

SUSE Linux Enterprise Server

11 SP3

www.suse.com

2013 年 5 月 23 日

管理指南



管理指南

版权所有 © 2006–2013 SUSE LLC 和贡献者。保留所有权利。

根据 GNU 自由文档许可证 (GNU Free Documentation License) 版本 1.2 或（根据您的选择）版本 1.3 中的条款，在此授予您复制、分发和/或修改本文档的许可权限；本版权声明和许可证附带不可变部分。许可证版本 1.2 的副本包含在题为“GNU 自由文档许可证”的部分。

有关 SUSE 和 Novell 商标，请参见 Novell 商标和服务标记列表 <http://www.novell.com/company/legal/trademarks/tmlist.html>。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 SUSE 或 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。SUSE LLC 及其附属公司、作者和译者对于可能出现的错误或由此造成的后果皆不承担责任。

目录

关于本指南	xiii
1 可用文档	xiv
2 反馈	xvi
3 文档约定	xvi
 I 支持任务和常见任务	 1
 1 YaST 联机更新	 3
1.1 联机更新对话框	4
1.2 安装增补程序	7
1.3 自动联机更新	8
 2 收集用于支持的系统信息	 11
2.1 概述	11
2.2 使用 Supportconfig 收集信息	11
2.3 向 Novell 提交信息	13
2.4 更多信息	15
 3 文本方式的 YaST	 17
3.1 在模块中导航	18
3.2 组合键的限制	19
3.3 YaST 命令行选项	20

4 使用快照程序生成快照/实现回滚	23
4.1 要求	23
4.2 使用快照程序撤销系统更改	24
4.3 手动创建和管理快照	34
4.4 限制	38
4.5 常见问题	39
4.6 在精简的 LVM 卷上使用快照程序	40
5 使用 VNC 远程访问	41
5.1 一次性 VNC 会话	41
5.2 持续 VNC 会话	43
6 使用命令行工具管理软件	47
6.1 使用 Zypper	47
6.2 RPM — 包管理器	60
7 Bash 和 Bash 脚本	71
7.1 什么是“外壳”?	71
7.2 编写外壳脚本	76
7.3 重定向命令事件	77
7.4 使用别名	78
7.5 在 Bash 中使用变量	79
7.6 将命令分组和组合	81
7.7 使用通用流程构造语句	82
7.8 更多信息	83
II 系统	85
8 64 位系统环境中的 32 位和 64 位应用程序	87
8.1 运行时支持	87

8.2 软件开发	88
8.3 Biarch 平台上的软件编译	89
8.4 内核规范	90
9 引导和配置 Linux 系统	93
9.1 Linux 引导进程	93
9.2 init 进程	96
9.3 通过 /etc/sysconfig 配置系统	104
10 引导加载程序 GRUB	107
10.1 通过 GRUB 引导	108
10.2 使用 YaST 配置引导加载程序	117
10.3 卸载 Linux 引导加载程序	122
10.4 创建引导 CD	123
10.5 图形 SUSE 屏幕	124
10.6 查错	124
10.7 有关详细信息	126
11 UEFI (统一可扩展固件接口)	127
11.1 安全引导	127
11.2 更多信息	134
12 特别的系统功能组件	135
12.1 特殊软件包的相关信息	135
12.2 虚拟控制台	141
12.3 键盘映射	142
12.4 语言和国家/地区特定的设置	143
13 打印机操作	147
13.1 打印系统工作流程	148

13.2 连接打印机的方法和协议	149
13.3 安装软件	149
13.4 网络打印机	150
13.5 从命令行打印	152
13.6 SUSE Linux Enterprise Server 中的特殊功能	152
13.7 查错	155
14 使用 udev 进行动态内核设备管理	163
14.1 /dev 目录	163
14.2 内核 uevents 和 udev	164
14.3 驱动程序、内核模块和设备	164
14.4 引导和启动设备设置	165
14.5 监视正在运行的 udev 守护程序	165
14.6 使用 udev 规则影响内核设备事件处理	166
14.7 永久设备命名	173
14.8 udev 使用的文件	173
14.9 更多信息	174
15 X Window 系统	175
15.1 手动配置 X Window 系统	175
15.2 安装和配置字体	181
15.3 更多信息	187
16 使用 FUSE 访问文件系统	189
16.1 配置 FUSE	189
16.2 可用 FUSE 插件	189
16.3 更多信息	190

III 移动计算机 191

17 Linux 中的移动计算 193

17.1 便携式计算机	193
17.2 移动硬件	200
17.3 手提电话和 PDA	200
17.4 更多信息	200

18 无线 LAN 203

18.1 WLAN 标准	203
18.2 操作方式	204
18.3 身份验证	205
18.4 加密	206
18.5 用 YaST 配置	207
18.6 建立 WLAN 的提示和技巧	214
18.7 查错	215
18.8 更多信息	217

19 电源管理 219

19.1 省电功能	219
19.2 高级配置和电源接口 (ACPI)	220
19.3 硬盘的休眠	222
19.4 查错	224
19.5 更多信息	226

20 使用 Tablet PC 227

20.1 安装 Tablet PC 包	228
20.2 配置手写板设备	229
20.3 使用虚拟键盘	229
20.4 旋转显示器	229

20.5 使用手势识别	230
20.6 用手写笔记录和绘制	232
20.7 查错	234
20.8 更多信息	235

IV 服务 237

21 基本联网知识 239

21.1 IP 地址和路由	242
21.2 IPv6 — 下一代的因特网	245
21.3 名称解析	253
21.4 使用 YaST 配置网络连接	254
21.5 NetworkManager	274
21.6 手动配置网络连接	276
21.7 设置联接设备	290
21.8 作为拨号助手的 smpppd	294

22 网络中的 SLP 服务 297

22.1 安装	297
22.2 激活 SLP	298
22.3 SUSE Linux Enterprise Server 中的 SLP 前端	298
22.4 通过 SLP 安装	298
22.5 通过 SLP 提供服务	299
22.6 更多信息	300

23 使用 NTP 同步时间 301

23.1 使用 YaST 配置 NTP 客户端	301
23.2 手动配置网络中的 NTP	305
23.3 运行时动态时间同步	305

23.4 设置本地参考时钟	306
23.5 与外部时间参考 (ETR) 的时钟同步	307

24 域名系统 309

24.1 DNS 术语	309
24.2 安装	310
24.3 用 YaST 配置	310
24.4 启动 BIND 名称服务器	321
24.5 /etc/named.conf 配置文件	322
24.6 区域文件	326
24.7 区域数据的动态更新	330
24.8 安全事务	330
24.9 DNS 安全性	331
24.10 更多信息	332

25 DHCP 333

25.1 使用 YaST 配置 DHCP 服务器	334
25.2 DHCP 软件包	344
25.3 DHCP 服务器 dhcpcd	345
25.4 更多信息	348

26 使用 NetworkManager 349

26.1 NetworkManager 的用例	349
26.2 启用或禁用 NetworkManager	350
26.3 配置网络连接	351
26.4 使用 KNetworkManager	353
26.5 使用 GNOME NetworkManager 小程序	357
26.6 NetworkManager 和 VPN	359
26.7 NetworkManager 和安全性	361

26.8 常见问题	362
26.9 查错	363
26.10 更多信息	364
27 Samba	365
27.1 术语	365
27.2 启动和停止 Samba	367
27.3 配置 Samba 服务器	367
27.4 配置客户端	373
27.5 将 Samba 用作登录服务器	374
27.6 带有 Active Directory 的网络中的 Samba 服务器	375
27.7 有关详细信息	376
28 通过 NFS 共享文件系统	379
28.1 术语	379
28.2 安装 NFS 服务器	380
28.3 配置 NFS 服务器	380
28.4 配置客户端	387
28.5 更多信息	390
29 文件同步	393
29.1 可用的数据同步软件	393
29.2 选择程序时的决定性因素	394
29.3 CVS 简介	397
29.4 rsync 简介	399
29.5 有关详细信息	401
30 Apache HTTP 服务器	403
30.1 快速入门	403
30.2 配置 Apache	405

30.3 启动和停止 Apache	418
30.4 安装、激活和配置模块	421
30.5 使 CGI 脚本运行	428
30.6 使用 SSL 设置安全性 Web 服务器	430
30.7 避免安全性问题	436
30.8 查错	438
30.9 更多信息	439
31 使用 YaST 设置 FTP 服务器	443
31.1 启动 FTP 服务器	444
31.2 FTP 常规设置	445
31.3 FTP 性能设置	446
31.4 身份验证	446
31.5 专家设置	447
31.6 更多信息	447
32 Squid 代理服务器	449
32.1 有关代理缓存的一些事实	449
32.2 系统要求	451
32.3 启动 Squid	452
32.4 配置文件 /etc/squid/squid.conf	454
32.5 配置透明代理	459
32.6 cachemgr.cgi	461
32.7 squidGuard	463
32.8 使用 Calamaris 生成缓存报告	465
32.9 更多信息	466
33 使用 SFCB 的基于 Web 的企业管理	467
33.1 简介和基本概念	467

33.2 设置 SFCB	468
33.3 SFCB CIMOM 配置	474
33.4 高级 SFCB 任务	487
33.5 更多信息	494

V 查错 497

34 帮助和文档 499

34.1 文档目录	500
34.2 手册页	501
34.3 信息页	502
34.4 联机资源	503

35 常见问题及其解决方案 505

35.1 查找和收集信息	505
35.2 安装问题	508
35.3 引导问题	517
35.4 登录问题	519
35.5 网络问题	526
35.6 数据问题	530
35.7 IBM System z: 将 initrd 用作救援系统	543

A 网络示例 547

B GNU Licenses 549

B.1 GNU Free Documentation License	549
--	-----

关于本指南

本指南设计为由专业网络和系统管理员在操作 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：

支持任务和常见任务

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。一个可用设备技术、高可用性配置及高级管理功能的明细表向管理员介绍了该系统。

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 支持许多硬件体系结构，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。

移动计算机

便携式计算机、移动设备（如 PDA 或手机）和 SUSE Linux Enterprise 之间的通讯需要特别注意。要注意省电以及将不同设备集成到不断变化的网络环境中。同时要了解提供所需功能的后台技术。

服务

SUSE Linux Enterprise 被设计为一个网络操作系统。它提供大量网络服务（例如 DNS、DHCP、Web、代理和身份验证服务）并很好地集成到包括 MS Windows 客户端和服务器的异构环境中。

查错

概述了在需要更多信息或要用系统执行特定任务时该从何处查找帮助信息和其他文档。还可以查看最常见的问题和疑难杂症的汇编集，并了解如何自行解决这些问题。

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。

有关该产品可用文档的概述和最新文档更新，请参见 <http://www.suse.com/doc>。

1 可用文档

我们以不同的语言提供了这些手册的 HTML 和 PDF 版本。为用户和管理员提供了以下本产品的相关手册：

部署指南 (↑部署指南)

显示如何安装单个或多个系统，以及如何利用产品继承功能建立部署基础结构。有各种方法可供选择，可以选择使用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。

管理指南 [i]

涉及系统管理任务，包括维护、监视和自定义初始安装的系统。

安全指南 (↑安全指南)

介绍系统安全的基本概念，包括本地安全方面和网络安全方面。显示如何利用诸如 AppArmor（让您为每个程序指定可以读、写和执行的文件）等产品固有安全软件和审计系统（可靠地收集关于任何安全相关事件的信息）。

Security and Hardening Guide (↑*Security and Hardening Guide*)

处理安装和设置安全 SUSE Linux Enterprise Server 的特定事项以及进一步确保和强化安装所需的额外安装后步骤。支持管理员选择与安全相关的选项并做出决策。

系统分析和微调指南 (↑系统分析和微调指南)

关于问题检测、解决和优化的管理员指南。了解如何使用监视工具检查和优化系统以及如何有效管理资源。还包含常见问题和解决方案的概述以及其他帮助和文档资源。

Xen 虚拟化 (↑Xen 虚拟化)

提供了有关该产品虚拟化技术的简介。它是对应用程序各个字段以及 SUSE Linux Enterprise Server 支持的每个平台安装类型的概述，以及对安装过程的简短描述。

Virtualization with KVM for IBM System z (↑*Virtualization with KVM for IBM System z*)

提供了有关在 SUSE Linux Enterprise Server 上设置和管理 KVM（Kernel-based Virtual Machine，基于内核的虚拟机）虚拟化的简介。了解如何使用 libvirt 或 QEMU 管理 KVM。此指南还包含有关要求、限制和支持状态的详细信息。

AutoYaST (↑*AutoYaST*)

AutoYaST 是使用包含安装和配置数据的 AutoYaST 配置文件自动安装一个或多个 SUSE Linux Enterprise 系统而无需用户干预的系统。该手册将引导您完成自动安装的基本步骤，包括准备、安装和配置。

储存管理指南 (↑*储存管理指南*)

提供了关于如何管理 SUSE Linux Enterprise Server 上的储存设备的信息。

除了综合性手册，还提供几个快速入门指南：

安装快速入门 (↑*安装快速入门*)

列出系统要求，并指导您从 DVD 或 ISO 映像逐步安装 SUSE Linux Enterprise Server。

Linux 审计快速入门

概述如何启用和配置审计系统以及如何执行关键任务（如设置审计规则、生成报告和分析日志文件）。

AppArmor 快速入门

帮助您了解 AppArmor® 背后的主要概念。

Virtualization with Linux Containers (LXC) (↑*Virtualization with Linux Containers (LXC)*)

简要介绍了 LXC（轻量级“虚拟化”方法）并显示如何设置 LXC 主机和 LXC 容器。

在 `/usr/share/doc/manual` 下的已安装系统中或者桌面的帮助中心中可以找到大多数产品手册的 HTML 版本。在 <http://www.suse.com/doc>（您可从该处下载产品手册的 PDF 或 HTML 版本）上查找最新的文档更新。

2 反馈

提供了多种反馈渠道：

Bug 和增强请求

有关产品可用的服务和支持选项，请参见 <http://www.suse.com/support/>。

要报告产品组件的 bug，请从 <http://www.suse.com/support/> 登录 Novell Customer Center，然后选择 *我的支持 > 服务请求*。

用户意见

我们希望收到您对本手册和本产品中包含的其他文档的意见和建议。请使用联机文档每页底部的“用户注释”功能或转到 <http://www.suse.com/doc/feedback.html> 并在此处输入注释。

邮件

如有对本产品文档的反馈，也可以发送邮件至 doc-team@suse.de。请确保反馈中含有文档标题、产品版本和文档发布日期。要报告错误或给出增强建议，请提供问题的简要说明并指出相应章节编号和页码（或 URL）。

3 文档约定

以下是本手册中使用的版式约定：

- `/etc/passwd`：目录名称和文件名
- `placeholder`：将 `placeholder` 替换为实际值
- `PATH`：环境变量 `PATH`
- `ls`、`--help`：命令、选项和参数
- `user`：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

- **► amd64 em64t ipf:** 本段仅与体系结构 amd64、em64t 和 ipf 相关。箭头标记文本块的开始位置和结束位置。 ◀
- **► ipseries zseries:** 本段仅与体系结构 System z 和 ipseries 相关。箭头标记文本块的开始位置和结束位置。 ◀
- *跳舞的企鹅*（*企鹅*一章，↑ 其他手册）：这是对其他手册中的某章的参考。

部分 I. 支持任务和常见任务

YaST 联机更新

Novell 会一直为您的产品提供软件安全性更新。默认情况下，用更新小程序来保持您的系统是最新的。有关更新小程序的更多信息请参考第 9.4 节“保持系统最新”(第 9 章 *安装或删除软件*, ↑ *部署指南*)。本章涵盖用于更新软件包的备用工具：YaST 联机更新。

可以从软件更新安装源中获取 SUSE® Linux Enterprise Server 的最新增补程序。如果安装时已注册您的产品，则更新安装源已配置。如果未注册 SUSE Linux Enterprise Server，可通过运行 YaST 中的 **软件 > 联机更新配置** 来执行此操作，也可启动 **高级 > 注册** 以获取支持并获取更新安装源。或者，可以从信任的源中手动添加更新安装源。要添加或删除安装源，请使用 YaST 中的 **软件 > 软件安装源** 来启动安装源管理器。请在第 9.3 节“管理软件安装源和服务”(第 9 章 *安装或删除软件*, ↑ *部署指南*) 中了解更多有关安装源管理器的内容。

注意：访问更新编目时出错

如果您不能访问更新编目，可能是由于订购已过期。通常，SUSE Linux Enterprise Server 的订阅期为一年或三年，在此期间您可以访问更新编目。订购结束后，将拒绝您访问更新编目。

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

Novell 提供了不同相关性级别的更新：

安全性更新

修复严重的安全性危害，请务必安装。

推荐更新
修复可能危及计算机安全的问题。

可选更新
修复非安全性相关的问题或提供增强功能。

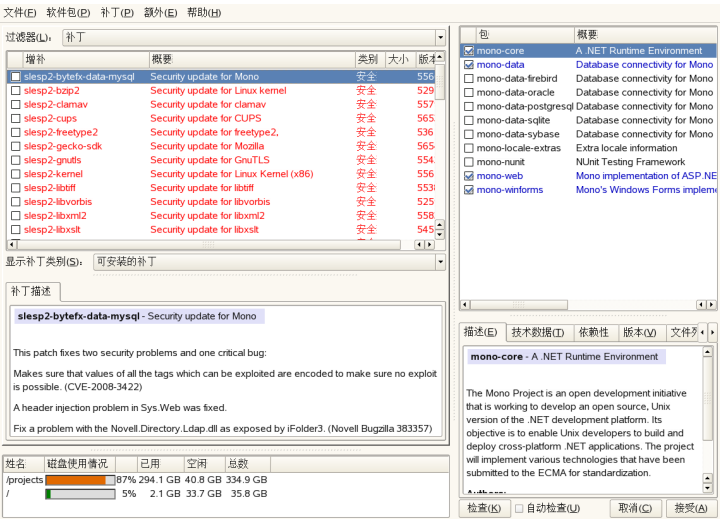
1.1 联机更新对话框

YaST 联机更新对话框以两种工具箱风格提供：GTK（适用GNOME）和Qt（适用KDE）。这两种界面在外观上有区别，但基本功能相同。以下部分简单介绍了每种界面。要打开对话框，请启动 YaST，并选择软件> 联机更新。也可以从命令行输入 `yast2 online_update` 来启动该对话框。

1.1.1 KDE 界面 (Qt)

联机更新窗口由四部分组成。

图 1.1 YaST 联机更新 — Qt 界面



左侧的摘要部分列出 SUSE Linux Enterprise Server 可用的增补程序。增补程序按安全相关性（安全性、推荐和可选）排序。您可以从显示增补程序类别中选择以下某个选项来更改摘要部分的视图：

需要的增补程序（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。

不需要的增补程序

适用于系统上未安装的包的增补程序，或要求已满足的增补程序（因为已从另一源对相关包进行了更新）。

所有增补程序

SUSE Linux Enterprise Server 可用的所有增补程序。

摘要部分的每个列表项都由符号和增补程序名称组成。如需了解可能符号及其含义的概述，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 *自动安装*、*自动更新*和*自动删除*。

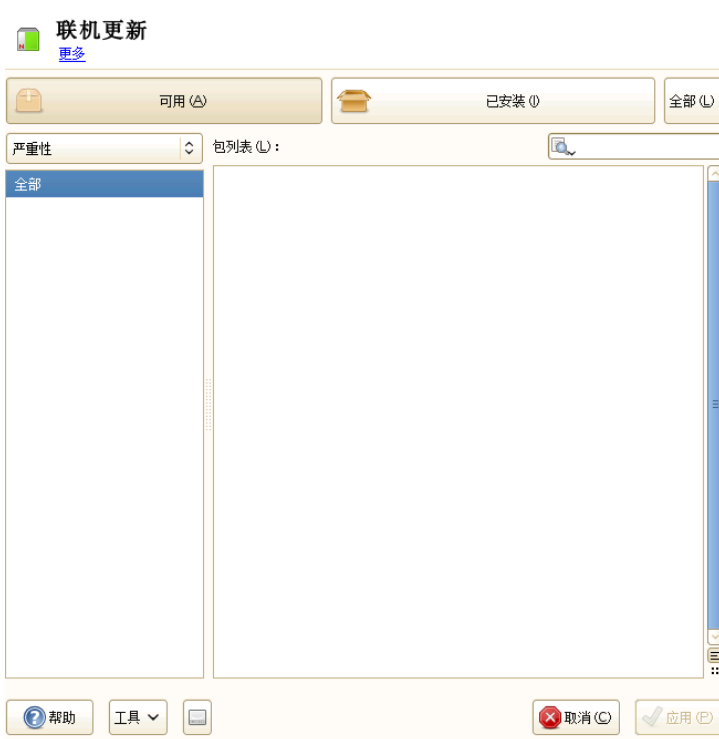
如果从非更新安装源的某个安装源安装最新包，此安装可能满足此包的某个增补程序的要求。在这种情况下，在增补程序摘要前会显示一个复选标记。该增补程序将显示在列表中，直到将其标记用于安装。这实际上不会安装增补程序（因为该包已经是最新的），而是将该增补程序标记为已安装。

在摘要部分选择一个项，可在对话框左下角的增补程序描述中查看简短描述。右上部分列出所选增补程序中包含的包（一个增补程序可以由多个包组成）。单击右上部分中的项可以查看有关增补程序中包含的各个包的细节。

1.1.2 GNOME 界面 (GTK)

联机更新窗口由四个主要部分组成。

图 1.2 YaST 联机更新 — GTK 界面



右上部分列出 SUSE Linux Enterprise Server 可用（或已安装的）增补程序。要根据安全相关性过滤增补程序，请在窗口左上部分单击相应的优先级项：安全性、推荐、可选或所有增补程序。

如果所有可用的增补程序都已安装，右上部分的包列表将不显示任何项。左下部分的框显示可用增补程序和已安装增补程序的数目，并且允许您切换到可用或已安装增补程序对应的视图。

在包列表部分选择一个项，可在对话框右下角查看增补程序描述和更多细节。由于一个增补程序可以由多个包组成，单击右下部分的适用于项可以查看相应增补程序中包含哪些包。

单击某个增补程序项将在窗口底部打开有关此增补程序详细信息的那一行。您可以在此处查看详细的增补程序描述以及可用的版本。您还可以选择安装可选增补程序（安全性和推荐增补程序已在安装时预选）。

1.2 安装增补程序

YaST“联机更新”对话框允许您一次性安装所有可用的增补程序，或者也可以手动选择要应用于系统的增补程序。还可以还原已应用于系统的增补程序。

默认情况下，您的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。一旦您单击接受或应用，将自动应用它们。

过程 1.1 使用 YaST 联机更新应用增补程序

- 1 启动 YaST，并选择软件 > 联机更新。
- 2 要自动应用您的系统当前可用的所有新增补程序（除了可选增补程序外），请单击应用或接受以启动预选择增补程序的安装过程。
- 3 先修改要应用的增补程序选择：
 - 3a 使用 GTK 和 Qt 界面分别提供的过滤器和视图。有关细节，请参见第 1.1.1 节“KDE 界面 (Qt)” [4] 和第 1.1.2 节“GNOME 界面 (GTK)” [5]。
 - 3b 按照您的需要和喜好激活或停用相应复选框 (GNOME) 或右键单击增补程序并从环境菜单选择相应操作 (KDE)，来选择或取消选择增补程序。

重要：始终应用安全性更新

但是，如果没有合理的理由，请不要取消选择任何安全性相关的增补程序。安全性增补程序修复严重的安全性危害，防止系统遭受攻击。

- 3c 多数增补程序包含几个包的更新。如果要更改单个包的操作，请右键单击包视图中的包，并选择一项操作 (KDE)。
 - 3d 要确认您的选择并应用所选增补程序，请单击应用或接受继续操作。
- 4 安装完成后，单击完成退出 YaST 联机更新。您的系统现在已是最新的了。

提示：禁用 **deltarpm**

默认情况下，更新会作为 **deltarpm**s 下载。由于从 **deltarpm** 重构建 **rpm** 包是一项需要大量内存和 CPU 时间的任务，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`。

1.3 自动联机更新

YaST 还提供设置每日、每周或每月自动更新的功能。要使用相应模块，需要先安装 `yast2-online-update-configuration` 包。

过程 1.2 配置自动联机更新

- 1 安装后，启动 YaST，并选择 **软件 > 联机更新配置**。

也可以从命令行输入 `yast2 online_update_configuration` 来启动该模块。

- 2 激活 *自动联机更新*。
- 3 选择是 *每日*、*每周* 还是 *每月* 更新。

某些增补程序（如需要许可协议的内核更新或包）需要用户交互，这可能会导致自动更新过程停止。

- 4 如果希望更新过程完全自动执行，请选择是否要 *跳过交互式增补程序*。

重要：跳过增补程序

如果选择跳过任何需要交互的包，请时常运行 *手动联机更新* 以同样安装这些增补程序。否则可能会错过重要的增补程序。

- 5 要自动接受任何许可协议，请激活 *同意许可证*。
- 6 要自动安装更新包推荐的所有软件包，请激活 *包含推荐的软件包*。

- 7 要按照类别（例如安全性或推荐）过滤增补程序，请激活*按类别过滤*，并从列表中添加适当的增补程序类别。只会安装选中类别的增补程序，而将跳过其他类别的增补程序。
- 8 单击*确定*确认您的配置。

收集用于支持的系统信息

如果遇到问题，可能会使用 `supportconfig` 命令创建系统报告。此工具会收集系统的相关信息，包括当前内核版本、硬件、已安装包、分区设置及其他信息。此报告可帮助 Novell 技术服务团队协助您解决所报告的问题或找到原因所在。该命令由默认安装包 `supportutils` 提供。

2.1 概述

Novell Support Link (NSL) 对 SUSE Linux Enterprise Server 来说是全新的。它是一种收集系统信息并允许您将收集到的数据上载到另一台服务器以供进一步分析的工具。

Novell Support Link 有两种使用方法：

1. 使用 YaST 支持模块。
2. 使用命令行实用程序 `supportconfig`。

YaST 支持模块调用 `supportconfig` 来收集系统信息。

2.2 使用 `Supportconfig` 收集信息

以下各节描述了如何在 YaST 中通过命令行以及可供选择的其他选项使用 `supportconfig`。

2.2.1 使用 YaST

要使用 YaST 收集系统信息，请如下操作：

- 1 打开 URL <http://www.novell.com/center/eservice> 并创建服务请求编号。
- 2 启动 YaST。
- 3 打开支持模块。
- 4 单击 *创建报告 tarball*。
- 5 从单选按钮列表选择一个选项。如果要先进行测试，请使用 *仅收集最少量的信息*。按 *下一步继续*。
- 6 输入您的联系信息。使用步骤 1 [12] 中的服务请求编号，并将其输入标为 *Novell 11 位服务请求编号* 的文本字段中。按 *下一步继续*。
- 7 开始收集信息。该过程完成后，按 *下一步继续*。
- 8 查看数据集合。按 *下一步继续*。
- 9 保存 tarball。如果要上载到 Novell customer center，请确保将日志文件 *tarball* 上载到 URL 中已激活。使用 *下一步完成操作*。

2.2.2 直接使用 Supportconfig

要从命令行使用 supportconfig，请执行如下操作：

- 1 打开外壳并转换为 root 用户。
- 2 运行 supportconfig，不使用任何选项。这会收集默认的系统信息。
- 3 等待工具完成操作。
- 4 默认的存档位置为 /var/log，文件名格式为 `nts_HOST_DATE_TIME.tbz`

2.2.3 常用的 supportconfig 选项

supportconfig 实用程序在调用时通常不带任何选项。使用 supportconfig --help 显示所有选项的列表或参见手册页。以下列表对更加常用的案例进行了简述：

- 使用最小选项 (-m) 来减少所收集的信息量：

```
supportconfig -m
```

- 在输出中包含附加的联系人信息（在一行中）：

```
supportconfig -E tux@example.org -N "Tux Penguin" -O "Penguin Inc." ...
```

- 针对某个问题进行查错时，可能您只想收集关于当前所研究问题领域的信息。例如，如果 LVM 出了问题，并且最近在默认 supportconfig 输出中发现了该问题。作出更改后，您想要收集最新的 LVM 信息。以下命令将收集最少的 supportconfig 信息，且仅 LVM 信息。

```
supportconfig -i LVM
```

要查看完整的功能列表，请运行：

```
supportconfig -F
```

如果您需要相反的区域，可使用 -x 选项来排除区域。可以结合使用 -i 和 -x 两个选项。

- 收集已经过轮换的日志文件。在日志记录较多的环境下或当重引导后 syslog 轮换日志时发生内核崩溃的情况下，此项功能尤为有用。

```
supportconfig -l
```

2.3 向 Novell 提交信息

您可以使用 YaST 支持模块或 supportconfig 命令行实用程序向 Novell 提交系统信息。当发生服务器问题，且希望获得 Novell 帮助，您需要打开一个服务请求，然后向 Novell 提交服务器信息。以下描述了 YaST 和命令行两种方法。

注意：隐私声明

Novell 将系统报告视为机密数据。有关详细信息，请转到 <http://www.novell.com/company/legal/privacy/> 参见我们的隐私承诺。

过程 2.1 通过 YaST 向 Novell 提交信息

- 1 打开 URL <http://www.novell.com/center/eservice> 并创建服务请求编号。
- 2 写下 11 位服务请求编号。以下示例中将假设该服务请求编号为 12345678901。
- 3 在 YaST 支持模块窗口中单击创建报告 *tarball*。
- 4 选择使用自定义单选按钮。按下一步继续。
- 5 输入联系人信息，填写 *Novell 11 位服务请求编号*，并包含 Novell 的上载目标 URL。
 - 对于安全上载目标，请使用：<https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}>。
 - 对于常规的 FTP 上载目标，请使用 <ftp://ftp.novell.com/incoming>（美国地区客户）或 <ftp://support-ftp.suse.com/in>（欧洲、中东和非洲地区客户）。

按下一步继续。信息收集开始。该过程完成后，按下一步继续。

- 6 查看收集的数据，并使用从数据中删除来删除要上载到 Novell 的 *tarball* 中排除的任何文件。按下一步继续。
- 7 默认情况下，*tarball* 的副本将保存到 `/root` 下。确认您使用的 Novell 上载目标为以上所述之一，且将日志文件 *tarball* 上载到 URL 中已激活。按下一步完成。
- 8 单击完成。

过程 2.2 通过 *supportconfig* 向 Novell 提交信息

- 1 打开 URL <http://www.novell.com/center/eservice> 并创建服务请求编号。

2 写下 11 位服务请求编号。以下示例中将假设该服务请求编号为 12345678901。

3 具有因特网连接的服务器：

3a 要使用默认上载目标，请运行：

```
supportconfig -ur 12345678901
```

3b 对于安全上载目标，请在同一行中使用以下命令：

```
supportconfig -r 12345678901 -U  
'https://secure-www.novell.com/upload?appname=supportconfig&file={tarball}'
```

4 不具有因特网连接的服务器：

4a 运行以下命令：

```
supportconfig -r 12345678901
```

4b 手动将 `/var/log/nts_SR12345678901*tbz tarball` 上载到我们的 FTP 服务器（美国地区客户请使用 <ftp://ftp.novell.com/incoming>；欧洲、中东和非洲地区客户请使用 <ftp://support-ftp.suse.com/in>）。

4c 也可以使用服务请求 URL <http://www.novell.com/center/eservice> 将 `tarball` 附加到您的服务请求。

5 一旦 `tarball` 上载到我们 FTP 服务器的接收目录，它就会自动附加到您的服务请求中。

2.4 更多信息

请在以下文档中查找关于收集系统信息的更多信息：

- `man supportconfig` — `supportconfig` 的手册页
- `man supportconfig.conf`—`supportconfig` 配置文件的手册页

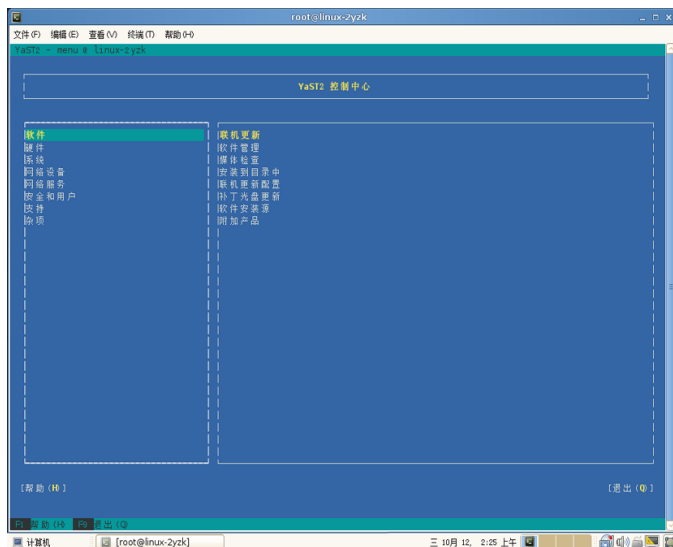
- <http://www.novell.com/communities/print/node/4097> — 使用 supportconfig 检查基本服务器运行状况
- <http://www.novell.com/communities/print/node/4827> — 创建自己的 supportconfig 插件
- <http://www.novell.com/communities/print/node/4800> — 创建中心 supportconfig 安装源

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。

文本模式的 YaST 使用 ncurses 库提供简单的伪图形用户界面。默认情况下已安装 ncurses 库。用于运行 YaST 的终端仿真器支持的最小大小为 80x25 个字符。

图 3.1 文本方式下 YaST 的主窗口



以文本模式启动 YaST 时，会显示“YaST 控制中心”（请参见图 3.1）。该窗口包含三个区域。左侧方框中显示各种模块所属的类别。此方框在 YaST 启动后处于活动状态，因此以白色粗边框进行标记。活动类别处于高亮显示状态。右侧方框提供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。

启动“YaST 控制中心”时，类别软件将自动处于选中状态。使用 ↓ 键和 ↑ 键可更改类别。要从类别中选择某个模块，请使用 → 激活右侧方框，然后使用 ↓ 和 ↑ 选择此模块。按住箭头键在可用模块列表中滚动。选择的模块将高亮显示。按 Enter 启动活动模块。

模块中的各种按钮和选择字段包含一个高亮显示的字母（默认为黄色）。使用 Alt + **highlighted_letter** 可直接选择按钮，而无需使用 Tab 键导航。通过按 Alt + Q 组合键或选择 *退出* 并按 Enter 退出 YaST 控制中心。

提示：刷新 YaST 对话框窗口

如果 YaST 对话框窗口损坏或变形（例如在调整窗口大小时），请按 Ctrl + L 来刷新并恢复其内容。

3.1 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 3.2 节“组合键的限制” [19]。

在按钮和选择列表中导航

使用 Tab 键在按钮和包含选择列表的框架之间导航。要以相反顺序导航，请使用 Alt + Tab 键或 Shift + Tab 组合。

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 ← 会导致更改活动方框或当前选择列表（如同在“控制中心”中），也可以使用此组合键。

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。或者，可以使用 Alt + **highlighted_letter** 直接选择单选按钮和复

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。

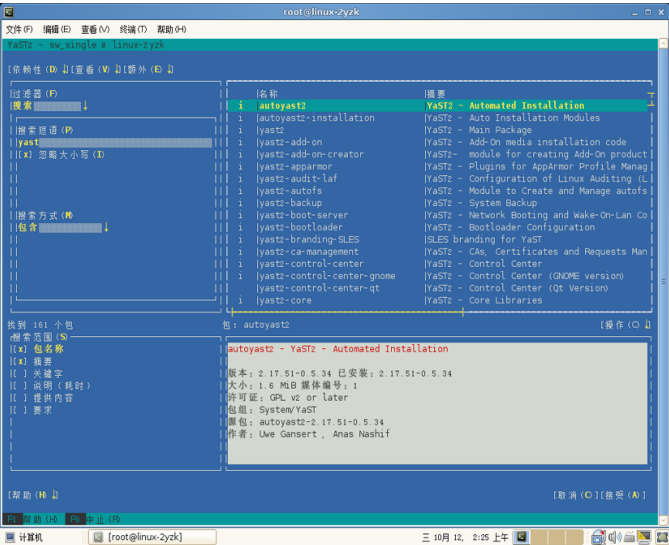
功能密钥

使用 **F** 键（**F1** 到 **F12**）可快速访问各种按钮。YaST 屏幕底部行中显示可用的 **F** 键快捷方式。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（“细节”、“信息”、“添加”、“删除”等）。可以将 **F10** 用作接受、确定、下一步和完成。按 **F1** 可访问 YaST 帮助。

在 ncurses 方式中使用导航树

某些 YaST 模块使用窗口左侧的导航树选择配置对话框。使用箭头键（**↑** 和 **↓**）在树中导航。使用空格键打开或关闭树中的项。在 ncurses 方式中，在导航树中进行选择之后必须按 **Enter** 键，才能显示所选对话框。这是一种有意行为，目的是在浏览导航树时避免耗时的重绘。

图 3.2 软件安装模块



3.2 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**

可以代替 **Alt** 而使用 **EscAlt** 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** 组合键由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。

3.3 YaST 命令行选项

除了文本方式界面之外，**YaST** 还提供了一个纯命令行界面。要获取 **YaST** 命令行选项列表，请输入：

```
yast -h
```

3.3.1 启动单个模块

为了节省时间，可以直接启动单个 **YaST** 模块。要启动模块，请输入：

```
yast <module_name>
```

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`。例如，要启动网络模块，请输入 `yast lan`。

3.3.2 从命令行安装包

如果知道包名称且包是由您的任何活动安装源提供的，则可以使用命令行选项 `-i` 安装该包：

```
yast -i <package_name>
```

或

```
yast --install <package_name>
```

package_name 可以是一个简短的包名称（例如 `gvim`，这是使用依赖性检查安装的），也可以是 `rpm` 包的完整路径（这是不使用依赖性检查安装的）。

如果需要具有 YaST 未提供的功能的，基于命令行的软件管理实用程序，请考虑使用 `zypper`。这个新实用程序使用相同的软件管理库，这也是 YaST 包管理器的基础。第 6.1 节“使用 Zypper”[47] 中涵盖了 `zypper` 的基本用法。

3.3.3 YaST 模块的命令行参数

为了在脚本中使用 YaST 功能，YaST 提供了对单个模块的命令行支持。并非所有模块都具有命令行支持。要显示某个模块的可用选项，请输入：

```
yast <module_name> help
```

如果模块不提供命令行支持，将以文本方式启动，并显示以下消息：

```
This YaST module does not support the command line interface.
```


使用快照程序生成快照/实现回滚

能够生成文件系统快照以便在 Linux 上实现回滚，这是过去常常要求提供的功能。如今，快照程序与 Btrfs 文件系统或精简的 LVM 卷相结合，填补了这一空白。

Btrfs 是全新的 Linux 写入时复制文件系统。它支持为子卷（每个物理分区中的一或多个单独的可装入文件系统）生成文件系统快照（复制子卷在某个时间点的状态）。您可以使用快照程序对这些快照进行管理。快照程序提供命令行和 YaST 界面。

默认情况下，会在 SUSE Linux Enterprise Server 上设置快照程序和 Btrfs，以供在使用 YaST 和 zypper 更改系统时作为“撤销工具”使用。将在运行 YaST 模块或 zypper 的之前和之后创建快照。快照程序可让您对这两张快照进行比较，并在两张快照之间存在差异时提供还原方法。您还可以使用这些工具按小时创建系统子卷的快照，以实现系统备份。

4.1 要求

由于 Btrfs 是 SUSE Linux Enterprise Server 上唯一支持快照的文件系统，所以想要生成“快照”的所有分区或子卷上都需要设置它。

4.1.1 快照和磁盘空间

创建快照时，快照与原始点都会指向文件系统中的同一个块。因此一开始时快照并不占用额外的磁盘空间。但如果修改了原始文件系统中的数据，则会复制

已更改的数据块，同时将旧的数据块作为快照保留。因此，快照就将占用与已修改数据相同的空间。所以久而久之，分配给快照的空间便会不断增长。其结果是，即便从包含快照的 Btrfs 文件系统删除文件可能也不会释放磁盘空间！

注意：快照存储位置

快照始终驻留在“生成快照”的同一个分区或子卷，而无法将快照存储到其他分区或子卷。

因此，包含快照的分区需要比“常规”分区大才行。确切的空间大小主要取决于要保留的快照数量以及数据更改量。一般来说，您应考虑使用两倍于常规使用磁盘空间的空间大小。

提示：释放磁盘空间/磁盘用量

为了释放包含快照的 Btrfs 分区的磁盘空间，您需要删除不再需要的快照，而不是文件。旧快照比新快照占用的磁盘空间更多。

因为 `df` 不会显示 Btrfs 文件系统上的正确磁盘用量，所以您需要使用命令 `btrfs filesystem df 安装点`。目前，Btrfs 工具还不支持显示分配给快照的磁盘空间大小。

升级服务包时，由于会更改大量数据（包更新），将导致快照占用大量系统子卷的磁盘空间。因此对于不再需要的快照，建议执行手动删除。

快照程序也可以用来在以 ext3 或 XFS 格式化的精简 LVM 卷上创建和管理快照（参见第 4.6 节“在精简的 LVM 卷上使用快照程序”[40]）。

4.2 使用快照程序撤销系统更改

&productname 上的快照程序经过预配置，可以用来撤销 zypper 和 YaST 所做更改。要实现此功能，请对快照程序进行配置，使其在每次运行 zypper 和 YaST 的前后创建一个快照对。您也可以使用快照程序来恢复被意外删除或修改的系统文件。要实现此功能需按小时创建备份。

默认情况下，上述的自动快照针对根分区及其子卷所配置。若想让 /home 等其他分区也可以生成快照，您可以创建自定义配置。

4.2.1 撤销 YaST 和 zypper 更改

如果在安装时使用 `Btrfs` 设置根分区，则将自动安装快照程序（经过预配置，支持对 YaST 或 zypper 的更改执行回滚）。每次启动 YaST 模块或 zypper 事务时，会创建两张快照：即截获模块启动之前文件系统状态的“前快照”以及截获模块完成之后状态的“后快照”。

您可以使用 YaST 快照程序模块或 `snapper` 命令行工具，通过从“前快照”恢复文件来撤销 YaST 或 zypper 所做的更改。您也可以使用该工具比较这两张快照，以查看更改了哪些文件。您还可以显示文件的两个版本之间的差异 (`diff`)。

由于 Linux 是多任务系统，因此可能还会有 YaST 或 zypper 以外的其他进程在前快照与后快照之间的时间段内对数据进行修改。如果是这种情况，完全还原至前快照也将撤销由其他进程所做的更改。大多数情况下，这是不需要的，因此强烈建议您在开始回滚之前仔细查看两张快照之间的更改。如果需要保留其他进程所做的更改，则选择要回滚到的文件。

重要：限制

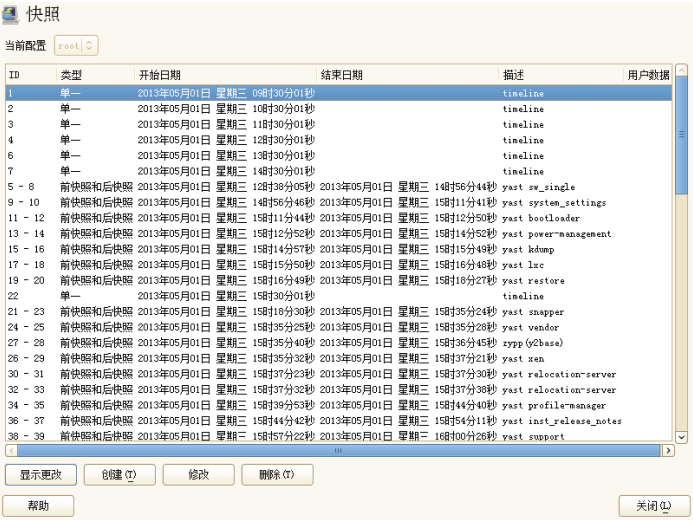
在尝试使用快照程序的回滚机制之前，请务必了解快照程序的限制。有关详细信息，请参见第 4.4 节“限制”[38]。

注意：快照的存储时间

默认情况下，会保留最后的 100 个 YaST 和 zypper 快照。如果超过这一数值，将删除最旧的快照。

过程 4.1 使用 YaST 快照程序模块撤销更改

- 1 从 YaST 中的其他部分或通过输入 `yast2 snapper` 来启动快照程序模块。
- 2 务必将当前配置设置为根。除非手动添加自己的快照程序配置，否则请始终做此设置。
- 3 从列表中选择前后快照对。YaST 和 zypper 快照对都属于前后类型。在说明栏中，YaST 快照以 `yast 模块名称` 标记；zypper 快照以 `zypp (zypper)` 标记。



4 单击**显示更改**，会打开一个文件列表显示两张快照之间的差异。下图显示添加用户 `tester` 后发生更改的文件列表。



5 查看文件列表。要显示文件的前后版本之间的“差异”，请从列表选中该文件。下图显示添加用户 `tester` 之后 `/etc/passwd` 发生的更改。



6 要恢复一组文件，请通过勾选相应的复选框选择相关的文件或目录。单击恢复选定，然后单击是以确认该操作。



要恢复单一文件，请单击其名称以激活该文件的差异视图。单击从第一个快照恢复，然后单击是以予以确认。

过程 4.2 使用 *snapper* 命令撤销更改

- 1 运行 `snapper list -t pre-post` 以获取 YaST 与 `zypper` 快照的列表。在说明栏中，YaST 快照以 `yast` 模块名称标记；`zypper` 快照以 `zypp` (`zypper`) 标记。

```
~ # snapper list -t pre-post
  Pre # | Post # | Pre Date                    | Post Date                    | Description
-----+-----+-----+-----+-----+
    4   |    5   | Tue Jan 10 14:39:14 2012    | Tue Jan 10 14:39:33 2012    | yast system_settings
    65   |   66   | Thu Jan 12 17:18:10 2012    | Thu Jan 12 17:18:23 2012    | zypp(zypper)
    68   |   69   | Thu Jan 12 17:25:46 2012    | Thu Jan 12 17:27:09 2012    | zypp(zypper)
    73   |   74   | Thu Jan 12 17:32:55 2012    | Thu Jan 12 17:33:13 2012    | yast system_settings
    75   |   76   | Thu Jan 12 17:33:56 2012    | Thu Jan 12 17:34:42 2012    | yast users
    77   |   92   | Thu Jan 12 17:38:36 2012    | Thu Jan 12 23:13:13 2012    | yast snapper
    83   |   84   | Thu Jan 12 22:10:33 2012    | Thu Jan 12 22:10:39 2012    | zypp(zypper)
    85   |   86   | Thu Jan 12 22:16:58 2012    | Thu Jan 12 22:17:09 2012    | zypp(zypper)
    88   |   89   | Thu Jan 12 23:10:42 2012    | Thu Jan 12 23:10:46 2012    | zypp(zypper)
    90   |   91   | Thu Jan 12 23:11:40 2012    | Thu Jan 12 23:11:42 2012    | zypp(zypper)
   108   |  109   | Fri Jan 13 13:01:06 2012    | Fri Jan 13 13:01:10 2012    | zypp(zypper)
```

- 2 使用 `snapper status 前..后` 命令以获取快照对的已更改文件列表。文件内容发生了更改会以 `c` 标记、添加了文件会以 `+` 标记、删除了文件会以 `-` 标记。以下示例显示安装 `ncftp` 包的快照对。

```
~ # snapper status 108..109
+... /usr/bin/ncftp
+... /usr/bin/ncftpbatch
+... /usr/bin/ncftpget
+... /usr/bin/ncftpls
[...]
```

```
+... /usr/share/man/man1/ncftpspooler.1.gz
c... /var/cache/zypp/solv/@System/cookie
c... /var/cache/zypp/solv/@System/solv
c... /var/lib/rpm/Basenames
c... /var/lib/rpm/Dirnames
c... /var/lib/rpm/Filemd5s
c... /var/lib/rpm/Group
c... /var/lib/rpm/Installtid
c... /var/lib/rpm/Name
c... /var/lib/rpm/Packages
c... /var/lib/rpm/Providename
c... /var/lib/rpm/Provideversion
c... /var/lib/rpm/Requirename
c... /var/lib/rpm/Requireversion
c... /var/lib/rpm/Shalheader
c... /var/lib/rpm/Sigmd5
c... /var/lib/zypp/SoftLocks
```

- 3** 要显示某份文件的差异，请运行 `snapper diff 前..后 文件名`。如果没有指定文件名，则会显示所有文件的差异。

```
~ # snapper diff 108..109 /var/lib/zypp/SoftLocks
--- /.snapshots/108/snapshot/var/lib/zypp/SoftLocks 2012-01-12
23:15:22.408009164 +0100
+++ /.snapshots/109/snapshot/var/lib/zypp/SoftLocks 2012-01-13
13:01:08.724009131 +0100
@@ -1,4 +1,2 @@
-# zypp::SoftLocksFile generated Thu Jan 12 23:10:46 2012
-#
-ncftp
-#
+# zypp::SoftLocksFile generated Fri Jan 13 13:01:08 2012
+##
```

- 4** 要恢复一或多份文件，请运行 `snapper -v undochange 前..后 文件名`。如果没有指定文件名，则会恢复所有已更改的文件。

```
~ # snapper -v undochange 108..109
create:0 modify:16 delete:21
undoing change...
deleting /usr/share/man/man1/ncftpspooler.1.gz
deleting /usr/share/man/man1/ncftpput.1.gz
[...]
deleting /usr/bin/ncftpls
deleting /usr/bin/ncftpget
deleting /usr/bin/ncftpbatch
deleting /usr/bin/ncftp
modifying /var/cache/zypp/solv/@System/cookie
modifying /var/cache/zypp/solv/@System/solv
modifying /var/lib/rpm/Basenames
modifying /var/lib/rpm/Dirnames
modifying /var/lib/rpm/Filemd5s
modifying /var/lib/rpm/Group
modifying /var/lib/rpm/Installtid
modifying /var/lib/rpm/Name
modifying /var/lib/rpm/Packages
modifying /var/lib/rpm/Providename
modifying /var/lib/rpm/Provideversion
modifying /var/lib/rpm/Requirename
modifying /var/lib/rpm/Requireversion
modifying /var/lib/rpm/Shalheader
modifying /var/lib/rpm/Sigmd5
modifying /var/lib/zypp/SoftLocks
undoing change done
```

4.2.2 使用快照程序从每小时备份恢复文件

除了 YaST 和 zypper 快照外，快照程序还会按小时创建系统分区 (/) 的快照。您可以使用这些备份快照来恢复被意外删除或修改而无法恢复的文件。您也可以使用快照程序的差异功能来找到在某个时间点所做的修改。

每小时备份快照属于单一类型，并标有时间线说明。要从这些快照恢复文件，请按照过程 4.1, “使用 YaST 快照程序模块撤销更改” [25]或过程 4.2, “使用 snapper 命令撤销更改” [28]中的说明操作。

注意：快照的存储时间

默认情况下，会保留最近十天、最近十个月以及最近十年的首张快照。有关详细信息，请参见例 4.1 “时间线配置示例” [32]。

4.2.3 创建并修改快照程序配置

每一个分区或 Btrfs 子卷都有一个专用的配置文件用于定义快照程序的行为方式。这些配置文件位于 /etc/snapper/configs/ 下。使用快照程序为 / 目录安装的默认配置以 root 命名。它负责创建并管理 YaST 和 zypper 快照，还包括 / 的每小时备份快照。

您可以为使用 Btrfs 格式化的其他分区或 Btrfs 分区上的现有子卷创建自己的配置。在以下示例中，我们将设置快照程序配置，以便对驻留在单独的、以 Btrfs 格式化且安装点为 /srv/www 的分区的 Web 服务器数据进行备份。

您可以使用 snapper 本身或 YaST 的快照程序模块来从这些快照恢复文件。在 YaST 中，您需要选择您的当前配置，同时还需要使用全局开关 -c（例如 snapper -c myconfig list）指定 snapper 的配置。

要创建新的快照程序配置，请运行 snapper create-config:

```
snapper -c www-data❶ create-config  
/srv/www❷
```

- ❶ 配置文件的名称。
- ❷ 分区或 Btrfs 子卷生成快照的安装点。

此命令将使用合理的默认值（取自 `/etc/snapper/config-templates/default`）创建新的配置文件 `/etc/snapper/config-templates/www-data`。

提示：配置默认值

新配置的默认值取自 `/etc/snapper/config-templates/default`。要使用自己的一组默认值，请在相同的目录中创建此文件的副本然后按照需要进行调整。要使用此功能，请在 `create-config` 命令中指定 `-t` 选项：

```
snapper -c www-data create-config -t my_defaults /srv/www
```

4.2.3.1 调整配置文件

要调整配置文件，您需要使用编辑器对其进行修改。该文件中包含采用 `键=值` 格式的键/值对。只有 `值` 可更改。

SUBVOLUME

分区或子卷生成快照的安装点。不更改。

FSTYPE

分区的文件系统类型。不更改。

NUMBER_CLEANUP

定义当快照总数超出 `NUMBER_LIMIT` 中指定的数值 *同时* 快照超出 `NUMBER_MIN_AGE` 中指定的时限是否自动删除旧快照。有效值：`yes`、`no`

注意：限制和时限

`NUMBER_LIMIT` 和 `NUMBER_MIN_AGE` 始终会同时进行评估。只有同时符合这两个条件才会删除快照。如果想不考虑时限而始终保留一定数量的快照，则可将 `NUMBER_MIN_AGE` 设置为 0。另外，如果快照超过一定时限之后不想再保留，则可将 `NUMBER_LIMIT` 设置为 0。

NUMBER_LIMIT

定义当 `NUMBER_CLEANUP` 设置为 `yes` 时要保留的快照数量。

NUMBER_MIN_AGE

定义快照在自动删除前必须保留的最小时限（以秒为单位）。

TIMELINE_CREATE

如果设置为 yes，则会每小时创建一次快照。这是目前唯一的自动创建快照的方法，因此强烈建议您将其设置为 yes。有效值：yes、no

TIMELINE_CLEANUP

定义当快照数量超出 *TIMELINE_LIMIT_** 选项指定的数值*同时*快照超出 TIMELINE_MIN_AGE 中指定的时限是否自动删除旧快照。有效值：yes、no

TIMELINE_MIN_AGE

定义快照在自动删除前必须保留的最小时限（以秒为单位）。

TIMELINE_LIMIT_HOURLY、TIMELINE_LIMIT_DAILY、
TIMELINE_LIMIT_MONTHLY、TIMELINE_LIMIT_YEARLY

按小时、天、月、年保留的快照数量。

例 4.1 时间线配置示例

```
TIMELINE_CREATE="yes"
TIMELINE_CLEANUP="yes"
TIMELINE_MIN_AGE="1800"
TIMELINE_LIMIT_HOURLY="10"
TIMELINE_LIMIT_DAILY="10"
TIMELINE_LIMIT_MONTHLY="10"
TIMELINE_LIMIT_YEARLY="10"
```

此示例配置能够实现按小时生成将自动清理的快照。TIMELINE_MIN_AGE 和 TIMELINE_LIMIT_* 始终会同时进行评估。在本示例中，快照删除前的最小保留时限设置为 30 分钟（1800 秒）。因为我们会每小时创建一次快照，所以确保了只会保留最近的快照。如果 TIMELINE_LIMIT_DAILY 设置为非零值，则表示还会保留当天的首张快照。

快照保留

- 每小时：最近创建的十张快照。
- 每天：保留最近十天内每天创建的首张快照。
- 每月：保留最近十个月内每月的最后一天创建的首张快照。

- 每年：保留最后十年内每年的最后一天创建的首张快照。

4.2.3.2 以普通用户身份使用快照程序

默认情况下，只能由 `root` 用户使用快照程序。但在特定情况下，某些组或用户也需要创建快照或通过还原至快照来撤销更改：

- 网管想要生成 `/srv/www` 的快照。
- 数据库管理员想要生成数据库的快照。
- 用户想要生成其主目录的快照。

此类情况下，可以创建为用户和（或）组授予权限的快照程序配置。除了此项配置更改外，还需要将相应的 `.snapshots` 目录设置为可以让指定用户读取和访问。

过程 4.3 让普通用户可以使用快照程序

请注意，此过程中的所有步骤都需要由 `root` 运行。

- 1 如果不存在，则请为用户可以使用快照程序的分区或子卷创建快照程序配置。有关指导，请参见第 4.2.3 节“创建并修改快照程序配置”[30]。示例：

```
snapper --config web_data create /srv/www
```

- 2 在 `/etc/snapper/configs/名称` 下创建配置文件，其中“名称”为您在上一步中使用 `-c/--config` 指定的值（例如 `/etc/snapper/configs/web_data`）。按照需要进行调整；有关详细信息，请参见第 4.2.3.1 节“调整配置文件”[31]。

- 3 为 `ALLOW_USERS` 和（或）`ALLOW_GROUPS` 设置值，以分别为用户和（或）组授予权限。多个条目需要使用 `Space` 分隔。例如，要为用户 `www_admin` 授予权限，可输入：

```
ALLOW_USERS="www_admin"
```

- 4 授予对快照目录 `路径/.snapshots` 的读取和访问权限。`路径` 将被您在此过程的第一步中指定的子卷替代。示例：

```
chmod a+rx /srv/www/.snapshots
```

此时，指定的用户和（或）组便可以使用指定的快照程序配置。您可以使用 `list` 命令对其进行测试，例如：

```
www_admin:~ > snapper -c web_data list
```

4.2.4 禁用自动快照

如果您在安装期间使用 `Btrfs` 设置了根分区，则快照程序会每小时自动生成系统快照，同时生成 `YaST` 和 `zypper` 事务的前后快照。您可以禁用这些任务中的任意一个任务，方式如下：

禁用每小时快照

编辑 `/etc/snapper/configs/root` 并将 `TIMELINE_CREATE` 设置为 `no`：

```
TIMELINE_CREATE="no"
```

禁用 `zypper` 快照

卸载 `snapper-zypp-plugin` 包

禁用 `YaST` 快照

编辑 `/etc/sysconfig/yast2` 并将 `USE_SNAPPER` 设置为 `no`：

```
USE_SNAPPER="no"
```

4.3 手动创建和管理快照

通过配置，快照程序将不只限于自动创建和管理快照；您也可以使用命令行工具或 `YaST` 模块手动创建快照对（“前后”）或单个快照。

所有快照程序操作皆针对现有配置执行（有关详细信息，请参见第 4.2.3 节“创建并修改快照程序配置”[30]）。您可以只为存在配置的分区或卷生成快照。默认情况下使用系统配置 (`root`)。如果想要为自己的配置创建或管理快照，则需要明确选择。使用 `YaST` 中的 *当前配置* 下拉菜单，或在命令行上指定 `-c`（即 `snapper -c 我的配置 命令`）。

4.3.1 快照元数据

每一张快照均由快照本身以及一些元数据组成。创建快照时，您还需要指定元数据。修改快照就意味着更改其元数据—您无法修改其内容。每一张快照可以使用以下元数据：

- **类型**：快照类型，有关详细信息，请参见第 4.3.1.1 节“快照类型”[35]。不能更改此数据。
- **编号**：快照的唯一编号。不能更改此数据。
- **前编号**：指定相应前快照的编号。仅适用于后类型。不能更改此数据。
- **说明**：快照的说明。
- **用户数据**：扩展的说明。此处您可使用逗号分隔的“键=值”列表格式指定自定义数据：`reason=testing_stuff, user=tux`
- **清理算法**：快照的清理算法。有关详细信息，请参见第 4.3.1.2 节“清理算法”[36]。

4.3.1.1 快照类型

快照程序能够分清三种不同类型的快照：前快照、后快照以及单一快照。从物理上讲，这三种快照没有什么不同，但快照程序会针对不同类型采用不同的处理方式。

前

修改前的文件系统快照。每一张前快照都有一个对应的后快照。例如，YaST/zypper 自动快照。

张贴

修改后的文件系统快照。每一张后快照都有一个对应的前快照。例如，YaST/zypper 自动快照。

single

独立的快照。例如，每小时自动生成的快照。此为创建快照时的默认类型。

4.3.1.2 清理算法

快照程序提供有三种清理旧快照的算法。这些算法以每天计划作业方式执行。快照的清理频率在分区或子卷的快照程序配置中定义（有关详细信息，请参见第 4.2.3.1 节“调整配置文件”[31]）。

数量

当达到某一快照计数时将删除旧快照。

时间线

将删除超过一定时限的旧快照，但保留一定量的每小时、每天、每月和每年快照。

无差异前后快照对

将删除无差异的前后快照对。

4.3.2 创建快照

通过运行 `snapper create` 或单击 YaST 的快照程序模块中的 *创建* 来创建快照。以下示例解释了如何从命令行创建快照。使用 YaST 界面会比较简单。

提示：快照说明

为了便于日后确定快照的用途，您应始终指定有意义的说明。甚至可以通过用户数据选项指定更多信息。

```
snapper create --description "2013 年第二周快照"
```

创建默认 (root) 配置的独立快照（单一类型）并附加说明。因为没有指定清理算法，将不会自动删除快照。

```
snapper --config home create --description "在 ~tux 中清理"
```

为名为 home 的自定义配置创建独立快照（单一类型）并附加说明。因为没有指定清理算法，将不会自动删除快照。

```
snapper --config home create --description "每日数据备份"  
--cleanup-algorithm timeline
```

为名为 home 的自定义配置创建独立快照（单一类型）并附加说明。一旦符合为配置中的时间线清理算法指定的条件，便会自动删除文件。

```
snapper create --type pre--print-number--description
```

"Apache 配置清理之前"

创建前类型的快照并打印快照编号。创建用于保存“之前”和“之后”状态的快照对所需的首个命令。

```
snapper create --type post--pre-number 30--description
```

"Apache 配置清理之后"

创建后类型的快照且其对应的前快照编号为 30。创建用于保存“之前”和“之后”状态的快照对所需的第二个命令。

```
snapper create --command COMMAND--description "命令前后"
```

运行命令前后自动创建快照对。此选项仅在于命令行上使用 **snapper** 时可用。

4.3.3 修改快照元数据

您可以使用快照程序修改说明、清理算法以及快照的用户数据。其他元数据均无法更改。以下示例解释了如何从命令行修改快照。使用 YaST 界面会比较简单。

要在命令行上修改快照，您需要知道其编号。使用 `snapper list` 可显示所有快照及其编号。

YaST 的快照程序模块已列出所有快照。从列表中选择一个快照，然后单击修改。

```
snapper modify --cleanup-algorithm "timeline" 10
```

修改默认(root)配置的第 10 张快照的元数据。清理算法设置为 `timeline`。

```
snapper --config home modify --description "每日备份"
```

```
--cleanup-algorithm "timeline"120
```

修改名为 `home` 的自定义配置的第 120 张快照的元数据。将设置新的说明并取消设置清理算法。

4.3.4 删除快照

要使用 YaST 的快照程序模块删除快照，请从列表中选择快照然后单击删除。

要使用命令行工具删除快照，需要知道其编号。运行 `snapper list` 命令获取快照编号。要删除快照，请运行 `snapper delete 编号`。

提示：删除快照对

删除前快照时，您应始终删除与其对应的后快照（反之亦然）。

```
snapper delete 65
```

删除默认 (root) 配置的第 65 张快照。

```
snapper -c home delete 89 90
```

删除名为 home 的自定义配置的第 89 张和第 90 张快照。

提示：旧快照占用的磁盘空间更多

如果您要删除快照以释放硬盘上的空间（有关详细信息，请参见第 4.1.1 节“快照和磁盘空间” [23]），请务必首先删除旧快照。快照生成的时间越长，其占用的空间就越大。

也可以通过每日计划作业自动删除快照。有关详细信息，请参见第 4.3.1.2 节“清理算法” [36]。

4.4 限制

虽然 Btrfs 以及快照程序已准备好可以正式发布，但对于它们的后续开发仍在继续。该产品目前还存在以下限制。这些问题计划将在后续版本中得到解决。

4.4.1 数据一致性

目前还没有机制能在创建快照时确保数据的一致性。如果在创建快照的同时写入文件（例如数据库）都将导致文件损坏或写入不完整。恢复此类文件会产生问题。因此强烈建议您要始终仔细查看已更改文件及其差异的列表。请只恢复确实需要执行回滚操作的文件。

4.4.2 还原用户添加

通常，`/home` 位于单独分区。此类单独分区不属于执行 YaST 回滚操作的默认配置。因此，在使用快照程序还原用户添加时不会删除用户的主分区。强烈建议您使用 YaST 的 *用户和组管理* 工具来删除用户。

4.4.3 在 `/boot` 上以及引导加载程序的更改无法回滚

目前，无法从 `Btrfs` 分区引导 SUSE Linux Enterprise Server。因此在为系统分区使用 `Btrfs` 时，一旦安装便会创建 `/boot` 的单独分区。由于 `/boot` 不支持快照，因此以下限制仅适用于 YaST/zypper 回滚：

引导加载程序上的任何配置更改无法回滚

只有 `/etc` 中的引导加载程序配置文件可以执行回滚。大部分配置文件驻留在 `/boot` 下无法执行回滚。

内核安装无法实现完全回滚

内核本身及其 `initrd` 安装在 `/boot` 分区中，而内核模块或源分别安装在 `/var/lib` 和 `/usr/src` 中。此外，每一个内核安装还会更改 `/boot` 中的引导加载程序配置文件。因此，无论您何时执行涉及撤销内核安装的回滚操作，都需要手动从 `/boot` 删除内核及其 `initrd`，并通过删除该内核的引导条目调整引导加载程序配置。

4.5 常见问题

为什么快照程序从不显示 `/var/log`、`/tmp` 以及其他目录中的更改？

对于某些目录（例如 `/var/log`），我们决定禁用“快照生成”，因为还原日志会让问题难以搜索。为了将路径从“快照生成”中排除，我们为该路径创建了子卷。以下安装点被排除在 SUSE Linux Enterprise Server 上的“快照生成”路径之外：

- `/opt`
- `/srv`

- /tmp
- /var/crash
- /var/log
- /var/run
- /var/spool
- /var/tmp

我可以从引导加载程序引导快照吗？

目前还不可行。SUSE Linux Enterprise Server 上的引导加载程序目前还不支持从 Btrfs 分区引导。

4.6 在精简的 LVM 卷上使用快照程序

除了在 Btrfs 文件系统上生成快照之外，快照程序还支持在使用 ext3 或 XFS 格式化的精简 LVM 卷（不支持在常规 LVM 卷上生成快照）上“生成快照”。有关详细信息以及设置指导，请参见第 15.2 节“LVM 配置”（第 15 章 高级磁盘设置, ↑部署指南）。

为了在精简 LVM 卷上使用快照程序，您需要为其创建快照程序配置。在 LVM 上要使用 `--fstype=lvm`（文件系统）指定文件系统。由于目前支持 ext3 和 XFS，因此 ext3 或 xfs 对于文件系统是有效值。示例：

```
snapper -c lvm create-config --fstype="lvm(xfs)" /thin_lvm
```

您可以按照第 4.2.3.1 节“调整配置文件”[31]中的说明根据需要调整此配置。然后，您便可以使用快照程序创建和管理快照、恢复文件以及撤销更改了（如上所述）。

使用 VNC 远程访问

利用虚拟网络计算（Virtual Network Computing，VNC）可以通过图形桌面控制远程计算机（与远程外壳访问相对）。VNC 是独立于平台的并允许您从任何操作系统访问远程计算机。

SUSE Linux Enterprise Server 支持两种不同种类的 VNC 会话：自客户端启动起在 VNC 连接期间“在线”的一次性会话和始终“在线”直到被明确终止的永久会话。

注意：会话类型

一台计算机可在不同端口上同时提供两种会话，但当会话打开后不能从一种类型转换为另一种类型。

5.1 一次性 VNC 会话

一次性会话由远程客户端启动。它在服务器上启动图形登录屏幕。这样您就可以选择启动会话的用户，并且如果登录管理器支持，还可以选择桌面环境。一旦终止与此类 VNC 会话的客户端连接，则此会话中启动的所有应用程序也将终止。一次性 VNC 会话不能共享，但可以在一台主机上同时存在多个会话。

过程 5.1 启用一次性 VNC 会话

- 1 启动 YaST > 网络服务 > 远程管理 (VNC)。
- 2 选中允许远程管理。

- 3 如果需要，还可以选中**打开防火墙中的端口**（例如，当网络接口配置为在外部区域中时）。如果有多个网络接口，请通过**防火墙细节**将打开防火墙端口限制为特定的接口。
- 4 单击**完成**确认您的设置。
- 5 如果不是所有需要的包都可使用，则需要批准安装缺少的包。

注意：可用配置

SUSE Linux Enterprise Server 上的默认配置对会话使用 1024x768 像素（颜色深度 16 位）。会话在端口 5901（对于“普通”VNC 查看器，等同于 VNC 显示器 1）和端口 5801 上可用（对于 Web 浏览器）。

其他配置可在不同端口上使用，请参见第 5.1.2 节“配置一次性 VNC 会话”[43]。

VNC 显示器编号和 X 显示器编号是独立于一次性会话的。VNC 显示器编号手动指派给服务器支持的每个配置（如上例中的 :1）。只要 VNC 会话启动时带任一配置，就会自动获取可用 X 显示器编号。

5.1.1 启动一次性 VNC 会话

要启动一次性 VNC 会话，必须在客户端计算机上安装 VNC 查看器。SUSE Linux 产品上的标准查看器是 `tightvnc` 包提供的 `vncviewer`。您也可以使用 Web 浏览器和 Java 小程序查看 VNC 会话。

要启动 VNC 查看器并启动带服务器默认配置的会话，请使用以下命令：

```
vncviewer jupiter.example.com:1
```

若不使用 VNC 显示器编号，您也可以指定带两个冒号的端口号：

```
vncviewer jupiter.example.com::5901
```

或者通过输入以下 URL 使用支持 Java 的 Web 浏览器查看 VNC 会话：

```
http://jupiter.example.com:5801
```

5.1.2 配置一次性 VNC 会话

如果不需要或想修改默认配置，则可以跳过此部分。

一次性 VNC 会话通过 `xinetd` 守护程序启动。配置文件位于 `/etc/xinetd.d/vnc`。默认情况下提供六个配置块：三个用于 VNC 查看器（`vnc1` 到 `vnc3`），另外三个用于 Java 小程序（`vnchttpd1` 到 `vnchttpd3`）。默认情况下，只有 `vnc1` 和 `vnchttpd1` 是活动的。

要激活配置，请在第一列用 `#` 字符注释掉 `disable = yes` 行，或者完全删除该行。要停用配置，请取消注释或添加该行。

`xvnc` 服务器可以通过 `server_args` 选项来配置；有关选项列表，请参见 `Xvnc --help`。

当添加自定义配置时，请确保它们未使用已由其他配置、其他服务或同一主机上的现有永久 VNC 会话使用的端口。

通过输入以下命令激活配置更改：

```
rcxinetd reload
```

重要：防火墙和 VNC 端口

按照过程 5.1，“启用一次性 VNC 会话”[41] 中的描述激活远程管理时，端口 5801 和 5901 将在防火墙中打开。如果用于 VNC 会话的网络接口受防火墙保护，则为 VNC 会话激活更多端口时，需要手动打开各个端口。有关指导，请参见第 15 章 *Masquerading and Firewalls* (↑安全指南)。

5.2 持续 VNC 会话

永久 VNC 会话在服务器上启动。该会话和其上启动的所有应用程序运行时不考虑客户端连接，直到会话被终止。

可以从多个客户端同时访问持续会话。为了便于演示，我们选择一个较为理想的配置，一个客户端具有完全访问权限，所有其他客户端只具有查看访问权限。另一个用例是教员可能需要访问学员桌面的培训系统。但是，大多数时间，您可能不希望共享您的 VNC 会话。

相对于启动显示管理器的一次性会话，永久会话启动准备操作桌面（作为启动 VNC 会话的用户运行）。

永久会话访问受到两种可用密码类型的保护：

- 授予完全访问权限的普通密码或
- 可选仅查看密码，授予非交互（仅查看）访问权限。

一个会话可一次具有两种类型的多个客户端连接。

过程 5.2 启动持续 VNC 会话

- 1 打开外壳，确保以拥有 VNC 会话的用户身份登录。
- 2 如果用于 VNC 会话的网络接口受防火墙保护，则需要手动打开防火墙中您的会话所使用的端口。如果启动多个会话，还可以选择打开一个端口范围。有关如何配置防火墙的细节，请参见第 15 章 *Masquerading and Firewalls* (↑安全指南)。

`vncserver` 对显示器 :1 使用端口 5901，对显示器 :2 使用端口 5902，依次类推。对于永久会话，VNC 显示器和 X 显示器通常具有相同编号。

- 3 要其他具有 1024x769 像素和颜色深度为 16 的会话，请输入以下命令：

```
vncserver -geometry 1024x768 -depth 16
```

`vncserver` 命令在未给定编号时会挑选未用的显示器编号并打印出选择。有关更多选项，请参见 `man 1 vncserver`。

当首次运行 `vncviewer` 时，它请求完全访问会话的密码。如果需要，还可以提供密码用于会话的仅查看访问。

这里提供的密码还用作同一用户将来启动会话的密码。这些密码可以用 `vncpasswd` 命令更改。

重要：安全考虑因素

确保使用长度够长的高强度密码（八个或更多字符）。不要共享这些密码。

由于 VNC 连接未加密，可窃听两台计算机间网络的人员可以在会话刚开始时传输密码期间读取密码。

要终止会话，请从 VNC 查看器中关闭运行于 VNC 会话内的桌面环境，像您关闭普通本地 X 会话那样关闭它。

如果希望手动终止会话，请在 VNC 服务器上打开外壳并确保您已作为拥有要终止的 VNC 会话的用户登录。运行以下命令来终止在显示器 :1 上运行的会话：

```
vncserver -kill :1
```

5.2.1 连接持续 VNC 会话

要连接持续 VNC 会话，必须安装 VNC 查看器。SUSE Linux 产品上的标准查看器是 `tightvnc` 包提供的 `vncviewer`。您也可以使用 Web 浏览器和 Java 小程序查看 VNC 会话。

要启动 VNC 查看器并连接 VNC 服务器的显示器 :1，请使用命令

```
vncviewer jupiter.example.com:1
```

若不使用 VNC 显示器编号，您也可以指定带两个冒号的端口号：

```
vncviewer jupiter.example.com::5901
```

或者通过输入以下 URL 使用支持 Java 的 Web 浏览器查看 VNC 会话：

```
http://jupiter.example.com:5801
```

5.2.2 配置持续 VNC 会话

通过编辑 `$HOME/.vnc/xstartup` 可以配置持续 VNC 会话。默认情况下此外壳脚本启动 `xterm` 和 `twm` 窗口管理器。要改为启动 GNOME 或 KDE，请将 `twm` 开头的行替换为以下行之一：

```
/usr/bin/gnome    # GNOME  
/usr/bin/startkde # KDE
```

注意：每个用户一种配置

持续 VNC 会话在单个按用户配置中进行配置。一个用户启动的多个会话都使用相同的启动文件和密码文件。

使用命令行工具管理软件

本章描述 Zypper 和 RPM，这是两个用于管理软件的命令行工具。有关此环境中使用的术语定义（例如，安装源、增补程序或更新），请参见第 9.1 节“术语定义”（第 9 章 安装或删除软件, ↑部署指南）。

6.1 使用 Zypper

Zypper 是一个命令行包管理器，用于安装、更新和删除包及管理安装源。Zypper 的语法与 rug 的相似。与 rug 相反，Zypper 不需要在场景后运行 zmd 守护程序。有关 rug 兼容性的更多信息，请参见 `man zypper` 的“COMPATIBILITY WITH RUG”部分。这一点对于完成远程软件管理任务或从外壳脚本管理软件尤其有用。

6.1.1 一般使用

Zypper 的常用语法为：

```
zypper [global-options] command [command-options] [arguments] ...
```

不需要括在括号中的组件。执行 Zypper 最简单的方式是，键入其名称后跟一个命令。例如，将所有需要的增补程序应用于系统类型：

```
zypper patch
```

或者，可以从一个或多个全局选项中选择，方法是：只需在命令前面键入这些选项。例如，`--non-interactive` 表示运行命令时不询问任何问题（自动应用默认回答）：

```
zypper --non-interactive patch
```

要使用特定于某一特定命令的选项，请在此命令后面键入这些选项。例如，`--auto-agree-with-licenses` 表示将所有必需的增补程序应用到系统，不要求确认任何许可证（它们会被自动接受）：

```
zypper patch --auto-agree-with-licenses
```

某些命令需要一个或多个自变量。例如，使用安装命令时，需要指定安装哪个（哪些）包：

```
zypper install mplayer
```

某些选项也需要自变量。用以下命令可列出所有已知模式：

```
zypper search -t pattern
```

您可以组合上述所有模式。例如，以下命令将在冗长模式下从 `factory` 安装源安装 `mplayer` 和 `amarok` 包：

```
zypper -v install --from factory mplayer amarok
```

`--from` 选项确保了在从指定安装源请求包时保留所有安装源的启用状态（用于解析任何依赖项）。

多数 Zypper 命令都有 `dry-run` 选项，它模拟给定的命令。它可用于测试。

```
zypper remove --dry-run MozillaFirefox
```

Zypper 支持用于标识事务的全局 `--userdata` 字符串选项。用户定义的字符串将传递到 `/var/log/zypp/history` 中的 `zypper` 历史日志和快照程序。

```
zypper --userdata string patch
```

6.1.2 使用 Zypper 安装和删除软件

要安装或删除包，请使用以下命令：

```
zypper install package_name  
zypper remove package_name
```

