

SUSE Linux Enterprise Desktop

10 SP2

www.novell.com

2008 4 10

部署指南



部署指南

所有内容的版权都属于 © Novell, Inc.

法律声明

本手册受 Novell 知识产权的保护。复制、复印或分发本手册，表示您明确同意遵守本许可协议的条款。

本手册可如上或作为捆绑软件包的一部分免费复制、复印或分发（电子和/或打印格式），前提是满足以下条件：

本版权声明及作者和贡献者姓名清晰明确地出现在复制、复印和分发的所有副本上。复制和/或分发本手册（尤其是打印格式）仅限于非商业用途。将本手册或其一部分用于任何其他用途，都必须事先获得 Novell, Inc 的明确授权。

有关 Novell 商标的列表，请参见 Novell 商标和服务标记列表 (<http://www.novell.com/company/legal/trademarks/tmlist.html>) [<http://www.novell.com/company/legal/trademarks/tmlist.html>]。* Linux 是 Linus Torvalds 的注册商标。所有第三方商标均属其各自所有者的财产。商标符号（®、™ 等）代表 Novell 商标；星号 (*) 代表第三方商标。

本指南力求涵盖所有细节。但这并不确保本指南准确无误。无论是 Novell, Inc.、SUSE LINUX 产品 GmbH、作者还是翻译人员都不对任何可能的错误或因错误造成的任何后果负责。

目录

关于本指南	xiii
部分 I 部署	1
1 SUSE Linux Enterprise Desktop 的计划	3
1.1 硬件要求	4
1.2 使用 SUSE Linux Enterprise Desktop 的原因	4
2 部署策略	7
2.1 最多部署 10 个工作站	7
2.2 最多部署 100 个工作站	9
2.3 部署 100 多个工作站	16
3 使用 YaST 进行安装	17
3.1 系统启动以进行安装	17
3.2 安装工作流程	19
3.3 引导屏幕	19
3.4 语言	22
3.5 媒体检查	22
3.6 许可证协议	23
3.7 安装方式	23
3.8 时钟和时区	24
3.9 安装设置	24
3.10 执行安装	29
3.11 已安装系统的配置	30
3.12 图形登录	36

4	远程安装	37
4.1	远程安装的安装方案	37
4.2	设置存放安装源的服务器	45
4.3	准备目标系统的引导	53
4.4	引导用于安装的目标系统	63
4.5	监视安装过程	67
5	自动安装	71
5.1	简单的大规模安装	71
5.2	基于规则的自动安装	81
5.3	有关详细信息	86
6	部署自定义预安装	87
6.1	准备主计算机	88
6.2	自定义 Firstboot 安装	88
6.3	复制主安装	96
6.4	个性化安装	96
7	高级磁盘设置	97
7.1	LVM 配置	97
7.2	软 RAID 配置	103
8	使用 YaST 进行系统配置	109
8.1	YaST 语言	110
8.2	YaST 控制中心	110
8.3	软件	111
8.4	硬件	124
8.5	系统	131
8.6	网络设备	140
8.7	网络服务	141
8.8	AppArmor	144
8.9	安全性和用户	145
8.10	虚拟化	153
8.11	杂项	153
8.12	文本方式的 YaST	156
8.13	通过命令行管理 YaST	159
8.14	从命令行使用 rug 更新包	161
8.15	SaX2	164
8.16	故障诊断	170
8.17	更多信息	170

9 更新 SUSE Linux Enterprise	171
9.1 更新 SUSE Linux Enterprise	171
9.2 安装服务包	173
9.3 从 V9 到 V10 的软件更改	183
 部分 II 管理	 195
 10 GNOME 配置（供管理员使用）	 197
10.1 默认情况下使用 GConf	198
10.2 自定义菜单	220
10.3 安装主题	231
10.4 配置字体	237
10.5 MIME 类型	238
10.6 设置屏幕保护程序	240
10.7 会话管理	241
10.8 提升性能	242
10.9 隐藏目录	249
10.10 配置 SMB 打印机的安全性说明	251
10.11 禁用 GNOME Desktop 功能	252
10.12 自动启动应用程序	254
10.13 自动装入和管理媒体设备	255
10.14 更改首选应用程序	255
10.15 用 Sabayon 管理配置文件	255
10.16 添加文档模板	259
 11 KDE 配置（供管理员使用）	 261
11.1 使用“KIOSK 管理工具”管理配置文件	261
11.2 手动管理配置文件	269
 12 Active Directory 支持	 275
12.1 集成 Linux 和 AD 环境	275
12.2 有关 Linux AD 支持的背景信息	276
12.3 为 Active Directory 配置 Linux 客户机	281
12.4 登录到 AD 域	283
12.5 更改密码	285
 13 Linux 中的访问控制列表	 287
13.1 传统文件权限	287
13.2 ACL 的优势	288
13.3 定义	289

13.4	处理 ACL	290
13.5	应用程序中的 ACL 支持	297
13.6	更多信息	297
14	系统监视实用程序	299
14.1	调试	299
14.2	文件和文件系统	301
14.3	硬件信息	304
14.4	联网	306
14.5	/proc文件系统	307
14.6	进程	310
14.7	系统信息	314
14.8	用户信息	318
14.9	时间和日期	318
15	使用 Shell	319
15.1	Bash shell 入门	319
15.2	用户和访问权限	330
15.3	重要的 Linux 命令	333
15.4	vi 编辑器	343
部分 III	系统	347
16	64 位系统环境中的 32 位和 64 位应用程序	349
16.1	运行时支持	349
16.2	软件开发	350
16.3	Biarch 平台上的软件编译	350
16.4	内核规范	351
17	引导和配置 Linux 系统	353
17.1	Linux 引导进程	353
17.2	init 进程	356
17.3	通过 /etc/sysconfig 配置系统	364
18	引导加载程序	367
18.1	选择引导加载程序	368
18.2	通过 GRUB 引导	368
18.3	使用 YaST 配置引导加载程序	376
18.4	卸载 Linux 引导加载程序	381

18.5	创建引导 CD	381
18.6	图形 SUSE 屏幕	382
18.7	查错	383
18.8	有关详细信息	384
19	特别的系统功能组件	385
19.1	特殊软件包的相关信息	385
19.2	虚拟控制台	392
19.3	键盘映射	392
19.4	语言和国家/地区特定的设置	393
20	打印机操作	397
20.1	打印系统工作流程	398
20.2	连接打印机的方法和协议	399
20.3	安装软件	399
20.4	设置打印机	400
20.5	网络打印机	404
20.6	图形打印接口	406
20.7	从命令行打印	407
20.8	SUSE Linux Enterprise 中的特殊功能	407
20.9	查错	410
21	使用 udev 进行动态内核设备管理	419
21.1	/dev 目录	419
21.2	内核 uevents 和 udev	420
21.3	驱动程序、内核模块和设备	420
21.4	引导和启动设备设置	421
21.5	调试 udev 事件	421
21.6	使用 udev 规则影响内核设备事件处理	422
21.7	永久设备命名	423
21.8	已替换的 hotplug 包	423
21.9	有关详细信息	424
22	Linux 中的文件系统	427
22.1	术语	427
22.2	Linux 中的主要文件系统	428
22.3	其他一些支持的文件系统	432
22.4	Linux 中对大型文件的支持	433
22.5	有关详细信息	434

23	X 窗口系统	437
23.1	手动配置 X Window 系统	437
23.2	安装和配置字体	443
23.3	更多信息	448
24	通过 PAM 进行鉴定	449
24.1	PAM 配置文件的结构	449
24.2	sshd 的 PAM 配置	451
24.3	PAM 模块的配置	453
24.4	有关详细信息	455
25	Linux 中的移动计算	457
25.1	便携式计算机	457
25.2	移动硬件	464
25.3	手提电话和 PDA	465
25.4	更多信息	465
26	PCMCIA	467
26.1	用 pccardctl 控制 PCMCIA 卡	468
26.2	PCMCIA 详述	468
26.3	故障诊断	471
27	系统配置配置文件管理	475
27.1	术语	476
27.2	设置 SCPM	477
27.3	使用图形用户界面配置 SCPM	478
27.4	使用命令行配置 SCPM	483
27.5	故障诊断	486
27.6	更多信息	487
28	电源管理	489
28.1	省电功能	489
28.2	APM	490
28.3	ACPI	492
28.4	硬盘的休眠	498
28.5	powersave 包	499
28.6	YaST 电源管理模块	507

29 无线通讯	513
29.1 无线 LAN	513
29.2 蓝牙	522
29.3 红外线数据传送	532
29.4 管理 UMTS/3G 网络连接	535
 部分 IV 服务	 539
30 基本联网知识	541
30.1 IP 地址和路由	544
30.2 IPv6 下一代的因特网	546
30.3 名称解析	553
30.4 使用 YaST 配置网络连接	555
30.5 使用 NetworkManager 管理网络连接	569
30.6 手动配置网络连接	571
30.7 作为拨号助手的 smpppd	585
 31 网络中的 SLP 服务	 587
31.1 激活 SLP	587
31.2 SUSE Linux Enterprise 中的 SLP 前端	588
31.3 用 SLP 提供服务	588
31.4 有关详细信息	589
 32 使用 NTP 同步时间	 591
32.1 使用 YaST 配置 NTP 客户机	591
32.2 在网络中配置 xntp	594
32.3 设置本地参考时钟	595
 33 使用 NIS	 597
33.1 配置 NIS 客户机	597
 34 配置 eDirectory 鉴定	 599
34.1 设置工作站使用 eDirectory 鉴定	600
34.2 用 iManager 为 eDirectory 鉴定启用用户	603
34.3 关闭 LUM 和 eDirectory 鉴定	605
 35 LDAP - 目录服务	 607
35.1 对比 LDAP 和 NIS	608

35.2	LDAP 目录树的结构	609
35.3	使用 YaST 配置 LDAP 客户机	612
35.4	在 YaST 中配置 LDAP 用户和组	619
35.5	浏览 LDAP 目录树	620
35.6	有关详细信息	622
36	Samba	625
36.1	术语	625
36.2	启动和停止 Samba	626
36.3	配置 Samba 服务器	627
36.4	配置客户机	632
36.5	将 Samba 用作登录服务器	633
36.6	有关详细信息	634
37	通过 NFS 共享文件系统	635
37.1	安装所需软件	635
37.2	使用 YaST 导入文件系统	635
37.3	手动导入文件系统	636
37.4	使用 YaST 导出文件系统	638
37.5	手动导出文件系统	643
37.6	采用 Kerberos 的 NFS	646
37.7	更多信息	646
38	文件同步	647
38.1	可用的数据同步软件	647
38.2	选择程序时的决定性因素	648
38.3	CVS 简介	651
38.4	rsync 简介	654
部分 V	安全性	657
39	伪装和防火墙	659
39.1	使用 iptables 过滤包	659
39.2	关于伪装的基础知识	661
39.3	防火墙基础知识	662
39.4	SUSEfirewall2	663
39.5	有关详细信息	667

40 SSH: 安全性网络操作	669
40.1 OpenSSH 软件包	669
40.2 ssh 程序	670
40.3 scp — 安全复制	670
40.4 sftp — 安全的文件传送	671
40.5 SSH 守护程序 (sshd) — 服务器端	671
40.6 SSH 鉴定机制	672
40.7 X、鉴定和转发机制	673
 41 网络鉴定 — Kerberos	 675
41.1 Kerberos 术语	675
41.2 Kerberos 的工作原理	677
41.3 从用户的角度讨论 Kerberos	680
41.4 有关详细信息	680
 42 对分区和文件进行加密	 683
42.1 用 YaST 设置已加密的文件系统	684
42.2 使用加密的用户主目录	686
42.3 使用 vi 加密单个 ASCII 文本文件	687
 43 通过 AppArmor 限制特权	 689
43.1 安装 Novell AppArmor	690
43.2 启用和禁用 Novell AppArmor	690
43.3 构建应用程序的配置文件入门	691
 44 安全性和机密性	 699
44.1 本地安全和网络安全	700
44.2 一些常用的安全提示和技巧	707
44.3 使用中央安全报告地址	709
 部分 VI 查错	 711
 45 帮助和文档	 713
45.1 使用 SUSE 帮助中心	713
45.2 手册页	717
45.3 信息页	718
45.4 Linux 文档计划	718
45.5 Wikipedia: 免费的联机百科全书	718
45.6 指南和手册	719

45.7	包文档	719
45.8	Usenet	720
45.9	标准和规范	721

46 常见问题及其解决方案 723

46.1	查找和收集信息	723
46.2	安装问题	725
46.3	引导问题	733
46.4	登录问题	736
46.5	网络问题	741
46.6	数据问题	745

关于本指南

本指南设计为由专业网络和系统管理员在实际计划、部署、配置及操作 SUSE Linux Enterprise® 的过程中使用。同样，本指南旨在确保 SUSE Linux Enterprise 正确配置并且网络上的必需服务可用，使其在初始安装时正常运行。本指南不包含用于确保 SUSE Linux Enterprise 与用户企业的应用程序软件兼容或者其核心功能符合那些要求的过程。它假定已经进行了对完全要求的审计、已经请求安装或者已经请求用于此类审计的测试安装。

本指南包含如下内容：

部署

安装 SUSE Linux Enterprise 之前，选择最适合您的环境的部署策略和磁盘设置。了解如何手动安装系统，如何使用网络安装设置以及如何执行自动安装。配置用 YaST 安装的系统，使其适应您的要求。

管理

SUSE Linux Enterprise 提供了大量工具，用于自定义系统的各个方面。本部分介绍其中几个。

系统

通过研究本部分了解关于底层操作系统的更多信息。SUSE Linux Enterprise 支持许多硬件架构，您可以利用这点调试自己的应用程序，使之在 SUSE Linux Enterprise 上运行。引导加载程序和引导过程信息有助于您了解 Linux 系统的工作方式以及您自己的自定义脚本和应用程序与该系统的调和方式。

服务

SUSE Linux Enterprise 被设计为一个网络操作系统。SUSE® Linux Enterprise Desktop 包含对许多网络服务的客户端支持。它可以很好地集成到包括 MS Windows 客户机和服务器在内的异构环境中。

安全性

该版本的 SUSE Linux Enterprise 包括几个与安全性相关的功能。它附带 Novell® AppArmor，使您可以通过限制权限保护应用程序。也包括安全登录、防火墙及文件系统加密。

查错

SUSE Linux Enterprise 包括众多应用程序、工具和文档，便于您在遇到问题时使用。详细讨论了在 SUSE Linux Enterprise 中可能发生的最常见问题及其解决方法。

1 反馈

我们希望听到您对本手册和本产品中包含的其他文档的意见和建议。请使用每页联机文档底部的用户意见功能并发表您的意见。

2 文档更新

有关该文档的最新版本，请参阅 SUSE Linux Enterprise Desktop 万维网站点 [<http://www.novell.com/documentation/sled10/index.html>]。

3 其他文档

有关本产品的附加文档，请参阅 <http://www.novell.com/documentation/sled10/index.html>：

GNOME 用户指南

GNOME 桌面及其最重要的应用程序的综合指南。

KDE 用户指南

KDE 桌面及其最重要的应用程序的综合指南。

Novell AppArmor Administration Guide

Novell AppArmor 的详细管理指南，介绍用于提供环境中安全性的应用程序限制。

有关 SUSE® Linux Enterprise Server 产品的文档概述，请参阅 <http://www.novell.com/documentation/sles10/index.html>。以下手册仅用于 SUSE Linux Enterprise Server：

入门指南

有关安装类型和工作流程的基本信息。

Architecture-Specific Information

准备 SUSE Linux Enterprise Server 安装目标所需要的特定于架构的信息。

Installation and Administration

SUSE Linux Enterprise Server 安装与管理的详细信息。

Novell AppArmor Administration Guide

Novell AppArmor 的详细管理指南，介绍用于提供环境中安全性的应用程序限制。

Storage Administration Guide

管理 SUSE Linux Enterprise 上的不同类型存储设备的介绍。

Heartbeat Guide

用 Heartbeat 设置高可用性场景的深入管理指南。

Novell Virtualization Technology User Guide

基于 SUSE Linux Enterprise 和 Xen* 虚拟技术的虚拟解决方案介绍。

本手册中的许多章节包含到附加文档资源的链接。这包括系统上提供的附加文档以及因特网上提供的文档。

4 文档约定

以下是本手册中使用的版式约定：

- `/etc/passwd`：文件名和目录名
- `placeholder`：将 `placeholder` 替换为实际值
- `PATH`：环境变量 `PATH`
- `ls`、`--help`：命令、选项和参数
- 用户：用户和组
- `Alt`、`Alt + F1`：按键或组合键；这些键以大写形式显示，如在键盘上一样
- 文件，文件 > 另存为：菜单项，按钮

- *跳舞的企鹅*（*企鹅*一章，↑其他手册）：这是对其他手册中的章节的引用。

部分 I. 部署

SUSE Linux Enterprise Desktop 的计划

1

本章将主要用于面临必须在其站点部署 SUSE® Linux Enterprise Desktop 的任务的公司系统管理员。将 SUSE Linux Enterprise Desktop 部署到整个站点必须要仔细计划并考虑以下问题：

使用 SUSE Linux Enterprise Desktop 工作站是为了什么？

确定 SUSE Linux Enterprise Desktop 的用途，并确保所用的软硬件符合这些要求。在部署到整个站点前，考虑在单台计算机上测试您的设置。

要安装多少工作站？

确定部署 SUSE Linux Enterprise Desktop 的范围。根据计划安装的数量，考虑不同的安装方法或用 SUSE Linux Enterprise 的独特 AutoYaST 技术进行批量安装。关于这个主题的更多信息，请参考第 2 章 **部署策略** [7]。

如何为您的部署获取软件更新？

Novell 为您的产品提供的所有增补程序都可以下载到已注册用户。在 <http://www.novell.com/suselinuxportal> 中注册并查找增补程序支持数据库。

本地部署需要帮助吗？

Novell 提供对 SUSE Linux Enterprise Desktop 所有主题的培训、支持和咨询。有关详细信息，请参见 <http://www.novell.com/products/desktop/>。

1.1 硬件要求

需要满足 SUSE Linux Enterprise Desktop 的最低硬件要求，才能成功安装并运行 SUSE Linux Enterprise Desktop。包含了最基本、最关键的软件和迷你图形用户界面的 SUSE Linux Enterprise Desktop 最小安装至少需要：

- Intel* Pentium* III, 500 MHz
- 256 MB 物理 RAM
- 800 MB 可用磁盘空间
- 800 x 600 显示器分辨率

对于包括您选择的桌面环境（GNOME 或 KDE）和大量应用程序的 SUSE Linux Enterprise Desktop 标准安装，推荐以下配置：

- Intel Pentium IV, 2.4 GHz 或更高，或任何 AMD64 或 Intel 64 处理器
- 1—2 个物理 CPU
- 512 MB 物理 RAM 或者更高
- 1024 x 768 显示器分辨率（或更高）

1.2 使用 SUSE Linux Enterprise Desktop 的原因

选择 SUSE Linux Enterprise Desktop 以及确定已安装系统的用途时，请考虑以下几个因素：

丰富的应用程序

SUSE Linux Enterprise Desktop 提供的丰富软件对企业环境中的专业用户和家庭用户或较小网络中的用户都很有吸引力。

操作简便

SUSE Linux Enterprise Desktop 来自两个为企业设计的桌面环境：GNOME 和 KDE。它们都能使用户愉快地适应 Linux 系统，同时保持效率和生产率。要详细了解这两个桌面，请参见 *GNOME 用户指南* 和 *KDE 用户指南*。

支持移动用户

NetworkManager 技术已充分集成到 SUSE Linux Enterprise Desktop 及它的两个桌面环境中，移动用户可尽情享受方便地连接到有线和无线网络并在其间自由切换。

无缝集成到现有网络中

SUSE Linux Enterprise Desktop 的设计使之成为多功能的网络成员。它能与不同类型的网络协作：

纯粹的 Linux 网络 SUSE Linux Enterprise Desktop 是完整的 Linux 客户程序，支持传统 Linux 和 Unix* 环境中使用的所有协议。它能与由其他 SUSE Linux 或 SUSE Linux Enterprise 计算机组成的网络很好地集成。支持 LDAP、NIS 和本地鉴定。

Windows 网络 SUSE Linux Enterprise Desktop 支持用 Active Directory 作为鉴定源。它为您提供了安全而稳定的 Linux 操作系统的一切优点，同时还提供与其他 Windows 客户机的方便交互以及从 Linux 客户机操纵 Windows 用户的手段。在 [第 12 章 *Active Directory 支持*](#) [275] 中论述了这个功能的细节。

Windows 和 Novell 网络 有了 Novell 及其网络专门技术的支持，SUSE Linux Enterprise Desktop 自然会为您提供对 Novell 技术的支持，例如 GroupWise、Novell Client for Linux 以及 iPrint，还提供了对 Novell eDirectory 服务的鉴定支持。

使用 Novell AppArmor 的应用程序安全性

SUSE Linux Enterprise Desktop 通过强制实施为您的应用程序定制的安全性配置文件来保证应用程序的安全。要了解有关 Novell AppArmor 的详细信息，请参见 <http://www.novell.com/documentation/apparmor/>。

部署策略

部署 SUSE® Linux Enterprise 有几种不同的方法。有各种各样的方法可供选择，可以选择使用物理媒体的本地安装或网络安装服务器，也可以选择使用远程控制、高度自定义的自动安装技术进行大规模部署。选择最符合您的要求的方法。

提示: 将 Xen Virtualization 用于 SLED

您可以使用 Xen 虚拟化技术来测试 SUSE Linux Enterprise Desktop 的虚拟实例；然后再将它转出到实际的硬件。您还可以测试 Windows*-in-SLED 的基本安装。关于 SUSE Linux Enterprise 可用的虚拟技术的更多信息，请参阅 <http://www.novell.com/documentation/vmserver/index.html>。

2.1 最多部署 10 个工作站

如果您的 SUSE Linux Enterprise 部署仅包含 1 到 10 个工作站，最简便的 SUSE Linux Enterprise 部署方法是如第 3 章 **使用 YaST 进行安装** [17]中所述的纯手动安装。手动安装可以按照您的要求用几种不同的方法完成：

从 SUSE Linux Enterprise 媒体进行安装 [8]

如果想安装单个断开连接的工作站，请考虑使用此方法。

通过使用 SLP 来从网络服务器进行安装 [8]

如果想安装一个工作站或几个工作站并且拥有通过 SLP 宣布的网络安装服务器，请考虑使用此方法。

从网络服务器进行安装 [9]

如果想安装一个工作站或几个工作站并且网络安装服务器可用，请考虑使用此方法。

表 2.1 从 SUSE Linux Enterprise 媒体进行安装

安装源	SUSE Linux Enterprise 媒体工具包
要求手动交互的任务	<ul style="list-style-type: none">• 插入安装媒体• 引导安装目标• 更改媒体• 决定 YaST 安装范围• 用 YaST 系统配置系统
远程控制的任务	无
细节	第 3.1.2 节 “从 SUSE Linux Enterprise 媒体进行安装” [18]

表 2.2 通过使用 SLP 来从网络服务器进行安装

安装源	含有 SUSE Linux Enterprise 安装媒体的网络安装服务器
要求手动交互的任务	<ul style="list-style-type: none">• 插入引导磁盘• 引导安装目标• 决定 YaST 安装范围• 用 YaST 配置系统
远程控制的任务	无，但此方法可以与 VNC 组合

细节

第 3.1.3 节 “通过使用 SLP 来从网络服务器进行安装” [18]

表 2.3 从网络服务器进行安装

安装源	含有 SUSE Linux Enterprise 安装媒体的网络安装服务器
要求手动交互的任务	<div><ul style="list-style-type: none">• 插入引导磁盘• 提供引导选项• 引导安装目标• 决定 yast 安装范围• 用 YaST 配置系统</div>
远程控制的任务	无，但此方法可以与 VNC 组合
细节	第 3.1.4 节 “从没有 SLP 的网络源安装” [19]

2.2 最多部署 100 个工作站

随着越来越多的工作站需要安装，您肯定不愿意再手动安装和配置每个工作站。有许多自动或半自动的方法，还有几个可执行安装的选项可以使用最少物理用户交互，甚至不用物理用户交互。

在考虑使用全自动的方法之前，要考虑到情况越复杂，安装时间将越长。如果您的部署有时间限制，可以选不太复杂的方法，以便使其更快速地进行。大规模的部署以及那些需要远程执行的部署，可以采用自动的方法。

从以下选项中选择：

通过 VNC— 静态网络配置的简单远程安装 [10]

对于小规模或中等规模的静态网络安装，请考虑使用此方法。需要有网络、网络安装服务器及 VNC 查看器应用程序。

通过 VNC— 动态网络配置的简单远程安装 [11]

对于小规模或中等规模的通过 DHCP 的动态网络安装，请考虑使用此方法。需要有网络、网络安装服务器及 VNC 查看器应用程序。

通过 VNC— PXE 引导和 LAN 唤醒的远程安装 [12]

在应该通过网络安装并无需与安装目标进行物理交互的小规模或中等规模情况下，请考虑使用此方法。要求有网络、网络服务器、网络引导映像、网络可引导目标硬件及 VNC 查看器应用程序。

通过 SSH— 静态网络配置的简单远程安装 [12]

对于小规模或中等规模的静态网络安装，请考虑使用此方法。要求有网络、网络安装服务器及 SSH 客户应用程序。

通过 SSH— 静态网络配置的简单远程安装 [13]

对于小规模或中等规模的通过 DHCP 的动态网络安装，请考虑使用此方法。要求有网络、网络安装服务器及 SSH 客户应用程序。

通过 SSH— PXE 引导和 LAN 唤醒的远程安装 [13]

在应该通过网络安装并无需与安装目标进行物理交互的小规模或中等规模情况下，请考虑使用此方法。要求有网络、网络服务器、网络引导映像、网络可引导目标硬件及 SSH 客户应用程序。

简单的大规模安装 [14]

对相同计算机的大规模部署，请考虑使用此方法。如果进行配置是为了使用网络引导，则完全不需要与目标系统的物理交互。需要有网络、网络安装服务器、远程控制应用程序（如 VNC 查看器或 SSH 客户程序）以及 AutoYaST 配置配置文件。如果使用网络引导，也需要有网络引导映像和网络可引导硬件。

基于规则的自动安装 [15]

到各种类型硬件的大规模部署，请考虑使用此方法。如果进行配置是为了使用网络引导，则完全不需要与目标系统的物理交互。需要有网络、网络安装服务器、远程控制应用程序（如 VNC 查看器或 SSH 客户程序）、几个 AutoYaST 配置配置文件及 AutoYaST 的规则安装。如果使用网络引导，也需要有网络引导映像和网络可引导硬件。

表 2.4 通过 VNC— 静态网络配置的简单远程安装

安装源	网络
-----	----

准备工作	<ul style="list-style-type: none"> • 设置安装源 • 从安装媒体引导
控制和监视	远程：VNC
最适合	有不同硬件的小规模和中等规模部署情况
缺点	<ul style="list-style-type: none"> • 每台计算机必须单独安装 • 引导需要物理访问
细节	第 4.1.1 节 “通过 VNC 静态网络配置进行简单远程安装” [38]

表 2.5 通过 VNC— 动态网络配置的简单远程安装

安装源	网络
准备工作	<ul style="list-style-type: none"> • 设置安装源 • 从安装媒体引导
控制和监视	远程：VNC
最适合	有不同硬件的小规模和中等规模部署情况
缺点	<ul style="list-style-type: none"> • 每台计算机必须单独安装 • 引导需要物理访问
细节	第 4.1.2 节 “通过 VNC 动态网络配置进行简单远程安装” [39]

表 2.6 通过 VNC—PXE 引导和 LAN 唤醒的远程安装

安装源	网络
准备工作	<ul style="list-style-type: none">• 设置安装源• 配置 DHCP、TFTP，PXE 引导和 WOL• 从网络引导
控制和监视	远程：VNC
最适合	<ul style="list-style-type: none">• 有不同硬件的小规模和中等规模部署情况• 完全远程安装；跨站点部署
缺点	每台计算机必须手动安装
细节	第 4.1.3 节 “通过 VNC—PXE Boot 和“网络唤醒”进行远程安装” [40]

表 2.7 通过 SSH—静态网络配置的简单远程安装

安装源	网络
准备工作	<ul style="list-style-type: none">• 设置安装源• 从安装媒体引导
控制和监视	远程：SSH
最适合	<ul style="list-style-type: none">• 有不同硬件的小规模和中等规模部署情况• 低带宽连接到目标
缺点	<ul style="list-style-type: none">• 每台计算机必须单独安装

- 引导需要物理访问

细节

第 4.1.4 节 “通过 SSH 静态网络配置进行简单远程安装” [41]

表 2.8 通过 SSH—静态网络配置的简单远程安装

安装源	网络
准备工作	<ul style="list-style-type: none">• 设置安装源• 从安装媒体引导
控制和监视	远程：SSH
最适合	<ul style="list-style-type: none">• 有不同硬件的小规模和中等规模部署情况• 低带宽连接到目标
缺点	<ul style="list-style-type: none">• 每台计算机必须单独安装• 引导需要物理访问
细节	第 4.1.5 节 “通过 SSH 动态网络配置进行简单远程安装” [43]

表 2.9 通过 SSH—PXE 引导和 LAN 唤醒的远程安装

安装源	网络
准备工作	<ul style="list-style-type: none">• 设置安装源• 配置 DHCP、TFTP，PXE 引导和 WOL• 从网络引导

控制和监视	远程：SSH
最适合	<ul style="list-style-type: none"> • 有不同硬件的小规模和中等规模部署情况 • 完全远程安装；跨站点部署 • 低带宽连接到目标
缺点	每台计算机必须单独安装
细节	第 4.1.6 节 “通过 SSH—PXE Boot 和“网络唤醒”进行远程安装” [44]

表 2.10 简单的大规模安装

安装源	最好是网络
准备工作	<ul style="list-style-type: none"> • 收集硬件信息 • 创建 AutoYaST 配置文件 • 设置安装服务器 • 分发配置文件 • 设置网络引导（DHCP、TFTP、PXE、WOL） <p>或</p> <p>从安装媒体引导目标</p>
控制和监视	通过 VNC 或 SSH 本地或远程
最适合	<ul style="list-style-type: none"> • 大规模部署情况 • 相同硬件 • 不能访问系统（网络引导）

缺点	仅适用于有相同硬件的计算机
细节	第 5.1 节 “简单的大规模安装” [71]
<hr/>	
表 2.11 基于规则的自动安装	
<hr/>	
安装源	最好是网络
准备工作	<ul style="list-style-type: none">• 收集硬件信息• 创建 AutoYaST 配置文件• 创建 AutoYaST 规则• 设置安装服务器• 分发配置文件• 设置网络引导（DHCP、TFTP、PXE、WOL） 或 从安装媒体引导目标
控制和监视	通过 SSH 或 VNC 本地或远程
最适合	<ul style="list-style-type: none">• 不同硬件• 跨站点部署
缺点	复杂规则安装
细节	第 5.2 节 “基于规则的自动安装” [81]
<hr/>	

2.3 部署 100 多个工作站

中涉及的有关中等安装规模的大部分情况同样适于大规模部署。第 2.1 节“最多部署 10 个工作站” [7] 然而，由于安装目标越来越多，全自动安装方法利大于弊。

很值得花时间在 AutoYaST 中创建一套成熟的规则和级别框架以满足大规模部署站点的要求。根据安装项目的规模，无需单独接触每个目标将为您节省大量的时间。

使用 YaST 进行安装

用 YaST 安装 SUSE Linux Enterprise® 系统，它是安装和配置系统的核心工具。YaST 可指导您完成整个安装过程和系统的基本配置。在安装和配置期间，YaST 会分析您当前的系统设置和硬件部件，根据这一分析提议安装设置。默认 YaST 在窗口左边显示所有安装步骤的概述，并提供每一步的联机帮助文本。单击 *帮助* 查看帮助文本，单击 *步骤* 切换回概述。

如果您是第一次使用 SUSE Linux Enterprise，多数情况下最好按默认的 YaST 提议操作，但您也可以根据您的需要和希望，按此处所述调整设置来微调您的系统。基本系统配置的许多部分（例如用户帐户或系统语言）都可以在安装过程完成后修改。

3.1 系统启动以进行安装

您可以从 SUSE Linux Enterprise CD 或 DVD 之类的本地安装源安装 SUSE Linux Enterprise，也可以从 FTP、HTTP、SLP 或 NFS 服务器等网络源安装。这些方法都需要物理访问系统来进行安装并且在安装期间需要进行用户交互。无论安装源如何，安装步骤基本相同。

3.1.1 引导选项

除 CD 或 DVD 之外，还存在其他引导选项，如果从 CD 或 DVD 引导时出现问题，就可以使用这些引导选项。中介绍了这些选项。[表 3.1 “引导选项”](#) [18]

表 3.1 引导选项

引导选项	说明
DVD/CD-ROM	这是最简单的引导选项。如果系统具有 Linux 支持的本地 CD/DVD-ROM 驱动器，则可以使用此选项。
软盘	用于生成引导软盘的映像位于 CD/DVD 1 上的 <code>/boot</code> 目录中。在同一目录中还提供了一个 <code>README</code> 文件。
PXE 或 BOOTP	这一选项必须得到系统的 BIOS 或固件的支持，而且网络中必须有一个可用的引导服务器。还可以用另一个 SUSE Linux Enterprise 系统来执行此任务。
硬盘	SUSE Linux Enterprise 也可以从硬盘来进行引导。为此，请将内核 (<code>linux</code>) 和安装系统 (<code>initrd</code>) 从 CD/DVD 1 上的目录 <code>/boot/loader</code> 中复制到硬盘，并向引导加载程序添加相应的项。

3.1.2 从 SUSE Linux Enterprise 媒体进行安装

要从媒体安装，请将第一张 CD 或 DVD 插入系统的相应驱动器中进行安装。重新引导系统以便从媒体引导，打开引导屏幕。

3.1.3 通过使用 SLP 来从网络服务器进行安装

如果您的网络设置支持 OpenSLP，并且已将网络安装源配置为通过 OpenSLP 声明自己，请使用其他引导选项或从媒体引导系统。在引导屏幕中，选择所需的安装选项。按 **F3** 和 **F4**，然后选择 *SLP*。

安装程序会使用 OpenSLP 检索网络安装源的位置并使用 DHCP 配置网络连接。如果 DHCP 网络配置失败，则会提示手动输入相应参数。然后，安装将按照如下所述进行。

3.1.4 从没有 SLP 的网络源安装

如果您的网络设置不支持用 OpenSLP 获取网络安装资源，请从媒体引导系统，或使用其他引导选项。在引导屏幕中，选择所需的安装选项。按 F3 和 F4，然后选择所需的网络协议（NFS、HTTP、FTP 或 SMB）。提供服务器地址和安装媒体的路径。

安装程序会使用 OpenSLP 检索网络安装源的位置并使用 DHCP 配置网络连接。如果 DHCP 网络配置失败，则会提示手动输入相应参数。然后，安装将按照如下所述进行。

3.2 安装工作流程

SUSE Linux Enterprise 的安装主要可分为三部分：准备、安装和配置。在准备阶段期间，您将配置一些基本参数，如语言、时间和桌面类型。在安装阶段期间，您将确定要安装的软件、安装位置以及已安装系统的引导方式。完成安装后，计算机将重引导为新安装的系统并开始配置。在这个阶段，您将设置用户和密码，并配置网络和因特网访问以及硬件部件（如打印机）。

3.3 引导屏幕

引导屏幕将显示安装过程的多个选项。从硬盘引导是默认选中的，它会引导已安装系统，因为 CD/DVD 经常会留在驱动器中。要安装系统，请用箭头键选择一个安装选项。相关的选项有：

安装

常规安装方式。将启用所有常用的硬件功能。将启用所有最新的硬件功能。

安装 — 禁用 ACPI

如果常规安装失败，则可能是因为系统硬件不支持 ACPI（高级配置和电源接口）造成的。如果是这种情况，请使用此选项进行安装，这样将没有 ACPI 支持。

安装 — 禁用本地 APIC

如果常规安装失败，可能是由于系统硬件不支持本地 APIC（高级可编程中断控制器）。如果是这种情况，请使用此选项进行安装，这样将没有本地 APIC 支持。

如果没有把握，请先尝试以下选项之一：禁用 *Installation—ACPI* 或 *Installation—Safe* 设置。

安装 — 安全设置

引导使用了 DMA 方式（用于 CD-ROM 驱动器）且禁用了电源管理功能的系统。

救援系统

启动不带图形用户界面的最小 Linux 系统。有关详细信息，请参见“[使用应急系统](#)”一节 [752]。

内存测试

通过反复的读写操作过程来测试系统的 RAM。通过重引导来终止测试。有关详细信息，请参见[第 46.2.5 节 “无法引导”](#) [729]。

菜单中的安装选项只禁用问题最大的功能。如果需要禁用或设置其他功能，请使用引导选项提示。在以下地址查找内核参数的详细信息：<http://en.opensuse.org/Linuxrc>。

用屏幕底部栏中指示的功能键更改语言、监视器分辨率或安装源，或者添加硬件供应商的其他驱动程序：

F1 帮助

获取引导屏幕的活动元素的上下文相关帮助。

F2 语言

选择安装的显示语言。默认语言为英语。

F3 其他选项

启用更多可设置的安装选项。

按下 F3 后，可以设置其他选项：

F3 视频方式

选择安装的多种图形显示方式。如果图形安装出现问题，则选择文本方式。

F4 源

通常情况下都是从插入的安装媒体来执行安装。在此处，选择其他源，如 FTP 或 NFS 服务器。如果在具有 SLP 服务器的网络中执行安装，则可以使用此选项选择服务器上可用的安装源。有关 SLP 的更多详细信息，请参见[第 31 章 网络中的 SLP 服务](#) [587]。

F5 驱动程序

按此键可通知系统您有一个可选的、含有 SUSE Linux Enterprise 驱动程序更新的磁盘。通过文件菜单，可在安装开始前直接从 CD 装载驱动程序。如果选择是，系统将在安装过程中的适当时间提示您插入更新磁盘。默认选项为否 — 不装载驱动程序更新。

启动安装后，SUSE Linux Enterprise 将装载和配置最小 Linux 系统以运行安装过程。要在此过程中查看引导讯息和版权声明，请按 Esc 键。此过程完成后，YaST 安装程序将启动并显示图形安装程序。

提示: 无鼠标安装

如果安装程序没有正确检测到您的鼠标，请用 Tab 键进行浏览，用箭头键卷屏，用 Enter 键确认选择。

3.3.1 提供访问 SMT 服务器的数据

如果您的网络提供了 SMT 服务器来提供本地更新源，则您需要为客户机提供服务器的 URL。客户机和服务器仅通过 HTTPS 协议通讯，因此，如果服务器证书不是由证书授权者颁发的，则您还需要输入该证书的路径。必须在引导提示符处输入此信息。

smturl

SMT 服务器的 URL。该 URL 具有固定的格式，为 `https://FQN/center/regsvc/` FQN 必须是 SMT 服务器的完全限定的主机名。示例：

```
smturl=https://smt.example.com/center/regsvc/
```

smtcert

SMT 服务器证书的位置。指定以下位置之一：

URL

可以下载证书的远程位置（http、https 或 ftp）。示例：

```
smtcert=http://smt.example.com/smt-ca.crt
```

软盘

指定软盘上的位置。必须在引导时插入软盘，如果没有软盘，系统将不会提示您插入。值必须以字符串 floppy 开头，后跟证书的路径。示例：

```
smtcert=floppy/smt/smt-ca.crt
```

本地路径

本地计算机上证书的绝对路径。示例：

```
smtcert=/data/inst/smt/smt-ca.crt
```

交互式

使用询问可在安装期间打开一个弹出菜单，您可在其中指定证书的路径。请勿将此选项用于 **AutoYaST**。示例

```
smtcert=ask
```

停用证书安装

如果证书将由外接式附件产品安装，或您将使用由正式证书授权者颁发的证书，请使用已完成选项。示例：

```
smtcert=done
```

警告：当心键入错误

确保您输入的值是正确的。如果尚未正确指定 `smturl`，更新源的注册将失败。如果输入了错误的 `smtcert` 值，系统将提示您输入证书的本地路径。

如果未指定 `smtcert`，它将默认为 `http://FQN/smt.crt`，其中 `FQN` 为 **SMT** 服务器的名称。

3.4 语言

通常可以根据需要配置 **YaST** 和 **SUSE Linux Enterprise** 使用不同的语言。此处选择的语言也用于键盘布局。另外，**YaST** 使用此语言设置来猜测系统时钟的时区。这些设置可以在稍后选择要在系统上安装的辅助语言时进行修改。

您可在稍后的安装过程中更改语言，如第 3.9 节“**安装设置**”[24]中所述。有关已安装系统中语言设置的信息，请参见第 8.1 节“**YaST 语言**”[110]。

3.5 媒体检查

仅当从使用下载的 **ISO** 创建的媒体安装时，才会显示“媒体检查”对话框。如果从原始媒体集安装，则将跳过该对话框。

媒体检查将检查媒体的完整性。要开始媒体检查，请选择包含安装媒体的驱动器，然后单击**启动检查**。检查可能需要一段时间。

要测试多个媒体，请等至对话框中显示了结果讯息，然后再更改媒体。如果检查的最后一个媒体并非您开始安装时所使用的媒体，YaST将提示您使用适当媒体，然后再继续安装。

警告: 媒体检查失败

如果媒体检查失败，则表明您的媒体已损坏。请勿继续安装，因为安装可能会失败，或您可能会丢失数据。请更换损坏的媒体，然后重新开始安装过程。

如果媒体检查的结果表明没有问题，请单击**下一步**继续安装。

3.6 许可证协议

请通读显示在屏幕上的许可证协议。如果同意这些条款，请选择**是**，我同意此许可证协议，然后单击**下一步**确认您的选择。如果您不同意此许可证协议，则不允许您安装 SUSE Linux Enterprise，并且安装将终止。

3.7 安装方式

系统分析（YaST 试图在您的计算机上查找其他已安装系统或已有的 SUSE Linux Enterprise 系统）完成后，YaST 会显示可用的安装模式：

新安装

选择该选项从头开始新安装。

更新现有系统

选择该选项更新到较新的版本。关于系统更新的更多信息，请参见[第 9 章 更新 SUSE Linux Enterprise](#) [171]。

其他选项

该选项使您可以放弃安装和引导，或者修复已安装的系统。要引导已安装的 SUSE Linux Enterprise，请选择**引导已安装的系统**。如果引导已安装的 SUSE Linux Enterprise 时有问题，请参见[第 46.3 节 “引导问题”](#) [733]。

为修复引导失败的已安装系统，请选择**修复已安装的系统**。有关系统修复选项的说明，请参见“**使用 YaST 系统修复**”一节 [748]。

注意: 更新已安装系统

只有已安装过较早的 SUSE Linux Enterprise 系统时才可以更新。如果未安装任何 SUSE Linux Enterprise 系统，则只能执行全新安装。

3.8 时钟和时区

在此对话框中，从列表中选择您所在地区和时区。在安装期间，将根据所选的安装语言预先选择这两项。在**硬件时钟设置**下选择**本地时间**和**UTC(GMT)**。此选择取决于计算机上 BIOS 硬件时钟的设置。如果将它设置为与 UTC 相对应的 GMT，则您的系统便可以依赖 SUSE Linux Enterprise 在标准时间和夏令时之间自动切换。单击**更改**可设置当前日期和时间。安装后，单击**下一步**继续安装。

3.9 安装设置

在进行了全面的系统分析之后，YaST 将显示所有安装设置的合理建议。可在**概述**选项卡中更改基本设置，**专家**选项卡中有高级选项。要修改建议的值，请单击**更改**，然后选择要更改的类别，或单击其中一个标题。在完成了对显示在这些对话框中的项的配置之后，总是会返回到摘要窗口，而且每次返回此窗口都会进行相应的更新。

提示: 将更改重设置为默认值

您可通过单击**更改 > 重设置为默认值**将所有更改重设置为默认值。随后 YaST 会再次显示原始提示。

3.9.1 概述

在**概述**选项卡下，列出了在常规安装环境下有时需要手动干预的那几个选项。在此处修改分区、软件选项和区域设置。

分区

在大多数情况下，YaST 都能给出合理的分区方案，您可以直接接受而不必更改。YaST 还可以用于自定义分区，但要更改分区，您必须是有经验的用户。

首次选择分区时，YaST 的“分区”对话框将显示建议的分区设置。要接受这些设置，请单击 *接受提议*。

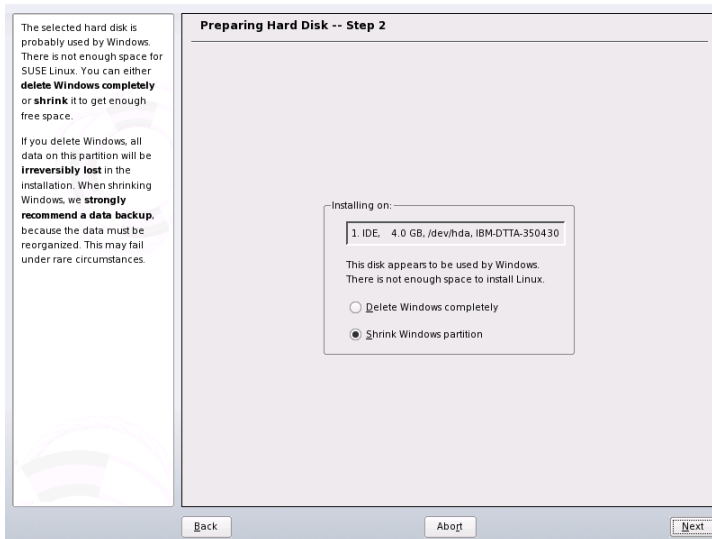
要对提议进行微小改动，请选择 *该提议中的基础分区设置*，并在下个对话框中调整分区。要获得完全不同的分区，请选择 *创建自定义分区设置*。在下一个对话框中，请选择要分区的特定磁盘，或者如果您想要访问所有磁盘，请选择 *自定义分区*。有关自定义分区的更多信息，请参考 [第 8.5.5 节 “使用 YaST 分区程序”](#) [132]SUSE Linux Enterprise Server 文档。

建议的分区模式应具有足够的磁盘空间。如果实施您自己的分区模式，请注意系统分区的绝对最小空间为 5 GB。建议至少 10 GB。文档、音乐文件和图像之类的个人数据需要额外空间。

调整 Windows 分区的大小

如果先前选择了包含 Windows FAT 或 NTFS 分区的硬盘作为安装目标，则 YaST 可以将该分区删除或缩小。如果所选硬盘只包含一个包括整个硬盘的 Windows 分区，则此功能尤其有用（请参见 [图 3.1 “对 Windows 分区进行操作的可能选项”](#) [26]）。

图 3.1 对 Windows 分区进行操作的可能选项



如果选择完全删除 *Windows*，则会将 *Windows* 分区标记为要删除，空间将用于安装 SUSE Linux Enterprise。

警告: 删除 Windows

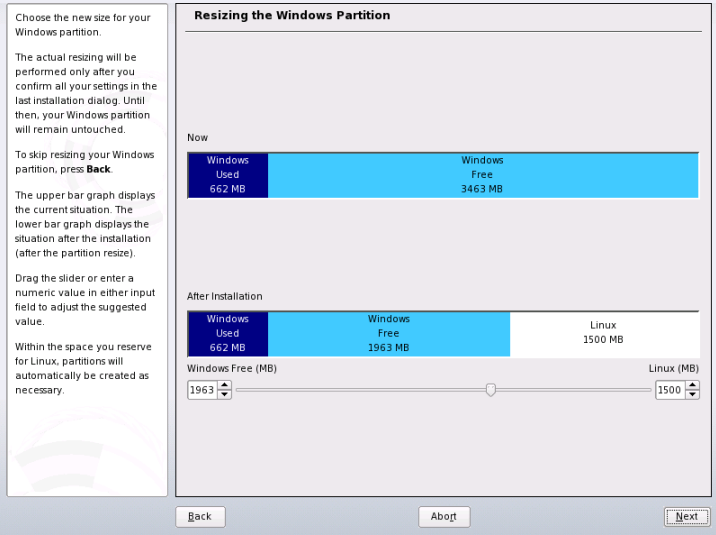
如果删除 *Windows*，则在格式化开始后，将丢失所有数据，无法恢复。

要缩小 *Windows* 分区，需要中断安装并引导 *Windows* 为缩小分区作准备。对于所有 *Windows* 文件系统，请执行以下步骤：

1. 停用虚拟内存文件（如果有）。
2. 运行 `scandisk`。
3. 运行 `defrag`。

在这些准备步骤后，重新启动 SUSE Linux Enterprise 安装。在使用 Linux 分区设置时，请选择缩小 *Windows* 分区。在快速检查分区之后，YaST 将打开一个显示有调整 *Windows* 分区大小建议的对话框。

图 3.2 调整 Windows 分区的大小



第一个条形图显示 Windows 当前占用了多少磁盘空间以及仍有多少空间可用。第二个条形图显示根据 YaST 的当前建议，调整大小后空间如何分布。请参阅图 3.2 “调整 Windows 分区的大小” [27]。要更改建议的设置，请使用滑块或输入字段来更改分区大小。

如果通过选择下一步退出该对话框，则将储存该设置并将返回到上一个对话框。在对硬盘进行格式化之前，实际调整大小将在稍后进行。

重要: 写到 NTFS 分区

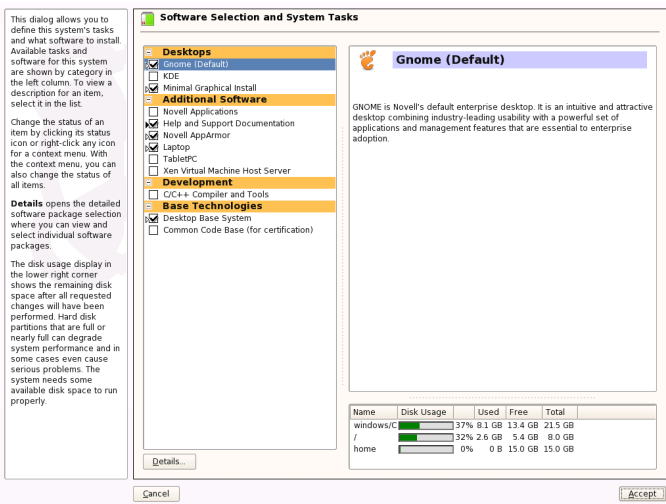
默认情况下，WINDOWS NT、Windows 2000 以及 Windows XP 使用 NTFS 文件系统。SUSE Linux Enterprise 包括对 NTFS 文件系统的基本写访问支持，但此功能的作用有限。这意味着您可以从 Linux 读取 Windows 文件或重写这些文件，但是您不能扩展或删除它们。

软件

SUSE Linux Enterprise 包含许多用于各种应用目的的软件包。在建议窗口中单击软件以启动软件选择并根据需要修改安装范围。从中间的列表选择您的模式，并在窗口右侧部分中查看说明。每种模式都包含一些特定功能所需的软件包（例

如多媒体或办公软件)。如果希望根据要安装的软件包来获取更为详细的选项, 请选择**细节**切换到 YaST 软件管理器。请参阅图 3.3 “使用 YaST 软件管理器安装和去除软件” [28]。

图 3.3 使用 YaST 软件管理器安装和去除软件



以后任何时候, 您都可以安装其他软件包, 或从系统中删除软件包。有关详细信息, 请参见第 8.3.1 节 “安装和去除软件” [111]。

语言

要更改系统语言或配置对第二语言的支持, 请选择**语言**。从列表中选择一种语言。主语言用作系统语言。选择一种或多种次语言, 用于在无需安装其他软件包的情况下, 即可随时切换到这些语言之一。

3.9.2 专家

如果您是高级用户, 希望配置引导、更改时区或默认运行级别, 请选择**专家**选项卡。它显示的以下额外条目未包含在概述选项卡上:

系统

此对话框将显示 YaST 能够获取的关于您计算机的所有硬件信息。可在列表中选择任意项，然后单击 [详细信息](#) 以查看关于所选项的详细信息。高级用户还可通过选择系统设置来更改 PCI ID 设置和内核设置。

附加产品

附加媒体的已添加源显示在概述中。开始 SUSE Linux Enterprise 的安装前，如果需要请在此处添加、去除或修改附加产品。

引导

YaST 会为您的系统建议引导配置。通常，您可以保持这些设置不变。但是，如果您需要自定义设置，则可修改对系统的建议。有关信息，请参见 [第 18.3 节 “使用 YaST 配置引导加载程序” \[376\]](#)。

时区

这和先前在 [第 3.8 节 “时钟和时区” \[24\]](#) 中显示的配置相同。

默认运行级别

SUSE Linux Enterprise 可以引导到不同的运行级别。通常情况下无需更改此处的任何内容，但是如果需要，可使用此对话框设置默认的运行级别。有关运行级别配置的信息，请参见 [第 17.2.3 节 “使用 YaST 配置系统服务（运行级别）” \[362\]](#)。

3.10 执行安装

在指定所有安装设置后，在建议窗口中单击接受开始安装。通过单击安装确认。某些软件可能需要许可证确认。如果您选择的软件包括此类软件，则将显示许可证确认对话框。单击接受以安装软件。如果不同意许可证，则单击我不同意，那么将不会安装软件。

根据系统性能和所选的软件，安装通常需要 15 到 30 分钟的时间。在此过程中，将放映一个幻灯片来介绍 SUSE Linux Enterprise 的功能。选择 [细节](#) 可切换到安装日志。在安装了所有包后，YaST 会立即引导新的 Linux 系统，此后您就可以配置硬件和设置系统服务了。

3.11 已安装系统的配置

系统现已安装，但尚未配置供使用。尚未配置任何用户、硬件或服务。如果配置在进行到此阶段中的某个步骤时失败，则其将重新启动并继续从最后一个成功的步骤开始。

首先，提供系统管理员帐户密码（`root` 用户）。配置因特网访问和网络连接。利用有效的因特网连接，您可以将系统更新作为安装的一部分来执行。您还可以连接到一个鉴定服务器，以便在本地网络中集中管理用户。最后，配置连接到计算机的硬件设备。

3.11.1 系统管理员 “root” 的密码

`root` 是超级用户（即系统管理员）的名称。与有权或无权在系统上执行特定操作的普通用户不同，`root` 用户不受权限限制，他们可以执行一切操作，包括：更改系统配置、安装程序以及设置新硬件。如果用户忘记他们的密码或遇到其他有关系统的问题，`root` 用户可以提供帮助。`root` 帐户应只用于系统管理、维护和修复工作。以 `root` 用户的身份登录来进行日常工作相当危险，因为一个错误操作就可能导致系统文件丢失，而且无法挽回。

为了进行校验，必须两次输入 `root` 用户的密码。切勿忘记 `root` 密码。一旦输入，就不能在系统中检索此密码。

键入密码时，字符将由圆点代替，因此您无法看到正在键入的字符串。如果您不确定是否键入了正确的字符串，请使用 *测试键盘布局* 字段来进行测试。

SUSE Linux Enterprise 可对密码使用 DES、MD5 或 Blowfish 加密算法。默认加密类型是 Blowfish。要更改加密类型，请单击 *专家选项 > 加密类型* 并选择新类型。

以后，可随时在已安装系统中更改 `root` 权限。要进行此操作，请运行 YaST 并启动 *安全和用户 > 用户管理*。

3.11.2 主机名和域名

主机名是网络中的计算机名称。域名是网络的名称。主机名和域是默认设置的。如果您的系统是某个网络的一部分，则主机名在此网络中必须是唯一的，但网络中所有主机的域名必须是相同的。

在许多网络中，系统通过 DHCP 来接收其名称。在这种情况下，无需修改主机名和域名。代为选择通过 *DHCP* 更改主机名。要能够使用此主机名来访问您的系统（即使您的系统未连接到网络），请选择将主机名写到 `/etc/hosts`。如果您经常在不重新启动桌面环境的情况下更改网络（例如，在不同的 WLAN 之间切换），则请勿启用此选项，因为当 `/etc/hosts` 中的主机名更改时，桌面系统可能会无法区分。

要在安装后随时更改主机名设置，请使用 YaST 网络设备 > 网卡。有关更多信息，请参见第 30.4.1 节“使用 YaST 配置网卡”[555]。

3.11.3 网络配置

默认设置下，将启用带有 *NetworkManager* 小程序的用户控制界面。*NetworkManager* 是只需最小程度的用户干预就可以自动连接的一种工具。它最适合移动计算。如果要用无 *NetworkManager* 的传统方式，请单击禁用 *NetworkManager*。有关 *NetworkManager* 的更多详细信息，请参见第 30.5 节“使用 *NetworkManager* 管理网络连接”[569]。

此配置步骤还允许您配置系统的网络设备并进行安全性设置，例如，设置防火墙或代理。要以后再配置网卡连接，请选择跳过配置，并单击下一步。网络硬件的配置工作也可以在系统安装完毕后进行。如果跳过网络设备配置，系统将保持脱机，无法获取任何可用更新。

除了设备配置，还可在此步骤中配置以下网络设置：

网络模式

启用或禁用 *NetworkManager*，如上所述。

防火墙

默认情况下，在所有已配置的网络接口上启用 *SuSEfirewall2*。要对此计算机全局禁用防火墙，请单击禁用。如果启用了防火墙，则可打开 SSH 端口以便允许通过安全壳层进行远程连接。要打开详细的防火墙配置对话框，请

单击**防火墙**。有关详细信息，请参见第 39.4.1 节“使用 YaST 配置防火墙”[664]。

IPv6

默认启用 IPv6 支持。要禁用它，请单击**禁用 IPv6**。有关 IPv6 的更多信息，请参见第 30.2 节“IPv6 — 下一代的因特网”[546]。

VNC 远程管理

要通过 vnc 远程管理计算机，请单击**更改 > vnc 远程管理**，启用远程管理，然后在防火墙中打开端口。如果有多个网络设备并且希望选择要打开端口的网络设备，则单击**防火墙细节**，然后选择网络设备。还可使用更安全的选项—SSH 来进行远程管理。

代理

如果具有控制网络中因特网访问的代理服务器，则在此对话框中配置代理 URL 和鉴定细节。

提示: 将网络配置重设置为默认值

单击**更改 > 重设置为默认值**将网络设置重设置为原始建议值。这会放弃所作的任何更改。

测试因特网连接

在配置完网络连接后，可对其进行测试。为此，YaST 建立至 SUSE Linux Enterprise 服务器的连接，并下载最新的发行说明。安装过程结束时请阅读这些说明。测试成功也是联机注册和更新的先决条件。

如果有多个网络接口，请校验是否使用了正确的网卡来连接到因特网。如果不是，请单击**更改设备**。

要开始测试，请选择**是，测试因特网连接**，然后单击**下一步**。在下一个对话框中，查看测试进程和测试结果。可通过**查看日志**获得有关测试过程的详细信息。如果测试失败，请单击**上一步**返回到网络配置以更正输入。

如果不希望此时测试连接，请选择**否，跳过此测试**，然后单击**下一步**。这样还会跳过下载发行说明、配置客户中心和联机更新。可在最初配置系统后随时执行这些步骤。

3.11.4 Novell Customer Center 配置

要获取技术支持和产品更新，请先注册并激活产品。*Novell Customer Center* 配置会帮助执行此操作。

如果您是脱机状态并希望跳过此步骤，请选择*以后配置*。这样还会跳过 SUSE Linux Enterprise 联机更新。

在*为方便起见可包含中*，选择注册时是否发送未经请求的附加信息。这将简化注册步骤。单击*细节*可获取有关数据保密和所收集数据的详细信息。

除激活并注册您的产品外，该模块还会向您的配置添加官方更新编目。该编目提供对已知 bug 或安全问题的修复，它们可通过联机更新安装。

除了更新编目外，还会添加两个带有 ATI 和 NVidia 图形卡官方驱动程序的编目。尽管 SUSE Linux Enterprise 带有这些卡的开放源代码驱动程序，但是，图形卡制造商直接提供的官方驱动程序可以提供附加功能。为了添加这些编目，需要导入其公共 GnuPG 密钥（这些密钥用来确保编目是由编目拥有者提供的）。单击*信任密钥*，然后单击*导入*以添加该编目。单击*跳过包*，然后单击*中止阻止*将特定编目添加到您的配置。

要使这些编目保持有效，请选择*定期与 Customer Center 同步*。此选项将检查您的编目并添加新可用的编目，或去除旧编目。它不会改动手动添加的编目。

提示: 技术支持

有关更多技术支持信息，请参见<http://www.novell.com/support/products/desktop/>。

3.11.5 联机更新

如果 *Novell Customer Center* 配置成功，则选择是否执行 YaST 联机更新。如果这些服务器上有任何增补程序包，请立即下载并安装它们，以修复已知错误或安全问题。有关如何在已安装系统中执行联机更新的指导，请参见第 8.3.5 节“**YaST 联机更新**” [119]

重要: 下载软件更新程序

根据因特网连接的带宽和更新文件的大小, 更新程序的下载可能需要一些时间。如果增补程序系统本身进行了更新, 则联机更新将重启动, 并在重启动后下载更多的增补程序。如果更新了内核, 则系统将在完成配置前进行重引导。

3.11.6 用户数

如果已在先前的安装步骤中成功配置了网络访问, 则现在您可以从若干用户管理选项中进行选择。如果尚未配置网络连接, 请创建本地用户帐户。有关用户管理的详细信息, 请参见 [第 8.9.1 节 “用户管理”](#) [145]SUSE Linux Enterprise Server 文档。

本地 (/etc/passwd)

在已安装的主机上对用户进行本地管理。此选项适用于独立工作站。用户数据由本地文件 `/etc/passwd` 管理。无论是否有可用的网络, 进入此文件的所有用户都可以登录系统。

如果 YaST 发现了以前版本的 SUSE Linux Enterprise 或使用 `/etc/passwd` 的另一个系统, 则可以导入本地用户。要执行该操作, 请选中从以前的安装中读取用户数据并单击选择。在下一个对话框中选择要导入的用户, 并单击确定。

LDAP

在 LDAP 服务器上对网络中的所有系统进行集中用户管理。有关更多信息, 请参见 [第 35.3 节 “使用 YaST 配置 LDAP 客户机”](#) [612]。

NIS

在 NIS 服务器上对网络中的所有系统进行集中用户管理。有关更多信息, 请参见 [第 33.1 节 “配置 NIS 客户机”](#) [597]。

Windows 域

在 Linux 和 Windows 混用的网络中经常使用 SMB 鉴定。有关详细信息, 请参见 [第 12.3 节 “为 Active Directory 配置 Linux 客户机”](#) [281]。

eDirectory LDAP

eDirectory 鉴定用于 Novell 网络。

注意: 鉴定菜单的内容

如果使用自定义软件包选择, 而菜单中缺少一种或多种鉴定方式, 所需软件包可能未安装。

您可以与选定的用户管理方式一起使用 Kerberos 鉴定。这对于将 SUSE Linux Enterprise 集成到 Active Directory 域很关键, 在[第 12 章 Active Directory 支持 \[275\]](#)中对此有说明。要使用 Kerberos 鉴定, 请选择安装 *Kerberos* 鉴定。

3.11.7 发行说明

完成用户鉴定设置后, YaST 即显示发行说明。建议您阅读这些内容, 因为其中包含手册印刷时未涵盖的重要的最新信息。如果已测试因特网连接, 请阅读最新版本的发行说明, 该说明可从 SUSE Linux Enterprise 的服务器获取。安装后, 请使用[杂项 > 发行说明](#)来查看发行说明。

3.11.8 硬件配置

在安装结束时, YaST 将打开一个对话框, 用于配置图形卡以及与系统连接的其他硬件部件。单击相应部件来启动硬件配置。YaST 在很大程度上会自动检测和配置设备。

如[第 8.4 节 “硬件” \[124\]](#)中所述, 您可以跳过任何外围设备, 并在以后配置它们。要跳过配置, 请选择[跳过配置](#), 然后单击[下一步](#)。

但您应立即配置图形卡。尽管一般情况下可以接受 YaST 配置的显示设置, 但就分辨率、颜色深度以及其他图形功能而言, 大多数用户都会有明显的个人偏好。要更改这些设置, 请选择相应的项, 然后将值设置为期望的值。要测试新配置, 请单击[测试配置](#)。

提示: 将硬件配置重设置为默认值

您可以单击[更改 > 重设置为默认值](#)取消更改。随后 YaST 会再次显示原始提示。

3.11.9 完成安装

安装成功后，YaST 将显示 *安装已完成* 对话框。在此对话框中，选择是否为 AutoYaST 复制新安装的系统。要进行此操作，请选择为 *AutoYaST 复制此系统*。当前系统的配置文件储存在 `/root/autoyast.xml` 中。

AutoYaST 系统用于自动安装一个或多个 SUSE Linux Enterprise 系统而无需用户操作。AutoYaST 安装是通过使用具有安装和配置数据的控制文件来执行的。单击最后一个对话框中的 *完成* 来完成 SUSE Linux Enterprise 的安装。

3.12 图形登录

现在即已安装和配置了 SUSE Linux Enterprise。除非您已启用自动登录功能或已自定义默认运行级别，否则就应在屏幕上看到图形登录界面，在其中输入用户名和密码登录至系统。如果激活了自动登录，则将自动启动桌面。

有关 KDE 或 GNOME 桌面环境的简介，请参见 *KDE 快速入门* 和 *GNOME 快速入门*。在 *KDE 用户指南* 和 *GNOME 用户指南* 中查找关于 KDE 或 GNOME 的桌面环境及其上运行的应用程序的详细信息。

远程安装

可以用几种不同的方式安装 SUSE Linux Enterprise®。除了在第 3 章 *使用 YaST 进行安装* [17] 中介绍的通常所用的媒体安装方式之外，还可以选择多种基于网络的安装方式，甚至可以用完全无人值守的安装方式来安装 SUSE Linux Enterprise。

两种方法均使用两个简短列表进行介绍：一个列出此方法的先决条件，另一个则说明基本过程。随后，将会就这些安装方案用到的所有技术提供更详细的信息。

注意

在以下各节中，将存放新安装的 SUSE Linux Enterprise 的系统称为 *目标系统* 或 *安装目标*。术语 *安装源* 用于所有的安装数据源。这包括物理媒体（如 CD 和 DVD）以及在网络中分发安装数据的网络服务器。

4.1 远程安装的安装方案

本节将介绍远程安装的最常用安装方案。对于每种方案，请仔细查看先决条件列表并遵循该方案的概述过程。如果需要特定步骤的详细说明，请访问各种方案的链接。

重要

X Windows 系统的配置不是任何远程安装过程的一部分。在安装完成后，请以 root 登录到目标系统，输入 `telinit 3`，然后启动 **SaX2**，配置图形硬件。

4.1.1 通过 VNC 静态网络配置进行简单远程安装

此类型安装仍然需要对物理系统进行一定程度的访问以便引导安装。安装本身完全由使用 VNC 连接到安装程序的远程工作站控制。在使用[第 3 章 使用 YaST 进行安装](#) [17]中的手动安装方式时需要用户干预。

对于此类型安装，请确保满足以下要求：

- 远程安装源：带有活动网络连接的 NFS、HTTP、FTP 或 SMB
- 具有有效网络连接的目标系统
- 具有有效网络连接和 VNC 查看器软件或支持 Java 的浏览器（Firefox、Konqueror、Internet Explorer 或 Opera）的控制系统
- 用于引导目标系统的物理引导媒体（CD 或 DVD）
- 有效的静态 IP 地址已分配给安装源和控制系统
- 可分配到目标系统的有效静态 IP 地址

要执行此种安装，请执行如下操作：

- 1 按[第 4.2 节 “设置存放安装源的服务器”](#) [45]中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。对于 SMB 安装源，请参阅[第 4.2.5 节 “管理 SMB 安装源”](#) [52]。
- 2 使用 SUSE Linux Enterprise 媒体工具包中的第一张 CD 或 DVD 来引导目标系统。

- 3 在出现目标系统的引导屏幕时，使用引导选项提示来设置相应的 VNC 选项和安装源的地址。第 4.4 节“引导用于安装的目标系统”[63]中对此有详细描述。

目标系统引导后进入一个基于文本的环境，它给出了网络地址和显示编号，任何 VNC 查看器应用程序或浏览器都可以藉此寻址到图形安装环境。VNC 安装将通过 OpenSLP 发布自身通告，并且在 `service:/` 方式或 `slp:/` 方式下使用 Komqueror 可将其找到。

- 4 在控制工作站上，按第 4.5.1 节“VNC 安装”[67]中所述打开 VNC 查看应用程序或万维网浏览器，并连接到目标系统。
- 5 按第 3 章 使用 YaST 进行安装 [17]中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。
- 6 完成安装。

4.1.2 通过 VNC 动态网络配置进行简单远程安装

此类型安装仍然需要对物理系统进行一定程度的访问以便为安装进行引导。网络配置是通过 DHCP 进行的。安装本身完全由使用 VNC 连接到安装程序的远程工作站控制，但是仍需要用户对实际配置工作进行干预。

对于此类型安装，请确保满足以下要求：

- 远程安装源：带有活动网络连接的 NFS、HTTP、FTP 或 SMB
- 具有有效网络连接的目标系统
- 具有有效网络连接和 VNC 查看器软件或支持 Java 的浏览器（Firefox、Konqueror、Internet Explorer 或 Opera）的控制系统
- 用于引导目标系统的物理引导媒体（CD、DVD 或自定义的引导磁盘）
- 运行提供 IP 地址的 DHCP 服务器

要执行此种安装，请执行如下操作：

- 1 按第 4.2 节 “设置存放安装源的服务器” [45]中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。对于 SMB 安装源，请参阅第 4.2.5 节 “管理 SMB 安装源” [52]。
- 2 使用 SUSE Linux Enterprise 媒体工具包中的第一张 CD 或 DVD 来引导目标系统。
- 3 在出现目标系统的引导屏幕时，使用引导选项提示来设置相应的 VNC 选项和安装源的地址。中对此有详细描述。第 4.4 节 “引导用于安装的目标系统” [63]。

目标系统引导后进入一个基于文本的环境，它给出了网络地址和显示编号，任何 VNC 查看器应用程序或浏览器都可以藉此寻址到图形安装环境。VNC 安装将通过 OpenSLP 发布自身通告，并且在 `service:/` 方式或 `slp:/` 方式下使用 Komqueror 可将其找到。
- 4 在控制工作站上，按第 4.5.1 节 “VNC 安装” [67]中所述打开 VNC 查看应用程序或万维网浏览器，并连接到目标系统。
- 5 按第 3 章 使用 YaST 进行安装 [17]中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。
- 6 完成安装。

4.1.3 通过 VNC—PXE Boot 和“网络唤醒”进行远程安装

此类型安装是完全无人值守的。目标计算机是远程启动和引导的。只有实际安装时才需要用户交互。此方式适用于跨站点部署。

要执行此类型安装，请确保满足以下要求：

- 远程安装源：带有活动网络连接的 NFS、HTTP、FTP 或 SMB
- TFTP 服务器
- 为网络运行 DHCP 服务器
- 目标系统支持 PXE 引导、联网和网络唤醒，且已插入并连接到网络

- 具有有效网络连接和 VNC 查看器软件或支持 Java 的浏览器（Firefox、Konqueror、Internet Explorer 或 Opera）的控制系统

要执行此类型安装，请执行如下操作：

- 1 按第 4.2 节“设置存放安装源的服务器”[45]中所述设置安装源。选择 NFS、HTTP、或 FTP 网络服务器或按第 4.2.5 节“管理 SMB 安装源”[52]中所述配置 SMB 安装源。
- 2 设置存放引导映像（可被目标系统拉出）的 TFTP 服务器。中对此进行了描述。第 4.3.2 节“设置 TFTP 服务器”[56]。
- 3 设置 DHCP 服务器以向所有计算机提供 IP 地址，并向目标系统显示 TFTP 服务器的位置。中对此进行了描述。第 4.3.1 节“设置 DHCP 服务”[54]。
- 4 准备目标系统的 PXE 引导。中对此有详细描述。第 4.3.5 节“准备目标系统的 PXE 引导”[62]。
- 5 使用“网络唤醒”开始目标系统的引导过程 中对此进行了描述。第 4.3.7 节“局域网唤醒”[62]。
- 6 在控制工作站上，按第 4.5.1 节“VNC 安装”[67]中所述打开 VNC 查看应用程序或万维网浏览器，并连接到目标系统。
- 7 按第 3 章 使用 YaST 进行安装 [17]中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。
- 8 完成安装。

4.1.4 通过 SSH 静态网络配置进行简单远程安装

此类型安装仍然需要对目标系统进行一定程度的访问，以便为安装进行引导以及确定安装目标的 IP 地址。安装本身完全由使用 SSH 连接到安装程序的远程工作站控制。在使用第 3 章 使用 YaST 进行安装 [17]中所述的常规安装时需要用户干预。

对于此类型安装，请确保满足以下要求：

- 远程安装源：带有活动网络连接的 NFS、HTTP、FTP 或 SMB
- 具有有效网络连接的目标系统
- 具有有效网络连接和有效 SSH 客户机软件的控制系统
- 目标系统的物理引导媒体（CD、DVD 或自定义的引导磁盘）
- 有效的静态 IP 地址已分配给安装源和控制系统
- 可分配到目标系统的有效静态 IP 地址

要执行此种安装，请执行如下操作：

- 1 按第 4.2 节 “设置存放安装源的服务器” [45]中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。对于 SMB 安装源，请参阅第 4.2.5 节 “管理 SMB 安装源” [52]。
- 2 使用 SUSE Linux Enterprise 媒体工具包中的第一张 CD 或 DVD 来引导目标系统。
- 3 在出现目标系统的引导屏幕时，使用引导选项提示来设置相应的网络连接参数、安装源地址以及 SSH 支持。中对此有详细描述。第 4.4.3 节 “使用自定义引导选项” [65]。

目标系统引导后进入一个基于文本的环境，它给出了一个网络地址，通过该地址，任何 SSH 客户机都可以寻址到图形安装环境。
- 4 在控制工作站上，按“连接到安装程序”一节 [69]中所述打开终端窗口并连接到目标系统。
- 5 按第 3 章 使用 YaST 进行安装 [17]中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。
- 6 完成安装。

4.1.5 通过 SSH 动态网络配置进行简单远程安装

此类型安装仍然需要对目标系统进行一定程度的访问，以便为安装进行引导以及确定安装目标的 IP 地址。安装本身完全由使用 VNC 连接到安装程序的远程工作站控制，但是仍需要用户对实际配置工作进行干预。

对于此类型安装，请确保满足以下要求：

- 远程安装源：带有活动网络连接的 NFS、HTTP、FTP 或 SMB
- 具有有效网络连接的目标系统
- 具有有效网络连接和有效 SSH 客户机软件的控制系统
- 用于引导目标系统的物理引导媒体（CD 或 DVD）
- 运行提供 IP 地址的 DHCP 服务器

要执行此种安装，请执行如下操作：

- 1 按第 4.2 节“设置存放安装源的服务器”[45]中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。对于 SMB 安装源，请参阅第 4.2.5 节“管理 SMB 安装源”[52]。
- 2 使用 SUSE Linux Enterprise 媒体工具包中的第一张 CD 或 DVD 来引导目标系统。
- 3 在出现目标系统的引导屏幕时，使用引导选项提示来设置相应的网络连接参数、安装源位置以及 SSH 支持。关于如何使用这些参数的详细说明，请参见第 4.4.3 节“使用自定义引导选项”[65]。

目标系统引导后进入一个基于文本的环境，它给出了一个网络地址，通过该地址，任何 SSH 客户机都可以寻址到图形安装环境。
- 4 在控制工作站上，按“连接到安装程序”一节[69]中所述打开终端窗口并连接到目标系统。
- 5 按第 3 章使用 YaST 进行安装[17]中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。

6 完成安装。

4.1.6 通过 SSH—PXE Boot 和“网络唤醒”进行远程安装

此类安装是完全无人值守的。目标机器是远程启动和引导的。

要执行此类型安装，请确保满足以下要求：

- 远程安装源：带有活动网络连接的 NFS、HTTP、FTP 或 SMB
- TFTP 服务器
- 为网络运行 DHCP 服务器，向需要安装的主机提供一个静态 IP
- 目标系统支持 PXE 引导、联网和网络唤醒，且已插入并连接到网络
- 具有有效网络连接和 SSH 客户机软件的控制系統

要执行此类型安装，请执行如下操作：

- 1 按第 4.2 节“设置存放安装源的服务器”[45]中所述设置安装源。选择 NFS、HTTP 或 FTP 网络服务器。有关 SMB 安装源的配置，请参阅第 4.2.5 节“管理 SMB 安装源”[52]。
- 2 设置存放引导映像（可被目标系统拉出）的 TFTP 服务器。中对此进行了描述。第 4.3.2 节“设置 TFTP 服务器”[56]。
- 3 设置 DHCP 服务器以向所有计算机提供 IP 地址，并向目标系统显示 TFTP 服务器的位置。中对此进行了描述。第 4.3.1 节“设置 DHCP 服务”[54]。
- 4 准备目标系统的 PXE 引导。中对此有详细描述。第 4.3.5 节“准备目标系统的 PXE 引导”[62]。
- 5 使用“网络唤醒”开始目标系统的引导过程 中对此进行了描述。第 4.3.7 节“局域网唤醒”[62]。
- 6 在控制工作stations上，按第 4.5.2 节“SSH 安装”[69]中所述启动 SSH 客户机并连接到目标系统。

- 7 按第 3 章 使用 *YaST* 进行安装 [17] 中所述执行安装。在目标系统重引导从而完成安装的最后一部分后，需要重连接到目标系统。
- 8 完成安装。

4.2 设置存放安装源的服务器

根据用作 SUSE Linux Enterprise 网络安装源的计算机上所运行的操作系统，服务器配置可有多种选择。设置安装服务器的最简单方法是使用 SUSE Linux Enterprise Server 9 或 10 或 SUSE Linux 9.3 及更高版本上的 YaST。在其他版本的 SUSE Linux Enterprise Server 或 SUSE Linux Enterprise 上，需要手动设置安装源。

提示

您甚至可以将 Microsoft Windows 计算机用作 Linux 部署的安装服务器。有关详细信息，请参见第 4.2.5 节“管理 SMB 安装源” [52]。

4.2.1 使用 YaST 设置安装服务器

YaST 提供了一个用于创建网络安装源的图形工具。它支持 HTTP、FTP 和 NFS 网络安装服务器。

- 1 以 root 登录到充当安装服务器的计算机上。
- 2 启动 *YaST* > 其他 > 安装服务器。
- 3 选择服务器类型（HTTP、FTP 或 NFS）。所选的服务器服务将在系统每次启动时自动启动。如果所选服务器类型中的某项服务已经在系统上运行，但您希望对该服务器进行手动配置，则请通过不配置任何网络服务来取消激活服务器服务的自动配置。在这两种情况下，都需要定义服务器上可用安装数据所在的目录。
- 4 配置所需的服务器类型。此步骤与服务器服务的自动配置相关。如果取消激活自动配置，则将跳过此步骤。

定义安装数据所在的 FTP 或 HTTP 服务器的根目录的别名。该安装源以后将放在 `ftp://Server-IP/Alias/name(ftp)` 或 `http://Server-IP/Alias/Name(HTTP)` 下。Name 代表安装源的名称，该名称将在下面的步骤中定义。如果您在上一步中选择了 NFS，请定义通配符和导出选项。可在 `nfs://Server-IP/Name` 下访问 NFS 服务器。有关 NFS 和导出选项的详细信息，请参见第 37 章 [通过 NFS 共享文件系统](#) [635]。

提示: 防火墙设置

务必使服务器系统的防火墙设置允许 HTTP、NFS 和 FTP 端口的数据流量。如果当前不允许，则请启动 YaST 防火墙模块并打开对应的各个端口。

- 5 配置安装源。在将安装媒体复制到你目标位置前，请先定义该安装源的名称（理想情况是容易记忆的产品和版本的缩写）。YaST 允许提供安装媒体的 ISO 映像来取代安装 CD 副本。如果希望使用 ISO 映像，请激活相关的复选框并指定 ISO 文件所在的本地目录路径。依据使用此安装服务器分发的产品而定，可能需要更多插件 CD 或服务包 CD，且可能需要将这些 CD 添加为额外的安装源。要通过 OpenSLP 在网络中就安装服务器发布通告，请激活相应的选项。
-

提示

如果您的网络设置支持此选项，请考虑通过 OpenSLP 就安装源发布通告。这样就无需在每台目标计算机上输入网络安装路径。将使用 SLP 引导选项引导这些目标系统，并且无需进一步的配置就可以找到网络安装源。有关该选项的详细信息，请参见第 4.4 节 [“引导用于安装的目标系统”](#) [63]。

- 6 上载安装数据。配置安装服务器过程中最冗长的一步是复制实际的安装 CD。按 YaST 要求的顺序插入媒体，然后等待复制过程结束。当安装源完全复制完毕后，选择完成返回到现有信息源的概要并关闭配置。

现在您的安装服务器就已完全配置好并准备提供服务了。它将在每次系统启动时自动启动。不需要执行额外操作。如果您在最初的步骤中使用 YaST 取消了所选网络服务的自动配置，则只需正确地手动配置和启动该服务即可。

要取消对某个安装源的激活，请选定要去除的该安装源，然后选择删除。安装数据将从系统去除。要取消对网络服务的激活，请使用各个 YaST 模块。

如果您的安装服务器需要向多个版本的产品提供安装数据，请启动 YaST 安装服务器模块并在现有安装源的概要中选择添加，以便配置新的安装源。

4.2.2 手动设置 NFS 安装源

重要

我们假定您在将充当安装服务器的计算机上使用任何种类的基于 SUSE Linux 的操作系统。如果不是这种情况，请查看其他供应商关于 NFS 的文档，而不是以下章节。

设置 NDS 安装源大致分为两步执行。第一步：创建存放安装数据的目录结构，然后将安装媒体全部复制到该结构中。第二步：将存放安装数据的目录导出到网络。

要创建存放安装数据的目录，请执行如下操作：

1 以 root 身份登录。

2 创建稍后用于存放所有安装数据的目录，然后切换到该目录。例如：

```
mkdir install/product/productversion
cd install/product/productversion
```

将 *product* 替换为产品名称的缩写，将 *productversion* 替换为包含该产品名称和版本的字符串。

3 对媒体工具包中的每张 CD，执行以下命令：

3a 将安装 CD 的所有内容复制到安装服务器目录中：

```
cp -a /media/path_to_your_CD-ROM_drive .
```

将 *path_to_your_CD-ROM_drive* 替换为 CD 或 DVD 驱动器所在的实际路径。该路径可以是 *cdrom*、*cdrecorder*、*dvd* 或 *dvdrecorder*，这取决于系统中使用的驱动器类型。

3b 将目录重命名为 CD 编号。

```
mv path_to_your_CD-ROM_drive CDx
```

将其中的 *x* 替换您 CD 的实际编号。

在 SUSE Linux Enterprise Server 上，可以使用 YaST 通过 NFS 导出安装源。按如下所示继续：

- 1 以 root 身份登录。
- 2 启动 *YaST* > 网络服务 > *NFS* 服务器。
- 3 选择启动和打开防火墙中的端口，然后单击下一步。
- 4 选择添加目录并浏览含有安装源的目录，此情况下指 *productversion*。
- 5 选择添加主机，然后输入用于存放导出的安装数据的计算机的主机名。除了在此处指定主机名之外，还可以使用通配符、网络地址范围或只用网络的域名。输入合适的导出选项或保留默认值，在大多数设置中默认值可有效工作。关于在导出 NFS 共享中使用的语法的更多信息，请阅读导出手册页。
- 6 单击完成。存放 SUSE Linux Enterprise 安装源的 NFS 服务器将自动启动并集成到引导过程中。

如果您希望通过 NFS 手动导出安装源而不是使用 YaST NFS 服务器模块，请执行如下操作：

- 1 以 root 身份登录。
- 2 打开文件 `/etc/exports`，然后输入以下行：

```
/productversion *(ro,root_squash,sync)
```

这将把目录 `//productversion` 导出到该网络中的任意主机或能够连接到该服务器的任意主机。为了限制对该服务器的访问，请使用网络掩码或域名取代常规通配符 `*`。请参见导出手册页获取详细信息。保存并退出该配置文件。

- 3 要将 NFS 服务添加到系统引导期间已启动的服务器的列表中，请执行以下命令：

```
insserv /etc/init.d/nfsserver
insserv /etc/init.d/portmap
```

- 4 使用 `rcnfsserver start` 启动 NFS。如果需要在以后更改 NFS 服务器的配置，请修改配置文件，然后通过 `rcnfsserver restart` 命令重新启动 NFS 守护程序。

通过 OpenSLP 就该 NFS 服务器发布通告，可使网络中的所有客户机都获知其地址。

- 1 以 root 身份登录。
- 2 输入目录 `/etc/slp.reg.d/`。
- 3 创建一个名为 `install.suse.nfs.reg` 的配置文件，在其中包含以下几行：

```
# Register the NFS Installation Server
service:install.suse:nfs://$HOSTNAME/path_to_instsource/CD1,en,65535
description=NFS Installation Source
```

将 `path_to_instsource` 替换为服务器上的安装源的实际路径。

- 4 保存该配置文件，然后使用 `rcslpd start` 启动 OpenSLP 守护程序。

关于 OpenSLP 的更多信息，请参见位于 `/usr/share/doc/packages/openslp/` 下的包文档，或参见第 31 章 [网络中的 SLP 服务](#) [587]。

4.2.3 手动设置 FTP 安装源

创建 FTP 安装源与创建 NFS 安装源非常相似。也可以通过 OpenSLP 在整个网络上就 FTP 安装源发布通告。

- 1 按第 4.2.2 节“[手动设置 NFS 安装源](#)”[47]中所述创建存放安装源的目录。
- 2 配置 FTP 服务器以分发安装目录的内容：
 - 2a 以 root 身份登录，然后使用 YaST 包管理器安装 `vsftpd` 包。

2b 输入 FTP 服务器根目录：

```
cd /srv/ftp
```

2c 在 FTP 根目录中创建存放安装源的子目录：

```
mkdir instsource
```

将 *instsource* 替换为产品名称。

2d 将已经存在的安装储存库的内容装入该 FTP 服务器的更改根目录环境中。

```
mount --bind path_to_instsource /srv/ftp/instsource
```

将 *path_to_instsource* 和 *instsource* 替换为符合您设置的值。
如果需要将其永久保留，请将其添加到 */etc/fstab*。

2e 通过 *vsftpd* 启动 *vsftpd*。

3 通过 OpenSLP 就安装源发布通告（如果网络设置对此支持）：

3a 在 */etc/slp.reg.d/* 下创建一个名为 *install.suse.ftp.reg* 的配置文件，其中包含以下几行：

```
# Register the FTP Installation Server
service:install.suse:ftp://$HOSTNAME/srv/ftp/instsource/CD1,en,65535
description=FTP Installation Source
```

将 *instsource* 替换为服务器上的安装源目录的实际名称。
service: 行应作为一个连续无中断的行输入。

3b 保存该配置文件，然后使用 *rcslpd start* 启动 OpenSLP 守护程序。

4.2.4 手动设置 HTTP 安装源

创建 HTTP 安装源与创建 NFS 安装源非常相似。也可以通过 OpenSLP 在整个网络上就 HTTP 安装源发布通告。

1 按第 4.2.2 节“手动设置 NFS 安装源”[47]中所述创建存放安装源的目录。

2 配置 HTTP 服务器以分发安装目录的内容：

2a 安装万维网服务器 Apache。

2b 输入 HTTP 服务器的根目录（/srv/www/htdocs）并创建用于存放安装源的子目录：

```
mkdir instsource
```

将 *instsource* 替换为产品名称。

2c 创建一个从安装源位置到万维网服务器根目录（/srv/www/htdocs）的符号链接：

```
ln -s /path_instsource /srv/www/htdocs/instsource
```

2d 修改 HTTP 服务器的配置文件（/etc/apache2/default-server.conf），使其遵循符号链接。替换以下行：

```
Options None
```

使用

```
Options Indexes FollowSymLinks
```

2e 使用 `rcapache2 reload` 重载 HTTP 服务器配置。

3 通过 OpenSLP 就安装源发布通告（如果网络设置对此支持）：

3a 在 /etc/slp.reg.d/ 下创建一个名为 `install.suse.http.reg` 的配置文件，其中包含以下几行：

```
# Register the HTTP Installation Server
service:install.suse:http://$HOSTNAME/srv/www/htdocs/instsource/CD1/,en,65535
description=HTTP Installation Source
```

将 *instsource* 替换为服务器上的安装源的实际路径。service: 行应作为一个连续无中断的行输入。

- 3b** 保存该配置文件，然后使用 `rcslpd restart` 启动 OpenSLP 守护程序：

4.2.5 管理 SMB 安装源

通过使用 SMB，您可以从 Microsoft Windows 服务器导入安装源，甚至可以在周围没有 Linux 机器的情况下开始 Linux 部署。

要设置存放 SUSE Linux Enterprise 安装源的导出 Windows 共享，请执行如下操作：

- 1 登录到 Windows 机器。
- 2 启动“资源管理器”，然后新建一个用于存放整个安装树的文件夹，并将其命名为诸如 `INSTALL` 等名称。
- 3 根据 Windows 文档中所述的过程导入此共享。
- 4 输入此共享，创建名为 *product* 的子文件夹。请将 *product* 替换为实际产品名。
- 5 输入 `INSTALL/product` 文件夹并将每张 CD 或 DVD 复制到独立的文件夹，比如 `CD1` 和 `CD2`。

要将 SMB 装入共享用作安装源，请执行如下操作：

- 1 引导安装目标。
- 2 选择安装：
- 3 按 **F4** 选择安装源。
- 4 选择 SMB，然后输入 Windows 计算机的名称或 IP 地址、共享名（在本例中为 `INSTALL/product/CD1`）、用户名和密码。

按 **Enter** 键，YaST 将启动，然后您就可以执行安装了。

4.2.6 使用服务器上安装媒体的 ISO 映像

您不用将物理媒体手动复制到服务器目录下，而是可以将安装媒体的 ISO 映像安装到安装服务器中并将它们用作安装源。要设置使用 ISO 映像，而不是媒体副本的 HTTP、NFS 或 FTP 服务器，请执行以下操作：

- 1 下载 ISO 映像并将它们保存到用作安装服务器的计算机上。
- 2 以身份 `root` 登录。
- 3 按照第 4.2.2 节“手动设置 NFS 安装源”[47]、第 4.2.3 节“手动设置 FTP 安装源”[49]或第 4.2.4 节“手动设置 HTTP 安装源”[50]中的说明，选择并创建安装数据的合适位置。
- 4 创建每张 CD 或 DVD 的子目录。
- 5 要将各个 ISO 映像安装和解开到最终位置，请发出以下命令：

```
mount -o loop path_to_iso path_to_instsource/product/mediumx
```

将 *path_to_iso* 替换为 ISO 映像本地副本的路径，将 *path_to_instsource* 替换为服务器的目录，将 *product* 替换为产品名称以及将 *mediumx* 替换为您正使用的媒体类型（CD 或 DVD）和编号。

- 6 多次重复上述步骤，以安装产品所需的全部 ISO 映像。
- 7 按照第 4.2.2 节“手动设置 NFS 安装源”[47]、第 4.2.3 节“手动设置 FTP 安装源”[49]或第 4.2.4 节“手动设置 HTTP 安装源”[50]中的说明，与往常一样启动安装服务器。

4.3 准备目标系统的引导

此部分讨论复杂引导场景中需要的配置任务。其中包含了 DHCP、PXE 引导、TFTP 和网络唤醒的“准备应用”配置示例。

4.3.1 设置 DHCP 服务

有两种方法设置 DHCP 服务器。对于 SUSE Linux Enterprise Server 9 及更高版本，YaST 将向进程提供图形界面。任何其他基于 SUSE Linux 产品的用户和非 SUSE Linux 用户应该手动编辑配置文件或使用其操作系统供应商提供的前端。

重要

以下章节只讲述准备 DHCP 服务器以支持 PXE 引导所需要的配置更改。有关 DHCP 配置的详细信息，请参见操作系统供应商提供的手册。

用 YaST 设置 DHCP 服务器

要宣布到网络用户机的 TFTP 服务器位置并指定安装目标应该使用的引导映像文件，请向 DHCP 服务器配置添加两个声明。

- 1 以 root 身份登录到主管 DHCP 服务器的计算机。
- 2 启动 *YaST > 网络服务 > DHCP 服务器*。
- 3 完成基本 DHCP 服务器安装的安装向导。
- 4 当遇到退出启动对话框的警告时，选择专家设置并选择是。
- 5 在配置声明对话框中，选择新系统所在的子网并单击编辑。
- 6 在子网配置对话框中，选择添加来向子网配置添加新选项。
- 7 选择 filename 并输入 pxelinux.0 作为值。
- 8 添加另一选项 (next-server) 并设置 TFTP 服务器地址的值。
- 9 选择确定和完成以完成 DHCP 服务器配置。

要配置 DHCP 以向特定主机提供静态 IP 地址，请输入 DHCP 服务器配置模块的专家设置 (步骤 4 [54]) 并添加主机类型的新声明。将选项 hardware 和 fixed-address 添加到此主机声明并提供适当的值。

手动设置 DHCP 服务器

除了向网络客户机提供自动地址分配外，所有 DHCP 服务器还需要就 TFTP 服务器 IP 地址和应由目标机器上的安装例程导入的文件发布通告。

- 1 以 root 身份登录到主管 DHCP 服务器的计算机。
- 2 向位于 `/etc/dhcpd.conf` 下的 DHCP 服务器配置文件中追加以下几行：

```
group {
    # PXE related stuff
    #
    # "next server" defines the tftp server that will be used
    next server ip_tftp_server:
    #
    # "filename" specifies the pxelinux image on the tftp server
    # the server runs in chroot under /srv/tftpboot
    filename "pxelinux.0";
}
```

将 *ip_of_the_tftp_server* 替换为 TFTP 服务器的实际 IP 地址。关于 `dhcpd.conf` 中可用选项的更多信息，请参见 `dhcpd.conf` 手册页。

- 3 执行 `rcdhcpd restart` 重新启动 DHCP 服务器。

如果打算或正在将 SSH 用于 PXE 和网络唤醒安装的远程控制，请专门指定 DHCP 应提供给安装目标的 IP 地址。要实现此设置，请根据以下示例修改上述的 DHCP 配置：

```
group {
    # PXE related stuff
    #
    # "next server" defines the tftp server that will be used
    next server ip_tftp_server:
    #
    # "filename" specifies the pxelinux image on the tftp server
    # the server runs in chroot under /srv/tftpboot
    filename "pxelinux.0";
    host test { hardware ethernet mac_address;
                fixed-address some_ip_address; }
}
```

`host` 语句引入了安装目标的主机名。要将主机名和 IP 地址与特定主机绑定，则必须了解系统的硬件（NAC）地址并指定它。请将本例中使用的所有变量替换为符合您环境的实际值。

在重新启动 DHCP 服务器之后，它将向所指定的主机提供一个静态 IP，从而使您能够通过 SSH 连接到该系统。

4.3.2 设置 TFTP 服务器

在 SUSE Linux Enterprise Server 和 SUSE Linux Enterprise 上使用 YaST 设置 TFTP 服务器，或者在任何其他支持 xinetd 和 tftp 的 Linux 操作系统上手动完成。一旦目标系统成功引导并发出请求，FTP 服务器就会将引导映像发送到该目标系统。

使用 YaST 设置 TFTP 服务器

- 1 以 root 身份登录。
- 2 启动 *YaST* > 网络服务 > *TFTP 服务器*，并安装请求的包。
- 3 单击 *启用* 以确保服务器启动并包含在引导例程中。之后您就无需为此再进行任何操作。xinetd 将在引导时启动。
- 4 单击 *打开防火墙中的端口* 以在您计算机上运行的防火墙中打开相应的端口。如果您的服务器上未运行任何防火墙，则该选项不可用。
- 5 单击 *浏览* 以查找引导映像目录。默认目录 /tftpboot 是自动创建并选定的。
- 6 单击 *完成* 以应用设置并启动服务器。

手动设置 TFTP 服务器

- 1 以 root 身份登录，然后安装 tftp 包和 xinetd 包。
- 2 如果这两个包不可用，请创建 /srv/tftpboot 目录和 /srv/tftpboot/pxelinux.cfg 目录。
- 3 按第 4.3.3 节“使用 PXE 引导”[57]中所述添加引导映像所需的相应文件。
- 4 修改位于 /etc/xinetd.d/ 下的 xinetd 的配置，以确保 TFTP 服务器在引导时启动：

4a 如果该配置文件不存在，请使用 `touch tftp` 命令在该目录下创建一个名为 `tftp` 的文件。然后运行 `chmod 755 tftp`。

4b 打开文件 `tftp`，添加以下几行：

```
service tftp
{
    socket_type          = dgram
    protocol             = udp
    wait                = yes
    user                 = root
    server               = /usr/sbin/in.tftpd
    server_args          = -s /srv/tftpboot
    disable              = no
}
```

4c 保存该文件，然后使用 `rcxinetd restart` 命令重启 `xinetd`。

4.3.3 使用 PXE 引导

在 Preboot Execution Environment (PXE) Specification(<http://www.pix.net/software/pxeboot/archive/pxespec.pdf>) 中可获取一些技术背景信息以及 PXE 的完整规范。

1 切换到您的安装储存库所在目录，然后输入以下命令将 `linux`、`initrd`、`message` 和 `memtest` 文件复制到 `/srv/tftpboot` 目录中：

```
cp -a boot/loader/linux boot/loader/initrd
    boot/loader/message boot/loader/memtest /srv/tftpboot
```

2 通过 YaST 直接从 CD 或 DVD 安装 `syslinux` 包。

3 输入以下命令来将 `/usr/share/syslinux/pxelinux.0` 文件复制到 `/srv/tftpboot` 目录中：

```
cp -a /usr/share/syslinux/pxelinux.0 /srv/tftpboot
```

4 切换到安装储存库所在目录，然后输入以下命令，将 `isolinux.cfg` 文件复制到 `/srv/tftpboot/pxelinux.cfg/default`：

```
cp -a boot/loader/isolinux.cfg /srv/tftpboot/pxelinux.cfg/default
```

- 5 编辑 `/srv/tftpboot/pxelinux.cfg/default` 文件，将以 `gfxboot`、`readinfo` 和 `framebuffer` 开头的行去除。
- 6 在默认的 `failsafe` 和 `apic` 标签的追加行中插入以下条目：

```
insmod=kernel module
```

通过此输入框，输入所需的网络内核模块来支持 PXE 客户机上的网络安装。用您的网络设备的适当模块名替代 `kernel module`。

```
netdevice=interface
```

此条目定义了必须用于网络安装的客户端网络接口。它只在客户端配备了多块网卡的情况下才需要，且必须根据具体情况采用相应的值。如果客户端安装了一块网卡，则该条目可以省略。

```
install=nfs://ip_instserver/path_instsource/CD1
```

该条目定义了用于客户机安装的分发服务器和安装源。请将 `ip_instserver` 替换为安装服务器的实际 IP 地址。

`path_instsource` 应替换为安装源的实际路径。对于 HTTP、FTP 或 SMB 源，除了应将协议前缀分别替换为 `http`、`ftp` 或 `smb`，其他地方都是相似的。

重要

如果需要向安装例程指定其他引导选项，如 SSH 或 VNC 引导参数，请将它们追加到 `install` 条目中。在 [第 4.4 节“引导用于安装的目标系统”](#) [63] 提供了参数的概述和一些例子。

以下是一个 `/srv/tftpboot/pxelinux.cfg/default` 文件示例。请根据自己的网络设置调整协议前缀，并通过向 `install` 条目添加 `vnc` 或 `vncpassword` 选项，或者添加 `usessh` 和 `sshpassword` 选项来指定要用于连接到安装程序的首选方法。由 \ 分隔的多个行必须分别作为一个连续的行输入，其中不能有换行符，也不能有 \。

```
default linux
```

```
# default  
label linux
```

```

kernel linux
    append initrd=initrd ramdisk_size=65536 insmod=e100 \
        install=nfs://ip_instserver/path_instsource/product/CD1

# failsafe
label failsafe
    kernel linux
    append initrd=initrd ramdisk_size=65536 ide=nodma apm=off acpi=off \
        insmod=e100 install=nfs://ip_instserver/path_instsource/product/CD1

# apic
label apic
    kernel linux
    append initrd=initrd ramdisk_size=65536 apic insmod=e100 \
        install=nfs://ip_instserver/path_instsource/product/CD1

# manual
label manual
    kernel linux
    append initrd=initrd ramdisk_size=65536 manual=1

# rescue
label rescue
    kernel linux
    append initrd=initrd ramdisk_size=65536 rescue=1

# memory test
label memtest
    kernel memtest

# hard disk
label harddisk
    localboot 0

implicit      0
display       message
prompt        1
timeout       100

```

将 *ip_instserver* 和 *path_instsource* 替换为您设置中使用的值。

以下一节简要介绍了在此设置中使用的 **PXELINUX** 选项。关于可用选项的更多信息，在位于 `/usr/share/doc/packages/syslinux/` 下的 `syslinux` 包中。

4.3.4 PXELINUX 配置选项

此处列出的选项是 **PXELINUX** 配置文件中所有可用选项中的一部分。

`DEFAULT kernel options...`

用于设置默认内核命令行。如果 PXELINUX 自动引导，则该选项的作用相当于已在引导提示符处输入了在 DEFAULT 后输入的所有内容（表示自动引导的 auto 选项除外，它是自动添加的）。

如果不存在任何配置文件或配置文件中不存在 DEFAULT 条目，则默认情况为内核名称 “linux” 且不带任何选项。

`APPEND options...`

用于向内核命令行添加一个或多个选项。添加的这些选项对自动引导和手动引导都适用。这些选项添加在内核命令行的最前面，通常允许用显式输入的内核选项覆盖它们。

`LABEL label KERNEL image APPEND options...`

表示如果将 *label* 输入为要引导的内核，则 PXELINUX 将取代引导 *image*，并且将使用指定的 APPEND 选项代替文件的全局部分中指定的选项（在首个 LABEL 命令之前）。*image* 的默认值与 *label* 的相同，如果未指定 APPEND，则默认情况下使用全局条目（如果有）。最多允许 128 个 LABEL 条目。

请注意 GRUB 使用以下语法：

```
title mytitle
    kernel my_kernel my_kernel_options
    initrd myinitrd
```

PXELINUX 使用以下语法：

```
label mylabel
    kernel mykernel
    append myoptions
```

标签的数据报处理如同文件名一样，且在数据报处理之后，它们必定是唯一的。例如，“v2.1.30” 和 “v2.1.31” 这两个标签在 PXELINUX 下是无法区分的，因为它们在数据报处理之后成为同一个 DOS 文件名。

kernel 不必是 Linux 内核，它可以是引导扇区或 COMBOOT 文件。

`APPEND -`

表示不追加任何内容。在 LABEL 段中用一个连字符作为参数的 APPEND 可用于覆盖全局 APPEND。

LOCALBOOT *type*

在 PXELINUX 上，指定 LOCALBOOT 0 取代 KERNEL 选项表示调用该特定标签，这样就会从本地磁盘引导而不是从内核引导。

自变量	说明
0	执行正常引导
4	在“通用网络驱动程序接口”（UNDI）驱动程序仍然驻留在内存中的情况下执行本地引导
5	在整个 PXE 堆栈（包括 UEFI 驱动程序）仍然驻留于内存中的情况下执行本地引导

不定义所有其他的值。如果对 UEFI 或 PXE 堆栈不甚了解，请指定 0。

TIMEOUT *time-out*

表示在自动引导之前在引导提示符下等待的时间（以 1/10 秒为单位）。一旦用户按了键盘上的任意键，超时将立即取消（假设从用户完成命令开始）。如果超时值为零，则将完全禁用超时（这也是默认值）。允许的最大超时值为 35996（即小于一小时）。

PROMPT *flag_val*

如果 flag_val 为 0，则仅当按下 Shift 或 Alt 键，或者在 Caps Lock 或 Scroll Lock 状态下，才显示引导提示符（这是默认设置）。如果 flag_val 为 1，则始终显示引导提示符。

F2 *filename*
F1 *filename*
...etc...
F9 *filename*
F10 *filename*

当在引导提示符下按下功能键时，将显示指定的文件。这可以用于执行预引导联机帮助（大致是关于内核命令行选项）。为了向后兼容先前的发行版，F10 也可以输入为 F0。请注意目前尚无法将文件名与 F11 和 F12 绑定。

4.3.5 准备目标系统的 PXE 引导

请将 PXE 选项包含在 BIOS 引导序列中来为系统 BIOS 的 PXE 引导作准备。

警告: BIOS 引导顺序

在 BIOS 中，不要将 PXE 选项置于硬盘引导选项的前面。否则，在每次引导该系统时，它都会尝试重安装自己。

4.3.6 准备目标系统的网络唤醒

网络唤醒 (WOL) 要求在安装之前启用相应的 BIOS 选项。此外，请记住目标系统的 MAC 地址。该数据是启动网络唤醒所需要的。

4.3.7 局域网唤醒

“网络唤醒”允许通过一个发送时包含计算机 MAC 地址的特定网络包来打开该计算机的电源。由于全球的每台机器都有一个唯一的 MAC 标识，所以无需担心会意外地错开机器的电源。

重要: 不同网段的“网络唤醒”

如果控制机器与要唤醒的安装目标不在同一网段，请将要发送的 WOL 请求配置为多点广播，或远程控制该网段上的某台机器充当这些请求的发送方。

SUSE Linux Enterprise Server 9 及更高版本的用户可以使用名为 WOL 的 YaST 模块来方便地配置“网络唤醒”。基于 SUSE Linux 操作系统的其他版本的用户可以使用命令行工具。

4.3.8 使用 YaST 的“网络唤醒”

- 1 以 root 身份登录。
- 2 启动 *YaST* > 网络服务 > WOL。
- 3 单击添加并输入目标系统的主机名和 MAC 地址。

- 4 要打开此计算机，请选择适当的输入框并单击唤醒。

4.3.9 手动进行网络唤醒

- 1 以 root 身份登录。
- 2 启动 *YaST* > 软件管理，然后安装包 `netdiag`。
- 3 打开一个终端，然后以 root 身份输入以下命令来唤醒目标：

```
ether-wake mac_of_target
```

请将 `mac_of_target` 替换为目标机器的实际 MAC 地址。

4.4 引导用于安装的目标系统

除了在第 4.3.7 节“局域网唤醒”[62]和第 4.3.3 节“使用 PXE 引导”[57]中提到的那些方法之外，主要有两种方法来自定义用于安装的引导过程。您既可以使用默认的引导选项和功能键，也可以使用安装引导屏幕上的引导选项提示来指定安装内核对该特定硬件可能需要的任何引导选项。

4.4.1 使用默认的引导选项

引导选项在第 3 章 *使用 YaST 进行安装* [17]中有详细描述。通常，只需选择安装即可开始安装引导过程。

如果发生问题，请使用安装 — 禁用 *ACPI* 或安装 — 安全设置。有关安装过程故障诊断的更多信息，请参见第 46.2 节“安装问题”[725]。

4.4.2 使用 F 键

屏幕底部的菜单栏提供了某些安装中所需的几项高级功能。使用 F 键可以指定其他选项传递到安装路由，而不需要了解这些参数（参见第 4.4.3 节“使用自定义引导选项”[65]）的详细语法。

请查看下表以了解所有的可用选项。要访问可用的整个组的 F 键，请先按 F3。

表 4.1 安装期间的 F 键

键	目的	可用选项	默认值
F1	提供帮助	无	无
F2	选择安装语言	所有支持的语言	英语
F3	更改安装屏幕分辨率	<ul style="list-style-type: none">• 文本方式• VESA• 分辨率 #1• 分辨率 #2• ...	<ul style="list-style-type: none">• 默认值取决于您的图形硬件
F4	选择安装源	<ul style="list-style-type: none">• CD-ROM 或 DVD• SLP• FTP• HTTP• NFS• SMB• 硬盘	CD-ROM 或 DVD
F5	应用驱动程序更新磁盘	驱动程序	无

4.4.3 使用自定义引导选项

使用合适的引导选项将帮助简化安装过程。许多参数也可以在以后使用 `linuxrc` 例程进行配置，但是使用引导选项则更方便。在一些自动安装中，引导选项可通过 `initrd` 或 `info` 文件提供。

下表列出了本章中提到的所有安装方案及其所需的引导参数和对应的引导选项。完全按它们在该表中出现的顺序予以全部追加，可获取一个引导选项字符串，该字符串将交给安装例程。例如（全部在一行上）：

```
install=... netdevice=... hostip=...netmask=... vnc=... vncpassword=...
```

将该字符串中的所有值 (...) 替换为适用于您安装的值。

表 4.2 本章中使用的安装（引导）方案

安装方案	引导时所需的参数	引导选项
第 3 章 使用 <i>YaST</i> 进行安装 [17]	无：系统自动引导	不需要任何选项
第 4.1.1 节 “通过 VNC 静态网络配置进行简单远程安装” [38]	<ul style="list-style-type: none">• 安装服务器的位置• 网络设备• IP 地址• 网络掩码• 网关• VNC 支持• VNC 密码	<ul style="list-style-type: none">• <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code>• <code>netdevice=some_netdevice</code>(仅当有多个网络设备可用时才需要)• <code>hostip=some_ip</code>• <code>netmask=some_netmask</code>• <code>gateway=ip_gateway</code>• <code>vnc=1</code>• <code>vncpassword=some_password</code>

安装方案	引导时所需的参数	引导选项
第 4.1.2 节 “通过 VNC 动态网络配置进行简单远程安装” [39]	<ul style="list-style-type: none"> • 安装服务器的位置 • VNC 支持 • VNC 密码 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code> • <code>vnc=1</code> • <code>vncpassword=some_password</code>
第 4.1.3 节 “通过 VNC—PXE Boot 和“网络唤醒”进行远程安装” [40]	<ul style="list-style-type: none"> • 安装服务器的位置 • TFTP 服务器的位置 • VNC 支持 • VNC 密码 	不适用；进程通过 PXE 和 DHCP 管理
第 4.1.4 节 “通过 SSH 静态网络配置进行简单远程安装” [41]	<ul style="list-style-type: none"> • 安装服务器的位置 • 网络设备 • IP 地址 • 网络掩码 • 网关 • SSH 支持 • SSH 密码 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code> • <code>netdevice=some_netdevice</code>(仅当有多个网络设备可用时才需要) • <code>hostip=some_ip</code> • <code>netmask=some_netmask</code> • <code>gateway=ip_gateway</code> • <code>usessh=1</code> • <code>sshpassword=some_password</code>
第 4.1.5 节 “通过 SSH 动态网络配置进行简单远程安装” [43]	<ul style="list-style-type: none"> • 安装服务器的位置 • SSH 支持 • SSH 密码 	<ul style="list-style-type: none"> • <code>install=(nfs,http,ftp,smb):///path_to_instmedia</code> • <code>usessh=1</code>

安装方案	引导时所需的参数	引导选项
		<ul style="list-style-type: none">• <code>sshpassword=some_password</code>
第 4.1.6 节 “通过 SSH—PXE Boot 和“网络唤醒”进行远程安装” [44]	<ul style="list-style-type: none">• 安装服务器的位置• TFTP 服务器的位置• SSH 支持• SSH 密码	不适用；进程通过 PXE 和 DHCP 管理

提示: 有关 **linuxrc** 引导选项的更多信息

在 `/usr/share/doc/packages/linuxrc/linuxrc.html` 中可找到更多用于引导 Linux 系统的 **linuxrc** 引导选项的信息。

4.5 监视安装过程

有多个用于远程监视安装过程的选项。如果在引导安装时已指定了正确的引导选项，则可以使用 VNC 或 SSH 从远程工作站控制安装和系统配置。

4.5.1 VNC 安装

您可以使用任意 VNC 查看器软件从几乎所有的操作系统远程控制 SUSE Linux Enterprise 的安装。本节介绍如何使用 VNC 查看器应用程序或万维网浏览器进行安装。

准备进行 VNC 安装

在准备 VNC 安装时，只需要为安装目标指定合适的引导选项供初始安装引导过程使用即可。（请参见第 4.4.3 节 “使用自定义引导选项” [65]）。目标系统引导后进入一个基于文本的环境中，并等待 VNC 客户机连接到安装程序。

安装程序就 IP 地址发布通告，并显示需要连接用于安装的编号。如果您具有对目标系统的物理访问权，该信息将在系统完成安装引导后立即显示。在 VNC 客户端软件出现提示时，请输入该数据，并输入 VNC 密码。

因为安装目标通过 OpenSLP 发布自身通告，所以您可以通过 SLP 浏览器检索安装目标的地址信息，而无需通过物理方式连接到安装程序本身（只要您的网络设置和所有机器都支持 OpenSLP）：

- 1 启动 KDE 文件和 Web 浏览器 Konqueror。
- 2 在位置栏中输入 `service://yast.installation.suse`。随后目标系统将在 Konqueror 屏幕中显示为一个图标。单击该图标启动 KDE VNC 查看器，在其中可以执行安装。或者，使用提供的 IP 地址运行 VNC 查看器软件，并在 IP 地址的末尾添加 `:1` 以显示安装正在运行。

连接到安装程序

主要有两种方法可连接到 VNC 服务器（本例中为安装目标）。您既可以在任意操作系统上启动单独的 VNC 查看器应用程序，也可以使用支持 Java 的 Web 浏览器进行连接。

您可以使用 VNC 从任意其他操作系统（包括其他 Linux flavors、Windows 或 Mac OS）控制 Linux 系统的安装。

请确保在 Linux 计算机上已安装了 `tightvnc` 包。在 Windows 机器上，请安装此应用程序的 Windows 端口，它可在 TightVNC 主页上获取（<http://www.tightvnc.com/download.html>）。

要连接到目标机器上运行的安装程序，请执行如下操作：

- 1 启动 VNC 查看器。
- 2 输入由 SLP 浏览器或安装程序自身提供的安装目标的 IP 地址和显示编号。

ip_address:display_number

随后会在桌面上打开一个窗口，其中显示的 YaST 屏幕与正常本地安装中所显示的相同。

使用万维网浏览器连接到安装程序，将使您完全不必依赖任何 VNC 软件或底层操作系统。只要浏览器应用程序启用了 Java 支持，就可以使用任意浏览器

（Firefox、Internet Explorer、Konqueror、Opera 等等）来执行 Linux 系统的安装。

要执行 VNC 安装，请执行如下操作：

- 1 启动首选的万维网浏览器。

- 2 在地址栏中输入以下内容：

```
http://ip_address_of_target:5801
```

- 3 在看到输入 VNC 密码的提示时输入此密码。浏览器窗口此刻显示的 YaST 屏幕与正常本地安装中所显示的相同。

4.5.2 SSH 安装

通过使用 SSH，您可以使用任意 SSH 客户端软件远程控制 Linux 机器的安装。

准备进行 SSH 安装

除了安装相应的软件包（用于 Linux 的 OpenSSH 和用于 Windows 的 PuTTY），您只需指定相应的引导选项来为安装启用 SSH。有关细节，请参见[第 4.4.3 节“使用自定义引导选项”](#) [65]。默认情况下，OpenSSH 安装在所有基于 SUSE Linux 的操作系统上。

连接到安装程序

- 1 检索安装目标的 IP 地址。如果您具有对目标计算机的物理访问权，就请采用初始引导后安装例程显示在控制台上的 IP 地址。否则，请采用 DHCP 服务器配置中分配给此特定主机的 IP 地址。

- 2 在命令行中输入以下命令：

```
ssh -X root@ip_address_of_target
```

将 `ip_address_of_target` 替换为安装目标的实际 IP 地址。

- 3 在看到输入用户名的提示时，输入 `root`。

- 4 在系统提示输入密码时，输入已通过 SSH 引导选项设置的密码。在成功通过鉴定之后，将出现一个安装目标的命令行提示符。
- 5 输入 `yast` 起动安装程序。将打开一个窗口，其中显示如第3章 *使用 YaST 进行安装* [17]中所述的正常 YaST 屏幕。

自动安装

AutoYaST 使您可以在许多计算机上并行安装 SUSE® Linux Enterprise。AutoYaST 技术在使部署适应异构硬件方面具有很大灵活性。本章讲述如何准备简单的自动安装并勾勒出包含不同硬件类型和安装目的的高级方案。

5.1 简单的大规模安装

重要：相同硬件

该方案假设您正在使用完全相同的硬件配置向一组计算机批量部署 SUSE Linux Enterprise。

要准备 AutoYaST 大规模安装，请执行以下操作：

- 1 如第 5.1.1 节 “创建 AutoYaST 配置文件” [72] 中所述创建 AutoYaST 配置文件，该配置文件包含您的部署所需的安装细节。
- 2 如第 5.1.2 节 “分发配置文件并确定 `autoyast` 参数” [73] 中所述，确定 AutoYaST 配置文件的来源以及要传递到安装例程的参数。
- 3 如第 5.1.3 节 “提供安装数据” [76] 所述确定 SUSE Linux Enterprise 安装数据源。
- 4 如第 5.1.4 节 “设置引导方案” [76] 中所述确定并设置自动安装引导方案。

- 5 如第 5.1.5 节“创建 info 文件”[78]所述，通过手动添加参数或创建 info 文件，将命令行传递到安装例程。
- 6 如第 5.1.6 节“启动并监视自动安装”[81]中所述，启动自动安装进程。

5.1.1 创建 AutoYaST 配置文件

AutoYaST 配置文件告诉 AutoYaST 安装的内容以及如何配置已安装系统以最终获得完整的现成系统。可以用几种不同方式创建：

- 从参照计算机将新安装复制到一组相同的计算机
- 使用 AutoYaST GUI 创建并修改配置文件，使其符合您的要求
- 使用 XML 编辑器，从头开始创建配置文件

要复制新的参照安装，请执行以下操作：

- 1 执行正常安装。
- 2 完成硬件配置并阅读发行说明后，如果默认情况下尚未选中复制 *AutoYaST* 安装文件，则选中它。这样就创建了 `/root/autoinst.xml` 现成配置文件，可以用于创建此特定安装的副本。

要使用 AutoYaST GUI 从现有的系统配置创建配置文件并对其进行符合您的需要的修改，请执行以下操作：

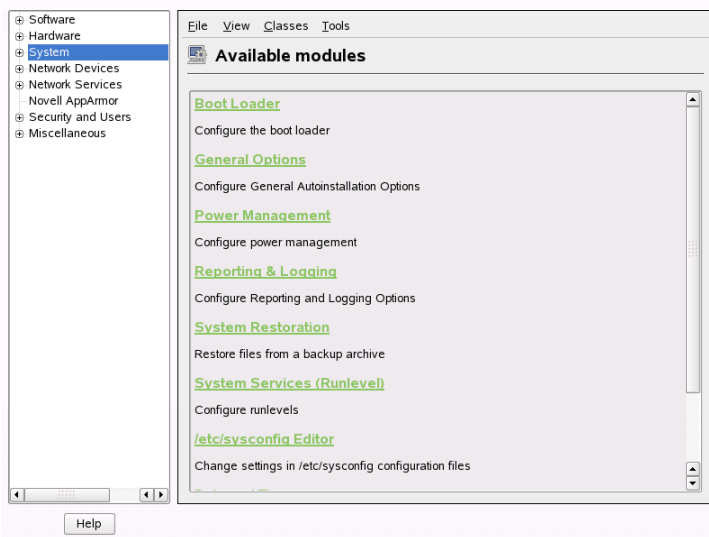
- 1 作为 `root` 启动 YaST。
- 2 选择 *其他 > 自动安装* 来启动图形 AutoYaST 前端。
- 3 选择 *工具 > 创建参照控制文件* 以准备 AutoYaST，将当前系统配置镜像到 AutoYaST 配置文件。
- 4 除了默认资源（如引导加载程序、分区和软件选择）之外，可以通过查看 *创建参照控制文件* 列表内的项目，将系统的各种其他方面添加到配置文件。
- 5 单击 *创建* 使 YaST 收集所有系统信息并将其写到新配置文件。

6 要继续，请选择下列操作之一：

- 如果配置文件完整且符合您的要求，请选择文件 > 另存为并输入配置文件的名称（如 `autoinst.xml`）。
- 从树视图向左选择适当的配置内容（如“硬件/打印机”）并单击配置来修改参照配置文件。相应的 YaST 模块启动，但您的设置被写入 AutoYaST 配置文件而不是应用到系统。完成之后，选择文件 > 另存为并输入适当的配置文件名。

7 使用文件 > 退出退出 AutoYaST 模块。

图 5.1 使用 AutoYaST 前端编辑 AutoYaST 配置文件



5.1.2 分发配置文件并确定 `autoyast` 参数

AutoYaST 配置文件可以以几种不同的方式分发。根据分发配置文件数据所用的协议，不同的 AutoYaST 参数用来将配置文件的位置告知客户机上的安装例程。配置文件的位置可以通过引导提示或引导后装载的 `info` 文件传递到安装例程。下列选项可用：

配置文件位置	参数	说明
文件	autoyast=file:///路径	使安装例程在指定路径中（如果是在 CD-ROM 顶级目录中，则为源根目录的相对路径 — file:///autoinst.xml）查找控制文件。
设备	autoyast=device:///路径	使安装例程在储存设备上查找该控制文件。只需要设备名 — 如果 /dev/sda1 是错误的，则使用 sda1。
软盘	autoyast=floppy:///路径	使安装例程查找软盘驱动器中软盘上的控制文件。如果想从 CD-ROM 引导，此选项特别有用。 如果无法从软盘获取控制文件，AutoYaST 会自动扫描计算机上连接的所有 USB 设备。
USB（闪存）磁盘	autoyast=usb:///路径	此选项触发搜索 USB 连接设备上的控制文件的操作。
NFS	autoyast=nfs:///服务器/路径	使安装路由从 NFS 服务器上检索控制文件。
HTTP	autoyast=http:///服务器/路径	使安装例程从 HTTP 服务器上检索控制文件。
HTTPS	autoyast=https:///服务器/路径	使安装例程从 HTTPS 服务器上检索控制文件。
TFTP	autoyast=tftp:///服务器/路径	使安装例程从 TFTP 服务器上检索控制文件。
FTP	autoyast=ftp:///服务器/路径	使安装例程从 FTP 服务器上检索控制文件。

用与实际安装匹配的值来替代服务器和路径。

AutoYaST 包含一项功能，可以使某些配置文件绑定到客户机的 MAC 地址。无需改变 `autoyast=` 参数就可以同一安装过程使用不同配置文件安装不同的实例。

要使用此功能，请执行以下操作：

- 1 使用客户机的 MAC 地址作为文件名来创建不同配置文件，并将其放置到 HTTP 服务器来存放您的 AutoYaST 配置文件。

- 2 在创建 `autoyast=` 参数时，删除包括文件名在内的实际路径，例如：

```
autoyast=http://192.0.2.91/
```

- 3 启动自动安装。

YaST 尝试以下列方式确定配置文件位置：

1. YaST 使用自身的 IP 地址（以大写十六进制的形式）搜索配置文件，例如，192.0.2.91 是 C000025B。
2. 如果找不到该文件，YaST 将去除一位十六进制数字并重试。这种做法将重复 8 次，直至找到具有正确文件名的文件。
3. 如果仍然不成功，它将尝试用客户机的 MAC 地址作为文件名来查找文件。例如，客户机的 MAC 地址是 0080C8F6484C。
4. 如果以 MAC 地址命名的文件没有找到，YaST 将搜索名为 `default`（小写）的文件。YaST 用以搜索 AutoYaST 配置文件的示例地址顺序如下：

```
C000025B
C000025
C00002
C0000
C000
C00
C0
C
0080C8F6484C
default
```

5.1.3 提供安装数据

安装数据以产品 CD 或 DVD 方式提供或使用网络安装源提供。如果将产品 CD 用作安装源，则需要对客户机进行物理访问来完成安装，因为引导进程需要手动启动，CD 需要更换。

要提供网络上的安装源，请如第 4.2.1 节“使用 YaST 设置安装服务器”[45]所述设置网络安装服务器（HTTP、NFS、FTP）。使用 info 文件将服务器位置传递到安装例程。

5.1.4 设置引导方案

客户机可以用以下几种不同的方式引导：

网络引导

关于常规远程安装，可以使用“网络唤醒”和 PXE 启动自动安装，通过 TFTP 导入引导映像和控制文件并从任意网络安装服务器选择安装源。

可引导 CD-ROM

可以使用原始 SUSE Linux Enterprise 媒体引导系统进行自动安装并从网络位置或软盘导入控制文件。或者，创建自定义 CD-ROM，存放安装源和 AutoYaST 配置文件。

以下几节简要叙述网络引导或 CD-ROM 引导的基本程序。

准备网络引导

中讨论了如何使用“网络唤醒”、PXE 和 TFTP 进行网络引导。第 4.1.3 节“通过 VNC—PXE Boot 和“网络唤醒”进行远程安装”[40] 要使用已介绍的步骤进行自动安装，请修改起重要作用的 PXE Linux 配置文件 (/srv/tftp/pxelinux.cfg/default)，以使其包含指向 AutoYaST 配置文件位置的 autoyast 参数。标准安装的示例项如下：

```
default linux

# default label linux
kernel linux append initrd=initrd ramdisk_size=65536 insmod=e100 \
install=http://192.168.0.22/install/suse-enterprise/
```


自动安装的相同示例如下：

```
default linux

# default label linux
kernel linux append initrd=initrd ramdisk_size=65536 insmod=e100 \
install=http://192.168.0.22/install/suse-enterprise/ \
autoyast=nfs://192.168.0.23/profiles/autoinst.xml
```

用安装中使用的数据替代示例 IP 地址和路径。

准备从 CD-ROM 引导

AutoYaST 安装中可以使用几种从 CD-ROM 引导的方法。请从下列方案中选择：

从 SUSE Linux Enterprise 媒体引导，通过网络获取配置文件

如果完全基于网络的方案不可能执行（例如，如果硬件不支持 PXE），则使用此方法，您可以对在几乎整个过程中安装的系统进行物理访问。

需要对包含每：

- SUSE Linux Enterprise 媒体
- 提供配置文件数据的网络服务器（详见第 5.1.2 节“分发配置文件并确定 autoyast 参数” [73]）
- 包含 info 文件的软盘，以告知安装例程在哪里找到配置文件

或

访问系统引导提示，以便在手动输入 autoyast= 参数的地方进行安装

从 SUSE Linux Enterprise 媒体引导并安装，从软盘获取配置文件

如果完全基于网络的安装方案不起作用，则使用此方法。它要求对要安装的系统进行物理访问以打开目标计算机，或者，在第二种情况下，按照引导提示输入配置文件位置。无论哪种情况都可能需要根据安装范围更改媒体。

需要对包含每：

- SUSE Linux Enterprise 媒体

- 存放配置文件和 info 文件的软盘

或

访问目标的引导提示以输入 `autoyast= 参数`

从自定义媒体引导并安装，从媒体获取配置文件

如果需要安装有限数量的软件包且目标数量相对较低，则要考虑创建自定义 CD，以存放安装数据和配置文件（尤其是在安装中没有网络可用的情况下）。

5.1.5 创建 info 文件

针对目标的安装例程需要清楚 AutoYaST 框架的不同组件。这要通过创建命令行来完成，命令行包含查找 AutoYaST 组件、安装源所需要的所有参数以及控制安装进程所需要的参数。

这要通过根据安装引导提示手动传递这些参数来进行，或者通过提供由安装例程 (`linuxrc`) 读取的名为 `info` 的文件来进行。前者要求对任何要安装的客户机进行物理访问，这便使得这种方法不适合于大规模部署。后者使您能够提供一些媒体上的 `info` 文件，该文件要在自动安装前准备好并插入客户机驱动器。或者，如“[准备网络引导](#)”一节 [76]所示使用 PXE 引导并将 `linuxrc` 参数包括在 `pxelinux.cfg/default` 文件中。

下列参数一般用于 `linuxrc`。如果需要更多信息，请参阅 `/usr/share/doc/packages/autoyast` 下的 AutoYaST 包文档。

重要: 分隔参数和值

当根据引导提示向 `linuxrc` 传递参数时，请使用 `=` 分隔参数和值。当使用 `info` 文件时，请使用 `:` 分隔参数和值。

关键字	值
<code>netdevice</code>	网络安装所使用的网络设备（根据 BOOTP/DHCP 的请求）。仅在几个网络设备可用的条件下需要。

关键字	值
hostip	如果是空的，客户机将发送 BOOTP 请求。否则，客户机将使用指定数据进行配置。
netmask	网络掩码。
网关	网关。
nameserver	名称服务器。
autoyast	自动安装所使用的控制文件的位置，如 autoyast=http://192.168.2.1/profiles/。
install	安装源的位置，如 install=nfs://192.168.2.1/CDs/。
vnc	如果设置为 1，则启用 VNC 远程控制安装。
vncpassword	VNC 密码。
usessh	如果设置为 1，则启用 SSH 远程控制安装。

如果自动安装方案包含 DHCP 客户机配置和网络安装源，而且您想使用 VNC 监视安装过程，则 info 如下所示：

```
autoyast:profile_source install:install_source vnc:1 vncpassword:some_password
```

如果要在安装时间使用静态网络安装，则 info 文件将如下所示：

```
autoyast:profile_source \  
install:install_source \  
hostip:some_ip \  
netmask:some_netmask \  
gateway:some_gateway
```

\ 表示添加换行符是为了保证可读性。所有的选项必须作为一个连续的字符串输入。

info 数据可以几种不同的方式用于 linuxrc：

- 作为软盘根目录内的文件，该软盘在安装时应是客户机软盘驱动器内。
- 作为初始 RAM 磁盘的根目录内的文件，该磁盘用于引导来自自定义安装媒体的系统或通过 PXE 引导的系统。
- 作为 AutoYaST 配置文件的组成部分。在这种情况下，AutoYaST 文件需要被命名为 `info` 来使 `linuxrc` 对其进行语法分析。以下是该方法的示例。

`linuxrc` 在配置文件中寻找字符串 (`start_linuxrc_conf`)，该字符串表示文件的开始。如果找到，它将从该字符串开始对该内容进行语法分析并在找到字符串 `end_linuxrc_conf` 时完成。这些选项以如下方式储存在配置文件中：

```
....
<install>
....
    <init>
        <info_file>
<![CDATA[
#
# Don't remove the following line:
# start_linuxrc_conf
#
install: nfs:server/path
vnc: 1
vncpassword: test
autoyast: file:///info

# end_linuxrc_conf
# Do not remove the above comment
#
]]>

        </info_file>
    </init>
.....
</install>
....
```

`linuxrc` 装载包含引导参数的配置文件而非传统的 `info` 文件。`install:` 参数指向安装源的位置。`vnc` 和 `vncpassword` 指示将 VNC 用于安装监视。`autoyast` 参数告诉 `linuxrc` 将 `info` 视作 AutoYaST 配置文件。

5.1.6 启动并监视自动安装

在提供了上述所有基础设施（配置文件、安装源和 `info` 文件）之后，可以继续启动自动安装。根据引导和监视进程的所选方案，可能需要与客户机进行物理交互：

- 如果客户机系统从任何一种物理媒体（产品媒体或自定义 CD）进行引导，需要将这些媒体插入客户机驱动器内。
- 如果客户机不是通过“网络唤醒”打开的，至少需要打开客户机。
- 如果没有选择远程控制自动安装，来自 AutoYaST 的图形反馈则要发送到客户机附带监视器，或者，如果使用无外设客户机，则发送到串行控制台。

要启用远程控制自动安装，请如第 5.1.5 节“创建 `info` 文件”[78]中所述使用 VNC 或 SSH 参数，并如第 4.5 节“监视安装过程”[67]所述，从另一台计算机连接到客户机。

5.2 基于规则的自动安装

以下几节讲述使用 AutoYaST 的基于规则安装的基本概念并提供示例方案，使您能够创建自定义自动安装。

5.2.1 了解基于规则的自动安装

基于规则的 AutoYaST 安装使您能够处理异构硬件环境：

- 您的站点包含不同供应商的硬件吗？
- 计算机是在您不同硬件配置的站点上吗（例如，使用不同设备或使用大小不同的内存和磁盘）？
- 您要通过横跨不同的域进行安装并需要区分这些域吗？

基于规则的自动安装所做的基本上是通过把几个配置文件合成一个而生成自定义配置文件以匹配异构方案。每个规则描述一个特定的安装功能（例如磁盘大小）并告诉 AutoYaST 当规则匹配时使用哪个配置文件。描述不同安装功能的几个规则都组合到一个 AutoYaST `rules.xml` 文件中。然后规则堆栈将被处

理，AutoYaST 通过把可以匹配 AutoYaST 规则的不同配置文件合成为一个来生成最后的配置文件。有关该过程的示例，请参阅第 5.2.2 节“基于规则自动安装的示例方案” [83]。

基于规则的 AutoYaST 在计划和执行 SUSE Linux Enterprise 部署方面具有很大的灵活性。您可以执行以下操作：

- 创建规则来匹配 AutoYaST 中的任何预定义系统特性
- 使用逻辑操作器将多个系统特性（如磁盘大小和内核体系结构）组合成一个规则
- 通过运行 shell 脚本并将其输出传递到 AutoYaST 框架来创建自定义规则。自定义规则的数量限于 5 个。

注意

有关 AutoYaST 规则创建和使用方法的更多信息，请参阅规则和类别一章 `/usr/share/doc/packages/autoyast2/html/index.html` 下的包文档。

要准备基于规则的 AutoYaST 大规模安装，请执行以下操作：

- 1 创建几个 AutoYaST 配置文件，这些配置文件包含第 5.1.1 节“创建 AutoYaST 配置文件” [72]中描述的异构安装所需的安装细节。
- 2 定义规则以匹配第 5.2.2 节“基于规则自动安装的示例方案” [83]中所显示的硬件安装的系统特性。
- 3 如第 5.1.2 节“分发配置文件并确定 autoyast 参数” [73]中所述，确定 AutoYaST 配置文件的来源以及要传递到安装例程的参数。
- 4 如第 5.1.3 节“提供安装数据” [76]所述确定 SUSE Linux Enterprise 安装数据源。
- 5 如第 5.1.5 节“创建 info 文件” [78]所述，通过手动添加参数或创建 info 文件，将命令行传递到安装例程。
- 6 如第 5.1.4 节“设置引导方案” [76]中所述确定并设置自动安装引导方案。
- 7 如第 5.1.6 节“启动并监视自动安装” [81]中所述，启动自动安装进程。

5.2.2 基于规则自动安装的示例方案

要基本了解如何创建规则，请考虑图 5.2 “AutoYaST 规则” [84]中描述的如下示例。一次性 AutoYaST 安装下列设置：

打印服务器

计算机只需要无桌面环境的最小化安装和一套有限的软件包。

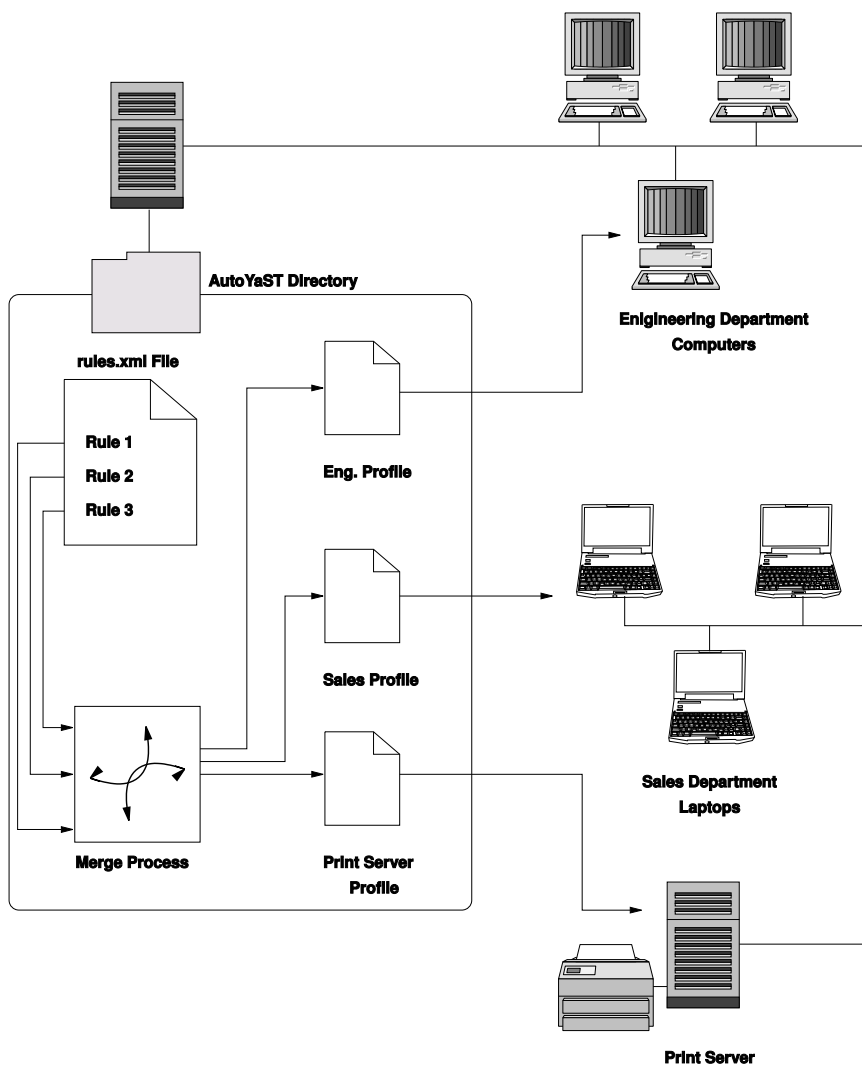
工程设计部的工作站

这些计算机需要桌面环境和一整套开发软件。

销售部的笔记本电脑

这些计算机需要桌面环境和一套有限的专用应用程序（如办公和日历软件）。

图 5.2 AutoYaST 规则



在第一步中，请使用第 5.1.1 节“创建 AutoYaST 配置文件”[72]中所述的方法之一来为每次使用情况创建配置文件。在本例中，您将创建 `print.xml`、`engineering.xml` 和 `sales.xml`。

在第二步中，请创建规则来区分三种硬件类型并且告诉 AutoYaST 使用哪个配置文件。使用类似于下列方法的算法来设置规则：

1. 该计算机有 192.168.27.11 的 IP 地址吗？然后将其设为打印服务器。
2. 该计算机拥有 PCMCIA 硬件和 Intel 芯片组吗？然后将其视为 Intel 笔记本电脑并安装销售部软件选择。
3. 如果以上均不正确，则将该计算机视为开发人员工作站并进行相应的安装。

大致上，这可以转换为具有下列内容的 rules.xml 文件：

```
<?xml version="1.0"?>
<!DOCTYPE autoinstall SYSTEM "/usr/share/autoinstall/dtd/rules.dtd">
<autoinstall xmlns="http://www.suse.com/1.0/yast2ns"
xmlns:config="http://www.suse.com/1.0/configns">
  <rules config:type="list">
    <rule>
      <hostaddress>
        <match>192.168.27.11</match>
        <match_type>exact</match_type>
      </hostaddress>
      <result>
        <profile>print.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
    </rule>
    <rule>
      <haspcmcia>
        <match>1</match>
        <match_type>exact</match_type>
      </haspcmcia>
      <custom1>
        <script>
if grep -i intel /proc/cpuinfo > /dev/null; then
echo -n "intel"
else
echo -n "non_intel"
fi;
          </script>
        <match>*</match>
        <match_type>exact</match_type>
      </custom1>
      <result>
        <profile>sales.xml</profile>
        <continue config:type="boolean">>false</continue>
      </result>
      <operator>and</operator>
    </rule>
```

```

<rule>
  <haspcmcia>
    <match>0</match>
    <match_type>exact</match_type>
  </haspcmcia>
</result>
  <profile>engineering.xml</profile>
  <continue config:type="boolean">false</continue>
</result>
</rule>
</rules>
</autoinstall>

```

当分发规则文件时，请确保 `rules` 目录位于 `autoyast=protocol:serverip/profiles/URL` 指定的 `profiles` 下。AutoYaST 首先寻找包含文件名为 `rules.xml` 的 `rules` 子目录，然后装载并且合并规则文件中指定的配置文件。

剩余的自动安装程序像往常一样进行。

5.3 有关详细信息

有关 AutoYaST 技术的更详细的信息，请参阅随软件安装的文档。它位于 `/usr/share/doc/packages/autoyast2` 下。该文档的最新版本可以在 http://www.suse.de/~ug/autoyast_doc/index.html 找到。

部署自定义预安装

将自定义 SUSE Linux Enterprise 预安装到大量相同的计算机上，使您不必在每一台上单独安装，并使最终用户感到安装是标准化的。使用 YaST firstboot 创建自定义预安装映像，并确定涉及最终用户交互的最终个性化步骤的工作流程。这与允许完全自动化安装的 AutoYaST 不同；有关更多信息，请参见第 5 章 *自动安装* [71]。

创建自定义安装、部署到硬件及使最终产品个性化包括以下步骤：

- 1 准备磁盘要复制到客户机的主计算机。有关更多信息，请参考第 6.1 节 *“准备主计算机”* [88]。
- 2 自定义 firstboot 工作流程。有关更多信息，请参考第 6.2 节 *“自定义 Firstboot 安装”* [88]。
- 3 复制主计算机磁盘，将映像转到客户机磁盘上。有关更多信息，请参考第 6.3 节 *“复制主安装”* [96]。
- 4 让最终用户个性化 SUSE Linux Enterprise 的实例。有关更多信息，请参考第 6.4 节 *“个性化安装”* [96]。

6.1 准备主计算机

为 firstboot 工作流程准备主计算机，请按以下步骤操作：

- 1 将安装媒体插入主计算机中。
- 2 引导计算机。
- 3 执行包含所有必要配置步骤的正常安装，等待安装好的计算机进行引导。同时安装 `yast2-firstboot` 包。
- 4 要定义自己的最终用户 YaST 配置步骤工作流程，或将自己的 YaST 模块添加到该工作流程，请转到第 6.2 节“自定义 Firstboot 安装”[88]。否则的话，直接转到步骤 5 [88]。
- 5 以 `root` 启用 firstboot:
 - 5a 创建空文件 `/etc/reconfig_system` 触发 firstboot 的执行。成功完成 firstboot 配置后，该文件将被删除。用以下命令创建该文件：

```
touch /etc/reconfig_system
```
 - 5b 通过 YaST 运行级别编辑器启用 firstboot 服务。
- 6 转到第 6.3 节“复制主安装”[96]。

6.2 自定义 Firstboot 安装

自定义 firstboot 安装可能涉及若干不同组件。对它们的自定义是可选的。如果不做任何更改，firstboot 会用默认设置执行安装。下列选项可用：

- 按第 6.2.1 节“自定义 YaST 讯息”[89]中所述自定义最终用户收到的讯息。
- 按第 6.2.2 节“自定义许可证操作”[90]中所述自定义许可证和许可证操作。
- 按第 6.2.3 节“自定义发行说明”[90]中所述自定义要显示的发行说明。

- 如第 6.2.4 节“自定义工作流程” [91]中所述，自定义安装中涉及的组件的顺序和编号。
- 如第 6.2.5 节“配置其他脚本” [96]中所述配置其他可选脚本。

要自定义其中的任何组件，请调整以下配置文件：

`/etc/sysconfig/firstboot`

配置 `firstboot` 的不同方面，例如发行说明、脚本和许可证操作。

`/etc/YaST2/firstboot.xml`

通过启用或禁用组件或者添加自定义组件，配置安装工作流程。

6.2.1 自定义 YaST 讯息

默认情况下，SUSE Linux Enterprise 的安装包含几条默认讯息，它们会在安装过程的特定阶段被本地化并显示。这些讯息包括欢迎讯息、许可证讯息和安装结束时的祝贺讯息。您可以将其中任何讯息替换成自己的版本，并在安装中包含它们的本地化版本。要包含您自己的欢迎讯息，请按以下步骤继续：

- 1 作为 `root` 登录。
- 2 打开 `/etc/sysconfig/firstboot` 配置文件，并应用以下更改：
 - 2a 将 `FIRSTBOOT_WELCOME_DIR` 设置为希望存储包含欢迎讯息和本地化版本的文件的目录路径，例如：


```
FIRSTBOOT_WELCOME_DIR="/usr/share/firstboot/"
```
 - 2b 如果欢迎讯息的文件名不是 `welcome.txt` 和 `welcome_locale.txt`（其中，`locale` 与诸如“`cs`”或“`de`”的 ISO 639 语言代码相匹配），请在 `FIRSTBOOT_WELCOME_PATTERNS` 中指定文件名模式。例如：


```
FIRSTBOOT_WELCOME_PATTERNS="mywelcome.txt"
```

如未设置，将假定为默认值 `welcome.txt`。
- 3 创建欢迎文件和本地化版本，并将它们置于 `/etc/sysconfig/firstboot` 配置文件中指定的目录中。

按类似方法继续，配置自定义许可证并完成讯息。这些变量是 `FIRSTBOOT_LICENSE_DIR` 和 `FIRSTBOOT_FINISH_FILE`。

6.2.2 自定义许可证操作

您可以自定义安装系统对不接受许可证协议的用户所作出的反应。系统对用户未能接受许可证有三种不同的反应方式：

halt

`firstboot` 安装已中止，整个系统关闭。这是默认设置。

继续

`firstboot` 安装继续。

中止

`firstboot` 安装已中止，但系统尝试引导。

作出选择，将 `LICENSE_REFUSAL_ACTION` 设置为适当的值。

6.2.3 自定义发行说明

根据您是否更改了 SUSE Linux Enterprise 的实例，您可能需要让最终用户了解新操作系统的重要方面。标准安装用户发行说明，在安装的最后阶段之一显示，目的是为用户提供重要信息。要让您自己修改过的发行说明作为 `firstboot` 安装的一部分显示，请执行以下步骤：

- 1 创建您自己的发行说明文件。如 `/usr/share/doc/release-notes` 中的示例文件所示使用 **RTF** 格式，并将结果另存为 `RELEASE-NOTES.en.rtf`（英语）。
- 2 在原始版本附近存储本地化版本（可选），并将文件名中的 `en` 部分替换为实际 **ISO 639** 语言代码，如 `de`（德语）。
- 3 从 `/etc/sysconfig/firstboot` 打开 `firstboot` 配置文件，并将 `FIRSTBOOT_RELEASE_NOTES_PATH` 设置为保存发行说明文件的实际目录。

6.2.4 自定义工作流程

默认情况下，标准 firstboot 工作流程包含以下部分：

- 语言选择
- 欢迎
- 许可证协议
- 主机名
- 网络
- 时间和日期
- 桌面
- 根密码
- 用户鉴定方法
- 用户管理
- 硬件配置
- 完成安装

这一 firstboot 安装工作流程的标准布局不是必需的。您可以启用或禁用特定组件，或将您自己的模块挂接到工作流程中。要修改 firstboot 工作流程，请手动编辑 firstboot 配置文件 `/etc/YaST2/firstboot.xml`。该 XML 文件是标准 `control.xml` 文件的子集，YaST 使用该文件控制安装工作流程。

以下概述所提供的背景知识足够您用于修改 firstboot 安装工作流程。请在其中查看 firstboot 配置文件的基本语法，以及如何配置关键元素。

例 6.1 配置提议屏幕

```
...
<proposals config:type="list">❶
  <proposal>❷
    <name>firstboot_hardware</name>❸
    <mode>installation</mode>❹
    <stage>firstboot</stage>❺
    <label>Hardware Configuration</label>❻
    <proposal_modules config:type="list">❼
      <proposal_module>printer</proposal_module>❽
    </proposal_modules>
  </proposal>
</proposal>
...
</proposals>
```

- ❶ 所有提议的树枝都应是 firstboot 工作流程的一部分。
- ❷ 各条提议的树枝。
- ❸ 提议的内部名称。
- ❹ 该提议的方式。不要在此处作任何更改。对于 firstboot 安装，必须设置为安装。
- ❺ 调用此提议的安装过程阶段。不要在此处作任何更改。对于 firstboot 安装，必须设置为 firstboot。
- ❻ 提议上要显示的标签。
- ❼ 所有属于提议屏幕的模块的树枝。
- ❽ 属于提议屏幕的一个或多个模块。

firstboot 配置文件的下一部分由工作流程定义组成。此处必须列出应为 firstboot 安装工作流程一部分的所有模块。

例 6.2 配置工作流程部分

```
<workflows config:type="list">
  <workflow>
    <defaults>
      <enable_back>yes</enable_back>
      <enable_next>yes</enable_next>
      <archs>all</archs>
    </defaults>
    <stage>firstboot</stage>
    <label>Configuration</label>
    <mode>installation</mode>
    ... <!-- list of modules -->
  </modules>
</workflow>
</workflows>
...
```

工作流程部分的总体结构和提议部分很相似。树枝包含工作流程元素，工作流程元素都包括和例 6.1 “配置提议屏幕”[92]中所介绍的提议相同的阶段、标签和方式信息。最显著的差别是默认设置部分，它包含工作流程组件的基本设计信息：

enable_back

在所有对话框中包含上一步按钮。

enable_next

在所有对话框中包含下一步按钮。

archs

指定在其上使用该工作流程的硬件体系结构。

例 6.3 配置工作流程组件列表

```
<modules config:type="list">❶
  <module>❷
    <label>Language</label>❸
    <enabled config:type="boolean">false</enabled>❹
    <name>firstboot_language</name>❺
  </module>
</modules>
```

❶ 所有工作流程组件的树枝。

- ② 模块定义。
- ③ 随模块显示的标签。
- ④ 启用或禁用工作流程中该组件的开关。
- ⑤ 模块名称。模块本身必须位于 `/usr/share/YaST2/clients` 下，并具有文件后缀名 `.ycp`。

要更改 `firstboot` 安装过程中提议屏幕的编号或顺序，请按以下步骤操作：

- 1 在 `/etc/YaST2/firstboot.xml` 处打开 `firstboot` 配置文件。
- 2 删除或添加提议屏幕，或更改现有提议屏幕的顺序：
 - 要删除整个提议，请从提议部分删除提议元素（包括其所有子元素），并从工作流程删除单个模块元素（及子元素）。
 - 要添加新的提议，请创建新的提议元素，并填入所有必需的子元素。请确保提议作为 `/usr/share/YaST2/clients` 中的 `YaST` 模块存在。
 - 要更改提议的顺序，请在工作流程中前后移动包含提议屏幕的各个模块元素。请注意，与其他要求提议和工作流程组件有特定顺序的安装步骤间可能存在依赖关系。

- 3 应用更改并关闭配置文件。

默认设置不符合您的要求时，始终可以更改配置步骤的工作流程。启用或禁用工作流程中的特定模块，或添加您自己的自定义模块。

要切换 `firstboot` 工作流程中模块的状态，请按以下步骤操作：

- 1 打开 `/etc/YaST2/firstboot.xml` 配置文件。
- 2 将已启用元素的值从 `true` 改为 `false` 可禁用该模块，或从 `false` 改为 `true` 再次启用它。

```
<module>
  <label>Time and Date</label>
  <enabled config:type="boolean">true</enabled>
```

```
<name>firstboot_timezone</name>
</module>
```

3 应用更改并关闭配置文件。

要向工作流程添加自定义模块，请按以下步骤继续：

- 1 创建您自己的 YaST 模块，将模块文件 `module_name.ycp` 保存在 `/usr/share/YaST2/clients` 中。
- 2 打开 `/etc/YaST2/firstboot.xml` 配置文件。
- 3 确定您的新模块要在工作流程的哪一点运行。这样做时，请确保考虑到并已解决与工作流程中其他步骤之间可能存在的依赖性。
- 4 在模块树枝中创建新的模块元素，并添加相应的子元素：

```
<modules config:type="list">
...
  <module>
    <label>my_module</label>
    <enabled config:type="boolean">true</enabled>
    <name>filename_my_module</name>
  </module>
</modules>
```

4a 在标签元素中输入要在模块上显示的标签。

4b 请确保已启用已设置为 `true`，将您的模块包括在工作流程中。

4c 在名称元素中输入您模块的文件名。省略完整路径和 `.ycp` 后缀。

5 应用您的设置并关闭配置文件。

提示: 有关详细信息

关于 YaST 开发的更多信息，请参阅 <http://developer.novell.com/wiki/index.php/YaST>。

6.2.5 配置其他脚本

可配置 firstboot，使之在完成 firstboot 工作流程后执行其他脚本。要向 firstboot 序列添加其他脚本，请执行以下步骤：

- 1 打开 `/etc/sysconfig/firstboot` 配置文件，确保为 `SCRIPT_DIR` 指定的路径正确。默认值为 `/usr/share/firstboot/scripts`。
- 2 创建您的 shell 脚本，将它保存在指定的目录中，应用适当的文件许可权限。

6.3 复制主安装

用您可以获得的任何映像机制复制主计算机磁盘，将映像转到目标计算机。

6.4 个性化安装

引导已复制磁盘映像后，firstboot 会启动，安装会严格按第 6.2.4 节“自定义工作流程”[91]中的安排继续。只有 firstboot 工作流程配置中包含的组件会启动。任何其他安装步骤都将跳过。最终用户可调整语言、键盘、网络和密码设置，以个性化工作站。这一过程完成后，firstboot 已安装系统的行为就会像 SUSE Linux Enterprise 的任何其他实例一样。

高级磁盘设置

高级系统配置需要特定的磁盘设置。所有常用分区任务都可以用 YaST 完成。为实现块设备的统一设备命名，请使用 `/dev/disk/by-id/` 下的块设备。逻辑卷管理 (LVM) 是一种磁盘分区模式，旨在比标准设置中使用的物理分区更加灵活。它的快照功能方便了数据备份的创建。独立磁盘冗余阵列 (RAID) 提高了数据完整性、增强了性能和容错能力。

7.1 LVM 配置

本节简要介绍 LVM 的原理及其基本功能，这些功能使 LVM 在许多情况下都很有用。在 [第 7.1.2 节“用 YaST 配置 LVM”](#) [99] 中，将学习如何用 YaST 设置 LVM。

警告

使用 LVM 可能会增加一些风险，例如数据丢失。这些风险还包括应用程序崩溃、电源故障及有问题的命令。在实施 LVM 或重配置卷前，请保存数据。决不要在没有备份的情况下工作。

7.1.1 逻辑卷管理器

逻辑卷管理器 (LVM) 支持在多个文件系统上灵活分配硬盘空间。开发逻辑卷管理器是因为有时只有在安装过程中初始分区完成后才需要更改硬盘空间的分段。因为在运行的系统中修改分区比较困难，LVM 提供了内存空间的虚拟池（卷组，简称 VG），如果需要，可以从中生成逻辑卷 (LV)。操作系统访问这些逻

辑卷而不是物理分区。卷组可以跨多个磁盘，这样多个磁盘或部分磁盘可以构成一个 VG。LVM 以这种方式提供了一种对物理磁盘空间的抽象，从而能够以比物理分区更方便、更安全的方式更改硬盘空间的分段。和 [第 8.5.5 节“使用 YaST 分区程序”](#) [132] 中提供了有关物理分区的背景信息。“[分区类型](#)”一节 [133]

图 7.1 物理分区与 LVM

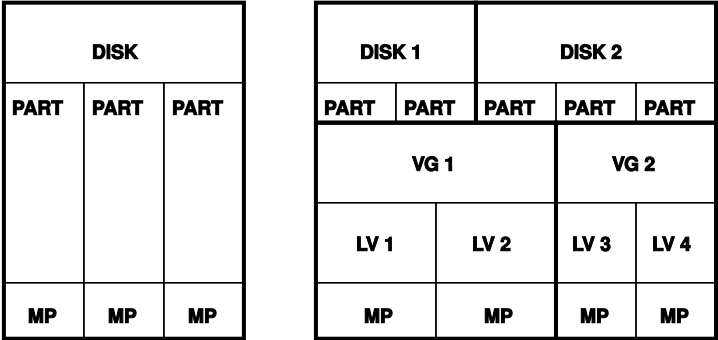


图 7.1 “物理分区与 LVM” [98]比较物理分区（左）和 lvm 分段（右）。在左侧，将一个磁盘分成 3 个物理分区 (PART)，每个分区指派了一个装入点 (MP)，以便操作系统可以访问它们。在右侧，有两个磁盘，一个磁盘分为 2 个物理分区，另一个磁盘分为 3 个物理分区。定义了两个 LVM 卷组 (VG1 和 VG2)。VG1 包含 DISK1 中的 2 个分区和 DISK2 中的 1 个分区。VG2 包含 DISK2 中剩余的 2 个分区。在 LVM 中，将卷组中包含的物理磁盘分区称为物理卷 (PV)。在卷组中，定义了 4 个逻辑卷（从 LV1 到 LV4），操作系统可通过相关的装入点使用这些逻辑卷。不同逻辑卷之间的边界不一定是任何分区边界。请参见本示例中 LV 1 和 LV 2 之间的边界。

LVM 功能：

- 可以将多块硬盘或多个分区合并为一个较大的逻辑卷。
- 如果配置合适，当可用空间用完后，可以扩大 LV（例如 /usr）。
- 通过使用 LVM，可以在正在运行的系统中添加硬盘或 LV。但这需要能执行此类操作的可热插拔的硬件。
- 可以激活将逻辑卷的数据流分布在多个物理卷上的“分带方式”。如果这些物理卷驻留在不同的磁盘上，则可以提高读写性能，这与 RAID 0 类似。
- 使用快照功能可以在正在运行的系统中执行一致的备份（尤其适合服务器）。

通过这些功能，使用 LVM 还对频繁使用的家用 PC 或小型服务器有用。如果您的数据储存量（如数据库、音乐档案或用户目录）不断增长，则 LVM 正是您所需要的工具。此工具支持您使用大于物理硬盘的文件系统。LVM 的另一个优点是最多可以添加 256 个 LV。但是，请记住，使用 LVM 与使用传统的分区截然不同。位于 <http://tldp.org/HOWTO/LVM-HOWTO/> 的官方 LVM HOWTO 提供了有关配置 LVM 的说明和详细信息。

从内核版本 2.6 开始，您便可以使用 LVM 版本 2 了，该版本向下兼容以前的 LVM，从而使您能继续管理以前的卷组。在创建新卷组时，决定是使用新格式还是使用向下兼容的版本。LVM2 不需要任何内核增补程序。它利用集成在内核 2.6 中的设备映射程序。该内核只支持 LVM V2。因此本章说到 LVM 时总是指 LVM V2。


7.1.2 用 YaST 配置 LVM

YaST 专家分区程序完成 YaST LVM 配置（请参阅 [第 8.5.5 节“使用 YaST 分区程序”](#) [132]）。此分区工具用于编辑和删除现有分区并创建用于 LVM 的新分区。在此，首先单击 **创建 > 不格式化创建 LVM 分区**，然后选择 **0x8e Linux LVM** 作为分区标识符。创建好所有要与 LVM 一起使用的分区后，请单击 **LVM 开始 LVM 配置**。

创建卷组

如果系统上仍无卷组存在，则系统将提示您添加一个卷组（请参阅 [图 7.2“创建卷组”](#) [100]）。也可以通过 **添加组** 创建其他组，但通常单独一个卷组就已足够。建议使用 **system** 作为包含 SUSE Linux Enterprise® 系统文件的卷组名。物理区域大小定义卷组中物理块的大小。卷组中的所有磁盘空间都是按此大小的区块来处理的。通常将这个值设置为 **4 MB**，并允许物理卷和逻辑卷的最大大小采用 **256 GB**。如果要设置大于 **256 GB** 的逻辑卷，则只应增加物理区域大小（例如，增加到 **8、16 或 32 MB**）。

图 7.2 创建卷组



Create a Volume Group

Now we have to create a volume group.
Typically you don't have to change anything,
but if you are an expert, feel free to change
our defaults:

Volume Group Name:

Physical Extent Size

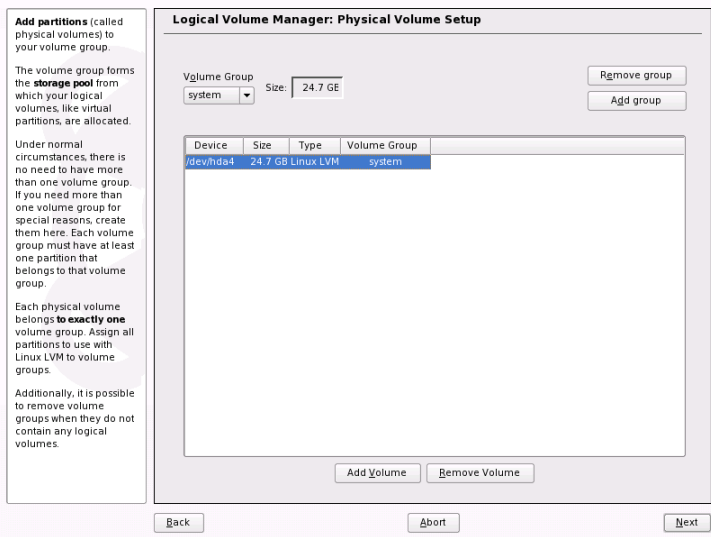
☐ Use Old LVM1 Compatible Metadata Format

配置物理卷

创建了卷组之后，以下对话框将列出类型为“Linux LVM”或“Linux native”的所有分区。未显示交换分区或 DOS 分区。如果已将某个分区指派给卷组，则在列表中显示此卷组的名称。用“--”表示未指派的分区。

如果存在多个卷组，请在选择框的左上角设置当前卷组。使用右上角的按钮可以创建其他卷组和删除现有的卷组。只能删除没有指派任何分区的卷组。指派给卷组的所有分区还被称为物理卷 (PV)。

图 7.3 物理卷设置

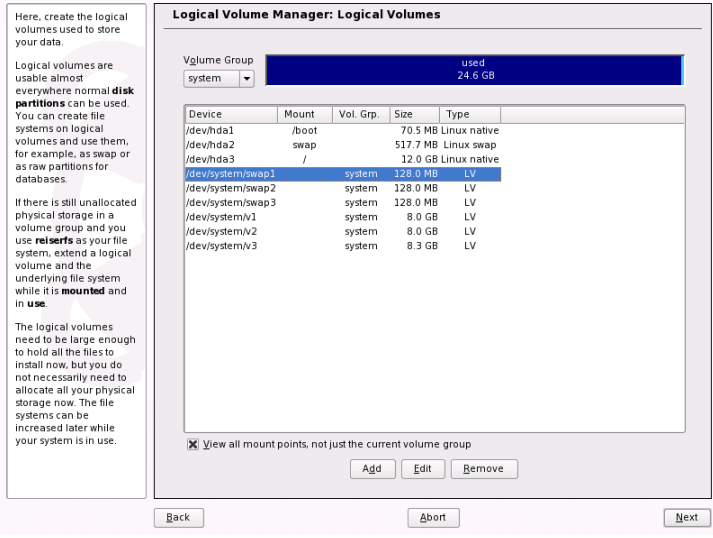


要将以前未指派的分区分添加到所选的卷组中，请先单击该分区，然后单击**添加卷**。此时，卷组的名称就被输入到所选分区的旁边。将为 LVM 预留的所有分区指派给卷组。否则，分区中的空间仍处于未使用状态。在退出对话框前，必须为每个卷组指派至少一个物理卷。在指派所有物理卷后，单击**下一步**继续逻辑卷的配置。

配置逻辑卷

在用物理卷填充了卷组后，请定义操作系统应在下一个对话框中使用的逻辑卷。在选择对话框的左上角设置当前卷组。接着，显示当前卷组中的可用空间。下面的列表包含该卷组中的所有逻辑卷。这里列出了为其指派装入点的所有普通 Linux 分区、所有交换分区和所有现有的逻辑卷。根据需要，添加、编辑和去除逻辑卷，直到卷组中的所有空间都用完为止。请为每个卷组至少指派一个逻辑卷。

图 7.4 逻辑卷管理

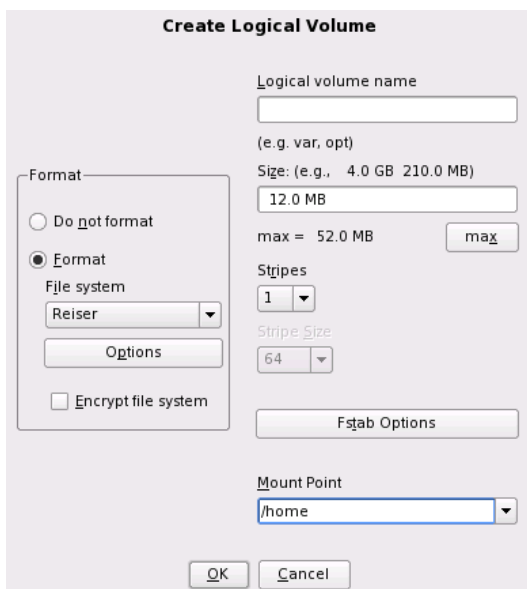


要创建新逻辑卷，请单击添加并填写打开的弹出窗口。对于分区，输入大小、文件系统和装入点。通常，文件系统（如 **reiserfs** 或 **ext2**）是在逻辑卷上创建的，然后为其指定装入点。在已安装系统的这个装入点可以找到储存在此逻辑卷中的文件。另外，可以在多个物理卷（分带）之间分布逻辑卷中的数据流。如果这些物理卷驻留在不同的硬盘上，则通常会提高读写性能（与 **RAID 0** 类似）。但是，只有可以将 **LV** 所需的硬盘空间平均分配给 **n** 个物理卷，才能正确创建有 **n** 个分带的分带 **LV**。例如，如果只有两个物理卷可用，则不可能存在有三个分带的逻辑卷。

警告: 分带

在此，**YaST** 无法校验有关分带项的正确性。这里所犯的任何错误只有以后在磁盘上实施 **LVM** 时才能显现。

图 7.5 创建逻辑卷



The image shows a 'Create Logical Volume' dialog box. It has a title bar 'Create Logical Volume'. Inside, there's a 'Logical volume name' text box. Below it, a hint '(e.g. var, opt)'. Then a 'Size: (e.g., 4.0 GB 210.0 MB)' label with a text box containing '12.0 MB'. To the right of the size box, it says 'max = 52.0 MB' with a 'max' button. Below the size box is a 'Stripes' dropdown menu set to '1'. To its right is a 'Stripe Size' dropdown menu set to '64'. Below these is an 'Fstab Options' button. At the bottom is a 'Mount Point' dropdown menu set to '/home'. On the left side, there's a 'Format' section with two radio buttons: 'Do not format' (unselected) and 'Format' (selected). Below the 'Format' radio button is a 'File system' dropdown menu set to 'Reiser'. Below that is an 'Options' button. At the bottom of the 'Format' section is a checkbox for 'Encrypt file system' which is unchecked. At the very bottom of the dialog are 'OK' and 'Cancel' buttons.

