包装器配置文件 408 10.4.3 练习 10-2: 配置 TCP 包装器 409 认证目标 10.05 可插拔身份验证 模块 410 10.5.1 配置文件 410 10.5.2 控制标记 411 10.5.3 PAM 文件的格式 412 10.5.4 练习 10-3: 配置 PAM 415 10.5.5 PAM 和基于用户的 安全 415 10.5.6 练习 10-4: 使用 PAM 限制用户访问 416 认证目标 10.06 保护文件和 GPG2 的 更多信息 417 10.6.1 GPG2 命令 417 10.6.2 当前的 GPG2 配置 417 10.6.3 GPG2 加密选项 418 10.6.4 生成 GPG2 密钥 418 10.6.5 使用 GPG2 密钥保护 文件 420 10.7 认证小结 421 10.8 小练习 421 10.9 自测题 422 10.10 实验题 424 10.11 自测题答案 424 10.12 实验题答案 425 第 11 章 系统服务和 SELinux 429 认证目标 11.01 Red Hat 系统配置 430 11.1.1 服务管理 431 11.1.2 系统服务 431 11.1.3 配置过程简介 433 11.1.4 可用配置工具 433 认证目标 11.02 安全增强型 Linux 434 11.2.1 SELinux 布尔值目录中的 选项 434	11.2.2 SELinux 布尔值的服务 类别 435 11.2.3 使用 SELinux Management 工具配置布尔值 436 11.2.4 布尔值设置 436 11.2.5 SELinux 文件上下文 440 11.2.6 练习 11-1: 使用合适的 SELinux 上下文配置新 目录 441 认证目标 11.03 Secure Shell 服务器 441 11.3.1 SSH 配置命令 442 11.3.2 SSH 配置文件 442 11.3.3 基本的加密通信 443 11.3.4 为基于密钥的身份验证 创建私钥/公钥对 444 11.3.5 配置 SSH 服务器 445 11.3.6 SSH 基于用户的安全 451 11.3.7 SSH 基于主机的安全 451 认证目标 11.04 安全和配置 检查表 452 11.4.1 安装服务器服务 452 11.4.2 基本配置 454 11.4.3 确保服务在重启之后 存活 454 11.4.4 通过安全层审查访问 455 11.4.5 练习 11-2: 查看 iptables 和 TCP 包装器的不同 效果 457 11.5 认证小结 458 11.6 小练习 458 11.7 自测题 459 11.8 实验题 461 11.9 自测题答案 461 11.10 实验题答案 462 第 12 章 RHCE 管理任务 465 认证目标 12.01 系统维护自动化 466 12.1.1 标准的管理脚本 466
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

12.1.2 脚本命令	468	13.1.7 测试电子邮件服务器	501
12.1.3 创建自己的管理脚本	469	13.1.8 练习 13-1：为电子邮件创建 用户	501
12.1.4 练习 12-1：创建脚本	470	认证目标 13.02 配置 Postfix	501
认证目标 12.02 内核运行时参数	471	13.2.1 配置文件	501
12.2.1 sysctl 与 /etc/sysctl.conf 如何一起运行	471	13.2.2 main.cf 配置文件	504
12.2.2 /etc/sysctl.conf 文件中的 设置	471	13.2.3 /etc/aliases 配置文件	506
12.2.3 练习 12-2：禁止响应 ping 命令	472	13.2.4 master.cf 配置文件	507
认证目标 12.03 创建 RPM 程序包	473	13.2.5 测试当前的 Postfix 配置	507
12.3.1 源 RPM	473	13.2.6 配置 Postfix 身份验证	507
12.3.2 RPM 源的目录结构	474	13.2.7 配置传入的电子邮件	508
12.3.3 创建自定义源代码	475	13.2.8 配置通过智能主机的 中继	509
12.3.4 更多 Prep 程序包	476	13.2.9 练习 13-2：切换服务	509
12.3.5 创建自己的 spec 文件	476	认证目标 13.03 另一种 SMTP 服务： sendmail	509
12.3.6 构建自己的 RPM	479	13.3.1 sendmail 基础	510
12.3.7 构建 RPM	480	13.3.2 配置文件	510
认证目标 12.04 特殊网络选项	481	13.3.3 sendmail.mc 宏文件	511
12.4.1 配置特殊 IP 路由	481	13.3.4 submit.mc 宏文件	515
12.4.2 设置 Kerberos 客户	483	13.3.5 配置 sendmail 接受来自其他 系统的电子邮件	516
12.4.3 连接到远程 iSCSI 存储	487	13.3.6 配置 sendmail 以将电子 邮件中继到智能主机	516
12.5 认证小结	488	13.3.7 配置基于用户和基于主机的 sendmail 安全	517
12.6 小练习	489	13.3.8 测试 sendmail 的当前 配置	517
12.7 自测题	490	13.4 认证小结	518
12.8 实验题	491	13.5 小练习	518
12.9 自测题答案	491	13.6 自测题	519
12.10 实验题答案	492	13.7 实验题	520
第 13 章 电子邮件服务器	495	13.8 自测题答案	520
认证目标 13.01 各种电子邮件 代理	496	13.9 实验题答案	521
13.1.1 定义和协议	497	第 14 章 Apache Web 服务器	525
13.1.2 相关邮件服务器程序包	497	认证目标 14.01 Apache Web 服务器	526
13.1.3 使用 alternatives 命令选择 电子邮件系统	498	14.1.1 Apache 2.2	527
13.1.4 一般用户安全	499		
13.1.5 邮件日志记录	499		
13.1.6 常见的安全问题	500		

14.1.2 LAMP 栈 527 14.1.3 安装 527 14.1.4 练习 14-1: 安装 Apache 服务器 528 14.1.5 Apache 配置文件 529 14.1.6 分析默认的 Apache 配置 529 14.1.7 主要的 Apache 配置文件 530 14.1.8 简单 Web 服务器的基本 Apache 配置 532 14.1.9 Apache 日志文件 533 认证目标 14.02 标准的 Apache 安全配置 533 14.2.1 端口和防火墙 534 14.2.2 Apache 和 SELinux 534 14.2.3 模块管理 537 14.2.4 Apache 的安全性 537 14.2.5 练习 14-2: Apache Welcome 和 noindex.html 故事 539 14.2.6 练习 14-3: 创建文件 540 14.2.7 基于主机的安全 541 14.2.8 基于用户的 security 541 认证目标 14.03 专用 Apache 目录 542 14.3.1 通过 .htaccess 文件控制 543 14.3.2 受密码保护的访问 543 14.3.3 主目录访问 543 14.3.4 组管理的目录 545 14.3.5 练习 14-4: Web 目录的密码保护 546 认证目标 14.04 一般虚拟主机和安全虚拟主机 547 14.4.1 标准虚拟主机 548 14.4.2 安全虚拟主机 549 14.4.3 创建新的 SSL 证书 552 14.4.4 测试页面 555 14.4.5 语法检查程序 555 14.4.6 Apache 故障检修 555	14.4.7 练习 14-5: 创建虚拟 Web 服务器 556 认证目标 14.05 部署基本 CGI 应用程序 557 14.5.1 Apache CGI 文件的配置变更 557 14.5.2 创建简单的 CGI 脚本 558 14.5.3 连接网站 558 14.6 认证小结 559 14.7 小练习 560 14.8 自测题 560 14.9 实验题 562 14.10 自测题答案 562 14.11 实验题答案 563 第 15 章 Samba 文件服务器 567 认证目标 15.01 Samba 服务 568 15.1.1 安装 Samba 服务 569 15.1.2 Samba 的背景 570 15.1.3 端口、防火墙和 Samba 570 15.1.4 配置 Samba 的 SELinux 布尔值 571 15.1.5 配置 Samba 的 SELinux 文件类型 572 15.1.6 Samba 守护进程 572 15.1.7 Samba 服务器全局配置 573 15.1.8 Samba 共享目录 579 15.1.9 使 Samba 加入域 583 15.1.10 Samba 用户数据库 583 15.1.11 创建一个公共共享 584 15.1.12 练习 15-1: 配置 Samba 主目录共享 585 15.1.13 Samba Web 管理工具 586 15.1.14 测试 /etc/samba/smb.conf 文件的修改 591 15.1.15 回顾基于用户和主机的 Samba 安全 592 15.1.16 回顾基本的 Samba 共享 593
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>15.1.17 练习 15-2: 配置 Samba 共享 593</p> <p>认证目标 15.02 Samba 客户端 594</p> <ul style="list-style-type: none"> 15.2.1 命令行工具 594 15.2.2 挂载选项 595 15.2.3 自动挂载 Samba 共享 595 <p>认证目标 15.03 Samba 故障排查 595</p> <ul style="list-style-type: none"> 15.3.1 Samba 问题的确定 596 15.3.2 查看本地日志文件 597 15.3.3 启用远程访问 597 <p>15.4 认证小结 598</p> <p>15.5 小练习 598</p> <p>15.6 自测题 599</p> <p>15.7 实验题 600</p> <p>15.8 自测题答案 600</p> <p>15.9 实验题答案 601</p> <p>第 16 章 更多文件共享服务 605</p> <p>认证目标 16.01 NFS 服务器 606</p> <ul style="list-style-type: none"> 16.1.1 RHEL 6 的 NFS 选项 607 16.1.2 NFS 的基本安装 607 16.1.3 NFS 服务器的基本 配置 607 16.1.4 配置 NFS 完成基本 操作 609 16.1.5 /home 目录的特殊 要求 611 16.1.6 /etc/sysconfig/nfs 中的 固定端口 612 16.1.7 使 NFS 与 SELinux 协同 工作 614 16.1.8 NFS 的瓶颈和限制 615 16.1.9 性能提示 617 16.1.10 NFS 安全指令 617 16.1.11 基于主机的安全 选项 618 16.1.12 基于用户的安全 选项 618 16.1.13 练习 16-1: NFS 619 	<p>认证目标 16.02 测试 NFS 客户端 619</p> <ul style="list-style-type: none"> 16.2.1 NFS 挂载选项 620 16.2.2 在/etc/fstab 中配置 NFS 621 16.2.3 无磁盘的客户端 621 16.2.4 软挂载 621 16.2.5 NFS 的当前状态 622 <p>认证目标 16.03 vsFTP 服务器 622</p> <ul style="list-style-type: none"> 16.3.1 vsFTP 的基本配置 622 16.3.2 vsFTP 的主配置文件 623 16.3.3 其他 vsFTP 配置文件 626 16.3.4 为 vsFTP 配置 SELinux 支持 627 16.3.5 端口、防火墙和 vsFTP 628 16.3.6 练习 16-2: 配置基本的 vsFTP 服务器 628 16.3.7 仅匿名下载配置 629 <p>16.4 认证小结 629</p> <p>16.5 小练习 630</p> <p>16.6 自测题 631</p> <p>16.7 实验题 632</p> <p>16.8 自测题答案 632</p> <p>16.9 实验题答案 633</p> <p>第 17 章 管理服务: DNS、FTP 和日志 637</p> <p>认证目标 17.01 域名服务基本结构 639</p> <ul style="list-style-type: none"> 17.1.1 基本参数 639 17.1.2 DNS 程序包选项 639 17.1.3 不同类型的 DNS 服务器 640 <p>认证目标 17.02 DNS 服务器的最低 配置 640</p> <ul style="list-style-type: none"> 17.2.1 BIND 配置文件 640 17.2.2 高速缓存域名服务器 641 17.2.3 启动域名服务器 643 17.2.4 转发域名服务器 643 17.2.5 从高速缓存域名服务器 转发 644 17.2.6 BIND 故障排查命令 644
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

17.2.7 练习 17-1: 设置自己的 DNS 服务器 645	17.5.2 NTP 的安全约束 654
认证目标 17.03 设置系统使用报表 646	17.6 认证小结 654
17.3.1 系统使用命令 646	17.7 小练习 655
17.3.2 系统状态服务 647	17.8 自测题 656
17.3.3 搜集系统状态生成 日志 648	17.9 实验题 658
17.3.4 准备系统状态报表 648	17.10 自测题答案 658
认证目标 17.04 配置系统日志	17.11 实验题答案 659
服务器 649	
17.4.1 系统日志模块 650	附录 A 为模拟考试准备一个系统 663
17.4.2 启用日志客户端 650	附录 B 模拟考试 1: RHCSA 667
17.4.3 配置日志服务器 650	附录 C 模拟考试 2: RHCSA 671
17.4.4 配置日志客户端 651	附录 D 模拟考试 3: RHCE 模拟 考试 1 675
17.4.5 只允许指定的系统 访问 652	附录 E 模拟考试 4: RHCE 模拟 考试 2 679
认证目标 17.05 网络时间服务器	附录 F CD 使用说明 683
服务 652	
17.5.1 NTP 服务器配置文件 652	



第 1 章

准备 Red Hat 操作型 认证考试

认证目标

- ✓ 1.01 RHCSA 和 RHCE 认证考试
- ✓ 1.02 基本的硬件要求
- ✓ 1.03 获得 Red Hat 企业版 Linux
- ✓ 1.04 安装要求
- ✓ 1.05 安装选项
- ✓ 1.06 系统设置选项
- ✓ 1.07 配置默认的文件共享服务
- ✓ 小练习
- ✓ 自测题

Red Hat 认证考试颇具挑战性。虽然本书的内容围绕 Red Hat 认证系统管理员考试(Red Hat Certified System Administrator, RHCSA)，但是它也为那些想通过 Red Hat 认证工程师(Red Hat Certified Engineer, RHCE)考试的人提供了基础。正如本书的前言和本章中提到的那样，Red Hat 提供了若干培训课程以帮助有志人士通过这些考试。

本章的重点是系统安装。安装完成后得到一个 Red Hat Enterprise Linux(RHEL)的通用平台，并用这个系统测试本书后面的内容。本章介绍 Red Hat 默认虚拟机(VM)解决方案，即基于内核的虚拟机(Kernel-based Virtual Machine)对硬件系统的要求。社区企业操作系统(Community Enterprise Operating System, CentOS)和 ScientificLinux(Scientific Linux)等重构版本实质上与 RHEL 完全一样，因此用户也可以使用这些解决方案。这些重构版本与 RHEL 版本之间的唯一差别在于商标和对库的访问，这将在第 7 章中讨论。

如果对 Red Hat 需求的以前版本熟悉，那么可能会注意到 Red Hat 考试的最新变化。Red Hat 不再举办 RHCT 考试，现在取而代之的是 RHCSA。虽然在许多方面 RHCSA 与 RHCT 十分相似，但是也有几个重要的区别。大多数 RHCSA 的考试目标都包含在 RHCT 考试中。然而，RHCSA 并不比 RHCT 简单，现在它是参加 RHCE 考试的先决条件。RHCSA 的许多要求都是 RHCE 目标的一部分。

尽管如此，Red Hat 建议参加 RHCSA 考试的考生必须有 1~3 年 bash shell、用户管理、系统监测、基本网络设置、软件更新以及其他内容的相关经验。详细情况已在本书的前言中介紹过。

如果你是 Linux 或 Unix 的新手，则仅用本书是不够的。本书不够详细，至少没有按 Linux 或其他基于 Unix 操作系统的新手所希望的那样详细。阅读本书后，如果仍感觉到知识上的不足，可以参考以下入门教材：

- *Linux Administration: A Beginner's Guide*, 由 Wale Soyink 编写，麦格劳-希尔教育出版集团出版(2008)。该书介绍了 Linux 操作系统的详细操作步骤。
- *Security Strategies in Linux Platforms and Applications*, 由 Michael Jang 编写(Jones & Bartlett, 2010)。该书详细地介绍了加强 Linux 系统和网络安全的各种方法。
- *LPIC-1 in Depth*, Michael Jang 编写(Course Technology PTR, 2009)该书介绍了许多 Linux 专业人员在获取 RHCSA 和 RHCE 认证之前的资格证书考试。

在安装 Red Hat 企业版 Linux(RHEL)之前，必须具备合适的硬件基础。必须拥有一个 64 位 CPU 的硬件系统，它具有硬件虚拟功能(hardware virtualization)。详细情况将在本章中讨论。总的说来，尽管 RHCSA 和 RHCE 不属于硬件考试，但一些基本的硬件知识是任何 Linux 系统管理员的基本要求。至于 Linux 操作系统，你需要购买 RHEL 的一个版本，或者使用一个由第三方根据 Red Hat 公开发布的源代码生成的重构版本。

如果你有过操作其他 Unix 类型操作系统(如 Solaris、AIX 或 HP-UX)的经验，那么准备好在开始时不再使用那些默认设置。Ubuntu 和 Red Hat 发布之间有些重要的区别。当 Red Hat 开发了自己的 Linux 发布时，该公司有了一些与标准 Unix 实践不一致的选择。当我教授 Red Hat 的 RH300 的课时，具有上述背景知识的学生会感觉课程和 RHCE 考试之间有分歧。

为了编写本书，我作为 Linux 系统管理用户 root 执行了大部分的命令。我们不鼓励直接以 root 用户的身份登录到系统，除非你正在管理一个计算机系统。然而，由于 RHCSA 和 RHCE 考试是为了测试考生的系统管理技能，因此你以超级管理员(root)的身份执行本书的命令是允许

的，但是你还要知道如何建立拥有部分或全部管理员权限的普通用户。

考试内幕

虚拟主机

RHCSA 假定你知道“如何将一个物理机配置为虚拟机”。换言之，你需要准备一个可以提供虚拟机服务的系统，因为需要在这些虚拟机上安装 RHEL 的其他实例或者安装微软 Windows 等其他操作系统。

RHEL 是以 Red Hat 默认虚拟机系统(即 KVM)为基础的。由于 CentOS 和 Scientific Linux 等合适的重构版本都使用相同的源代码，因此它们也使用 KVM。在本章中你不仅要安装 RHEL，而且还要安装支持 KVM 的其他软件包。

默认的文件共享配置服务

RHCSA 管理员必须知道如何“将一个系统配置为可在其上运行默认配置的 HTTP 服务器”和“将一个系统配置为可在其上运行默认配置的 FTP 服务器”。这两个服务的默认解决方案是使用 Apache Web 服务器和非常安全的 FTP(vsFTP)服务器。虽然这些服务可能非常复杂，但是在这些服务器上配置文件共享所需要的步骤却非常简单。事实上，这些服务不需要对默认的配置文件做任何修改。本章提到的一些相关配置步骤要依赖于后面章节介绍的技术。

RHCSA 最早发布的目标在措词上稍有不同：“用 HTTP/FTP 部署文件共享服务”。我认为，从这里可以看出 Red Hat 这些目标的意图。为此，你要分析如何根据他们的默认配置文件将这些服务设置为文件服务器的方法。

使用 Red Hat 的其他版本

在本章中你还需要利用付费的订阅版本或演示用 DVD 安装 RHEL 6。当然你也可以使用一个重构版本。然而，尽管 RHEL 6 部分是以 Fedora Linux 的发行版本为基础的，但是实际上它在某些方面是以 Fedora 12 和 Fedora 13 的发行版本为基础。因此，如果你使用的是 Fedora 12 和 Fedora 13，则配置文件在某些情形可能与 RHEL 6 的配置有较大的差异。Fedora 后来的版本的特性很可能没有出现在 RHEL 6 中。

认证目标 1.01 RHCSA 和 RHCE 认证考试

Red Hat 最早在 1999 年开始举行认证考试。从那时起 Red Hat 考试不断演化。前面提到的 RHCT 是 RHCE 的一个完全子集。现在，RHCSA 包含 RHCE 但不包括与之密切相关的主题。

此外，Red Hat 考试的重点在于实际动手配置。从 2003 年开始去掉了多项选择题。更近的是从 2009 年开始，Red Hat 简化了考试内容，删除了在裸机上安装 Linux 的要求(然而又在 2011 年提出修改，要求考生掌握如何在 VM 上通过网络安装 Linux 系统)。此外，在考试中不再单独设置与故障排除(troubleshooting)有关的内容。详细信息可以访问 www.redhat.com/certification/faq。

考试提示

Red Hat 为 RHCSA 和 RHCE 考试培训课程提供了“预评估”考试，它们分别对应于 RH134 和 RH254 课程。每个课程都有相应的 Red Hat 网页，在这些网页上都可以找到相应的测试内容。Red Hat 在提供这些预评估测试之前要求考生提供联系信息。

1.1.1 考试体验

Red Hat 认证考试属于实践动手操作型考试。正因为如此，这些考试在整个行业中被公认为真正具有实际操作能力的标志。通过 Red Hat 考试的考生自然比那些只通过标准式多项选择题型认证考试的考生要优秀许多。

考试开始后，考生面对的是一个真实的系统。考生需要回答一些实际的配置问题，它们都与每个认证考试目标中的题目有关，详细内容查阅 <http://www.redhat.com/certification/rhcsa/objectives/> 和 <http://www.redhat.com/certification/rhce/objectives/> 网页上的介绍。自然，本书致力于帮助你掌握这些网页上提到的技术。

虽然在考试期间考生无法访问 Internet，但是可以使用 man 手册、Info 信息以及/usr/share/doc/directories 目录中的在线文档。当然这里假定已经安装了相关的程序包。

此外，Red Hat 认证考试采用电子格式。虽然简单的使用说明可能会用英语这样的本地语言来描述，但是 Red Hat 也用 12 种不同语言提供 RHCSA 和 RHCE 考试，它们是英语、简体中文、繁体中文、荷兰语、法语、意大利语、日语、韩语、葡萄牙语、俄语、西班牙语和土耳其语。如果你希望使用上述替代语言，请通过 training@redhat.com 或 1-866-626-2994 联系 Red Hat 培训中心。

Red Hat 为这两个考试提供相应的培训课程。这些课程的大纲可以从 www.redhat.com 网站上下载。虽然本书无法取代这些课程，但是本书的内容与这些课程的大纲一致。本书包含了这些考试的考核目标。

考试提示

在本书前言的表 2 中详细列出了本书覆盖的 RHCSA 和 RHCE 考试知识点。

1.1.2 RHCSA 认证考试

RHCSA 认证考试要求考生具有在真实物理系统和虚拟系统上配置网络连接、系统安全、自定义文件系统、软件更新和用户管理等操作的能力。从根本上说，RHCSA 考试覆盖了管理和配置企业中 Linux 工作站所需的技术。

RHCSA 认证考试的时间为两个半小时。考试一开始，考生就要在一个真实的 RHEL 系统上执行操作。对系统所做的任何修改都必须在重启后才能够保存下来。当考生完成某个操作时，监考老师检查考生的系统配置是否符合考试要求。例如，如果考试题目要求考生“建立、删除和修改本地用户账户”，则使用 vi 编辑器还是图形用户管理器工具编辑相关的配置文件并不重要。只要考生没有作弊行为，考试只看最后生成的结果。

1.1.3 RHCE 认证考试

RHCE 认证考试是为了测试考生配置物理服务器或虚拟服务器的能力，要求在其上配置如 Apache、vsFTP、网络文件系统(NFS)、Samba、Postfix 邮件服务、远程登录以及其他功能的网络服务。此外，还测试考生对安全增强 Linux(security enhanced Linux, SELinux)、防火墙、网络连接及其他功能等复杂配置选项的处理能力。从根本上说，如果考生通过 RHCE 考试，则人事部门经理会确信该考生具有管理他们企业中的 Linux 系统的资格。

RHCE 考试时间为两个小时。考试一开始就要求考生在一个真实的 RHEL 系统上执行操作。与 RHCSA 一样，对系统所做的任何修改都必须能够在系统重启后保留下来。在任何情况下，考生是用 nano 编辑器还是 GUI 工具来配置相关的配置文件并不重要。只要考生没有作弊，则只看生成的结果。

Red Hat 培训课程中介绍的少许内容已超出 Red Hat 考试课程大纲的要求。虽然这些内容目前还不是考试范围内，但它们可能会出现在未来的 Red Hat 考试中。

1.1.4 如果只准备参加 RHCSA 考试

众所周知，Red Hat 偶尔会对考试要求做微小的修改。未来的修改要以 Red Hat Rapid Track 课程，即 RH199/RH200 的大纲为基础。因此，如果你不是在最近几个月里参加 RHCSA 考试，则要注意这个课程的大纲，实际上它很可能反映出未来 RHCSA 考试的趋势。

1.1.5 不断演变的要求

Red Hat 考试的要求也在不断发生变化，这从 RHCT 与 RHCSA 之间的差异就可以看出，也可以从考试的形式上看出考试的变化，例如不再要求在裸机上安装系统。事实上，这个变化经过两年后才在 RHEL 5 中使用。在 RHEL 发布的第一个月里变化发生。因此，如果你要准备 RHCSA 或 RHCE 考试，需要注意相关考试的考试目标。此外，Red Hat 通过 WordPress 博客发布网站 <http://redhatcertification.wordpress.com/> 上发布公告宣布删除考试中有关独立故障排除的内容。

认证目标 1.02 基本的硬件要求

现在开始详细介绍 Red Hat 企业版 Linux 的硬件配置。尽管现在有些制造商继续保留自己的 Linux 驱动程序，但是大多数 Linux 硬件支持来自于第三方志愿者的工作。幸运的是，Linux 用户形成了一个巨大的社区，其中的许多人为 Linux 系统开发了驱动程序，并发布在 Internet 上供大家免费使用。当某个硬件开始流行时，对该硬件的驱动支持肯定会在 Internet 上的某个地方出现，而且将会集成到 Linux 的各个不同版本中，其中包括 RHEL。

1.2.1 硬件兼容性

如果你只有一个 32 位的系统，则需要花些钱。KVM 是 RHEL 6 默认的虚拟机解决方案。Red Hat 将其配置为只能在 64 位系统上运行。幸运的是，当今市场上销售的大多数 PC 机和服务器都属于 64 位系统。即使是慢速的 Intel i3 CPU 也可以运行 64 位操作系统。在笔记本电脑中甚至使用 Intel Atom CPU 的 64 位版本。对于来自 Advanced Micro Device 公司的 CPU 也有类

似的对比。

在为 Linux 系统购买新机时要小心。虽然 Linux 在最近几年里已取得很大的进展，而且在当今绝大多数的服务器和 PC 机上安装 Linux 系统也不会存在问题，但是你还是不要理所当然地认为，Linux 可以安装在任何计算机上或者在任何系统上都可以完美无瑕地运行。对于目前最新的手提电脑，更不要有这种假设(你要参加 Red Hat 考试必须准备一个 64 位的系统)。手提电脑经常使用专用配置，使得它只有经过逆向工程才能使用 Linux。例如，当我在一台 2010 年生产的名牌商用手提电脑上安装 RHEL 6 时，必须做一些额外的工作才能使它的无线网卡在 RHEL 中正常工作。

服务器或 PC 机的体系结构决定了系统使用的组件及它们之间的连接方法。换言之，体系结构不仅仅描述了 CPU 的细节，还包括了对硬盘、网卡、键盘、图形显示卡等其他硬件的标准。所有软件都是针对某个特定计算机体系结构而设计的。

即使某个制造商基于一种 CPU 开发了一个设备，但是它可能在 Linux 中无法工作。因此，重要的是要知道一个计算机的体系结构。从严格意义上说，如果你想知道自己的硬件是否与 Red Hat 相兼容或者是否得到 Red Hat 支持，则要查看 <http://hardware.redhat.com/hcl/> 上的硬件兼容列表。

考试提示

虽然有必要知道 Linux 与硬件交互的方式，但是 Red Hat 考试并不属于硬件考试。在 RHCE 考试目标中除了有 Internet 小型计算机系统接口(Internet Small Computer System Interface, iSCSI) 内容外，Red Hat 考试目标与硬件内容都没有直接关系。但为了练习考试内容，你需要安装 RHEL 6。为了配置一个 KVM 系统(它要求硬件支持的虚拟技术)，你需要一个 64 位的 CPU 和相关硬件的系统。

1.2.2 体系结构

虽然 RHEL 设计时已考虑到各种不同的体系结构，但是为了参加 RHCSA 和 RHCE 考试，你最好还是把重点放在 Intel/AMD 64 位或 x86_64 体系结构上。在编写本书的期间，这些考试只能在上述 CPU 的计算机上进行，因此考生无须担心与体系结构有关的问题，如专用的引导程序或者 64 位模块目录。虽然如此，定制化的 Red Hat 可以适用于各个不同的平台。

你可以在各种不同 CPU 的计算机上安装 RHEL 6，但是必须记住，为了测试一个系统是否满足 KVM 虚拟解决方案的条件，必须有一个 64 位的系统。Red Hat 支持以下 4 类不同的 CPU 体系结构：

- x86(32 位)
- Intel/AMD64(x86_64)
- IBM Power Architecture(64 位)
- IBM System Z Architecture

上述列表忽略了一项重要的内容。Red Hat 并没有为 Intel 安腾 CPU 提供 RHEL 6。为了确定系统的体系结构要执行以下命令：

```
# uname -p
```

如果你打算在 RHEL 6 上配置虚拟机，则必须选择支持硬件辅助虚拟技术(hardware-assisted virtualization)的体系结构以及启动硬件辅助虚拟技术的基本输入/输出系统(BIOS)或者通用可扩展固件接口(Universal Extensible Firmware Interface, UEFI)菜单选项。支持硬件辅助虚拟技术的配置文件在/proc/cpuinfo 文件中设置 vmx(Intel)或 svm(AMD)标志。

注意，不支持在 32 位系统上使用 UEFI 菜单安装 RHEL 6。

实际经验

如果你无法确定自己的系统属于哪个体系结构，则可以在商店里用发行的一个 CD 进行测试。经商店人员的允许后可以用 Live CD(或 DVD)启动系统。启动后，就能够通过命令行模式访问/proc/cpuinfo。你可能还要对 BIOS 或 UEFI 菜单稍作修改。如果一个系统已配置为支持硬件辅助虚拟技术，则在这个文件中肯定有 vmx 或 svm 标志，即使从 Live CD 发行版读取这个文件也是一样。

1.2.3 内存要求

虽然在较小的内存里也能运行 RHEL 6，但是 RAM 内存要求是由 Red Hat 安装程序的需要来确定的。对于基本的基于 Intel/AMD 的 32 位或 64 位系统，Red Hat 官方要求 512MB 的内存，但是建议每个系统至少要有 1GB 的内存。然而我曾在一个内存远小于此的 VM 上安装了 RHEL 6。在没有安装 GUI 的虚拟机里，甚至 200M 的内存都用不上。

当然，实际内存需要取决于在系统上可能同时运行每个程序的负荷。这包括了任何可能运行在物理 RHEL 6 系统上虚拟机所需要的内存。实际上不可能使用最大内存，因为理论上在 RHEL 6 里可以配置 128TB(即 128 000GB)的内存，但是这只是理论上而已。在 RHEL 系统上 Red Hat 所支持的最大内存是，32 位系统为 16GB，64 位系统为 2TB。

实际经验

如果你把 Linux 配置为服务器，则随着登录到此服务器的用户数量的增加内存需求也随之增加。在同一个系统上运行几个不同的虚拟机，情况也是如此。然而在配置了不同功能的虚拟机上，系统管理员通常会“超额预订”(overbook)内存。

1.2.4 硬盘选项

在计算机加载 Linux 之前，BIOS 或 UEFI 必须能够识别硬盘上的活动主分区，这个分区应该保存有 Linux 引导文件。这样，BIOS 或 UEFI 才可以配置并初始化这个硬盘，然后加载活动主分区上的 Linux 引导文件。有关硬盘和 Linux，你必须知道以下事实：

- 当今的计算机上可安装的硬盘数量已经增加。由于得到端口倍增技术的支持，很容易在一个系统上配置 16 个串行高级技术插件(Serial Advanced Technology Attachment, SATA)，前提是系统能够安装下这么多的硬盘。
老式的 PC 机只能安装 4 个并行高级技术插件(PATA)驱动器。
- 如果系统具有小型计算机系统接口(Small Computer System Interface, SCSI)，则系统可以最多安装 31 个不同的 SCSI 硬盘驱动器。

- 虽然可以按硬件最大的允许值安装 PATA、SATA 或 SCSI 驱动器，但是来自/boot 目录中的 Linux 引导文件只能引导前两个硬盘驱动器。如果 Linux 系统安装在后面的硬盘上，则需要能够被 BIOS/UEFI 识别的其他引导介质，如 USB 或 CD/DVD。(Red Hat 不再为引导软盘创建一个映像)。
- RHEL 6 甚至不需要安装在本地硬盘上。在安装过程中，专用存储设备选项支持使用存储区域网络(Storage Area Network, SAN)、直接访问存储设备(Direct Access Storage Devices, DASDs)独立冗余、磁盘阵列(Redundant Array Of Independent Disk, RAID)等。

1.2.5 网络连接

由于最初将 Linux 设计为 Unix 的克隆，因此它保留了 Unix 作为网络操作系统的优点。但是并非每个网络组件都适用于 Linux 系统。许多无线网络设备的制造商并没有推出相应的 Linux 驱动程序。很多时候，Linux 开发人员努力开发出合适的驱动程序并把它们嵌入到主要版本里，包括 RHEL。

1.2.6 虚拟机选项

正如虚拟技术使我们更容易建立多个系统，它也同样可以帮助我们配置很多个系统，每个系统专用于某个服务。为此，虚拟技术可以分为 5 类。这在前面已经提到的 *Security Strategies in Linux Platforms and Application* 一书曾论述到：

- **应用层(Application-level)** 如 WINE(Wine Is Not an Emulator)系统，它支持单个应用程序的安装。此时 WINE 允许在 Linux 系统安装专为微软 Windows 设计的程序，从广义上讲，这就是在虚拟机里配置一个应用程序的例子。
- **平台层的虚拟机(Platform-level VM)** 如 VMWare Player 和 Virtualbox 等应用程序，它们是平台层虚拟机的几个开源版本示例。为了安装一个不同的操作系统，它们对整个计算机系统进行仿真。
- **准虚拟技术(Paravirtualization)** 虽然在功能上它与平台层虚拟机相似，但是它需要较少的资源，而且通常需要如 Xen 那样的专用内核。
- **硬件辅助虚拟技术** 虚拟机通过硬件接口访问 CPU 的硬件功能，如前面曾提到的/proc/cpuinfo 文件中的 vmx 或 svm 标志。
- **裸机虚拟技术** 有些虚拟机系统包含一个虚拟机操作专用的最小操作系统。裸机虚拟技术的两个例子是 Vmware ESX 和 Citrix XenServer。

配置 RHEL 6 的 KVM 解决方案可以被看成为一个超级监管者，即一个支持在同一个 CPU 同时运行多个操作系统的 VM 监视器。KVM 替代了之前的默认设置 Xen。

实际经验

在很多开源的 Linux 版本里，KVM 已取代了 Xen。XenSource 属于 Citrix 公司，该公司自 RHEL 5 发布后就开始与微软合作。

认证目标 1.03 获得 Red Hat 企业版 Linux

RHCSA 和 RHCE 考试要测试考生 RHEL 的知识。当考生参加 RHCSA 或(与)RHCE 考试时，要在一台标准的 64 位计算机完成操作。为了获得 RHEL 的官方版本，你要向 Red Hat 订购。有时也可以使用试用版。但是，如果你准备考试时不需要 RHEL 考试的相同外观，也可以使用第三方的重构版本。这些重构版本使用与 RHEL 相同的源代码。除了商标和 Red Hat 网络外，它们在实际功能上与 RHEL 完全相同。

当你订购了 RHEL 或者获许使用 RHEL 的一个评估版本后，可以从 Red Hat Network(RHN)的 <https://rhn.redhat.com> 上下载 RHEL 6 版本。从这个网址上还可以下载一个网络引导光盘。甚至可以下载相关软件包的源代码。这些下载文件都是 ISO 格式，即其文件扩展名为.iso。可以使用 K3b、Brasero 甚至微软的相应工具把这些文件刻录到光盘上。或者安装一个虚拟机程序，虚拟 CD/DVD 驱动程序硬件由此直接指向 ISO 文件，这些内容将在第 2 章里介绍。除非你购买了正版光盘，否则刻录或使用这些 ISO 文件的工作要由自己来完成。

注意，本章这部分介绍的一些安装选项分散到几个不同的章节里，例如用 Red Hat 的 Disk Druid 工具配置分区的方法分散到多个小节里。

实际经验

ISO 是一个映像文件，它可以刻录到 CD/DVD 光盘上。这个名称的首字母缩写符不重要，因为它是基于政治上的妥协。

考试提示

虽然如何获得 RHEL 很重要，但是它不属于 RHCSA 和 RHCE 考试目标。

1.3.1 购买预订版本(subscription)

Red Hat 为台式机和服务器提供了不同的订阅模式。虽然 RHCSA 主要用于工作站，但是它也需要配置 HTTP 和 FTP 服务器。当然，RHCE 还要求配置各种服务器服务。因此，大多数读者需要一个服务器订阅模式。

服务器也有很多不同的订阅模式，这取决于 CPU 槽数和虚拟机客户端数量。安装了一个普通的 RHEL 订阅模式的系统只限于两个 CPU 槽和一个虚拟客户机。每个槽可以安装一个多核的 CPU。对于学术领域里的用户可以提供折扣。

1.3.2 获得评估版本

Red Hat 目前为 RHEL 提供一个 30 天试用期的评估版。Red Hat 要求这些用户必须提供一些个人信息。得到 Red Hat 的批准后就会从 Red Hat 得到如何下载 RHEL 版本的提示。更多的信息可以查看 www.redhat.com/rhel/details/eval 网页。这个 30 天的限制是指用户的系统与 Red Hat Network 之间访问的时间限制。过期后用户的 Linux 操作系统可以继续运行，但是无法得到更新，也没有后续支持。

1.3.3 第三方重构版本

为准备 Red Hat 考试并不一定要付费购买一个 Linux 操作系统，也不一定要使用受限制的订阅模式。为了遵循 Linux 的通用公共许可(General Public License, GPL)规定，Red Hat 通过 ftp.redhat.com 网址公开了每个 RHEL 软件包的源代码。然而，GPL 只要求 Red Hat 发布其源代码，它并没有要求 Red Hat 公开由这些源代码编译生成的二进制软件包。

实际经验

本书中对 GPL 和商标的描述并不出于法律方面的考虑，因此不能作为法律上的依据。

在商标法保护下，Red Hat 可以阻止其他人用它的商标(如红色的 Fedora 符号)发布软件。尽管如此，GPL 允许任何人编译源代码。如果他们要修改源代码，则他们只需要在同一个许可协议下发布自己的修改。几个第三方机构就是利用这个机会从发布的源代码中删除 Red Hat 商标，再对源代码进行编译得到重构版本，其功能与 RHEL 一样。

源代码以 Source RPM 软件包的格式发布，这意味着 RPM 包可以用 rpm 命令生成，此命令将在第 7 章介绍。然而，生成一个发布版本即使是从源代码编译生成也是一个比较困难的过程。但是一旦完成后，重构版本的功能与 RHEL 相同。不错，重构版本无法连接到 Red Hat Network，也无法从它那里得到更新。然而，Red Hat Network 不是 Red Hat 考试培训课程的一部分，而且重构版本的开发人员也可以利用与新 RHEL 软件包相关的源代码来确保自己的程序库及时得到更新。重构版本有两个选项：

- **社区企业操作系统**(Community Enterprise Operating System, CentOS) 被称为 CentOS 的重构版本是由几个经验丰富的程序员开发的，他们自 2002 年 RHEL 3 发布以来一直在开发 RHEL 源代码。详细情况可以浏览 www.centos.org 网站。
- **Scientific Linux** 该发行版是由美国政府的费米实验室和欧洲原子能组织(CERN)的专家们开发并得到他们的支持。这两个机构的相关人员是一些智商很高的科学家。更多的信息可以浏览 www.scientificlinux.org 网站。

实际经验

本书中的许多图片来自于 Scientific Linux 的屏幕截图，它是由 RHEL 6 的源代码生成的。此版本是这两个机构里的一些 Scientific 家开发的，这两个机构拥有世界上最卓越的科学家。

1.3.4 检查下载的文件

所有来自 RHN 网上的下载文件，Red Hat 都提供了校验码。这些校验码根据消息摘要 5(Message Digest 5, MD5)和 256 位安全散列算法(256 Secure Hash Algorithm, SHA256)生成的。可以用 md5sum 和 sha256 命令检查这些给定校验码的 ISO 文件的正确性。例如，下面的命令计算这个最早的 RHEL 6 DVD 的校验码。

```
# md5sum rhel-server-6.0-x86_64-dvd.iso
# sha256sum rhel-server-6.0-x86_64-dvd.iso
```

虽然下载的 DVD 通过这些测试是一件好事，但是这个结果不能保证这样的 DVD 没有错误。

认证目标 1.04 安装要求

根据 Red Hat 认证的博客，Red Hat 现在为认证考试提供了预安装的系统。因此，考生不需要从零开始，至少这个主机物理系统不是从零开始。但是考生需要设置一个练习系统。RHCSA 目标要求考生通过网络安装设置一个练习系统。在预安装的系统里，在给定其他要求的情况下，这意味着考生需要知道如何在基于 KVM 的虚拟机上执行网络安装。

本节介绍的安装要求适合于创建一个实验室的练习环境。此环境也可以作为其他 RHEL 系统的基线。在许多实际网络里，新的虚拟系统总是由基线生成或克隆过来。然后这些新系统专用于单个服务。

如果你要建立一个专用于测试虚拟机的物理主机系统，则必须有足够的空间保存一个主机物理系统和客户端虚拟机。本节建议你要建立 3 个用于测试的虚拟机。你可以考虑增加第 4 个虚拟机作为备份，当某个虚拟机由于某个错误或某故障而无法正常工作时，可以使用这个备份虚拟机。对于上述系统 80GB 的硬盘空间就足够了。经过精心计算，更少的磁盘空间和仅两个虚拟机也能应付。有关在虚拟机上配置 RHEL 6 的信息可以参考第 2 章。

实际经验

由于 Linux 文件系统的效率非常高，因此磁盘空间存储接近于最大容量，而且磁盘重组最小化。如果在微软格式的分区上配置一个虚拟机，则由于磁盘空间的碎片问题需要占用很大的额外空间。

1.4.1 不需要从零开始

在安装 RHEL 之前，回顾一下有关 RHCSA 和 RHCE 认证考试的最新信息是很有必要的。正如它在 <http://redhatcertification.wordpress.com/> 网站中所述，Red Hat 现在提供了：

- 预安装的系统；
- 电子化考题；

换言之，当考生坐下考试时，测试系统已安装好一个 RHEL 6 版本，并且以电子格式提供考试内容。至于问题的格式没有使用公开的信息。本书假定 Red Hat 考试的问题使用最基本的格式——即出现在 root 系统管理员的主目录(/root)的文本文件。

1.4.2 网络安装的优点

网络安装意味着在安装 RHEL 6 时不必为每个系统都使用整个 DVD 光盘。这意味着所有系统采用同一个安装包的安装模式。网络安装比起通过物理的 DVD 安装要快许多。

当网络安装与 Kickstart 文件(启动文件)和预引导执行环境(Pre-boot eXecution Environment, PXE)相结合时，则表现出特别强大的功能。在这种配置中，安装 RHEL 6 的全部工作只需要启动一个系统，然后把远程安装程序链接到合适的 Kickstart 文件，就这么简单。几分钟后，就得到一个完整的 RHEL 6 系统。

1.4.3 Red Hat 与虚拟机

RHCSA 考试的目标是要求考生“掌握物理机器的配置方法，使它可以寄宿虚拟客户机”。此外，它还建议“考生知道如何在虚拟机上执行众多的操作”，以及如何用启动文件(Kickstart)实现 RHEL 操作系统的自动安装。这与用启动文件在基于 KVM 的虚拟机上安装 RHEL 6 的方法相一致。

虚拟机的优点之一是它支持在虚拟的 CD/DVD 驱动器上使用 ISO 文件。对虚拟驱动器的文件访问速度不会受到物理 CD/DVD 驱动器的机械速度的影响。由于这种访问也不会受网络流量的影响，因此虚拟 CD/DVD 驱动器与主机系统对网络访问的速度一样快。

1.4.4 虚拟系统与物理系统

虚拟系统不能独立存在，它们需要连接到一个物理系统。即使像 VMware ESX 和 Citrix XenSource 这样的“裸机”虚拟技术解决方案也要由 Linux 内核编译生成，否则要依赖专用版本的 Linux 内核，此内核作为物理主机的操作系统。

然而，在单个物理系统上可以安装多个有效的虚拟系统。如果这些系统都致力于不同的服务，则它们会在不同的时刻加载到物理系统里。这样的加载方法很可能会“超额预订”了物理系统的内存和其他资源。

对考试来说，在物理系统还是在虚拟系统上执行安装并没有本质的区别，软件的功能还是一样。只要启用物理主机系统里的 IP 转接功能，则虚拟系统上的网络连接也采用同一种模式。

1.4.5 练习使用的预安装环境

本章配置的基线 RHEL 系统相对比较简单。它从一个 12GB 的虚拟硬盘上启动。这个硬盘部分空间的目录结构如表 1-1 所示。我们把它们配置为普通分区。这个硬盘的其余空间都还没有使用，在考试过程中需要把它配置为逻辑卷。

表 1-1 模型的分区表

位 置	大 小
/boot	500MB
/	8GB
/home	1 024MB
交换空间(Swap)	1 024MB

为了便于逻辑卷安装之后的配置，系统还包括另外两个 1GB 的虚拟硬盘。12GB 的硬盘空间和 8GB 的分区为 PVUFRHEL 6 软件提供了足够的空间。如果你的硬盘空间有限，最小可以使用 8GB 的硬盘，只是交换空间也要受到限制。Linux 里的交换空间是本地 RAM 的扩展，特别当系统资源不够时尤其如此。

RHEL 6 的最小基线安装模式并没有包括一个 GUI 工具。虽然在安装结束之后安装与 GUI 有关的程序组很容易，但是此过程需要安装多达几百 MB 的程序包，而且费时不少。为了在考试中节省时间，Red Hat 已经为考生提供了一个预安装系统，因此可以认为 Red Hat 提供的系统包括了 GUI 软件包。Red Hat 系统的默认 GUI 工具是 GNOME 台式环境(GNOME Desktop

Environment)。

实际经验

GNOME 是一个缩写符，但是它又包含在另一个缩写符中。它是 GNU 网络对象模型环境的首字母缩写符(GNU Network Object Model Environment)。GNU 本身又是一个递归形式的缩写符，它代表 GNU's Not Unix。Linux 系统有很多类似的递归缩写符，如 PHP，它代表 Hypertext Preprocessor。

内存空间的分配比较复杂，特别是虚拟机上的内存空间。在本书里，我们给虚拟机分配了 768MB 的内存空间，这足以启动 RHEL 安装过程的 GUI 图形演示。如果采用文本模式的安装过程，可以在 512MB 内存甚至更少的内存空间里运行 RHEL 6 GUI。由于不同的虚拟机很少同时使用同样大小的内存，因此我们总是“超额预订”内存空间。例如，在一个物理内存小于 3GB 的宿主物理机上我们可以建立 3 个虚拟机，且每个分配的内存空间为 1GB。虚拟机上的部分内存可能还没有使用，但是可以供物理宿主系统使用。

1.4.6 系统角色(System Role)