Zypper 知道安装和删除命令处理包的不同方式：

用完整包名称（和版本号）

```
zypper install MozillaFirefox
```

或

```
zypper install MozillaFirefox-3.5.3
```

用安装源别名和包名称

```
zypper install mozilla:MozillaFirefox
```

其中 mozilla 是用于安装的安装源别名。

用使用通配符的包名称

以下命令将安装名称以“Moz”开头的包。使用通配符要小心，特别是删除包的时候。

```
zypper install 'Moz*'
```

用功能

例如，如果您要安装 perl 模块但不知道包名称，功能就可以派上用场：

```
zypper install 'perl(Time::ParseDate)'
```

用功能和/或体系结构和/或版本

您可以指定功能以及体系结构（例如 i586 或 x86_64）和/或版本。版本前必须带有以下某个运算符：<（小于）、<=（小于等于）、=（等于）、>=（大于等于）或 >（大于）。

```
zypper install 'firefox.x86_64'
```

```
zypper install 'firefox>=3.5.3'
```

```
zypper install 'firefox.x86_64>=3.5.3'
```

用 RPM 文件的路径

您还可以指定包的本地或远程路径：

```
zypper install /tmp/install/MozillaFirefox.rpm
```

```
zypper install
```

```
http://download.opensuse.org/repositories/mozilla/SUSE_Factory/x86_64/MozillaFirefox-3.5.3-1.3.x86_64.rpm
```

要同时安装和删除包，请使用 +/- 修饰符。要同时安装 emacs 并删除 vim，请使用：

```
zypper install emacs -vim
```

要同时删除 emacs 并安装 vim，请使用：

```
zypper remove emacs +vim
```

为避免 - 开头的包名称被解释为命令行选项，要始终把它用作第二个自变量。如果做不到这点，在它之前加上 --：

```
zypper install -emacs +vim      # Wrong
zypper install vim -emacs       # Correct
zypper install -- -emacs +vim   # same as above
zypper remove emacs +vim       # same as above
```

如果（同时使用某个包）要自动删除在删除指定包后不再需要的任何包，请使用 --clean-deps 选项：

```
rm package_name --clean-deps
```

默认情况下，在安装或删除选定包之前或发生问题时，Zypper 会要求确认。您可以使用 --non-interactive 选项覆盖此行为。必须在实际命令（install、remove 和 patch）之前提供此选项，如下所示：

```
zypper --non-interactive install package_name
```

该选项允许在脚本和 cron 任务中使用 Zypper。

警告：不要删除必需的系统包

请勿删除如 glibc、zypper、kernel 之类的包。这些包是系统强制安装的，如果删除可能导致系统不稳定或完全停止运行。

6.1.2.1 安装或下载源包

如果要安装某包对应的源包，请使用：

```
zypper source-install package_name
```

使用此命令，还可安装指定包的版本依赖性。如果不想执行此操作，请如下所示添加开关 -D。要只安装版本依赖性，请使用 -d。

```
zypper source-install -D package_name # source package only
zypper source-install -d package_name # build dependencies only
```

当然，只有当安装源列表中启用了含有源包的安装源时，才能这样做（默认添加但不启用它）。请参见第 6.1.5 节“用 Zypper 管理安装源”[56] 了解有关安装源管理的细节。

可使用以下方法来获取安装源中所有源包的列表：

```
zypper search -t srcpackage
```

您也可以将所有已安装软件包的源包下载到本地目录。要下载源包，请使用：

```
zypper source-download
```

默认的下载目录是 `/var/cache/zypper/source-download`。您可以使用 `--directory` 选项更改下载目录。若只想显示缺失或多余的包而不进行下载或删除任何内容，请使用 `--status` 选项。要删除多余的源包，请使用 `--delete` 选项。要禁用删除，请使用 `--no-delete` 选项。

6.1.2.2 实用程序

要校验所有依赖性是否仍然满足，并修复缺少的依赖性，请使用：

```
zypper verify
```

除了依赖性必须满足外，某些包还“推荐”其他包。只有在实际可用并可安装时才会安装这些推荐包。如果推荐的包在推荐它们的包已安装（通过添加其他包或硬件）之后才可用，请使用以下命令：

```
zypper install-new-recommends
```

此命令在插入摄像头或 WLAN 设备后非常有用。如果可用，它将安装设备驱动程序和相关软件。只有在满足特定硬件依赖性后，才可安装驱动程序和相关软件。

6.1.3 使用 Zypper 更新软件

用 Zypper 更新软件有三种方式：安装包、安装包的新版本或更新整个分发包。后者用 `zypper dist-upgrade` 命令实现，该命令在第 6.1.4 节“用 zypper 升级分发包”[54] 中进行了讨论。

6.1.3.1 安装增补程序

要安装所有适用于您系统的正式发布增补程序，只需运行：

```
zypper patch
```

这种情况下，会对安装源中的所有可用增补程序进行相关性检查，如有需要，还会进行安装。注册 SUSE Linux Enterprise Server 安装之后，包含此类增补程

序的官方更新安装源将添加到您的系统中。上述命令就是为了在需要时应用它们所必须输入的全部内容。

Zypper 知道三种查询增补程序可用性的不同命令：

`zypper patch-check`

列出需要的增补程序数（适用于您的系统但尚未安装的增补程序）

```
~ # zypper patch-check
Loading repository data...
Reading installed packages...
5 patches needed (1 security patch)
```

`zypper list-patches`

列出需要的所有增补程序（适用于您的系统但尚未安装的增补程序）

```
~ # zypper list-patches
Loading repository data...
Reading installed packages...

Repository | Name | Version | Category | Status
-----+-----+-----+-----+-----
Updates for opensUSE 11.3 11.3-1.82 | lxsession | 2776 | security | needed
```

`zypper patches`

列出 SUSE Linux Enterprise Server 可用的所有增补程序，无论是否已安装或是否适用于您的安装。

还可以列出并安装与特定问题相关的增补程序。要列出特定的增补程序，请使用带以下选项的 `zypper list-patches` 命令：

`--bugzilla[=编号]`

列出 **Bugzilla** 问题的所有必需增补程序。如果只要列出特定 **bug** 的增补程序，则可以选择指定其 **bug** 编号。

`--cve[=编号]`

列出 **CVE**（通用漏洞披露）问题的所有必需增补程序，或者仅列出与特定 **CVE** 编号（如果已指定）匹配的增补程序。

要安装用于特定 **Bugzilla** 或 **CVE** 问题的增补程序，请使用以下命令：

```
zypper patch --bugzilla=number
```

或

```
zypper patch --cve=number
```

例如，要安装 CVE 编号为 CVE-2010-2713 的安全增补程序，请执行：

```
zypper patch --cve=CVE-2010-2713
```

6.1.3.2 安装更新

如果某个安装源只包含新包，但未提供增补程序，则 `zypper patch` 不会产生任何作用。要使用新的可用版本更新所有安装的包，请使用：

```
zypper update
```

要更新个别包，请用更新或安装命令指定包：

```
zypper update package_name  
zypper install package_name
```

可使用此命令来获取所有新的可安装包的列表：

```
zypper list-updates
```

请注意，此命令仅列出与以下准则匹配的包：

- 与已安装的包拥有相同的供应商，
- 由至少与已安装包拥有相同优先级的安装源提供，
- 可安装（满足所有依赖性）。

所有新的可用包（无论是否可安装）的列表可通过以下方式获取：

```
zypper list-updates --all
```

要找出新包不能安装的原因，使用上面描述的 `zypper install` 或 `zypper update` 命令即可。

6.1.3.3 升级到新产品版本

要轻松将安装升级到新产品版本（例如从 SUSE Linux Enterprise Server 11 升级到 SUSE Linux Enterprise Server 11 SP1），请先调整安装源，使其与当前的 SUSE Linux Enterprise Server 安装源匹配。有关细节，请参见第 6.1.5 节“用 Zypper 管理安装源”[56]。然后对必需的安装源使用 `zypper dist-upgrade` 命令。该

命令可确保安装当前启用的安装源上的所有包。有关详细说明，请参见第6.1.4节“用 zypper 升级分发包”[54]。

要将分发包升级限制为来自特定安装源的包，同时还考虑满足依赖性的其他安装源，请使用 `--from` 选项并按别名、编号或 URI 指定安装源。

注意: **zypper update** 和 **zypper dist-upgrade** 之间的区别

选择 `zypper update` 可以在保持系统完整性的前提下将包更新到您的产品版本可用的较新版本。`zypper update` 遵守以下规则：

- 不更改供应商
- 不更改体系结构
- 不降级
- 保留已安装的包

执行 `zypper dist-upgrade` 时，将安装来自当前启用的安装源的所有包。该规则是强制执行的，因此包可能更改供应商或体系结构，甚至降级。升级后不满足依赖性的所有包都将卸载。

6.1.4 用 zypper 升级分发包

用 `zypper` 命令行实用程序，可以将分发包升级到下一个版本。最为重要的是，您可以在正在运行的系统中启动系统升级过程。

此功能适用于要运行远程升级或在多数配置类似的系统上运行升级的高级用户。

6.1.4.1 开始用 zypper 升级前

为了避免在使用 `zypper` 升级过程中出现意外错误，请尽可能减少有风险的操作。

- 尽量关闭应用程序和不必要的服务，并注销所有普通用户。
- 在开始升级前禁用第三方安装源，或降低这些安装源的优先级，以确保来自默认系统安装源的包具有优先权。完成升级后再次启用它们，并编辑其版本字符串，使其与已升级的运行中系统的分发包版本号匹配。

6.1.4.2 升级过程

警告：检查系统备份

在真正开始升级过程前，请检查系统备份是否为最新且可恢复。因为以下许多步骤都必须手动输入，所以这一点尤其重要。

zypper 程序支持长命令名和短命令名。例如，您可以将 `zypper install` 缩写为 `zypper in`。下文中使用的是短命令名。

- 1 运行联机更新以确保软件管理堆栈为最新的。有关详细信息，请参见第 1 章 *YaST 联机更新* [3]。
- 2 配置要用作更新源的安装源。拥有此权限至关重要。使用 YaST（参见第 9.3 节“管理软件安装源和服务”（第 9 章 *安装或删除软件*, ↑*部署指南*）或 `zypper`（参见第 6.1 节“使用 Zypper” [47]）。以下步骤中用到的安装源名称可能因您的自定义而有所不同。

考虑准备或更新自己的安装服务器。有关背景信息，请参见第 14.2.1 节“使用 YaST 设置安装服务器”（第 14 章 *远程安装*, ↑*部署指南*）。

要查看当前的安装源，请输入：

```
zypper lr -u
```

- 2a** 将系统安装源的版本号从 11-SP2 增加到 11-SP3；使用如下命令添加新的安装源：

```
server=http://download.example.org
zypper ar $server/distribution/11-SP3/repo/oss/ SLE-11-SP3
zypper ar $server/update/11-SP3/ SLE-11-SP3-Update
```

并且删除旧安装源：

```
zypper rr SLE-11-SP2
zypper rr SLE-11-Update
```

- 2b** 禁用第三方安装源或其他 Open Build Service 安装源，因为 `zypper dup` 只能保证与默认安装源协同运行（将 *安装源别名* 替换为要禁用的安装源的名称）：

```
zypper mr -d repo-alias
```

或者，您也可以降低这些安装源的优先级。

注意：处理未解决的依赖性

`zypper dup` 会删除所有具有未解决的依赖性的包，但只要依赖性要求符合，它就会保留已禁用安装源的包。

`zypper dup` 保证了所有安装的包都来自某个可用的安装源。它不考虑已安装包的版本、体系结构或供应商，因此它仿效全新安装。安装源中不再可用的包会当作孤立包。如果无法满足这些包的依赖性要求则会将其卸载。如果这些包的依赖性能够满足，则不会卸载它们。

2c 完成后，用以下项检查安装源配置：

```
zypper lr -d
```

- 3 用 `zypper ref` 刷本地元数据和安装源内容。
- 4 用 `zypper up zypper` 从 11 SP1 安装源拉入 `zypper` 和包管理堆栈。
- 5 用 `zypper dup` 运行实际的分发包升级。系统会要求您确认 SUSE Linux Enterprise 和一些包的许可证，具体取决于已安装包的设置。
- 6 用 `SuSEconfig` 执行基本系统配置。
- 7 用 `shutdown -r now` 重引导系统。

6.1.5 用 Zypper 管理安装源

Zypper 的所有安装或增补程序命令均基于已知安装源列表。要列出系统已知的所有安装源，请使用命令：

```
zypper repos
```

结果将类似于与以下输出：

例 6.1 *Zypper — 已知安装源列表*

```
# | Alias
```

```
| Name
```

	Enabled	Refresh
1	SUSE-Linux-Enterprise-Server 11-0	SUSE-Linux-Enterprise-Server 11-0
	Yes	No
2	SLES-11-Updates	SLES 11 Online Updates
	Yes	Yes
3	broadcomdrv	Broadcom Drivers
	Yes	No

当在各个命令中指定安装源时，可以使用别名、URI 或 `zypper repos` 命令输出中的安装源编号。安装源别名是用于安装源处理命令中的安装源名称的简短版本。请注意，在修改安装源列表后，安装源编号可能会更改。别名本身不会更改。

默认情况下不显示安装源的 URI 或优先级之类的细节。用以下命令可以列出所有细节：

```
zypper repos -d
```

6.1.5.1 添加安装源

要添加安装源，请运行

```
zypper addrepo URI alias
```

URI 可以是因特网安装源、网络资源、目录、CD 或 DVD（有关细节请参见 http://en.opensuse.org/openSUSE:Libzypp_URIs）。别名是安装源的唯一简写标识符。您可以自由选择别名，唯一的例外情况是别名必须唯一。如果指定的别名已在使用，Zypper 将发出警告。

6.1.5.2 删除安装源

如果要从此列表中删除某个安装源，请将命令 `zypper removerepo` 和要删除的安装源的别名或编号结合使用。例如，要删除例 6.1 “Zypper — 已知安装源列表” [56] 中列为第三项的安装源，请使用以下命令：

```
zypper removerepo 3
```

6.1.5.3 修改安装源

用 `zypper modifyrepo` 启用或禁用安装源。您还可以用该命令更改安装源的属性（例如刷新行为、名称或优先级）。以下命令将会启用名为 `updates` 的安装源、打开自动刷新并将其优先级设置为 20：

```
zypper modifyrepo -er -p 20 'updates'
```

修改安装源并不限于单个安装源 — 您还可以按组操作：

- a: 所有安装源
- l: 本地安装源
- t: 远程安装源
- m 类型: 特定类型的安装源（其中类型可以是以下之一：`http`、`https`、`ftp`、`cd`、`dvd`、`dir`、`file`、`cifs`、`smb`、`nfs`、`hd` 和 `iso`）

要重命名安装源别名，请使用 `renamerepo` 命令。以下示例把别名从 `Mozilla Firefox` 改为 `firefox`：

```
zypper renamerepo 'Mozilla Firefox' firefox
```

6.1.6 用 Zypper 查询安装源和包

Zypper 提供各种查询安装源或包的方式。要获取所有可用的产品、模式、包或增补程序的列表，请使用以下命令：

```
zypper products
zypper patterns
zypper packages
zypper patches
```

要查询特定包的所有安装源，请使用 `search`。它用于包名称或（可选）包摘要和描述。搜索项中允许使用通配符 `*` 和 `?`。默认情况下搜索不区分大小写。

```
zypper search firefox          # simple search for "firefox"
zypper search "**fire*"        # using wildcards
zypper search -d fire          # also search in package descriptions and summaries
zypper search -u firefox       # only display packages not already installed
```

要搜索提供特殊功能的包，请使用命令 `what-provides`。例如，如果您想知道哪个包提供 `perl` 模块 `SVN::Core`，请使用以下命令：

```
zypper what-provides 'perl(SVN::Core)'
```

要查询个别包，请使用 `info` 命令，并用完整包名称作为自变量。它会显示包的详细信息。如果还要显示该包必需/推荐的包，则使用选项 `--requires` 和 `--recommends`：

```
zypper info --requires MozillaFirefox
```

`what-provides package` 类似于 `rpm -q --whatprovides package`，但是 `rpm` 只能查询 RPM 数据库（即所有已安装包的数据库）。另一方面，`Zypper` 将告诉您任意安装源的功能的提供商，而非仅已安装的安装源功能的提供商。

6.1.7 配置 Zypper

`Zypper` 现在随附配置文件，允许您永久更改 `Zypper` 的行为（系统范围或用户特定）。要进行系统范围更改，请编辑 `/etc/zypp/zypper.conf`。要进行用户特定的更改，请编辑 `~/.zypper.conf`。如果 `~/.zypper.conf` 尚不存在，则可使用 `/etc/zypp/zypper.conf` 作为模板：将其复制到 `~/.zypper.conf` 并按您的喜好调整。请参见文件中的注释，获取有关可用选项的帮助。

6.1.8 查错

如果访问来自配置的安装源的包时存在问题（例如，尽管您知道某个包在某个安装源中，但 `zypper` 找不到该包），可使用以下命令刷新安装源：

```
zypper refresh
```

如果不起作用，则尝试

```
zypper refresh -fdb
```

这会强制完全刷新和重建数据库，包括强制下载原始元数据。

6.1.9 btrfs 文件系统上的 Zypper 回滚功能

如果根分区使用 `btrfs` 文件系统且安装有 `snapper`，则 `zypper` 在将更改提交到文件系统以创建合适的文件系统快照时，会自动调用 `snapper`（通过 `snapper` 安装的脚本实现）。这些快照可用于还原 `zypper` 执行的任何更改。有关 `snapper` 的更多信息，请参见 `man snapper`。

当前，Zypper（和 YaST）只会为根文件系统生成快照，而无法配置其他子卷。默认文件系统不支持此功能。

6.2 RPM — 包管理器

RPM（RPM 程序包管理器）用于管理软件包。其主要命令为 `rpm` 和 `rpmbuild`。用户、系统管理员和包构建人员可以查询强大的 RPM 数据库以获得有关已安装软件的详细信息。

本质上，`rpm` 有五种模式：安装、卸装（或更新）软件包、重建 RPM 数据库、查询 RPM 库或独立 RPM 存档、包的完整性检查以及对包签名。`rpmbuild` 可用于从原始源构建可安装的包。

用特殊的二进制格式对可安装 RPM 存档进行打包。这些存档由要安装的程序文件和某些元信息组成，这些元信息供 `rpm` 在安装过程中配置软件包使用或者储存在 RPM 数据库中进行存档。RPM 存档通常具有扩展名 `.rpm`。

提示：软件开发包

对于许多包，已将软件开发所需的部件（库、标题、包含文件等）放入单独的包中。只有当您自己要自己编译软件时才需要这些开发包（例如最新的 GNOME 包）。可通过扩展名 `-devel` 标识这些开发包，例如包 `alsa-devel`、`gimp-devel` 和 `libkde4-devel`。

6.2.1 校验包真实性

RPM 包具有 GPG 签名。要校验 RPM 程序包的签名，请使用命令 `rpm --checksig 包-1.2.3.rpm` 决定该包是源自 Novell/SUSE 还是另一个可信设备。特别建议对来自因特网的更新包使用此命令。

6.2.2 管理包：安装、更新和卸装

通常，RPM 存档的安装十分简单：`rpm -i package.rpm`。使用此命令可以安装包，但前提是满足其依赖性并且不与其他包冲突。如果出现错误消息，`rpm` 将请求那些需要安装的包以满足依赖性要求。在后台，RPM 数据库确保不出现

冲突 — 一个特定文件只能属于一个包。通过选择不同的选项，您可以强制 rpm 忽略这些默认设置，但这只供专家用户使用。否则，将影响系统的完整性并可能使系统无法更新。

选项 `-U` 或 `--upgrade` 以及 `-F` 或 `--freshen` 可用于更新包（例如，`rpm -F package.rpm`）。此命令将删除旧版本的文件并立即安装新文件。两个版本之间的差别是 `-U` 安装系统中以前不存在的包，但 `-F` 只更新以前安装的包。更新时，rpm 使用以下策略小心更新配置文件：

- 如果配置文件未被系统管理员更改，则 rpm 将安装适当文件的新版本。系统管理员无需执行任何操作。
- 如果配置文件在更新前已由系统管理员更改，则 rpm 将以扩展名 `.rpmorig` 或 `.rpmsave`（备份文件）保存更改的文件并安装新包中的版本（但前提是原先安装的文件和较新的版本不同）。如果是这种情况，则将备份文件（`.rpmorig` 或 `.rpmsave`）与新安装的文件进行比较，并在新文件中再次进行更改。随后，确保删除所有 `.rpmorig` 和 `.rpmsave` 文件以避免以后的更新出现问题。
- 如果配置文件已存在并且 `.spec` 文件中指定了 `noreplace` 标签，则出现 `.rpmnew` 文件。

更新后，在使用 `.rpmsave` 和 `.rpmnew` 文件进行比较后应将它们删除，从而防止它们阻碍以后的更新。如果 RPM 数据库以前未能识别文件，则将其指派扩展名 `.rpmorig`。

否则，将使用 `.rpmsave`。换句话说，`.rpmorig` 是从异系统格式更新为 RPM 的结果。而 `.rpmsave` 是从较早的 RPM 更新为较新的 RPM 的结果。`.rpmnew` 不提供任何有关系统管理员是否对配置文件进行了任何更改的信息。`/var/adm/rpmconfigcheck` 中提供这些文件的列表。不覆盖某些配置文件（如 `/etc/httpd/httpd.conf`）以允许继续进行操作。

`-U` 开关不仅仅是使用 `-e` 选项进行卸载并使用 `-i` 选项进行安装的等效项。只要可能，就可以使用 `-U`。

要删除包，请输入 `rpm -e package.rpm`，仅删除包含未解析依赖性的包。例如，只要有其他程序需要 Tcl/Tk，理论上就不能删除它。即使是在这种情况下，RPM 也会向数据库寻求帮助。如果出于任何原因无法进行此删除操作（即使不存在其他依赖性），则最好使用选项 `--rebuilddb` 重建 RPM 数据库。

6.2.3 RPM 和增补程序

为了确保系统的操作安全性，必须时常在系统中安装更新包。以前，包中的bug只能通过替换整个包来解决。小文件中带 bug 的大型包容易导致这种情况的发生。不过 SUSE RPM 提供了一项功能，支持在包中安装增补程序。

以下使用 pine 的示例中对最重要的考虑事项进行了说明：

增补程序 RPM 是否适合我的系统？

要对此进行检查，请先查询包的已安装版本。对于 pine，可以通过以下命令完成：

```
rpm -q pine
pine-4.44-188
```

然后检查增补程序 RPM 是否适合此版本的 pine：

```
rpm -qp --basedon pine-4.44-224.i586.patch.rpm
pine = 4.44-188
pine = 4.44-195
pine = 4.44-207
```

此增补程序适用于 pine 的三个不同的版本。还列出示例中已安装的版本，从而可以安装增补程序。

增补程序将替换哪些文件？

在增补程序 RPM 中可以方便地找到受增补程序影响的文件。rpm 参数 -P 允许选择特殊的增补程序功能。使用以下命令显示文件列表：

```
rpm -qpPl pine-4.44-224.i586.patch.rpm
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

或者，如果已安装增补程序，则使用以下命令：

```
rpm -qPl pine
/etc/pine.conf
/etc/pine.conf.fixed
/usr/bin/pine
```

如何在系统中安装增补程序 RPM？

增补程序 RPM 的使用与普通 RPM 相同。唯一的区别就是必须已安装合适的 RPM。

系统中已安装了哪些增补程序，用于哪些包版本？

使用命令 `rpm -qPa` 可以显示系统中已安装的所有增补程序的列表。如果新系统中只安装了一个增补程序（如本示例中），则列表如下：

```
rpm -qPa
pine-4.44-224
```

如果以后要了解最初安装了哪个包版本，则可以在 **RPM** 数据库中获得此信息。对于 `pine`，可以通过以下命令显示此信息：

```
rpm -q --basedon pine
pine = 4.44-188
```

`rpm` 和 `rpmbuild` 的手册页中提供了详细信息（包括有关 **RPM** 的增补程序功能的信息）。

注意：SUSE Linux Enterprise Server 的官方更新

为了尽量减小更新的下载大小，SUSE Linux Enterprise Server 的官方更新未以增补程序 **RPM** 的形式提供，而是以增量 **RPM** 程序包提供。有关细节，请参见第 6.2.4 节“增量 **RPM** 包” [63]。

6.2.4 增量 **RPM** 包

增量 **RPM** 包包含旧版本和新版本的 **RPM** 包之间的差别。在旧 **RPM** 上应用增量 **RPM** 将得到全新的 **RPM**。不需要旧 **RPM** 的副本，因为增量 **RPM** 也可以与已安装的 **RPM** 一起工作。增量 **RPM** 包的大小甚至比增补程序 **RPM** 小，这有利于通过因特网传送更新包。缺点是，涉及增量 **RPM** 的更新操作与使用纯粹 **RPM** 或增补程序 **RPM** 进行更新的情况相比，占用的 CPU 周期要长得多。

`prepdeltarpm`、`writedeltarpm` 和 `applydeltarpm` 二进制文件是增量 **RPM** 套件（包 `deltarpm`）的一部分并帮助您创建和应用增量 **RPM** 包。使用以下命令，创建名为 `new.delta.rpm` 的增量 **RPM**。以下命令假设 `old.rpm` 和 `new.rpm` 是存在的：

```
prepdeltarpm -s seq -i info old.rpm > old.cpio
prepdeltarpm -f new.rpm > new.cpio
xdelta delta -0 old.cpio new.cpio delta
writedeltarpm new.rpm delta info new.delta.rpm
```

最后，删除临时工作文件 `old.cpio`、`new.cpio` 和 `delta`。

如果旧包已经安装，则使用 `applydeltarpm` 可以从文件系统重新构建新的 RPM：

```
applydeltarpm new.delta.rpm new.rpm
```

如果不访问文件系统而从旧 RPM 得到它，请使用 `-r` 选项：

```
applydeltarpm -r old.rpm new.delta.rpm new.rpm
```

关于技术详细信息，请参见 `/usr/share/doc/packages/deltarpm/README`。

6.2.5 RPM 查询

使用 `-q` 选项，`rpm` 将启动查询，从而能够查看 RPM 存档（通过添加选项 `-p`）并查询已安装包的 RPM 数据库。可以使用多个开关指定所需信息的类型。请参见表 6.1 “最重要的 RPM 查询选项” [64]。

表 6.1 最重要的 RPM 查询选项

<code>-i</code>	包信息
<code>-l</code>	文件列表
<code>-f FILE</code>	查询包含文件 <i>FILE</i> 的包（必须使用 <i>FILE</i> 指定完整路径）
<code>-s</code>	带有状态信息的文件列表（间接指定 <code>-l</code> ）
<code>-d</code>	仅列出文档文件（间接指定 <code>-l</code> ）
<code>-c</code>	仅列出配置文件（间接指定 <code>-l</code> ）
<code>--dump</code>	带有完整详细信息文件列表（将用于 <code>-l</code> 、 <code>-c</code> 或 <code>-d</code> ）
<code>--provides</code>	列出包中可被另一个包通过 <code>--requires</code> 请求的功能

<code>--requires, -R</code>	包需要的功能
<code>--scripts</code>	安装脚本（预安装、后安装、卸载）

例如，命令 `rpm -q -i wget` 显示例 6.2 “`rpm -q -i wget`” [65] 中所示的信息。

例 6.2 `rpm -q -i wget`

```
Name           : wget                               Relocations: (not relocatable)
Version        : 1.11.4                             Vendor: opensUSE
Release       : 1.70                                Build Date: Sat 01 Aug 2009
09:49:48 CEST
Install Date: Thu 06 Aug 2009 14:53:24 CEST      Build Host: build18
Group         : Productivity/Networking/Web/Utilities Source RPM:
wget-1.11.4-1.70.src.rpm
Size          : 1525431                             License: GPL v3 or later
Signature     : RSA/8, Sat 01 Aug 2009 09:50:04 CEST, Key ID b88b2fd43dbdc284
Packager      : http://bugs.opensuse.org
URL           : http://www.gnu.org/software/wget/
Summary       : A Tool for Mirroring FTP and HTTP Servers
Description   :
Wget enables you to retrieve WWW documents or FTP files from a server.
This can be done in script files or via the command line.
[...]
```

只有当您指定带有完整路径的完整文件名时，选项 `-f` 才起作用。根据需要提供任意多个文件名。例如，以下命令

```
rpm -q -f /bin/rpm /usr/bin/wget
```

产生：

```
rpm-4.8.0-4.3.x86_64
wget-1.11.4-11.18.x86_64
```

如果只知道部分文件名，则可以使用壳层脚本，如例 6.3 “搜索包的脚本” [65] 所示。当运行所显示的脚本时，将部分文件名以参数的形式传递给该脚本。

例 6.3 搜索包的脚本

```
#!/bin/sh
for i in $(rpm -q -a -l | grep $1); do
    echo "\"$i\" is in package:"
    rpm -q -f $i
    echo ""
done
```

命令 `rpm -q --changelog rpm` 按照日期显示特定包（此例中为 `rpm` 程序包）更改信息的详细列表。

借助已安装的 **RPM** 数据库，可以进行校验检查。使用 `-V`、`-y` 或 `--verify` 启动此操作。使用此选项，`rpm` 显示安装后已被更改的包中的所有文件。`rpm` 使用 8 个字符符号给出有关以下更改的一些提示：

表 6.2 RPM 校验选项

5	MD5 校验和
S	文件大小
L	符号链接
T	修改时间
D	主要和次要设备编号
U	拥有者
G	组
M	方式（权限和文件类型）

对于配置文件，将输出字母 `c`。例如，对于 `/etc/wgetrc`（`wget` 包）的更改：

```
rpm -V wget
S.5....T c /etc/wgetrc
```

RPM 数据库的文件被放置在 `/var/lib/rpm` 中。如果分区 `/usr` 的大小为 1 GB，则此数据库可能会占用将近 30 MB，特别是在完全更新之后。如果数据库比预期大得多，则最好使用选项 `--rebuilddb` 重建数据库。在执行此操作之前，制作旧数据库的备份。`cron` 脚本 `cron.daily` 每天制作数据库的副本（用 `gzip` 打包）并将这些副本储存在 `/var/adm/backup/rpmdb` 中。副本的数目是由 `/etc/sysconfig/backup` 中的变量 `MAX_RPMDDB_BACKUPS`（默认为 5）控制的。对于 1 GB 的 `/usr`，单个备份的大小大约为 1 MB。

6.2.6 安装和编译源包

所有源包都带有 `.src.rpm` 扩展名（源 RPM）。

注意：已安装的源包

源包可以从安装媒体复制到硬盘并使用 YaST 解压缩。但是，在包管理器中它们不会被标记为已安装 ([i])。这是因为源包不是在 RPM 数据库中输入的。只有已安装的操作系统软件列在 RPM 数据库中。安装“源包时，只将源代码添加到系统中。”

以下目录必须可用于 `/usr/src/packages` 中的 `rpm` 和 `rpmbuild`（除非在诸如 `/etc/rpmrc` 这样的文件中指定自定义设置）：

SOURCES

代表原始源（`.tar.bz2` 或 `.tar.gz` 文件等）和特定于发布版本的调整（多为 `.diff` 或 `.patch` 文件）

SPECS

代表 `.spec` 文件，类似于元 Makefile，该文件控制构建进程

BUILD

在此目录中解压缩、增补和编译所有源

RPMS

储存完整的二进制包的位置

SRPMS

这里是源 RPM

通过 YaST 安装源包时，所有必需的组件都安装在 `/usr/src/packages` 中：源和调整项在 SOURCES 中，相关 `.spec` 文件在 SPECS 中。

警告

不要对系统组件（`glibc`、`rpm`、`sysvinit` 等）进行试验，因为这将会影响系统的稳定性。

下面的示例使用 `wget.src.rpm` 包。安装源包后，应具有类似以下列表中的文件：

```
/usr/src/packages/SOURCES/wget-1.11.4.tar.bz2
/usr/src/packages/SOURCES/wgetrc.patch
/usr/src/packages/SPECS/wget.spec
```

`rpmbuild -b X /usr/src/packages/SPECS/wget.spec` 启动编译。`X` 是通配符，代表构建进程的不同阶段（有关详细信息，请参见 `--help` 的输出或 **RPM 文档**）。以下内容只是简要描述：

`-bp`

在 `/usr/src/packages/BUILD` 中准备源：解压和打增补程序。

`-bc`

执行与 `-bp` 相同的操作，但还进行编译。

`-bi`

执行与 `-bp` 相同的操作，但还安装生成的软件。注意：如果包不支持 **BuildRoot** 功能，则可能会重写配置文件。

`-bb`

执行与 `-bi` 相同的操作，但还创建二进制包。如果编译成功，二进制包应该在 `/usr/src/packages/RPMS` 中。

`-ba`

执行与 `-bb` 相同的操作，但还创建源 **RPM**。如果编译成功，二进制包应该在 `/usr/src/packages/SRPMS` 中。

`--short-circuit`

跳过某些步骤。

现在可以使用 `rpm -i` 或最好使用 `rpm -U` 来安装创建的二进制 **RPM**。使用 `rpm` 进行安装使它显示在 **RPM 数据库** 中。

6.2.7 使用 **build** 编译 **RPM** 包

许多包存在的风险是构建进程中会将许多不需要的文件添加到正在运行的系统中。为防止发生这种情况，请使用 `build`，它将创建构建包的已定义环境。要

建立这一 **chroot** 环境，**build** 脚本必须和完整的包树结构一起提供。可以通过 **NFS** 或从 **DVD** 使用硬盘上的此树。使用 `build --rpms directory` 设置位置。与 **rpm** 不同，**build** 命令在源目录中查找 `.spec` 文件。要用系统中 `/media/dvd` 下装入的 **DVD** 构建 **wget**（如上例所示），请以 **root** 用户身份使用以下命令：

```
cd /usr/src/packages/SOURCES/  
mv ../SPECS/wget.spec .  
build --rpms /media/dvd/suse/ wget.spec
```

随后，将在 `/var/tmp/build-root` 建立一个最小的环境。在此环境中构建包。完成后，生成的包位于 `/var/tmp/build-root/usr/src/packages/RPMS` 中。

build 脚本提供多个附加选项。例如，使脚本优先选择您自己的 **RPM**、忽略构建环境的初始化或者将 **rpm** 命令限制在上述阶段之一。使用 `build --help` 并通过阅读 **build** 手册页来访问更多信息。

6.2.8 用于 **RPM** 存档和 **RPM** 数据库的工具

Midnight Commander (mc) 可以显示 **RPM** 存档的内容并复制部分内容。它将存档表示为虚拟文件系统，提供 **Midnight Commander** 所有常用的菜单选项。使用 **F3** 键显示 **HEADER**。使用光标键和 **Enter** 键查看存档结构。使用 **F5** 键复制部分存档。

还提供充当 **YaST** 模块的功能齐全的包管理器。有关细节，请参见第 9 章 **安装或删除软件** (↑部署指南)。

Bash 和 Bash 脚本

今天，许多人使用具有诸如 KDE 或 GNOME 的图形用户界面 (GUI) 的计算机。尽管它们提供大量功能，但当要执行自动任务时，它们的用途非常有限。外壳是对 GUI 的很好补充，本章提供关于外壳（在本例中为 Bash）的某些方面的概述。

7.1 什么是“外壳”？

通常来说，外壳就是指 Bash（Bourne again 外壳）。在本章中提到“外壳”时，指的是 Bash。事实上，除了 Bash 还存在很多其他外壳（ash、csh、ksh、zsh、...），每种外壳都具备不同的功能和特征。如果需要关于其他外壳的更多信息，请在 YaST 中搜索外壳。

7.1.1 了解 Bash 配置文件

外壳可调用为：

1. **交互式登录外壳** 当登录计算机时需要使用此方式，即使用 `--login` 选项调用 Bash 或通过 SSH 登录到远程计算机时。
2. **“普通”交互式外壳** 这通常在启动 xterm、konsole、gnome 终端或类似工具时使用。
3. **非交互式外壳** 当在命令行调用外壳脚本时使用。

根据所用外壳的类型，会读取不同的配置文件。下表显示登录和非登录外壳的配置文件。

表 7.1 登录外壳的 *Bash* 配置文件

文件	描述
/etc/profile	不要修改此文件，否则在下一次更新时可能损坏您的修改！
/etc/profile.local	如果扩展 /etc/profile，请使用此文件
/etc/profile.d/	包含特定程序的系统范围配置文件
~/.profile	在此处插入特定于用户的登录外壳配置

表 7.2 非登录外壳的 *Bash* 配置文件

/etc/bash.bashrc	不要修改此文件，否则在下一次更新时可能损坏您的修改！
/etc/bash.bashrc.local	使用此文件插入系统范围的修改（仅 Bash）
~/.bashrc	在此处插入特定于用户的配置

此外，*Bash* 还使用更多文件：

表 7.3 用于 *Bash* 的特殊文件

文件	描述
~/.bash_history	包含已键入的所有命令的列表
~/.bash_logout	注销时执行

7.1.2 目录结构

下表简要介绍 Linux 系统上最重要的较高级别目录。以下列表中是关于这些目录和重要子目录的更多详细信息。

表 7.4 标准目录树概述

目录	内容
/	root 目录 — 目录树的起点。
/bin	基本二进制文件，例如系统管理员和普通用户都需要的命令。通常还包含外壳，如 Bash。
/boot	引导加载程序的静态文件。
/dev	访问特定于主机的设备所需的文件。
/etc	特定于主机的系统配置文件。
/home	储存系统上具有帐户的所有用户的用户主目录。但是，root 的用户主目录不在 /home 中，而是在 /root 中。
/lib	基本共享库和内核模块。
/media	可卸媒体的安装点。
/mnt	临时装入文件系统的安装点。
/opt	附加应用程序软件包。
/root	超级用户 root 的用户主目录。
/sbin	基本系统二进制文件。

目录	内容
/srv	系统提供的服务的数据。
/tmp	临时文件。
/usr	具有只读数据的辅助层次结构。
/var	变量数据，如日志文件。
/windows	只在系统上同时安装了 Microsoft Windows* 和 Linux 时可用。包含 Windows 数据。

以下列表提供有关这些目录中有哪些文件和子目录的更多详细信息，并给出一些示例：

/bin

包含 root 和其他用户都可使用的基本外壳命令。这些命令包括 ls、mkdir、cp、mv、rm 和 rmdir。/bin 也包含 Bash，它是 SUSE Linux Enterprise Server 中的默认外壳。

/boot

包含引导所需的数据，如引导加载程序、内核以及内核开始执行用户模式程序之前使用的其他数据。

/dev

储存代表硬件组件的设备文件。

/etc

包含控制诸如 X Window 系统等程序操作的本地配置文件。/etc/init.d 子目录包含引导过程中执行的脚本。

/home/*username*

储存在系统中建立帐户的所有用户的私人数据。这里的文件只能由其拥有者或系统管理员修改。默认情况下，电子邮件目录和个人桌面配置以隐藏文件和目录的形式位于此处。KDE 用户在 .kde4 中查找其桌面的个人配置数据；GNOME 用户在 .gconf 中查找该数据。

注意：网络环境中的用户主目录

如果在网络环境中工作，则您的用户主目录可能映射到文件系统中除 /home 之外的其他目录中。

/lib

包含引导系统和运行 root 文件系统所需的命令所需的基本共享库。共享库相当于 Windows 中的 DLL 文件。

/media

包含 CD-ROM、USB 记忆棒和数码相机（如果它们使用 USB）等可卸媒体的安装点。/media 通常包含除系统硬盘驱动器之外的各类驱动器。可卸媒体插入或连接到系统并装入之后，可以从此处访问该媒体。

/mnt

此目录提供临时装入的文件系统的安装点。root 可以在此处装入文件系统。

/opt

保留用于安装第三方软件。在此处可以找到可选软件和较大外接式附件程序包。

/root

root 用户的用户主目录。root 的个人数据位于此处。

/sbin

如 s 所表明，该目录储存超级用户的实用程序。/sbin 包含 /bin 中的二进制文件以及引导和恢复系统所需的其他二进制文件。

/srv

储存系统提供的服务（如 FTP 和 HTTP）的数据。

/tmp

此目录由需要临时储存文件的程序使用。

重要：在引导时清理 /tmp

储存在 /tmp 中的数据不能保证在系统重引导后仍存在。具体取决于 /etc/sysconfig/cron（该文件仅为示例）中的设置。

`/usr`

`/usr` 与用户无关，而是 UNIX 系统资源的缩写。`/usr` 中的数据是可以在符合文件系统层次结构标准 (FHS) 的各个主机之间共享的静态只读数据。此目录包含所有应用程序并建立文件系统辅助层次结构。**KDE4** 和 **GNOME** 也位于此处。`/usr` 储存有大量子目录，例如 `/usr/bin`、`/usr/sbin`、`/usr/local` 和 `/usr/share/doc`。

`/usr/bin`

包含一般可访问的程序。

`/usr/sbin`

包含为系统管理员保留的程序，例如维修功能。

`/usr/local`

在此目录中，系统管理员可以安装本地的独立于分发包的扩展。

`/usr/share/doc`

储存系统的各种文档文件和发行描述。在 `manual` 子目录中可以找到此手册的联机版本。如果安装了多种语言，则此目录可能包含这些手册不同语言的版本。

在 `packages` 下可以找到系统上安装的软件包中包含的文档。对于每个包，都会创建一个子目录 `/usr/share/doc/packages/packagename`，经常用于储存该包的自述文件，有时储存示例、配置文件或附加脚本。

如果系统上安装了操作指南，`/usr/share/doc` 还会包含 `howto` 子目录，其中有与 Linux 软件的安装和操作相关的许多任务的附加文档。

`/var`

`/usr` 用于储存静态只读的数据，而 `/var` 用于在系统操作期间写入并成为变量数据的数据，例如日志文件或假脱机数据。有关最重要日志文件的概述，可以在 `/var/log/` 下找到，请参见表 35.1 “日志文件” [505]。

7.2 编写外壳脚本

外壳脚本是执行所有类型任务的便捷方式：收集数据、在文本中搜索单词或短语以及许多其他有用的操作。以下示例显示用于打印文本的小外壳脚本：

例 7.1 用于打印文本的外壳脚本

```
#!/bin/sh ❶  
# Output the following line: ❷  
echo "Hello World" ❸
```

- ❶ 第一行开头是 *Shebang* 字符(#!)，它表示此文件是一个脚本。该脚本使用 *Shebang* 后的指定解释程序执行，在本示例中为 `/bin/sh`。
- ❷ 第二行是一个以哈希符号开头的注释。建议对较难理解的行进行注释以记住它们的作用。
- ❸ 第三行使用内置命令 `echo` 打印相应文本。

可以运行该脚本之前，需要一些先决条件：

1. 每个脚本都应包含一个 *Shebang* 行（始终和我们的上述示例一样）。如果脚本没有此行，则必须手动调用解释程序。
2. 可以将该脚本保存在任何位置。但是，建议将其保存在外壳可以找到的目录中。外壳中的搜索路径由环境变量 `PATH` 确定。通常，一般用户不具有对 `/usr/bin` 的写权限。因此，建议将脚本保存在用户目录 `~/bin/` 中。在上例中使用名称 `hello.sh`。
3. 该脚本需要可执行权限。使用以下命令设置权限：

```
chmod +x ~/bin/hello.sh
```

如果已满足上述所有先决条件，则可以按如下方式执行此脚本：

1. **作为绝对路径** 可以使用绝对路径执行脚本。在本例中为 `~/bin/hello.sh`。
2. **所有位置** 如果 `PATH` 环境变量包含脚本所在目录，则只需使用 `hello.sh` 即可执行脚本。

7.3 重定向命令事件

每个命令都可以使用三个通道输入或输出：

- **标准输出** 这是默认的输出通道。在命令打印某些内容时都会使用标准输出通道。
- **标准输入** 如果一个命令需要用户或其他命令输入，则使用此通道。

- **标准错误** 命令使用此通道报告错误。

要重定向这些通道，有以下可行的操作方式：

命令 > 文件

将该命令的输出保存为文件，将删除现有文件。例如，ls 命令会将其输出写入文件 listing.txt：

```
ls > listing.txt
```

命令 >> 文件

将命令输出追加到文件。例如，ls 命令会将其输出追加到文件 listing.txt：

```
ls >> listing.txt
```

命令 < 文件

读取该文件作为给定命令的输入。例如，read 命令会将此文件的内容读入变量：

```
read a < foo
```

命令 1 | 命令 2

将左侧命令的输出重定向为右侧命令的输入。例如，cat 命令会输出文件 /proc/cpuinfo 的内容。grep 使用此输出仅过滤出包含 cpu 的行：

```
cat /proc/cpuinfo | grep cpu
```

每个通道都有一个文件描述符：0（零）表示标准输入，1 表示标准输出，2 表示标准错误。允许在 < 或 > 字符前插入此文件描述符。例如，以下行搜索以 foo 开头的文件，但通过将错误重定向到 /dev/null 而抑制错误。

```
find / -name "foo*" 2>/dev/null
```

7.4 使用别名

别名是一个或多个命令的快捷方式定义。别名的语法为：

```
alias NAME=DEFINITION
```

例如，以下行定义了一个别名 lt，它输出一个长列表（选项 -l），将其按修改时间排序（-t），并在排序后反向打印（-r）：


```
alias lt='ls -ltr'
```

要查看所有别名定义，请使用 `alias`。使用 `unalias` 和相应的别名删除别名。

7.5 在 Bash 中使用变量

外壳变量可以是全局变量，也可以是局部变量。全局变量（或环境变量）可以在所有外壳中访问。而局部变量仅在当前外壳中可见。

要查看所有环境变量，请使用 `printenv` 命令。如果需要知道变量的值，请将变量名称作为自变量插入：

```
printenv PATH
```

也可以使用 `echo` 查看变量（无论是全局或本地变量）：

```
echo $PATH
```

要设置局部变量，请使用变量名后加等号和值：

```
PROJECT="SLED"
```

不要在等号两边插入空格，否则会出错。要设置环境变量，请使用 `export`：

```
export NAME="tux"
```

要删除变量，请使用 `unset`：

```
unset NAME
```

下表包含外壳脚本中可以使用的一些常见环境变量：

表 7.5 有用的环境变量

HOME	当前用户的用户主目录
HOST	当前主机名
LANG	当一个工具本地化后，它使用此环境变量中的语言。英语也可以设置为 C

PATH	外壳的搜索路径，冒号分隔的目录列表
PS1	指定在每个命令前打印的普通提示符
PS2	指定在执行多行命令时打印的辅助提示符
PWD	当前工作目录
USER	当前用户

7.5.1 使用自变量

例如，如果具有脚本 `foo.sh`，则可以如下执行：

```
foo.sh "Tux Penguin" 2000
```

要访问传递给脚本的所有自变量，您需要定位参数。`$1` 表示第一个自变量，`$2` 表示第二个自变量，依此类推。至多可以有九个参数。要获取脚本名称，请使用 `$0`。

以下脚本 `foo.sh` 打印从 1 到 4 的所有自变量：

```
#!/bin/sh
echo \"$1\" \"$2\" \"$3\" \"$4\"
```

如果使用上述自变量执行此脚本，将获取：

```
"Tux Penguin" "2000" "" ""
```

7.5.2 使用变量替换

变量替换将一个模式应用于变量的内容（从左侧或从右侧）。以下列表包含可能的语法格式：

```
${VAR#pattern}
    从左侧删除可能的最短匹配：
```

```
file=/home/tux/book/book.tar.bz2
echo ${file#*/}
home/tux/book/book.tar.bz2
```

`${VAR##pattern}`

从左侧删除可能的最长匹配:

```
file=/home/tux/book/book.tar.bz2
echo ${file##*/}
book.tar.bz2
```

`${VAR%pattern}`

从右侧删除可能的最短匹配:

```
file=/home/tux/book/book.tar.bz2
echo ${file%.*}
/home/tux/book/book.tar
```

`${VAR%%pattern}`

从右侧删除可能的最长匹配:

```
file=/home/tux/book/book.tar.bz2
echo ${file%%.*}
/home/tux/book/book
```

`${VAR/pattern_1/pattern_2}`

将来自 *pattern_1* 的 *VAR* 的内容替代为 *pattern_2*:

```
file=/home/tux/book/book.tar.bz2
echo ${file/tux/wilber}
/home/wilber/book/book.tar.bz2
```

7.6 将命令分组和组合

外壳允许您对命令执行连接和分组以有条件地执行。每个命令都返回一个退出码，该退出码确定操作是成功还是失败。如果是0，则命令成功，任何其他值都表示特定于该命令的一个错误。

以下列表显示可以如何将命令分组:

命令 1 ; 命令 2

顺序地执行这些命令。不检查退出码。以下行使用 `cat` 显示文件的内容，然后使用 `ls` 打印其文件属性，而不考虑退出码:

```
cat filelist.txt ; ls -l filelist.txt
```

命令 1 && 命令 2

如果左侧命令成功，则运行右侧命令（逻辑运算符 **AND**）。仅当上一个命令成功时，以下行才显示文件的内容并打印其文件属性（将其与列表中的上一项相比较）：

```
cat filelist.txt && ls -l filelist.txt
```

命令 1 || 命令 2

当左侧命令失败时运行右侧命令（逻辑运算符 **OR**）。以下行仅当在 `/home/tux/foo` 中创建目录失败时才会 在 `/home/wilber/bar` 中创建目录：

```
mkdir /home/tux/foo || mkdir /home/wilber/bar
```

```
funcname() { ... }
```

创建外壳函数。您可以使用定位参数访问其自变量。以下行定义用于打印短消息的函数 `hello`：

```
hello() { echo "Hello $1"; }
```

您可以如下调用此函数：

```
hello Tux
```

它会打印：

```
Hello Tux
```

7.7 使用通用流程构造语句

为了控制脚本的流程，外壳有 `while`、`if`、`for` 和 `case` 等构造语句。

7.7.1 if 控制命令

`if` 命令用于检查表达式。例如，以下代码测试当前用户是否是 `Tux`：

```
if test $USER = "tux"; then
    echo "Hello Tux."
else
    echo "You are not Tux."
fi
```

测试表达式既可以复杂也可以简单。以下表达式检查文件 `foo.txt` 是否存在：

```
if test -e /tmp/foo.txt ;
then
    echo "Found foo.txt"
fi
```

测试表达式也可以缩写为方括号中：

```
if [ -e /tmp/foo.txt ] ; then
    echo "Found foo.txt"
fi
```

在<http://www.cyberciti.biz/nixcraft/linux/docs/uniqlinuxfeatures/lsst/ch03sec02.html> 上可以找到更多有用表达式。

7.7.2 使用 **for** 命令创建循环

for 循环允许您对一系列项执行命令。例如，以下代码打印关于当前工作目录中 PNG 文件的某些信息：

```
for i in *.png; do
    ls -l $i
done
```

7.8 更多信息

关于 **Bash** 的重要信息在手册页 `man sh` 中提供。可以在以下列表中找到关于此主题的更多信息：

- <http://tldp.org/LDP/Bash-Beginners-Guide/html/index.html> — **Bash** 入门者指南
- <http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html> — **BASH** 编程 - 简介操作指南
- <http://tldp.org/LDP/abs/html/index.html> — 高级 **Bash** 脚本编写指南
- <http://www.grymoire.com/Unix/Sh.html> — **sh** - Bourne 外壳

部分 II. 系统

64 位系统环境中的 32 位和 64 位应用程序

SUSE® Linux Enterprise Server 可用于多个 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 Server 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 Server 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。

设计了适用于 64 位平台 ia64、ppc64、System z 和 x86_64 的 SUSE Linux Enterprise Server，这样现有的 32 位应用程序“无需任何设置”即可在 64 位环境中运行。相应的 32 位平台是 x86（对于 ia64）、ppc（对于 ppc64）和 x86（对于 x86_64）。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。当前的 ppc64 系统以 32 位方式运行大多数应用程序，但您可以运行 64 位应用程序。

8.1 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。

此规则的一个例外是 PAM（可插入身份验证模块）。SUSE Linux Enterprise Server 在身份验证过程中使用 PAM 作为在用户和应用程序之间充当媒介的

层。在另外还运行 32 位应用程序的 64 位操作系统上，始终需要安装两个版本的 PAM 模块。

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。通常预计会在 `/lib` 和 `/usr/lib` 下找到的 64 位对象文件，现在可以在 `/lib64` 和 `/usr/lib64` 下找到。这意味着 `/lib` 和 `/usr/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 32 位 `/lib` 目录的子目录包含的数据内容不依赖于字大小，则不移动这些目录。此方案符合 LSB（Linux 标准库）和 FHS（文件系统层次标准）。

► **ipf:** ia64 的 64 位库位于标准的 `lib` 目录中，没有 `lib64` 目录或 `lib32` 目录。ia64 在仿真下执行 32 位 x86 代码。一组基本库将安装在 `/emul/ia32-linux/lib` 和 `/emul/ia32-linux/usr/lib` 中。◀

8.2 软件开发

所有 64 位体系结构都支持 64 位对象的开发。32 位编译的支持级别取决于体系结构。GCC（GNU 编译器集合）和 `binutils`（包括汇编器 `as` 和链接器 `ld`）中的工具链有多个实施选项：

Biarch 编译器

使用 `biarch` 开发工具链可以生成 32 位对象和 64 位对象。`biarch` 开发工具链允许生成 32 位和 64 位对象。在几乎所有平台上，默认设置都是编译 64 位对象。如果使用特殊的标志，则可以生成 32 位对象。特殊标志是 `-m32`（对于 GCC）。用于 `binutils` 的标志是依赖于体系结构的，但 GCC 将正确的标志传送到链接器和汇编器。对于 `amd64`（支持 x86 和 `amd64` 指令的开发）、`System z` 和 `ppc64`，目前存在 `biarch` 开发工具链。32 位对象通常是在 `ppc64` 平台上创建的。`-m64` 标志用于生成 64 位对象。

无支持

SUSE Linux Enterprise Server 不支持在所有平台上直接开发 32 位软件。要在 ia64 下开发用于 x86 的应用程序，请使用对应的 SUSE Linux Enterprise Server 32 位版本。

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）。常规 SUSE Linux Enterprise Server 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。

8.3 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` 或 `rpmname-x86`（针对 ia64，如果第二个体系结构为 32 位体系结构），或者 `rpmname-64bit`（如果第二个体系结构为 64 位体系结构）。您还需要 `rpmname-devel` 包中各自的报头和库以及 `rpmname-devel-32bit` 或 `rpmname-devel-64bit` 中用于第二个体系结构的开发库。

例如，要在第二个体系结构为 32 位体系结构的系统（x86_64 或 System z）上编译使用 `libaio` 的程序，则需要以下 RPM：

`libaio-32bit`

32 位运行时包

`libaio-devel-32bit`

32 位开发的标题和库

`libaio`

64 位运行时包

`libaio-devel`

64 位开发的标题和库

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。

以下示例涉及使用 x86 作为第二个体系结构的 x86_64 系统。第二个体系结构为 ppc 的 ppc64 的示例类似。该示例不适用于不能建立 32 位包的 ia64。

1 使用 32 位编译器：

```
CC="gcc -m32"
```

2 指示链接器处理 32 位对象（始终使用 gcc 作为链接器前端）：

```
LD="gcc -m32"
```

3 设置组装机生成 32 位对象：

```
AS="gcc -c -m32"
```

4 指定链接器标志，如 32 位库的位置，例如：

```
LDFLAGS="-L/usr/lib"
```

5 指定 32 位对象代码库的位置：

```
--libdir=/usr/lib
```

6 指定 32 位 X 库的位置：

```
--x-libraries=/usr/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。

在 x86_64、ppc64 或 System z 上编译本机 32 位应用程序的 configure 调用示例可如下所示：

```
CC="gcc -m32"  
LDFLAGS="-L/usr/lib;"  
./configure --prefix=/usr --libdir=/usr/lib --x-libraries=/usr/lib  
make  
make install
```

8.4 内核规范

x86_64、ppc64 和 System z 的 64 位内核提供 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，必须在非 ppc64 平台上将少量应用程序（如 `lspci`）编译为 64 位程序才能正常工作。在 IBM System z 上，并非所有 `ioctl` 都在 32 位内核 ABI 中可用。

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：内核可装载模块

某些应用程序需要单独的内核可装载模块。如果要在 64 位系统环境中使用这种 32 位应用程序，请与此应用程序和 SUSE 的提供商联系以确保该内核可装载模块的 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 系统涉及不同组件。BIOS 初始化硬件本身，并通过引导加载程序启动内核。之后，init 的引导进程及运行级别将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。

9.1 Linux 引导进程

Linux 引导进程包括多个阶段，每个阶段由一个不同组件来代表。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** 在打开计算机之后，BIOS 将初始化屏幕和键盘并测试主内存。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几何属性之后，系统控制将从 BIOS 传递到引导加载程序。如果 BIOS 支持网络引导，则也可以配置提供引导加载程序的引导服务器。在 x86 系统上需要 PXE 引导。其他体系结构通常使用 BOOTP 协议获得引导加载程序。
2. **引导加载程序** 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权交给实际的操作系统（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 10 章 引导加载程序 GRUB [107]。对于网络引导，BIOS 充当了引导加载程序。它从引导服务器启动映像，然后启动系统。这完全不依赖本地硬盘。

3. **内核和 `initramfs`** 为了交接系统控制权，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`，可以处理真实 `root` 文件系统的装入。如果需要特殊硬盘驱动程序才能访问大容量储存，则这些程序必须在 `initramfs` 中。有关 `initramfs` 的详细信息，请参见第 9.1.1 节“`initramfs`”[94]。如果系统没有本地硬盘，则 `initramfs` 必须向内核提供 `root` 文件系统。这应该通过网络块设备（如 iSCSI 或 SAN）的帮助进行，但也可以使用 NFS 作为 `root` 设备。
4. **`initramfs` 中的 `init`** 此程序执行装入正确 `root` 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 `root` 文件系统后，对其进行错误检查并装入。如果此操作成功，将清除 `initramfs` 并执行 `root` 文件系统上的 `init` 程序。有关 `init` 的详细信息，请参见第 9.1.2 节“`initramfs` 上的 `init`”[95]。有关 `udev` 的详细信息，请参见第 14 章 *使用 `udev` 进行动态内核设备管理* [163]。
5. **`init`** `init` 通过提供不同功能的多个不同级别来处理实际的系统引导。有关 `init` 的介绍，请参见第 9.2 节“`init` 进程”[96]。

9.1.1 `initramfs`

`initramfs` 是一个内核可以装载到 RAM 磁盘的小型 `cpio` 归档。它提供了一个最小的 Linux 环境，可在装入实际 `root` 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 `root` 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 `root` 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 `root` 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。`root` 文件系统所需的模块可以由 `initramfs` 上的 `init` 来装载。装载模块后，`udev` 将为 `initramfs` 提供所需的设备。在引导过程的后面，更改 `root` 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。

如果需要更改已安装系统的硬件（例如硬盘），并且该硬件要求引导时内核中有不同的驱动程序，则必须更新 `initramfs`。操作方法和其前身 `init` 一样，

即调用 `mkinitrd`。调用 `mkinitrd`（不带任何参数）创建 `initramfs`。调用 `mkinitrd -R` 创建 `init`。在 SUSE® Linux Enterprise Server 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 `init`

引导加载程序装载 `initramfs` 或 `init` 的方式与内核相同。更新 `initramfs` 或 `init` 后无需重安装 GRUB，因为 GRUB 会在引导时从目录中搜索正确的文件。

9.1.2 `initramfs` 上的 `init`

`initramfs` 上的 `init` 的主要用途是准备真实 `root` 文件系统的装入和访问。`init` 负责以下任务，具体取决于您的系统配置。

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组件（最重要的组件是硬盘）。要访问最终的 `root` 文件系统，内核需要装载正确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` 会处理这些事件并在 `RAM` 文件系统的 `/dev` 中生成所需的特殊块文件。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 `root` 文件系统，则 `init` 将设置 `LVM` 或 `RAID` 以支持稍后对 `root` 文件系统的访问。在第 15 章 *高级磁盘设置* (↑部署指南) 中查找关于 `RAID` 和 `LVM` 的信息。

管理网络配置

如果将系统配置为使用通过网络装入的 `root` 文件系统（通过 NFS 装入），则 `init` 必须确保装载了正确的网络驱动程序，并确保将其设置为支持访问 `root` 文件系统。

如果文件系统驻留在一个联网的块设备（如 iSCSI 或 SAN）上，则到储存服务器的连接也由 `initramfs` 设置。

在初始引导期间作为安装过程的一部分调用 `init` 时，要执行的任务将与上述任务不同：

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 `init`。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 9.1.1 节“`initramfs`”[94]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开始。`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`。这些名称用于生成引导系统所需的自定义 `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。

装载安装系统或救援系统

正确识别硬件后，便会装载合适的驱动程序，`udev` 将创建特殊的设备文件，`init` 将使用实际 YaST 安装程序启动安装系统或者救援系统。

启动 YaST

最后，`init` 将启动 YaST，由后者启动包安装和系统配置。

9.2 `init` 进程

`init` 程序是进程 ID 为 1 的进程，负责按所要求的方式初始化系统。`init` 由内核直接启动，并且抵制信号 9（该信号通常会终止进程）。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` 文件中集中配置，其中运行级别已定义（请参见第 9.2.1 节“运行级别”[97]）。该文件还指定了在每个运行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。默认情况下，引导后启动的第一个脚本为 `/etc/init.d/boot`。完成系统初始化阶段后，系统将使用 `/etc/init.d/rc` 脚本把运行级别更改为默认运行级别。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（请参见第 9.2.2 节“Init 脚本”[99]）。

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。

9.2.1 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 9.1“可用运行级别”[97]。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）。不直接由内核本身评估的任何参数均将传递给 init。要引导到 `runlevel 3`，只需向引导提示符添加一个数字 3。

表 9.1 可用运行级别

运行级别	描述
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	除非管理员配置该运行级别，否则不使用用户定义

运行级别	描述
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 Server** 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。

警告：/etc/inittab 中的错误可能导致系统引导出现故障

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 使用命令 `telinit q` 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) 请求 init 更改到其他运行级别。
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。

9.2.2 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。对于 IBM System z 系统，仅在引导进程中或立即关闭系统（电源故障或通过“信号静止”）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中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 9.2 “可能的 `init` 脚本选项” [100] 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 9.2 可能的 `init` 脚本选项

选项	描述
<code>start</code>	启动服务。
<code>stop</code>	停止服务。
<code>restart</code>	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。
<code>reload</code>	在不停止和重新启动服务的情况下重新装载配置。
<code>force-reload</code>	如果服务支持，则重新装载配置。否则，要执行的步骤与指定 <code>restart</code> 时相同。
<code>status</code>	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）的帮助下可添加和删除这些链接。有关更多细节，请参见 `man 8 insserv`。

所有这些设置也可能在 YaST 模块的帮助下发生变化。如果需要在命令行上检查状态，请使用 `man 8 chkconfig` 手册页中所描述的工具 `chkconfig`。

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描述。

`boot`

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。它在由这些脚本触发的操作（运行几个子脚本，例如使特殊块文件变为可用的）完成之后停止。`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` 的进一步信息，请使用 `man 8 blogd`。

`boot` 脚本还负责启动 `/etc/init.d/boot.d` 中名称以 `s` 开头的脚本。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 `root` 密码后进行干预。上次执行的脚本是 `boot.local`。

`boot.local`

在此，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`。

`halt`

此脚本仅在更改为运行级别 0 或 6 时执行。在这里，它作为 `init` 或 `init` 来执行。是关闭还是重引导系统取决于调用 `halt` 的方式。如果在关闭系统过程中需要特殊命令，请将此类命令添加到 `init` 脚本。

`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。与 `/etc/init.d/boot` 脚本类似，该脚本是通过将所需运行级别用作参数从 `/etc/inittab` 调用的。

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。在第 9.2.1 节“运行级别”[97] 中可以找到有关 `init` 脚本的有用信息。

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副本，然后根据需要编辑相关程序和文件名、路径及其他细节。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 9.1 “最小的 `INIT INFO` 块”[102]。

例 9.1 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。在 `Required-Start:` 和 `Required-Stop:` 行中，指定停止服务本身时仍需运行的所有服务。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描述。

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` 对 `INIT INFO` 标题进行评估，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所需的链接。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 9.2.3 节“使用 YaST 配置 System Services (Runlevel)”[103]中描述的方法使用 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` 时将删除手动添加的服务。

9.2.3 使用 YaST 配置 System Services (Runlevel)

使用 `YaST > 系统 > System Services (Runlevel)` 启动此 YaST 模块后，它将显示一个概述，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描述。窗口下部提供了对所选服务的更为详细的描述。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。

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 Server 系统的默认运行级别是运行级别 5（有网络和 X 的完全多用户模式）。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 9.1 “可用运行级别” [97] 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描述。

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。

图 9.1 System Services (Runlevel)



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。选择确定即可将已更改的设置保存到磁盘。

9.3 通过 /etc/sysconfig 配置系统

SUSE Linux Enterprise Server 的主要配置是由 /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。

9.3.1 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易于使用的前端。无需了解需要更改的配置变量的实际位置，只需使用此模块的内置搜索功能，就可以按需更改配置变量的值，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新启动服务。

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 9.2 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与此变量的当前设置。在下面第三个窗口中，简要描述了变量的用途、可能的值、默认值以及此变量源自的实际配置文件。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新启动涉及的所有服务以使更改生效。

9.3.2 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。
- 2 使用 `telinit 1` 将系统转入单用户模式（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 `telinit 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 GRUB

本章描述了如何配置 SUSE® Linux Enterprise Server 中使用的引导加载程序 GRUB (Grand Unified Bootloader)。一个特殊的 YaST 模块可用于配置所有设置。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。

注意：使用 UEFI 的计算机上无 GRUB

配有传统 BIOS 的计算机和使用兼容支持模块 (CSM) 的 UEFI (统一可扩展固件接口) 计算机上都例行安装了 GRUB。在未启用 CSM 的 UEFI 计算机上，将自动安装 eLILO (假设 DVD1 已成功引导)。请参见系统上 `/usr/share/doc/packages/elilo/` 处的 eLILO 文档以了解细节。

本章主要介绍引导加载程序 GRUB 的引导管理和配置。第 9 章 *引导和配置 Linux 系统* [93] 中将引导过程作为一个整体进行了介绍。引导加载程序代表计算机 (BIOS) 和操作系统 (SUSE Linux Enterprise Server) 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：

MBR (Master Boot Record, 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。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 的最后两个字节必须包含静态

“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“容器”。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 root 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。

10.1 通过 GRUB 引导

GRUB 包括两个阶段。Stage 1 包括 512 字节，其唯一任务在于装载引导加载程序的第二阶段。随后，装载 stage 2。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，它能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。

Stage 2 可以访问多个文件系统。目前支持 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 还能够从包含符合“El Torito”规范的 ISO 9660 标准文件系统的 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) 进行更改不要求新安装引导管理器。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 的实际配置是基于四个文件进行的，下面对这四个文件进行介绍：

/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（请参见第 10.1.1.3 节“在引导过程中编辑菜单项”[113] 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 外壳正确安装引导加载程序所需的命令、参数和选项。

`/etc/sysconfig/bootloader`

此文件由使用 YaST 配置引导加载程序时以及每次安装新内核时所使用的 perl 引导加载程序库读取。它包含配置选项（例如内核参数）。默认情况下，这些配置选项会添加到引导加载程序配置文件中。

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方式输入引导命令。有关详细信息，请参见第 10.1.1.3 节“在引导过程中编辑菜单项”[113]。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。后者被称为 *GRUB 外壳*。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 `setup` 命令的形式集成在 GRUB 中。当装载了 Linux 后在 GRUB 外壳中可用。

10.1.1 文件 `/boot/grub/menu.lst`

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 10.2 节“使用 YaST 配置引导加载程序”[117] 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，就像在外壳中一样。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中的设备名在第10.1.1.1节“硬盘和分区的命名约定”[110]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。示例文件在第10.1.1.2节“示例菜单文件”[111]中有所介绍。

10.1.1.1 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/sda1。

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 PATA (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 10.1.2 节“文件 `device.map`”[113] 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 PATA (IDE) 硬盘（其第一个分区中包含 Linux）的系统上，可以按如下方式指定可引导内核：

```
(hd0,0)/boot/vmlinuz
```

10.1.1.2 示例菜单文件

以下示例描述了 GRUB 菜单文件的结构。此示例安装包括 `/dev/sda5` 下的 Linux 引导分区、`/dev/sda7` 下的根分区和 `/dev/sda1` 下的 Windows 安装。

```
gfxmenu (hd0,4)/boot/message❶
color white/blue black/light-gray❷
default 0❸
timeout 8❹

title linux❺
    root (hd0,4)
    kernel /boot/vmlinuz root=/dev/sda7 vga=791 resume=/dev/sda9
    initrd /boot/initrd

title windows❻
    rootnoverify (hd0,0)
    chainloader +l

title floppy❼
    rootnoverify (hd0,0)
    chainloader (fd0)+l
```

```

title failsafe⑧
    root (hd0,4)
    kernel /boot/vmlinuz.shipped root=/dev/sda7 ide=nodma \
    apm=off acpi=off vga=normal nosmp maxcpus=0 3 noresume
    initrd /boot/initrd.shipped

```

第一块定义了启动屏幕的配置：

- ❶ 背景图像 message 位于 /dev/sda5 分区的 /boot 目录中。
- ❷ 颜色模式：白色（前景）、蓝色（背景）、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。
- ❸ 会默认引导第一个 (0) 菜单项 title linux。
- ❹ 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。

- ❺ 第一项 (title linux) 负责引导 SUSE Linux Enterprise Server。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（例如根分区和 VGA 方式）也被追加在此处。根分区是根据 Linux 命名约定 (/dev/sda7/) 指定的，因为此信息将由内核读取而与 GRUB 无关。initrd 也位于第一块硬盘的第一个逻辑分区中。
- ❻ 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。
- ❼ 下一项支持从软盘进行引导，而无需修改 BIOS 设置。
- ❽ 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（请参见第 10.1.1.3 节“在引导过程中编辑菜单项” [113]）。

10.1.1.3 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 35.3 “美式键盘布局” [513]。

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
    root(hd0,0)
    kernel /vmlinuz root=/dev/sda3 additional parameter
    initrd /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。

10.1.2 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 PATA (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。BIOS 中的引导顺序设为 PATA 先于 SCSI 的系统的示例 `device.map` 文件可能如下所示：

```
(fd0) /dev/fd0
(hd0) /dev/sda
(hd1) /dev/sdb
```

或

```
(fd0) /dev/fd0
(hd0) /dev/disk-by-id/DISK1 ID
(hd1) /dev/disk-by-id/DISK2 ID
```

因为 PATA (IDE)、SCSI 和其他硬盘的顺序取决于各种因素，并且 Linux 无法标识映射，所以可以在文件 `device.map` 中手动设置顺序。如果在引导时遇到问题，请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。

注意：最大硬盘数量

GRUB 使用 BIOS 服务对硬盘寻址。这是通过软件中断 `Int13h` 进行的。由于 `Int13h` 处理的最大磁盘数限制为 8 个，因此 GRUB 仅可从 `Int13h` 处理的这些磁盘中引导，即使存在更多磁盘（此情况通常出现在多路径系统上）。因此，安装期间创建的 `device.map` 文件将仅包含 `Int13h` 处理的最多 8 个磁盘。

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
```

10.1.3 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 外壳正确安装引导加载程序所需的命令、参数和选项。

```
setup --stage2=/boot/grub/stage2 --force-lba (hd0,1) (hd0,1)
quit
```

该命令将告知 GRUB 使用位于第一个硬盘 (`hd0,1`) 的第二个分区上的引导映像将引导加载程序自动安装到同一分区上。需要 `--stage2=/boot/grub/stage2` 参数在已装入的文件系统中安装 `stage2` 映像。一些 BIOS 具有不正确的 LBA 支持实施，`--force-lba` 提供了解决方案以忽略这些故障。

10.1.4 文件 /etc/sysconfig/bootloader

仅在使用 YaST 配置引导加载程序时以及每次安装新内核时会用到此配置文件。它由 perl 引导加载程序库评估，此库会相应地修改引导加载程序配置文件（例如，对于 GRUB 为 /boot/grub/menu.lst）。/etc/sysconfig/bootloader 不是 GRUB 特定的配置文件 - 其值适用于 SUSE Linux Enterprise Server 上安装的任何引导加载程序。

注意：内核更新后的引导加载程序配置

每次安装新内核时，perl 引导加载程序都会使用 /etc/sysconfig/bootloader 中指定的默认值写入新的引导加载程序配置文件（例如，对于 GRUB 为 /boot/grub/menu.lst）。如果要使用自定义内核参数集，请确保根据需要调整 /etc/sysconfig/bootloader 中的相关默认值。

LOADER_TYPE

指定在系统（例如 GRUB 或 LILO）上安装的引导加载程序。不要修改，而是使用 YaST 更改引导加载程序，如过程 10.6,“更改引导加载程序类型”[121]中所述。

DEFAULT_VGA / FAILSAFE_VGA / XEN_VGA

引导期间使用的 framebuffer 的屏幕分辨率和颜色深度是通过内核参数 vga 配置的。这些值定义对于默认引导项、failsafe 和 XEN 项使用哪种分辨率和颜色深度。以下值为有效值：

表 10.1 屏幕分辨率和颜色深度参考

	640x480	800x600	1024x768	1280x1024	1600x1200
8bit	0x301	0x303	0x305	0x307	0x31C
15bit	0x310	0x313	0x316	0x319	0x31D
16bit	0x311	0x314	0x317	0x31A	0x31E
24bit	0x312	0x315	0x318	0x31B	0x31F

DEFAULT_APPEND / FAILSAFE_APPEND / XEN_KERNEL_APPEND

自动追加到引导加载程序配置文件中的默认值、故障安全以及 XEN 引导项的内核参数（vga 除外）。

CYCLE_DETECTION / CYCLE_NEXT_ENTRY

配置是否要使用引导周期检测，如果要使用，则配置在重引导周期要从 /boot/grub/menu.lst 引导的备用项（例如 Failsafe）。请参见 /usr/share/doc/packages/bootcycle/README 了解详细信息。

10.1.5 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 root 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。要阻止此类访问或防止用户引导某些操作系统，请设置引导密码。

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 root 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/sda7 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，将显示以下错误消息：

```
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**）。

10.2 使用 YaST 配置引导加载程序

在您的 SUSE Linux Enterprise Server 系统中配置引导加载程序的最简单方式就是使用 YaST 模块。在 YaST 控制中心，选择 **系统 > 引导加载程序**。如图 10.1 “引导加载程序设置”[117] 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 10.1 引导加载程序设置



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**。要删除现有的条目，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 10.1 节“通过 GRUB 引导”[108]。

使用引导加载程序安装选项卡查看并更改类型、位置和高级加载程序设置的相关设置。

单击其他访问高级配置选项。内置编辑器让您可以更改 GRUB 配置文件。有关详细信息，请参见第 10.1 节“通过 GRUB 引导”[108]。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 (MBR)，请选择恢复硬盘的主引导记录。

10.2.1 调整默认引导项

要更改默认引导的系统，请按如下所示继续：

过程 10.1 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 单击确定以激活这些更改。

10.2.2 修改引导加载程序位置

要修改引导加载程序的位置，请遵循以下步骤：

过程 10.2 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）。

从根分区引导

这将在 / 分区（这是默认分区）的引导扇区中安装引导加载程序。

从引导分区引导

这将在 /boot 分区的引导扇区中安装引导加载程序。

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。

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 **确定** 以应用您的更改。

10.2.3 更改引导加载程序超时值

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 10.3 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 通过键入新值、用鼠标单击相应的箭头键或使用键盘上的箭头键来更改 **超时**（以秒为单位）的值。
- 4 单击 **确定** 两次以保存更改。

警告：0 秒超时

将超时设置为 0 秒时，在引导时您将无法访问 GRUB。如果同时将默认引导选项设置为非 Linux 操作系统，事实上会禁用对 Linux 系统的访问。

10.2.4 设置引导密码

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 10.4 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 通过单击并键入两次密码激活*使用密码保护引导加载程序选项*。
- 4 单击*确定*两次以保存更改。

10.2.5 调整磁盘顺序

如果您的计算机有多个硬盘，则可以按照计算机的 BIOS 设置指定磁盘引导顺序（请参见第 10.1.2 节“文件 device.map”[113]）。为此，请执行如下操作：

过程 10.5 设置磁盘顺序

- 1 打开*引导加载程序安装选项卡*。
- 2 单击*引导加载程序安装详细信息*。
- 3 如果列出了多个磁盘，请选择一个，然后单击*向上*或*向下*来对显示的磁盘重新排序。
- 4 单击*确定*两次以保存更改。

10.2.6 配置高级选项

高级引导选项可以通过*引导加载程序安装 > 引导加载程序选项*来配置。通常情况下，不需要更改默认设置。

在分区表中设置活动标志，以引导分区

激活包含该引导加载程序的分区。一些旧操作系统（如 Windows 98）只能从活动分区中引导。

将通用引导代码写入 MBR 中

使用通用、独立于操作系统的代码替换当前 MBR。

调试标志

在调试模式中设置 GRUB，该模式可显示表明磁盘活动的消息。

隐藏引导菜单

隐藏引导菜单并引导默认项。

警告

隐藏引导菜单时，在引导时您将无法访问 GRUB。如果同时将默认引导选项设置为非 Linux 操作系统，事实上会禁用对 Linux 系统的访问。

使用受信任的 GRUB

启动支持受信任计算功能的受信任 GRUB。

图形菜单文件

显示引导屏幕时使用的图形文件的路径。

串行连接参数

如果您的计算机是通过串行控制台控制的，则可指定要使用的 COM 端口及其运行速度。还可以将终端定义设置为“串行”。有关细节，请参见 `info grub` 或 <http://www.gnu.org/software/grub/manual/grub.html>。