如果您已在系统上配置了 LVM，则可以立即输入现有的逻辑卷。在继续前，将适当的装入点指派给这些逻辑卷。通过下一步，返回到 YaST 专家分区程序并在此完成工作。

直接 LVM 管理

如果您已配置了 LVM 并希望更改某些设置，则可采用替代方法来完成这一工作。在 YaST 控制中心，选择系统 > LVM。基本上，此对话框允许执行如上所述相同的操作，但不允许执行物理分区操作。此对话框在两个列表中显示了现有的物理卷和逻辑卷，并且可以使用已介绍的方法来管理 LVM 系统。

7.2 软 RAID 配置

RAID（独立磁盘冗余阵列）的用途是将多个硬盘分区合并成一个大的虚拟硬盘，以便优化性能和/或数据安全性。大多数 RAID 控制器使用 SCSI 协议，因为对大量硬盘，它可用比 IDE 协议更高效的方式寻址，更适于命令的并行处理。还有一些支持 IDE 或 SATA 硬盘的 RAID 控制器。软件 RAID 具有 RAID 系统

的优势，并且没有硬件 RAID 控制器的额外成本。但是这需要一些 CPU 时间以及内存，所以不适用于真正高性能的计算机。

7.2.1 RAID 级别

借助于 YaST, SUSE® Linux Enterprise 可以将多块硬盘合并成一个软 RAID 系统，这是硬件 RAID 的一个非常合理的备选解决方案。RAID 暗示将多块硬盘合成一个 RAID 系统的多种策略，这些策略的目标、优点及特点各不相同。这些变化形式通常称作 *RAID 级别*。

常用的 RAID 级别如下：

RAID 0

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

RAID 1

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

RAID 2 和 RAID 3

这些不是典型的 RAID 实现。级别 2 在位一级而不是块一级对数据进行分带。级别 3 则利用专用的校验磁盘在字节一级进行分带，但不能同时处理多个请求。这两种级别都极少使用。

RAID 4

级别 4 与级别 0 一样，也是在块一级进行分带，只是结合使用了专用的校验磁盘。当数据盘发生故障时，则可以利用奇偶校验数据来制作一块替代盘。

不过，这块校验磁盘可能造成写访问的瓶颈。尽管如此，有时仍使用级别 4。

RAID 5

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

其他 RAID 级别

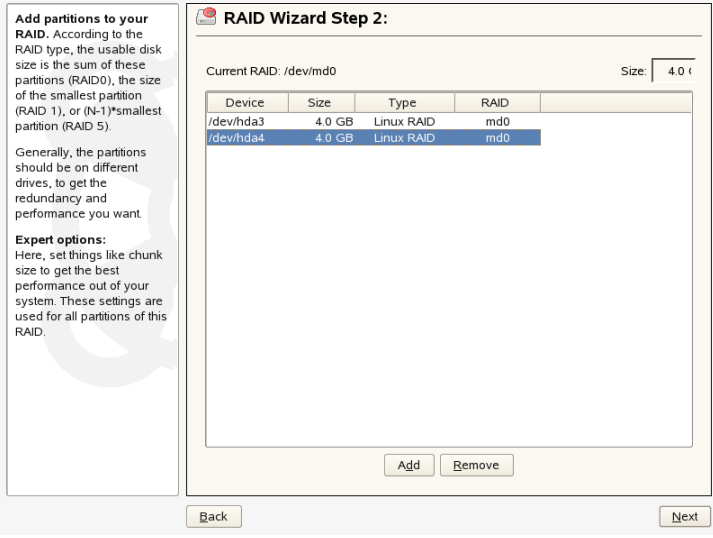
其他多种 RAID 级别也已开发出来（RAIDn、RAID 10、RAID 0+1、RAID 30、RAID 50 等），其中某些级别属于硬件厂商创建的专有实施方法。由于这些级别并不是很普及，所以在此不再赘述。

7.2.2 使用 YaST 配置软 RAID

YaST Expert Partitioner 完成 YaST 软 RAID 配置，如第 8.5.5 节“使用 YaST 分区程序”[132]中所述。此分区工具用于编辑和删除现有分区并创建用于软 RAID 的新分区。利用该工具可创建 Raid 分区，方法是首先单击 *创建* > *不格式化*，然后选择 *0xFD Linux RAID* 作为分区标识符。对于 RAID 0 和 RAID 1，至少需要两个分区，对于 RAID 1，通常只需要两个分区。如果使用 RAID 5，则至少需要 3 个分区。建议只采用相同大小的分区。应将 RAID 分区储存在不同硬盘上，以降低由于某块硬盘出现问题而丢失数据的风险（RAID 1 和 5），同时还可以优化 RAID 0 的性能。创建了所有用于 RAID 的分区后，请单击 *RAID* > *创建 RAID* 开始 RAID 配置。

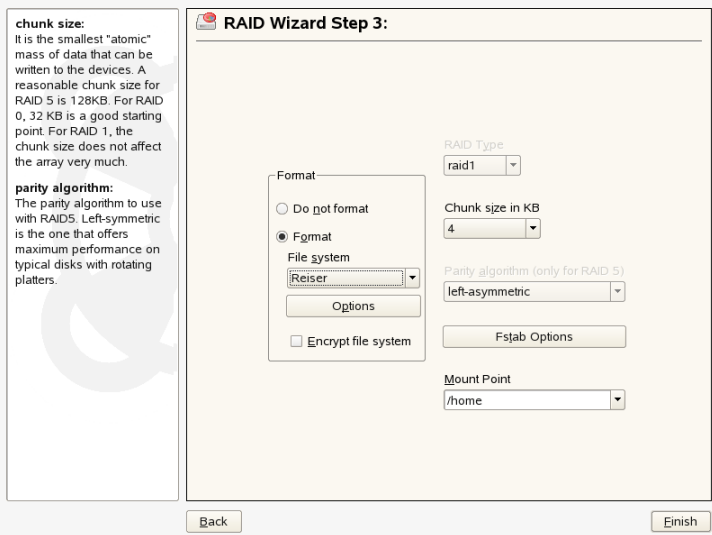
在下一个对话框中选择 RAID 级别 0、1 和 5（有关详细信息，请参见第 7.2.1 节“RAID 级别”[104]）。单击下一步后，随即显示的对话框将列出类型为“Linux RAID”或“Linux native”的所有分区（请参见图 7.6“RAID 分区”[106]）。未显示交换分区或 DOS 分区。如果已将某个分区指派给 RAID 卷，则在列表中显示此 RAID 设备的名称（例如，/dev/md0）。用“--”表示未指派的分区。“”

图 7.6 RAID 分区



要将以前未指派的分区添加到所选的 RAID 卷中，请先单击该分区，然后单击添加。此时，RAID 设备的名称就被输入到所选分区的旁边。指派所有为 RAID 保留的分区。否则，分区中的空间仍处于未使用状态。指派了所有分区后，单击下一步进入设置对话框，从中对性能进行微调（请参见图 7.7“文件系统设置”[107]）。

图 7.7 文件系统设置



与传统的分区一样，设置所用的文件系统，以及RAID卷的加密方法和装入点。选中持久性超级块确保在引导时以这种方式识别 RAID 分区。单击完成完成配置后，请查看 /dev/md0 设备和专家分区工具中指示为 *RAID* 的其他设备。

7.2.3 查错

查看文件 /proc/mdstats 以确定 RAID 分区是否受损。如果系统出现故障，请关闭 Linux 系统并用以同样方式分区的新硬盘替换出现问题的硬盘。然后重新启动您的系统并输入命令 mdadm /dev/mdX --add /dev/sdX。将“X”替换为您的特定设备标识符。此命令会自动将该硬盘集成到 RAID 系统并进行完全重建。

7.2.4 有关详细信息

位于下列位置的 HOWTO 文档提供了软 RAID 的配置说明和详细信息：

- http://www.novell.com/documentation/sles10/stor_evms/data/bookinfo.html

- `/usr/share/doc/packages/mdadm/Software-RAID.HOWTO.html`
- <http://en.tldp.org/HOWTO/Software-RAID-HOWTO.html>

另外还可参考 Linux RAID 邮件列表，如<http://marc.theaimsgroup.com/?l=linux-raid&r=1&w=2>。

使用 YaST 进行系统配置

在 SUSE Linux Enterprise 中，YaST 同时处理系统的安装和配置。本章将介绍系统部件（硬件）、网络访问、安全性设置和用户管理的配置。可在第 8.12 节“文本方式的 YaST”[156]中找出基于文本的 YaST 界面简介。对于手动系统配置的描述，请参见第 17.3 节“通过 /etc/sysconfig 配置系统”[364]。

通过 YaST 使用各种 YaST 模块对系统进行配置。根据硬件平台和所安装的软件，将用不同的方法来访问已安装系统中的 YaST。

在 KDE 或 GNOME 中，从主菜单启动“YaST 控制中心”。在 YaST 启动之前，计算机将提示您输入 root 密码，因为 YaST 需要系统管理员权限来更改系统文件。

要从命令行启动 YaST，请输入命令 `su`（用于更改为 root 用户）和 `yast2`。要启动文本方式的 YaST，请输入 `yast` 而非 `yast2`。此外，也可以使用命令 `yast` 来从虚拟控制台启动此程序。

如果硬件平台不支持它们自己的显示设备，并要在其他主机上进行远程管理，应远程运行 YaST。首先，在主机上打开要显示 YaST 的控制台，然后输入命令 `ssh -X root@<system-to-configure>` 来登录到要配置为 root 的系统，并将 X 服务器输出重定向到您的终端。在 SSH 成功登录后，输入 `yast2` 以图形方式启动 YaST。

要在另一系统以文本方式启动 YaST，请使用 `ssh root@<system-to-configure>` 来打开连接。然后使用 `yast` 启动 YaST。

为了节省时间，可以直接启动单个 YaST 模块。要启动某个模块，请输入 `yast2 module_name`。要查看系统上所有可用模块名称的列表，请使用 `yast2 -l` 或 `yast2 --list`。例如，要启动网络模块，请输入 `yast2 lan`。

8.1 YaST 语言

要更改 YaST 的语言，请在 YaST 控制中心中选择系统 > 语言选择。选择语言，退出 YaST 控制中心并从系统中注销，然后再次登录。下次启动 YaST 时会使用新的语言设置。这也会变更整个系统的语言。

如果需要用不同的语言工作，但又不想更改系统语言设置，请运行 YaST 并将 `LANG` 变量设置为您首选的语言。以 `langcode_statecode` 格式使用长语言代码。例如，对于美国英语，请输入 `LANG="en_US" yast2`。

该命令使用指定的语言启动 YaST。该语言仅对此 YaST 会话有效。终端、其他用户和其他会话的语言设置保持不变。

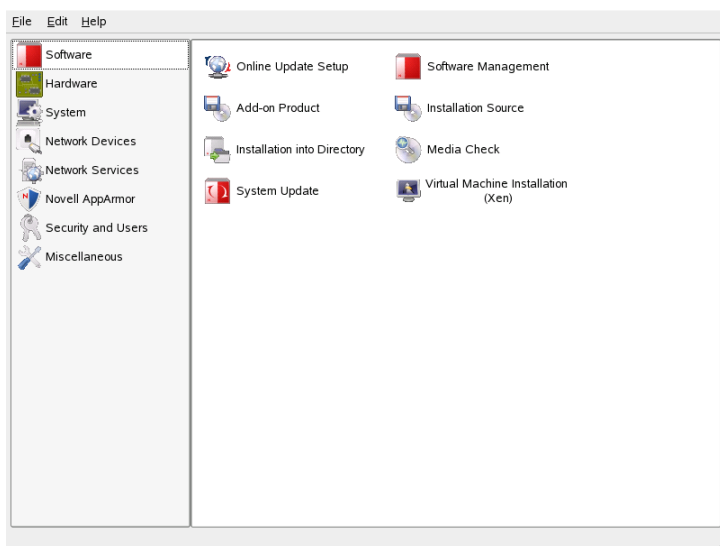
如果通过 SSH 远程运行 YaST，YaST 将使用您本地系统的语言设置。

8.2 YaST 控制中心

以图形方式启动 YaST 时，会打开 YaST 控制中心，如 [图 8.1 “YaST 控制中心”](#) [111] 所示。左侧框架包含可用的类别。单击一个类别时，右边框架中会列出该类别的内容。然后选择希望使用的模块。例如，如果选择 *硬件* 并单击右框架中的声卡，就会打开声卡的配置对话框。各个项目的配置通常需要多个步骤。按下一步继续进行下一步骤。

大部分模块的左框架会显示帮助文本，提供配置建议并说明所需条目。要在模块中获得不带帮助框架的帮助，请按 **F1** 键或选择 *帮助*。在选择希望的设置之后，通过在配置对话框的最后一页按接受来完成配置过程。同时会保存所做的配置。

图 8.1 YaST 控制中心



注意: YaST 软件管理 Gtk 和 Qt 前端

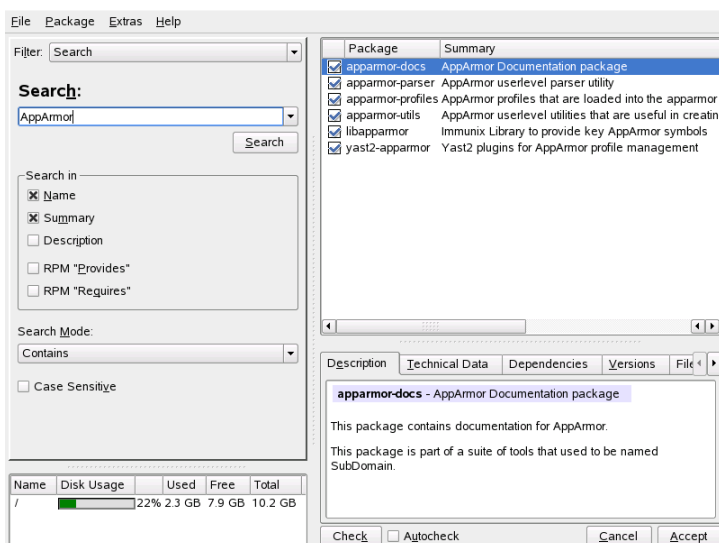
根据系统上安装的桌面，YaST 带有两个前端。默认情况下，YaST gtk 前端在 GNOME 桌面上运行，而 YaST qt 前端在其他桌面上运行。这可以通过 `/sbin/yast2` 脚本中的 `WANT_UI` 变量定义。gtk 前端在功能方面与手册中描述的 qt 前端很相似。gtk 软件管理模块是个例外，它与 qt 端口有很大的不同。

8.3 软件

8.3.1 安装和去除软件

要安装、卸载和更新计算机上的软件，请使用 **软件 > 软件管理**。这时会打开如图 8.2 “YaST 包管理器” [112] 中所示的包管理器对话框。

图 8.2 YaST 包管理器



在 SUSE® Linux Enterprise 中，软件是以 RPM 包的形式供用户使用的。通常包含有程序所需的所有项：程序本身、配置文件及所有文档。在包列表窗口右侧将显示各个包的列表。此列表的内容由当前选择的过滤器确定。例如，如果选择了模式过滤器，则包列表窗口将显示当前选择的所有包。

在包管理器中，每个包都有一个状态，它决定要对包执行的操作，如“安装”或“删除。”此状态通过位于行开头的状态框中的一个符号来显示。要切换某项目的状态，请右击此项目，然后从打开的菜单中单击或选择所需状态。根据当前情况，可能不能选择某些状态标志。例如，不能将尚未安装的包设置为“删除。”请使用帮助 > 符号来查看可用的状态标志。

包列表窗口中各个包所用的字体颜色提供了附加信息。安装媒体上存在有较新版本的已安装包显示为蓝色。版本号高于安装媒体上版本的已安装包显示为红色。但是，因为包的版本编号不总是线性的，这些信息可能会不完整，但足以指出有问题的包。必要时请检查版本号。

安装包

要安装包，请选择要安装的包，然后单击接受。所选包应带有安装状态图标。包管理器会自动检查依赖性并选择所需要的任何其他包（解决依赖性）。要在

单击接受前查看安装所需要的其他包，请从主菜单中选择其他 > 显示自动包更改。安装包后，单击安装更多可继续使用包管理器，或者单击完成将其关闭。

包管理器为安装提供要预先选择的分组。您可以不选择单个包，而是选择整个组。要查看这些组，请使用左框架中的过滤器。

提示: 所有可用包的列表

要显示安装媒体上的所有包，请使用过滤器包组，并在树的底部选择按字母顺序列出全部。SUSE Linux Enterprise 包含大量的包，可能需要一些时间来显示这个长列表。

安装和去除模式

模式过滤器根据用途（如桌面或办公应用程序）对程序包进行分组。列出多组模式过滤器和及安装过的预选包。

单击行开头的状态框以安装或卸载此模式。通过鼠标右击模式和使用上下文菜单来直接选择状态。右侧的包列表概览显示包含在当前模式中的包，从中可选择和取消选择各个包。

安装和去除语言支持

要找到特定于语言的包（例如程序的用户界面的翻译文本、文档和字体），请使用语言过滤器。此过滤器显示 SUSE Linux Enterprise 支持的所有语言列表。如果选择列出的语言之一，则右框架显示此语言可用的所有包。在这些包之中，将自动标记适用于当前软件选择的所有包以进行安装。

要从系统卸载语言，请从语言列表选择语言并取消选中行首的状态框。

注意

因为指定语言的包可能依赖于其他包，所以包管理器将选择安装其他包。

包和安装源

如果只想从指定来源查找包,用安装源过滤器。在默认设置中，此过滤器显示所有来自选择来源的包列表。要进一步限制此列表，使用第二过滤器。

要从已选安装源中查看所有已安装包的列表，请选择过滤器 **安装源**，然后从 **第二过滤器 选择安装摘要** 取消选择除 **保持** 外的所有复选框。

可以按常规方式更改各个包列表窗口中的包状态。但是，更改后的包可能就不再满足搜索条件。要从列表中去除这样的包，请使用**更新列表**来更新列表。

安装资源包

通常提供一个包含程序源文件的包。这些源文件不是运行程序所需要的，但您可能需要安装这些源文件来编译程序的自定义版本。

要为选择程序安装源，请选中 **源** 栏中的复选框。如果您看不到复选框，则您的安装源不包含包的源。

保存包选择

如果要在多台计算机上安装相同的包，您可以将配置保存到文件以用于其他系统。要保存包选择，请从菜单中选择**文件 > 导出**。要导入准备好的选择，请使用**文件 > 导入**。

重要: 硬件兼容性

因为此功能可保存确切的包列表，所以只有在源系统和目标系统上的硬件完全相同时，该功能才可靠。关于更复杂的情况，**第 5 章 自动安装** [71]中所述的 **AutoYaST** 可能是更好的选择。

去除包

要去除包，将为要去除的包指派正确的状态，然后单击**接受**。所选包应带有**删除**状态。如果其他已安装的包所需要的包被标记为要进行删除，包管理器就会发出一个警报，提供详细信息和可选解决方案。

重安装包

如果发现包中的文件受损，或者想要从安装媒介重安装包的原始版本，请重安装此包。要重安装包，请选择要重安装的包，然后单击**接受**。所选包应带有**更新**状态。如果安装的包发生依赖性问题，包管理器就会发出一个警报，提供详细信息和可选解决方案。

搜索包、应用程序和文件

要查找指定的包，请使用*搜索过滤器*。输入搜索字符串并单击*搜索*。通过指定各种搜索条件，您可以将搜索限制为仅显示少数几个包，甚至只显示一个包。您也可以在*搜索方式*中使用通配符和正则表达式定义特殊的搜索模式。

提示: 快速搜索

除了*搜索过滤器*外，包管理器的所有列表都具有快速搜索功能。只需输入一个字母，光标就会移动到列表中名称以此字母开头的第一个包。光标必须位于列表中（通过单击列表）。

要通过名称找到包，请选择*名称*，在搜索字段中输入要查找的包的名称，然后单击*搜索*。要通过描述中的文本找到包，请选择*摘要*和*描述*，输入搜索字符串，然后单击*搜索*。

要搜索包含某个特定文件的包，请输入此文件的名称，选择*RPM “提供”*，然后单击*搜索*。要查找取决于某个特定包的所有包，请选择*RPM “要求”*，输入包的名称，然后单击*搜索*。

如果您熟悉 SUSE Linux Enterprise 的包结构，则可以使用*包组过滤器*按主题查找包。这个过滤器按照主题（如应用程序、开发和硬件）在左侧以树结构对程序包进行排序。将分支展开得越深入，对包的选择就越具体。这意味着包列表窗口中显示的包就越少。

安装摘要

在选择要安装、更新或删除的包后，可使用*安装摘要*来查看安装摘要。它将显示当您单击*接受*时会如何影响包。使用左侧的复选框来过滤要在包列表窗口中显示的包。例如，要查看已经安装了哪些包，请取消选中除*保持*之外的所有复选框。

可以按常规方式更改各个包列表窗口中的包状态。但是，相应的包可能就不再满足搜索条件。要从列表中去掉这样的包，请使用*更新列表*来更新列表。

有关包的信息

使用右下方框架中的选项卡可获取有关所选包的信息。如果有包的另一版本可用，您可以获得两个版本的信息。

带有所选包的说明的说明选项卡自动处于活动状态。要查看有关包大小、版本、安装媒体的信息和其他技术细节，请选择技术数据。有关提供的和需要的文件的信息在依赖性中 要查看各安装源的可用版本，请单击版本。

磁盘使用情况

在选择软件期间，模块左下方的资源窗口会显示所有已装入文件系统的预计磁盘使用情况。每次选择后，带颜色的条形图都会增长。只要它保持为绿色，就表明仍有足够的空间。随着不断接近磁盘空间上限，条柱的颜色会逐渐变为红色。如果选择安装的包过多，就会显示一个警报。

检查依赖性

某些包依赖于其他包。这意味着这些包中的软件只有在其他包已安装的情况下才能正常工作。还有某些包具有相同或类似的功能。如果这些包使用相同的系统资源，就不应同时安装它们（包冲突）。

在启动包管理器时，它会检查系统并显示已安装的包。当您选择安装或去除包时，包管理器能自动检查依赖性并选择所需要的任何其他包（解决依赖性）。如果选择或取消选择了存在冲突的包，包管理器会指出存在冲突并提供解决此问题的建议（解决冲突）。

要激活依赖性自动检查，请选择位于信息窗口下的自动检查。激活自动检查后，包状态的任何更改都将触发自动检查。这是一个很有用的功能，因为这将永久地监视包选择的一致性。但这一进程会消耗资源并可能使包管理器运行速度下降。因此，默认情况下不会激活自动检查。无论自动检查的状态如何，当您通过接受确认选择后将执行一致性检查。

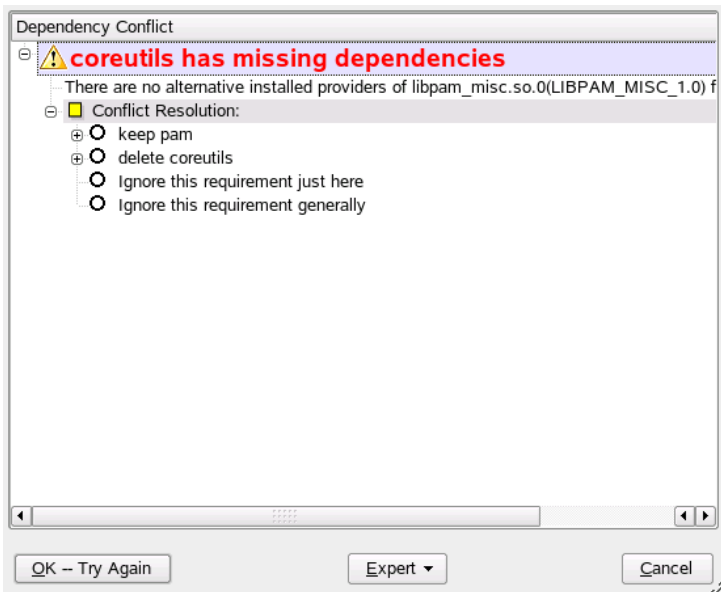
如果单击检查（在信息窗口的下面），包管理器将检查当前包选择是否会造成任何未解决的包依赖性或冲突。如果出现未解决的依赖性，将自动选择所需的其他包。如果出现包冲突，包管理器将打开一个对话框来显示这些冲突，并给出解决问题的多种选择。

例如，可能无法同时安装 sendmail 和 postfix。图 8.3 “包管理器的冲突管理”[117]显示了冲突讯息，提示您作出决定。已经安装了 postfix。因此，您可以选择不安装 sendmail、去除 postfix 或冒险同时安装二者并忽略冲突。

警告: 处理包冲突

除非您的经验非常丰富，否则请在处理包冲突时接受 YaST 的建议，因为不这样的话，您的系统的稳定性和功能就可能会受到现有冲突的影响。

图 8.3 包管理器的冲突管理



安装 -devel 包

包管理器提供用于快捷地安装 devel 和调试包的功能。要为已安装的系统安装所有 devel 包，请选择其他 > 安装所有匹配的 -devel 包。要为已安装的系统安装所有调试包，请选择其他 > 安装所有匹配的 -debuginfo 包。

8.3.2 安装“附加产品”

附加产品是您系统的扩展。您可以安装第三方附加产品或 SUSE Linux Enterprise 的一个特定扩展，比如 SDK 附加或一个二进制驱动器 CD。要增加一项新的附加产品，使用 软件 > 附加产品。您可以选择不同的产品媒体类型，如 CD、

FTP 或本地目录。您也可使用 ISO 文件直接工作。要增加一个扩充作为 ISO 文件媒体, 选择 *本地目录* 然后选择 *ISO 图象*。

成功添加一个扩充媒体后, 将会出现一个包管理器窗口。如果此扩充提供一个新模式, 在 *模式过滤器* 里查看新项目。要查看特定安装源的所有包列表, 选择 *安装源过滤器* 并选择特定安装源。用包组从已选扩充里查看包, 选择第二过滤器 *包组*。

提示: 创建自定义的附加产品

用 YaST 附件创建程序创建您自己的附加产品。在 http://developer.novell.com/wiki/index.php/Creating_Add-On_Media_with_YaST 上读取关于 YaST 附件创建程序的信息。在 http://developer.novell.com/wiki/index.php/Creating_Add-Ons 上查找技术背景信息。

8.3.3 选择安装源

您可以使用若干类型的多个安装源。选择他们然后用 *软件 > 安装源* 来激活他们的安装或更新功能。启动时, 会显示先前注册的所有安装源的列表。从 CD 进行正常安装后, 仅列出安装 CD。单击 *添加* 将其他安装源包含在此列表中。源可以是 CD 和 DVD, 也可以是网络源, 如 NFS 和 FTP 服务器。甚至可以选择本地硬盘上的目录作为安装媒体。请查看详细的 YaST 帮助文本以获取更多详细信息。

所有已注册安装源在列表的第一列都有一个激活状态。单击 *激活* 或 *取消激活* 来启用或禁用各安装源。在安装软件包或更新程序期间, YaST 会从已激活安装源列表中选择一个适当的项。选择 *关闭* 退出此模块时, 当前设置将被保存并应用到配置模块 *软件管理* 和 *系统更新*。

8.3.4 注册 SUSE Linux Enterprise

要获取技术支持和产品更新, 必须注册和激活系统。如果安装期间跳过了注册, 请从 *软件 Novell Customer Center 配置* 模块注册。此对话框与第 3.11.4 节 “*Novell Customer Center 配置*” [33] 中所述的对话框一样。

8.3.5 YaST 联机更新

使用 YaST 联机更新来安装重要的更新和改进。包含增补程序的特定于产品的更新编目中提供 SUSE Linux Enterprise 的最新更新。添加或删除目录,用 软件> 安装源模块（第 8.3.3 节“选择安装源”[118]里的说明。）

注意: 访问更新编目时出错

如果无法访问更新编目，可能是由于订阅已过期。通常，SUSE Linux Enterprise 带有一年或三年订阅，在此期间您可以访问更新编目。一旦订阅结束，将拒绝访问。

拒绝访问更新编目时，您将看到一条警告讯息，建议您访问不 Novell Customer Center 并检查您的订阅。可从 <http://www.novell.com/center/> 访问 Novell Customer Center。

要用 YaST 安装更新和改进，请运行 软件> 联机更新。您系统当前可用的所有新增补程序（除了可选增补程序外）都已标记为安装。单击接受会自动安装这些增补程序。安装完成后，用完成确认。您的系统现在已是最新的了。

术语定义

包

包是 rpm 格式的压缩文件，包含特定程序的文件。

增补程序

增补程序包含一个或多个包（可能是完整的包或者 patchrpm 或 deltarpm 包），也可能引入对尚未安装的包的依赖性。

patchrpm

patchrpm 仅包含从它首次为 SUSE Linux Enterprise 10 发布以来的已更新文件。其下载大小通常比包大小要小的多。

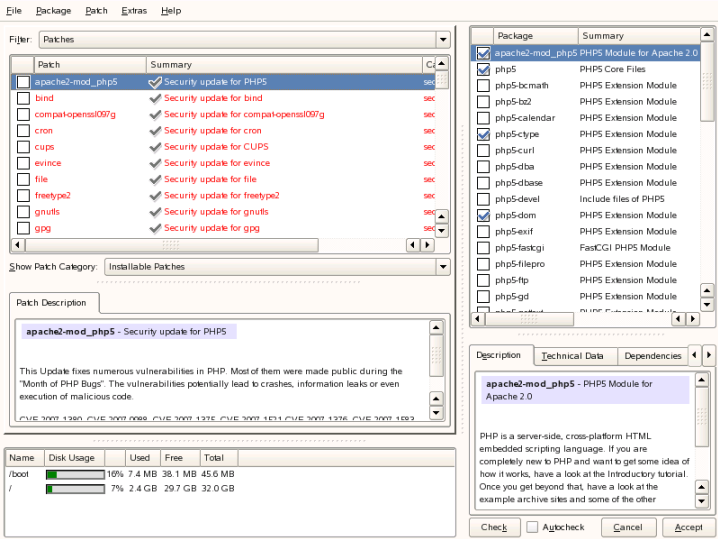
deltarpm

deltarpm 仅包含某个包的两个已定义版本之间的二进制 diff，因此其下载大小最小。安装前，必须在本地计算机上重建 rpm 包。

手动安装增补程序

联机更新窗口由 5 个部分组成。左边是所有可用增补程序的列表。在增补程序列表下可找到选定增补程序的说明。左栏底部显示磁盘使用率。右栏列出了选定增补程序中所含的包（一个增补程序可由多个包组成），底下是选定包的说明。

图 8.4 YaST 联机更新



增补程序显示列出了 SUSE Linux Enterprise 的可用增补程序。增补程序是按安全相关性排序的。增补程序名称的颜色，以及鼠标光标下的一个弹出窗口指示增补程序的安全状态：安全（红色）、建议（蓝色）或可选（黑色）。有三个不同的增补程序视图。可以使用显示增补程序类别切换视图。

可安装增补程序（默认视图）

当前未安装的适用于系统上已安装的包的增补程序。

可安装和已安装的增补程序

应用到系统上安装的包的所有增补程序

所有增补程序

SUSE Linux Enterprise 可用的所有增补程序。

列表项由符号和增补程序名称组成。要查看可能出现的符号的列表，请按 **Shift + F1**。安全性和建议增补程序需要的操作是自动预设置的。这些操作有 *Autoinstall*、*Autoupdate* 或 *Autodelete*。可选增补程序的操作没有预置 — 右键单击某个增补程序然后从列表中选择操作。

如果从不是更新编目的某个编目安装最新的包，可能通过此安装满足此包的某个增补程序的要求。在这种情况下，在增补程序摘要前会显示一个复选标记。该增补程序将显示在列表中，直到将其标记用于安装。这实际上不会安装增补程序（因为该包已经是最新的），而是将该增补程序标记为已安装。

多数增补程序包含几个包的更新。要更改单个包的操作，请在包窗口中右键单击某个包，并选择操作。按需要标记所有增补程序和包后，单击接受。

提示: 禁用 **deltarpm**

由于从 **deltarpm** 重建 **rpm** 包是一项需要大量内存、CPU 和时间资源的任务，某些设置或硬件配置可能需要禁用 **deltarpm** 以提高性能。要禁用 **deltarpm**，请编辑文件 `/etc/zypp/zypp.conf`，并将 `download.use_deltarpm` 设置为 `false`。

更新软件的另一种备选方法就是使用 KDE 和 GNOME 的 ZENworks 更新程序小程序。ZENworks 更新程序能够帮助监视新增补程序。它还提供快速更新功能。有关更多信息，请参考第 1.16 节“用 ZEN 工具管理包”（第 1 章 *KDE 桌面入门*，↑KDE 用户指南）。

8.3.6 自动联机更新

YaST 还能安装自动更新。选择 **软件 > 自动联机更新**。配置 **每日** 或 **每周** 更新。有些增补程序（如内核更新）需要用户交互，交互可能会导致自动更新停止。请选中 **跳过交互增补程序** 使更新过程自动进行。在这种情况下，请手动运行 **联机更新** 安装需要交互的增补程序。

选中仅下载增补程序后，将在指定时间下载增补程序但不会进行安装。它们必须手动进行安装。默认情况下，增补程序将下载到 **rug** 超速缓存目录 `/var/cache/zmd/web`。使用命令 `rug get-prefs cache-directory` 获取当前 **rug** 超速缓存目录。有关 **rug** 的详细信息，请参阅第 8.14 节“从命令行使用 **rug** 更新包” [161]。

8.3.7 从增补程序 CD 更新

软件部分中的增补程序 CD 更新模块从 CD 而非 FTP 服务器安装增补程序。其优势在于使用 CD 可以更快地进行更新。插入增补程序 CD 后，CD 上的所有增补程序都将在对话框中显示。从增补程序列表中选择要安装的包。如果不存在增补程序 CD，模块就会发出一条错误讯息。插入增补程序 CD，然后重新启动此模块。

8.3.8 更新系统

用软件 > 系统更新可更新已装在系统上的 SUSE Linux Enterprise 版本。在操作期间，只能更新应用程序软件，而不能更新基础系统。要更新基础系统，请从安装媒体（如 CD）引导计算机。在 YaST 中选择安装方式时，应选择更新。

更新系统的过程与全新安装类似。最初，YaST 会检查系统，确定适当的更新策略，并将结果显示在建议对话框中。单击更改或各个项以更改任意细节。

更新选项

设置您的系统的更新方法。有两个选项可用。

用“基于选择的新软件和功能安装”更新。

要将整个系统更新到最新软件版本，请选择一个预先定义的选择。这些选择可确保安装先前不存在的包。

仅更新已安装的包

此选项仅更新系统上已存在的包。不会安装任何新功能。

此外，可以使用删除过时的包来去除新版本中不存在的包。默认情况下将预先选择此选项，以避免过时的包无谓地占用硬盘空间。

包

单击包来启动包管理器并选择或取消选择要更新的各个包。应使用一致性检查来解决任何包冲突。中详细介绍了包管理器的使用。[第 8.3.1 节“安装和去除软件”](#) [111]。

备份

在更新期间，某些包的配置文件可能会被替换为新版本的包的配置文件。因为您可能会修改当前系统中的某些文件，包管理器通常会保留被替换文件的备份副本。利用此对话框可确定这些备份的范围。

重要: 备份的范围

这里的备份不包括软件。它只包括配置文件。

语言

此处会列出系统上当前安装的主要和其他语言。可通过在显示的配置中单击语言或通过更改 > 语言来更改语言。（可选的）调整键盘布局和时区以适应使用该主要语言的地区。有关语言选择的详细信息请参见第 8.5.13 节“语言选择”[139]。

有关更新的重要信息

系统更新是一个非常复杂的过程。对于每个程序包，YaST 必须首先检查计算机上已安装的版本，然后确定需要执行哪些步骤来正确地以新版本替换旧版本。YaST 同时会尝试采用已安装包的任何个人设置。

多数情况下，YaST 可以顺利地使用新版本替换旧版本。在执行更新之前应备份现有的系统，以确保在更新期间不会丢失现有配置。在完成更新后可以手动解决冲突。

8.3.9 安装到“目录”

此 YaST 可让您将包安装到指定的目录。确定放置 root 目录的位置、命名目录的方式和希望安装的系统 and 软件类型。进入了此模块后，YaST 会确定系统设置并列出默认目录、安装说明和要安装的软件。通过单击更改来编辑默认设置。必须通过单击接受来确认所有更改。在完成所有修改之后，连续单击下一步直到通知安装完成。单击完成退出对话框。

8.3.10 检查媒体

如果在使用 SUSE Linux Enterprise 安装媒体时遇到任何问题，您可以使用 **软件 > 媒体检查** 来检查 CD 或 DVD。您自行烧录的媒体更容易发生媒体问题。要检查一张 SUSE Linux Enterprise CD 或 DVD 是否有错误，只要将该媒体插入驱动器中并运行此模块即可。单击 **启动**，YaST 将检查媒体的 MD5 校验和。这可能要花几分钟时间。如果检测到有任何错误，则不应使用此媒体进行安装。

8.4 硬件

必须首先按照供应商的说明安装或连接新硬件。打开外部设备，并启动正确的 YaST 模块。YaST 将自动检测大多数设备并显示其技术数据。如果自动检测失败，YaST 将提供一个设备列表（型号、供应商等），您可从中选择合适的设备。有关详细信息，请参考随硬件提供的文档。

重要: 型号指定

如果您选择的型号未包括在设备列表中，可尝试使用具有类似指定的型号。但在某些情况下型号必须完全匹配，因为类似指定常常不具有兼容性。

8.4.1 蓝牙

用 **硬件 > 蓝牙** 配置蓝牙设备。单击 **启用蓝牙服务** 来开始配置。中详细说明了蓝牙配置。“**使用 YaST 配置蓝牙**”一节 [524]

8.4.2 红外设备

用 **硬件 > 红外线设备** 配置红外线设备。单击 **启动 IrDa** 开始配置。您可在配置 **端口** 和 **波特率限制**。有关红外线设备的信息，请参见第 29.3 节“**红外线数据传输**” [532]。

8.4.3 图形卡和监视器

使用 **硬件 > 图形卡和监视器** 配置图形卡和监视器。它使用 SaX2 界面，如第 8.15 节 “SaX2” [164] 中所述。

8.4.4 打印机

通过 **硬件 > 打印机** 配置打印机。如果打印机正确地连接到系统，则应该会自动检测到打印机。有关使用 YaST 配置打印机的详细说明，请参阅第 20.4 节 “设置打印机” [400]。

8.4.5 硬盘控制器

通常情况下会在安装期间配置系统的硬盘控制器。如果添加了控制器，请使用 **硬盘 > 磁盘控制器** 将它们集成到系统中。您也可以修改现有配置，但通常没有必要这样做。

此对话框显示已检测到的硬盘控制器的列表，并使您可以使用特定参数指派合适的内核模块。在将当前设置永久保存在系统中之前，应使用 **测试内核装载** 来检查它们是否正常工作。

警告: 硬盘控制器的配置

在将设置永久保存在系统之前，建议您对其进行测试。错误设置会导致系统不能引导。

8.4.6 硬件信息

使用 **硬件 > 硬件信息** 显示检测到的硬件和技术数据。单击树的任意节点以获取有关设备的更多信息。在提交需要硬件信息的支持请求等时，此模块特别有用。

单击 **保存到文件** 将显示的硬件信息保存到文件。选择需要的目录和文件名，然后单击 **保存** 以创建文件。

8.4.7 IDE DMA 方式

使用**硬件 > IDE DMA**方式可激活或取消激活已安装系统中的 IDE 硬盘、IDE CD 和 DVD 驱动器的 DMA 方式。此模块对 SCSI 设备没有任何作用。DMA 方式可大幅提高系统的性能和数据传送速度。

在安装期间，当前的 SUSE Linux Enterprise 内核会自动激活硬盘的 DMA 方式，但不激活 CD 驱动器的 DMA 方式，因为对所有驱动器均默认激活 DMA 方式常会造成 CD 驱动器出现问题。使用 DMA 模块来为您的驱动器激活 DMA 方式。如果设备支持 DMA 方式而没有任何问题，通过激活 DMA 可提高您的驱动器的数据传送速度。

注意

DMA（直接内存访问）意味着可以将您的数据不经处理器控制而直接传送到 RAM。

8.4.8 游戏杆

通过**硬件 > 游戏杆**配置连接到声卡的游戏杆。在提供的列表中选择游戏杆类型。如果未列出您的游戏杆，则选择**通用模拟游戏杆**。选择了游戏杆之后，请确保游戏杆已连接，然后单击**测试**来测试功能。单击**继续**，YaST 会安装所需文件。在出现**游戏杆测试**窗口之后，通过沿各个方向移动游戏杆和按所有按钮来测试游戏杆。窗口中应显示每次移动。如果您对设置满意，则单击**确定**返回到模块，并单击**完成**以完成配置。

如果是 USB 设备，则无需此配置。插入游戏杆即可使用。

8.4.9 键盘布局

要配置控制台的键盘，请以文本方式运行 YaST，然后使用**硬件 > 键盘布局**。单击模块之后，将显示当前布局。要选择其他键盘布局，请从提供的列表中选择所希望的布局。在**测试**中按键盘上的按键以测试布局。

单击**专家设置**来微调设置。通过在**启动状态**中选择所需的设置来调整键重复率以及延迟并配置启动状态。对于要锁定的设备，输入要应用 Scroll Lock、Num

Lock 和 Caps Lock 设置的以空格隔开的设备列表。单击 **确定** 以完成微调。最后，在完成了所有选择之后，单击 **接受** 以使更改生效。

要设置图形环境的键盘，请运行图形 YaST，然后选择 **键盘布局**。有关图形配置的信息，请参见 [第 8.15.3 节 “键盘属性”](#) [169]。

8.4.10 鼠标方式

为图形环境配置鼠标时，请单击 **鼠标型号** 以访问 SaX2 鼠标配置。有关详细信息，请参见 [第 8.15.2 节 “鼠标属性”](#) [168]。

要配置文本环境的鼠标，请以文本方式使用 YaST。在进入文本方式并选择 **硬件 > 鼠标模型** 后，使用键盘箭头键来从提供的列表中选择鼠标。然后单击 **接受** 以保存设置并退出模块。

8.4.11 扫描程序

连接并打开扫描仪，然后选择 **硬件 > 扫描仪** 以进行配置。可以自动检测大多数支持的扫描仪。选择要配置的扫描仪，然后单击 **编辑**。如果未列出扫描仪，请单击 **添加** 以打开手动配置对话框。从列表中选择相应的供应商和型号并单击下一步来继续安装。要修改某个已配置的扫描仪，请选中它并单击 **编辑**。

在通过自动检测或用户选择确定了扫描仪之后，将执行安装。单击 **完成** 以完成安装。如果安装成功，就会显示一条相应的讯息。要在安装后测试扫描仪，请将文档插入到扫描仪中并单击 **其他 > 测试**。

未检测到扫描仪

只能自动检测支持的扫描仪。无法检测连接到另一台网络主机上的扫描仪。手动配置将区别三种扫描仪：USB 扫描仪、SCSI 扫描仪和网络扫描仪。

USB 扫描仪

选择扫描仪后，YaST 将尝试装载 USB 模块。如果您的扫描仪非常新，就可能不会自动装载这些模块。这时将自动转到一个对话框，您可以在其中手动装载 USB 模块。有关详细信息，请参考 YaST 帮助文本。

SCSI 扫描仪

一般情况下会检测到 SCSI 设备。指定设备，如 `/dev/sg0`。如果出现问题，请参阅 YaST 帮助文本。请记住，在连接或断开 SCSI 扫描仪之前，始终关闭系统。

网络扫描仪

输入 IP 地址或主机名。要配置网络扫描仪，请参考数据库文章在 *Linux 中扫描* (<http://en.opensuse.org/SDB:SDB>)。

如果未检测到您的扫描仪，原因可能是不支持此设备。但有时也会检测不到支持的扫描仪。如果出现这种情况，应手动选择扫描仪。如果能够在供应商和型号列表中找到您要使用的扫描仪，则将其选中。否则应选择取消。有关可用于 Linux 的扫描仪的信息，请参考 <http://cdb.suse.de/> 和 <http://www.sane-project.org/>。

警告: 手动指派扫描仪

只有在您完全有把握的情况下才能手动指派扫描仪。错误选择可能会损坏您的硬件。

故障诊断

无法检测到您的扫描仪的原因可能是以下之一：

- 不支持此扫描仪。请参考 <http://cdb.suse.de/> 查看与 Linux 兼容的设备列表。
- 没有正确安装 SCSI 控制器。
- 您的 SCSI 端口存在终止问题。
- SCSI 数据线过长。
- 此扫描仪具有一个 Linux 不支持的 SCSI 指示灯控制器。
- 此扫描仪存在缺陷。

警告

不能在系统正在运行时连接或断开 SCSI 扫描仪。应首先关闭系统。

8.4.12 电视和广播卡

注意: USB 电视卡

在 YaST 中未配置支持的 DVB 电视卡。它们是可热插拔的。要开始看电视，请将卡连接到计算机并打开您最喜欢的电视节目。

使用 **硬件 > 电视卡** 配置电视和广播卡。如果自动检测到您的电视和广播卡，就会将其在列表中显示出来。此时，选择卡，然后单击 **编辑**。如果未检测到您的卡，请单击 **添加**。如果已经配置了电视或广播卡，请选择要修改的卡，然后单击 **编辑**。

在自动检测硬件期间，YaST 会尝试向您的卡指派正确的调谐器。如果您没有把握，可保留默认 (*已识别*) 并检查它是否正常工作。如果不能设置所有通道，请单击 **选择调谐器** 并从列表中选择正确的调谐器类型。

如果熟悉技术详细信息，可以使用专家对话框来进行电视或广播卡的设置。请在此对话框中选择内核模块及其参数。此外还应检查您的电视卡驱动程序的所有参数。为此，应选择相应的参数并在参数行中输入新值。单击 **应用** 确认新值，或单击 **重设置** 来恢复默认值。

如果您的电视或广播卡连接到安装的声卡，请配置音频设置。使用电缆来将电视或广播卡的输出与声卡的外部音频输入相连接。如果尚未配置您的声卡，应按照第 8.4.13 节 “Sound” [129] 中的介绍选择 **配置声卡** 来配置它。

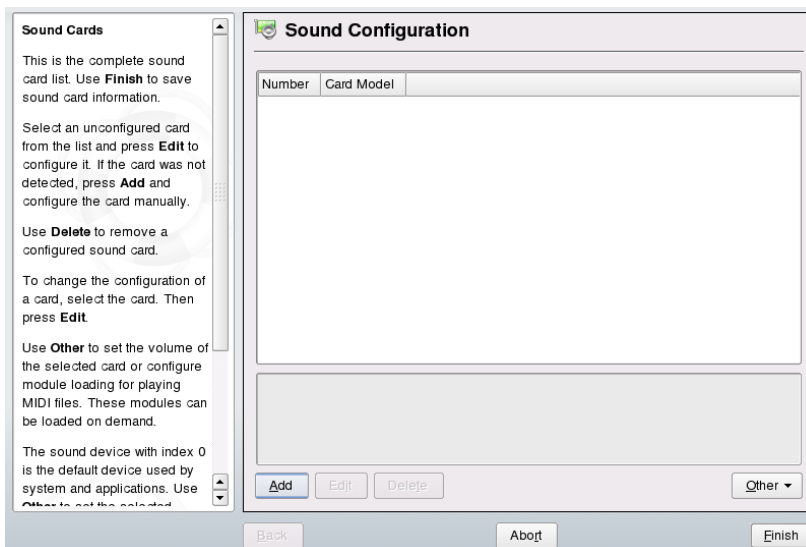
如果您的电视或广播卡具有扬声器插孔，就可以直接连接扬声器而无需使用声卡。有的电视卡没有任何声音功能（如用于 CCD 相机的那些电视卡），不需要对其进行音频配置。

编辑配置时，您还可以通过单击 **电视频道** 来配置电视台。设置您所在区域的正确的 **电视标准** 和 **频率表** 并单击 **扫描频道**。此时显示一个电台列表。在完成了扫描之后，单击 **确定** 以返回到配置对话框。

8.4.13 Sound

大多数声卡是可以自动检测到的，并在初始安装期间用合理的值配置。要稍后安装添加的卡或修改设置，请使用 **硬件 > 声音**。还可以切换卡的顺序。

图 8.5 声音配置



如果 YaST 无法自动检测到您的声卡，请执行以下操作：

- 1 单击添加打开一个对话框，在此对话框中选择一个声卡供应商和型号。有关详细信息，请参考声卡文档。/usr/share/doc/packages/alsa/cards.txt和中提供了 ALSA 所支持的声卡及其对应声卡模块的参考列表。<http://www.alsa-project.org/alsa-doc/> 完成选择后，单击下一步。
- 2 在声卡配置中，在第一个设置屏幕中选择配置级别：

快速自动设置

不要求您进一步执行配置和任何声卡测试。这时将自动配置声卡。

常规设置

调整输出音量并播放测试声音。

可更改选项的高级设置

手动自定义所有设置。

在此对话框中，还有用于游戏杆配置的一个快捷方式。单击游戏杆配置并在以下对话框中选择游戏杆类型来配置游戏杆。单击下一步继续。

- 3 在声卡音量中，测试您的声卡配置并调整音量。您应从总音量的 10% 开始，以免损坏您的听力或扬声器。在您单击**测试**时应听到一段测试声音。如果听不到任何声音，请增大音量。按**下一步 > 完成**完成声音配置。

要更改声卡的配置，请转至**声音配置**对话框，选择显示的卡模型并单击**编辑**。
使用**删除**完全去除声卡。

单击**其他手动自定义**以下选项之一：

卷

使用此对话框设置音量。

启动序列器

要播放 MIDI 文件，请选中此选项。

设置主卡

单击**设置**为主卡调整声卡的序列。索引为 0 的声音设备是系统和应用程序所用的默认设备。

在 YaST 声音模块中单击**完成后**，就会保存所有已安装声卡的音量和配置。混音器设置会保存进文件 `/etc/asound.conf`。asound.conf 会被附加在文件 `/etc/modprobe.d/sound` 和 `/etc/sysconfig/hardware` 的末尾。

8.5 系统

此模块组旨在帮助您管理系统。此组中的所有模块都是与系统相关的，并且充当各种有价值的工具来确保系统正确运行和有效管理数据。

8.5.1 备份

使用**系统 > 系统备份**创建系统和数据的备份。但是，此模块创建的备份不包括整个系统。通过在硬盘上保存重要储存区域（如分区表或主引导记录 (MBR)）来备份系统，它们在您尝试恢复系统时非常重要。它还包括在系统安装时获取用于 AutoYaST 的 XML 配置。备份数据的方法是保存可在安装媒体上访问的包的已更改文件、不可访问的整个包（如联机更新）和不属于包的文件（如 `/etc` 或 `/home` 下的目录中的一些配置文件）。

8.5.2 恢复

使用系统 > 系统恢复，从使用系统备份创建的备份档案中恢复系统。首先指定这些档案的位置（可移动媒体、本地硬盘或网络文件系统）。单击 下一步以查看各档案的说明和内容，并选择从档案中恢复哪些内容。

您也可以卸载自上次备份以来添加的包，或者重安装自上次备份以来删除的包。这两个步骤将把您的系统准确地恢复到上次备份时的状态。

警告: 系统恢复

由于此模块通常安装、替换和卸载很多的包和文件，所以仅当您具有备份经验时才能使用它。否则可能会丢失数据。

8.5.3 引导加载程序配置

要配置计算机现有系统的引导，请使用系统 > 引导加载程序模块。有关如何使用 YaST 配置引导加载程序的详细说明，请参考 [第 18.3 节 “使用 YaST 配置引导加载程序”](#) [376]。

8.5.4 LVM

逻辑卷管理器 (LVM) 是一种利用逻辑驱动器对硬盘进行自定义分区的工具。有关 LVM 的信息，请参见 [第 7.1 节 “LVM 配置”](#) [97]。

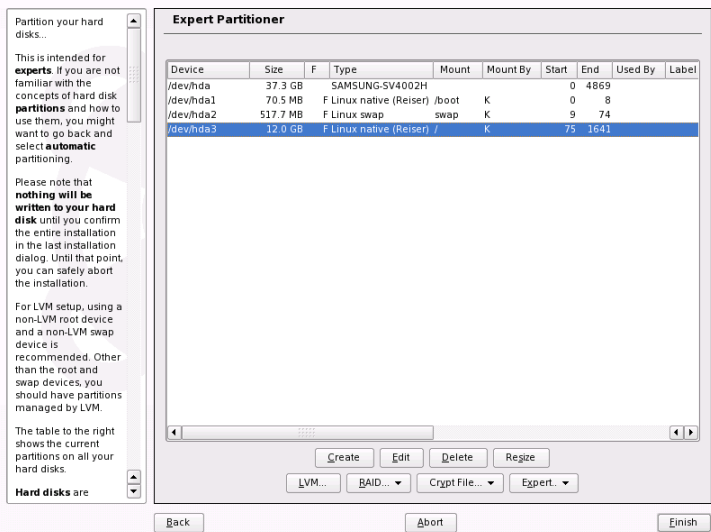
8.5.5 使用 YaST 分区程序

使用如 [图 8.6 “YaST 分区程序”](#) [133] 所示的专家分区程序，可以手动修改一个或多个硬盘的分区。可以添加、删除和编辑分区，并对分区重调整大小。请仍从 YaST 模块中获取软 RAID、和 LVM 配置。

警告: 对运行中的系统重分区

尽管可能在系统运行时对其进行重分区，但发生导致数据丢失的错误的风险很高。尽量避免对已安装的系统进行重分区，在对已安装的系统进行重分区前请始终对数据进行完全备份。

图 8.6 YaST 分区程序



YaST 专家分区程序对话框中列出了所有已连接硬盘上的所有现有分区或建议分区。其中将整个硬盘作为不带编号的设备列出，如 `/dev/hda` 或 `/dev/sda`。将分区作为这些设备的一部分列出，如 `/dev/hda1` 或 `/dev/sda1`。此外还显示硬盘的大小、类型、文件系统和装入点以及硬盘的分区。装入点描述分区在 Linux 文件系统树中的位置。

如果在安装期间运行专家对话框，还会列出并自动选中所有可用硬盘空间。要为 SUSE Linux Enterprise® 提供更多磁盘空间，请在列表中自下而上（从硬盘的最后一个分区向上到第一个分区）释放所需空间。例如，如果您有 3 个分区，则不能将第 2 个分区专用于 SUSE Linux Enterprise，而为其他操作系统保留第 3 个和第 1 个分区。

分区类型

每个硬盘都有一个分区表，其中有 4 个项。分区表中的一项可以对应于一个主分区或一个扩展分区。但只允许有一个扩展分区项。

主分区由指派给特定操作系统的一系列连续的柱面（物理磁盘区域）组成。仅使用主分区时，限制每个硬盘最多具有 4 个分区，因为超过 4 个分区就不能与分区表相符。这就是使用扩展分区的原因。扩展分区同样是一系列连续的磁盘

柱面，但扩展分区本身可以再分为多个逻辑分区。逻辑分区不要求在分区表中有对应的项。换句话说，扩展分区是逻辑分区的容器。

如果需要 4 个以上的分区，请创建一个扩展分区作为第 4 个分区或第 4 个分区之前的分区。这个扩展分区应包括全部剩余的可用柱面范围。然后在扩展分区中创建多个逻辑分区。对于 SCSI、SATA 和 Firewire 磁盘，逻辑分区的最大数目是 15 个，对于 (E)IDE 磁盘是 63 个。对 Linux 使用哪种类型的分区没有什么关系。主分区和逻辑分区都可以。

创建分区

要从头开始创建分区，请按以下步骤操作：

- 1 选择**创建**。如果连接了多个硬盘，则会出现一个选择对话框，可以在其中选择要用于新分区的硬盘。
- 2 指定分区类型（主要类型和扩展类型）。最多可以创建 4 个主分区或 3 个主分区和 1 个扩展分区。在扩展分区内，可以创建多个逻辑分区（请参见“[分区类型](#)”一节 [133]）。
- 3 如有必要，选择要使用的文件系统和装入点。YaST 会为所创建的每个分区建议一个装入点。有关各种文件的详细信息，请参考 [第 22 章 Linux 中的文件系统](#) [427]。
- 4 如果您的设置需要其他文件系统选项，请指定它们。例如，如果您需要永久设备名称，则此操作是必需的。关于可用选项的细节，请参阅“[编辑分区](#)”一节 [134]。
- 5 单击**确定** > *应用*应用您的分区设置并退出分区模块。

如果安装期间创建了分区，将返回到安装概述屏幕。

编辑分区

在创建新分区或修改现有分区时，请设置各种参数。对于新分区，YaST 会设置适当的参数，而且通常无需进行任何修改。要手动编辑您的分区设置，请按以下步骤继续：

- 1 选择分区。

2 单击 *编辑* 来编辑分区并设置以下参数：

文件系统 ID

即使不希望在此阶段格式化分区，仍需要为它指派一个文件系统 ID 来确保正确注册分区。可能值包括 *Linux*、*Linux swap*、*Linux LVM* 和 *Linux RAID*。有关 LVM 和 RAID 的详细信息，请参考第 7.1 节“*LVM 配置*”[97]和第 7.2 节“*软 RAID 配置*”[103]。

文件系统

在此处更改文件系统或格式化分区。更改文件系统或重格式化分区将以不可逆转的方式从该分区删除所有数据。有关各种文件系统的细节，请参阅第 22 章 *Linux 中的文件系统* [427]。

文件系统选项

在此可设置所选文件系统的各种参数。多数情况下可接受默认设置。

加密文件系统

如果激活加密，则将所有数据以加密形式写入硬盘。这可以提高敏感数据的安全性，但会稍微降低系统速度，因为加密需要一些时间。有关文件系统加密的详细信息，请参见第 42 章 *对分区和文件进行加密* [683]。

Fstab 选项

指定在全局文件系统管理文件 (`/etc/fstab`) 中包含的各种参数。默认设置对大多数安装已经足够。例如，您可以将文件系统标识从设备名称更改为卷标。在卷标中，可以使用除 `/` 和空格之外的所有字符。

装入点

指定应将分区装入文件系统树中的哪个目录。请从各个 YaST 建议中选择，或输入任何其他名称。

3 选择 *确定* > *应用* 可激活分区。

专家选项

使用专家可打开包含以下命令的菜单：

重读取分区表

重读取磁盘中的分区。例如，在文本控制台中进行手动分区后需要此命令。

删除分区表和磁盘标签

此命令将完全覆盖以前的分区表。例如，如果非常规磁盘标签出现问题，则可以使用此命令。使用此方法，硬盘中的所有数据都将丢失。

更多分区提示

以下部分包含有关分区的一些提示，它们会在您设置系统时帮助您作出正确决定。

提示: 柱面值

注意，不同的分区工具可能从 0 或 1 开始计算分区的柱面。计算柱面数时，应始终使用最后一个和第一个柱面值之间的差，并加上 1。

如果使用 YaST 执行分区且在系统中检测到其他分区，则也将这些分区添加到文件 `/etc/fstab` 文件中，以便能够方便地访问此数据。此文件包含系统中的所有分区及其属性，如文件系统、装入点和用户许可权限。

例 8.1 `/etc/fstab`: 分区数据

```
/dev/sda1    /data1      auto        noauto,user 0 0
/dev/sda5    /data2      auto        noauto,user 0 0
/dev/sda6    /data3      auto        noauto,user 0 0
```

这些分区（无论是 Linux 还是 FAT 分区）都指定了选项 `noauto` 和 `user`。这允许任何用户都可以根据需要装入或卸装这些分区。由于安全原因，YaST 不会自动在这里输入 `exec` 选项（当从此位置执行程序时需要此选项）。但是，如果要从那里运行程序，您可以手动输入此选项。如果出现“bad interpreter（错误解释器）”或“Permission denied”（权限被拒绝）等系统讯息，则需要执行此操作。

分区和 LVM

从专家分区工具中，使用 *LVM* 访问 LVM 配置（请参阅第 7.1 节“LVM 配置”[97]）。但是，如果系统中已经存在有效的 LVM 配置，当您在会话中首次进入 LVM 配置时将自动激活该配置。这种情况下，凡是包含属于激活卷组的分区的磁盘都无法进行重分区，因为当硬盘上有任何活动分区时，Linux 内核就无法重读取已经修改的该硬盘分区表。不过，如果系统上已存在有效的 LVM 配置，则不必进行物理重分区。但需要更改逻辑卷的配置。

在物理卷(PV)的开始位置，将有关卷的信息写入到分区中。要将这样的分区重用于 LVM 之外的其他用途，最好删除此卷的开始位置。例如，在 VG system 和 PV /DEV/sda2 中，可以通过命令 `dd if=/dev/zero of=/dev/sda2 bs=512 count=1` 完成此操作。

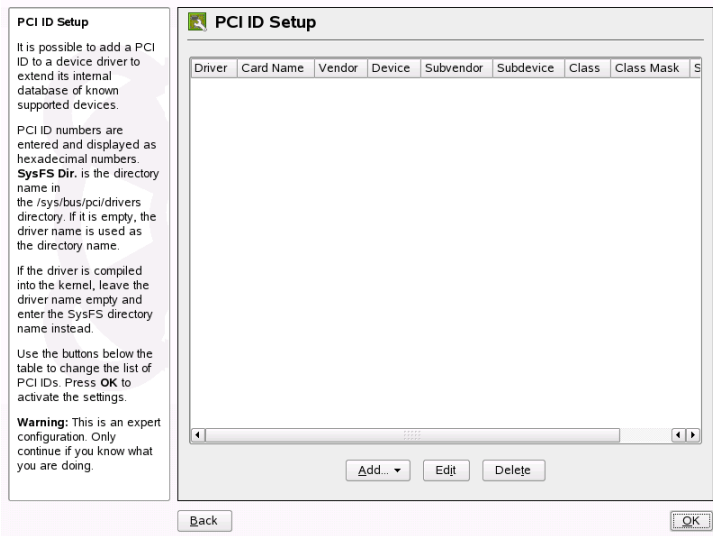
警告: 用于引导的文件系统

用于引导的文件系统（根文件系统或 /boot）不能储存在 LVM 逻辑卷上。而应将其储存在通常的物理分区中。

8.5.6 PCI 设备驱动程序

所有内核驱动器支持的设备 ID 列表包含在该驱动器内。一个不在驱动程序数据库中的新设备，即使能用现有某个驱动程序，也不被视为对该设备的支持。用系统的这个 YaST 模块您可以添加 PCI ID。只允许高级用户尝试使用此 YaST 模块。

图 8.7 添加一个 PCI ID



要添加 ID，请单击添加并选择指派方式：方法是从列表中选择 PCI 设备或手动输入 PCI 值。在第一个选项里，从选择列表里选择 PCI 设备并输入驱动程序名

和目录名。如果不输入目录名，则驱动程序名称将用作目录名。当手动指定 PCI ID 值的时候，输入正确的数据设置 PCI ID。单击**确定**保存修改。

要编辑 PCI ID，从列表中选择要编辑的设备驱动器并单击**编辑**。编辑其信息然后单击**确定**保存修改。要删除某个 ID，请选中该驱动器并单击**删除**。该 ID 立即不在列表里显示。完成后，单击**确定**。

8.5.7 电源管理

系统 > 电源管理模块提供使用节能技术工作的帮助。此功能对延长便携式计算机的工作时间非常重要。使用此模块的详情请参见 [第 28.6 节 “YaST 电源管理模块”](#) [507]。

8.5.8 Powertweak 配置

Powertweak 是一种 SUSE Linux 实用程序，它通过调整某些内核和硬件配置来将系统调整到最佳性能。只有高级用户才可使用此程序。通过系统 > *Powertweak* 启动后，它会检测系统设置并在模块的左框架中以树形式列出系统设置。您还可以使用**搜索**来查找配置变量。选择要调整的选项，以在屏幕上显示该选项及其目录和设置。要保存设置，请单击**完成**，然后单击 **确定** 确认。

8.5.9 配置文件管理器

使用系统 > **配置文件管理**（YaST 系统配置配置文件管理 (SCPM) 模块）来创建、管理和切换系统配置。它尤其适用于在不同位置（在不同网络中）和由不同用户使用的便携式计算机。这个功能对于固定计算机来说也同样有用，因为它使您可使用多种不同的硬件部件或测试配置。有关 SCPM 基础知识和处理的详细信息，请参见[第 27 章 系统配置配置文件管理](#) [475]。

8.5.10 系统服务（运行级别）

使用系统 > **系统服务（运行级别）**配置运行级别和以运行级别启动的服务。有关 SUSE Linux Enterprise 的运行级别的详细信息和 YaST 运行级别编辑器的介绍，请参考[第 17.2.3 节 “使用 YaST 配置系统服务（运行级别）”](#) [362]。

8.5.11 /etc/sysconfig 编辑器

目录 `/etc/sysconfig` 所包含的文件中具有 SUSE Linux Enterprise 最重要的设置。使用 `系统 > /etc/sysconfig Editor` 修改值并将值保存到各配置文件。通常情况下不需要手动编辑，因为在安装包或配置服务时会自动调整这些文件。有关 `/etc/sysconfig` 和 YaST `sysconfig` 编辑器的详细信息，请参考 [第 17.3.1 节“使用 YaST Sysconfig 编辑器更改系统配置”](#) [364]。

8.5.12 时间和日期的设置

安装期间已经初始设置了时区，但是您可以使用 `系统 > 时间和日期` 进行更改。您也可以更改当前系统日期和时间。

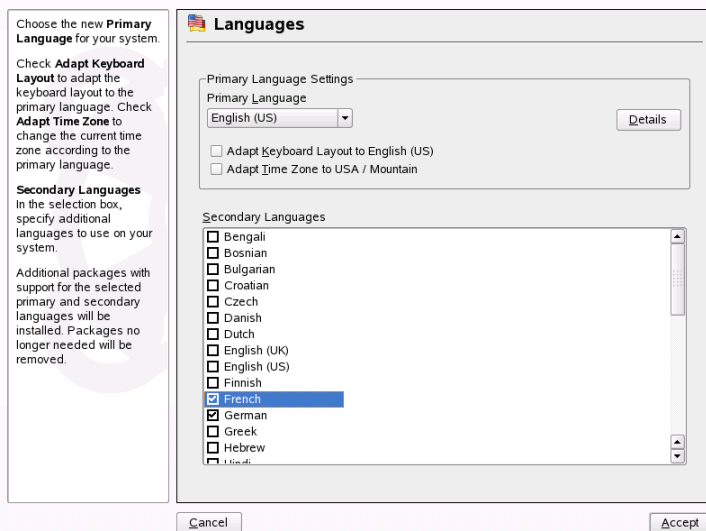
要更改时区，请在左栏选择区域，在右栏选择位置和时区。使用 `硬件时钟设置` 为将系统时钟设置为 `本地时间` 或 `UTC`（世界协调时间）。`UTC` 在 Linux 系统中会经常使用，而使用其他操作系统的机器（如 Microsoft Windows）多数使用本地时间。

通过更改设定当前系统时间和日期。在打开的对话框中，输入新的值或用箭头按钮进行调整，以此修改时间和日期。单击 `应用` 保存更改。

8.5.13 语言选择

安装期间会设置系统的主要和次要语言。但是，可以使用 `系统 > 语言` 来随时更改主要和次要语言。在 YaST 中设置的主要语言将应用于整个系统，包括 YaST 和桌面环境。这是您希望在大部分时间使用的语言。次要语言为由于各种原因，用户在某些时候需要的语言，如桌面语言或文字处理。

图 8.8 设置语言



在**主要语言**中选择用于系统的主要语言。要将键盘或时区调整到该设置，请启用**调整键盘布局**或**调整时区**。

使用**细节**设置如何为 root 设置区域设置变量。使用**细节**还可将主要语言设置为主列表中不可用的方言。这些设置会写入到文件 `/etc/sysconfig/language` 中。

8.6 网络设备

所有连接到系统的网络设备必须先进行初始化才能被服务使用。这些设备的检测和配置是在模块组**网络设备**中完成的。

8.6.1 DSL、SDN、调制解调器或网卡

要配置 DSL、ISDN、网络接口或调制解调器，请从**网络设备**部分选择相应的模块。对于自动检测到的设备，请从列表中选择它，然后单击**编辑**。如果未检测到您的设备，请单击**添加**并手动选择它。要编辑现有设备，请选中该设备，然

后单击 *编辑*。有关详细信息，请参见 [第 30.4 节 “使用 YaST 配置网络连接”](#) [555]。有关无线网络接口，请参见 [第 29 章 无线通讯](#) [513]。

提示: CDMA 和 GPRS 调制解调器

您可以在 YaST 调制解调器模块中将支持的 CDMA 和 GPRS 调制解调器配置为常规的调制解调器。

8.6.2 Fax

用 *网络设备 > 传真* 配置传真系统。可以为一个或多个用户设置传真系统，但每个用户必须拥有一个唯一的传真号码。添加或编辑用户时，请配置用户名、传真号、外发 MSN、站 ID、标题和所希望的操作。

8.6.3 电话答录机

使用 *网络设备 > 电话答录机* 可将您的 SUSE Linux Enterprise 系统配置为具备电话答录机的功能。可以对一个或多个用户配置此功能，但每个用户必须拥有一个唯一的电话号码。添加或编辑用户时，请配置用户名、电话号码、延迟、持续时间和所希望的操作。指派 PIN（个人识别号）可允许用户远程访问机器。

8.7 网络服务

此组包含在网络中配置各种服务的工具。这包括名称解析、用户鉴定和文件服务。

8.7.1 邮件传送代理

如果您使用 sendmail、postfix 或服务提供商的 SMTP 服务器来发送电子邮件，可在 *网络服务 > 邮件传送代理* 中配置您的邮件设置。您可以通过 fetchmail 程序获取邮件，还可以为此输入服务提供商的 POP3 或 IMAP 服务器的详细信息。此外，还可使用自己选择的邮件程序（如 KMail 或 Evolution）来设置您的访问数据。在这种情况下就不需要此模块。

要使用 YaST 配置您的邮件，请在第一个对话框中指定要使用的因特网连接类型。请选择以下选项之一：

Permanent

如果使用专线连接到因特网，请选择此选项。您的计算机将永久联机，所以不需要拨号。如果您的系统是具有中央电子邮件服务器的本地网络的一部分，请选择此选项来确保自己能够永久访问电子邮件。

拨号

此项适用于在家中有电脑、不在网络中但有时连接到因特网的用户。

没有连接

如果既不能访问因特网，又不在某个网络中，就无法发送或接收电子邮件。

通过选择该选项，您可以使用 AMaViS 对接收和发送的电子邮件激活病毒扫描。在您激活电子邮件过滤功能时，将自动安装此包。在以下对话框中，指定外发邮件服务器（通常是您的服务提供商的 SMTP 服务器）和进入邮件的参数。设置不同用户用于接收邮件的多种 POP 或 IMAP 服务器。通过使用此对话框，您也可以指派别名、使用伪装或设置虚拟域。单击 **完成** 退出邮件配置。

8.7.2 其他可用服务

YaST 网络服务提供了许多其他网络模块。

DNS 和主机名

执行此操作使用该模块配置主机名和 DNS（如果在配置网络设备时没有完成这些设置）。还可使用它来更改主机名和域名。如果已经正确配置了提供商来实现 DSL、调制解调器或 ISDN 接入，名称服务器列表将包含自动从提供程序数据中提取的项。如果您位于本地网络中，则可能会通过 DHCP 接收您的主机名，这种情况下不应修改此名称。

主机名

引导并在小型网络中时，您可以使用 *主机名* 代替 DNS 进行主机名解析。此模块中的项反映文件 `/etc/hosts` 的数据。有关详细信息，请参见“[/etc/hosts](#)”一节 [576]。

Kerberos 客户机

如果在您的网络中有 Kerberos 服务器用于网络鉴定，使用 *Kerberos 客户机*。

LDAP 客户机

如果在网络中使用 LDAP 进行用户鉴定，请配置 *LDAP 客户机* 中的客户机。有关 LDAP 的信息和使用 YaST 进行客户机配置的详细说明，请参阅第 35.3 节“使用 YaST 配置 LDAP 客户机” [612]。

NFS 客户机

使用 NFS 客户机，在您自己的文件树中装入 NFS 服务器提供的目录。使用 *NFS 客户机* 来配置您的系统以访问网络中的 NFS 服务器。介绍了 YaST 模块并提供了有关 NFS 的背景信息。第 37 章 *通过 NFS 共享文件系统* [635]。

NIS 客户机

如果在控制中心运行 NIS 服务器管理用户数据，并分发给客户，在这里设置客户机。有关 NIS 客户机和使用 YaST 进行配置的详细信息，请参阅第 33.1 节“配置 NIS 客户机” [597]。

NTP 客户机

NTP（网络时间协议）是一个用于同步网络上硬件时钟的协议。有关 NTP 的信息和使用 YaST 进行配置的说明，请参阅第 32 章 *使用 NTP 同步时间* [591]。

网络服务 (xinetd)

使用 *网络服务* 来配置在引导 SUSE Linux Enterprise 时要启动的网络服务（如 *finger*、*talk* 和 *ftp*）。这些服务使外部主机可以连接到您的计算机。可以为每个服务配置多个参数。默认情况下，不启动管理个别服务的主服务（*inetd* 或 *xinetd*）。

启动此模块时，选择是否启动 *inetd* 或 *xinetd*。可以用标准服务选择启动所选的守护程序。此外，可以用 *添加*、*删除* 和 *编辑* 来撰写自己的服务选择。

警告: 配置网络服务 (xinetd)

在系统上撰写和调整网络服务是一个复杂的过程，要求您全面了解 Linux 服务的概念。默认设置通常就足够了。

代理

在 *代理* 中配置因特网代理客户机设置。单击 *启用代理*，然后输入需要的代理设置。您可以通过单击 *测试代理设置* 来测试这些设置。会出现一个小窗口通知您代理设置是否正确工作。在输入并测试了设置之后，通过单击 *接受* 来保存设置。

远程管理

要通过另一台计算机来远程管理您的计算机，请使用 *远程管理*。要远程维护系统，请使用 VNC 客户程序（如 *krdc* 或支持 Java 的浏览器）。尽管使用 VNC 的远程管理非常简单和快速，但是它没有使用 SSH 安全，您在使用 VNC 服务器时应始终记住这点。有关安装 VNC 客户程序的详细信息，请参见 [第 4.1.1 节“通过 VNC 静态网络配置进行简单远程安装”](#) [38]。

在 *远程管理设置* 中选择 *允许远程管理* 以允许远程管理。选择 *不允许远程管理* 将禁用此功能。单击 *打开防火墙中的端口* 以允许访问您的计算机。单击 *防火墙细节* 将显示防火墙中的端口打开的网络接口。选择希望使用的接口并单击 *确定* 以返回到主对话框。单击 *接受* 完成配置。

强烈建议使用 YaST *远程管理* 模块来在计算机上配置 VNC。尽管 SaX2 接口也允许您设置远程访问属性，但是它不能替代 YaST。它只允许您将 X 服务器配置为主机以供 VNC 会话。有关更多信息，请参考 [第 8.15.6 节“远程访问属性”](#) [170]。

路由选择

使用 *路由选择* 来配置数据在网络上采用的路径。在大多数情况下，只需在默认网关中输入系统的 IP 地址，通过该 IP 地址来发送所有数据。要创建更复杂的配置，请使用 *专家配置*。

Windows 域成员资格

在包含 Linux 和 Windows 主机的异构网络中，Samba 控制着这两个世界之间的通讯。用 *Samba 客户机* 模块，可以把您的电脑设置为一个 Windows 域的成员。有关 Samba 和客户机的设置信息，参见 [第 36 章 Samba](#) [625]。

8.8 AppArmor

Novell AppArmor 旨在为服务器和工作站提供简单易用的应用程序安全。Novell AppArmor 是一个访问控制系统，该系统使您能够指定每个程序可以读取、写入和执行的文件。要在系统上启用或禁用 Novell AppArmor，请使用 *AppArmor 控制面板*。有关 Novell AppArmor 的信息和使用 YaST 进行客户机配置的详细说明，请参阅 *Novell AppArmor Administration Guide* (↑Novell AppArmor Administration Guide)。

8.9 安全性和用户

多用户功能是 Linux 的一个基本特点。因此，多个用户可以相互独立地在同一个 Linux 系统上工作。每个用户都有一个由登录名标识的用户帐户和一个用于登录系统的个人密码。所有用户都有自己的主目录，其中储存着他们的个人文件和配置。

8.9.1 用户管理

使用安全性和用户 > 用户管理创建和编辑用户。它提供系统中用户的概述，包括：NIS、LDAP、Samba 和 Kerberos 用户（请求时）。如果您属于扩展网络，请单击设置过滤器按地理位置列出所有用户。您还可以通过单击自定义过滤器来自定义过滤器设置。

提示：在不关闭模块的情况下应用配置更改

每次需要进行多项配置更改并想避免为每个更改重新启动用户和组配置时，请使用立即写入更改在不退出配置模块的情况下保存更改。

添加用户

要添加新的用户，请如下继续操作：

- 1 单击“添加”。
- 2 为用户数据输入必需的数据。如果您不需要为此新用户调整任何其他の詳細设置，请继续步骤 5 [145]。
- 3 要更改用户的 ID、主目录名、默认主目录、组、组成员资格、目录权限或登录 shell，请打开细节选项卡并更改默认值。
- 4 要调整用户的密码失效、长度和失效警告，请使用密码设置选项卡。
- 5 通过单击接受写入用户帐户配置。

新用户随后就可以使用创建的登录名和密码登录。

删除用户

要删除用户，请如下继续操作：

- 1 从列表中选择用户。
- 2 单击 *删除*。
- 3 确定如何删除或保留要删除的用户的主目录。
- 4 单击 *是*来应用设置。

更改登录配置

要更改登录配置，请执行如下操作：

- 1 从列表中选择用户。
- 2 单击 *编辑*。
- 3 调整 *用户数据*、*细节*和*密码设置*下的设置。
- 4 通过单击 *接受*保存用户帐户配置。

管理加密的用户主目录

可以将加密用户主目录作为用户帐户的一部分来创建。要为用户创建加密的用户主目录，请执行以下操作：

- 1 单击“*添加*”。
- 2 为*用户数据*输入必需的数据。
- 3 在*细节*选项卡中，激活*使用加密用户主目录*。
- 4 单击 *接受*应用您的设置。

要为现有用户创建加密用户主目录，请执行以下操作：

- 1 在列表中选择用户并单击 *编辑*。
- 2 在 *细节* 选项卡中，启用 *使用加密用户主目录*。
- 3 输入选定用户的密码。
- 4 单击 *接受* 应用您的设置。

要禁用用户主目录的加密，请执行以下操作：

- 1 在列表中选择用户并单击 *编辑*。
- 2 在 *细节* 选项卡中，禁用 *使用加密用户主目录*。
- 3 输入选定用户的密码。
- 4 单击 *接受* 应用您的设置。

有关加密用户主目录的详细信息，请参阅 [第 42.2 节 “使用加密的用户主目录”](#) [686]。

自动登录

警告: 使用自动登录

在任何允许许多人进行物理访问的系统上，使用自动登录功能有潜在的安全风险。访问此系统的任何用户都能操纵系统上的数据。如果系统包含机密数据，请勿使用自动登录功能。

如果您是系统的唯一用户，则可以配置自动登录。它在启动后将用户自动登录到系统。只有一个选定用户可以使用自动登录功能。自动登录仅适用于 KDM 或 GDM。

要激活自动登录，请从用户列表选择用户并单击 *专家选项* > *登录设置*。然后选择 *自动登录* 并单击 *确定*。

要取消激活此功能，请选择用户并单击 *专家选项* > *登录设置*。然后取消选择 *自动登录* 并单击 *确定*。

不用密码登录

警告: 允许不用密码登录

在任何允许许多人进行物理访问的系统上，使用不用密码登录功能有潜在的安全风险。访问此系统的任何用户都能操作系统上的数据。如果系统包含机密数据，请勿使用此功能。

当用户在登录管理器中输入用户名后，不用密码登录会自动将用户登录到系统中。这可用于系统上的多个用户，并且仅适用于 **KDM** 或 **GDM**。

要激活此功能，请从用户列表选择用户并单击 **专家选项 > 登录设置**。然后选择 **不用密码登录** 并单击 **确定**。

要取消激活此功能，请从用户列表选择禁用此功能的用户并单击 **专家选项 > 登录设置**。然后取消选中 **不用密码登录** 并单击 **确定**。

禁用用户登录

如果用户不应能登录到系统但其身份应管理几个与系统相关的任务时，要创建这样的用户，请在创建用户帐户时禁用用户登录。按如下所示继续：

- 1 单击“添加”。
- 2 为用户数据输入必需的数据。
- 3 选中禁用用户登录。
- 4 单击接受应用您的设置。

要为现有用户禁用登录，请执行以下操作：

- 1 在列表中选择用户并单击编辑。
- 2 选中用户数据中的禁用用户登录。
- 3 单击接受应用您的设置。

强制实施密码策略

在有多个用户的系统上，最好至少强制实施基本的密码安全性策略。用户应该定期更改其密码并使用不能轻易识破的可靠密码。关于如何强制实施更严格的密码规则的信息，请参考第8.9.3节“本地安全”[151]。要强制实施密码循环，请创建密码失效策略。

要为新用户配置密码失效策略，请执行以下操作：

- 1 单击“添加”。
- 2 在*用户数据*中输入必需的数据。
- 3 调整*密码设置*中的值。
- 4 单击*接受应用您的设置*。

要为现有用户更改密码失效策略，请执行以下操作：

- 1 在列表中选择用户并单击*编辑*。
- 2 调整*密码设置*中的值。
- 3 单击*接受应用您的设置*。

您可以通过指定特定帐户的失效日期来限制该用户帐户的生命周期。以 *YYYY-MM-DD* 格式指定失效日期，并保留用户配置。如果未提供失效日期，则用户帐户永不失效。

更改新用户的默认设置

创建新的本地用户时，YaST使用几个默认设置。您可以更改这些默认设置来满足要求：

- 1 选择 *专家选项 > 新用户的默认设置*
- 2 将更改应用于以下任何项或所有项：
 - *默认组*

- 次要组
- 默认登录 *shell*
- 用户主目录的路径代理
- 用户主目录的架构
- 用户主目录的 *Umask*
- 默认的失效日期
- 密码失效登录可用后的天数

3 单击接受应用您的更改。

可使用本地安全性模块更改与安全性相关的几个其他默认设置。相关信息请参见 [第 8.9.3 节“本地安全”](#) [151]。

更改密码加密

注意

密码加密中的更改仅适用于本地用户。

SUSE Linux Enterprise 可使用 DES、MD5 或 Blowfish 进行密码加密。加密方法的默认密码是 Blowfish。如 [第 3.11.1 节“系统管理员“root”的密码”](#) [30]中所述，加密方法是在系统安装期间设置的。要更改已安装系统中的密码加密方法，请选择 [专家选项 > 密码加密](#)。

更改鉴定和用户源

如 [第 3.11.6 节“用户数”](#) [34]中所述，用户管理方法（如 NIS、LDAP、Kerberos 或 Samba）是在安装期间设置的。要更改已安装系统中的用户鉴定方法，请选择 [专家选项 > 鉴定和用户源](#)。该模块提供配置概述和配置客户机的选项。使用此模块还能够进行高级客户程序配置。

8.9.2 组管理

要创建和编辑组，请选择 *安全性和用户 > 组管理*，或单击用户管理模块中的 *组*。这两个对话框的功能相同，用于创建、编辑或删除组。

此模块提供所有组的概述。与用户管理对话框相同，可以通过单击 *设置过滤器* 来更改过滤器设置。

要添加组，请单击 *添加* 并输入相应的数据。通过选择对应的框在列表中选择组成员。单击 *接受* 以创建组。要编辑组，从列表中选择要编辑的组并单击 *编辑*。完成必要的修改后单击 *接受* 进行保存。要删除组，请从列表中将其选中，然后单击 *删除*。

单击 *专家选项* 以进行高级组管理。有关这些选项的详细信息请参见 [第 8.9.1 节“用户管理”](#) [145]。

8.9.3 本地安全

要将一组安全设置应用于整个系统，请使用 *安全性和用户 > 本地安全性*。这些设置包括引导、登录、密码、用户创建和文件权限的安全。SUSE Linux Enterprise 提供三种预配置的安全集：*主工作站*、*网络工作站*和*网络服务器*。使用 *细节* 修改默认设置。要创建您自己的方案，请使用 *自定义设置*。

详细的或自定义的设置包括：

密码设置

为了使系统在接受新密码之前对其进行安全性检查，请单击 *检查新密码* 和 *复杂密码测试*。设置新创建用户的密码的最小长度。定义密码的有效期间以及提前多少天在用户登录文本控制台时发出密码过期警报。

引导设置

通过选择所需的操作来设置如何解释组合键 **Ctrl + Alt + Del**。通常情况下，在文本控制台中输入这个组合键时会导致系统重引导。除非您的计算机或服务器是公共访问的，而您又担心有人会在没有授权的情况下执行此操作，否则不要修改此设置。如果选择 *停止*，这个组合键将关闭系统。如果选择 *忽略*，将忽略此组合键。

如果您使用 KDE 登录管理器 (KDM)，请在 *KDM* 的关闭行为中设置关闭系统所需的权限。可为 *仅根用户*（系统管理员）、*所有用户*、*无人*或 *本地用户* 提供许可权。如果选择 *无人*，就只能通过文本控制台关闭系统。

登录设置

通常情况下，在登录尝试失败后，需要等数秒之后才能尝试再次登录。这样就使密码嗅探器难以登录。还可以选择激活 *记录成功登录尝试*。如果您怀疑某人试图盗取您的密码，可检查 `/var/log` 中系统日志文件中的项。启用 *允许远程图形登录*，可允许其他用户通过网络访问您的图形登录屏幕。由于这一访问功能具有潜在的安全风险，所以在默认情况下它处于非活动状态。

用户添加

每个用户都有一个数字用户 ID 和一个字母用户 ID。二者之间的相互关系是使用文件 `/etc/passwd` 建立起来的，而且应尽可能地保持唯一性。使用此屏幕中的数据，可定义在添加新用户时指派给用户 ID 的数字部分的数字范围。对于用户来说，这一数字最小应为 500。自动生成的系统用户以 1000 开头。以与组 ID 设置相同的方法来继续设置。

其他设置

要使用预定义的文件权限设置，请选择 *简单*、*安全*或 *高度警惕*。对大多数用户而言使用 *容易* 就足够了。*高度警惕* 设置的限制极为严格，并可以作为自定义设置的基本操作级别。如果选择 *高度警惕*，应注意某些程序可能不能正确工作或甚至不能工作，原因是用户不再具有访问某些文件的权限。

还设置了哪个用户应启动 `updatedb` 程序（如果安装了此程序）。该程序每天定期自动运行或在引导后自动运行，并生成一个数据库 (`locatedb`)，其中储存着每个文件在您的计算机上的位置。如果选择 *无人*，则任何用户都只能在数据库中找到任何其他（未授权）用户均可看到的路径。如果选择 `root`，则将索引所有本地文件，原因是 `root` 是超级用户，可以访问所有目录。请确保取消激活了选项 *根路径中的当前目录*和 *一般用户的路径中的当前目录*。只有高级用户才应考虑使用这些选项，因为若使用错误，这些设置可能会产生严重的安全性风险。单击 *启用 Magic SysRq Keys*，则即使在系统崩溃的情况下您也能对系统进行某些控制。

按 *完成* 以完成安全性配置。

8.9.4 防火墙

SuSEfirewall2 可以保护您的计算机免受来自因特网的攻击。用 *安全性和用户 > 防火墙* 对其进行设置。有关 SuSEfirewall2 的详细信息，请参见 [第 39 章 伪装和防火墙](#) [659]。

提示: 自动激活防火墙

YaST 会在每个已配置的网络接口上自动启动具有适当设置的防火墙。只有您希望使用自定义设置重配置防火墙或取消它时，才启动此模块。

8.10 虚拟化

虚拟化允许在一台物理机器上运行多个操作系统。为不同系统提供的硬件都是虚拟化的。虚拟化 YaST 模块提供 Xen 虚拟化系统的配置。

以下模块在 *虚拟化* 部分中可用：

安装 Hypervisor 和工具

在开始使用 Xen 之前，请安装支持 Xen 并带有相关工具的内核。要安装它们，请使用 *虚拟化 > 安装 Hypervisor 和工具*。安装后，重引导系统以使用 Xen 内核。

创建虚拟机

在成功安装了 Xen hypervisor 和工具后，可以在虚拟服务器上安装虚拟机。要安装虚拟机器，请使用 *虚拟化 > 创建虚拟机器*。

8.11 杂项

YaST 控制中心有若干个模块无法轻易归入前六个模块组。这些模块可用于查看日志文件、从供应商 CD 安装驱动程序等。

8.11.1 自动安装

AutoYaST 工具用于自动安装。在 *其他 > 自动安装* 中，准备此工具的配置文件。使用 AutoYaST 自动安装的详情，请参阅第 5 章 *自动安装* [71]。关于使用自动安装模块的信息，请参阅第 5.1.1 节 “创建 AutoYaST 配置文件” [72]。

8.11.2 支持查询

其他 > 支持查询 可用来收集所有需要的系统信息，以便支持团队查明您的问题，这样您就能尽快获得解决帮助。关于您的查询，请在以下窗口选择问题类别。当所有信息都被集合后，将其附加在您的支持请求。

8.11.3 版本发行说明

发行说明是有关安装、更新、配置和技术问题的重要信息来源。发行说明将通过联机更新不断更新和发布。使用 *其他 > 发行说明* 来查看发行说明。

8.11.4 启动日志

在 *其他 > 启动日志* 中查看有关计算机的启动的信息。当系统发生问题或进行故障诊断时，您可能会首先希望查看此模块。它显示引导日志 `/var/log/boot.msg` 中包含计算机启动时显示的屏幕讯息。查看此日志有助于确定计算机是否正确启动，以及所有服务和功能是否正确启动。

8.11.5 系统日志

使用 *其他 > 系统日志* 来查看 `var/log/messages` 中跟踪计算机操作的系统日志。这里还记录着内核讯息，并按照日期和时间进行排序。使用顶部的框查看特定系统组件的状态。系统日志和引导日志模块中可能有以下选项：

`/var/log/messages`

这是常规系统日志文件。在此处，您可以查看内核讯息、作为 `root` 登录的用户和其他非常有用的信息。

`/proc/cpuinfo`

此选项显示处理器信息，包括处理器类型、制造商、型号和性能。

`/proc/dma`

此选项显示当前使用的 DMA 通道。

`/proc/interrupts`

此选项显示正在使用的中断和已使用的中断数量。

`/proc/iomem`

此选项显示输入/出内存的状态。

`/proc/ioports`

此选项显示当时正在使用的 I/O 端口。

`/proc/meminfo`

此选项显示内存状态。

`/proc/modules`

此选项显示各个模块。

`/proc/mounts`

此选项显示当前装入的设备。

`/proc/partitions`

此选项显示所有硬盘的分区。

`/proc/version`

此选项显示当前的 Linux 版本。

`/var/log/YaST2/y2log`

此选项显示所有 YaST 日志讯息。

`/var/log/boot.msg`

此选项显示关于系统启动的信息。

`/var/log/faillog`

此选项显示登录故障。

`/var/log/warn`

此选项显示所有系统警告。

8.11.6 供应商驱动程序 CD

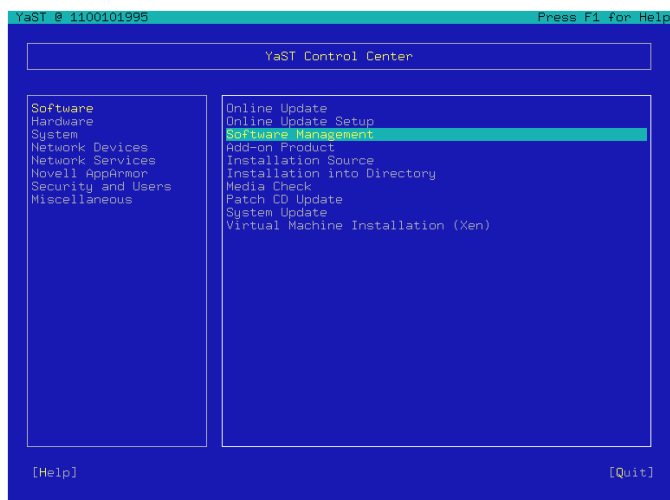
使用 *其他 > 供应商驱动程序 CD*，从包含 SUSE Linux Enterprise 驱动程序的 Linux 驱动程序 CD 安装设备驱动程序。当从头开始安装 SUSE Linux Enterprise 时，在安装后应使用此 YaST 模块从供应商 CD 装载所需的驱动程序。

8.12 文本方式的 YaST

本节所针对的读者是在其系统上不运行 X 服务器而依赖于基于文本的安装工具的系统管理员和专家。它提供了与以文本方式启动和操作 YaST 有关的基本信息。

当以文本方式启动 YaST 时，将首先出现 YaST 控制中心。请参见图 8.9 “文本方式下 YaST 的主窗口” [156]。该窗口包含三个区域。左框架有一个深白色边框，其中列出各个模块所属的类别。它使用有色背景来指示活动类别。具有狭窄的白色边框的右框架提供了活动类别中可用模块的概述。底部框架中包含帮助和退出按钮。

图 8.9 文本方式下 YaST 的主窗口



启动 YaST 控制中心时，将自动选择软件类别。使用 ↓ 键和 ↑ 键可更改类别。要从所选类别启动某个模块，请按 → 键。模块选择此时显示有深色边框。使

用↓键和↑键可选择所需模块。按住箭头键在可用模块列表中滚动。选中某个模块后，即会以彩色背景显示模块标题，同时在底部框架中显示简要说明。

按 Enter 键启动所需模块。模块中的各种按钮和选择字段中包含一个具有不同颜色（默认为黄色）的字母。使用 Alt + yellow_letter 可直接选择按钮，而无需使用 Tab 键导航到那里。通过按 Alt + Q 组合键或选择退出并按 Enter 退出 YaST 控制中心。

8.12.1 在模块中导航

下面在介绍 YaST 模块中的控制元素时，均假定所有功能键和 Alt 组合键都可用并且没有被指派不同的全局功能。有关可能出现的异常的信息，请参见第 8.12.2 节“组合键的限制”[158]。

在按钮和选择列表中导航

使用 Tab 和 Alt + Tab 或 Shift + Tab 可在按钮和包含选择列表的框架中导航。

在选择列表中导航

使用箭头键（↑和↓）可浏览包含选择列表的活动框架中的各个元素。如果框架内的项超出了框架宽度，请使用 Shift + → 或 Shift + ← 来左右水平滚动。也可以使用 Ctrl + E 或 Ctrl + A。如果使用 → 或 ← 键会导致更改活动框架或当前选择列表（像在控制中心中那样），则可以使用此组合键。

按钮、单选项按钮和复选框

要选择带空方括号（复选框）或空圆括号（单选按钮）的按钮，请按 Space 或 Enter 键。也可以直接使用 Alt + yellow_letter 来选择单选按钮和复选框。在这种情况下，无需使用 Enter 键进行确认。如果使用 Tab 键导航到某个项目，请按 Enter 键执行所选操作或激活相应的菜单项。

功能密钥

使用各功能键（F1 到 F12）可快速访问多个按钮。功能键和按钮的实际映射关系取决于活动 YaST 模块，因为不同的模块提供不同的按钮（详细信息、信息、添加、删除等）。可以将 F10 键用作确定、下一步和完成。按 F1 键可访问 YaST 帮助，其中显示了与各个 F 键对应的功能。

图 8.10 软件安装模块



8.12.2 组合键的限制

如果您的窗口管理器使用全局 Alt 组合键，则 YaST 中的 Alt 组合键可能无效。像 Alt 或 Shift 这样的键也可能被终端设置占用。

使用 Esc 代替 Alt

Esc 可以代替 Alt 来执行 Alt 快捷键。例如，Esc + H 可代替 Alt + H。（首先按 Esc，然后按 H 键。）

使用 Ctrl + F 和 Ctrl + B 执行向后和向前导航

如果 Alt 和 Shift 组合键被窗口管理器或终端占用，可改用组合键 Ctrl + F（向前）和 Ctrl + B（向后）。

功能键的限制

功能键也可用于执行多种功能。某些功能键可能会被终端占用而不能用于 YaST。但 Alt 组合键和功能键应该始终在纯文本控制台上完全可用。

8.13 通过命令行管理 YaST

任务只需执行一次时，图形或 `ncurses` 界面通常是最佳的解决方案。如果任务需要重复执行，则可能使用 YaST 命令行界面更佳简便。自定义脚本也可以使用此界面来自动执行任务。

要查看系统上所有可用模块名称的列表，请使用 `yast -l` 或 `yast --list`。要显示某个模块的可用选项，请输入 `yast module_name help`。如果模块没有命令行模式，则会显示告知您此情况的讯息。

要显示某个模块命令选项的帮助，请输入 `yast module_name command help`。要设置选项值，请输入 `yast module_name command option=value`。

因为已存在具有同样功能的命令行工具，所以某些模块不支持命令行模式。涉及的模块和可用命令行工具为：

`sw_single`

`sw_single` 提供包管理和系统更新功能。请在脚本中使用 `rug`，而不是 YaST。请参考 [第 8.14 节 “从命令行使用 rug 更新包”](#) [161]。

`online_update_setup`

`online_update_setup` 配置系统的自动更新。它可以用 `cron` 进行配置。

`inst_suse_register`

使用 `inst_suse_register` 来注册您的 SUSE Linux Enterprise。关于注册的详细信息，请参见 [第 8.3.4 节 “注册 SUSE Linux Enterprise”](#) [118]。

`hwinfo`

`hwinfo` 提供系统的硬件信息。命令 `hwinfo` 也可以实现同样的功能。

`GenProf`、`LogProf`、`SD_AddProfile`、`SD_DeleteProfile`、`SD_EditProfile`、`SD_Report` 和 子域

这些模块控制或配置 AppArmor。AppArmor 具有自己的命令行工具。

8.13.1 管理用户

用于用户管理的 YaST 命令与传统的命令不一样，它们考虑到了创建、修改或去除用户时系统上已配置的鉴定方法和默认用户管理设置。例如，您在添加用

户期间或之后无需创建用户主目录或复制 `skel` 文件。输入用户名和密码后，所有其他设置将按照默认配置自动完成。命令行提供的功能与图形界面一样。

YaST `users` 模块用于用户管理。要显示命令行选项，请输入 `yast users help`。

要添加多个用户，请用要添加用户的列表来创建一个 `/tmp/users.txt` 文件。每行输入一个用户名并使用以下脚本：

例 8.2 添加多个用户

```
#!/bin/bash
#
# adds new user, the password is same as username
#

for i in `cat /tmp/users.txt`;
do
    yast users add username=$i password=$i
done
```

与添加一样，您可以删除 `tmp/users.txt` 中定义的用户。

例 8.3 去除多个用户

```
#!/bin/bash
#
# the home will be not deleted
# to delete homes, use option delete_home
#

for i in `cat /tmp/users.txt`;
do
    yast users delete username=$i
done
```

8.13.2 配置网络和防火墙

脚本中通常需要网络和防火墙配置命令。请使用 `yast lan` 配置网络，使用 `yast firewall` 来配置防火墙。

要显示 YaST 网卡配置选项，请输入 `yast lan help`。要显示 YaST 防火墙卡配置选项，请输入 `yast firewall help`。YaST 网络和防火墙配置始终保持不变。重引导后，无需再次执行脚本。

要显示网络的配置摘要，请使用 `yast lan list`。例 8.4 “`yast lan list` 的输出样本” [161] 输出中的第 1 项是设备 ID。要获取设备配置的详细信息，请使用 `ast lan show id=<number>`。此示例中正确的命令为 `yast lan show id=0`。

例 8.4 `yast lan list` 的输出样本

```
0           Digital DECchip 21142/43, DHCP
```

YaST 防火墙配置的命令行界面是用来启用和禁用服务、端口或协议的快捷方法。要显示允许的服务、端口和协议，请使用 `yast firewall services show`。要获取如何启用服务或端口的示例，请使用 `yast firewall services help`。要启用伪装，请输入 `yast firewall masquerade enable`。

8.14 从命令行使用 `rug` 更新包

`rug` 使用 `zmd` 守护程序根据提供的命令来安装、更新和去除软件。它可以从本地文件或服务器安装软件。您可以使用已知为服务的一个或多个远程服务器。对于本地文件，支持的服务是 `mount`，对于服务器，支持的服务是 `yum` 或 `ZENworks`。

`rug` 将软件从服务器排序为编目（也称为通道），这些编目对应相似软件的组。例如，一个编目可包含来自更新服务器的软件以及来自第三方软件供应商的软件。可以订阅各个编目以控制可用包的显示并防止意外安装不需要的软件。通常只对您所订阅的编目中的软件执行操作。

8.14.1 从 `rug` 获取信息

`rug` 可以提供大量有用的信息。它使您可以检查 `zmd` 的状态、查看注册的服务和编目或查看关于可用增补程序的信息。

如果一段时间内不使用 `zmd`，可将其切换为休眠方式。要检查 `zmd` 状态并重激活该守护程序，请使用 `rug ping`。此命令将唤醒 `zmd` 并记录其状态信息。

要查看已注册的服务，请使用 `rug sl`，要查看您的系统支持哪些服务，请使用 `rug st`。

要查找新的增补程序，请使用 `rug pch`。要获取关于增补程序的信息，请输入 `rug patch-info patch`。

8.14.2 订购 rug 服务

默认情况下，新安装的系统订购了几项服务。要添加新服务，请使用 `rug sa URI service_name`。将 `service_name` 替换为能标识新服务的有意义并且唯一的字符串。

注意: 访问更新编目时出错

如果无法访问更新编目，可能是由于订阅已过期。通常，SUSE Linux Enterprise 带有一年或三年订阅，在此期间您可以访问更新编目。一旦订阅结束，将拒绝访问。

拒绝访问更新编目时，您将看到一条警告讯息，建议您访问不 Novell Customer Center 并检查您的订阅。可从 <http://www.novell.com/center/> 访问 Novell Customer Center。

8.14.3 用 rug 安装和去除软件

要从任何已订购的编目安装软件包，请使用 `rug in package_name`。要仅从选定编目进行安装，请使用 `-c catalog name`。用 `rug if package_name` 获取关于包的更多信息。

要去除软件包，请使用 `rug rm package_name`。如果其他包依赖该包，`rug` 将显示它们的名称、版本和类型。确认您确实要去除该包。

8.14.4 管理 rug 用户

`rug` 的主要优点之一是其用户管理。通常，只有 `root` 能更新或安装新包。使用 `rug`，您可以把更新系统的权限指派给其他用户，并对其进行限制（例如，只能更新不能去除软件）。您可分发的特权包括：

安装

用户可安装新软件

锁定

用户可给包上锁

去除

用户可去除软件

订阅

用户可修改通道订阅

信赖

用户被视为可信，因此他可以安装包而不需要包签名

升级

用户可以更新软件包

查看

此项允许用户查看已安装的软件和通道内可用的软件。此选项只用于远程用户，通常允许本地用户查看已安装和可用包。

超级用户

允许除用户管理和设置（只能在本地执行）以外的其他所有 `rug` 命令。

要授予某用户更新系统的权限，请使用命令 `rug ua username upgrade`。使用用户名替换 `username`。要取消某用户特权，请使用命令 `rugudusername`。要列出注明权限的用户列表，请使用 `rugul`。

要更改用户的当前特权，请使用 `rugue username`，并用所需用户名替换 `username`。将获得选定用户的权限的列表。`edit` 命令是交互式的。使用加号 (+) 或减号 (-) 来添加或去除用户特权，然后按 **Enter** 键。例如，授予用户删除软件的权利，输入 + 删除。保存并且退出，在空白提示符处按 **Enter** 键。

8.14.5 安排更新

使用 `rug`，可以自动更新系统（例如，通过脚本）。最简单的示例就是全自动更新。要完成此操作，请作为 `root` 配置执行 `rug up -y` 的 `cron` 作业。`up -y` 选项从编目下载并安装增补程序而不要求确认。

但是，您可能不想自动安装增补程序，而是想在以后检索并选择要安装的增补程序。如果只想下载增补程序，请使用命令 `rug up -dy`。`up -dy` 选项从您的编目下载增补程序而不要求确认，并将它们保存到 `rug` 超速缓存中。`rug` 超速缓存的默认位置是 `/var/cache/zmd`。

8.14.6 配置 `rug`

`rug` 使您可以通过一组自选设置自定义其设置。有些自选设置是在安装期间预配置的。使用命令 `rug get` 可获取可用自选设置的列表。要编辑自选设置，请输入 `rugset preference`。例如，如果需要通过代理更新系统，则调整设置。在下载更新之前，向代理服务器发送用户名和密码。要完成此操作，请使用以下命令：

```
rug set proxy-url url_path
rug set proxy-username name
rug set proxy-password password
```

使用您的代理服务器的名称替换 `url_path`。使用您的用户名替换 `name`。使用您的密码替换 `password`。

8.14.7 更多信息

要从命令行获取有关更新的更多信息，请输入 `rug --help` 或查看 `rug(1)` 手册页。`--help` 选项也适用于所有 `rug` 命令。例如，如果需要关于 `rug update` 的帮助，请输入 `rug update --help`。

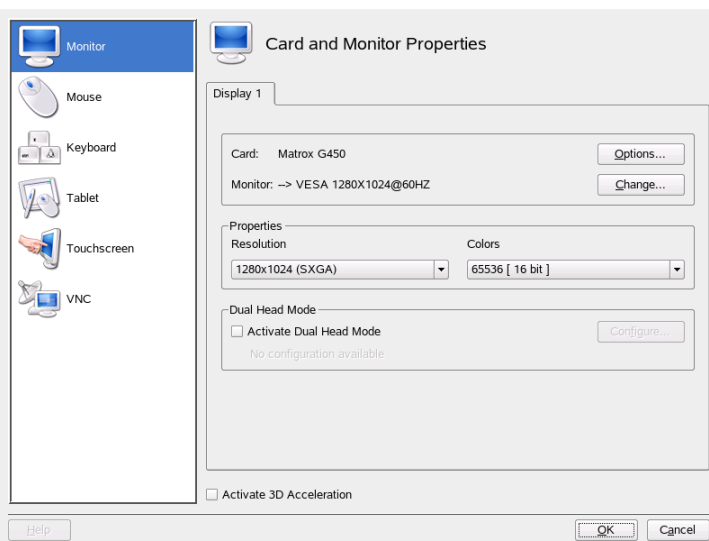
8.15 SaX2

通过 **硬件 > 图形卡和监视器** 配置系统的图形环境。这会打开 SUSE 高级 X11 配置接口 (SaX2)，您可以在其中配置设备(如鼠标、键盘或显示设备)。此界面还可以通过使用 **计算机 > 更多应用程序 > 系统 > Sax2** 从 GNOME 主菜单中访问或通过使用 **系统 > 配置 > SaX2** 从 GNOME 主菜单访问。

8.15.1 卡和监视器属性

在**卡和监视器属性**中调整图形卡和显示设备的设置。如果您安装了多个图形卡，则每个设备会显示在不同的对话框中，可以通过选项卡来使用对话框。在对话框的顶部，可查看选定图形卡与与该图形卡连接的监视器的当前设置。如果可以将多个屏幕与卡连接（双头），则会显示主输出上的监视器。通常，在安装期间系统会自动检测到卡和显示设备。但是，您可以手动调整一些参数，甚至完全更改显示设备。

图 8.11 卡和监视器属性



提示: 自动检测新的显示硬件

如果在安装后更改了显示硬件，请在命令行上使用 `sax2 -r` 让 **SaX2** 检测您的硬件。您必须是 `root` 用户才能通过命令行运行 **SaX2**。

图形卡

不能更改图形卡，因为仅支持已知型号，并且将自动检测这些型号。但是，您可以更改影响卡的行为的一些选项。通常，并不需要更改，因为安装期间系统已适当地设置了这些选项。如果您是专家并且希望精确调整一些选项，则单击

图形卡旁的选项并选择要更改的选项。要将所需值指派到特定选项，在选择该选项之后出现的对话框中输入该值。单击 **确定** 关闭选项对话框。

监视程序

要更改监视器的当前设置，请单击监视器旁的 **更改**。将会打开一个新对话框，您可以在其中调整各种特定于监视器的设置。此对话框有若干用于各个监视器操作部分的选项卡。选择第一个选项卡来在两个列表中手动选择显示设备的供应商和型号。如果未列出监视器，则您可以选择适合需要的 **VESA** 或 **LCD** 方式，如果您有供应商驱动程序磁盘或 **CD**，则单击 **使用磁盘** 并遵循屏幕上的指示来使用。选中 **激活 DPMS** 来使用显示电源管理信号。系统通常已正确设置显示大小（*监视器的几何属性*）和同步频率（*监视器的水平和垂直同步频率的范围*），但您也可以手动修改这些值。在进行了所有的调整之后，单击 **确定** 关闭此对话框。

警告: 更改监视器频率

虽然提供有安全机制，但在手动更改所允许的监视器频率时仍要非常小心。不正确的值可能损坏监视器。更改频率之前，您应始终参考监视器的手册。

分辨率和颜色深度

可以从对话框中间的两个列表直接选择分辨率和颜色深度。您在此处选择的分辨率表示要使用的最高分辨率。最低为 **640x480** 的所有常用分辨率也会被自动添加到配置中。根据使用的图形桌面，您稍后可以切换为任意选项而无需重配置。

双头

如果您的计算机上安装了带有两个输出的图形卡，则您可以将两个屏幕与系统连接。连接到相同图形卡的两个屏幕被称为 **双头**。**SaX2** 会自动检测系统中的多个显示设备并会相应地准备配置。要使用图形卡的双头方式，请选中对话框底部的 **激活双头方式** 并单击 **配置** 来在双头对话框中设置双头选项和屏幕排列。

在此对话框的顶部有一行选项卡，每个选项卡对应于系统中的一个图形卡。选择要配置的卡并在下面的对话框中设置其多头选项。在多头对话框的上方，单击 **更改** 来配置其他屏幕。可能的选项与第一个屏幕的选项相同。从列表中选择此屏幕使用的分辨率。在三个可能的多头方式中选择一个。

克隆多头

在此方式下，所有监视器均显示相同的内容。鼠标仅在主屏幕上可见。

Xinerama 多头

所有屏幕组合起来构成一个大屏幕。可以将程序窗口放置在所有屏幕上，也可以调整为填满多个监视器的某一大小。

注意

Linux 目前尚未提供对 Xinerama 多头环境的 3D 支持。在这种情况下，SaX2 将取消 3D 支持。

双头环境的排列描述各个屏幕的顺序。默认情况下，SaX2 将配置符合检测出的屏幕的顺序的标准布局，将所有屏幕从左到右排列成一行。在对话框的 *排列* 部分，通过选择一个顺序按钮来确定监视器排列的方式。单击 *确定* 关闭对话框。

提示: 通过便携式计算机使用投影机

要将投影机连接到便携式计算机，请激活双头模式。在这种情况下，SaX2 以 1024x768 的分辨率和 60 hz 的刷新率配置外部输出。这些值对多数投影机都非常适用。

多头

如果在计算机中安装了多个图形卡，则可以为系统连接多个屏幕。连接到不同图形卡的两个或多个屏幕被称为 *多头*。SaX2 会自动检测系统中的多个图形卡并会相应地准备配置。默认情况下，SaX2 将配置符合所检测出的图形卡的顺序的标准布局，将所有屏幕从左到右排列成一行。其他 *排列* 选项卡允许手动更改此布局。在网格中拖动表示各个屏幕的图标，并单击 *确定* 来关闭对话框。

测试配置

在完成对监视器和图形卡的配置后，在主窗口中单击 *确定*，然后测试您的设置。这可以确保您的配置适合自己的设备。如果图像不稳定，请通过按 **Ctrl+Alt+Backspace** 来立即终止测试，然后降低刷新率或分辨率和颜色深度。

注意

无论您是否运行测试，所有修改均在您重新启动 X 服务器后被激活。

8.15.2 鼠标属性

在 *鼠标属性* 中调整鼠标的设置。如果您有安装了不同驱动程序的多只鼠标，则每个驱动程序会显示在不同的选项卡中。使用相同驱动程序运行的多个设备会显示为一只鼠标。要激活或取消当前选定的鼠标，请使用对话框顶部复选框。在复选框的下面可以查看该鼠标的当前设置。通常，会自动检测到鼠标，但是如果自动检测失败，您可以手动更改。请参考鼠标文档来获取型号描述。单击 *更改* 以从两个列表中选择供应商和型号，然后单击 *确定* 来确认选择。在对话框的选项部分中，设置用于运行鼠标的各种选项。

激活 3 键仿真

如果您的鼠标只有两个按键，则当您同时单击两个按键即是仿真第三个按键。

激活鼠标滚轮

选中此框以使用滚轮。

Invert X-Axis 和 *Invert Y-Axis*

如果选择了以下选项之一，请将鼠标指针向相反方向移动。对触摸屏，该功能有时很有用。

用鼠标按键模拟滚轮

如果您的鼠标没有滚轮，但是您希望使用类似功能，则您可以为此功能指派一个附加按键。选择要使用的按钮。在按此按键时，鼠标的任何移动都会被转换为滚轮命令。此功能对于轨迹球特别有用。

当您对设置满意时，单击 *确定* 来确认更改。

注意

只有在您重新启动 X 服务器之后，您在此处所做的更改才会生效。

8.15.3 键盘属性

使用此对话框来调整在图形环境中操作键盘的设置。在对话框的上边，选择类型、语言布局和变体。使用对话框底部的测试字段来检查特殊字符是否正确显示。从中间的列表中选择要使用的其他布局 and 变体。根据桌面的类型，可以在运行的系统中切换这些选项而无需重配置。在您单击*确定*之后，将立即应用更改。

8.15.4 图形输入板属性

使用此对话框来配置连接到您系统的图形输入板。单击*图形输入板*选项卡来从列表中选择供应商和型号。目前支持有限数量的图形输入板。要激活输入板，选中对话框顶部的*激活此输入板*。

在*端口和方式*对话框中，配置到输入板的连接。SaX2 支持将图形输入板配置为连接到 USB 端口或串口端口。如果将输入板连接到串行端口，请校验此端口。`/dev/ttyS0` 指第 1 个串行端口。`/dev/ttyS1` 指第 2 个串行端口。其他端口使用类似的表示法。从列表选择适当的选项并选择适合您需要的主输入板方式。

如果您的图形输入板支持电子笔，则在*电子笔*中配置电子笔。添加橡皮和笔，并在单击*属性*之后设置它们的属性。

当您对设置满意时，单击*确定*来确认更改。

8.15.5 触摸屏属性

使用此对话框来配置连接到您系统的触摸屏。如果您安装了多个触摸屏，则每个设备会显示在不同的对话框中，可以通过选项卡来使用对话框。要激活当前选定的触摸屏，请选中对话框顶部的*指派要显示的触摸屏*。从下面的列表中选择供应商和型号并在底部设置相应的*连接端口*。您可以配置连接到 USB 端口或串口端口的触摸屏。如果触摸屏连接到串行端口，请校验此端口。`/dev/ttyS0` 指第 1 个串行端口。`/dev/ttyS1` 指第 2 个串行端口。其他端口使用类似的表示法。当您对设置满意时，单击*确定*来确认更改。

8.15.6 远程访问属性

VNC（*虚拟网络计算*）是一个客户机/服务器解决方案，允许通过简单易用的瘦客户机访问远程 X 服务器。此客户程序可用于多种操作系统，包括 Microsoft Windows、Apple 的 MacOS，以及 Linux。有关 VNC 的其他信息，请参见 <http://www.realvnc.com/>。

使用此对话框来将 X 服务器配置为 VNC 会话的主机。如果您希望 VNC 客户程序与 X 服务器连接，则选中允许使用 VNC 协议来访问显示。设置密码以限制对启用 VNC 的 X 服务器的访问。如果同时有多个 VNC 客户程序应连接到 X 服务器，则选中允许多个 VNC 连接。通过 HTTP 端口中选择激活 HTTP 访问并设置要使用的端口，就能够进行 HTTP 访问。

当您对设置满意时，单击确定来保存更改。

8.16 故障诊断

目录 `/var/log/YaST2` 中记录了所有错误讯息和警报。查找 YaST 问题的最重要文件是 `y2log`。

8.17 更多信息

可在以下万维网站点和目录中找到有关 YaST 的更多信息：

- `/usr/share/doc/packages/yast2` - 本地 YaST 开发文档
- http://www.opensuse.org/YaST_Development - openSUSE wiki 中的 YaST 项目页
- <http://forge.novell.com/modules/xfmod/project/?yast> - 另一 YaST 项目页

更新 SUSE Linux Enterprise

SUSE® Linux Enterprise 使您可以将现有系统更新为新版本而不用完全重安装系统。不需新安装。用户主目录和系统配置等旧数据保持不变。在产品使用周期内，您可以使用“服务包”提高系统安全性和更正软件缺陷。从本地 CD 或 DVD 驱动器安装或从中央网络安装源安装。

9.1 更新 SUSE Linux Enterprise

例如，如果您要从 Novell Linux Desktop 9 更新到 SUSE Linux Enterprise Desktop 10，请遵循本节描述的步骤。如果要从 SUSE Linux Enterprise 10 SP1 更新到 SUSE Linux Enterprise 10 SP2，也可以遵循这些步骤。

从旧版本到新版本，软件的大小有增长的趋势。“”因此，在进行更新之前，请使用 `df` 查看可用分区空间。如果您怀疑磁盘空间不足，请在进行更新和重分区系统前保护好您的数据。对于每个分区应该具有多少空间，没有一般的经验可以借鉴。空间要求取决于特定的分区配置文件和选定的软件。

9.1.1 准备工作

在进行更新之前，将旧的配置文件复制在单独的媒体上（例如磁带设备、可卸硬盘、USB 记忆棒或 ZIP 驱动器）以保护数据。这主要适用于储存在 `/etc` 中的文件以及 `/var` 和 `/opt` 中的一些目录和文件。最好将 `/home`（HOME 目录）中的用户数据也写入备份媒体。以 `root` 用户的身份备份此数据。只有 `root` 用户具有读取所有本地文件的权限。

在开始更新之前，记录必要的根分区信息。命令 `df /` 可以列出根分区的设备名。在例 9.1 “使用 `df -h` 列示信息” [172] 中，要记录的根分区是 `/dev/hda3`（作为 `//` 装入）。

例 9.1 使用 `df -h` 列示信息

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/hda3	74G	22G	53G	29%	/
tmpfs	506M	0	506M	0%	/dev/shm
/dev/hda5	116G	5.8G	111G	5%	/home
/dev/hda1	39G	1.6G	37G	4%	/windows/C
/dev/hda2	4.6G	2.6G	2.1G	57%	/windows/D

9.1.2 可能的问题

如果将默认系统从上一版本更新到这一版本，则 YaST 将分析出所需更改并执行更改。根据您的自定义，一些更新步骤或整个更新过程都可能失败，此时必须将备份数据复制回来。开始系统更新之前检查以下问题。

检查 `/etc` 中的 `passwd` 和 `group`

在更新系统之前，确保 `/etc/passwd` 和 `/etc/group` 不包含任何语法错误。为此，以 `root` 用户身份启动校验实用程序 `pwck` 和 `grpck` 并消除任何报告的错误。

PostgreSQL

在更新 PostgreSQL (`postgres`) 之前，先转储数据库。请参见 `pg_dump` 的手册页。只有当实际上是在更新之前使用了 PostgreSQL 时才需要执行此操作。

9.1.3 使用 YaST 进行更新

完成了第 9.1.1 节“准备工作” [171] 中介绍的准备过程后可以开始更新系统了：

- 1 （可选）准备安装服务器。有关背景信息，请参见第 4.2.1 节“使用 YaST 设置安装服务器” [45]。

- 2 像进行安装时那样引导系统，如 [第 3.1 节“系统启动以进行安装”](#) [17] 中所述。在 YaST 中，请选择语言并在安装方式对话框中选择更新。不要选择全新安装。
- 3 YaST 确定是否有多个根分区。如果只有一个根分区，则继续下一步。如果有多个根分区，则选择正确的分区并单击下一步（的示例中选中了 `/dev/hda3` [第 9.1.1 节“准备工作”](#) [171]）进行确认。YaST 在此分区中读取旧的 `fstab` 进行分析，并装入此处列出的文件系统。
- 4 在安装设置对话框中，请根据需要调整设置。通常情况下，可保留默认设置不动，但如果要增强系统，则选中软件选择子菜单中提供的包或添加其他语言支持。
 - 4a 单击更新选项只更新已经安装的软件（只更新已安装的包）或根据选定的模式对系统添加新软件和功能。建议接受该建议。稍后可以用 YaST 进行调整。
 - 4b 您也可以备份各种系统组件 (*Backup*)。选择备份将减慢更新进程的速度。如果没有最近的系统备份，则使用此选项。
- 5 单击接受并确认开始更新以开始软件安装过程。

在安装结束时请阅读发行声明，然后单击完成以重新启动计算机并登录。

9.2 安装服务包

用服务包更新一个 SUSE Linux Enterprise 安装。有几种不同方法可以应用服务包。即可更新现有的安装，也可用服务包媒体开始全新安装。这里介绍可能的系统更新和设置中央网络安装源的情形。

提示: 安装更改

阅读服务包媒体里的安装指导以进一步了解更改。

9.2.1 为服务包媒体设置网络安装源

初次安装 SUSE Linux Enterprise，在网络上有一个为所有客户服务的中央安装源要比用一套物理媒体分别对他们进行安装要高效的多。

在 SUSE Linux Enterprise 上使用 YaST 设置一个网络安装源

基本上，按照 [第 4.2 节 “设置存放安装源的服务器”](#) [45] 里列出的过程操作即可。只需要添加另外一个安装源 `SLE-10-SP-x-arch`、`SLES-10-SP-x-arch` 或 `SLED-10-SP-x-arch`（`x` 是服务包的编号，`arch` 是您硬件体系结构的名称），并且让这个服务包能够被 NFS、HTTP 或 FTP 使用。

9.2.2 安装服务包

注意

要将现有 SUSE Linux Enterprise 10 系统更新为 SUSE Linux Enterprise 10 Service Pack (SP)，请参见 [第 9.2.3 节 “更新到服务包”](#) [176]。

安装 SUSE Linux Enterprise 服务包与安装原始 SUSE Linux Enterprise 媒体的方法很类似。在原始安装中，可选择从本地 CD 或 DVD 驱动器安装或从中央网络安装源安装。

从本地 CD 或 DVD 驱动器安装

在启动 SUSE Linux Enterprise SP 的新安装之前，请确保所有的服务包安装媒体（CD 或 DVD）都可用。

过程 9.1 从服务包媒体引导

- 1 插入第一张 SUSE Linux Enterprise SP 媒体（CD 1 或 DVD 1）后引导计算机。一个类似于 SUSE Linux Enterprise 10 原始安装的引导屏幕就会出现。
- 2 选择安装并按照 [第 3 章 使用 YaST 进行安装](#) [17] 中的 YaST 安装说明所述继续。

网络安装

在启动 SUSE Linux Enterprise SP 网络安装前，确认满足以下要求：

- 根据 [第 9.2.1 节 “为服务包媒体设置网络安装源”](#) [174] 建立的网络安装源。
- 连接安装服务器和目标计算机的有效网络连接，目标计算机要包含一个名称服务、DHCP（可选，但对于 PXE 引导是必需的）和 OpenSLP（可选）。
- 引导目标系统的 SUSE Linux Enterprise SP CD 1 或 DVD 1 或根据 [第 4.3.5 节 “准备目标系统的 PXE 引导”](#) [62] 为 pxe 引导安装的目标系统。

网络安装 — 从 CD 或 DVD 引导

要用 SP CD 或 DVD 作为引导媒体执行网络安装，请执行如下操作：

- 1 插入 SUSE Linux Enterprise SP CD 1 或 DVD 1 后引导计算机。一个类似于 SUSE Linux Enterprise 10 原始安装的引导屏幕就会出现。
- 2 选择安装从 CD 引导 SP 内核，然后使用 F3 启用更多选项，最后用 F4 选择网络安装源的类型（FTP、HTTP、NFS 或 SMB）。
- 3 提供相应的路径信息或选择 *SLP* 作为安装源。
- 4 从所提供的服务器里选择相应的安装服务器，或用引导选项提示提供安装源类型和实际地址（如 [第 3.1.4 节 “从没有 SLP 的网络源安装”](#) [19] 中所示）。YaST 启动。

按 [第 3 章 使用 YaST 进行安装](#) [17] 中所述完成安装。

网络安装 — PXE 引导

要通过网络执行 SUSE Linux Enterprise 服务包网络安装，请执行以下操作：

- 1 按照 [第 4.3.5 节 “准备目标系统的 PXE 引导”](#) [62] 调整您的 DHCP 服务器设置以提供 PXE 引导需要的地址信息。
- 2 设置 TFTP 服务器来存储 PXE 引导需要的引导映像。

用 SUSE Linux Enterprise 服务包的第一张 CD 或 DVD 执行此操作，或按照 [第 4.3.2 节 “设置 TFTP 服务器”](#) [56] 的说明进行。

- 3 在目标计算机上准备 PXE 引导和局域网唤醒。
- 4 对目标系统引导进行初始化，并用 VNC 远程连接到此计算机正运行的安装例程上。有关更多信息，请参见第 4.5.1 节“VNC 安装”[67]。
- 5 接受许可协议，然后选择语言、默认桌面以及其他安装设置。
- 6 单击是，安装开始安装。
- 7 照常继续安装（输入 root 的密码，完成网络设置，检测网络连接，激活联机更新服务，选择用户鉴定方法并输入用户名和密码）。

有关安装 SUSE Linux Enterprise 的详细说明，请参见第 3 章 *使用 YaST 进行安装* [17]。

9.2.3 更新到服务包

将系统更新到服务包 (SP) 功能级别有两种首选方法。一种方法是从 SP 媒体引导。另一种方法是运行“YaST 联机更新”或 zen-updater，然后选择更新到服务包 X 增补程序。通过更新到新的功能级别，可为系统提供新驱动程序或软件增强等附加功能。

警告: 请勿忽略更新到服务包增补程序

如果没有选择更新到服务包增补程序，系统将保持先前的功能级别，且您将只在有限的时间内（对于 SUSE Linux Enterprise 10 SP2，该期限现在延长到 6 个月）获得错误修复和安全更新。因此，为了获得持续系统完整性，建议尽早切换到新功能级别。

其他更新方法有手动运行 rug 命令、使用增补程序 CD（请参见第 8.3.7 节“从增补程序 CD 更新”[122]），或使用本地安装的 SMT 系统。

从 SP 媒体引导以进行更新

从 SP 媒体引导并选择更新作为 YaST 中的安装方式。关于详细信息和如何完成更新，请参阅第 9.1.3 节“使用 YaST 进行更新”[172]。

用 YaST 联机更新启动

在启动 YaST 联机更新以更新到 SP 功能级别之前，请确保符合以下要求：

- 整个更新过程中系统必须联机，因为此过程需要访问 Novell Customer Center。
- 如果安装涉及第三方软件或附加软件，请在另一台机器上测试此过程，以确保更新不会破坏相关性。
- 确保整个过程成功完成。否则系统将不一致。

先完全安装服务包 1 之后，才能更新到服务包 2。如果尚未安装服务包 1，请先如“SUSE Linux Enterprise GA 到 SP1 和 SP2”一节 [181]中所述更新到服务包 1。

图 9.1 服务包 1 包管理更新

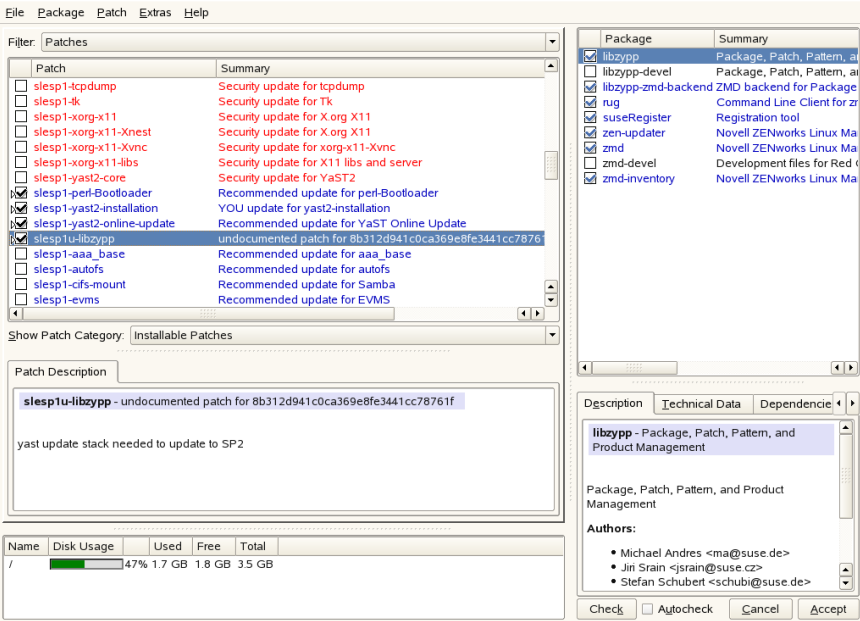
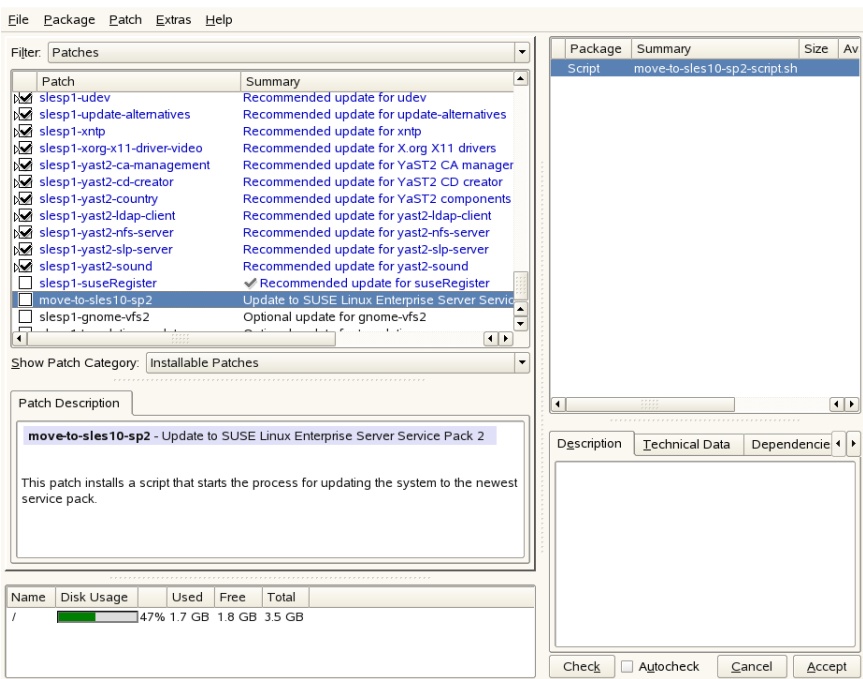


图 9.2 更新到 Service Pack 2



注意

在使用“YaST 联机更新”的更新迁移期间，ZMD 堆栈被更新且 ZMD 守护程序也会重新启动。因此，建议避免使用任何其他软件管理工具，例如 `rug`、`zen-updater`、`zen-installer` 和 `zen-remover`。建议在迁移期间退出 `zen-updater`。

- 1 在运行的 SUSE Linux Enterprise 系统中，选择 **计算机 > YaST > 软件 > 联机更新**。

如果不是以 `root` 用户登录，系统提示时输入 `root` 密码。

- 2 则显示 **联机更新** 对话框。会预先选择几个增补程序。向下滚动增补程序列表，校验确实已预先选择了与管理相关的增补程序和 SUSE Linux Enterprise 10 SP2 维护堆栈更新 (`slesplu-libzypp`)。然后按接受以应用选定更新。

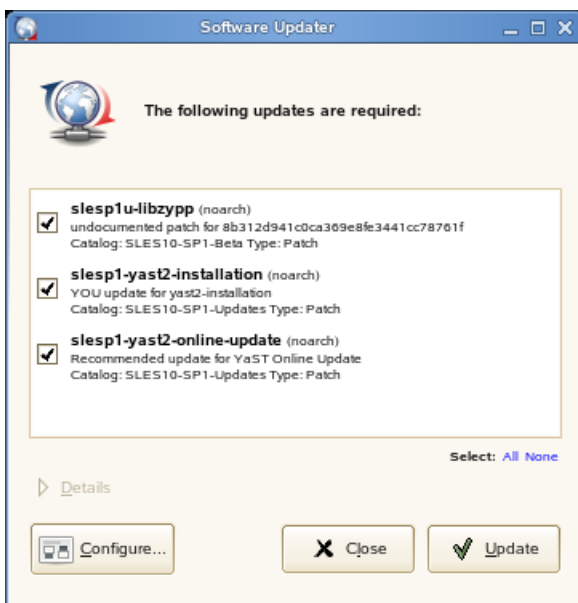
- 3 增补程序下载和安装对话框将跟踪进度日志。当总进度达到 100% 时，请单击关闭。然后联机更新将自动重新启动。
- 4 重新启动后，按接受以应用所有可用更新和一个新内核。安装后，必须重引导系统。
- 5 在重新启动的联机更新中，现在应向下滚动增补程序列表并选择更新到服务包 2 (move-to-sled10-sp2)，如图 9.2 “更新到 Service Pack 2” [178] 中所示。在弹出窗口中，单击接受确认已开始更新到服务包功能级别的过程。

move-to-sled10-sp2 增补程序标记为可选。如果没有选择它，您的系统将停留在 SP1 功能级别，且您将只在有限的时间里（SP2 可用后 6 个月）可以获得错误修复和安全更新。
- 6 增补程序下载和安装对话框跟踪迁移增补程序安装的进展日志。当总进展达到 100% 时，请单击完成。
- 7 再次启动 YaST 联机更新。应用 product-sled10-sp2 和 slesp2o-sp2_online 增补程序，将系统更新到 SP2 级别。如果在以前的步骤中安装了 move-to-sled10-sp2，会预先选择这两个增补程序（因为是必需的）。
- 8 单击关闭以完成到 SUSE Linux Enterprise 10 SP2 的更新，然后重引导。

使用 zen-updater 启动

请先确保满足“用 YaST 联机更新启动”一节 [177] 中列出的要求，再使用 zen-updater 启动联机更新以更新到 SP 功能级别。

图 9.3 应用 SLE10 SP2 维护堆栈更新



- 1 在正在运行的 SUSE Linux Enterprise 系统中，通过单击底部的更新程序图标启动 zen-updater。

提示: 唤醒 ZMD

如果看到 **ZMD** 未在运行讯息，请以 root 身份通过 `rczmd status` 检查 **ZMD** 是否处于活动状态。如果出现问题，请输入 `rug restart --clean` 以强制重新启动并清理 **ZMD** 及其数据库。

如果不是以 root 用户登录，系统提示时输入 root 密码。

- 2 应用系统所有可用的维护更新。
- 3 应用 SLE10 SP2 维护堆栈更新(slesp1u-libzypp)。应预先选择这些项目，单击更新可启动此步骤。解析所有依赖性后，单击应用。完成时通过单击关闭而确认弹出的讯息。
- 4 在重新启动的软件更新程序中，向下翻页并选择可选的 `move-to-sled10-sp2` 增补程序并应用。如果没有选择它，您的系统将

停留在 SP1 功能级别，且您将只在有限的时间里（SP2 可用后 6 个月）可以获得错误修复和安全更新。

- 5 在软件更新程序中，应用 `product-sled10-sp2` 和 `slesp2o-sp2_online` 增补程序以将系统更新为 SP2 级别。如果在之前的步骤中安装了 `move-to-sled10-sp2`，则这两个增补程序都是必需的，因此会预先选择。
- 6 单击关闭以完成到 SUSE Linux Enterprise 10 SP2 的更新，然后重引导。

使用 rug

有关 rug 命令行工具的背景信息，请参见第 8.14 节“从命令行使用 rug 更新包”[161]。如果需要编写脚本的解决方法来进行更新，请使用 rug。

请先确保满足“用 YaST 联机更新启动”一节 [177]中列出的要求，再使用 rug 启动联机更新以更新到 SP 功能级别。

下面是将系统迁移到 SP2 增补程序级别所需的最小命令序列：

```
rug up -t patch -g security && rug ping -a
# the following command will also install slesplu-libzyp
rug up -t patch -g recommended && rug ping -a
rug in -t patch move-to-sled10-sp2 && rug ping -a
rug refresh
rug up -t patch -g recommended && rug ping -a
reboot
```

注意

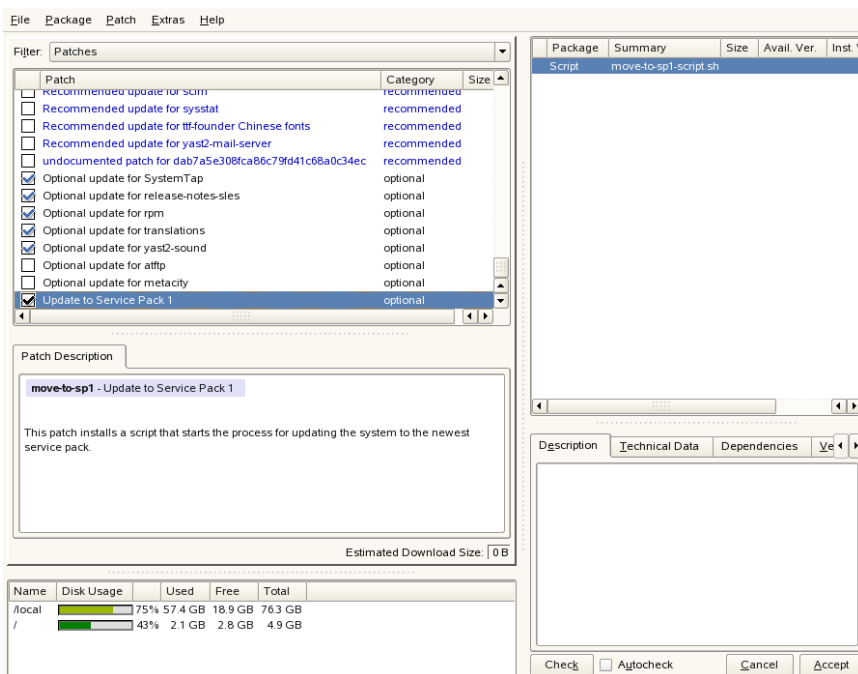
`rug ping -a` 确保在先前的 rug 命令后已完成 ZMD 初始化。

SUSE Linux Enterprise GA 到 SP1 和 SP2

注意

仅当您的系统仍然在 GA 增补程序级别运行时，以下步骤才适用。

图 9.4 更新到 Service Pack 1



- 1 在运行的 SUSE Linux Enterprise 系统 (GA) 中，选择计算机 > YaST > 软件 > 联机更新。

如果不是以 root 用户登录，系统提示时输入 root 密码。

- 2 则显示联机更新对话框。如图 9.4 “更新到 Service Pack 1” [182] 中所示，下滚增补程序列表并选择更新到 Service Pack 1。在弹出窗口中，单击接受确认已开始更新到服务包功能级别的过程。
- 3 增补程序下载和安装对话框跟踪迁移增补程序安装的进展日志。当总进展达到 100% 时，请单击完成。
- 4 再次运行联机更新。一旦完成，在增补程序下载和安装中单击关闭。在第二次运行期间，YaST 将安装内核和所有其他软件。
- 5 在过程日志末尾看到 *Installation Finished* 报告时，单击完成。

6 要完成更新，请手动重引导系统以激活新内核。

现在，SUSE Linux Enterprise 已在 SP1 增补程序级别运行了。继续“[用 YaST 联机更新启动](#)”一节 [177]以将系统升级为 SP2 增补程序级别。

9.3 从 V9 到 V10 的软件更改

以下内容详细介绍了 V9 到 V10 各方面进行的更改。本摘要指出了是否已完全重置基本设置、是否已将配置文件移动到其他位置以及是否对常用应用程序进行了重大更改。此处将介绍用户级别或管理员级别的重大修改，它将影响系统的日常使用。

注意: 从 SLES 10 到 SLES 10 SP 1 的软件更改

要查看从 SUSE Linux Enterprise Server 10 到 SUSE Linux Enterprise Server 10 SP1 的软件和配置更改的详细列表，请参阅 `service pack` 的发行说明。在已安装的系统用 YaST 发行说明模块查看它们。

9.3.1 多个内核

可以同时安装多个内核。此功能旨在支持管理员从一个内核升级到另一个内核，方法是安装新内核，确认新内核能按预期运行后，卸载旧内核。尽管 YaST 尚不支持此功能，仍可以使用 `rpm -i package.rpm` 通过 shell 轻松地安装和卸载内核。

默认的引导加载程序菜单中包含一个内核项。在安装多个内核前，为这些加装的内核添加一个对应项很有用，这样便于选择这些内核。在安装新内核前处于活动状态的内核可以作为 `vmlinuz.previous` 和 `initrd.previous` 进行访问。通过创建类似于默认项的引导加载程序项，并令此项指向 `vmlinuz.previous` 和 `initrd.previous` 而不是 `vmlinuz` 和 `initrd`，可以访问先前活动的内核。另外，GRUB 和 LILO 支持带通配符的引导加载程序项。有关详细信息，请参考 GRUB 信息页 (`info grub`) 和 `lilo.conf` (5) 手册页。

9.3.2 内核模块的更改

以下内核模块已不再可用：

- `km_fcdsl` — avm FRITZ!Card Dsl
- `km_fritzcap`i — avm FRITZ! ISDN 适配器

对以下内核模块包的内部进行了更改：

- `km_wlan` — 用于无线 lan 卡的各种驱动程序。Atheros WLAN 卡的 `madwifi` 驱动程序已经从 `km_wlan` 中去除。`madwifi` 可用作一个独立包。

由于技术原因，必须除去对 Ralink WLAN 卡的支持。分发中未包含以下模块并且以后也不会添加这些模块：

- `ati-fglrx` — ati FIREGL 显卡
- `nvidia-gfx` — nvidia GFX 驱动程序
- `km_smartlink-softmodem` — smart Link 软调制解调器

9.3.3 tar 语法更为严格

`tar` 的使用语法现在更加严格。`tar` 选项必须出现在指定文件或目录之前。追加选项（诸如 `--atime-preserve` 或 `--numeric-owner`）在文件或目录指定之后，会使 `tar` 失败。请检查备份脚本。诸如以下的命令不再有效：

```
tar czf etc.tar.gz /etc --atime-preserve
```