在理想情况下，你建立多个系统，每个专用于不同的角色。一个网络使用专用 DNS(Domain Name Service)服务器、专用的 DHCP(Dynamic Host Configuration Protocol)服务器以及专用的 Samba 文件共享服务器等，它就会更安全。此时，一个系统的安全受到威胁也不会影响其他服务。

但是，这是不现实的，特别是在 Red Hat 考试里。表 1-2 列出实验室 1 里 3 个系统各自的角色。

表 1-2 测试系统的各个角色

系 统	角 色
server1	本书中用到的工作站和服务器，配置为 192.168.112.0/24 网络上的 server1.example.com 的域名。本书假定它的固定 IP 地址为 192.168.122.50
tester1	安全 Shell(Secure Shell)服务器，它支持远程访问，配置为 192.168.122.0/24 网络上的 tester1.example.com 服务器。它可能还包括用于客户端测试的服务器，如域名服务(DNS)。本书假定它的固定地址 IP 地址为 192.168.122.150
outsider1	使用第三个 IP 地址上的工作站，它的域名配置为 outsider1.example.org。有些服务不允许从该工作站访问。本书假定它的固定 IP 地址为 192.168.100.100

在此网络里还隐含着第 4 个系统，即用来寄宿虚拟机的物理主机。当需要配置多个网络时，此主机用虚拟网卡连接到其他网络。本书建立了一个名为 maui.example.com 的系统。下面这段信息来自于 ifconfig 命令的执行结果，它显示 virbr0 和 virbr1 这两个网络适配器，它们分别连接到两个网络：

```

virbr0 Link encap:Ethernet HWaddr 9E:56:D5:F3:75:51
      inet addr:192.168.122.1 Bcast:192.168.122.255 Mask:255.255.255.0
virbr1 Link encap:Ethernet HWaddr 86:23:B8:B8:04:70
      inet addr:192.168.100.1 Bcast:192.168.100.255 Mask:255.255.255.0

```

当然，你可以改变每个系统的域名和 IP 地址，它们只是本书使用的默认值。server1.example.com

是指定的考试系统，用于解决实际 Red Hat 考试要求时的练习。为方便起见，我还在物理主机系统上建立了几个 RHCE 服务。

tester1 系统将用来验证 server1 系统上的配置。例如，如果我们已经用不同的名称配置了两个虚拟网站，则从 tester1 系统应该能够访问这两个网站。Red Hat 考试假定考生把一个系统作为客户端连接到 Samba 和 LDAP 等服务器。此外还假定一个 DNS 服务器已配置了合适的主机名和 IP 地址。虽然，Kerberos 等服务器的配置已超出 RHCSA /RHCE 考试的范围，但是在考试中其他系统可能作为客户端访问这些服务器。

最后，outsider1 系统实质上相当于 Internet 等外部网络的一个随机系统。已给 server1 服务器上的某些服务设置适当的安全参数，因此 outsider1 不能访问这些服务。

如前所述，最好有第 4 个虚拟系统，万一这里 3 个虚拟系统的某一个无法正常工作。在按这里的要求配置之前阅读第 2 章内容。本章主要介绍物理主机系统的配置。

认证目标 1.05 安装选项

即使是 Linux 初学者也可以用 CD/DVD 安装 RHEL 6。虽然本节讨论和安装有关的一些选项，但是重点却放在基线系统的创建。建立基线系统后，它可以用这个基线系统建立其他自定义 RHEL 6 系统。

此外，安装过程也是一个深入学习 RHEL 6 的好机会。安装结束后，引导介质和逻辑卷都需要重新配置。但是由于预安装的物理系统现在是 Red Hat 考试的规范方式，因此有关逻辑卷的详细讨论在第 6 章里。

本节介绍的步骤假定，实验题 2 建立和配置的 RHEL 6 安装文件已与 FTP 服务器建立连接。如果你直接从完整的 DVD 安装 RHEL 6，则步骤会不一样。

1.5.1 引导媒介

在安装 RHEL 6 时，最简单的办法是直接从光驱启动 RHEL 6。虽然重构版可能会提供 CD 盘，但是只有 Red Hat 提供 RHEL 6 DVD 盘。它也提供 ISO 格式的引导媒介。有了这些媒介，就不用考虑独立的引导盘，也不用担心网络连接。但是某些机构不会把 RHEL 6 DVD 光盘发送给每个用户。有时，系统根本就没有 CD/DVD 驱动器。从本质上说，共有 4 种方法启动 RHEL 6 安装过程：

- 从 RHEL 6 DVD 盘引导
- 从网络上的 RHEL 引导 CD 盘引导
- 从 USB Key 引导
- 利用 PXE 网络引导卡从 Kickstart 服务器引导

后面三种方法一般都假定从网络上安装 RHEL。已购买了订阅版本的用户可以使用 Red Hat 网络上的安装程序和引导媒介。重构版本的发行者也会提供服务器供用户安装。

有些 Red Hat 文档认为，网络引导 CD 盘不适用于 64 位的、带 UEFI 接口的系统。我认为，这不是真实的。它在我的基于 UEFI 手提电脑和服务器上都能正常工作。更多的信息可以阅读 Red Hat Bugzilla 661135 文档。虽然如此，如果你需要建立一个引导 USB Key，则必须在 RHEL

6 DVD 盘里 images/子目录下找到 efidisk.img 文件，然后把这个映像文件写入到 USB key 里。如果此 USB key 安装在/dev/sdd 设备上，则用下面的命令写入此映像：

```
# dd if=efidisk.img of=/dev/sdd
```

注意，如果/dev/sdd 驱动器里有数据，则这个命令会覆盖这个驱动器中的全部数据。

实际经验

必须知道如何为自己的系统创建一个启动盘。当系统出现故障时，安装启动盘或 USB Key 可以当作急救盘使用。在引导提示符后，Rescue Installed System(急救安装系统) 选项最终把系统带到急救模式，后者会自动挂载正确的卷并恢复受损的文件或目录。

1.5.2 用 CD/DVD 或引导 USB 启动安装

现在你可以通过网络引导 CD 盘、DVD 安装盘或安装 USB Key 启动一个目标系统。当系统打开并解压几个文件后就会出现 RHEL 安装屏幕，并至少有以下 4 个选项：

- 安装或升级现有的系统(Install or upgrade an existing system);
- 用基本的视频驱动程序安装系统(Install system with basic video driver);
- 修复已安装的系统(Rescue installed system);
- 从本地驱动器引导(Boot from local drive)。

第一个选项适用于大多数用户。如果选择第一个选项后图形显示出现问题，则要重新启动系统并选择第二个选项。第二个选项指定在老式 SVGA(Super Video Graphics Association)监视器上使用 VESA(Video Electronics Standard Association)适配器。

与 Red Hat 安装程序(或称为 Anaconda)有关的还有两个模式：文本模式和图形模式。虽然图形模式最小需要 512MB 的内存，但是在稍微小一些的内存里也可以选择图形安装模式。但是，如果内存足够而且喜欢文本安装模式，则要返回到 RHEL 安装屏幕，高亮显示 Install Or Upgrade An Existing System 选项，然后按 Tab 键，就会出现以下一行内容：

```
> vmlinuz initrd=initrd.img
```

强制执行文本安装模式，需要在这行代码的末尾加上 text 单词。

实际经验

虽然 Red Hat 公开发布的资料建议图形模式安装至少需要 512MB 的内存，但是在 KVM 机上的实验表明，在 VM 机上执行 GUI 安装至少需要 652MB 内存。

1.5.3 基本的安装步骤

基本 RHEL 的安装过程很简单，任何参加 Red Hat 认证考试的考生都应该对此了如指掌。这里介绍的大多数步骤只作为参考，重要的是要掌握第 2 章介绍的高级配置的安装过程，即使用 Kickstart 文件的安装过程。

这些步骤的顺序也不是一成不变的，取决于是从 CD/DVD 启动还是从网络启动。本地系统是否已安装了 Linux 以前版本、是否有 Linux 格式化的分区等都会影响安装步骤的顺序。在本

节里，我们这样假定：

- 通过 RHEL 6 网络引导盘启动网络安装。
- 系统的内存至少为 652MB。
- 可以访问保存有安装文件的 FTP 服务器，如 Lab 2 配置的 FTP 服务器。
- RHEL 6 是本地计算机上的唯一操作系统。

但是，双引导是允许的。事实上，我编写本书所用的 Intel I7 手提电脑就是一个三引导共存的系统，即 RHEL 6 系统与 Windows 7 系统和 Ubuntu 10.04 系统共存。如果你是在一个专用的物理机上或虚拟机上安装系统，则基本的步骤是一样的。作为虚拟机需要一个物理主机，我假设先在物理系统上安装 RHEL 6 系统。

最有效也是最可靠的办法是，从远程服务器上用文本模式或图形模式安装 Red Hat 企业版 Linux。为此，本章的 Lab 2 配置了一个 FTP 服务器，它保存了 RHEL 6 安装文件。也可以在 Apache 等 HTTP 服务器上创建这些安装文件，这要在本章的后面介绍。

安装过程中的安装步骤顺序并不是都一样。其顺序与是从 DVD 启动安装还是从网络安装 CD 启动都有关，也与文本安装模式或图形安装有关，甚至与是否使用 RHEL 6 的重构发行版有关。事实上，下面这些操作说明相当于两种不同安装方法的混合，这具体取决于步骤 2 的选择。事实上，重构发行版的开发人员也会对安装步骤稍作修改。你实际看到的安装过程可能会与这里的有很大区别。因此对下面的操作指令必须灵活使用：

(1) 用 RHEL DVD、RHEL 网络引导 CD 或引导 USB Key 启动自己的计算机。这里我们假设通过网络引导 CD 启动。通常出现 5 个选项：

- 安装或升级一个现有系统(Install Or Upgrade An Existing System)
- 用基本的视频驱动程序安装系统(Install System With Basic Video Driver)
- 修复已安装的系统(Rescue installed system)
- 从本地驱动器引导(Boot from local drive)
- 内存测试(Memory Test)

(2) 图 1-1 显示了 Scientific Linux 重构版的选项，它们与真正的 RHEL 6 DVD 的选项相同。安装 RHEL 时，只有前两个选项可以使用。试试第一个选项。如果在安装过程中图形安装模式无法进行，则重启系统。试试第二个选项。

如果首次使用 RHEL 6 安装 DVD 盘，并且想检查第(4)步的选项，则按下 Tab 键，再添加一个空格，在出现的命令行中输入 askmethod 命令，然后按回车键。然而，输入这个命令后，首先以文本形式出现“Choose A Language And Keyboard Type”信息，这将在步骤(9)和步骤(10)中介绍。此外，这个操作会跳过步骤(3)将要介绍的“Disc Found”屏幕。

(3) 系统出现 Disc Found 屏幕。即使有足够的内存可用，网络安装过程的前几个步骤是以文本模式启动的(这实际是属于低分辨率的图形模式)。此时的选项无法用鼠标点击。在这种模式下，用 TAB 键在各个选项之间切换，并用 SPACE 键和 ENTER 键选取或取消一个选项。

(4) 如果愿意，也可以用 Disc Found 屏幕去测试媒介(磁盘)的完整性。如果磁盘通过测试当然很好，但是不能保证这样的磁盘肯定不会出错。如果你选择测试，请注意当测试结束后，磁盘会被弹出。接受测试或者跳过这一步，开始第(5)步。

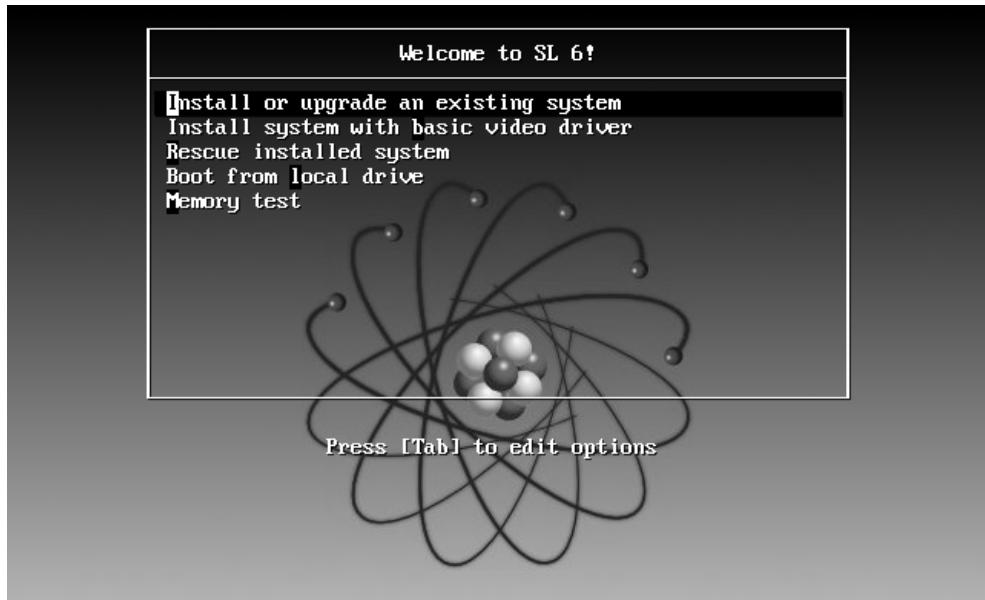


图 1-1 安装过程屏幕上出现的引导选项

如果你要测试在基于 KVM 的虚拟机中用作 CD/DVD 光盘上的 ISO 文件的完整性，则系统会在不改变虚拟机中媒介状态的情况下“弹出”这个文件。你必须中断连接，然后恢复 KVM Detail 屏幕中的媒介，这将在第 2 章讨论。

(5) 选择安装方法。出现如图 1-2 所示的 4 个选项。这些选项都容易理解：

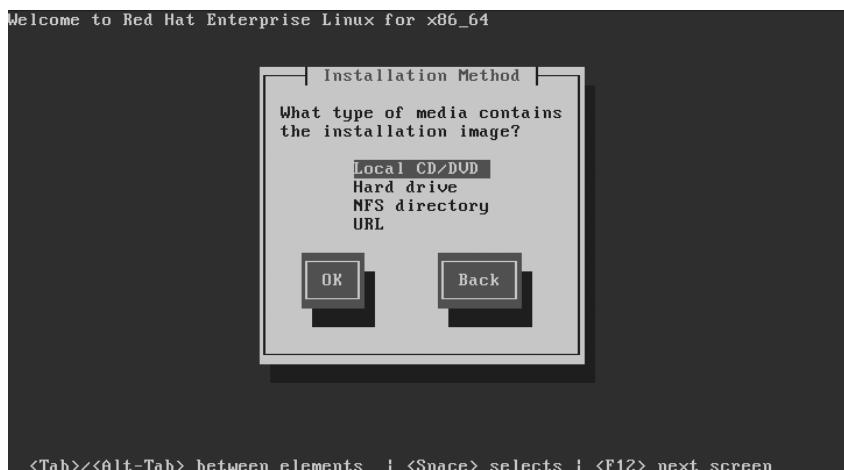


图 1-2 选择一个安装方法

- 如果加载了 CD/DVD(或相应的 ISO 文件)，则可以使用 Local CD/DVD 方法；
- Hard Drive 方法假设 RHEL 6 ISO 文件在本地硬盘的一个分区上可用。如果选择这个选项，安装程序会提示你指定这个文件所在的卷和目录；
- NFS Directory 假定安装文件来自一个共享的 NFS 目录；
- URL，统一资源定位器的简称，要求安装文件保存在一个 Apache 服务器和一个 FTP 服务器上。

考虑到由 Lab 2 配置的 FTP 服务器, 选择 URL 并单击 OK 按钮。

(6) 在如图 1-3 所示的 Configure TCP/IP 屏幕中选择 IP 地址的配置方法。选项要能够支持 IPv4 或 IPv6 地址的 DHCP 客户端模式, (如果家用路由器等网络 DHCP 服务器不支持 IPv6, 则选择 IPv6 的 DHCP 模式会使安装过程变慢)。由于考试系统需要固定的 IPv4 地址, 因此选择 Manual Configuration(至少对于 IPv4 地址是如此)。给表 1-2 所示的三个系统设置固定的 IPv4 地址。不管如何, KVM 目前只支持 IPv4。

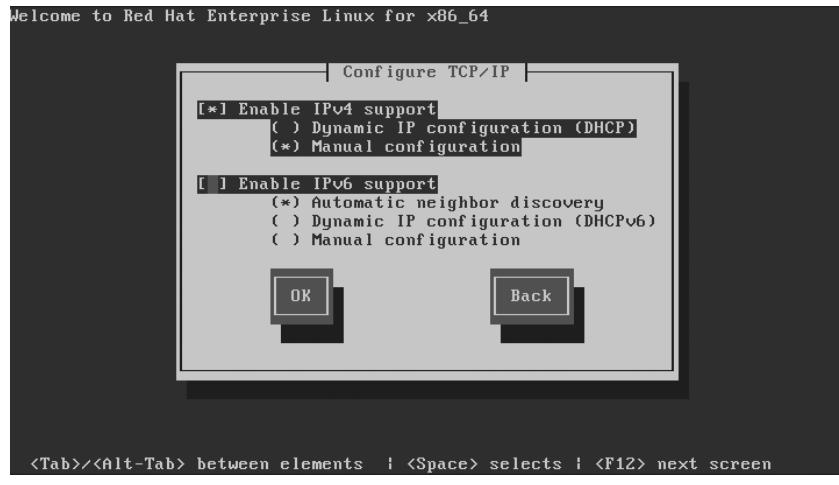


图 1-3 配置网络寻址的类型

(7) 为系统指定一个 IPv4 地址、网关地址和域名服务器。如果你不知道如何下手, 则现在正是一个好时机规划一个 Lab 1 所描述的网络。如果在一个虚拟机配置一个系统, 则网关地址可能是 192.168.122.1 或 192.168.100.1 这样的形式, 它们与 IP 地址在同一个子网中。本书为 server1.example.com 系统指定了 192.168.122.50 IPv4 地址, 而名字服务器即 DNS 服务器的 IP 地址通常与网关的地址相同。或者对于家庭网络里的一个物理系统, 通常把网关和名字服务器的 IP 地址设置为家用路由器的 IP 地址。

(8) 把自己的计算机连接到远程 FTP 服务器。如图 1-4 所示, 输入 FTP 服务器的主机名或 IP 地址以及共享目录。

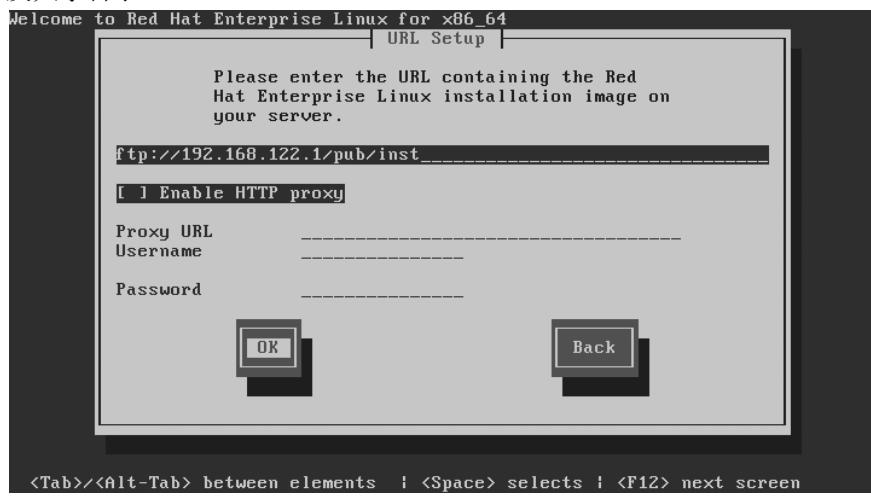


图 1-4 输入安装服务器的 URL 地址

(9) 如果连接成功且安装文件可用，则会看到第一个安装画面。如果计算机的内存足够，则会出现一个图形界面。单击 Next 按钮继续下一步。

(10) 选择安装过程中使用的语言，如图 1-5 所示。默认是英语，有 50 多个不同语言供用户选择。

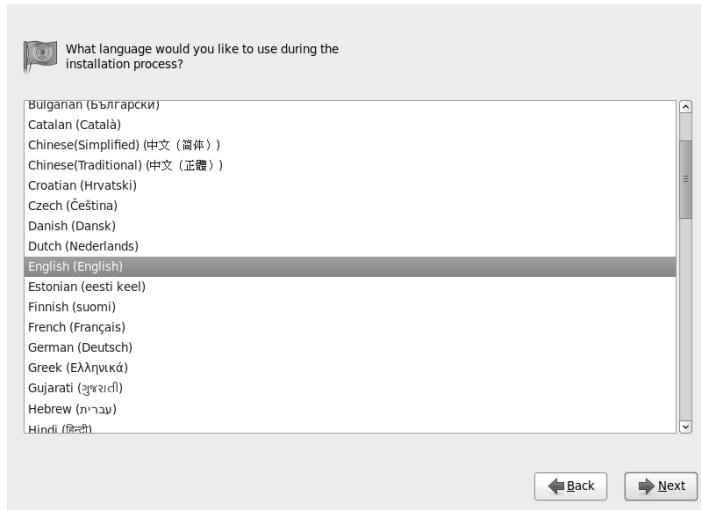


图 1-5 选择安装过程中使用的语言

(11) 选择键盘类型。默认的键盘随所选择的语言而改变。

实际经验

如果安装过程中遇到问题，分析第 3 个、第 4 个和第 5 个控制终端里的消息，按下 Alt+F3、Alt+F4 或 Alt+F5。按 Alt+F2 出现一个命令行。按 CTRL+Alt+F6 返回 GUI 屏幕。如果采用文本安装模式，则要按 Alt+F1 返回这个屏幕。

(12) 下一个界面与本地或专用的存储设备有关。如果你的计算机有一个或多个“普通”本地硬盘驱动器(如 SATA、PATA 或 KVM 系统上的虚拟硬盘)，选择 Basic Storage Device(基本存储设备)并单击 Next。

(13) 如果系统采用多个新硬盘，经询问你是否确认对这些硬盘所做的修改。

(14) 如果自己的计算机中已经安装了 RHEL 的一个早期版本(或者类似的可识别的 Linux 操作系统)，则会看到一个新的安装选项。如果出现这个选项则选中，否则跳过这一步。

(15) 现在要求输入本地系统的域名，如 server1.example.com。单击 Configure Network 打开网络连接工具(将在第 5 章介绍)，有时候在第(6)步配置好的网络参数可能不会出现在这个工具中。做相应的修改并单击 Next 按钮继续。

(16) 现在会出现一个世界地图，选择本系统所在的时区。System Clock Uses UTC 选项是指本地硬件时钟和格林威治时间的原子钟表示。(UTC 是非英语单词的缩写符，该缩写也是基于政治考虑)。虽然与微软的 Windows 不兼容，但是 UTC 选项可以选择夏令时。做适当的修改并单击 Next 继续。

(17) 下一个步骤就是为超级管理员设计口令，需要输入两次。输入口令后，单击 Next 按钮继续。

(18) 下一个步骤是如图 1-6 所示, 确定所配置的本地和远程硬盘空间的使用方案。各个选项在图 1-6 中已解释清楚。现在归纳如下:

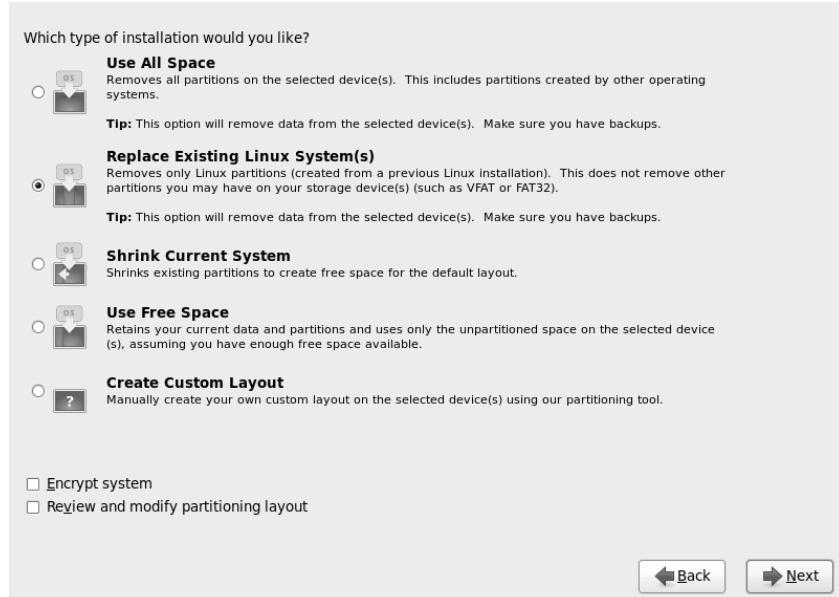


图 1-6 分区规划选项

- **Use All Space**(使用所有空间) 删除所有配置硬盘上的分区, 包括那些由非 Linux 操作系统创建的分区;
- **Replace Existing Linux System(s)**(替换现有的 Linux 系统) 删除全部 Linux 格式的分区, 包括那些由 Linux 其他版本(如 Fedora 和 Ubuntu Linux)创建的分区;
- **Shrink Current System**(缩减当前系统) 考虑到当前可用分区上的未用空间, 压缩这些分区, 压缩后得到的空间可以用于新的安装;
- **Use Free Space**(使用未用空间) 把现有的未用空间用于新安装;
- **Create Custom Layout**(创制定制化的布局) 支持个性化配置, 即在安装过程中使用 Disk Druid、Red Hat 磁盘分区工具;
- **Encrypt system**(加密系统) 对安装过程中创建的分区进行加密。第 6 章将介绍如何对一个现有分区进行加密以及如何对加密分区进行管理。
- **Review and modify partitioning layout**(检查和修改分区的布局) 启动 Disk Druid 工具, 详细内容 1.5.4 节介绍。

在这里我们选择 Create Custom Layout。注意, 这个选项会取消 Encrypt system 和 Review and modify partitioning layout 后面两个选项。单击 Next 继续。

(19) 如果系统安装了多个硬盘, 则选择要安装 RHEL 6 的硬盘。图 1-7 给出了一个示例。本章之前提到的每个基线安装选择 12GB 的硬盘。硬盘的实际大小将显示为多少 MB, 可能相差几个百分比, 这个差异不在 Red Hat 考试范围内。

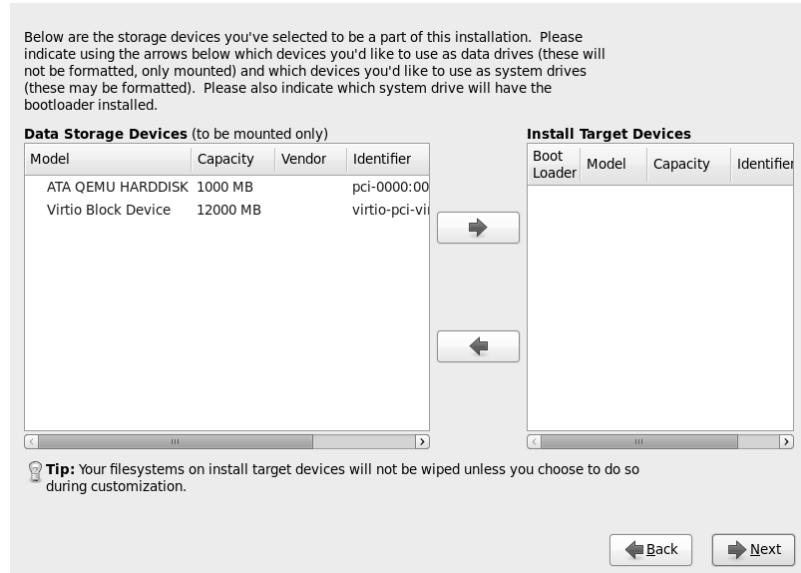


图 1-7 从可用的本地硬盘中选择一个

(20) 此时单击指向右侧的箭头选取 12GB 的硬盘，就会看到 12GB 硬盘出现在右手边的 Install Target Devices 窗口中，单击 Next 继续，看到如图 1-8 所示的 Please Select A Device 屏幕，这是 Disk Druid 工具的主界面。有关这个工具的详细内容将在第 1.5.4 节讨论。

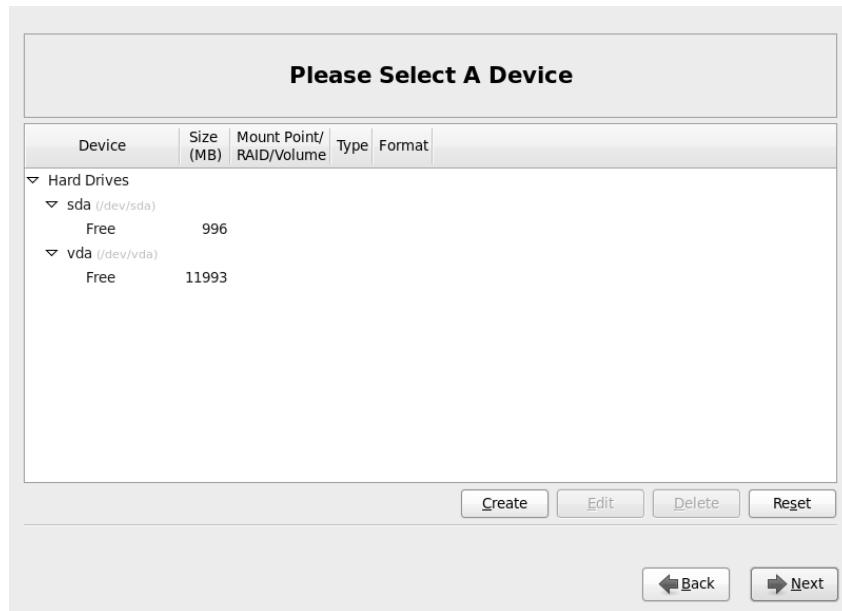


图 1-8 在 Please Select A Device 屏幕中的分区配置

1.5.4 准备在分区上安装

虽然可以创建更多的分区，但是 RHEL 在单个 SATA、SCSI、PATA 或虚拟硬盘驱动器上最多只能识别 16 个分区。创建一个分区后，可以在 Linux 中把一个目录直接挂载到此分区上，或

者把此分区指定为一个 RAID 设备或逻辑卷的一部分。

为定义一个分区，你可能需要有关命名约定、不同文件系统的配置、交换空间的使用、逻辑卷和 RAID 阵列等背景知识。这里只是概括性介绍，详细内容见第 6 章，其中包括 Red Hat 考试以及真实系统需要的操作。

1. 命名约定

Linux 为磁盘分区规定了一个简单的命名标准：3 个字母后跟一个数字。第一个字母表示磁盘的类型(s 表示 PATA、SATA 或 SCSI, v 表示基于 KVM 的虚拟机上的虚拟磁盘)。第二个字母 d 表示磁盘，第三个字母表示这磁盘的相对位置，从 a 开始。例如，第一个 SATA 驱动器为 sda，其后是 sdb、sdc 和 sdd。

后面的数字是根据主分区、扩展分区或逻辑分区的相对位置。主分区上可以包含有操作系统的引导文件。可以把硬盘配置为一个扩展分区，该扩展分区可以包含多个逻辑分区。

硬盘只限于 4 个主分区。如果 4 个主分区不够，可将一个扩展分区当作最后的主分区。此扩展分区然后就可以分割成为多个逻辑分区。因此在规划分区布局时，必须保证扩展分区足够大。

每个分区都与 Linux 设备文件相关联，至少就是这么简单的。例如，第一个 SATA 驱动器上的第一个逻辑分区对应的设备文件名为 /dev/sda5。

卷是一段已格式化的空间的一个通用名字，该空间用于存储数据。卷可以是分区、RAID 阵列或者与逻辑卷管理(Logical Volume Management, LVM)相关联的逻辑卷。

文件系统是卷为保存文件而格式化的方式。例如，Red Hat 使用第四类扩展文件系统(ext4)作为它的卷的默认格式。在 Linux 访问数据的标准方法是先把此文件系统挂载到一个目录。例如，当把 /dev/sda1 分区格式为 ext4 文件系统时，它可以挂载到 /boot 这样的目录。我们经常这样说“把 /dev/sda1 文件系统挂载到 /boot 目录上”。详细内容参见第 6 章。

2. 独立的文件系统卷

通常情况下要为 RHEL 6 创建几个卷。即使在默认配置中，RHEL 至少要配置有 3 个卷：一个是顶级根目录(/)，一个是 /boot 目录，一个是 Linux 交换空间。此外，可能还要为 /home、/opt、/tmp 和 /var 等定义额外的卷。这些卷也适合于网站、专用用户群以及其他任何自定义目录。/boot 目录必须在普通分区上，而其他目录可以配置在逻辑分区或 RAID 阵列上。

按这种方式分割硬盘的可用空间可以保证系统、应用程序和用户文件相互独立。这有助于保护被 Linux 内核文件和其他应用程序占用的磁盘空间。文件不能跨过卷保存。例如，像 Web 服务器这样的应用程序可能要占用大量的磁盘空间，但是不会侵占 Linux 内核占用的空间。另一个优点是，当硬盘上出现坏点，数据受到损坏的风险降低了，修复的时间也减少了，因此磁盘的稳定性得到加强。

虽然创建更多的卷有很多优点，但是这并不总是最好的解决办法。当硬盘空间有限时，分区数必须保持在最小数目。例如，在一个 4GB 的硬盘要安装 3 000MB 的软件包，则一个专用的 /var 或 /home 卷很快会用完磁盘空间。

3. Linux 交换空间

Linux 交换空间通常配置在一个专用的分区上或一个逻辑卷上。它作为当前正在运行的程

序的虚拟内存用来扩展系统的有效内存。但是不可以多购买一些内存并淘汰掉交换空间。即使你的系统有几 GB 的内存空间, Linux 也要把一些不经常使用的程序和数据移动到交换空间。正因为如此, 交换空间的 RAID 阵列是没有多大意义, 谁还会对内存中的碎片进行备份呢?

Red Hat 对交换空间的分配方式取决于内存的大小和本地硬盘上可用空间的大小。对于 2GB 以下的系统, 默认的交换空间为内存空间的 2 倍。对于大于 2GB 的系统, 交换空间为内存的大小加上 2GB。但是这些规则并非一成不变。几 GB 的工作站经常只分配很少的交换空间。在我的家用服务器中, 有 8GB 的内存和 4GB 的交换空间, 该交换空间很少使用。但是在连几个月里都没有重新启动的系统或者总是不断要求某个服务的计算机中, 则可能需要经常使用交换空间。不管如何, 安装过程默认分配的交换空间不在一个专用分区上, 而是作为一个逻辑卷。

4. 有关逻辑卷的基本信息

从一个分区上创建逻辑卷需要以下步骤。这些概念的详细内容以及执行这些步骤的实际命令将在第 6 章中介绍。如果在安装过程中创建一个逻辑卷, 则有些步骤会自动执行。

- 把这个分区的卷标改为逻辑卷。
- 把带卷标的分区初始化为物理卷。
- 把一个或多个物理卷合并成一个卷组。
- 一个卷组可以分割为多个逻辑卷。
- 然后可以把一个逻辑卷格式化为 Linux 文件系统或作为交换空间;
- 格式化后的逻辑卷可以挂载到一个目录上或作为交换空间。

5. 有关 RAID 阵列的基本信息

在 RHEL 6 发布之前, RAID 是 RHCT /RHCE 认证的必考内容。由于它不再出现在 RHCSA / RHCE 认证目标中或这些考试培训课程的提纲中, 因此暂时不讨论这个问题。无论如何, RHEL 6 配置的 RAID 属于软件 RAID。这个缩写符即独立冗余磁盘阵列(Redundant Array of Independent Disks)可能会引起误解, 因为软件 RAID 通常是建立在独立的分区上。冗余的产生是由于使用了不同物理磁盘上的分区。

1.5.5 分区创建练习

现在回到安装过程。如果你到现在为止都跟着前面介绍的步骤操作, 而且系统有足够的内存, 则会看到 Disk Druid Please Select A Device 屏幕, 如图 1-8 所示。

在这个屏幕中, 你有机会配置分区、逻辑卷和 RAID 阵列。

(1) 按前面表 1-1 的描述配置标准分区。如果硬盘的空间足够大, 大分区是允许的。而且如果正在建立的物理主机系统包含几个虚拟机, 则大分区是必需的。单击图 1-9 中的 Create 按钮可以创建标准分区、逻辑卷和 RAID 阵列, 并且选择 Standard Partition 并单击 Create 继续下一步。

(2) 现在会看到如图 1-10 所示的 Add Partition 窗口。它有以下几个选项:

- **Allowable Drivers**(允许驱动程序) 为安装起见, 只在虚拟硬盘驱动器上配置分区, 并把它的卷标设置为 Virtio Block Device;
- **Mount Point**(加载点), 它就是一个目录(如/boot), 此目录中的文件保存在此分区上。你可以输入加载点, 或者利用下拉列表, 从中选择常用的加载点目录;

- **File System Type**(文件系统类型), 采用默认的 ext4 文件系统足够了。在下拉列表中还有其他格式选项, 可以使用物理卷、RAID 阵列和交换空间配置;
- **Size of the Partition**(分区的大小(MB))。这时, 表 1-1 定义了为该基线系统配置各个分区。

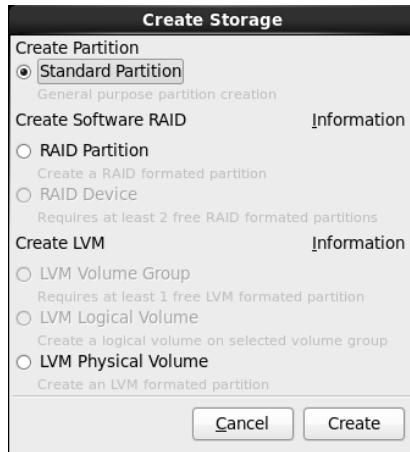


图 1-9 可以创建各种存储设备

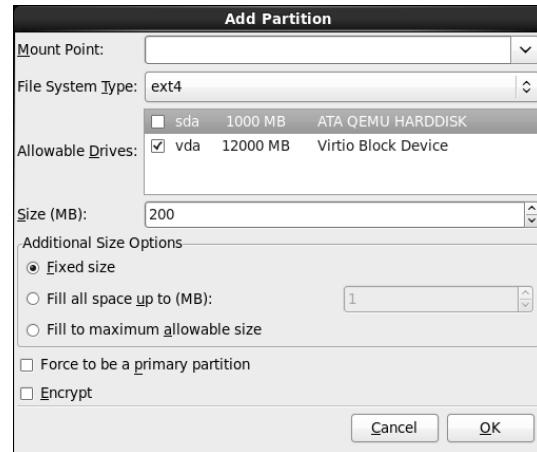


图 1-10 添加一个分区

现在是练习的时候。首先, 讨论在安装过程中如何创建和配置分区, 此外讨论如何把文件系统分配给一个分区或一个逻辑卷。

1.5.6 练习 1-1: 在安装过程中进行分区

这是 RHEL 6 安装过程的一个同步练习。虚拟机上的错误很容易恢复, 因为重新启动安装过程相当容易。本练习从图 1-8 所示的 Please Select A Device 屏幕开始, 继续图 1-9 和图 1-10 所示的屏幕。此外我们假设物理内存足够, 可以选择图形安装模式。

- (1) 开始创建个性化的布局。如果从空白的硬盘开始, 则不需要配置分区。如果硬盘的空间不够, 则删除已配置的分区;
- (2) 练习创建一个普通分区。单击 Create 打开 Create Storage 窗口。选择 Standard Partition 选项, 并单击 Create 按钮打开如图 1-10 所示的 Add Partition 窗口。设置一个合适的挂载点, 如/home/user。单击 File System Type 下拉文本框并浏览可用的格式。如果有多个硬盘可以使用, 必须选择合适的硬盘驱动器;
- (3) 保留默认的 ext4 File System Type, 单击 OK 按钮继续;
- (4) 用前面介绍的步骤再创建一个分区。在本练习中, 默认的 200MB 足够了, 我们假设有足够的磁盘空间可以使用;
- (5) 现在再次单击 Create 按钮, 选择 LVM Physical Volume(LVM), 然后单击 Create 按钮, 注意系统出现 Add Partition 窗口和 Physical Volume(LVM) File System Type。如果有多个磁盘可用, 必须从中选择一个合适的硬盘, 单击 OK;
- (6) 重复刚才的步骤创建第二个 LVM 分区。如果有多个硬盘可以使用, 必须选择一个不同于第(5)步中所选的硬盘;
- (7) 单击 Create, 现在应选择 LVM Volume Group 选项, 并单击 Create;
- (8) 在 Make LVM Volume Group 窗口中, 单击 Physical Extent 下拉框浏览可用的 Physical

Extents，它是卷组的单位。通常不需要做任何改变；

- (9) 确保所有 Physical Volumes To Use 选项都是激活的。
- (10) 单击 Add 打开 Make Logical Volume 窗口。
- (11) 输入一个合适的挂载点，如 /home/volume。默认显示 Logical Volume Name，可以用任何合适的文件名作为逻辑卷的名字。设置一个空间大小，它不要把全部可用的空间都用完。单击 OK。
- (12) 检查 Make LVM Volume Group 窗口中的结果，单击 OK 并检查原来分区窗口中的结果。
- (13) 现在该执行一些清除操作。单击 Cancel 返回到原来的主分区窗口。单击 Reset 把磁盘恢复到练习前的配置。

现在练习已经完成，分区配置情况至少应该反映表 1-1 中的最小值。其中一个可能结果如图 1-11 所示。如果操作过程出现一个错误，则选择一个分区并单击 Edit 按钮。在出现的 Edit Partition 窗口中含有相同的选项。不同的分区以及分区大小的适度变化在 Red Hat 考试中无关紧要。

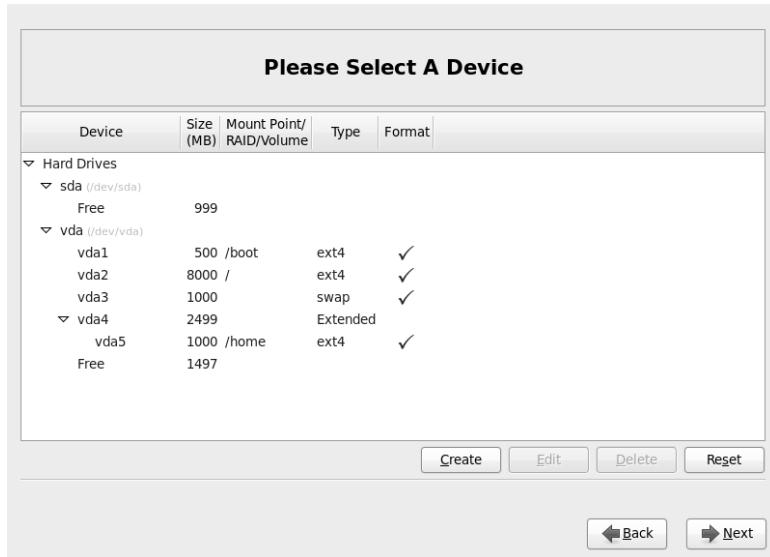


图 1-11 分区配置示例

为了完成安装过程的这一部分操作，单击 Next 按钮。如果出现一个格式警告(Format Warning)窗口，则表示已经创建的分区上还有数据，这是最后一次可以选择取消的机会。假设一切都符合要求，则单击 Format 按钮继续下一步骤操作。在下一个窗口中单击 Write Changes To Disk。

1.5.7 配置引导加载程序

GRUB 是 Linux 标准的引导加载程序，它的全名是 GRand Unified Bootloader。RHEL 6 使用比较早的 GRUB 版本即 GRUB 0.97，它是一个行之有效的引导加载程序。对于双引导配置，图 1-12 中的配置是合理的默认值。在虚拟机上，配置画面更加简单，在大多数情形下不需要做任何改变。

实际经验

术语“引导加载程序”(boot loader)和 bootloader 可以互换。这两个都经常出现在 Red Hat 文档中。

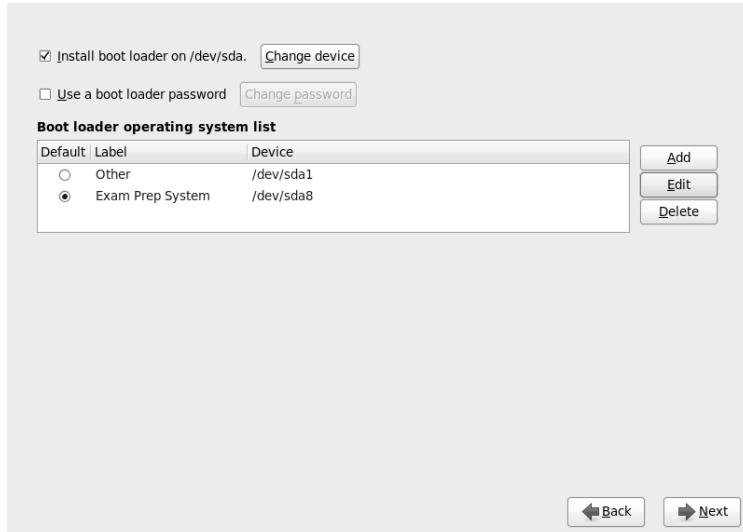


图 1-12 配置引导加载程序

考试提示

Linux 加载程序(Linux Loader, LILO)在最近 10 年里没有得到 Red Hat 的支持。此外，虽然 GRUB 2.0 可以使用，但是它也没有得到 RHEL 6 的支持，至少最初的版本不支持。

- **Install Boot Loader On /dev/sda(在/dev/sda 上安装引导加载程序)** 此选项将把引导加载程序安装到检测到(noted)的硬盘驱动器的主引导记录上。如果没有安装另一个引导程序，这样是可行的。
- **Use A Boot Loader Password(使用引导加载密码)** 可以保护系统的安全。第 5 章将介绍，如果没有引导加载密码，则任何可以访问引导菜单的用户都可以访问 Linux 系统，而且只要引导到运行级 1 就拥有系统管理员的全部权限。
- **Boot Loader Operating System List(可引导加载的操作系统列表)** 列出了检测到的操作系统。虽然在实际应用中，列表的第二项可能会是微软的 Windows 操作系统，但是在 Red Hat 考试中只有 RHEL 6 操作系统。

虽然可以为其他操作系统的菜单增加一个记录，但是这不适用于同一个系统上的其他 Linux 系统。因此更有效的方法是，在安装结束后直接修改 GRUB 引导加载程序的配置。

虽然我们可以设置引导加载密码，但在任何以 RHEL 6 为本地计算机唯一操作系统的系统上可接受默认值。做一些适当的修改，单击 Next 按钮继续下一操作。

1.5.8 RHEL 6 中的所有程序包

RHEL 6 安装 DVD 盘上有超过 2 500 个程序包。这个数目还不包括其他通过 Red Hat Network 发布的程序包。面对这么多的程序包，重要的是把它们进行分类。在完成 GRUB 引导加载程序