使用串行控制台

如果您的计算机是通过串行控制台控制的，则可激活此选项并指定要使用的 COM 端口及其运行速度。请参见 `info grub` 或 <http://www.gnu.org/software/grub/manual/grub.html#Serial-terminal>

10.2.7 更改引导加载程序类型

在引导加载程序安装中设置引导加载程序类型。SUSE Linux Enterprise Server 中的默认引导加载程序是 GRUB。要使用 LILO 或 ELILO，请如下操作：

警告：LILO 不受支持

不建议使用 LILO——它在 SUSE Linux Enterprise Server 上不受支持。仅在特殊情况下才使用它。

过程 10.6 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 Server 期间不可用。

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 Server 期间不可用。

4 单击确定两次以保存更改。

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。

10.3 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，然后单击系统 > 引导加载程序启动引导加载程序模块。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。

10.4 创建引导 CD

如果使用引导管理器引导系统时出现问题或不能将引导管理器安装在硬盘磁盘上，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 10.7 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，并更改为新创建的 *iso* 目录：

```
mkdir -p iso/boot/grub && cd iso
```

3 将内核、文件 *stage2_eltorito*、*initrd*、*menu.lst* 和 *message* 复制到 *iso/boot/*：

```
cp /boot/vmlinuz boot/  
cp /boot/initrd boot/  
cp /boot/message boot/  
cp /usr/lib/grub/stage2_eltorito boot/grub  
cp /boot/grub/menu.lst boot/grub
```

4 将 *root (hdx, y)* 项替换为 *root (cd)* 以指向 CD-ROM 设备。您可能还需要调整消息文件、内核和 *initrd* 的路径，它们应分别指向 */boot/message*、*/boot/vmlinuz* 和 */boot/initrd*。调整后，*menu.lst* 的显示应与以下示例类似：

```
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消息。

5 用以下命令创建 ISO 映像：

```
genisoimage -R -b boot/grub/stage2_eltorito -no-emul-boot \  
-boot-load-size 4 -boot-info-table -iso-level 2 -input-charset utf-8 \  
-o grub.iso /tmp/iso
```

6 使用您选择的实用程序将最终文件 `grub.iso` 刻录到 CD 上。不要将 ISO 映像作为数据文件刻录，而要使用刻录实用程序中刻录 CD 映像的选项。

10.5 图形 SUSE 屏幕

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 10 章 *引导加载程序 GRUB* [107] 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*。在内核中禁用帧缓冲区支持也会自动禁用启动屏幕。

警告：无支持

如果使用自定义内核运行 SUSE，则它不能为系统提供任何支持。

10.6 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描述。一些问题在知识库（位于 <http://www.suse.com/support>）的文章中有所涉及。用搜索对话框搜索 *GRUB*、*boot* 和 *引导加载程序* 之类的关键字。

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。在此情况下，请更新 BIOS。

如果将 Linux 安装在未在 BIOS 中注册的其他硬盘上，GRUB 也会返回此错误消息。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。

包含多个硬盘的系统不会进行引导

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 PATA (IDE) 磁盘视为 `hd0`，将 SCSI 磁盘视为 `hd1`，尽管 BIOS 中的引导顺序是相反的（SCSI 先于 PATA）。

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。

10.7 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。还请参见 grub 信息页面。您也可以在位于“的支持数据库中搜索关键字”GRUB<http://www.novell.com/support>获得有关特殊问题的信息。

UEFI（统一可扩展固件接口）

UEFI（统一可扩展固件接口）是用于系统硬件自带的固件、系统所有的硬件组件以及操作系统之间的接口。

UEFI 在 PC 系统上的应用范围越来越广，因此正在逐渐替代传统的 PC-BIOS。例如，UEFI 能够很好地支持 64 位系统，提供安全的引导（“安全引导”，要求固件为 2.3.1c 或以上版本）。安全引导是其最为重要的特性之一。最后还有一个要点：带有 UEFI 的标准固件将能够应用于所有 x86 平台。

除此之外，UEFI 还具有以下优点：

- 从带有 GUID 分区表 (GPT) 的大磁盘（超过 2 TiB）引导。
- 独立于 CPU 的架构和驱动程序。
- 带有网络功能的灵活的预操作系统环境。
- 通过 PC-BIOS 式仿真支持引导老式操作系统的 CSM（兼容支持模块）。

有关详细信息，请参见http://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface。以下部分仅针对部分功能在 SUSE Linux Enterprise 中的实施方式而列举一些提示，并不代表 UEFI 的整体概述。

11.1 安全引导

在 UEFI 领域中，要想保障引导程序的安全，需要建立一个信任链。“平台”是信任链的可信根；在使用 SUSE Linux Enterprise 的情况下，可将主板和板载固件

视为“平台”。换言之，它是硬件供应商、从硬件供应商流向组件制造商的信任链、OS 供应商等。

系统通过公共密钥加密法表示信任。硬件供应商将所谓的“平台密钥 (PK)”放入固件中，代表可信根。操作系统供应商与其他方将其密钥与“平台密钥”签署在一起，以此记录他们之间的信任关系。

最后，除非这些“可信的”密钥之一（即 OS 引导加载程序、位于一些 PCI Express 卡的闪存上或磁盘上的一些驱动程序，或者更新的固件本身）签署了代码，否则要求固件不得执行该代码，从而建立安全保障。

基本上，如果您想要使用“安全引导”，则需要使用固件信任的密钥对您的 OS 加载程序进行签名，并且需要 OS 加载程序验证其加载的内核是否可信。

可以将密钥交换密钥 (KEK) 添加到 UEFI 密钥数据库中。这样，其他证书只要签署了 PK 的私用部分，即可由您使用。

11.1.1 在 SUSE Linux Enterprise 上实施

默认情况下安装微软的密钥交换密钥 (KEK)。

注意：需要 GUID 分区表 (GPT)

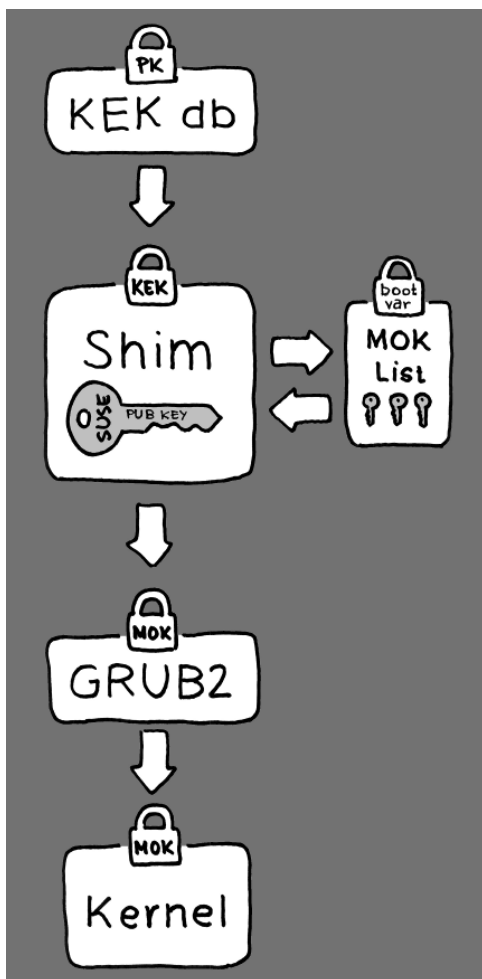
“安全引导”特性要求 GUID 分区表 (GPT) 使用主引导记录 (MBR) 替代旧的分区。

如果安装期间 YaST 检测到 EFI 模式，则会设法创建 GPT 分区。UEFI 预期会在 FAT 格式的 EFI 系统分区 (ESP) 上查找到 EFI 程序。

支持 UEFI 安全引导基本上要求具有固件认可作为可信密钥的数字签名的引导加载程序。密钥需要预先为固件所信任（无需任何手动干预），才能供 SUSE Linux Enterprise 客户使用。

有两种办法可以实现。一种是与硬件供应商合作，让其签署 SUSE 密钥，然后 SUSE 会使用该 SUSE 密钥签署引导加载程序；另一种是通过微软的 Windows 徽标认证计划使引导加载程序获得认证，并使微软认可 SUSE 签名密钥（也就是让引导加载程序签有其 KEK）。至此，SUSE 使引导加载程序获得了 UEFI 签名服务（在此情况下为 Microsoft）的签名。

图 11.1 UEFI: 安全引导流程



SUSE在实施层使用 shim 加载程序。这是一种可以避免法律纠纷的智能解决方案，能够大幅简化认证和签名步骤。shim 加载程序的任务是加载 eLILO 或 GRUB2 等引导加载程序并加以验证；进而该引导加载程序将加载仅获得一个 SUSE 密钥签名的内核。SUSE 在全新安装的 SLE11 SP3 上提供此功能，并要求启用 UEFI 安全引导。

可信用户分为以下两类：

- 首先是持有密钥的用户。平台密钥 (PK) 几乎允许所有操作。密钥交换密钥 (KEK) 的许可范围与 PK 一致，但不能更改 PK。
- 其次是能够以物理方式访问机器的任何用户。具有物理访问权限的用户可以重引导机器并对 UEFI 进行配置。

UEFI 提供下列两类变量以满足这些用户的需求：

- 第一类变量即所谓的“已鉴定的变量”。该变量仅有在变量新值的签名密钥与变量旧值的签名密钥一致时，才可以通过引导程序内部（即所谓的“引导服务环境”）以及运行的 OS 加以更新。而且，您只能向这类变量追加或将其更改为序列号更高的数值。
- 第二类变量即所谓的“仅供引导服务使用的变量”。引导进程中运行的任何代码都可以获取这些变量。在结束引导进程并准备启动 OS 的时间间隔内，引导加载程序必须调用 `ExitBootServices` 呼叫。此后将无法获取这些变量，OS 也无法接触到这些变量。

各类 UEFI 密钥列表属于第一类，因为该类变量除了允许联机更新外，还允许添加密钥、驱动程序、固件指纹以及将其列入黑名单。第二类变量即“仅供引导服务使用的变量”。在既安全又能应用开放源、并因此与 GPLv3 兼容的情况下，该类变量有助于实施安全引导。

SUSE 首先启动 shim。这是一个简单短小的 EFI 引导加载程序，最初由 Fedora 开发。它通过两种证书签名，一种是由 SUSE KEK 签名的证书，另一种是由微软签发的证书，具体取决于系统中的 UEFI 密钥数据库中有哪些 KEK 可用。

这样一来，shim 即可加载并执行。

shim 随后继续验证其想要加载的引导加载程序是否可信。默认情况下，shim 会使用其主体中所嵌入的独立的 SUSE 证书。此外，shim 还允许“登记”其他密钥，用于覆盖默认的 SUSE 密钥。下文将这些密钥称为“机器拥有者密钥”或缩写为 MOK。

接下来，引导加载程序会验证内核，然后加以引导。该内核将在模块上执行同样的操作。

11.1.2 MOK (机器拥有者密钥)

如果用户 (“机器拥有者”) 想要更换引导进程的任何组件, 则会用到“机器拥有者密钥 (MOK)”。他们可以借助 `mokutils` 工具对组件签名及管理 MOK。

登记进程开始重引导机器, 并在 shim 加载期间中断引导进程 (例如按下某个按键)。shim 随后转入登记模式, 允许用户使用引导分区上的文件的密钥替换默认的 SUSE 密钥。如果用户选择这样做, 则 shim 将计算该文件的哈希, 并将计算结果置入“仅供引导服务”的变量中。这样, shim 可以检测到文件除引导服务之外出现的任何更改, 从而避免篡改用户核准的 MOK 列表。

上述各步都在引导期间产生, 此时仅执行已经验证的代码。因此, 只有控制台上所示的一位用户可以使用机器拥有者的一组密钥。它不可能是远程访问 OS 的恶意程序或骇客, 因为骇客或恶意程序只能更改文件, 但无法更改存储在“仅供引导服务使用”的变量中的哈希。

引导加载程序经 shim 加载和验证后, 如果需要验证内核以免验证代码重复, 则会调用回 shim。为此, Shim 将使用同一份 MOK 列表并通知引导加载程序能否加载内核。

这样, 您就可以安装自己的内核或引导加载程序。您只需要安装一组新的密钥, 并在首次重引导期间以物理方式呈现, 从而予以授权。由于 MOK 集是一个密钥列表而非单独一个 MOK, 因此您可以让 shim 信任来自若干不同供应商的密钥, 从而允许引导加载程序进行双重或多重引导。

11.1.3 引导自定义内核

以下内容基于 http://en.opensuse.org/openSUSE:UEFI#Booting_a_custom_kernel。

安全引导不会阻止您使用自行编译的内核。您只需要使用自己的证书在该内核上签名, 并让固件或 MOK 得以识别该证书。

1 创建一个自定义的 X.509 密钥以及用于签名的证书:

```
openssl req -new -x509 -newkey rsa:2048 -keyout key.asc \
-out cert.pem -nodes -days 666 -subj "/CN=$USER/"
```

有关创建证书的详细信息，请参见http://en.opensuse.org/openSUSE:UEFI_Image_File_Sign_Tools#Create_Your_Own_Certificate。

2 将密钥和证书打包成 PKCS#12 结构：

```
openssl pkcs12 -export -inkey key.asc -in cert.pem \
    -name kernel_cert -out cert.p12
```

3 生成用于 pesign 的 NSS 数据库：

```
certutil -d . -N
```

4 将 PKCS#12 中包含的密钥和证书导入 NSS 数据库：

```
pk12util -d . -i cert.p12
```

5 使用 pesign 将新签名“赋予”内核：

```
pesign -n . -c kernel_cert -i arch/x86/boot/bzImage \
    -o vmlinuz.signed -s
```

6 列出内核映像上的签名：

```
pesign -n . -S -i vmlinuz.signed
```

此时，您可以照常在 `/boot` 中安装内核。由于内核现有一个自定义的签名，因此需要将用于签名的证书导入 UEFI 固件或 MOK 中。

7 将证书转为 DER 格式，以供导入固件或 MOK：

```
openssl x509 -in cert.pem -outform der -out cert.der
```

8 将证书复制到 ESP 以简化访问：

```
sudo cp cert.der /boot/efi/
```

9 使用 mokutil 自动启动 MOK 列表。

此外，若要手动启动 MOK，也可以采用这一过程：

9a 重引导。

9b 在 GRUB 菜单中，按“c”键。

9c 类型:

```
chainloader $efibootdir/MokManager.efi
boot
```

9d 选择从磁盘登记密钥。

9e 导航至 cert.der 文件并按 Enter。

9f 按照指导登记密钥。正常情况下应按“0”，然后按“y”予以确认。

除此之外，固件菜单也可能提供了多种向“签名数据库”中添加新密钥的方式。

11.1.4 限制

以安全引导模式引导时，会有以下限制：

- 在 UEFI 系统中不会将混合式 ISO 映像识别为可引导的映像。因此，SP3 不支持从 USB 设备进行 UEFI 引导。
- 为确保他人无法轻易绕过安全引导，系统在安全引导下运行时会禁用部分内核特性。
- 引导加载程序、内核以及内核模块必须经过签名。
- kexec 和 kdump 处于禁用状态。
- 休眠（挂起到磁盘）处于禁用状态。
- 无法访问 /dev/kmem 和 /dev/mem，连根用户也不例外。
- 无法访问 I/O 端口，连根用户也不例外。所有 X11 图形驱动程序必须使用内核驱动程序。
- 无法通过 sysfs 访问 PCI BAR。
- 无法使用 ACPI 中的 custom_method。
- 无法使用 asus-wmi 模块的 debugfs。

- 参数 `acpi_rsdp` 对内核完全失去影响。

11.2 更多信息

- <http://www.uefi.org> —UEFI 主页列出了当前的 UEFI 规范。
- 由 Olaf Kirch 与 Vojtěch Pavlík 撰写的博文（上述章节内容主要取材于这些博文）：
 - <http://www.suse.com/blogs/uefi-secure-boot-plan/>
 - <http://www.suse.com/blogs/uefi-secure-boot-overview/>
 - <http://www.suse.com/blogs/uefi-secure-boot-details/>
- <http://en.opensuse.org/openSUSE:UEFI> —UEFI 与 openSUSE。

特别的系统功能组件

本章首先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。

12.1 特殊软件包的相关信息

程序 `bash`、`cron`、`logrotate`、`locate`、`ulimit` 和 `free` 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。

12.1.1 `bash` 包和 `/etc/profile`

`Bash` 是默认的系统外壳。在用作登录外壳时，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. ~/.profile
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。执行以下外壳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。

12.1.2 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 12.1 “/etc/crontab 中的项” [136] 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 12.1 /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。必须直接将此文件装载到编辑器中，然后对其进行修改并保存。

许多包将外壳脚本安装到目录 /etc/cron.hourly、/etc/cron.daily、/etc/cron.weekly 和 /etc/cron.monthly，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，请删除通常使用 /etc/crontab 项的时戳文件（请参见例 12.2 “/etc/crontab：删除时戳文件”[137]，它删除了每个整点之前的 hourly 和每天凌晨 2:14 的 daily 等）。

例 12.2 /etc/crontab：删除时戳文件

```
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 设置为应启动 cron.daily 的时间。MAX_NOT_RUN 的设置确保日常任务被触发运行，即使用户在很长时间里没有在指定的 DAILY_TIME 打开计算机。MAX_NOT_RUN 的最大值为 14 天。

为了清楚起见，将日常系统维护任务分布在多个脚本中。这些脚本包含在包 aaa_base 中。例如，/etc/cron.daily 包含组件 suse.de-backup-rpmdb、suse.de-clean-tmp 或 suse.de-cron-local。

12.1.3 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，这些文件附于包 apache2 (/etc/logrotate.d/apache2) 和 syslogd (/etc/logrotate.d/syslog) 中。

例 12.3 /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。

12.1.4 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。

12.1.5 ulimit 命令

使用 **ulimit**（用户限制）命令可以为系统资源的使用设置限制并使其显示出来。**ulimit** 对于限制应用程序的可用内存尤其有用。设置可用内存限制后，可以防止应用程序占用过多系统资源，而导致操作系统变慢甚至挂起。

可以对 **ulimit** 使用多个选项。要限制使用内存，请使用表 12.1 “**ulimit**：为用户设置资源” [139] 中列出的选项。

表 12.1 *ulimit*: 为用户设置资源

-m	最大驻留集大小
-v	壳层可用虚拟内存的最大量
-s	堆栈的最大大小
-c	创建的核心文件的最大大小
-a	所有当前限制均已报告

可以在 `/etc/profile` 中创建系统范围的项。在这里可以创建核心文件（编程人员调试时需要使用）。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 12.4 *ulimit*: `~/.bashrc` 中的设置

```
# Limits maximum resident set size (physical memory):
ulimit -m 98304

# Limits of virtual memory:
ulimit -v 98304
```

必须以 KB 为单位指定内存分配。有关详细信息，请参见 `man bash`。

重要

并非所有外壳都支持 `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。

12.1.6 free 命令

`free` 命令显示系统中的可用内存总量、已用物理内存和交换空间，以及内核占用的缓冲区和缓存。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，内核中还包含其他缓存，如 `slab` 缓存，其中储存着用于网络访问的缓存。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）上述缓存。

但是如果您的目的是找出当前所用的 RAM 量，则在 `/proc/meminfo` 中查找此信息。

12.1.7 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，这些页面中提供了更多深入说明。`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。

12.1.8 使用 man 命令选择手册页

要阅读手册页，请输入 `man 手册页`。如果不同章节存在同名手册页，所有手册页都会带相应部分编号列出。选择要显示的一个手册页。如果在数秒内未输入部分编号，将显示第一个手册页。

如果要将此更改为默认系统行为，请在外壳初始化文件（如 `~/.bashrc`）中设置 `MAN_POSIXLY_CORRECT=1`。

12.1.9 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 会读取包含用户、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此文件中。

通过 SUSE Linux Enterprise Server，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，可安装众多外接式附件包：`emacs-auctex`（LaTeX）、`psgml`（SGML 和 XML）、`gnuserv`（客户端和服务端操作）等。

12.2 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

显示内核消息。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`。

12.3 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/.emacs
/etc/skel/.gnu-emacs
/etc/skel/.vimrc
/etc/csh.cshrc
/etc/termcap
/usr/share/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，可以如 `/etc/X11/Xmodmap` 中所说明的启用 **Compose** 键（多键）。

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** 的信息可以在 `/usr/share/doc/packages/xkeyboard-config`（`xkeyboard-config` 包的一部分）所列的文档中找到。

12.4 语言和国家/地区特定的设置

该系统在很大程度上实现了国际化，可修改以满足本地需要。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、时间和日期、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（请参见手册页 `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_` 前缀的形式传递到外壳，它们代表所列出的类别。下面列出了相关外壳配置文件。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（请参见第 9.3.1 节“使用 YaST Sysconfig 编辑器更改系统配置”[105]）。此类变量的值包含语言代码、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>]]
```

12.4.1 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（参见 http://en.wikipedia.org/wiki/ISO_3166）中列出。

只有设置可以在 `/usr/lib/locale` 中找到其可用描述文件的值才有意义。可以使用命令 `localedef` 基于 `/usr/share/i18n` 中的文件创建更多描述文件；描述文件是 `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）的描述文件：

```
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。此设置现已过时，因为 `UTF-8` 也可涵盖欧元符号。仅当应用程序支持 `ISO-8859-15` 而不是 `UTF-8` 时，它才有用。

在以前的版本中，在对 `/etc/sysconfig/language` 执行任何更改后必须运行 `SuSEconfig`。`SuSEconfig` 之后将更改写入 `/etc/SuSEconfig/profile` 和 `/etc/SuSEconfig/csh.login`。登录时，这些文件由 `/etc/profile`（对于 `Bash`）或 `/etc/csh.login`（对于 `tcsh`）读取。

在最近的版本中，`/etc/SuSEconfig/profile` 已替换为 `/etc/profile.d/lang.sh`，`/etc/SuSEconfig/csh.login` 则替换为 `/etc/profile.d/lang.csh`。但如果这两个旧文件存在，登录时仍会读取它们。

进程链现在如下所示：

- 对于 `Bash`：`/etc/profile` 读取 `/etc/profile.d/lang.sh`，后者则分析 `/etc/sysconfig/language`。

- 对于 **tcsh**：/etc/csh.login 在登录时读取 /etc/profile.d/lang.csh，后者则分析 /etc/sysconfig/language。

这确保了在下次登录到相应外壳时 /etc/sysconfig/language 的任何更改均可用，而无需先运行 **SuSEconfig**。

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 用于程序消息，请包括 LC_MESSAGES=es_ES，这样消息将以西班牙语显示。

12.4.2 ~/.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
```

12.4.3 语言支持的设置

消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 中的消息文件不存在，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。

12.4.4 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。该包可从 SUSE Linux Enterprise SDK 中获取。SDK 是 SUSE Linux Enterprise 的外接式附件产品，可从 http://www.novell.com/developer/sle_sdk.html 下载。
- 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>。
- Bruno Haible 撰写的 *Unicode-Howto* 可在 <http://tldp.org/HOWTO/Unicode-HOWTO-1.html> 中获得。

打印机操作

SUSE® Linux Enterprise Server 支持用许多类型的打印机进行打印，包括远程网络打印机。可以手动或使用 YaST 配置打印机。有关配置描述，请参见第 8.5 节“设置打印机”(第 8 章 使用 YaST 设置硬件组件, ↑部署指南)。启动和管理打印任务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，请参见第 13.7 节“查错”[155]。

CUPS（通用 Unix 打印系统）是 SUSE Linux Enterprise Server 中的标准打印系统。

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任务。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。

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 任务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，可以生成令人满意的打印效果。Linux 可能无法使用某些特殊打印机功能。除了 HP 开发的 HPLIP (HP Linux Imaging and Printing) 之外，目前尚无其他打印机制造商开发 Linux 驱动程序并在开放源代码许可证下将这些驱动程序提供给 Linux 经销商。

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 13.7.1 节“打印机没有标准打印机语言支持”[155]。

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.linuxfoundation.org/OpenPrinting/>

包含打印机数据库的 OpenPrinting 主页。数据库显示最新的 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 Server 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。

<http://pages.cs.wisc.edu/~ghost/>

Ghostscript 网页

`/usr/share/doc/packages/ghostscript-library/catalog.devices`
包含的驱动程序列表。

13.1 打印系统工作流程

用户创建一个打印任务。该打印任务包含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，例如特定于打印机的选项。

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任务，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，则过滤器系统将数据转换为打印机专用的数据。这样做需要一个适合您的打印

机的打印机驱动程序。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。

13.2 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。

► **System z:** CUPS 或 LPRng 不支持 z/VM 提供的可与 IBM System z 大型机进行本地连接的打印机和类似设备。在这些平台上，只能通过网络进行打印。必须根据打印机制造商的描述安装网络打印机的电缆。 ◀

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。

13.3 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。SUSE Linux Enterprise Server 安装期间将预安装多个 PPD 文件。

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 13.6.2 节 “多种包中的 PPD 文件” [153] 和第 13.7.2 节 “没有合适的 PPD 文件可用于 PostScript 打印机” [156]。

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, 如第 8.5.1.1 节 “使用 YaST 添加驱动程序” (第 8 章 *使用 YaST 设置硬件组件*, ↑*部署指南*) 中所述。随后, 可以在打印机设置过程中选择 PPD 文件。

如果打印机制造商希望您安装整个软件包, 请务必小心。首先, 此类安装将导致丢失 SUSE Linux Enterprise Server 提供的支持; 其次, 打印命令可能以不同

的方式运行，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。

13.4 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。尽管大部分支持的协议都已标准化，但某些制造商可能修改了标准。他们仅提供适用于少数操作系统的驱动程序。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。

CUPS 支持 `socket`、`LPD`、`IPP` 和 `smb` 协议。

`socket`

套接字是指将纯文本打印数据直接发送到 TCP 套接字的连接。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）

`LPD` 协议如 RFC 1179 中所述。使用此协议，打印机队列 ID 等任务相关数据将在发送实际打印数据之前发送。因此，配置 `LPD` 协议时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。`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` 协议的相对较新的协议 (1999)。使用 `IPP`，所传送的与任务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。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`（随 `nmap` 包提供）来确定协议。`nmap` 检查主机端口是否打开。例如：

```
nmap -p 35,137-139,515,631,9100-10000 printerIP
```

13.4.1 使用命令行工具配置 CUPS

CUPS 可使用 `lpinfo`、`lpadmin` 和 `lpoptions` 之类的命令行工具配置。您需要一个设备 URI，该 URI 由一个后端（例如并行端口）和多个参数组成。要确定系统上的有效设备 URI，请使用命令 `lpinfo -v | grep "://"`：

```
# lpinfo -v | grep "://"
direct usb://ACME/FunPrinter%20XL
direct parallel:/dev/lp0
```

使用 `lpadmin`，CUPS 服务器管理员可以添加、删除或管理打印队列。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 URI。

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(8)` 的手册页。

在系统安装期间，某些选项被设置为默认值。可以为每个打印任务修改这些选项（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 ~/.cups/lpoptions。但是，根设置将写到 /etc/cups/lpoptions。

13.5 从命令行打印

要从命令行打印，请输入 `lp -d 队列名称 文件名`，使用相应的名称替换队列名称和文件名。

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（通常无需指定文件名），例如 `lp -d 队列名称`。

13.6 SUSE Linux Enterprise Server 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 Server。这里将介绍一些最重要的更改。

13.6.1 CUPS 和防火墙

执行默认 SUSE Linux Enterprise Server 安装后，SuSEFirewall2 处于活动状态，且网络接口配置为处于外部区域中，该区域将阻止进来的通讯。第 15.4 节“SuSEfirewall2”（第 15 章 *Masquerading and Firewalls*, ↑安全指南）中提供了有关 SuSEFirewall2 配置的更多信息。

13.6.1.1 CUPS 客户端

通常 CUPS 客户端在使用防火墙的可信网络环境中的常规工作站上运行。在这种情况下，建议将网络接口配置为在内部区域中，这样可以从网络内部访问工作站。

13.6.1.2 CUPS 服务器

如果 CUPS 服务器在受防火墙保护的可信网络环境中，则应将网络接口配置为在防火墙的内部区域中。建议不要在不可信网络环境中安装 CUPS 服务器，除非留心该服务器受到特殊防火墙规则和 CUPS 配置中的安全设置的保护。

13.6.2 多种包中的 PPD 文件

YaST 打印机配置使用 `/usr/share/cups/model` 中安装的 PPD 文件为 CUPS 设置队列。为查找适用于打印机型号的 PPD 文件，YaST 将对硬件检测过程中确定的供应商和型号以及所有 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。

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。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 `gutenprint` 包中的 `Gutenprint` 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。

13.6.2.1 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

13.6.2.2 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。

YaST 通常首选 manufacturer-PPD 文件。但是，如果没有合适的 manufacturer-PPD 文件，将选择带有项 *NickName: ... Foomatic ... (recommended) 的 Foomatic PPD 文件。

13.6.2.3 gutenprint 包中的 Gutenprint PPD 文件

Gutenprint（以前称为 GIMP-Print）中的 CUPS 过滤器 `rastertogutenprint`（而不是 `foomatic-rip`）可用于许多非 PostScript 打印机。gutenprint 包中提供了该过滤器和适合的 Gutenprint PPD 文件。Gutenprint PPD 文件位于 /usr/share/cups/model/gutenprint/ 中并具有项 *NickName: ... CUPS+Gutenprint 和 *cupsFilter: ... rastertogutenprint。

13.6.2.4 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。YaST 倾向于使用 manufacturer-PPDs 中的 PPD 文件。如果型号名称不匹配，则 YaST 不能使用 manufacturer-PPDs 包中的 PPD 文件。如果

manufacturer-PPDs 包对于相似型号（如 Funprinter 12xx 系列）仅包含一个 PPD 文件，则可能发生这种情况。在这种情况下，请手动在 YaST 中选择相应的 PPD 文件。

13.7 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。

13.7.1 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，所以这些打印机也称作 *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 打印机可切换成以 GDI 方式或一种标准打印机语言进行操作。请参见打印机手册以了解这是否可行。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。

与其花时间尝试使专有 Linux 驱动程序运行，购买支持标准打印机语言（最好是 PostScript）的打印机可能更经济高效。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。

13.7.2 没有合适的 PPD 文件可用于 PostScript 打印机

如果 `manufacturer-PPDs` 包不包含适用于 PostScript 打印机的 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 文件的许可证协议条款。然后使用 `cupstestppd` 实用程序来确认 PPD 文件是否与“Adobe PostScript 打印机描述文件格式规范 V4.3”相符合，如果实用程序返回“FAIL，”则描述 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。

13.7.3 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 13.1“`/etc/modprobe.conf`：第一个并行端口的中断方式”[157]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=nones`。

例 13.1 /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
```

13.7.4 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 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，响应应该描述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 13.2“来自 lpd 的错误消息”[157] 中的响应，则问题是由远程 lpd 引起的。

例 13.2 来自 lpd 的错误消息

```
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

CUPS 网络服务器可以在 UDP 端口 631 上广播其队列，默认每 30 秒广播一次。因此，以下命令可用于测试网络中是否存在广播 CUPS 网络服务器。执行此命令之前，务必停止本地 CUPS 守护程序。

```
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 13.3 “来自 CUPS 网络服务器的广播” [158] 所示。

例 13.3 来自 CUPS 网络服务器的广播

```
ipp://192.168.2.202:631/printers/queue
```

► **System z:** 要考虑到 IBM System z 以太网设备默认情况下不接收广播这一情况。 ◀

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任务。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任务时，有时会导致出现问题。由于这是打印服务器计算机中的假脱机程序导致的，目前尚无解决此问题的方法。作为变通方法，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 13.4 节“网络打印机” [150]。

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，请参见 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。

13.7.5 打印件有问题但没有错误消息

对于打印系统，打印任务完成的标志是 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特定于打印机的数据），则打印系统不会对此进行通知。如果打印机无法打印特定于打印机的数据，请选择另一个更适合该打印机的 PPD 文件。

13.7.6 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。后端用于确定在将数据传送报告为不可行前应执行的失败尝试次数。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 cupsenable 命令重新启用打印。

13.7.7 CUPS 浏览：删除打印任务

如果 CUPS 网络服务器通过浏览向客户端主机广播其队列并且客户端主机上合适的本地 cupsd 处于活动状态，则客户端 cupsd 接受来自应用程序的打印任务并将它们转发到服务器上的 cupsd。当服务器上的 cupsd 接受打印任务后，会为该任务指派一个新的任务号。因此，客户端主机上的任务号与服务器上的

任务号不同。因为通常都将打印任务立即转发，所以不能用客户端主机上的任务号将其删除，原因是一旦将打印任务转发到服务器 cupsd，客户端 cupsd 就会将打印任务视为已完成。

要删除服务器上的打印任务，请使用命令（例如 `lpstat -h cups.example.com -o`）确定服务器上的任务号，前提是此服务器尚未完成该打印任务（即尚未完全将其发送到打印机）。使用此任务号，可以删除服务器上的打印任务：

```
cancel -h cups.example.com queue-jobnumber
```

13.7.8 有问题的打印任务和数据传送错误

如果在打印过程中关闭打印机或计算机，则打印任务将保留在队列中。再次打开计算机（或打印机）后，打印将继续。必须使用 `cancel` 从队列中删除有问题的打印任务。

如果打印任务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。要调整此情况，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 打印任务可能仍在队列中，因为只有在将任务完全发送到打印机后才会将它们删除。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` 可以删除打印任务。
- 3 即使已将打印任务从队列中删除，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置打印机。然后插入纸张并打开打印机。

13.7.9 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 删除 `/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*` 中的消息以确定问题的原因。

13.7.10 更多信息

SUSE 知识库 (<http://www.suse.com/support/>) 中提供了对许多特定问题的解决方案。通过对 CUPS 的文本搜索找到相关文章。

使用 udev 进行动态内核设备管理

14

内核几乎可以添加或删除运行系统中的任何设备。设备状态的更改（无论插入还是删除设备）需要传播给用户空间。插入或者识别设备后需要进行配置。某个设备已识别状态的任何更改都需要通知给此设备的用户。udev 可提供所需的基础结构来动态维护 `/dev` 目录中的设备节点文件和符号链接。udev 规则提供了将外部工具插入内核设备事件处理的方式。这使您能够自定义 udev 设备处理，例如通过添加特定脚本来作为内核设备处理的一部分执行，或者请求并导入额外数据以在设备处理期间评估。

14.1 `/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，则删除此设备节点。

`/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提供的。手动创建或修改的文件在重引导时是有意不保存的。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。

14.2 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。

每次添加或删除设备时，内核都会发送 `uevent` 来向 `udev` 通知更改。一旦启动，`udev` 守护程序便会读取和分析 `/etc/udev/rules.d/*.rules` 文件中提供的所有规则，并将它们保留在内存中。如果更改、添加或删除了规则文件，则守护程序可以使用命令 `udevadm control reload_rules` 重新装载所有规则在内存中的表示形式。运行 `/etc/init.d/boot.udev reload` 时也会执行此操作。有关 `udev` 规则及其语法的更多细节，请参见第 14.6 节“使用 `udev` 规则影响内核设备事件处理”[166]。

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键、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核心 `uevent`。

14.3 驱动程序、内核模块和设备

设备的内核总线驱动程序探测。对于每个检测到的设备，内核都会在驱动程序核心将 `uevent` 发送到 `udev` 守护程序时创建内部设备结构。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。所有这些操作均由 `udev` 自动触发。

14.4 引导和启动设备设置

在 `udev` 守护程序运行之前的引导进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 `root` 文件系统中，并且此时不可用。为了弥补此损失，内核提供了一个 `uevent` 文件，该文件位于 `sysfs` 文件系统每个设备的设备目录中。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` 触发器中所有 `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 鼠标可能不会由早期引导逻辑初始化，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。不用手动搜索可能连接的设备，`udev` 会在 `root` 文件系统可用后直接从内核请求所有设备事件，以便 USB 鼠标设备的事件可以再次运行。现在它在装入的 `root` 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。

14.5 监视正在运行的 `udev` 守护程序

程序 `udevadm monitor` 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[1185238505.276660] add    /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UDEV   [1185238505.279198] add    /devices/pci0000:00/0000:00:1d.2/usb3/3-1
(usb)
UEVENT[1185238505.279527] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UDEV   [1185238505.285573] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0 (usb)
UEVENT[1185238505.298878] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UDEV   [1185238505.305026] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10 (input)
UEVENT[1185238505.305442] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
UEVENT[1185238505.306440] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
UDEV   [1185238505.325384] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/event4 (input)
```

```
UDEV [1185238505.342257] add
/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10/mouse2 (input)
```

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于主磁盘事件从硬件查询的数据。

`udevadm monitor --env` 显示完整的事件环境：

```
ACTION=add
DEVPATH=/devices/pci0000:00/0000:00:1d.2/usb3/3-1/3-1:1.0/input/input10
SUBSYSTEM=input
SEQNUM=1181
NAME="Logitech USB-PS/2 Optical Mouse"
PHYS="usb-0000:00:1d.2-1/input0"
UNIQ=""
EV=7
KEY=70000 0 0 0 0
REL=103
MODALIAS=input:b0003v046DpC03Ee0110-e0,1,2,k110,111,112,r0,1,8,amlsfw
```

udev 也将消息发送给 **syslog**。用于控制将哪些消息发送到系统日志的默认系统日志优先级在 **udev** 配置文件 `/etc/udev/udev.conf` 中指定。可以使用 `udevadm control log_priority=level/number` 更改正在运行的守护程序的日志优先权。

14.6 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、添加指向该节点的符号链接或者运行作为事件处理一部分的特定程序。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。**udev** 手册页中描述了有关规则

语法和提供用来与数据匹配或导入数据的关键字的详细信息。以下示例规则提供了 udev 规则语法的基本介绍。这些示例规则全部取自 `/etc/udev/rules.d/50-udev-default.rules` 下的 udev 默认规则集。

例 14.1 示例 udev 规则

```
# console
KERNEL=="console", MODE="0600", OPTIONS="last_rule"

# serial devices
KERNEL=="ttyUSB*", ATTRS{product}=="[Pp]alm*Handheld*", SYMLINK+="pilot"

# printer
SUBSYSTEM=="usb", KERNEL=="lp*", NAME="usb/%k", SYMLINK+="usb%k", GROUP="lp"

# kernel firmware loader
SUBSYSTEM=="firmware", ACTION=="add", RUN+="firmware.sh"
```

`console` 规则由三个键构成：一个匹配键 (`KERNEL`) 和两个赋值键 (`MODE`、`OPTIONS`)。`KERNEL` 匹配规则搜索设备列表以查找类型为 `console` 的所有项。只有完全匹配才有效，才能触发执行此规则。在这种情况下，`MODE` 关键字为设备节点指派特殊权限，仅为该设备的拥有者指派读写权限。`OPTIONS` 关键字将该规则标记为此类型的所有设备最后采用的规则。匹配此特殊设备类型的任何后续规则都不产生任何影响。

`50-udev-default.rules` 中不再提供 `serial devices` 规则，但该规则仍然值得考虑。该规则由两个匹配关键字 (`KERNEL` 和 `ATTRS`) 和一个赋值关键字 (`SYMLINK`) 构成。`KERNEL` 关键字搜索类型为 `ttyUSB` 的所有设备。该关键字使用 `*` 通配符匹配这些设备中的几个。第二个匹配关键字 `ATTRS` 检查任何 `ttyUSB` 设备的 `sysfs` 中的 `product` 属性文件是否包含特定字符串。赋值关键字 (`SYMLINK`) 将符号链接添加至该设备的 `/dev/pilot` 下。此关键字中使用的运算符 (`+=`) 告知 `udev` 进一步执行此操作，即使前面或后面的规则添加其他符号链接。由于此规则包含两个匹配关键字，因此仅当两个条件都满足时，才应用。

`printer` 规则处理 **USB** 打印机，其中包含两个匹配关键字 (`SUBSYSTEM` 和 `KERNEL`)，并且必须同时应用这两个关键字，才能应用整个规则。三个赋值键处理该设备类型的命名 (`NAME`)、符号设备链接 (`SYMLINK`) 的创建，以及此设备类型的组成员资格 (`GROUP`)。在 `KERNEL` 关键字中使用通配符 `*` 将使其匹配若干 `lp` 打印机设备。`NAME` 和 `SYMLINK` 关键字中都使用了替换项，以便按内部设备名称扩展这些字符串。例如，指向第一个 `lp` **USB** 打印机的符号链接为 `/dev/usb/lp0`。

kernel firmware loader 规则用于使 **udev** 在运行时期间通过外部助手脚本装载其他固件。SUBSYSTEM 匹配关键字搜索 firmware 子系统。ACTION 关键字检查是否添加了属于 firmware 子系统的任何设备。RUN+= 关键字触发执行 firmware.sh 脚本，以便找到应装载的固件。

所有规则具有一些共同的特征：

- 每个规则由一个或多个以逗号分隔的关键字值对构成。
- 关键字的运算由运算符确定。udev 规则支持多个不同的运算符。
- 每个给定值必须用引号引起来。
- 规则文件的每一行代表一个规则。如果一个规则超过一行，请使用 \ 合并不同行，就像在壳层语法中一样。
- udev 规则支持与 *、? 和 [] 模式匹配的外壳式模式。
- udev 规则支持替换。

14.6.1 在 udev 规则中使用运算符

创建可以从若干不同运算符选择的关键字，具体取决于希望创建的关键字类型。匹配关键字通常仅用于查找匹配或明显不匹配搜索值的值。匹配关键字包含以下运算符之一：

==

比较等于性。如果关键字包含搜索模式，则匹配该模式的所有结果均有效。

!=

比较不等于性。如果关键字包含搜索模式，则匹配该模式的所有结果均有效。

赋值关键字可以使用下面的任何运算符：

=

为关键字指派值。如果关键字以前由一系列值构成，关键字将重置，并且仅指派一个值。

`+=`

为包含一系列项的关键字添加一个值。

`:=`

指派最终值。不允许后面的规则进行任何后续更改。

14.6.2 在 udev 规则中使用替换项

udev 规则支持使用占位符和替换项。请按照在其他任何脚本中的相同方式使用。在 udev 规则中可使用以下替换项：

`%r`、`$root`

设备目录 `/dev`（默认）。

`%p`、`$devpath`

`DEVPATH` 的值。

`%k`、`$kernel`

`KERNEL` 的值或内部设备名称。

`%n`、`$number`

设备号。

`%N`、`$tempnode`

设备文件的临时名称。

`%M`、`$major`

设备的主编号。

`%m`、`$minor`

设备的次编号。

`%s{attribute}/$attr{attribute}`

`sysfs` 属性的值（由 `attribute` 指定）。

`%E{variable}`、`$attr{variable}`

环境变量的值（由 `variable` 指定）。

`%c`、`$result`
PROGRAM 的输出。

`%%`
% 字符。

`$$`
\$ 字符。

14.6.3 使用 udev 匹配关键字

匹配关键字描述应用 udev 规则之前必须满足的条件。以下匹配关键字可用：

ACTION
事件操作的名称，如 `add` 或 `remove`（添加或删除设备时）。

DEVPATH
事件设备的设备路径，如 `DEVPATH=/bus/pci/drivers/ipw3945`，用于搜索与 `ipw3945` 驱动程序有关的所有事件。

KERNEL
事件设备的内部（内核）名称。

SUBSYSTEM
事件设备的子系统，如 `SUBSYSTEM=usb`（用于与 USB 设备有关的所有事件）。

ATTR{*filename*}
事件设备的 `sysfs` 属性。例如，要匹配 `vendor` 属性文件名中包含的字符串，可以使用 `ATTR{vendor}=="On[sS]tream"`。

KERNELS
让 udev 向上搜索设备路径以查找匹配的设备名称。

SUBSYSTEMS
让 udev 向上搜索设备路径以查找匹配的设备子系统名称。

DRIVERS

让 `udev` 向上搜索设备路径以查找匹配的设备驱动程序名称。

ATTRS{*filename*}

让 `udev` 向上搜索设备路径以查找具有匹配的 `sysfs` 属性值的设备。

ENV{*key*}

环境变量的值，如 `ENV{ID_BUS}="ieee1394"`，用于搜索与该 FireWire 总线 ID 有关的所有事件。

PROGRAM

让 `udev` 执行外部程序。程序必须返回退出码零，才能成功。程序的输出（打印到 `stdout`）可用于 `RESULT` 关键字。

RESULT

匹配上次 `PROGRAM` 调用的输出字符串。在与 `PROGRAM` 关键字相同的规则中包含该关键字，或在后面的一个中。

14.6.4 使用 `udev` 指派关键字

与上述匹配键相比，赋值键未描述必须满足的条件。它们将值、名称和操作指派给由 `udev` 维护的设备节点。

NAME

将创建的设备节点的名称。在一个规则设置节点名称之后，将对该节点忽略带有 `NAME` 关键字的其他所有规则。

SYMLINK

与要创建的节点有关的符号链接名称。多个匹配的规则可添加要使用设备节点创建的符号链接。也可以通过使用空格字符分隔符号链接名称，在一个规则中为一个节点指定多个符号链接。

OWNER, GROUP, MODE

新设备节点的权限。此处指定的值重写已编译的任何值。

ATTR{*key*}

指定要写入事件设备的 `sysfs` 属性的值。如果使用 `==` 运算符，也将使用该关键字匹配 `sysfs` 属性的值。

ENV{*key*}

告知 udev 将变量导出到环境。如果使用 == 运算符，也将使用该关键字匹配环境变量。

RUN

告知 udev 向程序列表添加要为该设备执行的程序。请记住，将此程序限制于很短的任务，以免妨碍此设备的后续事件。

LABEL

添加 GOTO 可跳至的标签。

GOTO

告知 udev 跳过一些规则，继续执行具有按 GOTO 关键字引用的标签的规则。

IMPORT{*type*}

将变量装载入外部程序输出之类的事件环境中。udev 导入不同类型的若干变量。如果未指定任何类型，udev 将尝试根据文件许可权限的可执行位来自行确定类型。

- program 告知 udev 执行外部程序并导入其输出。
- file 告知 udev 导入文本文件。
- parent 告知 udev 从父设备导入储存的关键字。

WAIT_FOR_SYSFS

告知 udev 等待要为某个设备创建的指定 sysfs 文件。例如，
WAIT_FOR_SYSFS="ioerr_cnt" 通知 udev 等待 ioerr_cnt 文件创建完成。

OPTIONS

OPTION 关键字可能有若干值：

- last_rule 告知 udev 忽略后面的所有规则。
- ignore_device 告知 udev 完全忽略此事件。
- ignore_remove 告知 udev 忽略后面针对设备的所有删除事件。

- `all_partitions` 告知 `udev` 为块设备上的所有可用分区创建设备节点。

14.7 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` 还维护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
```

14.8 udev 使用的文件

`/sys/*`

Linux 内核提供的虚拟文件系统，用于导出所有当前已知设备。此信息由 `udev` 用于在 `/dev` 中创建设备节点

`/dev/*`

动态创建的设备节点和引导时从 `/lib/udev/devices/*` 复制的静态内容

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。

14.9 更多信息

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。

udevadm

udevadm 可用于控制 udev 的运行时行为、请求内核事件、管理事件队列，以及提供简单的调试机制。

udevd

有关 udev 事件管理守护程序的信息。

X Window 系统

X Window 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 Window 系统环境的安装和优化，并提供了关于在 SUSE® Linux Enterprise Server 中使用字体的背景信息。

提示：IBM System z：配置图形用户界面

IBM System z 没有 X.Org 支持的任何输入和输出设备。因此，本部分中描述的任何配置过程均不适用。有关 IBM System z 的更多相关信息，请参见第 4 章在 IBM System z 上安装 (↑部署指南)。

15.1 手动配置 X Window 系统

默认设置下，以第 8.2 节“设置图形卡和监视器” (第 8 章 使用 YaST 设置硬件组件, ↑部署指南) 中所述用 SaX2 界面配置 X Window 系统。或者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 Window 系统时要小心。在完成配置前，切勿启动 X Window 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 Server 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，但并不能保证所提供的�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 Window 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

使用 `X -configure` 配置您的 X 安装（如果之前尝试 SUSE Linux Enterprise Server 的 `SaX2` 失败）。如果您的安装涉及专有的仅二进制驱动程序，则 `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 15.1 “`/etc/X11/xorg.conf` 中的部分” [176] 中列出了可用的部分类型。

表 15.1 `/etc/X11/xorg.conf` 中的部分

类型	含义
Files	用于字体和 RGB 颜色表的路径。
ServerFlags	服务器行为的常规切换。
Module	服务器应装载的模块列表。
InputDevice	在此部分中配置输入设备，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。

类型	含义
Monitor	使用的显示器。此部分的重要元素是标识符（稍后在 Screen 定义中引用）、刷新率 VertRefresh 和同步频率限制（HorizSync 和 VertRefresh）。这些设置采用的单位为 MHz、kHz 和 Hz。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。
Modes	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 /usr/share/doc/howto/en/html/XFree86-Video-Timings-HOWTO）提供了各个数字值含义的细节（在 howtoenh 包中提供）。要手动计算 VESA 方式，可使用工具 cvt。例如，要计算 1680x1050@60Hz 监视器的模式行，请使用命令 <code>cvt 1680 1050 60</code> 。
Device	特定的图形卡。系统通过其描述性名称来参考图形卡。本部分中的可用选项高度依赖于所用驱动程序。例如，如果使用 i810 驱动程序，请在手册页 <code>man 4 i810</code> 中查找有关各种可用选项的更多信息。
Screen	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

类型	含义
	(Virtual) 的大小、用于此屏幕的 ViewPort 和 Modes。 请注意，某些驱动程序要求 Display 部分中某个位置内必须存在所用的全部配置。例如，如果使用便携式计算机并希望使用比内部 LCD 更大的外部监视器，可能需要在 Modes 行结尾处添加内部 LCD 支持的更大分辨率。
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。

15.1.1 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 15.1 “文件 /etc/X11/xorg.conf 的 Screen 部分” [178] 类似。

例 15.1 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]"⑦
Monitor         "Monitor[0]"
EndSection

```

- ① Section 确定该部分的类型，在本示例中是 Screen。
- ② DefaultDepth 决定默认使用的颜色深度（除非明确指定其他颜色深度）。
- ③ 对每种颜色深度指定不同的 Display 子部分。
- ④ Depth 决定对本组 Display 设置使用的颜色深度。可能的值有 8、15、16、24 和 32，尽管并非所有 X 服务器模块或分辨率都支持所有这些值。
- ⑤ 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。

- ⑥ 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。

15.1.2 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，有一个 `/usr/lib/xorg/modules/drivers` 目录或 `/usr/lib64/xorg/modules/drivers` 目录，用于 64 位操作系统目录。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/packages/package_name` 中驱动程序模块的描述文件中。通常还可以在手册页（`man xorg.conf`、`man 4 <driver module>` 和 `man 4 chips`）中找到有效的选项。

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。

15.1.3 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）。可以使用实用程序 `cvt` 生成 VESA 方式。有关更多信息，请参见 `cvtman cvt` 的手册页。

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。

如果您要创建自己的监视器描述，则应非常熟悉 `/usr/share/X11/doc` 中的文档。安装包 `xorg-x11-doc` 以查找 PDF 和 HTML 页面。

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。这种方式可用于大多数图形卡和监视器的组合。

15.2 安装和配置字体

在 SUSE Linux Enterprise Server 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（请参见第 15.2.1 节“X11 核心字体”[182]）。要启用字体，安装目录应是 `/etc/fonts/fonts.conf` 中配置的目录的子目录（请参见第 15.2.2 节“Xft”[183]），或用 `/etc/fonts/suse-font-dirs.conf` 包含到此文件中。

以下是 `/etc/fonts/fonts.conf` 中的摘录。该文件是标准的配置文件，应适合大多数配置。它还定义包含的目录 `/etc/fonts/conf.d`。在此目录中，

以两位数字开头的文件或符号链接均由 `fontconfig` 装载。有关此功能的更详细描述，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>
```

`/etc/fonts/suse-font-dirs.conf` 会自动生成，以引入应用程序（多为第三程序，如 LibreOffice、Java 或 Adobe Reader）随附的字体。以下是典型项：

```
<dir>/usr/lib/Adobe/Reader9/Resource/Font</dir>
<dir>/usr/lib/Adobe/Reader9/Resource/Font/PPM</dir>
```

要在整个系统安装其他字体，请手动将字体文件复制到适当的目录（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，请参见其手册页 (`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* 和 *fontconfig* 系统。下面几节简要介绍这两种系统。

15.2.1 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消除锯齿处理和子像素显示的情况下支持可缩放字体，并且对许多语言而言，装载具有

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>。要删除不需要的路径，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 服务器的外壳启动 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 Server 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 Server 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-*）。

15.2.2 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（包括消除锯齿）。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 Server 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 控制。应向 /etc/fonts/local.conf 和用户特定的配置文件 ~/.fonts.conf 添加特殊配置。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>
```

来禁用所有字体的消除锯齿处理，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>
```

来禁用特定字体的消除锯齿处理。

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。要找出可用的可缩放字体 (`: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：

```
Lucida Sans:style=Demibold:weight=200
DejaVu Sans:style=Bold Oblique:weight=200
Lucida Sans Typewriter:style=Bold:weight=200
DejaVu Sans:style=Oblique:weight=80
Lucida Sans Typewriter:style=Regular:weight=80
```

```
DejaVu Sans:style=Book:weight=80
DejaVu Sans:style=Bold:weight=200
Lucida Sans:style=Regular:weight=80
```

可以使用 `fc-list` 查询的重要参数包括：

表 15.2 *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。
file	包含字体的文件的名称。
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。

参数	含义和可能值
<code>pixelsize</code>	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。

15.3 更多信息

安装包 `xorg-x11-doc` 和 `howtoenh` 以更深入地了解 X11。有关 X11 开发的更多信息，请参见该项目的主页：<http://www.x.org>。

手册页中详细描述了包 `xorg-x11-driver-video` 随附的多个驱动程序。例如，如果使用 `nv` 驱动程序，在 `man 4 nv` 中可以找到有关此驱动程序的更多信息。

有关第三方驱动程序的信息位于 `/usr/share/doc/packages/<package_name>` 中。例如，`x11-video-nvidiaG01` 的文档在安装包之后位于 `/usr/share/doc/packages/x11-video-nvidiaG01` 中。

使用 FUSE 访问文件系统

FUSE 是用户空间中的文件系统 (*file system in userspace*) 的缩写。这表示您可以将文件系统作为非特权用户配置和装入。通常，此任务需要您是根用户。FUSE 自身是一个内核模块。它与插件组合，允许您扩展 FUSE 以访问几乎所有文件系统，如远程 SSH 连接、ISO 映像等。

16.1 配置 FUSE

可以使用 FUSE 之前，必须安装包 `fuse`。根据要使用的文件系统，您需要作为独立包提供的附加插件。FUSE 插件未随 SUSE Linux Enterprise 提供。

一般您不必配置 FUSE，只需使用即可。但是建议创建一个合并所有安装点的目录。例如，可以创建目录 `~/mounts` 并在该处插入不同文件系统的子目录。

16.2 可用 FUSE 插件

FUSE 依赖于插件。下表列出常用插件。FUSE 插件未随 SUSE Linux Enterprise 提供。

表 16.1 可用 FUSE 插件

<code>fuseiso</code>	使用 CD-ROM 映像中的 ISO9660 文件系统装入映像
----------------------	---------------------------------

ntfs-3g	装入 NTFS 卷（有读写支持）
sshfs	基于 SSH 文件传输协议的文件系统客户端
wdfs	装入 WebDAV 文件系统

16.3 更多信息

有关更多信息，请参见 FUSE 主页 <http://fuse.sourceforge.net>。

部分 III. 移动计算机

Linux 中的移动计算

移动计算主要与便携式计算机、PDA 和手提电话（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。

17.1 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。这是因为必须考虑可交换性、空间要求和能耗等条件。移动硬件的制造商已开发了标准接口，如可用于扩展便携式计算机硬件的 PCMCIA（个人计算机内存卡国际协会）、迷你 PCI 和迷你 PCIe。此标准涉及内存卡、网络接口卡、ISDN 卡（和调制解调器卡）以及外部硬盘。

提示：SUSE Linux Enterprise Server 和 Tablet PC

SUSE Linux Enterprise Server 也支持 Tablet PC。Tablet PC 附带触摸板/数字转换器，使您可以使用数字笔甚至指尖代替鼠标和键盘直接在屏幕上编辑数据。它们的安装和配置与其他任何系统类似。有关 Tablet PC 安装和配置的介绍，请参见第 20 章 *使用 Tablet PC* [227]。

17.1.1 省电

由于在制造便携式计算机时加入了能量优化系统组件，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 Server 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：

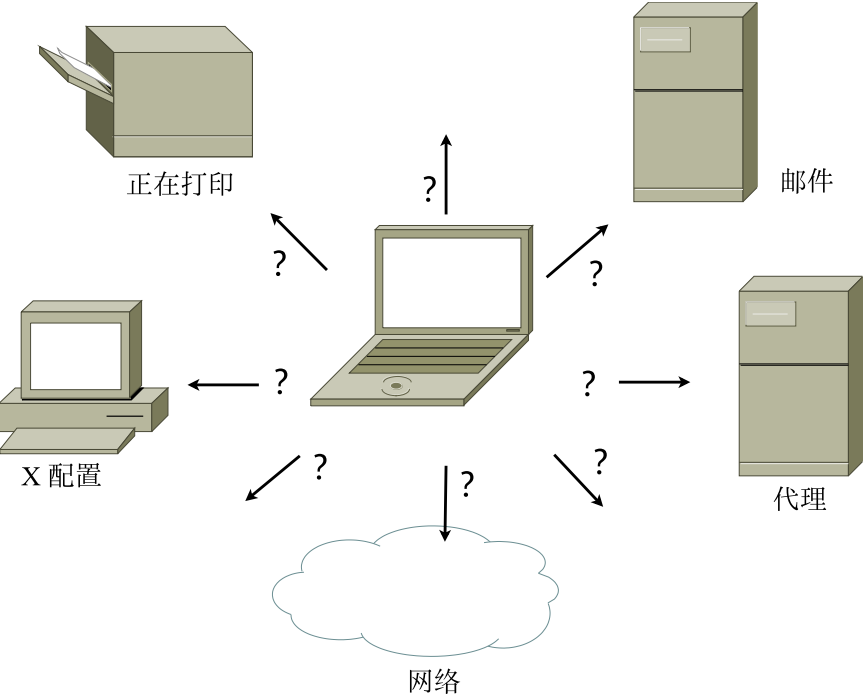
- 节制 CPU 流速。
- 在暂停期间关闭显示器。
- 手动调节显示器亮度。
- 断开不使用的支持热插拔的附件（USB CD-ROM、外部鼠标、不使用的 PCMCIA 卡、WLAN 等）。
- 在硬盘闲置时降低其转速。

有关 SUSE Linux Enterprise Server 电源管理的详细背景信息，可参见第 19 章 *电源管理* [219]。

17.1.2 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。很多服务都依赖于环境，而且必须重配置底层客户端。SUSE Linux Enterprise Server 会为您处理该任务。

图 17.1 在现有环境中集成移动计算机



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、名称解析、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（图形环境）

如果您的便携式计算机暂时连接到投影仪或外部监视器，则需要有其他显示配置。

SUSE Linux Enterprise Server 提供几种方法可将便携式计算机集成到现有的操作环境中：

NetworkManager

是为便携式计算机上的移动联网特别设计的。它让您能够轻松地在网络环境之间或不同网络类型之间进行自动切换，例如，移动宽带（如 GPRS、EDGE 或 3G）、无线 LAN 和以太网。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，请参见第 26.4 节“使用 KNetworkManager”[353] 和第 26.5 节“使用 GNOME NetworkManager 小程序”[357]。

表 17.1 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。

提示：DNS 配置和各种类型的网络连接

如果您经常携带便携式计算机出行并需要更改不同类型的网络连接，那么 NetworkManager 将是您的好助手，只要所有 DNS 地址均已使用 DHCP 正确指派。如果一些连接使用静态 DNS 地址，请将其添加到 /etc/sysconfig/network/config 中的 NETCONFIG_DNS_STATIC_SERVERS 选项。

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端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 还可用于安装系统，从而最大限度地减少搜索合适安装源的工作量。有关 SLP 的更多详细信息，请参见第 22 章 *网络中的 SLP 服务* [297]。

17.1.3 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。以下各节描述了 SUSE Linux Enterprise Server 为各项任务提供的最为重要的应用程序。

17.1.3.1 系统监视

SUSE Linux Enterprise Server 提供了两种 KDE 系统监视工具：

电源管理

*电源管理*是一个允许您调整 KDE 桌面的节能行为的应用程序。一般来说，您可以通过*电池监视器*托盘图标访问电源管理，该图标根据当前的电源类型而变化。打开电源管理配置对话框的另一种方式是通过 *Kickoff 应用程序启动器*：应用程序 > 配置桌面 > 高级 > 电源管理。

单击*电池监视器*托盘图标访问配置节能行为的选项。可以从显示的五个电源配置文件中选择一个最适合您需要的配置文件。例如，*演示文稿模式*通常将禁用屏幕保护程序和电源管理，从而使您的演示不会被系统事件中断。单击*更多...*打开更加复杂的配置屏幕。在此可以编辑各个配置文件和设置高级电源管理选项及通知，比如，便携式计算机盖闭合或电池电量不足时应执行的操作。

系统监视程序

系统监视器（也称为 *KSysguard*）将可测量的系统参数收集到一个监视环境中。它默认情况下将输出信息显示在 2 个选项卡中。*进程表*提供有关当前正在运行的进程的详细信息，比如，CPU 负载、内存使用情况或进程 ID 号和 nice 值。已收集数据的显示和过滤可以进行自定义 — 要添加新类型的进程信息，左键单击进程表标题，并选择要隐藏或要添加到视图中的列。也可以监视不同数据页中的不同系统参数，或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。

在 GNOME 环境中，使用*电源管理*自选设置和*系统监视器*。

17.1.3.2 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。这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帐户储存电子邮件。必须对电子邮件客户端进行配置，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。使用邮件客户端中实施的SMTP服务器（而非系统范围的MTA Postfix 或 Sendmail）来发送邮件，从而可收到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。使用最广泛的一种实用程序是称为rsync的命令行工具。有关更多信息，请参见其手册页(`man 1 rsync`)

17.1.3.3 无线通讯

便携式计算机不仅可以通过电缆连接到家庭或办公网络，而且还可以使用无线连接访问其他计算机、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18章无线LAN[203]。

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。它还可用于连接一定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

无线系统组件。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。

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任务。

17.1.4 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。

强大的身份验证

除了通过登录名和密码的标准身份验证外，还使用生物特征身份验证。SUSE Linux Enterprise Server 支持指纹身份验证。有关细节，请参见第 7 章 *Using the Fingerprint Reader* (↑安全指南)。

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 11 章 *Encrypting Partitions and Files* (↑安全指南)中对如何使用 SUSE Linux Enterprise Server 创建加密分区进行了描述。在使用 YaST 添加用户时还可以创建加密的用户主目录。

重要：数据安全性与挂起磁盘

在发生挂起磁盘事件期间，不会卸载加密的分区。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

不管使用的方式如何，任何数据传输都应该是安全的。有关 Linux 和网络的安全问题，请参见第 1 章 *Security and Confidentiality* (↑安全指南)。有关无线局域网的安全措施，请参见第 18 章 *无线 LAN* [203]。

17.2 移动硬件

SUSE Linux Enterprise Server 支持通过防火墙 (IEEE 1394) 或 USB 自动检测移动储存设备。术语 *移动储存设备* 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。要安全卸载这些媒体的任何一项，请使用任意文件管理器的安全删除 (KDE) 或卸载卷 (GNOME) 功能。

外部硬盘（USB 和火线）

一旦系统正确识别外部硬盘，其图标即会显示在文件管理器中。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。

17.3 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第 17.1.3.3 节“无线通讯”[198] 中描述。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描述。

Evolution 和 Kontact 中已内置与 Palm, Inc. 制造的手持设备进行同步的支持功能。与设备的第一次连接可以借助向导轻松执行。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）。

17.4 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。此网站的各个部分讨论了便携式计算机、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.opensuse.org/opensuse-mobile-de/>。在该列表中，用户和开发人员讨论了有关 SUSE Linux Enterprise Server 中移动计算的各方面问题。用英文发送的邮件都有答复，但存档信息中大部分都只有德文信息。请使用 <http://lists.opensuse.org/opensuse-mobile/> 用英文发送邮件。

关于 OpenSync 的信息可以在 <http://en.opensuse.org/OpenSync> 上找到。

无线 LAN

无线 LAN（无线局域网，WLAN）是移动计算不可或缺的一部分。当今，大多数笔记本电脑都配有内置 WLAN 卡。本章介绍如何用 YaST 设置 WLAN 卡，加密传输，以及使用提示和诀窍。

18.1 WLAN 标准

WLAN 卡用 IEEE 组织提供的 802.11 标准通讯。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细节（请参见表 18.1 “各种 WLAN 标准的概述” [203]）。此外，许多公司实施了带专有或设计功能的硬件。

表 18.1 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 旧	2.4	2	已过时；目前市场上不销售采用此标准的最终设备
802.11a	5	54	不易受干扰
802.11b	2.4	11	较少使用

名称	频带 (GHz)	最大传送速率 (MBit/s)	记事
802.11g	2.4	54	广泛采用，向后兼容 11b
802.11n	2.4 和/或 5	300	常用
802.11ad	2.4/5/60	最多 7000	2012 年发布，当前较少使用

SUSE® Linux Enterprise Server 不支持 802.11 旧卡。使用 802.11a、802.11b、802.11g 和 802.11n 的大多数卡受支持。新卡通常符合 802.11n 标准，但是使用 802.11g 的卡仍然可用。

18.2 操作方式

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。很难选择正确的身份验证方法。各种可用加密方法有各自的优点和缺陷。

无线网络基本上可以分为三种网络模式：

通过访问点的受管模式（基础结构模式）

受管网络具有一个管理元素，即访问点。在这种模式（也称为基础结构模式）中，网络中的 WLAN 站的全部连接都通过访问点运行，访问点也充当以太网的连接点。为了确保只有经过授权的工作站才能连接，使用了多种身份验证机制（WPA 等）。

专用模式（对等网络）

特殊网络没有访问点。各站之间直接通讯，因此专用网络通常比受管网络速度更快。但是，在专用网络中，传送范围和参与工作站的数目都受到很大限制。它们也不支持 WPA 身份验证。如果打算使用 WPA 安全性，不应使用专用模式。

主模式

在主模式中您的网卡用作访问点。它只在您的 WLAN 卡支持此模式时起作用。<http://linux-wless.passsys.nl> 上有您的 WLAN 卡的细节。

18.3 身份验证

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身份验证和加密方法。IEEE 802.11 标准最初的版本在术语 WEP（有线等效隐私）下对这些方法进行了描述。但是，WEP 经证明是不安全的（请参见第 18.6.3 节“安全性”[215]），因此 WLAN 行业（组织名为 *Wi-Fi 联盟*）制订了一个名为 WPA 的扩展，用以弥补 WEP 的缺陷。后来的 IEEE 802.11i 标准包含了 WPA 和一些其他的身份验证及加密方法。IEEE 802.11i 也称为 WPA2，因为 WPA 基于 802.11i 的草稿版本。

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身份验证机制：

无（开放）

开放系统是不要求身份验证的系统。任何工作站都可以加入网络。不过，可以使用 WEP 加密；请参见第 18.4 节“加密”[206]。

共享密钥（按照 IEEE 802.11）

在此过程中，使用 WEP 密钥进行身份验证。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。在身份验证过程中，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 密钥来进行身份验证和加密，因此不能提高网络的安全性。具有正确 WEP 密钥的工作站可以进行身份验证、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身份验证都不能进行通讯。

WPA-PSK（或称为 WPA-Personal，根据 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（或称为 WPA-Enterprise，根据 IEEE 802.1x）

实际上，WPA-EAP（扩展身份验证协议）不是一个身份验证系统，而是一个传输身份验证信息的协议。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 服务器来验证用户。EAP 提供三种不同的方法用于连接和鉴定服务器：

- 传输层安全 (EAP-TLS): TLS 身份验证依赖于服务器和客户端的证书互换。首先, 服务器为客户端 (客户端会评估服务器) 提供其证书。如果证书被认为有效, 则接下来客户端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。
- 隧道传输层安全 (EAP-TTSL)
- 受保护的可扩展身份验证协议 (EAP-PEAP): TTLS 和 PEAP 都是两阶段协议。在第一个阶段, 将建立安全连接, 在第二个阶段, 将交换客户端身份验证数据。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。

18.4 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。

某些供应商实施了非标准的“动态 WEP”。它与 WEP 的工作完全相同, 也具有相同弱点, 不同之处在于密钥管理设备会定期更改密钥。

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 对密钥管理进行了描述。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。

18.5 用 YaST 配置

重要：无线网络中的安全风险

如果未加密 WLAN 连接，则第三方便可以截获所有网络数据。务必使用某种受支持的身份验证和加密方法保护您的网络通讯。

使用您的硬件允许的最佳的可行加密方法。但是，要使用某种加密方法，网络中的所有设备都必须支持这种方法，否则它们无法相互通讯。例如，如果路由器支持 WEP 和 WPA，但 WLAN 卡的驱动程序仅支持 WEP，则 WEP 是您可以使用的加密方法。即便使用 WEP 进行弱加密，也比根本不加密要好。相关信息请参考第 18.4 节“加密”[206] 和第 18.6.3 节“安全性”[215]。

要用 YaST 配置无线 LAN，需要定义以下参数：

IP 地址

使用静态 IP 地址或让 DHCP 服务器动态将 IP 地址指派给接口。

操作方式

定义如何将计算机集成到 WLAN，具体取决于网络拓扑。有关的背景信息，请参见第 18.2 节“操作方式”[204]。

网络名称 (ESSID)

标识网络的唯一字符串。

身份验证和加密细节

根据网络使用的身份验证和加密方法，需要输入一个或多个密钥和/或证书。

有多个输入选项可用于输入对应的密钥：*通行密码*、*ASCII*（仅适用于 WEP 身份验证方法）和*十六进制*。

18.5.1 停用 NetworkManager

安装过程中常常会检测到 WLAN 卡。如果计算机是移动计算机，默认情况下 NetworkManager 通常处于激活状态。如果要用 YaST 配置 WLAN 卡，需要先停用 NetworkManager：

1 以用户 root 启动 YaST。

- 2 在 YaST Control Center 中，选择**网络设备 > 网络设置**打开网络设置对话框。

如果网络当前正由 NetworkManager 控制，您会看到一条警告消息：YaST 无法编辑网络设置。

- 3 要通过 YaST 启用编辑功能，单击**确定**消除这条消息，然后在全局选项选项卡上激活**通过 ifup 的传统方法**。
- 4 如需进一步配置，请继续第 18.5.2 节“访问点配置”[208] 或第 18.5.3 节“建立专用网络”[212] 中的操作。

否则，单击**确定**确认您的更改，以写入网络配置。

18.5.2 访问点配置

在此部分，可了解如何配置能连接到（外部）访问点的 WLAN 卡，或如何在 WLAN 卡支持的情况下使用 WLAN 卡作为访问点。有关无访问点的网络配置，请参见第 18.5.3 节“建立专用网络”[212]。

过程 18.1 配置 WLAN 卡以使用访问点

- 1 启动 YaST，打开**网络设置**对话框。
- 2 切换到**概述**选项卡，其中列出了系统检测到的所有网卡。如果您需要常规网络配置的更多信息，请参见第 21.4 节“使用 YaST 配置网络连接”[254]。
- 3 从列表中选择无线网卡并单击**编辑**以打开“网卡设置”对话框。
- 4 在**地址**选项卡上，配置是对计算机使用动态还是静态 IP 地址。一般 *DHCP* 最好使用**动态地址**。
- 5 单击**下一步**继续到**无线网卡配置**对话框。
- 6 要使用 WLAN 卡连接到访问点，请将**操作方式**设置为**受管**。

但是如果使用 WLAN 卡作为访问点，请将**操作方式**设置为**主管**。请注意，并非所有 WLAN 卡都支持这种方式。

注意：使用 WPA-PSK 或 WPA-EAP

如果要使用 WPA-PSK 或 WPA-EAP 身份验证模式，操作方式必须设置为受管。

- 7 要连接到某个网络，请输入网络名称 (ESSID)。也可以单击扫描网络，并从可用无线网络列表中选择网络。

为实现相互通讯，无线网络中的所有工作站都需要相同的 ESSIDu163。如果未指定任何 ESSID，则 WLAN 卡会自动与具有最佳信号强度的访问点关联。

注意：WPA 身份验证需要 ESSID

如果选择 WPA 身份验证，必须设置网络名称 (ESSID)。

- 8 为您的网络选择身份验证方式。哪个方式适合，取决于 WLAN 卡的驱动程序和网络中其他设备的能力。
- 9 如果选择将身份验证方式设置为不加密，请单击下一步完成配置。确认有关可能存在的安全风险的消息，单击确定关闭概述选项卡（显示新配置的 WLAN 卡）。

如果选择任何其他身份验证方式，则继续过程 18.2, “输入加密细节” [210] 中的操作。

图 18.1 YaST: 配置无线网卡

无线网卡配置

在此可设置用于无线联网的 最重要的设置。操作方式取决于网络拓扑结构。操作方式 可以是 专用 (对等网络, 没有访问点)、 受管 (由访问点管理的网... [更多](#)

无线设备设置

操作方式 (P) :

爱普

网络名称 (ESSID) (I) :

扫描网络

身份验证方式 (A) :

WEP - 开放式

密钥输入类型

☒ 密码短语 (P) ☐ ASCII (A) ☐ 十六进制 (H)

加密键 (K) :

专家设置 (E) WEP 密钥 (W)

帮助

中止 (C)

后退 (B)

下一步 (N)

过程 18.2 输入加密细节

以下身份验证方法需要加密密钥：*WEP - 打开*、*WEP - 共享密钥*和 *WPA-PSK*

对于 WEP，通常只需要一个密钥，但是最多可以为工作站定义 4 个不同的 WEP 密钥。需要将其中一个密钥设置为默认密钥，并用于加密。其他密钥用于解密。默认情况下，使用 128 位的密钥长度，但也可以选择将长度设置为 64 位。

为了更加安全，WPA-EAP 使用 RADIUS 服务器验证用户身份。在服务器上进行身份验证有三种不同的方法：TLS、TTLS 和 PEAP。WPA-EAP 所需的身份凭证和证书取决于对 RADIUS 服务器使用的身份验证方法。请向系统管理员索取所需的信息和身份凭证。YaST 在 `/etc/cert` 下搜索任何证书。因此，请将为您提供的证书保存在这个位置，并将对这些文件的访问限制为 0600（所有者读写权限）。

1 要为 *WEP* — 打开或 *WEP* — 共享密钥输入密钥：

1a 将密钥输入类型设置为通行密码、ASCII 或十六进制。

1b 输入对应的加密密钥（一般只使用一个密钥）：

如果选择了通行密码，请输入从中按照指定密钥长度（默认 128 位）生成密钥的短语或字符串。

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。

1c 要将密钥长度调整为较少的位数（可能旧硬件需要这样做），请单击 *WEP 密钥* 并将 *密钥长度* 设置为 64 位。*WEP 密钥* 对话框还会显示目前为止已输入的 WEP 密钥。除非明确将另一个密钥设置为默认密钥，否则 YaST 始终使用第一个密钥作为默认密钥。

1d 要为 WEP 输入更多的密钥，或要修改某个密钥，请选择对应项并单击 *编辑*。选择 *密钥输入类型* 并输入密钥。

1e 单击 *确定* 确认更改。

2 为 *WPA-PSK* 输入密钥：

2a 选择输入方法 *通行密码* 或 *十六进制*。

2b 输入相应的 *加密密钥*。

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。

3 如果选择了 *WPA-EAP* 身份验证，请单击下一步切换到 *WPA-EAP* 对话框，在那里输入网络管理员给您的身份凭证和证书。

3a 选择 RADIUS 服务器用于验证身份的 *EAP* 方式。接下来需要输入的细节取决于所选的 *EAP* 方式。

3b 对于 TLS，提供身份、*客户端证书*、*客户端密钥* 和 *客户端密钥密码*。为了增强安全性，还可以配置用于验证服务器的身份的 *服务器证书*。

TTLS 和 PEAP 都需要身份和密码，而 *服务器证书* 和 *匿名身份* 是可选的。

3c 要进入 WPA-EAP 设置的高级身份验证对话框，请单击 *细节*。

3d 选择 EAP-TTLS 或 EAP-PEAP 通讯第二阶段的身份验证方法（内部身份验证）。方法的选择取决于您在上一个对话框中为 RADIUS 服务器选择的身份验证方法。