关于更多信息，请参见 `tar` 信息页。

9.3.4 用于网络鉴定的 Kerberos

Kerberos 已代替 heimdal 成为默认的网络鉴定方法。不能自动转换现有的 heimdal 配置。在系统更新过程中，配置文件的备份副本将按表 9.1 “备份文件” [184] 中所示创建。

表 9.1 备份文件

旧文件	备份文件
<code>/etc/krb5.conf</code>	<code>/etc/krb5.conf.heimdal</code>

旧文件	备份文件
/etc/krb5.keytab	/etc/krb5.keytab.heimdal

客户机配置 (/etc/krb5.conf) 与 heimdal 的配置很相似。如果没有任何特殊配置，完全可以将 kpasswd_server 参数替换为 admin_server。

不能复制与服务器相关 (kdc 和 kadmind) 的数据。系统更新后，旧的 heimdal 数据库在 /var/heimdal 下仍可用；MIT kerberos 在 /var/lib/kerberos/krb5kdc 下维护其数据库。更多信息请参见 [第 41 章 网络鉴定 — Kerberos](#) [675]。

9.3.5 Hotplug 事件由 udev 守护程序处理

Hotplug 事件现在已经完全由 udev 守护程序 (udev) 处理。不再使用 /etc/hotplug.d 和 /etc/dev.d 中的事件多路转换器系统。相反，udev 会根据规则直接调用所有的热插拔帮助程序工具。Udev 和其他包提供 Udev 规则和帮助程序工具。

9.3.6 安装期间激活防火墙

为提高安全性，安装结束时在建议对话框中激活附带的防火墙解决方案 SUSEFirewall2。这意味着最初将关闭所有端口，如果需要，可以在建议对话框中将其打开。默认情况下，不能从远程系统登录。此外，还会影响网络浏览和多路广播应用程序，如 SLP、Samba (“网络邻居”) 以及某些游戏程序。您可以使用 YaST 对防火墙设置进行微调。

如果在安装或配置服务过程中需要进行网络访问，则相应的 YaST 模块将为所有内部和外部接口打开所需的 TCP 和 UDP 端口。如果不想这样，则在 YaST 模块中关闭端口或指定其他具体的防火墙设置。

9.3.7 KDE 和 IPv6 支持

默认情况下，不能在 KDE 中启用 IPv6 支持。您可以使用 YaST 的 /etc/sysconfig 编辑器启用该支持。禁用此功能的原因在于 IPv6 地址得不到所有

因特网服务提供者的充分支持，从而导致浏览万维网时出现错误讯息，并且显示万维网网页时出现延迟。

9.3.8 联机更新和增量包

联机更新现支持一种特殊的RPM包，这种包仅储存与给定基础包不同的二进制内容。这项技术显著减少了包的大小并缩短了下载时间。不过，因需要重组最终包，致使CPU负载加重。关于技术详细信息，请参见 `/usr/share/doc/packages/deltarpm/README`。

9.3.9 打印系统配置

安装结束时（建议对话框），必须在防火墙配置中打开打印系统所需的端口。CUPS 需要端口 631/TCP 和端口 631/UDP，要执行一般操作，不应关闭这两个端口。要通过 LPD 或 SMB 进行打印，还应该打开端口 515/TCP（用于以前的 LPD 协议）和 Samba 使用的端口。

9.3.10 更改为 X.Org

兼容性链接简化了从 XFree86 到 X.Org 的更改，这些链接支持访问使用以前名称的重要文件和命令。

表 9.2 命令

XFree86	X.Org
XFree86	Xorg
xf86config	xorgconfig
xf86cfg	xorgcfg

表 9.3 /var/log中的日志文件

XFree86	X.Org
XFree86.0.log	Xorg.0.log
XFree86.0.log.old	Xorg.0.log.old

在更改为 X.Org 的过程中，将包的名称从 XFree86* 重命名为 xorg-x11*。

9.3.11 X.Org 配置文件

配置工具 SaX2 将 X.Org 配置设置写入 /etc/X11/xorg.conf。在从头安装过程中，不会创建从 XF86Config 到 xorg.conf 的任何兼容性链接。

9.3.12 取消了 XView 和 OpenLook 支持

已删除包 xview、xview-devel、xview-devel-examples、olvwm 和 xtoolpl。以前只提供了 XView (OpenLook) 基础系统。在系统更新后将不再提供 XView 库。更重要的是，OLVWM (OpenLook Virtual Window Manager) 也将不再可用。

9.3.13 适用于 X11 的终端模拟器

已去除了多个终端模拟器，原因是不再进行维护或者在默认环境下不能使用，尤其是不支持 UTF-8。SUSE Linux Enterprise Server 提供各种标准终端，如 xterm、KDE 终端、GNOME 终端和 mlterm（适用于 X 的多语言终端模拟器，有可能代替 aterm 和 eterm）。

9.3.14 OpenOffice.org (OOo)

目录

OOo 现在安装在 /usr/lib/ooo-2.0 而不是 /opt/OpenOffice.org 中。用户设置的默认目录现在是 ~/.ooo-2.0 而不是 ~/OpenOffice.org1.1。

包装程序

一些新包装程序可用于启动 OOo 部件。新名称显示在 表 9.4 “包装程序” [188] 中。

表 9.4 包装程序

旧名称	新建
/usr/X11R6/bin/OOo-calc	/usr/bin/oocalc
/usr/X11R6/bin/OOo-draw	/usr/bin/oodraw
/usr/X11R6/bin/OOo-impress	/usr/bin/ooimpress
/usr/X11R6/bin/OOo-math	/usr/bin/oomath
/usr/X11R6/bin/OOo-padmin	/usr/sbin/oopadmin
/usr/X11R6/bin/OOo-setup	—
/usr/X11R6/bin/OOo-template	/usr/bin/oofromtemplate
/usr/X11R6/bin/OOo-web	/usr/bin/ooweb
/usr/X11R6/bin/OOo-writer	/usr/bin/oowriter
/usr/X11R6/bin/OOo	/usr/bin/ooffice
/usr/X11R6/bin/OOo-wrapper	/usr/bin/ooo-wrapper

包装程序现在支持使用选项 `--icons-set` 在 KDE 和 GNOME 图标之间进行切换。不再支持以下选项：`--default-configuration`、`--gui`、`--java-path`、`--skip-check`、`--lang`（语言现在由区域设置决定）、`--messages-in-window` 和 `--quiet`。

KDE 和 GNOME 支持

可以在 OpenOffice_org-kde 和 OpenOffice_org-gnome 包中获得 KDE 和 GNOME 扩展。

9.3.15 混音器 kmix

预设混音器 `kmix` 作为默认设置。对于高端硬件，还提供其他混音器，如 `QAMix/KAMix`、`envy24control`（仅限 `ICE1712`）或 `hdspmixer`（仅限 `RME Hammerfall`）。

9.3.16 DVD 烧录

以往，从 `cdrecord` 包中应用 `cdrecord` 二进制文件的增补程序以支持 DVD 烧录功能。而现在安装的新二进制文件 `cdrecord-dvd` 即提供这个增补程序。

`dvd+rw-tools`包中的 `growisofs` 程序现在支持烧录所有 DVD 媒体（`DVD+R`、`DVD-R`、`DVD+RW`、`DVD-RW`、`DVD+RL`）。尝试用此程序来代替经过修补的 `cdrecord-dvd`。

9.3.17 在内核提示符处启动手动安装

手动安装方式已不再出现在引导加载程序屏幕上。不过，您仍可以在引导提示符处使用 `manual=1` 令 `linuxrc` 转换为手动方式。通常不必这样做，因为您可以在内核提示符处直接设置安装选项，例如 `textmode=1` 或将 `URL` 设为安装源。

9.3.18 JFS：不再支持

由于 JFS 的技术问题，不再支持 JFS。其中虽仍有内核文件系统驱动程序，但 `YaST` 不提供具有 JFS 的分区。

9.3.19 用 AIDE 替换 Tripwire

作为入侵检测系统，请使用 `AIDE`（包名称为 `aide`），它是在 `GPL` 下发布的。`SUSE Linux` 上不再提供 `Tripwire`。

9.3.20 PAM 配置

新配置文件（包含更多信息的注释）

common-auth
auth 部分的默认 PAM 配置

common-account
帐户部分的默认 PAM 配置

common-password
密码更改的默认 PAM 配置

common-session
会话管理的默认 PAM 配置

您应该在特定于应用程序的配置文件中包括这些默认的配置，因为修改和维护一个文件比修改和维护系统中以往有的约 40 个文件要容易些。如果您稍后安装某个应用程序，该程序将继承已应用的更改，而且管理员也不必记着调整该配置。

所做的更改很简单：如果您使用下面的配置文件（应该是多数应用程序的默认配置）：

```
##PAM-1.0
auth      required      pam_unix2.so
account   required      pam_unix2.so
password  required      pam_pwcheck.so
password  required      pam_unix2.so      use_first_pass use_authtok
#password required      pam_make.so      /var/yp
session   required      pam_unix2.so
```

可以将其改为：

```
##PAM-1.0
auth      include      common-auth
account   include      common-account
password  include      common-password
session   include      common-session
```

9.3.21 使用 su 成为超级用户

默认情况下，调用 su 成为 root 并没有为 root 设置 PATH。如果要更改 su 的默认行为，则调用 su - 使用 root 的完整环境启动登录 shell，或者在 /etc/default/su 中将 ALWAYS_SET_PATH 设置为 yes。

9.3.22 powersave 包中的更改

/etc/sysconfig/powersave 中的配置文件已更改：

表 9.5 拆分 /etc/sysconfig/powersave 中的配置文件

旧名称	现在拆分为
/etc/sysconfig/powersave/ common	common
	cpufreq
	事件
	battery
	休眠
	thermal

/etc/powersave.conf 已不再使用。现有变量已移至 [表 9.5 “拆分 /etc/sysconfig/powersave 中的配置文件”](#) [191] 中列出的文件。如果更改 /etc/powersave.conf 中的“event”变量，则必须在 /etc/sysconfig/powersave/events 中进行调整。

休眠状态的名称从：

- 暂停（ACPI S4、APM 暂停）
- 待机（ACPI S3、APM 待机）

收件人：

- 暂停到磁盘（ACPI S4、APM 暂停）
- 暂停到 RAM（ACPI S3、APM 暂停）
- 待机（ACPI S1、APM 待机）

9.3.23 Powersave 配置变量

为保持一致性更改 powersave 配置变量的名称，但 sysconfig 文件仍保持不变。有关详细信息，请参见 [第 28.5.1 节“配置 powersave 包”](#) [500]。

9.3.24 PCMCIA

cardmgr 不再管理 PC 卡。而是与 Cardbus 卡和其他子系统相同，由内核模块管理 PC 卡。通过 hotplug 执行所有需要的操作。pcmcia 启动已去除的脚本，并将 cardctl 替换为 pccardctl。有关更多信息，请参见 `/usr/share/doc/packages/pcmciautils/README.SUSE`。

9.3.25 设置 D-BUS 进行 .xinitrc 中的进程间通信

现在许多应用程序都依靠 D-BUS 进行进程间通信 (IPC)。调用 `dbus-launch` 会启动 `dbus-daemon`。系统范围内的 `/etc/X11/xinit/xinitrc` 使用 `dbus-launch` 来启动窗口管理器。

如果具有本地 `~/.xinitrc` 文件，则必须相应地进行更改。否则像 `f-spot`、`banshee`、`tomboy` 这样的应用程序或网络管理器 `banshee` 可能会失败。保存旧的 `~/.xinitrc`。接着使用以下命令将新的模板文件复制到主目录中：

```
cp /etc/skel/.xinitrc.template ~/.xinitrc
```

最后，从已保存的 `.xinitrc` 添加定制的内容。

9.3.26 NTP 相关的文件已重命名

因为要与 LSB 兼容（Linux 标准库），大多数配置文件和初始化脚本都从 `xntp` 重命名为 `ntp`。这些新文件名是：

- `/etc/slp.reg.d/ntp.reg`
- `/etc/init.d/ntp`
- `/etc/logrotate.d/ntp`
- `/usr/sbin/rcntp`
- `/etc/sysconfig/ntp`

9.3.27 GNOME 应用程序的文件系统更改通知

为了确保正常运行，GNOME 应用程序依赖于文件系统更改通知支持。仅对于本地文件系统，安装 `gamin` 包（推荐）或运行 FAM 守护程序。对于远程文件系统，在服务器和客户机上都运行 FAM 并通过 FAM 打开 RPC 调用的防火墙。

GNOME（`gnome-vfs2` 和 `libgda`）包含一个包装程序，它选择 `gamin` 或 `fam` 来提供文件系统更改通知：

- 如果 FAM 守护程序未运行，最好使用 `gamin`（理由：Inotify 只有 `gamin` 才支持，它对于本地文件系统更为高效）。
- 如果 FAM 守护程序在运行，最好用 FAM（理由：如果 FAM 在运行，可能需要远程通知，只有 FAM 支持该功能）。

9.3.28 启动 FTP 服务器 (vsftpd)

默认情况下，`xinetd` 不再启动 `vsftpd` FTP 服务器。它现在是一个独立守护程序，必须使用 YaST 运行时编辑器来配置它。

9.3.29 Firefox 1.5: Url Open 命令

使用 Firefox 1.5 时，应用程序打开 Firefox 实例或窗口的方法已经更改。新方法在以前的版本中已说明了一部分，在以前的版本中行为是在包装程序脚本中实施的。

如果应用程序不使用 `mozilla-xremote-client` 或 `firefox -remote`，则不需要更改任何内容。否则，打开 `url` 的新命令是 `firefox url`，并且此时 `firefox` 是否已经运行并不重要。如果已经正在运行，则它遵循从其他应用程序打开链接中配置的自选设置。

从命令行，可以通过使用 `firefox -new-window url` 或 `firefox -new-tab url` 来影响行为。

部分 II. 管理

GNOME 配置（供管理员使用）

本章讨论以下主题：

- 第 10.1 节 “默认情况下使用 **GConf**” [198]
- 第 10.2 节 “自定义菜单” [220]
- 第 10.3 节 “安装主题” [231]
- 第 10.4 节 “配置字体” [237]
- 第 10.5 节 “**MIME** 类型” [238]
- 第 10.6 节 “设置屏幕保护程序” [240]
- 第 10.7 节 “会话管理” [241]
- 第 10.8 节 “提升性能” [242]
- 第 10.9 节 “隐藏目录” [249]
- 第 10.10 节 “配置 **SMB** 打印机的安全性说明” [251]
- 第 10.11 节 “禁用 **GNOME Desktop** 功能” [252]
- 第 10.12 节 “自动启动应用程序” [254]
- 第 10.13 节 “自动装入和管理媒体设备” [255]
- 第 10.14 节 “更改首选应用程序” [255]

- [第 10.15 节 “用 Sabayon 管理配置文件”](#) [255]
- [第 10.16 节 “添加文档模板”](#) [259]

10.1 默认情况下使用 GConf

GConf 是一种用于存储应用程序自选设置的系统，它简化了用户自选设置的管理。管理员可使用 GConf 执行以下操作：

- 为所有用户设置特定自选设置的必须值。这可控制用户是否能够更新特定自选设置。
- 为所有用户设置特定自选设置的默认值。
- 对自选设置定义文件中指定的自选设置使用建议值。
- 阅读有关每个自选设置的文档。

当自选设置值更改时，GConf 还可本地或通过网络通知应用程序。因此，更改自选设置时，使用该自选设置的所有应用程序都会立即更新。

GConf 可提供自选设置数据库（类似于简单的文件系统）。此文件系统包含层次结构组织的密钥。每个密钥可能是包含多个密钥的目录，或密钥具有值。例如，密钥 `/apps/metacity/general/titlebar_font` 包含一个整数值，该值提供 Metacity 窗口管理器的标题栏字体大小。

GConf 具有以下组件：

- [第 10.1.1 节 “GConf 储存库”](#) [199]
- [第 10.1.2 节 “GConf 守护程序”](#) [203]
- [第 10.1.3 节 “GConf 命令行工具”](#) [204]
- [第 10.1.8 节 “配置编辑器”](#) [218]

10.1.1 GConf 储存库

GConf 储存库中的每个自选设置都表示为密钥值对。GConf 自选设置密钥是储存库中的一个元素，它与一个应用程序自选设置对应。例

如，`/apps/gnome-session/options/show_splash_screen` 自选设置密钥与“会话”自选设置工具中的“登录时显示启动屏幕”选项对应。GNOME Desktop 用户界面不包含 GConf 储存库中的任何自选设置密钥。例如，“面板”自选设置工具内不包含与 `/apps/panel/global/tooltips_enabled` 密钥对应的选项。

储存库的构造类似于简单的分级文件系统。储存库包含以下对象：

- 目录，与使用 GConf 储存库的应用程序对应。例如，文件系统包含目录 `/apps/metacity`。
- 子目录，与自选设置的类别对应。例如，文件系统包含目录 `/apps/metacity/general`。
- 特殊文件，这些文件列出目录中的自选设置密钥并包含有关密钥的信息。例如，如果密钥与 HTTP 代理自选设置有关，则包含有关这些密钥的信息的文件位于目录 `/system/http_proxy` 中。
- `/schemas` 目录包含描述所有自选设置密钥的文件。

通常，自选设置密钥具有简单的值，如字符串、整数或字符串列表和整数列表。储存库中自选设置密钥的格式取决于用于读取储存库的后端模块。以下是当使用可扩展标记语言（XML）读取储存库时的 `/desktop/gnome/interface/font_name` 自选设置密钥示例：

```
<entry name="font_name" mtime="1038323555" muser="user123" type="string">
<stringvalue>Sans 10</stringvalue>
</entry>
```

注意

当本指南引用自选设置密钥时，会向密钥名称添加到密钥的路径。例如，将作为 `/desktop/gnome/interface/font_name` 引用 `/desktop/gnome/interface` 中的 `font_name` preference 密钥。

GConf 配置源

GConf 存储库包含成为配置源的一系列存储位置。配置源列在 `/etc/opt/gnome/opt/gnome/gconf/gconf-version-number/` 路径下的 GConf 路径文件中。每个用户都有一个路径文件。路径文件指定每个配置源的以下信息：

- 用于读取存储库的后端模块
- 存储库的许可权限
- 存储库的位置

GConf 路径文件还包含包括指示信息。默认情况下，GConf 路径文件的内容如下所示：

```
xml:readonly:/etc/opt/gnome/opt/gnome/gconf/gconf.xml.mandatory
include /etc/opt/gnome/opt/gnome/gconf/2/local-mandatory.path
include "${HOME}/.gconf.path"
include /etc/opt/gnome/opt/gnome/gconf/2/local-defaults.path
xml:readwrite:${HOME}/.gconf
xml:readonly:/etc/opt/gnome/opt/gnome/gconf/gconf.xml.defaults
```

当 GConf 搜索自选设置值时，它会以路径文件中指定的顺序读取配置源。下表描述路径文件中的配置源：

表 10.1 路径文件中的配置源

配置源	说明
强制	此配置源的权限设置为“只读”。用户无法覆盖此源中的值，因此源中的自选设置为必需。

配置源	说明
用户	配置源存储在用户主目录中的 <code>.gconf</code> 目录中。用户设置自选设置时，会将新的自选设置信息添加到此位置。 可使用“配置编辑器”来修改用户配置源。
默认	此配置源包含默认自选设置。

路径文件中的配置源的顺序确保必需自选设置覆盖用户自选设置。顺序还确保用户自选设置覆盖默认自选设置。即，GConf 通过以下优先级顺序应用自选设置：

1. 必需自选设置
2. 用户指定的自选设置
3. 默认自选设置

GConf 路径文件中的包括指示信息使系统管理员能够指定其他配置源：

表 10.2 其他配置源

包含的配置源	说明
<code>/etc/opt/gnome/opt/gnome/gconf/2/local-mandatory.path</code>	存储特定系统的必需自选设置值。
<code>\${HOME}/.gconf.path</code>	指定用户主目录中 <code>.gconf.path</code> 文件中配置源的位置。
<code>/etc/opt/gnome/opt/gnome/gconf/2/local-defaults.path</code>	存储特定系统的默认自选设置值。

GConf 模式

GConf 模式是一个用于 GConf 模式密钥和 GConf 模式对象的集合术语。下表说明了模式密钥和模式对象以及它们与自选设置密钥的关系：

表 10.3 模式密钥和对象

项目	说明
自选设置密钥	GConf 存储库中的元素，与应用程序自选设置对应。
模式密钥	存储自选设置密钥的模式对性的密钥。
模式对象	配置源中的元素，包含有关自选设置密钥的信息，例如以下信息： <ul style="list-style-type: none">• 使用自选设置密钥的应用程序的名称• 自选设置密钥所需的值的类型（例如，整数和布尔值等等）• 自选设置密钥的默认值• 有关自选设置密钥的简短文档

以下是自选设置密钥、模式密钥和模式对象的示例：

表 10.4 自选设置密钥、模式密钥和模式对象示例

自选设置密钥：	/desktop/gnome/interface/font_name
模式密钥：	/schemas/desktop/gnome/interface/font_name
模式对象：	<pre><schema> <applyto>/desktop/gnome/interface/font_name</applyto> <key>/schemas/desktop/gnome/interface/font_name</key> <owner>gnome</owner> <type>string</type> <default>Sans 10</default> <locale name="C"></pre>

```
<short>Default font</short> <long>Name of the
default font used by gtk+.</long> </locale>
```

可将模式密钥与自选设置密钥关联。例如，以下
/desktop/gnome/interface/font_name 密钥包含模式密钥：

```
<entry name="font_name" mtime="1034873859"
schema="/schemas/desktop/gnome/interface/font_name"/>
```

将模式密钥与自选设置密钥关联时，自选设置会使用模式密钥的模式对象中所指定的建议值。建议值包含在模式对象中的 <default> 元素中。默认情况下，默认配置源中的所有自选设置密钥都与模式密钥关联。

模式通常存储在默认配置源中。

GConf 模式定义文件

模式生成于模式定义文件。模式定义文件定义特定应用程序中所有密钥的特征。模式定义文件具有 .schemas 扩展名。

模式定义文件包含在 /etc/opt/gnome/opt/gnome/gconf/schemas 目录中。可使用模式定义文件来创建新的配置源。

一些模式定义文件与 GNOME Desktop 用户界面的一部分紧密对应。例如，system_http_proxy.schemas 与“网络代理”自选设置工具对应。其他模式定义文件包含不在 GNOME Desktop 用户界面中的自选设置密钥。例如，/apps/panel/global/tooltips_enabled 密钥不存在。

GNOME Desktop 用户界面某些部分所包含的自选设置表示来自多个模式定义文件的自选设置密钥。例如，“键盘快捷方式”自选设置工具所包含的自选设置表示来自 panel-global-config.schemas 和 metacity.schemas 文件的密钥。

10.1.2 GConf 守护程序

GConf 守护程序称为 gconfd-2。当自选设置值更改时，它会通知应用程序。例如，可在“菜单和工具栏”自选设置工具中选择以在工具栏中只显示图标。在自选设置工具中选择此选项时，将会即时更新所有打开的应用程序上的工具栏。守护程序可本地运行，或通过网络访问守护程序。

GConf 守护程序的实例启动时将面向每个用户。用户无需处理复杂的问题，如认证和数据安全性。守护程序启动时，它会装载 GConf 路径文件。守护程序还管理应用程序和配置源之间的所有访问。

当应用程序请求自选设置密钥的值时，守护程序会如下搜索配置源：

1. 通过路径文件中指定的顺序来在每个配置源中搜索自选设置密钥的值。
2. 如果找到值，则返回值。
3. 如果未找到值，则通过路径文件中指定的顺序来在每个配置源中搜索与自选设置密钥对应的模式密钥。
4. 如果找到模式密钥，则检查模式密钥的值。
5. 如果模式密钥的值是模式对象，则返回模式对象 <default> 元素中的建议值。

GConf 守护程序还可超速缓存自选设置密钥值。所有应用程序都使用此超速缓存，因此应用程序只需访问配置源一次。

要终止 GConf 守护程序，请使用以下命令：

```
gconftool-2 --shutdown
```

10.1.3 GConf 命令行工具

GConf 包含称为 gconftool-2 的命令行工具。可使用 gconftool-2 来执行以下任务：

- 设置密钥的值
- 显示密钥的值
- 安装应用程序时，从模式定义文件安装模式

例如，可使用以下命令来显示 /desktop/gnome 目录和子目录中的所有密钥的值：

```
gconftool-2 --recursive-list /desktop/gnome
```


下表列出可与 `gconftool-2` 命令一起使用的一些选项：

表 10.5 *gconftool-2 选项*

选项	功能
<code>--all-dirs</code>	列出指定目录中的所有子目录。
<code>--all-entries</code>	显示指定目录中所有密钥的值。
<code>--config-source</code> <i>configuration-source</i>	与 <code>--direct</code> 选项一起使用以指定要使用的配置源。如果不使用此选项来指定配置源，则命令将在路径文件中的所有配置源上运行。
<code>--direct</code>	与 <code>--config-source</code> 选项一起使用以直接访问配置源。使用此选项时，GConf 会避开服务器。使用此选项之前，请确保 GConf 守护程序 <code>gconfd-2</code> 未运行。
<code>--dump</code>	生成列表，该列表包含指定 GConf 存储库目录中的所有自选设置密钥。列表包含 <code><gconfentryfile></code> 元素中所有密钥的 XML 说明。 例如，可重定向此选项的输出以生成列出了与面板配置相关的所有密钥的文件。可将 <code>--load</code> 选项与此文件一起使用。
<code>--获取</code>	显示指定的自选设置密钥的值。还显示指定模式密钥的模式对象中元素的值。
<code>--help</code>	显示有关 <code>gconftool-2</code> 命令的帮助讯息以及可与此命令一起使用的选项。
<code>--load=filename</code>	将配置源当前目录中的自选设置密钥的值设置为指定文件中的值。指定的文件必须在 <code><gconfentryfile></code> 元素中包含 XML 说明。

选项	功能
<code>--long-desc=description</code>	与 <code>--set-schema</code> 选项一起使用以指定模式密钥的长说明。
<code>--makefile-install-rule</code>	向应用程序安装模式定义文件。
<code>--owner=owner</code>	与 <code>--set-schema</code> 选项一起使用以指定模式密钥的拥有者。
<code>--recursive-list</code>	显示指定目录中所有子目录中的所有自选设置密钥的值。
<code>--recursive-unset</code>	将目录中所有子目录中的所有自选设置密钥的值从用户设置重置为默认配置源中的设置。
<code>--set</code>	<p>设置自选设置密钥的值并将值写入到用户配置源。将其与 <code>--type</code> 选项一起使用以指定希望设置的值的数据类型。例如，以下命令设置用户配置源中 <code>/apps/gnome-terminal/profiles/Default/background_color</code> key 的值：</p> <pre>gconftool-2 --set "/apps/gnome-terminal/profiles/Default/background_color" --type string "#000000"</pre> <p>还可将其与 <code>--direct</code> 选项和 <code>--config-source</code> 选项一起使用以将值写入到其他配置源中。</p>
<code>--set-schema</code>	<p>设置模式密钥中特性的值并将值写入到默认配置源。</p> <p>将其与以下选项一起使用以指定希望更新的特性：</p> <ul style="list-style-type: none"> • <code>--type</code> • <code>--short-desc</code>

选项	功能
	<ul style="list-style-type: none">• <code>--long-desc</code>• <code>--owner</code> <p>例如，以下命令在模式密钥中设置 <code>/apps/gnome-terminal/profiles/Default/background_color</code> 密钥的短说明：</p> <pre>gconftool-2 --set-schema "/schemas/apps/gnome-terminal/profiles/Default/background_color" --short-desc "Default background color of terminal"</pre>
<code>--short-desc=description</code>	与 <code>--set-schema</code> 选项一起使用以指定模式密钥的简短说明。
<code>--shutdown</code>	终止 GConf 守护程序。
<code>--type=data-type</code>	<p>设置自选设置密钥的值时，指定数据类型。当设置模式密钥中的特性值时，也可以使用此选项。 以下是有效数据类型：</p> <ul style="list-style-type: none">• 布尔• 浮点• 整数• 列表• 对• 字符串
<code>--unset</code>	将自选设置密钥值从用户设置重置为默认配置源中的设置。

选项	功能
<code>--usage</code>	显示有关 <code>gconftool-2</code> 命令的简短帮助讯息以及可与此命令一起使用的选项。

10.1.4 设置自选设置值

可设置自选设置密钥的必需值或默认值。在更改必需自选设置值或用户默认自选设置值之前，必须确保所有用户都没有运行 GConf 守护程序。

重要

更改必需自选设置值或用户默认自选设置值之前，必须确保所有用户已注销。

要设置自选设置密钥的必需值或默认值，请使用 `gconftool-2` 命令，如下所示：

```
gconftool-2 --direct --config-source configuration-source --type data-type
--set preference-keyvalue
```

例如，要将 `wwwproxy.xyz.com` 设置为必需 HTTP 代理主机，则使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/opt/gnome/gconf/gconf.xml.mandatory --type string
--set /system/http_proxy/host wwwproxy.xyz.com
```

用户不能覆盖此自选设置值。

还可使用 `gconftool-2` 命令来设置默认值。例如，要将默认工作空间数设置为 5，则使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/opt/gnome/gconf/gconf.xml.defaults --type int
--set /apps/metacity/general/num_workspaces 5
```

用户可以覆盖此自选设置值。

10.1.5 设置常规自选设置

以下章节说明如何向常规自选设置指派必需或默认值：

- “设置 HTTP 代理自选设置”一节 [209]
- “设置打印管理器自选设置”一节 [209]
- “设置工作空间数”一节 [210]
- “设置键盘无障碍操作性自选设置”一节 [210]
- “设置键盘快捷方式自选设置”一节 [211]
- “设置键盘快捷方式自选设置”一节 [211]

设置 HTTP 代理自选设置

要设置 HTTP 代理自选设置，可修改 `/system/http_proxy/` 中的自选设置密钥值。例如，要设置 HTTP 代理主机的必需值，则使用以下命令：

```
gconftool-2 --direct --config-source  
xml:readwrite:/etc/opt/gnome/opt/gnome/gconf/gconf.xml.mandatory --type string  
--set /system/http_proxy/host proxy-name
```

要设置 HTTP 代理主机的默认值，则使用以下命令：

```
gconftool-2 --direct --config-source  
xml:readwrite:/etc/opt/gnome/opt/gnome/gconf/gconf.xml.defaults --type string  
--set /system/http_proxy/host proxy-name
```

还可设置其他与 HTTP 代理相关的自选设置。有关更多信息，请参见 `system_http_proxy.schemas` 模式定义文件。

设置打印管理器自选设置

要设置打印管理器的自选设置，可修改 `/apps/gnome-print-manager location` 中的自选设置密钥值。例如，如果不希望用户查看其他用户的打印作业，可如下设置必需值：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.mandatory --type bool --set
/apps/gnome-print-manager/show_all_jobs false
```

要设置此自选设置的默认值，则使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.defaults --type bool --set
/apps/gnome-print-manager/show_all_jobs false
```

还可设置其他打印管理器自选设置。有关更多信息，请参见 `gnome-print-manager.schemas` 模式定义文件。

设置工作空间数

要设置必需工作空间数，可使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.mandatory --type int --set
/apps/metacity/general/num_workspaces integer
```

要设置默认工作空间数，可使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.defaults --type int --set
/apps/metacity/general/num_workspaces integer
```

还可设置其他窗口管理器自选设置。有关更多信息，请参见 `metacity.schemas` 模式定义文件。

设置键盘无障碍操作性自选设置

要设置键盘无障碍操作性自选设置，可修改 `/desktop/gnome/accessibility/keyboard location` 中的自选设置密钥值。例如，如果希望设置必需值以便启用键盘无障碍操作性功能，则使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.mandatory --type bool --set
/desktop/gnome/ accessibility/keyboard/enable true
```

要设置此自选设置的默认值，则使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.defaults --type bool --set
/desktop/gnome/
accessibility/keyboard/enable false
```

还可设置其他键盘操作性自选设置。有关更多信息，请参见 `desktop_gnome_accessibility_keyboard.schemas` 模式定义文件。

设置键盘快捷方式自选设置

要设置键盘快捷方式自选设置，可修改 `/apps/metacity/global_keybindings` 位置中的自选设置密钥值。例如，您可能会希望用户只使用 `Alt+F3` 键盘快捷方式来打开“运行应用程序”对话框。要设置此必需值，请使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.mandatory --type string --set
/apps/metacity/global_keybindings '<Alt>F3'
```

还可设置其他键盘快捷方式自选设置。有关更多信息，请参见 `metacity.schemas` 模式定义文件。

设置面板和面板对象自选设置

`panel-default-setup.entries` 文件指定 GNOME Desktop 中的以下面板细节：

- 面板数
- 面板类型
- 面板属性
- 面板内容

配置各个面板和面板对象是非常复杂的任务。必须首先理解 `panel-default-setup.entries` 文件的结构。有关详细信息，参见“[指定各个面板和面板对象](#)”一节 [212]。

要设置各个面板和面板对象的自选设置，必须在配置源中设置许多自选设置的值。执行此操作最简单的方式是将 `gconftool-2` 命令与 `--dump` and `--load` 选

项一起使用。有关详细信息，参见“[设置各个面板和面板对象的自选设置](#)”一节 [214]。

指定各个面板和面板对象

`panel-default-setup.entries` 文件包含指定面板和面板内容的部分，并且该文件指定模式密钥的值。此文件位于 `/etc/opt/gnome/gconf/schemas` 目录中。

`panel-default-setup.entries` 文件的结构如下所示：

1. 指定 GNOME Desktop 中面板、小程序和其他面板对象的常规结构的密钥。

以下密钥指定 GNOME Desktop 中显示的面板数、面板对象数和小程序数：

- `/apps/panel/default_setup/general/toplevel_id_list`
- `/apps/panel/default_setup/general/object_id_list`
- `/apps/panel/default_setup/general/applet_id_list`

这些密钥还向每个面板、面板对象和小程序指派标识符。例如，以下 `panel-default-setup.entries` 中的样本指定在 GNOME Desktop 中显示一个面板：

```
<entry>
  <key>toplevel_id_list</key>
  <schema_key>/schemas/apps/panel/general/toplevel_id_list
</schema_key>
  <value>
    <list type="string">
      <value>
        <string>bottom_panel</string>
      </value>
    </list>
  </value>
</entry>
```

在 `panel-default-setup.entries` 文件中，标识符 `bottom_panel` 标识底部边缘面板。

2. 指定面板属性的密钥。

面板属性密钥的结构如下所示：

/apps/panel/default_setup/toplevels/panel-name/panel-property-key

例

如，/apps/panel/default_setup/toplevels/bottom_panel/size
密钥指定底部面板的大小。

3. 指定面板对象、面板对象属性和驻留对象的面板的密钥。

例如，panel-default-setup.entries 中的以下示例指定位于底部面板左侧的“主菜单”对象：

```
<entrylist base="/apps/panel/default_setup/objects/main_menu">
  <entry>
    <key>object_type</key>
    <schema_key>/schemas/apps/panel/objects/object_type</schema_key>
    <value>
      <string>menu-object</string>
    </value>
  </entry>
  <entry>
    <key>toplevel_id</key>
    <schema_key>/schemas/apps/panel/objects/toplevel_id</schema_key>
    <value>
      <string>bottom_panel</string>
    </value>
  </entry>
  <entry>
    <key>position</key>
    <schema_key>/schemas/apps/panel/objects/position</schema_key>
    <value>
      <int>0</int>
    </value>
  </entry>
  .
  .
  .
</entrylist>
```

4. 指定小程序、小程序自选设置和驻留小程序的面板的密钥。

例如，panel-default-setup.entries 中的以下示例指定底部面板中的“窗口列表”小程序：

```
<entrylist base="/apps/panel/default_setup/applets/window_list">
  <entry>
    <key>object_type</key>
```

```

        <schema_key>/schemas/apps/panel/objects/object_type
    </schema_key>
    <value>
        <string>bonobo-applet</string>
    </value>
</entry>
<entry>
    <key>toplevel_id</key>
    <schema_key>/schemas/apps/panel/objects/toplevel_id
</schema_key>
    <value>
        <string>bottom_panel</string>
    </value>
</entry>
<entry>
    <key>position</key>
    <schema_key>/schemas/apps/panel/objects/position
</schema_key>
    <value>
        <int>2</int>
    </value>
</entry>
.
.
.
<entry>
    <key>bonobo_iid</key>
    <schema_key>/schemas/apps/panel/objects/bonobo_iid_type</schema_key>

    <value>
        <string>OAFIID:GNOME_WindowListApplet</string>
    </value>
</entry>
</entrylist>

```

OAFIID 是小程序的唯一标识符。要查找特定小程序的 OAFIID，请参见位于 `/usr/lib/bonobo/servers` 目录中小程序的 `.server` 文件。例如，以下 `GNOME_Wncklet_Factory.server` 节选显示“窗口列表”小程序的 OAFIID：

```

<oaf_server iid="OAFIID:GNOME_WindowListApplet"
type="factory" location="OAFIID:GNOME_Wncklet_Factory">

```

设置各个面板和面板对象的自选设置

- 1 登录 GNOME 会话，然后根据需要配置面板。

- 2 将 `--dump` 选项与 `gconftool-2` 命令行工具一起使用以生成包含面板配置 XML 说明的文件。

`--dump` 选项会生成一个列表，该列表包含指定 GConf 存储库目录中的所有自选设置密钥。

例如，以下命令会在称为 `my-panel-setup.entries` 的文件中创建默认面板配置的 XML 说明：

```
gconftool-2 --dump /apps/panel/profiles/default > my-panel-setup.entries
```

- 3 在文本编辑器中打开 `my-panel-setup.entries` 文件，然后根据需要修改文件。

例如，您可能会希望更改桌面项文件的位置。以下是使用 `--dump` 选项生成的文件的节选：

```
<entry>
  <key>objects/object_16/launcher_location</key>
  <schema_key>/schemas/apps/panel/objects/launcher_location
</schema_key>
  <value>
    <string>hadjaha-00adce02f7.desktop</string>
  </value>
</entry>
```

在以上示例中，您可能会希望将对 `hadjaha-00adce02f7.desktop` 的引用更改为可通用的其他桌面项文件。

使用 `--dump` 选项生成面板配置时，面板对象的位置为绝对位置。您可能会希望将这些位置更改为相对位置。位于面板最左侧的对象的位置值为 0。下一个对象的位置值为 1，并以此类推。如果希望对象位置为面板右侧的相对位置，则将 `right_stick` 密钥的值设置为 `True`。

- 4 将 `--load` 选项与 `gconftool-2` 命令行工具一起使用以将默认配置源的值设置为 `my-panel-setup.entries` 文件中的值。

例如，以下命令会将默认配置源中的密钥值设置为 `my-panel-setup.entries` 中的对应密钥值：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.defaults --load
my-panel-setup.entries
```

10.1.6 设置外观与使用体验自选设置

以下章节说明如何向外观与使用体验自选设置指派必需或默认值：

- “设置面板和面板对象自选设置”一节 [211]
- “设置背景自选设置”一节 [217]
- “设置启动图像自选设置”一节 [217]

设置字体自选设置

要设置字体自选设置，可修改两个自选设置密钥的值。下表显示要修改的密钥和这些密钥所对应的用户界面部分：

表 10.6 字体自选设置密钥

GConf 位置	用户界面组件
/desktop/gnome/interface/ font_name	字体自选设置工具，应用程序字体选项
/apps/nautilus/preferences/ desktop_font	字体自选设置工具，桌面字体选项

例如，要将 Sans 12 设置为必需应用程序字体，可使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.mandatory --type string --set
/desktop/gnome/interface/font_name "Sans 12"
```

要将 Palatino 12 设置默认桌面对象字体，可使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.defaults --type string --set
/apps/nautilus/preferences/desktop_font "palatino 12"
```

设置背景自选设置

要设置桌面背景的背景自选设置，可在 `/desktop/gnome/background` 中修改自选设置密钥的值。例如，要设置背景的必需图像，可使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.mandatory --type string --set
/desktop/gnome/background/picture_filename filename.png
```

要设置此自选设置的默认值，则使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.defaults --type string --set
/desktop/gnome/background/picture_filename filename.png
```

还可设置其他背景自选设置。有关更多信息，请参见 `desktop_gnome_background.schemas` 模式定义文件。

设置启动图像自选设置

要设置启动图像自选设置，可在 `/apps/gnome-session/options/` 中修改自选设置密钥的值。例如，如果不希望用户看到启动图像，可如下设置必需值：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.mandatory --type bool --set
/apps/gnome-session/options/show_splash_screen false
```

要设置此自选设置的默认值，则使用以下命令：

```
gconftool-2 --direct --config-source
xml:readwrite:/etc/opt/gnome/gconf/gconf.xml.defaults --type bool --set
/apps/gnome-session/options/show_splash_screen false
```

还可设置其他启动图像自选设置。有关更多信息，请参见 `gnome-session.schemas` 模式定义文件。

10.1.7 恢复默认自选设置值

要恢复用户的默认自选设置值，可使用以下命令：

```
gconftool-2 --direct --config-source user-configuration-source
--recursive-unset
```

将 `user-configuration-source` 替换为用户主目录中 `.gconf` 目录中的配置源。

此命令可将所有子目录中的所有自选设置密钥的值从用户设置重置为默认配置源中的设置。

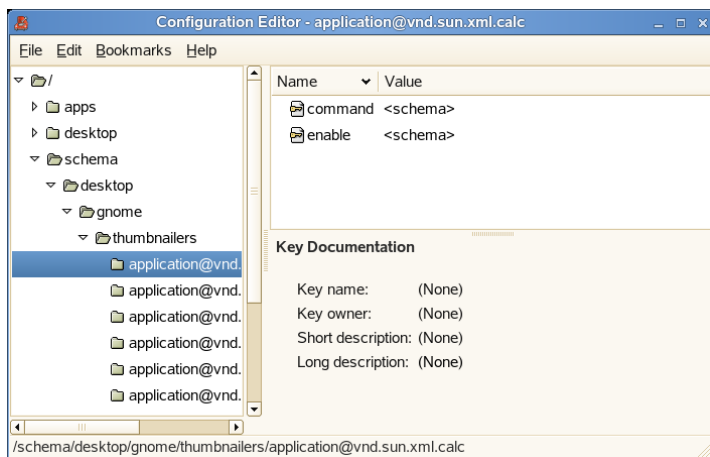
10.1.8 配置编辑器

“配置编辑器”（GConf 编辑器）使您能够查看和编辑 GConf 存储库中存储的密钥值。

要打开“配置编辑器”：

- 1 按 `Alt+F2` 打开“运行应用程序”对话框。
- 2 输入 `gconf-editor`，然后单击运行。

图 10.1 配置编辑器窗口



“配置编辑器”窗口包含以下窗格：

树

使您能够浏览 GConf 存储库中的目录和子目录。使用此窗格显示希望在修改窗格中修改的密钥。树窗格位于窗口的左侧。

修改

显示选定 GConf 存储库目录中的密钥。使用此窗格选择希望修改的密钥和修改密钥的值。修改窗格位于窗口右侧的上方。

修改窗格中密钥旁边的图标表示可输入的密钥值类型。例

如，`/system/http_proxy/use_http_proxy` 密钥旁边的选中标记图标表示可为密钥输入布尔值。

该图标还表示您是否可以编辑密钥的值。例如，模式密钥旁的密钥图标表示不能修改密钥的值。

文档

显示当前选定密钥的文档。可使用此窗格获取有关 GConf 自选设置密钥的更多信息。

可复制密钥的名称以便将密钥粘贴到其他应用程序中。还可向密钥添加书签。

修改密钥的值

- 1 使用树窗格显示希望在修改窗格中修改的密钥。
- 2 单击要修改的密钥。
- 3 要更改整数密钥或字符串密钥的值，请单击密钥的 *值列*，然后为密钥输入新的值。
- 4 要更改布尔密钥的值，请单击密钥的 *值列*。

复制密钥名称

- 1 在修改窗格中单击希望复制名称的密钥。
- 2 单击 *编辑 > 复制密钥名称*。
- 3 如果需要，可将密钥的名称粘贴到其他应用程序中。

对密钥使用书签

要访问书签中的密钥，可从“书签”菜单选择密钥。

添加书签

- 1 在修改窗格中单击希望添加书签的密钥。
- 2 单击 *书签 > 添加书签*。

删除书签

- 1 单击 *书签 > 编辑书签*。
将显示“编辑书签”对话框。
- 2 从左侧列表选择书签，然后单击 *删除*。
- 3 单击 *关闭*。

10.2 自定义菜单

SUSE Linux Enterprise10 让您可以以下列方式之一编辑菜单：

- [第 10.2.1 节 “用 Alacarte 自定义 GNOME 主菜单”](#) [220]
- [第 10.2.2 节 “使用桌面和目录项文件自定义 GNOME 菜单”](#) [228]

10.2.1 用 Alacarte 自定义 GNOME 主菜单

Alacarte 应用程序使您可以自定义 GNOME 主菜单。用户可以编辑自己的菜单，管理员可以用计算机上的帐户自定义所有用户的菜单。系统范围的菜单还可以分发到其他计算机。

注意

在后续的系统更新期间不会重写对主菜单所作的更改。生成最新的菜单视图后将应用更改。

本节包含下列内容：

- “安装 Alacarte”一节 [221]
- “启动 Alacarte”一节 [222]
- “编辑菜单”一节 [222]
- “更改系统范围的菜单”一节 [227]
- “将系统范围的菜单分发给其他计算机”一节 [227]

安装 Alacarte

安装 SUSE Linux Enterprise Desktop 时不会安装 Alacarte。要安装 Alacarte：

1 单击 *计算机控制中性系统YaST*。

将打开 YaST 控制中心。

2 （条件）如果受到提示，请输入 `root` 密码。

3 单击 *软件软件管理*。

4 在搜索框中，输入 Alacarte，然后单击 *搜索*。

5 选择 *Alacarte*，然后单击 *接受*。

6 受到提示时，插入指定的安装媒体。

例如，如果正在使用 CD，请插入 SUSE Linux Enterprise Desktop CD 2。

7 单击 *确定*。

当系统检查相关性时，请等待一会，然后再安装 Alacarte。

8 当系统询问是否要安装更多软件包时，单击 *否*。

Alacarte 现已安装，两个图标已添加到 GNOME 控制中心。

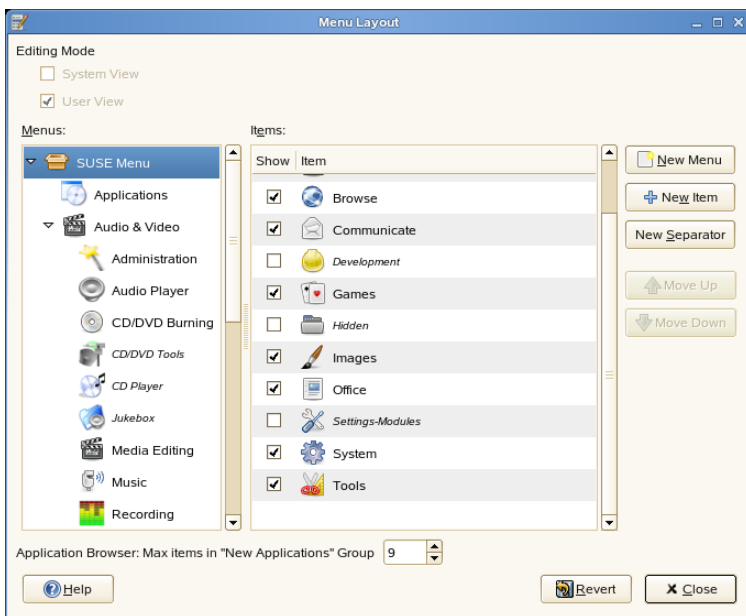
启动 Alacarte

- 1 单击计算机控制中心外观。
- 2 单击主菜单编辑器。

有两个主菜单编辑器图标。将鼠标放在它们上面，以确定哪一个用于系统范围的更改，哪一个用于您自己的本地菜单。如果正在为系统上的所有用户修改菜单或者想要将菜单分发到其他计算机，请使用系统范围的版本。使用常规版本来修改您自己的菜单。

将打开菜单布局窗口。

图 10.2 Alacarte 菜单布局窗口



您现在可以编辑菜单。

编辑菜单

本节描述了以下可以编辑主菜单的方式：

- “查找菜单项”一节 [223]
- “重新排列菜单项”一节 [224]
- “创建新的分隔符”一节 [224]
- “显示或隐藏菜单项”一节 [224]
- “从主菜单删除项”一节 [224]
- “重命名菜单项”一节 [225]
- “更改项目的类属名称”一节 [225]
- “将新项目添加到主菜单”一节 [225]
- “更改新的应用程序组中允许的最大项目数”一节 [226]

重要

如果是第一次使用 **Alacarte**，在注销和再登录之前，对菜单的更改不会生效。以后，更改会在您作出更改时立即显示。

注意

有些 **Alacarte** 功能（如嵌套组和插入分隔符的功能）仅在您使用 **GNOME** 菜单的旧版本时才适用。

查找菜单项

菜单布局窗口的排列方式为左边菜单列表中主菜单的子菜单和右边项目列表的选定菜单中的项。子菜单中的组嵌套在该子菜单下面。要查找项目，请单击菜单列表中子菜单旁边的箭头，选择包含该项目的组，然后在项目列表中找到该项目。

例如，要查找“录音机”应用程序：

- 1 如“启动 **Alacarte**”一节 [222]中所述启动 **Alacarte**。
- 2 单击菜单列表中音频和视频子菜单旁边的箭头，然后选择录音组。

3 查找项目列表中的“录音机”。

重新排列菜单项

您可以使用 Alacarte 更改主菜单中显示项的顺序。例如，您可能想要将频繁使用的应用程序放在菜单顶部或其组的顶部以便查找。

要移动该项，请单击它并将它拖到菜单中的新位置。您可以将该项移动到同一菜单中的新位置，或者将其放到菜单列表中的项上，以将其移动到新菜单或组。

创建新的分隔符

分隔符作为可见信号可使其更容易在菜单中找到项。

注意

在 GNOME 菜单的当前版本中不会使用分隔符。添加分隔符不会起作用。但是，如果您安装并使用 GNOME 菜单的旧版本，可以使用分隔符。

要创建分隔符：

1 选择要显示分隔符的空间上的项。

对于查找项的帮助，请参阅[“查找菜单项”一节](#) [223]。

2 单击新的分隔符。

新的分隔符出现在项列表中选定的项下。象其他菜单项一样，您也可以将分隔符拖到新的位置。要删除分隔符，请参阅[“从主菜单删除项”一节](#) [224]。

显示或隐藏菜单项

要显示或隐藏项，请在项列表中找到该项，然后选中或取消选中该项旁边的复选框。当您隐藏项时，它保留在项列表中，下次决定要让它显示在菜单中时可以显示它。要从项列表中删除项，请参阅[“从主菜单删除项”一节](#) [224]。

从主菜单删除项

有两种方式可以将项从主菜单中去除：

- 要去除项但要将它保留在“项目”列表中，这样您才能轻松地将它添加到菜单，如“[显示或隐藏菜单项](#)”一节 [224]中所述来隐藏项。
- 要从“项”列表中删除项目，以便不再显示它，请右键单击该项并单击删除。

注意

不能隐藏分隔符。只能添加或删除它们。

如果您要显示已删除的项目，必须添加它，就象对新的应用程序那样。请参阅“[将新项目添加到主菜单](#)”一节 [225]获得关于添加应用程序的信息。

重命名菜单项

- 1 如“[查找菜单项](#)”一节 [223]中所述，查找要更改名称的菜单项。
- 2 右键单击该项目，然后单击属性。
- 3 将当前名称替换为您要赋予该项目的名称，然后单击关闭。

旧名称将替换为菜单中的新名称。

更改项目的类属名称

主菜单中每个项目名称下都会显示简短的描述名称。这个名称被称为类属名称。要更改类属名称：

- 1 如“[查找菜单项](#)”一节 [223]中所述，查找要更改类属名称的菜单项。
- 2 右键单击该项目，然后单击属性。
- 3 将当前类属名称替换为您要赋予该项目的类属名称，然后单击关闭。

旧的类属名称将替换为菜单中的新名称。

将新项目添加到主菜单

您可以将新项目添加到主菜单。这在您安装应用程序时特别有用，但是如果您有其他当前未显示在菜单上的应用程序，这也很有用。您还可以将目录、链接或其他类型的项目添加到菜单。

要将应用程序添加到主菜单：

- 1 在菜单列表中，单击包含您要添加应用程序的组的菜单旁边的箭头，然后选择组。

该组的内容显示在*项目*列表中。

- 2 单击*新建项目*。
- 3 为该项目输入名称和类属名称。
- 4 单击*浏览*并找到该项目。
- 5 选择该项目。
- 6 单击*类型*列表，然后选择项目类型。

例如，如果您要添加目录，单击该列表并选择*目录*。如果您正在添加应用程序，请保留默认项目类型：*应用程序*。

- 7 （可选）要将图标指定给这个新项目，请单击*无图标*，然后为该项目选择图标。

如果您未选择图标，则该项目将显示在菜单中，且无图标。

- 8 单击*关闭*。

如“**重新排列菜单项**”一节 [224]中所述，将项目添加到菜单后，可以将它移动到您想要它在菜单中显示的位置。

更改新的应用程序组中允许的最大项目数

安装应用程序时，通常会将它添加到主菜单它的组中以及*新应用程序*组中。

注意

有些应用程序在安装时不会将它们添加到菜单。您可以使用“**将新项目添加到主菜单**”一节 [225]中提供的说明自己将这些应用程序添加到主菜单中。

默认情况下，*新应用程序*组最多可包含9个项目。添加了第9个新应用程序后，后续的新应用程序将替换该组中最旧的项目。

要更改“新应用程序”组中允许的应用程序的最大数目：

- 1 打开 Alacarte。
- 2 单击**应用程序浏览器**：新应用程序组中的最大项目数旁边的向上箭头或向下箭头来增加或减少该数目。
- 3 单击**关闭**。

更改系统范围的菜单

Alacarte 使您可以为系统上的所有用户编辑系统范围的主菜单，并将其分发到其他计算机。要使用新菜单，这些其他系统无需相同的设置。

注意

更改系统范围的菜单需要对您要更改菜单的计算机有管理特权。

要更改系统范围的菜单并分发它：

- 1 使用系统范围的菜单编辑器的启动器打开 Alacarte。
有关更多信息，请参见“**启动 Alacarte**”一节 [222]。
- 2 输入 `root` 密码。
- 3 如“**编辑菜单**”一节 [222]中所述，对菜单作出所需更改。
- 4 单击**关闭**。

您现在所作的更改会显示给系统的所有用户。

将系统范围的菜单分发给其他计算机

对系统范围菜单所作的更改将保存在 `/etc/opt/gnome/alacarte-system` 目录中。要在其他计算机上使用此菜单：

- 1 将 `/etc/opt/gnome/alacarte-system` 目录复制到其他计算机。

- 2 将以下行从原始系统上的 `/etc/profile.d/xdg-environment.sh` 文件复制到目标系统上的 `/etc/profile.d/xdg-environment.sh` 文件：

```
#START SECTION ADDED BY ALACARTE
export XDG_DATA_DIRS=/etc/opt/gnome/alcarte_system:$XDG_DATA_DIRS
export XDG_CONFIG_DIRS=/etc/opt/gnome/alcarte_system:$XDG_CONFIG_DIRS
#END SECTION ADDED BY ALACARTE
```

10.2.2 使用桌面和目录项文件自定义 GNOME 菜单

GNOME Desktop 操作菜单的方式使您能够执行以下操作：

- 轻松自定义菜单层次结构。菜单层次结构并非基于文件系统层次结构之上。可编辑少量文件来自定义菜单层次结构。无需修改应用程序或移动文件。
- 轻松安装应用程序。安装应用程序时，无需向应用程序提供有关菜单层次结构的信息。
- 配置菜单以便用户无法修改菜单。

GNOME Desktop 中的菜单使用以下组件：

- 桌面项文件
- 目录项文件

桌面项文件

桌面项文件是一种数据文件，它提供有关菜单中项的信息。此文件指定项的详细信息，如名称、要运行的命令或图标。它还包含关键字，这些关键字确定项在菜单层次结构中的位置。桌面项文件的文件扩展名为 `.desktop`。

以下是示例桌面项文件：

```
[Desktop Entry]
Encoding=UTF-8
Name=Calculator
Comment=Perform calculations
Exec=gcalc
Icon=gcalc.png
Terminal=false
```



```
Type=Application
Categories=GNOME;Application;Utility;
X-GNOME-DocPath=gcalctool/gcalctool.xml
```

下表说明桌面项文件中最重要的密钥。

表 10.7 桌面项文件密钥

桌面项密钥	说明
编码	指定桌面项文件的编码。
名称	指定项的名称。此名称显示在菜单中项的上方。
注释	指定项的简短说明。将鼠标指向菜单中的项时，会作为工具提示显示注释。
Exec	指定从菜单选择项时要执行的命令。
图标	指定表示项的图标的文件名。不指定文件扩展名或到文件名的路径。
终端	<p>指定 Exec 密钥中的命令是否在终端窗口中运行。如果值为 True，则命令将在终端窗口中运行。</p> <p>如果命令不创建运行窗口，则此密钥的值必须设置为 True。</p>
类型	<p>指定项的类型。该值为以下一个值：</p> <ul style="list-style-type: none">• 应用程序： 对启动应用程序的项使用此选项。• 链接： 对链接到文件、文件夹或FTP站点的项使用此选项。
类别	<p>指定说明项的关键字。关键字以分号(;)分隔。要查看标准类别关键字列表，请参见桌面菜单规范：freedesktop.org [http://www.freedesktop.org]</p> <p>文件夹信息文件会将关键字映射到菜单。</p>

桌面项密钥	说明
X-GNOME-DocPath	指定在应用程序名称上从菜单项弹出菜单选择“帮助”时将显示的帮助文件。

有关桌面项文件中的密钥的更多信息，请参见桌面项规范：<http://www.freedesktop.org>。

注意

面板启动器和桌面对象也使用桌面项文件。这些桌面项文件提供与菜单中的项相同的信息。例如，当用户选择启动器或对象时，桌面项文件会提供要运行的命令。

目录项文件

目录项文件是一种数据文件，它提供有关菜单的信息。目录项文件指定菜单的详细信息，如名称、工具提示和图标。目录项文件的文件扩展名为 `.directory`。

以下是示例目录项文件：

```
[Desktop Entry]
Name=Accessories
Comment=Accessories menu
Icon=gnome-util.png
Type=Directory
```

下表说明目录项文件中最重要的密钥。

表 10.8 目录项文件密钥

目录项密钥	说明
名称	指定菜单上显示的菜单名称。
注释	指定菜单的简短说明。将鼠标指向菜单时，会作为工具提示显示注释。

目录项密钥	说明
图标	指定表示菜单的图标的文件名。不指定文件扩展名或到文件名的路径。
类型	指定菜单的类型。此密钥的值始终为“目录”。

编辑菜单

SUSE Linux Enterprise 使用 freedesktop.org 菜单规范。该规范使用以下文件和目录：

表 10.9 菜单文件位置

文件	说明
/etc/xdg/menus/ applications.menu	该文件包含默认应用程序菜单布局的 XML 定义。如果用户有其自己的应用程序菜单，它会替换系统范围的菜单。
/etc/xdg/menus/ applications-merged	该目录包含 <DefaultMergeDirs> 元素中所含的默认合并目录。您可以在该位置添加新的 <Menu> 文件。
/etc/xdg/menus/ preferences.menu	该文件包含 GNOME 控制中心的 XML 定义。

关于添加和删除菜单项的更多详细信息，请参见桌面菜单规范 [<http://standards.freedesktop.org/menu-spec/latest>] 万维网站点。

10.3 安装主题

主题是一组协调的设置，它指定 GNOME Desktop 某部分的视觉外观。用户可选择主题以更改 GNOME Desktop 的外观。

主题包含影响 GNOME Desktop 各个部分的设置，如下所示：

控件

确定窗口、面板和小程序的视觉外观。它还确定窗口、面板和小程序上显示的符合 GNOME 的界面项目的视觉外观，如菜单、图标和按钮等。某些可用的控制设置选项专门用于特殊的辅助性要求。用户可从“主题”自选设置工具中的“控制”选项卡部分选择控制设置的选项。

窗口框架

只确定窗口四周的框架的外观。用户可从“主题”自选设置工具中的“窗口边框”选项卡部分选择窗口框架的选项。

图标

确定面板和桌面背景上的图标的外观。用户可从“主题”自选设置工具中的“图标”选项卡部分选择图标的选项。

10.3.1 主题索引文件

每个主题都有索引文件，索引文件定义主题特征。索引文件的名称为 /opt/gnome/share/themes/theme-name/index.theme。

以下是示例主题索引文件：

```
[Desktop Entry]
Type=X-GNOME-Metatheme
Name=High Contrast Large
Name[es]=Alto contraste grande
Comment=Large black-on-white text and icons
Comment[es]=Textos e iconos grandes en negro sobre blanco
Encoding=UTF-8
[X-GNOME-Metatheme]
GtkTheme=HighContrastLargePrint
IconTheme=HighContrast
MetacityTheme=Atlanta
ApplicationFont=sans 18
```

下表说明主题索引文件中的密钥：

表 10.10 主题索引文件密钥

索引文件密钥	说明
类型	指定此主题确定多个主题选项的外观，如控制、窗口框架和图标。

索引文件密钥	说明
名称	主题名称，在“主题”自选设置工具中显示。
注释	主题的简短说明，显示在“主题”自选设置工具的主题名称下。
GtkTheme	与“主题”自选设置工具中的控制设置对应。指定控制设置选项所适用的窗口、面板和小程序。
IconTheme	与“主题”自选设置工具中的图标设置对应。指定图标设置选项所适用的面板和桌面背景。
MetacityTheme	与“主题”自选设置工具中的窗口框架设置对应。指定窗口框架设置选项所适用的窗口。
ApplicationFont	与“字体”自选设置工具中的应用程序字体设置对应。

10.3.2 安装新的控制选项

可在“主题”自选设置工具中为控制添加新的选项。控件选项位于 `/opt/gnome/share/themes` 目录中。文件系统中控制选项的典型结构如下所示。

选项文件

```
/opt/gnome/share/themes/option-name/gtk-2.0/gtkrc
```

图形文件

```
/opt/gnome/share/themes/option-name/pixmaps/*.*
```

通常情况下，控制设置的新选项会作为 `.tar.gz` 文件提供。要安装新的控制选项，请解压缩 `.tar.gz` 文件，然后将 `.tar` 文件解压缩到 `/opt/gnome/share/themes` 目录中。

用户可为控制设置安装自己的选项。如果用户为控制设置安装选项，则选项将存储在 `$HOME/.themes` 目录中。

10.3.3 安装新的窗口框架选项

可在“主题”自选设置工具中为窗口框架设置添加新的选项。窗口框架选项位于 `/opt/gnome/share/themes/option-name/metacity-1` 目录中。文件系统中窗口框架选项的典型结构如下所示。

选项文件

```
/opt/gnome/share/themes/option-name/metacity-1/  
metacity-theme-1.xml
```

图形文件

```
/opt/gnome/share/themes/option-name/metacity-1/*.*
```

通常情况下，窗口框架设置的新选项会作为 `.tar.gz` 文件提供。要安装新的窗口框架选项，请解压缩 `.tar.gz` 文件，然后将 `.tar` 文件解压缩到 `/opt/gnome/share/themes` 目录中。

用户可为窗口框架设置安装自己的选项。如果用户为窗口框架设置安装选项，则选项将存储在 `$HOME/.themes` 目录中。

10.3.4 安装新的图标选项

可在“主题”自选设置工具中为图标设置添加新的选项。图标选项位于 `/opt/gnome/share/icons/option-name` 目录中。文件系统中图标选项的典型结构如下所示。

选项文件

```
/opt/gnome/share/icons/option-name
```

图形文件

```
/opt/gnome/share/icons/option-name/icons/*.*
```

通常情况下，图标设置的新选项会作为 `.tar.gz` 文件提供。要安装新的图标选项，请解压缩 `.tar.gz` 文件，然后将 `.tar` 文件解压缩到 `/opt/gnome/share/icons` 目录中。

用户可为图标设置安装自己的选项。如果用户为图标设置安装选项，则选项将存储在 `$HOME/.icons/option-name` 目录中。

10.3.5 为主题安装图标

GNOME Desktop 提供了多个主题，这些主题设计为满足用户的特殊视觉需要。例如，一些主题是为视力差的用户设计的。可能需要多个版本的图标以便图标能够在每个主题中正确显示图标。

可能需要为应用程序安装新图标。安装新图标时，必须创建多个版本的图标以便在主题中正确显示图标。必须创建多个版本的以下类型图标：

- GNOME Desktop 中在应用程序内使用的图标
- GTK+ 应用程序或 GTK+ 库图标内部使用的图标

可使用多种格式创建图标（例如，Portable Network Graphic（PNG）格式）。桌面环境图标的建议大小为 48 x 48 像素；使用此大小，大部分主题可重新调整图标大小。

安装新图标时，请创建以下 48 x 48 像素版本的图标：

- 常规图标
- 低对比度图标
- 高对比度图标
- 反转高对比度图标

如果可能的话，还为以上每个图标创建 16 x 16 像素版本以用于无需大字体的主题。

将图标安装到 [第 10.3.2 节“安装新的控制选项”](#) [233] 或 [第 10.3.3 节“安装新的窗口框架选项”](#) [234] 中为主题指定的图像文件位置。例如，要将图标添加到 HighContrastLargePrint 主题，请将图标添加到 `/opt/gnome/share/themes/`

HighContrastLargePrint/pixmaps 目录中。向相关主题文件添加对图标的引用。例如，要将图标添加到 HighContrastLargePrint 主题，则将对图标的引用添加到 /opt/gnome/share/themes/HighContrastLargePrint/gtk-2.0/gtkrc 文件中。修改主题的 gtkrc 文件以将图标与 GTK 库图标标识符关联。

有关如何为应用程序启动器和面板创建图标的更多信息，请参见 Icon Themes [<http://www.freedesktop.org/Standards/icon-theme-spec>]。

10.3.6 创建自定义控制选项

如果控制设置的选项不适合用户需要，则可以创建自定义控制选项。

- 1 在 /opt/gnome/share/themes 目录中为选项创建目录结构。

使用和其他选项相同的目录结构。例如，要创建名为 SmallPrint 的选项，可创建以下目录：

- /opt/gnome/share/themes/SmallPrint
- /opt/gnome/share/themes/SmallPrint/gtk-2.0

- 2 查找与用户需求最接近的 gtkrc 文件，然后将文件复制到新选项的 gtk-2.0 目录中。
- 3 在文本编辑器中打开 gtkrc 文件，然后根据需要修改界面元素的特性。
- 4 （视具体情况而定）如果新选项包含图像，则在新选项的像素映射目录中安装新选项的图像。

如果新选项使用来自其他选项的图像，则无需为新选项创建图像副本。相反，请确保 gtkrc 文件的 pixmap_path 项中对图像的引用是正确的。

用户现在可以为控制设置选择新选项了。

有关 gtkrc 文件的更多信息，请参见 *GTK+ Reference Manual* [<http://developer.gnome.org/doc/API/2.0/gtk/index.html>]。

10.4 配置字体

GNOME Desktop 使用 fontconfig 字体配置和自定义库。fontconfig 库可使用所有类型的字体，包括 PostScript Type 1 字体和 TrueType* 字体。fontconfig 库提供系统上可用的所有字体的列表。为了编译此列表，fontconfig 会搜索 `/etc/fonts/fonts.conf` 文件中列出的目录。要查看系统上可用的所有字体，请访问系统上文件管理器中的 `fonts:///` 位置。

有关 fontconfig 库的更多信息，请参见 Fontconfig [<http://freedesktop.org/software/fontconfig>] 万维网站点。

10.4.1 字体替换

当所有字体或个别字符不存在时，fontconfig 库会执行字体替换。如果系统需要显示不可用的字体，fontconfig 会尝试显示其他相似字体。例如，如果万维网页面请求显示 Verdana 字体，但是系统上未安装该字体，则 fontconfig 会显示相似字体，如 Helvetica。相似字体列表定义在 `/etc/opt/gnome/fonts/fonts.conf` 文件中。

如果系统需要显示选定字体中不存在的字符，则 fontconfig 会尝试显示其他类似字体中的字符。例如，可能会选择 Bitstream Vera Sans 作为“文本编辑器”应用程序的字体。Bitstream Vera 字体系列不包含西里尔字符。如果打开包含西里尔字符的文档，则文本编辑器将使用包含西里尔字符的相似字体来显示字符。

fontconfig 库还定义字体的别名（例如，`serif`、`sans-serif` 和 `monospace`）。为字体选择别名时，系统会使用在 `/etc/opt/gnome/fonts/fonts.conf` 中为该别名定义的第一个字体。

10.4.2 为所有用户添加字体

- 1 将字体文件复制到 `/etc/opt/gnome/fonts/fonts.conf` 文件的目录中。

通常情况下，字体存储在 `/opt/gnome/share/fonts/` 目录中。

- 2 （视具体情况而定）fontconfig 库会自动更新字体列表。如果字体列表未更新，则运行以下命令：

`fc-cache directory-name`

10.4.3 为单个用户添加字体

- 1 将字体文件复制到用户的 `$HOME/.fonts` 目录中。

如果在文件管理器中将字体拖到 `fonts:///` 位置，则字体文件会复制到 `$HOME/.fonts` 目录中。

- 2 （视具体情况而定）`fontconfig` 库会自动更新字体列表。如果字体列表未更新，则运行以下命令：

`fc-cache directory-name`

10.5 MIME 类型

多功能互联网邮递伸延（**MIME**）类型可识别文件的格式。**MIME** 类型使应用程序能够读取文件。应用程序（如因特网浏览器和电子邮件应用程序）会使用 **MIME** 类型处理不同类型的文件。例如，电子邮件应用程序可使用 **MIME** 类型来检测电子邮件所附加文件类型。

Nautilus 文件管理器使用 **MIME** 类型来识别文件类型。文件管理器需要知道文件的 **MIME** 类型以执行以下任务：

- 在合适的应用程序中打开文件
- 显示说明文件类型的字符串
- 显示合适的图标来表示文件
- 显示可打开文件的其他应用程序列表

有时必须确定文件的正确 **MIME** 类型。这通常是通过检查文件的名称或内容，在数据库中查看正确的 **MIME** 类型实现的。如果添加新的应用程序（即扩展数据库），则必须确保其他应用程序可识别与应用程序关联的文件。例如，您可能想添加以下内容：

- `image/png` 文件应使用 **Gimp** 编辑。

- image/png 文件用英语描述就是 Portable network graphics 文件。
- 文件名以 .png 结尾的文件，类型应为 image/png。

您可以用图形编辑器（例如 MIME-Editor [<http://rox.sourceforge.net/phpwiki/index.php/MIME-Editor>]）编辑数据库，或者通过用以下所述格式创建名为 \$XDG_DATA_HOME/mime/packages/Override.xml 的文件手动编辑。关于 XDG_variables 的信息，请参见 Base directory Specification [http://freedesktop.org/wiki/Standards_2fbasedir_2dspec]。

安装新应用程序后，它会在 \$XDG_DATA_DIRS/mime/packages 中安装带有该应用程序名称的文件。例如，运行 Gimp 的 /configure && make install 命令将创建 /usr/local/share/mime/packages/gimp.xml。

该文件具有以下格式：

```
<?xml version="1.0" encoding="UTF-8"?>
<mime-info xmlns="http://www.freedesktop.org/standards/shared-mime-info">
  <mime-type type="image/png">
    <comment xml:lang="en">PNG image</comment>
    <comment xml:lang="af">png bleed</comment>
    ...
    <magic priority="50">
      <match type="string" value="\x89PNG" offset="0"/>
    </magic>
    <glob pattern="*.png"/>
  </mime-type>
</mime-info>
```

它提供两种语言的注释，一条按文件内容识别 PNG 文件的规则，以及一条按文件名识别 PNG 文件的规则。您可以在一个 application.xml 文件中提供几种信息。您无需提供基本软件包中已有的任何信息。

如果其他元素已映射到名称空间，也可以添加它们以避免冲突。例如：

```
<desktop:can-edit-with>gimp.desktop</desktop:can-edit-with>
```

这表示已命名的桌面项文件描述了可编辑 image/png 文件的应用程序。

添加到数据库的信息应为静态（例如，“Gimp 可编辑 PNG 文件。”），而不是配置（例如，“Gimp 是首选的 PNG 文件编辑器。”）。有关存储配置信息的更多信息，请参见共享配置系统规范 [http://freedesktop.org/wiki/Standards_2fconfig_2dspec]。

安装了 `application.xml` 文件后，请运行 `update-mime-database` 命令来重建输出文件。该程序会检查文件的语法是否正确，将其中信息与 `packages` 目录中的另一个 XML 文件中的信息合并。它随后就会将识别文件的规则放入一组文件中，每种类型的信息放入其他文件中（例如 `$XDG_DATA_DIR/mime/image/png.xml`），其他程序可以方便地在其中访问信息。

卸载该应用程序后，将删除 `application.xml` 文件。再次运行 `update-mime-database`，从数据库删除信息。

10.6 设置屏幕保护程序

屏幕保护程序是屏幕未使用时替换屏幕上的图像的应用程序。GNOME Desktop 的屏幕保护程序为 `XScreenSaver`。以下章节说明如何设置 `XScreenSaver` 应用程序的自选设置以及如何修改可用于屏幕保护程序的显示器。

10.6.1 设置屏幕保护程序自选设置

默认屏幕保护程序自选设置存储在 `/usr/X11R6/lib/X11/app-defaults/XScreenSaver` 中的 `XScreenSaver` 文件中。

要修改屏幕保护程序自选设置，用户可使用“屏幕保护程序”自选设置工具。当用户修改屏幕保护程序自选设置时，自选设置存储在用户主目录 `$HOME/.xscreensaver` 文件中。有关屏幕保护程序自选设置的信息，请参见 *GNOME Desktop User Guide* [<http://www.gnome.org/learn/users-guide/2.6>]。

用户还可运行 `/usr/X11R6/bin/xscreensaver-demo` 命令来打开 `XScreenSaver` 对话框。

要为所有用户设置默认屏幕保护程序自选设置，可修改 `XScreenSaver` 文件。还可使用 `XScreenSaver` 对话框创建 `$HOME/.xscreensaver` 文件，然后将文件复制到 `XScreenSaver` 文件的位置中。

要恢复用户的默认设置，请从用户主目录删除 `$HOME/.xscreensaver` 文件。如果 `$HOME/.xscreensaver` 文件不存在，则将使用 `XScreenSaver` 文件中的默认自选设置。

提示

XScreenSaver 的默认显示行为将显示空白屏幕。空白屏幕可能会使用户感到困惑。可能会希望更改此默认显示行为。

要激活屏幕保护程序自选设置的更改，请使用以下命令来重新装载屏幕保护程序自选设置：

```
xscreensaver-command -restart
```

10.6.2 修改屏幕保护程序显示器

屏幕保护程序使用户能够选择一个或多个屏幕保护程序显示器。屏幕保护程序显示器是屏幕未使用时在用户屏幕上显示图像的应用程序。XScreenSaver 文件和 `$HOME/.xscreensaver` 文件中列出了屏幕保护程序显示器。

要添加新的屏幕保护程序显示器，请将显示器的可执行文件添加到显示器所在的目录中。将屏幕保护程序显示器的命令添加到 XScreenSaver 文件中或 `$HOME/.xscreensaver` 文件中。请包含在整个屏幕（非窗口）中运行屏幕保护程序显示器所需的参数。例如，可能会希望包含 `-root` 选项以在整个屏幕中显示屏幕保护程序显示器。

要禁用屏幕保护程序显示器，可在自选设置文件中向屏幕保护程序显示器的命令开头添加减号（-）。以下 `$HOME/.xscreensaver` 文件节选显示已禁用的 Qix (solid) 屏幕保护程序显示器：

```
- "Qix (solid)"  qix -root -solid -segments 100
```

10.7 会话管理

在用户登录到 GNOME Desktop 到用户注销期间会发生会话。登录管理器认证用户后，将启动会话管理器。会话管理器使用户能够管理会话。例如，用户可保存会话状态并在下次登录时返回该会话。

至少有以下应用程序在会话中运行：

- 会话管理器，`gnome-session`。
- GConf X 设置守护程序，`gnome-settings-daemon`。

- `gnome-panel` 应用程序，它在 GNOME Desktop 中运行面板。
- Metacity 窗口管理器。

下表列出了包含默认会话信息的文件：

表 10.11 默认会话信息文件

文件	说明
<code>/opt/gnome/share/gnome/default.session</code>	默认会话文件。此文件中存储默认会话细节。
<code>\$HOME/.gnome2/session</code>	用户会话文件。当用户修改会话时，细节将会存储在此文件中。

要为所有用户设置默认会话细节，可修改默认会话文件。

要恢复用户的默认会话设置，请从用户主目录删除会话文件。如果用户会话文件不存在，则将使用 `/opt/gnome/share/gnome/default.session` 中的默认设置。

要将当前会话保存为默认会话，用户可运行 `gnome-session-save` 命令。

GNOME 也支持自动启动。有关详细信息，参见 [第 10.12 节“自动启动应用程序”](#) [254]。

10.8 提升性能

本节讨论若干自选设置，可更改这些设置以提升 GNOME Desktop 的性能。可使用 `gconftool-2` 命令来设置用户的自选设置值。本节中的示例命令显示如何在用户配置源中设置值。

还可使用 `--direct` 和 `--config-source` 选项来设置自选设置的必需值或默认值。可在脚本中使用 `gconftool-2` 命令来设置一些自选设置的值。有关 `gconftool-2` 命令以及可与该命令一起使用的选项的更多信息，请参见 [第 10.1 节“默认情况下使用 GConf”](#) [198]。

10.8.1 减少 CPU 使用率

可以设置一些自选设置来减少 GNOME Desktop 的 CPU 使用率。

使用需要较少 CPU 资源的主题选项

一些窗口框架主题选项会装载图像文件来绘制窗口框架。其他选项使用更简单的技术来绘制窗口框架。Crux 窗口框架选项会装载图像文件，但是在 CPU 资源有限的系统上使用时，其速度较慢。要减少 CPU 使用率，可使用以下窗口框架选项：

- Atlanta
- Esco

以下窗口框架选项使用的 CPU 资源也少于 Crux：

- AgingGorilla
- Bright
- Metabox

提示

当与反转控制选项一起使用时，Metabox 不太有效，如 HighContrastInverse。将 Atlanta 与反转控制选项一起使用。

要更改窗口框架主题选项，可使用以下命令：

```
gconftool-2 --type string --set /apps/metacity/general/theme option-name
```

例如，要使用 Atlanta，请运行以下命令：

```
gconftool-2 --type string --set /apps/metacity/general/theme Atlanta
```

用户还可使用“主题”自选设置工具来选择合适的选项。

可使用“Metacity 主题查看器”来检测窗口框架选项的性能和预览选项。要启动“Metacity 主题查看器”，请使用以下命令：

```
metacity-theme-viewer option-name
```

例如，要检测 Atlanta 的性能并预览 Atlanta，请使用以下命令：

```
metacity-theme-viewer Atlanta
```

在菜单中关闭图标显示

菜单中的某些项会在项旁边显示图标。要关闭此功能，请使用以下命令：

```
gconftool-2 --type bool --set /desktop/gnome/interface/menus_have_icons false
```

用户还可使用“菜单和工具栏”自选设置工具来取消选择“在菜单中显示图标”选项。

关闭启动屏幕

默认情况下，当用户登录桌面环境时，会显示启动屏幕。当用户登录时，会在启动屏幕上显示图标。可关闭启动屏幕来减少登录时的 CPU 使用率。

要关闭启动屏幕，请使用以下命令：

```
gconftool-2 --type bool --set /apps/gnome-session/options/show_splash_screen false
```

关闭面板动画

用户显示或隐藏面板时，面板会以动画形式显示或隐藏。要关闭面板动画，请使用以下命令：

```
gconftool-2 --type bool --set /apps/panel/global/enable_animations false
```

用户还可使用“面板”自选设置工具来取消选择“抽屉和面板动画”选项。

提升文件管理器性能

Nautilus 文件管理器包含一些可进行修改以提升性能的功能。

修改性能自选设置

文件管理器包含与性能相关的自选设置。这些自选设置都使用以下三个值。

表 10.12 与性能相关的自选设置

值	说明
总是	对本地文件和其他文件系统上的文件执行操作。
local_only	仅对本地文件执行操作。使用该值可减少 CPU 使用率。
never	永不执行操作。使用该值可减少 CPU 使用率和网络流量。

下表说明文件管理器的性能自选设置。要获得最佳性能，请将自选设置的值设置为“永远不”。

表 10.13 文件管理器性能自选设置

自选设置	说明
show_icon_text	<p>指定何时在表示文件的图标中预览该文本文件的内容。要永远不预览文本文件的内容，请使用以下命令：</p> <pre>gconftool-2 --type string --set /apps/nautilus/preferences/ show_icon_text never</pre>

用户还可执行以下步骤：

1. 在文件管理器窗口中单击 **编辑 > 自选设置**，然后单击 **预览**。
2. 为“在图标中显示文本”自选设置选择一个选项。

show_directory_item_counts	<p>指定何时显示文件夹中的项数。要永远不显示文件夹中的项数，请使用以下命令：</p> <pre>gconftool-2 --type string --set /apps/nautilus/preferences/ show_directory_item_counts never</pre>
----------------------------	---

用户还可执行以下步骤：

自选设置	说明
	<ol style="list-style-type: none">1. 在文件管理器窗口中单击 编辑 > 自选设置，然后单击 预览。2. 为“项计数”自选设置选择一个选项。
show_image_thumbnails	<p>指定何时显示图像文件的缩略图。要永远不显示缩略图，请使用以下命令：</p> <pre>gconftool-2 --type string --set /apps/nautilus/preferences/ show_image_thumbnails never</pre> <p>用户还可执行以下步骤：</p> <ol style="list-style-type: none">1. 在文件管理器窗口中单击 编辑 > 自选设置，然后单击 预览。2. 为“显示缩略图”自选设置选择一个选项。
preview_sound	<p>指定何时预览声音文件的内容。要永远不预览声音文件的内容，请使用以下命令：</p> <pre>gconftool-2 --type string --set /apps/nautilus/preferences/preview_sound never</pre> <p>用户还可执行以下步骤：</p> <ol style="list-style-type: none">1. 在文件管理器窗口中单击 编辑 > 自选设置，然后单击 预览。2. 为“预览声音文件”自选设置选择一个选项。

关闭侧窗格、工具栏和位置栏

文件管理器包含一些使您能够关闭侧窗格和工具栏的自选设置。关闭侧窗格和工具栏可提升文件管理器性能。

要关闭侧窗格，请使用以下命令：

```
gconftool-2 --type bool --set /apps/nautilus/preferences/start_with_sidebar false
```

要关闭工具栏，请使用以下命令：

```
gconftool-2 --type bool --set /apps/nautilus/preferences/start_with_toolbar false
```

还可关闭位置栏。用户可使用 **Ctrl+L** 键盘快捷键来在需要时显示位置栏。

要关闭位置栏，请使用以下命令：

```
gconftool-2 --type bool --set /apps/nautilus/preferences/start_with_location_bar false
```

关闭桌面

文件管理器包含一个使用户能够使用 Nautilus 管理桌面的自选设置。可禁用桌面以提升性能。但是，如果禁用桌面，则无法

- 使用“桌面”菜单。
- 使用文件管理器来更改桌面背景的模式或颜色。
- 使用桌面对象，如“回收站”。（将不在桌面上显示桌面对象。）

要禁用桌面，请使用以下命令：

```
gconftool-2 --type bool --set /apps/nautilus/preferences/show_desktop false
```

10.8.2 减少 X 窗口系统网络流量

可以设置一些自选设置来减少 GNOME Desktop 上的 X 窗口系统网络流量。

使用产生较少网络流量的主题选项

如果块中的像素使相同颜色，则所有远程显示协议不会传输像素块中的每一个像素。要减少 X 窗口系统网络流量，可使用以下使用单色的窗口框架选项：

- Atlanta
- Esco

有关如何更改主题选项的信息，请参见[“使用需要较少 CPU 资源的主题选项”一节](#) [243]。

在菜单中关闭图标显示

菜单中的某些项会在项旁边显示图标。如果图标位于其他文件系统上或如果面板显示在远程主机上，则此功能可能会增加 X 窗口系统网络流量。

有关如何关闭此功能的信息，请参见[“在菜单中关闭图标显示”一节](#) [244]。

10.8.3 减少颜色使用和提升显示质量

一些现代计算机系统支持 24 位颜色（即，16,777,216 色）。但是。许多用户仍然使用仅支持 8 位颜色（256 色）的系统。GNOME Desktop 使用安全调色板。此调色板是一种常用 216 色调色板，它设计为优化支持 8 位颜色的系统上的颜色使用。但是，一些 GNOME Desktop 的视觉组件是为支持 24 位颜色的系统而设计的。

以下显示问题可能会在仅支持 8 位颜色的系统上发生：

- 窗口、图标和背景图像可能显示有纹理。一些主题、背景图像和图标使用网络安全调色板中所没有的颜色。不在调色板中的颜色会被替换为最接近的颜色或量化近似色，这会导致外观有纹理。
- 不使用网络安全调色板的应用程序具有更少的可用颜色；因此，可能会发生颜色错误。一些颜色可能不会显示在应用程序的用户界面中，如果应用程序无法分配颜色，则一些应用程序可能会崩溃。
- 当用户在使用网络安全调色板的应用程序和不使用此调色板的应用程序之间切换时，可能会发生颜色闪烁。不使用网络安全调色板的应用程序可能会使用自定义色图。使用自定义色图时，其他视觉组件可能会丢失颜色，然后变成不可视。

以下章节说明如何对仅支持 8 位颜色的系统优化 GNOME Desktop 外观。

选择使用网络安全调色板的主题选项

一些窗口框架主题选项使用在网络安全调色板中的颜色。Bright 和 Esco 使用网络安全调色板中的颜色并且使用 8 位颜色显示设置时不会有其他窗口框架选项

的纹理外观。使用 8 位视觉模式时，可使用 **Bright** 或 **Esco** 来获得最佳颜色显示。

有关如何更改主题选项的信息，请参见“[使用需要较少 CPU 资源的主题选项](#)”一节 [243]。

通过关闭菜单中的图标显示来减少颜色使用

菜单中的某些项会在项旁边显示图标。如果图标包含网络安全调色板中所没有的颜色，则此功能可能会增加使用的颜色数。

有关如何关闭此功能的信息，请参见“[在菜单中关闭图标显示](#)”一节 [244]。

通过关闭启动屏幕来减少颜色使用

可关闭启动屏幕来确保有更多颜色可用于 GNOME Desktop 和应用程序。

有关如何关闭启动屏幕的信息，请参见“[关闭启动屏幕](#)”一节 [244]。

通过对背景使用单色来减少颜色使用

对桌面背景使用单色。这会减少 GNOME Desktop 使用的颜色数。

要为背景设置单色，请使用以下命令：

```
gconftool-2 --type string --set /desktop/gnome/background/picture_options none
gconftool-2 --type string --set /desktop/gnome/background/color_shading_type
solid
gconftool-2 --type string --set /desktop/gnome/background/primary_color
\#hexadecimal-color
```

用户还可使用“背景”自选设置工具来为背景选择单色。

10.9 隐藏目录

下表说明 GNOME Desktop 添加到用户主目录的隐藏目录。隐藏目录是名称以句点 (.) 开头的目录。

表 10.14 添加到用户主目录的隐藏目录

目录	说明
<code>.esd_auth</code>	包含 GNOME 声音守护程序（Enlightened Sound Daemon（ESD））的认证 cookie。
<code>.gconf</code>	包含用户的 GConf 配置源。用户设置自选设置时，会将新的自选设置信息添加到此位置。
<code>.gconfd</code>	包含以下 GConf 守护程序详细信息： <ul style="list-style-type: none">• 配置信息• 由可操作对象引用（IOP）引用的对象锁定信息• IOR 引用的对象状态信息
<code>.gnome</code>	包含存在 GConf 存储库中的用户特定应用程序数据。例如，此目录包含用户的 MIME 类型信息和会话信息。
<code>.gnome-desktop</code>	Nautilus 文件管理器包含使用户能够使用文件管理器来管理桌面的自选设置。如果选择此选项，则目录将包含以下对象： <ul style="list-style-type: none">• 桌面上的对象（例如，“本地”对象；“回收站”对象和其他启动器）。这些对象会作为桌面项文件显示在目录中。例如，<code>starthere.desktop</code> 文件包含到“在此开始”位置的链接。• 安装的可移动媒体卷。 文件管理器还包含使用户能够将主目录用作桌面目录而非 <code>.gnome-desktop</code> 的自选设置。如果用户选中此选项，则主目录中的内容将显示为桌面对象。
<code>.gnome2</code>	包含存在 GConf 存储库中的用户特定应用程序数据，例如以下信息：

目录	说明
	<ul style="list-style-type: none"> • 键盘快捷方式信息 • 窗口位置信息 • 面板启动器的桌面项文件 <p>此目录还包含用户特定菜单数据，如果用户修改菜单，则将在此处存储详细信息。</p>
<code>.gnome2-private</code>	（忽略此目录。该目录当前无用）。
<code>.metacity</code>	包含 Metacity 窗口管理器的会话数据。
<code>.nautilus</code>	<p>包含特定于使用的文件管理器数据，例如以下数据：</p> <ul style="list-style-type: none"> • 用户使用的目录元数据 • 用户添加的 Nautilus 徽标 • Nautilus 桌面图像
<code>.themes</code>	包含用户添加的控制主题选项、窗口框架主题选项和图标主题选项。用户可从“主题”自选设置工具添加主题。
<code>.thumbnails</code>	包含用户的图像缩略图。图像缩略图在文件管理器中使用。文件管理器包含用户可选择以停止生成缩略图图像的自选设置。
<code>.xscreensaver</code>	包含屏幕保护程序配置数据和屏幕保护程序自选设置数据。

10.10 配置 SMB 打印机的安全性说明

Windows 网络共享也称为 Samba 或 SMB 共享。在 SMB 共享上配置打印机时，必须输入打印队列的用户名和密码。

用户名和密码存储在 `/etc/opt/gnome/cups/printers.conf` 文件中的未加密文本中。具有 `root` 用户权限的用户对此文件具有只读许可权限，因此所有具有 `root` 用户权限的用户都可读取打印队列的用户名和密码。

要减少可能发生的安全性违例所产生的影响，请确保将访问打印队列所需的用户名和密码仅用于打印队列。这可确保将所有可能发生的安全性违例限制于未授权使用打印队列。

10.11 禁用 GNOME Desktop 功能

GNOME Desktop 包含可用于限制对某些功能进行访问的功能。这些可禁用（或锁定）功能使您能够限制用户可在计算机上执行的操作。例如，您可能会希望在商业展示时防止在非公用计算机上执行命令行操作。

可通过设置 GConf 密钥来禁用功能（请参见第 10.1 节“默认情况下使用 GConf”[198]）。还可使用“配置编辑器”应用程序来在用户配置源中设置 GConf 密钥（请参见第 10.1.8 节“配置编辑器”[218]）。

10.11.1 禁用锁定屏幕和注销

要禁用锁定屏幕和注销功能，请将

`/apps/panel/global/disable_lock_screen` 密钥和
`/apps/panel/global/disable_log_out` 密钥设置为 `True`。

禁用锁定屏幕和注销功能时，会从面板去除以下项：

- 从“主菜单”除去“锁定屏幕”和“注销”用户菜单项
- 从“添加到面板 > 操作”菜单去除“锁定”和“注销”菜单项

要打开此菜单，请鼠标右键单击面板上的空白区域，然后单击 *添加到面板 > 操作*。

- 从“菜单栏”小程序中的“操作”菜单去除“锁定屏幕”和“注销”用户菜单项

此外，会禁用面板上的所有“锁定屏幕”按钮和“注销”按钮。

10.11.2 禁用命令行操作

要禁用命令行操作，请将

`/desktop/gnome/lockdown/disable_command_line` 密钥设置为 `True`。

禁用命令行操作时，用户界面中会发生以下更改：

- 将从以下菜单去除“运行应用程序”菜单项：
 - 主菜单
 - “添加到面板”菜单中的“操作”子菜单
 - “菜单栏”小程序中的“操作”菜单
- 将禁用面板上的所有“运行”按钮。

要禁用命令行操作，还必须去除启动终端应用程序的菜单项。例如，您可能会希望去除包含以下命令的菜单项：

- **GNOME Terminal** 命令（`/opt/gnome/bin/gnome-terminal`）
- `/usr/bin/xterm`
- `/usr/bin/setterm`

将从以下菜单去除这些项：

- 主菜单
- “添加到面板 > 启动位置”菜单

要禁用命令行操作，还必须禁用“命令行”小程序。要禁用此小程序，请将此小程序添加到 `/apps/panel/global/disabled_applets` 密钥中。禁用“命令行”小程序时，将从“主菜单”和“添加到面板 > 实用程序”菜单去除“命令行”小程序。

10.11.3 禁用面板配置

要禁用面板配置，请将 `/apps/panel/global/locked_down` 密钥设置为 `True`。

禁用面板配置时，用户界面中会发生以下更改：

- 将从“面板”和“抽屉”弹出菜单去除以下项：
 - 添加到面板
 - 删除该面板
 - 属性
 - 新建面板
- 将禁用启动器弹出菜单。
- 将从“小程序”弹出菜单去除以下项：
 - 从面板中去除
 - 锁定
 - 移动
- 将禁用“主菜单”弹出菜单。
- 将禁用“启动器”拖动功能以使用户无法将启动器拖到面板中或从面板拖动启动器。
- 将禁用“面板”拖动功能以使用户无法将面板拖到新位置。

10.12 自动启动应用程序

要在 GNOME 中自动启动应用程序，请使用以下方式之一：

- **对每个用户运行应用程序：** 将 `.desktop` 文件放入 `/opt/gnome/share/autostart` 或 `/opt/gnome/share/gnome/autostart` 中。

- 对单个用户运行应用程序： 将 `.desktop` 文件放入 `~/.config/autostart` 中。

要禁用自动启动的应用程序，请将 `X-Autostart-enabled=false` 添加到 `.desktop` 文件。

10.13 自动装入和管理媒体设备

GNOME 卷管理器 (`gnome-volume-manager`) 监视和卷相关的事件，用用户指定的策略响应。您可以用 GNOME 卷管理器自动装入热插拔驱动器和插入的可移动媒体，自动运行程序，自动播放音频 CD 和视频 DVD，自动从数码相机导入照片。

自动启动 GNOME 卷管理器。要禁用 GNOME 卷管理器，请将 `x-autostart-enabled=false` 添加到 `/opt/gnome/share/gnome/autostart/gnome-volume-manager.desktop` 文件。

您可以用 GConf Editor 配置 GNOME 卷管理器设置。按 `Alt+F2` 打开 GConf Editor 从而打开“运行应用程序”对话框，输入 `gconf-editor`，然后单击运行。GNOME 卷管理器位于 `/desktop/gnome/volume_manager` 下。

10.14 更改首选应用程序

要更改用户的首选应用程序，请编辑 `/etc/opt/gnome/gnome_defaults.conf`。

编辑文件后，请运行 `SuSEconfig --module gnome-vfs2`。

10.15 用 Sabayon 管理配置文件

Sabayon 是您可用于创建和应用桌面环境配置文件的系统管理工具。配置文件使默认设置和限制集合，可应用于各个用户或用户组。Sabayon 允许您用图形工具编辑 GConf 默认设置和强制密钥。

配置文件定义是通过和用户要运行的会话类似的图形会话实现的，只不过是桌面窗口中。您可以用通常方式更改属性（例如桌面背景、工具栏和可用的小程序）。Sabayon 还会检测对多数桌面应用程序中默认设置的更改。

留在模拟用户主目录或桌面的文件或文档会包含在完成的配置文件中。这包括许多特定于应用程序的数据库，例如 Tomboy notes。使用该机制，可以方便地以新用户容易访问的方式提供介绍性说明或模板。

用户配置文件可从父级配置文件继承其设置，覆盖或添加特定值。这会启用分级设置。例如，您可以定义 Employee 配置文件，并从中导出 Artist 和 Quality Assurance 配置文件。

除了提供默认设置外，Sabayon 也可以锁定设置。这可以使设置免于被用户更改。例如，您可以指定桌面背景不能更改为您提供的默认设置以外的背景。它可以防止随意更改设置，减少了潜在的帮助台呼叫次数，并能使用和 kiosk 相似的环境。但是，它并不能提供绝对的安全性，不应如此依赖它。

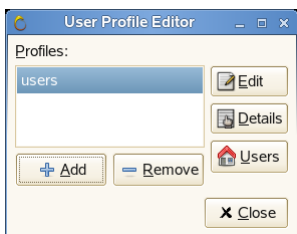
Sabayon 还提供了内置锁定支持的应用程序和常规用户接口元素列表，包括 Epiphany、OpenOffice.org 和 GNOME 面板。例如，可设置面板，只允许向它添加特定小程序，禁止更改它在屏幕上的位置或大小。类似地，可在所有使用它的应用程序间禁用“保存”菜单项，禁止用户保存文档。

配置文件可转移到其他计算机上。它们位于 `/etc/opt/gnome/desktop-profiles/` 中，每个配置文件都保存在单独的 ZIP 文件中。

10.15.1 创建配置文件

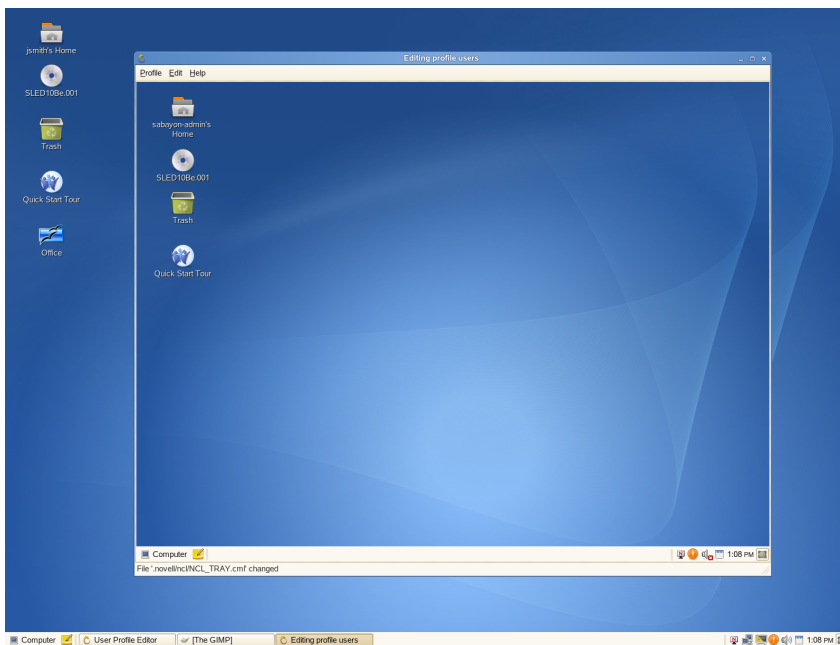
配置文件保存在位于 `/etc/opt/gnome/desktop-profiles` 中的 ZIP 文件中。您保存的每个配置文件都存储在 `name-of-the-profile.zip` 形式的单独的 ZIP 文件中。您可以将配置文件复制或移动到其他计算机。

- 1 单击 **计算机 > 更多应用程序 > 系统 > 桌面配置文件编辑器**。
- 2 如果您不是以 root 用户身份登录的，请输入 root 密码，然后单击继续。



- 3 单击“添加”。
- 4 指定配置文件名称，然后单击添加。
- 5 选择配置文件，然后单击编辑。

会在 Xnest 窗口中打开新的桌面会话。



- 6 在 Xnest 窗口中，根据需要更改设置。

您更改的每一设置都会显示在 Xnest 窗口中。

您可以选择让每个设置都变为强制的（单击 Xnest 窗口中的**编辑 > 实施强制**）忽略设置（单击**编辑 > 更改 > 忽略**），或使某设置成为默认设置（既不选择忽略，也不选择强制）。

- 7 要锁定用户设置，请在 Xnest 窗口中单击**编辑 > 锁定**。

可以从下列选项中选择：

面板： 允许您锁定面板，禁用强制退出，禁用锁定屏幕，禁用注销，并在已禁用小程序列表中禁用任何小程序。

OpenOffice： 允许您为 OpenOffice.org 文档定义宏安全性级别，载入和保存选项及用户界面选项。

Epiphany 万维网浏览器： 让您可以隐藏菜单栏、使窗口变为全屏显示，并禁用退出、任意 URL、书签和工具栏编辑以及不安全的协议。

- 8 要保存该配置文件，请单击**配置文件 > 保存**。

该配置文件保存在 `/etc/opt/gnome/desktop-profiles` 中。

- 9 单击**配置文件 > 退出**关闭 Xnest 窗口，然后单击**关闭退出 Sabayon**。

10.15.2 应用配置文件

您可以将配置文件应用到工作站上的单个用户或所有用户。

- 1 单击**计算机 > 更多应用程序 > 系统 > 桌面配置文件编辑器**。
- 2 如果您不是以 root 用户身份登录的，请输入 root 密码，然后单击**继续**。
- 3 选择要应用的配置文件，然后单击**用户**。



4 请选择要使用这个配置文件的用户。

要对这个工作站上的所有用户应用这个配置文件，请单击 *对所有用户使用此配置文件*。

5 单击关闭。

10.16 添加文档模板

要为用户添加文档模板，请在用户的用户主目录中填充 `Templates` 目录。您可以通过将文件复制到 `~/Templates` 为每个用户手动执行该操作，或者在创建用户前通过将包含文档的 `Templates` 目录添加到 `/etc/skel` 在系统范围内执行该操作。

用户通过右键单击桌面然后选择 *创建文档*，从模板中创建一个新的文档。

KDE 配置（供管理员使用）

KDE 是一种可灵活配置的桌面环境。除了可针对个人用户来进行配置，管理员还可以创建全局配置。这使得系统管理员能够提供环境的自定义默认设置。组和各个用户之间的设置可能不同。还可以限制用户可更改的设置。此外，可以限制用户和组访问 KDE 或 KDE 中的功能。

例如，这些全局配置使管理员能够按照企业特征来设置公司范围的桌面，用户将无法更改此桌面。还可以向组织内的不同组指派特定于任务并且只能访问有限应用程序集的配置文​​件。

KDE 在称为配置文件的固定目录树中读取和存储所有配置文件。配置文件是默认设置和限制的集合，可应用于个别用户或用户组。这些配置文件由 KIOSK 框架处理。使用图形“KIOSK 管理工具”来生成和管理配置文件，或可手动编辑并在配置文件中创建文件及结构。

11.1 使用“KIOSK 管理工具”管理配置文件

“Kiosk 管理工具”使您能够通过桌面策略、环境限制和菜单定义来定义配置文件。它使您能够修改现有配置文件，并使您能够将配置文件指派给组 and 用户。Kiosk 还使您能够自动将配置文件部署到远程主机。

可从 KDE 主菜单或通过 `Alt + F2` 及命令 `kiosktool` 来启动“Kiosk 管理工具”。

11.1.1 新建配置文件

要创建新的配置文件，请单击**添加新配置文件**。在打开的对话框中，输入**配置文件名**和**简短说明**。您还可指定配置文件的拥有者。此处指定的用户必须具有该配置文件目录的写访问权限。还需要知道在此处指定的用户的密码。请参见“**向本地计算机部署配置文件**”一节 [263]以获取有关配置文件目录的更多信息。

可以通过**配置文件属性**随时更改在此处输入的数据。

11.1.2 设置配置文件

通过选择现有配置文件并单击**设置配置文件**，为所有 KDE 组件设置配置，例如图标、菜单及文件关联。选择组件后，通过选中各项的复选框激活限制。使用鼠标选择项会显示帮助文本，说明限制将产生的效果。

项说明您能够禁用的特定功能（如**禁用注销选项**）或说明您能够锁定的配置选项（如**锁定屏幕保护程序设置**）。通过执行此操作，当配置文件正在使用时，功能或配置选项不可用。

除了禁用功能和锁定配置选项，您还能配置桌面本身的外观。选择组件**桌面图标**、**桌面背景**、**屏幕保护程序**、**KED 菜单**和**面板**时，将会有两个附加按钮：**设置**和**预览**。单击**设置**时，将装载当前选定配置文件的桌面设置，该设置将覆盖您自己的桌面设置。现在，您可以如同配置自己桌面那样进行更改。通过单击**保存**来确认更改时，所作更改会永久添加到配置文件中并且恢复您自己的桌面设置。

11.1.3 向用户和组指派配置文件

当您创建一个配置文件时，默认情况下它不是“激活”的。首先请将它指派到用户或组。**指派配置文件**将打开一个对话框，您可以在其中向不同用户或组指派所有现有的配置文件。如果将向用户或组应用多个配置文件，则将使用所有配置文件中的设置。如果配置文件包含的设置与其他配置文件中的设置有冲突，则将优先采用较早列出的配置文件中的设置。如果对特定用户应用一个配置文件，而对该用户所属的组应用另一个配置文件，则将应用相同规则。

重要：远程主机上的用户和组

可对本地计算机上的组 and 用户指派配置文件。如果准备向远程服务器部署配置文件，请确保远程主机中所需的用户和组也可在本地计算机上进行访问（例如，通过使用 NIS）。

11.1.4 部署配置文件

“KIOSK 管理工具”不仅使您能够向本地计算机部署配置文件，还使您能够向远程计算机部署配置文件。例如，执行此操作时，您可以将配置文件部署到 NFS 服务器上，然后从 NFS 服务器将配置文件导出到网络上的所有客户机中。

向本地计算机部署配置文件

如果在运行“KIOSK 管理工具”的计算机上部署配置文件，则无需手动操作，管理工具会在启动时对“发现的”配置文件执行操作。默认情况下，所有配置文件都存储在 `/var/lib/kde-profiles` 下，只有 root 用户才能够对此目录执行写操作。建议不要更改此设置。

但是，如果需要更改写入配置文件的位置，请选择 **设置 > 配置 KIOSK 管理工具**，然后更改基本目录。

还可以（但不推荐）将配置文件分发到不同的位置。在配置对话框中，取消选择 **将所有配置文件存储在相同目录下**。执行此操作后，创建配置文件时必须指定该配置文件的目录。

向远程计算机部署配置文件

退出“KIOSK 管理工具”时，“Kiosk 管理工具配置（**设置 > 配置 KIOSK 管理工具**）使您能够在远程主机上指定上载配置文件的位置。此上载机制使用 fish 协议。配置对话框中的 **服务器 URL** 字段通过 `fish://root@host/` 初始化。使用远程服务器上文件的拥有者替换 root，并使用远程主机名替换 host。默认情况下，使用与本地主机上相同的目录。要更改此设置，单击 **打开文件对话框** 在远程服务器上指定一个新的目录。输入远程用户的密码后，可浏览目录。默认情况下，将向指定的 **服务器 URL** 附加本地主机上的目录。可使用 **剥离** 来更改此设置。

默认情况下，KDE 希望将其配置文件放在 `/var/lib/kde-profiles/` 中。如果将配置文件部署到远程计算机上的此目录中或部署到 NFS 服务器上的目录中并且客户机客使用此路径来访问该目录，则无需执行其他操作。否则，调整 `/etc/kde3rc`。有关详细信息，请参见<http://lxr.kde.org/source/KDE/kdelibs/kdecore/doc/README.kiosk>。

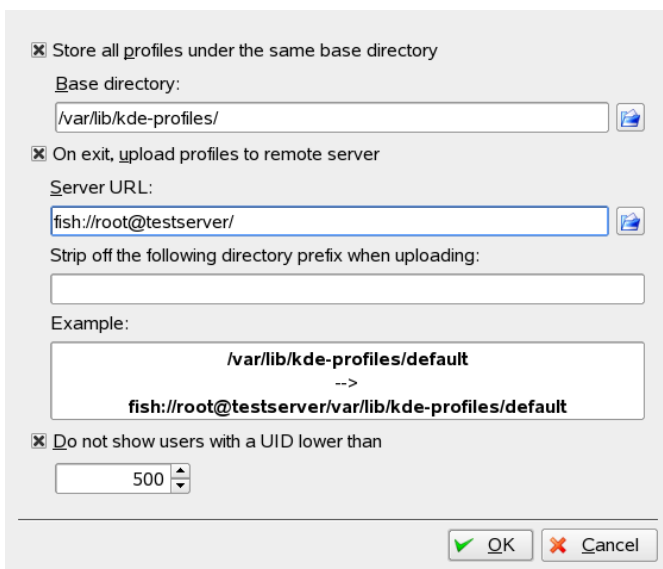
11.1.5 例如：创建和指派配置文件

在以下示例中，将创建名为 `myCompany` 的配置文件并将其指派给远程主机 `testserver` 上的用户 `tester`。



- 1 可从 KDE 主菜单或通过 `Alt + F2` 及命令 `kiosktool` 来启动“Kiosk 管理工具”。
- 2 通过 `设置 > 配置 KIOSK` 打开配置对话框。在本地计算机上，默认情况下所有配置文件都存储在 `/var/lib/kde-profiles/` 中。并且，默认情况下将不显示 UID 低于 500 的用户。

在此示例中，应将配置文件部署到默认配置文件位置中名为 `testserver` 的远程主机。因此，请激活 *On exit* 并且将服务器 URL 更改为 `fish://root@testserver/`。


图 11.1 配置“KIOSK 管理工具”



The screenshot shows a configuration window for the KIOSK Admin Tool. It contains several options and input fields:

- ☒ Store all profiles under the same base directory
Base directory: 
- ☒ On exit, upload profiles to remote server
Server URL: 
- Strip off the following directory prefix when uploading:

Example:

/var/lib/kde-profiles/default
-->
fish://root@testserver/var/lib/kde-profiles/default
- ☒ Do not show users with a UID lower than
 

At the bottom right are **OK** and **Cancel** buttons.

3 打开添加新配置文件对话框并创建名为 myCompany 的新配置文件。

图 11.2 添加配置文件



The screenshot shows the 'Add New Profile' dialog box in the KIOSK Admin Tool. It has a menu bar with 'File', 'Settings', and 'Help'. The title bar says 'KIOSK Admin Tool' and the window title is 'Add New Profile'. The dialog contains the following fields:

- Profile name:
- Short description:
- Files in this profile will be owned by: 
- Directory for this profile:

At the bottom are **Cancel** and **Add** buttons.

单击**完成**以保存新配置文件。在保存文件之前将提示您输入 `root` 密码。

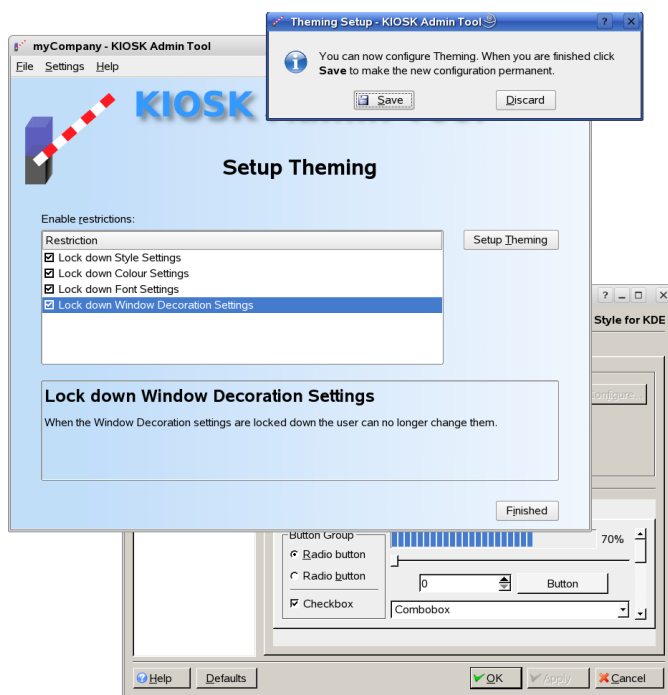
- 4 单击**设置配置文件**将打开一个对话框，可在其中配置 KDE 的各个方面。

图 11.3 设置配置文件



例如，如果选择**主题设置**并选择**设置主题**，则将打开主题的配置对话框。在此处所作的所有更改都不会影响当前的桌面，但是在**主题设置**窗口中通过**保存**确认更改后，这些更改将会被添加到您正在操作的配置文件中。

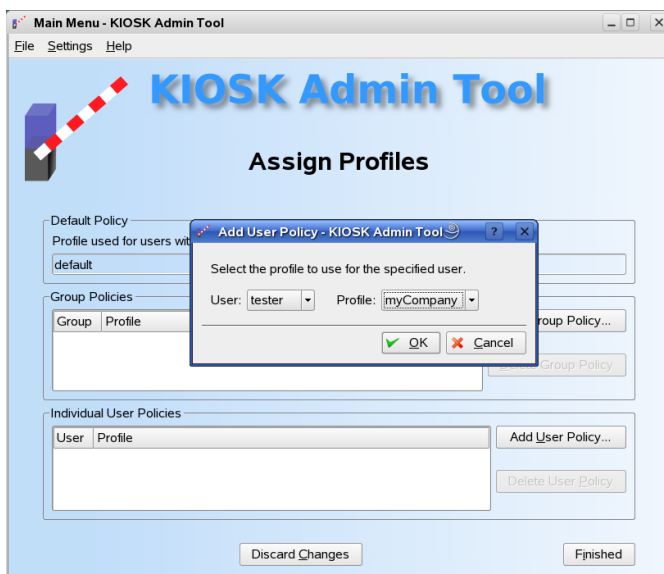
图 11.4 设置主题



设置完配置文件后，可通过单击完成返回主菜单。

- 5 通过单击指派配置文件将配置文件指派给个别的用户或组。

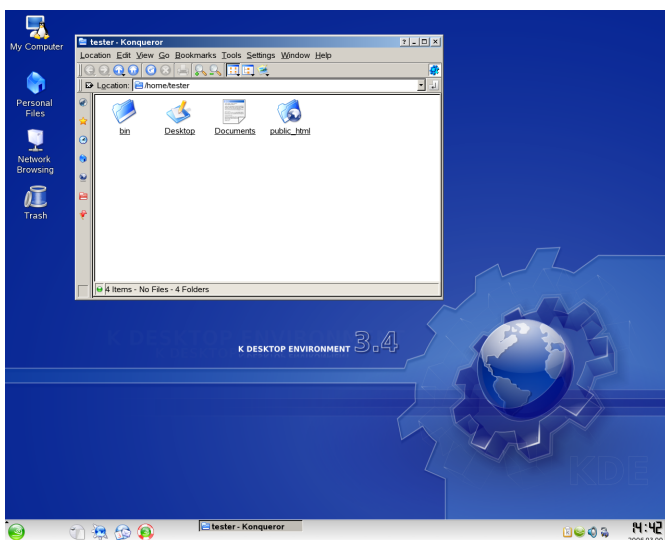
图 11.5 指派配置文件



通过单击完成返回主菜单。

- 6 现在可在本地计算机上使用配置文件。在将配置文件部署到远程主机之前，可对其进行测试。通过鼠标右键单击桌面并选择切换用户 > 启动新会话来启动新会话，然后作为用户 `tester` 登录。

图 11.6 使用中的配置文件



通过注销 `tester` 来返回您自己的桌面。如果您需要作出更改，请再次启动安装程序。否则请退出 KIOSK 管理工具。退出时，“KIOSK 管理工具”会将所有配置文件部署到 `testserver`。在 `testserver` 上您必须输入 `root` 密码来执行此操作。因为在此示例中配置文件被部署到默认 KDE 配置文件位置，因此无需执行其他操作。下次 `tester` 登录 `testserver` 时，将使用 `myCompany` 配置文件。

11.2 手动管理配置文件

如果希望使用图形工具来手动编辑配置文件，则 KIOSK 框架也允许您如此操作。配置文件中的每个配置文件都是一个纯文本文件，可使用选择的编辑器来编辑该纯文本文件。“KDE Source Repository”（<http://websvn.kde.org/trunk/KDE/kdelibs/kdecore/README.kiosk?view=markup>）中详细说明了 KIOSK 的配置和部署选项。请参考此资源以获取详细信息。下面将只说明使用 KIOSK 框架所需的基础设置。

11.2.1 文件系统层级

KDE 会在固定目录树中读取和存储 KDE 环境本身以及 KDE 应用程序使用的文件，在此上下文中也称为“配置文件”。在默认情况下，有两个目录：`/opt/kde3` 和 `~/.kde`。`~/.kde` 目录包含了特定于用户的设置。`/opt/kde3` 目录包含了数据包里的数据和配置文件。不建议在这两个目录中执行更改，因为更改会被下一次更新覆盖。因此，作为系统管理员，您可以创建 KIOSK 框架使用的其他树。附加固定目录树的默认位置为 `/var/lib/kde-profiles`。您可以在 `/etc/kde3rc` 中添加自定义位置。有关详细信息，请参见 KIOSK 文档。

固定目录树包含以下目录（但并不需要存在所有目录）：

```
bin
    可执行文件

cgi-bin
    帮助中心脚本

lib
    库

socket-<HOSTNAME>
    通信套接字

tmp-<HOSTNAME>
    临时文件

cache-<HOSTNAME>
    超速缓存的数据

共享
    应用程序和配置数据
```

其中，`share` 目录包含以下子目录：

```
share/applications
    KDE 菜单中显示的所有应用程序的 .desktop 文件

share/applnk
    KDE 菜单结构
```

share/config
应用程序和组件的配置文件以及全局配置文件 kdeglobals

share/icons
图标（按每个主题分类）、尺寸和用途类别

share/mimelnk
类型为 **mime** 的 .desktop 文件

share/wallpapers
可用作背景图的图像

优先权

KDE 会扫描系统已知的所有目录树。当特定文件存在于多个目录树中时，优先级顺序将确定所使用的文件。

扫描配置文件时，将应用附加规则。通常情况下，将合并具有相同名称的多个配置文件的内容。但是，如果多次定义了相同配置密钥，则文件中优先级最高的密钥将确定使用的值。

优先原则是：

1. 用户目录（`~/kde`）
2. `/etc/kde3rc` 中配置的目录
3. 系统范围内的默认目录（`/opt/kde3`）

作为用户，可通过设置变量 `$KDEDIRS` 来覆盖此顺序。应使用冒号（`:`）隔开目录。第一个目录的优先级最高，最后一个目录的优先级最低。

11.2.2 配置文件格式

会使用 UTF-8 格式将 KDE 配置文件存储在文本文件中。每个配置选项包含一个密钥和值对，并且位于组内：

```
[Group 1]
key=value
key 2=value 2
```

密钥和值前后的空格将被忽略。但是，密钥和值都可如以上示例中所示包含空格。如果某值会以空格开始或结束，或包含换行或特殊字符，请使用以下特殊代码：

- `\s`: 空格
- `\t`: Tab 键
- `\r`: 回车
- `\n`: 换行
- `\\`: backslash

Shell 扩展

为了使用动态生成的值，KDE 允许您使用 *shell* 扩展。如果密钥后跟 `[$e]`，则将激活 *shell* 扩展。使用此构造时，会在首次读取值时将值写入文件中。通过使用 `[$ie]`，您可以锁定此行为，这样每次读取配置文件时都会评估扩展。Shell 扩展使您能够将环境变量或命令输出用作值。

```
[example group]
UserName=$USER
Group=$(id -g)
HomeDirectory=$HOME
```

本地化

可使用添加到密钥项中的语言代码来本地化所有配置值：

```
[example group]
Label=Language
Label[de]=Sprache
Label[ru]=Язык
```

配置项锁定

可以保护所有配置不被覆盖。您可以锁定所有配置文件、组或各个密钥。可以通过以下三种方式来锁定：在文件开头的单独一行上添加 `[si]` 来锁定文件；将 `[Si]` 放在组名称之后来锁定组；将 `[si]` 放在密钥后来锁定密钥。

```
[example group][$i]
    Label=Language

[example group 2]
    UserName[$i]=$USER
```

11.2.3 激活配置文件

在文件系统的任何地方都可以创建配置文件。要使 KDE 环境读取您的配置文件，必须将配置文件放在 `/etc/kde3rc` 中以使系统能够找到配置文件。已在该目录配置默认配置文件位置 `/var/lib/kde-profiles/`。

默认情况下，自定义配置文件不会与用户或组关联。可在位于 `/etc/kde-user-profile` 中的用户配置文件映射文件中执行此关联。默认配置文件无需执行此操作。如果在 `/var/lib/kde-profiles/` 下创建名为“default”的配置文件，则该文件将自动与此计算机上的所有用户关联（默认情况下并不存在此配置文件）。

关于激活配置文件，将它们映射到用户的更多细节，请参见 KIOSK 框架文档。

11.2.4 示例

SUSE Linux Enterprise 附带三个预定义配置文件（`redmond`、`simplified` 和 `Thinclient`），这些配置文件位于 `/var/lib/kde-profiles/`。可将这些配置文件用作模版来创建您自己的配置文件。

Active Directory 支持

Active Directory* (AD) 是一种目录服务，基于 LDAP、Kerberos 和 Microsoft Windows 用来管理资源、服务和人员的其他服务。在 MS Windows 网络中，AD 提供关于这些对象的信息，限制对其中任何对象的访问，并强制执行策略。SUSE Linux Enterprise® 可用于加入现有的 AD 域，并将您的 Linux 计算机整合到 Windows 环境中。

12.1 集成 Linux 和 AD 环境

通过将 Linux 客户机配置为加入现有 Active Directory 域的 Active Directory 客户机，可获得纯粹的 SUSE Linux Enterprise Linux 客户机上无法提供的各种功能：

用 SMB 浏览共享文件和文件夹

Nautilus（GNOME 文件管理器）和 Konqueror（KDE 中对应的文件管理器）都支持通过 SMB 浏览共享资源。

通过 SMB 共享文件和文件夹

Gnome 文件管理器 Nautilus 和其对应的 KDE 文件管理器 Konqueror 都支持文件夹和文件共享，就象在 Windows 中那样。

访问并操作 Windows 服务器上的用户数据

通过 Nautilus 和 Konqueror，用户能够访问其 Windows 用户数据并能编辑、创建和删除 Windows 服务器上的文件和文件夹。用户无需重复输入密码就能访问他们的数据。

脱机鉴定

即使用户脱机（例如使用便携式计算机）或AD服务器由于其他原因不可用时，用户也可以登录并访问他们在Linux计算机上的本地数据。

Windows 密码更改

Linux 中的 ASD 支持端口强制实施储存在 Active Directory 中的公司密码策略。显示管理器和控制台支持密码更改讯息并接受您的输入。甚至可以使用 Linux `passwd` 命令设置 Windows 密码。

通过 Kerberized 应用程序一次签到

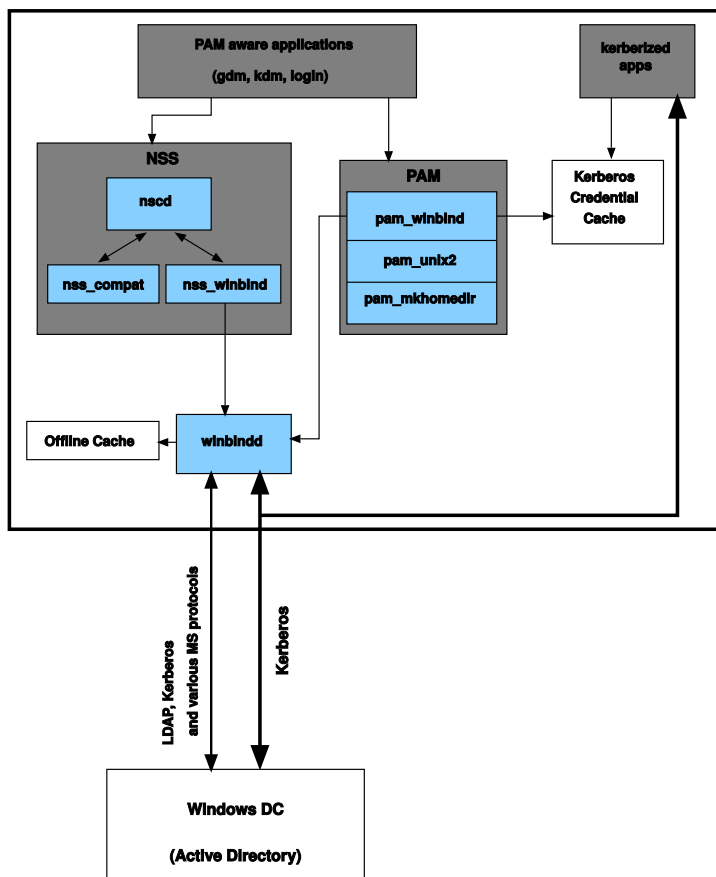
两个桌面的许多应用程序都支持 Kerberos (*kerberized*)，这意味着它们可以透明地为用户处理鉴定，而无需在万维网服务器、代理服务器、群件应用程序或其他位置重输入密码。

下节简要介绍大多数此类功能的技术背景。关于文件和打印机共享的指导，请参见 *GNOME 用户指南* 和 *KDE 用户指南*，在其中您可以了解 GNOME 和 KDE 应用程序世界支持 AD 的更多信息。

12.2 有关 Linux AD 支持的背景信息

许多系统组件需要无故障交互，以便将 Linux 客户程序集成到现有的 Windows Active Directory 域。图 12.1 “Active Directory 鉴定纲要” [277] 重点介绍了最突出的那些组件。以下几节主要讲述 AD 服务器和客户机交互中关键事件的基础进程。

图 12.1 Active Directory 鉴定纲要



为了与目录服务进行通信，客户机至少需要与服务器共享两个协议。

LDAP

LDAP 是一种为管理目录信息而优化的协议。带有 AD 的 Windows 域控制器可以使用 LDAP 协议与客户机交换目录信息。要了解有关 LDAP 概述及其开放源端口 OpenLDAP 的详细信息，请参阅第 35 章 *LDAP - 目录服务* [607]。

Kerberos

Kerberos 是可信的第三方鉴定服务。其所有客户机均信任 Kerberos 对另一台客户机的身份判断，从而支持采用 Kerberos 的一次签到 (SSO) 解决方案。

Windows 支持 Kerberos 实施，因此即使是 Linux 客户机也可以使用 Kerberos SSO。有关 Linux 中 Kerberos 的详细信息，请参阅第 41 章 *网络鉴定 — Kerberos* [675]。

以下客户机组件处理帐户和鉴定数据：

Winbind

本解决方案最核心的部分是 winbind 守护程序，它是 Samba 项目的组成部分，可以处理与 AD 服务器的所有通信。

NSS（名称服务转换）

NSS 例程提供名称服务信息。针对用户和组的命名服务由 nss_winbind 提供。此模块与 winbind 守护程序直接交互。

PAM（可插拔鉴定模块）

AD 用户的用户鉴定是通过 pam_winbind 模块实现的。Linux 客户机上 AD 用户的用户主目录创建是由 pam_mkhomedir 处理的。pam_winbind 模块与 winbind 直接交互。有关 PAM 概述的更多信息，请参阅第 24 章 *通过 PAM 进行鉴定* [449]。

可感知 PAM 的应用程序（如登录例程及 GNOME 和 KDE 显示管理器）与 PAM 及 NSS 层交互，以便对 Windows 服务器进行鉴定。支持 Kerberos 鉴定的应用程序（如文件管理器、万维网浏览器或电子邮件客户程序）使用 Kerberos 身份凭证超速缓存来访问用户的 Kerberos 票证，因此而成为 SSO 框架的组成部分。

12.2.1 域加入

在域加入过程中，服务器和客户机确立安全关系。在客户机上，需要执行下列任务来加入 Window 域控制器提供的现有 LDAP 和 Kerberos SSO 环境。整个加入过程由 YaST 域成员资格模块来处理，该模块可以在安装过程中运行或在已安装系统中运行：

- 1 找到了提供 LDAP 和 KDC（密钥发布中心）服务的 Windows 域控制器。
- 2 加入客户机的计算机帐户是在目录服务中创建的。
- 3 客户机的初始票证授予票证 (TGT) 已经获得并储存于其本地 Kerberos 身份凭证超速缓存。客户机需要此 TGT 来获得进一步的票证，使其可以联系其他服务，如联系目录服务器进行 LDAP 查询。

4 NSS 和 PAM 配置要进行调整，使客户机能对域控制器进行鉴定。

客户机引导过程中，将启动 winbind 守护程序并检索计算机帐户的初始 Kerberos 票证。winbindd 自动刷新计算机票证以保持其有效。为了跟踪当前的帐户策略，winbindd 定期查询域控制器。

12.2.2 域登录和用户主目录

Gnome 和 KDE 的登录管理器 GDM 和 KDM 已经被扩展以处理 AD 域登录。用户可以选择登录其计算机已加入的主域或主域的域控制器已经与之确立信任关系的可信域之一。

如第 12.2 节“有关 Linux AD 支持的背景信息”[276]中所述，用户鉴定由多个 PAM 模块调解。用于对 Active Directory 或 NT4 域进行客户机鉴定的 pam_winbind 模块非常清楚可能妨碍用户登录的 Windows 错误条件。Windows 错误代码被转换为相应的用户可读错误讯息，这些讯息是 PAM 通过任意支持的方法（GDM、KDM、控制台和 SSH）在登录中提供的：

密码已失效

用户看到一条讯息，说明密码已经失效，需要更改。系统会直接提示输入新密码，如果新密码不符合公司密码政策（例如密码太短、太简单或已用过）会通知用户。如果用户的密码更改失败，会显示原因，提示输入新密码。

帐户被禁用

用户看到一条错误讯息，说明其帐户已被禁用，应该与系统管理员取得联系。

帐户已锁定

用户看到一条错误讯息，说明其帐户已被锁定，应该与系统管理员取得联系。

密码必须更改

用户可以登录，但会收到警告说密码很快就必须更改了。该警告会在密码失效前三天发出。失效后，用户就不能再登录了。

工作站无效

只允许用户从特定工作站登录，而当前 SUSE Linux Enterprise 计算机不在该列表中，会显示一条消息，说明该用户不能从该工作站登录。

登录时段无效

只允许用户在工作时段登录，如果试图在工作时段之外登录，就会显示一条消息，说明现在不能登录。

帐户已失效

管理员可为特定用户帐户设置失效时间。如果该用户试图在该失效时间以后登录，则会看到一条消息，说明帐户已失效，不能用于登录。

在成功鉴定的过程中，pam_winbind 从 Active Directory 的 Kerberos 服务器中获得票证授予票证 (TGT) 并将其储存在用户的身份凭证超速缓存中。它也负责更新后台中的 TGT 且不需要任何用户交互。

SUSE Linux Enterprise 支持 AD 用户本地用户主目录。如果按第 12.3 节“为 Active Directory 配置 Linux 客户机”[281]中所述通过 YaST 进行配置，用户主目录在 Windows (AD) 用户首次登录时创建到 Linux 客户机。这些主目录在外观上与标准的 Linux 用户主目录完全一样，并且其运行不依赖 AD 域控制器。使用本地用户主目录，可访问该计算机上的用户数据。如果 Linux 客户机已配置为执行脱机鉴定，即使 AD 服务器断开连接也可以执行该操作。

12.2.3 办公服务和策略支持

公司环境中的用户必须能够成为漫游用户，如：切换网络，甚至在断开连接的情况下工作一段时间。为使用户能够登录断开连接的计算机，已经将大量的超速缓存集成到 winbind 守护程序。winbind 守护程序即使在脱机状态下都可强制实施密码策略。它跟踪失败的登录尝试次数并根据 Active Directory 中配置的策略做出反应。在默认情况下将禁用脱机支持，必须在 YaST 域成员资格模块中明确地启用它。

就像在 Windows 中一样，域控制器不可用时，用户仍可用断开连接前获得的 Kerberos 有效票证访问网络资源（除了 AD 服务器本身之外）。域控制器联机时才能处理密码更改。从 AD 服务器断开连接时，用户不能访问保存在该服务器上的任何数据。工作站与网络完全断开连接并稍后再次连接到公司网络时，SUSE Linux Enterprise 会在用户锁定台式机和解除锁定（例如使用台式机屏幕保护程序）时立即获得新的 Kerberos 票证。

12.3 为 Active Directory 配置 Linux 客户机

需要对网络设置做些调整以确保客户机和服务器的正常交互之后，客户机才能加入 AD 域。

DNS

配置客户机，以便使用可将 DNS 请求转发到 AD DNS 服务器的 DNS 服务器。或者配置您的计算机，将 AD DNS 服务器用作名称服务数据源。

NTP

要成功地进行 Kerberos 鉴定，客户机必须准确设置其时间。强烈建议用中央 NTP 时间服务器执行该操作（这也可以是 Active Directory 域控制器上运行的 NTP 服务器）。如果您的 Linux 主机和域控制器之间的时钟相位差超过特定限制，Kerberos 鉴定会失败，客户机只能用较弱的 NTLM (NT LAN Manager) 鉴定登录。

DHCP

如果客户机使用 DHCP 动态网络配置，则要配置 DHCP 来向客户机提供相同的 IP 和主机名。如有可能，使用静态 IP 地址以确保安全。

防火墙

要浏览您的网上邻居，请完全禁用防火墙，或将用于浏览的接口标记为内部区域的一部分。

要更改客户机上的防火墙设置，请作为 root 登录并启动 YaST 防火墙模块。选择接口。从接口列表选择网络接口并单击更改。选择内部区域并单击确定应用您的设置。单击下一步 > 接受退出防火墙设置。要禁用防火墙，只需将服务启动设置为手动并单击下一步 > 接受退出防火墙模块。

AD 帐户

除非 AD 管理员给您提供了该域有效的用户帐户，否则您不能登录 AD 域。使用 AD 用户名和密码从 Linux 客户机登录到 AD 域。

安装期间加入现有的 AD 域或稍后在已安装的系统中使用 YaST 激活 SMB 用户认证。第 3.11.6 节“用户数”[34]中介绍了安装期间的域加入。

注意

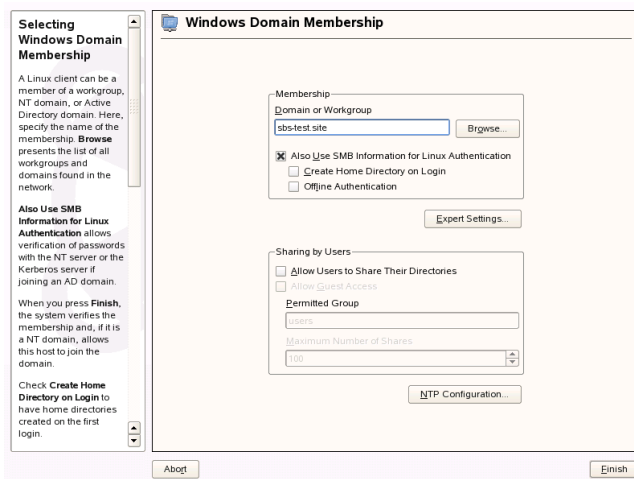
当前只有 Administrator 之类的域管理员帐户可将 SUSE Linux Enterprise 加入到 Active Directory。

要在运行系统中连接 AD 域，请按如下所示继续：

过程 12.1 加入 AD 域

- 1 以 root 身份登录并启动 YaST。
- 2 启动网络服务 > Windows 域成员资格。
- 3 在 Windows 域成员资格屏幕的域或工作组中输入要加入的域（请参见图 12.2 “确定 Windows 域成员资格” [282]）。如果您主机上的 DNS 设置与 Windows DNS 服务器正确集成，请以 DNS 格式 (mydomain.mycompany.com) 输入 AD 域名。如果输入简短域名（也叫 Windows 2000 之前的域名），YaST 要靠 NetBIOS 名称解析（而不是 DNS）来找出正确的域控制器。要从可用域列表中选择，请使用浏览列出 NetBIOS 域，然后选择所需的域。

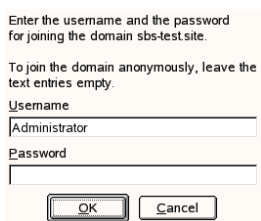
图 12.2 确定 Windows 域成员资格



- 4 选中也使用 SMB 信息进行 Linux 鉴定以使用 SMB 源进行 Linux 鉴定。

- 5 选中**登录时创建用户主目录**以在 Linux 计算机上为 AD 用户自动创建本地用户主目录。
- 6 选中**脱机鉴定**让您的域用户即使在 AD 服务器暂时不可用或者无网络连接的情况下也能够登录。
- 7 如果要更改 Samba 用户和组的 UID 和 GID，请选择**专家设置**。仅在需要时让 DHCP 检索 WINS 服务器。当一些计算机仅通过 WINS 系统解析时，将出现这种情况。
- 8 为 AD 环境配置 NTP 时间同步，方法是选择 *NTP 配置* 并输入相应的服务器名称或 IP 地址。如果已经在独立 YaST NTP 配置模块中输入了相应的设置，则不需要该步骤。
- 9 单击**完成**并在提示时确认域连接。
- 10 在 AD 服务器上提供 Windows 管理员密码并单击**确定**（请参见图 12.3 “提供 Administrator 凭证” [283]）。

图 12.3 提供 Administrator 凭证



Enter the username and the password for joining the domain sbs-test.site.

To join the domain anonymously, leave the text entries empty.

Username
Administrator

Password

OK Cancel

在加入 AD 域之后，使用桌面显示管理器或控制台从工作站登录。

12.4 登录到 AD 域

如果您的计算机已经过配置来对 Active Directory 进行鉴定，且您拥有有效的 Windows 用户身份，则可以使用 AD 身份凭证登录到计算机。对台式机环境（GNOME 和 KDE）、控制台、SSH 和能识别 PAM 的任何其他应用程序，都支持登录。

重要: 脱机鉴定

SUSE Linux Enterprise 支持脱机鉴定, 使您即使在客户机与网络断开连接时也能保持登录到客户机。这可以使您在移动状态下继续工作, 例如您可以在乘飞机时继续工作, 而不必进行网络连接。

12.4.1 GDM 和 KDM

要对 AD 服务器进行 GNOME 客户机鉴定, 请执行以下操作:

- 1 选择域。
- 2 输入您的 Windows 用户名并按 Enter。
- 3 输入 Windows 密码并按 Enter。

要对 AD 服务器进行 KDE 客户机鉴定, 请执行以下操作:

- 1 选择域。
- 2 输入 Windows 用户名。
- 3 输入 Windows 密码并按 Enter。

如果配置是这样, SUSE Linux Enterprise 会在每个 AD 鉴定用户第一次登录时, 在本地计算机上创建用户主目录。这使您可以从 SUSE Linux Enterprise 的 AD 支持中受益, 同时仍可使用功能健全的 Linux 计算机。

12.4.2 控制台登录

除了用图形前端登录到 AD 客户机外, 还可以用基于文本的控制台登录, 甚至用 SSH 远程登录。

要从控制台登录到 AD 客户机, 请在 `login:` 提示处输入 `DOMAIN\user`, 并提供密码。

要使用 SSH 远程登录到 AD 客户机, 请执行以下操作:

- 1 在登录提示符处，输入：

```
ssh DOMAIN\user@hostname
```

\ 域和登录分界符用另一个 \ 号转义了。

- 2 提供用户密码。

12.5 更改密码

SUSE Linux Enterprise 能帮助用户选择符合公司安全策略的合适的新密码。底层 PAM 模块会从域控制器检索当前的密码策略设置。它会以登录消息的方式告诉您用户帐户特定密码通常的质量要求。如 Windows 中的对应程序一样，SUSE Linux Enterprise 提供了以下消息描述：

- 密码历史设置
- 密码最短长度要求
- 密码最短时限
- 密码复杂度

只有成功满足了所有要求后，密码更改过程才算成功。密码状态的反馈会同时通过显示管理器和控制台提供。

GDM 和 KDM 提供有关密码失效的反馈并以交互模式提示输入新密码。要通过显示管理器更改密码，只要按照提示提供密码信息。

要更改 Windows 密码，可以使用标准 Linux 实用程序 `passwd` 而无需在服务器上操作该数据。要更改 Windows 密码，请执行以下操作：

- 1 登录控制台。
- 2 输入 `passwd`。
- 3 在系统提示输入当前密码时输入新密码。
- 4 输入新密码。

- 5 重输入新的密码进行确认。如果新密码不符合 Windows 服务器上的策略，此信息将反馈给您并提示您输入另一个密码。

要从 GNOME 桌面更改 Windows 密码，请按以下步骤操作：

- 1 单击面板左边缘的计算机图标。
- 2 选择控制中心。
- 3 从个人部分，选择更改密码。
- 4 输入旧密码。
- 5 输入并确认新密码。
- 6 保留对话框中的关闭，应用设置。

要从 KDE 桌面更改 Windows 密码，请按以下步骤操作：

- 1 从主菜单选择个人设置。
- 2 选择安全和隐私。
- 3 单击密码和用户帐户。
- 4 单击更改密码。
- 5 输入您当前的密码。
- 6 输入并确认新密码，按确认应用设置。
- 7 按文件 > 退出退出个人设置。

Linux 中的访问控制列表

可以将 POSIX ACL（访问控制列表）作为文件系统对象的传统权限概念的扩展来使用。利用 ACL，可以比传统权限概念更灵活地定义权限。

POSIX ACL 这一术语表明它是一种真正的 *POSIX*（可移植操作系统接口）标准。由于多种原因，相应的标准草案 POSIX 1003.1e 和 POSIX 1003.2c 已被撤销。但是，在属于 UNIX 系列的许多系统上使用的 ACL 都基于这两个草案，并且本章中介绍的文件系统 ACL 的实施也遵照这两个标准。有关它们的信息，请参见 <http://wt.xpilot.org/publications/posix.1e/>。

13.1 传统文件权限

中解释了传统 Linux 文件权限的基础。第 15.2 节“用户和访问权限”[330] 更多高级功能有 `setuid`、`setgid` 和粘滞位。

13.1.1 `setuid` 位

在某些情况下，访问权限可能过于严格。因此，Linux 另有一些设置，允许为执行特定操作临时更改当前用户和组标识。例如，`passwd` 程序通常要求拥有根权限才能访问 `/etc/passwd`。此文件包含一些重要信息，如用户主目录及用户和组 ID。因此，普通用户将无法更改 `passwd`，因为授予所有用户直接访问此文件的权限太过危险。解决该问题的一种可行方案就是 *setuid* 机制。`setuid`（设置用户 ID）是一个特殊的文件特性，它指示系统使用特定用户 ID 执行已相应标记的程序。以 `passwd` 命令为例：

```
-rwsr-xr-x 1 root shadow 80036 2004-10-02 11:08 /usr/bin/passwd
```

您可以看见 `s`，它表示为用户许可设置了 `setuid` 位。通过设置 `setuid` 位，启动 `passwd` 命令的所有用户都以根用户身份执行该命令。

13.1.2 setgid 位

`setuid` 位适用于用户。而对组而言也有一个等价的属性：`setgid` 位。设置了此位的程序基于保存该程序的组 ID 运行，而不论是哪个用户启动了该程序。因此，在设置了 `setgid` 位的目录中，所有新建文件和子目录都被指派到该目录所属的组。请考虑下面的示例目录：

```
drwxrws--- 2 tux archive 48 Nov 19 17:12 backup
```

您可以看见 `s`，它表示为组许可设置了 `setgid` 位。目录的拥有者和组 `archive` 的成员可以访问此目录。不是该组成员的用户会“映射”到各自的组中。“`---`”所有写入文件的有效组 ID 为 `archive`。例如，以组 ID `archive` 运行的备份程序即便没有根特权也能访问此目录。

13.1.3 粘滞位

另外还可以设置粘滞位。属于可执行程序粘滞位和属于目录粘滞位在作用上有所不同。如果属于某个程序，以这种方式标记的文件将被装入 RAM，而不必在每次使用时从硬盘读取。由于目前硬盘的速度已经足够快，此特性已经很少使用。如果为目录指派了此位，则可以防止用户删除彼此的文件。典型示例如 `/tmp` 目录和 `/var/tmp` 目录：

```
drwxrwxrwt 2 root root 1160 2002-11-19 17:15 /tmp
```

13.2 ACL 的优势

传统情况下，会为 Linux 系统上的每个文件对象定义三组权限。这三组权限包括用于每种类型用户（即文件拥有者、组和其他用户这三种用户）的读(`r`)、写(`w`)和执行(`x`)许可权限。此外，还可以设置设置用户 ID、设置组 ID 和粘滞位。这种简缩概念完全适用于大多数实际情况。但对于较复杂的方案或高级应用程序，系统管理员在以前必须采用多种技巧来避开传统权限概念的限制。

可以将ACL作为传统文件权限概念的扩展来使用。它们可用于向单个用户或组分配权限，即使这些权限并不与原始拥有者或所属组相对应。访问控制列表是Linux内核的一项功能。目前，ReiserFS、Ext2、Ext3、JFS和XFS都支持访问控制列表。通过使用ACL，无需在应用程序级别实施复杂的权限模型就可以实现复杂的方案。

如果您想用Linux服务器代替Windows服务器，则ACL的优势尤为明显。即使在移植后，一些已连接的工作站仍可以继续在Windows下运行。Linux系统利用Samba向Windows客户机提供文件和打印服务。有了Samba支持访问控制列表，则既可以在Linux服务器上配置用户权限，也可以在具有图形用户界面的Windows（仅限Windows NT和更高版本）中配置用户权限。利用winbindd（samba套件的一部分），甚至可以向仅存在于Windows域中而在Linux服务器中没有任何帐户的用户分配权限。

13.3 定义

用户类别

传统的POSIX许可权限概念使用三类用户在文件系统中指派权限：拥有者、拥有的组和其他用户。可以为每个用户类别设置三个权限位，用于分配读(r)、写(w)和执行(x)权限。

访问 ACL

各种文件系统对象（文件和目录）的用户和组访问权限均通过访问ACL来确定。

默认 ACL

默认ACL只能应用于目录。它们确定文件系统对象在创建时从其父目录继承的权限。

ACL 项

每个ACL都包含一组ACL项。ACL项中包含一个类型、一个此项所关联的用户或组的限定符和一组权限。对于某些项类型，未定义组或用户的限定符。

13.4 处理 ACL

表 13.1 “ACL 项类型” [290]总结了 ACL 项 6 种可能出现的类型，每种类型都定义了一个或一组用户的权限。拥有者项定义了拥有该文件或目录的用户的权限。所属组项定义了文件所属组的权限。超级用户可以使用 `chown` 或 `chgrp` 更改拥有者或所属组，而在这种情况下，拥有者和所属组项表示新的拥有者和所属组。每个已命名用户项定义了在该项的限定符字段中指定的用户的权限。每个已命名组项定义了在该项的限定符字段中指定的组的权限。只有已命名用户和已命名组项具有非空的限定符字段。其他项定义了所有其他用户的权限。

通过定义这些项中的有效权限和要屏蔽的权限，掩码项进一步限制了已命名用户、已命名组和所属组项授予的权限。如果权限同时存在于上述项之一和掩码中，它们就是有效的。仅包含在掩码或实际项中的权限是无效的 — 表示未授予这些权限。拥有者和所属组项中定义的所有权限始终有效。中的示例说明了这种机制。**表 13.2 “屏蔽访问权限”** [291]。

有两种基本的 ACL 类：一种是最小 ACL，仅包含用于类型拥有者、所属组和其他的项，对应于文件和目录的传统权限位。另一种是扩展 ACL，它比前一种要复杂得多。它必须包含一个掩码项，并可能包含若干已命名用户和已命名组类型的项。

表 13.1 ACL 项类型

类型	文本形式
拥有者	<code>user::rwx</code>
已命名用户	<code>user:name:rwx</code>
所属组	<code>group::rwx</code>
已命名组	<code>group:name:rwx</code>
掩码	<code>mask::rwx</code>
其他	<code>other::rwx</code>

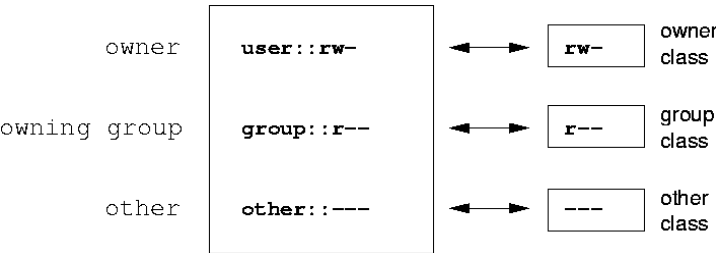
表 13.2 屏蔽访问权限

项类型	文本形式	许可权限
已命名用户	user:geeko:r-x	r-x
掩码	mask::rw-	rw-
	有效权限:	r--

13.4.1 ACL 项和文件方式权限位

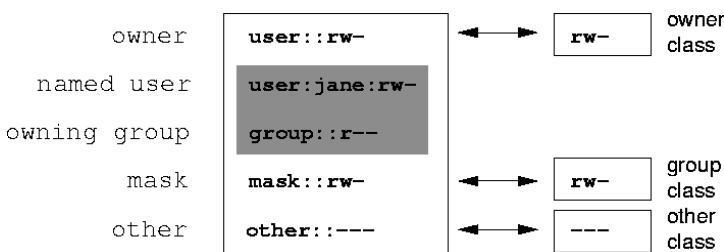
图 13.1 “最小 ACL：与许可权限位相比的 ACL 项” [291]和图 13.2 “最小 ACL：与许可权限位相比的 ACL 项” [292]说明了最小 ACL 和扩展 ACL 这两种情况。这些图分为三块：左边一块显示 ACL 项的类型规范，中间一块显示一个示例 ACL，右边一块显示对应于传统权限概念的各个权限位（如 ls-l 所显示的）。在这两种情况下，拥有者权限均被映射到 ACL 拥有者项。其他类别权限也被映射到各自的 ACL 项。但是，组类别权限的映射在这两种情况中是不同的。

图 13.1 最小 ACL：与许可权限位相比的 ACL 项



对于最小 ACL（没有屏蔽），组类别许可权限被映射到 ACL 项所属的组。中显示了这一工具。图 13.1 “最小 ACL：与许可权限位相比的 ACL 项” [291]对于扩展 ACL（具有屏蔽），组类别许可权限被映射到屏蔽项。中显示了这一工具。图 13.2 “最小 ACL：与许可权限位相比的 ACL 项” [292]。

图 13.2 最小 ACL：与许可权限位相比的 ACL 项



不管应用程序是否具有 ACL 支持，这种映射方式都可以确保应用程序的流畅交互。通过权限位方式分配的访问权限表示通过 ACL 所进行的所有其他“微调”的上限。“”对权限位的更改将由 ACL 反映出来，反之亦然。

13.4.2 具有访问 ACL 的目录

命令行上显示 `getfacl` 和 `setfacl` 的情况下，您可以访问 ACL。以下示例演示了这些命令的用法。

在创建目录之前，使用 `umask` 命令来定义每次创建文件对象时应屏蔽哪些访问权限。命令 `umask 027` 设置了默认权限，即为拥有者分配全部权限 (0)，拒绝组写访问 (2)，并且不为其他用户分配任何权限 (7)。umask 实际上屏蔽了相应的权限位或将它们关闭。有关详细信息，请参考 `umask` 手册页。

`mkdir mydir` 创建具有由 `umask` 设置的默认权限的 `mydir` 目录。使用 `ls -dl mydir` 来检查是否已正确分配所有权限。该示例的输入为：

```
drwxr-x--- ... tux project3 ... mydir
```

使用 `getfaclmydir`，检查 ACL 的初始状态。这样会得出如下信息：

```
# file: mydir
# owner: tux
# group: project3
user::rwx
group::r-x
other::---
```

输出的前三行显示了目录的名称、拥有者和所属组。随后三行包含三个 ACL 项，即拥有者、所属组和其他。事实上，对于最小 ACL，`getfacl` 命令不会生成您使用 `ls` 所不能获得的任何信息。

使用以下命令修改 ACL，为附加用户 `geeko` 和附加组 `mascots` 指派读、写和执行权限：

```
setfacl -m user:geeko:rw,group:mascots:rw mydir
```

选项 `-m` 提示 `setfacl` 修改现有的 ACL。以下参数指示要修改的 ACL 项（各项之间用逗号隔开）。最后部分指定了应该对其应用这些修改的目录的名称。使用 `getfacl` 命令来查看所生成的 ACL。

```
# file: mydir
# owner: tux
# group: project3
user::rw
user:geeko:rw
group::r-x
group:mascots:rw
mask::rw
other:---
```

除了为用户 `geeko` 和组 `mascots` 创建的项外，还生成了一个掩码项。系统自动设置此掩码项，以便使所有权限生效。`setfacl` 自动使现有的掩码项与已修改的设置相适应，但前提是不要用 `-n` 取消此功能。掩码为组类别中的所有项定义了最大有效访问权限。其中包括已命名用户、已命名组和所属组。由 `ls-dl mydir` 显示的组类别权限位现在与掩码项相对应。

```
drwxrw-x---+ ... tux project3 ... mydir
```

输出的第一栏包含一个附加的 `+`，表明此项存在一个扩展 ACL。

根据 `ls` 命令的输出，掩码项的权限包含写访问权限。传统情况下，这样的权限位意味着所属组（这里是 `project3`）也具有对 `mydir` 目录的写访问权限。但是，所属组的有效访问权限对应于为所属组和掩码定义的权限的重叠部分——在我们的示例中是 `r-x`（参阅表 13.2 “屏蔽访问权限” [291]）。对本例中的所属组的有效权限而言，即使是在添加了 ACL 项之后，也未发生任何改变。

用 `setfacl` 或 `chmod` 编辑掩码项。例如，使用 `chmod g-w mydir`。`ls -dl mydir` 输出以下结果：

```
drwxr-x---+ ... tux project3 ... mydir
```

`getfaclmydir` 提供以下输出：

```
# file: mydir
# owner: tux
# group: project3
user::rw
user:geeko:rw          # effective: r-x
```