的配置后，我们将看到如图 1-13 所示的选项。这个屏幕允许我们把本地系统配置成我们所需要的功能，要根据自己的目标选择程序包。如果你安装一个本地物理系统是为了建立基于 KVM 的虚拟机，则选择 Virtual Host；如果你要创建虚拟客户机(或者其他专用的服务器)，选择 Basic Server。在 Red Hat 考试中，要求考生在基本的操作系统安装完成后安装一些额外的软件。其他的选项如表 1-3 所示，随着重构发行版的不同，这些选项可能变化很大。

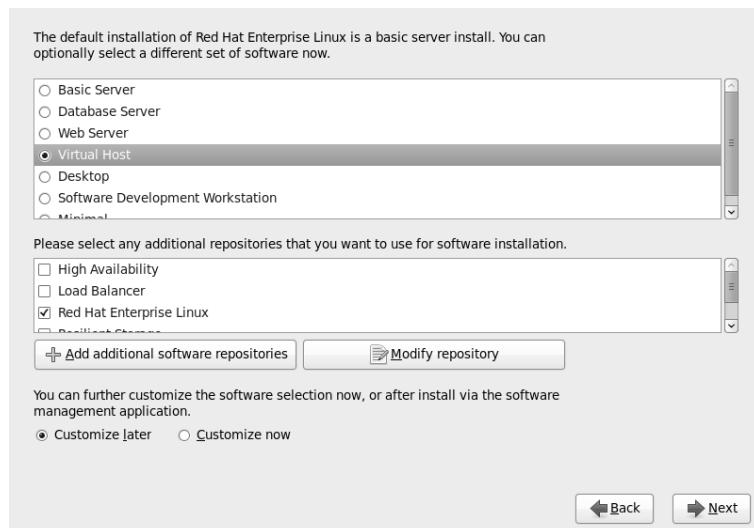


图 1-13 功能安装选项

表 1-3 安装软件的分类

分类	说明
基本服务器	安装 Red Hat 的基本程序包，且把系统当作一个服务器
数据库服务器	包括 MySQL 和 PostgreSQL 数据库程序包
Web 服务器	用 Apache Web 服务器创建一个系统
虚拟主机(Virtual Host)	用 KVM 虚拟机系统配置一个系统
Desktop(桌面)	包括桌面生产程序包
软件开发工作站	添加修改和编译软件的工具
Minimal(最小安装)	最小 Linux 操作系统所需要的程序包

要在生产环境中建立一个真正安全的基线，可以考虑最小安装。越少的程序包意味越少的弱点。只添加真正需要的程序包，黑客就无法利用没有安装的程序包。

实际经验

在 Linux 世界中，黑客(hacker)一词表示那些想创建更好软件的且怀有善意的人们。术语怪客(cracker)是指那些不怀好意、想闯入其他人系统的人们。

表中列出的程序库(Repository)在需要添加额外的服务器功能时有用。顾名思义，图 1-13 中没有被选取的程序库支持以不同的分类安装软件，其中包括了存储群集，具有高可靠性的系统或者可以平衡高流量服务负载的系统。由于它们都是属于 Red Hat 的程序库，并且由 Red Hat

来维护，因此有些第三方程序库可能不会重复图中列出的一些程序库的可用性和功能。

如果你想把系统重定向到本地或内部程序库以控制其他人在他们自己系统上安装的程序库，则单击 **Modify Repository**。它允许你指定到本地系统的哪个位置可以找新的程序库和它们的最新版本。

实际经验

有些开发小组可以安装没有得到 Red Hat 支持的软件。在 <http://atrpms.net> 和 <http://rpmrepo.org> 这两个网站可以找到两个示例。

本章保留默认的 Red Hat Enterprise Linux 程序库(或者例如 CentOS/Scientific Linux 的重构版本的默认程序库)，必须选择 **Customize Now**，否则无法跟上第 1.5.9 节内容。单击 **Next** 继续。

1.5.9 基线程序包

本节概括地介绍在 RHEL 6 安装过程中可以使用的程序库。在考试中，可能会要求考生用 Red Hat Add/Remove Software 工具引用这些程序库组中的一个。用 **yum grouplist** 命令也可以得到可用程序包组的列表。更多的信息可以阅读第 7 章的内容。

Red Hat 程序包组是根据逻辑关系进行组织的。例如，与特定语言有关的程序包都在 **Language** 程序包组中。重要的是选择真正需要的程序包组。安装的程序包越少意味着有更多的空间可以保存自己个人数据和监测系统所需要的日志文件。

1.5.10 程序包组

本节以最简洁的方法逐一介绍在 RHEL 安装过程可以使用的程序包组。如图 1-14 所示，在左侧窗格中有高级别的程序包组，如桌面(**Desktops**)程序包组；常规的程序包组在右侧的窗格中，如 X Window System。每个程序包组都有相应的 RPM 详细信息，这些信息都保存在一个 XML 文件中，要浏览这些文件的内容可以切换到 RHEL 安装 DVD 盘，并在/repo/目录中阅读*-comps-rhel6-Server.xml.gz 压缩文件。

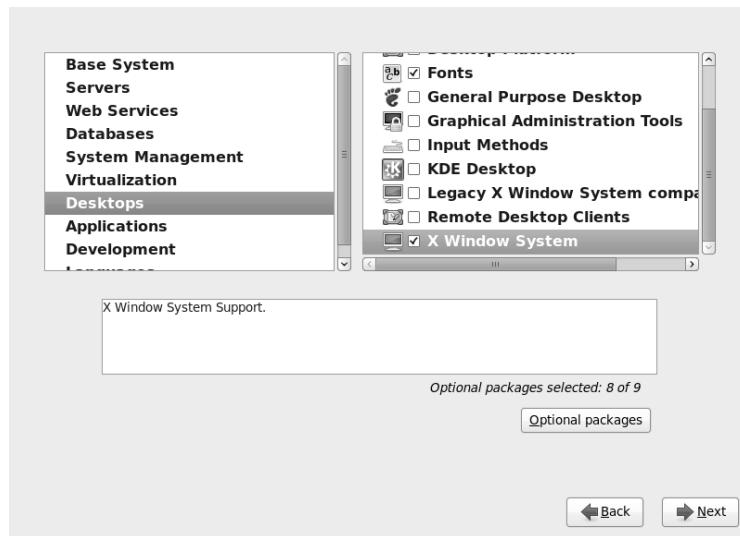


图 1-14 Red Hat 企业版 Linux 程序包组

现在举例说明程序包组的详细内容。选择 Desktop 并单击 Optional Packages，这会打开 Packages In Desktop 窗口，如图 1-15 所示。把这个列表与前面提到的 XML 文件进行比较。强制性的程序包不会出现在相关的窗口，因为它们的安装是由相应的程序包组来决定。根据 XML 标签的意义，默认的程序包是默认选取的，而可选程序包可以不选。

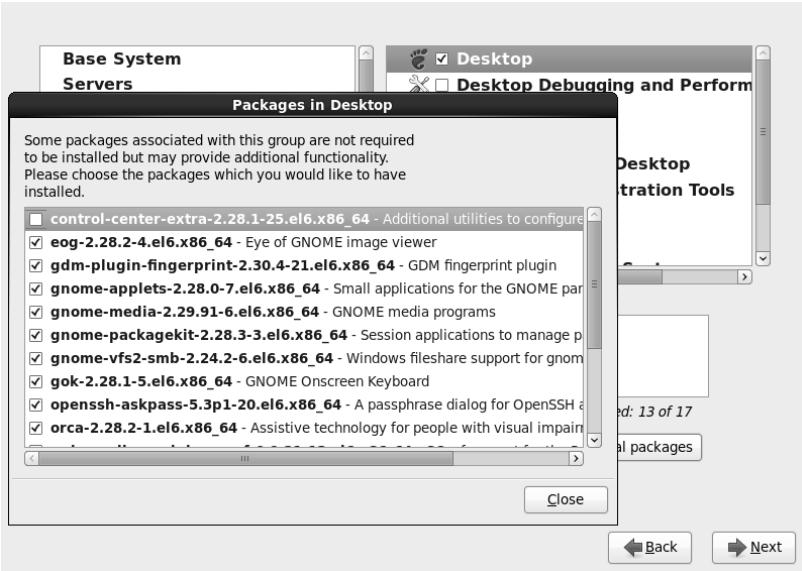


图 1-15 RHEL 桌面程序包组的详细内容

你最好花点时间研究这个屏幕。仔细分析每个程序包组中的程序包。我们就能了解默认安装要安装哪些类型的程序包。安装过程中如果不添加它们也没关系。当然还可以用 rpm 和 yum 命令或者第 7 章介绍的 Add/Remove Packages 工具添加它们。

如果 XML 文件太难理解，则只需要记下程序包组的名称。根据这个名称，就可以在安装结束后找到相关程序包的列表。例如，下面这个命令确定 base 程序包组中的强制的、默认的和可选的程序包：

```
$ yum groupinfo base
```

本书中创建了两种不同的基本安装模式。一种基线适合于虚拟机的主机系统，另一种适合于安装在虚拟机上。两种基线都包含了相对最小的 GUI 安装模式，因为大多数 Linux 管理员为方便起见都喜欢并排打开多个命令行控制台。因此在安装过程中选择了下面的程序包组：

- **Desktops/Desktop** 包括基本的 GNOME 桌面环境。
- **Desktops-Fonts** 安装了字体以改进 GUI 的系统可读性。
- **Desktops-X Window System** 添加了与 GUI 有关的服务器程序包。
- **Application-Internet Browser** 增加了 Firefox Web 浏览器。

程序包组分成不同的几类。例如，为了选择 X Window System 程序包组，首先选择左侧窗格中的 Desktop 目录，接下来选择右侧窗格中的 X Window System 程序包组。

除此之外，对于配置了基于 KVM 的虚拟机的物理主机系统，确保已经包含了可视化软件包组。如果在安装前选择了虚拟主机系统目录，则会自动包含上述软件。

选择了所需要的程序包后，单击 Next 按钮，Anaconda 则继续执行安装过程。当安装过程结束时，最后会看到一个屏幕，它确认安装过程，并带有一个重新启动系统的选项。

实际经验

在本书使用的系统中，同时安装了 OpenOffice.org 软件和 GIMP 程序包(GNU 图像操作程序)。

1.5.11 系统重启

安装结束后看到一个最后的信息，其中有一个选项要求重启系统。如果你是在物理系统上安装 RHEL 6，不要忘了弹出或拿走引导盘和/或安装 DVD 盘。

如果 RHEL 6 是安装在基于 KVM 的虚拟机上，则需要改变引导设备。如果这个设备还没有打开，则单击 Applications | System Tools | Virtual Machine Manager 命令，若系统提示则输入超级系统管理员的口令，并双击需要重启的虚拟机，然后按照下面步骤修改引导设备：

- (1) 在与虚拟机相关的窗口中，单击 View | Details。
- (2) 出现如图 1-16 所示的窗口。在这个窗口中，单击 Boot Options。

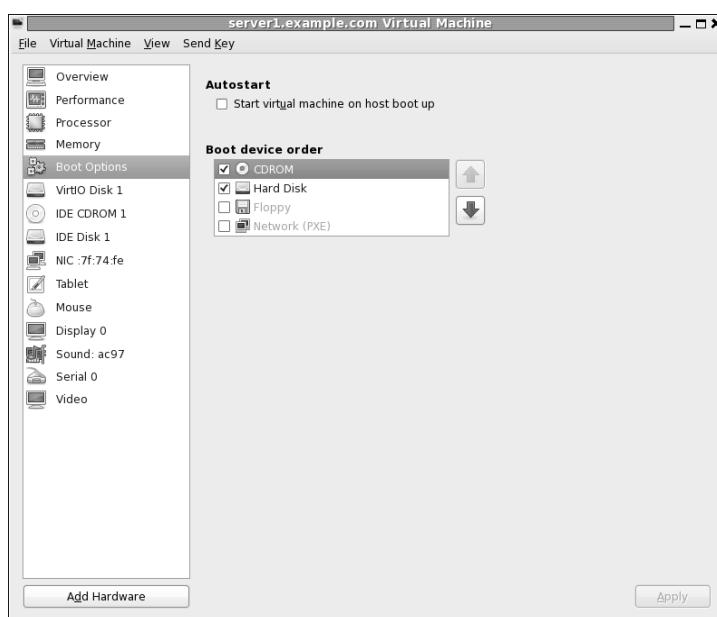


图 1-16 虚拟机管理器中的引导设备

- (3) 如果默认的引导设备已设置为 CDROM，则必须用箭头按钮把它改为 Hard Disk(反之亦然)。选择后单击 Apply。注意，这些改变直到 KVM 虚拟机下次开机才生效。
- (4) 单击 View | Console。如果还没有这样做，则单击 Reboot 结束 RHEL 6 的安装过程。
- (5) 单击 Virtual Machine | Shut Down | Force Off。当出现提示则选择确认。
- (6) 单击 Virtual Machine | Run，系统则会正常引导并进入到刚安装的系统。

实际经验

在编写本书的时候，Virtual Machine | Shut Down | Reboot 和 Virtual Machine | Shut Down | Shut Down 菜单选项不起作用。

在大多数安装过程中，RHEL 6 会启动在本章后面讨论的第一个引导进程。

认证目标 1.06 系统设置选项

基线配置非常重要。一旦配置好基线系统，就可以根据把它克隆后按需要安装很多系统。在实际的网络上，一个好的基线可以用来创建专用于某些特定服务的系统。为了启动远程访问，系统必须具有一个安全 Shell(Secure Shell, SSH)服务器，普通用户可以对其进行设置。

对引导过程，RHEL 6 包含了 Upstart 系统的一个实现程序，它取代了基于 Unix 的 SysVInit 系统。它决定了系统引导时使用的控制台、服务和显示器以及系统启动时使用的运行级(runlevel)。有些系统使用远程认证，将其配置好后连接到远程服务，从远程服务器读取用户名和密码验证。虽然这些系统也在其他章中有论述，但是本节提供的信息足以建立一个基线系统。

1.6.1 第一引导进程

首先，有一个进程是大多数 RHEL 6.0 系统在安装完成后第一次引导时启动的，它就是第一引导进程。尽管这个进程有一个功能类似的文本模式版本，但本章前面介绍的默认安装会得到该进程的 GUI 版本。本节介绍的步骤是以实际 RHEL 6 的安装为基础，重构发行版的步骤可能会不一样。

- (1) 它启动一个欢迎屏幕，单击 Forward 继续；
- (2) 第一引导进程继续处理许可证协议，该协议在 RHEL 6 和重构发行版中是不同的。(Scientific Linux 6 甚至不需要这一步)。如果你拒绝了许可证协议，系统提示你将 RHEL 6 关闭并从本地系统中删除。如果接受此许可证协议，选择 Yes 并单击 Forward 继续下一步；
- (3) 提示用户把系统连接到 Red Hat Network。如果单击 Why Should I Connect to RHN，则会出现一个如图 1-17 所示的窗口；

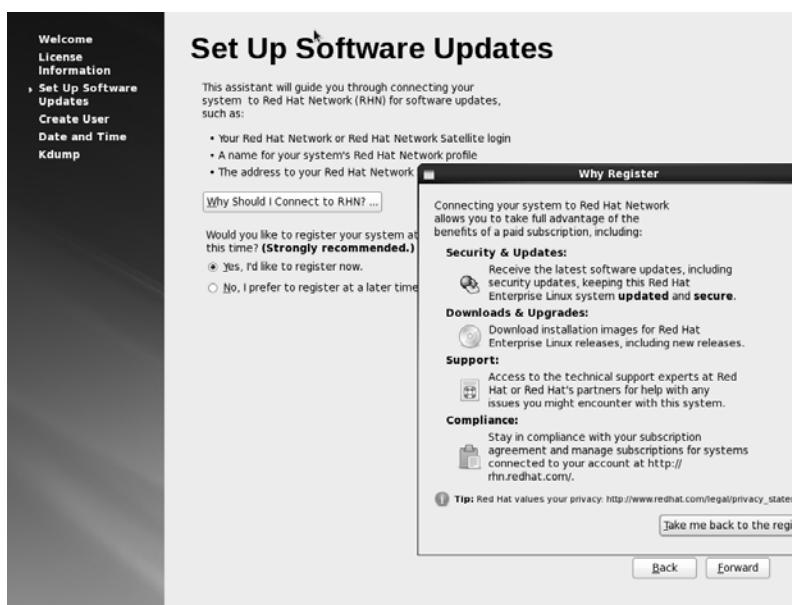


图 1-17 单击 Why Should I Connect to RHN 后出现的窗口

(4) 注册时需要一个 RHN 账户和一个可用的订阅。这不是 RHCSA /RHCE 要求的内容，选择 No 并单击 Forward 继续；

(5) 接着出现注册的理由。为了避免在这个时候进行注册。单击 No Thanks, I'll Connect Later 继续。稍后可以用 `rhn_register` 命令在 RHN 进行注册；

(6) 出现一个提示窗口，说明本地系统还没有安装软件更新。在第 7 章中执行这个操作。单击 Forward 继续；

(7) 虽然这一步骤并非安装过程必需的，但稍后它允许用户为系统创建普通用户。虽然我们可以连接到远程用户数据库，但是此时需要创建一个普通本地用户。如果单击 Advanced，它会打开 Red Hat User Manager(用户管理器)，可以帮助你输入用户的个人信息，这将在第 8 章讨论。至少创建一个本地用户，单击 Forward 继续下面的操作；

(8) 现在要为本地系统建立一个日期和时间。显示的日期和时间是本地硬件的日期和时间。如果选择 Synchronize Date And Time Over the Network(与网络的日期和时间同步)选项，则这个窗口显示可用的 NTP 服务器。这是根据 Date/Time Properties 工具所选择的选项，该工具的用法将在第 5 章简要介绍并在第 17 章详细介绍。根据需要修改后单击 Forward 继续下一步操作；

(9) 除非系统有大量的内存，否则会出现这样的消息“Insufficient memory to configure kdump”，这会收集与内核崩溃有关的数据。单击 OK 或者做适当的修改，并单击 Finish。

如果还没有安装 GNOME Desktop Environment 和 X Window System 这类 GUI 工具，则会看到不同于第一引导工具的文本模式，如图 1-18 所示。即使已经设置了 GUI 选项，也可以用 `setup` 命令启动该工具的其他等效程序。



图 1-18 文本模式的安装工具

文本模式的安装工具包含了 6 个工具。它们的功能将在不同章中详细介绍。

1.6.2 默认的安全设置

RHEL 6 安装结束后，还有一些与 SELinux 和基于 iptables 的防火墙相关的默认设置。这里只概括性地介绍这些默认设置，不做深入讨论。有关安全选项的详细信息请阅读第 4 章、第 10 章和其他内容。

首先，默认情况下 SELinux 在强制模式下被启用，用 `sestatus` 命令可以确认这个设置，输出信息如下：

```
SELinux status:          enabled
SELinuxfs mount:        /selinux
Current mode:           enforcing
Mode from config file: enforcing
Policy version:         24
Policy from config file: targeted
```

第4章将介绍有关 SELinux 和 RHCSA 考试的更多信息。如果你要考 RHCE，还要学习第10章的 SELinux 配置方法以及它支持的各种服务。

如果想了解当前 `iptables` 命令的详细内容，需要分析 `/etc/sysconfig/iptables` 文件。它就是 `iptables` 服务使用的文件，该文件是执行 `/etc/init.d/iptables` 脚本的结果。下面这一行内容就是来自此文件，它允许外界通过端口 22 访问本系统。

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
```

SSH 支持本地系统的远程管理，端口 22 是 SSH 服务使用的默认端口号。如果网络连接正常，则可以远程连接到这个系统。如果本地系统的 IP 地址是 192.168.122.50，则用下面的命令可以远程连接到 michael 用户的账户：

```
# ssh michael@192.168.122.50
```

配置 SSH 服务器以进一步加强安全级别。详细内容请阅读第 11 章。

1.6.3 虚拟机的特殊设置选项

在基于 KVM 的虚拟主机中，可以看到额外的防火墙规则。例如，在系统虚拟机中的 `/etc/sysconfig/iptables` 文件有如下一行额外规则，它接受由物理桥接网络设备传来的流量。

```
-I FORWARD -m physdev --physdev-is-bridged -j ACCEPT
```

它利用动态文件 `/proc/sys/net/ipv4/ip_forward` 完成 IPv4 网络连接功能中活动 IP 的转发功能。这是一个二进制文件，如果它的值置为 1，则 IPv4 转发功能启动。如果要永久性设置此项，则打开 `/etc/sysctl.conf` 文件并确保把下面的指令置为 1。

```
net.ipv4.ip_forward=1
```

为了将此修改立即应用于本地系统，要执行以下命令：

```
# sysctl -p
```

有关这方面的用法将在第 5 章有关网络配置内容中简要介绍。有关 `/proc` 文件系统的细节属于 RHCE 的考试内容，将在第 12 章讨论。

认证目标 1.07 配置默认的文件共享服务

RHCSA 考试教程的一个要求是“配置一个系统以运行一个默认配置的 FTP 服务器”以及“配置一个系统以运行一个默认配置的 FTP 服务”。现在我们分析这两句话的含意。RHEL 6 上默认的 HTTP 服务器就是 Apache Web 服务器，而相应的默认的 FTP 服务器是 vsFTP 服务器。

虽然这些服务的配置细节属于 RHCE 范围，但是在默认的安装方式下系统都已包含了默认安装中的基本功能。我们可以验证默认安装的设置，然后再进一步将这些服务设置为共享文件，具体说就是从安装 DVD 上复制过来的文件。

将这些服务配置为共享文件非常简单。不需要对主要的配置文件做任何修改。假设 SELinux 已启用(在考试中它肯定已启用)，则基本步骤如下：

- 把 RHEL 6 安装 DVD 盘的内容复制到合适的目录；
- 确实已使用 SELinux 正确的上下文配置此目录的内容；
- 将上述服务配置为指向开始目录，系统启动后就该特定。

不同的服务其实现步骤自然也不一样。这里介绍的操作过程是最基本的。如果遇到新的命令或服务，仅是这些基本的内容也许不够。有关 mount 命令的更多信息请阅读第 6 章。想深入了解 SELinux 请阅读第 4 章。有关 Apache Web 服务和 vsFTP 服务可分别阅读第 14 章和第 16 章。

1.7.1 挂载和复制安装 DVD 盘

你可能已经知道了 mount 命令可以把分区或 DVD 驱动器这样的设备连接到某个特定目录。例如，下面的命令将标准的 DVD 驱动器挂载到/media 目录上。

```
# mount /dev/dvd /media
```

RHEL 6 在/dev 目录中包含了很多类似的设备文件。使用 ls -l 命令可以确认这些文件都链接到/dev/sr0 设备文件上：

```
# ls -l /dev/dvd
# ls -l /dev/dvdrw
# ls -l /dev/cdrom
```

如果 DVD 驱动器已正确配置，则应该在/etc/filesystems 文件中自动找到合适的文件系统格式。此时的文件系统格式为 iso9660，它是 ISO 标准，常用于 CD 和 DVD 格式。我们有理由认为 DVD 已经正确配置。否则前面的 mount 命令就会出现如下的错误消息：

```
mount: you must specify the filesystem type
```

最可能的原因是 ISO 文件中存在错误或者 DVD 的文件刻录方式有错误。至于 ISO 文件，它很容易直接挂载到一个目录上，根本不需要物理的 DVD 驱动器。下面这个命令用于 RHEL 6 DVD：

```
# mount -o loop rhel-server-6.0-x86_64-dvd.iso /media
```

下一步是把 DVD 的内容复制到 FTP 或 HTTP 服务器共享的目录中。一般来说，下面这个

命令确保以档案模式(-a)和递归形式(-r)复制文件。命令中的句点(.)包含了隐含文件。该命令把这些文件复制到上述目录中：

```
# cp -ar /media/. /path/to/dir
```

实际使用的目录取决于服务器。当然，也可以将服务器配置为使用除默认位置的其他目录。

1.7.2 设置一个默认配置的Apache服务器

在Red Hat实现中，Apache Web服务器使用/var/www/html目录保存HTML文件。在此目录下建立的子目录可以用于文件共享。这是针对Red Hat程序包安装生成的默认Apache配置。尽管如此，必须确保在现有的防火墙中打开80端口。

把Apache配置为RHEL安装服务器的过程与配置vsFTP的过程相似。练习1-2中要求把Apache服务器配置为一个安装服务器。首先用下面命令确保Apache服务器已安装：

```
# yum install httpd
```

如果这命令执行成功，就会在/etc/httpd/conf目录中找到主要的Apache配置文件httpd.conf和在/var/www/html目录中主要的数据目录。但是要记住，千万不要修改这个配置文件。为了确保默认安装能正常运行，首先用下面的命令启动Apache服务：

```
# /etc/init.d/httpd start
```

接着，在安装有Apache的系统中打开一个浏览器，并用如下的URL地址http://127.0.0.1/导航到本地主机(localhost)IP地址。以下是来自RHEL 6 Scientific Linux重构版本的示例，如图1-19所示。

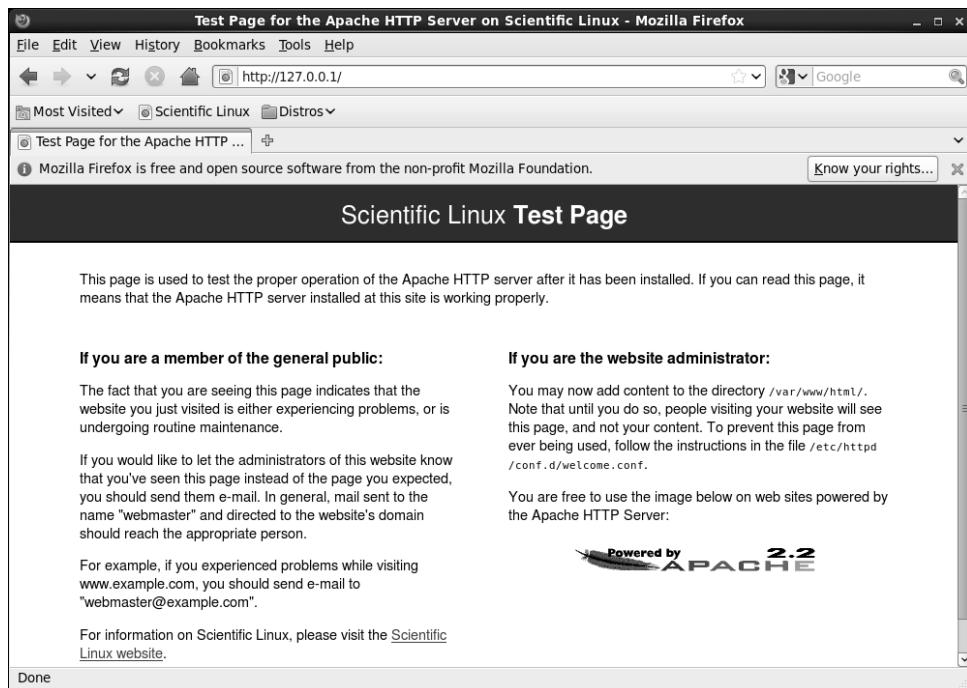


图1-19 默认Apache服务器运行的证明

如果本地防火墙中的端口 80 已打开，则从远程系统可以访问这个页面。此外，要确保下次 RHEL 6 启动时 Apache 服务会自动启动，办法之一是用下面的命令：

```
# chkconfig httpd on
```

在引导过程中如何控制 Apache 服务等有关内容可以阅读第 11 章。虽然第 11 章属于 RHCE 考试范围，但这里的 `chkconfig` 命令很简单。

1.7.3 练习 1-2：把 Apache 服务器配置为安装服务器

在这个练习中，我们要安装 Apache Web 服务器，并且把它配置为一个适合于 RHEL 6 安装的文件服务器。需要准备一个 DVD 副本或者 ISO 格式的相关下载文件。本练习的操作步骤包括创建合适的目录、复制安装文件、设置一个适合的 SELinux 上下文、打开现有防火墙中的 80 端口以及重新启动 Apache 服务。这些都是基本步骤，Apache 配置的详细过程将在第 14 章中讨论。

(1) 把 RHEL 6 DVD 挂载到一个空目录上。可以使用以下两个命令，第一个命令挂载一个实际的物理 DVD，第二个命令挂载 ISO 文件：

```
# mount /dev/dvd /media
# mount -o loop rhel-server-6.0-x86_64-dvd.iso /media
```

(2) 为安装文件创建一个适合的目录。由于 Apache Web 服务器文件的标准目录是`/var/www/html`，最简单的办法是用下面的命令在此目录下建立一个子目录：

```
# mkdir /var/www/html/inst
```

(3) 从挂载的 DVD 中将文件复制到新目录中：

```
# cp -ar /media/. /var/www/html/inst/
```

(4) 使用 `chcon` 命令确保这些文件具有正确的 SELinux 安全上下文。命令中的-R 可以使用从复制的安装文件递归生成的修改。`--reference=/var/www/htm` 开关选项转而应用来自此目录的默认 SELinux 上下文。

```
# chcon -R --reference=/var/www/html/ /var/www/html/inst
```

(5) 打开与 Apache Web 服务器相关的 80 端口。启动 `system-config-firewall` 命令很容易打开端口。如果这太复杂，则可以用下面的命令禁用当前系统上的防火墙。第 4 章和第 10 章将详细介绍如何配置防火墙。

```
# iptables -F
```

(6) 确保使用下面的命令启动 Apache Web 服务器：

```
# /etc/init.d/httpd restart
```

Apache Web 服务器现在可以作为文件服务器使用，该服务器共享 RHEL 6 DVD 的安装文件。为了验证，把浏览器指向此服务器的 IP 地址和 `inst/` 目录。如果 IP 地址为 192.168.0.200 则使用下面的导航地址：

<http://192.168.0.200/inst>

如果成功，则看到如图1-20所示的页面，里面有许多可以下载和单击的文件：

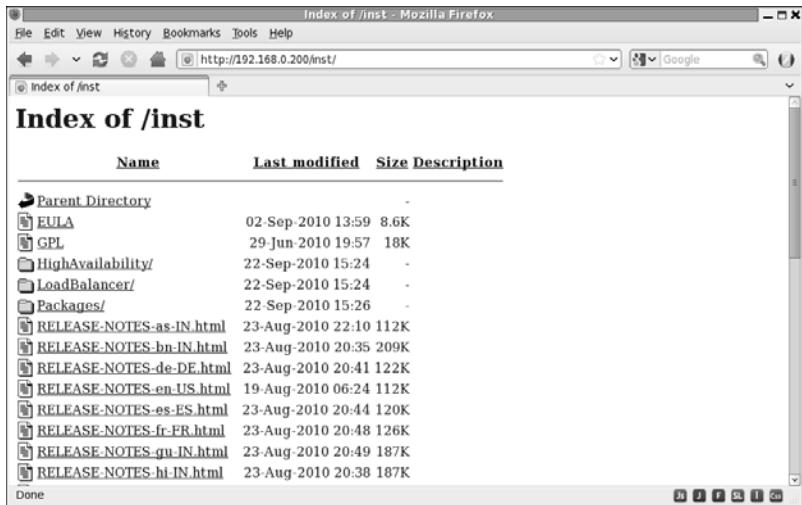


图1-20 可下载文件

1.7.4 通过FTP服务器共享复制文件

vsFTP服务器的Red Hat实现中包含一个/var/ftp/pub目录，用来保存发布文件。出于安装文件的考虑，我们可以创建/var/ftp/pub/inst目录。为了使系统与SELinux兼容，需要用一个命令修改这些文件的安全上下文。当启动或重新启动vsFTP服务器，它就可以用作安装服务器。此过程在Lab 2中有详细描述。假设系统已使用RHN或者从重构发行版与远程库建立了正确的连接，则用下面的命令安装最新版本的vsFTP：

```
# yum install vsftpd
```

如果安装成功，就会在/etc/vsftpd目录中找到主要的vsFTP配置文件——vsftpd.conf，并在/var/ftp/pub中找到主要数据目录。不要对此配置文件做任何修改，因为这是默认配置服务器的需求。确保用下面的命令启动vsFTP服务：

```
# /etc/init.d/vsftpd start
```

因为现在Web浏览器可以访问FTP服务器，所以只要导航到`ftp://127.0.0.1/`地址就可以验证本地系统上FTP服务器的默认配置。如果使用Firefox Web浏览器，则默认的结果如图1-21所示。这里显示出的pub/目录实质上就是/var/ftp/pub目录。

注意vsFTP服务器的安全。单击窗口中的Up To Higher Level Directory超链接。当前目录不会改变。连接到此FTP的用户无法看到上一级目录，即/var/ftp，更不能从上一级目录下载文件。这个安全概念就是所谓的chroot监狱(chroot jail)。这个概念常用在域名服务器(DNS)等其他系统上以加强主机系统的安全。

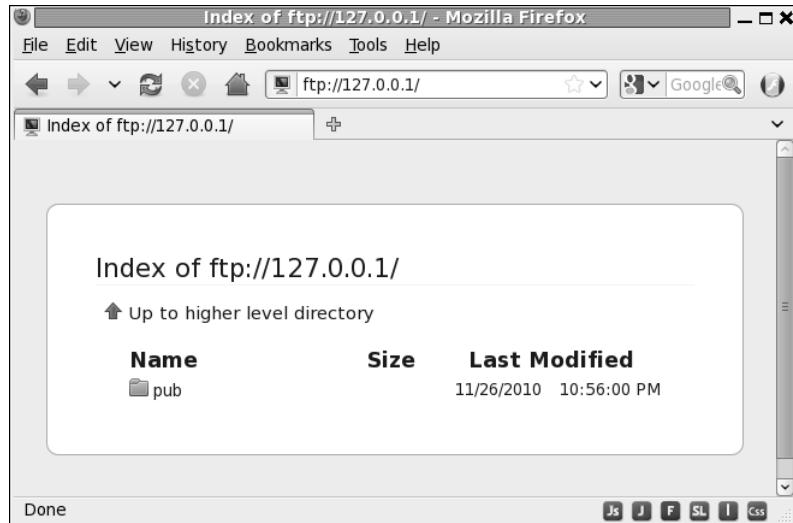


图 1-21 访问默认 FTP 服务器

如果在本地防火墙中端口 21 已打开，则也可以从远程系统访问这个 FTP 服务器。此外，还要确保 vsFTP 服务器在下次 RHEL 6 启动后自动启动。方法之一是使用下面的命令：

```
# chkconfig vsftpd on
```

vsFTP 后面的 d 表示 daemon。有关在引导过程中如何控制 vsFTP 等服务的更多内容可以阅读第 11 章。第 11 章虽然属于 RHCE 内容，但是应该不难记住这个 chkconfig 命令。

1.8 认证小结

RHCSA 和 RHCE 考试并不是针对初学者。本章介绍安装一个基本的 RHEL 系统以及本书后面用到的程序包和设置。上述两个考试属于实践性的、动手性的考试。当考生坐下开始考试时，面对的是一个真实的 RHEL 系统，需要解决这个系统的一些问题以及配置这个系统。RHCSA 考试还包括了系统管理方面的技能。

Red Hat 考试现在假设使用 64 位的系统。Red Hat 允许仅在 RHEL 6 的 64 位系统中配置 KVM 虚拟机。RHCSA 考试要求把 RHEL 6 配置为一个虚拟主机。

通过 Red Hat 网络的订阅服务，可以从相应的账户下载 RHEL 安装 ISO 文件。由于 RHEL 软件是在开源许可证协议下发布的，因此 CentOS 和 Scientific Linux 等第三方可以在没有引用 Red Hat 商标的情况下使用此开源代码。也可以使用这些重构版本为 RHCSA 和 RHCE 考试做准备。

为了练习本书后面几章学到的技术，最好建立 RHEL 6 的多个安装模式。为此，建议配置三类系统。虽然许多人在学习中不可能有多余的三台物理计算机，但是利用虚拟机可以在单个物理计算机上安装三个这样的系统。

对 Linux 的初学者而言，RHEL 6 的安装相对比较简单，因此本章没有对每个细节都进行介绍，但是它是以 Lab 2 创建的网络安装源为基础的。安装完成后第一引导进程因是否安装了 GUI 而异。

1.9 小练习

下面是第1章与认证目标有关的几个重要知识点。

RHCSA 和 RHCE 考试

- RHCSA 是不同于 RHCE 的考试。
- Red Hat 考试都是动手操作型考试，其中没有多选题。
- 如果你正在准备 RHCSA 考试，重点是本书的第1章～第9章。如果要参加 RHCE 考试，则要掌握本书全部内容，但是重点是第1章和第10章～第17章。

基本的硬件要求

- 虽然 RHEL 6 可以安装在各种不同的体系结构上，但是为了准备 RHCE 考试需要有 64 位硬件辅助虚拟技术的硬件系统。
- 安装 Red Hat RHEL 6 的硬件系统至少要有 512MB 内存。内存小于这个数量也是可以的，特别是在没有 GUI 功能的系统上。在 KVM 虚拟机上安装 GUI 需要更多的内存。
- RHEL 6 可以安装在本地计算机上，也可以安装在各种网络硬盘上。

获取 Red Hat 企业版 Linux

- Red Hat 考试都使用 Red Hat 企业版 Linux。
- 可以使用 RHEL 6 的订阅版和测试版。
- 自从 Red Hat 发布了 RHEL 6 的源代码后，第三方可以免费根据 Red Hat 开源代码生成自己的发行版。
- 第三方重构的 RHEL 6 在功能上与 Red Hat 直接发行的 Red Hat 完全一样，只是无法访问 Red Hat 网络。
- 比较著名的重构版本有 CentOS 和 Scientific Linux。

安装要求

- Red Hat 宣布，试卷在预先安装好的系统中也以电子形式提供给考生。
- RHCSA 要求把一个物理主机配置为一个虚拟主机。
- RHEL 6 最基本的虚拟机解决方案是 KVM。
- 为了模拟网络通信，有必要建立多个虚拟机。

安装选项

- 可以通过多种引导媒介启动安装过程。
- RHEL 6 可以从 DVD、本地硬盘、NFS 目录、Apache Web 服务器或 FTP 服务器启动安装过程。
- RHEL 6 必须安装在单独一个卷上，此卷至少要有一个顶级 root 目录、/boot 目录和 Linux 交换空间。

- RHEL 6 包含了各种类型的程序包组。

系统设置选项

- 安装后的第一个步骤是执行第一引导进程(First Boot Process)。
- 默认时, Linux 启动 SELinux 和基于 iptables 的防火墙。

配置默认的文件共享服务

- RHCSA 考试要求考生掌握以默认配置模式部署 HTTP 和 FTP 服务器的技术。
- 与 HTTP/FTP 协议相关的默认服务是 Apache Web 服务器和 vsFTP 服务器。
- 部署默认 HTTP 或 FTP 服务器的方法之一是用 RHEL DVD 上的安装文件进行配置。

1.10 自测题

下面的题目有助于更好地理解本章的内容。由于 Red Hat 考试不用选择题, 因此本书也不提供选择题, 这些题目只用来测试你对本章的理解。虽然本章介绍的内容只是“先决条件”, 也可以使用其他方法。Red Hat 考试注重于结果的推导过程, 而不是死记一些无关紧要的内容。

RHCSA 和 RHCE 考试

1. RHCE 考试有多少道选择题? RHCSA 考试呢?
-

基本的硬件要求

2. 假设现有基于 Intel 的 PC 机, RHEL 6 默认使用哪种虚拟技术?

 3. 要在 RHEL 6 上配置 KVM 需要多少位的 CPU?
-

获得 Red Hat 企业版 Linux

4. 说出一个基于 RHEL 开源代码的第三方 Linux 重构版本的名字。
-

安装要求

5. 在 RHCSA 和 RHCE 考试中安装操作的考试时间为多少?
-

安装选项

6. 列出两个不同安装模式的媒介, 它们都可以引导 RHEL 6 的安装程序。
-
-

7. 说出在 RHEL 6 安装过程中可被设置和格式化以存储数据的三类卷。

8. 假如你已把 RHEL 6 DVD 挂载到/media 目录上。在这个 DVD 中有 XML 文件，此文件包含程序包和程序包组。在哪个目录中可以找到这个 XML 文件？

系统设置选项

9. 哪个命令可以启动与文本模式第一次引导进程相同的菜单。

10. 哪个服务可以通过默认的防火墙？

配置默认的文件共享服务

11. 哪个标准目录作为 vsFTP 服务器的 RHEL 6 实现的文件共享目录？

12. 在 Apache Web 服务器中，HTML 文件保存在哪个标准目录中？

1.11 实验题

第一个实验题很基本，目的是促使你用网络和网络连接术语思考问题。第二个实验题帮助你配置一个安装服务器。第三个实验题启发你分析 Linux Professional Institute 对系统管理各个方面的要求。

实验题 1

在这个实验题中，你要为 Red Hat 网络规划一个系统。要把三台计算机配置成 RHEL 6 系统。其中两个配置在同一个域中，即 example.com，这两个计算机的主机名字分别为 server1 和 tester1。第三个计算机配置在第二个域(example.org)中，它的主机名字为 outsider1。

在 example.com 域中的一个计算机即 server1 上配置两个网卡。或者这些系统是 KVM 虚拟主机的两个客户机，IP 转发功能使这两个计算机可以相互通信，尽管它们处在不同的网络上。本实验题的重点是 IPv4 的寻址。

- example.com 域上的系统将在 192.168.122.0/24 网络上被配置。
- example.org 域上的系统将在 192.168.100.0/24 网络上被配置。

理想的情形是把 server1.example.com 系统设置为工作站和服务器。本章介绍的基本操作指令也足够了，它们将在系统安装完成后指导你安装和配置服务。它将是本书实践操作的主要系统。第 2 章将介绍在此系统上安装 RHEL 6，在其他章中及本书的末尾的示例考试中也将克隆该系统。

tester1.example.com 是一个只能通过 SSH 服务进行远程访问的系统。有时非认证考试所必需的服务器服务配置在 outsider1.example.org 网络上。通过它来测试认证考试所需要的客户机。

实验题 2

此实验题假设你已下载了基于 RHEL DVD 的 ISO 文件，如 CentOS 或 Scientific Linux 等重构版本。基于 DVD 的 ISO 文件十分重要，因为它有两个目的。它将成为本章前面介绍过的安装程序库或第 7 章配置的安装程序包。本实验题只包括在 vsFTP 服务器上配置上述文件所需要的命令。

虽然，Red Hat 考试要在一个预安装好的系统完成，但是相关的要求建议考生能够通过网络安装系统，也能够配置 Kickstart 安装。在考试过程中不需要 Internet 访问，也不需要访问 Red Hat 网络或任何其他的 Internet 程序库。

1. 为安装文件创建一个目录。用下面的命令创建/var/ftp/pub/inst 目录(如果操作错误，则 vsFTP 不能正确安装)。

```
# mkdir /var/ftp/pub/inst
```

2. 把 RHEL 6 安装 DVD 盘插入到驱动器。如果驱动器不能自动挂载，则先用 mount/dev/cdrom/media 命令挂载驱动器。(如果所有的 ISO 文件都在 Downloads/子目录中，则要把上面的命令改为 mount -ro loop Downloads/rhel*.iso/media)。

3. 复制 RHEL 6 安装 DVD 所需要的文件。用 cp -ar /source/. /var/ftp/pub/inst 命令，其中 source 是加载点目录(如 /media/)。不要忘了句点(.)，它可确保已复制了.discinfo 文件在内的隐藏文件。

4. 确保可以自由访问自己的 vsFTP 服务器。用 Firewall 配置工具打开本地系统上的端口 21。有关防火墙有 SELinux 更多的信息阅读第 4 章。

5. 如果本地系统已启动了 SELinux，则执行下面的命令把适当的 SELinux 安全上下文应用于新目录上的文件。