3e 如果自动确定设置不起作用，请选择特定的 *PEAP* 版本以强制使用某个 PEAP 实施。

4 单击 *确定* 确认更改。概述选项卡显示新配置的 WLAN 卡的细节。

5 单击 *确定* 完成配置并离开该对话框。

18.5.3 建立专用网络

在某些情况下连接两台装有 WLAN 卡的计算机很有用。要用 YaST 建立专用网络，请执行以下操作：

1 启动 YaST 并打开网络设置对话框。

2 切换到概述选项卡，从列表中选择无线网卡，然后单击 *编辑* 打开网卡设置对话框。

3 选择静态指派 IP 地址，输入以下数据：

- *IP 地址*：192.168.1.1。将第二台计算机上的该地址改为 192.168.1.2（举例）。
- *子网掩码*：/24
- *主机名*：选择您喜欢的任何名称。

4 按下一步继续。

5 将操作方式设置为专用。

6 选择网络名称 (*ESSID*)。它可以是任何名称，但必须用于专用网络的每台计算机。

- 7 为您的网络选择身份验证方式。哪个方式适合，取决于 WLAN 卡的驱动程序和网络中其他设备的能力。
- 8 如果选择将身份验证方式设置为不加密，请单击下一步完成配置。确认有关可能存在的安全风险的消息，单击确定关闭显示新配置的 WLAN 卡的概述选项卡。

如果选择任何其他身份验证方式，则继续过程 18.2, “输入加密细节” [210] 中的操作。
- 9 如果没有安装 `smpppd`，YaST 会要求您安装。
- 10 使用相同的网络名称 (*ESSID*)、相同的身份验证方式和不同的 IP 地址，相应地配置网络中的其他 WLAN 卡。

18.5.4 设置其他配置参数

配置 WLAN 卡时，一般不需要更改预配置的设置。但是，如果需要详细地配置 WLAN 连接，YaST 允许您调整以下设置：

通道

指定应运行 WLAN 站的通道。只有在专用和主管模式下才需要此设置。在受控方式下，网卡将自动搜索访问点的可用通道。

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。

电源管理

当您在旅途中时，使用节能技术有助于最大限度地提高电池的运行时间。有关电源管理的详细信息，请参考第 19 章 *电源管理* [219]。使用电源管理可能影响连接质量并增加网络延迟。

访问高级选项：

- 1 启动 YaST 并打开网络设置对话框。
- 2 切换到概述选项卡，从列表中选择无线网卡，单击编辑打开网卡设置对话框。
- 3 单击下一步继续到无线网卡配置对话框。
- 4 单击专家设置。
- 5 在专用方式下，可以选择提供的一个通道（11 到 14，具体取决于您所在国家/地区），用于在您的工作站和其他工作站之间进行通信。在主管方式下，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。
- 6 选择要使用的位率。
- 7 输入要连接到的访问点的 MAC 地址。
- 8 选择是否使用电源管理。
- 9 单击确定确认您的更改，单击下一步，再单击确定完成配置。

18.6 建立 WLAN 的提示和技巧

以下工具和提示可以帮助您监视和提高 WLAN 的速度、稳定性以及安全性。

18.6.1 实用程序

包 wireless-tools 中包含可用于设置无线 LAN 特定参数和获取统计数字的实用程序。有关更多信息，请参阅http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html。

18.6.2 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。在操作中，可以在命令行（Link Quality 字段）上使用 iwconfig 实用程序检查信号强度，也可以使用 KDE 或 GNOME 提供的

NetworkManager 小程序进行检查。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。

iwspy 命令可用于显示 WLAN 统计数字：

```
iwspy wlan0
wlan0      Statistics collected:
  00:AA:BB:CC:DD:EE : Quality:0   Signal level:0   Noise level:0
  Link/Cell/AP      : Quality:60/94 Signal level:-50 dBm  Noise level:-140
  dBm (updated)
  Typical/Reference : Quality:26/94 Signal level:-60 dBm  Noise level:-90
  dBm
```

18.6.3 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。

对于私用，可使用 WPA-PSK（如果可用）。尽管 Linux 在大多数硬件组件上支持 WPA，但某些驱动程序不提供 WPA 支持。在启用 WLAN 功能的旧访问点和路由器上可能也无法使用 WPA。对于此类设备，请确认是否可以通过固件更新实现 WPA。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。

为您的身份验证方式使用强密码。例如，网页 <https://www.grc.com/passwords.htm> 能生成随机的 64 个字符的密码。

18.7 查错

如果 WLAN 卡没有响应，请检查以下先决条件是否满足：

1. 您是否知道 WLAN 卡的设备名称？通常它是 wlan0。请用工具 ifconfig 进行检查。
2. 您检查了需要的固件吗？请参见 /usr/share/doc/packages/wireless-tools/README.firmware 以获取更多信息。

3. 路由器的 ESSID 是否已广播并可见（未隐藏）？

18.7.1 检查网络状态

用命令 `iwconfig` 可得到您的无线连接的重要信息。例如，以下行会显示 ESSID、无线模式、频率、信号是否加密、链接质量等等：

```
iwconfig wlan0
wlan0 IEEE 802.11abg ESSID:"guest"
      Mode:Managed  Frequency:5.22GHz  Access Point: 00:11:22:33:44:55
      Bit Rate:54 Mb/s   Tx-Power=13 dBm
      Retry min limit:7   RTS thr:off   Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality:62/92   Signal level:-48 dBm  Noise level:-127 dBm
      Rx invalid nwid:0   Rx invalid crypt:0   Rx invalid frag:0
      Tx excessive retries:10   Invalid misc:0   Missed beacon:0
```

您也可以使用 `iwlist` 命令获得上述信息。例如，以下行显示当前的比特率：

```
iwlist wlan0 rate
wlan0      unknown bit-rate information.
          Current Bit Rate=54 Mb/s
```

如果您想大致了解当前有多少访问点可用，也可以用 `iwlist` 命令实现。它会提供“cells”列表，外观如下：

```
iwlist wlan0 scanning
wlan0 Scan completed:
      Cell 01 - Address: 00:11:22:33:44:55
              Channel:40
              Frequency:5.2 GHz (Channel 40)
              Quality=67/70  Signal level=-43 dBm
              Encryption key: off
              ESSID:"Guest"
              Bit Rates: 6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s;
                        24 Mb/s; 36 Mb/s; 48 Mb/s
              Mode: Master
              Extra:tsf=0000111122223333
              Extra: Last beacon: 179ms ago
              IE: Unknown: ...
```

18.7.2 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://old-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。

18.7.3 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`。

18.8 更多信息

可在以下页面中找到更多信息：

http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Wireless.html

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。

tuxmobil.org

有关 Linux 下的移动计算机的实用信息。

<http://www.linux-on-laptops.com>

有关便携式计算机上 Linux 的更多信息。

电源管理

► **System z:** IBM System z 中不存在本章介绍的功能和硬件，因而本章介绍的内容与这些平台无关。 ◀

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。ACPI（高级配置和电源接口）在所有通用计算机（便携式计算机、台式机和服务器）上都可用。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的都符合这些要求。还可以通过控制 CPU 频率调节以达到省电或降低噪音的目的。

19.1 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。ACPI 中的主要功能和它们的用法为：

待机

不支持

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。

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 ACPI 的内核例程执行暂挂到磁盘。

电池监视

ACPI 检查电池充电状态并提供相关信息。另外，当达到临界电量状态时，它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。

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）、限制和使处理器进入休眠 (C-state)。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。

19.2 高级配置和电源接口 (ACPI)

ACPI 旨在支持操作系统设置和控制各个硬件组件。ACPI 取代即插即用电源管理 (PnP) 和高级电源管理 (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，请参见第 19.2.2 节“故障诊断” [221]。

19.2.1 控制 CPU 性能

CPU 可以采用三种节能方法：

- 频率和电压调节

- 限制时钟频率 (T-state)
- 使处理器进入休眠 (C-state)

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。

仅当处理器忙时，才需要进行频率调节和限制，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-state。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，最佳方法是由内核按需调节器控制动态频率调节。

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。

有关详细信息，请参见第 11 章 *Power Management* (↑系统分析和微调指南)。

19.2.2 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。更多情况下，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。

有时，计算机会对通过 USB 或 FireWire 挂接的硬件感到困惑。如果一台计算机拒绝引导，请拔下所有不需要的硬件，然后再次重试。

引导后，用命令 `dmesg | grep -2i acpi` 来监视系统的引导消息（或所有消息，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（区分系统描述表）可替换为改进的版本。在这种情况下，将忽略 BIOS 中有问题的 DSDT。第 19.4 节“查错”[224]中对这一过程进行了介绍。

在内核配置中，可以使用开关来激活 ACPI 调试消息。如果编译和安装的是带有 ACPI 调试功能的内核，则会显示详细信息。

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。

19.2.2.1 更多信息

- <http://tldp.org/HOWTO/ACPI-HOWTO/>（详细的 ACPI HOWTO 文档，包含 DSDT 增补程序）
- <http://www.acpi.info>（高级配置和电源接口规范）
- <http://www.lesswatts.org/projects/acpi/>（Sourceforge 中的 ACPI4Linux 项目）
- <http://acpi.sourceforge.net/dsdt/index.php>（Bruno Ducrot 开发的 DSDT 增补程序）

19.3 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，如果要最大程度地节能，请使用 `hdparm` 命令测试以下某些方法。

它可用于修改各种磁盘设置。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 `pdflush` 守护程序监视。当数据达到一定的有效期限限制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 `pdflush` 设置为较短的时间间隔可以获得最好的数据完整性。它会每 5 秒钟检查一次缓冲区并将数据写入硬盘。以下变量很有用：

```
/proc/sys/vm/dirty_writeback_centisecs
```

包含截至 `pdflush` 线程唤醒的延迟（以百分之一秒为单位）。

```
/proc/sys/vm/dirty_expire_centisecs
```

定义最晚在什么时间范围之后应写出未写入页。默认值是 3000，表示 30 秒。

```
/proc/sys/vm/dirty_background_ratio
```

`pdflush` 开始写入未写入页之前未写入页的最大百分比。默认值是 5%。

```
/proc/sys/vm/dirty_ratio1
```

当未写入页超出总内存的此百分比后，将强制进程在其时间范围内写入未写入缓冲区，而不是继续写入。

警告：对数据完整性的损害

更改为 `pdflush` 守护程序设置将损害数据完整性。

除了这些进程之外，`Btrfs`、`Ext3`、`Ext4` 等日记文件系统会独立于 `pdflush` 写入它们的元数据，这也会妨碍硬盘降速。

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。

19.4 查错

文件 `/var/log/messages` 中记录了所有错误消息和警报。以下几个部分介绍最常见的问题。

19.4.1 硬件支持已激活 ACPI，但功能不工作

如果遇到 ACPI 问题，请在 `dmesg` 输出中使用 `dmesg|grep -i acpi` 命令搜索 ACPI 特定的消息。

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。

过程 19.1 在 BIOS 中更新 DSDT 表

对于以下过程，请确保安装以下包：`kernel-source`、`pmtools` 以及 `mkinitrd`。

- 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 计算机语言），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 如果已下载表的文件扩展名是 `.asl`（ACPI 源语言），请执行以下命令编译扩展名：

```
iasl -sa file.asl
```

- 3 将（生成的）文件 `DSDT.asl` 复制到任意位置（建议复制到 `/etc/DSDT.asl`）。
- 4 编辑 `/etc/sysconfig/kernel` 并相应地调整指向 `DSDT` 文件的路径。
- 5 启动 `mkinitrd`。一旦安装了内核并使用 `mkinitrd` 创建了 `initrd` 文件，引导系统时就会集成并装载修改过的 `DSDT`。

19.4.2 CPU 频率不工作

请参见内核源以确认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。如果安装了 `kernel-source` 包，则在 `/usr/src/linux/Documentation/cpu-freq/*` 中可找到此信息。

19.4.3 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。

当系统尝试卸载有问题的模块时，会停止系统或不触发暂挂事件。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。日志文件 `/var/log/pm-suspend.log` 包含关于所发生的情况以及哪里可能有错误的详细信息。修改 `/usr/lib/pm-utils/defaults` 中的 `SUSPEND_MODULES` 变量以在暂挂或待机之前卸载有问题的模块。

19.5 更多信息

- http://en.opensuse.org/SDB:Suspend_to_RAM — 如何使“暂挂到RAM”工作
- <http://old-en.opensuse.org/Pm-utils> — 如何修改常规暂挂框架

使用 Tablet PC

SUSE® Linux Enterprise Server 自带对 Tablet PC 的支持。从下面可了解如何安装和配置 Tablet PC 并发现接受数字笔输入的一些有用的 Linux* 应用程序。

支持以下 Tablet PC:

- 具有串行和 USB Wacom 写字板（基于手写笔）、触摸屏或多点触摸设备的 Tablet PC。
- 具有 FinePoint 设备的 Tablet PC，例如 Gateway C210X/M280E/CX2724 或 HP Compaq TC1000。
- 具有触摸屏设备的 Tablet PC，例如 Asus R2H、Clevo TN120R、Fujitsu Siemens Computers P-Series、LG C1、Samsung Q1/Q1-Ultra。

安装 Tablet PC 包并正确配置数字手写笔之后，即可将手写笔（也称手写输入笔）用于以下操作及应用程序的输入：

- 登录到 KDM 或 GDM
- 在 KDE 和 GNOME 桌面上解除屏幕锁定
- 也可以由其他定点设备（如鼠标或触摸板）触发的操作，例如，在屏幕上移动光标、启动应用程序、关闭窗口、调整窗口大小、移动窗口、移动窗口焦点及拖放对象
- 在 X Window System 中使用手势识别
- 用 GIMP 绘图

- 用如 Jarnal 或 Xournal 之类的应用程序记录或绘制或者用 Dasher 编辑大量文本。

20.1 安装 Tablet PC 包

Tablet PC 所需的包包含在 TabletPC 安装模式中 — 如果已在安装期间选择，应已在系统上安装以下包：

- `cellwriter`：基于字符的手写输入板
- `jarnal`：基于 Java 的记录应用程序
- `xournal`：用于记录和绘制的应用程序
- `xstroke`：X Window System 的手势识别程序
- `xvkbd`：X Window System 的虚拟键盘
- `x11-input-fujitsu`：Fujitsu P 系列 手写板的 X 输入模块
- `x11-input-evtouch`：一些具有触摸屏的 Tablet PC 的 X 输入模块
- `xorg-x11-driver-input`：用于输入设备的 X 输入模块，包括用于 Wacom 设备的模块。

如果未安装这些包，请通过命令行手动安装所需包，或在 YaST 中对安装选择 TabletPC 模式。

20.2 配置手写板设备

安装期间，会默认配置写字板或触摸设备。如果存在 Wacom 设备配置问题，可在命令行使用 `xsetwacom` 更改设置。

20.3 使用虚拟键盘

要登录 KDE 或 GNOME 桌面或解除屏幕锁定，您可以照常输入用户名和密码或通过登录字段下方显示的虚拟键盘 (xvkbd) 输入。要配置键盘或访问集成帮助，请单击左下角的 `xvkbd` 字段打开 `xvkbd` 主菜单。

如果输入不可见（或未传输到所需的窗口），请通过单击 `xvkbd` 中的焦点然后单击应获取键盘事件的窗口而重定向焦点。

图 20.1 xvkbd 虚拟键盘



如果想在登录后使用 `xvkbd`，请从主菜单将其启动或从外壳输入 `xvkbd`。

20.4 旋转显示器

使用 `KRandRTray` (KDE) 或 `gnome-display-properties` (GNOME) 直接手动旋转显示内容或调节显示内容大小。`KRandRTray` 和 `gnome-display-properties` 都是针对 X 服务器的 RANDR 扩展的小程序。

从主菜单启动 `KRandRTray` 或 `gnome-display-properties`，或者输入 `krandrtray` 或 `gnome-display-properties` 从壳层启动这个小程序。启动小程序之后，

小程序图标通常将添加到系统托盘。如果 `gnome-display-properties` 图标在系统盘中未自动显示，请务必在监视器分辨率设置对话框中激活在面板中显示显示器。

要使用 `KRandRTray` 旋转显示器，请右键单击图标并选择配置显示器。从配置对话框选择所需方向。

要使用 `gnome-display-properties` 旋转显示器，请右键单击图标并选择所需方向。显示器将立即倾斜到新的方向。同时，图形手写板的方向也发生改变，因此它仍然可以正确解释手写笔的活动。

如果更改桌面方向时遇到问题，请参见第 20.7 节“查错”[234] 以获取更多信息。

20.5 使用手势识别

SUSE Linux Enterprise Server 同时包含 `CellWriter` 和 `xstroke` 以识别手势。两个应用程序都接受使用笔或其他指向设备执行的手势作为 X Window 系统上应用程序的输入。

20.5.1 使用 `CellWriter`

通过 `CellWriter`，您可以将字符写入单元格网格中，写的内容会便于按字符识别。写完之后，您可以将输入发送到当前有焦点的应用程序。可以使用 `CellWriter` 识别手势之前，需要培训应用程序使其识别您的手写内容。您需要培训某个键映射的每个字符（未培训的字符不会激活，从而不能使用）。

过程 20.1 培训 `CellWriter`

- 1 从主菜单中或从命令行使用 `cellwriter` 启动 `CellWriter`。在第一次启动时，`CellWriter` 会自动以培训模式启动。在培训模式中，它会显示当前所选键映射的一组字符。
- 2 将要用于一个字符的手势输入相应字符的单元格。第一次输入时，背景色更改为白色，而字符本身会以浅灰色显示。重复该手势多次，直到该字符颜色更改为黑色。未培训的字符会在浅灰色或棕色背景中显示（因桌面颜色模式而异）。
- 3 重复此步骤，直到为 `CellWriter` 培训了所需的所有字符。

- 4 如果要培训 CellWriter 输入另一种语言，请单击 **设置**按钮并从 **语言**选项卡选择语言。关闭配置对话框。单击 **培训**按钮并从 *CellWriter* 窗口右下角的下拉框中选择键映射。现在为新的键映射重复培训。
- 5 完成键映射的培训之后，单击 **培训**按钮切换到普通模式。

在普通模式中，CellWriter窗口显示可用于输入手势的两个空单元格。单击 **Enter** 按钮后这些字符才会发送到另一个应用程序，因此可以在将字符用作输入之前更正或删除它们。已识别为低可信度的字符将高亮显示。要更正输入，请使用在右键单击单元格显示的上下文菜单。要删除字符，请使用笔的橡皮或按鼠标中键清除单元格。在 CellWriter 中完成输入之后，通过单击应用程序的窗口定义哪个应用程序应收到输入。然后通过单击 **Enter** 将输入发送到该应用程序。

图 20.2 使用 CellWriter 识别手势



如果在 CellWriter 中单击 **键**按钮，将会得到一个虚拟键盘，可以使用其代替手写识别。

要隐藏 CellWriter，请关闭 CellWriter 窗口。现在该应用程序显示为系统盘中的图标。要再次显示输入窗口，请单击系统盘中的图标。

20.5.2 使用 Xstroke

使用 xstroke，在 X Window 系统中，可以将手势用于手写笔或其他定点设备，以此作为应用程序输入。xstroke 字母表是类似于 Graffiti* 字母表的 unistroke 字母表。一旦将其激活，它会将输入发送至当前聚焦的窗口中。

- 1 从主菜单启动 xstroke，或从外壳输入 xstroke。这将在您的系统盘中添加铅笔图标。
- 2 启动要使用手写笔创建文本输入的应用程序（例如，终端窗口、文本编辑器或 LibreOffice Writer）。

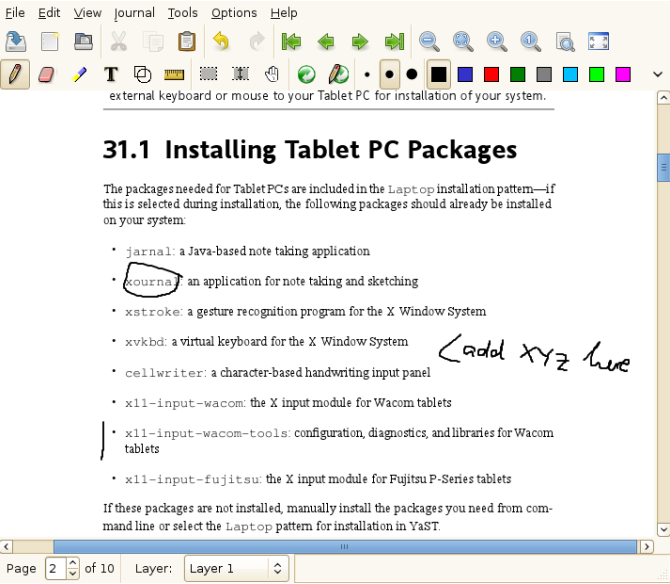
- 3 要激活手势识别方式，请单击一次铅笔图标。
- 4 用手写笔或其他定点设备在图形手写板上执行手势。`xstroke` 截获手势并将它们传送到聚焦的应用程序窗口中显示的文本中。
- 5 要在不同窗口中切换聚焦，请用手写笔单击所需窗口并在按住鼠标一会儿（或使用桌面控制中心定义的键盘快捷方式）。
- 6 要停用手势识别方式，请再次单击铅笔图标。

20.6 用手写笔记录和绘制

要用手写笔创建绘图，可以使用如 GIMP 之类的专业图形编辑器或者尝试使用记事应用程序（Xournal 或 Jarnal）。借助 Xournal 和 Jarnal，您可以用手写笔记事、创建绘图或为 PDF 文件添加注释。作为一个适用于多个平台的基于 Java 的应用程序，Jarnal 也提供基本协作功能。有关详细信息，请参见 <http://www.dklevine.com/general/software/tcl000/jarnal-net.htm>。保存内容时，Jarnal 以存档格式 (*.jaj) 储存数据，这其中也包含 SVG 格式的文件。

从主菜单启动 Jarnal 或 Xournal 或者从外壳输入 Jarnal 或 Xournal。例如，要给 Xournal 中的 PDF 文件添加注释，请选择文件 > 注解 *PDF* 然后在文件系统中打开 PDF 文件。使用手写笔或其他指针设备注解 PDF，然后通过文件 > 导出到 *PDF* 来保存更改。

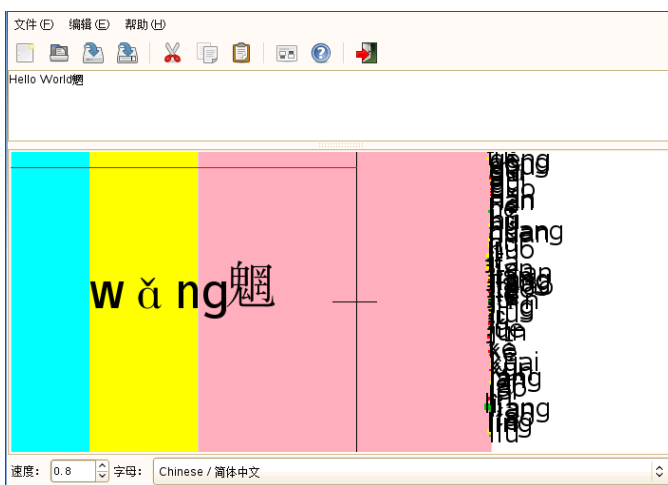
图 20.3 用 Xournal 注解 PDF



Dasher 是另一个有用的应用程序。它适用于键盘输入不实际或不可用的情况。只需稍加练习，您就可以只需使用手写笔（或其他输入设备——甚至装备了眼球跟踪器）即能熟练输入大量文本。

从主菜单启动 Dasher 或从外壳输入 dasher。沿一个方向移动手写笔，应用程序将开始放大到右侧的字母区。从穿过中间十字准线的字母开始，创建或预测文本，且将文本打印到窗口的上方。要停止或开始写入，请用手写笔单击一下显示器。在窗口底部修改缩放速度。

图 20.4 用 Dasher 编辑文本



Dasher 概念适用于多种语言。有关更多信息，请参考 Dasher 网站，其中提供了完整文档、演示及培训文本。请参见 <http://www.inference.phy.cam.ac.uk/dasher/>。

20.7 查错

虚拟键盘不显示在登录屏幕上

有时，虚拟键盘不会显示在登录屏幕上。要解决此问题，请按 **Ctrl + Alt + <—** 或按 Tablet PC 上的相应键（如果使用无集成键盘的 slate 模型）重新启动 X 服务器。如果虚拟键盘仍然未显示，请将外部键盘连接到 slate 模型并使用硬件键盘登录。

Wacom 图形手写板的方向未更改

使用 `xrandr` 命令，可以在外壳中更改显示器方向。输入 `xrandr --help` 可查看可用选项。要同时更改图形手写板方向，需要按以下描述修改命令：

- 对于常规方向（0°方向）：

```
xrandr -o normal && xsetwacom --set "Serial Wacom Tablet" Rotate NONE
```

- 对于 90°旋转（顺时针，纵向）：

```
xrandr -o right && xsetwacom --set "Serial Wacom Tablet" Rotate CW
```

- 对于 180° 旋转（横向）：

```
xrandr -o inverted && xsetwacom --set "Serial Wacom Tablet" Rotate HALF
```

- 对于 270° 旋转（逆时针，纵向）：

```
xrandr -o left && xsetwacom set --"Serial Wacom Tablet" Rotate CCW
```

请注意，上面的命令随 `xsetwacom list` 命令的输出而异。将 "Serial Wacom Tablet" 替换为手写输入笔或触摸设备的输出。如果您有一个具有触摸支持的 Wacom 设备（可以在写字板上使用手指移动光标），则还需要旋转触摸设备。

20.8 更多信息

这里提到的一些应用程序不提供集成联机帮助，但是您可以在 `/usr/share/doc/package/packageName` 或以下站点找到关于您所安装系统的用法和配置的实用信息：

- 有关 Xournal 手册，请参见 <http://xournal.sourceforge.net/manual.html>
- Jarnal 文档位于 <http://jarnal.wikispaces.com/>
- 有关 xstroke 手册页，请参见 <http://davesource.com/Projects/xstroke/xstroke.txt>
- 有关配置 X 的 HOWTO，请参见 Linux Wacom 网站：http://sourceforge.net/apps/mediawiki/linuxwacom/index.php?title=Configuring_X
- 有关 Dasher 项目详细信息的网站，请参见 <http://www.inference.phy.cam.ac.uk/dasher/>
- 有关 CellWriter 的更多信息和文档，请参见 <http://risujin.org/cellwriter/>

- 有关 `gnome-display-properties` 的信息，请参见 <http://old-en.opensuse.org/GNOME/Multiscreen>

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。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。在本章中，仅描述基础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。表 21.1 “TCP/IP 系列协议中的若干协议” [239] 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。由 TCP/IP 连接而成的网络构成了全球网络，也称作“因特网”。

RFC 代表*注释请求*。RFC 由一些文档组成，用来描述各种因特网协议和操作系统及其应用程序的实施过程。RFC 文档用来描述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。这些文档可在 <http://www.ietf.org/rfc.html> 获得。

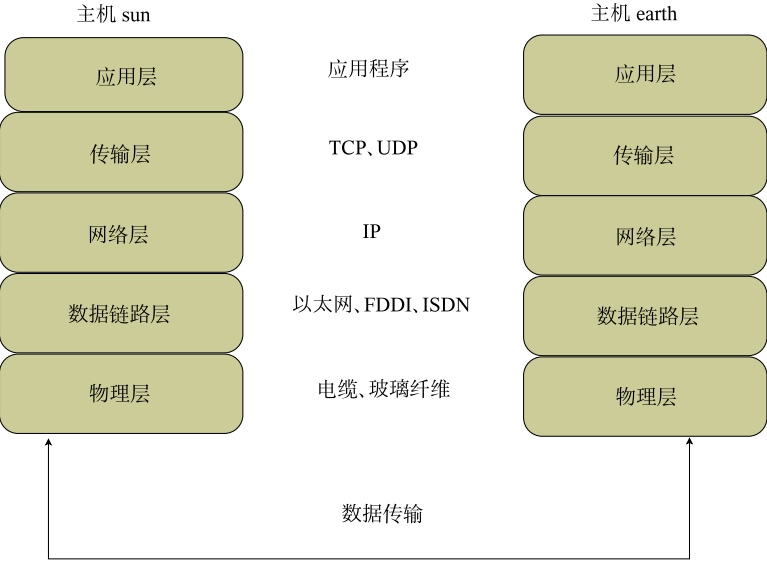
表 21.1 TCP/IP 系列协议中的若干协议

协议	描述
TCP	传送控制协议：面向连接的安全协议。要传输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 确定在传输过程中是否有任何数据丢失或发生混乱。只要涉及到数据序列就会实施 TCP。

协议	描述
UDP	用户数据报协议：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，也可能丢失数据。 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 21.1 “TCP/IP 的简化层次模型”[241] 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（例如以太网）的支持。

图 21.1 TCP/IP 的简化层次模型

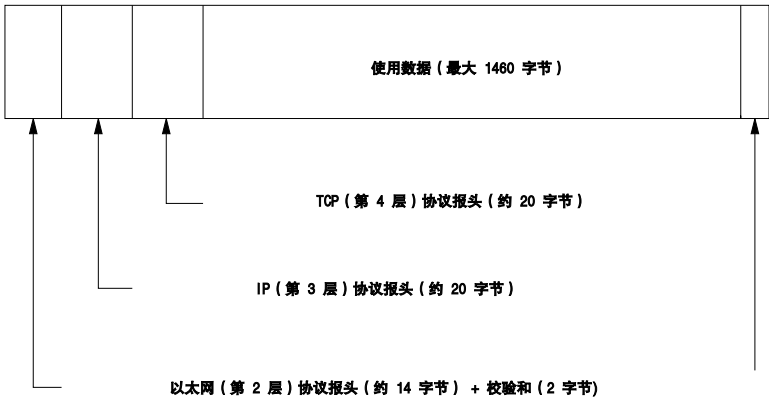


该图为每一层都提供了一到两个示例。层次按照抽象程度排序。最底层非常接近硬件。最上层则几乎就是硬件的完全抽象化。每一层都有自己的特殊功能。每一层的特殊功能多隐含在其描述中。数据链路层和物理层表示所用的物理网络（如以太网）。

几乎所有硬件协议都在面向数据包的基础上发挥作用。要传送的数据收集在包中（一次无法发送所有数据）。TCP/IP 包最大约为 64 KB。包通常要小得多，因为可能受到网络硬件的限制。以太网上的数据包最大约为 1500 字节。通过以太网发送数据时，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的数据。演示了一个通过以太网电缆传送的示例 TCP/IP 数据包。图 21.2 “TCP/IP 以太网包”[242] 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 21.2 TCP/IP 以太网包



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。正像剥洋葱皮那样，在每一层中都要从传输数据中删除协议报头。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。

21.1 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 21.2 节“IPv6 — 下一代的因特网”[245]。

21.1.1 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 21.1 “编写 IP 地址”[242] 的第二行所示的格式书写。

例 21.1 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。它在全球只能使用一次。这条规则也有例外，但这些例外与下文无关。

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。但是，此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）。

21.1.2 网络掩码和路由

网络掩码用于定义子网的地址范围。如果两台主机位于同一子网中，它们可直接相互访问。如果它们位于不同子网中，则需要用于处理此子网的所有通讯的网关地址才能相互访问。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掩码进行“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。

要了解网络掩码如何工作，可查看例 21.2“将 IP 地址链接到网络掩码”[243]。网络掩码有 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。因为网络掩码总是由多个连续的 1 位组成，所以也可仅计算网络掩码中的位数。在例 21.2“将 IP 地址链接到网络掩码”[243] 中，第一个 24 位也可写作 192.168.0.0/24。

例 21.2 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 21.2 特定地址

地址类型	描述
基本网络地址	这是网络掩码和该网络中的任意地址，如例 21.2 “将 IP 地址链接到网络掩码” [243] 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”。可以使用此地址以及通过 IPv4 定义的完整 127.0.0.0/8 回写网络中的所有地址为您自己的计算机设置一个连接。对于 IPv6，仅存在一个回写地址 (:::1)。

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 21.3 “专用 IP 地址域” [245] 中。

表 21.3 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

21.2 IPv6 — 下一代的因特网

重要：IBM System z：IPv6 支持

IBM System z 硬件的 CTC 和 IUCV 网络连接不支持 IPv6。

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 通信，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。以下各节进一步描述了 IPv6 带来的改进和优点，以及如何从旧协议过渡到新协议。

21.2.1 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 21.2.2 节“地址类型和结构”[247]。

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）。

无论路由器是否已连接到交换机，路由器都应发送带标志的定期广告，告诉网络中的主机应如何交互。有关更多信息，请参见 RFC 2462 和 `radvd.conf` (5) 手册页以及 RFC 3315。

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 21.2.3 节“IPv4 与 IPv6 并存”[251]。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）。

21.2.2 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。它们之间用冒号(:)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 21.3 “示例 IPv6 地址” [248]

例 21.3 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 21.4 “指定前缀长度的 IPv6 地址” [248] 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 21.4 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 21.4 “各种 IPv6 前缀” [248] 中。

表 21.4 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

前缀（十六进制）	定义
	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。
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 21.2.3 节“IPv4 与 IPv6 并存”[251])，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以传递到该主机，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。

21.2.3 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 21.2.2 节“地址类型和结构”[247]）。

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描述。

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 中对此进行了描述。

21.2.4 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 6.16.1.3 节“网络配置”(第 6 章 *使用 YaST 进行安装*, ↑*部署指南*)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 网络设置模块。在全局设置选项卡上，根据需要选中或取消选中 *启用 IPv6* 选项。如果要在下次重引导前暂时启用它，请以 root 用户身份输入 `modprobe -i ipv6`。一旦装载 `ipv6` 模块，基本上就无法卸载了。

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stations上管理路由选择表。工作stations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stations对 IPv6 地址使用哪个前缀和哪个路由器。或者，可以使用 `zebra/quagga` 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 `ifcfg-tunnel (5)` 手册页。

21.2.5 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。

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。

21.3 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。这些名称构成了具有层次结构的系统，各个名称组成部分之间用句点分隔。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 `jupiter.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 *root* 名称服务器。这些 *root* 名称服务器管理顶级域，并由网络信息中心 (NIC) 运行。每个 *root* 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。拨号协议在建立连接后提供名称服务器地址。有关如何在 SUSE® Linux Enterprise Server 中配置针对名称服务器的访问，请参

见第 21.4.1.4 节“配置主机名和 DNS”[262]。有关如何设置您自己的名称服务器，请参见第 24 章 域名系统 [309]。

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。

注意：MDNS 和 .local 域名

.local 顶级域由解析程序视为 link-local 域。DNS 请求作为多路广播 DNS 请求（而不是常规 DNS 请求）发送。如果已在名称服务器配置中使用 .local 域，必须在 /etc/host.conf 中关闭此选项。有关更多信息，请参见 host.conf 手册页。

如果要在安装期间关闭 MDNS，请使用 nomdns=1 作为引导参数。

有关多路广播 DNS 的详细信息，请参见 <http://www.multicastdns.org>。

21.4 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 21.6 节“手动配置网络连接”[276]。

在 SUSE Linux Enterprise Desktop 上（NetworkManager 默认已激活），所有网卡均已配置。如果 NetworkManager 未激活，仅具有链路的第一个接口（已连接网络电缆）会自动配置。可随时在已安装系统中配置额外的硬件。以下各节将介绍 SUSE Linux Enterprise Server 支持的所有网络连接类型的网络配置。

提示：IBM System z：热插拔网卡

IBM System z 平台支持网卡热插拔，但不支持通过 DHCP 进行自动网络集成（与 PC 情况相同）。检测到网卡后需要手动配置接口。

21.4.1 使用 YaST 配置网卡

要在 YaST 中配置有线或无线网卡，请选择 **网络设备 > 网络设置**。启动模块后，YaST 显示 **网络设置** 对话框，带有四个选项卡：**全局选项**、**概述**、**主机名/DNS** 和 **路由选择**。

通过全局选项选项卡可设置常规联网选项，如使用 NetworkManager、IPv6 和常规 DHCP 选项。有关详细信息，请参见第 21.4.1.1 节“配置全局联网选项”[255]。

概述选项卡包含关于已安装网络接口和配置的信息。会列出已正确检测到的所有网卡及其名称。您可在该对话框中手动配置新卡、删除或更改其配置。如果要手动配置未自动检测到的卡，请参见第 21.4.1.3 节“配置未检测到的网卡”[261]。如果要更改已配置卡的配置，请参见第 21.4.1.2 节“更改网卡的配置”[256]。

通过主机名/DNS 选项卡可设置计算机的主机名和要使用的服务器名称。有关详细信息，请参见第 21.4.1.4 节“配置主机名和 DNS”[262]。

路由选择选项卡用于配置路由选择。有关更多信息，请参见第 21.4.1.5 节“配置路由选择”[264]。

图 21.3 配置网络设置



21.4.1.1 配置全局联网选项

通过 YaST 网络设置模块的全局选项选项卡可设置重要的全局联网选项，如使用 NetworkManager、IPv6 和 DHCP 客户端选项。这些设置适用于所有网络接口。

在网络设置方法中，选择管理网络连接的方法。如果希望 NetworkManager 桌面小程序管理所有接口的连接，则选择通过 *NetworkManager* 的用户控制方法。此选项非常适用于在多个有线和无线网络之间切换。如果您没有运行桌面环境（GNOME 或 KDE）或者您的计算机是 Xen 服务器、虚拟系统，又或在网络中提供网络服务（如 DHCP 或 DNS），请使用通过 *ifup* 的传统方法。如果使用 NetworkManager，则应使用 nm-applet 配置网络选项，并且网络设置模块的概述、主机名/DNS和路由选择选项卡会被禁用。有关 NetworkManager 的更多信息，请参见第 26 章 使用 *NetworkManager* [349]。

在 IPv6 协议设置中，选择是否希望使用 IPv6 协议。可将 IPv6 与 IPv4 一起使用。默认情况下激活 IPv6。但是在不使用 IPv6 协议的网络中，如果禁用 IPv6 协议，响应时间会更快。如果要禁用 IPv6，请取消选中启用 IPv6 选项。这样将为 IPv6 禁用内核模块自动加载。这将在重引导后应用。

在 DHCP 客户端选项中，配置 DHCP 客户端的选项。如果希望 DHCP 客户端要求服务器始终广播其响应，则选中请求广播响应。如果您的计算机在不同网络之间移动，则可能需要选中此选项。在单个网络上，每个 DHCP 客户端的 DHCP 客户端标识符必须不同。如果保留为空，会默认为网络接口的硬件地址。但是，如果正在运行若干使用相同网络接口（即相同硬件地址）的虚拟机，则在此处指定唯一的自由格式标识符。

要发送的主机名指定 dhcpcd 向 DHCP 服务器发送消息时用于主机名选项的字符串。某些 DHCP 服务器会根据此主机名（动态 DNS）来更新名称服务器区域（转发和反转记录）。此外，有些 DHCP 服务器要求要发送的主机名选项字段包含来自客户端的 DHCP 消息中的特定字符串。选择 AUTO 可发送当前主机名（即 /etc/HOSTNAME 中所定义的）。将选项字段保留为空即可不发送任何主机名。如果您不希望根据 DHCP 中的信息更改默认路由，则取消选中通过 DHCP 更改默认路由。

21.4.1.2 更改网卡的配置

要更改网卡的配置，请在 YaST 网络设置 > 概述中已检测到的网卡列表中选择 一个网卡，然后单击编辑。将显示网卡设置对话框，可在其中使用常规、地址和硬件选项卡调整网卡配置。有关无线网卡配置的信息，请参见第 18.5 节“用 YaST 配置” [207]。

配置 IP 地址

您可在网卡设置对话框的地址选项卡中设置网卡的 IP 地址或 IP 地址的确定方法。同时支持 IPv4 和 IPv6 地址。网卡可设置为无 IP 地址（对于绑定设备很有用）、静态指派的 IP 地址（IPv4 或 IPv6）或通过 DHCP 和/或 Zeroconf 指派的动态地址。

如果使用动态地址，则选择是使用仅 DHCP 版本 4（用于 DHCPv4）、DHCP 版本 6（用于 DHCPv6）还是 DHCP 版本 4 和 6。

如果可能，安装期间的首个带链接的可用网卡将会通过 DHCP 自动配置为使用自动 IP 地址。在 SUSE Linux Enterprise Desktop 上（NetworkManager 默认已激活），所有网卡均已配置。

注意：IBM System z 和 DHCP

在 IBM System z 平台上，只有具备 MAC 地址的网卡才支持基于 DHCP 的地址配置。属于这种情况的只有 OSA 和 OSA Express 网卡。

如果使用的是 DSL 线路，但 ISP（因特网服务提供商）没有指派静态 IP，此时还应使用 DHCP。如果决定使用 DHCP，则在 YaST 网卡配置模块的网络设置对话框全局选项选项卡的 DHCP 客户端选项中配置细节。在请求广播响应中指定 DHCP 客户端是否应要求服务器始终广播其响应。如果您的计算机是在不同网络间移动的移动客户端，则可能需要使用此选项。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 DHCP 客户端标识符来区分。

DHCP 比较适合客户端配置，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 网卡配置模块的概述选项卡的已检测到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，选择静态指派的 IP 地址。
- 3 输入 IP 地址。IPv4 和 IPv6 地址均可使用。在子网掩码中输入子网掩码。如果使用 IPv6 地址，则对于前缀长度使用 /64 格式的子网掩码。

或者，您可以为此地址输入一个完全限定的主机名，该主机名将写入到 /etc/hosts 配置文件。

4 单击下一步。

5 要激活配置，请单击确定。

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。要配置名称服务器，请按照第 21.4.1.4 节“配置主机名和 DNS”[262] 中所述进行。要配置网关，请按照第 21.4.1.5 节“配置路由选择”[264] 中所述进行。

配置别名

一个网络设备可以有多个 IP 地址，称为别名。

注意：别名是兼容功能

这些所谓的别名表示标签只适用于 IPv4。对于 IPv6 则忽略它们。使用 `iproute2` 网络接口可以有一个或多个地址。

要用 YaST 为网卡设置别名，请如下继续操作：

- 1 在 YaST 网卡配置模块的概述选项卡的已检测到网卡列表中选择一个网卡，然后单击编辑。
- 2 在地址 > 附加地址选项卡中，单击添加。
- 3 输入别名、IP 地址和网络掩码。不要在别名中包含接口名称。
- 4 单击确定。
- 5 单击下一步。
- 6 要激活配置，请单击确定。

更改设备名称和 Udev 规则

可更改网卡在使用时的设备名称。还可确定 `udev` 是通过网卡的硬件 (MAC) 地址还是通过总线 ID 来标识网卡。在大型服务器中，更偏向于使用后者，以便减少网卡的热交换。要使用 YaST 来设置这些选项，请如下继续操作：

- 1 在 YaST 网络设置模块的概述选项卡的已检测到网卡列表中选择一个网卡，然后单击编辑。

- 2 转到**硬件**选项卡。当前设备名称显示在 *Udev 规则* 中。单击**更改**。
- 3 选择 **udev** 应通过网卡的 *MAC 地址* 还是 *总线 ID* 来识别网卡。网卡的当前 MAC 地址和总线 ID 显示在对话框中。
- 4 要更改设备名称，请选中 **更改设备名称** 选项并编辑名称。
- 5 单击**确定**然后单击**下一步**。
- 6 要激活配置，请单击**确定**。

更改网卡内核驱动程序

对于某些网卡，可能会提供某些内核驱动程序。如果网卡已配置，YaST 允许从可用的合适驱动程序列表中选择一个要使用的内核驱动程序。还可为内核驱动程序指定选项。要使用 YaST 来设置这些选项，请如下继续操作：

- 1 在 YaST 网络设置模块的**概述**选项卡的已检测到网卡列表中选择一个网卡，然后单击**编辑**。
- 2 转到**硬件**选项卡。
- 3 在**模块名称**中选择要使用的内核驱动程序。在**选项**中为所选驱动程序输入所有选项，形式为 `option=value` 。如果使用多个选项，应用空格分隔这些选项。
- 4 单击**确定**然后单击**下一步**。
- 5 要激活配置，请单击**确定**。

激活网络设备

如果您使用通过 `ifup` 的传统方法，则可以配置为在引导期间、连接电缆后或检测到网卡后启动设备，也可以配置为手动或从不启动设备。要更改设备启动，请如下继续操作：

- 1 在 YaST 中，在**网络设备 > 网络设置**中的已检测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。

选择在引导时可在系统引导时启动设备。使用在电缆连接时将对任何现有物理连接监视接口。使用在热插拔时将在接口可用时立即设置。这与在引导时选项很相似，唯一区别是如果引导时不存在接口，不会发生错误。选择手动可通过 `ifup` 手动控制接口。选择从不将不启动设备。通过 *NFSroot* 与在引导时相似，但使用 `rcnetwork stop` 命令时接口不会关闭。如果您使用 `nfs` 或 `iscsi root` 文件系统，则选择此选项。

3 单击下一步。

4 要激活配置，请单击确定。

通常，仅系统管理员可以激活或停用网络接口。如果希望任何用户均能通过 *KInternet* 激活此接口，请选择通过 *KInternet* 为非 *root* 用户启用设备控制。

设置最大传输单位大小

您可为接口设置最大传输单位 (MTU)。MTU 是指允许的最大包大小（以字节为单位）。更高的 MTU 可带来更高的带宽效率。但是较大的包有时可能会堵塞较慢的接口，从而增加后续包的延迟。

1 在 YaST 中，在网络设备 > 网络设置中的已检测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，从设置 MTU 列表中选择所需项。

3 单击下一步。

4 要激活配置，请单击确定。

配置防火墙

无须输入详细的防火墙设置（如第 15.4.1 节“Configuring the Firewall with YaST”（第 15 章 *Masquerading and Firewalls*, ↑安全指南）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 打开 YaST 网络设备 > 网络设置模块。在概述选项卡中，从已检测到的网卡列表中选择一个网卡，然后单击编辑。

2 进入网络设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：

防火墙已禁用

此选项只有在禁用防火墙和防火墙未在运行时才可用。仅当计算机属于受外部防火墙保护的大型网络时才使用此选项。

自动指派区域

此选项只有在启用防火墙后才可用。防火墙正在运行且接口自动指派给防火墙区域。包含关键字 `any` 的区域或外部区域将用于此类接口。

内部区域（未保护）

防火墙正在运行，但不会强制执行任何规则来保护此接口。当计算机属于受外部防火墙保护的大型网络时才使用此选项。当计算机具有多个网络接口时，此选项还可用于连接到内部网络的接口。

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）网络流量影响。这是默认选项。

4 单击下一步。

5 单击确定即可激活配置。

21.4.1.3 配置未检测到的网卡

可能未正确检测到您的网卡。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。还可以配置特殊网络设备类型，例如网桥、绑定、TUN 或 TAP。要配置未检测到的网卡（或特殊设备），请如下操作：

- 1 在 YaST 中的 **网络设备 > 网络设置 > 概述** 对话框中，单击 **添加**。
- 2 在 **硬件** 对话框中，从可用选项中设置接口的 **设备类型** 和 **配置名称**。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。或者，如果需要，您可定义要用于网卡的 **内核模块名称** 及其 **选项**。

在 *Ethtool* 选项中，您可以为接口设置 ifup 使用的 *ethtool* 选项。可用选项请参见 *ethtool* 手册页。如果选项字符串以 - 开始（例如 -K 接口名称 rx on），字符串中的第二项将替换为当前接口名。否则的话（例如 autoneg off speed 10）是 ifup 后跟 -s 接口名。

- 3 单击下一步。
- 4 在 *常规、地址和硬件* 选项卡中，配置所有所需的选项，如接口的 IP 地址、设备激活或防火墙区域。有关配置选项的更多信息，请参见第 21.4.1.2 节“更改网卡的配置” [256]。
- 5 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 18 章 *无线 LAN* [203] 中获得。
- 6 单击下一步。
- 7 要激活新网络配置，请单击 *确定*。

21.4.1.4 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已经可用，则已为计算机自动生成主机名并且已激活 *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 转到 YaST 中的 *网络设备模块中的网络设置 > 主机名/DNS* 选项卡。
- 2 输入 *主机名*，如果需要，也输入 *域名*。如果此计算机是邮件服务器，则该域特别重要。请注意，主机名是全局性的，应用于所有网络接口。

如果使用 *DHCP* 获取 IP 地址，则计算机的主机名将由 *DHCP* 自动设置。如果您连接到不同网络，您可能希望禁用此行为，因为它们可能指派不同主机名，而在运行时更改主机名可能会导致图形桌面混乱。要禁用使用 *DHCP* 获取 IP 地址，请取消选中 *通过 DHCP 更改主机名*。

指派主机名给回写 IP 会将您的主机名与 */etc/hosts* 中的 127.0.0.2（回写）IP 地址关联。如果您想让主机名即使在没有活动的网络时也随时可解析，这是有用的选项。

- 3 在修改 DNS 配置中，请选择修改 DNS 配置（名称服务器、搜索列表以及 /etc/resolv.conf 文件的内容）的方式。

如果选择了使用默认策略选项，则配置由 netconfig 脚本处理，该脚本合并了静态定义的数据（通过 YaST 或在配置文件中）与动态获取的数据（来自 DHCP 客户端或 NetworkManager）。在大多数情况下，此默认策略就足够了。

如果选择了仅手动选项，则不允许 netconfig 修改 /etc/resolv.conf 文件。但是，此文件可手动编辑。

如果已选择自定义策略选项，则应指定用于定义合并策略的自定义策略规则字符串。该字符串包含了接口名称的逗号分隔列表，可考虑作为设置的有效源。除了使用完整接口名外，也可使用如下的基本通配符来匹配多个接口。例如，eth* ppp? 首先以所有 eth 为目标，然后是 ppp0 到 ppp9 的所有接口。有两个特殊策略值表示如何应用 /etc/sysconfig/network/config 文件中定义的静态设置：

STATIC

静态设置必须与动态设置合并到一起。

STATIC_FALLBACK

仅当动态配置不可用时，才使用静态设置。

有关更多信息，请参见 man 8 netconfig。

- 4 输入名称服务器并填写域搜索列表。名称服务器必须由 IP 地址指定（如 192.168.1.116），而非由主机名指定。域搜索选项卡中指定的名称是用于解析主机名（无指定域）的域名。如果使用多个域搜索，则使用逗号或空格分隔域。

- 5 要激活配置，请单击确定。

也可以使用 YaST 从命令行编辑主机名。YaST 所做更改会立即生效（手动编辑 /etc/HOSTNAME 文件时则不是这样）。要更改主机名，请使用以下命令：

```
yast dns edit hostname=hostname
```

要更改名称服务器，请使用以下命令：

```
yast dns edit nameserver1=192.168.1.116
```

```
yast dns edit nameserver2=192.168.1.116
```

```
yast dns edit nameserver3=192.168.1.116
```

21.4.1.5 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 中，转到 *网络设置 > 路由选择*。
- 2 输入 *默认网关*（如果需要是 **IPv4** 和 **IPv6**）的 **IP 地址**。默认网关与每个可能的目标匹配，但是如果存在任何与所需地址匹配的其他项，则使用该项代替默认路由。
- 3 可在 *路由选择表* 中输入多个项。输入 *目标网络 IP 地址*、*网关 IP 地址* 和 *网络掩码*。选择将流量路由到定义的网络要经过的设备（减号代表任何设备）。要忽略这些值中的任何值，请使用减号 -。要在表中输入默认网关，请在 *目标* 字段中使用默认。

注意

如果使用更多的默认路由，则可以指定用于确定具有更高优先级的路由的度量选项。要指定度量选项，则在 *选项* 中输入 `-metricnumber`。默认情况下使用具有最高度量的路由。如果网络设备已断开连接，则删除其路由并使用下一个路由。但是，当前内核在静态路由选择中不使用度量，仅路由选择守护程序（如 **multipathd**）才在静态路由中使用度量。

- 4 如果系统是路由器，则在 *网络设置* 中启用 *IP 转发* 选项。
- 5 要激活配置，请单击 *确定*。

21.4.2 调制解调器

提示：IBM System z：调制解调器

IBM System z 平台不支持对这类硬件进行配置。

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。如果调制解调器已自动检测到，请转到调制解调器设备选项卡，并通过单击添加打开用于手动配置的对话框。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

与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 21.4 调制解调器配置



调制解调器参数

输入所有的调制解调器配置值。调制解调器设备指定与调制解调器连接的端口。 ttyS0、ttyS1... [更多](#)

调制解调器设备 (U) :

/dev/modem

拨号前缀 (如果需要) (O) :

拨号方式

特殊设置

☒ 音频拨号 (A)

☒ 扬声器打开 (S)

☐ 脉冲拨号 (P)

☒ 检测拨号音 (E)

细节 (D)

 帮助

 取消 (C)

 后退 (B)

 下一步 (N)

如果位于专用交换分机 (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 附带的描述了解相关信息。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没有 root 许可权限的普通用户，请激活通过 KInternet 为非 root 用户启用设备控制。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**。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。仅当您的因特网连接成本较低时才使用此功能，因为某些程序要求定期从因特网请求数据。

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。

自动重新连接

如果启用了此选项，则连接失败后会自动重新建立连接。

忽略提示

此选项将禁用对来自拨号服务器的任何提示检测。如果连接建立速度很慢，或根本不能建立连接，可尝试此选项。

外部防火墙接口

选择此选项将激活防火墙并将接口设置为外部的。这样您的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。单击确定可关闭此对话框。

21.4.3 ISDN

提示：IBM System z：ISDN

IBM System z 平台不支持对这类硬件进行配置。

使用此模块可以为系统配置一个或多个 ISDN 网卡。如果 YaST 没有检测到您的 ISDN 网卡，请在 *ISDN* 设备选项卡中单击添加，然后手动选择您的网卡。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 21.5 ISDN 配置

 **contr0 的 ISDN 低级配置**

如果选择引导时，则在系统引导过程中 装载驱动程序。如果选择手动，则必须使用 rcisdn start 命令启动驱动程序。只有根用 ... [更多](#)

ISDN 卡信息

制造商

ISDN 卡

Abocom/Magitek

2BD1

驱动程序 (D):

HiSax driver

ISDN 协议

☒ Euro-*ISDN* (EDSS1)(E)

☐ 1TR6(E)

☐ 专线(L)

☐ NI1(L)

国家/地区 (C):

德国

代码 (D):

+49

区域号码 (A):

拨号前缀 (D):

☒ 启动 ISDN 日志 (L)

激活设备 (D):

在引导时

帮助

取消

后退

确定

在下一个对话框中（如图 21.5 “ISDN 配置” [267] 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 *1TR6*。如

果是在美国，请选择 *NI1*。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，提供您的区域号码和拨号前缀（如果需要）。如果不希望记录所有 ISDN 流量，则取消选中 *启动 ISDN 日志* 选项。

激活设备定义应如何启动 ISDN 接口：使用在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 21.6 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的不同而变化：

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。有关进一步的信息，请参见电话交换机随附的文档。

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启动防火墙为链接启用防火墙。要使不具备管理员权限的普通用户能够激活或停用接口，请选择通过 *Kinternet* 为非 root 用户启用设备控制。

单击*细节*打开一个对话框，在其中可实施更为复杂的连接模式，这与普通的家庭用户无关。通过选择*确定*退出*细节*对话框。

在下一个对话框中配置 IP 地址设置。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。要激活这些设置，请选择*确定*。

21.4.4 电缆调制解调器

提示：IBM System z：电缆调制解调器

IBM System z 平台不支持对这类硬件进行配置。

在某些国家/地区，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。

根据您的ISP提供的描述，配置网卡时选择*动态地址*或*静态指派的IP地址*。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。

21.4.5 DSL

提示：IBM System z：DSL

IBM System z 平台不支持对这类硬件进行配置。

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。

- 以太网上的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

在*DSL配置概述*对话框的*DSL设备*选项卡中，您将找到已安装DSL设备的列表。要更改DSL设备的配置，请在列表中选择该设备，然后单击*编辑*。如果单击*添加*，则可手动配置新DSL设备。

基于PPPoE或PPTP配置DSL连接时，要求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21.4.1节“使用YaST配置网卡”[254]）。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*动态地址*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。

在第一个 DSL 配置对话框（请参见图 21.7 “DSL 配置” [272]）中，首先应选择 PPP 方式及 DSL 调制解调器连接到的以太网卡（多数情况下是 eth0）。然后使用激活设备指定是否应在引导进程中建立 DSL 链接。单击通过 *KInternet* 为非 root 用户启用设备控制可授权普通用户无需 root 权限即可使用 KInternet 激活或停用接口。

在下一个对话框中，选择您的国家/地区并从该国家/地区运营的众多 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。

图 21.7 DSL 配置



DSL 配置

在此可设置 DSL 连接 最重要的设置。 首先，请选择 PPP 方式。 可以是 PPP over Ethernet (… [更多](#))

DSL 连接设置

PPP 方式 (M):

PPP 方式相关设置

VPI/VCI (V):

Ethernet 网卡 (E)

未知设备
未知 - 未指派 IP 地址

更改设备 (C)

配置网卡 (C)

服务器名或 IP 地址 (S):

10.0.0.138

激活设备 (D):

手动

☒ 通过 KInternet 为非 root 用户启用设备控制 (N)

帮助

取消 (C)

后退 (B)

下一步 (N)

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 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。所有这些都会包含在订阅到 T-DSL 后收到的信息中。

21.4.6 IBM System z：配置网络设备

用于 IBM System z 的 SUSE Linux Enterprise Server 支持几种不同类型的网络接口。可使用 YaST 来配置所有接口。

21.4.6.1 qeth-hsi 设备

要将 `qeth-hsi` (Hipersockets) 接口添加到已安装系统中，请启动 YaST 中的 **网络设备 > 网络设置** 模块。选择标记为 *Hipersocket* 的设备之一以用作 **READ** 设备地址，然后单击 **编辑**。输入设备编号供读、写和控制通道（例如设备编号格式：0.0.0600）。然后单击“下一步”。在 **网络地址设置** 对话框中，为新接口指定 IP 地址和网络掩码，然后按 **下一步** 和 **确定** 退出网络配置。

21.4.6.2 qeth-ethernet 设备

要将 `qeth-ethernet` (IBM OSA Express 以太网卡) 接口添加到已安装系统中，请启动 YaST 中的 **网络设备 > 网络设置** 模块。选择标有 *IBM OSA 快速以太网卡* 的任一设备以用作“读”设备地址并单击 **编辑**。输入设备编号供读、写和控制通道（例如设备编号格式：0.0.0600）。输入所需端口名称、端口号（如果适用）和一些附加选项（请参见手册 *Linux for IBM System z: Device Drivers, Features, and Commands*, http://www.ibm.com/developerworks/linux/linux390/documentation/novell_suse.html）、您的 IP 地址及相应的网络掩码。单击 **下一步** 和 **确定** 退出网络配置。

21.4.6.3 ctc 设备

要将 `ctc` (IBM 并行 CTC 适配器) 接口添加到已安装系统中，请启动 YaST 中的 **网络设备 > 网络设置** 模块。选择标记为 *IBM 并行 CTC 适配器* 的设备之一，用作读取通道，然后单击 **配置**。选择适合您设备的 **设备设置**（通常为兼容性方式）。指定您的 IP 地址和远程合作伙伴的 IP 地址。如果需要，可使用 **高级 > 详细设置** 调整 MTU 的大小。单击 **下一步** 和 **确定** 退出网络配置。

警告

不建议使用此接口。在 SUSE Linux Enterprise Server 的未来版本中将不支持此接口。

21.4.6.4 lcs 设备

要将 `lcs` (IBM OSA-2 适配器) 接口添加到已安装系统中, 请启动 YaST 中的 **网络设备 > 网络设置** 模块。选择标记为 *IBM OSA-2 适配器* 的设备之一, 然后单击 **配置**。输入所需端口号、一些附加选项 (请参见位于 http://www.ibm.com/developerworks/linux/linux390/documentation_novell_suse.html 的手册 *Linux for IBM System z: Device Drivers, Features, and Commands*) (Linux for IBM System z: 设备驱动程序、功能和命令)、您的 IP 地址和相应的网络掩码。单击 **下一步** 和 **确定** 退出网络配置。

21.4.6.5 IUCV 设备

要将 `iucv` (IUCV) 接口添加到已安装系统中, 请启动 YaST 中的 **网络设备 > 网络设置** 模块。选择标记为 *IUCV* 的设备并单击 **编辑**。YaST 会提示输入 IUCV 合作伙伴的名称 (同级)。输入该名称 (此项区分大小写), 然后选择 **下一步**。指定您的合作伙伴的 *IP 地址* 和 *远程 IP 地址*。如果需要, 在 **常规选项卡** 上设置 *MTU* 大小。单击 **下一步** 和 **确定** 退出网络配置。

警告

不建议使用此接口。在 SUSE Linux Enterprise Server 的未来版本中将不支持此接口。

21.5 NetworkManager

NetworkManager 是用于便携式计算机和其他可移动计算机的理想解决方案。有了 NetworkManager, 您在移动中配置网络接口和切换网络时就无需担心了。

21.5.1 NetworkManager 和 ifup

但是 NetworkManager 并非适用于所有情况的解决方案, 因此您仍可在用于管理网络连接 (ifup) 的传统方法和 NetworkManager 之间进行选择。如果您希望使用 NetworkManager 管理网络连接, 则在 YaST 网络设置模块中启用 NetworkManager (如第 26.2 节 “启用或禁用 NetworkManager” [350] 中所述), 然后使用 NetworkManager 配置网络连接。有关使用案例的列表以及如何配置和使用 NetworkManager 的详细说明, 请参见第 26 章 *使用 NetworkManager* [349]。

ifup 和 NetworkManager 之间的某些区别包括：

root 特权

如果使用 NetworkManager 进行网络设置，则可以使用一个小程序，随时从您的桌面环境内轻松地切换、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。

传统的 ifup 配置也提供一些切换、停止或启动连接的途径（需要或不需要用户干预），就像用户管理的设备那样。但是，这总是需要有 root 特权才能更改或配置网络设备。这对于移动计算是个常见问题，因为移动计算不可能预配置所有的连接功能。

网络连接的类型

传统配置和 NetworkManager 都可以处理与无线网络（WEP、WPA-PSK 和 WPA-Enterprise 访问）和使用 DHCP 及静态配置的有线网络之间的网络连接。它们还支持拨号、DSL 和 VPN 连接。使用 NetworkManager 还可以连接移动宽带（3G）调制解调器，而传统配置则不能进行这种连接。

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具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。

21.5.2 NetworkManager 功能和配置文件

用 NetworkManager 创建的各网络连接设置储存在配置的配置文件中。用 NetworkManager 或 YaST 配置的系统连接将保存在 `/etc/networkmanager/system-connections/*` 或 `/etc/sysconfig/network/ifcfg-*` 中。用户定义的任何连接储存在 GConf (GNOME) 或 `$HOME/.kde4/share/apps/networkmanagement/*` (KDE) 中。

在未配置配置文件的情况下，NetworkManager 自动创建一个，命名为 `Auto$INTERFACE-NAME`。这样做是试图无需为任意多的（安全）案例进行任何配置就能使用。如果自动创建的配置文件不适合您的需要，请用 KDE 或 GNOME 提供的网络连接配置按需要修改它们。有关更多信息，请参考第 26.3 节“配置网络连接”[351]。

21.5.3 控制和锁定 NetworkManager 功能

在中央管理的计算机上，某些 NetworkManager 功能可以用 PolicyKit 控制或禁用，例如，如果允许某用户修改管理员定义的连接，或者允许某用户定义自己的网络配置。要查看或更改各 NetworkManager 策略，请启动 PolicyKit 的授权工具。在左侧的树中 *network-manager-settings* 条目下找到它们。有关 PolicyKit 的介绍以及如何使用它的详细信息，请参见 第 9 章 *PolicyKit* (↑安全指南)。

21.6 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。

当内核检测到某个网卡并创建相应的网络接口时，会根据设备发现的顺序或装载内核模块的顺序为设备指派一个名称。只有在非常简单或严格控制的硬件环境中，才能预测默认内核设备名称。允许在运行时添加或删除硬件的系统或者支持自动配置设备的系统不能期望在各个重引导之间由内核指派稳定的网络设备名称。

但是，所有系统配置工具均依赖持久性接口名称。该问题通过 udev 解决。udev 永久网络生成器 (`/lib/udev/rules.d/75-persistent-net-generator.rules`) 会生成匹配硬件的规则（默认情况下使用其硬件地址），并为该硬件分配永久唯一接口。网络接口的 udev 数据库储存在文件 `/etc/udev/rules.d/70-persistent-net.rules` 中。文件中的每一行描述一个网络接口并指定其永久名称。系统管理员可通过编辑 `NAME=""` 项来更改指派的名称。也可以使用 YaST 修改永久规则。

表 21.5 “手动网络配置脚本” [276] 总结了网络配置中涉及的最重要脚本。

表 21.5 手动网络配置脚本

命令	功能
<code>ifup</code> 、 <code>ifdown</code> 、 <code>ifstatus</code>	<code>if</code> 脚本启动或停止网络接口，或者返回指定接口的状态。有关更多信息，请参见 <code>ifup</code> 手册页。

命令	功能
rcnetwork	rcnetwork 脚本可用于启动、停止或重新启动所有网络接口（或某个指定接口）。使用 rcnetwork stop、rcnetwork start 和 rcnetwork restart 可分别停止、启动和重新启动网络接口。如果要停止、启动或重新启动一个接口，请在命令后加上该接口名称，例如 rcnetwork restart eth0。 rcnetwork status 命令显示接口的状态、其 IP 地址以及 DHCP 客户端是否正在运行。通过 rcnetwork stop-all-dhcp-clients 和 rcnetwork restart-all-dhcp-clients，您可停止或重新启动运行在网络接口上的 DHCP 客户端。

有关 udev 和永久设备名称的更多信息，请参见第 14 章 *使用 udev 进行动态内核设备管理* [163]。

21.6.1 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。

21.6.1.1 /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。此外，如果常规设置应只用于一个接口，则 dhcp 文件中的大多数变量可用于 ifcfg-* 文件。但是，/etc/sysconfig/network/config 中的大多数变量是全局变量，不能在 ifcfg-files 中被覆盖。例如，NETWORKMANAGER 或 NETCONFIG_* 变量是全局变量。

有关 `ifcfg.template` 的信息，请参见第 21.6.1.2 节 “`/etc/sysconfig/network/config` 和 `/etc/sysconfig/network/dhcp`” [278]。

► **System z:** IBM System z 不支持 USB。接口文件的名称和网络别名包含特定于 System z 的元素，例如 `qeth`。 ◀

21.6.1.2 `/etc/sysconfig/network/config` 和 `/etc/sysconfig/network/dhcp`

文件 `config` 包含 `ifup`、`ifdown` 和 `ifstatus` 行为的常规设置。`dhcp` 包含 DHCP 的设置。这两个配置文件中的变量已注释掉。`/etc/sysconfig/network/config` 中的一些变量也可用于 `ifcfg-*` 文件，在这些文件中它们具有更高优先级。`/etc/sysconfig/network/ifcfg.template` 文件列出可以按接口指定的变量。但是，`/etc/sysconfig/network/config` 中的大多数变量是全局变量，不能在 `ifcfg-files` 中被覆盖。例如，`NETWORKMANAGER` 或 `NETCONFIG_*` 变量是全局变量。

21.6.1.3 `/etc/sysconfig/network/routes` 和 `/etc/sysconfig/network/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，如回写、以太网、ISDN、PPP 和虚设设备。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。

IPv4 和 IPv6 的统一格式现在如下所示：

```
prefix/lengthgateway - [interface]
```

对应的兼容性格式则如下所示：

```
prefixgatewaylength [interface]
```

对于 IPv4，仍可使用子网掩码旧格式：

```
ipv4-networkgatewayipv4-netmask [interface]
```

以下示例等效：

```
2001:db8:abba:cafe::/64 2001:db8:abba:cafe::dead - eth0
208.77.188.0/24 208.77.188.166 - eth0

2001:db8:abba:cafe:: 2001:db8:abba:cafe::dead 64 eth0
208.77.188.0 208.77.188.166 24 eth0

208.77.188.0 208.77.188.166 255.255.255.0 eth0
```

21.6.1.4 /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`）。可在文件中指定多个域名。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。可在多行中指定多个名称服务器，每个以 `nameserver` 开始。注释以 `#` 符号开头。例 21.5 “`/etc/resolv.conf`” [280] 显示 `/etc/resolv.conf` 的内容。

但是，`/etc/resolv.conf` 不应手动编辑。而是由 `netconfig` 脚本生成。要定义静态 DNS 配置而不使用 YaST，请手动编辑 `/etc/sysconfig/network/config` 文件中的相应变量：

```
NETCONFIG_DNS_STATIC_SEARCHLIST
    用于主机名查找的 DNS 域名列表
```

NETCONFIG_DNS_STATIC_SERVERS

用于主机名查找的名称服务器 IP 地址列表

NETCONFIG_DNS_FORWARDER

定义必须要配置的 DNS 转发器的名称

要使用 `netconfig` 禁用 DNS 配置，请设置 `NETCONFIG_DNS_POLICY=''`。有关 `netconfig` 的更多信息，请参见 `man 8 netconfig`。

例 21.5 /etc/resolv.conf

```
# Our domain
search example.com
#
# We use dns.example.com (192.168.1.116) as nameserver
nameserver 192.168.1.116
```

21.6.1.5 /sbin/netconfig

`netconfig` 是一个用于管理附加网络配置设置的模块化工具。它合并了静态定义的设置和自动配置机制根据预定义策略以 DHCP 或 PPP 形式提供的设置。通过调用负责修改配置文件和重启动服务或相似操作的 `netconfig` 模块将所需更改应用于系统。

`netconfig` 识别三种主要操作。`netconfig modify` 和 `netconfig remove` 命令由诸如 DHCP 或 PPP 的守护程序用于在 `netconfig` 中提供设置或从中删除设置。仅 `netconfig update` 命令可用于用户：

`modify`

`netconfig modify` 命令修改特定于当前接口和服务的动态设置并更新网络配置。`Netconfig` 从标准输入或使用 `--lease-file filename` 选项指定的文件中读取设置，并将其储存在内部，直到系统重引导（或者执行下一个修改或删除操作）。已存在的相同接口和服务组合设置将会重写。该接口由 `-i interface_name` 参数指定。该服务由 `-s service_name` 参数指定。

`remove`

`netconfig remove` 命令为指定接口和服务组合删除由修改操作提供的动态设置并更新网络配置。该接口由 `-i interface_name` 参数指定。该服务由 `-s service_name` 参数指定。

update

`netconfig update` 命令使用当前设置更新网络配置。当策略或静态配置更改时，这非常有用。如果要仅更新指定服务（`dns`、`nis` 或 `ntp`），请使用 `-m module_type` 参数。

`netconfig` 策略和静态配置设置可手动定义或者使用 YaST 在 `/etc/sysconfig/network/config` 文件中定义。由自动配置工具以 `DHCP` 或 `PPP` 形式提供的动态配置设置由这些工具通过 `netconfig modify` 和 `netconfig remove` 操作直接递送。`NetworkManager` 也使用 `netconfig modify` 和 `netconfig remove` 操作。启用 `NetworkManager` 时，`netconfig`（在策略模式 `auto` 中）仅使用 `NetworkManager` 设置，忽略任何其他接口使用传统 `ifup` 方法配置的设置。如果 `NetworkManager` 不提供任何设置，也将静态设置用作备份。不支持混合使用 `NetworkManager` 和传统 `ifup` 方法。

有关 `netconfig` 的更多信息，请参见 `man 8 netconfig`。

21.6.1.6 /etc/hosts

在此文件中，如例 21.6 “`/etc/hosts`”[281] 中所示，将为主机名指派 IP 地址。如果未实施名称服务器，则将与其建立 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 21.6 /etc/hosts

```
127.0.0.1 localhost
192.168.2.100 jupiter.example.com jupiter
192.168.2.101 venus.example.com venus
```

21.6.1.7 /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。请参见例 21.7 “`/etc/networks`”[281]。

例 21.7 /etc/networks

```
loopback      127.0.0.0
localnet      192.168.0.0
```

21.6.1.8 /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 21.6 “/etc/host.conf 的参数” [282] 显示了可用的参数。例 21.8 “/etc/host.conf” [282] 中显示了 /etc/host.conf 的示例。

表 21.6 /etc/host.conf 的参数

<i>order hosts、bind</i>	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）：
	<i>hosts</i> ：搜索 /etc/hosts 文件
	<i>bind</i> ：访问名称服务器
	<i>nis</i> ：使用 NIS
<i>multi on/off</i>	定义 /etc/hosts 中输入的主机是否可以具有多个 IP 地址。
<i>nospoof on spoofalert on/off</i>	这些参数影响名称服务器 <i>spoofing</i> ，但对网络配置没有任何影响。
<i>trim domainname</i>	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）。此选项仅当本地域名在 /etc/hosts 文件中时才有用，但仍应通过附带的域名进行识别。

例 21.8 /etc/host.conf

```
# We have named running
order hosts bind
# Allow multiple address
multi on
```

21.6.1.9 /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 库参考手册》。

查询的顺序是在文件 `/etc/nsswitch.conf` 中定义的。例 21.9 “`/etc/nsswitch.conf`” [283] 中显示了 `nsswitch.conf` 的示例。注释以 `#` 符号开头。在本例中，`hosts` 数据库下的项意味着通过 DNS（请参见 第 24 章 域名系统 [309]）将请求发送到 `/etc/hosts` (files)。

例 21.9 `/etc/nsswitch.conf`

```
passwd:      compat
group:       compat

hosts:       files dns
networks:    files dns

services:    db files
protocols:   db files
rpc:         files
ethers:      files
netmasks:    files
netgroup:    files nis
publickey:   files

bootparams:  files
automount:   files nis
aliases:     files nis
shadow:      compat
```

表 21.7 “通过 `/etc/nsswitch.conf` 可用的数据库” [283] 中列出了 NSS 上可用的“数据库”。表 21.8 “NSS“数据库”的配置选项” [284] 中列出了 NSS 数据库的配置选项。

表 21.7 通过 `/etc/nsswitch.conf` 可用的数据库

aliases	sendmail 实施的邮件别名；请参见 <code>man5 aliases</code> 。
ethers	以太网地址。
netmasks	网络及其子网掩码的列表。只有在使用子网划分时才需要。

group	对于 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。
publickey	NFS 和 NIS+ 使用的 Secure_RPC 的公钥和密钥。
password	getpwent 使用的用户密码；请参见 passwd(5) 手册页。
protocols	网络协议，由 getprotoent 使用；请参见 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。
services	getservent使用的网络服务。
shadow	用户阴影密码，由 getspnam 使用；请参见 shadow(5) 手册页。

表 21.8 NSS“数据库”的配置选项

files	直接访问文件，例如 /etc/aliases
db	通过数据库访问

<code>nis、nisplus</code>	NIS，另请参见 第 3 章 <i>Using NIS</i> (↑安全指南)
<code>dns</code>	仅可用作 <code>hosts</code> 和 <code>networks</code> 的扩展名
<code>compat</code>	仅可用作 <code>passwd</code> 、 <code>shadow</code> 和 <code>group</code> 的扩展名

21.6.1.10 /etc/nscd.conf

此文件用于配置 `nscd`（名称服务缓存守护程序）。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` 重新启动 `nscd` 可缩短此等待时间。

21.6.1.11 /etc/HOSTNAME

这包含附带了域名的完全限定的主机名。当引导计算机时，此文件将被多个脚本读取。它只能包含一行（在此行中设置主机名）。

21.6.2 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保存更改。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。

21.6.2.1 使用 ip 配置网络接口

`ip` 是用来显示和配置网络设备、路由选择、策略路由选择以及隧道的工具。

`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：

`link`

此对象表示网络设备。

`address`

此对象表示设备的 IP 地址。

邻区

此对象表示 ARP 或 NDISC 缓存项。

`route`

此对象表示路由选择表项。

`rule`

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 addradd 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 addgateway 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 `ip help` 或参见 `ip(8)` 手册页。`help` 选项还可用于所有 `ip` 子命令。例如，如果需要有关 `ip addr` 的帮助，请输入 `ip addr help`。可在 `/usr/share/doc/packages/iproute2/ip-cref.pdf` 中找到 `ip` 手册。

21.6.2.2 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` 将据此显示一条消息，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功能：它还能提供关于连接质量的一些基本信息。在例 21.10 “命令 `ping` 的输出” [287] 中，可查看 `ping` 输出示例。倒数第二行包含有关已传输的包数、丢失的包和 `ping` 的总运行时间的信息。

您可以使用主机名或 IP 地址（例如 `pingexample.com` 或 `ping192.168.3.100`）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 example.com`。

例 21.10 命令 `ping` 的输出

```
ping -c 3 example.com
PING example.com (192.168.3.100) 56(84) bytes of data.
64 bytes from example.com (192.168.3.100): icmp_seq=1 ttl=49 time=188 ms
64 bytes from example.com (192.168.3.100): icmp_seq=2 ttl=49 time=184 ms
```

```
64 bytes from example.com (192.168.3.100): 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` 来更改间隔。例如，要将 `ping` 间隔延长为十秒，则输入 `ping -i 10 example.com`。

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 example.com`。

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。

提示：Ping IPv6 地址

对于 IPv6 地址，请使用 `ping6` 命令。请注意，要 `ping` 本地链路地址，必须用 `-I` 指定接口。如果通过 `eth1` 可获取地址，则以下命令有效：

```
ping6 -I eth1 fe80::117:21ff:feda:a425
```

21.6.2.3 使用 `ifconfig` 配置网络

`ifconfig` 是一种网络配置工具。

注意：ifconfig 和 ip

`ifconfig` 工具已过时。请改为使用 `ip`。与 `ip` 相比，您只能将 `ifconfig` 用于接口配置。它将接口名称限制为 9 个字符。

毫无疑问，`ifconfig` 可显示当前活动接口的状态。如例 21.11 “`ifconfig` 命令的输出” [288] 中所见，`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（HWaddr 的值）。

例 21.11 `ifconfig` 命令的输出