```
group::r-x
group:mascots:rwx      # effective: r-x
mask::r-x
other::---
```

执行 `chmod` 命令将写权限从组类别位去除后，从 `ls` 命令的输出就可看出掩码位肯定已被相应地更改了：写权限再次被限制为 `mydir` 的所有者。`getfacl` 的输出证实了这一点。这个输出包含了对有效权限位与原始权限不对应的所有项的注释，因为已根据掩码项对它们进行了过滤。可以随时用 `chmod g+w mydir` 来恢复原始权限。

13.4.3 具有默认 ACL 的目录

目录可以具有默认 ACL，这是一种特殊的 ACL，它定义的是此目录下的对象在创建时继承的访问权限。默认 ACL 影响子目录和文件。

默认 ACL 的效果

将目录的默认 ACL 的权限传递到文件和子目录时，有两种方式：

- 子目录继承父目录的默认 ACL 作为其默认 ACL 和访问 ACL。
- 文件继承默认 ACL 作为其访问 ACL。

创建文件系统对象的所有系统调用都使用 `mode` 参数，该参数定义新创建的文件系统对象的访问权限。如果父目录没有默认 ACL，则从 `mode` 参数传递的权限中去除 `umask` 定义的权限位，同时将结果分配到新对象。如果父目录存在默认 ACL，则分配到新对象的权限位对应于 `mode` 参数的权限和默认 ACL 中定义的权限的重叠部分。这种情况下忽略了 `umask`。

默认 ACL 的应用

以下三个示例说明了目录和默认 ACL 的主要操作：

1. 将默认 ACL 添加到现有目录 `mydir`，语句为：

```
setfacl -d -m group:mascots:r-x mydir
```

`setfacl` 命令的 `-d` 选项使 `setfacl` 在默认 ACL 中执行以下修改（选项 `-m`）。

仔细查看此命令的结果：

```
getfacl mydir

# file: mydir
# owner: tux
# group: project3
user::rwx
user:geeko:rwx
group::r-x
group:mascots:rwx
mask::rwx
other:---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other:---
```

`getfacl` 返回访问 ACL 和默认 ACL。默认 ACL 由以 `default` 开头的所有行组成。虽然您只是对 `mascots` 组的一个项执行 `setfacl` 命令来创建默认 ACL，但 `setfacl` 将自动复制访问 ACL 中的所有其他项来创建有效的默认 ACL。默认 ACL 对访问权限没有直接效果。它们只在创建文件系统对象时起作用。这些新对象只从其父目录的默认 ACL 中继承权限。

2. 在下一个示例中，我们将使用 `mkdir` 在 `mydir` 中创建一个子目录，它将继承默认 ACL。

```
mkdir mydir/mysubdir

getfacl mydir/mysubdir

# file: mydir/mysubdir
# owner: tux
# group: project3
user::rwx
group::r-x
group:mascots:r-x
mask::r-x
other:---
default:user::rwx
default:group::r-x
default:group:mascots:r-x
default:mask::r-x
default:other:---
```

根据预期，新创建的子目录 `mysubdir` 具有父目录的默认 ACL 的权限。`mysubdir` 的访问 ACL 准确反映了 `mydir` 的默认 ACL。该目录将向其从属对象传递的默认 ACL 也是相同的。

3. 使用 `touch` 在 `mydir` 目录中创建一个文件，例如 `touch mydir/myfile`。`ls -l mydir/myfile` 输出以下结果：

```
-rw-r-----+ ... tux project3 ... mydir/myfile
```

`getfacl mydir/myfile` 的输出是：

```
# file: mydir/myfile
# owner: tux
# group: project3
user::rw-
group::r-x      # effective:r--
group:mascots:r-x  # effective:r--
mask::r--
other::---
```

当创建新文件时，`touch` 使用值为 `0666` 的 `mode`，这意味所创建的新文件具有用于所有用户类别的读和写权限，前提是 `umask` 或默认 `ACL` 中不存在任何其他限制（请参阅“[默认 ACL 的效果](#)”一节 [294]）。实际上，这意味着 `mode` 值中不包含的所有访问权限均将从各自的 `ACL` 项中去除。虽然没有从组类别的 `ACL` 项中去除任何权限，但仍修改了掩码项来屏蔽不在 `mode` 中设置的权限。

这种方式确保应用程序（如编译器）与 `ACL` 的流畅交互。您可以创建具有有限访问权限的文件，然后将其标记为可执行文件。`mask` 机制确保适当的用户和组可以在需要时执行它们。

13.4.4 ACL 检查算法

在为任何进程或应用程序授予访问受 `ACL` 保护的文件系统对象的权限之前，将应用检查算法。作为基本规则，按照以下序列检查 `ACL` 项：拥有者、命名用户、所属组或命名组以及其他组。访问将根据最适合进程的项进行处理。权限不能累加。

如果某个进程属于多个组并且潜在适合多个组项，情况会更为复杂。这时将从具有所需权限的合适项中随机选择一个。它与是哪些项触发了最终结果“已授权访问”无关。“”同样，如果合适的组项中没有包含所需的权限，则随机选择的项将触发最终结果“访问被拒绝”。“”

13.5 应用程序中的 ACL 支持

ACL 可用于实施非常复杂的权限方案以满足目前应用程序的要求。可以用一种智能方式将传统权限概念和 ACL 结合在一起。像 Samba 和 Konqueror 一样，基本的文件命令（`cp`、`mv`、`ls` 等）支持 ACL。

遗憾的是，许多编辑器和文件管理器仍缺少 ACL 支持。例如，当用 Emacs 复制文件时，这些文件的 ACL 会丢失。当用编辑器修改文件时，文件的 ACL 有时会被保留，有时则会丢失，这取决于所使用编辑器的备份方式。如果编辑器将更改写入原始文件，访问 ACL 就会被保留。如果编辑器将已更新的内容保存到一个新文件，然后将此文件重命名为旧文件名，则 ACL 就可能丢失，除非此编辑器支持 ACL。除了 star 存档程序外，当前没有任何其他备份应用程序保留 ACL。

13.6 更多信息

有关 ACL 的详细信息，请参见 <http://acl.bestbits.at/>。另请参见 `getfacl(1)`、`acl(5)` 和 `setfacl(1)` 的手册页。

系统监视实用程序

一些程序和机制（在此对其中的某些进行了介绍）同时介绍了可用于日常工作的一些实用程序，以及它们最重要的参数。

对于所介绍的每个命令，都将提供相关输出的示例。在这些示例中，第一行是命令本身（在>或#符号提示后）。使用方括号([...])表示省略，必要时对较长的行进行换行。较长的行的换行符由反斜线(\)表示。

```
# command -x -y
output line 1
output line 2
output line 3 is annoyingly long, so long that \
    we have to break it
output line 3
[...]
output line 98
output line 99
```

这里尽量缩短对每个实用程序的说明，从而介绍尽量多的实用程序。手册页中提供了所有命令的详细信息。大多数命令还接受参数--help，该参数将生成可能参数的简要列表。

14.1 调试

14.1.1 指定必需的库：ldd

使用命令 ldd 查找出哪些库将装载指定为参数的动态可执行文件。

```
tux@mercury:~> ldd /bin/ls
linux-gate.so.1 => (0xffffe000)
librt.so.1 => /lib/librt.so.1 (0xb7f97000)
libacl.so.1 => /lib/libacl.so.1 (0xb7f91000)
libc.so.6 => /lib/libc.so.6 (0xb7e79000)
libpthread.so.0 => /lib/libpthread.so.0 (0xb7e67000)
/lib/ld-linux.so.2 (0xb7fb6000)
libattr.so.1 => /lib/libattr.so.1 (0xb7e63000)
```

静态二进制文件不需要任何动态库。

```
tux@mercury:~> ldd /bin/sash
not a dynamic executable
tux@mercury:~> file /bin/sash
/bin/sash: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), for
GNU/Linux 2.6.4, statically linked, for GNU/Linux 2.6.4, stripped
```

14.1.2 程序运行的库调用：ltrace

命令 `ltrace` 使您可以跟踪进程的库调用。此命令的使用方式与 `strace` 类似。参数 `-c` 输出所发生的库调用的次数和持续时间：

```
tux@mercury:~> ltrace -c find ~
% time      seconds  usecs/call   calls      function
-----
34.37      6.758937          245    27554  __errno_location
33.53      6.593562          788     8358  __fprintf_chk
12.67      2.490392          144   17212  strlen
11.97      2.353302          239    9845  readdir64
 2.37      0.466754           27   16716  __ctype_get_mb_cur_max
 1.17      0.230765           27    8358  memcpy
[...]
 0.00      0.000036           36         1  textdomain
-----
100.00     19.662715          105717 total
```

14.1.3 程序运行的系统调用：strace

实用程序 `strace` 使您可以跟踪当前运行的进程的所有系统调用。以正常方式输入命令，在行开头添加 `strace`：

```
tux@mercury:~> strace ls
execve("/bin/ls", ["ls"], [/ 61 vars *]) = 0
uname({sys="Linux", node="mercury", ...}) = 0
brk(0) = 0x805c000
access("/etc/ld.so.preload", R_OK) = -1 ENOENT (No such file or \
directory)
```



```

open("/etc/ld.so.cache", O_RDONLY)          = 3
fstat64(3, {st_mode=S_IFREG|0644, st_size=89696, ...}) = 0
mmap2(NULL, 89696, PROT_READ, MAP_PRIVATE, 3, 0) = 0xb7ef2000
close(3)                                     = 0
open("/lib/librt.so.1", O_RDONLY)           = 3
read(3, "\177ELF\1\1\1\0\0\0\0\0\0\0\3\0\3\0\1\0\0\0000\36\0"... , 512) \
    = 512
fstat64(3, {st_mode=S_IFREG|0755, st_size=36659, ...}) = 0
[...]
stat64(1, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) \
    = 0xb7ca7000
write(1, "bin Desktop Documents music\TM...", 55bin Desktop Documents \
    \ music      Music public_html tmp
) = 55
close(1)                                     = 0
munmap(0xb7ca7000, 4096)                    = 0
exit_group(0)                               = ?

```

例如，要跟踪打开特定文件的所有尝试，请使用以下命令：

```

tux@mercury:~> strace -e open ls .bashrc
open("/etc/ld.so.cache", O_RDONLY)          = 3
open("/lib/librt.so.1", O_RDONLY)           = 3
open("/lib/libacl.so.1", O_RDONLY)          = 3
open("/lib/libc.so.6", O_RDONLY)            = 3
open("/lib/libpthread.so.0", O_RDONLY)      = 3
open("/lib/libattr.so.1", O_RDONLY)         = 3
[...]

```

要跟踪所有子进程，请使用参数 `-f`。可以在很大程度上控制 `strace` 的行为和输出格式。有关信息，请参见 `man strace`。

14.2 文件和文件系统

14.2.1 确定文件类型：file

命令 `file` 可通过检查 `/etc/magic` 而确定一个文件或一个文件列表的类型。

```

tux@mercury:~> file /usr/bin/file
/usr/bin/file: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), \
    for GNU/Linux 2.2.5, dynamically linked (uses shared libs), stripped

```

参数 `-f` 列表指定带有要检查的文件名的列表的文件。 `-z` 允许 `file` 查看压缩文件的内部：

```
tux@mercury:~> file /usr/share/man/man1/file.1.gz
usr/share/man/man1/file.1.gz: gzip compressed data, from Unix, max compression
tux@mercury:~> file -z /usr/share/man/man1/file.1.gz
/usr/share/man/man1/file.1.gz: ASCII troff or preprocessor input text \
(gzip compressed data, from Unix, max compression)
```

14.2.2 文件系统和它们的使用：mount、df 和 du

命令 `mount` 显示在哪个装入点装入哪个文件系统（设备和类型）：

```
tux@mercury:~> mount
/dev/sda3 on / type reiserfs (rw,acl,user_xattr)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
udev on /dev type tmpfs (rw)
devpts on /dev/pts type devpts (rw,mode=0620,gid=5)
/dev/sda1 on /boot type ext2 (rw,acl,user_xattr)
/dev/sda4 on /local type reiserfs (rw,acl,user_xattr)
/dev/fd0 on /media/floppy type subfs (rw,nosuid,nodev,noatime,fs=floppyfss,p
```

使用命令 `df` 可以获得有关文件系统全部使用情况的信息。参数 `-h`（或 `--human-readable`）将输出转换为普通用户可以理解的形式。

```
tux@mercury:~> df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3        11G   3.2G   6.9G   32% /
udev            252M   104K   252M    1% /dev
/dev/sda1        16M    6.6M    7.8M   46% /boot
/dev/sda4        27G    34M    27G    1% /local
```

使用命令 `du` 可以显示给定目录及其子目录中所有文件的总大小。使用参数 `-s` 将不输出详细信息。`-h` 再次将数据转化为人可读的格式：

```
tux@mercury:~> du -sh /local
1.7M    /local
```

14.2.3 有关 ELF 二进制文件的其他信息

用 `readelf` 实用程序来读取二进制文件的内容。这甚至可用于为其他硬件体系结构生成的 ELF 文件：

```
tux@mercury:~> readelf --file-header /bin/ls
ELF Header:
  Magic:   7f 45 4c 46 01 01 01 00 00 00 00 00 00 00 00 00
```

```

Class: ELF32
Data: 2's complement, little endian
Version: 1 (current)
OS/ABI: UNIX - System V
ABI Version: 0
Type: EXEC (Executable file)
Machine: Intel 80386
Version: 0x1
Entry point address: 0x8049b60
Start of program headers: 52 (bytes into file)
Start of section headers: 81112 (bytes into file)
Flags: 0x0
Size of this header: 52 (bytes)
Size of program headers: 32 (bytes)
Number of program headers: 9
Size of section headers: 40 (bytes)
Number of section headers: 30
Section header string table index: 29

```

14.2.4 文件属性：stat

命令 stat 显示文件属性：

```

tux@mercury:~> stat /etc/profile
  File: `/etc/profile'
  Size: 8080          Blocks: 16          IO Block: 4096   regular file
Device: 806h/2054d   Inode: 64942         Links: 1
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2007-07-16 23:28:18.000000000 +0200
Modify: 2006-09-19 14:45:01.000000000 +0200
Change: 2006-12-05 14:54:55.000000000 +0100

```

参数 --filesystem 将生成指定文件所在文件系统的属性详细信息：

```

tux@mercury:~> stat /etc/profile --filesystem
  File: "/etc/profile"
    ID: 0          Namelen: 255          Type: reiserfs
Block size: 4096      Fundamental block size: 4096
Blocks: Total: 2622526   Free: 1809771      Available: 1809771
Inodes: Total: 0        Free: 0

```

14.3 硬件信息

14.3.1 PCI 资源：lspci

命令 `lspci` 列出 PCI 资源：

```
mercury:~ # lspci
00:00.0 Host bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
    DRAM Controller/Host-Hub Interface (rev 01)
00:01.0 PCI bridge: Intel Corporation 82845G/GL[Brookdale-G]/GE/PE \
    Host-to-AGP Bridge (rev 01)
00:1d.0 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #1 (rev 01)
00:1d.1 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #2 (rev 01)
00:1d.2 USB Controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) USB UHCI Controller #3 (rev 01)
00:1d.7 USB Controller: Intel Corporation 82801DB/DBM \
    (ICH4/ICH4-M) USB2 EHCI Controller (rev 01)
00:1e.0 PCI bridge: Intel Corporation 82801 PCI Bridge (rev 81)
00:1f.0 ISA bridge: Intel Corporation 82801DB/DBL (ICH4/ICH4-L) \
    LPC Interface Bridge (rev 01)
00:1f.1 IDE interface: Intel Corporation 82801DB (ICH4) IDE \
    Controller (rev 01)
00:1f.3 SMBus: Intel Corporation 82801DB/DBL/DBM (ICH4/ICH4-L/ICH4-M) \
    SMBus Controller (rev 01)
00:1f.5 Multimedia audio controller: Intel Corporation 82801DB/DBL/DBM \
    (ICH4/ICH4-L/ICH4-M) AC'97 Audio Controller (rev 01)
01:00.0 VGA compatible controller: Matrox Graphics, Inc. G400/G450 (rev 85)
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM) \
    Ethernet Controller (rev 81)
```

使用 `-v` 可以生成更加详细的列表：

```
mercury:~ # lspci
[...]
02:08.0 Ethernet controller: Intel Corporation 82801DB PRO/100 VE (LOM)\
    Ethernet Controller (rev 81)
    Subsystem: Fujitsu Siemens Computer GmbH: Unknown device 1001
    Flags: bus master, medium devsel, latency 66, IRQ 11
    Memory at d1000000 (32-bit, non-prefetchable) [size=4K]
    I/O ports at 3000 [size=64]
    Capabilities: [dc] Power Management version 2
```

从文件 `/usr/share/pci.ids` 中获取有关设备名称解析的信息。此文件中未列出的 PCI ID 标有“未知设备”。

参数 `-vv` 生成程序可查询的所有信息。要查看纯数字值，请使用参数 `-n`。

14.3.2 USB 设备：lsusb

`lsusb` 命令可列出所有 USB 设备。使用 `-v` 选项，可打印更加详细的列表。详细信息从目录 `/proc/bus/usb/` 中读取。以下是连有 USB 设备集线器、内存条、硬盘和鼠标的 `lsusb` 的输出。

```
mercury:/ # lsusb
Bus 004 Device 007: ID 0ea0:2168 Ours Technology, Inc. Transcend JetFlash \
    2.0 / Astone USB Drive
Bus 004 Device 006: ID 04b4:6830 Cypress Semiconductor Corp. USB-2.0 IDE \
    Adapter
Bus 004 Device 005: ID 05e3:0605 Genesys Logic, Inc.
Bus 004 Device 001: ID 0000:0000
Bus 003 Device 001: ID 0000:0000
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 005: ID 046d:c012 Logitech, Inc. Optical Mouse
Bus 001 Device 001: ID 0000:0000
```

14.3.3 关于 SCSI 设备的信息：scsiinfo

`scsiinfo` 命令可列出关于 SCSI 设备的信息。使用选项 `-l`，可列出系统已知的所有 SCSI 设备（通过 `lsscsi` 命令可获取类似的信息）。下面是 `scsiinfo -i /dev/sda` 的输出，它提供关于一个硬盘的信息。选项 `-a` 可提供更加详细的信息。

```
mercury:/ # scsiinfo -i /dev/sda
Inquiry command
-----
Relative Address          0
Wide bus 32               0
Wide bus 16               1
Synchronous neg.         1
Linked Commands           1
Command Queueing          1
SftRe                     0
Device Type               0
Peripheral Qualifier      0
Removable?                0
Device Type Modifier      0
ISO Version               0
ECMA Version              0
ANSI Version              3
AENC                      0
TrmIOP                    0
```

```
Response Data Format                2
Vendor:                            FUJITSU
Product:                           MAS3367NP
Revision level:                     0104A0K7P43002BE
```

该选项 `-d` 可产生缺陷列表，带有两个硬盘坏区表：第一个是供应商提供的（制造商表），第二个是操作中显示的坏区列表（增长表）。如果增长表中的项目数增加，则最好更换硬盘。

14.4 联网

14.4.1 显示网络状态：netstat

`netstat` 显示的是网络连接、路由表 (`-r`)、接口 (`-i`)、伪装连接 (`-M`)、多点广播成员 (`-g`) 和统计信息 (`-s`)。

```
tux@mercury:~> netstat -r
Kernel IP routing table
Destination      Gateway          Genmask         Flags   MSS Window  irtt Iface
192.168.2.0      *                255.255.254.0   U        0  0        0 eth0
link-local       *                255.255.0.0     U        0  0        0 eth0
loopback         *                255.0.0.0       U        0  0        0 lo
default          192.168.2.254   0.0.0.0         UG        0  0        0 eth0

tux@mercury:~> netstat -i
Kernel Interface table
Iface  MTU Met  RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0   1500  0 1624507 129056      0      0  7055      0      0      0 BMNRU
lo     16436  0  23728      0      0      0  23728      0      0      0 LRU
```

显示网络连接或统计数据时，可指定要显示的套接字类型：`TCP(-t)`、`UDP(-u)` 或 `raw(-r)`。`-p` 选项显示套接字所属程序的 `PID` 和名称。

下例列出了所有 `TCP` 连接和使用这些连接的程序。

```
mercury:~ # netstat -t -p
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Pro

tcp      0      0 mercury:33513 www.novell.com:www-http ESTABLISHED 6862/fi
tcp      0    352 mercury:ssh mercury2.:trc-netpoll ESTABLISHED
19422/s
tcp      0      0 localhost:ssh localhost:17828 ESTABLISHED -
```

下面，显示 `TCP` 协议的统计信息：

```
tux@mercury:~> netstat -s -t
Tcp:
  2427 active connections openings
  2374 passive connection openings
  0 failed connection attempts
  0 connection resets received
  1 connections established
  27476 segments received
  26786 segments send out
  54 segments retransmitted
  0 bad segments received.
  6 resets sent
[...]
```

```
TCPAbortOnLinger: 0
TCPAbortFailed: 0
TCPMemoryPressures: 0
```

14.5 /proc文件系统

/proc 文件系统是一个伪文件系统，在该文件系统中，内核以虚拟文件的形式保留重要信息。例如，使用以下命令显示 CPU 类型：

```
tux@mercury:~> cat /proc/cpuinfo
processor       : 0
vendor_id      : AuthenticAMD
cpu family     : 6
model          : 8
model name     : AMD Athlon(tm) XP 2400+
stepping       : 1
cpu MHz        : 2009.343
cache size     : 256 KB
fdiv_bug       : no
[...]
```

用下列命令查询中断的分配和使用：

```
tux@mercury:~> cat /proc/interrupts
CPU0
 0:   3577519      XT-PIC  timer
 1:     130       XT-PIC  i8042
 2:      0       XT-PIC  cascade
 5:   564535      XT-PIC  Intel 82801DB-ICH4
 7:      1       XT-PIC  parport0
 8:      2       XT-PIC  rtc
 9:      1       XT-PIC  acpi, uhci_hcd:usb1, ehci_hcd:usb4
10:      0       XT-PIC  uhci_hcd:usb3
11:    71772      XT-PIC  uhci_hcd:usb2, eth0
12:   101150      XT-PIC  i8042
14:   33146       XT-PIC  ide0
```

```

15:      149202      XT-PIC  ide1
NMI:      0
LOC:      0
ERR:      0
MIS:      0

```

一些重要的文件及其内容如下：

```

/proc/devices
    可用设备

```

```

/proc/modules
    装载的内核模块

```

```

/proc/cmdline
    内核命令行

```

```

/proc/meminfo
    有关内存使用的详细信息

```

```

/proc/config.gz
    当前运行的内核的 gzip 压缩配置文件

```

文本文件 `/usr/src/linux/Documentation/filesystems/proc.txt` 中提供了详细信息。在 `/proc/NNN` 目录中提供了当前运行进程的信息，其中 `NNN` 是相关进程的进程 ID (PID)。每个进程都可以在 `/proc/self/` 中找到它自己的特性：

```

tux@mercury:~> ls -l /proc/self
lrwxrwxrwx 1 root root 64 2007-07-16 13:03 /proc/self -> 5356
tux@mercury:~> ls -l /proc/self/
total 0
dr-xr-xr-x 2 tux users 0 2007-07-16 17:04 attr
-r----- 1 tux users 0 2007-07-16 17:04 auxv
-r--r--r-- 1 tux users 0 2007-07-16 17:04 cmdline
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 cwd -> /home/tux
-r----- 1 tux users 0 2007-07-16 17:04 environ
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 exe -> /bin/ls
dr-x----- 2 tux users 0 2007-07-16 17:04 fd
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 loginuid
-r--r--r-- 1 tux users 0 2007-07-16 17:04 maps
-rw----- 1 tux users 0 2007-07-16 17:04 mem
-r--r--r-- 1 tux users 0 2007-07-16 17:04 mounts
-rw-r--r-- 1 tux users 0 2007-07-16 17:04 oom_adj
-r--r--r-- 1 tux users 0 2007-07-16 17:04 oom_score
lrwxrwxrwx 1 tux users 0 2007-07-16 17:04 root -> /
-rw----- 1 tux users 0 2007-07-16 17:04 seccomp

```



```

-r--r--r-- 1 tux users 0 2007-07-16 17:04 smaps
-r--r--r-- 1 tux users 0 2007-07-16 17:04 stat
[...]
dr-xr-xr-x 3 tux users 0 2007-07-16 17:04 task
-r--r--r-- 1 tux users 0 2007-07-16 17:04 wchan

```

maps文件中包含可执行文件和库的地址指派:

```

tux@mercury:~> cat /proc/self/maps
08048000-0804c000 r-xp 00000000 03:03 17753      /bin/cat
0804c000-0804d000 rw-p 00004000 03:03 17753      /bin/cat
0804d000-0806e000 rw-p 0804d000 00:00 0         [heap]
b7d27000-b7d5a000 r--p 00000000 03:03 11867      /usr/lib/locale/en_GB.utf8/
b7d5a000-b7e32000 r--p 00000000 03:03 11868      /usr/lib/locale/en_GB.utf8/
b7e32000-b7e33000 rw-p b7e32000 00:00 0
b7e33000-b7f45000 r-xp 00000000 03:03 8837        /lib/libc-2.3.6.so
b7f45000-b7f46000 r--p 00112000 03:03 8837        /lib/libc-2.3.6.so
b7f46000-b7f48000 rw-p 00113000 03:03 8837        /lib/libc-2.3.6.so
b7f48000-b7f4c000 rw-p b7f48000 00:00 0
b7f52000-b7f53000 r--p 00000000 03:03 11842      /usr/lib/locale/en_GB.utf8/
[...]
b7f5b000-b7f61000 r--s 00000000 03:03 9109        /usr/lib/gconv/gconv-module
b7f61000-b7f62000 r--p 00000000 03:03 9720        /usr/lib/locale/en_GB.utf8/
b7f62000-b7f76000 r-xp 00000000 03:03 8828        /lib/ld-2.3.6.so
b7f76000-b7f78000 rw-p 00013000 03:03 8828        /lib/ld-2.3.6.so
bfd61000-bfd76000 rw-p bfd61000 00:00 0         [stack]
ffffe000-fffff000 ---p 00000000 00:00 0         [vdso]

```

14.5.1 procinfo

命令 procinfo 对 /proc 文件系统中的重要信息进行了总结:

```

tux@mercury:~> procinfo
Linux 2.6.18.8-0.5-default (geeko@buildhost) (gcc 4.1.2 20061115) #1 2CPU

Memory:      Total      Used      Free      Shared      Buffers
Mem:         2060604    2011264    49340      0         200664
Swap:        2104472      112     2104360

Bootup: Tue Jul 10 10:29:15 2007      Load average: 0.86 1.10 1.11 3/118 21547

user   :      2:43:13.78    0.8%  page in :      71099181  disk 1:  2827023r 968
nice   :    1d 22:21:27.87   14.7%  page out:    690734737
system:    13:39:57.57     4.3%  page act:   138388345
IOwait:    18:02:18.59     5.7%  page dea:   29639529
hw irq:     0:03:39.44     0.0%  page flt:  9539791626
sw irq:     1:15:35.25     0.4%  swap in :           69
idle    :    9d 16:07:56.79   73.8%  swap out:           209
uptime:    6d 13:07:11.14      context :   542720687

```

```

irq 0: 141399308 timer          irq 14: 5074312 ide0
irq 1: 73784 i8042             irq 50: 1938076 uhci_hcd:usb1, ehci_
irq 4: 2                       irq 58: 0 uhci_hcd:usb2
irq 6: 5 floppy [2]           irq 66: 872711 uhci_hcd:usb3, HDA I
irq 7: 2                       irq 74: 15 uhci_hcd:usb4
irq 8: 0 rtc                   irq 82: 178717720 0 PCI-MSI e
irq 9: 0 acpi                  irq169: 44352794 nvidia
irq 12: 3                      irq233: 8209068 0 PCI-MSI 1

```

要查看所有信息，请使用参数 `-a`。参数 `-nN` 每 *N* 秒更新一次信息。在这种情况下，按 `Q` 键终止程序。

默认情况下显示累积值。使用参数 `-d` 将生成差异值。`procinfo -dn5` 显示最近 5 秒内更改的值：

14.6 进程

14.6.1 进程间通讯：ipcs

命令 `ipcs` 生成当前正在使用的 IPC 资源的列表：

```

----- Shared Memory Segments -----
key          shmid      owner      perms      bytes      nattch     status
0x00000000   58261504    tux        600         393216      2           dest
0x00000000   58294273    tux        600         196608      2           dest
0x00000000   83886083    tux        666         43264       2
0x00000000   83951622    tux        666         192000      2
0x00000000   83984391    tux        666         282464      2
0x00000000   84738056    root       644         151552      2           dest

----- Semaphore Arrays -----
key          semid      owner      perms      nsems
0x4d038abf   0          tux        600         8

----- Message Queues -----
key          msqid      owner      perms      used-bytes   messages

```

14.6.2 进程列表：ps

命令 `ps` 生成进程的列表。书写大多数参数时一定不能带减号。请参考 `ps --help` 可获得简要帮助或者参考主页获得详细帮助。

使用 `ps axu` 列出所有进程以及用户和命令行信息：

```
tux@mercury:~> ps axu
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.0    696   272 ?        S    12:59   0:01 init [5]
root         2  0.0  0.0      0     0 ?        SN   12:59   0:00 [ksoftirqd
root         3  0.0  0.0      0     0 ?        S<   12:59   0:00 [events]
[...]
tux      4047  0.0  6.0 158548 31400 ?        Ssl  13:02   0:06 mono-best
tux      4057  0.0  0.7   9036  3684 ?        Sl   13:02   0:00 /opt/gnome
tux      4067  0.0  0.1   2204   636 ?        S    13:02   0:00 /opt/gnome
tux      4072  0.0  1.0  15996  5160 ?        Ss   13:02   0:00 gnome-scre
tux      4114  0.0  3.7 130988 19172 ?        SLl  13:06   0:04 sound-juic
tux      4818  0.0  0.3   4192  1812 pts/0    Ss   15:59   0:00 -bash
tux      4959  0.0  0.1   2324   816 pts/0    R+   16:17   0:00 ps axu
```

要检查有多少个 `sshd` 进程正在运行，请将选项 `-p` 与命令 `pidof` 一起使用，这将列出给定进程的进程 ID。

```
tux@mercury:~> ps -p `pidof sshd`
  PID TTY          STAT TIME COMMAND
 3524 ?           Ss      0:00 /usr/sbin/sshd -o PidFile=/var/run/sshd.init.pid
 4813 ?           Ss      0:00 sshd: tux [priv]
 4817 ?           R        0:00 sshd: tux@pts/0
```

可以根据需要设置进程列表的格式。选项 `-L` 返回所有关键字的列表。输入以下命令可以生成所有进程按内存使用量排序的列表：

```
tux@mercury:~> ps ax --format pid,rss,cmd --sort rss
  PID  RSS CMD
    2     0 [ksoftirqd/0]
    3     0 [events/0]
    4     0 [khelper]
    5     0 [kthread]
   11     0 [kblockd/0]
   12     0 [kacpid]
  472     0 [pdflush]
  473     0 [pdflush]
[...]
 4028 17556 nautilus --no-default-window --sm-client-id default2
 4118 17800 ksnapshot
 4114 19172 sound-juicer
 4023 25144 gnome-panel --sm-client-id default1
 4047 31400 mono-best --debug /usr/lib/beagle/Best.exe --autostarted
 3973 31520 mono-beagled --debug /usr/lib/beagle/BeagleDaemon.exe --bg --aut
```

14.6.3 进程树：pstree

命令 `pstree` 生成树结构的进程列表：

```

tux@mercury:~> pstree
init--NetworkManagerD
    |-acpid
    |-3*[automount]
    |-cron
    |-cupsd
    |-2*[dbus-daemon]
    |-dbus-launch
    |-dcopserver
    |-dhcpcd
    |-events/0
    |-gpg-agent
    |-hald--hald-addon-acpi
    |   `--hald-addon-stor
    |-kded
    |-kdeinit--kdesu---su---kdesu_stub---yast2---y2controlcenter
    |   |-kio_file
    |   |-klauncher
    |   |-konqueror
    |   |-konsole--bash---su---bash
    |   |   `--bash
    |   `--kwin
    |-kdesktop---kdesktop_lock---xmatrix
    |-kdesud
    |-kdm--X
    |   `--kdm---startkde---kwrapper
[...]
```

参数 `-p` 将进程 ID 添加到给定的名称。要让命令行也显示出来，请使用 `-a` 参数：

14.6.4 进程：top

`top` 命令（代表“进程表”）可显示进程的列表，该列表每两秒钟刷新一次。要终止程序，请按 `Q` 键。参数 `-n 1` 在显示一次进程列表后终止程序。下面是 `top -n 1` 命令的示例输出：

```
tux@mercury:~> top -n 1
top - 17:06:28 up 2:10, 5 users, load average: 0.00, 0.00, 0.00
Tasks: 85 total, 1 running, 83 sleeping, 1 stopped, 0 zombie
Cpu(s): 5.5% us, 0.8% sy, 0.8% ni, 91.9% id, 1.0% wa, 0.0% hi, 0.0% si
Mem: 515584k total, 506468k used, 9116k free, 66324k buffers
Swap: 658656k total, 0k used, 658656k free, 353328k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1	root	16	0	700	272	236	S	0.0	0.1	0:01.33	init
2	root	34	19	0	0	0	S	0.0	0.0	0:00.00	ksoftirqd/0
3	root	10	-5	0	0	0	S	0.0	0.0	0:00.27	events/0
4	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	khelper
5	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	kthread
11	root	10	-5	0	0	0	S	0.0	0.0	0:00.05	kblockd/0
12	root	20	-5	0	0	0	S	0.0	0.0	0:00.00	kacpid
472	root	20	0	0	0	0	S	0.0	0.0	0:00.00	pdflush
473	root	15	0	0	0	0	S	0.0	0.0	0:00.06	pdflush
475	root	11	-5	0	0	0	S	0.0	0.0	0:00.00	aio/0
474	root	15	0	0	0	0	S	0.0	0.0	0:00.07	kswapd0
681	root	10	-5	0	0	0	S	0.0	0.0	0:00.01	kseriod
839	root	10	-5	0	0	0	S	0.0	0.0	0:00.02	reiserfs/0
923	root	13	-4	1712	552	344	S	0.0	0.1	0:00.67	udev
1343	root	10	-5	0	0	0	S	0.0	0.0	0:00.00	khubb
1587	root	20	0	0	0	0	S	0.0	0.0	0:00.00	shpchpd_event
1746	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_control
1752	root	15	0	0	0	0	S	0.0	0.0	0:00.00	wl_bus_master1
2151	root	16	0	1464	496	416	S	0.0	0.1	0:00.00	acpid
2165	messageb	16	0	3340	1048	792	S	0.0	0.2	0:00.64	dbus-daemon
2166	root	15	0	1840	752	556	S	0.0	0.1	0:00.01	syslog-ng
2171	root	16	0	1600	516	320	S	0.0	0.1	0:00.00	klogd
2235	root	15	0	1736	800	652	S	0.0	0.2	0:00.10	resmgrd
2289	root	16	0	4192	2852	1444	S	0.0	0.6	0:02.05	hald
2403	root	23	0	1756	600	524	S	0.0	0.1	0:00.00	hald-addon-acpi
2709	root	19	0	2668	1076	944	S	0.0	0.2	0:00.00	NetworkManagerD
2714	root	16	0	1756	648	564	S	0.0	0.1	0:00.56	hald-addon-stor

如果当 top 正在运行时按 F 键，则将打开一个菜单，使用该菜单可以对输出的格式进行全面更改。

参数 -U *UID* 只监视与特定用户关联的进程。将 *UID* 替换为用户 ID。top -u `Id -u` 基于用户名返回用户 *UID*，并显示他的进程。

14.7 系统信息

14.7.1 系统活动信息：sar

要使用 `sar`，需要运行 `sadc`（系统活动数据收集程序）。使用 `rcsysstat \{start|status\}` 检查其状态或启动它。

`sar` 可以生成关于几乎所有重要的系统活动的各种报告，其中包括 CPU、内存、IRQ 使用率、IO 或联网。对于这许多选项，要在这进行进一步的解释是非常复杂的。请参见各种文档中的参考手册页上的例子。

14.7.2 内存使用：free

实用程序 `free` 检查 RAM 使用情况。将显示有关可用内存和已使用内存以及交换区域的详细信息：

```
tux@mercury:~> free
              total        used        free      shared    buffers     cached
Mem:          515584        501704        13880           0        73040        334592
-/+ buffers/cache:      94072        421512
Swap:          658656           0        658656
```

选项 `-b`、`-k`、`-m` 和 `-g` 分别以字节、KB、MB 或 GB 为单位显示输出。参数 `-d delay` 可以确保显示每 *delay* 秒刷新一次。例如，`free -d 1.5` 每 1.5 秒进行一次更新。

14.7.3 访问文件的用户：fuser

它可用于确定当前哪些进程或用户正在访问特定的文件。例如，假定您需要卸装已装入 `/mnt` 的文件系统。`umount` 返回“设备正忙”。然后可使用 `fuser` 命令确定哪些进程正在访问该设备：

```
tux@mercury:~> fuser -v /mnt/*

              USER          PID ACCESS COMMAND
/mnt/notes.txt  tux      26597 f..... less
```

在终止 `less` 进程之后（该进程在另一个终端上运行），便可以成功卸装该文件系统了。

14.7.4 内核信号缓冲区：dmesg

Linux 内核在信号缓冲区中保存某些讯息。要查看这些讯息，请输入命令 `dmesg`：

```
$ dmesg
[...]  
end_request: I/O error, dev fd0, sector 0  
subfs: unsuccessful attempt to mount media (256)  
e100: eth0: e100_watchdog: link up, 100Mbps, half-duplex  
NET: Registered protocol family 17  
IA-32 Microcode Update Driver: v1.14 <tigran@veritas.com>  
microcode: CPU0 updated from revision 0xe to 0x2e, date = 08112004  
IA-32 Microcode Update Driver v1.14 unregistered  
boot splash: status on console 0 changed to on  
NET: Registered protocol family 10  
Disabled Privacy Extensions on device c0326ea0(lo)  
IPv6 over IPv4 tunneling driver  
powernow: This module only works with AMD K7 CPUs  
boot splash: status on console 0 changed to on
```

以前的事件记录在文件 `/var/log/messages` 和 `/var/log/warn` 中。

14.7.5 打开的文件的列表：lsof

要查看为具有进程 ID `PID` 的进程打开的所有文件的列表，请使用 `-p`。例如，要查看当前 `shell` 使用的所有文件，请输入：

```
tux@mercury:~> lsof -p $$  
COMMAND  PID  USER  FD   TYPE DEVICE        SIZE  NODE NAME  
bash     5552 tux    cwd   DIR    3,3      1512 117619 /home/tux  
bash     5552 tux    rtd   DIR    3,3        584    2 /  
bash     5552 tux    txt   REG    3,3  498816  13047 /bin/bash  
bash     5552 tux    mem   REG    0,0          0 [heap] (stat: No such  
bash     5552 tux    mem   REG    3,3  217016 115687 /var/run/nscd/passwd  
bash     5552 tux    mem   REG    3,3  208464  11867 /usr/lib/locale/en_GB.  
bash     5552 tux    mem   REG    3,3  882134  11868 /usr/lib/locale/en_GB.  
bash     5552 tux    mem   REG    3,3 1386997  8837 /lib/libc-2.3.6.so  
bash     5552 tux    mem   REG    3,3  13836  8843 /lib/libdl-2.3.6.so  
bash     5552 tux    mem   REG    3,3  290856 12204 /lib/libncurses.so.5.5  
bash     5552 tux    mem   REG    3,3  26936 13004 /lib/libhistory.so.5.1  
bash     5552 tux    mem   REG    3,3 190200 13006 /lib/libreadline.so.5.  
bash     5552 tux    mem   REG    3,3    54 11842 /usr/lib/locale/en_GB.  
bash     5552 tux    mem   REG    3,3  2375 11663 /usr/lib/locale/en_GB.  
bash     5552 tux    mem   REG    3,3   290 11736 /usr/lib/locale/en_GB.  
bash     5552 tux    mem   REG    3,3   52 11831 /usr/lib/locale/en_GB.  
bash     5552 tux    mem   REG    3,3   34 11862 /usr/lib/locale/en_GB.  
bash     5552 tux    mem   REG    3,3   62 11839 /usr/lib/locale/en_GB.
```

```
bash 5552 tux mem REG 3,3 127 11664 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 56 11735 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 23 11866 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 21544 9109 /usr/lib/gconv/gconv-m
bash 5552 tux mem REG 3,3 366 9720 /usr/lib/locale/en_GB.
bash 5552 tux mem REG 3,3 97165 8828 /lib/ld-2.3.6.so
bash 5552 tux 0u CHR 136,5 7 /dev/pts/5
bash 5552 tux 1u CHR 136,5 7 /dev/pts/5
bash 5552 tux 2u CHR 136,5 7 /dev/pts/5
bash 5552 tux 255u CHR 136,5 7 /dev/pts/5
```

使用了特殊 shell 变量 \$\$，它的值是 shell 的进程 ID。

如果不带任何参数使用命令 `lsuf`，它将列出当前打开的所有文件。由于有数千个打开的文件，大多数情况下不必列出所有这些文件。但是，所有文件的列表可以与搜索功能组合在一起产生有用的列表。例如，列出所有使用过的字符设备：

```
tux@mercury:~> lsuf | grep CHR
bash 3838 tux 0u CHR 136,0 2 /dev/pts/0
bash 3838 tux 1u CHR 136,0 2 /dev/pts/0
bash 3838 tux 2u CHR 136,0 2 /dev/pts/0
bash 3838 tux 255u CHR 136,0 2 /dev/pts/0
bash 5552 tux 0u CHR 136,5 7 /dev/pts/5
bash 5552 tux 1u CHR 136,5 7 /dev/pts/5
bash 5552 tux 2u CHR 136,5 7 /dev/pts/5
bash 5552 tux 255u CHR 136,5 7 /dev/pts/5
X 5646 root mem CHR 1,1 1006 /dev/mem
lsuf 5673 tux 0u CHR 136,5 7 /dev/pts/5
lsuf 5673 tux 2u CHR 136,5 7 /dev/pts/5
grep 5674 tux 1u CHR 136,5 7 /dev/pts/5
grep 5674 tux 2u CHR 136,5 7 /dev/pts/5
```

14.7.6 内核和 udev 事件序列浏览器： udevmonitor

`udevmonitor` 可监听由 `udev` 规则发送的内核 `uevent` 和 `event` 并能将事件的设备路径 (DEVPATH) 打印到控制台。当连接 USB 记忆棒时会出现一系列事件：


```

UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UEVENT[1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806687] add@/class/scsi_host/host4
UEVENT[1138806687] add@/class/usb_device/usbdev4.10
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2
UDEV [1138806687] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806687] add@/class/scsi_host/host4
UDEV [1138806687] add@/class/usb_device/usbdev4.10
UEVENT[1138806692] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UEVENT[1138806692] add@/block/sdb
UEVENT[1138806692] add@/class/scsi_generic/sg1
UEVENT[1138806692] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/devices/pci0000:00/0000:00:1d.7/usb4/4-2/4-2.2/4-2.2
UDEV [1138806693] add@/class/scsi_generic/sg1
UDEV [1138806693] add@/class/scsi_device/4:0:0:0
UDEV [1138806693] add@/block/sdb
UEVENT[1138806694] add@/block/sdb/sdb1
UDEV [1138806694] add@/block/sdb/sdb1
UEVENT[1138806694] mount@/block/sdb/sdb1
UEVENT[1138806697] umount@/block/sdb/sdb1

```

14.7.7 X11 客户机所使用的服务器资源： xrestop

xrestop 提供每个连接的 X11 客户机服务器端资源的统计信息。输出与第 14.6.4 节“进程：top”[312] 非常相似。

```

xrestop - Display: localhost:0
Monitoring 40 clients. XErrors: 0
Pixmaps: 42013K total, Other: 206K total, All: 42219K total

```

res-base	Wins	GCS	Fnts	Pxms	Misc	Pxm mem	Other	Total	PID	Identifier
3e00000	385	36	1	751	107	18161K	13K	18175K	?	NOVELL: SU
4600000	391	122	1	1182	889	4566K	33K	4600K	?	amaroK - S
1600000	35	11	0	76	142	3811K	4K	3816K	?	KDE Deskto
3400000	52	31	1	69	74	2816K	4K	2820K	?	Linux Shel
2c00000	50	25	1	43	50	2374K	3K	2378K	?	Linux Shel
2e00000	50	10	1	36	42	2341K	3K	2344K	?	Linux Shel
2600000	37	24	1	34	50	1772K	3K	1775K	?	Root - Kon
4800000	37	24	1	34	49	1772K	3K	1775K	?	Root - Kon
2a00000	209	33	1	323	238	1111K	12K	1123K	?	Trekstor25
1800000	182	32	1	302	285	1039K	12K	1052K	?	kicker
1400000	157	121	1	231	477	777K	18K	796K	?	kwin
3c00000	175	36	1	248	168	510K	9K	520K	?	de.comp.la
3a00000	326	42	1	579	444	486K	20K	506K	?	[opensuse-
0a00000	85	38	1	317	224	102K	9K	111K	?	Kopete
4e00000	25	17	1	60	66	63K	3K	66K	?	YaST Contr
2400000	11	10	0	56	51	53K	1K	55K	22061	suseplugge
0e00000	20	12	1	50	92	50K	3K	54K	22016	kded

3200000	6	41	5	72	84	40K	8K	48K	?	EMACS
2200000	54	9	1	30	31	42K	3K	45K	?	SUSEWatche
4400000	2	11	1	30	34	34K	2K	36K	16489	kdesu
1a00000	255	7	0	42	11	19K	6K	26K	?	KMix
3800000	2	14	1	34	37	21K	2K	24K	22242	knotify
1e00000	10	7	0	42	9	15K	624B	15K	?	KPowersave
3600000	106	6	1	30	9	7K	3K	11K	22236	konqueror
2000000	10	5	0	21	34	9K	1K	10K	?	klipper
3000000	21	7	0	11	9	7K	888B	8K	?	KDE Wallet

14.8 用户信息

14.8.1 哪些用户在执行哪些操作：w

使用命令 `w`，可以查看哪些用户登录到系统上以及每个用户正在执行哪些操作。例如：

```
tux@mercury:~> w
 16:33:03 up 3:33, 2 users, load average: 0.14, 0.06, 0.02
USER      TTY      LOGIN@  IDLE   JCPU   PCPU WHAT
tux      :0        16:33   ?xdm?   9.42s  0.15s /bin/sh /opt/kde3/bin/startk
tux      pts/0     15:59    0.00s  0.19s  0.00s w
```

如果其他系统的任何用户远程登录，则参数 `-f` 将显示这些用户从其上建立连接的计算机。

14.9 时间和日期

14.9.1 使用 `time` 进行时间度量

用 `time` 实用程序的命令来确定花费的时间。此实用程序有两个版本：内置 `shell` 和程序 (`/usr/bin/time`)。

```
tux@mercury:~> time find . > /dev/null

real    0m4.051s
user    0m0.042s
sys     0m0.205s
```

使用 Shell

引导 Linux 系统时，您通常会被定向到一个图形用户界面，此界面将引导您完成登录过程以及与系统的后续交互操作。图形用户界面已变得越来越重要且易于使用，但这并不是与系统通信的唯一方式。您也可以使用面向文本的通信方式，如通常称为 shell 的命令行解释器，在 shell 中可以输入命令。Linux 提供通过图形用户界面启动 shell 窗口的选项，因此您可以方便地使用两种方式。

在管理中，基于文本的应用程序对于通过慢速网络链接控制计算机或在您希望作为 root 在命令行上执行任务时非常重要。对于 Linux“菜鸟”，在 shell 中输入命令可能不太习惯，但不久后您就会意识到 shell 不仅仅是为管理员而准备的——其实，shell 通常是执行日常任务的最快捷、最方便的方式。

UNIX 或 Linux 有多个 shell。SUSE® Linux Enterprise 中的默认 shell 是 Bash (GNU Bourne-Again Shell)。

本章介绍使用 shell 时必须了解的一些基础知识。包含以下主题：如何输入命令、Linux 的目录结构、如何使用文件和目录以及如何使用一些基本功能、Linux 的用户和权限概念、重要 shell 命令的概要以及 vi 编辑器（Unix 和 Linux 系统中始终可用的默认编辑器）的简短描述。

15.1 Bash shell 入门

在 Linux 中，您可以使用与图形用户界面并行的命令行并在两者之间轻松切换。要通过 KDE 中的图形用户界面启动终端窗口，请单击面板中的 Konsole 图标。在 GNOME 中，单击面板中的 GNOME 终端图标。

此时出现 Konsole 或 GNOME 终端窗口，窗口的第一行显示类似于图 15.1 “Bash 终端窗口示例”[320]所示的提示符。此提示符通常显示您的登录名（在本例中为 tux）、计算机的主机名（此处为 knox）以及当前路径（本例中您的用户主目录，用波浪符 ~ 表示）。当您登录到远程计算机时，您始终可以通过此信息了解到您当前在哪个系统上工作。当光标移到该提示后面时，您可以直接向所在计算机系统发送命令。

图 15.1 Bash 终端窗口示例



15.1.1 输入命令

一条命令包含若干元素。第一个元素总是真正的命令，随后是参数或选项。通过使用 ←、→、←—、Del 和 Space，您可以输入和编辑命令。您还可以添加选项或更正输入错误。按 Enter 时命令将被执行。

重要: 没有消息就是好消息

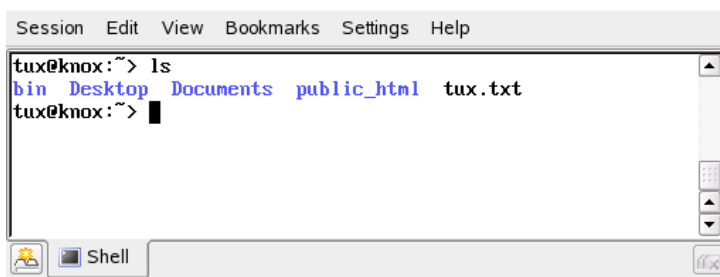
该 shell 很简洁：与某些图形用户界面不同，它在执行命令后通常不提供确认讯息。只有在出现问题或错误的情况下才会显示讯息。

使用命令来删除对象时也要牢记这点。输入 rm 之类的命令删除文件之前，您应了解是否确实要去除此对象：它会被无可挽回地删除，而不会询问您。

使用不带选项的命令

用一个简单的例子看看命令的结构：ls 命令，用于列出目录内容。此命令可带选项也可不带选项。只输入 ls 命令将显示当前目录的内容：

图 15.2 `ls` 命令



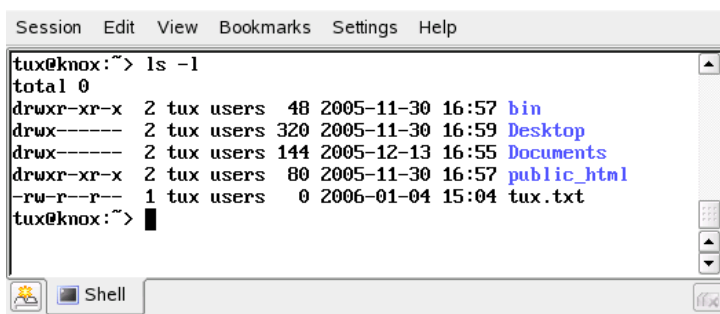
```
Session Edit View Bookmarks Settings Help
tux@knox:~> ls
bin Desktop Documents public_html tux.txt
tux@knox:~> █
```

与其他操作系统不同，Linux 中的文件可带有 `.txt` 等文件扩展名，但扩展名不是必需的。这会造成难以区分 `ls` 输出中的文件和文件夹。默认设置下的颜色可给您提示：目录通常以蓝色显示，文件以黑色显示。

使用带选项的命令

要获得有关目录内容的更多细节，最好使用带选项字符串的 `ls` 命令。选项可修改命令的工作方式，使您能够使用命令来执行特定任务。选项以连字符为前缀，通过空格与命令分隔。命令 `ls -l` 将显示同一目录中内容的详细信息（长列表格式）：

图 15.3 `ls -l` 命令



```
Session Edit View Bookmarks Settings Help
tux@knox:~> ls -l
total 0
drwxr-xr-x  2 tux users  48 2005-11-30 16:57 bin
drwx----- 2 tux users 320 2005-11-30 16:59 Desktop
drwx----- 2 tux users 144 2005-12-13 16:55 Documents
drwxr-xr-x  2 tux users  80 2005-11-30 16:57 public_html
-rw-r--r--  1 tux users   0 2006-01-04 15:04 tux.txt
tux@knox:~> █
```

每个对象名称的左侧都会显示几列有关此对象的信息。最重要的原则如下：第一列显示对象的文件类型（在本例中，`d` 为目录，`-` 为普通文件）。接下来的 9 列显示对象的用户权限。第 11 和 12 列显示文件拥有者和组的名称（本例中为 `tux` 和 `users`）。有关用户权限和 Linux 的用户概念的详细信息，请参见

第 15.2 节 “用户和访问权限” [330]。下一列显示文件大小，单位为字节。然后显示上次更改的日期和时间。最后一列显示对象名称。

如果您想要了解更多信息，您可以组合 `ls` 命令的两个选项并输入 `ls -la`。shell 此时还会显示目录中的隐藏文件，通过在前面加一个圆点来表示（例如 `.hiddenfile`）。

获得帮助

任何用户都没有必要记忆所有命令的所有选项。如果您记住了命令名称但对选项不太确定，您可以先输入命令，紧接着输入一个空格和 `--help`。许多命令都有这个 `--help` 选项。输入 `ls --help` 可以显示 `ls` 命令的所有选项。

15.1.2 Linux 目录结构

shell 不提供与文件管理器中的树视图类似的目录和文件图形化概览，因此有关 Linux 系统中的默认目录结构的基础知识非常有用。您可以将目录视为储存文件、程序和子目录的电子文件夹。层次中的顶级目录是根目录，用 `/` 表示。从此目录可以访问其他所有目录。

图 15.4 显示了 linux 中的标准目录树，其中的用户主目录包含示例用户 `yxz`、`linux` 和 `tux`。`/home` 目录包含用于储存个人用户私人文件的目录。

注意: 网络环境中的用户主目录

如果您在网络环境中工作，您的用户主目录可能不是 `/home`。可将它映射到文件系统中的任何目录。

以下列表简要说明了 Linux 中的标准目录。

图 15.4 标准目录树节选

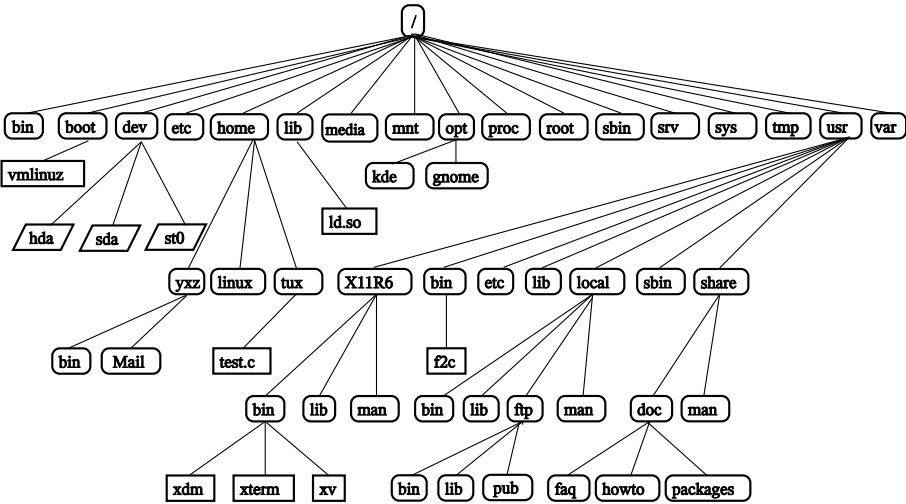


表 15.1 标准目录树概述

//	根目录，目录树的起点
/home	用户的个人目录
/etc	重要的系统配置文件
/bin、/sbin	引导过程中早期所需的程序（/bin）和管理员的程序（/sbin）
/usr、/usr/local	所有应用程序和本地的、与发布版无关的扩展（/usr/local）
/usr/bin、/usr/sbin	通常可访问的程序（/usr/bin）和供系统管理员访问的程序（/usr/sbin）
/usr/share/doc	各种文档文件
/tmp、/var/tmp	临时文件（不要在此目录中保存文件，除非您不需要这些文件）

15.1.3 使用目录和文件

要寻址某一特定文件或目录，您必须指定通向该目录或文件的路径。指定路径的方法有两种：

- 从根目录到相应文件的完整（绝对）路径
- 从当前目录开始的路径（相对路径）

绝对路径始终以斜线开头。相对路径的开头没有斜线。

注意: Linux 区分大小写

Linux 在文件系统中区分大小写。例如，Linux 区别对待输入的 `test.txt` 和 `Test.txt`。输入文件名或路径时请牢记这点。

要更改目录，请使用 `cd` 命令。

- 要切换到用户主目录，请输入 `cd`。
- 用一个圆点 (`.`) 表示当前目录。这主要对其他命令（`cp`、`mv` 和 ...）有用。
- 树的上一级用两个点 (`..`) 来表示。例如，要切换到当前目录的父目录，请输入 `cd ..`。

文件寻址示例

第 15.1.3 节 “使用目录和文件” [324] 中的 `cd` 命令使用相对路径。您也可以使用绝对路径。例如，假设您要将文件从用户主目录复制到 `/tmp` 的一个子目录：

1 首先，通过用户主目录在 `/tmp` 中创建一个子目录：

1a 如果当前目录不是用户主目录，请输入 `cd ~` 切换到用户主目录。无论在文件系统中的何处，您都可以输入 `cd ~` 进入用户主目录。

- 1b** 在用户主目录中输入 `mkdir /tmp/test`。`mkdir` 代表“make directory”，即创建目录。此命令会在 `/tmp` 目录下创建一个名为 `test` 的新目录。此时，使用绝对路径来创建目录。
- 1c** 此时要检查目录中的变化，请输入 `ls -l /tmp`。`/tmp` 目录的内容列表中应出现新目录 `test`。
- 2** 接下来，在用户主目录中创建一个新文件并将使用相对路径它复制到 `/tmp/test` 目录。
 - 2a** 输入 `touch myfile.txt`。带有 `myfile.txt` 选项的 `touch` 命令会在当前目录下创建一个新的空文件，名为 `myfile.txt`。
 - 2b** 输入 `ls -l` 进行检查。内容的列表中应出现新文件。
 - 2c** 输入 `cp myfile.txt ../tmp/test`。这会将 `myfile.txt` 复制到 `/tmp/test` 目录，文件名不会改变。
 - 2d** 输入 `ls -l /tmp/test` 进行检查。`/tmp/test` 目录的内容列表中应出现文件 `myfile.txt`。

要列出其他用户主目录的内容，请输入 `ls ~username`。在图 15.4 “标准目录树节选”[323]的示例目录树中，其中一个样本用户是 `tux`。这样，使用 `ls ~tux` 就会列出 `tux` 用户主目录的内容。

注意: 处理文件名或目录名中的空格

如果文件名包含空格，可在空格前面使用反斜杠 (`\`) 将空格转义或将文件名包含在单引号或双引号中。否则 **Bash** 会将 `My Documents` 这样的文件名解释为两个文件或目录的名称。单引号和双引号的区别在于双引号中可发生变量扩展。而单引号确保 **shell** 按字面查看括起来的字符串。

15.1.4 shell 的实用功能

在 **Bash** 中输入命令可能包含大量键入操作。以下介绍 **Bash** 的一些功能，这些功能可大大简化您的工作，省去大量按键操作。

历史记录和完成

默认情况下，**Bash** 会“记忆”您输入的命令。此功能称为*历史记录*。要重复以前输入过的命令，请按 **↑** 键，直到所希望的命令在提示符处出现。按 **↓** 键以在先前输入命令列表中执行向前移动。使用 **Ctrl + R** 可在历史记录中搜索。

在按 **Enter** 键执行命令之前，可编辑选定的命令，如更改文件名。要编辑命令行，只需使用箭头键将光标移至所需位置并开始键入。

键入文件名或目录名的前几个字母后即补全完整的名称，这是 **Bash** 的另一个实用功能。只需在键入前几个字母后按 **→|** 键即可实现此功能。如果可唯一标识文件名或路径，则会立即补全并且光标移动到文件名的末端。然后您可以输入命令的下一选项（如有必要）。如果文件名或路径不能唯一确定（因为有多个文件名以这些字母开头），则只会将它们补全到之后会有多个选项的那一点。此时再按一次 **→|** 键可获取选项列表。然后您可以输入文件或路径的下一字母并按 **→|** 键重试补全。借助 **→|** 补全文件名和路径的同时，您可以检查您要输入的文件或路径是否确实存在（而且您可以保证拼写无误）。

通配符

shell 的便捷之处还体现在支持路径名扩展的通配符上。通配符是可代表其他字符的字符。**Bash** 提供三种不同的通配符：

?

完全匹配任一字符

*

匹配任意数目的字符

[set]

匹配在方括号中指定的字符组中的任一字符，这里用字符串 *set* 表示字符组。作为 *set* 的一部分，还可以使用语法 *[:class:]* 指定字符类别，其中类别可以是 *alnum*、*alpha* 或 *ascii* 等。

使用 **!** 组开头的或 **^(*!set*)** 匹配 *set* 标识的字符之外的任一字符。

假设 *test* 目录包含文件 *Testfile*、*Testfile1*、*Testfile2* 和 *datafile*。

- 命令 `ls Testfile?` 会列出文件 *Testfile1* 和 *Testfile2*。

- 命令 `ls Testfile?` 会列出文件 `Testfile1` 和 `Testfile2`。
- 使用 `ls Test*`，列表还会包含 `Testfile`。
- 命令 `ls *fil*` 用于显示所有示例文件。
- 使用 `set` 通配符代表最后字符是数字的所有样本文件：`ls Testfile[1-9]` 或使用类：`ls Testfile[[:digit:]]`。

四个通配符中匹配范围最广的是星号。使用它可以将某个目录内的所有文件复制到另一个目录，或通过一个命令删除所有文件。例如，使用命令 `rm *fil*` 可以删除当前目录中文件名包含字符串 *fil* 的所有文件。

使用 Less 和 More 查看文件

Linux 包含两个直接在 shell 中查看文本文件的小程序：`less` 和 `more`。不必启动编辑器来阅读 `Readme.txt` 之类的文件，只需输入 `less Readme.txt` 即可在控制台窗口中显示其中的文本。使用 **Space** 可以向下滚动一页。使用 **Page Up** 和 **Page Down** 可以在文本中前后移动。要退出 `less`，请按 **Q**。

除使用 `less` 之外，您还可以使用 `more` 这种较早的程序。不过，该程序使用起来不太方便，因为它不允许向后滚动。

`less` 程序得名于 *less is more*（少即是多）原则，并且还可用来方便地查看命令输出。要了解该程序的这种功能，请参见“[重定向和管道](#)”一节 [327]。

重定向和管道

通常，shell 的标准输出界面是您的屏幕或控制台窗口，而标准输入设备是键盘。但是，您可用通过 shell 的功能将输入或输出重定向到另一对象，如文件名或另一命令。例如，借助 **>** 和 **<** 符号，您可以将命令的输出转发到一个文件（输出重定向），或者将某文件用作命令的输入（输入重定向）。举例来说，若要将 `ls` 等命令的输出写入文件，请输入 `ls -l > file.txt`。这会创建一个名为 `file.txt` 的文件，此文件包含 `ls` 命令所生成的当前目录的内容列表。但是，如果已存在名为 `file.txt` 的文件，则此命令会覆盖现有文件。要防止这种情况，请使用 **>>**。输入 `ls -l >> file.txt` 只会将 `ls` 命令的输出追加到名为 `file.txt` 的现有文件。如果不存在此文件，则会创建它。

有时将文件用作命令的输入也很实用。例如，通过 `tr` 命令，您可以替换重定向向文件的字符，并将结果写入标准输出，即屏幕。假设要将上例中 `file.txt` 的所有字符 `t` 替换为 `x` 并将结果输出到屏幕上。输入 `tr t x < file.txt` 即可完成此操作。

标准错误输出和标准输出一样，都发送至控制台。要将标准错误输出重定向到名为 `errors` 的文件，则需要在相应命令中追加 `2> errors`。如果追加的是 `>& alloutput`，标准输出和标准错误都将保存到名为 `alloutput` 的文件中。

使用管线或管道也是一种重定向，虽然管道的使用并不局限于文件。通过管道 (`|`)，您可以组合多个命令，将命令的输出用作下一命令的输入。例如，要在 `less` 中查看内容或当前目录，请输入 `ls | less`。这只是在 `ls` 命令正常输出过长时才有意义。例如，当您使用 `ls /dev` 命令查看 `dev` 目录的内容时，您只能在窗口中看到一小部分。而使用 `ls /dev | less` 命令则能够查看整个列表。

15.1.5 存档和数据压缩

您已经创建了一些文件和目录，现在该考虑一下存档和数据压缩的问题了。假定您想将整个 `test` 目录打包在一个文件中，以便备份到 USB 存储器或通过电子邮件发送。要执行该操作，请使用命令 `tar`（代表 *tape archiver*，即磁带存档程序）。使用 `tar --help` 可查看 `tar` 命令的所有选项。下面对最重要的一些选项进行了说明：

- c
（代表 `create`）创建新档案。
- t
（代表 `table`）显示档案中的内容。
- x
（代表 `extract`）对档案解包。
- v
（代表 `verbose`）创建档案时在屏幕上显示所有文件。
- f
（代表 `file`）为档案文件选择一个文件名。创建档案时，此选项总应放在最后。

要将 `test` 目录下的所有文件和子目录打包到名为 `testarchive.tar` 的档案中，请指定以下操作：

- 1 打开 shell。
- 2 使用 `cd` 来转到 `test` 目录所在的用户主目录。
- 3 输入 `tar -cvf testarchive.tar test`。 `-c` 选项会创建存档文件，使其成为 `-f` 所指示的文件。 `-v` 选项会按照这些文件的处理顺序列出文件。
- 4 可使用 `tar -tf testarchive.tar` 查看档案文件的内容。

`test` 目录及其所有文件和目录都在您的硬盘上保持不变。要对档案解包，请输入 `tar -xvf testarchive.tar`，但目前不要尝试。

对文件压缩，典型的选择是 `gzip`，为了得到更好的压缩率，也可选择 `bzip2`。只需输入 `gzip testarchive.tar`（或 `bzip2 testarchive.tar`，但本例中使用的是 `gzip`）。通过 `ls`，您可以看到文件 `testarchive.tar` 已不复存在，取而代之的是文件 `testarchive.tar.gz`。这个文件要小得多，因此也更适于通过电子邮件传送或储存在 USB 储存器上。

现在，将该文件解包到先前创建的 `test2` 目录中。这需要输入 `cp testarchive.tar.gz test2` 将文件复制到该目录中。使用 `cd test2` 转至该目录。扩展名为 `.tar.gz` 的压缩档案可用 `gunzip` 命令解压缩。输入 `gunzip testarchive.tar.gz` 将生成文件 `testarchive.tar`，然后还需使用 `tar -xvf testarchive.tar` 命令抽取或执行 *untar* 操作。您也可以使用以下命令一次完成解压缩并抽取压缩存档：`tar -xvf testarchive.tar.gz`（不再需要添加 `-z` 选项）。通过 `ls`，您会看到新建的 `test` 目录，其内容与用户主目录中的 `test` 目录的内容完全相同。

15.1.6 清理

经过上面的速成培训，您应该对 Linux shell 或命令行的基础知识有了一定的了解。最后，您最好使用 `rm` 和 `rmdir` 命令删除各种测试文件和文件夹，清理您的用户主目录。在 [第 15.3 节“重要的 Linux 命令”](#) [333] 中，查找最重要命令的列表及其功能的简要描述。

15.2 用户和访问权限

自 20 世纪 90 年代初期推出以来，Linux 一直是一种多用户系统。它支持任意数目的用户同时操作。用户在自己的工作站上启动会话之前必须先登录到系统中。每个用户都有一个用户名及对应的密码。设置用户名和密码可以确保未经授权的用户无法查看他们无权查看的文件。而且，进行这种设置后，通常也不可能对系统进行较大改动（如安装新程序），或者限制普通用户执行此类操作。只有根用户或*超级用户*才能不受限制地对系统进行更改并且不受限制地访问所有文件。有效运用这种概念的用户只在必要时才使用不受限制的根用户权限登录，这样可以减小意外丢失数据的风险。由于一般情况下只有根用户才能删除系统文件或格式化硬盘，所以来自特洛伊木马的威胁或意外输入破坏性命令的风险得以显著降低。

15.2.1 文件系统权限

一般而言，Linux 文件系统系统中的每个文件都属于某个用户和某个组。可以为这些专有组和其他所有组授予读、写或执行这些文件的权限。

在这种情况下，可以将组定义为具有特定集合权限的一组相互连接的用户。例如，可以将共同处理某个项目的组称为 `project3`。Linux 系统中的每个用户都是至少一个专有组（通常是 `users`）的成员。可以根据需要设置系统中组的数目，但只有根用户才能添加组。每个用户都可以使用 `groups` 命令查出自己所属的组。

文件访问

文件系统系统中的权限组织结构不同于文件和目录的组织结构。使用 `ls -l` 命令可以显示文件权限信息。命令输出可能如 [例 15.1 “显示文件权限的示例输出”](#) [330] 中所示。

例 15.1 显示文件权限的示例输出

```
-rw-r----- 1 tux project3 14197 Jun 21 15:03 Roadmap
```

如第三列中所示，此文件属于用户 `tux`。该文件被指派给组 `project3`。要确定 `Roadmap` 文件的用户权限，必须仔细检查第一列。

-	rw-	r--	---
---	-----	-----	-----

类型	用户权限	组权限	其他用户的权限
----	------	-----	---------

此列含有一个前置字符，后接九个字符，每三个字符为一组。这十个字符中的第一个字符代表文件系统组件的类型。连字符(-)表示这是一个文件。也可以用d表示目录、l表示链接、b表示块设备，或指明字符设备。

后面的三组字符遵循标准模式。前三个字符表示该文件可读(r)还是不可读(-)。中间的w表示可以编辑相应的对象，而连字符(-)意味着不能写入该文件。排在第三位的x表示可以执行该对象。由于本例中的文件是不可执行的文本文件，所以不必为这个特定文件授予可执行权限。

在本例中，作为文件 Roadmap 的拥有者，tux 有权读(r)写(w)该文件，但无法执行它(x)。project3 组中的成员可以读取该文件，但不能修改或执行它。其他用户无权访问此文件。通过 ACL (Access Control List，访问控制列表)可以指派其他权限。

目录许可权限
 目录的访问权限类型用d来表示。对目录而言，各种权限的含义稍有不同。

例 15.2 显示目录权限的示例输出

```
drwxrwxr-x 1 tux project3 35 Jun 21 15:15 ProjectData
```

在 **例 15.2“显示目录权限的示例输出”** [331] 中，很容易识别出目录 ProjectData 的拥有者 (tux) 和所属组 (project3)。与 **文件访问** [330] 中的文件访问权限相比，设置读权限(r)表示可以显示该目录的内容。写权限(w)表示可以创建新文件。执行权限(x)表示用户可以转到此目录。上例中，用户 tux 及组 project3 中的成员可以转到 ProjectData 目录(x)、查看其中的内容(r)并添加或删除文件(w)。其他用户的权限则受到限制。他们可以进入目录(x)并浏览其中的内容(r)，但不能插入任何新文件(w)。

15.2.2 修改文件权限

更改访问权限
 文件或目录的访问权限可以由拥有者更改，当然也可以由 root 用户更改；更改时要使用命令chmod，后接更改权限的参数及一个或多个文件名。参数可归为四类：

1. 用户相关参数

- u (用户) — 文件的拥有者
- g (组) — 文件所属的组
- o (其他) — 其他用户 (如果未指定参数, 更改将应用到所有类别)

2. 用于删除 (-)、设置 (=) 或插入 (+) 的字符

3. 缩写

- r—读
- w—写
- x—执行

4. 一个文件名或由空格分隔的多个文件名

例如, 在 [例 15.2 “显示目录权限的示例输出” \[331\]](#) 中, 如果用户 tux 还想授予其他用户写入 (w) 目录 ProjectData 的权限, 则可以使用命令 `chmod o+w ProjectData` 执行该操作。

不过, 如果该用户不希望任何用户具有写权限 (其本人除外), 则可以输入命令 `chmod go-w ProjectData` 执行该操作。要防止所有用户向 ProjectData 添加新文件, 请输入 `chmod -w ProjectData`。现在, 如果不首先重建写许可权, 则即使拥有者也无法在目录中创建新文件。

更改所有权

另有一些重要的命令可用来控制文件系统组件的所有权和权限, 这些命令包括 `chown` (更改拥有者) 和 `chgrp` (更改组)。使用命令 `chown` 可将文件所有权转让给另一用户。不过, 只有根用户才有权执行该操作。

假定 [例 15.2 “显示目录权限的示例输出” \[331\]](#) 中的文件 Roadmap 不应再属于 tux, 而应属于用户 geeko, 则根用户应该输入 `chown geeko Roadmap`。

`chgrp` 用于更改文件的组所有权。不过, 文件的拥有者必须是新组的成员。这样, 使用命令 `chgrp project4 ProjectData`, [例 15.1 “显示文件权限的示例输出” \[330\]](#) 中的用户 tux 即可将文件 ProjectData 所属的组更换为 project4, 只要该用户是这个新组的成员。

15.3 重要的 Linux 命令

本节将讨论最重要的命令。本章所列命令只是众多命令中的一小部分。伴随各个命令列出了参数，并且适当的时候还给出了典型的示例应用程序。有关各个命令的详细信息，请使用 `man`，并在后面键入命令名称来查看其手册页，例如 `man ls`。

在参考手册页中，用 `PgUp` 和 `PgDn` 可以上下移动。用 `Home` 和 `End` 可以切换显示文档的开头和结尾。按 `Q` 可以结束这种查看模式。使用 `man man` 可以了解有关 `man` 命令本身的更多信息。

下面的概述中使用不同的字体来表示各个命令元素。实际命令及其必需选项始终显示为命令选项。需要指定的内容或非必需参数均放在 [方括号] 中。

按需调整设置。如果没有名称为 `file` 的文件存在，就不需要写入 `ls file`。通常可以将几个参数组合起来，例如用 `ls -la` 来代替 `ls -l -a`。

15.3.1 文件命令

下节将列出最重要的文件管理命令。它包括从总体文件管理到文件系统 `ACL` 操纵的所有文件管理命令。

文件管理

`ls[options][files]`

如果运行 `ls` 时未附加任何参数，程序将以缩写格式列出当前目录中的内容。

`-l`
详细列表

`-a`
显示隐藏文件

`cp[options]source target`
将 `source` 复制到 `target`。

-i
在覆盖现有 `target` 之前等待确认（如果需要）

-r
递归复制（包含子目录）

`mv[options]source target`
将 `source` 复制到 `target`，然后删除原始 `source`。

-b
在移动 `source` 之前创建该文件的备份副本

-i
在覆盖现有 `targetfile` 之前等待确认（如果需要）

`rm[options]files`
从文件系统中删除指定文件。除非使用选项 `-r`，否则不能使用 `rm` 删除目录。

-r
删除所有现有子目录

-i
在删除各个文件之前等待确认

`ln[options]sourcetarget`
创建从 `source` 到 `target` 的内部链接。通常这种链接直接指向同一文件系统上的 `source`。但是，如果执行带 `-s` 选项的 `ln` 命令，则可以创建一个符号链接，仅指向 `source` 所在的目录，支持跨文件系统的链接。

-s
创建符号链接

`cd[options][directory]`
更改当前目录。执行不带任何参数的 `cd` 命令将转到用户主目录。

`mkdir[options]directory`
创建新目录。

`rmdir[options]directory`
删除指定的目录（如果该目录已清空）。

`chown[options] username[:[group]]files`

将文件所有权转让给具有指定用户名的用户。

`-R`

更改所有子目录中的文件和目录

`chgrp[options]groupnamefiles`

将特定 `file` 的组所有权转让给具有指定组名的组。如果文件所有者既是当前组也是新组的成员，该拥有者只能转让组所有权。

`chmod[options]modefiles`

更改访问权限。

`mode` 参数有三部分：`group`、`access` 和 `access type`。组可接受以下字符：

`u`

用户

`g`

组

`o`

其他

对于 `access`，用 `+` 可以授予权限，用 `-` 可以拒绝授予权限。

`access type` 受以下选项控制：

`r`

读

`w`

写

`x`

执行 - 执行文件或切换到目录

`s`

设置 `uid` 位 — 就像由文件所有者启动那样启动应用程序或程序。

也可以选择使用数字代码。此代码的四位数字由值 4、2 和 1 之和组成 - 即二进制掩码的十进制结果。第一位设置“设置用户 ID (SUID) (4)”标志、“设置组 ID (2)”和粘滞 (1) 位。第二位定义文件拥有者的权限。第三位定义组成员的权限，最后一位设置其他所有用户的权限。用 4 设置读权限，2 设置写权限，1 设置执行文件的权限。文件的拥有者通常都会收到 6 或 7，表示可执行文件。

`gzip[parameters]files`

此程序使用复杂的数学算法压缩文件内容。以这种方式压缩的文件的扩展名为 `.gz`，而且使用前需解压缩。要压缩若干文件甚至是整个目录，请使用 `tar` 命令。

`-d`

将打包的 `gzip` 文件解压缩，使其恢复原始大小，并且能够正常处理（类似命令 `gunzip`）

`taroptionsarchivefiles`

`tar` 将一个或多个文件放入档案。压缩是可选操作。`tar` 是相当复杂的命令，可以附带若干选项。最常用的选项如下：

`-f`

将输出结果写入文件，而不是按惯例显示在屏幕上

`-c`

创建新的 `tar` 档案

`-r`

将文件添加到现有档案中

`-t`

输出档案内容

`-u`

添加文件，但仅适用于文件比档案中已有的文件更新的情况

`-x`

将档案中的文件解包（抽取）

`-z`

用 `gzip` 将生成的档案打包

`-j`
用 bzip2 压缩生成的档案

`-v`
列出已处理的文件

由 tar 创建的档案文件以 `.tar` 结尾。如果这个 tar 档案还使用 gzip 进行了压缩, 则以 `.tgz` 或 `.tar.gz` 结尾。如果是使用 bzip2 压缩的, 则以 `.tar.bz2` 结尾。

locatepatterns

只有在安装 `findutils-locate` 包后, 此命令才可用。使用 `locate` 命令可以查找指定文件所处的目录。如果需要, 可使用通配符来指定文件名。该程序的速度非常快, 因为它使用专为此目的创建的数据库 (而不是搜索整个文件系统)。但这一事实也导致了一个重大缺陷: `locate` 无法找到其数据库最近更新后创建的任何文件。以根用户身份使用 `updatedb` 可以生成该数据库。

updatedb[options]

此命令可以对 `locate` 使用的数据库进行更新。要包含所有现有目录中的文件, 请以根用户身份运行程序。最好通过追加与号 (&) 令程序在后台运行, 这样您就可以紧接着处理同一命令行 (`updatedb &`)。此命令通常作为 **daily cron** 作业运行 (请参见 `cron.daily`)。

find[options]

使用 `find` 可以在指定目录中搜索文件。第一个参数指定搜索的起始目录。选项 `-name` 后面必须紧跟搜索字符串, 字符串中也可以包含通配符。与使用数据库的 `locate` 不同, `find` 扫描的是实际目录。

用于访问文件内容的命令

file[options][files]

使用 `file` 可检测指定文件的内容。

`-z`
尝试查看压缩文件的内部

cat[options]files

`cat` 命令用于显示文件的内容, 使用它可以将所有内容连续打印输出到屏幕上。

`-n`
在左侧对输出编号

`less[options]files`

此命令可用于浏览指定文件的内容。使用 **PgUp** 和 **PgDn** 可以向上或向下滚动半屏，使用 **Space** 可以向下滚动一整屏。使用 **Home** 和 **End** 可以跳转至文件的开头和结尾。按 **Q** 可以退出程序。

`grep[options]searchstringfiles`

grep 命令用于在指定文件中查找特定的搜索字符串。如果找到搜索字符串，该命令将显示找到的 `searchstring` 所在的行及文件名。

`-i`
忽略大小写

`-H`
只显示各个文件的名称，不显示文本行

`-n`
另外显示含有匹配项的行的编号

`-l`
只列出其中不含 `searchstring` 的文件

`diff[options]file1file2`

diff 命令用于比较任意两个文件的内容。该程序生成的输出将列出所有不匹配的行。这是只需发送程序变更而不是全部源代码的编程人员经常使用的命令。

`-q`
只报告两个文件是否不同

`-u`
生成一个“统一”的 `diff`，从而增加输出的可读性。“”

文件系统

`mount[options][device]mountpoint`

使用此命令可以将任意数据介质（如硬盘、CD-ROM 驱动器和其他设备）装入 Linux 文件系统的某个目录。

-r

只读装入

-t filesystem

指定文件系统，通常包括：`ext2`（表示 Linux 硬盘）、`msdos`（表示 MS-DOS 介质）、`vfat`（表示 Windows 文件系统）、`iso9660`（表示 CD）。

对于没有在 `/etc/fstab` 中定义的硬盘，还须同时指定设备类型。在这种情况下只能由根用户装入。如果其他用户也应该能够装入文件系统，则应在 `/etc/fstab` 文件的对应行中输入选项 `user`（用逗号分隔多个用户），并保存所做更改。有关详细信息，请参见 `mount(1)` 手册页。

`umount [options] mountpoint`

此命令可用于从文件系统中卸载装入的驱动器。为防止数据丢失，请在将可移除的数据媒体从其所在驱动器中移除之前运行此命令。通常只有根用户才能运行 `mount` 和 `umount` 命令。要使其其他用户也能运行这些命令，需编辑 `/etc/fstab` 文件，以便为相应的驱动器指定选项 `user`。

15.3.2 系统命令

下节列出了用于检索系统信息以及控制进程和网络的几个最重要的命令。

系统信息

`df [options] [directory]`

`df`（可用磁盘）命令如不与任何选项一同使用，则可以显示磁盘空间总量、当前占用磁盘空间以及所有已装入驱动器上的可用空间等相关信息。如果指定了目录，则只显示有关该目录所在的驱动器的信息。

-h

以用户可读的格式显示占用的块数（以 GB、MB 或 KB 为单位）

-T

文件系统的类型（`ext2`、`nfs`，等等）

`du [options] [path]`

执行此命令时若不带任何参数，则可以显示当前目录中的文件和子目录所占用的磁盘空间总量。

-a
显示各个文件的大小

-h
以用户可读的格式输出

-s
仅显示计算的总大小

`free [options]`

`free` 命令用于显示有关占用 **RAM** 和交换空间的信息，可指明这两个类别中的空间总量和占用量。有关更多信息，请参见第 19.1.6 节“**free 命令**”[390]。

-b
以字节为单位输出

-k
以 **KB** 为单位输出

-m
以 **MB** 为单位输出

`date [options]`

这个简单程序可以显示当前系统时间。如果以根用户身份运行，该程序也可用于更改系统时间。有关该程序的详细信息，请参见 `date(1)` 手册页。

进程

`top [options]`

`top` 提供有关当前运行的进程的快速概览。按 **H** 键可访问一个页面，其中简要说明了用于自定义该程序的主要选项。

`ps [options] [process ID]`

如果运行时未指定任何选项，此命令将显示一个表，其中包含您已经启动的所有程序或进程。此命令的选项前不带连字符。

`aux`

显示所有进程的详细列表，不区分拥有者

`kill [options] process ID`

有时程序并不能正常终止。多数情况下，通过在执行 `kill` 命令时指定相应的进程 `ID` 就应能够停止此类异常程序（请参阅 `top` 和 `ps`）。`kill` 将发送 *TERM* 信号，指示程序自行关闭。如果仍无效，可使用以下参数：

-9

发送一个 *KILL* 信号而不是 *TERM* 信号，这将在几乎所有情况下终止指定的进程。

`killall [options] processname`

此命令类似 `kill`，但它使用进程名（而不是进程 `ID`）作为参数，可以取消具有该名称的所有进程。

网络

`ping [options] 主机名或 IP 地址`

`ping` 命令是用于测试 **TCP/IP** 网络基本功能的标准工具。它可以向目标主机发送一个小的数据包，请求立即回复。如果发送有效，`ping` 将据此显示一条消息，指明网络链接基本有效。

-c 编号

确定要发送的包总数，并且在发送这些包后终止（默认情况下未设置任何限制）。

-f

flood ping：发送尽可能多的数据包；这是为 `root` 用户保留的用于测试网络的常用方法

-i 值

指定发送两个数据包之间的时间间隔（默认值：1 秒）。

`nslookup`

域名系统将域名解析为 **IP** 地址。使用此工具可以将查询发送到名称服务器（**DNS** 服务器）。

`telnet [options] 主机名或 IP 地址 [port]`

Telnet 实际上是一种因特网协议，能支持您跨网络在远程主机上操作。**telnet** 同时也是一个 **Linux** 程序的名称，该程序使用此协议支持远程计算机上的操作。

警告

切勿在第三方可能“窃听的网络上使用 Telnet。”特别是在因特网上，请使用 ssh 之类的加密传送方法，避免恶意使用密码（请参阅有关 ssh 的参考手册页）。

杂项

`passwd [options] [username]`

用户可以使用此命令随时更改自己的密码。root 用户管理员可以使用该命令更改系统中任意用户的密码。

`su [options] [username]`

使用 su 命令可在当前正在运行的会话中以其他用户名登录。指定用户名和相应的密码。采用 root 用户身份时无需提供密码，因为根用户有权采用任意用户的身份。在未指定用户名的情况下使用该命令时，系统将提示您输入根用户密码并切换到超级用户（根用户）。

-

使用 `su -` 可为另一个用户启动登录 shell

`halt [options]`

为避免丢失数据，您应该始终使用此程序关闭系统。

`reboot [options]`

与 halt 的操作相同，只不过系统会立即重引导。

`clear`

此命令用于清空控制台中的可见区域。该命令不带选项。

15.3.3 有关详细信息

本章所列命令只是众多命令中的一小部分。有关其他命令的信息或更详细的信息，建议您参考 O'Reilly 出版的《*Linux in a Nutshell*》。

15.4 vi 编辑器

文本编辑器仍用于执行许多系统管理任务和编程。在 Unix 世界中，vi 是一款很好的编辑器，它提供了便于使用的编辑功能，而且比许多具有鼠标支持的编辑器更符合人体工程学。

15.4.1 操作方式

注意: 按键的显示

在下面找到使用按键就可以在 vi 中输入的一些命令。它们以大写方式显示在键盘上。如果要输入大写的字母，则会通过显示按键组合明确说明，其中包括 Shift 键。

vi 基本上使用三种操作模式：*插入模式*、*命令模式*和*扩展模式*。根据操作方式，各按键具有不同的功能。启动时，vi 通常被设置为命令方式。首先需要了解如何在这些方式之间进行切换：

命令方式切换到插入方式

此时有许多选择，其中使用 **A** 可以进行追加，使用 **I** 可以进行插入，使用 **O** 可以在当前行下创建一个新行。

插入方式切换到命令方式

按 **Esc** 键退出插入方式。不能在插入方式下终止 vi，所以一定要习惯于按 **Esc** 键。

命令方式切换到扩展方式

通过输入冒号 (:) 可以激活 vi 的扩展方式。扩展或 **ex** 方式类似于一个独立的面向行的编辑器，可用于多种简单和较复杂的任务。

扩展方式切换到命令方式

在扩展方式下执行命令后，编辑器将自动返回命令方式。如果决定不在扩展方式下执行任何命令，请使用 **<—** 键删除冒号。编辑器即返回到命令方式。

必须先从插入方式切换到命令方式，之后才能切换到扩展方式。

vi 与其他编辑器一样，也有自己的终止程序的过程。您不能在插入方式下终止 vi。首先，按 *Esc* 键退出插入方式。接下来有两种选择：

1. **退出而不保存：**要终止编辑器而不保存更改，请输入：-Q-!（在命令方式中）。感叹号 (!) 使 vi 忽略任何更改。
2. **保存并退出：**有多种可能的方法可保存更改并终止编辑器。在命令方式下，使用 Shift + Z Shift + Z。要使用扩展方式保存所有更改并退出程序，请输入 -W-Q。在扩展方式中，w 表示写，q 表示退出。

15.4.2 使用 vi

vi 可用作常规编辑器。在插入方式下，可以输入文本，也可以使用 <— 和 Del 删除文本。使用箭头键可以移动光标。

但这些控制键经常会出现问题，因为有许多终端类型使用特殊键代码。这时就要使用命令方式。按 *Esc* 键从插入方式切换到命令方式。在命令方式下，使用 H、J、k 和 l 键移动光标。这些键具有以下功能：

H	左移一个字符
J	下移一行
K	上移一行
L	右移一个字符

在命令方式下，允许命令采用多种变化形式。要多次执行一个命令，只需要在输入实际命令之前输入重复次数即可。例如，输入 5L 可将光标右移 5 个字符。

表 15.2 “vi 编辑器中的简单命令” [344] 中显示了重要命令的选择。此列表不完整。可在 第 15.4.3 节 “有关详细信息” [345] 的文档中找到更完整的列表

表 15.2 vi 编辑器中的简单命令

Esc	更改为命令方式
-----	---------

I	改为插入模式（字符显示在当前光标位置）
一个	改为插入模式（字符插入到当前光标位置之后）
Shift + A	改为插入模式（在行末添加字符）
Shift + R	更改为替换方式（覆盖旧文本）
R	替换光标下的字符
O	改为插入模式（在当前行之后插入新行）
Shift + O	改为插入模式（在当前行之前插入新行）
X	删除当前字符
D - D	删除当前行
D - W	删除到当前单词的末尾
C - W	改为插入模式（用随后输入的内容覆盖当前单词的剩余部分）
U	复原上一个命令
Ctrl + R	重做复原的更改
Shift + J	连接下一行与当前行
.	重复上一个命令

15.4.3 有关详细信息

vi 支持多种不同的命令。它支持使用宏、快捷方式、命名缓冲区和许多其他有用的功能。本手册不包含各种选项的详细描述。SUSE Linux Enterprise 附带 vim（经过改进的 vi），它是 vi 的改进版本。此应用程序有许多信息源：

- vimtutor 是 vim 的交互式教程。

- 在 vim 中，输入命令 `:help` 可以获得有关许多主题的帮助。
- 上联机提供了一本有关 vim 的参考书。<http://www.truth.sk/vim/vimbook-OPL.pdf>
- 位于 <http://www.vim.org> 上的 vim 项目万维网网页提供了各类新闻、邮件列表和其他文档。
- 因特网上有许多 vim 源：<http://www.selflinux.org/selflinux/html/vim.html>、<http://www.linuxgazette.com/node/view/9039> 和 http://www.apmaths.uwo.ca/~xli/vim/vim_tutorial.html。有关指向各教程的链接，请参见<http://linux-universe.com/HOWTO/Vim-HOWTO/vim-tutorial.html>。

重要: VIM 许可证

vim 是一款“慈善软件”，这意味着作者不对此软件收取任何费用，但鼓励您进行捐款以支持一项非营利计划。此项目恳请帮助乌干达的可怜儿童。有关详细信息，请访问<http://iccf-holland.org/index.html>、<http://www.vim.org/iccf/> 和 <http://www.iccf.nl/>。

部分 III. 系统

64 位系统环境中的 32 位和 64 位应用程序

16

SUSE Linux Enterprise® 可用于 64 位平台。但是这并不表示内含的所有应用程序都已移植到 64 位平台上。SUSE Linux Enterprise 支持在 64 位系统环境中使用 32 位应用程序。本章简单介绍了如何在 64 位 SUSE Linux Enterprise 平台上实现这种支持。它解释了如何执行 32 位应用程序（运行时支持）以及应该如何编译 32 位应用程序以使它们既可以在 32 位系统环境中运行，又可以在 64 位系统环境中运行。另外，您还可以了解有关内核 API 的信息和 32 位应用程序如何在 64 位内核下运行的解释。

用于 64 位平台 amd64 和 Intel 64 的 SUSE Linux Enterprise 被设计为可以让现有的 32 位应用程序无需进行额外设置便可以在 64 位环境下运行“。”这种支持意味着您可以继续使用所需的 32 位应用程序，而无需等待对应的 64 位端口可用。

16.1 运行时支持

重要：应用程序版本之间的冲突

如果某个应用程序在 32 位和 64 位环境中都可用，则两个版本的并行安装必定会导致出现问题。在这种情况下，在两个版本中选一个，然后安装并使用这一版本。

若要正确执行，每个应用程序都需要一系列库。不巧的是，这些库的 32 位和 64 位版本的名称是相同的。必须通过另一种方法对它们加以区分。

为了保持与 32 位版本的兼容性，这些库在系统中的储存位置与在 32 位环境中相同。在 32 位和 64 位环境中，libc.so.6 的 32 位版本都位于 /lib/libc.so.6 下。

所有 64 位库和对象文件都位于名为 lib64 的目录中。通常可以在 /lib、/usr/lib 和 /usr/X11R6/lib 下找到的 64 位对象文件现在可以在 /lib64、/usr/lib64 和 /usr/X11R6/lib64 下找到。这意味着 /lib、/usr/lib 和 /usr/X11R6/lib 下有储存 32 位库的空间，因此两个版本的文件名都可以保持不变。

如果对象目录的数据内容不取决于此大小，则不移动 32 位 /lib 目录的任何子目录。例如，X11 字体仍位于 /usr/X11R6/lib/X11/fonts 下的常规位置。此方案符合 LSB（Linux 标准库）和 FHS（文件系统层次标准）。

16.2 软件开发

biarch 开发工具链允许生成 32 位和 64 位对象。默认为编译 64 位对象。通过使用特殊标志也可以生成 32 位对象。对于 GCC，此特殊标志是 -m32。

必须以一种独立于体系结构的形式编写所有头文件。安装的 32 位和 64 位库必须具有与安装的头文件匹配的 API（应用程序编程接口）。普通 SUSE Linux Enterprise 环境是根据此原则设计的。如果是手动更新的库，请自行解决此问题。

16.3 Biarch 平台上的软件编译

若要在 Biarch 体系结构上为其他体系结构开发二进制代码，则必须另外安装用于第二个体系结构的各个库。这些包称为 rpmname-32bit。您还需要 rpmname-devel 包中各自的标题和库以及 rpmname-devel-32bit 中用于第二个体系结构的开发库。

大多数开放源代码程序使用基于 autoconf 的程序配置。若要使用 autoconf 配置第二个体系结构的程序，请通过运行带有附加环境变量的 configure 脚本覆盖 autoconf 的常规编译器和链接器设置。

以下示例涉及 x86 为第二个体系结构的 x86_64 系统。

1 使用 32 位编译器：

```
CC="gcc -m32"
```

- 2 指示链接器处理 32 位对象（总是使用 gcc 作为链接器前端）：

```
LD="gcc -m32"
```

- 3 设置组装器生成 32 位对象：

```
AS="gcc -c -m32"
```

- 4 确定 libtool 等的库是否来自 /usr/lib：

```
LDFLAGS="-L/usr/lib"
```

- 5 确定库是否储存在 lib 子目录中：

```
--libdir=/usr/lib
```

- 6 确定是否使用了 32 位 X 库：

```
--x-libraries=/usr/X11R6/lib/
```

并不是每个程序都需要这些变量。根据各个程序对这些变量进行调整。

```
CC="gcc -m32" \
LDFLAGS="-L/usr/lib;" \
    .configure \
        --prefix=/usr \
        --libdir=/usr/lib
make
make install
```

16.4 内核规范

x86_64 的 64 位内核提供了 64 位和 32 位内核 ABI（应用程序二进制接口）。后者与对应的 32 位内核的 ABI 相同。这意味着 32 位应用程序可以以与 32 位内核交流的相同方式与 64 位内核进行交流。

64 位内核系统调用的 32 位仿真不支持系统程序使用的某些 API。这取决于平台。因此，必须编译少量的应用程序，如 `lspci`

64 位内核只能装载专门为此内核编译的 64 位内核模块。不能使用 32 位内核模块。

提示

某些应用程序需要单独的内核可装载模块。如果要在 64 位系统环境中使用此类 32 位应用程序，请与此应用程序的提供商和 Novell 联系以确保内核可装载模块的 64 位版本和内核 API 的 32 位编译版本可用于此模块。

引导和配置 Linux 系统

引导 Linux 系统包括多个不同组件。硬件本身是由 BIOS 初始化，而 BIOS 通过引导加载程序启动内核。此后，引导过程（包括 `init` 和 `runlevel`）完全受操作系统控制。`runlevel` 概念使您可以维护日常使用的设置，也可以对系统执行维护任务。

17.1 Linux 引导进程

Linux 引导进程包括多个阶段，每个阶段由一个组件来代表。下表概要总结了引导进程并介绍了所涉及的所有主要组件。

1. **BIOS** 在打开计算机后，BIOS 将初始化屏幕和键盘并测试主存储器。直到这一阶段，计算机不访问任何大容量储存媒体。随后，将从 CMOS 值装载有关当前日期、时间和最重要的外设的信息。当识别出第一块硬盘及其空间之后，系统控制将从 BIOS 传递到引导加载程序。
2. **Boot Loader** 第一块硬盘的前 512 个字节的物理数据扇区将被装载到主存储器中，位于此扇区开始位置的引导加载程序将接管系统控制。引导加载程序执行的命令决定了引导进程剩余的部分。因此，第一块硬盘的前 512 个字节被称为主引导记录 (MBR)。引导加载程序随后将控制传递到实际的操作系统（在本例中即 Linux 内核）。有关 Linux 引导加载程序 GRUB 的详细信息，请参见第 18 章 引导加载程序 [367]。
3. **内核和 `initramfs`** 为了传递系统控制，引导加载程序将内核和基于 RAM 的初始文件系统 (`initramfs`) 装载到内存中。内核可以直接使用 `initramfs` 的内容。`initramfs` 包含一个小的可执行文件，称为 `init`，可以进行真实文件系

统的装入处理。如果在访问大容量存储区之前需要特殊硬盘驱动程序，则这些程序必须在 `initramfs` 中。有关 `initramfs` 的详细信息，请参见第 17.1.1 节“`initramfs`” [354]。

4. **initramfs 中的 init** 这个程序执行装入正确的根文件系统所需的所有操作，如为所需的文件系统提供内核功能以及为带有 `udev` 的大容量储存控制器提供设备驱动程序。找到根文件系统后，对其进行错误检查并装入。如果该操作成功，将清除 `initramfs` 并执行根文件系统上的 `init` 程序。有关 `init` 的详细信息，请参阅第 17.1.2 节“`initramfs 中的 init`” [355]。有关 `udev` 的更多信息，请参见第 21 章 *使用 `udev` 进行动态内核设备管理* [419]。
5. **init** `init` 通过提供不同功能的多个不同的级别来处理系统的实际引导。有关 `init` 的介绍，请参见第 17.2 节“`init 进程`” [356]。

17.1.1 initramfs

`initramfs` 是一个小型 `cpio` 归档，在此内核可以装载到 RAM 磁盘。它提供了一个最小的 Linux 环境，可在装入实际根文件系统之前执行程序。这个最小的 Linux 环境由 BIOS 例程装载进内存，而且除了需要足够的内存外没有特别的硬件要求。`initramfs` 必须始终提供一个名为 `init` 的可执行文件，该文件应该执行根文件系统中实际的 `init` 程序以使引导进程继续进行。

在能够装入根文件系统并启动操作系统之前，内核需要相应的驱动程序来访问根文件系统所在的设备。这些驱动程序可能包括用于特定类型硬盘的特殊驱动程序，甚至还可能包括访问网络文件系统所需的网络驱动程序。可使用 `initramfs` 上的 `init` 装载根目录文件系统所需的模块。模块装载之后，`udev` 将为 `initramfs` 提供所需的设备。在引导过程的后面，更改根文件系统之后需要重新生成设备。通过 `boot.udev`（使用 `udevtrigger` 命令）来完成此操作。

如果需要在已安装的系统中更改硬件（例如硬盘），并且该硬件要求在引导时内核中有其他驱动程序，则必须更新 `initramfs` 文件。其操作方法和其前身 `initrd` 一样，即调用 `mkinitrd`。调用 `mkinitrd` 无需任何参数便可创建 `initramfs`。调用 `mkinitrd -R` 创建 `initrd`。在 SUSE Linux Enterprise® 中，要装载的模块由 `/etc/sysconfig/kernel` 中的变量 `INITRD_MODULES` 指定。安装后，自动将此变量设置为正确的值。将严格按照这些模块在 `INITRD_MODULES` 中出现的顺序来装载它们。只有您依赖正确的设备文件 `/dev/sd?` 设置时，这才显得重要。然而，在当前系统下，也可以使用 `/dev/disk/` 下的设备文件。这些文件以几个子目录的形式排序，分别为 `by-id`、

by-path 和 by-uuid，并始终代表相同的磁盘。也可以在安装时通过指定相应的装入选项完成此操作。

重要: 更新 `initramfs` 或 `initrd`

引导加载程序装载 `initramfs` 或 `initrd` 的方式与内核相同。在更新 `initramfs` 或 `initrd` 后无需重安装 GRUB，因为 GRUB 会在引导时搜索目录以获得正确的文件。

17.1.2 `initramfs` 中的 `init`

`initramfs` 中的 `init` 的主要用途是准备真实根文件系统的装入和访问。根据系统配置的不同，`init` 负责以下任务。

装载内核模块

根据硬件配置的不同，可能需要一些特殊的驱动程序来访问计算机的硬件部件（特别是硬盘）。要访问根文件系统，内核需要装载适当的文件系统驱动程序。

提供块特殊文件

内核对每个装载的模块生成设备事件。`udev` 处理这些事件，并在 RAM 文件系统上的 `/dev` 中生成必需的块特殊文件。没有这些特殊文件，文件系统和其他设备将不可访问。

管理 RAID 和 LVM 设置

如果将系统配置为在 RAID 或 LVM 下保存根文件系统，则 `init` 将设置 LVM 或 RAID 以支持稍后对根文件系统的访问。有关 RAID 的信息请参阅第 7.2 节“软 RAID 配置”[103]。有关 LVM 的信息，请参阅第 7.1 节“LVM 配置”[97]。可在 *Storage Administration Guide* 中查找有关 EVMS 和特殊存储设置的信息。

管理网络配置

如果对系统进行配置以使用通过网络装入的根文件系统（通过 NFS 装入），则 `init` 必须确保装载了适当的网络驱动器，并确保对其进行设置以允许对根文件系统的访问。

在初始引导期间调用 `init` 时（安装进程一部分），要执行的任务将与前面提到的任务不同：

查找安装媒体

启动安装进程时，计算机将通过安装媒体中的 YaST 安装程序装载一个安装内核和一个特殊的 `initrd`。YaST 安装程序在 RAM 文件系统中运行，它需要有关安装媒体位置的信息以访问安装媒体并安装操作系统。

启动硬件识别并装载适当的内核模块

如第 17.1.1 节“`initramfs`”[354]中所述，引导进程从可用于大多数硬件配置的一组最小的驱动程序启动。`init` 将启动初始硬件扫描进程，以确定适合您的硬件配置的一组驱动程序。引导进程所需的模块名写进 `/etc/sysconfig/kernel` 中的 `INITRD_MODULES`。这些名称用来生成引导该系统所需要的自定义 `initramfs`。如果模块不是用于引导，而是用于冷插入，则模块要写进 `/etc/sysconfig/hardware/hwconfig-*`。本目录下用配置文件描述的所有设备均要在引导过程中进行初始化。

装载安装系统或应急系统

一旦正确地识别出硬件并装载了适当的驱动程序并且 `udev` 创建了设备特殊文件后，`init` 就会启动安装系统，其中包含实际的 YaST 安装程序或应急系统。

启动 YaST

最后，`init` 将启动 YaST，由后者启动包安装和系统配置。

17.2 `init` 进程

`init` 程序是进程 ID 为 1 的进程，负责按所要求的方式对系统进行初始化。`init` 由内核直接启动，并且抵制信号 9（该信号通常会杀死进程）。所有其他程序由 `init` 直接启动，或由它的其中一个子进程启动。

`init` 在 `/etc/inittab` 文件中进行集中配置，其中运行级别已定义（请参阅第 17.2.1 节“运行级别”[357]）。该文件还指定了在每个级别有哪些服务和守护程序可用。根据 `/etc/inittab` 中的项，`init` 将运行若干个脚本。为了清楚起见，这些称作 *init* 脚本的脚本都位于目录 `/etc/init.d` 中（请参阅第 17.2.2 节“`Init` 脚本”[359]）。

启动和关闭系统的整个过程是由 `init` 维护的。从这一点来看，可以将内核视为一个后台进程，其任务是维护所有其他进程，以及根据其他程序的请求来调整 CPU 时间和硬件访问。

17.2.1 运行级别

在 Linux 中，运行级别定义了系统如何启动以及正在运行的系统中有哪些服务可用。在引导后，系统会按照 `/etc/inittab` 中的 `initdefault` 行所定义的方式启动。通常是 3 或 5。请参见表 17.1 “可用运行级别” [357]。也可以选择 在引导时指定运行级别（例如，在引导提示符后添加运行级别号）。任何不直接由内核本身求值的参数均将被传递给 `init`。要引导到 `runlevel 3`，只需向引导提示符添加一个数字 3。

表 17.1 可用运行级别

运行级别	说明
0	系统暂停
S 或 1	单用户方式
2	没有远程网络的本地多用户方式（NFS 等）
3	有网络的完全多用户方式
4	未使用
5	有网络和 X 显示管理器的完全多用户方式 — KDM、GDM 或 XDM
6	系统重引导

重要：避免运行级别 2 与通过 NFS 装入的分区

如果您的系统通过 NFS 装入了 `/usr` 分区，则不应使用运行级别 2。如果程序文件或库丢失，系统可能会异常运行，因为 NFS 设备不能以运行级别 2（没有远程网络的本地多用户方式）提供。

要在系统运行时更改运行级别，请输入 `telinit` 和作为参数的相应数字。仅允许系统管理员执行该操作。下表总结了运行级别区域中最重要的命令。

`telinit 1` 或 `shutdown now`
系统更改为单用户方式。该方式用于系统维护和管理任务。

```
telinit 3
```

启动了所有基本的程序和服务（包括网络），允许普通用户登录并在不具备图形环境的系统中工作。

```
telinit 5
```

启用了图形化环境。通常启动诸如 XDM、GDM 或 KDM 之类的显示管理器。如果启用 `autologin`，则本地用户便可登录到预先选择的窗口管理器（GNOME 或 KDE 或其他任何窗口管理器）中。

```
telinit 0 或 shutdown -h now
```

系统暂停。

```
telinit 6 或 shutdown -r now
```

系统暂停后重引导。

运行级别 5 是所有 SUSE Linux Enterprise 标准安装中的默认运行级别。提示用户使用图形界面登录，或者默认用户将自动登录。如果默认运行级别是 3，必须按照 [第 23 章 X 窗口系统](#) [437] 中的说明正确配置 X 窗口系统，才能将运行级别切换为 5。完成切换后，请通过输入 `telinit 5` 来检查系统是否以预期方式运行。如果一切合乎预期，就可以使用 YaST 将默认运行级别设置为 5。

警告: `/etc/inittab` 中的错误可能导致系统引导出现问题

如果 `/etc/inittab` 损坏，则可能无法正常引导系统。因此，在编辑 `/etc/inittab` 时要特别小心。在重引导计算机前，使 `init` 使用 `telinit q` 命令重读 `/etc/inittab`。

通常情况下，更改运行级别时会发生两件事情。首先是启动当前运行级别的停止脚本，同时关闭当前运行级别必需的一些程序。然后启动新运行级别的启动脚本。在大多数情况下，这时会启动多个程序。例如，将运行级别从 3 更改到 5 时会发生以下情况：

1. 通过输入 `telinit 5`，管理员 (`root`) 要求 `init` 更改为另一个运行级别。
2. `init` 检查当前运行级别 (`runlevel`) 并确定是否应使用新的运行级别作为参数来启动 `/etc/init.d/rc`。
3. `rc` 现在调用当前运行级别的停止脚本，但仅限新运行级别中没有启动脚本的那些停止脚本。在本例中，这些就是位于 `/etc/init.d/rc3.d`（旧

的运行级别是 3) 中以 `K` 开头的所有脚本。`K` 后跟的编号指定使用 `stop` 参数运行脚本的顺序，因为有很多依赖性要考虑。

- 4. 最后要启动的是新运行级别的启动脚本。在本例中，这些是位于 `/etc/init.d/rc5.d` 中以 `S` 开头的脚本。`S` 后跟的编号确定启动脚本的顺序。

当更改为与当前运行级别相同的运行级别时，`init` 仅检查 `/etc/inittab` 的更改，并启动相应的步骤（例如，在另一个界面上启动 `getty` 所需的步骤）。使用命令 `telinit q` 也达到到相同的作用。

17.2.2 Init 脚本

`/etc/init.d` 中有两种类型的脚本：

由 `init` 直接执行的脚本

仅在引导过程中或在启动系统立即关闭时（电源故障或用户按了 `Ctrl + Alt + Del` 组合键）时才会发生这种情况。这些脚本的执行是在 `/etc/inittab` 中定义的。

由 `init` 间接执行的脚本

这些脚本在更改运行级别时运行并始终调用主脚本 `/etc/init.d/rc`，后者能够确保相关脚本以正确顺序运行。

所有脚本位于 `/etc/init.d` 中。引导时运行的脚本是通过指向 `/etc/init.d/boot.d` 的符号链接调用的。用于更改运行级别的脚本也是通过符号链接从一个子目录（`/etc/init.d/rc0.d` 到 `/etc/init.d/rc6.d`）进行调用的。这仅仅是为了清楚起见，并避免在多个运行级别使用时出现重复脚本。因为每个脚本既可以作为启动脚本也可以作为停止脚本来执行，这些脚本必须理解 `start` 和 `stop` 参数。这些脚本还必须理解 `restart`、`reload`、`force-reload` 和 `status` 选项。对这些不同的选项进行了解释。[表 17.2 “可能的 `init` 脚本选项” \[359\]](#) 由 `init` 直接运行的脚本没有这些链接。需要时，可以从运行级别独立运行它们。

表 17.2 可能的 `init` 脚本选项

选项	说明
启动	启动服务。

选项	说明
停止	停止服务。
restart	如果服务正在运行，则首先将其停止，然后重新启动。 如果服务未在运行，则启动服务。
reload	在不停止和重新启动服务的情况下重装载配置。
force-reload	如果服务支持，则重装载配置。否则，要执行的步骤与指定 restart 时相同。
status	显示服务的当前状态。

每个特定于运行级别的子目录中的链接使将脚本与不同的运行级别相关联成为可能。在安装或卸载包时，在程序 `insserv`（或使用 `/usr/lib/lsb/install_initd`，它是调用此程序的一个脚本）的帮助下可添加和去除这些链接。有关详细信息，请参见手册页 `insserv(8)`。

所有这些设置也可能在 YaST 模块的帮助下发生变化。如果需要检查命令行的状态，请使用 `chkconfig(8)` 手册页中所描述的 `chkconfig` 工具。

下面分别简要介绍最先或最后启动的引导和停止脚本，并对脚本的维护进行了说明。

引导

在使用 `init` 直接启动系统时执行。它与选择的运行级别无关，而且仅执行一次。这时将装入 `/proc` 和 `/dev/pts` 文件系统，并激活 `blogd`（引导日志记录守护程序）。如果在更新或安装后首次引导系统，则会启动初始系统配置。

`blogd` 守护程序是由 `boot` 和 `rc` 启动的第一个服务。在由这些脚本触发的操作（运行几个子脚本，例如使块特殊文件变为可用的）完成之后它停止。`blogd` 将所有屏幕输出写入日志文件 `/var/log/boot.msg`（前提是装入的 `/var` 是可读写的）。否则，`blogd` 将缓冲所有屏幕数据，直到 `/var` 可用。有关 `blogd` 的详细信息，请参见手册页 `blogd(8)`。

脚本 `boot` 还负责启动 `/etc/init.d/boot.d` 中名称以 `s` 开头的所有脚本。在这里，将检查文件系统并根据需要配置回路设备。同时设置系统时

间。如果在自动检查和修复文件系统时出错，系统管理员可以在输入根密码后进行干预。最后执行的是脚本 `boot.local`。

`boot.local`

在这里，输入引导时在更改为某个运行级别之前执行的其他命令。这类似于 DOS 系统上的 `AUTOEXEC.BAT`。

`boot.setup`

在从单用户方式更改为任何其他运行级别时均执行该脚本，它负责许多基本设置，如键盘布局和虚拟控制台的初始化。

`halt`

仅当更改为运行级别 0 或 6 时执行该脚本。它在这里作为 `halt` 或 `reboot` 来执行。是关闭系统还是重引导系统取决于调用 `halt` 的方式。

`rc`

此脚本调用当前运行级别的相应停止脚本和新选择的运行级别的启动脚本。

您可以创建自己的脚本并方便地将它们集成到上面描述的方案中。有关格式化、命名和组织自定义脚本的说明，请参考 **LSB** 的规范以及 `init`、`init.d`、`chkconfig` 和 `insserv` 的手册页。此外还可以参见 `startproc` 和 `killproc` 的手册页。

警告: 有问题的 `init` 脚本可能会使您的系统暂停

有问题的 `init` 脚本可能会使您的计算机挂起。应认真编辑这些脚本，如果可能，应在多用户环境中对它们进行严格测试。中有一些有关 `init` 脚本的有用信息。[第 17.2.1 节“运行级别” \[357\]](#)。

要为给定程序或服务创建自定义 `init` 脚本，请使用文件 `/etc/init.d/skeleton` 作为模板。以新名称保存此文件的备份，然后根据需要编辑相关程序和文件名、路径及其他详细信息。您可能还需要用自己的部分来增强此脚本，以便 `init` 过程可以触发正确的操作。

位于顶部的 `INIT INFO` 块是脚本的一个必需部分，应进行编辑。请参见[例 17.1“最小的 `INIT INFO` 块” \[362\]](#)。

例 17.1 最小的 INIT INFO 块

```
### BEGIN INIT INFO
# Provides:          FOO
# Required-Start:    $syslog $remote_fs
# Required-Stop:     $syslog $remote_fs
# Default-Start:     3 5
# Default-Stop:      0 1 2 6
# Description:       Start FOO to allow XY and provide YZ
### END INIT INFO
```

在 INFO 块第一行上 Provides: 后, 指定由此 init 脚本控制的程序或服务的名称。在 Required-Start: 和 Required-Stop: 行中, 指定在启动或停止服务本身之前, 需要启动或停止的所有服务。这些信息稍后用于生成脚本名的编号 (可以在运行级别目录中找到)。在 Default-Start: 和 Default-Stop: 后, 指定应自动启动或停止的服务所在的运行级别。最后, 在 Description: 下, 提供对相关服务的简短说明。

要创建从运行级别目录 (/etc/init.d/rc?.d/) 到 /etc/init.d/ 中相应脚本的链接, 请输入命令 `insserv new-script-name`。insserv 程序对 INIT INFO 标题进行求值, 以便为运行级别目录 (/etc/init.d/rc?.d/) 中的启动和停止脚本创建必要的链接。此程序还负责保证每个运行级别的启动和停止顺序正确无误, 方法是在这些链接的名称中包含必要的数字。如果要使用图形工具来创建这样的链接, 请按照 [第 17.2.3 节“使用 YaST 配置系统服务 \(运行级别\)”](#) [362] 中说明的方法使用 YaST 提供的运行级别编辑器。

如果应将已存在于 /etc/init.d/ 中的脚本集成到现有运行级别方案中, 请立即通过 insserv 或启用 YaST 的运行级别编辑器中的相应服务在运行级别目录中创建链接。您的更改将在下次重引导时生效 — 新服务将自动启动。

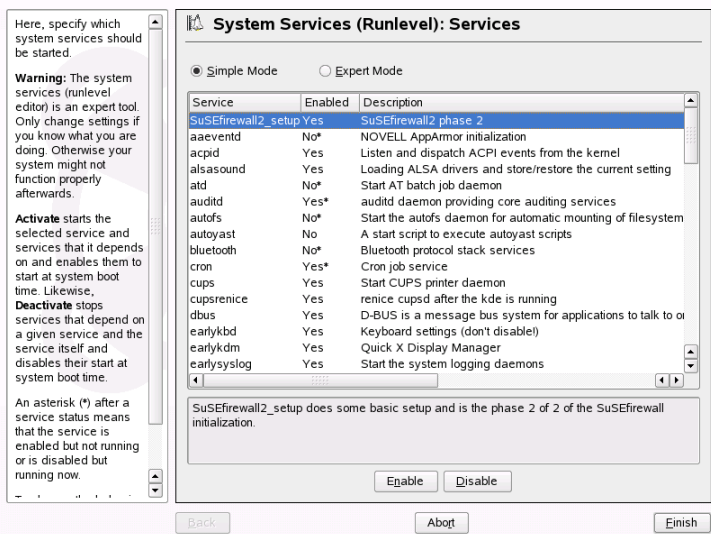
不要手动设置这些链接。如果 INFO 块中出错, 则在稍后为其他服务运行 insserv 时将会出现问题。下次为此脚本运行 insserv 时将去除手动添加的服务。

17.2.3 使用 YaST 配置系统服务 (运行级别)

使用 `YaST > 系统 > 系统服务 (运行级别)` 启动此 YaST 模块后, 它将显示一个概要, 列出所有可用的服务和每个服务的当前状态 (禁用或启用)。确定是以简单方式还是以专家方式使用此模块。默认的简单方式足以完成大多数操作。左边的列显示服务的名称, 中间的列指示其当前状态, 而右边的列则给出简短

说明。窗口下部提供了对所选服务的更为详细的说明。若要启用某个服务，请首先在表中选定它，然后选择启用。同样的步骤可用于禁用服务。

图 17.1 系统服务（运行级别）



要对所启动或停止的服务所在运行级别进行更具体的控制，或者更改默认运行级别，请先选择专家方式。将在顶部显示当前默认的运行级别或“initdefault”（默认情况下将系统引导至的运行级别）。通常情况下，SUSE Linux Enterprise 系统的默认运行级别是运行级别 5（有网络和 X 的完全多用户方式）。运行级别 3（有网络的完全多用户方式）是合适的替代选择。

此 YaST 对话框用于选择一个运行级别（如 表 17.1 “可用运行级别” [357] 中所列）作为新的默认运行级别。此外，可使用此窗口中的表来启用或禁用各个服务和守护程序。此表列出可用的服务和守护程序，显示它们当前是否已在您的系统上启用，如果已启用，则指示它们用于哪些运行级别。用鼠标选择其中的一行后，请单击表示运行级别（B、0、1、2、3、5、6 和 S）的复选框来确定所选服务或守护程序的运行级别。未对运行级别 4 进行定义，目的是供用户创建自定义运行级别。表概要下方提供了当前所选服务或守护程序的简要说明。

用启动、停止或刷新来确定是否应激活某服务。刷新状态用来检查当前状态。设置或重设置用于选择是将更改应用到系统，还是恢复启动运行级别编辑器之前存在的设置。选择完成即可将已更改的设置保存到磁盘。

警告: 有问题的运行级别设置可能会对您的系统造成损害

有问题的运行级别设置可能会导致系统无法使用。在应用您的更改之前，请确保您清楚这些设置可能产生的结果。

17.3 通过 `/etc/sysconfig` 配置系统

SUSE Linux Enterprise 的主配置是由 `/etc/sysconfig` 中的配置文件控制的。只有与 `/etc/sysconfig` 中的各个文件相关的脚本才会读取它们。这样有很多好处，例如确保了网络设置只需要由与网络相关的脚本来分析。

可以使用两种方法编辑系统配置。使用 YaST `sysconfig` 编辑器或手动编辑配置文件。

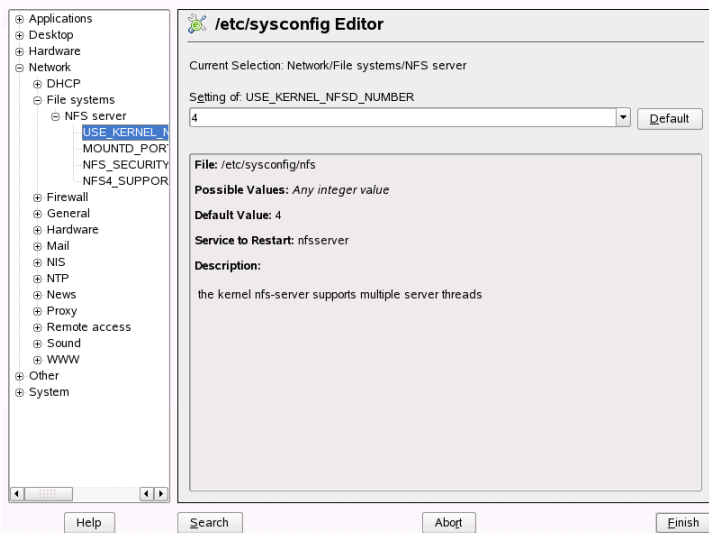
17.3.1 使用 YaST Sysconfig 编辑器更改系统配置

YaST `sysconfig` 编辑器为系统配置提供了一种使用方便的前端。无需了解需要更改的配置变量的实际位置，只需使用该模块的内置搜索功能，就可以根据需要更改配置变量的值，并使 YaST 负责应用这些更改以及根据 `sysconfig` 中设置的值更新配置和重启动服务。

警告: 修改 `/etc/sysconfig/*` 文件可能会对您的安装造成损害

如果没有足够的经验和知识，切勿修改 `/etc/sysconfig` 文件。否则可能会对您的系统造成巨大损害。`/etc/sysconfig` 中的文件包含对每个变量的简短注释，解释了这些变量的实际作用。

图 17.2 使用 sysconfig 编辑器进行系统配置



YaST sysconfig 对话框分为三个部分。对话框左边的部分显示了一个树视图，其中列出了所有可配置变量。当您选择某个变量时，右边的部分会显示当前选择和此变量的当前设置。在下部的第三个窗口中，简要说明了变量的用途、可能的值、默认值以及作为此变量来源的实际配置文件。此对话框还提供了有关更改变量后将执行哪些配置脚本，以及作为更改的结果将启动哪些新服务等信息。YaST 将提示您确认更改，并通知您在选择完成退出对话框后将执行哪些脚本。在这里还可以选择需要现在跳过而在以后启动的服务和脚本。YaST 将自动应用所有的更改并重启动涉及的所有服务以使更改生效。

17.3.2 手动更改系统配置

要手动更改系统配置，请执行如下操作

- 1 成为 root 用户。
- 2 使用 `init 1` 将系统转入单用户方式（运行级别 1）。
- 3 使用您选择的编辑器根据需要对配置文件进行更改。

如果不使用 YaST 来更改 `/etc/sysconfig` 中的配置文件，则要确保将空变量值用两个引号表示 (`KEYTABLE=""`)，并将含有空白的值用引号括起来。只包括一个单词的值不需要用引号括起来。

- 4 执行 `SUSEconfig` 来确保更改生效。
- 5 使用类似 `init default_runlevel` 的命令将系统返回到先前的运行级别。使用系统的默认运行级别替代 `default_runlevel`。如果想返回有网络和 X 的完全多用户方式，请选择 5；如果希望在有网络的完全多用户方式下工作，请选择 3。

这一过程主要用于更改整个系统范围的配置，例如网络配置。若要进行较小的更改，不一定要切换到单用户方式，但这样做可以完全确保正确重新启动所有相关的程序。

提示: 配置自动系统配置

要禁用 `SUSEconfig` 设定的自动系统配置，请将 `/etc/sysconfig/suseconfig` 中的变量 `ENABLE_SUSECONFIG` 设置为 `no`。如果要使用 `SUSE` 安装支持，请不要禁用 `SUSEconfig`。也可以部分禁用自动配置。

引导加载程序

本章介绍如何配置 GRUB（在 SUSE Linux Enterprise® 中使用的引导加载程序）。一个特殊的 YaST 模块可用于执行所有设置。如果您不熟悉在 Linux 中进行引导的相关内容，请阅读下面几节获得一些背景信息。本章还介绍了使用 GRUB 进行引导时经常遇到的一些问题和它们的解决方案。

本章主要介绍引导加载程序 GRUB 的引导管理和配置。中将引导过程作为一个整体进行了介绍。[第 17 章 引导和配置 Linux 系统](#) [353] 引导加载程序代表计算机 (BIOS) 和操作系统 (SUSE Linux Enterprise) 之间的接口。引导加载程序的配置直接影响到操作系统的启动。

本章经常出现以下术语，可能需要进行解释：

主引导记录

MBR 的结构是由独立于操作系统的约定定义的。前 446 个字节为程序代码保留。它们通常保存部分引导加载程序或操作系统选择器。随后的 64 个字节为最多包含 4 项的分区表提供空间（请参阅[“分区类型”一节](#) [133]）。分区表包含有关硬盘分区和文件系统类型的信息。操作系统需要使用此表来处理硬盘。如果 MBR 中有传统通用代码，则只应将一个分区标记为活动。MBR 的最后两个字节包含静态“幻数” (AA55)。一些 BIOS 会将包含不同值的 MBR 视为无效，因此引导时不会考虑此 MBR。

引导扇区

引导扇区是硬盘分区（除扩展分区之外）上的前几个扇区，扩展分区只充当其他分区的“树枝”。引导扇区具有 512 字节的空间，引导扇区储存用于引导安装在各个分区上的操作系统的代码。这适用于经过格式化的 DOS、Windows 和 OS/2 分区的引导扇区，这些扇区还包含文件系统的一些重要的基本数据。相比之下，Linux 分区的引导扇区在设置文件系统（而不是 XFS）

之后最初是空的。因此，即使 Linux 分区包含内核和有效的根文件系统，它也不能通过自身进行引导。储存了引导系统的有效代码的引导扇区具有与 MBR 中的最后两个字节 (AA55) 相同的幻数。

18.1 选择引导加载程序

默认情况下，引导加载程序 GRUB 用于 SUSE Linux Enterprise 中。但是，在某些情况下以及对于特殊的硬件和软件，使用 LILO 可能是必需的。如果您更新较早的 SUSE Linux Enterprise 版本（该版本使用 LILO），则将安装 LILO。

有关安装和配置 LILO 的信息可以在支持数据库中的关键字“LILO”和文件 `/usr/share/doc/packages/lilo` 下获得。

18.2 通过 GRUB 引导

GRUB (Grand Unified Bootloader) 由两段组成。stage1 包含 512 个字节，它的唯一任务就是装载引导加载程序的第二段。随后，装载 stage2。这一段包含引导加载程序的主要部分。

在一些配置中，可以使用中间段 1.5，它从适当的文件系统中找到并装载第二段。如果可能，将在安装时或使用 YaST 初始设置 GRUB 时默认选择此方法。

stage2 可以访问许多文件系统。当前，支持 Ext2、Ext3、ReiserFS、Minix，以及 Windows 使用的 DOS FAT 文件系统。在某种程度上还支持 BSD 系统使用的、XFS、UFS 和 FFS。从版本 0.95 开始，GRUB 还能够从包含 ISO 9660 标准文件系统、符合“El Torito”规范的 CD 或 DVD 进行引导。即使是在引导系统之前，GRUB 也可以访问支持的 BIOS 磁盘设备（BIOS 检测到的软盘或硬盘、CD 驱动器和 DVD 驱动器）的文件系统。因此，对 GRUB 配置文件 (`menu.lst`) 进行更改不要求重安装引导管理器。当引导系统时，GRUB 重装载菜单文件以及内核或初始 ram 磁盘 (`initrd`) 的有效路径和分区数据，并对这些文件进行定位。

GRUB 的实际配置是基于三个文件进行的，下面对这三个文件进行介绍：

/boot/grub/menu.lst

此文件包含有关可通过 GRUB 进行引导的分区或操作系统的所有信息。没有这些信息，GRUB 命令行将提示用户如何继续（请参阅“[在引导过程中编辑菜单项](#)”一节 [373] 获取详细信息）。

/boot/grub/device.map

此文件将 GRUB 和 BIOS 符号中的设备名转换为 Linux 设备名。

/etc/grub.conf

此文件包含 GRUB shell 正确安装引导加载程序所需的命令、参数和选项。

可以通过多种方式控制 GRUB。可以在图形菜单（启动屏幕）中选择现有配置的引导项。配置是从文件 menu.lst 装载的。

在 GRUB 中，在引导前可以更改所有引导参数。例如，可以通过这种方式更正编辑菜单文件时出现的错误。还可以在输入提示符处以交互的方式输入引导命令（请参阅“[在引导过程中编辑菜单项](#)”一节 [373]）。GRUB 能够在引导前确定内核和 initrd 的位置。通过这种方式，您甚至可以引导在引导加载程序配置中不存在任何项的已安装操作系统。

GRUB 实际上以两个版本存在：作为引导加载程序以及作为 /usr/sbin/grub 中的普通 Linux 程序。此程序被称为 *GRUB shell*。它在已安装系统中提供 GRUB 的仿真，并且可用来安装 GRUB 或在应用新设置之前对其进行测试。将 GRUB 作为引导加载程序安装在硬盘或软盘上的功能以 install 和 setup 命令的形式集成在 GRUB 中。当装载了 Linux 后在 GRUB shell 中可用。

18.2.1 GRUB 引导菜单

带有引导菜单的图形启动屏幕基于 GRUB 配置文件 /boot/grub/menu.lst，该文件包含有关可以通过菜单引导的所有分区或操作系统的所有信息。

每次引导系统时，GRUB 都从文件系统装载菜单文件。出于此原因，不必每次更改文件后都重安装 GRUB。使用 YaST 引导加载程序修改 GRUB 配置，如第 18.3 节“[使用 YaST 配置引导加载程序](#)”[376] 中所述。

菜单文件中包含命令。语法非常简单。每行都包含一条命令，后跟可选参数，可选参数之间用空格隔开，就像在 shell 中一样。出于历史原因，某些命令允许在第一个参数前使用 =。注释以井号 (#) 开头。

若要在菜单概述中标识菜单项，请为每项设置一个 `title`。关键字 `title` 后的文本（包括任何空格）显示为菜单中的可选择选项。当选择此菜单项时，将执行下一个 `title` 前的所有命令。

最简单的情况是重定向到其他操作系统的引导加载程序。命令是 `chainloader`，参数通常是 GRUB 中另一个分区的引导块 `block notation`。例如：

```
chainloader (hd0,3)+1
```

GRUB 中的设备名在“[硬盘和分区的命名约定](#)”一节 [370] 中有所解释。此示例指定第一个硬盘第四个分区中的第一个块。

使用命令 `kernel` 指定内核映像。第一个参数是指向分区中内核映像的路径。命令行上的其他参数将被传递到内核。

如果内核不具有访问根分区的内置驱动程序，或者使用了具有高级热插拔功能的最新 `linux` 系统，则必须用单独的 GRUB 命令指定 `initrd`，该命令的唯一参数便是指向 `initrd` 文件的路径。因为 `initrd` 的装载地址会被写入装载的内核映像中，所以 `initrd` 命令必须紧接在 `kernel` 命令之后。

命令 `root` 简化了内核和 `initrd` 文件的指定。`root` 的唯一参数是一个设备或分区。此设备用于所有内核、`initrd` 或下一个 `root` 命令前未显式指定设备的其他文件路径。

每个菜单项的末尾都间接指定 `boot` 命令，因此无需将其写入菜单文件中。但是，如果以交互方式使用 GRUB 进行引导，则必须在最后输入 `boot` 命令。该命令本身没有参数。它只引导装载的内核映像或指定的链装载程序。

在写入所有菜单项之后，将其中一项定义为 `default` 项。否则，将使用第一项（项 0）。您还可以指定在一段时间后引导默认项的超时值（以秒为单位）。`timeout` 和 `default` 通常在各菜单项前面。示例文件在“[示例菜单文件](#)”一节 [371] 中有所介绍。

硬盘和分区的命名约定

GRUB 用于硬盘和分区的命名约定不同于普通 `Linux` 设备使用的命名约定。它更类似于 BIOS 执行的简单磁盘枚举，而语法类似于一些 `BSD` 衍生程序中使用的语法。在 GRUB 中，分区的编号从 0 开始。它表示 `(hd0, 0)` 是第一块硬盘的第一个分区。在普通台式机上，作为 `Primary Master`（第一个 IDE 控制器上的主设备）连接的硬盘所对应的 `Linux` 设备名为 `/dev/hda1`。

4 个可能的主分区所分配的分区号为 }0 到 3。逻辑分区的编号从 4 开始：

```
(hd0,0)    first primary partition of the first hard disk
(hd0,1)    second primary partition
(hd0,2)    third primary partition
(hd0,3)    fourth primary partition (usually an extended partition)
(hd0,4)    first logical partition
(hd0,5)    second logical partition
```

GRUB 依赖于 BIOS 设备，它不区分 IDE、SATA、SCSI 和硬件 RAID 设备。BIOS 或其他控制器识别的所有硬盘将按照 BIOS 中显示的引导顺序进行编号。

不过，通常不能将 Linux 设备名准确映射为 BIOS 设备名。它借助某种算法生成这一映射并将其保存到文件 `device.map` 中，可以根据需要对该文件进行编辑。有关文件 `device.map` 的信息在 [第 18.2.2 节“文件 `device.map`”](#) [374] 中有所介绍。

完整的 GRUB 路径包含写在括号中的设备名和指向指定分区的文件系统中文件的路径。路径以斜线开头。例如，在具有一个 IDE 硬盘（该硬盘的第一个分区中包含 Linux）的系统上，可以按如下方式指定可引导内核：

```
(hd0,0)/boot/vmlinuz
```

示例菜单文件

以下示例说明了 GRUB 菜单文件的结构。该示例安装包括 `/dev/hda5` 下的 Linux 引导分区、`/dev/hda7` 下的引导分区和 `/dev/hda1` 下的 Windows 安装。

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8

title linux
    kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
    initrd (hd0,4)/initrd

title windows
    chainloader (hd0,0)+1

title floppy
    chainloader (fd0)+1
```

```
title failsafe
    kernel (hd0,4)/vmlinuz.shipped root=/dev/hda7 ide=nodma \
    apm=off acpi=off vga=normal nosmp maxcpus=0 3
    initrd (hd0,4)/initrd.shipped
```

第一块定义了启动屏幕的配置：

gfxmenu (hd0,4)/message

背景图像 message 位于 /dev/hda5 分区的顶级目录中。

color white/blue black/light-gray

色彩模式：白色（前景色）、蓝色（背景色）、黑色（所选内容）、浅灰色（所选内容的背景）。颜色方案对启动屏幕没有任何影响，它只影响通过按 **Esc** 键退出启动屏幕后所访问的可自定义的 **GRUB** 菜单。

default 0

第一个菜单项 `title linux` 是默认情况下引导的对象。

timeout 8

如果 8 秒钟后无任何用户输入，**GRUB** 将自动引导默认项。要检测自动引导，请删除 `timeout` 行。如果设置 `timeout 0`，**GRUB** 将立即引导默认项。

第二块（也就是最大的块）列出了各个可引导的操作系统。各个操作系统的不同部分由 `title` 引出。

- 第一项 (`title linux`) 负责引导 **SUSE Linux Enterprise**。内核 (`vmlinuz`) 位于第一块硬盘的第一个逻辑分区（引导分区）。内核参数（例如引导分区和 **VGA** 方式）也被追加在此处。引导分区是根据 **Linux** 命名约定 (`/dev/hda7/`) 指定的，这是因为此信息将被内核读取而与 **GRUB** 无关。`initrd` 也位于第一块硬盘的第一个逻辑分区中。
- 第二项负责装载 **Windows**。**Windows** 将从第一块硬盘的第一个分区 (`hd0,0`) 引导。命令 `chainloader +1` 将导致 **GRUB** 读取并执行指定分区的第一个扇区。
- 下一项支持从软盘进行引导，而无需修改 **BIOS** 设置。
- 引导选项 `failsafe` 用一组内核参数启动 **Linux**，这些参数使 **Linux** 甚至可以在有问题的系统上引导。

随时可以根据需要更改菜单文件。GRUB 会在下次引导时使用修改后的设置。使用 YaST 或所选的编辑器对文件进行永久编辑。或者，使用 GRUB 的编辑功能可以按交互方式进行临时更改（请参阅[“在引导过程中编辑菜单项”一节 \[373\]](#)）。

在引导过程中编辑菜单项

在图形引导菜单中，使用箭头键选择要引导的操作系统。如果选择 Linux 系统，则可以在引导提示符处输入其他引导参数。若要直接编辑个别菜单项，请按 **Esc** 键退出启动屏幕并进入 GRUB 基于文本的菜单，然后按 **E** 键。通过这种方式进行的更改仅适用于当前引导，不会被永久采用。

重要：引导过程中的键盘布局

US 键盘布局是引导时唯一可用的键盘布局。请参见[图 46.1 “美式键盘布局” \[729\]](#)的图。

编辑菜单条目简化了无法再进行引导的有问题系统的修复工作，因为可以通过手动输入参数规避引导加载程序中有点问题的配置文件。在引导过程中手动输入参数还可用于测试新设置而避免损坏本机系统。

在激活编辑方式后，可以使用箭头键选择要编辑其配置的菜单项。若要使配置可以编辑，请再次按 **E** 键。通过这种方式，可以编辑不正确的分区或路径指定，从而防止它们对引导进程产生负面影响。按 **Enter** 键退出编辑方式并返回菜单。随后按 **B** 键引导此项。可以进行的进一步操作显示在底部的帮助文本中。

若要永久输入更改的引导选项并将它们传递到内核，则以 `root` 用户身份打开文件 `menu.lst` 并将相应的内核参数追加到现有的行上，用空格分隔：

```
title linux
    kernel (hd0,0)/vmlinuz root=/dev/hda3 additional parameter
    initrd (hd0,0)/initrd
```

GRUB 会在下次引导系统时自动采用新参数。或者，还可以通过 YaST 引导加载程序模块进行此更改。将新参数追加到现有的行上，用空格分隔。

18.2.2 文件 device.map

文件 `device.map` 将 GRUB 和 BIOS 设备名映射为 Linux 设备名。在包含 IDE 和 SCSI 硬盘的混合系统中，GRUB 必须通过特殊过程尝试确定引导顺序，因为 GRUB 不能访问 BIOS 上有关引导顺序的信息。GRUB 会将此分析的结果保存在文件 `/boot/grub/device.map` 中。对于 BIOS 中引导顺序设置为 IDE 在 SCSI 之前的系统，文件 `device.map` 如下所示：

```
(fd0)  /dev/fd0
(hd0)  /dev/hda
(hd1)  /dev/sda
```

因为 IDE、SCSI 和其他硬盘的顺序取决于不同的因素，并且 Linux 无法标识映射，所以可以在 `device.map` 文件中手动设置顺序。如果在引导时遇到问题，则检查此文件中的顺序是否对应于 BIOS 中的顺序，如果需要，使用 GRUB 提示符 对其进行临时修改。引导了 Linux 系统之后，便可以使用 YaST 引导加载程序模块或所选的编辑器对文件 `device.map` 进行永久编辑。

重要: SATA 磁盘

根据控制器，将 SATA 磁盘识别为 IDE (`/dev/hdx`) 或 SCSI (`/dev/sdx`) 设备。

在手动更改 `device.map` 之后，请执行以下命令重安装 GRUB。此命令导致重装文件 `device.map` 并且执行 `grub.conf` 中列出的命令：

```
grub --batch < /etc/grub.conf
```

18.2.3 文件 /etc/grub.conf

除了 menu.lst 和 device.map 之外，第三个重要的 GRUB 配置文件就是 /etc/grub.conf。此文件包含 GRUB shell 正确安装引导加载程序所需的命令、参数和选项：

```
root (hd0,4)
    install /grub/stage1 (hd0,3) /grub/stage2 0x8000 (hd0,4)/grub/menu.lst
quit
```

各个项的含义：

root (hd0,4)

此命令指示 GRUB 将以下命令应用到第一块硬盘的第一个逻辑分区（引导文件的位置）。

install parameter

应使用参数 install 来运行命令 grub。应将引导加载程序的 stage1 安装在扩展分区树枝（/grub/stage1 (hd0,3)）中。此配置较为深奥，但是在许多情况下适用。应将 stage2 装载到内存地址 0x8000（/grub/stage2 0x8000）中。最后一项((hd0,4)/grub/menu.lst) 指示 GRUB 查找菜单文件的位置。

18.2.4 设置引导密码

即使是在引导操作系统之前，GRUB 也支持对文件系统的访问。没有根权限的用户可以访问 Linux 系统中的文件，而一旦引导系统后，他们将无权访问这些文件。若要阻止这种访问或防止用户引导某些操作系统，可以设置引导密码。

重要：引导密码和启动屏幕

如果对 GRUB 使用引导密码，则不显示通常的启动屏幕。

以 root 用户身份按如下步骤设置引导密码：

- 1 在根提示符处，使用 grub-md5-crypt 加密密码：

```
# grub-md5-crypt
Password: ****
Retype password: ****
Encrypted: $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

- 2 将经过加密的字符串粘贴到 menu.lst 文件的全局部分：

```
gfxmenu (hd0,4)/message
color white/blue black/light-gray
default 0
timeout 8
password --md5 $1$lS2dv/$JOYcdxIn7CJk9xShzzJVw/
```

现在，只有在按 **P** 键并输入密码后，才可以在引导提示符处执行 **GRUB** 命令。但是，用户仍可以从引导菜单引导所有操作系统。

- 3 要防止从引导菜单引导一个或多个操作系统，请将项 lock 添加到 menu.lst 中不输入密码就不能引导的每个部分。例如：

```
title linux
    kernel (hd0,4)/vmlinuz root=/dev/hda7 vga=791
    initrd (hd0,4)/initrd
    lock
```

在重引导系统并从引导菜单中选择 **Linux** 项后，将显示以下错误讯息：

```
Error 32: Must be authenticated
```

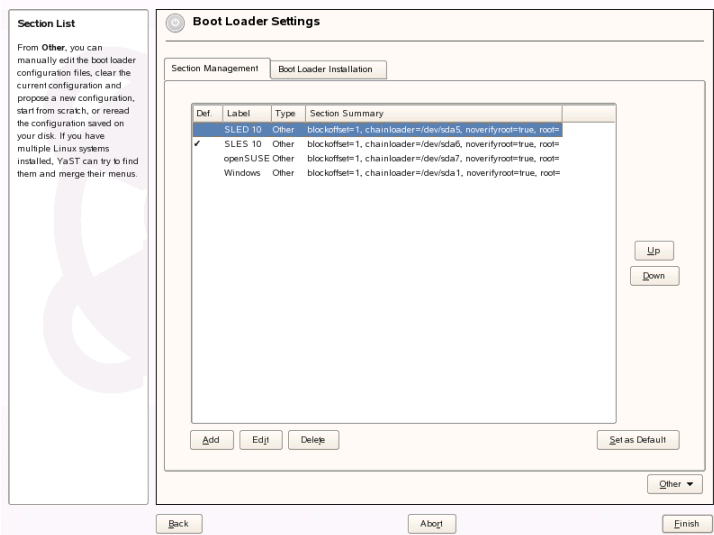
按 **Enter** 键进入该菜单。然后按 **P** 键，系统将提示您输入密码。在输入密码并按 **Enter** 键之后，将引导所选的操作系统（在本例中为 **Linux**）。

18.3 使用 YaST 配置引导加载程序

在您的 SUSE Linux Enterprise 系统中配置引导加载程序最简单的方式就是使用 YaST 模块。在 YaST 控制中心，选择系统 > 引导加载程序。如图 18.1 “Boot

Loader 设置”[377]中所示，它将显示您系统的当前引导加载程序配置，并允许您进行更改。

图 18.1 Boot Loader 设置



使用扇区管理选项卡可编辑、更改和删除单个操作系统的引导加载程序扇区。若要添加某个选项，请单击添加。要更改现有选项的值，请用鼠标选中它，然后单击编辑。要去除现有的条目，请选择它，单击删除。如果对引导加载程序选项不熟悉，请先阅读第 18.2 节“通过 GRUB 引导”[368]。

使用引导加载程序安装选项卡查看并更改类型、位置和高级装载程序设置的相关设置。

从单击其他后打开的下拉菜单中访问高级配置选项。内置编辑器让您可以更改 GRUB 配置文件（细节请参见第 18.2 节“通过 GRUB 引导”[368]）。也可以删除现有配置并从头开始或让 YaST 建议新配置。也可以向磁盘写入配置或从磁盘重新读取配置。要恢复在安装期间保存的原始主引导记录，请选择恢复硬盘的主引导记录。

18.3.1 引导加载程序类型

在引导加载程序安装中设置引导加载程序类型。SUSE Linux Enterprise 中默认的引导加载程序是 GRUB。如要使用 LILO，请执行如下操作：

过程 18.1 更改引导加载程序类型

- 1 选择引导加载程序安装选项卡。
- 2 对于引导加载程序，请选择 *LILO*。
- 3 在打开的对话框中，选择以下某个操作：

建议新配置

让 YaST 推荐一个新的配置。

转换当前配置

让 YaST 转换当前的配置。在转换配置时，有些设置可能会丢失。

从头开始新的配置

编写自定义配置。此操作在安装 SUSE Linux Enterprise 期间时不可用。

读取保存在磁盘上的配置

装载自己的 `/etc/lilo.conf`。此操作在安装 SUSE Linux Enterprise 期间不可用。

- 4 单击确定保存更改
- 5 在主对话框中单击完成以应用更改。

转换时，旧的 GRUB 配置将保存到磁盘上。如要使用它，只需将引导加载程序类型改回 GRUB，然后选择恢复转换前保存的配置。此操作仅在已安装的系统上可用。

注意: 自定义引导加载程序

如果想要使用 GRUB 或 LILO 以外的引导加载程序，请选择不安装任何引导加载程序。在选择该选项之前，请仔细阅读您的引导加载程序文档。

18.3.2 引导加载程序位置

要更改引导加载程序的位置，请遵循以下步骤：

过程 18.2 更改引导加载程序位置

- 1 选择引导加载程序安装选项卡，然后为引导加载程序位置选择以下某个选项：

从引导分区引导

/boot分区的引导扇区。

从扩展分区引导

这将在扩展分区容器中安装引导加载程序。

从主引导记录引导

本操作会在第一个磁盘的MBR中安装引导加载程序（根据BIOS中预设的引导顺序）。

从引导分区引导

这将在 // 分区的引导扇区安装引导加载程序。

自定义引导分区

手动使用此选项来指定引导加载程序的位置。

- 2 单击结束来应用更改。

18.3.3 默认系统

要更改默认引导的系统，请按如下所示继续：

过程 18.3 设置默认系统

- 1 打开扇区管理选项卡。
- 2 从列表中选择所需的条目。
- 3 单击设为默认。

- 4 单击完成以激活这些更改。

18.3.4 引导加载程序超时

引导加载程序不会立即引导默认系统。超时期间，可以选择要引导的系统或编写一些内核参数。要设置引导加载程序超时值，请执行如下操作：

过程 18.4 更改引导加载程序超时值

- 1 打开引导加载程序安装选项卡。
- 2 单击引导加载程序选项。
- 3 用鼠标单击相应的方向键或者使用键盘上的方向键来更改超时秒数中的值，或者输入新的值。
- 4 单击确定。
- 5 单击完成以保存更改。

18.3.5 安全性设置

使用此 YaST 模块，还可以设置密码来保护引导。这提供了更高的安全性级别。

过程 18.5 设置引导加载程序密码

- 1 打开引导加载程序安装选项卡。
- 2 单击引导加载程序选项。
- 3 在菜单界面密码中设置密码。
- 4 单击确定。
- 5 单击完成以保存更改。

18.4 卸载 Linux 引导加载程序

YaST 可用于卸载 Linux 引导加载程序并将 MBR 恢复为安装 Linux 之前的状态。在安装过程中，YaST 自动创建原始 MBR 的备份副本并根据请求进行恢复。

要卸载 GRUB，请启动 YaST 引导加载程序模块（系统 > 引导加载程序）。选择其他 > 恢复硬盘的主引导记录然后选择是，重写加以确认。

18.5 创建引导 CD

如果使用引导管理器引导系统时出现问题或如果不能将引导管理器安装在硬盘的 MBR 或软盘上，那么还可以创建包含所有必需的 Linux 启动文件的可引导 CD。这需要您的系统中安装有 CD 刻录机。

用 GRUB 创建可引导 CD-ROM 只需要特殊形式的 *stage2*（名为 *stage2_eltorito*）以及自定义的 *menu.lst*（可选）。不需要标准文件 *stage1* 和 *stage2*。

过程 18.6 创建引导 CD

1 将目录更改为要创建 ISO 映像的目录，例如：`cd /tmp`

2 创建 GRUB 的子目录：

```
mkdir -p iso/boot/grub
```

3 将内核、文件 *stage2_eltorito*、*initrd*、*menu.lst* 和 *message* 复制到 *iso/boot/*：

```
cp /boot/vmlinuz iso/boot/  
cp /boot/initrd iso/boot/  
cp /boot/message iso/boot/  
cp /usr/lib/grub/stage2_eltorito iso/boot/grub  
cp /boot/grub/menu.lst iso/boot/grub
```

4 调整 *iso/boot/grub/menu.lst* 中的路径条目使其指向 CD-ROM 设备。执行此操作的方法是将路径名中硬盘的设备名（以 *(sd*)* 格式列出）替换为 CD-ROM 驱动器的设备名（即 *(cd)*）：

```
timeout 8  
default 0
```

```
gfxmenu (cd)/boot/message

title Linux
    root (cd)
    kernel /boot/vmlinuz root=/dev/sda5 vga=794 resume=/dev/sda1 \
    splash=verbose showopts
    initrd /boot/initrd
```

使用 `splash=silent` 代替 `splash=verbose` 来防止引导过程中出现引导讯息。

5 用以下命令创建 ISO 映像：

```
mkisofs -R -b boot/grub/stage2_eltorito -no-emul-boot \
-boot-load-size 4 -boot-info-table -o grub.iso /tmp/iso
```

6 使用您选择的实用程序将最终文件 `grub.iso` 烧录到 CD 上。不要将 ISO 映像作为数据文件烧录，而要使用烧录实用程序中烧录 CD 映像的选项。

18.6 图形 SUSE 屏幕

从 SUSE Linux 7.2 开始，如果将选项 `vga=value` 用作内核参数，则会在第一个控制台上显示图形 SUSE 屏幕。如果您使用 YaST 进行安装，则将依照所选的分辨率和图形卡自动激活此选项。可以根据需要通过三种方法禁用 SUSE 屏幕：

在必要时禁用 SUSE 屏幕。

在命令行上输入命令 `echo 0 >/proc/splash` 以禁用图形屏幕。要将其再次激活，请输入 `echo 1 >/proc/splash`。

默认禁用 SUSE 屏幕。

将内核参数 `splash=0` 添加到您的引导加载程序配置中。[第 18 章 引导加载程序 \[367\]](#) 提供了有关此内容的详细信息。但是，如果您倾向于使用文本方式（这是早期版本中的默认方式），请设置 `vga=normal`。

完全禁用 SUSE 屏幕

编译新内核并禁用帧缓冲支持中的选项使用启动屏幕而不是引导徽标。

提示

在内核中禁用帧缓冲支持也会自动禁用启动屏幕。如果您使用自定义内核运行 SUSE，则它不能为系统提供任何支持。

18.7 查错

本节列出使用GRUB进行引导的一些常见问题并提供可能解决方案的简短说明。在位于支持数据库 <http://support.novell.com/> 的文章中介绍了其中一些问题。用搜索对话框搜索 *GRUB*、*引导*和*引导加载程序*之类的关键词。

GRUB 和 XFS

XFS 未在分区引导块中为 *stage1* 预留任何空间。因此，不要指定 XFS 分区作为引导加载程序的位置。此问题可以通过创建单独的引导分区（不使用 XFS 进行格式化）得到解决。

GRUB 报告 GRUB Geom 错误

当引导系统时，GRUB 将检查连接的硬盘的磁盘空间。有时，BIOS 将返回不一致的信息，GRUB 将报告 GRUB Geom 错误。如果出现这种情况，请使用 LILO 或更新 BIOS。有关安装、配置和维护 LILO 的详细信息，可以在支持数据库中关键字“LILO”下获得。

如果将 Linux 安装在未在 BIOS 中注册的其他硬盘上，GRUB 也会返回此错误讯息。找到并正确装载了引导加载程序的 *stage1*，但未找到 *stage2*。可以通过在 BIOS 中注册新硬盘解决此问题。

包含 IDE 和 SCSI 硬盘的系统未引导

安装时，YaST 可能没有正确确定硬盘的引导顺序。例如，GRUB 可能将 `/dev/hda` 视为 `hd0` 并将 `/dev/sda` 视为 `hd1`，虽然 BIOS 中的引导顺序是相反的（SCSI 先于 IDE）。

在这种情况下，在引导进程中借助 GRUB 命令行对硬盘进行更正。在引导系统后，编辑 `device.map` 永久应用新映射。然后，检查 `/boot/grub/menu.lst` 和 `/boot/grub/device.map` 文件中的 GRUB 设备名，并使用以下命令重安装引导加载程序：

```
grub --batch < /etc/grub.conf
```

从第二块硬盘引导 Windows

某些操作系统（例如 Windows）只能从第一块硬盘进行引导。如果这样的操作系统安装在第一块硬盘之外的硬盘上，您可以影响相应菜单项的逻辑更改。

```
...
title windows
    map (hd0) (hd1)
```

```
map (hd1) (hd0)
chainloader (hd1,0)+1
...
```

在此示例中，将从第二块硬盘启动 Windows。出于此目的，请使用 `map` 更改硬盘的逻辑顺序。此更改不会影响 GRUB 菜单文件中的逻辑。因此，必须为 `chainloader` 指定第二块硬盘。

18.8 有关详细信息

有关 GRUB 的大量信息可以在 <http://www.gnu.org/software/grub/> 处获得。还请参阅 grub 信息页面。您也可以在位于 <http://www.novell.com/support> 的支持数据库中搜索关键字“GRUB”获得有关特殊问题的信息。

特别的系统功能组件

本章提供有关各种软件包、虚拟控制台和键盘布局的信息。讨论诸如 `bash`、`cron` 和 `logrotate` 等软件组件，因为在最后的发行周期中已对这些组件进行了更改或增强。即使这些组件很小或者被认为不太重要，但是用户可能希望更改它们的默认行为，因为这些组件通常是与系统紧密结合的。本章的最后是有关语言和国家/地区特定设置（I18N 和 L10N）的内容。

19.1 特殊软件包的相关信息

程序 `bash`、`cron`、`logrotate`、`locate`、`ulimit` 和 `free`，以及文件 `resolv.conf` 对于系统管理员和许多用户是非常重要的。手册页和信息页是命令相关信息的两个有用来源，但是它们并不是始终可用的。GNU Emacs 是一种流行的并且非常容易配置的文本编辑器。