```
# chcon -R -t public_content_t /var/ftp/
```

6. 现在用下面的命令激活 FTP 服务器：

```
# service vsftpd restart
```

7. 测试结果。在一个远程系统上，应该能用 lftp 命令和它的 IP 地址连接到本地 FTP 服务器上。一旦建立连接，可以在 pub/inst 子目录中找到安装文件。

实验题 3

Red Hat 考试是一个挑战。在这个实验题中，要求考生从稍有不同的方面来分析 Red Hat 考试的先决条件。如果考生对此考试还举棋不定的话，则 Linux Professional Institute 有一级考

试，这个考试可以详细测试考生的基本技能。此外，一级考试还包括许多与准备 Red Hat 认证考试有关的命令。

为此，先分析有关考试 101 和考试 102 的详细目标。访问 www.lpi.org 网站可以了解这些目标。如果对这些考试目标中列出的大多数文件、术语和工具比较有把握，则可以准备开始学习 Red Hat 考试的内容。

1.12 自测题答案

RHCSA 和 RHCE 考试

1. 任何 Red Hat 考试都没有多选题。考试中有多选题几乎是十年前的事。现在，Red Hat 考试都是测试考生的操作能力。

基本的硬件要求

2. RHEL 6 的默认虚拟技术是 KVM。虽然现在有许多很不错的虚拟技术，但是 KVM 是 RHEL 6 支持的默认选项。

3. 64。为了在 RHEL 6 上配置 KVM，需要一个带有一个或多个 64 位 CPU 的系统。

获得 Red Hat 企业版 Linux

4. 由 RHEL 6 的源代码可以生成几种不同的重构版。其中两个就是 CentOS 和 Scientific Linux。可能还有其他的版本。

安装要求

5. 此题目没有正确答案。虽然 Red Hat 考试现在是在预安装的系统中进行的，但是我们也可以在现有的 RHEL 安装系统中的一个虚拟机上安装一个 RHEL 6。

安装选项

6. 为了安装 RHEL，可以使用的引导媒介有 CD、DVD 和 USB stick。Red Hat 不再在软盘上建立引导媒介。

7. 在安装过程中，考生可以配置和格式化普通的分区、RAID 阵列和逻辑卷以存储数据。

8. 在指定的条件下，考生在`/media/repo`目录中找到这个指定的 XML 文件。

系统设置选项

9. 命令为 `setup`，它要求用户必须有超级系统管理员的权限。

10. RHEL 6 默认的防火墙允许访问安全 Shell 服务，即 SSH 服务。

配置默认的文件共享服务

11. 当 RHEL 6 实现了 vsFTP 服务器服务，则此服务的默认文件共享目录是`/var/ftp/pub`。

12. 当 RHEL 6 实现了 Apache Web 服务器，则保存 HTML 文件的标准目录是`/var/www/html`。

1.13 实验题答案

实验题 1

在配置一个连接到 Internet 上的网络时，考生希望它能够访问 Internet 上的一些系统，同时拒绝这些系统访问其他一些系统。为此此实验题提供一个系统架构，考生可以用该系统架构准备 RHCSA/RHCE 考试。

由于 RHCSA 考试在许多方面相当于配置一个工作站的练习，因此为准备考试配置一个网络并非十分必要。但是，RHCSA 考试包含了与服务器有关的内容，如 FTP 和 HTTP 文件服务器的配置，因此参加 RHCSA 考试的考生不可以完全忽略网络内容。

随着虚拟机的发展，硬件的成本不再成为在家准备 Red Hat 考试的用户的障碍。然而，RHCSA 要求考生能够配置虚拟机。Red Hat 默认的虚拟解决方案是 KVM，它只能在 64 位系统的 RHEL 6 系统上配置。

虽然动态 IPv4 地址用在大多数工作站上，但是在许多情形下，如 DNS 服务器和 email 服务，静态的 IPv4 地址可能更合适。如果已知这些服务器的 IP 地址，则客户端更容易配置。因此对于这样的系统，更好的办法是设置静态 IPv4 地址。

三系统是我们的最低要求，因为与防火墙有关的规则通常不能应用于本地系统上。第二个系统是一个远程客户端，它可以访问本地服务器的服务，第三个系统是远程客户端，它不能访问本地服务器。

当然，真实的网络远比这复杂。希望你创建一个连接更多系统的网络。

在第 2 章中，当在基于 KVM 的虚拟机上安装了 RHEL 6 后，就希望以此系统为基线克隆出其他系统。事实上，许多企业正是这样做的。有了虚拟机技术，我们可以让一个或多个 RHEL 6 系统专用于某个特定的服务，如 Apache Web 服务器。

实验题 2

在 Red Hat 考试期间，考生不能访问 Internet，但许多安装模式和更新需要访问 Internet 以从 Internet 上下载安装文件和最新程序。

当你配置来自远程系统上的 RHEL 6 DVD 安装盘上的文件时，其效果相当于配置另外一个安装程序包。此外这些文件支持网络安装，这属于 RHCSA 考试要求。

相关操作步骤与 vsFTP 服务器(受 SELinux 保护)的配置有关。不要害怕 SELinux。然而，正如本实验题所显示的那样，vsFTP 服务器的配置非常简单。虽然 SELinux 的使用似乎使考生望而却步，但是它是必考内容。本操作中介绍的命令说明了在 vsFTP 服务器应用 SELinux 功能。第 4 章将讨论如何在其他情形使用 SELinux。

实验题 3

本实验题初看起来非常怪，因为它涉及 Linux 另一个认证的要求。然而，许多 Linux 管理员非常重视 Linux Professional Institute(LPI)的考试。LPI 颁发许多很好的证书。许多 Linux 管理员努力准备 LPIC Level 1(一级)考试，并且通过了考试。通过了 LPIC 101 和 102 考试为参加 RHCSA

和 RHCE 考试建立扎实的基础。

如果你为了在 Linux 方面有一个比较好的基础，可以参阅本章开头介绍的参考书。

Red Hat 考试是一个巨大的挑战。RHCSA 和 RHCE 考试的某些要求看起来很吓唬人的。在目前这个时候，你可能无法理解某些内容，这是可以理解的，这也正是本书的目的。然而，如果对 `ls`、`cd` 和 `cp` 等基本的命令行工具感到力不从心，则你需要先掌握好 Linux 的基本操作。但是许多考生通过自学和实践操作都能顺利跨越这个障碍。



第 2 章

虚拟机与自动安装

认证目标

- ✓ 2.01 配置 Red Hat KVM
- ✓ 2.02 在 KVM 上配置虚拟机
- ✓ 2.03 自动安装选项
- ✓ 2.04 用 SSH 管理系统
- ✓ 2.05 考虑添加命令行工具
- ✓ 小练习
- ✓ 自测题

虽然 RHEL 6 系统安装是 RHCSA 认证目标之一，但是 Red Hat 也宣称他们的考试使用预先安装好的系统。换言之，考生在考试期间不需要在裸机安装 RHEL 6 操作系统。但是，虚拟机的管理和 Kickstart 安装属于 RHCSA 考试要求范围之内，即要求考生通过网络、用手工方法或者借助于 Kickstart 方法在虚拟机上安装 RHEL 6 软件。

第 1 章已讨论了安装过程的基本步骤。这一章假设你在安装过程中同时创建了一个虚拟客户端。但是可能需要在安装结束后安装和配置 KVM。当然，这里假设这个系统使用 64 位的 CPU。

Kickstart 方法是属于 Red Hat 系统的自动安装模式。它从一个文本文件开始读取安装指令。此文件提供了 RHEL 6 安装程序的响应。有了这些响应内容，RHEL 6 安装程序就可以自动执行，不需要用户介入。

当用于测试、学习或服务的系统安装完成后，就可以对它们进行远程管理。掌握 SSH 连接技术不仅是 RHCSA 考试的一个基本要求，也是实际工作中一个卓越的技术。

本书引用的菜单选项都来自 GNOME 桌面工作环境。如果使用其他桌面环境，如 KDE 桌面，则步骤可能会稍有不同。

认证目标 2.01 配置 Red Hat KVM

在第 1 章中，我们使用了安装 VM 所需要的软件包配置了物理的 64 位 RHEL 6 系统。如果其他都失败，则此配置步骤可以帮助你创建 RHEL 6 的多个安装模式。但是如果 RHEL 安装系统没有所需要的程序包，那么该怎么办呢？

有了这些正确的程序包，就可以建立 KVM 模块、访问虚拟机配置命令，并且可以为一组虚拟机创建详细的配置命令。本节介绍的一些命令在某种程度是后面几章内容的预览。但是首先必须讨论这样一个问题：既然真实的物理硬件系统可以触手可得，为什么很多人还想使用虚拟机。

考试内幕

管理虚拟机

RHCSA 考试认证目标要求考生掌握以下内容：

- 访问虚拟机的控制台。
- 启动和退出虚拟机。
- 将系统配置为在系统引导时启动虚拟机。
- 安装 Red Hat 企业版 Linux 系统作为虚拟客户机。

有充足的理由认为讨论中的虚拟机采用了 Red Hat 默认的虚拟机解决方案，即 KVM 解决方案。虽然在第 1 章中已经在 64 位系统的 RHEL 6 安装过程中安装了此解决方案，但是考试可能会要求在真实系统上安装一个相关的程序包。此外，Red Hat 提供了一个虚拟机管理器图形控制台用来管理虚拟机。当然，这个虚拟机管理器工具是命令行工具的一个前端，命令行工具也可以用来安装一个系统。这些工具都可以用来配置系统，使得它在引导过程中可以自动启动。

虽然在第 1 章曾提到，Red Hat 博客建议在预安装系统上进行考试，但是并没有把虚拟机的安装操作排除在考试之外。因此在本章中要学习如何在 KVM 上建立 RHEL 6 的安装模式。

Kickstart 安装方法

RHCSA 认证目标要求考生掌握:

- 用 Kickstart 方法自动安装 Red Hat 企业版 Linux。

为此，每个 RHEL 安装模式都包含一个 Kickstart 文件示例，该文件是以给定的安装模式为基础的。本章将学习如何用这个文件自动完成安装。这比我们想象的要难一些，因为首先要修改 Kickstart 样本文件，暂时不考虑不同系统的独特配置参数。但是系统配置后，你就以此 Kickstart 文件为基线，根据需要生成任意多个 RHEL 安装系统。

访问远程系统

RHCSA 认证目标要求考生掌握以下内容:

- 用 SSH 和 VNC 访问远程系统。

如果系统管理员都要亲自跑到他们所管理的每个系统那里，则他们的大部分时间都要浪费在从这个系统到另一个系统的路上。有了安全壳(Secure Shell, SSH)和虚拟网络计算(Virtual Network Computing, VNC)这样的工具，系统管理员可以远程执行管理操作。本章的重点是 SSH 的使用，而第 9 章的重点则是 VNC 的配置。虽然，SSH 是 RHEL 6 标准配置中自动安装的，但是密码短语(pass-phrases)等个性化配置选项则属于 RHCE 考试范围。

实际经验

警告：基于 KVM 的虚拟机不能用于生产系统。但是本书就是在这样的 RHEL 6 系统完成的。

2.1.1 选择虚拟机的理由

好像每个人都想进入虚拟机这个世界。是的，他们应该进入这个虚拟机世界。过去，许多企业都要为每个服务分配一个不同的专用物理系统。实际上，为了保证系统的可靠性，企业可能为每个服务分配两个或两个以上的系统。当然，也可以在单个系统上实现多个服务。事实上，这正是属于 Red Hat 考试的内容。但是在主要关注系统安全的企业中，为降低风险，多个系统专用于单个服务。

如果系统经过正确的配置，则每个服务都能配置在其专用的虚拟机上。可以在一个本地的物理计算机上安装 10 个虚拟机。由于不同的服务通常在不同的时刻使用内存和 CPU 周期，因此超额分配本地物理系统上的内存和 CPU 资源是一个合理的想法。例如，在一个 8GB 的系统中，经常可以给此系统的 10 个虚拟机各分配 1GB 的内存。

实际上，系统管理员可能用 2 个物理系统代替老式网络上的 10 个物理系统。在每个物理系统上的 10 个虚拟机每个都需要安装两次。当然，这两个物理系统需要功能强大的硬件系统的支持，否则节省的费用是相当可观的。不仅节省了硬件成本，也节省了附加设备费用、能源消耗和其他费用。

2.1.2 假设必须安装 KVM

如果你需要在 RHEL 6 安装任何类型的软件，则 Add/Remove Software 工具可以大显身手。先以普通用户登录到 GUI 环境。为了从 GUI 环境打开这个工具，单击 System | Administration | Add/Remove Software。只要已经与 RHN 网络或第三方重构发行版的程序库建立了正确的连接，

就需要花一些时间进行搜索。在左侧窗格中单击 Virtualization 旁边的箭头，就会出现 4 个虚拟程序包组。单击 Virtualization 程序包级并且选择这个组中的第一个程序包，如图 2-1 所示。

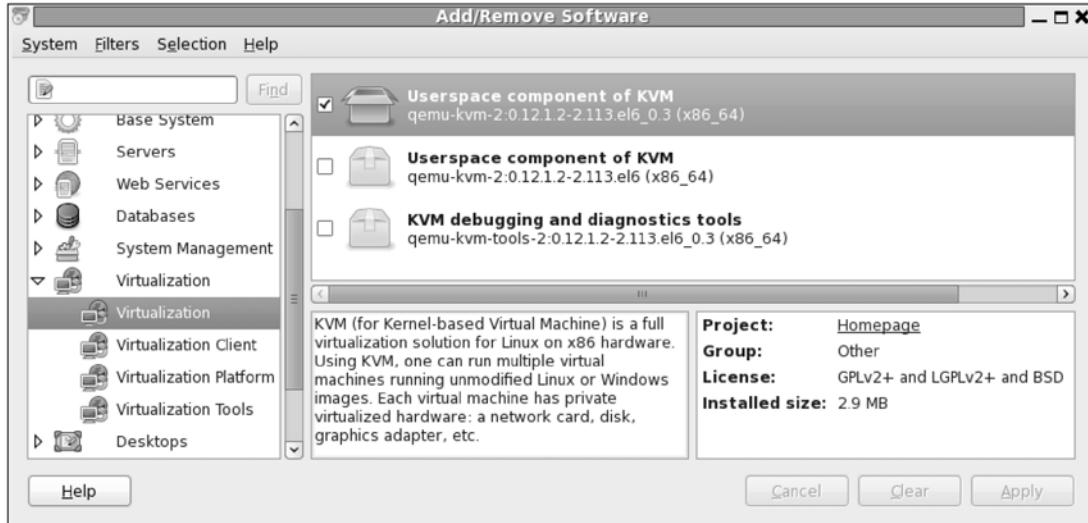


图 2-1 添加/删除软件工具

这里的列表可能过于复杂。在图 2-1 中可以看到 `qemu-kvm` 程序包有两个不同版本。一般而言，只需要最新版本的安装程序包。安装 KVM 程序，你要做的只是从 `Virtualization`、`Virtualization Client`、`Virtualization Platform` 等程序包组中选择合适的程序包，如果不记得如表 2-1 的列表，就选择所有虚拟程序包的最新版本即可。

表 2-1 与虚拟化相关的程序包

程 序 包	说 明
<code>qemu-kvm</code>	主要的 KVM 程序包
<code>python-virtinst</code>	创建虚拟机所需要的命令行工具和程序库
<code>virt-manager</code>	GUI 虚拟机管理工具
<code>virt-top</code>	虚拟机统计命令
<code>virt-viewer</code>	GUI 连接程序，连接到已配置好的虚拟机
<code>libvirt</code>	C 语言工具包，提供 libvirt 服务
<code>libvirt-client</code>	为虚拟客户机提供的 C 语言工具包

这里仅列出 7 个程序包。当然，在大多数配置中还需要依赖于其他相关的程序包。只能在 64 位 CPU 的 RHEL 6 物理系统上配置虚拟机真正所需要的程序包。虽然这些程序包没有一个出现在 `Virtualization Tools` 组中，但是这些程序包可能是实际工作中非常有用的工具，它包括了用于读取和管理虚拟机磁盘镜像文件的工具。如果需要将 Xen 镜像文件转换为 VMware 格式的镜像文件，则可以用 `virt-v2v` 软件包。

用 `Add/Remove Software` 工具安装软件十分容易，只需要选取(或取消)需要安装的程序包并单击 `Apply` 按钮。如果还需要安装它们相关的程序包，则出现一个完整列表，列出这些程序包，让用户选择。当然，在命令行接口要用 `yum install packagename` 命令安装这些程序包。

2.1.3 选择正确的 KVM 模块

在大多数情况下，只要选择了正确的程序包即可。系统会自动加载合适的模块。在 KVM 工作之前，必须加载相关的模块。因此要运行以下命令：

```
# lsmod | grep kvm
```

如果 KVM 模块正确载入，则会看到如下的两组模块：

```
kvm_intel    45578      4
kvm         291875      1 kvm_intel
```

或

```
kvm_amd    35678      4
kvm        261575      1 kvm_amd
```

从模块的名字可以知道，输出结果取决于 CPU 制造商。如果没有看到这个输出信息，则首先要保证已经选择了正确的硬件。正如第 1 章中曾指出，在/proc/cpuinfo 文件中必须有 svm 或 vmx 标志。否则，需要对系统的 BIOS 或 UEFI 菜单进行额外的配置。有些菜单包含了与硬件虚拟技术有关的具体选项，则应该启动这些选项。

如果/proc/cpuinfo 文件有前面提到这两个标志中的一个，下一步的操作是载入可应用的模块。最简单的方法是使用 modprobe 命令，下面这个命令也会载入其他相关的模块，不管系统属于 kvm_intel 或 kvm_amd 结构：

```
# modprobe kvm
```

2.1.4 配置虚拟机管理程序

虚拟机管理器(Virtual Machine Manager)是 virt-manager 程序包的一部分。在 GUI 工具中，可以利用同名的一个命令启动这个程序包。或者在 GNOME 桌面环境中，选择 Applications | System Tools | Virtual Machine Manager 菜单，这个命令会打开如图 2-2 所示的 Virtual Machine Manager 窗口。

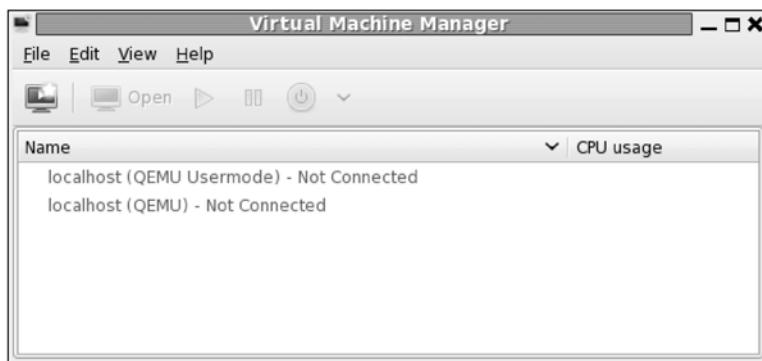


图 2-2 Virtual Machine Manager 窗口

有时候两个超级监视程序(也称为虚拟机监视程序)显示在本地主机系统上。这些超级监视

程序与 QEMU 一起作为虚拟机中的处理器仿真器。QEMU 是快速仿真器(quick emulator)的缩写符。当出现一个用户模式的仿真器时，在 64 位系统上运行一个 32 位应用程序则是可行的，但是效率不高。在大多数情况下，用户都希望用本地主机(QEMU)的正常模式创建和管理虚拟机。

实际经验

在 RHEL 6 发行版中，QEMU 用户模式仿真器存在一个 bug，即 <https://bugzilla.redhat.com> 网上的 bug634876。只要更新 virt-manager 程序包就可以解决这个问题。

1. 连接到超级监视程序(Hypervisors)

需要时也可以远程配置和管理基于 KVM 的虚拟机。所需要的全部操作只是连接到远程的超级监视程序。为此，单击 File | Add Connection，打开 Add Connection 窗口，在这个窗口中选择：

- 超级监视程序(Hypervisor)，通常即 KVM 或 Xen(Xen 是 RHEL 5 的默认超级监视程序，但 RHEL 6 不支持它)。
- 连接可以是本地的，也可以是 SSH 等远程连接。

如果选择远程连接，需要提供远程系统的主机名或 IP 地址。

2. 用超级监视程序进行配置

每个超级监视程序都需要详细配置。右击本地主机(QEMU)超级监视程序，从弹出的菜单中选择 Details，它打开一个以本地系统名字为首 Details 为尾的窗口，如图 2-3 所示。

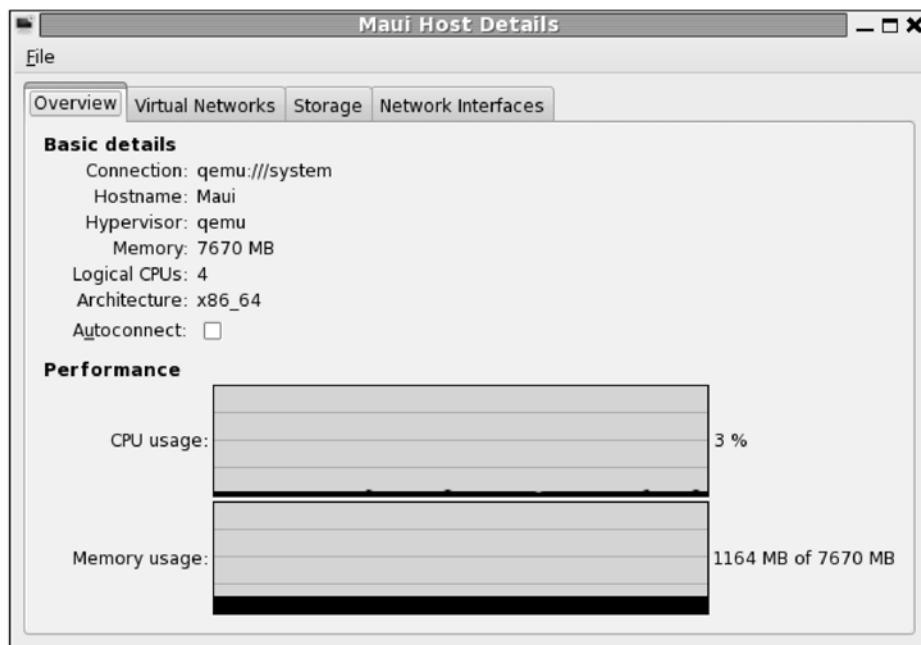


图 2-3 虚拟机主机详细信息

从图 2-3 可以看出，Overview 选项卡列出虚拟机配置的基本参数，这些参数将在表 2-2 中讨论。

表 2-2 虚拟机主机详细参数说明

参 数	说 明
Connection	超级监视程序的统一资源标识符(URI)
Hostname	虚拟机主机的主机名字
Hypervisor	KVM 使用的 QEMU 程序
Memory	物理系统给虚拟机分配的内存大小
Logical CPU	CPU 核的数量, 4 表示 4 个 CPU 或四核系统
Architecture	CPU 的体系结构
Autoconnect	是否在引导过程中自动连接到超级监视程序

接下来继续讨论当前超级监视程序的主机详细窗口。

3. 超级监视程序的虚拟网络

现在我们来分析在虚拟机管理器中为虚拟机配置的网络。在当前超级监视程序的宿主机详细窗口中, 单击 Virtual Networks 标签, 默认的虚拟网络如图 2-4 所示, 它是用超级监视程序创建的虚拟机创建的标准网络。

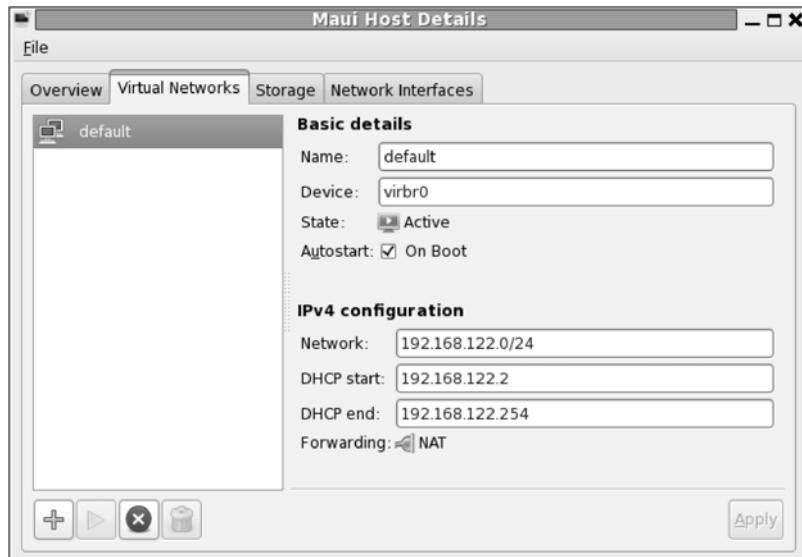


图 2-4 虚拟机主机详细内容

你会注意到, 根据配置, 这个给定的网络在虚拟机引导时会自动启动。因此, 如果在虚拟机上配置了合适的虚拟网卡, 并利用动态主机配置协议(DHCP)的一个客户端命令, 就可以自动从给定的 IP 地址中分配得到一个 IP 地址。从图中可以看到, 这个给定的 IP 地址还可以用网络地址转换技术(Network Address Translation, NAT) 实现转接功能。

利用图中左下角的按钮可以添加新的虚拟网络、启动或停止一个正在工作的虚拟网络以及删除这个网络。练习 2-1 要求建立第二个虚拟网络。第 2.1.6 节将继续用到当前超级监视程序的主机详细窗口。

2.1.5 练习 2-1: 创建第二个虚拟网络

本练习将利用 GUI 虚拟机管理程序在标准 KVM 超级监视程序上创建第二个虚拟网络。这个练习需要一个已经配置好的 RHEL 6 系统, 它是以 RHEL 6 的一个 in-process 安装模式为基础, 并且假设已安装本章前面讨论的虚拟机管理程序。

- (1) 右击标准本地主机(QEMU) 超级监视程序, 在弹出的菜单中选择 Details。
- (2) 在以本地系统名称表示的 Details 窗口中, 选择 Virtual Networks 标签。
- (3) 单击 Virtual Network 标签左下角的加号(+)按钮, 打开 Create A New Virtual Network Wizard。
- (4) 阅读操作指示, 接下来要按照这样指示进行操作。单击 Forward 继续。
- (5) 给新的虚拟网络指定一个名字。本书使用 outsider 名字。单击 Forward 继续。
- (6) 如果还没有输入 IP 地址, 则在 Network 文本框中输入 192.168.100.0/24 IP 地址。系统会自动为其他网络信息计算正确记录, 如图 2-5 所示。单击 Forward 继续。

实际经验

注意, 要防止输入的 IP 地址与本地网上的现有硬件(如路由器或无线接入点的 IP 地址)发生冲突。例如, 至少保留电缆“调制解调器”使用的 192.168.100.1 IP 地址用于维护。此时刚才使用的 192.168.100.0/24 网络地址就会使这个调制解调器专用的 IP 地址无法访问。如果遇到这样的硬件则要改变网络地址, 如图 2-5 所示。



图 2-5 选择 IPv4 地址空间

(7) 现在可以为这个网络选择 IP 地址段, 这个地址可以由一个 DHCP 客户端设定的。在第 1 章的表 1-2 中, 我们为此网络上的 outsider1.example.org 系统分配了一个静态 IP 地址。只要前面提到的 192.168.100.100 这个 IP 地址在 DHCP 可分配的 IP 地址段之外, 就不需要做任何改变。修改后单击 Forward 继续下一步。

(8) 现在, 我们想要得到这样一个系统, 它可以把网络通信量转发给物理网络, 因为这是此网络与其他虚拟网络上的系统或者不同虚拟机进行通信的唯一方法。其目的就是任何工作于

NAT 模式的物理设备可以隐藏这些系统，阻止远程主机看到这些系统。如果我们不把来自虚拟机的路由消息限制到某个特定物理网卡，则“转发到物理网络”这个功能就无法实现。这些选项在本章后面的 Network Interfaces 标签中讨论。做适当的选择后单击 Forward 继续下一步操作。

(9) 仔细核对整个配置过程的操作，如果满意单击 Finish 按钮。现在新建的虚拟机系统和网卡可以使用该 outsider 网络。

1. 超级监视程序的虚拟存储

现在来介绍为虚拟机管理器中的虚拟机配置的虚拟存储空间。在当前超级监视程序的主机详细信息窗口中单击 Storage 标签。在图 2-6 所示的默认文件系统目录中，把 /var/lib/libvirt/images 目录配置为虚拟映像。这样的映像文件实质上是一个非常大的文件，它们从硬盘中保留了存储空间供虚拟机用。

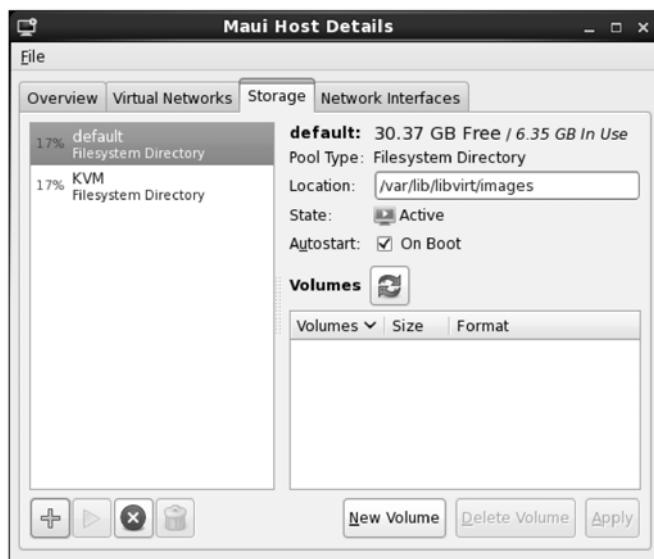


图 2-6 虚拟机存储细节

这些大型文件会很容易摧毁很多系统。控制这些文件的一个办法是给 /var/lib/libvirt/images 目录分配一个专用的分区或逻辑卷。

由于我已经把一个分区的绝大部分可用空间分配给 /home 目录，因此选择在这个目录创建一个专用存储区。为此创建了 /home/michael/KVM 目录，它用来保存虚拟硬盘驱动器所要用到的 VM 文件。

下面的命令首先要以普通用户的身份建立一个目录，然后以 root 用户身份登录到系统，给这个目录设置合适的 SELinux 安全上下文，再删除 /var/lib/libvirt/images 目录，最后重建这个目录并连接到用户的目录上。

```
$ mkdir /home/michael/KVM
$ su - root
# chcon -R --reference /var/lib/libvirt/images /home/michael/KVM
# rmdir /var/lib/libvirt/images
# ln -s /home/michael/KVM /var/lib/libvirt/images
```

这样配置的一个优点是，保留了 /var/lib/libvirt/images 目录的默认 SELinux 配置，这些配置参数是由 /etc/selinux/targeted-contexts/files 目录中 file_contexts 文件定义的。换言之，该配置留存了 SELinux 的 relabel。有关 SELinux 的重新标志(relabel)将在第 11 章介绍。

2. 超级监视程序的虚拟网络接口

现在分析在虚拟机管理程序中为虚拟机配置的虚拟网络接口。在当前超级监视程序的主机详细窗口中单击 Network Interfaces 标签。图 2-7 所示的网络接口设备指定了 KVM 虚拟机可以连接的物理设备。

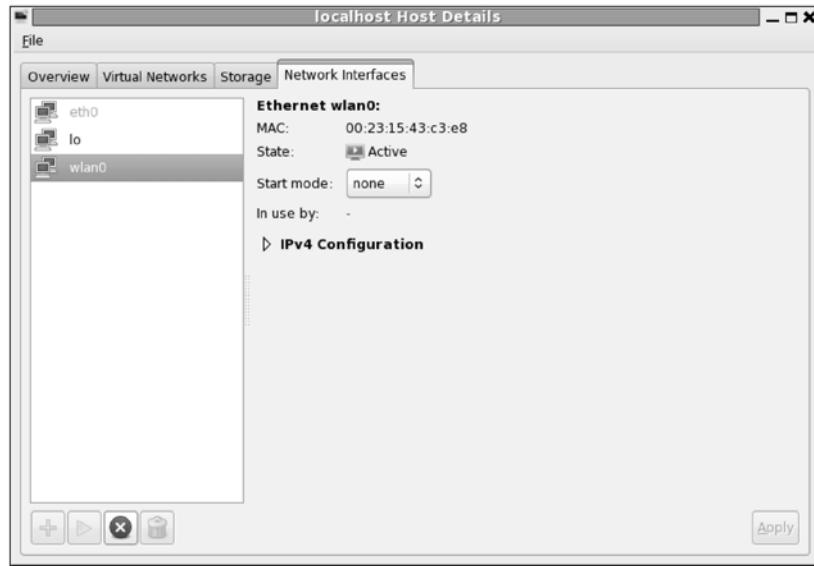


图 2-7 虚拟机网卡

如果本地系统通过第一个标准以太网卡进行连接，则 eth0 设备的默认配置就足够了。一个正确配置的虚拟机即使考虑到第一章提到的防火墙、IP 地址转发选项，也应该能够访问外部网络。图 2-7 还定义了另外一个接口 wlan0。这是典型的无线网络接口的设备文件。

采用与 Virtual Network 和 Storage 标签的相同方法添加另一个网络接口，方法是单击 Network Interface 标签的左下角加号按钮，它打开 Configure Network Interface 窗口，这个窗口可用于配置四种不同类型的网络接口中的任何一个：

- Bridge(桥接)，把一个物理接口与一个虚拟接口绑定在一起，常用于 Xen 中。
- Bond(绑定) 连接两个或两个以上的网络接口，就像它们是一个接口一样。
- Ethernet(以太网方式) 建立一个虚拟接口作为桥接。
- VLAN 把一个真实的或虚拟的网络接口连接到虚拟机上。

认证目标 2.02 在 KVM 上配置虚拟机

在 KVM 上配置一个虚拟机的过程非常简单，特别是使用虚拟机超级监视程序。实质上，

所要做的事情是右击所需要的超级监视程序，再选择 New，然后根据提示进行操作。但是由于理解此过程每个操作步骤非常必要，因此必须仔细阅读这个过程的每一步操作。新创建的虚拟机不仅可以在 GUI 工具中进行配置，也可以在命令行接口中进行配置。与其他 Linux 服务一样，最终得到的虚拟机将在文本文件中进行配置。

2.2.1 在 KVM 上配置虚拟机

按照本节的指示进行操作。打开 GUI 桌面中的虚拟机管理器，也可以从基于 GUI 的命令行中打开，即在命令行中执行 virt-manager 命令。用这种方法比起用 GUI 的菜单命令能更快打开虚拟机管理器。右击本地主机(QEMU)超级监视程序并从弹出的菜单中选择 Connect。如果出现提示，则输入 root 管理员的密码。按下面的操作步骤建立一个虚拟机，并以第 1 章曾提到的 server1.example.com 作为它的域名。现在为新建一个虚拟机执行以下操作：

(1) 右击本地主机(QEMU)超级监视程序，在弹出的菜单中选择 New，打开一个 New VM 窗口(新建虚拟机)，如图 2-8 所示。

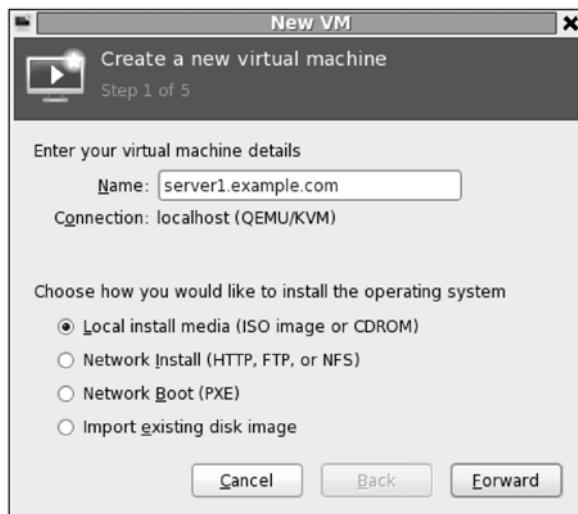


图 2-8 新建一个虚拟机

(2) 为这个新建的虚拟机输入一个名称，为配合本书后面的讨论，必须将这个虚拟机命名为 server1.example.com。

(3) 现在选择安装媒介是来自本地安装媒介(ISO 映像文件或 CDROM)还是来自网络安装服务器。此服务器必须是 HTTP、NFS 或 FTP 协议服务器。选择本地安装媒介，单击 Forward 继续(在实验题 1 中，利用网络安装模式重新执行这个过程)。

(4) 如果可以使用本地 CD/DVD 驱动器，则 Use CDROM or DVD 这个选项处于可选状态，如图 2-9 所示。但是在本例中选择 Use ISO Image 并单击 Browse 按钮导航到 RHEL 6 DVD 所在的位置或网络引导 ISO 映像文件所在的位置。此外，还需要使用 OS Type 和 Version 下拉列表选择一个操作系统类型和版本，如图 2-9 所示。

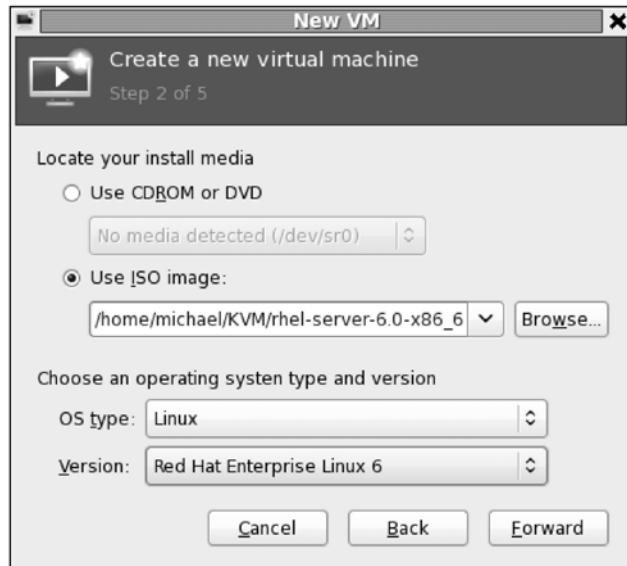


图 2-9 虚拟机安装媒介选项

(5) 给新建的虚拟机分配内存大小和 CPU 数。要注意，本章和第 1 章为 RHEL 6 规定了最低要求。在图 2-10 中，用比较小的字体说明系统可用的内存大小和 CPU 个数，选择合适的选项单击 Forward 继续。

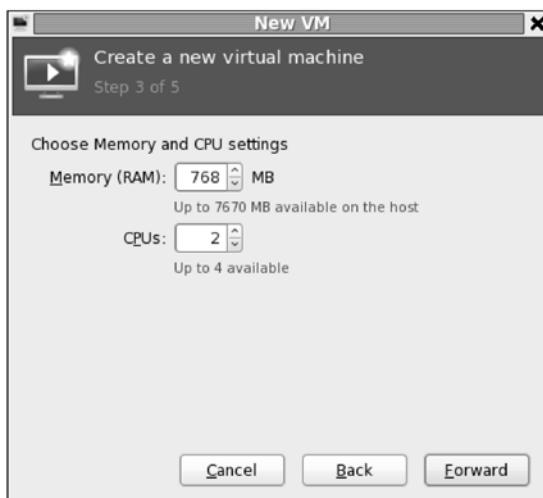


图 2-10 虚拟机的内存和 CPU 选项

(6) 现在为这个虚拟机设置硬盘驱动器，如图 2-11 所示。虽然可以在专用的物理卷中设置一个硬盘，但是标准的做法是将一个大文件创建为虚拟机硬盘驱动器。虽然这些文件的默认位置是 /var/lib/libvirt/images/ 目录，但是正如本章前曾提到的也可以是其他目录。在考试中，/var/lib/libvirt/images 目录空间很可能远大于实际需要。图 2-11 中的 Select managed or other existing storage(选择可管理存储空间或其他现有的存储空间)选项会在另外一个预配置的硬盘池中创建一个虚拟驱动器。

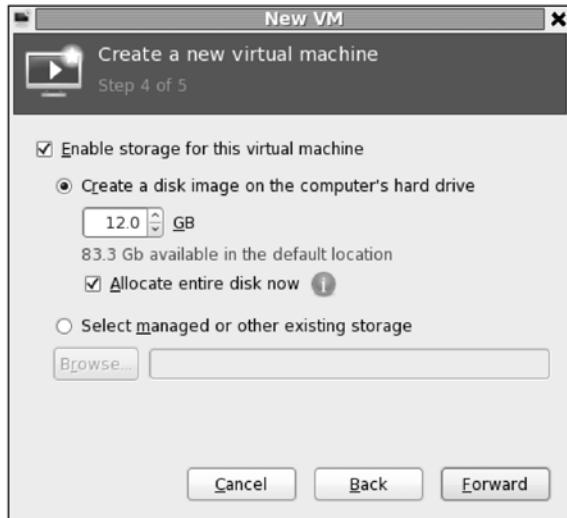


图 2-11 建立一个虚拟硬盘驱动

(7) 确保虚拟驱动器大小为 12GB，并且选择 Allocate entire disk now 选项，单击 Forward 继续。

(8) 在下一个窗口中确认前面所执行的全部选择。单击 Advanced Option 打开如图 2-12 的选项。

我们可能还需要选择可用的虚拟网络。如果完成了练习题 2-1，则 192.168.100.0/24 网络地址选项应该会出现在这个列表中。

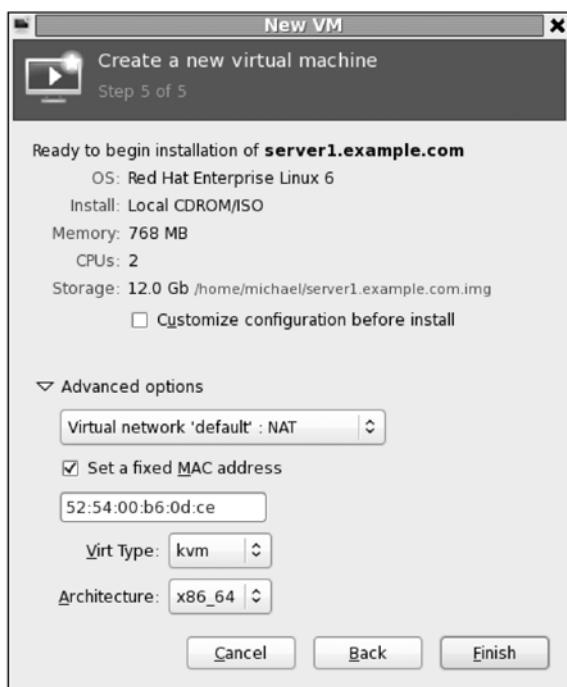


图 2-12 建立一个虚拟硬盘驱动器

(9) 系统创建这个虚拟机可能需要花一点时间，此过程包括分配一个大型文件作为虚拟机硬盘。当创建过程完成时，虚拟机管理器会自动在 VNC 窗口中从 RHEL 6 安装 DVD 启动这个新建的虚拟系统。

(10) 如果新创建的系统不能自动启动，则此虚拟机会出现在图 2-2 所示的虚拟机管理器的窗口中。现在可以选取这个新建的虚拟机(本例中它的名字就是 server1.example.org)，单击 Open。

(11) 现在继续在这个虚拟机中开始安装 RHEL 6。

如果在安装过程中想要验证 DVD 安装文件的完整性，则安装程序会弹出此 DVD。但是 KVM 并不承认这个“弹出”动作，此时需要单击 View | Details，然后选择 IDE CDROM1 选项，单击 Disconnect，再单击 Connect。在出现的 Choose Media 窗口中选择合适的文件，是 DVD ISO 映像文件或 CDROM 作为物理媒介。

(12) 在选择软件时，需要注意的是本系统是一个虚拟客户机，而不是第 1 章配置的虚拟主机，因此在安装过程中不需要添加任何虚拟程序包。在虚拟机上使用主机上的基本服务器足够了，但是需要添加桌面、字体、X Window 系统和 Internet 浏览器等程序包组。

(13) 当安装完成后，单击 Reboot。如果系统又要从 DVD 盘上启动，则需要交换 DVD 和硬盘的引导顺序。如果系统可以直接从硬盘引导，则安装过程结束。

(14) 如果系统要从 DVD 引导，则需要关闭此系统，为此要单击 Virtual Machine | Shut Down | Force Off(现在 Shut Down | Shut Down 命令不起作用)。

(15) 如果这是第一次执行这个命令序列，则虚拟机管理器会出现提示信息要求你确认，单击 Yes。

(16) 现在单击 View | Details 命令。

(17) 在左侧的窗格中选择 Boot Options(引导选项)，如图 2-13 所示。

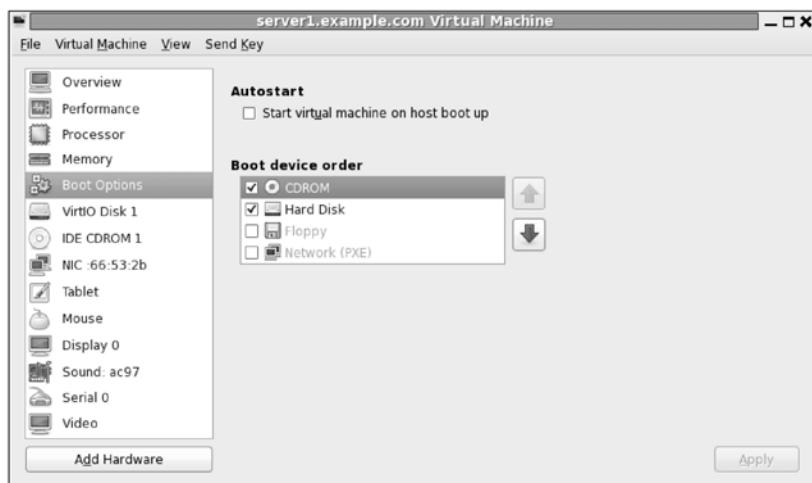


图 2-13 虚拟机的引导选项

(18) 改变引导顺序的另外一个办法是高亮显示 CDROM，然后单击向下箭头按钮。单击 Apply，否则不会保存所做的修改。

(19) 单击 View | Console，再单击 Virtual Machine | Run，系统会自动引导到第 1 章曾介绍过的第一引导(First Boot)进程。

使用虚拟机另外一个理由是可以多添加几个虚拟硬盘驱动器。该过程因虚拟机方案的不同而异。在 RHEL 6 中，如果使用默认的虚拟解决方案即 KVM 解决方案，则单击 View | Details 命令并从出现的机器窗口中进行这个操作。在这个窗口中会看到 Add Hardware 选项。

考试经验

本节介绍的步骤说明了如何实现访问虚拟机的终端的 RHCSA 认证目标，也提出了一种可用于启动虚拟机和禁用虚拟机的方法。

2.2.2 练习 2-2：添加虚拟硬盘驱动器

本练习要在基于 KVM 的虚拟机上创建另外一个虚拟硬盘驱动器。假设现有一个 KVM 虚拟机用于此目的，并使用了一个 GUI 虚拟机管理器。当然，既然是 KVM，这就表示该本地物理系统支持硬件虚拟化。

- (1) 打开虚拟机管理器。从 GUI 的命令行输入 virt-manager 命令。
- (2) 选择普通的本地(QEMU)超级监视程序。如果还没连接到，则右击它并从弹出的菜单中选择 Connect。这一步可能会自动操作。
- (3) 如果出现提示窗口，就输入 root 管理员的密码并单击 Authenticate 按钮。
- (4) 右击一个现有的虚拟机，从弹出的菜单中单击 Open。
- (5) 单击 View | Details，在出现窗口的左下角单击 Add Hardware。
- (6) 在出现的 Add New Virtual Machine 窗口中，从下拉菜单中选择 Storage，然后单击 Forward 继续。
- (7) 在出现的 Storage 窗口中，如图 2-14 所示。设置一个 1.0GB 的硬盘，选择 Allocate entire disk now 这个选项，再选择 IDE 设备类型，从 Cache 模式选择默认值(设备类型也可以选择 SCSI、USB 或虚拟硬盘)。



图 2-14 Storage 窗口细节

- (8) 将出现一个所选择配置的窗口。如果符合要求，单击 Finish 将创建一个新的虚拟硬盘驱动器。

(9) 重复前面的步骤创建第二个 1GB 虚拟硬盘。为了更好地了解 KVM，最好设置另一类型的硬盘如 SCSI 硬盘，但这不是必需的。

(10) 下次启动这个系统时，从启动账户中执行 `fdisk -l` 命令，可以确认刚配置的虚拟硬盘设备。

2.2.3 KVM 配置文件

基于 KVM 的虚拟机通常配置在两个不同的目录中：`/etc/libvirt` 和 `/var/lib/libvirt`。当一个 KVM 虚拟机配置好后，就会在 `/etc/libvirt/qemu` 目录中生成 xml 格式的文件。例如，图 2-15 就是来自 VMI 配置文件的一段内容，此虚拟机是用来准备本书内容的(`server1.example.com.xml`)。

虚拟机的重要参数已经标注出来。例如，内存的大小用 KB 表示，分配了两个虚拟 CPU，KVM 是仿真器，硬盘可以在 `/var/lib/libvirt/images` 目录中的 `server1.example.com.img` 文件中找到等。

虽然可以直接对这个配置文件进行编辑，但是在用 `/etc/init.d/libvirtd restart` 命令重新启动 `/etc/init.d` 目录中的 `libvirtd` 脚本之前，对此文件所做的修改不会实现。

2.2.4 从命令行控制虚拟机

当然，命令行工具也可以用来创建、克隆、转换和安装 RHEL 6 上的虚拟机。为此要用到关键命令有 `virt-install`、`virsh` 和 `virt-clone`。`virsh` 是一个非常有用的命令，可用来实现 RHCSA 两个不同的认证目标。

1. `virt-install` 命令

使用虚拟机管理器可以执行本章前面介绍的操作。只需要使用 `virt-install - prompt` 命令。此命令自动提示用户输入前面提到所需要的信息。分析图 2-16 中的命令和提示信息。