```
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` 或参见 `ifconfig (8)` 手册页。

21.6.2.4 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以及添加或删除路由。

注意：`route` 和 `ip`

程序 `route` 已过时。请改为使用 `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 21.12 `route -n` 命令的输出

```

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` 或参见 `route (8)` 手册页。

21.6.3 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 21.9 “网络程序的一些启动脚本” [290]

表 21.9 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。如果 <code>network</code> 服务未启动，则不实施任何网络接口。
<code>/etc/init.d/xinetd</code>	启动 <code>xinetd</code> 。 <code>xinetd</code> 可用于使服务器服务在系统上可用。例如，它可以在初始化 FTP 连接时启动 <code>vsftpd</code> 。
<code>/etc/init.d/rpcbind</code>	启动用于将 RPC 程序号转换为通用地址的 <code>rpcbind</code> 实用程序。它是 RPC 服务所必需的，如 NFS 服务器。
<code>/etc/init.d/nfsserver</code>	启动 NFS 服务器。
<code>/etc/init.d/postfix</code>	控制 <code>postfix</code> 进程。
<code>/etc/init.d/ypserv</code>	启动 NIS 服务器。
<code>/etc/init.d/ypbind</code>	启动 NIS 客户端。

21.7 设置联接设备

对于某些系统，需要实施高于典型以太网设备的标准数据安全性或可用性要求的网络连接。在这些情况下，可以将多个以太网设备聚合到单个绑定设备。

联接设备的配置通过联接模块选项来完成。其行为主要受联接设备模式的影响。默认情况下是 mode=active-backup，即如果活动从属设备发生故障，则其他从属设备将变成活动从属设备。

提示：联接和 Xen

联接设备只对于有多个真实网卡可用的计算机有效。这意味着在大多数配置中，您仅应在 Domain0 中使用联接配置。换言之，只有当您多个网卡指派给一个 VM Guest 系统时，在 VM Guest 中设置联接才有效。

要配置联接设备，请使用以下过程：

- 1 运行 YaST > 网络设备 > 网络设置。
- 2 使用添加并将设备类型更改为联接。按下一步继续。

网卡设置

常规

地址

硬件

绑定从属

设备类型

绑定

配置名称

bond0

无链接和 IP 设置（绑定从属）

动态地址

DHCP

DHCP 版本 4 和 6

静态指派 IP 地址

IP 地址

子网掩码

主机名

附加地址

别名

IP 地址

网络掩码

添加

编辑

删除

帮助

取消

后退

下一步

- 3 选择如何为联接设备指派 IP 地址。有三种方法可供选择：

- 无 IP 地址
- 动态地址（使用 DHCP 或 Zeroconf）
- 静态指派的 IP 地址

基本联网知识

291

使用最适合您环境的方法。

- 4 在联接从属选项卡中，通过激活相关复选框选择应加入到联接中的以太网设备。
- 5 编辑联接驱动程序选项。以下模式可用于配置：
 - balance-rr
 - active-backup
 - balance-xor
 - 广播
 - 802.3ad
 - balance-tlb
 - balance-alb
- 6 确保将参数 `miimon=100` 添加到联接驱动程序选项。如果没有此参数，则不会定期检查数据完整性。
- 7 单击下一步，然后单击确定退出 YaST 以创建设备。

有关所有模式以及更多选项的详细说明，可在安装 `kernel-source` 程序包后参见 `/usr/src/linux/Documentation/networking/bonding.txt` 中的 *Linux* 以太网联接驱动程序操作指南。

21.7.1 联接从属的热插拔

在特定网络环境（如高可用性）下，有几种情况需要替换联接从属接口。原因可能在于网络设备持续故障。解决方案是设置联接从属的热插拔。

按常规配置联接（按照 `man 5 ifcfg-bonding`），例如：

```
ifcfg-bond0
    STARTMODE='auto' # or 'onboot'
    BOOTPROTO='static'
```

```
IPADDR='192.168.0.1/24'  
BONDING_MASTER='yes'  
BONDING_SLAVE_0='eth0'  
BONDING_SLAVE_1='eth1'  
BONDING_MODULE_OPTS='mode=active-backup miimon=100'
```

但要使用 `STARTMODE=hotplug` 和 `BOOTPROTO=none` 指定从属：

```
ifcfg-eth0  
    STARTMODE='hotplug'  
    BOOTPROTO='none'  
  
ifcfg-eth1  
    STARTMODE='hotplug'  
    BOOTPROTO='none'
```

`BOOTPROTO=none` 使用 `ethtool` 选项（如果提供），但不要在 `ifup eth0` 上设置链路，因为从属接口由联接主接口控制。

`STARTMODE=hotplug` 会让从属接口在可用之时自动加入联接。

必须更改 `/etc/udev/rules.d/70-persistent-net.rules` 中的 `udev` 规则，使之按照总线 ID（`udev KERNELS` 关键字等于使用 `hwinfo --netcard` 后出现的“SysFS BusID”）而不是 MAC 地址与设备匹配。这样变更后便可替换有问题的硬件（插在相同插槽中的网卡具有不同的 MAC），并可避免在联接更改其所有从属接口的 MAC 地址时产生混淆。

例如：

```
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",  
KERNELS=="0000:00:19.0", ATTR{dev_id}=="0x0", ATTR{type}=="1",  
KERNEL=="eth*", NAME="eth0"
```

在引导时，`/etc/init.d/network` 不会等待热插拔从属接口，但会等待联接准备就绪，而这需要至少有一个从属接口可用。当从系统中去除一个从属接口时（从 NIC 驱动程序拆联接、执行 NIC 驱动程序的 `rmmod` 命令或 PCI 热插拔去除为 `true`），内核会自动从联接中将其去除。当向系统添加新网卡时（替换插槽中的硬件），`udev` 会使用基于总线的网卡设备名称规则将其重命名为从属接口的名称，并为其调用 `ifup` 命令。`ifup` 命令会自动调用以将新网卡加入联接。

21.8 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。用桌面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。

在这种环境下需使用 `smpppd` (SUSE Meta PPP Daemon)。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。

21.8.1 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`，请将此选项设置为 `yes`。`smpppd` 侦听端口 3185。

如果将此参数设置为 `yes`，则还必须相应设置 `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 ipmax 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端仅限于授权主机。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，所有客户端都有权访问 `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。

21.8.2 为远程使用配置 `cinternet`

`cinternet` 可用于控制本地或远程 `smpppd`。`cinternet` 是图形 `KInternet` 的命令行形式。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 `cinternet`。此文件仅使用四个选项：

`sites = list of sites`

`list of sites`，其中前端搜索 `smpppd`。前端将按照在此指定的选项顺序来测试这些选项。`local` 规定建立到本地 `smpppd` 的连接。`gateway` 指向网关上的 `smpppd`。`config-file` 表示应建立到 `/etc/smpppd-c.conf` 中 `server` 和 `port` 选项指定的 `smpppd` 连接。`slp` 命令前端通过 SLP 连接到发现的 `smpppd`。

`server = server`

运行 `smpppd` 的主机。

`port = port`

运行 `smpppd` 的端口。

`password = password`

为 `smpppd` 选择的密码。

如果 `smpppd` 处于活动状态，请尝试访问它。例如，使用 `cinternet --verbose --interface-list`。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端的配置。要配置网络客户端（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端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 Server 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 为联网客户端（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 Server 中的 SLP 支持

提供 SLP 支持的服务包括 cupsd、rsyncd、ypserv、openldap2、ksysguardd、saned、kdm、vnc、login、smpppd、rpasswd、postfix 和 sshd（通过 fish）。

22.1 安装

将默认安装所有必需的包。但是，如果您要通过 SLP 提供服务，请确认 openslp-server 已安装。

22.2 激活 SLP

要用 SLP 提供服务，您的系统上必须运行 `slpd`。如果计算机仅作为客户端操作，且不提供服务，则无需运行 `slpd`。类似 SUSE Linux Enterprise Server 中的大多数系统服务，`slpd` 守护程序通过单独的 `init` 脚本来控制。安装后，默认情况下停用守护程序。要将其临时激活，请作为 `root` 运行 `rcslpd start`，或运行 `rcslpd stop` 停止它。使用 `restart` 或 `status` 可分别执行重启或状态检查。如果希望引导时 `slpd` 始终处于活动状态，请在 YaST 系统 > 系统服务（运行级别）中启用 `slpd`，或以 `root` 身份运行 `insserv slpd` 命令。

22.3 SUSE Linux Enterprise Server 中的 SLP 前端

要在您的网络中查找通过 SLP 提供的服务，请使用 SLP 前端，比如 `slptool`（`openslp` 包）或 YaST：

slptool

`slptool` 是可用于在网络中发布 SLP 查询或发布专有服务的命令程序。

`slptool --help` 列出所有可用的选项和函数。例如，要在当前网络中查找自行发布的所有时间服务器，请运行以下命令：

```
slptool findsrvs service:ntp
```

YaST

YaST 也提供 SLP 浏览器。但是，该浏览器不能从 YaST 控制中心访问。要启动该浏览器，请作为 `root` 用户运行 `yast2 slp`。单击左侧的 *服务类型* 可获取有关服务的更多信息。

22.4 通过 SLP 安装

如果在网络内提供了带 SUSE Linux Enterprise Server 安装媒体的安装服务器，则可以通过 SLP 注册和提供。有关详细信息，请参见第 14.2 节“设置存放安装源的服务器”（第 14 章 远程安装, ↑部署指南）。如果选定 SLP 安装，`linuxrc` 将在系统从选定引导媒体引导之后启动 SLP 查询，并显示找到的安装源。

22.5 通过 SLP 提供服务

SUSE Linux Enterprise Server 中的许多应用程序都已使用 `libslp` 库集成了 SLP 支持。如果服务未符合 SLP 支持，请使用以下方法之一使其可通过 SLP 发布。

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。这是一个注册扫描仪服务的示例：

```
## 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。

该注册文件还包含 `watch-port-tcp` 和 `description` 这两个变量。`watch-port-tcp` 通过使 `slpd` 检查相关服务的状态，链接 SLP 服务对该服务是否活动的发布。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描述。

提示：YaST 和 SLP

在模块对话框中激活 SLP 后，由 YaST 代理的某些服务（如安装服务器或 YOU 服务器）会为您自动执行此注册。然后，YaST 为这些服务创建注册文件。

通过 `/etc/slp.reg` 进行的静态注册

此方法与使用 `/etc/slp.reg.d` 的步骤之间唯一的区别在于，所有服务在中心文件中分组。

使用 `slptool` 进行的动态注册

如果某个服务须动态注册，而无需配置文件，请使用 `slptool` 命令行实用程序。相同的实用程序还可用于取消某个现有服务产品的注册，而无需重启动 `slpd`。

22.6 更多信息

RFC 2608、2609、2610

RFC 2608 主要描述了 SLP 的定义。RFC 2609 更详细地描述了所用服务 URL 的语法；RFC 2610 则对通过 SLP 的 DHCP 进行了描述。

<http://www.openslp.org>

OpenSLP 项目的主页。

`/usr/share/doc/packages/openslp`

此目录包含附于 `openslp-server` 包中的 SLP 的文档，其中 `README.SuSE` 包含 SUSE Linux Enterprise Server 细节、RFC 和两个介绍性的 HTML 文档。希望使用 SLP 功能的程序员可在 `openslp-devel` 包中包括的 *编程指南* 中找到更多信息。

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。内置硬件时钟往往不能满足数据库或群集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。NTP 提供了解决这些问题的机制。NTP 服务借助网络中的可靠时间服务器持续调整系统时间。它还支持对本地参考时钟（如无线电控制的时钟）进行管理。

23.1 使用 YaST 配置 NTP 客户端

附于 `ntp` 包中的 NTP 守护程序 (`ntpd`) 预设置为使用本地计算机时钟作为时间参考。但是，请只在没有更精确的时间源的情况下才使用硬件时钟。YaST 为 NTP 客户端的配置提供方便。

23.1.1 基本配置

YaST NTP 客户端配置（*网络服务 > NTP 配置*）由选项卡组成。在*常规设置*选项卡上设置 `ntpd` 启动模式和要查询的服务器。

仅手工

如果您想手动启动 ntpd 守护程序，请选择仅手动。

立即和引导时

选择立即和引导时可在引导系统时自动启动 ntpd。强烈建议使用此设置。然后按照第 23.1.2 节“更改基本配置”[302]所述配置服务器。

23.1.2 更改基本配置

供客户端查询的服务器和其他时间资源列在常规设置选项卡的下半部分。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端的日志文件。

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：

图 23.1 YaST: NTP 服务器



服务器

在选择下拉列表（请参见图 23.1“YaST: NTP 服务器”[302]）中，确定是使用本地网络（本地 NTP 服务器）中的时间服务器设置时间同步，还是会考虑所在时区（公共 NTP 服务器）的基于因特网的时间服务器设置时间同步。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，用**测试**来测试所选服务器是否可用。**选项**使您可以指定 `ntpd` 的其他选项。

使用**访问控制**选项，您可限制远程计算机通过您的计算机上运行的守护程序所能执行的操作。仅在选中安全设置选项卡（请参见图 23.2 “高级 *NTP* 配置：安全设置”[304]）上的**限制 *NTP* 服务仅用于已配置的服务器**后，才能启用此字段。选项对应于 `/etc/ntp.conf` 中的 `restrict` 子句。例如，`nomodify notrap noquery` 禁止服务器修改计算机的 *NTP* 设置并禁止使用 *NTP* 守护程序的陷阱工具（一种远程事件记录功能）。建议将这些限制用于超出您控制范围的服务器（例如在因特网上）。

有关详细信息，请参见 `/usr/share/doc/packages/ntp-doc`（`ntp-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端。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/ntp-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

如果希望客户端通过广播接收信息，请在此字段中输入应接受来自哪个地址的相应数据包。

图 23.2 高级 NTP 配置：安全设置



在安全设置选项卡（请参见图 23.2“高级 NTP 配置：安全设置”[304]）中，确定 ntpd 是否应在 chroot jail 中启动。默认情况下，在 *Chroot Jail* 中运行 NTP 守护程序是被激活的。当 ntpd 受到攻击时这可以提高安全性，因为这种方式可以防止攻击者危害整个系统。

限制 NTP 服务用于配置过的服务器通过禁止远程计算机查看和修改您计算机的 NTP 设置以及禁止使用用于远程事件记录的陷阱工具，从而增强了系统的安全性。一旦启用，这些限制将适用于所有远程计算机，除非您在常规设置选项卡中针对时间源列表中的个别计算机覆盖了访问控制选项。对于所有其他远程计算机，仅允许查询本地时间。

如果 SuSEfirewall2 处于活动状态（默认），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。

23.2 手动配置网络中的 NTP

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 `rcntp start` 初始化 `ntpd` 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大约需要一个小时的时间。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 机制用作客户端：第一种方法是客户端可以定期从已知服务器查询时间。在存在许多客户端的情况下，这种方法会给服务器带来很高的负荷。第二种方法是客户端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。

23.3 运行时动态时间同步

如果在无网络连接的情况下引导系统，则 `ntpd` 将启动，但是它无法解析在配置文件中设置的时间服务器的 DNS 名称。如果通过加密的 WLAN 使用网络管理器，则可能发生这种情况。

如果希望 `ntpd` 在运行时解析 DNS 名称，则必须设置 `dynamic` 选项。然后，当引导后建立网络时，`ntpd` 将再次查找名称并可以访问时间服务器以获取时间。

手动编辑 `/etc/ntp.conf` 并将 `dynamic` 添加到一个或多个 `server` 项：

```
server ntp.example.com dynamic
```

或使用 YaST 并如下操作：

- 1 在 YaST 中单击 *网络服务 > NTP 配置*。
- 2 选择要配置的服务器。然后单击 *编辑*。
- 3 激活 *选项* 字段并添加 `dynamic`。如果已输入其他选项，请用空格分隔。
- 4 单击 *确定* 关闭编辑对话框。重复之前的步骤以根据需要更改所有服务器。
- 5 最后单击 *确定* 保存设置。

23.4 设置本地参考时钟

软件包 `ntpd` 包含用于连接本地参考时钟的驱动程序。`ntp-doc` 包的文件 `/usr/share/doc/packages/ntp-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 NTP 中，实际配置通过伪 IP 地址实现。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/ntp-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 `ntp-doc` 包之后，可以在目录 `/usr/share/doc/packages/ntp-doc` 中找到 NTP 的文档。文件 `/usr/share/doc/packages/ntp-doc/refclock.html` 提供指向描述驱动程序参数的驱动程序页的链接。

23.5 与外部时间参考 (ETR) 的时钟同步

支持与外部时间参考 (ETR) 时钟同步。外部时间参考每 2^{20} (2 的 20 次幂) 微秒发出一次振荡器信号和同步信号, 以将连接的所有服务器的 TOD 时钟保持同步。

两个 ETR 计算机可以连接到一台计算机。如果时钟偏移超过同步检查容差, 所有 CPU 都会获得一次计算机检查, 表示该时钟已失步。如果发生这种情况, 在该时钟再次同步前, 所有与支持 XRC 的设备进行的 DASD I/O 都将停止。

通过两个 `sysfs` 属性可激活 ETR 支持; 请以 `root` 身份运行下列命令:

```
echo 1 > /sys/devices/system/etr/etr0/online
echo 1 > /sys/devices/system/etr/etr1/online
```


域名系统

需要使用 DNS（域名系统）将域名和主机名解析成 IP 地址。这样，可以将 IP 地址指派给主机名，例如将 192.168.2.100 指派给 jupiter。在设置您自己的名称服务器前，请阅读第 21.3 节“名称解析”[253]中有关 DNS 的一般信息。以下配置示例都涉及到 BIND。

24.1 DNS 术语

区域

域名称空间由一些区域组成。例如，如果您有 example.com，则您的 com 域中会有 example 部分（或区域）。

DNS 服务器

DNS 服务器是维护域的名称和 IP 信息的服务器。主 DNS 服务器可用于主要区域、次要服务器可用于从属区域，不含有任何区域的从属服务器可用于缓存。

主区域 DNS 服务器

主区域包含网络中的所有主机，DNS 服务器主区域储存域中所有主机的最新记录。

从属区域 DNS 服务器

从属区域是主区域的副本。从属区域 DNS 服务器将使用区域传送操作从其主服务器获取区域数据。只要从属区域 DNS 服务器具有有效（没到期）的区域数据，便会对区域作出权威响应。如果从属服务器不能获取区域数据的新副本，它将停止响应区域。

转发器

转发器是您的 DNS 服务器应将无法应答的查询发送到的 DNS 服务器。使用 `netconfig`，以便在一个配置中启用不同配置源（另请参见 `man 8 netconfig`）。

记录

记录就是有关名称和 IP 地址的信息。有关支持的记录及其语法的描述可在 BIND 文档中获取。以下是一些特殊记录：

NS 记录

NS 记录会告诉命名服务器哪些计算机负责给定域区域。

MX 记录

MX（邮件交换）记录描述在因特网中定向邮件时要联系的计算机。

SOA 记录

SOA（起始授权机构）记录是区域文件中的第一条记录。当使用 DNS 在多台计算机之间同步数据时，使用 SOA 记录。

24.2 安装

要安装 NFS 服务器，请启动 YaST 并选择 **软件 > 软件管理**。选择 **视图 > 模式**，然后选择 *DHCP* 和 *DNS 服务器*。确认安装相关的包来完成安装进程。

24.3 用 YaST 配置

使用 YaST DNS 模块为本地网络配置 DNS 服务器。第一次启动此模块时，会启动向导，提示您做出一些有关服务器管理的决定。完成此初始设置后，将产生基本服务器配置。使用专家模式可处理更高级的配置任务，例如设置 ACL、日志记录、TSIG 密钥和其他选项。

24.3.1 向导配置

向导由三个步骤或对话框组成。您可以在对话框的适当位置进入专家配置方式。

- 1 第一次启动模块时，您将看到图 24.1 “DNS 服务器安装：转发器设置” [311]中显示的转发器设置对话框将打开。*Netconfig DNS* 策略确定应提供转发器的设备或您是否希望自己提供转发器列表。有关 *netconfig* 的更多信息，请参见 `man 8 netconfig`。

图 24.1 DNS 服务器安装：转发器设置

DNS 服务器安装: 转发器设置

☐ PPP 守护程序设置转发器

☒ 手动设置转发器(M)

添加 IP 地址

IP 地址(D):

192.168.27.1

添加(A)

转发器列表(L)

192.168.27.1

删除(D)

取消(C)

下一步(N)

转发器是接收您的 DNS 服务器自己无法应答的查询的 DNS 服务器。输入它们的 IP 地址，然后单击添加。

- 2 *DNS* 区域对话框由多个部分组成，负责管理区域文件（如第 24.6 节“区域文件” [326]中所述）。对于新区域，请在名称中为其提供一个名称。要添加反向区域，名称必须以 `.in-addr.arpa` 结尾。最后选择类型（主、从属或转发）。参见图 24.2 “DNS 服务器安装：DNS 区域” [312]。单击编辑可配置现有区域的其他设置。要删除区域，请单击删除。

图 24.2 DNS 服务器安装: DNS 区域

DNS 服务器安装: DNS 区域

添加新区域(D)

名字	类型
example.com	主

添加(A)

已配置的 DNS 区域

区域	类型
example.com	主

删除(D)

编辑(E)

后退(B) 中止(R) 下一步(N)

- 3 在最后对话框中，您可以通过单击 **打开防火墙中的端口** 打开防火墙中的 DNS 端口。然后决定是否在引导时启动 DNS 服务器（**开启**或**关闭**）。您还可以激活 LDAP 支持。请参见图 24.3 “DNS 服务器安装: 完成向导” [313]。

图 24.3 DNS 服务器安装：完成向导

DNS 服务器安装: 完成向导

☐ 打开防火墙中的端口(F)

防火墙细节(D)

防火墙已禁用

☐ LDAP 支持处于活动状态(L)

启动行为

☐ 打开(N): 立即启动和在引导时

☒ 关闭(F): 仅手动启动

• 转发器:

• 域: .. localhost, 0.0.127.in-addr.arpa, example.com

DNS 服务器专家配置(E)...

后退(B)

中止(R)

完成(F)

24.3.2 专家配置

启动此模块后，YaST将打开一个窗口，其中显示了多个配置选项。完成此窗口会生成具有基本功能的 DNS 服务器配置：

24.3.2.1 币筐

在启动下，定义是要在引导系统时启动 DNS 服务器，还是手动启动 DNS 服务器。要立即启动 DNS 服务器，请单击立即启动 DNS 服务器。要停止 DNS 服务器，请单击立即停止 DNS 服务器。要保存当前设置，请选择保存设置并立即重新装载 DNS 服务器。您可以用打开防火墙中的端口打开防火墙中的 DNS 端口，并用防火墙细节修改防火墙设置。

通过选择 *LDAP* 支持处于活动状态，让 *LDAP* 数据库管理区域文件。重新启动 *DNS* 服务器或提示重装载其配置时，*DNS* 服务器将立刻挑选出写入到 *LDAP* 数据库的任何区域数据更改。

24.3.2.2 转发器

如果您的本地 *DNS* 服务器无法应答请求，则会尝试将请求转发给转发器（如果进行了这样的配置）。转发器可手动添加到转发器列表。如果在拨号连接中转发器不是静态的，则 *netconfig* 会处理配置。有关 *netconfig* 的更多信息，请参见 `man 8 netconfig`。

24.3.2.3 基本选项

在这一部分，设置基本的服务器选项。从选项菜单中，选择所需的项，然后在相应输入字段中指定值。选择添加包括新的条目。

24.3.2.4 日志记录

要设置 *DNS* 服务器应该记录的内容和记录方法，请选择 *日志记录*。在 *日志类型* 下，指定 *DNS* 服务器将日志数据写入的位置。选择系统日志来使用系统级日志文件 `/var/log/messages`，或选择文件来指定另一个文件。对于后者，请额外指定一个名称、最大文件大小（以兆字节为单位）以及要储存的日志文件版本数。

在附加日志记录下可以使用其他一些选项。启用 *记录所有的 DNS 查询* 将记录每个查询，在这种情况下，日志文件可能会变得非常大。出于这个原因，如果不是为了调试，则最好不要启用此选项。要记录区域更新期间 *DHCP* 和 *DNS* 服务器之间的通讯数据，请启用 *记录区域更新*。要记录将区域从主服务器传送到从属服务器期间的数据流量，请启用 *记录区域传送*。请参见图 24.4 “*DNS* 服务器：日志记录” [315]。

图 24.4 DNS 服务器：日志记录



24.3.2.5 ACL

使用此对话框定义 ACL（访问控制列表）来强制执行访问限制。在名称下提供不同的名称后，在值下指定具有下列形式的IP地址（带有或不带有网络掩码）：

```
{ 192.168.1/24; }
```

配置文件的语法要求地址以分号结尾且放在花括号中。

24.3.2.6 TSIG 密钥

TSIG（事务签名）的主要用途是保护 DHCP 和 DNS 服务器间通讯的安全性。这些内容在第 24.8 节“安全事务”[330]中有所介绍。

要生成 TSIG 密钥，请在标为密钥 ID 的字段中输入一个唯一名称，并指定储存密钥的文件（文件名）。用生成确认选择。

要使用以前创建的密钥，请将密钥 ID 字段保留为空，并在文件名下选择储存这个密钥 ID 的文件。选择后，请用添加按钮进行确认。

24.3.2.7 DNS 区域（添加从属区域）

要添加从属区域，请选择 *DNS 区域*，然后选择区域类型从属，写入新区域名称并单击添加。

在主 *DNS 服务器 IP* 下的区域编辑器子对话框中，指定从属服务器将从中获取数据的主服务器。要限制对此服务器的访问，可从列表选择一个 ACL。

24.3.2.8 DNS 区域（添加主区域）

要添加主区域，请选择 *DNS 区域*，然后选择区域类型主，写入新区域名称并单击添加。当添加主区域时，也需要一个反向区域。例如，当添加区域 `example.com`（指向子集 `192.168.1.0/24` 中的主机）时，也应为包含的 IP 地址范围添加一个反时向区域。按照定义，应命名为 `1.168.192.in-addr.arpa`。

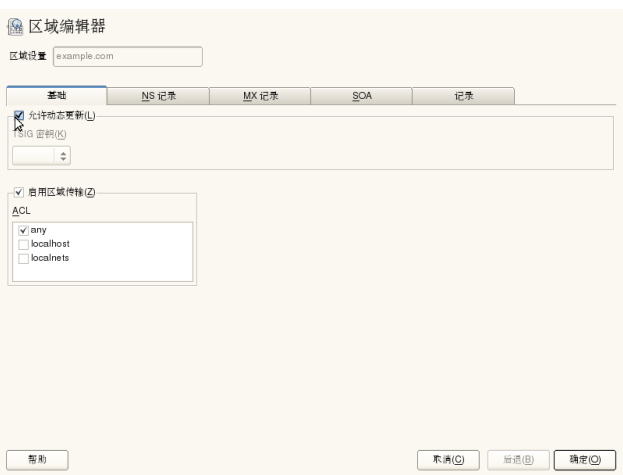
24.3.2.9 DNS 区域（编辑主区域）

要编辑主区域，请选择 *DNS 区域*，从表中选择主区域，最后单击编辑。该对话框包含几个页面：基本（第一个打开的页面）、*NS 记录*、*MX 记录*、*SOA* 和记录。

图 24.5 “DNS 服务器：区域编辑器（基本）”[317]中显示的基本对话框用于定义动态 DNS 的设置以及指向客户端和从属名称服务器的区域传送的访问选项。要允许动态更新区域，请选择允许动态更新及相应的 TSIG 密钥。必须在更新操作开始前定义密钥。要启用区域传送，请选择相应的 ACL。必须已经定义了 ACL。

在基本对话框中，选择是否启用区域传输。使用所列 ACL 来定义谁能够下载区域。

图 24.5 DNS 服务器：区域编辑器（基本）



区域编辑器（NS 记录）

*NS 记录*对话框用于为指定的区域定义备用名称服务器。确保已将自己的名称服务器包括在列表中。要添加记录，请在要添加的名称服务器下输入其名称，然后用*添加*按钮确认。请参见图 24.6 “DNS 服务器：区域编辑器（NS 记录）” [318]。

图 24.6 DNS 服务器：区域编辑器（NS 记录）

区域编辑器（MX 记录）

要将当前区域的邮件服务器添加到现有的列表中，请输入相应的地址和优先级值。执行完此操作后，请选择**添加**进行确认。请参见图 24.7 “DNS 服务器：区域编辑器（MX 记录）” [319]。

图 24.7 DNS 服务器：区域编辑器（MX 记录）

区域编辑器

区域设置example.com

基础NS 记录MX 记录SOA记录

要添加的邮件服务器

地址(A)

优先级(P)

0

添加(A)

邮件中继列表

邮件服务器	优先级
-------	-----

删除(D)

取消(C)

中止(B)

确定(O)

区域编辑器 (SOA)

此页用于创建 SOA（起始授权机构）记录。有关各选项的描述，请参见例 24.6 “/var/lib/named/example.com.zone 文件” [326]。通过 LDAP 管理的动态区域不支持更改 SOA 记录。

图 24.8 DNS 服务器：区域编辑器 (SOA)

区域编辑器

区域设置example.com

基础NS 记录MX 记录SOA记录

序列(A)
2008100700

刷新(E)
3
单元(U)
小时

TTL(L)
2
单元(U)
天

重试(Y)
1
单元(U)
小时

失效时间(D)
1
单元(M)
周

最小值(M)
1
单元(D)
天

取消(C)

中止(B)

确定(O)

区域编辑器（记录）

此对话框用于管理名称解析。在*记录密钥*中，输入主机名并选择其类型。*A* 记录表示主要项。此项的值应为一个 IP 地址。*CNAME* 是别名。对于要根据 *NS* 记录和 *MX* 记录选项卡中提供的信息而扩展的详细或部分记录，应使用类型 *NS* 和 *MX*。这三种类型解析为现有的 *A* 记录。*PTR* 用于反向区域。它与 *A* 记录相反，例如：

```
hostname.example.com. IN A 192.168.0.1
1.0.168.192.in-addr.arpa IN PTR hostname.example.com.
```

注意：编辑反向区域

添加正向区域后，返回到主菜单并选择该反向区域以进行编辑。在选项卡*基础*中激活复选框*自动生成记录的区域*，然后选择正向区域。这样，对正向区域的所有更改都会反向区域中更新。

24.4 启动 BIND 名称服务器

在 SUSE® Linux Enterprise Server 系统上，已预配置名称服务器 BIND（*Berkeley* 因特网名称域），因此可以在安装后立即启动此名称服务器而不会出现任何问题。如果您已有一个有效的因特网连接并在 `/etc/resolv.conf` 中输入了 `127.0.0.1` 作为 `localhost` 的名称服务器地址，那么您已经在使用名称解析功能了，而不需要知道提供商的 DNS。BIND 通过 `root` 名称服务器执行名称解析，这个过程非常慢。通常，应将提供商的 DNS 及其 IP 地址输入配置文件 `/etc/named.conf` 的 `forwarders` 下，以确保能进行有效而安全的名称解析。如果到目前为止是这种情况，则该名称服务器将作为仅用于缓存的纯名称服务器运行。只有在配置了该名称服务器自己的区域后，它才能成为正确的 DNS。在 `/usr/share/doc/packages/bind/config` 中可找到简单的示例。

提示：名称服务器信息的自动适应

根据因特网连接或网络连接的类型，名称服务器信息可以自动适应当前的情况。要执行此操作，将 `/etc/sysconfig/network/config` 文件中的 `NETCONFIG_DNS_POLICY` 变量设置为自动。

但是不要设置正式域，而是让负责机构指派给您。即使您有自己的域且提供商管理此域，也最好不要使用此域，因为如果使用此域，BIND 将不转发对此域的请求。例如，此域不能访问提供商的 Web 服务器。

要启动名称服务器，请以 `root` 用户身份输入命令 `rcnamed start`。如果右侧出现绿色的“完成”，则说明已成功启动名为 `named` 的名称服务器进程。请用 `host` 或 `dig` 程序立即在本地系统上测试名称服务器，该测试应返回 `localhost` 作为默认服务器，地址为 `127.0.0.1`。如果未返回所需的结果，则 `/etc/resolv.conf` 可能包含不正确的名称服务器项或此文件根本不存在。如果是第一次测试，请输入 `host 127.0.0.1`，此命令应始终有效。如果收到错误消息，请使用 `rcnamed status` 查看服务器是否确实在运行。如果名称服务器未启动或出现意外的行为，则通常可以在日志文件 `/var/log/messages` 中找到原因。

要将提供商的名称服务器（或网络上正在运行的名称服务器）用作转发器，请在 `options` 部分的 `forwarders` 下输入相应的一个或多个 IP 地址。例 24.1 “`named.conf` 中的转发选项” [322] 中包含的地址仅用作示例。请根据您的设置调整这些项。

例 24.1 *named.conf* 中的转发选项

```
options {
    directory "/var/lib/named";
    forwarders { 10.11.12.13; 10.11.12.14; };
    listen-on { 127.0.0.1; 192.168.1.116; };
    allow-query { 127/8; 192.168/16 };
    notify no;
};
```

`options` 项后跟区域的项 `localhost` 和 `0.0.127.in-addr.arpa`。“.”下的 `type hint` 项应始终存在。无需修改相应的文件，应照原样使用。还要确保每个项都以“;”结束，同时确保花括号位于正确的位置。在更改配置文件 `/etc/named.conf` 或区域文件后，通知 BIND 使用 `rcnamed reload` 重新读取这些文件。用 `rcnamed restart` 停止并重启动名称服务器也会获得相同的效果。输入 `rcnamed stop` 可以随时停止服务器。

24.5 */etc/named.conf* 配置文件

BIND 名称服务器本身的所有设置都储存在文件 `/etc/named.conf` 中。但是，将要处理的域的区域数据（由主机名、IP 地址等组成）储存在目录 `/var/lib/named` 下单独的文件中。稍后将介绍其详细信息。

`/etc/named.conf` 大致分为两部分。一部分是存放常规设置的 `options` 部分，另一部分由各个域的 `zone` 项组成。而 `logging` 部分和 `acl`（访问控制列表）项是可选的。注释行以 `#` 符号或 `//` 开头。例 24.2 “基本的 `/etc/named.conf`” [322]显示了一个最小的 `/etc/named.conf`。

例 24.2 基本的 */etc/named.conf*

```
options {
    directory "/var/lib/named";
    forwarders { 10.0.0.1; };
    notify no;
};

zone "localhost" in {
    type master;
    file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "127.0.0.zone";
};
```

```
zone "." in {  
    type hint;  
    file "root.hint";  
};
```

24.5.1 重要的配置选项

`directory "filename";`

指定目录，BIND 可以在该目录中找到包含区域数据的文件。通常，此目录是 `/var/lib/named`。

`forwarders { ip-address; };`

指定在无法直接解析 DNS 请求的情况下应将其转发到的名称服务器（大多数情况下是提供商的名称服务器）。将 `ip-address` 替换为 IP 地址，如 `192.168.1.116`。

`forward first;`

在尝试通过 root 名称服务器解析 DNS 请求前，对 DNS 请求进行转发。可以写入 `forward only`（而不是 `forward first`）转发所有请求并且不将任何请求发送到 root 名称服务器。这可以用于防火墙配置。

`listen-on port 53 { 127.0.0.1; IP 地址; };`

指示 BIND 通过哪些网络接口和哪个端口来接受客户端查询。不需要显式指定 `port 53`，因为 53 是默认端口。输入 `127.0.0.1` 允许接收来自 Localhost 的请求。如果完全省略此项，则在默认情况下使用所有接口。

`listen-on-v6 port 53 {any; };`

指示 BIND 应通过哪个端口侦听 IPv6 客户端请求。唯一可以替代 `any` 的是 `none`。就 IPv6 而言，服务器只接受通配符地址。

`query-source address * port 53;`

如果防火墙阻止外发的 DNS 请求，则需要此项。此项指示 BIND 从端口 53 向外部发送请求，而不使用端口号大于 1024 的任何端口。

`query-source-v6 address * port 53;`

指示 BIND 将哪个端口用于 IPv6 查询。

`allow-query { 127.0.0.1; net; };`

定义客户端可以自此发送 DNS 请求的网络。将 *net* 替换为地址信息，如 `192.168.2.0/24`。末尾的 `/24` 是网络掩码的缩写表示（在本例中为 `255.255.255.0`）。

`allow-transfer !*;;`

控制哪些主机可以请求区域传送。在本例中，用 `! *`。如果没有此项，则可以从没有限制的任何位置请求区域传送。

`statistics-interval 0;`

如果缺少此项，则 BIND 每小时在 `/var/log/messages` 中生成几行统计信息。将其设置为 `0` 可以完全禁止生成此类统计信息，也可以设置时间间隔（以分钟为单位）。

`cleaning-interval 720;`

此选项定义 BIND 间隔多长时间清除其缓存。每次出现此选项都会在 `/var/log/messages` 中触发一项。时间是以分钟为单位指定的。默认值为 `60` 分钟。

`interface-interval 0;`

BIND 定期在网络接口中搜索新接口或不存在的接口。如果将该值设置为 `0`，则不执行搜索，BIND 只侦听启动时检测到的接口。否则，采用分钟定义时间间隔。默认值是 `60` 分钟。

`notify no;`

指定 `no` 将阻止其他名称服务器在区域数据被更改或名称服务器被重启时得到通知。

有关可用选项的列表，请阅读手册页 `man 5 named.conf`。

24.5.2 日志记录

可以在 BIND 中详细配置日志记录的内容、方式和位置。通常，默认设置就已足够。例 24.3 “禁用日志记录的项” [325] 显示了此项最简单的形式，并完全抑制任何日志记录。

例 24.3 禁用日志记录的项

```
logging {  
    category default { null; };  
};
```

24.5.3 区域项

例 24.4 *example.com* 的区域项

```
zone "example.com" in {  
    type master;  
    file "example.com.zone";  
    notify no;  
};
```

在 `zone` 后，指定要管理的域的名称 (`example.com`)，后跟 `in` 和用花括号括起来的相关选项块，如例 24.4 “*example.com* 的区域项” [325] 所示。要定义从属区域，请将 `type` 切换为 `slave` 并将管理此区域的名称服务器指定为 `master`（它可能是另一个主区域的从属区域），如例 24.5 “*example.net* 的区域项” [325] 所示。

例 24.5 *example.net* 的区域项

```
zone "example.net" in {  
    type slave;  
    file "slave/example.net.zone";  
    masters { 10.0.0.1; };  
};
```

区域选项：

`type master;`

通过指定 `master`，指示 BIND 由本地名称服务器对区域进行处理。这假定已用正确的格式创建了区域文件。

`type slave;`

从另一个名称服务器传送此区域。必须将它与 `masters` 一起使用。

`type hint;`

区域 `.`（`hint` 类型）用于设置 `root` 名称服务器。此区域定义可以保留原样。

文件 `example.com.zone` 或文件 “`slave/example.net.zone`”；

此项指定域的区域数据所在的文件。从属区域不需要此文件，因为此数据是从另一个名称服务器中获取的。要区分主文件和从属文件，请对从属文件使用目录 `slave`。

```
masters { server-ip-address; };
```

只有从属区域需要此项。它指定应从哪个名称服务器传送区域文件。

```
allow-update {! *; };
```

此选项控制外部写访问，这将允许客户端创建 DNS 项 — 出于安全原因，通常不希望出现这种情况。没有此项，就不允许进行区域更新。上述项可以实现相同的结果，因为 `! *` 有效地禁止了此类操作。

24.6 区域文件

所需的区域文件有两种类型。一种类型是将 IP 地址指派给主机名，另一种类型则正相反：为 IP 地址提供主机名。

提示：在区域文件中使用点（句点）

此 “.” 在区域文件中有重要的含义。如果给出主机名而末尾没有加 .，则会追加区域。通过完整域名指定的完整主机名必须以 . 结尾，避免再将域添加到主机名上。“.” 丢失或放错位置可能是名称服务器配置出错最常见的原因。

首先研究以下区域文件 `example.com.zone`，该区域文件负责域 `example.com`，如例 24.6 “`/var/lib/named/example.com.zone` 文件” [326]所示。

例 24.6 `/var/lib/named/example.com.zone` 文件

```
1. $TTL 2D
2. example.com. IN SOA      dns root.example.com. (
3.                  2003072441 ; serial
4.                  1D        ; refresh
5.                  2H        ; retry
6.                  1W        ; expiry
7.                  2D )      ; minimum
8.
9.                  IN NS     dns
10.                  IN MX    10 mail
11.
12. gate            IN A      192.168.5.1
13.                IN A      10.0.0.1
```



```

14. dns          IN A          192.168.1.116
15. mail         IN A          192.168.3.108
16. jupiter     IN A          192.168.2.100
17. venus       IN A          192.168.2.101
18. saturn      IN A          192.168.2.102
19. mercury     IN A          192.168.2.103
20. ntp         IN CNAME     dns
21. dns6        IN A6      0      2002:c0a8:174::

```

第 1 行:

\$TTL 定义默认存活时间，它适用于此文件中的所有项。在本例中，项在两天 (2 D) 内有效。

第 2 行:

这是 SOA (Start Of Authority, 起始授权机构) 控制记录开始的位置:

- 在第一个位置，要管理的域的名称是 `example.com`。此域名以“.”结尾，否则可能会再次追加区域。或者，可以在这里输入 `@`，在这种情况下，可以从 `/etc/named.conf` 中的相应项中抽取区域。
- IN SOA 之后是用作此区域主服务器的名称服务器的名称。此名称从 `dns` 扩展为 `dns.example.com`，因为它没有以“.”结尾。
- 随后是负责此名称服务器的用户的电子邮件地址。因为 `@` 符号已经有特殊含义，所以在这里改为输入“.”。对于 `root@example.com`，该项必须显示为类似 `root.example.com`。此“.”必须包含在末尾，以防止添加区域。
- (和) 之间包含的所有行组成 SOA 记录。

第 3 行:

serial number 可以是任一数字，每次更改此文件时此数字都会增加。需要将这些更改通知给辅助名称服务器 (从属服务器)。为此，日期和运行数字常采用 10 位数字格式，书写方式为 YYYYMMDDNN，这已成为惯用格式。

第 4 行:

refresh rate 指定二级名称服务器校验区域 serial number 的时间间隔。在本例中，此时间间隔为一天。

第 5 行:

`retry rate` 指定二级名称服务器在出现错误时尝试再次联系主服务器的时间间隔。这里的时间间隔是两小时。

第 6 行:

`expiration time` 指定二级名称服务器在无法重新联系上主服务器时将在多长时间后丢弃缓存的数据。在本例中为一周。

第 7 行:

SOA 记录中的最后一项指定 `negative caching TTL` — 缓存来自其他服务器的未解析 DNS 查询结果的时间。

第 9 行:

`IN NS` 指定负责此域的名称服务器。`dns` 扩展为 `dns.example.com`, 因为它没有以 `"."` 结尾。可以有多个与此行类似的行 — 一行用于主名称服务器, 其他各行分别用于每个二级名称服务器。如果 `/etc/named.conf` 中未将 `notify` 设置为 `no`, 则会将区域数据的更改通知给这里列出的所有名称服务器。

第 10 行:

`MX` 记录指定接受、处理和转发域 `example.com` 的电子邮件的邮件服务器。在本例中, 邮件服务器是主机 `mail.example.com`。主机名称前面的数字是优先顺序值。如果有多个 `MX` 项, 则首先采用具有最小值的邮件服务器, 如果向此服务器递送邮件失败, 则尝试采用具有稍大一些值的邮件服务器。

第 12–19 行:

这些都是实际的地址记录, 在这里将一个或多个 IP 地址指派到主机名。名称在此处列出, 不带 `"."`, 因为这些名称不包含自己的域, 因此会将 `example.com` 添加到所有名称。因为主机 `gate` 有两个网卡, 所以为其指派两个 IP 地址。只要主机地址是传统地址 (IPv4), 就将使用 `A` 标记该记录。如果地址是 IPv6 地址, 则使用 `AAAA` 标记此项。

注意: IPv6 语法

IPv6 记录与 IPv4 记录的语法稍有不同。由于可能进行碎片整理, 所以需要在寻址前提供有关缺失位的信息。要仅使用所需数目的 “0” 填写 IPv6 地址, 请在地址中的正确位置添加两个冒号。

```
pluto      AAAA 2345:00C1:CA11::1234:5678:9ABC:DEF0
pluto      AAAA 2345:00D2:DA11::1234:5678:9ABC:DEF0
```

第 20 行：
别名 ntp 可用于解决 dns（CNAME 表示 规范名称）。

伪域 in-addr.arpa 用于 IP 地址到主机名的反向查找。它被追加到采用反向表示法的地址的网络部分。因此，将 192.168 解析成 168.192.in-addr.arpa。参见 例 24.7 “反向查找” [329]。

例 24.7 反向查找

```
1. $TTL 2D
2. 168.192.in-addr.arpa.    IN SOA dns.example.com. root.example.com. (
3.                          2003072441      ; serial
4.                          1D              ; refresh
5.                          2H              ; retry
6.                          1W              ; expiry
7.                          2D )            ; minimum
8.
9.                          IN NS          dns.example.com.
10.
11. 1.5                     IN PTR         gate.example.com.
12. 100.3                   IN PTR         www.example.com.
13. 253.2                   IN PTR         cups.example.com.
```

第 1 行：
\$TTL 定义应用于此处所有项的标准 TTL。

第 2 行：
此配置文件应激活网络 192.168 的反向查找。由于 区域名为 168.192.in-addr.arpa，因此不应添加到主机名中。因此，所有主机名都以完整格式输入 — 带有域并以 "." 结尾。其余的项对应于上一个 example.com 示例介绍的那些内容。

第 3–7 行：
请参见关于 example.com 的上一个示例。

第 9 行：
此行也是指定负责此区域的名称服务器。但这次采用完整形式输入名称，带有域且末尾带有 "."。

第 11–13 行：

这些都是提示各自主机上 IP 地址的指针记录。只在行的开头输入 IP 地址的最后一部分，在末尾不加“.”。将区域追加到这个地址（不带 `.in-addr.arpa`）将产生采用反向顺序的完整 IP 地址。

通常，可以在 BIND 的不同版本间传输区域，不会产生任何问题。

24.7 区域数据的动态更新

术语*动态更新*指添加、更改或删除主服务器区域文件中的项的操作。RFC 2136 对此机制进行了介绍。通过添加可选的 `allow-update` 或 `update-policy` 规则，可以为每个区域项单独配置动态更新。不应手动编辑要动态更新的区域。

用命令 `nsupdate` 将要更新的项传送到服务器。有关此命令的精确语法，请查看关于 `nsupdate` 的手册页 (`man 8 nsupdate`)。出于安全原因，应使用第 24.8 节“安全事务”[330] 中介绍的 TSIG 密钥执行此类更新。

24.8 安全事务

借助于基于共享密钥（也称为 TSIG 密钥）的事务签名 (TSIG) 可以实现安全事务。本节介绍如何生成和使用此类密钥。

不同服务器间的通信和区域数据的动态更新需要安全事务。依靠密钥进行访问控制比只靠 IP 地址进行访问控制要安全得多。

使用下列命令生成 TSIG 密钥（有关细节，请参见 `man dnssec-keygen`）：

```
dnssec-keygen -a hmac-md5 -b 128 -n HOST host1-host2
```

此命令创建两个文件，名称与下面的名称类似：

```
Khost1-host2.+157+34265.private Khost1-host2.+157+34265.key
```

密钥本身（类似于 `ejIkuCyyGJwwuN3xAteKgg==` 的字符串）位于这两个文件中。要将密钥用于事务，必须将第二个文件 (`Khost1-host2.+157+34265.key`) 传送到远程主机，而且最好采用安全的方式（例如，使用 `scp`）传送。在远程服务器上，密钥必须包括在文件 `/etc/named.conf` 中以实现 `host1` 和 `host2` 之间的安全通信：

```
key host1-host2 {
    algorithm hmac-md5;
    secret "ejIkuCyyGJwwuN3xAteKgg==";
};
```

警告：/etc/named.conf 的文件权限

确保正确限制了 /etc/named.conf 的权限。此文件的默认值是 0640，拥有者为 root 和组 named。或者，可以将密钥移到具有特殊限制权限的另一个文件中，然后将该文件包括在 /etc/named.conf 中。要包括外部文件，请使用：

```
include "filename"
```

用带有密钥的文件的绝对路径替换 filename。

要使服务器 host1 能使用 host2（在本例中，其地址为 10.1.2.3）的密钥，服务器的 /etc/named.conf 必须包含下列规则：

```
server 10.1.2.3 {
    keys { host1-host2. };
};
```

必须将类似的项包括在 host2 的配置文件中。

向为 IP 地址和地址范围定义的任何 ACL（访问控制列表，请不要与文件系统的 ACL 混淆）添加 TSIG 密钥可以实现事务安全性。相应的项如下所示：

```
allow-update { key host1-host2. };
```

BIND 管理员参考手册的 update-policy 对此主题进行了详细介绍。

24.9 DNS 安全性

RFC 2535 中介绍了 DNSSEC（即 DNS 安全性）。BIND 手册讨论了可用于 DNSSEC 的工具。

被认为是安全的区域必须有一个或多个与之关联的区域密钥。这些密钥是通过 dnssec-keygen 生成的，就像主机密钥一样。当前使用 DSA 加密算法来生成这些密钥。应使用 \$INCLUDE 规则将所生成的公共密钥包括在相应的区域文件中。

使用命令 `dnssec-signzone`，您可以创建生成的密钥集（`keyset-` 文件），将它们以安全方式传送到父区域并加以签名。这会生成要包含在 `/etc/named.conf` 中的针对每个区域的文件。

24.10 更多信息

有关其他信息，请参见安装在 `/usr/share/doc/packages/bind` 下的包 `bind-doc` 中的 *BIND Administrator Reference Manual*（BIND 管理员参考手册）。另外，请考虑参考该手册中所引用的 RFC 和 BIND 附带的手册页。`/usr/share/doc/packages/bind/README.SuSE` 包含有关 SUSE Linux Enterprise Server 中的 BIND 的最新信息。

DHCP

动态主机配置协议 (DHCP) 用于从服务器集中指派网络设置，而不必在每个工作站本地逐一配置这些设置。被配置为使用 DHCP 的主机不能控制它自己的静态地址。DHCP 使它能够根据服务器的指示完全且自动地对自身进行配置。如果在客户端使用 NetworkManager，则根本无需配置客户端。在更改了环境并且一次只能使用一个活动的接口时，它才有用。请勿在运行 DHCP 服务器的计算机上使用 NetworkManager。

提示：IBM System z：DHCP 支持

在 IBM System z 平台上，DHCP 仅在使用 OSA 和 OSA Express 网卡的接口上工作。现在只有这些网卡具有 MAC，因为需要 MAC 来实现 DHCP 自动配置功能。

配置 DHCP 服务器的方法之一是使用网卡的硬件地址（在大多数情况下应是固定的）来标识每个客户端，然后在客户端每次连接到服务器时为其提供相同的设置。另一种方法是对 DHCP 进行配置，从为此设置的地址池来为每个相关客户端动态指派地址。在后一种情况下，DHCP 服务器每次在收到客户端请求时都会尝试向它指派相同的地址，即使相隔较长的时间也是如此。只有在网络中包含的客户端数不超过地址数时，它才生效。

DHCP 简化了系统管理员的工作。与地址和网络配置相关的任何更改（甚至是较大的更改）一般都可以通过编辑服务器的配置文件来集中完成。这比重配置众多工作站要方便得多。此外，还可以更方便地将计算机（尤其是新计算机）集成到网络中，因为现在可以从池中为它们指派 IP 地址。如果经常在不同的网络中使用便携式计算机，则从 DHCP 服务器检索适当的网络设置特别有用。

在本章中，DHCP 服务器将在工作站所在的子网内运行，即 192.168.2.0/24（网关为 192.168.2.1）。它具有固定的 IP 地址 192.168.2.254，并提供两个地址范围：192.168.2.10 至 192.168.2.20 以及 192.168.2.100 至 192.168.2.200。

DHCP 服务器不仅提供 IP 地址和网络掩码，还提供客户端要使用的主机名、域名、网关和名称服务器地址。此外，DHCP 还允许您集中配置许多其他参数，例如客户端可能从中巡回检测当前时间的时间服务器，甚至是打印服务器。

25.1 使用 YaST 配置 DHCP 服务器

要安装 DHCP 服务器，请启动 YaST 并选择 **软件 > 软件管理**。选择 **过滤器 > 模式**，然后选择 **DHCP 和 DNS 服务器**。确认安装相关的包来完成安装进程。

重要：LDAP 支持

可以将 YaST DHCP 模块设置为本地储存服务器配置（在运行 DHCP 服务器的主机上），或使其配置数据由 LDAP 服务器管理。如果要使用 LDAP，请在配置 DHCP 服务器前设置 LDAP 环境。

有关 LDAP 的更多信息，请参见第 4 章 *LDAP—A Directory Service*（[↑安全指南](#)）。


使用 YaST DHCP 模块 (`yast2-dhcp-server`) 可设置自己的用于本地网络的 DHCP 服务器。此模块能以向导模式或专家配置模式运行。

25.1.1 初始配置（向导）

第一次启动此模块时，向导启动，提示您做出一些有关服务器管理的基本决定。完成此初始设置将生成一个非常基本的服务器配置，此配置可以使服务器在各基本方面正常工作。专家方式可用于处理更高级的配置任务。按如下所示继续：

- 1 从该列表中选择 DHCP 服务器应侦听的接口，然后单击 **选择**。随后，请选择 **针对所选接口打开防火墙** 打开此接口的防火墙，单击 **下一步**。请参见图 25.1 “DHCP 服务器：卡选择” [335]。

图 25.1 DHCP 服务器：卡选择

 DHCP 服务器向导 (第 1 步/共 4 步): 卡选择

DHCP 服务器的网卡

已选择	接口名	设备名	IP
x	br0	DHCP 地址	
	br1	DHCP 地址	
	ib1	DHCP 地址	

选择(S)

取消选择(D)

☒ 针对所选接口打开防火墙(F)

帮助

中止(B)

后退(B)

下一步(N)

- 2 使用此复选框来确定是否由 LDAP 服务器自动储存您的 DHCP 设置。在输入字段中，提供 DHCP 服务器应管理的所有客户端的网络细节。这些细节包括域名、时间服务器地址、主名称服务器和二级名称服务器的地址、打印和 WINS 服务器的地址（对于同时包含 Windows 和 Linux 客户端的混合网络）、网关地址和租用时间。请参见图 25.2 “DHCP 服务器：全局设置” [336]。

图 25.2 DHCP 服务器：全局设置

DHCP 服务器向导 (第 2 步/共 4 步): 全局设置

☐

LDAP 支持

DHCP 服务器名称 (可选)

域名(D)

example.com

主名称服务器 IP

192.168.1.116

二级名称服务器 IP(S)

默认网关(路由器)(G)

192.168.2.1

NTP 时间服务器(T)

192.168.1.116

打印服务器(P)

WINS 服务器(W)

192.168.1.110

默认租用时间(L)

4

单位(U)

小时

帮助

中止(B)

后退(B)

下一步(N)

3 配置如何为客户端指派动态 IP 地址。为此，应首先指定服务器为 DHCP 客户端指派地址时使用的 IP 范围。所有这些地址必须由同一个网络掩码来覆盖。还要指定租用时间，在此期间客户端可以保留它的 IP 地址，而无需请求续期。（可选）指定最长租用时间 — 这是服务器为特定客户端保留某个 IP 地址的时间。请参见图 25.3 “DHCP 服务器：动态 DHCP” [337]。

336 管理指南

图 25.3 DHCP 服务器：动态 DHCP

 DHCP 服务器向导 (第 3 步/共 4 步): 动态 DHCP

子网信息

当前网络(N)

172.22.0.0

当前网络掩码(M)

255.255.0.0

掩码位(I)

16

最小 IP 地址(I)

172.22.0.1

最大 IP 地址(X)

172.22.255.254

IP 地址范围

第一个 IP 地址(F)

192.168.2.100

最后一个 IP 地址(L)

192.168.2.128

☐ 允许动态 BOOTP(B)

租用时间

默认值(D)

4

单位(U)

小时

最大值(M)

2

单位(T)

天

同步 DNS 服务器(S)... ~

帮助

中止(B)

后退(B)

下一步(N)

4 定义 DHCP 服务器应如何启动。指定 DHCP 服务器是在引导系统时自动启动还是在需要时（例如进行测试时）手动启动。单击完成以完成对服务器的配置。请参见图 25.4 “DHCP 服务器：启动” [337]。

图 25.4 DHCP 服务器：启动

 DHCP 服务器向导 (第 4 步/共 4 步): 启动

启动服务

☒ 引导时(B)

☐ 手动(M)

DHCP 服务器专家配置(E)...

帮助

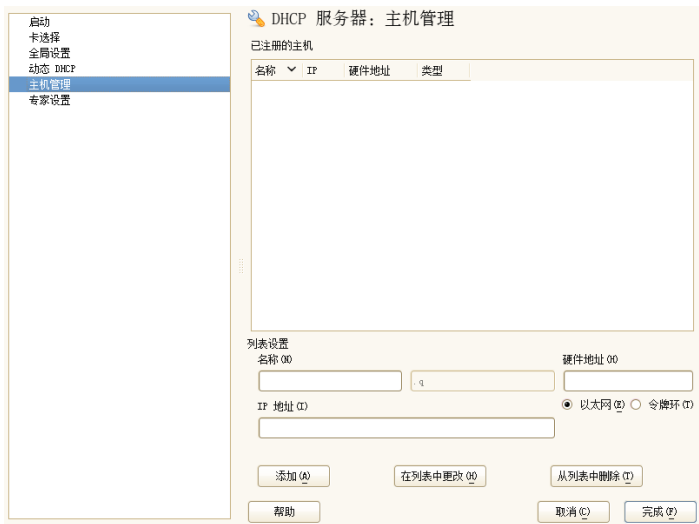
中止(B)

后退(B)

完成(F)

5 除了按上文所述方式使用动态 DHCP 之外，您也可以将服务器配置为以准静态方式指派地址。请使用窗口下部提供的输入字段来指定要以此方式管理的一组客户端。具体地说就是提供客户端的名称和 IP 地址，以及硬件地址和网络类型（令牌环或以太网）。使用添加、编辑和从列表中删除来修改在窗口上部显示的客户端列表。请参见图 25.5 “DHCP 服务器：主机管理” [338]。

图 25.5 DHCP 服务器：主机管理



25.1.2 DHCP 服务器配置（专家）

除了前面介绍的配置方法外，还有一种专家配置方式，用于从方方面面精确调整 DHCP 服务器设置。单击启动对话框中的 *DHCP 服务器* 专家配置（参见图 25.4 “DHCP 服务器：启动” [337]）以启动专家配置。

Chroot 环境和声明

在第一个对话框中，选择启动 *DHCP 服务器*，使现有的配置可编辑。DHCP 服务器的行为的一个重要功能就是它能够在 chroot 环境或 chroot jail 中运行，以保证服务器主机的安全。如果 DHCP 服务器受到了外部攻击，则攻击者仍将被封锁在 chroot jail 中，从而阻止他们进入系统的其他部分。对话框的下部显示了一个树视图，列出了已经定义的声明。请使用添加、删除和编辑来修改它们。如果选择高级，就会进入其他专家对话框。参见图 25.6 “DHCP 服务器：Chroot Jail 和声明” [339]。选择添加后，请定义要添加的声

明的类型。使用高级，可查看服务器的日志文件、配置 TSIG 密钥管理以及根据 DHCP 服务器的设置调整防火墙的配置。

图 25.6 DHCP 服务器：Chroot Jail 和声明



选择声明类型

DHCP 服务器的全局选项由许多声明组成。使用此对话框可设置声明类型子网、主机、共享网络、组、地址池和类别。此示例显示了新子网的选择（请参见图 25.7 “DHCP 服务器：选择声明类型” [340]）。

图 25.7 DHCP 服务器：选择声明类型

声明类型

声明类型

☒ 子网(S)

☐ 主机(H)

☐ 共享网络(N)

☐ 组(G)

☐ 地址池(P)

☐ 类(C)

中止(B)

下一步(N)

子网配置

此对话框用于指定新子网的 IP 地址和网络掩码。在对话框的中部，使用添加、编辑和删除修改所选子网的 DHCP 服务器启动选项。要为子网设置动态 DNS，请选择动态 DNS。

图 25.8 DHCP 服务器：配置子网

子网配置

网络地址(N)

192.168.27.0

网络掩码(M)

255.255.255.0

选项	值
allow	1400

添加(A)

编辑(E)

删除(D)

动态 DNS(D)

中止(B)

确定(O)

TSIG 密钥管理

如果在前面的对话框中选择了配置动态 DNS，现在就可以配置密钥管理来实现安全区域传送。选择确定将进入另一个对话框，在其中可以配置动态 DNS 的接口（请参见图 25.10 “DHCP 服务器：动态 DNS 的接口配置” [343]）。

图 25.9 DHCP 服务器：TSIG 配置



TSIG 密钥管理

添加现有的 TSIG 密钥

文件名(E) 浏览(W)... 添加(A)

创建新的 TSIG 密钥

密钥 ID(K) 文件名(F) 浏览(W)... 生成(G)

当前 TSIG 密钥

密钥 ID	文件名
-------	-----

删除(D)

后退(B) 中止(R) 确定(O)

动态 DNS：接口配置

通过选择**为此子网启用动态 DNS**，可以为子网激活动态 DNS。完成激活后，请使用下拉列表来选择正向和反向区域的 TSIG 密钥，同时确保这些密钥对于 DNS 和 DHCP 服务器是相同的。使用**更新全局动态 DNS 设置**，您可以根据动态 DNS 环境自动更新和调节全局 DHCP 服务器设置。最后需要定义每个动态 DNS 应更新哪些正向和反向区域，同时分别为两个区域指定主名称服务器的名称。选择**确定**返回子网配置对话框（请参见图 25.8 “DHCP 服务器：配置子网” [341]）。再次选择**确定**将返回最初的专家配置对话框。

图 25.10 DHCP 服务器：动态 DNS 的接口配置

接口配置

☒ 对此子网启用动态 DNS(E)

正向区域 TSIG 密钥(K)

example

反向区域 TSIG 密钥(K)

example

☐ 更新全局动态 DNS 设置(U)

区域(Z)

反向区域(V)

主 DNS 服务器(P)

主 DNS 服务器(I)

后退(B)

中止(R)

确定(O)

网络接口配置

要定义 DHCP 服务器应侦听的接口并调整防火墙配置，请从专家配置对话框中选择高级 > 接口配置。从所显示的接口列表中，选择一个或多个应由 DHCP 服务器侦听的接口。如果希望使所有子网中的客户端都能够与服务器通讯，同时如果服务器主机也运行防火墙，则相应调整防火墙。要执行此操作，选择修改防火墙设置。然后，YaST 将 SuSEfirewall2 的规则调整为新的条件（请参见图 25.11 “DHCP 服务器：网络接口和防火墙” [344]），之后您可以通过选择确定返回到原始对话框。

图 25.11 DHCP 服务器：网络接口和防火墙



在完成所有配置步骤后，选择**确定**关闭对话框。服务器现在将以新配置启动。

25.2 DHCP 软件包

DHCP 服务器和 DHCP 客户端都可用于您的产品。可用的 DHCP 服务器是 `dhcpcd`（由因特网系统联盟发布）。在客户端，选择两个不同的 DHCP 客户端之一：`dhcpc-client`（也来自 ISC）和 `dhcpcd` 包中的 DHCP 客户端守护程序。

默认情况下，系统上已安装 `dhcpcd`。此程序非常易于处理，且在每次系统引导时会自动启动以监视 DHCP 服务器。它不需要配置文件即可工作，而且可以直接用在大多数标准设置中。对于更复杂的情况，请使用 ISC `dhcpc-client`，它是通过配置文件 `/etc/dhclient.conf` 来控制的。

25.3 DHCP 服务器 dhcpd

任何 DHCP 系统的核心都是动态主机配置协议守护程序。根据配置文件 `/etc/dhcpd.conf` 中定义的设置，此服务器租出地址并监视它们的使用。通过更改此文件中的参数和值，系统管理员可以在许多方面影响程序的行为。让我们看一下例 25.1 “配置文件 `/etc/dhcpd.conf`” [345] 中的基本示例 `/etc/dhcpd.conf` 文件。

例 25.1 配置文件 `/etc/dhcpd.conf`

```
default-lease-time 600;           # 10 minutes
max-lease-time 7200;             # 2  hours

option domain-name "example.com";
option domain-name-servers 192.168.1.116;
option broadcast-address 192.168.2.255;
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;

subnet 192.168.2.0 netmask 255.255.255.0
{
    range 192.168.2.10 192.168.2.20;
    range 192.168.2.100 192.168.2.200;
}
```

这个简单的配置文件足以使 DHCP 服务器在网络中指派 IP 地址。确保在每行末尾插入一个分号，否则将不能启动 `dhcpd`。

示例文件可以分为三部分。第一部分定义了将 IP 地址租出给请求它的客户端的默认秒数 (`default-lease-time`)，超过此时间就应申请续期。此部分还包含一个最大期限语句，在此期限内计算机可以保留 DHCP 服务器指派的 IP 地址而无需申请续期 (`max-lease-time`)。

第二部分在全局级别上定义了一些基本网络参数：

- `option domain-name` 行用于定义网络的默认域。
- `option domain-name-servers` 项用于指定 DNS 服务器将 IP 地址解析为主机名（反之亦然）时使用的值（最多 3 个）。理想情况下，应在设置 DHCP 之前在您的计算机上或网络中的其他位置配置一个名称服务器。这个名称服务器应为每个动态地址定义一个主机名（反之亦然）。要了解如何配置您自己的名称服务器，请参见第 24 章 域名系统 [309]。

- 行 `option broadcast-address` 定义了请求客户端应该使用的广播地址。
- `option routers` 用于设置服务器在无法将数据包发送到本地网络上的主机时应将其发送到的位置（根据所提供的源和目标主机地址以及子网掩码）。在大多数情况下，尤其是在较小的网络中，此路由器与因特网网关完全相同。
- `option subnet-mask` 用于指定为客户端指派的网络掩码。

文件的最后一部分用于定义网络，其中包含子网掩码。最后指定一个地址范围，DHCP 守护程序将使用此范围来向相关的客户端指派 IP 地址。在例 25.1 “配置文件 `/etc/dhcpd.conf`” [345] 中，可以为客户端指派 192.168.2.10 和 192.168.2.20 之间以及 192.168.2.100 和 192.168.2.200 之间的任何地址。

在编辑这几行后，应可以使用命令 `rcdhcpd start` 来激活 DHCP 守护程序。随后将可以立即使用它。使用命令 `rcdhcpd check-syntax` 来执行简单的语法检查。如果配置出现意外问题（服务器由于错误而中止或在启动时不返回 `done`）通过在主系统日志 `/var/log/messages` 或控制台 10 (`Ctrl + Alt + F10`) 上查找相关信息，可发现出现的问题。

在默认 SUSE Linux Enterprise Server 系统上，基于安全原因，将在 `chroot` 环境中启动 DHCP 守护程序。必须将配置文件复制到 `chroot` 环境，以便守护程序能够找到它们。通常情况下无需担心这一点，因为命令 `rcdhcpd start` 会自动复制这些文件。

25.3.1 具有固定 IP 地址的客户端

DHCP 可用来向特定客户端指派预定义的静态地址。显式指派的地址始终优先于来自地址池的动态地址。静态地址永远不会像动态地址那样过期。例如，对于动态地址而言，如果没有足够的地址可用，服务器需要在客户端之间重新分发这些地址。

为了识别配置有静态地址的客户端，`dhcpd` 将使用硬件地址，这是全局唯一的固定数字代码，其中包含 6 对八进制数，用于标识所有网络设备（例如 `00:30:6E:08:EC:80`）。如果将相应的各行（如例 25.2 “配置文件的添加项” [347] 中的行）添加到例 25.1 “配置文件 `/etc/dhcpd.conf`” [345] 的配置文件，DHCP 守护程序会将相同的一组数据指派到相应的客户端。

例 25.2 配置文件的添加项

```
host jupiter {  
    hardware ethernet 00:30:6E:08:EC:80;  
    fixed-address 192.168.2.100;  
}
```

在第1行中输入相应客户端的名称（`hostname`，此处为 `jupiter`），在第2行中输入 MAC 地址。在 Linux 主机上，使用命令 `ip link show` 后跟网络设备（例如 `eth0`）来查找 MAC 地址。输出应包含如下内容：

```
link/ether 00:30:6E:08:EC:80
```

在上面的示例中，自动为带有 MAC 地址为 `00:30:6E:08:EC:80` 的网卡的客户端指派 IP 地址 `192.168.2.100` 和主机名 `jupiter`。虽然也支持在 IBM 系统上常见的 `token-ring`，但在几乎所有情况下，要输入的硬件类型都是以太网，

25.3.2 SUSE Linux Enterprise Server 版本

为了提高安全性，ISC 的 DHCP 服务器的 SUSE Linux Enterprise Server 版本附带由 Ari Edelkind 编写的 `non-root/chroot` 增补程序。这使得 `dhcpd` 能够使用用户 ID `nobody` 来运行，并可以在 `chroot` 环境（`/var/lib/dhcp`）中运行。要实现这一点，必须使配置文件 `dhcpd.conf` 位于 `/var/lib/dhcp/etc` 中。`init` 脚本在启动时会自动将文件复制到此目录。

通过文件 `/etc/sysconfig/dhcpd` 中的项来控制与此特性相关的服务器的行为。如果不希望在 `chroot` 环境中运行 `dhcpd`，请将 `/etc/sysconfig/dhcpd` 中的变量 `DHCPD_RUN_CHROOTED` 设置为“no”。

为了使 `dhcpd` 甚至能够解析来自 `chroot` 环境的主机名，还必须复制其他一些配置文件：

- `/etc/localtime`
- `/etc/host.conf`
- `/etc/hosts`
- `/etc/resolv.conf`

在启动 `init` 脚本时，将把这些文件复制到 `/var/lib/dhcp/etc/`。如果通过 `/etc/ppp/ip-up` 这样的脚本动态修改这些文件，则无论这些文件需要任何更改，都必须同时考虑这些副本。但是，如果配置文件仅指定 IP 地址（而不是主机名），就不需要担心这一点。

如果您的配置中包含应复制到 `chroot` 环境中的其他文件，请在文件 `etc/sysconfig/dhcpd` 中的变量 `DHCPD_CONF_INCLUDE_FILES` 下设置它们。为了确保 DHCP 日志记录功能即使在 `syslog-ng` 守护程序重新启动后也能保持运行，文件 `/etc/sysconfig/syslog` 中必须有附加条目 `SYSLOGD_ADDITIONAL_SOCKET_DHCP`。

25.4 更多信息

有关 DHCP 的更多信息，请访问因特网系统联盟网站(<http://www.isc.org/products/DHCP/>)。也可在 `dhcpd`、`dhcpd.conf`、`dhcpd.leases` 和 `dhcp-options` 手册页中获得相关信息。

使用 NetworkManager

NetworkManager 是用于便携式计算机和其他可移动计算机的理想解决方案。它支持网络连接的顶级加密类型和标准，包括 802.1x 保护的网络的连接。802.1X 是“基于端口的网络访问控制的本地和城域网 IEEE 标准”。使用 NetworkManager，您就无需担心在移动时配置网络接口以及切换有线或无线网络的问题。NetworkManager 可自动连接到已知无线网络或并行管理多个网络连接 — 然后将最快的连接用作默认连接。而且，您还可手动在可用网络之间切换，并使用系统盘中的小程序管理网络连接。

不只可激活一个连接，也可同时激活多个。这样您可以将便携式计算机从以太网连接拔出后仍通过无线连接保持连接状态。

26.1 NetworkManager 的用例

NetworkManager 提供了完善而直观的用户界面，可使用户轻松地切换其网络环境。但是，NetworkManager 在以下情况下不适用：

- 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。
- 计算机为 Xen 服务器或系统是 Xen 内的虚拟系统时。

26.2 启用或禁用 NetworkManager

在便携式计算机上，默认情况下 NetworkManager 处于启用状态。但是，任何时候都可以在 YaST 网络设置模块中启用或禁用它。

- 1 运行 YaST 然后转到 *网络设备 > 网络设置*
 - 2 将打开 *网络设置* 对话框。转到 *全局选项* 选项卡。
 - 3 要通过 NetworkManager 配置和管理您的网络连接，请：
 - 3a 在 *网络设置方法* 字段中选择 *通过 NetworkManager 的用户控制方法*。
 - 3b 单击 *确定* 并关闭 YaST。
 - 3c 按照第 26.3 节 “配置网络连接” [351] 中所述通过 NetworkManager 配置您的网络连接。
 - 4 要停用 NetworkManager 并以传统方法控制网络，请：
 - 4a 在 *网络设置方法* 字段中选择 *通过 ifup 的传统方法*。
 - 4b 单击 *确定*。
 - 4c 通过 YaST 设置您的网卡，即通过 DHCP 或静态 IP 地址进行自动配置。还可以通过 YaST 配置您的调制解调器：
 - 对于拨号连接，请使用 *网络设备 > 调制解调器*。
 - 要配置内部或 USB ISDN 调制解调器，请选择 *网络设备 > ISDN*。
 - 要配置内部或 USB DSL 调制解调器，请选择 *网络设备 > DSL*。
- 在第 21.4 节 “使用 YaST 配置网络连接” [254] 和第 18 章 *无线 LAN* [203] 中查找使用 YaST 进行网络配置的详细描述。

26.3 配置网络连接

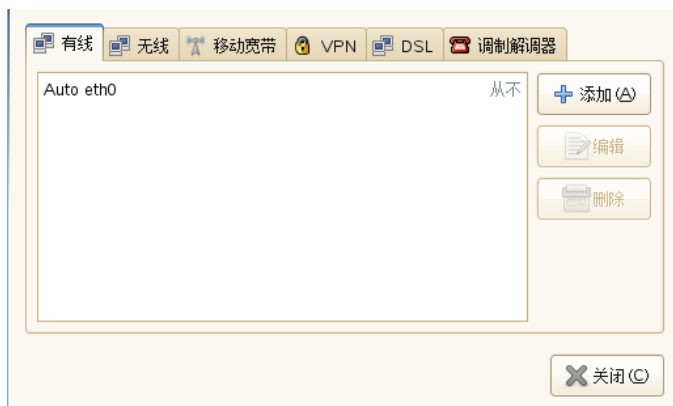
在 YaST 中启用 NetworkManager 后，使用 KDE 和 GNOME 中提供的 NetworkManager 前端配置网络连接。两个前端的网络配置对话框都很相似。它们显示所有网络连接类型的选项卡，例如有线、无线、移动宽带、DSL 和 VPN 连接。在每个选项卡上都可以添加、编辑或删除该类型的连接。在 KDE 配置对话框中，只有该连接类型在您的系统上可用（根据硬件和软件）时，才激活相应的选项卡。默认情况下，KNetworkManager 还在每个选项卡上显示输入字段和选项的全面工具提示。

注意：蓝牙连接

目前不能使用 NetworkManager 配置蓝牙连接。

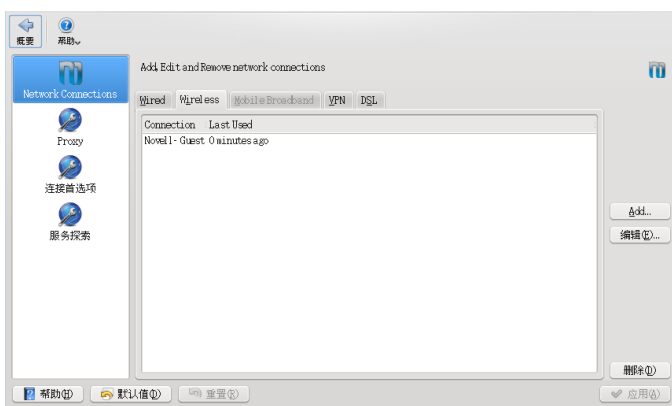
要在 GNOME 中打开网络配置对话框，请打开主菜单并单击右边的网络条目。还可以按 **Alt + F2** 并输入 `nm-connection-editor`，或在 GNOME 控制中心中选择系统 > 网络连接。

图 26.1 GNOME 网络连接对话框



如果使用 KDE，打开主菜单并单击配置桌面。在个人设置中，选择网络设置（在常规选项卡上），以打开网络配置对话框。

图 26.2 KDE 网络配置对话框



或者也可以从系统盘中的 NetworkManager 小程序启动配置对话框。在 KDE 中左键单击图标并选择 **管理连接**。在 GNOME 中右键单击图标并选择 **编辑连接**。

注意：选项的可用性

根据您的系统设置，可能不允许您配置连接。在安全环境中，某些选项可能被锁定或要求 root 权限。请咨询系统管理员以了解细节。

过程 26.1 添加或编辑连接

用 NetworkManager 配置网络连接时，还可以定义可由所有用户共享的系统连接。与用户连接相比，系统连接在 NetworkManager 启动之后、任何用户登录前就可用。有关两类连接的更多细节，请参见第 26.7.1 节“用户和系统连接”[361]。

目前系统连接选项在 KDE 中不可用。在这种情况下，要设置系统连接，需使用 YaST。

注意：隐藏网络

要连接“隐藏”网络（不广播其服务的网络），必须知道该网络的服务集标识符 (SSID) 或扩展服务集标识符 (ESSID)。不能自动检测到隐藏网络。

- 1 在“网络配置”对话框中，单击要使用的连接类型的选项卡。
- 2 单击 **添加** 创建新连接或选择现有连接再单击 **编辑**。

- 3 输入连接名称和连接细节。
- 4 对于隐藏网络，请输入 ESSID 和加密参数。
- 5 如果每个连接类型有多台物理设备（例如您的计算机装有两块以太网卡或两块无线网卡），可将该连接绑定到特定的设备。

如果使用 KDE，用*限制到接口*选项即可实现。如果用 GNOME，输入您要将连接绑定到的设备的 *MAC 地址*，确认您的设置。

- 6 要让 NetworkManager 自动使用某个连接，请为此连接激活以下选项：*自动连接* (KDE) 或*尽可能保持连接* (GNOME)。
- 7 要将某连接变为系统连接，请激活*对所有用户可用* (GNOME)。要创建和编辑系统连接，需要 root 权限。

确认您的更改后，新配置的网络连接就会出现在您左键单击 NetworkManager 小程序后显示的列表中。

图 26.3 KNetworkManager — 已配置并可用的连接



26.4 使用 KNetworkManager

NetworkManager 的 KDE 前端是 KNetworkManager 小程序。如果为 NetworkManager 控制设置了网络，则小程序通常通过桌面环境自动启动且显示为系统盘中的图标。

如果您的系统盘没有显示任何网络连接图标，该小程序可能未启动。按 **Alt + F2** 键并输入 `knetworkmanager` 可手动启动它。

KNetworkManager 只显示您配置了连接的无线网络。当超出无线网络范围或拔出网络电缆时，它会隐藏连接，这样您始终可以清楚地看到哪些连接是可用的。

26.4.1 管理有线网络连接

如果您的计算机已通过网络电缆连接到现有网络上，则使用 KNetworkManager 选择网络连接。

- 1 单击小程序的图标可显示具有可用网络的菜单。在菜单中选中当前使用的连接，并标记为活动。
- 2 如果您要对有线网络使用其他配置，请单击 *管理连接* 并按过程 26.1, “添加或编辑连接” [352] 中所述添加其他有线连接。
- 3 单击 KNetworkManager 图标，选择新配置的连接以激活它。

26.4.2 管理无线网络连接

默认情况下，KNetworkManager 只显示您配置了连接的无线网络 — 假定它们可用并可见。第一次连接到无线网络可如下进行操作：

过程 26.2 连接到无线网络

- 1 左键单击小程序图标，选择 *创建网络连接*。KNetworkManager 显示可用且可见无线网络的列表，包括信号强度和安全性的细节。
- 2 要连接到可见网络，从列表中选择网络，单击 *连接*。如果网络已加密，将打开一个对话框。选择网络使用的安全类型并输入相应的身份凭证。
- 3 要连接到没有广播其服务集标识（SSID 或 ESSID）并因此无法被自动检测到的网络，请选择 *通过 WLAN 接口连接到其他网络*。
- 4 在打开的对话框中输入 SSID 或 ESSID，并视需要设置加密参数。
- 5 确认更改，单击 *确定*。NetworkManager 现在将激活新的连接。
- 6 要终止连接并禁用无线联网，请单击小程序图标并取消选中 *启用无线*。如果您在飞机上或在不允许使用无线网络的任何其他环境中，则此选项可能很有用。

显式选中的无线网络将尽可能始终保持连接。如果那时插入网络电缆，任何设置为 *自动连接* 的连接都将连接，而无线连接也保持连接。

26.4.3 将无线网卡配置为接入点

如果无线网卡支持接入点方式，则可以使用 NetworkManager 来进行配置。

注意：选项的可用性

根据您的系统设置，可能不允许您配置连接。在安全环境中，某些选项可能被锁定或要求 `root` 权限。请咨询系统管理员以了解细节。

- 1 单击 KNetworkManager 小程序并选择 **创建网络连接 > 新建专用网络**。
- 2 在以下配置对话框中，在 *SSID* 字段中输入网络的名称。



The image shows a configuration window for a new wireless connection. At the top, there is a 'Connection Name (N):' field with the text '新建无线连接'. Below this are two unchecked checkboxes: '自动连接 (A)' and '系统连接 (S)'. There are three tabs: '无线 (W)' (selected), '无线安全性 (E)', and 'IP 地址 (I)'. Under the '无线 (W)' tab, there are several fields: 'SSID (I):' with a '扫描 (C)' button, '模式 (M):' set to '对等' (Ad-hoc), 'BSSID (B):' with a placeholder '_:_:_:_:_:_', '限于接口 (R):' set to '任意' (Any), and 'MTU (U):' set to '自动' (Automatic). At the bottom right are '确定 (O)' and '取消 (C)' buttons.