19.1.1 `bash` 包和 `/etc/profile`

`Bash` 是默认的系统 shell。在用作登录 shell 时，它将读取几个初始化文件。`Bash` 按照这些文件在列表中出现的顺序处理它们：

1. `/etc/profile`
2. `~/.` 配置文件
3. `/etc/bash.bashrc`

4. ~/.bashrc

在 ~/.profile 或 ~/.bashrc 中进行自定义设置。要确保正确处理这些文件，需要将基本设置从 /etc/skel/.profile 或 /etc/skel/.bashrc 复制到用户的主目录中。建议在更新后从 /etc/skel 复制这些设置。执行以下 shell 命令可防止个人调整的损失：

```
mv ~/.bashrc ~/.bashrc.old
cp /etc/skel/.bashrc ~/.bashrc
mv ~/.profile ~/.profile.old
cp /etc/skel/.profile ~/.profile
```

然后从 *.old 文件将个人调整复制过来。

19.1.2 cron 包

如果要在预定义的时间在后台定期自动运行命令，请使用 cron 工具。cron 是由特殊格式的时间表驱动的。这些表有一部分是系统附带的，但如有需要，用户可以自行编写表。

cron 表位于 /var/spool/cron/tabs 中。/etc/crontab 用作系统范围的 cron 表。输入在时间表之后且在此命令之前运行此命令的用户名。在例 19.1 “/etc/crontab 中的项” [386] 中，输入的是 root。位于 /etc/cron.d 中的包特定的表具有相同的格式。请参见 cron 手册页 (man cron)。

例 19.1 /etc/crontab 中的项

```
1-59/5 * * * * root test -x /usr/sbin/atrun && /usr/sbin/atrun
```

不能通过调用命令 crontab -e 来编辑 /etc/crontab。必须直接将该文件装载到编辑器中，对其进行修改，然后保存。

许多包将 shell 脚本安装到目录 /etc/cron.hourly、/etc/cron.daily、/etc/cron.weekly 和 /etc/cron.monthly 中，它们的执行是由 /usr/lib/cron/run-crons 控制的。/usr/lib/cron/run-crons 每隔 15 分钟在主表 (/etc/crontab) 中运行一次。这样可以确保在适当的时间运行可能被忽略的进程。

要运行 hourly、daily 或在自定义时间运行其他周期性维护脚本，请去除通常使用 /etc/crontab 项的时戳文件（请参见例 19.2 “/etc/crontab：去除时戳文件” [387]，它去除了每个整点之前的 hourly 和每天早上 2:14 的 daily 等）。

例 19.2 /etc/crontab: 去除时戳文件

```
59 * * * * *    root    rm -f /var/spool/cron/lastrun/cron.hourly
14 2 * * *      root    rm -f /var/spool/cron/lastrun/cron.daily
29 2 * * 6      root    rm -f /var/spool/cron/lastrun/cron.weekly
44 2 1 * *      root    rm -f /var/spool/cron/lastrun/cron.monthly
```

或者，在 `/etc/sysconfig/cron` 中将 `DAILY_TIME` 设置为 `cron.daily` 应该启动的时间。`MAX_NOT_RUN` 的设置确保日常作业被触发运行，即使用户在很长时间内没有在指定的 `DAILY_TIME` 打开计算机。`MAX_NOT_RUN` 的最大值为 14 天。

为了清楚起见，将日常系统维护作业分布在多个脚本中。这些脚本包含在包 `aaa_base` 中。例如，`/etc/cron.daily` 中包含组件 `suse.de-backup-rpmdb`、`suse.de-clean-tmp` 或 `suse.de-cron-local`。

19.1.3 日志文件：包 logrotate

有许多系统服务（守护程序）以及内核本身定期将系统状态和特定事件记录到日志文件中。这样，管理员可以定期检查系统在某一时刻的状态，识别错误或故障功能，并精确诊断它们。这些日志文件通常储存在 `FHS` 指定的 `/var/log` 中，文件大小每天都会增长。`logrotate` 包可以帮助控制这些文件的生长。

用文件 `/etc/logrotate.conf` 配置 `logrotate`。特别地，`include` 规范主要配置了其他要读取的文件。在 `/etc/logrotate.d` 中产生日志文件、安装的各个配置文件的程序。例如，随包 `apache2(/etc/logrotate.d/apache2)` 和 `syslogd(/etc/logrotate.d/syslog)` 一起提供的文件。

例 19.3 */etc/logrotate.conf* 的示例

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own lastlog or wtmp - we'll rotate them here
#/var/log/wtmp {
#   monthly
#   create 0664 root utmp
#   rotate 1
#}

# system-specific logs may be also be configured here.
```

通过 **cron** 控制 **logrotate**，并通过 `/etc/cron.daily/logrotate` 每天对其进行调用。

重要

使用 **create** 选项可以读取管理员在 `/etc/permissions*` 中进行的所有设置。确保没有因个人修改而引起的冲突。

19.1.4 locate 命令

locate 是一个用于查找文件的命令，它不包括在已安装软件的标准范围内。如果需要，请安装包 **findutils-locate**。**updatedb** 进程将在每天晚上或引导系统约 15 分钟后自动启动。

19.1.5 ulimit 命令

使用 `ulimit` (*user limits*) 命令，可以对系统资源的使用设置限制并将这些信息显示出来。`ulimit` 尤其适用于限制应用程序可用的内存。使用此命令，可以防止某个应用程序自己占用太多内存，这可能导致系统停顿。

可以对 `ulimit` 使用多个选项。要限制使用内存，请使用 [表 19.1 “ulimit：为用户设置资源”](#) [389] 中列出的选项。

表 19.1 *ulimit*：为用户设置资源

<code>-m</code>	物理内存的最大大小
<code>-v</code>	虚拟内存的最大大小
<code>-s</code>	堆栈的最大大小
<code>-c</code>	核心文件的最大大小
<code>-a</code>	显示限制设置

可以在 `/etc/profile` 中创建系统范围的项。在这里可以创建编程人员进行调试所需的 `核心文件`。普通用户不能增加系统管理员在 `/etc/profile` 中指定的值，但可以在 `~/.bashrc` 中进行特殊输入。

例 19.4 *ulimit*：~/.bashrc 中的设置

```
# Limits of physical memory:
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

必须以 **KB** 为单位指定内存大小。有关详细信息，请参见 `man bash`。

重要

并非所有 `shell` 都支持 `ulimit` 指令。如果您依赖于这些限制的内含设置，则 `PAM`（例如 `pam_limits`）提供了全面的调整功能。

19.1.6 free 命令

如果您的目的是查看当前使用了多少 RAM，则 `free` 命令可能会令人产生误解。`/proc/meminfo` 中提供了此信息。目前，使用 Linux 等现代操作系统的用户实际上无需过多地担心内存。可用 RAM 的概念可追溯到统一内存管理之前。可用内存不是好的内存这种说法非常适用于 Linux。因此，Linux 一直在平衡超速缓存方面下功夫，不允许实际上存在可用或未使用的内存。

内核基本上不直接管理任何应用程序或用户数据。而是在一个页超速缓存中管理应用程序和用户数据。如果内存不足，它的某些部分会被写入交换分区或文件中，借助于 `mmap` 命令，可以最先从这些交换分区或文件中读取这些部分（请参见 `man mmap`）。

此外，内核中还包含其他超速缓存，如 *slab* 超速缓存，其中储存着用于网络访问的超速缓存。这也许能够解释 `/proc/meminfo` 中计数器之间的差异。通过 `/proc/slabinfo` 可以访问大多数（但并非全部）*slab* 超速缓存。

19.1.7 /etc/resolv.conf 文件

系统通过文件 `/etc/resolv.conf` 处理域名解析。

此文件仅由脚本 `/sbin/modify_resolvconf` 进行更新，任何其他程序都没有直接修改 `/etc/resolv.conf` 的权限。只有实施这条规则才能确保系统的网络配置和相关文件保持一致。

19.1.8 手册页和信息页

对于某些 GNU 应用程序（如 `tar`），已不再保留手册页。对于这些命令，可使用 `--help` 选项快速查看信息页，其中提供更多深入的说明。`info` 是 GNU 的超文本系统。通过输入 `info info` 可以看到此系统的介绍。通过输入 `emacs -f Info` 可使用 Emacs 查看信息页，也可以在控制台中使用 `info` 直接查看信息页。还可以使用 `tkinfo`、`xinfo` 或 帮助系统来查看信息页。

19.1.9 GNU Emacs 的设置

GNU Emacs 是一个复杂的工作环境。下面几节介绍当启动 GNU Emacs 时处理的配置文件。有关详细信息，请参见 <http://www.gnu.org/software/emacs/>。

启动时，Emacs 读取包含用户、系统管理员和经销商的设置的多个文件以进行自定义或预配置。初始化文件 `~/.emacs` 被安装到 `/etc/skel` 中各个用户的主目录中。`.emacs` 又会读取文件 `/etc/skel/.gnu-emacs`。要自定义程序，请（通过 `cp /etc/skel/.gnu-emacs ~/.gnu-emacs`）将 `.gnu-emacs` 复制到用户主目录并在那里进行所需的设置。

`.gnu-emacs` 将文件 `~/.gnu-emacs-custom` 定义为 `custom-file`。如果用户通过 Emacs 中的 `customize` 选项进行设置，则这些设置将保存到 `~/.gnu-emacs-custom` 中。

通过 SUSE® Linux Enterprise，emacs 包将文件 `site-start.el` 安装在目录 `/usr/share/emacs/site-lisp` 中。文件 `site-start.el` 在初始化文件 `~/.emacs` 之前进行装载。除其他作用之外，`site-start.el` 确保自动装载通过 Emacs 扩充包分发的特殊配置文件（例如 `psgml`）。此类型的配置文件也位于 `/usr/share/emacs/site-lisp` 中，总是以 `suse-start-` 开头。本地系统管理员可以在 `default.el` 中指定整个系统范围的设置。

初始化文件下的 EMACS 信息文件中提供了有关这些文件的详细信息：<info:/emacs/InitFile> 此位置还提供了有关如何禁止装载这些文件（如果需要）的信息。

Emacs 的部件被分成多个包：

- 基础包 `emacs`。
- `emacs-x11`（通常已安装）：支持 X11 的程序
- `emacs-nox`：不支持 X11 的程序。
- `emacs-info`：info 格式的联机文档。
- `emacs-el`：Emacs Lisp 中未编译的库文件。运行时不需要这些库文件。

- 如果需要，可安装众多附加软件包：emacs-auctex（用于 LaTeX）、psgml（用于 SGML 和 XML）、gnuserv（用于客户机和服务器操作）以及其他。

19.2 虚拟控制台

Linux 是一个多用户和多任务的系统。即使是在独立计算机系统上也可以感受到这些功能的好处。在文本方式下，提供了 6 个虚拟控制台。可以使用 Alt + F1 到 Alt + F6 在这些控制台间切换。第 7 个控制台是为 X 保留的，而第 10 个控制台显示内核讯息。可以通过修改文件 /etc/inittab 指定更多的控制台或减少控制台。

要从 x 切换到控制台而不将其关闭，请使用 Ctrl + Alt + F1 到 Ctrl + Alt + F6。要返回到 X，请按 Alt + F7。

19.3 键盘映射

为了标准化程序的键盘映射，对以下文件进行了更改：

```
/etc/inputrc
/etc/X11/Xmodmap
/etc/skel/.Xmodmap
/etc/skel/.exrc
/etc/skel/.less
/etc/skel/.lesskey
/etc/csh.cshrc
/etc/termcap
/usr/lib/terminfo/x/xterm
/usr/share/X11/app-defaults/XTerm
/usr/share/emacs/VERSION/site-lisp/term/*.el
```

这些更改只影响使用 terminfo 项的应用程序或其配置文件被直接更改（vi、less 等）的应用程序。不是系统附带的应用程序应该根据这些默认设置进行调整。

在 X 下，可以使用 Ctrl + Shift（右边的）访问组合键 (multikey)。同时可以在 /etc/X11/Xmodmap 中看到对应的项。

可以通过“X 键盘扩展”(XKB) 进行进一步的设置。桌面环境 GNOME (gswitchit) 和 KDE (kxkb) 也使用此扩展。

提示: 更多信息

有关 **XKB** 的信息, 请参见 `/etc/X11/xkb/README` 和那里列出的文档。

有关中文、日文和韩文 (CJK) 输入的详细信息, 请参阅 **Mike Fabian** 的网页:
<http://www.suse.de/~mfabian/suse-cjk/input.html>

19.4 语言和国家/地区特定的设置

该系统在很大程度上实施了国际化, 可通过灵活的方式进行修改以满足本地需要。换句话说, 国际化 (*I18N*) 允许特定的本地化 (*L10N*)。I18N 和 L10N 这两个缩写词使用原单词的第一个和最后一个字母, 中间的数字表示省略的字母数。

设置是通过文件 `/etc/sysconfig/language` 中定义的 `LC_` 变量进行的。这不仅指本地语言支持, 还指消息 (语言)、字符集、排序顺序、日期和时间、数字和货币等类别。这些类别中的每一种都可以使用其自己的变量直接定义或使用文件 `language` 中的主变量间接定义 (请参阅手册页 `man locale`)。

`RC_LC_MESSAGES`、`RC_LC_CTYPE`、`RC_LC_COLLATE`、`RC_LC_TIME`、`RC_LC_NUMERIC`、`RC_LC_MONETARY`

这些变量以不带 `RC_` 前缀的形式传递到 `shell`, 它们代表所列出的类别。下面列出了相关 `shell` 配置文件。可以使用命令 `locale` 显示当前设置。

`RC_LC_ALL`

此变量 (如果设置) 将覆盖上述变量的值。

`RC_LANG`

如果未设置上述的任何变量, 则这是后备变量。默认情况下, 只设置 `RC_LANG`。这便于用户输入他们自己的值。

`ROOT_USES_LANG`

`yes` 或 `no` 变量。如果将其设置为 `no`, 则 `root` 用户始终在 `POSIX` 环境中工作。

这些变量可通过 **YaST** `sysconfig` 编辑器进行设置 (请参阅第 17.3.1 节 “使用 **YaST Sysconfig** 编辑器更改系统配置” [364])。此类变量的值中包含语言代码、国家/地区代码、编码和修饰符。各部分之间通过特殊字符连接:

```
LANG=<language>[[[_<COUNTRY>].<Encoding>[@<Modifier>]]
```

19.4.1 一些示例

语言和国家/地区代码始终应该一起设置。语言设置遵循 ISO 639 标准（可从 <http://www.evertype.com/standards/iso639/iso639-en.html> 和 <http://www.loc.gov/standards/iso639-2/> 上获取）。国家/地区代码在 ISO 3166（可从 http://www.din.de/gremien/nas/nabd/iso3166ma/codlstpl/en_listpl.html 上获取）中列出。

只有设置可以在 `/usr/lib/locale` 中找到其可用说明文件的值才有意义。可以使用命令 `localedef` 基于 `/usr/share/i18n` 中的文件创建更多说明文件；说明文件是 `glibc-i18ndata` 包的一部分。可以使用以下命令创建 `en_US.UTF-8`（用于英国英语和美国英语）的说明文件：

```
localedef -i en_US -f UTF-8 en_US.UTF-8
```

```
LANG=en_US.UTF-8
```

如果在安装过程中选择的是美国英语，则这是默认设置。如果选择了其他语言，则将支持该语言，但仍使用 UTF-8 作为字符编码。

```
LANG=en_US.ISO-8859-1
```

这会将语言设置为英语，将国家/地区设置为美国，将字符集设置为 ISO-8859-1。此字符集不支持欧元符号，但它有时可用于尚未进行更新以支持 UTF-8 的程序。随后，**Emacs** 等程序将对定义字符集的字符串（在本例中为 ISO-8859-1）进行求值。

```
LANG=en_IE@euro
```

上例将欧元符号显式包含在语言设置中。严格来说，此设置目前已过时，因为 UTF-8 也包含欧元符号。该设置仅在应用程序不支持 UTF-8 但支持 ISO-8859-15 时才有用。

SUSEconfig 读取 `/etc/sysconfig/language` 中的变量并将必需的更改写入 `/etc/SuSEconfig/profile` 和 `/etc/SuSEconfig/csh.cshrc`。`/etc/SuSEconfig/profile` 被 `/etc/profile` 读取或用作其数据的来源。`/etc/SuSEconfig/csh.cshrc` 被用作 `/etc/csh.cshrc` 的数据来源。这使设置在整个系统范围内可用。

用户可以通过相应地编译他们的 `~/ .bashrc` 覆盖系统默认值。例如，如果不想将整个系统范围的 `en_US` 用于程序讯息，请包括 `LC_MESSAGES=es_ES`，这样讯息将以西班牙语显示。

19.4.2 `~/ .i18n`中的语言环境设置

如果您对系统默认的区域设置不满意，请根据 **Bash** 脚本编写语法更改 `~/ .i18n` 中的设置。`~/ .i18n` 中的项覆盖来自 `/etc/sysconfig/language` 中的系统默认值。使用相同的变量名而不使用 `RC_` 名称空间前缀，例如，使用 `LANG` 而不是 `RC_LANG`：

```
LANG=cs_CZ.UTF-8
LC_COLLATE=C
```

19.4.3 语言支持的设置

讯息类别中的文件通常只储存在对应的语言目录（例如 `en`）中以保留后备。如果将 `LANG` 设置为 `en_US` 并且 `/usr/share/locale/en_US/LC_MESSAGES` 中的讯息文件不存在，则它将使用 `/usr/share/locale/en/LC_MESSAGES`。

还可以定义后备语言，例如，将布列塔尼语作为法语的后备语言，将加利西亚语作为葡萄牙语的后备语言。

```
LANGUAGE="br_FR:fr_FR"
```

```
LANGUAGE="gl_ES:es_ES:pt_PT"
```

如果需要，可改用挪威语变体 **Nynorsk** 和 **Bokmal**（将其他后备语言设置为 `no`）：

```
LANG="nn_NO"
```

```
LANGUAGE="nn_NO:nb_NO:no"
```

或

```
LANG="nb_NO"
```

```
LANGUAGE="nb_NO:nn_NO:no"
```

请注意，在挪威语中，`LC_TIME` 的处理方式也有所不同。

可能会出现一个问题，那就是无法正确识别用于分隔成组数位的分隔符。如果 LANG 设置为仅两个字母的语言代码（如 de），但使用的定义文件 `glibc` 位于 `/usr/share/lib/de_DE/LC_NUMERIC`，则将出现此问题。因此必须将 `LC_NUMERIC` 设置为 `de_DE` 以使系统能够识别出分隔符定义。

19.4.4 有关详细信息

- 《GNU C 库参考手册“》中的“区域设置和国际化”一章。”它包含在 `glibc-info` 中。
- Markus Kuhn 编写的 *Unix/Linux 的 UTF-8 和 Unicode 常见问题解答*，当前位于 <http://www.cl.cam.ac.uk/~mgk25/unicode.html>。
- *Unicode-Howto*，作者 Bruno Haible: `/usr/share/doc/howto/en/html/Unicode-HOWTO.html`。

打印机操作

SUSE Linux Enterprise® 支持用许多类型的打印机进行打印，包括远程网络打印机。打印机可以用 YaST 或手动进行配置。启动和管理打印作业时既可以使用图形实用程序，也可以使用命令行实用程序。如果打印机未能按预期正常工作，请参阅第 20.9 节“查错”[410]。

CUPS 是 SUSE Linux Enterprise 中的标准打印系统。CUPS 高度面向用户。在很多情况下，它与 LPRng 兼容或者可以相对方便地进行调整。仅出于兼容性的原因，LPRng 包括在 SUSE Linux Enterprise 中。

可以根据接口（例如 USB 或网络）以及打印机语言对打印机进行区分。购买打印机时，请确认打印机具有一个您的硬件上可用的接口（比如 USB 或并行接口）和合适的打印机语言。可以按照以下三类打印机语言对打印机进行分类：

PostScript 打印机

Linux 和 Unix 中的内部打印系统使用 PostScript 这种打印机语言生成并处理大部分打印作业。这种语言已经有很长的历史并且非常有效。如果打印机可以直接处理 PostScript 文档而不需要在打印系统中通过附加步骤转换这些文档，则可以降低可能出现的错误的数目。因为 PostScript 打印机购买许可证要花费大量的成本，所以购买这些打印机的花费比不带 PostScript 解释器的打印机要高得多。

标准打印机（PCL 和 ESC/P 等语言）

虽然这些打印机语言有相当长的历史，但它们仍在进行扩展以处理打印机中的新功能。对于已知的打印机语言，打印系统可以借助 Ghostscript 将 PostScript 作业转换为相应的打印机语言。这一处理阶段被称为解释。最有名的语言有 PCL（主要是 HP 打印机及其克隆产品使用）和 ESC/P（Epson 打印机使用）。这些打印机语言通常受 Linux 支持，可以生成相当好的打

印效果。Linux 可能不能处理非常新以及非常特别的打印机的一些功能，原因是开放源代码的开发人员可能仍在开发这些功能的代码。除了 HP 开发的 `hpijs` 驱动程序之外，当前尚没有其他打印机制造商开发 Linux 驱动程序并在开发源代码许可证下将这些驱动程序提供给 Linux 经销商。这些打印机中大多数价格适中。

专有打印机（也称作 GDI 打印机）

这些打印机不支持任何常见的打印机语言。这些打印机使用自己的无文档记录打印机语言，该语言在发布新版本时可能发生变化。通常只有 Windows 驱动程序供这些打印机使用。有关更多信息，请参见第 20.9.1 节“**打印机没有标准打印机语言支持**”[411]。

在您购买新打印机之前，请参考以下资源以了解您要购买的打印机的支持情况：

<http://www.linuxprinting.org/>

LinuxPrinting.Org 打印机数据库。

<http://www.cs.wisc.edu/~ghost/>

Ghostscript 万维网网页

`/usr/share/doc/packages/ghostscript/catalog.devices`

包括的驱动程序的列表。

联机数据库总是显示最新的 Linux 支持状态。但是，Linux 分发只能集成生产时可用的驱动程序。因此，在最新的 SUSE Linux Enterprise 版本发布时，当前标为“完全支持”的打印机不一定具有此状态。这样，数据库不一定可以指出正确的状态，只是提供大致估计而已。

20.1 打印系统工作流程

用户创建一个打印作业。该打印作业包含有要打印的数据以及假脱机程序的信息，例如打印机的名称或打印机队列的名称，还可能包括过滤器的信息，例如打印机特定的选项。

每台打印机至少有一个专用打印机队列。假脱机程序储存着队列中的打印作业，直到所需打印机已做好接收数据的准备。打印机准备就绪后，假脱机程序通过过滤器和后端将数据发送到打印机。

过滤器将转换正在打印的应用程序生成的数据（通常为 PostScript 或 PDF，也可能为 ASCII、JPEG 等）特定于打印机的数据（PostScript、PCL、ESC/P 等）。PPD 文件中描述了打印机的功能。PPD 文件包含打印机特定的选项以及在打印机上启用这些选项所需的参数。过滤器系统用于确保用户选择的选项被启用。

如果使用的是 PostScript 打印机，则过滤器系统将数据转换为打印机特定的 PostScript。这样做不需要打印机驱动程序。如果使用的是非 PostScript 打印机，则过滤器系统会使用 Ghostscript 将数据转换为打印机特定的数据。这样做需要一个适合您的打印机的 Ghostscript 打印机驱动程序。后端从过滤器接收打印机特定的数据，然后将其传递到打印机。

20.2 连接打印机的方法和协议

可以通过多种方法将打印机连接到系统。CUPS 打印系统的配置不能区分本地打印机和通过网络连接到系统的打印机。在 Linux 中，必须按照打印机制造商提供的手册中所说明的方法连接本地打印机。CUPS 支持串口、USB、并口和 SCSI 连接。有关打印机连接的更多信息，请阅读位于http://en.opensuse.org/SDB:CUPS_in_a_Nutshell的支持数据库中的文章 *CUPS in a Nutshell*。

警告: 更改处于运行状态系统中的电缆连接

当将打印机连接到计算机时，一定不要忘记操作期间只能插入或拔下 USB 设备。为防止损坏系统或打印机，请在更改任何非 USB 连接前先关闭系统。

20.3 安装软件

PPD（PostScript 打印机描述）是描述属性（例如，分辨率）和选项（例如，双面打印单位的可用性）的计算机语言。这些描述对于使用 CUPS 中的各个打印机选项是必需的。如果没有 PPD 文件，打印数据将被以“原始”状态转发到打印机，通常这不是希望出现的情况。“”在 SUSE Linux Enterprise 安装过程中，将预安装多个 PPD 文件，使系统甚至可以使用不带 PostScript 支持的打印机。

要配置 PostScript 打印机，最佳的方法是获得一个合适的 PPD 文件。包 `manufacturer-PPDs` 中提供许多 PPD 文件，标准安装会自动安装此包。请参见第 20.8.3 节“多种包中的 PPD 文件”[408]和第 20.9.2 节“没有合适的 PPD 文件可用于 PostScript 打印机”[411]。

可以将新 `ppd` 文件储存在目录 `/usr/share/cups/model/` 中或使用 YaST 添加到打印系统中（请参见“[用 YaST 添加 PPD 文件](#)”一节 [403]）。随后，可以在安装过程中选择 PPD 文件。

如果打印机制造商要求您除修改配置文件之外安装整个软件包，则一定要注意。首先，这种安装将导致丢失 SUSE Linux Enterprise 提供的支持；其次，打印命令将以不同的方式工作，系统可能不再能处理其他制造商的设备。出于此原因，不建议安装制造商软件。

20.4 设置打印机

YaST 可用于配置直接连接到您计算机的本地打印机（通常带有 USB 或并行端口），或设置通过网络打印。还可以用 YaST 为您的打印机添加 PPD (PostScript Printer Description) 文件。

20.4.1 配置本地打印机

如果检测到未配置的本地打印机，YaST 会自动启动配置它。如果能够自动设置并行或 `usb` 端口并检测到所连接的打印机，则 YaST 能够自动配置打印机。打印机型号也必须列在自动硬件检测期间使用的数据库中。

如果打印机型号未知或无法自动检测出来，请手动配置它。没有自动检测到打印机，可能的原因有两个：

- 打印机无法正确识别自身。这可能适用于很老的设备。试试按“[手动配置](#)”一节 [400]中所述配置打印机。
- 如果手动配置不起作用，就不可能在打印机和计算机间进行通讯。检查电缆和插头，确保打印机连接正确。如果是这种情况，问题可能并非和打印机相关，而是与 USB 或并行端口有关。

手动配置

要手动配置打印机，请在 YaST 控制中心中选择 **硬件 > 打印机**。这将打开 **打印机配置** 主窗口，窗口上部列出了检测到的设备。下半部分列出了目前为止已配置的所有队列（关于打印队列的更多信息，请参见 [第 20.1 节 “打印系统工作流程”](#) [398]）。如果未检测到打印机，配置窗口的两部分都将是空的。用 **编辑更改**

列出的打印机的配置，或用添加安装未自动检测出来的打印机。编辑现有的配置会使用[手动添加本地打印机](#) [401]中相同的对话框。

在打印机配置中，您还可以删除现有的条目。单击其他将打开具有高级选项的列表。选择[重新启动检测](#)以手动启动自动打印机检测。如果有多台打印机连接到计算机，或者为某打印机配置了多个队列，可标记活动条目为默认设置。[CUPS 专家设置和更改 IPP 侦听](#)是高级配置选项 — 细节请参考[第 20 章 打印机操作](#) [397]。

过程 20.1 手动添加本地打印机

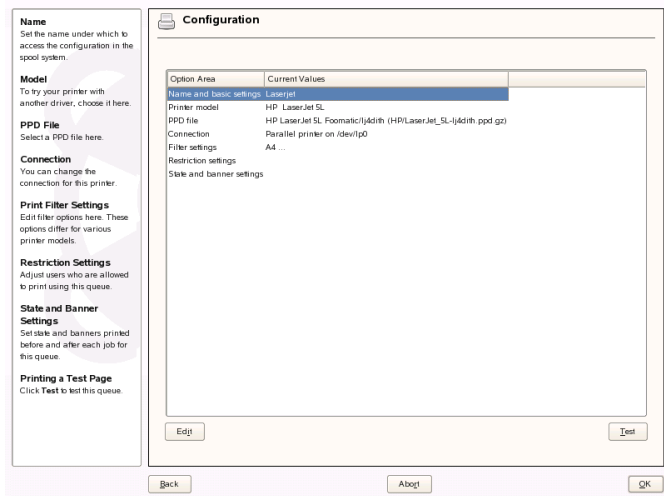
提示: YaST 打印测试

为了确保一切工作正常，应使用 YaST 的打印测试功能对关键配置步骤进行检查。测试页还提供了有关测试的配置的重要信息。如果输出不正常（例如有多页几乎是空白的），则应首先取出所有纸张，然后从 YaST 停止测试，这样便可以停止打印机。

- 1 启动 YaST，选择硬件 > 打印机打开打印机配置对话框。
- 2 单击添加打开打印机类型窗口。
- 3 选择直接连接的打印机。
- 4 选择该打印机要连接的端口（通常是 USB 或并行端口），在下个配置屏幕中选择设备。建议在此时[测试打印机连接](#)。如果出现问题，请选择正确的设备，或选择[返回](#)回到上个对话框。
- 5 在队列名称中，设置打印队列。必须指定打印名称。建议选择一个方便识别的名称，用该名称您以后可以在应用程序的打印对话框中认出该打印机。用[打印机说明](#)和[打印机位置](#)进一步描述打印机。这是可选的，但如果您有多台打印机连接到一台计算机上，或者安装打印机服务器，就很有用。应选中[执行本地过滤](#)，这是本地打印机必需的。
- 6 在打印机型号中用制造商和型号指定打印机。如果未列出您的打印机，您可以尝试制造商列表中的 `UNKNOWN MANUFACTURER`，从型号列表选择适当的标准语言（控制打印机的一组命令）（请参见打印机的文档查找打印机可接受哪种语言）。如果不起作用，请参见[“用 YaST 添加 PPD 文件”一节](#) [403]了解其他可能的解决方案。

7 配置屏幕列出了打印机安装的摘要。从 YaST 模块的开始屏幕编辑现有打印机配置时，也会显示该对话框。

图 20.1 打印机配置摘要



该摘要包含以下条目，您也可以编辑进行修改：

- 名称和基本设置、打印机型号和连接可用于按该步骤更改已有的条目。
- 有关 PPD 文件的细节，请参见“用 YaST 选择备用 PPD 文件”一节 [403]。
- 用过滤器设置微调打印机设置。在这里配置页面大小、颜色模式和分辨率之类的选项。
- 默认设置下，每个用户都能使用打印机。用限制设置列出禁止使用打印机的用户或允许使用它的用户。
- 举例来说，用状态和标题页设置，您可以通过更改其状态取消激活打印机，指定每个作业前后是否打印开始标题页或结束标题页的页面（默认是不打印）。

用 YaST 添加 PPD 文件

如果您的打印机未在打印机型号对话框中显示，则缺少您型号的 PPD (PostScript Printer Description) 文件（第 20.3 节“安装软件”[399]中有关于 PPD 文件的更多信息）。用添加 PPD 文件至数据库从本地文件系统或 FTP、HTTP 服务器添加 PPD 文件。

直接从您的打印机供应商或打印机的驱动程序 CD 获得 PPD 文件（细节请参见第 20.9.2 节“没有合适的 PPD 文件可用于 PostScript 打印机”[411]）。另一个 PPD 文件的来源是 <http://www.linuxprinting.org/>，“Linux 打印数据库”。从 linuxprinting.org 下载 PPD 文件时，请记住它总显示最新的 Linux 支持状态，SUSE Linux Enterprise 未必符合。

用 YaST 选择备用 PPD 文件

对许多打印机型号，都有几个 PPD 文件可用。配置打印机时，YaST 默认为标有推荐的那个，这是一般规则。要获取某打印机可用的 PPD 文件列表，请在配置中选择 PPD 文件，然后单击编辑。请参见图 20.1“打印机配置摘要”[402]。

通常没有必要更改 PPD 文件，YaST 选择的 PPD 文件应能产生最佳效果。但是，如果希望彩色打印机只打印黑白两种颜色，使用不支持彩色打印的 PPD 文件最为方便。如果用 PostScript 打印机打印图形时遇到性能问题，从 PostScript PPD 文件换到 PCL PPD 文件（假定您的打印机能读 PCL）可能有帮助。

20.4.2 用 YaST 配置网络打印机

无法自动检测到网络打印机。必须使用 YaST 打印机模块手动进行配置。视您的网络设置而定，可以打印到打印服务器（CUPS、LPD、SMB 或 IPX）或直接打印到网络计算机（首选通过 TCP）。关于在您的环境中配置网络打印机的细节，请咨询您的网络管理员。

过程 20.2 使用 YaST 配置网络打印机

- 1 启动 YaST 并选择硬件 > 打印机，以打开打印机配置对话框。
- 2 单击添加，以打开打印机类型窗口。

- 3 选择**网络打印机**以打开一个对话框，并在对话框中指定由网络管理员提供的进一步详细信息。

20.5 网络打印机

网络打印机可以支持多种协议，其中某些甚至是同时进行的。虽然大多数支持的协议是标准化的，但某些制造商因为测试尚未正确实施标准的系统或要提供标准中未提供的功能，所以对标准进行了扩展（修改）。于是制造商提供仅用于几个操作系统的驱动程序，解决使用这些系统遇到的困难。不过很少提供 Linux 驱动程序。当前的情况是您在执行操作时不能假定每个协议都可以在 Linux 中正常工作。因此，您可能需要试验不同的选项来实现工作正常的配置。

重要: 远程访问设置

默认情况下，**cupsd** 仅侦听内部网络接口 (`localhost`)。设置 **CUPS** 网络服务器时，您需要调整 `/etc/cups/cupsd.conf` 中的侦听指令以侦听外部网络。

CUPS 支持 `socket`、`LPD`、`IPP` 和 `smb` 协议。

套接字

套接字是指未先执行数据握手就将数据发送到因特网套接字所使用的连接。一些常用的套接字端口号包括 9100 或 35。设备 URI（统一资源标识符）的语法为 `socket://打印机 IP:端口`，例如 `socket://192.168.2.202:9100/`。

LPD（行式打印机守护程序）

RFC 1179 中对经过证明的 LPD 协议进行了介绍。在此协议下，在发送实际打印数据之前，将先发送一些与作业相关的数据，例如打印机队列的 ID。因此，在为数据传送配置 LPD 协议之前，必须指定打印机队列。不同打印机制造商的实施非常灵活，可以接受任何名称作为打印机队列。如果需要，打印机手册应该指出要使用的名称。通常使用 `LPT`、`LPT1`、`LP1` 或类似的名称。可以在不同 Linux 或 Unix 主机的 CUPS 系统中配置 LPD 队列。LPD 服务的端口号是 515。示例设备 URI 有 `lpd://192.168.2.202/LPT1`。

IPP（因特网打印协议）

IPP 是一个基于 HTTP 协议的相对较新的 (1999) 协议。使用 IPP，所传送的与作业有关的数据比其他协议要多一些。CUPS 使用 IPP 进行内部数据传送。这是在两个 CUPS 服务器之间转发队列的首选协议。要正确配置 IPP，

必须提供打印队列的名称。IPP 的端口号是 631。示例设备 URI 有
`ipp://192.168.2.202/ps` 和
`ipp://192.168.2.202/printers/ps`。

SMB (Windows 共享)

CUPS 还支持在连接到 Windows 共享的打印机上进行打印。用于此目的的协议是 SMB。SMB 使用端口号 137、138 和 139。示例设备 URI 有
`smb://user:password@workgroup/smb.example.com/printer`、
`smb://user:password@smb.example.com/printer` 和
`smb://smb.example.com/printer`。

必须在配置之前确定打印机支持的协议。如果制造商未提供所需的信息，则可以使用命令 `nmap` (附带 `nmap` 包) 来猜测协议。`nmap` 检查主机是否有打开的端口。例如：

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

20.5.1 使用命令行工具配置 CUPS

除了用 YaST 设置 CUPS 选项，配置网络打印机时，CUPS 也可以用命令行工具进行配置，比如 `lpadmin` 和 `lpoptions`。您需要一个设备 URI，该 URI 由一个后端 (例如 USB) 和多个参数 (例如 `/dev/usb/lp0`) 组成。例如，完整的 URI 可能是 `parallel:/dev/lp0` (连接到第一个并行端口的打印机) 或 `usb:/dev/usb/lp0` (所检测到的第一个连接到 USB 端口的打印机)。

使用 `lpadmin`，CUPS 服务器管理员可添加、去除或管理类和打印队列。要添加打印队列，请使用以下语法：

```
lpadmin -p queue -v device-URI -P PPD-file -E
```

使用指定的 PPD 文件 (`-p`)，则设备 (`-v`) 将用作队列 (`-P`)。这意味着如果要手动配置打印机，则必须了解 PPD 文件和设备名称。

不要使用 `-E` 作为第一个选项。对于所有 CUPS 命令，将 `-E` 用作第一个参数设置使用加密连接。要启用打印机，必须使用 `-E`，如下面的示例所示：

```
lpadmin -p ps -v parallel:/dev/lp0 -P \  
/usr/share/cups/model/Postscript.ppd.gz -E
```

以下示例配置了网络打印机：

```
lpadmin -p ps -v socket://192.168.2.202:9100/ -P \  
/usr/share/cups/model/Postscript-levell.ppd.gz -E
```

有关 `lpadmin` 的更多选项，请参考 `lpadmin(1)` 的手册页。

在系统安装期间，某些选项被设置为默认值。可以为每个打印作业修改这些选项（根据所使用的打印工具）。也可以使用 `YaST` 来更改这些默认选项。使用命令行工具设置默认选项，如下所示：

1 首先，列出所有选项：

```
lpoptions -p queue -l
```

示例：

```
Resolution/Output Resolution: 150dpi *300dpi 600dpi
```

激活的默认选项通过加星号前缀 (*) 进行标识。

2 使用 `lpadmin` 更改选项：

```
lpadmin -p queue -o Resolution=600dpi
```

3 检查新设置：

```
lpoptions -p queue -l
```

```
Resolution/Output Resolution: 150dpi 300dpi *600dpi
```

普通用户运行 `lpoptions` 时，设置将写到 `~/.lpoptions`。但是，根设置将写到 `/etc/cups/lpoptions`。

20.6 图形打印接口

像 `xpp` 这样的工具和 KDE 程序 `KPrinter` 都提供了一个图形界面，用于选择队列以及设置 `cups` 标准选项和通过 PPD 文件可用的打印机特定的选项。您甚至可以使用 `KPrinter` 作为非 KDE 应用程序的标准打印接口。在这些应用程序的打印对话框中，指定 `kprinter` 或 `kprinter --stdin` 作为打印命令。使用的命令取决于应用程序的数据传输方式 — 只需通过尝试看哪个能启动 `KPrinter`。如果正确设置，应用程序无论何时发布打印作业均应打开 `KPrinter` 对话框，这样您就可以使用此对话框来选择队列并设置其他打印选项了。这要求应用程序本身的打印设置不能与 `KPrinter` 的打印设置冲突，而且在启用 `KPrinter` 后，只能通过它来更改打印选项。

20.7 从命令行打印

要从命令行打印，请输入 `lp -d queuefilename filename`，使用相应的名称替换 *queuefilename* 和 *filename*。

有些应用程序依赖于 `lp` 命令来进行打印。在这种情况下，请在应用程序的打印对话框中输入正确的命令（通常无需指定 *filename*），例如 `lp -d queuefilename`。

20.8 SUSE Linux Enterprise 中的特殊功能

已对 CUPS 的许多功能进行了调整以用于 SUSE Linux Enterprise。这里将介绍一些最重要的更改。

20.8.1 CUPS 和防火墙

执行默认 SUSE Linux Enterprise 安装后，`SUSEfirewall2` 是活动的，且将外部网络设备配置为在外部区域中（该区域将阻塞入站通讯）。使用 CUPS 时，必须调整这些默认设置。在[第 39.4 节“SUSEfirewall2”](#)^[663]中提供了有关 `SUSEfirewall2` 配置的更多信息。

CUPS 客户程序

通常 CUPS 客户程序在使用防火墙的网络中的常规工作站上运行。在这种情况下，建议将外部网络设备配置为在内部区域中，这样可以使网络内部访问工作站。

CUPS 服务器

如果 CUPS 服务器在受防火墙保护的网路中，则应将外部网络设备配置为在防火墙的内部区域中。属于外部区域时，需要打开 TCP 和 UDP 端口 631，以便可以在网络中访问 CUPS 服务器。

20.8.2 CUPS 打印服务中的更改

BrowseAllow 和 BrowseDeny 的一般功能

为 BrowseAllow 和 BrowseDeny 设置的访问权限适用于发送到 cupsd 的所有类型的包。/etc/cups/cupsd.conf 中的默认设置如下所示：

```
BrowseAllow @LOCAL
BrowseDeny All
```

和

```
<Location />
  Order Deny,Allow
  Deny From All
  Allow From 127.0.0.1
  Allow From 127.0.0.2
  Allow From @LOCAL
</Location>
```

这样，只有 LOCAL 主机可以访问 CUPS 服务器上的 cupsd。LOCAL 主机是其 IP 地址属于非 PPP 接口（未设置其 IFF_POINTOPOINT 标志的接口）并且其 IP 地址与 CUPS 服务器属于同一个网络的主机。将立即拒绝来自所有其他主机的包。

默认激活 cupsd

在标准安装中，将自动激活 cupsd，从而可以方便地访问 CUPS 网络服务器的队列，而无需执行任何其他手动操作。“BrowseAllow 和 BrowseDeny 的一般功能”一节 [408] 中所述的项目是此功能的重要前提，否则对于 cupsd 自动激活，安全性将不够。

20.8.3 多种包中的 PPD 文件

YaST 打印机配置仅使用系统上 /usr/share/cups/model/ 中安装的 PPD 文件为 CUPS 设置队列。为查找用于某个打印机型号的合适的 ppd 文件，YaST 将在硬件检测过程中确定的供应商和型号与存在于系统上 /usr/share/cups/model/ 中的所有 PPD 文件中的供应商和型号进行比较。为此，YaST 打印机配置根据从 PPD 文件抽取的供应商和型号信息生成一个数据库。当您从供应商和型号列表中选择打印机时，将收到符合该供应商和型号的 PPD 文件。

仅使用 PPD 文件而不使用其他信息源的配置的优点在于可以随意修改 `/usr/share/cups/model/` 中的 PPD 文件。YaST 打印机配置可以识别更改并重生供应商和型号数据库。例如，如果您具有 PostScript 打印机，通常您不需要 `cups-drivers` 包中的 Foomatic PPD 文件或 `cups-drivers-stp` 包中的 Gimp-Print PPD 文件。而可以将您的 PostScript 打印机的 PPD 文件直接复制到 `/usr/share/cups/model/`（如果它们尚不存在于 `manufacturer-ppds` 包中）以实现打印机的最佳配置。

cups 包中的 CUPS PPD 文件

为 PostScript 级别 1 和级别 2 打印机调整的 Foomatic PPD 文件对 `cups` 包中的通用 PPD 文件进行了补充：

- `/usr/share/cups/model/Postscript-level1.ppd.gz`
- `/usr/share/cups/model/Postscript-level2.ppd.gz`

cups-drivers 包中的 PPD 文件

通常，Foomatic 打印机过滤器 `foomatic-rip` 与非 PostScript 打印机的 Ghostscript 一起使用。合适的 Foomatic PPD 文件具有项“`*NickName: ... Foomatic/Ghostscript driver`”和“`*cupsFilter: ... foomatic-rip`”。这些 PPD 文件位于 `cups-drivers` 包中。

如果具有项 `*NickName: ... Foomatic ... (recommended)` 的 Foomatic PPD 文件符合打印机型号并且 `manufacturer-PPDs` 包不包含更合适的 PPD 文件，则 YaST 倾向于使用 Foomatic PPD 文件。

cups-drivers-stp 包中的 Gimp-Print PPD 文件

Gimp-Print 中的 CUPS 过滤器 `rastertoprinter`（而不是 `foomatic-rip`）可用于许多非 PostScript 打印机。`cups-drivers-stp` 包中提供此过滤器和合适的 Gimp-Print PPD 文件。Gimp-Print PPD 文件位于 `/usr/share/cups/model/stp/` 中并具有项 `*NickName: ... CUPS+Gimp-Print` 和 `*cupsFilter: ... rastertoprinter`。

manufacturer-PPDs 包中来自打印机制造商的 PPD 文件

manufacturer-PPDs 包中包含来自打印机制造商的 PPD 文件，这些文件是在充分自由的许可证下发布的。应该用打印机制造商的合适 PPD 文件配置 PostScript 打印机，因为此文件支持使用 PostScript 打印机的所有功能。如果满足以下条件，YaST 倾向于使用 manufacturer-PPDs 包中的 PPD 文件：

- 硬件检测过程中确定的供应商和型号符合 manufacturer-PPDs 包的 PPD 文件中的供应商和型号。
- manufacturer-PPDs 包中的 PPD 文件是唯一适合该打印机型号的 PPD 文件，或者有一个具有 *NickName: ... Foomatic/Postscript (recommended) 项的 Foomatic PPD 文件，该项也符合该打印机型号。

因此，在以下情况下，YaST 不使用 manufacturer-PPDs 包中的任何 PPD 文件：

- manufacturer-PPDs 包中的 PPD 文件不符合供应商和型号。如果 manufacturer-PPDs 包只包含用于类似型号的 PPD 文件（例如，如果某个型号系列中的各个型号没有单独的 PPD 文件，而是在 PPD 文件中以类似于 Funprinter 1000 series 的形式指定型号名），则可能发生这种情况。
- 不“建议”使用 Foomatic PostScript PPD 文件。这可能是由于该打印机型号在 PostScript 方式中不能充分有效地操作。例如，因为打印机内存太少而导致它在这种方式中不可靠，或者因为处理器太弱而导致打印机速度太慢。此外，因为 PostScript 支持只作为可选模块提供，所以打印机可能不默认支持 PostScript。

如果 manufacturer-PPDs 包中的 PPD 文件适合 PostScript 打印机，但 YaST 由于上述原因不能对其进行配置，则在 YaST 中手动选择相应的打印机型号。

20.9 查错

下面几节介绍一些最常遇到的打印机硬件和软件问题以及解决或避免这些问题的方法。讨论的主题有 GDI 打印机、PPD 文件和端口配置。另外还讨论常见网络打印机问题、打印件问题以及队列处理。

20.9.1 打印机没有标准打印机语言支持

这些打印机不支持任何常见的打印机语言，只能使用专门的专有控制系列来进行寻址。因此这些打印机只能用于制造商提供了驱动程序的操作系统版本。GDI 是 Microsoft* 为图形设备开发的编程接口。通常制造商只提供 Windows 的驱动程序，而因为 Windows 驱动程序使用 GDI 界面，所有这些打印机也被称作 *GDI 打印机*。实际问题不是编程接口，而是这些打印机只能通过相应打印机型号的专用打印机语言进行处理。

某些 GDI 打印机可进行切换以 GDI 方式或一种标准打印机语言进行操作。请参见打印机手册看这是否可行。有些型号需要有专门的 Windows 软件来进行切换（注：Windows 打印机驱动程序在通过 Windows 进行打印时可能总是将打印机切换回 GDI 模式）。对于其他 GDI 打印机，还有针对标准打印机语言的扩展模块。

某些制造商为他们的打印机提供专有驱动程序。专有打印机驱动程序的缺点在于不能保证这些驱动程序可用于已安装的打印系统，也不能保证它们适合各种硬件平台。相反，支持标准打印机语言的打印机不依赖于特殊的打印系统版本或特殊的硬件平台。

与其花时间使专有 Linux 驱动程序工作，不如购买一台支持的打印机，这样更经济一些。这可以一次性全部解决驱动程序问题，从而无需安装并配置特殊驱动程序软件，也无需获取由于打印系统中开发的新功能而必须安装的驱动程序更新。

20.9.2 没有合适的 PPD 文件可用于 PostScript 打印机

如果 manufacturer-PPDs 包不包含任何用于 PostScript 打印机的合适 PPD 文件，则可以使用打印机制造商提供的驱动程序 CD 上的 PPD 文件或从打印机制造商万维网网页下载合适的 PPD 文件。

如果以 zip 存档 (.zip) 或自解压缩 zip 存档 (.exe) 的形式提供 PPD 文件，则用 unzip 命令将其解包。首先，查看 PPD 文件的许可协议条款。然后使用 cupstestppd 实用程序来确认 PPD 文件是否与“Adobe PostScript 打印机说明文件格式规范 V4.3”相符合，如果实用程序返回“FAIL，”则说明 PPD 文件中的错误很严重，可能导致重大问题。应该解决 cupstestppd 报告的问题点。如果需要，询问打印机制造商是否提供合适的 PPD 文件。

20.9.3 并行端口

最安全的方法是将打印机直接连接到第一个并行端口并在 BIOS 中选择以下并行端口设置：

- I/O 地址：378（十六进制）
- 中断：无关
- 模式：Normal、SPP 或 Output Only
- DMA：禁用

如果即便进行了这些设置仍无法对并行端口上的打印机进行寻址，则按照 BIOS 中的设置在 `/etc/modprobe.conf` 中以 `0x378` 形式显式输入 I/O 地址。如果有两个并行端口，分别被设置为 I/O 地址 378 和 278（十六进制），则以 `0x378,0x278` 形式输入这两个端口。

如果中断 7 可用，则可以用 **例 20.1 “`/etc/modprobe.conf`：第一个并行端口的中断方式”** [412] 中显示的项将其激活。在激活中断方式之前，检查文件 `/proc/interrupts` 看看哪些中断仍在使用中。只显示当前正在使用的中断。根据哪些硬件部件处于活动状态，这可能会有所变化。用于并行端口的中断一定不能被任何其他设备使用。如果您不确定，则使用巡回检测方式，设置 `irq=none`。

例 20.1 `/etc/modprobe.conf`：第一个并行端口的中断方式

```
alias parport_lowlevel parport_pc
options parport_pc io=0x378 irq=7
```

20.9.4 网络打印机连接

确定网络问题

将打印机直接连接到计算机。出于测试目的，将该打印机配置为本地打印机。如果打印机可以工作，则问题与网络有关。

检查 TCP/IP 网络

TCP/IP 网络和名称解析必须可以正常工作。

检查远程可访问性

默认情况下，`cupsd` 仅侦听内部网络接口 (`localhost`)。检查 `/etc/cups/cupsd.conf` 中的侦听指令是否允许从外部网络访问：

```
Listen 192.168.2, *:631
```

检查防火墙设置

CUPS 服务器需要在内部防火墙区域中时或者处于外部区域时必须能够通过 UDP 和 TCP 端口 631 发送和接收数据。

检查远程 lpd

使用以下命令测试是否可以与 *host* 上的 `lpd` (端口 515) 建立 TCP 连接：

```
netcat -z host 515 && echo ok || echo failed
```

如果不能建立与 `lpd` 的连接，则 `lpd` 可能不处于活动状态或可能存在基本网络问题。

以 `root` 用户身份使用以下命令查询远程 *host* 上 *queue* 的状态报告 (可能非常长)，前提是相应的 `lpd` 处于活动状态并且主机接受查询：

```
echo -e "\004queue" \  
| netcat -w 2 -p 722 host 515
```

如果 `lpd` 不响应，则它可能不处于活动状态或可能存在基本网络问题。如果 `lpd` 响应，响应应该说明为什么在主机的队列上不能进行打印。如果您接收到类似 **例 20.2 “来自 `lpd` 的错误讯息”** [413] 中的响应，则问题是由远程 `lpd` 引起的。

例 20.2 来自 `lpd` 的错误讯息

```
lpd: your host does not have line printer access  
lpd: queue does not exist  
printer: spooling disabled  
printer: printing disabled
```

检查远程 cupsd

默认情况下，CUPS 网络服务器应该每隔 30 秒在 UDP 端口 631 上广播其队列。因此，以下命令可用于测试网络中是否有 CUPS 网络服务器。

```
netcat -u -l -p 631 & PID=$! ; sleep 40 ; kill $PID
```

如果广播 CUPS 网络服务器存在，则输出如 **例 20.3 “来自 CUPS 网络服务器的广播”** [414] 所示。

例 20.3 来自 CUPS 网络服务器的广播

```
ipp://192.168.2.202:631/printers/queue
```

以下命令可用于测试是否可以与 *host* 上的 cupsd (端口 631) 建立 TCP 连接:

```
netcat -z host 631 && echo ok || echo failed
```

如果不能建立与 cupsd 的连接, 则 cupsd 可能不处于活动状态或可能存在基本网络问题。如果 cupsd 处于活动状态并且主机接受查询, `lpstat -h host -l -t` 会返回 *host* 上所有队列的状态报告 (可能非常长)。

下一个命令用于测试 *host* 上的 *queue* 是否接受由单个回车字符组成的打印作业。不应打印任何内容。可能会弹出一页空白纸。

```
echo -en "\r" \  
| lp -d queue -h host
```

对网络打印机或打印服务器计算机进行查错

当在打印服务器计算机中运行的假脱机程序要处理大量打印作业时, 有时会导致出现问题。因为这是由打印服务器计算机中的假脱机程序引起的, 所以没什么办法。作为替代解决方法, 可以直接通过 TCP 套接字对连接到打印服务器计算机的打印机进行寻址来绕过打印服务器计算机中的假脱机程序。请参见第 20.5 节“网络打印机”[404]。

这样, 打印服务器计算机仅用作数据传送 (TCP/IP 网络和本地打印机连接) 各种不同形式之间的转换器。要使用此方法, 您需要知道打印服务器计算机上的 TCP 端口。如果打印机连接在打印服务器计算机上并且打开了电源, 则通常可以在打开打印服务器计算机的电源后使用 `nmap` 包中的 `nmap` 实用程序确定此 TCP 端口。例如, `nmap IP-address` 可能会在打印服务器打印机中产生以下输出:

Port	State	Service
23/tcp	open	telnet
80/tcp	open	http
515/tcp	open	printer
631/tcp	open	cups
9100/tcp	open	jetdirect

此输出指出可以在端口 9100 上通过 TCP 套接字对连接到打印服务器计算机的打印机进行寻址。默认情况下, `nmap` 只检查在 `/usr/share/nmap/nmap-services` 中列出的一些常见的端口。要检查所有可能的端口, 请使用命令 `nmap -p from_port-to_port IP-address`。这可能要花一些时间。有关详细信息, 请参考 `nmap` 的手册页。

输入如下命令

```
echo -en "\rHello\r\f" | netcat -w 1 IP-address port  
cat file | netcat -w 1 IP-address port
```

将字符串或文件直接发送到相应的端口以测试是否可以在该端口上对打印机进行寻址。

20.9.5 打印件有问题但没有错误讯息

对于打印系统，打印作业完成的标志是 CUPS 后端完成到接收方（打印机）的数据传送。如果在接收方的进一步处理失败（例如，如果打印机无法打印打印机特定的数据），则打印系统不会对此进行通知。如果打印机无法打印打印机特定的数据，则选择另一个更适合该打印机的 PPD 文件。

20.9.6 禁用的队列

如果向接收方传送数据在多次尝试后都失败，则 CUPS 后端（例如 USB 或 socket）向打印系统（向 cupsd）报告一个错误。后端决定在报告数据传送无法完成之前是否继续尝试以及进行多少次尝试。由于继续尝试可能也是徒劳，cupsd 将禁用相应队列的打印。在消除了问题的起因后，系统管理员必须使用 `/usr/bin/enable` 命令重启用打印。

20.9.7 CUPS 浏览：删除打印作业

如果 CUPS 网络服务器通过浏览向客户机主机广播其队列并且客户机主机上合适的本地 cupsd 处于活动状态，则客户机 cupsd 接受来自应用程序的打印作业并将它们转发到服务器上的 cupsd。当 cupsd 接受打印作业后，会为该作业指派一个新的作业号。因此，客户机主机上的作业号与服务器上的作业号不同。因为通常都将打印作业立即转发，所以不能用客户机主机上的作业号将其删除，原因是一旦将打印作业转发到服务器 cupsd，客户机 cupsd 就会将打印作业视为已完成。

要删除服务器上的打印作业，请使用命令（例如 `lpstat -h cups.example.com -o`）确定服务器上的作业号（必须在服务器尚未完成该打印作业，即尚未完全将其发送到打印机的情况下）。使用此作业号，可以删除服务器上的打印作业：

```
cancel -h cups.example.com queue-jobnumber
```

20.9.8 有问题的打印作业和数据传送错误

如果打印进程中将打印机关闭或关闭计算机，则打印作业保留在队列中，当打开打印机或重引导计算机后，打印继续。必须使用 `cancel` 从队列中去除有问题的打印作业。

如果打印作业有问题或主机和打印机之间的通讯出现错误，则打印机会打印出很多张带有乱码的纸张，这是因为它不能正确处理数据。要解决此问题，请执行以下步骤：

- 1 要停止打印，请将所有纸张从喷墨打印机中取出或打开激光打印机的纸盒。高质量的打印机具有一个用于取消当前打印件的按钮。
- 2 打印作业可能仍在队列中，因为只有在将作业完全发送到打印机后才会将它们去除。使用 `lpstat -o` 或 `lpstat -h cups.example.com -o` 可以检查哪个队列当前正在打印。使用 `cancel queue-jobnumber` 或 `cancel -h cups.example.com queue-jobnumber` 可以删除打印作业。
- 3 即使已将打印作业从队列中删除，某些数据仍会被传送到打印机。检查 CUPS 后端进程是否仍在为相应的队列运行并将其终止。例如，对于连接到并行端口的打印机，可以使用命令 `fuser -k /dev/lp0` 终止仍在访问打印机（更准确地说是并行端口）的所有进程。
- 4 通过关闭打印机一段时间完全重设置打印机。然后插入纸张并打开打印机。

20.9.9 对 CUPS 打印系统进行调试

使用以下通用过程确定 CUPS 打印系统中的问题：

- 1 在 `/etc/cups/cupsd.conf` 中设置 `LogLevel debug`。
- 2 停止 `cupsd`。
- 3 去除 `/var/log/cups/error_log*` 从而无需搜索非常长的日志文件。

- 4 启动 cupsd。
- 5 重复导致问题的操作。
- 6 检查 /var/log/cups/error_log* 中的讯息以确定问题的原因。

使用 udev 进行动态内核设备管理

21

从版本 2.6 开始，内核几乎可以添加或去除正在运行的系统中的任何设备。设备状态的更改（无论插入还是去除设备）需要通知用户空间。一旦插入或者发现设备时就需要进行配置。特定设备的用户需要知道此设备的所有状态更改。udev 提供必需的结构来动态维护设备节点文件以及 `/dev` 目录中的符号链接。udev 规则提供一种将外部设备插入到内核设备事件处理的方法。这使得您可以定制 udev 设备处理，例如通过添加特定脚本作为内核设备处理的一部分来执行，或者请求并导入额外数据从而在设备处理期间进行评估。

21.1 `/dev` 目录

`/dev` 目录中的设备节点提供对相应的内核设备的访问。使用 udev 时，`/dev` 目录反映内核的当前状态。每个内核设备都有相应的设备文件。如果设备从系统断开，则去除此设备节点。

`/dev` 目录的内容保存在临时文件系统中，所有文件都是在每个系统启动时从头创建的。手动创建或有意更改的文件不会在重引导后保留下来。无论相应内核设备的状态如何都出现在 `/dev` 目录中的静态文件和目录，可以放置在 `/lib/udev/devices` 目录中。系统启动时，此目录的内容复制到 `/dev` 目录，它们与 `/lib/udev/devices` 中的文件具有相同的所有权和许可权限。

21.2 内核 uevents 和 udev

必需的设备信息由 sysfs 文件系统导出。对于内核检测到并已初始化的设备，将创建一个带有该设备名称的目录。它包含带有特定于设备属性的属性文件。每次添加或去除设备时，内核发送 **uevent** 来通知 **udev** 此情况。

一旦启动后，**udev** 守护程序从 `/etc/udev/rules.d/*.rules` 文件读取并解析所有提供的规则并将它们保存在内存中。如果更改、添加或去除规则文件，则守护程序接收一个事件并更新该规则在内存中的表示。

每个接收到的事件都根据所提供的规则集进行匹配。这些规则可以增加或更改事件环境关键字、为要创建的设备节点请求特定名称、添加指向该节点的符号链接或者添加设备节点创建后运行的程序。从内核 **netlink** 套接字接收驱动程序内核 **uevent**。

21.3 驱动程序、内核模块和设备

设备的内核总线驱动程序探测。内核为每个检测到的设备创建内部设备结构，驱动程序内核将 **uevent** 发送到 **udev** 守护程序。总线设备通过特殊格式的 ID 来标识自己，这可以识别设备的类型。通常，这些 ID 由供应商和产品 ID 以及其他特定于子系统的值组成。每个总线都有自己对于这些 ID 的方案，称为 **MODALIAS**。内核获取设备信息，由此组成一个 **MODALIAS** ID 字符串，并将该字符串与事件一起发送。对于 USB 鼠标，如下所示：

```
MODALIAS=usb:v046DpC03Ed2000dc00dsc00dp00ic03isc01ip02
```

每个设备驱动程序都带有它可以处理的设备的已知别名列表。这个列表包含在内核模块文件中。程序 **depmod** 读取 ID 列表并在内核的 `/lib/modules` 目录中为所有当前可用的模块创建文件 `modules.alias`。使用这种基础结构，模块的装载就如为每个带有 **MODALIAS** 关键字的事件调用 **modprobe** 一样简单。如果调用 **modprobe \$MODALIAS**，它将组成该设备的设备别名与模块提供的别名相匹配。如果找到匹配的项，则装载该模块。这个通过 **udev** 触发并且自动发生。

21.4 引导和启动设备设置

在 `udev` 守护程序运行之前的引导过程中发生的所有设备事件都会丢失，因为处理这些事件的基础结构保存在根文件系统中，并且此时不可用。为了弥补损失，内核为 `sysfs` 文件系统上的每个设备提供一个 `uevent` 文件。通过将 `add` 写入到该文件，内核将再次发送引导时丢失的相同事件。`/sys` 中所有 `uevent` 文件的简单循环将再次触发所有事件来创建设备节点并执行设备设置。

例如，在引导期间出现的 USB 鼠标可能不会在早期引导逻辑中初始化，因为驱动程序在那时不可用。此设备发现的事件丢失并且不能为该设备查找内核模块。不是手动搜索可能连接的设备，`udev` 在根文件系统可用后直接从内核请求所有设备事件，所以 USB 鼠标设备的事件可以再次运行。现在它在装入的根文件系统上找到内核模块，因此可以初始化 USB 鼠标。

在用户空间，设备冷插入序列和运行时期间发现的设备之间没有明显的区别。在这两种情况下，使用相同的规则来匹配并且运行相同的配置程序。

21.5 调试 `udev` 事件

程序 `udevmonitor` 可以用于将驱动程序核心事件和 `udev` 事件处理的计时可视化。

```
UEVENT[1132632714.285362] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UEVENT[1132632714.288166] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UEVENT[1132632714.309485] add@/class/input/input6
UEVENT[1132632714.309511] add@/class/input/input6/mouse2
UEVENT[1132632714.309524] add@/class/usb_device/usbdev2.12
UDEV [1132632714.348966] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2
UDEV [1132632714.420947] add@/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
UDEV [1132632714.427298] add@/class/input/input6
UDEV [1132632714.434223] add@/class/usb_device/usbdev2.12
UDEV [1132632714.439934] add@/class/input/input6/mouse2
```

`UEVENT` 行显示内核已经通过 `netlink` 发送的事件。`UDEV` 行显示已经完成的 `udev` 事件处理程序。计时以微秒为单位显示。`UEVENT` 和 `UDEV` 之间的时间是 `udev` 用于处理此事件或者 `udev` 守护程序延迟执行从而同步此事件与相关以及已运行的事件的时间。例如，硬盘分区的事件总是等待主磁盘设备事件完成，因为分区事件可能依赖主磁盘事件从硬件查询的数据。

`udevmonitor --env` 显示完整的事件环境：

```
UDEV [1132633002.937243] add@/class/input/input7
UDEV_LOG=3
ACTION=add
DEVPATH=/class/input/input7
SUBSYSTEM=input
SEQNUM=1043
PHYSDEVPATH=/devices/pci0000:00/0000:00:1d.1/usb2/2-2/2-2:1.0
PHYSDEVBUS=usb
PHYSDEVDRIVER=usbhid
PRODUCT=3/46d/c03e/2000
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.1-2/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0 0 0 0 0
REL=103
```

`udev` 也将讯息发送给 `syslog`。用于控制将哪些讯息发送到 `syslog` 的默认 `syslog` 优先权在 `udev` 配置文件 `/etc/udev/udev.conf` 中指定。可以使用 `udevcontrol log_priority=level/number` 来更改正在运行的守护程序的日志优先权。

21.6 使用 `udev` 规则影响内核设备事件处理

`udev` 规则可以与内核添加到事件本身的属性或者内核导出到 `sysfs` 的任何信息相匹配。规则还可以从外部程序请求其他信息。根据提供的规则匹配每个事件。所有规则都位于 `/etc/udev/rules.d` 目录下。

规则文件中的每一行至少包含一个关键字值对。有两种类型的关键字，匹配关键字和指派关键字。如果所有匹配关键字与它们的值匹配，则应用此规则并将指派关键字指派给特定的值。匹配规则可以指定设备节点的名称、将符号链接指向该节点或者运行特定程序作为事件处理的一部分。如果找不到匹配的规则，则使用默认设备节点名来创建设备节点。在 `udev` 手册页中描述了规则语法和提供用来匹配或导入数据的关键字。

21.7 永久设备命名

动态设备目录和 `udev` 规则基础结构可以为所有磁盘设备提供固定名称，而不考虑它们的识别顺序或设备使用的连接。内核创建的每个相应的块设备由工具根据有关特定总线、驱动器类型或者文件系统的特殊知识进行检查。除了动态内核提供的设备节点名，`udev` 还保留各种指向该设备的永久符号链接：

```
/dev/disk
|-- by-id
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B -> ../../sda
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part1 -> ../../sda1
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part6 -> ../../sda6
|   |-- scsi-SATA_HTS726060M9AT00_MRH453M4HWHG7B-part7 -> ../../sda7
|   |-- usb-Generic_STORAGE_DEVICE_02773 -> ../../sdd
|   |-- usb-Generic_STORAGE_DEVICE_02773-part1 -> ../../sdd1
|-- by-label
|   |-- Photos -> ../../sdd1
|   |-- SUSE10 -> ../../sda7
|   |-- devel -> ../../sda6
|-- by-path
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0 -> ../../sda
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part1 -> ../../sda1
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part6 -> ../../sda6
|   |-- pci-0000:00:1f.2-scsi-0:0:0:0-part7 -> ../../sda7
|   |-- pci-0000:00:1f.2-scsi-1:0:0:0 -> ../../sr0
|   |-- usb-02773:0:0:2 -> ../../sdd
|   |-- usb-02773:0:0:2-part1 -> ../../sdd1
`-- by-uuid
    |-- 159a47a4-e6e6-40be-a757-a629991479ae -> ../../sda7
    |-- 3e999973-00c9-4917-9442-b7633bd95b9e -> ../../sda6
    |-- 4210-8F8C -> ../../sdd1
```

21.8 已替换的 hotplug 包

先前使用的 `hotplug` 包已经完全替换为 `udev` 和 `udev` 相关的内核基础结构。先前 `hotplug` 基础结构的以下部分已经过时或者功能已经被 `udev` 取代：

```
/etc/hotplug/*.agent
    不再需要或者移动到 /lib/udev

/etc/hotplug/*.rc
    已经替换为 /sys/*/uevent 触发器
```

`/etc/hotplug/blacklist`

替换为 `modprobe.conf` 中的 `blacklist` 选项

`/etc/dev.d/*`

替换为 `udev` 规则 `RUN` 关键字

`/etc/hotplug.d/*`

替换为 `udev` 规则 `RUN` 关键字

`/sbin/hotplug`

替换为侦听 `netlink` 的 `udev`d，仅用在初始 `RAM` 文件系统中，直到根文件系统可以装入后才禁用它

`/dev/*`

替换为动态 `udev` 和 `/lib/udev/devices/*` 中的静态内容

以下文件和目录包含 `udev` 基础结构的关键元素：

`/etc/udev/udev.conf`

主 `udev` 配置文件

`/etc/udev/rules.d/*`

`udev` 事件匹配规则

`/lib/udev/devices/*`

静态 `/dev` 内容

`/lib/udev/*`

从 `udev` 规则调用的帮助程序

21.9 有关详细信息

有关 `udev` 基础结构的更多信息，请参见以下手册页：

`udev`

有关 `udev`、关键字、规则和其他重要配置问题的常规信息。

`udevinfo`

`udevinfo` 可以用于从 `udev` 数据库查询设备信息。

udev

有关 udev 事件管理守护程序的信息。

udevmonitor

udevmonitor 将内核和 udev 事件序列显示给控制台。这个工具主要用于调试。

Linux 中的文件系统

SUSE Linux Enterprise® 随许多不同的文件系统发送，包括 ReiserFS、Ext2、Ext3 和 XFS，安装时可从中选择。每个文件系统都有其自身的优缺点，更适合某种场合的需要。专业高性能安装与和家庭用户的安装需要选择的文件系统可能不同。

22.1 术语

元数据

文件系统 - 确保能正确组织和访问磁盘上所有数据的内部数据结构。从本质上讲，它是“有关数据的数据”。“”几乎每个文件系统都有自己的元数据结构，这也是文件系统为何表现出不同性能特性的部分原因。维护元数据的完整性非常重要，因为如果不这样，则可能无法访问文件系统中的所有数据。

inode

Inode 包含关于文件的各种信息，包括大小、链接数、指向实际储存文件内容的磁盘块的指针以及创建、修改和访问的日期和时间。

日记

在文件系统的上下文中，日记是包含某种日志的磁盘上结构，文件系统将要对本系统中的元数据所做的更改储存在此日志中。日记可以显著缩短 Linux 系统的恢复时间，因为它取消了在系统启动时检查整个文件系统这一冗长的搜索过程。而只是重放日记。

22.2 Linux 中的主要文件系统

与两三年前不同，为 Linux 系统选择文件系统不再是花几秒钟就能完成的操作（选择 Ext2 或 ReiserFS）。从版本 2.4 开始，内核提供了多种供选择的文件系统。下面概述了这些文件系统的基本工作原理以及它们的优点。

您一定要记住一点，即没有任何一个文件系统能适合所有应用环境。每个文件系统都有各自的特定优点和缺点，必须将这些因素考虑在内。但是，即使是最复杂的文件系统也不能替代合理的备份策略。

本章中使用的术语 *数据完整性和数据一致性* 并不是指用户空间数据（您的应用程序写入其文件的数据）的一致性。此数据是否一致必须由应用程序本身控制。

重要: 设置文件系统

除非本章另行声明，否则可以使用 YaST 执行设置或更改分区和文件系统所需的所有步骤。

22.2.1 ReiserFS

作为 2.4 内核版本的正式的重要功能之一，ReiserFS 作为 2.2.x SUSE 的内核补丁提供，因为 V6.4. ReiserFS 是由 Hans Reiser 和 Namesys 开发团队设计的。ReiserFS 已证明它自己是 Ext2 功能强大的替代系统。ReiserFS 的主要优点是更高的磁盘空间利用率、更高的磁盘访问性能以及更快的崩溃恢复速度。

以下内容是对 ReiserFS 优点的详细说明：

更高的磁盘空间利用率

在 ReiserFS 中，采用一种名为 B^{*}-Tree（平衡树）的结构组织所有数据。这种树结构有助于提高磁盘空间的利用率，这是因为可以将小文件直接储存在 B^{*} 树叶节点而不是其他位置，并且只维护一个指向实际磁盘位置的指针。此外，不按照 1 KB 或 4 KB 的大块来分配储存区，而是根据所需的准确大小进行。另一个优点是 inode 的动态分配。这使得此文件系统比传统的文件系统（例如 Ext2）更灵活，而传统文件系统中的 inode 密度必须在创建文件系统时指定。

更高的磁盘访问性能

对于小文件，文件数据和“stat_data”(inode)信息经常被储存在相邻的位置。这样通过一个磁盘 I/O 操作就可以访问它们，这意味着只需访问磁盘一次就可以检索到所有需要的信息。

更快的崩溃恢复速度

使用日记来跟踪最近的元数据更改使对文件系统的检查可以很快完成，即使对大型文件系统也是如此。

通过数据日记确保可靠性

ReiserFS 还支持与 Ext3 一节 [第 22.2.3 节“Ext3”](#) [430] 中介绍过的概念类似的数据日记和有序数据方式。默认方式是 data=ordered，它确保了数据和元数据的完整性，但只对元数据使用日记。

22.2.2 Ext2

Ext2 的起源可以追溯到 Linux 历史的早期。1992 年 4 月推出了 Ext2 的前身 Extended File System（扩展文件系统），并将其集成到 Linux 0.96c 中。扩展文件系统经过多次修改，并（像 Ext2 一样）成为多年来最流行的 Linux 文件系统。但随着日记文件系统的创建以及其恢复时间的大大缩短，Ext2 的重要性逐渐降低。

简要总结 Ext2 的优点有助于您了解为什么它以前是（在某些领域现在仍是）许多 Linux 用户最喜欢使用的 Linux 文件系统。

可靠性

Ext2 确实是一个“老古董”，它经历了许多改进和频繁的测试。“”这可能是人们将其称之为坚如磐石的文件系统的原因。在系统中断后，如果无法彻底卸装文件系统，则 e2fsck 将开始分析文件系统数据。系统使元数据恢复一致的状态，并将挂起的文件或数据块写入指定的目录（名为 lost+found）。与日记文件系统相比，e2fsck 会分析整个文件系统，而不仅仅是最近修改的元数据位。这种操作所花的时间要远远超过检查日记文件系统的日志数据所花的时间。根据文件系统的大小，此过程可能需要半小时或更长时间。因此，对于任何要求高可用性的服务器，不要选择 Ext2。但是，因为 Ext2 不维护日记且使用的内存也少得多，所以其速度常常超过其他文件系统。

可方便地升级

Ext2 的代码是 Ext3 成为广受欢迎的下一代文件系统的坚实基础。它的可靠性和稳定性与日记文件系统的优点完美地结合在一起。

22.2.3 Ext3

Ext3 是由 Stephen Tweedie 设计的。与所有其他下一代文件系统不同，Ext3 并没有采用全新的设计原则。它是在 Ext2 的基础上设计的。这两个文件系统密切相关。可以方便地在 Ext2 文件系统中建立 Ext3 文件系统。Ext2 和 Ext3 最重要的区别是 Ext3 支持日记。总之，Ext3 有三个主要优点：

方便并高度可靠地从 Ext2 升级

因为 Ext3 以 Ext2 代码为基础并且共享 Ext2 的磁盘上格式和元数据格式，所以从 Ext2 升级到 Ext3 非常简单。与转换到其他日记文件系统不同，转换到 Ext3 只需要花几分钟，而转换到其他日记文件系统（如 ReiserFS 或 XFS）会相当繁琐（备份整个文件系统并从头开始重创建文件系统）。这样操作还很安全，因为从头重创建整个文件系统很可能出现问题。考虑到等待升级到日记文件系统的现有 Ext2 系统的数量，就很容易明白为什么 Ext3 对许多系统管理员来说如此重要。从 Ext3 降级到 Ext2 与升级一样简单。只需彻底卸载 Ext3 文件系统，然后作为 Ext2 文件系统重装入即可。

可靠性和性能

某些其他日记文件系统采用“仅元数据”的日记方法。“”这意味着元数据始终保持一致的状态，但无法自动保证文件系统数据本身一致。Ext3 的设计既可以照顾到元数据，又可以照顾到数据。“照顾”的程度可以自定义。在 `data=journal` 方式中启用 Ext3 可以提供最大的安全性（数据完整性），但因为要将元数据和数据都记入日记，所以可能降低系统的速度。一个相对较新的方法是采用 `data=ordered` 方式，这种方式确保了数据和元数据的完整性，但只对元数据使用日记。文件系统驱动程序收集与一次元数据更新对应的所有数据块。这些数据块在更新元数据之前被写入磁盘中。这样，在不牺牲性能的情况下，元数据和数据的一致性得以实现。第三个可以使用的选项是 `data=writeback`，它允许在将某些数据的元数据提交给日记后，将这些数据写入主文件系统。在性能方面，此选项常被认为是最佳选项。但它在维护内部文件系统完整性的同时，允许以前的数据在系统崩溃并恢复后再次出现在文件中。除非指定了其他选项，否则运行 Ext3 时，`data=ordered` 为默认设置。

22.2.4 将 Ext2 文件系统转换为 Ext3

要将 Ext2 文件系统转换为 Ext3，请按如下所示继续：

- 1 通过作为 root 运行 `tune2fs -j` 创建 Ext3 日志。此命令将用默认参数创建 Ext3 日记。

要自己确定日志的大小和所在的设备，请改为运行 `tune2fs -j`，同时带所需的日志选项 `size=` 和 `device=`。可以在 `tune2fs` 程序的 `tune2fs` 手册页中获得关于此程序的更多信息。

- 2 要确保正确地识别 Ext3 文件系统，请作为 root 编辑文件 `/etc/fstab`，将为对应的分区指定的文件系统类型从 `ext2` 更改为 `ext3`。此更改将在下次重引导后生效。
- 3 要引导设置为 Ext3 分区的根文件系统，请将模块 `ext3` 和 `jbd` 包含在 `initrd` 中。要执行此操作，请作为 root 编辑 `/etc/sysconfig/KERNEL`，将 `ext3` 和 `jbd` 添加到 `INITRD_MODULES` 变量。保存更改后，请运行 `mkinitrd` 命令。这将构建一个新的 `initrd`，并准备使用它。

22.2.5 XFS

SGI 在 20 世纪 90 年代初开始开发 XFS，最初计划将 XFS 作为 IRIX OS 的文件系统。开发 XFS 的目的是创建一个高性能的 64 位日记文件系统来满足当今对计算能力的极高要求。XFS 适合操纵大型文件，在高端硬件上表现优异。但即使是 XFS 也有缺点。与 ReiserFS 类似，XFS 非常注重元数据的完整性，但不太注重数据的完整性。

快速回顾 XFS 的关键功能将解释为什么此文件系统被证明是在高端计算方面其他日记文件系统的强大竞争对手。

通过使用分配组实现高伸缩性

在创建 XFS 文件系统时，文件系统底层的块设备被分成 8 个或 8 个以上相同大小的线性区域。这些线性区域被称为分配组。每个分配组管理自己的 inode 和可用空间。实际上，可以将分配组看作文件系统中的文件系统。因为分配组相互独立，所以内核可同时对多个分配组进行寻址。此功能对 XFS 优异的可伸缩性非常关键。独立分配组的概念自然适合多处理器系统的需要。

通过有效管理磁盘空间获得高性能

可用空间和 `inode` 是由分配组内的 B^+ 树处理的。使用 B^+ 树将大大增强 XFS 的性能和可伸缩性。XFS 使用延迟分配。它通过将进程分成两部分来处理分配。将挂起事务储存在 RAM 中并保留适当数量的空间。XFS 仍不决定应储存数据的准确位置（指出文件系统块）。此决定将被延迟到最后的时刻。某些生存期很短的临时数据可能永远不会被储存到磁盘上，这是因为在 XFS 决定保存它们的实际位置时，这些数据可能已经过时了。这样，XFS 增强了写性能，并减少了文件系统碎片的数目。因为延迟分配引起写事件的频率比其他文件系统引起写事件的频率要低，所以如果写操作期间发生系统崩溃，则数据丢失可能会更加严重。

进行预分配以避免文件系统碎片

在将数据写入文件系统前，XFS 保留（预分配）文件所需的可用空间。这样会大大减少文件系统碎片的数目。因为文件的内容不会分散在整个文件系统中，所以性能得以提高。

22.3 其他一些支持的文件系统

表 22.1 “Linux 中的文件系统类型” [432] 对 linux 支持的其他一些文件系统进行了总结。支持这些文件系统主要是为了确保与不同类型的媒体或异操作系统实现兼容和数据交换。

表 22.1 *Linux 中的文件系统类型*

<code>cramfs</code>	压缩的 <i>ROM</i> 文件系统：一种经压缩的只读 <i>ROM</i> 文件系统。
<code>hpfs</code>	高性能文件系统：IBM OS/2 标准文件系统，只在只读方式下支持此文件系统。
<code>iso9660</code>	CD-ROM 上的标准文件系统。
<code>minix</code>	此文件系统源自有关操作系统的学术项目，是在 Linux 中使用的第一个文件系统。目前，它被用作软盘的文件系统。
<code>msdos</code>	<i>fat</i> （最初由 DOS 使用的文件系统）现在已被多种操作系统采用。

ncpfs	通过网络装入 Novell 卷的文件系统。
nfs	网络文件系统：在此文件系统中，可以将数据储存在网络中的任何计算机上，并可以通过网络授予访问权限。
smbfs	Windows 等产品使用服务器讯息块来支持通过网络进行文件访问。
sysv	在 SCO UNIX、Xenix 和 Coherent（用于个人电脑的商用 UNIX 系统）上使用。
ufs	供 BSD、SunOS 和 NeXTSTEP 使用。只在只读方式下支持此文件系统。
umsdos	MSDOS 上的 UNIX：应用于常规 fat 文件系统上，通过创建特殊文件获得 UNIX 功能（权限、链接和长文件名）。
vfat	虚拟 FAT：fat 文件系统的扩展（支持长文件名）。
ntfs	Windows NT 文件系统，只读。

22.4 Linux 中对大型文件的支持

最初，Linux 支持的最大文件大小为 2 GB。在大量使用多媒体之前，只要用户不在 Linux 中操纵大型数据库，这个大小已足够了。但由于服务器计算变得越来越重要，所以当使用一组应用程序必须使用的新接口时，对内核和 C 库进行了修改以支持大小大于 2 GB 的文件。当今，几乎所有的主要文件系统都提供 LFS 支持，从而允许您执行高端计算。[表 22.2“文件系统的最大大小（磁盘上格式）”](#) [433] 概述了 Linux 文件和文件系统的当前限制。

表 22.2 文件系统的最大大小（磁盘上格式）

文件系统	文件大小（字节）	文件系统大小（字节）
Ext2 或 Ext3（1 KB 块大小）	2^{34} (16 GB)	2^{41} (2 TB)
Ext2 或 Ext3（2 KB 块大小）	2^{38} (256 GB)	2^{43} (8 TB)

文件系统	文件大小（字节）	文件系统大小（字节）
Ext2 或 Ext3（4 KB 块大小）	2^{41} (2 TB)	2^{44} -4096（16 TB-4096 字节）
Ext2 或 Ext3（8 KB 块大小） （系统采用 8 KB 的页，与 Alpha 类似）	2^{46} (64 TB)	2^{45} (32 TB)
ReiserFS v3	2^{46} (64 TB)	2^{45} (32 TB)
XFS	2^{63} (8 EB)	2^{63} (8 EB)
NFSv2（客户端）	2^{31} (2 GB)	2^{63} (8 EB)
NFSv3（客户端）	2^{63} (8 EB)	2^{63} (8 EB)

重要: Linux 内核限制

表 22.2 “文件系统的最大大小（磁盘上格式）” [433]介绍了有关磁盘上格式的限制。2.6 内核自身的大小限制同样适用于其处理的文件和文件系统大小。限制如下：

文件大小
在 32 位系统上，文件不能超过 2 TB（ 2^{41} 字节）。

文件系统大小
文件系统最大可以为 2^{73} 字节大小。但是，目前可用的硬件尚不会超出这一限制。

22.5 有关详细信息

上面介绍的每个文件系统项目都有自己的主页，可以在其中找到邮件列表信息、更多文档和常见问题解答。

- <http://e2fsprogs.sourceforge.net/>
- <http://www.zipworld.com.au/~akpm/linux/ext3/>

- http://chichkin_i.zelnet.ru/namesys/
- <http://oss.sgi.com/projects/xfst/>
- <http://oss.oracle.com/projects/ocfs2/>

可以在 *IBM developerWorks* 中找到关于 linux 文件系统的多部分综合性教程，网址为：<http://www-106.ibm.com/developerworks/library/l-fs.html> Wikipedia 项目 http://en.wikipedia.org/wiki/Comparison_of_file_systems#Comparison 中有文件系统的深入比较（不只是 Linux 文件系统）。

X 窗口系统

X 窗口系统 (X11) 是 UNIX 中图形用户界面的实际标准。X 是基于网络的，可以使在一个主机上启动的应用程序显示在通过任何类型的网络（LAN 或 Internet）连接的另一个主机上。本章介绍了 X 窗口系统环境的安装和优化，并提供了关于在 SUSE Linux Enterprise® 中使用字体的背景信息。

23.1 手动配置 X Window 系统

默认设置下，X 窗口系统以第 8.15 节“SaX2”[164]中所述 SaX2 界面配置。或者也可以通过编辑其配置文件手动配置它。

警告：错误的 X 配置可能会损坏您的硬件。

配置 X 窗口系统时要小心。在完成配置前，切勿启动 X 窗口系统。错误配置的系统可能会对您的硬件造成无法修复的损坏（此情况尤其针对于固定频率的监视器）。该书和 SUSE Linux Enterprise 的创建者不对导致的任何损坏负责。这里提供的信息已经仔细斟酌，但不能保证所提供的所有方法均正确且不会对您的硬件造成任何损坏。

命令 `sax2` 会创建 `/etc/X11/xorg.conf` 文件。这是 X 窗口系统的主配置文件。请在此查找与图形卡、鼠标和监视器有关的所有设置。

重要: 使用 X -configure

用 X -configure 配置您的 X 安装（如果之前尝试 SUSE Linux Enterprise 的 **SaX2** 失败）。如果您的安装涉及专用的仅二进制驱动程序，X -configure 不起作用。

下面小节介绍配置文件 `/etc/X11/xorg.conf` 的结构。它由多个部分组成，每个部分处理配置的某个特定方面。每个部分都以关键字 `Section` `<designation>` 开头，以 `EndSection` 结尾。以下惯例适用于所有章节：

```
Section "designation"
    entry 1
    entry 2
    entry n
EndSection
```

表 23.1 “`/etc/X11/xorg.conf` 中的部分” [438]中列出了可用的部分类型。

表 23.1 `/etc/X11/xorg.conf` 中的部分

类型	含义
文件	用于字体和 RGB 颜色表的路径。
ServerFlags	服务器行为的常规切换。
模块	服务器应载入的模块列表。
InputDevice	此部分配置输入设备，例如键盘和特殊输入设备（触摸板、游戏杆等）。此部分的重要参数有 <code>Driver</code> 以及定义 <code>Protocol</code> 和 <code>Device</code> 的选项。对连接到计算机的每个设备，通常都有一个 <code>InputDevice</code> 部分。
监视程序	使用的显示器。此部分的重要元素是标识符（稍后在 <code>Screen</code> 定义中引用）、刷新率 <code>VertRefresh</code> 和同步频率限制（ <code>Horizsync</code> 和 <code>VertRefresh</code> ）。这些设置采用的单位为 <code>MHz</code> 、 <code>kHz</code> 和 <code>Hz</code> 。通常，服务器拒绝不符合监视器规格的任何方式行。这样可防止意外地将过高的频率发送到监视器。

类型	含义
方式	特定屏幕分辨率的方式行参数。可以根据用户给出的值由 SaX2 计算出这些参数，并且通常无需更改这些参数。您可以在此时进行手动干预，例如当要连接固定频率监视器时。HOWTO 文件（位于 <code>/usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO</code> ）提供了各个数字值含义的细节（在 <code>howtoenh</code> 包中提供）。
设备	特定的图形卡。系统通过其描述性名称来引用图形卡。
屏幕	将 Monitor 和 Device 放在一起以组成 X.Org 的所有必要设置。在 Display 子部分中，指定虚拟屏幕 (Virtual) 的大小、ViewPort 以及此屏幕所用的 Modes。
ServerLayout	单个或多头配置的布局。此部分将输入设备 InputDevice 和显示设备 Screen 绑定在一起。
DRI	提供 Direct Rendering Infrastructure (DRI) 的信息。

下面详细介绍 Monitor、Device 和 Screen。X.Org 和 `xorg.conf` 的手册页提供了有关其他部分的详细信息。

`xorg.conf` 中可以存在多个不同的 Monitor 和 Device 部分。甚至可以存在多个 Screen 部分。ServerLayout 部分确定使用其中哪个部分。

23.1.1 Screen 部分

Screen 部分将 Monitor 部分与 Device 部分结合起来并确定要使用的分辨率和颜色深度。Screen 部分与 [例 23.1 “文件 `/etc/X11/xorg.conf` 的 Screen 部分” \[440\]](#) 类似。

例 23.1 文件 `/etc/X11/xorg.conf` 的 `Screen` 部分

```
Section "Screen"❶
    DefaultDepth 16❷
    SubSection "Display"❸
        Depth 16❹
        Modes "1152x864" "1024x768" "800x600"❺
        Virtual 1152x864❻
    EndSubSection
    SubSection "Display"
        Depth 24
        Modes "1280x1024"
    EndSubSection
    SubSection "Display"
        Depth 32
        Modes "640x480"
    EndSubSection
    SubSection "Display"
        Depth 8
        Modes "1280x1024"
    EndSubSection
    Device "Device[0]"
    Identifier "Screen[0]"❼
    Monitor "Monitor[0]"
EndSection
```

- ❶ Section 确定该部分的类型，在本示例中是 `Screen`。
- ❷ `DefaultDepth` 决定默认使用的颜色深度（除非明确指定其他颜色深度）。
- ❸ 对每种颜色深度指定不同的 `Display` 子部分。
- ❹ `Depth` 决定对本组 `Display` 设置使用的颜色深度。可用值有 8、15、16、24 和 32，尽管并非所有 X 服务器模块或分辨率都可以支持所有这些值。
- ❺ `Modes` 部分由可能的屏幕分辨率列表组成。X 服务器从左到右检查此列表。对于每个分辨率，X 服务器均会在 `Modes` 部分中搜索合适的 `Modeline`。`Modeline` 取决于监视器和图形卡的功能。`Monitor` 设置确定最终的 `Modeline`。

找到的第一个分辨率是 `Default mode`。使用 `Ctrl+Alt++`（在数字小键盘上）向右切换到列表中的下一个分辨率。使用 `Ctrl+Alt+-`（在数字小键盘上）切换到上一个。这使您能够在 X 运行时改动分辨率。

- ❻ 包含 `Depth 16` 的 `Display` 子部分的最后一行指出了虚拟屏幕的大小。虚拟屏幕的最大可能大小取决于图形卡中安装的内存量和所需的颜色深度，而不取决于监视器的最大分辨率。如果忽略此行，虚拟分辨率就是物理分

分辨率。因为目前的图形卡都具有大量视频内存，所以您可以创建非常大的虚拟桌面。但是，如果您将大部分视频内存用于虚拟桌面，则可能不能再使用 3D 功能。例如，如果图形卡有 16 MB 视频 RAM，则当采用 8 位颜色深度时，虚拟屏幕最多可以有 4096x4096 个像素。但建议不要将所有内存用于虚拟屏幕，因为图形卡的内存还要用于多种字体和图形超速缓存，对于加速卡而言尤其如此。

- ⑦ 行 Identifier (这里是 Screen[0]) 为此部分指定一个定义的名称，在随后的 ServerLayout 部分中可以使用此名称唯一引用这个部分。行 Device 和 Monitor 指定属于此定义的图形卡和监视器。这些行仅仅是通过 Device 和 Monitor 部分的相应名称或标识符指向这些部分的链接。下面详细讨论这些部分。

23.1.2 Device 部分

Device 部分描述特定的图形卡。您可以在 xorg.conf 中包含任意多个设备项，前提是要使用关键字 Identifier 对这些项的名称进行区分。如果您安装了多个图形卡，通常按顺序对这些部分进行编号。第一个设备称为 Device[0]，第二个设备称为 Device[1]，依此类推。以下文件是从安装有 Matrox Millennium PCI 图形卡（由 SaX2 配置）的计算机的 Device 部分摘出的一段：

```
Section "Device"
    BoardName      "MGA2064W"
    BusID          "0:19:0"❶
    Driver         "mga"❷
    Identifier      "Device[0]"
    VendorName     "Matrox"
    Option         "sw_cursor"
EndSection
```

- ❶ BusID 是指安装图形卡的 PCI 或 AGP 插槽。它与使用命令 lspci 显示的 ID 相匹配。X 服务器需要采用十进制形式的详细信息，但 lspci 以十六进制形式显示这些信息。BusID 的值由 SaX2 自动检测。
- ❷ Driver 的值由 SaX2 自动设置，指定哪个驱动程序用于您的图形卡。如果此卡是 Matrox Millennium，则将驱动程序模块称为 mga。然后，X 服务器通过 drivers 子目录的 Files 部分中定义的 ModulePath 进行搜索。在标准安装中，是 /usr/X11R6/lib/modules/drivers 或 /usr/X11R6/lib64/modules/drivers 目录。然后将 _drv.o 添加到名称中。因此，对于 mga 驱动程序，将装载驱动程序文件 mga_drv.o。

还可以通过其他选项影响 X 服务器或驱动程序的行为。在 Device 部分中设置的选项 `sw_cursor` 就是这方面的一个示例。此选项取消激活硬件鼠标光标并使用软件显示鼠标光标。根据驱动程序模块，有不同的选项可用，它们位于目录 `/usr/share/doc/package_name` 中驱动程序模块的说明文件中。通常还可以在手册页（`man xorg.conf`、`man X.Org` 和 `man 4 chips`）中查看有效的选项。

如果图形卡有多个视频连接器，可以将这一个卡的不同设备配置为单一视图。使用 `SaX2` 以这种方式对图形接口进行设置。

23.1.3 Monitor 部分和 Modes 部分

与 Device 部分类似，Monitor 和 Modes 部分分别描述一个监视器。配置文件 `/etc/X11/xorg.conf` 可以包含任意多个 Monitor 部分。每个 Monitor 部分使用行 `UseModes`（如果可用）引用一个 Modes 部分。如果没有 Modes 部分可用于 Monitor 部分，X 服务器将根据常规同步值计算相应值。服务器布局部分指定相关的 Monitor 部分。

只有有经验的用户才可以设置监视器定义。`modeline` 是 Monitor 部分的重要组成部分。方式行设置相应分辨率的水平定时和垂直定时。Monitor 部分储存有监视器属性（特别是所允许的频率）。

警告

除非您对监视器和图形卡功能有深入了解，否则建议不要更改 `modelien`，因为这可能严重损坏监视器。

尝试过开发自己的监视器说明的人应对 `/usr/X11R6/lib/X11/doc/` 中的文档非常熟悉（必须安装 `xorg-x11-doc` 包）。

现在，很少需要手动指定方式行。如果您使用的是最新的多频同步监视器，则通常由 X 服务器通过 DDC 直接从监视器中读取允许的频率和最佳分辨率，如 `SaX2` 配置一节所述。如果由于某种原因无法执行此操作，请使用 X 服务器中包含的 VESA 方式之一。这种方式可用于几乎所有图形卡和监视器的组合。

23.2 安装和配置字体

在 SUSE Linux Enterprise 中安装附加字体非常简单。只需要将字体复制到位于 X11 字体路径中的任何目录即可（请参阅第 23.2.1 节“X11 核心字体”[444]）。安装目录应是 /etc/fonts/fonts.conf 中配置的目录的子目录（请参见第 23.2.2 节“Xft”[445]），或用 /etc/fonts/suse-font-dirs.conf 包含到此文件中。

以下是 /etc/fonts/suse-font-dirs.conf 中的摘录。因为此文件被链接到目录 /etc/fonts/conf.d（由 /etc/fonts/fonts.conf 包含），所以它包含在该配置中。在此目录中，以两位数字开头的所有文件或符号链接均由 fontconfig 装载。有关此功能的更详细说明，请参见 /etc/fonts/conf.d/README。

```
<!-- Font directory list -->
<dir>/usr/share/fonts</dir>
<dir>/usr/X11R6/lib/X11/fonts</dir>
<dir>/opt/kde3/share/fonts</dir>
<dir>/usr/local/share/fonts</dir>
<dir>~/ .fonts</dir>
<dir>~/ .fonts/kde-override</dir>
<include ignore_missing="yes">suse-font-dirs.conf</include>
```

/etc/fonts/suse-font-dirs.conf 会自动生成，以引入随（多为第三方）应用程序附送的字体，如 OpenOffice.org、Java 或 Adobe Acrobat Reader。/etc/fonts/suse-font-dirs.conf 的典型条目外观如下：

```
<dir>/usr/lib/ooo-2.0/share/fonts</dir>
<dir>/usr/lib/ooo-2.0/share/fonts/truetype</dir>
<dir>/usr/lib/jvm/java-1.5.0-sun-1.5.0_update10/jre/lib/fonts</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font</dir>
<dir>/usr/X11R6/lib/Acrobat7/Resource/Font/PFM</dir>
```

要在整个系统安装其他字体，请手动将字体文件复制至适当的目录（如 root），例如 /usr/share/fonts/truetype。或者，可以使用 KDE 控制中心中的 KDE 字体安装程序来执行此任务。结果是一样的。

您还可以创建符号链接，而不复制实际字体。例如，如果已装入的 Windows 分区上的字体已获得许可并要使用，则可能要执行此操作。随后，运行 `SuSEconfig --module fonts`。

`SuSEconfig --module fonts` 执行脚本 `/usr/sbin/fonts-config`，该脚本处理字体的配置。有关此脚本的更多信息，请参阅其手册页 (`man fonts-config`)。

上面的过程同样适用于位图字体、TrueType 和 OpenType 字体以及 Type1 (PostScript) 字体。可以将所有这些字体类型安装在任何目录中。

X.Org 包含两个完全不同的字体系统：旧的 *X11* 核心字体系统和新设计的 *Xft* 及 *fontconfig* 系统。下面几节简要介绍这两种系统。

23.2.1 X11 核心字体

目前，X11 核心字体系统不仅支持位图字体，还支持可缩放字体（例如 Type1 字体）、TrueType 以及 OpenType 字体。X11 核心字体系统只在没有反锯齿处理和子像素显示的情况下支持可缩放字体，并且装载许多语言具有字形的大型可缩放字体可能需要较长的时间。也支持 Unicode 字体，但使用它们的速度比较慢，而且需要更多内存。

X11 核心字体系统带有一些固有缺陷。它已经过时，而且不再能以有意义的方式扩展。虽然为了实现向后兼容而不得不保留 X11 核心字体系统，但应尽可能使用更先进的 Xft 和 fontconfig 系统。

为了执行相应的操作，X 服务器需要知道它可使用的字体以及在系统中的哪些位置可找到这些字体。这由 `FontPath` 变量来处理，该变量包含所有有效系统字体目录的路径。在其中每个目录中，一个名为 `fonts.dir` 的文件会列出此目录中的可用字体。`FontPath` 由 X 服务器在启动时生成。它将在配置文件 `/etc/X11/xorg.conf` 的每个 `FontPath` 项中搜索有效的 `fonts.dir` 文件。这些项位于 `Files` 部分。使用 `xset q` 可显示实际的 `FontPath`。运行时也可以使用 `xset` 更改该路径。要添加其他路径，请使用 `xset+fp <path>`。要去除不需要的路径，请使用 `xset-fp <path>`。

如果 X 服务器已经处于活动状态，则可以使用命令 `xsetfp rehash` 使装入的目录中新安装的字体可用。通过 `SuSEconfig--module fonts` 执行此命令。因为命令 `xset` 需要访问正在运行的 X 服务器，所以只有当从可以访问正在运行的 X 服务器的 shell 启动 `SuSEconfig--module fonts` 时，此命令才能发挥作用。实现此操作最简单的方法是通过输入 `su` 和 `root` 密码获得 `root` 权限。`su` 会将启动 X 服务器的用户的访问权限转移到 `root` 外壳。要检查是否正确安装了字体以及是否可以通过 X11 核心字体系统使用字体，请使用命令 `xlsfonts` 列出所有可用字体。

默认情况下，SUSE Linux Enterprise 使用 UTF-8 区域设置。因此，应首选 Unicode 字体（xlsfonts 输出中以 iso10646-1 结尾的字体名称）。可以使用 `xlsfonts | grep iso10646-1` 列出所有可用的 Unicode 字体。几乎所有在 SUSE Linux Enterprise 中可用的 unicode 字体都至少包括欧洲语言所需的字形（以前编码为 iso-8859-*）。

23.2.2 Xft

从一开始，Xft 的编程人员就确保该系统可以很好地支持可缩放字体（包括反锯齿处理）。如果使用 Xft，则是由使用字体的应用程序显示字体，而不是像 X11 核心字体系统中由 X 服务器显示字体。采用这种方式，相应的应用程序能够访问实际字体文件并完全控制如何显示字形。这就为正确显示多种语言的文本奠定了基础。直接访问字体文件对于用于打印的嵌入字体非常有用，因为这样可以确保打印输出与屏幕输出看上去完全一样。

在 SUSE Linux Enterprise 中，两个桌面环境 KDE 和 GNOME、Mozilla 和许多其他应用程序均已默认使用 Xft。使用 Xft 的应用程序在数目上已经超过了使用以前的 X11 核心字体系统的应用程序。

Xft 使用 fontconfig 库来查找字体并影响字体的显示方式。fontconfig 的属性由全局配置文件 `/etc/fonts/fonts.conf` 和用户特定的配置文件 `~/.fonts.conf` 控制。所有这些 fontconfig 配置文件的开头必须是

```
<?xml version="1.0"?>
<!DOCTYPE fontconfig SYSTEM "fonts.dtd">
<fontconfig>
```

并且结尾必须是

```
</fontconfig>
```

要添加用于搜索字体的目录，请追加类似下面内容的一行：

```
<dir>/usr/local/share/fonts/</dir>
```

但通常没有必要这样做。默认情况下，已经在 `/etc/fonts/fonts.conf` 中输入了用户特定的目录 `~/.fonts`。因此，要安装附加字体，只需将它们复制到 `~/.fonts` 即可。

您还可以插入用来确定字体外观的规则。例如，输入

```
<match target="font">
```

```

<edit name="antialias" mode="assign">
  <bool>false</bool>
</edit>
</match>

```

来禁用所有字体的反锯齿处理，或输入

```

<match target="font">
  <test name="family">
    <string>Luxi Mono</string>
    <string>Luxi Sans</string>
  </test>
  <edit name="antialias" mode="assign">
    <bool>false</bool>
  </edit>
</match>

```

来禁用特定字体的反锯齿处理。

默认情况下，大多数应用程序使用字体名称 `sans-serif`（或等效的 `sans`）、`serif` 或 `monospace`。它们不是真正的字体，而只是可解析为合适的字体（取决于语言设置）的别名。

用户可以方便地将规则添加到 `~/.fonts.conf` 中，以将这些别名解析为他们喜欢的字体：

```

<alias>
  <family>sans-serif</family>
  <prefer>
    <family>FreeSans</family>
  </prefer>
</alias>
<alias>
  <family>serif</family>
  <prefer>
    <family>FreeSerif</family>
  </prefer>
</alias>
<alias>
  <family>monospace</family>
  <prefer>
    <family>FreeMono</family>
  </prefer>
</alias>

```

因为几乎所有应用程序都默认使用这些别名，所以这几乎影响到整个系统。这样，您可以方便地在几乎所有位置都使用自己喜欢的字体，而无需在各个应用程序中修改字体设置。

使用 `fc-list` 命令可以查看已安装了哪些字体以及哪些字体可用。例如，命令 `fc-list` 返回所有字体的列表。要查看可用的可缩放字体 (`:scalable=true`) 中有哪些包含希伯来语 (`:lang=he`) 所需的所有字形、它们的字体名称 (`family`)、字型 (`style`)、粗细 (`weight`) 以及包含这些字体的文件的名称，请输入以下命令：

```
fc-list ":lang=he:scalable=true" family style weight
```

此命令的输出类似于下面：

```
FreeSansBold.ttf: FreeSans:style=Bold:weight=200
FreeMonoBoldOblique.ttf: FreeMono:style=BoldOblique:weight=200
FreeSerif.ttf: FreeSerif:style=Medium:weight=80
FreeSerifBoldItalic.ttf: FreeSerif:style=BoldItalic:weight=200
FreeSansOblique.ttf: FreeSans:style=Oblique:weight=80
FreeSerifItalic.ttf: FreeSerif:style=Italic:weight=80
FreeMonoOblique.ttf: FreeMono:style=Oblique:weight=80
FreeMono.ttf: FreeMono:style=Medium:weight=80
FreeSans.ttf: FreeSans:style=Medium:weight=80
FreeSerifBold.ttf: FreeSerif:style=Bold:weight=200
FreeSansBoldOblique.ttf: FreeSans:style=BoldOblique:weight=200
FreeMonoBold.ttf: FreeMono:style=Bold:weight=200
```

可以使用 `fc-list` 查询的重要参数包括：

表 23.2 *fc-list* 的参数

参数	含义和可能值
family	字体系列的名称，如 FreeSans。
foundry	字体的制造商，如 urw。
style	字型，如 Medium、Regular、Bold、Italic 或 Heavy。
lang	字体支持的语言，例如 de 表示德语，ja 表示日语，zh-TW 表示繁体中文，zh-CN 表示简体中文。
weight	字体粗细，例如 80 表示常规粗细，200 表示粗体。
slant	倾斜，通常 0 表示不倾斜，100 表示斜体。
文件	包含字体的文件的名称。

参数	含义和可能值
outline	true 表示外框字体，false 表示其他字体。
scalable	true 表示可缩放字体，false 表示其他字体。
bitmap	true 表示位图字体，false 表示其他字体。
pixelsize	以像素为单位表示的字体大小。与 <code>fc-list</code> 一起使用时，此选项仅对位图字体有意义。

23.3 更多信息

安装包 `xorg-x11-doc` 和 `howtoenh` 以获得关于 X11 的详细信息。有关 X11 开发的更多信息，请参见该项目的主页：<http://www.x.org>。

通过 PAM 进行鉴定

Linux 在鉴定进程中使用 PAM（可插拔鉴定模块）作为用户和应用程序之间的中间层。PAM 模块在系统范围内可用，所以任何应用程序都可以请求这些模块。本章介绍模块化鉴定机制的工作原理和配置方法。

系统管理员和编程人员经常要将访问限制在系统的某些部分或限制对应用程序某些功能的使用。如果不使用 PAM，则每次引入新的鉴定机制（例如 LDAP、Samba 或 Kerberos）时都必须对应用程序进行调整。但是，此过程相当耗费时间并且容易出现错误。避免这些缺点的一种方法是将应用程序从鉴定机制中分开并将鉴定委托给集中管理的模块。当需要使用最近所需的鉴定方案时，只要调整或编写合适的 PAM 模块供相关程序使用即可。

依赖于 PAM 机制的每个程序在目录 `/etc/pam.d/programname` 中都有自己的配置文件。这些文件定义用于鉴定的 PAM 模块。另外，`/etc/security` 下有用于 PAM 模块的全局配置文件，这些文件定义这些模块的精确行为（例如 `pam_env.conf`、`pam_pwcheck.conf`、`pam_unix2.conf` 和 `time.conf`）。使用 PAM 模块的每个应用程序实际上调用一组 PAM 函数，这些函数随后将处理不同配置文件中的信息并将结果返回到调用这些函数的应用程序。

24.1 PAM 配置文件的结构

PAM 配置文件中的每一行最多包含 4 列：

```
<Type of module> <Control flag> <Module path> <Options>
```

PAM模块是成批处理的。不同类型的模块具有不同的用途。例如一个模块检查密码，另一个模块校验访问系统的位置，第三个模块读取用户特定的设置。PAM 可以识别四种不同类型的模块：

`auth`

这种类型的模块的用途是检查用户的真实性。传统上，这是通过查询密码完成的，但也可以借助芯片卡或通过生物测定学（指纹或虹膜扫描）实现。

帐户

这种类型的模块检查用户是否具有使用所请求服务的一般权限。例如，应执行这种检查以确保任何人都不能使用失效帐户的用户名进行登录。

`password`

这种类型的模块的用途是启用鉴定令牌的更改。在大多数情况下，这是密码。

会话

这种类型的模块负责管理和配置用户会话。在鉴定前后启动这些模块以在系统日志中注册登录尝试并配置用户的特定环境（邮件帐户、用户主目录、系统限制等）。

第二列包含的控制标志影响所启动模块的行为：

`required`

在进行鉴定之前，必须先成功处理带有此标志的模块。在处理带有 `required` 标志的模块失败后，将继续处理带有相同标志的所有其他模块，之后用户才会收到有关鉴定尝试失败的讯息。

`requisite`

也必须成功处理带有此标志的模块，处理方式在很大程度上与带有 `required` 标志的模块类似。但是，如果某个带有此标志的模块失败，将立即向用户提供反馈并且不再继续处理其他模块。如果成功，则将处理随后的模块，就像带有 `required` 标志的任何模块一样。`requisite` 标志可用于基本过滤器，该过滤器检查进行正确鉴定所必需的某些条件是否存在。

`sufficient`

在成功处理带有此标志的模块后，发出调用的应用程序立即收到处理成功的讯息并且不再处理其他模块，但前提是前面没有带有 `required` 标志的模块失败。带有 `sufficient` 标志的模块失败没有任何直接后果，所有随后的模块都将按其各自的顺序进行处理。

optional

带有此标志的模块成功或失败不会产生任何直接后果。此标志可用于只用来显示讯息（例如，通知用户收到了邮件）而不采取任何进一步操作的模块。

包含

如果给出此标志，则在此处插入指定为参数的文件。

只要模块位于默认目录 `/lib/security`（对于 SUSE Linux Enterprise® 支持的所有 64 位平台，默认目录是 `/lib64/security`）中，就无需显式指定模块路径。第四列可能包含给定模块的选项，例如 `debug`（启用调试）或 `nullok`（允许使用空密码）。

24.2 sshd 的 PAM 配置

为了说明 PAM 背后的工作原理，让我们看一下 `sshd` 的 PAM 配置这一实际示例：

例 24.1 `sshd` 的 PAM 配置

```
##PAM-1.0
auth      include      common-auth
auth      required      pam_nologin.so
account   include      common-account
password  include      common-password
session   include      common-session
# Enable the following line to get resmgr support for
# ssh sessions (see /usr/share/doc/packages/resmgr/README.SuSE)
#session  optional      pam_resmgr.so fake_ttyname
```

应用程序（在本例中是 `sshd`）的典型 PAM 配置包含 4 个 `include` 语句，引用 4 种模块类型的配置文件：`common-auth`、`common-account`、`common-password` 和 `common-session`。这 4 个文件包含每种模块类型的默认配置。通过将它们包含在内而不是单独为每个 PAM 应用程序调用各个模块，在管理员更改默认值时可自动更新 PAM 配置。以前，在 PAM 发生更改或安装新应用程序时，必须手动调整所有应用程序的所有配置文件。而现在 PAM 配置是通过中央配置文件进行的，每个服务的 PAM 配置都将自动继承所有的更改。

第一个包括文件(`common-auth`)调用 `auth` 类型的两个模块：`pam_env` 和 `pam_unix2`。请参见例 24.2 “`auth` 部分的默认配置” [452]。

例 24.2 *auth* 部分的默认配置

```
auth    required    pam_env.so
auth    required    pam_unix2.so
```

第一个模块 `pam_env` 装载文件 `/etc/security/pam_env.conf` 以按照此文件中指定的内容设置环境变量。这可以用于将 `DISPLAY` 变量设置为正确的值，原因是 `pam_env` 模块知道进行登录的位置。第二个模块 `pam_unix2` 根据 `/etc/passwd` 和 `/etc/shadow` 检查用户的登录名和密码。

在成功调用 `common-auth` 中指定的模块后，第三个模块 `pam_nologin` 将检查文件 `/etc/nologin` 是否存在。如果存在，则只有 `root` 用户方可登录。在 `sshd` 得到登录是否成功的任何反馈之前，整批 `auth` 模块都将完成处理。假设这批模块中的所有模块都带有 `required` 控制标志，则必须先成功处理所有这些模块，在此之后 `sshd` 才能收到有关处理成功的讯息。如果其中的某个模块不成功，则仍将继续处理整批模块，在此之后 `sshd` 才能得到处理失败的通知。

成功处理了 `auth` 类型的所有模块后，将立即处理另一个 `include` 语句（在本例中即例 24.3 “*account* 部分的默认配置” [452] 中的语句）。`common-account` 只包含 `pam_unix2` 一个模块。如果 `pam_unix2` 返回的结果证明用户存在，则 `sshd` 会收到一条处理成功的消息，然后处理下一批模块 (`password`)，如例 24.4 “*password* 部分的默认配置” [452] 中所示。

例 24.3 *account* 部分的默认配置

```
account required    pam_unix2.so
```

例 24.4 *password* 部分的默认配置

```
password required    pam_pwcheck.so    nullok
password required    pam_unix2.so      nullok use_first_pass use_authtok
#password required    pam_make.so      /var/yp
```

此外，`sshd` 的 PAM 配置只涉及一条引用 `password` 模块的默认配置的 `include` 语句，这些模块位于 `common-password` 中。当应用程序请求鉴定令牌的更改时，必须成功完成这些模块（控制标志 `required`）。更改密码或另一个鉴定令牌需要进行安全检查。使用 `pam_pwcheck` 模块可完成此操作。随后使用的 `pam_unix2` 模块存有来自 `pam_pwcheck` 的任何旧密码和新密码，因此用户无需再次鉴定。该模块还确保不能绕过 `pam_pwcheck` 所执行的检查。只要前面的 `account` 或 `auth` 类型的模块被配置为指出失效的密码，就应该使用 `password` 类型的模块。

例 24.5 session 部分的默认配置

```
session required      pam_limits.so
session required      pam_unix2.so
session optional      pam_umask.so
```

最后，调用 `session` 类型的模块（捆绑在 `common-session` 文件中）以根据相关用户的设置来配置会话。虽然再次处理 `pam_unix2`，但由于在该模块的相应配置文件 `pam_unix2.conf` 中指定了 `none` 选项，所以没有实际后果。`pam_limits` 模块装载文件 `/etc/security/limits.conf`，该文件定义对某些系统资源使用的限制。当用户注销时，将再次调用 `session` 模块。

24.3 PAM 模块的配置

某些 PAM 模块是可配置的。对应的配置文件位于 `/etc/security` 中。本节简要介绍与 `sshd` 示例相关的一些配置文件 - `pam_unix2.conf`、`pam_env.conf`、`pam_pwcheck.conf` 和 `limits.conf`。

24.3.1 pam_unix2.conf

传统的基于密码的鉴定方法是由 PAM 模块 `pam_unix2` 控制的。它可以从 `/etc/passwd`、`/etc/shadow`、NIS 映射、NIS+ 表或 LDAP 数据库中读取必要的数据库。通过配置各个应用程序自己的 PAM 选项或通过编辑 `/etc/security/pam_unix2.conf` 进行全局配置可以影响此模块的行为。中说明了该模块一个非常基本的配置文件。例 24.6 “`pam_unix2.conf`” [453]

例 24.6 pam_unix2.conf

```
auth:      nullok
account:
password:      nullok
session:      none
```

用于模块类型 `auth` 和 `password` 的 `nullok` 选项指定允许相应类型的帐户使用空密码。允许用户更改他们帐户的密码。`session` 类型的模块的 `none` 选项指定不为它记录任何讯息（这是默认设置）。通过文件本身中的注释和 `pam_unix2(8)` 的手册页可以了解其他配置选项。

24.3.2 pam_env.conf

此文件可用于定义调用 `pam_env` 模块时为用户设置的标准化环境。它允许您使用以下语法预设环境变量：

```
VARIABLE [DEFAULT=[value]] [OVERRIDE=[value]]
```

`VARIABLE`

要设置的环境变量的名称。

```
[DEFAULT=[value]]
```

设置的管理员所需的默认值。

```
[OVERRIDE=[value]]
```

可能由 `pam_env` 查询并设置的值，覆盖默认值。

有关 `pam_env` 如何使用的典型示例就是 `DISPLAY` 变量的调整，在发生远程登录是该变量会改变。中显示了这一工具。例 24.7 “`pam_env.conf`” [454]

例 24.7 `pam_env.conf`

```
REMOTEHOST      DEFAULT=localhost OVERRIDE=@{PAM_RHOST}
DISPLAY         DEFAULT=${REMOTEHOST}:0.0 OVERRIDE=${DISPLAY}
```

第一行将 `REMOTEHOST` 变量的值设置为 `localhost`，当 `pam_env` 不能确定任何其他值时就会使用该值。`DISPLAY` 变量又包含 `REMOTEHOST` 的值。文件 `/etc/security/pam_env.conf` 中的注释提供了详细信息。

24.3.3 pam_pwcheck.conf

此配置文件用于 `pam_pwcheck` 模块，该模块为所有 `password` 类型的模块读取此文件中的选项。储存在此文件中的设置优先于单个应用程序的 PAM 设置。如果尚未定义应用程序特定的设置，则应用程序使用全局设置。例 24.8 “`pam_pwcheck.conf`” [454] 指示 `pam_pwcheck` 允许使用空密码和修改密码。文件 `/etc/security/pam_pwcheck.conf` 中介绍了模块的更多选项。

例 24.8 `pam_pwcheck.conf`

```
password:      nullok
```

24.3.4 limits.conf

可以在文件 `limits.conf` 中以用户或组为基础设置的系统限制，该文件由 `pam_limits` 模块读取。该文件允许您设置硬限制（根本不能超出的限制）和软限制（可以临时超出的限制）。要了解语法和可用选项，请阅读文件中包含的注释。

24.4 有关详细信息

在已安装系统的 `/usr/share/doc/packages/pam` 目录中，可以找到以下附加文档：

README 文件

在此目录的最高一级，存有一些常规 README 文件。子目录 `modules` 保存有关可用 PAM 模块的 README 文件。

Linux-PAM 系统管理员指南

此文档包括系统管理员应该了解的有关 PAM 的所有内容。它讨论了一系列主题，从配置文件的语法到 PAM 的安全特性。此文档以 PDF 文件、HTML 格式和纯文本格式提供。

Linux-PAM 模块编写人员手册

此文档从开发人员的角度对多个主题进行了总结，提供了有关如何编写符合标准的 PAM 模块的信息。此文档以 PDF 文件、HTML 格式和纯文本格式提供。

Linux-PAM 应用程序开发人员指南

此文档包括要使用 PAM 库的应用程序开发人员所需的所有内容。此文档以 PDF 文件、HTML 格式和纯文本格式提供。

Thorsten Kukuk 开发了许多 PAM 模块并提供了有关这些模块的信息，网址为：
<http://www.suse.de/~kukuk/pam/>。

Linux 中的移动计算

移动计算主要与便携式计算机、PDA、手提电话以及它们之间的数据交换关联。移动硬件部件（如外部硬盘、闪存盘或数码相机）可连接到便携式计算机或台式机。移动计算方案中涉及了许多软件组件，一些应用程序是专门为移动定制的。

25.1 便携式计算机

便携式计算机的硬件不同于普通台式机的硬件。这是因为交换能力、占用空间和能耗能之类的标准都是要考虑的属性。移动硬件制造商已经开发了 PCMCIA（个人计算机存储卡国际协会）标准。该标准涉及存储卡、网络接口卡、ISDN 卡和调制解调器卡以及外部硬盘等多个硬件。在 Linux 中如何实现对上述硬件的支持、配置期间需要考虑哪些事项、哪些软件可用于控制 PCMCIA，以及如何对可能的问题查错，这些内容均在 [第 26 章 PCMCIA](#) [467] 中进行了说明。

25.1.1 省电

由于在制造便携式计算机时加入了能量优化系统部件，这使得不必连接电源线即可使用便携式计算机。这些部件在省电方面所起的作用并不亚于操作系统。SUSE Linux Enterprise® 支持各种影响便携式计算机能耗的方法，在使用电池供电时，这些方法对计算机运行时间的影响各不相同。下面的列表按照省电方面作用从大到小排列：

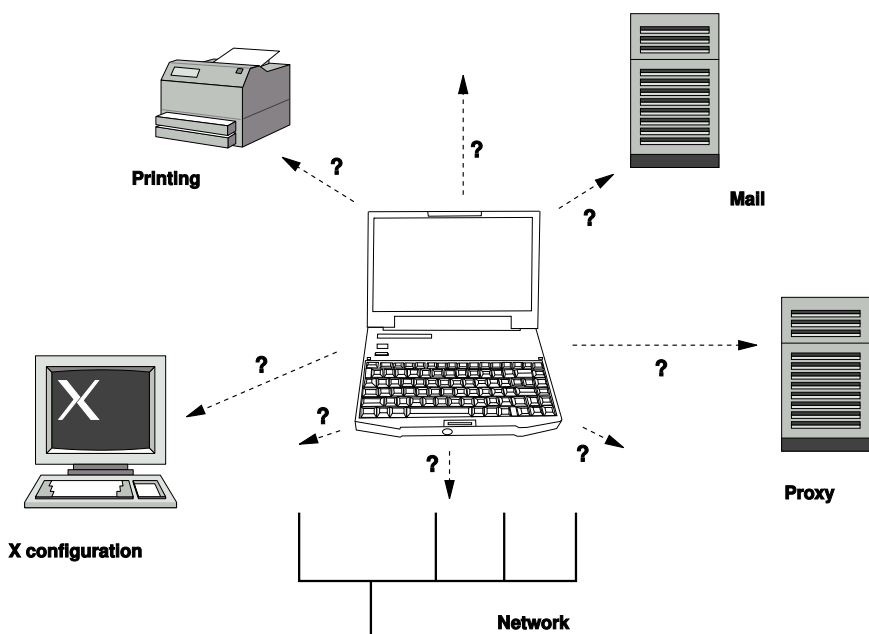
- 节制 CPU 流速
- 在暂停期间关闭显示器
- 手动调节显示器亮度
- 断开不使用的支持热插拔的附件（USB CD-ROM、外部鼠标、不使用的 PCMCIA 卡等）
- 在硬盘闲置时降低其转速

有关 SUSE Linux Enterprise 中的电源管理以及运行 YaST 电源管理模块的详细背景信息，请参见[第 28 章 电源管理](#) [489]。

25.1.2 在变化的操作环境中集成

在用于移动计算时，您的系统需要适应变化的操作环境。很多服务都依赖环境而且必须重配置底层客户端。SUSE Linux Enterprise 会为您处理该任务。

图 25.1 在网络中集成便携式计算机



对于在小型家庭网络和办公网络之间往来通讯的便携式计算机，受影响的服务包括：

网络

这包括 IP 地址分配、域名解析、因特网连接以及与其他网络的连接。

打印

必须存在可用打印机的当前数据库和可用的打印服务器（具体取决于网络）。

电子邮件和代理

就像在打印中那样，当前必须存在一组相应的服务器。

X

如果您的便携式计算机暂时连接到投影机或外部监视器，则需要有其他显示配置。

SUSE Linux Enterprise 提供了几种方法可将便携式计算机集成到现有的操作环境中：

SCPM

SCPM（系统配置配置文件管理）允许将系统的任意配置状态储存为一种称为“配置文件”的快照。可以为不同的情况创建配置文件。在变化的环境（家庭网络、办公网络）中操作系统时，这些配置文件十分有用。可以随时在配置文件间切换。有关 SCPM 的详细信息，请参见第 27 章 [系统配置配置文件管理](#) [475]。可以在 KDE 中使用 Kicker 小程序 Profile Chooser 在配置文件之间切换。该应用程序要求在切换之前提供 root 密码。

NetworkManager

NetworkManager是为便携式计算机上的移动网络连接特别设计的。它能够简单而自动地在各种网络环境和网络类型（如无线 LAN 和以太网）之间切换。NetworkManager 支持无线局域网中的 WEP 和 WPA-PSK 加密。它也支持拨号连接（使用 smpppd）。这两种桌面环境（GNOME 和 KDE）均包含 NetworkManager 的前端。关于桌面小程序的更多信息，请参阅第 13 章 [管理网络连接](#) (↑KDE 用户指南)和 *GNOME 用户指南*。

表 25.1 NetworkManager 的用例

我的电脑...	使用 NetworkManager
是便携式计算机	是
有时与不同网络连接	是
提供网络服务（例如 DNS 或 DHCP）	否
仅使用静态 IP 地址	否

在不应使用 NetworkManager 来处理网络配置时，请使用 YaST 工具配置联网。

SLP

服务位置协议 (SLP) 简化了便携式计算机与现有网络的连接。没有 SLP，便携式计算机的管理员通常需要详细了解网络中可用的服务。使用 SLP 则可以向本地网络中的所有客户机广播某种服务是否可用。支持 SLP 的应用程序可以处理 SLP 发送的信息，并进行自动配置。SLP 甚至还可用于安装系统，而不必再费事地搜索适合的安装源。有关 SLP 的更多详细信息，请参见第 31 章 [网络中的 SLP 服务](#) [587]。

SCPM 的重点在于启用和维护可再现的系统状况。而 SLP 可用于自动执行联网计算机的大部分配置工作，从而极大地简化了配置工作。

25.1.3 软件选择

在移动使用中有不同的特殊任务领域，它们由专用软件实现：系统监视（特别是电池充电）、数据同步和与外围设备及因特网的无线通讯。以下各节说明了 SUSE Linux Enterprise 为各项任务提供的最为重要的应用程序。

系统监视

SUSE Linux Enterprise 提供了两种 KDE 系统监视工具：

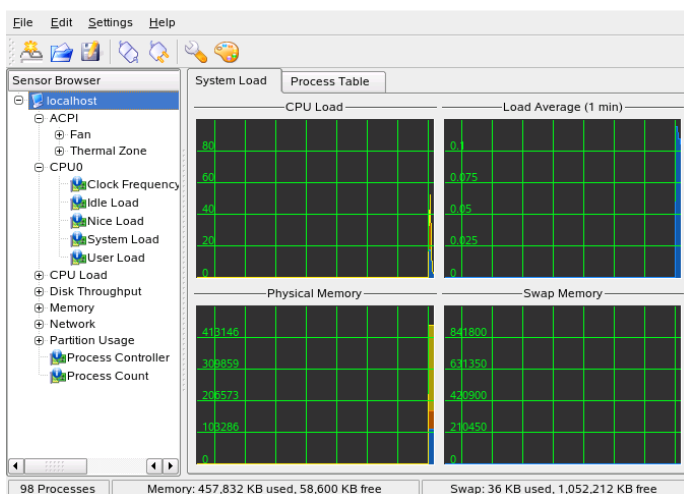
KPowersave

KPowersave 是可以在控制面板中显示充电电池状态的小程序。该图标将随电源类型调整显示。如果使用交流电，则显示一个小的插头图标。如果使用电池，则改为显示电池图标。提供 root 密码之后，相应的菜单会打开用于电源管理的 YaST 模块。这样就可以为不同电源设置系统的行为。有关电源管理和相应 YaST 模块的信息，请参见[第 28 章 电源管理](#) [489]。

KSysguard

KSysguard 是一个独立的应用程序，它可以将所有可测量系统参数收集到一个监视环境中。KSysguard 提供用于 ACPI（电池状态）、CPU 负载、网络、分区和内存使用等方面的监视程序。它还可以查看和显示所有的系统进程。可以自定义收集到的数据的表示和过滤方式。可以监视不同数据页中的不同系统参数，也可以跨网络并行收集不同计算机上的数据。KSysguard 还可以在不具备 KDE 环境的计算机上作为守护程序运行。有关此程序的详细信息，请参见此程序中集成的帮助功能或 SUSE 帮助页。

图 25.2 使用 KSysguard 监视电池状态



在 GNOME 桌面中，请使用面板小程序 GNOME ACPI 和应用程序系统监视器。

同步数据

如果要在以下两种工作方式（在与网络断开的移动计算机上工作和在办公室中的联网工作站上工作）之间切换，则需要所有实例间保持同步处理数据。要同步的可能包括电子邮件文件夹、目录和单个文件，这些数据需要保持最新，以便在途中和办公室中处理。适用于这两种情况的解决方案如下：

同步电子邮件

在办公室网络中使用 IMAP 帐户存储电子邮件。随后可以从工作站使用任意断开连接但支持 IMAP- 的电子邮件客户机（如 *Applications* 中所述的 Mozilla Thunderbird Mail、Evolution 或 KMail）来访问这些电子邮件。必须对电子邮件客户机进行配置，以便始终从同一文件夹访问已发送邮件。这样能确保在完成同步过程之后可以提供所有信件及其状态信息。使用邮件客户机中实施的 SMTP 服务器来发送邮件，取代系统范围内使用的 MTA postfix 或 sendmail 来接收有关未发送邮件的可靠反馈。

同步文件和目录

有若干实用程序适合在便携式计算机和工作站之间同步数据。有关详细信息，请参见 [第 38 章 文件同步](#) [647]。

无线通讯

便携式计算机不仅可以通过缆线连接家庭或办公网络，而且可以无线连接到其他计算机、外设、手提电话或 PDA。Linux 支持三种类型的无线通讯：

WLAN

WLAN在这三种无线技术中覆盖范围最广，是唯一一种适用于大型网络（有时甚至是在空间上分离的网络）的操作技术。单独的计算机可以通过互连形成独立的无线网络或访问因特网。称为访问点的设备充当支持 WLAN 设备的基站，并作为访问因特网的中介。移动用户可以在多个访问点之间切换，这取决于所在位置以及哪个访问点提供的连接最佳。类似移动电话的情况，WLAN 用户可以访问一个大型网络，而不必被集中到某个位置来访问这个网络。有关 WLAN 的详细信息请参见第 29.1 节“无线 LAN”[513]。

蓝牙

蓝牙技术是所有无线技术中应用范围最广的技术。与 IrDA 一样，蓝牙技术可用于计算机（便携式计算机）和 PDA 或手提电话之间的通信。它还可用于连接视线范围内的多台计算机。蓝牙技术还可用于连接键盘或鼠标之类的无线系统部件。但这种技术的覆盖范围还不够大，无法将远程系统连接到网络中。WLAN 是穿越墙壁之类的有形障碍物进行通讯的首选技术。有关蓝牙技术、其应用程序和配置的更多信息，请参见第 29.2 节“蓝牙”[522]。

IrDA

IrDA 是覆盖范围最小的无线技术。通讯双方必须在彼此的视线范围之内。无法穿越墙壁这样的障碍物。将文件从便携式计算机传送到手提电话就是 IrDA 的一种应用方式。使用 IrDA 即可覆盖由便携式计算机到手提电话之间的较短路径。要在较大范围内将文件传输给接收方，则需要通过移动网络来处理。IrDA 的另一种应用方式就是在办公室中无线传送打印作业。有关 IrDA 的更多信息，请参见第 29.3 节“红外线数据传送”[532]。

25.1.4 数据安全

要防止他人未经授权访问您的便携式计算机上的数据，您最好同时采用多种方式。可以在以下方面采取各种可能的安全措施：

防止被盗

始终尽可能地利用实物来防止您的系统被盗。零售店中就出售各种防盗工具，如锁链。

保护系统中的数据

重要数据不仅要在传送过程中加密，而且要在硬盘上加密。这样即使被盗也能保证数据不外泄。第 42 章 [对分区和文件进行加密](#) [683] 中对如何使用 SUSE Linux Enterprise 创建加密分区进行了说明。

重要：数据安全性和暂挂到磁盘

在发生暂挂到磁盘事件期间，不会卸装加密的分区。因此，任何人只需窃取硬件然后对硬盘发出 `resume` 命令就可以获取这些分区上的所有数据。

网络安全

无论采用哪种形式传送数据，任何形式的传送都应受到保护。有关 Linux 和网络的常见安全性问题，请参见第 44 章 [安全性和机密性](#) [699]。有关无线联网的安全措施，请参见第 29 章 [无线通讯](#) [513]。

25.2 移动硬件

SUSE Linux Enterprise 支持通过防火墙 (IEEE 1394) 或 USB 自动检测移动储存设备。术语 *移动存储设备* 适用于任何种类的防火墙或 usb 硬盘、USB 闪存驱动器，或数码相机。这些设备在经相应的接口和系统连接之后，将立刻被检测到并配置。GNOME 和 KDE 的文件管理器均可灵活操作移动硬件项目。要安全卸载任何此类媒体，请使用两个文件管理器中任意一个管理器的弹出功能。在 *GNOME 用户指南* 和 *KDE 用户指南* 中有更多的详细说明。

外部硬盘（USB 和火线）

一旦系统正确识别出外部硬盘，相应的图标即显示在 *我的电脑 (KDE)* 或 *计算机 (GNOME)* 中的已装入驱动器列表中。单击该图标将显示该驱动器的内容。可以在此创建文件夹和文件，并执行编辑或删除操作。要将系统指定的硬盘名称重命名，请右击该图标，从打开的菜单中选择相应的菜单项。只有在文件管理器中才能显示这种名称更改。将设备装入 `/media` 中的描述符将不受影响。

USB 闪存盘

系统会按照处理外部硬盘的方式来处理这些设备。同样也可以重命名文件系统中的项。

数码相机（USB 和火线）

系统识别出的数码相机也作为外部驱动器显示在文件管理器的概览中。如第 1.4.6 节“使用 Konqueror 访问数码相机”（第 1 章 *KDE 桌面入门*, ↑*KDE 用户指南*）中所述，KDE 允许读取和访问 URL `camera:/` 中的图片。随后可以使用 *digiKam* 或 *f-spot* 对图像进行处理。用 *GIMP* 进行照片的高级处理。关于 *digiKam* 和 *The GIMP* 的简短介绍，请参阅第 19 章 *管理数码图像集*（↑*KDE 用户指南*）和第 18 章 *使用 GIMP 操纵图形*（↑*KDE 用户指南*）。查找关于 *GNOME 用户指南* 中 *f-spot* 的更多信息。

25.3 手提电话和 PDA

台式计算机系统或便携式计算机可以通过蓝牙或 IrDA 与手提电话进行通信。有些手提电话型号两种协议都支持，另一些则只支持其中的一种。这两种协议的使用范围以及相应的展开文档都已在“**无线通讯**”一节 [463] 中说明。手提电话自带的手册中对如何在手提电话上配置这些协议进行了说明。第 29.2 节“**蓝牙**” [522] 和第 29.3 节“**红外线数据传送**” [532] 中则对 Linux 端的配置进行了说明。

Evolution 和 *Kontakt* 中已经内置了与 Palm, Inc. 制造的手持设备进行同步的支持功能。最初与手持设备连接时，无论使用哪种应用程序都可以借助向导轻松连接。一旦配置了针对 *Palm Pilots* 的支持，则需要确定应该同步哪种数据（地址、约会等）。关于更多信息，请参阅 *KDE 用户指南* 和 *GNOME 用户指南*。*Kontakt* 中集成的 *KPilot* 程序也可以作为单独的实用程序来运行。中对此进行了描述。第 6 章 *使用 KPilot 与掌上计算机进行同步*（↑*KDE 用户指南*）

25.4 更多信息

<http://tuxmobil.org> 是与移动设备和 Linux 有关的所有问题的集中参考来源。该万维网站点的各个章节论述了便携式计算机、PDA、手提电话和其他移动硬件的软硬件问题。

<http://www.linux-on-laptops.com> 中也提供了与 <http://tuxmobil.org> 类似的参考资源。可以在此站点中找到有关便携式计算机和手持设备的信息。

SUSE 维护着一个德文邮件列表，专门讨论便携式计算机这一主题。请参见 <http://lists.suse.com/archive/suse-laptop>。在这个列表中，用户

和开发人员讨论的是有关 SUSE Linux Enterprise 中的移动计算的各个方面的问题。用英文投递的信件都有答复，但存档信息中大部分都只有德文信息。

如果便携式计算机出现 SUSE Linux Enterprise 电源管理问题，建议阅读 `/usr/share/doc/packages/powersave` 中的 README 文件。此目录经常包含来自测试人员和开发人员的最新反馈，所以为解决这类问题提供了有价值的提示。

PCMCIA

PCMCIA 经常用来指硬件本身，尽管该术语来自将所有可能类型的个人计算机卡标准化的组织 *个人计算机存储卡国际协会*。起初，*PCMCIA* 只包括个人计算机卡（使用像 ISA 卡那样的 16 位总线），但后来也包括了 CardBus 卡（使用 32 位总线）。Linux 支持的 *PCMCIA* 硬件的范围很广。另外，Linux 还包括管理 *PCMCIA* 的工具。

PCMCIA 卡主要用在不同用途的移动计算中。例子有：

- Ethernet 和无线 LAN 适配器
- 蓝牙卡
- 存储卡（闪存、SRAM 和其他）
- 存储卡适配器（SD、MMC、SmartMedia、CompactFlash 和 MemoryStick）
- 调制解调器

多数卡的管理都是通过 `udev` 和 `hotplug` 静默处理的。需要用户交互时，请使用 `pccardctl` 命令。有关 *PCMCIA* 的背景信息，请参阅第 26.2 节“*PCMCIA 详述*”[468]。有关 `pccardctl` 的详细信息，请参阅第 26.1 节“用 `pccardctl` 控制 *PCMCIA* 卡”[468]。

26.1 用 pccardctl 控制 PCMCIA 卡

卡管理通常由 udev 和 hotplug 处理，而无需任何用户介入。当自动进程不能正常工作时，通过 pccardctl 命令可手动控制卡。

以下是一些最重要的 pccardctl 命令的列表。所有这些命令必须以 root 身份执行：

`pccardctl insert`

如果没有自动检测到卡，通知客户机驱动程序已插入了卡。

`pccardctl eject`

手动弹出卡，通知客户机驱动程序将弹出卡。切断插槽电源。如果您注意到 [第 26.3.2 节“和 PCMCIA 有关的常规暂停问题”](#) [473] 中描述的暂停和恢复有问题，该选项特别有用。

`pccardctl suspend`

关闭并禁用插槽电源，但不弹出卡（取消相应模块的绑定）。

`pccardctl resume`

给插槽上电，恢复 suspend 事件前的配置。

有关细节，请参考 pccardctl 的手册页。

26.2 PCMCIA 详述

以下小节概述了 PCMCIA 设备插入机器时，Linux 系统中会发生什么。组件会相互作用，要支持 PCMCIA 设备需满足许多要求。

以下是 Linux 中 PCMCIA 初始化进程的非常粗略的概述：

1. PCMCIA 桥（或插槽）必须按 [第 26.2.1 节“桥初始化”](#) [469] 中描述的那样正确设置。前提条件有：
 - 该桥的适当驱动程序
 - PC 卡的额外 I/O 和内存范围

2. 正确设置桥后，桥的驱动程序检测到卡的存在，并按 第 26.2.2 节“卡的初始化” [470] 中的描述触发其初始化：
 - a. 确定卡的类型。
 - b. 提供正确的电压。
 - c. 向卡指派 I/O 和内存范围，及 IRQ 行。
 - d. 通过绑定适当的卡驱动程序，触发卡或设备的初始化。
 - e. 对于某些卡，需要上载卡信息结构 (CIS)。
3. 最后，设置接口本身使之可用。有关详细信息，请参见 第 26.2.3 节“接口设置” [471]。

26.2.1 桥初始化

多数 PCMCIA 桥是 PCI 设备，同样处理。桥的初始化过程可总结如下：

1. 热插拔创建 PCI 事件。
2. udev 调用 /sbin/hwup 装载驱动程序。/sbin/hwup 在 /etc/sysconfig/hardware 中检查现有设备配置。如果找到了适当的配置，将使用那个配置。否则，/sbin/hwup 用内核提供的 modalias 字符串调用 modprobe，装载驱动程序模块。
3. 发送新的热插拔事件（每个 PCMCIA 插槽一个）。
4. 如果只使用 CardBus 卡，将省略以下步骤：
 - a. pcmcia_socket 事件触发 udev 调用 /sbin/hwup 并装载 pcmcia 内核模块。
 - b. /etc/pcmcia/config.opts 中指定的所有 I/O 和内存范围都将添加到插槽。
 - c. 内核中的卡服务检查这些范围。如果 /etc/pcmcia/config.opts 中的内存范围错误，该步骤将使机器崩溃。有关如何调试和修复该故障的信息，请参阅 第 26.3.1 节“PCMCIA 引起的机器崩溃” [471]。

成功完成这些步骤后，桥就完全初始化了。此后，桥本身按以下小节中所述进行初始化。

26.2.2 卡的初始化

插入 PCMCIA 卡导致的事件可归纳如下：

1. 发生一个热插拔事件。对于 PC 卡，这是 `pcmcia` 事件。对于 CardBus 卡，这是 `pci` 事件。
2. 对于任何事件，`udev` 调用 `/sbin/hwup` 装载驱动程序模块。模块名称要么在 `/etc/sysconfig/hardware` 下的 `hwcfg*` 文件中指定，或通过 `modprobe modalias`。
3. 如果需要，设备初始化将触发固件热插拔事件。将搜索固件并装载它。
4. 设备驱动程序注册接口。

完成这些步骤后，系统按下一节中的描述继续进行接口设置。

如果您的卡是 PC 卡，可能需要 `/etc/sysconfig/pcmcia` 中以下参数中的一些，以便完全支持它，使之无故障运行。

PCMCIA_LOAD_CIS

PC 卡的固件称为 *CIS*（卡信息结构）。它提供了卡的额外实施细节。`hwup` 检查卡的内置 *CIS* 的完整性，如果卡的 *CIS* 证明有缺陷，尝试从磁盘装入其他 *CIS*。默认设置是 `yes`。要禁用从磁盘装载 *CIS*，将这个变量设置为 `no`。

PCMCIA_ALLOW_FUNC_MATCH

Linux 设备驱动程序包含一个设备 ID 表，该表告诉驱动程序要处理哪个设备。这意味着只支持其标识为内核所支持的那些设备。要支持其标识未列出的那些卡，可使用功能匹配。这意味着驱动程序不是由标识选择，而是由卡（例如网卡）的功能选择，可对任何插入的具有该功能的 PC 卡（例如网卡）作出响应。默认设置是 `yes`。要禁用功能匹配，将这个变量设置为 `no`。

PCMCIA_COLDPLUG_REINSERT

引导前已插入的卡有时无法检测到。为防止发生这种情况，将 PCMCIA_COLDPLUG_REINSERT 设置为 yes 将卡软弹出并软插入。默认设置是 no。

26.2.3 接口设置

根据卡类型，成功完成初始化后将注册不同接口。接口注册是由 udev 的 hotplug 处理的。有关 udev 和 hotplug 的详细信息，请参阅 [第 21 章 使用 udev 进行动态内核设备管理](#) [419]。

26.3 故障诊断

以下是 PCMCIA 偶尔会遇到的最常见问题列表。有关更多信息，在 PCMCIA README(/usr/share/doc/packages/pcmciautils/README.SuSE) 中可用。

26.3.1 PCMCIA 引起的机器崩溃

PCMCIA 引导中启动时，机器崩溃。要找出机器崩溃的原因，如下所述手动设置。仔细地手动设置 PCMCIA 时，可以清楚地辨认出导致机器崩溃的步骤或组件。一旦辨认出了故障原因，就可以避开有问题的步骤或组件。

要手动设置 PCMCIA，请执行以下操作：

- 1 阻止 PCMCIA 在系统引导时启动，并通过向引导提示符添加以下选项启用选项 sysrq 以便更方便地进行调试：

```
init=3 pcmcia=off sysrq=1
```

有关 sysrq 的更多信息，请参见 /usr/src/linux/Documentation/sysrq.txt。

- 2 将系统引导到基于文本的环境，并以 root 身份登录。
- 3 向内核添加适当的 PCMCIA 模块：

```
/sbin/modprobe yenta_socket  
/sbin/modprobe pcmcia
```

4 启动 PCMCIA 插槽：

```
/sbin/pcmcia-socket-startup N
```

用插槽编号替换 *N*。对每个插槽重复该步骤。

- 5 如果以上步骤使机器崩溃了，可能是由于在 `/etc/pcmcia/config.opts` 中指定了错误的 I/O 或内存范围引起的。要防止发生这种情况，请执行以下操作之一：

- 排除 `/etc/pcmcia/config.opts` 中的范围，重试插槽设置。
- 如下所述手动添加范围。

成功地手动添加了适当的范围后，通过在 `/etc/pcmcia/config.opts` 中包括它们永久设置。

- 6 成功完成插槽设置后，卡初始化和接口设置按 [第 26.2.2 节“卡的初始化”](#) [470] 和 [第 26.2.3 节“接口设置”](#) [471] 中描述的生效。

要手动添加 I/O 范围，请执行如下操作（对每个插槽）：

- 1 切换到保存范围配置的目录（在本例中是 `pcmcia_socket0`，其他插槽编号各有不同）：

```
cd /sys/class/pcmcia_socket/pcmcia_socket0
```

- 2 执行以下命令：

```
echo begin - end > available_resources_io
```

用新范围开始和结束的地址更换 *begin* 和 *end*。正确值只能通过试错确定。

手动添加以下范围：

```
echo 0x800 - 0x8ff > available_resources_io  
echo 0xc00 - 0xcff > available_resources_io
```

和 `/etc/lilo.conf` 中的以下行相当：

```
include port 0x800-0x8ff, port 0xc00 0xcff
```

对 `available_resources_mem` 下的内存范围也适用相同步骤。

重要: 标识有问题的默认设置

如果发现随本产品交付的默认配置文件 (`/etc/pcmcia/config.opts`) 中的范围有问题, 在 <http://bugzilla.novell.com> 中提交错误, 使开发人员可以调查该问题。

26.3.2 和 PCMCIA 有关的常规暂停问题

暂停系统的任何时候 (暂停到磁盘、到 RAM 或待机), 不要在系统处于暂停模式时插入或拔出任何硬件。否则系统可能无法正常恢复。

要在暂停时自动弹出 PCMCIA 卡, 请执行如下操作:

- 1 以 root 身份登录。
- 2 打开文件 `/etc/powersave/sleep`。
- 3 设置以下变量:

```
SUSPEND2DISK_EJECT_PCMCIA="yes"
SUSPEND2RAM_EJECT_PCMCIA="yes"
STANDBY_EJECT_PCMCIA="yes"
```

- 4 保存文件以便应用设置。

如果暂停时需要弹出其他模块, 执行以上操作, 向以下变量添加模块名称:

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
```

有关 powersave 守护程序的一般信息, 请参见 [第 28.5 节 “powersave 包”](#) [499]。

26.3.3 更多信息

在 `/usr/share/doc/packages/pcmciautils/README.SuSE` 中可找到有关 PCMCIA 的最新信息。有关 PCMCIA 硬件及其使用领域的全面概述, 请转

到官方 PCMCIA 万维网站点 (<http://www.pcmcia.org/pccard.htm>)。要检查某种卡或设备通常是否受 Linux 支持，请参阅 http://tuxmobil.org/pcmcia_linux.html 上的 *Linux PCMCIA/CF/CardBus Card Survey*。

系统配置配置文件管理

借助于 SCPM（系统配置配置文件管理），可以调整计算机的配置以适应不同的操作环境或硬件配置。SCPM 管理一组用于不同方案的系统配置文件。使用 SCPM 可以在系统配置文件之间方便地切换，从而无需手动重配置系统。

某些情况需要经过修改的系统配置。这对在不同位置运行的移动计算机而言是很常见的情况。如果要使用普通硬件部件之外的其他硬件部件临时运行台式机系统，SCPM 需要手动配置。恢复最初的系统配置也会很容易，同时可以重现对系统配置的修改。利用 SCPM，可以在自定义的配置文件中保存系统配置的任何部分。

SCPM 的主要应用领域是便携式计算机上的网络配置。不同的网络配置通常需要对其他服务（例如，电子邮件或代理）进行不同的设置。SCPM 还可以用于其他方面，例如在家里和办公室使用不同的打印机、为开会时使用多媒体投影仪而设置的自定义 X 服务器配置、旅行时采用的特殊省电设置以及海外子公司所在的不同时区。

27.1 术语

以下是 SCPM 文档和 YaST 模块中使用的一些术语。

系统配置

计算机的完整配置。它包括所有基础设置，例如硬盘分区的使用、网络设置、时区选择和键盘映射。

配置文件或系统配置文件

预留的并且可以随时恢复的状态。

活动配置文件

最后选择的配置文件。这并不意味着当前系统配置完全与此配置文件对应，因为配置可以随时进行修改。

资源

有助于系统配置的元素。资源可以是文件或包含元数据（例如用户）、权限或访问时间的软链接。资源也可以是在此配置文件中运行、但在另一个配置文件中取消的系统服务。

资源组

每个资源都属于一个特定的资源组。这些组包含逻辑上在一起的所有资源，大多数组既包含服务又包含其配置文件。组装由 SCPM 管理的资源非常容易，原因是此操作不需要了解所需服务的配置文件。SCPM 附带有足以满足大多数方案的预配置资源组的集合。

27.2 设置 SCPM

以下部分将通过一个现实生活的例子来介绍 SCPM 的配置：一台移动计算机可以在几个不同的网络中运行。此方法面临的主要问题是：

- 多变的网络环境，比如在家是无线 LAN，而在公司以太网
- 家庭打印机配置与公司打印机配置不同

要启动和运行 SCPM 并使其管理不断变化的系统配置，请按如下所示继续：

- 1 向面板中添加 Profile Chooser 小程序并对其进行配置以使用户能够切换，如第 27.3.1 节“配置 Profile Chooser 面板小程序”[478]中所述。
- 2 如第 27.3.2 节“配置基本 SCPM 设置”[478]中所述使用 YaST 配置文件管理器模块配置 SCPM。
- 3 使用 SUMF (SCPM Unified Management Front-End) 为每个不同的设置创建一个配置文件，如第 27.3.3 节“新建配置文件”[480]中所述。
- 4 切换到适用于当前形式的配置文件，如第 27.3.4 节“切换配置文件”[481]中所述。

如果想使用其命令行界面来控制 SCPM，请参见第 27.4 节“使用命令行配置 SCPM”[483]来获取详细信息。

27.3 使用图形用户界面配置 SCPM

下面向您介绍用于控制配置文件设置的图形工具。

27.3.1 配置 Profile Chooser 面板小程序

在使用 Profile Chooser 控制系统配置之前，请将它配置为在登录时自动启动：

- 在 GNOME 中，右击面板并从可用小程序的列表中选择 Profile Chooser。
- 在 KDE 中，选择系统 > 桌面小程序 > *Profile Chooser* 将 Profile Chooser 添加到面板。

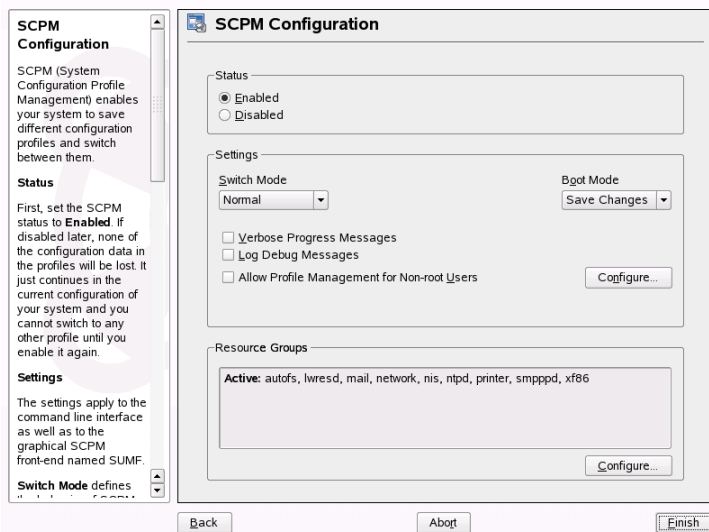
27.3.2 配置基本 SCPM 设置

通过 YaST 配置 SCPM 的基本行为。

- 1 从主菜单启动 YaST，然后选择 YaST 配置文件管理器。
- 2 在系统配置配置文件中，单击选项，然后选择启用。
- 3 通过选择冗长进度讯息和/或日志调试讯息来确定应该使用的冗长 SCPM。
- 4 确定适用于设置的切换方式：
 - 切换到其他配置文件时，SCPM 是否应该列出所作的所有更改并将这些更改保存到活动的配置文件中？选择常规或保存更改。
 - 切换时，SCPM 是否应该丢弃更改的任何资源配置？选择丢弃更改。
- 5 设置引导方式，并确定引导触发配置文件切换时是保存还是丢弃对当前配置文件的更改。
- 6 确保所需的所有资源组在资源组部分显示的活动选项中均有描述。如果需要其他资源组，请使用配置资源来调整资源。有关详细信息，请参见第 27.3.6 节“配置资源组”[482]。

对于示例方案，不需要配置其他资源，因为打印机和网络资源是默认包含的。

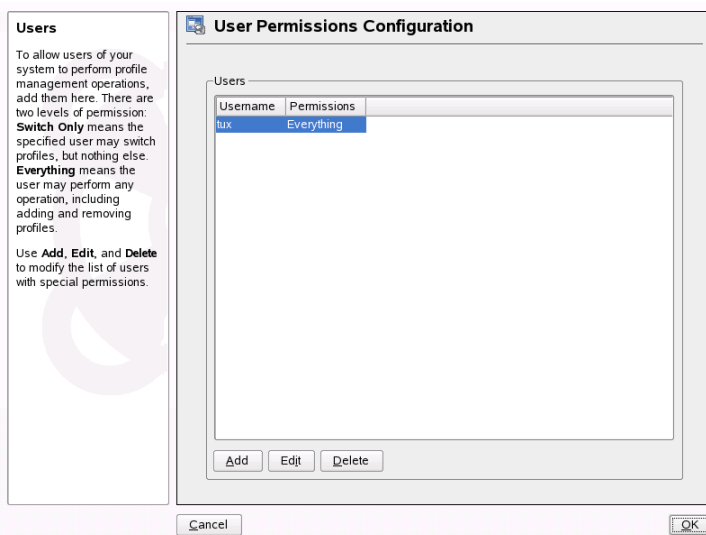
图 27.1 YaST: SCPM 基础配置



为了使用户而不是 `root` 能够管理配置文件，请执行以下步骤：

- 1 从主菜单启动 YaST，然后选择 YaST 配置文件管理器。
- 2 选择允许根用户以外的用户管理配置文件。请参阅图 27.2 “YaST：配置 SCPM 用户” [480]。
- 3 单击配置。
- 4 单击添加来添加有权管理配置文件的任何用户。
- 5 对于每个用户，请指定他是只具有切换权限还是允许此用户切换、修改和创建配置文件。
- 6 单击完成来应用设置并关闭 YaST。

图 27.2 YaST: 配置 SCPM 用户



27.3.3 新建配置文件

启用 SCPM 后，您会有一个包含当前系统配置的配置文​​件，名为 `default`。创建符合其他设置要求的其他配置文件。

要根据当前系统配置添加新的配置文件，请按如下所示继续：

- 1 右击 **Profile Chooser** 并选择 **运行配置文件管理器 (SUMF)**。
- 2 选择 **配置文件 > 添加**。
- 3 输入新配置文件的名称，然后单击 **确定**。
- 4 确定新的配置文件是否应该是活动的配置文件。

如果选择了是，则 SCPM 会在创建后立即切换为新的配置文件。

对于此示例，请执行以下操作：

- 1 在主页设置中，启用 SCPM。

- 2 通过启动 SUMF、选择 *配置文件* > *编辑* 并输入新名称将 default 配置文件重命名为更为直观的名称。
- 3 在设置生效时，启动 SUMF 并为当前系统环境创建配置文件。

一旦有了需要的所有配置文件，便可在需要其他系统设置时进行切换。中对配置文件切换进行了介绍。第 27.3.4 节 “切换配置文件” [481]。

27.3.4 切换配置文件

切换配置文件有两种方式。可以在引导时选择新配置文件，或者在运行系统中切换配置文件。

要在引导时选择配置文件，请按如下所示继续：

- 1 在引导屏幕中，按 F2 键可以进入其他选项菜单。
- 2 按 F3 键可以访问可用配置文件的列表。
- 3 使用方向键选择相应的配置文件并单击 Enter。

系统引导进选中配置。

要在运行系统中切换配置文件，请按如下所示继续：

- 1 确保您可以作为非 root 用户切换配置文件。如果您不能进行切换，请参见第 27.3.2 节 “配置基本 SCPM 设置” [478]。
- 2 单击 Profile Chooser 面板小程序。
- 3 使用方向键在打开的菜单中选择需要的配置文件，然后单击 Enter。SCPM 将检查修改过的资源，并提示您确认切换。如果在切换前已对系统配置进行了更改，则在您切换到其他配置文件时，请选择是保存还是丢弃它们。

27.3.5 编辑配置文件

要调整已更改的环境的现有配置文件（例如要更改家庭网络的打印机配置），请按如下所示继续：

- 1 如第 27.3.4 节“切换配置文件”[481]中所述，切换到要调整的配置文件。在此示例中，选择家庭配置文件。
- 2 使用相应的 YaST 模块更改要调整的资源。在此示例中，运行 YaST 打印机配置。
- 3 应用配置更改并请求配置文件切换后，SCPM 会询问这些更改是否要永久性地应用到之前活动的配置文件。

提示: 强行更新配置文件

如果要强行更新活动的配置文件，请单击 **Profile Chooser** 面板小程序配置文件选项菜单中的配置文件。它将重装载您的配置文件，并且会询问您是应用还是丢弃配置更改。

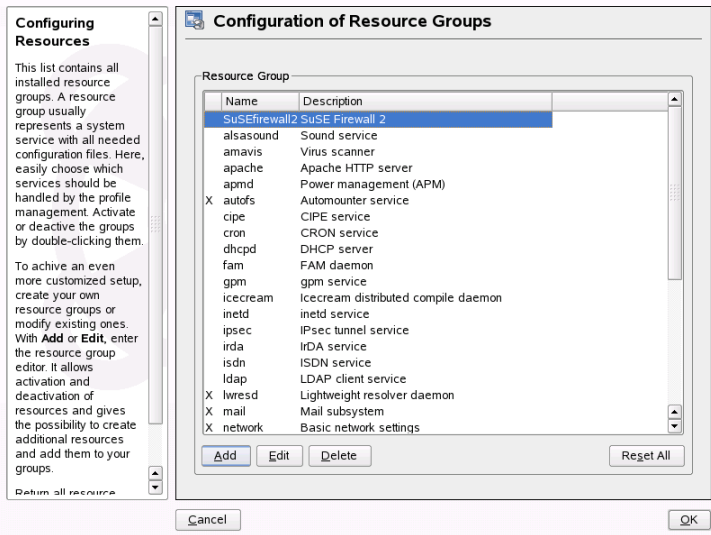
27.3.6 配置资源组

SCPM 附带了一组预定义的资源组，它们可默认包含在任何配置文件中。但是，有些方法还需要包含其他的资源和资源组。

要更改资源配置，请执行如下操作：

- 1 从主菜单启动 YaST 然后启动 YaST 配置文件管理器模块。
- 2 在系统配置配置文件管理对话框中，单击对话框的资源组部分中的配置。
系统中可用的所有资源组均在图 27.3 “配置资源组”[483]中列出。
- 3 要添加或编辑资源组：
 - 3a 设置或编辑资源组和描述。
 - 3b 输入相应的资源（资源和/或服务）并删除不需要的资源。要重设置所选资源的状态（丢弃对资源所进行的任何更改并返回到初始配置值），请选择重设置组。
 - 3c 单击确定退出资源配置。
- 4 单击确定将所作更改保存到活动的配置文件中。

图 27.3 配置资源组



27.4 使用命令行配置 SCPM

本节介绍 SCPM 的命令行配置。了解如何启动、配置 SCPML 并使用配置文件。

27.4.1 启动 SCPM 并定义资源组

在使用前，必须激活 SCPM。使用 `scpmenable` 激活 SCPM。如果是第一次运行，则将初始化 SCPM，这需要花几秒钟。可以随时用 `scpm disable` 取消激活 SCPM，以防止意外切换配置文件。随后的重激活只是继续初始化。

默认情况下，SCPM 处理网络和打印机设置以及 X.Org 配置。要管理特殊的服务或配置文件，请激活相应的资源组。要列出预定义的资源组，请使用 `scpmlist_groups`。要只查看已经激活的资源组，请使用 `scpmlist_groups -a`。请在命令行以 `root` 用户身份发出这些命令。