```
<domain type='kvm'>
  <name>server1.example.com</name>
  <uuid>d60a8c0a-d795-c0fc-893f-174ac0f37f6e</uuid>
  <memory>786432</memory>
  <currentMemory>786432</currentMemory>
  <vcpu>2</vcpu>
  <os>
    <type arch='x86_64' machine='rhel6.0.0'>hvm</type>
    <boot dev='hd' />
    <boot dev='cdrom' />
  </os>
  <features>
    <acpi />
    <apic />
    <pae />
  </features>
  <clock offset='utc' />
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/libexec/qemu-kvm</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='raw' cache='none' />
      <source file='/var/lib/libvirt/images/server1.example.com.img' />
      <target dev='vda' bus='virtio' />
      <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0' />
    </disk>
    <disk type='file' device='cdrom'>
      <driver name='qemu' type='raw' />
      <source file='/var/lib/libvirt/images/rhel-server-6.0-x86_64-boot.iso' />
      <target dev='(hdc)' bus='ide' />
      <readonly />
      <address type='drive' controller='0' bus='1' unit='0' />
    </disk>
  </devices>
</domain>
```

图 2-15 KVM 虚拟机的配置文件内容

```
[root@Maui ~]# virt-install --prompt
What is the name of your virtual machine? tester1.example.com
How much RAM should be allocated (in megabytes)? 768
What would you like to use as the disk (file path)? /home/michael/KVM/tester1.example
.com.img
How large would you like the disk (/home/michael/KVM/tester1.example.com.img) to be (
in gigabytes)? 12
What is the install CD-ROM/ISO or URL? ftp://192.168.122.1/pub/inst

Starting install...
Retrieving file .treeinfo... | 3.3 kB 00:00 ...
Retrieving file vmlinuz... | 7.2 MB 00:00 ...
Retrieving file initrd.img... | 57 MB 00:00 ...
Allocating 'tester1.example.com.img' | 12 GB 00:00 ...
Creating domain... | 0 B 00:00
Domain installation still in progress. You can reconnect to
the console to complete the installation process.
```

图 2-16 用 virt-install 命令配置一个虚拟机

对于许多人来说，这比配置 GUI 虚拟机管理器要简单许多。图 2-16 末尾的消息(即从 Creating domain…开始的信息) 启动一个 VNC 窗口，它显示这个给定安装程序的图形视图。

考试提示

virt-install 命令是实现 RHCSA 认证目标即“把 Red Hat 企业版 Linux 系统安装成虚拟客户机”的一个重要方法。

如果使用 virt-install 命令时出现错误，则按下 CTRL+C 放弃安装。但是要注意，刚创建的虚拟机仍在运行。现在该虚拟机有一个配置文件和虚拟硬盘。如果对同一个虚拟机重新执行 virt-install 命令，则会出现一个错误信息。因此如果确实想使用同名的虚拟机，则必须执行以下步骤：

(1) 停止刚创建虚拟机。对于如图 2-16 所示的 tester1.example.com 系统，则可以用下面的命令终止它的运行：

```
# virsh destroy tester1.example.com
```

(2) 删除/etc/libvirt/qemu 目录相关的 XML 配置文件。对于给定的系统名称，这个文件名是 tester1.example.com.xml。

(3) 需要时也可以删除虚拟硬盘文件，此文件通常建立在/var/lib/libvirt/images 目录中。但如果这个文件具有可接受的大小，这并非必需，因为它是可以重用的。对于这个给定的虚拟系统名字，这个文件名是 tester1.example.com.img。

(4) 用下面的命令重新启动虚拟机守护进程(daemon)，从内存中删除 tester1.example.com 系统：

```
# /etc/init.d/libvirtd restart
```

(5) 现在可以在同名的虚拟机上执行 virt-install 命令。

2. virt-install 命令与 Kickstart 安装方法

对于本章后面将要介绍的 Kickstart 安装方法，不能用 virt-install--prompt 命令引用一个 Kickstart 配置文件。为此需要先理解 virt-install 命令的几个重要的开关选项，如表 2-3 所示。

表 2-3 virt-install 命令的开关选项

开关选项	说 明
-n(--name)	给虚拟机设置一个名字
-r(--ram)	给虚拟机设置内存空间(单位为 MB)
--disk	定义虚拟硬盘, 常与 path=/var/lib/libvirt/images/virt.img 一起使用
-l(--location)	指定安装文件的目录或 URL 地址(与--location 等效)
-x(--extra-args=)	包含额外的数据, 如 Kickstart 文件的 URL 地址

例如, 下面的 virt-install 命令从名为 ks1.cfg 的 Kickstart 文件自动安装得到一个名为 outsider/.example.org 的系统。ks1.cfg 文件来自于给定 IP 地址的 FTP 服务器。新创建的系统需要 734MB 的内存和一个地址为 outsider1.example.org.img 的虚拟硬盘。

```
# virt-install -n outsider1.example.org -r 768 --disk \
path=/var/lib/libvirt/images/outsider1.example.org.img \
-l ftp://192.168.122.1/pub/inst \
-x "ks=ftp://192.168.122.1/pub/ks1.cfg"
```

如果在由前面的基于 KVM 安装得到的个性化 Kickstart 文件上执行 virt-install 命令则可能会失败。标准的基于 KVM 的安装方法在/dev/vda 设备上配置第一个虚拟硬盘。相反, virt-install 命令假定第一个虚拟硬盘位于/dev/sda 设备上。为解决这个差别, 需要对本章后面要介绍的 Kickstart 文件进行修改。

前面提到的配置文件包含许多开关选项。绝大多数这些开关选项的用法在 virt-install 命令 man 手册的例子中得到详细说明。只有-x 例外, 它是--extra-args=开关的另一种形式。你可能还会注意到另外几个的开关选项, 它们可能有用, 但是在 RHEL 6 安装中不需要。但是, 它们可用来查找某个给定的 Kickstart 文件。因此要记住这个额外参数的格式, 它要用引号表示如下:

```
--extra-args="ks=ftp://192.168.122.1/pub/ks1.cfg"
```

3. virsh 命令

virsh 命令启动现有 KVM 虚拟机的一个前端。当它单独使用时, 它会把普通的命令行格式转换为以下提示符的格式:

```
virsh #
```

在这个提示符后输入 help 命令, 它显示几个命令的用法, 其中一部分命令如表 2-4 所示。并非所有 help 命令的输出结果在 KVM 中都有效。那些可用的 virsh 命令都能直接在 bash shell 提示符后运行。例如, virsh list --all 命令列出全部配置好的虚拟机, 不管它们当前是否正在运行。在 KVM 环境中, 每个虚拟机的名字都是一个域, 该域供不同的 virsh 命令使用。

表 2-4 在 virsh 提示符后可以执行的命令

virsh 命令	说 明
autostart<domain>	在主机系统的引导过程中启动一个域
capabilities	列出本地超级监视程序的全部功能
edit<domain>	编辑这个域的 XML 格式的配置文件

(续表)

virsh 命令	说 明
List--all	列出全部域
start<domain>	启动给定的域
shutdown<domain>	“优雅”地关闭给定的域

我在自己的系统上执行 virsh --list all 命令，以下是该命令的执行结果：

```
Id Name           State
-----
- server1.example.com shut off
- tester1.example.com shut off
```

掌握 virsh 命令的正确使用可以实现 RHCSA 的两个认证目标。第一，下面的命令启动前面提到的 server1.example.com 系统：

```
# virsh start server1.example.com
```

不幸的是，virsh shutdown 命令在编写本书的时候还不能起作用。因此为了从命令行终止一个虚拟机的运行，必须使用一个较复杂的命令：

```
# virsh destroy server1.example.com
```

virsh destroy 命令开关选项在功能上等效于拔掉物理系统的电源线。由于这个操作可能会产生不同的问题，因此终止一个虚拟机运行的最好办法是在虚拟机内使用 poweroff 命令。

实际经验

shutdown 命令在 Kickstart 配置文件中可以在命令行中关闭一个系统，而 poweroff 属于功能指令(functional 命令)。

即使在最安全的系统中，电源故障也时有发生。内核更新需要系统重新启动。这时在虚拟主机的启动过程中虚拟机能够自动启动是非常有用的方法。

此外，virsh 命令是确保一个虚拟机在下次系统启动时自动启动最简单的方法。例如，下面的命令保证在主机系统过程中启动前面提到的 tester1.example.com 系统。

```
# virsh autostart tester1.example.com
```

只有当主机系统和虚拟机系统的启动过程都完成后，才可以用 ssh 命令正常连接到虚拟机系统。但在虚拟主机的 GUI 中，仍然还要启动虚拟机管理器，并连接到相应的管理程序(Hypervisor)，才可以连接到 tester1.example.com 系统的虚拟终端。

此命令在 /etc/libvirt/qemu/autostart 目录建立一个软链接文件。要反向此过程需要执行下面的命令：

```
# virsh autostart --disable tester1.example.com
```

或者从这个目录中删除目标虚拟机名后面的软链接文件。

考试提示

为启动和关闭一个虚拟机，可以使用 `virsh start vmname` 和 `virsh destroy vmname` 这两个命令，命令中的 `vmname` 表示虚拟机名。虚拟机名可以从 `virsh list all` 命令的输出结果看出。

4. virt-clone 命令

`virt-clone - prompt` 命令可以克隆一个现有的虚拟机系统。在开始克隆操作之前，必须先关闭需要克隆的系统。它的用法非常简单。图 2-17 是其中一个示例，它从 `server1.example.com` 系统克隆得到 `tester1.example.com` 系统。

```
[root@Maui ~]# virt-clone --prompt
What is the name of the original virtual machine? server1.example.com
What is the name for the cloned virtual machine? tester1.example.com
What would you like to use as the cloned disk (file path) for '/var/lib/libvirt/images/server1.example.com.img'? /var/lib/libvirt/images/tester1.example.com.img
What would you like to use as the cloned disk (file path) for '/var/lib/libvirt/images/server1.example.com-1.img'? /var/lib/libvirt/images/tester1.example.com-1.img
What would you like to use as the cloned disk (file path) for '/var/lib/libvirt/images/server1.example.com-2.img'? /var/lib/libvirt/images/tester1.example.com-2.img
Allocating 'tester1.example.com.img' | 12 GB 01:23
Allocating 'tester1.example.com-1.img' | 1.0 GB 00:01
Allocating 'tester1.example.com-2.img' | 1.0 GB 00:01
Clone 'tester1.example.com' created successfully.
[root@Maui ~]#
```

图 2-17 克隆一个虚拟机

克隆过程一旦完成，不仅会在指定的目录中找到前面提到的硬盘驱动映像文件，而且还会在 `/etc/libvirt/qemu` 文件中找到此虚拟机的一个新的 XML 格式的配置文件。

首次引导一个克隆得到的虚拟机时，最好在运行级 1 引导这个虚拟机。第 5 章将详细说明运行级 1 不会启动很多的服务，甚至不会启动网络连接。此时，可以修改任何给定的网络配置参数，如在生产式网络上的主机名和 IP 地址。此外，需要确保所做的修改是针对相关的网卡，这样可以避免对原来网卡产生冲突。

虽然用这种方法克隆一个或两个虚拟机并不困难，但是想象一下克隆几十个虚拟机，而它们后来都需要配置为不同服务的情况。此时如果有更多的自动操作，则过程会更加简单。为此，Red Hat 提供了一个名为 Kickstart 的系统。

认证目标 2.03 自动安装选项

Kickstart 是 Red Hat 为自动安装 RHEL 提供的一个解决方案。我们把安装过程中每一步执行的操作看作是一个问题。有了 Kickstart，就可以用一个文本文件自动得到这些问题的回答。此外还可以很快地设置相同的系统。因此，Kickstart 文件可以用于 Linux 系统的快速部署和发布。

此外，安装过程正好是一个更好学习 RHEL 6 的机会，不仅学习有关引导媒介的知识，还可以学习在安装完成后有关分区、逻辑卷的配置。由于虚拟机的出现，在 Kickstart 的帮助下，在一个新建的虚拟机上实现自动安装不再是一件困难的事。

本节所提到的步骤假定第 1 章的实验题 2 创建和配置了与 FTP 服务器连接的 RHEL 6 安装文件。

2.3.1 Kickstart 基本原理

在执行 Kickstart 安装时，遇到的一个问题是，它并没有包含基本安装完成后的用户自定义设置。尽管可以把这些参数包括在安装后的脚本中，但是这已超了 RHCSA 考试的范围。

有两个方法可以创建所需要的 Kickstart 配置文件：

- 从 root 用户的主目录/root 下的文件 anaconda-ks.cfg 文件开始。
- 利用 system-config-kickstart 命令启动图形模式的 Kickstart Configurator(Kickstart 配置程序)。

第一个方法允许我们使用由 Anaconda 为本地系统创建的 Kickstart 模板文件，即保存在/root 目录中的 anaconda-ks.cfg。第二个方法即 Kickstart Configurator 将在本章后面详细讨论。

为不同系统定制 anaconda-ks.cfg 文件相对比较容易。后面我们就要介绍如何为不同的硬盘空间大小、主机名字和 IP 地址以及其他参数定制这个文件的内容。

考试经验

最好的办法是经常浏览 <https://bugzilla.redhat.com> 上的内容，及时了解这些关键程序存在的 bug，这对于 Kickstart 尤为重要。例如，bug 624536 说明基于 NFS 的 Kickstart 安装存在很多问题。虽然这个 bug 已被 bug 602455 替代，但是这些问题仍然还存在。

2.3.2 设置对 Kickstart 的本地访问

当 Kickstart 文件配置好后，我们就可以把它安装在 USB Key、CD、空闲的分区甚至软盘等本地媒介上。(不要笑，许多虚拟机系统包括 KVM 使虚拟软盘驱动器的使用更容易)。为此按照下面的基本步骤进行操作：

- (1) 根据需要配置并编辑 anaconda-ks.cfg 文件，稍后将详细介绍这步操作。
- (2) 挂载用到的本地媒介。你可能需要以 root 用户的身份运行 fdisk -l 命令以识别正确的设备文件。如果驱动器不能自动挂载，可以用 mount /dev/sdb /mnt 命令挂载驱动器。
- (3) 把 Kickstart 文件复制到刚挂载的本地媒介上，并命名为 ks.cfg(其他名字也可以，ks.cfg 只是 Red Hat 文档中最常用的一个文件名)。
- (4) 确保 ks.cfg 文件对所有用户至少拥有读权限。如果 SELinux 在本地系统中已启动，则安全上下文通常与同一个目录中的其他文件相匹配。更多信息请参考第 4 章。

注意，在 FTP 服务器上一个 Kickstart 配置文件可能存在安全上的风险。它就像是一个系统的 DNA。如果怪客得到这个文件，他就可以用该文件建立这个系统的副本，研究如何闯入这个系统并且修改这个系统的数据。由于此文件通常包含 root 系统管理员密码，因此在系统第一次启动时需要修改这个密码。

实际经验

使用 Kickstart 配置文件时必须格外小心。除非 root 用户直接登录被禁用，否则此文件肯定包含有 root 管理员的密码。如果此密码已加密，则怪客用合适的工具和这个 Kickstart 配置文件的一个副本就可以用比我们预想的更快的速度来破解这个密码。

- (5) 现在可以在不同的系统使用这个 Kickstart 媒介。稍后要在后面的一个练习中执行此操作。

(6) 现在尝试访问本地媒介上的 Kickstart 文件。启动 RHEL 6 安装 CD/DVD。当第一个菜单出现时，选择 **Install Or Upgrade An Existing System** 并按下 Tab 键。肯定会出现如下的命令给 Anaconda 安装管理程序。光标会出现在该命令后的末尾。

```
vmlinuz initrd=initrd.img
```

(7) 在此命令行的末尾添加 Kickstart 文件的位置信息，例如，下面添加的信息表示此文件保存在第二个硬盘驱动器的第一个分区上，此硬盘可能是 USB 驱动器。

```
ks=hd:sdb1:/ks.cfg
```

或者，如果 Kickstart 文件保存在引导 CD 上，则添加以下命令：

```
ks=cdrom:/ks.cfg
```

或者，如果 Kickstart 文件保存在第一个软盘驱动器上，则输入下面的位置信息：

```
ks=hd:fd0:/ks.cfg
```

这种方法需要不断尝试，可能会有错误。确实，设备文件是按顺序分配名字(sda、sdb、sdc 等)。然而，除非我们用给定的存储媒介引导 Linux，否则无法确定哪个设备文件指定给一个特定的设备驱动器。

2.3.3 建立 Kickstart 的网络访问

在本地媒介上创建一个 Kickstart 文件会很耗时间，特别是为了装载这个文件需要不断从这个系统跑到另一个系统。通常情况下，在网络服务器上建立 Kickstart 文件效率会比较高。一个符合逻辑的位置是安装文件所使用的同一个网络服务器。例如，根据第 1 章实验题 2 创建的 FTP 服务器，假定有一个 ks.cfg 文件保存在这个 FTP 服务器的 /var/ftp/pub 目录中。而且，SELinux 上下文必须与此目录的上下文相匹配，这可以用下面的命令得到验证：

```
# ls -Zd /var/ftp/pub
# ls -Z /var/ftp/pub
```

当 /var/ftp/pub 目录中有一个合适的 ks.cfg 文件，我们就可以在前面第 6 步用到的 vmlinuz initrd=initrd.img 命令行末尾添加如下的指示符：

```
ks=ftp://192.168.122.1/pub/ks.cfg
```

同样的选项也适用于保存在 NFS 或 HTTP 服务器上的 Kickstart 文件，如下所示：

```
ks=nfs:192.168.122.1/ks.cfg
ks=http://192.168.122.1/ks.cfg
```

但如果前面提到的 Bug 624536 还没有解决，则不能在 NFS 上共享 Kickstart 文件。

如果在本地网络上有一个可操作的 DNS 服务器，则可以把此目标服务器的主机或完全限定域名代替前面的 IP 地址。

实际经验

Red Hat 正努力简化基于 Kickstart 安装服务器的创建过程。更多信息请访问 <https://fedorahosted.org/cobbler/> 中的 Cobbler 项目。

2.3.4 示例 Kickstart 文件

本节内容是以我在基于 KVM 的虚拟机上安装 RHEL 6 时生成的 anaconda.cfg 文件为基础，增加了一些注释。虽然可以将此文件当作示例使用，但是必须根据自己的硬件和网络进行定制。本节只是简要介绍 Kickstart 文件的处理过程。你自己的 Kickstart 文件可能会不一样。

考试提示

不同于 Red Hat 的 其他程序包可用的文档，在 RHEL 6 系统中可用的 Kickstart 文档非常少。换言之，在考试中考生无法从 /usr/share/doc 目录中的 man 页面或文件得到任何帮助。当考生不能确定某个命令是否包括在 Kickstart 文件中时，可以参考本章后面要介绍的 Kickstart Configurator。

虽然大多数选项都不言自明，但我还是要在此文件中给每个命令加上注释。这个文件只说明一小部分可用的命令。有关此文件每个命令的详细用法可以阅读最新的 RHEL 6 安装指南，它可以从 <http://docs.redhat.com/docs/en-US> 下载。

在创建 Kickstart 文件时要遵循下面的基本规则和指示：

- 通常情况下要保持指示符的顺序不变，但有时根据是用本地媒介还是用网络进行安装发生少许变化也是可以的。
- 不需要使用全部选项发生少许变化也是可以的。
- 如果遗漏了一个必需的选项，系统会提示用户输入。
- 不要害怕修改，例如，默认情况下与分区有关的指示符都已被注释掉。
- 允许换行。

实际经验

如果遗漏了一个选项，安装过程会停下来。通过这种办法很容易检查 Kickstart 文件是否正确配置。但是由于 Kickstart 选项要改变硬盘上的分区，甚至这些选项的测试可能会存在风险。因此，最好在一个测试系统上测试 Kickstart 文件，或者更好的办法是在一个专用的测试虚拟机上进行测试。

下面是来自我的 anaconda-ks.cfg 文件之一中的代码。前两行是注释，说明此文件是在 RHEL 6 的安装过程中创建的。

```
# Kickstart file automatically generated by anaconda.
#version=RHEL6
```

第一个命令很简单，它启动安装过程。默认使用第一个可用的本地媒介，本例中即第一个 RHEL 安装 DVD/CD 或 USB Key。

```
install
```

下一个命令是指定安装文件的源。如果使用 RHEL DVD 则输入 cdrom。如果使用 NFS 服

务器进行安装，则还要指定 URI 如下。如果在本地网络有可用的 DNS 服务器，可以把 IP 地址替换为服务器的域名。

```
nfs --server=192.168.122.1 --dir=/inst
```

此外，替换上述中的一个命令还可以配置到 FTP 或 HTTP 的一个连接。这里要指定的是在第 1 章创建的 FTP 和 HTTP 安装服务器上的目录。

```
url --url http://192.168.122.1/inst
```

或

```
url --url ftp://192.168.122.1/pub/inst
```

如果代表 RHEL 6 DVD 的 ISO 文件保存在本地的硬盘分区上，则也可以指定这个文件。例如，下面的指示符指向/dev/sda10 分区上的 ISO CD 或 DVD。

```
harddrive --partition=/dev/sda10 --dir=/home/michael/
```

`lang` 命令指定在安装过程中使用的语言。当此文件遗漏了某个命令而引起安装终止，则此命令就非常有用。`keyboard` 命令顾名思义，因为它指定了配置本系统所使用的键盘：

```
lang en_US.UTF-8
keyboard us
```

如果本地网络中有一个 DHCP 服务器，则 `network` 命令是必需的，也是最简单的：`network --device eth0 --bootproto static`。反之，下面的命令配置静态 IP 地址，同时设置了掩码地址(--netmask)、网关地址(--gateway)，DNS 服务器(--nameserver)和计算机名字(--hostname)。

```
network --device eth0 --bootproto static --ip 192.168.122.150 --netmask
255.255.255.0 --gateway 192.168.122.1 --nameserver 192.168.122.1 --hostname
tester1.example.com
```

注意，`network` 命令的全部选项都必须在同一行中，当选项超过文本编辑器的空间时换行是允许的。如果为另一个不同的系统中创建这个文件，不要忘了对 IP 地址和主机名做相应修改。注意，如果在安装过程没有配置网络，则网络信息不会保存到对象 `anaconda-ks.cfg` 文件中。由于 `network` 指示符的复杂性，可以用 Kickstart Configurator 设置该指示符，或者在安装完成后设置网络。

由于 `root` 用户的密码是 RHEL 6 安装过程的一部分，因此 Kickstart 配置文件可以用加密形式指定 `root` 用户的密码。虽然加密并不是必需的，但是它至少可以拖延系统安装完成后怪客想闯入系统的时间。由于相关的密码哈希函数与/etc/shadow 文件所用的相同，因此可以从这个文件复制所需要的密码：

```
rootpw --iscrypted $6$5UrLfXTk$CsCW0nQytrUuvycuLT317/
```

为安全起见，建议启用防火墙指示符。当它与`--service=ssh` 一起使用时，根据它在/etc/service 文件中的定义方式可以指定一个穿过防火墙的服务器端口。

```
firewall --service=ssh
```

接着，authconfig 命令设置了影子密码程序组(Shadow Password Suite)(--enableshadow)，并为密码加密设置了 512 位的 SHA 加密算法(--passalgo=sha512)，以及用指纹识别器进行身份验证。用 SHA512 算法加密的密码是从\$6 开始，如 root 管理员密码所示。

```
authconfig --enableshadow --passalgo=sha512
--enablefingerprint
```

selinux 指示符可以设置为--enforcing、--permissive 或--disable 等值：

```
selinux --enforcing
```

timezone 指示符与时区设置的长列表有关。tzdata 程序包的文档中有时区设置的详细说明。对列表的全部内容执行 rpm -ql tzdata 命令。默认情况下，Red Hat 使用--utc 开关选项把硬件时钟设置为格林威治标准时间。该设置支持夏令时的自动转换。下面这个设置可以在/usr/share/zoneinfo 目录中的一个子目录和文件中找到。

```
timezone America/Los_Angeles
```

默认的引导装载程序是 GRUB，通常它必须安装在硬盘的主引导记录中(Master Boot Record, MBR)。插入--driveorder 开关选项指定安装有引导装载程序的驱动器，用--append 开关选项指定启动内核的命令。虽然给定的开关选项 crashkernel=auto 保证系统崩溃时能自动选择可用的内容，但是 RHEL 6 的早期报告建议你需要将其替换为像 crashkernel=128M@16M 那样的指定内存位置。

```
bootloader --location=mbr --driveorder=vda
--append="crashkernel=auto rhgb quiet"
```

指示符后面的注释表明，最重要的是清除现有的一组分区。首先，用 clearpart --drivers=vda --all --initlabel 指示符清除 vda 虚拟硬盘驱动器上的全部卷。如果这个硬盘以前还未曾用过，则 initlabel 选项对此硬盘进行初始化处理。当然，在此命令生效之前必须删除它前面的注释符(#)。随后的 ignoredisk 指示符只在前面提到的 vda 驱动器上定义卷。当然，这只有当目标虚拟机上有一个指定的虚拟硬盘才会起作用(在该虚拟机上可以指定 PATA 或 SCSI 驱动器，但是这会与前面这些指示符发生冲突)。

```
# The following is the partition information you requested
# Note that any partitions you deleted are not expressed
# here so unless you clear all partitions first, this is
# not guaranteed to work
clearpart --drives=vda --all --initlabel
ignoredisk --only-use=vda
```

如果你打算用 Kickstart 文件和前面提到的 virt-install 命令，则需要用 sda 设备替换 vda 设备，因为 virt-install 命令通常不承认虚拟硬盘驱动设备文件。

需要改变紧随之后的分区(part)指示符。它们必须指定目录、文件系统格式(--fstype)和大小(--size，以 MB 为单位)。

```
part /boot --fstype=ext4 --size=500
```

```
part / --fstype=ext4 --size=8000
part swap --size=1000
part /home --fstype=ext4 --size=1000
```

注意，你的 anaconda-ks.cfg 文件可能还包含--onpart 指示符，它定义了像/dev/vda1 这样的分区设备文件。如果该分区已经存在就会产生一个错误。因此如果看到--onpart 指示符，最简单的办法是删除它们。否则安装过程开始之前必须建立这些分区，这可是一个难处理的任务。

虽然建立 RAID 和逻辑卷还有其他分区选项，但是毫无疑问，Red Hat 考试的重点是在安装结束之后如何创建这些卷。如果想试试逻辑卷等其他选项，则需要创建自己的 Kickstart 文件。如果从不同的 VM 安装机上建立这个 Kickstart 文件那是最好不过了。不过需要注意的是，该 Kickstart 文件按如下的顺序(这个顺序很重要)配置物理卷(PVs)、卷组(VGs)和逻辑卷(LVs)。

```
#part pv.KKb1QT-Smlq-TNoC-L4Ww --grow --size=1
#volgroup vg_minimalrhel6 --pesize=4096 pv.KKb1QT-Smlq-TNoC-L4Ww
#logvol / --fstype=ext4 --name=lv_root --vgname=vg_minimalrhel6 --size=51200
#logvol swap --name=lv_swap --vgname=vg_minimalrhel6 --size=1504
```

以 KK 开头的字母数字串是全球统一标识符(Universally Unique Identifier, UUID)的缩写表示。有关逻辑卷配置方法的更多信息可以阅读第 8 章内容。

默认的 Kickstart 文件可能包含一个 repo 指示符。它指向第 1 章实验题 2 创建的 FTP 网络安装源，必须删除这个指示符或者把它注释掉，如下所示：

```
#repo --name="Red Hat Enterprise Linux"
--baseurl=ftp://192.168.122.1/pub/ --cost=100
```

为了确保系统能真正完成安装过程，这里要插入 reboot、shutdown、halt 或 poweroff 指示符。我本人喜欢使用 shutdown 指示符。如果不想启动前面曾提到的第一引导进程，也可以插入 firstboot --disabled 指示符。由于在 Kickstart 文件中无法响应第一引导进程要求，因此--disabled 指示符有利于 Kickstart 安装模式的自动化。

```
shutdown
firstboot --disabled
```

如果打算重用一个现存的、基于 KVM 的虚拟机，则可能需要关闭系统以把引导媒介从 CD/DVD 改为硬盘，因此推荐使用下面的指示符：

```
shutdown
```

接着是通过 Kickstart 配置文件安装的程序包组列表。这些程序包组的名字可以从 RHEL 6 DVD 上/repodat 目录中的*-comps-rhel6-Server.xml 文件中找到，这在第 1 章中曾介绍过。由于此列表太长，下面只列出其中部分程序包组(前面有@符号)和程序包名字：

```
%packages
@ base
@ console-internet
...
```

```
nss-pam-ldapd
perl-DBD-SQLite
%end
```

安装这些程序包组后，就可以在下面的指示符后指定安装后的命令。例如，可以建立定制的配置文件。但是%post 指示符和之后任何参数都不是必需的。

```
%post
```

2.3.5 练习 2-3：创建和使用示例 Kickstart 文件

本练习中，我们将使用 anaconda-ks.cfg 文件把安装系统从一个计算机复制到另一个相同硬件配置的计算机上。本练习将在第二台计算机上安装所有把相同的程序包和相同的分区配置。此练习甚至还为 Kickstart 文件配置了 SELinux 上下文。

由于本练习的目的是安装与当前安装系统完全相同的程序包，因此不需要对/root 目录中默认 anaconda-ks.cfg 文件的程序包组或程序包做任何改变。本练习假定可以访问第 1 章实验题 2 建立的网络安装源。

本练习的操作步骤假设当前至少有两个不同的基于 KVM 的虚拟机，它们都有足够的磁盘空间和其他资源。

- (1) 检查/root/anaconda-ks.cfg 文件，将它复制为 ks.cfg。

- (2) 如果在此文件已有 network 指示符，则将它修改为指向 IP 地址为 192.168.122.150、主机名为 tester1.example.com 的系统。如果带有该主机名和 IP 地址的系统已经存在，则使用同一网络上的其他主机名和 IP 地址。如果没有这个指示符，则不需要任何修改。网络设置可以在安装完成后使用第 3 章介绍的方法进行配置。

- (3) 确保在 ks.cfg 文件中的与驱动器和分区有关的指示符置于活动状态，因为默认在 /root/anaconda-ks.cfg 文件中它们都已被注释掉。要特别注意 clearpart 指示符，给它添加--all 开关参数就会删除全部分区；添加--initlabel 开关选项则对新建立的分区进行初始化。如果系统有不止一个硬盘驱动器，则用--drivers=vda 开关选项选择基于 KVM 的虚拟机的第一个虚拟驱动器。

- (4) 检查与 URL 地址或 nfs 目录有关的安装服务器所在的位置。本实验题假设通过 192.168.122.1 的 IP 地址和 pub/inst/子目录可以访问一个 FTP 服务器。如果是另外一个 IP 地址或目录，则做相应的修改。

- (5) 确保下面的指示符插入到文件末尾的%post 指示符之前。

```
shutdown
firstboot --disabled
```

- (6) 把 ks.cfg 文件复制到安装服务器的基目录。如果这是一个 vsFTP 服务器，则目录是/var/ftp/pub。保证所有用户对此文件都有读权限，方法之一是使用下面的命令。

```
# chmod +r /var/ftp/pub/ks.cfg
```

- (7) 假设基目录是/var/ftp/pub，则用下面的命令设置此文件的 SELinux 上下文。

```
# chcon --reference /var/ftp/pub /var/ftp/pub/ks.cfg
```

(8) 确保当前的防火墙不会阻止与安装服务器有关的端口通信，详细信息请查看第 4 章。最简单但却不太安全的方法是使用下面的命令：

```
# iptables -F
```

(9) 准备第二个计算机，确保它有足够的硬盘空间。此第二个计算机可以是本地主机上一个基于 KVM 的虚拟机。把第二个计算机引导到 RHEL 6 DVD 上。

(10) 在 Red Hat 安装菜单中选择第一个菜单项，并按下 Tab 键，它会在屏幕的底部显示启动指示符。在此列表的末尾添加以下指示符：

```
ks=ftp://192.168.122.1/pub/ks.cfg
```

如果 Kickstart 文件是在另一个服务器上或在本地媒介上，则做相应的替换。

可以看到现在系统安装程序创建了一个与第一个系统完全相同的基本配置。如果安装过程在重新引导之前停止，则表示 Kickstart 文件存在问题，这很可能是由于安装信息不足。

2.3.6 Kickstart 配置程序

即使喜欢在命令行工作的用户也会从 Red Hat 的 Kickstart 配置程序(Kickstart Configurator)GUI 工具学到不少知识。它包含了建立一个 Kickstart 配置文件要用到的绝大多数基本选项。用下面的命令可以安装这个程序：

```
# yum install system-config-kickstart
```

作为一个与安装过程有关的 GUI 工具，此命令通常包含许多依赖选项。当我在自己的系统上安装这个程序时，这个命令竟然有 27 个这些选项。这意味着这个命令安装了总共 28 个程序包。

实际经验

有些人可能对书面语言的规范使用比较敏感，可能会反对 Kickstart Configurator 这个术语。但是它只是 Red Hat 给一个 GUI 配置工具的一个名字而已。

既然你已经掌握了 Kickstart 文件的基本内容，现在就可以通过图形化的 Kickstart 配置程序进一步巩固这些知识。它可以帮助你了解更多 Kickstart 文件的配置方法。在安装了正确的程序包后，可以用 system-config kickstart 命令在 GUI 命令行中启动这个 Kickstart 配置程序。如果想从本地系统的默认设置来启动该配置程序，则使用 anaconda-ks.cfg 文件如下：

```
# system-config-kickstart /root/anaconda-ks.cfg
```

上述命令打开如图 2-18 所示的 Kickstart 配置程序(当然，如可能最好先备份 anaconda-ks.cfg 文件)。

实际经验

启动 Kickstart 配置程序之前，最好确保通过 RHN 与远程的 RHEL 6 库有一个活动的连接。或者也可以使用第 7 章介绍的技术，将本地系统连接到在第 1 章的实验题 2 创建的安装源。

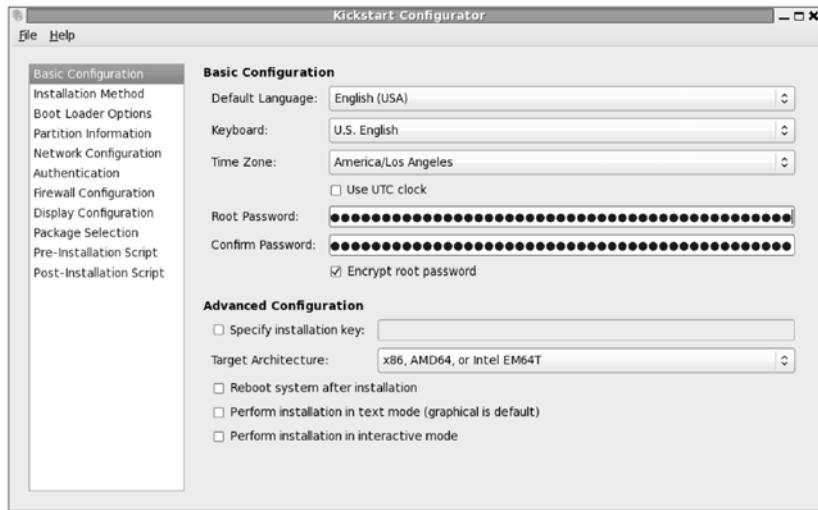


图 2-18 Kickstart 配置程序

图 2-18 说明了几个基本的安装步骤。如果已经安装过 RHEL，则这些步骤都看起来非常相似。

在左侧窗格中有几个其他选项，每个都对应于不同的 Kickstart 命令。为了深入了解 Kickstart，可以尝试配置其中一些参数。用 File | Save 命令保存文件的这些设置，文件名由你自己来决定，然后用文本编辑器查看这个文件。或者用 File | Preview 命令查看不同配置对 Kickstart 文件的影响。

接下来将简单介绍左侧窗格中的每个选项。全面掌握 Kickstart 配置程序的用法有助于更好地理解安装过程。

基本配置

在基本配置(Basic Configuration)界面中，我们可以给以下选项设置参数：

- **默认的语言(Default Language)** 给安装过程和操作系统指定默认的语言。
- **键盘(Keyboard)** 设置默认的键盘，通常要与语言相对应。
- **时区(Time Zone)** 把计算机的硬件时钟设置为 UTC 的原子时间，后者即为格林威治标准时间。
- **超级系统管理员密码(Root Password)** 指定超级系统管理员的密码，可能需要加密。
- **目标体系结构(Target Architecture)** 可用于为不同的系统定制 Kickstart 文件。
- **安装后重新引导系统(Reboot System After Installation)** 在 Kickstart 文件的末尾添加 reboot 命令。
- **按文本模式执行系统安装(Perform System Installation In Text Mode)** 支持按文本模式执行自动安装。当安装过程自动化后，安装模式就不重要了。
- **按交互模式执行安装(Perform Installation In Interactive Mode)** 允许用户查看 Kickstart 安装的操作步骤。

安装方法

Installation Method(安装方法)选项很容易理解。你可能是第一次安装 Linux，也可能是升级一个已安装的系统。安装方法和输入内容都取决于安装文件所在的位置。例如，如果选择 NFS

安装方法，则 Kickstart 配置程序需要用户输入 NFS 服务器的名字或 IP 地址以及 RHEL 安装文件的共享目录。

在 Kickstart 文件中，可以设置从 CD/DVD、本地的硬盘分区或者 NFS、HTTP 或 FTP 标准网络服务器中的一个启动 RHEL 的安装。

引导装载程序选项

接着列出了引导装载程序的选项。默认的引导装载程序是 GRUB，在引导过程为进一步加强系统的安全 GRUB 支持密码的加密。

Linux 引导装载程序通常安装在 MBR 上。如果系统属于 Linux 和微软 Windows 的双引导系统，则可以配置 Windows 引导装载程序(也可以用 Partition Magic 或 System Commander 等引导装载程序)指向位于 Linux 分区中第一个扇区的 GRUB。

分区信息

分区信息(Partition Information)选项决定了安装程序配置系统上硬盘的方式。虽然它支持标准分区和 RAID 分区，但是它并不支持 LVM 组的配置。Clear Master Boot Record(清除主引导记录)选项允许用户删除老式硬盘上的 MBR，这些老式硬盘可能存在问题。只要在 Kickstart 文件中插入 zerobmr yes 命令即可。

实际经验

如果想保留 MBR 上 Partition Magic 或 Windows 7 Bootmgr 等其他的引导装载程序，则不要使用 zerombr yes 这个选项。

是否删除分区取决于它们是否已创建为 Linux 文件系统。如果使用一个新的硬盘，则必须选择 Initialize the Disk Label 选项。单击 Add 命令出现 Partition Options 对话框。

网络配置

网络配置(Network Configuration)组允许用户为目标计算机的网卡设置 IP 地址。可以为某个计算机设置一个专用的静态 IP 地址，或者使用 DHCP 服务器。单击 Add Network Device 出现 Network Device Information 窗口。

验证

验证(Authentication)组选项允许我们给用户密码设置两个安全模式：影子密码(Shadow Password)和密码的 Hash 加密算法。前者对/etc/shadow 文件中的密码进行加密。这一组选项还允许用户设置各种协议的验证信息。

- **NIS** 网络信息服务(Network Information Service) 连接到网络上一个登录验证数据库，此网络由 Unix 和 Linux 计算机组成。
- **LDAP** 在这里，轻型目录访问协议(Lightweight Directory Access Protocol， LDAP)是另外一个登录验证数据库。
- **Kerberos 5** MIT 强加密系统，用来验证网络上的用户。
- **Hesiod** 它与 Kerberos 5 有关。
- **SMB** Samba(CIFS)服务器连接到微软 Windows 模式的网络，用来验证登录用户。

- **Name Switch Cache** 它与 NIS 有关，用来查找密码和用户组。

防火墙配置

防火墙配置(Firewall Configuration)选项组用于为对象计算机配置默认的防火墙。在大多数系统中，我们要尽量把可信任服务的个数保持在最小值。但在 Red Hat 考试中要求在单个系统设置很多服务，这就需要在防火墙中配置多个受信任的服务。

在这一组选项中，我们也可以配置基本的 SELinux 参数。Active 和 Disable 选项容易理解，Warn 选项对应于 SELinux 的 Permissive 实现。更多内容请阅读第 4 章。

显示配置

Display Configuration 选项组支持基本的 Linux GUI 安装。实际安装取决于这组选项中程序包和程序包组的选择。虽然关于基于 GUI 的管理工具与基于文本的管理工具的优越性存在很多争议，但是基于文本的管理工具更加稳定。正是由于这个原因(还有其他)，许多 Linux 管理员甚至并不安装 GUI 程序。但如果在一系列工作站上安装 Linux(这可以用一系列的 Kickstart 文件来实现)，则这些工作站的用户很可能不是系统管理员。

此外，可以启动或禁用 Setup Agent，又称为第一引导进程。如果需要全自动安装，则要禁用 Setup Agent 选项。

程序包选择

Package Selection 选项组允许我们选择需要通过 Kickstart 文件安装的程序包组。应该把它看成为在安装过程中的定制安装窗口。

如前所述，如果当前没有连接到远程库(如 RHN 更新库)或前面提到的安装服务器，则相关界面是空的。

安装脚本

可以在 Kickstart 文件中添加预安装和滞后安装脚本。滞后安装(Post-Installation)脚本更常用，通常用来配置 Linux 操作系统的其他部分。例如，如果你想创建一个记录员工福利信息的目录，则可以添加一个滞后安装脚本，它可以用 cp 命令把这些文件复制到网络服务器上。

认证目标 2.04 用 SSH 管理系统

默认情况下，Red Hat 企业版 Linux 系统安装了 SSH 程序。RHCSA 考试对 SSH 的要求很简单，考生只需要知道如何用它访问远程系统。因此本节只介绍客户端如何用 ssh 命令访问远程系统。

如前所述，标准的 RHEL 6 安装会默认安装 SSH 程序。虽然默认情况下防火墙是激活的，但是标准 RHEL 6 防火墙将端口 22 处于开着状态以允许 SSH 访问。相关的配置文件保存在/etc/ss 目录中。SSH 服务器的详细配置属于 RHCE 考试的范围。相关的客户端命令有 scp 和 sftp，它们都要在本节中介绍。

SSH 守护程序是安全的，因为它对消息进行加密。换言之，侦听网络的用户读不到 SSH 客户端与服务器之间传递的消息，这在像 Internet 这样公共网络中是非常必要的。RHEL 加入 SSH

版本 2, SSH 2 是 SSH 1 的增强版, 前者包含了密钥交换算法。想了解 RHCE 考试中对 SSH 的要求请参阅第 11 章。

2.4.1 配置 SSH 客户端

SSH 客户端主要的配置文件是/etc/ssh/ssh_config。每个用户可以有自己的 SSH 客户端配置参数, 它们保存在~/.ssh/config 文件中。默认情况下配置文件中有 4 个指示符。第一个是 Host * 指示符, 它将其他指示符应用于所有连接。

```
Host *
```

下一个指示符支持用通用安全服务应用程序编程接口(Generic Security Service Application Programming Interface)对客户端/服务器进行验证:

```
GSSAPIAuthentication yes
```

下一个指示符支持对 GUI 工具的远程访问。X11 是在 Linux 使用的 X Window System 服务器的传统名字。

```
ForwardX11Trusted yes
```

下一个指示符允许客户端设置几个环境变量。其细节因不同的 Linux 系统而略有差别。

```
SendEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
SendEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
SendEnv LC_IDENTIFICATION LC_ALL
```

这为从命令行访问远程系统做好准备。

2.4.2 命令行访问

本节介绍使用 ssh 命令的标准访问方法。为访问一个远程系统, 需要知道该远程系统的用户名和密码。默认情况下允许 ssh 直接访问 root 账户。例如, 使用以下命令访问前面提到的 server1 系统上的 root 账户:

```
$ ssh root@server1.example.com
```

下面这个命令效果相同:

```
$ ssh -l root server1.example.com
```

如果没有用户名, ssh 命令就以本地系统的当前用户名访问远程系统。例如, 如果我从自己的 michael 用户账户执行下面的命令:

```
$ ssh server1.example.com
```

则 ssh 命令认为我以 michael 用户名登录到 server1.example.com 系统。如果这个命令是第一次用于两个系统, 则会出现类似于以下的消息:

```
$ ssh server1.example.com
The authenticity of host 'server1.example.com (192.168.122.50)'
```

```

can't be established.
RSA key fingerprint is b9:8a:c8:cd:c3:02:87:b3:1c:a9:a7:ed:d8:9c
:28:b8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'server1.example.com,192.168.122.50'
(RSA) to the list of known hosts.
michael@server1.example.com's password:

```

这类 ssh 命令的一个漏洞是它在网络上发送密码的方式。更安全的访问方法是用基于密码短语方法访问 1 024 位(或更多)私钥/公钥对。但是这个更加安全的选项是属于 RHCE 的考试范围，将在第 11 章讨论。当客户端与 SSH 服务器建立起连接，就会把远程密钥的指纹的副本添加到用户的`~/.ssh/known_hosts` 文件中。对于来自远程系统的公开密钥，采用 RSA 加密算法。RSA 是此算法的三位设计者的姓的首字母，即 Rivest、Shamir 和 Adelman。公钥传给远程系统，私钥保存在本地系统中以与授权的远程请求相匹配。

一旦用 ssh 建立起连接，就可以在此远程系统做任何任何属于权限范围内的操作。例如，用户甚至可以用 poweroff 命令关闭远程系统。在执行这个命令后，可以用 exit 命令退出远程系统。

2.4.3 SSH 的其他命令行工具

如果想用类似 FTP 的模式访问远程系统，则 sftp 命令正好合适。尽管这个命令不可以使用`-l` 开关选项，但是它仍然可以用于登录到远程系统上任何用户的账户。虽然普通的 FTP 通信采用明文模式，但是 sftp 命令的通信却以加密的形式传递文件。

另外，如果只是想在加密的连接线路中复制文件，则可以使用 scp 命令。例如，我在本书中生成了一些截图，它们是第 1 章和第 2 章配置的虚拟机的测试结果。为了把这些截图传送给本人的手提计算机，我使用一个如下所示的命令，它把 F02-20.tif 文件从本地目录复制到远程系统的`/home/michael/RHook/Chapter2` 目录中。

```
# scp F02-20.tif michael@server1:/home/michael/RHook/Chapter2/
```

除非已经建立了基于密码短语的连接(将在第 11 章中讨论)，否则这个命令会要求 server1 服务器上的 michael 用户输入密码。当密码验证通过后，scp 命令就把 F02-20.tif 文件以加密的形式复制到名为 server1 服务器的远程系统上的指定目录中。

2.4.4 SSH 图形化访问

ssh 命令可以用来在网络上传递 GUI 工具。这听起来有点怪，但是如果本地系统当作 GUI 服务器，同时从远程系统上调用远程 GUI 客户端应用程序，则可使用该命令。

默认情况下，SSH 服务器和客户端配置文件都已经设置好以支持在网络上进行 X11 通信。所需要的全部操作只是用`-X` 开关选项连接到远程系统。例如，可以使用图 2-19 中的命令序列来管理远程系统的用户。



图 2-19 用 SSH 访问远程 GUI

认证目标 2.05 考虑添加命令行工具

你可能想添加几个命令行工具以帮助系统管理员管理各种 Linux 系统。本书后面将使用这些工具来确保各种服务器正常操作。虽然最好用 Evolution 和 Thunderbird 这样的 e-mail 客户端测试像 Postfix 这样的服务，但是像 telnet、nmap 和 mutt 等命令可以用在命令行窗口远程检查这些服务。为通过 Red Hat 考试，需要在下载像 Evolution 这样复杂的工具时用这些工具测试、诊断和解决系统问题。虽然 ssh 命令可以实现远程访问 GUI 工具，但是与这类工具进行通信可能会非常耗时。

从管理角度而言，我们感兴趣的工具有：

- telnet 和 nmap 可以验证对开放端口的远程访问。
- mutt 作为一个 e-mail 客户端可以验证一个 email 服务器的功能。
- elink 作为 Web 浏览器，它确保 Web 服务是可以访问的。
- 在命令完成后可以用 lftp 访问 FTP 服务器。

2.5.1 用 telnet 检查端口

telnet 命令其实非常强大。任何对明文客户端存在的安全风险有所了解的人都对 telnet 命令有所顾忌。用 telnet 登录到远程服务器的用户确实以明文的方式传递他们的用户名、口令和其他命令。只要有一个像 Ethereal 的分析器，任何人都很容易读取得这些数据。

但是 telnet 的作用远不止这些。当它在本地行动时，它可以验证一个服务的运行。例如，下面这个命令验证了本地系统的 vsFTP 运行情况：