- 3 在无线安全选项卡上设置加密。

重要：不受保护的无线网络是有安全风险的。

如果将安全设置为无，任何人都可以连接到您的网络，重复使用您的连接并截取您的网络连接。要限制对访问点的访问，确保连接安全，请使用加密。您可在基于 WEP 和 WPA 的各种加密方法之间进行选择。如果不能肯定哪种技术最适合，请阅读第 18.3 节“身份验证”[205]。

- 4 在 *IP 地址* 选项卡上，确保配置选项设置为共享（是专用网络的默认选项）。
- 5 单击 *确定* 确认您的配置。

26.4.4 自定义 KNetworkManager

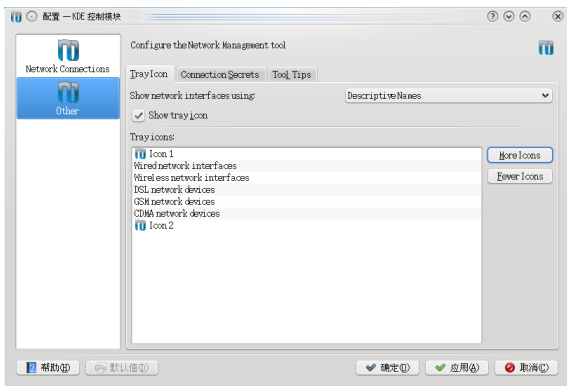
您可以自定义 KNetworkManager 的某些方面：系统盘中显示的图标数、显示哪些工具提示，以及如何储存您的网络连接的密码和身份凭证。有关最后一方面的详细信息，请参考第 26.7.2 节“储存密码和身份凭证”[361]。

要浏览可用选项，请右键单击 NetworkManager 系统盘，选择 *管理连接*，单击配置对话框左侧的 *其他*。

过程 26.3 为 KNetworkManager 配置多个系统盘图标

因为 KNetworkManager 可以同时保持多个活动连接，您可能希望能一眼看清若干连接的状态信息。您可以用系统盘中的多个 NetworkManager 图标实现这一点，其中每个都代表不同的连接类型组（例如，一个图标用于，另一个图标用于无线连接）。

- 1 在配置对话框中切换到 *托盘图标* 选项卡。
- 2 单击 *更多图标*。列表中将显示新的图标项。
- 3 选择您要用该图标表示的网络连接类型，将它们归入各自的图标下。



4 确认更改。

现在系统盘显示多个 NetworkManager 图标，您可从中访问绑定到该图标的连接类型。

如过程 26.1, “添加或编辑连接” [352] 中所述配置网络连接时，KNetworkManager 还允许您自定义为该连接显示的图标。要更改图标，单击连接名称旁的图标按钮，在出现的对话框中选择您想选择的图标。确认更改后，新图标将显示在单击系统盘中的 KNetworkManager 图标时显示的可用连接列表中。

26.5 使用 GNOME NetworkManager 小程序

在 GNOME 中，可通过 GNOME NetworkManager 小程序控制 NetworkManager。如果为 NetworkManager 控件设置了网络，则小程序通常通过桌面环境自动启动且显示为系统盘中的图标。

如果您的系统盘没有显示任何网络连接图标，该小程序可能未启动。按 Alt + F2 键并输入 nm-applet 可手动启动它。

26.5.1 管理有线网络连接

如果您的计算机已通过网络电缆连接到现有网络上，则使用 NetworkManager 小程序选择网络连接。

- 1 单击小程序的图标可显示具有可用网络的菜单。在菜单中选择当前使用的连接。
- 2 要切换到另一个网络，请从列表中选择它。
- 3 要关闭所有网络连接，包括有线的和无线的，请右键单击小程序图标并取消选中**启用联网**。

26.5.2 管理无线网络连接

可用的可见无线网络在无线网络下的 GNOME NetworkManager 小程序菜单中列出。每个网络的信号强度也会显示在菜单中。加密无线网络是用保护物图标标记的。

过程 26.4 连接到无线网络

- 1 要连接到无线网络，请左键单击小程序图标，从可用无线网络列表中选择一项。
- 2 如果网络已加密，将打开一个对话框。它显示网络使用的加密类型（无线安全），根据各自的加密和身份验证设置，还有许多输入字段。输入适当的身份凭证。
- 3 要连接到没有广播其服务集标识符（SSID 或 ESSID）并因此无法被自动检测到的网络，请单击 NetworkManager 图标并选择**连接到隐藏无线网络**。
- 4 在打开的对话框中的**网络名称**中输入 SSID 或 ESSID，并视需要设置加密参数。
- 5 要禁用无线联网，请右键单击小程序图标并取消选中**启用无线**。如果您在飞机上或在不允许使用无线网络的任何其他环境中，则此选项可能很有用。

显式选中的无线网络将尽可能始终保持连接。如果在此期间插入网线，则会连接任何设置为**尽可能保持连接**的连接，而无线连接也会保持连接状态。

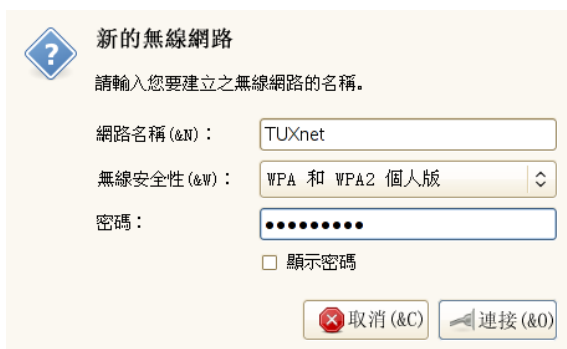
26.5.3 将无线网卡配置为接入点

如果无线网卡支持接入点方式，则可以使用 NetworkManager 来进行配置。

注意：选项的可用性

根据您的系统设置，可能不允许您配置连接。在安全环境中，某些选项可能被锁定或要求 `root` 权限。请咨询系统管理员以了解细节。

- 1 单击 NetworkManager 小程序并选择新建无线网络。



新的無線網路

請輸入您要建立之無線網路的名稱。

網路名稱 (&N): TUXnet

無線安全性 (&W): WPA 和 WPA2 個人版

密碼:

☐ 顯示密碼

取消 (&C) 連接 (&O)

- 2 输入网络名称并用无线安全下拉菜单设置要用的加密。

重要：不受保护的无线网络是有安全风险的。

如果将无线安全设置为无，任何人都可以连接到您的网络，重复使用您的连接并截获您的网络连接。要限制对访问点的访问，确保连接安全，请使用加密。您可在基于 WEP 和 WPA 的各种加密方法之间进行选择。如果不能肯定哪种技术最适合，请阅读第 18.3 节“身份验证”[205]。

26.6 NetworkManager 和 VPN

NetworkManager 支持多种虚拟专用网 (VPN) 技术。对于每种技术，SUSE Linux Enterprise Server 都带有提供 NetworkManager 的常规支持的基础包。此外，还需要为您的小程序安装特定于桌面的包。

NovellVPN

要使用此 VPN 技术，请安装

- NetworkManager-novellvpn 和
- NetworkManager-novellvpn-kde4 或
NetworkManager-novellvpn-gnome。

对 KDE 的 NovellVPN 支持目前尚不可用，但正在努力解决。

OpenVPN

要使用此 VPN 技术，请安装

- NetworkManager-openvpn 和
- NetworkManager-openvpn-kde4 或
NetworkManager-openvpn-gnome。

vpnc (Cisco)

要使用此 VPN 技术，请安装

- NetworkManager-vpnc 和
- NetworkManager-vpnc-kde4 或
NetworkManager-vpnc-gnome。

PPTP（点对点隧道协议）

要使用此 VPN 技术，请安装

- NetworkManager-pptp 和
- NetworkManager-pptp-kde4 或
NetworkManager-pptp-gnome。

在安装包后，按照第 26.3 节“配置网络连接”[351]中所述配置 VPN 连接。

26.7 NetworkManager 和安全性

NetworkManager 区分两种类型的无线连接，即可信和不可信。可信连接是您过去明确选择的任何网络。所有其他连接均为不可信连接。可信连接用访问点的名称和 MAC 地址识别。使用 MAC 地址可以确保带有可信连接名称的不同访问点不可使用。

NetworkManager 定期扫描是否存在可用的无线网络。如果找到多个可信网络，则自动选择最近使用的可信网络。如果所有网络均不可信，则 NetworkManager 等待您的选择。

如果加密设置改变，但名称和 MAC 地址不变，则 NetworkManager 将尝试连接，但首先会要求您确认新的加密设置并提供任意更新（如新密钥）。

如果您从使用无线连接切换到脱机模式，则 NetworkManager 会将 SSID 或 ESSID 设为空白。这可以确保断开网卡连接。

26.7.1 用户和系统连接

NetworkManager 可识别两种类型的连接：用户和系统连接。用户连接是第一个用户登录时对 NetworkManager 可用的连接。会向该用户询问任何必需的身份凭证，当该用户注销时，连接会断开并从 NetworkManager 中删除。定义为系统连接的连接可以由所有用户共享，并在启动 NetworkManager 之后（任何用户登录之前）立即可用。如果是系统连接，必须在创建连接时提供所有身份凭证。此类系统连接可用于自动连接到要求授权的网络。有关如何用 NetworkManager 配置用户连接或系统连接的信息，请参考第 26.3 节“配置网络连接”[351]。

对于 KDE，目前不支持用 NetworkManager 配置系统连接（改为使用 YaST）。

26.7.2 储存密码和身份凭证

如果不想每次连接到加密网络时都要再次输入身份凭证，则可以使用特定于桌面的工具 GNOME 密钥环管理器或 KWalletManager 将身份凭证加密储存在磁盘上，并用主密码保护。

NetworkManager 还从证书储存检索用于安全连接（例如加密的有线、无线或 VPN 连接）的证书。有关更多信息，请参考第 12 章 *Certificate Store* (↑安全指南)。

26.8 常见问题

下面是关于使用 NetworkManager 配置特殊网络选项的一些常见问题。

如何将连接绑定到特定设备？

默认情况下，NetworkManager 中的连接是特定于设备类型的：它们适用于同一类型的所有物理设备。如果每个连接类型有多台物理设备可用（例如您的计算机装有两块以太网卡），您可以把一个连接绑定到特定设备。

在 GNOME 中要达到此目的，先查找设备的 MAC 地址（使用小程序中提供的连接信息，或使用诸如 nm-tool 或 ifconfig 等命令行工具的输出）。然后启动配置网络连接的对话框，选择您要修改的连接。在有线或无线选项卡上，输入设备的 MAC 地址，并确认更改。

如果使用 KDE，则可启动配置网络连接的对话框，选择要修改的连接。在以太网或无线选项卡上，使用限制到接口选项选择要把连接绑定到的网络接口。

如果检测到同一 ESSID 有多个接入点，如何指定特定接入点？

当有不同无线波段 (a/b/g/n) 的多个接入点时，默认情况下会自动选择信号最强的接入点。要覆盖此值，配置无线连接时请使用 BSSID 字段。

基本服务集标识 (BSSID) 可唯一标识每个基本服务集。在基础结构基本服务集中，BSSID 是无线接入点的 MAC 地址。在独立（特别）基本服务集中，BSSID 是本地管理的 MAC 地址（从 46 位数字随机生成）。

如第 26.3 节“配置网络连接”[351]中所述启动配置网络连接的对话框。选择要修改的无线连接，然后单击编辑。在无线选项卡上，输入 BSSID。

如何将网络连接与其他计算机共享？

主设备（连接到因特网的设备）不需要任何特殊配置。但是，需要如下配置连接到本地集线器或计算机的设备：

1. 如第 26.3 节“配置网络连接”[351]中所述启动配置网络连接的对话框。选择要修改的连接，然后单击编辑。如果用 GNOME，切换到 IPv4 设置选

项卡，从方法下拉列表中选择共享给其他计算机。如果用 KDE，切换到 *IP 地址* 选项卡，从配置下拉列表选择共享。这将启用 IP 通讯转发并运行该设备上的 DHCP 服务器。在 NetworkManager 中确认更改。

2. 由于 DHCP 服务器使用端口 67，请确保该端口没有被防火墙阻止：在共享连接的计算机上，启动 YaST 并选择安全和用户 > 防火墙。切换到允许的服务类别。如果 DHCP 服务器尚未显示为允许的服务，请从待允许的服务中选择 DHCP 服务器，然后单击添加。在 YaST 中确认更改。

如何对自动（DHCP、PPP、VPN）地址提供静态 DNS 信息？

如果 DHCP 服务器提供无效的 DNS 信息（和/或路由），则可以覆盖它。如第 26.3 节“配置网络连接”[351]中所述启动配置网络连接的对话框。选择要修改的连接，然后单击编辑。如果用 GNOME，切换到 *IPv4 设置* 选项卡，从方法下拉列表中，选择仅自动 (DHCP) 地址。如果用 KDE，切换到 *IP 地址* 选项卡，从配置下拉列表选择仅自动 (DHCP) 地址。在 DNS 服务器和搜索域字段中输入 DNS 信息。要忽略自动获取的路由，请单击路由 (GNOME) 并激活相应的复选框，或从 (KDE) 选项卡底部的下拉列表中选择路由并激活相应的复选框。确认更改。

有用户登录密码保护的网路前，如何使 NetworkManager 连接到该网路？

定义可以用于此类用途的系统连接。有关更多信息，请参考第 26.7 节“NetworkManager 和安全性”[361]。

26.9 查错

可能出现连接问题。与 NetworkManager 相关的一些常见问题包括小程序不启动或缺少 VPN 选项。解决方法和预防这些问题的方法随使用的工具而定。

NetworkManager 桌面小程序未启动

如果网络设置为 NetworkManager 控制，GNOME 和 KDE NetworkManager 小程序自动启动。若小程序未启动，则按照第 26.2 节“启用或禁用 NetworkManager”[350]中所述检查是否在 YaST 中启用了 NetworkManager。然后确保也已安装用于您的桌面环境的相应包。如果正在使用 KDE 4，则包为 NetworkManager-kde4。对于 GNOME 用户，包为 NetworkManager-gnome。

如果桌面小程序已经安装，但出于某种原因没有运行，则手动启动它。如果安装了桌面小程序，但由于某些原因没有运行，用命令 `nm-applet` (GNOME) 或 `knetworkmanager` (KDE) 手动启动它。

NetworkManager 小程序不包括 VPN 选项

对 NetworkManager、小程序以及针对 NetworkManager 的 VPN 的支持在不同的包中分发。如果 NetworkManager 小程序不包括 VPN 选项，请检查带有 NetworkManager 的 VPN 支持的包是否已安装。有关详细信息，请参见第 26.6 节 “NetworkManager 和 VPN” [359]。

没有可用的网络连接

如果您已正确配置网络连接并且网络连接的所有其他组件（路由器等等）也已启动并在正常运行，则重新启动计算机上的网络接口有时可能有帮助。要执行此操作，请作为 `root` 登录到命令行，然后运行 `rcnetwork restart`。

26.10 更多信息

可在以下网站和目录中找到有关 NetworkManager 的更多信息：

NetworkManager 项目页

<http://projects.gnome.org/NetworkManager/>

KDE NetworkManager 前端

<http://userbase.kde.org/NetworkManagement>

包文档

还可以在以下目录中找到 NetworkManager 和 GNOME、KDE NetworkManager 小程序的最新信息：

- `/usr/share/doc/packages/NetworkManager/`,
- `/usr/share/doc/packages/NetworkManager-kde4/`，以及
- `/usr/share/doc/packages/NetworkManager-gnome/`。

Samba

使用 Samba，可以将 Unix 计算机配置为 Mac OS X、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（Web 界面）或通过手动编辑配置文件来配置 Samba。

27.1 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（服务器消息块）协议。Microsoft 发布该协议以便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端上安装 TCP/IP 协议。

提示：IBM System z：NetBIOS 支持

IBM System z 仅通过 TCP/IP 支持 SMB。这些系统上不提供 NetBIOS 支持。

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 是为用于提供名称服务的计算机之间进行通讯而设计的软件接口 (API)。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。网络上的任何计算机均可以保留所需数量的名称，前提是这些名称均未使用。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，或本机使用 DNS。Samba 默认采用这种方式。

Samba 服务器

Samba 服务器向客户端提供 SMB/CIFS 服务和 NetBIOS over IP 命名服务。对于 Linux，Samba 服务器有三个守护程序：`smbd` 用于 SMB/CIFS 服务，`nmbd` 用于命名服务，`winbind` 用于身份验证。

Samba 客户端

Samba 客户端是一种能够通过 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 系统提供客户端。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 客户端运行任何守护程序。

共享

SMB 服务器通过共享为其客户端提供资源。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。客户端可以根据打印机的名称来访问打印机。

DC

域控制器 (DC) 是处理域中的帐户的服务器。为了复制数据，一个域中可有更多域控制器可用。

27.2 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 27.3.1 节“使用 YaST 配置 Samba 服务器”[367]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）**，并检查 winbind、smb 和 nmb。从命令行，使用 `rcsmb stop && rcnmb stop` 停止 Samba 所需的服务，然后使用 `rcnmb start && rcsmb start` 启动它们；rcsmb 依赖于 winbind（如果需要）。

27.3 配置 Samba 服务器

SUSE® Linux Enterprise Server 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。

27.3.1 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**。

27.3.1.1 初始 Samba 配置

第一次启动此模块时，*Samba* 安装对话框启动，提示您做出一些有关服务器管理的基本决定。配置结束时，系统会提示您输入 Samba 管理员密码（*Samba root* 密码）。以后启动时，会显示 *Samba* 配置对话框。

Samba 安装对话框包括两个步骤和详细设置（可选）：

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，指定服务器是应该充当主域控制器 (PDC)、备份域服务器 (BDC) 还是根本不充当域控制器。按下一步继续。

如果不想再继续详细的服务器配置，请单击**确定**确认。然后在最后的弹出框中，设置 *Samba root* 密码。

稍后可以在 *Samba* 配置对话框的**启动、共享、身份、可信域和 LDAP** 设置选项卡中更改所有设置。

27.3.1.2 高级 Samba 配置

在 Samba 服务器模块第一次启动时，*Samba* 配置对话框会在两个初始步骤后立即显示，如第 27.3.1.1 节“初始 Samba 配置”[367]所述。使用它调整您的 Samba 服务器配置。

编辑配置之后，单击**确定**保存设置。

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 27.2 节“启动和停止 Samba”[367]。

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。

允许用户共享目录使允许的组中的组成员可以与其他用户共享他们拥有的目录。例如，*users* 用于本地范围，*DOMAIN\Users* 用于域范围。该用户必须还确保文件系统权限允许访问。最大共享数可限制可以创建的共享的总数。要允许访问用户共享而无需身份验证，请启用**允许来宾访问**。

身份

在**身份**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）。可以使用 Microsoft Windows Internet Name Service (WINS) 进行名称解析。在这种情况下，激活使用 *WINS* 进行主机名解析，并确

定是否通过 *DHCP* 检索 *WINS* 服务器。要设置专家全局设置或设置用户身份验证源，例如 *LDAP* 而不是 *TDB* 数据库，请单击高级设置。

可信域(T)

要使其他域的用户能够访问您的域，在可信域选项卡中进行适当的设置。要添加新域，请单击添加。要除去所选的域，请单击删除。

LDAP 设置

在选项卡 *LDAP* 设置中，您可以确定要用于身份验证的 *LDAP* 服务器。要测试到 *LDAP* 服务器的连接，请单击测试连接。要设置专家 *LDAP* 设置或使用默认值，请单击高级设置。

有关 *LDAP* 配置的更多信息，请参见第 4 章 *LDAP—A Directory Service* (↑安全指南)。

27.3.2 使用 SWAT 管理 Web

Samba 服务器管理的备用工具是 *SWAT* (*Samba Web* 管理工具)。它提供了一个简单的 *Web* 接口，可用来配置 *Samba* 服务器。要使用 *SWAT*，请在 *Web* 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 root* 帐户，则请使用系统 *root* 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”)。

27.3.3 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。

27.3.3.1 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，除非此名称已指派给网络中的其他计算机。如果 DNS 名称不可用，请使用

netbiosname=MYNAME 设置服务器名称。有关此参数的更多细节，请参见 smb.conf 手册页。

```
os level = 20
```

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）。有了 Samba 3 版本系列，就几乎不必再覆盖默认设置 (20) 了。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，如 2。有关此重要主题的更多信息，可以在《Samba 3 操作指南》的“网络浏览”一章中找到；有关《Samba 3 操作指南》的更多信息，请参见第 27.7 节“有关详细信息”[376]。

如果网络中没有任何其他 SMB 服务器（如 Windows 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，同时又需要它们互相通讯，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。

27.3.3.2 共享

以下示例描述了如何使 CD-ROM 驱动器和用户目录 (homes) 对 SMB 客户端可用。

[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。删除第一列中的分号，以便与 Samba 共享 CD-ROM 驱动器。

例 27.1 CD-ROM 共享（已停用）

```
;[cdrom]
;      comment = Linux CD-ROM
;      path = /media/cdrom
;      locking = No
```

[cdrom] 和 comment

[cdrom] 部分项是网络上的所有 SMB 客户端均可看到的共享的名称。

可以添加一个附加 comment 来进一步描述此共享。

```
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 27.2 [homes] 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。这样就可以将用户的共享访问权仅限制于此用户。

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。

27.3.3.3 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 提供以下检查许可权限的方式：

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)

此变体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`)

从客户端来看，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身份验证。此设置还需要 `password server` 参数。

ADS 级安全性 (`security = ADS`)

在该模式中，Samba 将在 Active Directory 环境中充当域成员。要在该模式中工作，运行 Samba 的计算机需要安装并配置 Kerberos。必须使用 Samba 将该计算机加入到 ADS 领域。该步骤可通过使用 YaST *Windows 域成员资格* 模块完成。

域级安全性 (`security = domain`)

仅当计算机已加入到 Windows NT 域中时，该模式才能正常工作。Samba 将尝试验证用户名和密码，方法是将其传递到 Windows NT 主或备份域控制器。与 Windows NT 服务器所采用的方式相同。它期望将加密密码参数设置为 `yes`。

选择共享、用户或域级安全性适用于整个服务器。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。

有关此主题的更多信息，可以在《Samba 3 操作指南》中找到。对于一个系统上的多个服务器，应注意选项 `interfaces` 和 `bind interfaces only`。

27.4 配置客户端

客户端只能通过 TCP/IP 访问 Samba 服务器。NetBEUI 和通过 IPX 的 NetBIOS 不能与 Samba 共用。

27.4.1 使用 YaST 配置 Samba 客户端

配置 Samba 客户端来访问 Samba 或 Windows 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 NT 或 Active Directory 域或工作组。如果激活将 *SMB 信息也用于 Linux 身份验证*，则用户身份验证将在 Samba、NT 或 Kerberos 服务器上运行。

单击专家设置获取高级配置选项。例如，使用装入服务器目录表启用自动装入服务器用户主目录和身份验证。这样用户就能访问位于 CIFS 上的用户主目录。有关细节，请参见 `pam_mount` 手册页。

完成所有设置后，请确认对话框以完成配置。

27.5 将 Samba 用作登录服务器

在主要由 Windows 客户端组成的网络中，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 27.3 “`smb.conf` 中的 `global` 部分” [374]

例 27.3 `smb.conf` 中的 `global` 部分

```
[global]
    workgroup = TUX-NET
    domain logons = Yes
    domain master = Yes
```

如果使用加密密码进行校验，则 Samba 服务器必须能够处理加密密码。

`[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 域概念要求的域帐户：

```
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。

```
add machine script = /usr/sbin/useradd -g nogroup -c "NT Machine Account" \
-s /bin/false %m\${
```

要确保 Samba 能够正确执行此脚本，请选择具有必需的管理员权限的 Samba 用户，并将其添加到 `ntadmin` 组中。然后可以使用以下命令为属于此 Linux 组的所有用户指派 Domain Admin 状态：

```
net groupmap add ntgroup="Domain Admins" unixgroup=ntadmin
```


有关此主题的更多信息，请参见《Samba 3 操作指南》第 12 章，此指南可以在 `/usr/share/doc/packages/samba/Samba3-HOWTO.pdf` 中找到。

27.6 带有 Active Directory 的网络中的 Samba 服务器

如果您同时运行 Linux 服务器和 Windows 服务器，则可以构建两个独立的身份验证系统和网络，或者将服务器连接到使用一个中央身份验证系统的网络。由于 Samba 可以与 Active Directory 域相结合，因此您可以将 SUSE Linux Enterprise Server 连接 Active Directory (AD)。

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 6.16.1.7 节“用户身份验证方法”(第 6 章 *使用 YaST 进行安装*, ↑ *部署指南*) 介绍了如何在安装期间加入域。

要在运行系统中连接 AD 域，请按如下所示继续：

- 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* 屏幕上的域或工作组中输入要加入的域。

图 27.1 确定 Windows 域成员资格

- 4 选中*也使用 SMB 信息进行 Linux 身份验证*以在 SUSE Linux Enterprise Server 上使用 SMB 源进行 Linux 身份验证。
- 5 单击*确定*并在提示时确认域连接。
- 6 在 AD 服务器上提供 Windows Administrator 的密码，并单击*确定*。

现在您的服务器已经设置了从 Active Directory 域控制器获取认证数据。

27.7 有关详细信息

关于 Samba 的详细信息，请参见数字文档。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。examples 子目录中提供了一个带注释的示例配置 (`smb.conf.SUSE`)。

Samba 小组提供的《Samba 3 操作指南》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，可以在 `/usr/`

share/doc/packages/samba/Samba 3-HOWTO.pdf 中找到《Samba 3 操作指南》。

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。久经验证的网络文件系统 (NFS) 与黄页协议 NIS 协同工作。要使用可以与 LDAP 协同工作并且也可以使用 Kerberos 的更安全协议，请选中 NFSv4。结合使用 pNFS，您可以突破性能瓶颈。

NFS 与 NIS 一起使用时网络面向用户是透明的。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，而与当前使用的终端无关。

重要：需要 DNS 的原因

从理论上讲，所有导出都可以仅使用 IP 地址来完成。为避免超时，您需要一个有效的 DNS 系统。至少为了日志记录目的也应使用 DNS，因为 mountd 守护程序执行反向查找。

28.1 术语

下面是 YaST 模块中使用的术语。

导出

由 NFS 服务器导出的目录，客户端可将其集成到系统中。

NFS 客户端

NFS 客户端是通过网络文件系统协议使用来自 NFS 服务器的 NFS 服务的系统。TCP/IP 协议已集成到 Linux 内核中；无需再安装任何其他软件。

NFS 服务器

NFS 服务器向客户端提供 NFS 服务。运行中的服务器依赖于以下守护程序：
nfsd（工作）、idmapd（到 ID 的用户和组名映射，反之亦然）、statd
（文件锁定）和 mountd（装入请求）。

pNFS

并行 NFS，属于 NFSv4 的一种协议扩展。任何 pNFS 客户端都可以直接访问 NFS 服务器上的数据。

28.2 安装 NFS 服务器

NFS 服务器软件不会默认安装。如果您按照第 28.3 节“配置 NFS 服务器”[380]中的说明配置 NFS 服务器，则系统会自动提示您安装所需的包。或者，使用 YaST 或 zypper 安装包 `nfs-kernel-server`。

与 NIS 一样，NFS 也是一个客户端/服务器系统。然而，一台计算机可以充当这两种角色 — 它可以通过网络提供文件系统（导出），也可以从其他主机装入文件系统（导入）。

28.3 配置 NFS 服务器

可通过 YaST 配置 NFS 服务器或手动配置它。NFS 还可与 Kerberos 结合来进行身份验证。

28.3.1 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。服务器还可为组的所有成员提供应用程序，而无需在每台主机上本地安装应用程序。

要设置此类服务器，请继续执行以下步骤：

过程 28.1 设置 NFSv3 服务器

- 1 启动 YaST 并选择 **网络服务 > NFS 服务器**；请参见图 28.1 “NFS 服务器配置工具”[381]。系统会提示您安装其他软件。

图 28.1 NFS 服务器配置工具



- 2 激活启动单选按钮。
- 3 如果防火墙在您的系统 (SuSEfirewall2) 中处于活动状态，请选中在防火墙中打开端口。YaST 会针对 NFS 服务器更改其配置，方法是启用 `nfs` 服务。
- 4 请将启用 NFSv4 复选框保留为禁用状态。
- 5 如果您需要安全访问服务器，请单击启用 GSS 安全性。先决条件是您的域中安装了 Kerberos 并且服务器和客户端都已采用 Kerberos 系统。单击下一步。
- 6 单击对话框上半部分中的添加目录以导出您的目录。
- 7 如果您尚未配置允许的主机，系统会自动弹出另一个对话框及相应的选项，供您输入客户端信息。输入主机通配符（通常您可以保留默认值不变）。

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 * 表示所有计算机都能访问服务器）和 IP 网络。

8 单击完成以完成配置。

28.3.1.1 为 NFSv4 客户端导出

对于固定的 NFSv4 客户端集合，可以导出的目录有两种，一是作为伪 root 文件系统的目录，一是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，为相同客户端导出的所有文件系统在其下各就各位。对于一个或一组客户端，服务器上只有一个目录可以配置为伪 root 目录以供导出。对于此客户端，通过将它们绑定到伪 root 目录中现有的子目录可以导出多个目录。

例如，假定选择目录 `/exports` 作为能访问服务器的所有客户端的伪 root 目录。然后将其添加到所导出目录的列表，并确保为此目录输入的选项包含 `fsid=0`。如果有另一个目录 `/data` 也需要通过 NFSv4 导出，请将此目录同样添加到该列表。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 *Bindmount 目标* 中。

要将服务器设置为导出 NFSv4 客户端目录，请使用过程 28.1, “设置 NFSv3 服务器” [380] 中的一般指南，但以下步骤需要更改：

- 1 在第一个对话框中，选中 *启用 NFSv4*。
- 2 在第一个对话框中输入适当的 NFSv4 域名。

请确保名称与访问此特定服务器的任何 NFSv4 客户端的 `/etc/idmapd.conf` 文件中的名称相同。此参数用于（服务器和客户机上）NFSv4 支持所需的 `idmapd` 守护程序。如果没有特殊要求，请将它保留为 `localdomain`（默认值）。

单击下一步后，显示的对话框包含两个部分。上半部分包含两列，名为 *目录* 和 *绑定装入目标*。服务将立即可用。

- 3 单击对话框上半部分中的 *添加目录* 以导出您的目录，并单击 *确定* 进行确认。
- 4 在 *主机通配符文本* 字段和选项中输入主机名。

在选项文本字段中，将 `fsid=0` 纳入以逗号分隔的选项列表中，以将目录配置为伪 `root` 目录。如果此目录应该绑定到一个已配置的伪 `root` 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。

Bindmount 目标列不可直接编辑，而是概要列出目录及其性质。

5 单击完成以完成配置。

28.3.1.2 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 `*` 表示所有计算机都能访问服务器）和 IP 网络。

图 28.2 “用 NFSv2 和 v3 导出目录” [383]中显示了此对话框。关于这些选项的详细描述，请参见 `man exports`。单击完成以完成配置。

图 28.2 用 NFSv2 和 v3 导出目录

28.3.1.3 并存的 v3 和 v4 导出

NFSv3 和 NFSv4 导出可以在一台服务器上并存。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。

考虑第 28.3.1.1 节“为 NFSv4 客户端导出”[382]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。

28.3.2 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`。要启动或重启服务，请运行命令 `rcnfsserver restart`。如果在 `/etc/sysconfig/nfs` 中配置了 NFSv4，这还将启动 `rpc.idmapd`。NFS 服务器依赖于运行的 RPC 端口映射器。所以，还请使用 `rcrpcbind restart` 启动或重启端口映射器服务。

28.3.2.1 用 NFSv4 导出文件系统

NFSv4 是 SUSE Linux Enterprise Server 上可用的 NFS 协议的最新版本。配置 NFSv4 导出的目录的过程与先前的 NFS 版本略有不同。

`/etc/exports`

`/etc/exports` 文件包含项列表。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,crossmnt)
/export/data 192.168.1.2(rw,bind=/data,sync)
```

在此，使用 IP 地址 192.168.1.2 标识允许的客户端。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 (@my-hosts)。

指定 fsid=0 的目录是特殊的。它是所导出的文件系统的 root，有时称为伪 root 文件系统。该目录还必须具有 crossmnt，以可以使用 NFSv4 正确操作。通过 NFSv4 导出的所有其他目录必须装入到该点下面。如果要导出不在该导出 root 目录下的目录，则需要将其绑定到导出树中。可以使用 bind= 语法进行该操作。

在上述示例中，/data 不在 /export 下，因此导出 /export/data，并指定 /data 目录应绑定到该名称。目录 /export/data 必须存在，通常应为空。

当从该服务器装入客户端时，应只是装入 servername:/ 而不是 servername:/export。无需同时装入 servername:/data，因为它将在装入 servername:/ 的目录下自动显示。

/etc/sysconfig/nfs

/etc/sysconfig/nfs 文件包含一些决定 NFSv4 服务器守护程序行为的参数。务必将参数 NFS4_SUPPORT 设置为 yes。NFS4_SUPPORT 决定 NFS 服务器是否支持 NFSv4 导出和客户端。

/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 的映射并答复客户端。它必须同时在服务器和客户端上针对 NFSv4 运行，因为 NFSv4 仅将名称用于通讯。

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身份验证机制来实现。

对于客户端和服务端，必须在 /etc/idmapd.conf 文件中将参数 Domain 设为相同值。如果您不确定，请在服务器和客户端文件中将域保留为 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
```

关于更多参考，请阅读 `idmapd` 和 `idmapd.conf` 的手册页：`man idmapd` 和 `man idmapd.conf`。

启动和停止服务

更改 `/etc/exports` 或 `/etc/sysconfig/nfs` 后，通过 `rcnfsserver restart` 启动或重新启动 NFS 服务器服务。更改 `/etc/idmapd.conf` 后，使用 `killall -HUP rpc.idmapd` 命令重新装载配置文件。

如果 NFS 服务必须在引导时启动，则运行 `chkconfig nfsserver on` 命令。

28.3.2.2 用 NFSv2 和 NFSv3 导出文件系统

这部分特定于 NFSv3 和 NFSv2 导出。请参见第 28.3.1.1 节“为 NFSv4 客户端导出”[382]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 地址可使用通配符替换为一个或一组客户端名称甚或网络组（如 `*.abc.com`）。

有关所有选项及其含义的详细说明，请参见 `exports` 的手册页 (`man exports`)。

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。

28.3.3 采用 Kerberos 的 NFS

要对 NFS 使用 Kerberos 身份验证，必须启用 GSS 安全性。在初始 YaST“NFS 服务器”对话框中选择启用 GSS 安全。必须具有一个有效的 Kerberos 服务器才能使用此功能。YaST 不会设置服务器，而是仅使用所提供的功能。如果希望使用 Kerberos 进行身份验证，则除了 YaST 配置外，还必须首先至少完成以下步骤，才能运行 NFS 配置：

- 1 请确保服务器和客户端都在同一 Kerberos 域中。它们必须访问相同的 KDC（密钥分发中心）服务器并共享其 `krb5.keytab` 文件（在任何计算机上的默认位置是 `/etc/krb5.keytab`）。有关 Kerberos 的更多信息，请参见第 6 章 *Network Authentication with Kerberos* (↑安全指南)。
- 2 在客户端上用 `rcgssd start` 启动 `gssd` 服务。
- 3 在客户端上用 `rcsvcgssd start` 启动 `svcgssd` 服务。

有关配置采用 Kerberos 的 NFS 的更多信息，请参见第 28.5 节“更多信息”[390] 中的链接。

28.4 配置客户端

要将主机配置为 NFS 客户端，无需安装其他软件。将默认安装所有需要的包。

28.4.1 使用 YaST 导入文件系统

授权用户可以用 YaST NFS 客户端模块从 NFS 服务器将 NFS 目录装入本地文件树。按如下所示继续：

过程 28.2 导入 NFS 目录

- 1 启动 YaST NFS 客户端模块。

- 2 单击 *NFS* 共享选项卡中的 **添加**。输入 NFS 服务器的主机名、要导入的目录以及用于装入此目录的本地安装点。
- 3 若要使用防火墙并允许从远程计算机访问服务，请启用 *NFS* 设置选项卡中的 **打开防火墙中的端口**。防火墙状态将显示在复选框旁边。
- 4 使用 NFSv4 时，请确保已选中 **启用 NFSv4** 复选框，并且 *NFSv4* 域名包含 NFSv4 服务器所用的值。默认域为 `localdomain`。
- 5 单击 **确定保存更改**。

配置写入 `/etc/fstab`，并将装入指定的文件系统。当您稍后启动 YaST 配置客户端时，它还将读取此文件中的现有配置。

28.4.2 手动导入文件系统

手动从 NFS 服务器导入文件系统的先决条件是运行 RPC 端口映射器。作为 `root` 用户输入 `rcrpcbind start` 来启动它。然后就可以使用 `mount` 将远程文件系统像本地分区那样装入文件系统中：

```
mount host:remote-path local-path
```

例如要从 `nfs.example.com` 计算机导入用户目录，使用：

```
mount nfs.example.com:/home /home
```

28.4.2.1 使用自动装入服务

`autofs` 守护程序可用于自动装入远程文件系统。请在 `/etc/auto.master` 文件中添加以下条目：

```
/nfsmounts /etc/auto.nfs
```

如果 `auto.nfs` 文件正确填充，`/nfsmounts` 目录将作为客户端上所有 NFS 装入的 `root` 目录。文件名为 `auto.nfs` 是为了方便，也可以选择其他名称。在 `auto.nfs` 中为所有 NFS 装入添加条目，如下所示：

```
localdata -fstype=nfs server1:/data  
nfs4mount -fstype=nfs4 server2:/
```

以 root 身份用 `rcautoofs 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 `autoofs` 服务时编辑 `/etc/auto.master` 文件，则必须用 `rcautoofs restart` 重新启动自动装入程序才能使更改生效。

28.4.2.2 手动编辑 `/etc/fstab`

通常，`/etc/fstab` 中的 NFSv3 装入项如下：

```
nfs.example.com:/data /local/path nfs rw,noauto 0 0
```

也可以将 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 `nfs.example.com:` 后面用 `/` 指定远程文件系统。`/etc/fstab` 中 NFSv4 装入的示例行如下所示：

```
nfs.example.com:/ /local/pathv4 nfs4 rw,noauto 0 0
```

`noauto` 选项可禁止在启动时自动装入文件系统。如果您要手动安装各文件系统，可以缩短只指定安装点的安装命令：

```
mount /local/path
```

请注意，如果您没有输入 `noauto` 选项，系统的初始化脚本将在启动时处理这些文件系统的装入。

28.4.3 并行 NFS (pNFS)

NFS 是最老的协议之一，开发于上世纪八十年代。因此，如果您要共享小文件，NFS 通常能够满足需求。但是，如果您要传送大文件或大量的客户端要访问数据，则 NFS 会陷入瓶颈并且严重影响系统性能。这是因为文件迅速变大，而以太网的相关速度没有完全跟上。

当您请求“普通”NFS 服务器中的文件时，服务器会查找文件元数据、收集所有数据并通过网络将数据传送到您的客户端。但是，无论文件的大小如何，性能瓶颈都会凸显出来：

- 如果是小文件，则大部分时间都花在收集元数据上
- 如果是大文件，则大部分时间花在将数据从服务器传送到客户端上

pNFS 或并行 NFS 则突破了此种限制，因为它将文件系统元数据从数据位置分离出来。因此，pNFS 需要两类服务器：

- 一个 *metadata* 或控制服务器，用于处理所有与数据无关的通讯
- 一或多个储存服务器，用于储存数据

元数据和储存服务器组成单独一个逻辑 NFS 服务器。当客户端要读取或写入时，元数据服务器会告诉 NFSv4 客户端使用哪个储存服务器访问文件块。客户端可以直接访问该服务器上的数据。

SUSE Linux Enterprise 仅在客户端上支持 pNFS。

28.4.3.1 使用 YaST 配置 pNFS 客户端

请执行过程 28.2, “导入 NFS 目录” [387]中所述的步骤，但选中 *pNFS (v4.1)* 复选框以及可选的 *NFSv4* 共享。YaST 会执行所有必要步骤，并且会在文件 `/etc/exports` 中写入全部所需选项。

28.4.3.2 手动配置 pNFS 客户端

请参阅第 28.4.2 节 “手动导入文件系统” [388]着手配置。大多数配置通过 NFSv4 服务器完成。对于 pNFS，唯一的区别是将 `minorversion` 选项和元数据服务器 `MDS_服务器` 添加到您的 `mount` 命令：

```
mount -t nfs4 -o minorversion=1 MDS_SERVER MOUNTPOINT
```

为方便调试，请更改 `/proc` 文件系统中的值：

```
echo 32767 > /proc/sys/sunrpc/nfsd_debug
echo 32767 > /proc/sys/sunrpc/nfs_debug
```

28.5 更多信息

除了 `exports`、`nfs` 和 `mount` 的手册页外，还可在 `/usr/share/doc/packages/nfsidmap/README` 中找到关于配置 NFS 服务器和客户端的信息。有关更多联机文档，请参见以下网站：

- 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 的描述，请参见 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，请参考 Linux NFSv4 FAQ [<http://www.citi.umich.edu/projects/nfsv4/linux/faq/>]（Linux NFSv4 常见问题）。

文件同步

现今，很多人都在同时使用若干台计算机——一台在家用，一台或多台在办公室用，还可能会在途中使用便携式计算机、平板电脑或智能手机。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。

29.1 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。

29.1.1 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安装源，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安装源，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。冲突仅显示在客户端上并在客户端上解决。

29.1.2 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。这不仅适用于文本文件，还适用于二进制文件。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。

29.2 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。

29.2.1 客户端/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，所有客户端都通过中央服务器来同步文件。所有客户端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 实际在客户端模式下工作，但任何客户端都可用作服务器。

29.2.2 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。

29.2.3 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。

29.2.4 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，只有一个客户端会受影响。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。为了安全起见，还可以使用 RCS 之类的分版本系统。

29.2.5 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。

29.2.6 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。

29.2.7 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 还要求服务器为安装源准备额外的空间。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。

29.2.8 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。

29.2.9 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。用户应该了解安装源和本地数据之间如何交互。对数据的更改首先要在本地与安装源合并。使用命令 `cvs update` 可完成上述操作。然后必须使用命令 `cvs commit` 将数据发回安装源。一旦了解了此过程，新手也就能毫不费力地使用CVS了。

29.2.10 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（安全外壳）使用，从而防止遭受此类攻击。应避免通过rsh（远程外壳）运行CVS。也不建议在不安全的网络中使用*pserver*机制访问CVS。

29.2.11 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 29.1 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
客户端/服务器	客户端-服务器	客户端-服务器
可移植性	Lin、Un*x、Win	Lin、Un*x、Win

	CVS	rsync
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	++	+

29.3 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，因为文件的所有变体都永久储存在 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。

29.3.1 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 安装源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端上都安装了 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。在客户端选择或创建目录，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
```

29.3.2 使用 CVS

现在，在所有主机上都可以使用 `cvsco synchome` 将该同步安装源签出。该操作将在客户端上创建新的子目录 `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安装源中。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，则需要签出同步安装源（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

本地文件与安装源中的当前版本冲突。

?

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。

29.4 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 Web 服务器的完整目录树的服务器，这些 Web 服务器定期镜像到 DMZ 中的 Web 服务器。

29.4.1 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外壳，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。

随后可以从客户端系统测试传送。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。

29.5 有关详细信息

CVS

有关 CVS 的重要信息可以在主页 <http://www.cvshome.org> 中找到。

rsync

有关 `rsync` 的重要信息，请参见手册页 `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` 的网站 <http://rsync.samba.org/> 上可以找到关于该项目的最新消息。

Apache HTTP 服务器

根据 <http://www.netcraft.com/> 上的调查，Apache HTTP 服务器 (Apache) 所占的市场份额超过了 50%，它是世界上使用最为广泛的一种 Web 服务器。由 Apache 软件基金会 (<http://www.apache.org/>) 开发的 Apache 适用于大多数操作系统。SUSE® Linux Enterprise Server 包含 Apache 版本 2.2。本章将介绍如何安装、配置和设置 Web 服务器；如何使用 SSL、CGI 和其他模块；以及如何对 Apache 进行查错。

30.1 快速入门

借助本节，快速设置并启动 Apache。您必须是 root 才能安装和配置 Apache。

30.1.1 要求

在尝试设置 Apache Web 服务器之前，请确保满足以下要求：

1. 计算机的网络配置正确。有关该主题的详细信息，请参见第 21 章 *基本联网知识* [239]。
2. 通过与时间服务器同步来维护计算机的准确系统时间。这一点是必需的，因为 HTTP 协议的多个部分依赖于正确的时间。请参见第 23 章 *使用 NTP 同步时间* [301] 来了解该主题的更多信息。
3. 将安装最新的安全更新。如果存在疑问，请运行 YaST 联机更新。

4. 默认 Web 服务器端口 (80) 将在防火墙中打开。为此，配置 SuSEFirewall2 以允许外部区域中的服务 *HTTP* 服务器。这可以使用 YaST 完成。有关详细信息，请参见第 15.4.1 节 “Configuring the Firewall with YaST” (第 15 章 *Masquerading and Firewalls*, ↑安全指南)。

30.1.2 安装

默认情况下，在 SUSE Linux Enterprise Server 上不安装 Apache。要用“即装即用”的标准预定义配置来安装它，请按如下所示继续：

过程 30.1 用默认配置安装 Apache

- 1 启动 YaST，然后选择软件 > 软件管理。
- 2 选择过滤器 > 模式，然后选择服务器功能中的 *Web* 和 *LAMP* 服务器。
- 3 确认安装相关的包来完成安装进程。

安装包括多处理模块 `apache2-prefork` 和 `PHP5` 模块。有关模块的详细信息，请参见第 30.4 节 “安装、激活和配置模块” [421]。

30.1.3 开始

可以自动在引导时启动 Apache 或手动启动它。

过程 30.2 自动启动 Apache

- 1 要确保 Apache 在引导期间自动在运行级别 3 和 5 启动，请执行以下命令：

```
chkconfig -a apache2
```

- 2 或者启动 YaST，然后选择系统 > 系统服务（运行级别）。
- 3 搜索 *apache2* 并启用该服务。

Web 服务器将立即启动。

- 4 单击完成以保存更改。

系统配置为在引导期间自动在运行级别 3 和 5 启动 Apache。

有关 SUSE Linux Enterprise Server 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 9.2.3 节“使用 YaST 配置 System Services (Runlevel)” [103]。

要使用外壳手动启动 Apache，请运行 `rcapache2 start`。

过程 30.3 检查 Apache 是否正在运行

如果在启动 Apache 时没有收到错误消息，这通常表示 Web 服务器正在运行。测试 Apache 是否正在运行：

- 1 启动浏览器，然后打开 <http://localhost/>。

如果 Apache 已启动并正在运行，您将看到一个测试页，指示“它正在运行！”。

- 2 如果看不到此页面，请参见第 30.8 节“查错” [438]。

既然 Web 服务器已在运行，因此可以添加您自己的文档、根据需要调整配置或通过安装模块来添加功能。

30.2 配置 Apache

SUSE Linux Enterprise Server 提供两个配置选项：

- 手动配置 Apache [408]
- 使用 YaST 配置 Apache [413]

手动配置可提供更详细的信息，但没有 YaST GUI 方便。

重要：配置更改后重新装载或重新启动 Apache

大多数配置更改需要重新装载（有些还需要重新启动）Apache 后才能生效。使用 `rcapache2 reload` 或第 30.3 节“启动和停止 Apache” [418] 中所述的某个重新启动选项手动重新装载 Apache。

如果用 YaST 配置 Apache，则可通过将 *HTTP* 服务设置为已启用（如第 30.2.3.2 节“HTTP 服务器配置” [417] 中所述）来自动执行此操作。

30.2.1 Apache 配置文件

本部分概述了 Apache 配置文件。如果使用 YaST 进行配置，则不需要使用这些文件；但如果以后要切换到手动配置，则此信息可能有用。

Apache 配置文件可在两个不同位置处获取：

- `/etc/sysconfig/apache2` [406]
- `/etc/apache2/` [406]

30.2.1.1 `/etc/sysconfig/apache2`

`/etc/sysconfig/apache2` 控制 Apache 的某些全局设置，例如要装载的模块、要包含的其他配置文件、启动服务器时应同时启动的标志，以及应添加到命令行的标志。此文件中的每个配置选项都有详细记录，因此在此不再描述。对于一般用途的 Web 服务器，`/etc/sysconfig/apache2` 中的设置应足以满足所有配置需要。

30.2.1.2 `/etc/apache2/`

`/etc/apache2/` 托管 Apache 的所有配置文件。下面描述了每个文件的用途。每个文件均包含几个配置选项（也称为指令）。这些文件中的每个配置选项都有详细记录，因此在此不再描述。

Apache 配置文件按如下所示组织：

```
/etc/apache2/
|
|- charset.conv
|- conf.d/
|   |
|   |- *.conf
|
|- default-server.conf
|- errors.conf
|- httpd.conf
|- listen.conf
|- magic
|- mime.types
|- mod_*.conf
|- server-tuning.conf
|- ssl.*
```



```
| - ssl-global.conf
| - sysconfig.d
|   |
|   | - global.conf
|   | - include.conf
|   | - loadmodule.conf . .
|
| - uid.conf
| - vhosts.d
|   | - *.conf
```

/etc/apache2/ 中的 Apache 配置文件

charset.conv

指定要用于不同语言的字符集。不要编辑此文件。

conf.d/*.conf

其他模块添加的配置文件。可在需要时将这些配置包含进虚拟主机配置。有关示例请参见 `vhosts.d/vhost.template`。如此操作后，可以为不同的虚拟主机提供不同的模块集。

default-server.conf

具有合理默认值的所有虚拟主机的全局配置。除了更改值之外，还可以使用虚拟主机配置来覆盖它们。

errors.conf

定义 Apache 如何响应错误。要为所有虚拟主机自定义这些消息，请编辑此文件。否则在您的虚拟主机配置中覆盖这些指令。

httpd.conf

主 Apache 服务器配置文件。请勿更改此文件。它主要包含 `include` 语句和全局设置。重写此处列出的相关配置文件中的全局设置。更改您的虚拟主机配置中的特定于主机的设置（例如文档根目录）。

listen.conf

将 Apache 绑定到特定的 IP 地址和端口。基于名称的虚拟主机也在此处配置。有关细节，请参见“基于名称的虚拟主机”一节 [410]。

magic

`mime_magic` 模块的数据帮助 Apache 自动确定 MIME 类型的未知文件。不要更改此文件。

`mime.types`

MIME 类型可由系统识别（它实际上是一个指向 `/etc/mime.types` 的链接）。不要编辑此文件。如果需要添加此处没有列出的 MIME 类型，那么请将它们添加到 `mod_mime-defaults.conf`。

`mod_*.conf`

默认情况下安装的模块的配置文件。有关细节，请参见第 30.4 节“安装、激活和配置模块”[421]。注意，可选模块的配置文件储存在目录 `conf.d` 中。

`server-tuning.conf`

包含不同 MPM（请参见第 30.4.4 节“多处理模块”[425]）的配置指令以及控制 Apache 性能的常规配置选项。在此处更改时，请对 Web 服务器进行合理的测试。

`ssl-global.conf` 和 `ssl.*`

全局 SSL 配置和 SSL 证书数据。有关细节，请参见第 30.6 节“使用 SSL 设置安全性 Web 服务器”[430]。

`sysconfig.d/*.conf`

从 `/etc/sysconfig/apache2` 自动生成的配置文件。请勿更改这些文件，而应编辑 `/etc/sysconfig/apache2`。不要在此目录中放置其他配置文件。

`uid.conf`

指定运行 Apache 的用户和组 ID。不要更改此文件。

`vhosts.d/*.conf`

虚拟主机配置应位于此处。该目录包含使用和不使用 SSL 的虚拟主机的模板文件。该目录中以 `.conf` 结尾的所有文件均自动包含在 Apache 配置中。有关详细信息，请参见第 30.2.2.1 节“虚拟主机配置”[409]。

30.2.2 手动配置 Apache

手动配置 Apache 包括作为 `root` 用户来编辑纯文本配置文件。

30.2.2.1 虚拟主机配置

术语*虚拟主机*指的是 Apache 在一台物理计算机上为多个统一资源标识符 (URI) 提供服务的能力。这意味着在一台物理计算机上的一个 Web 服务器可以运行几个域（例如 `www.example.com` 和 `www.example.net`）。

通常的做法是使用虚拟主机来节省管理精力（只需维护一个 Web 服务器即可）和硬件费用（每个域不需要专用的服务器）。虚拟主机可以是基于名称、基于 IP 或基于端口的。

要列出所有现有虚拟主机，请使用命令 `httpd2 -S`。这将输出一个列表，显示默认服务器和所有虚拟主机以及它们的 IP 地址和侦听端口。此外，该列表还针对每个虚拟主机包含一项，显示其在配置文件中的位置。

可以通过 YaST（如“虚拟主机”一节 [415]中所述）或通过手动编辑配置文件来配置虚拟主机。默认情况下，SUSE Linux Enterprise Server 中的 Apache 在 `/etc/apache2/vhosts.d/` 中为每个虚拟主机准备了一个配置文件。该目录中扩展名为 `.conf` 的所有文件均会自动包含到配置中。虚拟主机的基本模板将在目录 `vhost.template` 或 `vhost-ssl.template` 中提供，以用于带有 SSL 支持的虚拟主机。

提示：始终创建虚拟主机配置

建议您始终创建虚拟主机配置文件，即使您的 Web 服务器仅主管一个域。这样不但可以将特定于域的配置保存在一个文件中，还可以只需移动、删除或重命名虚拟主机的配置文件就能始终回退到有效的基本配置。因此，还应该为每个虚拟主机创建单独的配置文件。

使用基于名称的虚拟主机时，建议设置将在域名与虚拟主机配置不匹配时使用的默认配置。默认虚拟主机即最先装载其配置的虚拟主机。由于配置文件的装载顺序取决于文件名，因此请以下划线字符 (`_`) 作为默认虚拟主机配置的文件名开头，以确保最先装载它（例如：`_default_vhost.conf`）。

`<VirtualHost></VirtualHost>` 块保存适用于特定域的信息。当 Apache 接收到客户端对某已定义虚拟主机的请求时，将使用此部分包含的指令。几乎所有指令均可用在虚拟主机环境中。请参见 <http://httpd.apache.org/docs/2.2/mod/quickreference.html> 来获取有关 Apache 的配置指令的进一步信息。

基于名称的虚拟主机

使用基于名称的虚拟主机，每个IP地址能服务于多个网站。Apache使用客户端发送的HTTP报头中的主机字段来将请求连接到某个虚拟主机声明中匹配的ServerName项。如果找不到匹配的ServerName，则默认使用第一个指定的虚拟主机。

指令NameVirtualHost告诉Apache在哪个IP地址以及（可选）哪个端口上侦听客户端发出的在HTTP报头中包含域名的请求。此选项是在配置文件/etc/apache2/listen.conf中配置的。

第一个自变量是完全限定的域名，但建议使用IP地址。第二个自变量是可选的端口。默认情况下，使用端口80并通过Listen指令进行配置。

IP地址和端口号都可以使用通配符*来接收所有接口上的请求。IPv6地址必须括在方括号中。

例 30.1 基于名称的VirtualHost项的变体

```
# NameVirtualHost IP-address[:Port]
NameVirtualHost 192.168.3.100:80
NameVirtualHost 192.168.3.100
NameVirtualHost *:80
NameVirtualHost *
NameVirtualHost [2002:c0a8:364::]:80
```

打开VirtualHost标记将使先前使用NameVirtualHost声明的IP地址（或全限定域名）在基于名称的虚拟主机配置中显示为参数。之前使用NameVirtualHost指令声明的端口号是可选的。

允许使用通配符*代替IP地址。该语法仅当和NameVirtualHost *中的通配符一起使用时才有效。当使用IPv6地址时，地址必须括在方括号中。

例 30.2 基于名称的VirtualHost指令

```
<VirtualHost 192.168.3.100:80>
...
</VirtualHost>

<VirtualHost 192.168.3.100>
...
</VirtualHost>

<VirtualHost *:80>
...
</VirtualHost>
```

```
<VirtualHost *>
    ...
</VirtualHost>

<VirtualHost [2002:c0a8:364::]>
    ...
</VirtualHost>
```

基于 IP 的虚拟主机

这种备选的虚拟主机配置要求为计算机设置多个 IP。Apache 的一个实例储存多个域，并为每个域指派一个不同的 IP。

物理服务器必须为每个基于 IP 的虚拟主机指定一个 IP 地址。如果计算机没有多个网卡，也可以使用虚拟网络接口（IP 别名）。

以下示例显示 Apache 在 IP 为 192.168.3.100 且主管其他两个 IP 为 192.168.3.101 和 192.168.3.102 的域的计算机上运行的情况。请为每个虚拟服务器指定一个单独的 VirtualHost 块。

例 30.3 基于 IP 的 VirtualHost 指令

```
<VirtualHost 192.168.3.101>
    ...
</VirtualHost>

<VirtualHost 192.168.3.102>
    ...
</VirtualHost>
```

在此，VirtualHost 指令只针对除 192.168.3.100 以外的接口。当还为 192.168.3.100 配置 Listen 指令时，必须创建单独的、基于 IP 的虚拟主机才能应答对该接口的 HTTP 请求，否则应用在默认服务器配置 (/etc/apache2/default-server.conf) 中找到的指令。

基本虚拟主机配置

每个虚拟主机配置中至少要有以下指令，这样才能设置虚拟主机。请参见 /etc/apache2/vhosts.d/vhost.template 获取更多选项。

```
ServerName
    主机所在的全限定域名。
```

DocumentRoot

Apache 应该为此主机提供文件的目录路径。出于安全考虑，在默认情况下禁止访问整个文件系统，所以必须在目录容器中显示地解锁此目录。

ServerAdmin

服务器管理员的电子邮件地址。例如，此地址将显示在 Apache 创建的错误页面上。

ErrorLog

该虚拟主机的错误日志文件。尽管不必为每个虚拟主机创建单独的错误日志文件，但是通常建议执行此操作，因为这样能使错误调试变得容易些。/var/log/apache2/ 是 Apache 日志文件的默认目录。

CustomLog

该虚拟主机的访问日志文件。尽管不必为每个虚拟主机创建单独的访问日志文件，但是通常建议执行此操作，因为这样可单独分析每个主机的访问统计数字。/var/log/apache2/ 是 Apache 日志文件的默认目录。

综上所述，出于安全考虑，在默认情况下禁止访问整个文件系统。因此，明确解除已放置 Apache 应提供的文件所在目录的锁定，例如 DocumentRoot：

```
<Directory "/srv/www/www.example.com/htdocs">
    Order allow,deny
    Allow from all
</Directory>
```

完整的配置文件外观如下所示：

例 30.4 基本 VirtualHost 配置

```
<VirtualHost 192.168.3.100>
    ServerName www.example.com
    DocumentRoot /srv/www/www.example.com/htdocs
    ServerAdmin webmaster@example.com
    ErrorLog /var/log/apache2/www.example.com_log
    CustomLog /var/log/apache2/www.example.com-access_log common
    <Directory "/srv/www/www.example.com/htdocs">
        Order allow,deny
        Allow from all
    </Directory>
</VirtualHost>
```

30.2.3 使用 YaST 配置 Apache

要使用 YaST 配置 Web 服务器，请启动 YaST，并选择 *网络服务 > HTTP 服务器*。第一次启动此模块时，*HTTP 服务器向导* 会启动，提示您做出一些有关服务器管理的基本决定。完成向导后，在您每次调用 *HTTP 服务器* 模块时，*HTTP 服务器配置* 对话框都会启动。有关详细信息，请参见第 30.2.3.2 节“HTTP 服务器配置”[417]。

30.2.3.1 HTTP 服务器向导

HTTP 服务器向导包括五个步骤。在对话框的最后一步中，您可以进入专家配置方式进行更特定的设置。

网络设备选择

在这里，指定 Apache 用以侦听进来的请求的网络接口和端口。可以选择现有网络接口及其各自 IP 地址的任意组合。可以使用其他服务未预留的所有三个范围内的端口（公认端口、注册端口和动态或私用端口）。默认设置是在端口 80 上侦听所有网络接口（IP 地址）。

选中 *打开防火墙中的端口*，在防火墙中打开 Web 服务器侦听的端口。要使 Web 服务器在网络（LAN、WAN 或公共因特网）中可用，这样做是必要的。仅在测试时不必对 Web 服务器进行外部访问的情况下，关闭端口是有用的。如果有多个网络接口，请单击 *防火墙细节...* 以指定要在哪些接口上打开端口。

单击 *下一步* 继续配置。

模块

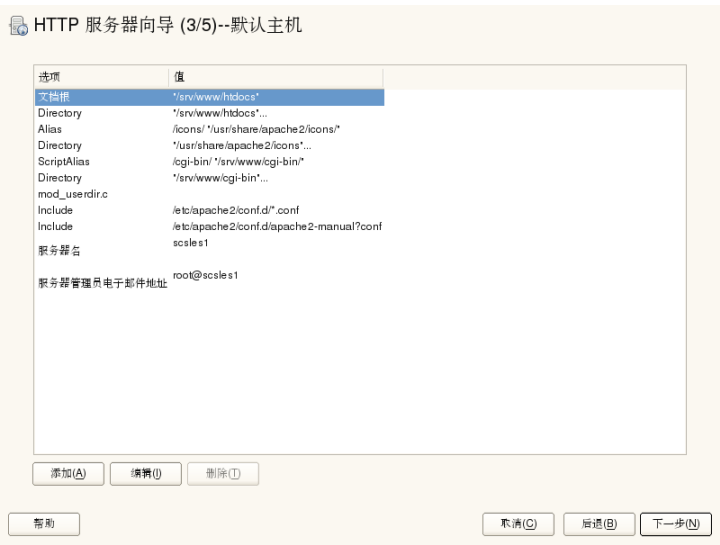
模块配置选项允许激活或停用 Web 服务器应支持的脚本语言。要激活或停用其他模块，请参见“服务器模块”一节 [418]。单击 *下一步* 进入下一个对话框。

默认主机

该选项与默认的 Web 服务器相关。正如第 30.2.2.1 节“虚拟主机配置”[409]中所述，Apache 可以在一台物理计算机上为多台虚拟主机提供服务。配置文件中首先声明的虚拟主机通常被称为 *默认主机*。每个虚拟主机都将继承默认主机的配置。

要编辑主机设置（也称为指令），在表中选择适当的项，然后单击编辑。要添加新指令，请单击添加。要删除指令，请选择该主机，然后单击删除。

图 30.1 HTTP 服务器向导：默认主机



这里是服务器默认设置的列表：

Document Root

Apache 为此主机提供文件的目录路径。`/srv/www/htdocs` 是默认位置。

Alias

借助 Alias 指令，URL 可以被映射到物理文件系统位置。这意味着可以通过对某路径进行 URL 别名判别来访问该路径（即使是在文件系统中文档根目录之外的路径）。

默认的 SUSE Linux Enterprise Server Alias/icons 指向显示在目录索引视图中的 Apache 图标所在的 `/usr/share/apache2/icons`。

ScriptAlias

和 Alias 指令类似，ScriptAlias 指令将 URL 映射到文件系统位置。不同之处在于 ScriptAlias 将目标目录指定为 CGI 位置，意味着 CGI 脚本应该在此位置执行。

Directory

设置 `Directory` 后，便可包含一组只能应用于指定目录的配置选项。

目录 `/srv/www/htdocs`、`/usr/share/apache2/icons` 和 `/srv/www/cgi-bin` 的访问和显示选项是在此处配置的。不需要更改默认值。

Include

使用 `include`，还可指定其他配置文件。已预配置两个 `Include` 指令：`/etc/apache2/conf.d/` 是包含与外部模块一起提供的配置文件的目录。使用此指令可包含该目录中以 `.conf` 结尾的所有文件。使用第二个指令可包含 `/etc/apache2/conf.d/apache2-manual.conf`（`apache2-manual` 配置文件）。

Server Name

这指定了客户端用来联系 Web 服务器的默认 URL。使用完全限定的域名 (FQDN) 到达 Web 服务器（位于 `http://FQDN/`）或其 IP 地址。不能在此处随意选择名称 — 服务器在此名称下必须是“已知”的。

Server Administrator E-Mail

服务器管理员的电子邮件地址。例如，此地址将显示在 Apache 创建的错误页面上。

完成默认主机步骤后，单击下一步继续完成配置。

虚拟主机

在本步骤中，向导显示已配置的虚拟主机（请参见第 30.2.2.1 节“虚拟主机配置”[409]）的列表。如果启动 YaST HTTP 向导前未进行手动更改，将不显示虚拟主机。

要添加主机，请单击添加以打开一个对话框，可在其中输入有关该主机的基本信息，如服务器名称、服务器内容根 (DocumentRoot) 和管理员电子邮件。服务器解析用来确定如何识别主机（基于名称或基于 IP）。通过更改虚拟主机 ID 指定名称或 IP 地址

单击下一步进入虚拟主机配置对话框的第二部分。

在虚拟主机配置的第二部分中，可以指定是否启用 CGI 脚本以及用于这些脚本的目录。还可启用 SSL。如果要启用，还必须指定证书的路径。请参见第 30.6.2 节“使用 SSL 配置 Apache”[435]了解有关 SSL 和证书的细节。使用目录索引选项，

可指定在客户端请求目录时所显示的文件（默认情况下为 `index.html`）。如果要更改此选项，请添加一个或多个文件名（用空格分隔）。使用启用公共 *HTML*，用户公共目录 (`~user/public_html/`) 的内容可显示在 `http://www.example.com/~user` 下的服务器上。

重要：创建虚拟主机

不能随意添加虚拟主机。如果使用基于名称的虚拟主机，必须在网络上解析每个主机名。如果使用基于 IP 的虚拟主机，则仅可向每个可用的 IP 地址指定一个主机。

摘要

这是本向导的最后一步。在此，确定 Apache 服务器启动的方式和时间：何时引导或手动引导。另请参见迄今为止所作配置的简短摘要。如果对设置满意，单击完成以完成配置。如果要进行更改，请单击后退直至显示所需的对话框。单击 *HTTP 服务器专家配置* 打开第 30.2.3.2 节“HTTP 服务器配置”[417]中所述的对话框。

图 30.2 HTTP 服务器向导：摘要



30.2.3.2 HTTP 服务器配置

*HTTP 服务器配置*对话框还允许您对配置进行比在向导（它只在您首次配置 Web 服务器时运行）中更多的调整。它由四个如下所述的选项卡组成。在此处更改的配置选项都不会立即生效，始终需要使用完成来确认更改从而使其生效。单击中止退出配置模块并丢弃所作更改。

监听端口和地址

在 *HTTP Service* 中，选择应该运行（启用）还是停止（禁用）Apache。在侦听端口中，添加、编辑或删除服务器可用的地址和端口。默认设置是在端口 80 上侦听所有接口。应始终选中打开防火墙中的端口，否则无法从外部访问 Web 服务器。仅在测试时不必对 Web 服务器进行外部访问的情况下，关闭端口是有用的。如果有多个网络接口，请单击*防火墙细节...*以指定要在哪些接口上打开端口。

使用*日志文件*查阅访问日志或错误日志。如果要测试配置，这很有用。该日志文件将在单独的窗口中打开，您还可从该窗口重新启动或重新装载 Web 服务器。有关详细信息，请参见第 30.3 节“启动和停止 Apache”[418]。这些命令将立即生效，并且其日志消息也会立即显示。

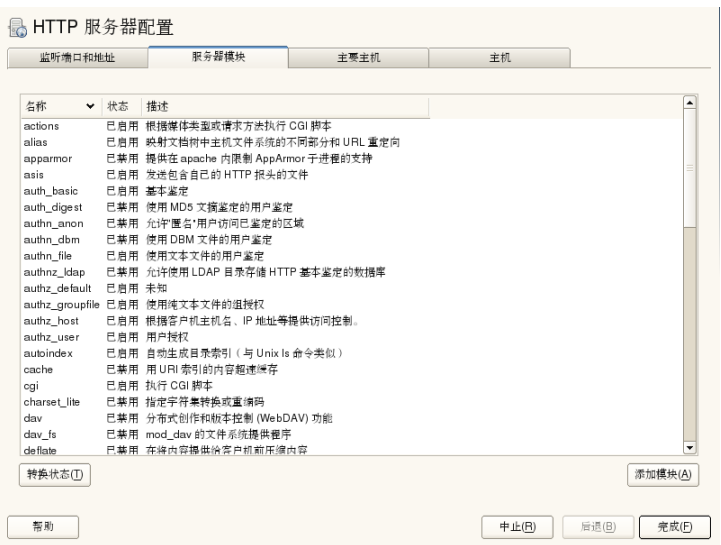
图 30.3 HTTP 服务器配置：侦听端口和地址



服务器模块

可以通过单击*切换状态*来更改 Apache2 模块的状态（启用或禁用）。单击*添加模块*可添加已安装但还未列出的新模块。要了解模块的更多信息，请参见第 30.4 节“安装、激活和配置模块”[421]。

图 30.4 HTTP 服务器配置：服务器模块



主要主机

这些对话框与上述对话框相同。请参见“默认主机”一节 [413]和“虚拟主机”一节 [415]。

30.3 启动和停止 Apache

如果使用 YaST 配置（如第 30.2.3 节“使用 YaST 配置 Apache”[413]中所述），则 Apache 在引导时在运行级别 3 和 5 启动，在运行级别 0、1、2 和 6 停止。您可以使用 YaST 的运行级别编辑器或命令行工具 `chkconfig` 更改此行为。

要在正在运行的系统上启动、停止或操作 Apache，请使用 `init` 脚本 `/usr/sbin/rcapache2`。有关 `init` 脚本的常规信息，请参见第 9.2.2 节“Init 脚本” [99]。`rcapache2` 命令使用以下参数：

`status`

请检查 Apache 是否已启动。

`start`

如果 Apache 未在运行，则启动它。

`startssl`

如果支持 SSL 的 Apache 未在运行，则启动它。有关 SSL 支持的详细信息，请参见第 30.6 节“使用 SSL 设置安全性 Web 服务器” [430]。

`stop`

通过终止父进程来停止 Apache。

`restart`

停止然后重新启动 Apache。如果 Web 服务器没有预先运行，则启动它。

`try-restart`

仅当 Apache 已在运行时才停止并重新启动它。

`reload` 或 `graceful`

通过建议所有生成的 Apache 进程在关闭之前首先完成其请求来停止 Web 服务器。每个进程终止时，会替换为一个新启动的进程，继而导致 Apache 完全“重新启动”。

提示：在生产环境中重新启动 Apache

要激活 Apache 配置更改而不致使连接中断，请使用 `rcapache2 reload` 命令。

`restart-graceful`

启动另一台用于立即处理所有进来的请求的 Web 服务器。Web 服务器的上一个实例将继续处理用 `GracefulShutdownTimeout` 配置的已定义时间段的所有现有请求。

`rcapache2 restart-graceful` 在升级到新版本或更改需要重新启动的配置选项时很有用。使用此选项确保将服务器停机时间减至最短。

需要设置 `GracefulShutdownTimeout`，否则 `restart-graceful` 将导致经常性重新启动。如果设置为零，该服务器将无限期地等待，直至所有剩余请求都全部完成。

如果原始 **Apache** 实例无法清除所有必需资源，则正常重新启动可能会失败。这种情况下，该命令将执行正常停止。

`stop-graceful`

在使用 `GracefulShutdownTimeout` 配置已定义的时间段后停止 Web 服务器，以便确保可以完成现有请求。

需要设置 `GracefulShutdownTimeout`，否则 `stop-graceful` 将导致经常性重新启动。如果设置为零，该服务器将无限期地等待，直至所有剩余请求都全部完成。

`configtest` 或 `extreme-configtest`

在不影响运行的 Web 服务器的情况下检查配置文件的语法。由于此检查是在服务器每次启动、重新装载或重新启动时强制执行的，所以通常不需要明确运行测试（如果发现配置错误，则 Web 服务器将不会启动、重新装载或重新启动）。`extreme-configtest` 选项将以 `nobody` 用户身份启动 Web 服务器，并实际装载该配置，因此可以检测出更多错误。请注意，尽管已装载此配置，但仍不能测试 SSL 设置，因为 `nobody` 不能读取 SSL 证书。

`probe`

探测重载的必要性（检查配置是否已更改）并向 `rcapache2` 命令建议应该使用的参数。

`server-status` 和 `full-server-status`

分别转储不全或完整状态屏幕。需要安装 `lynx` 或 `w3m` 并启用 `mod_status` 模块。此外，还必须将状态添加到文件 `/etc/sysconfig/apache2` 中的 `APACHE_SERVER_FLAGS`。

提示：其他标志

如果向 `rcapache2` 指定其他标志，则这些标志将传到 Web 服务器。

30.4 安装、激活和配置模块

Apache 软件是以模块化方式构建的：除某些核心任务外的所有功能都是通过模块处理的。到目前为止，即使是 HTTP 也是由模块（`http_core`）处理的。

Apache 模块可以在构建时编译进 Apache 二进制文件中或在运行时动态装载。请参见第 30.4.2 节“激活和取消激活”[422]以获取有关如何动态装载模块的详细信息。

Apache 模块可以划分为四个不同的类别：

基础模块

默认情况下，基础模块将编译到 Apache 中。SUSE Linux Enterprise Server 的 Apache 中仅编译了 `mod_so`（装载其他模块时需要）和 `http_core`。所有其他对象都可用作共享对象：它们可在运行时被包含，而不是包含在服务器二进制文件本。

扩展模块

通常，扩展模块包含在 Apache 软件包中，但一般不静态编译到服务器中。在 SUSE Linux Enterprise Server 中，它们可用作共享对象，可以在运行时装载进 Apache。

外部模块

标注为外部的模块不包含在正式 Apache 发行版中。但是 SUSE Linux Enterprise Server 提供了其中的几种。

多处理模块 (MPM)

MPM 负责接受和处理对 Web 服务器的请求，代表 Web 服务器软件的核心。

30.4.1 模块安装

如果如第 30.1.2 节“安装”[404]中所述执行了默认安装，则表示已安装以下模块：所有基本和扩展模块、多处理模块 Prefork MPM 以及外部模块 `mod_php5` 和 `mod_python`。

可以通过启动 YaST 并选择软件 > 软件管理来安装其他外部模块。现在请选择过滤器 > 搜索并搜索 *apache*。在其他包中，结果列表将包含所有可用的外部 Apache 模块。

30.4.2 激活和取消激活

手动或用 YaST 激活或停用特定模块。在 YaST 中，需要使用第 30.2.3.1 节“HTTP 服务器向导”[413]中所述的模块配置启用或禁用脚本语言模块（PHP5、Perl 和 Python）。可以按“服务器模块”一节[418]中所述启用或禁用所有其他模块。

如果要手动激活或停用模块，则分别使用命令 `a2enmod mod_foo` 或 `a2dismod mod_foo`。`a2enmod -l` 将输出当前所有活动模块的列表。

重要：包含外部模块的配置文件

如果已经手动激活外部模块，则确保在所有虚拟主机配置中装载其配置文件。外部模块的配置文件位于 `/etc/apache2/conf.d/` 下，并且在默认情况下不装载。如果每个虚拟主机上都需要相同的模块，则可以从此目录包含 `*.conf`。否则包含各个文件。请参见 `/etc/apache2/vhost.d/vhost.template` 获取示例。

30.4.3 基础模块和扩展模块

Apache 文档中对所有基础模块和扩展模块均进行了详细的描述。此处仅提供大多数重要模块的简短描述。请参见 <http://httpd.apache.org/docs/2.2/mod/> 以了解有关每个模块的详细信息。

`mod_actions`

请求某个特定 MIME 类型（如 `application/pdf`）、带特定扩展名的文件（如 `.rpm`）或某个特定请求方法（如 `GET`）时，提供执行脚本的方法。默认情况下启用此模块。

`mod_alias`

提供 `Alias` 和 `Redirect` 指令，可使用这些指令将 URI 映射到特定目录（别名）或将请求的 URL 重定向到其他位置。默认情况下启用此模块。

`mod_auth*`

身份验证模块提供不同的身份验证方法：使用 `mod_auth_basic` 的基本身份验证或使用 `mod_auth_digest` 的摘要身份验证。Apache 2.2 中的摘要身份验证仍处于试验阶段。

`mod_auth_basic` 和 `mod_auth_digest` 必须与身份验证提供程序模块 `mod_authn_*`（例如，用于基于文本文件的身份验证的 `mod_authn_file`）结合，并与授权模块 `mod_authz_*`（例如，用于用户授权的 `mod_authz_user`）结合。

有关该主题的更多信息可以从 *Authentication HOWTO* 中获取，网址是 <http://httpd.apache.org/docs/2.2/howto/auth.html>。

`mod_autoindex`

当不存在索引文件（例如 `index.html`）时，`Autoindex` 将生成目录列表。这些索引的外观是可配置的。默认情况下启用此模块。但是，在默认情况下，目录列表将通过 `Options` 指令禁用，重写虚拟主机配置中的此设置。此模块的默认配置文件位于 `/etc/apache2/mod_autoindex-defaults.conf` 处。

`mod_cgi`

执行 CGI 脚本时需要 `mod_cgi`。默认情况下启用此模块。

`mod_deflate`

可使用此模块配置 Apache，使其在传递给定文件类型之前实时压缩这些文件类型。

`mod_dir`

`mod_dir` 提供 `DirectoryIndex` 指令，它可用来配置在请求目录时自动传递的文件（默认使用 `index.html`）。当目录请求不包含尾部斜线时，它还能自动重定向到正确的 URL。默认情况下启用此模块。

`mod_env`

控制传递到 CGI 脚本或 SSI 页面的环境。环境变量可设置或取消设置，或者从调用 `httpd` 进程的壳层传递。默认情况下启用此模块。

`mod_expires`

使用 `mod_expires`，便可通过发送 `Expires` 报头来控制代理和浏览器缓存刷新文档的频率。默认情况下启用此模块。

`mod_include`

`mod_include` 允许您使用服务器端包含（SSI），它能提供动态生成 HTML 页面的基本功能。默认情况下启用此模块。

mod_info

在 <http://localhost/server-info/> 下提供服务器配置的完整概述。出于安全考虑，始终应该限制对此 URL 的访问。默认情况下，仅允许 localhost 访问此 URL。mod_info 是在 `/etc/apache2/mod_info.conf` 中配置的。

mod_log_config

使用此模块可配置 Apache 日志文件的外观。默认情况下启用此模块。

mod_mime

mime 模块负责根据文件名的扩展名（例如适用于 HTML 文档的 `text/html`）传递具有正确 **MIME** 报头的文件。默认情况下启用此模块。

mod_negotiation

对于内容协商是必需的。请参见 <http://httpd.apache.org/docs/2.2/content-negotiation.html> 获取更多信息。默认情况下启用此模块。

mod_rewrite

提供 `mod_alias` 的功能，但功能更全且更为灵活。使用 `mod_rewrite`，便可根据多个规则、请求报头等来重定向 URL。

mod_setenvif

基于客户端的请求细节（如客户端发送的浏览器字符串或客户端的 IP 地址）来设置环境变量。默认情况下启用此模块。

mod_speling

`mod_speling` 尝试自动更正 URL 中的印刷错误，例如大小写错误。

mod_ssl

在 Web 服务器和客户端之间启用加密连接。有关详细信息，请参见第 30.6 节“使用 SSL 设置安全性 Web 服务器” [430]。默认情况下启用此模块。

mod_status

在 <http://localhost/server-status/> 下提供有关服务器活动和性能的信息。出于安全考虑，始终应该限制对此 URL 的访问。默认情况下，仅允许 localhost 访问此 URL。mod_status 是在 `/etc/apache2/mod_status.conf` 中配置的

`mod_suexec`

`mod_suexec` 允许您在不同的用户和组下运行 CGI 脚本。默认情况下启用此模块。

`mod_userdir`

在 `~user/` 下启用可用的特定于用户的目录。必须在配置中指定 `UserDir` 指令。默认情况下启用此模块。

30.4.4 多处理模块

SUSE Linux Enterprise Server 提供了两个不同的多处理模块 (MPM) 供 Apache 使用：

- Prefork MPM [425]
- 第 30.4.4.2 节 “Worker MPM” [425]

30.4.4.1 Prefork MPM

prefork MPM 实现非线程的预生成 Web 服务器。它使 Web 服务器在行为上类似于 Apache 版本 1.x。在该版本中，它隔离每个请求并通过派生单独的子进程来处理请求。这样，有问题的请求就不会影响其他请求，避免了 Web 服务器被锁定。

此基于进程的方法 prefork MPM 虽然提供了稳定性，但比相应的 worker MPM 消耗更多的系统资源。prefork MPM 被视为是基于 Unix 操作系统的默认 MPM。

重要：本文档中的 **MPM**

本文档假设 Apache 使用 prefork MPM。

30.4.4.2 Worker MPM

worker MPM 提供一种多线程 Web 服务器。线程是一种“更小”的进程。线程相对于进程的优点是它占用较少的资源。worker MPM 并非仅生成子进程，还通过在服务器进程中使用线程来处理请求。预派生的子进程是多线程的。此方法相比 prefork MPM，使 Apache 消耗更少的系统资源，从而提高了 Apache 的执行效率。

一个主要缺点是 worker MPM 的稳定性：如果一个线程损坏，进程的所有线程都会受影响。最严重的情况会导致服务器崩溃。特别是在负载很重的情况下，如果将通用网关接口 (CGI) 与 Apache 一起使用，则可能由于线程无法与系统资源通信而发生内部服务器错误。将 worker MPM 与 Apache 一起使用的另一个争议是并非所有可用的 Apache 模块都是线程安全的，因此它不能与 worker MPM 结合使用。

警告：将 PHP 模块与 MPM 一起使用

并非所有可用的 PHP 模块都是线程安全的。强烈建议不要将 worker MPM 与 mod_php 一起使用。

30.4.5 外部模块

在此处查找随 SUSE Linux Enterprise Server 提供的所有外部模块的列表。

mod-apparmor

向 Apache 添加支持以将 AppArmor 限制提供给由模块（如 mod_php5 和 mod_perl）处理的各个 CGI 脚本。

包名称：apache2-mod_apparmor

更多信息：第 IV 部分 “Confining Privileges with AppArmor” (↑安全指南)

mod_mono

mod_auth_kerb 提供访问 Apache Web 服务器的 Kerberos 身份验证。

包名称：apache2-mod_auth_kerb

更多信息：<http://modauthkerb.sourceforge.net/configure.html>

mod_mono

使用 mod_mono 允许您在服务器中运行 ASP.NET 页。

包名：apache-mod_mono

配置文件：/etc/apache2/conf.d/mod_mono.conf

mod_perl

mod_perl 使您能够在嵌入的解释器中运行 Perl 脚本。服务器中嵌入的持久解释器能够避免启动外部解释器并且不会损失 Perl 启动时间。

包名称: apache2-mod_perl

配置文件: /etc/apache2/conf.d/mod_perl.conf

更多信息: /usr/share/doc/packages/apache2-mod_perl

mod_php5

PHP 是一种服务器端、跨平台 HTML 嵌入式脚本编写语言。

包名称: apache2-mod_php5

配置文件: /etc/apache2/conf.d/php5.conf

更多信息: /usr/share/doc/packages/apache2-mod_php5

mod_python

mod_python 允许将 Python 嵌入到 Apache HTTP 服务器中以增强性能并使基于 Web 的应用程序的设计更为灵活。

包名称: apache2-mod_python

更多信息: /usr/share/doc/packages/apache2-mod_python

mod_security

mod_security 提供用于保护 Web 应用程序免受一系列攻击的 Web 应用程序防火墙。它可以实现对 HTTP 流量的监控和实时分析。

包名称: apache2-mod_security2

配置文件: /etc/apache2/conf.d/mod_security2.conf

更多信息: /usr/share/doc/packages/apache2-mod_security2

文档: <http://modsecurity.org/documentation/>

30.4.6 编译

高级用户可以通过编写自定义模块来扩展 Apache。要开发 Apache 模块或编译第三方模块，就需要 apache2-devel 包以及相应的开发工具。

apache2-devel 还包含 apxs2 工具，此工具是编译其他 Apache 模块所必需的。

apxs2 允许从源代码编译和安装模块（包括对配置文件进行必要的更改），这将创建可在运行时装载入 Apache 的 *动态共享对象 (DSO)*。

apxs2 二进制文件在 /usr/sbin 中：

- /usr/sbin/apxs2 — 适于构建用于处理任何 MPM 的扩展模块。安装位置为 /usr/lib/apache2。
- /usr/sbin/apxs2-prefork — 适用于 prefork MPM 模块。安装位置为 /usr/lib/apache2-prefork。
- /usr/sbin/apxs2-worker — 适用于 worker MPM 模块。安装位置为 /usr/lib/apache2-worker。

使用以下命令从源代码安装并激活模块：