```
scpm list_groups -a

nis                Network Information Service client
mail               Mail subsystem
```

ntpd	Network Time Protocol daemon
xf86	X Server settings
autofs	Automounter service
network	Basic network settings
printer	Printer settings

使用 `scpm activate_group NAME` 或 `scpm deactivate_group NAME` 可以激活或取消激活某个组。用相关组名替换 `NAME`。

27.4.2 创建和管理配置文件

激活 SCPM 后，名为 `default` 的配置文件已经存在。可以使用 `scpm list` 获得所有可用配置文件的列表。这一现有的配置文件也是活动配置文件，可以使用 `scpm active` 进行校验。配置文件 `default` 是一个基本配置，其他配置文件都是从该配置派生的。为此，应该首先创建应在所有配置文件中相同的设置。然后，用 `scpmreload` 将这些修改储存在活动配置文件中。可以以 `default` 配置文件为基础，进行复制和重命名以生成新配置文件。

可以使用两种方法来添加新配置文件。如果新配置文件（这里名为 `work`）应基于配置文件 `default`，请用 `scpmcopy default work` 创建此配置文件。命令 `scpmswitch work` 可以切换为新配置文件，然后可以对其进行修改。您可能要为特殊目的修改系统配置并将更改保存到新配置文件中。命令 `scpmadd work` 将创建一个新配置文件，方法是将当前系统配置保存在配置文件 `work` 中并将其标记为活动配置文件。随后运行 `scpm reload` 将更改保存到配置文件 `work` 中。

使用命令 `scpm rename x y` 和 `scpm delete z` 重命名或删除配置文件。例如，要将 `work` 重命名为 `project`，请输入 `scpmrename work project`。要删除 `project`，请输入 `scpm delete project`。不能删除活动配置文件。

27.4.3 切换配置配置文件

可以使用命令 `scpm switch work` 切换到另一个配置文件（在本例中是配置文件 `work`）。切换到活动配置文件以将系统配置的已修改设置包括在配置文件中。此操作对应于命令 `scpmreload`。

切换配置文件时，SCPM 首先检查已修改了活动配置文件的哪些资源。然后，SCPM 查询是将每个资源的修改添加到活动配置文件中，还是将它们删除。如果需要这些资源的单独列表（如 SCPM 以前的版本中那样），请使用带有 `-r` 参数的 `switch` 命令：`scpm switch -r work`。

```
scpm switch -r work
```

```
Checking for modified resources
Checking for Resources to be started/shut down
Checking for dependencies
Restoring profile default
```

随后，SCPM 将当前系统配置与要切换到的配置文件进行比较。在这个阶段，SCPM 评估由于相互依赖性或为反映配置中的更改，需要停止或重新启动哪些系统服务。这类似于部分系统重引导，系统的一小部分进行重引导，而其余部分继续运行，无任何影响。也就是在此时系统服务停止，写入所有已修改的资源（例如配置文件），然后重新启动系统服务。

27.4.4 高级配置文件设置

您可以为通过 `scpmlist` 显示的每个配置文件输入说明。对于活动配置文件，请使用 `scpmset description "text"` 进行设置。对于不活动的配置文件，请提供配置文件名，例如 `scpm set description "text" work`。有时在切换配置文件时可能需要执行一些不是由 SCPM 提供的其他操作。每个配置文件最多可以附加 4 个可执行文件。将在切换进程的不同阶段调用这些文件。这些阶段被称为：

`prestop`

离开配置文件时，在停止服务前运行

`poststop`

离开配置文件时，在停止服务之后运行

`prestart`

激活配置文件时，在启动服务之前运行

`poststart`

激活配置文件时，在启动服务之后运行

使用命令 `set` 插入这些操作，方法是输入 `scpm set prestop filename`、`scpmset poststop filename`、`scpm set prestart filename` 或

`scpm set poststart filename`。这些脚本必须可执行并且引用了正确的解释器。

警告: 集成自定义脚本

对超级用户 (`root`) 来说, 将由 **SCPM** 执行的其他脚本必须是可读的和可执行的。必须阻止所有其他用户对这些文件的访问。输入命令 `chmod 700 filename` 和 `chown root:root filename` 向 `root` 用户授予对这些文件的独占权限。

用 `set` 和 `get` 查询输入的所有其他设置。例如, 命令 `scpm get poststart` 返回 `poststart` 调用的名称, 如果未附加任何对象, 则不返回任何内容。使用 `"` 覆盖可以重置这些设置。使用命令 `scpm set prestop ""` 可以去除附加的 `prestop` 程序。

可以使用与添加注释相同的方法将所有 `set` 和 `get` 命令应用到任何一个配置文件中。例如, `scpm get prestop filename work` 或 `scpmget prestop work`。

27.5 故障诊断

本节介绍使用 SCPM 时经常遇到的问题。了解这些问题是如何产生的和如何解决这些问题。

27.5.1 SCPM 和 NetworkManager

NetworkManager 和 **SCPM** 共享功能。将机器集成到现有网络, 隐藏此事务使用户看不到它。**NetworkManager** 将自动运行, 它适用于任何新环境。**SCPM** 用于恢复预定义的系统设置。

不能并行使用 **NetworkManager** 和 **SCPM**, 因为 **NetworkManager** 不会提供可由 **SCPM** 恢复的配置。对于需要可重现设置的所有用户来说, **SCPM** 非常有用。如果只需要调整网络设置组件, 则经常切换网络的任何个人用户都应该使用 **NetworkManager**。如果您想使用 **SCPM** 来管理您的系统配置, 而用 **NetworkManager** 来管理网络连接, 请从 **SCPM** 去除网络资源。如果想使用 **SCPM** 来管理网络配置, 请禁用 **NetworkManager**。

27.5.2 在切换进程中终止

有时，SCPM 会在切换过程中停止工作。这可能是由某个外部原因引起的，例如用户中止、电源故障或甚至是 SCPM 本身的错误。如果出现这种情况，则在您下次启动 SCPM 时将显示一条错误讯息，指出 SCPM 已被锁定。这是出于系统安全的考虑，因为储存在其数据库中的数据可能与系统的状态不同。要解决此问题，请运行 `scpm recover`。SCPM 执行上次运行时缺少的所有操作。您还可以运行 `scpm recover -b`，它尝试撤消上次运行时所有已执行的操作。如果使用 YaST 配置文件管理器，则在启动时将获得提供执行上述命令的恢复对话框。

27.6 更多信息

SCPM 信息页 (`info scpm`) 中可找到最新文档。 `/usr/share/doc/packages/scpm` 提供了开发人员所需的信息。

电源管理

电源管理对于便携式计算机特别重要，但对于其他系统也是有用的。有两种技术：APM（高级电源管理）和 ACPI（高级配置和电源界面）。除了这两项技术，还可以通过控制 CPU 频率调节达到省电或降低噪声的目的。这些选项可以手动配置或使用特殊的 YaST 模块配置。

电源管理对于便携式计算机特别重要，但对于其他系统也是有用的。所有现代计算机（便携式计算机、台式机和服务器）上都提供有 ACPI（高级配置与电源接口）。电源管理技术需要合适的硬件和 BIOS 例程。大多数便携式计算机、许多目前的台式机和服务器都符合这些要求。还可以通过控制 CPU 频率调节以达到省电或降低噪声的目的。

APM 用在许多以前的计算机上。因为 APM 主要由在 BIOS 中实施的功能集组成，所以 APM 支持的级别因硬件的不同而有所不同。而这对 ACPI 而言就更是如此，ACPI 更加复杂。因此，实际上很难决定是向您推荐 APM 还是 ACPI。在您的硬件上测试各种过程，然后选择支持情况最好的技术即可。

28.1 省电功能

省电功能不仅对便携式计算机的移动使用很重要，而且对台式机系统也很重要。电源管理系统 APM 和 ACPI 中的主要功能及其用途是：

待机

此运行方式将关闭屏幕显示。在某些计算机上，处理器性能会受到限制。此功能对应于 ACPI 状态 S1 或 S2。

暂挂（到内存）

此方式将整个系统状态写入 RAM。随后，除 RAM 外，整个系统都进入休眠状态。在此状态下，计算机消耗的电量非常少。此状态的优点是无需引导和重新启动应用程序就可以在数秒内将工作恢复到原来的进度。此功能对应于 ACPI 状态 S3。对此状态的支持仍在开发中，因此目前主要依靠硬件来实现支持。

休眠（暂挂到磁盘）

在此运行方式下，将整个系统状态写入硬盘并关闭系统电源。至少要有一个像 RAM 一样大的交换分区才能写入所有活动的数据。从该状态重激活大约需要 30 至 90 秒的时间。将恢复到暂停之前的状态。某些制造商提供这种方式的有用的混合变体（例如 IBM Thinkpad 中的 RediSafe）。对应的 ACPI 状态是 S4。在 Linux 中，由独立于 APM 和 ACPI 的内核例程执行暂挂到磁盘。

电池监视

ACPI 和 APM 检查电池电量状态并提供相关信息。另外，当达到临界电量状态时，两个系统都将协调要执行的操作。

自动关闭电源

关闭后，将关闭计算机的电源。当在电池电量用完前立即执行自动关闭时，此功能特别重要。

系统部件的关闭

关闭硬盘是整个系统中省电潜力最大的一个方面。根据整个系统的可靠性，硬盘可以休眠一段时间。但是，休眠期间丢失数据的风险也会增加。可使用 ACPI（至少从理论上说可行）取消激活或在 BIOS 设置中永久禁用其他组件（如可处于特殊省电模式的 PCI 设备）。

处理器速度控制

在 CPU 方面，有三种方法可以节省电能：频率和电压调节（也称为 PowerNow! 或 Speedstep）、节流和让处理器休眠（C 状态）。根据计算机的运行方式，还可以将这三种方法结合起来使用。

28.2 APM

APM BIOS 本身会执行一些省电功能。在许多便携式计算机上，可以使用组合键或通过合上机盖来激活待机状态和暂挂状态，无需任何特殊的操作系统功能。

但是，要通过命令激活这些方式，则必须在暂停系统前触发某些特定的操作。要查看电池电量水平，需要特殊的程序包和合适的内核。

SUSE Linux Enterprise® 内核具有内置的 APM 支持。但是，只有在 BIOS 中未实施 ACPI 且检测到 APM BIOS 的情况下才能激活 APM。要激活 APM 支持，必须在引导提示符下使用 `acpi=off` 禁用 ACPI。输入 `cat /proc/apm` 检查 APM 是否处于活动状态。由多个数字组成的输出表示一切正常。现在应该能使用命令 `shutdown-h` 关闭计算机。

不完全符合标准的 BIOS 实施可能使 APM 出现问题。可以使用特殊的引导参数来避免某些问题。在引导提示符下以 `apm=parameter` 形式输入所有参数，*parameter* 为以下的一个：

`on or off`

启用或禁用 APM 支持。

`(no-)allow-ints`

在执行 BIOS 功能时允许中断。

`(no-)broken-psr`

BIOS 的 “GetPowerStatus” 功能工作不正常。

`(no-)realmode-power-off`

关闭前将处理器重设置为实际方式。

`(no-)debug`

在系统日志中记录 APM 事件。

`(no-)power-off`

在关闭后关闭系统电源。

`bounce-interval=n`

暂停事件后的一段时间（以百分之一秒为单位），在这段时间中将忽略其他暂停事件。

`idle-threshold=n`

系统不活动百分比，从这个百分比开始执行 BIOS 功能 `idle`（0 表示始终执行，100 表示从不执行）。

`idle-period=n`

开始测量系统活动前所经过的时间（以百分之一秒为单位）。

不再使用 APM 守护程序 (apmd)。其功能现在由新的 powersaved 处理，后者也支持 ACPI 并能提供许多其他功能。

28.3 ACPI

ACPI（高级配置和电源接口）支持操作系统设置和控制各个硬件部件。ACPI 可以取代 PnP 和 APM。它提供有关电池、AC 适配器、温度、风扇和系统事件（例如“合上机盖”或“电池电量低”）的信息。

BIOS 提供包含有关各个部件和硬件访问方法信息的表。操作系统使用这些信息执行指派中断或激活和取消激活部件等任务。因为操作系统执行 BIOS 中储存的命令，所以功能取决于 BIOS 实施。/var/log/boot.msg 中报告了 ACPI 能够检测并装载的表。有关对 ACPI 问题进行故障诊断的详细信息，请参阅[第 28.3.4 节“故障诊断”](#) [497]。

28.3.1 使用 ACPI

如果内核在引导系统时检测到 ACPI BIOS，则会自动激活 ACPI。某些较旧的计算机可能需要引导参数 `acpi=force`。计算机必须支持 ACPI 2.0 或更高版本。检查 /var/log/boot.msg 中的内核引导讯息，了解是否已激活了 ACPI。

随后，必须装载多个模块。这是由 Aacpid 的启动脚本完成的。如果这些模块中的任何一个模块引起问题，则可以在 /etc/sysconfig/powersave/common 中排除相应模块的装载或卸载。系统日志 (/var/log/messages) 包含模块的讯息，使您了解检测到了哪些组件。

/proc/acpi 目前包含多个文件，这些文件提供有关系统状态的信息，也可用于更改某些状态。某些功能仍在开发中，所以尚不能使用，而对某些功能的支持主要取决于制造商的实施。

通过 cat 可以读取所有文件（dsdt 和 fadt 除外）。在某些文件中，可使用 echo（例如 `echo X > file`）来修改设置，以指定适用于 X 的值。能够简化访问这些值的其中一种可行方法就是使用 powersave 命令，它将充当 Powersave 守护程序的前端。下面介绍一些最重要的文件：

```
/proc/acpi/info
    有关 ACPI 的一般信息。
```


`/proc/acpi/alarm`

这里指定应将系统从休眠状态唤醒的时间。当前不完全支持此功能。

`/proc/acpi/sleep`

提供有关可能的休眠状态的信息。

`/proc/acpi/event`

在这里报告所有事件并由 Powersave 守护程序 (powersaved) 对这些事件进行处理。如果没有任何守护程序访问该文件，则可以使用 `cat`

`/proc/acpi/event` 读取事件（如短暂单击电源按钮或合上机盖）（用 **Ctrl + C** 终止）。

`/proc/acpi/dsdt` 和 `/proc/acpi/fadt`

这些文件包含 ACPI 表 DSDT（区分系统说明表和 FADT（固定 ACPI 说明表））。可以使用 `acpidmp`、`acpidisasm` 和 `dmdecode` 读取这些文件。包 `pmtools` 中提供了这些程序及其文档。例如，`acpidmpDSDT` | `acpidisasm`。

`/proc/acpi/ac_adapter/AC/state`

显示是否连接了 AC 适配器。

`/proc/acpi/battery/BAT*/{alarm,info,state}`

有关电池状态的详细信息。通过将 `info` 中的 `last full capacity` 与 `state` 中的 `remaining capacity` 进行比较来读取电量水平。一个更方便的方法是使用第 28.3.3 节“ACPI 工具”[496] 中引入的特殊程序之一。可以在 `alarm` 中指定电量水平，达到该电量水平将触发电池事件（例如警告、低和严重）。

`/proc/acpi/button`

该目录中包含各种切换模式的相关信息，比如便携式计算机机盖和按钮。

`/proc/acpi/fan/FAN/state`

显示风扇当前是否处于活动状态。将 0（开）或 3（关）写入此文件可以手动激活或取消激活风扇。但是，当系统变得过热时，内核中的 ACPI 代码和硬件（或 BIOS）将覆盖此设置。

`/proc/acpi/processor/*`

为系统中的每个 CPU 保留了一个单独的子目录。

`/proc/acpi/processor/*/info`

有关处理器省电选项的信息。

```
/proc/acpi/processor/*/power
```

有关当前处理器状态的信息。C2 旁边的星号表示处理器处于空闲状态。这是最常见的状态，可以从 usage 值中观察到。

```
/proc/acpi/processor/*/throttling
```

可用于设置处理器时钟的节流。通常，可以将节流分为 8 个级别。这与 CPU 的频率控制无关。

```
/proc/acpi/processor/*/limit
```

如果守护程序自动控制性能（已过时）和节流，则可以在这里指定最大限制。某些限制是由系统确定的。某些限制可由用户进行调整。

```
/proc/acpi/thermal_zone/
```

每个热区有单独的子目录。热区是具有类似热属性的区域，其编号和名称由硬件制造商指定。但是，很少实施 ACPI 提供的许多功能。而温度控制通常是由 BIOS 处理的。因为关系到硬件的使用寿命，所以操作系统很少有机会进行干预。因此，部分文件只具有理论价值。

```
/proc/acpi/thermal_zone/*/temperature
```

热区的当前温度。

```
/proc/acpi/thermal_zone/*/state
```

此状态指出一切是否 ok 或 ACPI 是采用 active 散热还是 passive 散热。对于独立于 ACPI 的风扇控制，此状态始终是 ok。

```
/proc/acpi/thermal_zone/*/cooling_mode
```

选择由 ACPI 控制的散热方法。选择被动散热方式（性能较低，但很经济）还是主动散热方式（全部性能，但有风扇噪音）。

```
/proc/acpi/thermal_zone/*/trip_points
```

允许您确定温度限制，达到这些温度限制将触发特定操作（例如，被动散热或主动散热、暂停(hot)或关闭(critical)）。DSDT 中定义了可能的操作（取决于设备）。ACPI 规范中确定的临界点是 critical、hot、passive、active1 和 active2。即使不是实施所有临界点，也必须始终在此文件中以此顺序输入它们。例如，项 echo 90:0:70:0:0 > trip_points 将 critical 的温度设置为 90，将 passive 的温度设置为 70（所有温度以摄氏度为单位）。

```
/proc/acpi/thermal_zone/*/polling_frequency
```

如果在温度改变时没有自动更新 `temperature` 中的值，请在这里切换巡回检测方式。使用命令 `echo X >`

`/proc/acpi/thermal_zone/*/polling_frequency` 将每 `X` 秒查询一次温度。设置 `X=0` 禁用巡回检测。

不需要手动编辑这些设置、信息和事件。这可以通过 **Powersave** 守护程序 (`powersaved`) 及其各种前端（例如 `powersave`、`kpowersave` 和 `wmpowersave`）来完成。请参阅第 28.3.3 节“**ACPI 工具**”[496]。

28.3.2 控制 CPU 性能

CPU 可以采用三种省电方法。根据计算机的运行方式，还可以将这三种方法结合起来使用。省电还意味着系统温度不会升得过高并且激活风扇的频率会降低。

频率和电压调节

PowerNow! 和 **Speedstep** 是 AMD 和 Intel 为这一技术指定的名称。但是，其他制造商的处理器中也应用了这一技术。CPU 的时钟频率及其核心电压同时降低，因而采用这一技术所节省的电量远远超过了线性省电量。这意味着，如果频率减半（一半的性能），所节省的电量远不止一半。此技术独立于 **APM** 或 **ACPI**。可使用两种主要的方法来执行 CPU 频率调节：通过内核本身或通过用户空间应用程序。因此，可以在 `/sys/devices/system/cpu/cpu*/cpufreq/` 下设置不同的内核管理器。

userspace governor

如果设置了用户空间管理器，则内核会将对 CPU 频率调节的控制指定给用户空间应用程序（通常是守护程序）。在 SUSE Linux Enterprise 分发中，此守护程序是 `powersaved` 程序包。使用此实施时，将根据当前系统负载调整 CPU 的频率。默认情况下，将使用某个内核实施。但是，在某个硬件上或对于特定处理器或驱动器，用户空间实施仍是唯一的工作解决方法。

ondemand governor

它是动态 CPU 频率策略的内核实施，应该可在大多数系统上运行。只要系统负载过高，CPU 频率将立即增加。它在系统负载较低时也较低。

conservative governor

此管理器与按需实现相似，只是使用更保守的策略。对于 CPU 频率增加之前的特定时间内，系统的负载必须很高。

powersave governor

静态地将 cpu 频率设置为最低。

performance governor

静态地将 cpu 频率设置为最高。

节流时钟频率

此技术将忽略一定百分比的 CPU 时钟信号脉冲。如果节流 25%，则将忽略四分之一的脉冲，如果节流 87.5%，则只有八分之一的脉冲到达处理器。但是，采用这种方法所节省的电量稍微低于线性省电量。通常，只有在频率调节不可用或要最大程度节省电量时才使用节流。此技术也必须由特殊的进程控制。系统接口是 `/proc/acpi/processor/*/throttling`。

使处理器进入休眠状态

操作系统在处理器不执行任何任务时使处理器进入休眠状态。在这种情况下，操作系统向 CPU 发送一个 `halt` 命令。有三种状态：C1、C2 和 C3。最经济的状态是 C3，在这种状态下，连处理器高速缓存与主存之间的同步都将暂停。因此，只有在没有任何其他设备通过总线主控芯片活动修改主存储器的内容时才能应用此状态。某些驱动程序禁止使用 C3。当前状态显示在 `/proc/acpi/processor/*/power` 中。

只有当处理器忙时，才需要进行频率调节和节流，这是因为当处理器处于空闲状态时总是会应用最经济的 C 状态。如果 CPU 忙，则建议采用的省电方法是频率调节。处理器经常只在部分负载的状态下工作。在这种情况下，可以以较低的频率运行。通常，由内核按需管理器 (kernel on demand governor) 或一个守护程序（如 `powersaved`）控制的动态频率调节是最佳方法。如果使用电池工作或如果您想让计算机冷却或安静，则静态设置为低频率会非常有用。

节流应作为最后没有办法时采用的方法，例如，虽然系统负载很高，但为延长电池工作时间而采用节流。但是，如果节流程度过高，某些系统将不会正常运行。此外，如果 CPU 处理的任务量很少，则 CPU 节流就没什么作用。

在 SUSE Linux Enterprise 中，这些技术是由 `powersave` 守护程序控制的。对此配置进行了说明。第 28.5 节“`powersave` 包”[499]

28.3.3 ACPI 工具

一系列相对全面的 ACPI 实用程序包含这样一些工具：只显示信息（例如，电池电量水平和温度）的工具（`acpi`、`klaptopdaemon` 和 `wmacpimon` 等）、简化对

/proc/acpi 中的结构进行访问的工具或协助监视更改的工具（akpi、acpiw 和 gtkacpiw）以及用于编辑 BIOS 中 ACPI 表的工具（包 pmtools）。

28.3.4 故障诊断

问题有两种不同的类型。一种是内核的 ACPI 代码可能包含未及时检测出的错误。在这种情况下，可以通过下载获得解决方案。而另一种更常见的问题，是由 BIOS 引起的。有时，会故意将一些不符合 ACPI 规范的配置集成在 BIOS 中，用于避免其他常用操作系统中 ACPI 实施中的错误。在 ACPI 实施中有严重错误的硬件部件会被记录在一个黑名单中，防止 Linux 内核对这些部件使用 ACPI。

在遇到问题时，首先要做的是更新 BIOS。如果计算机根本未引导，则使用以下引导参数之一可能会解决问题：

pci=noacpi

不使用 ACPI 配置 PCI 设备。

acpi=ht

只执行简单的资源配置。不要将 ACPI 用于其他目的。

acpi=off

禁用 ACPI。

警告：不使用 ACPI 引导会出现问题

某些较新的计算机（特别是 SMP 系统和 AMD64 系统）需要 ACPI 以正确配置硬件。在这些计算机上，禁用 ACPI 可能会产生问题。

引导后，用命令 `dmesg | grep -2i acpi` 来监视系统的引导讯息（或所有讯息，因为问题可能不是由 ACPI 引起的）。如果在分析 ACPI 表时出错，则最重要的表 (DSDT) 可替换为更高的版本。在这种情况下，将忽略 BIOS 中有问题的 DSDT。中对这一过程进行了介绍。[第 28.5.4 节“查错”](#) [505]

在内核配置中，可以使用开关来激活 ACPI 调试讯息。如果已编译并安装了具有 ACPI 调试功能的内核，则支持对详细信息执行错误专家搜索。

如果遇到 BIOS 或硬件问题，则最好与制造商联系。特别是如果制造商不常对 Linux 提供支持，他们就应该面对这些问题。只有在制造商意识到有很多客户在使用 Linux 时，他们才会重视这一问题。

更多信息

有关 ACPI 的其他文档和帮助：

- <http://www.cpqlinux.com/acpi-howto.html>（详细的 ACPIHOWTO 文档，包含 DSDT 增补程序）
- <http://www.intel.com/technology/iapc/acpi/faq.htm> (ACPI FAQ @Intel)
- <http://acpi.sourceforge.net/>（Sourceforge 中的 ACPI4Linux 项目）
- <http://www.poupinou.org/acpi/>（Bruno Ducrot 开发的 DSDT 增补程序）

28.4 硬盘的休眠

在 Linux 中，如果不使用硬盘，则可以使硬盘完全进入休眠状态，或者在更经济或更安静的方式下运行。在目前的便携式计算机上，您无需手动关闭硬盘，因为硬盘会在不运行时自动进入经济的运行方式。但是，如果要最大限度地省电，请尝试使用以下一些方法。powersaved 和 YaST 电源管理模块可以控制大多数的功能，这将在第 28.6 节“YaST 电源管理模块”[507]中作进一步的讨论。

hdparm 应用程序可用于修改多种硬盘设置。选项 -y 将硬盘立即切换到待机方式。-Y 使硬盘进入休眠状态。hdparm -S x 会使硬盘在一段时间（未活动）后减慢运行速度。将 x 替换如下：0 表示禁用此机制，导致硬盘持续运行。值 1 到 240 表示的时间为所选的值乘以 5 秒。值 241 到 251 对应的时间分别是 30 分钟的 1 到 11 倍。

使用选项 -B 可以控制硬盘的内部省电选项。在 0 到 255 之间选择一个值，0 表示最大省电方式，255 表示最大吞吐量方式。结果取决于所使用的硬盘，难以估算。要让硬盘安静一些，请使用选项 -M。在 128 到 254 之间选择一个值，128 表示最安静，254 表示速度最快。

通常，让硬盘进入休眠状态并不容易。在 Linux 中，大量的进程对硬盘执行写操作，因而会经常将其唤醒。因此，一定要了解 Linux 如何处理需要写入硬盘的数据。首先，在 RAM 中对所有数据进行缓冲。此缓冲区由内核更新守护程序 (kupdated) 进行监视。当数据达到一定的有效期限或缓冲区已被填充到一定程度时，就会清理缓冲区，将其中的内容写入硬盘。缓冲区大小是动态的，取决于内存的大小和系统负载。默认情况下，将 kupdated 设置为较短的时间间隔可以获得最好的数据完整性。它每 5 秒检查一次缓冲区，当数据存放时间超过 30 秒或缓冲区填充程度达到 30% 时，它会向 bdflush 守护程序发出通知。随后，bdflush 守护程序将数据写入硬盘。此守护程序还独立于 kupdated 写入数据，例如，当缓冲区已满时。

警告: 对数据完整性的损害

更改内核更新守护程序设置将损害数据完整性。

除了这些进程之外，日记文件系统（例如 ReiserFS 和 Ext3）独立于 bdflush 写入它们的元数据，这也会妨碍硬盘减慢运行速度。为了避免这种情况，已为移动设备开发了特殊的内核扩展。有关详细信息，请参见 `/usr/src/linux/Documentation/laptop-mode.txt`。

另一个重要因素是活动程序的行为方式。例如，好的编辑器会定期将当前已修改文件的隐藏备份写入硬盘，而这会唤醒磁盘。可以禁用此类功能，但这会影响数据的完整性。

在此连接中，邮件守护程序 postfix 使用变量 `POSTFIX_LAPTOP`。如果将此变量设为 `yes`，则 postfix 访问硬盘的频率将显著降低。但是，如果增加 kupdated 的时间间隔，则这样做没有什么作用。

28.5 powersave 包

powersave 包中包含了先前描述的所有省电功能。通常来说，由于对低能源消耗的需求的增加，它的某些功能在工作站和服务器的上也相应变得重要，例如暂停、待机或 CPU 频率调节。

此包包含计算机的所有电源管理功能。它支持使用 ACPI、APM、IDE 硬盘以及 PowerNow! 或 SpeedStep 技术的硬件。包 `apmd`、`acpid`、`ospm` 和 `cpufreqd`（现在是 `cpuspeed`）中的功能已被合并到 powersave 包中。这

些包中的守护程序（除了充当 acpi 事件多路转换器的 `acpid`）不应该与 `powersave` 守护程序并发运行。

即使您的系统未包含上面列出的所有硬件元素，也应使用 `powersave` 守护程序控制省电功能。因为 `ACPI` 和 `APM` 是互斥的，所以您的计算机上只能使用其中一个系统。此守护程序将自动检测硬件配置中的任何更改。

28.5.1 配置 `powersave` 包

`powersave` 的配置分布在多个文件中。此处列出的所有配置选项都包含有关其功能的其他文档。

`/etc/sysconfig/powersave/common`

此文件包含 `powersave` 守护程序的一般设置。例如，通过增大变量 `DEBUG` 的值可以增加 `/var/log/messages` 中调试讯息的数量。

`/etc/sysconfig/powersave/events`

`powersave` 守护程序需要此文件来处理系统事件。可以将事件指派给外部操作，也可以指派给守护程序本身执行的操作。对于外部操作，守护程序尝试运行 `/usr/lib/powersave/scripts/` 中的可执行文件（通常是 `Bash` 脚本）。预定义的内部操作有：

- `ignore`
- `throttle`
- `dethrottle`
- `suspend_to_disk`
- `suspend_to_ram`
- `standby`
- `do_suspend_to_disk`
- `do_suspend_to_ram`
- `do_standby`
- 通知

- `screen_saver`
- `reread_cpu_capabilities`

`throttle` 按 `MAX_THROTTLING` 中定义的值减慢处理器的速度。此值取决于当前方案。`dethrottle` 设置处理器发挥全部性能运行。
`suspend_to_disk`、`suspend_to_ram` 和 `standby` 触发休眠方式的系统事件。这三个操作通常负责触发休眠方式，但应始终将它们与特定的系统事件关联起来。

目录 `/usr/lib/powersave/scripts` 包含处理事件的脚本：

`switch_vt`

如果暂停或待机后屏幕移位，则可以使用此脚本。

`wm_logout`

保存设置并从 GNOME、KDE 或其他窗口管理器中注销。

`wm_shutdown`

保存 GNOME 或 KDE 设置并关闭系统。

`set_disk_settings`

执行 `/etc/sysconfig/powersave/disk` 中所作的磁盘设置。

例如，如果设置了变量

```
EVENT_GLOBAL_SUSPEND2DISK="prepare_suspend_to_disk
do_suspend_to_disk"
```

，则用户一旦将休眠方式暂挂到磁盘的命令提供给 `powersaved`，就将按指定的顺序处理这两个脚本或操作。守护程序首先运行外部脚本 `/usr/lib/powersave/scripts/prepare_suspend_to_disk`。在成功处理此脚本后，守护程序运行内部操作 `do_suspend_to_disk`，然后在此脚本卸载了关键模块并停止了服务后，将计算机设置为休眠方式。

可修改休眠按钮事件的操作，如 `EVENT_BUTTON_SLEEP="notify suspend_to_disk"` 中所示。在这种情况下，`X` 中会出现一个弹出窗口或者控制台上会出现一条讯息，从而提示用户操作暂停。随后，将生成事件 `EVENT_GLOBAL_SUSPEND2DISK`，从而执行指定的操作和安全暂挂方式。可以使用 `/etc/sysconfig/powersave/common` 中的变量 `NOTIFY_METHOD` 自定义内部操作 `notify`。

`/etc/sysconfig/powersave/cpufreq`

包含用来优化动态 CPU 频率设置以及是否使用用户空间或内核实施的变量。

`/etc/sysconfig/powersave/battery`

包含电池电量限制和其他电池特定的设置。

`/etc/sysconfig/powersave/sleep`

在此文件中，激活休眠方式并确定在暂停事件或待机事件之前应卸载哪些关键模块以及停止哪些服务。当系统恢复时，将重装载这些模块并重新启动这些服务。例如，甚至可以延迟已触发的休眠方式以便保存文件。默认设置主要涉及 USB 和 PCMCIA 模块。暂停或待机失败通常是由某些模块引起的。有关确定错误的详细信息，请参见 [第 28.5.4 节“查错”](#) [505]。

`/etc/sysconfig/powersave/thermal`

激活散热和热量控制。文件 `/usr/share/doc/packages/powersave/README.thermal` 中提供了有关此主题的详细信息。

`/etc/sysconfig/powersave/disk`

此配置文件包含根据硬盘所作的操作和设置。

`/etc/sysconfig/powersave/scheme_*`

提供多种耗电量与特定部署方案相适应的方案。许多方案都是预配置的，使用时无需进行更改。可以在这里保存自定义方案。

28.5.2 配置 APM 和 ACPI

暂停和待机

有三种基本的 ACPI 休眠方式和两种 APM 休眠方式：

暂停到磁盘（ACPI S4、APM 暂停）

将整个内存内容保存到硬盘。计算机完全关闭且不消耗任何电源。此休眠方式是默认启用的，并且应该在所有系统上都有效。

暂停到 RAM（ACPI S3、APM 暂停）

将所有设备的状态保存到主存储器。只有主存储器继续消耗电源。SUSE Linux Enterprise 通常不支持该休眠方式（尽管您可以对许多计算机使用它）。

默认启用该休眠方式，但只有数据库中将当前计算机列为能够支持该方式时，才会执行。该数据库包含在 `suspend` 包提供的 `/usr/sbin/s2ram` 二进制数据中。

要修改默认参数（例如，要通常情况下禁用暂挂到 `ram` 休眠方式，或者即使对数据库中未列出的计算机也强制执行它），可在 `/etc/sysconfig/powersave/sleep` 配置文件中查找关于可用选项的更多信息。

要了解关于 `s2ram` 二进制数据的更多信息，请参阅 `README` 文件（`/usr/share/doc/packages/suspend`）。

待机（ACPI S1、APM 待机）

关闭某些设备（取决于制造商）。

为了正确处理暂挂、待机和恢复，确保在文件 `/etc/sysconfig/powersave/events` 中设置了以下默认选项（SUSE Linux Enterprise 安装之后的默认设置）：

```
EVENT_GLOBAL_SUSPEND2DISK=
    "prepare_suspend_to_disk screen_saver do_suspend_to_disk"
EVENT_GLOBAL_SUSPEND2RAM=
    "prepare_suspend_to_ram screen_saver do_suspend_to_ram"
EVENT_GLOBAL_STANDBY=
    "prepare_standby screen_saver do_standby"
EVENT_GLOBAL_RESUME_SUSPEND2DISK=
    "restore_after_suspend_to_disk"
EVENT_GLOBAL_RESUME_SUSPEND2RAM=
    "restore_after_suspend_to_ram"
EVENT_GLOBAL_RESUME_STANDBY=
    "restore_after_standby"
```

自定义电池状态

文件 `/etc/sysconfig/powersave/battery` 中定义了三个电池电量水平（用百分比表示），在达到这些电池电量水平时，将触发系统警报或特定的操作。

```
BATTERY_WARNING=12
BATTERY_LOW=7
BATTERY_CRITICAL=2
```

配置文件 `/etc/sysconfig/powersave/events` 中定义了电池电量水平降至指定限度时执行的操作或脚本。可以按 [第 28.5.1 节“配置 powersave 包”](#) [500] 中所述修改按钮的标准操作。

```
EVENT_BATTERY_NORMAL="ignore"  
EVENT_BATTERY_WARNING="notify"  
EVENT_BATTERY_LOW="notify"  
EVENT_BATTERY_CRITICAL="wm_shutdown"
```

调整耗电量以适应各种情况

可以根据电源类型调整系统行为。当系统从 AC 电源断开并使用电池运行时，应降低系统的耗电量。同样，系统一连接到 AC 电源，性能就应自动提高。CPU 频率、IDE 省电功能和许多其他参数都可以进行修改。

`/etc/sysconfig/powersave/events`中定义了计算机从 AC 电源断开或连接到 AC 电源时要执行的操作。在 `/etc/sysconfig/powersave/common` 中选择要使用的方案：

```
AC_SCHEME="performance"  
BATTERY_SCHEME="powersave"
```

这些方案被储存在 `/etc/sysconfig/powersave` 下的文件中。文件名采用 `scheme_name-of-the-scheme` 的格式。该示例参考了两个模式：`scheme_performance` 和 `scheme_powersave`。`performance`、`powersave`、`presentation` 和 `acoustic` 是预配置的。借助于 YaST 电源管理模块（第 28.6 节“YaST 电源管理模块”[507]中有述），可以编辑、创建、删除现有的方案，也可以将其与不同的电源状态关联起来。

28.5.3 其他 ACPI 功能

如果您使用 ACPI，则可以控制系统对 *ACPI 按钮*（电源、休眠、机盖打开和机盖合上）的响应。在 `/etc/sysconfig/powersave/events` 中配置操作的执行。有关各个选项的解释，请参考此配置文件。

```
EVENT_BUTTON POWER="wm_shutdown"
```

当按下电源按钮后，系统将通过关闭相应的窗口管理器（KDE、GNOME、fvwm 等）进行响应。

```
EVENT_BUTTON SLEEP="suspend_to_disk"
```

当按下休眠按钮后，系统会被设置为暂挂到磁盘方式。

EVENT_BUTTON_LID_OPEN="ignore"

当机盖打开时，不执行任何操作。

EVENT_BUTTON_LID_CLOSED="screen_saver"

当机盖合上时，激活屏幕保护程序。

EVENT_OTHER="ignore"

如果守护程序遇到了未知事件，则此事件将发生。未知事件包括某些机器上的 ACPI 热键。

如果在指定时间内 CPU 负载未超过指定的限制，则可以进一步限制 CPU 性能。在 PROCESSOR_IDLE_LIMIT 中指定负载限度，在 CPU_IDLE_TIMEOUT 中指定超时值。如果 CPU 负载保持在限度之下的时间长于超时值，则将激活 EVENT_PROCESSOR_IDLE 中配置的事件。如果 CPU 再度处于忙碌状态，将执行 EVENT_PROCESSOR_BUSY。

28.5.4 查错

文件 /var/log/messages 中记录了所有错误讯息和警报。如果您未能找到所需的信息，请使用文件 /etc/sysconfig/powersave/common 中的 DEBUG 增加 powersave 讯息的详细程度。请将变量的值增加到 7，或甚至增加到 15，然后重新启动守护程序。/var/log/messages 中更详细的错误讯息应有助于您找到错误。以下几节介绍 powersave 最常见的问题。

硬件支持已激活 ACPI，但功能不工作

如果使用 ACPI 时遇到问题，请使用命令 `dmesg|grep -i acpi` 在 dmesg 的输出中搜索 ACPI 特定的讯息。可能需要更新 BIOS 来解决问题。请转到便携式计算机制造商的主页，查找已更新的 BIOS 版本，然后安装它。要求制造商遵循最新的 ACPI 规范。如果在更新 BIOS 后错误仍然存在，则按以下步骤用已更新的 DSDT 替换 BIOS 中有问题的 DSDT 表。

- 1 从 <http://acpi.sourceforge.net/dsdt/index.php> 为您的系统下载 DSDT。检查是否已解压缩并编译了此文件，如果文件扩展名是 .aml（ACPI 机器语言），则表明已完成这些操作。如果是这种情况，请继续执行第 3 步。
- 2 如果下载的表的文件扩展名是 .asl（ACPI 源语言），则必须使用 iasl（pmtools 包）对其进行编译。为此，请输入命令 `iasl -sa`

file.asl。提供了最新版本的 iasl (Intel ACPI 编译器) <http://developer.intel.com/technology/iapc/acpi/downloads.htm>

- 3 将文件 DSDT.acpi 复制到任何位置 (建议的位置为 /etc/DSDT.acpi) 。编辑 /etc/sysconfig/kernel 并相应地调整指向 DSDT 文件的路径。启动 mkinitrd (包 mkinitrd) 。一旦安装了内核并使用 mkinitrd 创建了 initrd, 引导系统时就会集成并装载已修改的 DSDT。

CPU 频率不工作

请参考内核源代码 (kernel-source) 查看是否支持您的处理器。您可能需要特殊内核模块或模块选项来激活 CPU 频率控制。/usr/src/linux/Documentation/cpu-freq/* 中提供了此信息。如果需要特殊模块或模块选项, 则通过变量 CPUFREQD_MODULE 和 CPUFREQD_MODULE_OPTS 在文件 /etc/sysconfig/powersave/cpufreq 中进行配置。

暂挂和待机不工作

ACPI 系统由于 DSDT 实现 (BIOS) 有问题, 可能在暂挂和待机中会遇到问题。如果出现这种情况, 请更新 BIOS。

在 ACPI 和 APM 系统上: 试卸载有问题的模块时, 系统被阻止执行操作或暂停事件未被触发。如果您未卸载模块或停止阻止成功暂停的服务, 也会发生相同的情况。在这两种情况下, 尝试确定阻止采用休眠方式的有问题的模块。/var/log/suspend2ram.log 和 /var/log/suspend2disk.log 中的 powersave 守护程序生成的日志文件对确定有问题的模块很有用。如果计算机未进入休眠方式, 则原因在最后卸载的模块上。请配置 /etc/sysconfig/powersave/sleep 中的下列设置以在暂停或待机前卸载有问题的模块。

```
UNLOAD_MODULES_BEFORE_SUSPEND2DISK=""
UNLOAD_MODULES_BEFORE_SUSPEND2RAM=""
UNLOAD_MODULES_BEFORE_STANDBY=""
SUSPEND2DISK_RESTART_SERVICES=""
SUSPEND2RAM_RESTART_SERVICES=""
STANDBY_RESTART_SERVICES=""
```

如果您在不断变化的网络环境中使用暂停或待机, 或将暂停或待机用于远程装入的文件系统 (例如 Samba 和 NIS), 请使用 automounter 装入它们, 或在上述变量中添加相应的服务, 例如 smbfs 或 nfs。在远程装入的文件系统进入暂停或待机前, 如果某个应用程序访问此文件系统, 则无法正确停止服务且无法

正确卸装该文件系统。在恢复系统后，文件系统可能被损坏，因此必须重装入文件系统。

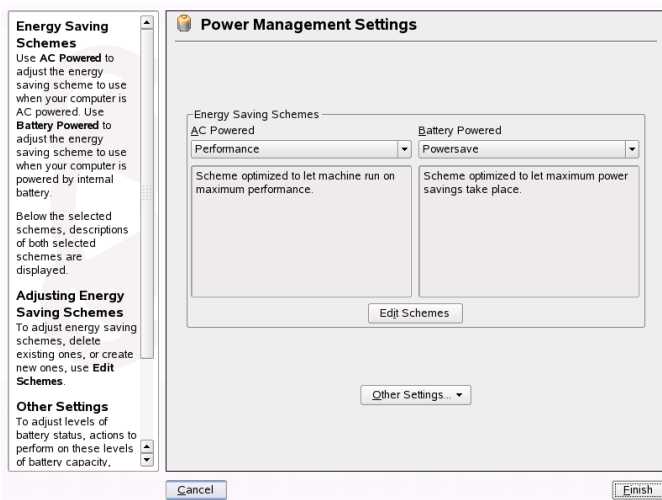
28.5.5 有关详细信息

- `/usr/share/doc/packages/powersave` — 本地 Powersave 守护程序文档
- <http://powersave.sourceforge.net> — 最新 powersave 守护程序文档
- http://www.opensuse.org/Projects_Powersave — openSUSE wiki 中的项目页

28.6 YaST 电源管理模块

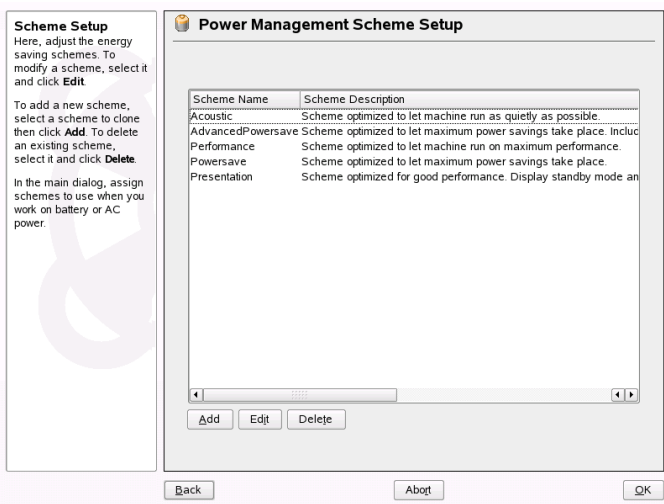
YaST 电源管理模块可以配置先前所述的所有电源管理设置。在通过系统 > 电源管理从“YaST 控制中心”启动此模块时，会打开此模块的第一个对话框（请参阅图 28.1 “方案选择” [507]）。

图 28.1 方案选择



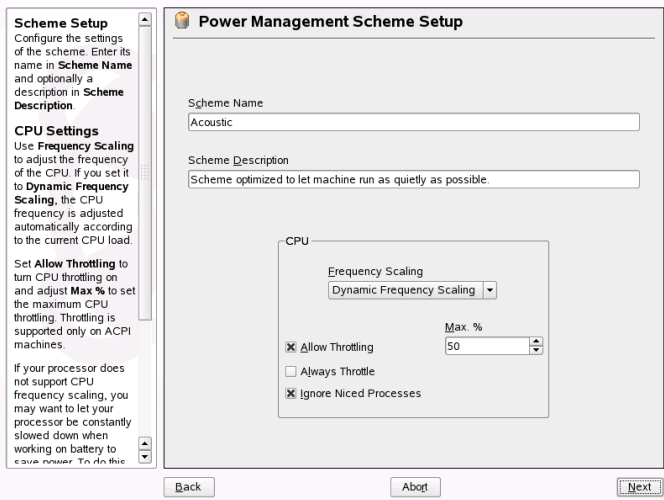
在此对话框中，选择使用电池运行和使用 AC 运行时要使用的方案。要添加或修改方案，请单击 **编辑方案**，这将打开现有方案的概述，如 **图 28.2 “现有方案的概述”** [508] 所示。

图 28.2 现有方案的概述



在方案概述中，选择要修改的方案，然后单击 **编辑**。要创建新方案，请单击 **添加**。这两种情况打开的是同一个对话框，如 **图 28.3 “配置方案”** [509] 所示。

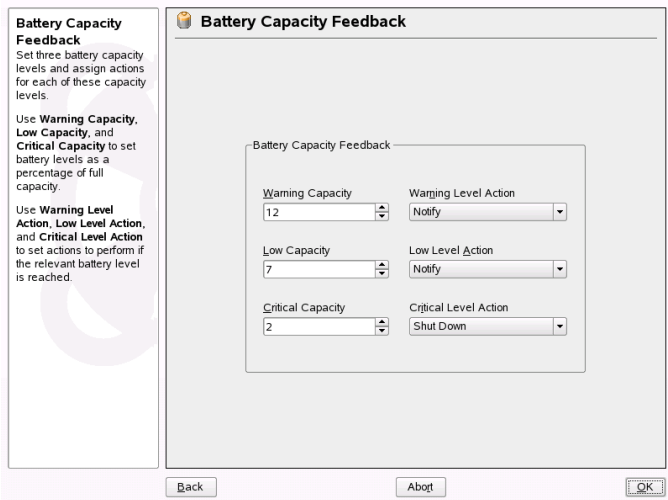
图 28.3 配置方案



首先，为新方案或已编辑的方案输入合适的名称和说明。确定此方案是否应控制 CPU 性能及如何控制 CPU 性能。确定是否应使用频率调节和节流以及应使用的频率调节和节流范围，确定调整 CPU 频率时是否应忽略低优先级进程（低优先级进程）。随后的对话框是针对硬盘的，它定义了待机策略是为实现最佳性能还是为实现最大省电。声音策略控制硬盘的噪音级别（少数几种硬盘支持这一功能）。散热策略确定要使用的散热方法。遗憾的是 BIOS 很少支持这种类型的热量控制。请阅读 `/usr/share/doc/packages/powersave/powersave_manual.html#Thermal` 以了解如何使用风扇和被动散热方法。

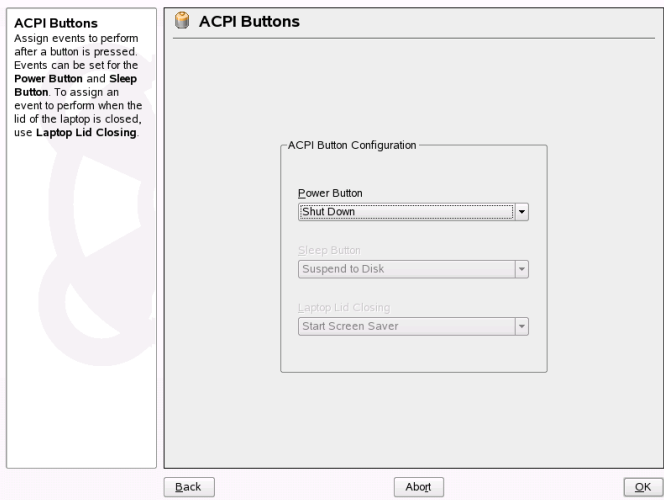
可以在最初的对话框中使用电池警告、ACPI 设置或暂挂权限进行全局电源管理设置。通过单击其他设置并从菜单选择相应项来访问这些控制。单击电池警告以访问电池电量水平对话框，如图 28.4 “电池电量水平” [510] 所示。

图 28.4 电池电量水平



每当电量水平降至特定的可配置限制之下时，系统的BIOS就会通知操作系统。在此对话框中定义三个限制：警告电量、电量低和临界电量。当电量水平降至这些限制之下时将触发特定的操作。通常，前两个状态只触发发送给用户的通知。第三个关键电量水平触发关闭操作，原因是剩余的电量不足以支持系统继续运行。选择合适的电量水平和所需的操作，然后单击确定返回到起始对话框。

图 28.5 ACPI 设置



通过 *ACPI* 设置访问用于配置 *ACPI* 按钮的对话框。图 28.5 “*ACPI* 设置” [511] 中显示了这一工具。对 *ACPI* 按钮进行的设置确定系统应如何对特定的开关进行响应。配置系统对按电源按钮、按休眠按钮和合上便携式计算机盖的响应。单击确定完成配置并返回到起始对话框。

单击启用暂停进入一个对话框，可以在这个对话框中确定此系统的用户是否及如何使用暂停或待机功能。单击确定返回到主对话框。再次单击确定退出此模块并确认您的电源管理设置。

无线通讯

可以通过多种方法使用 Linux 系统与其他计算机、手提电话或外围设备进行通信。WLAN（无线 LAN）可用于将便携式计算机联网。蓝牙可用于将单独的系统部件（鼠标、键盘）、外围设备、手提电话、PDA 和单独的计算机互相连接。IrDA 通常用于与 PDA 或手提电话的通讯。全球移动通信系统 (UMTS) 也称为 3G，可以提供几种多媒体服务，例如浏览万维网或收发讯息。本章介绍这些技术及其配置。

29.1 无线 LAN

无线 LAN 已成为移动计算的不可缺少的一部分。当今，大多数笔记本电脑都配有内置 WLAN 卡。用于 WLAN 卡无线通讯的 802.11 标准是由 IEEE 组织制订的。最初，此标准实现的最大传送速率是 2 Mbit/s。此后，此标准进行了多次补充以提高数据传送速率。这些补充定义了调制、传送输出和传送速率等详细内容：

表 29.1 各种 WLAN 标准的概述

名称	频带 (GHz)	最大传送速率 (MBit/s)	记事
802.11	2.4	2	已过时；目前市场上不销售采用此标准的最终设备
802.11b	2.4	11	广泛采用
802.11a	5	54	较少使用
802.11g	2.4	54	向后兼容 11b

此外还有一些专有标准，如 Texas Instruments 对 802.11b 进行调整后形成的标准（有时也称为 802.11b+），其最大传送速率为 22 Mbit/s。但采用这种标准的卡的普及程度有限。

29.1.1 硬件

SUSE Linux Enterprise® 不支持 802.11 卡。支持采用 802.11a、802.11b 和 802.11g 的大多数卡。现在新推出的卡通常符合 802.11g 标准，但采用 802.11b 的卡仍然是可用的。通常，支持具有以下芯片的卡：

- Aironet 4500、4800
- Atheros 5210、5211、5212
- Atmel at76c502、at76c503、at76c504、at76c506
- Intel PRO/Wireless 2100、2200BG、2915ABG 和 3945ABG
- Intersil Prism2/2.5/3
- Intersil PrismGT
- Lucent/Agere Hermes
- Texas Instruments ACX100、ACX111

- ZyDAS zd1201

还支持许多很少用到且市面上不再有售的较早的卡。*Absolute Value Systems* 的万维网站点中提供了一个列表，详尽列出了各种 WLAN 卡及其使用的芯片，网址是：http://www.linux-wlan.org/docs/wlan_adapters.html.gz 查找各种 WLAN 芯片的概述：<http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/ListeChipsatz>。

有些卡需要固件映像，该映像必须在初始化驱动程序时载入卡中。Intersil PrismGT、Atmel 以及 TI ACX100 和 ACX111 就是这种情况。使用 YaST 联机更新可以方便地安装固件。SUSE Linux Enterprise 附带了 Intel PRO/Wireless 卡的固件，在检测到此类型的卡时，YaST 将自动安装该卡。已安装系统的 `/usr/share/doc/packages/wireless-tools/README.firmware` 中提供了有关此主题的详细信息。

29.1.2 功能

在无线联网中，会使用各种技术和配置来确保连接的快速、高质量和安全。不同的操作类型适合不同的设置。很难选择正确的鉴定方法。各种可用加密方法有各自的优点和缺陷。

操作方式

无线网络基本上可分为受管网络和特殊网络。受管网络具有一个管理元素，即访问点。在这种方式（也称为基础结构方式）中，WLAN 工作站在网络中的所有连接都通过访问点运行，后者也可用作与以太网的连接。特殊网络没有访问点。各个工作站直接互相通讯。在特殊网络中，传送范围和参与工作站的数目都受到很大限制。因此，采用访问点通常更加有效。甚至可以将 WLAN 卡用作访问点。大多数卡支持此功能。

与使用缆线连接的网络相比，无线网络中的数据更容易被截获，无线网络更容易受到攻击，所以各标准都包括了鉴定和加密方法。IEEE 802.11 标准最初的版本在术语 WEP 下对这些方法进行了说明。但是，WEP 被证明是不安全的（请参见“**安全性**”一节 [521]），因此 WLAN 行业（组织名为 *Wi-Fi 联盟*）制订了一个名为 WPA 的新扩展，用以弥补 WEP 的缺陷。后来的 IEEE 802.11i 标准（也称为 WPA2，因为 WPA 基于 802.11i 的草案版本）包括 WPA 和其他一些鉴定和加密方法。

鉴定

为了确保只有经过授权的工作站才能连接，受管网络中使用了多种鉴定机制：

打开

开放系统是不要求鉴定的系统。任何工作站都可以加入网络。不过，可以使用 WEP 加密（请参见“加密”一节 [517]）。

共享密钥（按照 IEEE 802.11）

在此过程中，使用 WEP 密钥进行鉴定。但不建议采用此过程，因为它使 WEP 密钥容易受到攻击。攻击者所要做的一切就是侦听工作站和访问点之间的通讯足够长时间。在鉴定过程中，双方将交换相同的信息，一次使用的是加密形式，一次使用的是未加密形式。这使得可以使用适当的工具来重建密钥。由于方法使用 WEP 密钥来进行鉴定和加密，因此不能提高网络的安全性。具有正确 WEP 密钥的工作站可以鉴定、加密和解密。不具有密钥的工作站无法解密接收到的包。因此，无论它是否必须对本身进行鉴定都不能进行通讯。

WPA-PSK（按照 IEEE 802.1x）

WPA-PSK（PSK 代表“预共享密钥”）的工作方式与共享密钥过程类似。所有参与工作站和访问点需要相同的密钥。该密钥长度为 256 位，通常以密码短语形式输入。此系统不需要像 WPA-EAP 那样的复杂密钥管理，并且更适合个人使用。因此，有时将 WPA-PSK 称为 WPA“家庭”。“”

WPA-EAP（按照 IEEE 802.1x）

实际上，WPA-EAP 不是一个鉴定系统，而是一个传输鉴定信息的协议。WPA-EAP 用于保护企业中的无线网络。在个人网络中，很少使用 WPA-EAP。因此，WPA-EAP 有时称为 WPA“企业”。“”

WPA-EAP 需要 Radius 服务器来鉴定用户。EAP 提供了连接和鉴定服务器的三种不同方式：TLS (Transport Layer Security)、TTLS (Tunneled Transport Layer Security) 和 PEAP (Protected Extensible Authentication Protocol)。在 nutshell 中，这些选项的作用如下所示：

EAP-TLS

TLS 鉴定依赖于服务器和客户机的证书互相交换。首先，服务器为客户机（客户机会评估服务器）提供其证书。如果证书被认为有效，则接下来客户机会对服务器提供其证书。当 TLS 是安全的，它要求在网络中具有运转的认证管理基础结构。此基础结构在专用网络中很少见。

EAP-TTLS 和 PEAP

TTLS 和 PEAP 都是两个阶段的协议。在第一个阶段，将建立安全性，在第二个阶段，将交换客户机鉴定数据。在需要认证管理的情况下，它们所需的认证管理费用比 TLS 要少得多。

加密

有多种加密方法可确保所有未授权用户不能读取无线网络中交换的数据包并且不能访问网络：

WEP（在 IEEE 802.11 中定义）

此标准使用 RC4 加密算法，最初密钥长度为 40 位，后来也使用 104 位的密钥。通常，将此长度声明为 64 位或 128 位，这取决于是否包括初始化矢量的 24 位。但是，此标准有一些缺陷。攻击者能够成功攻击此系统生成的密钥。不过，使用 WEP 总比根本不加密网络要好。

TKIP（在 WPA/IEEE 802.11i 中定义）

WPA 标准中定义的这一密钥管理协议使用与 WEP 相同的加密算法，但弥补了其缺陷。由于为每个数据包生成一个新密钥，从而有效阻止了对这些密钥的攻击。TKIP 与 WPA-PSK 一起使用。

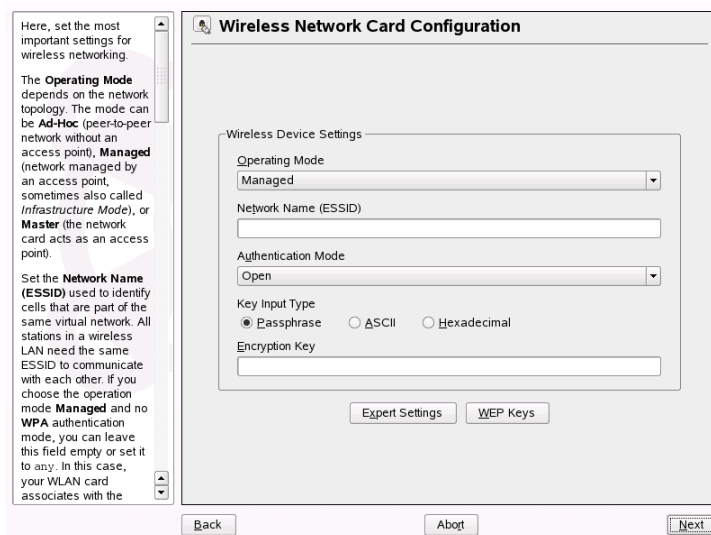
CCMP（在 IEEE 802.11i 中定义）

CCMP 对密钥管理进行了说明。通常，它用于与 WPA-EAP 连接，但也可以与 WPA-PSK 一起使用。加密依照 AES 进行，该加密比 WEP 标准的 RC4 加密更强大。

29.1.3 用 YaST 配置

要配置您的无线网卡，请启动 YaST 网卡模块。还可在此处选择是使用 YaST 还是使用 NetworkManager 来管理网卡。如果选择 YaST，则在网络地址设置中选择设备类型无线，然后单击下一步。在无线网卡配置（如图 29.1 “YaST：配置无线网卡” [518] 所示）中为 WLAN 操作进行基本设置：

图 29.1 YaST: 配置无线网卡



操作方式

我们可以将工作站以三种不同的方式集成到 WLAN 中。适用的模式取决于通讯所用的网络：特殊网络（对等网络，无访问点）、受管网络（网络由访问点管理）或者主网络（您的网卡应用作访问点）。要使用 WPA-PSK 或 WPA-EAP 方式，必须将操作方式设置为受控。

网络名称 (ESSID)

为实现相互通讯，无线网络中的所有工作站都需要相同的 ESSID。如果未指定任何内容，则网卡会自动选择一个访问点，但它可能不是您所希望使用的。

鉴定方式

为您的网络选择合适的鉴定方式：开放、共享密钥、WPA-PSK 或 WPA-EAP。如果选择了 WPA 鉴定，则必须设置网络名称。

专家设置

单击此按钮将打开一个对话框，用于对 WLAN 连接进行详细配置。下面的内容提供了此对话框的详细说明。

完成基本设置后，即可将您的工作站部署在 WLAN 中。

重要: 无线网络中的安全性

确保使用所支持的鉴定和加密方法之一来保护您的网络通讯。如果未加密 WLAN 连接, 则第三方便可以截获所有网络数据。即使进行弱加密 (WEP) 也比根本不加密要好。相关信息请参考 [“加密”一节 \[517\]](#) 和 [“安全性”一节 \[521\]](#)。

根据所选的鉴定方法, YaST 会提示您在另一个对话框中微调这些设置。对于 *开放*, 无需进行任何配置, 因为此设置实施的是无需鉴定的未加密操作。

共享密钥

设置密钥输入类型。选择 *通行密码*、*ASCII* 或 *十六进制*。您最多可以保留 4 个不同的密钥来加密所传送的数据。单击 *WEP 密钥* 进入密钥配置对话框。设置密钥长度: *128 位* 或 *64 位*。默认设置是 *128 位*。在对话框底部的列表区域中, 最多可以指定 4 个不同的密钥, 您的工作站将使用这些密钥进行加密。按 *设置默认密钥* 可将其中一个密钥定义为默认密钥。除非更改默认设置, 否则 YaST 会将第一个输入的密钥用作默认密钥。如果删除了标准密钥, 则必须将其他密钥中的一个手动标记为默认密钥。单击 *编辑* 可以修改现有列表项或创建新密钥。此时将出现一个弹出窗口, 提示您选择输入类型 (*通行密码*、*ASCII* 或 *十六进制*)。如果选择的是 *通行密码*, 则输入一个单词或字符串, 将从该单词或字符串按照先前指定的长度生成密钥。*ASCII* 要求为 *64 位* 密钥输入 5 个字符, 为 *128 位* 密钥输入 13 个字符。如果选择的是 *十六进制*, 则按照十六进制表示法为 *64 位* 密钥输入 10 个字符, 或为 *128 位* 密钥输入 26 个字符。

WPA-PSK

要输入用于 WPA-PSK 的密钥, 请选择输入方法 *通行密码* 或 *十六进制*。在 *通行密码* 方式下, 输入必须为 8 到 63 个字符。在 *十六进制* 方式下, 请输入 64 个字符。

WPA-EAP

输入网络管理员提供的身份凭证。对于 TLS, 请提供身份、*客户机证书*、*客户机密钥* 和 *服务器证书*。TTLS 和 PEAP 需要身份和密码。*服务器证书* 和 *匿名身份* 为可选。YaST 会在 /etc/cert 下搜索所有证书, 因此将提供给您的证书保存到此位置中并将这些文件的访问权限限制为 0600 (所有者读写)。

单击 *细节* 可进入 WPA-EAP 设置的高级鉴定对话框。选择 *EAP-TTLS* 或 *EAP-PEAP* 通信第二阶段的鉴定方法。如果在前面的对话框中已选择 TTLS, 则选择任意、MD5、GTC、CHAP、PAP、MSCHAPv1 或 MSCHAPv2。如果

已选择 **PEAP**，则选择任意、MD5、GTC 或 MSCHAPv2。如果自动确定的设置不起作用，则 **PEAP** 版本可用于强制使用特定的 **PEAP** 实施。

单击 **专家设置** 可退出 **WLAN** 连接的基本配置对话框并进入专家配置对话框。此对话框中有以下选项可用：

通道

只有在特殊和主方式下才需要指定 **WLAN** 工作站要在其上工作的通道。在受控方式下，网卡将自动搜索访问点的可用通道。在特殊方式下，可从提供的 12 个通道中选择一个，用于在您的工作站和其他工作站之间进行通信。在主方式下，确定您的网卡应该在哪个通道上提供访问点功能。此选项的默认设置是 *自动*。

位速率

根据网络的性能，您可能要为从一点到另一点之间的传送设置特定位速率。在默认设置 *自动* 中，系统会尽可能地使用最高数据传送速率。一些 **WLAN** 卡不支持比特率设置。

接入点

在具有多个访问点的环境中，通过指定 **MAC** 地址可以预先选择多个访问点中的一个。

29.1.4 实用程序

hostap（包 **hostap**）用于将 **WLAN** 卡作为访问点运行。有关此软件包的详细信息，请访问项目主页 (<http://hostap.epitest.fi/>)。

kismet（包 **kismet**）是一个网络诊断工具，使用它可以监听 **WLAN** 包流量。通过这种方式，您可以检测到网络中的所有入侵企图。有关详细信息，请参见手册页和 <http://www.kismetwireless.net/>。

29.1.5 建立 **WLAN** 的提示和技巧

这些提示可帮助精确调整 **WLAN** 的速度、稳定性和安全性。

稳定性和速度

无线网络的性能和可靠性主要取决于参与的工作站是否能够清楚地接收到来自其他工作站的信号。障碍物（例如，墙壁）极大地削弱了信号。信号强度越低，传送速率就越慢。在网络运行过程中，可以在命令行（Link Quality 字段）中使用 Iwconfig 实用程序或使用 NetworkManager 或 KNetworkManager 来检查信号强度。如果信号质量存在问题，可尝试将设备放在其他位置，或调整访问点天线的位置。很多 PCMCIA WLAN 卡都配有辅助天线，可充分提高接收效果。制造商指定的速率（例如 54Mbit/s）是一个额定值，它表示理论最大值。实际上，最大数据吞吐量不大于该值的一半。

安全性

如果要建立一个无线网络，则一定要记住，如果不实施任何安全措施，则传送范围内的任何人都可以方便地访问此网络。因此，一定要激活某种加密方法。所有 WLAN 卡和访问点都支持 WEP 加密。虽然这并非完全安全，但还是对潜在攻击者设置了一道屏障。WEP 通常可满足个人使用。WPA-PSK 的安全性更好，但不能在较早的访问点或具有 WLAN 功能的路由器中实施。在某些设备上，可以通过固件更新来实施 WPAu163 此外，Linux 在所有硬件组件上不支持 WPA。在准备此文档时，WPA 只适用于采用 Atheros、Intel PRO/Wireless 或 Prism2/2.5/3 芯片的卡。在 Prism2/2.5/3 上，仅当使用 hostap 驱动程序时，WPA 才能运行（请参见“有关 Prism2 卡的问题”一节 [522]）。如果 WPA 不可用，则使用 WEP 要好过不加密。在具有高级安全要求的企业中，无线网络工作时必须采用 WPA。

29.1.6 查错

如果 WLAN 卡未能作出响应，请检查您是否下载了所需的固件。请参考第 29.1.1 节“硬件” [514]。以下几段介绍了一些常见问题。

多个网络设备

现在的便携式计算机通常都有网卡和 WLAN 卡，如果使用 DHCP（自动地址指派）来配置这两个设备，则您可能会遇到名称解析和默认网关的问题。可以 Ping 路由器但不能浏览因特网就是这方面问题的典型示例。位于 http://en.opensuse.org/SDB:Name_Resolution_Does_Not_Work_with

[_Several_Concurrent_DHCP_Clients](#) 的支持数据库提供了一篇有关这一主题的文章。

有关 Prism2 卡的问题

采用 Prism2 芯片的设备有多个驱动程序可用。不同的卡与不同的驱动程序之间的适用性是不一样的。使用这些卡时，只有在使用 hostap 驱动程序时，才能实施 WPA。如果这样的卡不能正常工作或根本不工作，或者您要使用 WPA，请参见 `/usr/share/doc/packages/wireless-tools/README.prism2`。

WPA

SUSE Linux Enterprise 是最近才支持 WPA 的，并且仍然在开发中。因此，YaST 并不支持配置所有 WPA 鉴定方法。不是所有无线 LAN 卡和驱动程序都支持 WPA。一些卡需要更新固件以启动 WPA。如果要使用 WPA，请参见 `/usr/share/doc/packages/wireless-tools/README.wpa`。

29.1.7 有关详细信息

Jean Tourrilhes 开发了用于 Linux 的无线工具，他的因特网网页上有很多关于无线网络的有用信息。请参见http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html。

29.2 蓝牙

蓝牙是用于连接各种设备（例如，移动电话、PDA、外围设备、便携式计算机，或者键盘或鼠标等系统部件）的无线技术。蓝牙 (Bluetooth) 取自丹麦国王 Harold Bluetooth 的名字，正是他结束了斯堪的纳维亚半岛分裂混战的状态。蓝牙徽标是以 Rune（古代北欧文字）的“H”（像一颗星星）和“B”的组合为基础设计的。

蓝牙在多个重要方面区别于 IrDA。首先，各个设备不需要直接“看到”对方；其次，可以在网络中连接多个设备。但最大数据传送速率是 720Kbps（在当前版本 1.2 中）。理论上，蓝牙甚至可以穿墙进行通讯。但实际上，这取决于墙和设备类的属性。有三种设备类的传送范围在 10 到 100 米之间。

29.2.1 基础

以下几节介绍了蓝牙的基本工作原理。了解需要符合哪些软件要求、蓝牙如何与系统交互以及蓝牙配置文件的工作原理。

软件

为了能够使用蓝牙，您需要蓝牙适配器（内置适配器或外部设备均可）、驱动器和蓝牙协议堆栈。Linux 内核已包含使用蓝牙所需的基本驱动程序。Bluez 系统用作协议堆栈。为了确保应用程序能使用蓝牙，必须安装基础包 `bluez-libs` 和 `bluez-utils`。这些包提供了多个所需的服务和实用程序。此外，某些适配器（如 **Broadcom** 或 **AVM BlueFritz!**）需要安装 `bluez-firmware` 包。`bluez-cups` 包支持通过蓝牙连接进行打印。如果想调试 Bluetooth 连接中的问题，请安装程序包 `bluez-hcidump`。

常规交互

蓝牙系统由 4 个提供所需功能的互相关联的层组成：

硬件

实现 Linux 内核支持所需的适配器和合适的驱动程序。

配置文件

用于控制蓝牙系统。

守护程序

由配置文件控制并提供功能的服务。

应用程序

应用程序允许用户使用和控制守护程序提供的功能。

当插入蓝牙适配器时，热插拔系统将装载相应的驱动程序。在装载驱动程序后，系统检查配置文件以查看是否要启动蓝牙。如果要启动蓝牙，则它确定要启动的服务。根据此信息，启动相应的守护程序。安装时检测蓝牙适配器。如果找到一个或多个蓝牙适配器，则启用蓝牙。否则取消激活蓝牙系统。此后添加的任何蓝牙设备都必须手动启用。

配置文件

在蓝牙中，服务是通过配置文件（例如，文件传送配置文件、基本打印配置文件和个域网配置文件）进行定义的。为使某台设备能使用另一台设备的服务，这两台设备都必须理解同一个配置文件，即设备包和手册中通常缺少的一些信息。遗憾的是，某些制造商没有严格遵守各配置文件的定义。不过，设备间的通讯通常能顺畅进行。

在下文中，本地设备是在物理上与计算机连接的那些设备。而只能通过无线连接进行访问的所有其他设备都被称为远程设备。

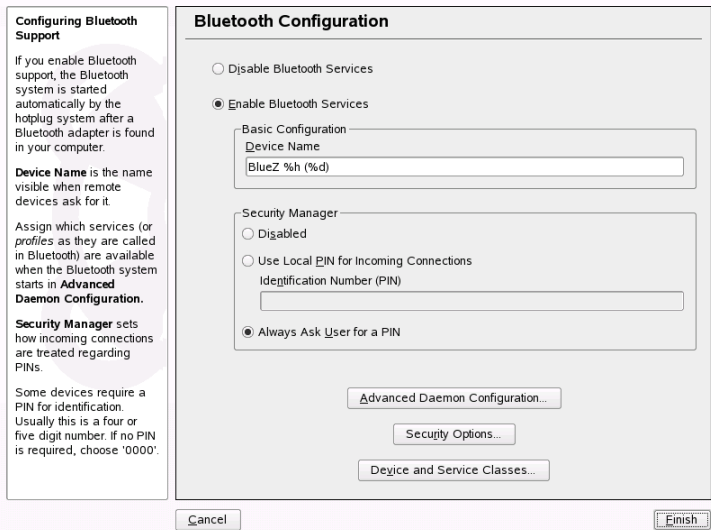
29.2.2 配置

本节介绍蓝牙配置。了解涉及哪些配置文件、需要哪些工具以及如何使用 YaST 或手动配置蓝牙。

使用 YaST 配置蓝牙

使用 YaST 蓝牙模块（如 [图 29.2 “YaST 蓝牙配置”](#) [525] 中所示）在系统上配置蓝牙支持。一旦热插拔在系统中检测到蓝牙适配器（例如，在引导时或插入适配器时），将使用该模块中配置的设置自动启动蓝牙。

图 29.2 YaST 蓝牙配置



配置的第一步是确定在您的系统中是否要启动蓝牙服务。如果已启用了蓝牙服务，则可以配置两项内容。首先配置设备名。这是您的计算机被发现时其他设备显示的名称。有两个占位符可用，其中 %h 代表系统的主机名（这很有用，例如，如果主机名由 DHCP 动态分配），而 %d 则插入接口号（只有在计算机中安装了多个蓝牙适配器时才有用）。例如，如果在此字段中输入 Laptop %h 且 DHCP 将名称 unit123 指派给计算机，则其他远程设备将您的计算机识别为 Laptop unit123。

参数安全性管理器与远程设备尝试连接时本地系统的行为相关。不同之处是在对 PIN 码的处理上。这种处理要么允许任何设备不使用 PIN 进行连接，要么确定在需要 PIN 时如何选择正确的 PIN。可在相应的输入字段中输入 PIN（储存在配置文件中）。如果设备尝试连接，则它首先使用这个 PIN。如果连接失败，则它切换为不使用 PIN 进行连接。为获得最大的安全性，最好选择始终要求用户提供 PIN。此选项允许您对不同的（远程）设备使用不同的 PIN。

单击高级守护程序配置进入用于选择和配置可用服务（在蓝牙中称为配置文件）的对话框。所有可用服务都显示在列表中，可以通过单击激活或取消激活启用或禁用这些服务。单击编辑打开一个对话框，可以在这个对话框中为所选服务（守护程序）指定其他参数。除非您熟悉服务，否则请不要进行任何更改。在完成守护程序的配置后，单击确定退出此对话框。

回到主对话框中，单击安全性选项进入安全性对话框并指定加密、鉴定和扫描设置。然后，退出安全性对话框返回主对话框。在单击完成关闭主对话框后，就可以使用蓝牙系统了。

您还可以从主对话框进入设备和服务类对话框。蓝牙设备被分为不同的设备类。请在此对话框中为您的计算机选择正确的设备类，如台式计算机或便携式计算机。与服务类不同，设备类不太重要，但也在这里进行设置。有时，远程蓝牙设备（如移动电话）如果可以检测到在系统中设置的正确服务类，则只允许特定的功能。对于要在允许与计算机之间传送文件之前获得名为“对象传送”类的移动电话而言，往往是这种情况。您可以选择多个类。但无需为了“以防万一”而选择所有的类。“”在大多数情况下，默认选择应足够了。

要使用蓝牙设置网络，请激活高级守护程序配置对话框中的 *PAND*，然后单击编辑设置守护程序的方式。对于一个有效的蓝牙网络连接，一个 *pand* 必须在监听方式下运行，而对应的同级必须在搜索方式下运行。默认情况下，预设值为监听方式。调整本地 *pand* 的行为。此外，在 YaST 网卡模块中配置 *bnepX* 接口（*x* 代表系统中的设备编号）。

手动配置蓝牙

Bluez 系统各个部件的配置文件都位于目录 `/etc/bluetooth` 中。唯一的例外是用于启动部件的文件 `/etc/sysconfig/bluetooth`，该文件由 YaST 模块进行修改。

只有用户 `root` 可以修改下面介绍的配置文件。目前，尚没有用于更改所有设置的图形用户界面。可以使用 YaST 蓝牙模块设置最重要的设置，如“使用 YaST 配置蓝牙”一节 [524] 中所述。所有其他设置都只能在出现特殊情况时由有经验的用户进行设置。通常，默认设置就能满足要求。

使用 PIN 号码可以基本防止不需要的连接。移动电话在建立第一个联系时（或在电话上建立设备联系时）通常查询 PIN。为使两台设备能进行通讯，这两台设备必须用相同的 PIN 对自身进行标识。在计算机上，PIN 位于文件 `/etc/bluetooth/pin` 中。

重要：蓝牙连接的安全性

尽管有 PIN，但两台设备之间的数据传送也不是完全安全的。默认情况下，蓝牙连接的鉴定和加密处于取消激活状态。对某些蓝牙设备而言，激活鉴定和加密可能产生通信问题。

可以在配置文件 `/etc/bluetooth/hcid.conf` 中更改各种设置，例如设备名和安全性方式。通常，默认设置可以满足要求。此文件包含介绍各个设置选项的注释。

所包含文件中有两部分分别被指定为 `options` 和 `device`。前一部分包含 `hcid` 用于启动的一般信息，后一部分包含用于各个本地蓝牙设备的设置。

`options` 部分中最重要的设置之一是 `security auto;`。如果设置为 `auto`，则 `hcid` 尝试对进来的连接使用本地 PIN。如果失败，则它切换到 `none` 并建立连接。为提高安全性，应将默认设置设置为 `user`，以确保每次建立连接时都要求用户输入 PIN。

在 `device` 部分设置在另一个设备中显示该计算机所使用的设备名。本部分定义设备类，例如台式机、便携式计算机或服务器。还在这里启用或禁用鉴定和加密。

29.2.3 系统部件和实用程序

蓝牙的可操作性取决于各种服务的交互。至少需要两个后台守护程序：`hcid`（主机控制器接口守护程序）和 `sdpd`（服务发现协议守护程序），前者充当蓝牙设备的接口并控制蓝牙设备，而通过后者设备可以找到主机提供的服务。如果在启动系统时未自动激活 `hcid` 和 `sdpd`，则可以使用命令 `rcbluetooth start` 激活这两个守护程序。必须以 `root` 用户身份执行此命令。

下面几段简要介绍了可用于使用蓝牙的最重要的 `Shell` 工具。尽管现在可以使用各种图形组件来控制蓝牙，但这些程序也值得您去关注。

某些命令只能以 `root` 用户身份执行。这包含用于测试远程设备连接的命令 `l2pingdevice_address`。

hcitool

使用 `hcitool` 来确定是否检测到本地和远程的设备。命令 `hcitool dev` 列出本地设备。输出为每个检测到的本地设备生成一行，格式为 `interface_namedevice_address`。

可以使用命令 `hcitool inq` 搜索远程设备。对每个检测到的设备将返回三个值：设备地址、时钟偏差和设备类。设备地址很重要，因为其他命令用它来标

识目标设备。时钟偏差主要用于技术目的。而设备类以十六进制值的形式指定设备类型和服务类型。

使用 `hcitool` 名称设备地址来确定远程设备的设备名称。对于远程计算机，设备类和设备名对应于其 `/etc/bluetooth/hcid.conf` 中的信息。使用本地设备地址将生成错误输出。

hciconfig

命令 `/usr/sbin/hciconfig` 提供有关本地设备的详细信息。如果不带任何参数执行 `hciconfig`，则输出将显示设备名 (`hciX`) 等设备信息、物理设备地址 (12 位数字，形式为 `00:12:34:56:78`) 和有关已传送数据量的信息。

`hciconfig hci0 name` 显示当您的计算机接收来自远程设备的请求时它返回的名称。除查询本地设备的设置外，`hciconfig` 还可修改这些设置。例如，`hciconfig hci0 name TEST` 将名称设置为 `TEST`。

sdptool

通过特定的设备使用 `sdptool` 来检查哪个服务是可用的。命令 `sdptool browse device_address` 返回某个设备的所有服务。使用命令 `sdptool search service_code` 搜索特定的服务。此命令扫描所有可访问的设备来搜索请求的服务。如果其中一台设备提供服务，则此程序将输出此设备返回的完整服务名及简短说明。输入不带参数的 `sdptool` 可以查看所有可能的服务代码列表。

29.2.4 图形应用程序

在 *Konqueror* 中，输入 URL `bluetooth:/` 列出本地和远程蓝牙设备。双击某个设备可以获得此设备提供的服务的概述。如果将鼠标指针移过其中一个指定的服务，则浏览器的状态栏将显示将哪个配置文件用于此服务。如果您单击服务，会出现对话框，询问您要保存、使用服务（必须启动应用程序）还是取消操作。如果您不希望此对话框再次显示，而是要始终执行所选的操作，则选中特定复选框。对于某些服务，尚不提供支持。而对于其他服务，可能需要安装附加包。

29.2.5 示例

本节介绍两个典型的可能蓝牙方案的示例。第一个示例说明如何通过蓝牙在两台主机之间建立网络连接。第二个示例介绍计算机和移动电话之间的连接。

两台主机间的网络连接

在第一个示例中，在主机 *H1* 和 *H2* 之间建立网络连接。这两台主机包含蓝牙设备地址 *baddr1* 和 *baddr2*（通过上面介绍的 `hcitooldev` 命令在这两台主机上确定）。应用 IP 地址 192.168.1.3 (*H1*) 和 192.168.1.4 (*H2*) 标识这两台主机。

蓝牙连接是借助 `pand`（personal area networking daemon，个人域网络守护程序）建立的。必须由用户 `root` 执行以下命令。这里主要介绍蓝牙特定的操作，不提供网络命令 `ip` 的详细说明。

输入命令 `pand -s` 在主机 *H1* 上启动 `pand`。随后，可以通过命令 `pand -c baddr1` 在主机 *H2* 上建立连接。如果您在其中一台主机上输入 `ip link show` 以列出可用的网络接口，则输出应包含如下所示的项：

```
bnep0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000  
link/ether 00:12:34:56:89:90 brd ff:ff:ff:ff:ff:ff
```

输出应包含本地设备地址 *baddr1* 或 *baddr2*，而不是 `00::12::34:56:89:90`。现在，必须为此接口指派一个 IP 地址并将此接口激活。在 *H1* 上，使用以下两个命令执行此操作：

```
ip addr add 192.168.1.3/24 dev bnep0  
ip link set bnep0 up
```

在 *H2* 上，使用以下命令：

```
ip addr add 192.168.1.4/24 dev bnep0  
ip link set bnep0 up
```

现在，可从 IP 地址为 192.168.1.3 的 *H2* 访问 *H1*。使用命令 `ssh 192.168.1.4` 从 *H1* 访问 *H2*（假定 *H2* 运行 `sshd`，SUSE Linux Enterprise® 中默认激活此程序）。也可以以普通用户身份运行命令 `ssh 192.168.1.4`。

将数据从移动电话传送到计算机

第二个示例说明如何将使用带有内置数码相机的移动电话拍摄的照片传送到计算机（传送多媒体讯息不会产生额外的费用）。尽管各种移动电话上的菜单结构有所不同，但过程通常十分类似。如有必要，请参考您的电话的手册。本示例介绍将 Sony Ericsson 移动电话中的照片传送到便携式计算机的过程。计算机上必须提供服务 Obex-Push，并且计算机必须向移动电话授予访问权限。第一步是在便携式计算机上使服务可用。需要在便携式计算机上运行特殊的服务守护程序才能从电话获取数据。如果安装了程序包 kbluetooth，则不需要启动特殊的守护程序。如果没有安装 kbluetooth，则请使用 bluez-utils 程序包中的 opd 守护程序。用以下命令启动该守护程序：

```
opd --mode OBEX --channel 10 --daemonize --path /tmp --sdp
```

使用两个重要的参数：--Sdp 向 sdpd 注册服务，--path /tmp 指示程序保存接收数据的位置（在本例中保存到 /tmp）。您还可以指定具有写访问权限的任何其他目录。

如果使用 kbluetooth，则当在便携式计算机上接收到照片时，将提示您输入目录。

现在，移动电话必须联系上计算机。为此，打开电话中的连接菜单，然后选择蓝牙。如有必要，请在选择我的设备前单击打开。选择新设备并让电话搜索便携式计算机。如果检测到设备，其名称显示在屏幕上。选择与便携式计算机关联的设备。如果出现 PIN 查询，则输入 /etc/bluetooth/pin 中指定的 PIN。现在，您的电话就能识别便携式计算机了，并能与便携式计算机交换数据。退出当前菜单并转到图像菜单。选择要传送的图像并按更多。在下一个菜单中，按发送选择传送方式。选择通过蓝牙。便携式计算机将被作为目标设备列出。选择便携式计算机开始传送。图像随即被保存在使用 opd 命令指定的目录中。可以采用相同的方法将音频曲目传送到便携式计算机。

29.2.6 故障诊断

如果在建立连接时遇到困难，则根据以下列表继续操作。请记住，错误可能发生在连接的任何一端，或甚至两端都有错误。如果可能，请使用另一个蓝牙设备重现所发生的问题，以校验目前的设备是否有问题。

本地设备是否列在 `hcitooldev` 的输出中？

如果此输出中未列出本地设备，则可能是未启动 `hcid` 或设备未被识别为蓝牙设备。产生这种情况有多种原因。设备可能有问题或缺少正确的驱动程序。内置蓝牙的便携式计算机通常有一个用于无线设备（例如，WLAN 和蓝牙）的开关。请查看便携式计算机的手册以了解您的设备是否有这样一个开关。用命令 `rcbluetoothrestart` 重新启动蓝牙系统，并检查 `/var/log/messages` 中是否报告了任何错误。

您的蓝牙适配器是否需要固件文件？

如果需要，请安装 `bluez-bluefw` 并用 `rcbluetoothrestart` 重新启动蓝牙系统。

`hcitoolinq` 的输出是否返回其他设备？

请多次测试此命令。连接可能受到干扰，因为其他设备也在使用蓝牙的频段。

PIN 是否匹配？

检查计算机的 PIN 号码（在 `/etc/bluetooth/pin` 中）是否与目标设备的 PIN 号码相匹配。

远程设备是否能“看到”您的计算机？

尝试从远程设备建立连接。检查此设备是否能看到您的计算机。

是否可以建立网络连接（请参见“[两台主机间的网络连接](#)”一节 [529]）？

“[两台主机间的网络连接](#)”一节 [529] 中所述的设置可能由于几种原因而不起作用。例如，这两台计算机中的一台可能不支持 SSH。尝试

`ping 192.168.1.3` 或 `ping 192.168.1.4`。如果有效，则检查 `sshd` 是否是活动的。另一个问题可能是，在这两台设备中，有一台设备的网络设置与示例中的地址 `192.168.1.x` 冲突。如果是这种情况下，请尝试使用不同的地址，例如 `10.123.1.2` 和 `10.123.1.3`。

便携式计算机是否显示为目标设备（请参见“[将数据从移动电话传送到计算机](#)”一节 [530]）？移动设备是否识别便携式计算机上的 Obex-Push 服务？

在我的设备中，选择相应的设备并查看服务的列表。如果未显示 Obex-Push（甚至在更新列表后也未显示），则问题是由便携式计算机上的 `opd` 引起的。校验该 `opd` 已激活并且您有该指定目录的写权限。

中所述的情况在反方向上是否可行？“[将数据从移动电话传送到计算机](#)”一节 [530]

如果安装了 `obexftp` 包，则可在某些设备上使用命令 `obexftp -b device_address -B 10 -p image`。已对多部 Siemens 和 Sony Ericsson

移动电话进行了测试，可以正常工作。请参见 `/usr/share/doc/packages/obexftp` 中的文档。

如果安装了 `bluez-hcidump` 程序包，则可以使用 `hcidump -x` 检查在设备之间发送的数据。有时输出有助于提示发生问题的地方，但是请注意它实际上只是“明文”的一部分。”

29.2.7 更多信息

其他某些（最新）文档可从 `/usr/share/doc/packages/bluez-Uutils/` 获取（提供德语和英语版本）。

对于蓝牙的使用和配置，<http://www.holtmann.org/linux/bluetooth/> 提供了各种说明的广泛概述。其他有用的信息和说明：

- 集成在内核中的蓝牙协议堆栈的正式 HOWTO 文档：<http://bluez.sourceforge.net/howto/index.html>
- 连接到 PalmOS PDA：<http://www.cs.ucl.ac.uk/staff/s.zachariadis/btpalmlinux.html>

29.3 红外线数据传送

IrDA（红外线数据标准协会）是通过红外线进行无线通讯的行业标准。目前市场上销售的许多便携式计算机都配有与 IrDA 兼容的收发器，支持与其他设备（例如打印机、调制解调器、LAN 或其他便携式计算机）进行通讯。数据传送速率从 2400bps 到 4Mbps。

有两种 IrDA 工作方式。标准方式 SIR，通过串行接口访问红外线端口。这种方式可以在几乎所有系统上使用，足以满足大多数要求。更快的方式 FIR，要求 IrDA 芯片有特殊的驱动程序。因为缺少适当的驱动程序，所以并非所有芯片类型都可以以 FIR 方式工作。在计算机的 BIOS 中设置所需的 IrDA 方式。BIOS 还显示了 SIR 方式使用了哪个串行接口。

可在 Werner Heuser 所写的 IrDA Howto 文档（<http://tuxmobil.org/Infrared-HOWTO/Infrared-HOWTO.html>）中找到关于 IrDA 的信息。另外，请参见 Linux Irda 项目万维网站点（<http://irda.sourceforge.net>）。

29.3.1 软件

内核包中包含所需的内核模块。包 `irda` 提供了支持红外线接口所需的帮助应用程序。安装此包后，可以在 `/usr/SHARE/doc/packages/irda/readme` 中找到文档。

29.3.2 配置

在引导系统时，不会自动启动 IrDA 系统服务。请使用 YaST IrDA 模块激活此服务。在此模块中只可以修改一个设置：红外线设备的串行接口。测试窗口显示两个输出。其中一个是 `irdadump` 的输出，它记录了所有发送的和接收的 IrDA 包。此输出应包含计算机的名称以及传送范围内所有红外线设备的名称。在第 29.3.4 节“故障诊断”[534]中显示了这些讯息的示例。窗口的下部列出了存在 IrDA 连接的所有设备。

IrDA 消耗相当多的电池电量，这是因为每隔几秒就会发送一个发现包以检测其他外围设备。因此，如果使用电池电源，则只在必要时才应启动 IrDA。输入命令 `rcirdastart` 激活 IrDA，或输入 `rcirdastop` 取消激活 IrDA。当激活接口时，系统将自动装载所有需要的内核模块。

如果是首选，在文件中手动配置 `/etc/sysconfig/irda`。此文件只包含一个变量 `IRDA_PORT`，它确定在 SIR 方式下要使用的接口。

29.3.3 用法

可以将数据发送到设备文件 `/dev/irlpt0` 进行打印。设备文件 `/dev/irlpt0` 就像普通 `/dev/lp0` 电缆接口一样，只是它通过红外线以无线方式发送打印数据。要进行打印，确保打印机位于计算机红外线接口的可视范围内并且启动了红外线支持。

可以使用 YaST 打印机模块配置通过红外线接口运行的打印机。未自动检测到打印机，您必须进行以下操作以对其进行手动配置：单击添加 > 直接连接的打印机。选择 *IrDA 打印机* 并单击下一步以配置打印机设备。通常，`irlpt0` 是正确的连接。单击结束来应用设置。提供了在 Linux 中操作打印机的详细信息。第 20 章 打印机操作 [397]。

通过设备文件 `/dev/ircomm0` 可以与其他主机以及移动电话或其他类似设备进行通讯。例如，Siemens S25 和 Nokia 6210 移动电话可以通过使用红外线接口的 `wvdial` 应用程序拨号并连接到因特网。还可以与 Palm Pilot 同步数据，但前提是已将相应的应用程序的设备设置设置为 `/dev/ircomm0`。

如果愿意，您可以只对支持打印机或 IrCOMM 协议的设备进行寻址。通过特殊应用程序（例如 `irobexpalm` 和 `irobexreceive`）可以对支持 IROBEX 协议的设备（例如 3Com Palm Pilot）进行寻址。有关信息，请参考 *IR-HOWTO* (<http://tldp.org/HOWTO/Infrared-HOWTO/>)。irdadump 输出中设备名后的方括号中列出了此设备支持的协议。IrLAN 协议支持仍在开发中。”

29.3.4 故障诊断

如果连接到红外线端口的设备不响应，请使用命令 `irdadump`（以 root 用户身份）检查计算机是否识别其他设备。当 Canon BJC-80 打印机在计算机的可视范围内时，会经常出现类似 例 29.1 “irdadump 的输出” [534] 的内容：

例 29.1 irdadump 的输出

```
21:41:38.435239 xid:cmd 5b62bed5 > ffffffff S=6 s=0 (14)
21:41:38.525167 xid:cmd 5b62bed5 > ffffffff S=6 s=1 (14)
21:41:38.615159 xid:cmd 5b62bed5 > ffffffff S=6 s=2 (14)
21:41:38.705178 xid:cmd 5b62bed5 > ffffffff S=6 s=3 (14)
21:41:38.795198 xid:cmd 5b62bed5 > ffffffff S=6 s=4 (14)
21:41:38.885163 xid:cmd 5b62bed5 > ffffffff S=6 s=5 (14)
21:41:38.965133 xid:rsp 5b62bed5 < 6cac38dc S=6 s=5 BJC-80
                        hint=8804 [Printer IrCOMM ] (23)
21:41:38.975176 xid:cmd 5b62bed5 > ffffffff S=6 s=* earth
                        hint=0500 [ PnP Computer ] (21)
```

如果没有输出或其他设备不回应，则检查接口的配置。校验是否使用了正确的接口。有时红外线接口位于 `/dev/ttyS2` 或 `/dev/ttyS3`，并且有时使用了 IRQ 3 之外的中断。可以在几乎每台便携式计算机的 BIOS 设置菜单中检查和修改这些设置。

还可以使用普通数码摄像机来帮助确定红外线 LED 是否发光。大多数数码摄像机都可以看到红外线，但人眼却看不到。

29.4 管理 UMTS/3G 网络连接

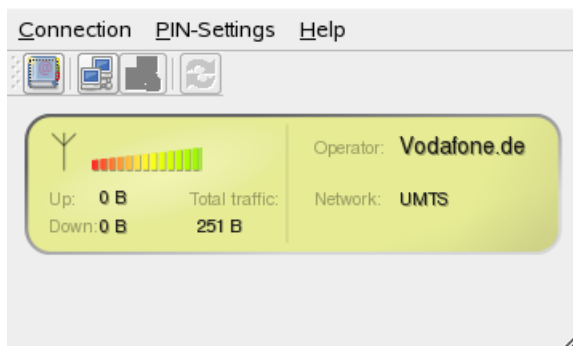
全球移动通信系统 (UMTS) 也称为 3G，是一种可以提供几种多媒体服务（例如浏览万维网或收发信息）的蜂窝电话技术。UMTS 卡（有 PCMCIA 卡或 Express 卡）可以连接到您的计算机或便携式计算机，与 SIM（订购者身份模块）卡结合使用时，使用 UMTS 网络将您的计算机连接到因特网提供商。

要使用 SUSE Linux Enterprise® 中包含的 UMTS 模块，您需要安装 `umtsmon` 包（默认情况下没有安装）。它包含用于控制 UMTS（或 GPRS/EDGE）卡的软件。使用 UMTSmon 应用程序可以控制网络连接。建立网络连接后，就可以使用您选择的万维网浏览器冲浪因特网了。

安装 `umtsmon` 包并将您的 UMTS 卡连接到计算机以后，请确保 `smpppd` 服务正在运行：启动 YaST，选择系统 > 系统服务（运行级别），然后检查 `smpppd` 的状态。如果尚未启用 `smpppd`，请单击启用。接收到确认讯息后，请单击完成退出该模块。

现在通过主菜单或按 **Alt + F2** 组合键并输入 `umtsmon` 来启动 UMTSmon。通常会提示您输入 SIM 卡的 PIN，然后会显示 UMTSmon 主窗口。

图 29.3 UMTSmon 主窗口



如果不想每次都输入 PIN，也可以禁用对卡的 PIN 保护。要进行此操作，请选择 **PIN 设置 > 禁用 PIN**，并输入您的 PIN 进行确认。如果您需要更改 PIN，请选择 **PIN 设置 > 更改 PIN**。

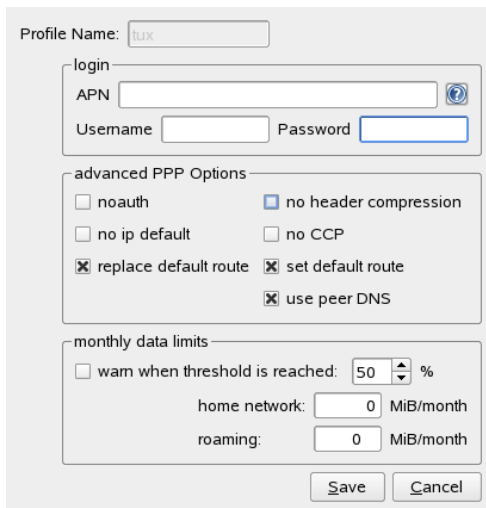
29.4.1 配置 UMTSmon

在连接到网络前，请先检查并配置 UMTSmon 中的网络设置。要定义网络运营商，请选择 **连接 > 选择网络运营商**。要搜索可用的网络，请单击 **查找网络**。执行搜索后，请从列表中选择运营商，然后单击 **选择**。

过程 29.1 管理配置文件

可以创建不同配置文件以不同情况下使用。

- 1 从菜单中选择 **管理配置文件**。
- 2 要创建新的配置文件，请单击 **添加配置文件**；或者，要更改现有配置文件，从列表选择一个配置文件并单击 **编辑配置文件**。



The screenshot shows a configuration window for UMTSmon. At the top, there is a text field for 'Profile Name' containing the value 'tux'. Below this is a 'login' section with three input fields: 'APN', 'Username', and 'Password'. The 'advanced PPP Options' section contains several checkboxes: 'noauth' (unchecked), 'no header compression' (checked), 'no ip default' (unchecked), 'no CCP' (unchecked), 'replace default route' (checked), 'set default route' (checked), and 'use peer DNS' (checked). The 'monthly data limits' section has a checkbox 'warn when threshold is reached' (unchecked), a spinner box set to '50' with a '%' symbol, and two more input fields: 'home network' set to '0' MiB/month and 'roaming' set to '0' MiB/month. At the bottom right are 'Save' and 'Cancel' buttons.

- 3 输入从您的提供商获得的 *APN*（接入点名）、*用户名*和*密码*，然后单击**保存**。
- 4 如果已经创建了几个配置文件，请从列表选择一个并设置为*活动*。
- 5 要从列表中去掉配置文件，请选择它并单击**删除配置文件**。

也可以定义或限制要使用的连接类型 (UMTS/GSM/GPRS)。要进行此操作, 请选择 **连接 > 无线电自选设置** 并根据需要更改选项。如果禁用 **信号强度和下载统计自动更新**, 这些参数不会在 UMTSmon 主窗口中自动刷新。在这种情况下, 需要单击 **显示时刷新运营商/信号/无线电统计图标** 以显示当前参数。

29.4.2 监视 UMTS/3G 网络连接

要连接到现有网络, 请选择 **连接 > 连接** 或单击工具栏中的 **以默认配置文件连接** 图标。建立连接后, 根据您使用的卡类型, UMTSmon 主窗口将显示信号强度和通讯。并非所有的卡在现有网络连接过程中都能够自动监视信号强度。

注意: 估算总通讯值

注意主窗口中的 **总通讯量** 值仅是近似值, 不一定反映真实值。如果您同提供商之间的合同是基于传输的数据量的, 请注意不要超过总量。

要停止连接, 请选择 **连接 > 断开连接**, 或单击工具栏中的 **断开连接** 图标。

29.4.3 查错

如果在建立连接或运行 UMTSmon 时遇到困难, 则根据以下列表继续操作。

当前登录的用户是否可以访问 UMTS 卡设备, 该设备是否属于 dialout 组?
连接到您的计算机的 UMTS 卡通常列出为 `/dev/ttyUSB*` 或 `/dev/noz0`。

使用 `ls -l /dev/ttyUSB*` 或 `ls -l /dev/noz0` 检查这些设备的访问权限。如果 root 仍然列为拥有者, 且设备不属于 dialout 组, 请使用以下命令将当前用户和 dialout 组设置为拥有者 (需要 root 许可权限):

```
chown user.dialout /dev/ttyUSB*
chown user.dialout /dev/noz0
```

请注意, 当前用户需要在 dialout 组中才能连接到网络。重新启动 UMTSmon 后, 用户现在应该可以建立网络连接了。

`/etc/sysconfig/network` 是否包含一个名为 `ifcfg-raw0` 的文件?
需要此文件才能与 `smpppd` 建立连接。如果 `/etc/sysconfig/network` 中没有此文件, 请使用该名称创建一个空文件。

```
touch ifcfg-raw0
```

是否仍然不能使用 UMTSmon 建立网络连接？
以 root 身份运行以下命令：

```
touch /etc/sysconfig/network/ifcfg-raw0
rcsmpppd restart
```

尝试使用 UMTSmon 重连接到网络。建立连接后，请检查通过 /sbin/route -n 获取的内核 IP 路由选择表。如果 ppp0 列为目标 0.0.0.0 的 Iface，则应该包含一个如下所示的条目：

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	10.64.64.64	0.0.0.0	UG	0	0	0	ppp0

29.4.4 更多信息

在已安装系统下的 /usr/share/doc/packages/umtsmon/README.SUSE 中查找关于 UMTSmon 的更多其他（最新）文档

部分 IV. 服务

基本联网知识

Linux 提供集成进各类网络结构中所需的联网工具和功能。TCP/IP 是 Linux 惯用的协议，具有多种服务和特殊功能，本章将对此进行介绍。使用网卡、调制解调器或其他设备的网络访问可以通过 YaST 来配置。也可以手动进行配置。不过本章的讨论仅限于基本机制和相关网络配置文件。

Linux 和其他 Unix 操作系统均使用 TCP/IP 协议。该协议不是单个网络协议，而是提供多种服务的一系列网络协议。中所列的协议专用于在两台计算机之间通过 TCP/IP 交换数据。表 30.1 “TCP/IP 系列协议中的若干协议” [541] 由 TCP/IP 连接而成的网络构成了世界范围的网络，就整体而言也称作“因特网”。“”

RFC 代表注释请求。RFC 由一些文档组成，用来说明各种因特网协议和操作系统及其应用程序的实施过程。RFC 文档用来说明如何设置因特网协议。要进一步了解某个协议，请参见相应的 RFC 文档。可以通过 <http://www.ietf.org/rfc.html> 访问这些联机文档。

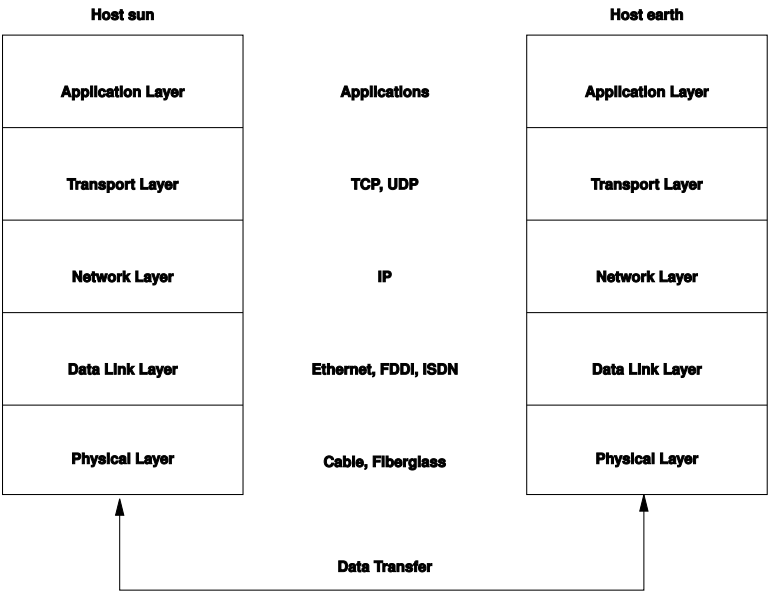
表 30.1 TCP/IP 系列协议中的若干协议

协议	说明
TCP	传送控制协议：面向连接的安全协议。要传送的数据首先由应用程序作为数据流发送，然后由操作系统转换为相应的格式。数据到达目标主机上的相应应用程序时采用最初发送时的原始数据流格式。TCP 确定传送过程中是否丢失了数据，并确保格式没有混乱。只要涉及到数据序列就会实施 TCP。

协议	说明
UDP	用户数据报文协议：无连接、不安全的协议。要传送的数据以应用程序生成的数据包的形式发送。不能保证数据以正确的顺序到达接收方，还可能丢失数据。UDP 适用于面向记录的应用程序。它的等待时间比 TCP 稍短。
ICMP	因特网控制消息协议：这实际上不是一个面向最终用户的协议，而是一个特殊的控制协议，用来发出错误报告，还可以控制参与 TCP/IP 数据传送的计算机的行为。此外，它还提供一种特殊的回应方式，可以通过 ping 程序查看该方式。
IGMP	因特网组管理协议：此协议控制实施 IP 多路广播时的计算机行为。

如图 30.1 “TCP/IP 的简化层次模型” [542] 中所示，数据交换在不同的层中进行。实际的网络层是通过 IP（因特网协议）的不安全数据传送。IP 的上面是 TCP（传送控制协议），它能够确保一定程度的数据传送安全性。IP 层又受底层硬件相关协议（例如 Ethernet）的支持。

图 30.1 TCP/IP 的简化层次模型

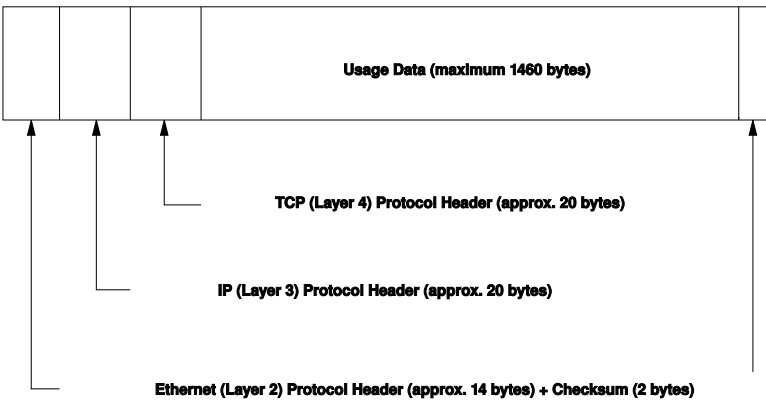


该图为每一层都提供了一到两个示例。层次按照抽象程度排序。最底层非常接近硬件。最上层则几乎就是硬件的完全抽象化。每一层都有自己的特殊功能。每一层的特殊功能多隐含在其说明中。数据链路层和物理层表示所用的物理网络（如 Ethernet）。

几乎所有硬件协议都在面向数据包的基础上发挥作用。因为无法一次传送所有数据，所以要将这些数据封装在包中。TCP/IP 包最大约为 64 KB。通常的包还要小得多，因为可能还要受到网络硬件的限制。Ethernet 上的数据包最大约为 1500 字节。通过 Ethernet 发送数据时，TCP/IP 包不能超过这个限额。如果传送更多数据，操作系统需要发送更多的数据包。

为使层实现其指定功能，必须在数据包中保存与每层相关的附加信息。这些信息保存在数据包的报头中。每一层都在每个新包的开头附加一小块称为协议报头的数据。演示了一个通过 Ethernet 电缆传送的示例 TCP/IP 数据包。图 30.2 “TCP/IP Ethernet 包” [543] 校验和位于包的末尾而不是开头，这样更便于网络硬件处理。

图 30.2 TCP/IP Ethernet 包



当应用程序通过网络发送数据时，数据会穿越每个层次，所有传递都在 Linux 内核中实施（只有物理层除外）。每一层都负责准备好数据，以便传递到下一层。最底层最后负责发送数据。接收数据时则逆向执行整个过程。正像剥洋葱那样，在每一层中都要从传输数据中去除协议报头。最后，传输层负责使数据可供目标上的应用程序使用。通过这种方式，每一层只与其上一层或下一层通讯。对于应用程序，无论数据是通过 100 Mbit/s（兆位/秒）的 FDDI 网络传送还是通过 56 Kbit/s（千位/秒）的调制解调器线路传送，都与此无关。同样，只要数据包的格式正确，传送哪种数据对数据线也无关紧要。

30.1 IP 地址和路由

各节的论述仅限于 IPv4 网络。有关 IPv6 协议（IPv4 的后续协议）的信息，请参见 [第 30.2 节“IPv6 — 下一代的因特网”](#) [546]。

30.1.1 IP 地址

因特网上的每台计算机都有一个唯一的 32 位地址。这些 32 位（或 4 字节）地址通常按 [例 30.1“编写 IP 地址”](#) [544] 的第二行所示的格式书写。

例 30.1 编写 IP 地址

```
IP Address (binary):  11000000 10101000 00000000 00010100
IP Address (decimal):      192.      168.      0.      20
```

在十进制格式中，四字节以十进制数书写，其间以句点分隔。IP 地址被指派给主机或网络接口。除此之外不能用在其他任何地方。这条规则也有例外，但这些例外与以下讯息无关。

IP 地址中的点表示分级系统。直到 20 世纪 90 年代，IP 地址仍然有严格的分类。不过，这个系统经证实太过死板，已经废止。现已改为使用无类别路由 - （CIDR，无类别域间路由）。

30.1.2 网络掩码和路由

网络掩码用于定义子网的地址范围。如果两台主机在同一个子网中，则它们可直接相互访问，如果不在同一个子网中，则需要网关地址，它处理子网和其他网络之间的所有流量。要检查两个 IP 地址是否位于同一个子网中，只需分别将两个地址与网络屏蔽进行“AND”操作。“”如果结果相同，则两个 IP 地址在同一个本地网络中。如果结果不同，则仅能通过网关连接远程 IP 地址和远程接口。

要了解网络屏蔽如何工作，可查看 [例 30.2“将 IP 地址链接到网络掩码”](#) [545]。网络屏蔽有 32 位，它确定属于网络的 IP 地址是多少。对于所有为 1 的位，将它们在 IP 地址中的相应位标记为属于网络。对于所有为 0 的位，标记为属于子网。这意味着为 1 的位越多，子网就越小。因为网络屏蔽总是由多个连续的 1 位组成，所以也可仅计算网络屏蔽中的位数。在 [例 30.2“将 IP 地址链接到网络掩码”](#) [545] 中，第一个 24 位也可写作 192.168.0.0/24。

例 30.2 将 IP 地址链接到网络掩码

```
IP address (192.168.0.20):  11000000 10101000 00000000 00010100
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
-----
Result of the link:         11000000 10101000 00000000 00000000
In the decimal system:      192.      168.      0.      0

IP address (213.95.15.200): 11010101 10111111 00001111 11001000
Netmask   (255.255.255.0):  11111111 11111111 11111111 00000000
-----
Result of the link:         11010101 10111111 00001111 00000000
In the decimal system:      213.      95.      15.      0
```

再举个例子：通过同一以太网电缆相连的所有计算机通常都位于同一子网中，可直接访问。即使用交换机或网桥物理分隔该子网，这些主机仍然可以直接访问。

仅在网关是为目标网络配的时，才能访问本地子网外部的 IP 地址。通常情况下，只有一个网关处理所有外部流量。然而，也可能为不同的子网配置多个网关。

如果配置了网关，所有的外部 IP 包将发送到相应的网关。此网关随后会尝试以相同的方式转发该包（从主机到主机）直到到达目标主机或超过该包的 TTL（存活时间）。

表 30.2 特定地址

地址类型	说明
基本网络地址	这是网络掩码和该网络中的任意地址，如 例 30.2 “将 IP 地址链接到网络掩码” [545] 中的 Result（结果）所示。不能将此地址指派给任何主机。
广播地址	这大体表示“访问此子网内的所有主机”。要生成此地址，需要将网络掩码反转为二进制格式，并使用逻辑 OR 链接到基本网络地址。因此，以上示例会生成 192.168.0.255。该地址无法指派给任何主机。
本地主机	地址 127.0.0.1 指派给每台主机的“回路设备”。“”可以使用此地址与您自己的计算机建立连接。

由于 IP 地址必须在全球范围内唯一，您不能随机选择地址。共有三个地址域可用于建立基于 IP 的专用网络。这些地址无法与因特网上的其他地址建立任何连接，因为它们不能通过因特网传送。这些地址域在 RFC 1597 中指定，并且列在表 30.3 “专用 IP 地址域” [546] 中。

表 30.3 专用 IP 地址域

网络/网络掩码	域
10.0.0.0/255.0.0.0	10.x.x.x
172.16.0.0/255.240.0.0	172.16.x.x – 172.31.x.x
192.168.0.0/255.255.0.0	192.168.x.x

30.2 IPv6 — 下一代的因特网

由于 WWW（万维网）的出现，过去十五年中越来越多的计算机开始通过 TCP/IP 通讯，这使因特网有了突飞猛进的发展。自从 1990 年在 CERN (<http://public.web.cern.ch>) 任职的 Tim Berners-Lee 开创了 WWW，因特网主机的数量已从几千台猛增至上亿台。

如上所述，IPv4 地址只有 32 位。而且还有不少 IP 地址丢失 - 因网络组织结构的原因而无法使用。子网中可用的地址数量是位数的平方减 2。举例来说，某个子网可以有 2 个、6 个或 14 个可用地址。如果要将 128 台主机连接到因特网，您的子网要提供 256 个 IP 地址，其中只有 254 个可用，因为有两个 IP 地址需要供该子网本身的结构使用：广播和基础网络地址。

在当前的 IPv4 协议下，DHCP 或 NAT（网络地址转换）是用来避免出现地址短缺的典型机制。这些方法与用来分隔专用地址空间和公用地址空间的规定相结合，肯定能够缓解短缺状况；它们的问题在于不仅配置烦琐，而且也加重了维护的负担。要在 IPv4 网络内设置主机，您需要若干地址项，如主机本身的 IP 地址、子网掩码、网关地址，可能还要提供名称服务器地址。所有这些项都是必需的，而且无法从其他任何地方得到这些项。

利用 IPv6，地址的短缺和复杂的配置都将成为过去。以下各节进一步说明了 IPv6 带来的改进和优点，以及如何从旧协议过渡到新协议。

30.2.1 优点

新协议中最为重要同时也最为显著的改进在于对可用地址空间的极大扩容。IPv6 地址由 128 位值而不是传统的 32 位值组成，它提供的 IP 地址数目多达 10 的 15 次方的若干倍。

不过，IPv6 与以前的不同不仅限于长度，其内部结构也发生了变化，这种结构可以包含更多的有关系统和系统所属网络的具体信息。有关详细信息，请参见第 30.2.2 节“地址类型和结构”[548]。

以下列出了新协议的其他一些优点：

自动配置

IPv6 使网络可以支持“即插即用”，这意味着无需任何手动配置即可将新安装的系统集成到（本地）网络中。“”新主机可以使用其自动配置机制，依赖名为邻居发现 (ND) 的协议从邻近的路由器提供的信息中得到自己的地址。这种方法不要求管理员参与，并且无需维护用于分配地址的中央服务器 - 这是 ipv4 无法媲美的（在 ipv4 中需要使用 DHCP 服务器来自动分配地址）。

移动能力

利用 IPv6，为一个网络接口同时指派多个地址成为可能。这使得用户能方便地访问几个网络，可比作手机公司提供的国际漫游服务：您携带手机出境时，手机一旦进入相应区域就会自动登录外国服务，因此无论您在哪儿，都可以用同一号码联系您，并且可以像在家乡一样拨打电话。

安全通讯

在 IPv4 中，网络安全是一项附加功能。IPv6 则将 IPsec 作为其核心功能之一，允许系统通过安全隧道通讯，避免被因特网上的外来者窃听。

向后兼容性

实际上，要想将整个因特网一下子从 IPv4 转换为 IPv6 是不可能的。因此，这两个协议不仅要能在因特网上同时存在，还应能够同时存在于一个系统中，这一点至关重要。要实现这一点，一方面两种地址应兼容（IPv4 地址可以轻松转换为 IPv6 地址），另一方面还要使用一定数量的隧道。请参见第 30.2.3 节“IPv4 与 IPv6 并存”[551]。此外，系统可以依赖双栈 IP 技术同时支持两种协议，这意味着系统中有两种完全分开的网络堆栈，从而避免这两种版本的协议相互影响。

通过多路广播的自定义服务

在 IPv4 中，有些服务（如 SMB）需要向本地网络中的所有主机广播其数据包。IPv6 则采用一种更为精确的方式，通过多路广播支持服务器对主机寻址，即对属于一组的若干主机寻址（这不同于通过广播对所有主机寻址或通过单路广播对每台主机逐个寻址）。将哪些主机作为一组来寻址可能要取决于具体的应用程序。可使用一些预定义的组来寻址，例如对所有名称服务器寻址（所有名称服务器多路广播组），或对所有路由器寻址（所有路由器多路广播组）。

30.2.2 地址类型和结构

如上所述，目前的 IP 协议在两个重要方面有缺陷：IP 地址日益短缺，配置网络、维护路由选择表的任务变得越来越复杂和艰难。IPv6 通过将地址空间扩展到 128 位解决了第一个问题。通过引入分级地址结构，结合先进的网络地址分配技术和多宿主功能（将多个地址指派给同一个设备，从而支持对多个网络的访问），第二个问题也迎刃而解。

使用 IPv6 时，了解三种类型的地址十分有用：

单路广播

这类地址只与一个网络接口关联。采用这类地址的包只传递到一个目标。因此，使用单路广播地址可以将包传送到本地网络或因特网上的单个主机。

多路广播

这类地址与一组网络接口相关。采用这类地址的包将传递到属于该组的所有目标。多路广播地址主要供特定网络服务使用，用于以有序的方式与特定的主机组通讯。

任意广播

这类地址与一组接口相关。采用这类地址的包将根据基础路由协议的原则，传递给该组中与发送方最为接近的成员。任意广播地址便于主机在特定网络区域内找到提供特定服务的服务器。同一类型的所有服务器都具有相同的任意广播地址。在请求服务时，主机会收到路由协议决定的最接近它的服务器的回复。如果出于某种原因此服务器无法回复，协议会自动选择距离稍远一些的服务器，依此类推。

IPv6 地址分为八组，每组四位数字，代表十六位，采用十六进制表示法。各组之间用冒号(:)分隔。可以删除某组中的前置零字节，但不能删除组中或组末的零。另一个约定是：连续的零字节若超过四个，则可以省略为双冒号形式。

不过，每个地址只允许有一个这样的 ::。中演示了这种简写表示法，其中的三行全部表示同一地址。**例 30.3 “示例 IPv6 地址”** [549]

例 30.3 示例 IPv6 地址

```
fe80 : 0000 : 0000 : 0000 : 0000 : 10 : 1000 : 1a4
fe80 :    0 :    0 :    0 :    0 : 10 : 1000 : 1a4
fe80 :                               : 10 : 1000 : 1a4
```

IPv6 地址的每个部分都有明确的功能。前面的字节构成前缀，用于指定地址类型。中间部分是地址的网络部分，但可以不用。地址的结尾构成主机部分。在 IPv6 中，网络掩码是通过在地址末尾的斜杠后指明前缀的长度来定义的。**例 30.4 “指定前缀长度的 IPv6 地址”** [549] 中的地址包含上述信息，即：前 64 位构成地址的网络部分，后 64 位构成地址的主机部分。换言之，64 表示网络掩码由左起的 64 个 1 位值构成。正如 IPv4，要用 AND 将 IP 地址与子网值结合起来，以确定主机位于同一子网中还是其他网络中。

例 30.4 指定前缀长度的 IPv6 地址

```
fe80::10:1000:1a4/64
```

IPv6 可以识别几种预定义的前缀类型。其中有些列在 **表 30.4 “各种 IPv6 前缀”** [549] 中。

表 30.4 各种 IPv6 前缀

前缀（十六进制）	定义
00	IPv4 地址和 IPv6 上的 IPv4 兼容地址。这些用于与 IPv4 保持兼容。要使用这些地址，仍然需要依赖路由器将 IPv6 包转换为 IPv4 包。有若干特殊地址（如用于回路设备的地址）也采用此前缀。
2 或 3 作为第一个数字	可聚合全局单路广播地址。类似 IPv4 的情况，可以指定某个接口作为特定子网的一部分。目前，有以下地址空间：2001::/16（生产质量地址空间）和 2002::/16（6to4 地址空间）。
fe80::/10	链路本地地址。不应路由带有这种前缀的地址，而只能从同一子网中访问。

前缀（十六进制） 定义	
fec0::/10	站点本地地址。可以路由这种地址，但只局限在它们所属的组织网络之内。实际上，这些是相当于当前的专用网络地址空间（如 10.x.x.x）的 IPv6 地址。
ff	这些是多路广播地址。

单路广播地址由三个基本部分组成：

公共拓扑结构

第一部分（也包含上述前缀之一）用于通过公共因特网路由数据包。其中包含提供因特网访问的公司或机构的相关信息。

站点拓扑结构

第二部分包含要将包传递到的子网的路由信息。

接口 ID

第三部分标识要将包传递到的接口。其中允许使用 MAC。由于 MAC 是硬件厂商编程到设备中的全球唯一的固定标识符，配置过程得到了极大简化。事实上，前 64 个地址位共同构成 EUI-64 令牌，后 48 位从 MAC 中提取，其余的 24 位包含有关令牌类型的特殊信息。这样还可以将 EUI-64 令牌指派给没有 MAC 的接口，如基于 PPP 或 ISDN 的接口。

在这个基础结构之上，IPv6 还区分五种不同的单路广播地址：

:: (未指定)

在首次初始化接口时，即无法通过其他方法确定地址时，这类地址可用作主机的源地址。

:::1 (回路)

回路设备的地址。

IPv4 兼容地址

IPv6 地址由 IPv4 地址和 96 个零位组成的前缀构成。这类兼容地址用于隧道通讯进程（请参见第 30.2.3 节“IPv4 与 IPv6 并存”[551]），以便 IPv4 和 IPv6 主机与在纯 IPv4 环境中操作的其他主机通讯。

映射到 IPv6 的 IPv4 地址

这类地址以 IPv6 表示法指定纯 IPv4 地址。

本地地址

有两类地址可供本地使用：

链路本地

这类地址只能在本地子网中使用。不能将源地址或目标地址采用此类地址的包路由到因特网或其他子网。这些地址包含特殊的前缀 (fe80::/10) 和网卡的接口 ID，中间部分为零字节。这类地址在自动配置过程中使用，用于与同一子网中的其他主机通讯。

站点本地

可以将采用这类地址的包路由到其他子网，但不能路由到更广阔的因特网 - 不能跨越组织自身的网络。这类地址用于内部网，相当于 IPv4 定义的专用地址空间。其中包含特殊的前缀 (fec0::/10)、接口 ID，及指定子网 ID 的 16 位域。其余部分也是零字节。

作为 IPv6 引进的全新功能，每个网络接口通常可以获得多个 IP 地址，这个功能的优点即在于：可以通过同一接口访问多个网络。其中一个网络可以使用 MAC 和已知前缀进行完全的自动配置，这样一启用 IPv6（使用链路本地地址），即可访问本地网络中的所有主机。由于其中使用了 MAC，所用的任何 IP 地址都是全球唯一的。地址中只有指定站点拓扑结构和公共拓扑结构的部分才是可变部分，这取决于主机当前运行所在的实际网络。

要使主机在不同网络间切换，主机至少需要两个地址。其中之一 - 本地地址，不仅包含接口 ID 而且包含该主机通常所属的本地网络的标识符（以及相应的前缀）。本地地址是静态地址，因此一般不变。所有要发送到移动主机的包仍可传递到该主机，不管它是在本地网络还是其他任何网络中操作。这一点得益于 IPv6 引进的全新功能，如无状态自动配置和邻居发现。除本地地址之外，移动主机还获得一个或多个额外的地址，这些地址属于该主机漫游到的外地网络。这些地址称为转交地址。本地网络有一种功能，可以在主机漫游到外地时转发要发送给该主机的所有包。在 IPv6 环境中，这项任务由本地代理来完成，该代理可以接收要发送到本地地址的所有包，并通过隧道进行转发。另一方面，发送到转交地址的那些包可直接转发到移动主机，而不必进行任何特殊的迂回处理。

30.2.3 IPv4 与 IPv6 并存

将与因特网相连的所有主机从 IPv4 迁移到 IPv6 是一个逐步的过程。这两种协议将在未来一定时间内并存。通过双栈技术来实施这两种协议，可以在同一系统上同时支持这两种协议。但这仍然没有解决支持 IPv6 的主机如何与 IPv4 主

机通讯，以及应如何通过当前网络（主要基于 IPv4）传输 IPv6 包的问题。最好的解决方案就是提供隧道处理功能和兼容地址（请参见 第 30.2.2 节“地址类型和结构”[548]）。

IPv6 主机多少孤立于（全球）IPv4 网络，它可通过隧道通讯：IPv6 包封装为 IPv4 包，以便在 IPv4 网络中移动。这种在两个 IPv4 主机间的连接被称为隧道。要实现这种功能，包必须包含 IPv6 目标地址（或相应的前缀），以及隧道接收端的远程主机的 IPv4 地址。根据主机管理员间的协议，可以手动配置基本的隧道。这也称作静态隧道。

但是，静态隧道的配置和维护往往过于烦琐，不能适应日常通讯需要。因此，IPv6 提供了三种不同的动态隧道方法：

6over4

IPv6 包被自动封装为 IPv4 包，并通过支持多路广播的 IPv4 网络发送。这种方法诱导 IPv6 将整个网络（因特网）视为一个巨大的局域网 (LAN)。这样即可自动确定 IPv4 隧道的接收端。不过，这种方法不够灵活，并且还因为 IP 多路广播在因特网上尚未普及而不易推行。因此，它提供的解决方案仅适用于支持多路广播的小型公司网络或机构网络。RFC 2529 中对这种方法作出了规定。

6to4

利用这种方法，可以从 IPv6 地址自动生成 IPv4 地址，从而支持孤立的 IPv6 主机通过 IPv4 网络进行通讯。不过，用这种方法在孤立的 IPv6 主机和因特网之间通讯时存在一些问题。RFC 3056 中对这种方法进行了说明。

IPv6 隧道中介程序

这种方法依赖特殊的服务器为 IPv6 主机提供专用隧道。RFC 3053 中对此进行了说明。

30.2.4 配置 IPv6

要配置 IPv6，通常无需在各个工作stations上执行任何更改。默认情况下启用 IPv6。安装期间，您可以在第 3.11.3 节“网络配置”[31]中所述的网络配置步骤中禁用它。要在已安装系统上禁用或启用 IPv6，请使用 YaST 网卡。不要更改方式，单击下一步。然后选择卡，单击地址选项卡中的高级 > IPv6。要手动启用 IPv6，请以 root 身份输入 `modprobe ipv6`。

由于 IPv6 使用自动配置，将给网卡指派链路-本地网络中的地址。一般不在工作站上管理路由选择表。工作站可以使用路由器广告协议查询网络路由器，了解应实施的前缀和网关。使用 radvd 程序可以设置 IPv6 路由器。此程序会通知工作站对 IPv6 地址使用哪个前缀和哪个路由器。或者，可以使用 zebra 自动配置两个地址和路由选择。

有关如何使用 `/etc/sysconfig/network` 文件设置各种隧道的信息，请参见 ifup (8) 手册页。

30.2.5 有关详细信息

上文的概述中并未全面论述 IPv6 这一主题。有关这种新协议的深入讨论，请参见以下联机文档和书目：

<http://www.ipv6.org/>

学习 IPv6 知识的起点。

<http://www.ipv6day.org>

启动您自己的 IPv6 网络所需的所有信息。

<http://www.ipv6-to-standard.org/>

已启用 IPv6 的产品列表。

<http://www.bieringer.de/linux/IPv6/>

在此可找到 Linux IPv6-HOWTO 以及许多与该主题有关的链接。

RFC 2640

有关 IPv6 的基础 RFC。

IPv6 Essentials

Silvia Hagen 所著的 *IPv6 Essentials*(ISBN 0-596-00125-8) 中描述了该主题的所有重要方面。

30.3 名称解析

DNS 有助于将 IP 地址指派给一个或多个名称，并将名称指派给 IP 地址。在 Linux 中，这种转换通常由一种特殊的称为 bind 的软件来完成。负责这种转换

的计算机称为**名称服务器**。这些名称构成了分级系统，各个名称组成部分之间用圆点分隔。不过，这个名称层次与上述 IP 地址层次无关。

考虑以 `hostname.domain` 格式书写的完整名称，如 `earth.example.com`。完整名称，即**完全限定的域名 (fqdn)**，由主机名和域名 (`example.com`) 组成。后者还包含**顶级域或 TLD (com)**。

TLD 的指派由于历史原因已经变得十分混乱。传统的指派方法是美国所用的三字母域名，而世界其他地方采用的标准是双字母 ISO 国家/地区代码。此外，2000 年还引进了较长的 TLD，表示特定的活动领域（例如 `.info`、`.name` 和 `.museum`）。

在因特网发展的早期阶段（1990 年之前），文件 `/etc/hosts` 被用来储存因特网上表示的所有计算机的名称。后来事实证明随着接入因特网的计算机与日俱增，这种方法很快就行不通了。为此人们开发了一个分散式数据库，以十分分散的方式储存主机名。这个数据库类似名称服务器，它并不储存与因特网上的所有主机相关的数据，但可以向其他名称服务器发送请求。

位于层次顶级的是**根名称服务器**。这些根名称服务器管理顶级域，并由网络信息中心 (NIC) 运行。每个根名称服务器都了解负责特定顶级域的名称服务器。有关顶级域 NIC 的信息，请参见 <http://www.internic.net>。

DNS 不仅可以解析主机名，还能够为整个域识别出负责接收整个域的电子邮件的主机 - **邮件交换器 (MX)**。

为解析 IP 地址，您的计算机必须了解至少一个名称服务器及其 IP 地址。借助 YaST 可以轻松指定这样的名称服务器。如果建立的是调制解调器拨号连接，则根本无需手动配置名称服务器。拨号协议可以在建立连接后提供名称服务器的地址。

whois 协议与 DNS 密切相关。使用此程序可以快速找出负责特定域的服务器。

30.4 使用 YaST 配置网络连接

Linux 上有多个支持的联网类型。其中多数使用不同的设备名，配置文件分布在文件系统上的多个位置。关于手动网络配置方面的详细概述，请参见第 30.6 节“手动配置网络连接” [571]。

在安装过程中，可使用 YaST 自动配置所有已检测的接口。安装后，可在已安装的系统中随时配置额外的硬件。以下各节将介绍 SUSE Linux Enterprise 支持的所有类型的网络连接的配置。

30.4.1 使用 YaST 配置网卡

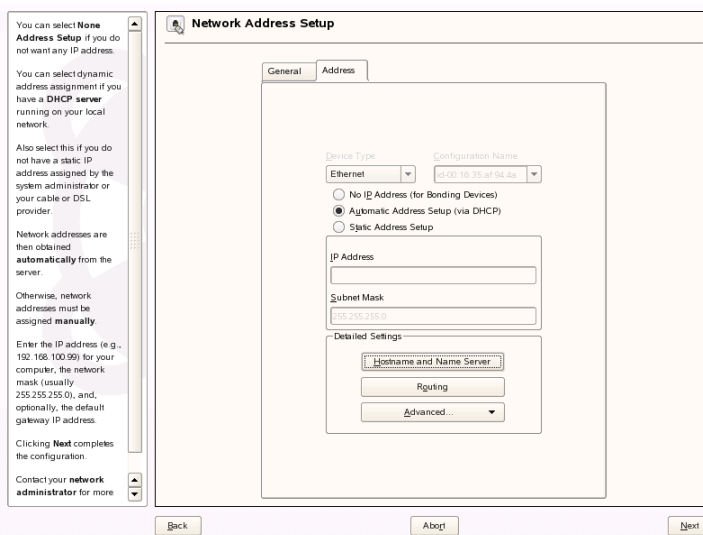
要在 YaST 中配置网络有线网卡或无线网卡，请选择网络设备 > 网卡。启动 YaST 模块后，其中将显示一个常规网络配置对话框。选择是使用 YaST 还是 NetworkManager 来管理所有网络设备。如果想使用 YaST 按照传统方法配置网络，请选中通过 *ifup* 的传统方法，然后单击下一步。要使用 NetworkManager，请选择使用 *NetworkManager* 控制用户，然后单击下一步。有关 NetworkManager 的更多详细信息，请参见第 30.5 节“使用 NetworkManager 管理网络连接” [569]。

注意: 网络连接方法和 Xen

NetworkManager 不能用于 Xen。Xen 中只能使用通过 *ifup* 的传统方法。

下一对话框的上部会显示列个列表，列出适用于配置的所有网卡。所有已正确检测的网卡将连同其名称一起列出。要更改选定设备的配置，请单击编辑。可使用添加配置未能检测到的设备，如“配置未检测到的网卡”一节 [561]中所述。

图 30.3 配置网卡



更改网卡的配置

要更改网卡的配置，请在 YaST 网卡配置模块中已检测到的网卡列表中选择—个网卡，然后单击**编辑**。将显示**网络地址设置**对话框，可在其中使用**地址**和**常规**选项卡调整网卡配置。有关无线网卡配置的信息，请参见第 29.1.3 节“**用 YaST 配置**” [517]。

配置 IP 地址

安装期间可用的有线网卡可能会自动被配置为使用自动地址设置和 DHCP。

如果您用的是 DSL 线路，但 ISP 没有指派静态 IP，则此时还应该使用 DHCP。如果决定使用 DHCP，请在 **DHCP 客户机** 选项中配置详细信息。可通过选择**高级 > DHCP 选项**来从**地址**选项卡查找此对话框。指定 DHCP 服务器是否应始终允许广播请求并允许使用标识符。如果您使用虚拟主机设置，其中不同的主机都通过同一接口通信，则需要用标识符来区分它们。

DHCP 比较适合客户机配置，但不太适合服务器配置。要设置静态 IP 地址，请如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表选择一个网卡，然后单击编辑。
- 2 在地址选项卡中，选择静态地址设置。
- 3 输入 IP 地址和子网掩码。
- 4 单击“下一步”。
- 5 要激活配置，请单击完成。

如果使用静态地址，则不会自动配置名称服务器和默认网关。要配置网关，请单击路由选择并添加默认网关。要配置名称服务器，请单击主机名和名称服务器并添加名称服务器和域的地址。

配置别名

一个网络设备可以有多个 IP 地址，称为别名。要为网络设置别名，请如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表选择一个网卡，然后单击编辑。
- 2 在地址选项卡中，选择高级 > 其他地址。
- 3 单击“添加”。
- 4 输入别名、IP 地址和网络掩码。
- 5 单击确定。
- 6 再次单击“确定”。
- 7 单击“下一步”。
- 8 要激活配置，请单击完成。

配置主机名和 DNS

如果安装期间没有更改网络配置并且有线网卡可用，则将为计算机自动生成主机名并且会激活 DHCP。这同样适用于主机连接到网络环境所需的名称服务信息。如果网络地址设置使用了 DHCP，则会向域名服务器列表自动填充相应数据。如果希望使用静态设置，则手动设置这些值。

要更改计算机名称并调整名称服务器搜索列表，则如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表中选择一个网卡，然后单击 **编辑**。
- 2 在 **地址** 选项卡中，单击 **主机名和名称服务器**。
- 3 要禁用 DHCP 驱动的主机名配置，请取消选择 **通过 DHCP 更改主机名**。
- 4 输入 **主机名**，如果需要，还输入 **域名**。
- 5 要禁用 DHCP 驱动的名称服务器列表更新，请取消选择 **通过 DHCP 更新名称服务器和搜索列表**。
- 6 输入名称服务器和域搜索列表。
- 7 单击 **确定**。
- 8 单击“**下一步**”。
- 9 要激活配置，请单击 **完成**。

配置路由选择

要使计算机能够与其他计算机和其他网络进行通信，必须提供路由选择信息以使网络流量使用正确的路径。如果使用 DHCP，则将自动提供此信息。如果使用静态设置，则必须手动添加此数据。

- 1 在 YaST 网卡配置模块的已检测到的网卡列表中选择一个网卡，然后单击 **编辑**。
- 2 在 **地址** 选项卡中，单击 **路由选择**。

- 3 输入默认网关的 IP。
- 4 单击确定。
- 5 单击“下一步”。
- 6 要激活配置，请单击完成。

添加特殊硬件选项

有时，网卡模块会需要特殊参数以正确运行。要使用 YaST 来设置这些参数，请如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表中选择一个网卡，然后单击编辑。
- 2 在地址选项卡中，单击高级 > 硬件细节。
- 3 在选项中，为网卡输入参数。如果两个网卡配置为使用相同模块，则这些参数将同时用于这两个网卡。
- 4 单击确定。
- 5 单击“下一步”。
- 6 要激活配置，请单击完成。

启动设备

如果您使用通过 ifup 的传统方法，则可以在引导期间、连接电缆后、检测到网卡后、手动启动或从不启动要配置的设备。要更改设备启动，请如下继续操作：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表中选择一个网卡，然后单击 *编辑*。
- 2 在 *常规* 选项卡中，从 *设备激活* 选择所希望的项。
- 3 单击“下一步”。
- 4 要激活配置，请单击 *完成*。

配置防火墙

无须输入详细的防火墙设置（如第 39.4.1 节“使用 YaST 配置防火墙”[664]中所述），您就能在设备设置过程中确定设备的基本防火墙设置。按如下所示继续：

- 1 在 YaST 网卡配置模块的已检测到的网卡列表中选择一个网卡，然后单击 *编辑*。
- 2 进入网络配置对话框的 *常规* 选项卡。
- 3 确定应指派接口的防火墙区域。下列选项可用：

无区域，阻塞所有交通

将阻塞此接口的所有通讯。

内部区域（未保护）

防火墙运行，但不会强制执行任何规则来保护此接口。仅当计算机属于受外置防火墙保护的大型网络时才使用此选项。

隔离区域

隔离区域是位于内部网络和（恶意）因特网之前的附加防线。可从内部网络和因特网访问指派到此区域的主机，但指派到此区域的主机无法访问内部网络。

外部区域

防火墙在此接口上运行并且全面保护其不受其他（假设为恶意）网络流量攻击。这是默认选项。

- 4 单击“下一步”。
- 5 单击完成即可激活配置。

配置未检测到的网卡

网卡可能会未被正确检测到。在此情况下，已检测到网卡列表中不会包含此网卡。如果确定系统包含网卡的驱动程序，则可以手动对其进行配置。要配置未检测到的网卡，请如下继续操作：

- 1 单击“添加”。
- 2 从可用选项（配置名称和模块名称）设置接口的设备类型。如果网卡为 PCMCIA 或 USB 设备，则激活相应的复选框，并选择下一步退出此对话框。否则，请在从列表中选择中选择您的网卡型号。然后，YaST 将自动选择适合网卡的内核模块。

硬件配置名称指定 `/etc/sysconfig/hardware/hwcfg-*` 文件的名称，该文件包含网卡的硬件设置。它包含内核模块的名称以及初始化硬件所需的选项。

- 3 单击“下一步”。
- 4 在地址选项卡中，设置接口的设备类型、配置名称和 IP 地址。要使用静态地址，请选择静态地址设置，然后完成 IP 地址和子网掩码。在此处，还可选择配置主机名、名称服务器和路由选择详细信息（请参见“配置主机名和 DNS”一节 [558]和“配置路由选择”一节 [558]）。

如果选择无线作为接口的设备类型，则在下一个对话框中配置无线连接。有关无线设备配置的详细信息可在第 29.1 节“无线 LAN” [513]中获得。

- 5 在常规选项卡中，设置防火墙区域和设备激活。通过用户控制向一般用户授权连接控制。
- 6 单击“下一步”。
- 7 要激活新网络配置，请单击完成。

有关配置名称约定的信息，请参见 `getcfg(8)` 的手册页。

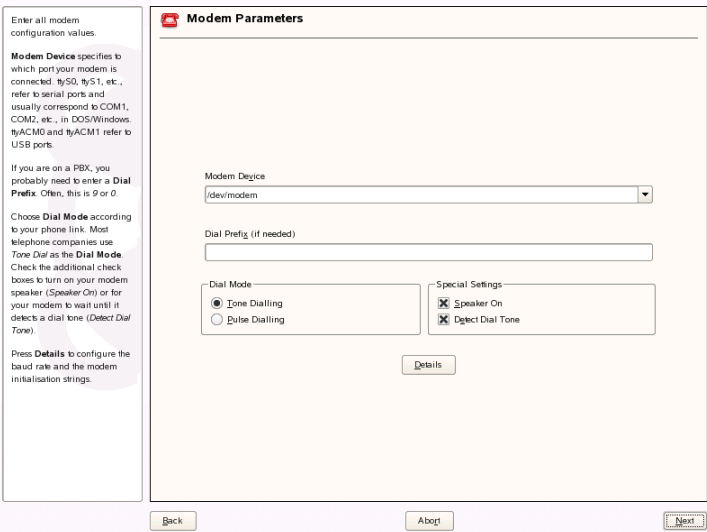
30.4.2 调制解调器

在 YaST 控制中心中，可以在网络设备 > 调制解调器 下访问调制解调器配置。如果未自动检测到您的调制解调器，请单击添加，打开用于手动配置的对话框。在随后打开的对话框中，请在调制解调器设备下输入调制解调器连接到的接口。

提示: CDMA 和 GPRS 调制解调器

就跟配置普通调制解调器一样，用 YaST 调制解调器模块配置支持的 CDMA 和 GPRS 调制解调器。

图 30.4 调制解调器配置



如果处在专用交换机 (PBX) 之后，则可能需要输入拨号前缀。该前缀通常是零。请参考随 PBX 附带的说明了解相关信息。同时还要选择使用音频拨号还是脉冲拨号、是否打开扬声器，以及调制解调器是否应在检测到拨号音之前一直等待。如果调制解调器连接到交换机，则不应启用最后一个选项。

在细节之下，设置波特率和调制解调器的初始化字符串。只有在调制解调器不是自动检测到的或者需要特殊设置才能传送数据时，才应更改以上设置。这种情况主要发生在 ISDN 终端适配器上。单击确定可退出此对话框。要将调制解调器的控制权委托给不具备根权限的普通用户，请激活用户控制。这样，不具

备管理员权限的用户即可激活或取消激活某个接口。在**拨号前缀正则表达式**下，指定正则表达式。KInternet 中的**拨号前缀**（可由普通用户修改）必须符合此正则表达式。如果将此字段留空，用户则无法在不具备管理员权限的情况下设置其他**拨号前缀**。

在下一个对话框中，选择 ISP（因特网服务提供者）。要从您所在国家/地区的 ISP 的预定义列表中进行选择，请选择**国家/地区**。也可以单击**新建**打开一个对话框，从中为您的 ISP 提供数据。这些数据包括用于拨号连接的名称、ISP 的名称，以及 ISP 提供的登录名和密码。启用**始终询问密码**，在您每次连接时都提示输入密码。

在最后一个对话框中，指定附加连接选项：

按需拨号

如果启用**按需拨号**，请设置至少一个名称服务器。

连接后修改 DNS

默认情况下启用此选项，其作用是在每次连接因特网时都更新名称服务器地址。

自动检索 DNS

如果提供者未在连接后传送其域名服务器，则禁用此选项并手动输入 DNS 数据。

愚蠢方式

默认情况下该选项是启用的。通过它可以忽略 ISP 服务器发送的输入提示，防止它们影响连接进程。

外部防火墙接口

选择此选项将激活 SUSEfirewall2 并将接口设置为外部。这样系统就可以在连接到因特网期间防范外部攻击。

空闲超时（秒）

使用此选项可以指定网络不活动的时间，一超过该时间调制解调器即自动断开连接。

IP 详细信息

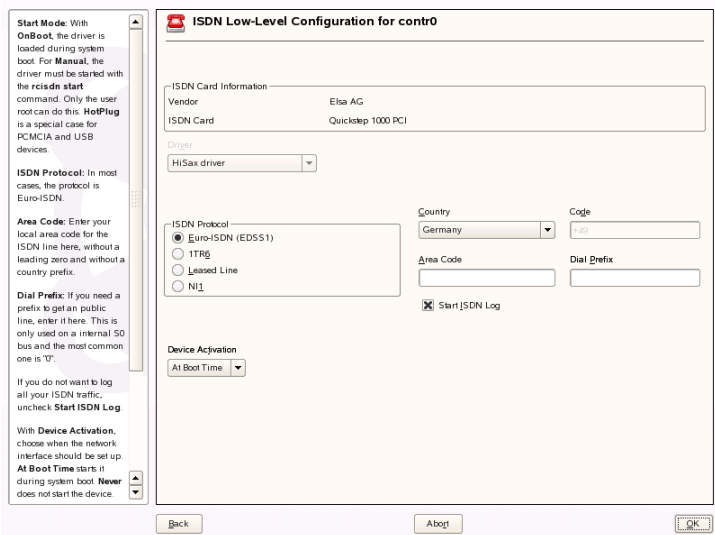
使用此选项可打开地址配置对话框。如果您的 ISP 没有为您的主机指派动态 IP 地址，请禁用**动态 IP 地址**，然后输入主机的本地 IP 地址及远程 IP 地址。请向您的 ISP 询问这些信息。保持**默认路由**的启用状态，然后通过选择**确定**关闭该对话框。

选择下一步可返回初始对话框，其中显示调制解调器配置的概要。选择完成可关闭此对话框。

30.4.3 ISDN

使用此模块可以为系统配置一个或多个 ISDN 网卡。如果 YaST 未能检测到您的 ISDN 网卡，则请单击添加并以手动方式选择。可以使用多个接口，但您可以为一个接口配置多个 ISP。在随后的对话框中，设置该网卡正常工作所需的 ISDN 选项。

图 30.5 ISDN 配置

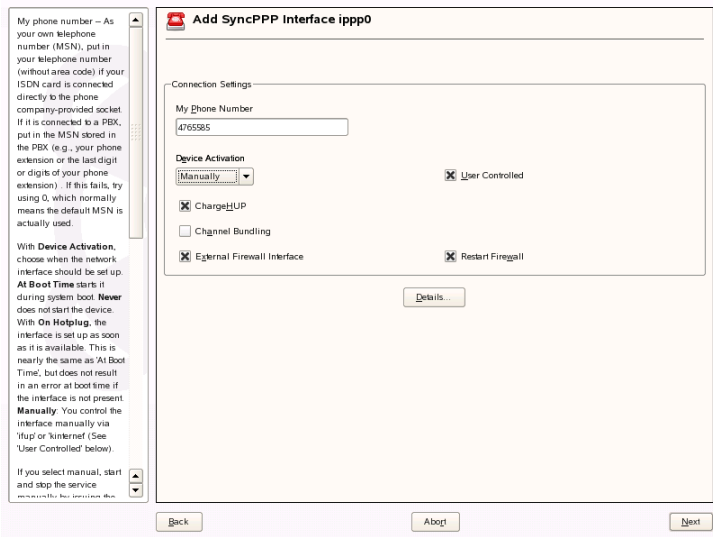


在下一个对话框中（如图 30.5 “ISDN 配置” [564] 所示），选择要使用的协议。默认值是 *Euro-ISDN (EDSS1)*，但是对于旧式或大型交换机，请选择 *ITR6*。如果是在美国，请选择 *NII*。在相关字段中选择您所在的国家/地区。相应的国家/地区代码将显示在该字段旁边的字段中。最后，提供您的区号和拨号前缀（如果需要）。

设备激活定义如何启动 ISDN 接口：使用引导时可以在系统每次引导时初始化 ISDN 驱动程序。手动要求您以 root 的身份使用命令 `rcisdn start` 来装载 ISDN 驱动程序。热插拔，用于 PCMCIA 或 USB 设备，用于在插入设备后加载驱动程序。在完成这些设置后，请选择确定。

在下一个对话框中，为您的ISDN网卡指定接口类型，并将ISP添加到现有接口中。接口的类型可能是 SyncPPP 或 RawIP，但多数 ISP 以 SyncPPP 方式操作，如下文所述。

图 30.6 ISDN 接口配置



要为我的电话号码输入的值取决于特定的设置：

ISDN 网卡直接连接到电话插座

标准的 ISDN 线路提供三个电话号码（称为多用户号码或 MSN）。如果用户需要更多号码，最多可提供十个号码。必须在此处输入其中一个 MSN，但不要区号。如果输入的号码有误，您的电话运营商将自动退回到为您的 ISDN 线路指派的第一个 MSN。

ISDN 网卡连接到专用交换机

同样，配置可能随安装设备不同而变化：

- 1. 适用于家庭的小型专用交换机 (PBX) 大多使用 Euro-ISDN (EDSS1) 协议进行内部呼叫。这些交换机具有内部 S0 总线，并对与它们连接的设备使用内部号码。

将其中一个内部号码用作您的 MSN。您应该至少能够使用支持直接向外拨号的交换机的 MSN 之一。如果无效，则尝试使用一个零。有关进一步信息，请参见随电话交换机附带的文档。

2. 为公司设计的大型电话交换机通常使用 1TR6 协议用于内部呼叫。它们的 MSN 称为 EAZ 并且通常对应直拨号码。要在 Linux 中配置，只需输入 EAZ 的最后一位即可。如果各种方法都行不通，可尝试 1 到 9 之间的各位数字。

要在下一个收费单位开始之前及时终止连接，请启用 *ChargeHUP*。但要记住，该选项不是对每个 ISP 都奏效。您也可以通过选择相应的选项启用信道绑定（多链接 PPP）。最后，您可以通过选择外部防火墙接口和重新启动防火墙为链接启用 SUSEfirewall2。要使不具备管理员权限的普通用户能够激活或取消激活接口，请选中 *用户控制*。

*细节*将打开一个对话框，在其中配置回拨方式、到此接口的远程连接和其他 *ippd* 设置。通过选择 *确定*退出 *细节*对话框。

在下一个对话框中设置 IP 地址。如果您的提供者没有为您指定静态 IP，请选择 *动态 IP 地址*。否则，根据 ISP 指定的信息，使用提供的字段输入您主机的本地 IP 地址及远程 IP 地址。如果接口应该成为与因特网连接的默认路由，请选择 *默认路由*。每台主机都只能有一个接口配置为默认路由。选择 *下一步*可退出此对话框。

使用随后的对话框，您可以设置您所在的国家/地区并选择 ISP。列表中的 ISP 都只是 *call-by-call*（通过呼叫进行呼叫）提供者。如果列表中未列出您的 ISP，请选择 *新建*。随即打开 *提供者参数*对话框，可以在其中输入 ISP 的所有详细信息。输入电话号码时，切勿在数字之间加空格或逗号。最后，输入 ISP 为您提供的登录名和密码。输完之后，请选择 *下一步*。

要在独立工作站上使用 *按需拨号*，还需指定名称服务器（DNS 服务器）。多数 ISP 都支持动态 DNS，这意味着每次用户连接时，都由 ISP 发送名称服务器的 IP 地址。不过，对于单个工作站，您仍然需要提供 192.168.22.99 之类的占位符地址。如果您的 ISP 不支持动态 DNS，请指定 ISP 的名称服务器 IP 地址。如果需要，可以为连接指定超时值 — 即网络不活动的时间（以秒计），一超过该时间即自动终止连接。选择 *下一步*确认设置。YaST 将显示配置好的接口的概要。要使所有这些设置有效，请选择 *完成*。

30.4.4 电缆调制解调器

在有些国家/地区（例如奥地利和美国），人们往往通过有线电视网访问因特网。有线电视用户通常将调制解调器一端接在有线电视插座上，另一端与计算机网卡相连（使用 10Base-TG 双绞线）。随后电缆调制解调器就能通过固定 IP 地址提供专用因特网连接。

在配置网卡时需要根据您的 ISP 提供的说明选择 *自动地址设置（通过 DHCP）* 或 *静态地址设置*。目前多数提供商都使用 DHCP。通常只有特殊的公司帐户才使用静态 IP 地址。

有关配置电缆调制解调器的进一步信息，请联机访问 http://en.opensuse.org/SDB:Setting_Up_an_Internet_Connection_via_Cable_Modem_with_SuSE_Linux_8.0_or_Higher，阅读关于这一主题的“支持数据库”文章。

30.4.5 DSL

要配置 DSL 设备，请从 YaST 网络设备部分选择 *DSL* 模块。这个 YaST 模块包含若干对话框，可以在这些对话框中基于以下协议之一设置 DSL 链接参数。

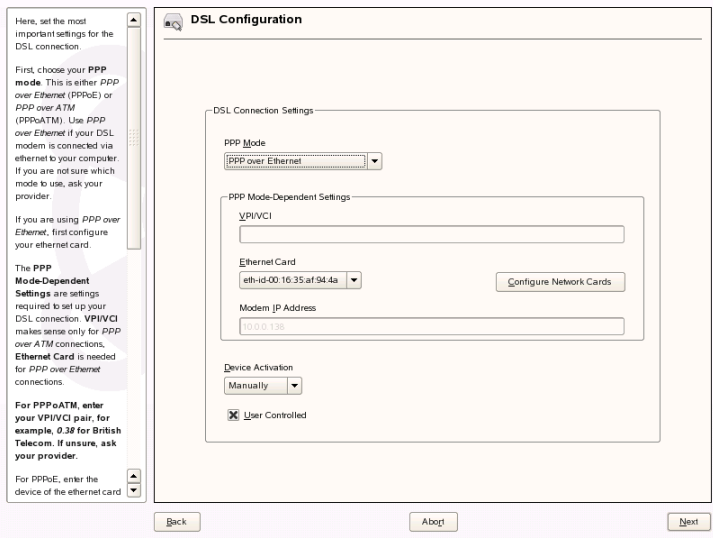
- Ethernet 上的 PPP (PPPoE)
- ATM 上的 PPP (PPPoATM)
- 用于 ADSL 的 CAPI (Fritz 网卡)
- 点对点隧道协议 (Pptp) — 奥地利

基于 PPPoE 或 PPTP 配置 DSL 连接时，要求已经正确设置相应的网卡。如果尚未这样做，应首先通过选择 *配置网卡* 来配置网卡（请参见第 30.4.1 节“使用 YaST 配置网卡”[555]）。使用 DSL 链接时，可以自动指派地址但并不通过 DHCP，这就是不应启用 *自动地址设置（通过 DHCP）* 选项的原因。相反，应该为接口输入静态虚设地址，如 192.168.22.1。在子网掩码中，输入 255.255.255.0。如果配置的是独立工作站，则将默认网关留空。

提示

IP 地址字段和子网掩码中的值只是占位符。它们只用于初始化网卡，而不会将 DSL 链接表示成这样。

图 30.7 DSL 配置



要着手配置 DSL（请参见图 30.7 “DSL 配置” [568]），首先应选择 PPP 方式及 DSL 调制解调器连接到的 Ethernet 网卡（多数情况下是 eth0）。然后使用设备激活指定是否应在引导进程中建立 DSL 链接。单击用户控制可授权不具备根权限的普通用户通过 KInternet 激活或取消激活接口。使用该对话框还可以选择您所在的国家/地区，并可以在该区域内的若干 ISP 中进行选择。随后的所有 DSL 配置对话框的详细信息都取决于目前已设置的选项，因此下面几段只对这些对话框进行了简要介绍。有关可用选项的详细信息，请阅读这些对话框中提供的详细帮助信息。

要在独立工作站上使用按需拨号，还需指定名称服务器（DNS 服务器）。多数 ISP 都支持动态 DNS — 每次用户连接时，都由 ISP 发送名称服务器的 IP 地址。不过，对于单个工作站，应提供 192.168.22.99 之类的占位符地址。如果您的 ISP 不支持动态 DNS，请输入 ISP 提供的名称服务器 IP 地址。

空闲超时（秒）定义网络不活动的时间，一超过该时间即自动终止连接。合理的超时值介于 60 到 300 秒之间。如果禁用了按需拨号，则最好将超时值设置为零以防止自动挂断。

T-DSL 的配置与 DSL 的设置非常相似。只需将 *T-Online* 选为您的提供者，YaST 将打开 T-DSL 配置对话框。在此对话框中，提供 T-DSL 所需的一些其他信息——线路 ID、T-Online 号码、用户代码和密码。所有这些信息都会包含在订阅到 T-DSL 后收到的信息中。

30.5 使用 NetworkManager 管理网络连接

NetworkManager 是一种用于移动工作站的理想解决方案。有了 NetworkManager，您无需担忧要在更改位置时重配置网络接口和在网络之间切换。NetworkManager 可以自动连接到已知的 WLAN 网络。如果有两种或多种连接选择，则连接速度可能会更快一些。

NetworkManager 在以下情况下不适用：

- 您要通过一个接口使用多个提供商拨号。
- 您的计算机是网络的路由器。
- 您的计算机将为网络中的其他计算机（例如，DHCP 或 DNS 服务器）提供网络服务。
- 您的计算机为 Xen 服务器或您的系统是 Xen 内的虚拟系统。
- 您想在网络配置管理中使用 SCPM。如果同时使用 SCPM 和 NetworkManager，SCPM 就无法控制网络资源。请参阅第 27.5.1 节“SCPM 和 NetworkManager”[486]。
- 您想要同时使用多个活动的网络连接。

要在安装期间启用或禁用 NetworkManager，请单击网络配置的网络模式中的启用 NetworkManager 或禁用 NetworkManager。要在已安装系统上启用或禁用 NetworkManager，请遵循以下步骤：

- 1 打开 YaST。

2 选择网络设备 > 网卡。

3 在第一个屏幕上，将网络安装方法选项设置到使用 *NetworkManager* 的用户控制来使用 *NetworkManager*。要禁用 *NetworkManager*，将网络安装方法设置到通过 *ifup* 的传统方法。

选择方法后，请使用通过 DHCP 或静态 IP 地址的自动配置安装网卡，或配置您的调制解调器。在[第 30.4 节“使用 YaST 配置网络连接”](#) [555]和[第 29.1 节“无线 LAN”](#) [513]中查找 YaST 网络配置的描述。直接在 *NetworkManager* 中配置所支持的无线网卡。

要配置 *NetworkManager*，请使用 *NetworkManager* 小程序。*KDE* 和 *GNOME* 都具有各自的 *NetworkManager* 小程序。有关细节，请参见 *KDE 用户指南* 和 *GNOME 用户指南*。相应的小程序会随着桌面环境一起自动启动。该小程序之后会在系统盘中显示为图标。这两种小程序的功能相似，但是它们的接口有些不同。它们还能用在支持标准系统盘的其他图形环境中。

30.5.1 ifup 和 NetworkManager 的区别

如果使用 *NetworkManager* 进行网络安装，则可以使用一个小程序，随时从您的桌面环境内轻松地开关、停止或启动网络连接。*NetworkManager* 也可以改变和配置无线网卡连接，无需 `root` 特权。因此，*NetworkManager* 是一种用于移动工作站的理想解决方案。

使用 *ifup* 的传统配置也提供一些开关、停止或启动连接的方法，或需要或不需要用户参与（如用户管理设备），但通常需要 `root` 特权来改变或配置网络设备。这对于移动计算常常是个问题，因为移动计算不可能预配置所有的连接功能。

传统配置和 *NetworkManager* 都可以处理与无线网络（WEP、WPA-PSK 和 WPA-Enterprise 访问）、拨号连接和使用 DHCP 和静态配置的有线网络之间的网络连接。它们也支持通过 VPN 的连接。

NetworkManager 尝试使用可用的最好连接使您的计算机随时保持连接状态。如果可用，它使用最快的有线连接。如果网络电缆意外断开，它将尝试重连接。它可以从您的无线连接列表中找到带有最佳信号强度的网络并自动用其进行连接。要用 *ifup* 获得同样的功能，需要花功夫进行配置。

30.5.2 有关详细信息

有关 NetworkManager 的信息，可以从以下万维网站点和目录处获取：

- <http://www.gnome.org/projects/NetworkManager/>—NetworkManager 项目页
- <http://en.opensuse.org/Projects/KNetworkManager>—NetworkManager KNetworkManager 项目页

30.6 手动配置网络连接

应该始终将手动配置网络软件作为最后的选择。建议使用 YaST。但是，对网络配置背景信息的了解将对您使用 YaST 有所帮助。

可以通过热插拔检测并配置所有内置网卡及热插拔网卡（PCMCIA、USB 和某些 PCI 卡）。系统以两种不同的方式处理网卡，首先将其作为物理设备对待，其次将其作为接口对待。设备的插入或检测将触发一个热插拔事件。此热插拔事件通过脚本 hwup 触发设备的初始化。当将网卡作为新网络接口进行初始化时，内核将生成另一个热插拔事件，该事件触发通过 ifup 设置接口的操作。

内核按照接口注册的时间顺序对接口名进行编号。对于名称的指派，初始化顺序是决定性的。如果多个网卡中的一个失败，则所有随后初始化的网卡的编号将发生变化。对于真正的可热插拔网卡，连接设备的顺序非常重要。

为了实现灵活的配置，设备（硬件）的配置和接口的配置是分开进行的，配置到设备和接口的映射不再以接口名为基础进行管理。设备配置位于 `/etc/sysconfig/hardware/hwcfg-*` 中。接口配置位于 `/etc/sysconfig/network/ifcfg-*` 中。指派配置名的方式使这些名称可以描述所关联的设备和接口。因为以前从驱动程序到接口名的映射需要静态接口名，所以 `/etc/modprobe.conf` 中不再进行此映射。在新概念中，此文件中的别名项可能导致不希望出现的副作用。

配置名（`hwcfg-` 或 `ifcfg-` 后的任何内容）可以通过插槽、设备特定的 ID 或接口名对设备进行描述。例如，某个 PCI 卡的配置名可能是 `bus-pci-0000:02:01.0`（PCI 插槽）或 `vpid-0x8086-0x1014-0x0549`（厂商和产品 ID）。关联接口的名称可能是 `bus-pci-0000:02:01.0` 或 `wlan-id-00:05:4e:42:31:7a`（MAC 地址）。

若要将某个网络配置指派给某种类型的任何一个卡（一次只插入一个该类型的卡）而不是某个特定的卡，请选择不是非常特定的配置名。例如，可以将 `bus-pcmcia` 用于所有 PCMCIA 卡。另一方面，可以通过在前面加上接口类型对名称进行限制。例如，可以为连接在 USB 端口上的 WLAN 卡指派 `wlan-bus-usb`。

系统始终使用对接口或提供接口的设备描述最清楚的配置。搜索最合适的配置是由 `getcfg` 处理的。`getcfg` 的输出提供可用于描述设备的所有信息。`getcfg` 的手册页中介绍了有关指定配置名的详细信息。

使用上面介绍的方法，即使不总是以相同的顺序初始化网络设备，也可以用正确的配置对网络接口进行配置。但是，接口的名称仍取决于初始化顺序。有两种方法可以确保对特定网卡的接口进行可靠的访问：

- `getcfg-interfaceconfiguration name` 返回关联的网络接口的名称。因此，在某些配置文件中，可以输入配置名（例如，防火墙、`dhcpcd`、路由、多种虚拟网络接口（隧道））而不是非持久的接口名。
- 自动向每个接口指定永久接口名。可以根据需要调整它们。创建接口名时，请按 `/etc/udev/rules.d/30-net_persistent_names.rules` 中所述继续。但是，持久性名称 `pname` 不应该与内核可能自动指派的名​​称相同。因此，不允许使用 `eth*`、`tr*` 和 `wlan*` 等名称。请改用 `net*` 或者像 `external`、`internal` 或 `dmz` 等描述性名称。确保同一个接口名仅使用一次。接口名中的字符的范围是 `[a-zA-Z0-9]`。只能紧接在接口注册之后为接口指派持久性名称，这意味着必须重装载网卡的驱动程序或者必须执行 `hwupdevice description`。命令 `rcnetworkrestart` 不足以实现此目的。

重要：使用持久性接口名

持久性接口名的使用尚未在所有领域中进行测试。因此，某些应用程序不能顺畅地处理所选的接口名。

`ifup` 需要现有的接口，因为它不初始化硬件。硬件的初始化是由命令 `hwup` 处理的（由 `hotplug` 或 `coldplug` 执行）。当初始化设备时，将通过 `hotplug` 为新接口自动执行 `ifup`，如果启动方式是 `onboot`、`hotplug` 或 `auto` 并且启动了 `network` 服务，则将设置接口。以前，命令 `ifupinterfacename` 触发硬件初始化。目前的过程与以前的过程相反。首先初始化硬件部件，随后执行所有其他操作。这样，使用现有的这组配置，总能以可能的最佳方式配置数目不固定的设备。

表 30.5 “手动网络配置脚本”[573]总结了网络配置中所涉及的最重要的脚本。只要有可能，硬件和接口将对脚本进行区分。

表 30.5 手动网络配置脚本

配置阶段	命令	功能
硬件	hw{up,down,status}	热插拔子系统执行此 hw* 脚本来初始化设备、撤消初始化或查询设备的状态。hwup 的手册页中提供了详细信息。
接口	getcfg	getcfg 可用于查询与配置名或硬件描述关联的接口名。getcfg 的手册页中提供了详细信息。
接口	if{up,down,status}	if* 脚本启动现有的网络接口或返回指定接口的状态。ifup 的手册页中提供了详细信息。

有关热插拔和持久性设备名的详细信息在第 21 章 使用 udev 进行动态内核设备管理[419]中有所介绍。

30.6.1 配置文件

本节对网络配置文件进行了概述并解释了它们的作用和所使用的格式。

/etc/syconfig/hardware/hwcfg-*

这些文件包含网卡和其他设备的硬件配置。它们包含所需的参数，例如内核模块、启动方式和脚本关联。有关详细信息，请参见 hwup 的手册页。不管现有硬件如何，都会在启动冷插拔时应用 hwcfg-static-* 配置。

/etc/sysconfig/network/ifcfg-*

这些文件包含网络接口的配置。它们包含启动方式和 IP 地址等信息。可能的参数在 ifup 的手册页中有所介绍。另外，如果应将常规设置只用于一个接口，则文件 dhcp、wireless 和 config 中的所有变量都可用于 ifcfg-* 文件。

/etc/sysconfig/network/{config,dhcp,wireless}

文件 config 包含 ifup、ifdown 和 ifstatus 行为的常规设置。dhcp 包含用于无线 LAN 卡的 DHCP 和 wireless 设置。对所有这三个配置文件中的变量都进行了注释，它们还可用于 ifcfg-* 文件中，该文件将以较高的优先级处理这三个配置文件。

/etc/sysconfig/network/{routes,ifroute-*}

在这里确定 TCP/IP 包的静态路由。在 /etc/sysconfig/network/routes 文件中输入各种系统任务所需的所有静态路由：主机的路由、主机通过网关的路由以及网络的路由。对于需要个别路由的每个接口，定义另一个配置文件：/etc/sysconfig/network/ifroute-*。用接口名称替换 *。路由选择配置文件中的项如下所示：

# Destination	Dummy/Gateway	Netmask	Device
#			
127.0.0.0	0.0.0.0	255.255.255.0	lo
204.127.235.0	0.0.0.0	255.255.255.0	eth0
default	204.127.235.41	0.0.0.0	eth0
207.68.156.51	207.68.145.45	255.255.255.255	eth1
192.168.0.0	207.68.156.51	255.255.0.0	eth1

路由目标位于首列。此列可以包含网络或主机的 IP 地址，或者在有可访问名称服务器时，包含完全限定的网络或主机名。

第二列包含默认网关或通过其可访问主机或网络的网关。第三列包含网关后的网络或主机的子网掩码。例如，网关后主机的掩码为 255.255.255.255。

第四列只与本地主机连接的网络有关，如回路、Ethernet、ISDN、PPP 和虚拟设备。必须在此输入设备名。

（可选）可以使用第五列来指定路由的类型。不需要的列中应该包含一个减号-，这样才能确保分析程序正确解析命令。关于详细信息，请参见 `routes(5)` 手册页。

/etc/resolv.conf

在此文件中指定主机所属的域（关键字 `search`）。同时列出的还有要访问的名称服务器地址的状态（关键字 `nameserver`）。可以指定多个域名。当解析不是完全限定的名称时，将尝试通过附加单独的 `search` 项生成一个完全限定的名称。通过输入多行可以输入多个名称服务器，每行都以 `nameserver` 开头。注释以 `#` 符号开头。YaST 在此文件中输入指定的名称服务器。**例 30.5** “`/etc/resolv.conf`” [575] 显示 `/etc/resolv.conf` 的内容。

例 30.5 `/etc/resolv.conf`