```
$ telnet localhost 21
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 (vsFTPd 2.2.2)
```

“转义字符(Escape Charater)”是 CTRL 键和右方括号(])同时按下来的字符。在屏幕上输入这个命令组合会出现 telnet>提示符。在这个提示下用 quit 命令可以退出。

```
^]
telnet> quit
```

通常情况下甚至不用执行 Escape Character 就可以退出 telnet 提示符窗口，只需要输入 QUIT 命令即可。

如果 vsFTP 没有运行或者如果它的通信端口不是 21，则会看到如下的响应：

```
Trying 127.0.0.1...
telnet: connect to address 127.0.0.1: Connection refused
```

如果系统没有安装防火墙，则利用远程系统也会得到相同的结果。但是如果防火墙阻止了 21 端口的通信，则会看到类似于下面的信息：

```
telnet: connect to address 192.168.122.50: No route to host
```

有些服务如 Postfix 电子邮件服务器默认情况下只接受来自本地的连接。此时，不管有没有防火墙，当我们连接一个远程系统时都看到“连接被拒绝”的消息。

2.5.2 用 nmap 检查端口

nmap 命令是一个功能强大的端口扫描工具。正因为如此，nmap 开发者的网站上有这样的描述：“当 nmap 命令使用不正确时，nmap 很可能会使(但是很少)使用者遇到 ISP 的起诉、解雇、驱逐、甚至监禁”。尽管如此，它已包含在标准 RHEL 6 库中。因此它的合法使用已得到 Red Hat 的支持。用 nmap 命令可以快速确定在本地和在远程打开的服务。例如，如图 2-20 的 nmap localhost 命令检测到并列出那些正在本地系统上运行的服务。

```
[root@server1 ~]# nmap localhost
Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-29 09:47 PST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000070s latency).
Hostname localhost resolves to 2 IPs. Only scanned 127.0.0.1
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
[root@server1 ~]#
```

图 2-20 在本地应用端口扫描程序

但是与此相反，如果从远程系统上执行端口扫描，则看起来似乎只有一个端口是打开的。这说明此服务器上的防火墙起作用。

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-11-29 09:52 PST
Nmap scan report for server1.example.com (192.168.122.50)
Host is up (0.00027s latency).
```

```
Not shown: 999 filtered ports
PORT STATE SERVICE
22/tcp open ssh
```

2.5.3 配置 e-mail 客户端

对于参加 Red Hat 考试的考生来说, GUI email 客户端的配置过程应该是易如反掌的。但是, 对于命令行 email 客户端, 事情就不是这样, 命令行客户端常用来测试 Postfix 和发送邮件等标准 e-mail 服务器的功能。例如, 当一个服务器配置为邮局协议 (Post Office Protocol, POP) 电子邮件服务器时, 或者此邮件服务器用几乎无所不在的 POP3 版本发送邮件时, 可以用下面的命令进行检查:

```
# mutt -f pop://username@host
```

既然 GUI 的 e-mail 客户端对读者来说很容易, 因此本节的其余部分重点介绍命令行的 email 客户端。

2.5.4 命令行电子邮件

测试本地邮件系统的一个方法是使用内置的命令行 mail 工具。它提供了一个简单的基于文本的接口。邮件系统把每个用户的邮件保存在与每个用户名相关的/var/mail 目录中。用 mail 工具阅读邮件的用户也可以回复、转发或甚至相关的信息。

当然可以用其他任何邮件阅读程序, 如 mutt 或者与 GUI Web 浏览器自带的邮件管理程序测试自己的邮件系统。其他邮件阅读程序把信息保存在不同的目录。例如, pine 工具可以为 mj 用户的邮件, 并把邮件保存在/home/mj/mail 目录中。如果在本地系统上已启动简单邮件传输协议服务器(Simple Mail Transfer Protocol, SMTP), 则像 mutt、mail 和 pine 这样的邮件阅读程序可以用来发送信息。

mail 命令有两个基本的用法。第一个是先输入邮件主题然后是邮件内容, 完成后按 CTRL-D, 然后在 Cc: 一行中输入其他地址(如果有必要的话)。按下回车键就把邮件发送出去, 且 mail 程序终止运行并返回到命令行。

```
$ mail Michael
Subject: Test Message
Sent and received
Cc: mjang@example.com
$
```

也可以把一个文件以邮件的文本内容的方式重定向到另一个用户。例如, 下面的命令把/etc/hosts 的副本发送给 root 用户, 邮件名为“hosts file”。

```
$ mail -s 'hosts file' < /etc/hosts root@localhost
```

2.5.5 阅读邮件信息

默认情况下, mail 系统不会为某个用户打开, 除非在相应的文件中有邮件。当 mail 系统打开后, 用户就会看到新邮件和已经阅读邮件的列表。如果用户想要为某个账户打开 mail 系统,

则需要输入邮件的编号并按下回车键。如果没有输入参数直接按回车，则 mail 工具会认为要阅读下一个还没阅读的邮件。为删除一个邮件，可以在邮件后面使用 d 命令，或用 d#删除编号为 # 的邮件。

或者，在本地的 /var/mail 目录里，在用户定义的文件里读取邮件内容。这个目录里的文件都按相应的用户名命名的。

2.5.6 文本和图形浏览器的使用

Linux 包含了多个图形化浏览器。访问普通网站或安全网站要用相应的协议，即超文本传输协议(Hypertext Transfer Protocol, HTTP)或超文本传输协议安全(Hypertext Transfer Protocol, Secure, HTTPS)。任何 Linux 用户都会使用图形化浏览器。

也许你并不是总能访问 GUI，特别是不能从远程的系统访问 GUI。任何情况下，基于文本的浏览器速度比较快。在 Red Hat Linux 中标准的基于文本的浏览器是 elinks。当 elinks 程序包安装后，可以用它在命令行打开任何所想要访问的网站。例如，图 2-21 说明了 elinks http://www.mheducation.com 命令的结果。

为退出 elinks 程序，只需要按下 ECS 键进入菜单栏，然后按下 F | X 并接受提示信息，即可退出 elinks 浏览器。

如果需要配置一个 Web 服务器，最容易的办法是确保它只用简单的文本页面，不需要 HTML 代码。例如，可以在主页中添加以下的文本：

```
This is my home page
```

然后就可以运行 elinks home.html 命令在 elinks 浏览器中浏览这段文本。如果已经在第 1 章介绍的 /var/www/html/inst 目录中建立一个 Apache 文件服务器，则也可以用 elinks 查看用以下命令复制到此服务器上的文件：

```
$ elinks http://192.168.122.1/inst
```

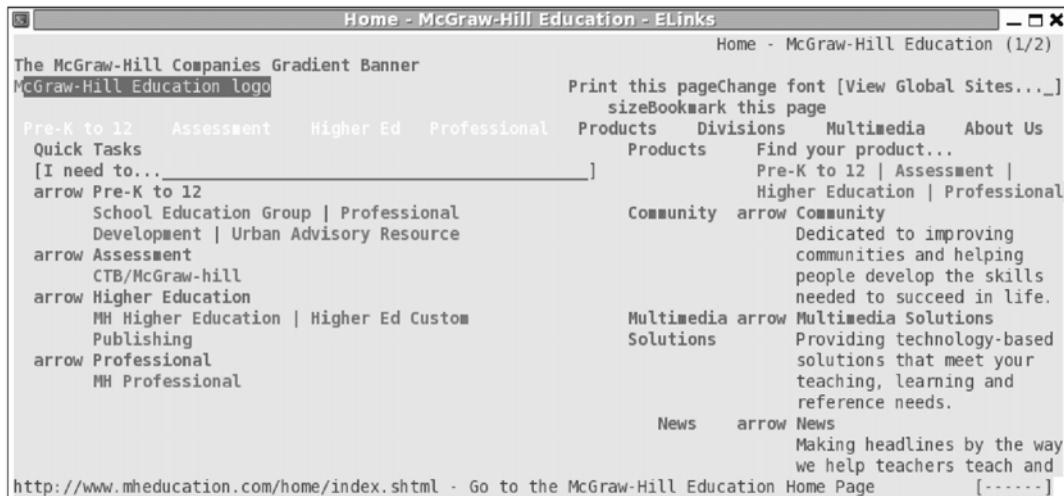


图 2-21 elinks 浏览器

2.5.7 用 lftp 访问 URL

最初的 FPP 客户端软件都是一个简单的命令行, 它是提供了简单高效的接口的面向文本的客户端应用程序。大多数 Web 浏览器提供一个图形接口, 也可以用作 FTP 客户端。

任何 FTP 客户端允许用户查看目录树和文件。把 ftp 当作客户端是很容易的一件事。我们可以用 ftp 命令连接到像 ftp.redhat.com 这样的服务器, 如下所示:

```
# ftp ftp.redhat.com
```

但是在这个客户端需要输入用户名和密码。输入一个匿名用户名和一个随机的密码就可以访问 Red Hat FTP 服务器, 但如果用户偶然输入一个真实的用户名和密码, 则这些数据将会用明文格式发送, 在此网络上任何碰巧使用网络分析仪应用程序的人都可以看到这些数据。奇怪的是, 在标准的 RHEL 6 安装中竟然没有安装 ftp 命令客户端程序。

这只是 lftp 比 ftp 较好的一个理由。它会自动尝试匿名登录而不会要求用户输用户名或口令。此外, 它还支持命令补全(Command Completion)功能, 该功能有助于访问带有长名称的文件和目录。

当然, 大多数 FTP 客户端都存在安全风险, 因为它们都以明文的形式传送数据。但是, 只要此命令仅限于用在对公开服务器的匿名访问, 则风险可以最小化。归根结底, 当我们用 lftp 命令从公共服务器上下载 Linux 软件包, 不大可能会暴露任何私人信息。

如果可以接受风险, 则可以用 lftp 命令登录 FTP 服务器, 而这些 FTP 服务器允许使用用户名和口令。这对于正为 RHCE 考试做准备的考生就可以建立非常安全的 FTP 服务器(vsFTP)。用户 michael 可以用下面的命令登录到这样一个服务器:

```
$ lftp ftp.example.org -u michael
```

在 lftp 客户端可以执行很多不同的命令, 如图 2-22 所示。其中一些命令将在表 2-5 中讨论。

```
[root@Maui ~]# lftp ftp.redhat.com
lftp ftp.redhat.com:~> help
!<shell-command>                               (commands)
alias [<name> [<value>]]                      bookmark [SUBCMD]
cache [SUBCMD]                                     cat [-b] <files>
cd <dir>                                         chmod [OPTS] mode file...
close [-a]                                         [re]cls [opts] [path/] [pattern]
debug [<level>|off] [-o <file>]                 du [options] <dirs>
exit [<code>|bg]                                    get [OPTS] <rfile> [-o <lfile>]
glob [OPTS] <cmd> <args>                         help [<cmd>]
history -w file|-r file|-c|-l [cnt]            jobs [-v]
kill all|<job_no>                                lcd <dir>
lftp [OPTS] <site>                                ls [<args>]
mget [OPTS] <files>                               mirror [OPTS] [remote [local]]
mkdir [-p] <dirs>                                 module name [args]
more <files>                                      mput [OPTS] <files>
mrm <files>                                       mv <file1> <file2>
[re]nlist [<args>]                                open [OPTS] <site>
pget [OPTS] <rfile> [-o <lfile>]                put [OPTS] <lfile> [-o <rfile>]
pwd [-p]                                           queue [OPTS] [<cmd>]
quote <cmd>                                         repeat [OPTS] [delay] [command]
rm [-r] [-f] <files>                             rmdir [-f] <dirs>
scache [<session_no>]                            set [OPT] [<var> [<val>]]
site <site_cmd>                                   source <file>
torrent [-O <dir>] <file>                         user <user> [URL] [<pass>]
version                                            wait [<jobno>]
zcat <files>                                       zmore <files>
lftp ftp.redhat.com:~> ■
```

图 2-22 lftp 的命令

表 2-5 标准 lftp 客户端命令

命 令	说 明
cd	切换远程主机上的当前工作目录
ls	列表显示远程主机上的文件
get	从远程主机上取回文件
mget	用通配符或文件名全称从远程主机上取回多个文件
put	把本机的文件上传到远程主机上
mput	把一组文件上传到远程主机上
pwd	显示远程主机上的当前工作目录
quit	终止 FTP 会话
!ls	列出本地计算机上当前目录中的文件
lcd	切换本地主机目录用于上传或下载
!pwd	显示本地主机的当前工作目录

与 Telnet 会话相似，几乎所有可以在 FTP 提示符后执行的命令都运行远程主机上。我们也可以在 FTP 提示符后执行常用的 shell 命令，只需要在命令前面加一个感叹号(!)。

表中列出的只是 lftp 命令的一个子集。如果用户记不起某个命令的用法，输入 help cmd 就可以得到这个命令的详细说明。

2.6 认证小结

考虑到虚拟技术在当前计算机环境中的重要性，因此 Red Hat 把 KVM 作为 RHCSA 考试的一部分也并不奇怪。假设已经与一个合适的程序库建立起一个有效的连接，则安装与 KVM 有关的程序包是一件非常容易的事。可以用 modprobe kvm 这样的命令确保已安装了合适的模块。然后用虚拟机管理程序配置 RHEL 6 系统上的基于 KVM 的虚拟机。我们也可以用 virt-install、virt-clone 和 virsh 这些命令安装、克隆和管理这些虚拟机。

我们可以用 Kickstart 文件实现整个安装过程的自动化。每个 RHEL 系统都有一个 Kickstart 模板文件，它保存在 /root 目录中。对它进行修改后，可用于在其他系统上实现 RHEL 的自动安装。或者也可以用 GUI Kickstart 配置程序建立一个合适的 Kickstart 文件。

对于所有这些系统，远程访问是必需的。SSH 命令可以用来在 Linux 系统之间建立远程的加密通信。RHCSA 考试要求你掌握 SSH 客户端的使用。ssh 命令可以用来登录到远程系统。ssh -X 命令甚至可以用来访问远程的 GUI 应用程序。scp 复制命令可以通过加密的连接复制文件。

在检查和排除 RHEL 服务故障时，使用几个命令行工具会给我们带来很大的方便。telnet 命令可以通过所选择的端口连接到远程服务。nmap 命令可以用作端口扫描。mutt 命令可以检查 e-mail 服务器的功能。elinks 命令可以用作命令行浏览器。最后，lftp 命令是一个非常好的 FTP 客户，它支持命令补全功能。

2.7 小练习

下面是本章与认证目标有关的几个重要知识点。

为 Red Hat 配置 KVM 虚拟机

- KVM 需要的程序包属于虚拟化技术程序包组的一部分。
- 基于 KVM 的虚拟机可以用虚拟机管理程序来配置。
- KVM 需要的模块包含 `kvm` 和 `kvm_intel` 或 `kvm_amd`。

在 KVM 上配置一个虚拟机

- 基于 KVM 的虚拟机默认的存储目录是`/var/lib/libvirt/images`。
- 虚拟机配置文件保存在`/etc/libvirt`的各个子目录中。
- 用虚拟机管理程序可以访问虚拟机终端控制台，该虚拟机管理程序可以用 `virt-manager` 命令启动 GUI 工具。
- 用 `virt-install`、`virt-clone` 和 `virsh` 命令可以安装、克隆和配置虚拟机。
- `virsh list --all` 命令列出所有已配置好的虚拟机。
- `virsh autostart vmname` 命令可以把名为 `vmname` 的虚拟机配置为在主机引导时自动启动。
- `virsh destroy vmname` 命令等效于切断名为 `vmname` 虚拟机的电源。

自动安装选项

- 系统安装的过程记录在`/root/anaconda-ks.cfg` Kickstart 文本文件中。
- 可以直接修改 Kickstart 文件，也可以用 Kickstart 配置工具进行修改。
- Kickstart 文件可以在本地媒介中或从网络服务器上调用。

用 SSH 管理

- SSH 默认安装在 RHEL 6 上，它甚至可以穿过默认防火墙。
- `ssh` 命令可以用来安全地访问远程系统，它甚至可以用来访问远程 GUI 工具。
- `ssh` 相关的命令包含 `sftp` 和 `scp`。

添加命令行工具

- 系统管理员有时只用命令行验证对服务器的访问。
- `telnet` 和 `nmap` 命令可用来验证对开放端口的远程访问。
- `mutt` 电子邮件客户端可以用来验证 `email` 服务器的功能。
- `elinks` 控制台 Web 浏览器可以验证一个 Web 服务器是否正确工作。
- `lftp` 客户端可以用它的命令补全功能的优点来验证是对 FTP 服务器的访问。

2.8 自测题

下面的习题用来检查读者对本章内容的掌握程度。由于 Red Hat 考试没有多选题，因此本书中不提供任何选择题。这些题目专门用来测试读者对本章的理解。Red Hat 考试注重于得到结果的过程，而不是死记硬背一些无关紧要的内容。许多问题可能不止一个答案。

为 Red Hat 配置 KVM

- 说出与 KVM 有关的内核模块名。
-

- 说出在 GUI 中配置 KVM 虚拟机工具的名字。
-

配置 KVM 上的虚拟机

- 哪个命令可以启动 GUI 中的虚拟机管理程序？
-

- 默认情况下虚拟机管理程序把虚拟硬盘保存在哪个目录中？
-

- 哪个命令可用于新建一个虚拟机？
-

自动安装选项

- 哪个命令可以启动基于 GUI 的 Kickstart 配置工具？
-

- /root 目录中哪个文件记录 RHEL 的安装过程？
-

- 在 Kickstart 配置文件中，哪些指示符与网络连接有关？
-

- 如果安装 FTP 服务器位于 `ftp://server1.example.com/pub/inst`，则在 Kickstart 配置文件中，哪个指示符指向这个服务器？
-

- 在 Kickstart 配置文件中，哪个指示符会在安装完成后关闭系统？
-

用 SSH 进行管理

11. ssh 命令的哪个开关选项可用于确定远程登录的一个不同用户。

12. ssh 命令的哪个开关选项启用对远程 GUI 工具的访问。

添加命令行工具

13. 用哪个命令可以确定一个服务器是否运行在 IP 地址为 192.168.11.1 的系统上且使用 25 端口？

14. 哪个命令可以用来验证 IP 地址为 192.168.122.1 的远程系统上存在活动和可用的服务？

2.9 实验题

本章几个实验题属于安装练习。应该在实验机上做这些练习。有些实验题要求删除系统中的全部数据。虽然这些操作都属于 RHCSA 考试的范围，但是有些读者可能没有支持 KVM 的硬件系统。代替 KVM 的方法是使用如 VMware 的虚拟机解决方案。可以从 www.vmware.com 下载 VMware 软件，或者从 www.virtualbox.org 下载 Virtualbox 开源代码版本。

Red Hat 试卷采用电子形式。因此，在本章及后面几章中的大多数实验题都可以从本书配书光盘上读取，本章的实验题保存在 Chapter2 子目录中。假如现在仍然没有在自己的系统中安装一个 RHEL 6，参考本书第 1 章的第一个实验题的安装指示。

实验题 1

本实验题要在基于 KVM 的虚拟机上安装一个 RHEL 系统，得到一个基本的服务器。至少需要 12GB 的硬盘空间(11GB 用来保存数据，1GB 用来交换空间，假设内存至少为 512MB)。如果要执行 GUI 安装程序，则内存至少需要 652MB。此外还需要为两个虚拟硬盘保留各 1GB 的空间(因此总共需要 14GB)。

本实验题假设要在一个基于 KVM 的虚拟机上完成 RHEL 安装。为了启动安装，打开一个 GUI 工具并运行 virt-manager 命令。如果不能自动打开，则右击 Localhost(QEMU) 选项，并从弹出的菜单中选择 Connect。如果系统要求输入口令，则输入 root 管理员的口令。连接成功后，右击同一个选项并选择 New，它启动一个向导用于帮助用户配置一个虚拟机。

如果我们要配置一个将在后面几章中使用的虚拟机，则这个虚拟机就是第 1 章中提到过的 server1.example.com 系统。

理想情况下，这个系统有足够的空间，可以安装至少 4 个大小不同的虚拟机，包括第 1 章中定义的三个系统和一个备用系统。换言之，60GB 空间的逻辑卷或分区应该足够了。

本操作介绍的步骤是通用的。至此，你已经积累了一定的 RHEL 6 安装经验。无论如何，

具体的操作步骤会因安装类型和引导媒介而异。

- (1) 启动第一个RHEL 6 网络引导CD。在欢迎屏幕中选择 Install Or Upgrade An Existing System。(如果你使用 RHEL 6 DVD 则按下 TAB 键，在 initrd=initrd.img 指示符后加上 askmethod)。
- (2) 根据第 1 章介绍的步骤启动 RHEL 6 的安装过程。
- (3) 根据提示，在一个由 KVM 虚拟机配置的网络上设置本地系统。网络地址默认为 192.168.122.0/24，对于 server1.example.com 系统，它的 IP 地址为 192.168.122.50。
- (4) 在合适的时候，把系统指向第 1 章建立的基于 FTP 的安装服务器上。如果按照第 1 章的操作指示，则此服务器位于 ftp://192.168.122.1/pub/inst。
- (5) 根据提示输入一个主机名，即 server1.example.com。在该界面中有一个 Configure Network 按钮。单击此按钮，在出现的窗口中输入 IPv4 网络信息。
- (6) 在适当的时候选择定制分区方法。
- (7) 建立第一个分区，磁盘空间大约为 500MB，格式化为 ext4 文件系统，并把它分配到/boot 目录。
- (8) 建立第二个分区，存储空间为 1GB(如果空间足够也可以大一点)，保存为交换空间。
- (9) 建立第三个分区，大小为 8GB，格式化为 ext4 文件系统，把它指定为顶层的根目录即/。
- (10) 建立另一个分区，大小为 1GB，把它指定为/home 目录。
- (11) 继续安装过程。
- (12) 选择需要安装的自定义程序包组。包括一个 GUI 工具，X Window 服务器，不需要在虚拟机中安装虚拟程序包。
- (13) 正常结束安装过程。
- (14) 根据提示重新启动系统，以 root 用户身份登录。执行 poweroff 命令结束本实验题。

2.10 自测题答案

配置 Red Hat 的 KVM

1. 与 KVM 有关的三个内核模块：kvm、kvm_intel 和 kvm_amd。
2. 在 GUI 里配置基于 KVM 虚拟机的工具是虚拟机配置程序。

配置 KVM 上的虚拟机

3. 启动 GUI 中虚拟机管理程序的命令是 virt-manager。由于菜单并不总是可以使用，因此顺序单击 Application | System Tools | Virtual Machine Manager 菜单项并不是一个可接受的答案。
4. 虚拟机管理程序的虚拟硬盘使用的默认目录是 /var/lib/libvirt/images。
5. 用来新建一个虚拟机的命令是 virt-install。

自动安装选项

6. 启动基于 CUI 的 Kickstart 配置工具的命令是 system-config-kickstart。
7. 在 /root 目录中记录 RHEL 安装过程的 Kickstart 文件名为 anaconda-ks.cfg。
8. 在 Kickstart 配置文件中，与网络连接有关的指示符是 network。

9. 指向给定 FTP 安装服务器的指示符是 url --url ftp://server1.example.com/pub/inst。
10. 在 Kickstart 配置文件中在安装完成后关闭系统的指示符是 shutdown。

用 SSH 进行管理

11. 在 ssh 命令中用来确定远程登录的不同用户的开关选项是-l。
12. 在 ssh 命令中，启动访问远程 GUI 工具的开关选项是-X，也可以用-Y 开关选项。

添加命令行工具

13. 为检查一个服务器是否在 IP 地址为 129.168.122.1 的系统上且端口 25 上运行可以使用 telnet 192.168.122.1 25 命令。
14. 为验证在 IP 地址为 129.168.122.1 的远程系统上活动的和可用的服务，可以使用 nmap 192.168.122.1 命令。

2.11 实验题答案

实验题 1

虽然本实验题很简单，但是它可以增加你对 KVM 虚拟机的信心。实验题完成后，应该能以 root 管理员的身份登录到这个虚拟机，并对系统做以下检查：

1. 检查挂载的目录和可用的空间。下面这个命令用来确认这些已挂载的目录和相关卷上的可用空间。

```
# mount  
# df -m
```

2. 假设你已连接到 Internet 且已订阅了 Red Hat Network，则必须把系统更新为最新内容。如果你使用一个重构发行版，则可以访问这些版本的公开库。不管哪种情况，执行以下命令以确保本地系统是最新的：

```
# yum update
```

本实验题验证“把 Red Hat 企业版系统安装成一个虚拟客户端”的能力。

实验题 2

记住，本章以及本书后面的所有实验题都可以在本书附带的光盘上找到。实验题 2 至实验题 8 出现在这个光盘的 Chapter2/子目录里。

系统克隆存在的问题之一是如何加入网卡的硬件地址。地址冲突可能会给网络带来问题。因此用户不仅要修改 IP 地址，而且还需要把唯一的硬件地址分配某个网卡。由于存在这些问题，KVM 通常为克隆的系统设置一个不同的网卡。例如，如果原系统有一个 eth0 网卡且网卡有一个硬件地址，则克隆系统的网卡为 eth1，而且采用另一个硬件地址。

如果你认为这太麻烦了，完全可以删除克隆系统，因为在 RHCSA 考试要求里并没有提到

VM 克隆系统。但是，如果备份了另外一个不同的系统则可能会大有用处。而且这也正是实验题 4(Kickstart 安装模式)学到的技术的最佳时机。

实验题 3

本实验题的目的是介绍如何用命令行方法配置基于 KVM 的虚拟机。如果还没有根据第 1 章的要求建立 4 个不同的虚拟机(三个虚拟机和一个备份系统)，现在就是最好的时机。一个方法是使用 `virt-install` 命令和`--prompt` 开关。该命令要求用户输入以下信息：

- 分配的内存，至少需要 512MB(基于 GUI 的安装系统需要 652MB)。
- 虚拟光盘文件路径，它必须与实验题 2 创建的虚拟光盘相同。
- 如果那个文件还不存在，则还说明虚拟光盘的大小。
- 在第 1 章实验题 2 里创建的 FTP 安装服务器的 URL 地址。或者使用第 1 章介绍的 HTTP 安装服务。

现在就可以正常完成这个安装过程，或者运行一个实验题 5 创建的安装系统的变异版。

实验题 4

如果你还没有 Kickstart 配置方面的经验，则需要反复的尝试。但是最好现在就遇到这些问题，而不是在 Red Hat 考试时或工作中遇到。如果无需帮助你就能够建立一个可以用来安装系统的 Kickstart 文件，则说明你完全可以应付 RHCSA 考试中的挑战。

有一个常见的问题与刚刚创建的虚拟光盘有关。它们必须先初始化，这正是 `clearpart` 指示符的`--initlabel` 开关的作用。

实验题 5

如果你最近首次执行 Kickstart 安装，则最好再来一次。如果现在练习，则意味着你在考试中可以较快地建立 Kickstart 安装。这还仅仅是开始，想象一下，假如你的老板需要几十台虚拟机，它们使用相同的软件和卷，再假设它们之间的唯一差别是主机名和网络参数，如果你能很快地完成这个任务，可以想象这对你的自信心有多大的帮助。

如果你能够从命令行中用 `virt-install` 命令建立一个 Kickstart 安装，则把它安装在远程的虚拟主机上将会更加容易。你能够从远程位置配置新的系统，这会提升你在工作组里的地位。

如果你还没有根据第 1 章的要求建立起四个不同的虚拟机(三个虚拟机和一个备份系统)，现在就是最好的时机。

为了在 `virt-install` 命令里使用一个 Kickstart 文件，需要使用普通的命令开关。由于不允许考生把本书带入考场，因此你尽量不要看本书的主要内容去完成本实验题。你可以参考 `virt-install` 命令的使用网页，在这个手册里可以找到全部重要参数，但是`-x` 或`--extra-args` 除外，它们是用来访问 Kickstart 文件的 URL 地址。

必须把 `ks=` 指示符和 Kickstart 文件的 URL 地址放在引号里。新系统安装完成就算成功。

实验题 6

本实验题旨在理解 `ssh` 命令作为客户端的用法。加密算法必须是透明的，不能影响任何通过 SSH 连接管理远程系统的命令。

实验题 7

对于 RHCSA 几个不同的认证目标，本实验题是相当重要的。一旦掌握其过程，那么实际的操作就相当简单。在完成本实验题后，你应该对自己在以下方面的能力有信心：

- 启动和停止虚拟机器；
- 配置系统以在引导时启动虚拟机器。

本实验题也提供了一个远程访问虚拟机的控制台的方法。

实验题 8

本实验题是为了增加你对两个重要的网络故障排除工具的熟悉程度。它们就是 telnet 和 nmap。具有一定 Linux 经验的网络管理员可能更喜欢其他工具。如果熟悉 nc 等其他工具那最好不过了，因为结果才重要。



第 3 章

基本的命令行技术

认证目标

- ✓ 3.01 shell
- ✓ 3.02 标准命令行工具
- ✓ 3.03 文本文件的管理
- ✓ 3.04 本地在线文档
- ✓ 3.05 网络入门
- ✓ 3.06 网络配置与故障排除
- ✓ 小练习
- ✓ 自测题

Red Hat 认证考试是极具挑战性。本章介绍 RHCSA 考试的一些要求，这些要求过去曾是现已淘汰的 RHCT 认证考试的先决条件。其中许多要求规定了基本的命令行工具，这些工具都与 Linux Professional Institute 提供的初级证书考试有关。

由于这些命令行技术不再是 RHCSA 考试的先决条件，因此本章把它们与网络配置目标结合在一起。配置网络连接时要用到这些命令行工具的一部分。

由于大多数准备参加 RHCSA 考试的考生都已经熟悉了这些命令行工具，因此本章将简单介绍相关内容。在阅读本章后如果仍然觉得需要深入了解这些内容，可以阅读第 1 章介绍的其他优秀的 Linux 入门教材。

Linux 专家(gurus)应该能看出，为了尽可能缩短本章的篇幅，本书简化了许多主题内容。但由于大多数 IT 专业人士都是该领域的专家，因此可能对本章的某些主题没有把握，这是完全可以理解的。事实上，许多有经验的 Linux 管理员并不经常使用每个命令。许多考生通过自学和实践很快弥补这方面的差距。

考试内幕

shell

与 shell 有关的 RHCSA 认证目标都是非常普通的：

- 访问 shell 命令提示符并用正确的语法发布命令；掌握管道和 I/O 重定向功能。

Linux 默认的 shell 是 bash，它代表“Bourne-Again shell”。事实上，最初发布的 RHCSA 认证目标指定使用 bash。然而，许多 Linux 专家也使用其他 shell。

不管选择哪个 shell，都需要知道如何进入到 shell 提示窗口并在提示窗口中执行常用命令。有些基本命令也在其他认证目标中介绍。我们很容易从控制台和 GUI 打开一个 shell 提示窗口。

管道和重定向

在 Linux 中经常把 shell 的数据输入输出看成信息流。一个基本的 Linux 技术是能够重定向这些输入输出流。正如 RHCSA 认证目标所要求的那样，考生应能够：

- 掌握输入/输出重定向符(>、>>、|、2>等)的使用。

上述括号中的操作符可以重定向来自命令输出，命令错误、数据文件以及其他形式的数据流。

文件和目录的管理

进入命令行窗口后，下一个需要掌握的基本技术是文件和目录的管理。利用相关的命令，我们可以在 Linux 目录树中到处导航，并执行相关认证目标要求的所有操作：

- 建立/删除/复制/移动文件和目录。
- 创建硬链接和软链接。

分析文本输出

大多数 Linux 配置文件都采用文本格式。正因为如此，必须理解和分析经过 shell 的文本流。为此需要掌握 grep 命令类的工具的使用，它可以帮助我们找到所需要的信息。通过这种方法分析如何实现以下的认证目标：

- 用 grep 和正则表达式分析文本输出。

本地帮助文档的多样性

虽然在 Red Hat 考试期间是不可以访问 Internet 的，但是这不重要。Google 并不是你唯一的朋友。Linux 的许多程序包都已安装了一些非常好的文档，此外也可以使用命令手册。以下的认证目标不言而喻，它描述了与大多数 Linux 在线文档有关的命令和目录。

- 用 man、info 和/usr/share/doc 目录的文件可以定位、阅读和使用系统文档。
此认证目标还包括另一个有趣的要求：
 - 注意：Red Hat 考试中可能会用到一些 Linux 企业版中并不包含的应用程序，目的是测验考生实现上述目标的能力。

大多数 Linux 开发人员都只使用系统文档规定的基本参数。Red Hat 的“注解”(Note)内容是否将一些重要的信息隐藏在/usr/share/doc 目录中的手册页面或文件中？Note 这个词提醒你要考虑到这种情况。

使用文本编辑器

为了配置 Linux，需要知道如何编辑文本文件。对那些 Linux 的初学者而言，这属于另外一种范例。尽管像 OpenOffice.org Writer 和微软 word 等字处理软件也可以生成文本格式文件，但是在关键配置文件的一个错误可能会使 Linux 系统无法启动。因此需要掌握如何实现以下认证目标：

- 创建和编辑文本文件。

管理网络服务

虽然有非常优秀的 GUI 工具可以帮助用户管理网络服务，但是用这样的工具很容易产生错误。命令行工具可以帮助用户直接管理和了解网络服务，或通过相关的配置文件管理网络服务。相应的认证目标是：

- 启动、停止和检查网络服务的状态。
当然，这个目标要求考生要理解 IP 网络连接的基本概念。

网络配置和名称解析

名称解析是基于一个主机名数据库，或者像 server1.example.com 这样的完全限定域名(fully qualified domain names, FQDN)和如 192.168.122.50 这样的 IP 地址。名称解析还依赖于本地主机名、保存在本地/etc/local/hosts 中的域名和 IP 地址数据库，以及域名解释服务器(DNS)上的可用数据库。这就是对以下 RHCSA 认证目标的解释：

- 配置网络和主机名的静态解析模式和动态解析模式。
Red Hat 首次发布 RHCSA 认证目标时，这个目标被分解成两个目标。虽然这些目标不再是 Red Hat 的官方内容，但是它们确实提供了网络配置和主机名解释的更丰富的内容：

- 管理网络设备：掌握基本的 IP 网络/路由、静态或动态配置 IP 地址/默认值。
- 管理名称解析：设置本地主机名、配置/etc/hosts、配置使用现有的 DNS 服务器。

虽然网络故障排除不再是初级 Red Hat 考试的一部分，但是，我们处理网络配置和名称解析问题所使用的方法可以更好地帮助我们理解网络的工作模式。

认证目标 3.01 shell

shell 是一个用户接口，它也可用作命令行解释器。在 Linux 中，shell 是一个解释程序，它允许我们用各种命令与 Linux 进行交互。只要有合适的文件权限，我们就可以在脚本文件中设置命令，需要时甚至可以在深更半夜时执行这些脚本文件。Linux shell 可以按各种顺序处理命令，这取决于我们如何管理每个命令的输入和输出。每个 shell 对命令所作的解释部分取决于它所使用的变量和参数。

Linux 中默认的 shell 是 bash，也称为 Bourne-Again shell。本书的主要命令是基于这些命令在 bash 中的用法。但是也存在很多其他的 shell，而且它们也有很多用户。只要能安装相应的 RPM 程序包，则用户可以启动任何一个 shell。需要时可以在/etc/passwd 文件中改变每个用户的默认 shell。

3.1.1 其他 shell

RHEL 6 中有 4 种 shell，用户可以选择自己的命令行解释程序。虽然 bash 是默认的 shell，但是长期使用 Linux 和 Unix 的用户可能喜欢其他 shell：

- **bash** 默认的 Bourne-Again shell，它是以 Stephen Bourne 最早开发的命令行解释程序为基础。
- **dash** 一个比 bash 更简单、功能较少但速度更快的 shell。
- **tsh** Unix C shell 的增强版。
- **zsh** 一个高级 shell，类似于 Korn shell。

这些 shell 都在/bin 目录中配置。如果用户想把其中一个作为默认的 shell，则并非难事。最直接的方法是在/etc/passwd 文件中修改默认 shell。例如，此文件中应用于我的一个普通账户的一行内容是：

```
michael:x:1000:1000:Michael Jang:/home/michael:/bin/bash
```

例如，要把默认的 shell 改为 dash，只需要把/bin/bash 改为/bin/dash。

考试提示

尽管对大多数 Linux 用户来说很容易，但是 RHCA 一个认证目标的一部分是“访问 shell 提示符”。现在你应该知道如何访问不同的 shell 提示符窗口。

3.1.2 终端控制台

默认情况下，RHEL 系统可以使用 6 个命令行控制台。它们是由/etc/init 目录中的 start-ttys.conf 文件定义的。打开该文件就会发现这些控制台是为运行级 2、3、4、5 定义的。这 6 个控制台分别由/dev/tty1 到/dev/tty6 这 6 个设备文件来控制的。当系统配置了一个 GUI，则它使用 /dev/tty1。我们可以配置更多的虚拟控制台，但是受为 root 管理员用户分配的控制台数量限制。root 管理员用户配置文件为/etc/securetty。

通常情况下，要在控制台之间切换，要按下 Alt 和每个控制台对应的功能键。例如，Alt+F2 键可以切换到第二个控制台。但是在 RHEL GUI 中，Alt+F2 键组合用来启动 Run Application 工具。

具。因此，需要按 **Ctrl+Alt+F2** 才可以切换到第二个控制台。

登录文本控制台时会看到如下的提示信息，但是具体内容可能会因 RHEL 的版本、内核的版本号以及系统的主机名而稍有差异：

```
Red Hat Enterprise Linux release 6.0 (Santiago)
Kernel 2.6.32-71.el6.x86_64 on x86_64

server1 login:
```

用图形模式登录时会更加直观，如图 3-1 所示，但是需要安装 GNOME 显示管理程序(GNOME Display Manager, GDM)。

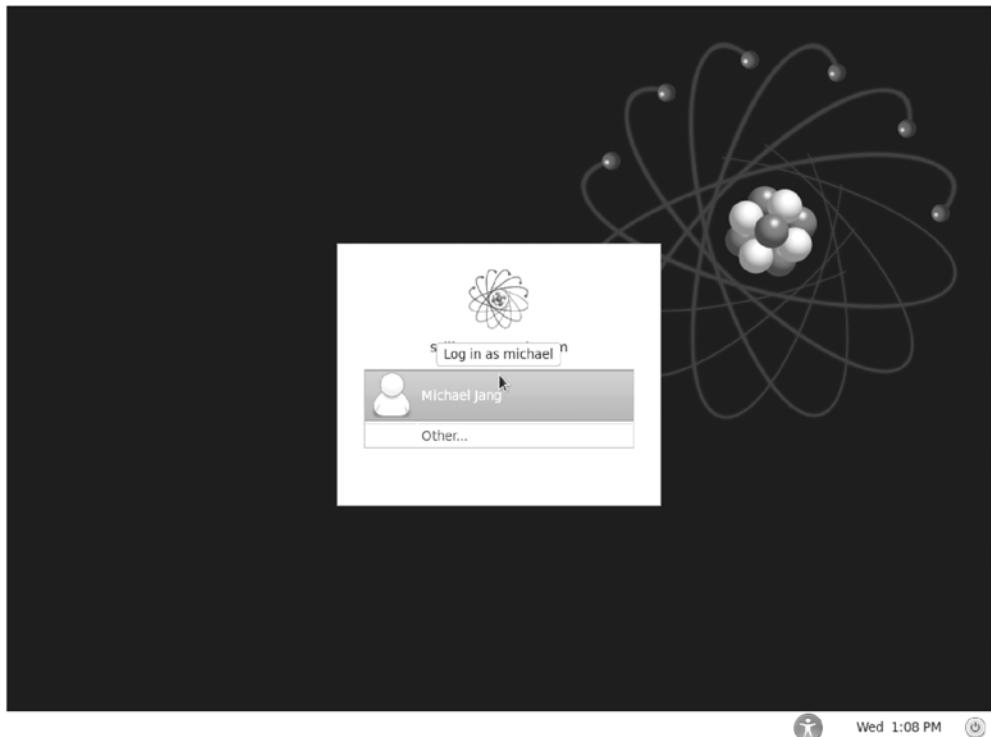


图 3-1 第一个 GUI 登录控制台

3.1.3 GUI shell 接口

登录到 GUI 后，访问 `bash` 就很容易。如果我们使用默认的 GNOME 桌面环境，则单击 `Application | System Tools | Terminal`。传统上，管理员总是从控制台控制计算机的。但在许多情况下从 GUI 环境访问命令行控制台可能会更加方便，特别当多个控制台并排出现在屏幕上时。右击 GUI 终端界面可以打开另外的终端窗口。需要时它还支持终端窗口之间的复制与粘贴。

本书使用的命令行截图都是以 GUI 的命令行窗口为依据，部分原因是在白色屏幕上的黑字更容易阅读。

3.1.4 普通用户与管理员用户的区别

在命令行窗口可以执行的命令取决于登录账户所拥有的权限。现在有两个基本的提示符。

下面是普通用户登录后看到的提示符:

```
[michael@server1 ~]$
```

注意, 屏幕上出现了用户名、本地系统的主机名、当前目录和\$提示符。\$是普通用户的标准提示符。在本书的前言中曾提到, 普通用户执行命令后只显示如下内容:

```
$
```

与此相反, 在同一个系统上来看看超级管理员用户的提示符。它与普通用户的提示信息相似, 除账户名不同外, 唯一的区别是提示符:

```
[root@server1 ~]#
```

因此超级管理账户执行的命令显示结果如下:

```
#
```

除所有权、权限外, 普通用户与管理员用户的其他差别将在第 8 章中介绍。

3.1.5 文本流与命令重定向

Linux 使用三个基本数据流。数据输入流, 数据输出流和向另一个方向发送的错误。这些流分别被称为标准输入(stdin)、标准输出(stdout)和标准错误(stderr)。通常情况下, 输入来自键盘, 输出到屏幕, 而错误要发送到一个缓存中。错误消息也可以发送到屏幕(作为文本流 2)。在下面的示例中, filename 是 cat 命令的输入流。

```
# cat filename
```

当执行 cat filename 这个命令时, 系统把文件的内容作为标准输出发送到屏幕。

也可以把这些流重定向入或重定向出文件。例如, 有一个名为 database 的程序和一个包含大量数据的数据文件。用左重定箭头(<)可以把此数据文件的内容发送到这个数据库程序。如下所示, 这里的数据文件(datafile)被当作标准输入:

```
# database < datafile
```

标准输入也可以来自某一个命令的左侧。例如, 当我们需要翻页浏览引导信息时, 可用管道把 dmesg 和 less 两个命令组合在一起:

```
# dmesg | less
```

这里把 dmesg 命令的输出重定向为 less 的标准输入。后者对前者的输出内容进行翻页浏览, 就像它是一个独立文件一样。

标准输出重定向也一样容易。例如, 下面的命令用右向重定向符(>)把 ls 命令的输出发送到名为 filelist 的文件中。

```
# ls > filelist
```

还可以用双重定向箭头命令如 ls>>filelist 在当前文件的末尾添加标准的输出流。

如果认为某个程序会产生错误, 则用下面的命令重定向此程序的错误流:

```
# program 2> err-list
```

考试提示

>、>>、2> 和 | 等命令重定向符在 RHCSA 认证目标中属于“输入/输出重定向符”。

认证目标 3.02 标准命令行工具

虽然 Linux 初学者可能更喜欢使用 GUI，但管理 Linux 系统最有效的工具还是命令行接口。虽然目前存在一些很好的 GUI 工具，但是这些工具的外观和操作模式随不同的发行版而异。与此相反，如果我们掌握了标准的命令行工具，则可以方便自如地操作每个 Linux 发行版。

有两组基本的命令用来管理 Linux 文件。一组是操作 Linux 文件和目录，另一组实际上可以对文件做更进一步的操作。记住，在任何对 Linux 文件的操作中，我们可以利用前面执行过的命令的历史(HISTORY)记录(之所以用大写字母表示，是因为它是一个标准的环境变量)，以及命令自动补全功能。自动补全功能允许我们用 Tab 键完成一个命令或文件名，或者给我们提供绝对路径的选项。

几乎所有的 Linux 命令都有开关选项。利用这些选项可以执行更多的操作。本章不涉及这些选项的用法。如果你对这些选项不熟悉，而可以用 man 文档。仔细研究这些选项，然后在 Linux 中进行测试。只有不断实践才会理解这些命令的强大功能。

考试提示

本节只讨论 Linux 中的最常用命令，只介绍这些命令的几个最基本的功能。尽管如此，本节要求你用正确的语法执行命令，这正是 RHCSA 认证目标所要求的。

3.2.1 文件与目录的概念

如前所述，在 Linux 中任何东西都可以表示为文件。目录是特殊类型的文件，它是保存其他文件的容器。为了找到重要的文件，需要介绍一些基本概念，它们告诉你当前所在的位置以及如何从一个目录切换到另一个目录。该命令就是 pwd 命令、波浪形字符(~)和路径。使用波浪形字符(~)可以切换到用户的主目录；而路径是描述 Linux 目录树中位置的一个概念。与它们紧密相关的是在执行命令时搜索的目录，它与一个名为 PATH 的环境变量有关。掌握了这些概念后，就可以用 cd 命令在目录之间切换。

1. pwd 命令

在命令行接口，当前目录可能是顶层目录(即为根目录，用/表示)，也可能是一个子目录。pwd 命令可以确定当前目录。试试这个命令，它显示一个相对于顶层根目录(/)的目录名。有了这个信息，必要时我们就可以切换到其他目录。顺便指出，pwd 是打印工作目录这三个单词的首字符(print working directory)(它与现代的打印机没有任何关系)。例如，当我在自己的主目录中执行 pwd 命令，则看到下面的输出信息：

```
/home/michael
```

2. 波浪符(~)

使用标准的登录方式时，每个 Linux 用户都处于一个主目录中。波浪符(~)可以用来表示当前用户的主目录。例如，当用户 john 登录时，它处在/home/john 主目录中。与此对应，root 管理员用户的主目录是/root。