```
cd /path/to/module/source; apxs2 -cia  
mod_foo.c
```

其中，-c 编译该模块，-i 安装该模块，-a 激活该模块。apxs2 的其他选项在 apxs2(1) 手册页中有描述。

30.5 使 CGI 脚本运行

Apache 的通用网关接口 (CGI) 允许您使用程序或脚本（通常指 CGI 脚本）创建动态内容。可以用任何编程语言来编写 CGI 脚本。通常使用诸如 Perl 或 PHP 之类的脚本语言。

为了使 Apache 能够递送由 CGI 脚本创建的内容，需要激活 mod_cgi。另外还需要 mod_alias。默认情况下启用这两种模块。请参见第 30.4.2 节“激活和取消激活” [422] 来获取有关激活模块的详细信息。

警告：CGI 安全性

允许服务器执行 CGI 脚本是一项潜在的安全性漏洞。请参见第 30.7 节“避免安全性问题” [436] 以了解更多信息。

30.5.1 Apache 配置

在 SUSE Linux Enterprise Server 中，仅允许在目录 `/srv/www/cgi-bin/` 中执行 CGI 脚本。已配置此位置来执行 CGI 脚本。如果已经创建了虚拟主机配置（请参见第 30.2.2.1 节“虚拟主机配置”[409]）并且想将脚本放置在特定于主机的目录中，必须解锁并配置此目录。

例 30.5 VirtualHost CGI 配置

```
ScriptAlias /cgi-bin/ "/srv/www/www.example.com/cgi-bin/"❶
```

```
<Directory "/srv/www/www.example.com/cgi-bin/">  
  Options +ExecCGI❷  
  AddHandler cgi-script .cgi .pl❸  
  Order allow,deny❹  
  Allow from all  
</Directory>
```

- ❶ 指示 Apache 在此目录中将所有文件作为 CGI 脚本处理。
- ❷ 启用 CGI 脚本执行
- ❸ 指示服务器将扩展名为 `.pl` 和 `.cgi` 的文件视为 CGI 脚本。根据需要进行调整。
- ❹ `Order` 和 `Allow` 指令将控制默认访问状态以及 `Allow` 和 `Deny` 指令的评估顺序。在这种情况下，“allow”语句将在“deny”语句之前评估，并且启用通用访问。

30.5.2 运行示例脚本

CGI 编程不同于“常规”编程，因为 CGI 程序和脚本前面必须有一个 MIME 类型的报头，例如 `Content-type: text/html`。此报头将发送到客户端，所以它知道所接收内容的类型。其次，脚本的输出必须是客户端（通常是 Web 浏览器）所理解的，例如 HTML（大多数情况）、纯文本或图像。

在 `/usr/share/doc/packages/apache2/test-cgi` 下提供的简单测试脚本是 Apache 包的一部分。它将某些环境变量的内容输出为纯文本。将此脚本复制到 `/srv/www/cgi-bin/` 或您虚拟主机的脚本目录 (`/srv/www/www.example.com/cgi-bin/`) 中，并将它命名为 `test.cgi`。

可通过 Web 服务器访问的文件应由用户 `root` 拥有。有关更多信息，请参见第 30.7 节“避免安全性问题”[436]。由于该 Web 服务器是由不同用户运行的，

所以 CGI 脚本必须可被世界各地的用户执行和读取。更改为 CGI 目录并使用命令 `chmod 755 test.cgi` 来应用正确的权限。

现在调用 `http://localhost/cgi-bin/test.cgi` 或 `http://www.example.com/cgi-bin/test.cgi`。应该能看到“CGI/1.0 测试脚本报告”。

30.5.3 CGI 查错

如果没有看到测试程序的输出而是看到了错误消息，则请检查以下项：

CGI 查错

- 是否在更改配置后重装载了服务器？请检查 `rcapache2 probe`。
- 如果已经配置了自定义 CGI 目录，那么该配置是否正确？如果不确定，请尝试默认 CGI 目录 `/srv/www/cgi-bin/` 中的脚本并用 `http://localhost/cgi-bin/test.cgi` 调用它。
- 文件权限是否正确？更改为 CGI 目录并执行 `ls -l test.cgi`。它的输出应该以下面的字符串开头

```
-rwxr-xr-x 1 root root
```
- 确保脚本中没有编程错误。如果还未更改 `test.cgi`，则问题应该不大，但是如果正在使用您自己的程序，则始终要确保它们没有编程错误。

30.6 使用 SSL 设置安全性 Web 服务器

只要在 Web 服务器和客户端之间传送敏感数据（如信用卡信息），就需要具有带身份验证的安全的加密连接。`mod_ssl` 使用安全套接字层（SSL）和传输层安全（TLS）协议来为客户端和 Web 服务器之间的 HTTP 通信提供强有力的加密机制。使用 SSL/TLS 时，将在 Web 服务器和客户端之间建立专用连接。能够确保数据完整性，并且客户端和服务器能够彼此验证。

基于此目的，服务器在回答对 URL 的任何请求之前，会发送一个 SSL 证书，其中包含证明服务器有效身份的信息。反过来，这保证了该服务器对于通信来说

是唯一正确的终端。此外，证书使得在客户端和服务端之间建立起加密连接，确保在不泄露敏感的明文内容的情况下传输信息。

`mod_ssl` 不实施 SSL/TSL 协议本身，而是充当 Apache 和 SSL 库之间的接口。在 SUSE Linux Enterprise Server 中，将使用 OpenSSL 库。OpenSSL 将自动随 Apache 安装。

将 `mod_ssl` 与 Apache 一起使用的最明显效果就是 URL 的前缀为 `https://`（而不是 `http://`）。

提示：示例证书

安装包 `apache2-example-certificates` 时将提供一个假定公司“Snake Oil”的示例证书。

30.6.1 创建 SSL 证书

为了将 SSL/TSL 与 Web 服务器一起使用，需要创建 SSL 证书。在 Web 服务器和客户端之间授权时需要此证书，以便每一方都能明确地识别另一方。为了确保证书的完整性，证书必须由所有用户都信任的一方签署。

您可创建三种类型的证书：“虚设”证书（仅用于测试）、自我签名证书（用于信任您的指定用户群）和由独立的、众所周知的证书颁发机构 (CA) 签署的证书。

创建证书一般分为两步。首先，生成证书颁发机构的私用密钥，然后使用此密钥签署服务器证书。

提示：更多信息

要想更多地了解 SSL/TSL 的概念和定义，请参见 http://httpd.apache.org/docs/2.2/ssl/ssl_intro.html。

30.6.1.1 创建“虚拟”证书

虚设证书的生成非常简单。只需调用脚本 `/usr/bin/gensslcert` 即可。它创建或重写下列文件。利用 `gensslcert` 的可选开关调整证书。调用 `/usr/bin/gensslcert -h` 了解更多信息。

- /etc/apache2/ssl.crt/ca.crt
- /etc/apache2/ssl.crt/server.crt
- /etc/apache2/ssl.key/server.key
- /etc/apache2/ssl.csr/server.csr
- /root/.mkcert.cfg

还会将 ca.crt 的副本放在 /srv/www/htdocs/CA.crt 下以供下载。

重要：仅供测试

不能在生产系统上使用虚设证书。它只能用来测试。

30.6.1.2 创建自签署证书

如果要为内部网或指定用户群设置安全的 Web 服务器，只需通过您自己的证书颁发机构 (CA) 来签署证书即可。

创建自签署证书由 9 个交互的步骤组成。更改为目录 /usr/share/doc/packages/apache2，然后运行以下命令：`./mkcert.sh make --no-print-directory /usr/bin/openssl /usr/sbin/ custom`。请勿从此目录外运行该命令。程序将提供一系列的提示，其中一部分需要用户输入。

过程 30.4 使用 *mkcert.sh* 创建自签署的证书

1 决定用于证书的签名算法

选择 RSA (R, 默认值)，因为一些旧的浏览器在使用 DSA 时存在问题。

2 生成 CA 的 RSA 私用密钥 (1024 位)

不需要交互。

3 生成 CA 的 X.509 证书签署请求

在此处创建 CA 的判别名。这要求您回答几个问题，例如国家/地区名称或组织名称。输入有效数据，因为在此处输入的内容稍后会显示在证书中。无需回答所有问题。如果有问题不适用于您或者您不想回答，请使用“.”。常用名就是 CA 自身名称，请选择一个有意义的名称，例如 *My company CA*。

重要：CA 的常用名

CA 的常用名必须不同于服务器的常用名，因此请勿在此步骤中选择完全限定的主机名。

4 为自签署的 CA 生成 X.509 证书

选择证书版本 3（默认值）。

5 生成 SERVER 的 RSA 私用密钥（1024 位）

不需要交互。

6 生成 SERVER 的 X.509 证书签署请求

为此处的服务器密钥创建判别名。问题与 CA 判别名的问题几乎相同。在此处输入的数据适用于 Web 服务器，而且可以与 CA 的数据不同。（例如，如果服务器在其他地方）

重要：选择常用名

在此处输入的常用名必须是安全服务器的完全限定的主机名（例如，**www.example.com**）。否则，在访问 Web 服务器时，浏览器将发出一条警告，指示在证书与服务器不匹配。

7 生成由 CA 签署的 X.509 证书

选择证书版本 3（默认值）。

8 使用通行密码加密 CA 的 RSA 私用密钥以确保安全性

强烈建议使用密码加密 CA 的私用密钥，所以请选择 Y 并输入一个密码。

9 使用通行密码加密服务器的 RSA 私用密钥以确保安全性

使用密码加密服务器密钥要求您在每次启动 Web 服务器时输入此密码。这对于在引导时自动启动服务器或重新启动 Web 服务器有点困难。因此，通常在回答此问题时选择 N。要了解在没有使用密码加密时您的密钥是不受保护的，并且保证只有授权个人才有权访问此密钥。

重要：加密服务器密钥

如果选择使用密码加密服务器密钥，则请在 `/etc/sysconfig/apache2` 中增加 `APACHE_TIMEOUT` 的值。否则，在启动之前您没有足够的时间输入通行密码，这样服务器将无法停止。

脚本结果页面上将出现一个储存它已经生成的证书和密钥的列表。与脚本输出结果不同的是，文件没有在本地图录 `conf` 中生成，而是在 `/etc/apache2/` 下的适当位置处生成。

最后一步就是将 CA 证书文件从 `/etc/apache2/ssl.crt/ca.crt` 复制到用户可以访问的位置，从而将它合并到 Web 浏览器中已知、可信的 CA 的列表中。否则，浏览器将指示证书是由未知授权者发出的。证书的有效期为 1 年。

重要：自我签名证书

仅在 Web 服务器上使用自签署证书，此证书必须可由知道并相信您是证书授权者的人员访问。例如，不建议在公共商店使用此类证书。

30.6.1.3 获取正式签署的证书

签署证书的正式证书颁发机构有很多。证书是由值得信任的第三方签署的，所以可以完全相信。公共操作安全 Web 服务器通常具有正式签署的证书。

最常见的正式 CA 是 Thawte (<http://www.thawte.com/>) 或 Verisign (<http://www.verisign.com>)。这些 CA 以及其他 CA 已合并到所有浏览器中，所以由这些证书颁发机构签署的证书将被浏览器自动接受。

请求正式签署的证书时，无需向 CA 发送证书。相反，请发出证书签署请求 (CSR)。要创建 CSR，请调用脚本 `/usr/share/ssl/misc/CA.sh -newreq`。

首先，脚本将询问加密 CSR 的密码。然后，会要求您输入判别名。这要求您回答几个问题，例如国家/地区名称或组织名称。输入有效的数据，在此输入的所有内容稍后都会显示在证书中并供检查。无需回答所有问题。如果有问题不适

用于您或者您不想回答，请使用“.”。常用名就是 CA 自身名称，请选择一个有意义的名称，例如 *My company* CA。最后，必须输入询问密码和备用的公司名称。

在调用脚本的目录中查找 CSR。文件名是 `newreq.pem`。

30.6.2 使用 SSL 配置 Apache

Web 服务器端的 SSL 和 TLS 请求的默认端口是 443。在端口 80 上的“普通”Apache 侦听和端口 443 上支持 SSL/TLS 的 Apache 侦听之间没有冲突。事实上，HTTP 和 HTTPS 可以使用相同的 Apache 实例运行。通常使用一个虚拟主机将请求发送到端口 80 和端口 443 以区分虚拟服务器。

重要：防火墙配置

记住在端口 443 上为支持 SSL 的 Apache 打开防火墙。可以按第 15.4.1 节“Configuring the Firewall with YaST”（第 15 章 *Masquerading and Firewalls*, ↑ *安全指南*）中所述使用 YaST 来完成此操作。

在全局服务器配置中，SSL 模块默认情况下处于启用状态。如果它在您的主机上已禁用，请使用以下命令激活它：`a2enmod ssl`。要最终启用 SSL，需要使用标志“SSL”启动服务器。要执行此操作，请调用 `a2enflag SSL`。如果打算使用密码加密服务器证书，则还应增加 `/etc/sysconfig/apache2` 中 `APACHE_TIMEOUT` 的值，这样在 Apache 启动时，您就有足够的时间输入通行密码。重新启动服务器可使这些更改生效。仅重装载是不够的。

虚拟主机配置目录中包含模板 `/etc/apache2/vhosts.d/vhost-ssl.template`，该模板带有详细记录的特定于 SSL 的指令。请参见第 30.2.2.1 节“虚拟主机配置” [409] 了解通用虚拟主机配置。

要开始操作，请将模板复制到 `/etc/apache2/vhosts.d/mySSL-host.conf` 并对其进行编辑。调整以下指令的值应该就足够了：

- `DocumentRoot`
- `ServerName`
- `ServerAdmin`

- ErrorLog
- TransferLog

30.6.2.1 基于名称的虚拟主机和 SSL

默认情况下，不能在仅具有一个 IP 地址的服务器上运行多个启用了 SSL 的虚拟主机。基于名称的虚拟主机要求 Apache 了解已请求了哪些服务器名称。SSL 连接问题在于，此类请求只能在已建立 SSL 连接之后读取（通过使用默认虚拟主机）。因此用户将收到警告消息，指示证书与服务器名称不匹配。

SUSE Linux Enterprise Server 随附称为服务器名称指示 (SNI) 的 SSL 协议扩展，它在 SSL 协商过程中发送虚拟域的名称，从而解决了这一问题。这样服务器就能提前“切换”到正确的虚拟域，并向浏览器显示正确的证书。

SNI 在 SUSE Linux Enterprise Server 上默认启用。为了使基于名称的虚拟主机能够使用 SSL，可如“基于名称的虚拟主机”一节 [410] 中所述配置服务器（请注意，需要将端口 443 而不是端口 80 用于 SSL）。

重要：SNI 浏览器支持

客户端也必须支持 SNI。尽管大多数浏览器都支持 SNI，但一些用于移动硬件的浏览器以及 Windows* XP 上的 Internet Explorer 和 Safari 仍缺少 SNI 支持。有关详细信息，请参见http://en.wikipedia.org/wiki/Server_Name_Indication。

使用指令 `SSLStrictSNIVHostCheck` 配置如何处理不支持 SNI 的浏览器。在服务器配置中设置为 `on` 时，所有虚拟主机都将拒绝不支持 SNI 的浏览器。在 `VirtualHost` 指令中设置为 `on` 时，对此特定主机的访问将被拒。

在服务器配置中设置为 `off` 时，服务器的行为类似于不支持 SNI。SSL 请求将由定义的第一个虚拟主机（端口 443）处理。

30.7 避免安全性问题

对公共因特网开放的 Web 服务器需要不断加强管理。对于软件和意外的错误配置，安全问题似乎都是不可避免的。有关如何处理这些问题，在此有一些提示。

30.7.1 最新软件

在 Apache 软件中发现漏洞时，SUSE 将会发出安全忠告。其中包含修复漏洞的描述，用户应该尽快地依次采纳这些描述。SUSE 安全性声明可以从以下位置处获取：

- 网页 <http://www.novell.com/linux/security/securitysupport.html>
- 邮件列表存档 <http://lists.opensuse.org/opensuse-security-announce/>
- RSS 递送 http://www.novell.com/linux/security/suse_security.xml

30.7.2 DocumentRoot 权限

在 SUSE Linux Enterprise Server 中，默认情况下，DocumentRoot 目录 (/srv/www/htdocs) 和 CGI 目录 (/srv/www/cgi-bin) 都属于用户和组 root。您不能更改这些权限。如果任何用户都可写入这些目录，则任何用户都可以将文件放入这些目录中。之后，具有 wwwrun 权限（该权限允许用户随意访问文件系统资源）的 Apache 可能会执行这些文件。使用 /srv/www 的子目录可存放虚拟主机的 DocumentRoot 和 CGI 指令，并确保目录和文件属于用户和组 root。

30.7.3 文件系统访问权

默认情况下，在 /etc/apache2/httpd.conf 中拒绝对整个文件系统的访问。不应该重写这些指令，而是要明确启用对 Apache 可读的所有目录的访问权。有关详细信息，请参见“基本虚拟主机配置”一节 [411]。如此操作后，请确保任何重要文件（例如密码或系统配置文件）均不能从外部读取。

30.7.4 CGI 脚本

Perl、PHP、SSI 或任何其他编程语言中的交互脚本基本上可以运行任意命令，因此存在通常的安全性问题。将从服务器执行的脚本只能从服务器管理员信任的源安装，允许用户运行他们拥有的脚本通常不是好的做法。还建议对所有脚本执行安全性审计。

为了尽可能简化脚本的管理，通常会将 CGI 脚本的执行限制于特定目录而不是全局使用它们。指令 `ScriptAlias` 和 `Option ExecCGI` 用于配置。SUSE Linux Enterprise Server 默认配置不允许从任何位置执行 CGI 脚本。

所有 CGI 脚本都会作为同一个用户运行，所以不同的脚本可能会彼此冲突。模块 `suEXEC` 允许您在不同的用户和组下运行 CGI 脚本。

30.7.5 用户目录

启用用户目录（使用 `mod_userdir` 或 `mod_rewrite`）时，一定不要使用 `.htaccess` 文件，这些文件允许用户重写安全设置。至少应该使用指令 `AllowOverride` 来限制用户的注册。在 SUSE Linux Enterprise Server 中，`.htaccess` 文件是默认启用的，但是用户在使用 `mod_userdir`（请参见 `/etc/apache2/mod_userdir.conf` 配置文件）时不能覆盖任何 `Option` 指令。

30.8 查错

如果 Apache 不启动、网页不可访问或用户无法连接到 Web 服务器，那么找出问题的原因是很重要的。下面是几处查找错误描述的常见位置和需要检查的重要事项：

rcapache2 的输出

不要使用二进制文件 `/usr/sbin/httpd2` 启动和停止 Web 服务器，而应使用 `rcapache2` 脚本（如第 30.3 节“启动和停止 Apache”[418]中所述）。它详细描述了错误，甚至还提供解决配置错误的提示。

日志文件和详细程度

不管是致命错误还是非致命错误，都请检查 Apache 日志文件了解原因，主要是默认位于 `/var/log/apache2/error_log` 的错误日志文件。此外，如果需要日志文件记录得更详细一些，可以使用 `LogLevel` 指令来控制所记录消息的详细程度。

提示：简单测试

使用命令 `tail -F /var/log/apache2/my_error_log` 查看 Apache 日志消息。然后运行 `rcapache2 restart`。现在，请尝试连接浏览器并检查输出。

防火墙和端口

常见错误之一是在服务器的防火墙配置中未打开针对 Apache 的端口。如果使用 YaST 配置 Apache，有一个单独的选项可用于处理此特定问题（请参见第 30.2.3 节“使用 YaST 配置 Apache”[413]）。如果正在手动配置 Apache，则请通过 YaST 的防火墙模块打开 HTTP 和 HTTPS 的防火墙端口。

如果借助于以上所有信息仍无法找到错误原因，请检查http://httpd.apache.org/bug_report.html 的联机 Apache 错误数据库。此外，可以通过<http://httpd.apache.org/userslist.html> 上的邮件列表联系 Apache 用户社区。建议使用的新闻组是 comp.infosystems.www.servers.unix。

30.9 更多信息

包 `apache2-doc` 中包含有关本地安装和参考的多种本地化版本的完整 Apache 手册。它在默认情况下是不安装的，最快的安装方法是使用命令 `zypper in apache2-doc`。一旦安装，Apache 手册便可从<http://localhost/manual/> 获取。还可在 Web 上的<http://httpd.apache.org/docs-2.2/> 访问它。特定于 SUSE 的配置提示可以在目录 `/usr/share/doc/packages/apache2/README.*` 中获得。

30.9.1 Apache 2.2

有关 Apache 2.2 中新功能的列表，请参见http://httpd.apache.org/docs/2.2/new_features_2_2.html。可以在<http://httpd.apache.org/docs-2.2/upgrading.html> 获得有关从版本 2.0 升级到 2.2 的信息。

30.9.2 Apache 模块

有关第 30.4.5 节“外部模块”[426]中简述的外部 Apache 模块的更多信息，可在以下位置找到：

mod-apparmor

<http://en.opensuse.org/SDB:AppArmor>

mod-auth_kerb

<http://modauthkerb.sourceforge.net/>

mod_mono

http://www.mono-project.com/Mod_mono

mod_perl

<http://perl.apache.org/>

mod_php5

<http://www.php.net/manual/en/install.unix.apache2.php>

mod_python

<http://www.modpython.org/>

mod_security

<http://modsecurity.org/>

30.9.3 开发

有关开发 Apache 模块和涉及 Apache Web 服务器项目的更多信息，可以从以下位置处获得：

Apache 开发人员信息

<http://httpd.apache.org/dev/>

Apache 开发人员文档

<http://httpd.apache.org/docs/2.2/developer/>

使用 Perl 和 C 编写 Apache 模块

<http://www.modperl.com/>

30.9.4 其他来源

如果遇到特定于 SUSE Linux Enterprise Server 中的 Apache 的问题，请访问 <http://www.novell.com/support> 中的技术信息搜索。http://httpd.apache.org/ABOUT_APACHE.html 提供了对 Apache 历史的介绍。此页还解释此服务器为什么被称为 Apache。

使用 YaST 设置 FTP 服务器

使用 YaST *FTP 服务器* 模块，可以将计算机配置为 FTP（文件传输协议）服务器。匿名用户和/或经身份验证的用户可以连接到您的计算机并使用 FTP 协议下载文件。根据配置，可能还可以将文件上传到 FTP 服务器。YaST 为系统上所安装的各种 FTP 服务器守护程序提供了统一的配置界面。

您可以使用 YaST *FTP 服务器* 配置模块来配置两个不同的 FTP 服务器守护程序：

- vsftpd（非常安全的 FTP 守护程序）和
- pure-ftpd

只能配置已安装的服务器。

vsftpd 和 pure-ftpd 服务器的配置选项略有不同，尤其是专家设置对话框中的选项。本章介绍了 vsftpd 服务器所用的设置。

如果 YaST FTP 服务器模块在您的系统中不可用，请安装 `yast2-ftp-server` 包。

要使用 YaST 配置 FTP 服务器，请执行以下步骤：

- 1 打开 YaST 控制中心并选择 **网络服务 > FTP 服务器** 或以 `root` 的身份运行 `yast2 ftp-server` 命令。
- 2 如果您的系统未安装任何 FTP 服务器，YaST FTP 服务器模块启动时将询问您要安装哪个服务器。选择服务器并确认对话框。如果安装有两台服务器，请选择首选服务器并单击 **确定**。

- 3 在 *启动* 对话框中，配置 FTP 服务器的启动选项。有关详细信息，请参见第 31.1 节“启动 FTP 服务器” [444]。

在 *常规* 对话框中，配置 FTP 目录、欢迎消息、文件创建掩码和各种其他参数。有关详细信息，请参见第 31.2 节“FTP 常规设置” [445]。

在 *性能* 对话框中，设置会影响 FTP 服务器负载的参数。有关详细信息，请参见第 31.3 节“FTP 性能设置” [446]。

在 *身份验证* 对话框中，设置匿名用户和/或已通过身份验证的用户是否可以使用 FTP 服务器。有关详细信息，请参见第 31.4 节“身份验证” [446]。

在 *专家设置* 对话框中，配置 FTP 服务器的操作模式、SSL 连接和防火墙设置。有关详细信息，请参见第 31.5 节“专家设置” [447]。

- 4 按完成以保存配置。

31.1 启动 FTP 服务器

在 *FTP 启动* 对话框的 *服务启动* 框架中，设置 FTP 的启动方式。可以在系统引导期间自动启动服务器和手动启动服务器之间选择。如果只应在请求 FTP 连接后启动 FTP 服务器，请选择 *通过 xinetd*。

FTP 服务器的当前状态显示在 *FTP 启动* 对话框的 *打开和关闭* 框架中。通过单击 *立即启动 FTP* 来启动 FTP 服务器。要停止服务器，请单击 *立即停止 FTP*。更改服务器设置后，单击 *立即保存设置并重启动 FTP*。使用完成离开配置模块也将保存您的配置。

FTP 启动 对话框的 *所选服务* 框架会显示所用的 FTP 服务器：vsftpd 或 pure-ftpd。如果两台服务器都已安装，可以在它们之间切换 — 当前配置会自动转换。

图 31.1 FTP 服务器配置 — 启动



31.2 FTP 常规设置

在 *FTP* 常规设置对话框的常规设置框架中，可以设置连接到 *FTP* 服务器后会显示的欢迎消息。

如果选中 *Chroot 任何人* 选项，登录后会将所有本地用户放入其用户主目录的 *chroot jail* 中。此选项会牵涉到安全性问题，尤其是在用户拥有上载许可权限或进行壳层访问时，所以启用此选项时请务必小心。

如果选中详细日志记录选项，就会将所有 *FTP* 请求和响应记录在日志中。

可以限制由匿名用户和/或已通过身份验证的用户使用 *umask* 创建的文件的许可权限。在匿名 *Umask* 中为匿名用户设置文件创建掩码，在已通过身份验证的用户 *Umask* 中为已通过身份验证的用户设置文件创建掩码。掩码应输入为带有前导零的八进制数字。有关 *umask* 的更多信息，请参见 *umask* 手册页 (`man 1p umask`)。

在 *FTP* 目录框架中，设置用于匿名用户和已通过身份验证的用户的目录。按浏览可以从本地文件系统选择要使用的目录。匿名用户的默认 *FTP* 目录为 */srv/*

ftp。请注意，vsftpd并未允许所有用户都可对此目录进行写操作。将改为创建带有匿名用户的写许可权限的子目录 upload。

注意：FTP 目录的写许可权限

pure-ftpd 服务器允许匿名用户的 FTP 目录可以进行写操作。在服务器之间切换时，在切换回 vsftpd 服务器之前，请先确保使用 pure-ftpd 的目录中的写许可权限已删除。

31.3 FTP 性能设置

在性能对话框中，设置会影响 FTP 服务器负载的参数。最大闲置时间是远程客户端在 FTP 命令间可能会花费的最长时间（以分钟为单位）。如果长时间处于非活动状态，远程客户端会断开。单 IP 最大连接数确定了可从单个 IP 地址连接的最大客户端数。最大用户数确定了可连接的最大客户端数。任何其他客户端都将收到错误消息。

最大数据传送速度（以 KB/s 为单位）分别是在本地已通过身份验证的用户的本地最大速度和匿名客户端的匿名用户最高速度中设置的。速度设置的默认值为 0，表示数据传送速度不受限制。

31.4 身份验证

在身份验证对话框的启用/禁用匿名和本地用户框架中，可以设置允许访问您的 FTP 服务器的用户。您可以在以下选项中选择：仅为匿名用户授予访问权限、仅为经身份验证的用户授予访问权限或为两种类型的用户授予访问权限。

如果希望用户可以将文件上传到 FTP 服务器，请选中身份验证对话框上传框架中的允许上传。在此，通过选中相应的框甚至可以为匿名用户上传或创建目录。

注意：vsftp — 允许匿名用户上传文件

如果使用的是 vsftpd 服务器且希望匿名用户可以上传文件或创建目录，就必须在匿名 FTP 目录中创建带有所有用户的写许可权限的子目录。

31.5 专家设置

FTP 服务器可以在主动或被动模式下运行。默认情况下，服务器在被动模式下运行。要切换到主动模式中，只需取消选中专家设置对话框中的*启用被动模式*选项。也可更改服务器上用于数据流的端口范围，方法是：调整*被动模式最小端口*和*被动模式最大端口*选项。

如果想在客户端和服务器之间进行加密通讯，可以*启用 SSL*。检查要支持的协议版本，指定用于 SSL 加密连接的 DSA 证书。

如果您的系统受到防火墙的保护，请选中*打开防火墙中的端口*以启用至 FTP 服务器的连接。

31.6 更多信息

有关 FTP 服务器的更多信息，请参见 `pure-ftpd`、`vsftpd` 和 `vsftpd.conf` 的手册页。

Squid 代理服务器

Squid 是广泛用于 Linux 和 UNIX 平台的代理缓存。这表示它会将请求的因特网对象（例如 Web 或 FTP 服务器上的数据）储存在离请求工作站更近（与服务器相比）的计算机上。可以在多个层次结构中设置它以确保最佳的响应时间和使用较低的带宽（即使在对最终用户来说是透明的方式）。可以使用其他软件如 squidGuard 来过滤 Web 内容。

Squid 可以充当代理缓存。它将来自客户端（这里指来自 Web 浏览器）的对象请求重定向至服务器。当服务器回复所请求的对象后，它会将这些对象传递给客户端并在硬盘缓存中保存对象副本。缓存的一个优点就是：当多个客户端请求同一对象时，可以从硬盘缓存中提供该对象。这样客户端接收数据的速度要比从因特网接收快得多。此过程还可以减少网络流量。

除实际的缓存外，Squid 还提供众多功能，如在代理服务器的相互通讯的层次之间分配负载、为所有访问代理的客户端定义严格的访问控制列表、借助其他应用程序允许或拒绝对特定网页的访问以及生成有关频繁访问的网页的统计数字供评估用户的浏览习惯。Squid 不是通用代理。通常只充当 HTTP 连接的代理。它支持 FTP、Gopher、SSL 和 WAIS 等协议，但不支持其他因特网协议，如 Real Audio、新闻或视频会议。由于 Squid 只支持使用 UDP 协议在不同的缓存间通讯，所以很多其他多媒体程序都不受支持。

32.1 有关代理缓存的一些事实

作为代理缓存，Squid 的使用方法分为几种。与防火墙结合使用时，能够提高安全性。可以一起使用多个代理。还能确定应该缓存的对象的类型以及缓存的时间。

32.1.1 Squid 和安全性

Squid 可以与防火墙结合起来，通过使用代理缓存防止内部网络遭受外部攻击。防火墙会拒绝 Squid 之外的所有客户端对外部服务的访问。所有 Web 连接都必须通过代理方式建立。经过此配置后，Squid 便可全面控制 Web 访问。

如果防火墙配置中包含 DMZ，代理应该在此区域内操作。第 32.5 节“配置透明代理”[459]描述了如何实施透明代理。它能简化客户端的配置，因为在这种情况下，它们不需要代理的任何信息。

32.1.2 多个缓存

可以配置 Squid 的几个实例从而在它们之间交换对象。这样会减少系统负载，同时提高找到本地网络中已有对象的几率。还可以配置缓存层次，以便能够将对象请求转发给同级缓存或父级缓存 — 使其从本地网络中的其他缓存或直接从数据源获取对象。

为了不给网络增加总体数据流量，为缓存层次选择适当的拓扑结构是十分重要的。对于超大型网络，合理的做法是：为每个子网配置一个代理服务器并将其连接至父代理，再通过父代理连接至 ISP 的代理缓存。

所有这些通讯都通过在 UDP 协议之上运行的 ICP（因特网缓存协议）来处理。缓存间的数据传送使用基于 TCP 的 HTTP（超文本传送协议）来处理。

要找到从中可获得对象的最合适的服务器，一个缓存会向所有同级代理发送 ICP 请求。同级代理会通过 ICP 响应回复请求（如果检测到对象就回复 HIT 代码，如果未检测到则回复 MISS 代码）。如果发现多个 HIT 响应，代理服务器会根据哪个缓存回复最快或哪个最近等因素决定从哪个服务器下载。如果没有收到满意的响应，该请求将被发送至父缓存。

提示

为了避免网络中不同缓存中的对象重复，还会使用其他 ICP 协议，如 CARP（缓存阵列路由协议）或 HTCP（超文本缓存协议）。网络中维护的对象越多，找到所需对象的可能性就越大。

32.1.3 缓存因特网对象

网络中的对象并不全都是静态的。网络中有许多动态生成的 CGI 页面、访问计数器和加密的 SSL 内容文档。由于每次访问这类对象时它们都会更改，所以它们不会被缓存。

一直以来的问题是：储存在缓存中的所有其他对象应在保留多久。要确定保留时间，缓存中的所有对象都会被指派几种可能状态之一。Web 和代理服务器会通过为这些对象添加报头来找出对象的状态（如“Last modified”或“Expires”）以及相应的日期。同时还会使用其他报头指定不能缓存对象。

缓存中的对象通常会因为缺少可用硬盘空间而使用 LRU（最近最少使用）之类的算法进行替换。一般来说，这意味着代理会销毁未被请求时间最长的对象。

32.2 系统要求

最重要的事情是确定系统必须承受的最大网络负载。由于负载峰值可能是日均值的四倍，因此要特别注意负载峰值。如果不能确定，最好高估系统要求，因为让 Squid 在接近其处理能力限值的状态下工作可能会严重影响其服务质量。以下几节按重要程度依次阐述了各个系统要素。

32.2.1 硬盘

速度在缓存过程中起到重要作用，所以此要素值得特别关注。对于硬盘，此参数通过以毫秒衡量的*随机搜索时间*来描述。Squid 从硬盘读取或写入硬盘的数据块一般都较小，因此硬盘的搜索时间比其数据吞吐量更重要。如果要考虑代理的话，高转速硬盘可能会是更好的选择，因为高转速硬盘允许读写磁头更快定位到所需位置。使系统加速的一种可能办法是同时使用多个磁盘或采用分带 RAID 阵列。

32.2.2 磁盘缓存的大小

在小型缓存中，HIT（在其中找到所请求的对象）的概率会很小，因为该缓存很容易被占满，所以较少请求的对象很快被较新的请求对象替代。例如，如果缓存的可用空间为 1GB，而用户每天只浏览 10MB，那么占满缓存至少要 100 天。

确定所需缓存大小的最简便方法就是考虑连接的最大传送速度。1 Mbit/s（兆比特/秒）连接的最大传送速度为 125 KB/s。如果所有流量都进入缓存，1 小时累计可达 450 MB；假设所有流量都是在八小时工作时间之内产生的，那么每天将达到 3.6 GB。由于连接速度一般不会达到流量上限，所以可以认为缓存处理的数据总量约为 2 GB。这就是为什么要在 Squid 示例中使用 2 GB 的磁盘空间来保证一天的浏览数据都能缓存。

32.2.3 RAM

Squid 所需内存 (RAM) 大小直接与缓存中的对象数有关。Squid 还会在主存储器中储存缓存对象引用和经常请求的对象，以加速对这些数据的检索。随机存储器比硬盘快得多。

除此之外，Squid 还要在内存中保存其他数据，如：所有已处理 IP 地址的表、准确域名缓存、最常请求的对象、访问控制列表、缓冲区等等。

拥有足够的内存对于 Squid 进程非常重要，因为如果必须交换到磁盘的话，系统性能会显著降低。可以使用 `cachemgr.cgi` 工具来管理缓存内存。该工具在第 32.6 节“`cachemgr.cgi`”[461]中有介绍。

32.2.4 CPU

Squid 并不是需要大量使用 CPU 的程序。处理器的负载只会在装载或检查缓存内容时才会增加。使用多处理器计算机并不会提高系统性能。要提高效率，最好是购买速度更快的硬盘或增加内存。

32.3 启动 Squid

如果尚未安装，请安装 `squid` 包。`squid` 不属于默认 SUSE Linux Enterprise Server 安装范围。

Squid 在 SUSE® Linux Enterprise Server 中已预先配置，因此安装后即可立即启动。为保证顺利启动，应该对网络进行配置，使其至少能连接一个名称服务器和因特网。如果拨号连接使用动态 DNS 配置，则可能出现问题。在这种情况下，至少应该输入名称服务器，因为如果在 `/etc/resolv.conf` 中找不到 DNS 服务器，Squid 便不会启动。

32.3.1 用于启动和停止 Squid 的命令

要启动 Squid，在命令行中以 root 身份输入 `rcsquid start`。首次启动时，必须首先在 `/var/cache/squid` 中定义缓存的目录结构。启动脚本 `/etc/init.d/squid` 会自动进行定义，该过程可能需要几秒钟甚至几分钟的时间。如果右侧显示绿色的完成，表明已成功装载 Squid。要在本地系统上测试 Squid 的功能，请在浏览器中输入 `localhost` 作为代理，输入 `3128` 作为端口。

要允许用户从本地系统和其他系统访问 Squid 和因特网，需要将配置文件 `/etc/squid/squid.conf` 中的项 `http_access deny all` 改为 `http_access allow all`。但在这样做时，要考虑到此操作会让所有人都不受任何限制地访问 Squid。因此，应定义控制访问代理的 ACL。有关此内容的详细信息，请参见第 32.4.2 节“访问控制选项”[457]。

修改配置文件 `/etc/squid/squid.conf` 后，Squid 必须重装载该配置文件。可通过 `rcsquid reload` 执行此操作。或者，通过 `rcsquid restart` 彻底重启动 Squid。

可以使用命令 `rcsquid status` 来检查代理是否正在运行。使用命令 `rcsquid stop` 将关闭 Squid。这需要一些时间，因为 Squid 在断开同客户端的连接并将其数据写入磁盘前会等候最多半分钟（`/etc/squid/squid.conf` 中的 `shutdown_lifetime` 选项）。

警告：终止 Squid

使用命令 `kill` 终止 Squid，否则 `killall` 可损坏缓存。要能够重启动 Squid，必须删除损坏的缓存。

如果 Squid 在成功启动后不久就终止，请检查名称服务器项是否有误或者是否缺少 `/etc/resolv.conf` 文件。Squid 会在 `/var/log/squid/cache.log` 文件中记录启动失败的原因。如果应该在系统引导时自动装载 Squid，请使用 YaST 运行级别编辑器激活所需的 Squid 运行级别。请参见第 9.2.3 节“使用 YaST 配置 System Services (Runlevel)”[103]。

卸载 Squid 并不会删除缓存层次或日志文件。要删除这些内容，请手动删除 `/var/cache/squid` 目录。

32.3.2 本地 DNS 服务器

建立本地 DNS 服务器很有意义，即便并不用它来管理自己的域。它仅起到缓存专用名称服务器的作用，并且可以在无需任何特殊配置的情况下通过 root 名称服务器解析 DNS 请求（请参见第 24.4 节“启动 BIND 名称服务器”[321]）。如何完成上述操作，取决于您在配置因特网连接的过程中是否选择了动态 DNS。

动态 DNS

使用动态 DNS 时，因特网服务提供商通常在建立因特网连接过程中设置 DNS 服务器，并自动调整本地文件 `/etc/resolv.conf`。可以使用 `NETCONFIG_DNS_POLICY` `sysconfig` 变量在文件 `/etc/sysconfig/network/config` 中控制此行为。使用 YaST `sysconfig` 编辑器将 `NETCONFIG_DNS_POLICY` 设置为 `""`（请参见第 9.3.1 节“使用 YaST Sysconfig 编辑器更改系统配置”[105]）。然后在文件 `/etc/resolv.conf` 中输入本地 DNS 服务器，localhost 的 IP 地址是 127.0.0.1。这样 Squid 一启动就能找到本地名称服务器。

为了使服务提供商的名称服务器可访问，必须在配置文件 `/etc/named.conf` 中的 `forwarders` 下输入其名称及 IP 地址。使用动态 DNS，通过将 `sysconfig` 变量 `NETCONFIG_DNS_POLICY` 设置为 `auto`，可以在建立连接时自动执行上述操作。

静态 DNS

有了静态 DNS，在建立连接时自动 DNS 调整便不会发生，所以不需要更改任何 `sysconfig` 变量。但是，必须按如上所述在文件 `/etc/resolv.conf` 中输入本地 DNS 服务器。此外，必须在文件 `/etc/named.conf` 中的 `forwarders` 下手动输入提供商的静态名称服务器及其 IP 地址。

提示：DNS 和防火墙

如果运行了防火墙，应确保 DNS 请求能够通过。

32.4 配置文件 `/etc/squid/squid.conf`

所有 Squid 代理服务器设置都在 `/etc/squid/squid.conf` 文件中进行。首次启动 Squid 时，不必在此文件中进行任何更改，但是外部客户端最初不具备

访问权。代理可供 `localhost` 使用。默认端口为 3128。预安装的配置文件 `/etc/squid/squid.conf` 提供了有关选项的详细信息和许多示例。几乎所有项都以 `#` 开头（各行都标有注释）并且在行尾可找到相关描述。给定值几乎总与默认值相关，因此多数情况下，仅删除注释符号而不更改任何参数实际上没有什么影响。如果可能，保持示例不变，并将选项连同修改的参数一起插入下一行。这样，便可容易地恢复默认值，并将其与所作更改进行比较。

提示：更新后调整配置文件

如果已从较早的 Squid 版本更新，建议编辑新的 `/etc/squid/squid.conf`，并只应用以前文件中的更改。如果试图使用旧的 `squid.conf`，则配置可能不起作用，因为有时会修改选项并添加新的更改。

32.4.1 常规配置选项（选择）

`http_port 3128`

这是 Squid 侦听客户端请求所用的端口。默认端口为 3128，但也常使用 8080。如果需要，可指定多个以空格分隔的端口号。

`cache_peer hostnametypeproxy-porticp-port`

在此输入父代理（如果您想使用 ISP 的代理）。在 *主机名* 中输入要使用代理的名称或 IP 地址，在 *类型* 中输入 `parent`。对于 `proxy-port`，输入同样是由父代理运营商设置的在浏览器中使用的端口号（通常为 8080）。如果父代理的 ICP 端口未知并且该端口的使用与提供商无关，请将 `icp-port` 设为 7 或 0。此外，端口号后应指定 `default` 和 `no-query` 以禁止使用 ICP 协议。借助提供商的代理，Squid 就可以像普通浏览器那样操作了。

`cache_mem 8 MB`

此项定义 Squid 可用于常用答复的内存大小。默认为 8 MB。它不指定 Squid 的内存使用率，并且可能已经超过。

`cache_dir ufs /var/cache/squid/ 100 16 256`

`cache_dir` 项定义在磁盘上储存所有对象的目录。末尾的数字表示可用的最大磁盘空间（以 MB 为单位）以及第一级和第二级目录数。不要改动 `ufs` 参数。默认情况下，在 `/var/cache/squid` 目录内占用 100 MB 磁盘空间，并在该目录内创建 16 个子目录，每个又可以再包含 256 个子目录。指定要使用的磁盘空间时，应预留足够的磁盘空间。在此最为合理的值应该是

可用磁盘空间的 50%（最小）到 80%（最大）。在增大目录的后两个数字时一定要小心，因为目录过多也可能导致性能问题。如果有多个磁盘共享缓存，请输入多个 *cache_dir* 行。

`cache_access_log /var/log/squid/access.log` , `cache_log /var/log/squid/cache.log` ,
`cache_store_log /var/log/squid/store.log`

这三个条目将指定 Squid 记录其所有操作的路径。通常不做任何更改。如果 Squid 因使用频繁而负担过重，则可能需要将缓存和日志文件分散到多个磁盘上。

`emulate_httpd_log off`

如果该项设置为 *on*，则可以获取可读的日志文件。但有一些评估程序不能对此作出解释。

`client_netmask 255.255.255.255`

有了此条目，便可在日志文件中屏蔽客户端的 IP 地址。如果在此输入 255.255.255.0，IP 地址的最后一位将被设为 0。可以使用此方式来保护客户端的隐私。

`ftp_user Squid@`

使用此项可以设置 Squid 执行匿名 FTP 登录时应使用的密码。在此可以指定有效的电子邮件地址，因为有些 FTP 服务器需要通过这种方式来验证有效性。

`cache_mgr webmaster`

一个电子邮件地址，Squid 在意外崩溃时会向该地址发送信件。默认为 *webmaster*。

`logfile_rotate 0`

如果运行 `squid -k rotate`，Squid 可以循环使用受保护的日志文件。在此过程中会给文件编号，并且在达到指定值后重写最旧的文件。默认值为 0，因为 SUSE Linux Enterprise Server 中日志文件的存档和删除是由配置文件 `/etc/logrotate/squid` 中设置的 cron job（定时执行的任务）完成的。

`append_domain <domain>`

使用 *append_domain* 可指定自动追加的域（如果没有指定域）。通常，在此输入的是您自己的域，所以在浏览器中输入 `www` 将访问您自己的 Web 服务器。

`forwarded_for on`

如果将此项设置为 *off*，Squid 会将客户端的 IP 地址和系统名称从 HTTP 请求中删除。否则，它会向标题中添加以下行

```
X-Forwarded-For: 192.168.0.1
```

`negative_ttl 5 minutes; negative_dns_ttl 5 minutes`

一般不必更改这些值。但如果使用拨号连接，因特网有时可能无法访问。Squid 会记录失败的请求并拒绝发出新的请求，即便重新建立因特网连接也无济于事。在这种情况下，将分钟更改为秒。然后单击浏览器中的重新装载，拨号进程会在几秒钟后重新启动。

`never_direct allow acl_name`

要防止 Squid 直接从因特网接受请求，应使用上述命令强制连接到另一个代理。事先必须已在 *cache_peer* 中输入该代理。如果将 *acl_name* 指定为 *all*，会强制所有请求直接转发给父代理。有时这可能是必要的，例如在您的提供商严格规定使用它的代理或拒绝通过其防火墙直接访问因特网时。

32.4.2 访问控制选项

Squid 为控制针对代理的访问提供了一套周密的系统。通过实施 ACL 可以轻松并全面地进行配置。这涉及一些依次处理的规则的列表。使用 ACL 之前必须先定义 ACL。一些默认的 ACL 已经存在，如 *all* 和 *localhost*。但是，仅仅定义 ACL 并不意味着实际应用 ACL。只有在与 *http_access* 规则一同使用时才不是这样。

`acl <acl_name> <type> <data>`

ACL 至少需要三个规范值来定义。名称 *<acl_name>* 可以任意选择。对于 *<type>*，可以在多种不同的选项中选择（在 */etc/squid/squid.conf* 文件的 *ACCESS CONTROLS* 部分中可以找到这些选项）。*<data>* 的值取决于各 ACL 的类型，并且可以从文件中读取（例如，通过主机名、IP 地址或 URL）。以下是一些简单的示例：

```
acl mysurfers srcdomain .my-domain.com
acl teachers src 192.168.1.0/255.255.255.0
acl students src 192.168.7.0-192.168.9.0/255.255.255.0
acl lunch time MTWHF 12:00-15:00
```

`http_access allow <acl_name>`

http_access 定义谁可以使用代理，以及谁能够访问因特网上的什么内容。为此必须指定 ACL。上面已经定义了 *localhost* 和 *all*，这两个 ACL 可以通过 *deny* 或 *allow* 相应地拒绝或允许访问。可以创建一个包含任何数量 *http_access* 项的列表，按从上到下的顺序处理各个项，并且根据出现的先后顺序允许或拒绝访问相应的 URL。最后一项应始终是 *http_access deny all*。在下例中，*localhost* 可随意访问任何内容，而其他所有主机全部被拒绝访问。

```
http_access allow localhost
http_access deny all
```

在另外一个使用这些规则的示例中，*teachers* 组总能访问因特网。*students* 组只能在星期一到星期五的午餐时间访问。

```
http_access deny localhost
http_access allow teachers
http_access allow students lunch time
http_access deny all
```

为提高可读性，只应该在 `/etc/squid/squid.conf` 文件的指定位置输入带有 *http_access* 项的列表。即在文本

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
```

和最后的

```
http_access deny all
```

`redirect_program /usr/bin/squidGuard`

使用此选项可以指定重定向器（如 *squidGuard*），允许阻止不需要的 URL。通过代理身份验证和适当的 ACL 可以控制不同的用户组访问因特网。*squidGuard* 是一个可以安装和配置的独立包。

`auth_param basic program /usr/sbin/pam_auth`

如果必须在代理上验证用户，请设置一个相应的程序（如 *pam_auth*）。当首次访问 *pam_auth* 时，用户会看到一个用于输入用户名和密码的登录窗口。此外，仍然需要 ACL，只允许提供有效登录信息的客户端使用因特网：

```
acl password proxy_auth REQUIRED

http_access allow password
http_access deny all
```

可以用授权用户名的列表或指向此类列表的路径来替换 *proxy_auth* 后的 *REQUIRED*。

`ident_lookup_access allow <acl_name>`

使用此选项，可以为 ACL 定义的所有客户端都运行 *ident* 请求以查找各个用户的身份。如果对 *<acl_name>* 应用 *all*，此选项对所有客户端都有效。另外，必须在所有客户端上运行 *ident* 守护程序。对于 Linux，可为此安装 *pidentd* 包。对于 Microsoft Windows，可从因特网上下载免费软件。为确保只有成功进行 *ident* 查找的客户端才有权访问，请在此定义相应的 ACL：

```
acl identhosts ident REQUIRED

http_access allow identhosts
http_access deny all
```

这里同样需要用授权用户名列表来替换 *REQUIRED*。使用 *ident* 会明显延缓访问时间，因为每个请求都要重复进行 *ident* 查找。

32.5 配置透明代理

使用代理服务器的常用方式如下：Web 浏览器向代理服务器中的某端口发送请求，代理提供这些所需的对象（不论它们是否在其缓存中）。在网络中使用时，可能出现以下几种情况：

- 出于安全考虑，建议所有客户端都使用代理来浏览因特网。
- 所有客户端都必须使用代理，无论客户端是否清楚这一点。
- 网络中的代理已转移，但是现有客户端应保留其原有配置。

在所有这些情况下，都可以使用透明代理。原理很简单：代理截获并应答 Web 浏览器的请求，所以 Web 浏览器接收到所请求的页面，但并不知道它们来自何处。正如名称中指出的那样，整个处理过程完全是透明的。

32.5.1 /etc/squid/squid.conf 中的配置选项

要通知 *squid* 作为透明代理使用，请使用透明选项，该选项位于主配置文件 */etc/squid/squid.conf* 中的标记 *http_port* 处。重启动 *squid* 后，要执

行的唯一操作就是重配置防火墙，将 http 端口重定向到 http_port 中给定的端口。在以下 squid 配置行中，它是端口 3128。

```
http_port 3128 transparent
```

32.5.2 使用 SuSEfirewall2 配置防火墙

现在借助端口转发规则，通过防火墙将所有入站请求重定向到 Squid 端口。可使用附带的工具 SuSEFirewall2 完成此操作，如第 15.4.1 节“Configuring the Firewall with YaST”（第 15 章 *Masquerading and Firewalls*, ↑安全指南）中所述。可以在 /etc/sysconfig/SuSEfirewall2 中找到其配置文件。配置文件的项已进行适当注释。要设置透明代理，必须配置几个防火墙选项：

- 设备指向因特网：FW_DEV_EXT="eth1"
- 设备指向网络：FW_DEV_INT="eth0"

定义防火墙上从不可信的（外部）网络（如因特网）访问的端口和服务（请参见 /etc/services）。在下例中，仅对外部提供 Web 服务：

```
FW_SERVICES_EXT_TCP="www"
```

定义防火墙上从安全（内部）网络访问的端口或服务（请参阅 /etc/services），包括通过 TCP 和 UDP：

```
FW_SERVICES_INT_TCP="domain www 3128"  
FW_SERVICES_INT_UDP="domain"
```

这会允许访问万维网服务和 Squid（Squid 的默认端口为 3128）。服务“域”代表 DNS（域名服务）。此服务很常用。如果不需要，只需将其从上面的项中删除并将下面的选项设置为 no：

```
FW_SERVICE_DNS="yes"
```

最重要的选项是选项数字 15：

例 32.1 防火墙配置：选项 15

```
# 15.)  
# Which accesses to services should be redirected to a local port on  
# the firewall machine?  
#
```

```
# This option can be used to force all internal users to surf via
# your squid proxy, or transparently redirect incoming webtraffic to
# a secure webserver.
#
# Format:
# list of <source network>[,<destination network>,<protocol>[,dport[:lport]]
# Where protocol is either tcp or udp. dport is the original
# destination port and lport the port on the local machine to
# redirect the traffic to
#
# An exclamation mark in front of source or destination network
# means everything EXCEPT the specified network
#
# Example: "10.0.0.0/8,0/0,tcp,80,3128 0/0,172.20.1.1,tcp,80,8080"
```

上面的注释显示了需要遵循的语法。首先，输入访问代理防火墙的内部网络的 IP 地址和网络掩码。其次，输入这些客户端请求发往的 IP 地址和网络掩码。如果使用的是 Web 浏览器，请指定网络 0/0（表示“至任意地址的通配符”）。之后，输入这些请求最初发送到的端口以及所有这些请求最终要重定向到的端口。由于 Squid 能够支持 HTTP 以外的协议，可将请求从其他端口重定向至代理，如 FTP（端口 21）、HTTPS、或 SSL（端口 443）。在本例中，Web 服务（端口 80）重定向至代理端口（端口 3128）。如果要添加更多网络或服务，必须在对应项中用空格分隔它们。

```
FW_REDIRECT="192.168.0.0/16,0/0,tcp,80,3128"
```

要启动防火墙及其新配置，请更改 /etc/sysconfig/SuSEfirewall12 文件的项。必须将 START_FW 项设置为 "yes"。

按第 32.3 节“启动 Squid”[452]所述启动 Squid。要了解是否一切正常，请检查 /var/log/squid/access.log 中的 Squid 日志。Squid 只有 Web 服务（端口 80）应该是打开的。要使用 nmap 扫描端口，命令语法为 nmap -O IP_address。

32.6 cachemgr.cgi

缓存管理器 (cachemgr.cgi) 是一个 CGI 实用程序，用于显示正运行的 Squid 进程占用内存的相关统计数字。这也是在不登录服务器的情况下，管理缓存和查看统计数字的一种更便捷的方式。

32.6.1 设置

首先，必须在系统上运行 Web 服务器。按第 30 章 *Apache HTTP 服务器* [403] 中所示配置 Apache。要检查 Apache 是否已在运行，以 root 身份输入命令 `rcapache status`。如果显示如下消息：

```
Checking for service httpd: OK
Server uptime: 1 day 18 hours 29 minutes 39 seconds
```

表示 Apache 正在该计算机上运行。如果未运行，则输入 `rcapache start` 以使用 SUSE Linux Enterprise Server 默认设置启动 Apache。最后一个设置步骤是将文件 `cachemgr.cgi` 复制到 Apache 目录 `cgi-bin`。对 32 位环境，它工作原理如下：

```
cp /usr/lib/squid/cachemgr.cgi /srv/www/cgi-bin/
```

在 64 位环境中，`cachemgr.cgi` 文件位于 `/usr/lib64/squid/` 下，将它复制到 Apache 目录的命令如下：

```
cp /usr/lib64/squid/cachemgr.cgi /srv/www/cgi-bin/
```

32.6.2 /etc/squid/squid.conf 中的缓存管理器 ACL

缓存管理器所需的原文件中有一些默认设置。首先定义两个 ACL，然后 `http_access` 选项将使用这些 ACL 将访问权限从 CGI 脚本授权到 Squid。第一个 ACL 最为重要，因为缓存管理器要通过 `cache_object` 协议尝试与 Squid 通讯。

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

以下规则向 Apache 授权对 Squid 的访问权限：

```
http_access allow manager localhost
http_access deny manager
```

这些规则假定 Web 服务器和 Squid 运行在同一台计算机上。如果缓存管理器与 Squid 间的通讯是另一台计算机上的 Web 服务器发出的，应如例 32.2 “访问规则” [463] 所示包含额外的 ACL。

例 32.2 访问规则

```
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl webserver src 192.168.1.7/255.255.255.255 # webserver IP
```

然后在例 32.3 “访问规则” [463]中添加规则以允许从 Web 服务器访问。

例 32.3 访问规则

```
http_access allow manager localhost
http_access allow manager webserver
http_access deny manager
```

为管理器配置密码以访问更多选项，如远程关闭缓存或查看有关缓存的更多信息。为此，应配置项 `cachemgr_passwd`，设置用于管理器和可查看选项列表的密码。此列表在 `/etc/squid/squid.conf` 中显示为项注释的一部分。

每次一更改配置文件，就应重新启动 Squid。使用 `rcsquid reload` 可以轻松地重新启动。

32.6.3 查看统计数字

访问相应的网站 — <http://webserver.example.org/cgi-bin/cachemgr.cgi>。按继续来浏览不同的统计数字。

32.7 squidGuard

本节的目的并不是要解释 squidGuard 的详细配置，而只是介绍该程序并为使用该程序提些建议。要深入了解配置问题，请参见 squidGuard 的网站 <http://www.squidguard.org>。

squidGuard 是一款用于 Squid 的免费 (GPL)、灵活而快捷的过滤器、重定向器和访问控制器插件。使用它可以针对 Squid 缓存定义多种访问规则，对不同用户组加以不同的限制。squidGuard 使用 Squid 的标准重定向接口。squidGuard 可以执行以下操作：

- 将某些用户的万维网访问权限制为只能访问一组可接受的或知名万维网服务器或 URL。

- 防止某些用户访问某些列出的或在黑名单中列出的 Web 服务器或 URL。
- 防止某些用户访问与一组正则表达式或单词匹配的 URL。
- 将拦截的 URL 重定向至基于 CGI 的“智能”信息页面。“”
- 将未注册用户重定向至注册表单。
- 将横幅重定向至空白 GIF。
- 使用基于时间、周中各天、日期等的不同访问规则。
- 对不同用户组使用不同规则。

squidGuard 和 Squid 不能用于：

- 编辑、过滤或审查文档内的文本。
- 编辑、过滤或审查 HTML 嵌入脚本语言，如 JavaScript 或 VBScript。

在使用 squidGuard 之前，请先进行安装。提供最小的配置文件，如 `/etc/squidguard.conf`。可在 <http://www.squidguard.org/Doc/examples.html> 中找到配置示例。以后可尝试更为复杂的配置设置。

接下来，如果客户机请求列在黑名单中的网站，则创建一个虚设的“拒绝访问”页面或复杂点的 CGI 页面来重定向 Squid。强烈建议使用 Apache。

现在，配置 Squid 以使用 squidGuard。使用 `/etc/squid/squid.conf` 文件中的以下项：

```
redirect_program /usr/bin/squidGuard
```

名为 `redirect_children` 的另一选项配置在该计算机上运行的“重定向”（在此例中是 squidGuard）进程数。设置的进程越多，所需的 RAM 就越多。先尝试较低的数字（例如 4）。

```
redirect_children 4
```

最后，通过运行 `rcsquid reload` 让 Squid 装载新配置。现在，可以通过浏览器测试这些设置。

32.8 使用 Calamaris 生成缓存报告

Calamaris 是一个 Perl 脚本，用来以 ASCII 或 HTML 格式生成缓存活动的报告。它可以处理本机 Squid 访问日志文件。Calamaris 的主页为<http://Calamaris.Cord.de/>。此工具不属于 SUSE Linux Enterprise Server 默认安装范围—要使用它，请安装 calamaris 包。

以 root 身份登录，然后输入 `cat access.log | calamaris 选项 > reportfile`。在通过管道输出一个以上日志文件时，日志文件要按时间先后排列，较早的文件先输出，这一点很重要。该程序有一些选项：

提示：壳层和文件序列

如果您有多个相似的文件，例如 `access.log.1`、`access.log.2` 等，默认壳层 **Bash** 在列出 `access.log` 文件时会对这些不在数列的文件进行排序。`*` 时不会按数字顺序排列那些文件。为解决这个问题，可使用语法 `access.log.{1..42}`，生成一个使用数字 1 到 42 扩展的文件列表。

-a

输出所有可用报告

-w

以 HTML 格式输出报告

-l

在报告标题处包含消息或徽标

有关不同选项的详细信息，可通过 `man calamaris` 在该程序的手册页中找到。

典型示例如下：

```
cat access.log.{10..1} access.log | calamaris -a -w \  
> /usr/local/httpd/htdocs/Squid/squidreport.html
```

这会将报告放入 Web 服务器目录。需要通过 Apache 来查看这些报告。

32.9 更多信息

访问 Squid 的主页 <http://www.squid-cache.org/>。在此可找到“Squid 用户指南”及有关 Squid 的大量 FAQ（常见问题解答）信息。

安装该程序后，在 howtoenh 中有一个关于透明代理的小的使用描述文件 `/usr/share/doc/howto/en/txt/TransparentProxy.gz`。此外还通过 squid-users@squid-cache.org 提供 Squid 的邮件列表。其存档文件位于 <http://www.squid-cache.org/mail-archive/squid-users/> 中。

使用 SFCB 的基于 Web 的企业 管理

33

33.1 简介和基本概念

SUSE® Linux Enterprise Server (SLES) 提供一组基于开放标准的工具，用于统一管理不同的计算系统和环境。我们的企业解决方案实现 Distributed Management Task Force 所提出的标准。以下段落描述了它们的基本组件。

Distributed Management Task Force, Inc (DMTF) 是业内引领企业和因特网环境管理标准开发的公司。他们的目标是统一管理标准和计划，开发出集成度更高、成本更低、可互操作性更好的管理解决方案。DMTF 标准为控制和通讯提供通用系统管理组件。他们的解决方案是独立于平台和技术的。基于 *Web* 的企业管理和通用信息模型是其关键技术之一。

基于 Web 的企业管理 (WBEM) 是一整套管理和因特网标准技术。开发 WBEM 的意图是统一企业计算环境的管理。它为该行行业提供了使用 Web 技术并且良好集成的管理工具集。WBEM 由以下标准组成：

- 数据模型：通用信息模型 (CIM) 标准
- 编码规范：CIM-XML 编码规范
- 传输机制：通过 HTTP 的 CIM 操作

通用信息模型是描述系统管理的概念信息模型。它并不局限于特定的实施，能在管理系统、网络、服务和应用程序之间交换管理信息。CIM 有两部分：CIM 规范和 CIM 纲要。

- *CIM* 规范描述语言、命名和元纲要。元模式是模型的正式定义。它定义用来表示模型及其用途以及语义的术语。元模式的元素有类、属性和方法。元纲要也支持使用指令和关联作为类的类型，使用参考作为属性的类型。
- *CIM* 纲要可提供实际模型描述。它提供具有属性和关联的类集合，这些类可提供易理解的概念框架，在该框架内可组织关于受管环境的可用信息。

“通用信息模型对象管理器”（CIMOM）是一种 CIM 对象管理器，或更确切地说，它是一个根据 CIM 标准管理对象的应用程序。CIMOM 管理 CIMOM 提供程序与 CIM 客户端（管理员管理系统的位置）之间的通讯。

CIMOM 提供程序是在 CIMOM 内执行客户端应用程序请求的特定任务的软件。每个提供者实施 CIMOM 模式的一个或多个方面。这些提供程序直接与硬件交互。

Standards Based Linux Instrumentation for Manageability (SBLIM) 是设计用来支持基于 Web 的企业管理 (WBEM) 的工具集。SUSE® Linux Enterprise Server 使用名为小规模 CIM 中介程序的 SBLIM 项目提供的开放源 CIMOM（或 CIM 服务器）。

小规模 CIM 中介程序是设计用于资源有限或嵌入式环境中的 CIM 服务器。它设计为同时保持模块化与轻量级。它是基于开放标准的，支持 CMPI 提供程序、CIM-XML 编码和管理对象格式 (MOF)。它可以灵活配置，并且即便提供程序崩溃也仍然表现稳定。它也很容易访问，因为它支持各种传输协议，例如 HTTP、HTTPS、Unix 域套接字、Service Location Protocol (SLP) 和 Java Database Connectivity (JDBC)。