```
# Our domain
search example.com
#
# We use sun (192.168.0.20) as nameserver
nameserver 192.168.0.20
```

某些服务（例如 `pppd(wvdial)`、`ipppd(isdn)`、`dhcpcd` 和 `dhclient`）、`pcmcia` 和 `hotplug` 通过脚本 `modify_resolvconf` 修改文件 `/etc/resolv.conf`。如果文件 `/etc/resolv.conf` 已被此脚本临时修改，则它将包含预定义的注释，给出有关修改它的服务的信息、备份原始文件的位置以及如何关闭自动修改机制。如果 `/etc/resolv.conf` 被多次修改，则该文件以嵌套的形式包括修改。即使还原的顺序不同于进行修改的顺序，也可以以一种彻底的方式进行还原。可能需要这种灵活性的服务包括 `isdn`、`pcmcia` 和 `hotplug`。

如果未以正常、彻底的方式终止服务，则可以使用 `modify_resolvconf` 恢复原始文件。另外，在系统引导时，将检查是否有由未彻底终止产生的、经修改的 `resolv.conf`（例如，系统崩溃后），如果有，则将恢复原始（未经修改的）`resolv.conf`。

YaST 使用命令 `modify_resolvconfcheck` 检查 `resolv.conf` 是否已被修改并将随后警告用户这些更改将在恢复文件后丢失。除此之外，YaST 将不使用 `modify_resolvconf`，这意味着通过 YaST 更改 `resolv.conf` 的效果与

任何手动更改的效果相同。在两种情况下，更改都具有永久效果。上述服务请求的修改只是临时的。

/etc/hosts

在此文件中，如 [例 30.6](#) “/etc/hosts” [576] 中所示，将为主机名指派 IP 地址。如果未实施名称服务器，则将其建立 IP 连接的所有主机必须列在此处。在此文件中为每个主机输入一行，包含 IP 地址、完全限定的主机名和主机名。IP 地址必须在每行的开头，各项用空格和制表符隔开。注释总是以 # 符号开头。

例 30.6 /etc/hosts

```
127.0.0.1 localhost
192.168.0.20 sun.example.com sun
192.168.0.1 earth.example.com earth
```

/etc/networks

在这里，网络名称被转换为网络地址。格式类似于 hosts 文件的格式，只是网络名称在地址的前面。请参阅 [例 30.7](#) “/etc/networks” [576]。

例 30.7 /etc/networks

```
loopback      127.0.0.0
localnet      192.168.0.0
```

/etc/host.conf

此文件控制名称解析，即通过解析程序库转换主机名和网络名称。此文件只用于链接到 libc4 或 libc5 的程序。对于当前的 glibc 程序，请参见 /etc/nsswitch.conf 中的设置。参数必须始终单独在一行上。注释以 # 符号开头。[表 30.6](#) “/etc/host.conf 的参数” [577] 显示了可用的参数。[例 30.8](#) “/etc/host.conf” [577] 中显示了 /etc/host.conf 的示例。

表 30.6 /etc/host.conf 的参数

order hosts, bind	指定访问服务以进行名称解析的顺序。可用参数有（使用空格或逗号隔开）： hosts: 搜索 /etc/hosts 文件 bind: 访问名称服务器 nis: 使用 NIS
multi on/off	定义 /etc/hosts 中输入的主机是否可以具有多个 IP 地址。
nospoof on spoofalert on/off	这些参数影响名称服务器 <i>spoofing</i> ，但除此之外，它们对网络配置没有任何影响。
trim domainname	在主机名解析后，指定的域名与主机名分开（只要主机名包括域名）。此选项仅当来自本地域的名称在 /etc/hosts 文件中时才可用，但仍要用附加的域名进行组织。

例 30.8 /etc/host.conf

```
# We have named running
order hosts bind
# Allow multiple addrs
multi on
```

/etc/nsswitch.conf

GNU C Library 2.0 的引入与 名称服务转换 (NNS) 的引入是同时进行的。有关详细信息，请参见 nsswitch.conf (5) 手册页和 *GNU C Library 参见手册*。

查询的顺序是在文件 /etc/nsswitch.conf 中定义的。中显示了 nsswitch.conf 的示例。例 30.9 “/etc/nsswitch.conf” [578] 注释以 # 符号开头。在本例中，hosts 数据库下的项意味着通过 DNS 将请求发送到 /etc/hosts (files)。

例 30.9 */etc/nsswitch.conf*

```
passwd:      compat
group:       compat

hosts:       files dns
networks:    files dns

services:    db files
protocols:   db files

netgroup:    files
automount:   files nis
```

表 30.7 “通过 */etc/nsswitch.conf* 可用的数据库” [578] 中列出了 NSS 上可用的“数据库”。另外，近期将推出 automount、bootparams、netmasks 和 publickey。表 30.8 “NSS“数据库”的配置选项” [579] 中列出了 NSS 数据库的配置选项。

表 30.7 通过 */etc/nsswitch.conf* 可用的数据库

aliases	sendmail 实施的邮件别名；请参阅 man5 aliases。
ethers	Ethernet 地址。
组	getgrent 使用的用户组。另请参见 group 的手册页。
hosts	gethostbyname 和类似函数使用的主机名和 IP 地址。
netgroup	网络中用于控制访问权限的主机和用户列表，请参见 netgroup(5) 手册页。
networks	getnetent 使用的网络名称和地址。
密码	使用的用户密码；请参阅 passwd(5) getpwent 手册页。
protocols	网络协议，由 getprotoent 使用；请参阅 protocols(5) 手册页。

rpc	getrpcbyname和类似函数使用的远程过程调用名称和地址。
服务	getservent使用的网络服务。
shadow	用户阴影密码，由getspnam使用；请参阅 shadow(5) 手册页。

表 30.8 NSS“数据库”的配置选项

文件	直接访问文件，例如 /etc/aliases
db	通过数据库访问
nis、nisplus	NIS，另请参见 第 33 章 使用 NIS [597]
dns	仅可用作 hosts 和 networks 的扩展名
compat	仅可用作 passwd、shadow 和 group 的扩展名

/etc/nscd.conf

此文件用于配置 nscd（名称服务超速缓存守护程序）。请参见 nscd(8) 和 nscd.conf(5) 手册页。默认情况下，passwd 和 groups 的系统项由 nscd 进行缓存。这对于目录服务（例如 NIS 和 LDAP）的性能很重要，因为如果不是这样，每次访问名称或组都需要网络连接。默认情况下，不对 hosts 进行缓存，因为 nscd 中缓存主机的机制将导致本地系统无法信任正向和反向查找检查。请设置缓存 DNS 服务器，而不是让 nscd 缓存名称。

如果激活 passwd 的缓存，则通常需要 15 秒才能识别新添加的本地用户。通过使用命令 rcnscdrestart 重启动 nscd 可缩短此等待时间。

/etc/HOSTNAME

此文件提供不附带域名的主机名。当引导计算机时，此文件将被多个脚本读取。它可能只包含一行，该行中设置了主机名。

30.6.2 测试配置

向配置文件写配置之前，可对其进行测试。要设置测试配置，请使用 `ip` 命令。要测试连接，请使用 `ping` 命令。也可使用较早的配置工具 `ifconfig` 和 `route`。

命令 `ip`、`ifconfig` 和 `route` 会直接更改网络配置，而不会在配置文件中说明更改。如果未在正确的配置文件中输入配置，重引导时将丢失已更改的网络配置。

使用 `ip` 配置网络接口

`ip` 是用来显示和配置路由选择、网络设备、策略路由选择以及隧道的工具。它被设计为替换较早的工具 `ifconfig` 和 `route`。

`ip` 是非常复杂的工具。它的常用语法为 `ip options object command`。可使用以下对象：

链接

此对象表示网络设备。

地址

此对象表示设备的 IP 地址。

neighbour

此对象表示 ARP 或 NDISC 超速缓存项。

路由

此对象表示路由选择表项。

规则

此对象表示路由选择策略数据库中的规则。

maddress

此对象表示多路广播地址。

mroute

此对象表示多路广播路由超速缓存项。

tunnel

此对象表示 IP 上的隧道。

如果未提供命令，则将使用默认命令，通常为 `list`。

使用命令 `ip link set device_name command` 更改设备状态。例如，要取消激活设备 `eth0`，请输入 `ip link set eth0 down`。要重激活它，可使用 `ip link set eth0 up`。

激活设备后，可对设备进行配置。要设置 IP 地址，可使用 `ip addr add ip_address + dev device_name`。例如，要将接口 `eth0` 的地址设置为带标准广播（选项 `brd`）的 `192.168.12.154/30`，则输入 `ip addr add 192.168.12.154/30 brd + dev eth0`。

要拥有活动连接，还必须配置默认网关。要设置系统的网关，请输入 `ip route get gateway_ip_address`。要将一个 IP 地址转换为另一个 IP 地址，请使用 `nat:ip route add nat_ip_address via other_ip_address`。

要显示所有设备，可使用 `ip link ls`。要只显示正在运行的接口，可使用 `ip link ls up`。要打印设备的接口统计信息，可输入 `ip -s link ls device_name`。要查看设备的地址，请输入 `ip addr`。在 `ip addr` 的输出中，还可找到有关设备 MAC 地址的信息。要显示所有路由，可使用 `ip route show`。

有关使用 `ip` 的更多信息，请输入 `iphelp` 或查看 `ip(8)` 手册页。`help` 选项还可用于所有 `ip` 对象。例如，如果希望阅读 `ipaddr` 的帮助，请输入 `ipaddr help`。可在 `/usr/share/doc/packages/iproute2/ip-cref.pdf` 中找到 `ip` 手册。

使用 ping 测试连接

`ping` 命令是用于测试 TCP/IP 连接是否有效的标准工具。它使用 ICMP 协议来将小数据包和 `ECHO_REQUEST` 数据报文发送到目标主机，并请求即时答复。如果发送有效，`ping` 将据此显示一条讯息，指明网络链接基本有效。

`ping` 不仅能测试两台计算机之间的连接：它还能提供关于连接质量的基本信息。在例 30.10 “命令 `ping` 的输出” [582] 中，可查看 `ping` 输出示例。倒数第二行包含有关已发送的包数、丢失的包和 `ping` 运行的总时间量的信息。

您可以使用主机名或 IP 地址（例如 `pingexample.com` 或 `ping130.57.5.75`）作为目标。程序会一直发送包，直到您按 **Ctrl + C**。

如果只需要检查连接功能，则可使用 `-c` 选项来限制包数。例如，要将 `ping` 限制为三个包，请输入 `ping-c 3 192.168.0.`。

例 30.10 命令 `ping` 的输出

```
ping -c 3 example.com
PING example.com (130.57.5.75) 56(84) bytes of data.
64 bytes from example.com (130.57.5.75): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (130.57.5.75): icmp_seq=2 ttl=49 time=184 ms
64 bytes from example.com (130.57.5.75): icmp_seq=3 ttl=49 time=183 ms
--- example.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 183.417/185.447/188.259/2.052 ms
```

两个包之间的默认时间间隔为一秒。`ping` 提供了选项 `-i` 来更改时间间隔。例如，要将 `ping` 时间间隔延长为十秒，则输入 `ping-i 10 192.168.0.`。

在带有多个网络设备的系统中，有时通过特定接口地址发送 `ping` 将会非常有用。要执行此操作，可将 `-I` 选项结合选定设备名称一起使用，例如 `ping-I wlan1 192.168.0.`。

有关使用 `ping` 的更多选项和信息，请输入 `ping-h` 或查看 `ping (8)` 手册页。

使用 `ifconfig` 配置网络

`ifconfig` 是传统的网络配置工具。与 `ip` 相比，您只能将 `ifconfig` 用于接口配置。如果希望配置路由选择，可使用 `route`。

注意: `ifconfig` 和 `ip`

程序 `ifconfig` 已过时。请使用 `ip`。

毫无疑问，`ifconfig` 可显示当前活动接口的状态。在例 30.11 “命令 `ifconfig` 的输出”[583]中可见 `ifconfig` 具有非常整齐和详细的输出。输出的第一行中还包含关于设备 MAC 地址的信息和 `HWaddr` 的值。

例 30.11 命令 `ifconfig` 的输出

```
eth0      Link encap:Ethernet  HWaddr 00:08:74:98:ED:51
          inet6 addr: fe80::208:74ff:fe98:ed51/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:634735 errors:0 dropped:0 overruns:4 frame:0
          TX packets:154779 errors:0 dropped:0 overruns:0 carrier:1
          collisions:0 txqueuelen:1000
          RX bytes:162531992 (155.0 Mb)  TX bytes:49575995 (47.2 Mb)
          Interrupt:11 Base address:0xec80

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8559 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8559 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:533234 (520.7 Kb)  TX bytes:533234 (520.7 Kb)

wlan1     Link encap:Ethernet  HWaddr 00:0E:2E:52:3B:1D
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20e:2eff:fe52:3b1d/64 Scope:Link
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50828 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43770 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:45978185 (43.8 Mb)  TX bytes:7526693 (7.1 Mb)
```

有关使用 `ifconfig` 的更多选项和信息，请输入 `ifconfig-h` 或参阅 `ifconfig` (8) 手册页。

使用 `route` 配置路由选择

`route` 是用于操作 IP 路由选择表的程序。可使用它来查看路由选择配置和添加或去除路由。

注意: `route` 和 `ip`

程序 `route` 已过时。请使用 `ip`。

如果需要有关路由选择配置的快速而又易懂的信息来确定路由选择问题，则 `route` 将非常有用。要查看当前路由配置，请输入 `route-n` 作为 `root`。

例 30.12 命令 `-n` 的输出

```
route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags   MSS Window  irtt Iface
10.20.0.0        *               255.255.248.0   U        0  0        0 eth0
link-local       *               255.255.0.0     U        0  0        0 eth0
loopback         *               255.0.0.0       U        0  0        0 lo
default          styx.exam.com   0.0.0.0         UG       0  0        0 eth0
```

有关使用 `route` 的更多选项和信息，请输入 `route-h` 或参阅 `route (8)` 手册页。

30.6.3 启动脚本

除了上面介绍的配置文件之外，还有多个脚本在引导计算机时装载网络程序。只要系统切换到某个多用户运行级别，就将启动这些脚本。中介绍了其中的一些脚本。[表 30.9 “网络程序的一些启动脚本” \[584\]](#)。

表 30.9 网络程序的一些启动脚本

<code>/etc/init.d/network</code>	此脚本处理网络接口的配置。硬件必须已被 <code>/etc/init.d/coldplug</code> （通过 <code>hotplug</code> ）初始化。如果未启动 <code>network</code> 服务，当通过热插拔插入网络接口时，不实施任何网络接口。
<code>/etc/init.d/inetd</code>	启动 <code>xinetd</code> 。 <code>xinetd</code> 可用于在系统上提供服务器服务。例如，它可以在初始化 <code>FTP</code> 连接时启动 <code>vsftpd</code> 。
<code>/etc/init.d/portmap</code>	启动 <code>RPC</code> 服务器所需的端口映射器，例如 <code>NFS</code> 服务器。
<code>/etc/init.d/nfsserver</code>	启动 <code>NFS</code> 服务器。
<code>/etc/init.d/postfix</code>	控制 <code>postfix</code> 进程。
<code>/etc/init.d/ypserv</code>	启动 <code>NIS</code> 服务器。

30.7 作为拨号助手的 smpppd

部分家庭用户不具备连接到因特网的专线。而是使用拨号连接。根据所用的拨号方法（ISDN 或 DSL），连接受 `ippd` 或 `pppd` 的控制。基本上，只要正确启动这些程序就可以联网了。

如果采用包月付费方式（拨号连接不产生任何附加费用），则只需启动相应的守护程序。用 KDE 小程序或命令行界面来控制拨号连接。如果因特网网关不是您所用的主机，最好通过网络主机来控制拨号连接。

这时就需要 `smpppd` 了。该程序为辅助程序提供统一的界面，并且可以双向执行。首先，它要对所需的 `pppd` 或 `ippd` 编程，并控制其拨号属性。然后，向用户程序提供各种提供商，并传送有关当前连接状态的信息。由于还可以通过网络来控制 `smpppd`，该程序适用于从专用子网中的工作站控制与因特网的拨号连接。

30.7.1 配置 smpppd

YaST 可以自动配置由 `smpppd` 提供的连接。同时还会预先配置实际的拨号程序 `KInternet` 和 `cinternet`。只有在配置 `smpppd` 的附加功能（如远程控制）时，才需要手动设置。

`smpppd` 的配置文件为 `/etc/smpppd.conf`。默认情况下并未启用远程控制。此配置文件最重要的选项包括：

`open-inet-socket = yes/no`

要通过网络控制 `smpppd`，必须将此选项设置为 `yes`。`smpppd` 的监听端口为 3185。如果此参数设置为 `yes`，则还需相应设置 `bind-address`、`host-range` 和 `password` 等参数。

`bind-address = ip address`

如果主机有多个 IP 地址，使用此参数可以确定 `smpppd` 应在哪个 IP 地址上接受连接。默认值是监听所有地址。

`host-range = min ip max ip`

参数 `host-range` 用于定义网络范围。IP 地址属于这一范围的主机将被授予访问 `smpppd` 的权限。此范围之外的所有主机均不具备访问权。

`password = password`

通过指派密码可使客户机仅限于授权主机。由于这是个纯文本密码，不应高估该密码提供的安全性。如果未指派任何密码，所有客户机都有权访问 `smpppd`。

`slp-register = yes/no`

使用此参数，可以通过 SLP 在网络中声明 `smpppd` 服务。

关于 `smpppd` 的详细信息，请参见 `smpppd(8)` 和 `smpppd.conf(5)` 手册页。

30.7.2 配置供远程使用的 KInternet、cinternet 和 qinternet

KInternet、cinternet 和 qinternet 可用于控制本地或远程 `smpppd`。cinternet 是图形 KInternet 的命令行版本。qinternet 与 KInternet 基本相同，但不使用 KDE 库，所以可以在没有 KDE 库的情况下使用，并且必须单独安装。要使这些实用程序可用于远程 `smpppd`，请手动编辑配置文件 `/etc/smpppd-c.conf` 或使用 KInternet。此文件仅使用三个选项：

`sites = list of sites`

此选项可以向前端通知 `smpppd` 的搜索位置。前端将按照在此指定的选项顺序来测试这些选项。选项 `local` 指示与本地 `smpppd` 建立连接。`gateway` 指向网关上的 `smpppd`。将按照 `config-file` 的 `server` 中的指定建立连接。`slp` 指示前端连接通过 SLP 发现的 `smpppd`。

`server = server`

在此指定 `smpppd` 运行所在的主机。

`password = password`

插入为 `smpppd` 选择的密码。

如果 `smpppd` 处于活动状态，现在即可访问它，例如通过 `cinternet--verbose--interface-list` 来访问。如果此时遇到困难，请参见 `smpppd-c.conf(5)` 和 `cinternet(8)` 手册页。

网络中的 SLP 服务

制定 *服务位置协议* (SLP) 是为了简化本地网络中联网客户机的配置。要配置网络客户机（包括所有必需服务），管理员通常需要对网络中提供的服务器有详细了解。SLP 可以向本地网络中的所有客户机声明选中服务是否可用。支持 SLP 的应用程序则可以利用这一发布信息并进行自动配置。

SUSE Linux Enterprise® 支持使用 SLP 提供的安装源进行安装，并且包含许多集成了 SLP 支持的系统服务。YaST 和 Konqueror 都有适用于 SLP 的前端。您可以使用 SLP 为联网客户机（如系统上的安装服务器、文件服务器或打印服务器）提供核心功能。

重要: SUSE Linux Enterprise 中的 SLP 支持

提供 SLP 支持的服务包括 cupsd、rsyncd、ypserv、openldap2、openwbem (CIM)、ksysguardd、saned、kdm vnc login、smpppd、rpasswd、postfix 和 sshd（通过 fish）。

31.1 激活 SLP

要用 SLP 提供服务，您的系统上必须运行 slpd。如果只需发出服务查询，则不必启动此守护程序。类似 SUSE Linux Enterprise 中的大多数系统服务，slpd 守护程序通过单独的初始化脚本来控制。默认情况下该守护程序处于非活动状态。要在会话期间激活该守护程序，请以 root 身份运行 `rcslpdstart` 来启动它，运行 `rcslpdstop` 来停止它。使用 `restart` 或 `status` 可分别执行重启或状态检查。如果默认激活 slpd，请在 YaST 系统 > 系统服务（运行级别）中启用

slpd，或以 root 身份运行一次 `insserv slpd` 命令。这样即可在引导系统时将 slpd 自动加入要启动的一组服务。

31.2 SUSE Linux Enterprise 中的 SLP 前端

要查找您网络中 SLP 提供的服务，请使用 SLP 前端。SUSE Linux Enterprise 包含几个前端：

slptool

slptool 是一个简单的命令行程序，可用于在网络中声明 SLP 查询或声明专有服务。slptool--help 列出了所有可用选项和功能。也可以从处理 SLP 信息的脚本调用 slptool。

YaST SLP 浏览器

YaST 包含一个单独的 SLP 浏览器，可以在树图中列出本地网络中通过 SLP 声明的所有服务。用 *网络服务 > SLP 浏览器* 查找它。

Konqueror

用作网络浏览器时，Konqueror 可以在 `slp:/` 中显示本地网络中的所有可用的 SLP 服务。单击主窗口中的图标可获得有关相关服务的详细信息。如果在 Konqueror 中使用 `service:/`，在浏览器窗口中单击相关图标可与选定服务建立连接。

31.3 用 SLP 提供服务

SUSE Linux Enterprise 中的许多应用程序都已使用 libslp 库集成了 SLP 支持。如果服务未集成 SLP 支持，请使用以下方法之一使其可通过 SLP 声明。

通过 /etc/slp.reg.d 进行的静态注册

为每个新服务创建单独的注册文件。下面显示了注册扫描仪服务的文件的示例：

```
## Register a saned service on this system
## en means english language
## 65535 disables the timeout, so the service registration does
## not need refreshes
service:scanner.sane://$HOSTNAME:6566,en,65535
```



```
watch-port-tcp=6566
description=SANE scanner daemon
```

此文件中最重要的一行是以 *service:* 开头的服务 URL。其中包含服务类型 (scanner.sane) 以及该服务在服务器上的地址。*\$HOSTNAME* 自动用完整主机名替换。随后是可以找到相关服务的 TCP 端口的名称, 端口与主机名之间用冒号分隔。然后输入服务的显示语言及以秒计的注册持续时间。应该用逗号分隔服务 URL 之后的各项内容。将注册持续时间设置为 0 到 65535 之间的值。0 表示禁止注册。65535 表示取消所有限制。

注册文件中还包含两个变量, *watch-tcp-port* 和 *description*。*watch-tcp-port* 链接 SLP 服务, 声明相关服务是否是通过使 *slpd* 检查服务的状态来激活的。第二个变量为显示在适合的浏览器中的服务提供了更为准确的说明。

通过 */etc/slp.reg* 进行的静态注册

与 */etc/slp.reg.d* 过程的唯一差别即在于: 这种注册方式要将所有服务都集中到一个核心文件中。

使用 *slptool* 进行的动态注册

如果应该从专有脚本为某项服务注册 SLP 支持, 请使用 *slptool* 命令行前端。

31.4 有关详细信息

以下来源提供了有关 SLP 的详细信息:

RFC 2608、2609、2610

RFC 2608 主要说明了 SLP 的定义。RFC 2609 更详细地说明了所用服务 URL 的语法; RFC 2610 则对通过 SLP 的 DHCP 进行了说明。

<http://www.openslp.org/>

OpenSLP 项目的主页。

/usr/share/doc/packages/openslp

此目录包含有关 SLP 的所有现有文档, 其中包括 *README.SuSE* (包含 SUSE Linux Enterprise 详细信息、上述 RFC 和两个介绍性的 HTML 文档)。要使用 SLP 功能的编程人员应该安装 *openslp-devel* 包, 以便参见随包附带的 *编程人员指南*。

使用 NTP 同步时间

NTP（网络时间协议）机制是用于同步网络上的系统时间的协议。首先，计算机从作为可靠时间源的服务器获得时间。然后将此计算机用作网络中其他计算机的时间源。这样做有双重目的：既可维护绝对时间，又可保持网络中所有计算机系统时间的同步。

维护确切的系统时间在许多情况下都非常重要。内置硬件(BIOS)时钟往往不能满足数据库这样的应用程序的要求。手动更正系统时间可能会导致许多严重问题，例如向后调整时间将使关键应用程序出现故障。在网络中，通常需要同步所有计算机上的系统时间，但是手动调整时间是一种不好的方法。`xntp` 提供了解决这些问题的机制。该机制随时借助网络中的可靠时间服务器调整系统时间。它还支持对本地参考时钟（如无线电控制的时钟）进行管理。

注意

要通过 Active Directory 启用时间同步，请遵循[加入 AD 域 \[282\]](#)中的说明。

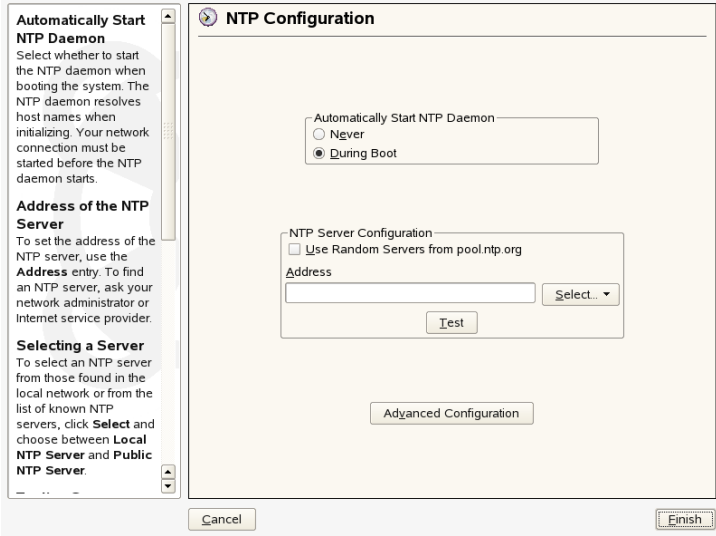
32.1 使用 YaST 配置 NTP 客户机

`xntp` 已预先设置为以本地计算机时钟为时间参考。但是，只有在没有更精确的时间源的情况下才使用 (BIOS) 时钟最为替代。YaST 为 NTP 客户机的配置提供方便。对于不运行防火墙的系统，请使用快速或高级配置。对于受到防火墙保护的系统，高级配置可能打开 `SuSEfirewall2` 中需要的端口。

32.1.1 快速的 NTP 客户机配置

快速 NTP 客户机配置（网络服务>NTP 配置）由两个对话框组成。在第一个对话框中设置 xntpd 的启动方式和要查询的服务器。要在引导系统时自动启动 xntpd，请单击引导期间。然后指定 NTP 服务器配置。如果不能使用本地时间服务器，则单击使用来自 pool.ntp.org 的随机服务器，或者单击选择访问要为网络选择合适的时间服务器的第二个对话框。

图 32.1 YaST：配置 NTP 客户机

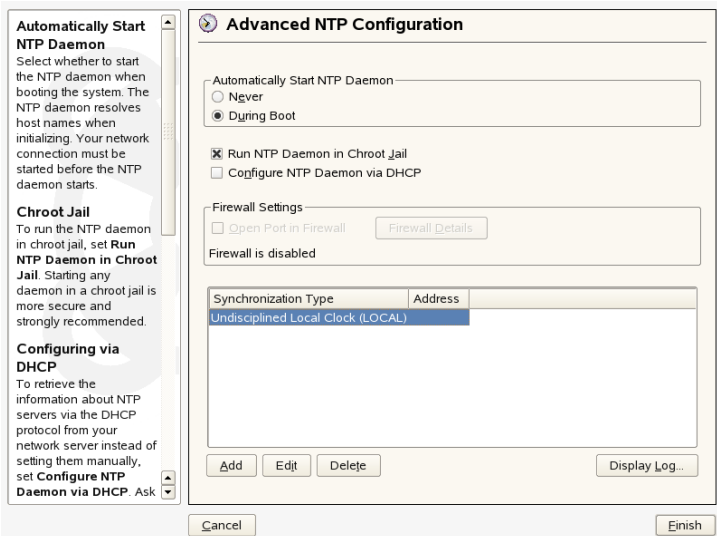


在详细的服务器选择对话框中，确定是使用本地网络中（本地 NTP 服务器）的时间服务器实施时间同步，还是使用考虑到所在时区的基于因特网的时间服务器（公共 NTP 服务器）实施时间同步。要使用本地时间服务器，请单击查找启动 SLP 查询，查找网络中的可用时间服务器。从搜索结果列表中选择最适合的时间服务器，然后单击确定退出该对话框。要使用公共时间服务器，请选择您所在的国家或地区（时区），并从公共 NTP 服务器列表中选择适合的服务器，然后单击确定退出该对话框。在主对话框中，可单击测试测试选定服务器的可用性，单击完成退出该对话框。

32.1.2 高级 NTP 客户机配置

选择快速配置中所述的启动方式之后，可以通过选择NTP 客户机模块的主对话框中的高级配置对 NTP 客户机进行复杂配置（如图 32.1 “YaST：配置 NTP 客户机” [592]所示）。

图 32.2 YaST：复杂的 NTP 配置



在高级 NTP 配置中，确定是否应在 chroot jail 中启动 xntpd。默认情况下，在 Chroot Jail 中运行 NTP 守护程序是被激活的。在 chroot jail 中启动可以在遭受通过 xntpd 发起的攻击时提高安全性，因为这种方式可以防止攻击者危害整个系统。选择通过 DHCP 配置 NTP 守护程序，可以设置 NTP 客户机通过 DHCP 获取网络中可用的 NTP 服务器列表。

如果 SuSEfirewall 为默认的活动状态，则请启用打开防火墙中的端口。如果保持端口的关闭状态，则不可能建立与事件服务器的连接。

供客户机查询的服务器和其他时间资源列在下半部分。使用添加、编辑和删除可按需修改此列表。显示日志使您能够查看客户机的日志文件。

单击添加可添加新的时间信息源。在随后的对话框中，选择要与其进行时间同步的源类型。下列选项可用：

服务器

可供您选择 NTP 服务器的另一个对话框（如第 32.1.1 节“快速的 NTP 客户机配置”[592]所述）。激活用于初始同步，可以在引导系统时触发服务器和客户机之间的时间信息同步。选项使您可以指定 xntpd 的其他选项。有关详细信息，请参见 /usr/share/doc/packages/xntp-doc（xntp-doc 包的一部分）。

同级

同级是一台要与其建立对称关系的计算机：它将同时用作时间服务器和客户机。要在同一网络中用同级代替某个服务器，请输入系统的地址。该对话框的其他部分与服务器对话框相同。

无线电时钟

要在系统中使用无线电时钟来同步时间，请在此对话框中输入时钟类型、单元号码、设备名和其他选项。单击驱动程序校准可对该驱动程序进行微调。有关本地无线电时钟如何操作的详细信息，请参见 /usr/share/doc/packages/xntp-doc/refclock.html。

发出的广播

也可以通过在网络内广播的方式来传送时间信息和查询。在此对话框中，输入应将这类广播信息发送到的地址。除非使用了像无线电控制的时钟这样的可靠时间源，否则不要激活广播。

进来的广播

如果希望客户机通过广播接收信息，请在此字段中输入应接受来自哪个地址的相应数据包。

32.2 在网络中配置 xntp

要使用网络中的时间服务器，最简便的方式就是设置服务器参数。例如，如果可以从网络访问名为 ntp.example.com 的时间服务器，请通过添加以下行将其名称添加到文件 /etc/ntp.conf 中：

```
server ntp.example.com
```

要添加更多时间服务器，请使用关键字 server 插入更多行。使用命令 rcntpd start 初始化 xntpd 后，等待时间稳定并且创建用于更正本地计算机时钟的偏移文件需要大约一个小时的时间。利用偏移文件，只要计算机一启动，就可以

计算出硬件时钟的系统误差。可以立即使用更正功能，使系统时间保持较高的稳定性。

有两种方法可将 NTP 机制用作客户机：第一种方法是客户机可以定期从已知服务器查询时间。在存在许多客户机的情况下，这种方法会给服务器带来很高的负荷。第二种方法是客户机可以等待网络中的广播时间服务器发送 NTP 广播。这种方法的缺点在于服务器的可靠性是未知的，而且如果服务器发出错误信息将导致严重问题。

如果通过广播获取时间，则不需要服务器名称。此时只需在配置文件 `/etc/ntp.conf` 中输入 `broadcastclient` 一行。要以独占方式使用一个或多个已知时间服务器，请在以 `servers` 开头的行中输入它们的名称。

32.3 设置本地参考时钟

软件包 `xntp` 包含用于连接本地参考时钟的驱动程序。`xntp-doc` 包的文件 `/usr/share/doc/packages/xntp-doc/refclock.html` 中提供了受支持时钟的列表。每个驱动程序都有一个关联数字。在 `xntp` 中，实际配置是通过伪 IP 地址来完成的。时钟被输入 `/etc/ntp.conf` 文件，就像已经在网络中存在一样。为此专门给它们指派了 `127.127.t.u` 格式的特殊 IP 地址。其中 `t` 代表时钟的类型并确定要使用的驱动程序，`u` 代表设备并确定要使用的接口。

通常，各个驱动程序都有特殊的参数来描述配置详细信息。文件 `/usr/share/doc/packages/xntp-doc/drivers/driverNN.html`（其中 `NN` 是驱动程序的编号）提供了有关特定类型时钟的信息。例如，“8 型”时钟（通过串行接口的无线电时钟）需要额外的方式更精确地指定时钟。以 Conrad DCF77 接收模块为例，该模块需要使用 `mode 5`。要使用此时钟作为首选参考，应指定关键字 `prefer`。由此构成的 Conrad DCF77 接收模块的完整 `server` 行如下：

```
server 127.127.8.0 mode 5 prefer
```

其他时钟也采用相同的模式。安装 `xntp-doc` 包之后，可以在目录 `/usr/share/doc/packages/xntp-doc/` 中找到 `xntp` 的文档。文件 `/usr/share/doc/packages/xntp-doc/refclock.html` 提供指向描述驱动程序参数的驱动程序页的链接。

使用 NIS

一旦网络内的多个 UNIX 系统都要访问公共资源，那么对于该网络内的所有计算机，所有用户和组身份是否相同就显得很重要了。网络对用户应该是透明的：无论他们用哪台计算机，他们总觉得是在同样的环境中。可以通过 NIS 和 NFS 服务完成此操作。NFS 通过网络分发文件系统，详细信息请参见 [第 37 章 通过 NFS 共享文件系统](#) [635]。

NIS（网络信息服务）可以说是一种数据库式服务，用于跨网络访问 `/etc/passwd`、`/etc/shadow` 和 `/etc/group` 的内容。NIS 也可用于其他目的（如提供 `/etc/hosts` 或 `/etc/services` 之类文件的内容），但这里不作介绍。人们常把 NIS 称作 *YP*，也就是网络中的“电话黄页”。

33.1 配置 NIS 客户机

使用 YaST 模块 *NIS 客户程序* 将工作站配置为使用 NIS。请选择主机是已有静态 IP 地址，或接受由 DHCP 发布的静态 IP 地址。DHCP 还提供 NIS 域和 NIS 服务器。如果使用静态 IP 地址，请手动指定 NIS 域和 NIS 服务器。请参阅 [图 33.1 “设置 NIS 服务器的域和地址”](#) [598]。使用查找可让 YaST 在整个网络中搜索活动的 NIS 服务器。根据本地网络的大小，此进程可能会耗费一定的时间。广播可在指定的服务器没有响应后，在本地网络中寻找 NIS 服务器。

也可通过在 *NIS 服务器地址* 中输入服务器地址（用空格分隔）来指定多个服务器。

根据本地安装，您可能还想激活 automounter。如果需要，此选项还会安装其他软件。

在专家设置中，如果不希望其他主机能查询您的客户机所用的服务器，请取消选中只应答本地主机。通过选中断开的服务器，客户机将能够接收通过非特权端口通讯的服务器的答复。有关进一步信息，请参阅 `manypbind`。

完成设置后，请单击完成保存更改并返回 YaST 控制中心。

图 33.1 设置 NIS 服务器的域和地址

Enter your NIS domain, such as `example.com`, and the NIS server's address, such as `nis.example.com` or `10.20.1.1`.

Specify multiple servers by separating their addresses with spaces.

The **Broadcast** option enables searching in the local network to find a server after the specified servers fail to respond. It is a security risk.

If you are using **DHCP** and the server provides the NIS domain name or servers, you can enable their use here. DHCP itself can be set up in the network module.

Automounter is a daemon that mounts directories automatically, such as users' home directories. It is assumed that its configuration files (`auto*`) already exist, either locally or over NIS.

Configuration of NIS client

☐ Do not use NIS
☒ Use NIS

NIS client—
☐ Automatic Setup (via DHCP)
☒ Static Setup

NIS Domain

Addresses of NIS servers

☐ Broadcast

Additional NIS Domains

☐ Start Automounter

配置 eDirectory 鉴定

可以用 Novell® Linux User Management (LUM) 配置网络上的 SUSE® Linux Enterprise Desktop 工作站，这样用户就可以用他们的 Novell eDirectory™ 用户名和密码而不是他们本地的 Linux 工作站用户名和密码登录到它们。用 LUM 和 eDirectory 管理用户登录信息，就不必在每台 SUSE Linux Enterprise Desktop 工作站上的 `/etc/passwd` 和 `/etc/shadow` 文件中创建本地用户了。它还可以通过将用户帐户合并到管理的中心，简化用户帐户管理。

您可以用 eDirectory 工具和技术来管理对网络上的 Linux 资源的访问。通过鉴定后，用户就有了 eDirectory 中指定的权限和特权。这些是和通常保存在本地帐户或重定向到其他鉴定方法（例如 NIS）相同的权限和特权。eDirectory 中保存的用户帐户信息使用户能够访问您网络上的文件和打印机资源。

用户可以用 `login`、`ftp`、`ssh`、`su`、`rsh`、`rlogin`、`xm` (KDE) 和 `gdm` (GNOME) 之类的访问方式登录到 SUSE Linux Enterprise Desktop 工作站。他们只需要输入 eDirectory 用户名和密码。他们无需记住完整环境，LUM 会搜索 eDirectory 中的正确用户。

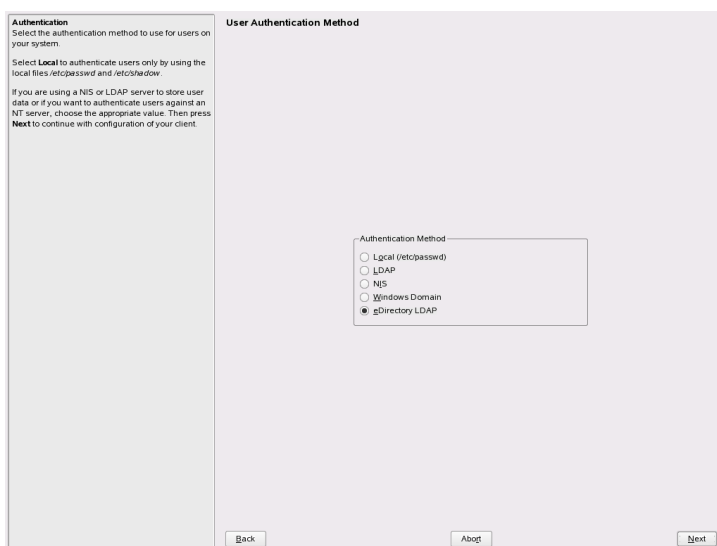
本节将指引您完成设置 SUSE Linux Enterprise Desktop 工作站使用 eDirectory 鉴定所需的步骤，包括为 eDirectory 鉴定配置 SUSE Linux Enterprise Desktop 工作站以及在 eDirectory 服务器上启用用户。关于 LUM 以及配置您的 eDirectory 8.6.x、8.7.x 或 8.8.x 服务器使用 LUM 的详细信息，请参见 *Novell Linux User Management Technology Guide* [<http://www.novell.com/documentation/oes/lumadgd/data/bookinfo.html>]。

34.1 设置工作站使用 eDirectory 鉴定

在用户使用他们的 eDirectory 用户名和密码登录之前，SUSE Linux Enterprise Desktop 工作站必须配置有 Linux User Management 组件。您可以在安装期间设置 eDirectory 鉴定，也可以在安装之后随时用 YaST 设置它。

要在安装 SUSE Linux Enterprise Desktop 期间安装并配置 LUM，请在用户鉴定方法窗口中选择 *eDirectory LDAP* 作为鉴定方法，然后完成以下 [步骤 2 \[600\]](#) 到 [步骤 10 \[603\]](#) 的步骤。如果尚未安装，会提示您安装 `yast2-linux-user-mgmt` 软件包。

图 34.1 用户鉴定方法

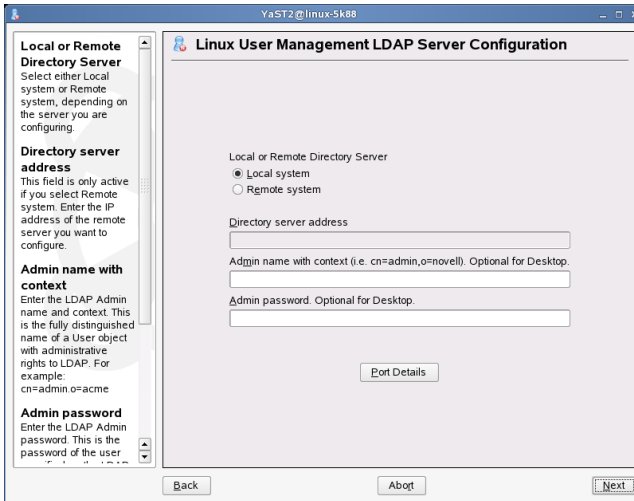


要在已在运行的工作stations上安装和配置 LUM：

- 1 启动 YaST，并选择 **安全和用户 > Linux 用户管理**。

如果在 YaST 中看不到 *Linux 用户管理* 项，请先选择 **软件 > 软件管理**，然后安装 `yast2-linux-user-mgmt` 包。

- 2 在 *Linux 用户管理 LDAP 服务器配置* 窗口中，指定 eDirectory 是在计算机本身（本地系统）上运行还是在网络上的其他计算机（远程系统）上运行。



3 如果 eDirectory 在远程系统上运行，请指定远程系统的 IP 地址。

4 或者，请提供 eDirectory admin 名称，环境和 Admin 密码。

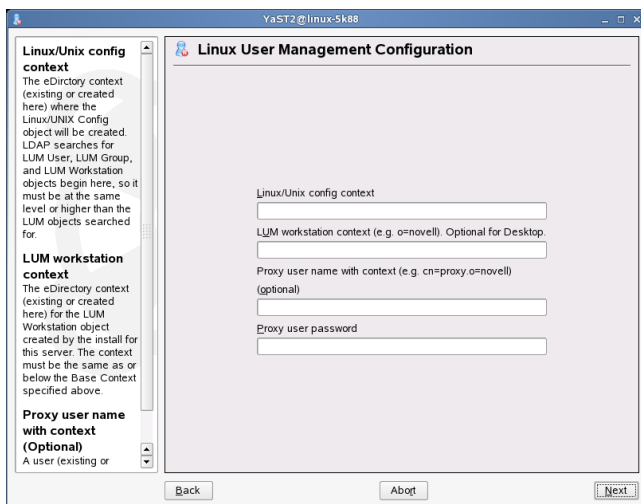
Admin 名称和环境必须以 LDAP 语法输入，在这种语法中用逗号而不是用句点（例如：cn=admin,o=novell）。

重要

如果您没有在 eDirectory 树下创建对象的权限，请将这些字段留空。请联系 eDirectory 管理员，向其提供客户机的主机名，并要求其用您的主机名创建一个 LUM 工作站对象。询问从哪里可以获取 LDAP 服务器的 CA 证书副本，并将此证书放置在 /var/nam 目录中。

CA 证书的名称与 /etc/nam.conf 文件中“preferred-server”项的名称匹配，且扩展名为 .der。您可以输入 `namconfig get preferred-server` 获取名称。例如，如果 `namconfig get preferred-server` 返回 `server.xyz.com`，则您的证书文件名是 `.server.xyz.com.der`。

5 单击下一步，然后指定 Linux/UNIX 配置对象的位置。



Linux/UNIX Config 对象保存一个网络上 Linux/UNIX 工作站对象的位置（环境）列表。它还控制创建用户和组对象时用于指派为用户 ID (UID) 和组 ID (GID) 的编号范围。配置 LUM 时将在 eDirectory 服务器上创建这个对象，它通常位于 eDirectory 树的上级树枝上（例如：o=novell）。对于该环境，请联系您的 eDirectory 管理员。

有关更多信息，请参见 *Novell Linux User Management Technology Guide* 中的 Understanding eDirectory Objects and Linux [<http://www.novell.com/documentation/oes/lumadgd/data/bx3sbv9.html>]。

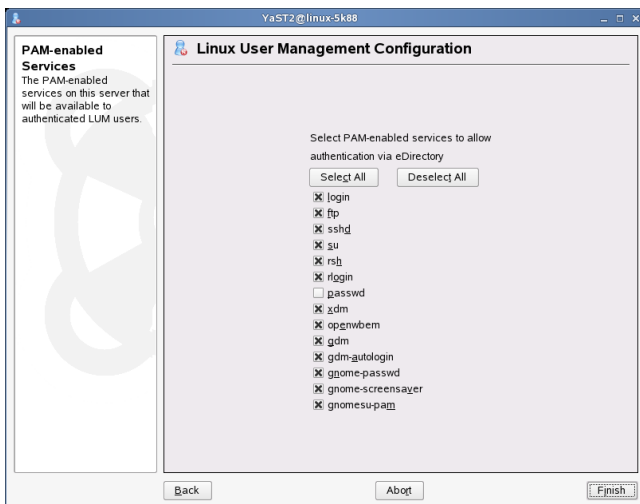
6 （可选）指定 LUM 工作站对象的位置。

LUM 工作站对象代表用户登录的实际计算机。如果您具有在 eDirectory 树下创建对象（即您可以指定 **步骤 4** [601] 中的 eDirectory Admin 名称、环境和密码）的权限，则该对象将作为工作站配置的一部分自动创建，并且通常位于 eDirectory 树下的组织 (O) 或组织单元 (OU) 容器中。您也可以通过单击 iManager 中的 *Linux User Management* > *创建 Linux 工作站对象* 来创建一个 LUM 工作站对象。

7 如果禁用了 LDAP 服务器的匿名绑定，请指定一个在 LDAP 树上有权限的代理用户名，环境和代理用户密码。

8 单击 下一步继续。

9 请选择用 eDirectory 进行鉴定的登录访问方式。



10 单击完成。

安装并配置 LUM 技术会设置 SUSE Linux Enterprise Desktop 工作站根据保存在 eDirectory 上的用户帐户信息来验证登录请求。用户必须用 iManager 创建 eDirectory 用户帐户，并为 LUM 扩展，同时他们的用户对象必须与他们将要登录的工作站相关联，这样用户才能登录。有关更多信息，请参见第 34.2 节“用 iManager 为 eDirectory 鉴定启用用户”[603]。

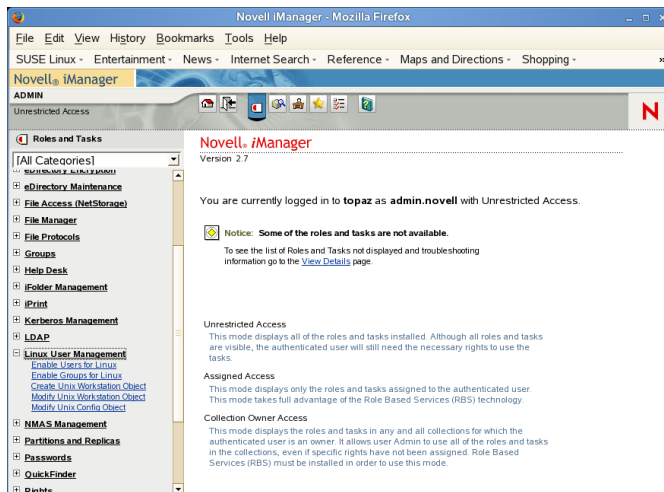
34.2 用 iManager 为 eDirectory 鉴定启用用户

如果 Linux User Management 组件安装正确，您可以用 eDirectory 和 iManager 指定哪些用户可访问网络上的 SUSE Linux Enterprise Desktop 计算机。iManager 是用于管理 eDirectory 对象的基于浏览器的实用程序。它运行于诸如 Mozilla*、Firefox*、Netscape* Navigator* 或者 Internet Explorer 之类的网络浏览器中。

当您在 iManager 中创建用户或组帐户时，会提示您用“LUM 启用”用户对象或组对象。对于 Linux 您也可以使用 iManager 来启用现有的用户对象或组对象。

每次您为 eDirectory 鉴定配置 SUSE Linux Enterprise Desktop 工作站时，启用 LUM 的 eDirectory 用户必须与工作站关联后才能从该工作站登录。

- 1 通过在网络浏览器的地址字段输入以下地址来起动 iManager: `http://target_server/nps/iManager`，其中 `target_server` 是 eDirectory 服务器的 IP 地址或域名。会提示您提供 Admin 用户的完整环境（例如：`admin.novell`）和密码。
- 2 确保您在角色和任务视图中，方式是单击顶部按钮栏上的角色和任务图标，然后在左侧导航面板中选择 *Linux 用户管理*。



- 3 单击为 *Linux* 启用用户，选择要启用的用户对象，然后单击下一步。

当扩展 eDirectory 用户对象暂挂 Linux 用户登录属性时，则是 *LUM* 已启用或者已为 *Linux* 启用。为 *Linux* 启用之后，用户只需使用 Telnet、SSH 或其他支持的方法（参见步骤 9 [603]）并输入用户名和密码即可方便地访问 Linux 计算机。将重定向访问请求以查找储存在 eDirectory 中的相应用户名和登录信息。

为 Linux 扩展之后，eDirectory 用户对象将保存和 Linux 相关的属性，例如用户 ID、主组 ID、主组名称、用户主目录的位置和首选 shell。

- 4 请将用户指派到组中，然后单击下一步。

该组及其对应的组 ID 将被指派为用户的主 GID。如果所选的用户帐户已具有主 GID，则将此组的 GID 作为次 GID 指派给用户。您可以选择以下的一种方式将用户指派到组中：

现有的 eDirectory 组

如果尚未为 Linux 启用该组对象，则将扩展其属性以包括 Linux 登录特性。您可以单击对象选择器图标浏览树以查找现有组。

现有的支持 Linux 的组

该选项允许您选择现有的 eDirectory 组对象。如果您使用对象选择器浏览，则只能查看并选择已用 Linux 登录特性扩展的那些组对象。

创建新的支持 Linux 的组

您可以用该选项创建新的 eDirectory 组对象。创建后，组对象进行扩展以包括 Linux 登录特性。

5 请选择组中用户有权访问的工作站，然后单击下一步。

6 单击完成应用更改，然后单击确定。

现在用户应该可以用他们的 eDirectory 用户登录凭证登录他们的 SUSE Linux Enterprise Desktop 工作站了。

34.3 关闭 LUM 和 eDirectory 鉴定

有时您需要关闭工作站接受从 eDirectory 登录的功能。您可以通过从工作站删除 LUM 软件永久地关闭此功能。您可以通过停止 `namcd` 守护程序临时禁用 eDirectory 鉴定。

要停止 `namcd`，请打开 shell 窗口，并输入 `rcnamcd stop`。

要打开 eDirectory 鉴定和 LUM，请打开 shell 窗口并输入 `rcnamcd start`。

LDAP - 目录服务

轻量级目录访问协议 (LDAP) 是一组设计用来访问和维护信息目录的协议。LDAP 可用于多种目的，如用户和组管理、系统配置管理或地址管理。本章简要介绍 `openldap` 的工作原理以及如何使用 YaST 管理 LDAP 数据。尽管实施多个 LDAP 协议，但本章着重介绍 OpenLDAP 实施。

在联网环境中保持重要信息组织有序并且访问便捷是非常重要的。这可以通过目录服务实现。目录服务就像常见的电话黄页，可以将信息组织得井然有序，便于快速搜索。

理想情况下，应该有一个中央服务器将数据组织到目录中，并使用特定协议将其分发给所有客户机。数据以特定的方式组织，以支持众多应用程序进行访问。这样，各种日历工具和电子邮件客户程序就不必保持自己的数据库，只需访问中央储存库即可。这种方式极大地减轻了管理这些信息的工作。利用 LDAP 之类的开放且标准化的协议，可以保证让尽量多的客户应用程序都能访问这些信息。

这里所说的目录实际上是指一种为快速有效的读取和搜索而优化的数据库。

- 为支持大量并行读取访问，需要限制写访问，只允许管理员执行次数较少的更新。要对常规数据库进行优化，使其能够在短时间内接受尽量多的数据。
- 由于只能在受限模式下执行写访问，所以可以采用目录服务来管理几乎不变的静态信息。常规数据库中的数据通常频繁变化（动态数据），而公司名录中的电话号码并不像会计数字（举例来说）那样经常变化。
- 管理静态数据时，极少更新现有数据集。而处理动态数据时，特别是在涉及像银行帐户或会计帐户这样的数据集时，数据的一致性举足轻重。如果

要将从某处减去的数目加到另一个位置，必须在一个事务中同时执行这两个运算，以确保数据存量保持平衡。数据库支持处理这类事务，而目录却不。短期内数据之间的不一致在目录中是完全可以接受的。

LDAP 这类目录服务并不是为支持复杂的更新或查询机制而设计的。访问此服务的所有应用程序都应能够便捷地获取访问权。

35.1 对比 LDAP 和 NIS

Unix 系统管理员以往使用 NIS 服务在网络内进行名称解析和数据分发。/etc 中的文件所包含的配置数据以及目录 group、hosts、mail、netgroup、networks、passwd、printcap、protocols、rpc 和 services 都通过客户程序在网络中分发。这些文件很容易维护，因为它们都是简单的文本文件。但随着数据量的不断增大，处理起来就会因为缺乏组织结构而愈发困难。NIS 仅适用于 Unix 平台。就是说它不适合在异构网络中充当集中式数据管理工具。

有别于 NIS，LDAP 服务不仅仅适用于单纯的 Unix 网络。Windows 2000 之后的服务器都支持 LDAP 作为目录服务。上述应用程序任务在非 Unix 系统中同样受支持。

LDAP 原理适用于所有需要集中管理的数据结构。以下是一些应用示例：

- 用于替代 NIS 服务
- 邮件路由选择（postfix、sendmail）
- 邮件客户机（如 Mozilla、Evolution 和 Outlook）的通讯录
- 为 BIND9 名称服务器管理区域说明
- 异构网络中使用 Samba 进行用户鉴定

可以扩展此列表，因为 LDAP 是可扩展的，这是 NIS 所不能及的。由于更便于搜索数据，明确定义的数据层次结构简化了对大量数据的管理。

35.2 LDAP 目录树的结构

要深入了解 LDAP 服务器工作方式和数据存储方式的背景知识，关键在于了解数据在服务器上的组织方式，以及该结构如何可以使 LDAP 能够提供对所需数据的快速访问。要成功进行 LDAP 设置，还需要熟悉一些基本 LDAP 术语。本节介绍 LDAP 目录树的基本布局，并提供了在 LDAP 环境中使用的基本术语。如果您已经了解一些 LDAP 背景知识，只是想了解如何在 SUSE Linux Enterprise 中设置 LDAP 环境，可跳过这个介绍部分。

LDAP 目录具有树形结构。目录中的所有项（称为对象）在此层次结构中都有确定的位置。此层次结构称为*目录信息树 (DIT)*。指向所需项的完整路径（可以明确标识该项）被称为*判别名*或 DN。沿路径指向此项的单个节点称为*相对判别名*或 RDN。通常可以向以下两种可能类型之一指派对象：

树枝

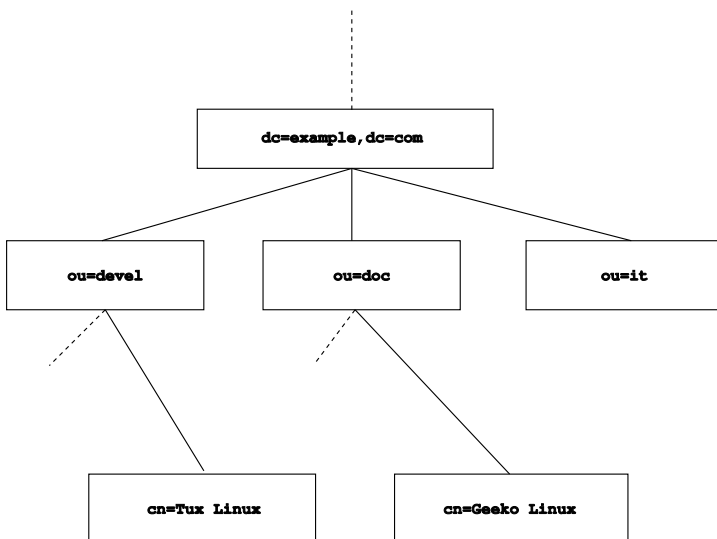
这些对象本身可以包含其他对象。这些对象类包括 root（目录树的根元素，实际并不存在）、c（国家/地区）、ou（组织单元）和 dc（域组件）。此模型类似文件系统中的目录（文件夹）。

叶

这些对象位于分支的末梢，没有任何从属对象。person、InetOrgPerson 或 groupofNames 都属于此类对象。

目录层次的顶端有一个根元素 root。其中可包含 c（国家/地区）、dc（域组件）或 o（组织）作为从属元素。LDAP 目录树中的关系在下例中尤为明显，如 [图 35.1 “LDAP 目录的结构”](#) [610] 所示。

图 35.1 LDAP 目录的结构



完整的图是一个虚构的目录信息树。其中描述了三个层次上的项。每一项都对应图中的一个框。在本例中，虚构的雇员 *Geeko Linux* 的完整有效判别名为 `cn=Geeko Linux, ou=doc, dc=example, dc=com`。该名称是通过将 RDN `cn=Geeko linux` 添加到前一项的 DN `ou=doc, dc=example, dc=com` 而构成的。

应该储存 DIT 的对象类型是按照模式全局确定的。对象类型由对象类决定。对象类决定必须或可以给相关对象指派哪些特性。因此，方案中必须包含所需应用方案中使用的所有对象类和特性的定义。已存在一些常用方案（请参见 RFC 2252 和 2256）。不过，可以创建自定义方案或使用多个互补的方案（如果 LDAP 服务器的运行环境要求这样做）。

表 35.1 “常用对象类和特性” [611] 提供了示例所用的 `core.schema` 和 `inetorgperson.schema` 中的对象类的简要概览（包括必需特性和有效特性值）。

表 35.1 常用对象类和特性

对象类	含义	示例项	必需特性
dcObject	<i>domainComponent</i> (域的名称 组件)	示例	dc
organizationalUnit	<i>organizationalUnit</i> (组织单 元)	doc	ou
inetOrgPerson	<i>inetOrgPerson</i> (内部网或因特 网中与个人有关的数据)	Geeko Linux	sn 和 cn

例 35.1 “引自 [schema.core](#)” [611]引自一个方案指令，并附有解释（为便于解释对行进行了编号）。

例 35.1 引自 *schema.core*

```
#1 attributetype (2.5.4.11 NAME ( 'ou' 'organizationalUnitName')
#2         DESC 'RFC2256: organizational unit this object belongs to'
#3         SUP name )
...
#4 objectclass ( 2.5.6.5 NAME 'organizationalUnit'
#5         DESC 'RFC2256: an organizational unit'
#6         SUP top STRUCTURAL
#7         MUST ou
#8 MAY (userPassword $ searchGuide $ seeAlso $ businessCategory
        $ x121Address $ registeredAddress $ destinationIndicator
        $ preferredDeliveryMethod $ telexNumber
        $ teletexTerminalIdentifier $ telephoneNumber
        $ internationaliSDNNumber $ facsimileTelephoneNumber
        $ street $ postOfficeBox $ postalCode $ postalAddress
        $ physicalDeliveryOfficeName
        $ st $ l $ description) )
...
```

特性类型 *organizationalUnitName* 和相应的对象类 *organizationalUnit* 在此仅作为示例。第 1 行说明特性的名称、其唯一 **OID**（对象标识符）（数字），及特性缩写方式。

第 2 行通过 **DESC** 对该特性进行了简要说明。在此还提到了定义所基于的相应 **RFC**。第 3 行中的 **SUP** 表明此特性所属的上级特性类型。

从第 4 行开始是对象类 `organizationalUnit` 的定义；与特性定义类似，该定义也包含对象类的 OID 和名称。第 5 行对该对象类进行了简要说明。第 6 行通过项 `SUP top` 表明此对象类不从属于其他对象类。第 7 行以 `MUST` 开头，列出必须与类型为 `organizationalUnit` 的对象一同使用的所有特性类型。第 8 行以 `MAY` 开头，列出可以与此对象类一同使用的所有特性类型。

有关方案用法的详尽介绍，请参见文档 `OpenLDAP`。安装 `OpenLDAP` 之后，可以在 `/usr/share/doc/packages/openldap2/admin-guide/index.html` 中找到该文档。

35.3 使用 YaST 配置 LDAP 客户机

YaST 包含一个用于设置基于 LDAP 的用户管理的模块。如果安装期间未启用此功能，请通过选择 **网络服务 > LDAP 客户机** 来启动模块。YaST 会自动启用 LDAP 所需的任何 PAM 和 NSS 相关更改并安装所需文件。

35.3.1 标准过程

进程在客户机的后台运行的背景知识可帮助您理解 YaST LDAP 客户机模块是如何运行的。如果为进行网络鉴定激活了 LDAP 或是调用了 YaST 模块，系统会安装软件包 `pam_ldap` 和 `nss_ldap` 并调整两个相应的配置文件。`pam_ldap` 是负责在登录进程和 LDAP 目录（作为鉴定数据源）之间进行协商的 PAM 模块。将安装专用模块 `pam_ldap.so` 并调整 PAM 配置（请参见例 35.2 “为适应 LDAP 而调整的 `pam_unix2.conf`” [612]）。

例 35.2 为适应 LDAP 而调整的 `pam_unix2.conf`

```
auth:      use_ldap
account:   use_ldap
password:  use_ldap
session:   none
```

手动配置其他服务使用 LDAP 时，请将该服务对应的 PAM 配置文件中的 PAM LDAP 模块加入 `/etc/pam.d`。可以在 `/usr/share/doc/packages/pam_ldap/pam.d/` 中找到为适应各种服务而调整过的配置文件。将相应文件复制到 `/etc/pam.d` 中。

使用 `nss_ldap` 可以对通过 `nsswitch` 机制执行的 `glibc` 名称解析进行调整，使其适应 LDAP 的部署。安装此包时将在 `/etc` 中创建新的调整过的文件

nsswitch.conf。有关nsswitch.conf工作的更多信息，请参见第 30.6.1 节“配置文件”[573]。nsswitch.conf 中必须存在以下行才能进行用户管理及 LDAP 鉴定。请参见例 35.3 “nsswitch.conf 中的调整”[613]。

例 35.3 nsswitch.conf 中的调整

```
passwd: compat
group: compat

passwd_compat: ldap
group_compat: ldap
```

这些行指示 glibc 的解析程序库首先评估 /etc 中的相应文件，而后还要访问作为鉴定和用户数据来源的 LDAP 服务器。测试这种机制，例如通过使用命令 getent passwd 读取用户数据库中的内容。返回的结果集不仅应该包含您系统中本地用户的调查结果，还应包含所有储存在 LDAP 服务器上的用户的调查结果。

要防止通过 LDAP 管理的普通用户使用 ssh 或 login 登录该服务器，文件 /etc/passwd 和 /etc/group 都需要添加另外一行。这一行在 /etc/passwd 中为 +:::/:sbin/nologin，在 /etc/group 中为 +:::。

35.3.2 配置 LDAP 客户端

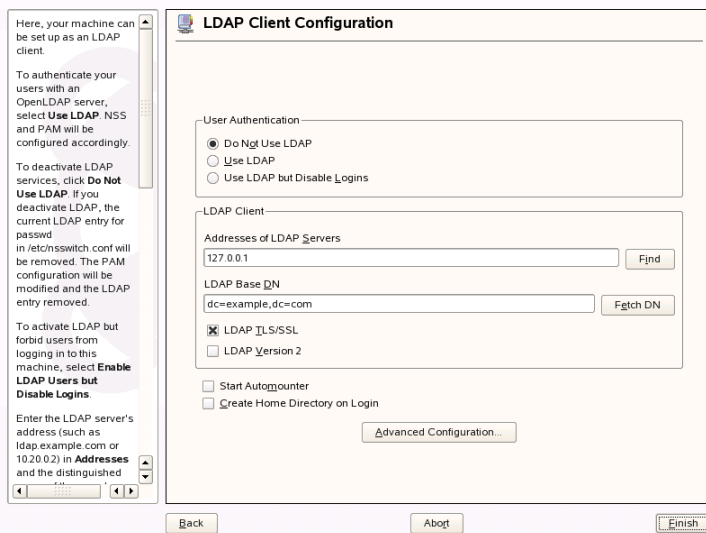
在 YaST 初始调整了 nss_ldap、pam_ldap、/etc/passwd 和 /etc/group 之后，您只需将客户机连接到服务器并使 YaST 通过 LDAP 来管理用户。中描述了基本设置。“基本配置”一节 [613]

使用 YaST LDAP 客户端来进一步配置 YaST 组 and 用户配置模块。这包括为新用户和组执行默认设置和为用户或组指派的属性数和性质。LDAP 用户管理允许您为用户和组指派比传统用户或组管理解决方案更多的不同属性。中对此进行了描述。“配置 YaST 组和用户管理模块”一节 [616]

基本配置

如果您选择 LDAP 用户管理或当您在已安装系统的 YaST 控制中心中选择网络服务 > LDAP 客户端时，基本 LDAP 客户端配置对话框（图 35.2 “YaST：LDAP 客户程序的配置”[614]）在安装期间会打开。

图 35.2 YaST: LDAP 客户程序的配置

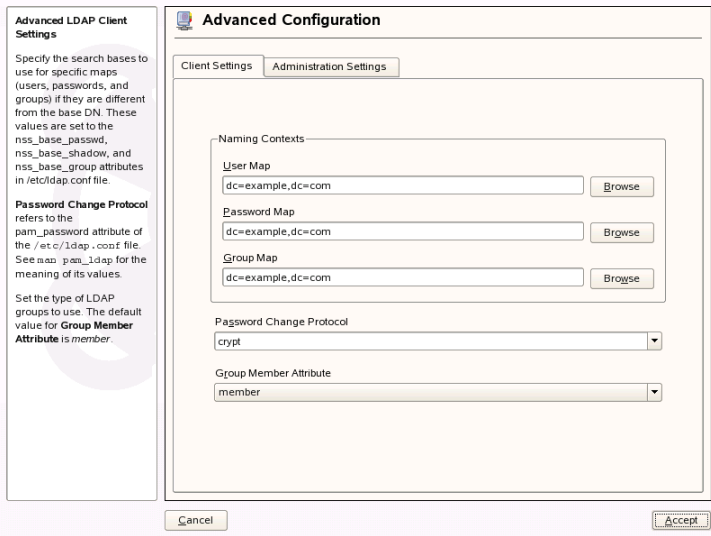


要针对 OpenLDAP 服务器来鉴定机器的用户并通过 OpenLDAP 来启用用户管理，请按如下操作：

- 1 单击使用 *LDAP* 以启用 *LDAP*。如果您希望使用 *LDAP* 来进行鉴定但不希望其他用户登录到此客户机，则选择使用 *LDAP* 但禁用登录。
- 2 输入要使用的 *LDAP* 服务器的 IP 地址。
- 3 输入 *LDAP* 基本 *DN* 以在 *LDAP* 服务器上选择搜索基础。要自动检索基本 *DN*，请单击获取 *DN*。然后 YaST 会在上面指定的服务器地址检查所有 *LDAP* 数据库。从 YaST 给出的搜索结果中选择适当的基本 *DN*。
- 4 如果需要与服务器进行 *TLS* 或 *SSL* 受保护通信，则选择 *LDAP TLS/SSL*。
- 5 如果 *LDAP* 服务器仍然使用 *LDAPv2*，则通过选择 *LDAP* 版本 2 来显式启用此协议版本。
- 6 选择启动 *Automounter* 来在客户机上装入远程目录，如远程管理的 */home*。
- 7 选择登录时创建用户主目录可在用户第一次登录时自动创建用户主目录。

8 单击结束来应用设置。

图 35.3 YaST：高级配置



要作为管理员修改服务器上的数据，请单击高级配置。以下对话框显示在两个选项卡中。请参见图 35.3 “YaST：高级配置” [615]。

- 1 在客户机设置选项卡中，根据需要来调整以下设置：
 - 1a 如果用户、密码和组的搜索基础与指定 *LDAP* 基本 *DN* 的全局搜索基础不同，则在用户映射、密码映射和组映射中输入这些不同的命名上下文。
 - 1b 指定密码更改协议。无论何时更改密码，使用的标准方法都为 *crypt*，它表示使用 *crypt* 生成的密码哈希值。有关此选项和其他选项的详细信息，请参见 *pam_ldap* 手册页。
 - 1c 指定与组成员属性一起使用的 *LDAP* 组。默认值为 *member*。
- 2 在管理设置中，调整以下设置：
 - 2a 通过配置基本 *DN* 来设置储存用户管理数据的基础。

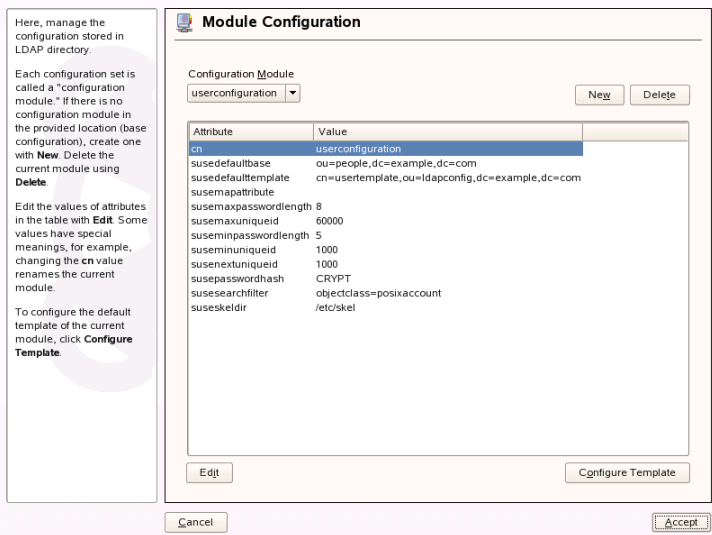
- 2b** 为管理员 *DN* 输入合适的值。此 *DN* 必须与 `/etc/openldap/slapd.conf` 中指定的 `rootdn` 值相同以使此特定用户能够处理 LDAP 服务器上储存的数据。输入完整的 *DN*（例如 `cn=Administrator、dc=example` 和 `dc=com`）或激活追加基本 *DN*，使您输入 `cn=Administrator` 时能够自动添加基本 *DN*。
- 2c** 单击 *创建默认配置对象* 以在服务器上创建基本配置对象以通过 LDAP 启用用户管理。
- 2d** 如果您的客户机在网络中应作为用户主目录的文件服务器，请选中 *此机器上的用户主目录*。
- 2e** 使用 *密码策略* 部分选择、添加、删除或修改要使用的密码策略设置。用 YaST 配置密码策略是 LDAP 服务器安装的一部分。
- 2f** 单击 *接受* 以关闭 *高级配置*，然后单击 *结束* 以应用设置。

使用 *配置用户管理* 设置编辑 LDAP 服务器上的项。随后将根据服务器上储存的 ACL 和 ACI 授予对服务器上的配置模块的访问权。请遵循“[配置 YaST 组 and 用户管理模块](#)”一节 [616] 中说明的过程。

配置 YaST 组和用户管理模块

使用 YaST LDAP 客户程序可以调整 YaST 模块使其适应用户和组管理，并按需扩展这些模块。使用个别属性的默认值来定义模板以简化数据注册。在此创建的预设值将作为 LDAP 对象储存在 LDAP 目录中。用户数据的注册仍使用常用的用户和组管理的 YaST 模块来完成。注册的数据作为 LDAP 对象储存在服务器上。

图 35.4 YaST：模块配置



模块配置对话框 (图 35.4 “YaST：模块配置” [617]) 允许创建新模块、选择和修改现有配置模块并设计和修改此类模块的模板。

要创建新的配置模块，请执行以下操作：

- 1 单击 **新建** 并选择要创建的模块的类型。对于用户配置模块，选择 `suseuserconfiguration`，对于组配置，选择 `susegroupconfiguration`。
- 2 为新模板选择名称。内容视图随即显示一个表，列出此模块允许使用的所有特性及其指派值。除所有已设置的特性之外，该列表还包含当前方案允许的但当前未使用的所有其他特性。
- 3 接受预设值或通过选择相关属性来调整要在组和用户配置中使用的默认值（按 **编辑**，然后输入新值）。只需通过更改模块的 `cn` 属性来重命名模块。单击 **删除** 将删除当前所选模块。
- 4 在单击 **接受** 之后，新的模块将添加到选择菜单中。

用于组和用户管理的 YaST 模块会内嵌带有合理标准值的模板。要编辑与配置模块关联的模板，请如下执行操作：

- 1 在模块配置对话框中，单击配置模板。
- 2 根据您的需要来确定指派给此模板的常规属性的值或将某些值保留为空。LDAP 服务器将删除空特性值。
- 3 修改、删除或添加新对象（LDAP 树中的用户或组配置对象）的新默认值。

图 35.5 YaST: 对象模板的配置

Here, configure the template used for creating new objects (like users or groups).

Edit the template attribute values with **Edit**. Changing the **cn** value renames the template.

The second table contains a list of **default values**, used for new objects. Modify the list by adding new values and editing or removing current ones.

Object Template Configuration

Attribute	Value
cn	usertemplate
susenamingattribute	uid
suseplugin	UsersPluginLDAPAll
susesecondarygroup	

Edit

Default Values for New Objects

Attribute of Object	Default Value
homedirectory	/home/%uid
loginshell	/bin/bash

AddEditDelete

Cancel

Accept

通过将模块的 `susedefaulttemplate` 特性值设置为调整过的模板的 DN，可以将模板与模块连接起来。

提示

通过用变量代替绝对值的方法，可以从其他特性为某个特性创建默认值。例如，创建新用户时，将从 `sn` 和 `givenName` 的特性值自动创建 `cn=%sn %givenName`。

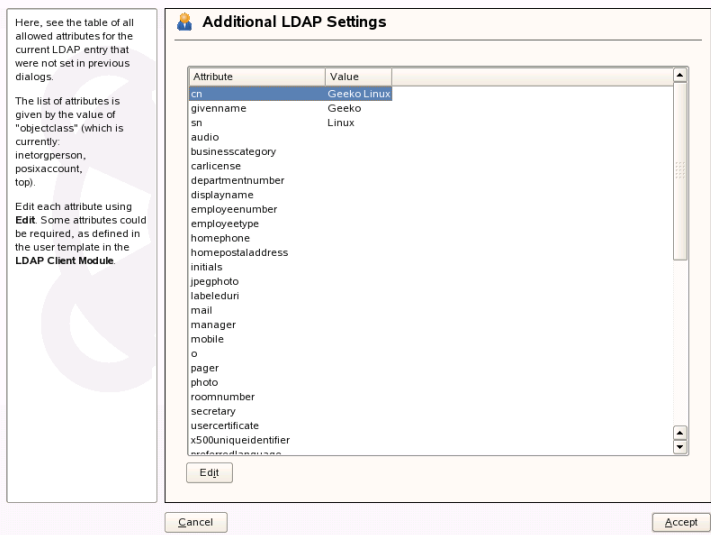
在所有模块和模板经过正确配置能够运行后，可以使用 YaST 按通常方式注册新组和用户。

35.4 在 YaST 中配置 LDAP 用户和组

用户和组数据的实际配置过程与不使用 LDAP 时的过程相差无几。下面简要说明了用户管理过程。管理组的过程与此相似。

- 1 通过安全性和用户 > 用户管理访问 YaST 用户管理。
- 2 使用设置过滤器来限制用户查看 LDAP 用户并输入根 DN 的密码。
- 3 单击添加并输入新用户的配置。将打开一个有四个选项卡的对话框：
 - 3a 在用户数据选项卡中指定用户名、登录和密码。
 - 3b 选中详细信息选项卡以输入新用户的组成员、登录 shell 和主目录。如果需要，将默认值更改为符合您需要的值。可以使用“配置 YaST 组和用户管理模块”一节 [616] 中描述的过程来定义默认值以及这些密码设置。
 - 3c 修改或接受默认密码设置。
 - 3d 进入插件选项卡，选择 LDAP 插件，然后单击启动以配置指派给新用户的其他 LDAP 属性（请参见图 35.6 “YaST：其他 LDAP 设置” [620]）。
- 4 单击接受以应用这些设置并关闭用户配置。

图 35.6 YaST: 其他 LDAP 设置



最初的用户管理输入表单提供了 *LDAP* 选项。通过此选项可以对一组现有用户应用 LDAP 搜索过滤器，或者通过选择 *LDAP 用户和组配置* 转至用于配置 LDAP 用户和组的模块。

35.5 浏览 LDAP 目录树

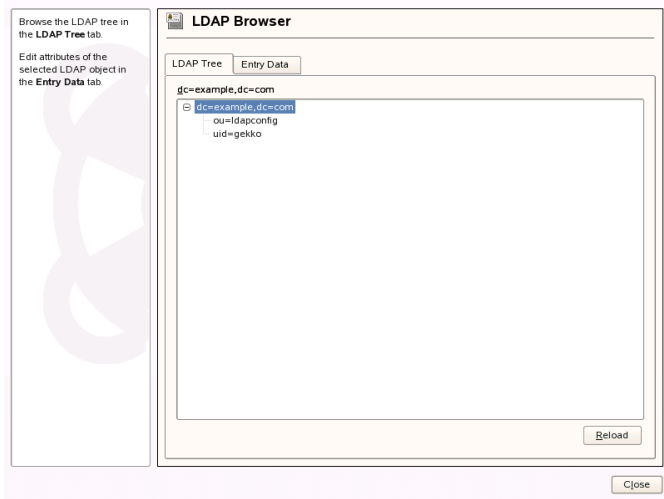
要方便地浏览 LDAP 目录树及其所有条目，请使用 YaST LDAP 浏览器：

- 1 作为 root 登录。
- 2 启动 YaST > 网络服务 > LDAP 浏览器。
- 3 输入 LDAP 服务器地址、AdministratorDN 和该服务器的 RootDN 密码（如果您需要这两者才能读写服务器上储存的数据）。

或者选择匿名访问，不提供密码即可对目录进行读访问。

LDAP 树选项卡会显示您的计算机所连接的 LDAP 目录的内容。单击项目可展开其子项。

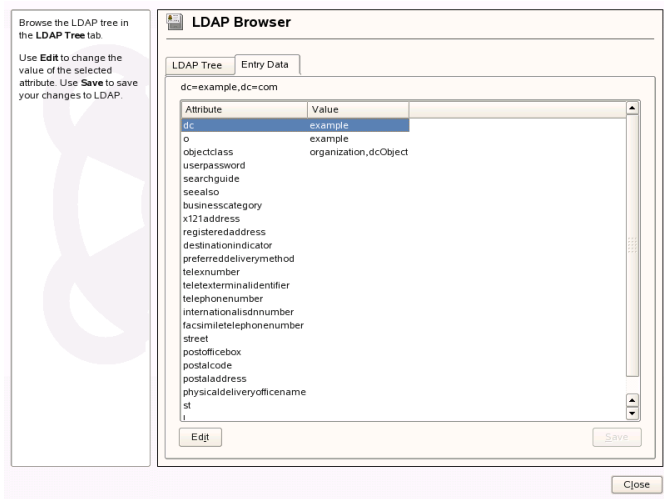
图 35.7 浏览 LDAP 目录树



4 要查看任何条目的细节，请在LDAP树视图选择它，打开条目数据选项卡。

将显示所有和该条目相关的特性和值。

图 35.8 浏览条目数据



- 5 要更改这些特性的值，请选择该特性，单击 *编辑*，输入新值，单击 *保存*，在看到提示时提供 RootDN 密码。
- 6 用 *关闭* 退出 LDAP 浏览器。

35.6 有关详细信息

本章特意排除了一些较为复杂的主题，如 SASL 配置，或如何通过建立复制 LDAP 服务器在多台从属服务器上分配工作量。有关这两个主题的详细信息，请参见 *OpenLDAP 2.2 Administrator's Guide*。

OpenLDAP 项目的万维网站点为初级和高级 LDAP 用户提供了丰富的文档：

OpenLDAP Faq-O-Matic

涉及 OpenLDAP 的安装、配置和使用的非常详尽的问答集锦。请参见 <http://www.openldap.org/faq/data/cache/1.html>。

快速入门指南》

为首次安装 LDAP 服务器提供了简明的分步说明。请参见 <http://www.openldap.org/doc/admin22/quickstart.html> 或已安装系统中的 `/usr/share/doc/packages/openldap2/admin-guide/quickstart.html`。

OpenLDAP 2.2 管理员指南

对 LDAP 配置的所有重要事项的详细介绍，包括访问控制和加密。请参见 <http://www.openldap.org/doc/admin22/> 或已安装系统上的 `/usr/share/doc/packages/openldap2/admin-guide/index.html`。

Understanding LDAP（了解 LDAP）

关于 LDAP 基本原理的详尽的一般性介绍：<http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf>。

LDAP 印刷文献资料：

- *LDAP System Administration* Gerald Carter 著 (ISBN 1-56592-491-6)
- *Understanding and Deploying LDAP Directory Services* Howes、Smith 和 Good 著 (ISBN 0-672-32316-8)

关于 LDAP 这一主题最后还可以参见相应的 RFC（请求注释）2251 到 2256。

Samba

使用 Samba，可以将 Unix 计算机配置为 DOS、Windows 和 OS/2 计算机的文件和打印服务器。Samba 已经发展成为一个功能完备且相当复杂的产品。使用 YaST、SWAT（万维网接口）或配置文件来配置 Samba。

36.1 术语

以下是 Samba 文档和 YaST 模块中使用的一些术语。

SMB 协议

Samba 使用基于 NetBIOS 服务的 SMB（服务器讯息块）协议。迫于 IBM 的压力，Microsoft 发布了该协议，这样其他软件制造商能够与 Microsoft 域网络建立连接。使用 Samba 时，SMB 协议在 TCP/IP 协议之上工作，所以必须在所有客户机上安装 TCP/IP 协议。

CIFS 协议

（常用因特网文件系统）协议是 Samba 支持的另一种协议。CIFS 定义网络中使用的标准远程文件系统访问协议，使用户组能够一起工作并在网络中共享文档。

NetBIOS

NetBIOS 是为计算机之间进行通讯而设计的软件接口 (API)。这里提供了一种名称服务。它使连接到网络的计算机能够为自己保留名称。之后便可以根据名称对这些计算机进行寻址。没有任何中心进程来检查这些名称。网络上的任何机器均可以保留所需数量的名称，前提是这些名称均未使用。现在可以为不同的网络体系结构实施 NetBIOS 接口。NetBEUI 是与网络硬

件结合相对密切的一种实施，但它常被称为 NetBIOS。使用 NetBIOS 实施的网络协议包括 Novell 的 IPX（通过 TCP/IP 的 NetBIOS）和 TCP/IP。

通过 TCP/IP 发送的 NetBIOS 名称与 `/etc/hosts` 中使用的名称或 DNS 定义的名称没有相同之处。NetBIOS 使用它自己的、完全独立的命名约定。但为了方便管理，仍建议您使用与 DNS 主机名对应的名称。Samba 默认采用这种方式。

Samba 服务器

Samba 服务器是一种能够向客户机提供 SMB/CIFS 服务和 NetBIOS 基于 IP 命名服务的服务器。对 Linux，Samba 服务器有两个守护程序：用于 SMB/CIFS 服务的 `smnd` 和用于命名服务的 `nmbd`。

Samba 客户机

Samba 客户机是一种能够通过 SMB 协议从 Samba 服务器使用 Samba 服务的系统。所有常见操作系统（Mac OS X、Windows 和 OS/2 等）都支持 SMB 协议。必须在所有计算机上安装 TCP/IP 协议。Samba 为多种不同的 UNIX 系统提供客户机。对于 Linux，有一个用于 SMB 的内核模块，它允许在 Linux 系统级别上集成 SMB 资源。不需要对 Samba 客户机运行任何守护程序。

共享

SMB 服务器通过共享为其客户机提供硬件空间。共享就是服务器上的打印机和目录及其子目录。可以通过名称来导出并访问共享。可以将共享名称设置为任何名称 — 它不一定是导出目录的名称。也可以为打印机指派一个名称。客户机可以根据打印机的名称来访问打印机。

36.2 启动和停止 Samba

引导时可以自动启动或停止 Samba 服务器，或者手动执行这两个操作。启动和停止策略是第 36.3.1 节“使用 YaST 配置 Samba 服务器”[627]中所述的 YaST Samba 服务器配置的一部分。

要使用 YaST 停止或开始运行 Samba 服务，请使用系统 > 系统服务（运行级别）。从命令行，使用 `rcsmb stop` 和 `rcnmb stop` 停止 Samba 所需的服务，然后使用 `rcnmb start` 和 `rcsmb start` 启动它们。

36.3 配置 Samba 服务器

SUSE Linux Enterprise® 中的 Samba 服务器可通过两种不同方式配置：用 YaST 或手动方式。手动配置可提供更详细的信息，但没有 YaST GUI 方便。

36.3.1 使用 YaST 配置 Samba 服务器

要配置 Samba 服务器，请启动 YaST 并选择*网络服务 > Samba 服务器*。首次启动模块时，*Samba 服务器安装*对话框将打开以提示您选择几个基本选项来管理服务器，然后在配置结束时提示您输入 Samba 根用户密码。为了在稍后启动，*Samba 服务器配置*对话框将显示。

Samba 服务器安装对话框由两步组成：

工作组名或域名

在*工作组名或域名*中选择一个现有名称或输入一个新的名称，然后单击下一步。

Samba 服务器类型

在下一步中，指定服务器是否应该充当 PDC，然后单击下一步。

稍后，可以在 *Samba 服务器配置*对话框中使用标识选项卡来更改 *Samba 服务器* 安装的所有设置。

使用 YaST 的高级 Samba 配置

首次启动 Samba 服务器模块时，*Samba 服务器配置*对话框紧接着*Samba 服务器安装*对话框显示。使用它调整您的 Samba 服务器配置。

编辑配置后，单击*完成*关闭配置。

启动服务器

在*启动*选项卡中，配置 Samba 服务器的启动。若想在每次系统引导时启动服务，请选择*引导时*。要激活手动启动，请选择*手动*。有关启动 Samba 服务器的更多信息，请参见第 36.2 节“*启动和停止 Samba*”[626]。

在此选项卡中，还可以打开防火墙中的端口。为此应选择*打开防火墙中的端口*。如果有多个网络接口，则请通过单击*防火墙细节*、选择接口并单击*确定*来为 Samba 服务选择网络接口。

共享

在共享选项卡中，确定要激活的 Samba 共享。存在一些预定义的共享，例如主页和打印机。使用*切换状态*可在*活动*和*不活动*之间进行切换。单击*添加*可添加新共享，单击*删除*可删除选中共享。

身份

在标识选项卡中，确定与主机关联的域（*基本设置*）以及是否在网络中使用备用主机名（*NetBIOS 主机名*）。要设置专家全局设置或设置用户鉴定，请单击*高级设置*。

36.3.2 使用 SWAT 管理万维网

Samba 服务器管理的备用工具是 SWAT（Samba 万维网管理工具）。它提供了一个简单的万维网接口，可用来配置 Samba 服务器。要使用 SWAT，请在万维网浏览器中打开 <http://localhost:901> 并以 root 用户身份登录。如果没有特殊的 Samba 根帐户，则请使用系统根帐户。

注意: 激活 SWAT

Samba 服务器安装完成后，SWAT 将不激活。要激活它，请在 YaST 中打开*网络服务 > 网络服务 (xinetd)*、启用网络服务配置、从表中选择 *swat*，然后单击*切换状态*（“开”或“关”）。

36.3.3 手动配置服务器

如果想将 Samba 用作服务器，请安装 samba。Samba 的主要配置文件是 `/etc/samba/smb.conf`。可以将此文件分为两个逻辑部分。`[global]` 部分包含中央和全局设置。`[share]` 部分包含各个文件和打印机共享。通过这种方式，可以在 `[global]` 部分中有区别地或全局地设置有关共享的详细设置，这样可以提高配置文件的结构透明性。

global 部分

需要对 [global] 部分的以下参数进行调整以满足网络设置的要求，以便其他计算机能够在 Windows 环境中通过 SMB 访问 Samba 服务器。

workgroup = TUX-NET

此行将 Samba 服务器指派到工作组。将 TUX-NET 替换为您的网络环境的适当工作组。您的 Samba 服务器将出现在其 DNS 名称下，除非此名称已被指派给网络中的任何其他计算机。如果 DNS 名称不可用，请使用 `netbiosname=MYNAME` 设置服务器名称。有关此参数的详细信息，请参见 `mansmb.conf`。

os level = 2

此参数确定您的 Samba 服务器是否会尝试成为其工作组的 LMB（本地主浏览器）。为了避免现有 Windows 网络受到配置错误的 Samba 服务器的任何影响，应选择非常低的值。有关这一重要主题的详细信息，请参见文件 `BROWSING.txt` 和 `BROWSING-Config.txt`，它们位于包文档的 `textdocs` 子目录下。

如果网络中没有任何其他 SMB 服务器（如 Windows NT 或 2000 服务器），并且您希望 Samba 服务器保留一份本地环境中存在的所有系统的列表，请将 `os level` 设置为一个较高的值（例如 65）。然后便可以选择您的 Samba 服务器作为本地网络的 LMB。

在更改此设置时，应认真考虑这样做对现有 Windows 网络环境的影响。应该首先在一个孤立网络中或一天中的非重要时间测试这些更改。

wins support 和 wins server

为了将您的 Samba 服务器集成到具有活动 WINS 服务器的现有 Windows 网络中，应启用 `wins server` 选项并将其值设置为 WINS 服务器的 IP 地址。

如果将您的 Windows 计算机连接到单独的子网，同时又希望它们互相通讯，则需要设置一个 WINS 服务器。要将 Samba 服务器转变为这样的 WINS 服务器，请设置选项 `wins support = Yes`。确保网络中只有一个 Samba 服务器启用了此设置。切勿在您的 `smb.conf` 文件中同时启用选项 `wins server` 和 `wins support`。

共享

以下示例说明了如何使 CD-ROM 驱动器和用户目录 (homes) 对 SMB 客户机可用。

[cdrom]

为了避免意外地使 CD-ROM 驱动器变得可用，应使用注释标记（在本例中是分号）取消这些行。去除第一列中的分号，以便与 Samba 共享 CD-ROM 驱动器。

例 36.1 CD-ROM 共享

```
;[cdrom]
;      comment = Linux CD-ROM
;      path = /media/cdrom
;      locking = No
```

[cdrom] 和 comment

[cdrom] 项是网络上的所有 SMB 客户机均可看到的共享的名称。可以添加一个附加 comment 来进一步说明此共享。

```
path = /media/cdrom
path 导出目录 /media/cdrom。
```

通过严格限制的默认配置，可使这种共享仅对此系统上存在的用户可用。如果应使此共享对所有用户可用，请向配置中添加一行 `guest ok = yes`。此设置为网络上的所有用户提供读权限。建议您认真处理此参数。在 [global] 部分使用此参数时更应如此。

[homes]

[home] 共享在这里特别重要。如果用户具有 Linux 文件服务器的有效帐户和密码以及自己的主目录，则该用户可以连接到此共享。

例 36.2 主共享

```
[homes]
comment = Home Directories
valid users = %S
browseable = No
read only = No
create mask = 0640
directory mask = 0750
```

[homes]

只要没有其他共享使用连接到 SMB 服务器的用户的共享名称，就会使用 [homes] 共享指令动态生成一个共享。所生成的共享的名称就是用户名。

`valid users = %S`

一旦成功建立连接，就会使用共享的具体名称替换 %S。对于 [homes] 共享，用户名始终是 %S。这样就可以将对用户的共享的访问权限严格限制在此用户。

`browseable = No`

此设置使共享在网络环境中不可见。

`read only = No`

默认情况下，Samba 通过 `read only = Yes` 参数来禁止对任何已导出共享的写访问。要使共享可写，请设置值 `read only = No`，它与 `writable = Yes` 是等效的。

`create mask = 0640`

那些不是基于 MS Windows NT 的系统不能理解 UNIX 权限的概念，所以它们在创建文件时不能指派权限。参数 `create mask` 定义了为新创建文件指派的访问权限。这仅适用于可写共享。事实上，此设置意味着拥有者具有读写权限，且拥有者的主组的成员具有读权限。`valid users = %S` 禁止读访问，即使该组具有读权限。要使该组能够进行读或写访问，应取消 `valid users = %S` 一行。

安全性级别

要提高安全性，可以使用密码来保护每个共享访问。SMB 提供了 3 种可能的方式来检查权限：

共享级安全性 (`security = share`)

严格地为一个共享指派一个密码。任何知道此密码的用户都可以访问此共享。

用户级安全性 (`security = user`)

这里将用户的概念引入了 SMB。每个用户都必须使用自己的密码在服务器上注册。注册后，服务器可以根据用户名来授予访问各个已导出共享的权限。

服务器级安全性 (security = server):

从客户机来看, Samba 好像是在用户级别方式下工作。但它实际将所有密码查询传递到另一个用户级别方式下的服务器来执行鉴定。此设置需要一个附加参数 (password server)。

共享、用户和服务器级安全性的选择适用于整个服务器。无法既为服务器配置的某些共享提供共享级安全性, 同时又为其他共享提供用户级安全性。但是, 您可以为系统上每个已配置的 IP 地址运行单独的 Samba 服务器。

有关此主题的详细信息, 请参阅 Samba HOWTO 文档集。对于一个系统上的多个服务器, 应注意选项 interfaces 和 bind interfaces only。

36.4 配置客户机

客户机只能通过 TCP/IP 访问 Samba 服务器。NetBEUI 和通过 IPX 的 NetBIOS 不能与 Samba 共用。

36.4.1 使用 YaST 配置 Samba 客户机

配置 Samba 客户机来访问 Samba 服务器上的资源 (文件或打印机)。在 *网络服务 > Windows 域成员资格* 对话框中输入域或工作组。单击浏览来显示所有可用的组和域, 然后可以用鼠标来选择它们。如果激活将 *SMB 信息也用于 Linux* 鉴定, 则用户鉴定将在 Samba 服务器上运行。在完成所有设置后, 单击完成完成配置。

36.4.2 Windows 9x 和 ME

Windows 9x 和 ME 都内置了对 TCP/IP 的支持。但默认情况下并不安装此支持。要添加 TCP/IP, 请转到 *控制面板 > 系统*, 然后选择 *添加 > 协议 > Microsoft 的 TCP/IP*。重引导您的 Windows 计算机后, 双击网络环境的桌面图标便可以找到 Samba 服务器。

提示

要使用 Samba 服务器上的打印机，请安装对应 Windows 版本的标准或 Apple-PostScript 打印机驱动程序。最好将其链接到 Linux 打印机队列，它接受 Postscript 作为一种输入格式。

36.5 将 Samba 用作登录服务器

在主要由 Windows 客户机组成的网络中，使用户只能使用有效帐户和密码进行注册通常是最好的选择。在基于 Windows 的网络中，此任务由主域控制器 (PDC) 来处理。您可以使用配置为 PDC 的 Windows NT 服务器，但是此任务也可以借助 Samba 服务器来完成。中显示了必须在 `smb.conf` 的 `[global]` 部分设置的项。[例 36.3 “smb.conf 中的 global 部分”](#) [633]

例 36.3 `smb.conf` 中的 `global` 部分

```
[global]
workgroup = TUX-NET
domain logons = Yes
domain master = Yes
```

如果将已加密密码用于校验目的（这是保持完好的 MS Windows 9X 安装、MS Windows NT 4.0 service pack 3 和所有以后版本产品的默认设置），则 Samba 服务器必须能够处理它们。`[global]` 部分中的 `encrypt passwords = yes` 项启用了此功能（对于 Samba 版本 3，这是默认设置）。此外，还需要以适合 Windows 的加密格式来准备用户帐户和密码。使用命令 `smbpasswd -a name` 可完成此任务。使用以下命令为计算机创建 Windows NT 域概念要求的域帐户：

例 36.4 设置计算机帐户

```
useradd hostname\$$
smbpasswd -a -m hostname
```

使用 `useradd` 命令可添加一个美元符号。命令 `smbpasswd` 在使用参数 `-m` 时自动插入此符号。带注释的配置示例 (`/usr/share/doc/packages/Samba/examples/smb.conf.SuSE`) 包含自动执行此任务的设置。

例 36.5 计算机帐户的自动设置

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \  
-s /bin/false %m$
```

为了确保 Samba 可以正确执行此脚本，应选择具有所需管理员权限的 Samba 用户。为此，请选择一个用户并将其添加到 `ntadmin` 组。然后可以使用以下命令来为属于此 Linux 组的所有用户指派 Domain Admin 状态：

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```

有关此主题的详细信息，请参见位于 `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf` 的 Samba HOWTO 文档集的第 12 章。

36.6 有关详细信息

关于 Samba 的详细信息，请参阅数字文档。在命令行输入 `apropossamba` 可显示一些手册页；如果安装了 Samba 文档，也可以浏览 `/usr/share/doc/packages/samba` 目录获得更多的联机文档和示例。可以在 `examples` 子目录中找到带注释的示例配置 (`smb.conf.SuSE`)。

Samba 开发小组提供的 Samba HOWTO 文档集中有一节专门介绍查错。此外，文档的第 V 部分提供了检查配置的逐步指南。安装包 `samba-doc` 后，可在 `/usr/share/doc/packages/samba/Samba-HOWTO-Collection.pdf` 中找到 Samba HOWTO 集。

有关 LDAP 和从 Windows NT 或 2000 迁移的详细信息，请参见 `/usr/share/doc/packages/samba/examples/LDAP/smbldap-tools-*/doc`，其中 * 是您的 `smbldap` 工具版本。

通过 NFS 共享文件系统

在企业环境中通过网络分发和共享文件系统是一项常见任务。NFS 是经过充分证实的系统，还可以与黄页协议 NIS 系统协同使用。要使用可以与 LDAP 协同使用、并且 Kerberos 化的更安全的协议，请选中 NFSv4。

又如第 33 章 *使用 NIS* [597] 所述，NFS 与 NIS 一起，使网络对用户是透明的。利用 NFS，可以通过网络分发任意文件系统。进行适当的设置后，用户将发现自己始终处于同一环境中，而与其当前使用的终端无关。

37.1 安装所需软件

要将主机配置为 NFS 客户机，无需安装其他软件。配置 NFS 客户机所需的所有包都将默认安装。

NFS 服务器软件不会默认安装。要安装 NFS 服务器软件，请启动 YaST 并选择 **软件 > 软件管理**。立即选择 **过滤器 > 模式** 并选择 **其他服务器** 或使用 **搜索选项** 搜索 NFS 服务器。确认包的安装以完成安装进程。

37.2 使用 YaST 导入文件系统

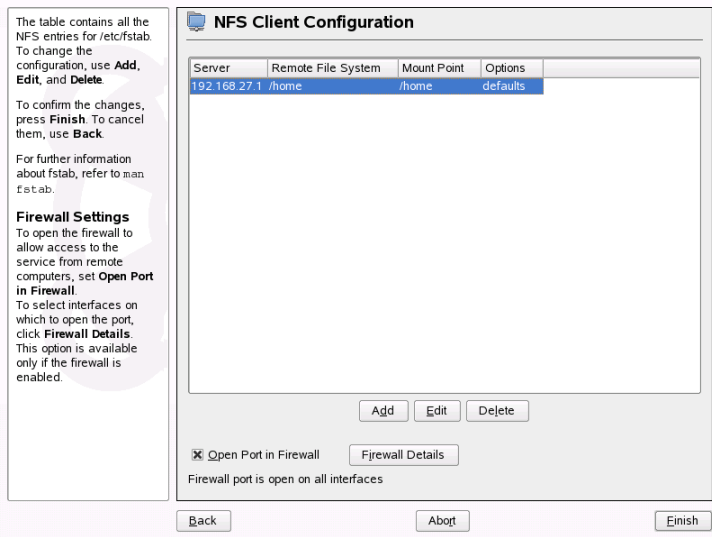
经过授权的用户都可以将 NFS 服务器中的 NFS 目录装入自己的文件目录树。使用 YaST 的 NFS 客户程序模块可以完成上述操作。只需输入 NFS 服务器的主机名、要导入的目录以及要在本地的哪个装入点装入此目录。在第一个对话框中单击 **添加** 后，这些更改即会生效。单击 **打开防火墙中的端口** 打开防火墙，以

便访问远程计算机上的服务。防火墙状态将显示在复选框旁边。单击完成保存更改。请参阅图 37.1 “使用 YaST 配置 NFS 客户机” [636]。

配置写入 /etc/fstab，并将装入指定的文件系统。当您稍后启动 YaST 配置客户程序时，它还将读取此文件中的现有配置。

当前只能手动导入 NFSv4 文件系统。这在第 37.3 节 “手动导入文件系统” [636] 中有说明。

图 37.1 使用 YaST 配置 NFS 客户机



37.3 手动导入文件系统

还可以从 NFS 服务器手动导入文件系统。前提条件是要运行 RPC 端口映射器，以 root 身份输入 rcpportmapstart 即可启动它。一旦满足了这个前提条件，通过以下方式使用 mount 命令，可以在文件系统中象装入本地硬盘那样装入远程导出的文件系统。

```
mount host:remote-path local-path
```

如果应该导入某台计算机（如 sun）上的用户目录，请使用以下命令：


```
mount sun:/home /home
```

37.3.1 导入 NFSv4 文件系统

必须在客户机上运行 `idmapd` 服务才能执行 NFSv4 导入。用 `rcidmapd start` 从命令提示符处启动 `idmapd` 服务。使用 `rcidmapd status` 检查 `idmapd` 的状态。

`idmapd` 服务将其参数存储在 `/etc/idmapd.conf` 文件中。将 `Domain` 参数的值保留为 `localdomain`。确保为 NFS 客户机和 NFS 服务器指定的值相同。

通过从 `shell` 提示符输入命令来执行 NFSv4 导入。要导入 NFSv4 远程文件系统，请使用以下命令：

```
mount -t nfs4 host:/ local-path
```

将 `host` 替换为主管一个或多个 NFSv4 导出的 NFS 服务器，并将 `local-path` 替换为装入的客户机中的目录位置。例如，要将用 `sun` 上的 NFSv4 导出的 `/home` 导入到 `/local/home`，请使用以下命令：

```
mount -t nfs4 sun:/ /local/home
```

服务器名称和冒号后跟的远程文件系统路径是 `“/”`。这与为 `v3` 导入指定的方式不同，执行 `v3` 导入时要提供远程文件系统的确切路径。此概念称为伪文件系统，这在第 37.4.1 节“为 NFSv4 客户机导出”[640]中有说明。

37.3.2 使用自动装入服务

除了装入通常的本地设备，`autofs` 守护程序还可以用于自动安装远程文件系统。要执行此操作，请在 `/etc/auto.master` 文件中添加以下条目：

```
/nfsmounts /etc/auto.nfs
```

如果 `auto.nfs` 文件正确完成，`/nfsmounts` 目录将作为客户机上所有 NFS 装入的根目录。文件名为 `auto.nfs` 是为了方便，也可以选择其他名称。在选定的文件（如果没有的话，就创建一个）中，如以下示例所示，添加所有 NFS 装入的条目：

```
localdata -fstype=nfs server1:/data
nfs4mount -fstype=nfs4 server2:/
```

用 `rcautofs start` 激活设置。对于此示例，`/nfsmounts/localdata`，`server1` 的 `/data` 目录将通过 NFS 装入，`server2` 的 `/nfsmounts/nfs4mount` 将通过 NFSv4 装入。

如果在运行 `autofs` 服务时编辑 `/etc/auto.master` 文件，则必须重新启动自动装入程序才能使更改生效。请用 `rcautofs restart` 执行此操作。

37.3.3 手动编辑 `/etc/fstab`

通常，`/etc/fstab` 中的 NFS 装入条目如下：

```
host:/data /local/path nfs rw,noauto 0 0
```

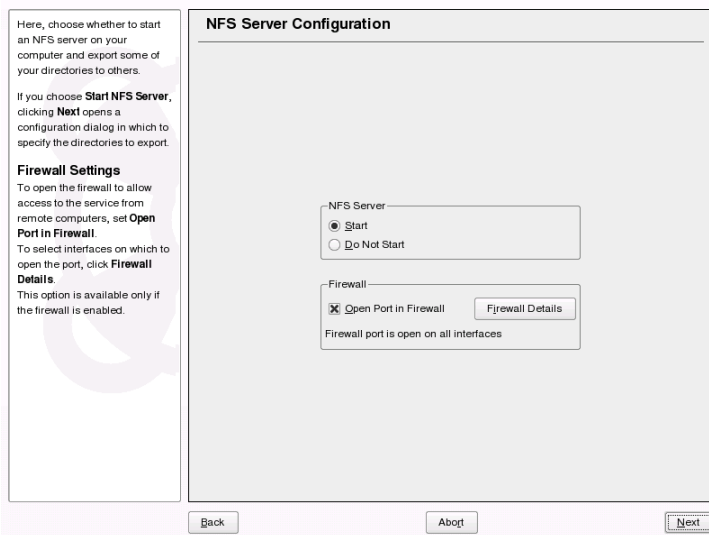
也可以手动将 NFSv4 装入添加到 `/etc/fstab` 文件中。对于这些装入，请在第三列中使用 `nfs4` 而不是 `nfs`，并确保在第一列中的 `host:` 后面用 `//` 指定远程文件系统。在 `/etc/fstab` 中保存该信息的优点是可以缩短装入命令，只提供本地装入点，例如：

```
mount /local/path
```

37.4 使用 YaST 导出文件系统

使用 YaST 将网络中的某台主机转换为 NFS 服务器，即将目录和文件导出到所有有权访问它的主机的服务器。这样做可以为同一工作组中的所有成员提供应用程序，而不必在每台主机的本地都安装应用程序。要安装此类服务器，请启动 YaST 并选择 **网络服务 > NFS 服务器**。打开一个如 [图 37.2 “NFS 服务器配置工具”](#) [639] 中所示的对话框。

图 37.2 NFS 服务器配置工具

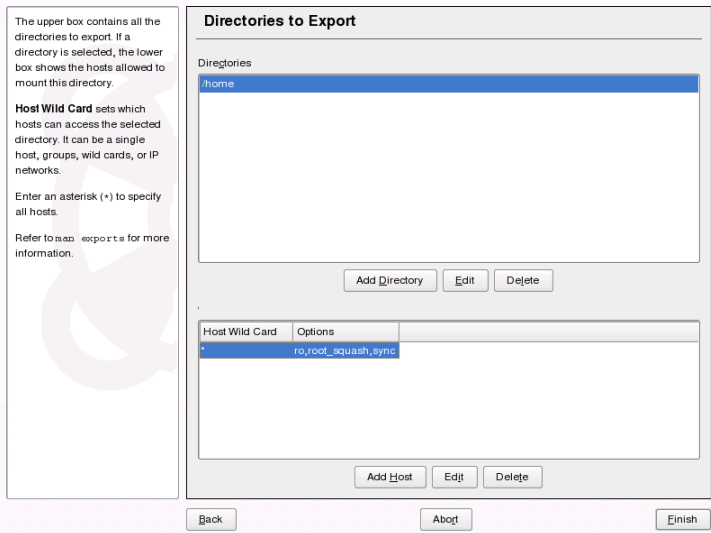


接着，激活启动 *NFS* 服务器并输入 *NFSv4* 域名。

如果您需要安全访问服务器，请单击启用 *GSS* 安全性。前提条件是您的域中安装了 *Kerberos* 并且服务器和客户机都已采用 *Kerberos* 系统。单击下一步。

在上面的文本字段中，输入要导出的目录。在下面输入应能访问这些目录的主机。图 37.3 “使用 *YaST* 配置 *NFS* 服务器” [640] 中显示了此对话框。该图显示了在先前对话框中启用 *NFSv4* 的场景。绑定装入目标显示在右边的窗格中。关于更多的细节，请参考左边窗格中显示的帮助。在对话框的下半部分，有四个可以为每个主机设置的选项：单主机、网络组、通配符和 *IP* 网络。关于这些选项的详细说明，请参阅导出手册页。单击完成以完成配置。

图 37.3 使用 YaST 配置 NFS 服务器



重要: 自动配置防火墙

如果系统启用了防火墙 (SuSEfirewall2)，在选择打开防火墙中的端口后，YaST 会通过启用 `nfs` 服务使防火墙的配置适应 NFS 服务器。

37.4.1 为 NFSv4 客户机导出

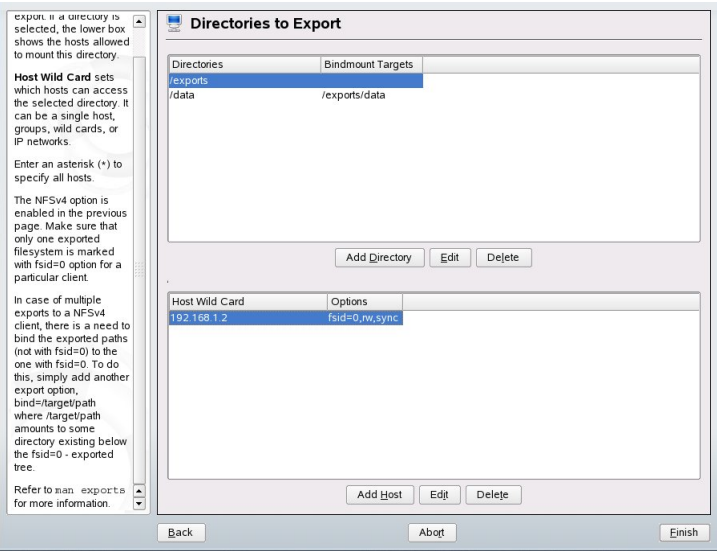
激活启用 NFSv4 支持 NFSv4 客户机。用 NFSv3 的客户机仍可访问服务器已导出的目录，如果它们已适当导出的话。这在第 37.4.3 节“并存的 v3 和 v4 导出”[643]中有说明。

激活 NFSv4 之后，请输入适当的域名。请确保输入访问此特定服务器的任何 NFSv4 客户机的 `/etc/idmapd.conf` 文件中存在的相同名称。此参数用于（服务器和客户机上）NFSv4 支持所需的 `idmapd` 服务。如果没有特殊要求，请将它保留为 `localdomain`（默认值）。有关详细信息，参见第 37.7 节“更多信息”[646]。

单击“下一步”。接下来的对话框有两部分。上半部分包含两列，名为目录和绑定装入目标。目录是直接可编辑的列，它列出了要导出的目录。

对于固定的客户机集合，有两类目录可以导出：作为伪根文件系统的目录；绑定到伪文件系统的某个子目录的目录。此伪文件系统作为基本点，为相同客户机导出的所有文件系统在其次各就各位。对于一个或一组客户机，服务器上只有一个目录可以配置为伪根目录以供导出。对于这个客户机，通过将它们绑定为伪根目录中现有的子目录可以导出多个目录。

图 37.4 用 NFSv4 导出目录



在对话框的下半部分，输入特定目录的客户程序（通配符）和导出选项。在上半部分添加目录后，用于输入客户机和选项信息的另一个对话框会自动弹出。然后，单击添加主机添加新客户机（客户机集）。

在打开的小对话框中，输入主机通配符。可以为每个主机设置四类主机通配符：单主机（名称或 IP 地址）、网络组、通配符（如 * 表示所有机器都能访问服务器）和 IP 网络。然后，在选项中，将 fsid=0 包含在逗号分隔的选项列表中，以将目录配置为伪根目录。如果此目录应该绑定到一个已配置的伪根目录下的另一个目录，请确保在选项列表中使用 bind=/target/path 提供目标绑定路径。

例如，假定选择目录 /exports 作为能访问服务器的所有客户机的伪根目录。然后将这添加到上半部分并确保为此目录输入的选项包含 fsid=0。如果另一个目录 /data 也需要用 NFSv4 导出，请将此目录添加到上半部分。为此输入选项时，请确保 bind=/exports/data 在列表中，并且 /exports/data 已

经是 `/exports` 的现有子目录。选项 `bind=/target/path` 中的任何更改（添加、删除或更改值）都会反映在绑定装入目标中。此列不是可以直接编辑的列，它总结了目录及其属性。信息完成后，请单击完成来完成配置或单击启动来重新启动服务。

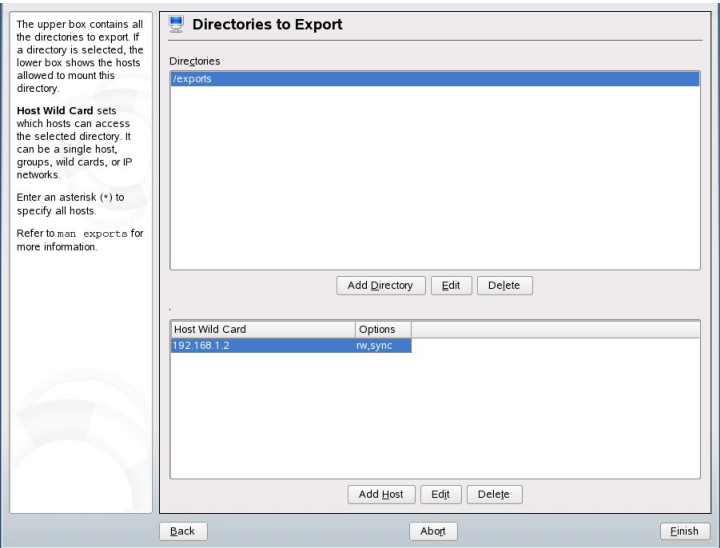
37.4.2 NFSv3 和 NFSv2 导出

请确保未在初始对话框中选中启用 *NFSv4*，然后单击下一步。

下一个对话框包含两部分。在上面的文本字段中，输入要导出的目录。在下面输入应能访问这些目录的主机。可以为每个主机设置四类主机通配符：单主机（名称或 IP 地址）、网络组、通配符（如 * 表示所有机器都能访问服务器）和 IP 网络。

图 37.4 “用 NFSv4 导出目录” [641] 中显示了此对话框。关于这些选项的详细说明，请参阅 `man exports`。单击完成以完成配置。

图 37.5 用 NFSv2 和 v3 导出目录



37.4.3 并存的 v3 和 v4 导出

NFSv3 和 NFSv4 导出可以在一个服务器上并存。在初始的配置对话框中启用了 NFSv4 之后，选项列表中不包含 `fsid=0` 和 `bind=/target/path` 的导出将作为 v3 导出处理。考虑图 37.4 “用 NFSv4 导出目录” [641] 中的示例。如果添加另一个目录（如 `/data2`），然后在相应的选项列表中使用添加目录不会提供 `fsid=0` 或 `bind=/target/path`，此导出将作为 v3 导出。

重要

自动配置防火墙

如果系统启用了 `SuSEfirewall2`，在选择了打开防火墙中的端口后，YaST 会通过启用该服务使防火墙的配置适应 NFS 服务器。

37.5 手动导出文件系统

NFS 导出服务的配置文件是 `/etc/exports` 和 `/etc/sysconfig/nfs`。除了这些文件之外，NFSv4 服务器配置还需要 `/etc/idmapd.conf`。要启动或重新启动服务，请运行命令 `rcnfsserver restart` 和 `rcidmapd restart`。NFS 服务器依赖于运行的 RPC 端口映射器。所以，还请使用 `rcportmap restart` 启动或重新启动端口映射器。

37.5.1 用 NFSv4 导出文件系统

NFSv4 是 SUSE Linux Enterprise 10 上可用的 NFS 协议的最新版本。用 NFSv4 配置导出目录的过程与先前的版本略有不同。

`/etc/exports` 文件

此文件包含条目列表。每个条目表示共享的目录以及共享的方式。`/etc/exports` 中的条目通常包含：

```
/shared/directory host(option_list)
```

例如：

```
/export 192.168.1.2(rw,fsid=0,sync)
/data 192.168.1.2(rw,bind=/export/data,sync)
```

在选项列表中指定了 `fsid=0` 的目录称为伪根文件系统。此处使用了 IP 地址 192.168.1.2。您可以使用主机名、表示一组主机的通配符（`*.abc.com`、`*` 等）或网络组。

对于一组固定的客户机，NFSv4 可导出两种目录：

- 选择作为伪根文件系统的单一目录。在此例中，`/exports` 是伪根目录，因为在此条目的选项列表中指定了 `fsid=0`。
- 选定与伪文件系统的某些现有子目录绑定的目录。在上述条目示例中，`/data` 就是与伪文件系统 `/export` 的现有子目录 (`/export/data`) 绑定的目录。

伪文件系统是顶级目录，在其下，需要用 NFSv4 导出的所有文件系统都各就各位。对于一个或一组客户机，在服务器上只能配置一个目录作为导出的伪根目录。对于这个或这组客户机，可通过将其他多个目录绑定到伪根目录的某个现有子目录进行导出。

/etc/sysconfig/nfs

此文件包含几个决定 NFSv4 服务器守护程序行为的参数。重要的是，参数 `NFSv4_SUPPORT` 必须设置为 `yes`。此参数决定了 NFS 服务器是否支持 NFSv4 导出和客户机。

/etc/idmapd.conf

Linux 计算机上的每个用户都有一个名称和 ID。`idmapd` 针对服务器的 NFSv4 请求执行名称到 ID 的映射并答复客户机。这必须同时在服务器和客户机上针对 NFSv4 运行，因为 NFSv4 在其通讯中仅使用名称。

对于可能正在使用 NFS 共享文件系统的计算机，请确保在这些计算机间为用户指定用户名和 ID (uid) 的方式一致。这可以使用 NIS、LDAP 或域中的任何统一的域鉴定机制来实现。

要实现正确的功能，必须为客户机和服务器设置相同的参数 `Domain`。如果您不确定，请在服务器和客户机文件中将域保留为 `localdomain`。配置文件样本如下：


```
[General]

Verbosity = 0
Pipefs-Directory = /var/lib/nfs/rpc_pipefs
Domain = localdomain

[Mapping]

Nobody-User = nobody
Nobody-Group = nobody
```

除非确定您在执行正确操作，否则请勿更改这些参数。关于更多参考，请阅读 `idmapd` 和 `idmapd.conf` 的手册页：`man idmapd`、`man idmapd.conf`。

启动和停止服务

更改 `/etc/exports` 或 `/etc/sysconfig/nfs` 后，通过 `rcnfsdserver restart` 启动或重新启动 NFS 服务器服务。更改 `/etc/idmapd.conf` 后，请用 `rcidmapd restart` 启动或重新启动 `idmapd` 服务。请确保两个服务都在运行。

37.5.2 用 NFSv2 和 NFSv3 导出文件系统

这特定于 NFSv3 和 NFSv2 导出。请参阅第 37.5.1 节“用 NFSv4 导出文件系统”[643]了解用 NFSv4 导出。

用 NFS 导出文件系统涉及两个配置文件：`/etc/exports` 和 `/etc/sysconfig/nfs`。通常，`/etc/exports` 文件条目的格式如下：

```
/shared/directory host(list_of_options)
```

例如：

```
/export 192.168.1.2(rw,sync)
```

其中，目录 `/export` 是与选项列表为 `rw,sync` 的主机 `192.168.1.2` 共享的。该 IP 地址可使用通配符（如 `*.abc.com`）甚至网络组替换为一个或一组客户机名称。

关于所有选项及其含义的详细说明，请参阅 `exports` (`man exports`) 的手册页。

更改 `/etc/exports` 或 `/etc/sysconfig/nfs` 后，请用命令 `rcnfsserver restart` 启动或重新启动 NFS 服务器。

37.6 采用 Kerberos 的 NFS

要对 NFS 使用 Kerberos 鉴定，必须启用 GSS 安全性。要执行此操作，请在初始 YaST 对话框中选择启用 GSS 安全性。另外，完成下列步骤：

- 请确保服务器和客户机都在同一 Kerberos 域中。这意味着它们访问相同的 KDC（密钥分发中心）服务器并共享其 `krb5.keytab` 文件（在任何机器上的默认位置是 `/etc/krb5.keytab`）。
- 在客户机上用 `rcgssd start` 启动 `gssd` 服务。
- 在客户机上用 `rcsvcgssd start` 启动 `svcgssd` 服务。

关于配置采用 Kerberos 的 NFS 的更多信息，请参阅第 37.7 节“更多信息”[646] 中的链接。

37.7 更多信息

除了 `exports`、`nfs` 和 `mount` 的手册页外，还可在 `/usr/share/doc/packages/nfs-tls/README` 和以下万维网文档中找到关于配置 NFS 服务器和客户机的信息：

在 SourceForge [<http://nfs.sourceforge.net/>] 上联机查找详细的技术文档。

关于设置采用 Kerberos 的 NFS 的说明，请参阅 NFS Version 4 Open Source Reference Implementation [<http://www.citi.umich.edu/projects/nfsv4/linux/krb5-setup.html>]

如果您对 NFSv4 有疑问，请参阅 Linux NFSv4 Frequently Asked Questions [<http://www.citi.umich.edu/projects/nfsv4/linux/faq/>] 常见问题解答。

文件同步

现今有很多人都在同时使用多台计算机 — 一台在家用，一台或多台在办公室用，还可能携带便携式计算机或 PDA 在路上用。很多文件是所有这些计算机上共同需要的。所以，您可能希望能在所有计算机上工作，修改文件，让所有计算机都能提供最新的数据。

38.1 可用的数据同步软件

数据同步对于通过快速网络永久互联的计算机而言并不是个问题。在这种情况下，使用 NFS 这样的网络文件系统并将文件储存在服务器上，就可以支持所有主机通过网络访问相同的数据。但如果网络连接较差或者不是永久连接，这种方法就行不通了。使用便携式计算机在途中工作时，所有所需文件的副本都必须位于本地硬盘上。不过，您需要随后同步修改的文件。在一台计算机上修改某个文件后，一定要更新该文件在所有其他计算机上的副本。对于零星的副本，可以用 `scp` 或 `rsync` 手动更新。但如果涉及大量文件，这个过程要复杂得多，您必须小心操作，避免出现旧文件覆盖新文件之类的错误。

警告：数据丢失风险

开始通过同步系统管理数据之前，您应该熟悉所用的程序并测试其功能。一定要对重要文件进行备份。

使用程序可以通过各种方法自动执行数据同步，从而克服手动同步数据时既耗时又容易出错的缺点。以下概要的目的只是让您大致了解这些程序的工作原理及它们的用法。如果打算使用它们，请阅读相应的程序文档。

38.1.1 CVS

CVS 主要用于对程序源代码进行版本管理；使用它可以在多台计算机上保留文件的副本。因此，该程序也适用于数据同步。CVS 在服务器上维护一个中央储存库，其中保存着文件和对文件的更改。本地执行的更改将提交到该储存库，并能够通过更新从其他计算机检索。这两个过程都必须由用户启动。

若多台计算机上都发生了更改，CVS 能够非常灵活地处理错误。这些更改将被合并，若发生在同一行上，则会报告冲突。发生冲突时，数据库仍保持一致状态。冲突仅显示在客户机上并在客户机上解决。

38.1.2 rsync

在无需版本控制但需要通过慢速网络连接同步大型目录结构时，rsync 工具可以提供较为完善的机制，仅传送文件中的更改。其中不仅涉及文本文件，还包括二进制文件。为检测文件间的差异，rsync 会将文件划分为多个块，并计算各个块的校验和。

检测更改需要消耗一定的资源。要使用 rsync，准备同步的系统应能够伸缩自如。RAM 尤为关键。

38.2 选择程序时的决定性因素

在决定使用哪个程序时请考虑几个重要因素。

38.2.1 客户机/服务器与对等模式

在分发数据时，常用的有两个模型。在第一个模型中，所有客户机都通过中央服务器来同步文件。所有客户机都应能够访问该服务器（至少能偶尔为之）。CVS 使用该模型。

另一个模型是让所有联网主机作为同级相互同步数据。rsync 实际在客户机模式下工作，但任何客户机都可用作服务器。

38.2.2 可移植性

CVS 和 rsync 还适用于其他很多操作系统，包括各种 Unix 和 Windows 系统。

38.2.3 交互与自动

在 CVS 中，数据同步是由用户手动启动的。这样可以有效控制要同步的数据并易于解决冲突。不过，如果同步间隔过长，就容易发生冲突。

38.2.4 冲突：事件和解决方案

在 CVS 中很少发生冲突，即便是多人同时在一个大型程序项目上协作时也不例外。这是因为合并文档时基于的是单个行。发生冲突时，只有一个客户机会受影响。通常很容易解决 CVS 中发生的冲突。

rsync 中不提供冲突解决功能。用户自己要避免意外覆盖文件，并手动解决所有可能的冲突。为安全起见，还可以使用 RCS 之类的版本控制系统。

38.2.5 选择和添加文件

在 CVS 中，必须使用命令 `cvsadd` 明确添加新目录和文件。这样用户可以更有效地控制要同步的文件。但另一方面，这样也容易遗漏新文件，特别是在有大量文件时，很容易忽略 `cvs update` 输出中的问号。

38.2.6 历史

CVS 的另一个功能是能够重建旧文件版本。每次一有更改都可以插入一个简短的编辑注释，以后根据文件内容和这些注释就很容易跟踪文件的变化。这对论文和程序文本大有帮助。

38.2.7 数据量和硬盘要求

所有相关主机的硬盘上都要有足够的可用于所有分发数据的空间。CVS 还要求服务器为储存库准备额外的空间。文件历史记录也储存在服务器上，这进一步

增加了空间要求。更改文本格式的文件时，只需保存修改的那些行。而二进制文件则要求在每次更改文件时都要有与文件大小相同的额外空间。

38.2.8 GUI

有经验的用户通常从命令行运行CVS。不过，图形用户界面也适用于Linux（如cervisia）以及其他操作系统（如wincvs）。许多开发工具（如kdevelop）及文本编辑器（如Emacs）都提供针对CVS的支持。在这些前端上解决冲突往往较为容易。

38.2.9 用户友好

rsync相当容易使用，还适合初学者。CVS某种程度上较难操作。用户应该了解储存库和本地数据之间如何交互。对数据的更改首先要在本地与储存库合并。使用命令 `cvs update` 可完成上述操作。然后必须使用命令 `cvs commit` 将数据发回储存库。一旦了解了此过程，新手也就能毫不费力地使用CVS了。

38.2.10 预防攻击

在传送数据的过程中，最好防止数据被拦截或操纵。CVS和rsync可以方便地通过ssh（安全shell）使用，从而防止遭受此类攻击。应避免通过rsh（远程shell）运行CVS。也不建议在不安全的网络中使用*pserver*机制访问CVS。

38.2.11 防止数据丢失

开发人员使用CVS来管理程序项目已有很长时间，所以该程序极为稳定。由于能够保存开发历史记录，CVS甚至能够预防某些用户错误，如意外删除文件。

表 38.1 文件同步工具的功能：-- = 很差，- = 差或不可用，o = 中等，+ = 好，++ = 很棒，x = 可用

	CVS	rsync
客户机/服务器	客户机-服务器	客户机-服务器

	CVS	rsync
可移植性	Lin、Un*x、Win	Lin、Un*x、Win
交互能力	x	x
速度	o	+
冲突	++	o
文件选择	所选/文件、目录	目录
历史	x	-
硬盘空间	--	o
GUI	o	-
难易程度	o	+
攻击	+(ssh)	+(ssh)
数据丢失	++	+

38.3 CVS 简介

如果经常编辑各个文件并且这些文件以 ASCII 文本或程序源代码文本之类的格式储存，则应该使用 CVS 来进行同步。用 CVS 同步其他格式的数据（如 JPEG 文件）固然可行，但这会产生大量数据，因为文件的所有变化都永久储存在 CVS 服务器中。这种情况下将无法利用 CVS 的大多数功能。只有在所有工作站都可以访问同一服务器时，才能使用 CVS 同步文件。

38.3.1 配置 CVS 服务器

服务器是储存所有有效文件（包括所有文件的最新版本）的主机。任何固定的工作站都可以充当服务器。如果可能，应该对 CVS 储存库的数据进行定期备份。

配置 CVS 服务器时，通过 SSH 授予用户访问服务器的权限是一种不错的方式。如果用户在服务器上的用户名为 `tux`，并且在服务器和客户机上都安装了 CVS 软件，则必须在客户端设置以下环境变量：

```
CVS_RSH=ssh CVSROOT=tux@server:/serverdir
```

可使用命令 `cvsinit` 从客户端初始化 CVS 服务器。只需执行一次初始化。

最后，必须给同步指派名称。仅在客户机上选择或创建目录，以包含要使用 CVS 来管理的文件（该目录也可以为空）。目录的名称同时也是同步的名称。在本例中，目录名为 `synchome`。转到此目录并输入以下命令，将同步名称设置为 `synchome`：

```
cvs import synchome tux wilber
```

许多 CVS 命令都需要注释。为此，CVS 会启动一个编辑器（在环境变量 `$EDITOR` 中定义的编辑器；如果未定义任何编辑器，则使用 `vi`）。通过提前在命令行中输入注释（如下例所示），可以避免调用编辑器。

```
cvs import -m 'this is a test' synchome tux wilber
```

38.3.2 使用 CVS

现在，在所有主机上都可以使用 `cvsco synchome` 将该同步储存库签出。该操作将在客户机上创建新的子目录 `synchome`。要向服务器提交更改，请转到目录 `synchome`（或其子目录之一），然后输入 `cvscommit`。

默认情况下，所有文件（包括子目录）都要提交给服务器。若仅提交单个文件或目录，请按 `cvscommit file1 directory1` 中的方式进行指定。在将新文件和目录提交给服务器之前，必须使用 `cvsadd file1 directory1` 之类的命令先将其添加到储存库中。随后再使用 `cvscommit file1 directory1` 命令提交新添加的文件和目录。

如果转到另一个工作站，则需要签出同步储存库（如果在同一工作站上的较早会话中尚未执行该操作）。

使用 `cvsupdate` 开始与服务器同步。如 `cvsupdate file1 directory1` 所示更新各个文件或目录。要查看当前文件与服务器上储存的版本的差异，请使用命令 `cvsdiff` 或 `cvsdiff file1 directory1`。使用 `cvs-nq update` 可以查看哪些文件将受到更新的影响。

以下是更新期间显示的一些状态符号：

U

已更新本地版本。这将影响服务器提供的和本地系统缺少的所有文件。

M

已修改本地版本。若服务器发生更改，可以将差异并入本地副本。

P

已使用服务器上的版本修补本地版本。

C

本地文件与储存库中的当前版本冲突。

?