因此，cd ~命令的效果取决于用户名。例如，如果以用户 mj 登录到系统，则 cd~命令导航到 /home/mj 目录，如果以 root 用户登录到系统，则此命令导航到/root 目录。在目录树中任何位置都可以用 ls ~命令列出自己主目录中的内容。稍后将介绍 cd 和 ls 命令的使用。当我以 root 用户登录到系统并执行 ls 命令，就会看到如下内容：

```
anaconda-ks.cfg install.log install.log.syslog
```

顺便指出，这些文件说明在安装过程中发生的事情，即安装了哪些程序包，在本地系统添加了哪些用户和组等。anaconda-ks.cfg 命令是 Kickstart 自动安装的重要工具，这在第 2 章已经讨论过。

3. 目录路径

使用 Linux 目录时需要掌握路径的两个基本概念：绝对路径和相对路径。绝对路径是从顶层目录(即 root 目录/)的角度来描述完整的目录结构。相对路径是以当前目录为基准。相对路径的最前面没有斜杠。

掌握绝对目录与相对目录的区别很重要。特别当创建一个脚本文件时，绝对目录是必需的。否则脚本会从其他目录开始执行，这会导致意想不到的结果。例如，假如当前在顶层 root 目录，我们想用相对路径备份/home 目录。如果恢复该备份时我们正好在/home 目录中，则 michael 用户的文件就会恢复到/home/home/michael 目录中。

相反，如果用绝对路径备份/home 目录，则在恢复这些备份文件时当前目录不起作用。备份数据会恢复到正确的目录中。

4. 环境路径

严格来说，在执行一个命令时必须引用这个命令的完整路径。例如，既然 ls 命令是在/bin 目录中，因此用户应该执行/bin/ls 命令以列出当前目录中的文件。

有了 PATH 环境变量，命令前不需要加上它的完整路径。当我们在命令行输入一个命令时，bash shell 自动会在 PATH 环境变量的路径中搜索这个命令。从一个控制台切换到另一个控制台，环境变量总保持不变。

为了确定当前用户的 PATH 环境变量的内容，只需要执行 echo \$PATH 命令。这会看到在屏幕上输出一系列目录。在 RHEL 6 中，普通用户的 PATH 变量与 root 用户的 PATH 变量的差别不大。

```
$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin

# echo $PATH
/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin
```

现在，普通用户与 root 用户的 PATH 变量包含的目录几乎完全相同，但是差别还是有的，那就是搜索目录的顺序。例如，/usr/bin 和/usr/sbin 这两个目录都可以使用 system-config-keyboard 命令。从普通用户和超级管理员用户 PATH 变量的默认内容可以看出，由于 PATH 变量存在的差别，因此两者的执行方法不一样。

PATH 是由/etc/profile 文件的当前设置参数全面决定的。你可能注意到，系统为 UserID(UID)0 用户与其他用户配置的 PATH 内容不大一样。UID 0 对应于 root 管理员用户。

某个用户的 PATH 变量可以由该用户主目录中的一个适当的记录来加以定制，此隐藏文件名为.profile。

5. cd 命令

在 Linux 中切换目录非常容易。只要用 cd 并列出目标目录的绝对路径即可。如果使用相对路径，务必记住目标目录取决于当前目录。

默认情况下，单独使用 cd 命令可以导航到用户的主目录，该命令不需要波浪形符。

3.2.2 文件列表和 ls 命令

既然已经知道了从一个目录导航到另一个目录的命令，现在该来看看目录中有哪些文件。这就要用到 ls 命令。

Linux 的 ls 命令加上合适的开关选项，是一个功能非常强大的命令。正确使用 ls 命令可以获得文件的全部信息，如创建日期、最后访问日期和文件大小等。可以按任何顺序排列文件，这对我们非常有用。ls 命令的几个重要变化形式是，ls -a 显示隐藏文件，ls -l 长列表显示文件，ls -t 按时间顺序排列文件，ls -i 显示的 inode 数。这些开关选项可以组合使用。我经常用 ls -ltr 命令显示最近修改的文件。-d 开关选项与其他选项一起可以提供当前目录的更多信息。

ls -Z 命令的一个很重要的作用是返回 SELinux 上下文。分析图 3-2 中的输出结果，system_u、object_r、var_t 和 s0 等输出信息表示这些文件的当前 SELinux 上下文。在 RHCSA 考试中(RHCE 考试也一样)，考生需要配置一个启动 SELinux 服务系统。从第 4 章开始将介绍如何为系统的每个服务配置 SELinux。

```
[root@server1 ~]# \ls -Z /var/
drwxr-xr-x. root root system_u:object_r:acct_data_t:s0 account
drwxr-xr-x. root root system_u:object_r:var_t:s0 cache
drwxr-xr-x. root root system_u:object_r:var_t:s0 crash
drwxr-xr-x. root root system_u:object_r:cvs_data_t:s0 cvs
drwxr-xr-x. root root system_u:object_r:var_t:s0 db
drwxr-xr-x. root root system_u:object_r:var_t:s0 empty
drwxr-xr-x. root root system_u:object_r:gams_data_t:s0 games
drwxrwx--T. root gdm system_u:object_r:xserver_log_t:s0 gdm
drwxr-xr-x. root root system_u:object_r:var_lib_t:s0 lib
drwxr-xr-x. root root system_u:object_r:var_t:s0 local
drwxrwxr-x. root lock system_u:object_r:var_lock_t:s0 lock
drwxr-xr-x. root root system_u:object_r:var_log_t:s0 log
lrwxrwxrwx. root root system_u:object_r:mail_spool_t:s0 mail -> spool/mail
drwxr-xr-x. root root system_u:object_r:var_t:s0 nis
drwxr-xr-x. root root system_u:object_r:var_t:s0 opt
drwxr-xr-x. root root system_u:object_r:var_t:s0 preserve
drwxr-xr-x. root root system_u:object_r:var_t:s0 report
drwxr-xr-x. root root system_u:object_r:var_run_t:s0 run
drwxr-xr-x. root root system_u:object_r:var_spool_t:s0 spool
drwxrwxrwt. root root system_u:object_r:tmp_t:s0 tmp
drwxr-xr-x. root root system_u:object_r:var_yt:s0 yp
[root@server1 ~]#
```

图 3-2 当前的 SELinux 上下文

3.2.3 文件创建命令

有两个命令可用来创建新文件，它们是 `touch` 和 `cp`。也可以用 `vi` 文本编辑器创建一个新的文件。当然，尽管 `ln`、`mv` 和 `rm` 命令不会创建文件，但是它们确实可以用自己的方法管理文件。

1. touch 命令

新建一个文件的最简单方法也许是用 `touch` 命令。例如，`touch abc` 命令在本地目录中创建了一个名为 `abc` 的空文件。`touch` 命令也用来修改文件的最后访问日期。例如，试试下面三个命令：

```
# ls -l /etc/passwd
# touch /etc/passwd
# ls -l /etc/passwd
```

注意与每个 `ls -l` 命令的输出有关的日期和时间。文件的当前日期和时间都会发生改变，这与 `date` 命令有关。

2. cp 命令

`cp(copy)` 命令允许我们把一个文件的内容复制到同名或不同名的文件中，复制得到的文件可以在任何目录。例如，`cp file1 file2` 命令读取 `file1` 的内容，并将它保存到 `file2` 中。使用 `cp` 命令的一个风险是它会在不提示用户的情况下很容易覆盖掉不同目录中的文件。

`cp` 命令如`-r` 开关选项支持递归复制。例如，下面的命令将复制源目录中所有子目录以及相关文件。

```
# cp -ar /usr/share/doc/. /doc/
```

3. mv 命令

虽然在 Linux 中不能重命名一个文件，但是可以移动文件。`mv` 命令实质上是给文件贴上不同的标签。例如，`mv file1 file2` 命令就是把 `file1` 的名字改为 `file2`。除非把一个文件移动到另一个分区，否则这个文件的全部内容包括索引节点数(inode number)都没有改变。`mv` 命令也可用于目录。

4. ln 命令

链接文件允许用户编辑不同目录中的同一个文件。当链接文件是设备文件时，它们只代表一些比较常用的名字，如 `/dev/dvd`。链接文件可以是硬链接，也可以是软链接。

硬链接包含了文件的一个副本。只要硬链接文件是在同一个分区中，则它们的索引号相同。可以删除一个目录中的一个硬链接文件，但是它还存在于另一个目录中。例如，下面这个命令在实际的 Samba 配置文件和本地目录中的 `smb.conf` 之间建立了硬连接(`smb.conf`)。

```
# ln /etc/samba/smb.conf smb.conf
```

另一方面，软链接起着重定向的作用。当我们打开一个用软链接创建的文件时，则链接把我们重定向到原来的文件。如果我们删除原来的文件，则链接就中断。虽然软链接还在使用，但是它没有用。下面这个命令说明了如何创建一个软链接文件：

```
# ln -s /etc/samba/smb.conf smb.conf
```

5. rm 命令

rm 命令有点危险。Linux 命令行中没有回收站。因此当我们要用 **rm** 命令删除一个文件后，就很难恢复这个文件。

rm 命令也很强大。例如，当我们下载了 Linux 内核的源文件后，则在/root/rpmbuild/BUILD/kernel-2.6.32-71.1.el6 目录中有几千个文件。逐一删除这些文件是不切实际的，而 **rm** 命令提供了几个功能强大的选项。下面这个命令可以一次性删除所有这些文件：

```
# rm -rf /root/rpmbuild/BUILD/kernel-2.6.32-71.1.el6
```

-r 开关选项可以按递归方式进行，-f 开关选项可以覆盖掉任何安全措施，如系统为 root 用户创建的 alias 命令的安全措施。它仍然是一个十分危险的命令。例如，在下面的命令中，/ 与后面的目录名之间多了个空格。

```
# rm -rf / root/rpmbuild/BUILD/kernel-2.6.32-71.1.el6
```

这样一个简单的输入错误就会删除自顶层根目录开始的全部文件，然后删除 root/rpmbuild/BUILD/kernel-2.6.32-71.1.el6 子目录。

6. 目录创建和删除

mkdir 和 **rmdir** 命令用来创建和删除目录。这两个命令的使用方法取决于前面讨论的绝对目录和相对目录的概念。例如，下面的命令在当前目录中创建 test 子目录。但是如果用户现在 /home/michael 目录中，则完整的路径为/home/michael/test。

```
# mkdir test
```

也可以用下面的命令创建/test 目录：

```
# mkdir /test
```

必要时可以用下面的命令创建一串目录：

```
# mkdir -p /test1/test2/test3
```

上述命令相当于以下命令：

```
# mkdir /test1
# mksdir /test1/test2
# mkdir /test1/test2/test3
```

相反，**rmdir** 命令可以删除一个目录，条件是它必须是一个空目录。如果我们想删除前面 **mkdir** 命令创建的目录，则-p 选项特别有用。下面这个命令删除前面提到的目录和它的子目录，条件是这些目录必须都为空：

```
# rmdir -p /test1/test2/test3
```

7. alias 命令

alias 命令可以用来简化几个命令。对于 root 用户，默认的别名可以提供一点安全性。要查看当前用户的别名，只需要运行 alias 命令。下面是 Red Hat 为 root 用户设置的别名列表：

```
alias cp='cp -i'
alias l.='ls -d .* --color=auto'
alias ll='ls -l --color=auto'
alias ls='ls --color=auto'
alias mv='mv -i'
alias rm='rm -i'
alias which='alias | /usr/bin/which --tty-only --read-alias
--show-dot --show-tilde'
```

有些 alias 命令可以防止重要文件被错误删除。-i 开关选项在用 cp、mv 或 rm 命令删除或覆盖掉文件之前要求用户确认。同时还要注意，-f 开关选项取代这些命令的-i 开关选项。

实际经验

正如技术编辑所建议的那样，有些系统管理员为 rm 设置了别名：alias rm='mv -t ~/.Trash'。该目录中的文件相当于一个标准的回收站。GNOME 桌面系统的默认回收站目录可以在每个用户的.local/share/Trash/files/子目录中找到。

3.2.4 通配符

有时，我们可能并不知道文件的精确名字或者准确的搜索条件，此时可以使用通配符，特别是在本书介绍的命令中。三个基本的通配符如表 3-1 所示。

表 3-1 shell 中的通配符

通配符	说明
*	代表任意个字母数字字符(也表示 0 个字符)。例如，ls ab*命令就会列出以下文件名(假设有这些文件): ab、abc、abcd
?	代表一个任意的字母数字字符。例如，esab?命令返回当前目录中的以下文件名: abc、abd、abe
[]	范围选项。例如 ls ab[123]命令返回以下文件名(假设当前目录中有这些文件): ab1、ab2、ab3。也可以通过 ls ab[X-Z]命令返回以下文件名(假设当前目录有这些文件): abX、abY、abZ

实际经验

在 Linux 领域中，通配符有时也被称为文件名代换(globbing)。

3.2.5 文件搜索

大多数用户在学习 Linux 一段时间后就熟悉了一些重要的文件。例如，named.conf 是标准 DNS(Domain Name Service,DNS)服务器的关键配置文件，这些服务器是基于伯克利因特网名字域(Berkeley Internet Name Domain, BIND)的。但是并不很多人都能记得住 named.conf 示例文件以及很多有用的配置信息，这些信息保存在/usr/share/doc/bind-*/sample/etc 目录中。

为此，有两个基本命令可用于文件搜索：find 和 locate。

1. find 命令

find 命令在目录以及子目录中搜索所需要的文件。例如，当我们想找到 DNS 配置文件实例文件 named.conf 所在的目录，可以使用下面的命令，此命令从根目录开始搜索：

```
# find / -name named.conf
```

但是搜索的速度取决于本地系统的内存大小和处理能力。随着虚拟机的出现，CPU 的处理能力相对变弱。或者如果用户知道某个文件位于/usr 子目录树中，则可以从那个目录开始使用如下命令：

```
# find /usr -name named.conf
```

现在这个命令就可以更快地找到所需要的文件。

2. locate 命令

如果这一切还是太费时间，RHEL 允许用户创建一个数据库，它保存了全部的安装文件和目录。用 locate 命令搜索文件几乎是即时完成的，而且 locate 搜索不需要完整的文件名。locate 命令的缺点是此数据库通常每天只更新一次，这在/etc/cron.daily/mlocate.cron 脚本文件中有记录。

每 24 个小时才更新一次可能不够，特别是在 2 小时的考试期间。幸运的是，前面提到的这个脚本文件可以直接由 root 用户从命令行接口中执行。只需要输入这个文件的完整目录就行，就好像它是一个命令一样：

```
# /etc/cron.daily/mlocate.cron
```

考试提示

在参加 Red Hat 考试期间，我执行了前面提到这个 mlocate.cron 脚本，它帮助我更快地找到所需要的文件。

认证目标 3.03 文本文件的管理

Linux 和 Unix 都是通过一系列的文本文件进行管理的。Linux 系统管理员通常不喜欢用图形编辑器管理这些配置文件。像 WordPerfect、OpenOffice.org Writer 甚至微软的 Word 这类的编辑器通常会把文件保存为二进制格式，或者会添加上许多标志。除非文本文件按原始格式保存且不含任何标签，否则对文本做任何修改都可能导致 Linux 系统无法启动。

Linux 命令把文本文件当作数据流进行管理。你在前面已经看到重定向符和管道符等工具的作用。但是如果我没有合适的工具将数据进行分类处理，我们可能会被数据淹没了。但是即使在对文件进行编辑之前，也必须要知道如何在命令行接口读取这些文本文件。

3.3.1 文本流的读命令

前面已经学习了 cd、ls 和 pwd 用于处理 Linux 文件的命令。加上 find 和 locate 命令，我们已掌握了如何确定所需要文件的位置。

现在该是如何浏览、复制和移动文件的时候了。大多数 Linux 配置文件都是文本文件, Linux 编辑器就是文本编辑器。Linux 命令就是为读取文本文件而设计的。为确定当前目录中文件的类型, 可以试试 file *命令。

1. cat 命令

最简单的文本文件读取命令是 cat。cat filename 命令可以翻页显示 filename 文件的内容。它也可以处理多个文件名。它把多个文件的内容合并在一起, 并将其连续输出到屏幕上。也可以把输出结果重定向到自己喜欢的文件名中, 这将在后面的“文本流和命令重定向”一节中讨论。

2. less 和 more 命令

大文件需要一个可以让用户悠闲自在浏览文件内容的命令, 它们就是 more 和 less。用 more filename 命令可以翻页显示文本文件的内容, 每次一个屏幕从头到尾显示。使用 less filename 命令, 我们可以用 PAGE UP 和 PAGE DOWN 键向前或向后翻页查看同样的文本。这两个命令都支持 vi 模式搜索:

```
# less /var/log/messages
```

然后就可以翻页显示日志文件以搜索文件中的重要信息。接下来可以用向前的斜杠(/)和问号在文件中搜索。例如, 当我们执行了上述命令后, 就会出现如图 3-3 所示的窗口。

例如, 要在文件中向前搜索 “IPv4 tunneling”, 只要在命令行窗口的底部输入下面的内容即可:

```
/IPv4 tunneling
```

如果要按相反的方向搜索, 则只要把/改为? 即可。

```
Nov 29 08:15:02 server1 kernel: imklog 4.6.2, log source = /proc/kmsg started.
Nov 29 08:15:02 server1 rsyslogd: [origin software="rsyslogd" swVersion="4.6.2"
x-pid="1132" x-info="http://www.rsyslog.com"] (re)start
Nov 29 09:43:01 server1 NetworkManager[1219]: <error> [1291052581.244599] [nm-ma
nager.c:1312] user_proxy_init(): could not init user settings proxy: (3) Could n
ot get owner of name 'org.freedesktop.NetworkManagerUserSettings': no such name
Nov 29 09:43:04 server1 NetworkManager[1219]: <error> [1291052584.455664] [nm-ma
nager.c:1312] user_proxy_init(): could not init user settings proxy: (3) Could n
ot get owner of name 'org.freedesktop.NetworkManagerUserSettings': no such name
Nov 29 09:44:33 server1 kernel: ata2.00: exception Emask 0x0 SAct 0x0 SErr 0x0 a
ction 0x6
Nov 29 09:44:33 server1 kernel: sr 1:0:0:0: CDB: Test Unit Ready: 00 00 00 00 00
00
Nov 29 09:44:33 server1 kernel: ata2.00: cmd a0/00:00:00:00/00:00:00:00/a0
tag 0
Nov 29 09:44:33 server1 kernel: res 01/60:00:00:00/00:00:00:00/a0
Emask 0x3 (HSM violation)
Nov 29 09:44:33 server1 kernel: ata2.00: status: { ERR }
Nov 29 09:44:33 server1 kernel: ata2: soft resetting link
Nov 29 09:44:33 server1 kernel: ata2.00: configured for MWDMA2
Nov 29 09:44:33 server1 kernel: ata2: EH complete
Nov 29 19:05:56 server1 NetworkManager[1219]: <error> [1291086356.880466] [nm-ma
nager.c:1312] user_proxy_init(): could not init user settings proxy: (3) Could n
/var/log/messages
```

图 3-3 less 分布命令和 /var/log/messages 中的内容

less 命令有几个功能是 more 和 cat 这两个命令所没有的。它可以读取用 Gzip 格式压缩的文本文件, 通常这种文件的扩展名为.gz。例如, 许多在 shell 环境执行的标准命令的 man 文档都保存 /usr/share/man/man1 目录中。这个目录中的所有文件都被压缩成.gz 格式的文件。但用 less

命令不需要解压就可以读取这些文件的内容。

这就让我们想起 man 命令的使用。换言之，下面两个命令在功能上是等效的：

```
# man cat
# less /usr/share/man/man1/cat.1.gz
```

3. head 和 tail 命令

head 和 tail 是两个不同的命令，但是它们的用法完全相同。默认情况下，head filename 命令显示一个文件的前 10 行内容。tail filename 命令显示文件的最后 10 行内容。可以用-nxy 开关选项定义需要显示的行数。只要记住在定义行数时不要有空格。例如，tail -n15 /etc/passwd 命令显示/etc/passwd 文件的最后 15 内容。

Tail 命令特别有用，可用于解决执行过程中发生的问题。例如，如果当前系统正有一个问题，则下面的命令可以监测到试图登录到本系统的事件：

```
# tail -f /var/log/secure
```

3.3.2 处理文本流的命令

文本流就是数据的流动。例如，cat filename 命令把来自 filename 的数据流输出到屏幕上。当这些文件变大时，最好先用过滤器命令对这些流进行处理。

为此，Linux 引入了几个简单的命令帮助我们搜索、检查和对文件的内容排序。有些特殊的文件，它们包含其他文件。这些容器文件的一部分俗称为打包工具(tarball)。

实际经验

打包(tarball)是一种发布 Linux 程序包的常用方法。它们通常以一个压缩格式发布程序包，如.tar.gz 或.tgz 文件扩展名，它们把程序包都集中到一个文件中。

1. sort 命令

可以用多种方法对文件的内容进行排序。默认情况下，sort 命令按照字母顺序将文件内容按每行首字符进行排序。例如，sort /etc/passwd 命令把所有用户(包括与某些特定服务有关的用户)按用户名排序。

2. grep 和 egrep 命令

grep 命令使用搜索词搜索文件。它返回包含此搜索词的整行内容。例如，grep "Michael Jang" /etc/passwd 就会在/etc/passwd 文件中查找到本书作者的名字。

egrep 命令更加“宽容”，它允许我们在搜索中使用一些并不常见的字符，如+、?、|、(和)。虽然在 grep 命令中用反斜杠也可以搜索这些字符，但是用起来比较笨拙。

3. diff 命令

diff 是一个非常有用的命令，它可以找出两个文件的差别。如果已经使用过本章后面将要介绍的 Network Connections 工具，此工具会修改/etc/sysconfig/network-script 目录中的一个如 ifcfg-

eth0 文件的内容。

如果已经备份了 ifcfg-eth0 文件，则用 diff 命令可以找出/root 目录中的 ifcfg-eth0 与/etc/sysconfig/network-scripts 目录中 ifcfg-eth0 文件的差别：

```
# diff /root/ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-eth0
```

因此，如果已经把 ifcfg-eth0 文件备份到/root 目录中，则上面的命令会显示 Network Connections 工具对这个文件所做的修改。

4. wc 命令

wc 是单词统计(word count)的缩写符。它可以返回一个文件中的行数、单词数和字符数。wc 命令很容易使用，例如，wc -w filename 命令返回此文件的单词数。

5. sed 命令

sed 命令是流编辑(stream editor)的缩写符，用于搜索并修改文件中指定的单词甚至文本流。例如，下面的命令把 opsys 文件每一行的第一个 Windows 改为 Linux，并把结果保存到 newopsys 文件中：

```
# sed 's/Windows/Linux/' opsys > newopsys
```

但这还不是 sed 的全部功能。如果在 opsys 文件中的一行有不止一个 Windows，这个命令不会替换第二个 Windows，但是增加“全局”后缀符(g)就可以做到这一点：

```
# sed 's/Windows/Linux/g' opsys > newopsys
```

下面的示例确保所有用 writable=yes 指示符配置的 Samba 共享参数都被改为 writable=no：

```
# sed 's/writable = yes/writable = no/g' /etc/samba/smb.conf > ~/smb.conf
```

当然，在原来的/etc/samba/smb.conf 文件被覆盖之前，最好先浏览/root/smb.conf 文件中的内容。

6.awk 命令

awk 命令是以它的开发者命名的(Aho、Weinberger 和 Kernighan)，它更像是一个数据库操作命令。它用一个关键字确定所在的行，可以读取这行的从指定列开始的内容。一个常用的示例是它作用于/etc/passwd 文件。例如，下面这个命令输出所有用户名中有 mike 的用户名：

```
# awk '/mike/ {print $1}' /etc/passwd
```

3.3.3 在控制台编辑文本文件

RHCSA 认证目标的最初版本明确要求考生需要掌握 vim 的使用。严格地说，无论用哪个文本编辑器来编辑文本文件都没有关系。但我认为你应该了解 vim 编辑器的用法，显然 Red Hat 的许多人也同意我这个观点。vim 编辑器是 vi 编辑器改进版(vi improved)的缩写。安装后可以用 vi 命令启动 vim 编辑器。从现在开始我们就用 vi 代表这个编辑器。

我认为每个系统管理员都应对 vi 有一个基本的了解。虽然 emacs 可能更加灵活，也更加流

行，但是 vi 可以帮助我们解决一个有故障的系统。如果你曾经用紧急引导媒介恢复一个重要的配置文件，则 vi 可能是唯一可用的编辑器。

虽然 RHEL 6 也包含了对一个更加直观的 nano 编辑器的访问，但是掌握 vi 命令可以帮助我们快速确定 man 文档和其他文本文件中的关键内容。虽然 RHEL 急救媒介(rescue media)提供了更多的基于控制台的编辑器，但是这里之所以只介绍 vi 是因为 vi 是我最熟悉的编辑器。

应该掌握 vi 的两种基本模式：命令模式和插入模式。当我们用 vi 打开一个文件时，它就处于命令模式。有些命令会启动插入模式。打开一个文件很容易，用 vi filename 命令即可。默认情况下，这个命令启动 vi 的命令模式。图 3-4 是 vi 命令打开/etc/nsswitch.conf 文件的一个示例。

下面是对 vi 编辑器的最简单的介绍。要想掌握更多的内容有很多图书可以选择，另外有一个广泛使用的手册，它以 HOWTO 的格式介绍 vi 的用法，它来自于 www.tldp.org 网站上的 Linux 文档项目。也可以用 vimtutor 命令可以得到一个 vi 教程。

1. vi 的命令模式

处于命令模式时，除了编辑外还可以对一个文本文件做任何操作。在命令模式下可以使用的选项非常多且经常变化，用几本书也描述不完。归纳起来 vi 命令的选项可分为 7 类：

- **打开** 在命令行接口用 vi 编辑器打开一个文件，即执行 vi filename 命令。
- **搜索** 向前搜索，反斜杠(/)后面加上搜索词。记住，Linux 是大小写敏感的，因此要用 /Michael(而不是/michael)命令来搜索/etc/passwd 文件中“Michael”。向后搜索要用问号(?)。
- **写入** 保存编辑后的结果要用 w 命令。可以结合其他命令，如:wq 写入文件并退出 vi。
- **关闭** 用:q 命令退出 vi 编辑器。
- **放弃** 放弃任何修改要用:q!命令。
- **编辑** 可以用 vi 的很多命令编辑文件。例如，x 删除当前光标所在的字符；dw 删除当前光标所在单词；dd 删除当前行。记住，p 把字符复制到缓存中。U 取消前一次的修改。
- **插入** 有很多命令可以启动插入模式。按 i 在当前位置开始插入文本，按 o 在光标当前插入一空行。

2. 基本的文本编辑

在现在的 Linux 系统中，用 vi 编辑文件是一件非常容易的事。只需要常用的导航键(方向键、PAGEUP 和 PAGEDOWN)，然而用 i 和 o 等基本命令启动 vi 的插入模式，直接在文件中输入新的内容。当结束插入模式时，按 ESC 键返回到命令模式。这时可以保存、放弃编辑结果，

```

passwd:      files
shadow:      files
group:       files

#hosts:      db files nisplus nis dns
hosts:       files dns

# Example - obey only what nisplus tells us...
#services:   nisplus [NOTFOUND=return] files
#networks:   nisplus [NOTFOUND=return] files
#protocols:  nisplus [NOTFOUND=return] files
#rpc:        nisplus [NOTFOUND=return] files
#ethers:     nisplus [NOTFOUND=return] files
#netmasks:   nisplus [NOTFOUND=return] files
#bootparams: nisplus [NOTFOUND=return] files
#
# ethers:    files
# netmasks:  files
# networks: files
# protocols:files
# rpc:       files

```

图 3-4 用 vi 编辑/etc/nsswitch.conf 文件

并退出 vi 程序。

实际经验

vi 命令有几个专用的版本。vipw、vigr 和 visudo 命令分别用来编辑 /etc/passwd、/etc/group 和/etc/sudoers 文件。vipw -s 和 vigr -s 命令分别编辑/etc/shadow 和/etc/gshadow 文件。

3.3.4 练习 3-1: 用 vi 创建一个新用户

在这个练习中，我们通过 vi 文本编辑器编辑/etc/passwd 文件以创建一个新用户。虽然创建 Linux 新用户还有其他方法，这个练习可以用来验证使用 vi 和命令行接口的熟练程度。

(1) 打开 Linux 命令行窗口。以 root 用户登录并输入 vipw 命令。这个命令用 vi 编辑器打开 /etc/passwd 文件。

(2) 导航到文件的末尾。正如你所知道的，在命令模式下移动到文件末尾有很多办法，包括使用 DOWN ARROW 键、PAGEDOWN 键，或者 G 命令，甚至可以按 K 字符。

(3) 找到普通用户所在的一行。如果我们只想新建一个用户，这一行就是文件的最后一行，其中可能有一个 500 或更大的数。如果不存在普通用户，则找到第一行，它肯定是与 root 系统管理员有关，这一行在第 3 列和第 4 列有数字 0。

(4) 复制这一行内容。如果已经熟悉 vi 的操作，则应该知道如何用 yy 命令将整行内容复制到缓存中。这就是把整行内容“拽到”(yank)缓存中。然后用 p 命令把这一行内容粘贴到其他位置，可以粘贴任意多次。

(5) 修改用户名、用户 ID 和组 ID 以及用户全名和新用户的主目录。有关它们的详细信息请阅读第 8 章内容。例如，在下面的示例中，这些内容对应于 tweedle、501、501、Tweedle Dee 和/home/tweedle。确保用户名与主目录对应。

```
dbus:x:81:81:System message bus:/sbin/nologin
avahi-autopd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
vcsa:x:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:499:RealtimeKit:/proc:/sbin/nologin
abrt:x:498:498:/etc/abrt:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/sbin/nologin
nsLCD:x:65:55:LDAP Client User:/sbin/nologin
saslauthd:x:497:495:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89:/var/spool/postfix:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
ntp:x:38:38:/etc/ntp:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pulse:x:496:494:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72:::/sbin/nologin
oprofile:x:16:16:Special user account to be used by OProfile:/home/oprofile:/sbin/nologin
michael:x:500:500:Michael Jang:/home/michael:/bin/bash
tweedle:x:501:501:Tweedle Dee:/home/tweedle:/bin/bash
```

(6) 按下 ESC 键返回到命令模式，用:w 命令保存文件，然后用:q 退出 vi。(在 vi 中可以合并使用这两个命令。下次修改后要保存文件并且退出 vi 可以用:wq 命令)。

(7) 应该看到如下的消息：

```
You have modified /etc/passwd.
```

```
You may need to modify /etc/shadow for consistency.
Please use the command 'vipw -s' to do so.
```

该信息可能会被忽略，因为第8步会在/etc/shadow文件中添加合适的信息，但你无须直接修改/etc/shadow。

(8) 以root用户身份执行passwd newuser命令。给新用户设置一个密码。在本例中，这个新用户是tweedle。

(9) 过程还没有结束，每个用户还需要一个组。因此执行vigr命令。重复前面介绍的把某一合适的行复制到文本的末尾的步骤。注意，组名和组ID通常与用户名和用户ID相同。

(10) 只需要修改新增加一行中的组名和组ID。根据前面示例的信息，组名为tweedle，组ID为501。

(11) 重复前面提到的:wq命令保存文件并且关闭vi程序。实际上，我们会看到一个信息，表示这个文件是只读的。因此，要保存到这种“只读文件”中必须用:wq!命令，这会覆盖掉当前的设置。

(12) 注意以下信息：

```
You have modified /etc/group.
You may need to modify /etc/gshadow for consistency.
Please use the command 'vigr -s' to do so.
```

(13) 如前所述，用vigr-s命令打开/etc/gshadow文件。我们注意到这个文件的内容不多。找到合适一行进行复制，并修改组名。

(14) 重复刚才提到的:wq!命令，保存文件并关闭vi。

(15) 正确建立新用户还需要另外几个步骤。这些步骤与新用户的主目录、/etc/skel目录中的标准文件有关。详细内容请阅读第8章。

3.3.5 如果不喜欢vi

默认情况下，当我们执行edquota和crontab命令时，系统都会用vi编辑器打开相应的quota和cron作业配置文件。如果很不喜欢用vi，则用下面的命令可以改变默认编辑器：

```
# export EDITOR=/bin/nano
```

如果想改变所有用户的默认编辑器，则要把前面这一行命令添加到/etc/environment环境配置文件中。不是非得用vi编辑器修改/etc/environment文件不可，下面的命令可以把刚才提到的命令添加到/etc/environment文件的末尾。

```
# echo 'export EDITOR=/bin/nano' >> /etc/environment
```

由于nano编辑器相当直观，如图3-5所示，因此本书不提供此编辑器的用法。完整的使用手册可以从www.nano-editor.org/dist/v2.1/nano.html上下载。

如果喜欢用其他编辑器如emacs、pico或joe，也可以做类似的修改。

```

GNU nano 2.0.9          File: /etc/nsswitch.conf

# /etc/nsswitch.conf
#
# An example Name Service Switch config file. This file should be
# sorted with the most-used services at the beginning.
#
# The entry '[NOTFOUND=return]' means that the search for an
# entry should stop if the search in the previous entry turned
# up nothing. Note that if the search failed due to some other reason
# (like no NIS server responding) then the search continues with the
# next entry.
#
# Valid entries include:
#
#      nisplus           Use NIS+ (NIS version 3)
#      nis                Use NIS (NIS version 2), also called YP
#      dns                Use DNS (Domain Name Service)
#      files              Use the local files
#      db                 Use the local database (.db) files
[ Read 63 lines ]
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is ^V Next Page ^U Uncut Text ^I To Spell

```

图 3-5 用 nano 编辑器打开 /etc/nsswitch.conf 文件

3.3.6 用 GUI 工具编辑文本文件

毫无疑问, Red Hat 考试对 GUI 已经越来越友好。曾经有一段时间, RHCSA 认证目标包括了 gedit 文本编辑器。比较传统的 Linux 系统管理员可能会对此感到恐惧。(gedit 编辑器因此从 RHCSA 考试中删除)。

默认情况下系统没有安装 gedit 文本编辑器。但用 yum install gedit 命令安装 gedit 非常容易。一旦安装了 gedit 后, 单击 Applications | Accessories | gedit Text Editor 命令就可以启动它。由于它是一个直观的 GUI 文本编辑器, 因此它的用法很简单。不要纠缠于编辑器, 它们只不过是考试和实际工作的一个工具而已。

但如果要在远程系统上编辑配置文件, 我们可能无法访问远程系统上的 gedit, 特别当远程系统还没有安装 gedit 时。当然, 我们可以在任何 Red Hat 系统上安装 GUI 工具, 但是许多管理员建立的虚拟机是不带 GUI 的, 目的是为了节省空间并降低安全风险。

认证目标 3.04 本地在线文档

虽然在 RHCSA 考试期间无法访问 Internet, 但是考生可以使用 RHEL 6 系统已安装的大量在线帮助文档。这些文档从 man 页面开始, 它提供了大多数命令和大多数配置文件的选项和参数, 然后是 info 页面(相关信息页面)。很少命令和文件都有这样的帮助文档, 它们提供更详细的用法。

考试提示

Red Hat 宣称“为了评估考生使用帮助文档的能力, 允许考生在考试期间使用 Red Hat 企业版 Linux 中没有的应用程序”, 因此, 如果在/usr/share/doc 目录中可以找到与考试有关的重要信息不要感到惊奇。

许多程序包也把详尽的帮助文档保存在/usr/share/doc 目录中。可以将 ls 命令应用于这个目

录。这个目录中的每个子目录都包含了有关相应程序包功能的详细信息。当然还有其他更多的内容。

3.4.1 何时需要帮助文档

当我要了解某个命令的用法时首先要做的就是运行这个命令本身。如果此命令需要更多的信息，则它会请求用户输入，包括输入各种不同的选项。例如，仔细分析下面命令的输出信息：

```
$ yum
```

如果这种办法不起作用，则通常使用 -h 或 --help 开关选项会提供一些帮助信息。有时一个错误操作也可能提供帮助信息。下面这个命令的输出信息提示用户在 cd 命令中要使用合法的开关选项：

```
$ cd -h  
bash: cd: -h: invalid option  
cd: usage: cd [-L|-P] [dir]
```

有时-h 开关选项会提供更有用的信息，不妨分析 fdisk -h 命令的输出信息。但是-h 开关选项并不总是有效，有时--help 开关选项可能更有帮助。图 3-6 就是一个示例，它显示了 ps --help 命令的输出结果。

```

- All processes
-N negate selection
-a all w/ tty except session leaders
-d all except session leaders
-e all processes
T all processes on this terminal
a all w/ tty, including other users
g OBSOLETE -- DO NOT USE
r only running processes
x processes w/o controlling ttys
***** output format *****
-o,o user-defined -f full
-j,j job control s signal
-0,0 preloaded -o v virtual memory
-l,l long u user-oriented
-F extra full X registers
***** misc options *****
-V,V show version L list format codes f ASCII art forest
-m,m,-L,-T,H threads S children in sum y change -l format
-M,Z security data c true command name -c scheduling class
-w,w wide output n numeric WCHAN,UID -H process hierarchy
michael@Maui:$ ls bookRHCE6/Chapter3/
56503.doc Ch3Lab3 ch3.zip F03-01.tif F03-03.tif fifthedition
Backup Ch3Lab3testfile F03-01.png F03-02.tif F03-04.tif
michael@Maui:$ 

```

图 3-6 进程管理器(ps)命令的帮助信息

3.4.2 各种 man 页面

很少有人能记住每个命令的每个开关选项，这正是命令文档是如此重要的原因。大多数 Linux 命令都在称为 man 页面格式的文档中有详细的说明。当我们执行 man 这个命令时，RHEL 返回如下的信息：

What manual page do you want?

例如，假如我们想要建立一个物理卷，但却忘记了 `lvexpand` 命令的相关开关选项。为了浏览该命令的 man 文档，执行 `man lvexpand` 命令。正如其他命令一样，帮助文档中有 EXAMPLES

节, 如图 3-7 所示。如果你以前曾执行过 `lvexpand` 命令, 则这一节的内容会唤起你的记忆!

```

-r, --resizesfs
    Resize underlying filesystem together with the logical volume
    using fsadm(8).

Examples
    "lvextend -L +54 /dev/vg01/lvol10 /dev/sdk3" tries to extend the size
    of that logical volume by 54MB on physical volume /dev/sdk3. This is
    only possible if /dev/sdk3 is a member of volume group vg01 and there
    are enough free physical extents in it.

    "lvextend /dev/vg01/lvol01 /dev/sdk3" tries to extend the size of that
    logical volume by the amount of free space on physical volume
    /dev/sdk3. This is equivalent to specifying "-l +100%PVS" on the com-
    mand line.

    "lvextend -L+16M vg01/lvol01 /dev/sda:8-9 /dev/sdb:8-9"
    tries to extend a logical volume "vg01/lvol01" by 16MB using physical
    extents /dev/sda:8-9 and /dev/sdb:8-9 for allocation of extents.

SEE ALSO
    fsadm(8), lvm(8), lvcreate(8), lvconvert(8), lvreduce(8), lvresize(8),
    lvchange(8)

```

图 3-7 `lvexpand` man 页面的示例

大多数配置文件和命令都有这样的 man 页面, 而且有的还不止这些。假如我们记不得帮助文档的名字怎么办? 这时可以使用 `whatis` 和 `apropos` 命令。例如, 要找到标题中有 `nfs` 的 man 页面, 可以执行以下命令:

```
# whatis nfs
```

如果想找到描述中带有 `nfs` 的 man 页面, 则下述命令可以找到相关的命令:

```
# apropos nfs
```

但如果我们将只安装像 Samba 这样的服务(它与微软网络连接的 Linux 实现有关), 则执行 `whatis smb.conf` 和 `apropos smbpasswd` 命令可能不会得到任何信息。因为, 这些命令作用于 `/var/cache/man` 目录的数据库中。可以用 `/etc/cron.daily` 目录中的 `makewhatis.cron` 作业更新这个数据库。由于这个脚本是可执行文件, 因此下面的命令更新 man 页面的数据库:

```
# /etc/cron.daily/makewhatis.cron
```

假如考生在 Red Hat 考试中遇到这样一种情况: 帮助文档还没安装, 这可能有至少三个原因。相关的功能性程序包还没有安装。名为 man 页面的 RPM 程序包也还没有安装。有时有一个专门的程序包用于单独安装这些程序包的帮助文档。例如, 有一个名为 `system-config-users-doc` 程序包, 它包含了一个有关用户管理器(User Manager)配置工具使用的 GUI 格式的帮助文档。另外有一个 `httpd-manual` 程序包, 它是来自于 Apache Web 服务器的安装。

有时有多个帮助文档可以使用。仔细分析如下的输出信息, 它是由 `whatis wmbpasswd` 命令的执行结果:

```
smbpasswd      (5) - The Samba encrypted password file
smbpasswd      (8) - change a user's SMB password
```

数字(5)和数字(8)分别对应于 man 页面中的不同节。如果你对这些细节感兴趣, `man man` 命令可以输出这些内容。默认显示的 man 页面是命令。此时如果想要得到有关已加密的密码文件的

man 页面，需要执行下面的命令：

```
$ man 5 smbpasswd
```

按下 q 键退出帮助文档。

3.4.3 info 手册

可用的 info 手册非常有限。执行 ls/usr/share/info 命令可以列出全部的 info 文档。当一个命令的 info 手册不可用时，默认自动转到相应的 man 页面。

为了掌握更多 bash shell 的用法，执行 info bash 命令。正如图 3-8 所示，info 手册由节组成，要访问某一节，用光标移动到带星号的行并按下回车键。

退出 info 页面按下 q 键！

```
* Menu:
* Introduction::          An introduction to the shell.
* Definitions::           Some definitions used in the rest of this
                           manual.                                     §
* Basic Shell Features::  The shell "building blocks".
* Shell Built-in Commands:: Commands that are a part of the shell.
* Shell Variables::       Variables used or set by Bash.
* Bash Features::         Features found only in Bash.
* Job Control::          What job control is and how Bash allows you
                           to use it.
* Command Line Editing::  Chapter describing the command line
                           editing features.
* Using History Interactively:: Command History Expansion
* Installing Bash::        How to build and install Bash on your system.
* Reporting Bugs::         How to report bugs in Bash.
* Major Differences From The Bourne Shell:: A terse list of the differences
                                           between Bash and historical
                                           versions of /bin/sh.
* GNU Free Documentation License:: Copying and sharing this documentation.
* Indexes::                Various indexes for this manual.

--zz-Info: (bash.info.gz)Top, 44 lines --Bot-----
```

图 3-8 Info 手册示例

3.4.4 /usr/share/doc 目录中的文档细节

当我们列出/usr/share/doc 目录中的全部文档时，文档之多令人吃惊。但是，文档的质量取决于其设计者的工作。子目录包括安装程序包的名字和版本号。其中一些子目录只有一个文件，通常它以 COPYING 命名的，它包含了此软件发布的许可证。例如，大多数 system-config-* 程序包在相关的/usr/share/doc 目录中的 COPYING 文件中都有一个 GNU GPL 文件的副本。

有些文档目录包含有一些有用的示例。例如，sudo-* 子目录包含了系统管理控制用到的示例配置文件和指示符，当我们要给系统管理员配置不同的权限时，这些文件和指示符非常有用。

有时文档还包括 HTML 格式的全部文档文件。例如，看看 rsyslog-* 子目录，它包含了登录守护进程服务器的全部在线文档，这将在第 9 章和第 17 章讨论。

认证目标 3.05 网络入门

TCP/IP 是一系列按层组织的协议，也称为协议套件。它是专为 Unix 设计的，但是最终成

为 Internet 的通信标准。它利用 IP 地址组织一个网络。现在有很多 TCP/IP 工具和配置文件能帮助用户管理网络。

正如本章的 3.04 节中曾提到, 这里的论述过于简单。因此, 如果你认为这一节内容太多或不全面, 可以阅读第 1 章介绍的参考书。Linux 是专为网络连接设计的。除非比较全面地理解网络的基本概念, 否则没有切实可行的办法帮助考生通过 Red Hat 考试。

虽然当前网络的重点仍然是 IPv4 寻址模式, 但是有些组织已经开始转到 IPv6 网络。尽管, Internet 的 IPv4 地址已经用完, 但是支持 IPv6 网络路由的硬件仍然很少。希望在本书的“生存”期间这个情况会发生变化。

3.5.1 IPv4 数字与地址类

每个要在网络上进行通信的计算机必须有一个唯一的 IP 地址。有些地址已经永久地分配给某一个计算机, 这些就是静态地址。其他地址是从 DHCP 服务器那里租用一段时间的, 它们就是所谓的动态 IP 地址。

IPv4 地址分为 5 类, 如表 3-2 所示。一些学究式人物会发现这个表与 RFC1518 规定的每个 IPv4 类中的官方地址稍有不同, RFC1518 是由 Internet 工程任务组(Internet Engineering Task Force)制订的(www.ietf.org)。可分配地址段包含了可以分配给网络上一个计算机的 IP 地址。

表 3-2 IPv4 地址的分类

类	可分配地址段	说 明
A 类	1.1.1.1-126.255.255.254	一个网络最多可以连接 1 600 万台计算机
B 类	128.0.0.1-191.255.255.254	一个网络最多可以连接 65 000 台计算机
C 类	192.0.0.1-223.255.255.254	一个网络最多可以连接 254 台计算机
D 类	224.0.0.1-239.255.255.254	保留地址, 用于多播
E 类	240.0.0.1-255.255.255.254	保留地址, 用于测试

此外还有很多专用 IP 地址, 它们不可以分配给任何直接连接到 Internet 上的计算机。它们与 10.0.0.0、172.168.0.0 以及从 192.168.0.0 到 192.168.255.0 等网络地址相关联。

3.5.2 基本的 IPv6 寻址

多年前网络专家就预言 IPv4 会最终消亡。不错, Internet 上的 IPv4 地址并不够用。但借助于私有 IP 地址段, 企业级网络上的用户就不需要很多公用的 IP 地址。

尽管如此, IPv6 地址成为普遍使用的标准还需要一段时间。首先, IPv4 地址用 32 位二进制表示, 它用点分十进制表示法表示为 8 位组。而 IPv6 地址用 128 位二进制表示, 它采用 16 进制表示法。换言之, 在 IPv6 地址中可以包含以下数字:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f

一个 IPv6 地址通常分为 8 个组, 每组由 4 个十六进制数组成, 类似于 4abe:03e2:C132:69fa:0000:0000:c0b8:2148。用 ifconfig 命令可以显示本地系统的当前 IPv6 地址。

利用 128 位, IPv6 地址可以分很多类。首先介绍 IPv6 地址的三种格式。

- 单播地址(Unicast)** 单播地址对应于单个网络适配器。可路由单播地址包括一个 48 位的网络前缀、一个 16 位的子网标识符及 64 位接口标识符(与网络适配器硬件地址有关)。本地链路(link-local)单播地址还包括 10 位的前缀符、54 位的零和同样的 64 位接口标识符。本地链路单播地址是不可路由的。
- 多播地址(Multicast)** 多播地址可以用来向多个网络适配器同时发送消息。多播地址的组成各不相同。
- 任播地址(Anycast)** 任播地址用来向几个可选网络适配器的一个发送消息。它常用于系统的多备份服务，如一组 Web 服务器。任播地址的组成与单播地址相同。