33.2 设置 SFCB

要设置小规模 CIM 中介程序 (SFCB) 环境，请确保 SUSE Linux Enterprise Server 安装期间选择了 YaST 中的基于 Web 的企业管理模式。或者选择它作为组件安装到已在运行的服务器上。确保您的系统上安装了以下包：

cim-schema，通用信息模型 (CIM) 纲要

包含通用信息模型 (CIM)。CIM 是描述网络或企业环境中总体管理信息的模型。CIM 由规范和模式组成。规范定义与其他管理模型集成的详细信息。模式提供实际模型说明。

cmpi-bindings-pywbem

包含在 Python 中写入和运行 CMPI 类型的 CIM 提供程序的适配器。

cmpi-pywbem-base

包含基本系统 CIM 提供程序。

cmpi-pywbem-power-management

包含基于 DSP1027 的电源管理提供程序。

python-pywbem

包含通过 WBEM 协议调用 CIM 操作来查询和更新受管对象的 Python 模块。

cmpi-provider-register, CIMOM 中性提供程序注册实用程序

包含的实用程序允许 CMPI 提供程序包用 CIMOM 存在于系统上的任何内容注册。

sblim-sfcb, 小规模 CIM 中介程序

包含小规模 CIM 中介程序。它是通过 HTTP 协议与 CIM 操作保持一致的 CIM 服务器。它功能强大, 占用资源又少, 因此很适合嵌入式和资源有限的环境。SFCB 支持通过 Common Manageability Programming Interface (CMPI) 写入的提供程序。

sblim-sfcc

包含小规模 CIM 客户端库运行时库。

sblim-wbemcli

包含 WBEM 命令行界面。它是一个独立的命令行 WBEM 客户端, 特别适合基本的系统管理任务。

smis-providers

包含用于在 Linux 文件系统上处理卷和快照的提供程序。这些分别基于 SNIA 的 SMI-S 卷管理配置文件和 Copy Services 配置文件。

图 33.1 基于 Web 的企业管理模式的包选择

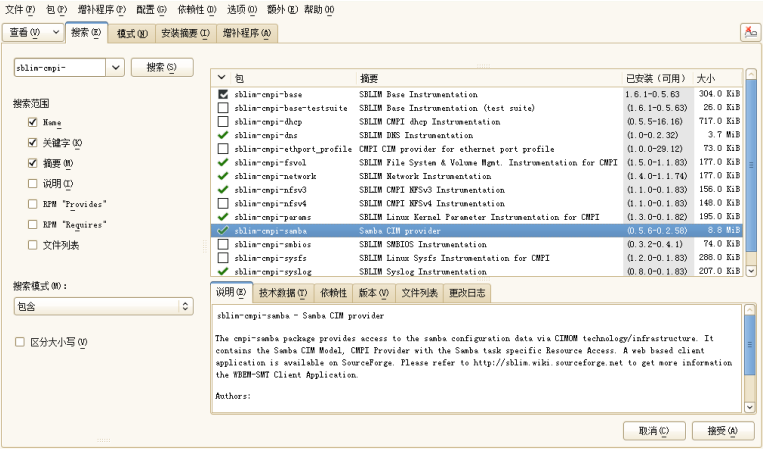


33.2.1 安装其他提供程序

SUSE® Linux Enterprise Server 软件安装源包含基于 Web 的企业安装模式中
没有的额外 CIM 提供程序。您可以在 YaST 软件安装模块中搜索模式

`sblim-cmpi-` 来方便地获取其列表和安装状态。这些提供程序涵盖了各种系统管理任务, 例如 `dhcp`、`NFS` 或内核参数设置。安装要用于 `SFCB` 的那些提供程序是很有用的。

图 33.2 其他 CIM 提供程序的包选择



33.2.2 启动、停止 SFCB 和检查其状态

CIM 服务器 sfcbd 守护程序是和基于 Web 的企业管理软件一起安装的，默认在系统启动时启动。下表描述如何启动、停止 sfcbd 和检查其状态。

表 33.1 用于管理 sfcbd 的命令

任务	Linux命令
启动 sfcbd	以 root 身份在命令行中输入 rcsfcb start。
停止 sfcbd	以 root 身份在命令行中输入 rcsfcb stop。
检查 sfcbd 状态	以 root 身份在命令行中输入 rcsfcb status。

33.2.3 确保安全访问

SFCB 的默认设置相对来说比较安全。但是也要检查对 SFCB 组件访问的安全性是否符合您的组织要求。

33.2.3.1 证书

安全套接字层 (SSL) 传输需要保证安全通讯的证书。安装 SFCB 时，会生成自我签名的证书。

您可以通过更改 `/etc/sfcb/sfcb.cfg` 中的 `sslCertificateFilePath:` `路径_文件名` 设置将默认证书的路径换成商业或自我签名证书。该文件必须是 PEM 格式。

默认生成的服务器证书位置如下：

```
/etc/sfcb/server.pem
```

注意：SSL 证书的路径

默认生成的证书文件 `servercert.pem` 和 `serverkey.pem` 储存在 `/etc/ssl/servercerts` 目录下。文件 `/etc/sfcb/client.pem`、`/etc/sfcb/file.pem` 和 `/etc/sfcb/server.pem` 是这些文件的符号链接。

如果想生成新证书，请在命令行中以 `root` 身份输入以下命令：

```
tux@mercury:~> sh /usr/share/sfcb/genSslCert.sh
Generating SSL certificates in .
Generating a 2048 bit RSA private key
.....+++
.+++
writing new private key to '/var/tmp/sfcb.0Bjt69/key.pem'
-----
```

默认情况下，该脚本在当前工作目录下生成证书 `client.pem`、`file.pem` 和 `server.pem`。如果希望脚本在 `/etc/sfcb` 目录中生成证书，需要将它追加到命令后。如这些文件已存在，将显示一条警告消息，而不会重写旧的证书。

```
tux@mercury:~> sh /usr/share/sfcb/genSslCert.sh /etc/sfcb
Generating SSL certificates in .
WARNING: server.pem SSL Certificate file already exists.
old file will be kept intact.
```

```
WARNING: client.pem SSL Certificate trust store already exists.  
old file will be kept intact.
```

必须从文件系统删除旧的证书并重新运行命令。

如果希望更改 SFCB 使用证书的方式，请参见第 33.2.3.3 节“身份验证”[473]。

33.2.3.2 端口

默认情况下，将 SFCB 配置为接受通过安全端口 5989 的所有通讯。以下段落描述通讯端口的设置和建议的配置。

端口 5989（安全）

SFCB 通讯通过 HTTPS 服务使用的安全端口。这是默认选项。通过此设置，当通过因特网在服务器和工作站之间发送通信时，将加密 CIMOM 和客户程序应用程序之间的所有通信。用户必须以客户端应用程序进行身份验证，才能连接到 SFCB 服务器。建议您保留该设置。为了让 SFCB CIMOM 能与必要的应用程序通讯，如果客户端应用程序与所监视的节点之间存在路由器和防火墙，必须在它们上面打开此端口。

端口 5988（不安全）

SFCB 通讯通过 HTTP 服务使用的不安全端口。在默认情况下会禁用该设置。通过此设置，当任何人在未经身份验证的情况下通过因特网在服务器和工作站之间发送通讯时，将打开并查看 CIMOM 和客户端应用程序之间的所有通讯。建议仅当尝试调试 CIMOM 问题时才使用此设置。在问题解决后，请将非安全端口选项设置回禁用。为了使 SFCB CIMOM 能够与需要非安全访问的必要应用程序进行通讯，必须在正在监视的客户端应用程序和节点之间的路由器和防火墙中打开此端口。

如果希望更改默认端口指派，请参见第 33.2.3.2 节“端口”[473]。

33.2.3.3 身份验证

SFCB 支持 HTTP 基本身份验证和基于客户端证书的身份验证（通过 SSL 连接的 HTTP）。基本 HTTP 身份验证通过在 SFCB 配置文件（默认是 `/etc/sfcb/sfcb.cfg`）中指定 `doBasicAuth=true` 来启用。SFCB 的 SUSE® Linux Enterprise Server 安装支持可嵌入身份验证模块 (PAM) 方式；因此本地 root 用户可以用本地 root 身份凭证验证至 SFCB CIMOM。

如果 `sslClientCertificate` 配置属性设置为 *accept* 或 *require*, SFCB HTTP 适配器通过 HTTP over SSL (HTTPS) 连接时, 会从客户端请求证书。如果指定了 *require*, 客户端**必须**提供有效的证书（根据通过 `sslClientTrustStore` 指定的客户端信任储存）。如果客户端未能提供, CIM 服务器将拒绝该连接。

`sslClientCertificate=accept` 设置可能不是显式的。如果同时允许基本和客户端证书身份验证, 它将很有用。如果客户端能提供有效的证书, 将建立 HTTPS 连接, 并且不会执行基本身份验证步骤。如果该功能不能校验证书, 则会发生 HTTP 基本身份验证。

33.3 SFCB CIMOM 配置

SFCB 是 CIM 服务器的“轻量级”实现, 但也是可以灵活配置的。有若干选项可控制其行为。您有三种基本方式可用来控制 SFCB 服务器:

- 设置相应环境变量
- 使用命令行选项
- 更改其配置文件

33.3.1 环境变量

有若干环境变量会直接影响 SFCB 的行为。您必须用 `rcsfcb restart` 重新启动 SFCB 守护程序使更改生效。

`PATH`

指定 `sfcbsd` 守护程序和实用程序的路径。

`LD_LIBRARY_PATH`

指定 `sfcb` 运行时库的路径。或者可以将此路径添加到系统范围的动态加载器配置文件 `/etc/ld.so.conf` 中。

`SFCB_PAUSE_PROVIDER`

指定提供程序的名称。SFCB 服务器会在第一次装载提供程序后暂停。然后您就可以将运行时调试程序加到提供程序的进程中, 以便调试。

SFCB_PAUSE_CODEC

指定 SFCB 编解码器（目前仅支持 http）的名称。SFCB 服务器将在第一次装载编解码器后暂停。然后您就可以将运行时调试程序加到进程中。

SFCB_TRACE

为 SFCB 指定调试消息的级别。有效值有 0（无调试消息）、1（关键调试消息）和 4（全部调试消息）。默认值是 1。

SFCB_TRACE_FILE

默认情况下，SFCB 将其调试消息输出到标准错误输出 (STDERR)。设置该值会将调试消息写入指定的文件。

SBLIM_TRACE

为 SBLIM 提供程序指定调试消息级别。有效值有 0（无调试消息）、1（关键调试消息）和 4（全部调试消息）。

SBLIM_TRACE_FILE

默认情况下，SBLIM 提供程序将把跟踪消息输出到 STDERR。设置该值会将调试消息写入指定的文件。

33.3.2 命令行选项

SFCB 守护程序 `sfcbsd` 有若干命令行选项，可以打开或关闭特定运行时功能。SFCB 守护程序启动时输入这些选项。

`-c, --config-file=FILE`

SFCB 守护程序启动时，默认会从 `/etc/sfcb/sfcb.cfg` 读取其配置。您可以用该选项指定备用配置文件。

`-d, --daemon`

强制 `sfcbsd` 及其子进程在后台运行。

`-s, --collect-stats`

打开运行时统计数字收集。各种 `sfcbsd` 运行时统计数字都会写入当前工作目录下的 `sfcbStat` 文件。默认情况下，不收集统计数字。

`-l, --syslog-level=LOGLEVEL`

指定系统日志的详细程度级别。`LOGLEVEL` 可以是 `LOG_INFO`、`LOG_DEBUG` 或 `LOG_ERR`（默认）。

`-k, --color-trace=日志级别`
以不同颜色打印每个进程的跟踪输出，以便调试。

`-t, --trace-components=NUM`
激活组件级跟踪消息，其中 *NUM* 是进行 OR 运算的位掩码整数，它定义要跟踪哪个组件。您指定 `-t ?` 后，它会列出所有组件及其相关整数位掩码：

```
tux@mercury:~> sfcbd -t ?
---   Traceable Components:      Int      Hex
---   providerMgr:                1 0x0000001
---   providerDrv:                2 0x0000002
---   cimxmlProc:                 4 0x0000004
---   httpDaemon:                 8 0x0000008
---   upCalls:                    16 0x0000010
---   encCalls:                   32 0x0000020
---   ProviderInstMgr:            64 0x0000040
---   providerAssocMgr:          128 0x0000080
---   providers:                  256 0x0000100
---   indProvider:                512 0x0000200
---   internalProvider:          1024 0x0000400
---   objectImpl:                 2048 0x0000800
---   xmlIn:                      4096 0x0001000
---   xmlOut:                     8192 0x0002000
---   sockets:                   16384 0x0004000
---   memoryMgr:                  32768 0x0008000
---   msgQueue:                   65536 0x0010000
---   xmlParsing:                 131072 0x0020000
---   responseTiming:             262144 0x0040000
---   dbpdaemon:                  524288 0x0080000
---   slp:                        1048576 0x0100000
```

能反映 `sfcbd` 的内部功能，但不会产生过多消息的有用值是 `-t 2019`。

33.3.3 SFCB 配置文件

SFCB 启动后从配置文件 `/etc/sfcb/sfcb.cfg` 读取其运行时配置。该行为在启动时可以用 `-c` 选项覆盖。

配置文件包含选项:值对，一行一对。当对此文件执行更改时，如果文本编辑器保存文件的格式是所使用环境的本机格式，则可以使用此文本编辑器更改文件。

由井号 (#) 注释的选项的所有设置都使用默认设置。

以下选项列表可能不完整。查看 `/etc/sfcb/sfcb.cfg` 和 `/usr/share/doc/packages/sblim-sfcb/README` 的内容以获取其完整列表。

33.3.3.1 httpPort

目的

指定 sfcbd 用于侦听接收自 CIM 客户端的 HTTP（非安全）请求的本地端口值。
默认值是 5988。

语法

httpPort: 端口号

33.3.3.2 enableHttp

目的

指定 SFCB 是否接受 HTTP 客户端的连接。默认为 false。

语法

enableHttp: 选项

选项	描述
true	启用 HTTP 连接。
false	禁用 HTTP 连接。

33.3.3.3 httpProcs

目的

指定在阻止新进来的 HTTP 请求之前，HTTP 客户端连接的最大并行数。默认值是 8。

语法

`httpProcs`: 最大连接数

33.3.3.4 httpUserSFCB、httpUser

目的

这些选项控制将运行 `http` 服务器的用户。如果 `httpUserSFCB` 为 `true`，`http` 将以 `SFCB` 主进程的同一用户身份运行。如果为 `false`，将使用为 `httpUser` 指定的用户名。此设置用于 `http` 和 `https` 服务器。如果 `httpUserSFCB` 设置为 `false`，则必须指定 `httpUser`。默认值为 `true`。

语法

`httpUserSFCB`: *true*

33.3.3.5 httpLocalOnly

目的

指定是否将 HTTP 请求限制为仅 `localhost`。默认为 `false`。

语法

`httpLocalOnly`: *false*

33.3.3.6 httpsPort

目的

指定 `sfcdb` 侦听来自 CIM 客户端的 HTTPS 请求的本地端口值。默认值是 5989。

语法

`httpsPort`: 端口号

33.3.3.7 enableHttps

目的

指定 SFCB 是否接受 HTTPS 客户端连接。默认值是 `true`。

语法

`enableHttps`: 选项

选项	描述
<code>true</code>	启用 HTTPS 连接。
<code>false</code>	禁用 HTTPS 连接。

33.3.3.8 httpsProcs

目的

指定在阻止新进来的 HTTPS 请求之前，HTTPS 客户端连接的最大并行数。默认为 8。

语法

`httpsProcs`: 最大连接数

33.3.3.9 enableInterOp

目的

指定 SFCB 是否为指示支持提供 *interop* 名称空间。默认值是 `true`。

语法

`enableInterOp`: 选项

选项	描述
true	启用 interop 名称空间。
false	禁用 interop 名称空间。

33.3.3.10 provProcs

目的

指定并发提供程序进程的最大数。达到这点之后，如果有新进来的请求要求装载新提供程序，则现有提供程序之一将自动卸载。默认值是 32。

语法

provProcs: 最大进程数

33.3.3.11 doBasicAuth

目的

根据客户端用户标识符打开或关闭它接受请求之前所做的基本身份验证。默认值为 true，表示执行基本客户端身份验证。

语法

doBasicAuth: 选项

选项	描述
true	启用基本身份验证。
false	禁用基本身份验证。

33.3.3.12 basicAuthLib

目的

指定本地库名称。SFCB 服务器将装载该库以验证客户端用户标识符。默认值是 `sfcBasicPAMAuthentication`。

语法

`provProcs`: 最大进程数

33.3.3.13 useChunking

目的

该选项启用或禁用 HTTP/HTTPS“分块”。如果启用，服务器将以小“块”形式将大量响应数据返回客户端，而不是缓存数据并以一个大块全部发回。默认值是 `true`。

语法

`useChunking`: 选项

选项	描述
<code>true</code>	启用 HTTP/HTTPS 数据分块。
<code>false</code>	禁用 HTTP/HTTPS 数据分块。

33.3.3.14 keepaliveTimeout

目的

指定一个连接上的 SFCB HTTP 进程在两次请求之间最多等待多少秒就终止。将它设置为 0 将禁用 HTTP keep-alive。默认值是 0。

语法

`keepaliveTimeout`: *秒*

33.3.3.15 keepaliveMaxRequest

目的

指定一个连接上连续请求的最大数。将它设置为 0 将禁用 HTTP keep-alive。默认值是 10。

语法

`keepaliveMaxRequest`: *连接数*

33.3.3.16 registrationDir

目的

指定注册目录，它包含提供程序的注册数据、分阶段区域和静态安装源。默认值是 `/var/lib/sfcb/registration`。

语法

`registrationDir`: *目录*

33.3.3.17 providerDirs

目的

指定 SFCB 搜索提供程序库的目录的空格分隔列表。默认值是 `/usr/lib64 /usr/lib64 /usr/lib64/cmpi`。

语法

`providerDirs`: *目录*

33.3.3.18 providerSampleInterval

目的

指定提供程序管理器间隔多少秒检查空闲的提供程序。默认值是 30。

语法

providerSampleInterval: 秒

33.3.3.19 providerTimeoutInterval

目的

指定提供程序管理器经过多少秒的间隔就卸载空闲的提供程序。默认值是 60。

语法

providerTimeoutInterval: 秒

33.3.3.20 providerAutoGroup

目的

如果提供程序注册文件未指定任何其他组，而该选项设置为 *true*，则同一共享库内的所有提供程序都将在同一进程中执行。

语法

providerAutoGroup: 选项

选项	描述
true	启用提供程序分组。
false	禁用提供程序分组。

33.3.3.21 sslCertificateFilePath

目的

指定包含服务器证书的文件的名称。该文件必须是 PEM (保密邮件, RFC 1421 和 RFC 1424) 格式。只有当 `enableHttps` 设置为 `true` 时才需要该文件。默认值是 `/etc/sfcb/server.pem`。

语法

`sslCertificateFilePath`: 路径

33.3.3.22 sslKeyFilePath

目的

指定包含服务器证书私用密钥的文件的名称。该文件必须是 PEM 格式且不能有通行密码的保护。该文件仅当 `enableHttps` 设置为 `true` 时才需要。默认值是 `/etc/sfcb/file.pem`。

语法

`sslKeyFilePath`: 路径

33.3.3.23 sslClientTrustStore

目的

指定包含客户端的 CA 或自我签名证书的文件的名称。该文件必须是 PEM 格式, 只有当 `sslClientCertificate` 设置为 `accept` 或 `require` 时才需要。默认值是 `/etc/sfcb/client.pem`。

语法

`sslClientTrustStore`: 路径

33.3.3.24 sslClientCertificate

目的

指定 SFCB 处理基于客户端证书的身份验证的方式。如果设置为 `ignore`，将不会从客户端请求证书。如果设置为 `accept`，它会从客户端请求证书，但即使客户端没有证书也不会失败。如果设置为 `require`，会在客户端不存在证书时拒绝客户端连接。默认值是 `ignore`。

语法

`sslClientCertificate`: 选项

选项	描述
<code>ignore</code>	禁止请求客户端证书。
<code>接受</code>	禁止请求客户端证书。 如果证书不存在，不会失败。
<code>require</code>	拒绝无有效证书的客户端连接。

33.3.3.25 certificateAuthLib

目的

指定用于请求基于客户端证书的用户身份验证的本地库名称。只有当 `sslClientCertificate` 未设置成 `ignore` 时才这样请求。默认值是 `sfcCertificateAuthentication`。

语法

`certificateAuthLib`: 文件

33.3.3.26 traceLevel

目的

指定 SFCB 的跟踪级别您可以通过设置环境变量 `SFCB_TRACE_LEVEL` 覆盖它。默认值是 0。

语法

`traceLevel`: 级别数

33.3.3.27 traceMask

目的

指定 SFCB 的跟踪掩码。您可以用命令行选项 `--trace-components` 覆盖它。默认值是 0。

语法

`traceMask`: 掩码

33.3.3.28 tracefile

目的

为 SFCB 指定跟踪文件。您可以通过设置环境变量 `SFCB_TRACE_FILE` 覆盖它。默认值是 `stderr`（标准错误输出）。

语法

`traceFile`: 输出

33.4 高级 SFCB 任务

本章涵盖了与 SFCB 使用相关的更多高级主题。要了解这些主题，您需要有 Linux 文件系统的基础知识，并具有使用 Linux 命令行的经验。本章包括以下任务：

- 安装 CMPI 提供程序
- 测试 SFCB
- 使用 `wbemcli` CIM 客户端

33.4.1 安装 CMPI 提供程序

要安装 CMPI 提供程序，您必须确保其共享库已复制到 `providerDirs` 配置选项所指定的目录之一，参见第 33.3.3.17 节“`providerDirs`”[482]。提供程序还必须用 `sfcbstage` 和 `sfcbrepos` 命令正确注册。

提供程序包通常是 SFCB 准备的，为此其安装过程负责进行正确的注册。多数 SBLIM 提供程序是为 SFCB 准备的。

33.4.1.1 类安装源

类安装源就是 SFCB 储存 CIM 类信息的位置。它通常由名称空间组件组成的目录树组成。典型的 CIM 名称空间如 `root/cimv2` 或 `root/interop`，它们会分别转换为文件系统上的类安装源目录路径

```
/var/lib/sfcb/registration/repository/root/cimv2
```

和

```
/var/lib/sfcb/registration/repository/root/interop
```

每个名称空间目录都包含文件 `classSchemas`。该文件中有该名称空间下注册的所有 CIM 类的已编译二进制表示。它还包含有关其 CIM 超类的必要信息。

此外，每个名称空间目录都可能包含文件 `qualifiers`，其中包含了该名称空间的所有限定符。`sfcbd` 重新启动时，类提供程序会扫描目录 `/var/lib/sfcb/`

registration/repository/ 及其全部子目录，以确定注册的名称空间。然后将解码 classSchemas 文件，为每个名称空间构建类的层次结构。

33.4.1.2 添加新类

SFCB 不能在线处理 CIM 类。您需要脱机添加、更改或删除类，用 `rscfcb restart` 重启动 SFCB 服务来注册这些更改。

为储存提供程序类和注册信息，SFCB 使用名为分阶段区域的位置。在 SUSE® Linux Enterprise Server 系统上，它就是 `/var/lib/sfcb/stage/` 下的目录结构。

为添加新的提供程序，您必须：

- 将提供程序类定义文件复制到分阶段区域目录的子目录 `./mofs(/var/lib/sfcb/stage/mofs)`。
- 将包含类名、提供程序类型和可执行库文件名的注册文件复制到 `./regs` 子目录。

分阶段目录中有两个默认的“mof”（类定义）文件：`indication.mof` 和 `interop.mof`。运行 `sfcbrepos` 命令后，`root` 阶段目录 `/var/lib/sfcb/stage/mofs` 下的 MOF 文件将复制到每个名称空间。`interop.mof` 将只编译到 *interop* 名称空间。

目录布局看上去如下所示：

```
tux@mercury:~> ls /var/lib/sfcb/stage
default.reg  mofs  regs

tux@mercury:~> ls /var/lib/sfcb/stage/mofs
indication.mof  root

tux@mercury:~> ls /var/lib/sfcb/stage/mofs/root
cimv2  interop  suse  virt

tux@mercury:~> ls -l /var/lib/sfcb/stage/mofs/root/cimv2 | less
Linux_ABIParameter.mof
Linux_BaseIndication.mof
Linux_Base.mof
Linux_DHCPElementConformsToProfile.mof
Linux_DHCPEntity.mof
[...]
OMC_StorageSettingWithHints.mof
OMC_StorageVolumeDevice.mof
```

```

OMC_StorageVolume.mof
OMC_StorageVolumeStorageSynchronized.mof
OMC_SystemStorageCapabilities.mof

tux@mercury:~> ls -l /var/lib/sfcb/stage/mofs/root/interop
ComputerSystem.mof
ElementConformsToProfile.mof
HostSystem.mof
interop.mof
Linux_DHCPElementConformsToProfile.mof
[.]
OMC_SMIElementSoftwareIdentity.mof
OMC_SMISubProfileRequiresProfile.mof
OMC_SMIVolumeManagementSoftware.mof
ReferencedProfile.mof
RegisteredProfile.mof

tux@mercury:~> ls -l /var/lib/sfcb/stage/regs
AllocationCapabilities.reg
Linux_ABIParameter.reg
Linux_BaseIndication.reg
Linux_DHCPGlobal.reg
Linux_DHCPRegisteredProfile.reg
[.]
OMC_Base.sfcb.reg
OMC_CopyServices.sfcb.reg
OMC_PowerManagement.sfcb.reg
OMC_Server.sfcb.reg
RegisteredProfile.reg

tux@mercury:~> cat /var/lib/sfcb/stage/regs/Linux_DHCPRegisteredProfile.reg
[Linux_DHCPRegisteredProfile]
    provider: Linux_DHCPRegisteredProfileProvider
    location: cmpiLinux_DHCPRegisteredProfile
    type: instance
    namespace: root/interop
#
[Linux_DHCPElementConformsToProfile]
    provider: Linux_DHCPElementConformsToProfileProvider
    location: cmpiLinux_DHCPElementConformsToProfile
    type: instance association
    namespace: root/cimv2
#
[Linux_DHCPElementConformsToProfile]
    provider: Linux_DHCPElementConformsToProfileProvider
    location: cmpiLinux_DHCPElementConformsToProfile
    type: instance association
    namespace: root/interop

```

SFCB 对每个提供程序使用自定义提供程序注册文件。

注意：SBLIM 提供程序注册文件

SBLIM 网站上的所有 SBLIM 提供程序都已包括用于生成 SFCB 的 .reg 文件的注册文件。

SFCB 注册文件的格式是：

```
[<class-name>]
  provider: <provide-name>
  location: <library-name>
  type: [instance] [association] [method] [indication]
  group: <group-name>
  unload: never
  namespace: <namespace-for-class> ...
```

其中：

<类名>

CIM 类名（必需）

<提供程序名称>

CMPI 提供程序名称（必需）

<位置名称>

提供程序库的名称（必需）

type

提供程序的类型（必需）它可以是以下的任意组合：instance、association、method 或 indication。

<组名>

可以将多个提供程序组合起来，在单一进程下运行，以进一步最小化运行时资源的占用。所有注册在同一 <组名> 下的提供程序都将在同一进程下执行。默认情况下每个提供程序作为单独的进程运行。

unload

指定提供程序的卸载策略。目前唯一支持的选项是 never，即指定不监视提供程序的空闲次数，也从不卸载。默认情况下，每个提供程序只要空闲次数超过配置文件中指定的值就卸载。

namespace

可执行本提供程序的名称空间的列表。这是必需的，尽管对于多数提供程序来说它就是 *root/cimv2*。

所有类定义和提供程序注册文件都储存在分阶段区域后，就需要用命令 `sfcbrepos -f` 重建 SFCB 类安装源。

您可以用这种方式添加、更改或删除类。重建类安装源后，用命令 `rscfcb restart` 重启 SFCB。

或者，SFCB 包包含一个实用程序，它会将提供程序类 `mof` 文件和注册文件复制到分阶段区域中正确的位置。

```
sfcbstage -r [provider.reg] [class1.mof] [class2.mof] ...
```

运行该命令后，您还需要重建类安装源并重启 SFCB 服务。

33.4.2 测试 SFCB

SFCB 包包括两个测试脚本：`wbemcat` 和 `xmltest`。

`wbemcat` 通过 HTTP 协议将原始 CIM-XML 数据发送到端口 5988 上正在侦听的指定 SFCB 主机（默认为本地主机）。然后它会显示返回的结果以下文件包含标准 `EnumerateClasses` 请求的 CIM-XML 表示：

```
<?xml version="1.0" encoding="utf-8"?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
  <MESSAGE ID="4711" PROTOCOLVERSION="1.0">
    <SIMPLEREQ>
      <IMETHODCALL NAME="EnumerateClasses">
        <LOCALNAMESPACEPATH>
          <NAMESPACE NAME="root"/>
          <NAMESPACE NAME="cimv2"/>
        </LOCALNAMESPACEPATH>
        <IPARAMVALUE NAME="ClassName">
          <CLASSNAME NAME=""/>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="DeepInheritance">
          <VALUE>TRUE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="LocalOnly">
          <VALUE>FALSE</VALUE>
        </IPARAMVALUE>
        <IPARAMVALUE NAME="IncludeQualifiers">
```

```

        <VALUE>FALSE</VALUE>
    </IPARAMVALUE>
    <IPARAMVALUE NAME="IncludeClassOrigin">
        <VALUE>TRUE</VALUE>
    </IPARAMVALUE>
    </IMETHODCALL>
</CIM></SIMPLEREQ>
</MESSAGE>
</CIM>

```

将该请求发送到 **SFCB CIMOM** 后，会返回具有已注册提供程序的所有支持类的列表。假定您将文件保存为 `cim_xml_test.xml`。

```

tux@mercury:~> wbemcat cim_xml_test.xml | less
HTTP/1.1 200 OK
Content-Type: application/xml; charset="utf-8"
Content-Length: 337565
Cache-Control: no-cache
CIMOperation: MethodResponse

<?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0">
<SIMPLERSP>
<IMETHODRESPONSE NAME="EnumerateClasses">
[... ]
<CLASS NAME="Linux_DHCPParamsForEntity" SUPERCLASS="CIM_Component">
<PROPERTY.REFERENCE NAME="GroupComponent" REFERENCECLASS="Linux_DHCPEntity">
</PROPERTY.REFERENCE>
<PROPERTY.REFERENCE NAME="PartComponent" REFERENCECLASS="Linux_DHCPParams">
</PROPERTY.REFERENCE>
</CLASS>
</IRETURNVALUE>
</IMETHODRESPONSE>
</SIMPLERSP>
</MESSAGE>
</CIM>

```

列出的类会随您在系统上安装的提供程序的不同而不同。

第二个脚本 `xmltest` 也用于将原始 **CIM-XML** 测试文件发送到 **SFCB CIMOM**。它会随即比较返回的结果和以前保存的“OK”结果文件。如果还不存在对应的“OK”文件，将创建它以备用：

```

tux@mercury:~> xmltest cim_xml_test.xml
Running test cim_xml_test.xml ... OK
Saving response as cim_xml_test.OK
tux@mercury:~> xmltest cim_xml_test.xml
Running test cim_xml_test.xml ... Passed

```

33.4.3 命令行 CIM 客户端：wbemcli

除了 `wbemcat` 和 `xmltest` 外，SBLIM 项目包含更高级的命令行 CIM 客户端 `wbemcli`。该客户端用于将 CIM 请求发送到 SFCB 服务器，并显示返回的结果。它独立于 CIMOM 库，可与所有 WBEM 兼容实现一起使用。

例如，如果您需要列出注册到您的 SFCB 的 SBLIM 提供程序实现的所有类，则将 “EnumerateClasses” (ec) 请求发送到 SFCB：

```
tux@mercury:~> wbemcli -dx ec http://localhost/root/cimv2
To server: <?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0"><SIMPLEREQ><IMETHODCALL \
  NAME="EnumerateClasses"><LOCALNAMESPACEPATH><NAMESPACE NAME="root"> \
    </NAMESPACE><NAMESPACE NAME="cimv2"></NAMESPACE> \
  </LOCALNAMESPACEPATH>
<IPARAMVALUE NAME="DeepInheritance"><VALUE>TRUE</VALUE> \
  </IPARAMVALUE>
<IPARAMVALUE NAME="LocalOnly"><VALUE>FALSE</VALUE></IPARAMVALUE>
<IPARAMVALUE NAME="IncludeQualifiers"><VALUE>FALSE</VALUE> \
  </IPARAMVALUE>
<IPARAMVALUE NAME="IncludeClassOrigin"><VALUE>TRUE</VALUE> \
  </IPARAMVALUE>
</IMETHODCALL></SIMPLEREQ>
</MESSAGE></CIM>
From server: Content-Type: application/xml; charset="utf-8"
From server: Content-Length: 337565
From server: Cache-Control: no-cache
From server: CIMOperation: MethodResponse
From server: <?xml version="1.0" encoding="utf-8" ?>
<CIM CIMVERSION="2.0" DTDVERSION="2.0">
<MESSAGE ID="4711" PROTOCOLVERSION="1.0">
<SIMPLERSP>
<IMETHODRESPONSE NAME="EnumerateClasses">
<IRETURNVALUE>
<CLASS NAME="CIM_ResourcePool" SUPERCLASS="CIM_LogicalElement">
<PROPERTY NAME="Generation" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="ElementName" TYPE="string">
</PROPERTY>
<PROPERTY NAME="Description" TYPE="string">
</PROPERTY>
<PROPERTY NAME="Caption" TYPE="string">
</PROPERTY>
<PROPERTY NAME="InstallDate" TYPE="datetime">
</PROPERTY>
[... ]
<CLASS NAME="Linux_ReiserFileSystem" SUPERCLASS="CIM_UnixLocalFileSystem">
<PROPERTY NAME="FSReservedCapacity" TYPE="uint64">
</PROPERTY>
```

```

<PROPERTY NAME="TotalInodes" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="FreeInodes" TYPE="uint64">
</PROPERTY>
<PROPERTY NAME="ResizeIncrement" TYPE="uint64">
<VALUE>0</VALUE>
</PROPERTY>
<PROPERTY NAME="IsFixedSize" TYPE="uint16">
<VALUE>0</VALUE>
</PROPERTY>
[...]
```

-dx 选项向您显示 wbemcli 发送到 SFCB 的实际 XML，以及收到的实际 XML。在以上示例中，众多返回类中的第一个就是 CIM_ResourcePool，后面是 Linux_ReiserFileSystem。类似的条目会对所有其他注册的类显示。

如果您省略 -dx 选项，wbemcli 会显示返回数据的简化表示：

```

tux@mercury:~> wbmcli ec http://localhost/root/cimv2
localhost:5988/root/cimv2:CIM_ResourcePool Generation=, ElementName=, \
    Description=, Caption=, InstallDate=, Name=, OperationalStatus=, \
    StatusDescriptions=, Status=, HealthState=, PrimaryStatus=, \
    DetailedStatus=, OperatingStatus=, CommunicationStatus=, InstanceID=, \
    PoolID=, Primordial=, Capacity=, Reserved=, ResourceType=, \
    OtherResourceType=, ResourceSubType=, \AllocationUnits=
localhost:5988/root/cimv2:Linux_ReiserFileSystem FSReservedCapacity=, \
    TotalInodes=, FreeInodes=, ResizeIncrement=, IsFixedSize=, NumberOfFiles=, \
    OtherPersistenceType=, PersistenceType=, FileSystemType=, ClusterSize=, \
    MaxFileNameLength=, CodeSet=, CasePreserved=, CaseSensitive=, \
    CompressionMethod=, EncryptionMethod=, ReadOnly=, AvailableSpace=, \
    FileSystemSize=, BlockSize=, Root=, Name=, CreationClassName=, CSName=, \
    CSCreationClassName=, Generation=, ElementName=, Description=, Caption=, \
    InstanceID=, InstallDate=, OperationalStatus=, StatusDescriptions=, \
    Status=, HealthState=, PrimaryStatus=, DetailedStatus=, OperatingStatus= \
    , CommunicationStatus=, EnabledState=, OtherEnabledState=, RequestedState= \
    , EnabledDefault=, TimeOfLastStateChange=, AvailableRequestedStates=, \
    TransitioningToState=, PercentageSpaceUse=
[...]
```

33.5 更多信息

有关 *WBEM* 和 *SFCB* 的细节，请参见以下来源：

<http://www.dmtf.org>

Distributed Management Task Force 网站

<http://www.dmtf.org/standards/wbem/>
Web-Based Enterprise Management (WBEM) 网站

<http://www.dmtf.org/standards/cim/>
通用信息模型 (CIM) 网站

<http://sblim.wiki.sourceforge.net/>
Standards Based Linux Instrumentation (SBLIM) 网站

<http://sblim.wiki.sourceforge.net/Sfcb>
小规模 CIM 中介程序 (SFCB) 网站

<http://sblim.wiki.sourceforge.net/Providers>
SBLIM 提供程序包

部分 V. 查错

帮助和文档

SUSE® Linux Enterprise Server 提供了各种信息和文档源，其中绝大部分已经集成在您的已安装系统中。

`/usr/share/doc` 中的文档

这一传统帮助目录包含各种文档文件以及系统的发行说明。它还包含子目录 `packages` 中的已安装包的信息。有关详细信息可以在第 34.1 节“文档目录” [500] 中找到。

外壳命令的手册页和信息页

使用外壳时，您不需要了解命令选项。外壳往往是通过手册页和信息页来提供集成帮助的。有关详细信息，请参见第 34.2 节“手册页” [501] 和第 34.3 节“信息页” [502]。

桌面帮助中心

KDE 桌面 (KDE help center) 和 GNOME 桌面 (Yelp) 的帮助中心按可搜索的形式提供了对系统上最重要的文档资源的集中访问方式。这些资源包括已安装应用程序、手册页、信息页以及随产品提供的 Novell/SUSE 手册的联机帮助。

某些应用程序的独立帮助包

当用 YaST 安装新软件时，大多数情况下会自动安装软件文档，并且这些文档通常会出现在您的桌面的帮助中心中。然而，某些应用程序（如 GIMP）可能具有不同的联机帮助包，可与 YaST 分开安装，并且未集成到帮助中心。

34.1 文档目录

在您安装的 Linux 系统上查找文档的传统目录是 `/usr/share/doc`。目录通常包含有关您的系统上已安装的包和发行说明、手册等等的信息。

注意：内容取决于所安装的包

在 Linux 领域，许多手册和其他各类文档都以包的形式提供，就像软件一样。`/usr/share/docs` 中的信息量和信息内容还取决于安装的（文档）包。如果您找不到这里提到的子目录，请检查各包是否都安装到您的系统上，必要时用 YaST 添加它们。

34.1.1 Novell/SUSE 手册

我们的书籍提供不同语言的 HTML 和 PDF 版本。在 `manual` 子目录下有您的产品可用的大多数 Novell/SUSE 手册的 HTML 版。有关对您的产品可用的所有文档的概述，请参见这些手册的前言。

如果安装了多种语言，`/usr/share/doc/manual` 可能包含这些手册的不同语言版本。两个桌面的帮助中心也提供 HTML 版本的 Novell/SUSE 手册。有关在安装媒体的何处能找到这些书的 PDF 和 HTML 版本的信息，请参见 SUSE Linux Enterprise Server 发行说明。它们位于所安装系统的 `/usr/share/doc/release-notes/` 下，或者也可以联机访问您的产品专属网站：<http://www.suse.com/doc/>。

34.1.2 HOWTO

如果系统上安装了操作指南包，`/usr/share/doc` 还会包含 `howto` 子目录，其中有与 Linux 软件的安装和操作相关的许多任务的附加文档。

34.1.3 包文档

在 `packages` 下可找到系统上安装的软件包中包含的文档。对每个包都会创建 `/usr/share/doc/packages/包名称`。它经常包含该包的自述文件，有时还

包含示例、配置文件或其他脚本。下表列出了 `/usr/share/doc/packages` 下常见的文件。这些条目都不是必需的，许多包可能只有其中一部分。

AUTHORS

主要开发者列表。

BUGS

已知 bug 或故障。还可能包含到 Bugzilla 网页的链接，您可以在该页面上搜索所有 bug。

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。

FAQ

从邮件列表或新闻组收集的问题和回答。

INSTALL

如何在系统上安装此包。因为您读到该文件前该包已安装，您可以放心地忽略该文件的内容。

README、README.*

软件的常规信息。例如用途和用法。

TODO

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。

34.2 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。许多页面都可以用 `man` 后面跟命令名来访问，例如 `man ls`。

手册页直接显示在外壳中。可以用 **Page ↑** 和 **Page ↓** 上下移动来浏览它们。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。手册页如表 34.1 “手册页 — 类别和描述” [502] 所示按类别进行排序（取自 `man` 命令本身的手册页）。

表 34.1 手册页 — 类别和描述

号码	描述
1	可执行程序或外壳命令
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> ）
9	内核例程（非标准）

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。

34.3 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。要查看特定命令的信息页，请输入 `info` 后面跟命令名，例如 `info ls`。您可以在外壳中直接用查看器浏览信息页，并显示名为“节点”的各个部分。的不同部分。用 **Space** 前移，用 **<—** 后移。在节点内，您也可以用 **Page ↑** 和 **Page ↓** 浏览，但

只有 **Space** 和 **<—** 仍会带您到上个或下个节点。按 **Q** 结束查看模式。并非每一个手册页都有信息页，反之亦然。

34.4 联机资源

除了安装在 `/usr/share/doc` 下的联机版 Novell 手册之外，您还可以访问 Web 上的产品特定手册和文档。有关 SUSE Linux Enterprise Server 所有适用文档的概述，请查看产品特定的文档网页（位于 <http://www.novell.com/documentation/>）。

如果要搜索更多产品相关信息，您也可以参见以下网站：

Novell 技术支持知识库

Novell 技术支持知识库的网址是 <http://www.novell.com/support/>。知识库中主要是一些针对 SUSE Linux Enterprise Server 的技术问题而给出的解决方案的文章。

Novell 论坛

Novell 有多个论坛，您可以进入讨论有关 Novell 产品的话题。如需获取一份列表，请参见 <http://forums.novell.com/>。

超酷解决方案

联机社区提供文章、提示、问答和可供免费下载的工具：<http://www.novell.com/communities/cool solutions>

KDE 文档

在文档中可以找到适合用户和管理员的 KDE 的多方面信息：<http://www.kde.org/documentation/>。

GNOME 文档

适用于 GNOME 用户、管理员和开发人员的文档可在 <http://library.gnome.org/> 上找到。

Linux 文档计划

Linux 文档计划（Linux Documentation Project, TLDP）由编写 Linux 相关文档的志愿者团队负责管理（请参见 <http://www.tldp.org>）。它可能是 Linux 相关的最全面的文档资源。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）。SUSE Linux Enterprise Server 上也有来自 TLDP 的部分文档

您可能需要使用通用搜索引擎。例如，如果在刻录 CD 或转换 LibreOffice 文件时遇到问题，请使用搜索项 Linux CD-RW 帮助或 OpenOffice 文件转换问题。Google™ 在 <http://www.google.com/linux> 上也有特定于 Linux 的搜索引擎，可能会对您有所帮助。

常见问题及其解决方案

本章将描述一系列可能发生的问题及其解决方法。即使您的情况并未精确地列在这里，也可能有足够相似的情况可提供解决您的问题的方法提示。

35.1 查找和收集信息

Linux 报告情况时是很详细的。在您的系统遇到问题时，有几个地方可以查看，大多数是 Linux 系统的标准问题，有一些是与 SUSE Linux Enterprise Server 系统相关的问题。多数日志文件可以用 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，然后选择问题类别。当所有信息都被集合后，将其附加在您的支持请求。

将出现最常检查的日志文件的列表，并附有其典型用途说明。包含 ~ 的路径是指当前用户的用户主目录。

表 35.1 日志文件

日志文件	描述
<code>~/ .xsession-errors</code>	来自当前运行的桌面应用程序的消息。
<code>/var/log/apparmor/</code>	来自 AppArmor 的日志文件，详细信息请参见第 IV 部分“Confining

日志文件	描述
	Privileges with AppArmor” (↑安全指南)。
/var/log/audit/audit.log	来自审计的日志文件，用来跟踪对系统的文件、目录或资源的任何访问，并跟踪系统调用。
/var/log/boot.msg	引导期间报告的来自内核的消息。
/var/log/mail.*	来自邮件系统的消息。
/var/log/messages	（运行时）来自内核和系统日志守护程序的消息。
/var/log/NetworkManager	NetworkManager 的日志文件，用于收集网络连接性问题
/var/log/samba/	包含 Samba 服务器及客户端日志消息的目录。
/var/log/SaX.log	来自 SaX 屏幕和 KVM 系统的硬件消息。
/var/log/warn	所有来自内核与系统日志守护程序的消息为“警告”或更高级别。
/var/log/wtmp	包含当前计算机会话的用户登录记录的二进制文件。可使用 last 查看它。
/var/log/Xorg.*.log	来自 X Window 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。

日志文件	描述
<code>/var/log/zypper.log</code>	zypper 的日志文件。

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 35.2: `/proc` 文件系统的系统信息

表 35.2 `/proc` 文件系统的系统信息

文件	描述
<code>/proc/cpuinfo</code>	包含处理器信息，包括处理器类型、制造商、型号和性能。
<code>/proc/dma</code>	显示当前使用的 DMA 通道。
<code>/proc/interrupts</code>	显示正在使用的中断和已使用的中断数量。
<code>/proc/iomem</code>	显示 I/O（输入/输出）内存的状态。
<code>/proc/ioports</code>	显示当时正在使用的 I/O 端口。
<code>/proc/meminfo</code>	显示内存状态。
<code>/proc/modules</code>	显示各个模块。
<code>/proc/mounts</code>	显示当前装入的设备。
<code>/proc/partitions</code>	显示所有硬盘的分区。
<code>/proc/version</code>	显示当前的 Linux 版本。

除了 `/proc` 文件系统外，Linux 内核还可通过 `sysfs` 模块（一个内存内的文件系统）导出信息。该模块表示了内核对象及其属性以及关系。有关 `sysfs` 的更多信息，请参见第 14 章 *使用 `udev` 进行动态内核设备管理* [163] 中 `udev` 的环境。表 35.3 包含 `/sys` 下最常见目录的概述。

表 35.3 /sys 文件系统的系统信息

文件	描述
/sys/block	包含系统中发现的每个块设备的子目录。通常多数是磁盘类设备。
/sys/bus	包含每个物理总线类型的子目录。
/sys/class	包含按设备功能类型分组的子目录（如图形、网络、打印机等）
/sys/device	包含全局设备层次结构。

Linux 带有一些用于系统分析和监视的工具。请参见第 2 章 *System Monitoring Utilities* (↑系统分析和微调指南)以选择在系统诊断中使用的最重要的工具。

以下包含的每个情景都以一个描述问题的标题开头，后跟一两段内容，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情景的交叉引用。

35.2 安装问题

安装问题是指计算机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类情况的变通方案。

35.2.1 检查媒体

如果您使用 SUSE Linux Enterprise Server 安装媒体时遇到任何问题，用软件 >，媒体检查检查安装媒体的完整性。您自己刻录的媒体更有可能出问题。要检查 SUSE Linux Enterprise Server 媒体，将它插入驱动器中，在 YaST 的媒体检查屏幕中单击启动检查。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。

图 35.1 检查媒体



35.2.2 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。

图 35.2 显示硬件信息



35.2.3 没有可用于引导的 DVD 驱动器

如果您的计算机没有可引导的 DVD-ROM 驱动器，或者 Linux 不支持您的驱动器，则有几中无需内置 DVD 驱动器便可安装计算机的方法：

从软盘引导

创建一张引导软盘，然后从软盘而非 DVD 引导。

使用外置的引导设备

如果您的 BIOS 和安装内核支持，从外部 DVD 驱动器引导。

通过 PXE 进行网络引导

如果计算机没有 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。详情请参见第 14.1.3 节“通过 VNC—PXE Boot 和网络唤醒进行远程安装”（第 14 章 远程安装, ↑部署指南）和第 14.1.6 节“通过 SSH—PXE Boot 和“网络唤醒”进行远程安装”（第 14 章 远程安装, ↑部署指南）。

35.2.3.1 从软盘引导 (SYSLINUX)

在某些较旧的计算机上，没有可用于引导的 DVD 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。

引导磁盘包括加载程序 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。

35.2.3.2 外置引导设备

Linux 支持多数的现有 DVD 驱动器。如果系统上既没有 DVD 驱动器也没有软盘驱动器，仍可能用通过 USB、FireWire 或 SCSI 连接的外部 DVD 驱动器引导系统。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。

35.2.4 从安装媒体引导失败

计算机不从安装媒体引导的一个原因可能是 BIOS 中的引导顺序的设置不正确。BIOS 引导顺序必须将 DVD 驱动器设置为第一引导项。否则计算机将尝试从其他媒体引导，通常为硬盘。关于更改 BIOS 引导顺序的指南可在随主板提供的文档中找到，也可以参见以下段落。

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 键之一。按此键，直到出现 BIOS 设置屏幕。

过程 35.1 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* 或 *BOOT ORDER* 的子项。引导顺序形如 C, A 或 A, C。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 35.2 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 选择磁盘实用程序。现在将显示所连接的硬件组件。
记下您 DVD 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 DVD 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 35.3 美式键盘布局



35.2.5 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，可能由于安装内核中缺少此类硬件的支持或该内核中包含的某些功能（如 ACPI，它仍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 DVD 留在驱动器中，然后使用 **Ctrl + Alt + Del** 或硬件重设置按钮来重引导计算机。
- 2 在出现引导屏幕时，按 **F5** 键，使用键盘上的箭头键浏览至无 *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 6 章 *使用 YaST 进行安装* (†部署指南)中所述的步骤进行安装。

如果此操作失败，请按照以上步骤继续，但应选择安全设置。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，请参见 `/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。

`pnpcapi=off`

在您的 BIOS 设置包含错误的中断或端口时，此选项用于串行或并行问题。

`notsc`

禁用时戳计数器。此选项可用于解决系统上的计时问题。这是一项新功能，如果看到计算机上有衰退，尤其是时间相关的或甚至完全挂起，此选项值得一试。

`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。否则就没有用处。

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。

35.2.6 无法启动图形安装程序

在将媒体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）。

过程 35.3 安装时更改屏幕分辨率

1 引导以安装。

- 2 按 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 6 章 *使用 YaST 进行安装* (↑部署指南)中所述的步骤进行安装。

过程 35.4 用文本方式进行安装

- 1 引导以安装。
- 2 按 F3，然后选择文本方式。
- 3 选择安装，然后按第 6 章 *使用 YaST 进行安装* (↑部署指南)中所述的步骤进行安装。

过程 35.5 VNC 安装

- 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 VNC 安装的密码。

- 3 选择安装，然后按 Enter 键启动安装。

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，显示一条消息，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 Server 计算机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 6 章 *使用 YaST 进行安装* (↑部署指南)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。

看到提示时，提供您的 VNC 查看器的 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。

35.2.7 只能启动简陋的引导屏幕

将媒体插入了驱动器，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。如果计算机的图形内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 35.2.5 节“无法引导”[513]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**。

35.3 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）。

35.3.1 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 无法在计算机上启动。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 接受许可证协议。
- 6 在安装模式屏幕中，选择修复已安装系统。
- 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。

其他导致计算机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。

35.3.2 无图形登录

如果计算机能够启动，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 Window 系统的配置上。要检查运行级别配置，请作为 root 用户登录，然后检查计算机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：

```
tux@mercury:~> grep "id:" /etc/inittab
id:5:initdefault:
```


如果返回的行表明计算机的默认运行级别（`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，您的桌面或 X Windows 软件可能配置错误或已损坏。请检验 `/var/log/Xorg.*.log` 中的日志文件，查找它尝试启动的 X 服务器发出的详细消息。如果桌面在启动时发生故障，它可能将错误消息记录到 `/var/log/messages` 中。如果这些错误消息指出问题出在 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。

提示：手动启动 X Window 系统

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 Window 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。

35.4 登录问题

登录问题是指计算机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）。

35.4.1 有效的用户名和密码组合失败

如果系统配置为使用网络身份验证或目录服务，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计算机。以下是计算机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 35.5 节“网络问题”[526]。
- 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，则表现为计算机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 35.5 节“网络问题”[526]。
- 如果将系统配置为使用 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 身份验证将不再工作，因为该身份验证依赖于整个网络的通用时钟同步。
- 系统的身份验证配置不正确。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，请参见第 2 章 *Authentication with PAM* (†安全指南)。
- 主分区是加密的。有关该主题的详细信息，请参见第 35.4.3 节“登录至加密的主分区失败”[523]。

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 root 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。

35.4.2 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身份验证，还是使用网络身份验证。

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。
- 验证该特定用户的 X Window 系统可能存在问题，尤其是在安装当前版本之前，该用户的主目录已被其他 Linux 分发版使用时。

要找到本地登录失败的原因，请执行如下操作：

- 1 在尝试调试整个身份验证机制之前，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”模块更改用户的密码。注意 Caps Lock 键，如果需要请解锁。
- 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，因为可以在该计算机上身份验证此用户。尝试找出任何与 X Window 系统或桌面（GNOME 或 KDE）有关的错误。有关更多信息，请参见第 35.4.4 节“登录成功但 GNOME 桌面发生故障”[524] 和第 35.4.5 节“登录成功但 KDE 桌面发生故障”[524]。
- 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` 文件删除。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 身份验证问题。然后再次尝试图形登录。
- 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 Window 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，请参见第 35.4.4 节“登录成功但 GNOME 桌面发生故障”[524] 或第 35.4.5 节“登录成功但 KDE 桌面发生故障”[524]。

以下是在特定的计算机上对特定用户的网络身份验证可能失败的常见原因：

- 用户可能输入了错误的密码。
- 用户名存在于计算机的本地身份验证文件中，但同时网络身份验证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。
- 用户无权登录到身份验证系统中的该特定主机。
- 计算机出于某种原因更改了主机名，而用户无权登录到该主机。
- 计算机无法访问包含该用户信息的身份验证服务器或目录服务器。
- 验证该特定用户的 X Window 系统可能存在问题，尤其是在安装当前办法之前，该用户的主目录已被其他 Linux 分发版使用时。

要通过网络身份验证找到登录问题的原因，请执行以下步骤：

- 1 在尝试调试整个身份验证机制之前，请检查用户所记的密码是否正确。
- 2 确定计算机在身份验证时要依赖的目录服务器，并确保计算机在正常运行且与其他计算机正常通讯。
- 3 确定该用户的用户名和密码在其他计算机上是否有效，以确保存在该用户的身份验证数据且已正确分发。
- 4 确定其他用户是否可以登录到该故障计算机。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消息。
- 5 尝试从控制台登录（使用 `Ctrl + Alt + F1`）。如果成功，则问题不在用户主目录中的 PAM 或目录服务器上，因为可以在该计算机上验证此用户。尝试找出任何与 X Window 系统或桌面（GNOME 或 KDE）有关的错误。有关更多信息，请参见第 35.4.4 节“登录成功但 GNOME 桌面发生故障”[524] 和第 35.4.5 节“登录成功但 KDE 桌面发生故障”[524]。
- 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` 文件删除。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 身份验证问题。然后再次尝试图形登录。

- 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 Window 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，请参见第 35.4.4 节“登录成功但 GNOME 桌面发生故障”[524] 或第 35.4.5 节“登录成功但 KDE 桌面发生故障”[524]。

35.4.3 登录至加密的主分区失败

对于便携式计算机建议使用加密的主分区。如果无法登录到您的便携式计算机，原因通常很简单：您的分区无法解锁。

在引导时，必须输入通行密码来解锁加密的分区。如果不输入它，引导进程继续，但保持分区锁定。

要解锁您的加密分区，请如下操作：

- 1 按 `Ctrl + Alt + F1` 切换到文本控制台。
- 2 成为 `root` 用户。
- 3 用以下步骤重新启动解锁进程：

```
/etc/init.d/boot.crypto restart
```

- 4 输入您的通行密码以解锁加密的分区。
- 5 用 `Alt + F7` 退出文本控制台并切换回登录屏幕。
- 6 如常登录。

35.4.4 登录成功但 GNOME 桌面发生故障

如果是这种情况，可能您的 GNOME 配置文件已损坏。可能出现的症状包括键盘不起作用、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，该计算机能正常运行。那么可能只需将用户的 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 电子邮件客户端数据）：

```
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。

35.4.5 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。将缓存数据删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。

要删除 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/ksocket-user
```

使用您的用户名来替换 *user*。将这两个目录删除只是删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：

- 对于 KDE3 使用以下命令：

```
mv .kde .kde-ORIG-RECOVER  
mv .skel .skel-ORIG-RECOVER
```

- 对于 KDE4 使用以下命令：

```
mv .kde4 .kde4-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 KDEDIR/share .kde/share
```

将 *KDEDIR* 替换为步骤 3 [525] 中的目录。

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。

35.5 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可能是某种网络问题造成的。本节介绍一个简单的核对表，您可以使用它来确定任何所遇到的网络问题的原因。

过程 35.6 如何识别网络故障

在检查计算机的网络连接时，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。确保您的网络电缆已正确插入计算机和路由器（或集线器等）。以太网连接器旁边的控制灯通常应全部激活。

如果连接失败，请检查网线在别的计算机上是否正常。如果正常，则可能是网卡引起了该问题。如果您的网络设置中有集线器或交换机，它们也可能有故障。

- 2 如果使用的是无线连接，请检查是否可与其他计算机建立此无线链接。如果没有，请联系无线网络的管理员。
- 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。如果本地计算机依赖于任何网络服务器进行身份验证，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计算机将无法“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 身份验证和 X 服务器功能。

NFS（文件服务）

如果任何应用程序所需的数据储存在 NFS 装入目录中，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 服务器发生故障而无法找到包含 `.gconf` 或 `.kde` 子目录的用户主目录，则该用户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）

如果任何应用程序需要储存在有故障的 Samba 服务器目录中的数据，它将不能启动或正常运行。

NIS（用户管理）

如果您的 SUSE Linux Enterprise Server 系统依赖有故障的 NIS 服务器提供用户数据，用户将无法登录此计算机。

LDAP（用户管理）

如果您的 SUSE Linux Enterprise Server 系统依赖有故障的 LDAP 服务器提供用户数据，用户将无法登录此计算机。

Kerberos（身份验证）

身份验证无法进行，登录至任何计算机都会失败。

CUPS（网络打印）

用户无法打印。

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/客户端设置，不涉及任何内部路由。假设服务器和客户端都是同一子网的成员，不需要额外的路由。

- 4a** 可使用 `ping IP 地址或主机名`（将主机名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，同时显示消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。可从其他计算机运行 `ping IP 地址或您的主机名` 命令来检查您的系统是否可达。如果可以 from 其他计算机访问您的计算机，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。要对该问题进行进一步的检查，请参见步骤

4b [528]。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。

- 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，用 YaST 网络设置模块（主机名/DNS 选项卡）调整此文件。

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。通常这些条目是 YaST 自动管理的，但最好谨慎地检查。

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。有关 DNS 的详细信息，请参见第 24 章 *域名系统* [309]。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计算机传递到其目标所经过的所有网关（跳跃）。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。

35.5.1 NetworkManager 问题

如果网络连接有问题，请按过程 35.6, “如何识别网络故障” [526] 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 用户身份打开外壳并登录。
- 2 重启动 NetworkManager:

```
rcnetwork restart -o nm
```
- 3 作为普通用户打开网页（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 26 章 *使用 NetworkManager* [349]。

35.6 数据问题

数据问题是指无论计算机是否能够正确引导，有一点是明确的，即系统上的数据损坏并且系统需要恢复。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 Server 提供了专用的 YaST 模块用于系统备份和恢复，此外还提供了一个救援系统，用于从外部恢复受损的系统。

35.6.1 管理分区映像

有时您需要从整个分区甚至硬盘来执行备份。Linux 附带了 `dd` 工具，后者可以用来创建磁盘的精确副本。与 `gzip` 一起使用可节约一些空间。

过程 35.7 备份和恢复硬盘

- 1 以用户 `root` 启动外壳。
- 2 选择源设备。通常形如 `/dev/sda`（标记为 `SOURCE`）。
- 3 确定要把您的映像储存在何处（标记为 `BACKUP_PATH`）。它不能与您的源设备相同。换句话说：如果从 `/dev/sda` 备份，则映像文件不得储存在 `/dev/sda` 下。
- 4 运行以下命令创建压缩映像文件：

```
dd if=/dev/SOURCE | gzip > /BACKUP_PATH/image.gz
```

- 5 用以下命令恢复硬盘：

```
gzip -dc /BACKUP_PATH/image.gz | dd of=/dev/SOURCE
```

如果您只需要备份某分区，将 `SOURCE` 占位符替换为您各自的分区。在这种情况下，映像文件可以位于同一硬盘上不同的分区中。

35.6.2 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消息，请选中向 *root* 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。

35.6.3 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、网络装入文件或可卸设备（如软盘或 DVD）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。

35.6.4 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 Server 提供两种不同方法来解决这些问题。您可以使用 YaST 系统修复功能，也可以引导救援系统。以下部分介绍这两种系统修复方法。

35.6.4.1 使用 YaST 系统修复

注意：键盘和语言设置

如果引导后更改了语言设置，您的键盘也随之调整。

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），在三个不同的方式中进行选择：

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 [533]。

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 [535]。

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所需的工具。有关详细信息，请参见“专家工具”一节 [536]。

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

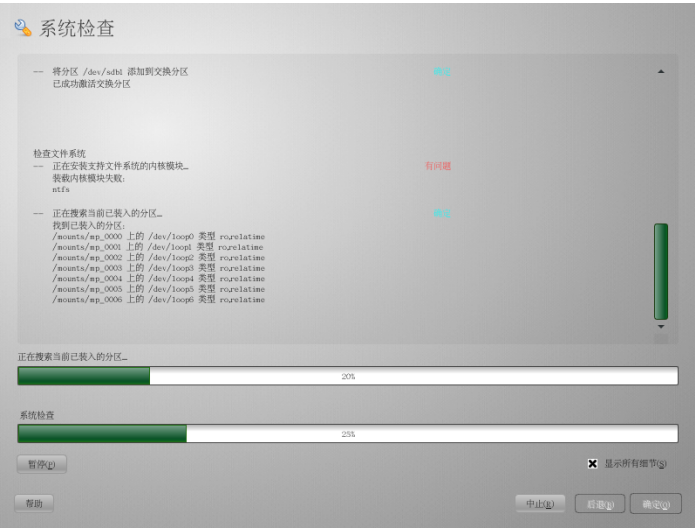
要启动 YaST 系统修复的自动修复方式，请如下执行操作：

- 1 将 SUSE Linux Enterprise Server 的安装媒体插入 DVD 驱动器中。
- 2 重引导系统。
- 3 在引导屏幕上选择 *修复已安装系统*。
- 4 确认许可协议并单击 *下一步*。

5 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 35.4 “自动修复方式” [534]。

图 35.4 自动修复方式



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：

检查分区表

检查所有检测到的硬盘的分区表的有效性和一致性。

检查交换区

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。

检查文件系统

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。

检查 fstab 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。

检查包数据库

这将检查执行最小安装的操作所需的所有包是否存在。虽然还可以分析基本包，但因为基本包数量太大，将花费很长时间。

检查引导加载程序配置

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 root 设备，并将检查 initrd 模块的可用性。

- 6 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消息。如果您确定拒绝建议的解决方案，您的系统将保持不变。

- 7 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 Server 的安装媒体插入 DVD 驱动器中。
- 2 重引导系统。
- 3 在引导屏幕上选择修复已安装系统。
- 4 确认许可协议并单击下一步。
- 5 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。YaST 不支持加密分区。如果您有加密分区，YaST 会通知您。

- 6 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消息。如果您确定拒绝建议的解决方案，您的系统将保持不变。

- 7 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 Server，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 将 SUSE Linux Enterprise Server 的安装媒体插入 DVD 驱动器中。
- 2 重引导系统。
- 3 在引导屏幕上选择**修复已安装系统**。
- 4 确认许可协议并单击**下一步**。
- 5 选择**导出工具**，再选择**修复选项**。
- 6 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：

安装新的引导加载程序

这将启动 YaST 引导加载程序配置模块。详细信息请参见第 10.2 节“使用 YaST 配置引导加载程序”[117]。

引导已安装系统

尝试引导已安装的 Linux 系统。

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。根据您的计算机速度和硬盘大小及速度，这可能要花一点时间。

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。

35.6.4.2 使用救援系统

SUSE Linux Enterprise Server 包含一个救援系统。该救援系统是一个小型 Linux 系统，可以装载到一个 RAM 磁盘并以 root 文件系统的形式装入，使您可以从外部访问 Linux 分区。使用该救援系统，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。
- 检查文件系统上的缺陷和启动自动修复进程。
- 访问“更改 root”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。
- 从安装有误的设备驱动程序或不可用内核恢复。

- 使用 `parted` 命令调整分区大小。在 GNU Parted 网站 <http://www.gnu.org/software/parted/parted.html> 上可以找到有关该工具的更多信息。

该救援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媒体上引导该救援系统：

- 1 将安装媒体插入 DVD 驱动器中。
- 2 重引导系统。
- 3 在引导屏幕上按 **F4** 并选择 *DVD-ROM*。然后从主屏幕选择救援系统。
- 4 在 **Rescue:** 提示符处输入 `root`。无需密码。

如果您的硬件安装不包含 DVD 驱动器，则可以从网络源引导救援系统。以下示例适用于远程引导的情形，如果使用另一引导媒体（例如 DVD），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 PXE 引导设置的配置，添加以下行：
`install=protocol://instsource` 和 `rescue=1`。但如果需要启动修复系统，请使用 `repair=1`。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 14.3.7 节“局域网唤醒”（第 14 章 远程安装, ↑部署指南）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。

一旦进入该救援系统，便可通过 **Alt + F1** 到 **Alt + F6** 键来使用虚拟控制台。

可以在 `/bin` 目录下找到外壳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`。

要查看系统消息，请使用命令 `dmesg` 或查看文件 `/var/log/messages`。

检查和操作配置文件

举一个可以通过该救援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。您可以通过救援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救援系统。
- 2 要在救援系统中装入位于 `/dev/sda6` 下的 `root` 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 `root` 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 从救援系统中卸载 `root` 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 `root` 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（请参见第 35.6.4.1 节“使用 YaST 系统修复”[533] 以了解细节）。但是，如果需要执行手动文件系统检查或修复，请引导救援系统。它包含检查并修复 `btrfs`、`ext2`、`ext3`、`ext4`、`reiserfs`、`xfs`、`dosfs` 和 `vfat` 文件系统的实用程序。

访问已安装系统

如果需要从救援系统访问已安装系统，需要在更改 `root` 环境中执行此操作。例如，修改引导加载程序配置或执行硬件配置实用程序。

要设置基于已安装系统的更改 **root** 环境，请执行以下步骤：

- 1 先从已安装系统和设备文件系统装入根分区（将设备名改为您当前的设置）：

```
mount /dev/sda6 /mnt
mount --bind /dev /mnt/dev
```

- 2 现在可以“更改 **root**”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 **root**”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。运行的内核是用救援系统引导的那个，不是用更改 **root** 环境引导的那个。它仅支持关键硬件，内核版本如果不完全一致，则无法从已安装系统中添加内核模块。始终用 `uname -r` 检查当前正在运行的（救援）内核版本，然后查明更改 **root** 环境中 `/lib/modules` 目录下是否有匹配的子目录。如果是，可以使用已安装模块；否则，需要提供其他媒体上的正确版本，比如 **USB** 记忆棒。很多时候，救援内核版本与已安装模块不同，这样您完全无法访问声卡等。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 **root**”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 [539] 中所述执行必要的步骤以访问已安装系统。
- 2 依据第 10 章 引导加载程序 *GRUB* [107] 中所述的 *GRUB* 配置原则，检查下列文件是否正确配置，如果需要进行修复。

- `/etc/grub.conf`
- `/boot/grub/device.map`
- `/boot/grub/menu.lst`
- `/etc/sysconfig/bootloader`

- 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 root”环境中注销并重引导该系统：

```
umount -a  
exit  
reboot
```

修复内核安装

内核更新会产生新的 **bug**，这样会影响系统运行。例如，系统某个硬件的驱动程序有故障，您就无法访问和使用该硬件。在这种情况下，需还原到上一个工作内核（如果在系统上可用），或从安装媒体安装原始内核。

提示：如何在更新后保留最后几个内核

为了防止内核更新出现故障后无法进行引导，请使用内核多版本功能，并告知 `libzypp` 在更新后保留哪些内核。

例如，要始终保留最后两个内核和当前正在运行的内核，请将

```
multiversion.kernels = latest,latest-1,running
```

添加到 `/etc/zypp/zypp.conf` 文件。

类似的情况是，当您需要重安装或更新不受 SUSE Linux Enterprise Server 支持的设备的已损坏驱动程序时。例如，当硬件供应商使用特定设备时，比如硬件 RAID 控制器，它需要一个二进制驱动程序才能被操作系统识别。供应商通常会发布含有固定版本或更新版本的必需驱动程序的驱动程序更新磁盘。

这两种情况下，您都需要以救援模式访问已安装系统，并修复内核相关问题，否则系统可能无法正确引导：

- 1 从 SUSE Linux Enterprise Server 安装媒体引导。
- 2 如果您正在从内核更新故障中恢复，请跳过此步骤。如果需要使用驱动程序更新磁盘(DUD)，请在出现引导菜单后按 F6 装载驱动程序更新，并选择驱动程序更新的路径或 URL，然后确认是。
- 3 从引导菜单中选择救援系统，并按 Enter。如果选择使用 DUD，将要求您指定储存驱动程序更新的位置。
- 4 在 Rescue：提示符处输入 root。无需密码。
- 5 手动将目标系统和“更改 root”装入新环境。有关详细信息，请参见“访问已安装系统”一节 [539]。
- 6 如果使用的是 DUD，请安装/重安装/更新有故障的设备驱动程序包。始终确保已安装的内核版本与您正在安装的驱动程序版本完全相同。

如果要修复有故障的内核更新安装，可以从安装媒体使用以下过程安装原始内核。

- 6a 使用 `hwinfo --cdrom` 命令确定您的 DVD 设备信息，使用 `mount /dev/sr0 /mnt` 命令装入设备。
- 6b 导航到 DVD 上储存内核文件的目录，例如，`cd /mnt/suse/x86_64/`。
- 6c 使用 `rpm -i` 命令安装具有您风格的必需 `kernel-*`、`kernel-*-base` 和 `kernel-*-extra` 包。
- 6d 安装完成后，检查与新安装内核相关的新菜单项是否已添加到引导加载程序配置文件（grub 的引导加载程序配置文件是 `/boot/grub/menu.lst`）。

- 7 更新配置文件，必要时可重初始化引导加载程序。有关详细信息，请参见“修改和重安装引导加载程序”一节 [540]。
- 8 从系统驱动器中删除所有可引导的媒体，然后重引导。

35.7 IBM System z：将 initrd 用作救援系统

如果升级或修改了 SUSE® Linux Enterprise Server for IBM System z 的内核，则可能会在不一致的状态下意外地重引导系统，这样会使已安装系统的标准 IPL 过程失败。之所以会出现这种情况，通常是因为已安装了新的或经过更新的 SUSE Linux Enterprise Server 内核，但尚未运行 `zip1` 程序来更新 IPL 记录。在这种情况下，请使用标准安装包作为救援系统，并从中执行 `zip1` 程序来更新 IPL 记录。

35.7.1 对救援系统执行初始程序装载

重要：使安装数据可用

为了使此方法生效，SUSE Linux Enterprise Server for IBM System z 安装数据必须为可用的。有关细节，请参见第 4.2.1 节“使安装数据可用”（第 4 章 在 *IBM System z* 上安装, ↑部署指南）。此外，您还需要设备的通道号和设备内包含 SUSE Linux Enterprise Server 安装的 `root` 文件系统的分区号。

首先，按照第 4.2 节“准备安装”（第 4 章 在 *IBM System z* 上安装, ↑部署指南）中所述对 SUSE Linux Enterprise Server for IBM System z 安装系统执行 IPL。随后将显示一个要使用的网络适配器的选择列表。

选择启动安装或系统，然后选择启动救援系统来启动救援系统。根据安装环境，现在必须确定网络调节器的参数和安装源。装载应急程序，并显示后面的登陆提示。

```
Skipped services in runlevel 3:  nfs nfsboot
```

```
Rescue login:
```

您可以作为 `root` 登录，而无需密码。

35.7.2 磁盘配置

在此情况下，没有做任何磁盘配置。需要在在能进入以前配置磁盘。

过程 35.8 配置 DASD

- 1 用以下的命令配置 DASD:

```
dasd_configure 0.0.0150 1 0
```

DASD 以 0.0.0150 连接。1 表示激活该磁盘（此位置若为 0 则将停用该磁盘）。0 表示磁盘“无 DIAG 模式”（1 使磁盘的 DAIG 访问可用）。

- 2 现在，DASD 为联机（用 `cat /proc/partitions` 检查），并可用于后续命令。

过程 35.9 配置 zFCP 磁盘

- 1 配置 zFCP 磁盘，首先要配置 zFCP 调节器。请使用以下命令完成该操作：

```
zfcps_host_configure 0.0.4000 1
```

0.0.4000 是调节器的连接目标通道 1 表示激活(0使调节器无效)。

- 2 调节器被激活后，可以配置磁盘。请使用以下命令完成该操作：

```
zfcps_disk_configure 0.0.4000 1234567887654321 8765432100000000 1
```

0.0.4000 是以前用的通道 ID, 1234567887654321 为 WWPN (国际端口号码 World wide Port Number), 而 8765432100000000 是 LUN (逻辑单位号码 logical unit number). 1 意味着激活该磁盘 (这里的 0 将使该磁盘无效)。

- 3 现在，zFCP 磁盘为联机（用 `cat /proc/partitions` 检查），并可用于后续命令。

35.7.3 装入 root 设备

如果所有所需设备都为联机，则现在应该能够装入 root 设备。假定 root 设备位于 DASD 设备的第 2 个分区 (`/dev/dasda2`)，则相应的命令是 `mount /dev/dasda2 /mnt`。

重要：文件系统一致性

如果没有正确关闭已安装系统，则最好在执行装入之前检查文件系统一致性。这样可避免意外丢失数据。在本例中，发出命令 `fsck /dev/dasda2` 以确保文件系统处于一致的状态。

通过只发布命令 `mount`，可以检查是否能够正确装入文件系统。

例 35.1 *Mount* 命令的输出

```
SuSE Instsys suse:/ # mount
shmfs on /newroot type shm (rw,nr_inodes=10240)
devpts on /dev/pts type devpts (rw)
virtual-proc-filessystem on /proc type proc (rw)
/dev/dasda2 on /mnt type reiserfs (rw)
```

35.7.4 更改为已装入的文件系统

为了使 `zipl` 命令从已安装系统的 `root` 设备而非救援系统读取配置文件，请使用 `chroot` 命令将 `root` 设备更改为已安装系统：

例 35.2 *chroot* 到已装入的文件系统

```
SuSE Instsys suse:/ # cd /mnt
SuSE Instsys suse:/mnt # chroot /mnt
```

35.7.5 执行 `zipl`

现在执行 `zipl` 用正确的值改写 IPL 记录。

例 35.3 使用 `zipl` 命令安装 IPL 记录

```
sh-2.05b# zipl
building bootmap : /boot/zipl/bootmap
adding Kernel Image : /boot/kernel/image located at 0x00010000
adding Ramdisk : /boot/initrd located at 0x00800000
adding Parmline : /boot/zipl/parmfile located at 0x00001000
Bootloader for ECKD type devices with z/OS compatible layout installed.
Syncing disks....
...done
```

35.7.6 退出救援系统

要退出救援系统，应首先使用 `exit` 退出由 `chroot` 命令打开的壳层。为了避免丢失任何数据，请使用 `sync` 命令将所有未使用的缓冲区清理到磁盘。现在更改为救援系统的 `root` 目录，然后卸载 SUSE Linux Enterprise Server for IBM System z 安装的 `root` 设备。

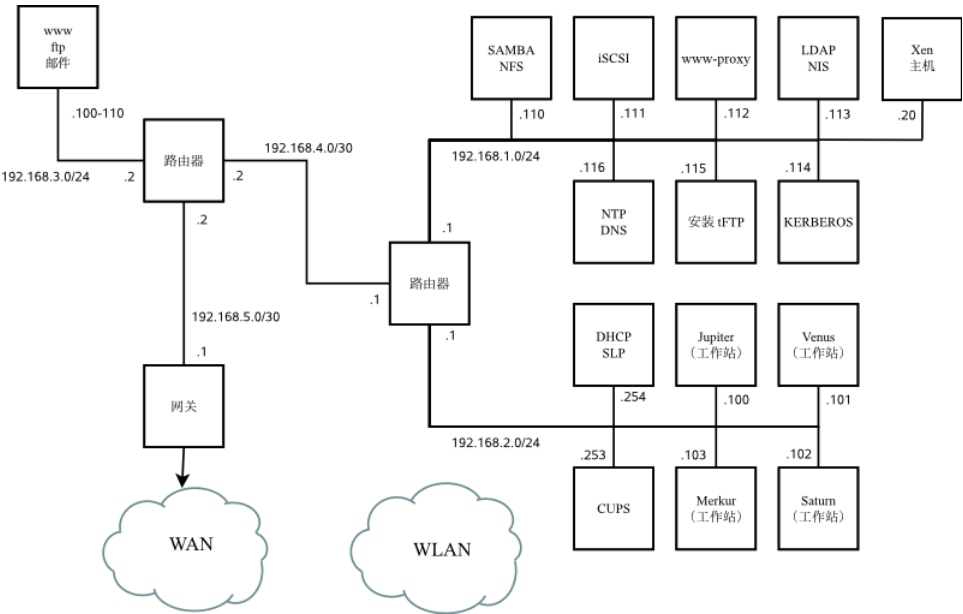
例 35.4 卸装文件系统

```
SuSE Instsys suse:/mnt # cd /  
SuSE Instsys suse:/ # umount /mnt
```

最后，使用 `halt` 命令暂停救援系统。现在便可以按照第 6.15.1 节“IBM System z：对已安装系统执行 IPL”（第 6 章 *使用 YaST 进行安装*, ↑*部署指南*）一章中的说明对 SUSE Linux Enterprise Server 系统进行初始程序装载了。

网络示例

此网络示例贯穿 SUSE® Linux Enterprise Server 文档的所有与网络相关的章节。





GNU Licenses

This appendix contains the GNU Free Documentation License version 1.2.

GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D Preserve all the copyright notices of the Document.
- E Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License, Version 1.2
or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled "GNU
Free Documentation License".
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