此文件在 CVS 中不存在。

状态 M 表示本地修改的文件。可以向服务器提交本地副本，也可以在删除本地文件后再次进行更新。更新后将能够从服务器中恢复缺失的文件。如果提交了本地修改的文件但提交的这个文件中的同一行发生了更改，则可能发生冲突（由 C 表示）。

在这种情况下，查看文件中的冲突标记（»> 和 «<），决定要采用哪个版本。由于这是一项令人不快的工作，您可以选择放弃更改，删除本地文件，然后输入 `cvsup` 从服务器恢复当前版本。

38.3.3 有关详细信息

本节仅对 CVS 的多种情况进行了简要介绍。以下 URL 提供了大量的文档：

- CVS: <http://www.cvshome.org>
- Rsync: <http://www.gnu.org/manual>

38.4 rsync 简介

如果需要定期传送大量数据而更改的数据量不是很大，则适用 rsync。举例来说，创建备份时的情况往往就是这样。另一种应用涉及临时服务器。临时服务器是储存万维网服务器的完整目录树的服务器，这些万维网服务器定期镜像到 DMZ 中的万维网服务器。

38.4.1 配置和操作

rsync 有两种操作方式。可用于存档或复制数据。要执行上述操作，目标系统上只需要有远程 shell，如 ssh。不过，rsync 也可用作守护程序，为网络提供目录。

rsync 的基本操作方式不需要任何特殊配置。rsync 能直接将完整目录镜像到其他系统中。举例来说，以下命令在名为 sun 的备份服务器上为 tux 的主目录创建了备份副本。

```
rsync -baz -e ssh /home/tux/ tux@sun:backup
```

以下命令用于回放该目录：

```
rsync -az -e ssh tux@sun:backup /home/tux/
```

到目前为止，该程序的操作方式与普通的复制工具 (如 scp) 的操作方式相差无几。

应该以“rsync”方式操作 rsync，以便充分利用其所有功能。这需要在其中一个系统上启动 rsyncd 守护程序。在文件 /etc/rsyncd.conf 中配置该守护程序。例如，要使目录 /srv/ftp 可用于 rsync，请使用以下配置：

```
gid = nobody
uid = nobody
read only = true
use chroot = no
transfer logging = true
log format = %h %o %f %l %b
log file = /var/log/rsyncd.log

[FTP]
    path = /srv/ftp
    comment = An Example
```

然后使用 `rcrsyncdstart` 启动 rsyncd。rsyncd 也可以在引导进程中自动启动。通过在 YaST 提供的运行级别编辑器中激活此服务或通过手动输入命令 `insservrsyncd`，都可以完成上述设置。也可以使用 `xinetd` 来启动 rsyncd。不过，建议只在很少使用 rsyncd 的服务器上采用这种启动方式。

下例还创建了一个列出所有连接的日志文件。此文件储存在 /var/log/rsyncd.log 中。

随后可以从客户机系统测试传送。请使用以下命令完成该操作：

```
rsync -avz sun::FTP
```

此命令列出服务器的 /srv/ftp 目录中现有的所有文件。此请求还记录在日志文件 /var/log/rsyncd.log 中。要启动实际的传送，请提供目标目录。使用 `.` 表示当前目录。例如：

```
rsync -avz sun::FTP .
```

默认情况下，使用 rsync 同步时不会删除任何文件。如果应强制删除，必须明确指定附加选项 `--delete`。为保证不删除任何较新的文件，可转而使用选项 `--update`。必须手动解决所有冲突。

38.4.2 有关详细信息

有关 rsync 的重要信息，请参阅手册页 `manrsync` 和 `manrsyncd.conf`。
`/usr/share/doc/packages/rsync/tech_report.ps` 专门提供了关于 rsync 工作原理的技术参考。在 rsync 的万维网站点 <http://rsync.samba.org/> 上可以找到关于该项目的最新消息。

如果要用 Subversion 或其他工具，请下载 SDK。请参见 http://developer.novell.com/wiki/index.php/SUSE_LINUX_SDK。

部分 V. 安全性

伪装和防火墙

只要在联网环境中使用 Linux，您就可以使用内核功能通过操纵网络包将内部网络区域和外部网络区域隔开。Linux netfilter 框架提供了一种建立有效防火墙的方法，可以将不同网络隔开。借助 iptables — 用于定义规则集的通用表结构 — 可以精确控制哪些包能通过网络接口。使用 SuSEfirewall2 和相应的 YaST 模块，您可以轻而易举地设置这种包过滤器。

39.1 使用 iptables 过滤包

部件 netfilter 和 iptables 负责网络包的过滤和操纵以及网络地址转换 (NAT)。过滤准则及与过滤准则关联的所有操作均储存在链中；各个网络包在到达时，必须依次与这些链进行匹配。要匹配的链储存在表中。使用 iptables 命令可以更改这些表和规则集。

Linux 内核维护以下三个表，分别对应包过滤器的不同功能：

过滤器

此表储存大多数过滤规则，因为它执行严格意义上的包过滤机制，例如，决定是让包通过 (ACCEPT) 还是将包丢弃 (DROP)。

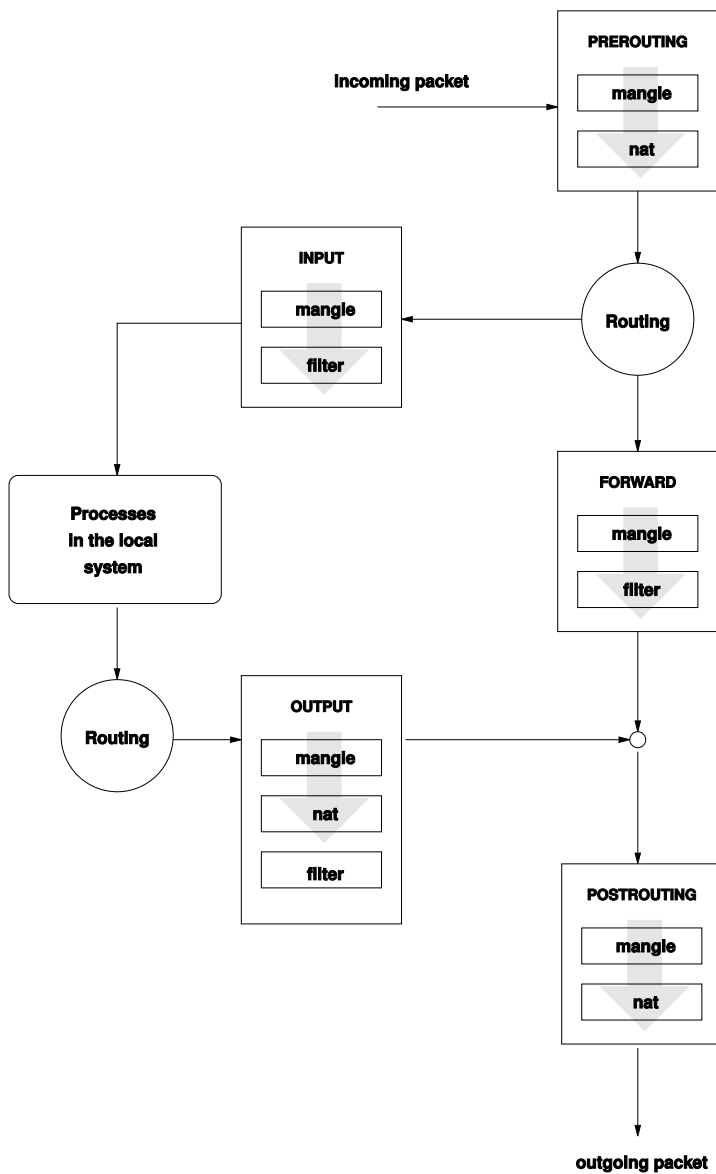
nat

此表定义对包的源地址和目标地址所做的任何更改。使用这些功能还能实现伪装，这是 NAT 的一个特例，用于将专用网络与因特网链接起来。

mangle

此表中的规则用于操纵 IP 报头中储存的值（如服务类型）。

图 39.1 iptable: 包的可能路径



这些表包含多个用于匹配包的预定义链:

PREROUTING

此链适用于入站包。

INPUT

此链适用于发往系统内部进程的包。

FORWARD

此链适用于仅在系统中路由的包。

OUTPUT

此链适用于从系统自身发出的包。

POSTROUTING

此链适用于所有出站包。

图 39.1 “iptables：包的可能路径” [660]演示了网络包在特定系统中传送时可能经过的路径。为了便于说明，图中将表作为链的各个部分列出，但实际上表本身储存了这些链。

在所有可能的情况中最简单的情况是：发往系统本身的入站包到达 `eth0` 接口。数据包首先要转到 `mangle` 表的 `PREROUTING` 链，然后转到 `nat` 表的 `PREROUTING` 链。随后的步骤（涉及包的路由选择）确定包的最终目标，这是系统自身的过程。在包经过 `mangle` 表和 `filter` 表的 `INPUT` 链后，只要与 `filter` 表的规则确实匹配，那么包将最终到达目标。

39.2 关于伪装的基础知识

伪装是 Linux 特有的一种 NAT（网络地址转换）形式。通过伪装可以将小型 LAN（其中的主机使用专用地址范围内的 IP 地址，请参阅第 30.1.2 节“网络掩码和路由” [544]）与因特网（使用正式的 IP 地址）连接起来。为使 LAN 主机能连接到因特网，需要将其专用地址转换为正式地址。这种转换是在路由器上完成的，路由器充当了 LAN 和因特网之间的网关。其中的原理只有简单的一条：路由器有多个网络接口，通常是一个网卡和与因特网连接的另一个接口。后者将路由器与外部世界链接起来，同时，还会有一个或多个其他网络接口将路由器与 LAN 主机链接起来。在本地网络中的这些主机连接到路由器的网卡（如 `eth0`）后，它们就可以将发往本地网络之外的所有包发送到其默认网关或路由器。

重要: 使用正确的网络掩码

在配置网络时, 确保所有本地主机的广播地址和网络掩码都相同。做不到这一点就会导致无法正确路由数据包。

如上所述, 只要有某台 LAN 主机要向因特网地址发送包, 这个包就会发送到默认路由器。但是, 必须先配置路由器, 然后才能转发这些包。由于安全原因, 默认安装中未启用它。要提供这种支持, 请将文件 `/etc/sysconfig/sysctl` 中的变量 `IP_FORWARD` 设置为 `IP_FORWARD=yes`。

连接的目标主机可以看到路由器, 但对内部网络中发出包的那台主机却毫不知情。伪装技术就是因此而得名的。由于要进行地址转换, 路由器自然成为所有回复包首先到达的目标。路由器必须能够识别这些入站包并转换其目标地址, 这样才能将包转发给本地网络中的正确主机。

由于入站通讯数据的路由选择取决于伪装表, 所以从外部根本无法打开与内部主机的连接。对于这种连接, 伪装表中不会有任何对应项。此外, 所有已建立的连接在该表中都被指派了一个状态项, 所以其他连接无法再使用该项。

受以上各种因素影响, 在使用某些应用程序协议, 如 ICQ、cucme、IRC (DCC、CTCP) 和 FTP (采用 PORT 方式) 时, 您可能会遇到一些问题。万维网浏览器、标准 FTP 程序和许多其他程序都使用 PASV 方式。就包过滤和伪装而言, 这种被动方式不容易出问题。

39.3 防火墙基础知识

在描述不仅可以提供和管理网络间的链接, 同时还能够控制网络间的数据流的机制时, 防火墙可能是最常使用的术语。严格地说, 本节所述的机制应该叫做包过滤器。包过滤器根据特定准则 (如协议、端口和 IP 地址) 来控制数据流。这样您就可以根据包的地址来拦截不应该发送到您网络中的包。举例来说, 若允许对万维网服务器进行公共访问, 应明确打开相应的端口。不过, 包过滤器并不扫描有合法地址的包的内容 (例如那些要发送到该万维网服务器的包)。例如, 即使是在入站包想要破坏万维网服务器上的 CGI 程序的情况下, 包过滤器仍然允许它们通过。

一种更有效但同时也更复杂的机制是将多种系统结合起来使用, 例如让包过滤器与应用程序网关或代理进行交互。在这种情况下, 包过滤器将拒绝所有发往禁用端口的包, 而只接受发往应用程序网关的包。此网关或代理伪装成服务器

的实际客户端。从某种意义上说，可以将这种代理视为应用程序使用的协议级的伪装主机。这种代理的一个示例就是 Squid（一种 HTTP 代理服务器）。要使用 Squid，必须将浏览器配置为通过代理通讯。代理超速缓存将提供请求的任何 HTTP 页，超速缓存中没有的页将由代理从因特网获取。再以 SUSE proxy-suite (proxy-suite) 为例，该程序为 FTP 协议提供了代理。

下一节着重介绍 SUSE Linux Enterprise 附带的包过滤器。有关包过滤和防火墙的详细信息，请阅读 howto 包中的 Firewall HOWTO（防火墙使用说明）。如果已安装此包，请阅读 HOWTO，方法是使用

```
less /usr/share/doc/howto/en/txt/Firewall-HOWTO.gz
```

39.4 SuSEfirewall2

SuSEfirewall2 是一个脚本，用来读取在 /etc/sysconfig/SuSEfirewall2 中设置的变量以生成一组 iptables 规则。该脚本定义了三个安全区域，但在以下示例配置中只涉及第一个和第二个安全区域：

外部区域

鉴于根本无法对外部网络进行控制，所以需要保护主机，使其免受外部网络的影响。在多数情况下，外部网络就是因特网，但也可能是其他不安全的网络，如 WLAN。

内部区域

内部网络是指专用网络，多为 LAN。如果此网络中的主机使用专用地址范围中的 IP 地址（请参见 [第 30.1.2 节“网络掩码和路由”](#) [544]），则必须启用网络地址转换 (NAT)，内部网络中的主机才能访问外部网络。

网络隔离区 (DMZ)

尽管从外部网络和内部网络都可以访问此区域内的主机，但这些主机本身无法访问内部网络。这种设置可用于在内部网络前再加一道防线，因为 DMZ 系统与内部网络是隔离的。

凡是过滤规则集没有明确允许通过的网络通讯数据，iptables 都一概禁止。因此，必须将入站通讯数据所流经的各个接口放入这三个区域之一。对于每个区域，都应定义所允许的服务或协议。规则集只适用于来自远程主机的包。防火墙不截获本地生成的包。

可以使用 YaST 进行上述配置（请参阅 [第 39.4.1 节“使用 YaST 配置防火墙”](#) [664]）。还可以在文件 /etc/sysconfig/SuSEfirewall2 中进行手动配

置，该文件已作适当注释。另外，`/usr/share/doc/packages/SuSEfirewall2/EXAMPLES` 还提供了一些示例方案。

39.4.1 使用 YaST 配置防火墙

重要: 自动配置防火墙

完成安装后，YaST 会在所有已配置接口上自动启动防火墙。如果在系统中配置并激活了某个服务器，YaST 可通过服务器配置模块中的选项 *打开防火墙中所选接口上的端口* 或 *打开防火墙中的端口* 修改自动生成的防火墙配置。某些服务器模块对话框包含 *防火墙细节* 按钮，用于激活其他服务和端口。YaST 防火墙配置模块可用于激活、取消激活防火墙或单独对其进行重配置。

可以从 YaST 控制中心访问图形化的 YaST 配置对话框。选择 *安全性和用户 > 防火墙*。该配置分为 7 个部分，可以在屏幕左侧的树结构上直接访问它们。

币筐

在该对话框中设置启动行为。在默认安装中将自动启动 SUSEfirewall2。也可以在这里启动和停止防火墙。要在正在运行的防火墙上实施新的设置，请使用 *保存设置并立刻重启动防火墙*。

接口

这里列出了所有已知的网络接口。要从区域中去除某接口，请选择此接口，并在按 *更改* 后选择 *未指派任何区域*。要向区域中添加某接口，请选择此接口，并在按 *更改* 后选择任一可用区域。也可以使用 *自定义* 来创建一个采用您自己的设置的特殊接口。

允许的服务

您需要此选项来从自己的系统向受保护区域提供服务。默认情况下，服务器仅免受外部区域的影响。明确允许使用外部主机可用的服务。在 *所选区域允许的服务* 中选择所需的区域后，激活该列表中的服务。

伪装

对外部网络（例如因特网），伪装隐藏您的内部网络，但内部网络中的主机可以透明地访问外部网络。伪装将阻塞从外部网络到内部网络的请求，而发自内部网络的请求从外部来看好像是由伪装服务器发出的。如果需要使外部网络能够使用内部计算机的特殊服务，则可以为服务添加特殊重定向规则。

广播

在该对话框中配置允许广播的 UDP 端口。将所需的各个端口号或服务添加到适当区域，以空格分隔。另请参见文件 `/etc/services`。

可以在这里启用未接受的广播日志记录。这样做可能会出现问题，因为 Windows 主机使用广播来互相识别，从而生成许多未接受的包。

IPsec 支持

在此对话框中配置是否允许从外部网络使用 IPsec 服务。在 *细节* 下配置可信的包。

日志记录级别

对于登录有两条规则：已接受和未接受的包。未接受的包为 **DROPPED** 或 **REJECTED**。可以为这两种包选择 *全部记录*、*只记录关键信息* 或 *不记录任何信息*。

完成防火墙配置后，选择下一步退出此对话框。然后打开面向区域的防火墙配置概要。在其中检查所有的设置。所有已允许使用的服务、端口和协议均在此概要中列出。要修改配置，请使用 *后退*。按 *接受* 即可保存您的设置。

39.4.2 手动配置

以下段落提供进行成功配置的分步说明。每个配置项都根据该项是与防火墙有关还是与伪装有关作了相应标记。如果适用，请使用端口范围（例如 `500:510`）。这里未涉及配置文件中提到的与 **DMZ**（网络隔离区）相关的内容。这些内容只适用于大型组织中较复杂的网络基础结构（公司网络），这需要大量配置以及对此主题的深入了解。

首先，使用 YaST 模块系统服务（运行级别）以您的运行级别（很可能是 3 或 5）启用 `SUSEfirewall2`。这会在 `/etc/init.d/rc?.d/` 目录中设置 `SUSEfirewall2_*` 脚本的符号链接。

FW_DEV_EXT（防火墙，伪装）

链接到因特网的设备。对于调制解调器连接，请输入 `ppp0`。对于 ISDN 链接，请使用 `ipp0`。DSL 连接使用 `dsl0`。指定 `auto` 使用与默认路由对应的接口。

FW_DEV_INT (防火墙, 伪装)

链接到内部专用网络的设备 (如 `eth0`)。如果内部网络不存在, 防火墙只保护它运行所在的主机, 则应将此项保留为空白。

FW_ROUTE (防火墙, 伪装)

如果需要伪装功能, 请将此项设置为 `yes`。内部主机对外将是不可见的, 因为因特网路由器将忽略内部主机的专用网络地址 (例如 `192.168.x.x`)。

对于未使用伪装功能的防火墙而言, 只有在您希望允许访问内部网络时才应将此项设置为 `yes`。在此情况下, 内部主机需要使用正式注册的 IP 地址。但在通常情况下, 应禁止从外部访问您的内部网络。

FW_MASQUERADE (伪装)

如果需要伪装功能, 则将此项设置为 `yes`。这实际上为内部主机提供了与因特网的直接连接。但更保险的做法是在内部网络主机和因特网主机之间设置代理服务器。代理服务器提供的服务不需要伪装。

FW_MASQ_NETS (伪装)

指定要伪装的主机或网络, 各个项之间要留有空格。例如:

```
FW_MASQ_NETS="192.168.0.0/24 192.168.10.1"
```

FW_PROTECT_FROM_INT (防火墙)

将此项设置为 `yes` 可以保护防火墙主机免遭来自内部网络的攻击。只有已经显式启用服务, 才可以在内部网络中使用这些服务。另请参见 `FW_SERVICES_INT_TCP` 和 `FW_SERVICES_INT_UDP`。

FW_SERVICES_EXT_TCP (防火墙)

输入应该可用的 TCP 端口。对于不应提供任何服务的家用普通工作站, 应将此项保留为空白。

FW_SERVICES_EXT_UDP (防火墙)

除非您运行 UDP 服务并希望此服务对外部可用, 否则将此项保留为空白。使用 UDP 的服务包括 DNS 服务器、IPsec、TFTP、DHCP 等。在此情况下, 请输入要使用的 UDP 端口。

FW_SERVICES_INT_TCP (防火墙)

使用此变量定义可用于内部网络的服务。变量表示法与 `FW_SERVICES_EXT_TCP` 的表示法相同, 但变量设置适用于内部网络。只有在 `FW_PROTECT_FROM_INT` 设置为 `yes` 时才需要设置此变量。

FW_SERVICES_INT_UDP (防火墙)
请参见 FW_SERVICES_INT_TCP。

配置防火墙后，请测试您的设置。以 root 身份输入 `SUSEfirewall2 start` 可创建防火墙规则集。然后，举例来说，可以从外部主机使用 `telnet` 查看是否确实会拒绝连接。此后，请查看 `/var/log/messages`，应能看到如下所示的内容：

```
Mar 15 13:21:38 linux kernel: SFW2-INext-DROP-DEFAULT IN=eth0
OUT= MAC=00:80:c8:94:c3:e7:00:a0:c9:4d:27:56:08:00 SRC=192.168.10.0
DST=192.168.10.1 LEN=60 TOS=0x10 PREC=0x00 TTL=64 ID=15330 DF PROTO=TCP
SPT=48091 DPT=23 WINDOW=5840 RES=0x00 SYN URGP=0
OPT (020405B40402080A061AFEB00000000001030300)
```

用于测试您的防火墙设置的其他包有 `nmap` 或 `nessus`。在安装相应的包后，`nmap` 的文档位于目录 `/usr/share/doc/packages/nmap` 中，`nessus` 的文档位于目录 `/usr/share/doc/packages/nessus-core` 中。

39.5 有关详细信息

`/usr/share/doc/packages/SUSEfirewall2` 中提供了有关 `SUSEfirewall2` 包的最新信息和其他文档。`netfilter` 和 `iptables` 项目的主页 <http://www.netfilter.org> 以多种语言提供了丰富的文档资料。

SSH：安全性网络操作

随着在联网环境中安装的计算机越来越多，常常需要从远程位置访问主机。通常，这意味着用户要发送登录名和密码字符串进行鉴定。只要以明文形式传送这些字符串，攻击者就可能会截获并恶意使用这些字符串获取对该用户帐户的访问权，而授权用户根本毫无察觉。一旦得逞，攻击者不仅可以控制所有用户文件，还可能利用此非法帐户获取管理员或 `root` 访问权，或侵入其他系统。过去常用 `telnet` 建立远程连接，但该程序没有采用加密形式或其他安全机制防止窃听。还存在其他未加保护的通讯信道，例如传统的 FTP 协议和某些远程复制程序。

SSH 套件通过对鉴定字符串（通常由登录名和密码构成）及主机间交换的所有其他数据进行加密，能够提供必要的保护。使用 SSH，虽然第三方仍可以记录数据流，但内容是经过加密的，除非了解加密钥，否则无法将其还原为明文。这样，SSH 在不安全的网络（如因特网）上实现了安全通讯。SUSE Linux Enterprise 附带的 SSH 程序是 OpenSSH。

40.1 OpenSSH 软件包

SUSE Linux Enterprise 会在默认情况下安装 OpenSSH 包。安装之后即可由程序 `ssh`、`scp` 和 `sftp` 来替代 `telnet`、`rlogin`、`rsh`、`rcp` 和 `ftp`。在默认配置中，只能使用 OpenSSH 实用程序访问 SUSE Linux Enterprise 系统，而且只能在防火墙允许访问的情况下访问。

40.2 ssh 程序

使用 ssh 程序可以登录到远程系统并以交互方式工作。该程序取代了 telnet 和 rlogin。slogin 程序只是指向 ssh 的符号链接。例如，使用命令 sshsun 登录到主机 sun。该主机会随后提示输入 sun 上的密码。

通过鉴定后，既可以使用远程命令行操作，也可以使用 YaST 之类的交互式应用程序操作。如果本地用户名不同于远程用户名，则可以使用不同的登录名通过 ssh-l augustine sun 或 sshaugustine@sun 登录。

此外，ssh 还提供了在远程系统上运行命令的功能（也就是 rsh 提供的功能）。下例在主机 sun 上运行命令 uptime 并创建了一个名为 tmp 的目录。程序输出显示在主机 earth 的本地终端上。

```
ssh otherplanet "uptime; mkdir tmp"
Password:
1:21pm up 2:17, 9 users, load average: 0.15, 0.04, 0.02
```

在此需要加引号，以便使用一个命令同时发送两条指令。只有加引号才能在 sun 上执行第二个命令。

40.3 scp — 安全复制

使用 scp 可以将文件复制到远程计算机。该程序取代了 rcp，是一个既安全又有加密功能的程序。例如，scpMyLetter.tex sun: 可以将文件 MyLetter.tex 从主机 earth 上复制到主机 sun 上。如果 earth 上的用户名不同于 sun 上的用户名，请使用 username@host 格式指定后者的用户名。此命令没有 -l 选项。

输入正确的密码后，scp 开始传送数据，同时显示一行不断增多的星号来模拟进度条。此外，该程序还能显示到达进度条右端的估计时间。通过提供选项 -q 可以取消显示所有输出。

scp 还提供了对整个目录的递归复制功能。命令 scp-r src/ sun:backup/ 可以将目录 src 的全部内容（包含所有子目录）都复制到主机 sun 上的 backup 目录。这个子目录若不存在，就会自动创建该子目录。

选项 `-p` 指示 `scp` 不更改文件的时间戳。`-c` 将对传送数据进行压缩。这会最大限度地减少要传送的数据量，但同时增加了处理器的负担。

40.4 sftp — 安全的文件传送

`sftp` 程序可以取代 `scp` 来执行安全的文件传送。在 `sftp` 会话期间，您可以使用许多来自 `ftp` 的命令。`sftp` 程序可能要优于 `scp`，特别是在传送文件名未知的数据时。

40.5 SSH 守护程序 (sshd) — 服务器端

要使用 SSH 客户程序 `ssh` 和 `scp`，必须在后台运行服务程序（即 SSH 守护程序），用于监听 TCP/IP port 22 上的连接。首次启动该守护程序时将生成三个密钥对。各密钥对均由私用密钥和公钥组成。因此，通常提到该过程，就认为它是基于公共密钥的。要保证通过 SSH 安全地通讯，必须限制只有系统管理员才能访问私用密钥文件。文件权限是在默认安装中相应设置的。只有在本地 SSH 守护程序才需要私用密钥，切勿将私用密钥提供给其他任何人。公钥组件（可通过扩展名 `.pub` 识别）将被发送到请求连接的客户机。所有用户都可以读取公钥组件。

连接请求是 SSH 客户机发出的。正在等待的 SSH 守护程序将与请求连接的 SSH 客户程序交换标识数据以比较协议和软件版本，防止通过错误的端口连接。由于请求是由最初的 SSH 守护程序的子进程回复的，所以可以同时建立多个 SSH 连接。

对于 SSH 服务器和 SSH 客户机间的通讯，OpenSSH 支持使用版本 1 和版本 2 的 SSH 协议。默认情况下使用的是版本 2 的 SSH 协议。用 `-1` 开关可以覆盖此默认设置，转而使用该协议的版本 -1。要在系统更新后继续使用版本 1，则请遵循 `/usr/share/doc/packages/openssh/README.SuSE` 中的指示信息。本文档还介绍了如何只通过几个步骤就将 SSH 1 环境转换为有效的 SSH 2 环境。

如果使用 SSH 版本 1，服务器将发送其公共主机密钥和一个服务器密钥（由 SSH 守护程序每小时重新生成一次）。这两个密钥都允许 SSH 客户机对自由选择的会话密钥加密（会话密钥会被发送到 SSH 服务器）。SSH 客户机还会通知服务器使用哪种加密方法（加密法）。

版本 2 的 SSH 协议不需要服务器密钥。但服务器端和客户端都要使用符合 Diffie-Helman 的算法来交换它们的密钥。

一定要使用私用主机密钥和服务器密钥对会话密钥解密，从公钥根本无法得出这些密钥。只有建立联系的 SSH 守护程序才能使用其私用密钥对会话密钥解密（请参阅 `man/usr/share/doc/packages/openssh/RFC.nroff`）。打开 SSH 客户机的冗长调试选项 `-v` 可以密切监视初始阶段的连接。

在与远程主机首次建立联系之后，客户机会将所有公共主机密钥储存在 `~/.ssh/known_hosts` 中。这会防止各种中间人攻击 — 外部 SSH 服务器试图使用伪造名称和伪造 IP 地址侵入系统。如果 `~/.ssh/known_hosts` 未包含某个主机密钥，或是因未能提供正确的私钥致使服务器无法对会话密钥解密，这两种情况下都可以检测到此类攻击。

建议将储存在 `/etc/ssh/` 中的私用密钥和公钥备份到安全的外部位置。这样就可以检测到密钥修改，并可以在重装后再次使用旧密钥。用户也就无需了解那些含糊不清的警告了。如果经过校验（尽管有警告）得知这确实是正确的 SSH 服务器，则必须从 `~/.ssh/known_hosts` 中去除有关此系统的现有项。

40.6 SSH 鉴定机制

现在开始执行实际的鉴定，最简单的鉴定形式就是上文提到的输入密码。SSH 的目的是提供安全且方便使用的软件。由于 SSH 是用来取代 `rsh` 和 `rlogin` 的，所以 SSH 必须也能提供一种适合日常使用的鉴定方法。SSH 是通过另一个密钥对（由用户生成）来实现该功能的。为此，SSH 包提供了一个帮助程序：`ssh-keygen`。输入 `ssh-keygen-t rsa` 或 `ssh-keygen-t dsa` 后就会生成密钥对，同时系统会提示您输入储存密钥所用的基本文件名。

确认默认设置并回应针对通行密码的请求。即使软件建议输入空的通行密码，仍建议您为此处说明的过程输入一个 10 到 30 个字符的通行密码。请不要使用简短的单词或短语。再次输入通行密码进行确认。随后，您将看到私钥和公钥的储存位置，在本例中为文件 `id_rsa` 和 `id_rsa.pub`。

使用 `ssh-keygen-p -t rsa` 或 `ssh-keygen-p -t dsa` 更改旧通行密码。将公钥组件（本例中为 `id_rsa.pub`）复制到远程计算机并保存到 `~/.ssh/authorized_keys` 中。下次建立连接时，系统将要求您使用通行密码对自身进行鉴定。如果系统没有要求鉴定，请校验这些文件的位置和内容。

从长期看，此过程比每次提供密码要麻烦。所以，SSH 包提供了另一种工具 `ssh-agent`，该工具可以在 X 会话期间保留私用密钥。整个 X 会话作为 `ssh-agent` 的子进程启动。为此，最简单的方法是将 `.xsession` 文件开始位置的变量 `usessh` 设置为 `yes` 并通过显示管理器（如 `KDM` 或 `XDM`）登录。也可以输入 `ssh-agentstartx`。

现在您就可以像平常那样使用 `ssh` 或 `scp` 了。如果按上文所述分发了公钥，系统就不再提示您输入密码。终止 X 会话或用密码保护应用程序（如 `xlock`）锁定该会话时一定要小心。

文件 `/usr/share/doc/packages/openssh/README.SuSE` 还介绍了由于引入版本 2 的 SSH 协议而产生的所有相关更改。

40.7 X、鉴定和转发机制

除上述有关安全方面的改进之外，SSH 还简化了远程 X 应用程序的用法。如果运行带选项 `-X` 的 `ssh`，远程计算机上会自动设置 `DISPLAY` 变量，而且所有 X 输出都将通过现有 SSH 连接导出到远程计算机上。同时，如果未经授权，其他人将无法截获通过此方法远程启动并在本地查看的 X 应用程序。

通过添加选项 `-A`，可以将 `ssh-agent` 鉴定机制转移到下一台计算机上。这样，您就可以在不同计算机上工作而无需输入密码，但前提是：已将公钥分发给目标主机并在其上正确保存。

上述两种机制在默认设置中均处于取消激活状态，但可以随时在全系统范围的配置文件 `/etc/ssh/sshd_config` 或用户的 `~/.ssh/config` 中永久激活这两种机制。

`ssh` 还可用于重定向 TCP/IP 连接。在下例中，SSH 分别用于重定向 SMTP 和 POP3 端口：

```
ssh -L 25:sun:25 earth
```

使用此命令，可以通过加密信道将定向到 `earth` 端口 25 (SMTP) 的任何连接重定向到 `sun` 上的 SMTP 端口。如果用户所用的 SMTP 服务器不具备 SMTP-AUTH 或 POP-before-SMTP 功能，此命令特别有用。从与网络相连的任意位置都可以将电子邮件传送到“家庭”邮件服务器进行递送。同样，使用以下命令，可以将 `earth` 上的所有 POP3 请求（端口 110）转发给 `sun` 的 POP3 端口：

```
ssh -L 110:sun:110 earth
```

必须以 `root` 身份执行这两个命令，因为连接指向有特权的本地端口。普通用户通过现有 `SSH` 连接发送和检索电子邮件。为此，必须将 `SMTP` 和 `POP3` 主机设置为 `localhost`。有关其他信息，请参见上述每个程序的手册页以及 `/usr/share/doc/packages/openssh` 下的文件。

网络鉴定 — Kerberos

除了通常的密码机制外，开放网络没有提供任何其他方法来确保工作站能够正确识别其用户。在一般的安装中，用户每次访问网络中的服务时都必须输入密码。Kerberos 提供了一种认证方法，采用这种方法，用户只要注册一次，就可整个网络中获得信任以完成会话的剩余操作。要拥有安全的网络，必须满足以下要求：

- 使所有用户可以对每个所需服务证明他们自己的身份，并确保任何用户都不能使用其他用户的身份。
- 确保每个网络服务器也能证明其身份。否则攻击者就可能冒充服务器并获取传送给服务器的敏感信息。这种概念被称为**相互认证**，因为在客户机和服务器之间进行了相互认证。

Kerberos 通过提供严格加密的认证来帮助您满足这些要求。下面内容说明这是如何实现的。这里仅讨论 Kerberos 的基本原理。有关详细的技术说明，请参考随 Kerberos 的实施提供的文档。

41.1 Kerberos 术语

以下词汇表定义了一些 Kerberos 术语。

身份凭证

用户或客户机需要提交某些身份凭证方可获得请求服务的授权。Kerberos 采用两种身份凭证 — 票证和鉴定器。

票证

票证是随服务器而不同的身份凭证，客户机使用票证在它请求提供服务的服务器上认证。它包含服务器的名称、客户机的名称、客户机的因特网地址、时戳、使用期限和随机会话密钥。所有这些数据都使用服务器的密钥进行了加密。

认证器

与票证相结合，认证器用于证明提交票证的客户机确实与其声称的身份相符。鉴定器由客户机名称、工作站 IP 地址、当前工作站时间组成。这些内容都使用会话密钥进行了加密，只有客户机和它请求提供服务的服务器才知道此密钥。与票证不同，鉴定器只能使用一次。客户机可以自己构建认证器。

主体

Kerberos 主体是可以对其指派票证的独特实体（用户或服务）。主体包含以下部分：

- **主部** — 主体的第一部分，如果主体是用户，则主部可以与您的用户名相同。
- **实例** — 描述主部特性的一些可选信息。此字符串和主部之间用一个 / 分隔。
- **Realm** — 指定您的 Kerberos 领域。通常情况下，领域就是您的大写域名。

相互认证

Kerberos 确保客户机和服务器都可以确定对方的身份。它们共享一个用来安全通讯的会话密钥。

会话密钥

会话密钥是由 Kerberos 生成的临时性私用密钥。客户机知道这些密钥。当客户机向服务器请求并收到票证后，将使用这些密钥来加密客户机和服务器之间的通讯。

重放

几乎所有在网络中发送的讯息都能够被窃听、盗取和重发送。在使用 Kerberos 的情况下，如果攻击者获取了包含您的票证和认证器的服务请求，则会非常危险。他随后可能会试图重发送此请求（重放）来冒充您。然而，Kerberos 实施了多种机制来解决此问题。

服务器或服务

服务用来指要执行的特定操作。此操作背后的进程被称为服务器。

41.2 Kerberos 的工作原理

Kerberos 通常被称为第三方可信认证服务，这意味着其所有客户机都信任 Kerberos 对另一个客户机身份的判断。Kerberos 保存着一个包含它的所有用户及其私用密钥的数据库。

要确保 Kerberos 值得信任，需要在一台专用计算机上运行认证和票证授予服务器。确保只有管理员能直接或通过网络访问此计算机。同时将在此计算机上运行的（网络）服务的数目降到最低 — 甚至可以不运行 sshd。

41.2.1 首次接触

在首次接触 Kerberos 时，您的操作与在常规网络系统进行的任何登录过程类似。输入您的用户名。这一信息和票证授予服务的名称被发送到鉴定服务器 (Kerberos)。如果认证服务器确定了您的身份，则它会生成一个随机的会话密钥，供以后在客户机和票证授予服务器之间使用。鉴定服务器现在将为票证授予服务器准备一个票证。该票证包含以下信息 — 都用会话密钥加密过，该密钥只有认证服务器和授予票证的服务器知道：

- 客户机和票证授予服务器的名称
- 当前时间
- 为此票证指派的有效期
- 客户机的 IP 地址
- 新生成的会话密钥

随后，还是以加密形式将此票证与会话密钥一起发送回客户机，但这次使用的是客户机的私用密钥。只有 Kerberos 和客户机知道此私用密钥，因为它从您的用户密码派生的。由于客户机已经收到了此响应，计算机将提示您输入密码。此密码被转换为一个密钥，利用它可解密认证服务器所发送的包。然后“解开”此包，并将密码和密钥从工作站的内存中删除。只要没有超过为用于获取其他票证的那个票证指定的有效期，工作站就能证明您的身份。

41.2.2 请求服务

要从网络中的任何服务器请求服务，客户机应用程序都需要向服务器证明其身份。因此，此应用程序生成一个认证器。认证器包含以下部分：

- 客户机的主体
- 客户机的 IP 地址
- 当前时间
- 校验和（由客户机选择）

所有这些信息都使用客户机为这个特殊服务器接收到的会话密钥进行了加密。用于服务器的鉴定器和票证会被发送到该服务器。该服务器使用自己的会话密钥副本来解密认证器，而该认证器为它提供所需的与请求其服务的客户机相关的所有信息，然后服务器将这些信息与票证中包含的信息进行对比。服务器将检查票证和认证器是否来自同一客户机。

如果在服务器端没有采取任何安全措施，则这一阶段是回放攻击的理想目标。某些人可能试图重发先前从网络上窃取的请求。为防止出现这种情况，服务器将不接受具有先前已收到过的时戳和票证的任何请求。此外，忽略时间戳与接收请求时的时间相差太大的请求。

41.2.3 相互鉴定

Kerberos 认证可以双向使用。这不仅是客户机是否是它所声称的那台客户机的问题。服务器本身也应能够向请求其服务的客户机认证自己。因此，它本身也将发送某种认证器。它将在客户机的鉴定器中接收的校验和加 1，然后使用它和客户机共享的会话密钥对其加密。客户机将此响应作为对服务器的真实性的校验，然后它们开始协作。

41.2.4 票证授予 — 联系所有服务器

设计票证一次用于一个服务器。这意味着您每次请求其他服务都必须获得新的票证。Kerberos 实施了一种机制来获取用于各个服务器的票证。这种服务被称为“票证授予服务”。票证授予服务与前面提到的任何服务一样，因此也使用已

介绍过的相同的访问协议。当应用程序需要一个尚未请求过的票证时，就会联系票证授予服务器。此请求包含以下部分：

- 被请求的主体
- 票证授予票证
- 认证器

与任何其他服务器一样，票证授予服务器现在将检查票证授予票证和鉴定器。如果确定它们有效，票证授予服务器将构建一个将在原始客户机和新服务器之间使用的新会话密钥。然后构建用于新服务器的票证，其中包含以下信息：

- 客户机的主体
- 服务器的主体
- 当前时间
- 客户机的 IP 地址
- 新生成的会话密钥

为新票证指派一个有效期，该有效期是票证授予票证的剩余有效期和服务的默认有效期二者中较短的一个。客户机接收此票证和会话密钥，它们是由票证授予服务发送的，但这次使用随原始票证授予票证一起提供的会话密钥来对响应进行加密。当联系新服务时，客户机可以解密此响应而不需要用户的密码。Kerberos 从而可以一个接一个地获取用于客户机的票证，而无需在登录时多次麻烦用户。

41.2.5 与 Windows 2000 的兼容性

Windows 2000 中包含了 Kerberos 5 的 Microsoft 实施。因为 SUSE Linux Enterprise® 使用 Kerberos 5 的 MIT 实现，请在 MIT 文档中寻找有用信息和指南。请参见第 41.4 节“有关详细信息”[680]。

41.3 从用户的角度讨论 Kerberos

理想情况下，用户与 Kerberos 的唯一接触是在工作站登录时发生的。登录进程包括获得一个票证授予票证。注销时，用户的 Kerberos 票证会自动损坏，这样其他人就不能模仿该用户。当用户的登录会话持续时间超过为票证授予的票证的最长时间限制时（合理的设置是 10 小时），票证的自动到期会带来一些不便因素。但用户可以通过运行 `kinit` 来获得一个新的票证授予票证。再次输入密码，Kerberos 无需其他认证即可获得对所需服务的访问。要获得由 Kerberos 为您静默获取的所有票证的列表，请运行 `klist`。

这里有一个短列表，列出了使用 Kerberos 鉴定的一些应用程序。在 `/usr/lib/mit/bin` 或 `/usr/lib/mit/sbin` 下可以找到这些应用程序。它们拥有普通 UNIX 和 Linux 应用程序的所有功能，同时具有由 Kerberos 管理的透明认证：

- `telnet`、`telnetd`
- `rlogin`
- `rsh`、`rcp`、`rshd`
- `ftp`、`ftpd`

您再也不必为了使用这些应用程序而输入密码，因为 Kerberos 已经证明了您的身份。如果在具有 Kerberos 支持的情况下进行编译，`ssh` 甚至可以将为一个工作站获得的所有票证转发到另一个工作站。如果使用 `ssh` 登录到另一个工作站，`ssh` 将确保票证的加密内容会根据新情况而调整。仅在工作站之间复制票证是不够的，因为票证中包含工作站特定信息（IP 地址）。XDM、GDM 和 KDM 也提供 Kerberos 支持。请阅读 <http://web.mit.edu/kerberos> 处的 *kerberos v5 unix 用户指南* 中有关 Kerberos 网络应用程序的更多信息。

41.4 有关详细信息

MIT Kerberos 的官方网站是 <http://web.mit.edu/kerberos>。因此，找出任何有关 Kerberos（包括 Kerberos 安装、用户和管理指南）的任何其他相关资源的链接。

<ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.PS> 处的文章提供了对 Kerberos 基本原理的十分宽泛的、非常易于理解的见识。它还提供了许多进一步研究和了解 Kerberos 的资源。

Kerberos FAQ 的官方网站是 <http://www.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html>。Brian Tung 编著的 *Kerberos — 网络鉴定系统* 一书 (ISBN 0-201-37924-4) 提供了深入和全面的信息。

对分区和文件进行加密

每个用户都有一些第三方不应能访问的机密数据。越是依赖移动计算以及在不同环境和网络中工作，就越应该小心处理数据。如果其他人可以通过网络或实际访问您的系统，建议对文件或整个分区进行加密。便携式计算机或可卸媒体（例如外部硬盘或 USB 记忆棒）有可能被盗或丢失。因此，建议对包含机密数据的文件部分进行加密。

可以通过以下几种加密方法来保护数据：

加密硬盘分区

可在安装期间或在已安装的系统中使用 YaST 创建加密分区。有关细节，请参考第 42.1.1 节“在安装过程中创建加密分区”[684]和第 42.1.2 节“在运行的系统上创建加密分区”[685]。此选项还可用于可移动媒体（如外部硬盘），如第 42.1.4 节“加密可移动媒体的内容”[686]中所述。

作为树枝创建加密文件

可以随时使用 YaST 在硬盘或可卸媒体上创建加密文件。之后可使用加密文件来储存其他文件或文件夹。有关更多信息，请参考第 42.1.3 节“作为树枝创建加密文件”[686]。

加密用户主目录

用 SUSE Linux Enterprise 还可以为用户创建加密的主目录。用户登录系统时，装入加密的用户主目录，内容对该用户可用。有关更多信息，请参考第 42.2 节“使用加密的用户主目录”[686]。

加密单个 ASCII 文本文件

如果只有少量 ASCII 文本文件存有敏感或机密数据，则可使用 vi 编辑器对这些文件逐个加密并加密保护。有关更多信息，请参考第 42.3 节“使用 vi 加密单个 ASCII 文本文件” [687]。

警告: 加密媒体提供有限的保护

本章中描述的方法仅提供有限的保护。无法保护正在运行的系统免受危害。成功装入加密媒体后，具有适当权限的所有用户都可以访问它。但是，加密媒体在计算机丢失或被窃的情况下，可以有效防止未经授权人员读取您的机密数据。

42.1 用 YaST 设置已加密的文件系统

使用 YaST 在安装期间或已安装的系统中加密分区或部分文件系统。但是，在已安装的系统中加密分区更加困难，因为必须重调整分区大小和更改现有分区。在此情况下，创建一个定义大小的加密文件来储存其他文件或部分文件系统可能更加方便。要加密整个分区，需要在分区布局中提供一个专用于加密的分区。默认情况下，YaST 的标准分区建议并不包括加密分区。请在分区对话框中手动添加此分区。

42.1.1 在安装过程中创建加密分区

警告: 密码输入

确保牢记加密分区的密码。没有这个密码，您将无法访问或恢复加密数据。

用于分区的 YaST 专家对话框提供了创建加密分区所需的选项。要创建新的加密分区，请执行以下操作：

- 1 通过系统 > 分区程序从“YaST 控制中心”运行 YaST 分区程序。
- 2 单击创建并选择一个主分区或逻辑分区。
- 3 为此分区选择所需的文件系统、大小和装入点。

- 4 如果只在必要时才装入加密文件系统，请启用 *Fstab* 选项中的不在系统启动时装入。
- 5 激活加密文件系统复选框。
- 6 单击“确定”。系统将提示您输入用于加密此分区的密码。不会显示该密码。为了避免输入错误，请输入两次密码。
- 7 单击确定完成此过程。现在已创建了新的加密分区。

除非已选中不在系统启动时装入，否则操作系统引导时将在装入分区前要求输入密码。装入分区后，此分区对所有用户都可用。

要在启动期间跳过装入加密分区，可在提示输入密码时按 **Enter** 键。然后，再次拒绝输入密码的提示。在此情况下，不装入加密文件系统，并且操作系统继续引导并阻止对您的数据的访问。

要访问引导时未装入的加密分区，请通过输入 `mount name_of_partition mount_point` 来手动装入分区。在系统提示时输入密码。完成分区装入后，使用 `umount name_of_partition` 卸载分区，以防止其他用户访问此分区。

在已存在多个分区的计算机上安装系统时，还可决定在安装期间加密现有分区。在此情况下，请遵循第 42.1.2 节“在运行的系统上创建加密分区”[685]中的描述并注意此操作将会损坏要进行加密的现有分区中的所有数据。

42.1.2 在运行的系统上创建加密分区

警告: 在运行的系统中激活加密

还可以在正在运行的系统上创建加密分区。但是，加密现有分区会损坏现有分区中的所有数据，并需要重调整现有分区的大小以及结构。

在正在运行的系统上，在“YaST 控制中心”中选择系统 > 分区。单击是继续。在 *Expert Partitioner* 中选择要加密的分区，并单击编辑。其余过程与第 42.1.1 节“在安装过程中创建加密分区”[684]中描述的过程相同。

42.1.3 作为树枝创建加密文件

除了使用分区，还可以创建特定大小的加密文件来储存包含机密数据的其他文件或文件夹。这种容器文件是从“YaST 专家分区程序”对话框中创建的。选择**加密文件**并输入该文件的完全路径及其大小。接受或更改建议的格式化设置和文件系统类型。指定装入点并确定是否应在系统引导时装入加密文件系统。

相对于加密分区，加密容器文件的优势在于可以添加加密文件而无须对硬盘进行重分区。可以借助于环路设备装入加密文件，而其行为方式与常规的分区类似。

42.1.4 加密可移动媒体的内容

YaST 将可移动媒体（如外部硬盘或 USB 闪存驱动器）当作任何其他硬盘一样处理。可按上述方法加密此类媒体中的树枝文件或分区。但是，请在 *Fstab* 选项对话框中启用**引导时不装入**，因为可移动媒体通常只在系统运行时连接。

如果已使用 YaST 对可卸设备进行了加密，KDE 和 GNOME 桌面会自动识别加密分区并在检测到该设备时提示输入密码。在运行 KDE 或 GNOME 时，如果插入 FAT 格式的可卸设备，输入密码的桌面用户自动成为设备的拥有者并可以读写文件。对于文件系统不是 FAT 的设备，请明确更改除 `root` 之外的用户的所有权，以便这些用户可以在该设备上读写文件。

42.2 使用加密的用户主目录

要防止用户主目录中的数据在被窃或硬盘被取下时丢失，请使用 YaST 用户管理模块以启用用户主目录加密。您可以为新的或现有的用户创建加密的用户主目录。要对现有用户主目录进行加密和解密，需要知道他们的登录密码。有关说明，请参见第 8.9.1 节“**用户管理**”[145]。

如第 42.1.3 节“**作为树枝创建加密文件**”[686]所述，加密主分区是在文件容器内创建的。会在 `/home` 下为每个加密用户主目录创建两个文件：

`LOGIN.img`

存放该目录的映像

`LOGIN.key`

映像密钥，受用户的登录密码保护。

登录时用户主目录会自动解密。在内部，该功能是通过 pam 模块 pam_mount 提供的。如果需要添加提供加密用户主目录的其他登录方法，必须在 `/etc/pam.d/` 中将该模块添加到相应的配置文件。有关更多信息，另请参见[第 24 章 通过 PAM 进行鉴定](#) [449] 和 pam_mount 的手册页。

警告: 安全性限制

对用户主目录加密并不能对其他用户的访问进行高度安全的防御。如果需要高度安全性，则不应物理共享该系统。

为增强安全性，请同时加密 swap 分区以及 `/tmp` 和 `/var/tmp` 目录，因为它们可能包含关键数据的临时映像。您可以按[第 42.1.1 节 “在安装过程中创建加密分区”](#) [684] 或[第 42.1.3 节 “作为树枝创建加密文件”](#) [686] 中所述，用 YaST 分区程序加密 swap、`/tmp` 和 `/var/tmp`。

42.3 使用 vi 加密单个 ASCII 文本文件

使用加密分区也有缺点，即在装入加密分区时，至少为 `root` 用户才能访问数据。要防止出现这种情况，可以在加密方式中使用 vi。

使用 `vi -x filename` 编辑新文件。vi 将提示您设置密码，然后加密文件的内容。只要您访问此文件，vi 就会要求您输入正确的密码。

要想更加安全，可以将加密文本文件放入加密分区中。建议使用此方法是因为 vi 使用的加密并不足够安全。

通过 AppArmor 限制特权

许多安全漏洞是*可信赖*程序中的错误产生的。可信赖程序运行时具有某些攻击者想获取的特权，如果程序中存在的错误导致攻击者得到了此特权，则程序丧失了可信赖性。

Novell® AppArmor 是一套应用程序安全解决方案，专门设计用于为可疑程序提供最低的特权限制。AppArmor 允许管理员指定程序可执行活动的域，方法是为该应用程序构建一个安全配置文件该程序可访问的文件列表和可执行的操作。

计算机系统的有效强化要求您将可调解特权的程序数目降至最低，然后尽可能保护程序的安全。通过 Novell AppArmor，您只需对环境中的易受攻击的程序构建配置文件，这大大减轻了对计算机进行强化所需要的工作量。AppArmor 配置文件强制执行策略，以确保程序不会执行预期操作之外的任何操作。

管理员只需注意易受攻击的应用程序并生成它们的配置文件。这样系统的强化可归结为构建和维护 AppArmor 配置文件集并监视 AppArmor 报告功能记录的策略违反或异常。

定义应用程序的 AppArmor 配置文件的构建非常直接和直观。AppArmor 销售时附有若干帮助创建配置文件的工具。您无需编程或处理脚本。需要管理员做的唯一任务是为每个需要强化的应用程序确定一个最严格访问和执行权限的策略。

只有在软件配置或所需的活动范围发生变化时才有必要更新或修改应用程序配置文件。AppArmor 提供直观的工具来处理配置文件的更新或修改。

用户完全不会觉察到 AppArmor。它在“后台”运行，无需任何用户交互操作。AppArmor 对系统性能没有明显影响。如果应用程序的某些活动没有包含在

AppArmor 配置文件中，或者应用程序的某些活动被 AppArmor 阻止，管理员必须调整此应用程序的配置文件以包括此类行为。

本指南简要介绍为了有效强化系统需要通过 AppArmor 执行的基本任务。要深入了解有关详细信息，请参见 *Novell AppArmor 管理指南*。

43.1 安装 Novell AppArmor

默认情况下，Novell AppArmor 会在每次安装 SUSE Linux Enterprise® 时来安装和运行，而忽略所安装的模式。AppArmor 的完整功能实例需要以下所列出的包

- apparmor-parser
- libapparmor
- apparmor-docs
- yast2-apparmor
- apparmor-profiles
- apparmor-utils
- 审计

43.2 启用和禁用 Novell AppArmor

默认情况下，Novell AppArmor 配置为在每次新安装 SUSE Linux Enterprise 时运行。可以通过两种方法来切换 AppArmor 状态：

使用 YaST 系统服务（运行级别）

通过在系统引导时所执行的脚本序列中去除和添加引导脚本来禁用或启用 AppArmor。状态更改会在下次系统引导时应用。

使用 Novell AppArmor 控制面板

可使用“YaST Novell AppArmor 控制面板”来通过在运行中的系统上关闭或打开 Novell AppArmor 来切换其状态。在控制面板中所执行的更改将即时应用。“控制面板”会触发 AppArmor 停止或启动事件并在系统引导序列中去除或添加它的引导脚本。

要通过从系统引导时所执行的脚本序列中去除 AppArmor 以永久禁用 AppArmor，请如下执行操作：

- 1 以 `root` 身份登录并启动 YaST。
- 2 选择 **系统 > 系统服务（运行级别）**。
- 3 选择 **专家方式**。
- 4 选择 `boot.apparmor` 并单击 **设置/重置 > 禁用服务**。
- 5 单击 **完成退出 YaST 运行级别工具**。

除非您明确重新启用 AppArmor，否则 AppArmor 在下次系统引导时将不会初始化并且保持非活动状态。使用 YaST 运行级别工具重新启用服务的操作与禁用服务的操作类似。

通过使用“AppArmor 控制面板”来在运行中的系统上切换 AppArmor 状态。应用这些更改并重引导系统后，这些更改将生效。要切换 AppArmor 的状态，请继续执行以下操作：

- 1 以 `root` 身份登录并启动 YaST。
- 2 然后选择 *Novell AppArmor > AppArmor 控制面板*。
- 3 选择 **启用 AppArmor**。要禁用 AppArmor，请取消选中此选项。
- 4 单击 **完成**以退出“AppArmor 控制面板”。

43.3 构建应用程序的配置文件入门

请仔细考虑以下事项以在系统上准备 Novell AppArmor 的成功部署：

- 1 确定要构建配置文件的应用程序。有关详细信息，请参见[第 43.3.1 节“选择要构建配置文件的应用程序”](#) [692]。
- 2 根据[第 43.3.2 节“构建和修改配置文件”](#) [693]中的简要说明构建需要的配置文件。检查结果并在必要时调整配置文件。
- 3 运行 AppArmor 报告并处理安全事件以跟踪系统上发生的事件。请参考[第 43.3.3 节“配置 Novell AppArmor 事件通知和报告”](#) [695]。

- 4 环境发生变化或者需要对 AppArmor 报告工具记录的安全事件作出反应时，更新您的配置文件。请参考 第 43.3.4 节 “更新您的配置文件” [697].

43.3.1 选择要构建配置文件的应用程序

您只需保护在您的特定设置中会受到攻击的程序，因此只需为真正运行的程序使用配置文件。使用以下列表来确定最可能的候选程序：

网络代理

具有开放网络端口的程序（服务器端和客户端）。邮件客户程序和万维网浏览器等用户客户程序也会调解权限。这些程序在运行时具有书写用户主目录的权限，而且他们会处理来自恶意远程来源的输入，如恶意的万维网网站和通过电子邮件发送的恶意代码。

万维网应用程序

万维网浏览器可以调用的程序，包括 CGI Perl 脚本、PHP 页面以及更复杂的万维网应用程序。

Cron 作业

cron 守护程序定期运行的程序可读取来自各种来源的输入。

要了解哪些进程当前以开放网络端口运行并且可能需要配置文件来进行限制，请作为 root 运行 aa-unconfined。

例 43.1 aa-unconfined 的输出

```
19848 /usr/sbin/cupsd not confined
19887 /usr/sbin/sshd not confined
19947 /usr/lib/postfix/master not confined
29205 /usr/sbin/sshd confined by '/usr/sbin/sshd (enforce)'
```

上例中标注为 not confined 的每个进程都可能需要定制的配置文件来进行限制。标注为 confined by 的进程已受 AppArmor 保护。

提示: 有关详细信息

有关选择正确的应用程序来构建配置文件的更多信息，请参见第 1.2 节 “Determining Programs to Immunize” (第 1 章 *Immunizing Programs*, ↑Novell AppArmor Administration Guide)。

43.3.2 构建和修改配置文件

SUSE Linux Enterprise 上的 Novell AppArmor 附带预配置的配置文件集，用于最重要的应用程序。除此之外，还可使用 AppArmor 来为所希望的任意应用程序创建您自己的配置文件。

管理配置文件有两种方式。一种是使用 YaST Novell AppArmor 模块提供的图形化前端，另一种是使用 AppArmor 套件自身提供的命令行工具。这两种方式的工作方式基本相同。

按第 43.3.1 节“选择要构建配置文件的应用程序”[692]中的说明运行 `aa-unconfined` 运行会确定一个可能需要配置文件以在安全模式下运行的应用程序列表。

对每个应用程序执行以下步骤以创建配置文件：

- 1 以 root 身份运行 `aa-genprof programname` 以使 AppArmor 创建应用程序配置文件的大致轮廓。

或

通过运行 `YaST > Novell AppArmor > 添加配置文件向导` 并指定要构建配置文件的应用程序的完整路径来建立基本的配置文件。

此时大致构建了一个基本的配置文件，同时 AppArmor 进入学习模式，这意味着它会记录您正在执行的程序的每个活动，但目前还不进行限制。

- 2 运行应用程序的所有操作，让 AppArmor 了解程序的每个活动。
- 3 通过在 `aa-genprof` 中输入 `S` 来使 AppArmor 分析在步骤 2 [693]中生成的日志文件。

或

通过在添加配置文件向导中单击扫描 AppArmor 事件的系统日志，然后执行向导中提示的操作直到完成配置文件来分析日志。

AppArmor 扫描在程序运行期间记录的日志，然后请求您为每个记录的事件设置访问权限。请对每个文件进行设置或使用通配。

- 4 依据应用程序的复杂性，可能必须重复 [步骤 2 \[693\]](#) 和 [步骤 3 \[693\]](#)。限制应用程序，在限制条件下执行应用程序并处理任何新的日志事件。要准确限制应用程序功能的完整范围，您可能必须经常重复此过程。
- 5 设置所有访问权限后，您的配置文件将被设置为强制模式。配置文件将被应用，AppArmor 根据刚创建的配置文件对应用程序进行限制。

如果某应用程序的现有配置文件处于提示模式，对此应用程序启动 `aa-genprof` 时，它的配置文件将在退出此学习周期后仍保留在学习模式下。有关更改配置文件模式的更多信息，请参见“`aa-complain—Entering Complain or Learning Mode`”一节（第 4 章 *Building Profiles from the Command Line*, ↑Novell AppArmor Administration Guide）和“`aa-enforce—Entering Enforce Mode`”一节（第 4 章 *Building Profiles from the Command Line*, ↑Novell AppArmor Administration Guide）。

使用您刚限制的应用程序执行您需要的每一项任务以测试您的配置文件设置。被限制的应用程序通常会顺利运行，您完全不会察觉到 AppArmor 活动。但是，如果您注意到应用程序行为失常，请检查系统日志以查看 AppArmor 对应用程序的限制是否太过严格。根据系统上所使用的日志机制，可从以下几个位置查找 AppArmor 日志条目：

`/var/log/audit/audit.log`

如果安装了 `audit` 包并且 `auditd` 正在运行，则将如下记录 AppArmor 事件：

```
type=APPARMOR msg=audit(1140325305.502:1407): REJECTING w access to
/usr/lib/firefox/update.test (firefox-bin(9469) profile
/usr/lib/firefox/firefox-bin active /usr/lib/firefox/firefox-bin)
```

`/var/log/messages`

如果未使用 `auditd`，则 AppArmor 事件会记录在 `/var/log/messages` 下的标准系统日志中。以下是示例条目：

```
Feb 22 18:29:14 dhcp-81 klogd: audit(1140661749.146:3): REJECTING w access
to /dev/console (mdnsd(3239) profile /usr/sbin/mdnsd active
/usr/sbin/mdnsd)
```

`dmesg`

如果 `auditd` 没有运行，则还可使用 `dmesg` 命令检查 AppArmor 事件：

```
audit(1140661749.146:3): REJECTING w access to /dev/console (mdnsd(3239)
profile /usr/sbin/mdnsd active /usr/sbin/mdnsd)
```

要调整配置文件，可按 [步骤 3 \[693\]](#) 所述再次分析与此应用程序相关的日志讯息。发出提示时，请确定访问权限或限制。

提示: 有关详细信息

有关配置文件构建和修改的更多信息，请参见第 2 章 *Profile Components and Syntax* (↑Novell AppArmor Administration Guide)、第 3 章 *Building and Managing Profiles with YaST* (↑Novell AppArmor Administration Guide) 和第 4 章 *Building Profiles from the Command Line* (↑Novell AppArmor Administration Guide)。

43.3.3 配置 Novell AppArmor 事件通知和报告

请在 Novell AppArmor 中设置事件通知，这样您可以查看安全性事件。事件通知是一项 Novell AppArmor 功能，可在发生所选严重性级别的系统 Novell AppArmor 活动时通知指定的电子邮件收件人。当前可在 YaST 界面中获得此功能。

要在 YaST 中设置事件通知，请执行以下操作：

- 1 确保您的系统上运行着用于传递事件通知的邮件服务器。
- 2 作为 `root` 登录并启动 YaST。然后选择 *Novell AppArmor > AppArmor 控制面板*)。
- 3 在启用安全事件通知中选择 *配置*。
- 4 为每种记录类型（*简要、汇总和详细*）设置报告频率、输入接收报告的电子邮件地址并确定要记录事件的严重性。要在事件报告中包含未知事件，请选择 *包含未知严重性的事件*。

注意: 选择要记录的事件

除非您对 AppArmor 的事件分类非常熟悉，否则选择通知所有安全级别的事件。

- 5 选择 *确定 > 完成* 退出此对话框以应用您的设置。

通过使用 Novell AppArmor 报告，您可以阅读日志文件中报告的重要 Novell AppArmor 安全事件，而不必手动筛选只对 aa-logprof 工具有用的繁杂讯息。您可以按照日期范围或程序名称对报告进行过滤，以减小报告的大小。

要配置 AppArmor 报告，请执行如下操作：

- 1 作为 `root` 登录并启动 YaST。选择 *Novell AppArmor > AppArmor 报告*。
- 2 从*执行安全摘要、应用程序审计和安全事件报告*中选择要检查或配置的报告类型。
- 3 选择*编辑*并提供请求的数据，以编辑报告生成频率、电子邮件地址、导出格式和报告位置。
- 4 要运行所选类型的报告，请单击*立即运行*。
- 5 选择*查看档案*并指定报告类型，以在给定类型的存档报告中浏览。

或

删除不需要的报告或添加新报告。

提示: 有关详细信息

有关在 Novell AppArmor 中配置事件通知的更多信息，请参见第 6.2 节“Configuring Security Event Notification” (第 6 章 *Managing Profiled Applications*, ↑Novell AppArmor Administration Guide)。可在第 6.3 节“Configuring Reports” (第 6 章 *Managing Profiled Applications*, ↑Novell AppArmor Administration Guide)中找到关于报告配置的更多信息。

43.3.4 更新您的配置文件

软件和系统配置会随着时间的流逝而更改。因此您经常需要对 AppArmor 的配置文件设置进行微调。AppArmor 会检查系统日志以查找策略违例或其他 AppArmor 事件，允许您对配置文件作相应的调整。您也可以使用[更新配置文件向导](#)解决应用程序行为超出配置文件定义的问题。

要更新配置文件集，请执行以下操作：

- 1 作为 `root` 登录并启动 YaST。
- 2 启动 *Novell AppArmor* > *更新配置文件向导*。
- 3 对于记录的任意资源或可执行文件，根据提示调整其访问或执行权限。
- 4 回答所有问题后离开 YaST。您的更改将被应用到对应的配置文件中。

提示: 有关详细信息

有关从系统日志更新配置文件的更多信息，请参见第 3.5 节 “Updating Profiles from Log Entries” (第 3 章 *Building and Managing Profiles with YaST*, ↑Novell AppArmor Administration Guide)。

安全性和机密性

Linux 或 UNIX 系统的一个主要特点就是能够同时处理多个用户（多用户），并允许这些用户在同一计算机上同时执行多项任务（多任务）。此外，操作系统对网络是透明的。用户往往不知道他们所用的数据和应用程序是他们自己的计算机本地提供的，还是通过网络提供的。

利用多用户功能时，不同用户的数据必须分开储存。要确保安全性和私密性。数据安全性早在计算机能够联网之前就已经是个关键问题。和今天一样，那时人们最担心的问题就是如何保持数据可用，即便数据丢失或是数据媒体（通常是硬盘）损坏也不受任何影响。

本节侧重说明机密性问题以及保护用户隐私的方法；但是，全面的安全观离不开一些过程，即：随时准备好定期更新、可行的和经过测试的备份副本，这一点再怎么强调都不为过。做不到这一点，您可能很难恢复数据——不仅是在出现硬件故障时，在怀疑有人未经授权访问和篡改文件时，也很难恢复数据。

44.1 本地安全和网络安全

访问数据有以下几种方式：

- 与拥有所需信息或能访问计算机数据的人进行人际交流
- 直接从计算机控制台访问（物理访问）
- 通过串行线路
- 使用网络链接

在上述所有情况下，用户只有在通过鉴定后才能访问相关资源或数据。万维网服务器在这方面可能较为宽松，但您仍不希望它向任何访问者透露您个人的所有数据。

在上面的列表中，第一种情况需要最大程度的人际互动，例如在您联系银行职员时，您需要证明自己就是银行帐号的持有人。然后您需要提供签名、PIN 或密码，来证明您就是您自己声称的那个人。有时候，有些人可能会通过提及一些大家都知道的零散信息，利用花言巧语骗取知情人的信任，诱导知情人说出机密信息。受骗人可能会被一步步地诱骗出更多信息，而自己却一直蒙在鼓里。这种手段在黑客内部称为**社会工程**。要防止受骗，您只能对人们进行教育，并且学会言辞谨慎，不轻易透露信息。在闯入计算机系统之前，攻击者通常将目标锁定在接待员、公司内的服务人员，甚至也可能是家庭成员。在很多情况下，最终发现这种利用社会工程手段发起的攻击时，通常为时已晚。

企图未经授权访问您数据的人也可能使用传统方法直接攻击您的硬件。因此，应该防止有人对计算机做手脚，让任何人都无法拆除、替换或损坏其部件。这也适用于各种备份，甚至是各种网络电缆或电线。还应保护引导过程，因为已知有些按键组合会引起异常行为。通过为 BIOS 和引导加载程序设置密码可以提供这方面的保护。

串行终端连接到串行端口，目前很多地方仍在使用这种连接方式。与网络接口不同，它们不依赖网络协议与主机通讯。通过一根缆线或是红外端口就可以在设备间发送纯字符数据。电缆本身是这种系统最薄弱的地方：连接了较旧的打印机后，很容易记录下流过电缆的数据。通过打印机做的事情也可以通过其他方式来完成，具体取决于攻击的强度。

在一台主机的本地读取文件需要一定的访问规则，这与打开网络连接访问其他主机上的服务器所需的规则不同。本地安全不同于网络安全。区别即在于：必须将数据放入包中才能发送到其他位置。

44.1.1 本地安全

关于本地安全，还要从计算机运行所在的位置的物理环境说起。在符合您的安全预期和需要的地点搭建计算机系统。本地安全的主要目标是将不同用户分隔开，防止某个用户假借其他用户的权限或身份。这是要遵守的一条基本规则，但这条规则对 `root`（根用户，对系统拥有最高权力）尤其适用。`root` 不必输入密码即具有其他任何本地用户的身份，还能够读取本地储存的所有文件。

44.1.2 密码

在 Linux 系统中，密码不是以纯文本格式储存的，而且也不能简单地将输入的文本字符串与保存的模式匹配。如果事实正好相反，只要有人取得了相应文件的访问权，就会危及系统中所有帐户的安全。所以要对储存的密码加密，并且每次输入时都要再次加密，而后对两个加密字符串进行比较。只有在无法将加密密码反向计算为原始文本字符串时，这种方式才能提高安全性。

实际上，这是通过一种特殊算法（亦称活门算法）实现的，因为该算法只能单向有效。截获加密字符串的攻击者无法通过简单地再次应用同一算法来获取您的密码。这需要测试所有可能的字符组合，直到有一种组合看似加密时的密码。对于八位字符密码，需要计算的可能组合是相当多的。

20 世纪 70 年代时，人们对这种方法是否比其他方法更安全存在争议，因为其中所用算法的计算速度相对较慢，几秒钟才能加密一个密码。而与此同时，PC 的处理能力已足够大，每秒可进行几十万次甚至是几百万次的加密。正因为这样，不应让普通用户看到加密密码（普通用户不能读取 `/etc/shadow`）。更重要的是，密码应该是不容易猜出的，以防因意外错误而暴露密码文件。因此，将“tantalize”这样的密码“转换”为“t@nt@1lz3”实际上没有任何帮助。

用相似的数字替换单词中的某些字母是不够安全的。利用字典来猜字的密码破解程序用的也是类似的替换方法。最好是编造出没有一般意义的词，即仅对您自己有意义的词，如句中各词的词首字母，或书名，如 Umberto Eco 撰写的“The Name of the Rose”。这样可以编写以下安全的密码：“TNotRbUE9”。相比之下，像“beerbuddy”或“jasmine76”这样的密码，即便是不太了解您的人也很容易猜出。

44.1.3 引导过程

配置系统，让其无法从软盘或 CD 引导；配置方法为：彻底拆除驱动器，或设置 BIOS 密码，将 BIOS 配置为只能从硬盘引导。通常，Linux 系统要通过引导加载程序来启动，这样您可以向引导内核传递更多选项。通过在 `/boot/grub/menu.lst` 中设置额外的密码可防止其他用户在引导期间使用这类参数（请参见第 18 章 [引导加载程序](#) [367]）。这对您的系统安全举足轻重。不仅内核本身以 `root` 权限运行，而且内核还是在系统启动时授予 `root` 权限的第一个权威对象。

44.1.4 文件权限

一般来说，执行某项任务时应始终尽量使用限制性最强的特权。例如，以 `root` 权限读写电子邮件是完全没有必要的。如果邮件程序有错误，攻击者则可能利用该错误，以该程序启动时所具有的权限发起攻击。如若遵守上述规则，则可以尽量减少可能的损失。

在 SUSE Linux Enterprise 分发包中包括的所有文件的权限经过了小心的选择。系统管理员在安装附加软件或其他文件时要特别小心，尤其是在设置权限位时。经验丰富且安全意识强的系统管理员始终在命令 `ls` 后使用 `-l` 选项获取详细的文件列表，这样他们可以立即检测出有错误的文件权限。错误的文件特性不仅意味着文件可能被更改或删除，`root` 还可能执行这些改过的文件；或者如果是配置文件，程序则可能以 `root` 权限使用这些文件。这使系统很容易受到攻击。这类攻击被称为布谷鸟蛋，因为程序（蛋）由另一个用户（鸟）执行（孵化），就像是布谷鸟诱骗其他鸟代其孵蛋。

SUSE Linux Enterprise 系统中的文件 `permissions`、`permissions.easy`、`permissions.secure` 和 `permissions.paranoid` 都位于 `/etc` 目录中。这些文件用于定义特殊权限（如全局可写目录），或为文件定义 `setuser ID` 位（设置了 `setuser ID` 位的程序不以启动该程序的用户的权限运行，而以文件拥有者的权限运行，这个权限多为 `root`）。管理员可以使用文件 `/etc/permissions.local` 添加自己的设置。

要定义 SUSE Linux Enterprise 的配置使用以上哪个文件来相应地设置权限，请选择 YaST 部分 [安全性和用户](#) 中的 [本地安全性](#)。要了解这一主题的详细信息，请阅读 `/etc/permissions` 中的注释，或参考 `chmod` 手册页 (`manchmod`)。

44.1.5 缓冲区溢出错误和格式字符串错误

只要程序要处理的数据可以或可能被用户更改，就应该加倍小心；但这个问题更应该是应用程序编程人员的问题而不是普通用户的问题。编程人员必须确保自己编写的应用程序以正确的方式解释数据，避免将这些数据写入内存时，因为内存区域过小而无法容纳。此外，程序应能够通过专用接口一致地传递数据。

如果写入内存缓冲区时未考虑该缓冲区的实际大小，则会发生缓冲区溢出。有时这些数据（即用户生成的数据）占用的空间会超过该缓冲区所能提供的空间。结果导致数据写出缓冲区，以致于在特定情况下，程序可能执行受用户（而不是编程人员）影响的程序顺序，而不只是处理用户数据。这种错误可能导致严重后果，特别是在使用特权执行程序时（请参见第 44.1.4 节“文件权限”[702]）。

格式字符串错误的作用方式略有不同，但同样也是用户输入导致了程序出错。多数情况下，这些编程错误会被以特殊权限执行的程序（setuid 程序和 setgid 程序）利用，这也意味着您可以通过取消这些程序的相应执行特权，来防止您的数据和系统受到这种错误的影响。同样，最好的办法是使用尽可能低的特权（请参见第 44.1.4 节“文件权限”[702]）。

鉴于缓冲区溢出错误和格式字符串错误都是与用户数据处理有关的错误，攻击者不仅可以在本地帐户具有访问权的情况下利用这些错误，还可以通过网络链接利用许多已报告的错误。因此，缓冲区溢出错误和格式字符串错误与本地安全和网络安全都有关系。

44.1.6 病毒

Linux 上确有病毒运行，这与某些人的说法正好相反。但是，已知的这些病毒是由它们的创作者为进行概念验证而发布的，目的是为证明这种技术可以发挥预期的作用。目前尚未发现上述病毒中有任何正在流行。

没有借以寄生的宿主，病毒将无法生存和传播。对于计算机病毒来说，这个“宿主”是病毒程序代码能写入的某个程序或系统中的重要储存区域（如主引导记录）。由于 Linux 支持多用户处理，所以它可以将写权限限制到特定文件，这对系统文件尤其重要。因此，以 root 权限执行一般操作无疑会增大系统受病毒感染的机率。相反，若遵循上述规则（即使用尽可能低的特权），感染病毒的机率会非常低。

除此之外，切勿在未真正了解某个因特网站点时就仓促执行其中的程序。SUSE Linux Enterprise 的 RPM 包具有加密签名，这是个数字标签，表明在生成包时已

经考虑到必要的安全措施。病毒的存在是管理员或用户缺乏必要的安全意识的典型表现，病毒使系统受到威胁，即使是设计上高度安全的系统也无法逃避。

不应将病毒和蠕虫混为一谈，后者属于全球网络的问题。蠕虫的传播不需要宿主。

44.1.7 网络安全

网络安全对于保护系统免遭外部攻击至关重要。典型的登录过程（即要求提供用户名和密码以进行用户鉴定）仍然是个本地安全问题。在通过网络登录的特定情况下，应该区分这两方面的安全问题。在实际鉴定之前发生的属于网络安全问题，之后发生的属于本地安全问题。

44.1.8 X 窗口系统和 X 鉴定

正如本文开头所述，网络透明特性是 UNIX 系统的核心特性之一。X（作为 UNIX 操作系统的窗口系统）能明显地利用这一特性。利用 X 系统，在远程主机上登录，然后启动一个图形化程序，令其随后通过网络发送并显示在您的计算机上，这个过程基本不成问题。

如果应该使用 X 服务器远程显示 X 客户机，X 服务器应该防止未经授权访问受其管理的资源（即显示）。更具体地说，必须给客户机指派特定权限。在 X 窗口系统中，有两种指派权限的方法，分别为基于主机的访问控制和基于 Cookie 的访问控制。前者依赖应该运行客户程序的主机的 IP 地址。所用的控制程序为 `xhost`。使用 `xhost` 可以将合法客户机的 IP 地址输入属于 X 服务器的小型数据库。不过，依赖 IP 地址进行鉴定不是十分安全。例如，如果另有用户在发送客户程序的主机上工作，该用户将同样能够访问 X 服务器 — 就像是有人盗取了 IP 地址。由于存在这些缺点，在此不再详述这种鉴定方法，但您可以通过 `manxhost` 了解更多相关信息。

使用基于 Cookie 的访问控制时，将生成一个只有 X 服务器和合法用户才知道的字符串，就像是某种身份证。这个 Cookie（该词并不指普通意义上的小甜饼，而是指里面有幸运签的中国幸运饼）在登录时储存在用户主目录下的文件 `.Xauthority` 中，并且可供要使用 X 服务器显示窗口的所有 X 客户机使用。用户可以使用工具 `xauth` 检查文件 `.Xauthority`。如果将 `.Xauthority` 重命名或者意外地从主目录中删除了该文件，则无法再打开任何新窗口或 X 客户机。有关 X 窗口系统安全机制的详细信息，请参见 Xsecurity 手册页 (`manXsecurity`)。

SSH（安全 shell）可用于对网络连接彻底加密并将其透明地转发给 X 服务器，而用户根本察觉不到这种加密机制。这也称为 X 转发。要实现 X 转发，需要在服务器端模拟 X 服务器，并在远程主机上为 shell 设置 DISPLAY 变量。有关 SSH 的更多详细信息，请参见 [第 40 章 SSH：安全性网络操作](#) [669]。

警告

如果不认为登录主机是安全主机，请不要使用 X 转发。在不安全的主机上启用 X 转发后，攻击者可能经由 SSH 连接通过鉴定，闯入您的 X 服务器并嗅探键盘输入之类的信息。

44.1.9 缓冲区溢出错误和格式字符串错误

如[第 44.1.5 节“缓冲区溢出错误和格式字符串错误”](#) [703]所述，缓冲区溢出错误和格式字符串错误应划归与本地安全和网络安全都有关系的问题。与这些错误的本地情况一样，若成功攻击了网络程序中的缓冲区溢出漏洞，常常可以获取 root 权限。即便不是这样，攻击者也可以利用该错误获取对非特权本地帐户的访问，以攻击系统中可能存在的其他任何漏洞。

一般来说，通过网络链接发起的针对缓冲区溢出错误和格式字符串错误的攻击当属远程攻击中最常见的形式。攻击的漏洞 — 用于攻击新发现的安全漏洞的程序 — 通常在安全邮件列表上发布。通过它们可以修补漏洞而不必了解代码的详细信息。多年来的经验表明：漏洞检测代码的存在成就了更为安全的操作系统，这显然是因为迫于压力，操作系统制造商不得不修复他们软件中的问题。在自由软件中，任何人都有权访问源代码（SUSE Linux Enterprise 提供所有可用源代码），并且任何人在发现漏洞及其漏洞检测代码后都可以提交增补程序来修复相应的错误。

44.1.10 拒绝服务

拒绝服务 (DoS) 攻击的目的是阻断某个服务器程序或甚至阻断整个系统，通过以下方式来实现阻断：使服务器过载、用垃圾包使服务器一直繁忙或利用远程缓冲区溢出。DoS 攻击往往只有一个目的：让服务不再可用。不过，一旦某个服务不再可用，通讯就易于受到中间人攻击（嗅探、TCP 连接劫持、欺骗），或发生 DNS 中毒。

44.1.11 中间人：嗅探、劫持、欺骗

一般而言，由身处通讯主机之间的攻击者发起的所有远程攻击都称为*中间人攻击*。几乎所有类型的中间人攻击都有一个共同特点，即受害人通常毫无察觉。这种攻击有多种变化形式，例如，攻击者可能会截获连接请求并自行将其转发给目标计算机。现在受害者就会在不知情的情况下与错误的主机建立连接，因为连接的这一端伪装为合法的目标计算机。

最简单的中间人攻击的形式称为*嗅探* — 攻击者“只是”监听通过网络传递的数据流。更为复杂的“中间人攻击”可能会试图接管已经建立的连接（劫持）。劫持之前，攻击者需要一段时间对数据包进行分析，以便能够推测出属于该连接的 TCP 顺序号。在攻击者最终夺取目标主机的角色后，受害人会注意到这一点，因为他们会收到一条错误讯息，说明连接因失败而终止。由于有些协议没有通过加密来预防劫持，只是在建立连接后执行简单的鉴定过程，这给攻击者创造了可乘之机。

欺骗类型的攻击是对数据包进行修改，使其包含虚假的源数据（通常是 IP 地址）。多数较活跃的攻击都依赖于发送这种虚假数据包 — 在 Linux 计算机上，发送包的任务只能由超级用户 (root) 执行。

上述很多攻击都是与 DoS 同时进行的。一旦攻击者发现有机会让某台主机突然宕机，即便是很短的时间，攻击者也容易发起猛烈攻击，因为主机将在一段时间内无法对抗攻击。

44.1.12 DNS 中毒

DNS 中毒指的是通过向 DNS 服务器回复伪造的 DNS 回复包，试图让该服务器向请求其发送信息的受害者发送特定数据，以此破坏 DNS 服务器的超速缓存。许多服务器都基于 IP 地址或主机名与其他主机保持信任关系。攻击者需要非常熟悉主机之间信任关系的实际结构，才能将自己伪装为受信主机之一。通常，攻击者会分析一些从服务器接收的包，获取必要信息。攻击者还常常需要对名称服务器适时发动 DoS 攻击。您可以使用加密连接，通过对要连接的主机的身份进行校验来保护自己。

44.1.13 蠕虫

蠕虫经常被误认为是病毒，但两者有着明显的区别。不同于病毒，蠕虫无需感染某个要寄生的主机程序。它们的特点就是尽快在网络结构中传播。以往的蠕虫，如 Ramen、Lion 或 Adore，全都利用 bind8 或 lprNG 之类的服务器程序中的已知安全漏洞。蠕虫的预防相对简单。鉴于在发现安全漏洞和蠕虫对服务器发起攻击之间有一段时间，很有可能及时提供受影响的程序的更新版本。只有管理员确实在受感染系统上安装了安全更新程序时，这种方法才有用。

44.2 一些常用的安全提示和技巧

要有效处理安全问题，关键在于随时关注安全方面的新动态并了解最新的安全问题。要保护您的系统免受各种问题的侵扰，最好的方式就是尽快获取并安装安全公告推荐的更新软件包。SUSE 使用邮件列表发布安全公告，您可以通过链接 <http://en.opensuse.org/Communicate/Mailinglists> 订阅该邮件列表。列表提供关于更新软件包的第一手信息，向其积极投稿的人当中还有 SUSE 安全小组的成员。 opensuse-security-announce@opensuse.org

邮件列表 opensuse-security@opensuse.org 提供了一个不错的论坛，可以在其中讨论任何相关的安全问题。在同一万维网网页上订阅该邮件列表。

bugtraq@securityfocus.com 是全球知名的安全邮件列表之一。建议阅读此列表，该列表每天要接收 15 到 20 条投递信息。有关详细信息，请参见 <http://www.securityfocus.com>。

下面是一些规则，可能有助于您处理基本的安全问题：

- 根据要对每个作业都尽量使用限制性最强的一组权限的规则，应避免使用 root 权限执行常规作业。这样即可降低受布谷鸟蛋或病毒攻击的风险，防止您自己犯错误。
- 如果可能，应尽量使用加密连接在远程计算机上工作。用 ssh（安全 shell）替代 telnet、ftp、rsh 和 rlogin，这应是标准做法。
- 避免使用仅基于 IP 地址的鉴定方法。

- 尽量使最重要的网络相关包保持最新，并且订阅相应的邮件列表，以接收这些程序（如 `bind`、`postfix`、`ssh` 等）的最新版本的声明。该做法同样适用于与本地安全相关的软件。
- 更改 `/etc/permissions` 文件，优化对系统安全至关重要的文件的权限。如果删除某个程序的 `setuid` 位，该程序很可能无法再正常执行作业。但从另一方面考虑，在多数情况下，该程序也将不再是个潜在的安全隐患。所以，您可以对全局可写目录和文件采取相同的做法。
- 禁用不是绝对需要的所有网络服务，以便服务器正常运行。这样可以让系统更加安全。使用程序 `netstat` 可以找到套接状态为 `LISTEN` 的打开端口。至于选项，建议使用 `netstat-ap` 或 `netstat-anp`。 `-p` 选项允许您查看哪个进程正以什么名称占用端口。

将 `netstat` 的结果与在主机外部执行的彻底端口扫描的结果进行比较。最适合执行这项作业的程序当属 `nmap`，该程序不仅可以检测计算机的端口，而且可以对哪些服务正等待端口处理作出一些判断。不过，端口扫描可能被认为是一种入侵行为，所以不要在未经管理员明确批准的情况下在主机上执行该操作。最后，要记住不仅要扫描 `TCP` 端口，而且要扫描 `UDP` 端口（使用选项 `-sS` 和 `-sU`），这一点至关重要。

- 要以可靠方式监视系统文件的完整性，请使用 `SUSE Linux Enterprise` 提供的程序 `AIDE`（高级入侵检测环境）。对 `AIDE` 创建的数据库加密，防止有人篡改。此外，在其他计算机上保留此数据库的备份副本，储存该副本的外部数据媒体不能通过网络链接连接到您的计算机。
- 安装任何第三方软件时都要小心谨慎。曾经有黑客在安全软件包的 `tar` 档案中嵌入了特洛伊木马病毒，不过幸好发现得及时。如果安装二进制软件包，则应确保下载站点是安全的。

`SUSE` 的 `RPM` 包都具有 `gpg` 签名。`SUSE` 使用以下密钥来签名：

```
ID:9C800ACA 2000-10-19 SUSE Package Signing Key <build@suse.de>
Key fingerprint = 79C1 79B2 E1C8 20C1 890F 9994 A84E DAE8 9C80 0ACA
```

命令 `rpm--checksig package.rpm` 显示校验和及未安装软件包的签名是否正确。可以在本版本的第一张 `CD` 上和全球多数密钥服务器上找到该密钥。

- 定期检查用户和系统文件的备份副本。考虑如果不测试备份是否有效，实际上它可能毫无价值。

- 检查日志文件。尽可能编写小型脚本搜索可疑项。无可否认，这并不是是一项非常烦琐的任务。最终，只有您才知道哪些项异常，哪些项正常。
- 使用 `tcp_wrapper` 限制访问计算机上运行的各个服务，这样您可以明确控制哪个 IP 地址可以连接到某个服务。有关 `tcp_wrapper` 的进一步信息，请参见 `tcpd` 和 `hosts_access` 的手册页（`man8 tcpd`、`manhosts_access`）。
- 使用 `SuSEfirewall` 可以增强 `tcpd` (`tcp_wrapper`) 提供的安全性。
- 设计具有冗余性的安全性对策，看到两次讯息总比没看到讯息好。

44.3 使用中央安全报告地址

如果您发现与安全有关的问题（请首先检查可用的更新软件包），请向 security@suse.de 发送电子邮件。请提供问题的详细说明以及涉及的软件包的版本号。SUSE 将尽快给予答复。建议您对电子邮件讯息进行 `pgp` 加密。SUSE 的 `pgp` 密钥为：

```
ID:3D25D3D9 1999-03-06 SUSE Security Team <security@suse.de>  
Key fingerprint = 73 5F 2E 99 DF DB 94 C4 8F 5A A3 AE AF 22 F2 D5
```

也可以从 <http://www.novell.com/linux/security/securitysupport.html> 下载该密钥。

部分 VI. 查错

帮助和文档

SUSE Linux Enterprise® 附带各种信息和文档源。通过 SUSE 帮助中心，您可以对系统中最重要文档资源进行集中访问，而且还可以进行搜索。这些资源包括所安装的应用程序的联机帮助；硬件和软件主题的手册页、信息页、数据库；以及随本产品提供的所有手册。

45.1 使用 SUSE 帮助中心

首次从主菜单（*SuSE 帮助中心*）或使用 shell 中的 `susehelp` 命令启动 SUSE 帮助中心时，将显示如图 45.1 “SUSE 帮助中心的主窗口” [714] 中所示的窗口。该对话框窗口包含三个主要区域：

菜单栏和工具栏

菜单栏提供主要的编辑、导航和配置选项。文件包含用于打印当前显示的内容的选项。在编辑下，可访问搜索功能。转至包含所有可用的导航：目录（帮助中心主页）、后退、前进和最后一个搜索结果。通过设置> 构建搜索索引，可以为所有选定信息源生成搜索索引。工具栏包含三个导航图标（前进、后退、主页），一个用于打印当前内容的打印机图标。

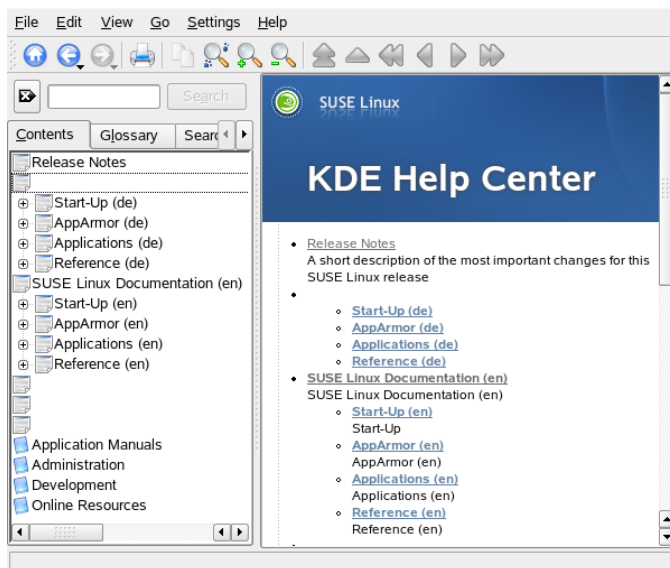
带有选项卡的导航区域

窗口左侧的导航区域有一个字段，用户可在选定的信息源中快速搜索在该字段中输入的内容。有关搜索的细节和在搜索选项卡中配置搜索功能的细节，请参见第 45.1.2 节 “搜索功能” [715]。目录选项卡以树结构显示了所有可用的和当前已安装的信息源。单击书图标可打开并浏览单个类别。

查看窗口

视图窗口始终显示当前选定的内容，如联机手册、搜索结果或万维网网页。

图 45.1 SUSE 帮助中心的主窗口



注意: 语言选择视图

SUSE 帮助中心中可用的文档取决于当前语言。更改语言后，树视图会发生变化。

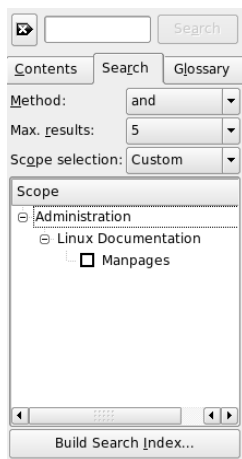
45.1.1 内容

通过 SUSE 帮助中心可以访问各种来源的有用信息。它包含用于 SUSE Linux Enterprise (*Start-Up*、*KDE 用户指南*、*GNOME 用户指南* 及 *Reference*) 的特殊文档、所有适用于工作站环境的信息源、已安装程序的联机帮助以及其他应用程序的帮助文本。此外，SUSE 帮助中心还提供对 SUSE 联机数据库的访问，这些数据库中包含 SUSE Linux Enterprise 的特殊硬件和软件问题。只要生成搜索索引，就可以轻松地搜索所有这些信息源。

45.1.2 搜索功能

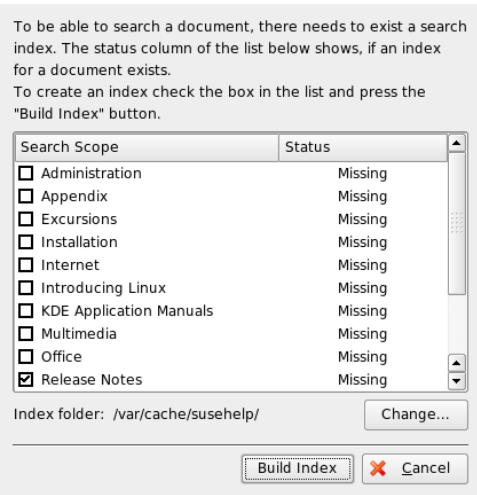
要搜索 SUSE Linux Enterprise 的所有已安装的信息源，需要生成一个搜索索引并设置许多搜索参数。为此，请打开搜索选项卡，如图 45.2 “配置搜索功能” [715]所示。

图 45.2 配置搜索功能



如果以前未生成搜索索引，那么当您单击搜索选项卡或输入搜索字符串然后单击搜索时，系统会自动提示您生成搜索索引。在用于生成搜索索引的窗口中（如图 45.3 “生成搜索索引” [716]所示），使用复选框确定要建立索引的信息源。当您通过构建索引退出对话框后，将生成索引。

图 45.3 生成搜索索引



要尽可能精确地限制搜索基数和搜索结果列表，请使用三个下拉菜单，确定显示的结果个数以及要搜索的信息源选择区域。下列选项可用来确定选择区域：

默认

搜索预定义的源选择内容。

所有

搜索全部源。

无

未选择任何要搜索的源。

自定义

通过在概述中选中各自相应的复选框来确定要搜索的源。

完成搜索配置后，单击搜索。相关的项目随即显示在视图窗口中，您只需用鼠标单击它们即可查看这些内容。

45.2 手册页

手册页是任何 Linux 系统的基本组成部分。它们介绍命令的用法以及所有可用的选项和参数。手册页如 [表 45.1 “手册页 — 类别和描述”](#) [717] 所示按类别进行排序（取自 `man` 命令本身的手册页）。

表 45.1 手册页 — 类别和描述

号码	说明
1	可执行程序或 shell 命令
2	系统调用（内核提供的函数）
3	库调用（程序库内的函数）
4	特殊文件（通常位于 <code>/dev</code> ）
5	文件格式和约定（ <code>/etc/fstab</code> ）
6	游戏
7	其他（包括宏软件包和约定），如 <code>man(7)</code> 、 <code>groff(7)</code>
8	系统管理命令（通常只用于 <code>root</code> 用户）
9	内核例程（非标准）

通常，手册页都是随关联的命令提供的。可以在帮助中心或者直接在 shell 中浏览手册页。要在 shell 中显示手册页，请使用 `man` 命令。例如，要显示 `ls` 的手册页，请输入 `man ls`。每个手册页包括标为 *NAME*、*SYNOPSIS*、*DESCRIPTION*、*SEE ALSO*、*LICENSING* 和 *AUTHOR* 的几个部分。根据具体的命令类型，可能还有其他部分。使用 `Q` 可退出手册页查看器。

另外一种显示手册页的方法是使用 Konqueror。例如，启动 Konqueror 并键入 `man:/ls`。如果某个命令具有多个不同的类别，Konqueror 会将这些类别显示为链接。

45.3 信息页

信息页是系统上另一个重要的信息来源。它们通常比手册页更为详细。可以使用信息浏览器浏览信息页并显示不同的部分（称作“节点”）。“”使用 `info` 命令可完成此任务。例如，要查看 `info` 命令本身的信息页，请在 shell 中输入 `info info`。

更加方便的方法是使用帮助中心或 Konqueror。启动 Konqueror 并键入 `info:/` 以查看顶级内容。要显示 `grep` 的信息页，请键入 `info:/grep`。

45.4 Linux 文档计划

Linux 文档计划 (The Linux Documentation Project, TLDP) 由一组编写 Linux 和 Linux 相关文档的自愿者负责管理（请参见 <http://www.tldp.org>）。这套文档包括初学者教程，但主要侧重于有经验的用户和职业系统管理员。TLDP 以免费许可的形式发布 HOWTO、常见问题和指南（手册）。

45.4.1 HOWTO

HOWTO 通常是指导完成特定任务的简短、非正式的分步指南。它是由专家为非专家以程序性的方式编写的。例如，如何配置 DHCP 服务器。HOWTO 位于 `howto` 软件包中，安装在 `/usr/share/doc/howto` 之下

45.4.2 常见问题

FAQ（常见问题）是一系列问题和解答。它们来自 Usenet 新闻组，该新闻组的目的是减少连续重复粘贴相同基本问题的情况。

45.5 Wikipedia：免费的联机百科全书

Wikipedia 是“供任何人阅读和编辑的多语种百科全书”（请参见 <http://en.wikipedia.org>）。Wikipedia 的内容由其用户创建，以免费许可 (GFDL) 的形式发布。任何访问者均可编辑文章，虽然这存在恶意删改的危险，但并没

有让访问者望而止步。它包含四十多万篇文章，您几乎可以找到任何主题的答案。

45.6 指南和手册

对于 Linux 主题，有范围广泛的指南和手册可用。

45.6.1 SUSE 手册

SUSE 提供详细的参考手册。我们以不同的语言提供了这些手册的 HTML 和 PDF 版本。可在 DVD 的目录 `docu` 中找到 PDF 文件。对于 HTML，请安装包 `opensuse-manual_LANG`（将 *lang* 替换为您首选的语言。）安装后，您可在 SUSE 帮助中心中找到它们。

45.6.2 其他手册

SUSE 帮助中心为各种主题或程序提供了其他手册和指南。有关详细信息，请参见<http://www.tldp.org/guides.html>。其中包括 *Bash Guide for Beginners*（Bash 初学者指南）、*Linux Filesystem Hierarchy*（Linux 文件系统层次）和 *Linux Administrator's Security Guide*（Linux 管理员安全指南）。指南通常比 HOWTO 或常见问题更为详尽。它们一般是由专家为专家编写的。其中一些手册虽然比较早，但仍然有效。使用 YaST 可安装手册和指南。

45.7 包文档

如果您在系统中安装包，则将创建目录 `/usr/share/doc/packages/packagename`。您可以从包维护程序查找文件以及从 SUSE 中查找其他信息。有时也有示例、配置文件、其他脚本等等可用。通常您可以找到以下文件，但是它们并不是标准的，并且有时不是所有文件都可用。

AUTHORS

此包的主要开发人员列表（通常也包含他们执行的任务）。

错误

此包的已知错误或故障。通常，它还包含到 Bugzilla 万维网网页的链接，您可以在该页面上搜索所有错误。

CHANGES , ChangeLog

每个版本的更改摘要。通常开发人员会对此感兴趣，因为它非常详细。

COPYING , LICENSE

许可信息。

常见问题

从邮件列表或新闻组收集的问题和回答。

INSTALL

在系统中安装此包的过程。通常您不需要此文件，因为您已安装了包。

README , README.*

有关如何使用该包和使用此包能够执行的操作等等的常规信息。

要执行的操作

尚未实施但是将来可能要实施的操作。

MANIFEST

带有简述的文件列表。

NEWS

描述此版本中的新增内容。

45.8 Usenet

Usenet 在因特网出现之前的 1979 年建立，它是最早的计算机网络之一，现在仍在使用。Usenet 文章的格式和传输方式与电子邮件非常相似，但它是为多对多通信而开发的。

Usenet 分为七个主题类别：comp.*计算机关联话题，misc.*其他主题，news.*新闻组关联话题rec.*消遣与娱乐，sci.*科技关联话题，soc.*社会话题，talk.*各种热点话题。顶级内容分为子组。例如，comp.os.linux.hardware 是 Linux 特定硬件问题的新闻组。

在张贴文章之前，将客户端连接到新闻服务器，然后订阅特定的新闻组。新闻客户端包括 Knode 或 Evolution。每个新闻服务器都与其他新闻服务器进行通信，与它们交换文章。您的新闻服务器可能没有包括所有新闻组。

Linux 用户的兴趣新闻组是 comp.os.linux.apps、comp.os.linux.questions 和 Comp.os.linux.hardware。如果您无法找到特定的新闻组，请访问 <http://www.linux.org/docs/usenetlinux.html>。按照 <http://www.faqs.org/faqs/usenet/posting-rules/part1/> 联机提供的 Usenet 一般规则进行操作。

45.9 标准和规范

有很多信息源都提供有关标准和规范的信息。

<http://www.linuxbase.org>

自由标准组织 (Free Standards Group) 是一个独立的旨在促进自由软件和开放源代码软件发布的非营利组织。该组织致力于制定独立于各版本的标准，以期实现上述目标。包括重要的 LSB (Linux Standard Base, Linux 标准库) 在内的若干标准均由该组织负责维护。

<http://www.w3.org>

万维网联合会 (World Wide Web Consortium, W3C) 当属最知名的标准化组织之一。该组织由 Tim Berners-Lee 在 1994 年 10 月创办，主要致力于万维网技术的标准化。W3C 提倡发布开放、不受许可证限制并且与制造商无关的规范，如 HTML、XHTML 和 XML。这些万维网标准由多个工作组分四个阶段完成，最后以 W3C 建议 (REC) 的形式公诸于世。

<http://www.oasis-open.org>

OASIS (Organization for the Advancement of Structured Information Standards, 结构化信息标准促进组织) 是一个国际联盟，专门负责开发万维网安全、电子商务、交易事务处理、物流和多个市场之间的互操作性等方面的标准。

<http://www.ietf.org>

因特网工程任务组 (Internet Engineering Task Force, IETF) 是一个十分活跃的国际合作组织，由众多研究人员、网络设计人员、供应商和用户组成。该组织侧重于开发因特网体系结构以及借助协议确保因特网平稳运行。

每个 IETF 标准均作为 RFC (Request for Comments, 请求注释) 发布，并且免费提供。RFC 有六种类型：推荐标准、草案标准、因特网标准、实验标

准、信息文档和历史标准。从狭义上讲，只有前三种（建议、草拟和完整标准）才属于 IETF 标准（请参见 <http://www.ietf.org/rfc/rfc1796.txt>）。

<http://www.ieee.org>

电气与电子工程师协会 (Institute of Electrical and Electronics Engineers, IEEE) 是负责在信息技术、电信、医药保健、运输和其他领域内制定标准的组织。IEEE 标准需付费才可获得。

<http://www.iso.org>

ISO (International Organization for Standards, 国际标准化组织) 委员会是全球最大的标准开发组织，负责维护由 140 多个国家/地区的国家/地区标准化协会构成的庞大网络。ISO 标准需付费才可获得。

<http://www.din.de> , <http://www.din.com>

德国标准化协会 (Deutsches Institut für Normung, DIN) 是经注册的科技领域内的协会。DIN 宣称该组织是“负责德国标准化的协会，并且在全球和欧洲标准化组织中代表德国的利益”。“”

该协会汇集了制造商、客户、贸易专业组织、服务公司、科学家和其他对制定标准有兴趣的人员。该协会制定的标准需付费才可获得，可通过 DIN 主页订购。

常见问题及其解决方案

本章将介绍可能发生的一些常见问题，并尽可能涵盖各种潜在的问题类型。另外，即使您所遇到的情况未在本章中列出，也可以找到类似的问题，这应该足以提供解决问题的提示。

46.1 查找和收集信息

Linux 会记录大量的详细信息。在您使用系统遇到问题时，有几个地方可以查看，大多数是 SUSE Linux Enterprise 系统的标准问题，有一些是特定于系统的问题。多数日志文件也可以用 YaST（*其他 > 启动日志*）查看。

YaST 可提供支持团队所需的所有系统信息。使用 *其他 > 支持查询*。选择有问题的类别。当所有信息都被集合后，将其附加在您的支持请求。

以下是一个列表，其中是最常用到的日志文件及其通常所包含的内容。

表 46.1 日志文件

日志文件	说明
<code>/var/log/boot.msg</code>	引导期间来自内核的讯息。
<code>/var/log/mail.*</code>	来自邮件系统的讯息。
<code>/var/log/messages</code>	运行时来自内核和系统日志守护程序的讯息。

日志文件	说明
/var/log/ NetworkManager	NetworkManager 的日志文件，用于收集网络连接性问题
/var/log/SaX.log	来自 SaX 屏幕和 KVM 系统的硬件讯息。
/home/user/ .xsession-errors	来自当前运行的桌面应用程序的讯息。请将 <i>user</i> 替换为实际用户名。
/var/log/warn	所有来自内核与系统日志守护程序的讯息被指定为“警告”级别或更高级别。
/var/log/wtmp	包含当前机器会话的用户登录记录的二进制文件。可使用 <code>last</code> 查看它。
/var/log/Xorg.*.log	来自 X Windows 系统的各种启动和运行时日志。在调试失败的 X 启动时，该日志很有用。
/var/log/YaST2/	包含 YaST 的操作及其结果的目录。
/var/log/samba/	包含 Samba 服务器及客户机日志讯息的目录。

除了日志文件外，您的计算机还可提供关于运行中的系统的信息。请参见[表 46.2: 系统信息](#)。

表 46.2 系统信息

文件	说明
/proc/cpuinfo	此选项显示处理器信息，包括处理器类型、制造商、型号和性能。
/proc/dma	此选项显示当前使用的 DMA 通道。
/proc/interrupts	此选项显示正在使用的中断和已使用的中断数量。

文件	说明
/proc/iomem	此选项显示 I/O（输入/输出）内存的状态。
/proc/ioports	此选项显示当时正在使用的 I/O 端口。
/proc/meminfo	此选项显示内存状态。
/proc/modules	此选项显示各个模块。
/proc/mounts	此选项显示当前装入的设备。
/proc/partitions	此选项显示所有硬盘的分区。
/proc/version	此选项显示当前的 Linux 版本。

Linux 带有一些用于系统分析和监视的工具。请参阅[第 14 章 系统监视实用程序 \[299\]](#)以选择在系统诊断中使用的最重要的工具。

以下包含的每个方案，都以一个描述问题的标题开头，后面是一、两段内容，提供建议的解决方案、解决方案详细信息的参考，以及对其他可能相关的方案的交叉引用。

46.2 安装问题

安装问题是指机器无法进行安装的情况。一种可能是完全无法进行安装，另一种是无法启动图形安装程序。本节将着重介绍几个您可能会遇到的典型问题，并提供可行的解决方案或针对此种情况的变通方案。

46.2.1 检查媒体

如果您使用 SUSE Linux Enterprise 安装媒体时遇到任何问题，可用软件>，媒体检查检查安装媒体的完整性。您自行烧录的媒体更容易发生媒体问题。要检查 SUSE Linux Enterprise CD 或 DVD，请将媒体插入驱动器，单击开始让 YaST 检查媒体的 MD5 校验和。这可能要花几分钟时间。如果检测到有任何错误，则不应使用此媒体进行安装。

46.2.2 硬件信息

使用 **硬件 > 硬件信息** 显示检测到的硬件和技术数据。单击树的任意节点以获取有关设备的更多信息。在提交需要硬件信息的支持请求等时，此模块特别有用。

单击 **保存到文件** 将显示的硬件信息保存到文件。选择需要的目录和文件名，然后单击 **保存** 以创建文件。

46.2.3 没有可用于引导的 CD-ROM 驱动器

如果您的计算机没有可引导的 CD-ROM 或 DVD-ROM 驱动器，或者 Linux 不支持您的驱动器，则有几类无需内置 CD 或 DVD 驱动器便可安装机器的方法：

从软盘引导

创建一张引导软盘，然后从软盘而非 CD 或 DVD 引导。

使用外置的引导设备

如果它受机器的 BIOS 和安装内核支持，就可从外置 CD 或 DVD 驱动器引导安装。

通过 PXE 进行网络引导

如果机器没有 CD 或 DVD 驱动器，但是提供了有效的以太网连接，则可以执行完全基于网络的安装。详情请参阅第 4.1.3 节“通过 VNC—PXE Boot 和“网络唤醒”进行远程安装” [40] 和第 4.1.6 节“通过 SSH—PXE Boot 和“网络唤醒”进行远程安装” [44]。

从软盘引导 (SYSLINUX)

在某些较老的计算机上，没有可用于引导的 CD-ROM 驱动器，但有软盘驱动器。要在此类系统上安装，需要创建引导磁盘，然后使用引导磁盘引导系统。

引导磁盘包括装载程序 SYSLINUX 和程序 linuxrc。SYSLINUX 支持在引导过程中选择内核以及指定所使用的硬件所需的任何参数。程序 linuxrc 支持为您的硬件装载内核模块并随后启动安装。

在从引导磁盘引导时，引导过程由引导加载程序 SYSLINUX (syslinux 包) 启动。当引导系统时，SYSLINUX 运行最小硬件检测，主要由以下步骤组成：

1. 该程序将检查 BIOS 是否提供符合 VESA 2.0 标准的帧缓冲支持并相应地引导内核。
2. 读取监视数据（DDC 信息）。
3. 读取第一个硬盘的第一个块 (MBR) 以在引导加载程序配置过程中将 BIOS ID 映射到 Linux 设备名。程序将尝试通过 BIOS 的 lba32 功能读取块以确定 BIOS 是否支持这些功能。

如果在 SYSLINUX 启动时按住 Shift 键，则将跳过所有这些步骤。出于查错的目的，请将行

```
verbose 1
```

插入 `syslinux.cfg` 中，以便引导加载程序显示当前正在执行哪个操作。

如果不能从软盘引导计算机，则可能需要将 BIOS 中的引导顺序更改为 A, C, CDROM。

外置引导设备

支持大多数 CD-ROM 驱动器。如果从 CD-ROM 驱动器引导时发生问题，请尝试使用 CD 集的 CD 2 引导。

如果系统没有 CD-ROM 或软盘驱动器，仍有希望使用通过 USB、FireWare 或 SCSI 连接的外置 CD-ROM 来引导系统。这主要取决于 BIOS 与所使用硬件的交互。如果遇到问题，有时执行 BIOS 更新可能会有用。

46.2.4 从安装媒体引导失败

无法引导机器以进行安装有两种可能的原因：

CD 或 DVD-ROM 驱动器无法读取引导映像

您的 CD-ROM 驱动器可能无法读取 CD 1 上的引导映像。在这种情况下，请使用 CD 2 来引导系统。CD 2 中包含了传统的 2.88 MB 引导映像，即使是不受支持的驱动器也能够读取该映像，该 CD 还允许您通过[第 4 章 远程安装](#) [37]中介绍的方法来执行网络安装。

BIOS 中的引导顺序不正确

BIOS 引导顺序中 CD-ROM 集必须设为第一引导项。否则机器将尝试从其他媒体引导，通常为硬盘。关于更改 BIOS 引导顺序的指导可在随主板提供的文档中找到，也可以参阅以下段落。

BIOS 是实现计算机最基本功能的软件。主板厂商提供专门为他们硬件设计的 BIOS。通常，BIOS 设置只能在一个特定时间（计算机引导时）访问。在此初始化阶段，计算机执行若干诊断硬件测试。其中一项测试就是内存检查，由内存计数器指示。当显示计数器时，请查找一行（通常在计数器下面，有时也在底部），该行提到要访问 BIOS 设置需要按的键。通常，要按的键是 Del 键、F1 键或 Esc 键。按此键，直到出现 BIOS 设置屏幕。

过程 46.1 更改 BIOS 引导顺序

- 1 使用由引导例程声明的适当键输入 BIOS，然后等待 BIOS 屏幕出现。
- 2 若要更改 AWARD BIOS 中的引导顺序，请查找 *BIOS FEATURES SETUP* 项。其他制造商可能对该项使用不同的名称，例如 *ADVANCED CMOS SETUP*。当您找到该项后，将其选中并按 Enter 键确认。
- 3 在所打开的屏幕中，查找名为 *BOOT SEQUENCE* 的子项。引导顺序通常被设置为 C, A 或 A, C 等。在前一种情况中，计算机首先搜索硬盘 (C)，然后搜索软盘驱动器 (A) 以查找可引导媒体。通过按 PgUp 键或 PgDown 键更改设置，直到顺序为 A、CDROM 和 C。
- 4 通过按 Esc 键离开 BIOS 设置屏幕。若要保存更改，请选择 *SAVE & EXIT SETUP* 或按 F10 键。若要确认应保存设置，按 Y 键。

过程 46.2 更改 SCSI BIOS (Adaptec 主机适配器) 中的引导顺序

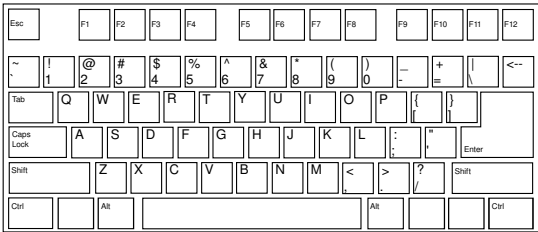
- 1 按 Ctrl + A 打开设置。
- 2 然后选择磁盘实用程序，其中将显示已连接的硬件。

记下您 CD-ROM 驱动器的 SCSI ID。
- 3 按 ESC 退出菜单。
- 4 打开配置适配器设置。在其他选项下，选择引导设备选项，然后按 Enter 键。

- 5 输入 CD-ROM 驱动器的 ID，然后再次按 Enter 键。
- 6 按 Esc 键两次以返回到 SCSI BIOS 的开始屏幕。
- 7 退出此屏幕，并确认是以引导计算机。

无论最终安装将使用何种语言及键盘布局，大多数 BIOS 配置使用下图所示的美式键盘布局：

图 46.1 美式键盘布局



46.2.5 无法引导

某些硬件类型（主要是过旧或非常新的硬件）可能无法安装。在许多情况下，可能由于从安装内核中丢失的此类硬件的支持或由该内核中包含的某些功能（如 ACPI，它会在某些硬件上引起问题）而引起的。

如果系统无法使用第一个安装引导屏幕上的标准安装方式进行安装，请尝试使用以下方法：

- 1 将第一张 CD 或 DVD 留在 CD-ROM 驱动器中，然后使用 Ctrl + Alt + Del 组合键或硬件重置按钮重引导计算机。
- 2 在出现引导屏幕时，使用键盘上的箭头键浏览至安装—禁用 ACPI，然后按 Enter 键启动引导和安装过程。此选项将禁用对 ACPI 电源管理技术的支持。
- 3 按第 3 章 使用 YaST 进行安装 [17]中所述的步骤进行安装。

如果这失败，请按照以上步骤继续，但应选择安装—安全设置。此选项将禁用 ACPI 和 DMA 支持。大多数硬件应使用此选项引导。

如果以上两个选项都失败，请使用引导选项提示向安装内核传递支持此硬件类型所需的任何其他参数。关于可用作引导选项的参数的更多信息，请参阅 `/usr/src/linux/Documentation/kernel-parameters.txt` 中的内核文档。

提示: 获取内核文档

安装 `kernel-source` 包以查看内核文档。

在引导安装之前，还有各种其他与 ACPI 相关的内核参数可在引导提示处输入：

`acpi=off`

此参数禁用计算机上的整个 ACPI 子系统。如果您的计算机根本不能处理 ACPI 或如果您认为是计算机中的 ACPI 导致问题的产生，则可以使用此参数。

`acpi=force`

始终启用 ACPI，即使计算机使用的是 2000 年以前的 BIOS。如果除了 `acpi=off` 之外还设置了此参数，则此参数将启用 ACPI。

`acpi=noirq`

不要将 ACPI 用于 IRQ 路由。

`acpi=ht`

只运行足够的 ACPI 来启用超线程。

`acpi=strict`

降低对不严格遵循 ACPI 规格的平台容许度。

`pci=noacpi`

禁用新 ACPI 系统的 PCI IRQ 路由。

`pnpacpi=off`

此选项用于您的 BIOS 设置包含错误中断或端口时发生的串行或并行问题。

`notsc`

禁用时戳计数器。此选项可用于解决系统上的计时问题。这是个新功能，如果在您的计算机上发现性能下降，尤其是与时间相关的性能下降，甚至是整个挂起，则值得尝试使用该选项。

`nohz=off`

禁用 `nohz` 功能。如果您的计算机挂起，则此选项可能有帮助。通常不需要此选项。

一旦确定了正确的参数组合，YaST 会自动将其写入引导加载程序配置中以确保系统下一次能够正确引导。

如果在装载内核或安装过程中出现无法解释的错误，则在引导菜单中选择 *内存测试* 以检查内存。如果 *内存测试* 返回一个错误，则通常这是硬件错误。

46.2.6 无法启动图形安装程序

在将第一张 CD 或 DVD 插入驱动器并重引导计算机之后，出现安装屏幕，但是在选择安装之后，图形安装程序没有启动。

有多种方法可解决此情况：

- 尝试为安装对话框另选一种屏幕分辨率。
- 选择文本方式进行安装。
- 使用图形安装程序进行远程安装（通过 VNC）。

要切换到其他屏幕分辨率以进行安装，请执行如下操作：

- 1 引导以安装。
- 2 按两下 **F3** 键打开一个菜单，从中选择一个较低的安装分辨率。
- 3 选择安装，然后按 **第 3 章 使用 YaST 进行安装** [17] 中所述的步骤进行安装。

要以文本方式进行安装，请执行如下步骤：

- 1 引导以安装。
- 2 按两下 **F3**，然后选择文本方式。
- 3 选择安装，然后按 **第 3 章 使用 YaST 进行安装** [17] 中所述的步骤进行安装。

要执行 VNC 安装，请执行如下操作：

- 1 引导以安装。
- 2 在引导选项提示下输入以下文本：

```
vnc=1 vncpassword=some_password
```

将 `some_password` 替换为用于安装的密码。

- 3 选择安装，然后按 **Enter** 开始安装，并在系统提示时对网络配置选择 DHCP。

系统未正确启动图形安装例程，而是仍以文本方式继续运行，接着暂停，显示一条讯息，其中包含了可通过浏览器界面或 VNC 查看器应用程序访问到安装程序的 IP 地址和端口号。

- 4 如果使用浏览器来访问安装程序，请启动浏览器并输入由未来 SUSE Linux Enterprise 机器上的安装例程提供的地址信息，然后按 **Enter** 键：

```
http://ip_address_of_machine:5801
```

随后浏览器窗口中将打开一个对话框，提示您输入 VNC 密码。输入密码，然后按第 3 章 *使用 YaST 进行安装* [17]中所述的步骤进行安装。

重要

通过 VNC 安装这一方法可在任意操作系统下的任意浏览器上进行，只要启用了 Java 支持即可。

如果您在所采用的操作系统上使用了任意种类的 VNC 查看器，请在看到提示时输入 IP 地址和密码。然后，将打开一个窗口，其中显示了多个安装对话框。照常进行安装。

46.2.7 只能启动简陋的引导屏幕

将第一张 CD 或 DVD 插入了驱动器，BIOS 例程结束，但是系统未启动图形引导屏幕。而是启动了一个非常简陋的基于文本的界面。如果机器的显存不足而无法生成图形引导屏幕，则可能发生这种情况。

虽然文本引导屏幕看起来比较简陋，但是它所提供的功能与图形引导屏幕几乎是相同的。

引导选项

与图形界面不同的是，不能使用键盘的鼠标键来选择其他引导选项。文本引导屏幕上的引导菜单提供了一些可在引导提示下输入的关键字。这些关键字与图形版本中提供的选项相对应。输入您的选择，然后按 **Enter** 键以启动引导过程。

自定义引导选项

在选择引导选项之后，请在引导提示下输入相应的关键字，或者根据 [第 46.2.5 节“无法引导”](#) [729] 中所述输入自定义引导选项。要启动安装过程，请按 **Enter** 键。

屏幕分辨率

使用 **F** 键来确定安装屏幕的分辨率。如果需要以文本方式引导，请选择 **F3**。

46.3 引导问题

引导问题是指系统不能正确引导时出现的情况（不能引导到期望的运行级别和登录屏幕）。

46.3.1 无法装载 GRUB 引导加载程序

如果硬件运行正常，则可能是由于引导加载程序已损坏而使 **Linux** 无法在机器上启动。在这种情况下，需要重安装引导加载程序。要重安装引导加载程序，请执行如下操作：

- 1 将安装介质插入驱动器中。
- 2 重引导计算机。
- 3 从引导菜单中选择安装。
- 4 选择一种语言。
- 5 接受许可协议。

- 6 在安装方式屏幕中，选择其他，然后将安装方式设置为修复已安装系统。
- 7 然后在“YaST 系统修复”模块中，选择专家工具，再选择安装新引导加载程序。
- 8 恢复原始设置并重安装引导加载程序。
- 9 退出“YaST 系统修复”模块并重引导系统。

如果由于某种原因，图形界面不显示，或宁愿手动修复系统，请参考“[使用应急系统](#)”一节 [752] 获取指导。

其他导致机器无法引导的原因可能与 BIOS 相关：

BIOS 设置

请检查 BIOS 中对硬盘驱动器的引用。如果在当前的 BIOS 设置中找不到硬盘驱动器本身，则 GRUB 可能就不能启动。

BIOS 引导顺序

请检查您的系统引导顺序中是否包含硬盘。如果未启用硬盘选项，即使系统正确安装，在访问所需的硬盘时仍可能无法引导。

46.3.2 不出现登录或提示

这种情况通常在内核更新失败后发生，称为 *kernel panic*，原因是该过程中最后阶段有时可以在系统控制台上的错误类型。如果实际上计算机刚刚在软件更新后重引导，则当前目标是使用旧的经过验证的 Linux 版本内核和关联文件重引导。这在引导过程中，可以如下在 GRUB 引导加载程序屏幕中进行：

- 1 使用重设置按钮重引导计算机。
- 2 当 GRUB 引导屏幕开始可见时，选择 *Linux--Failsafe* 然后按 Enter。计算机应使用内核的前一个版本及其关联文件引导。
- 3 引导过程完成之后，去除新安装的内核，并在需要的情况下，手动修改 `/boot/grub/menu.lst` 以将较旧的内核指定为默认选项。有关此配置文件中所使用的语法的详细信息，请参阅[第 18 章 引导加载程序](#) [367]。

不一定要更新此文件，因为部署过程中自动更新工具通常会为您修改它。

4 重引导.

如果因为 *Linux--Failsafe* 选项不能正确引导计算机而不能解决该问题，则使用安装媒体引导计算机。计算机引导之后，继续至[步骤 3](#) [734]和[步骤 4](#) [735]。

46.3.3 无图形登录

如果机器能够启动，但是无法引导到图形登录管理器中，则问题可能出在默认的运行级别选项或 X Windows 系统的配置上。要检查运行级别配置，请作为 root 用户登录，然后检查机器是否配置为引导到运行级别 5（图形桌面）。有一个快捷的检查方法就是检验 `/etc/inittab` 中的如下内容：

```
nld-machine:~ # grep "id:" /etc/inittab
id:5:initdefault:
nld-machine:~ #
```

如果返回的行表明机器的默认运行级别（`initdefault`）设置为 5，则它将引导到图形桌面。如果运行级别设置为其他任何数字，请使用“YaST 运行级别编辑器”模块将其设置为 5。

重要

请不要手动编辑运行级别配置。否则 `SuSEconfig`（由 YaST 运行）将在其下次运行时覆盖这些更改。如果需要在此处进行手动更改，请将 `/etc/sysconfig/suseconfig` 中的 `CHECK_INITTAB` 设置为 `no` 以禁用未来的 `SUSEconfig` 更改。

如果运行级别设置为 5，则您的桌面或 X Windows 软件可能发生损坏。请检验 `/var/log/Xorg.*.log` 中的日志文件，查找它尝试启动的 X 服务器发出的详细讯息。如果桌面在启动时发生故障，它可能将错误讯息记录到 `/var/log/messages` 中。如果这些错误讯息指出问题出在 X 服务器中的配置上，请尝试修正这些问题。如果图形系统仍无法启动，请考虑重安装图形桌面。

一项快速测试：如果用户当前登录到了控制台，`startx` 命令会强制 X Windows 系统使用已配置的默认值启动。如果这不起作用，它将把错误记录到控制台中。有关 X Windows 系统配置的更多信息，请参阅[第 23 章 X 窗口系统](#) [437]。

46.4 登录问题

登录问题是指机器实际上已引导到期望的欢迎屏幕或登录提示下，但是拒绝接受用户名和密码，或者虽然接受了用户名和密码，但是未能正确地运行（无法启动图形桌面、发生错误或转到了命令行等）。

46.4.1 有效的用户名和密码组合失败

如果系统配置为使用网络鉴定或目录服务，但由于某些原因无法从其已配置的服务器上检索到结果，则通常会发生此问题。只有作为唯一本地用户的 `root` 用户仍能登录到这些机器。以下是机器似乎能够运行但是无法正确处理登录的常见原因：

- 网络出现故障。有关此问题的进一步说明，请转到[第 46.5 节“网络问题”](#) [741]。
- DNS 在当时不起作用（这使得 GNOME 或 KDE 不起作用，并使系统无法向安全服务器发出经验证的请求）。如果是这种情况，则表现为机器对任何操作的响应都需要极其长的时间。有关该主题的详细信息，请参见[第 46.5 节“网络问题”](#) [741]。
- 如果系统配置为使用 Kerberos，则系统的本地时间与 Kerberos 服务器时间之间的差异可能超过了可接受的值（通常为 300 秒）。如果 NTP（网络时间协议）未正确地起作用，或者本地 NTP 服务器不起作用，则 Kerberos 鉴定将不再工作，因为该鉴定依赖于整个网络的通用时钟同步。
- 系统的鉴定配置不正确。请对相关的 PAM 配置文件进行检查以确定是否存在指令输入错误或排序错误。有关 PAM 的其他背景信息及相关配置文件的语法，请参阅[第 24 章 通过 PAM 进行鉴定](#) [449]。

在不涉及外部网络问题的所有情况下，解决方法是将系统重引导到单用户方式并修复配置，然后再次引导到操作方式并重试登录。要引导到单用户方式，请执行以下操作：

- 1 重引导系统。此时将出现引导屏幕，其中显示一个提示。
- 2 在引导提示下输入 1，使系统引导到单用户方式。
- 3 输入根用户的用户名和密码。

4 进行必要的一切更改。

5 在命令行中输入 `telinit 5` 以引导到完全的多用户和网络方式。

46.4.2 不接受有效的用户名和密码

这是到目前为止用户最常遇到的问题，因为有许多原因可能引起该问题。登录失败可由多种原因造成，取决于您是使用本地用户管理和鉴定，还是使用网络鉴定。

本地用户管理失败可由以下原因造成：

- 用户可能输入了错误的密码。
- 用户包含桌面配置文件的主目录已损坏或被写保护。
- 鉴定该特定用户的 X windows 系统可能存在问题，尤其是在安装当前产品之前，该用户的主目录已被其他 Linux 产品所使用时。

要找到本地登录失败的原因，请执行如下操作：

- 1 在尝试调试整个鉴定机制之前，请检查用户所记的密码是否正确。如果用户可能记错了密码，请使用“YaST 用户管理”模块来更改用户的密码。
- 2 以 root 用户身份登录并检查 `/var/log/messages` 以找到登录过程和 PAM 的错误消息。
- 3 尝试从控制台登录（使用 `Ctrl+Alt+F1`）。如果成功了，则问题不在 PAM 上，因为可以在该机器上鉴定此用户。尝试找出任何与 X Windows 系统或桌面（GNOME 或 KDE）有关的错误。有关更多信息，请参阅第 46.4.3 节“登录成功但 GNOME 桌面发生故障”[739]和第 46.4.4 节“登录成功但 KDE 桌面发生故障”[740]。
- 4 如果用户的主目录被其他 Linux 产品所使用，请将该用户主目录中的 `Xauthority` 文件去除。使用控制台登录（通过 `Ctrl + Alt + F1`），然后以该用户的身份运行 `rm .Xauthority`。这样应该可以消除该用户的 X 鉴定问题。然后重试图形登录。
- 5 如果图形登录依然失败，请使用 `Ctrl + Alt + F1` 进行控制台登录。尝试在另一个屏幕上启动 X 会话，第一个 `(:0)` 已经在使用中：

```
startx -- :1
```

这样应该可以显示图形屏幕和桌面。如果无效，请查看 X Windows 系统的日志文件（`/var/log/Xorg.displaynumber.log`）或您桌面应用程序的日志文件（用户主目录中的 `.xsession-errors`），以确定是否有任何违反规则的地方。

- 6 如果桌面由于配置文件损坏而无法启动，请参阅[第 46.4.3 节“登录成功但 GNOME 桌面发生故障”](#)[739]或[第 46.4.4 节“登录成功但 KDE 桌面发生故障”](#)[740]。

以下是在特定的机器上对特定用户的网络鉴定可能失败的常见原因：

- 用户可能输入了错误的密码。
- 用户名存在于机器的本地鉴定文件中，但同时网络鉴定系统也提供了该用户名，从而引起冲突。
- 主目录存在，但已损坏或不可用。该目录可能处于写保护状态或位于此刻无法访问的服务器上。
- 用户无权登录到鉴定系统中的该特定主机。
- 机器出于某种原因更改了主机名，而用户无权登录到该主机。
- 机器无法访问包含该用户信息的鉴定服务器或目录服务器。
- 鉴定该特定用户的 X windows 系统可能存在问题，尤其是在安装当前产品之前，该用户的主目录已被其他 Linux 产品所使用时。

要通过网络鉴定找到登录问题的原因，请执行以下步骤：

- 1 在尝试调试整个鉴定机制之前，请检查用户所记的密码是否正确。
- 2 确定机器在鉴定时要依赖的目录服务器，并确保机器在正常运行且与其他机器正常通信。
- 3 确定该用户的用户名和密码在其他机器上是否有效，以确保存在该用户的鉴定数据且已正确分发。
- 4 确定其他用户是否可以登录到该故障机器。如果其他用户可以毫无困难地登录或者 root 用户可以登录，请登录并检验 `/var/log/messages`

文件。找到与登录尝试相对应的时间戳记，然后确定 PAM 是否生成了任何错误讯息。

- 5 尝试从控制台登录（使用 **Ctrl + Alt + F1**）。如果成功了，则问题不在用户主目录中的 PAM 或目录服务器上，因为可以在该机器上鉴定此用户。尝试找出任何与 X Windows 系统或桌面（GNOME 或 KDE）有关的错误。有关更多信息，请参阅第 46.4.3 节“登录成功但 GNOME 桌面发生故障”[739]和第 46.4.4 节“登录成功但 KDE 桌面发生故障”[740]。
- 6 如果用户的主目录被其他 Linux 产品所使用，请将该用户主目录中的 `Xauthority` 文件去除。使用控制台登录（通过 **Ctrl + Alt + F1**），然后以该用户的身份运行 `rm .Xauthority`。这样应该可以消除该用户的 X 鉴定问题。然后重试图形登录。
- 7 如果图形登录依然失败，请使用 **Ctrl + Alt + F1** 进行控制台登录。尝试在另一个屏幕上启动 X 会话，第一个 (:0) 已经在使用中：

```
startx -- :1
```

这样应该可以显示图形屏幕和桌面。如果无效，请查看 X Windows 系统的日志文件（`/var/log/Xorg.displaynumber.log`）或您桌面应用程序的日志文件（用户主目录中的 `.xsession-errors`），以确定是否有任何违反规则的地方。

- 8 如果桌面由于配置文件损坏而无法启动，请参阅第 46.4.3 节“登录成功但 GNOME 桌面发生故障”[739]或第 46.4.4 节“登录成功但 KDE 桌面发生故障”[740]。

46.4.3 登录成功但 GNOME 桌面发生故障

如果这发生于特定用户，则可能是由于该用户的 GNOME 配置文件已损坏。可能出现的症状有键盘不起作用、屏幕几何图形变形，甚至整个屏幕变成灰色。而最重要的差别在于其他用户登录时，该机器能正常运行。如果属于这种情况，只需将用户的 GNOME 配置目录移到某个新位置，以便使 GNOME 初始化一个新的桌面，这样就能很快地解决此问题。虽然用户不得不重配置 GNOME，但不会丢失任何数据。

- 1 按 **Ctrl + Alt + F1** 切换到文本控制台。
- 2 用您的用户名登录。

3 将用户的 GNOME 配置目录移到某个临时位置：

```
mv .gconf .gconf-ORIG-RECOVER
mv .gnome2 .gnome2-ORIG-RECOVER
```

4 注销。

5 再次登录，但别运行任何应用程序。

6 通过以下命令将 ~/.gconf-ORIG-RECOVER/apps/ 目录复制回新的 ~/.gconf 目录，这样就能恢复您的个人应用程序配置数据（包括 Evolution 电子邮件客户程序数据）：

```
cp -a .gconf-ORIG-RECOVER/apps .gconf/
```

如果这引起登录问题，则尝试只恢复重要的应用程序数据并重配置其他的应用程序。

46.4.4 登录成功但 KDE 桌面发生故障

KDE 桌面不允许用户登录有多种原因。高速缓存数据以及 KDE 桌面配置文件的损坏都可能引起登录问题。

桌面在启动时会用到超速缓存数据，这将提高性能。如果数据损坏，则启动将变慢或完全失败。将超速缓存数据去除会强制桌面启动例程从头开始。这样会花费比正常启动更多的时间，但是在这之后数据将完好无缺，用户也可以登录。

要去除 KDE 桌面的高速缓存文件，请以 root 用户身份发出以下命令：

```
rm -rf /tmp/kde-user /tmp/socket-user
```

请将 *user* 替换为实际用户名。将这两个目录去除只是去除损坏的高速缓存文件，使用该过程并不会破坏实际数据。

损坏的桌面配置文件始终可以用初始配置文件替换。如果想要恢复用户所作的调整，请在使用默认配置值恢复配置之后，将这些调整从其临时位置小心地复制回原来的位置。

要将损坏的桌面配置替换为初始配置值，请执行如下操作：

1 按 Ctrl + Alt + F1 切换到文本控制台。

2 用您的用户名登录。

3 将 KDE 配置目录和 `.skel` 文件移到临时位置：

```
mv .kde .kde-ORIG-RECOVER
mv .skel .skel-ORIG-RECOVER
```

4 注销。

5 再次登录。

6 在成功启动桌面之后，将用户自己的配置复制回原来的位置：

```
cp -a .kde-ORIG-RECOVER/share .kde/share
```

重要

如果用户自己的调整先前引起了登录失败并仍然如此，请重复上述步骤，但是不要复制 `.kde/share` 目录。

46.5 网络问题

系统的许多问题可能都与网络相关，即使初看起来不是这样。例如，系统不允许用户登录的原因可能是某种网络问题造成的。本节将引入一个简单的核对表，您可以使用它来确定任何所遇到的网络问题的原因。

在检查机器的网络连接时，请执行如下操作：

1 如果使用的是以太网连接，请首先检查硬件。请确保网线已正确地插入计算机。以太网连接器旁边的控制灯（如果有的话）应全部亮起。

如果连接失败，请检查网线在别的机器上是否正常。如果正常，则可能是网卡引起了该问题。如果网络设置中包含集线器和交换机，也需要对它们进行检查。

2 如果使用的是无线连接，请检查是否可与其他机器建立此无线链接。如果无法建立，请与无线网络管理员联系。

3 一旦完成了对基本网络连通性的检查，请尝试找出没有响应的服务。收集设置中所需的所有网络服务器的地址信息。在相应的 YaST 模块中查找

这些信息，或者询问您的系统管理员。以下列表给出了设置中涉及的一些典型网络服务器问题以及服务中断的症状。

DNS（名称服务）

名称服务中断或发生故障会在许多方面影响网络运行。如果本地机器依赖于任何网络服务器进行鉴定，但由于名称解析问题而无法找到这些服务器，则用户甚至可能无法登录。网络中由中断的名称服务管理的机器将无法“看到”彼此且不能通信。“”

NTP（时间服务）

NTP 服务发生故障或完全中断可能会影响 Kerberos 鉴定和 X 服务器功能。

NFS（文件服务）

如果任何应用程序所需的数据存储在 NFS 安装目录中，则一旦此服务停止或配置错误，应用程序将无法启动或正常运行。最坏的情况是，如果由于 NFS 服务器宕机而无法找到包含 `.gconf` 或 `.kde` 子目录的主目录，则该主目录所属的用户的个人桌面配置将无法启动。

Samba（文件服务）

如果任何应用程序所需的数据存储在 Samba 服务器上的某个目录中，则一旦此服务停止，则应用程序将无法启动或正常运行。

NIS（用户管理）

如果您的 SUSE Linux Enterprise 系统依赖于 NIS 服务器提供用户数据，则一旦 NIS 服务停止，用户将无法登录到该机器。

LDAP（用户管理）

如果您的 SUSE Linux Enterprise 系统依赖于 LDAP 服务器提供用户数据，则一旦 LDAP 服务停止，用户将无法登录到该机器。

Kerberos（鉴定）

如果此服务停止，则鉴定将不起作用，且用户无法登录到任何机器。

CUPS（网络打印）

如果此服务停止，用户将无法进行打印。

4 请检查网络服务器是否正在运行并且您的网络设置是否允许您建立连接：

重要

下面介绍的调试步骤只适用于简单的网络服务器/客户机设置，不涉及任何内部路由。假设服务器和客户机都是同一子网的成员，不需要额外的路由。

- 4a** 可使用 `ping hostname`（将 `hostname` 替换为服务器的主机名）来检查各台服务器是否正在运行且能够对网络作出响应。如果此命令成功，表示您所查找的主机在正常运行，并且网络的名称服务配置正确。

如果 `ping` 命令失败，同时显示讯息目标主机不可访问，则表明您的系统或期望的服务器未正确配置或已宕机。可从其他机器运行 `ping your_hostname` 命令来检查您的系统是否可被访问。如果可以从其他机器访问您的机器，则服务器不会运行或正确配置。

如果 `ping` 命令失败，同时显示未知主机，则表示名称服务未正确配置或使用的主机名不正确。请使用 `ping -nipaddress` 尝试连接到这一没有名称服务的主机。如果成功，则请检查主机名的拼写是否正确以及网络中的名称服务是否配置正确。要对该问题进行进一步的检查，请参阅 [步骤 4b](#) [743]。如果 `ping` 命令仍然失败，则可能网卡未正确配置或网络硬件存在故障。有关此问题的信息，请参阅 [步骤 4c](#) [744]。

- 4b** 请使用 `host hostname` 来检查您尝试连接的服务器的主机名是否能够正确地转换为 IP 地址，反之亦然。如果此命令返回了该主机的 IP 地址，则名称服务已在正常运行。如果 `host` 命令失败，请检查您主机上所有与名称和地址解析相关的网络配置文件：

/etc/resolv.conf

此文件用于对当前使用的名称服务器和域进行跟踪。您可手动修改该文件，或者由 YaST 或 DHCP 自动调整。建议采用自动调整。但是，请确保此文件具有以下结构并且所有的网络地址和域名都正确无误：

```
search fully_qualified_domain_name
nameserver ipaddress_of_nameserver
```

此文件中可以包含多个名称服务器地址，但是其中必须至少有一个能够对您的主机提供正确的名称解析。如果需要，可使用“YaST DNS 和主机名”模块调整该文件。

如果网络连接是通过 DHCP 处理的，请在“YaST DNS 和主机名”模块中选择通过 *DHCP* 更改主机名和通过 *DHCP* 更新名称服务器和搜索列表，以启用 DHCP 来更改主机名和名称服务信息。

/etc/nsswitch.conf

此文件告诉 Linux 到何处查找名称服务信息。它应显示为：

```
...
hosts: files dns
networks: files dns
...
```

dns 条目是必需的。它告诉 Linux 要使用外部名称服务器。通常情况下，这些条目是由 YaST 自动建立的，但是不会影响检查。

如果主机上的所有相关条目均正确，请让系统管理员检查 DNS 服务器配置，以确定时区信息是否正确。如果确信主机和 DNS 服务器的 DNS 配置正确，请检查网络和网络设备的配置。

- 4c** 如果系统无法与网络服务器建立连接，并且已排除了名称服务出现问题的可能，则请检查网卡的配置。

请使用 `ifconfig network_device` 命令（以 root 用户的身份执行）来检查此设备是否已正确配置。确保 `inet address` 和 `Mask` 已正确配置。如果 IP 地址中出现错误或网络掩码中缺少一位，将使您的网络配置无法使用。如有必要，也在服务器上执行该检查。

- 4d** 如果名称服务和网络硬件已正确配置并正在运行，但是某些外部网络连接仍然长时间超时或完全失败，请使用 `traceroute`

`fully_qualified_domain_name` 命令（以 `root` 用户的身份执行）来跟踪这些请求所经过的网络路由。此命令将列出某一请求从您的机器传递到其目的地所经过的所有网关（中继）。它列出了每个中继的响应时间以及该中继是否可访问。请将 `traceroute` 和 `ping` 结合使用以确定故障原因并通知管理员。

一旦确定了网络故障的原因，就可以自行解决（如果问题出在您自己的计算机上），或告诉网络系统管理员您的发现，以便其重配置服务或修复必要的系统。

46.5.1 NetworkManager 问题

如果网络连接有问题，请按 [741] 中所述缩小范围。如果 `NetworkManager` 看上去是 `culprit`，请按如下步骤操作，获得日志，它会提供 `NetworkManager` 为何失效的线索：

- 1 以 `root` 用户身份打开 `shell` 并登录。
- 2 重新启动 `NetworkManager`：

```
rcnetwork restart -o nm
```
- 3 作为普通用户打开万维网页面（例如 <http://www.opensuse.org>）看是否能连接。
- 4 收集 `/var/log/NetworkManager` 中有关 `NetworkManager` 状态的任何信息。

有关 `NetworkManager` 的更多信息，请参考第 30.5 节“使用 `NetworkManager` 管理网络连接” [569]。

46.6 数据问题

数据问题是指无论机器是否能够正常引导，有一点是明确的，即系统上的数据损坏了，并且系统需要恢复。这些情况下需要对关键数据进行备份，以便您能够在系统出现故障时恢复故障前的状态。`SUSE Linux Enterprise` 提供了专用的 `YaST` 模块用于系统备份和恢复，此外还提供了一个应急系统，用于从外部恢复受损的系统。

46.6.1 备份关键数据

可使用“YaST 系统备份”模块轻松管理系统备份：

- 1 以 root 用户身份启动 YaST，然后选择 **系统 > 系统备份**。
- 2 创建一个存放备份所需的所有详细信息、存档文件的文件名以及备份范围和类型的备份配置文件：
 - 2a 选择 **配置文件管理 > 添加**。
 - 2b 输入存档文件的名称。
 - 2c 如果想要保留本地备份，请输入备份位置的路径。如果要将备份存档在网络服务器上（通过 NFS），请输入 IP 地址或服务器名称以及存放存档文件的目录。
 - 2d 确定存档类型，然后单击 **下一步**。
 - 2e 确定要使用的备份选项，例如是否要对不属于任何包的文件进行备份以及在创建存档文件之前是否显示文件列表。此外，确定是否使用耗费时间的 MD5 机制来确定更改过的文件。

使用专家进入备份整个硬盘区域的对话框。目前该选项仅适用于 Ext2 文件系统。
 - 2f 最后，设置搜索约束条件，以将某些不需要备份的系统区域排除在备份区域之外，如锁文件或高速缓存文件。添加、编辑或删除项目，直到符合要求为止，然后单击 **确定退出**。
- 3 一旦完成了配置文件设置，就可以单击 **创建备份** 立即开始备份，或者配置自动备份。此外，还可以创建用于其他各种用途的配置文件。

要为指定的配置文件配置自动备份，请执行如下操作：

- 1 在 **配置文件管理** 菜单中选择 **自动备份**。
- 2 选择 **自动启动备份**。

- 3 确定备份频率。选择每天、每周或每月。
- 4 确定备份开始时间。这些设置取决于所选择的备份频率。
- 5 确定是否保留旧的备份以及保留的个数。要自动接收备份过程自动生成的状态讯息，请选中*向根用户发送摘要邮件*。
- 6 单击*确定*以应用您的设置，首次备份将在指定的时间开始。

46.6.2 恢复系统备份

请使用“YaST 系统恢复”模块从备份恢复系统配置。可恢复整个备份，或选择已损坏并需要重置为先前状态的特定部分。

- 1 启动 *YaST* > 系统 > 系统恢复。
- 2 输入备份文件的位置。这可以是本地文件、网络安装文件或移动设备（如软盘或 CD）上的文件。然后单击*下一步*。

以下对话框显示了存档文件属性（如文件名、创建日期、备份类型和可选的注释）的摘要。
- 3 可单击*存档文件内容*来查看已存档的内容。单击*确定*可返回到*存档文件属性*对话框。
- 4 单击*专家选项*将打开一个对话框，在其中可对恢复过程进行微调。单击*确定*可返回到*存档文件属性*对话框。
- 5 单击*下一步*可打开要恢复的包的视图。按*接受*可恢复该存档文件中的所有文件，或者使用各个*全选*、*取消选择全部*和*选择文件*按钮对所选存档文件进行微调。如果 RPM 数据库损坏或被删除，且该文件包含在备份中，则只需使用*恢复 RPM 数据库*选项。
- 6 在单击*接受*之后，将恢复备份。在恢复过程完成后，单击*完成*将退出此模块。

46.6.3 恢复受损的系统

有多种原因会造成系统无法正常启动和运行。系统崩溃后造成文件系统损坏、配置文件损坏或引导加载程序配置损坏是最常见的原因。

SUSE Linux Enterprise 提供两种不同的方式来处理这种情况。您可以使用 YaST 系统修复功能，也可以引导应急系统。以下小节将介绍两种系统修复的功能。

使用 YaST 系统修复

在启动 YaST 系统修复模块之前，确定要运行该模块的方式以最佳满足您的需要。依据系统故障的严重性和原因以及您的专业知识，在三个不同的方式进行选择：

自动修复

如果由于未知原因系统发生故障并且您基本上不知道系统的哪个部分导致此故障，则使用 *自动修复*。将会对您安装的系统上的所有组件执行全面的自动化检查。有关此过程的详细描述，请参见“[自动修复](#)”一节 [748]。

自定义修改

如果您的系统发生故障并且您已经知道哪个组件导致此故障，则您可以通过将系统分析的范围限制于那些组件来缩短使用 *自动修复* 进行系统检查所需的长时间。例如，如果发生故障之前的系统消息指示包数据库出错，则您可以将分析和修复过程只限于检查和恢复系统的此部分。有关此过程的详细描述，请参见“[自定义修改](#)”一节 [750]。

专家工具

如果您已经清楚地知道哪个组件发生故障和修复此故障的方法，则您可以跳过分析运行并直接应用修复相关组件的所需的工具。有关详细信息，请参见“[专家工具](#)”一节 [751]。

选择以上描述的一个修复方式并按以下部分所述继续执行系统修复。

自动修复

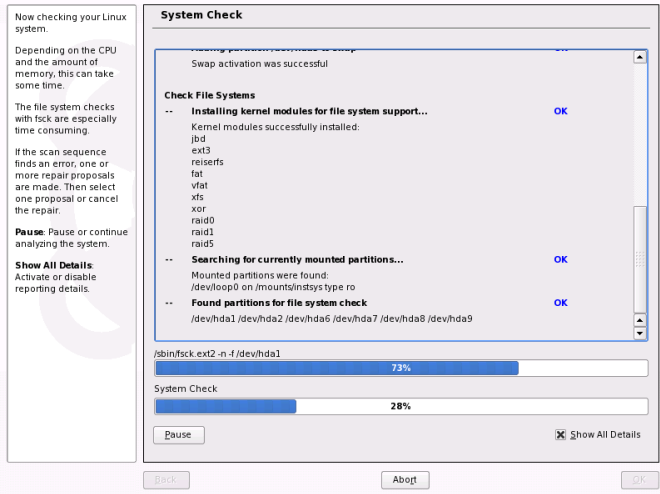
要启动 YaST 系统修复的自动修复方式，请如下执行操作：

- 1 将第一张 SUSE Linux Enterprise 安装媒体插入 CD 或 DVD 驱动器中。

- 2 重引导系统。
- 3 在引导屏幕中选择安装。
- 4 选择语言并单击下一步。
- 5 确认许可证协议并单击下一步。
- 6 在系统分析中，选择其他 > 修复已安装系统。
- 7 选择自动修复。

YaST 现在对已安装系统启动全面分析。屏幕的底部使用两个进度条显示此过程的进度。上面的进度条显示当前正在运行的测试的进度。下面的进度条显示分析进程的总体进度。上面的日志窗口用于跟踪当前运行的测试及其结果。请参见图 46.2 “自动修复方式” [749]。每次运行都会执行以下主要测试。这些测试又包含许多单独的子测试。

图 46.2 自动修复方式



所有硬盘的分区表

检查所有检测到的硬盘的分区表的有效性和一致性。

交换分区

检测并测试已安装系统的交换分区，并在合适的情况下建议激活交换分区。应该接受这一建议以实现更高的系统修复速度。

文件系统

所有检测到的文件系统都需要进行特定于文件系统的检查。

文件 `/etc/fstab` 中的项

检查文件中项的完整性和一致性。将装入所有有效的分区。

引导加载程序配置

检查已安装系统（GRUB 或 LILO）的引导加载程序配置的完整性和一致性。将检查引导和根设备，并将检查 `initrd` 模块的可用性。

包数据库

这将检查执行最小安装的操作所需的所有包是否存在。虽然还可以分析基础包，但因为基础包数量太大，将花费很长时间。

- 8 当出现错误时，过程将停止并打开一个对话框，其中描述了详细信息和可能的解决方案。

在接受建议修复之前仔细阅读屏幕讯息。如果您确定拒绝建议的解决方案，您的系统将保持不变。

- 9 在修复过程成功终止之后，单击 **确定** 和 **完成**，除去安装媒体。系统将自动重引导。

自定义修改

要启动自定义修复方式并选择性地检查所安装系统的某些组件，请如下执行操作：

- 1 将 SUSE Linux Enterprise 的第一张安装媒体插入 CD 或 DVD 驱动器中。
- 2 重引导系统。
- 3 在引导屏幕中选择安装。
- 4 选择语言并单击 **下一步**。
- 5 确认许可证协议并单击 **下一步**。

6 在系统分析中，选择其他 > 修复已安装系统。

7 选择自定义修复。

选择自定义修复将显示一组测试，这些测试最初都被标记为准备执行。这些测试的总范围和自动修复的测试范围一致。如果您清楚哪些方面没有损坏，则取消对应测试的标记。单击下一步将启动一个范围相对较小的测试过程，可能将显著缩短运行时间。

并不是所有的测试组都单独适用。fstab 项的分析会始终与文件系统（包括现有的交换分区）检查一起进行。YaST 会通过选择必需运行的最少测试数量来自动解决此类依赖性。

8 当出现错误时，过程将停止并打开一个对话框，其中描述了详细信息和可能的解决方案。

在接受建议修复之前仔细阅读屏幕讯息。如果您确定拒绝建议的解决方案，您的系统将保持不变。

9 在修复过程成功终止之后，单击确定和完成，除去安装媒体。系统将自动重引导。

专家工具

如果您熟悉 SUSE Linux Enterprise，并且已非常清楚系统中所需的修复，请跳过系统分析来直接应用工具。

要使用 YaST 系统修复模块的专家工具功能，请如下进行操作：

- 1 使用您用于初始安装（如第 3 章 使用 YaST 进行安装 [17] 中所述）的原始安装媒体来引导系统。
- 2 在系统分析中，选择其他 > 修复已安装系统。
- 3 选择专家工具，并选择一个或多个修复选项。
- 4 在修复过程成功终止之后，单击确定和完成，除去安装媒体。系统将自动重引导。

专家工具提供下列选项修复您的错误系统：

安装新的 Boot Loader

这将启动 YaST 引导加载程序配置模块。详细信息请参见第 18.3 节“使用 YaST 配置引导加载程序” [376]。

启动分区工具

这将启动 YaST 中的专家分区工具。

修复文件系统

这将检查已安装系统的文件系统。首先将向您提供所有检测到的分区的选择，您可以在其中选择要检查的分区。

恢复丢失的分区

可以尝试重建损坏的分区表。首先将显示检测到的硬盘的列表以供选择。单击确定开始检查。这可能要花一段时间，具体取决于处理能力和硬盘的大小。

重要: 重建分区表

重建分区表非常麻烦。YaST 尝试通过分析硬盘的数据扇区识别丢失的分区。在识别出丢失的分区之后，会添加它们以重建分区表。但是，此操作不能保证在所有可能的情况下都成功。

将系统设置保存到软盘

此选项将重要的系统文件保存到软盘上。如果这些文件中的某个文件被损坏，可以从磁盘恢复该文件。

校验安装的软件

这将检查包数据库的一致性和最重要包的可用性。使用此工具可以重安装任何损坏的已安装包。

使用应急系统

SUSE Linux Enterprise 包含一个救援系统。该应急系统是一个小型 Linux 系统，可以装载到一个 RAM 磁盘并以根文件系统的形式装入，使您可以从外部访问 Linux 分区。使用该应急系统，可以恢复或修改系统中任何一个重要的方面：

- 操作任意类型的配置文件。
- 检查文件系统中的缺陷和启动自动修复进程。

- 访问“更改根”环境下的已安装系统。
- 检查、修改和重安装引导加载程序配置。
- 使用 `parted` 命令调整分区大小。有关该工具的更多信息，请访问 GNU Parted 万维网站点 (<http://www.gnu.org/software/parted/parted.html>)。

该应急系统可以从各种来源和位置进行装载。最简单的选择是从原始安装 CD 或 DVD 上引导该应急系统：

- 1 将安装媒体插入 CD 或 DVD 驱动器中。
- 2 重引导系统。
- 3 在引导屏幕中，选择应急系统选项。
- 4 在 Rescue： 提示符处输入 `root`。无需密码。

如果硬件设置不包含 CD 或 DVD 驱动器，可以从网络源引导该救援系统。以下范例适用于远程引导的情形，如果使用另一引导媒体（例如软盘），则要相应地修改 `info` 文件，并像正常安装一样进行引导。

- 1 输入您的 PXE 引导设置的配置，并用 `rescue=protocol://instsource` 替换 `install=protocol://instsource`。如同正常安装的情况一样，`protocol` 代表任何一种所支持的网络协议（NFS、HTTP、FTP 等）；`instsource` 代表网络安装源的路径。
- 2 如第 4.3.7 节“局域网唤醒”[62]中所述，使用“网络唤醒”引导系统。
- 3 在 Rescue： 提示符处输入 `root`。无需密码。

一旦进入该应急系统，便可通过 `Alt + F1` 到 `Alt + F6` 键来使用虚拟控制台。

可以在 `/bin` 目录下找到 `shell` 和许多其他有用的实用程序，如 `mount` 程序。`sbin` 目录包含重要的用于查看和修复文件系统的文件和网络实用程序。此目录还包含用于系统维护的最重要的二进制文件，如 `fdisk`、`mkfs`、`mkswap`、`mount`、`mount`、`init` 和 `shutdown`，以及用于维护网络的 `ifconfig`、`ip`、`route` 和 `netstat`。目录 `/usr/bin` 包含 `vi` 编辑器、`find`、`less` 和 `telnet`。

要查看系统讯息，请使用命令 `dmesg` 或查看文件 `/var/log/messages`。

检查和操作配置文件

举一个可以通过该应急系统修复配置的例子，假设有一个被损坏的配置文件，使该系统无法正常引导。您可以通过应急系统修复该配置文件。

要操作配置文件，请执行以下步骤：

- 1 用上述方法之一启动应急系统。
- 2 要在应急系统中装入位于 `/dev/sda6` 下的根文件系统，请使用如下命令：

```
mount /dev/sda6 /mnt
```

系统所有目录现在均位于 `/mnt` 之下

- 3 将目录切换为所装入的根文件系统：

```
cd /mnt
```

- 4 在 `vi` 编辑器中打开有问题的配置文件。调整并保存配置。

- 5 从应急系统中卸载根文件系统：

```
umount /mnt
```

- 6 重引导计算机。

修复和检查文件系统

通常，不能在正在运行的系统上修复文件系统。如果遇到严重问题，您甚至都无法装入根文件系统，系统引导可能以显示 `kernel panic` 结束。在这种情况下，唯一的方法是从外部修复系统。强烈建议使用 **YaST** 系统修复功能执行此任务（请参见“**使用 YaST 系统修复**”一节 [748]以了解详细信息）。但是，如果需要执行手动文件系统检查或修复，请引导应急系统。该功能包含检查并修复 `ext2`、`ext3`、`reiserfs`、`xfs`、`dosfs` 以及 `vfat` 文件系统的实用程序。

访问已安装系统

如果需要从应急系统访问已安装系统，例如，要修改引导加载程序配置或执行硬件配置实用程序，则需要在“更改根”环境下进行。

要设置基于已安装系统的“更改根”环境，请执行以下步骤：

- 1 首先装入已安装系统和设备文件系统的根分区：

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

- 2 现在可以“更改根”为新的环境：

```
chroot /mnt
```

- 3 然后装入 /proc 和 /sys：

```
mount /proc
mount /sys
```

- 4 最后，装入已安装系统的剩余分区：

```
mount -a
```

- 5 现在可以访问已安装系统了。在重引导系统之前，请用 `umount -a` 卸载分区并用 `exit` 退出“更改根”环境。

警告：限制

尽管对已安装系统的文件和应用程序有完全访问权，但仍有一些限制。正在运行的内核是以前使用应急系统引导的内核。该内核只支持关键性硬件，不可能从已安装系统添加内核模块，除非内核版本完全一致（这没有可能性）。举例来说，这样您将无法访问声卡。也不可能启动图形用户界面。

还应注意，在使用 `Alt + F1` 到 `Alt + F6` 键切换控制台时，要退出“更改根”环境。

修改和重安装引导加载程序

有时，系统无法引导是因为引导加载程序配置已损坏。例如，如果没有正常工作的引导加载程序，启动例程将无法将物理驱动器转化为 Linux 文件系统中的实际位置。

要检查引导加载程序配置并重安装引导加载程序，请执行以下操作：

- 1 如“[访问已安装系统](#)”一节 [755]中所述执行必要的步骤以访问已安装系统。
- 2 依据[第 18 章 引导加载程序](#) [367]中所述 GRUB 配置原则，检查下列文件是否正确配置。

- /etc/grub.conf
- /boot/grub/device.map
- /boot/grub/menu.lst

如有必要，将修复程序应用于根分区及配置文件的设备映射(device.map)或位置。

- 3 使用以下命令序列重安装引导加载程序：

```
grub --batch < /etc/grub.conf
```

- 4 卸载分区，从“更改根”环境中注销并重引导该系统：

```
umount -a  
exit  
reboot
```