由于地址格式的多样性，IPv4 格式的广播地址不能使用。IPv6 则使用多播寻址方式。IPv6 地址也分为很多不同的地址段，如表 3-3 所示。默认情况下，IPv6 地址有时也可以表示为::/128 格式。

表 3-3 IP 地址分类

地 址	说 明
::1	回环地址
::	默认地址
::ffff:0000:0000	IPv4 映射到 IPv6 的地址，最后 8 位为 0
fe80::	本地链路地址，网络之间不能路由
fec0::	站点局部地址，只用于单个网络
ff::	多播地址
2000::	全局可路由的单播地址

3.5.3 如何用 IP 地址定义一个网络

定义一个网络需要三个重要的 IP 地址：网络地址、广播地址和子网掩码。网络地址就是地址段中的第一个 IP 地址；广播地址通常是同一个地址段中的最后一个 IP 地址。子网掩码可以帮助计算机识别两个不同的地址。可以把网络地址与广播地址之间的任何一个地址(不包括上述地址)分配给网络上的任何一台计算机。

实际经验

子网掩码也称为网络掩码或网掩码。例如，IPv4 一个子网掩码是 255.255.255.0，而 IPv6 一个子网掩码是/64。

现在用一个例子说明如何为一个私有网络分配地址段。私有网络地址从 192.168.122.0 开始，C 类网络的标准子网掩码地址是 192.168.122.1。基于上述两个地址，广播地址为 192.168.122.125，则分配特定网络上的 IP 地址段可以从 192.168.122.1 到 192.168.122.254。子网掩码也可以由相应的位数来定义，本例是 24。换言之，这个网络可以表示为 192.168.122.0/24。这就是所谓的无类域内路由(Classless Inter_Domain Routing, CIDR)表示法。

IPv6 网络也有一个类似的子网掩码概念，它总是使用 CIDR 表示法表示。例如，点对点网络的网掩码为/64。它允许 64 位地址用作 48 位的硬件地址。剩下的地址可以分配给特定的网卡。

标准的 IPv6 网络有一个/48 位的网掩码。它支持 16 位子网的配置。剩余的 64 位地址仍然可用于网卡上，正如前面的点对点网络那样。

与网络和网掩码相关的是网关的概念。这是一个定义了本地网络与外部网络之间的连接的 IP 地址。虽然网关 IP 地址也是本地网络的一部分，但是它是分配给外部网络上的一个系统或一个路由器。网关 IP 地址通常是在本地系统的路由表中配置的，可以用 route 或 netstat -r 命令定义路由表。这两个命令的用法将在第 3.5.4 节中介绍。

如果对这些内容不是很明白，可以参考 www.tldp.org 上 Linux 文档计划(Linux Documentation Project)中的 IP Sub-Networking Mini-HOWTO 和 Linux IPv6 HOWTO 内容。

3.5.4 工具、命令和网关

有很多工具可用来管理 Linux 计算机上的 TCP/IP 协议套件。四个比较重要的网络管理工具是 ping、ifconfig、arp、netstat 和 route。此外还有 IPv6 专用的 ping 命令 ping6。dhclient 命令经常用来自动完成这些命令的配置操作。

但这些只是命令而已。第 3.5.5 节将分析这样一些 Red Hat 文件，它们决定了在引导过程中自动配置网络需要调用的命令。这些命令由主要的网络配置服务脚本/etc/init.d/network 控制。使用 ifup 和 ifdown 等命令也可以手工调用这些命令。

1. ping 和 ping6 命令

ping 命令可以测试网络的连通性。它可以作用于本地系统的一个网络之内，也可以测试 Internet 上多个网络之间的连通性。本节假设 IP 地址为 192.168.122.50，本地网络上的网关地址是 192.168.122.1。如果用户发现网络连接有问题，则可以按顺序执行下面的 ping 命令。第一步测试计算机的 TCP/IP 的完整性：

```
# ping 127.0.0.1
```

通常在 Linux 中会不停地执行 ping 命令，要终止它的执行必须按下 CTRL+C。如果要想验证本地局域网的连接是否正常，可以用 ping 命令测试本地网卡的地址：

```
# ping 192.168.122.50
```

如果此命令运行正常，再用 ping 命令测试网络上另一个计算机的地址。然后开始跟踪到 Internet 的路由过程。用 ping 命令测试网关的地址，这里是 192.168.122.1。如果有可能，不妨用 ping 命令测试网络连接 Internet 的地址，此地址可能在网关的另一侧。最后，用 ping 命令测试一个在 Internet 处于活动状态的计算机的 IP 地址。

也可以用 www.google.com 这样的主机名代替 IP 地址。如果用主机名时不能正常工作，则很可能是包含了主机名和 IP 地址的数据库存在问题，这个数据库也常称为域名服务(Domain Name Service, DNS)、或 Berkeley Internet 名字域(Berkeley Internet Name Domain, BIND)或者名称服务器。也可能是/etc/hosts 配置文件存在问题。

相反，ping6 命令的用法几乎与 ping 命令完全相同。在 Red Hat 系统中，例外的情况是需要指定网络适配器。例如，下面的命令通过虚拟 virbr0 网卡测试前面提到的 IPv6 网络的连通性：

```
# ping6 -I virbr0 fe80::5652:ff:fe39:24d8
```

如果已经配置了全局 IPv6 地址，而且建立了到 Internet 的路由，Google 在 ipv6.google.com 提供了一个测试 IPv6 URL。

2. 用 ifconfig 命令检查当前网络适配器

ifconfig 命令可以显示活动网卡的当前状态，它也可以用于分配网络地址及其他功能。单独运行 ifconfig 命令可以检查本地系统上当前活动网卡的状态。如果怀疑系统可能少了一个网卡，可以试试 ifconfig -a 命令，它显示所有网卡的当前配置，不管它们当前是否是活动的。

下面用 ifconfig eth0 命令显示第一个以太网卡的当前配置参数：

```
# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:50:56:40:1E:6A
          inet addr:192.168.122.50 Bcast:192.168.122.255 Mask:255.255.255.0
          inet6 addr: fe80::2e0:4cff:fee3:d106/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:11253 errors:0 dropped:0 overruns:0 frame:0
            TX packets:1304 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:2092656 (1.9 Mb) TX bytes:161329 (157.5 Kb)
```

3. 用 ifconfig 命令配置网络适配器

也可以使用 ifconfig 命令来分配 IP 地址信息。例如，下面的命令将所标注的 IP 地址和网络掩码分配给 eth0 网络适配器：

```
# ifconfig eth0 192.168.122.150 netmask 255.255.255.0
```

第一个参数 eth0 表示需要配置的网卡，下一个参数 192.168.122.150 就是分配给此网卡的 IP 地址。为了保证修改有效，需要再次执行 ifconfig eth0 命令看看当前的设置。

利用合适的选项，ifconfig 命令可以为选定的网卡修改很多其他配置。表 3-4 列出其中部分开关选项。

表 3-4 ifconfig 开关

参 数	说 明
up	启用指定网卡
down	禁用指定网卡
netmask address	分配子网掩码地址
broadcast address	把地址分配给广播地址。很少使用，因为默认的广播地址是当前大多数网络的标准
metric N	给与网络适配器相关的路由表设置度量值(metric value)
mtu N	设置最大的传输单元 N，单位为字节
-arp	禁用地址解析协议(Address Resolution Protocol, ARP)，它会收集网卡的硬件地址
promisc	启用混杂模式，它允许网卡将所有包读取到 LAN 上的所有主机。可用于分析网络中出现的问题，或者尝试解读其他用户之间的信息
-promisc	禁用混杂模式

4. 启用和禁用网络适配器

可以使用 ifconfig 命令启用和禁用网络适配器。例如，下面的命令可以禁用和再次启用第一个以太网适配器：

```
# ifconfig eth0 down
# ifconfig eth0 up
```

但是，还有几个直观的脚本是专为控制网卡而设计的：ifup 和 ifdown。与 ifconfig 命令不同的是，它们都要调用合适的配置文件和 /etc/sysconfig/network-scripts 目录中的脚本，这些脚本的具体内容是关于如何控制网卡的启用和禁用。

例如，ifup eth0 命令根据 /etc/sysconfig/network-scripts 目录中的 ifcfg-eth0 配置文件和 ifcfg-eth 脚本启用第一个以太网卡。如果已经用本章后面将要介绍的网络连接工具配置了网卡，则 /etc/sysconfig/network-scripts 目录中的文件名可能会是类似 ifcfg-System_eth0 这样的名字。

5. 网络诊断工具 arp

ARP 协议在网络适配的硬件地址和一个 IP 地址之间建立对应关系。arp 命令输出一个本地计算机的硬件和 IP 地址表。arp 命令可以检测类似网络上重复 IP 地址这样的问题。此问题可能是由于不正确的系统克隆方法而引起的。需要时，arp 命令可以用来设置或修改硬件路由表。由于硬件地址是不可路由的，因此 arp 路由表仅限于本地网络。下面是一个 arp 命令示例，它显示本地数据库中的全部 arp 记录：

```
# arp
Address      Hwtype   Hwaddress          Flags Mask    Iface
192.168.122.150    ether   52:A5:CB:54:52:A2  C        eth0
192.168.100.100    ether   00:A0:C5:E2:49:02  C        eth0
192.168.122.1     ether   00:0E:2E:6D:9E:67  C        eth0
```

如果 ARP 表为空，则表示当前系统与本地网络上其他系统没有任何连接。Address 一列表示出局域网上已知的 IP 地址。Hwtype 一列列出适配器的硬件类型，而 HWaddress 一列显示适配器的硬件地址。

6. 用 netstat -r 和 route 命令显示路由表

netstat 命令功能很多。它可以显示网络连接可用的信道(channel)、接口统计数据以及其他信息。这个命令的一个重要形式是 netstat -r，它显示路由表，通过路由表我们可以看出系统将消息发送到哪里。在功能上它等效于 route 命令。在执行这个命令时，为了以数值格式显示 IP 地址，它经常与 -n 选项一起使用。

本地系统的路由表通常包含了对本地网关地址和默认路由的访问。例如，下面是 route -n 命令的输出结果：

```
Kernel IP routing table
Destination   Gateway     Genmask       Flags Metric Ref Use Iface
192.168.122.0 0.0.0.0   255.255.255.0 U        0      0    0    eth0
0.0.0.0       192.168.122.1 0.0.0.0     UG       0      0    0    eth0
```

`netstat -nr` 命令也会输出相同的路由表。在这个路由表中，网关地址是 192.168.122.1，这是目标 IP 地址(0.0.0.0)的网关，后者是默认的 IP 地址。换言之，凡不是不发送给 192.168.122.0 网络的任何消息都发送到这个网关地址。位于网关地址的系统(通常是一个路由器)负责把这个消息转发到外部网络。

当目标系统在局域网上则不需要网关，因此在这列中有一个星号(或 0.0.0.0)。Genmask 一列列出子网掩码。网络需要搜索一个与目标 IP 地址相适应的路由。依次把 IP 地址与目标网络进行比较，如果 IP 地址属于这些网络的一个就把消息发送那个网络。如果有一个网关地址，则把消息发送这个拥有此网关地址的计算机。Flags 列说明消息的路由方式。表 3-5 说明了 Flag 各个标志的意义。

表 3-5 netstat Flag 说明路由过程

标 志	说 明
G	通过网关路由
U	Iface 一列中的网络适配器已启动
H	通过此路由只能到达一个主机
D	这一行内容是由 ICMP 重定向消息生成的
M	这一行内容是由 ICMP 重定向消息修改的

相比之下，虽然 IPv6 的路由表更加复杂，但是原理还是一样的。换言之，IPv6 的网关地址对应于默认的 IPv6 路由，用::/128 地址表示。当 `route` 和 `netstat` 命令使用-A `inet6` 选项时可用于 IPv6 路由表。

7. 用 dhclient 命令动态配置 IP 地址

尽管命令的名称经常发生变化，但是其功能还是一样的。自从人们使用动态主机配置协议(DHCP)服务器分配 IPv4 地址，客户端需要一些命令调用此服务器的服务，这个关键的命令就是 `dhclient`。当它与网卡的设备名一起使用时，它向 DHCP 服务器请求一个 IP 地址和其他功能。事实上，像下面的命令调用 DHCP 服务的很多参数：

```
# dhclient eth0
```

一般而言，由 DHCP 服务器配置的任何网络参数包括 IP 地址、子网掩码、访问外部网络的网关地址以及此网络上任何 DNS 服务器的 IP 地址都是通过 DHCP 服务器得到配置的。

换言之，`dhclient eth0` 不仅能像 `ifconfig` 命令那样分配 IP 地址，而且还会在路由表中建立默认的路由(用 `route -n` 命令可以得到路由表)。此外，它还会把 DNS 服务器的 IP 地址添加到`/etc/resolv.conf` 配置文件中。

认证目标 3.06 网络配置与故障排除

至此，我们已经介绍了 IP 寻址和相关命令的基本用法，现在该是分析相关配置文件的时候了。这些配置文件决定了在引导过程中网络连接是否启用。如果启用，这些配置文件也决定了网络地址和路由方式是按文档要求静态配置的还是通过像 `dhclient` 命令动态配置的。

基本的网络配置只能验证网络上的系统可以用它们的 IP 地址进行通信。但这还不够。如果主机名(或 FQDN)配置不能起作用，则网络配置无法判断系统是否连接到 server1.example.com 这样的系统或者像 www.mheducation.com 这样的 URL 地址，因此仅用网络配置是不够的。

实际经验

最常见的网络故障是物理问题引起的。这里假定我们已经检查了全部的网络连接。对于虚拟机，这意味着虚拟机上或物理主机上的虚拟网卡不会被意外删除。

3.6.1 网络配置文件

如果网络配置有问题，第一件事情是检查网络的当前状态。为此执行以下命令：

```
# /etc/init.d/network status
```

这个命令列出所有已经配置的和活动的设备。如果在列表中，某一个关键设备如 eth0 没有标为活动(active)，这正好解释了网络不能工作的原因。最重要配置文件开始于/etc/sysconfig/network 文件，然后是/etc/sysconfig/network-scripts 目录中的文件。

有时系统出现错误。如果禁用了一个网络适配卡或无线连接中断，一个简单的解决办法是重新启动网络连接。下面这个命令用当前配置文件重新启动网络连接：

```
# /etc/init.d/network restart
```

如果网络连接服务无法用这种简单的方法重启，则需要分析配置文件。

1. /etc/sysconfig/network 文件

当执行 ifconfig 命令时没有任何输出信息，则表示所有网络设备都处于禁用状态。在执行 ifconfig -a 命令时，输出列表中任何已配置好的网络设备没有 UP 这个标志，则这进一步确定网络处于禁用状态。这时首先要做的就是检查/etc/sysconfig/network 配置文件的内容。这是一个很简单的文件，通常这个文件包含类似以下的内容：

```
NETWORKING=yes
HOSTNAME=server1.example.com
```

如果 NETWORKING=no，则表示/etc/init.d/network 脚本没有启动任何网络设备。另一个阻止网络启动的原因可能是这个脚本文件的状态。执行 chkconfig --list network 命令，输出结果应该如下所示：

```
network          0:off    1:off    2:on     3:on     4:on     5:on     6:off
```

如果运行级 3 到 5 旁边的参数为 off，则正是这个问题。为了保证一个服务能在正确的运行级上运行，需要执行 chkconfig network on 命令。有关 chkconfig 命令的更多信息请阅读第 5 章内容。

如果在一个系统上 IPv6 是启动的，则在此文件中看到如下的指示符：

```
NETWORKING_IPV6=yes
```

在这个配置文件中，如果所有的网络设备都使用同一个 IP 地址，则其他与配置有关的指示

符还有 GATEWAY。否则此配置或者受 dhclient 命令支持，或者通过专用网络设备的 IP 地址信息(即/etc/sysconfig/network-scripts 目录中的配置文件)设置的。

考试提示

正如第 5 章将要介绍的，类似网络连接的服务可以配置为在引导过程中启动。

2. /etc/sysconfig/network-scripts/ifcfg-lo 文件

讲到/etc/sysconfig/network-scripts 目录，网络连接的基础也许是回环地址(loopback)。这个地址是在此目录的 ifcfg-lo 文件中设置的。这个文件的内容可以理解此目录中的文件应用于网络设备的方式。默认情况下，在这个文件中有以下内容，行首是回环设备的名字：

```
DEVICE=lo
```

紧接着是 IP 地址(IPADDR)、网络掩码(NETMASK)和网络 IP 地址(NETWORK)以及相应的广播地址(BROADCAST)。

```
IPADDR=127.0.0.1
NETMASK=255.0.0.0
NETWORK=127.0.0.0
BROADCAST=127.255.255.255
```

接下来的几行指定设备在引导过程是否需要启动以及设备的常用名字：

```
ONBOOT=yes
NAME=loopback
```

3. /etc/sysconfig/network-scripts/ifcfg-eth0 文件

ifcfg-eth0 文件的内容依赖于第一个以太网络适配器的配置方式。例如，分析这样一个情形：网络连接只是为系统安装而设置的。GUI 安装过程中在配置主机名时，如果没有配置网络连接，则以后不能在这个系统上配置网络连接。此时，ifcfg-eth0 文件包含以下的指示符。先是设备名，然后是硬件地址：

```
DEVICE="eth0"
HWADDR="F0:DE:F3:06:C6:DB"
```

默认情况下，RHEL 6 使用一个名为网络管理器(Network Manager)的服务。如果网卡是由这个服务控制的，则要把下面的指示符设置为 yes：

```
NM_CONTROLLED="yes"
```

网络管理器是一个服务。为了确保这个服务正在运行，执行/etc/init.d/NetworkManager start 命令。当然如果在安装过程中还没有配置网络连接，则没有理由需要在引导过程启动它。

```
ONBOOT="no"
```

也可以直接对网络管理器进行配置。为此，可以把图 3-9 的配置文件当作向导。

当然，如果想使用 DHCP 服务器，则可以省略静态网络地址信息，并且要修改如下的提示符：

BOOTPROTO=dhcp

稍后将介绍如何用网络管理器的网络连接工具来修改网络设备的配置参数。但首先从另一个角度分析图 3-10 的内容，它说明了如何配置我的 RHEL 6 手提系统中的无线网卡。

图 3-9 网络管理器不能控制静态配置

图 3-10 无线网卡的配置

4. /etc/sysconfig/network-scripts/目录中的其他文件

`/etc/sysconfig/network-scripts` 目录中的绝大多数文件实际上都是脚本。换言之，它们是由一系列文本命令组成的可执行文件。其中大多数命令的脚本都是建立在 `ifup` 和 `ifdown` 命令之上且根据网络设备类型定制的文件。假如有一条专用的路由需要配置，则配置的参数必须保存此目录中一个专用文件中，且文件要用 `route-eth0` 这样的名字。这个专用的路由需要定义一个到远程网络地址/网络掩码时的网关。下面这个示例以第 1 章介绍的系统为基础，可能包含以下指示符：

```
ADDRESS0=192.168.100.100  
NETMASK0=255.255.255.0  
GATEWAY0=192.168.122.1
```

3.6.2 网络配置工具

Red Hat 提供两个工具用于配置 RHEL 6 中的网络设备。第一个是控制端网络配置工具，它可以在命令行用 `system-config-network` 命令来启动。第二个是网络连接工具(Network Connection)，它可以在 GUI 命令行中用 `nm-connection-editor` 命令来启动。

网络管理器也包含另一个工具用于显示网络服务的当前状态。其输出结果与 ifconfig 命令的结果相似。

控制台网络配置工具

顾名思义，这个工具可以在命令行控制台中启动，只需要执行 system-config-network 命令。作为一个控制台工具，可以用 Tab 键在各个选项之间进行切换，用空格或回车键选取高亮选项。既然这个工具不是网络管理器，因此为使用此工具配置的自定义参数配置起作用，必须禁用相关的设备。练习 3-2 说明了这个过程。

按下 TAB 直到 Quit 变成高亮，再按下回车键。至此在/etc/sysconfig/network-scripts 目录中生成了 ifcfg-eth0 文件的备份。利用 diff 命令，图 3-11 比较了两个不同配置的结果。一个配置是在安装过程中的用 DHCP 协议配置的 eth0 网卡配置，另一个配置是用 system-config-network 工具采用静态 IP 地址配置的。

表 3-6 详细说明了图 3-11 中的指示符。

```
[root@Maui ~]# diff ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-eth0
1,4c1,17
< DEVICE="eth0"
< HWADDR="F0:DE:F1:06:C6:DC"
< NM_CONTROLLED="yes"
< ONBOOT="no"
...
> DEVICE=eth0
> NM_CONTROLLED=yes
> ONBOOT=no
> BOOTPROTO=none
> NETMASK=255.255.255.0
> TYPE=Ethernet
> IPV6INIT=no
> USERCTL=no
> HWADDR=f0:de:f1:06:c6:dc
> DEFROUTE=yes
> PEERROUTES=yes
> IPV4_FAILURE_FATAL=yes
> NAME="System eth0"
> UUID=5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03
> IPADDR=192.168.122.60
> GATEWAY=192.168.122.1
> DNS1=192.168.122.1
[root@Maui ~]#
```

图 3-11 静态网格配置与动态网络配置之间的差异

表 3-6 /etc/sysconfig/network-scripts 目录中的网络配置指示符

指 示 符	说 明
DEVICE	网络设备，eth0 是第一个以太网卡
HWADDR	网卡的硬件地址
NM_CONTROLLED	布尔型指示符(yes 或 no)，规定网卡是否由 NetworkManager 服务来控制
ONBOOT	布尔型指示符，规定网络设备是否在引导过程中启动
BOOTPROTO	静态配置不需要设置，如要从 DHCP 服务器获得 IP 地址，则要设置为 DHCP
NETMASK	基于静态 IP 地址配置的网络掩码
TYPE	网络类型，通常是以太网
IPV6INIT	布尔型指示符，规定是否使用 IPv6 寻址
USERCTL	布尔型指示符，规定用户控制设备
DEFROUTE	布尔型指示符，是否使用默认的路由，由 route -n 定义
PEERROUTES	布尔型指示符，是否允许使用预定义的路由
IPV4_FAILURE_FATAL	布尔型指示符，当出现错误时是否支持网络失效
NAME	以太设备的名字。如果有这些设备，则它成为 System_eth0 这样的名字
UUID	设备的统一设备标识符
IPADDR	静态 IP 地址
GATEWAY	默认网关的 IP 地址

3.6.3 练习 3-2: 配置一个网卡

本练习用基于控制台的网络配置工具配置第一个以太网卡。我们只需要一个命令行接口。至于此命令行是否在 GUI 模式中并不重要。如果还没有以 root 用户登录到系统，则系统会要求我们输入 root 管理员的口令。为了配置一个网卡，必须执行以下操作：

- (1) 备份第一个以太网卡的当前配置文件。通常这个文件是 `ifcfg-eth0`，它保存在 `/etc/sysconfig/network-scripts` 目录中。对于其他网卡，如 `eth1`，做相应的替换(提示：使用 `cp` 而不是 `mv` 命令)。
- (2) 执行 `system-config-network` 命令。
- (3) 在出现的 Select Action 菜单中，Device Configuration 应该处于高亮状态。如有必要，按 TAB 键直到它变为高亮为止。然后按回车键。
- (4) 在出现的 Select A Device 屏幕中，第一个以太网卡应该处于高亮状态。如果是，则按回车键。
- (5) 在图 3-12 中出现的 Network Configuration 窗口中，Use DHCP 选项可能已经选中。如果是，则选取它，并按空格键取消它的选取。

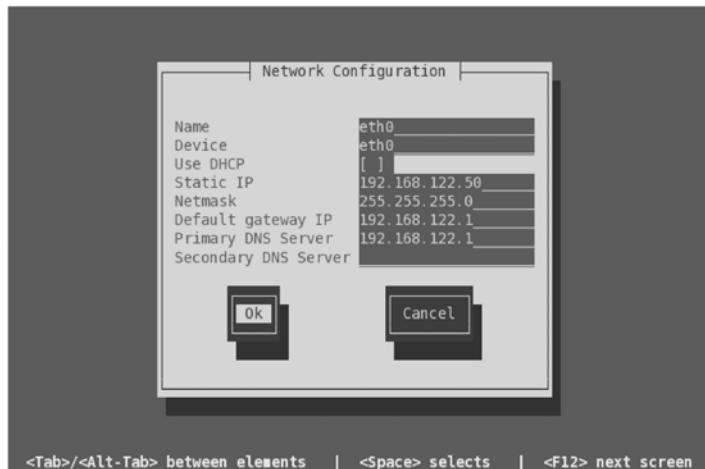


图 3-12 Network Configuration 窗口

- (6) 输入系统的 IP 地址信息。图中显示的参数是根据第 1 章为 `server1.example.com` 系统设置的参数。完成后，单击 OK 按钮，并按回车键。
- (7) 回到 Select A Device 屏幕。确保 Save 按钮已突出显示，然后按回车键。
- (8) 回到 Select Action 屏幕。确保 Save&Quit 按钮已突出显示，然后按回车键。
- (9) 用 `ifdown eth0` 命令断开第一个以太网卡，然后用 `ifup eth0` 命令重新启用它，然后用 `ifconfig eth0` 和 `route -n` 命令检查配置结果。网卡的配置参数和相应的路由表应该反映新的配置参数。
- (10) 为了恢复到原来的配置，把 `ifcfg-eth0` 文件恢复到 `/etc/sysconfig/network-scripts` 目录中，并用 `/etc/init.d/network restart` 命令重新启动网络。

网络管理器的网络连接工具

现在开始用到 RHEL 6 新推出的默认网络管理工具，即网络连接工具(Network Connections)

Tool)。由于多个网络连接上的用户很多，网络管理器需要在无线网络与以太网络连接之间实现无缝切换。但是这更适用于可移植系统，而非服务器。为此，我们需要知道如何用这个工具配置一个网卡。

实际上这并不是新内容。它被用在 Fedora Linux 测试平台上已经好几年了，只在 GUI 模式下运行。为启动它，可以执行 `nm-connection-editor` 命令或者单击 `System | Preferences | Network | Connections` 命令。它可以打开如图 3-13 所示的网络连接工具。



图 3-13 网络管理器的网络连接工具

从图 3-13 中可以看出，这个工具列出了检测到的第一个以太网卡，虽然之前这个网卡还没有使用。支持其他类型网络连接的配置的标签，如无线连接、可以连接到 3G 和 4G 网络的移动宽带网卡、虚拟专用网络(VPN)连接以及数字用户线路(Digital Subscribe Line, DSL)连接。在一个普通的服务器上，重要的是连接的可靠性，而这仍然要靠标准的有线以太设备。

选取第一个以太设备(eth0)并单击 `Edit`，这会打开如图 3-13 所示的 `Editing System` 窗口。注意在这个窗口中的以太设备名和系统的主机名。这意味着笔者是通过第 2 章介绍的 `ssh -X` 命令远程访问这个窗口的(如果是本地访问，则不会显示主机名)。

单击 `IPv4 Settings` 标签。除非以前已经配置过，否则系统认为此网卡使用 DHCP 服务器提供的配置参数。

单击 `Method` 下拉文本框。虽然它支持用几种不同的方法配置一个网卡，但在本例中我们只对手动(Manual)配置感兴趣。选择手工配置选项，则此窗口中的 `Address` 文本框里不再处于无效状态，现在输入系统的 IP 地址。根据第 1 章介绍的 `server1.example.com` 系统，相应的选项内容如下：

- **IP 地址(IP Address)** 192.168.122.50
- **网络掩码(Network Mask)** 255.255.255.0(在这个字段中，采用 CIDR 表示的 24 也是可接受的)
- **网关地址(Gateway Address)** 192.168.122.1
- **DNS 服务器(DNS Server)** 192.168.122.1
- **搜索域(Search Domains)** 不需要设置

- 此连接需要的 IPv4 寻址模式(Require Ipv4 Addressing For This Connection To Complete) 支持 IPv4 寻址
- 供所有用户使用(Available To All Users) 如果取消这个选项, 所有用户不能访问。

如果输入正确, 则第一个以太网卡配置窗口的标题与如图 3-14 中 Connection name 文本框中的内容一致。对于本例的配置, 全部配置参数保存在/etc/sysconfig/network-scripts 目录中的 ifcfg-System_`eth0` 文件中。



图 3-14 用 Network Setting 工具编辑以太网连接

3.6.4 主机名配置文件

RHEL 6 至少有 4 个主机名配置文件是比较重要的, 它们是/etc/sysconfig/network、/etc/nsswitch.conf、/etc/host 和/etc/resolv.conf。这四个文件一起提供了本地主机名、主机名和 IP 地址的数据 库、DNS 服务器的 IP 地址以及这些文件的访问顺序。

1. /etc/nsswitch.conf 文件

/etc/nsswitch.conf 文件定义了从认证到名称服务的所有内容的数据库搜索条目, 作为名称 服务器转换文件, 它包含了下面这一行内容, 该内容决定了先搜索哪个数据库。

```
hosts: files dns
```

当一个系统接收到搜索一个类似 outsider1.example.org 主机名的要求时, 上述的提示符表示 先搜索/etc/hosts 文件。如果在/etc/hosts 文件中找不到这个名字, 下一步就到可用的已配置的 DNS 服务器上搜索, 即通常到在/etc/resolv.conf 文件中配置的服务器上搜索。

一些比较早的软件组件使用/etc/host.conf 文件达到上述目的。这个文件中的记录非常简单, 因为它们支持在/etc/hosts 文件中的多记录搜索, 以及这样的搜索模式: 先搜索这个文件, 然后

搜索由 BIND(Berkeley Internet Name Domain)软件配置的 DNS 服务器。

```
multi on
order hosts,bind
```

2. /etc/hosts 文件

/etc/hosts 文件是一个静态数据库，它保存了主机名(或 FQDN 名)和它们的 IP 地址。它适用于小型的、相对静态的网络。而对于经常变化的网络，使用这个文件是一件非常痛苦的事。每次在网络中增加或移除一个系统，都要修改这个文件的内容——不仅要修改本地系统，而且要修改网络上的其他所有系统。

它非常适合于第 1 章创建的本地网络系统。一个简单的 hosts 文件可能包含类似于下面的内容：

```
192.168.122.50 server1.example.com
192.168.122.150 tester1.example.com
192.168.100.100 outsider1.example.org
127.0.0.1 localhost.localdomain localhost
::1 server1.example.com server1 localhost6.localdomain6 localhost6
```

由于增加了 IPv6 本地 IP 地址，因此简单地把这个文件复制到其他三个测试系统是不行的。但是把 server1 这样的内容改为/etc/hosts 文件中的 tester1 却并不困难。有时可能要在同一个 IP 地址上创建多个条目。例如，可以添加以下记录以指定 Web 服务器和 FTP 服务的 IP 地址。

```
192.168.122.50 www.example.com
192.168.122.150 ftp.example.com
```

3. /etc/resolv.conf 文件

记录 DNS 服务器位置的标准文件仍然还是/etc/resolv.conf 文件。

通常情况下它将包含一到两个记录，如下所示：

```
search example.com
nameserver 192.168.122.1
```

在 search 提示符后附带 example.com 域名后用于搜索简单的主机名。文件中的 nameserver 指示符定义了已配置的 DNS 服务器的 IP 地址。如果无法确定此 DNS 服务器是否可运行，则执行下面的命令：

```
# dig @192.168.122.1 mheducation.com
```

如有必要，替换/etc/resolv.conf 文件中 nameserver 指示符的 IP 地址。

3.6.5 主机名配置选项

在引导过程中，网络服务根据/etc/sysconfig/network 文件的内容确定本地主机名的值。如果此主机名已经设置为类似 tester1.example.com 这样的一个 FQDN 名字，则一切都没有问题。如前所述，这是一个简单的文件，其中主机名可能表示为如下形式的一个指示符：

```
HOSTNAME=tester1.example.com
```

当然,我们可以用 `hostname newname` 修改主机名的值。但这样的修改无法在`/etc/hosts`文件中或任何 DNS 服务器上反映出来,因此这样的修改没有多大用处。

3.6.6 网络管理器小程序

网络管理器也有一个小程序,它可以帮助用户管理已配置的网络连接。例如,在笔者的个人计算机中已配置了一个以太连接和一个无线连接。当左击此网络小程序时,它会显示可用的活动连接,如图 3-14 所示。注意有线网络和无线网络上所有可用的连接,可以根据需要选择不同的连接。此小程序的实际图标根据当前连接是否是活动的而有变化。这个小程序出现在 GNOME 桌面环境的右上角,顶层面板上接近日期和时间图标的位置。(为了保护笔者邻居的隐私,显示在图 3-15 中无线网络的名字已经部分被淡化)。

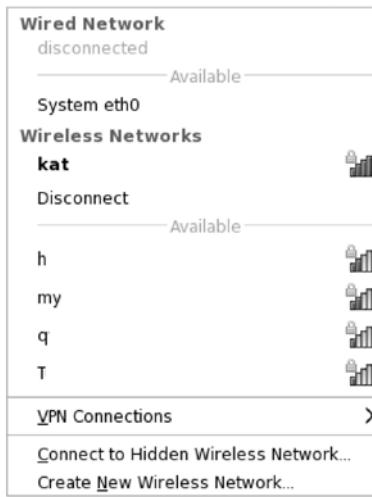


图 3-15 网络管理器小程序的一个菜单

当我们右击网络管理器(Network Manager)小程序时,它会打开一个菜单,里面有许多配置选项。这些选项可顾名思义,而且也不重要。

故障现象及解决方案	
网络连接中断	检查物理连接。执行 <code>ifconfig</code> 检查活动的连接。执行 <code>/etc/init.d/network status</code> 命令。查看 <code>/etc/sysconfig/network</code> 文件中的内容
无法访问远程系统	用 <code>ping</code> 命令测试对本地 IP 地址和远程 IP 地址的访问
当前网络参数发生冲突	检查 <code>/etc/sysconfig/network-scripts</code> 文件中的网络设备配置。使用网络连接工具查看设置
网络参数不一致	检查 <code>/etc/sysconfig/network-scripts</code> 文件中的网络设备配置参数,使用网络连接工具检查设置参数。这种现象说明了有静态网络配置的意图,做相应检查
主机名不能识别	检查 <code>/etc/sysconfig/network</code> 文件中的内容。执行 <code>hostname</code> 命令,检查 <code>/etc/hosts</code> 文件的一致性
远程主机名不能识别	检查 <code>/etc/hosts</code> 文件的内容,为合适的 DNS 服务器 IP 地址检查 <code>/etc/resolv.conf</code> 文件。运行 <code>dig</code> 命令以测试 DNS 服务器

3.7 认证小结

本章主要讨论两方面的内容。首先介绍以前参加 Red Hat 考试的先决条件，即基本命令行工具的使用。由于这些工具已成为 RHCSA 考试的主要内容，它们与网络配置相结合用于练习使用这些命令行工具。

命令行在 shell 环境中启动，shell 是一个命令解释器，它允许用户通过各个命令与操作系统进行交互。虽然在考试目标中没有明确指定哪个 shell，但是在大多数 Linux 发行版包括 RHEL 6 中都默认使用 bash。我们可以在默认的控制台之一或 GUI 的一个终端启动一个命令行窗口。在 bash 提示窗口中，可以通过 Linux 系统管理和配置的手段来管理文件和目录。由于大部分 Linux 文件都采用文本格式，因此它们可以创建为数据库，可以用许多命令对这些数据库进行搜索和修改。Linux 文本文件可以被当作数据流来解释和处理。为编辑一个文本文件，需要像 vim 和 gedit 这样文本编辑器。

Linux 的在线文档范围很广。只要在命令后面加上 -h 和 --help 开关选项，就可以提供此命令的用法。其次是 man 和 info 帮助文档。许多程序包都提供了很多帮助文档，这些文件都保存在 /usr/share/info 目录中。在绝大多数情况下，不需要访问 Internet 就可以找到所需要的帮助信息。

Linux 本身就是一个网络操作系统。像 eth0 这样的网络设备可以配置为 IPv4 和 IPv6 地址。网络检查和配置命令包括 ifconfig、ifup、ifdown 和 dhclient。其他有关的命令包括 arp、route、netstat 和 ping。相关的配置文件都由 /etc/sysconfig/network 启动，单个设备都在 /etc/sysconfig/network-scripts 目录中配置。网络设备既可以用 system-config-network 命令在控制台上进行配置，也可以用网络管理程序的网络连接工具进行配置。

3.8 小练习

以下是本章与认证目标有关的几个重要知识点。

shells

- Linux 默认的 shell 是 bash。
- 默认时最多有 6 个命令行控制台可供使用。如果系统已安装了 GUI，则它是第一个命令行控制台。
- 在 GUI 中可以打开多个命令行终端。
- shell 中可以使用 3 类数据流：stdin、stdout 和 stderr。因此在命令中可以用 >、>>、<、| 和 2> 等重定向符改变数据流的流向。

标准的命令行工具

- Linux 中任何内容最终都可以表示为文件。
- pwd 和 cd 等命令可用于切换目录。
- 目录路径、PATH 和波浪符(~)等概念可帮助用户理解和使用 shell 中的命令。
- ls、find 和 locate 等基本命令可以帮助用户找到文件和查看文件内容。

- touch、cp、ln、mv 和 rm 等是文件创建命令(或删除命令), 对应的目录创建和删除命令是 mkdir 和 rmdir。
- 用 alias 命令可以为用户定制命令。

文本文件的管理

- Linux 是通过一系列的文本配置文件来管理的。
- cat、less、more、head 和 tail 等命令可以将文本文件当作数据流来读取。
- 用 touch、cp、mv 和 rm 等命令可以创建、复制、移动和删除文件。用 ln 可以创建链接文件。用 alias 命令可以定制命令。
- sort、grep、egrep、wc、sed 和 awk 等命令属于文件过滤器, 它们支持文本流的处理。
- 掌握文本编辑器的使用是一项重要的技能。RHCSA 目标的早期版本要求掌握 vim 和 gedit 两个编辑器。

本地在线文档

- 如果需要获得一个命令的帮助, 则执行这个命令本身, 或者在命令中加上-h 或—help 开关。
- 命令的 man 帮助文档通常包含了使用示例。whatis 和 apropos 命令可以搜索不同主题的 man 帮助文档。
- 如果一个命令或文件有 info 帮助文档, 则肯定会在/usr/share/info 目录中找到。
- 许多程序包都提供了大量的帮助文档和示例, 它们都在/usr/share/doc 目录中。

网络入门

- IPv4 是 32 位地址。一共有 5 类 IPv4 地址和 3 类不同的专用 IPv4 地址集, 后者用于在 LAN 上设置 TCP/IP。
- IPv6 是 128 位地址。它分为单播地址、多播地址和任播地址。单播地址只限本地网络, 而且是可路由的。
- ping、ping6、arp、ifconfig 和 netstat 等工具可以用来诊断 LAN 上的故障。
- /etc/resolv.conf 等域名解析配置文件决定了一个系统如何找到正确的 IP 地址。使用 dhclient 命令可以从 DHCP 服务器配置该文件。

网络配置与故障排除

- Linux 网络连接从/etc/init.d/network 脚本和/etc/sysconfig/network 配置文件启动。
- 单个网络设备在/etc/sysconfig/network-scripts 目录中配置。
- 网络配置工具包括基于控制台的 system-config-network 命令和网络管理器的网络连接工具。
- 主机名配置文件包括/etc/nsswitch.conf、/etc/hosts 和/etc/resolv.conf 文件。

3.9 自测题

下面的练习题用于测验对本章内容的掌握程度。由于 Red Hat 考试没有多选题，因此本书不提供任何选择题。这些题目专门用来测试读者对本章的理解。Red Hat 考试注重于得到结果的过程，而不是死记一些无关紧要的内容。许多问题可能不止一个答案。

shell

- 说出 Linux 默认 shell 的名字。
-

- 在 GUI 中，用哪个组合键可以切换到虚拟控制台 3？
-

标准命令行工具

- 哪个命令可以创建/abc/def/ghi/jkl 目录串？
-

- 哪个符号代表当前用户的主目录？
-

文本文件的管理

- 哪个命令可以列出/var/log/messages 文件最后 10 行的内容？
-

- 哪个命令可以返回/var/log/dmesg 文件中包含 Linux 这个词的行？
-

本地在线文档

- 哪个命令搜索在 man 文档数据库中引用 passwd 命令和配置文件的文档？
-

- 假设已在第 5 节和第 8 节已为虚拟的 abcde 命令和文件建立了 man 帮助文档，输入哪个命令，它一定会显示第 5 节的 man 帮助文档？

网络入门

- 在 IPv4 寻址中，假设网络的地址为 192.168.100.0，且广播地址为 192.168.100.255，写出可分配的 IP 地址段。
-

10. 假设已给定第 9 题中的地址, 用哪个命令可以把 192.168.100.100 的 IPv4 地址分配给网络设备 eth0?
-

网络配置与故障排除

11. 写出与本地系统主机名有关配置文件的完整路径。
-

12. 写出本地系统上的第一个以太网适配器有关的配置文件的完整路径。
-

3.10 实验题

这几个实验题都是配置练习。读者只能在测试系统上做这些实验题。这里假设是在 KVM 之类的虚拟机上执行这些操作。

Red Hat 考试采用电子形式。因此在本章及后面几章中, 大多数实验题都可以从本书配书光盘上读取, 本章的实验题保存在 Chapter3/子目录中。假如现在仍然还没有在自己的系统中安装一个 RHEL 6, 则参考本书第 1 章的安装指示安装一个系统。

实验题的答案就在自测题答案之后。

3.11 自测题答案

shell

1. Linux 默认的 shell 是 bash, 也称为 Bourne-Again shell。
2. 在 GUI 环境下, 用 CTRL+ALT+F3 组合键可以切换到虚拟控制台 3。

标准的命令行工具

3. 创建/abd/def/ghi/jkl 目录串的单个命令是 mkdir -p /abc/def/ghi/jkl。
4. 表示当前用户的主目录的符号是波浪符(~)。

文本文件的管理

5. 列出/var/log/messages 文件最后 10 行内容的命令是 tail -n10 /var/log/messages。
6. 返回/var/log/dmesg 文件中包含 Linux 这个词的命令是 grep Linux /var/log/dmesg。也可以使用 cat /var/log/dmesg | grep Linux。

本地在线文档

7. 在 man 文档数据库中, 搜索引用 passwd 命令和配置文件文档的命令是 whatis passwd。apropos 和 man -k 命令则更进一步, 它们列出在命令和说明中有 passwd 一词的 man 帮助文档。

8. 调用第5节的帮助文档中虚拟 abcde 命令和文件的 man 帮助文档的命令是 man 5 abcde。

网络入门

9. 在提到的 IPv4 网络中可分配的 IP 地址段是从 192.168.100.1 到 192.168.100.254。

10. 假设已给定第9题中的地址，把 192.168.100.100 的 IPv4 地址分配给网络设备 eth0 的命令是 ifconfig eth0 192.168.100.100。

网络配置与故障排除

11. 本地系统主机名的配置文件的完整路径是/etc/hosts。

12. 本地系统上第一个以太网适配器的配置文件的完整路径是/etc/sysconfig/network-scripts/ifcfg-eth0。如果以前总是用网络连接工具配置网卡，则 ifcfg-System-eth0 也是可接受的。

3.12 实验题答案

实验题 1

此实验题测试这样一种情形：网络连接由于/etc/sysconfig/network 文件中 NETWORKING 指示符的设置而中断。如果这个指示符设置为 no，系统就会中断网络连接。其他参数都没有变化，特定网卡的 IP 地址信息仍然正确。当然也可以用其他方法启动网络连接，但是除非在此配置文件中设置 NETWORKING=yes，否则重新启动后系统还是存在原来的问题(即网络无法连接)。

本实验题中使用的脚本把/etc/sysconfig/network 目录中原来的副本备份到/root/backup 目录中。现在当这个实验题完成后，可以把这个文件恢复到原来的目录中。要注意，不可修改标志已应用于这个备份文件上，如果要把它从/root/backup 目录中删除，首先要用 chattr -i 命令去掉这个不可修改标志位。

实验题 2

本实验题给第一个以太网卡即 eth0 设置了一个无效的 IP 地址。第1章配置的标准是建立在 192.168.122.0/24 网络上。/etc/sysconfig/network-scripts 目录的配置文件可能会使用一个稍微不同的名字，这取决于适配器的配置方式。把目录中原来的配置文件移动到/root/backup 目录中。如果重新建立配置文件的努力失败了，则可以从/root/backup 目录恢复原来的配置文件。

要注意，不可修改标志已应用于这个备份文件上，如果要把它从/root/backup 目录中删除，首先要用 chattr -i 命令去掉这个不可修改标志位。

```
# chattr -i /root/backup/*
```

实验题 3

本实验题中断了系统的第一个以太网络设备。当此设备使用默认的设备文件名即 eth0 时，它就能运行。如果已经运行了网络管理器的网络连接工具且对默认的参数值没有做太多的修改，则它也能工作，因为 Ch3Lab3 脚本也可以中断 System_eth0 设备文件。

实验题 4

本实验题要替换/etc/resolv.conf 文件。假如本地网络已经使用位于 192.168.1.111 IP 地址的一个 DNS 服务器，则本实验题不会产生任何问题。把这个文件的初始版本移动到/root/backup 目录中。如果重新建立配置文件的努力失败了，则可以从/root/backup 目录恢复原来的配置文件。

实验题 5

在本实验题中，考生要在第 1 章建立的每个系统上创建/etc/hosts 文件。除了由网络管理器添加的本地系统参数外，在其他三个系统上的/etc/hosts 文件中的内容都一样。具体来说，这个文件应该包含以下内容：

```
192.168.122.50 server1 server1.example.com  
192.168.122.150 tester1 tester1.example.com  
192.168.100.100 outsider1 outsider1.example.org
```

这些系统是否在不同的 IP 网络上并不重要。只要系统之间有路由的路径，则每个/etc/hosts 文件中的数据就能起作用。网络管理器可能会插入重复的数据，但是这不会带来问题，条件是数据必须一致！事实上，可以为一个 IP 地址设置多个名字。例如笔者在 192.168.122.60 系统上建立了一个 Web 服务器，则可以在/etc/hosts 文件中添加以下记录：

```
192.168.122.50 www.example.com
```

实验题 6

前 4 行内容来自 eth0 网卡的原始配置文件。虽然 DEVICE、HWADDR、NM_CONTROLLED 和 ONBOOT 这 4 个指示符的值并没有改变，但是 RHEL 6 安装程序提供的格式却不一样。

实验题 7

如果考生曾使用过网络连接工具，则会看到有一个 ifcfg-System-eth0 文件取代了 ifcfg-eth0 文件。`system-config-network` 工具可以处理这个文件。只要做相应的替换即可。必须掌握与 USERCTRL、BOOTPROTO 和 DNS1 等指示符相关的参数设置。